Oracle® Enterprise Manager Cloud Control

Administrator's Guide for Oracle Autonomous Databases

13c Release 5
F37177-11
January 2025

ORACLE

Oracle Enterprise Manager Cloud Control Administrator's Guide for Oracle Autonomous Databases, 13c Release 5

F37177-11

Contents

Preface

This guide describes how you can use Oracle Enterprise Manager to discover, manage, and monitor Autonomous Databases.

Topics:

Audience

This guide is intended for Database Administrators (DBAs) who want to use Oracle Enterprise Manager to discover Autonomous Databases. It also provides high-level information on the Oracle Enterprise Manager features for Autonomous Databases.

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.

Accessible Access to Oracle Support

Oracle customers who 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 Resources

Here are links to related resources:

- For information on how to use Oracle Enterprise Manager for Oracle Databases, database concepts and features, see Oracle Database Documentation.
- For information on Oracle Cloud Infrastructure and Autonomous Databases, see:
  - Oracle Cloud Infrastructure Documentation
  - Autonomous Data Warehouse Documentation
  - Autonomous Transaction Processing Documentation
- For information on Oracle Enterprise Manager, see Oracle Enterprise Manager Documentation.

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

1

Use Oracle Enterprise Manager for Autonomous Databases

You can use Oracle Enterprise Manager to discover, manage, and monitor your Autonomous Databases.

Oracle Enterprise Manager supports the following Autonomous Databases and the term "Autonomous Databases" in this guide collectively refers to them:

- Autonomous Data Warehouse – Dedicated
- Autonomous Transaction Processing – Dedicated
- Autonomous Data Warehouse – Serverless
- Autonomous Transaction Processing – Serverless

Oracle Enterprise Manager is deployed either on Oracle Cloud Infrastructure or on-premises, and using it you can:

- Discover Autonomous Databases.
- Monitor the health and performance of Autonomous Databases and perform deep diagnostics on the Performance Hub.
- Perform database administration tasks such as storage management, and schema management tasks such as creating database objects.

Separate licensing is not required to use Oracle Enterprise Manager for Autonomous Databases. All the supported Oracle Enterprise Manager features for Oracle Databases are bundled with the Autonomous Database.

For information on:

- Oracle Enterprise Manager features for Autonomous Databases, see Monitoring and Administration Tasks.
- Oracle Database Features in Dedicated Autonomous Database Deployments, see Oracle Database Features in Autonomous Database on Dedicated Exadata Infrastructure in *Oracle Autonomous Database on Dedicated Exadata Infrastructure*.
- Oracle Database features in Autonomous Database – Serverless, see Autonomous Database for Experienced Oracle Database Users in *Using Oracle Autonomous Database Serverless*.

Topics:

About Autonomous Databases

Autonomous Databases are fully managed, preconfigured database environments that are created in Oracle Cloud Infrastructure.

Autonomous Databases are cloud databases that deliver end-to-end automation of tasks that are traditionally performed by DBAs, such as provisioning the database and monitoring security, availability, and performance. Using Autonomous Databases, you do not have to configure or manage any hardware, or install any software. After creating an Autonomous Database, you can scale the number of CPU cores or the storage capacity of the database at any time without impacting availability or performance.

Autonomous Databases are of the following types:

- **Autonomous Data Warehouse**, which provides an easy-to-use, fully autonomous data warehouse that scales elastically, delivers fast query performance and requires no database administration. It is designed to support all standard SQL and business intelligence (BI) tools, and provides all of the performance of the Oracle Database in an environment that is tuned and optimized for data warehouse workloads. For more information, see Autonomous Data Warehouse.
- **Autonomous Transaction Processing**, which is designed to support all standard business applications and delivers scalable query performance. Autonomous Transaction Processing provides all of the performance of the Oracle Database in an environment that is tuned and optimized for transaction processing workloads. For more information, see Autonomous Transaction Processing.

When you create an Autonomous Database, you have the following deployment options:

- **Dedicated Exadata Infrastructure**, which is a private database cloud in the public cloud. A completely dedicated compute, storage, network and database service for only a single tenant. Dedicated infrastructure provides for the highest levels of security isolation and governance.
- **Serverless**, which is an easy-to-use option that scales elastically and delivers fast query performance. Oracle autonomously operates all aspects of the database life cycle from database placement to backup and updates.

Most tasks related to Autonomous Databases are automated, however, you have to monitor, diagnose, and perform basic application-level administrative tasks. Here's where you can use Oracle Enterprise Manager and ensure:

- Alert-driven monitoring for visibility into availability and key metrics.
- In-depth application performance diagnostics and troubleshooting.
- Insight-driven utilization analysis built on aggregated monitoring, based on historical data.

About User Accounts

You must have certain Administrator accounts to use Oracle Enterprise Manager for Autonomous Databases.

The following table lists the Oracle Enterprise Manager Administrator accounts and the Autonomous Database-related tasks users assigned these can perform. For information on how to create administrators in Oracle Enterprise Manager, see Creating a New Administrator in *Oracle Enterprise Manager Cloud Control Security Guide*.

Administrator Account	Tasks
Super Administrator (`sysman`)	This is the Oracle Enterprise Manager Super Administrator and is created by default when Oracle Enterprise Manager is deployed. Specific to Autonomous Databases, the Super Administrator can: • Create Oracle Enterprise Database Administrator user accounts. • Grant privileges to manage Autonomous Databases.

Administrator Account	Tasks
Database Administrator	The Database Administrator is created and assigned by the Super Administrator, and has full access to the database and can perform any operation on the database. Specific to Autonomous Databases, the Database Administrator can: • Discover or delete Autonomous Databases. • Monitor Autonomous Databases. See Creating a Database Administrator Account in *Oracle Enterprise Manager Cloud Control Security Guide*.

Other than the two Oracle Enterprise Manager administrator accounts, you must also have the user accounts listed in the following table, which are created when the Autonomous Database is created.

User Account	Tasks
Database Admin User (`Admin`)	This is the super user for the Autonomous Database and is required for real-time database management. **Note**: The `Admin` user can also perform monitoring tasks, however, it is recommended that the Monitoring User (`adbsnmp`) account is used for monitoring.
Monitoring User (`adbsnmp`)	This user is created out-of-the-box when the Autonomous Database is created in Oracle Cloud Infrastructure. This account is locked by default and you can reset the password and unlock it using Oracle Enterprise Manager or any SQL client. The `adbsnmp` user can: • Discover the Autonomous Database in Oracle Enterprise Manager. • Collect Autonomous Database metrics. • View the data on the Performance Overview page. **Note:** The `adbsnmp` user account should have the following privileges to use Oracle Enterprise Manager for Autonomous Databases: • `grant connect to adbsnmp;` • `grant select_CATALOG_ROLE to adbsnmp;` • `grant select any dictionary to adbsnmp;` The `adbsnmp` user account is locked by default and you must unlock it using `alter user adbsnmp account unlock;`.

2

Discover Autonomous Databases

Autonomous Databases are created in Oracle Cloud Infrastructure and then discovered in Oracle Enterprise Manager for monitoring.

You can discover Autonomous Databases using Oracle Enterprise Manager deployed on Oracle Cloud Infrastructure or on premises. This chapter provides the prerequisite tasks, and the procedures to discover Autonomous Databases in Oracle Enterprise Manager using:

- Oracle Enterprise Manager Console
- EM CLI
- REST API

Topics:

Perform Prerequisite Tasks

You must perform certain prerequisite tasks to set up Oracle Enterprise Manager to work with Oracle Cloud Infrastructure and discover Autonomous Databases.

You can discover Autonomous Databases from Oracle Enterprise Manager deployed on Oracle Cloud Infrastructure or on premises. The prerequisite tasks that must be performed for each deployment scenario differ for Autonomous Databases – Dedicated and Autonomous Databases – Serverless, and depending on which Autonomous Database you want to discover, you must follow the instructions given in one of the following sections.

Topics:

Prerequisite Tasks for Autonomous Databases – Dedicated

To discover Autonomous Data Warehouse – Dedicated and Autonomous Transaction Processing – Dedicated in Oracle Enterprise Manager deployed on Oracle Cloud Infrastructure or on premises, you must first perform the prerequisite tasks listed in these sections:

Oracle Enterprise Manager Deployed on Oracle Cloud Infrastructure

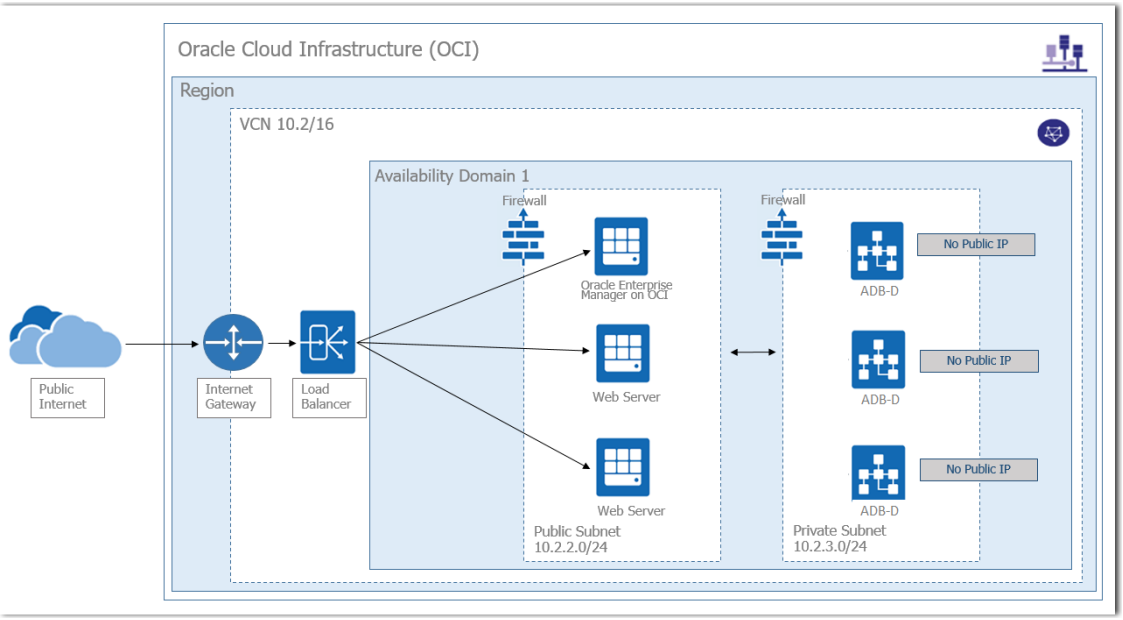
You can use Oracle Enterprise Manager deployed on Oracle Cloud Infrastructure and discover Autonomous Databases – Dedicated.

Before you discover Autonomous Databases – Dedicated, you must ensure that you have performed the following tasks:

- **Create an Autonomous Database – Dedicated in Oracle Cloud Infrastructure.** After you create the database, you must download the OCI Client Credential (Wallet) and save the `.zip` file to provide client access to the Autonomous Database – Dedicated.
  For information, see Create an Autonomous Database on Dedicated Exadata Infrastructure and Download Client Credentials in *Oracle Autonomous Database on Dedicated Exadata Infrastructure*.
- **Configure and deploy Oracle Enterprise Manager on Oracle Cloud Infrastructure.** Oracle Enterprise Manager should be deployed in a Public or Private subnet in the same VCN as the Autonomous Database – Dedicated.
  The Enterprise Manager Oracle Management Service (OMS) includes a central Oracle Management Agent to discover Autonomous Databases, which are treated as non-host targets. The central agent is installed by default on the OMS host and must have SQL*Net access to the Autonomous Database – Dedicated. Although, it is recommended that you use the central agent, you also have the option of using any other agent that is deployed on an existing Oracle Cloud Infrastructure Database system.

  For information, see the Setting Up Oracle Enterprise Manager on Oracle Cloud Infrastructure tutorial.
- **Review and use the specified connectivity option to connect Oracle Enterprise Manager on Oracle Cloud Infrastructure with the Autonomous Database – Dedicated.** The network path to an Autonomous Database – Dedicated is through a Virtual Cloud Network (VCN) and subnet defined by the dedicated infrastructure hosting the database. Usually, the subnet is defined as Private, meaning that there is no Public Internet access to the database. Private IP addresses are used to connect Oracle Enterprise Manager with the Autonomous Database – Dedicated in the VCN.
  For information, see:
  - Connect to Autonomous Database on Dedicated Exadata Infrastructure in *Oracle Autonomous Database on Dedicated Exadata Infrastructure*.
  - Private IP Addresses in Oracle Cloud Infrastructure documentation.

The following diagram provides an overview of how Oracle Enterprise Manager deployed on Oracle Cloud Infrastructure connects with Autonomous Databases – Dedicated.



In the diagram:

- Oracle Enterprise Manager is deployed using a Marketplace image in a Public subnet in a VCN.
  Note that in the diagram, the other Web Servers in the Public subnet are not a part of the Oracle Enterprise Manager deployment, but a part of a sample scenario that depicts a typical Oracle Cloud Infrastructure application deployment that connects with Autonomous Databases – Dedicated.
- Autonomous Databases – Dedicated are created in a Private subnet in the same VCN.
- Oracle Enterprise Manager connects with Autonomous Databases – Dedicated using a Private IP address.

Other Prerequisite Tasks

After the major components are in place, you must perform the following prerequisite tasks to discover an Autonomous Database – Dedicated.

1. Create an Oracle Cloud Infrastructure Identity and Access Management (IAM) group named **EMGroup**, and add the DBA who will be managing and monitoring the Autonomous Database – Dedicated using Oracle Enterprise Manager to this group. Note that this DBA user must have an account in Oracle Cloud Infrastructure.
   See To create a group in Oracle Cloud Infrastructure documentation.
2. Create the following policies to allow the DBA in **EMGroup** to manage and monitor the Autonomous Database – Dedicated using Oracle Enterprise Manager.

```
Allow group EMGroup to manage autonomous-database in compartment <compartment
in which the Autonomous Database resides>

Allow group EMGroup to manage orm-stacks in compartment <compartment in which
the Oracle Enterprise Manager stack resides>

Allow group EMGroup to manage instance-family in compartment <compartment in
which the Oracle Enterprise Manager stack resides>

Allow group EMGroup to manage volume-family in compartment <compartment in
which the Oracle Enterprise Manager stack resides>
```

```
Allow group EMGroup to manage load-balancers in compartment <compartment in
which the Oracle Enterprise Manager stack resides>

Allow group EMGroup to manage virtual-network-family in compartment
<compartment in which the Oracle Enterprise Manager stack resides>

Allow group EMGroup to manage file-family in compartment <compartment in which
the Oracle Enterprise Manager stack resides>

Allow group EMGroup to manage autonomous-database-family in compartment
<compartment in which the Oracle Enterprise Manager stack resides>

Allow group EMGroup to manage orm-jobs in compartment <compartment in which
the Oracle Enterprise Manager stack resides>

Allow group EMGroup to read resource-availability in compartment <compartment
in which the Autonomous Database resides> and <compartment in which the Oracle
Enterprise Manager stack resides>

Allow group EMGroup to read limits in compartment <compartment in which the
Autonomous Database resides> and <compartment in which the Oracle Enterprise
Manager stack resides>
```

> **Note:**
>
> For the last two policies listed above, to grant read access to `resource-availability` and `limits`, you must use separate statements for each compartment.

See To create a policy in Oracle Cloud Infrastructure documentation.

3. Create a security list and add the following ingress rules to ensure secure access:
   - Rule for accessing Oracle Enterprise Manager from the public network, allow Transmission Control Protocol (TCP) traffic for port `7803`.
   - Rule for accessing Autonomous Database – Dedicated from Oracle Enterprise Manager subnet and VCN, allow TCP/TCPS traffic for the port value specified in the `tnsnames.ora` file in the OCI Client Credential (Wallet).

   For information, see:
   - Security Lists in Oracle Cloud Infrastructure documentation.
   - Connect to Autonomous Database on Dedicated Exadata Infrastructure in *Oracle Autonomous Database on Dedicated Exadata Infrastructure*.
4. Unlock the `adbsnmp` user, which is created out-of-the-box when the Autonomous Database – Dedicated is created in Oracle Cloud Infrastructure. This account is locked by default and you can reset the password and unlock it using Oracle Enterprise Manager or a SQL client.

Oracle Enterprise Manager Deployed On Premises

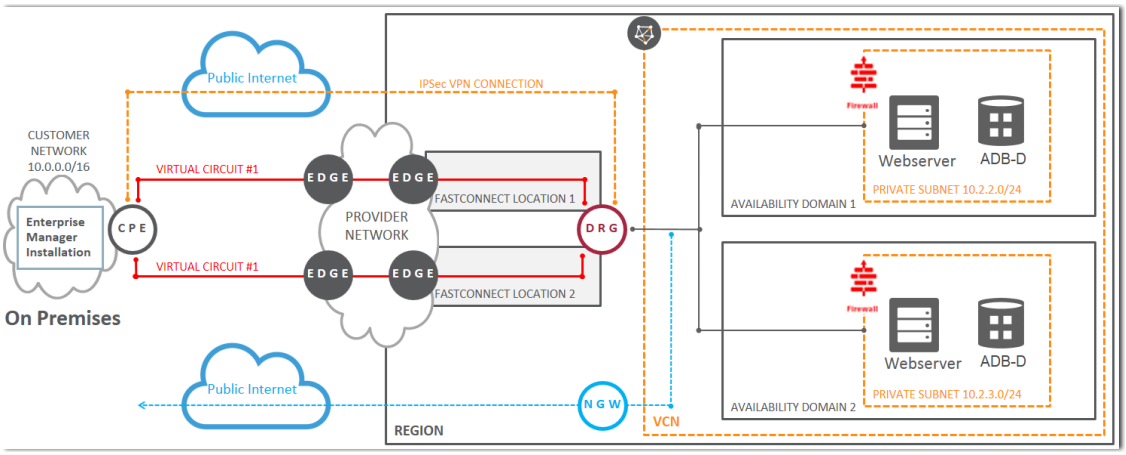
You can use Oracle Enterprise Manager deployed on premises to discover Autonomous Databases – Dedicated, including Autonomous Databases – Dedicated on Oracle Exadata Cloud at Customer.

Before you discover Autonomous Databases – Dedicated, you must ensure that you have performed the following tasks:

- **Create an Autonomous Database – Dedicated in Oracle Cloud Infrastructure.** After you create the database, you must download the OCI Client Credential (Wallet) and save the `.zip` file to provide client access to the Autonomous Database – Dedicated.
  For information, see Create an Autonomous Database on Dedicated Exadata Infrastructure and Download Client Credentials in *Oracle Autonomous Database on Dedicated Exadata Infrastructure*.
- **Deploy Oracle Enterprise Manager in your on-premises network.** The OMS includes a central Oracle Management Agent that can be used to discover Autonomous Databases, which are treated as non-host targets. The central agent is installed by default on the OMS host and must have SQL*Net access to the Autonomous Database – Dedicated. Note that if you have an existing on-premises database or an Oracle Cloud Infrastructure Database system in the same VCN where the Autonomous Database – Dedicated resides, you have the option of using the agent that monitors them, instead of the central agent.
  For information, see:
  - Upgrading the Enterprise Manager Cloud Control 13c Release 5 Software Only with Plug-ins in *Oracle Enterprise Manager Cloud Control Upgrade Guide*.
  - Overview of the Directories Created for an Enterprise Manager System in *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.
- **Review and use the specified connectivity options to connect Oracle Enterprise Manager deployed on premises with the Autonomous Database – Dedicated.** Oracle Enterprise Manager on premises connects with the Autonomous Database – Dedicated using a Private IP address, and you can use one of the following options to connect Oracle Enterprise Manager deployed in your on-premises network to the Autonomous Database – Dedicated in your VCN.
  - Site-to-Site VPN, which is an Internet Protocol Security (IPSec) VPN. IPSec VPN provides standards-based IPSec encryption over public internet. See Site-to-Site VPN in Oracle Cloud Infrastructure documentation.
  - FastConnect, which provides an easy way to create a dedicated, private connection between the on-premises network and the VCN in Oracle Cloud Infrastructure. See FastConnect in Oracle Cloud Infrastructure documentation.

  Note that you do not have host access to the Autonomous Database – Dedicated in Oracle Cloud Infrastructure. If required, web server instances in the Private subnet can initiate connections to the internet by way of a NAT gateway. See NAT Gateway in Oracle Cloud Infrastructure documentation.

The following diagram provides an overview of how Oracle Enterprise Manager deployed on premises connects and interacts with Autonomous Databases – Dedicated in Oracle Cloud Infrastructure.



In the diagram:

- Oracle Enterprise Manager is deployed in an on-premises network.
- The Autonomous Databases – Dedicated are created in Private subnets in a VCN in Oracle Cloud Infrastructure.
- The two connectivity options, Site-to-Site VPN and FastConnect, are displayed to demonstrate how Oracle Enterprise Manager deployed on premises connects with the Autonomous Database – Dedicated using these options.

Other Prerequisite Tasks

After the major components are in place, you must perform the following prerequisite tasks to discover an Autonomous Database – Dedicated.

1. Create an Oracle Cloud Infrastructure IAM group named **EMGroup**, and add the DBA who will be managing and monitoring the Autonomous Database – Dedicated using Oracle Enterprise Manager to this group. Note that this DBA user must have an account in Oracle Cloud Infrastructure.
   See To create a group in Oracle Cloud Infrastructure documentation.
2. Create the following policy to allow the DBA in **EMGroup** to manage and monitor the Autonomous Database – Dedicated using Oracle Enterprise Manager:
   ```
   Allow group EMGroup to manage autonomous-database in compartment <compartment in which the Autonomous Database resides>
   ```
   See To create a policy in Oracle Cloud Infrastructure documentation.
3. Create a security list and add the following ingress rule to ensure secure access:
   Rule for accessing Autonomous Database – Dedicated in the Oracle Cloud Infrastructure VCN from Oracle Enterprise Manager deployed on premises, allow TCP/TCPS traffic for the port value specified in the `tnsnames.ora` file in the OCI Client Credential (Wallet).

   For information, see:

   - Security Lists in Oracle Cloud Infrastructure documentation.
   - Connect to Autonomous Database on Dedicated Exadata Infrastructure in *Oracle Autonomous Database on Dedicated Exadata Infrastructure*.
4. Unlock the `adbsnmp` user, which is created out-of-the-box when the Autonomous Database – Dedicated is created in Oracle Cloud Infrastructure. This account is locked by default and you can reset the password and unlock it using Oracle Enterprise Manager or a SQL client.

Prerequisite Tasks for Autonomous Databases – Serverless

To discover Autonomous Data Warehouse – Serverless and Autonomous Transaction Processing – Serverless in Oracle Enterprise Manager deployed on Oracle Cloud Infrastructure or on premises, you must first perform the prerequisite tasks listed in these sections:

- Oracle Enterprise Manager Deployed on Oracle Cloud Infrastructure
- Oracle Enterprise Manager Deployed On Premises

Oracle Enterprise Manager Deployed on Oracle Cloud Infrastructure

You can use Oracle Enterprise Manager deployed on Oracle Cloud Infrastructure and discover Autonomous Databases – Serverless.

Oracle Enterprise Manager deployed on Oracle Cloud Infrastructure can access Autonomous Databases – Serverless with Private Endpoints or with Public Endpoints using a Service Gateway. The following sections provide information on both scenarios, however, it is recommended that you configure Private Endpoints to access Autonomous Databases – Serverless.

Access Autonomous Database – Serverless Using a Private Endpoint

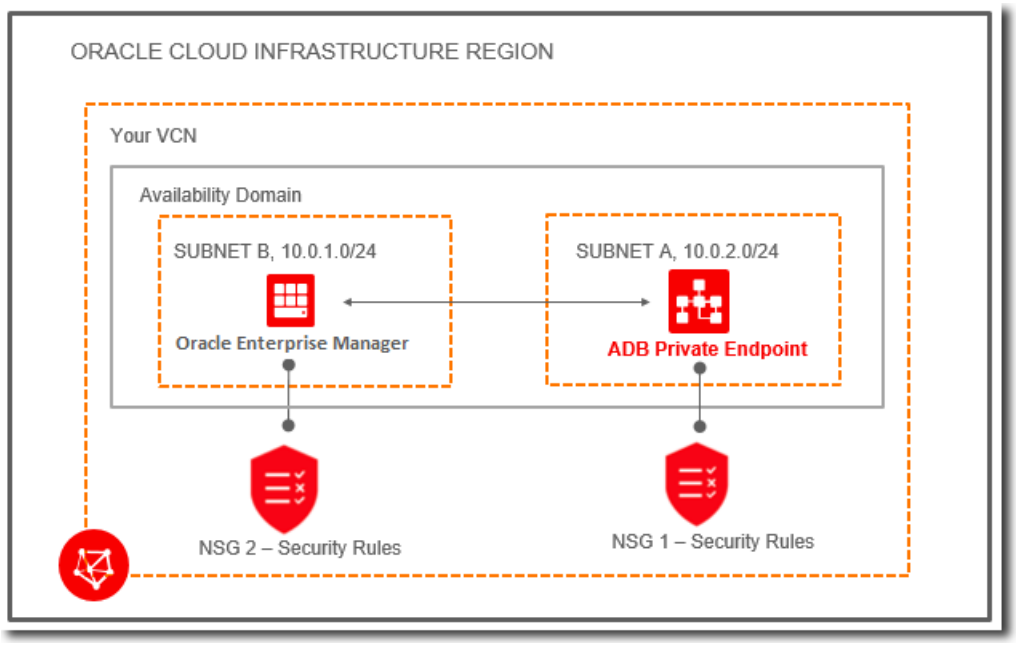
This section walks you through a scenario in which you enable private access from your Oracle Enterprise Manager deployed on Oracle Cloud Infrastructure to the Autonomous Database – Serverless in Oracle Services Network using a *private endpoint*. For information on Autonomous Databases – Serverless and private endpoints, see Configure Network Access with Private Endpoints in *Using Oracle Autonomous Database Serverless*.

- **Provision an Autonomous Database – Serverless with a Private Endpoint.** A private endpoint is a private IP address within your VCN that you can use to access the Autonomous Database – Serverless within Oracle Cloud Infrastructure. When you enable a private endpoint for an Autonomous Database – Serverless, the only access path to the database is through a VCN inside your Oracle Cloud Infrastructure tenancy. This is required for you to securely connect to the Autonomous Database – Serverless from Oracle Enterprise Manager. You can configure a private endpoint when you provision or clone an Autonomous Database – Serverless.
  For information, see Configure Private Endpoints When You Provision or Clone an Instance in *Using Oracle Autonomous Database Serverless*.
- **Download the Client Credentials (Wallet).** After you provision the database, you must download the OCI Client Credential (Wallet) and save the `.zip` file to provide client access to the Autonomous Database – Serverless.
  For information, see Download Client Credentials (Wallets) in *Using Oracle Autonomous Database Serverless*.
- **Configure and deploy Oracle Enterprise Manager on Oracle Cloud Infrastructure.** Oracle Enterprise Manager should be deployed using a marketplace image in a Public or Private subnet in the same VCN as the Autonomous Database – Serverless that was configured with private endpoints.
  The OMS includes a central Oracle Management Agent to discover Autonomous Databases, which are treated as non-host targets. The central agent is installed by default on the OMS host and must have SQL*Net access to the Autonomous Database – Serverless. Although, it is recommended that you use the central agent, you also have the option of using any other agent that is deployed on an existing Oracle Cloud Infrastructure Database system.

For information, see the Setting Up Oracle Enterprise Manager on Oracle Cloud Infrastructure tutorial.

- **Review and use the specified connectivity option to connect Oracle Enterprise Manager on Oracle Cloud Infrastructure with the Autonomous Database – Serverless.** With a private endpoint, database traffic remains private and within Oracle Cloud Infrastructure, thereby ensuring network security.
  For information on connecting from Oracle Enterprise Manager deployed on Oracle Cloud Infrastructure to an Autonomous Database – Serverless, see Example: Connecting from Inside Oracle Cloud Infrastructure VCN in *Using Oracle Autonomous Database Serverless*.

  The following diagram provides an overview of how Oracle Enterprise Manager deployed on Oracle Cloud Infrastructure connects with Autonomous Databases – Serverless using a private endpoint.



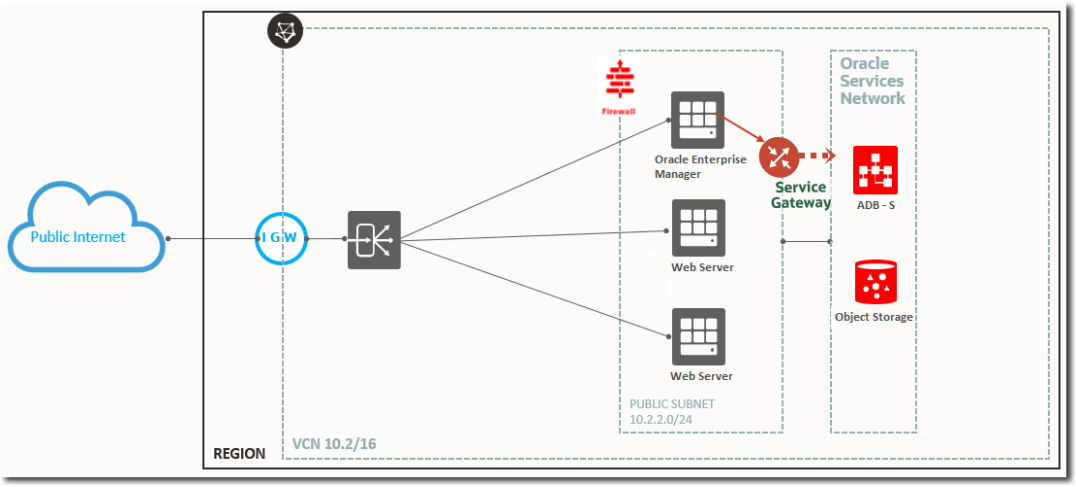
Access Autonomous Database – Serverless Using the Service Gateway

This section walks you through a scenario in which you enable access from your Oracle Enterprise Manager deployed on Oracle Cloud Infrastructure to the Autonomous Database – Serverless in the Oracle Services Network by using the *service gateway*. This method should only be used when the Autonomous Database – Serverless is not configured with a private endpoint. For information on Oracle Services Network and the Service Gateway, see Access to Oracle Services: Service Gateway in Oracle Cloud Infrastructure documentation.

- **Provision an Autonomous Database – Serverless.** As a first step, you must ensure that you have provisioned the Autonomous Database – Serverless.
  For information, see Provision an Autonomous Database Instance in *Using Oracle Autonomous Database Serverless*.
- **Download the Client Credentials (Wallet).** After you provision the database, you must download the OCI Client Credential (Wallet) and save the `.zip` file to provide client access to the Autonomous Database – Serverless.
  For information, see Download Client Credentials (Wallets) in *Using Oracle Autonomous Database Serverless*.

- **Configure and deploy Oracle Enterprise Manager on Oracle Cloud Infrastructure.** Oracle Enterprise Manager should be deployed in a Public or Private subnet in the same VCN as the Autonomous Database – Serverless.
  The OMS includes a central Oracle Management Agent to discover Autonomous Databases, which are treated as non-host targets. The central agent is installed by default on the OMS host and must have SQL*Net access to the Autonomous Database – Serverless. Although, it is recommended that you use the central agent, you also have the option of using any other agent that is deployed on an existing Oracle Cloud Infrastructure Database system.

  For information, see the Setting Up Oracle Enterprise Manager on Oracle Cloud Infrastructure tutorial.
- **Create a Service Gateway.** You must create a service gateway as a resource in the VCN. This will enable the Oracle Enterprise Manager Deployed on Oracle Cloud Infrastructure in your VCN to privately access Autonomous Database – Serverless in the Oracle Services Network, without exposing the data to the public internet.
  For information, see **Task 1 Create the service gateway** in Setting Up a Service Gateway in the Console in Oracle Cloud Infrastructure documentation.
- **Review and use the specified connectivity option to connect Oracle Enterprise Manager on Oracle Cloud Infrastructure with the Autonomous Database – Serverless.** The next step is to ensure that the subnet in which Oracle Enterprise Manager resides in your VCN has access to the service gateway. To do so, you must add a route rule in the private subnet's route table. To do so, follow the instructions given in **Task 2: Update routing for the subnet** in Setting Up a Service Gateway in the Console in Oracle Cloud Infrastructure documentation, and choose **Service Gateway** as the **Target Type** and the service CIDR label **All <region> Services in Oracle Services Network** as the **Destination Service**. The service gateway now provides access to the Autonomous Databases – Serverless within the region in Oracle Services Network.
  The following diagram provides an overview of how Oracle Enterprise Manager deployed on Oracle Cloud Infrastructure connects with Autonomous Databases – Serverless using a service gateway.



Other Prerequisite Tasks

After you have ensured that the major components are in place using one of the two options given above, you must perform the following prerequisite tasks to discover an Autonomous Database – Serverless for Oracle Enterprise Manager deployed on Oracle Cloud Infrastructure.

1. Create an Oracle Cloud Infrastructure IAM group named **EMGroup**, and add the DBA who will be managing and monitoring the Autonomous Database – Serverless using Oracle Enterprise Manager to this group. Note that this DBA user must have an account in Oracle Cloud Infrastructure.
   See To create a group in Oracle Cloud Infrastructure documentation.
2. Create the following policies to allow the DBA in **EMGroup** to manage and monitor the Autonomous Database – Dedicated using Oracle Enterprise Manager.

```
Allow group EMGroup to manage autonomous-database in compartment <compartment
in which the Autonomous Database resides>

Allow group EMGroup to manage orm-stacks in compartment <compartment in which
the Oracle Enterprise Manager stack resides>

Allow group EMGroup to manage instance-family in compartment <compartment in
which the Oracle Enterprise Manager stack resides>

Allow group EMGroup to manage volume-family in compartment <compartment in
which the Oracle Enterprise Manager stack resides>

Allow group EMGroup to manage load-balancers in compartment <compartment in
which the Oracle Enterprise Manager stack resides>

Allow group EMGroup to manage virtual-network-family in compartment
<compartment in which the Oracle Enterprise Manager stack resides>

Allow group EMGroup to manage file-family in compartment <compartment in which
the Oracle Enterprise Manager stack resides>

Allow group EMGroup to manage autonomous-database-family in compartment
<compartment in which the Oracle Enterprise Manager stack resides>

Allow group EMGroup to manage orm-jobs in compartment <compartment in which
the Oracle Enterprise Manager stack resides>

Allow group EMGroup to read resource-availability in compartment <compartment
in which the Autonomous Database resides> and <compartment in which the Oracle
Enterprise Manager stack resides>

Allow group EMGroup to read limits in compartment <compartment in which the
Autonomous Database resides> and <compartment in which the Oracle Enterprise
Manager stack resides>
```

   > **Note:**
   >
   > For the last two policies listed above, to grant read access to `resource-availability` and `limits`, you must use separate statements for each compartment.

   See To create a policy in Oracle Cloud Infrastructure documentation.
3. Create a security list and add the following ingress rules to ensure secure access:
   - Rule for accessing Oracle Enterprise Manager from the public network, allow Transmission Control Protocol (TCP) traffic for port `7803`.
   - Rule for accessing Autonomous Database – Serverless from Oracle Enterprise Manager subnet and VCN, allow TCPS traffic for the port value specified in the `tnsnames.ora` file in the OCI Client Credential (Wallet).

   For information, see:

- Security Lists in Oracle Cloud Infrastructure documentation.
- About Connecting to an Autonomous Database Instance in *Using Oracle Autonomous Database Serverless*.

4. Unlock the `adbsnmp` user, which is created out-of-the-box when the Autonomous Database – Serverless is created in Oracle Cloud Infrastructure. This account is locked by default and you can reset the password and unlock it using Oracle Enterprise Manager or a SQL client.

Oracle Enterprise Manager Deployed On Premises

You can use Oracle Enterprise Manager deployed on premises to discover Autonomous Databases – Serverless.

Oracle Enterprise Manager deployed on premises can access Autonomous Databases – Serverless with Private Endpoints or using Transit Routing using a Service Gateway. The following sections provide information on both scenarios, however, it is recommended that you configure Private Endpoints to access Autonomous Databases – Serverless.

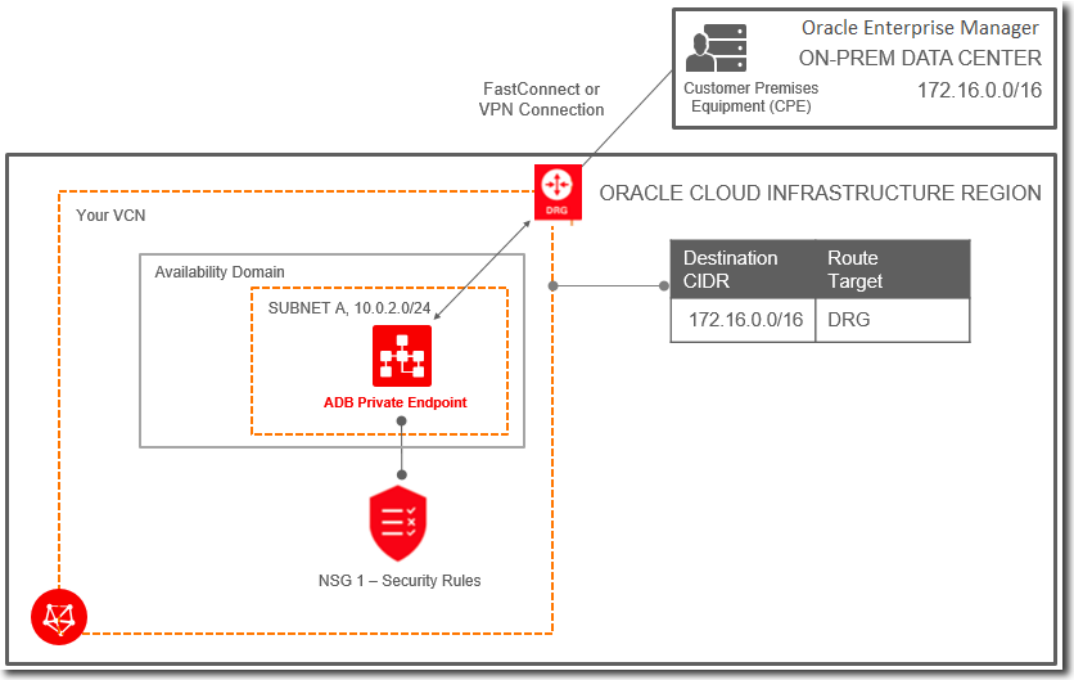
Access Autonomous Database – Serverless Using a Private Endpoint

This section walks you through a scenario in which you enable private access from your Oracle Enterprise Manager deployed on premises to the Autonomous Database – Serverless in Oracle Services Network using a *private endpoint*. For information on Autonomous Databases – Serverless and private endpoints, see Configure Network Access with Private Endpoints in *Using Oracle Autonomous Database Serverless*.

- **Provision an Autonomous Database – Serverless with a Private Endpoint.** A private endpoint is a private IP address within your VCN that you can use to access Autonomous Database – Serverless within Oracle Cloud Infrastructure. When you enable a private endpoint for an Autonomous Database – Serverless, the only access path to the database is through a VCN inside your Oracle Cloud Infrastructure tenancy. This is required for you to securely connect to the Autonomous Database – Serverless from Oracle Enterprise Manager. You can configure a private endpoint when you provision or clone an Autonomous Database – Serverless.
  For information, see Configure Private Endpoints When You Provision or Clone an Instance in *Using Oracle Autonomous Database Serverless*.
- **Download the Client Credentials (Wallet).** After you provision the database, you must download the OCI Client Credential (Wallet) and save the `.zip` file to provide client access to the Autonomous Database – Serverless.
  For information, see Download Client Credentials (Wallets) in *Using Oracle Autonomous Database Serverless*.
- **Deploy Oracle Enterprise Manager in your on-premises network.** The OMS includes a central Oracle Management Agent that can be used to discover Autonomous Databases, which are treated as non-host targets. The central agent is installed by default on the OMS host and must have SQL*Net access to the Autonomous Database – Serverless. Note that if you have an existing on-premises database or an Oracle Cloud Infrastructure Database system in the same VCN where the Autonomous Database – Serverless resides, you have the option of using the agent that monitors them, instead of the central agent.
  For information, see:
  - Upgrading the Enterprise Manager Cloud Control 13c Release 5 Software Only with Plug-ins in *Oracle Enterprise Manager Cloud Control Upgrade Guide*.
  - Overview of the Directories Created for an Enterprise Manager System in *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.

- **Review and use the specified connectivity option to connect Oracle Enterprise Manager on premises with the Autonomous Database – Serverless.** Oracle Enterprise Manager is deployed in an on-premises data center and connects privately to the Autonomous Database – Serverless, thereby ensuring that traffic does not go over public internet.
  For information on connecting from Oracle Enterprise Manager deployed on premises to an Autonomous Database – Serverless, see Example: Connecting from Your Data Center to Autonomous Database in *Using Oracle Autonomous Database Serverless*.

  The following diagram provides an overview of how Oracle Enterprise Manager deployed on premises connects with Autonomous Databases – Serverless using a private endpoint.



Access Autonomous Database – Serverless Using Transit Routing

This section walks you through a scenario in which you enable private access from your Oracle Enterprise Manager deployed on premises to the Autonomous Database – Serverless in Oracle Services Network using *Transit Routing*. This method should only be used when the Autonomous Database – Serverless is not configured with a private endpoint. For information on Transit Routing, see Overview of On-Premises Network Private Access to Oracle Services in Oracle Cloud Infrastructure documentation.

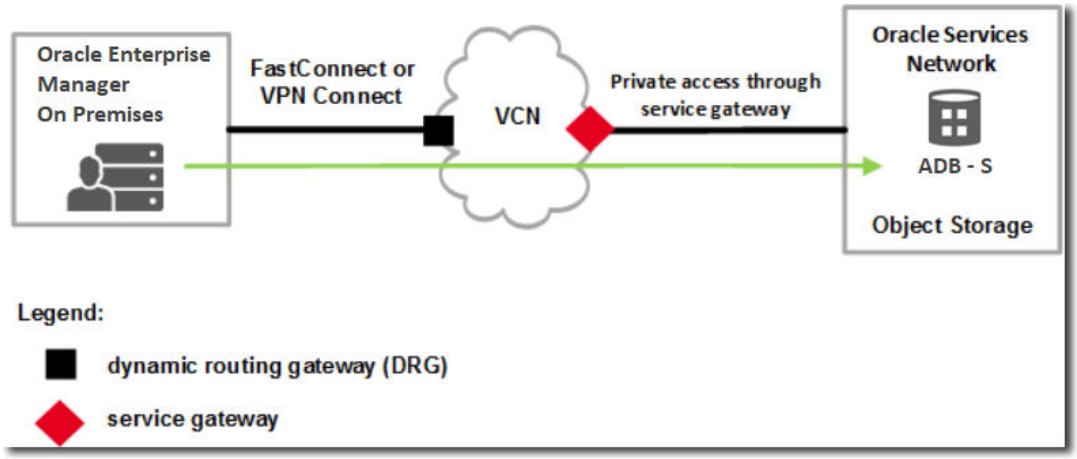
- **Provision an Autonomous Database – Serverless.** As a first step, you must ensure that you have provisioned the Autonomous Database – Serverless.
  For information, see Provision an Autonomous Database Instance in *Using Oracle Autonomous Database Serverless*.
- **Download the Client Credentials (Wallet).** After you provision the database, you must download the OCI Client Credential (Wallet) and save the `.zip` file to provide client access to the Autonomous Database – Serverless.
  For information, see Download Client Credentials (Wallets) in *Using Oracle Autonomous Database Serverless*.
- **Deploy Oracle Enterprise Manager in your on-premises network.** The OMS includes a central Oracle Management Agent that can be used to discover Autonomous Databases,

which are treated as non-host targets. The central agent is installed by default on the OMS host and must have SQL*Net access to the Autonomous Database – Serverless. Note that if you have an existing on-premises database or an Oracle Cloud Infrastructure Database system in the same VCN where the Autonomous Database – Serverless resides, you have the option of using the agent that monitors them, instead of the central agent.
For information, see:

- Upgrading the Enterprise Manager Cloud Control 13c Release 5 Software Only with Plug-ins in *Oracle Enterprise Manager Cloud Control Upgrade Guide*.
- Overview of the Directories Created for an Enterprise Manager System in *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.

- **Review and use the specified connectivity option to connect Oracle Enterprise Manager on premises with the Autonomous Database – Serverless.** Oracle Enterprise Manager is deployed in an on-premises data center and connects to a VCN using FastConnect private virtual circuit or Site-to-Site VPN. Each of these types of connections terminates in a dynamic routing gateway (DRG) that is attached to the VCN. The VCN also has a service gateway, which gives the VCN access to the Autonomous Database – Serverless. The traffic from Oracle Enterprise Manager deployed on premises transits through the VCN, through the service gateway, and to the Autonomous Database – Serverless. The responses return through the service gateway and VCN to Oracle Enterprise Manager deployed on premises.
  For information on how to configure transit routing directly through gateways, see the tasks given in **For routing directly between gateways** in Setting Up Private Access to Oracle Services in Oracle Cloud Infrastructure documentation.

  The following diagram provides an overview of how Oracle Enterprise Manager deployed on premises connects with Autonomous Databases – Serverless using transit routing.



Other Prerequisite Tasks

After you have ensured that the major components are in place using one of the two options given above, you must perform the following prerequisite tasks to discover an Autonomous Database – Serverless from Oracle Enterprise Manager deployed on premises.

1. Create an Oracle Cloud Infrastructure IAM group named **EMGroup**, and add the DBA who will be managing and monitoring the Autonomous Database – Serverless using Oracle Enterprise Manager to this group. Note that this DBA user must have an account in Oracle Cloud Infrastructure.
   See To create a group in Oracle Cloud Infrastructure documentation.

2. Create the following policy to allow the DBA in **EMGroup** to manage and monitor the Autonomous Database – Serverless using Oracle Enterprise Manager:
   `Allow group EMGroup to manage autonomous-database in <compartment in which the Autonomous Database – Serverless resides>`

   See To create a policy in Oracle Cloud Infrastructure documentation.
3. Create a security list and add the following ingress rule to ensure secure access:
   Rule for accessing Autonomous Database – Serverless in the Oracle Cloud Infrastructure VCN from Oracle Enterprise Manager deployed on premises, allow TCPS traffic for the port value specified in the `tnsnames.ora` file in the OCI Client Credential (Wallet).

   For information, see:

   - Security Lists in Oracle Cloud Infrastructure documentation.
   - About Connecting to an Autonomous Database Instance in *Using Oracle Autonomous Database Serverless*.
4. Unlock the `adbsnmp` user, which is created out-of-the-box when the Autonomous Database – Serverless is created in Oracle Cloud Infrastructure. This account is locked by default and you can reset the password and unlock it using Oracle Enterprise Manager or a SQL client.

Discover Autonomous Databases Using the Oracle Enterprise Manager Console

Autonomous Databases are treated as non-host targets in Oracle Enterprise Manager and are discovered manually using the declarative process.

Oracle Enterprise Manager supports a TCP connection and a secure TCP (TCPS) connection using the TLS protocol for Autonomous Databases – Dedicated, and only the TCPS connection using the TLS protocol for Autonomous Databases – Serverless.

1. From the **Setup** menu, select **Add Target**, and then select **Add Targets Manually**.
2. On the **Add Targets Manually** page, click **Add Target Manually** on the **Add Non-Host Targets Manually** tile.
3. In the **Add Target Manually** dialog box, select the host on which the agent that you are using to discover the Autonomous Database is installed and running.
4. In the **Target Type** field, enter and select the Autonomous Database type and click **Add**.

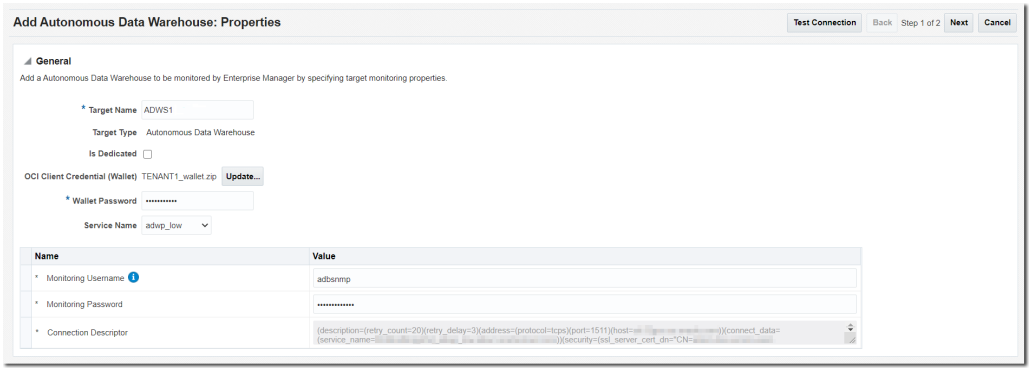
   Your options are **Autonomous Data Warehouse** and **Autonomous Transaction Processing** and Oracle Enterprise Manager discovers the selected target type on the host you selected in the previous step.
5. On the **Add <Autonomous Database Type>: Properties** page, specify the following monitoring details:
   a. Enter a name to identify the Autonomous Database target in the **Target Name** field.
   b. Select the **Is Dedicated** check box for Autonomous Data Warehouse – Dedicated and Autonomous Transaction Processing – Dedicated targets. If you are discovering Autonomous Data Warehouse – Serverless and Autonomous Transaction Processing – Serverless targets, then leave this check box unchecked.
   c. Upload the **OCI Client Credential (Wallet)** `.zip` file, which contains the credentials to access data in your Autonomous Database.

      After you upload the OCI client credential wallet `.zip` file, the **Service Name** and **Connection Descriptor** fields are automatically populated.

Note that you can change the **Service Name** value and opt for a secure TCP (TCPS) connection using the TLS protocol. It is recommended that you use the `low` or `low_tls` database service. For information on Database Service Names, see the Predefined Database Service Names for Autonomous Database section in the documentation for the Autonomous Database you are discovering.

d. Enter the **Wallet Password**. This is the password you set in the Oracle Cloud Infrastructure Console when downloading the OCI client credential wallet `.zip` file.

e. Enter the monitoring password. It is recommended that you use the `adbsnmp` user account and if you are a first time user, then you must enter a new password to reset it and unlock the `adbsnmp` user account. See About User Accounts.



6. Click **Test Connection** to test the connection made to the Autonomous Database.

> **Note:**
>
> If the network is slow, the following connection message may be displayed:
>
> `Connection failure may be due to a slow network, or due to the presence of an intervening firewall.`
>
> You can opt to click **OK** and the discovery process will continue asynchronously.

7. Click **Next** and review the displayed information.
8. Click **Submit**.

After you have discovered the Autonomous Database in Oracle Enterprise Manager, you can verify if the discovery was successful by clicking the **Targets** menu > **Databases** option. The Autonomous Database you discovered should be listed on the **Databases** page.
You can also check connectivity between the OMS host and agent and the Autonomous Database target using JDBC. To do so, you must obtain the following information from the OCI Client Credential (Wallet) `.zip` file:

- `Host`
- `Port`

Run the following command from the OMS host and agent:

```
nc -zv <host> <port>
```

For example:

```
nc -zv host-awwwh-scan.exadatasubnet.exadatainfrast...com 1521
```

Discover Autonomous Databases Using EM CLI

You can use the Oracle Enterprise Manager Command Line Interface (EM CLI) verb `add_cloud_db_target`, to discover an Autonomous Database in Oracle Enterprise Manager.

Format

```
emcli add_cloud_db_target
                -target_name="target_name"
                -target_type="target_type"
                -agent_host="agent_host"
                -zip_file_location="cred_file_zip_location"
                -
credentials="UserName:<db_username>;password:<db_password>;Role:<db_user_role>
"
                -wallet_password="wallet_password"
                -service_name="tns_service_name"
                [-is_dedicated="is_dedicated"]
                [-standby_agent_host="standby_agent_host"]
```

Options

- `-target_name`: Name of the Autonomous Database target.
- `-target_type`: Type of Autonomous Database. The target type value for **Autonomous Data Warehouse** databases is `oracle_cloud_adw` and the value for **Autonomous Transaction Processing** databases is `oracle_cloud_atp`.
- `-agent_host`: Host on which the agent that you are using to discover the Autonomous Database is installed and running.
- `-zip_file_location`: Location of the Oracle Cloud Infrastructure Client Credentials (Wallet) `.zip` file. The `.zip` file location should be accessible from the OMS host.
- `-credentials`: Monitoring user credentials. It is recommended that you use the `adbsnmp` user account. See About User Accounts.
- `-wallet_password`: The wallet password set in the Oracle Cloud Infrastructure Console when downloading the OCI Client Credential Wallet.
- `-service_name`: Predefined database service name of the Autonomous Database. The `low` database service is the default value and to perform monitoring and management tasks, it is recommended that you use the `low` database service.
  Note that Oracle Enterprise Manager supports both TCP and TCPS using the TLS protocol for Autonomous Databases – Dedicated, and only TCPS using the TLS protocol for Autonomous Databases – Serverless. The default protocol for Autonomous Databases – Dedicated is TCP.

  For information on Database Service Names, see the Predefined Database Service Names for Autonomous Database section in the documentation for the Autonomous Database you are discovering.
- `-is_dedicated`: `True` for an Autonomous Database – Dedicated and `False` for an Autonomous Database – Serverless. If a value is not specified for this parameter, then it defaults to Autonomous Database – Serverless.

- `-standby_agent_host`: Host on which a backup agent is installed. If the primary agent goes down or crashes, then the backup agent monitors the target. This is an optional parameter.

Example

```
emcli add_cloud_db_target
                -target_name="ATPD1"
                -target_type="oracle_cloud_atp"
                -agent_host="myhostname.example.com"
                -zip_file_location="/u01/oracle/atpd/wallet_ATPD1.zip"
                -credentials="UserName:adbsnmp;password:password;Role:Normal"
                -wallet_password="password"
                -service_name="ATPD1_low"
                -is_dedicated="True"
                -standby_agent_host="standbyhostname.example.com"
```

Discover Autonomous Databases Using REST API

You can discover an Autonomous Database in Oracle Enterprise Manager using REST API.

Feature	Description
URL	`https://<em_url>:<em_port>/em/websvcs/restful/emws/oracle.sysman.db/v0/discovery/add_cloud_db_target`
Request Header	Content-Type: application/json
Body	`'{ "target_name": "target_name", "target_type":"target_type", "agent_host": "agent_host", "zip_file_location":"cred_file_zip_location", "credentials":"UserName:<db_username>;password:<db_password>;Role:<db_user_role>", "wallet_password:"wallet_password", "service_name":"tns_service_name", "is_dedicated":"is_dedicated" "-standby_agent_host="standby_agent_host" }'` For descriptions, see Discover Autonomous Databases Using EM CLI.
Request Method	POST
Sample Response	`Successfully added target :<target name>`
Supported Since Release	EM DB Plug-in Bundle Patch 13.3.2.0.190731

3
Monitoring and Administration Tasks

After you have discovered Autonomous Databases, you can perform the following monitoring and administration tasks using Oracle Enterprise Manager for Autonomous Databases.

As you review the information available in the following table, note that:

- For Autonomous Databases, Oracle Enterprise Manager provides a subset of the features that it provides for Oracle Databases. The "more information" links in the following table currently take you to generic information on Oracle Enterprise Manager support for Oracle Databases, and all the features may not be available for Autonomous Databases.
- When you click the options in the user interface that take you to other Performance, Security, Schema, and Administration pages, the **Database Login** page is displayed and you must enter the Database Admin User credentials. These credentials can also be configured as named credentials. For information on named credentials, see Credentials Management in *Oracle Enterprise Manager Cloud Control Security Guide*.

Task	Description
Monitor the state and workload of the Autonomous Database on the Home page	To go to the Home page of the Autonomous Database: 1. From the **Targets** menu, select the **Databases** option. 2. On the **Databases** page, click the name of the Autonomous Database. The Home page enables you to proactively monitor: • **Load and Capacity** of the Autonomous Database. • Database **Incidents** that have occurred over the last 24 hours, if any. • Active session information in the **Performance** section, which includes: – The **Activity Class** chart that shows the average number of database sessions active for the past hour. – The **Services** chart that shows the average number of database sessions active for the past hour for database services. • Resource utilization on CPU, Active Sessions, Memory, and Data Storage charts in the **Resources** section. • SQL activity in the **SQL Monitor** section. The table in this section provides information on monitored SQL statement executions. For information on: • The Database Home page, see Monitoring General Database State and Workload in *Oracle Database 2 Day DBA*. • The options available in the **<Autonomous Database Type>** menu, see Monitoring and Managing Targets in *Oracle Enterprise Manager Cloud Control Monitoring Guide*. • Autonomous Database metrics, see Autonomous Databases in *Oracle Database Metric Reference Manual*.

Task	Description
Create a job to execute SQLs on your Autonomous Databases	Oracle Enterprise Manager's Job System enables you to create, manage, and edit a job, which is a schedulable unit of work that you define to automate commonly run tasks. For Autonomous Databases, you can use the **Execute SQL** job type to automate and schedule the execution of SQL commands. To create an **Execute SQL** job for an Autonomous Database: 1. Go to the Home page of the Autonomous Database and from the **<Autonomous Database>** menu, select **Job Activity**. The **Jobs** page is displayed with the Autonomous Database **Target Name** and **Target Type** selected in the **Search Criteria**. 2. Click **Create Job**. 3. In the **Select Job Type - Oracle Enterprise Manager** dialog box, select the **Execute SQL** job type and click **Select**. The **Create 'Execute SQL' Job** page is displayed. 4. Enter the following information in the **General** tab: a. **Name**: Enter a unique name for the job. b. **Description**: Optionally, add a description. c. **Automatic Attempts**: Optionally, specify the maximum number of times the job must be attempted, if it fails, and the number of minutes between each attempt. d. **Target Type**: Select your Autonomous Database target type. e. **Target**: Click **Add**, select the Autonomous Database target in the **Search and Select: Targets** dialog box, and click **Select**. f. **Maximum Parallel Executions**: Optionally, specify the maximum number of parallel executions. 5. In the **Parameters** tab, enter a single SQL or PL/SQL statement without a trailing `;` or `/`, and make changes to the other options, if required. 6. In the **Credentials** tab, provide the credentials to log in to the Autonomous Database. 7. In the **Schedule** tab, define the schedule of the **Execute SQL** job. 8. In the **Access** tab, review the Administrators and roles that have access to the job and click **Add** to add other administrators, if required. 9. Click **Submit**. A confirmation message that the job is created successfully is displayed on the **Jobs** page. For information on Enterprise Manager Jobs, see Job System Purpose and Overview in *Oracle Enterprise Manager Cloud Control Monitoring Guide*.

Task	Description
Monitor performance and diagnose issues on the Performance Hub, SQL Monitoring, AWR, and Advisors pages	Using Oracle Enterprise Manager, you can monitor the performance of an Autonomous Database and ensure that it performs optimally. From the **Performance** menu on the Home page of the Autonomous Database, you can select one of the following options: • **Performance Hub**: View all the performance data available for a specified time period. Once a time period is selected, the performance information is collected and presented based on performance subject areas. • **SQL**: Perform SQL monitoring and tuning tasks. This includes options such as: – **SQL Tuning Advisor** to submit SQL statements and obtain recommendations on how to tune the statements, along with a rationale and expected benefit. – **SQL Performance Analyzer** to determine the effect of a change on a SQL workload by identifying performance divergence for each SQL statement. – **SQL Tuning Sets** to group SQL statements and related metadata into a single object, which you can use as input to SQL tuning tools. • **AWR**: Use Automatic Workload Repository (AWR) and automate database statistics gathering by collecting, processing, and maintaining performance statistics for database problem detection and self-tuning purposes. This includes options such as: – **AWR Report** to generate an AWR report between two snapshots (two points in time). – **Compare Period Reports** to compare database performance between two periods of time (or two AWR reports with a total of four snapshots). • **Advisors Home**: View and use SQL advisors to optimize the database's performance. • **Automatic Indexing**: Automate index management tasks for 19c-based Autonomous Databases. Automatic indexing automatically creates, rebuilds, and drops indexes in a database based on the changes in application workload, thereby improving database performance. This includes the following options: – **Settings**: On the **Automatic Indexing Configuration Settings** page, you can enable and disable automatic indexing, specify the retention period for unused indexes and automatic indexing logs, and specify the schemas to be included or excluded from using automatic indexing. – **Activity Report**: On the **Automatic Indexing Activity Report** page, you can enter the following details and click **Generate Report** to view the details of the auto indexes generated in the database: * **Report Format**: Select the format in which you want the report to be generated. * **Sections**: Select the sections that you want displayed in the report. The **Summary**, **Index Details**, **Verification Details**, and **Errors** options are selected by default in the **Sections** field, and you can opt to remove any of these sections. * **Time Period**: Select the monitoring time period for which you want the report to be generated. If you select the default options, namely the **HTML** report format and all the options in the **Sections** field for a specific

Task	Description
	time period, then the following sections are displayed in the **Report Summary**: * **Overview of Executions**: This section displays the overall performance improvement factor as a result of the auto indexes, the number of times the auto index operations were completed, the number of times the auto index operations were interrupted, and fatal errors, if any. Note that the **Overview of Executions** section is displayed irrespective of which other section is selected in the **Sections** field. * For the **Summary** section option, the following bar graphs are displayed: * **Summary of Auto Indexes Actions** * **Summary of Auto Indexes SQL Actions** * **Summary of Manual Indexes** * For the **Errors** section option, the **Error Summary** pie chart is displayed. * For the **Index Details** section option, the following sections are displayed: * **Index: Created** * **Index: Dropped** You can click a row in the **Index: Created** and **Index: Dropped** sections to view more details such as the ID of the index that was created or dropped, the **Key**, and **Type**. You can also use the **Download All Index Created Details** and **Download All Index Dropped Details** options given in these sections to download the index details in a `.csv` format. * For the **Verification Details** section option, the **Verification Details** section is displayed, which includes the details of the SQLs for which auto indexes were generated and used. You can click a row in this section to view more details such as **SQL ID**, **SQL Text**, and **Improvement Factor**. If you select the **TEXT** report format in the **Report Format** field, then the same information is displayed in a plain text format and can be downloaded by clicking the**Text Download** option. • **Blocking Sessions**: Use to view the sessions that are blocking other sessions. The Blocking Sessions table provides information such as the **Sessions Blocked**, **Session ID**, and **Serial Number**. To view details about a specific session, click the **Select** option for that row and click **View Session**. To terminate a session, click the **Select** option, and then click **Kill Session**. For information on: • Monitoring performance on the Performance Hub, see Monitoring Performance Using the Performance Hub in *Oracle Database 2 Day DBA*. • Tuning SQL statements using the SQL Tuning Advisor, see Running the SQL Tuning Advisor in *Oracle Database 2 Day DBA*. • Managing auto indexes, see Managing Auto Indexes in *Oracle Database Administrator's Guide*. • *Oracle Database 2 Day + Performance Tuning Guide* • *Oracle Database SQL Tuning Guide* • *Oracle Database Testing Guide*

Task	Description
Test migration from an on-premises database to an Autonomous Database using the SQL Performance Analyzer workflow	Using the SQL Performance Analyzer workflow in Oracle Enterprise Manager, you can test the effects of a migration from an on-premises database to an Autonomous Database based on SQL Tuning Set performance. As prerequisite steps, you must: • Ensure that the source on-premises database and the target Autonomous Database are discovered in Enterprise Manager. • Capture the representative SQL workload from the source on-premises database and create a SQL Tuning Set. For information, see Creating a SQL Tuning Set in *Oracle Database 2 Day + Performance Tuning Guide*. • Move the SQL Tuning Set to the target Autonomous Database. For information, see Transporting SQL Tuning Sets in *Oracle Database 2 Day + Performance Tuning Guide*. To test the migration from an on-premises database to an Autonomous Database: 1. Go to the Home page of the Autonomous Database and from the **Performance** menu, select **SQL**, and then select **SQL Performance Analyzer Home**. If the **Database Login** page appears, then log in as a user with administrator privileges. For information on user privileges, see About User Accounts. 2. Click **Migrate to Oracle Autonomous Database**. 3. Enter the required information in the fields on the **Migrate to Oracle Autonomous Database** page. • **Task Information**: Enter task information such as the name of the task, the name of the SQL Tuning Set, and optionally a description of the task. • **Pre-Migration Trial**: The pre-migration trial is built from the SQL Tuning Set by default, and **Build from SQL Tuning Set** is the only available pre-migration trial option. • **Post-Migration Trial**: Select an option in the **Creation Method** and **Per-SQL Time Limit** lists. For information on these lists and what you must enter, see steps 4 and 5 in Testing Database Upgrades Using Cloud Control in *Oracle Database Testing Guide*. • **Trial Comparison**: In the **Comparison Metric** list, select the comparison metric to use for the comparison analysis. • **Schedule**: Select your time zone code and select **Immediately** or **Later** to schedule when the task should start. 4. Click **Submit**. The **SQL Performance Analyzer Home** page is displayed. In the **SQL Performance Analyzer Tasks** section, the details of the task are displayed. The **Last Run Status** displays **Processing** while the SQL statements are being processed. To refresh the status of the task, click **Refresh**. After the task completes, the **Last Run Status** column is updated to **Completed**. 5. Under **SQL Performance Analyzer Tasks**, select the task and click the link in the **Name** column. The **SQL Performance Analyzer Task** page is displayed and it has the following sections: • **SQL Tuning Set**: This section summarizes information about the SQL tuning set, including its name, owner, description, and the number of SQL statements it contains.

Task	Description
	• **SQL Trials**: This section includes a table that lists the SQL trials used in the SQL Performance Analyzer task. • **SQL Trial Comparisons**: This section contains a table that lists the results of the SQL trial comparisons. 6. Click the icon in the **Comparison Report** column. The **SQL Performance Analyzer Task Result** page appears. 7. Review the results of the performance analysis. For information, see Reviewing the SQL Performance Analyzer Report Using Oracle Enterprise Manager in *Oracle Database Testing Guide*. For information on: • SQL Tuning Sets, see Managing SQL Tuning Sets in *Oracle Database 2 Day + Performance Tuning Guide*. • SQL Performance Analyzer, see SQL Performance Analyzer in *Oracle Database Testing Guide*.
Copy a SQL Tuning Set (STS) from an on-premises database to an Autonomous Database	Oracle Enterprise Manager enables you to copy an STS from an on-premises database discovered in Enterprise Manager to an Autonomous Database discovered in Enterprise Manager by way of the Oracle Cloud Infrastructure Object Storage. For information on how to copy the STS, see the Copying a SQL Tuning Set from an On-premises Database to an Autonomous Database tutorial.

Task	Description

Backup and Recovery Management and Monitoring of Autonomous Databases	Using Oracle Enterprise Manager, you can monitor the list of backups of an Autonomous Database, schedule an on-demand backup, and perform a restore operation.
	As prerequisites to using this feature, you must:
	• Ensure that you have the required permissions to backup and restore Autonomous Databases and set up an Oracle Cloud Infrastructure Object Storage bucket to serve as a destination for your manual backups.
	• Set the `OCI_OCID` and `OCI_REGION` target properties manually for the Autonomous Database target. To do so, you can use the following EM CLI commands:
	`emcli set_target_property_value -property_records=<tn>:<tt>:OCI_OCID:<value>`
	`emcli set_target_property_value -property_records=<tn>:<tt>:OCI_REGION:<value>`
	`(tn=targetName, tt=targetType)`
	To go to the **Backups** page, from the **Availability** menu on the Home page of the Autonomous Database, select **Backups**. On the **Oracle Cloud Infrastructure Credentials** page, specify the named credentials defined in Enterprise Manager for the host and Oracle Cloud Infrastructure. For information on Named Credentials and their application, see Named Credentials in *Oracle Enterprise Manager Cloud Control Security Guide*.
	On the **Backups** page, you can:
	• View the list of backups of the Autonomous Database.
	• Schedule an on-demand backup.
	1. Click **Schedule Backup**.
	2. In the **Schedule Backup** dialog box, enter a name for the backup, specify the schedule details, and click **Submit**.
	• Perform restore operations.
	– To restore the database to the current or a specific time:
	1. Click **Restore**.
	2. In the **Restore** dialog box, select **Current Time** to restore the database to the current time, or select **Select Time** to restore the database to a specific time. By default, the current time is specified in the **Select Time** field.
	3. Select an option in the **Schedule** section to schedule the restore operation.
	4. Click **Submit**.
	– To restore the database to the end time of a selected backup:
	1. Click the icon in the **Action** column of the backup and click **Restore**.

Task	Description
	2. In the **Restore** dialog box, select **Select Time**. By default, the end time of the selected backup is specified in the **Select Time** field. 3. Select an option in the **Schedule** section to schedule the restore operation. 4. Click **Submit**.
Migrate workloads from an on-premises database to an Autonomous Database using the Database Migration Workbench	For information on the supported migration methods, prerequisite tasks, migration steps, and so on, see Database Migration Workbench in *Oracle Enterprise Manager Database Migration Workbench Guide*.

Task	Description
Keep the Autonomous Databases secure	Oracle Enterprise Manager provides security features that control how a database is accessed and used. From the **Security** menu on the Home page of the Autonomous Database, you can select one of the following options: • **Users**: Create a user with a valid user name and password to prevent unauthorized use. You can also associate specified privileges, roles, and so on with a user. • **Roles**: Create a role to group together privileges and other roles. This facilitates granting multiple privileges and roles to users. • **Profiles**: Create a profile, which is a set of user authorizations and privileges. If you add a user to a profile, then the authorizations and privileges defined in that profile are acquired by the user. • **Audit Settings**: Set up and adjust audit settings to monitor and record selected user database actions. • **Data Redaction**: Beginning with Enterprise Manager 13c Release 5 Update 8 (13.5.0.8), redact (mask) sensitive information that is displayed in applications without altering the underlying database blocks on disk or in cache. You can redact column data using one of the following methods: – **Full redaction**: Redacts all the contents of the column data. – **Partial redaction**: Redacts a portion of the column data. – **Regular expressions**: Uses regular expressions in both full and partial redaction. – **Random redaction**: Ensures that the redacted data presented to the querying application user appears as randomly generated values each time it is displayed, depending on the data type of the column. – **No redaction**: Enables you to test the internal operation of your redaction policies. For information on using Data Redaction in Enterprise Manager, see Managing Oracle Data Redaction Policies in Oracle Enterprise Manager in *Oracle Database Advanced Security Guide*. • **Database Vault**: Beginning with Enterprise Manager 13c Release 5 Update 11 (13.5.0.11), manage Oracle Database Vault and access the Oracle Database Vault Administrator pages to perform tasks such as propagating Oracle Database Vault configurations to other databases. For information on using Database Vault with Enterprise Manager, see Using Oracle Database Vault with Oracle Enterprise Manager in *Oracle Database Vault Administrator's Guide*. • **Privilege Analysis**: Perform a dynamic analysis of privileges and roles that a user account or database uses over time. You can then revoke unused grants and make other changes to better reflect the access a user requires. • **Virtual Private Database**: Create security policies to enforce row-level security policies at the object (table, view, or synonym) level, when the standard object privileges and associated database roles are insufficient to meet application security requirements. • **Cloud Credentials Store**: Store database user credentials along with other attributes as a database object in the Autonomous Database. The database credentials can be used to access a remote database or the Oracle Cloud Infrastructure Object Storage. On the **Cloud Credentials Store** page, select a database schema in the **Schema** drop-down list to view the credentials in the schema. To create a credential: 1. Click **Create** on the **Cloud Credentials Store** page.

Task	Description
	2. In the **Create Credential** dialog box: a. **Credential Name**: Enter an intuitive name for the credential. Note that the name of the credential cannot be edited at a later stage. b. **Username**: Enter the database user name or the OCID of the Oracle Cloud Infrastructure user. c. **Password**: Enter the database user password or the Object Storage authentication token. d. **Confirm Password**: Confirm the password added in the **Password** field. e. Click **OK**. You can click the icon in the **Action** column and click **Edit** or **Delete** to edit or delete the credential. Note that if editing the credential, you can only edit the user name and password and not the name of the credential. Also, when editing the credential, the **Username** and **Password** fields cannot be left blank.

Task	Description

Mask and subset sensitive data	Beginning with Oracle Enterprise Manager 13c Release 5 Update 10 (13.5.0.10), use the **Oracle Data Masking and Subsetting** solution for Autonomous Databases in Enterprise Manager to minimize data exposure in non-production environments. Using the components of this comprehensive solution, you can discover and mask sensitive production data and share only relevant data.
	To access the Data Masking and Subsetting components, go to the Home page of the Autonomous Database and click the **Security** menu. The Data Masking and Subsetting components include:
	• **Data Discovery**: Simplifies the effort of sensitive data discovery through automated discovery procedures and sensitive column types. These procedures not only discover columns holding sensitive information, but also discover the parent-child relationships between these columns that are defined in the database.
	• **Data Masking**: Enables the replacing of sensitive data with fictitious yet realistic looking data. It limits sensitive data proliferation by anonymizing sensitive production data.
	• **Data Subsetting**: Enables the downsizing of data by either deleting data or extracting a subset of data for sharing or archival. It minimizes risk by sharing only relevant data with teams and also reduces storage costs in non-production environments.
	Before you use Data Masking and Subsetting for Autonomous Databases, you must perform the following prerequisite tasks:
	• **Install SQL*Plus on the OMS host on which the Oracle Management Agent is installed**
	The SQL*Plus executable should be available in the agent's `$ORACLE_HOME/bin` location. This is required as the masking script uses SQL*Plus to perform the masking steps.
	• **Perform Autonomous Database-specific tasks for Data Masking and Subsetting (Optional)**
	– For Data Masking and Subsetting operations in which a custom path or export directory is specified, ensure that the directory is created on the Oracle Management Agent that is monitoring the Autonomous Database.
	– For Data Masking and Subsetting operations in which a pre-existing database directory is selected, ensure that the exact path is recreated on the Oracle Management Agent that is monitoring the Autonomous Database.
	• **Perform TCPS connection prerequisite tasks (Optional)**
	These tasks must only be performed for Autonomous Databases being monitored in Enterprise Manager with a TLS service name.
	1. Unzip the client credentials wallet in the `$ORACLE_HOME/$EMDROOT` directory of the Oracle Management Agent monitoring the Autonomous Database. For example:
	`cd /<path_to_installed_agent_location>/agent_13.5.0.0.0/`
	`unzip /<path_to_downloaded_wallet>/wallet.zip -d wallet`
	The wallet directory has files such as `tnsnames.ora` and `sqlnet.ora` and there should be no intermediate directories.

Task	Description

	2. Modify the `sqlnet.ora` file so that the `WALLET_LOCATION` points to the absolute path to the unzipped wallet folder. For example:
	
	`(METHOD_DATA=(DIRECTORY="/<path_to_installed_agent_location>/agent_13.5.0.0.0/wallet"))`
	
	Note:
	If the wallet is downloaded and unzipped in a directory other than `$ORACLE_HOME/$EMDROOT`, then the `WALLET_LOCATION` in `sqlnet.ora` should reflect the correct directory.
	
	3. Perform one of the following actions:
	– If the environment variable `$TNS_ADMIN` is defined, then copy the modified `sqlnet.ora` file to the `$TNS_ADMIN` directory. For example:
	
	`cp wallet/sqlnet.ora $TNS_ADMIN/`
	
	– If the environment variable `$TNS_ADMIN` is not defined, then copy the modified `sqlnet.ora` file to the `$EMDROOT/network/admin/` directory. For example:
	
	`cp wallet/sqlnet.ora /<path_to_installed_agent_location>/agent_13.5.0.0.0/network/admin`
	
	Note that if the directories mentioned above do not exist, then you must run the following command first:
	
	`mkdir -p /<path_to_installed_agent_location>/agent_13.5.0.0.0/network/admin`
	
	For information on using Data Masking and Subsetting components and the general workflow, see:
	• About Oracle Data Masking and Subsetting in *Oracle Data Masking and Subsetting Guide*
	• Database Security Data Masking and Subsetting workshop
	Extract the Exported Masking and Subsetting Data from the Autonomous Database
	1. Create cloud service credentials using `DBMS_CLOUD.CREATE_CREDENTIAL`. For information, see:
	• CREATE_CREDENTIAL Procedure in *Oracle Autonomous Database on Dedicated Exadata Infrastructure*
	• CREATE_CREDENTIAL Procedure in *Using Oracle Autonomous Database Serverless*
	2. Determine the database directory to which the files are exported, for example, `MASK_DUMP_DIR_SYSMAN_0`. For information on directories in Autonomous Databases, see:

Task	Description
	• Manage Directories in *Oracle Autonomous Database on Dedicated Exadata Infrastructure* • Creating and Managing Directories on Autonomous Database in *Using Oracle Autonomous Database Serverless* 3. List the files stored in the database directory using the following query: `SELECT * FROM DBMS_CLOUD.list_files('<name of the directory>');` 4. Place the files in Oracle Cloud Infrastructure Object Storage. For information, see: • PUT_OBJECT Procedure in *Oracle Autonomous Database on Dedicated Exadata Infrastructure* • PUT_OBJECT Procedure in *Using Oracle Autonomous Database Serverless* Note that for Autonomous Databases, the database directory, for example `MASK_DUMP_DIR_SYSMAN_0`, created during in-export masking is not deleted at the end of masking. You can use this directory in conjunction with `DBMS_CLOUD.PUT_OBJECT(...)` to upload the exported masking files to Object Storage and download the files to a location of your choice.
Perform Schema Management tasks	Oracle Enterprise Manager provides a comprehensive set of tools that allows you to manage all aspects of database objects such as tables, indexes, and views. From the **Schema** menu on the Home page of the Autonomous Database, you can select one of the following options to perform fundamental tasks such as creating, editing, and viewing schema objects: • **Database Objects**: Create and manage all aspects of database directory objects such as tables and indexes. • **Programs**: Manage the procedures, functions, triggers, and so on associated with the database. • **Materialized Views**: Work with materialized views and perform tasks such as creating materialized views, materialized view logs, refresh groups, and dimensions.

Task	Description
Work with Directory Objects	You can view the default and custom-created directories in an Autonomous Database on the **Directory Objects** page in Oracle Enterprise Manager. In addition, you can also create directory objects and transfer files from the directory to the Oracle Cloud Infrastructure Object Storage and from the Object Storage to the directory. For information on managing directories in Autonomous Databases, see: • Manage Directories in *Oracle Autonomous Database on Dedicated Exadata Infrastructure* • Creating and Managing Directories on Autonomous Database in *Using Oracle Autonomous Database Serverless* To go to the **Directory Objects** page, from the **Schema** menu, select **Database Objects**, and then select **Directory Objects**. Note that you must have administrator privileges to access and perform tasks on the **Directory Objects** page. To create a directory object: 1. Click **Create** on the **Directory Objects** page. 2. In the **Create Directory Object** dialog box: a. **Directory Name**: Enter a unique name for the directory or sub-directory. b. **Relative Path**: Specify a relative directory path. Note that you cannot provide the absolute path to the directory, and the relative path you specify will be appended to the absolute path. c. Click **OK**. After you create a directory object, you can click the name of the directory in the **Directory Name** column and go to the corresponding **Files** page. On the **Files** page, you can view all the files in the directory and perform the following tasks: • **Download files from the Object Storage to the database directory** 1. Click **Copy from Object Storage**. 2. In the **Copy from Object Storage** dialog box: a. **Database Credential for Object Storage**: Select the database credentials used to connect to Object Storage. Note that the database credentials must be stored in the **Cloud Credentials Store** in Enterprise Manager. For information on **Cloud Credentials Store**, see Cloud Credentials Store. b. **Object Storage URI**: Specify the URI to the Object Storage bucket in which the file resides. The URI must be in the following format: `https://objectstorage.<region>.oraclecloud.com/n/<namespace>/b/<bucket>/o/<object_name>` c. Click **OK**. • **Upload files from the database directory to the Object Storage** 1. Click the icon in the **Action** column and click **Copy to Object Storage**.

Task	Description
	2. In the **Copy to Object Storage** dialog box: a. **Database Credential for Object Storage**: Select the database credentials used to connect to Object Storage. Note that the database credentials must be stored in the **Cloud Credentials Store** in Enterprise Manager. For information on **Cloud Credentials Store**, see Cloud Credentials Store. b. **Object Storage URI**: Specify the URI to the Object Storage bucket in which the file resides. The URI must be in the following format: `https://objectstorage.<region>.oraclecloud.com/n/<namespace>/b/<bucket>/o/<object_name>` c. Click **OK**.

Task	Description
Create a database link from an Autonomous Database – Serverless to a target database	A database link enables you to access objects and perform operations on a remote (target) database, and is stored as an object in the schema. You can create a database link to a target database only from Autonomous Databases – Serverless, however, the target database can be an Autonomous Database, a Database Cloud Service instance, or an on-premises database in the schema. To use database links, the target database must be configured to use TCPS authentication, and the database link is created using a wallet (`cwallet.sso`). Autonomous Databases use TCPS authentication by default, and additional configuration is not required if your target database is an Autonomous Database. Other Oracle Databases must be configured to use TCPS authentication. For information, see Configuring Transport Layer Security Authentication in *Oracle Database Security Guide*. Before you create a database link in Oracle Enterprise Manager, you must: • Store the credentials used to access the target database in the **Cloud Credentials Store** in Enterprise Manager. For information, see Cloud Credentials Store. • Add the target database wallet, `cwallet.sso`, to a directory object on the **Directory Objects** page in Enterprise Manager. For information, see Work with Directory Objects. If creating a database link to an on-premises database, you must ensure that the target database wallet (`cwallet.sso`) is first uploaded to the Oracle Cloud Infrastructure Object Storage and then downloaded to the **Directory Objects** page. To go to the **Database Links** page, from the **Schema** menu, select **Database Objects** and then select **Database Links**. On the **Database Links** page, you can view previously created database links in a schema, if any, and create a database link. To create a database link: 1. Click **Create** on the **Database Links** page. 2. In the **Create Database Link** dialog box, you must provide the following information to create a link to the target database: a. **Name**: Enter an intuitive name for the database link. b. **Host Name**: Enter the host name of the target database. c. **Port Number**: Enter the port number of the target database. The port number should be between 1521 and 1525. d. **Service Name**: Enter the service name of the target database. e. **Distinguished Name (DN)**: Enter the DN value available in the server certificate. f. **Credential Name**: Select the credentials used to connect to the Object Storage. g. **Directory Object**: Select the directory object that contains the wallet of the target database. h. Click **OK**. After you create a database link, click the icon in the **Action** column and click **Test** to test the connection to the database link. To delete a database link, click the icon in the **Action** column and click **Delete**.

Task	Description
Perform Database Administration tasks such as Storage Management and Automated Maintenance	Oracle Enterprise Manager allows you to view and manage the storage structures of Autonomous Databases. From the **Administration** menu on the Home page of Autonomous Databases – Dedicated, you can select one of the following options. Note that for Autonomous Databases – Serverless, the **Storage** option is not available. • **Storage**: Manage your datafiles and tablespaces by clicking the corresponding option. Use **Automatic Undo Management** to view: – Name and size of undo tablespace – Auto-extend tablespace setting – Auto-tuned undo retention period – Minimum retention period Note that for Autonomous Databases, you cannot configure the **Undo** setting. This is a read-only view to understand the **Undo** configuration. • **Oracle Scheduler**: Use the **Automated Maintenance Tasks** option to enable the following maintenance tasks, which are performed automatically during maintenance windows: – **Optimizer Statistics Gathering**: Collects optimizer statistics for all schema objects in the database for which there are no statistics or only stale statistics. – **Automatic SQL Tuning**: Examines the performance of high-load SQL statements, and makes recommendations on how to tune those statements. For information on: • Performing storage tasks, see Performing Common Database Storage Tasks in *Oracle Database 2 Day DBA*. • Managing automated maintenance tasks, see Managing Automated Database Maintenance Tasks in *Oracle Database Administrator's Guide*.