ORACLE

Disaster Recovery Configuration for Oracle Analytics Cloud

Describes best practices for disaster recovery. Guidance for Oracle Analytics Cloud administrators who are responsible for developing and maintaining a robust disaster recovery plan that ensures business continuity and minimizes the impact of any disruptions.

January 2024, version 2.0

Disclaimer

Revision History

The following revisions have been made to this document since its initial publication.

DATE	REVISION
May 2023	Initial publication
Jan 2024	Updated publication

Author: Veera Raghavendra Rao Koka

Contributing Authors: Ahmed Awan, Amarpreet Nagra, Ravi Bhuma, Lisa Garczynski

Table of Contents

Terminology

This disaster recovery guide uses the following terms, acronyms, and abbreviations.

ADW – Oracle Autonomous Data Warehouse

CIDR – classless inter-domain routing

DBCS – Oracle Database Cloud Service

DR – disaster recovery

IAM – Oracle Identity and Access Management

IDCS – Oracle Identity Cloud Service

OAC – Oracle Analytics Cloud

- **Primary OAC instance -** An OAC instance created and used for production purposes. In this example, the OAC production instance was created in the OCI home region.
- **Disaster recovery OAC instance -** An OAC instance created as a backup for the production OAC instance. In this example, the OAC backup instance was created in the OCI DR region.
- **Source and Target OAC instance for the Data Migration utility**
    - **Source** – The OAC instance where you take a backup of the data files is the source OAC instance.
    - **Target** – The OAC instance where you restore the data files is the target OAC instance.

  Examples in this document use the OAC instance in the OCI home region (**Ashburn**) as the primary or source OAC instance. The OAC instance in the OCI DR region (**Phoenix**) is used as DR or target OAC instance.

OCI – Oracle Cloud Infrastructure

OCI regions – Regions and Availability Domains

- **OCI data regions** – Public Cloud Regions, OCI Data Regions
- **OCI home region -** When you sign up for OCI, Oracle creates a tenancy for you in one region. This is your home region. Your home region is where your IAM resources are defined. When you subscribe to another region, your IAM resources are available in the new region; however, the master definitions reside in your home region and can only be changed there.
- **OCI disaster recovery region -** When you subscribe to another region other than the home region for the same cloud services, create an OAC instance as a standby and use it when a disaster occurs.

OCID – Oracle Cloud Identifier

PAC – private access channel

RDG – remote Data Gateway

RPO – recovery point objective

RTO – recovery time objective

VCN – virtual cloud network

VPN – virtual private network

WAF – Web application firewall

For more information, refer to the Oracle Cloud Infrastructure Glossary.

Introduction

This document provides guidance and best practices for OAC administrators, OCI administrators, IDCS/IAM administrators, and database administrators who are responsible for disaster recovery of OAC services. The information in this guide will help administrators develop and maintain a robust disaster recovery plan that ensures business continuity and minimizes the impact of any disruptions.

Overview

Ensuring business continuity and disaster recovery is essential for OAC to withstand unforeseen disasters and natural calamities. One approach is to establish an active-passive model by creating a standby region geographically disparate from the production region.

The standby region, which may have fewer or equivalent services and resources to the production region, periodically receives replicated data such as application content (snapshot), system settings configuration, data source connections, and security data (users and groups). The standby region remains inactive until manually activated after a disruption in the production region.

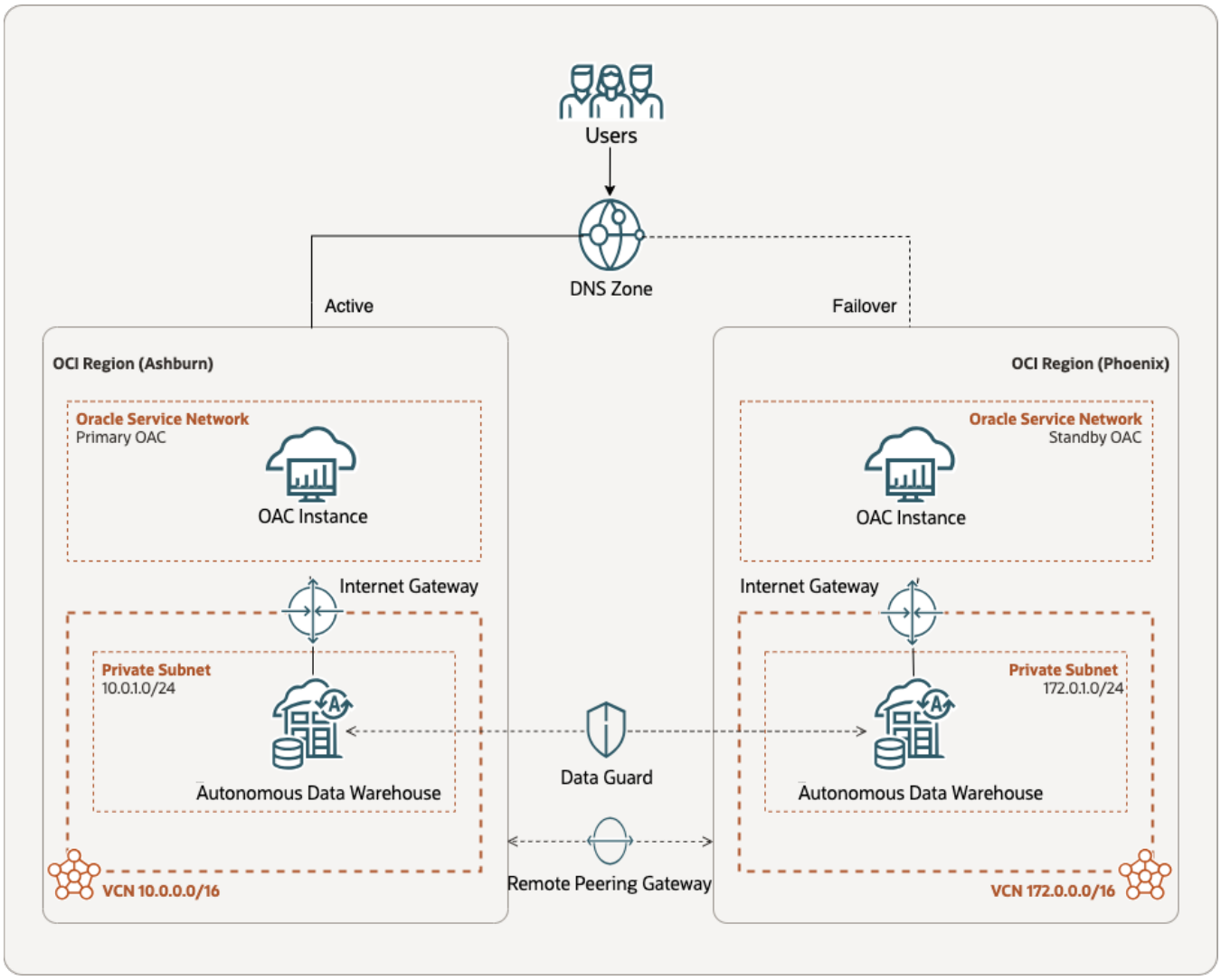
This document details the process for configuring disaster recovery using essential manual and automated tasks and outlines the associated limitations.

High-Level Steps

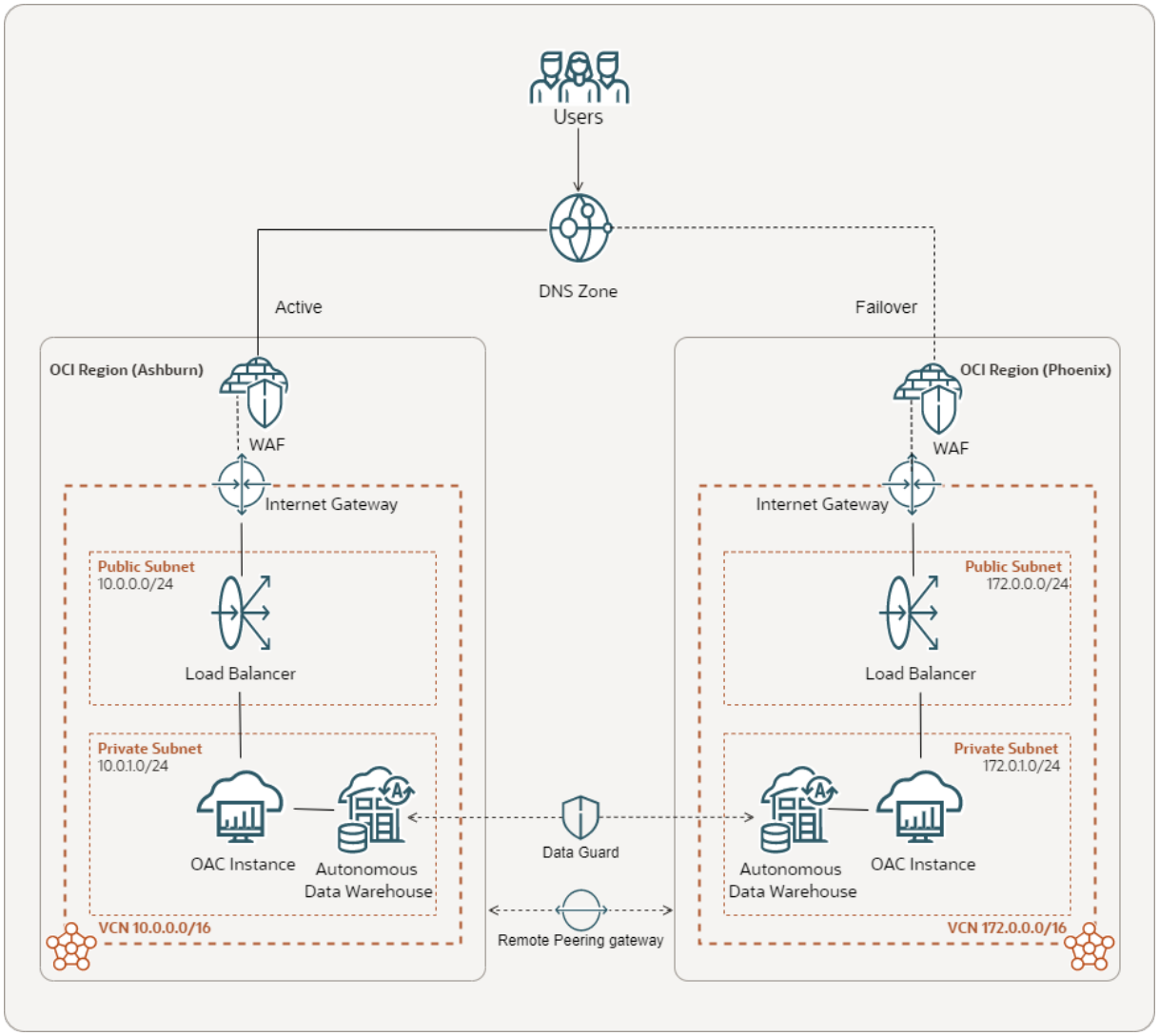
1. Subscribe to OCI Console Announcements.
2. Subscribe to a secondary region in OCI.
3. Set up IDCS or IAM identity domain for DR.
4. Configure the same users and groups in both the primary and DR OAC instances.
5. Configure the same external identity providers for single sign-on.
6. Create OAC instances in two different OCI regions.
7. To ensure proper network connectivity and prevent routing conflicts, configure your VCN with a non-overlapping CIDR range for both OCI regions.
8. To make DR easier to manage, configure PAC or RDG with the exact connection string for your on-premises or Oracle Cloud data sources on both the primary and DR OAC instances.
9. Set up a standby ADW or DBCS using Data Guard to replicate the data sources across the primary and DR regions.
10. Create object storage buckets in both OCI regions.
11. Use snapshots to replicate the content between the primary and DR OAC instances.
12. Configure the same SMTP server and system settings in both OAC instances.
13. Create the same vanity URL for both OAC instances.
14. Map the vanity URL DNS name to the active OAC instance IP address.
15. Configure the public OCI load balancer to access the private endpoint OAC instance and map the load balancer IP address to the DNS name.
16. Fallback from the DR OAC instance to the primary OAC instance using the snapshot and the Data Migration utility.

Architecture

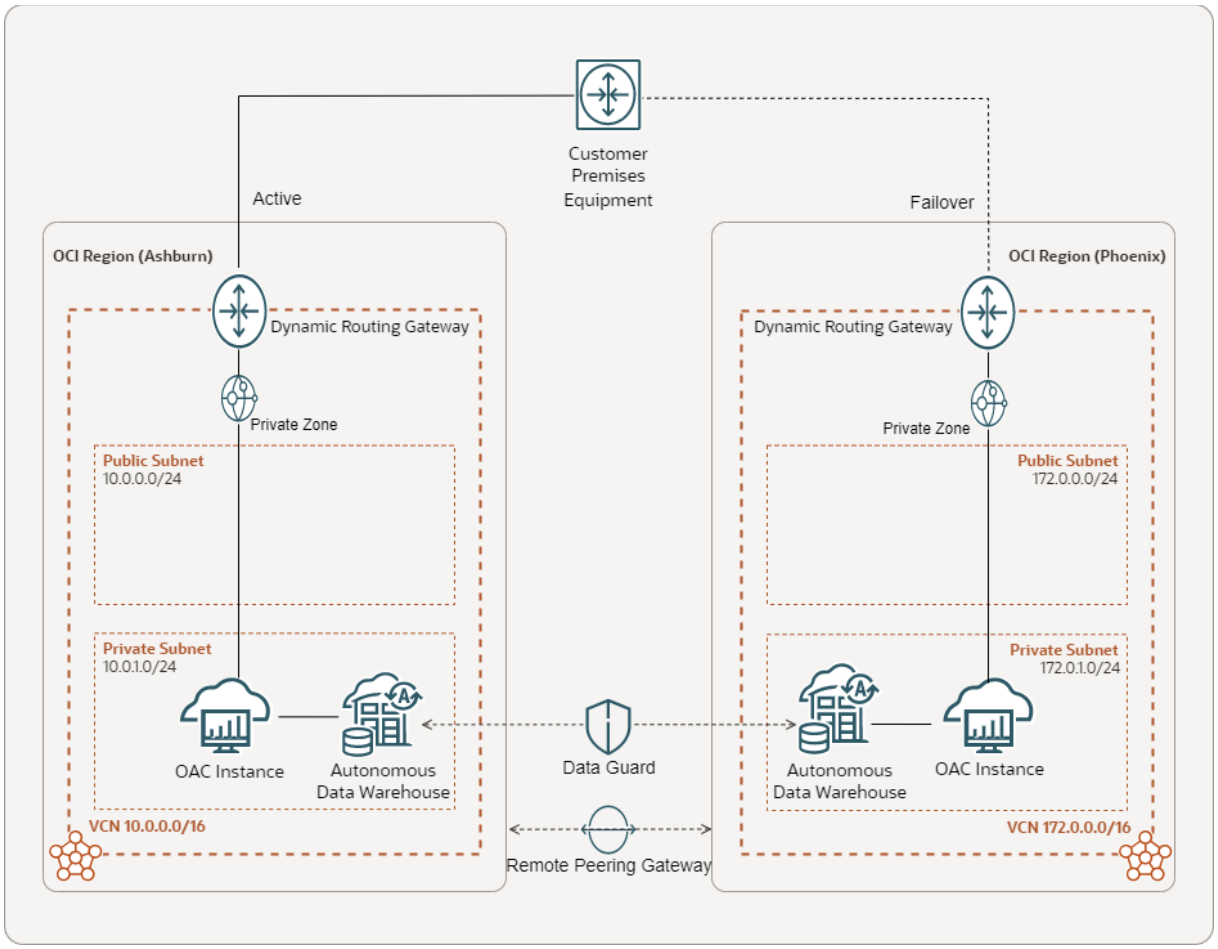
Oracle Analytics Cloud Disaster Recovery Architecture Across Different Oracle Cloud Infrastructure Regions



Oracle Analytics Cloud on a Public Endpoint with a Vanity URL



Oracle Analytics Cloud on a Private Endpoint with a Vanity URL and Public Load Balancer

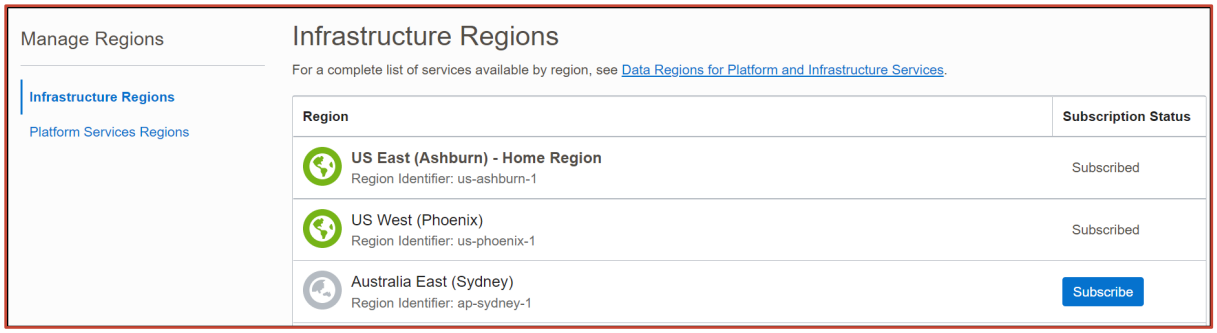


Oracle Analytics Cloud on Private Endpoint with a Vanity URL and Private DNS Zone

Subscribe to a Secondary Oracle Cloud Infrastructure Region

For example, if Ashburn in North America is your OCI home region, subscribe to another region in North America suitable as a DR for the home region such as Phoenix. Always select the home and DR regions in the same Oracle Cloud region to ensure compliance with regional data regulations. See Oracle Cloud Regions Worldwide.

Follow the table in the Disaster Recovery Region Pairings in the OCI commercial realm and select the respective region for DR.



This example shows an OCI tenancy subscribed to Ashburn and Phoenix.

Set Up Identity Cloud Service or IAM Identity Domain for Disaster Recovery

Tenancies with Oracle Identity Cloud Service

For disaster recovery of IDCS, it seems logical to create two IDCS stripes each in a different region, for example, Ashburn and Phoenix. However, we strongly discourage creating IDCS stripes in other OCI data regions.

For information about creating multiple IDCS stripes in different data regions, see About Multiple Instances.

Before creating the secondary IDCS stripe, consider the following:

The *Cloud Account Administrator* must grant *Identity Instance Creation Role* to the user creating the IDCS stripe.

You can create multiple IDCS stripes of the required license type in the home region. For example, Ashburn (North America data region).

You must always create secondary IDCS stripes in the OCI home region. You can't create secondary IDCS stripes in a different OCI region, even if they're located within the same OCI data region, such as North America.

You must extend the subscription to another OCI data region and then create a secondary IDCS stripe. See, Extending Your Subscription to Another Data Region.

You can configure a secondary IDCS stripe if you agree to have the secondary IDCS stripe in another OCI data region, such as Latin America, EMEA, and so on, which may violate the data existence region.

Tenancies with IAM Identity Domains

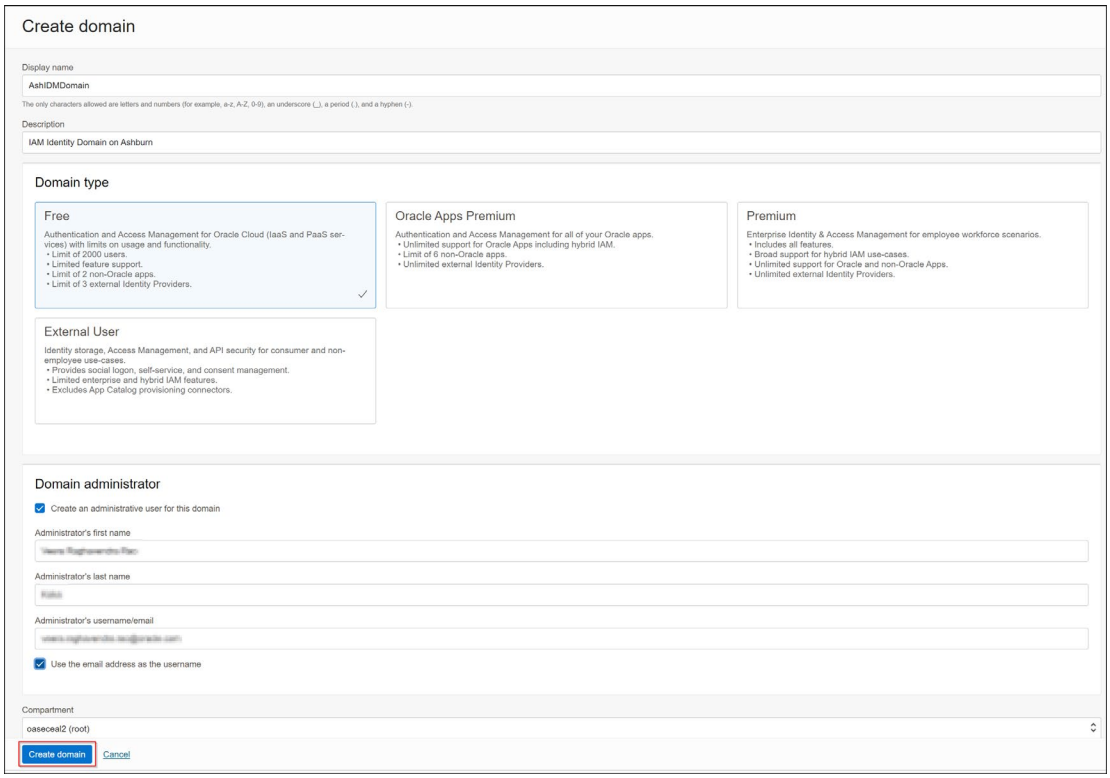
For disaster recovery of the IAM identity domain, it seems logical to create two domains each in a different region, for example, Ashburn and Phoenix. However, we strongly discourage creating domains in different OCI data regions.

Here are the steps to create multiple IAM Identity Domains in different regions.

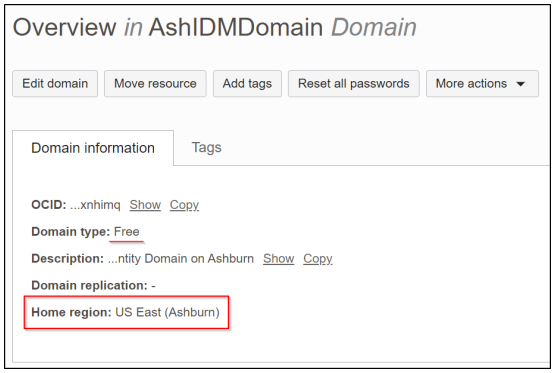
Create IAM Domain on the OCI Home Region (Ashburn)

Follow these steps to create an IAM identity domain for identity management.

1. Sign in to the tenancy's OCI Console as the default domain user and select the home region. For example, Ashburn.
2. Create a domain from the available **Domain types** (Free, Oracle Apps, Oracle Apps Premium, Premium, and External User). For more information on domain types, see IAM Identity Domain Types.



The home region of the IAM domain that you create will be the same as the current region of the OCI Console, for example US East (Ashburn).

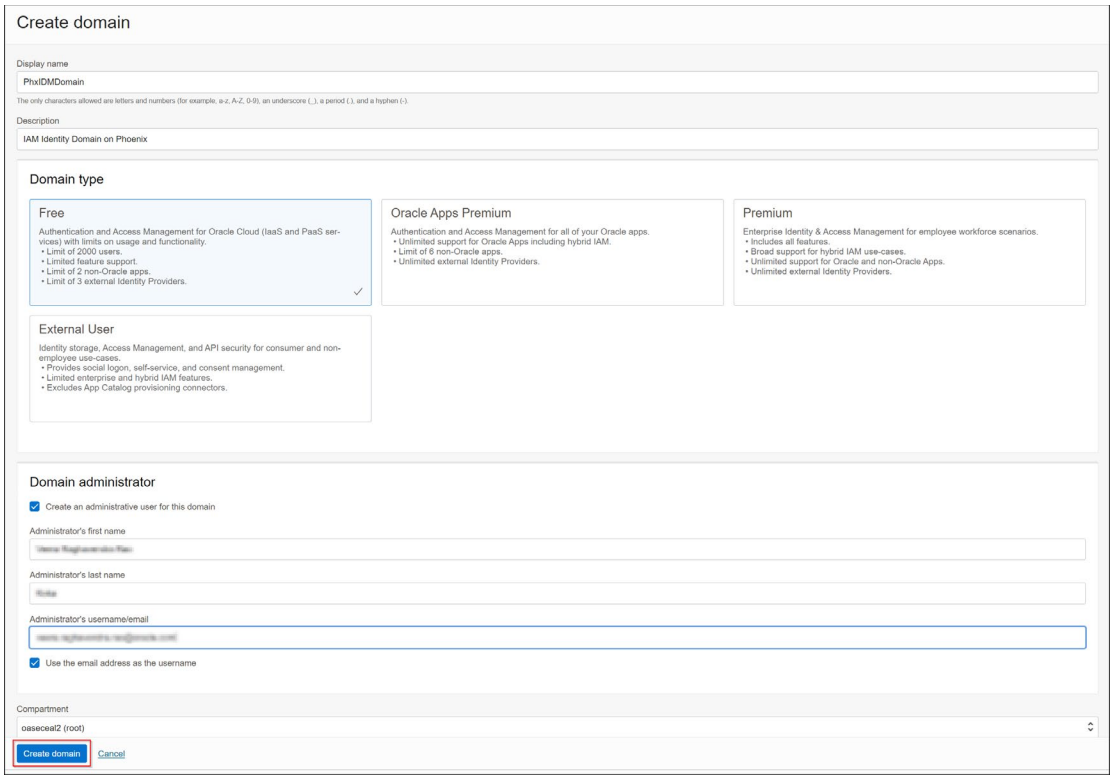


Create IAM Domain on the OCI Disaster Recovery Region (Phoenix)

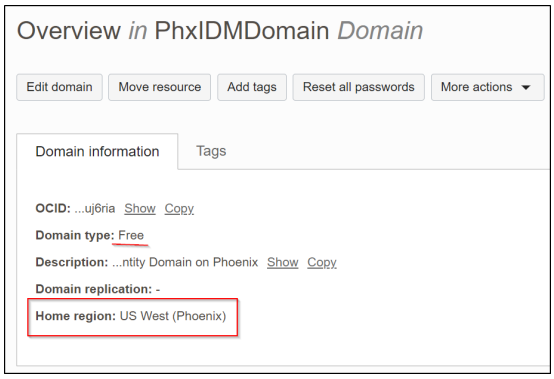
Follow these steps to create an IAM identity domain for identity management.

1. Sign in to the tenancy's OCI Console as the default domain user and select the DR region. For example, Phoenix.
2. Create a domain from the available **Domain types** (Free, Oracle Apps, Oracle Apps Premium, Premium, and External User). For more information on domain types, see IAM Identity Domain Types.

   Note: In this example, we select the **Free** domain type. There are certain limitations to using Free Tier identity domains so ensure that you choose the appropriate domain type for your requirements.



The home region for the IAM domain used for DR will be the same as the current region of the OCI Console, for example US West (Phoenix).



For more details on IAM identity domain types, feature availability for identity domain types, and IAM Object Limits, see Managing IAM.

Reasons to Discourage IDCS Stripes or IAM Domains on Different Data Regions

IDCS and IAM identity domains already have a DR mechanism. An outage on the IDCS or IAM identity domain home region, automatically triggers replication to the DR region. After this process completes, the IDCS or IAM identity domain services become operational.

During the replication time, users may be unable to access their services, and some limitations may exist when the services are available from the DR region.

Replication can take a few hours. Currently, there are no published RTO and RPO numbers from IDCS. See Disaster Recovery and Identity Domains and Disaster Recovery Region Pairings.

Since IDCS and IAM identity domains have a DR mechanism, we don't recommend you create IDCS stripes in other data regions or IAM identity domains in other OCI regions.

To enhance the resilience and availability of identity management for OAC services using IDCS, you can create IDCS stripes in different data regions and associate them with the OCI Console as a *Federation Identity Provider*. Furthermore, you can create an OAC instance in the OCI Console by signing in to the OCI Console as the IDCS stripe user and configuring the IDCS stripe as the identity management for the OAC instance. By leveraging this feature, you can effectively prepare your services for potential disruptions, ensuring that your services remain accessible and operational.

Since IDCS stripes are limited only to the home region, it's better to consider the DR feature provided by IDCS.

If you plan to have different IDCS stripes, we suggest using IDCS Foundation License for Secondary Stripes. See Oracle Identity Cloud Service (IDCS) Pricing Models.

> **Note:** In the future, all the tenancies that use IDCS for identity management will be upgraded to use IAM identity domains.

To enhance the resilience and availability of identity management for OAC services using identity domains, you can create IAM domains in different OCI regions. Furthermore, you can create an OAC instance in the OCI Console by signing in to the OCI Console as the IAM domain user and configuring the IAM domain as the identity management for the OAC instance. By leveraging this feature, you can effectively prepare your services for potential disruptions, ensuring that your services remain accessible and operational.

Using an IAM identity domain other than the Free type can incur extra costs depending on the domain type.

Due to the additional costs involved in having both home and DR regions for an IAM identity domain, users have two options. They can either set up a second IAM identity domain in the DR region or use the same IAM identity domain for both the primary and DR regions and rely on the default disaster recovery mechanism provided by the IAM identity domain.

Synchronize Users and Groups Between IDCS Stripes or IAM Domains

There are multiple ways to onboard users and groups into IDCS and IAM identity domains. The onboarding process is the same for IDCS and IAM identity domains.

Refer to the section **Multiple ways to onboard users and groups into the Oracle Identity Cloud Service (IDCS)** in the blog Single Sign-On Solutions for Oracle Analytics Server on On-Premises and on Oracle Cloud. This information also applies to IAM identity domains.

Use the approaches discussed in the above blog to onboard the users and groups into the home region and DR region IDCS stripes or IAM identity domains. See also, Managing IDCS Users and Managing IAM Users.

After successfully onboarding users and groups to the home region (primary) IDCS stripe or IAM identity domain, you must synchronize them with the DR region (secondary) IDCS stripe or IAM identity domain. You can do this using the *GenericSCIM - Client Credentials* template. See Synchronize Users and Groups Between Oracle Identity Cloud Service Instances.

Configure External Identity Providers with Single Sign-On

If an external identity provider is configured for single sign-on (SSO) in the home region IDCS stripe or IAM identity domain, configure the same identity provider for the DR region IDCS stripe or IAM identity domain.

Apply the same IDP policies, sign-on policies, network perimeter, and MFA if applicable.

Site-to-Site VPN and FastConnect

Site-to-Site VPN or FastConnect is required to connect on-premises networks to Oracle Cloud so that your OAC instances can connect to on-premises data sources using a private access channel (PAC).

For more information on Site-to-Site VPN, see Site-to-Site VPN.

For more information on FastConnect, see FastConnect Overview.

You can connect your OAC instance to remote on-premises data sources over a PAC or use Data Gateway. Usually, a PAC is better than using Data Gateway because it provides direct and secure connectivity without installing agents in between.

While a PAC offers you ongoing simplicity and better performance, it requires a VPN or some other direct network connectivity between Oracle Cloud and your data center, which is not required for Data Gateway.

Before you choose your preferred approach, use OAC's supported data source matrix to check whether you can use a PAC or Data Gateway to connect to your on-premises data sources. See Supported Data Sources.

Create an Oracle Analytics Cloud Instance in Each Region

For details, see Create Services with Oracle Analytics Cloud.

On the Oracle Cloud Infrastructure Console Home Region (Ashburn)

- Create a compartment
- Create a VCN for an OAC instance with a private endpoint
- Configure access control
- Define route rules
- Create an OAC instance in the public or private subnet of the VCN

Create a Compartment

1. Sign in to the OCI Console as an administrator on the home region. For example, Ashburn.
2. Navigate to **Identity & Security → Compartments → Create Compartment**. For example, **oacdr**.
3. Manage the policies for the new compartment as per your security requirements.

Tenancies that have IDCS for identity management:

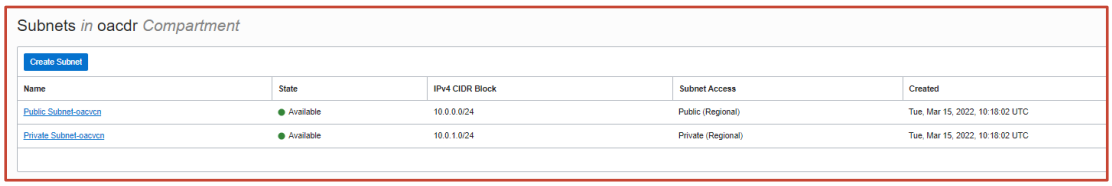
https://docs.oracle.com/en-us/iaas/Content/Identity/Concepts/policies.htm

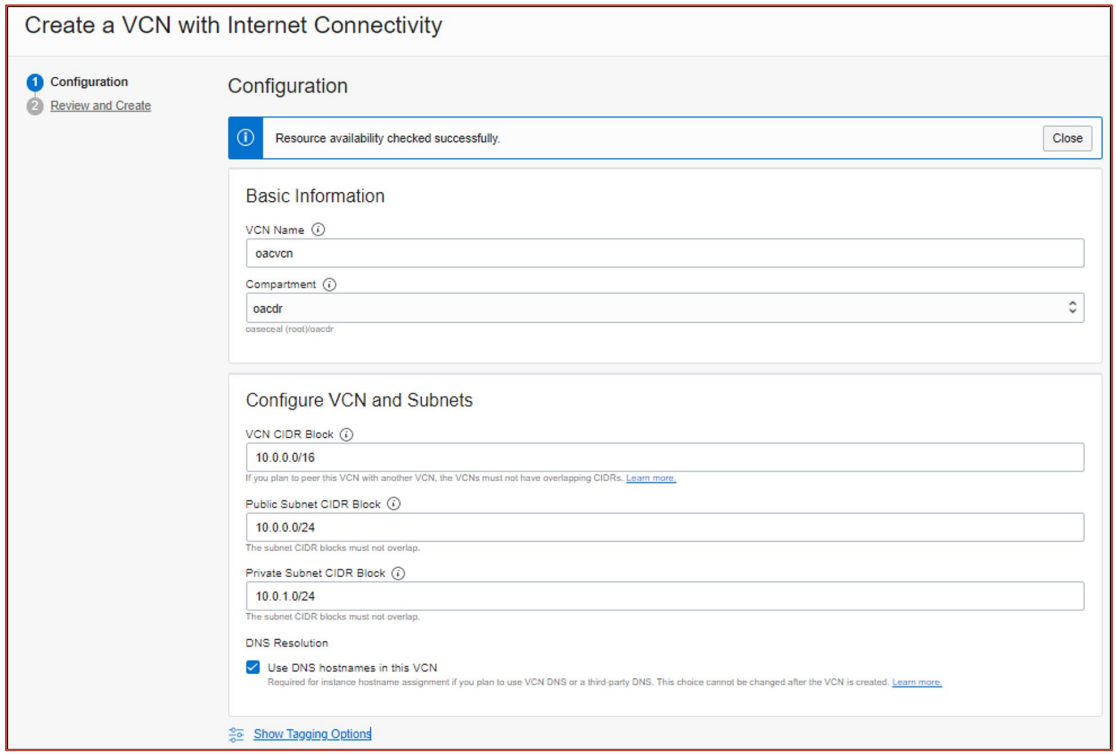
Tenancies that have IAM Identity Domains for identity management:

https://docs.oracle.com/en-us/iaas/Content/Identity/policieshow/how-policies-work.htm

Create a VCN for the OAC with a Private Endpoint

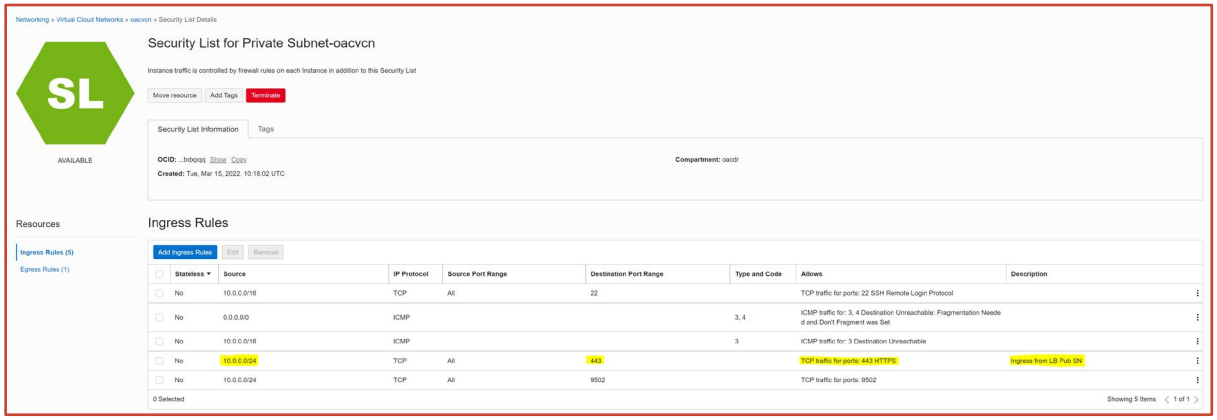
1. Sign in to the OCI Console as an administrator on the home region. For example, Ashburn.
2. Navigate to **Networking → Virtual Cloud Networks → Select the Compartment** (for example, **oacdr**) → **Start VCN Wizard → Create VCN with Internet Connectivity**.





Configure Access Control for OAC with a Private Endpoint

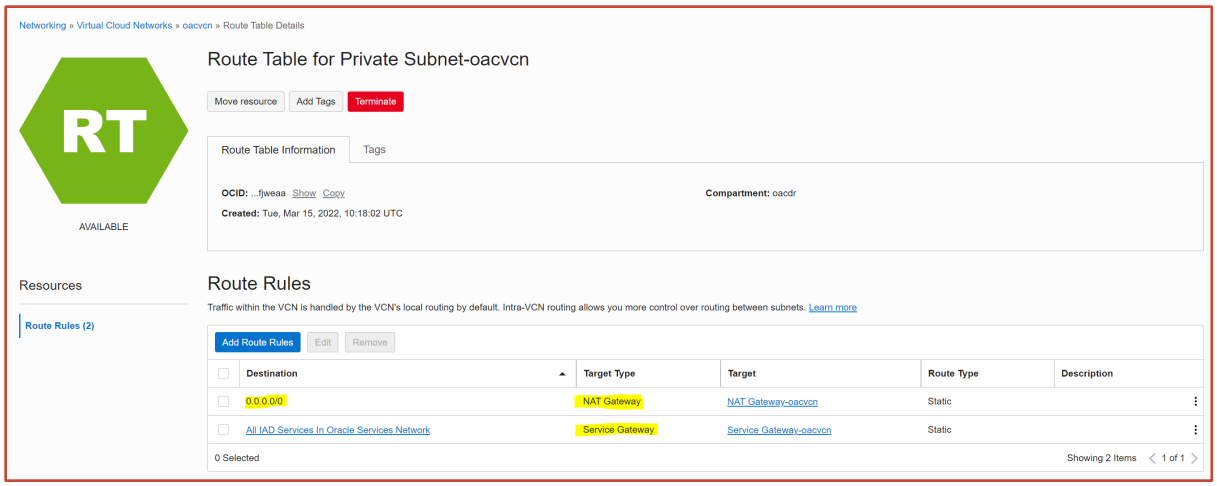
Add an ingress rule to access port 443 from a public subnet where the load balancer will be set up.



Note: Security rules are required on private subnets if you create the OAC instance with a private endpoint.

Add Route Rules for OAC with a Private Endpoint

Add a route rule for a private subnet for NAT Gateway and Service Gateway (exists if you create the VCN using the wizard).



Create an OAC Instance in the Public or Private Subnet of the VCN

Tenancies with IDCS

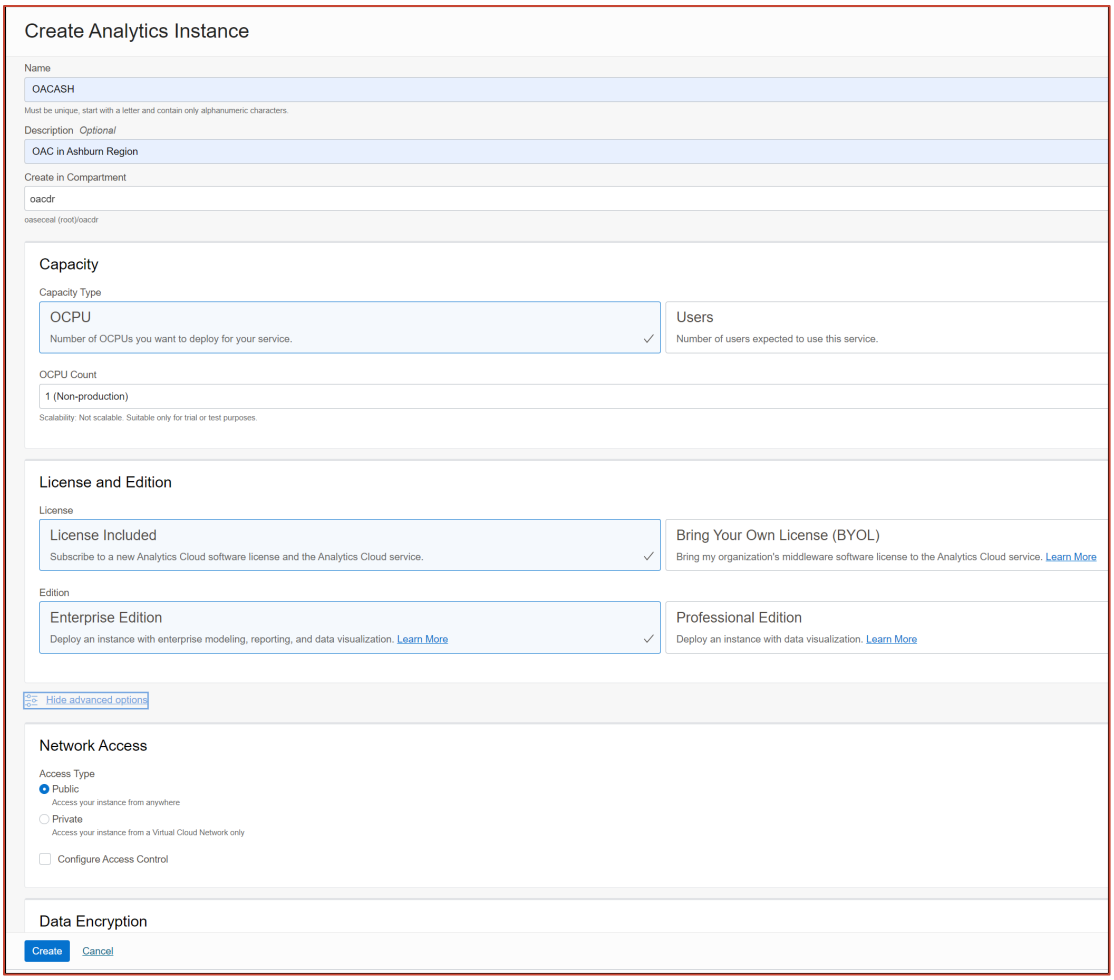
Follow instructions in the blog to create an OAC instance with the respective IDCS stripe for identity management: How to create OAC instances on OCI Native using multiple stripes or instances of IDCS.

1. Sign in to the OCI Console.
2. Select the required IDCS stripe.
3. Enter a Username and Password for the IDCS stripe. The user must have the policies required to create an OAC instance.
4. Navigate to **Analytics & AI → Analytics Cloud → Create Instance**.

Tenancies with IAM Identity Domain

In the previous section, we created an IAM identity domain on the OCI home region, for example Ashburn.

1. Sign in to the OCI Console.
2. Select the required identity domain.
3. Enter a Username and Password for the identity domain. The user must have the policies required to create an OAC instance.
4. Navigate to **Analytics & AI → Analytics Cloud → Create Instance**.



This example creates a public OAC instance. You can also create an OAC instance with a private endpoint.

On the Oracle Cloud Infrastructure Console Disaster Recovery Region (Phoenix)

- Use the existing compartment in the home region
- Create a VCN for an OAC instance with a private endpoint
- Configure access control
- Define route rules
- Create an OAC instance in the public or private subnet of the VCN

Create a Compartment

Use the *existing* compartment, for example **oacdr**, created in the Ashburn region.

1. Sign in to the OCI Console as an administrator on the home region. For example, Ashburn.
2. Change the region to the DR region. For example, Phoenix.
3. Navigate to **Identity & Security → Compartments → Select already created Compartment**. For example, **oacdr**.
4. Manage the policies for the compartment as per your security requirements.

Tenancies that have IDCS for identity management:

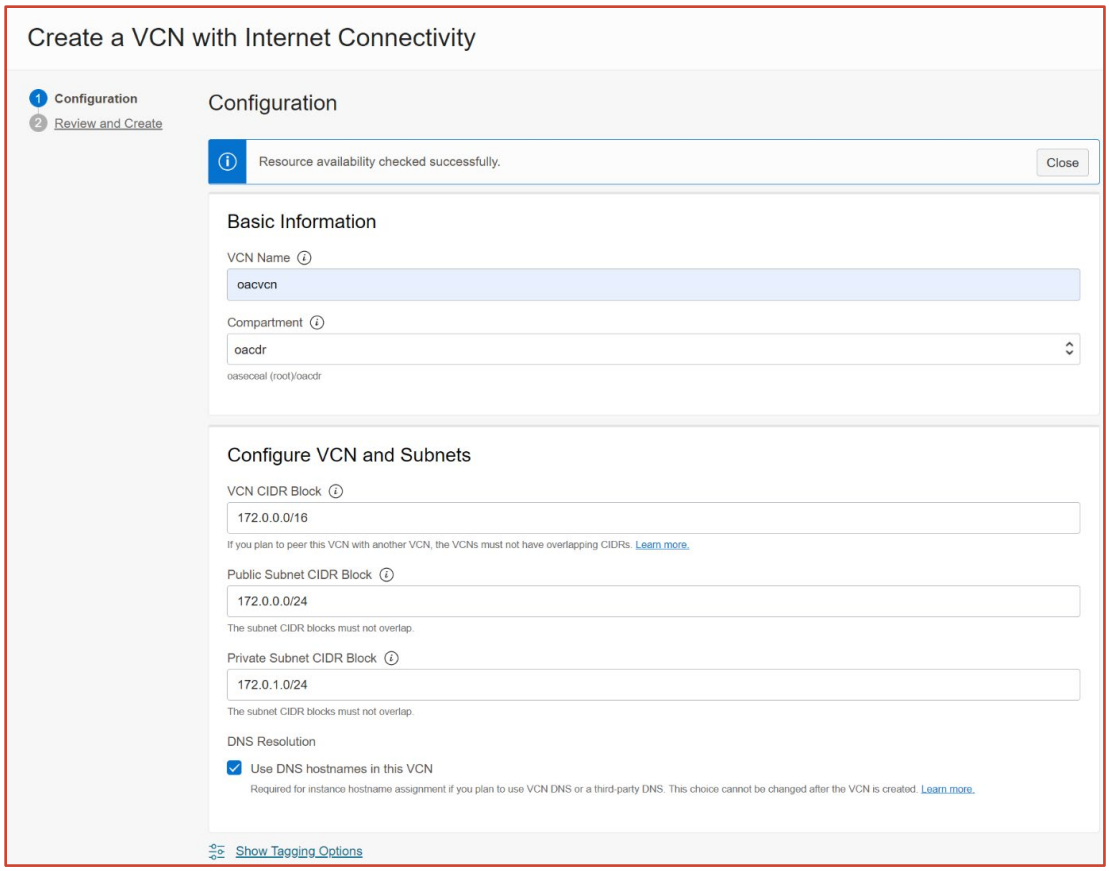
https://docs.oracle.com/en-us/iaas/Content/Identity/Concepts/policies.htm

Tenancies that have IAM Identity Domains for Identity Management:

https://docs.oracle.com/en-us/iaas/Content/Identity/policieshow/how-policies-work.htm

Create a VCN for the OAC Instance with a Private Endpoint

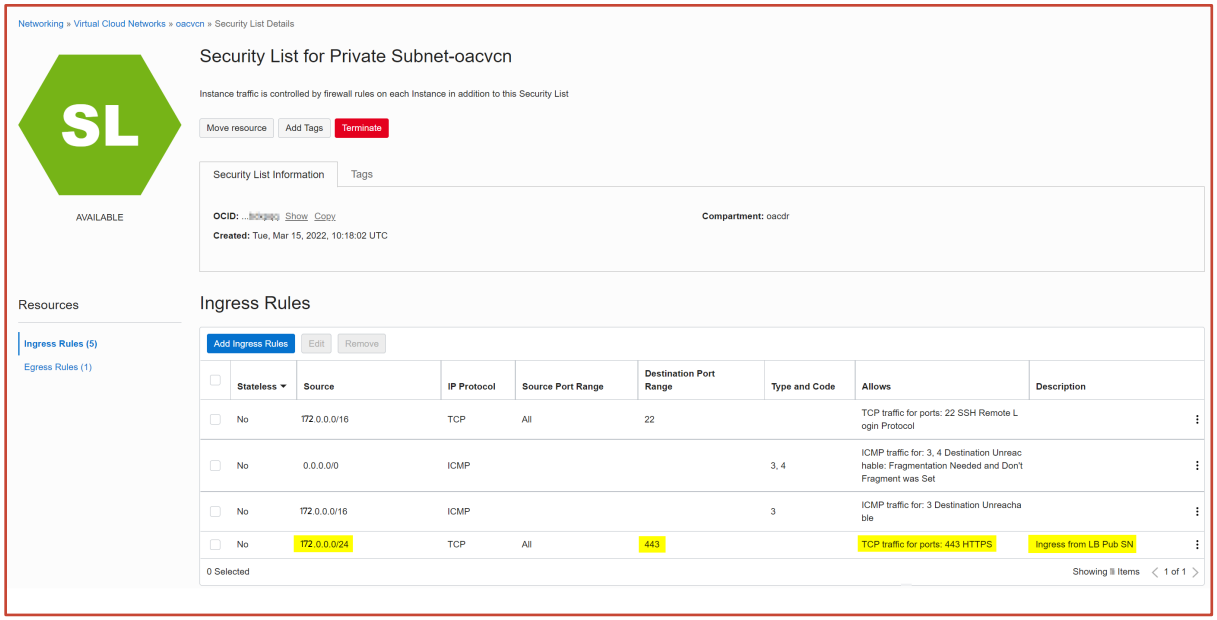
1. Sign in to the OCI Console as an administrator on the home region. For example, Ashburn.
2. Change the region to the DR region. For example, Phoenix.
3. Navigate to **Networking → Virtual Cloud Networks → Select the Compartment** (for example, oacdr) **→ Start VCN Wizard → Create VCN with Internet Connectivity**.



Note: When you create a VCN for a private OAC instance, ensure that the CIDR of the VCN doesn't match the VCN on the home region.

Configure Access Control for OAC with a Private Endpoint

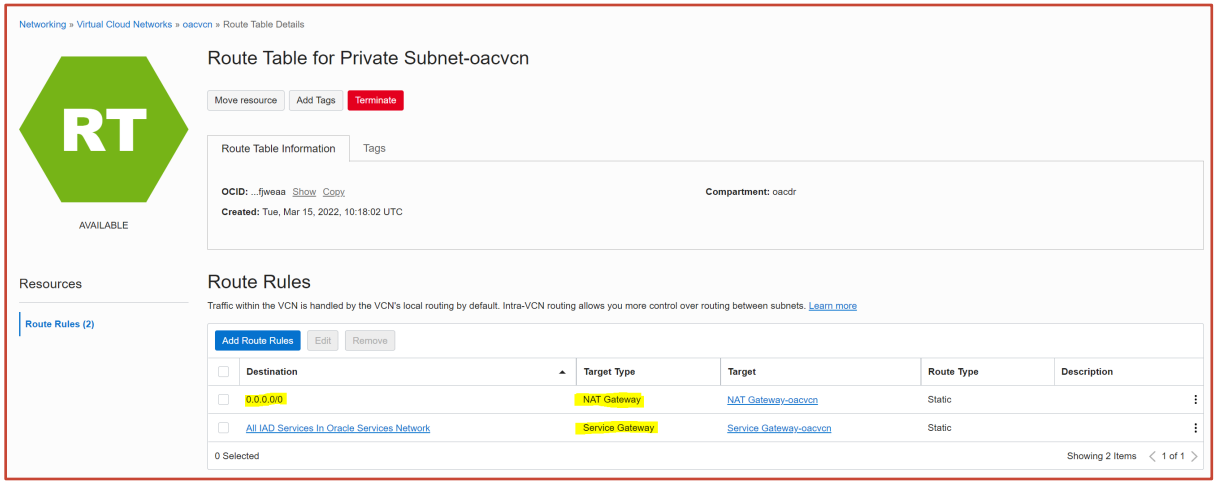
Add an ingress rule to access port 443 from a public subnet where the load balancer will be set up.



Note: Security rules are required on a private subnet if you create the OAC instance with a private endpoint.

Add Route Rules for OAC with a Private Endpoint

Add a route rule for a private subnet for NAT Gateway and Service Gateway (exists if you create the VCN using the wizard).



Create an OAC Instance in the Public or Private Subnet of the VCN

Tenancies with IDCS

Follow instructions in the blog to create an OAC instance with the respective IDCS stripe for identity management: How to create OAC instances on OCI Native using multiple stripes or instances of IDCS.

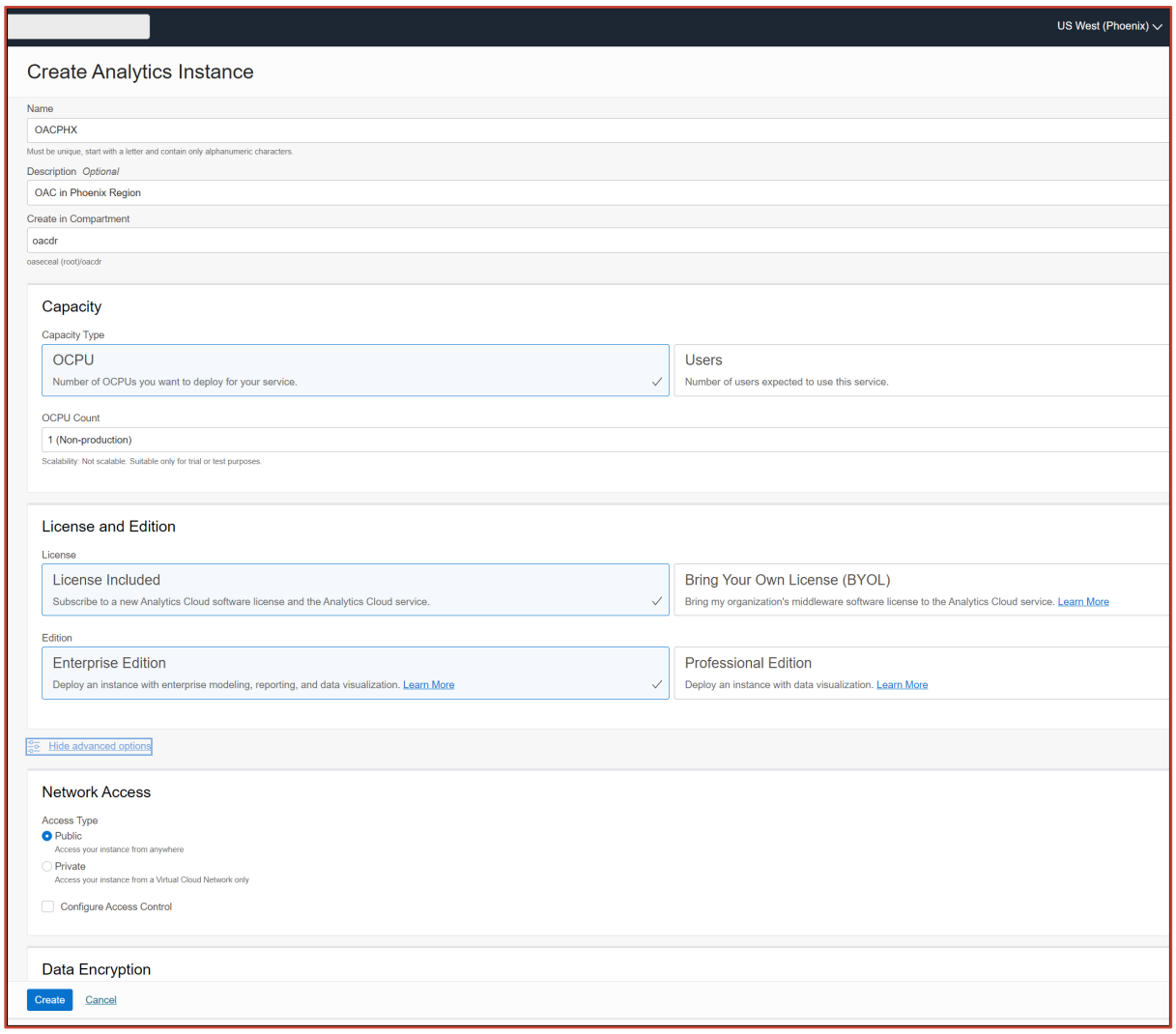
1. Sign in to the OCI Console.
2. Select the required IDCS stripe.

3. Enter a Username and Password for the IDCS stripe. The user must have the policies required to create an OAC instance.
4. Navigate to **Analytics & AI → Analytics Cloud → Create Instance**.

Tenancies with IAM Identity Domain

In the previous section, we created an IAM identity domain on the OCI DR region, for example Phoenix.

1. Sign in to the OCI Console.
2. Select the required identity domain.
3. Enter a Username and Password for the identity domain. The user must have the policies required to create an OAC instance.
4. Navigate to **Analytics & AI → Analytics Cloud → Create Instance**.



This example creates a public OAC instance. You can also create an OAC instance with a private endpoint.

Network Configuration

Earlier, we provided an example of how to create security rules within a private subnet when creating the VCN and its associated subnets.

Additional security rules may be required to access on-premises resources, servers, or data sources that are configured on the VCN or subnets of both regions.

Ensure that you create identical security rules on both the home region (Ashburn VCN's subnets) and DR region (Phoenix VCN's subnets) environments. This ensures that OAC instances across both regions can access identical resources, servers, and data sources on Oracle Cloud, on premises, or on the Internet.

> **Note:** This document doesn't provide detailed instructions for configuring security rules.

Maximizing Data Source Consistency and Availability

Use the same data sources for the OAC instances in the home region and the DR region.

On-Premises Data Source

You can connect OAC to on-premises data sources using a PAC or Data Gatway.

Ensure the primary and DR OAC instances are configured to the same on-premises data sources.

Ensure the OAC instances in the home region and DR region can connect to the on-premises data source with the same connection string using Site-to-Site VPN or FastConnect.

Oracle Autonomous Data Warehouse as a Data Source

Create an Oracle ADW instance in the home region and configure a*utomatic failover* with a remote standby database using Autonomous Data Guard.

The home region ADW should failover to the DR region's standby ADW.

Refer to the documentation and blogs below for more information.

Documentation

Autonomous Data Guard with Cross-Region Standby

Using Standby Databases with Autonomous Database for Disaster Recovery

Shared: Using Standby Databases with Autonomous Database for Disaster Recovery

Blogs

Announcing Autonomous Data Guard

Cross-Region Autonomous Data Guard - Your complete Autonomous Database disaster recovery solution

Your OAC instance uses an ADW wallet to connect to ADW. You can either use the instance wallet or the region wallet.

- Before 15th November 2022, the wallet file consists of the primary and standby ADW connection.
- From 15th November 2022, the wallet from the respective ADW instance has the respective connection details with the respective hostname. Hence, you must download the wallet from the primary and standby ADW instances.

Oracle Autonomous Database on Shared Exadata Infrastructure

ALERT: Update to connection strings for databases with Autonomous Data Guard enabled.

Hello,

You are receiving this email regarding an upcoming change that affects your Oracle Autonomous Database **ADW19C** in tenancy [redacted], region **ashburn**.

As you have enabled Cross-Region Autonomous Data Guard on one or more of your Autonomous Database instances, please note that after **15th Nov 2022** the database connection string provided in your database (in the downloadable wallet or retrieved from the database console or API) will no longer contain the host names of both the Primary and remote Standby databases. The Primary database connection string will contain only the Primary database hostname; similarly the remote Standby database connection string will contain only the remote database hostname.

This change does not affect databases with Autonomous Data Guard disabled.

How will this affect my service?

After **15th Nov 2022**, the wallet and connection string of your database, with cross-region Autonomous Data Guard enabled, will only contain the hostname of the current database from which the wallet or connection string was downloaded. Using this single-hostname connection string will no longer automatically attempt to connect to a second database hostname (since there isn't one), if the database with the first hostname is unavailable.

If your application currently uses a single wallet or connection string to connect to the Primary and remote Standby databases, Oracle recommends connecting to the database from your application running in the Primary region with the wallet or connection string downloaded from the Primary (source) database. Similarly, connect from your application running in the remote region with a wallet or connection string downloaded from the remote Standby database. If your application tier only runs in a single region, we recommend using the Primary database's wallet or connection when connecting to the Primary region database, and swapping in the wallet or connection string out with that from the remote database when connecting to the remote region database.

Post this update, if your connecting application requires a single connection string containing both the Primary and remote Standby database hostnames, you may construct this manually. You may also continue to use your downloaded database wallet or connection string retrieved before **15th Nov 2022**, which contains the hostname of both the Primary and Standby database.

Example connection strings for databases with Cross-Region Autonomous Data Guard enabled

Note: You may view your database connection strings on the database console by clicking the "DB Connection" button or by viewing the tnsnames.ora file in your downloaded wallet.

Current behavior before 15th Nov 2022

Mutual TLS connection string retrieved via the **Primary database console contains both Primary and remote Standby database hostnames:**

```
"(description_list= (failover=on) (load_balance=off) (description=
(retry_count=15)(retry_delay=3)(address=(protocol=tcps)(port=1522)
(host=adb.us-ashburn-1.oraclecloud.com))
(connect_data=(service_name=example1_adwfinance_high...oraclecloud.com))(security=(ssl_server_cert_dn="CN=adwc.uscom-
east-1.oraclecloud.com, OU=Oracle BMCS US, O=Oracle Corporation, L=Redwood City, ST=California, C=US")))
(description= (retry_count=15)(retry_delay=3)(address=(protocol=tcps)(port=1522)
(host=adb.us-phoenix-1.oraclecloud.com))
(connect_data=(service_name=example2_adwfinance_high....oraclecloud.com))(security=(ssl_server_cert_dn="CN=adwc.uscom-
east-1.oraclecloud.com, OU=Oracle BMCS US, O=Oracle Corporation, L=Redwood City, ST=California, C=US"))) )"
```

New behavior after 15th Nov 2022

Mutual TLS connection string retrieved via the **Primary database console contains only Primary database hostname:**

```
"(description_list= (failover=on) (load_balance=off) (description=
(retry_count=15)(retry_delay=3)(address=(protocol=tcps)(port=1522)
(host=adb.us-ashburn-1.oraclecloud.com))
(connect_data=(service_name=example1_adwfinance_high...oraclecloud.com))(security=(ssl_server_cert_dn="CN=adwc.uscom-
east-1.oraclecloud.com, OU=Oracle BMCS US, O=Oracle Corporation, L=Redwood City, ST=California, C=US"))))"
```

Mutual TLS connection string retrieved via the **remote database console contains only remote Standby database hostname:**

```
"(description_list= (failover=on) (load_balance=off) (description=
(retry_count=15)(retry_delay=3)(address=(protocol=tcps)(port=1522)
(host=adb.us-phoenix-1.oraclecloud.com))
(connect_data=(service_name=example2_adwfinance_high....oraclecloud.com))(security=(ssl_server_cert_dn="CN=adwc.uscom-
east-1.oraclecloud.com, OU=Oracle BMCS US, O=Oracle Corporation, L=Redwood City, ST=California, C=US"))))"
```

How can I contact Oracle with further questions regarding this announcement?

If you have general questions about preparing for this change, please contact us through the Autonomous Database customer forum or create a Service Request (SR) on My Oracle Support.

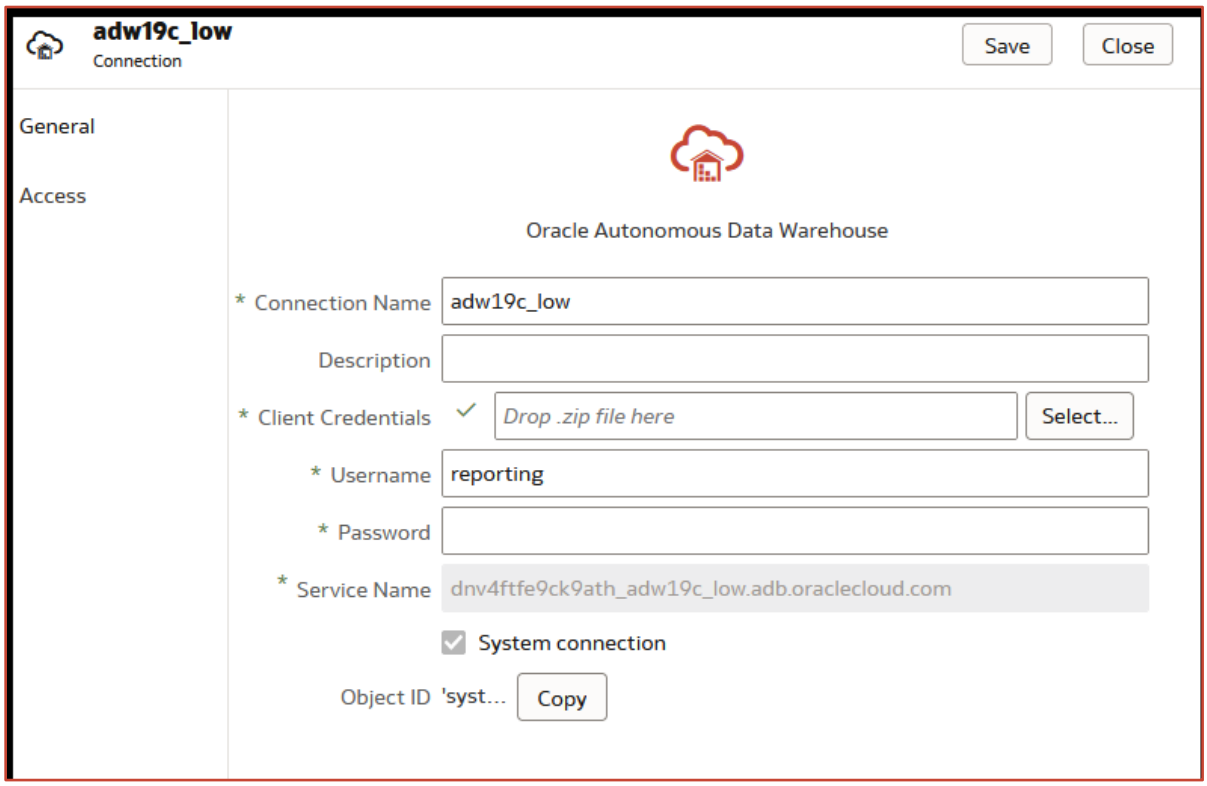
Due to the alert shown above, it's necessary to upload the standby ADW wallet to all Oracle ADW Database connections when the OAC DR instance points to the standby ADW instance.

Test Environment

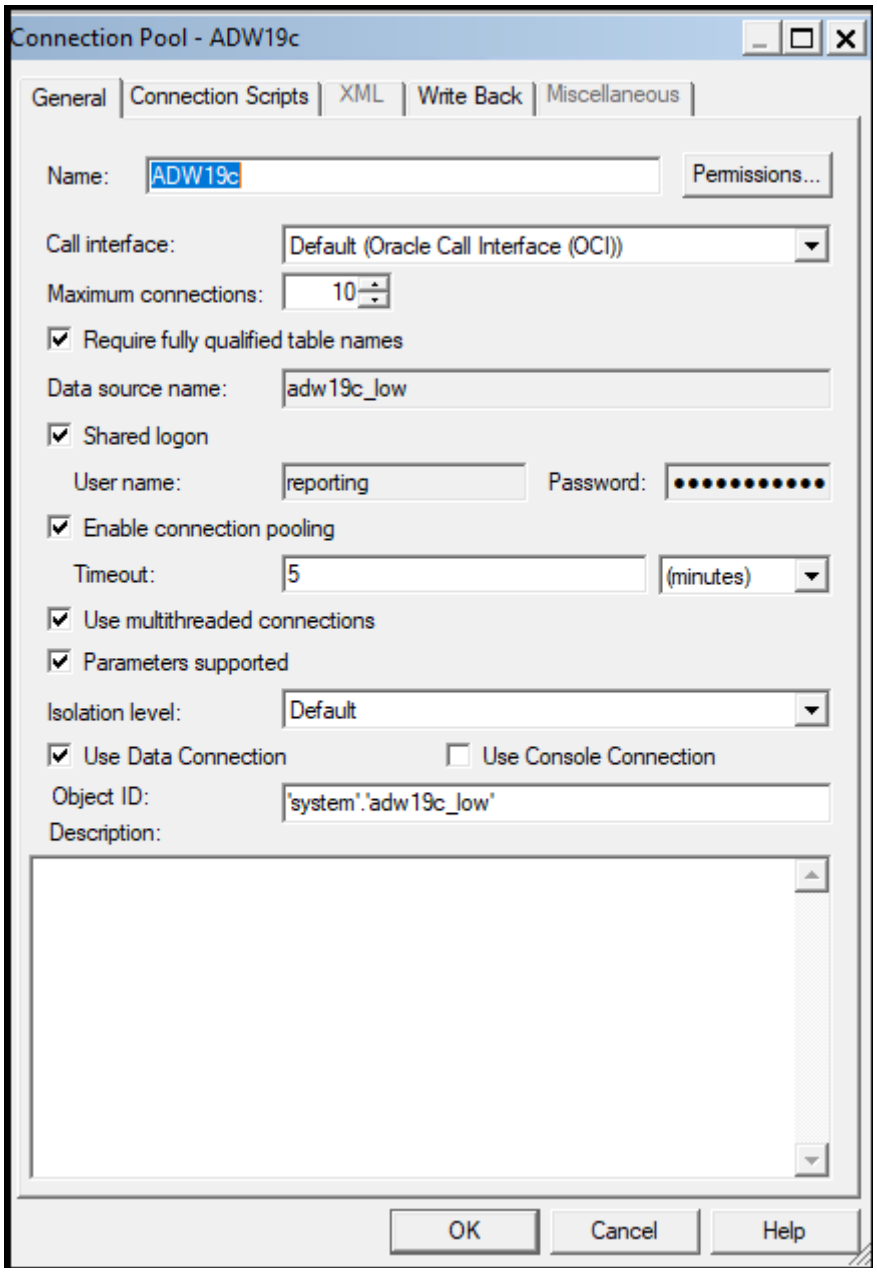
Region	Ashburn	Phoenix
Autonomous Database (ADW) – Sales db	ADW-19c	ADW-19c_Remote
ADW database service	adw_low (from wallet)	adw_low (from wallet)

Create a Connection to ADW in OAC Using a Wallet

1. In OAC, upload the wallet, enter the **Username** and **Password**, select **System connection**, and click **Save**.

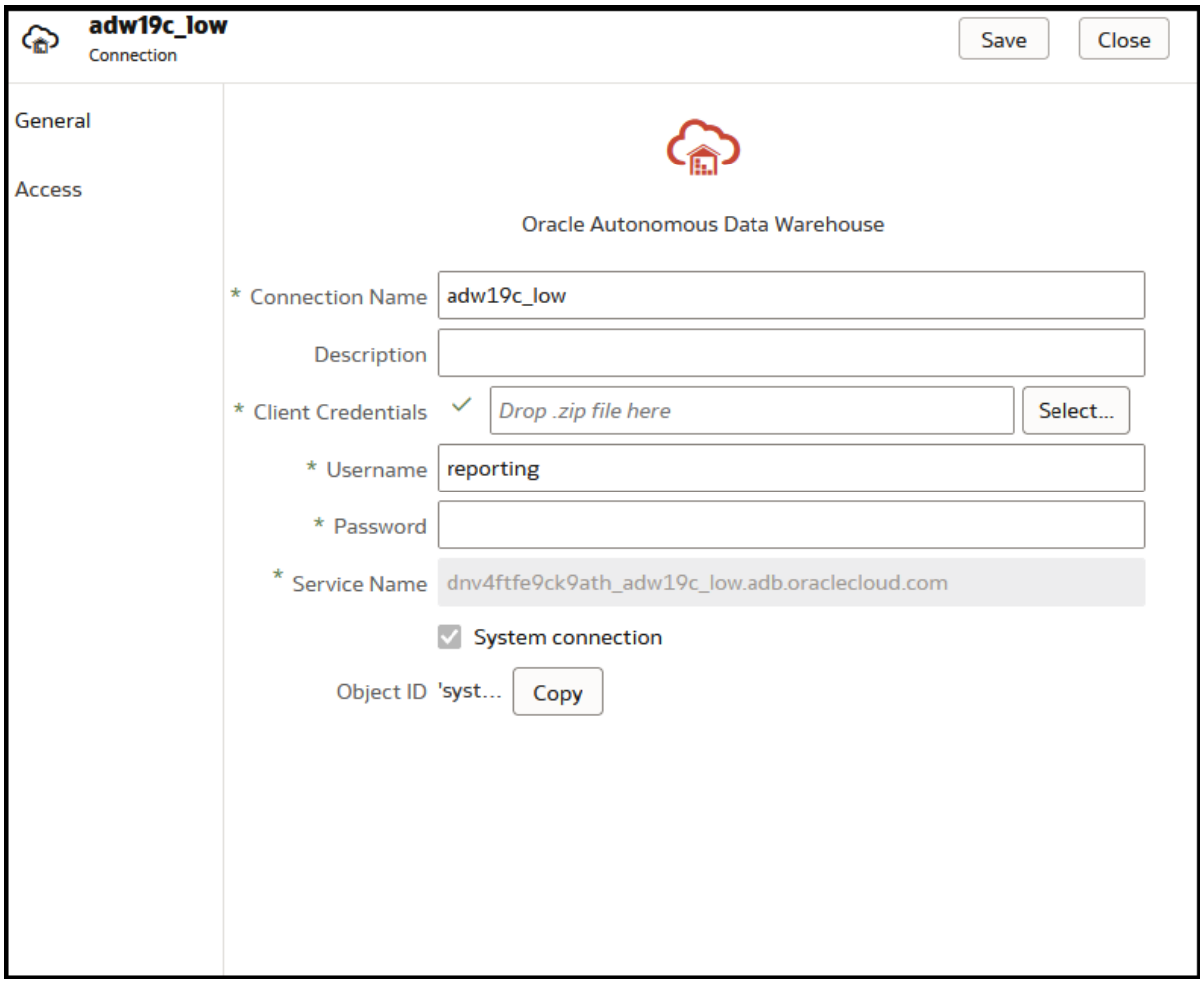


2. Click **Copy** to copy an **Object ID** that you can paste into your RPD.
3. In Model Administration Tool, for ADW connection pools, check the **Use Data Connection** option and paste the **Object ID** that you just copied.



See Connect to a Data Source Using a Data Connection.

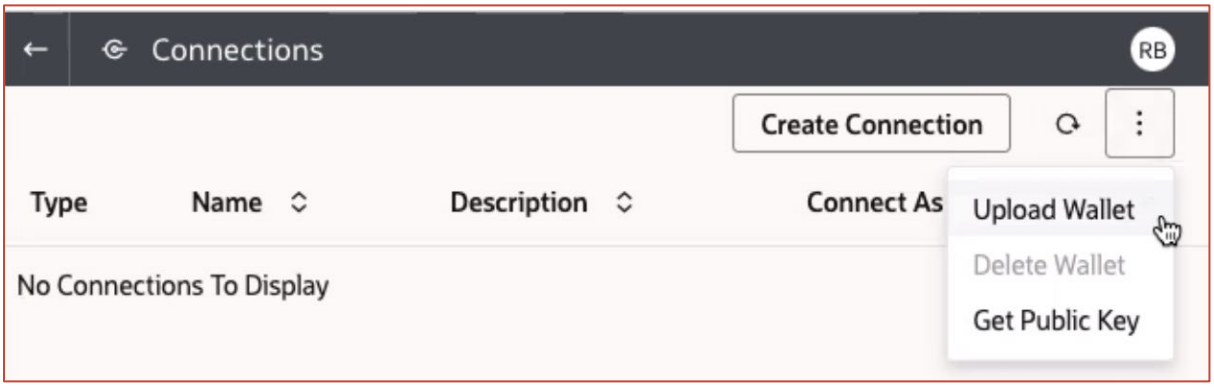
After the ADW switchover completes, update the wallet with the Phoenix ADW wallet and save the connection.



When you fallback to the OAC Ashburn instance, upload the wallet with the Ashburn ADW wallet (at the **Client Credentials** section for all the ADW connections), and save the connections on the Ashburn OAC instance.

Upload or replace the respective ADW wallets using the **Console → Connections** page in OAC. The wallet you upload here is used by semantic models (Data Modeler and RPD connection pools). Click either **Upload Wallet** to upload a wallet for the first time or **Replace Wallet** to update an existing one.

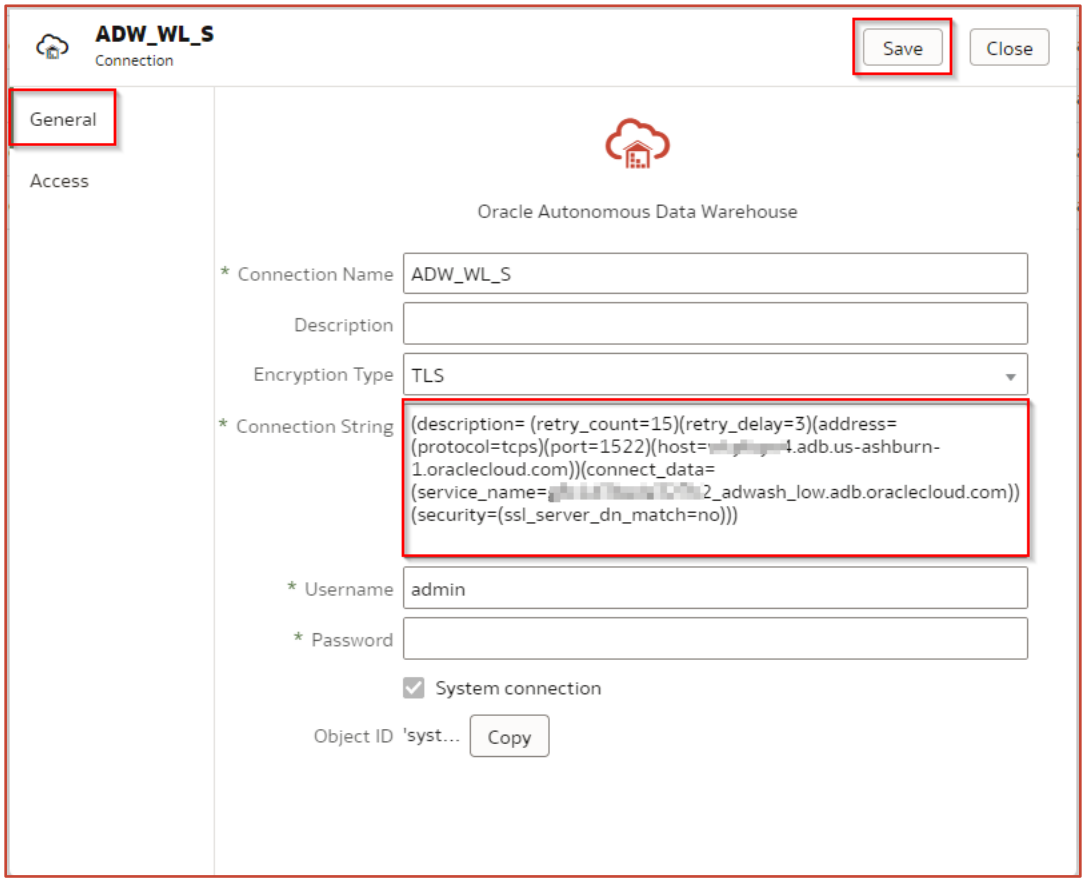
Click **Browse** and select the wallet file (`cwallet.sso`) from the unzipped ADW wallet folder.



ADW Wallet-less TLS Connection

For more details, see Securely Connecting to Autonomous DB Without a Wallet (Using TLS).

After restoring the primary OAC instance snapshot to the DR OAC instance, you need to modify the ADW wallet-less (TLS) connection string with the Phoenix ADW wallet-less (TLS) connection string.



Similarly, change the connection string after fallback from the DR OAC instance to the primary OAC instance.

Oracle Database Cloud Service as a Data Source

Create a primary Oracle Database on the Oracle Cloud home region while configuring Data Guard to the database. Create a Peer DB System as a standby database in the DR region.

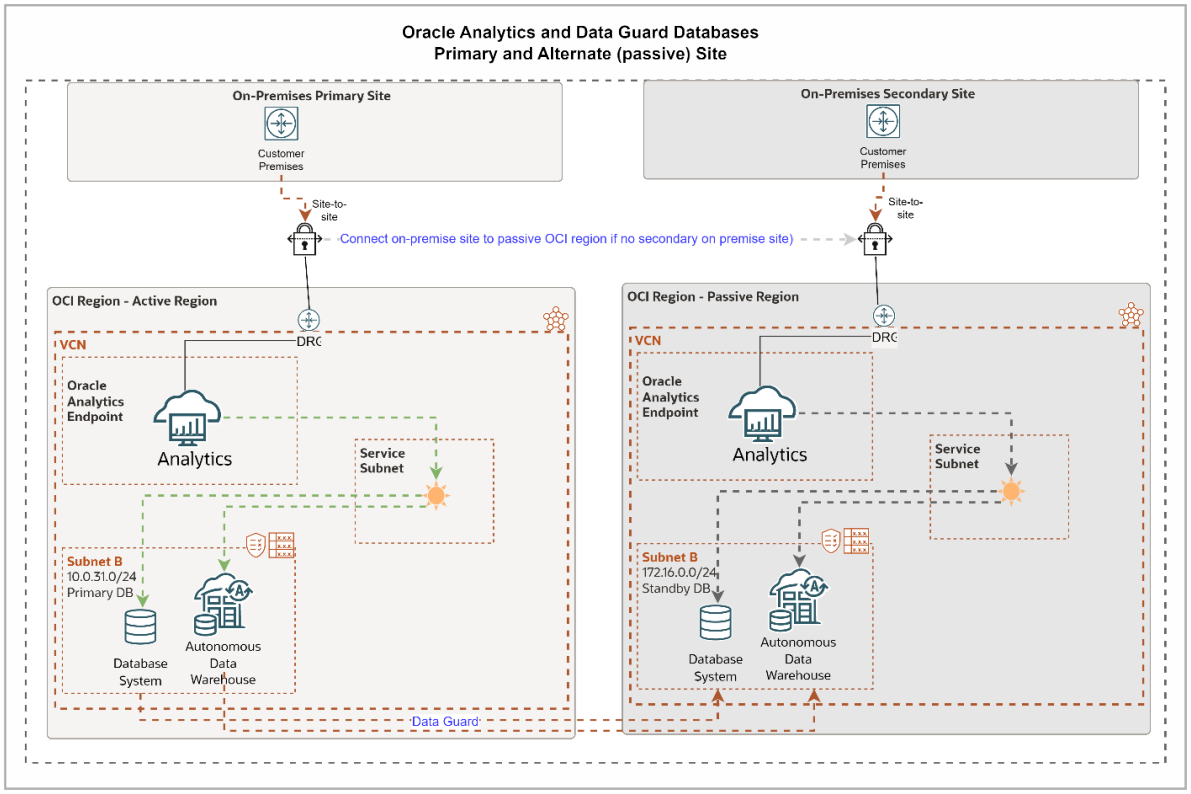
Using the Data Guard, replicate the primary database to the standby database and manage the failover too.

Refer to the following documentation and blogs for more information.

Use Oracle Data Guard on a DB System

Enable Oracle Data Guard on a DB System

https://docs.oracle.com/en-us/iaas/releasenotes/changes/83baf0ae-4352-41db-94eb-d0cb4d0058c5/



Oracle DBCS Already Configured with Different Hostnames and Service Names

While configuring the primary Oracle Database in the home region and the standby Oracle Database in the DR region, the hostnames and service names may differ. In such cases, the same connection string can't be used, which may require updating the connection string in the RPD or semantic model and the self-service data connections after restoring the snapshot and data files between the primary OAC instance and the DR OAC instance.

Example:

Primary Oracle Database Connection Details

- Hostname: oadb.sub12345678.oavcn.oraclevcn.com
- Port: 1521
- Servicename: PDB1.sub12345678.oavcn.oraclevcn.com
- Connection String: oadb.sub12345678.oavcn.oraclevcn.com:1521/PDB1.sub12345678.oavcn.oraclevcn.com

Standby Oracle Database Connection Details

- Hostname: oadbdr.sub87654321.dbvcn.oraclevcn.com
- Port: 1521
- Servicename: PDB1.sub87654321.dbvcn.oraclevcn.com
- Connection String: oadbdr.sub87654321.dbvcn.oraclevcn.com:1521/PDB1.sub87654321.dbvcn.oraclevcn.com

Test Environment

Region	Ashburn	Phoenix
Hostname	testdb-ash.oci.ash.oraclevcn.com	testdb-phx.oci.phx.oraclevcn.com
SCAN	testdb-ash-scan.oci.ash.oraclevcn.com	testdb-phx-scan.oci.phx.oraclevcn.com
Peer Databases – DBCS (HR db)	db_unique_name: testdb_iad instances: testdb1,testdb2	db_unique_name: testdb_phx1nx instances: testdb1,testdb2
DBCS database service	pdb1.mydomain.com	pdb1.mydomain.com

We recommend that you use a custom domain, such as **mydomain.com**, that is different from the DB_DOMAIN defined in the database so that the SERVICE_NAME is the same in both regions. If the domain is not specified in the srvctl command, the DB_DOMAIN is added automatically.

On the Primary DBCS Server:

```
srvctl add service -db testdb_iad -service "pdb1.mydomain.com" \
-preferred “testdb1,testdb2” -pdb testpdb  -notification TRUE \
-drain_timeout 300 -stopoption IMMEDIATE -role PRIMARY
```

On the Standby DBCS Server:

```
srvctl add service -db testdb_phx1nx -service "pdb1.mydomain.com" \
-preferred “testdb1,testdb2” -pdb testpdb -notification TRUE \
-drain_timeout 300 -stopoption IMMEDIATE -role PRIMARY
```

Use the Recommended DBCS Connection String for OAC to Enable Failover

JDBC URL Format Recommended for Connecting to DataGuard (Doc ID 2303116.1)

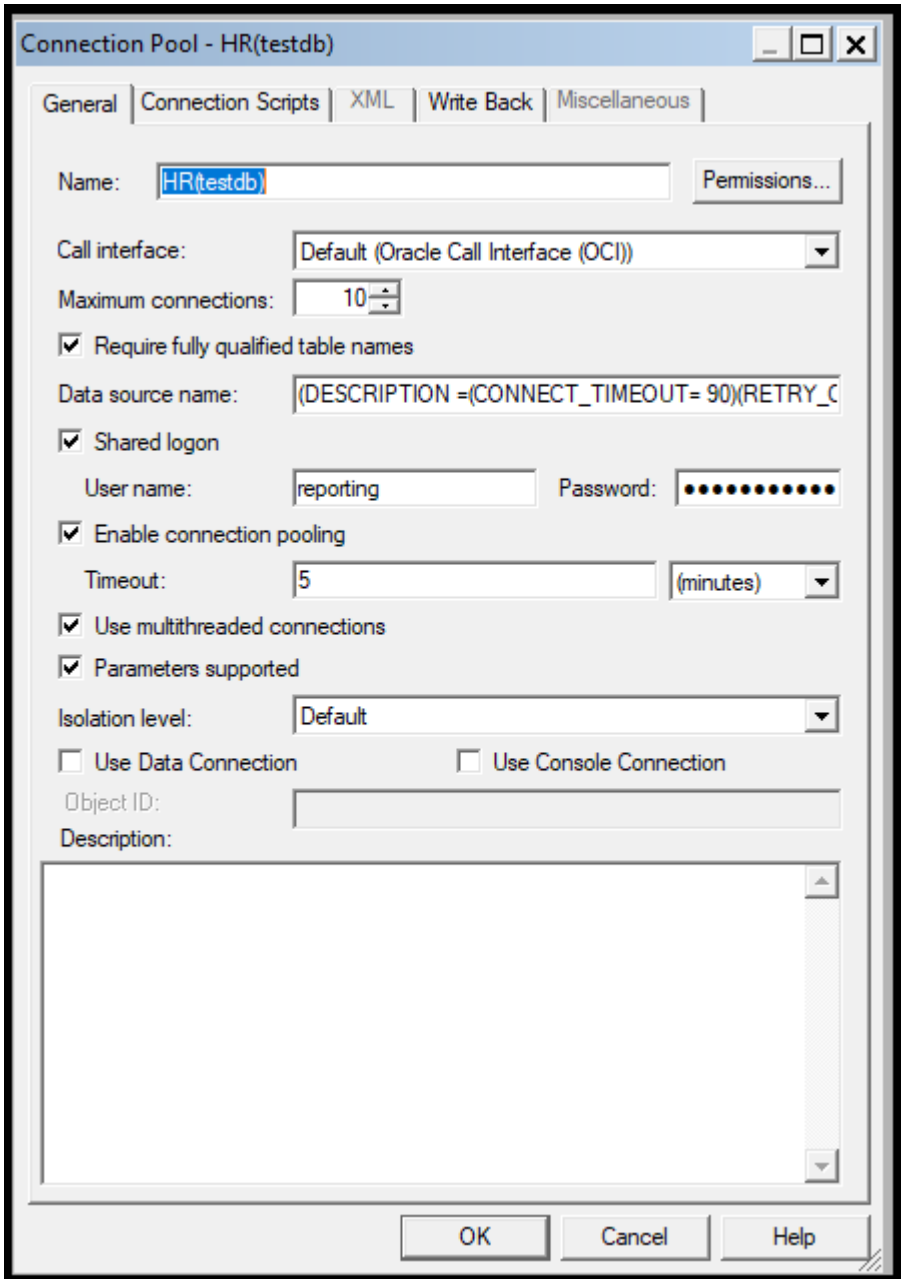
Application Checklist for Continuous Availability

```
(DESCRIPTION=(CONNECT_TIMEOUT=90)(RETRY_COUNT=3)(RETRY_DELAY=3)(TRANSPORT_CONNECT_TIMEOUT=3)(ADD
RESS_LIST=(LOAD_BALANCE=on)(ADDRESS=(PROTOCOL=tcp)(HOST=primary-scan)
(PORT=1521)))(ADDRESS_LIST=(LOAD_BALANCE=on)(ADDRESS=(protocol=tcp) (host=secondary-scan)
(PORT=1521)))(CONNECT_DATA=(SERVICE_NAME = pdb1.mydomain.com)))
```

Test Using SQL*Plus:

```
sqlplus
username/password@"(DESCRIPTION=(CONNECT_TIMEOUT=90)(RETRY_COUNT=3)(RETRY_DELAY=3)(TRANSPORT_CON
NECT_TIMEOUT=3)(ADDRESS_LIST=(LOAD_BALANCE=on)(ADDRESS=(PROTOCOL=tcp)(HOST=primary-scan)
(PORT=1521)))(ADDRESS_LIST=(LOAD_BALANCE=on)(ADDRESS=(protocol=tcp) (host=secondary-
scan)(PORT=1521)))(CONNECT_DATA=(SERVICE_NAME = pdb1.mydomain.com)))"
```

Provide the DBCS Connection String in the RPD DSN



The above connection string uses a common Service Name as we configured a custom domain but still uses a different SCAN address.

Alternatively, create a private zone in DNS. Creating a private zone in DNS simplifies the connection string to a single scan name. DNS will resolve the private zone scan name to the DBCS scan name based on the region. Be sure to add the private zone and DBCS scan to the PAC.

Networking → DNS Management → Zones (choose private tab) → Create Zone (for example **ceal.com**)

Add CNAME for **testdb-scan.ceal.com** and map to the real scan name (note this will be different for each region based on the original scan name).

Repeat this for both regions.

1. Create a private zone (for example, **ceal.com**) in the VCN Private View for the home region and DR region.
2. Add an “A-Record” in the private zone for **testdb.ceal.com** mapped to the primary Oracle Database IP address.
3. Repeat the same for the DR region (testdb.ceal.com == Secondary Oracle Database IP address).
4. If you have a SCAN address such as **testdb-ash-scan.oci.ash.oraclevcn.com**, create a CNAME record and map the **testdb-scan.ceal.com** to **testdb-ash-scan.oci.ash.oraclevcn.com**.
5. Repeat the same for the DR region. For example, if you have a SCAN address such as **testdb-phx-scan.oci.phx.oraclevcn.com**, create a CNAME record, and map the **testdb-scan.ceal.com** to **testdb-phx-scan.oci.phx.oraclevcn.com**.

After this workaround, we have the same connection string for the primary and standby Oracle Databases:

- testdb.ceal.com:1521/pdb1.mydomain.com
- testdb-scan.ceal.com:1521/pdb1.mydomain.com

Update the Connection String in the RPD to Reflect the Private Zone Scan Name

```
(DESCRIPTION=(CONNECT_TIMEOUT=90) (RETRY_COUNT=3) (RETRY_DELAY=3) (TRANSPORT_CONNECT_TIMEOUT=3)
(ADDRESS_LIST=(LOAD_BALANCE=on) (ADDRESS=(PROTOCOL=tcp) (HOST=testdb-scan.ceal.com)
(PORT=1521))) (CONNECT_DATA=(SERVICE_NAME = pdb1.mydomain.com)))
```

Add the Private Zone to the PAC

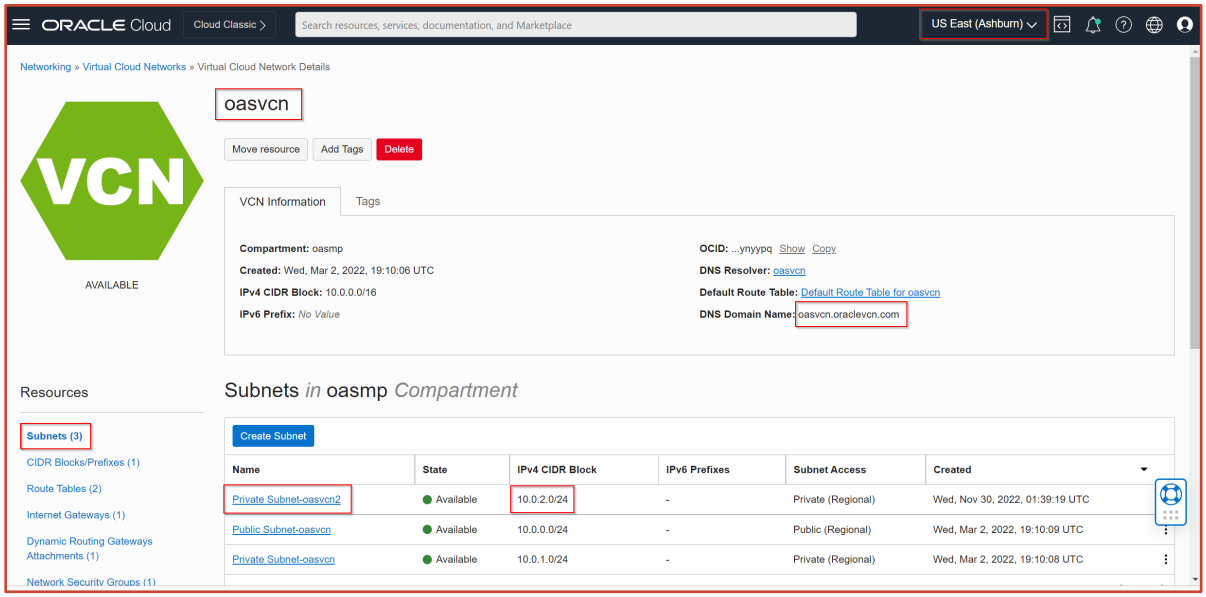
After snapshot migration, this workaround prevents you from needing to modify connection pools or connections in the RPD and OAC.

Create Oracle DBCS with the Same Hostnames and Service Names

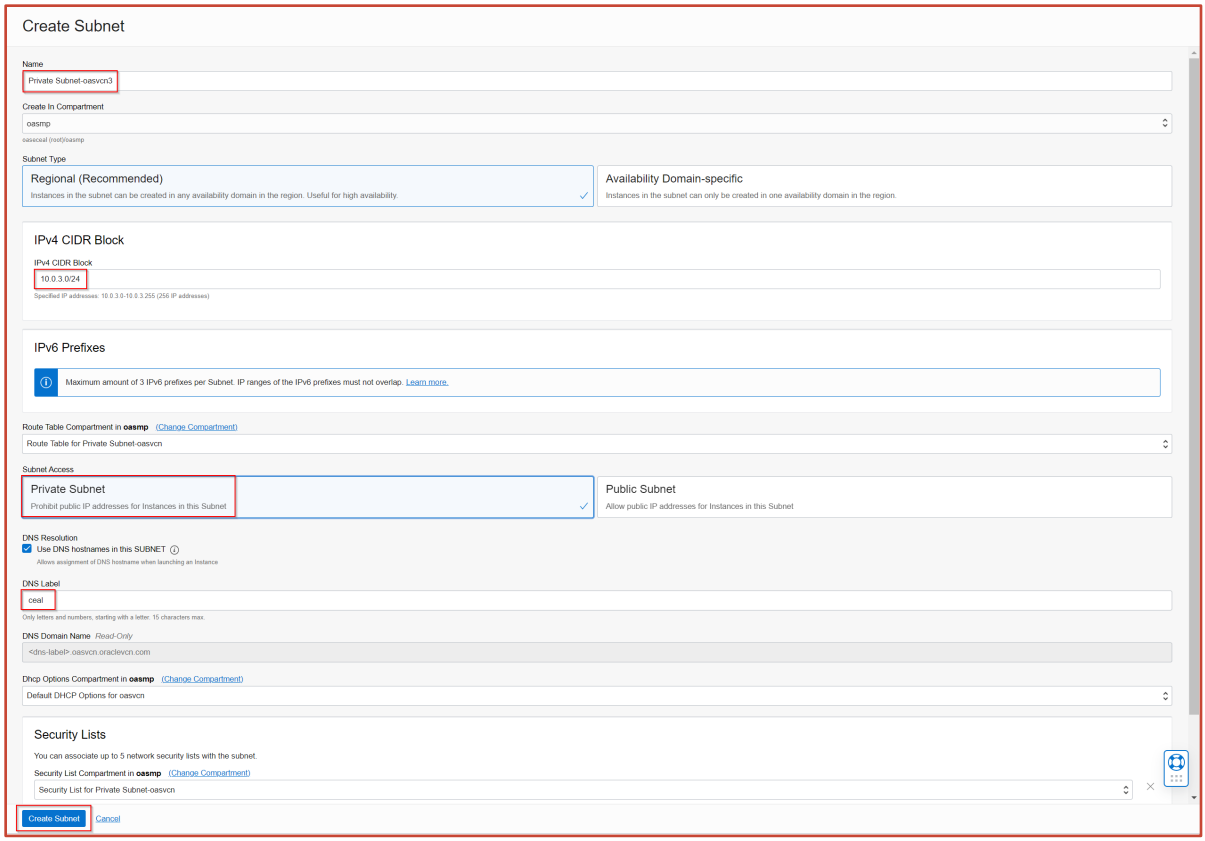
Another option is to create a VCN with the same name in both OCI regions or utilize an existing VCN with the same name in both OCI regions. Additionally, it's necessary to manually create a subnet with the same DNS label to ensure consistent service name resolution across the DR environment.

For example, the domain name can be **ceal.oasvcn.oraclevcn.com**.

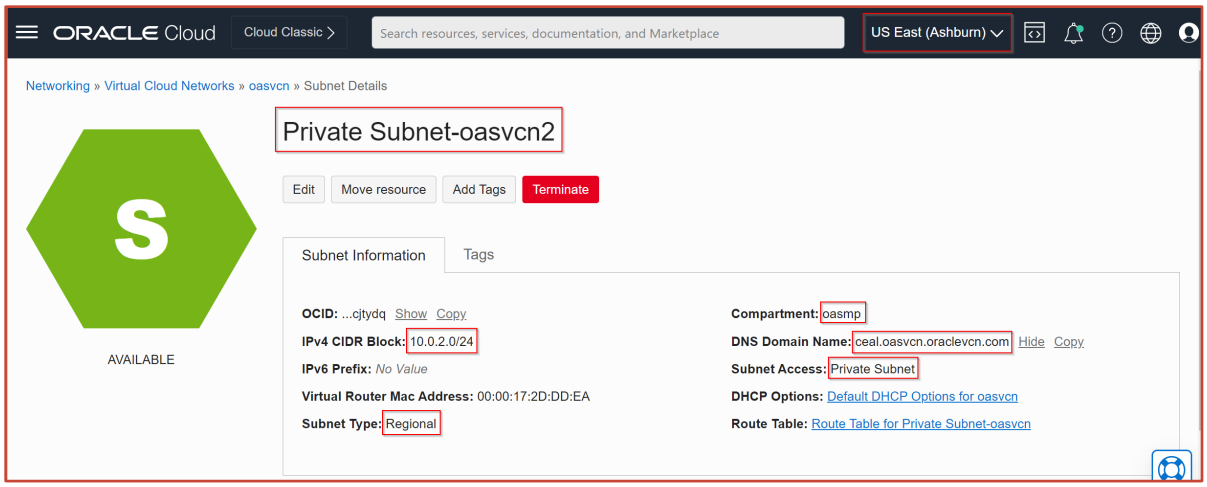
1. Sign in to the OCI Console.
2. Navigate to **Networking → Virtual Cloud Networks → Select Compartment (for example, oasmp) → Create a VCN or use Existing VCN (for example, oasvcn) → Subnets**.

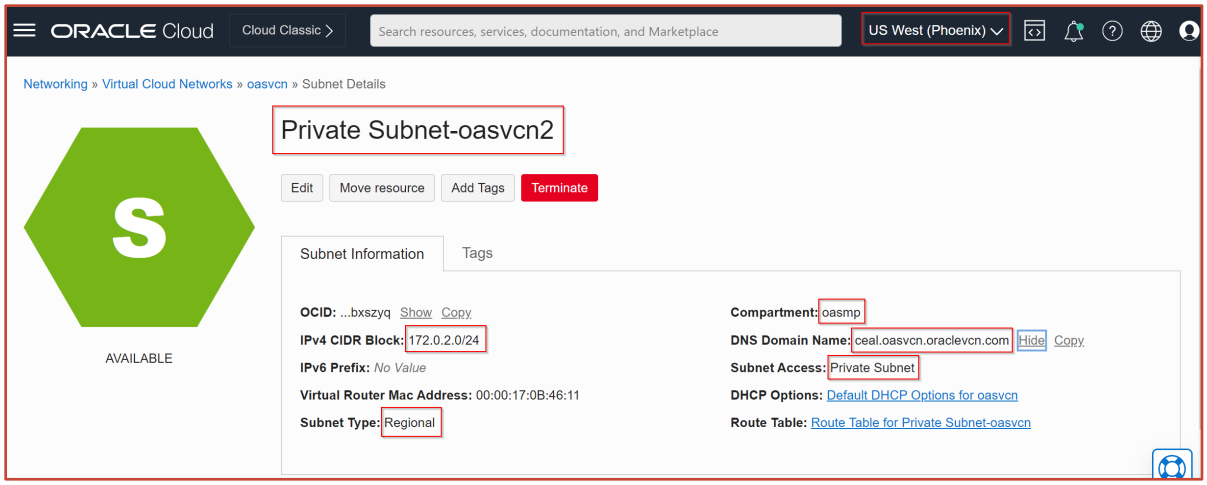


3. Create a private subnet. See the sample screenshot.



4. Similarly, in the DR region in the same compartment, create the same VCN (for example, **oasvcn**) and create a private subnet with the same DNS Label (for example, **ceal**).





Create the primary Oracle Database on this VCN and the private subnet.

When configuring the Data Guard, we recommend that you create the standby Oracle Database with the same VCN name and private subnet as the primary Oracle Database.

Connection strings for this example:

```
oadb.ceal.oasvcn.oraclevcn.com:1521/PDB1.ceal.oasvcn.oraclevcn.com
```

```
oadbdr.ceal.oasvcn.oraclevcn.com:1521/PDB1.ceal.oasvcn.oraclevcn.com
```

Since the hostnames of the primary and standby databases will not match, we recommend using the following workaround to address this issue:

1. Create a private zone (for example, ceal.oracle.com) in the VCN private view for the home and DR regions.
2. Add an “A-Record” in the private zone for oadb.ceal.oracle.com mapped to the primary Oracle Database IP address.
3. Repeat for the DR region.
4. If you have multiple nodes and so have a SCAN address such as oadb-scan.ceal.oasvcn.oraclevcn.com, create a CNAME record and map oadb-scan.ceal.oracle.com to oadb-scan.ceal.oasvcn.oraclevcn.com.
5. Repeat for the DR region.

By applying the workaround, you obtain the same connection string for both the primary and standby Oracle databases, as shown in this example:

```
oadb.ceal.oracle.com:1521/PDB1.ceal.oasvcn.oraclevcn.com
```

```
oadb.ceal.oracle.com:1521/PDB1.ceal.oasvcn.oraclevcn.com
```

After snapshot migration, this workaround prevents you from needing to modify connection pools or connections in the RPD and OAC.

PAC and RDG Configuration to Connect to Data Sources

This section outlines how to access the same data sources from the OAC instances in both regions. This document doesn't describe how to configure PAC or RDG.

Private Access Channel (PAC)

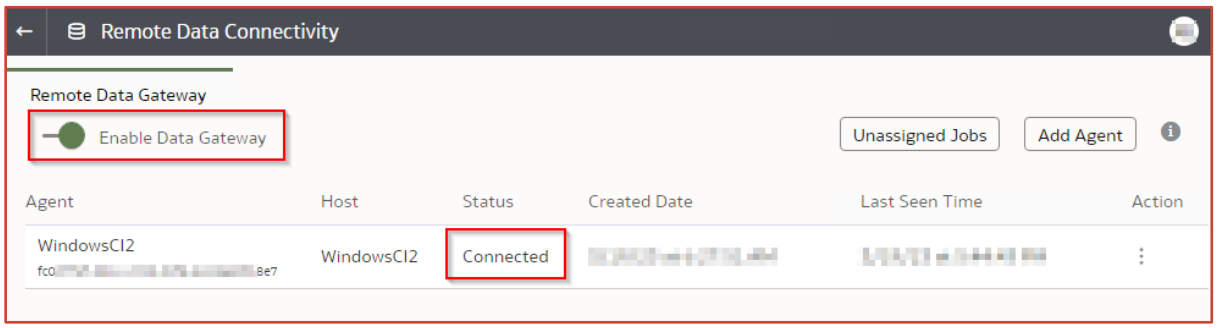
See Connect to Private Data Sources Through a Private Access Channel.

Allowlist the PAC egress IP addresses at the on-premises firewall for both OAC instances.

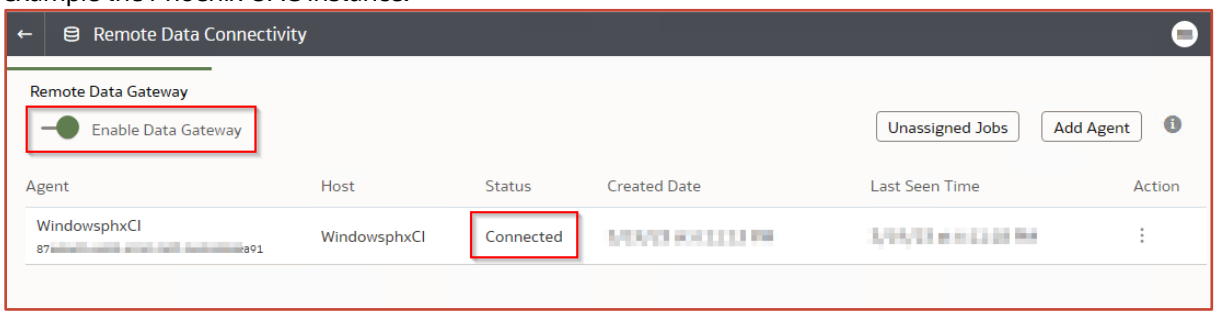
Remote Data Gateway (RDG)

See Connect to On-premise Data Sources Using Data Gateway.

Install the Data Gateway agent on the on-premises server and register the agent with the home region, for example the Ashburn OAC instance.

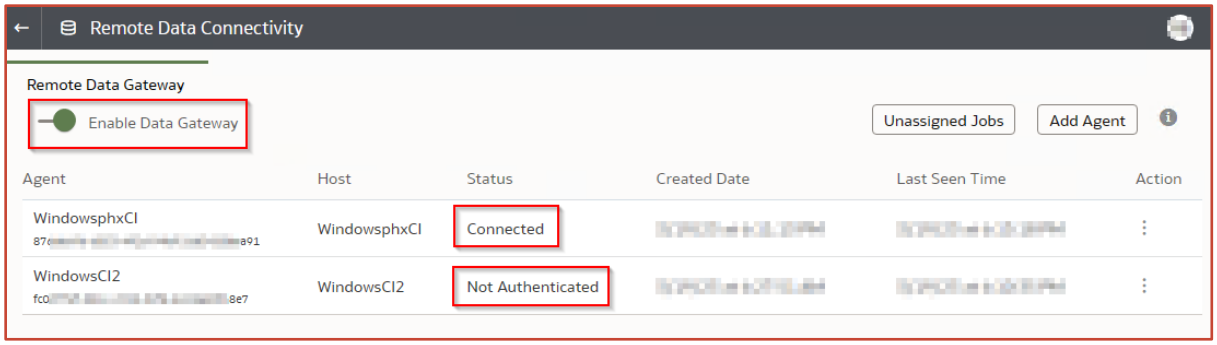


Similarly, install the Data Gateway agent on the on-premises server and register the agent with the DR region, for example the Phoenix OAC instance.



When you restore the snapshot of the primary OAC instance on the DR OAC instance, the Data Gateway agents of both the primary and DR instances will appear on the remote data connectivity page of the DR OAC instance.

The DR OAC instance displays the status of its Data Gateway agent as '`Connected`' and the status of the primary instance's data gateway agent as '`Not Authenticated`.'



If needed, the OAC administrator can delete any unnecessary Data Gateway agents. Having both Data Gateway agents in an OAC instance is not an issue, as only the region-specific Data Gateway agent is connected at any given time.

Create Object Storage Buckets in Each OCI Region

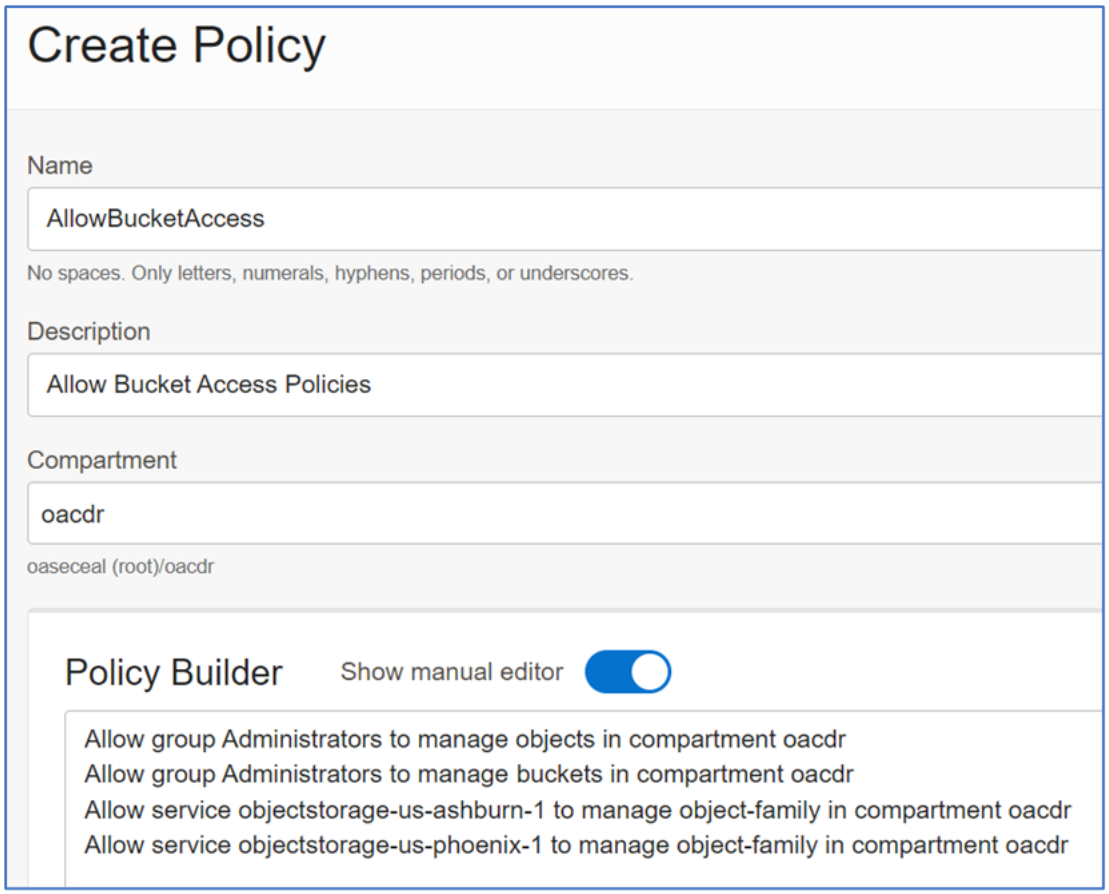
See Set Up an Oracle Cloud Storage Bucket for Snapshots.

Create Policies in the Compartment to Access the Buckets

Since the compartment is not regional, create policies for the compartment in the tenancy.

1. Create a compartment or use an existing compartment.
2. Create policies for the compartment.
   a. Log in to the OCI Console.
   b. Navigate to **Identity & Security → Policies → Select the Compartment → Create Policy**.
   c. Add the policies shown:

- Allow group Administrators to manage objects in compartment oacdr
- Allow group Administrators to manage buckets in compartment oacdr
- Allow service objectstorage-us-ashburn-1 to manage object-family in compartment oacdr
- Allow service objectstorage-us-phoenix-1 to manage object-family in compartment oacdr

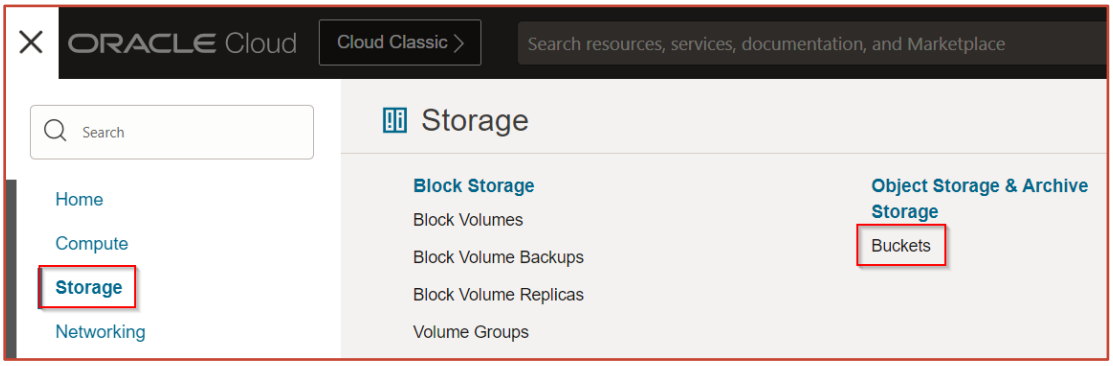


Create a Bucket in the Compartment Where the Policies are Set Up

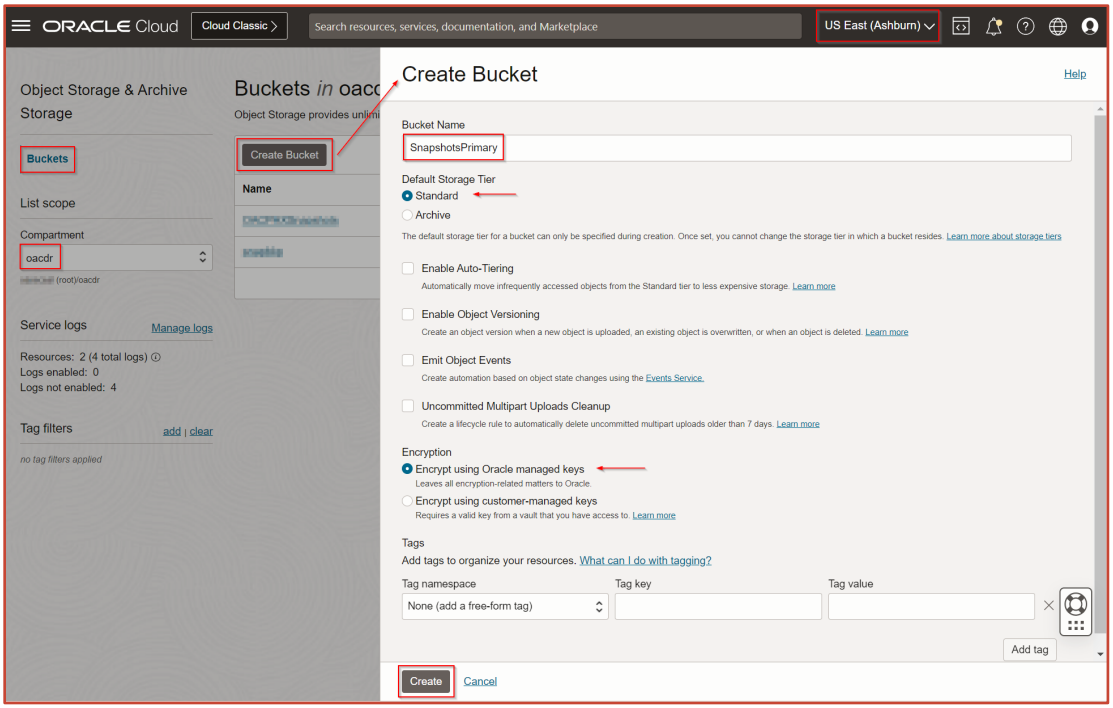
On the OCI Home Region (Ashburn)

Create a bucket in the home region (for example Ashburn), and enable the **Replication of the Bucket to the Destination Region** as the DR region (for example, Phoenix).

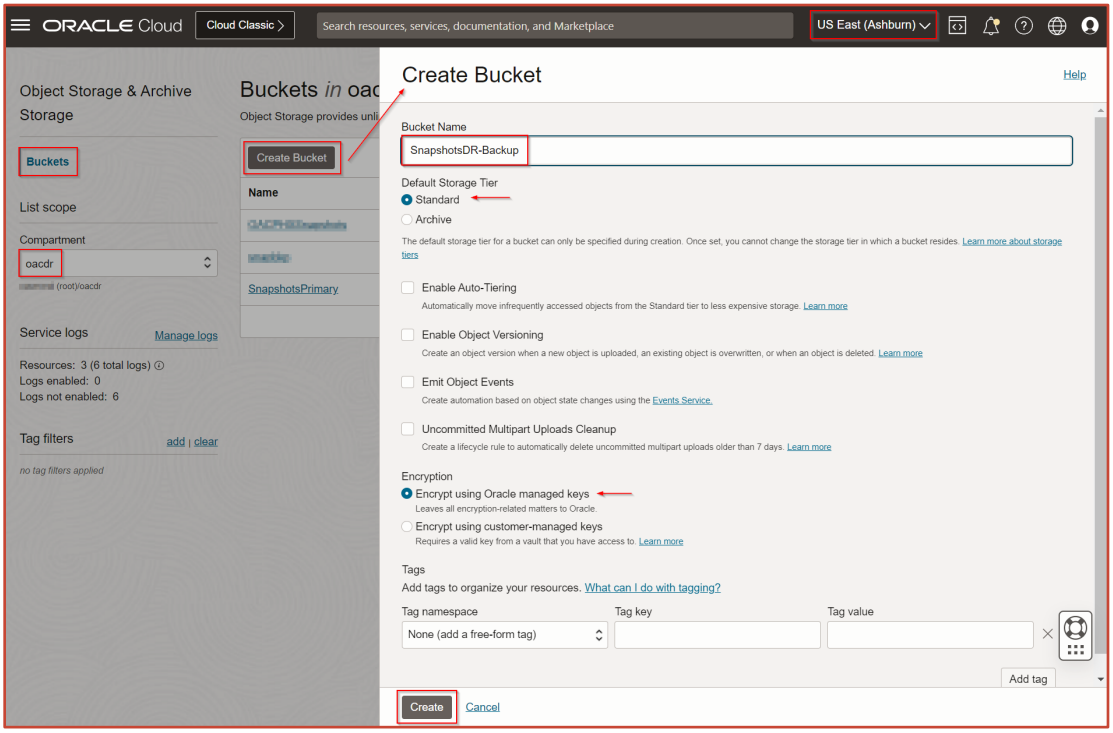
1. Create an object storage bucket in the home region to store snapshots from the home region OAC instance.



2. Create a bucket with a name such as **SnapshotsPrimary**.



3. Create another bucket in the home region for the backup of the DR region. For example, a bucket with a name such as **SnapshotsDR-Backup**.

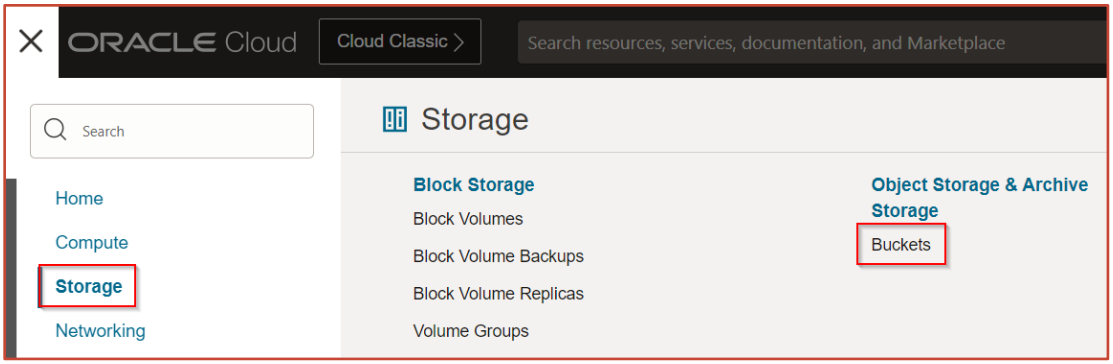


This is required if you need to create a snapshot at the DR OAC instance and restore it at the primary OAC instance during fallback.

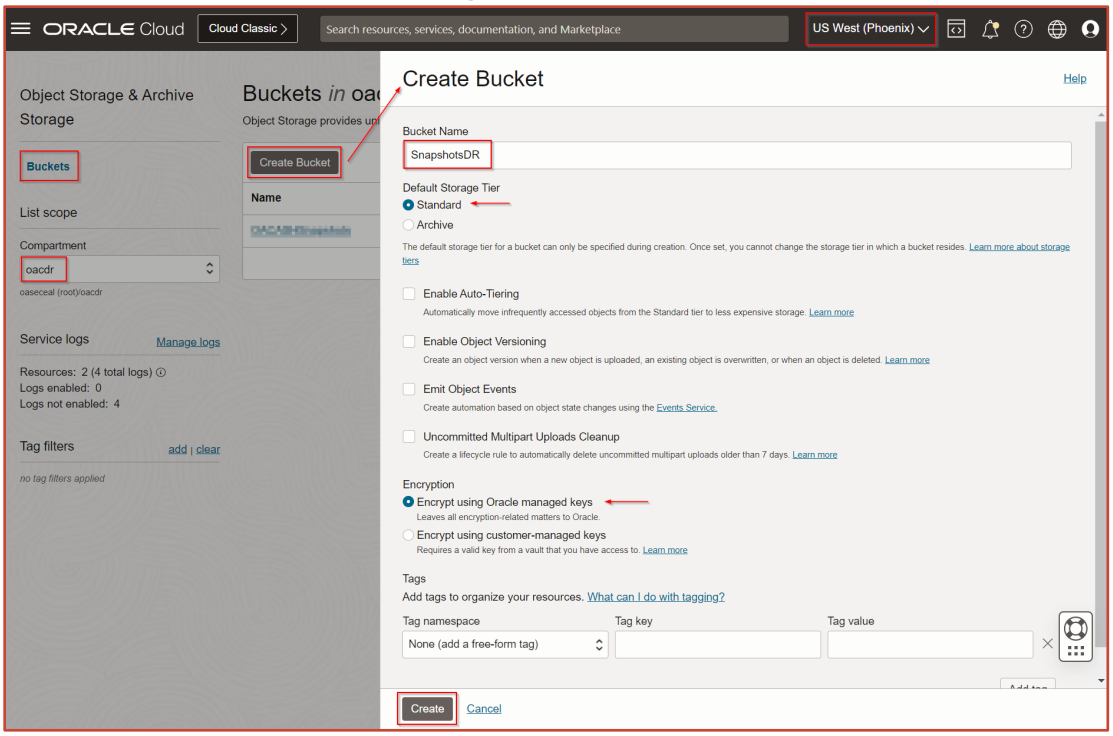
On the OCI Disaster Recovery Region (Phoenix)

Create another bucket in the DR region (for example, Phoenix), and enable the **Replication of the Bucket to the Destination Region** as the home region (for example, Ashburn).

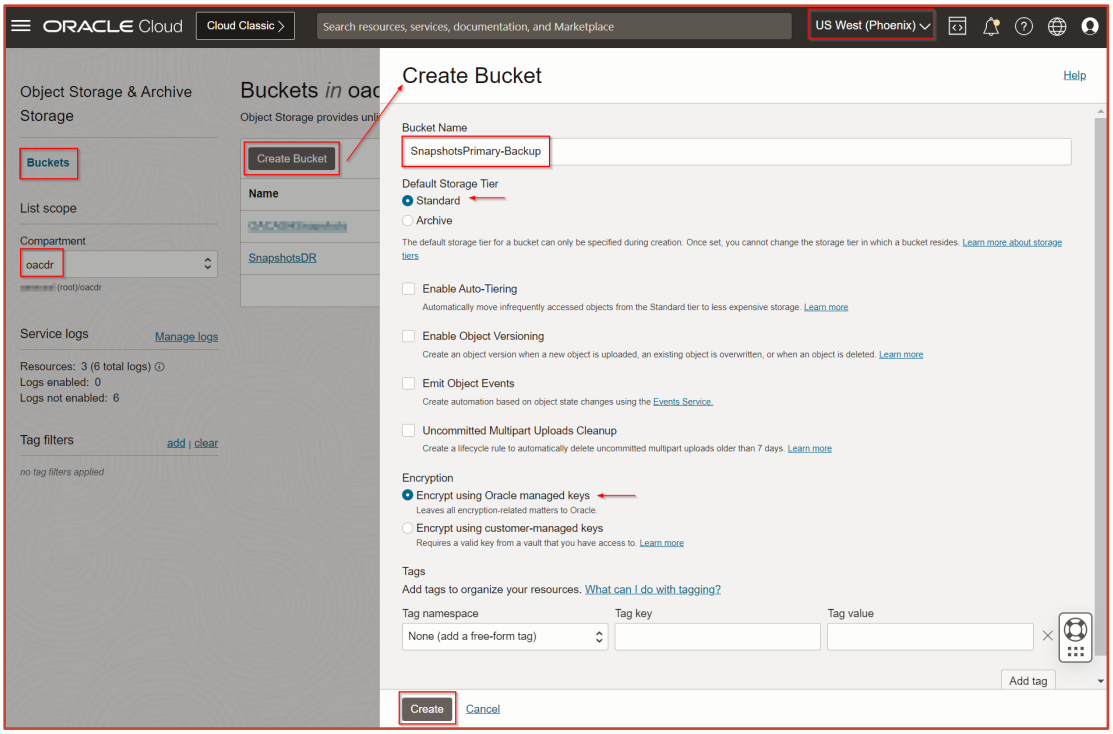
1. Create an object storage bucket in the DR region to store snapshots from the DR region OAC instance.



2. Create a bucket with a name such as **SnapshotsDR**.



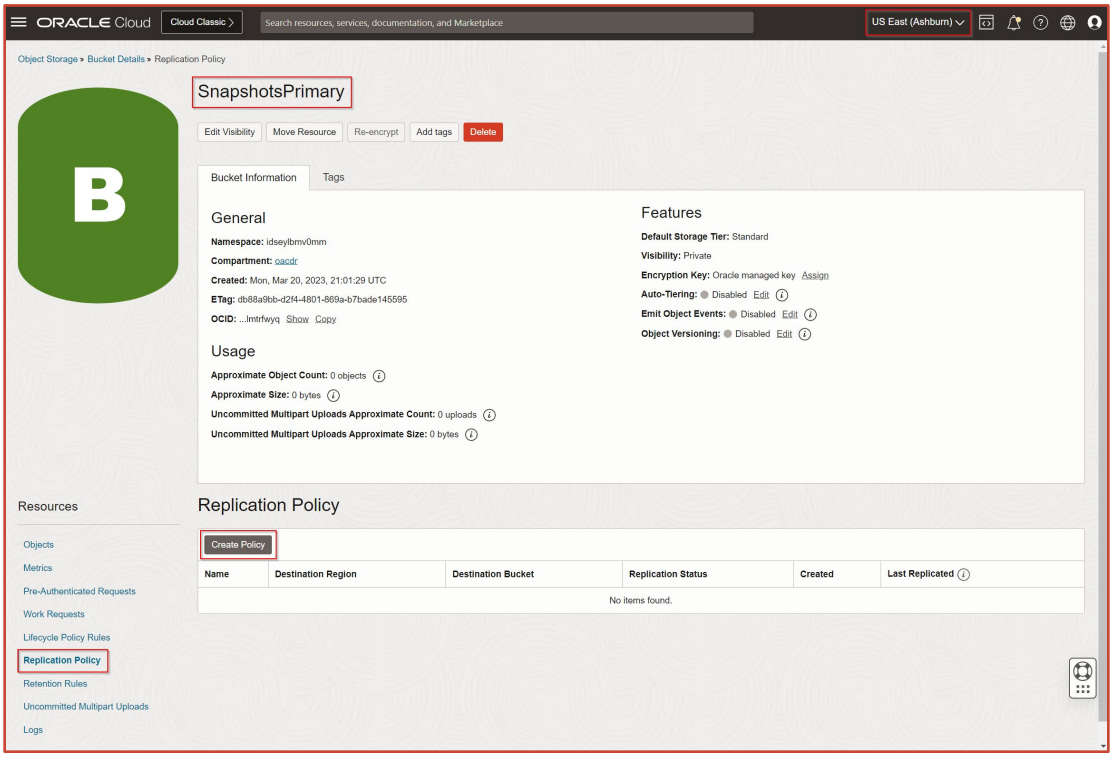
3. Create another bucket in the DR region for the backup of the home region bucket. For example, a bucket with a name such as **SnapshotsPrimary-Backup**.



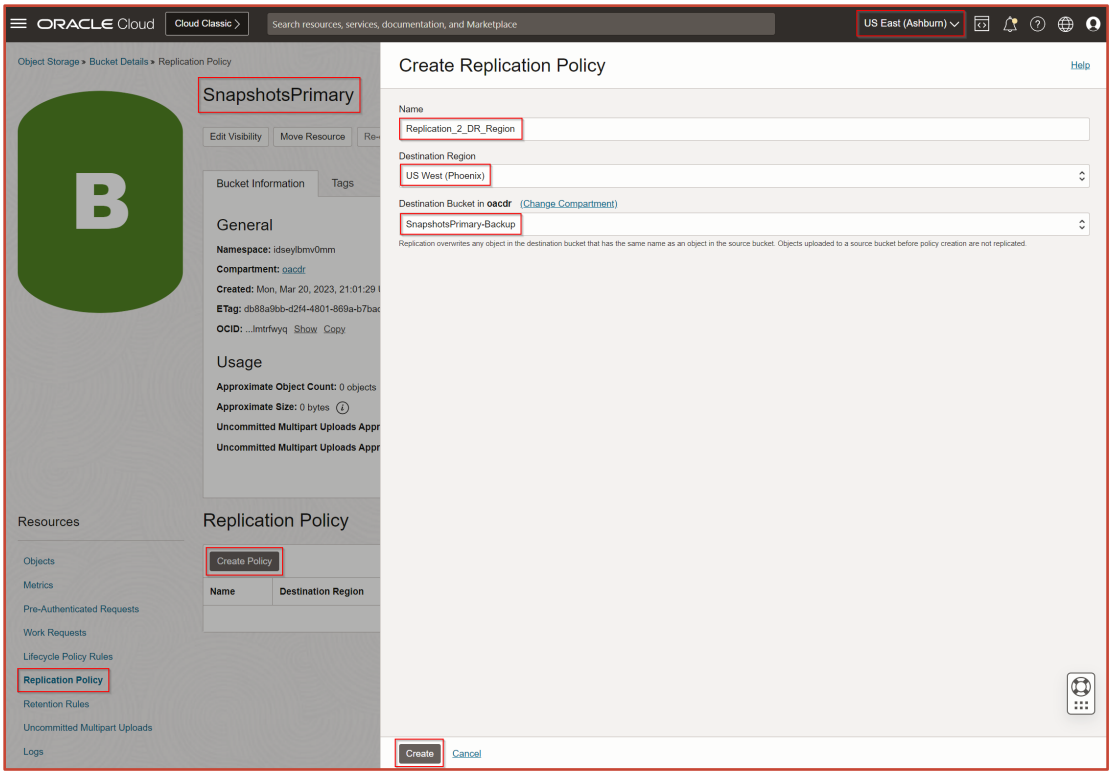
Enable Replication

On the OCI Home Region (Ashburn)

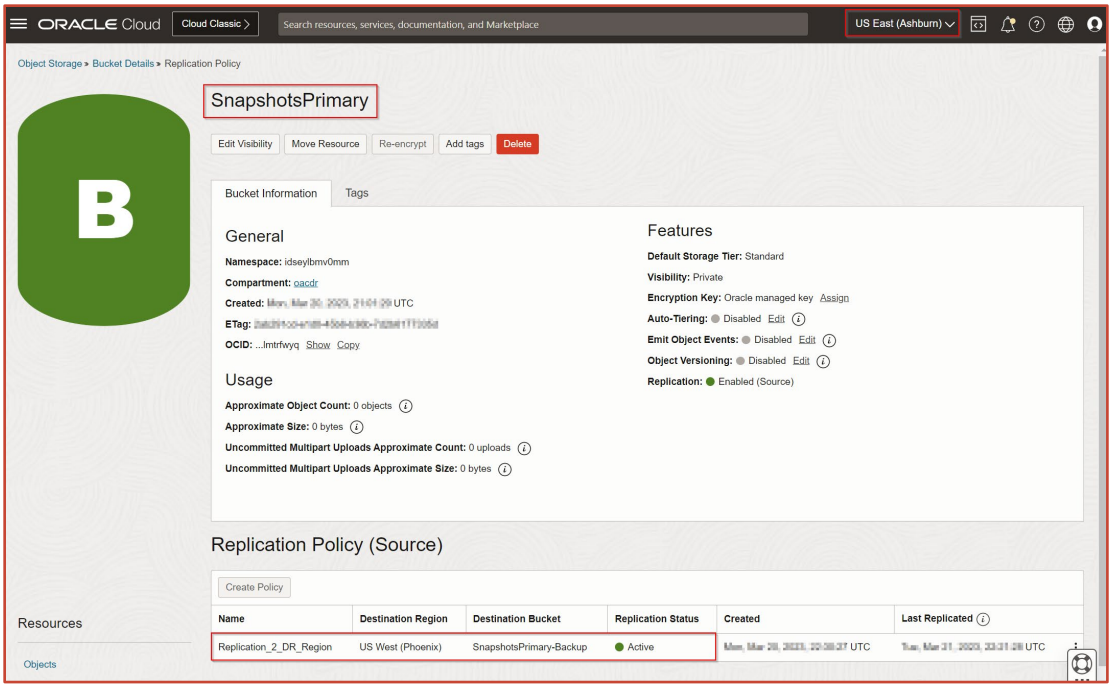
1. Create the replication policy for the bucket created in the home region.



2. Select the destination region as the DR region and the destination bucket as “**SnapshotsPrimary-Backup**“.

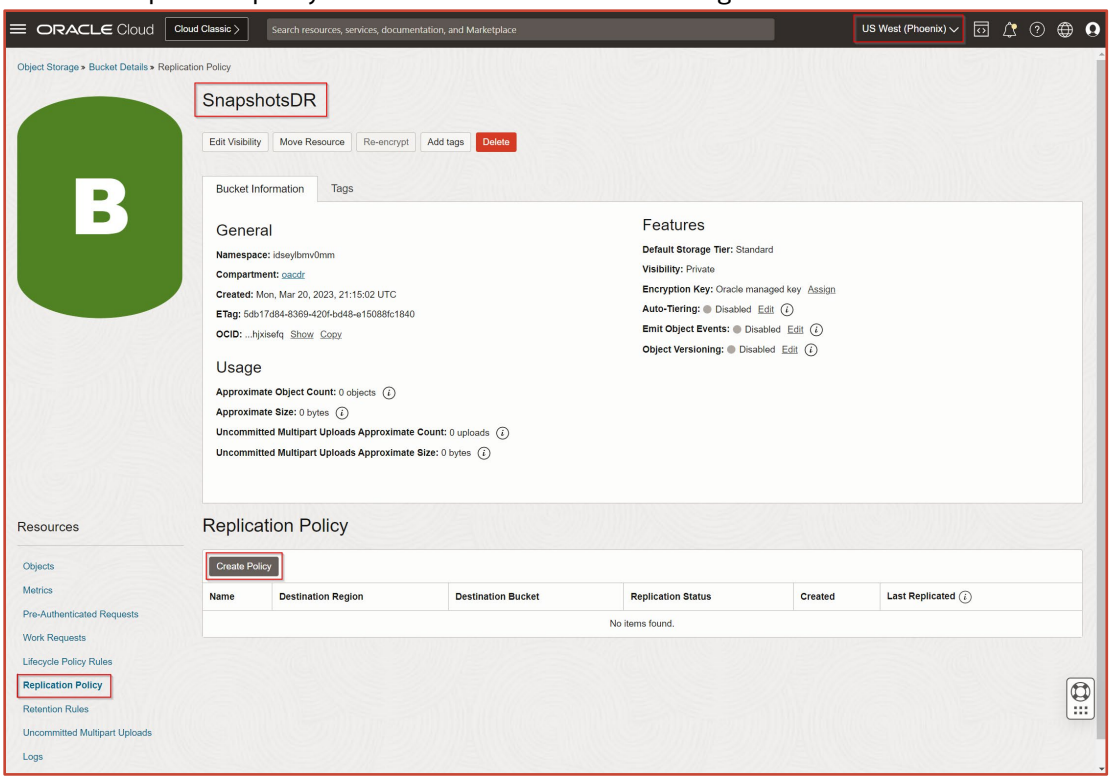


The replication policy is enabled.

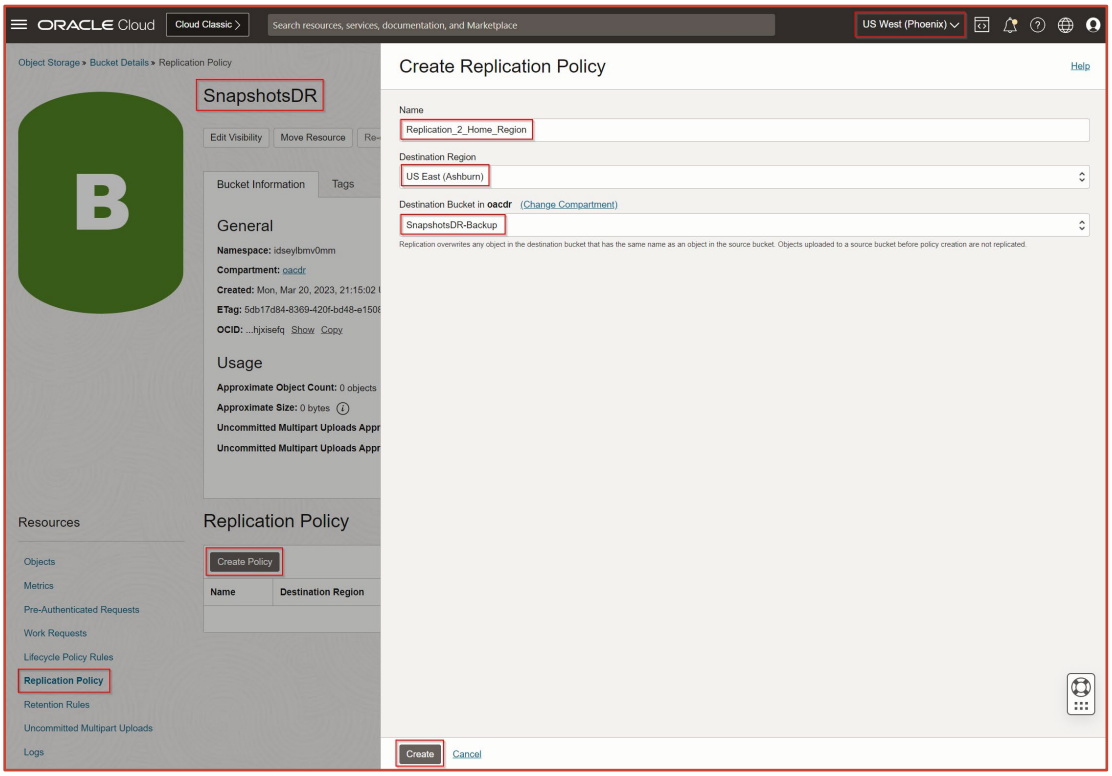


On the OCI Disaster Recovery Region (Phoenix)

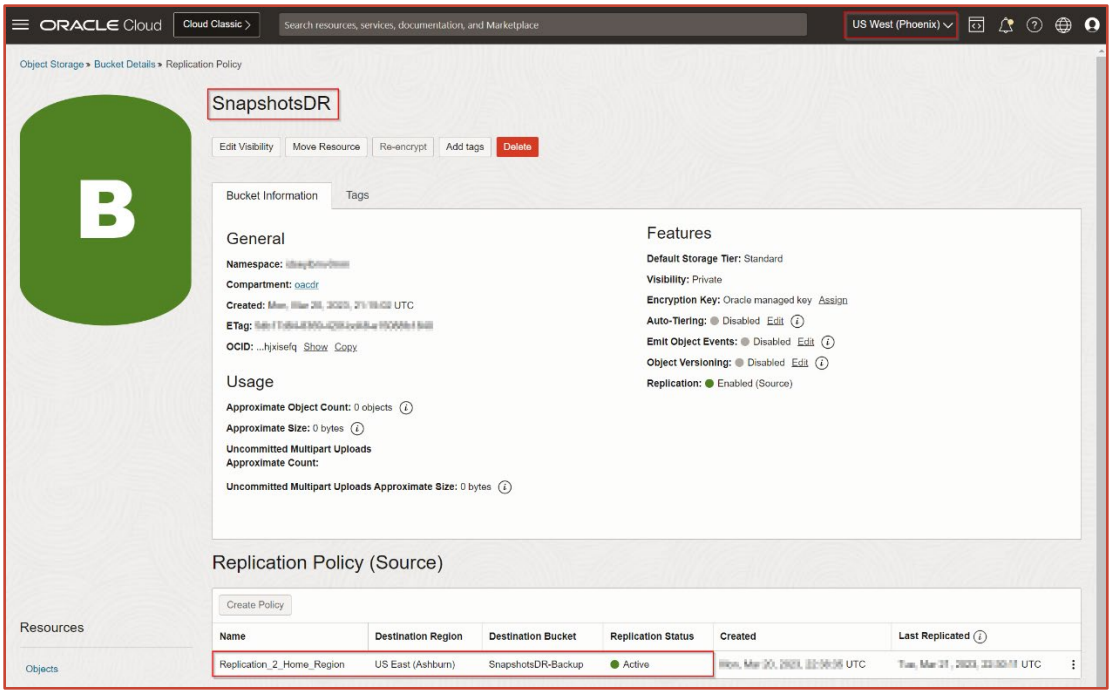
1. Create the replication policy for the bucket created in the DR region.



2. Select the destination region as the home region and the destination bucket as "**SnapshotsDR-Backup**".



The replication policy is enabled.



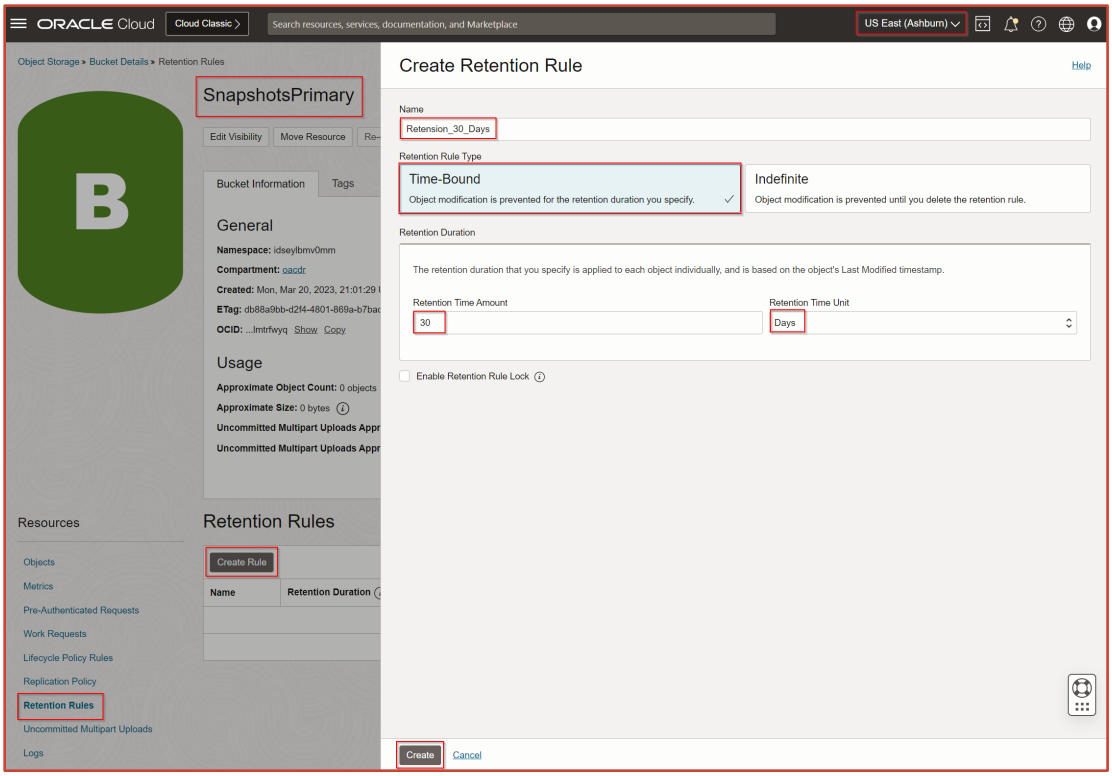
Create Retention Rule

To ensure that backup files are held for a specific period, create a retention rule (for example, 30 days). This retention rule keeps the backup files for 30 days, after which the system automatically deletes them.

On the OCI Home Region (Ashburn)

Create a retention rule that keeps backup files for 30 days, and then archives them using lifecycle policy rules.

1. Log in to the OCI Console.
2. Select the home region. For example, US East (Ashburn).
3. Navigate to **Storage → Buckets → Select the Compartment → Select the bucket created for OAC home region snapshots (SnapshotsPrimary)**.
4. In the Resources Section, click **Retention Rules → Create Rule**.
5. Create a Time-Bound rule for 30 days.

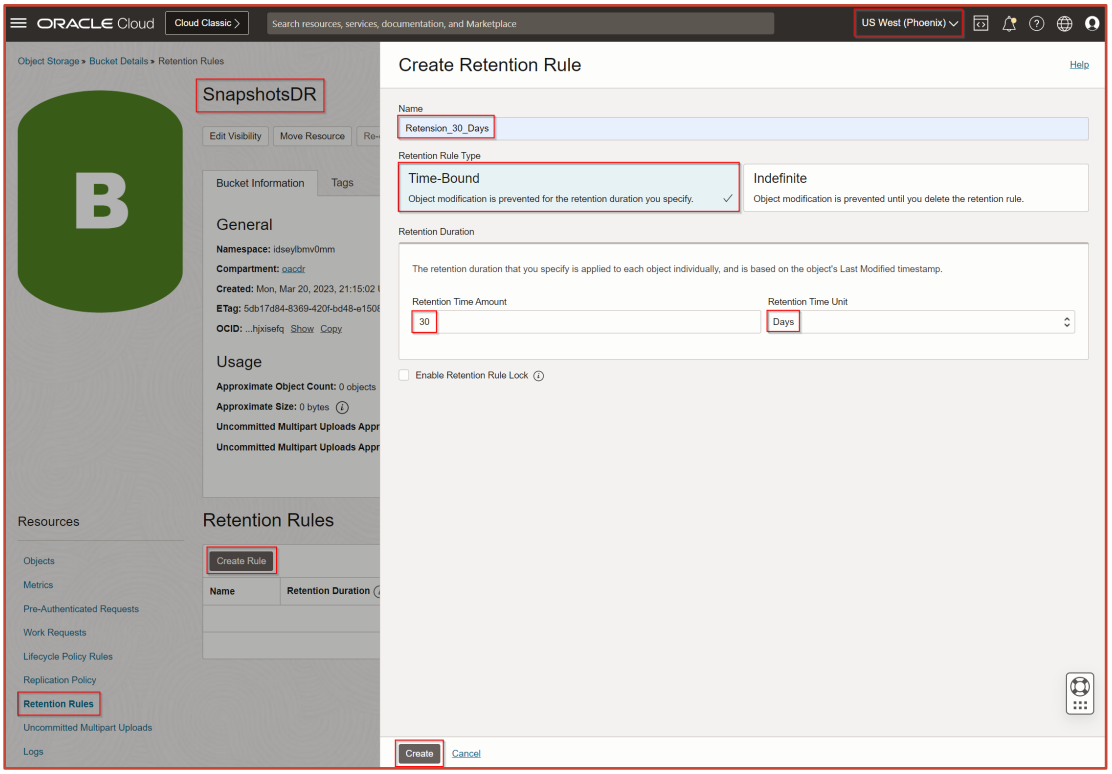


On the OCI Disaster Recovery Region (Phoenix)

Create a retention rule that keeps backup files for 30 days.

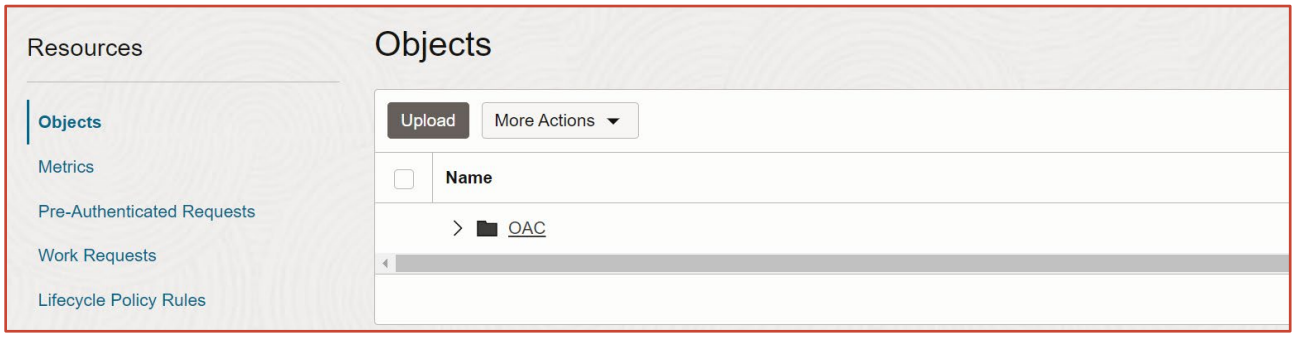
1. Log in to the OCI Console.
2. Select the DR region. For example, US West (Phoenix).
3. Navigate to **Storage → Buckets → Select the Compartment → Select the Bucket created for OAC DR region snapshots (SnapshotsDR).**
4. In the Resources Section, click **Retention Rules → Create Rule**.

5. Create a Time-Bound rule for 30 days.



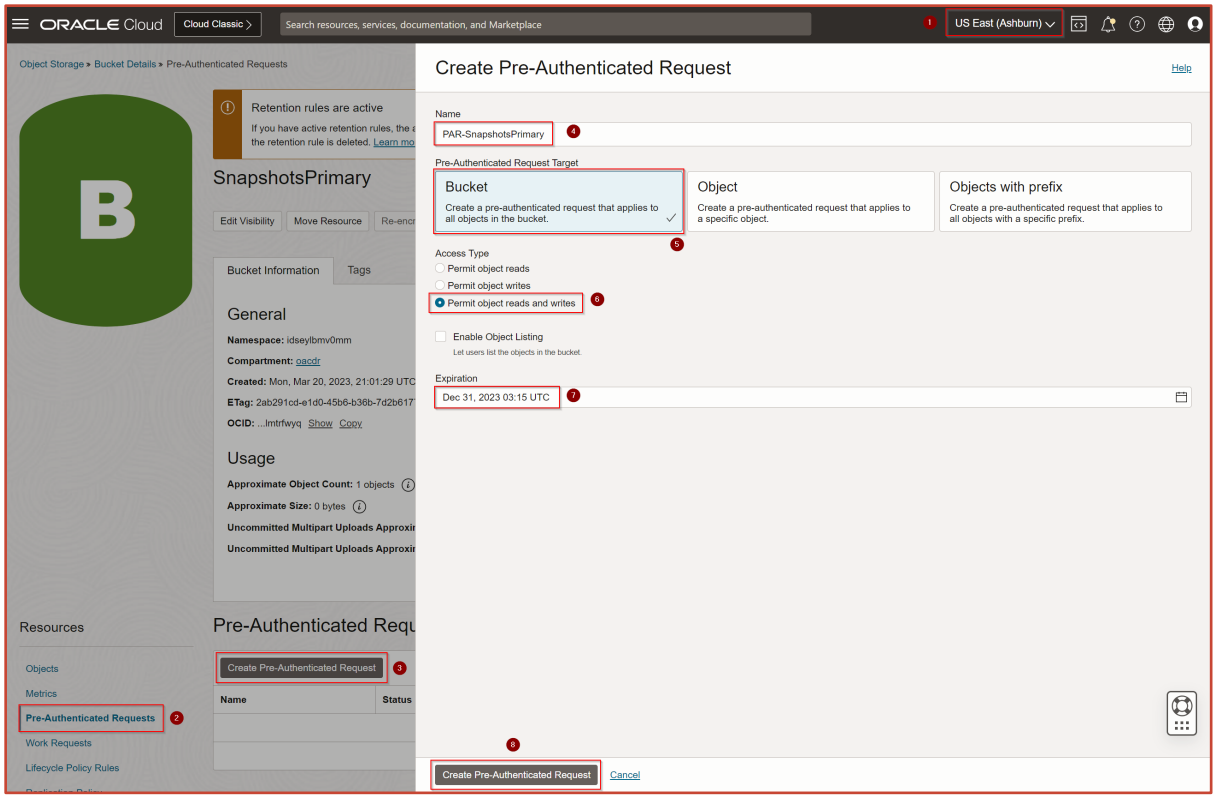
Create a Folder in Each Bucket

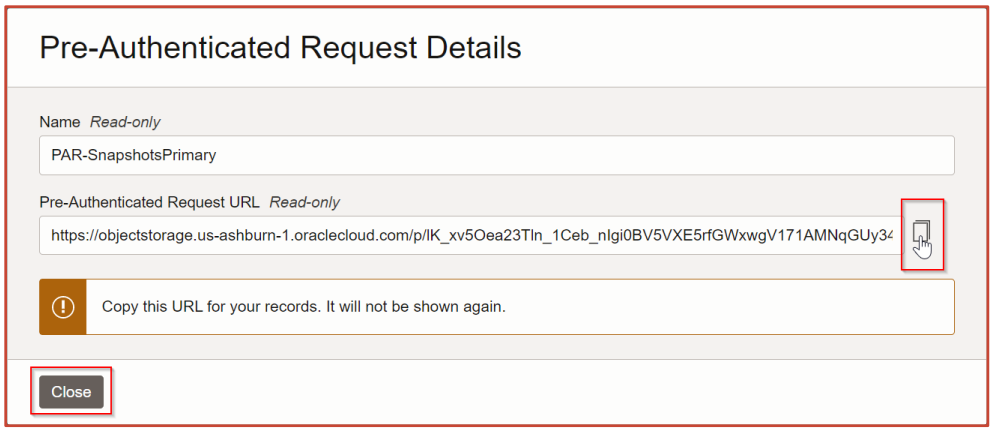
After enabling replication and retention policies, create a folder (for example, **OAC**) in the buckets **SnapshotsPrimary** and **SnapshotsDR**.



Create Pre-Authenticated Requests for Each Bucket

Go to the **SnapshotsPrimary** bucket in the Ashburn region, create a pre-authenticated request for the bucket, and copy the URL.





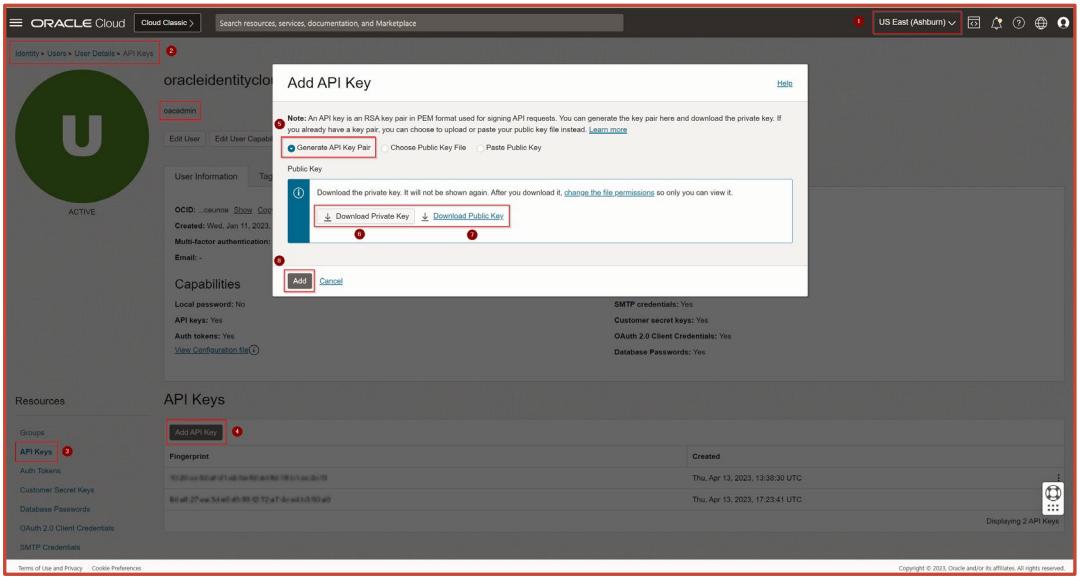
Copy the **Pre-Authenticated Request URL** and save it for use in automation scripts.

Repeat the same steps for the **SnapshotsDR** bucket in the Phoenix region and save the URL.

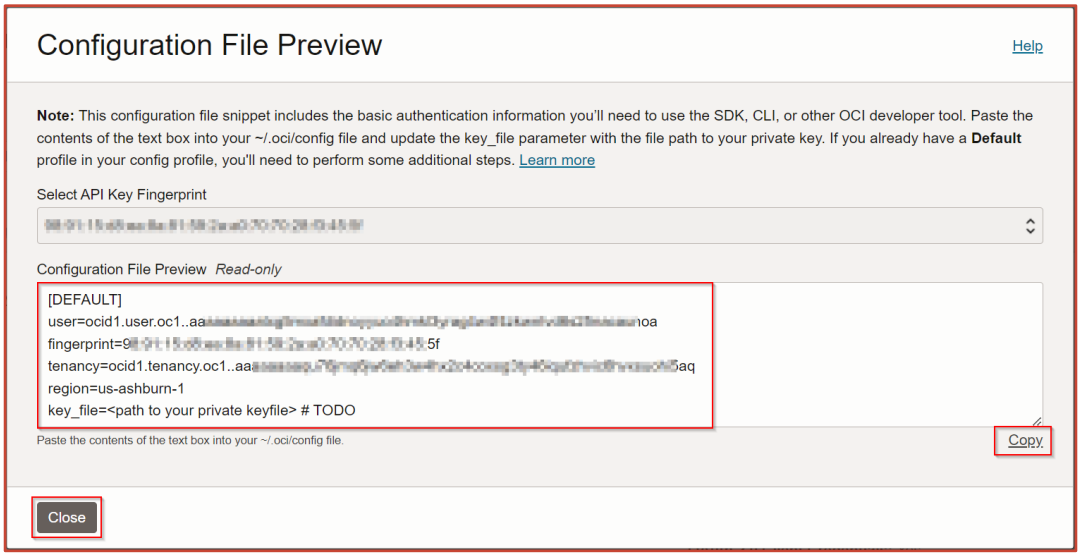
Generate the API Key Pair

In the OCI Console, generate the key pair and add it to the API Keys for the user who will run the migration scripts.

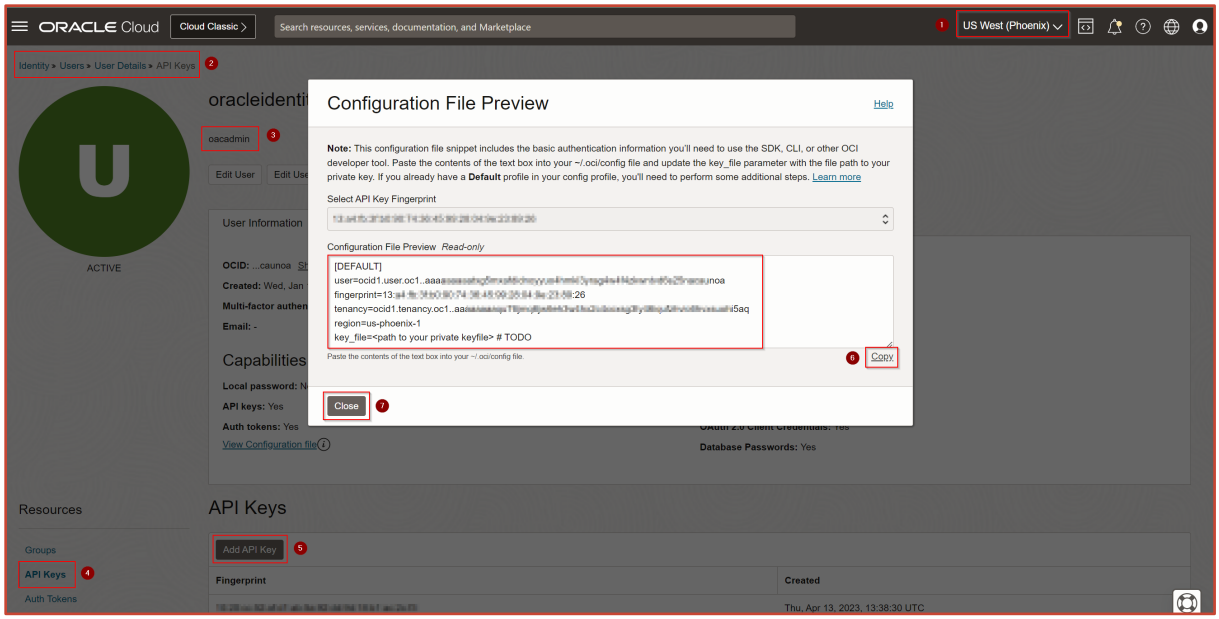
1. Log in to the OCI Console
2. Navigate to **Identity and Security > Users >** Select the required user.
3. Navigate to **API Keys >** Click on **Add API Key > Generate the API key pair > Download the private and public keys**.
4. Click **Add** to add the public key to the selected user's API key list.



5. Copy the user's **Configuration File Preview** and save the content for use with the migration scripts.



6. Similarly, generate the key pair for the same user in the DR OCI region, for example Phoenix. Download the private and public keys, copy the user's **Configuration File Preview** and save it for migration scripts.



Synchronize Content Across Both Oracle Analytics Cloud Instances

You use a *snapsho*t and the *Data Migration* utility to migrate content between the OAC instances.

Snapshot Artifacts

Snapshots contains the following artifacts:

- Catalog and its objects with permissions and properties
- Semantic model (RPD)
- Application roles and memberships
- Data files
- Data sets
- Object storage information
- Data visualization workbooks
- Data visualization projects
- Connections and their permissions, security, and so on.

For more information see:

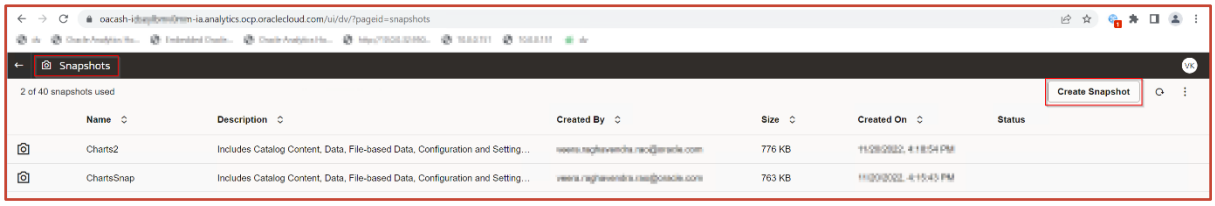
Migrate Oracle Analytics Cloud Using Snapshots

Export and Import Snapshots

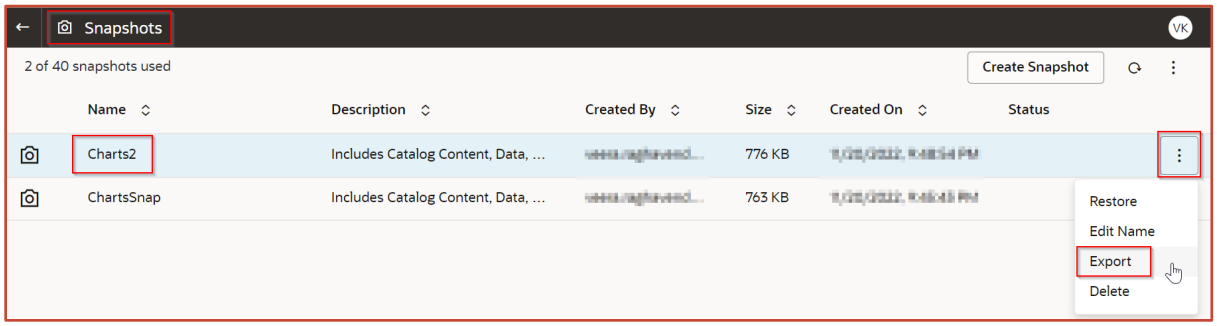
Tutorial on Snapshots

Create and Export a Snapshot

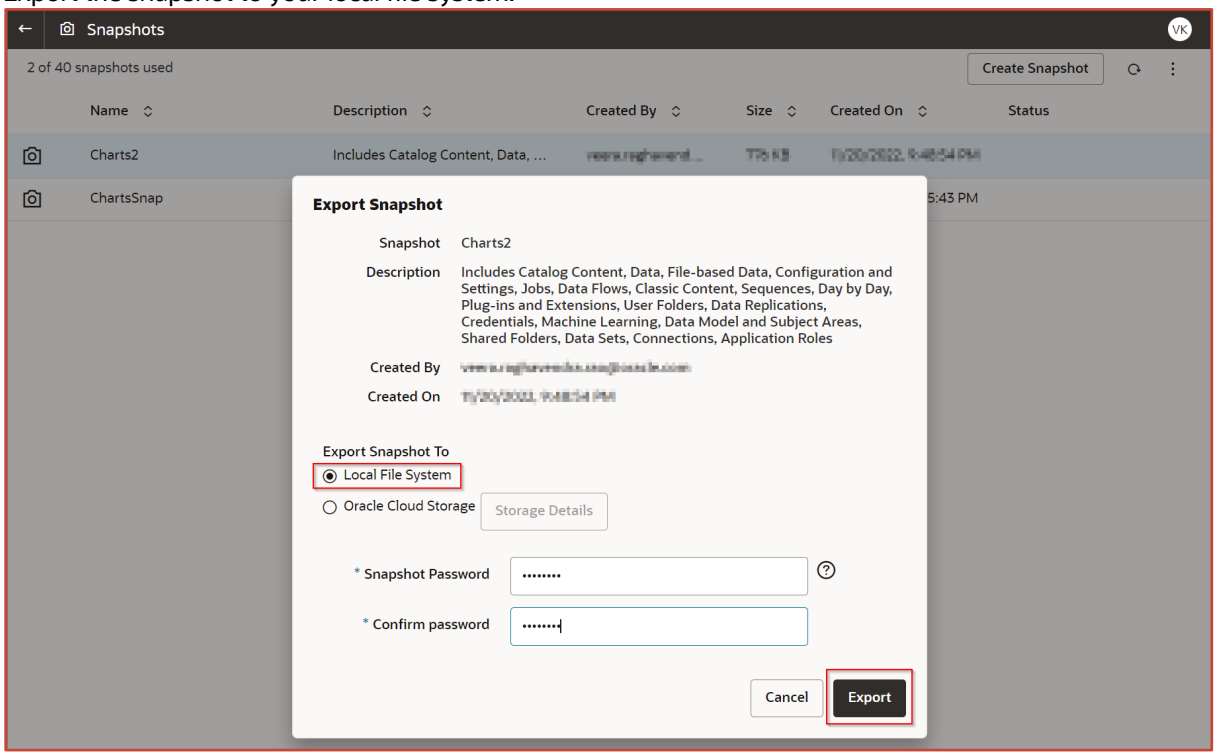
Create the snapshot.



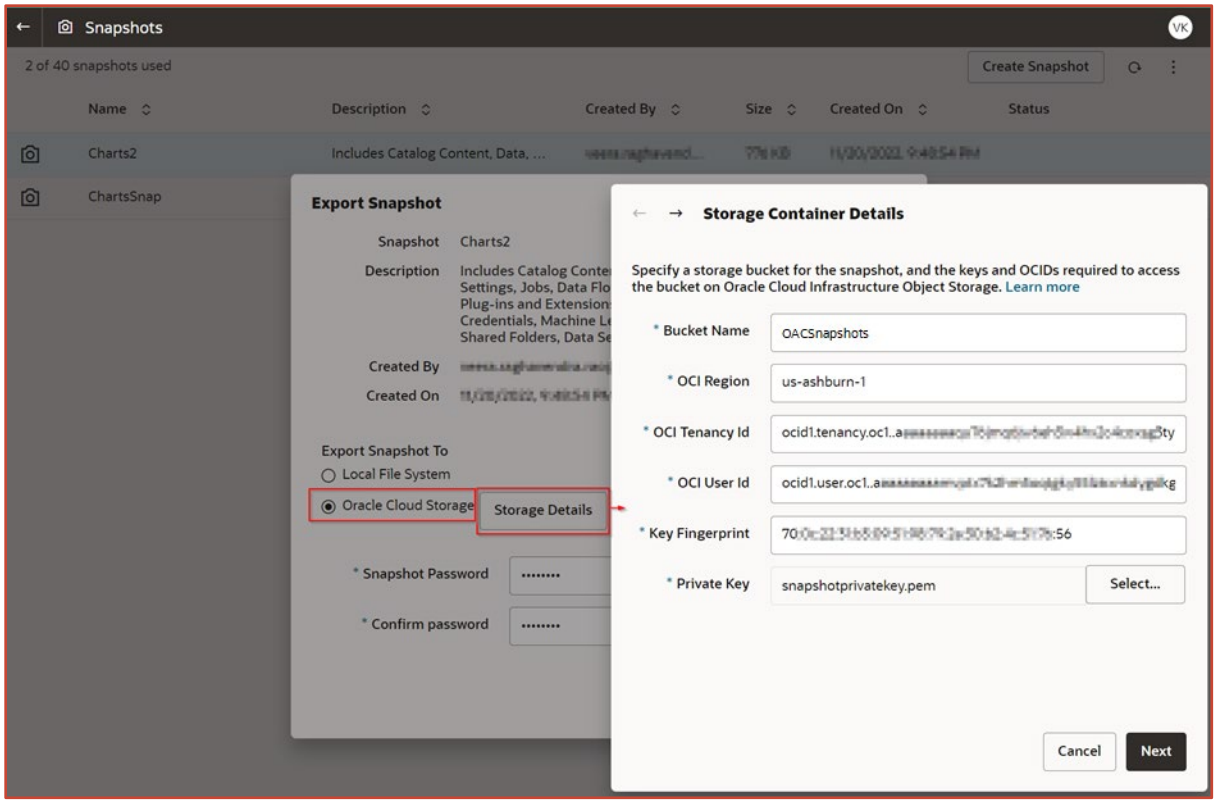
Export the snapshot.

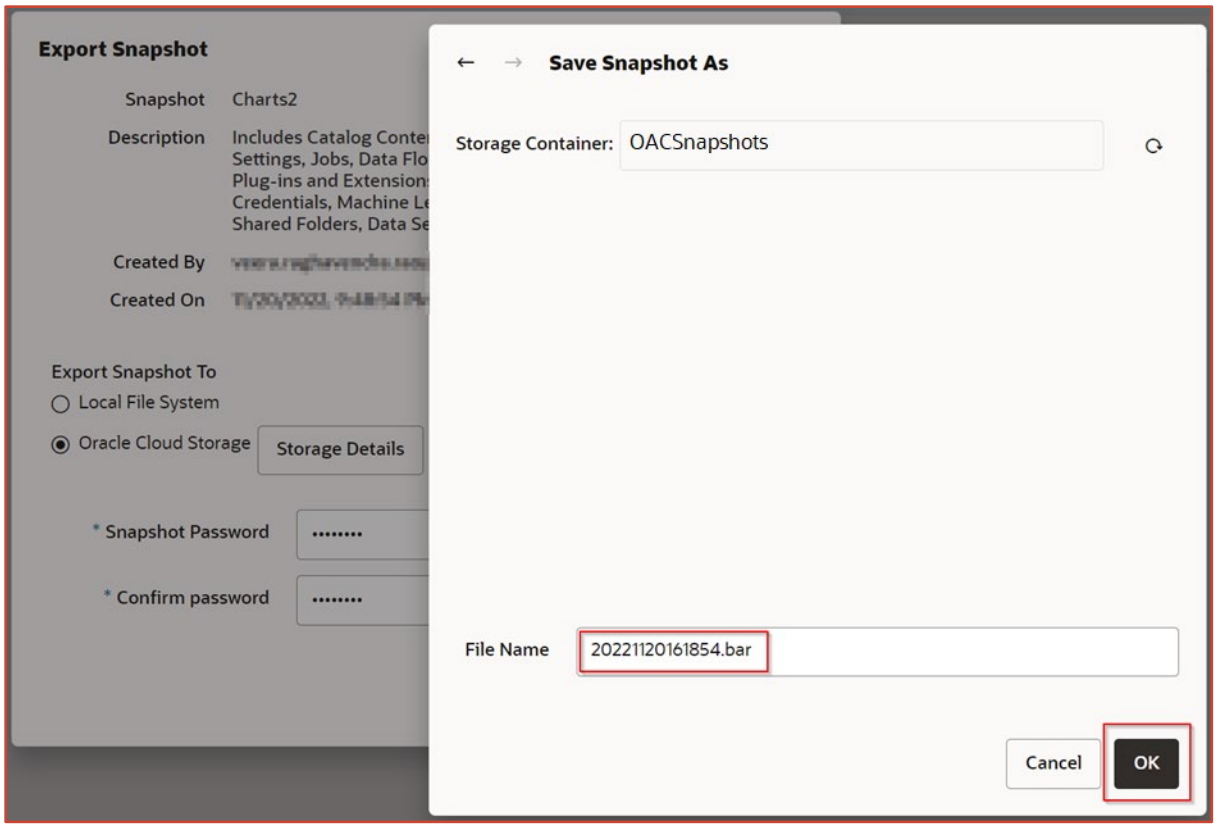


Export the snapshot to your local file system.

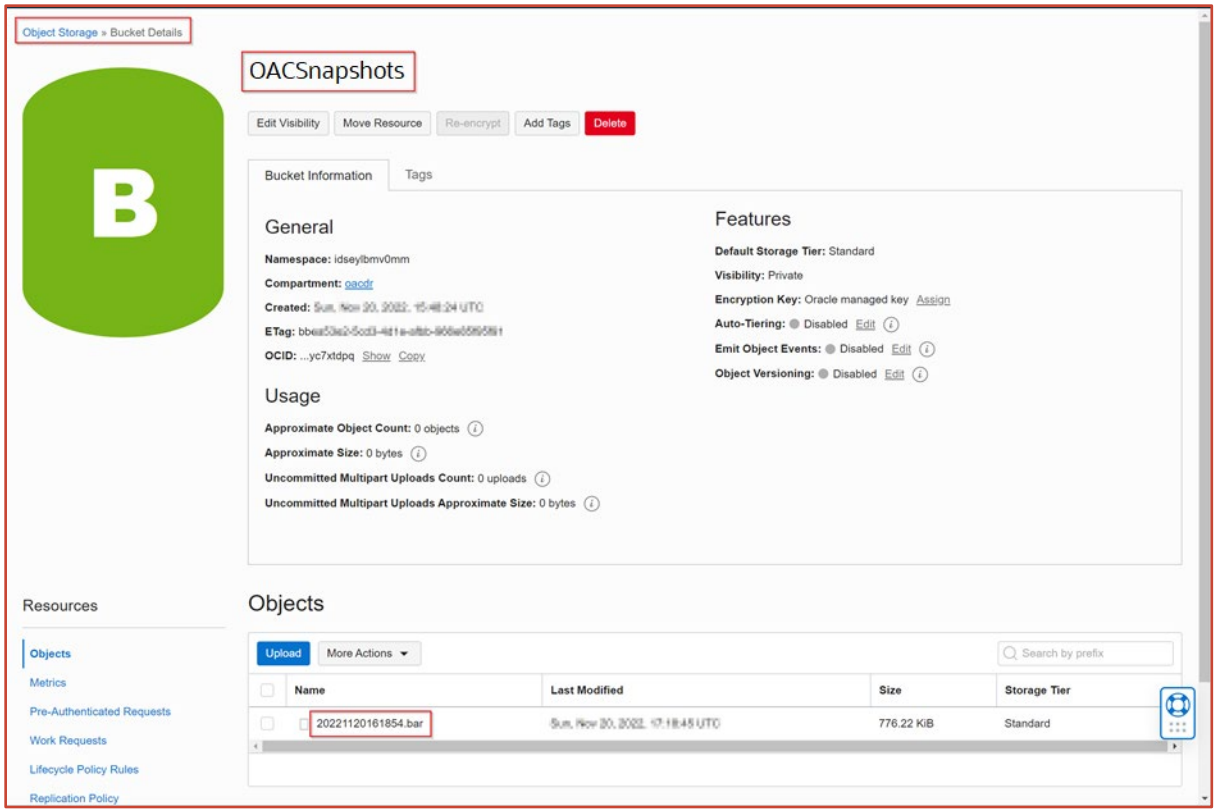


Or, export the snapshot to Oracle Cloud storage.





Click **Export** on the main Export Snapshot dialog.



During content replication across OCI regions, the snapshot created in the home region OAC instance doesn't migrate data files to the DR region OAC instance. For more information, see Migrate File-based Data.

Install JDK 1.8.0_361

The Data Migration utility requires Java 1.8.0+. Download the latest Java 1.8 361 updates from:

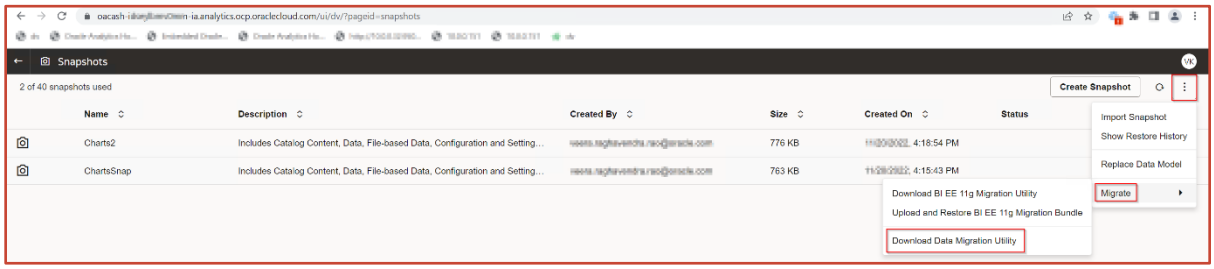
https://www.oracle.com/in/java/technologies/javase/javase8u211-later-archive-downloads.html

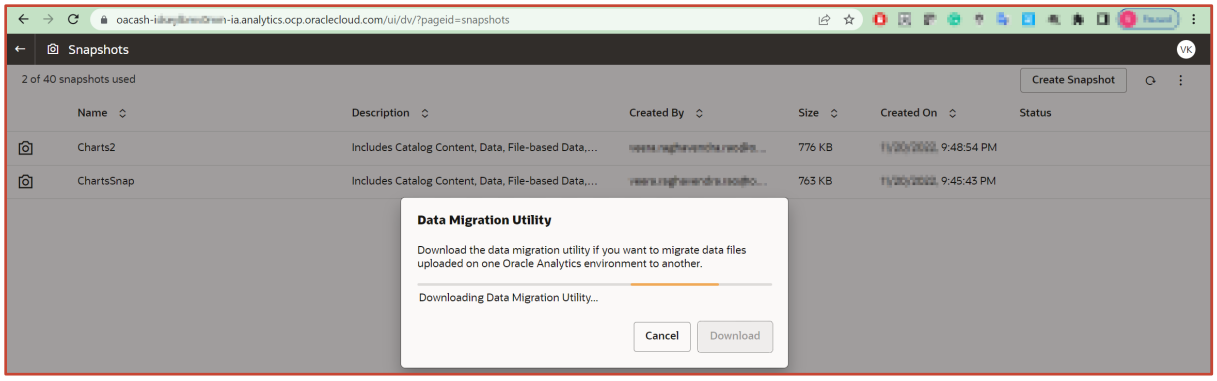
https://download.oracle.com/otn/java/jdk/8u361-b09/0ae14417abb444ebb02b9815e2103550/jdk-8u361-linux-x64.tar.gz

Download and Run the Data Migration Utility

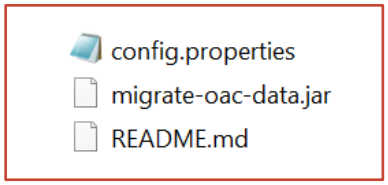
Use the Data Migration utility to back up data files from the home region OAC instance and restore them on the DR region OAC instance.

To obtain the Data Migration utility, go to the OAC home page and navigate to **Console > Snapshots > Migrate > Download Data Migration Utility**.





You download the **migrate-oac-data.zip** file to your local file system, and then copy it to a Windows/Linux/Mac OS machine, where you can unzip it.



There are two options when you run the Data Migration utility:

- **Option 1:** Migrate data files stored in your source environment directly to the target in a single step. For this option, you configure the section [MigrateData] in the config.properties file.
- **Option 2:** Download data files from your source OAC instance to your local environment and subsequently upload the data files to the target OAC instance. For this option, you configure sections [DownloadDataFiles] and [UploadDataFragments] in the config.properties file.

Option 1: Migrate data files directly from the source to the target in a single step

Utilize this option when the OAC instances in the home and DR regions are both active.

Import and restore the snapshot on the DR OAC instance and migrate the data files using the Data Migration utility.

```
[MigrateData]
# Specify whether the source environment is OAC, BICS, or DVCS.
SOURCE_ENVIRONMENT=OAC
# Source URL. Either OAC, BICS, or DVCS. For example: http://sourcehost.com:9704 or https://sourcehost.com:443
SOURCE_URL=https://oacash-[redacted]-ia.analytics.ocp.oraclecloud.com:443
# Name of a user with Administrator permissions in the source environment. For example: SourceAdmin
SOURCE_USERNAME=[redacted]@oracle.com
# Location of the source BAR file. For example:  /tmp/20190307095216.bar
BAR_PATH=/tmp/snapshotmigrate/BAR/20221120161854.bar

# Target Oracle Analytics Cloud URL. For example: http://targethost.com:9704 or https://sourcehost.com:443
TARGET_URL=https://oacphx-[redacted]-px.analytics.ocp.oraclecloud.com:443
# Name of a user with Administrator permissions in the target environment. For example: TargetAdmin
TARGET_USERNAME=[redacted]@oracle.com
```

```
/u01/app/jdk/bin/java -jar migrate-oac-data.jar -m -config config.properties
```

Restore the snapshot on the DR OAC instance to complete the migration.

Option 2: Download data files from the source and upload to the target in two steps

Utilize this option when the primary OAC instance in the home region is active and the OAC instance in the DR region is paused and only made active when needed.

Import and restore the snapshot on the DR OAC instance and migrate the data files using the Data Migration utility.

```
# Download Data Files: Download data files from the source environment to a local repository
[DownloadDataFiles]
# Specify whether the source environment is OAC, BICS, or DVCS.
SOURCE_ENVIRONMENT=OAC
# Source URL. Either OAC, BICS, or DVCS. For example: http://sourcehost.com:9704 or https://sourcehost.com:443
SOURCE_URL=https://oacash-[redacted]-ia.analytics.ocp.oraclecloud.com:443
# Source Administrator User Name
SOURCE_USERNAME=[redacted]@oracle.com
# Location for the source BAR file. For example:  /tmp/20190307095216.bar
BAR_PATH=/tmp/snapshotmigrate/BAR/20221120161854.bar
# Local data file directory.
# Make sure you have enough space to download the data files to this directory. For example: /tmp/mydatafiledir
DATA_FRAGMENTS_DIRECTORY=/tmp/snapshotmigrate/DF
# Data fragment size. Data files are downloaded in fragments. Default fragment size is 500MB.
MAX_DATA_FRAGMENT_SIZE_IN_MB=500

# Upload data files: Upload data files to the target Oracle Analytics Cloud.
[UploadDataFiles]
# Target Oracle Analytics Cloud URL. For example: http://targethost.com:9704 or or https://targethost.com:443
TARGET_URL=https://oacphx-[redacted]n-px.analytics.ocp.oraclecloud.com:443
# Name of a user with Administrator permissions in the target environment. For example: TargetAdmin
TARGET_USERNAME=[redacted]@oracle.com
# Local directory containing the data files you want to upload. For example: /tmp/mydatafiledir
DATA_FRAGMENTS_DIRECTORY=/tmp/snapshotmigrate/DF
# Location of the source BAR file. For example:  /tmp/20190307095216.bar
BAR_PATH=/tmp/snapshotmigrate/BAR/20221120161854.bar
```

Download the Data Files

```
/u01/app/jdk/bin/java -jar migrate-oac-data.jar -d -config config.properties
```

Upload the Data Files

```
/u01/app/jdk/bin/java -jar migrate-oac-data.jar -u -config config.properties
```

Restore the snapshot on the DR OAC instance to complete the migration.

1. Sign into your target OAC instance.
2. To expose the data files in OAC, you must restore the snapshot you used to migrate the rest of your content for a second time. This time, you must select the **Custom** restore option.
   a) Open the Console and click **Snapshots**.
   b) Select the snapshot containing your data files and click **Restore**.
   c) Select the **Custom** restore option.
   d) Select the option **File-based data**. Deselect all other options.
   e) Click **Restore**.
3. Verify that your data files are available.

Network Perimeters - Impact on the Data Migration Utility

Data file migration fails with the following errors when network perimeters are enabled for IDCS or IAM Domain.

```
[opc@autodr test]$ /home/opc/jdk1.8.0_361/bin/java -jar /home/opc/migrate-oac-data/migrate-
oac-data.jar -d -config config.properties
May 08, 2023 11:48:37 PM oracle.bi.bar.dr.util.DRUtils getOracleHome
INFO:   Oracle Home: /bi/app/fmw
Starting Data Migration Utility...
Log Path: /home/opc/migrate-oac-data/logs/1683589717625/datamigration.log
Set Loglevel INFO
Java Version: 1.8.0_361
Recommended Java Version: 1.8+
Status File Path: /home/opc/migrate-oac-data/logs/1683589717625/status.txt
Operation Selected : DownloadDataFiles

Invoking Data files download ...
Operation failed.  Reason: Source pod is not accessible from client. Please check source
OAC URL and credential. https://oac-xxxxxxxxxxxxx-ia.analytics.ocp.oraclecloud.com
Operation failed.  Reason: Source pod is not accessible from client. Please check source
OAC URL and credential. https:// oac-xxxxxxxxxxxxx-ia.analytics.ocp.oraclecloud.com
Data Migration Failed. Please check the log.
```

For example, if the OAC instance and the Data Migration utility instances are in public or private OCI subnets as shown in the table; you must allowlist the required IP CIDR ranges shown here.

Data Migration Utility Compute in Public or Private Subnet	OAC in Public or Private Subnet	Allowed IP Addresses for Network Perimeters
Public	Public	Public IP address of the Data Migration utility compute
Public	Private	240.0.0.0/4
Private	Public	240.0.0.0/4
Private	Private	240.0.0.0/4

See Public IP Ranges and Gateway IPs for Oracle Analytics Cloud Instances.

Automate Snapshot and Data File Back Up

You can also use REST APIs to manage and migrate snapshots.

- Manage Snapshots Using REST APIs
- REST API for Oracle Analytics Cloud

Prerequisites for Using OAC REST APIs to Automate Snapshots

- OAC BI Service Administrator Username and Password
- Create a confidential applications for source and target OAC instances in IDCS or IAM Domain
- Use a refresh token to generate OAuth token
- Configure an OCI object storage bucket for each source and target OAC instance (*described above*)
- Configure a pre-authenticated request URL for each bucket (*described above*)
- Generate an OCI API key pair (*described above*)

- Install JDK 1.8.0+ latest version (*described above*)
- OAC Data Migration utility (*described above*)
- Oracle-provided OAC instance DNS names for the source and target
- IDCS or IAM Domain URL

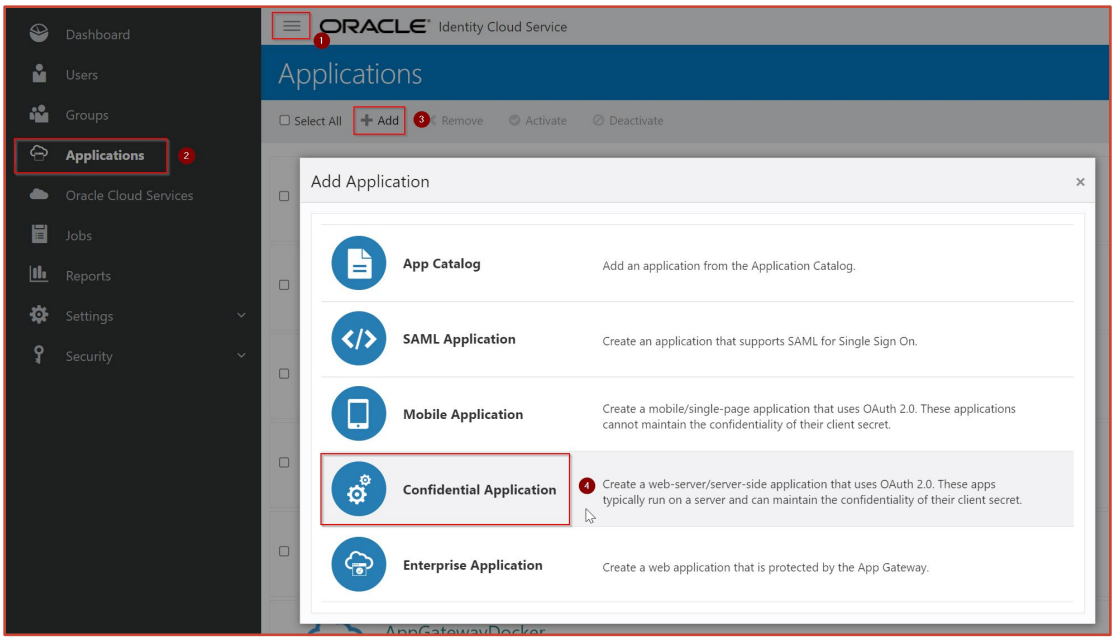
Create a Confidential Application for the Data Migration Utility

See Creating Confidential Application in IDCS and Creating Confidential Application in IAM Domain.

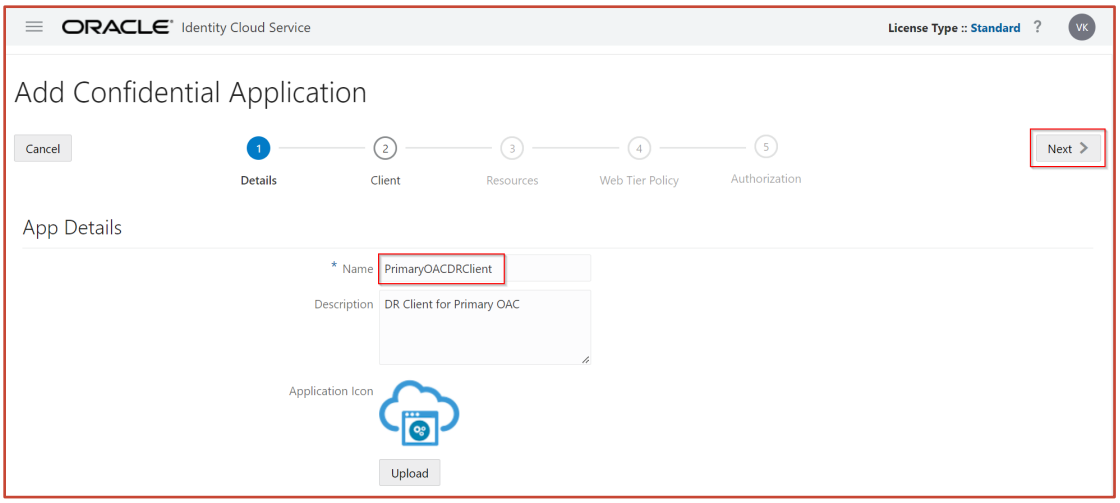
For the Source OAC Instance

1. Log in as an administrator to the IDCS Console or IAM Domain Administrator to the OCI Console and navigate to the IAM Domain where the OAC instance exists.

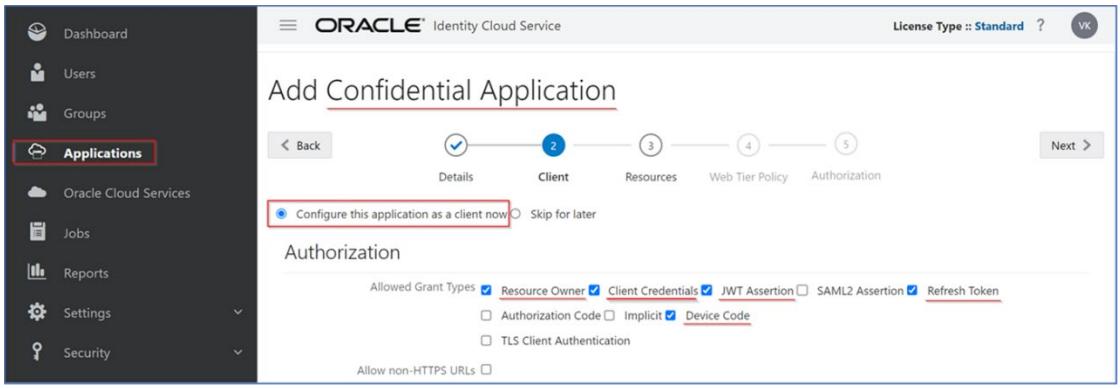
2. Click the left navigation bar, select **Applications** → Click **Add** → Select **Confidential Application**.



3. Enter **Name** and **Description** → click **Next.**



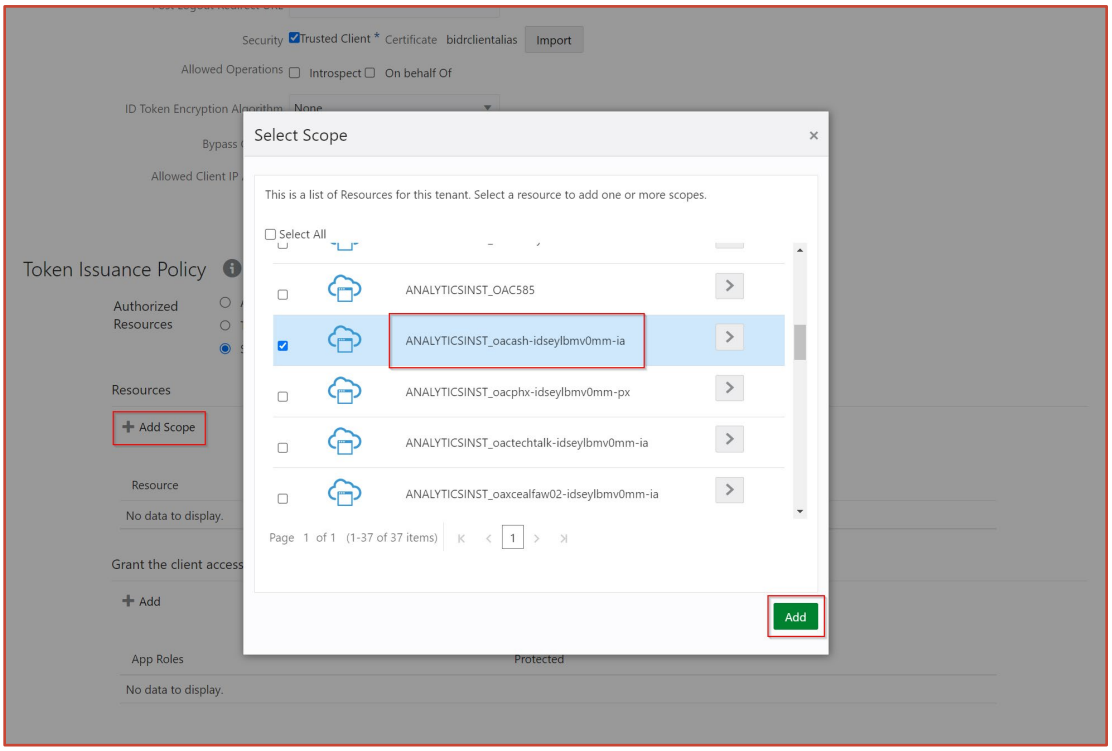
4. Select **Configure this application as a client now option → Select Allowed Grant Types**.



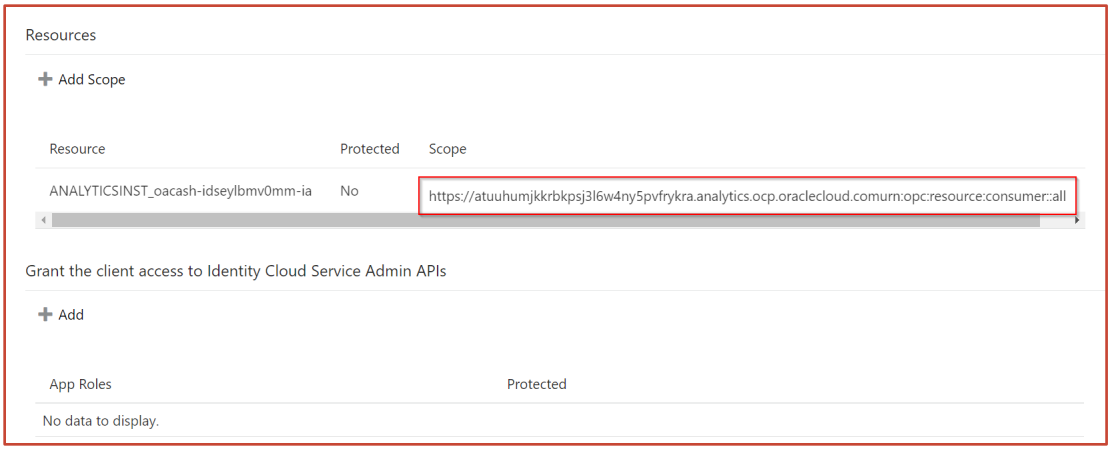
5. OAC supports multiple grant types for REST APIs. Select all the above options as the **Allowed Grant Types** but use **Refresh Token** for this example as the Grant Type. You can also select the required Grant Type only.

6. Add the scope for the confidential application.

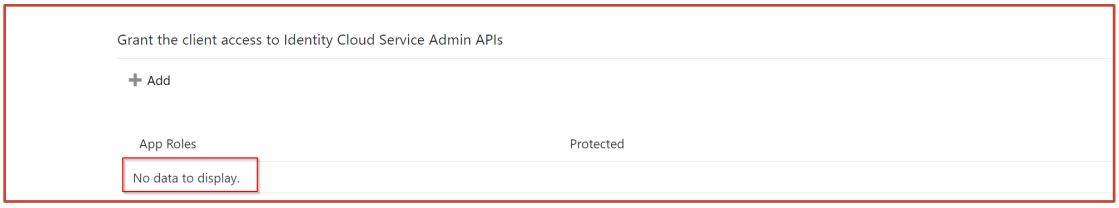
7. Select the Oracle Analytics Cloud (source) instance as the scope.



8. Copy the Scope URL after adding the source OAC instance (for automation input variable).

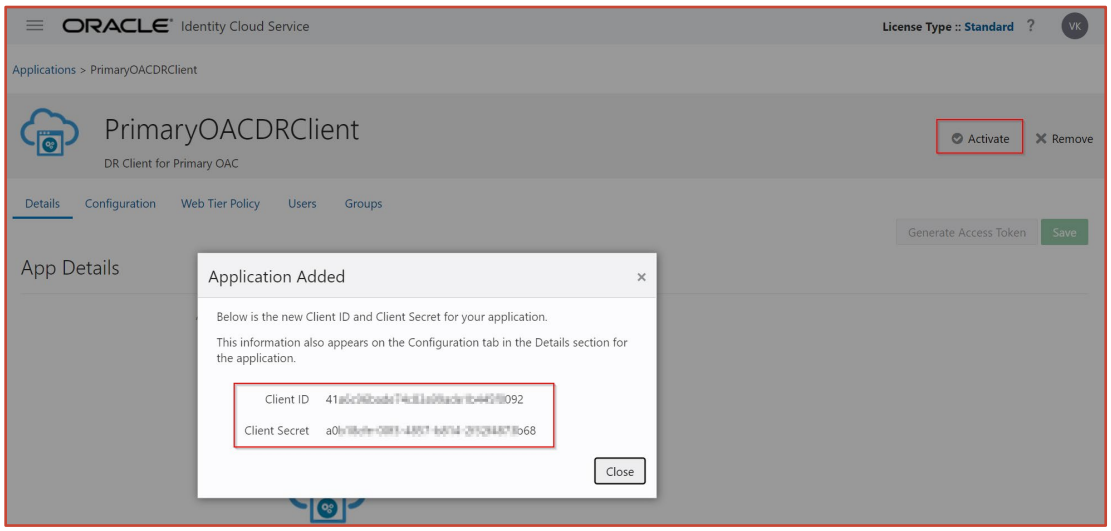


9. Don't grant any **App Roles** for the confidential application.



10. Click **Next** multiple times to reach finish, then click **Finish**.

11. The Client ID and Client Secret displays. Copy these values to use later.



Convert the ClientID:ClientSecret to base64 encoded value (for the automation script input variable):

```
echo -n “ClientIDValue:ClientSecretValue” | base64 -w 0
```

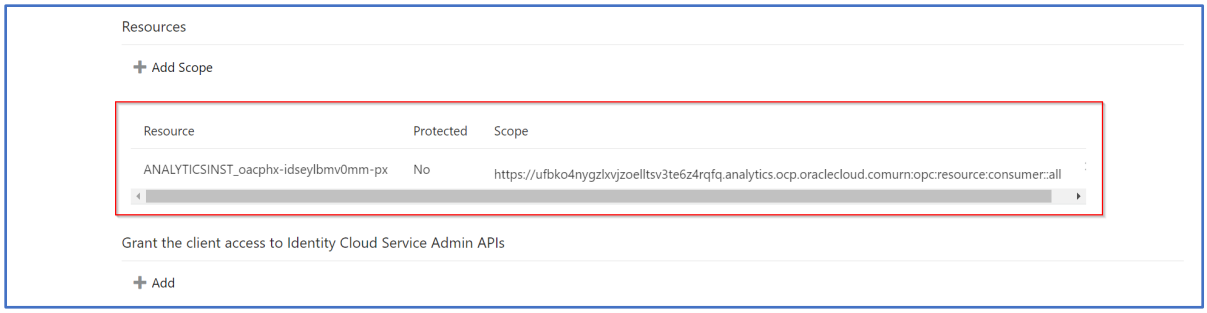
12. Click **Close**.

13. Click **Activate**.

For the Target OAC Instance

Repeat steps 1-14 for the target OAC instance.

While creating the confidential application, select the target OAC instance as the scope.



Copy the Scope URL after adding the target OAC instance (for automation script input variable).

If you use the same IDCS or IAM Domain for both OAC instances, you must add the DR OAC instance as another scope to the same confidential application created for the source OAC instance.

Configuration Attributes Required to Run OAC REST API Commands

To run OAC REST API commands, you must provide the following attributes from the OAuth client:

- ClientId — The OAuth client ID used to access the IDCS identity store.
- ClientSecret — The OAuth Client Secret (password) used to generate access tokens.
- Scope — Scope of the confidential application.
- IDCS URL — The IDCS or IAM Domain URL to get a token.

Sample Configuration Data

Client ID: eea4xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx33db

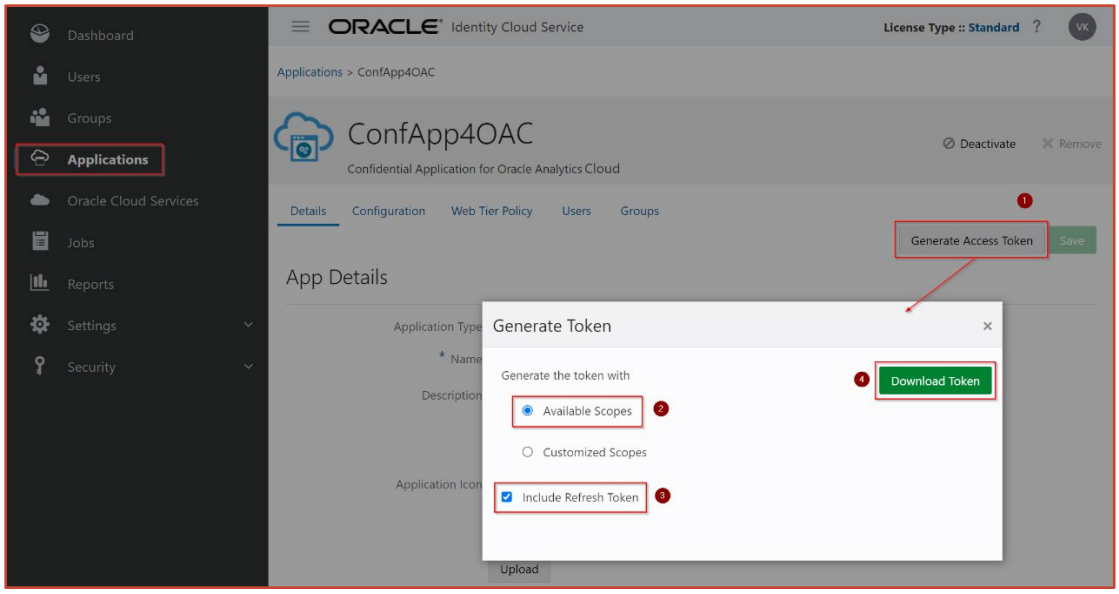
Client Secret: 6xxxxxxx6-0xx2-4xx9-axxb-0xxxxxxxxxxa

Scope: https://<xxxxxxxxxxxxxxxxxxxxx>.analytics.ocp.oraclecloud.comurn:opc:resource:consumer::all

IDCS URL: https://idcs-f5xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx03.identity.oraclecloud.com

Get the Refresh Token

1. Log in to the IDCS Admin Console or OCI Console for IAM Identity Domain.
2. In the IDCS Console, navigate to **Applications > Confidential Application**.
3. In the OCI Console for IAM Identity Domain, navigate to **Identity & Security > Domains > Required Domain > Applications > Confidential Application**.
4. Navigate to the **Details** tab and click **Generate Access Token**.
5. Select **Available Scopes** and **Include Refresh Token**.
6. Extract the refresh token value from the downloaded **tokens.tok** file.



{"app_access_token":"eyJ4NXQjUzI1NiIsIktMIVHWEtraWpNaQpxeDFsQ1drZlKFUFVJU0VkYklEdVpJUGdfVVUtbIEiLCJ4NXQiOiJ1S0h3cXpxMUJNaE5UFxEXbTRQS3ciLCJrawQiOiJTSUdCSU5HR0tFWSIsImFzZyI6IiJTMjU2Ias.eyJ1bGlhaGF
[illegible]
"refresh_token":"AgAqNzFjMDQzOWIyZDkwNzY4MzI1MGE3YzBmMDJmZjk4ODZlABCsNfL-FmmXQkuwR73GOhYCAAAAQOwZxjIcgBvYy0JCuHs14XFOaQz_XRcZAMIRPW4b0Mwicy3WVpCm4NxqqDDqfi-a3wmTfHPXPOvGQkfoTHMah5I-"}

Make a note of the refresh token value.

IDCS REST API Commands to Generate the Refresh Token

Generate the base64 encoded clientID and clientSecret

```
echo -n "eea4xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx33db:6xxxxxxx6-0xx2-4xx9-axxb-0xxxxxxxxxxa" | base64
-w 0
```

Generate the refresh token

This approach needs the **Resource Owner** and **Refresh Token** grant types to be selected in the confidential application.

```
curl --request POST " https://idcs-
f5xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx03.identity.oraclecloud.com/oauth2/v1/token" --header
"Authorization: Basic <base64 encoded ClientID:clientSecret> " --header 'Content-Type:
application/x-www-form-urlencoded' --data-urlencode 'grant_type=password' --data-urlencode
"username=<OAC_BIServiceAdministrator_UserName>" --data-urlencode "password=<User_Password>" --
data-urlencode "scope=
https://<xxxxxxxxxxxxxxxxxxxx>.analytics.ocp.oraclecloud.comurn:opc:resource:consumer::all
offline_access"
```

Capture the refresh token value from the output


```
{"access_token":"eyJ4NXQjUzI1NiI6IkttM1VBWEttaHpHa0pxeDFnQldrZ1RFOFVJU0VtYklEdVpJUGdYVVUtb1EiLCJ
4NXQiOiJ1S0h3cXp6M1c2S3czcWU3NnE5UFdXbTRQS3ciLCJraWQiOiJTSUdOSU5HX0tFWSIsImFsZyI6IlJTMjU2In0.....
.......................
jtlr6Njab5i5qW1A","token_type":"Bearer","expires_in":100,"refresh_token":"AgAgNzRjNDQxOWIyZDkwNG
Y4MzlkMGE3YzBmMDJmZjk4.....vy2w_41xmpg="}
```


Repeat the confidential application creation steps for the DR OAC instance in the DR IDCS stripe or in the DR region IAM identity domain. Add the scope as the DR OAC instance, and note the scope of the DR OAC instance. Also, get the refresh token value for the DR OAC instance as the target refresh token.

In the automation script folder, save the *source refresh token* value in the **source_refreshToken.txt** file.

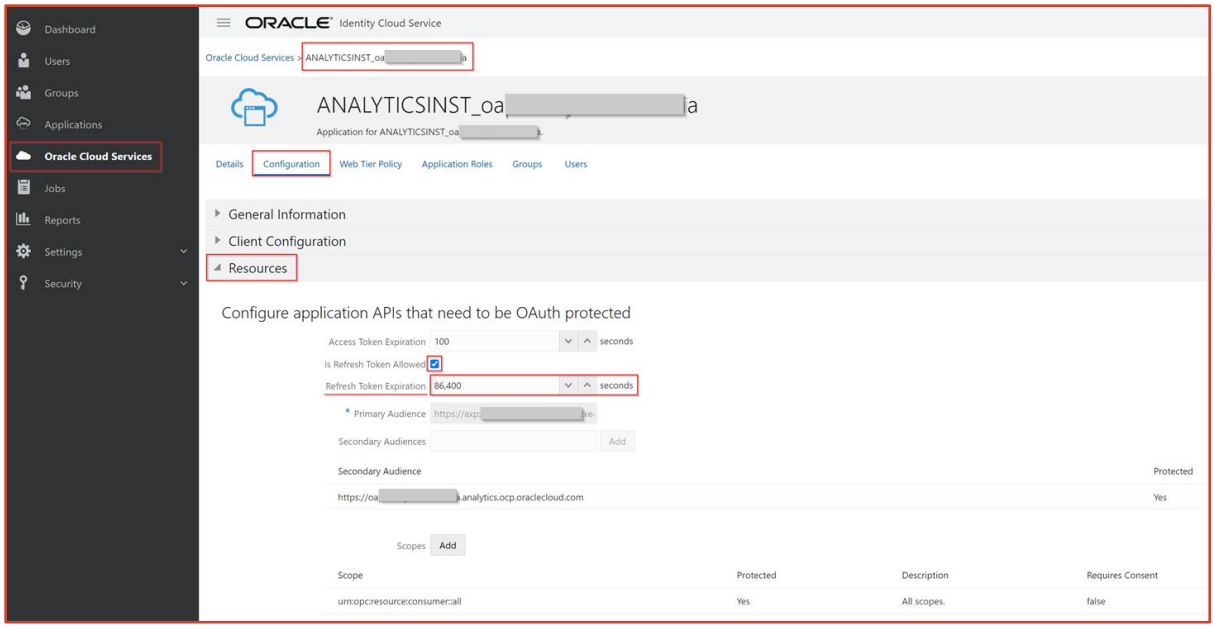
Save the *target refresh token* value in the **targetRefreshToken.txt** file in the automation script folder.

Saving the refresh token in the text files is a one-time task.

Ensure that the **Refresh Token Expiration** value exceeds the frequency of the REST API script execution.

For example, if you set the Refresh Token Expiration to 86,400 seconds, this is equivalent to 24 hrs. In this case, automation scripts must be executed daily with an interval *less than 24 hour* so that the refresh token is valid for the subsequent script execution.

The automation process renews the refresh token, uses the new refresh token while running the scripts, and saves the new refresh token to the **source_refreshToken.txt** and **targetRefreshToken.txt** files, respectively, so that the new token is valid for the next 24 hrs.



Note: The Access Token Expiration is 100 seconds, which may be sufficient. If a long-running script fails due to the access token expiry, you can increase the value accordingly.

Even though we use a confidential application and its grant types, the token expiry values are from the OAC application created in IDCS or IAM identity domain.

Download Automation Scripts

Ensure that JDK 1.8.0_361 and the Data Migration utility are available on the Linux machine where the automation scripts will run.

Download the script createSnapshot.sh. This script creates a snapshot and data files backup and stores the backup in Object Storage as a zip file.

Download the script registerSnapshot.sh. This script downloads the backup zip file, registers the snapshot, and restores it with the data files at the target OAC instance.

Configure SMTP Mail Servers

For mail server configuration, see Set Up an Email Server to Deliver Reports.

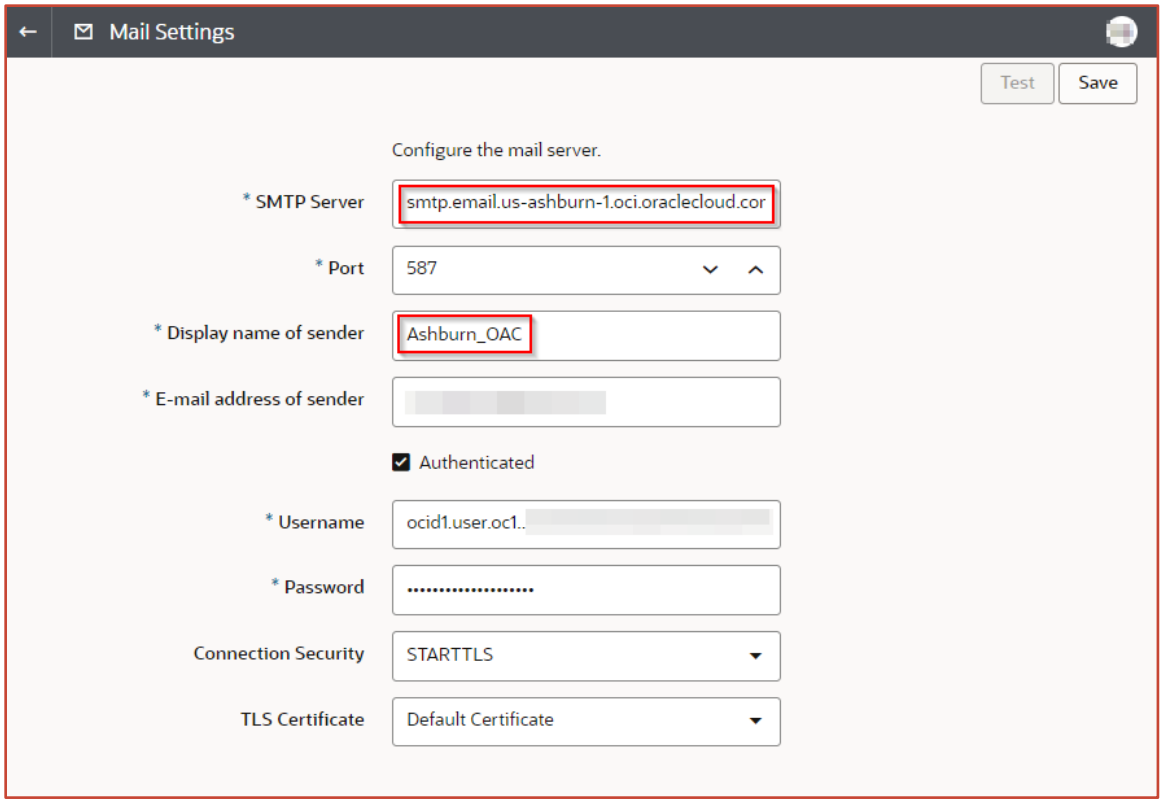
OCI mail server configuration requires that you allowlist the OCI data center IP ranges and Gateway IPs on your firewall to allow incoming emails from OCI. See Allowlisting IP Range and Gateway IPs.

- **Scenario 1:** You intend to utilize the same corporate SMTP server for mail server configuration on the primary and DR OAC instances. In this case, we recommended that you take note of the SMTP mail server configuration used in your primary OAC instance and use the same configuration information to set up the mail server on the DR OAC instance.
- **Scenario 2:** You intend to utilize the same OCI SMTP server for mail server configuration on the primary and DR OAC instances. In this case, we recommended that you take note of the OCI SMTP mail server configuration used in your primary OAC instance and use the same configuration information to set up the mail server on the DR OAC instance.
- **Scenario 3:** You intend to utilize the respective OCI region's SMTP server for mail server configuration on the respective OAC instance in the DR environment. The primary OAC instance on the OCI home region should use the home region SMTP server for mail server configuration in your primary OAC instance, The DR OAC instance on the OCI DR region should use the DR region SMTP server for mail server configuration in your DR OAC instance.

In all three scenarios, the mail server configuration for the DR OAC instance is overwritten with the mail server configuration of the primary OAC instance when the primary OAC instance snapshot is restored on the DR OAC instance.

In scenario 3, you must modify the mail server configuration of the DR OAC instance with the DR region's SMTP server details after restoring the snapshot.

Similarly, when falling back from the DR OAC instance to the primary OAC instance, you must modify the mail server configuration of the primary OAC instance with the primary OAC data region's SMTP server details after restoring the snapshot from the DR instance to the primary instance.



In scenarios 1 and 2, both OAC instances are configured with the same SMTP server details. This means that you don't need to modify the mail server configuration after restoring a snapshot, as the configuration remains the same, even after overwriting.

Understand Snapshot Migration Exclusions

Several items aren't included in a snapshot:

- Virus scanner configuration - Record the virus scanner configuration used in your source environment and use the same information to configure your virus scanner on the target. See Configure a Virus Scanner.
- Other snapshots saved in the source environment – If required, export them from the source OAC instance and import them to the DR OAC instance.
- System settings - Record the system settings used in your source environment and use the same information to configure your system settings on the target.
- Custom skins, CSS styles, and JavaScript - Record the customization used in your source environment and use the same information to configure your customizations on the target.

Length of Time to Create a Snapshot

Snapshot creation time depends on the amount of content in your OAC instance, that is, the size of your semantic model (RPD), content catalog, application roles, and so on.

Automating snapshot creation and data file backup using OAC REST APIs and the Data Migration utility eliminates the dependency on the browser's download limit. Using this method, the backup zip file is uploaded to Oracle Cloud storage. When you run the automation script, record how long it takes for the OAC snapshot to be created and uploaded to the cloud storage.

Snapshot Backup Frequency

How often you need to take snapshot backups depends on the length of time it takes to create the snapshot and upload it to cloud storage. Based on this, you can plan how often you run the automation script and how many snapshots you retain in storage.

Calculating your snapshot backup frequency is critical as it determines the potential data loss between the primary OAC instance snapshot creation time and the occurrence of a disaster event. There's a risk of data loss, if an end-user creates objects in the OAC instance between snapshot backups and a disaster event.

As the OAC instance used for DR is a production instance, we recommend that users do not develop new content (such as analyses and data visualization projects) in this production instance. This helps minimize data loss during a disaster event.

If a user does save any custom or personally developed content in their My Folders, there's a risk of data loss during the backup and restoration of a snapshot on the DR OAC instance.

Update Data Source Connection Strings After Snapshot Restore

When you restore a primary OAC instance snapshot onto the DR OAC instance, there might be limitations to the data source connection strings and wallets used for Oracle Autonomous Data Warehouse (ADW) or Oracle Database Cloud Service (DBCS) data sources. As a result, you might need to modify the connection strings for semantic models (RPD) or self-service data connections in the DR OAC instance.

To mitigate these limitations, we suggest you implement any such connection string modifications before you release the DR OAC instance to business users.

Create the Same Vanity URL for Both Oracle Analytics Cloud Instances.

Set up the same DNS name and SSL/TLS Certificate for the OAC instances on both the primary and DR regions. See Set Up a Vanity URL for Oracle Analytics Cloud on OCI Gen 2.

Consider the following scenarios:

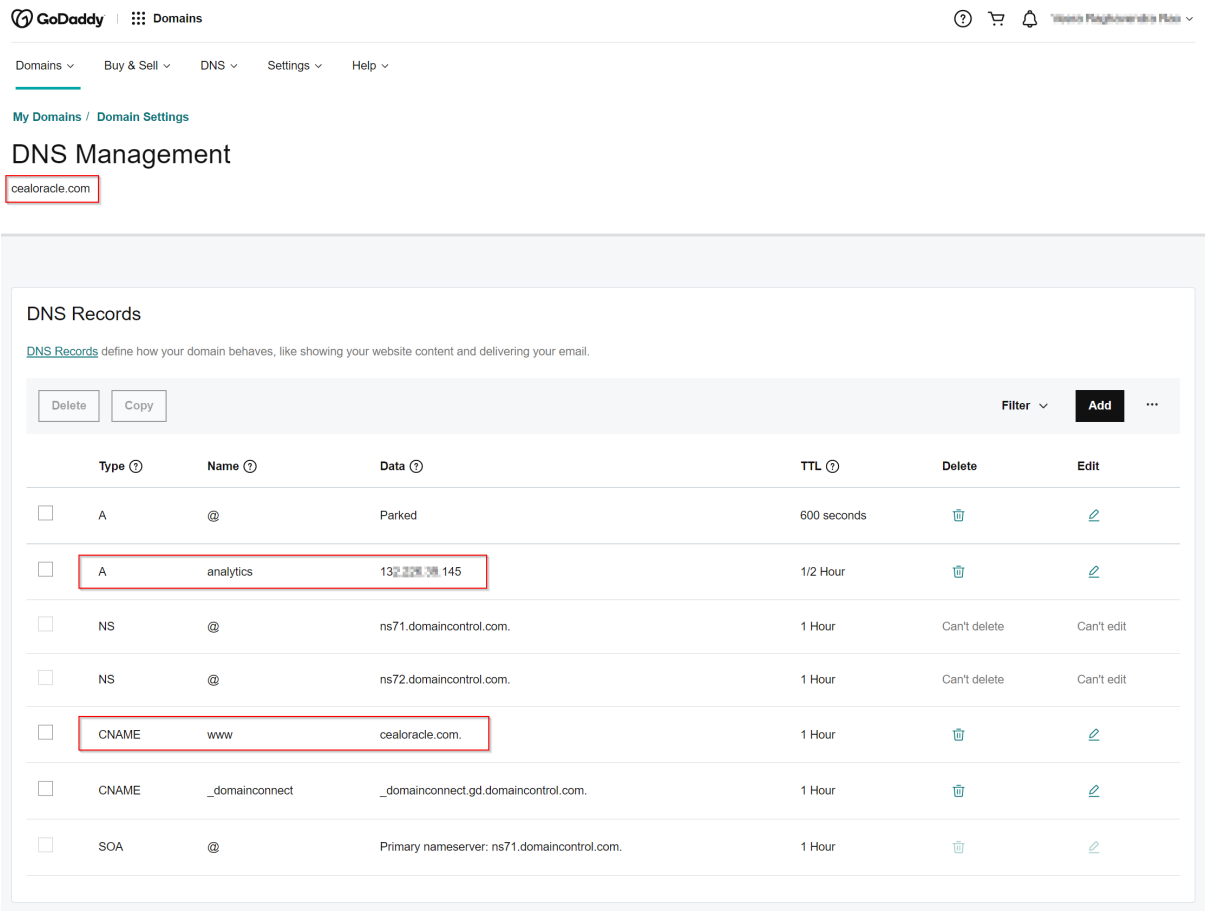
- **Scenario 1: Your OAC instances are in public subnet.** Configure the vanity URL and map the DNS name to the active OAC instance IP address.
- **Scenario 2: Your OAC instances are in a private subnet and used within a corporate network (VPN).** Configure the vanity URL and map the DNS name to the active OAC instance IP address.
- **Scenario 3: Your OAC instances are in a private subnet and used within a corporate network (VPN) and on the internet.** Create a public OCI load balancer as the front end for the OAC instances. Configure both the OAC vanity URL and OCI load balancer with the same DNS name and map the IP address of the active OAC instance load balancer to the DNS name.

Map the Vanity URL's DNS Name to the Active OAC Instance IP Address (Scenarios 1 and 2)

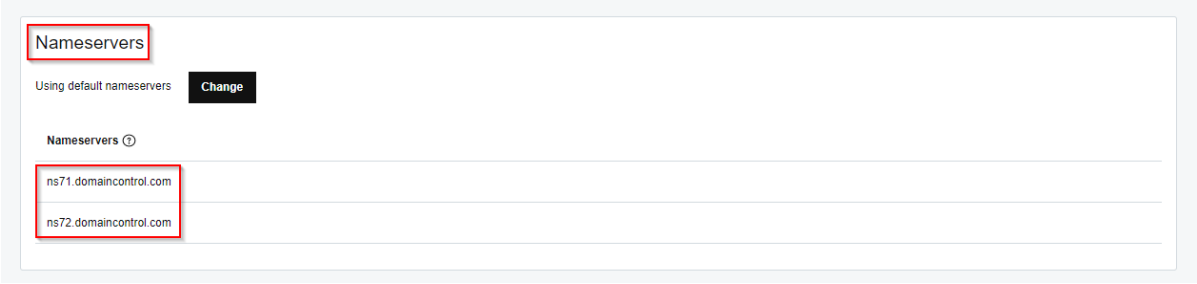
For Public OAC Access

If you want to provide public access to your OAC instance and your organization has an existing DNS domain, you can set up a vanity URL for both OAC instances and map the IP address of the active OAC instance to the DNS name in the domain's DNS management page. This allows users to always access the active OAC instance using the vanity URL.

This example uses the domain registrar GoDaddy.



GoDaddy NameServers page:



In GoDaddy DNS Management, create an **A Record** mapping the OAC instance IP address to the required subdomain. For example, **analytics.cealoracle.com**.

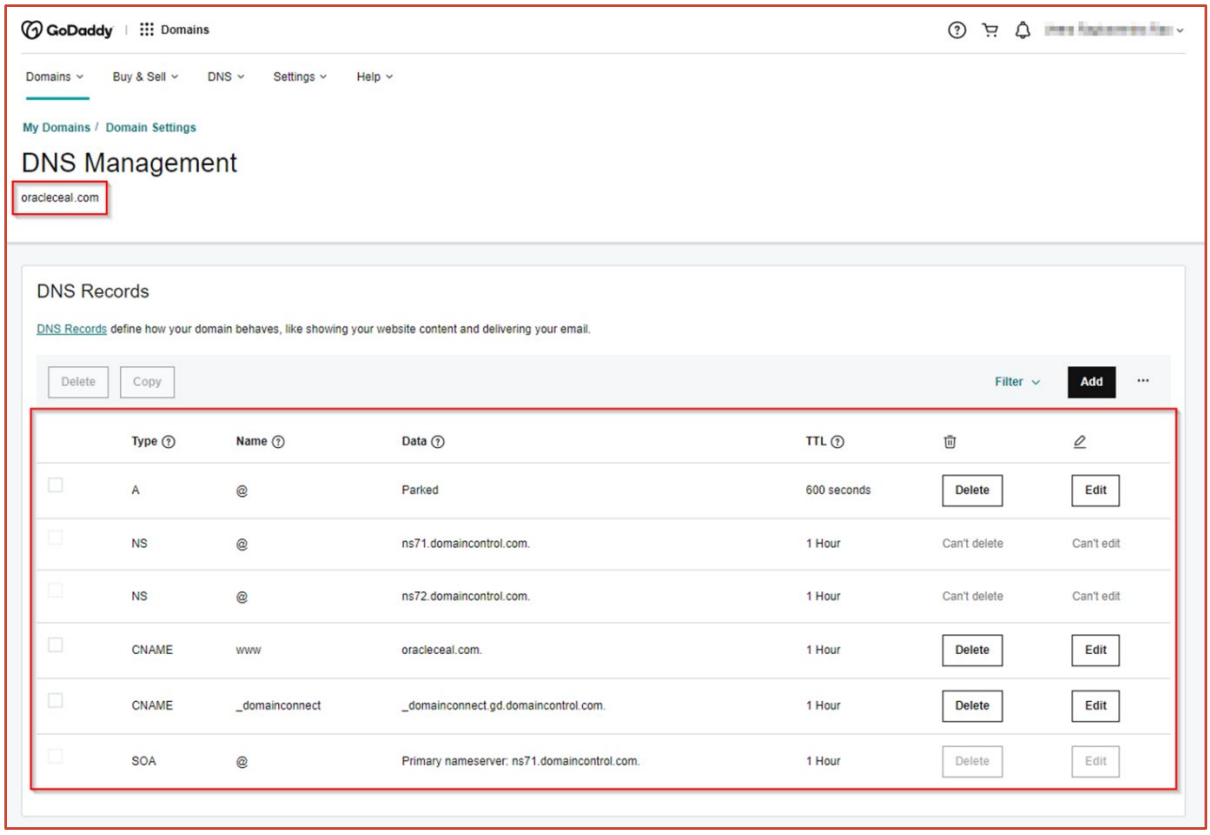
In a disaster recovery situation, map the DR OAC instance IP address to the DNS name in the domain's (GoDaddy) DNS management page.

You can also manage your organization's domain using delegated zones in OCI. However, Oracle isn't a registrar, so you must obtain a domain if needed.

> **Note:** You can't create the same public zone in multiple regions of OCI due to its public nature. Therefore, we recommend that you set up the public zone in the OCI DR region.

Get a Domain

For example, **oracleceal.com** from GoDaddy.

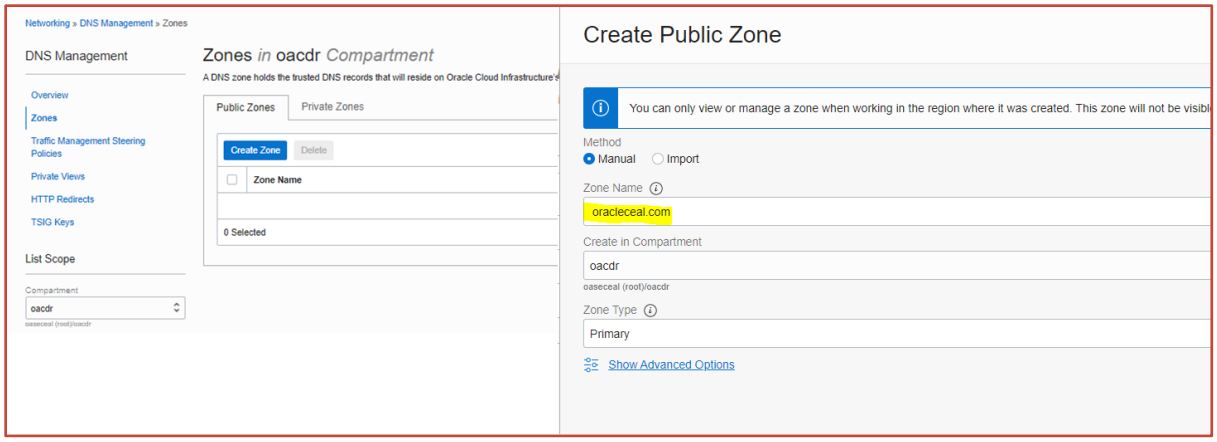


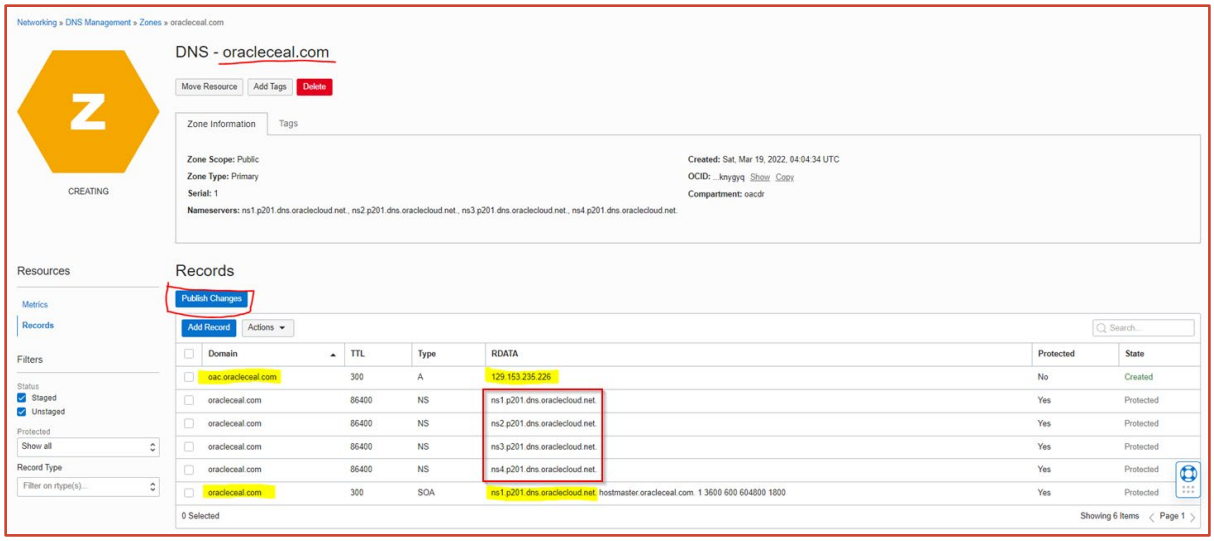
GoDaddy uses its own NameServers.

To delegate the domain, create a DNS zone in the OCI for that domain, and use the OCI nameservers at GoDaddy.

Create a Public Zone

In the OCI Console, navigate to **Networking → DNS Management → Zones → Create Zone**.



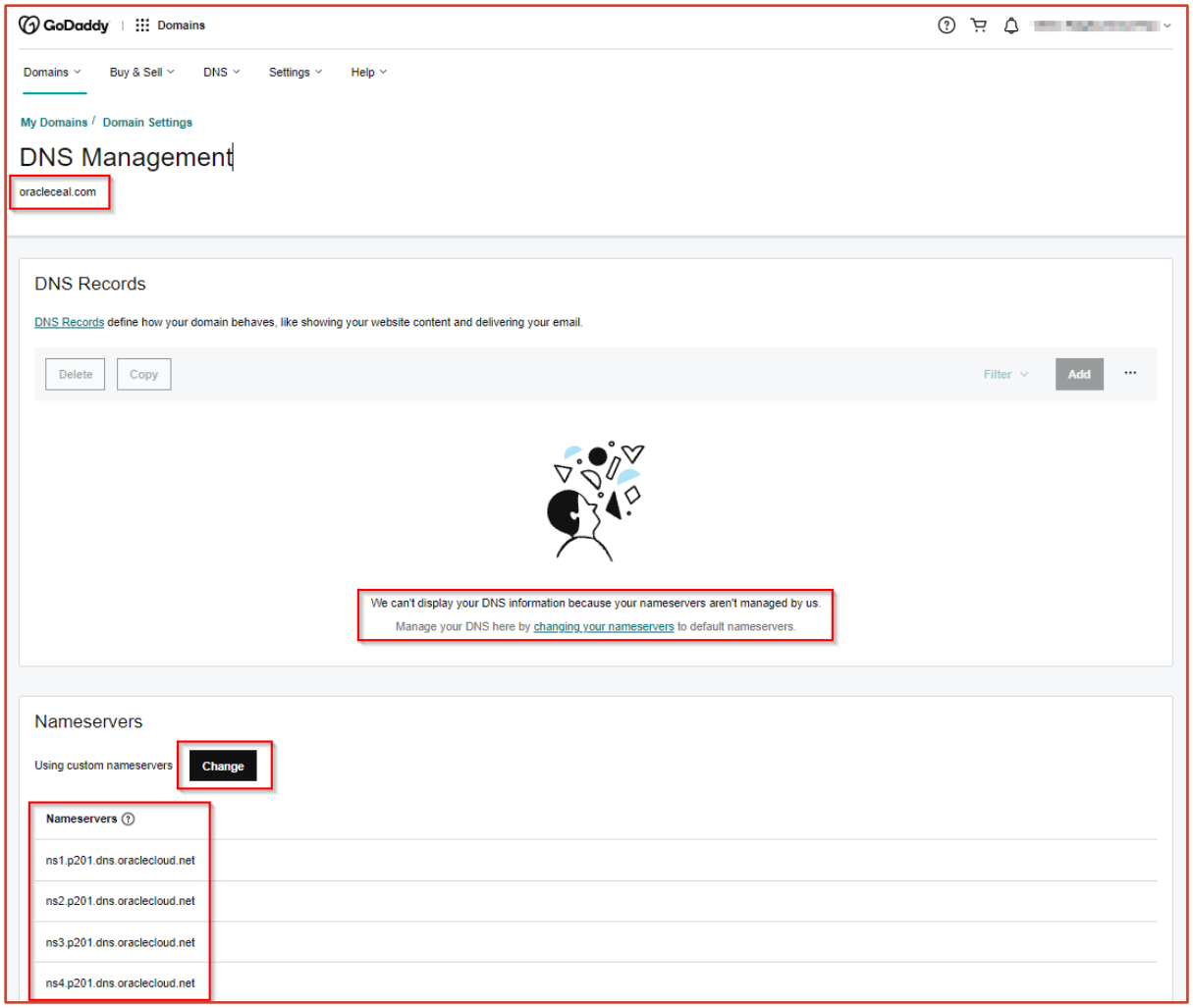


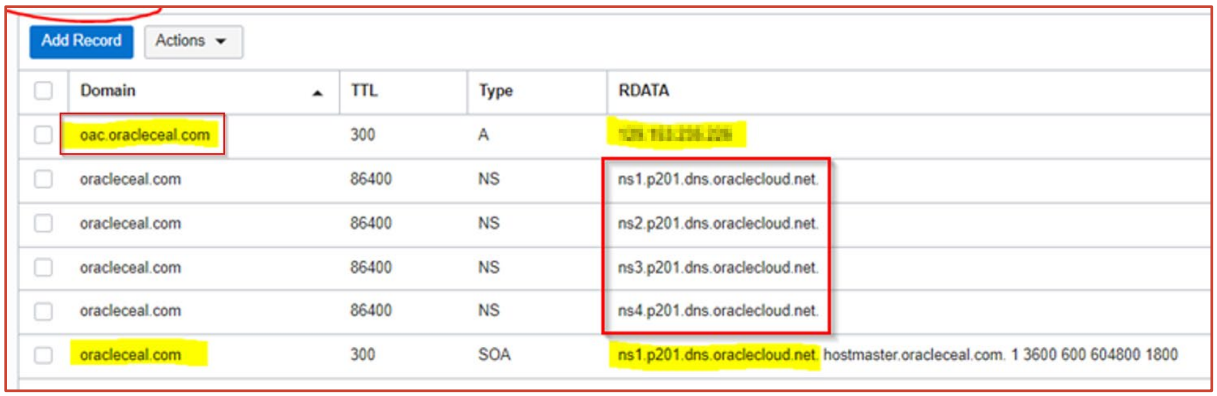
Obtain Name Server Hostnames of the OCI Public Zone

Add these Oracle name servers to your domain provider (for example GoDaddy).

Log in to the domain provider portal and change the name servers based on the DNS zone you created in OCI.

☐	oracleceal.com	86400	NS	ns1.p201.dns.oraclecloud.net.
☐	oracleceal.com	86400	NS	ns2.p201.dns.oraclecloud.net.
☐	oracleceal.com	86400	NS	ns3.p201.dns.oraclecloud.net.
☐	oracleceal.com	86400	NS	ns4.p201.dns.oraclecloud.net.
☐	oracleceal.com	300	SOA	ns1.p201.dns.oraclecloud.net. hostmaster.oracleceal.com. 1 3600 600 604800 1800





Once the domain is delegated to OCI, manage the DNS records from the OCI Console.

In GoDaddy DNS Management, create an **A Record** mapping the OAC instance IP address to the required sub domain. For example, **oac.oracleceal.com**.

In a disaster recovery situation, map the DR OAC instance IP address to the DNS name in the domain (GoDaddy) DNS management page.

> **Note:** You can't create the same public zone in multiple regions of OCI due to its public nature. Therefore, we recommend that you set up the public zone in the OCI DR region.

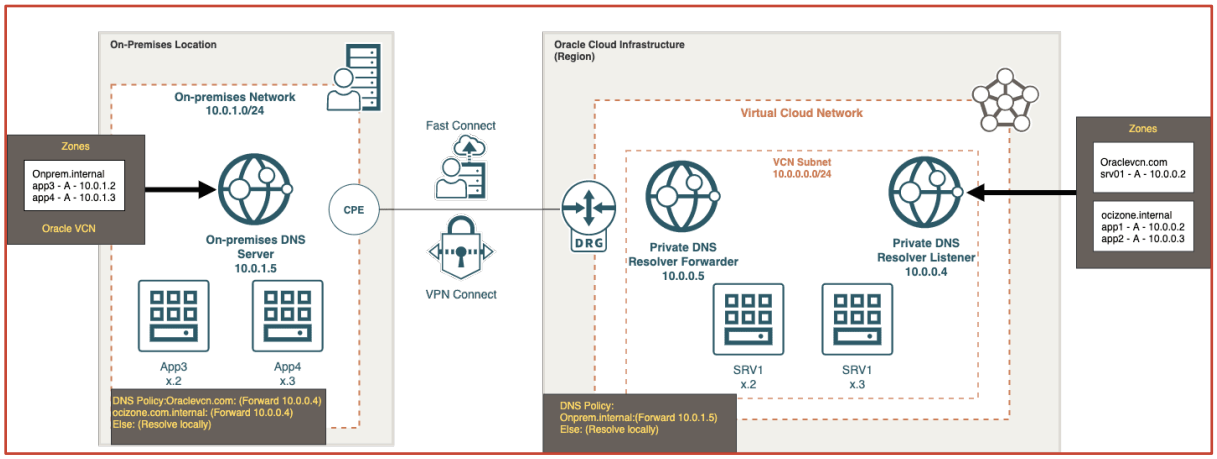
For Private OAC Access

After setting up the vanity URL at both OAC instances, map the IP address of the active OAC instance to the DNS name in the on-premises DNS servers.

You can also create private zones in OCI DNS management. See Private DNS.

- **Private DNS zones**: Private DNS zones contain DNS data only accessible from within a VCN such as private IP addresses. A private DNS zone has similar capabilities to an internet DNS zone but responds only to clients that can reach it through a VCN. Each zone belongs to a single view.

See the blog: OCI Private DNS - Common Scenarios.



Test the Vanity URL of the Active OAC instance:

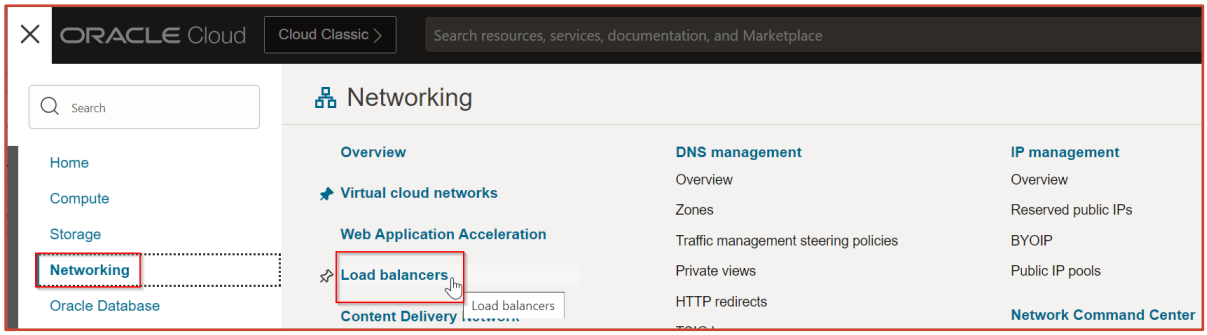
https://oac.cealoracle.com/ui/dv

Create a Public OCI Load Balancer in Both OCI Regions (Scenario 3)

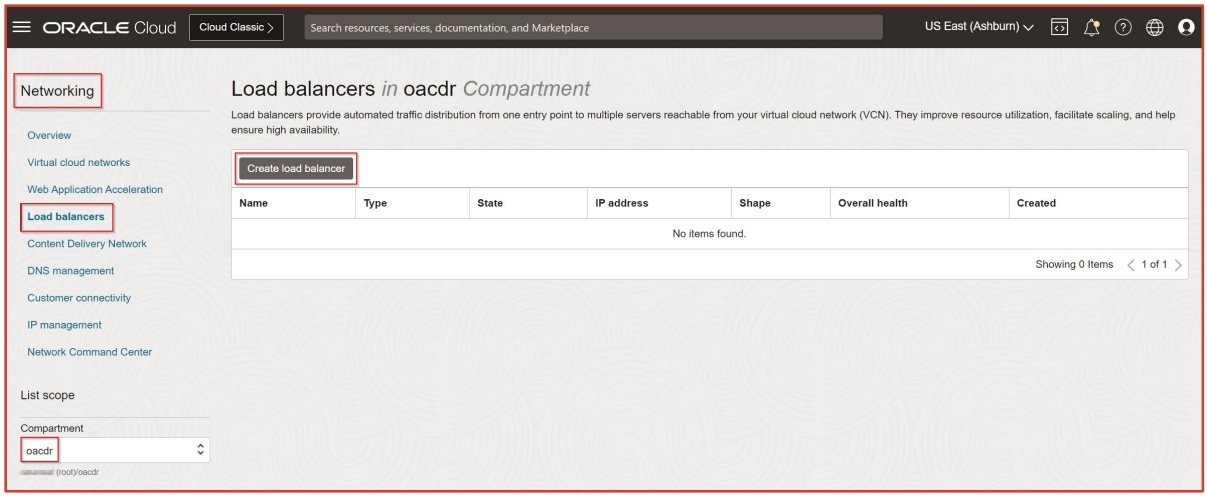
Create a public OCI load balancer and configure the OAC IP address as the backend of the load balancer.

- Use the Status Code 502 while configuring the Backend Set Health Check.
- Use the same certificate and private key generated and signed while configuring the vanity URL.

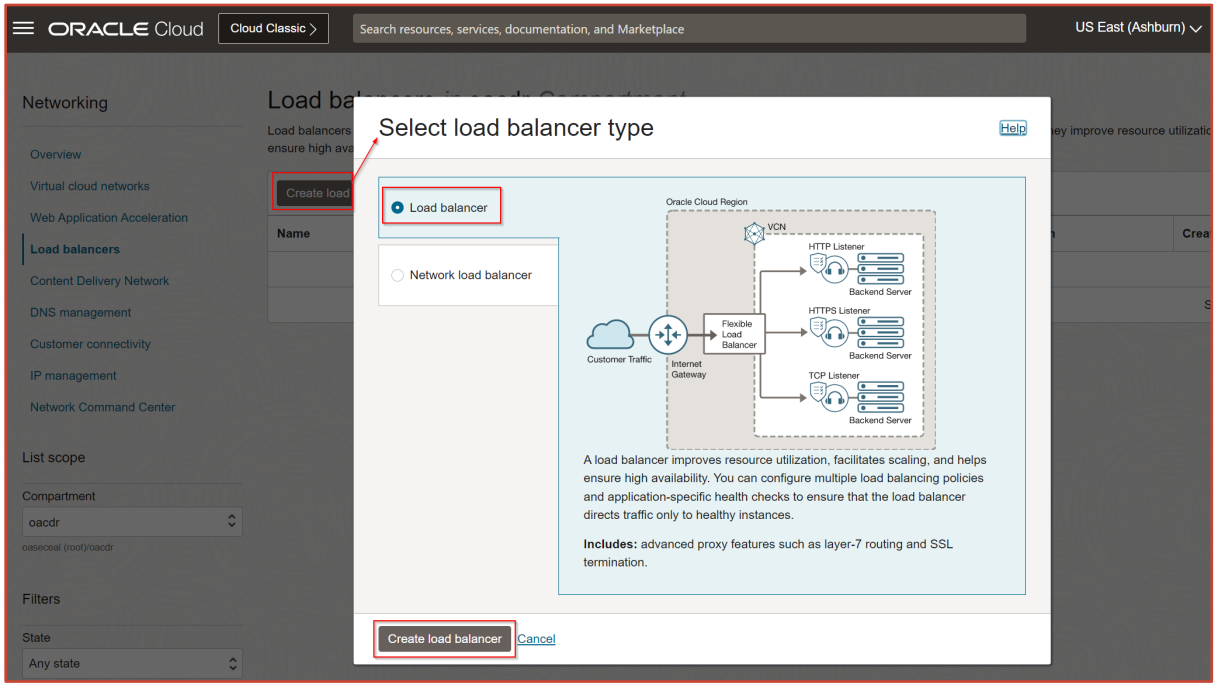
1. Log in to the OCI Console as an administrator.
2. Navigate to **Networking → Load Balancers**.



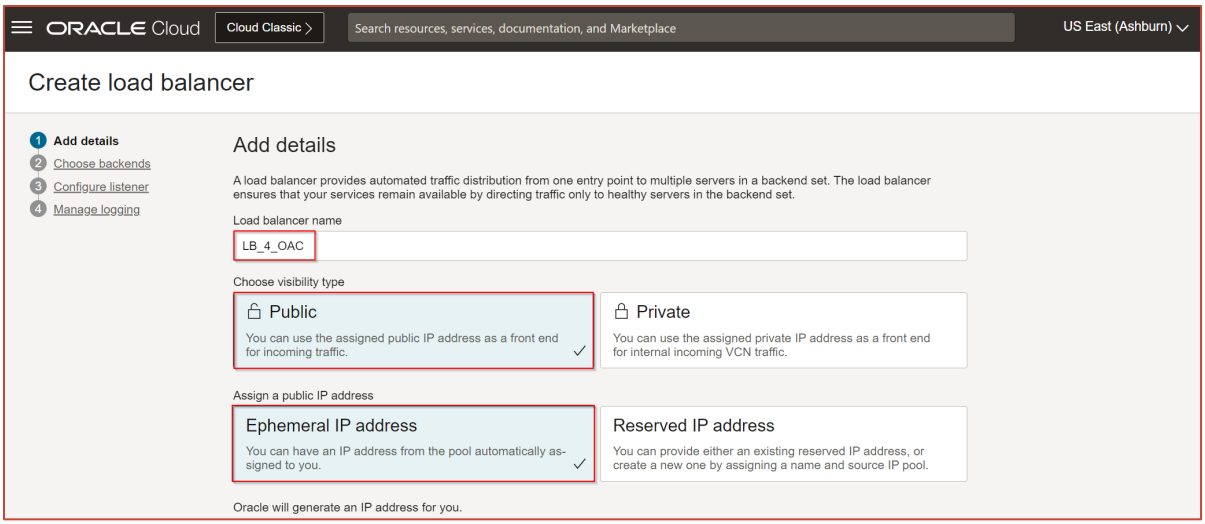
3. Select the compartment where you need to configure the load balancer.
4. Create a load balancer.



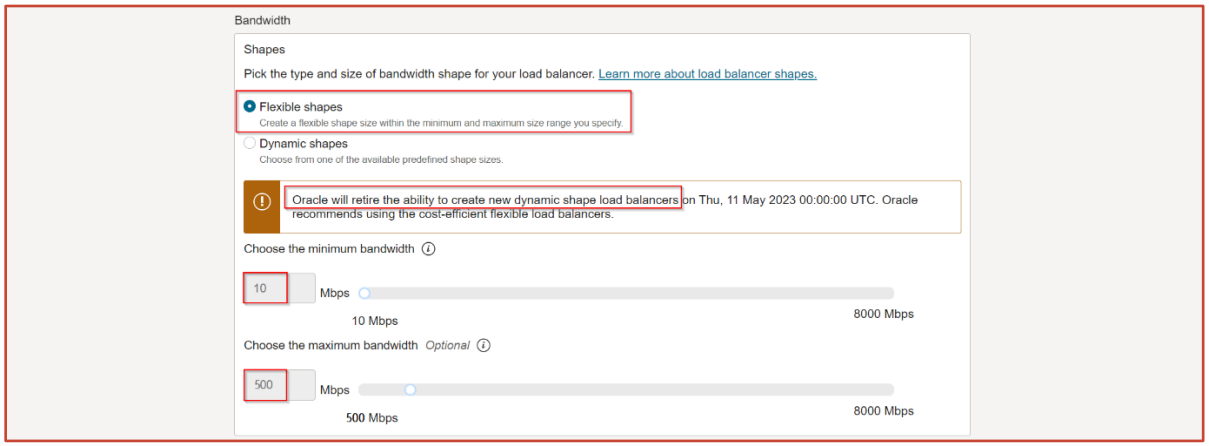
5. Select the load balancer type as **Load Balancer** and click **Create Load Balancer**.



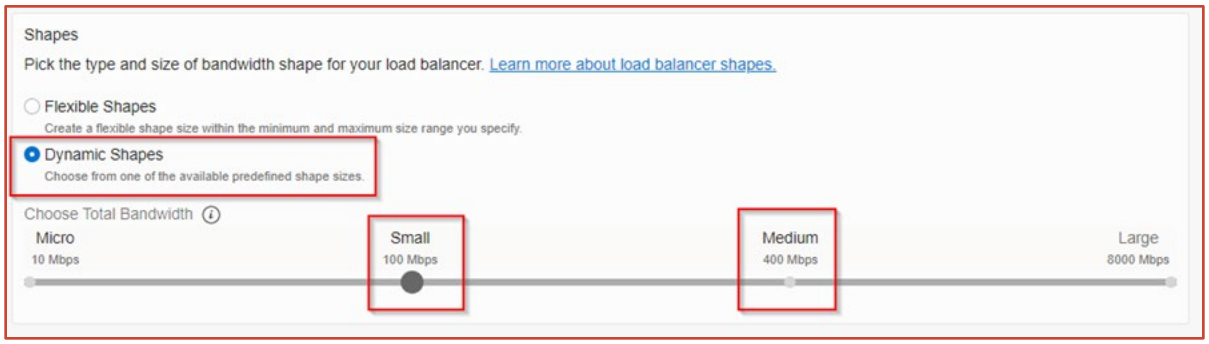
6. Create a public load balancer.



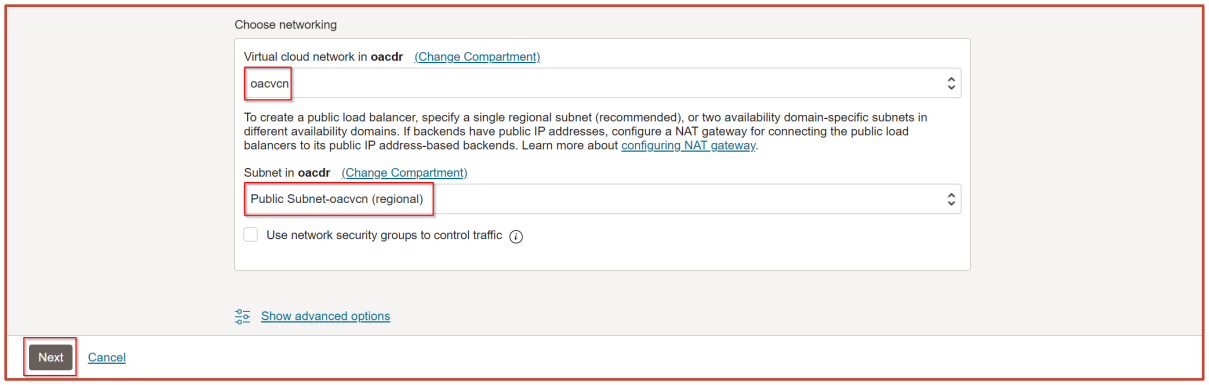
7. Select the **Flexible** shape.



Note: The **Dynamic** shape will be retired soon.



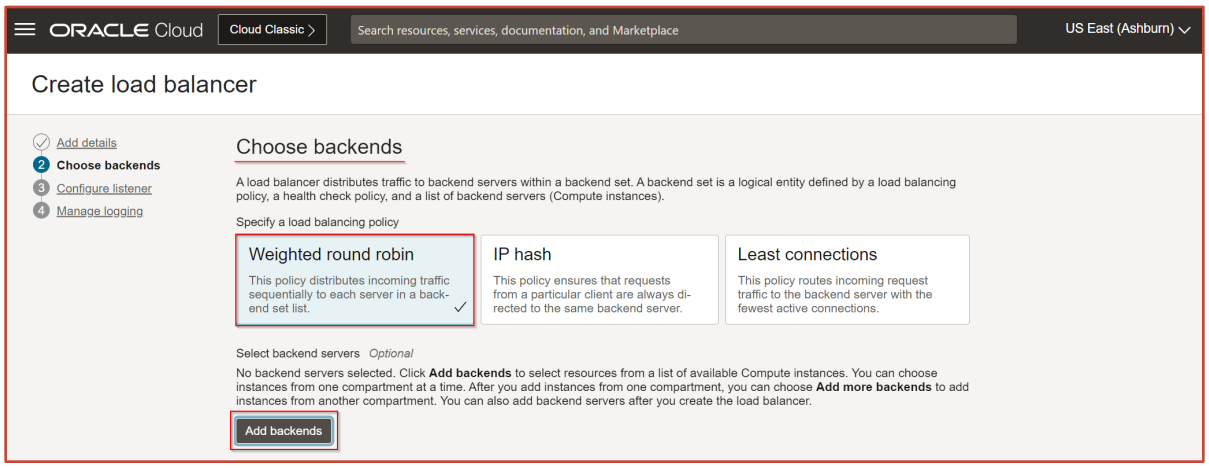
8. Select the network.



Click **Show Advanced Options → Security tab**. A Web Application Firewall (WAF) can be configured for securing OAC on Oracle Cloud. Configure WAF if you need extra protection.

9. Click **Next**, and specify the load balancer policy as **Weighted Round Robin.**

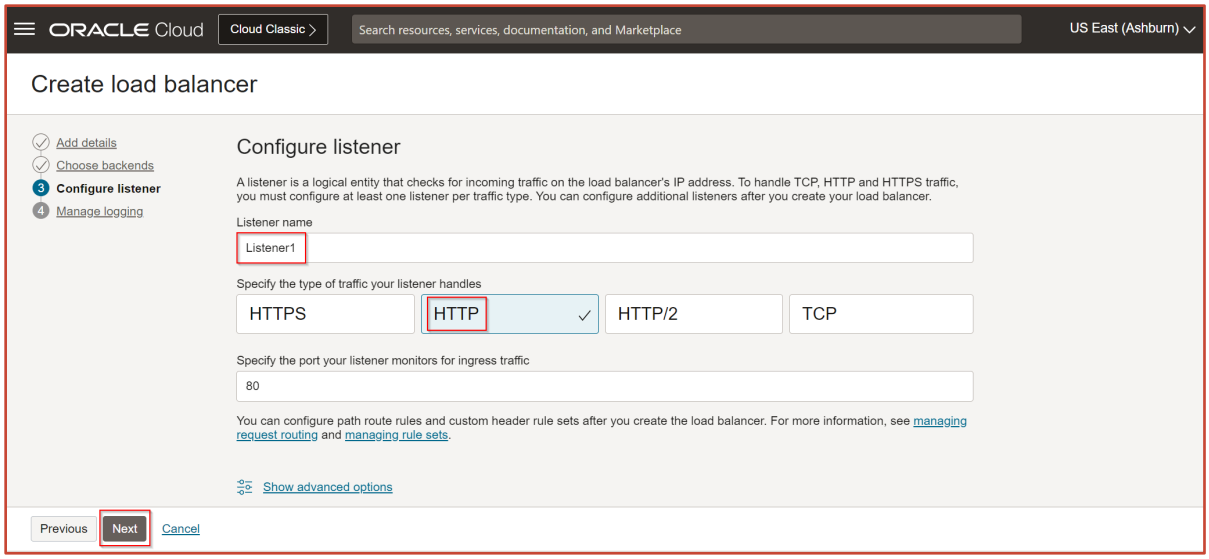
Note: You can use other policies based on the type of configuration required for the usage.



10. Since the OAC instance isn't listed when you select the backend, you can add the IP address of the OAC instance later. Also, you can skip the Health Check Policy with default values as this will be configured after the load balancer is configured.

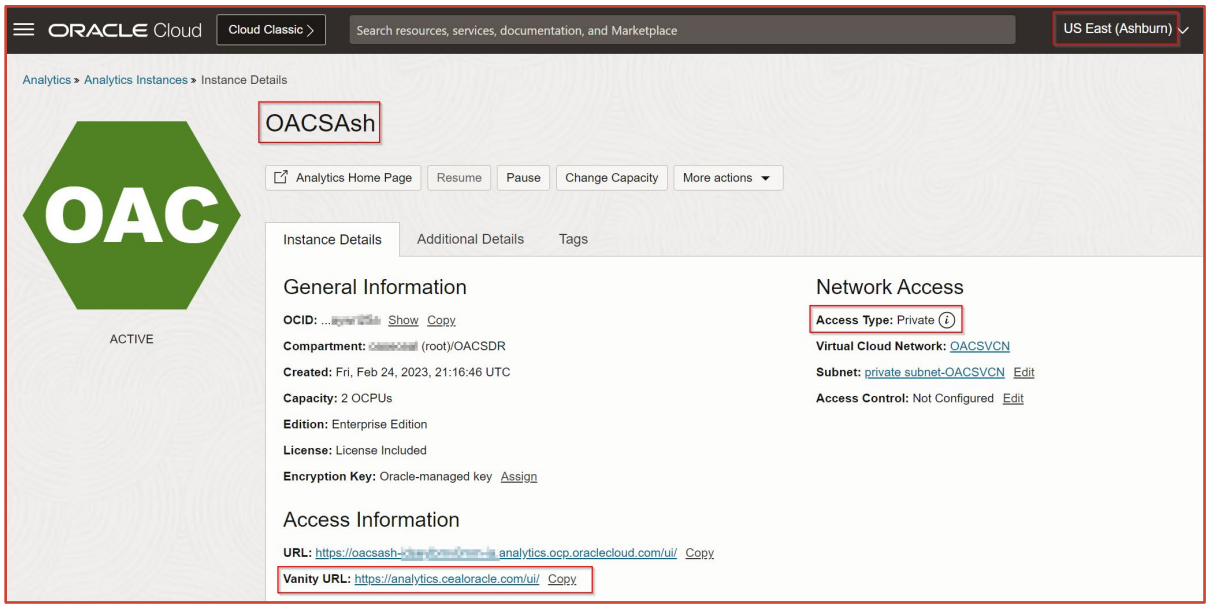
Click **Next**.

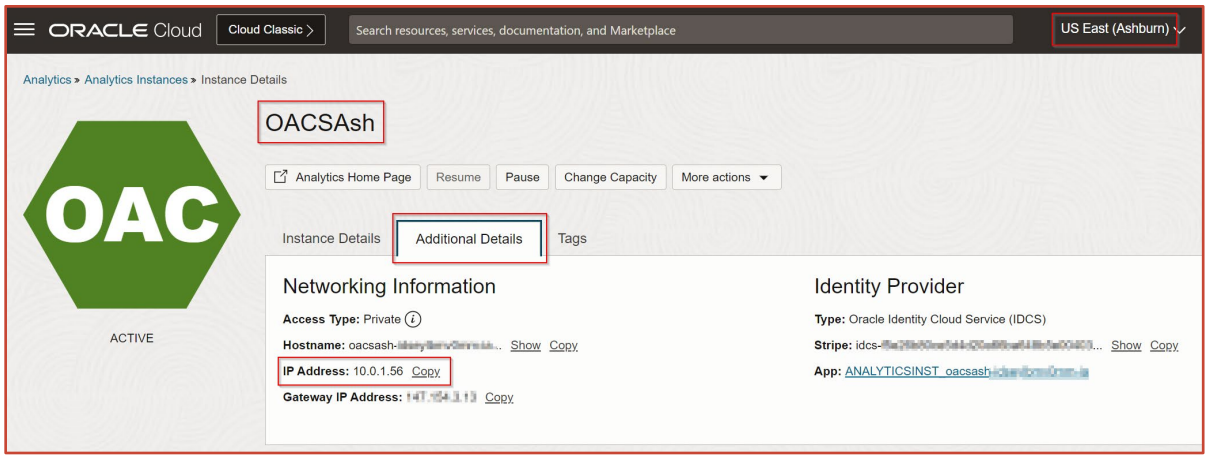
11. Configure the listener with the listener type as **HTTP**. You can update the load balancer later, with the listener type as **HTTPS**.



12. Enable the **Error Logs and Access Logs** and click **Submit**.

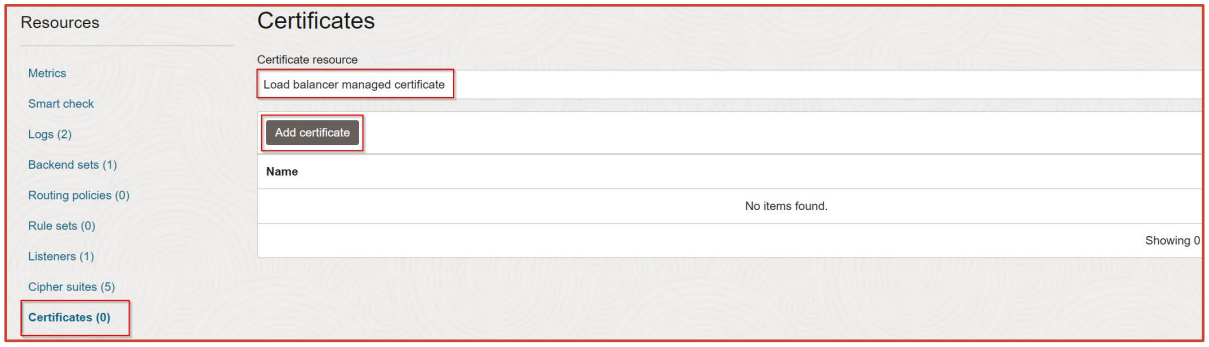
Get the private OAC instance IP address to configure as the backend for the load balancer.

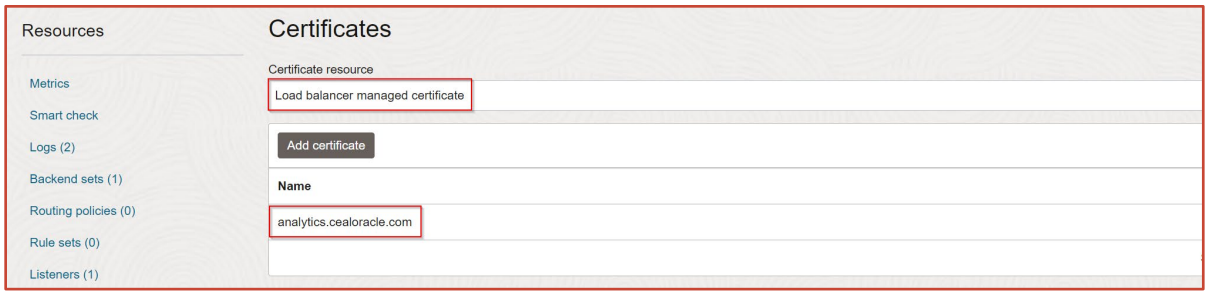




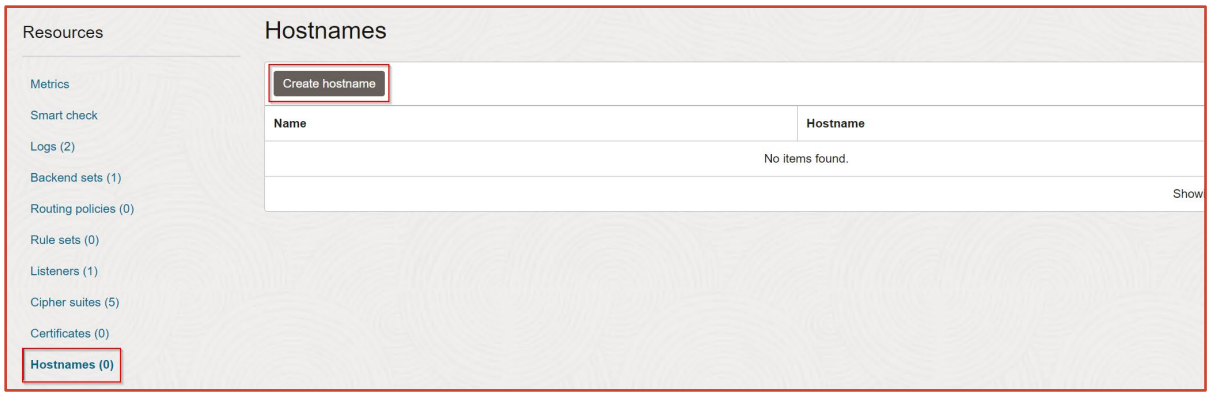
13. When the load balancer is created, add a certificate.

Note: Use the well-known public CA signed certificate, private key, and the CA chain certificate that you used when you created the vanity URL for the private OAC instance.

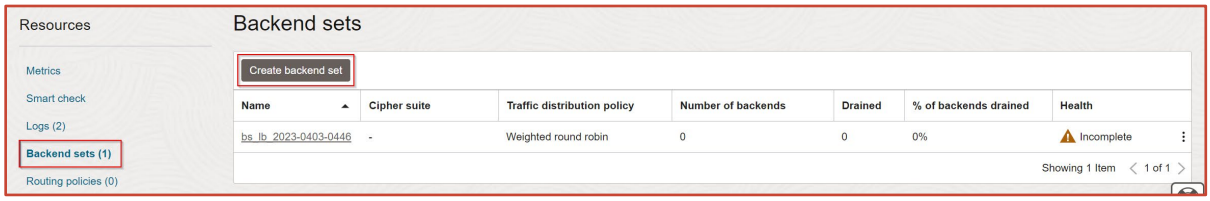




14. Add a hostname.



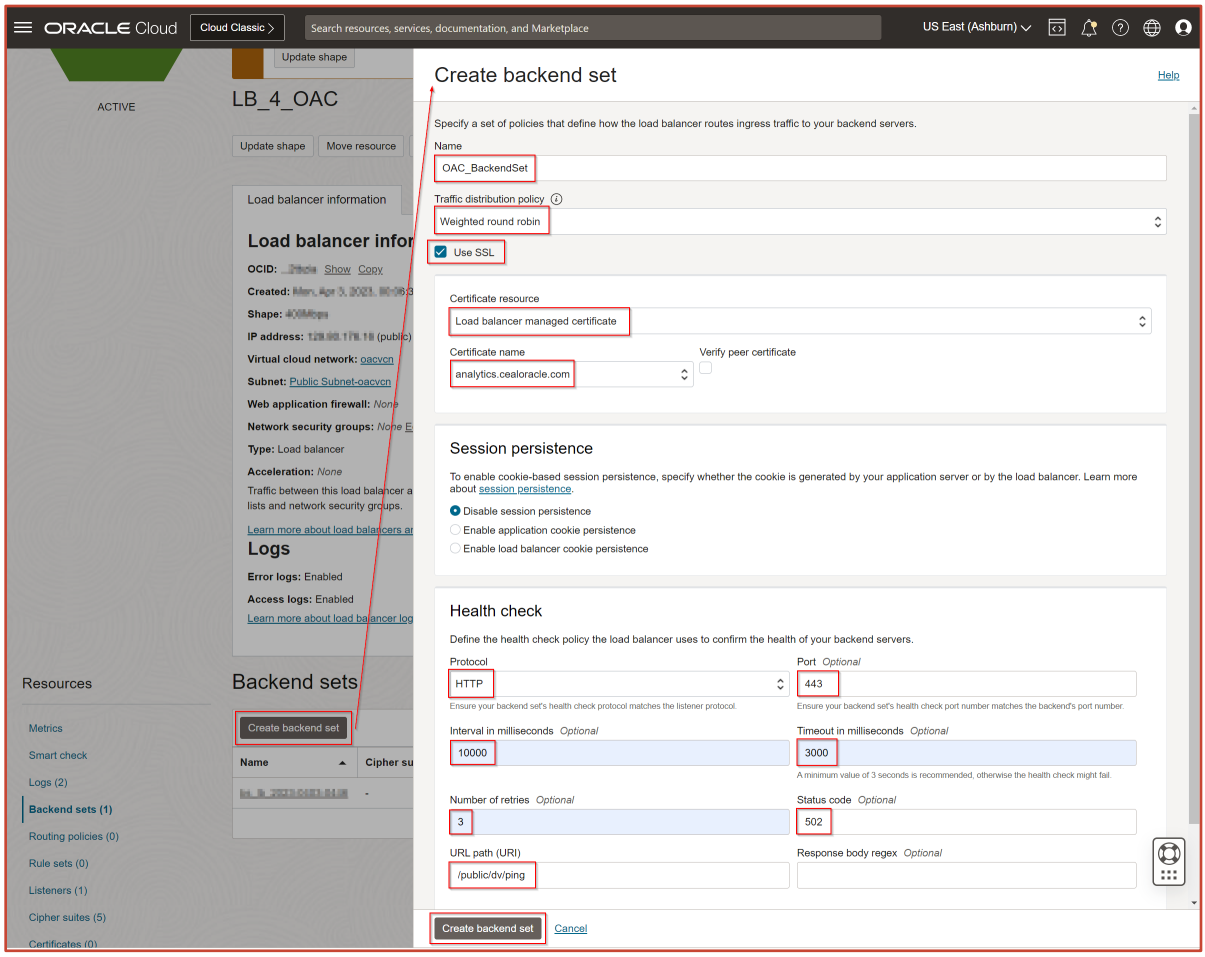
15. Create a new backend set.

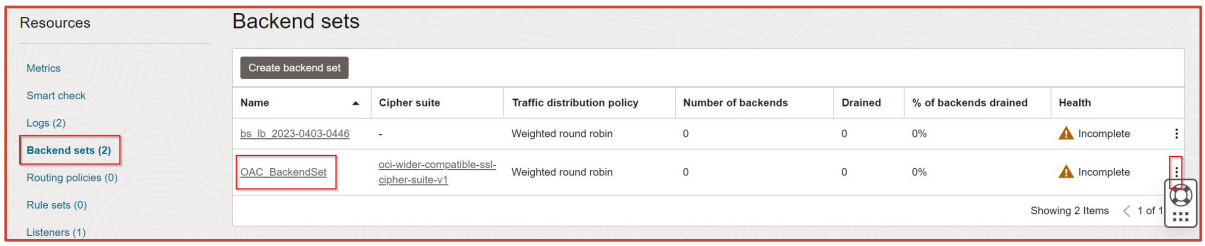


Select **Use SSL** since the OAC is SSL-enabled.

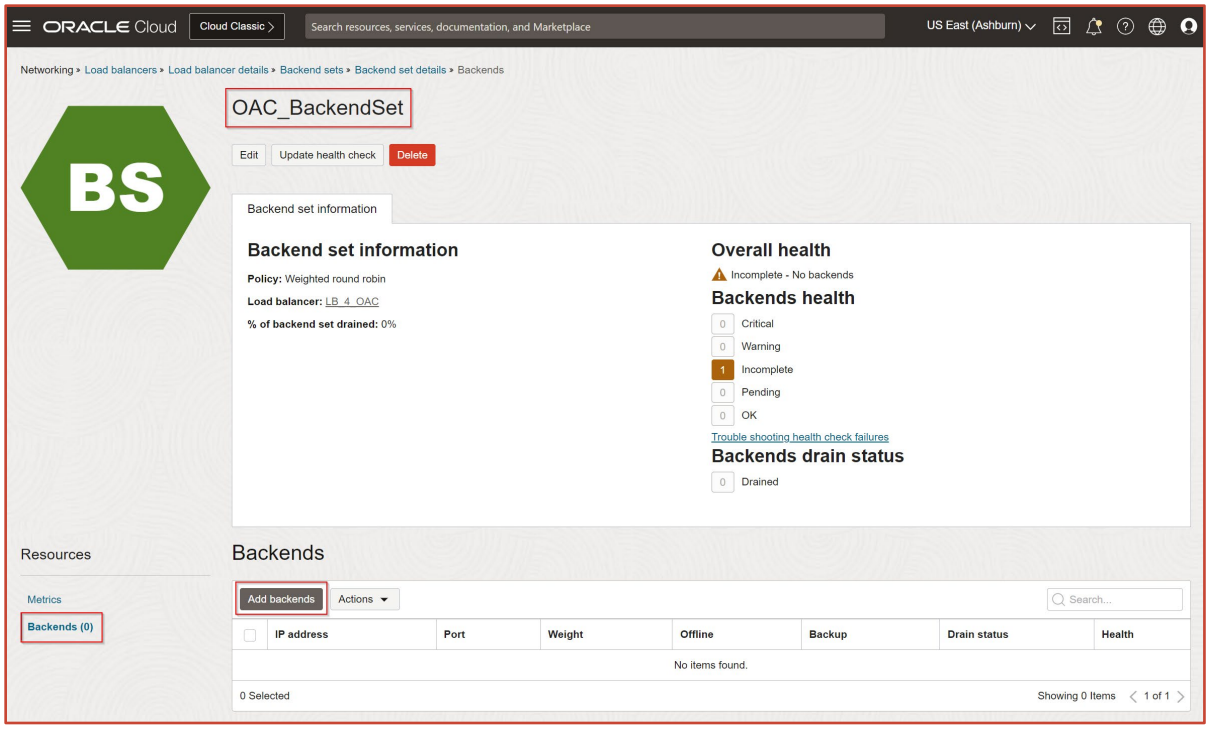
Use the certificate created in the previous steps.

Configure the **Health Check** as shown in the screenshot.





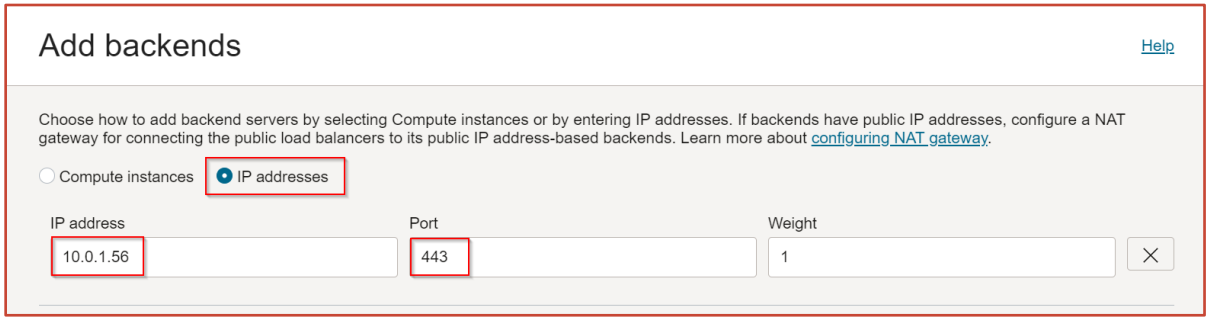
16. Add backends to the backend set.



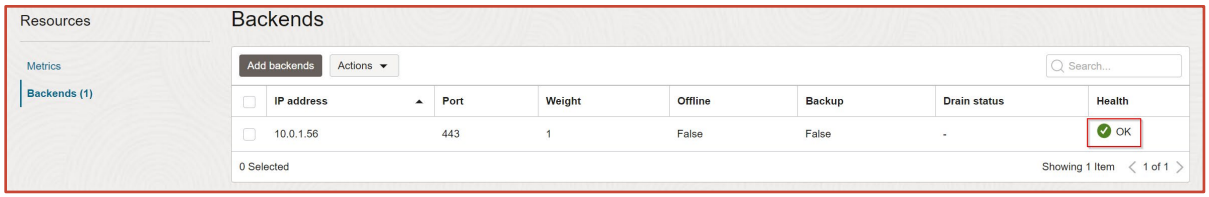
Note: The load balancer should be able to reach the private OAC instance.

Using the security list, configure the ingress rules to allow the load balancer to reach the OAC instance.

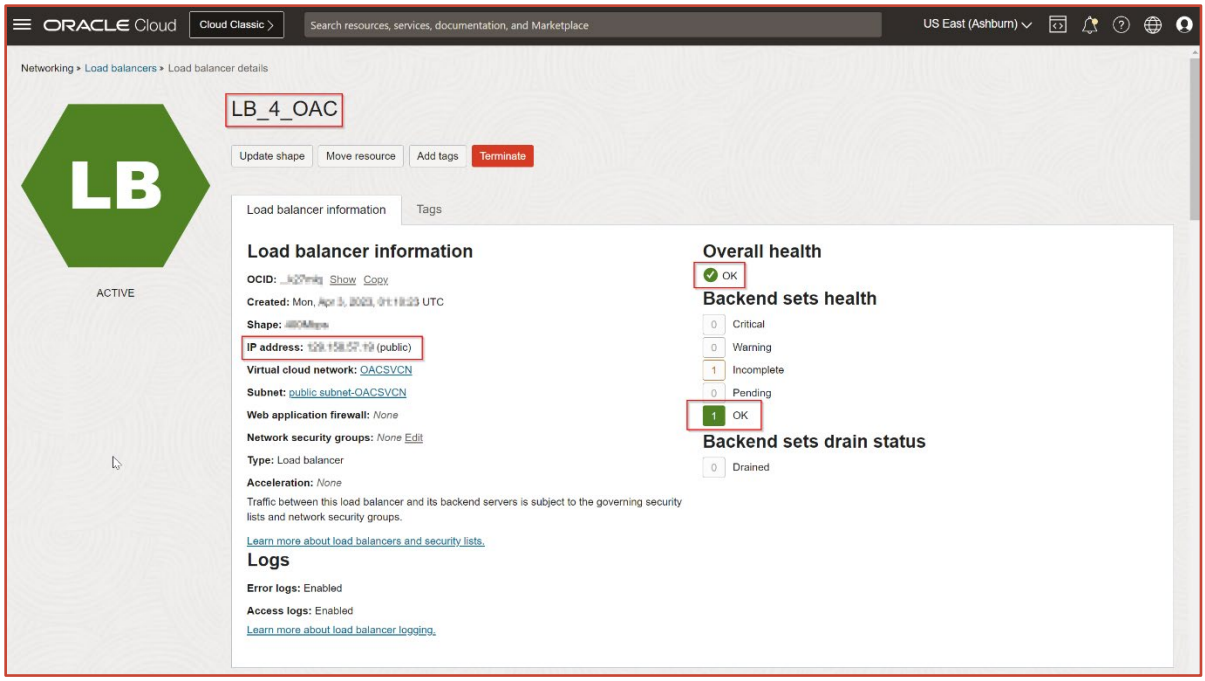
Note: If the load balancer and the private OAC instance are on different VCNs, you must set up local peering between the two VCNs using the Local Peering Gateway.



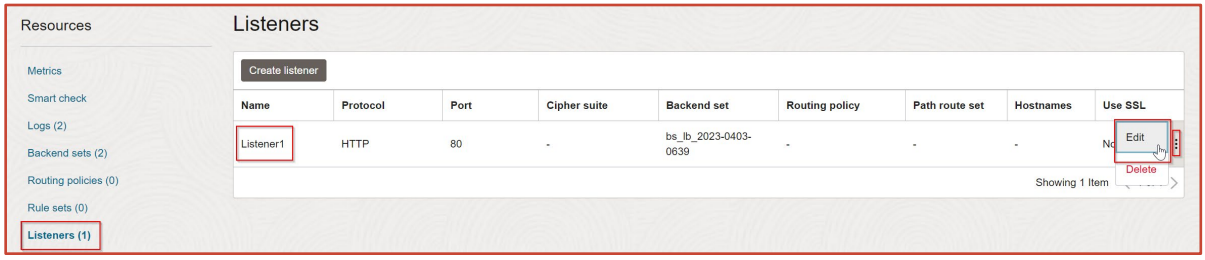
17. The Health should show **OK**.

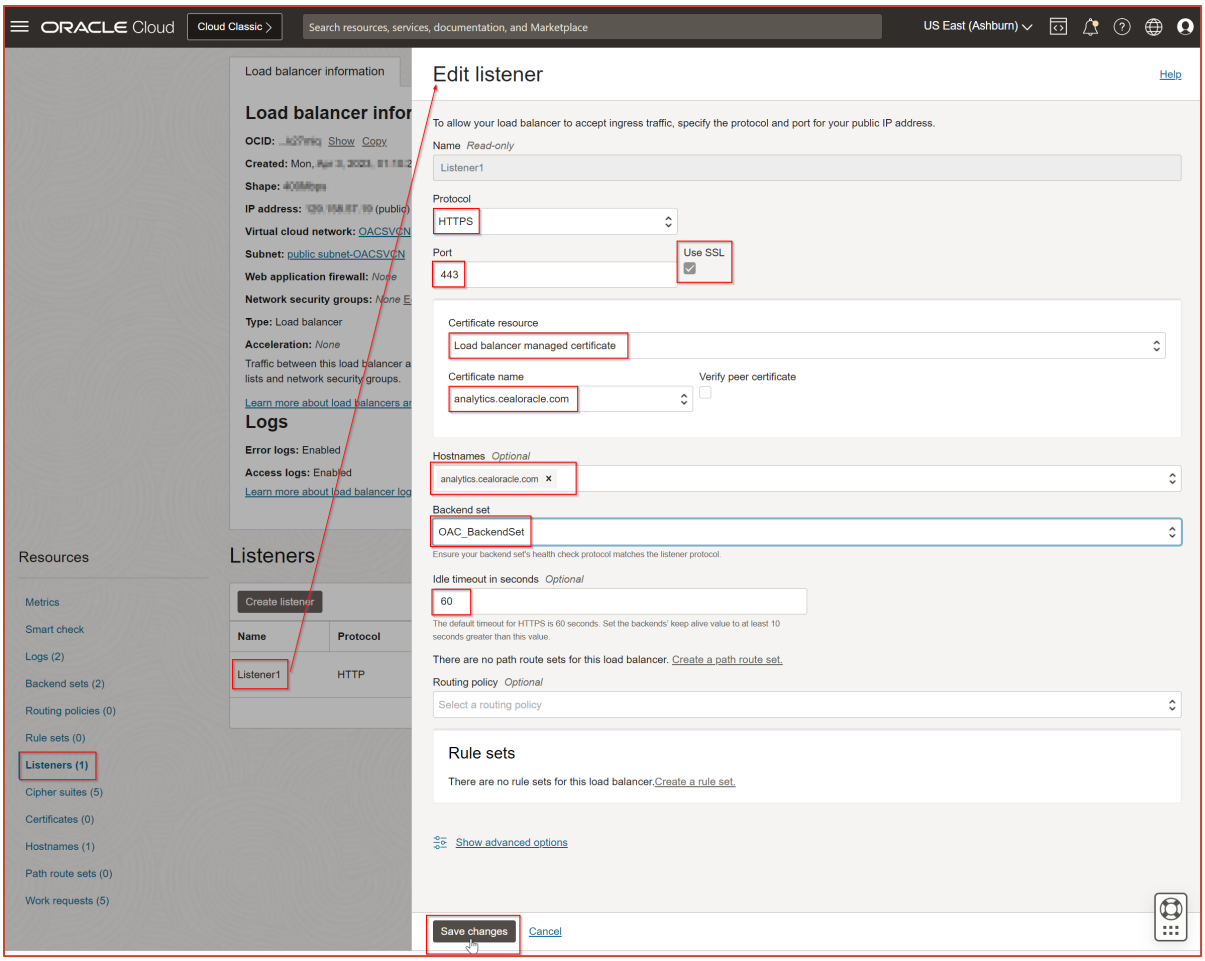


18. Overall health and backend set health should show **OK**.



19. After the load balancer is created, edit the listener and add the certificate, hostname, and the backend set.



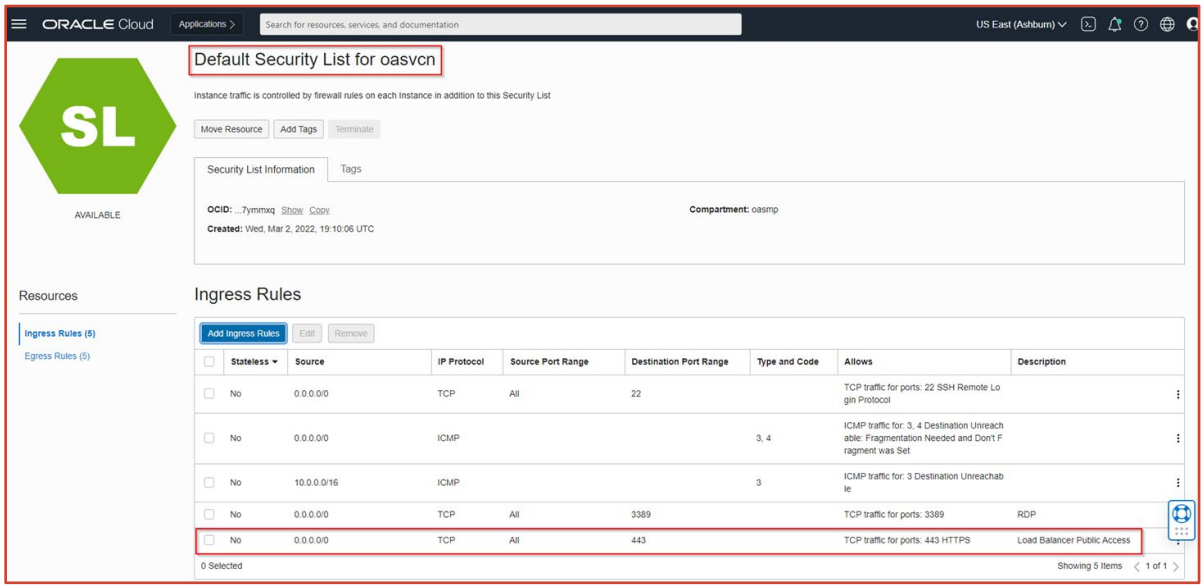


20. Delete the old backend set initially created with the load balancer.

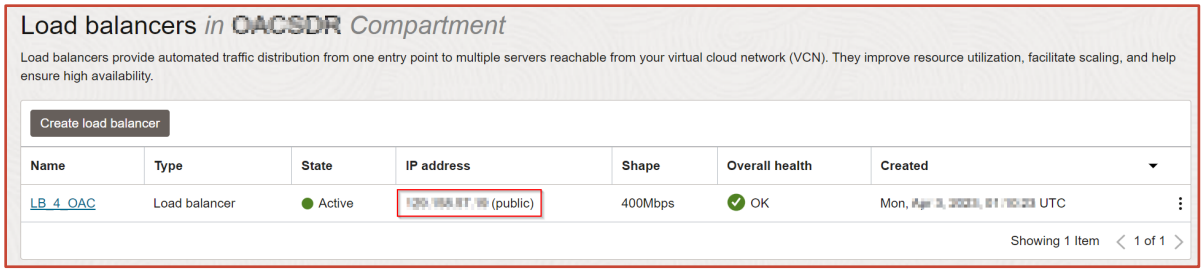
Refer to Timeout Settings.

21. Allow internet traffic to the load balancer's public subnet.

- Add an ingress rule to allow access from the internet (0.0.0.0/0) on port 443.



22. Add an **A Record** in the domain provider's DNS management screen.



Map the load balancer's public IP address to the DNS name in your DNS resolver and domain provider. For example, https://analytics.cealoracle.com/ui

Secure Oracle Analytics Cloud on Oracle Cloud by Enforcing OCI WAF

OCI's Web Application Firewall (WAF) is a cloud-based, PCI-compliant, global web application firewall service. By combining threat intelligence with consistent rule enforcement on Oracle Flexible Load Balancer, WAF strengthens and protects internet-facing web applications, API endpoints, and load balancers (public or private).

- Ensure that you have the required IAM policies to implement WAF. See Required IAM Service Policy.
- (Recommended) Use a separate compartment for your WAF policy to make management easier and more secure. See Managing Compartments.

Web application firewall policies encompass the overall configuration of your WAF service, including access rules, rate limiting rules, and protection rules. For information on how to implement access control and protection rules read the blog Securing Oracle Analytics Server on Oracle Cloud by Enforcing OCI WAF on Flexible Load Balancers.

Test End-to-End Connectivity with Network Path Analyzer

After configuring private access channel (PAC), Data Gateway (RDG), load balancer, and other supported scenarios for OAC, you can use the Network Path Analyzer to test end-to-end connectivity.

Use the Network Path Analyzer to:

- Troubleshoot routing and security misconfigurations causing connectivity issues.
- Validate that the logical network paths match your intent.
- Verify that the virtual network connectivity setup works as expected before sending traffic.

For more information about Network Path Analyzer, OAC, and OCI networking, read the blog Speed up Network Troubleshooting with Oracle Cloud Network Path Analyzer for Oracle Analytics Cloud.

ADW Switchover Using Data Guard

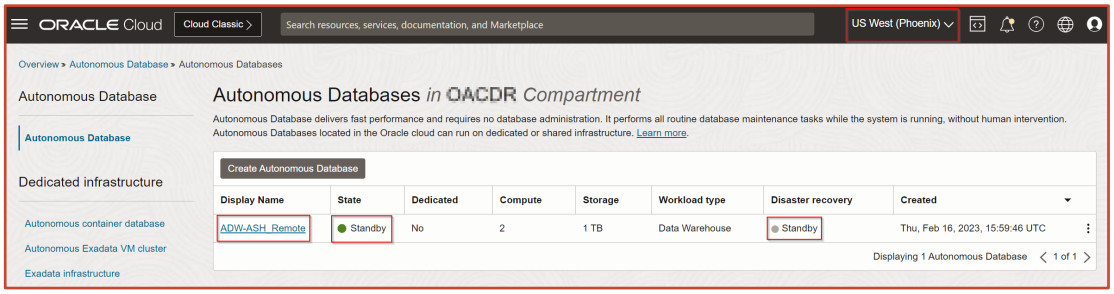
When a disaster occurs, switchover must be done in the DR region's standby ADW instance.

> **Note:** Cross-region switchover from the primary database of an Autonomous Data Guard association isn't supported.

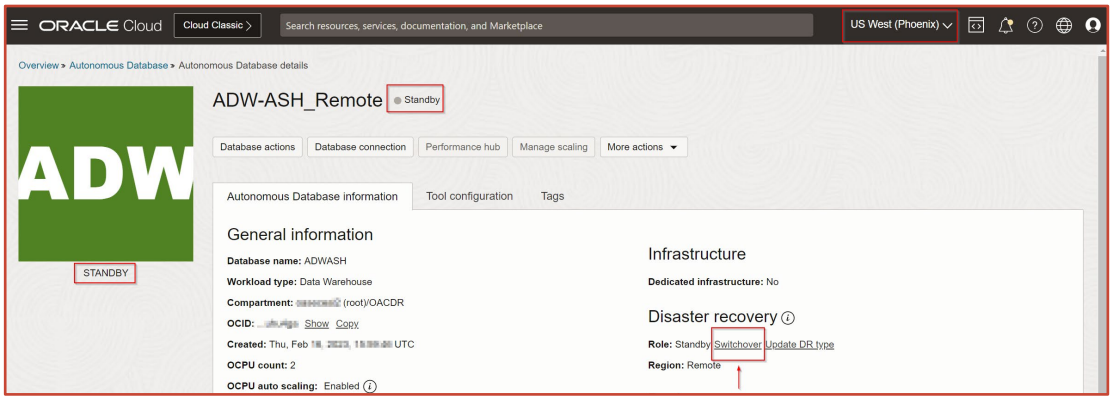
Perform the switchover operation on the standby database.

On the DR Region (Phoenix)

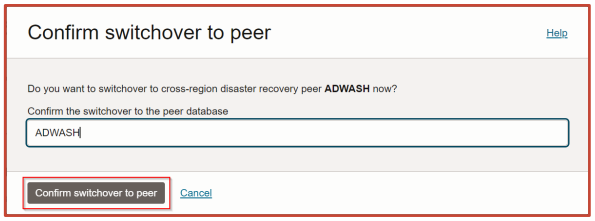
1. Log in to the OCI Console as an administrator.
2. Navigate to the ADW instance.



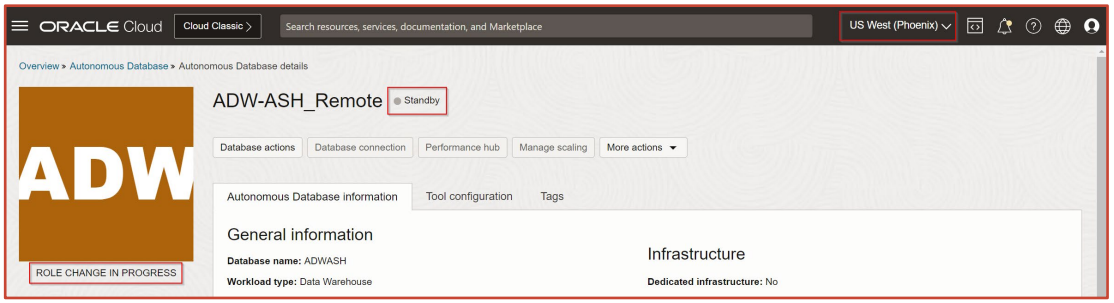
3. Click the **Switchover** option.



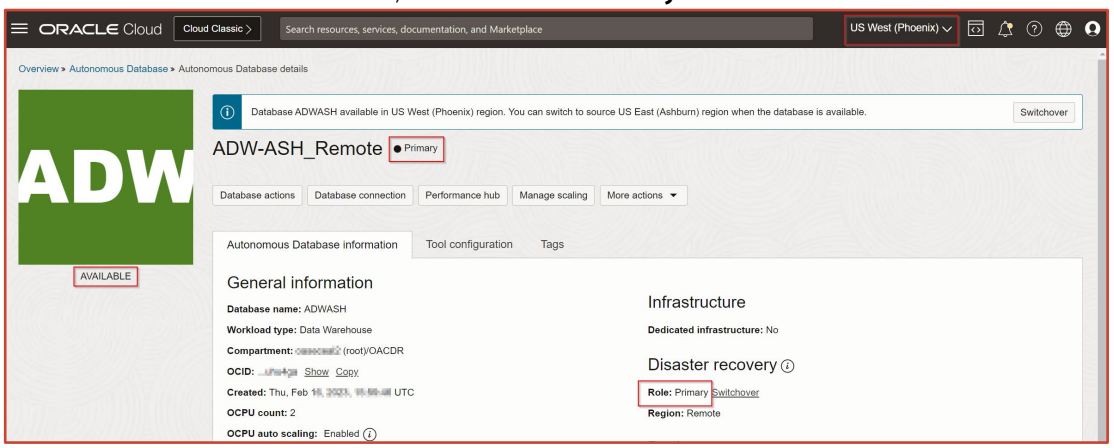
4. Confirm the switchover.



5. The status of the ADW changes to **ROLE CHANGE IN PROGRESS**.

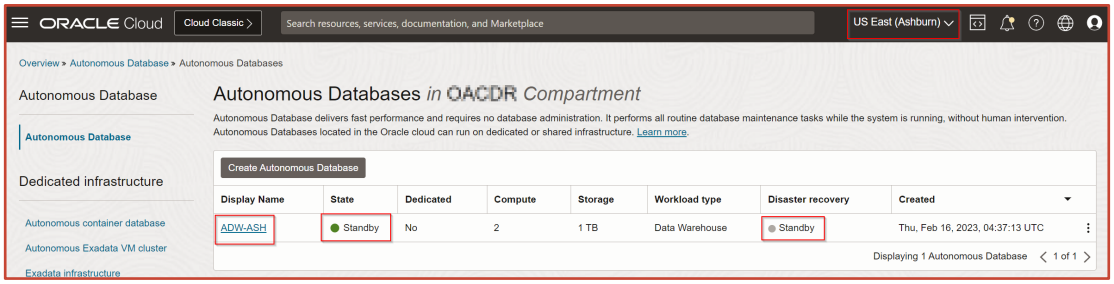


6. The Phoenix ADW is now available, and the Role is **Primary**.

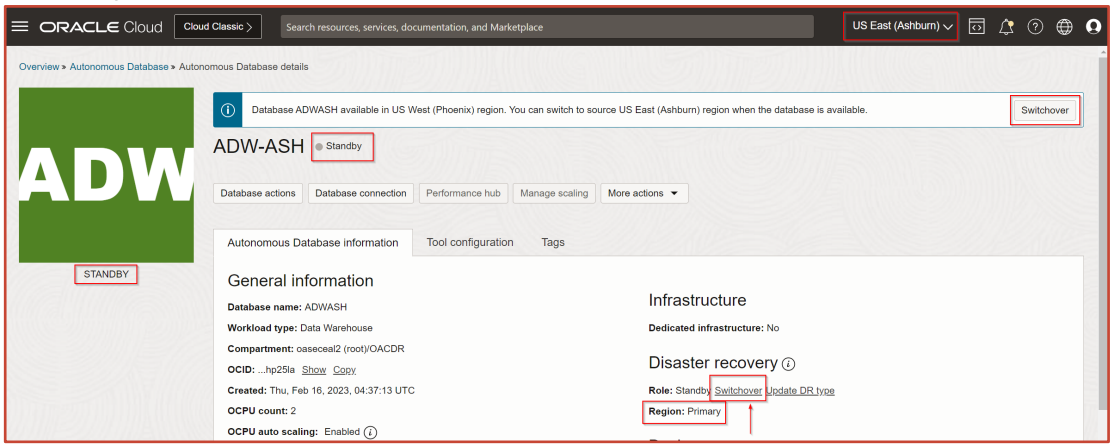


On the Home Region (Ashburn):

1. Log in to the OCI Console as an administrator.
2. Navigate to the ADW instance and check the status.



3. Fallback to the primary ADW on the home region can be performed using the switchover option followed by the same process.



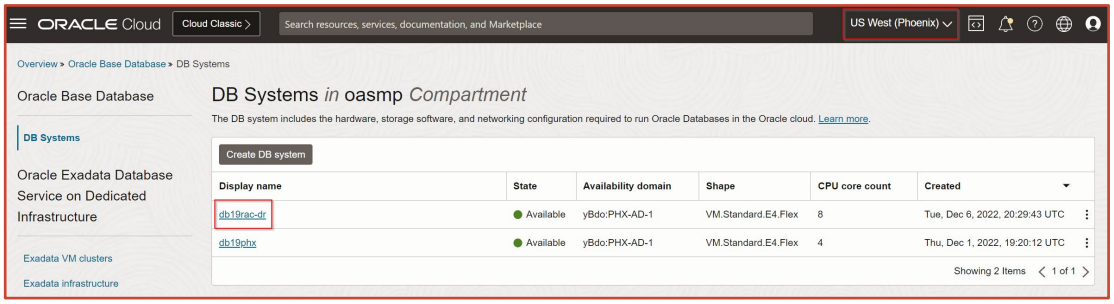
DBCS Switchover Using Data Guard

When a disaster occurs, a switchover must be done in the DR region's standby DBCS instance.

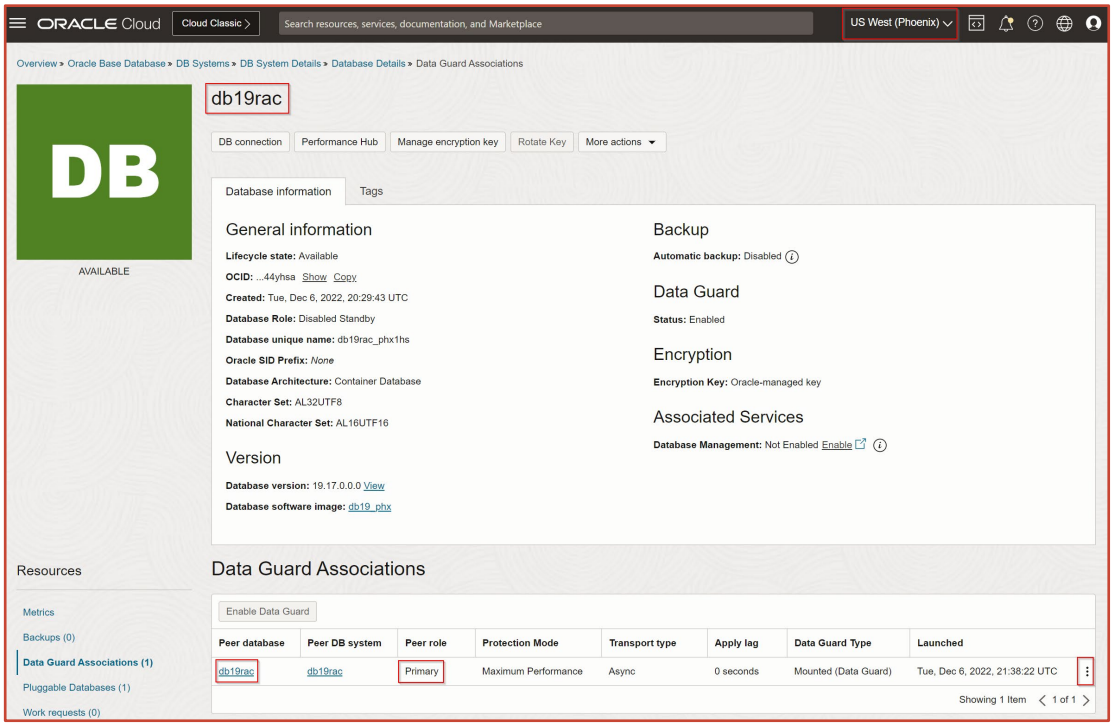
Perform the switchover operation on the standby database.

On the DR Region (Phoenix)

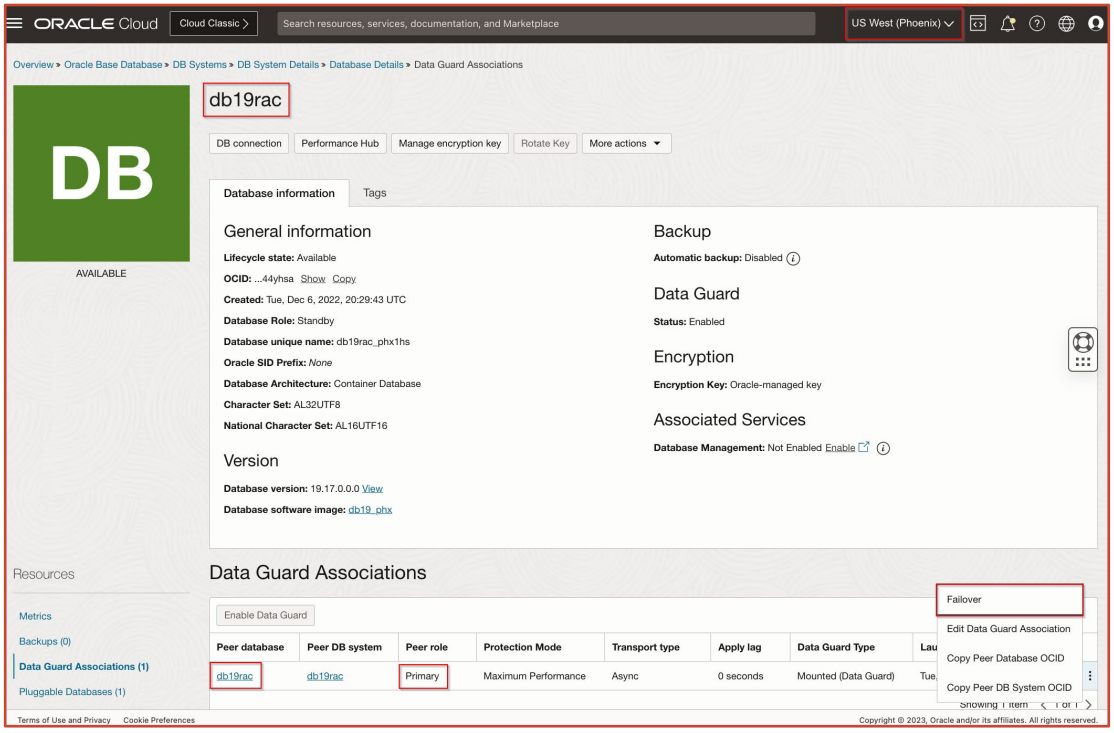
1. Log in to the OCI Console as an administrator.
2. Navigate to the DBCS instance.



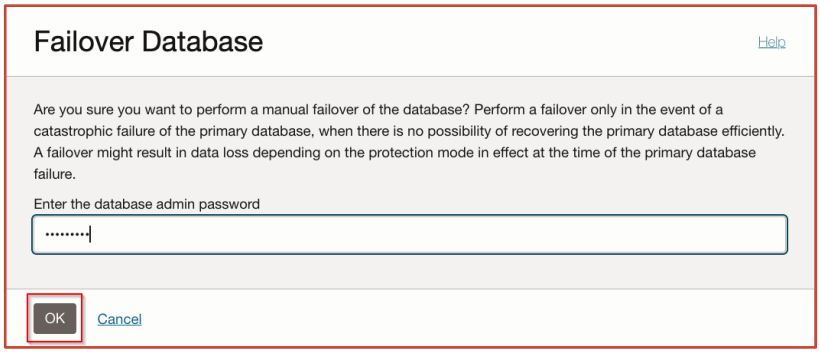
3. Navigate to **Oracle Base Database > DB Systems > DB System Details > Database Detail > Data Guard Associations**.



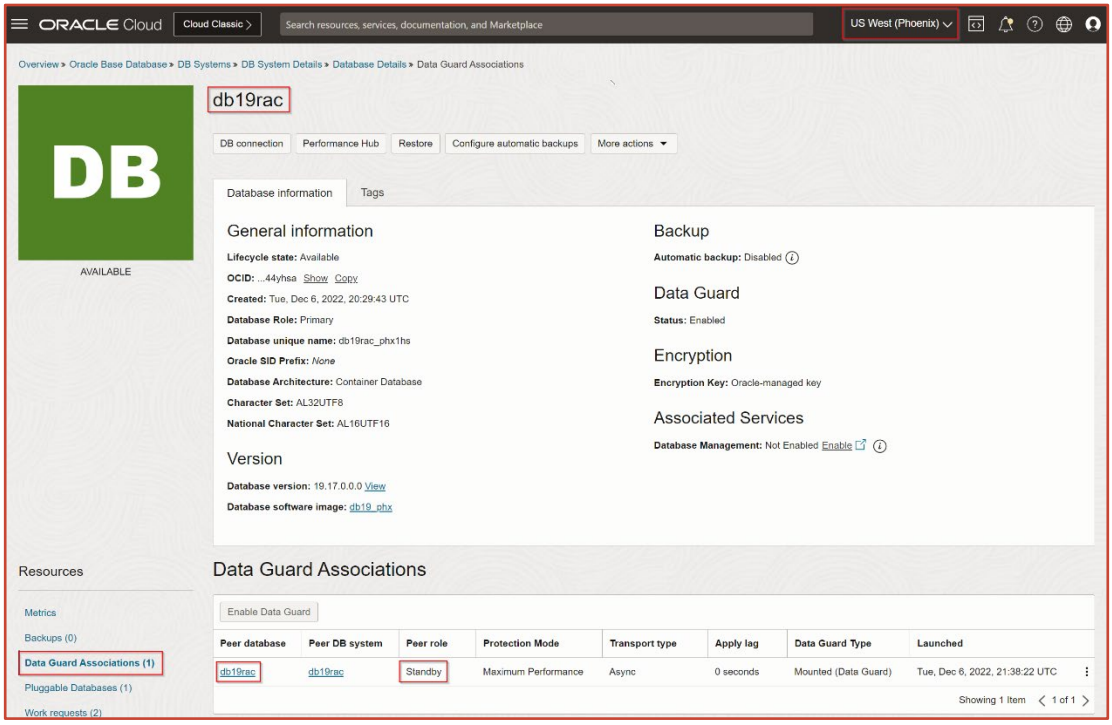
4. Click **Failover**.



5. Enter the administrator password.

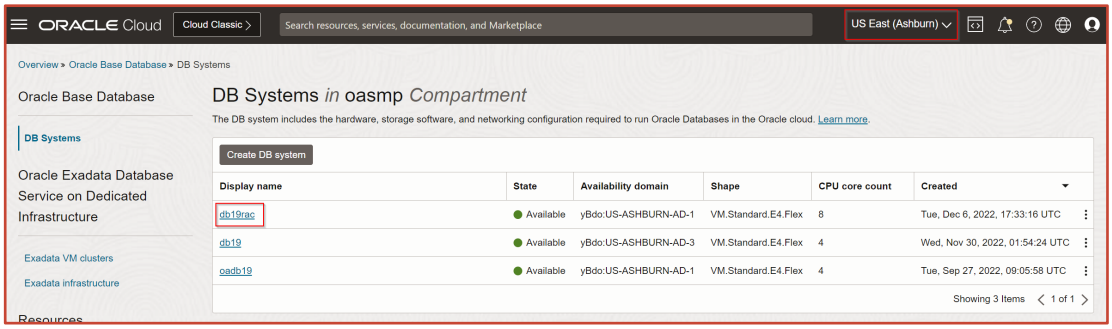


6. The status of the peer database updates to **Standby**.

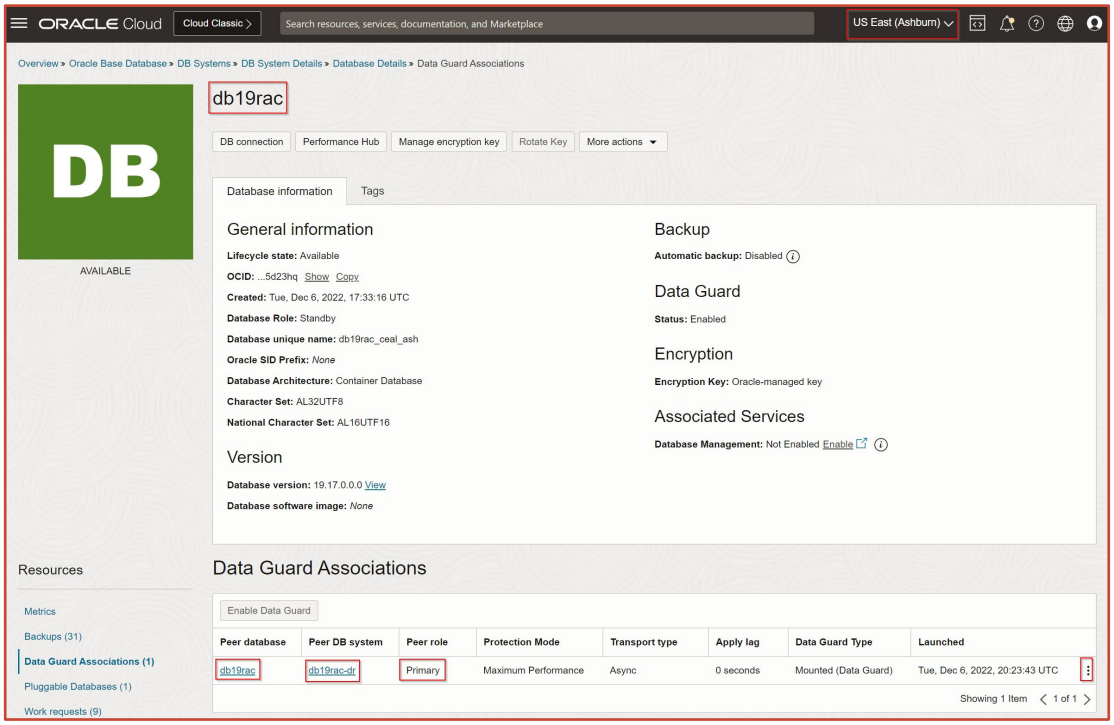


On the Home Region (Ashburn)

1. Log in to the OCI Console as an administrator.
2. Navigate to the DBCS instance and check the status.



3. Navigate to **Data Guard Associations**.



4. Fallback to the primary DBCS on home region can be performed using the Failover option, followed by the same process.

Fallback and Restore Limitations

In some OAC environments, end users only use the primary and DR OAC instances as consumers so there's no significant content development (analysis, dashboards, visualizations) in the production instance. In this case, you don't need to be concerned about losing data during a fallback from the DR OAC instance to the primary production OAC instance.

However, most OAC instances have some content development activity. In this case, you need to consider the loss of any objects created after a snapshot back up and any data loss resulting from the disaster event after restoring the OAC primary instance.

Fallback from Disaster Recovery OAC Instance to Primary OAC Instance using Snapshot Migration

In some disaster recovery situations, there are changes to artifacts (analyses, dashboards, visualization projects, catalog folder permissions, application roles and memberships, connections, datasets, and on) on the DR OAC instance. In such cases, we recommend that you create a snapshot and data files backup from the DR OAC instance and restore them to the primary OAC production instance.

You can use the automation scripts provided earlier in this document to complete this task (**createSnapshot.sh** and **registerSnapshot.sh**).

Subscribe to OCI Console Announcements

Customers can check the status of OCI from the OCI Service Health Dashboard. To ensure that you receive OCI console announcements that you consider relevant, create an announcement subscription. To subscribe to announcements, see Subscribing to Announcements.

From this dashboard, you can get status information about the services in your region. Notifications are delivered whenever OCI creates or resolves an incident.

For an overview, watch the video: Oracle Cloud Infrastructure Announcements: Overview.

Cost Considerations

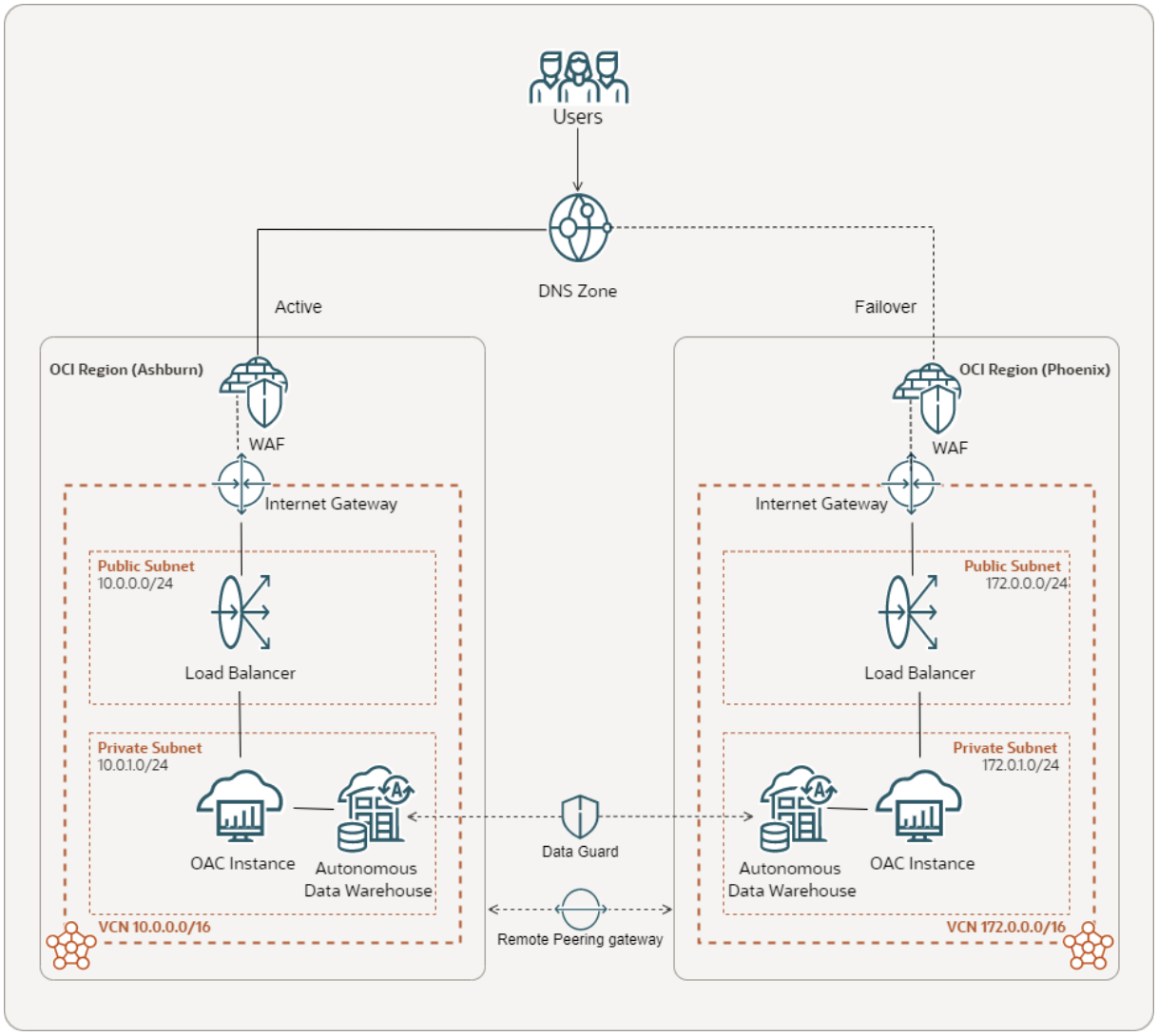
Since the DR OAC instance is a backup of the production instance, you might create the OAC instance with higher OCPUs, which might impact costs.

You can consider pausing the DR OAC instance and then resuming it on an as needed basis. For example, to run a DR drill and for a DR event.

You can automate pause and resume operations for OAC instances using the OCI CLI utility. See How to Stop and Start an OAC Instance using OCI Command Line Interface (CLI).

Perform DR Drills

This section describes a DR drill for a typical OAC environment (shown in the diagram).



A typical DR drill for OAC includes the following key steps:

- **Define the scope and objectives:** Clearly define the scope of the DR drill, including which OAC and OCI components will be included, what types of disasters or failure scenarios will be simulated, and what objectives need to be achieved during the drill.
- **Validate user replication and synchronization:** Since you need to synchronize users and groups from the primary IDCS or IAM domain to the DR IDCS or IAM domain during a DR event, validate that the mechanism is working as expected and can be used in case of a disaster.
- **Test back-up and recovery of OAC content:** Test the back-up and recovery of snapshots and data files using the automation scripts provided. If needed, extend the scripts to achieve your additional requirements.
- **Test failover and switchover of the database:** If you're using a DR solution, such as Oracle Active Data Guard, test the failover and switchover processes to ensure that they can be performed quickly and reliably in case of a disaster.
- **Test recovery of the OAC instance in the DR region:** Test the backup and recovery processes for your OAC environment by simulating a failure scenario, such as primary OAC instance unavailability. Ensure that you recover the dependant services (such as identity management), data sources, system settings, and snapshot of the DR OAC environment to a consistent state and that all your data is available and accurate.
- **Document results and lessons learned:** Document the results of the DR drill, including any issues, errors, or successes. Analyze the results and identify lessons learned and best practices to improve your DR strategy and processes for the future.

Conduct periodic DR drills to test whether the DR environment is consistent and operational if any disaster occurs.

Disaster Recovery Environment Set Up Checklist

One-Off Tasks

☐ Subscribe to OCI Console Announcements.

☐ Subscribe to a second OCI region to set up the DR environment.

☐ Create an IDCS stripe or IAM domain in the OCI DR region.

☐ Onboard users and groups into IDCS or IAM domain.

☐ Synchronize users and groups between the primary and DR IDCS or IAM domains.

☐ Configure the same external SSO identity providers in both the IDCS or IAM domains.

☐ Ensure the appropriate policies and roles are set up in the DR region.

☐ Create an OAC instance in both regions by logging in as the respective IDCS or IAM domain administrator.

☐ Create ADW or DBCS primary and standby instances using Data Guard.

☐ Set up FastConnect or Site-to-Site VPN if connecting to on-premises data sources.

☐ Establish connectivity to private data sources using PAC or RDG in both OAC instances.

☐ Upload and restore snapshot on both OAC instances.

☐ As best practice, ensure end-users create connections and datasets, and grant Full Control access to BIServiceAdministrator.

☐ Update data source connections with the respective region data source connection string.

☐ Configure SMTP mail server on both OAC instances.

☐ Configure system settings on both OAC instances.

☐ Create the same vanity URL on both OAC instances.

☐ Configure OCI load balancers in both OCI regions for both OAC instances.

☐ Configure WAF for the load balancers in both OCI regions.

☐ Map the load balancer IP address of the active OAC instance to the vanity URL DNS name.

☐ Configure security rules and route tables to allow access within OCI regions.

☐ Allowlist the OCI server IP addresses and required ports at your organization's firewall.

☐ Create object storage in both OCI regions to store OAC snapshots.

Recurring Tasks

☐ Use Data Guard to switchover the standby ADW or DBCS as primary in the OCI DR region.

☐ Ensure on-premises data sources are available in the DR OAC instance.

☐ Start RDG for the DR OAC instance in the on-premises network.

☐ Start DR OAC instance in the DR region.

☐ Map the OCI load balancer IP address of the active OAC instance to the vanity URL DNS name.

☐ Run the automation scripts to restore the latest snapshot on the DR OAC instance.

☐ Upload the ADW region-specific wallet in self-service data connections and Console connections.

☐ If you haven't maintained the same DBCS database connection string across the OCI regions, modify the self-service data connections and RPD connection pool connection string to connect the DR region databases.

☐ Review and update the ADW wallet-less (TLS) connection strings in the DR OAC instance.

☐ Recreate datasets created from data flows by rerunning the data flow after migration to the DR OAC instance.

☐ Enable scheduled agents after restoring the snapshot.

☐ If the DR OAC mail server isn't the same as the primary OAC mail server, review and update the mail server configuration.

☐ Verify all the systems settings after restoring the snapshot.

☐ Verify any customization configurations after restoring the snapshot.

☐ Test the DR OAC instance and release it for business users.

Roles and Responsibilities

OCI Administrator

- Subscribe to a secondary DR region
- Create OAC instances
- Create object storage for snapshots
- Create load balancers
- Create and maintain ADW and DBCS data sources instances
- Configure the primary and DR environments
- Configure OCI SMTP mail server

OAC Administrator

- Take regular backups of snapshots and data files and restore them

IDCS Administrator or IAM Domain Administrator

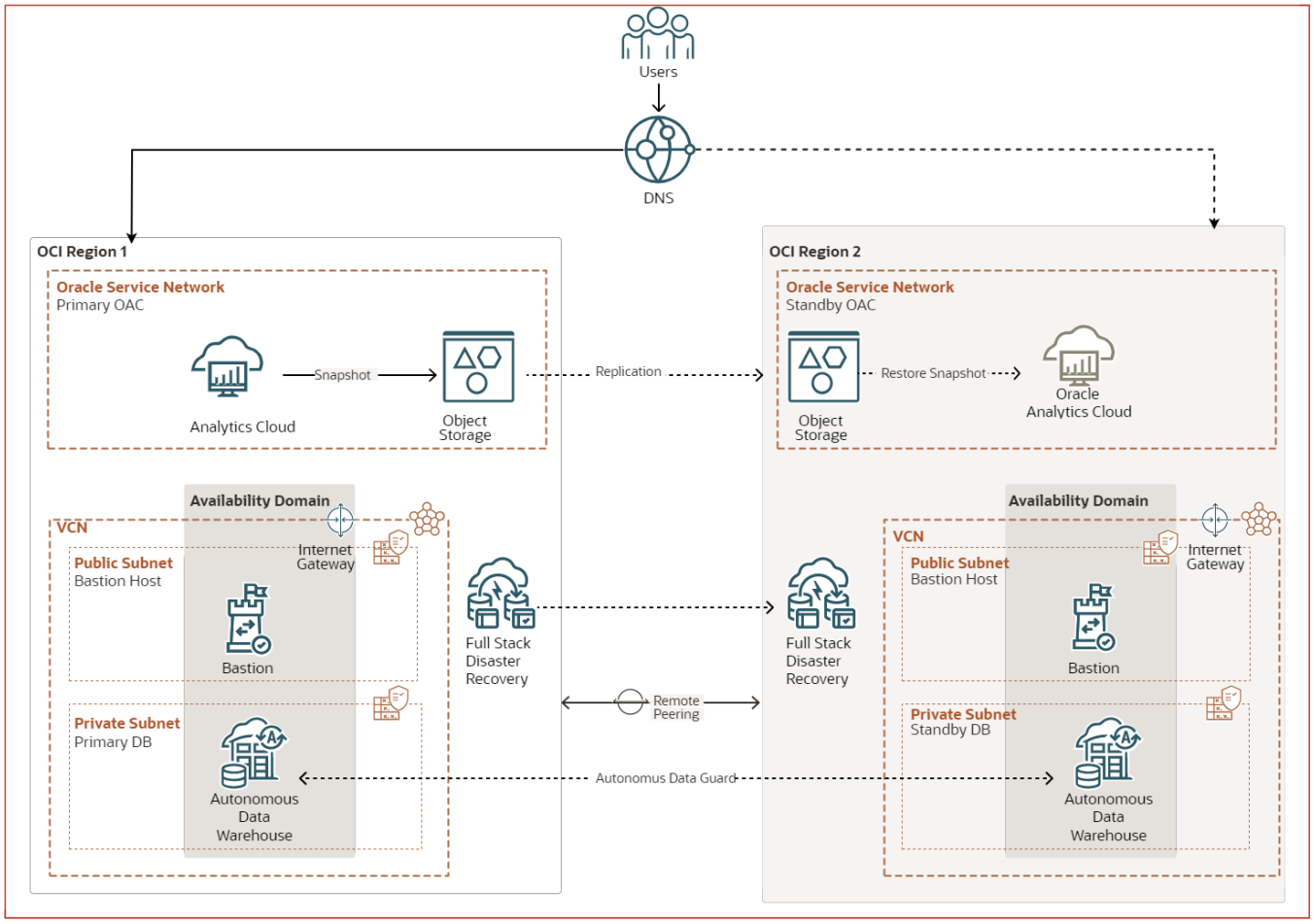
- Manage users and groups
- Configure identity management

Use Full Stack Disaster Recovery to Orchestrate OAC Disaster Recovery

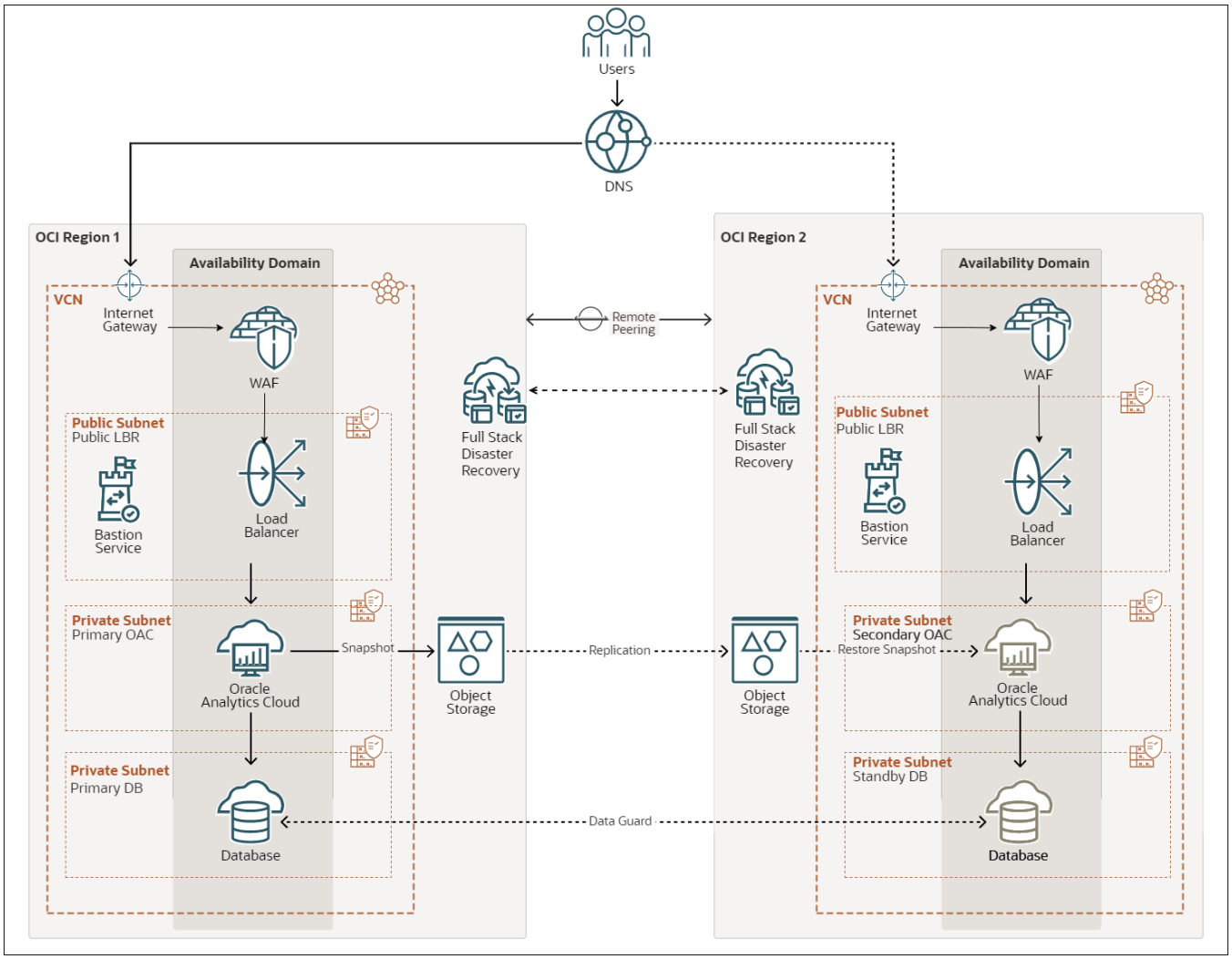
Oracle Analytics Cloud doesn't fall under the OCI feature Full Stack Disaster Recovery (FSDR). However, you can still use FSDR to orchestrate the automation scripts that you need to run to recover from a disaster event.

You use OCI CLI and OAC REST APIs to automate the steps performed during a DR drill and a disaster event. For details, see the next section, "Automation of the Disaster Recovery Environment set Up and DR Drill."

You can use these automation scripts, along with the other FSDR capabilities like switchover of ADW, DBCS, and Compute Instance creation, to manage the disaster recovery for OAC.



Architecture Diagram: Using FSDR for OAC Public Instances



Architecture Diagram: Using FSDR for OAC Private Instances

Automate Recovery for Oracle Analytics Cloud Using OCI Full Stack Disaster Recovery

To automate disaster recovery for OAC using OCI FSDR, follow the tutorial [Automate Recovery for Oracle Analytics Cloud Using OCI Full Stack Disaster Recovery].

Connect with us

Call +**1.800.ORACLE1** or visit **oracle.com**. Outside North America, find your local office at **oracle.com/contact**.

blogs.oracle.com facebook.com/oracle twitter.com/oracle