Contents

Preface

Audience v
Documentation Accessibility v
Related Documents v
Conventions v

1 Get Started

The Components of Dedicated Exadata Infrastructure 1-1
User Roles Associated with Dedicated Exadata Infrastructure 1-2
Service Maintenance of Dedicated Exadata Infrastructure 1-2
Access Control Within Dedicated Exadata Infrastructure 1-3
Compartment Quotas to Manage Resource Availability 1-4
Events and Notifications to Watch Resource Activity 1-5
Work Requests to Monitor Long-Running Operations 1-5
Typical Workflow 1-6
Access Autonomous Database in the Oracle Cloud Infrastructure Console 1-6
Getting Help and Contacting Oracle Support 1-7
Create a Service Request in My Oracle Support 1-7
Set Up Access to My Oracle Support 1-8

2 Plan Access Controls and Create Supporting Resources

3 Create and Manage Autonomous Exadata Infrastructure Resources

Create an Autonomous Exadata Infrastructure Resource 3-1
View Details of an Autonomous Exadata Infrastructure Resource 3-2
Change the Maintenance Schedule of an Autonomous Exadata Infrastructure Resource 3-4
View Scheduled and Past Maintenance of an Autonomous Exadata Infrastructure Resource 3-5
Move an Autonomous Exadata Infrastructure Resource to a Different Compartment 3-5
4 Create and Manage Autonomous Container Databases

Create an Autonomous Container Database 4-1
View Details of an Autonomous Container Database 4-2
Change the Maintenance Schedule of an Autonomous Container Database 4-4
Change the Maintenance Type of an Autonomous Container Database 4-5
View Scheduled and Past Maintenance of an Autonomous Container Database 4-5
Restart an Autonomous Container Database 4-6
Move an Autonomous Container Database to a Different Compartment 4-6
Terminate an Autonomous Container Database 4-7
View a List of Autonomous Container Databases 4-7
   View a List of Autonomous Container Databases in a Compartment 4-7
   View a List of Autonomous Container Databases in an Autonomous Exadata Infrastructure Resource 4-8

A Characteristics of Autonomous Exadata Infrastructure Resources

B Configuration Example: Network Isolation by Subnet

Step 1. Create Compartments B-2
Step 2. Create the VCN and Subnets B-2
Step 3. Create Groups B-5
Step 4. Create Policies B-6
Step 5. Assign Fleet Administrators B-7
Step 6. Create the Autonomous Exadata Infrastructure Resource B-7
Step 7. Create Autonomous Container Database Resources B-7
Step 8. Assign Database Administrators B-8

C Notifications Example: Emails for Maintenance Events

Step 1. Create a Notifications Topic C-2
Step 2. Add a Subscription to the Notifications Topic C-2
Step 3. Add an Events Service Rule C-3
Preface

This document describes how fleet administrators create and configure the Oracle Autonomous Database resources needed to permit other users to create Autonomous Database databases on dedicated Exadata infrastructure.

Audience

This document is intended for Oracle Cloud users who are designated as fleet administrators for Oracle Autonomous Database.

Documentation Accessibility

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.

Access to Oracle Support

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.

Related Documents

- Getting Started with Oracle Cloud
- Oracle Cloud Infrastructure Object Storage Documentation
- Oracle Data Integration Platform Cloud
- Storage Classic
- Oracle Cloud Infrastructure Object Storage
- GoldenGate Real-Time Data Replication in Cloud
- Using Oracle GoldenGate Cloud Service
- Getting Started with Oracle Analytics Cloud

Conventions

The following text conventions are used in this document.
<table>
<thead>
<tr>
<th>Convention</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>boldface</strong></td>
<td>Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.</td>
</tr>
<tr>
<td><em>italic</em></td>
<td>Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.</td>
</tr>
<tr>
<td><strong>monospace</strong></td>
<td>Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.</td>
</tr>
</tbody>
</table>
Get Started

The dedicated Exadata infrastructure feature of Oracle Autonomous Database enables you to create an Oracle Autonomous Database platform that is private and isolated to your use all the way down to the Oracle Exadata hardware running your database instances and storing your database data.

You define and use Oracle Cloud Infrastructure Networking and IAM (Identity and Access Management) resources to ensure secure and authorized use of your dedicated Autonomous Databases and the database resources that underlie them.

Topics

• The Components of Dedicated Exadata Infrastructure
• User Roles Associated with Dedicated Exadata Infrastructure
• Service Maintenance of Dedicated Exadata Infrastructure
• Access Control Within Dedicated Exadata Infrastructure
• Compartment Quotas to Manage Resource Availability
• Events and Notifications to Watch Resource Activity
• Work Requests to Monitor Long-Running Operations
• Typical Workflow
• Access Autonomous Database in the Oracle Cloud Infrastructure Console
• Getting Help and Contacting Oracle Support

The Components of Dedicated Exadata Infrastructure

The Oracle Autonomous Database dedicated Exadata infrastructure feature is based upon four kinds of Oracle Cloud resources:

• An **Autonomous Exadata Infrastructure** resource allocates an available Oracle Exadata Database Machine to you. Its primary purpose is to act as a bridge between the hardware and software components of your dedicated infrastructure. You must create at least one Autonomous Exadata Infrastructure resource before you can create any of the other kinds of dedicated infrastructure resources.

• An **Autonomous Container Database** resource provides a container for your Autonomous Databases. You can create multiple Autonomous Container Database resources in a single Autonomous Exadata Infrastructure resource, but you must create at least one before you can create any Autonomous Databases.

• An **Autonomous Database** resource is a user database. To create a dedicated Autonomous Database, you create an Autonomous Database, specifying “Data Warehouse” or “Transaction Processing” as its workload type and “Dedicated Infrastructure” as its deployment type. You can create many Autonomous Databases in a single Autonomous Container Database resource.
• An **Autonomous Backup** resource is a backup of an Autonomous Database. Oracle creates these resources for you automatically.

**User Roles Associated with Dedicated Exadata Infrastructure**

The tasks involved in setting up and using the Oracle Autonomous Database dedicated Exadata infrastructure feature can be grouped into three logical roles: a few people act as fleet administrators, more act as database administrators, and even more act as database users. A given person can assume one or more of these roles, depending on how you decide to isolate and distribute duties.

• **Fleet Administrator.** Fleet administrators create, monitor and manage Autonomous Exadata Infrastructure and Autonomous Container Database resources.

  To perform these duties, a fleet administrator must be an Oracle Cloud user whose permissions permit the management of these resources and permit the use of the networking resources that need to be specified when creating these resources.

• **Database Administrator.** Database administrators create, monitor and manage Autonomous Databases. Additionally, they create and manage Oracle Database users within these databases, and provide others the information necessary to access the database.

  To perform these duties, a database administrator must be an Oracle Cloud user whose permissions permit the management of Autonomous Database and Autonomous Backup resources and permit the use of the Autonomous Container Database and networking resources that need to be specified when creating an Autonomous Database. When creating an Autonomous Database resource, the database administrator defines and gains access to the ADMIN administrative user account for the database.

• **Database User.** Database users are the developers who write applications that connect to and use an Autonomous Database to store and access the data. Database users do not need Oracle Cloud accounts: they gain network connectivity to and connection authorization information for the database from the database administrator.

**Service Maintenance of Dedicated Exadata Infrastructure**

Oracle schedules and performs all patching and other maintenance operations on all dedicated Exadata infrastructure resources.

You can specify when such maintenance operations can occur, and what kind of database patching is performed.

**Specifying When Maintenance Can Occur**

In general, Oracle schedules and performs maintenance in the first week of every quarter. You can let Oracle handle maintenance scheduling, or you can set a specific maintenance window when Oracle can begin maintenance operations. You set this maintenance window at the Autonomous Exadata Infrastructure level, and it applies to
all Autonomous Container Databases and Autonomous Databases created in the Autonomous Exadata Infrastructure resource as well as to the resource itself.

Additionally, you can set a maintenance window for each individual Autonomous Container Database. If you do so, the window applies to all Autonomous Databases in the Autonomous Container Database as well as to the Autonomous Container Database itself.

**Tip:**

Oracle recommends that you set a maintenance window for at least Autonomous Exadata Infrastructure resources. Doing so will prevent maintenance operations from occurring at times that would be disruptive to regular database operations.

You can set the maintenance window for an Autonomous Exadata Infrastructure resource when you create it or you can set or change it later. See Create an Autonomous Exadata Infrastructure Resource or Change the Maintenance Schedule of an Autonomous Exadata Infrastructure Resource.

You can set the maintenance window for an Autonomous Container Database when you create it or you can set or change it later. See Create an Autonomous Container Database or Change the Maintenance Schedule of an Autonomous Container Database.

**Specifying What Kind of Patches to Apply**

One standard maintenance operation is to apply database software patches to your Autonomous Container Databases and, by extension, the Autonomous Databases created in them. By default, Oracle applies Release Updates (RUs). You can choose to have Oracle apply Release Update Revisions (RURs) instead on a container-database by container-database basis. You can do this when you create an Autonomous Container Database (see Create an Autonomous Container Database) or later (see Change the Maintenance Type of an Autonomous Container Database).

To help you decide whether to have Oracle apply RUs or RURs to a given Autonomous Container Database, see My Oracle Support Note 2285040.1, Release Update Introduction and FAQ.

**Viewing Upcoming Scheduled Maintenance**

You can view when any upcoming maintenance is scheduled for an Autonomous Exadata Infrastructure resource or an Autonomous Container Database. For instructions, see View Scheduled and Past Maintenance of an Autonomous Exadata Infrastructure Resource and View Scheduled and Past Maintenance of an Autonomous Container Database.

**Access Control Within Dedicated Exadata Infrastructure**

When configuring the dedicated Exadata infrastructure feature, you need to ensure that your cloud users have access to use and create only the appropriate kinds of cloud resources to perform their job duties. Additionally, you need to ensure that only authorized personnel and applications have access to the autonomous databases created on dedicated infrastructure. Otherwise, you run the risk of “runaway”
consumption of your dedicated infrastructure resources or inappropriate access to mission-critical data.

Therefore, before you begin creating and using the cloud resources that provide the dedicated infrastructure feature, you need to formulate an access control plan, and then institute by creating appropriate IAM (Identity and Access Management) and Networking resources.

The kinds of IAM resources you will use include:

- **Compartment**: A collection of related resources. Compartments are a fundamental component of Oracle Cloud Infrastructure for organizing and isolating your cloud resources.
- **Group**: A collection of users who all need the same type of access to a particular set of resources or compartment.
- **Policy**: A group of statements that specify who can access which resources, and how. Access is granted at the group and compartment level, which means you write a policy statement that gives a specific group a specific type of access to a specific type of resource within a specific compartment.

The kinds of Networking resources you will use include:

- **VCN (Virtual Cloud Network)**: A virtual, private network that you set up in a single Oracle Cloud Infrastructure region. It closely resembles a traditional network, with firewall rules and specific types of communication gateways that you can choose to use.
- **Subnet**: A subdivision you define in a VCN. Subnets contain VNICs (virtual network interface cards), which are attached to the dedicated infrastructure resources you create. Subnets act as a unit of configuration within the VCN: all VNICs in a given subnet use the same route table, security lists, and DHCP options. You can designate a subnet as either public or private when you create it. Private means VNICs in the subnet can't have public IP addresses. Public means VNICs in the subnet can have public IP addresses at your discretion.

Depending on how you decide to control access to autonomous databases, you will use various other kinds of Networking resources.

For guidance in formulating your access control plan and creating the resources to institute it, see Plan Access Controls and Create Supporting Resources.

**Compartment Quotas to Manage Resource Availability**

Oracle Autonomous Database supports the compartment quotas feature of Oracle Cloud Infrastructure. Using this feature you can restrict, on a compartment by compartment basis, the availability of the following dedicated infrastructure resources in your tenancy:

- OCPUs available to dedicated deployments of Autonomous Data Warehouse databases.
- Total data storage available to dedicated deployments of Autonomous Data Warehouse databases.
- OCPUs available to dedicated deployments of Autonomous Transaction Processing databases.
• Total data storage available to dedicated deployments of Autonomous Transaction Processing databases.

In brief, you use the compartment quotas feature by creating set, unset and zero policy statements to limit the availability of a given resource in a given compartment. For detailed information and instructions, see Compartment Quotas.

Events and Notifications to Watch Resource Activity

When Oracle Autonomous Database performs operations on resources, it sends events to the Events service. Using the Events service, you can create rules to capture these events and perform actions such as sending you emails using the Notifications service.

Tip:

See Notifications Example: Emails for Maintenance Events for a short end-to-end example of using the Events and Notifications services in this way.

This combination of Autonomous Database events, the Events service and the Notification service provide a very rich set of options for keeping abreast of resource activity because:

• Autonomous Database generates events for more than forty different operations, providing you fine-grained choices for resource tracking.

For listings of the operations that generate events, see Autonomous Exadata Infrastructure Event Types, Autonomous Container Database Event Types and Autonomous Database Event Types.

• The Events service supports arbitrary grouping of events in a single rule, providing flexible aggregation of the events you are interested in.

For more information about how the Events service works and how to set up the rules and actions it uses, see Overview of Events.

• The Notifications service supports sending notices to email, PagerDuty, Slack, custom HTTPS urls or Oracle Functions, providing you a wide variety of communication channels.

For more information about how the Notifications service works and how to set up the topics and subscriptions it uses, see Notifications Overview.

Work Requests to Monitor Long-Running Operations

Oracle Autonomous Database is integrated with the Oracle Cloud Infrastructure Work Requests feature. Work requests allow you to monitor long-running operations like the creation of an Autonomous Database. A work request is an activity log that enables you to track each step in the operation's progress. Each work request has an OCID that allows you to interact with it programmatically and use it for automation.

For a list of Oracle Autonomous Database operations that create work requests, see Work Requests Integration.
For general information on using work requests in Oracle Cloud Infrastructure, see Work Requests and Work Requests API.

**Typical Workflow**

To start using the Oracle Autonomous Database dedicated Exadata infrastructure feature, refer to the following tasks as a guide.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Determine and institute user access constraints</td>
<td>Determine the controls you deem necessary to ensure that your users have the appropriate access to the appropriate cloud resources to perform their job duties, and then create infrastructure resources to institute these controls.</td>
<td>Plan Access Controls and Create Supporting Resources</td>
</tr>
<tr>
<td>Confirm resource availability</td>
<td>Make sure your service limits show at least one Exadata.Quarter2.92 - X7 database resource available; request a service limit increase if necessary.</td>
<td>Service Limits in Oracle Cloud Infrastructure Documentation.</td>
</tr>
<tr>
<td>Create Autonomous Exadata Infrastructure resources</td>
<td>Create at least one Autonomous Exadata Infrastructure resource.</td>
<td>Create an Autonomous Exadata Infrastructure Resource</td>
</tr>
<tr>
<td>Create Autonomous Container Database resources</td>
<td>Create at least one Autonomous Container Database in an Autonomous Exadata Infrastructure.</td>
<td>Create an Autonomous Container Database</td>
</tr>
<tr>
<td>Create Autonomous Databases</td>
<td>Create at least one Autonomous Database in an Autonomous Container Database resource.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Administrator’s Guide to Oracle Autonomous Database Dedicated Deployments</td>
</tr>
</tbody>
</table>

**Access Autonomous Database in the Oracle Cloud Infrastructure Console**

2. Click the sign-in icon at the top of the page and then click Sign in to Cloud.
3. Enter the name of your cloud account in the Account field and then click Next.
4. On the Oracle Cloud Account Sign In page, enter your sign-in credentials and then click Sign In.
5. Click the menu icon in the top corner to display the side menu and then click Autonomous Data Warehouse or Autonomous Transaction Processing.

The Autonomous Databases page opens, showing the list of databases in your current Compartment.
Getting Help and Contacting Oracle Support

When using Autonomous Database on dedicated infrastructure, there will be times when you need to get help from the community or to talk to someone in Oracle support.

Chances are that someone else has likely asked your question in the past. To find out, use scoped search to look for answers in our documentation and our forum platforms. 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:oracle.com

If you don't find the answer, you can remove site:oracle.com to see whether one of the many public forums whose members discuss Oracle Cloud and Oracle Database give you the help you need.

If you can't find an answer to your question through search, you can submit a question to Cloud Customer Connect at cloudcustomerconnect.oracle.com, or you can create a service request to engage the Oracle Support team.

Create a Service Request in My Oracle Support

If you are having a technical issue using Autonomous Database on dedicated infrastructure, you can contact Oracle Support by creating a service request in My Oracle Support.

Note:
If you have not created a service request before, see Set Up Access to My Oracle Support to perform any necessary one-time activities to access My Oracle Support.

Tip:
Before following these steps, sign in to your Oracle Cloud account at cloud.oracle.com in a separate browser tab or window so that you can quickly and easily get any information you need to complete your service request.

1. Go to the My Oracle Support website at support.oracle.com and sign in with your Oracle account.
2. If you see "MY ORACLE SUPPORT" next to the Oracle logo at the top of the page, click Switch to Cloud Support.
3. Click Service Requests and then, after the page refreshes, click Create Technical SR.
   The Create Technical Service Request wizard is displayed.
4. For **Service Type**, select **Autonomous Database Dedicated**. The **Service Name** and **Problem Type** fields are displayed after **Service Type**.

5. For **Service Name**, select the value corresponding to your tenancy's CSI.

6. For **Problem Type**, locate and select the problem type that most fits your issue. For example, you might select Database Administration > General DB Admin Issues.

A list of information you need to provide for the problem type you selected appears after the **Description** field.

7. For **Problem Summary**, enter a brief statement (up to 100 characters) describing your issue.

8. For **Description**, enter a description (up to 2000 characters) of what went wrong, what you were doing that led up to it, and what you expected to happen.

9. Complete the list of required information that follows the **Description** field.

   In addition to information about when you ran into your problem, you are often asked to provide the name and OCID (Oracle Cloud Identifier) of your tenancy and the cloud resource or resources you are having a problem with.

   To get information about your tenancy, sign into your Oracle Cloud account, click the profile icon in the top corner to open the Profile menu, and then click the link for your tenancy to display a page that shows your tenancy's name, OCID and other information.

   To get similar information for a cloud resource (like a dedicated Autonomous Database), go to the details page for that resource.

10. Check that your contact information is correct, and then click **Next** to go to the **Additional Details** step.

11. At the **Additional Details** step, provide additional information about your issue, if requested, and upload any attachments that will make troubleshooting your issue easier. Then, click **Next** to go to the **Confirmation** step.

12. At the **Confirmation** step, check the information you have provided. If you need to change anything, click **Back** to go back and change information. When you are satisfied, click **Submit**.

   The Create Technical Service Request wizard closes and your newly created service request is displayed in the list of your Technical SRs.

---

**Set Up Access to My Oracle Support**

To create service requests with My Oracle Support, you must first perform these one-time activities:

- Get (or have) an Oracle account, sometimes called an oracle.com or Oracle SSO account. This account, different from your Cloud account, gives you access to a variety of services on the Oracle website, like making purchases through Oracle Store and logging service requests in My Oracle Support.

If you don't already have an Oracle account, see [Get an Oracle Account](#) for instructions.
• Use your Oracle account to register your tenancy's Customer Support Identifier (CSI) in My Oracle Support.
  See Register Your CSI Number in My Oracle Support for instructions.
• Link your Oracle account to your Cloud account in Oracle Cloud.
  See Link Your Oracle Account to Your Cloud Account for instructions.

Get an Oracle Account
2. Click the
   View Accounts icon. Then, under Oracle Account, click Create an Account.
   The Create Your Oracle Account page is displayed.
3. Enter your email address and other details in the appropriate fields. Be sure to complete all the required fields.
4. Click Create Account.
   After your account is created, you'll receive a confirmation email at the email address that you provided.
5. Follow the instructions in the email to verify your email address.

Register Your CSI Number in My Oracle Support
1. Get the CSI (Customer Support Identifier) number for your tenancy:
   a. Sign in to your Oracle Cloud account at cloud.oracle.com.
   b. Click the
      profile icon in the top corner to open the Profile menu. Then, click the link for your tenancy.
      A page showing information about your tenancy is displayed.
   c. In the Tenancy Information tab, locate the CSI Number field and note down your tenancy's CSI number.
2. Go to the My Oracle Support website at support.oracle.com and sign in with your Oracle Account.
3. If prompted, accept the My Oracle Support terms of use.
4. From the logged-in user menu, click My Account.
5. In the Support Identifiers section, click Request Access. The Support Identifiers section displays the accounts that your user name is currently associated with.
6. Enter your CSI number, an optional note to approver, and then click Request Access.
7. Enter your company name that owns the CSI number and click Validate.
8. Click Next and enter your contact details.
9. Accept the terms and conditions and click Next.
The status of your request is pending until you receive approval from the Customer User Administrator (CUA) for your tenancy's CSI.

Link Your Oracle Account to Your Cloud Account

1. Sign in to your Oracle Cloud account at cloud.oracle.com.
2. Click the icon in the top corner to open the navigation menu. Under Governance and Administration, go to Identity and click Users.
   A list of the users in your tenancy is displayed.
3. Find and click your user name.
   Your user details are displayed.
4. Click Link Support Account.
   The Oracle account sign in page prompts you to enter your Oracle credentials.
5. Enter the user name and password of the Oracle account that you used to register your CSI number in My Oracle Support, and then click Sign in.
   Your Cloud account is linked to the Oracle account. The e-mail address associated with the Oracle account is displayed in the user details in the field My Oracle Support account.
Plan Access Controls and Create Supporting Resources

When configuring the dedicated infrastructure feature of Oracle Autonomous Database, you need to ensure that your cloud users have access to use and create only the appropriate kinds of cloud resources to perform their job duties. Additionally, you need to ensure that only authorized personnel and applications have network access to the autonomous databases created on dedicated infrastructure.

To institute access controls for cloud users, you define policies that grant specific groups of users specific access rights to specific kinds of resources in specific compartments.

To institute network access controls, you create VCNs and subnets and then, using the same policy mechanism, permit only the appropriate VCN and subnet to be used when a dedicated infrastructure resource is created. Thus, you can ensure the proper network isolation of resources.

The following topics provide more information; they are:

- Policies and Policy Statements
- Network Isolation
- Best Practices When Planning and Instituting Access Controls
- Examples

Policies and Policy Statements

The primary tool you use to define access control for cloud users is the **policy**, an IAM (Identity and Access Management) resource containing policy statements that specify access in terms of "Who", "How", "What" and "Where".

The format of a policy statement is:

Allow
  group <group-name>
  to <control-verb> <resource-type>
  in compartment <compartment-name>

- **group <group-name>** specifies the "Who" by providing the name of an existing group, an IAM resource to which individual cloud users can be assigned.

  In the context of the dedicated infrastructure feature, FleetAdmin is an example of a group.

- **to <control-verb>** specifies the "How" using one of these predefined control verbs:
– **inspect**: the ability to list resources of the given type, without access to any confidential information or user-specified metadata that may be part of that resource.

– **read**: inspect plus the ability to get user-specified metadata and the actual resource itself.

– **use**: read plus the ability to work with existing resources, but not to create or delete them. Additionally, "work with" means different operations for different resource types.

– **manage**: all permissions for the resource type, including creation and deletion.

In the context of the dedicated infrastructure feature, a fleet administrator can manage autonomous container databases, while a database administrator can only use them to create autonomous databases.

• `<resource-type>` specifies the "What" using a predefined resource-type. The resource-type values for the dedicated infrastructure resources are:

  – autonomous-exadata-infrastructures
  
  – autonomous-container-databases
  
  – autonomous-databases
  
  – autonomous-backups

Because dedicated infrastructure resources use networking resources, some of the policy statements you create will refer to the `virtual-network-family` resource-type value. Also, you may create policy statements that refer to the `tag-namespaces` resource-type value if tagging is used in your tenancy.

• **in compartment `<compartment-name>`** specifies the "Where" by providing the name of an existing compartment, an IAM resource in which resources are created. Compartments are a fundamental component of Oracle Cloud Infrastructure for organizing and isolating cloud resources.

### Network Isolation

When fleet administrators create an Autonomous Exadata Infrastructure or Autonomous Container Database resource, and when database administrators create an Autonomous Database, they must specify an existing network subnet (in a network VCN) for the resource use.

Because these networking resources must already exist, you ensure network isolation and access control by:

1. Creating VCNs and subnets in different compartments that reflect your network isolation needs

2. Defining policies that ensure that only the right VCN and subnet are used when creating a given dedicated infrastructure resource.

### Best Practices When Planning and Instituting Access Controls

When planning and instituting your access controls for the dedicated infrastructure feature, you should consider these best practices.

• **Create a separate VCN that contains only private subnets.** In almost every case, the Autonomous Databases created on dedicated infrastructure house data that is company-sensitive and is normally accessible only from within the
company’s private network. Even the data shared with partners, suppliers, consumers and customers is made available to them through regulated, secure channels.

Therefore, the network access you provide to such databases should be private to your company. You can ensure this by creating a VCN that uses private subnets and an IPSec VPN or FastConnect to connect to your company’s private network. For information about setting up such a configuration, see Scenario B: Private Subnets with a VPN in Oracle Cloud Infrastructure Documentation.

For additional information about securing network connectivity to your databases, see Ways to Secure Your Network in Oracle Cloud Infrastructure Documentation.

- **Create at least two subnets.** You should create at least two subnets: one for Autonomous Exadata Infrastructure and Autonomous Container Database resources and one for resources associated with clients and applications of Autonomous Database.

- **Create at least two compartments.** You should create at least two compartments: one for Autonomous Exadata Infrastructure and Autonomous Container Database resources and one for Autonomous Database resources.

- **Create at least two groups.** You should create at least two groups: one for fleet administrators and one for database administrators.

Examples

Here are examples that show how to set up cloud resources to meet common access-control use cases.

- **Configuration Example: Network Isolation by Subnet.**
Create and Manage Autonomous Exadata Infrastructure Resources

Topics

- Create an Autonomous Exadata Infrastructure Resource
- View Details of an Autonomous Exadata Infrastructure Resource
- Change the Maintenance Schedule of an Autonomous Exadata Infrastructure Resource
- View Scheduled and Past Maintenance of an Autonomous Exadata Infrastructure Resource
- Move an Autonomous Exadata Infrastructure Resource to a Different Compartment
- Change the Network Security Groups Assigned to an Autonomous Exadata Infrastructure Resource
- Terminate an Autonomous Exadata Infrastructure Resource
- View a List of Autonomous Exadata Infrastructure Resources

Create an Autonomous Exadata Infrastructure Resource

You create an Autonomous Exadata Infrastructure resource from the Autonomous Exadata Infrastructure page.

1. Go to Autonomous Database in the Oracle Cloud Infrastructure Console.
   For instructions, see Access Autonomous Database in the Oracle Cloud Infrastructure Console.

2. In the side menu's list of Autonomous Database resource types, click Autonomous Exadata Infrastructure.
   The list of Autonomous Exadata Infrastructure resources in your current Compartment is displayed.

3. In the side menu’s Compartment list, choose the Compartment where you want to create an Autonomous Exadata Infrastructure resource.
   The list of Autonomous Exadata Infrastructure resources refreshes to show those in the selected Compartment.

4. Click Create Autonomous Exadata Infrastructure.

5. On the Create Autonomous Exadata Infrastructure page, enter the following:
   - Select a compartment: Confirm that the Compartment listed is the one in which you want to create the Autonomous Exadata Infrastructure resource.
• **Display name**: A user-friendly description or other information that helps you easily identify the resource. The display name does not have to be unique, and you can change it whenever you like.

• **Select an availability domain**: Choose the availability domain where you want the resource placed.

• **Select an Exadata system model and configuration**: Choose the type of Oracle Exadata Database Machine you want the allocate to this resource. For capacity information about the models and their configurations, see Characteristics of Autonomous Exadata Infrastructure Resources.

• **Configure the network settings**:
  a. Choose the Virtual Cloud Network (VCN) in which to launch this Autonomous Exadata Infrastructure resource, first changing Compartments to the one hosting the VCN if necessary.
  b. Choose the Subnet to which this Autonomous Exadata Infrastructure resource is to attach, first changing Compartments to the one hosting the Subnet if necessary. Do not use a subnet that overlaps with 141.144.75.0/24.
  c. If you are using network security groups (NSGs) to control network traffic, click **Use network security groups to control traffic** and then add the network security groups that Autonomous Exadata Infrastructure resource is to use.

• **Configure the automatic maintenance schedule**: to configure a preferred maintenance schedule, click **Modify Schedule** and then select **Specify a Schedule**.

Choose the months when Oracle can schedule maintenance. You must select at least one month in each quarter. Then select the week, weekday within that week and hour within that day when Oracle can begin performing maintenance operations on this Autonomous Exadata Infrastructure resource. When you are finished, click **Update Maintenance Schedule**.

• **Choose a license type**: Choose the type of license to use for Autonomous Databases created on this Autonomous Exadata Infrastructure resource.

6. If you want to use Tags, click **Show Advanced Options** and then enter the **TAG KEY** and **VALUE**. Tagging is a metadata system that allows you to organize and track resources within your tenancy. Tags are composed of keys and values which can be attached to resources.

7. Click **Create Autonomous Exadata Infrastructure**.

The list of Autonomous Exadata Infrastructure resources refreshes to show the new resource with a status of **Provisioning** until the new Autonomous Exadata Infrastructure resource is available.

---

**View Details of an Autonomous Exadata Infrastructure Resource**

You view the details of an Autonomous Exadata Infrastructure resource by going to its **Details** page.

1. Go to Autonomous Database in the Oracle Cloud Infrastructure Console.
For instructions, see Access Autonomous Database in the Oracle Cloud Infrastructure Console.

2. In the side menu's list of Autonomous Database resource types, click Autonomous Exadata Infrastructure.
   The list of Autonomous Exadata Infrastructure resources in your current Compartment is displayed.

3. In the side menu's Compartment list, choose the Compartment containing the Autonomous Exadata Infrastructure resource whose details you want to view.
   The list of Autonomous Exadata Infrastructure resources refreshes to show those in the selected Compartment.

4. Click the name of the Autonomous Exadata Infrastructure resource whose details you want to view.
   The Details page for the chosen Autonomous Exadata Infrastructure resource is displayed.

On this page you can perform a variety of actions.

<table>
<thead>
<tr>
<th>Action</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>View or copy the resource's endpoint name</td>
<td>On the Autonomous Exadata Infrastructure Information tab, click Show or Copy in the DB Infrastructure Endpoint Name field.</td>
</tr>
<tr>
<td>View details of the resource's Virtual Cloud Network (VCN)</td>
<td>On the Autonomous Exadata Infrastructure Information tab, click the name of the VCN in the Virtual Cloud Network field.</td>
</tr>
<tr>
<td>View or copy the resource's OCID</td>
<td>On the Autonomous Exadata Infrastructure Information tab, click Show or Copy in the OCID field.</td>
</tr>
<tr>
<td>Edit the resource's maintenance schedule</td>
<td>On the Autonomous Exadata Infrastructure Information tab, click (Edit) in the Maintenance Schedule field.</td>
</tr>
<tr>
<td>View upcoming and past maintenance</td>
<td>On the Autonomous Exadata Infrastructure Information tab, click (View) in the Next Maintenance field. A list of upcoming planned maintenance activities, if any, is displayed. To view past maintenance activities, click Maintenance History in the side menu.</td>
</tr>
<tr>
<td>Terminate the resource</td>
<td>Click Terminate and follow the instructions in Terminate an Autonomous Exadata Infrastructure Resource.</td>
</tr>
<tr>
<td>Apply tags to the resource</td>
<td>Click Apply Tag(s).</td>
</tr>
<tr>
<td>View the tags applied to the resource</td>
<td>Click the Tags tab.</td>
</tr>
</tbody>
</table>

At the bottom of the page a list of Autonomous Container Databases in the selected Compartment that use the chosen Autonomous Exadata Infrastructure resource is displayed. Using this list you can perform a variety of actions.
## Change the Maintenance Schedule of an Autonomous Exadata Infrastructure Resource

You change the maintenance schedule of an Autonomous Exadata Infrastructure resource from its Details page.

1. Go to the Details page of the Autonomous Exadata Infrastructure resource whose maintenance schedule you want to change.
   
   For instructions, see View Details of an Autonomous Exadata Infrastructure Resource.

2. Click the (Edit) link in the Maintenance schedule field.

3. On the Automatic Maintenance Schedule card, change settings as desired.
   
   Select No Preference to permit Oracle to schedule maintenance as needed, or select Specify a Schedule to restrict when Oracle can schedule maintenance:

```plaintext
<table>
<thead>
<tr>
<th>Action</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create an Autonomous Container Database</td>
<td>Click Create Autonomous Container Database and follow the instructions in Create an Autonomous Container Database.</td>
</tr>
<tr>
<td>View details of a listed Autonomous Container Database</td>
<td>In the list of Autonomous Container Databases, click the name of the one whose details you want to view.</td>
</tr>
<tr>
<td>Copy the OCID of a listed Autonomous Container Database</td>
<td>In the list of Autonomous Container Databases, click the menu in the row of the one whose OCID you want to copy and then click Copy OCID. The OCID is copied to your clipboard and the menu item changes to Copied.</td>
</tr>
<tr>
<td>Apply tags to a listed Autonomous Container Database</td>
<td>In the list of Autonomous Container Databases, click the menu in the row of the one you want to apply tags to and then click Apply Tag(s).</td>
</tr>
<tr>
<td>View the tags applied to a listed Autonomous Container Database</td>
<td>In the list of Autonomous Container Databases, click the menu in the row of the one whose tags you want to view and then click View Tag.</td>
</tr>
<tr>
<td>Terminate a listed Autonomous Container Database</td>
<td>In the list of Autonomous Container Databases, click the menu in the row of the one you want to terminate and then click Terminate. Then, in the Terminate Autonomous Container dialog:</td>
</tr>
<tr>
<td></td>
<td>1. Read the warning about terminating an Autonomous Container Database.</td>
</tr>
<tr>
<td></td>
<td>2. Enter the name of the Autonomous Container Database.</td>
</tr>
<tr>
<td></td>
<td>3. Click Terminate Autonomous Container to begin the termination process.</td>
</tr>
</tbody>
</table>
```
• Specify the permitted months. You must select at least one month per quarter.
• Specify the week within the selected months.
• Specify the day of the selected week.
• Specify the 4-hour window (on the specified day) when maintenance operations can begin.

4. When finished, click **Update Maintenance Schedule**.

View Scheduled and Past Maintenance of an Autonomous Exadata Infrastructure Resource

You view scheduled and past maintenance of an Autonomous Exadata Infrastructure resource from its **Details** page.

1. Go to the **Details** page of the desired Autonomous Exadata Infrastructure resource.
   
   For instructions, see View Details of an Autonomous Exadata Infrastructure Resource.

2. Click the (View) link in the **Next maintenance** field.
   
   The Autonomous Database Maintenance page lists any upcoming planned maintenance.
   
   To see a list of past maintenance, click **Maintenance History** in the side menu.

Move an Autonomous Exadata Infrastructure Resource to a Different Compartment

You can move an Autonomous Exadata Infrastructure resource to a different Oracle Cloud Infrastructure compartment.

**Note:**

• To move an Autonomous Exadata Infrastructure resource you must have the right to manage the resource in its current compartment and in the compartment you are moving it to.

• As soon as you move an Autonomous Exadata Infrastructure resource to a different compartment, the policies that govern the new compartment apply immediately and affect access to the resource. Therefore, both your and other Oracle Cloud users’ access to the resource may change, depending on the policies governing the user account’s access to resources. For example, a user may lose the ability to create Autonomous Container Databases on the resource, given its new compartment.

1. Go to the **Details** page of the Autonomous Exadata Infrastructure resource you want to move.
For instructions, see View Details of an Autonomous Exadata Infrastructure Resource.

2. Click Move Resource.

3. In the Move Resource to a Different Compartment page, select the new compartment.

4. Click Move Resource.

Change the Network Security Groups Assigned to an Autonomous Exadata Infrastructure Resource

You change the network security groups assigned to an Autonomous Exadata Infrastructure resource from its Details page.

1. Go to the Details page of the desired Autonomous Exadata Infrastructure resource.

   For instructions, see View Details of an Autonomous Exadata Infrastructure Resource.

2. Click the Edit link in the Network Security Groups field.

3. In the Edit Network Security Groups dialog, add or remove network security groups as desired.

4. Click Save Changes.

Terminate an Autonomous Exadata Infrastructure Resource

You terminate an Autonomous Exadata Infrastructure resource by clicking Terminate on its Details page.

1. Go to the Details page of the Autonomous Exadata Infrastructure resource you want to terminate.

   For instructions, see View Details of an Autonomous Exadata Infrastructure Resource.

2. Click Terminate.

3. In the Terminate Autonomous Exadata Infrastructure dialog:
   a. Read the warning about terminating an Autonomous Exadata Infrastructure resource.
   b. Enter the name of the Autonomous Exadata Infrastructure resource.
   c. Click Terminate Autonomous Exadata Infrastructure to begin the termination process.

View a List of Autonomous Exadata Infrastructure Resources

You view a list of Autonomous Exadata Infrastructure resources by going to the Autonomous Exadata Infrastructure page.
1. Go to Autonomous Database in the Oracle Cloud Infrastructure Console.
   For instructions, see Access Autonomous Database in the Oracle Cloud Infrastructure Console.

2. In the side menu’s list of Autonomous Database resource types, click Autonomous Exadata Infrastructure.

The **Autonomous Exadata Infrastructure** page is displayed, showing the list of Autonomous Exadata Infrastructure resources in your current Compartment. To see the list for a different Compartment, choose its name from the side menu’s **Compartment** list.

On this page you can perform a variety of actions.

<table>
<thead>
<tr>
<th>Action</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create an Autonomous Exadata Infrastructure resource</td>
<td>Click <strong>Create Autonomous Exadata Infrastructure</strong> and follow the instructions in Create an Autonomous Exadata Infrastructure Resource.</td>
</tr>
<tr>
<td>View details of a listed Autonomous Exadata Infrastructure resource</td>
<td>In the list of Autonomous Exadata Infrastructure resources, click the name of the resource whose details you want to view.</td>
</tr>
<tr>
<td>Copy the OCID of a listed Autonomous Exadata Infrastructure resource</td>
<td>In the list of Autonomous Exadata Infrastructure resources, click the menu in the row of the resource whose OCID you want to copy and then click <strong>Copy OCID</strong>. The OCID is copied to your clipboard and the menu item changes to <strong>Copied</strong>.</td>
</tr>
<tr>
<td>Apply tags to a listed Autonomous Exadata Infrastructure resource</td>
<td>In the list of Autonomous Exadata Infrastructure resources, click the menu in the row of the resource you want to apply tags to and then click <strong>Apply Tag(s)</strong>.</td>
</tr>
<tr>
<td>View the tags applied to a listed Autonomous Exadata Infrastructure resource</td>
<td>In the list of Autonomous Exadata Infrastructure resources, click the menu in the row of the resource whose tags you want to view and then click <strong>View Tag</strong>.</td>
</tr>
<tr>
<td>Terminate a listed Autonomous Exadata Infrastructure resource</td>
<td>In the list of Autonomous Exadata Infrastructure resources, click the menu in the row of the resource you want to terminate and then click <strong>Terminate</strong>. Then, in the <strong>Terminate Autonomous Exadata Infrastructure</strong> dialog:</td>
</tr>
<tr>
<td></td>
<td>1. <strong>Read the warning about terminating an Autonomous Exadata Infrastructure resource.</strong></td>
</tr>
<tr>
<td></td>
<td>2. Enter the name of the Autonomous Exadata Infrastructure resource.</td>
</tr>
<tr>
<td></td>
<td>3. Click <strong>Terminate Autonomous Exadata Infrastructure</strong> to begin the termination process.</td>
</tr>
</tbody>
</table>
4

Create and Manage Autonomous Container Databases

Topics

• Create an Autonomous Container Database
• View Details of an Autonomous Container Database
• Change the Maintenance Schedule of an Autonomous Container Database
• Change the Maintenance Type of an Autonomous Container Database
• View Scheduled and Past Maintenance of an Autonomous Container Database
• Restart an Autonomous Container Database
• Move an Autonomous Container Database to a Different Compartment
• Terminate an Autonomous Container Database
• View a List of Autonomous Container Databases

Create an Autonomous Container Database

You create an Autonomous Container Database from the Autonomous Container Databases page.

1. Go to Autonomous Database in the Oracle Cloud Infrastructure Console.
   For instructions, see Access Autonomous Database in the Oracle Cloud Infrastructure Console.

2. In the side menu’s list of Autonomous Database resource types, click Autonomous Container Database.
   The list of Autonomous Container Databases in your current Compartment is displayed.

3. In the side menu’s Compartment list, select the Compartment where you want to create an Autonomous Container Database.
   The list of Autonomous Container Databases refreshes to show those in the selected Compartment.

4. Click Create Autonomous Container Database.

5. On the Create Autonomous Container Database page, enter the following:
   • Select a compartment: Confirm that the Compartment listed is the one in which you want to create the Autonomous Exadata Infrastructure resource.
   • Display name: A user-friendly description or other information that helps you easily identify the resource. The display name does not have to be unique, and you can change it whenever you like.
• **Select an Autonomous Exadata Infrastructure:** select the Autonomous Exadata Infrastructure resource in which to place this resource, first changing Compartments to the one hosting the Autonomous Exadata Infrastructure resource if necessary.

• **Configure automatic maintenance:** to configure a preferred maintenance type or schedule, click **Modify Maintenance** to display the **Edit Automatic Maintenance** card. You can then:
  - Change the maintenance type from the default (**Release Update (RU)**) by selecting **Release Update Revision (RUR)** from the Maintenance type list.

  **Note:** Currently, the Release Update Revision (RUR) maintenance type is not a selectable option. When release update revisions become available for Autonomous Database, this option will become selectable.

  - Change the maintenance schedule from the default (**No preference**), which permits Oracle to schedule maintenance as needed based on the maintenance schedule of the Autonomous Exadata Infrastructure resource hosting the Autonomous Container Database, by selecting **Specify a schedule** and then selecting the months, weeks, days and hours for the schedule.

  When specifying a schedule, you should ensure that the schedule you define falls after the schedule of Autonomous Exadata Infrastructure resource hosting the Autonomous Container Database. If the Autonomous Exadata Infrastructure resource has a customized schedule, you can view its schedule by clicking **Show Autonomous Exadata Infrastructure maintenance schedule**. If the Autonomous Exadata Infrastructure resource doesn't have a customized schedule, its maintenance schedule will be automatically modified so that it precedes the Autonomous Container Database schedule you define.

When finished, click **Save Changes**.

6. Increase how long backups will be retained if necessary; that is, if the Autonomous Databases that will be created in this Autonomous Container Database require backup retention longer than the default 7 days.
   a. Click **Show Advanced Options** and then click **Management**.
   b. Change the **Backup retention policy** value to meet your needs.

7. Click **Create Autonomous Container Database**.

The list of Autonomous Container Databases refreshes to show the new Autonomous Container Database with a status of **Provisioning** until it is available.

---

**View Details of an Autonomous Container Database**

You view the details of an Autonomous Container Database by going to its **Details** page.

1. Go to Autonomous Database in the Oracle Cloud Infrastructure Console.
   For instructions, see **Access Autonomous Database in the Oracle Cloud Infrastructure Console**.

2. In the side menu's list of Autonomous Database resource types, click **Autonomous Container Database**.
The list of Autonomous Container Databases in your current Compartment is displayed.

3. In the side menu’s Compartment list, choose the Compartment containing the Autonomous Container Database whose details you want to view.

The list of Autonomous Container Databases refreshes to show those in the selected Compartment.

4. Click the name of the Autonomous Container Database whose details you want to view.

The Details page for the chosen Autonomous Container Database is displayed.

On this page you can perform a variety of actions.

<table>
<thead>
<tr>
<th>Action</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>View details of the Autonomous Container Database’s Autonomous Exadata Infrastructure resource</td>
<td>On the Autonomous Container Information tab, click the name of the Autonomous Exadata Infrastructure resource in the Autonomous Exadata Infrastructure field.</td>
</tr>
<tr>
<td>Edit the Autonomous Container Database’s backup retention policy</td>
<td>On the Autonomous Container Information tab, click (Edit) in the Backup Retention Policy field. Then, specify how long (as a number of days) backups are to be retained.</td>
</tr>
<tr>
<td>View or copy the Autonomous Container Database’s OCID</td>
<td>On the Autonomous Container Information tab, click Show or Copy in the OCID field.</td>
</tr>
<tr>
<td>Edit the Autonomous Container Database’s maintenance schedule</td>
<td>On the Autonomous Container Information tab, click (Edit) in the Maintenance Schedule field.</td>
</tr>
<tr>
<td>View upcoming and past maintenance</td>
<td>On the Autonomous Container Information tab, click (View) in the Next Maintenance field. A list of upcoming planned maintenance activities, if any, is displayed for both the Autonomous Container Database and the Autonomous Exadata Infrastructure resource containing it. To view past maintenance activities, click Maintenance History in the side menu.</td>
</tr>
<tr>
<td>Terminate the Autonomous Container Database</td>
<td>Click Terminate and follow the instructions in Terminate an Autonomous Container Database.</td>
</tr>
<tr>
<td>Apply tags to the Autonomous Container Database</td>
<td>Click Apply Tag(s).</td>
</tr>
<tr>
<td>View the tags applied to the Autonomous Container Database</td>
<td>Click the Tags tab.</td>
</tr>
</tbody>
</table>

At the bottom of the page is a list of Autonomous Databases in the selected Compartment that use the chosen Autonomous Container Database is displayed. Using this list you can perform a variety of actions.
### Action | Steps
--- | ---
Create an Autonomous Database | Click **Create Autonomous Database** and follow the instructions. *Provision Autonomous Database in Administrator's Guide to Oracle Autonomous Database Dedicated Deployments.*

View details of a listed Autonomous Database | In the list of Autonomous Databases, click the name of the one whose details you want to view.

Copy the OCID of a listed Autonomous Database | In the list of Autonomous Databases, click the menu in the row of the one whose OCID you want to copy and then click **Copy OCID**. The OCID is copied to your clipboard and the menu item changes to **Copied**.

Apply tags to a listed Autonomous Database | In the list of Autonomous Databases, click the menu in the row of the one you want to apply tags to and then click **Apply Tag(s)**.

View the tags applied to a listed Autonomous Database | In the list of Autonomous Databases, click the menu in the row of the one whose tags you want to view and then click **View Tag**.

Terminate a listed Autonomous Database | In the list of Autonomous Databases, click the menu in the row of the one you want to terminate and then click **Terminate**. Then, in the **Terminate Database** dialog:
1. Read the warning about terminating an Autonomous Database.
2. Enter the name of the Autonomous Database.
3. Click **Terminate Database** to begin the termination process.

### Change the Maintenance Schedule of an Autonomous Container Database

You change the maintenance schedule of an Autonomous Container Database from its **Details** page.

1. Go to the **Details** page of the Autonomous Container Database whose maintenance schedule you want to change.
   For instructions, see **View Details of an Autonomous Container Database**.
2. Click the **Edit** link in the **Maintenance Details** field.
3. On the **Edit Automatic Maintenance** card, change settings under **Configure the automatic maintenance schedule** as desired.
   - Select **No preference** to permit Oracle to schedule maintenance as needed based on the maintenance schedule of the Autonomous Exadata Infrastructure resource hosting the Autonomous Container Database.
• Select **Specify a schedule** to restrict when Oracle can schedule maintenance.
  – Specify the permitted months. You must select at least one month per quarter.
  – Specify the week (or weeks) within the selected months.
  – Specify the day (or days) of the selected week.
  – Specify the 4-hour window (or windows) when maintenance operations can begin.

When specifying a schedule, you should ensure that the schedule you define falls after the schedule of Autonomous Exadata Infrastructure resource hosting the Autonomous Container Database. If the Autonomous Exadata Infrastructure resource has a customized schedule, you can view its schedule by clicking Show Autonomous Exadata Infrastructure maintenance schedule. If the Autonomous Exadata Infrastructure resource doesn't have a customized schedule, its maintenance schedule will be automatically modified so that it precedes the Autonomous Container Database schedule you define.

4. When finished, click **Save Changes**.

### Change the Maintenance Type of an Autonomous Container Database

**Note:**

Currently, the Release Update Revision (RUR) maintenance type is not a selectable option. When release update revisions become available for Autonomous Database, this option will become selectable.

You change the maintenance type of an Autonomous Container Database from its **Details** page.

1. Go to the **Details** page of the Autonomous Container Database whose maintenance type you want to change.
   
   For instructions, see [View Details of an Autonomous Container Database](#).

2. Click the **Edit** link in the **Maintenance Details** field.

3. On the **Edit Automatic Maintenance** card, select **Release Update (RU)** or **Release Update Revision (RUR)** from the Maintenance type list.

4. When finished, click **Save Changes**.

### View Scheduled and Past Maintenance of an Autonomous Container Database

You view scheduled and past maintenance of an Autonomous Container Database from its **Details** page.

1. Go to the **Details** page of the desired Autonomous Container Database.
For instructions, see View Details of an Autonomous Container Database.

2. Click the (View) link in the Next maintenance field.

The Autonomous Database Maintenance page lists any upcoming planned maintenance, both for the Autonomous Container Database and the Autonomous Exadata Infrastructure resource that hosts it.

To see a list of past maintenance, click Maintenance History in the side menu.

### Restart an Autonomous Container Database

You restart an Autonomous Container Database by clicking Restart on its Details page.

The restart of an Autonomous Container Database occurs in a rolling fashion, first stopping and starting one of the container database's database instances and then stopping and starting its other database instance. Thus, at no time are the container database or any of the Autonomous Databases created in it unavailable.

1. Go to the Details page of the Autonomous Container Database you want to restart.

For instructions, see View Details of an Autonomous Container Database.

2. Click Restart.

3. In the Restart dialog:
   a. Enter the name of the Autonomous Container Database.
   b. Click Restart to begin the rolling restart operation.

### Move an Autonomous Container Database to a Different Compartment

You can move an Autonomous Container Database to a different Oracle Cloud Infrastructure compartment.

**Note:**

- To move an Autonomous Container Database you must have the right to manage it in its current compartment and in the compartment you are moving it to.
- As soon as you move an Autonomous Container Database to a different compartment, the policies that govern the new compartment apply immediately and affect access to the Autonomous Container Database. Therefore, both your and other Oracle Cloud users' access to it may change, depending on the policies governing the user account's access to resources. For example, a user may lose the ability to create Autonomous Databases in the Autonomous Container Database, given its new compartment.

1. Go to the Details page of the Autonomous Container Database you want to move.
For instructions, see View Details of an Autonomous Container Database.

2. Click **Move Resource**.

3. In the **Move Resource to a Different Compartment** page, select the new compartment.

4. Click **Move Resource**.

**Terminate an Autonomous Container Database**

You terminate an Autonomous Container Database by clicking **Terminate** on its **Details** page.

1. Go to the **Details** page of the Autonomous Container Database you want to terminate.
   
   For instructions, see View Details of an Autonomous Container Database.

2. Click **Terminate**.

3. In the **Terminate Autonomous Container** dialog:
   
   a. Read the warning about terminating an Autonomous Container Database.
   
   b. Enter the name of the Autonomous Container Database.
   
   c. Click **Terminate Autonomous Container** to begin the termination process.

**View a List of Autonomous Container Databases**

You can view a list of all Autonomous Container Databases in a Compartment or of just those in a particular Autonomous Exadata Infrastructure resource.

**View a List of Autonomous Container Databases in a Compartment**

You view a list of all Autonomous Container Databases in a Compartment by going to the **Autonomous Container Databases** page.

1. Go to Autonomous Database in the Oracle Cloud Infrastructure Console.
   
   For instructions, see Access Autonomous Database in the Oracle Cloud Infrastructure Console.

2. In the side menu’s list of Autonomous Database resource types, click **Autonomous Container Database**.

The **Autonomous Container Databases** page is displayed, showing the list of Autonomous Container Databases in your current Compartment. To see the list for a different Compartment, choose its name from the side menu’s **Compartment** list.

On this page you can perform a variety of actions.

<table>
<thead>
<tr>
<th>Action</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create an Autonomous Container Database</td>
<td>Click <strong>Create Autonomous Container Database</strong> and follow the instructions in Create an Autonomous Container Database.</td>
</tr>
<tr>
<td>Action</td>
<td>Steps</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>View details of a listed Autonomous Container Database</td>
<td>In the list of Autonomous Container Databases, click the name of the one whose details you want to view.</td>
</tr>
<tr>
<td>Copy the OCID of a listed Autonomous Container Database</td>
<td>In the list of Autonomous Container Databases, click the menu in the row of the one whose OCID you want to copy and then click <strong>Copy OCID</strong>. The OCID is copied to your clipboard and the menu item changes to <strong>Copied</strong>.</td>
</tr>
<tr>
<td>Apply tags to a listed Autonomous Container Database</td>
<td>In the list of Autonomous Container Databases, click the menu in the row of the one you want to apply tags to and then click <strong>Apply Tag(s)</strong>.</td>
</tr>
<tr>
<td>View the tags applied to a listed Autonomous Container Database</td>
<td>In the list of Autonomous Container Databases, click the menu in the row of the one whose tags you want to view and then click <strong>View Tag</strong>.</td>
</tr>
<tr>
<td>Terminate a listed Autonomous Container Database</td>
<td>In the list of Autonomous Container Databases, click the menu in the row of the one you want to terminate and then click <strong>Terminate</strong>. Then, in the <strong>Terminate Autonomous Container</strong> dialog:</td>
</tr>
<tr>
<td></td>
<td>1. Read the warning about terminating an Autonomous Container Database.</td>
</tr>
<tr>
<td></td>
<td>2. Enter the name of the Autonomous Container Database.</td>
</tr>
<tr>
<td></td>
<td>3. Click <strong>Terminate Autonomous Container</strong> to begin the termination process.</td>
</tr>
</tbody>
</table>

**View a List of Autonomous Container Databases in an Autonomous Exadata Infrastructure Resource**

You view a list of the Autonomous Container Databases in a particular Autonomous Exadata Infrastructure resource by going to that resource’s **Details** page.

1. Go to Autonomous Database in the Oracle Cloud Infrastructure Console.
   For instructions, see Access Autonomous Database in the Oracle Cloud Infrastructure Console.

2. In the side menu’s list of Autonomous Database resource types, click **Autonomous Exadata Infrastructure**.
   The list of Autonomous Exadata Infrastructure resources in your current Compartment is displayed.

3. In the side menu's **Compartment** list, choose the Compartment containing the Autonomous Exadata Infrastructure resource whose Autonomous Container Databases you want to view.
The list of Autonomous Exadata Infrastructure resources refreshes to show those in the selected Compartment.

4. Click the name of the Autonomous Exadata Infrastructure resource whose Autonomous Container Databases you want to view.

The Details page for the chosen Autonomous Exadata Infrastructure resource is displayed, showing at the bottom of the page a list of Autonomous Container Databases in the selected Compartment that use the chosen Autonomous Exadata Infrastructure resource.

Using this list of Autonomous Container Databases you can perform a variety of actions.

<table>
<thead>
<tr>
<th>Action</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create an Autonomous Container Database</td>
<td>Click Create Autonomous Container Database and follow the instructions in Create an Autonomous Container Database.</td>
</tr>
<tr>
<td>View details of a listed Autonomous Container Database</td>
<td>In the list of Autonomous Container Databases, click the name of the one whose details you want to view.</td>
</tr>
<tr>
<td>Copy the OCID of a listed Autonomous Container Database</td>
<td>In the list of Autonomous Container Databases, click the ( ) menu in the row of the one whose OCID you want to copy and then click Copy OCID. The OCID is copied to your clipboard and the menu item changes to Copied.</td>
</tr>
<tr>
<td>Apply tags to a listed Autonomous Container Database</td>
<td>In the list of Autonomous Container Databases, click the ( ) menu in the row of the one you want to apply tags to and then click Apply Tag(s).</td>
</tr>
<tr>
<td>View the tags applied to a listed Autonomous Container Database</td>
<td>In the list of Autonomous Container Databases, click the ( ) menu in the row of the one whose tags you want to view and then click View Tag.</td>
</tr>
</tbody>
</table>
| Terminate a listed Autonomous Container Database | In the list of Autonomous Container Databases, click the \( \) menu in the row of the one you want to terminate and then click Terminate. Then, in the Terminate Autonomous Container dialog:

1. Read the warning about terminating an Autonomous Container Database.
2. Enter the name of the Autonomous Container Database.
3. Click Terminate Autonomous Container to begin the termination process. |
Characteristics of Autonomous Exadata Infrastructure Resources

The following table lists the hardware and Oracle Cloud resource characteristics of Autonomous Exadata Infrastructure resources for the Exadata system models and configurations available in Oracle Autonomous Database.

<table>
<thead>
<tr>
<th>Specification</th>
<th>Exadata X7-2 Quarter Rack</th>
<th>Exadata X7-2 Half Rack</th>
<th>Exadata X7-2 Full Rack</th>
<th>Exadata X8-2 Quarter Rack</th>
<th>Exadata X8-2 Half Rack</th>
<th>Exadata X8-2 Full Rack</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Compute Nodes</td>
<td>2</td>
<td>4</td>
<td>8</td>
<td>2</td>
<td>4</td>
<td>8</td>
</tr>
<tr>
<td>— Total Maximum Number of Enabled CPU Cores</td>
<td>92</td>
<td>184</td>
<td>368</td>
<td>100</td>
<td>200</td>
<td>400</td>
</tr>
<tr>
<td>— Total RAM Capacity</td>
<td>1440 GB</td>
<td>2880 GB</td>
<td>5760 GB</td>
<td>1440 GB</td>
<td>2880 GB</td>
<td>5760 GB</td>
</tr>
<tr>
<td>Number of Exadata Storage Servers</td>
<td>3</td>
<td>6</td>
<td>12</td>
<td>3</td>
<td>6</td>
<td>12</td>
</tr>
<tr>
<td>— Total Raw Flash Storage Capacity</td>
<td>76.8 TB</td>
<td>153.6 TB</td>
<td>307.2 TB</td>
<td>76.8 TB</td>
<td>179.2 TB</td>
<td>358.4 TB</td>
</tr>
<tr>
<td>— Total Raw Disk Storage Capacity</td>
<td>360 TB</td>
<td>720 TB</td>
<td>1440 TB</td>
<td>504 TB</td>
<td>1008 TB</td>
<td>2016 TB</td>
</tr>
<tr>
<td>— Total Usable Storage Capacity</td>
<td>106 TB</td>
<td>212 TB</td>
<td>424 TB</td>
<td>149 TB</td>
<td>299 TB</td>
<td>598 TB</td>
</tr>
<tr>
<td>Maximum SQL Flash Read IOPS</td>
<td>1,194,000</td>
<td>2,388,000</td>
<td>4,776,000</td>
<td>1,194,000</td>
<td>2,388,000</td>
<td>4,776,000</td>
</tr>
<tr>
<td>Maximum SQL Flash Write IOPS</td>
<td>1,088,000</td>
<td>2,176,000</td>
<td>4,352,000</td>
<td>1,088,000</td>
<td>2,176,000</td>
<td>4,352,000</td>
</tr>
<tr>
<td>Maximum Number of Autonomous Container Databases</td>
<td>12 (See note)</td>
<td>12 (See note)</td>
<td>12 (See note)</td>
<td>12 (See note)</td>
<td>12 (See note)</td>
<td>12 (See note)</td>
</tr>
<tr>
<td>Maximum Number of Autonomous Databases per Autonomous Container Database</td>
<td>92 (See note)</td>
<td>184 (See note)</td>
<td>200 (See note)</td>
<td>100 (See note)</td>
<td>200 (See note)</td>
<td>200 (See note)</td>
</tr>
</tbody>
</table>

**Note:**

Oracle Autonomous Database does not currently support over-provisioning, the ability for multiple Autonomous Databases to share a single CPU core. Therefore, an Autonomous Exadata Infrastructure resource can currently support, across all its Autonomous Container Databases, up to as many Autonomous Databases as it has CPU cores. This maximum number will increase when Oracle Autonomous Database supports over-provisioning.
Configuration Example: Network Isolation by Subnet

Use Case

Acme Company has decided to use the dedicated infrastructure feature of Oracle Autonomous Database for its internal project teams and lines of business. The Acme I.T. department will take on the role of fleet administrator, creating and managing all Autonomous Exadata Infrastructure and Autonomous Container Database resources for the company. Each project team or line of business will have users who take on the database administrator role for their organization, creating autonomous databases for their database users (application developers, testers and deployers).

Acme I.T. will allocate resources to the organizations, making sure to provide autonomous container databases that meet the SLAs required by them. Additionally, in order to control the allocation of the resources fairly, Acme I.T. does not want any project team or line of business to have management access to the underlying dedicated infrastructure. Even further, Acme management gets audited by regulators, so it does not want Acme I.T. to be able to access the data that belongs to the different project teams or lines of business; that is, the data they are putting into their application databases.

Two project teams are the first to come on board: Roadrunner and Coyote. Neither the Roadrunner project team nor the Coyote project team wants the other team to be able to access its work in any way.

Resulting Resources Needed

- One VCN to provide network connectivity to all dedicated infrastructure resources. This VCN will connect to the Acme Company VPN using an IPSec VPN, and will have an Internet Gateway resource that blocks all incoming internet traffic. This VCN will be named DatabaseVCN.
- Three private subnets in the VCN to provide network access isolation, one for Autonomous Database resources, and one for each team to use for their client and mid-tier resources. These subnets will be named ITSubnet, RoadrunnerSubnet and CoyoteSubnet.
- Three compartments to provide resource isolation, one for the resources Acme I.T. creates and the private subnet those resources will use, and one each for the Roadrunner teams Coyote teams for its the autonomous databases and private subnet. These compartments will be named AcmeContainerDBs, RoadrunnerDBs and CoyoteDBs.
- Three groups to which users can be assigned, one each for Acme I.T., the Roadrunner team and the Coyote team. These groups will be named AcmeFAs, RoadrunnerDBAs and CoyoteDBAs.
- Three policies to specify user access to the resources in each of the compartments. These policies will be named AcmeContainerDBPolicy, RoadrunnerDBPolicy and CoyoteDBPolicy.
Two autonomous container databases, one that will be patched using RURs (release update revisions) to provide stability and one that will be patched using RUs (release updates) to provide access to the latest Autonomous Database features. These autonomous container databases will be named StableContainerDB and LatestContainerDB.

High-Level Steps

1. The security administrator for Acme Company’s cloud tenancy creates the AcmeContainerDBs, RoadrunnerDBs and CoyoteDBs compartments.
2. The network administrator for Acme Company’s cloud tenancy creates the DatabaseVCN VCN and the ITSubnet subnet in the AcmeContainerDBs compartment, and then creates the RoadrunnerSubnet and CoyoteSubnet subnets in the RoadrunnerDBs and CoyoteDBs compartments, respectively.
3. The security administrator creates the AcmeFAs, RoadrunnerDBAs and CoyoteDBAs groups.
4. The security administrator creates the AcmeContainerDBPolicy, RoadrunnerDBPolicy and CoyoteDBPolicy policies.
5. After the network administrator finishes creating DatabaseVCN and ITSubnet, the security administrator adds the cloud user of a designated Acme I.T. member to the AcmeFAs group.
6. The newly authorized fleet administrator creates an Autonomous Exadata Infrastructure resource in the AcmeContainerDBs compartment, specifying DatabaseVCN and ITSubnet as its VCN and subnet.
7. The fleet administrator creates the StableContainerDB and LatestContainerDB Autonomous Container Database resources in the AcmeContainerDBs compartment, specifying DatabaseVCN and ITSubnet as their VCN and subnet.
8. The security administrator adds designated cloud users to the RoadrunnerDBAs group, thus authorizing them as database administrators for the Roadrunner project team, and then repeats the process for CoyoteDBAs.

Step 1. Create Compartments

In this step, the security administrator for Acme Company’s cloud tenancy creates the AcmeContainerDBs, RoadrunnerDBs and CoyoteDBs compartments.

To perform this step, the security administrator follows the instructions in Managing Compartments in Oracle Cloud Infrastructure Documentation to create a compartment using the Oracle Cloud console. When following these instructions, the security administrator specifies the root compartment of the tenancy as the parent compartment of each of the three compartments.

Step 2. Create the VCN and Subnets

In this step, network administrator for Acme Company’s cloud tenancy creates the DatabaseVCN VCN and the ITSubnet subnet in the AcmeContainerDBs compartment, and then creates the RoadrunnerSubnet and CoyoteSubnet subnets in the RoadrunnerDBs and CoyoteDBs compartments, respectively.

To perform this step, the network administrator first confers with the Acme I.T. department’s networking to reserve a CIDR IP address range that will not conflict with
the company’s on-premises network. (Otherwise, the VCN would conflict with the on-premises network and an IPSec VPN could not be set up.) The reserved range is CIDR 10.0.0.0/16.

Then, the network administrator adapts the instructions in Scenario B: Private Subnets with a VPN in Oracle Cloud Infrastructure Documentation to create the VCN, the Subnets and other network resources using the Oracle Cloud console.

When adapting these instructions, the network administrator manually creates security lists (instead of using the default security lists) to isolate and separate security rules and thus make network management simpler. These security lists are:

- ITSecList: the basic security list for ITSubnet. It is used when the ITSubnet subnet is created.
- RoadrunnerSeclist: the basic security list for RoadrunnerSubnet. It is used when the RoadrunnerSubnet subnet is created.
- RoadrunnerToITSeclist: a security list to permit resources in RoadrunnerSubnet to access Roadrunner team autonomous databases in ITSubnet. Once created, this security list is added to the ITSubnet subnet.
- CoyoteSeclist: the basic security list for CoyoteSubnet. It is used when the CoyoteSubnet subnet is created.
- CoyoteToITSeclist: a security list to permit resources in CoyoteSubnet to access Coyote team autonomous databases in the ITSubnet. Once created, this security list is added to the ITSubnet subnet.

Security Rules in the ITSecList Security List

Here are the ingress rules created in the ITSecList security list.

<table>
<thead>
<tr>
<th>Stateless</th>
<th>Source IP</th>
<th>Protocol</th>
<th>Source Port Range</th>
<th>Destination Port Range</th>
<th>Type and Code</th>
<th>Allows</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>10.0.0.0/24</td>
<td>ICMP</td>
<td>All</td>
<td>All</td>
<td>ICMP traffic for: All</td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>10.0.0.0/24</td>
<td>UDP</td>
<td>All</td>
<td>All</td>
<td>UDP traffic for ports: All</td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>10.0.0.0/24</td>
<td>TCP</td>
<td>All</td>
<td>All</td>
<td>TCP traffic for ports: All</td>
<td></td>
</tr>
</tbody>
</table>

Here is the egress rule created in the ITSecList security list.

<table>
<thead>
<tr>
<th>Stateless</th>
<th>Destination IP</th>
<th>Protocol</th>
<th>Source Port Range</th>
<th>Destination Port Range</th>
<th>Type and Code</th>
<th>Allows</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>0.0.0.0/0</td>
<td>All Protocols</td>
<td>All</td>
<td>All</td>
<td>All traffic for all ports</td>
<td></td>
</tr>
</tbody>
</table>

Security Rules in the RoadrunnerSeclist Security List

Here are the ingress rules created in the RoadrunnerSeclist security list.
Stateless Source IP Protocol Source Port Range Destination Port Range Type and Code Allows
No 0.0.0.0/0 TCP All 22 TCP traffic for ports: 22 SSH Remote Login Protocol
No 0.0.0.0/0 TCP All 80 TCP traffic for ports: 80
No 0.0.0.0/0 TCP All 443 TCP traffic for ports: 443 HTTPS
No 0.0.0.0/0 TCP All 943 TCP traffic for ports: 943
No 0.0.0.0/0 UDP All 1194 UDP traffic for ports: 1194

Here is the egress rule created in the RoadrunnerSeclist security list.

Stateless Destination IP Protocol Source Port Range Destination Port Range Type and Code Allows
No 0.0.0.0/0 All Protocols All All traffic for all ports

Security Rules in the RoadrunnerToITSeclist Security List

Here are the ingress rules created in the RoadrunnerToITSeclist security list. Note that the source CIDR is 10.0.10.0/24, which is the CIDR of RoadrunnerSubnet.

Stateless Source IP Protocol Source Port Range Destination Port Range Type and Code Allows
No 10.0.10.0/24 TCP All 1521 TCP traffic for ports: 1521
No 10.0.10.0/24 TCP All 2484 TCP traffic for ports: 2484
No 10.0.10.0/24 TCP All 443 TCP traffic for ports: 443 HTTPS
No 10.0.10.0/24 TCP All 6200 TCP traffic for ports: 6200

No egress rules are created in the RoadrunnerToITSeclist security list.

Security Rules in the CoyoteSeclist Security List

Note that the CoyoteSeclist security list has the same set of security rules as does RoadrunnerSeclist. While a single security list could be created and used for both project teams, the network administrator has created separate security lists in case one of the project teams requires additional security rules.

Here are the ingress rules created in the CoyoteSeclist security list.
### Stateless Source IP Protocol Source Port Range Destination Port Range Type and Code Allows

<table>
<thead>
<tr>
<th>Stateless</th>
<th>Source IP Address</th>
<th>Protocol</th>
<th>Source Port Range</th>
<th>Destination Port Range</th>
<th>Type and Code</th>
<th>Allows</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>0.0.0.0/0</td>
<td>TCP</td>
<td>All</td>
<td>22</td>
<td>TCP traffic for ports: 22 SSH Remote Login Protocol</td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>0.0.0.0/0</td>
<td>TCP</td>
<td>All</td>
<td>80</td>
<td>TCP traffic for ports: 80</td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>0.0.0.0/0</td>
<td>TCP</td>
<td>All</td>
<td>443</td>
<td>TCP traffic for ports: 443 HTTPS</td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>0.0.0.0/0</td>
<td>TCP</td>
<td>All</td>
<td>943</td>
<td>TCP traffic for ports: 943</td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>0.0.0.0/0</td>
<td>UDP</td>
<td>All</td>
<td>1194</td>
<td>UDP traffic for ports: 1194</td>
<td></td>
</tr>
</tbody>
</table>

Here is the egress rule created in the CoyoteSeclist security list.

<table>
<thead>
<tr>
<th>Stateless</th>
<th>Destination IP Address</th>
<th>Protocol</th>
<th>Source Port Range</th>
<th>Destination Port Range</th>
<th>Type and Code</th>
<th>Allows</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>0.0.0.0/0</td>
<td>All Protocols</td>
<td>All</td>
<td>All</td>
<td>All traffic for all ports</td>
<td></td>
</tr>
</tbody>
</table>

### Security Rules in the CoyoteToITSeclist Security List

Here are the ingress rules created in the CoyoteToITSeclist security list. Note that the source CIDR is 10.0.11.0/24, which is the CIDR of CoyoteSubnet.

<table>
<thead>
<tr>
<th>Stateless</th>
<th>Source IP Address</th>
<th>Protocol</th>
<th>Source Port Range</th>
<th>Destination Port Range</th>
<th>Type and Code</th>
<th>Allows</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>10.0.11.0/24</td>
<td>TCP</td>
<td>All</td>
<td>1521</td>
<td>TCP traffic for ports: 1521</td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>10.0.11.0/24</td>
<td>TCP</td>
<td>All</td>
<td>2484</td>
<td>TCP traffic for ports: 2484</td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>10.0.11.0/24</td>
<td>TCP</td>
<td>All</td>
<td>443</td>
<td>TCP traffic for ports: 443 HTTPS</td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>10.0.11.0/24</td>
<td>TCP</td>
<td>All</td>
<td>6200</td>
<td>TCP traffic for ports: 6200</td>
<td></td>
</tr>
</tbody>
</table>

No egress rules are created in the CoyoteToITSeclist security list.

### Step 3. Create Groups

In this step, the security administrator creates the AcmeFAs, RoadrunnerDBAs and CoyoteDBAs groups.

To perform this step, the security administrator follows the instructions in Managing Groups in *Oracle Cloud Infrastructure Documentation* to create a group using the Oracle Cloud console.
Step 4. Create Policies

In this step, the security administrator creates the AcmeContainerDBPolicy, RoadrunnerDBPolicy and CoyoteDBPolicy policies.

To perform this step, the security administrator follows the instructions in Managing Policies in Oracle Cloud Infrastructure Documentation to create a policy using the Oracle Cloud console.

**Note:**

In addition to creating the required policy statements, in this example the security administrator also creates “USE tag-namespaces” policy statements to permit group members to assign existing tags to the resources they create. To permit group members to create tags as well as use existing tags, the security administrator would instead create “MANAGE tag-namespaces” policy statements.

When following these instructions for the AcmeContainerDBPolicy policy, the security administrator:

1. Sets the Compartment in the side menu to AcmeContainerDBs before clicking Create Policy.
2. Adds these Policy Statements:
   - Allow group AcmeFAs to MANAGE autonomous-exadata-infrastructures in compartment AcmeContainerDBs
   - Allow group AcmeFAs to MANAGE autonomous-container-databases in compartment AcmeContainerDBs
   - Allow group AcmeFAs to USE virtual-network-family in compartment AcmeContainerDBs
   - Allow group AcmeFAs to USE tag-namespaces in tenancy
   - Allow group RoadrunnerDBAs to READ autonomous-container-databases in compartment AcmeContainerDBs
   - Allow group CoyoteDBAs to READ autonomous-container-databases in compartment AcmeContainerDBs

When following these instructions for the RoadrunnerDBPolicy policy, the security administrator:

1. Sets the Compartment in the side menu to RoadrunnerDBs before clicking Create Policy.
2. Adds these Policy Statements:
   - Allow group RoadrunnerDBAs to MANAGE autonomous-databases in compartment RoadrunnerDBs
   - Allow group RoadrunnerDBAs to MANAGE autonomous-backups in compartment RoadrunnerDBs
- Allow group RoadrunnerDBAs to USE virtual-network-family in compartment RoadrunnerDBs
- Allow group RoadrunnerDBAs to MANAGE instance-family in compartment RoadrunnerDBs
- Allow group RoadrunnerDBAs to USE tag-namespaces in tenancy

When following these instructions for the CoyoteDBPolicy policy, the security administrator:

1. Sets the Compartment in the side menu to CoyoteDBs before clicking Create Policy.
2. Adds these Policy Statements:
   - Allow group CoyoteDBAs to MANAGE autonomous-databases in compartment CoyoteDBs
   - Allow group CoyoteDBAs to MANAGE autonomous-backups in compartment CoyoteDBs
   - Allow group CoyoteDBAs to USE virtual-network-family in compartment CoyoteDBs
   - Allow group CoyoteDBAs to MANAGE instance-family in compartment CoyoteDBs
   - Allow group CoyoteDBAs to USE tag-namespaces in tenancy

Step 5. Assign Fleet Administrators

In this step, the security administrator adds the cloud user of a designated Acme I.T. member to the AcmeFAs group.

To perform this step, the security administrator follows the instructions in Managing Users in Oracle Cloud Infrastructure Documentation to add a user to a group using the Oracle Cloud console.

Step 6. Create the Autonomous Exadata Infrastructure Resource

In this step, the fleet administrator follows the instructions in Create an Autonomous Exadata Infrastructure Resource to create an Autonomous Exadata Infrastructure resource in the AcmeContainerDBs compartment, specifying DatabaseVCN and ITSubnet as its VCN and subnet.

Step 7. Create Autonomous Container Database Resources

In this step, the fleet administrator follows the instructions in Create an Autonomous Container Database to create the StableContainerDB and LatestContainerDB Autonomous Container Database resources in the AcmeContainerDBs compartment, specifying DatabaseVCN and ITSubnet as their VCN and subnet. When creating StableContainerDB, the fleet administrator changes the Maintenance Type from its default of Release Update (RU) to Release Update Revision (RUR) and changes the Backup retention policy from its default of 7 Days to 30 Days.
Step 8. Assign Database Administrators

In this step, the security administrator adds designated cloud users to the RoadrunnerDBAs group, thus authorizing them as database administrators for the Roadrunner project team, and then repeats the process for CoyoteDBAs.

To perform this step, for each user the security administrator follows the instructions in Managing Users in Oracle Cloud Infrastructure Documentation to add a user to a group using the Oracle Cloud console.
Notifications Example: Emails for Maintenance Events

This example shows how to use the Events and Notifications services to generate emails when maintenance events occur on Autonomous Exadata Infrastructure and Autonomous Container Database resources. These maintenance events are:

- Maintenance Scheduled for an Autonomous Exadata Infrastructure resource
- Maintenance Reminder for an Autonomous Exadata Infrastructure resource
- Maintenance Begin for an Autonomous Exadata Infrastructure resource
- Maintenance End for an Autonomous Exadata Infrastructure resource
- Maintenance Scheduled for an Autonomous Container Database resource
- Maintenance Reminder for an Autonomous Container Database resource
- Maintenance Begin for an Autonomous Container Database resource
- Maintenance End for an Autonomous Container Database resource

Use Case

The I.T. department for Acme Company would like emails sent to its Fleet Administrators email group (autonomous-fleet-admin-group@acme.example.com) whenever a maintenance event occurs on any of its Autonomous Exadata Infrastructure or Autonomous Container Database resources. All of these resources are created in their AcmeContainerDBs compartment.

High-Level Steps

1. Create a notifications service topic.
2. Add an email subscription to the topic.
3. Add an events service rule to send maintenance events to the notifications service topic.

Note:

The user who performs these steps must have “manage ons-topics” and "manage ons-subscriptions" policies for the compartment in which the topic and subscription are created; for example:

```
allow group AcmeFAs to manage ons-topics in compartment AcmeContainerDBs
allow group AcmeFAs to manage ons-subscriptions in compartment AcmeContainerDBs
```
Step 1. Create a Notifications Topic

An administrator for Acme Company’s cloud tenancy creates the Acme-Autonomous-Maintenance notifications topic in the AcmeContainerDBs compartment.

1. On the Oracle Cloud Infrastructure Home page, click the menu icon in the top corner to display the side menu, hover over Application Integration to expand its submenu, and then select Notifications.

   The list of notifications topics in the root compartment is displayed.

2. In the side menu’s Compartment list, select the AcmeContainerDBs compartment.

   The list of notifications topics refreshes to show those in the AcmeContainerDBs compartment.

3. Click Create Topic to open the Create Topic window.

4. In the Create Topic window, enter Acme-Autonomous-Maintenance in the Name field and then click Create.

   The Create Topic window closes and the list of notifications topics refreshes to show the newly created topic.

For detailed information about creating topics, see Managing Compartments in Oracle Cloud Infrastructure Documentation.

Step 2. Add a Subscription to the Notifications Topic

An administrator for Acme Company’s cloud tenancy adds an email subscription to the Acme-Autonomous-Maintenance notifications topic.

1. Go to the Topic Details page for the Acme-Autonomous-Maintenance notifications topic by clicking its name in the list of notification topics in the AcmeContainerDBs compartment.

2. In the side menu’s Resources list, make sure Subscriptions is selected.

3. Click Create Subscription to open the Create Subscription window.

4. In the Create Subscription window, provide the following information:
   - In the Protocol list, select Email.
   - In the Email field, enter autonomous-fleet-admin-group@acme.example.com.

   When finished, click Create.

   The Create Subscription window closes and the Subscription Details page for the newly created subscription is displayed. Note that it is Pending confirmation.

5. Sign in to an email account that is part of the autonomous-fleet-admin-group group alias. Then, open the email "Oracle Cloud Infrastructure Notifications Service Subscription Confirmation" and confirm the email address.
Step 3. Add an Events Service Rule

An administrator for Acme Company’s cloud tenancy creates the Acme-Autonomous-Maintenance events service rule in the AcmeContainerDBs compartment, specifying maintenance events as the triggering condition and delivery to the Acme-Autonomous-Maintenance notifications topic as the action.

1. On the Oracle Cloud Infrastructure Home page, click the menu icon in the top corner to display the side menu, hover over Application Integration to expand its submenu, and then select Events Service.

2. In the side menu’s Compartment list, select the AcmeContainerDBs compartment.

   The list of rules shows the events service rules in the AcmeContainerDBs compartment.

3. Click Create Rule to open the Create Rule window.

4. In the Create Subscription window, enter Acme-Autonomous-Maintenance in the Display Name field and complete the Rule Conditions and Actions sections as follows:

   • **Rule Conditions**
     
     In the first list, select Event Type as the basis of the condition. Then, in the Service Name list, select Database. Finally, in the Event Type list, select the following event types one at a time:

     – Autonomous Container Database - Maintenance Begin
     – Autonomous Container Database - Maintenance End
     – Autonomous Container Database - Maintenance Reminder
     – Autonomous Container Database - Maintenance Scheduled
     – Autonomous Exadata Infrastructure - Maintenance Begin
     – Autonomous Exadata Infrastructure - Maintenance End
     – Autonomous Exadata Infrastructure - Maintenance Reminder
     – Autonomous Exadata Infrastructure - Maintenance Scheduled

   • **Actions**

     In the Action Type list, select Notifications. Then, in the Notifications Compartment list, select AcmeContainerDBs. Finally, in the Topic list, select Acme-Autonomous-Maintenance.

When finished, click Create Rule.

The Create Subscription window closes and the Details page for the newly created rule is displayed.