

The background features a light gray gradient with several abstract elements: a large gear icon in the upper left, a network of thin gray lines connecting various colored circles (red, gray, orange) across the top, and large, thick, overlapping red and pink curved shapes at the bottom.

ORACLE®
Cloud Infrastructure

Getting Started Guide

11/26/2019

Copyright © 2016, 2019, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement

between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>.

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> or visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs> if you are hearing impaired.

CONTENTS

CHAPTER 1 Welcome to Oracle Cloud Infrastructure	8
Introduction	8
Key Concepts and Terminology	14
Oracle Cloud Infrastructure's Free Tier	18
CHAPTER 2 Signing Up and Signing In for the First Time	23
Signing Up for Oracle Cloud Infrastructure	23
Understanding the Sign-In Options	23
Signing In to the Console	30
CHAPTER 3 Using the Console	33
Understanding Compartments	33
CHAPTER 4 Changing Your Password	48
To Change Your Password	48
CHAPTER 5 Checking Your Balance and Usage	53
Required IAM Policy	53
Working with Costs Analysis Tools	53
CHAPTER 6 Adding Users	57
About Users, Groups, and Policies	57
About Oracle Identity Cloud Service Federated Users	57
Sample Users and Groups	58

Table of Contents

Add a User with Oracle Cloud Administrator Permissions	58
Create a Compartment and Add a User with Access to It	59
CHAPTER 7 Tutorial - Launching Your First Linux Instance	64
Task Flow to Launch an Instance	65
Creating a Key Pair	66
Choosing a Compartment	69
Creating a Virtual Cloud Network	72
Launching a Linux Instance	75
Connecting to Your Instance	78
Adding a Block Volume	81
Cleaning Up Resources from the Tutorial	86
CHAPTER 8 Tutorial - Launching Your First Windows Instance	88
Task Flow to Launch a Windows Instance	88
Choosing a Compartment	89
Creating a Virtual Cloud Network	91
Launching a Windows Instance	94
Connecting to Your Windows Instance	97
Adding a Block Volume to a Windows Instance	98
Cleaning Up Resources from the Tutorial	101
CHAPTER 9 Getting Started with the Command Line Interface	103
Getting Started with the Command Line Interface	103
CHAPTER 10 Getting Started with the Terraform Provider	132
Terraform Overview	132
Download and Install Terraform	132
Download the Oracle Cloud Infrastructure Terraform Provider	133
For More Information	133
CHAPTER 11 Getting Started with Load Balancing	134
Before You Begin	134

Table of Contents

Tutorial Overview	139
Add Two Subnets to Your VCN to Host Your Load Balancer	139
Create the Load Balancer	143
Create a Backend Set	145
Add Backends (Servers) to Your Backend Set	147
Create the Listener for Your Load Balancer	152
Update Load Balancer Security Lists and Allow Internet Traffic to the Listener	153
Verify Your Load Balancer	155
Update Rules to Limit Traffic to Backend Servers	156
Delete Your Load Balancer	158
CHAPTER 12 Putting Data into Object Storage	159
Creating a Bucket	159
Uploading Files to a Bucket	160
What's Next	161
CHAPTER 13 Getting Started with Audit	162
Prerequisite	162
Using Audit to View Events	163
CHAPTER 14 Getting Started with Oracle Platform Services	167
Supported Platform Services	167
Understand the Infrastructure Prerequisites	168
Learn About Service-Specific Differences and Workflows	168
CHAPTER 15 Getting Started with Oracle Applications	170
Support for Oracle Applications	170
CHAPTER 16 Setting Up Your Tenancy	171
Create a Plan	171
Understanding Compartments	171
Consider Who Should Have Access to Which Resources	173
Sample Approaches to Setting Up Compartments	174

Table of Contents

CHAPTER 17 Contacting Support	176
Getting Help and Contacting Support	176
CHAPTER 18 Frequently Asked Questions	189
GLOSSARY	198

CHAPTER 1 Welcome to Oracle Cloud Infrastructure

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

Introduction

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

About the Services

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

Analytics for Applications empowers you with industry-leading, AI-powered, self-service analytics capabilities for data preparation, visualization, enterprise reporting, augmented analysis, and natural language processing.

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

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

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

Use **Compute** to provision and manage bare metal compute instances. You can launch an Oracle bare metal compute resource in minutes. Provision instances as needed to deploy and run your applications, just as you would in your on-premises data center. Managed Virtual Machine (VM) instances are also available for workloads that don't require dedicated physical servers or the high-performance of bare metal instances.

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

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

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

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

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

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

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

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

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

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

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

You can control access to Oracle Cloud Infrastructure using **IAM Service**. Create and manage compartments, users, groups, and the policies that define permissions on resources.

Oracle **Integration** is a fully managed, preconfigured environment where you can integrate your applications, automate processes, and create applications. Use integrations to design, monitor, and manage connections between your applications, selecting from our portfolio of over 50 adapters to connect with Oracle and third-party applications.

The **Key Management** service helps you centrally manage the encryption of your data.

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

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

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

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

Object Storage provides high throughput storage for unstructured data. Object Storage service enables near infinite storage capacity for large amounts of analytic data, or rich

CHAPTER 1 Welcome to Oracle Cloud Infrastructure

content like images and videos. Block volumes can be backed up to Object Storage for added durability.

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

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

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

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

Accessing Oracle Cloud Infrastructure

You can create and manage resources in the following ways:

- **Oracle Cloud Infrastructure Console**

The Console is an intuitive, graphical interface that lets you create and manage your instances, cloud networks, and storage volumes, as well as your users and permissions. See [Understanding Compartments](#).

- **Oracle Cloud Infrastructure APIs**

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

- **SDKs**

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

- **Command Line Interface (CLI)**

You can use a command line interface with some services. For more information, see "Developer Tools" in the *Oracle Cloud Infrastructure User Guide*.

- **Terraform**

Oracle supports Terraform. Terraform is "infrastructure-as-code" software that allows you to define your infrastructure resources in files that you can persist, version, and share. For more information, see [Getting Started with the Terraform Provider](#).

- **Ansible**

Oracle supports the use of Ansible for cloud infrastructure provisioning, orchestration, and configuration management. Ansible allows you to automate configuring and provisioning your cloud infrastructure, deploying and updating software assets, and orchestrating your complex operational processes. For more information, see [Ansible Modules](#).

- **Resource Manager**

Resource Manager is an Oracle Cloud Infrastructure service that allows you to automate the process of provisioning your Oracle Cloud Infrastructure resources. It helps you install, configure, and manage resources using the "infrastructure-as-code" model. For more information, see [Overview of Resource Manager](#).

CHAPTER 1 Welcome to Oracle Cloud Infrastructure

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

How Do I Get Started?

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

Key Concepts and Terminology

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

BARE METAL HOST

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

CHAPTER 1 Welcome to Oracle Cloud Infrastructure

REGIONS AND AVAILABILITY DOMAINS

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

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

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

REALM

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

CONSOLE

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

TENANCY

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

COMPARTMENTS

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

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

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

VIRTUAL CLOUD NETWORK (VCN)

A virtual cloud network is a virtual version of a traditional network—including subnets, route tables, and gateways—on which your instances run. A cloud network resides within a single region but includes all the region's availability domains. Each subnet you define in the cloud network can either be in a single availability domain or span all the availability domains in the region (recommended). You need to set up at least one cloud network before you can launch instances. You can configure the cloud network with an optional internet gateway to handle public traffic, and an optional IPSec VPN connection or FastConnect to securely extend your on-premises network.

INSTANCE

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

IMAGE

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

SHAPE

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

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

KEY PAIR

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

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

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

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

BLOCK VOLUME

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

OBJECT STORAGE

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

BUCKET

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

ORACLE CLOUD IDENTIFIER (OCID)

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

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

Oracle Cloud Infrastructure's Free Tier

Oracle Cloud Infrastructure's Free Tier is composed of a free promotional trial that allows you to explore a wide range of Oracle Cloud Infrastructure products, and a set of Always Free offers that never expire.

Free Trial

The Free Trial provides you with \$300 of cloud credits that are valid for up to 30 days. You may spend these credits on any eligible Oracle Cloud Infrastructure service.

Getting Started

[Start for Free](#)

For more information, and to see a complete list of services available to you during the trial, visit the [Free Trial website](#).



Tip

During sign up, choose the home region carefully. Most Always Free resources can be provisioned only in your home region.

For security purposes, most users will need a mobile phone number and a credit card to create an account. Your credit card will not be charged unless you upgrade your account.

What Happens When Your Trial Period Ends

After your trial ends, your account remains active. There is no interruption to the availability of the [Always Free Resources](#) you have provisioned. You can terminate and re-provision Always Free resources as needed.

Paid resources that were provisioned with your credits during your free trial are reclaimed by Oracle unless you upgrade your account.

Pay as You Go accounts are available with no commitment, or contact an [Oracle sales representative](#) in your location to learn about monthly and annual flex accounts that offers discounted pricing. See the [pricing details](#) learn more.

Always Free Resources

All Oracle Cloud Infrastructure accounts (whether free or paid) have a set of resources that are free of charge for the life of the account. These resources display the **Always Free** label in the Console.

Using the Always Free resources, you can provision a [virtual machine \(VM\) instance](#), an [Oracle Autonomous Database](#), and the networking, load balancing, and storage resources needed to support the applications that you want build. With these resources, you can do things like run small-scale applications or perform proof-of-concept testing.

The following list summarizes the Oracle Cloud Always Free-eligible resources that you can provision in your tenancy:

- **Compute** (up to two instances)
- **Autonomous Database** (up to two database instances)
- **Load Balancing** (one load balancer)
- **Block Volume** (up to 100 GB total storage)
- **Object Storage** (up to 20 GiB)

For detailed information about the Always Free resources, see [Details of the Always Free Resources](#).

You can find your tenancy's limits for Always Free resources in the Console. To check these limits: Open the navigation menu. Under **Governance and Administration**, go to **Limits, Quotas and Usage**.

Quickly Spinning Up Your Environment Using Terraform

Oracle offers a Terraform configuration file that lets you automatically create the full set of Always Free resources in a few minutes. You don't need to have experience with Terraform to use this file. To set up your Oracle Cloud environment, you log in to your account and then upload the file in the Console using the [Resource Manager](#) service. Resource Manager reads

the file and provisions the Always Free resources for you with the settings and configuration you need to start creating applications in the cloud.

Note that Terraform refers to the set of resources being provisioned as a "stack". For a general introduction to Terraform and the "infrastructure-as-code" model, see [Terraform: Write, Plan, and Create Infrastructure as Code](#).

To provision your Always Free using Terraform and Resource Manager

1. Download the Always Free Terraform configuration file (a .zip file) to your computer. To do this, navigate to <https://github.com/oracle/oci-quickstart-cloudnative> and follow the instructions in the `readme.md` file included in this repository.
2. Log into your Oracle Cloud Infrastructure account.
3. Open the navigation menu. Under **Solutions and Platform**, go to **Resource Manager** and click **Stacks**.
4. Click the **Create Stack** button to open the **Create Stack** dialog.
5. Add your downloaded configuration (.zip) file, either by dragging and dropping it onto the dialog's control, or by clicking **Browse** and navigating to the file location.
6. Optionally, provide a name for the new stack. If you don't provide a name, a default name is provided on the server.
7. Optionally, provide a description for the stack.
8. Optionally, select a different compartment from your current compartment in which to create the stack. To do so, select a compartment from the **Create In Compartment** drop-down.
9. Click **Next** to proceed to the **Configure Variables** panel.
10. The variables displayed in the **Configure Variables** panel are auto-populated from the Terraform file that you uploaded. You don't need to change these variables if you are provisioning your Always Free resources using the Terraform file provided by Oracle.
11. Click **Next** to proceed to the **Review** panel.
12. Verify your stack configuration, then click **Create** to create your stack.

Your set of Always Free resources should take no more than a few minutes to provision.

Upgrading to a Paid Account

You can upgrade to a paid account at any time through the Oracle Cloud Infrastructure Console. To do so, click the **Upgrade** link in the banner at the top of the Console web page. If you don't see an **Upgrade** link on the page you are viewing, you can click the **Oracle Cloud** logo at the top of the Console and then look for the Upgrade link in the sidebar on the right side of the Console home page.

Additional Information

See [Frequently Asked Questions: Oracle Cloud Infrastructure Free Tier](#) for answers to your questions about Free Tier accounts and resources.

CHAPTER 2 Signing Up and Signing In for the First Time

This chapter explains how to get Oracle Cloud Infrastructure and sign in to the Console for the first time.

Signing Up for Oracle Cloud Infrastructure

You can sign up for Oracle Cloud Infrastructure in the following ways:

- Contact your Oracle sales representative.
Your Oracle sales representative can provide you information about the pricing options available to your company.
- Go to https://cloud.oracle.com/en_US/tryit and sign up for the *Oracle Free Trial*.
When your request is processed, you will be provisioned a *tenancy* in Oracle Cloud Infrastructure. Oracle will send you a Welcome email with instructions for signing in to the Console for the first time. There is no charge unless you choose to **Upgrade to Paid**.

Understanding the Sign-In Options

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

About the Sign In Options

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

Sign Up for Free Oracle Cloud Promotion

Get \$300 of free credits for up to 3500 hours of Oracle Cloud usage for the next 30 days

User Name:
me@example.com

Password:
<signup password>

Complete Sign-up

Need help? Contact [Chat support](#)

**The sign up process
creates your user in two
identity systems**



**Oracle Cloud Infrastructure
IAM Service**

User Name: me@example.com
Password: <signup password>



Oracle Identity Cloud Service

User Name: me@example.com
Password: <signup password>

**The same username
and password you
chose are
provisioned in both
systems**

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

Oracle Cloud Infrastructure IAM

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

Oracle Identity Cloud Service

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

✓

Important

After the users are created, you manage them separately.

For example, if you change the password in IAM

It is not changed in IDCS

Oracle Cloud Infrastructure IAM Service
User Name: me@example.com
Password: <UPDATED password>

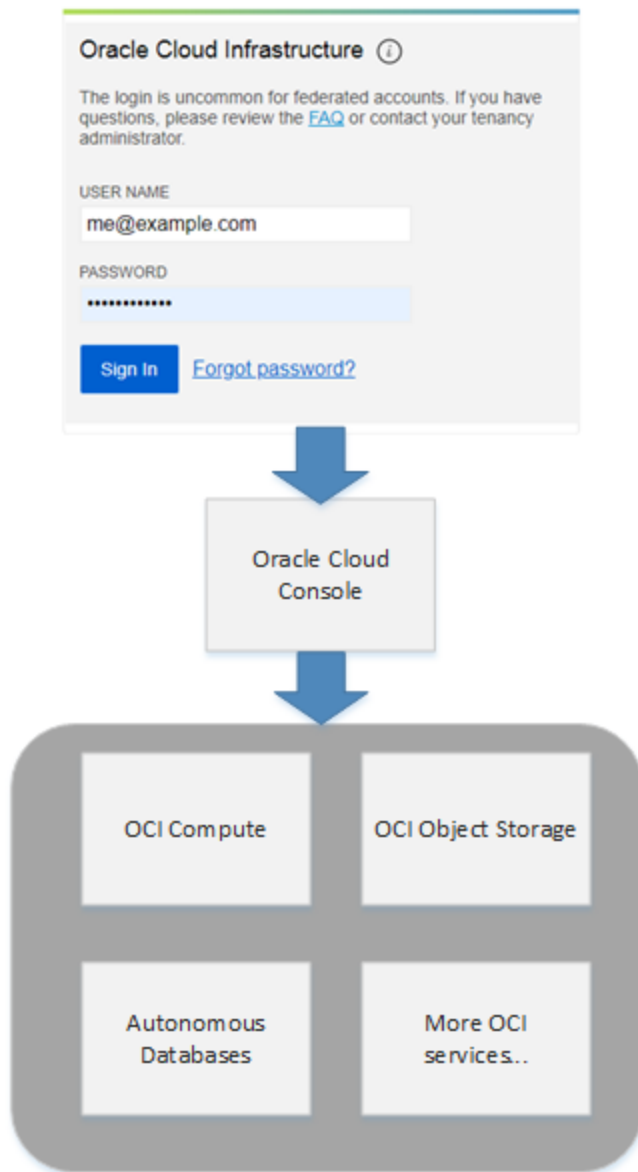
Oracle Identity Cloud Service
User Name: me@example.com
Password: <signup password>

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

When to Use Each Sign-In Option

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

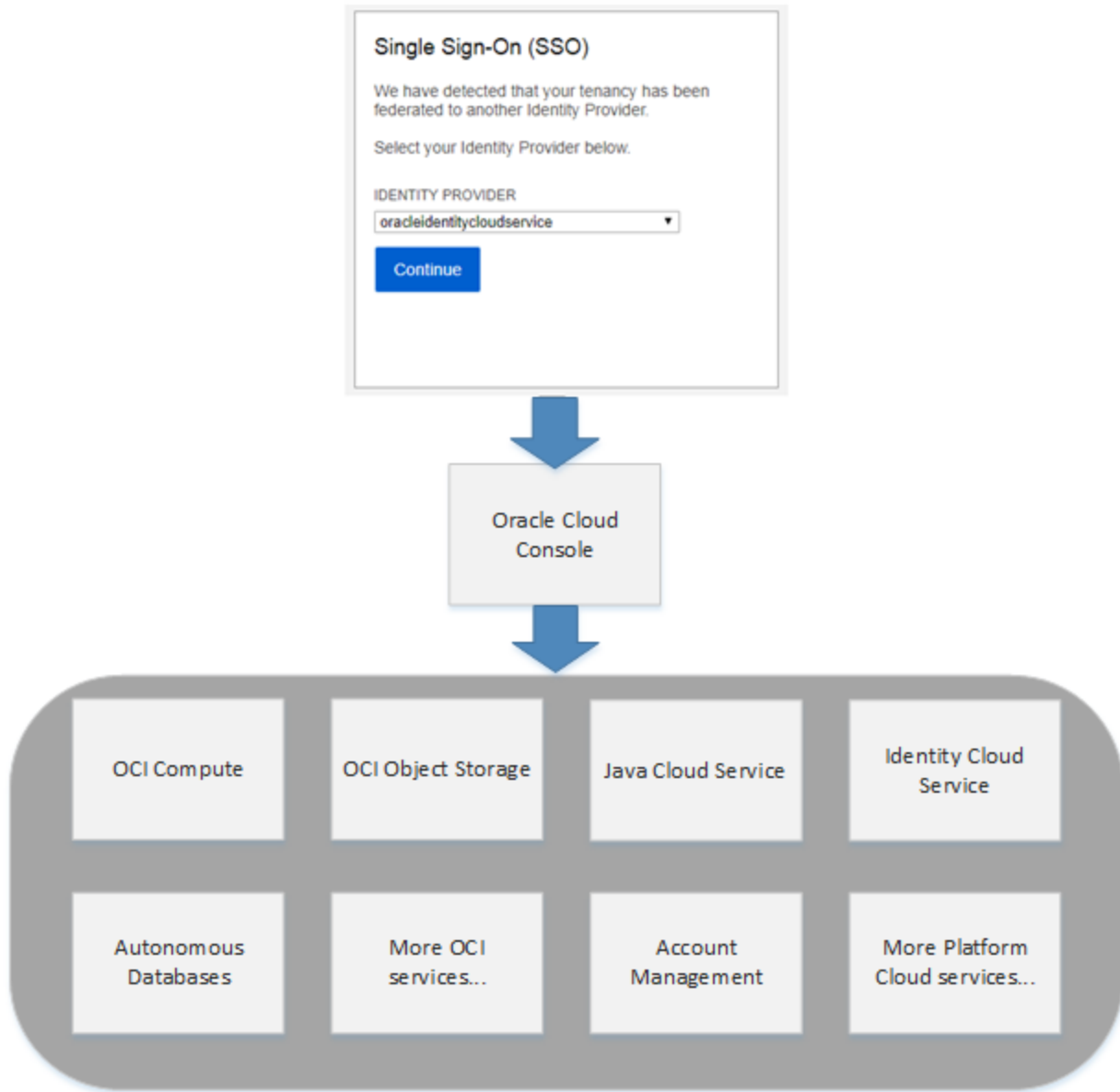
Oracle Cloud Infrastructure sign-on allows access to OCI services only



CHAPTER 2 Signing Up and Signing In for the First Time

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

Oracle Identity Cloud Service sign-on allows access to Oracle Cloud Infrastructure AND other cloud services



More Information About Managing Users in Oracle Cloud Identity Providers

[Managing Users in the IAM Service](#)

[Managing Oracle Identity Cloud Service Users and Groups in the Oracle Cloud Infrastructure Console](#)

[About Users, Groups, and Policies](#)

Signing In to the Console

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

Supported Browsers

Oracle Cloud Infrastructure supports the latest desktop versions of Google Chrome, Microsoft Edge, Internet Explorer 11, Safari, Firefox, and Firefox ESR. Note that private browsing mode is not supported for Firefox, Internet Explorer, or Edge. Mobile browsers are not supported.

Signing In for the First Time

To sign in to Oracle Cloud at <https://www.oracle.com/cloud/sign-in.html>, you need:

- Your cloud account name
- User name and password

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

1. Open a supported browser and go to <https://www.oracle.com/cloud/sign-in.html>.
2. Click **Sign In**.
3. Enter your **Cloud Account Name** and click **Next**.

CHAPTER 2 Signing Up and Signing In for the First Time

4. Enter your user name and temporary password from your welcome email. You will be prompted to change your temporary password.

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

About the Console URL

Alternatively, you can sign in directly to Oracle Cloud Infrastructure using the Console URL. When you sign up to use Oracle Cloud Infrastructure, you receive a customized URL for your organization. For example,

<https://console.us-ashburn-1.oraclecloud.com/?tenant=CompanyABC>

If you instead use the base URL (for example: <https://console.us-ashburn-1.oraclecloud.com>), you are prompted to specify your tenant (or cloud account name) on the sign-in page, along with your user name and password.

List of regional Console URLs

- <https://console.ap-mumbai-1.oraclecloud.com>
- <https://console.ap-seoul-1.oraclecloud.com>
- <https://console.ap-sydney-1.oraclecloud.com>
- <https://console.ap-tokyo-1.oraclecloud.com>
- <https://console.ca-toronto-1.oraclecloud.com>
- <https://console.eu-frankfurt-1.oraclecloud.com>
- <https://console.eu-zurich-1.oraclecloud.com>
- <https://console.sa-saopaulo-1.oraclecloud.com>
- <https://console.uk-london-1.oraclecloud.com>
- <https://console.us-ashburn-1.oraclecloud.com>
- <https://console.us-phoenix-1.oraclecloud.com>

Next Steps

Get to know the Console. See [Understanding Compartments](#).

Follow guided tutorials to [launch your first instance](#), [add users](#), or [put data into object storage](#).

Begin setting up your tenancy for other users. See [Create a Plan](#).

CHAPTER 3 Using the Console

This topic describes basic information about the Oracle Cloud Infrastructure Console.

To access the Console, you must use a [supported browser](#).

When you [sign in](#) to the Console you'll see the home page. The home page gives you quick links to the documentation and to Oracle Support. Use the service tabs in the upper right to create, manage, and view your cloud resources.

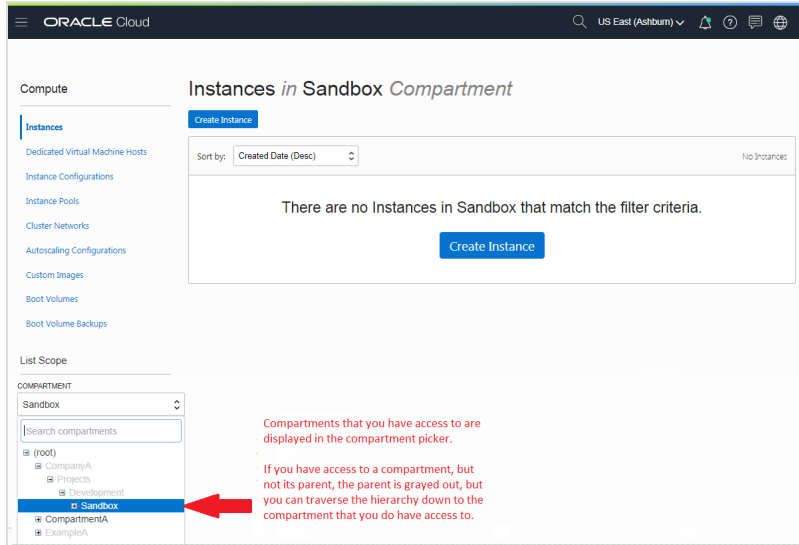
Understanding Compartments

After you select a service, you'll notice the compartments list on the left.

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

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

CHAPTER 3 Using the Console



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

For more details about compartments, see [Create a Plan](#) and [Managing Compartments](#).

Navigating to Oracle Cloud Infrastructure Services

Open the navigation menu in the upper left to work with related services and resources. For example, open the navigation menu and click **Compute** to work with the Compute service and compute instances.

To familiarize yourself with the Compute, Networking, and Block Volume services by following a guided workflow, see [Tutorial - Launching Your First Linux Instance](#).

To learn more about a specific service, see the appropriate topic in the *Oracle Cloud Infrastructure User Guide*.

- Analytics Cloud empowers business analysts and consumers with modern, AI-powered, self-service analytics capabilities for data preparation, visualization, enterprise reporting, augmented analysis, and natural language processing. To work with this service: Open the navigation menu. Under **Solutions and Platform**, go to **Analytics** and click **Analytics Cloud**.
- Analytics for Applications empowers you with industry-leading, AI-powered, self-service analytics capabilities for data preparation, visualization, enterprise reporting, augmented analysis, and natural language processing. After you meet the prerequisites, you can navigate to this service as follows: Open the navigation menu. Under **Solutions and Platform**, go to **Analytics** and click **Analytics Apps for Fusion**. See *Administering Oracle Analytics for Applications*.
- Archive Storage helps you store data that is accessed infrequently and requires long retention periods. To work with this service: Open the navigation menu. Under **Core Infrastructure**, click **Object Storage**. See "Overview of Archive Storage" in the *Oracle Cloud Infrastructure User Guide*.
- The Audit service helps you track activity in your environment. To work with this service: Open the navigation menu. Under **Governance and Administration**, go to **Governance** and click **Audit**. See "Overview of Audit" in the *Oracle Cloud Infrastructure User Guide*.
- Block Volume helps you dynamically provision and manage block storage volumes. To work with this service: Open the navigation menu. Under **Core Infrastructure**, go to **Block Storage** and click **Block Volumes**. See "Overview of Block Volume" in the *Oracle Cloud Infrastructure User Guide*.
- The Compute service helps you provision and manage compute hosts, known as *instances*, to meet your compute and application requirements. To work with this service: Open the navigation menu. Under **Core Infrastructure**, go to **Compute** and click **Instances**. See "Overview of the Compute Service" in the *Oracle Cloud Infrastructure User Guide*.
- Container Engine for Kubernetes helps you define and create Kubernetes clusters to enable the deployment, scaling, and management of containerized applications. To work with this service: Open the navigation menu. Under **Solutions and Platform**, go

to **Developer Services** and click **Container Clusters**. See "Overview of Container Engine for Kubernetes" in the *Oracle Cloud Infrastructure User Guide*.

- Content and Experience is a cloud-based content hub to drive omni-channel content management and accelerate experience delivery. It offers powerful collaboration and workflow management capabilities to streamline the creation and delivery of content and improve customer and employee engagement. To work with this service, open the navigation menu. Under the **Solutions and Platform** group, go to **Application Integration** and click **Content and Experience**.
- Data Safe is a fully-integrated Cloud service focused on the security of your data. It provides a complete and integrated set of features for protecting sensitive and regulated data in Oracle Cloud databases. Features include Security Assessment, User Assessment, Data Discovery, Data Masking, and Activity Auditing. To work with this service, Open the navigation menu. Under **Database**, click **Data Safe**.
- Data Transfer helps you easily and securely migrate your data in an offline manner to Oracle Cloud Infrastructure. To work with this service: Open the navigation menu. Under **Core Infrastructure**, go to **Object Storage** and click **Data Transfer**. See "Overview of Data Transfer" in the *Oracle Cloud Infrastructure User Guide*.
- The Database service helps you provision and manage Oracle databases. To work with this service: Open the navigation menu. Under **Database**, click **Bare Metal, VM, and Exadata**. See "Overview of the Database Service" in the *Oracle Cloud Infrastructure User Guide*.
- Digital Assistant is a platform that allows you to create and deploy digital assistants, which are AI-driven interfaces that help users accomplish a variety of tasks in natural language conversations. To work with this service: Open the navigation menu. Under **Data and AI**, click **Digital Assistant**.
- The DNS service helps you create and manage your DNS zones. To work with this service: Open the navigation menu. Under **Core Infrastructure**, go to **Networking** and click **DNS Zone Management**. See "Overview of the DNS Service" in the *Oracle Cloud Infrastructure User Guide*.
- The Email Delivery service helps you send large volume email and ensure that your message reaches your recipients' inboxes. To work with this service: Open the

navigation menu. Under **Solutions and Platform**, go to **Email Delivery**. See "Overview of the Email Delivery Service" in the *Oracle Cloud Infrastructure User Guide*.

- The Events service helps you create automation in your tenancy. To work with this service: Open the navigation menu. Under the **Solutions and Platform** group, go to **Application Integration** and click **Events Service**. See "Overview of Events" in the *Oracle Cloud Infrastructure User Guide*.
- The File Storage service helps you manage shared file systems, mount targets, and snapshots. To work with this service: Open the navigation menu. Under **Core Infrastructure**, click **File Storage**. See "Overview of File Storage" in the *Oracle Cloud Infrastructure User Guide*.
- The Functions service helps you build and deploy applications and functions. To work with this service: Open the navigation menu. Under **Solutions and Platform**, go to **Developer Services** and click **Functions**. See "Overview of Functions" in the *Oracle Cloud Infrastructure User Guide*.
- The Health Checks service helps you monitor the health of your endpoints. To work with this service: Open the navigation menu. Under **Solutions and Platform**, go to **Monitoring** and click **Health Checks**. See "Overview of the Health Checks Service" in the *Oracle Cloud Infrastructure User Guide*.
- The IAM service helps you set up administrators, users, and groups and specify their permissions. To work with this service: Open the navigation menu. Under **Governance and Administration**, click **Identity**. See "Overview of IAM" in the *Oracle Cloud Infrastructure User Guide*.
- Integration is a fully managed service that allows you to integrate your applications, automate processes, and create visual applications.
- The Key Management service helps you centrally manage the encryption of your data. To work with this service: Open the navigation menu. Under the **Governance and Administration** group, go to **Security** and click **Key Management**. See "Overview of Key Management" in the *Oracle Cloud Infrastructure User Guide*.
- Load Balancing helps you create a regional load balancer within your VCN. To work with this service: Open the navigation menu. Under the **Core Infrastructure** group, go to

Networking and click **Load Balancers**. See "Overview of Load Balancing" in the *Oracle Cloud Infrastructure User Guide*.

- Monitoring helps you monitor the health, capacity, and performance of your cloud resources by querying metrics and managing alarms. To work with this service: Open the navigation menu. Under **Solutions and Platform**, go to **Monitoring**. See "Overview of Monitoring" in the *Oracle Cloud Infrastructure User Guide*.
- Networking helps you set up virtual versions of traditional network components. To work with this service: Open the navigation menu. Under **Core Infrastructure**, go to **Networking** and click **Virtual Cloud Networks**. See "Overview of Networking" in the *Oracle Cloud Infrastructure User Guide*.
- Notifications helps you publish messages using topics and subscriptions. To work with this service: Open the navigation menu. Under **Solutions and Platform**, go to **Application Integration** and click **Notifications**. See "Overview of Notifications" in the *Oracle Cloud Infrastructure User Guide*.
- Object Storage helps you manage data as objects stored in containers. To work with this service: Open the navigation menu. Under **Core Infrastructure**, click **Object Storage**. See "Overview of Object Storage" in the *Oracle Cloud Infrastructure User Guide*.
- Registry helps you store, share, and manage development artifacts like Docker images in an Oracle-managed registry. To work with this service: Open the navigation menu. Under **Solutions and Platform**, go to **Developer Services** and click **Registry**. See "Overview of Registry" in the *Oracle Cloud Infrastructure User Guide*.
- Resource Manager helps you install, configure, and manage resources using the "infrastructure-as-code" model. To work with this service: Open the navigation menu. Under **Solutions and Platform**, go to **Resource Manager** and click **Stacks** or **Jobs**. See "Overview of Resource Manager" in the *Oracle Cloud Infrastructure User Guide*.
- The Traffic Management Steering Policies service helps you guide traffic to your endpoints based on various conditions, including endpoint health and the geographic origins of DNS requests. To work with this service: Open the navigation menu. Under **Core Infrastructure**, go to **Networking** and click **Traffic Management Steering Policies**. See "Overview of the Traffic Management Steering Policies Service" in the

Oracle Cloud Infrastructure User Guide.

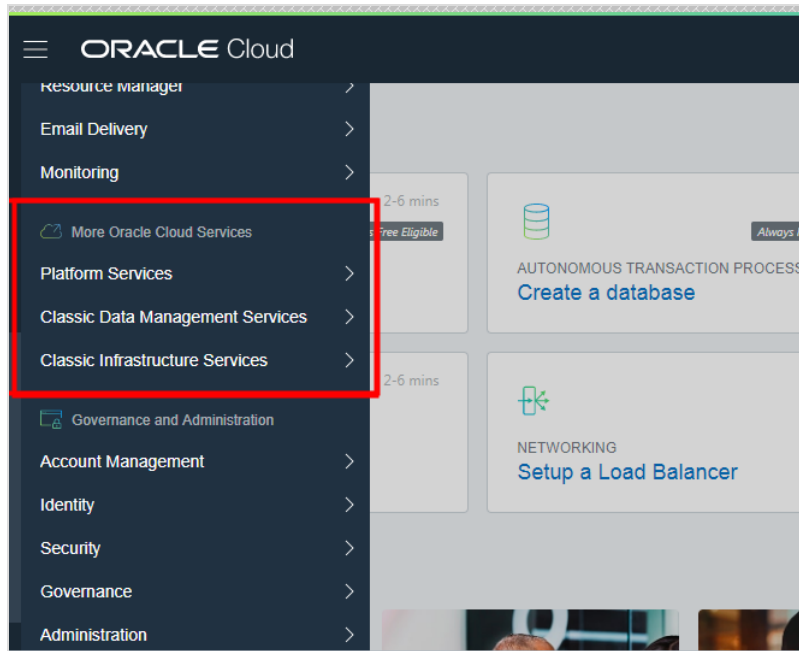
- The WAF service helps you to make your endpoints more secure by monitoring and filtering out potentially malicious traffic. To work with this service: Open the navigation menu. Under **Governance and Administration**, go to **Security** and click **WAF Policies**. See "Overview of the Web Application Firewall Service" in the *Oracle Cloud Infrastructure User Guide*.
- The WAF service helps you to make your endpoints more secure by monitoring and filtering out potentially malicious traffic. To work with this service: Open the navigation menu. Under **Governance and Administration**, go to **Security** and click **WAF Policies**. See "Overview of Work Requests" in the *Oracle Cloud Infrastructure User Guide*.

Navigating to More Oracle Cloud Services from the Console

For more details about accessing other Oracle Cloud offerings, see [Navigate to Your Cloud Services](#).

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

If your account also has Oracle Cloud Platform services, Oracle Cloud Infrastructure Classic services or Oracle Cloud Applications, then you can navigate to these services from the Oracle Cloud Console:



Navigating to Platform Services

Open the navigation menu. Under **More Oracle Cloud Services**, go to **Platform Services** and click the service you want to access.

Navigating to Classic Data Management Services

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

Navigating to Classic Infrastructure Services

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

Navigating to the Applications Console

If your Cloud account also has Cloud Applications services provisioned, then you'll have access to the Applications Console.

In the Console header, click **Applications** to switch to the Applications Console.

For more information about the consoles for these Oracle Cloud services, see [About the Consoles](#).

Filtering the Displayed List of Resources

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

Filters include:

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

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

Availability Domain: For resources that reside in a single availability domain, you can limit the list to the resources that reside in the availability domains you select. For a list of availability domain-specific resources, see [Resource Availability](#).

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

To filter a list of resources by a defined tag

1. Next to **Tag Filters**, click **add**.

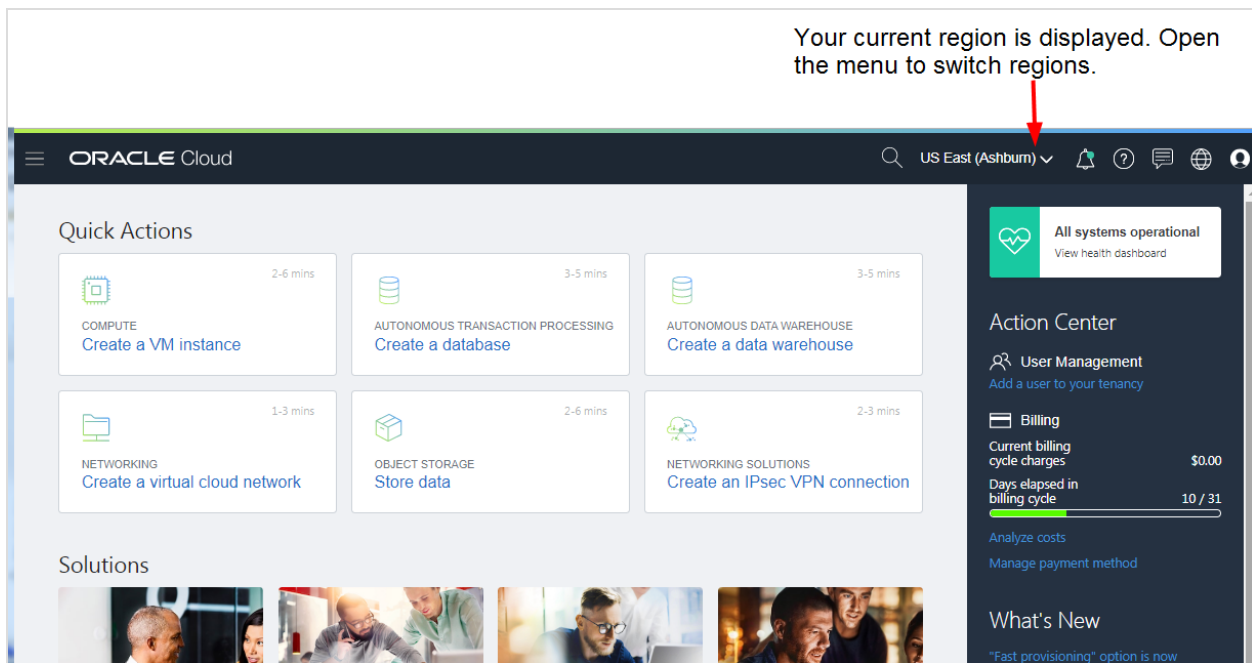
2. In the **Apply a Tag Filter** dialog, enter the following:
 - a. **Namespace:** Select the tag namespace.
 - b. **Key:** Select a specific key.
 - c. **Value:** Select from the following:
 - **Match Any Value** - returns all resources tagged with the selected namespace and key, regardless of the tag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

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

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

Switching Regions

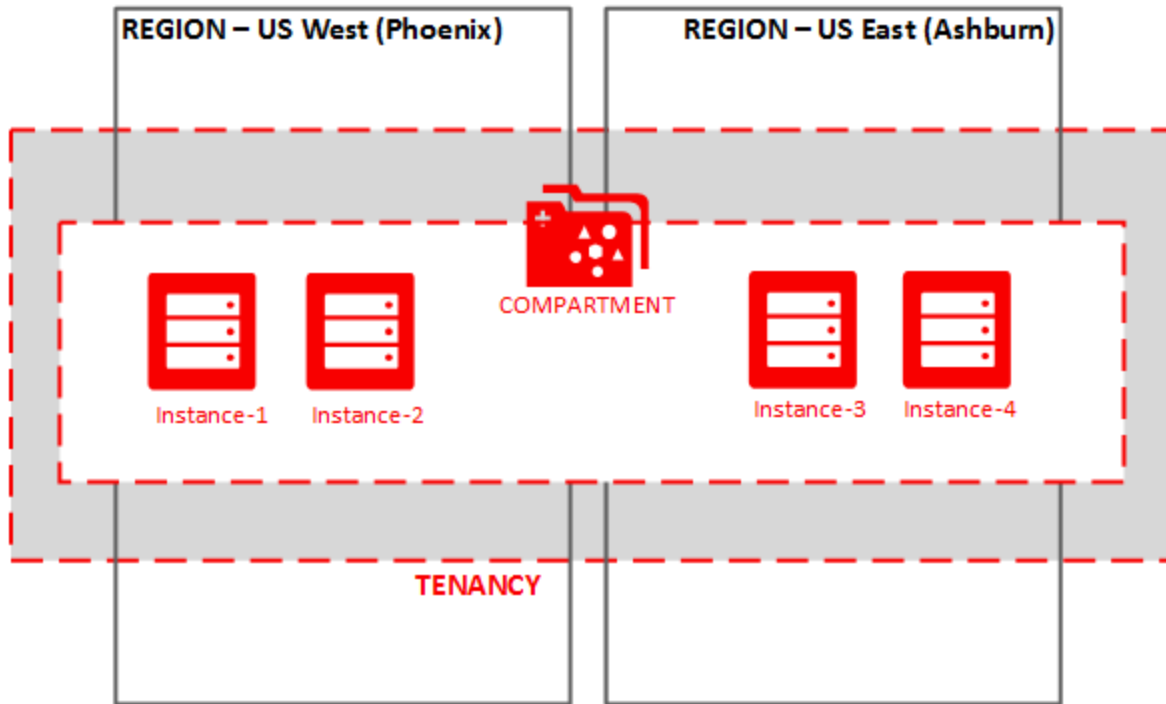
Your current region is displayed at the top of the Console. If your tenancy is subscribed to multiple regions, you can switch regions by selecting a different region from the **Region** menu.



Working Across Regions

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

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



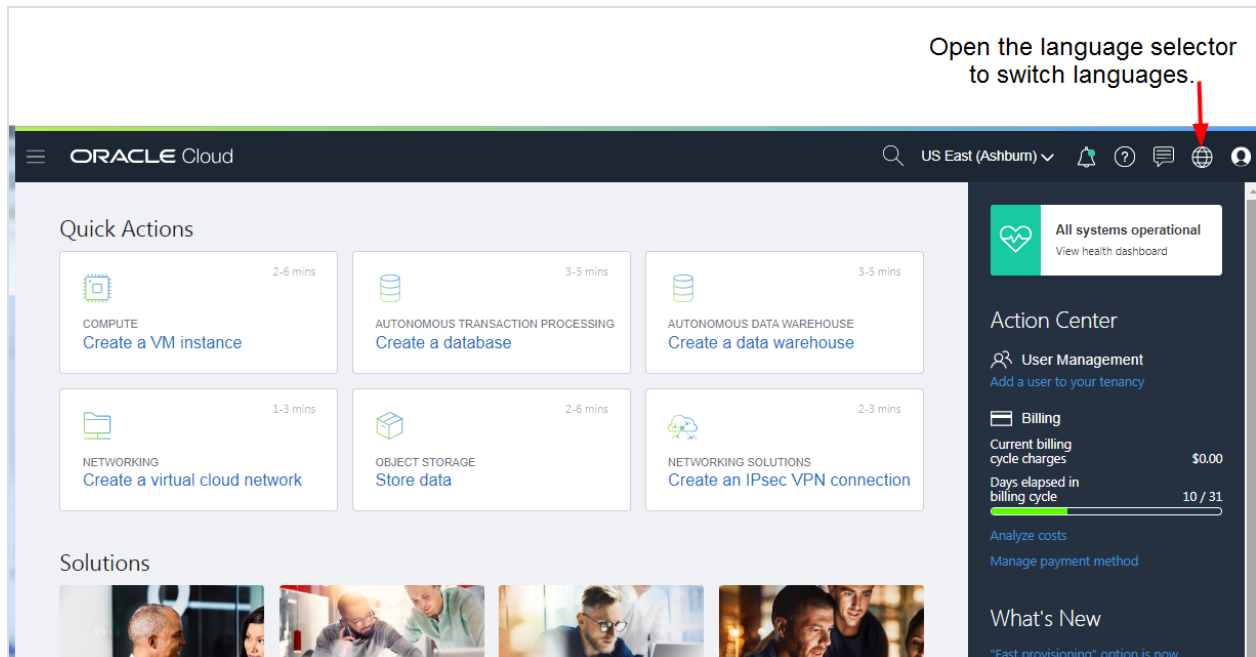
To view resources across regions that are in a specific compartment, you can use the [compartment explorer](#).

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

Switching Languages

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

CHAPTER 3 Using the Console



The language selector supports the following languages:

- Chinese (Simplified)
- Chinese (Traditional)
- Croatian
- Czech
- Danish
- Dutch
- English
- Finnish
- French (Canada)
- French (Europe)
- German

- Greek
- Hungarian
- Italian
- Japanese
- Korean
- Norwegian
- Polish
- Portuguese (Brazil)
- Portuguese (Portugal)
- Romanian
- Russian
- Serbian
- Slovak
- Slovenian
- Spanish
- Swedish
- Thai
- Turkish

The language you choose persists between sessions. However, the language setting is specific to the browser. If you change to a different browser, the Console displays text in the language last selected in the language selector. If it's the first time you're viewing the Console in a particular browser, the Console displays content according to the browser's language setting.

Entering Information to the Console



Warning

Avoid entering confidential information when assigning descriptions, tags, or friendly names to your cloud resources through the Oracle Cloud Infrastructure Console, API, or CLI.

Chat Online with an Oracle Representative

If you've signed up for an Oracle Cloud Free Trial, use the online chat to get help. If you've purchased Oracle Cloud services, it's recommended that you use [My Oracle Support](#) to get help.

To start a live online chat with an Oracle Support or Sales representative, do any of the following:

- Click the **Live Chat** icon at the top of the Console.
- Click the **Help** menu (🔍) and then select **Live Chat** from the menu.

Follow the prompts in the chat box to interact with an Oracle agent.

Signing Out

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

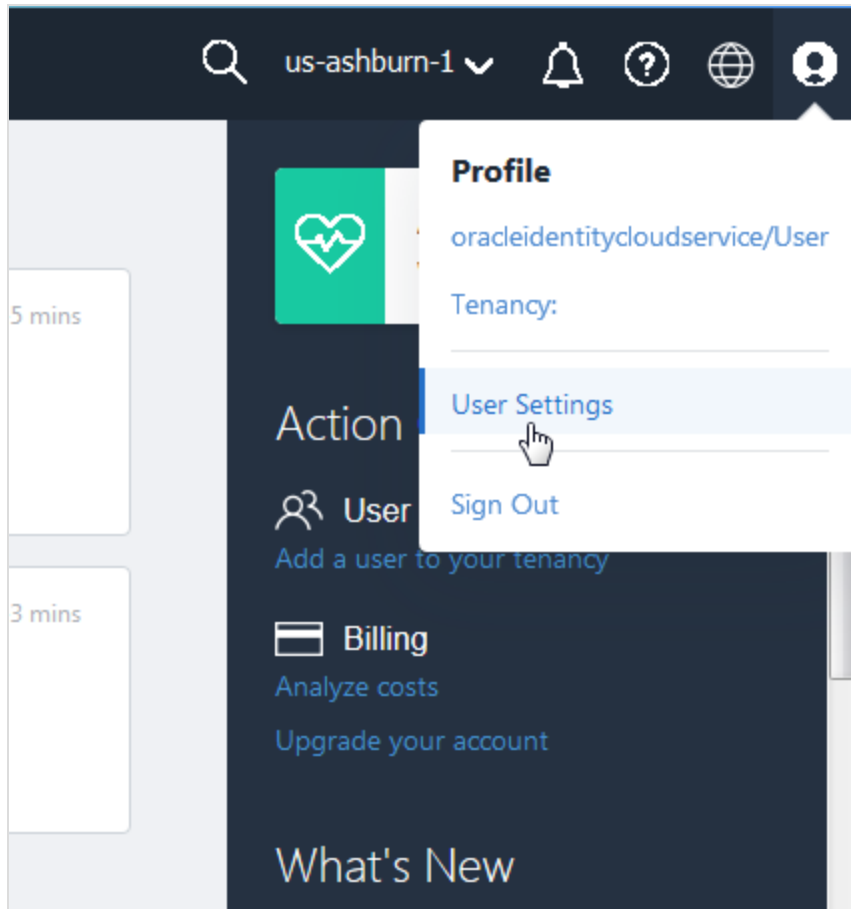
CHAPTER 4 Changing Your Password

This topic describes how users can change their own passwords.

To Change Your Password

Procedure for Oracle Identity Cloud Service users

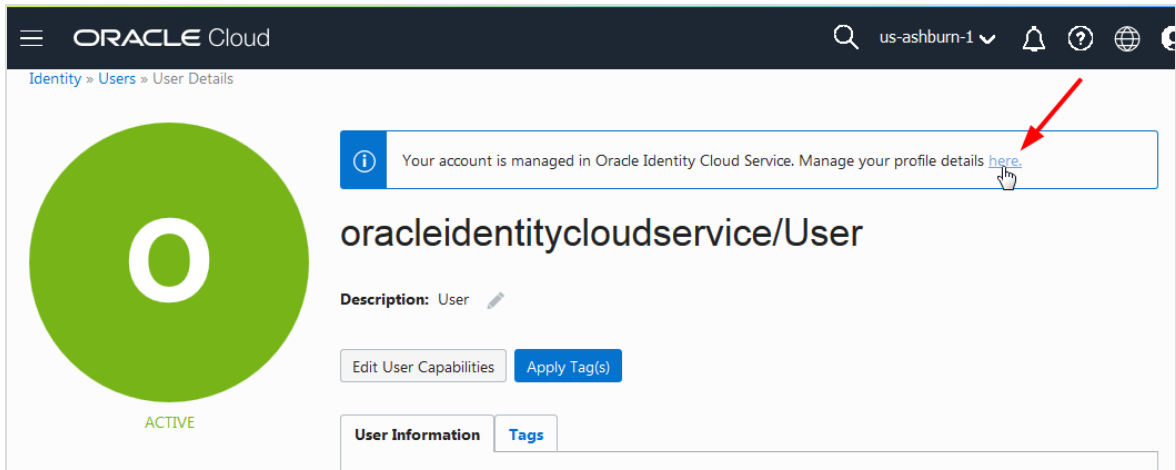
1. Open the **Profile** menu () and click **User Settings**.



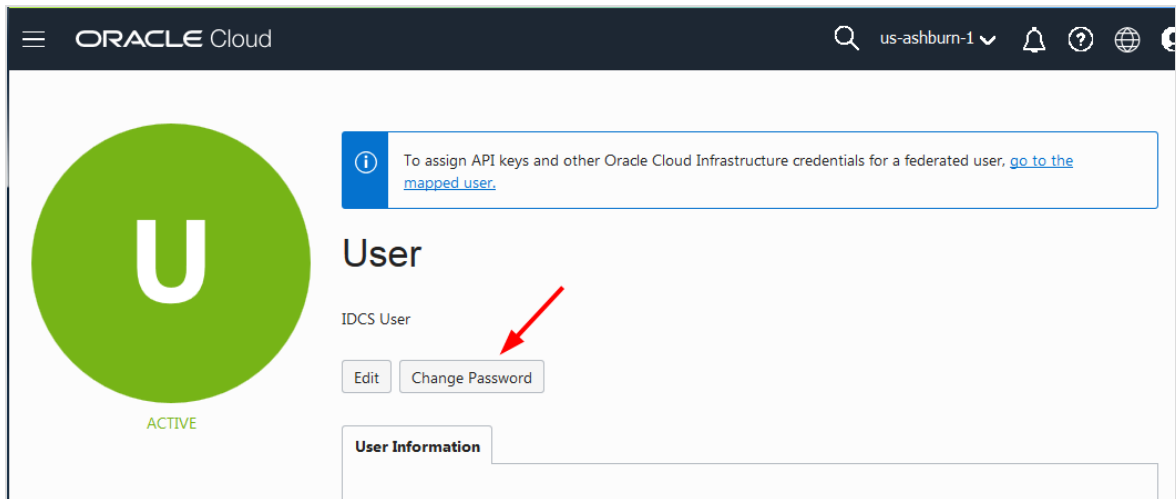
Your Oracle Cloud Infrastructure IAM service **User Details** page is displayed. Notice that your username is prefixed with the name of your IDCS federation, for example: `oracleidentitycloudservice/User`

2. The information banner at the top of the page tells you that your account is managed in Oracle Identity Cloud Service. Click the **here** link.

CHAPTER 4 Changing Your Password



3. Your Identity Cloud Service **User Details** page is displayed. Notice that on this page, your username is displayed without the prefix.



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

Procedure for local Oracle Cloud Infrastructure users

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

Signing in to cloud tenant:
ABCCorp
[Change tenant](#)

Single Sign-On (SSO)

We have detected that your tenancy has been federated to another Identity Provider.

Select your Identity Provider below and log in.

IDENTITY PROVIDER
OracleIdentityCloudService

[Continue](#)

Oracle Cloud Infrastructure

The login is uncommon for federated accounts. If you have questions, please contact your tenancy administrator.

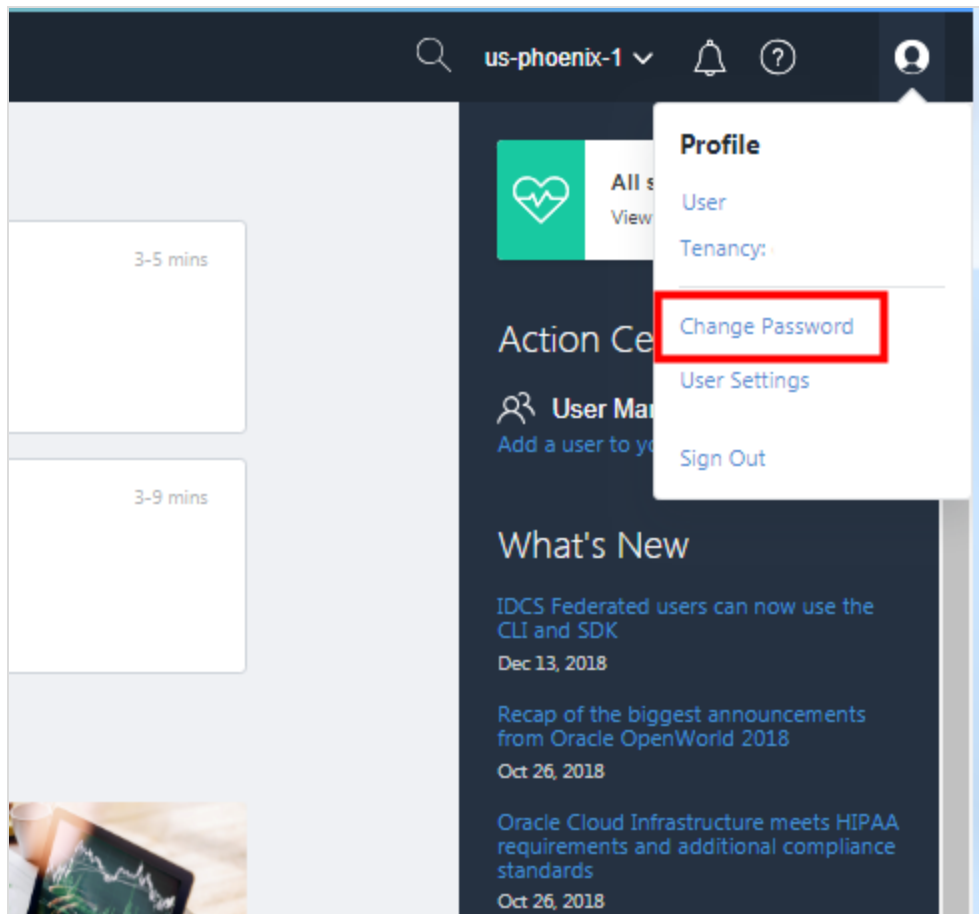
or

USER NAME
[Input field]

PASSWORD
[Input field]

[Sign In](#) [Forgot password?](#)

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



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

CHAPTER 5 Checking Your Balance and Usage

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

Required IAM Policy

To enable users to monitor the costs associated with this account, you will have to grant them access by writing a policy. If you're new to policies, see [Getting Started with Policies](#) and [Common Policies](#).

The following policy statement gives users in a specified group the ability to analyze costs in the tenancy:

Let users analyze costs

Type of access: Ability to see costs for the tenancy.

Where to create the policy: In the tenancy so that users in the *<Example_Group>* can see costs for the entire account.

```
Allow group <Example_Group> to read usage-reports
```

Working with Costs Analysis Tools

Most new customers in the United States who create new accounts after January 28, 2019 can use these tools. If you created your account prior to that date or you are from outside the United States, see [Managing Your Accounts, Promotions, and Subscriptions](#).

To filter costs by dates

1. Open the navigation menu. Under **Governance and Administration**, go to **Account Management** and click **Cost Analysis**.

2. In **Start Date**, select a date.
3. In **End Date**, select a date (within six months of the start date).
4. Click **Apply Filters**.

To filter costs by tags

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

To filter costs by compartments

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

To remove a compartment or tag filter

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

Changing Your Payment Method

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

Required IAM Policy

To upgrade to a paid account or change your credit card, you must be a member of the Administrators group. See [The Administrators Group and Policy](#).

Upgrade Your Free Account

Most new customers in the United States who create new accounts after January 28, 2019 can use these tools. If you created your account prior to that date or from outside the United States, use the following links:

- To upgrade to a paid account, see [Upgrade Your Free Oracle Cloud Promotion](#).
- To change your credit card, see [Update Your Account Details](#).

To upgrade to Pay-as-You-Go

1. Open the navigation menu. Under **Governance and Administration**, go to **Account Management** and click **Payment Method**.
2. Under **Account Type**, select **Pay-as-You-Go**.
3. Take one of the following actions:
 - Click **Edit** to review the current credit card
 - Click **Add a Credit Card**
4. Type or review your information and click **Finish**.
5. Read the terms and conditions and select the check box to indicate your agreement.
6. Click **Start Paid Account**.

To request a sales call

1. Open the navigation menu. Under **Governance and Administration**, go to **Account Management** and click **Payment Method**.
2. Under **Account Type**, select **Request a Sales Call**.

3. Type a phone number, an email address, or both.
4. Click **Submit**.

To change your payment method

You cannot change the payment method for promotional accounts.

1. Open the navigation menu. Under **Governance and Administration**, go to **Account Management** and click **Payment Method**.
2. Click **Edit Card**.
3. Type your information and click **Finish**.

CHAPTER 6 Adding Users

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

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

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

About Users, Groups, and Policies

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

About Oracle Identity Cloud Service Federated Users

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

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

For more details on managing federated users, see [Managing Oracle Identity Cloud Service Users and Groups in the Oracle Cloud Infrastructure Console](#).

You can also choose to use Oracle Cloud Infrastructure's IAM service as your identity provider to manage users and groups exclusively in the IAM service. These users can have permissions to use Oracle Cloud Infrastructure services only. If you want to manage users in the IAM service, see [Managing Users](#).

Sample Users and Groups

To help you understand how to set up users with the access permissions they need, perform the following tasks to set up these two basic types of users:

- An IDCS federated user with full administrator permissions (Cloud Administrator)
- An IDCS federated user with permissions to use one compartment only

Add a User with Oracle Cloud Administrator Permissions

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

Create a Cloud Administrator user

1. Open the navigation menu. Under **Governance and Administration**, go to **Identity** and click **Federation**.
2. Click your Oracle Identity Cloud Service federation. For most tenancies, the federation is named **OracleIdentityCloudService**.
The identity provider details page is displayed.
3. Click **Create IDCS User**.
4. In the **Create IDCS User** dialog enter the following:
 - **Username:** Enter a unique name or email address for the new user.
The value will be the user's login to the Console and must be unique across all

other users in your tenancy.

- **Email:** Enter an email address for this user. The initial sign-in credentials will be sent to this email address.
- **First Name:** Enter the user's first name.
- **Last Name:** Enter the user's last name.
- **Phone Number:** Optionally, enter a phone number.
- **Groups:** You can skip this step. You will be granting this user full administrator privileges.

5. Click **Create**.

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

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

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

7. Click **close** to close the dialog. You are returned to the **Users** list on the **Identity Provider Details** page.

8. Click the name of the user you just created. The **User Details** page is displayed.

9. Click **Manage Service Roles**.

10. Select the check box next to **Grant Cloud Account Administrator Access**.

11. Click **Save Role Selections**.

12. Click **Apply Service Role Settings**.

Create a Compartment and Add a User with Access to It

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

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

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

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

Create a sandbox compartment

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

Create an Oracle Cloud Infrastructure group

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

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

- **Description:** Enter a description (required).
4. Click **Create**.

Create a policy

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

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

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

This statement grants members of the SandboxGroup group full access to the Sandbox compartment.

7. Click **Create**.

Create an Oracle Identity Cloud Service group

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

1. Open the navigation menu. Under **Governance and Administration**, go to **Identity** and click **Federation**.
2. Click your Oracle Identity Cloud Service federation. For most tenancies, the federation is named **OracleIdentityCloudService**.
The identity provider details page is displayed.

3. Under **Resources**, click **Groups**.
4. Click create **IDCS Group**.
5. In the **Create IDCS Group** dialog enter the following:
 - **Name:** Enter a unique name for your group, for example, `IDCS_SandboxGroup`. Note that the name cannot contain spaces.
 - **Description:** Enter a description (required).
6. Click **Create**.

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

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

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

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

Users that are members of the Oracle Identity Cloud Service groups mapped to the Oracle Cloud Infrastructure groups are now listed in the Console on the Users page. See [Managing Federated Users in the Console](#) for more information on assigning these users additional credentials.

Create a user

1. Open the navigation menu. Under **Governance and Administration**, go to **Identity** and click **Federation**.
2. Click your Oracle Identity Cloud Service federation. For most tenancies, the federation is named **OracleIdentityCloudService**.
The identity provider details page is displayed.
3. Click **Create IDCS User**.
4. In the **Create IDCS User** dialog enter the following:
 - **Username:** Enter a unique name or email address for the new user. The value will be the user's login to the Console and must be unique across all other users in your tenancy.
 - **Email:** Enter an email address for this user. The initial sign-in credentials will be sent to this email address.
 - **First Name:** Enter the user's first name.
 - **Last Name:** Enter the user's last name.
 - **Phone Number:** Optionally, enter a phone number.
 - **Groups:** Select the group you created in the previous step, for example, **IDCS SandboxGroup**.
5. Click **Create**.
The user is created in Oracle Identity Cloud Service. This user can't access their account until they complete the password reset steps.
6. Click **Email Password Instructions** to send the password link and instructions to the user.
The password link is good for 24 hours. If the user does not reset their password in time, you can generate a new password link by clicking **Reset Password** for the user.

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

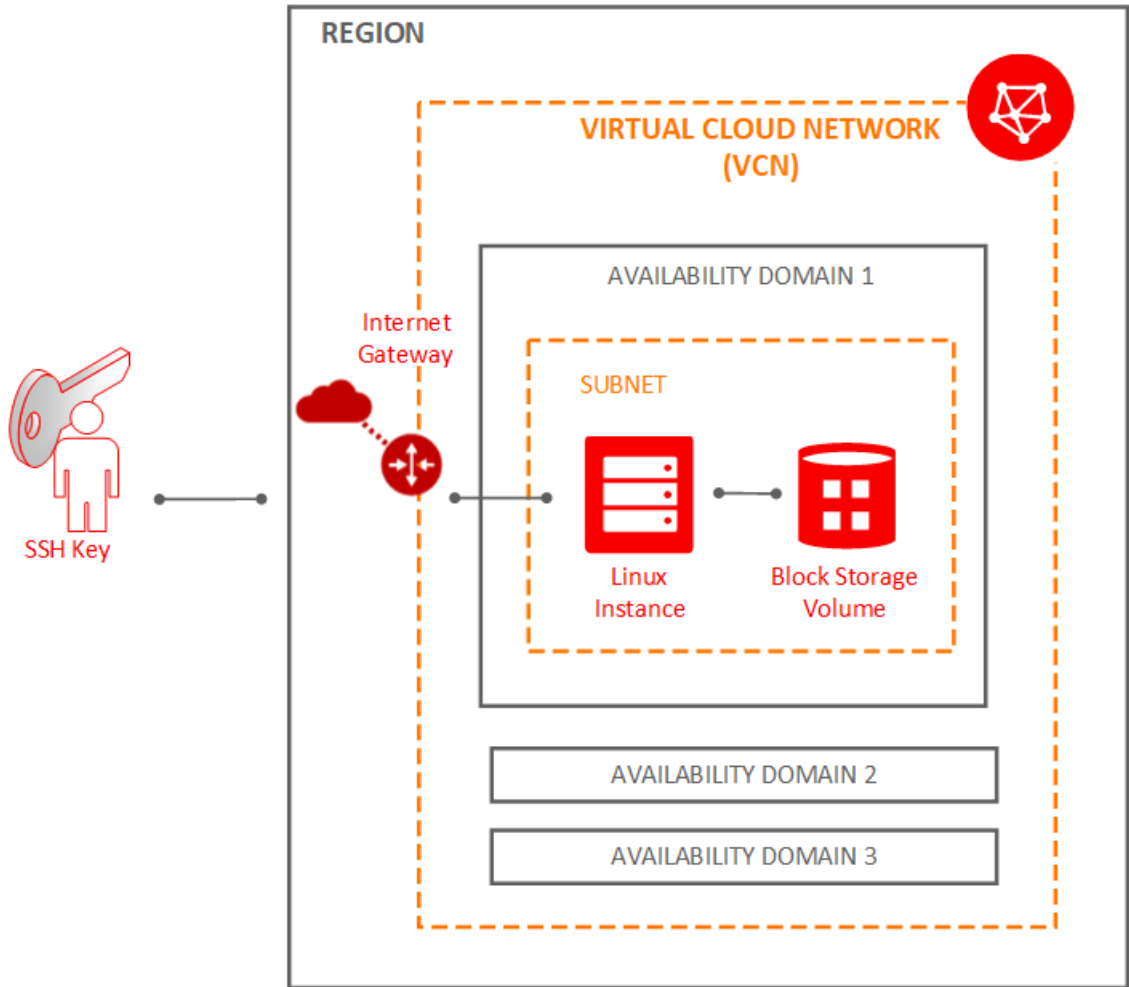
CHAPTER 7 Tutorial - Launching Your First Linux Instance

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

In this tutorial you will:

- Create a cloud network and subnet that enables internet access
- Launch an instance
- Connect to the instance
- Add and attach a block volume

The following figure depicts the components you create in the tutorial.



Task Flow to Launch an Instance

Instances use an SSH key pair instead of a password to authenticate a remote user. If you do not already have a key pair, your first task is to create one using common third-party tools. Next, prepare for your instance by launching a cloud network with subnets. You will then launch your instance into one of the subnets and connect to it. If you want to attach some

storage, continue with the tutorial to add a cloud block storage volume. When finished with the tutorial, be sure to terminate the resources that you created.

Prepare:

1. [Create a key pair](#).
2. [Choose a compartment for your resources](#).
3. [Create a cloud network](#).

Launch and connect:

4. [Launch an instance](#).
5. [Connect to your instance](#).

Add storage and clean up:

6. [Add a block volume \(optional\)](#).
7. [Clean up your resources](#).

Creating a Key Pair

Instances use an SSH key pair instead of a password to authenticate a remote user. A key pair file contains a private key and public key. You keep the private key on your computer and provide the public key every time you launch an instance.

To create key pairs, you can use a third-party tool such as OpenSSH on UNIX-style systems (including Linux, Solaris, BSD, and OS X) or PuTTY Key Generator on Windows.

Before You Begin

- If you already have an SSH-2 RSA key pair, you can use your existing pair and skip this step. Proceed to [Choosing a Compartment](#).
- If you're using a Linux distribution, you probably already have the `ssh-keygen` utility installed. To determine if it's installed, type `ssh-keygen` on the command line. If it's not

installed, you can download OpenSSH for UNIX from <http://www.openssh.com/portable.html> and install it.

- If you're using Windows and you don't already have the PuTTY Key Generator, download it from <http://www.putty.org> and install it.

Creating a Key Pair

Creating an SSH Key Pair on the Command Line

1. Open a shell or terminal for entering the commands.
2. At the prompt, enter `ssh-keygen` and provide a name and passphrase when prompted. The keys will be created with the default values: RSA keys of 2048 bits.

Alternatively, you can type a complete `ssh-keygen` command, for example:

```
ssh-keygen -t rsa -N "" -b 2048 -C "<key_name>" -f <path/root_name>
```

The command arguments are shown in the following table:

Argument	Description
<code>-t rsa</code>	Use the RSA algorithm.
<code>-N "<passphrase>"</code>	A passphrase to protect the use of the key (like a password). If you don't want to set a passphrase, don't enter anything between the quotes. A passphrase is not required. You can specify one as a security measure to protect the private key from unauthorized use.

Argument	Description
-b 2048	Generate a 2048-bit key. You don't have to set this if 2048 is acceptable, as 2048 is the default. A minimum of 2048 bits is recommended for SSH-2 RSA.
-C "<key_name>"	A name to identify the key.
-f <path/root_name>	The location where the key pair will be saved and the root name for the files.

Creating an SSH Key Pair on Windows Using PuTTY Key Generator

1. Find `puttygen.exe` in the PuTTY folder on your computer, for example, `C:\Program Files (x86)\PuTTY`. Double-click `puttygen.exe` to open it.
2. Specify a key type of SSH-2 RSA and a key size of 2048 bits:
 - In the **Key** menu, confirm that the default value of **SSH-2 RSA key** is selected.
 - For the **Type of key to generate**, accept the default key type of **RSA**.
 - Set the **Number of bits in a generated key** to 2048 if it is not already set.
3. Click **Generate**.
4. Move your mouse around the blank area in the PuTTY window to generate random data in the key.
When the key is generated, it appears under **Public key for pasting into OpenSSH authorized_keys file**.
5. A **Key comment** is generated for you, including the date and time stamp. You can keep the default comment or replace it with your own more descriptive comment.
6. Leave the **Key passphrase** field blank.

7. Click **Save private key**, and then click **Yes** in the prompt about saving the key without a passphrase.

The key pair is saved in the PuTTY Private Key (PPK) format, which is a proprietary format that works only with the PuTTY tool set.

You can name the key anything you want, but use the `ppk` file extension. For example, `mykey.ppk`.

8. Select *all* of the generated key that appears under **Public key for pasting into OpenSSH authorized_keys file**, copy it using **Ctrl + C**, paste it into a text file, and then save the file in the same location as the private key.
(Do not use **Save public key** because it does not save the key in the OpenSSH format.)
You can name the key anything you want, but for consistency, use the same name as the private key and a file extension of `pub`. For example, `mykey.pub`.
9. Write down the names and location of your public and private key files. You will need the public key when launching an instance. You will need the private key to access the instance via SSH.

Choosing a Compartment

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

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

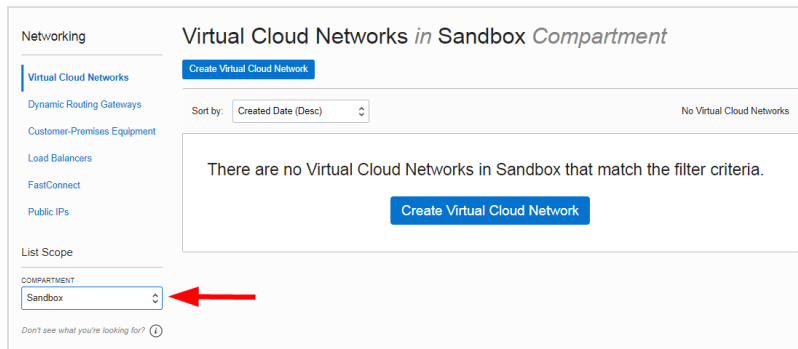
Before You Begin

[Sign in](#) to the Console.

Choosing a Compartment

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

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



Creating a Compartment

1. Open the navigation menu. Under **Governance and Administration**, go to **Identity** and click **Compartments**.
2. Click **Create Compartment**.
3. Enter the following:
 - **Name:** Enter "Sandbox".
 - **Description:** Enter a description (required), for example: "Sandbox compartment for the getting started tutorial". Avoid entering confidential information.

4. Click **Create Compartment**.

Your compartment is displayed in the list.

5. Switch to your new compartment by selecting it from the **Compartment** list on the left side of the Console.

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

Creating a Virtual Cloud Network

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

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

Before You Begin

- You or an administrator has created a compartment for your network. See [Choosing a Compartment](#).

Create a Cloud Network Plus Related Resources



Tip

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

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

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

2. Click **Create Virtual Cloud Network**.
3. Enter the following:
 - **Name:** Enter a name for your cloud network, for example, <your_initials>_Network. Avoid entering confidential information.
 - **Create in Compartment:** This field defaults to your current compartment. Select the compartment you want to create the VCN in, if not already selected.
 - Select **Create Virtual Cloud Network Plus Related Resources**. The dialog expands to list the items that will be created with your cloud network.
 - Accept the defaults for any other fields.
4. Scroll to the bottom of the dialog and click **Create Virtual Cloud Network**.

A confirmation page displays the details of the cloud network that you just created. The cloud network has the following resources and characteristics (some of which are not listed in the confirmation dialog):

- CIDR block range of 10.0.0.0/16
- An internet gateway
- A route table with a default route rule to enable traffic to and from the internet gateway
- A default security list. You will edit this default security list later in the tutorial.
- A public subnet in each availability domain.
- The VCN will automatically use the Internet and VCN Resolver for DNS.



Important

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

WHAT'S NEXT

Now you can launch an instance. See [Launching a Linux Instance](#).

Launching a Linux Instance

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

Before You Begin

- You have created a cloud network and subnet. See [Creating a Virtual Cloud Network](#).
- You have an SSH key pair. See [Creating a Key Pair](#).

Launching an Instance

1. Open the navigation menu. Under **Core Infrastructure**, go to **Compute** and click **Instances**.
2. Click **Create Instance**.
3. On the **Create Instance** page, enter the following:
 - **Name your instance:** Enter a name, for example: <your initials>_Instance. Avoid entering confidential information.
 - **Choose an operating system or image source:** Accept the default, Oracle Linux 7.x.
 - **Availability Domain:** Accept the default.
 - **Instance Type:** Accept the default, Virtual Machine.
 - **Instance Shape:** Accept the default, VM.Standard.E2.1.Micro (1 OCPU, 1 GB RAM).
The shape defines the number of CPUs and amount of memory allocated to the instance.
 - In the **Configure networking** section, do the following:

- **Virtual cloud network compartment:** Select the compartment containing the cloud network that you created.
 - **Virtual cloud network:** Select the cloud network that you created.
 - **Subnet compartment:** Select the compartment containing the subnet that was created with your cloud network.
 - **Subnet:** Select the subnet that was created with your cloud network.
 - Leave the **Use network security groups to control traffic** option cleared.
 - To create a public IP address for the instance, select the **Assign a public IP address** option.
 - **Boot volume:** Leave all the options cleared.
 - **Add SSH Key:** Select **Choose SSH key file**. Click **Choose Files**, navigate to the location where you saved the public key portion (.pub) of the SSH key file that you created, select the file and click **Open**.
4. Click **Create**.

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

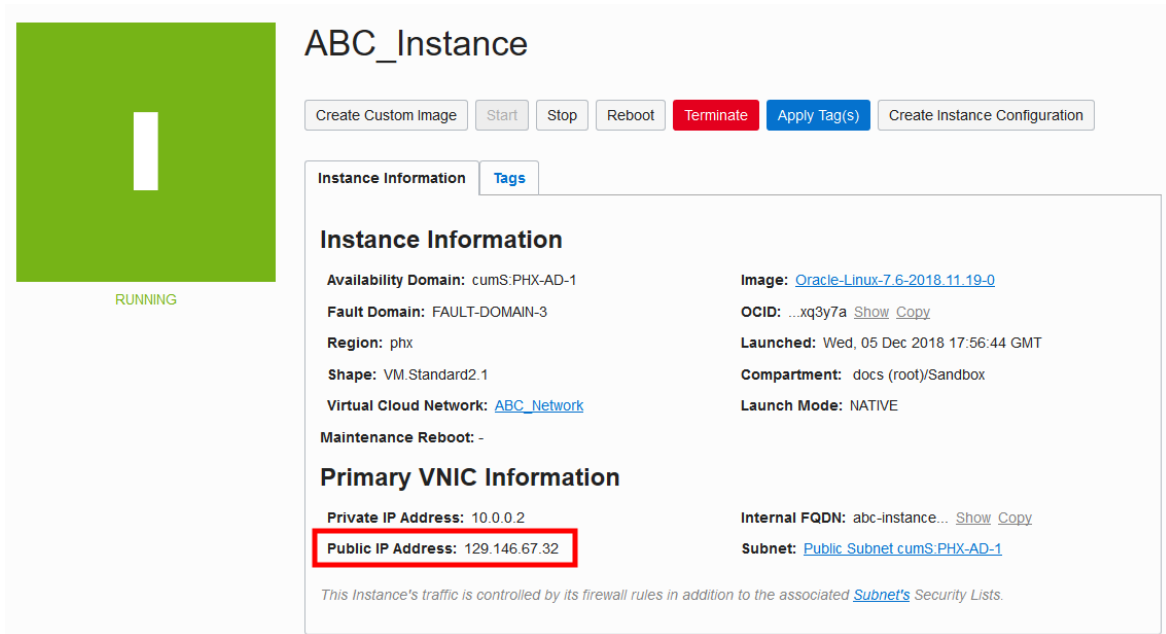
Getting the Instance Public IP Address

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

To get the instance public IP address:

CHAPTER 7 Tutorial - Launching Your First Linux Instance

1. Click the instance name to see its details.
2. The **Public IP Address** is displayed on the details page under **Primary VNIC Information**, as shown in the following image:



ABC_Instance

Create Custom Image Start Stop Reboot Terminate Apply Tag(s) Create Instance Configuration

Instance Information Tags

Instance Information

Availability Domain: cumS:PHX-AD-1
Fault Domain: FAULT-DOMAIN-3
Region: phx
Shape: VM.Standard2.1
Virtual Cloud Network: [ABC_Network](#)
Maintenance Reboot: -

Image: [Oracle-Linux-7.6-2018.11.19-0](#)
OCID: ...xq3y7a [Show Copy](#)
Launched: Wed, 05 Dec 2018 17:56:44 GMT
Compartment: docs (root)/Sandbox
Launch Mode: NATIVE

Primary VNIC Information

Private IP Address: 10.0.0.2
Public IP Address: 129.146.67.32
Internal FQDN: abc-instance... [Show Copy](#)
Subnet: [Public Subnet cumS:PHX-AD-1](#)

This Instance's traffic is controlled by its firewall rules in addition to the associated [Subnet's](#) Security Lists.

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

Connecting to Your Instance

You connect to a running instance by using a Secure Shell (SSH) connection. Most Linux distributions include an SSH client by default. For Windows, you can download a free SSH client called PuTTY from <http://www.putty.org>.

Before You Begin

- You know the public IP address of your instance. See [Launching a Linux Instance](#).
- You know the path to your private key file.

Connecting to Your Linux Instance Using SSH

Log in to your instance using SSH.

Connecting to Your Linux Instance from a Unix-style System

1. Use the following command to set the file permissions so that only you can read the file:

```
$ chmod 400 <private_key>
```

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

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

```
$ ssh -i <private_key> <username>@<public-ip-address>
```

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

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

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

Connecting to Your Linux Instance from a Windows System

1. Open `putty.exe`.
2. In the **Category** pane, expand **Window**, and then select **Translation**.
3. In the **Remote character set** drop-down list, select **UTF-8**. The default locale setting on Linux-based instances is UTF-8, and this configures PuTTY to use the same locale.
4. In the **Category** pane, select **Session** and enter the following:
 - **Host Name (or IP address):**
`<username>@<public-ip-address>`
`<username>` is the default name for the instance. For Oracle Linux and CentOS images, the default user name is `opc`. For the Ubuntu image, the default name is `ubuntu`.
`<public-ip-address>` is your instance public IP address that you retrieved from the Console
 - **Port:** 22
 - **Connection type:** SSH
5. In the **Category** pane, expand **Connection**, expand **SSH**, and then click **Auth**.
6. Click **Browse**, and then select your private key.
7. Click **Open** to start the session.
If this is your first time connecting to the instance, you might see a message that the server's host key is not cached in the registry. Click **Yes** to continue the connection.

Running Administrative Tasks on the Instance

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

WHAT'S NEXT

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

- Install software on the instance.
- Add a block volume. See [Adding a Block Volume](#).
- Add more users to work with Oracle Cloud Infrastructure. See [About Users, Groups, and Policies](#).
- Or, if you are finished with your instance, delete the resources that you created in the tutorial. See [Cleaning Up Resources from the Tutorial](#).

Adding a Block Volume

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

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

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

Creating a Volume

1. Open the navigation menu. Under **Core Infrastructure**, go to **Block Storage** and click **Block Volumes**.
2. Click **Create Block Volume**.
3. In the **Create Block Volume** dialog, enter the following:
 - **Create in Compartment:** This field defaults to your current compartment. Select the compartment you want to create the volume in, if not already selected.
 - **Name:** Enter a user-friendly name. Avoid entering confidential information.
 - **Availability Domain:** Select the same availability domain that you selected for your instance. If you followed the tutorial instructions when launching your instance, this is the first AD in the list. The volume and the instance must be in the same availability domain.
 - **Size:** Enter 50 to create a 50 GB block volume.
 - **Backup Policy:** Do not select a backup policy.
 - **Tags:** Leave the tagging fields blank.
4. Click **Create Block Volume**.

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

Attaching the Volume to an Instance

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

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



Tip

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

- **Access:** Select **Read/Write**.
6. Click **Attach**, and then click **Close**.

Connecting to the Volume

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

To connect to your volume:

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

The **iSCSI Commands and Information** dialog is displayed. Notice that the dialog displays specific identifying information about your volume (such as IP address and

port) as well as the iSCSI commands you'll need to use. The commands are ready to use with the appropriate information already included in each command.

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

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

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

```
sudo fdisk -l
```

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

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



Important

Connecting to Volumes on Linux Instances

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

WHAT'S NEXT

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

- Install your own software on the instance.
- Add more users to work with Oracle Cloud Infrastructure. See [About Users, Groups, and Policies](#).
- Or, if you are finished with your instance, delete the resources that you created in the tutorial. See [Cleaning Up Resources from the Tutorial](#).

Cleaning Up Resources from the Tutorial

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

Detach and Delete the Block Volume

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

Terminate the Instance

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

Delete the Virtual Cloud Network

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

CHAPTER 8 Tutorial - Launching Your First Windows Instance

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

In this tutorial you will:

- Create a cloud network and subnet that enables internet access
- Launch an instance
- Connect to the instance
- Add and attach a block volume

The following figure depicts the components you create in the tutorial.

Task Flow to Launch a Windows Instance

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

Prepare:

1. [Choose a compartment for your resources.](#)
2. [Create a cloud network.](#)

Launch and connect:

3. [Launch a Windows instance.](#)
4. [Connect to your Windows instance.](#)

Add storage and clean up:

5. [Add a block volume \(optional\).](#)
6. [Clean up your resources.](#)

Choosing a Compartment

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

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

Before You Begin

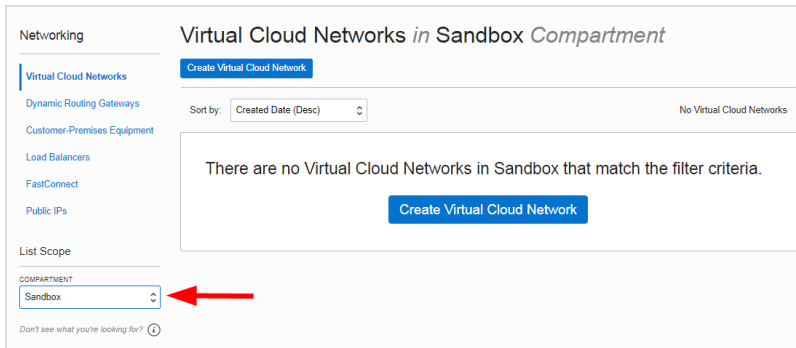
[Sign in](#) to the Console.

Choosing a Compartment

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

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

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



Creating a Compartment

1. Open the navigation menu. Under **Governance and Administration**, go to **Identity** and click **Compartments**.
2. Click **Create Compartment**.
3. Enter the following:
 - **Name:** Enter "Sandbox".
 - **Description:** Enter a description (required), for example: "Sandbox compartment for the getting started tutorial". Avoid entering confidential information.
4. Click **Create Compartment**.
Your compartment is displayed in the list.
5. Switch to your new compartment by selecting it from the **Compartment** list on the left side of the Console.

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

compartments, you must come back to the Sandbox compartment to see the resources that were created there.

Creating a Virtual Cloud Network

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

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

Before You Begin

- You or an administrator has created a compartment for your network. See [Choosing a Compartment](#).

Create a Cloud Network Plus Related Resources



Tip

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

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

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

2. Click **Create Virtual Cloud Network**.
3. Enter the following:
 - **Name:** Enter a name for your cloud network, for example, <your_initials>_Network. Avoid entering confidential information.
 - **Create in Compartment:** This field defaults to your current compartment. Select the compartment you want to create the VCN in, if not already selected.
 - Select **Create Virtual Cloud Network Plus Related Resources**. The dialog expands to list the items that will be created with your cloud network.
 - Accept the defaults for any other fields.
4. Scroll to the bottom of the dialog and click **Create Virtual Cloud Network**.

A confirmation page displays the details of the cloud network that you just created. The cloud network has the following resources and characteristics (some of which are not listed in the confirmation dialog):

- CIDR block range of 10.0.0.0/16
- An internet gateway
- A route table with a default route rule to enable traffic to and from the internet gateway
- A default security list. You will edit this default security list later in the tutorial.
- A public subnet in each availability domain.
- The VCN will automatically use the Internet and VCN Resolver for DNS.



Important

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

Edit the Default Security List to Allow Traffic to Your Windows Instance

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

To edit the VCN's security list:

1. Click the name of the VCN that you just created. Its details are displayed.
2. Under **Resources**, click **Security Lists**.
3. Click the default security list for your VCN.
Its details are displayed.
4. Click **Edit All Rules**.
5. Under **Allow Rules for Ingress**, click **+ Another Ingress Rule**.
6. Enter the following for your new rule:
 - a. **Source Type:** CIDR
 - b. **Source CIDR:** 0.0.0.0/0
 - c. **IP Protocol:** RDP (TCP/3389)
 - d. **Source Port Range:** All
 - e. **Destination Port Range:** 3389

7. When done, click **Save Security List Rules**.

WHAT'S NEXT

Now you can launch an instance. See [Launching a Windows Instance](#).

Launching a Windows Instance

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

Before You Begin

- You have created a cloud network and subnet. See [Creating a Virtual Cloud Network](#).

Launching an Instance

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



Important

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

- **Choose an operating system or image source:** Click **Change Image Source**. On the **Platform Images** tab, select **Windows Server 2016 Standard**. Review and accept the terms of use, and then click **Select Image**.
 - **Availability Domain:** Accept the default.
 - **Instance Type:** Accept the default, Virtual Machine.
 - **Instance Shape:** Accept the default, VM.Standard2.1 (1 OCPU, 15 GB RAM). The shape defines the number of CPUs and amount of memory allocated to the instance.
 - In the **Configure networking** section, do the following:
 - **Virtual cloud network compartment:** Select the compartment containing the cloud network that you created.
 - **Virtual cloud network:** Select the cloud network that you created.
 - **Subnet compartment:** Select the compartment containing the subnet that was created with your cloud network.
 - **Subnet:** Select the subnet that was created with your cloud network.
 - Leave the **Use network security groups to control traffic** option cleared.
 - To create a public IP address for the instance, select the **Assign a public IP address** option.
 - **Boot volume:** Leave all the options cleared.
4. Click **Create**.

CHAPTER 8 Tutorial - Launching Your First Windows Instance

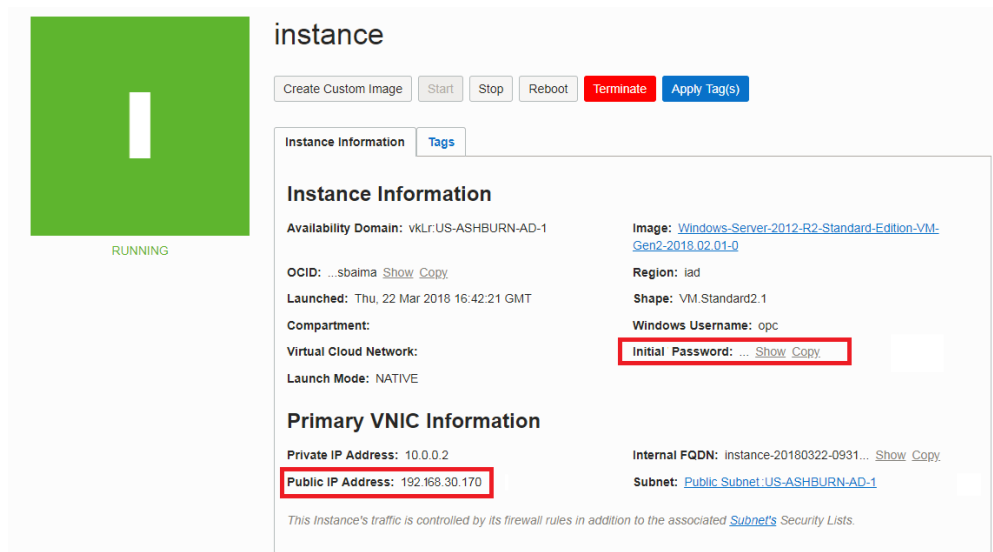
The instance is displayed in the Console in a provisioning state. Expect provisioning to take several minutes before the status updates to Running. Do not refresh the page. After the instance is running, allow another few minutes for the operating system to boot before you attempt to connect.

Getting the Instance Public IP Address and Initial Windows Password

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

To get the instance public IP address and initial password:

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



The screenshot displays the Oracle Cloud Console interface for an instance. On the left, a green square with a white 'I' icon represents the instance, with the status 'RUNNING' below it. The main content area is titled 'instance' and includes several action buttons: 'Create Custom Image', 'Start', 'Stop', 'Reboot', 'Terminate', and 'Apply Tag(s)'. Below these buttons, there are tabs for 'Instance Information' and 'Tags'. The 'Instance Information' section is expanded, showing the following details:

- Availability Domain:** vkLr.US-ASHBURN-AD-1
- Image:** [Windows_Server-2012-R2-Standard-Edition-VM-Gen2-2018.02.01-0](#)
- OCID:** ...sbaima [Show Copy](#)
- Region:** iad
- Launched:** Thu, 22 Mar 2018 16:42:21 GMT
- Shape:** VM.Standard2.1
- Compartment:**
- Windows Username:** opc
- Virtual Cloud Network:**
- Initial Password:** ... [Show Copy](#)
- Launch Mode:** NATIVE

The **Primary VNIC Information** section is also expanded, showing:

- Private IP Address:** 10.0.0.2
- Public IP Address:** 192.168.30.170
- Internal FQDN:** instance-20180322-0931... [Show Copy](#)
- Subnet:** [Public Subnet:US-ASHBURN-AD-1](#)

At the bottom, a note states: 'This Instance's traffic is controlled by its firewall rules in addition to the associated [Subnet's](#) Security Lists.'

3. To view the **Initial Password**, click **Show**.

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

Connecting to Your Windows Instance

You connect to a running Windows instance using Remote Desktop.

Before You Begin

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

Connecting to Your Windows Instance from a Remote Desktop Client

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

Running Administrative Tasks on the Instance

The default user, `opc`, has administrative privileges.

WHAT'S NEXT

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

- Install software on the instance.
- Add a block volume. See [Adding a Block Volume to a Windows Instance](#).
- Add more users to work with Oracle Cloud Infrastructure. See [About Users, Groups, and Policies](#).
- Or, if you are finished with your instance, delete the resources that you created in the tutorial. See [Cleaning Up Resources from the Tutorial](#).

Adding a Block Volume to a Windows Instance

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

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

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

Creating a Volume

1. Open the navigation menu. Under **Core Infrastructure**, go to **Block Storage** and click **Block Volumes**.
2. Click **Create Block Volume**.

3. In the **Create Block Volume** dialog box, enter the following:
 - **Create in Compartment:** This field defaults to your current compartment. Select the compartment you want to create the volume in, if not already selected.
 - **Name:** Enter a user-friendly name. Avoid entering confidential information.
 - **Availability Domain:** Select the same availability domain that you selected for your instance. If you followed the tutorial instructions when launching your instance, this will be the first availability domain in the list. The volume and the instance must be in the same availability domain.
 - **Size:** Enter 256 to create a 256 GB block volume.
4. Click **Create Block Volume**.

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

Attaching the Volume to an Instance

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

1. Find your instance: Open the navigation menu. Under **Core Infrastructure**, go to **Compute** and click **Instances**.
2. Click your instance name to view its details.
3. Click **Attach Block Volume**.
4. In the dialog box, enter the following:
 - a. **Block Volume Compartment:** Select the compartment where you created the block volume.
 - b. **Block Volume:** Select the block volume from the list.

- c. **Require CHAP Credentials:** Leave unselected.



Tip

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

5. Click **Attach**.

Connecting to the Volume

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

To connect to your volume:

1. Log on to your instance as described in [Connecting to Your Windows Instance](#).
2. Open the navigation menu. Under **Core Infrastructure**, go to **Compute** and click **Instances**.
3. Click your instance name to view the attached storage volume.
4. Click the Actions icon (three dots) next to the volume you just attached and then click **iSCSI Commands and Information**.

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

5. On your Windows instance, open the iSCSI Initiator.
For example: Open **Server Manager**, click **Tools**, and select **iSCSI Initiator**.

6. In the iSCSI Initiator Properties dialog box, click the **Discovery** tab.
7. Click **Discover Portal**.
8. Enter the block volume IP address and port. Click OK.
9. Click the **Targets** tab.
10. In the **Discovered Targets** region, select the volume IQN.
11. Click **Connect** and then click **OK** to close the dialog.
12. You are now ready to format (if needed) and mount the volume. To get a list of mountable iSCSI devices on the instance, in Server Manager, click **File and Storage Services** and then click **Disks**.
The 256 GB disk is displayed in the list.

WHAT'S NEXT

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

- Install your own software on the instance.
- Add more users to work with Oracle Cloud Infrastructure. See [About Users, Groups, and Policies](#).
- Or, if you are finished with your instance, delete the resources that you created in the tutorial. See [Cleaning Up Resources from the Tutorial](#).

Cleaning Up Resources from the Tutorial

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

Detach and Delete the Block Volume

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

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

Terminate the Instance

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

Delete the Virtual Cloud Network

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

CHAPTER 9 Getting Started with the Command Line Interface

This chapter provides a hands-on tutorial to using the Command Line Interface (CLI).

Getting Started with the Command Line Interface

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

About the Command Line Interface (CLI)

The CLI is a tool that lets you work with most of the available services in Oracle Cloud Infrastructure. The CLI provides the same core functionality as the Console, plus additional commands. The CLI's functionality and command help are based on the service's API.

Getting Help with Commands

You can get inline help using the `--help`, `-h`, or `-?` keywords. For example:

```
oci --help
```

```
oci bv volume -h
```

```
oci os bucket create -?
```

You can also [view all the CLI help](#) in your browser.

About the CLI Examples

The examples in this document are grouped as a command and a response, where:

- You are told what the command does, and given the command to use
- The result of the command is returned in a drop-down text box

CHAPTER 9 Getting Started with the Command Line Interface

The next example shows a command and response group.

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

```
oci os ns get
```

Response



Note

Understanding Response Output

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

```
{
  "data": "docs"
  "id":
  "ocid1.compartment.oc1..aaaaaaaa13gziqdhqol2pqli6astxxeyqdqey
g35nz5zxil2rggnx7jnhwa"
  "is-stateless": null
}
```

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

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

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

Before You Begin

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

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

Working in a Compartment

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

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

Choose a Compartment

Help: `oci iam compartment list -h`

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

```
oci iam compartment list -c <tenancy_id>
```

Command Example and Response

```
oci iam compartment list -c
ocidl.tenancy.oc1..aaaaaaaallfvgn0h9njji5u6ldrwb4l6aay2x87qatw2wte30f7141a19oom
```

```
{
  "data": [
    {
      "compartment-id":
"ocidl.tenancy.oc1..aaaaaaaallfvgn0h9njji5u6ldrwb4l6aay2x87qatw2wte30f7141a19oom",
      "description": "For testing CLI features",
      "id": "ocidl.tenancy.oc1..aaaaaaaallfvgn0h9njji5u6ldrwb4l6aay2x87qatw2wte30f7141a19oom",
      "inactive-status": null,
      "lifecycle-state": "ACTIVE",
```

CHAPTER 9 Getting Started with the Command Line Interface

```
    "name": "CLISandbox",
    "time-created": "2017-06-27T18:52:52.214000+00:00"
  },
  {
    "compartment-id":
"ocidl.tenancy.oc1..aaaaaaaa1fvgn0h9njji5u6ldrwb4l6aay2x87qatw2wte30f7141a19oom",
    "description": "for testing",
    "id": "ocidl.compartment.oc1..aaaaaaaasqn3hj6e5tq6slj4rpdqqa7qsyuqipmu4sv5ucmyp3rkmrhuv2q",
    "inactive-status": null,
    "lifecycle-state": "ACTIVE",
    "name": "CLISandbox",
    "time-created": "2017-05-12T21:31:27.709000+00:00"
  }
],
"opc-next-page": "      AAAAAAAAAAGLB28zJTjPUeNvgmLxg9QuJdAAZr110FfKymIMh4y1XItQkO_Xk6RXbGxCn8hgkYm_
pRpflv6hVoxrYTQsaoveGMkX6iwwwPY5dptL8AKlyogYSs7F3G92KG2EhrI7j4NoUBtJ4-
PTB53F2TZ31dReLsbzxBa3ljbwqQgwzQsUPYROLXA40EIJFdr2oYp67AzoZSW8jt8MWFC8y19PsHEEEBW1jw8TT7Lq8XL_
7mo5avasfsIYS7-VgP3ZFu6Y-Rab-gPntjsT4pLh91BkDKWzbyHr0OmH4W1rhTJ5HfZ8YGpA0Ntm7_rOyNBd06qeBU496AQHk24-U_
l9p4NvAvHuJ_fR-Z6ahgvWPlZQc1iCTR1J6leM7ED3JNehIV0onOVQvGquJpF2WeEWFPCioQaqf4iScqHEchV--3Mn2klyP_-
b4AsVtSPRFYG8UuiRACPzg6ENVFjyeGOk3rrHjLR3j7s6lpgdqtMOKZ1WtbOV8AcNON8ac1xJPN7O2YmjO3D0H4JmzXh_
GxRskTpk11D9En9zJXn99oWsNBOYgQQmv7s_7j82ZrXGoyOME-iT"
}
```

Create a Compartment

Help: `oci iam compartment create -h`

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

To create a compartment, run the following command.

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



Warning

Avoid entering confidential information when providing resource names or descriptions for any of the CLI commands.

Command Example and Response

```
oci iam compartment create --name CLIsandbox -c
ocid1.tenancy.oc1..aaaaaaaal1fvgn0h9njji5u6ldrwb4l6aay2x87qatw2wte30f7141a19oom --description "For
testing CLI features"
```

```
{
  "data": {
    "compartment-id": "ocid1.tenancy.oc1..aaaaaaaawuu4tdkysd2ups5fsc1gm5ksfjwmx6mwem5sbjyw5ob5ojq2vkxa",
    "description": "For testing CLI features",
    "id": "ocid1.compartment.oc1..aaaaaaaalkqnr7pfd92rdrwo5fm6fcoufoihlvd4ls4j9jjpge16vfyxrc11",
    "inactive-status": null,
    "lifecycle-state": "ACTIVE",
    "name": "CLIsandbox",
    "time-created": "2017-06-27T18:52:52.214000+00:00"
  },
  "etag": "24a4737ede9d34eae934c93e9549ee684a15efc8"
}
```



Tip

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

```
"compartment-id":  
"ocidl.tenancy.oc1..aaaaaaaawuu4tdkysd2ups5fsc1gm5ksfjwmx6mwem  
5sbjyw5ob5ojq2vkxa"
```

Creating a Virtual Cloud Network

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

1. Create the Virtual Cloud Network

Help: `oci network vcn create -h`

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

To create the VCN, run the following command.

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

Command Example and Response

```
oci network vcn create --compartment-id  
ocidl.compartment.oc1..aaaaaaaalkqnr7pfd92rdrwo5fm6fcoufoih1vd4ls4j9jjpgel6vfyxrc1l --display-  
name "cli_vcn" --dns-label sandboxvcn1 --cidr-block "10.0.0.0/16"
```

```
{  
  "data": {  
    "cidr-block": "10.0.0.0/16",
```

CHAPTER 9 Getting Started with the Command Line Interface

```
  "compartment-id":
"ocidl.compartment.oc1..aaaaaaaalkqnr7pfd92rdrwo5fm6fcoufoihlvd4ls4j9jjpge16vfyxrc11",
  "default-dhcp-options-id":
"ocidl.dhcptions.oc1.phx.aaaaaaaexnsdwsjmxnmmt4tpzkbyengrnfpgnqzlkzz7qfx6faeqfbtcfa",
  "default-route-table-id":
"ocidl.routetable.oc1.phx.aaaaaaaagdjure4rmk5dq6qqkftjtzyn7vctemqga3i6qrxvf23stedpujo2q",
  "default-security-list-id":
"ocidl.securitylist.oc1.phx.aaaaaaaax3cr5zqshmed7zf64bxcrx2zerinxhc52zrqe5w27hrau75j2q",
  "display-name": "cli_vcn",
  "dns-label": "sandboxvcn1",
  "id": "ocidl.vcn.oc1.phx.aaaaaaa6va8fxr1m4hvjzjk3nzo8x290qymdrwiblxw5qpzlm64rdd74vchr",
  "lifecycle-state": "AVAILABLE",
  "time-created": "2017-06-27T22:14:15.683000+00:00", "vcn-domain-name":
"sandboxvcn1.oraclevcn.com"
},
  "etag": "9037efc5"
}
```

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

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

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

Command Example and Response

```
oci network vcn list -c
ocidl.compartment.oc1..aaaaaaaalkqnr7pfd92rdrwo5fm6fcoufoihlvd4ls4j9jjpge16vfyxrc11
{
  "data": [
    {
      "cidr-block": "10.0.0.0/16",
      "compartment-id":
"ocidl.compartment.oc1..aaaaaaaalkqnr7pfd92rdrwo5fm6fcoufoihlvd4ls4j9jjpge16vfyxrc11",
      "default-dhcp-options-id":
"ocidl.dhcptions.oc1.phx.aaaaaaaexnsdwsjmxncbydrwrnfwspgnqzlkzz7qfmmt4tpzkx6faeqfbtcfa",
      "default-route-table-id":
"ocidl.routetable.oc1.phx.aaaaaaaagdjure4jtzyn7vctmqga3i6qrxvf2rmk5dqdrwqkft3stedpujo2q",
```

```
"default-security-list-id":
"ocidl.securitylist.oc1.phx.aaaaaaaaa3cr5zqsdrwx2zerinxhc52zrqe5wmed74bxczf27hrau75j2q",
  "display-name": "cli_vcn",
  "dns-label": "sandboxvcn1",
  "id": "ocidl.vcn.oc1.phx.aaaaaaaa6va8fxr1m4hvzjk3nzo8x290qymdrwiblxw5qpzlm64rdd74vchr",
  "lifecycle-state": "AVAILABLE",
  "time-created": "2017-06-27T22:14:15.683000+00:00",
  "vcn-domain-name": "sandboxvcn1.oraclevcn.com"
}
]
```

2. Configure a Security List Ingress Rule

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

When you create a VCN, a default security list is created for you. However, the Windows instance also requires inbound traffic enabled for port 3389. The preferred approach is creating a second list that addresses the Windows port requirement. You use the `--security-list-ids` option to associate both security lists with the subnet when you create it.



Note

Passing JSON Strings in the CLI

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

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

```
oci network security-list create -c <compartment_id> --egress-security-rules "[{"destination":
"<0.0.0.0/>", "protocol": "<6>", "isStateless": <true>, "tcpOptions": {"destinationPortRange":
```

```
<null>, "sourcePortRange": <null>}}" --ingress-security-rules [{"source": "<0.0.0.0/0>",  
"protocol": "<6>", "isStateless": <false>, "tcpOptions": {"destinationPortRange": {"max": <3389>,  
"min": <3389>}, "sourcePortRange": <null>}}] --vcn-id <vcn_id> --display-name <rule_name>
```

Command Example and Response

```
oci network security-list create -c  
ocid1.compartment.oc1..aaaaaaaalkqnr7pfd92rdrwo5fm6fcoufoihlvd4ls4j9jjpgel6vfyxrcl1 --egress-  
security-rules [{"destination": "0.0.0.0/0", "protocol": "6", "isStateless": true, "tcpOptions":  
{"destinationPortRange": null, "sourcePortRange": null}}] --ingress-security-rules [{"source":  
"0.0.0.0/0", "protocol": "6", "isStateless": false, "tcpOptions": {"destinationPortRange":  
{"max": 3389, "min": 3389}, "sourcePortRange": null}}] --vcn-id  
ocid1.vcn.oc1.phx.aaaaaaa6va8fxrlm4hvzjk3nzo8x290qymdrwiblxw5qpzlm64rdd74vchr --display-name  
port3389rule
```

```
{  
  "data": {  
    "compartment-id":  
"ocid1.compartment.oc1..aaaaaaaalkqnr7pfd92rdrwo5fm6fcoufoihlvd4ls4j9jjpgel6vfyxrcl1",  
    "display-name": "port3389rule",  
    "egress-security-rules": [  
      {  
        "destination": "0.0.0.0/0",  
        "icmp-options": null,  
        "is-stateless": true,  
        "protocol": "6",  
        "tcp-options": {  
          "destination-port-range": {  
            "max": null,  
            "min": null  
          },  
          "source-port-range": null  
        },  
        "udp-options": null  
      }  
    ],  
    "id":  
"ocid1.securitylist.oc1.phx.aaaaaaa7snx4jjfons6o2h33drwdh5hev6elir55hnrhi2ywqfnd5rcqk4q",  
    "ingress-security-rules": [  

```

```
{
  "icmp-options": null,
  "is-stateless": false,
  "protocol": "6",
  "source": "0.0.0.0/0",
  "tcp-options": {
    "destination-port-range": {
      "max": 3389,
      "min": 3389
    }
  },
  "source-port-range": null
},
"udp-options": null
}
],
"lifecycle-state": "AVAILABLE",
"time-created": "2017-08-23T19:50:58.104000+00:00",
"vcn-id": "ocid1.vcn.oc1.phx.aaaaaaa6va8fxr1m4hvezjk3nzo8x290qymdrwiblxw5qpzlm64rdd74vchr"
},
"etag": "d063779e"
}
```

3. Create a Subnet

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

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

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

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

```
oci iam availability-domain list -c <compartment_id>
```

Command Example and Response

```
oci iam availability-domain list -c
```


CHAPTER 9 Getting Started with the Command Line Interface

```
ocid1.compartment.oc1..aaaaaaaalkqnr7pfd92rdrwo5fm6fcoufoih1vd4ls4j9jjpge16vfyxrc11

{
  "data": [
    {
      "compartment-id":
"ocid1.compartment.oc1..aaaaaaaalkqnr7pfd92rdrwo5fm6fcoufoih1vd4ls4j9jjpge16vfyxrc11",
      "name": "EMIr:PHX-AD-1"
    },
    {
      "compartment-id":
"ocid1.compartment.oc1..aaaaaaaalkqnr7pfd92rdrwo5fm6fcoufoih1vd4ls4j9jjpge16vfyxrc11",
      "name": "EMIr:PHX-AD-2"
    },
    {
      "compartment-id":
"ocid1.compartment.oc1..aaaaaaaalkqnr7pfd92rdrwo5fm6fcoufoih1vd4ls4j9jjpge16vfyxrc11",
      "name": "EMIr:PHX-AD-3"
    }
  ]
}
```

To create a subnet in AD-1, run the following command.

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

Command Example and Response

```
oci network subnet create --vcn-id
ocid1.vcn.oc1.phx.aaaaaaaah2ast7desae6ok3amu64wozj3kskox75awryr5j2nd7tkocplajq -c
ocid1.compartment.oc1..aaaaaaaalkqnr7pfd92rdrwo5fm6fcoufoih1vd4ls4j9jjpge16vfyxrc11 --
availability-domain "EMIr:PHX-AD-1" --display-name CLISUB --dns-label "vminstances" --cidr-block
"10.0.0.0/16" --security-list-ids "
["ocid1.securitylist.oc1.phx.aaaaaaaaw7c62ybv4f5drwv2mup3f75aiquhbkbh4s676muq5t7j5tjckvlq","ocid1
.securitylist.oc1.phx.aaaaaaa7snx4jjfons6o2h33drwdh5hev6elir55hnrhi2ywqfnd5rcqk4q"]"

{
  "data": {
```

CHAPTER 9 Getting Started with the Command Line Interface

```
"availability-domain": "EMIR:PHX-AD-1",
"cidr-block": "10.0.0.0/16",
"compartment-id":
"ocidl.compartment.oc1..aaaaaaaalkqnr7pfd92rdrwo5fm6fcoufoihlvd4ls4j9jjpge16vfyxrc11",
  "dhcp-options-id":
"ocidl.dhcptoptions.oc1.phx.aaaaaaaaxnsdjmxnmmt4tpzkengrnfwspgnqzldr7qfx6cbyfaeqfbtcfa",
  "display-name": "CLISUB",
  "dns-label": "vminstances",
  "id": "ocidl.subnet.oc1.phx.aaaaaaaahvx05fhw7p320cxmdrwo5w1f50egig9cmdzslp1b1x16c5wvb5s2",
  "lifecycle-state": "PROVISIONING",
  "prohibit-public-ip-on-vnic": false,
  "route-table-id":
"ocidl.routetable.oc1.phx.aaaaaaaagdjqga3i6qrxvf23stedpre4rmkdrw6qeckftjtzyn7vctmujo2q",
  "security-list-ids": [
    "ocidl.securitylist.oc1.phx.aaaaaaaaw7c62ybv4f5drwv2mup3f75aiquhbkbh4s676muq5t7j5tjckvlq",
    "ocidl.securitylist.oc1.phx.aaaaaaa7snx4jjfons6o2h33drwdh5hev6elir55hnrhi2ywqfnd5rcqk4q"
  ],
  "subnet-domain-name": vminstances.sandboxvcn1.oraclevcn.com,
  "time-created": "2017-08-24T00:51:30.462000+00:00",
  "vcn-id": "ocidl.vcn.oc1.phx.aaaaaaa6va8fxrlm4hvzjk3nzo8x290qymdrwiblxw5qpzlm64rdd74vchr",
  "virtual-router-ip": "10.0.0.1",
  "virtual-router-mac": "00:00:17:7F:8A:D7"
},
"etag": "92d20c35"
}
```

4. Create an Internet Gateway

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

To create an Internet Gateway, run the following command.

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

Command Example and Response

```
oci network internet-gateway create -c
ocidl.compartment.oc1..aaaaaaaalkqnr7pfd92rdrwo5fm6fcoufoihlvd4ls4j9jjpge16vfyxrc11 --is-enabled
true --vcn-id ocidl.vcn.oc1.phx.aaaaaaa6va8fxrlm4hvzjk3nzo8x290qymdrwiblxw5qpzlm64rdd74vchr --
display-name sbgateway
```

```
{
  "data": {
    "compartment-id":
"ocid1.compartment.oc1..aaaaaaaalkqnr7pfd92rdrwo5fm6fcoufoih1vd4ls4j9jjpgel6vfyxrc11",
    "display-name": "sbgateway",
    "id":
"ocid1.internetgateway.oc1.phx.aaaaaaa3vcd7gmqqh4po6wnsjhcdkx1ddeqinmnbazz2wsh5gdrwt574ka",
    "is-enabled": true,
    "lifecycle-state": "AVAILABLE",
    "time-created": "2017-08-25T20:03:48.482000+00:00",
    "vcn-id": "ocid1.vcn.oc1.phx.aaaaaaa6va8fxr1m4hvzjk3nzo8x290qymdrwiblxw5qpzlm64rdd74vchr"
  },
  "etag": "d13fb7e3"
}
```

5. Add a Rule to the Route Table

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

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

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

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

Command Example and Response

```
oci network route-table list -c
ocid1.compartment.oc1..aaaaaaaalkqnr7pfd92rdrwo5fm6fcoufoih1vd4ls4j9jjpgel6vfyxrc11 --vcn-id
ocid1.vcn.oc1.phx.aaaaaaa6va8fxr1m4hvzjk3nzo8x290qymdrwiblxw5qpzlm64rdd74vchr
```

```
{
  "data": [
    {
      "compartment-id":
"ocid1.compartment.oc1..aaaaaaaalkqnr7pfd92rdrwo5fm6fcoufoih1vd4ls4j9jjpgel6vfyxrc11",
      "display-name": "Default Route Table for cli_vcn",
      "id":
"ocid1.routetable.oc1.phx.aaaaaaaagdjqga3i6qrxvf23stedpre4rmkdrw6qeekftjtzyn7vctmujo2q",
      "lifecycle-state": "AVAILABLE",
      "route-rules": [],
    }
  ]
}
```

CHAPTER 9 Getting Started with the Command Line Interface

```
"time-created": "2017-08-25T21:46:04.324000+00:00",
  "vcn-id": "ocidl.vcn.oc1.phx.aaaaaaaa6va8fxr1m4hvzjk3nzo8x290qymdrwiblxw5qpzlm64rdd74vchr"
}
]
}
```

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

To update the route rules, run the following command.

```
oci network route-table update --rt-id <route_table_id> --route-rules "
[{"cidrBlock":"<0.0.0.0/0>","networkEntityId":"<internet_gateway_id>"}]
WARNING: Updates to route-rules will replace any existing values. Are you sure you want to
continue? [y/N]: y
```

Command Example and Response

```
oci network route-table update --rt-id
ocidl.routetable.oc1.phx.aaaaaaagdjqga3i6qrxvf23stedpre4rmkdrw6qeqlftjtzyn7vctmujo2q --route-
rules "
[{"cidrBlock":"0.0.0.0/0","networkEntityId":"ocidl.internetgateway.oc1.phx.aaaaaaa3vcd7gmqqh4po6
wnsjhcdkxlddeqinmnbantz2wsh5gdrwt574ka"}]
WARNING: Updates to route-rules will replace any existing values. Are you sure you want to
continue? [y/N]: y
```

```
{
  "data": {
    "compartment-id":
"ocidl.compartment.oc1..aaaaaaaalkqnr7pfd92rdrwo5fm6fcoufoih1vd4ls4j9jjpgel6vfyxrc11",
    "display-name": "Default Route Table for cli_vcn",
    "id":
"ocidl.routetable.oc1.phx.aaaaaaa4kujevzdsnd7bh6aetvrhvzdrwcmmb1spmyj3pqwckchajvz6fa",
    "lifecycle-state": "AVAILABLE",
    "route-rules": [
      {
        "cidr-block": "0.0.0.0/0",
```

```
    "network-entity-id":
"ocidl.internetgateway.oc1.phx.aaaaaaaa3vcd7gmqgh4po6wnsjhcdkxlddeqinmnbazz2wsh5gdrwt574ka"
  }
  ],
  "time-created": "2017-08-25T23:46:04.324000+00:00", "vcn-id":
"ocidl.vcn.oc1.phx.aaaaaaaa6va8fxr1m4hvzjk3nzo8x290qymdrwiblxw5qpz1m64rdd74vchr"
  },
  "etag": "3fc998d8"
}
```

Preparing to Launch an Instance

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

- compartment-id
- availability-domain
- subnet-id
- image-id
- shape

1. Get Information About the Available Images

Help: `oci compute image list -h`

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

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

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

Command Example and Response

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

CHAPTER 9 Getting Started with the Command Line Interface

```
oci compute image list -c
ocidl.compartment.oc1..aaaaaaaaalkqnr7pfd92rdrwo5fm6fcoufoihlvd4ls4j9jjpge16vfyxrc11

{
  "base-image-id": null,
  "compartment-id": null,
  "create-image-allowed": true,
  "display-name": "Oracle-Linux-7.3-2017.03.03-0",
  "id": "ocidl.image.oc1.phx.aaaaaaaaevkccomzepja4yhahz6rguhqbuomuto7gdrw5hjimsig6syeqda",
  "lifecycle-state": "AVAILABLE",
  "operating-system": "Oracle Linux",
  "operating-system-version": "7.3",
  "time-created": "2017-03-03T19:04:30.824000+00:00"
}
```

2. Get Information About the Available Shapes

Help: `oci compute shape list -h`

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

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



Note

Shape and Block Volume Sizing

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

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

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

Command Example and Response

```
oci compute shape list -c
ocid1.compartment.oc1..aaaaaaaalkqnr7pfd92rdrwo5fm6fcoufoihlvd4ls4j9jjpgel6vfyxrc11 --
availability-domain "EMIr:PHX-AD-1"
```

```
{
  "data": [
    {
      "shape": "BM.Standard1.36"
    },
    {
      "shape": "VM.Standard1.1"
    },
    {
      "shape": "VM.Standard1.2"
    },
    {
      "shape": "VM.Standard1.4"
    },
    {
      "shape": "VM.Standard1.8"
    },
    {
      "shape": "VM.Standard1.16"
    },
    {
      "shape": "VM.DenseIO1.4"
    }
  ]
}
```

Launching a Linux Instance

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

1. Use a Public/Private Key Pair to Connect to the Instance

When you launch an instance using the CLI, you need an existing key pair to access the instance. (This key pair is not the same as an API signing key.)

2. Launch the Instance

Help: `oci compute instance launch -h`



Warning

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

To launch the Linux instance, run the following command.

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

Command Example and Response

```
oci compute instance launch --availability-domain "EMIr:PHX-AD-1" -c
ocid1.compartment.oc1..aaaaaaaalkqnr7pfd92rdrwo5fm6fcoufoihlvd4ls4j9jjpgel6vfyxrc11 --shape
"VM.Standard1.1" --display-name "Linux Instance" --image-id
ocid1.image.oc1.phx.aaaaaaa5yu6pw3riqtuhxzov7fdngi4tsteganmao54nq3pyxu3hxcuzmoa --ssh-
authorized-keys-file "C:\Users\testuser\.oci\linux_key.pem" --subnet-id
ocid1.subnet.oc1.phx.aaaaaaaahvx05fhw7p320cxmdrwo5wlf50egig9cmdzslplb1x16c5wvb5s2
```

```
{
  "data": {
    "availability-domain": "EMIr:PHX-AD-1",
    "compartment-id":
"ocid1.compartment.oc1..aaaaaaaalkqnr7pfd92rdrwo5fm6fcoufoihlvd4ls4j9jjpgel6vfyxrc11",
    "display-name": "Linux Instance",
    "extended-metadata": {},
    "id": "ocid1.instance.oc1.phx.abyhqljrtv7hhenrra6hsdrwjqvszcr2gs7c76tuuzc33iy16bz5mfnbw7q",
    "image-id":
"ocid1.image.oc1.phx.aaaaaaa5yu6pw3riqtuhxzov7fdngi4tsteganmao54nq3pyxu3hxcuzmoa",
```


CHAPTER 9 Getting Started with the Command Line Interface

```
"ipxe-script": null,
"lifecycle-state": "RUNNING",
"metadata": {
  "ssh_authorized_keys": "ssh-rsa
AAAAB3NzaABJQAAAQC1yc2EAAAEEAtaT/s9HZ24VeLUxcBNT//nPygk75BWP+kuQotPH4yP1tpqJvOBZoTKwoYa0BuoVcY4VP
1GkuCEUrpojZ5F6LybbVe0+ixpuxcPTRNZcVPZJfUVZqg7u8CCjih2T9qH9ZrOcXBJCyKrxEE2kkP4RunnS38MvuDnySYus/0
4V817sEudqWWQX88iZ04oV+Sc4vljbZiA0qNrlAJV5xfQHISL2Ejq8Q1JKaO2Mc6D4Ku/6qEwe0ihtPGoi0zFmPoWstfgc1Uq
TdiRsYECzzaWqVYpl7RO5h4pIP6/lgBfOsv/Dcg19ND7/qKnmJ4/9iKuacI2bm+HF2oR0gY4C2MvL3Q== rsa-key-
20817080\n"
},
"region": "phx",
"shape": "VM.Standard1.1",
"time-created": "2017-08-26T20:39:03.340000+00:00"
},
"etag": "2df9d1f14856a2e9a0cc239417f1ee829288b8badeb7ac6fb6d5b3553cbd148c--gzip"
}
```

3. Get VNIC Information for the Instance

Help: `oci compute instance list-vnics -h`

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

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

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

Command Example and Response

```
oci compute instance list-vnics --instance-id
ocid1.instance.oc1.phx.abcdefg6kykdowc8ozzvr4421kwp7apdrwk6wrj17su82d60c6sp4nap88d
```

```
{
  "data": [
    {
      "availability-domain": "EMIR:PHX-AD-1",
      "compartment-id":
"ocid1.compartment.oc1..aaaaaaaalkqnr7pfd92rdrwo5fm6fcoufoih1vd4ls4j9jjpgel6vfyxrc11",
      "display-name": "Linux Instance",
      "hostname-label": null,

```

```
"id": "ocidl.vnic.oc1.phx.abyhqljrxqrdruhj4nly7dp7ctr7xvclvejc7pu5rq77e37vlsq2a15y74a",
"lifecycle-state": "AVAILABLE",
"private-ip": "10.0.0.2",
"public-ip": "129.145.32.236",
"subnet-id":
"ocidl.subnet.oc1.phx.aaaaaaaaahvx05fhw7p320cxmdrwo5wlf50egig9cmdzs1plb1x16c5wvb5s2",
"time-created": "2017-08-24T00:51:30.462000+00:00"
}
[
}
```

4. Create a Block Volume for the Instance

Help: `oci bv volume create -h`

Create a block volume, using the minimum available size.



Warning

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

To create a block volume, run the following command.

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

Command Example and Response

```
oci bv volume create --availability-domain "EMTr:PHX-AD-1" -c
ocidl.compartment.oc1..aaaaaaaaalkqnr7pfd92rdrwo5fm6fcoufoihlvd4ls4j9jjpgel6vfyxrcl1 --size-in-mbs
51200 --display-name LinuxVol
```

```
{
  "data": {
    "availability-domain": "EMTr:PHX-AD-1",
    "compartment-id":
```

CHAPTER 9 Getting Started with the Command Line Interface

```
"ocid1.compartment.oc1..aaaaaaaalkqnr7pfd92rdrwo5fm6fcoufoih1vd41s4j9jjpge16vfyxrc11",
  "display-name": "LinuxVol1",
  "id": "ocid1.volume.oc1.phx.abyhq1sktp2ec7pdaz14y324drw51xruh5nxjrgbgqq7znsj5oo4t25nvcta",
  "lifecycle-state": "PROVISIONING",
  "size-in-mbs": 51200,
  "time-created": "2017-08-26T00:51:30.462000+00:00"
},
"etag": "720652578"
}
```

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



Tip

Finding out the Lifecycle State

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

5. Attach the Block Volume to the Instance

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

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

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

Command Example and Response

```
oci compute volume-attachment attach --instance-id
ocid1.instance.oc1.phx.abcdefg6kykdowc8ozzvr4421kwp7apdrwk6wrj17su82d60c6sp4nap88d --type iscsi
--volume-id ocid1.volume.oc1.phx.abyhq1jrgbktp2ec7pdaz14y324drw51xruh5nxt25gqq7znsj5oo4snvcta
```

```
{
  "data": {
    "attachment-type": "iscsi",
    "availability-domain": "EMIr:PHX-AD-1",
    "chap-secret": null,
    "chap-username": null,
    "compartment-id":
"ocidl.compartment.oc1..aaaaaaaalkqnr7pfd92rdrwo5fm6fcoufoihlvd4ls4j9jjpge16vfyxrc11",
    "display-name": null,
    "id":
"ocidl.volumeattachment.oc1.phx.abyhqlytoivg6eaybdrwb7mqms6utjrefofrplyip7filf3vtpk55h2hz1q",
    "instance-id":
"ocidl.instance.oc1.phx.abcdefgh6kykdowc8ozzvr4421kwp7apdrwk6wrj17su82d60c6sp4nap88d",
    "ipv4": null,
    "iqn": null,
    "lifecycle-state": "ATTACHING",
    "port": null,
    "time-created": "2017-08-26T00:55:30.462000+00:00",
    "volume-id": "ocidl.volume.oc1.phx.fewtr0p6pm9lj7h7rpf8w3drwlf4x9tadrw1sbs7n5qkx7dcu7bk"
  },
  "etag": "0c0afdb14a0a10ffc15283366798ac82f623433e6f5619eb2d4469612b32a332"
}
```

Launching a Windows Instance

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

1. Launch the Instance

Help: `oci compute instance launch -h`

To launch the Windows instance, run the following command.

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

Command Example and Response

```
oci compute instance launch --availability-domain "EMIr:PHX-AD-1" -c
ocid1.compartment.oc1..aaaaaaaalkqnr7pfd92rdrwo5fm6fcoufoihlvd4ls4j9jjpgel6vfyxrc11 --shape
"VM.Standard1.2" --display-name "Windows Instance" --image-id
ocid1.image.oc1.phx.aaaaaaa53cliastgvmueus5byytfldrwaibro2y4ywjebci5szc42e2b7ua --subnet-id
ocid1.subnet.oc1.phx.aaaaaaaaypsr25bzjmj3drwiha6lodzus3yn6xwgkcrqxdgafscirbhj5bpa
```

```
{
  "data": {
    "availability-domain": "EMIr:PHX-AD-1",
    "compartment-id":
"ocid1.compartment.oc1..aaaaaaaalkqnr7pfd92rdrwo5fm6fcoufoihlvd4ls4j9jjpgel6vfyxrc11",
    "display-name": "Windows Instance",
    "extended-metadata": {},
    "id": "ocid1.instance.oc1.phx.zsutzirph7cbrbx6rzu91stavdrw58puq3isknlr07zfc6rq6p9",
    "image-id":
"ocid1.image.oc1.phx.aaaaaaa53cliaskafbro2y4drwebci5szc4eus5bygvqmutflwqy2e2b7ua",
    "ipxe-script": null,
    "lifecycle-state": "PROVISIONING",
    "metadata": {},
    "region": "phx",
    "shape": "VM.Standard1.2",
    "time-created": "2017-08-26T00:51:30.462000+00:00"
  },
  "etag": "4ec3dale2415c49f55ed705c4d81edb2739da62946d36d73f816e8241e705b3b"
}
```

2. Get VNIC Information for the Instance

To get the VNIC information, run the following command.

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

3. Create a Block Volume for the Instance

To create a block volume, run the following command.

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

4. Attach the Block Volume to the Instance

To attach the Block Volume to the Windows instance, run the following command.

CHAPTER 9 Getting Started with the Command Line Interface

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

Connecting to Your Instances

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

1. Connect to Your Linux Instance

[Connecting to Your Instance](#) describes how to connect to a Linux instance from a Unix-style or Windows-style system.

2. Connect to Your Windows Instance

Help: `oci compute instance list-vnics -h` and `oci compute instance get-windows-initial-creds -h`

To connect to the instance using Remote Desktop Client (RDC), you need:

- The public IP address for the instance
- The initial Windows credentials

To get the public IP address of the Windows instance, run the following command.

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

Command Example and Response

```
oci compute instance list-vnics --instance-id ocid1.instance.oc1.phx.zsutzirph7cbrbx6rzu91stavdrw58puq3isknlr07zfc6r6p9
```

```
{
  "data": [
    {
      "availability-domain": "EMIr:PHX-AD-1",
      "compartment-id": "ocid1.compartment.oc1..aaaaaaaalkqnr7pfd92rdrwo5fm6fcoufoihlvd4ls4j9jjpge16vfyxrc11",
      "display-name": "Windows Instance",
      "hostname-label": null,
      "id": "ocid1.vnic.oc1.phx.abyhqljr5m5mmra3ecxasw6vdrwq5ft23dqn4dlr145hdggz6rgfdwpp4ija",

```

CHAPTER 9 Getting Started with the Command Line Interface

```
"lifecycle-state": "AVAILABLE",
"private-ip": "10.10.0.3",
"public-ip": "129.142.0.212",
"subnet-id":
"ocidl.subnet.oc1.phx.aaaaaaaahvx05fhw7p320cxmdrwo5w1f50egig9cmdzs1plb1x16c5wvb5s2",
"time-created": "2017-08-26T00:51:30.462000+00:00"
}
]
}
```

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

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

Command Example and Response

```
oci compute instance get-windows-initial-creds --instance-id
ocidl.instance.oc1.phx.zsutzirph7cbrbx6rzu91stavdrw58puq3isknlr07zfc6rqp9
```

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

[Connecting to Your Windows Instance](#) describes how to connect to your instance using RDC.

Cleaning Up the Test Environment

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

Detach and Delete the Block Volumes

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

CHAPTER 9 Getting Started with the Command Line Interface

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

1. Get the `volume-attachment-id`

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

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

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

Command Example and Response

```
oci compute volume-attachment list -c
ocidl.compartment.oc1..aaaaaaaaalkqnr7pfd92rdrwo5fm6fcoufoihlvd4ls4j9jjpge16vfyxrc11

{
  "data": [
    {
      "attachment-type": "iscsi",
      "availability-domain": "EMIr:PHX-AD-1",
      "chap-secret": null,
      "chap-username": null,
      "compartment-id":
"ocidl.compartment.oc1..aaaaaaaaalkqnr7pfd92rdrwo5fm6fcoufoihlvd4ls4j9jjpge16vfyxrc11",
      "display-name": null,
      "id":
"ocidl.volumeattachment.oc1.phx.abyhqlytoivg6eaybdrwb7mqqms6utjrefofrplyip7filf3vtpk55h2hzlq",
      "instance-id":
"ocidl.instance.oc1.phx.abcdefg6kykdowc8ozzvr4421kwp7apdrwk6wrj17su82d60c6sp4nap88d",
      "ipv4": "169.254.2.2",
      "iqn": "iqn.2015-12.com.oracleiaas:e3fd73db-b164-4d76-bc3f-f58b093989d0",
      "lifecycle-state": "ATTACHED",
      "port": 3260,
      "time-created": "2017-08-26T00:51:30.462000+00:00",
      "volume-id":
"ocidl.volume.oc1.phx.abyhqpa3ati7ggfjvba7y6dcg7imdrwskq4bd1jroo2cbwchrebuprxdvca"
    }
  ]
}
```

2. Detach the `volume-attachment-id`

CHAPTER 9 Getting Started with the Command Line Interface

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

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

Command Example and Response

```
oci compute volume-attachment detach --volume-attachment-id
ocid1.volumeattachment.oc1.phx.abyhqlytoivg6eaybdrwb7mqms6utjrefofrplyip7filf3vtpk55h2hzlq
Are you sure you want to delete this resource? [y/N]:
```



Tip

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

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

3. Delete the Block Volume

To delete the block volume, run the following command.

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

Command Example and Response

```
oci bv volume delete --volume-id
ocid1.volume.oc1.phx.abyhq1jroo2cbwchrpa3ati7ggfjvba7y6dcg7imnleskq4bdebuprxddvca --force
```

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

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

CHAPTER 9 Getting Started with the Command Line Interface

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

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

Terminate the Instances

Help: `oci compute instance terminate -h`

To delete the Linux instance, run the following command.

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

Command Example and Response

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

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

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

To delete the Windows instance, run the following command.

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

Command Example and Response

```
oci compute instance terminate --instance-id
ocid1.instance.oc1.phx.zsutzirph7cbrbx6rzu91stavdrw58puq3isknlr07zfc6r6p9
```

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

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

Delete the Virtual Cloud Network

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

It takes the following 2 steps to delete the VCN.

1. Delete the subnet

To delete the subnet, run the following command.

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

Command Example and Response

```
oci network subnet delete --subnet-id  
ocid1.subnet.oc1.phx.aaaaaaaahvx05fhw7p320cxmdrwo5wlf50egig9cmdzs1plb1x16c5wvb5s2 --force
```

None

2. Delete the virtual cloud network

To delete the VCN, run the following command.

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

Command Example and Response

```
oci network vcn delete --vcn-id  
ocid1.vcn.oc1.phx.aaaaaaa6va8fxr1m4hvzjk3nzo8x290qymdrwiblxw5qpzlm64rdd74vchr --force
```

None

CHAPTER 10 Getting Started with the Terraform Provider

This topic provides instructions for downloading and installing both Terraform and the Oracle Cloud Infrastructure Terraform provider, and provides a brief introduction to the key concepts for understanding and using the Oracle Cloud Infrastructure Terraform provider.

Terraform Overview

Terraform is "infrastructure-as-code" software that allows you to define your infrastructure resources in files that you can persist, version, and share. These files describe the steps required to provision your infrastructure and maintain its desired state; it then executes these steps and builds out the described infrastructure.

Terraform's configuration and execution building blocks are modules, which are self-contained configuration packages. You can use these modules to organize your code and to create reusable components. HashiCorp, the developer of Terraform, provides a library of open-source Terraform modules "out of the box" to support many common tasks.

To use Terraform for Oracle Cloud Infrastructure, you must download two components - Terraform from HashiCorp, and then the Oracle Cloud Infrastructure Terraform provider.

Download and Install Terraform

Download Terraform from the [HashiCorp download page](#). Ensure that you download the correct binary file for your system.



Important

The Oracle Cloud Infrastructure Terraform provider version 2.2.0 and greater requires Terraform version 0.10.1 or greater.

Download the Oracle Cloud Infrastructure Terraform Provider

Prerequisites for Installing and Using the Terraform Provider

- An Oracle Cloud Infrastructure account that has user credentials sufficient to execute a Terraform plan.
- A user in that account.
- Required keys and Oracle Cloud Infrastructure IDs (OCIDs). For guidance, see "Required Keys and OCIDs" in the *Oracle Cloud Infrastructure User Guide*.
- The correct Terraform binary file for your operating system (version 0.10.1 or greater).

Installing and Configuring the Terraform Provider

- For guidance on installing or on upgrading a previous version of the Oracle Cloud Infrastructure Terraform provider, see [Terraform Provider Version 3](#).
- For guidance on setting up the Terraform provider, see [Oracle Cloud Infrastructure Provider](#).

For More Information

- [GitHub](#)
- [Hashicorp Terraform Documentation](#)
- [Creating Terraform Modules](#)
- [Terraform Configurations](#)
- [Terraform Configuration Syntax](#)

CHAPTER 11 Getting Started with Load Balancing

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

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

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

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

Before You Begin

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

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

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

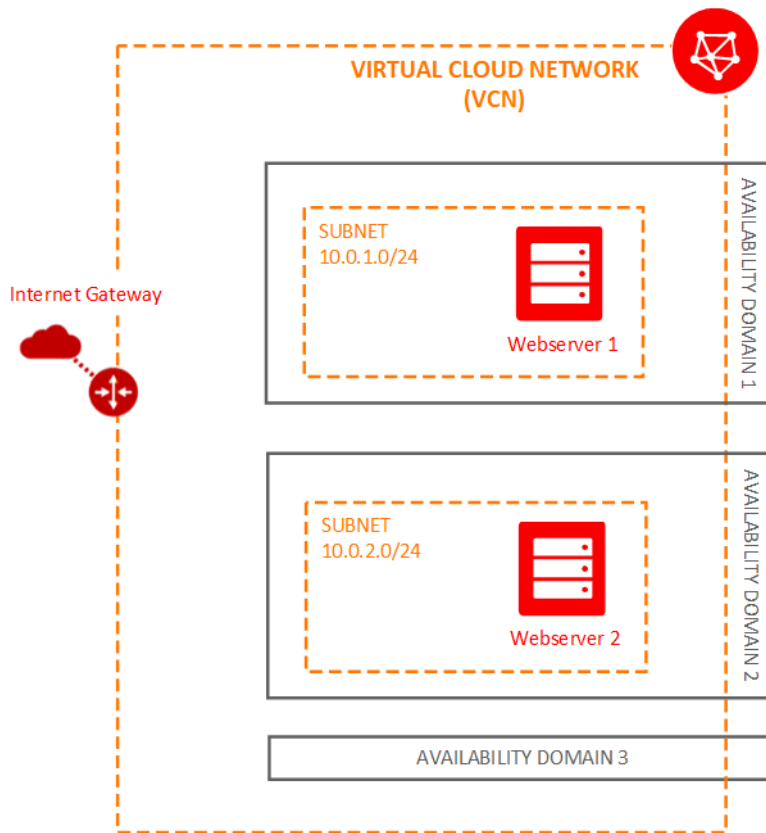


Tip

If you need an introduction to VCNs and instances, try the [Tutorial - Launching Your First Linux Instance](#) first.

VCN and Instance Setup

The following diagram shows the prerequisite VCN and instances:



Create a VCN

The quick VCN flow automatically creates three subnets (one in each availability domain), but you need instances in only two of them.

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

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

2. Click **Create Virtual Cloud Network**.
3. Enter the following:
 - **Name:** Enter a name for your cloud network, for example, LB_Network. Avoid entering confidential information.
 - **Create in Compartment:** This field defaults to your current compartment. Select the compartment you want to create the VCN in, if not already selected.
 - Select **Create Virtual Cloud Network Plus Related Resources**. The dialog expands to list the items that will be created with your cloud network.
 - Accept the defaults for any other fields.
4. Scroll to the bottom of the dialog and click **Create Virtual Cloud Network**.

A confirmation page displays the details of the cloud network that you just created. The cloud network has the following resources and characteristics (some of which are not listed in the confirmation dialog):

- CIDR block range of 10.0.0.0/16
- An internet gateway
- A route table with a default route rule to enable traffic to and from the internet gateway
- A default security list. You will edit this default security list later in the tutorial.
- A public subnet in each availability domain.
- The VCN will automatically use the Internet and VCN Resolver for DNS.

Launch two instances

This example uses the VM .Standard1.1 shape (one core and 7 GB of RAM). If you prefer, you can choose a larger shape.

1. Open the navigation menu. Under **Core Infrastructure**, go to **Compute** and click **Instances**.
2. Click **Create Instance**.
3. In the **Create Instance** dialog, enter the following:
 - a. **Name:** Enter a name, for example: Webserver1.
 - b. **Availability Domain:** Select the first availability domain in the list (AD-1).
 - c. **Image:** Select the Oracle-Linux-7.5 image.
 - d. **Shape:** Select VM Standard2.1 (1 OCPU, 15GB RAM)
 - e. **SSH Keys:** Paste in the public key portion of your SSH key pair. Ensure that you paste in only the string of characters that make up the key itself; do not include any comments from the key file.
If you do not have an SSH key pair, see [Creating a Key Pair](#).
 - f. **Virtual Cloud Network:** Select the cloud network you created.
 - g. **Subnet:** Select the public subnet in availability domain 1.
 - h. Click **Show Advanced Options** and for **Hostname:** Leave blank.
 - i. Click **Create Instance**.
4. Repeat the previous steps. This time, enter the name "Webserver2" and select the subnet in availability domain 2.

Start a web application on each instance

This example uses Apache HTTP Server.

1. Connect to your instance. If you need help, see [Connecting to Your Instance](#).
2. Run yum update:

CHAPTER 11 Getting Started with Load Balancing

```
sudo yum -y update
```

3. Install the Apache HTTP Server:

```
sudo yum -y install httpd
```

4. Allow Apache (HTTP and HTTPS) through the firewall:

```
sudo firewall-cmd --permanent --add-port=80/tcp
```

```
sudo firewall-cmd --permanent --add-port=443/tcp
```



Note

Open the Firewall

If you choose to run a different application than Apache, ensure that you run the preceding command to open the firewall for your application's port.

5. Reload the firewall:

```
sudo firewall-cmd --reload
```

6. Start the web server:

```
sudo systemctl start httpd
```

7. Add an index.htm file on each server that indicates which server it is, for example:

a. On Webserver 1:

```
sudo su
```

```
echo 'WebServer1' >/var/www/html/index.html
```

b. On Webserver 2:

```
sudo su
```

```
echo 'WebServer2' >/var/www/html/index.html
```

Tutorial Overview

In this tutorial, you create a public load balancer and verify it. A load balancer requires configuration of several components to be functional, and this tutorial walks you through each step to help you understand these components.

To create and test the load balancer, complete the following steps:

1. [Add two subnets to your VCN to host your load balancer.](#)
2. [Create a load balancer.](#)
3. [Create a backend set with health check.](#)
4. [Add backend servers to your backend set.](#)
5. [Create a listener.](#)
6. [Update the load balancer subnet security list and allow internet traffic to the listener.](#)
7. [Verify your load balancer.](#)
8. [Update rules to protect your backend servers.](#)
9. [Terminate your load balancer.](#)

Add Two Subnets to Your VCN to Host Your Load Balancer

Your load balancer must reside in different subnets from your application instances. This configuration allows you to keep your application instances secured in subnets with stricter access rules, while allowing public internet traffic to the load balancer in the public subnets.

To add the public subnets to your VCN:

Add a Security List

1. Open the navigation menu. Under **Core Infrastructure**, go to **Networking** and click **Virtual Cloud Networks**.
The list of VCNs in the current compartment is displayed.
2. Click the name of the VCN that includes your application instances.

3. Under **Resources**, click **Security Lists**.
4. Click **Create Security List**.
 - a. **Create in Compartment:** This field defaults to your current compartment. Select the compartment you want to create the security list in, if not already selected.
 - b. Enter a **Name**, for example, "LB Security List".
 - c. Delete the entry for the ingress rule and the entry for the egress rule. The security list must have no rules. The correct rules are added automatically during the load balancer workflow.
 - d. **Tags:** Leave as is (you can add tags later if you like).
 - e. Click **Create Security List**.
 - f. Return to your Virtual Cloud Network Details page.

Add a Route Table

1. Under **Resources**, click **Route Tables**.
2. Click **Create Route Table**. Enter the following:
 - a. **Create in Compartment:** This field defaults to your current compartment. Select the compartment you want to create the route table in, if not already selected.
 - b. **Name:** Enter a name, for example, "LB Route Table".
 - c. **Target Type:** Select Internet Gateway.
 - d. **Destination CIDR Block:** Enter 0.0.0.0/0.
 - e. **Compartment:** Select the compartment that contains your VCN's internet gateway.
 - f. **Target:** Select your VCN's internet gateway.
 - g. **Tags:** Leave as is (you can add tags later if you like).
 - h. Click **Create Route Table**.

Create the first subnet

1. Under **Resources**, click **Subnets**.
2. Click **Create Subnet**.
3. Enter or select the following:
 - a. **Name:** Enter a name, for example, "LB Subnet 1".
 - b. **Availability Domain:** Choose the first availability domain (AD-1).
 - c. **CIDR Block:** Enter 10.0.4.0/24.
 - d. **Route Table:** Select the LB Route Table you created.
 - e. **Subnet Access:** Select **Public Subnet**.
 - f. **DNS Resolution:** Select **Use DNS Hostnames in this Subnet**.
 - g. **DHCP Options:** Select Default DHCP Options for LB_Network.
 - h. **Security Lists:** Select the LB Security List you created.
 - i. **Tags:** Leave as is (you can add tags later if you like).
4. Click **Create**.

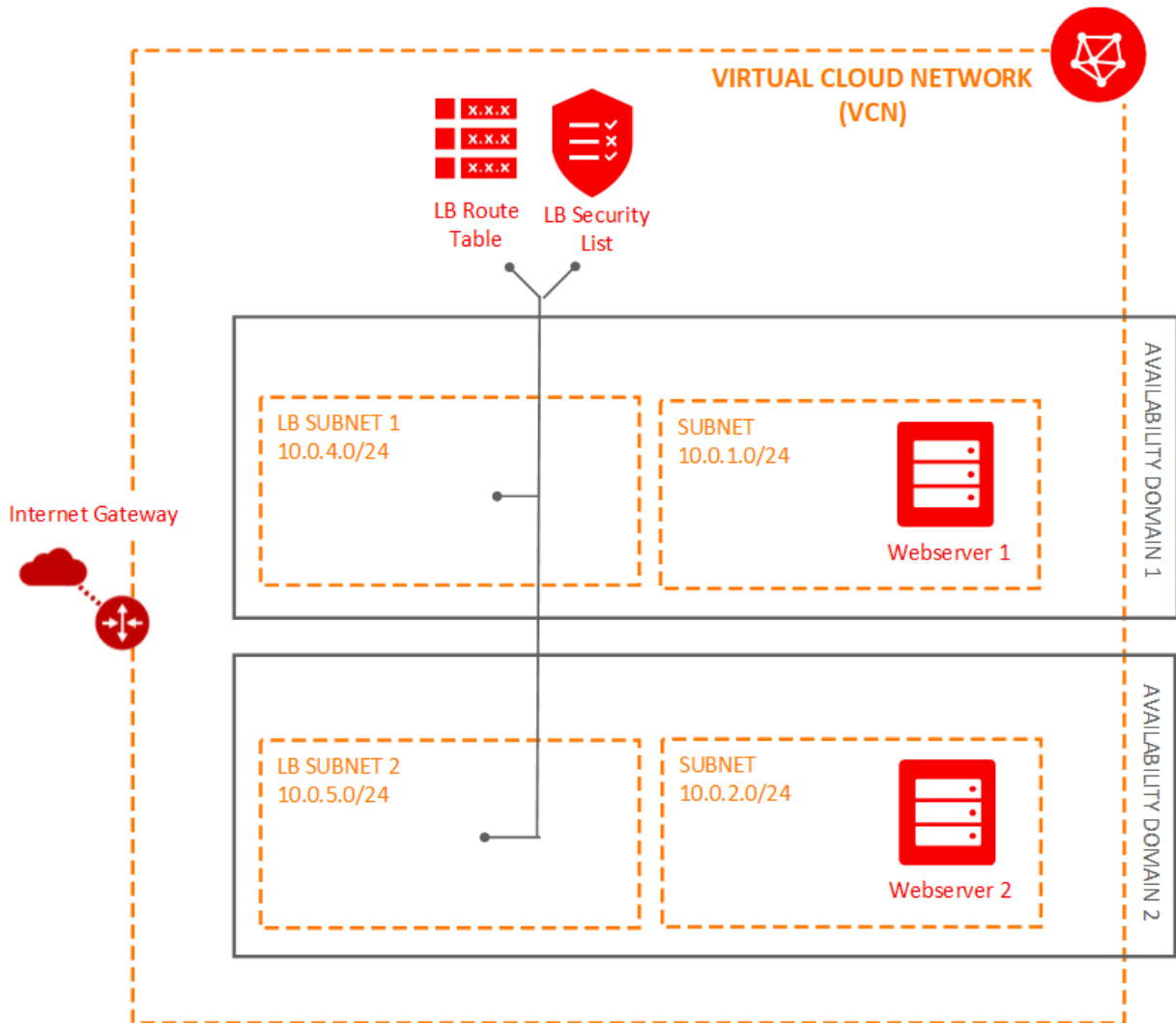
Create the second subnet

Create a second load balancer subnet in a different availability domain.

1. In the details page of your VCN, click **Create Subnet**.
2. Enter the following:
 - a. **Name:** Enter a name, for example, "LB Subnet 2".
 - b. **Availability Domain:** Choose the second availability domain (AD-2).
 - c. **CIDR Block:** Enter 10.0.5.0/24.
 - d. **Route Table:** Select the LB Route Table you created.
 - e. **Subnet Access:** Select **Public Subnet**.
 - f. **DNS Resolution:** Select **Use DNS Hostnames in this Subnet**.

- g. **DHCP Options:** Select Default DHCP Options for LB_Network.
 - h. **Security Lists:** Select the LB Security List you created.
 - i. **Tags:** Leave as is (you can add tags later if you like).
3. Click **Create**.

The following figure shows the new components added to the VCN:



Create the Load Balancer

When you create a public load balancer, you choose its shape (size) and you select two subnets, each in a different availability domain. This configuration ensures that the load

balancer is highly available. It is active in only one subnet at a time. This load balancer comes with a public IP address and provisioned bandwidth corresponding to the shape you chose.

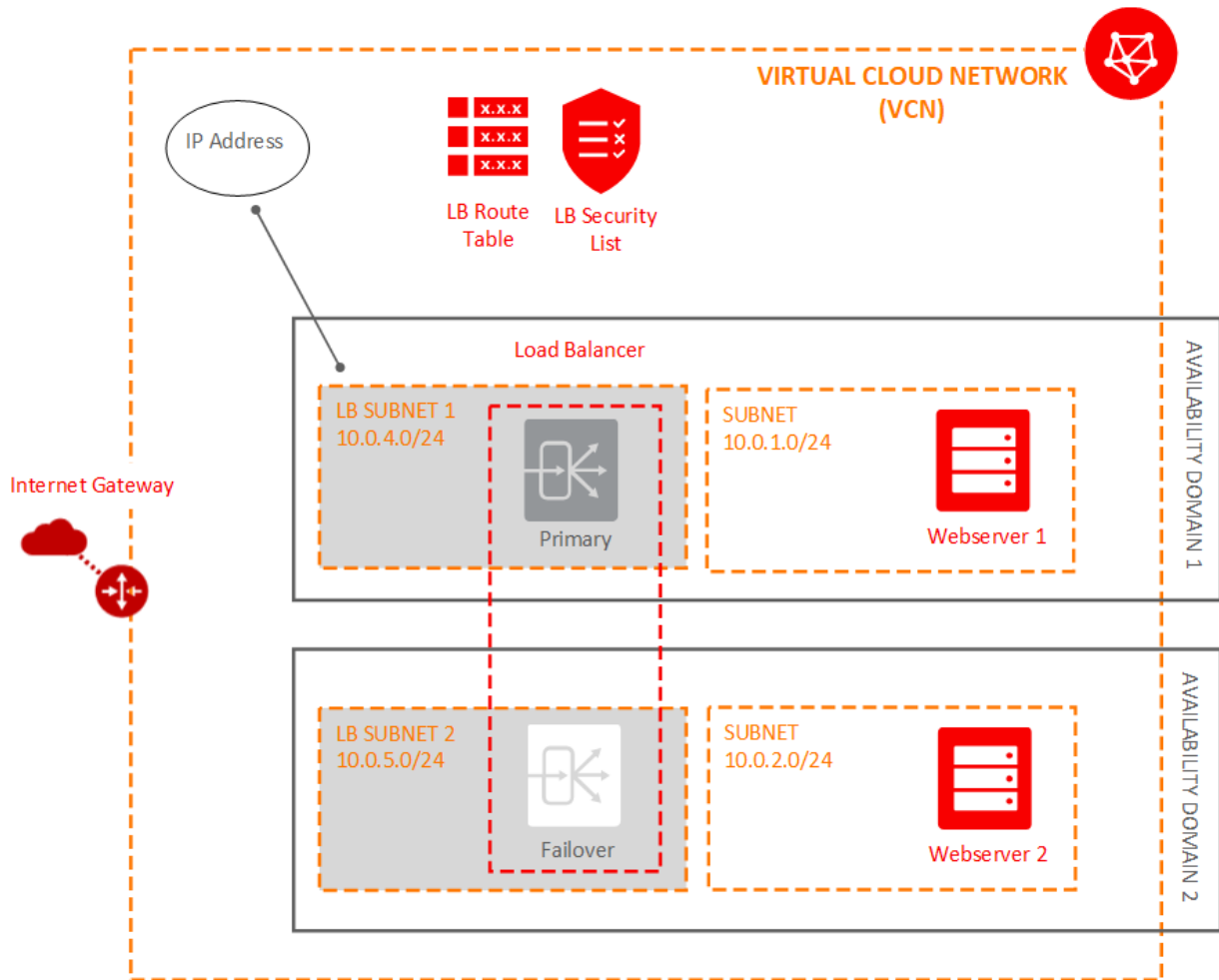


Tip

Although the load balancer resides in a subnet, it can direct traffic to backend sets that reside in any of the subnets within the VCN.

1. Open the navigation menu. Under the **Core Infrastructure** group, go to **Networking** and click **Load Balancers**.
Ensure that the Sandbox compartment (or the compartment designated for you) is selected on the left.
2. Click **Create Load Balancer**.
3. Enter the following:
 - **Name:** Enter a name for your load balancer.
 - **Shape:** Select 100 Mbps. The shape specifies the bandwidth of the load balancer. For the tutorial, use the smallest shape. The shape cannot be changed later.
 - **Virtual Cloud Network:** Select the virtual cloud network for your load balancer.
 - **Visibility:** Choose **Create Public Load Balancer**.
 - **Subnet (1 of 2):** Select LB Subnet 1.
 - **Subnet (2 of 2):** Select LB Subnet 2. The second subnet must be in a different availability domain than the first subnet you chose.
4. Click **Create**.

When the load balancer is created, you get a public IP address. You route all your incoming traffic to this IP address. The IP address is available from both subnets that you specified, but it is active in only one subnet at a time.



Create a Backend Set

A backend set is a collection of backend servers to which your load balancer directs traffic. A list of backend servers, a load balancing policy, and a health check script define each backend set. A load balancer can have multiple backend sets, but for this tutorial, you create only one backend set that includes both of your web servers.

In this step, you define the backend set policy and health check. You add your servers in a separate step.

To create the backend set:

1. Click the name of your load balancer and view its details.
2. Click **Create Backend Set**.
3. In the dialog box, enter:
 - a. **Name:** Give your load balancer backend set a name. The name cannot contain spaces.
 - b. **Policy:** Choose Weighted Round Robin.

What is a policy?

The policy determines how traffic is distributed to your backend servers.

- Round Robin - This policy distributes incoming traffic sequentially to each server in a backend set list. When each server has received a connection, the load balancer repeats the list in the same order.
 - IP Hash - This policy uses an incoming request's source IP address as a hashing key to route non-sticky traffic to the same backend server. The load balancer routes requests from the same client to the same backend server as long as that server is available.
 - Least Connections - This policy routes incoming non-sticky request traffic to the backend server with the fewest active connections.
4. Enter the Health Check details.

Load Balancing automatically checks the health of the instances for your load balancer. If it detects an unhealthy instance, it stops sending traffic to the instance and reroutes traffic to healthy instances. In this step, you provide the information required to check the health of servers in the backend set and ensure that they can receive data traffic.

 - **Protocol:** Select HTTP.
 - **Port:** Enter 80

- **URL Path (URI):** Enter /

The rest of the fields are optional and can be left blank for this tutorial.

5. Click **Create**.

When the Backend Set is created, the Work Request shows a status of Succeeded. Close the Work Request dialog box.

Add Backends (Servers) to Your Backend Set

After the backend set is created, you can add compute instances (backend servers) to it. To add a backend server, you can enter the OCID for each instance and your application port. The OCID enables the Console to create the security list rules required to enable traffic between the load balancer subnets and the instance subnets.



Tip

Security lists are virtual firewall rules for your VCN that provide ingress and egress rules to specify the types of traffic allowed in and out of a subnet. Update your VCN's security list rules to allow traffic flow between the load balancer subnets and the backend server subnets. In this step, you can have the security lists automatically updated by providing the instance OCIDs.

To add a server to your backend set:

1. On the details page of your load balancer, click **Backend Sets**. The backend set you just created is displayed.
2. Click the name of the backend set and view its details.
3. Click **Edit Backends**.

In the dialog:

1. Ensure that **Help me create proper security list rules** is checked.

What rules are added to my security lists?

The system updates the security list used by your load balancer subnets to allow egress traffic from the load balancer to each backend server's subnet:

- Updates to the security list for your load balancer subnets:
 - Allow egress traffic to the backend server 1 subnet (for example, Public-Subnet-AD1)
 - Allow egress traffic to the backend server 2 subnet (for example, Public-Subnet-AD2)

Egress Rules for LB Security List				
Stateful Rules				
Destination: 10.0.1.0/24	IP Protocol: TCP	Source Port Range: All	Destination Port Range: 80	Allows: TCP traffic for ports: all
Destination: 10.0.0.0/24	IP Protocol: TCP	Source Port Range: All	Destination Port Range: 80	Allows: TCP traffic for ports: all

The system updates the security list used by your backend server subnets to allow ingress traffic from the load balancer subnets:

- Updates to the security list for your backend server subnets:
 - Allow ingress traffic from load balancer subnet 1
 - Allow ingress traffic from load balancer subnet 2

CHAPTER 11 Getting Started with Load Balancing

Stateful Rules				
Source: 0.0.0.0/0	IP Protocol: TCP	Source Port Range: All	Destination Port Range: 22	Allows: TCP traffic for ports: all
Source: 0.0.0.0/0	IP Protocol: ICMP	Type and Code: 3, 4		Allows: ICMP traffic for: 3, 4 Destination Unreachable: Fragmentation Needed and Don't Fragment was Set
Source: 10.0.0.0/16	IP Protocol: ICMP	Type and Code: 3		Allows: ICMP traffic for: 3 Destination Unreachable
Source: 10.0.4.0/24	IP Protocol: TCP	Source Port Range: All	Destination Port Range: 80	Allows: TCP traffic for ports: all
Source: 10.0.5.0/24	IP Protocol: TCP	Source Port Range: All	Destination Port Range: 80	Allows: TCP traffic for ports: all

2. **OCID**: Paste the OCID of the first instance (Webserver1).

How do I get the OCID of an instance?

The OCID (Oracle Cloud Identifier) is displayed when you view the instance, both in the list view and on the details page.

- a. In the dialog, right-click **View Instances** and select a browser option to open the link in a new tab.

CHAPTER 11 Getting Started with Load Balancing

Edit Backends [help](#) [cancel](#)

Specify the Compute instance OCID or private IP address and the port for the web/application backend servers you want to include in this backend set.

[View instances](#)

Traffic between this load balancer and its backend servers is subject to the governing security lists.

[Learn more about Load Balancers and Security Lists.](#)

Backend 1 *Undefined: will not be submitted with the form*

<input checked="" type="checkbox"/> HELP ME CREATE PROPER SECURITY LIST RULES	INSTANCE OCID	PORT	WEIGHT
	<input type="text"/>	<input type="text"/>	<input type="text"/>

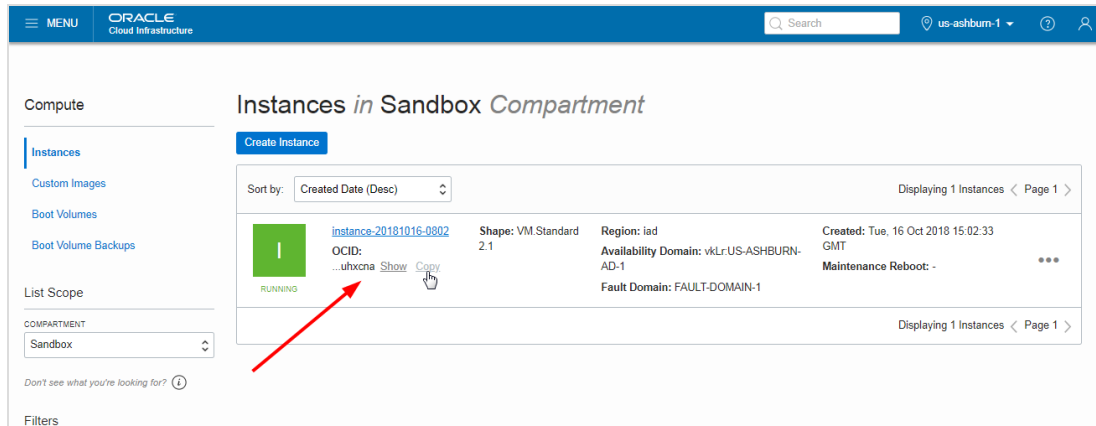
A new Console browser tab launches, displaying the instances in the current compartment.

- b. In the tab that just opened, if your instances are not in the current compartment, select the compartment to which the instance belongs. (Select from the list on the left side of the page.)

A shortened version of the OCID is displayed next to each instance.

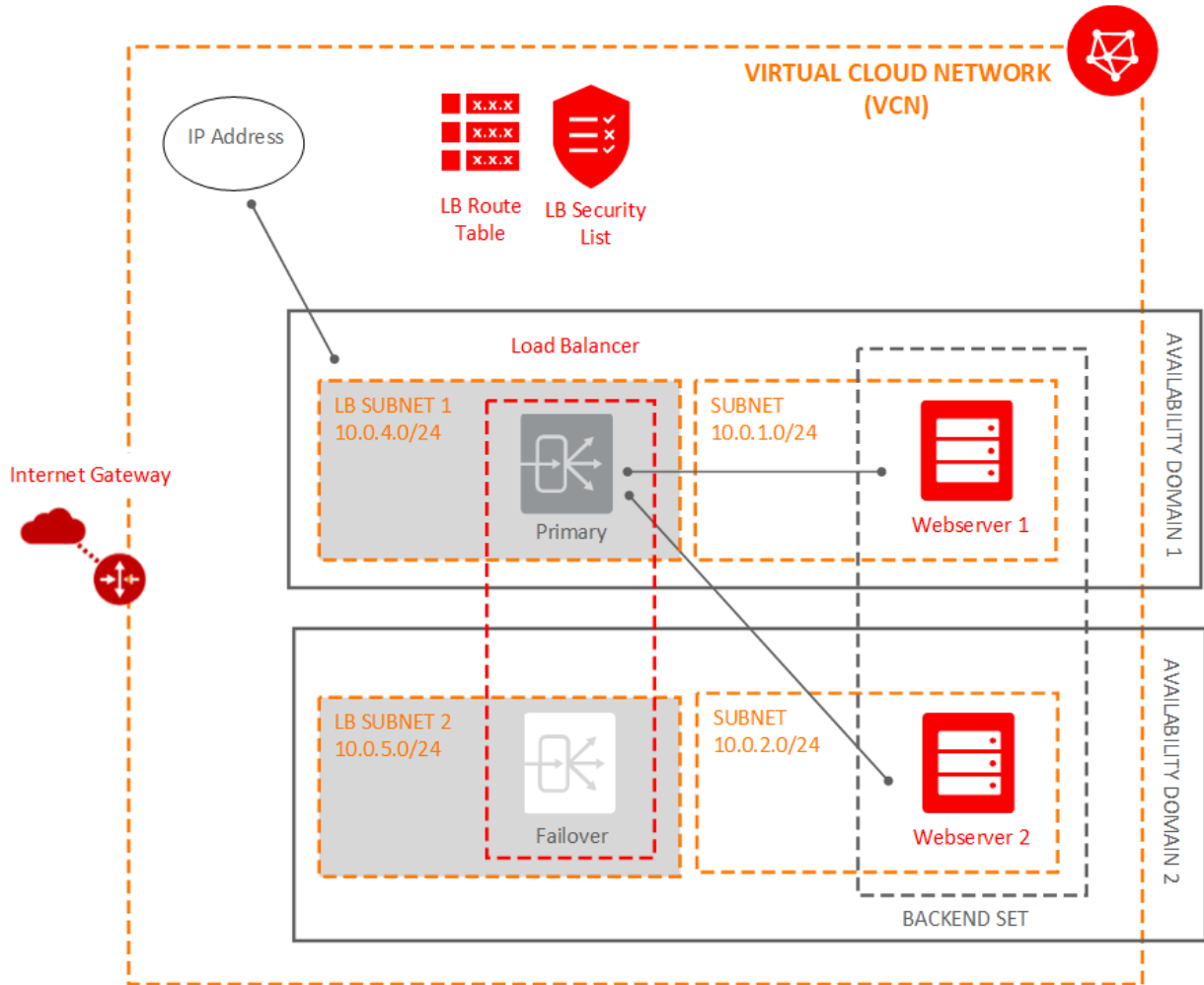
- c. Click **Copy** to copy the OCID. You can then paste it into the Instance ID field.

CHAPTER 11 Getting Started with Load Balancing



3. **Port:** Enter 80.
4. **Weight:** Leave blank to weight the servers evenly.
5. Repeat Steps 2 through 4, pasting in the OCID for the second instance (Webserver2).
6. Click **Create Rules**.

The following figure shows the components created in this task:



Create the Listener for Your Load Balancer

A listener is an entity that checks for connection requests. The load balancer listener listens for ingress client traffic using the port you specify within the listener and the load balancer's public IP.

In this tutorial, you define a listener that accepts HTTP requests on port 80.



Note

Listening on Multiple Ports

A listener can listen on one port. To listen on more ports (such as 443 for SSL), create another listener. For information on enabling SSL for your load balancer, see "Managing SSL Certificates" in the *Oracle Cloud Infrastructure User Guide*.

To create a listener:

1. On your Load Balancer Details page, click **Listeners**.
2. Click **Create Listener**.
3. Enter the following:
 - **Name:** Enter a friendly name.
 - **Protocol:** Select HTTP.
 - **Port:** Enter 80 as the port on which to listen for incoming traffic.
 - **Backend Set:** Select the backend set you created.
4. Click **Create**.

Update Load Balancer Security Lists and Allow Internet Traffic to the Listener

When you create a listener, you must also update your VCN's security list to allow traffic to that listener.

Allow the Listener to Accept Traffic

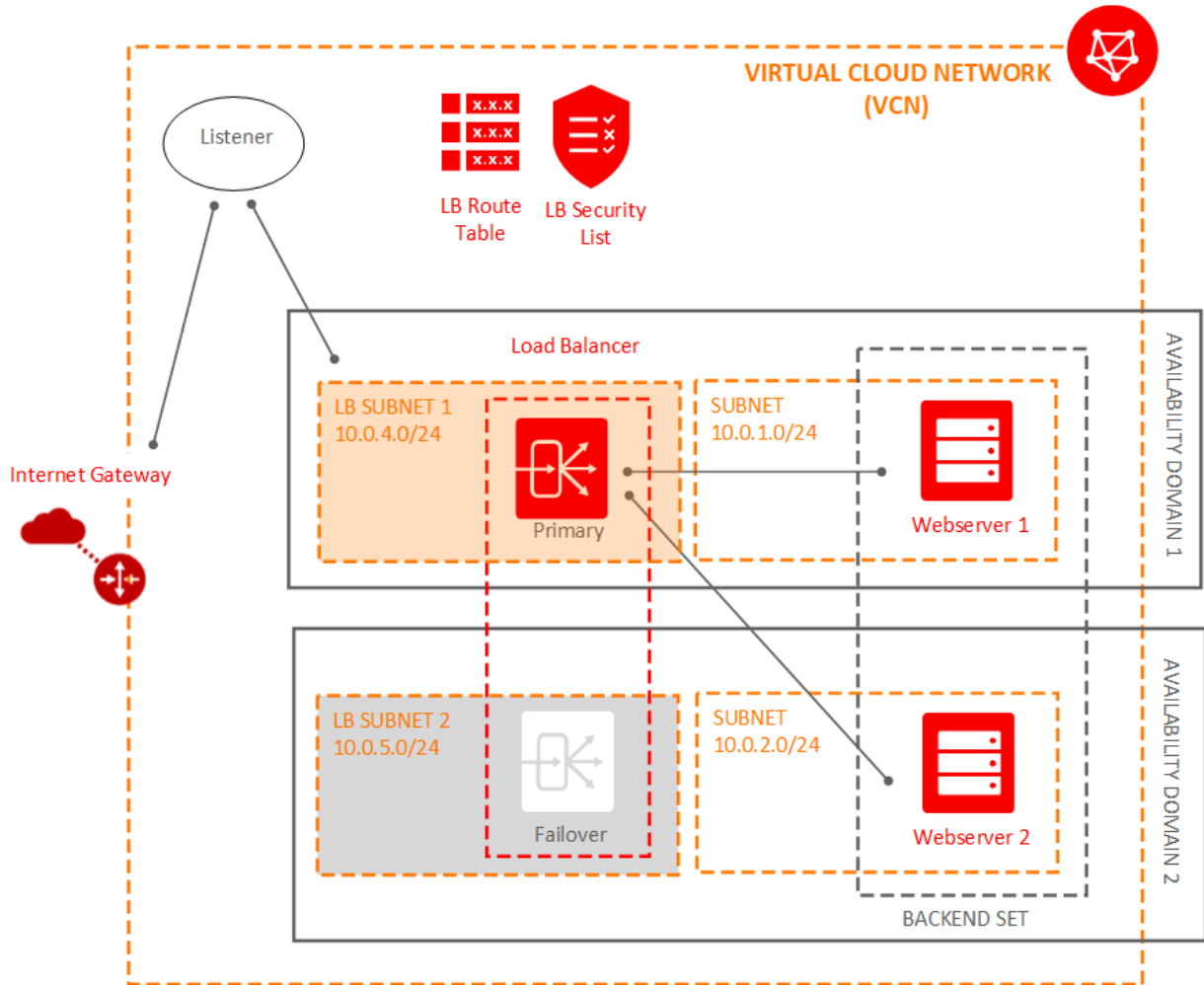
The subnets where the load balancer resides must allow the listener to accept traffic. To enable the traffic to get to the listener, update the load balancer subnet's security list.

To update the security list to allow the listener to accept traffic:

1. Open the navigation menu. Under **Core Infrastructure**, go to **Networking** and click **Virtual Cloud Networks**.
The list of VCNs in the current compartment is displayed.
2. Click **Security Lists**.
A list of the security lists in the cloud network is displayed.
3. Click the LB Security List.
The details are displayed.
4. Click **Edit All Rules**.
5. Under Allow Rules for Ingress, click **Add Rule**.
6. Enter the following ingress rule:
 - **Source Type:** Select CIDR
 - **Source CIDR:** Enter 0.0.0.0/0
 - **IP Protocol:** Select TCP
 - **Destination Port Range:** Enter 80 (the listener port).
7. Click **Save Security List Rules**.

If you created other listeners, add an ingress rule for each listener port to allow traffic to the listener. For example, if you created a listener on port 443, repeat the previous steps using **Destination Port Range:** 443.

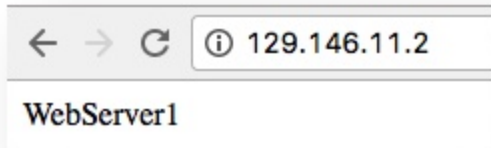
The following figure shows the component created in this task:



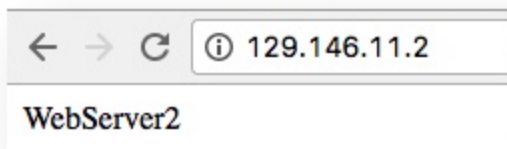
Verify Your Load Balancer

To test your load balancer's functionality, you can open a web browser and navigate to its public IP address (listed on the load balancer's detail page). If the load balancer is properly configured, you can see the name of one of the web server instances:

1. Open a web browser.
2. Enter the load balancer public IP address.
The index.htm page of one of your web servers appears.



3. Refresh the web page.
The index.htm page of the other web server now appears.



Because you configured the load balancer backend set policy as Round Robin, refreshing the page alternates between the two web servers.

Update Rules to Limit Traffic to Backend Servers

Update the default security list and the default route table to limit traffic to your backend servers. If you used the **Create Virtual Cloud Network Plus Related Resources** option to create your VCN and you are not going to terminate this load balancer immediately, these actions are important.

To delete the default route table rule:

CHAPTER 11 Getting Started with Load Balancing

1. Open the navigation menu. Under **Core Infrastructure**, go to **Networking** and click **Virtual Cloud Networks**.
2. Click the name of your VCN and review its details.
3. Under **Resources**, click **Route Tables**.
4. Click the Default Route Table for the VCN.
5. Click **Edit Route Rules**.
6. Click the **X** next to the route rule, and then click **Save**.

There are now no Route Rules for the default route table.

To edit the default security list rules:

1. Go to your **Virtual Cloud Network Details** page.
2. Under **Resources**, click **Security Lists**.
3. Click the Default Security List for the VCN.
4. Click **Edit All Rules**.
5. Under **Allow Rules for Ingress**, delete the following rules:

Action	Source CIDR	IP Protocol	Destination Port Range
Delete	0.0.0.0/0	TCP	22
Delete	0.0.0.0/0	ICMP	3,4
Delete	10.0.0.0/16	ICMP	3

6. Under **Allow rules for Egress**, delete the rule. There can be no Egress Rules.

Now your instances can receive data traffic from, and direct traffic to, only the load balancer subnets. You no longer can connect directly to your instance's public IP address.

Delete Your Load Balancer

When your load balancer becomes available, you are billed for each hour that you keep it running. Once you no longer need a load balancer, you can delete it. When the load balancer is deleted, you stop incurring charges for it. Deleting a load balancer does not affect the backend servers or subnets used by the load balancer.

To delete your load balancer:

1. Open the navigation menu. Under the **Core Infrastructure** group, go to **Networking** and click **Load Balancers**.
2. Choose the **Compartment** that contains your load balancer.
3. Next to your load balancer, click the Actions icon (three dots), and then click **Terminate**.
4. Confirm when prompted.

If you want to delete the instances and VCN you created for this tutorial, follow the instructions in [Cleaning Up Resources from the Tutorial](#).

CHAPTER 12 Putting Data into Object Storage

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

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

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

Creating a Bucket

To create a bucket to store objects:

1. Open the navigation menu. Under **Core Infrastructure**, click **Object Storage**.
A list of the buckets in the compartment you're viewing is displayed.
2. Select a compartment from the **Compartment** list on the left side of the page.
A list of existing buckets is displayed.
3. Click **Create Bucket**.
4. In the **Create Bucket** dialog box, specify the attributes of the bucket:
 - **Bucket Name:** The system generates a default bucket name that reflects the current year, month, day, and time, for example **bucket-20190306-1359**. If you change this default to any other bucket name, use letters, numbers, dashes, underscores, and periods. Do not include any confidential information.
 - **Storage Tier:** Select the tier in which you want to store your data. Available tiers include:
 - **Standard** is the primary, default Object Storage tier for storing frequently accessed data that requires fast and immediate access.

- **Archive** is a special tier for storing infrequently accessed data that requires long retention periods. Access to data in the **Archive** tier is not immediate. You must restore archived data before it's accessible. For more information, see "[Overview of Archive Storage](#)" in the *Oracle Cloud Infrastructure User Guide*.
 - **Object Events:** Select **Emit Object Events** if you want to enable the bucket to emit events for object state changes. For more information about events, see [Overview of Events](#).
 - **Encryption:** Buckets are encrypted with keys managed by Oracle by default, but you can optionally encrypt the data in this bucket using your own Key Management encryption key. To use Key Management for your encryption needs, select **Encrypt Using Customer-Managed Keys**. Then, select the **Vault Compartment** and **Vault** that contain the master encryption key you want to use. Also select the **Master Encryption Key Compartment** and **Master Encryption Key**. For more information about encryption, see [Overview of Key Management](#). For details on how to create a vault, see [Managing Vaults](#).
 - **Tags:** Optionally, you can apply tags. If you have permissions to create a resource, you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see [Resource Tags](#). If you are not sure if you should apply tags, skip this option (you can apply tags later) or ask your administrator.
5. Click **Create Bucket**.

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

Uploading Files to a Bucket

Object Storage supports individual files up to 50 GiB. You can use the Console to upload files 2 GiB or smaller. For larger files, use the SDK or API. See "Developer Tools" in the *Oracle Cloud Infrastructure User Guide*.

CHAPTER 12 Putting Data into Object Storage

To upload files to your bucket using the Console:

1. From the Object Storage Details screen, click the bucket name to view its details.
2. Click **Upload Objects**.
3. Select the object or objects to upload in one of two ways:
 - Drag files from your computer into the Drop files here ... section.
 - Click the **select files** link to display a file selection dialog box.

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

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

4. In the **Object name prefix field**, optionally specify a file name prefix for the file that you have selected to upload.
5. Click **Upload Objects**.

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

WHAT'S NEXT

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

CHAPTER 13 Getting Started with Audit

This chapter provides a hands-on tutorial to introduce you to the components of the Oracle Cloud Infrastructure Audit service.

The Oracle Cloud Infrastructure Audit service is included with your Oracle Cloud Infrastructure tenancy. The Audit service automatically records calls to the public application programming interface (API) endpoints for your Oracle Cloud Infrastructure tenancy. The service records events relating to the actions taken on the Oracle Cloud Infrastructure resources. Events recorded in the log can be viewed, retrieved, stored, and analyzed. These log events include information such as:

- ID of the caller
- target resource
- time of the recorded event
- request parameters
- response parameters

This task helps you get started with the Audit service by showing you how to find and view a specific event.

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

Prerequisite

To create an event to view, create and delete a VCN in the Networking service.

Create and Delete a VCN

1. Select the compartment (from the list on the left) in which you want to create the VCN.
2. Open the navigation menu. Under **Core Infrastructure**, go to **Networking** and click **Virtual Cloud Networks**.

3. Click **Create Virtual Cloud Network**.
4. Enter the following:
 - a. **Name:** Enter "Audit_Test".
 - b. Select **Create virtual cloud network only**.
 - c. **CIDR Block:** Enter "10.0.0.0/16".
 - d. Leave all other fields with their default settings. Click **Create Virtual Cloud Network**.

The VCN is displayed in the list.
5. Next to your VCN name, click the **OCID: Copy** link. You will use the OCID to help you find the event.
6. Terminate the VCN: Click the Actions icon (three dots), and then click **Terminate**. Confirm when prompted.

Using Audit to View Events

In this task, you will use Audit to find the delete VCN event.



Tip

Audit time stamps events according to Greenwich Mean Time (GMT). Before you get started, be aware of your local time zone offset.

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

The list of events that occurred in the current compartment is displayed. Audit logs are organized by compartment, so if you are looking for a particular event, you must know which compartment the event occurred in.
2. From the **Compartments** list, select the compartment in which you created the VCN.

The list of events for the compartment is displayed.

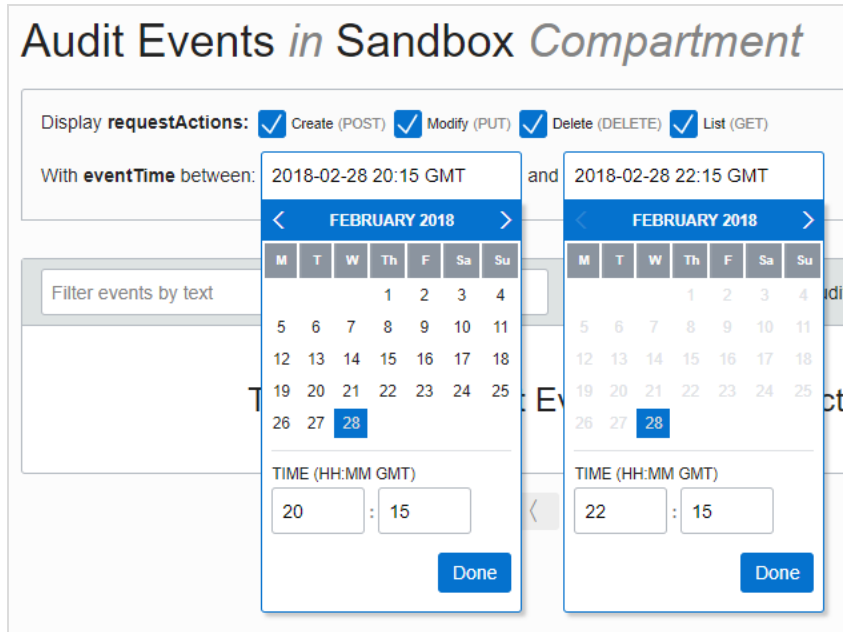
3. To find the delete VCN event, you can try the following filters:

Filter by time

- a. Click in the **Start Date** box to display the date and time editor.
- b. Select the current date from the calendar. Type or select values for hour and minute to approximate the preceding hour. Enter the time as Greenwich Mean Time (GMT) using 24-hour clock notation.
- c. Repeat the above steps to enter an end date for the current date and time, so that you filter results for the preceding hour.

Example

If you are located in the America/Los Angeles time zone and you are looking for an event that occurred between 1:15 PM and 2:15 PM local time on October 25, enter 21:15 and 22:15 to account for the GMT offset.



d. Click **Search**.

Filter events by keywords

You can further filter the results list to display only log entries that include a specific text string. Try the following entries to help you find the delete VCN event:



Tip

When you filter by keywords, use quotes to avoid results that have a similar string embedded in a longer string. For example, the quotes around the responseStatus "204" prevent matches of 204 embedded in a longer string somewhere else in the audit event.

- Filter by the responseStatus value
In the **Keywords** box, type "204" and click **Search** to display only events that returned the 204 (i.e., deleting resource) response status.
- Filter by requestResource value
In the **Keywords** box, paste the VCN OCID that you copied to your clipboard in the prerequisite step and click **Search**.
Review the events to find the DELETE event.

Filter events by request action types

- Filter by the request action types
In **Request Actions Types**, select "DELETE" and click **Search**.
The list filters to show only DELETE events. Scan the list to find your VCN termination event.
4. View the details of your event:
 - To see only the top-level details, click the down arrow to the right of an event.
 - To see lower-level details, click { . . . } to the right of the collapsed parameter.

CHAPTER 14 Getting Started with Oracle Platform Services

This chapter helps you get started with Oracle Platform Services on Oracle Cloud Infrastructure.



Note

Oracle Platform Services are not available in Oracle Cloud Infrastructure Government Cloud tenancies.

Supported Platform Services

The following platform services are supported on Oracle Cloud Infrastructure:

- Autonomous Analytics Cloud
- Autonomous API Platform Cloud Service
- Autonomous Data Warehouse Cloud
- Integration Cloud
- Autonomous Mobile Cloud Enterprise
- NoSQL Database Cloud
- Visual Builder
- Big Data Cloud
- Content and Experience Cloud
- Data Hub Cloud Service
- Data Integration Platform Cloud
- Database Cloud Service
- Developer Cloud Service

- Event Hub Cloud Service
- Java Cloud Service
- MySQL Cloud Service
- Oracle SOA Cloud Service

For services that are supported on both Oracle Cloud Infrastructure and Oracle Cloud Infrastructure Classic, you can choose Oracle Cloud Infrastructure during instance creation by selecting an appropriate region.

Understand the Infrastructure Prerequisites

Before creating instances of your service on Oracle Cloud Infrastructure, you must create certain resources in Oracle Cloud Infrastructure for use by your platform service instances.

See "Prerequisites for Oracle Platform Services on Oracle Cloud Infrastructure" in the *Oracle Cloud Infrastructure User Guide*.

Learn About Service-Specific Differences and Workflows

Broadly, the service features are the same regardless of the infrastructure you choose (Oracle Cloud Infrastructure or Oracle Cloud Infrastructure Classic), but differences may exist in some services. And the workflows for creating instances on Oracle Cloud Infrastructure may vary across services.

See the following documentation:

Service	More Information
Big Data Cloud	About Big Data Cloud Clusters in Oracle Cloud Infrastructure
Data Hub Cloud Service	About Oracle Data Hub Cloud Service Clusters in Oracle Cloud Infrastructure
Database Cloud Service	About Database Deployments in Oracle Cloud Infrastructure

CHAPTER 14 Getting Started with Oracle Platform Services

Service	More Information
Event Hub Cloud Service	About Oracle Event Hub Cloud Service - Dedicated Instances in Oracle Cloud Infrastructure
Java Cloud Service	About Java Cloud Service Instances in Oracle Cloud Infrastructure
MySQL Cloud Service	About MySQL Cloud Service Deployments in Oracle Cloud Infrastructure
Oracle SOA Cloud Service	About SOA Cloud Service Instances in Oracle Cloud Infrastructure Classic and Oracle Cloud Infrastructure

CHAPTER 15 Getting Started with Oracle Applications

This chapter helps you get started with Oracle Applications on Oracle Cloud Infrastructure.

Support for Oracle Applications

Oracle Cloud Infrastructure is an ideal place to host your Oracle Applications. You can deploy and manage Oracle applications on Oracle Cloud Infrastructure using the standard procedures found in the application product documentation, or using Oracle-provided automation solutions (available for some applications).

Oracle applications that meet the following criteria are supported:

- The application version is under Premier, Extended, or Sustained support.
- You plan to run the application on an operating system and database version that is supported on Oracle Cloud Infrastructure and certified for the application.

Oracle offers solutions and documentation to make deploying applications on Oracle Cloud Infrastructure easier. Solutions are available for the following applications:

- Oracle E-Business Suite
- Oracle JD Edwards EnterpriseOne
- Oracle PeopleSoft

The following Oracle Learning Library page describes the currently available solutions:

[Oracle Applications on Oracle Cloud Infrastructure](#)

CHAPTER 16 Setting Up Your Tenancy

After Oracle creates your tenancy in Oracle Cloud Infrastructure, an administrator at your company will need to perform some set up tasks and establish an organization plan for your cloud resources and users. Use the information in this topic to help you get started.



Tip

To quickly get some users up and running while you are still in the planning phase, see [About Users, Groups, and Policies](#).

Create a Plan

Before adding users and resources you should create a plan for your tenancy. Fundamental to creating your plan is understanding the components of the Oracle Cloud Infrastructure Identity and Access Management (IAM). Ensure that you read and understand the features of IAM. See "Overview of the IAM" in the *Oracle Cloud Infrastructure User Guide*.

Your plan should include the compartment hierarchy for organizing your resources and the definitions of the user groups that will need access to the resources. These two things will impact how you write policies to manage access and so should be considered together.

Use the following primer topics to help you get started with your plan:

- [Understanding Compartments](#)
- [Consider Who Should Have Access to Which Resources](#)

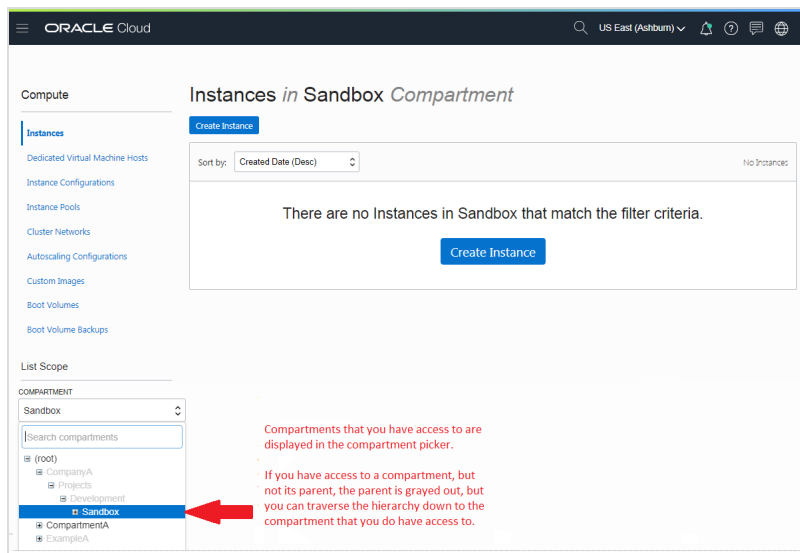
Understanding Compartments

Compartments are the primary building blocks you use to organize your cloud resources. You use compartments to organize and isolate your resources to make it easier to manage and secure access to them.

CHAPTER 16 Setting Up Your Tenancy

When your tenancy is provisioned, a root compartment is created for you. Your root compartment holds *all* of your cloud resources. You can think of the root compartment like a root folder in a file system.

The first time you sign in to the Console and select a service, you will see your one, root compartment.



You can create compartments under your root compartment to organize your cloud resources in a way that aligns with your resource management goals. As you create compartments, you control access to them by creating policies that specify what actions groups of users can take on the resources in those compartments.

Keep in mind the following when you start working with compartments:

- At the time you create a resource (for example, instance, block storage volume, VCN, subnet), you must decide in which compartment to put it.
- Compartments are logical, not physical, so related resource components can be placed in different compartments. For example, your cloud network subnets with access to an internet gateway can be secured in a separate compartment from other subnets in the same cloud network.

- You can create a hierarchy of compartments up to six compartments deep under the tenancy (root compartment).
- When you write a policy rule to grant a group of users access to a resource, you always specify the compartment to apply the access rule to. So if you choose to distribute resources across compartments, remember that you will need to provide the appropriate permissions for each compartment for users that will need access to those resources.
- In the Console, compartments behave like a filter for viewing resources. When you select a compartment, you only see resources that are in the compartment selected. To view resources in another compartment, you must first select that compartment. You can use the Search feature to get a list of resources across multiple compartments. See [Overview of Search](#).
- You can use the compartment explorer to get a complete view of all the resources (across regions) that reside in a specific compartment. See [Viewing All Resources in a Compartment](#).
- If you want to delete a compartment, you must delete all resources in the compartment first.
- Finally, when planning for compartments you should consider how you want usage and auditing data aggregated.

Consider Who Should Have Access to Which Resources

Another primary consideration when planning the setup of your tenancy is who should have access to which resources. Defining how different groups of users will need to access the resources will help you plan how to organize your resources most efficiently, making it easier to write and maintain your access policies.

For example, you might have users who need to:

- View the Console, but not be allowed to edit or create resources
- Create and update specific resources across several compartments (for example, network administrators who need to manage your cloud networks and subnets)

- Launch and manage instances and block volumes, but not have access to your cloud network
- Have full permissions on all resources, but only in a specific compartment
- Manage other users' permissions and credentials

To see some sample policies, see "Common Policies" in the *Oracle Cloud Infrastructure User Guide*.

Sample Approaches to Setting Up Compartments

Put all your resources in the tenancy (root compartment)

If your organization is small, or if you are still in the proof-of-concept stage of evaluating Oracle Cloud Infrastructure, you might consider placing all of your resources in the root compartment (tenancy). This approach makes it easy for you to quickly view and manage all your resources. You can still write policies and create groups to restrict permissions on specific resources to only the users who need access.

High-level tasks to set up the single compartment approach:

1. (Best practice) Create a sandbox compartment. Even though your plan is to maintain your resources in the root compartment, Oracle recommends setting up a sandbox compartment so that you can give users a dedicated space to try out features. In the sandbox compartment you can grant users permissions to create and manage resources, while maintaining stricter permissions on the resources in your tenancy (root) compartment. See [Create a Sandbox Compartment](#).
2. Create groups and policies. See "Common Policies" in the *Oracle Cloud Infrastructure User Guide*.
3. Add users. See "Managing Users" in the *Oracle Cloud Infrastructure User Guide*.

Create compartments to align with your company projects

Consider this approach if your company has multiple departments that you want to manage separately or if your company has several distinct projects that would be easier to manage separately.

In this approach, you can add a dedicated administrators group for each compartment (project) who can set the access policies for just that project. (Users and groups still must be added at the tenancy level.) You can give one group control over all their resources, while not allowing them administrator rights to the root compartment or any other projects. In this way, you can enable different groups at your company to set up their own "sub-clouds" for their own resources and administer them independently.

High-level tasks to set up the multiple project approach:

1. Create a sandbox compartment. Oracle recommends setting up a sandbox compartment so you can give users a dedicated space to try out features. In the sandbox compartment you can grant users permissions to create and manage resources, while maintaining stricter permissions on the resources in your tenancy (root) compartment.
2. Create a compartment for each project, for example, ProjectA, ProjectB.
3. Create an administrators group for each project, for example, ProjectA_Admins.
4. Create a policy for each administrators group.

Example:

```
Allow group ProjectA_Admins to manage all-resources in compartment ProjectA)
```

5. Add users. See "Managing Users" in the *Oracle Cloud Infrastructure User Guide*.
6. Let the administrators for ProjectA and ProjectB create subcompartments within their designated compartment to manage resources.
7. Let the administrators for ProjectA and ProjectB create the policies to manage the access to their compartments.

CHAPTER 17 Contacting Support

This chapter explains how to contact support about issues with Oracle Cloud Infrastructure.

Getting Help and Contacting Support

When using Oracle Cloud Infrastructure, there are times when you need to obtain help from the community, or to talk to someone in Oracle support. This topic helps you to understand these options.

1. Use a search engine

If it is a common issue, someone else has likely asked this question in the past. You can use scoped search to look for answers in our documentation and our forum platforms – Cloud Customer Connect and Stack Overflow. To perform a scoped search, go to your favorite search engine and specify the site URLs along with your specific search terms, as follows:

```
<Your Search Terms> (site:docs.cloud.oracle.com/iaas OR site:cloudcustomerconnect.oracle.com OR site:stackoverflow.com)
```

2. Post a question to our forums

If you can't find an answer to your question through search, submit a new question to one of the forums we support. This option is available to all customers.

Cloud Customer Connect

For any issue related to Oracle Cloud Infrastructure, including provisioning of new resources, console issues, identity, networking, documentation, storage, database, Edge services or other solutions, you can post a new question to our Cloud Customer Connect at:

<https://cloudcustomerconnect.oracle.com/resources/9c8fa8f96f/summary>

Stack Overflow

If you are creating an application that integrates with Oracle Cloud Infrastructure APIs, endpoints, or services, you can also use Stack Overflow forums for development-related questions. Tag your questions with [oracle-cloud-infrastructure](https://stackoverflow.com/questions/tagged/oracle-cloud-infrastructure), as follows:

<https://stackoverflow.com/questions/tagged/oracle-cloud-infrastructure>

3. Open a support service request



Note

This option is available to paid accounts. Customers using only Always Free resources are not eligible for Oracle Support. Limited support is available to Free Tier accounts with Free Trial credits. After you use all of your credits or after your trial period ends (whichever comes first), you must upgrade to a paid account to access Oracle Support. If you choose not to upgrade and continue to use Always Free Services, you will not be eligible to raise a service request in My Oracle Support.

If the preceding options did not resolve your issue and you need to talk to someone, you can go to [My Oracle Support](#) and create a service request.

In addition to support for technical issues, use [My Oracle Support](#) if you need to:

- Reset the password or unlock the account for the tenancy administrator
- Add or change a tenancy administrator
- Request a [service limit](#) increase



Important

Before you can create a service request for Oracle Cloud Infrastructure, you must have an `oracle.com` account and you must register your Oracle Cloud Infrastructure CSI with [My Oracle Support](#). See [Using My Oracle Support for the First Time](#) for details.

Creating a Service Request

To create a service request:

1. Go to [My Oracle Support](#) and sign in.
If you are not signed in to Oracle Cloud Support, click **Switch to Cloud Support** at the top of the page.
2. Click **Create Service Request**.
3. Select the following from the displayed menus:
 - **Service Type:** Select **Oracle Cloud Infrastructure** from the list.
 - **Service Name:** Select the appropriate option for your organization.
 - **Problem Type:** Select your problem type from the list.
4. Enter your contact information.
5. Enter a **Description**, and then enter the required fields specific to your issue. For most Oracle Cloud Infrastructure issues you need to include the OCID (Oracle Cloud Identifier) for each resource you need help with. See [Locating Oracle Cloud Infrastructure IDs](#) for instructions on locating these.

For help with any of the general fields in the service request or for information on managing your service requests, click **Help** at the top of the Oracle Cloud Support page.

Locating Oracle Cloud Infrastructure IDs

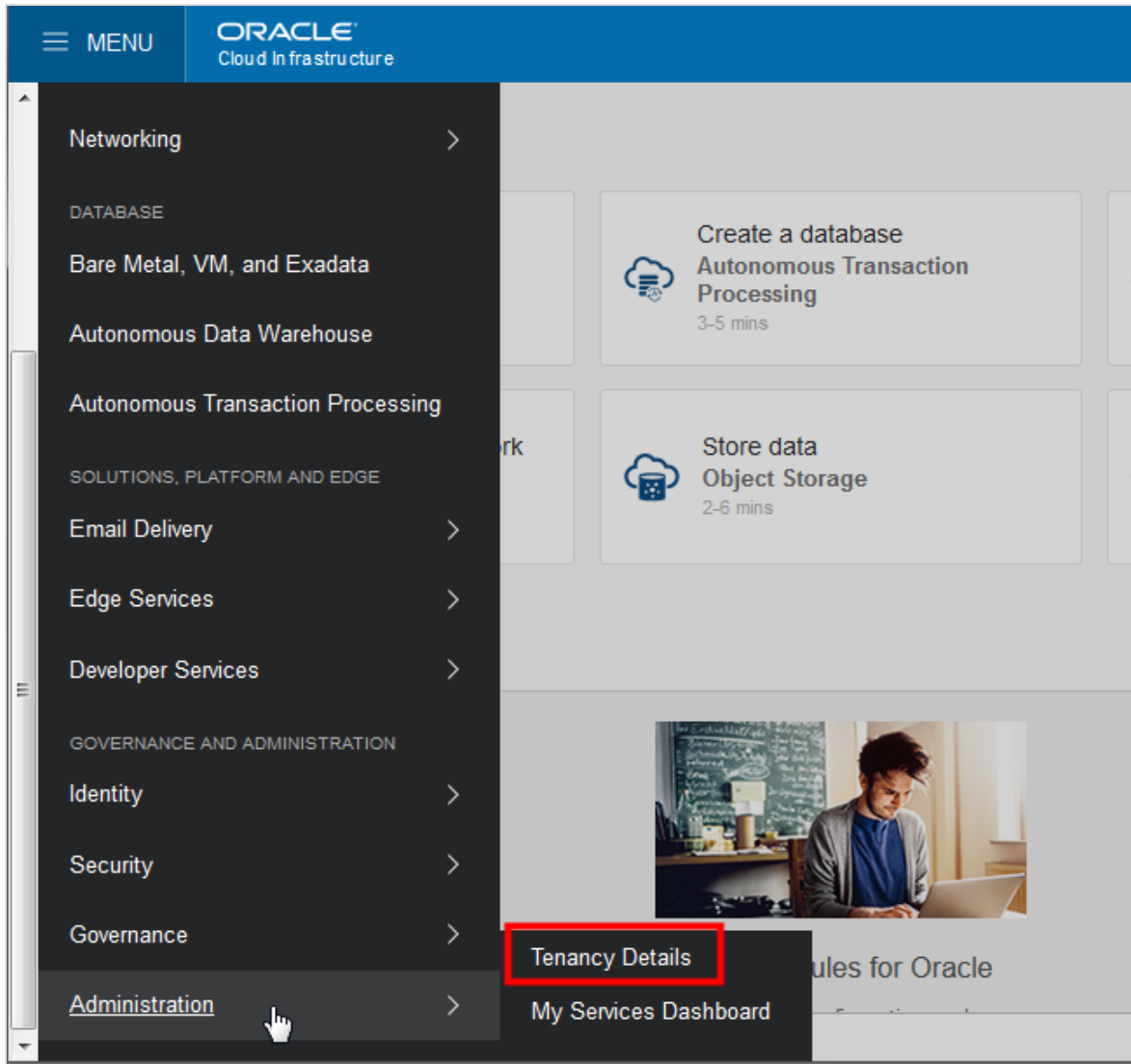
Use the following tips to help you locate identifiers you might be asked to provide.

Finding Your Customer Support Identifier (CSI)

The Customer Support Identifier (CSI) number is generated after you purchase Oracle Cloud services. This number can be found in several places, including in your contract document and also on your tenancy details page. You'll need the CSI number to register and log support requests in My Oracle Support (MOS).

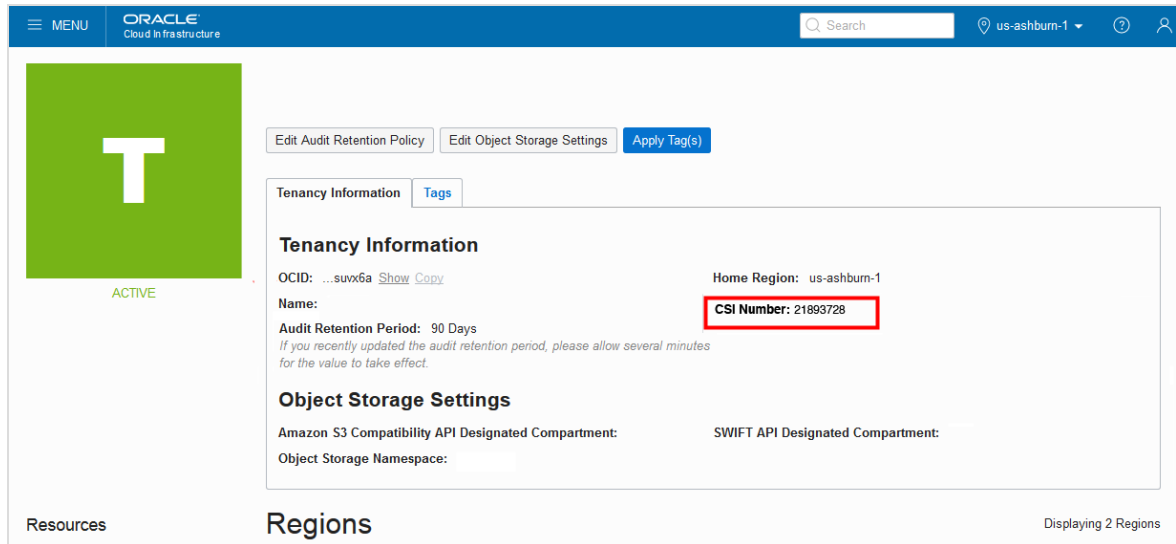
To find your CSI number:

1. Open the navigation menu, under Governance and Administration, go to **Administration** and click **Tenancy Details**.



2. The CSI number is shown under **Tenancy Information**.

CHAPTER 17 Contacting Support



The screenshot displays the Oracle Cloud Infrastructure console interface. At the top, there is a blue header with the Oracle logo and 'Cloud Infrastructure' text. A search bar and user profile are also visible. The main content area features a green square with a white 'T' representing the tenancy, with the word 'ACTIVE' below it. To the right of the tenancy icon are buttons for 'Edit Audit Retention Policy', 'Edit Object Storage Settings', and 'Apply Tag(s)'. Below these is a 'Tenancy Information' section with a 'Tags' tab. The 'Tenancy Information' section includes the following details:

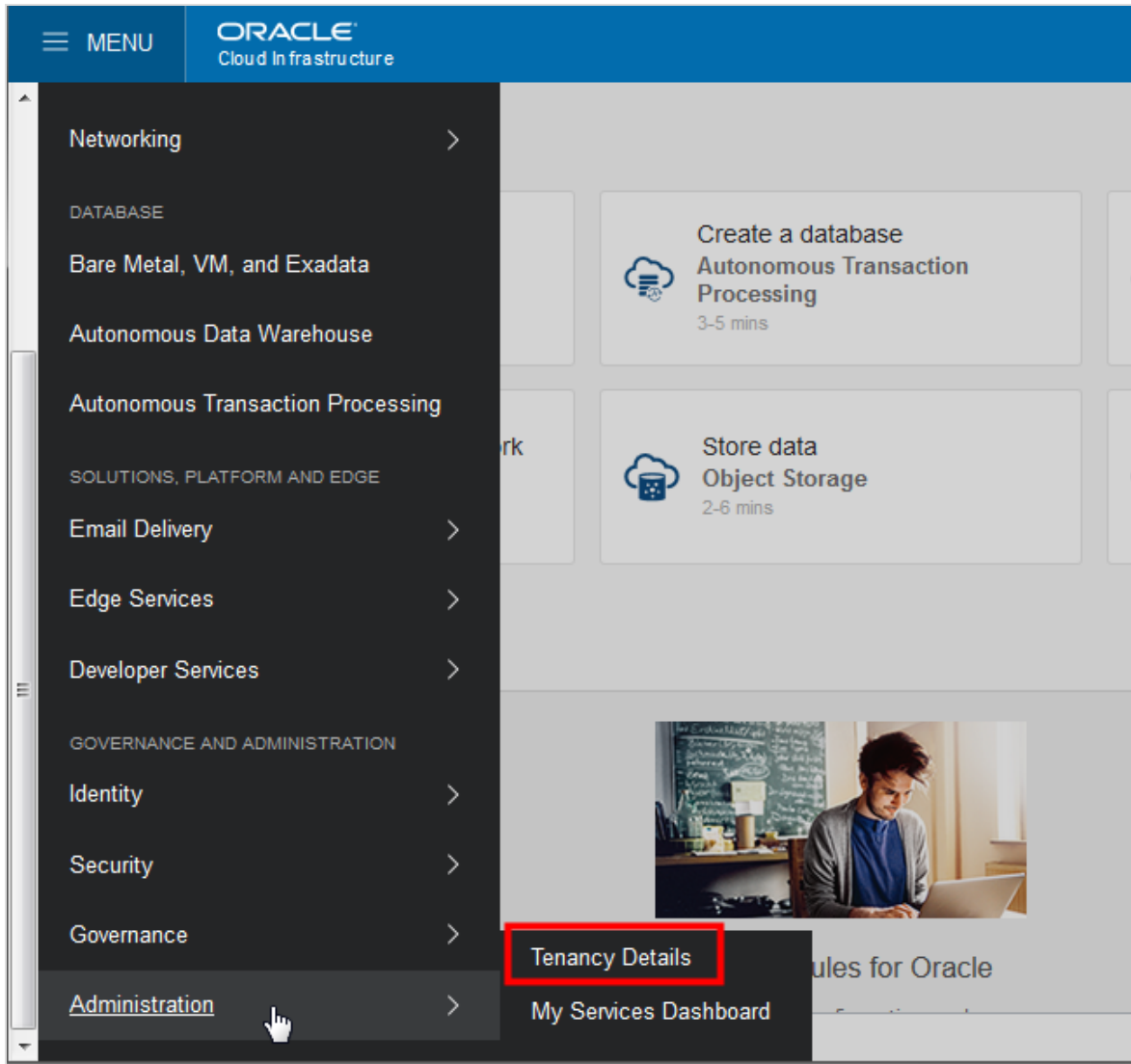
- OCID: ...suvx6a [Show Copy](#)
- Home Region: us-ashburn-1
- Name: **CSI Number: 21893728** (highlighted with a red box)
- Audit Retention Period: 90 Days
If you recently updated the audit retention period, please allow several minutes for the value to take effect.

Below the tenancy information is the 'Object Storage Settings' section, which includes fields for 'Amazon S3 Compatibility API Designated Compartment', 'SWIFT API Designated Compartment', and 'Object Storage Namespace'. At the bottom of the console, there are 'Resources' and 'Regions' sections, with a note that '2 Regions' are displayed.

Finding Your Tenancy OCID (Oracle Cloud Identifier)

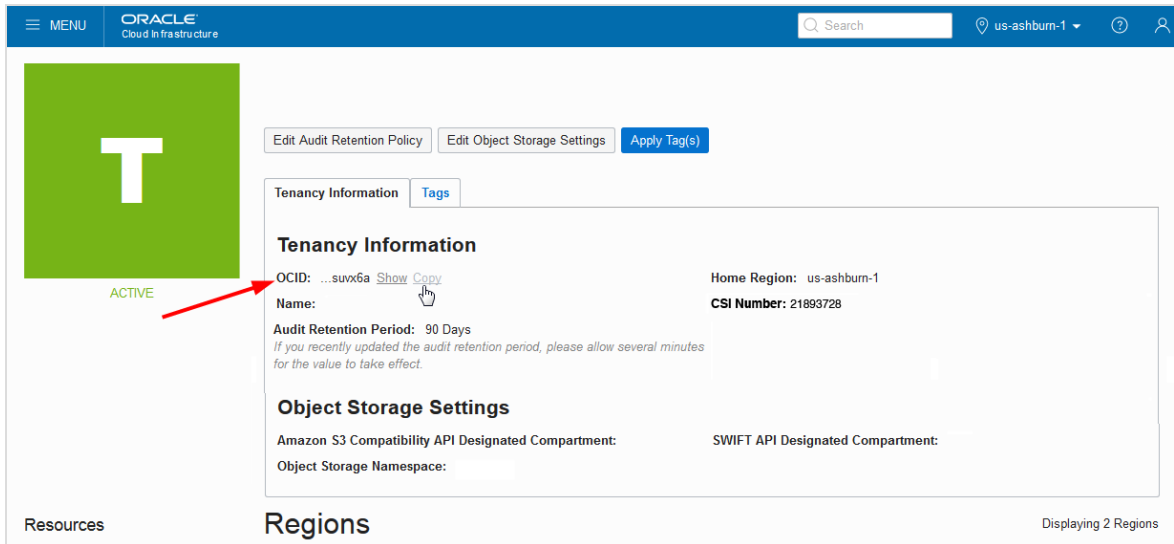
Get the tenancy OCID from the Oracle Cloud Infrastructure Console on the **Tenancy Details** page:

1. Open the navigation menu, under Governance and Administration, go to **Administration** and click **Tenancy Details**.



2. The tenancy OCID is shown under **Tenancy Information**. Click **Copy** to copy it to your clipboard.

CHAPTER 17 Contacting Support



Finding the OCID of a Compartment

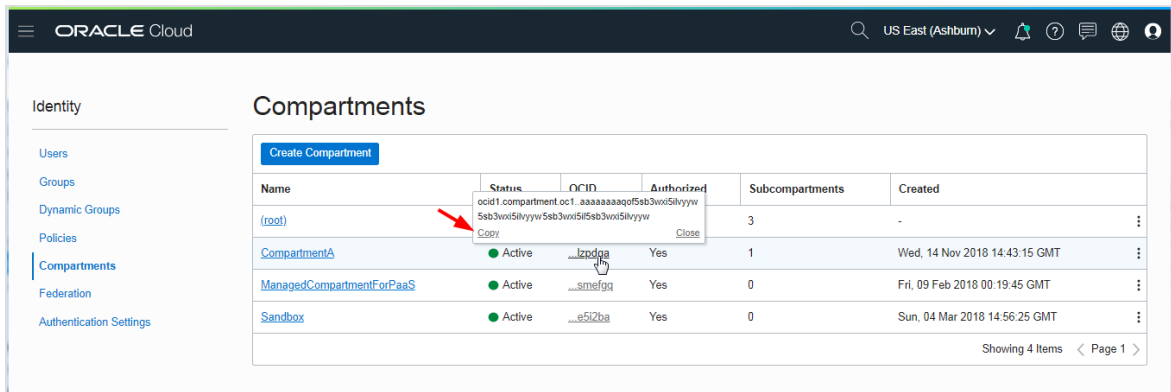
To find the OCID (Oracle Cloud Identifier) of a compartment:

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

A list of the compartments in your tenancy is displayed.

CHAPTER 17 Contacting Support

A shortened version of the OCID is displayed next to each compartment.



2. Click the shortened OCID string to view the entire value in a pop-up. Click **Copy** to copy the OCID to your clipboard. You can then paste it into the service request form field.

Finding the OCID of a Resource

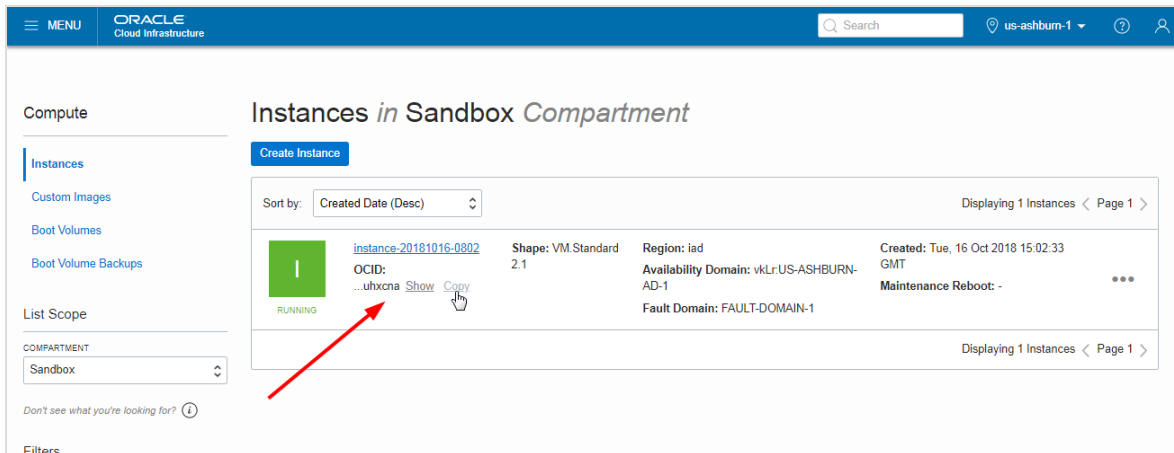
The OCID (Oracle Cloud Identifier) of a resource is displayed when you view the resource in the Console, both in the list view and on the details page.

For example, to get the OCID for a compute instance:

1. Open the Console.
2. Select the Compartment to which the instance belongs from the list on the left side of the page.
Note that you must have appropriate permissions in a compartment to view resources.
3. Open the navigation menu. Under **Core Infrastructure**, go to **Compute** and click **Instances**. A list of instances in the selected compartment is displayed.

CHAPTER 17 Contacting Support

A shortened version of the OCID is displayed next to each instance.



4. Click **Copy** to copy the OCID to your clipboard. You can then paste it into the service request form field.

Finding Your `opc-request-id` in the Console

To locate the `opc-request-id` value when you are using the Oracle Cloud Infrastructure Console, you must first access the developer tools in the browser in which you are running the Console. Depending on your browser, this is called either Developer Tools or Web Console and can be opened by clicking **F12**. In Safari on a Mac, it's called the Web Inspector.

1. Open your browser's developer tools by clicking **F12** (in Safari on Mac, click **Option + Cmd + i**).
2. Select the **Network** tab, then filter on **XHR**.



Note

Different browsers present filtering options in different ways. Firefox present an **XHR** filtering button on the **Network** tab UI. Internet Explorer and Edge provide a filter icon with the label **Content type**, which you click to expose an **XHR** filter.

3. Select results that return a 500 error to view the request details.
4. In the request details pane, click the **Headers** tab.
5. Locate and copy both the `opc-request-id` and `date` values and include them in your support ticket.

Using My Oracle Support for the First Time

Before you can create service requests with My Oracle Support, you need to have an Oracle Single Sign On (SSO) account and you need to register your Customer Support Identifier (CSI) with My Oracle Support.



Tip

Before you begin this procedure, have your CSI number available (see [Finding Your Customer Support Identifier \(CSI\)](#)).

To request an SSO account and register with My Oracle Support

1. Go to <https://support.oracle.com>.

2. Click **New user? Register here** to create your Oracle Single Sign On (SSO) account.
3. Enter your company e-mail address in the **Email address** field, complete the rest of the form, and then click **Create Account**. A verification email is generated.
4. Check your email account for an email from Oracle asking your to verify your email address.
5. Open the email and click Verify Email Address.
6. Sign in with the credentials you just set up.
7. At sign in, you are prompted to enter a **Note to the Approver** and the **Support Identifier** (your CSI).
8. Click **Request Access**.
9. Enter the first five characters of the name of the organization that owns the Customer Support Identifier (listed in the Welcome letter), and then click **Validate**. The support identifier appears in the table.
10. Click **Next**.
11. Enter your contact information and click **Next**.
12. Accept the terms and click **Next**.

The status of the request is pending until you receive approval from the Customer User Administrator (CUA) or from Oracle Support if you are the first person requesting this support identifier.

If you have previously registered, but need to add the CSI for Oracle Cloud Infrastructure

1. Go to <https://support.oracle.com> and sign in.
2. Navigate to the **My Account** page: Go to your user name at the of the page, open the menu, and then click **My Account**.
3. The **Support Identifiers** region displays the accounts that your user name is currently associated with.

4. Click **Request Access**.
5. Enter a **Note to the Approver** and then enter the **Support Identifier** (your CSI).
6. Enter the first five characters of the name of the organization that owns the Customer Support Identifier (listed in the Welcome letter), and then click **Validate**. The support identifier appears in the table.
7. Click **Next**.
8. Enter your contact information and accept the terms. Click **Next**.

The status of the request is pending until you receive approval from the Customer User Administrator (CUA).

For more information about signing in and using My Oracle Support, see [Registration, Sign In, and Accessibility Options](#) in *My Oracle Support Help*.

CHAPTER 18 Frequently Asked Questions

I'm not seeing Platform Services or Classic Services on my navigation menu. What happened?

Make sure that you are signing in with your Oracle Identity Cloud Service login credentials. To ensure that you sign in through IDCS:

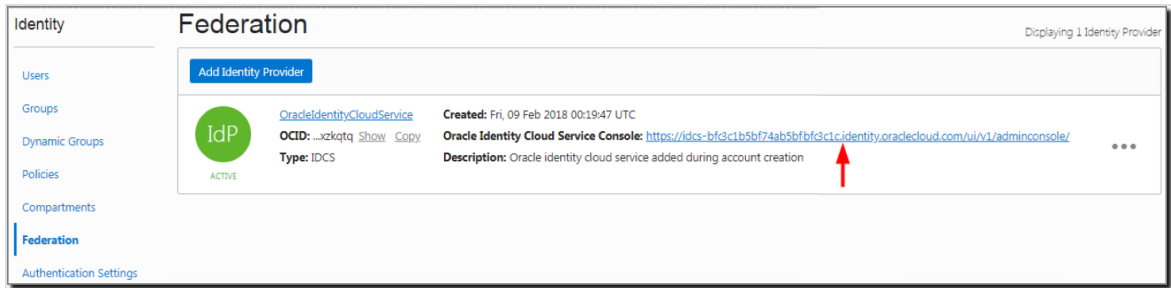
1. Start at: <https://cloud.oracle.com/sign-in>.
2. Enter your tenancy name and click **Next**. The IDCS sign in page is displayed.
3. Enter your username and password and click **Sign In**.
4. On the Console, open the navigation menu. If your account has access to Platform or Classic services, you'll see them displayed on the menu under **More Oracle Cloud Services**. See also [Navigating to More Oracle Cloud Services from the Console](#).

How do I get to my IDCS console?

To access the IDCS console:

1. Open the navigation menu. Under **Governance and Administration**, go to **Identity** and click **Federation**.
The list of identity providers is displayed. OracleIdentityCloudService is displayed in the list of identity providers, with details about the federation.
2. Click the link for **Oracle Identity Cloud Service Console**. An example is shown in the following screenshot.

CHAPTER 18 Frequently Asked Questions



The Oracle Identity Cloud service console opens in a new window.

My team needs reports that were only available from My Services. How can I get back to the old dashboard?

You can access the My Services dashboard by using this URL:

```
http://myservices-<tenancyname>.console.oraclecloud.com/mycloud/cloudportal/dashboard
```

where you replace *<tenancyname>* with your company's tenancy name.

Where can I find more information about the changes to other task workflows and navigation?

See [What's New in the Console](#).

What URLs can I use to sign in to the Oracle Cloud Infrastructure Console?

You can use any of the regional Console URLs to sign in. These are:

- <https://console.ap-mumbai-1.oraclecloud.com>
- <https://console.ap-seoul-1.oraclecloud.com>
- <https://console.ap-sydney-1.oraclecloud.com>
- <https://console.ap-tokyo-1.oraclecloud.com>

CHAPTER 18 Frequently Asked Questions

- <https://console.ca-toronto-1.oraclecloud.com>
- <https://console.eu-frankfurt-1.oraclecloud.com>
- <https://console.eu-zurich-1.oraclecloud.com>
- <https://console.sa-saopaulo-1.oraclecloud.com>
- <https://console.uk-london-1.oraclecloud.com>
- <https://console.us-ashburn-1.oraclecloud.com>
- <https://console.us-phoenix-1.oraclecloud.com>

On the sign-in page, you are prompted to enter your cloud tenant, your user name, and your password. Once authenticated, you are directed to a region your tenancy is subscribed to. You can [switch to other regions](#) you are subscribed to by using the region selector at the top of the Console.

How do I find my tenancy home region?

To find out what your home region is:

Open the **Profile** menu () and click **Tenancy: <your_tenancy_name>**.

The Tenancy details page shows your Home Region.

What are my Oracle Cloud Infrastructure account service limits (or resource quotas) and can I request more?

You can view your tenancy's service limits in the Console and request an increase. For more information and the default tenancy limits, see [Service Limits](#).

Where do I find information about what APIs are available?

Oracle Cloud Infrastructure provides a set of APIs for the core services (network, compute, block volumes) as well as for the IAM and the Object Storage services.

See "API Requests" in the *Oracle Cloud Infrastructure User Guide*.

What browsers can I use with the Console?

Oracle Cloud Infrastructure supports the latest desktop versions of Google Chrome, Microsoft Edge, Internet Explorer 11, Safari, Firefox, and Firefox ESR. Note that private browsing mode is not supported for Firefox, Internet Explorer, or Edge. Mobile browsers are not supported.

Why can't I sign in using Firefox?

If you are having trouble signing in to the Console using the Firefox browser, it might be due to one of the following conditions:

- You are in Private Browsing mode. The Console does not support Private Browsing mode. Open a new session of Firefox with Private Browsing turned off.

How do I know if I am in Private Browsing mode?

When you are in Private Browsing mode, a mask icon is displayed in the upper right corner of your Firefox window.

- You are not on the latest version of Firefox. Upgrade to the latest version. To check to see if you are on the latest version, follow these instructions:
<https://support.mozilla.org/en-US/kb/find-what-version-firefox-you-are-using>
When checking the version, note whether you are using Firefox or Firefox ESR.
- Your Firefox user profile is corrupted. To fix this issue:
 1. Upgrade to the latest version of Firefox.
 2. Create a new user profile and open Firefox with the new profile. See Mozilla Support for instructions on how to create a new user profile:
<https://support.mozilla.org/en-US/kb/profile-manager-create-and-remove-firefox-profiles>

If none of the above resolves your issue, contact [Oracle Support](#). In your problem description, make sure you specify whether you are using Firefox or Firefox ESR.


How do I change my password?

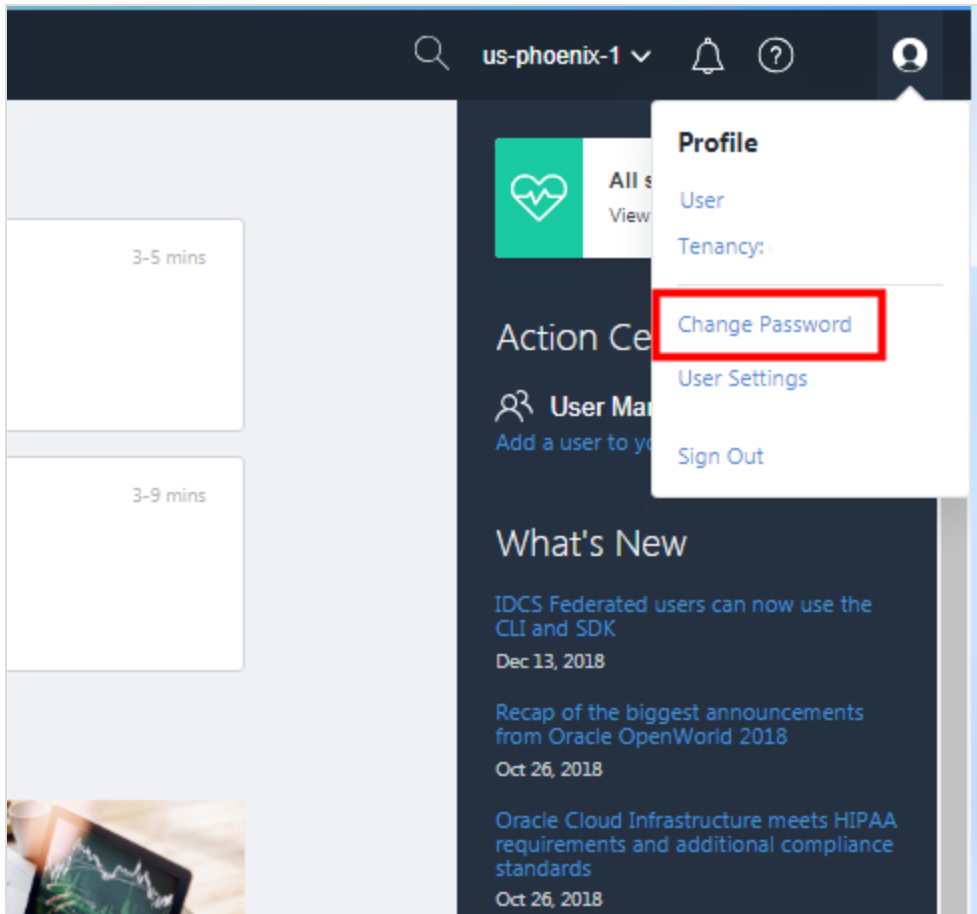


Note

For Federated Users

If your company uses an identity provider (other than Oracle Identity Cloud Service) to manage user logins and passwords, you can't use the Console to update your password. You do that with your identity provider.

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



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

How do I reset my password if I forget it?

If you added an email address to your user settings, you can use the **Forgot Password** link on the sign-in page to have a temporary password sent to you. If you don't have an email address included with your user details, then an administrator must reset your password.

CHAPTER 18 Frequently Asked Questions

Contact your administrator to reset your password for you. Your administrator will give you a temporary password that is good for 7 days. If you do not use it in 7 days, the password will expire and you'll need to get your administrator to create a new one-time password for you.

If you are the default or tenant administrator for your site and you forgot your password, contact [Oracle Support](#). For tips on filing a service request, see [Getting Help and Contacting Support](#).

How do I get support?

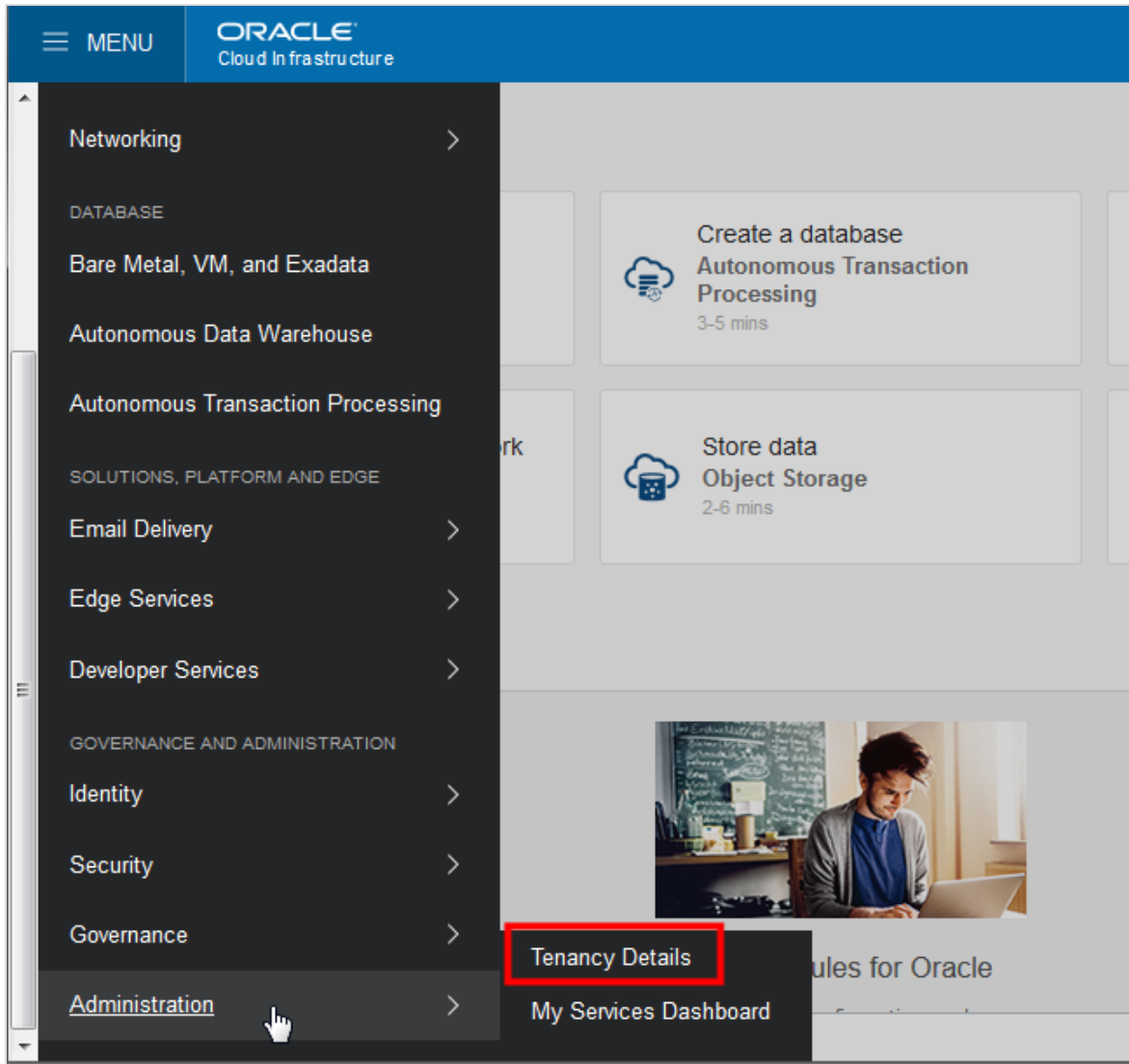
Go to [My Oracle Support](#). For tips on filing a service request, see [Getting Help and Contacting Support](#).

Where do I find my Tenancy OCID?

Get the tenancy OCID from the Oracle Cloud Infrastructure Console on the **Tenancy Details** page:

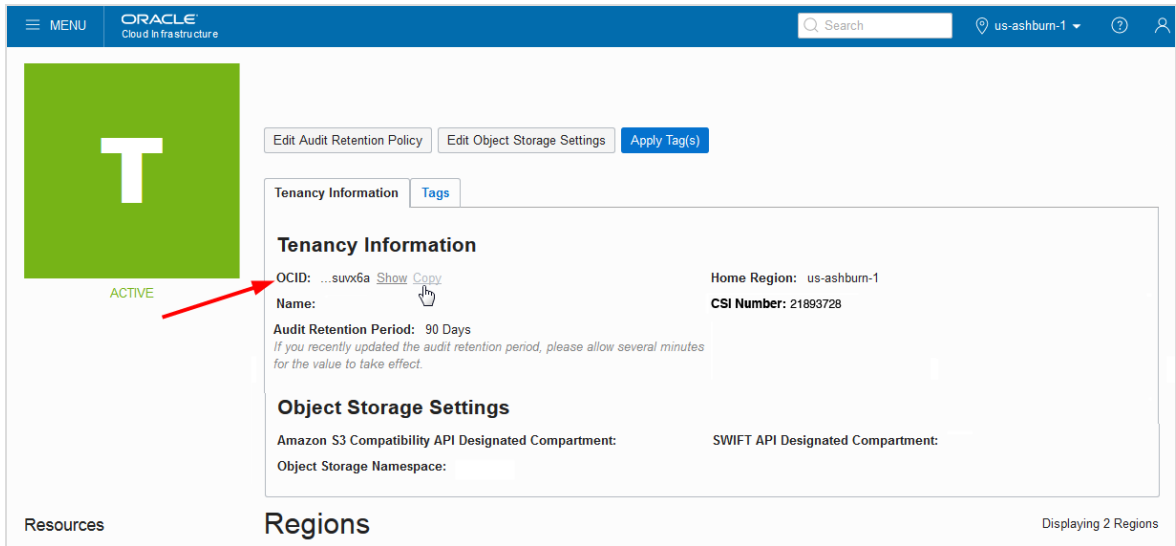
1. Open the navigation menu, under Governance and Administration, go to **Administration** and click **Tenancy Details**.

CHAPTER 18 Frequently Asked Questions



2. The tenancy OCID is shown under **Tenancy Information**. Click **Copy** to copy it to your clipboard.

CHAPTER 18 Frequently Asked Questions



The screenshot displays the Oracle Cloud Infrastructure console interface. At the top, there is a blue header with the Oracle logo and 'Cloud Infrastructure' text. A search bar and a location dropdown set to 'us-ashburn-1' are also visible. The main content area features a large green square with a white 'T' representing the tenancy, with the word 'ACTIVE' below it. To the right of this icon are three buttons: 'Edit Audit Retention Policy', 'Edit Object Storage Settings', and 'Apply Tag(s)'. Below these buttons are two tabs: 'Tenancy Information' (selected) and 'Tags'. The 'Tenancy Information' section contains the following details:

- Tenancy Information**
- OCID: ...suvx6a [Show](#) [Copy](#)
- Name:
- Audit Retention Period: 90 Days
If you recently updated the audit retention period, please allow several minutes for the value to take effect.
- Home Region: us-ashburn-1
- CSI Number: 21893728

Below the tenancy information is the 'Object Storage Settings' section, which includes fields for 'Amazon S3 Compatibility API Designated Compartment', 'Object Storage Namespace', and 'SWIFT API Designated Compartment'. At the bottom of the page, there are sections for 'Resources' and 'Regions', with a note that says 'Displaying 2 Regions'.

GLOSSARY

A

AD-specific subnet

A subnet that is specific to a particular availability domain (AD). Historically all subnets were AD-specific. Compare with regional subnets, which Oracle recommends over AD-specific subnets.

alarm

The trigger rule and query to evaluate and related configuration, such as notification details to use when the trigger is breached. Alarms passively monitor your cloud resources using metrics in Monitoring.

API key

A credential for securing requests to the Oracle Cloud Infrastructure REST API.

attach

Link a volume and instance together. Allows an instance to connect and mount the volume as a hard drive.

auth token

Oracle Cloud Infrastructure-generated token you use to authenticate with third-party APIs, such as a Swift client.

availability domain

One or more isolated, fault-tolerant Oracle data centers that host cloud resources such as instances, volumes, and subnets. A region contains one or more availability domains.

B

backend set

A logical entity defined by a list of backend servers, a load balancing policy, and a health check policy.

bare metal IaaS

A cloud infrastructure that allows you to utilize hosted physical hardware, as opposed to traditional software-based virtual machines, ensuring a high level of security and performance.

block storage volume

A virtual disk that provides persistent storage space for instances in the cloud.

bucket

A logical container for storing objects.

C

CHAP

Stands for Challenge-Handshake-Authentication-Protocol. It is a security protocol used by iSCSI for authentication between a volume and an instance.

Cloud Block Storage

A service that allows you to add block storage volumes to an instance in order to expand the available storage on that resource.

cloud network

A virtual version of a traditional network—including CIDRs, subnets, route tables, and gateways—on which your instance runs.

cluster network

A pool of high performance computing (HPC) instances that are connected with a high-bandwidth, ultra low-latency network.

compartment

A collection of related resources that can be accessed only by certain groups that have been given permission by an administrator in your organization.

Compute

A service that lets you provision and manage compute hosts, known as instances.

connect

Make an attached volume usable by an instance's guest OS.

CPE

The router at the edge of your on-premises network. The Networking service also has an object called a CPE, which is a virtual representation of your edge router. You create that object when setting up VPN Connect (an IPSec VPN) between Oracle and your on-premises network.

cross-connect

Used with Oracle Cloud Infrastructure FastConnect, specifically if you're using a third-party provider or colocated with Oracle in a FastConnect location. A cross-connect is the physical cable connecting your existing network to Oracle in the FastConnect location.

cross-connect group

Used with Oracle Cloud Infrastructure FastConnect, specifically if you're using a third-party provider or colocated with Oracle in a FastConnect location. A cross-connect group is a link aggregation group (LAG) that contains at least one cross-connect.

customer-premises equipment

The router at the edge of your on-premises network. The Networking service also has an object called a CPE, which is a virtual representation of your edge router. You create that object when setting up VPN Connect (an IPSec VPN) between Oracle and your on-premises network.

D

data point

(Monitoring service) A timestamp-value pair for the specified metric. Example: 2018-05-10T22:19:00Z, 10.4

DB System

A dedicated bare metal instance running Oracle Linux, optimized for running one or more Oracle databases. A DB System is a Database Service resource.

DHCP options

Configuration information that is automatically provided to the instances when they boot up.

dimension

(Monitoring service) A qualifier provided in a metric definition. Example: Resource identifier (resourceId), provided in the definitions of oci_computeagent metrics.

display name

A friendly name or description that helps you easily identify the resource.

DRG

An optional virtual router that you can add to your VCN to provide a path for private network traffic between your VCN and on-premises network.

DRG attachment

When you attach a dynamic routing gateway (DRG) to a virtual cloud network (VCN), the result is a DRG attachment object. To detach the DRG, you delete that attachment object.

dynamic group

A special type of IAM group that contains instances that match rules that you define (thus the membership can change dynamically as matching instances are terminated or launched). These instances act as "principal" actors and can make API calls to Oracle Cloud Infrastructure services according to IAM policies that you write for the dynamic group.

dynamic routing gateway

An optional virtual router that you can add to your VCN to provide a path for private network traffic between your VCN and on-premises network.

E

ephemeral public IP

A public IP address (and related properties) that is temporary and exists for the life of the instance it's assigned to. It can be assigned only to the primary private IP on a VNIC. Compare with reserved public IP.

Export

Controls how file systems are accessed by NFS clients when they connect to a mount target.

Export Options

A set of parameters that specify the level of access granted to NFS clients when they connect to a mount target.

F

FastConnect

FastConnect provides an easy way to create a dedicated, private connection between your data center or existing network and Oracle Cloud Infrastructure. FastConnect provides higher-bandwidth options, and a more reliable and consistent networking experience compared to internet-based connections.

FastConnect location

A specific data center where you can connect to Oracle Cloud Infrastructure by using FastConnect.

fault domain

A logical grouping of hardware and infrastructure within an availability domain to provide isolation of resources in case of hardware failure or unexpected software changes.

File System

An organized system of directories and folders where data is stored.

frequency

(Monitoring service) The time period between each posted raw data point for a given metric. (Raw data points are posted by the metric namespace to the Monitoring service.)

G

group

A collection of users who all need a particular type of access to a set of resources or compartment.

guest operating system

An operating system installed on a cloud instance.

guest OS

An operating system installed on a cloud instance.

H

health check

A test to confirm the availability of backend servers.

I

IaaS

A service that allows customers to rapidly scale up or down their computer infrastructure (computing, storage, or network).

IAM

The service for controlling authentication and authorization of users who need to use your cloud resources. Also called "IAM".

Identity and Access Management Service

The service for controlling authentication and authorization of users who need to use your cloud resources. Also called "IAM".

identity provider

A service that provides identifying credentials and authentication for federated users.

IdP

Short for "identity provider", which is a service that provides identifying credentials and authentication for federated users.

image

A template of a virtual hard drive that determines the operating system and other software for an instance.

Infrastructure-as-a-Service

A service that allows customers to rapidly scale up or down their computer infrastructure (computing, storage, or network).

instance

A bare metal or virtual machine (VM) compute host. The image used to launch the instance determines its operating system and other software. The shape specified during the launch process determines the number of CPUs and memory allocated to the instance.

instance wallet

An Autonomous Database instance wallet contains only credentials and keys for a single database instance.

internet gateway

An optional virtual router that you can add to your VCN. It provides a path for network traffic between your VCN and the internet.

interval

(Monitoring service) The time window used to convert the given set of raw data points. Example: 5 minutes

IPSec connection

The secure connection between a dynamic routing gateway (DRG) and customer-premises equipment (CPE), consisting of multiple IPSec tunnels. The IPSec connection is one of the components forming a site-to-site VPN between a virtual cloud network (VCN) and your on-premises network.

IPv6

An object that contains an IPv6 address and related properties. Currently IPv6 addressing is supported only in the US Government Cloud. Only instances in IPv6-enabled VCNs and IPv6-enabled subnets can have IPv6 addresses.

IQN

A unique ID assigned to an iSCSI device. Used when connecting a volume to an instance.

iSCSI

A TCP/IP based standard used for communication between a volume and attached instance.

iSCSI Qualified Name

A unique ID assigned to an iSCSI device. Used when connecting a volume to an instance.

K

key pair

A security mechanism consisting of a public key and a private key. Required (for example) for Secure Shell (SSH) access to an instance.

L

listener

An entity that checks for incoming traffic on the load balancer's public floating IP address.

local peering gateway

A component on a VCN for routing traffic to a locally peered VCN. "Local" peering means the two VCNs are in the same region. Compare with a remote peering connection.

local VCN peering

The process of connecting two VCNs in the same region so that their resources can communicate without routing the traffic over the internet or through your on-premises network.

LPG

A component on a VCN for routing traffic to a locally peered VCN. "Local" peering means the two VCNs are in the same region. Compare with a remote peering connection.

M

message

(Notifications and Monitoring services) An alert published to all subscriptions in the specified topic. Each message is delivered at least once per subscription.

metric

(Monitoring service) A measurement related to health, capacity, or performance of a given resource. Example: CpuUtilization

metric definition

(Monitoring service) A set of references, qualifiers, and other information provided by a metric namespace for a given metric.

metric namespace

(Monitoring service) Indicator of the resource, service, or application that emits the metric. Provided in the metric definition. Example: oci_computeagent

metric stream

(Monitoring service) An individual set of aggregated data for a metric. Typically specific to a resource.

Monitoring Query Language

(Monitoring service) The syntax used for metric and alarm queries.

Mount Point

A directory from which a client may access a remote File Storage Service file system.

Mount Target

An NFS endpoint that allows a file system to be accessed by clients.

MQL

(Monitoring service) Monitoring Query Language. The syntax used for metric and alarm queries. In the Console, MQL syntax of queries is displayed in Advanced Mode.

N

NAT gateway

An optional virtual router that you can add to your VCN to perform Network Address Translation (NAT). A NAT gateway gives cloud resources without public IP addresses access to the internet without exposing those resources to incoming internet connections.

network security group

One method for implementing security rules in a VCN. A network security group consists of a set of resources (VNICs or resources with VNICs) and security rules that apply to those resources. See also security rules and security lists.

notification destination

(Monitoring service) Protocol and other details for sending messages when the alarm transitions to another state, such as from "OK" to "FIRING."

NSG

One method for implementing security rules in a VCN. A network security group consists of a set of resources (VNICs or resources with VNICs) and security rules that apply to those resources. See also security rules and security lists.

O

object

Any type of data, regardless of content type, is stored as an object. The object is composed of the object itself and metadata about the object. Each object is stored in a bucket.

OCID

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

one-time password

A single-use Console password that Oracle assigns to a new user, or to an existing user who requested a password reset.

Oracle Cloud Identifier

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

OTP

A single-use Console password that Oracle assigns to a new user, or to an existing user who requested a password reset.

P

policy

An IAM document that specifies who has what type of access to your resources. It is used in different ways: to mean an individual statement written in the policy language; to mean a collection of statements in a single, named "policy" document (which has an Oracle Cloud ID (OCID) assigned to it); and to mean the overall body of policies your organization uses to control access to resources.

policy statement

Policies can contain one or more individual statements. Each statement gives a group a certain type of access to certain resources in a particular compartment.

primary IP

The private IP that is automatically created and assigned to a VNIC during creation.

primary VNIC

The VNIC that is automatically created and attached to an instance during launch.

private IP

An object that contains a private IPv4 address and related properties such as a hostname for DNS. Each instance automatically comes with a primary private IP, and you can add secondary ones.

private peering

One of the ways to use FastConnect. Private peering lets you extend your existing infrastructure into a virtual cloud network (VCN) in Oracle Cloud Infrastructure (for example, to implement a hybrid cloud, or a lift and shift scenario). Communication across the connection is with IPv4 private addresses (typically RFC 1918).

private subnet

A subnet in which instances are not allowed to have public IP addresses

private virtual circuit

A FastConnect virtual circuit that supports private peering.

public IP

An object that contains a public IP address and related properties. You control whether each private IP on an instance has an assigned public IP. There are two types: reserved public IPs and ephemeral public IPs.

public peering

One of the way to use FastConnect. Public peering lets your on-premises network access public services in Oracle Cloud Infrastructure without using the internet. For example, Object Storage, the Oracle Cloud Infrastructure Console and APIs, or public load balancers in your VCN. Communication across the connection is with IPv4 public IP addresses. Without FastConnect, the traffic destined for public IP addresses would be routed over the internet. With FastConnect, that traffic goes over your private physical connection.

public subnet

A subnet in which instances are allowed to have public IP addresses. When you launch an instance in a public subnet, you specify whether the instance should have a public IP address.

public virtual circuit

A FastConnect virtual circuit that supports public peering.

Q

query

(Monitoring service) The expression to evaluate for returning aggregated data. A valid query includes a metric, statistic, and interval. In the Console, you can view a query in Basic Mode or Advanced Mode. The latter displays the Monitoring Query Language (MQL) syntax.

R

realm

A logical collection of regions. Realms are isolated from each other and do not share any data. Your tenancy exists in a single realm and can access the regions that belong to that realm.

region

A collection of availability domains located in a single geographic location.

regional subnet

A subnet that spans all availability domains (ADs) in the region. Oracle recommends using regional subnets because they are more flexible and make it easier to implement failover across ADs. Compare with AD-specific subnets.

regional wallet

An Autonomous Database regional wallet contains credentials and keys for all Autonomous Databases in a specified region.

remote peering connection

A component on a dynamic routing gateway (DRG) for routing traffic to a remotely peered VCN. "Remote" peering means the two VCNs are in different regions. Compare with a local peering gateway.

remote VCN peering

The process of connecting two VCNs in different regions so that their resources can communicate without routing their traffic over the internet or through your on-premises network.

reserved public IP

A public IP address (and related properties) that you create in your tenancy and assign to your instances in a given region as you like. It persists in your tenancy until you delete it. It can be assigned to any private IP on a given VNIC, not just the primary private IP. Compare with ephemeral private IP.

resolution

(Monitoring service) The period between time windows, or the regularity at which time windows shift. Example: 1 minute

resource

The cloud objects that your company's employees create and use when interacting with Oracle Cloud Infrastructure.

route table

Virtual route table for your VCN that provides mapping for the traffic from subnets via gateways to external destinations.

RPC

A component on a dynamic routing gateway (DRG) for routing traffic to a remotely peered VCN. "Remote" peering means the two VCNs are in different regions. Compare with a local peering gateway.

S

secondary IP address

An additional private IP you've added to a VNIC on an instance. Each VNIC automatically comes with a primary private IP that cannot be removed.

secondary VNIC

An additional VNIC you've added to an instance. Each instance automatically comes with a primary VNIC that cannot be removed.

security list

One method for implementing security rules in a VCN. A security list consists of security rules that apply to all resources in any subnet that uses the security list. See also security rules and network security groups.

security rule

Virtual firewall rules for your VCN. Each security rule specifies a type of ingress or egress traffic allowed in or out of a resource or VNIC. Also see network security groups and security lists.

service gateway

An optional virtual router that you can add to your VCN. The gateway enables on-premises hosts or VCN hosts to privately access Oracle services (such as Object Storage and Autonomous Database) without exposing the resources to the public internet.

shape

A template that determines the number of CPUs and the amount of memory allocated to a newly created instance.

statement

Policies can contain one or more individual statements. Each statement gives a group a certain type of access to certain resources in a particular compartment.

statistic

The aggregation function applied to the given set of raw data points. Example: SUM

subnet

Subdivision of your VCN used to separate your network into multiple smaller, distinct networks.

subscription

(Notifications service) An endpoint for a topic; typically a URL or email address. Published messages are sent to each subscription for a topic.

suppression

(Monitoring service) A configuration to avoid publishing messages during the specified time range. Useful for suspending alarm notifications during system maintenance.

Swift password

(Deprecated. Use an auth token to authenticate with your Swift client.) Swift is the OpenStack object store service. A Swift password enables you to use an existing Swift client with Oracle Cloud Infrastructure Object Storage.

T

tenancy

The root compartment that contains all of your organization's compartments and other Oracle Cloud Infrastructure cloud resources.

tenant

The name assigned to a particular company's or organization's overall environment. Users provide their tenant when signing in to the Console.

topic

(Notifications service) A communication channel for sending messages to the subscriptions in the topic.

transit routing

A network setup in which your on-premises network uses a connected virtual cloud network (VCN) to reach Oracle resources or services beyond that VCN. You connect the on-premises network to the VCN with a FastConnect private virtual circuit or VPN Connect, and then configure the VCN routing so that traffic transits through the VCN to its destination beyond the VCN. You can use transit routing to access multiple VCNs from your on-premises network over a single FastConnect or VPN Connect. Or you can use it to give your on-premises network private access to Oracle services so that on-premises hosts use their private IP addresses and the traffic does not go over the internet.

trigger rule

(Monitoring service) The condition that must be met for the alarm to be in the firing state. A trigger rule can be based on a threshold or absence of a metric.

U

user

An individual employee or system that needs to manage or use your company's Oracle Cloud Infrastructure resources.

V

VCN

A virtual version of a traditional network—including CIDRs, subnets, route tables, and gateways—on which your instance runs.

virtual circuit

Used with Oracle Cloud Infrastructure FastConnect. An isolated network path that runs over one or more physical network connections to provide a single, logical connection between the edge of your existing network and Oracle Cloud Infrastructure.

virtual cloud network

A virtual version of a traditional network—including CIDRs, subnets, route tables, and gateways—on which your instance runs.

virtual machine

A software-based emulation of a full computer that runs within a physical host computer.

virtual network interface card

A VNIC enables an instance to connect to a VCN and determines how the instance connects with endpoints inside and outside the VCN. Each instance automatically comes with a primary VNIC,

Glossary

and you can add secondary ones. Other types of cloud resources also automatically get a VNIC upon creation (examples: load balancers, DB systems).

VM

A software-based emulation of a full computer that runs within a physical host computer.

VNIC

A VNIC enables an instance to connect to a VCN and determines how the instance connects with endpoints inside and outside the VCN. Each instance automatically comes with a primary VNIC, and you can add secondary ones. Other types of cloud resources also automatically get a VNIC upon creation (examples: load balancers, DB systems).

volume

A detachable block storage device that allows you to dynamically expand the storage capacity of an instance.

W

work request

An object that reports on the current state of an asynchronous service request.