ORACLE

Step-by-Step Instructions to Prepare for OCI Full Stack Disaster Recovery

Describes how to setup OCI Full Stack Disaster Recovery plan and execute it for Oracle Analytics Server on Oracle Cloud.

May 2024, version 1.0

Public

Disclaimer

This document in any form, software or printed matter, contains proprietary information that is the exclusive property of Oracle. Your access to and use of this confidential material is subject to the terms and conditions of your Oracle software license and service agreement, which has been executed and with which you agree to comply. This document and information contained herein may not be disclosed, copied, reproduced or distributed to anyone outside Oracle without prior written consent of Oracle. This document is not part of your license agreement nor can it be incorporated into any contractual agreement with Oracle or its subsidiaries or affiliates.

This document is for informational purposes only and is intended solely to assist you in planning for the implementation and upgrade of the product features described. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described in this document remains at the sole discretion of Oracle. Due to the nature of the product architecture, it may not be possible to safely include all features described in this document without risking significant destabilization of the code.

Revision History

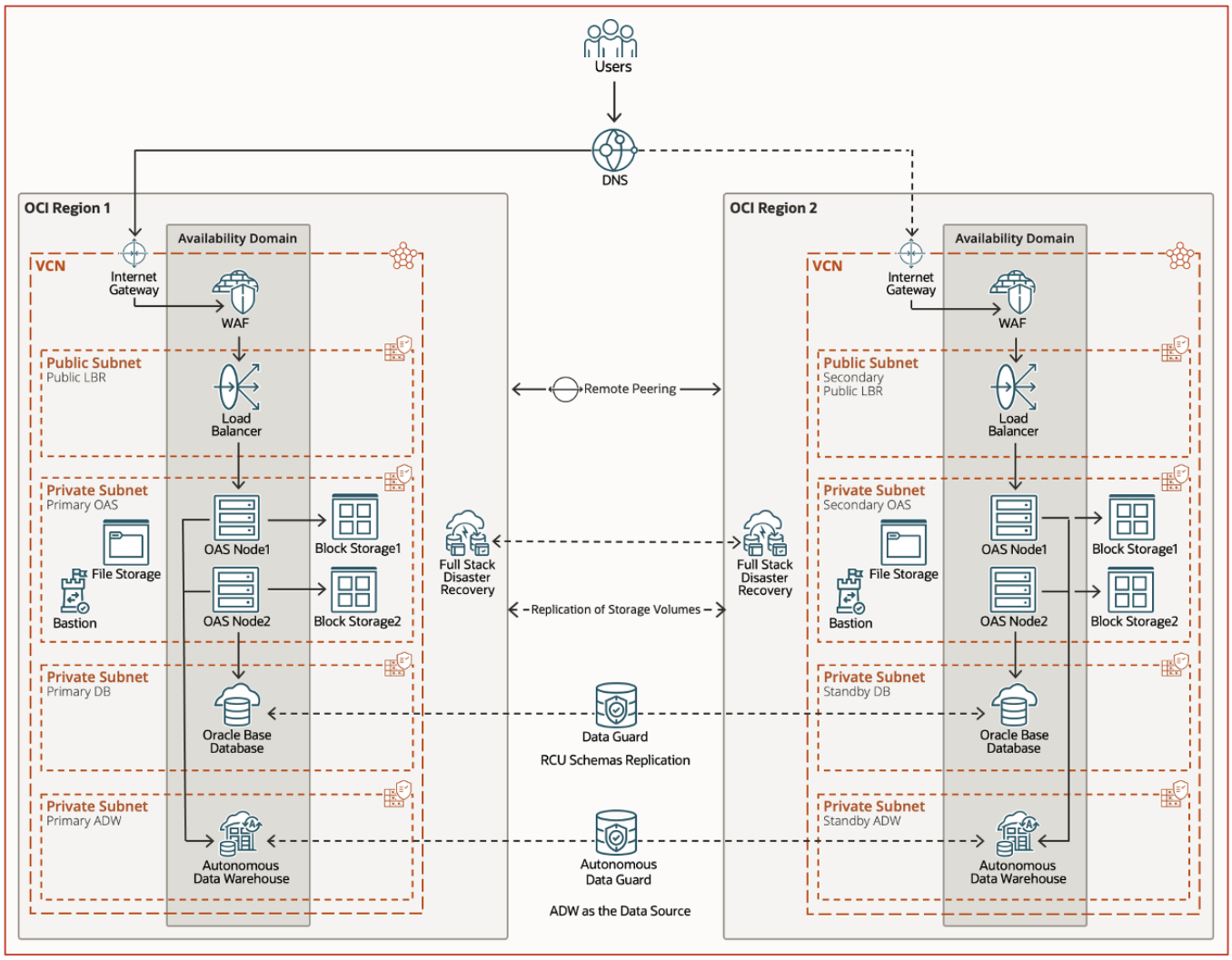
The following revisions have been made to this document since its initial publication.

DATE	REVISION
May 2024	Initial publication

Authors: Veera Raghavendra Rao Koka.

Table of Contents

Architecture



About Full Stack Disaster Recovery

Refer to the Full Stack DR documentation for more information, Overview of Full Stack Disaster Recovery.

Also, refer to the documentation to understand the Full Stack Disaster Recovery Terminology.

Refer to the OAC Full Stack DR Deployment documentation for more information on Full Stack DR, how it works, and Full Stack DR terminology Oracle Analytics Cloud Disaster Recovery automation using the OCI Full Stack Disaster Recovery.

Using this OCI feature, you can manage Oracle Analytics Server Disaster Recovery (DR) from one OCI region to another on Oracle Cloud.

There are two DR models with OCI Full Stack DR for OAS DR.

1. **Cold Standby:** A DR model in which very few or none of the components of the secondary OAS environment need to be pre-deployed in the standby region in preparation for a future DR transition. The OAS secondary environment is deployed as part of the DR transition. This model involves lower operating costs but a higher RTO.
2. **Warm Standby:** A DR model in which all the components of the secondary OAS environment are pre-deployed in the standby region to prepare for a future DR transition. This model involves higher operating costs but a lower RTO.

For **Cold Standby**, you must create the Standby DBCS and ADW instances using Data Guard in the OCI secondary region before Full Stack DR DR plan execution. Also, some components like VCN with the Subnets, Security Rules, and Network Security Groups should be configured for the OCI secondary region in the existing compartment created for the primary region.

During the FDSR DR plan execution, Full Stack DR orchestrates the primary DBCS and ADW switchover to standby, creates new compute instances for OAS, and starts OAS by calling the respective start-up scripts on the OAS compute VMs. The rest of the components are created at the DR plan execution time, hence the higher RTO.

For **Warm Standby**, you must create all the components like DBCS, ADW, VCN, Subnets, Security Rules, Network Security Groups, OAS Compute Instances, and Block Volumes and attach them to the compute instances and Load Balancer (all components that OAS DR requires) before Full Stack DR DR plan execution.

During the FDSR DR plan execution, Full Stack DR orchestrates the primary DBCS and ADW switchover to standby and starts all required compute instances and OAS by calling the respective start-up scripts on the OAS compute VMs. It also maps the Load Balancer IP Address to the required DNS Name (in the future release of Full Stack DR). As the components are created before the DR plan execution, it results in a lower RTO.

Refer to the blogs to configure the DR environment,

1. Disaster Recovery for Oracle Analytics Server on Oracle Cloud Using RCU Schemas and Block Volume Replication.
2. Disaster Recovery for Oracle Analytics Server on Oracle Cloud Using RCU Schemas Replication and File System Replication with Rsync.

NOTE: If the DBCS doesn't have a common connection string between the primary and standby, you may need to create a script to change the connection strings in the backend OAS compute VM files.

Prerequisites for Full Stack DR

- Based on your environment's components and resources, create an IAM policy with all the required access and permissions to the OCI components and resources for Full Stack DR.
- ADW should be configured for Standby in the OCI DR (Secondary) region using the Autonomous Data Guard.
- Using the Data Guard, DBCS should be configured for Standby in the OCI DR (Secondary) region.

- Create a Secret in an OCI Vault as Full Stack DR reads the DBCS admin password from a Secret in both the OCI regions.
- Create a Bucket Storage to store Full Stack DR logs in both the OCI regions.
- Ensure the Block Volume and File System mount instructions are entered in each OAS compute node's/etc/fstab file.
- Volume Group should be created with all the required Block and Boot Volumes of the OAS Compute nodes.
- Replicate the Volume Group to the OCI DR (Secondary) region.
- Replicate the File System to the OCI DR (Secondary) region.
- Create the Mount Target for the File System in the OCI DR (Secondary) region.
- Create Ingress and Egress Security Rules to access File System in the Private Subnet used for OAS and File System in the primary OCI region.
- Load Balancer should be configured as the front end for the OAS Compute nodes in the OCI primary region.
- In the OCI DR (secondary) region, a Load Balancer with the same SSL Certificates, Listener, Hostname, Rule sets, etc., should be configured as the primary LB, except for the Backends.
- Update the /etc/fstab file in the compute VMs with the File Storage details.

/etc/fstab entries as below:

```
[root@oas4fsdr2 opc]# cat /etc/fstab

#
# /etc/fstab
# Created by anaconda on Tue Jun 13 18:17:27 2023
#
# Accessible filesystems, by reference, are maintained under '/dev/disk'
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info
#
UUID=[redacted] /                       xfs     defaults,_netdev,_netdev 0 0
UUID=[redacted]          /boot/efi              vfat    defaults,uid=0,gid=0,umask=0077,shortname=winnt,_netdev,_netdev,x-initrd.mount 0 0
UUID=[redacted]                                 swap    defaults,_netdev,x-initrd.mount 0 0
#####################################
## ORACLE CLOUD INFRASTRUCTURE CUSTOMERS
##
## If you are adding an iSCSI remote block volume to this file you MUST
## include the '_netdev' mount option or your instance will become
## unavailable after the next reboot.
## SCSI device names are not stable across reboots; please use the device UUID instead of /dev path.
##
## Example:
## UUID="[redacted]"   /data1    xfs       defaults,noatime,_netdev      0      2
##
## More information:
## [redacted]/connectingtoavolume.htm
/dev/vg_app/vg_app-lv_app /u02/app      ext4    defaults,noatime,nodiratime,nodev,_netdev 0 2
/dev/vg_data/vg_data-lv_data /u02/data   ext4    defaults,noatime,nodiratime,nodev,_netdev 0 2
/dev/sdb /u01 ext4 defaults,_netdev,nofail 0 2
10.0.3.225:/FileSystem-20240516-0737-27 /sdd nfs defaults,nofail,nosuid,resvport 0 0
[root@oas4fsdr2 opc]#
```

This document covers the **Cold Standby** or **Moving Resources** scenario.

OCI components involved in the Full Stack DR Cold Standby approach are as follows:

OCI Region 1 (Primary region)		**OCI Region 2 (DR region)**
ADW Instance (Primary)	Create a Standby in the DR region using the Autonomous Data Guard	ADW Instance (Standby)
DBCS Instance (Primary)	Create a Standby in the DR region using the Data Guard	DBCS Instance (Standby)
Boot Volume of the OAS Compute VMs	Full Stack DR manages during the plan execution	
Block Volume of the OAS Compute VMs	Full Stack DR manages during the plan execution	
File System attached to OAS Compute VMs	Full Stack DR manages during the plan execution	
OAS Compute VMs	Full Stack DR manages during the plan execution	
Bastion Server to access private OAS nodes	Should be created in both regions prior to Full Stack DR Plan	Bastion Server to access private OAS nodes
Load Balancer	Should be created in both regions prior to Full Stack DR Plan	Load Balancer
Web Application Firewall (If needed)	Should be created in both regions prior to Full Stack DR Plan	Web Application Firewall (If needed)

Upon failover, Full Stack DR moves the OAS compute VMs, Block Volumes, and File Systems from the primary region to the DR region.

Similarly, Full Stack DR switches the resource/components from the DR region to the primary region.

NOTE: In a non-moving scenario, i.e., Warm Standby, all resources/components should exist in both regions and be configured before the Full Stack DR execution. Full Stack DR only orchestrates the switchover of the ADW and DBCS and starts the OAS compute VMs and the OAS application to make the DR region resources available to the end users.

Key points to remember

Full Stack DR allows the creation of the DR plans only from the secondary/standby DR protection group.

When switching from primary to secondary, create the DR Plan and execute it from the secondary OCI region.

When falling back from the secondary to the initial primary, create the DR Plan and execute it from the initial primary OCI region.

Create an IAM Policy for Full Stack DR

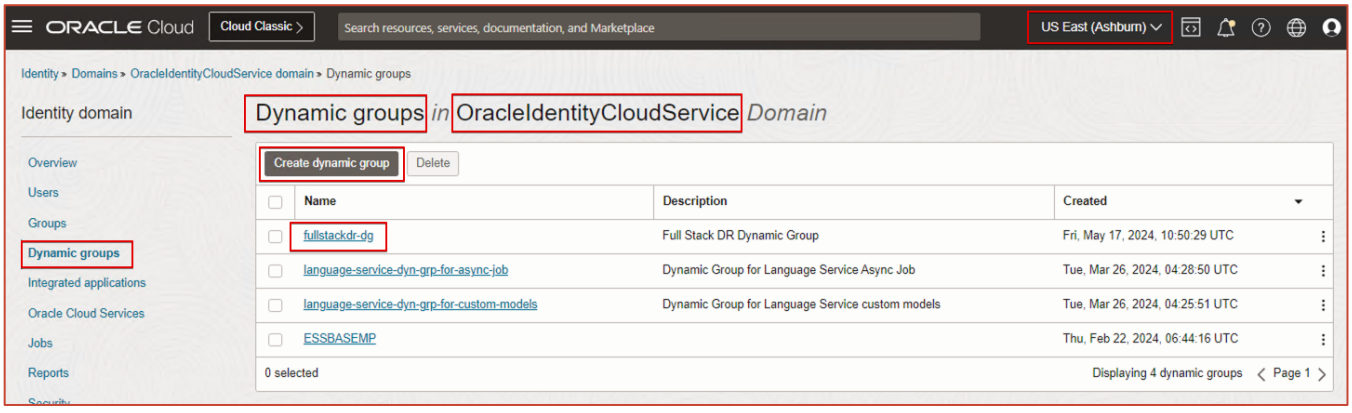
Refer to the blog, Configuring Identity and Access Management (IAM) policies to use Full Stack DR.

Create a Group in the IAM Domain where the OCI resources are associated

E.g., OracleIdentityCloudService (domain), Default (domain), etc.

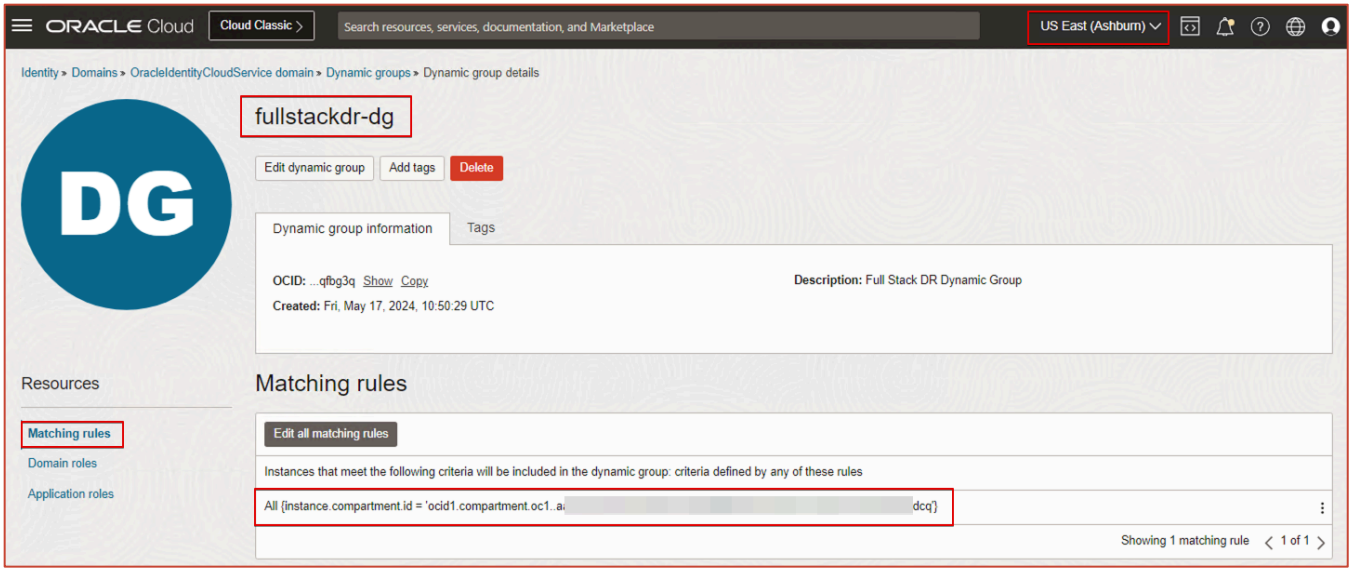
Create a group called “FullStackDRGroup” in the OracleIdentityCloudService (IAM Domain) and add the required users to it.

Create a Dynamic Group



Rule as

All {instance.compartment.id = '<compartment ocid value>'}



Policy Statements are as follows

Allow group OracleIdentityCloudService/FullStackDRGroup to manage disaster-recovery-family in compartment oasmp

Allow group OracleIdentityCloudService/FullStackDRGroup to manage buckets in compartment oasmp

Allow group OracleIdentityCloudService/FullStackDRGroup to manage objects in compartment oasmp

Allow group OracleIdentityCloudService/FullStackDRGroup to manage databases in compartment oasmp

Allow group OracleIdentityCloudService/FullStackDRGroup to manage autonomous-databases in compartment oasmp

Allow group OracleIdentityCloudService/FullStackDRGroup to manage instance-family in compartment oasmp

Allow group OracleIdentityCloudService/FullStackDRGroup to manage instance-agent-command-family in compartment oasmp

Allow group OracleIdentityCloudService/FullStackDRGroup to manage volume-family in compartment oasmp

Allow group OracleIdentityCloudService/FullStackDRGroup to read virtual-network-family in compartment oasmp

Allow group OracleIdentityCloudService/FullStackDRGroup to use subnets in compartment oasmp

Allow group OracleIdentityCloudService/FullStackDRGroup to use vnics in compartment oasmp

Allow group OracleIdentityCloudService/FullStackDRGroup to use network-security-groups in compartment oasmp

Allow group OracleIdentityCloudService/FullStackDRGroup to use private-ips in compartment oasmp

Allow group OracleIdentityCloudService/FullStackDRGroup to read fn-app in compartment oasmp

Allow group OracleIdentityCloudService/FullStackDRGroup to read fn-function in compartment oasmp

Allow group OracleIdentityCloudService/FullStackDRGroup to use fn-invocation in compartment oasmp

Allow group OracleIdentityCloudService/FullStackDRGroup use tag-namespaces in compartment oasmp

Allow group OracleIdentityCloudService/FullStackDRGroup read vaults in compartment oasmp

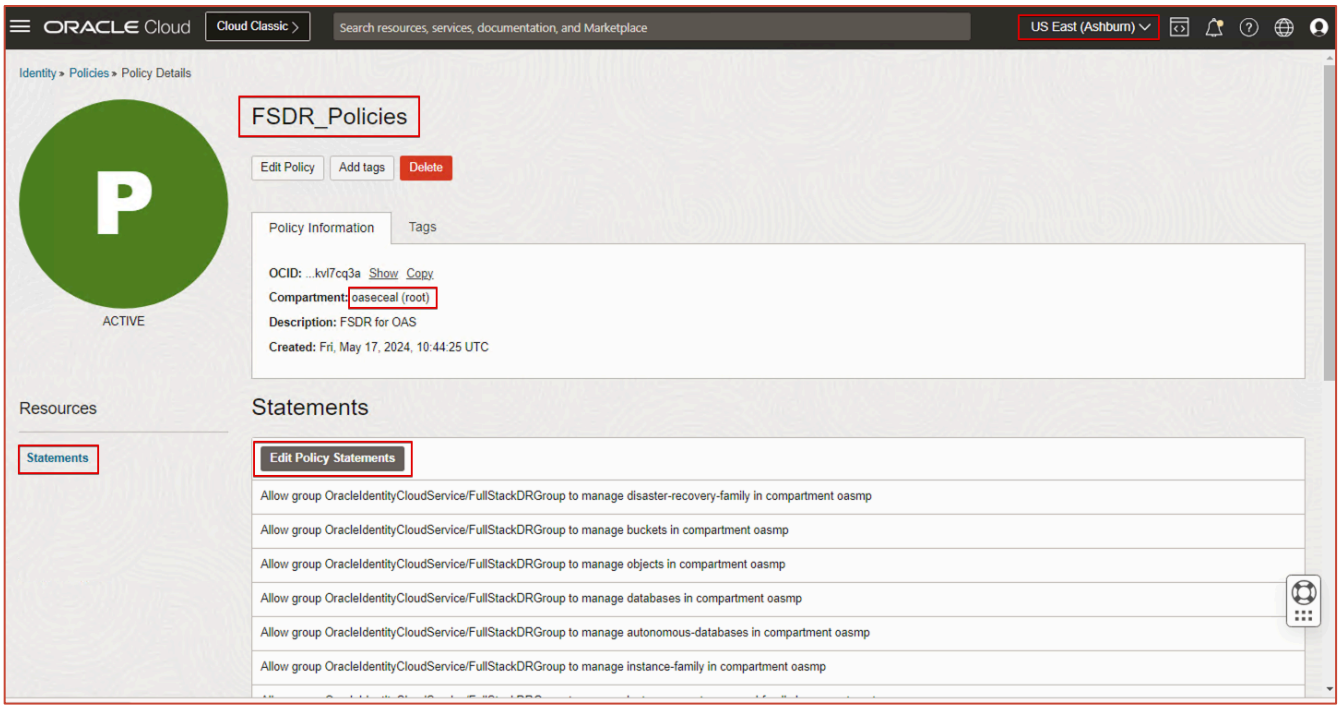
Allow group OracleIdentityCloudService/FullStackDRGroup read secret-family in compartment oasmp

Allow group OracleIdentityCloudService/FullStackDRGroup to manage load-balancers in compartment oasmp

Allow group OracleIdentityCloudService/FullStackDRGroup to manage network-load-balancers in compartment oasmp

Allow group OracleIdentityCloudService/FullStackDRGroup to manage file-family in compartment oasmp

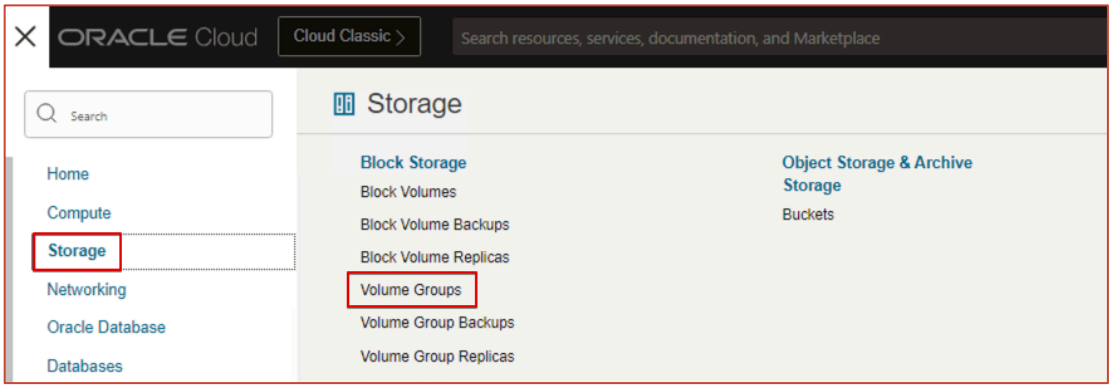
Allow dynamic-group OracleIdentityCloudService/fullstackdr-dg to use instance-agent-command-execution-family in compartment oasmp

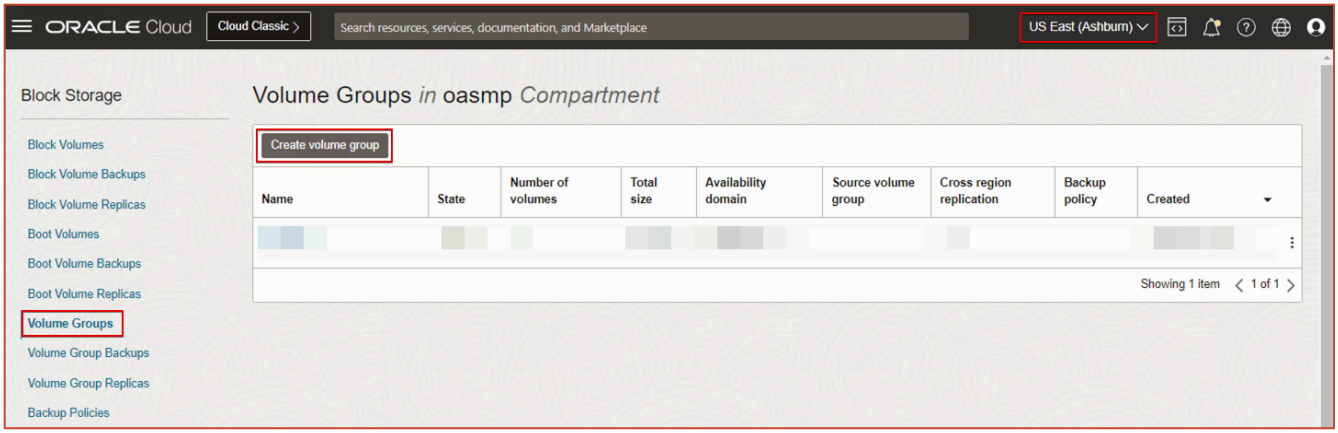


Create a Volume Group and Replicate it

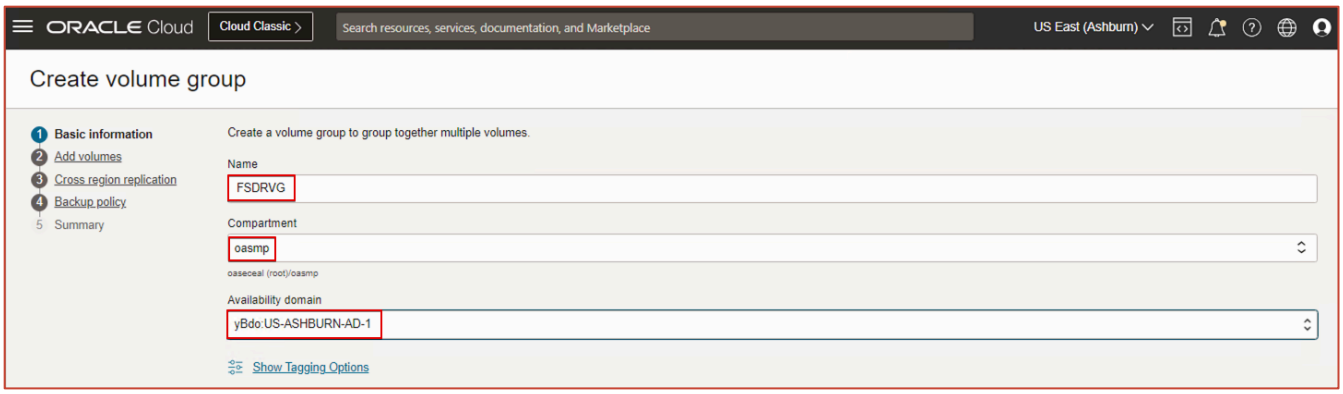
Sign in to the OCI Console

Navigate to Storage → Volume Groups → Create volume group.

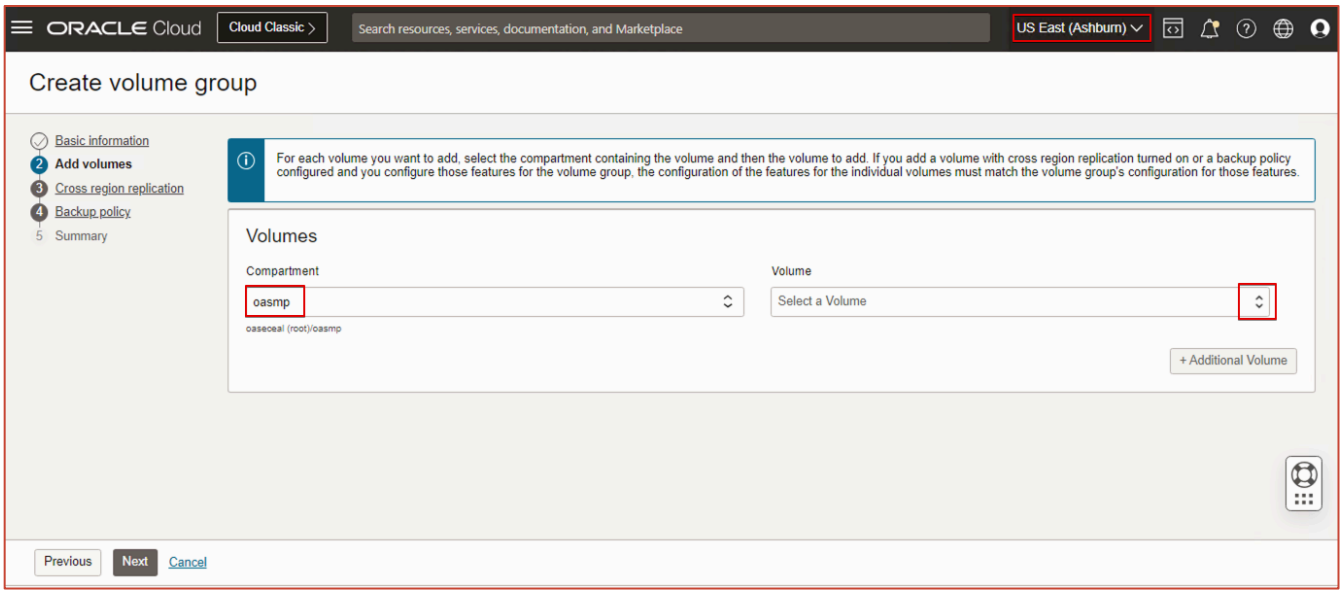




Create a Volume Group.



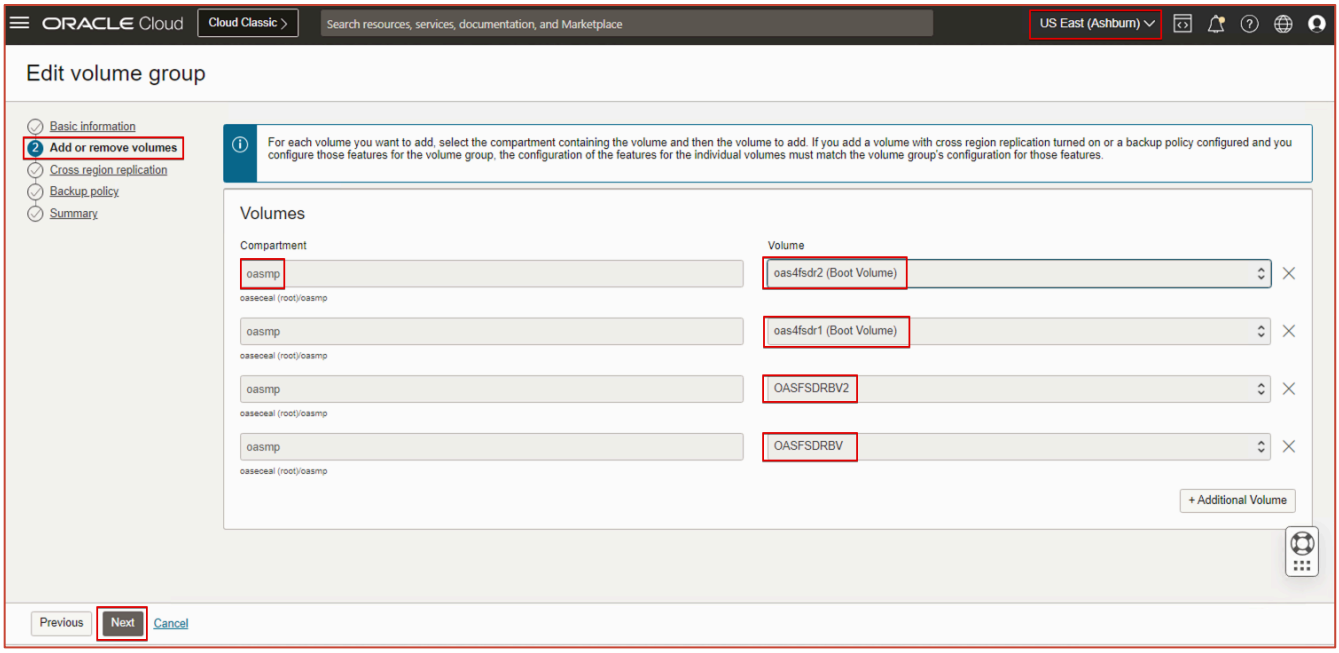
Click “Next”.

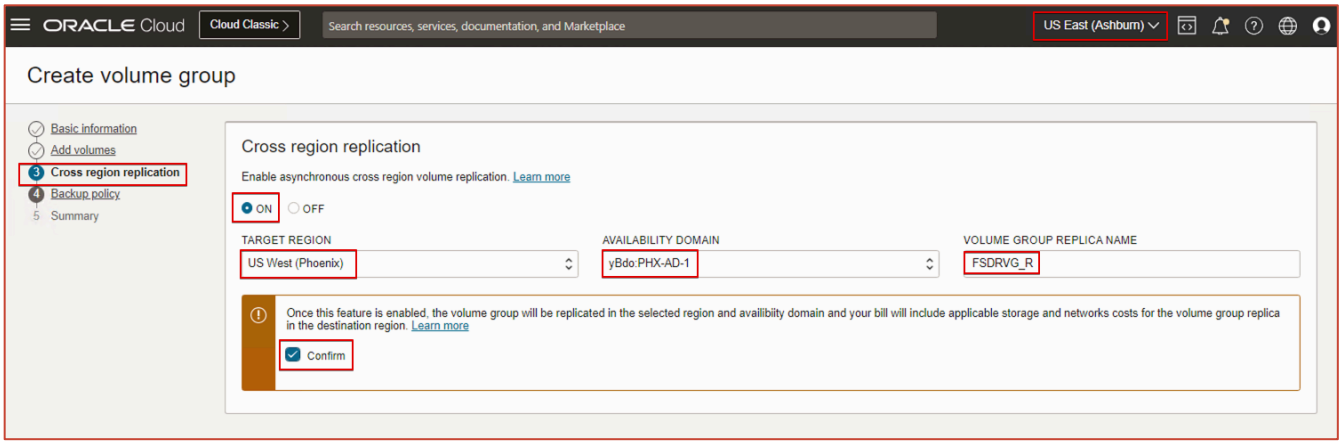


Select the Volume needed to be added to the Volume Group.

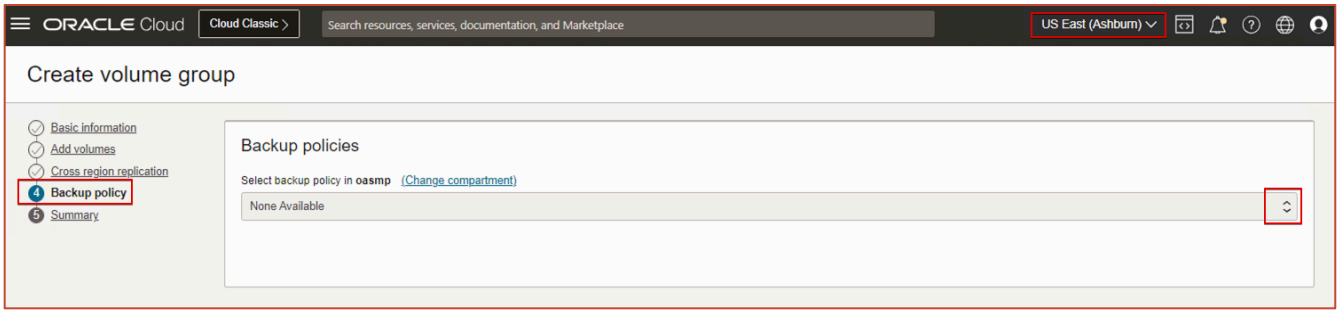
1. Boot Volume of the OAS compute instance 1
2. Block Volume of the OAS compute instance 1
3. Boot Volume of the OAS compute instance 2
4. Block Volume of the OAS compute instance 2

Add the Boot and Block volumes of all the OAS nodes in the cluster.

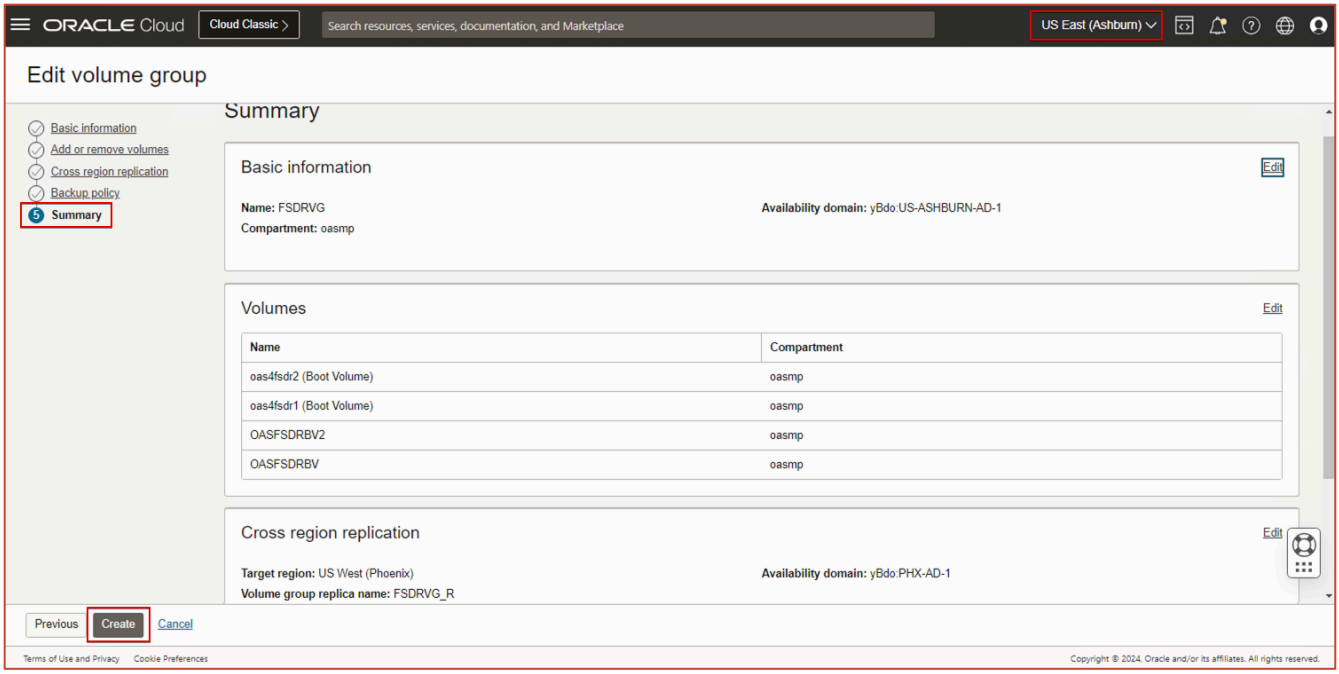




Click “Next”.



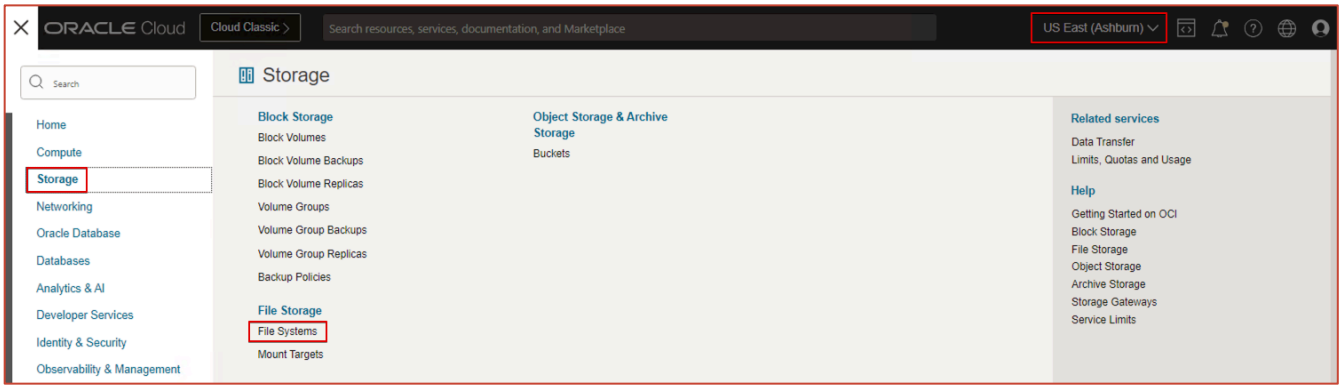
Click “Next”.



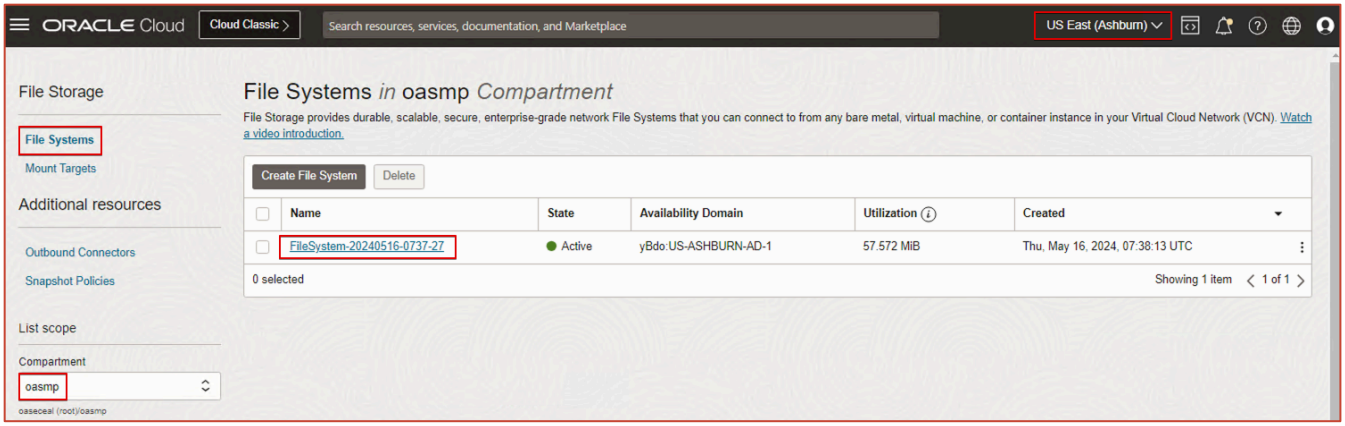
Replicate the File System

Sign in to the OCI Console

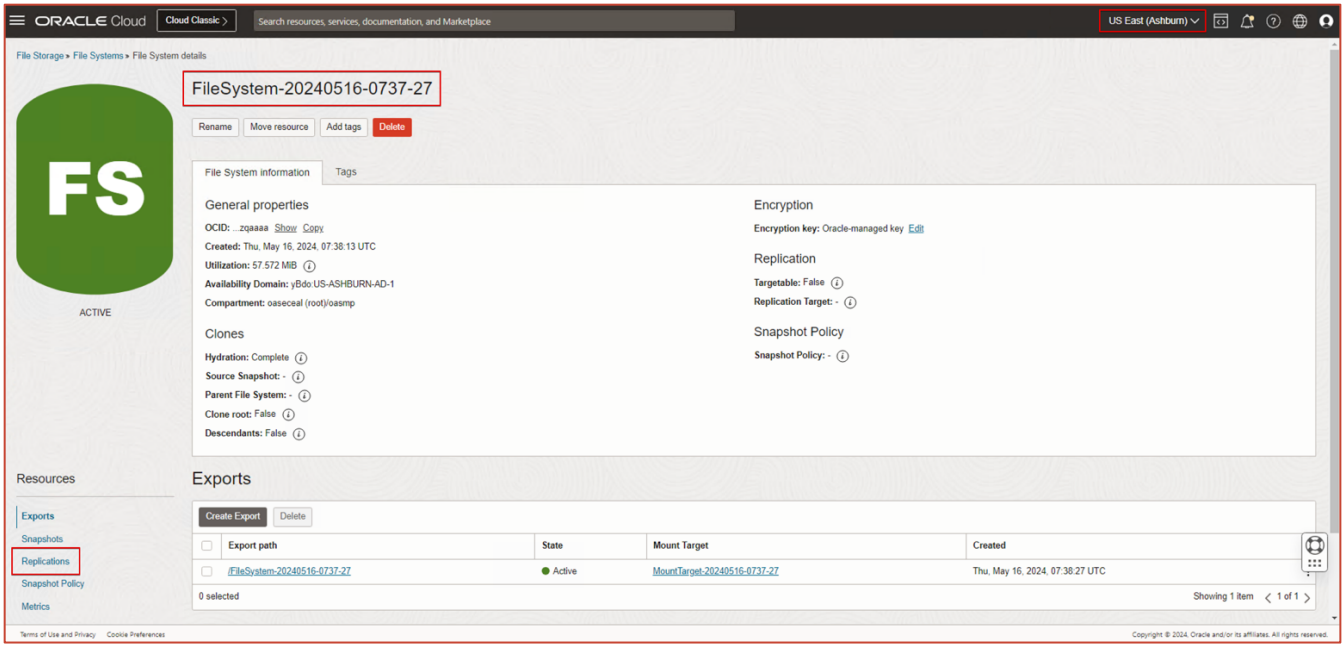
Navigate to Storage → File Systems.

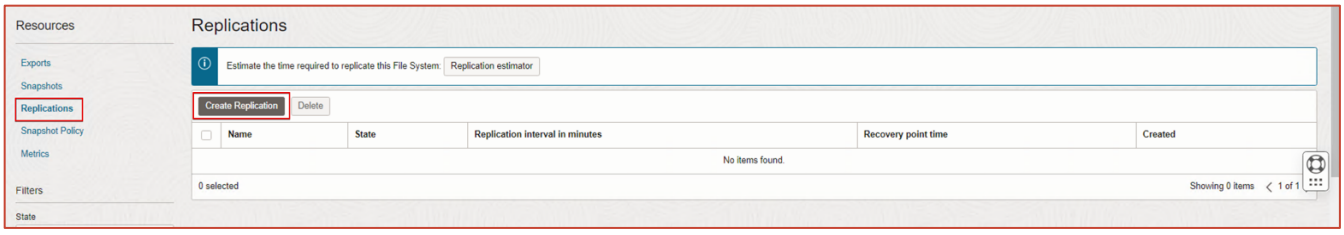


Select the existing File System mounted to the OAS compute instances.



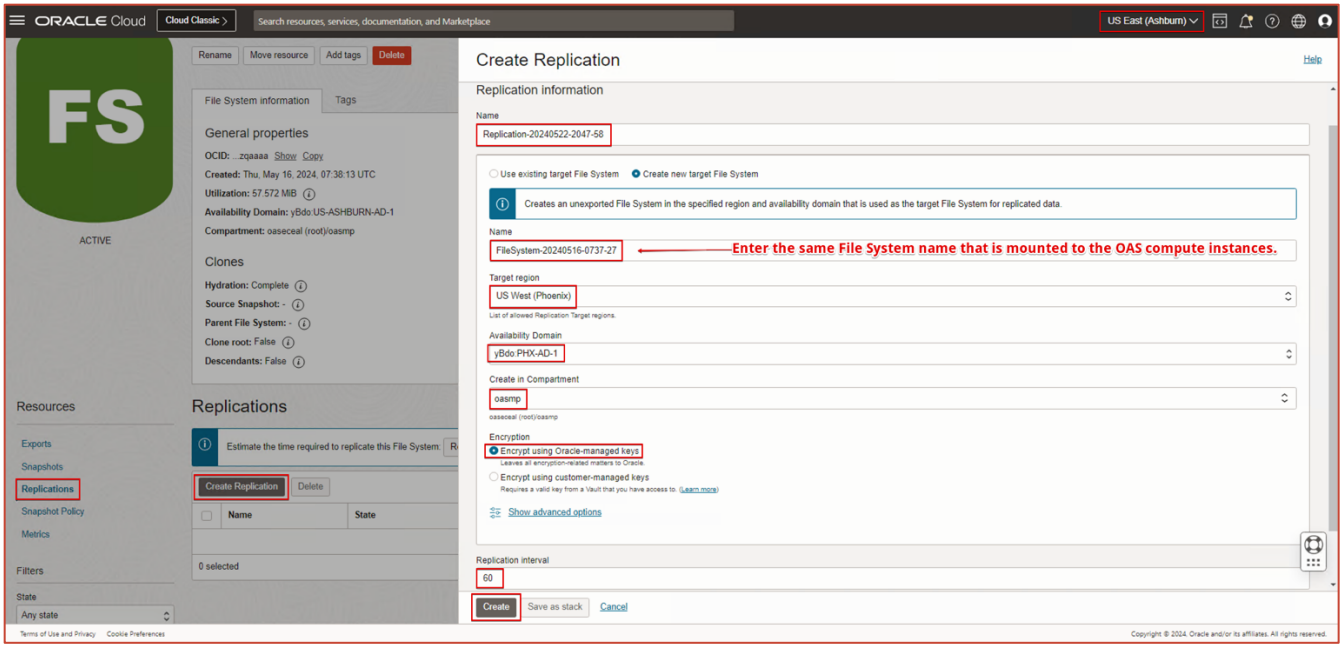
Create a replication



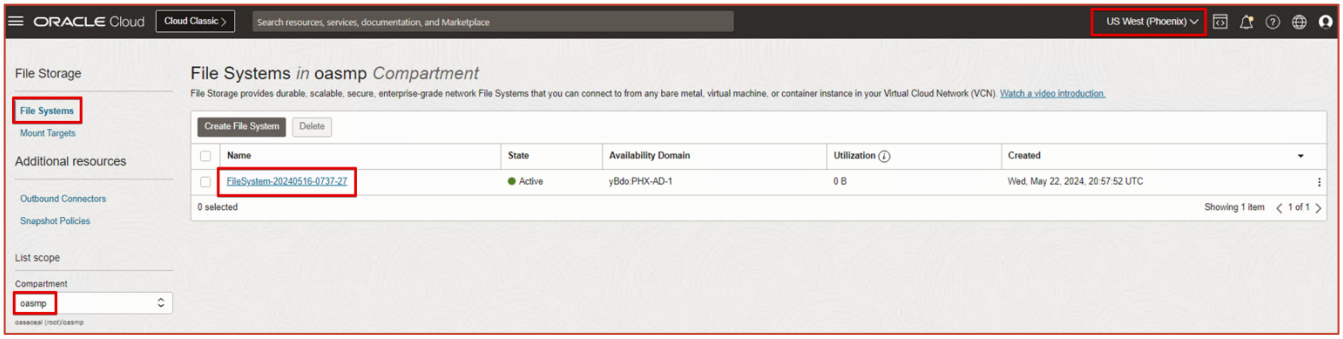


Use the same File System name mounted to the OAS compute instances while creating the Replication. E.g., FileSystem-20240516-0737-27

Using the same File System name makes identifying the replicated File System easy. You can use any name.

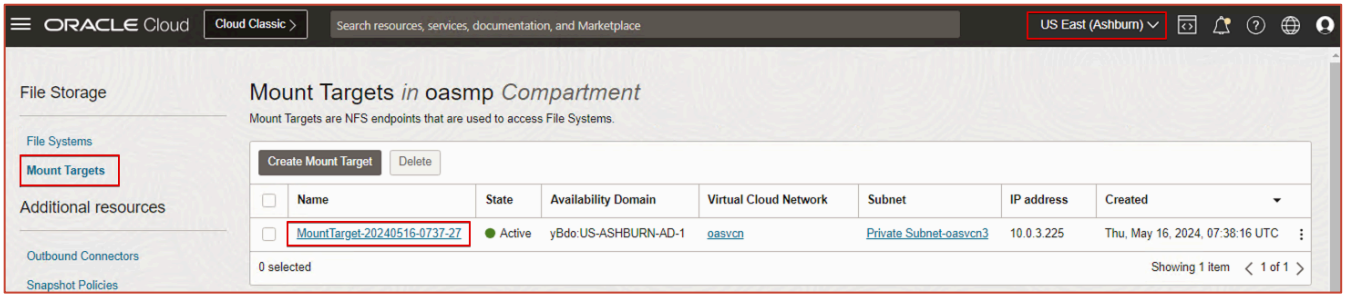


There will be a replication File System created in the OCI Secondary region i.e., Phoenix.



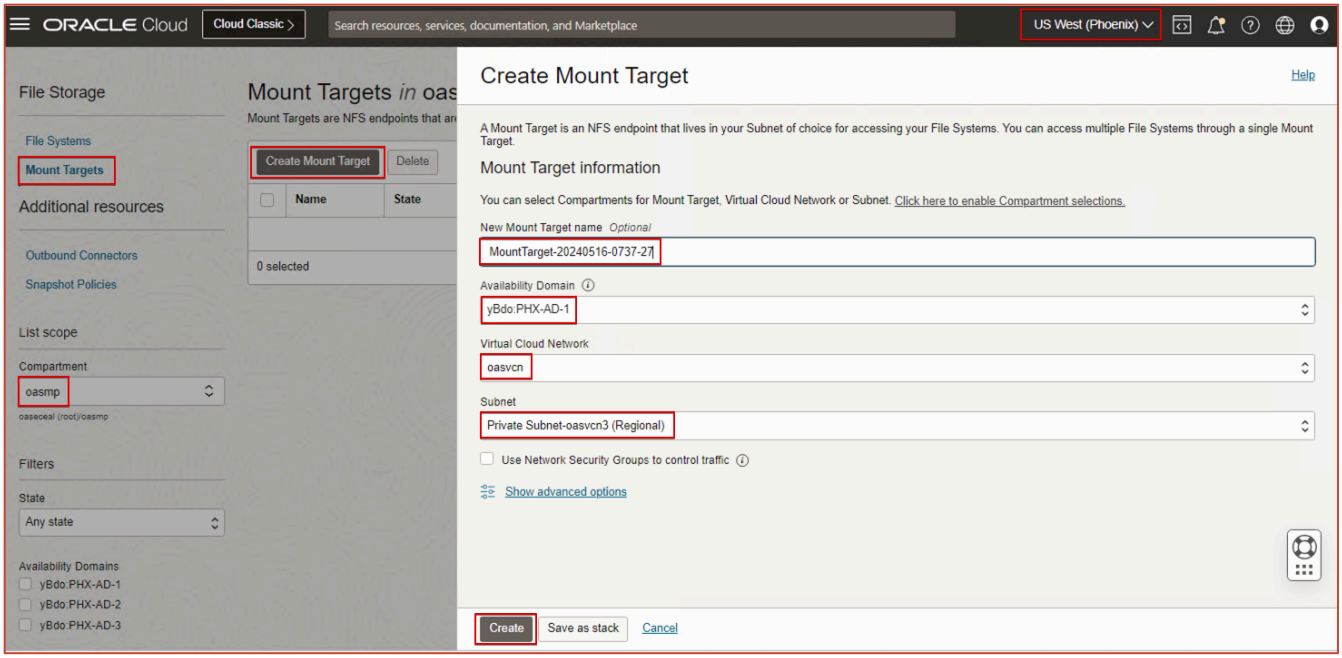
Create a Mount Target for the File System in the OCI Secondary Region

Get the Mount Target name from the primary region and create the Mount Target in the secondary region with the same name.



Create the Mount Target with the same name in the OCI Secondary (DR) region.

Using the same Mount Target name makes identifying the replicated File System's Mount Target easy. You can use any name.



Prepare OAS Compute Nodes to run Commands using the OCI Cloud Agent

After the OAS compute instances are created, OAS services should be started. To start the OAS services, start.sh script on the DOMAIN_HOME must be run on the primary OAS node, and the startNodeManager.sh script must be run on the secondary OAS instances.

To run such scripts or commands on the OAS compute instances using the Full Stack DR, you need the OCI Cloud Agent with run commands privileges. For more information, refer to the documentation, Running Commands on an Instance.

Running Commands with Administrator Privileges

If a command requires administrator permissions, you must grant administrator permissions to the Compute Instance Run Command plugin to be able to run the command. The plugin runs as the **ocarun** user.

The OCI Cloud Agent connects to the OAS compute instances as an **ocarun** user, then changes to an **oracle** user and runs the required scripts and commands.

To perform such actions, the **ocarun** user needs sudo permissions on the Linux instances.

Grant sudo permissions on OAS compute instances

1. On the instance, create a sudoers configuration file for the Compute Instance Run Command plugin:

```
vi ./101-oracle-cloud-agent-run-command
```

2. Allow the **ocarun** user to run all commands as sudo by adding the following line to the configuration file:

```
ocarun ALL=(ALL) NOPASSWD:ALL
```

You can optionally list specific commands. See the Linux man page for sudoers for more information.

3. Validate that the syntax in the configuration file is correct:

```
visudo -cf ./101-oracle-cloud-agent-run-command
```

If the syntax is correct, the follow message is returned:

```
./101-oracle-cloud-agent-run-command: parsed OK
```

4. Add the configuration file to `/etc/sudoers.d`:

```
sudo cp ./101-oracle-cloud-agent-run-command /etc/sudoers.d/
```

Create Ingress and Egress Security Rules to access the File System on the OCI Secondary (DR) Region

Add the Ingress and Egress security rules for the private subnet (172.0.3.0/24) used for OAS compute VMs with the required ports and protocols TCP and UDP.

Ingress:

TCP: 111,2048,2049,2050.

UDP: 111,2048.

Egress:

TCP: 111,2048,2049,2050

UDP: 111.

Configure Load Balancer for the OAS Compute Instances

Load Balancer should be configured as the front end for the OAS Compute nodes in the OCI primary region.

Configure an OCI Load Balancer for the OAS cluster environment. For more information, refer to the blog SSL Offloading at Oracle Cloud Infrastructure (OCI) Load Balancer for Oracle Analytics Server on Oracle Cloud Marketplace.

In the OCI DR (secondary) region, a Load Balancer with the same SSL Certificates, Listener, Hostname, Rule sets, etc., should be configured as the primary LB, except for the backends in a moving OAS compute instance type.

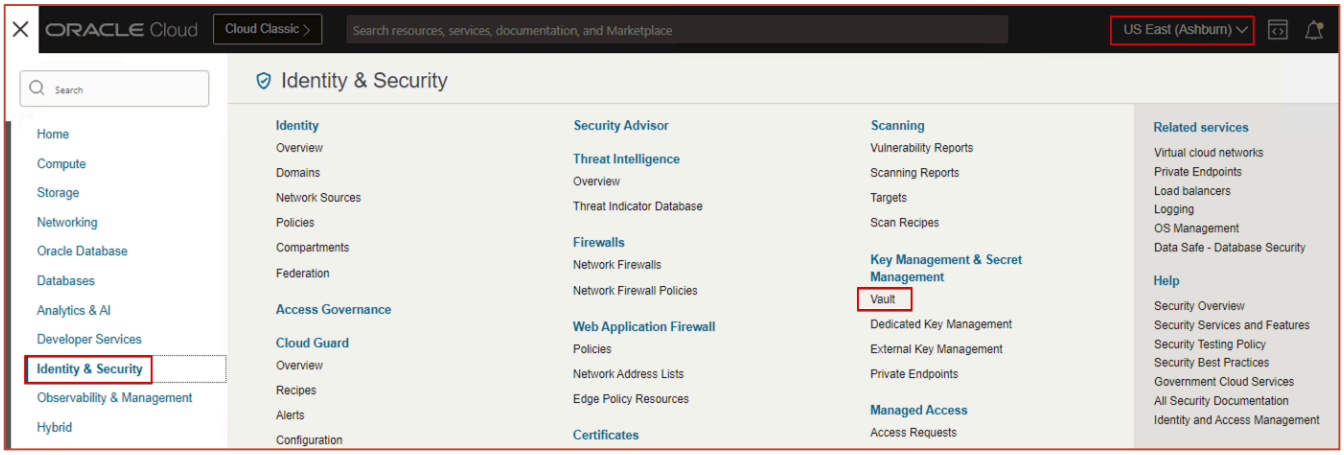
During the DR plan execution, the Load Balancer backends, i.e., the OAS compute instances, will be removed from the primary region LB. Once the OAS compute instances are created in the secondary region, they get added to the secondary region LB as backends.

Create a Secret Key in a Vault for the Admin Password of DBCS

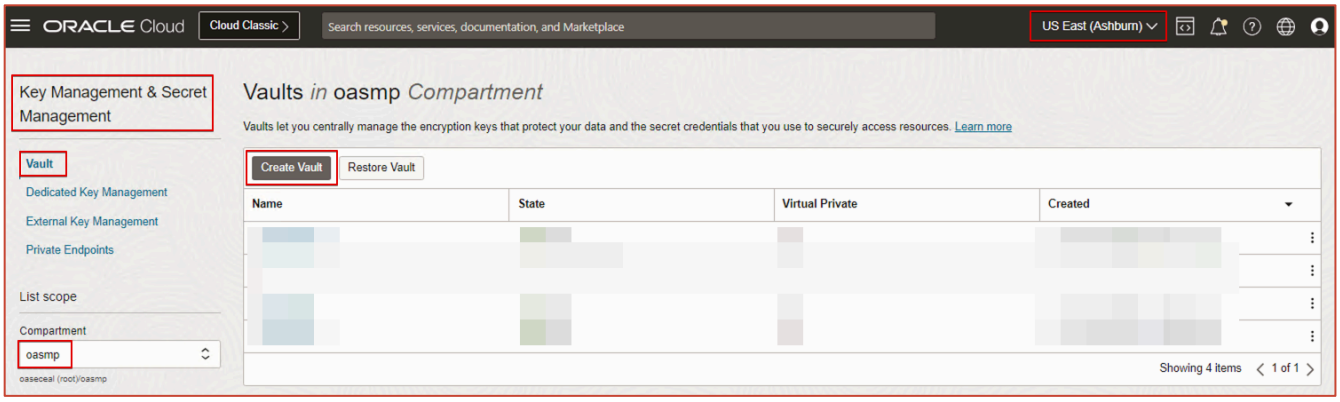
When you have an Oracle DBCS instance as a member of Full Stack DR, it needs the admin password to switch from the primary to the standby instance. The admin password cannot be entered as plain text; Full Stack DR reads it from a Secret in a Vault.

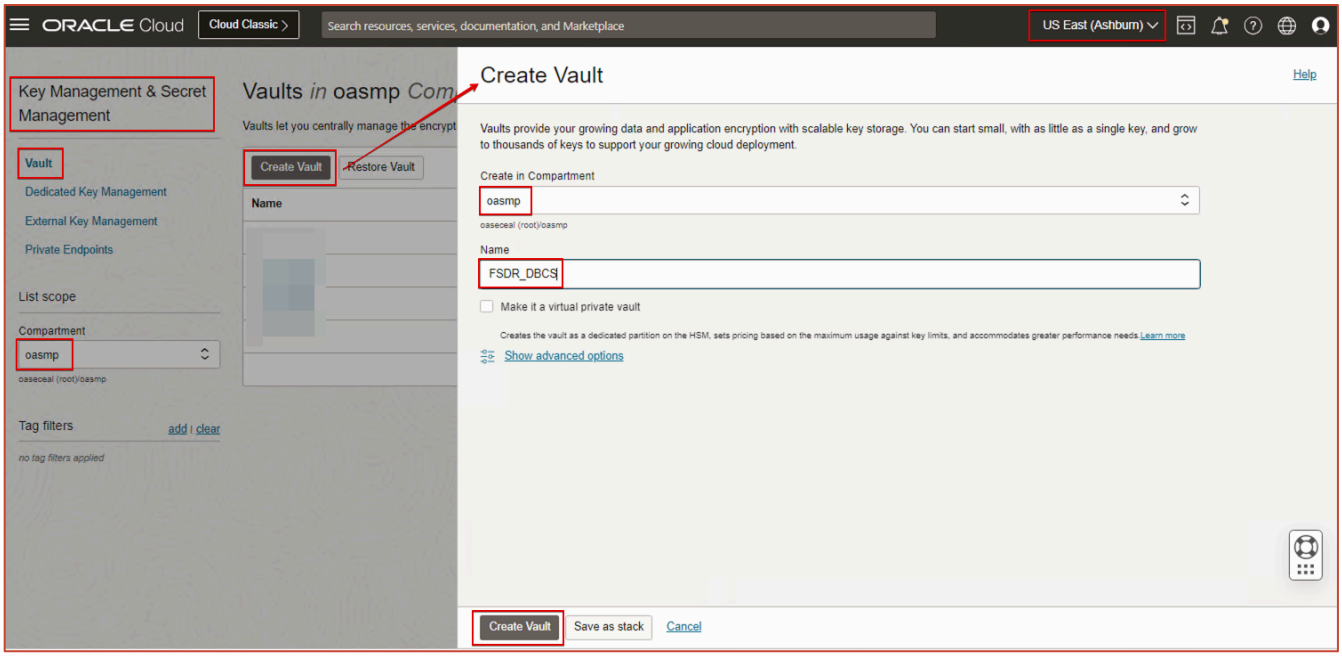
Sign in to the OCI Console

Navigate to Identity & Security → Key Management & Secret Management → Vault

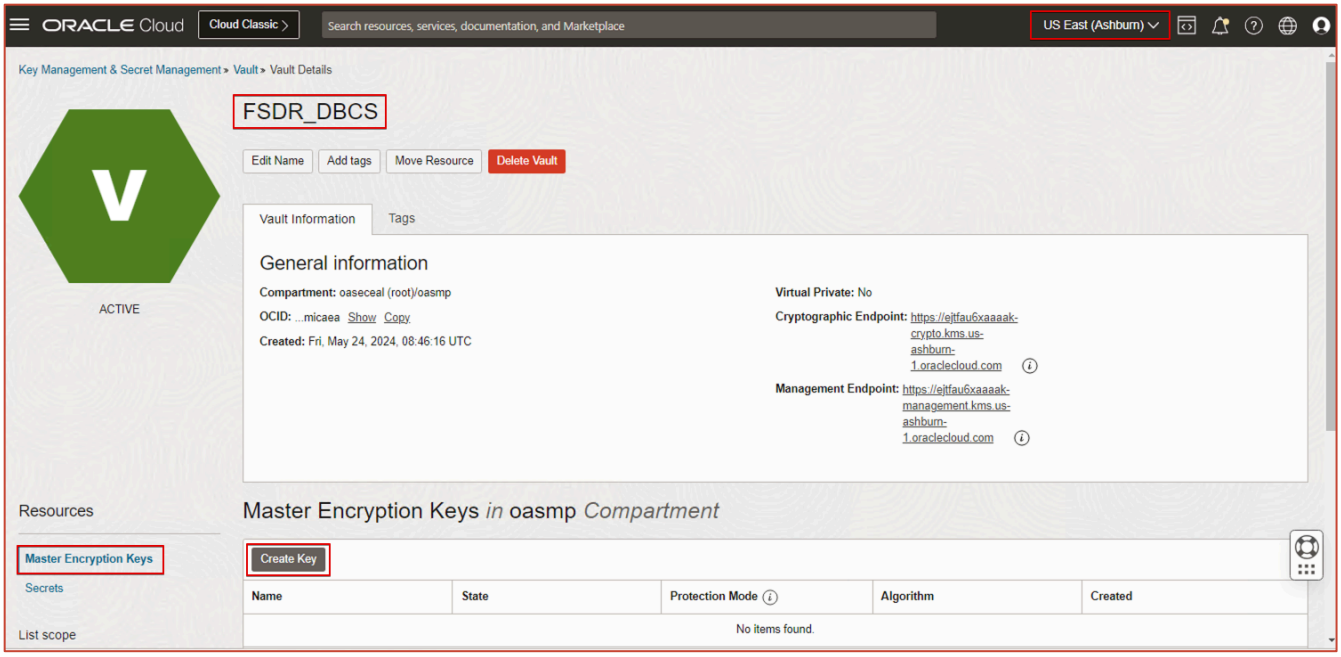


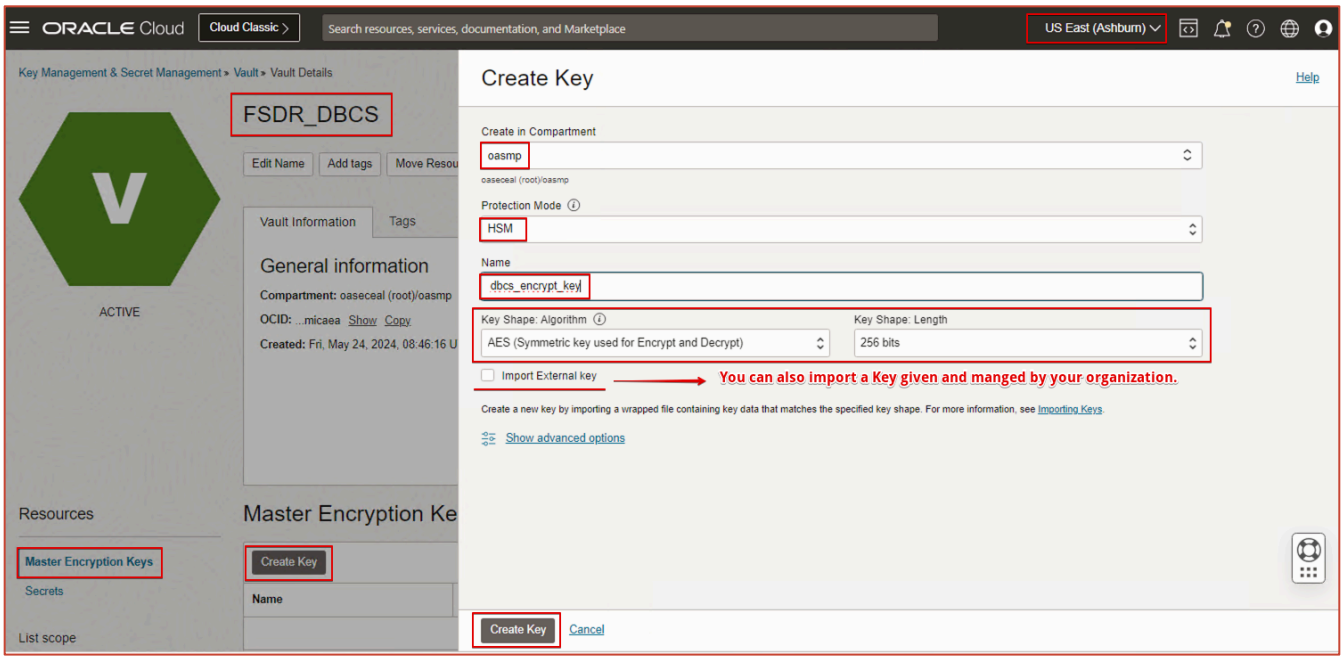
Create a Vault



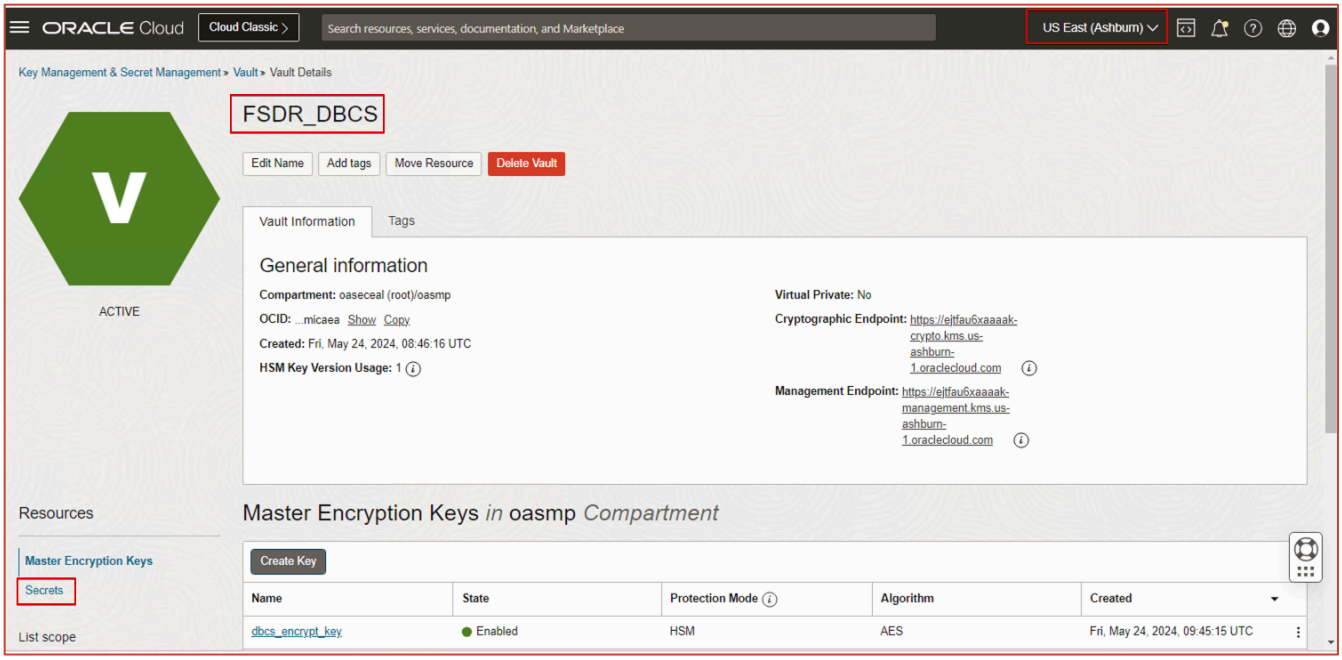


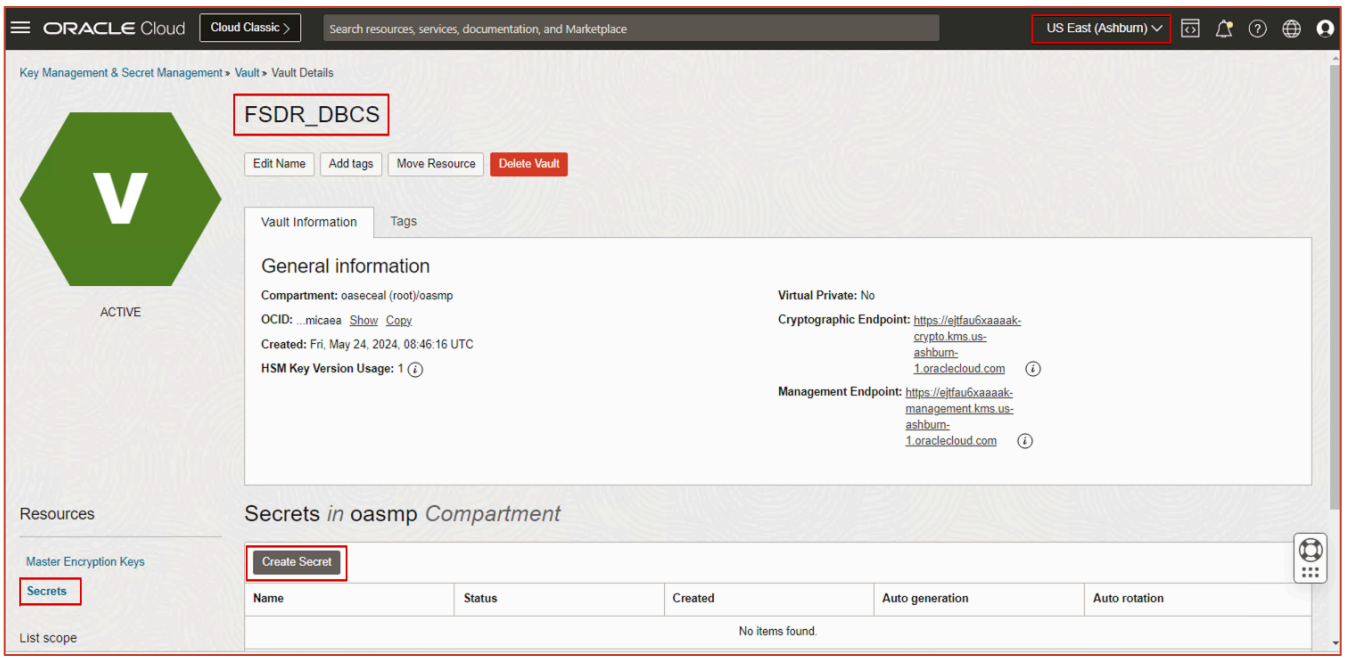
Create a Master Encryption Key

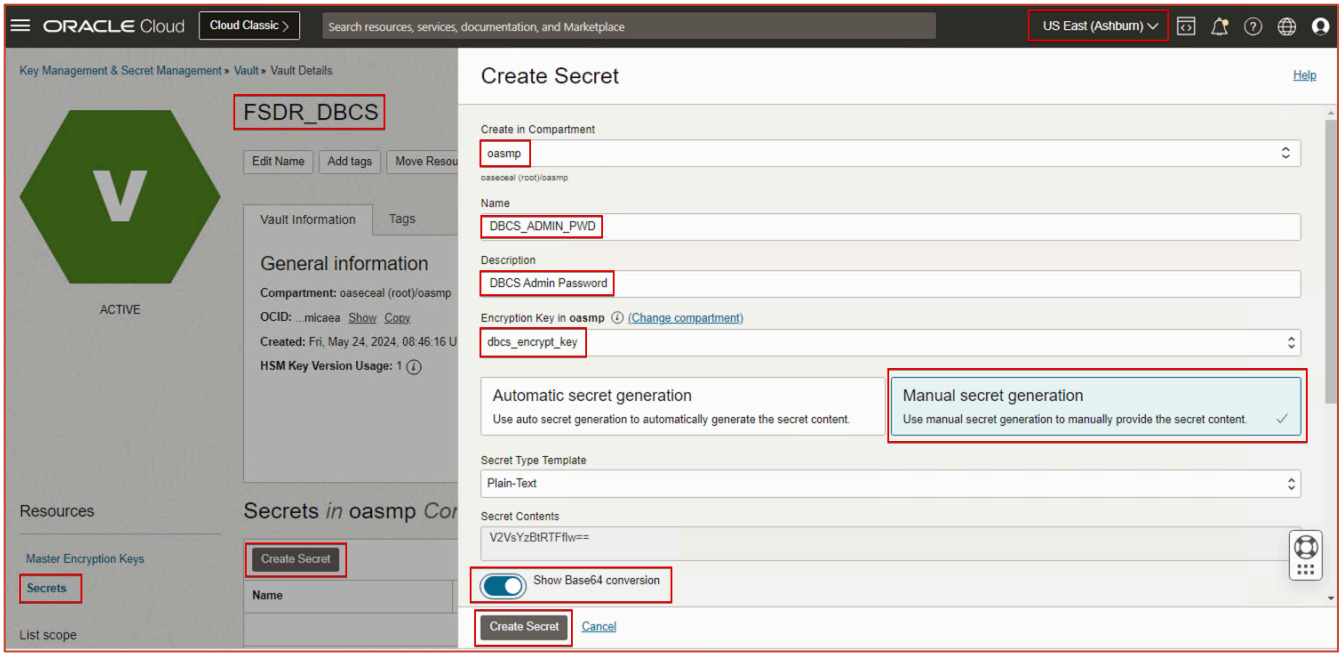




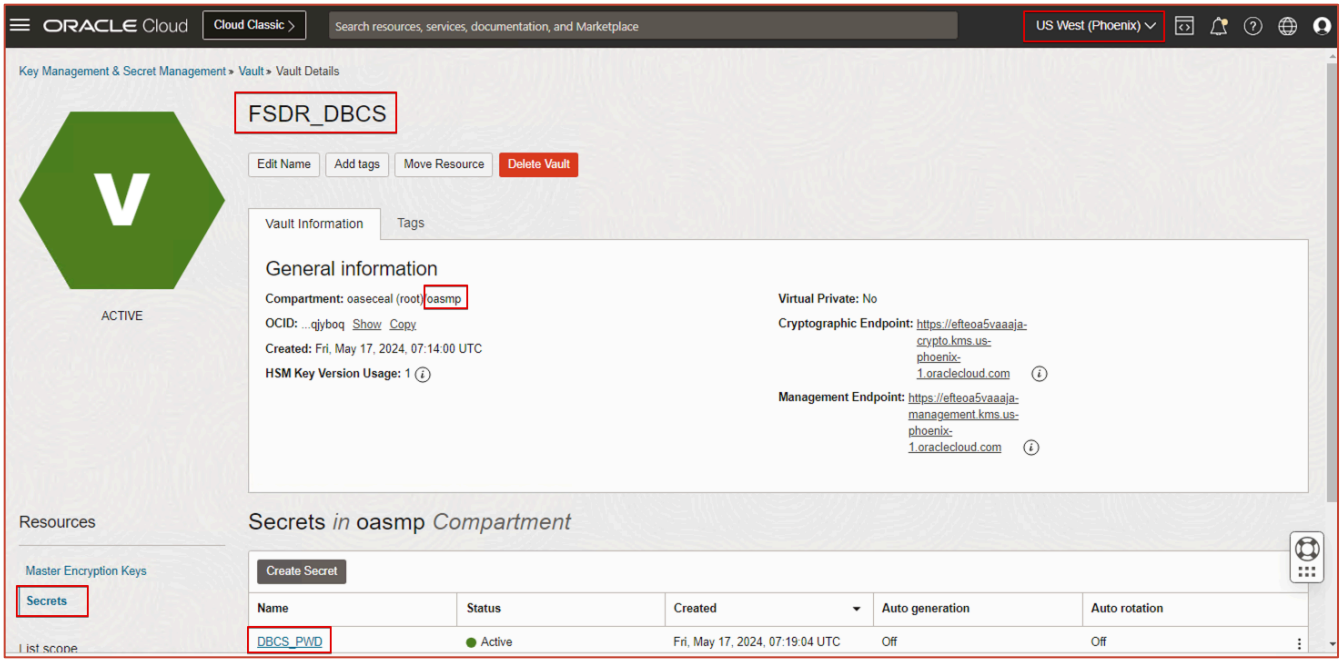
Create a Secret and encrypt it using the Master Encryption Key.







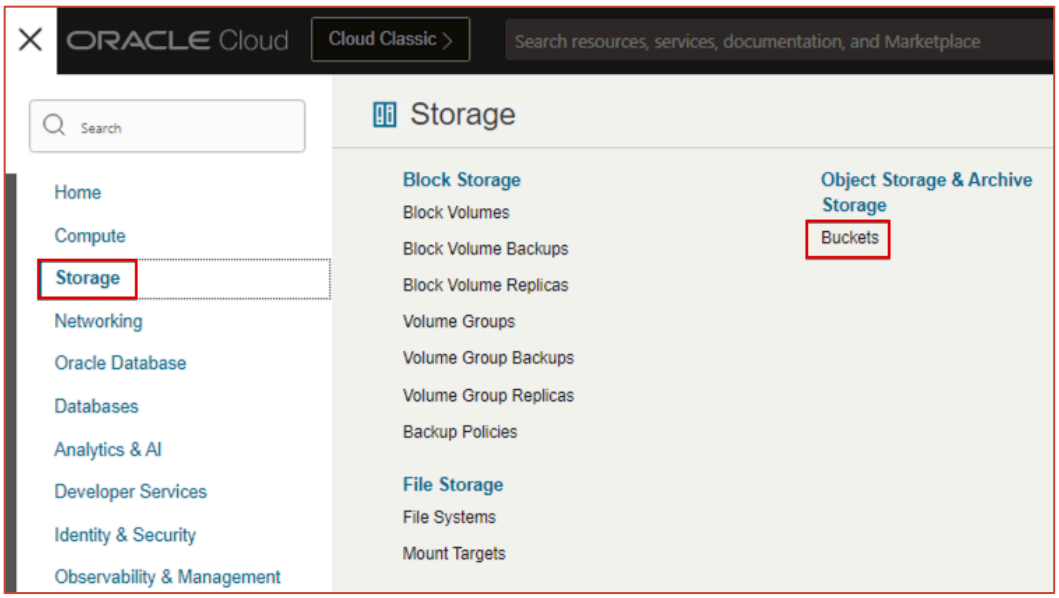
Similarly, create a Vault and Secret in the same Compartment (e.g., oasmp) in the OCI Secondary (DR) region.

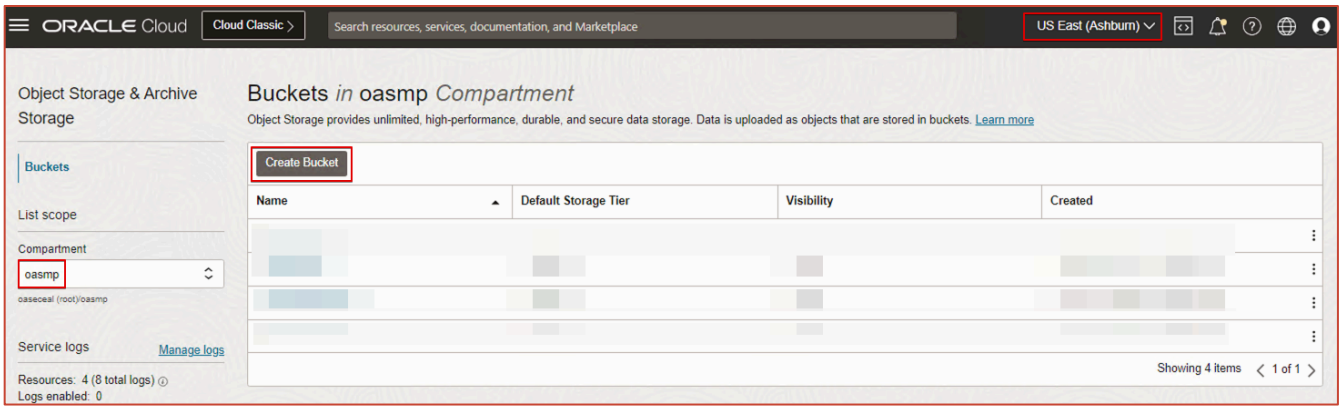


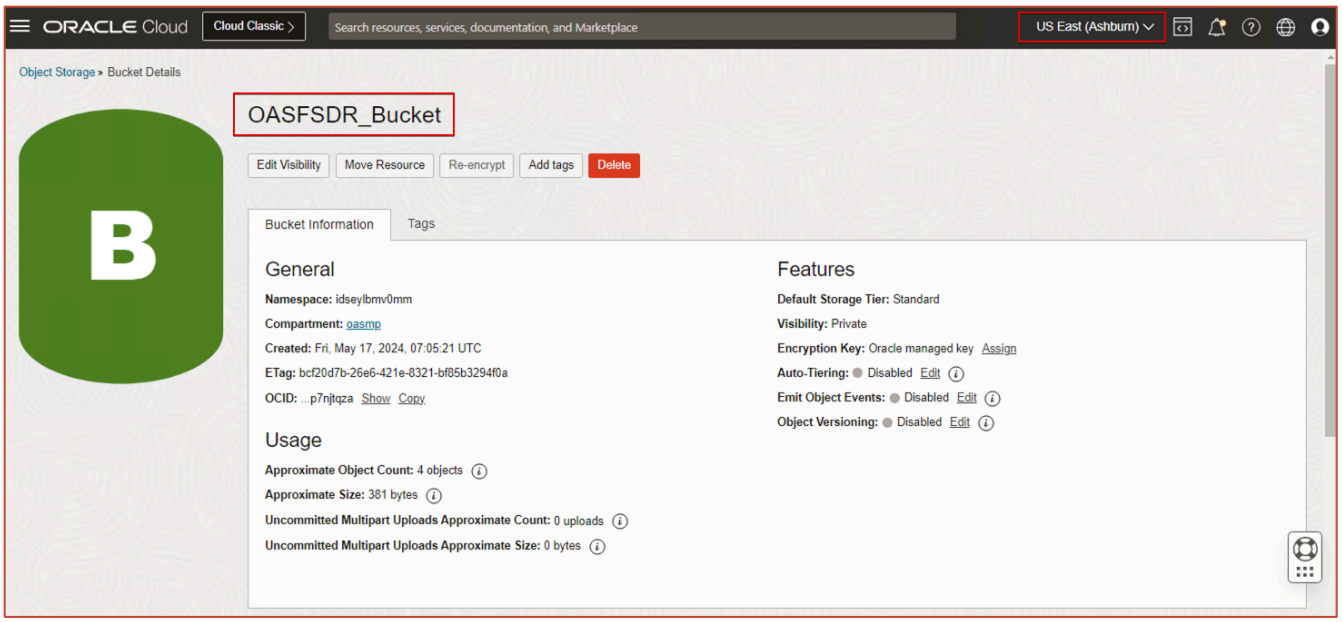
Create a Bucket to store DR Protection Group Logs

Sign in to the OCI console.

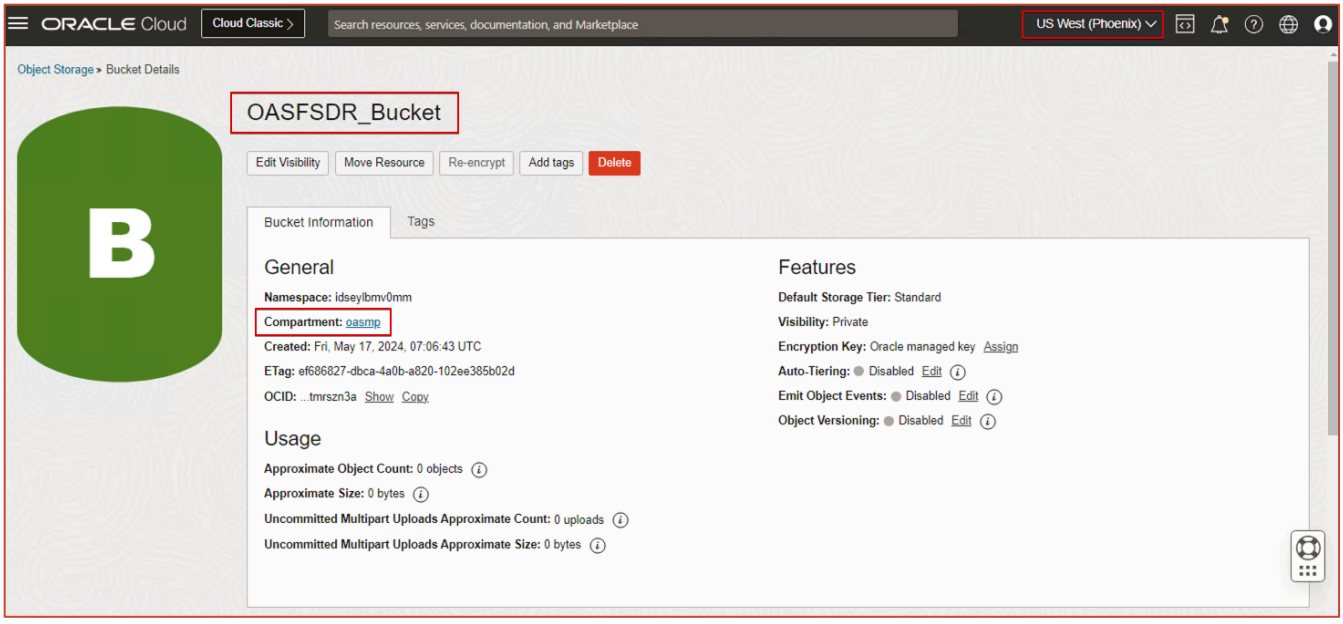
Navigate to Storage → Object Storage → Buckets.







Similarly, create a Bucket in the same Compartment (e.g., oasmp) in the OCI Secondary (DR) region.



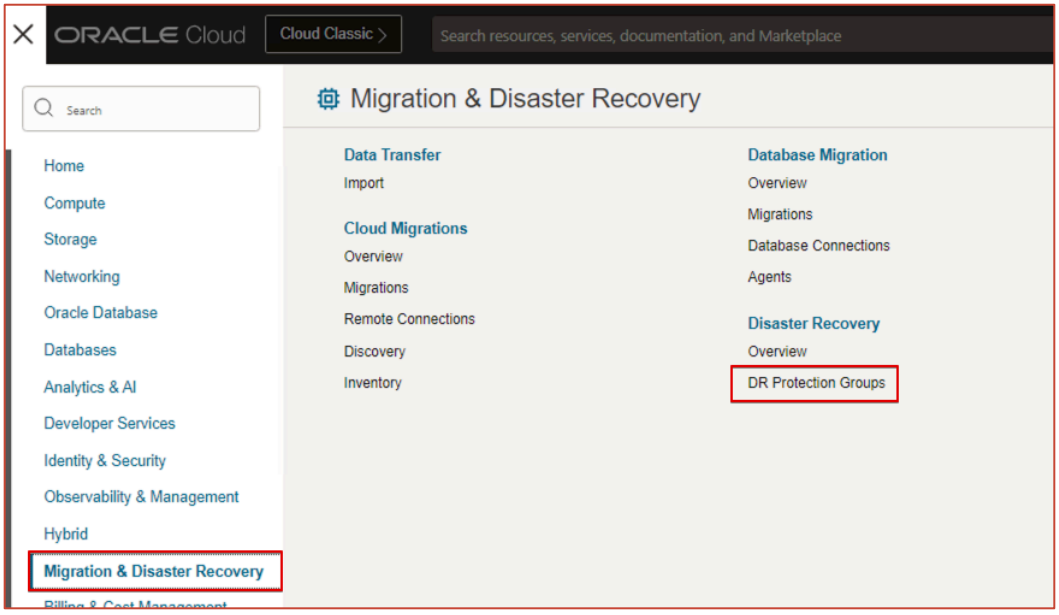
Since the prerequisites for the Full Stack DR have been met, let's proceed to create the Full Stack DR DR Protection Group.

Create a DR Protection Group

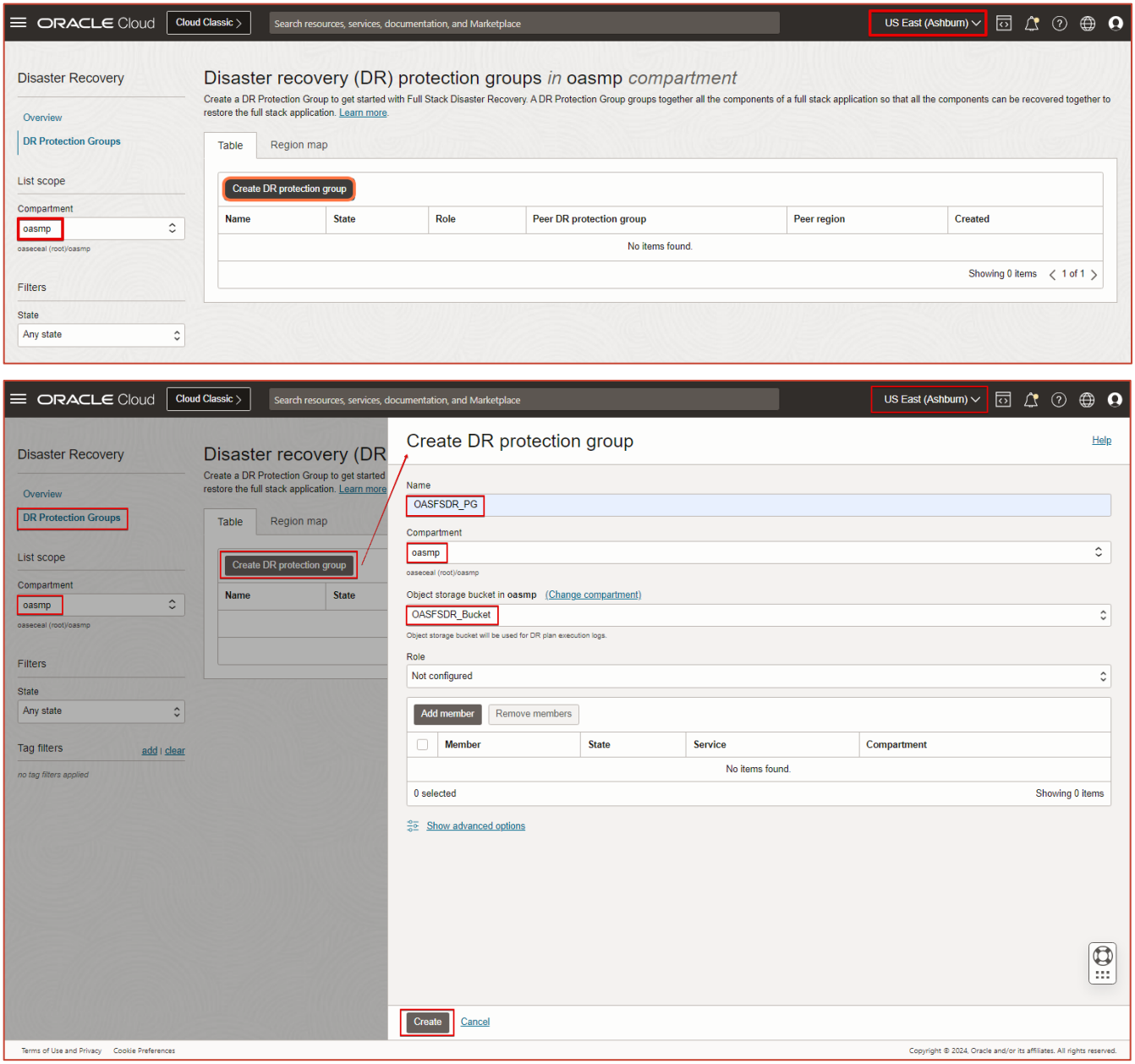
NOTE: Each task must be completed one after another; parallel tasks cannot be performed in both regions in the OCI Console. To perform parallel tasks, use the OCI CLI or SDK.

Sign in to the OCI Console

Navigate to Migration & Disaster Recovery → DR Protection Groups

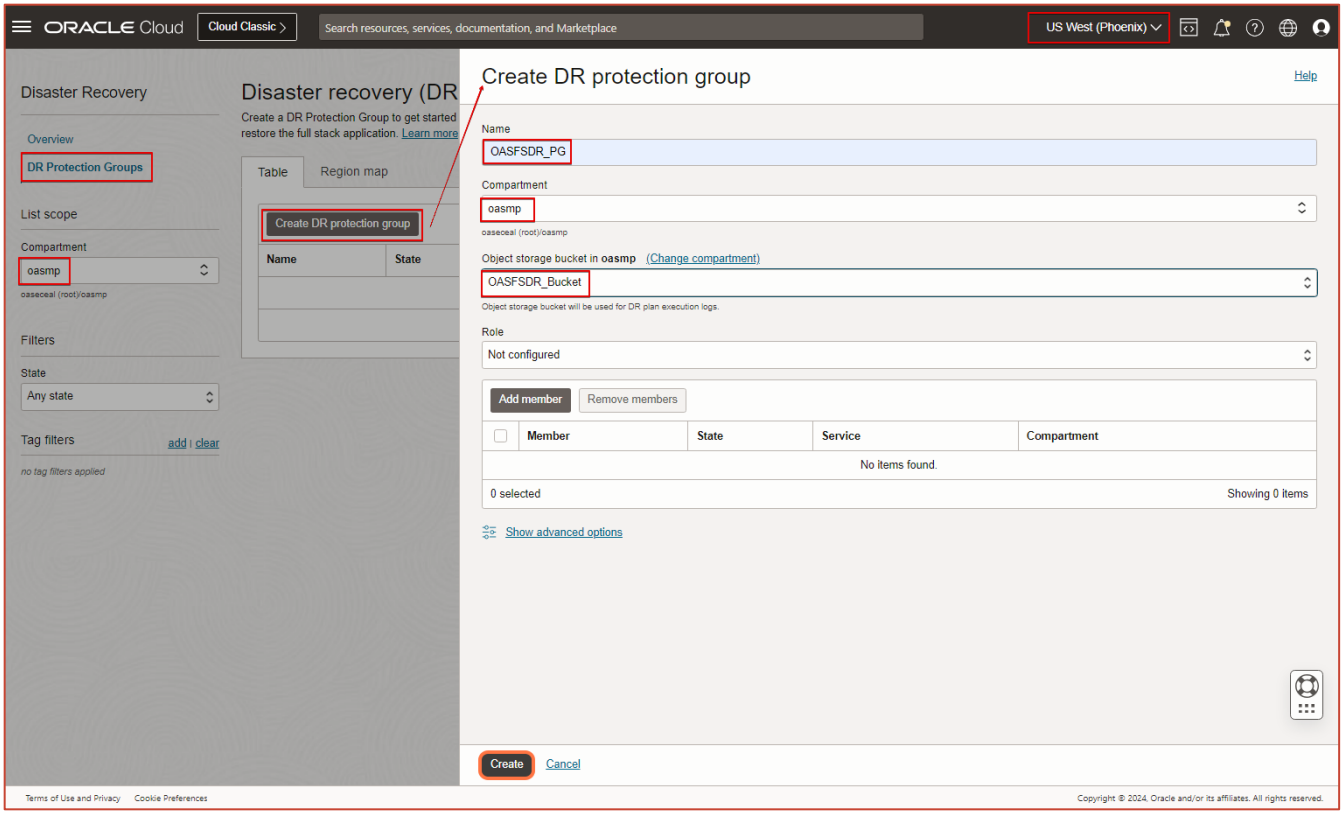


Click on “Create DR Protection Group”.



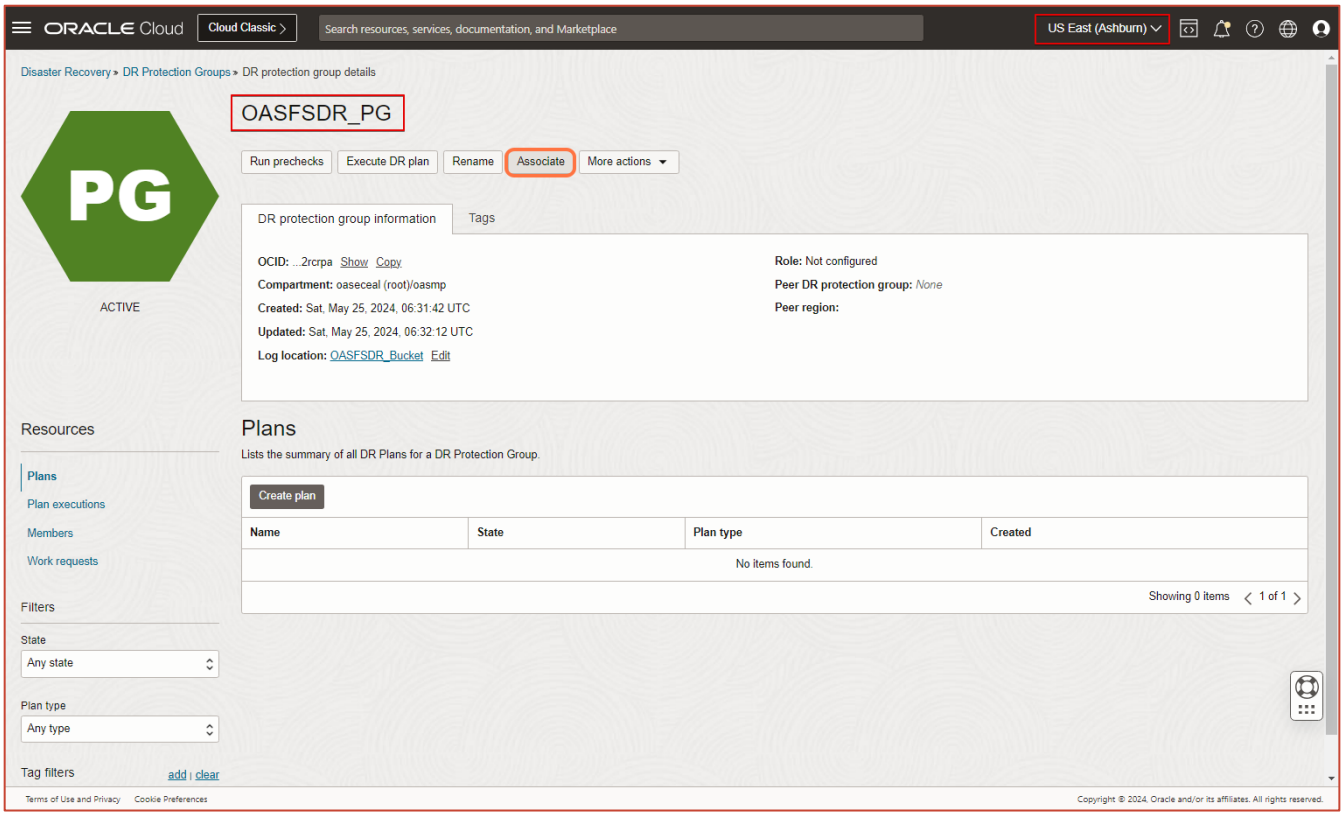
Create the DR Protection Group without Role and members initially.

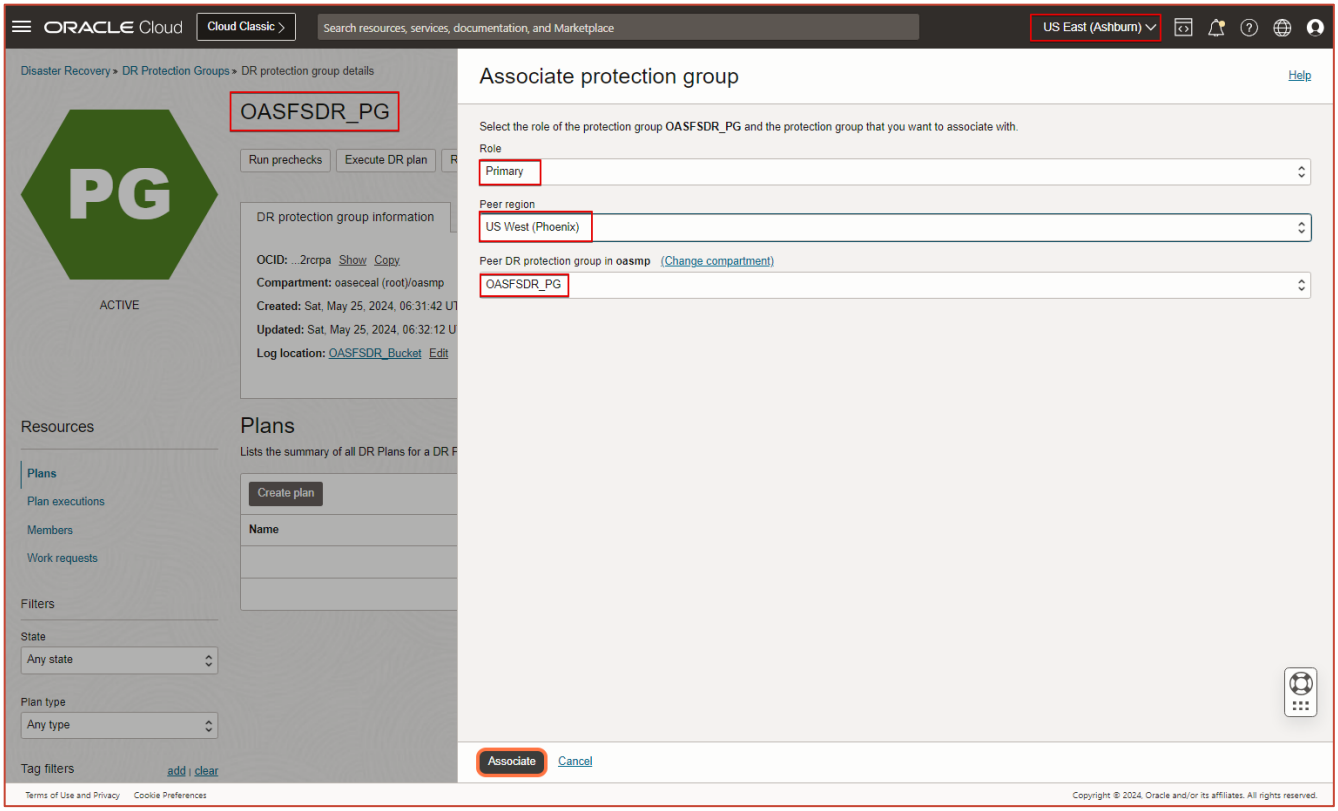
Create a similar DR Protection Group in the secondary (DR) OCI region. Don't assign any Role and Members initially.



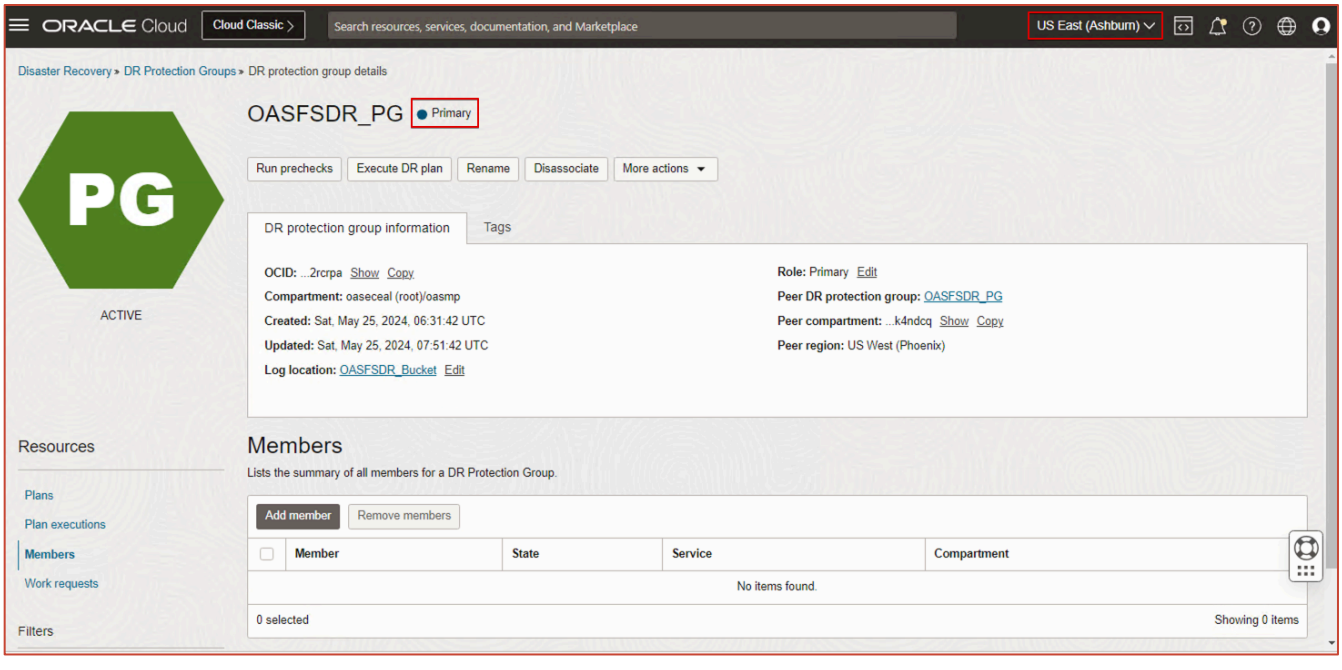
Associate the DR Protection Group to a Role

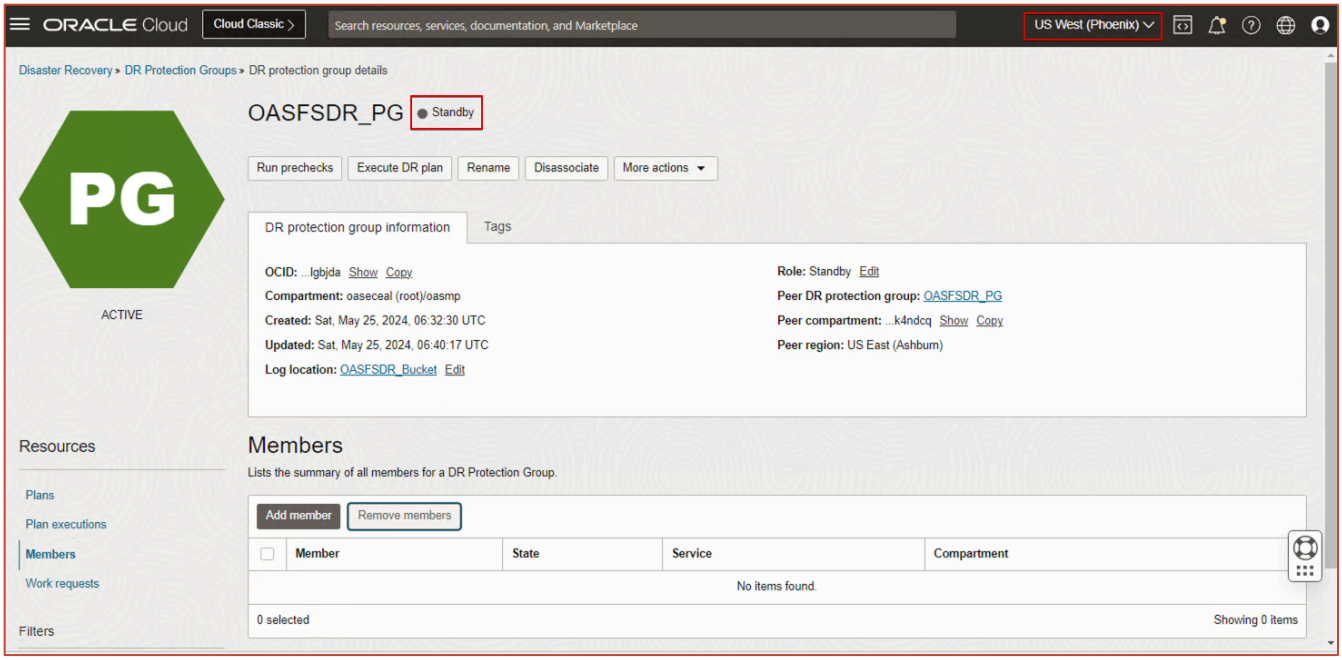
Associate the DR Protection Group to the primary role in the OCI primary region (e.g., Ashburn).





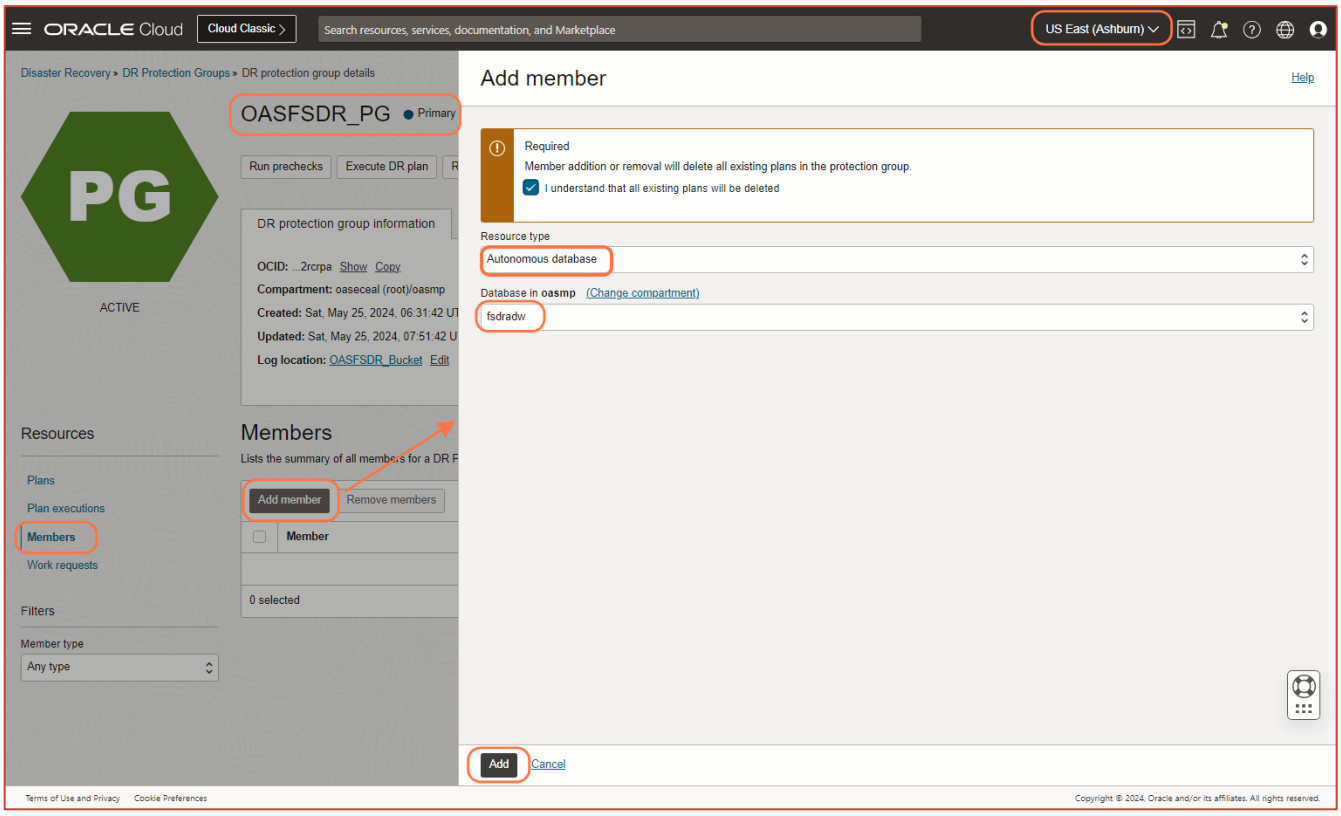
The DR Protection Group in the secondary OCI region (i.e., Phoenix) role will automatically be associated with standby.



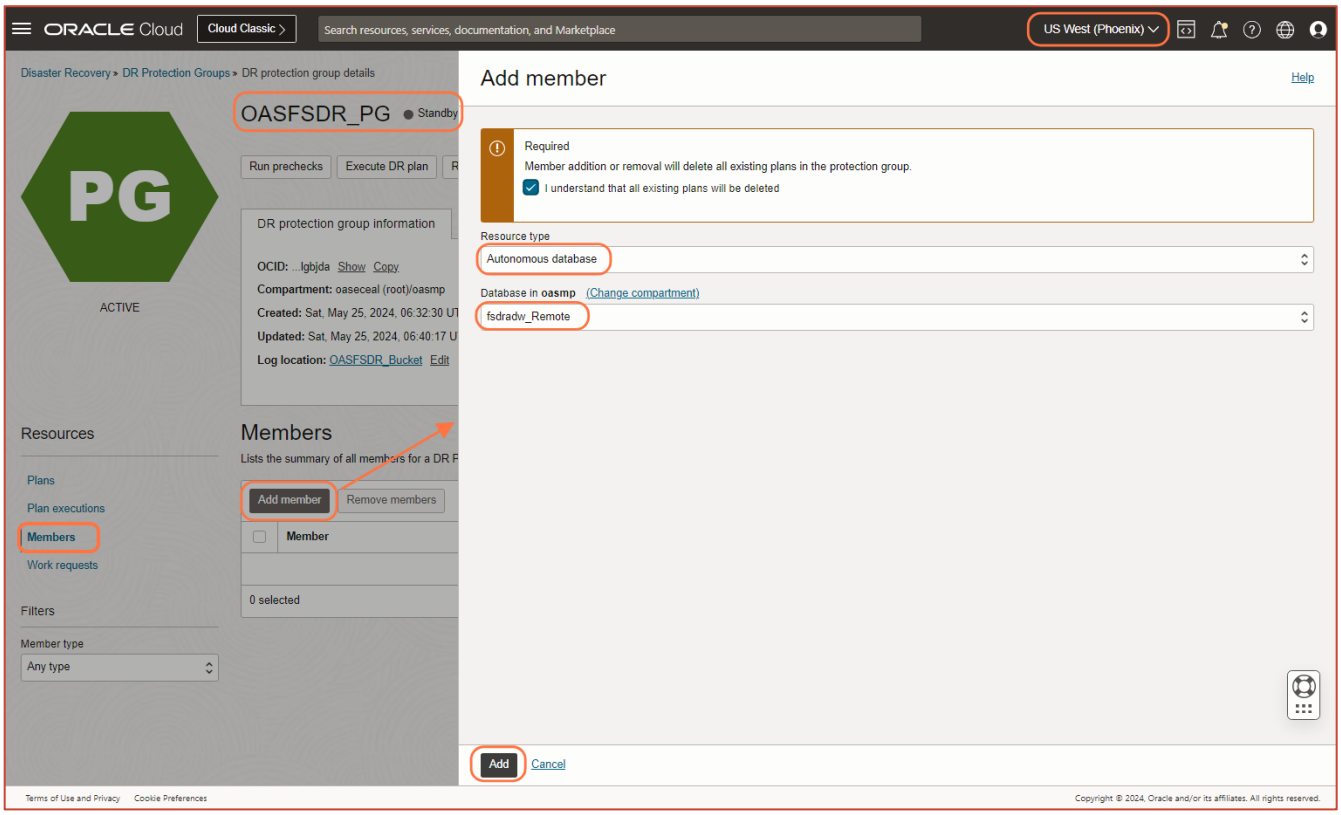


Add Members

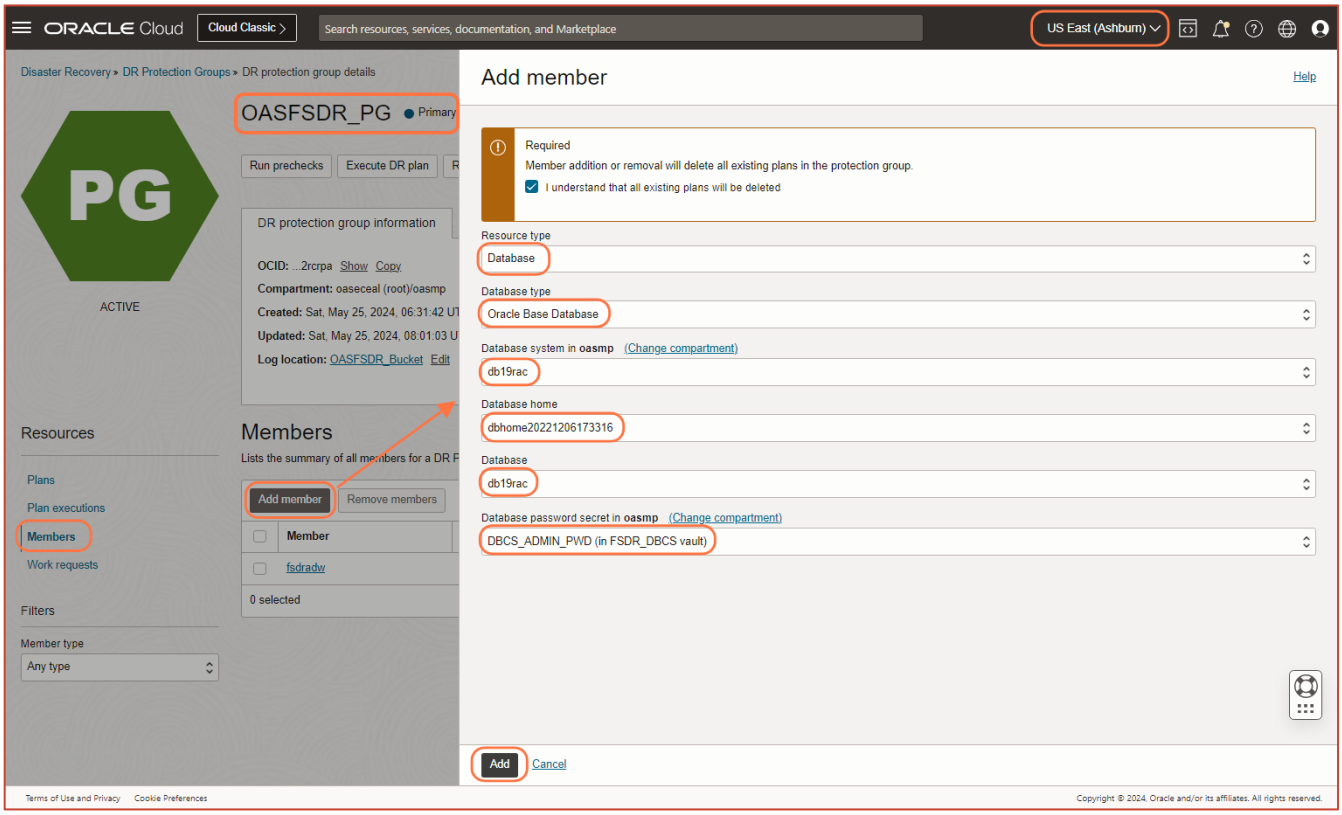
Add ADW primary Instance to the primary DR Protection Group



Add ADW standby Instance to the standby DR Protection Group

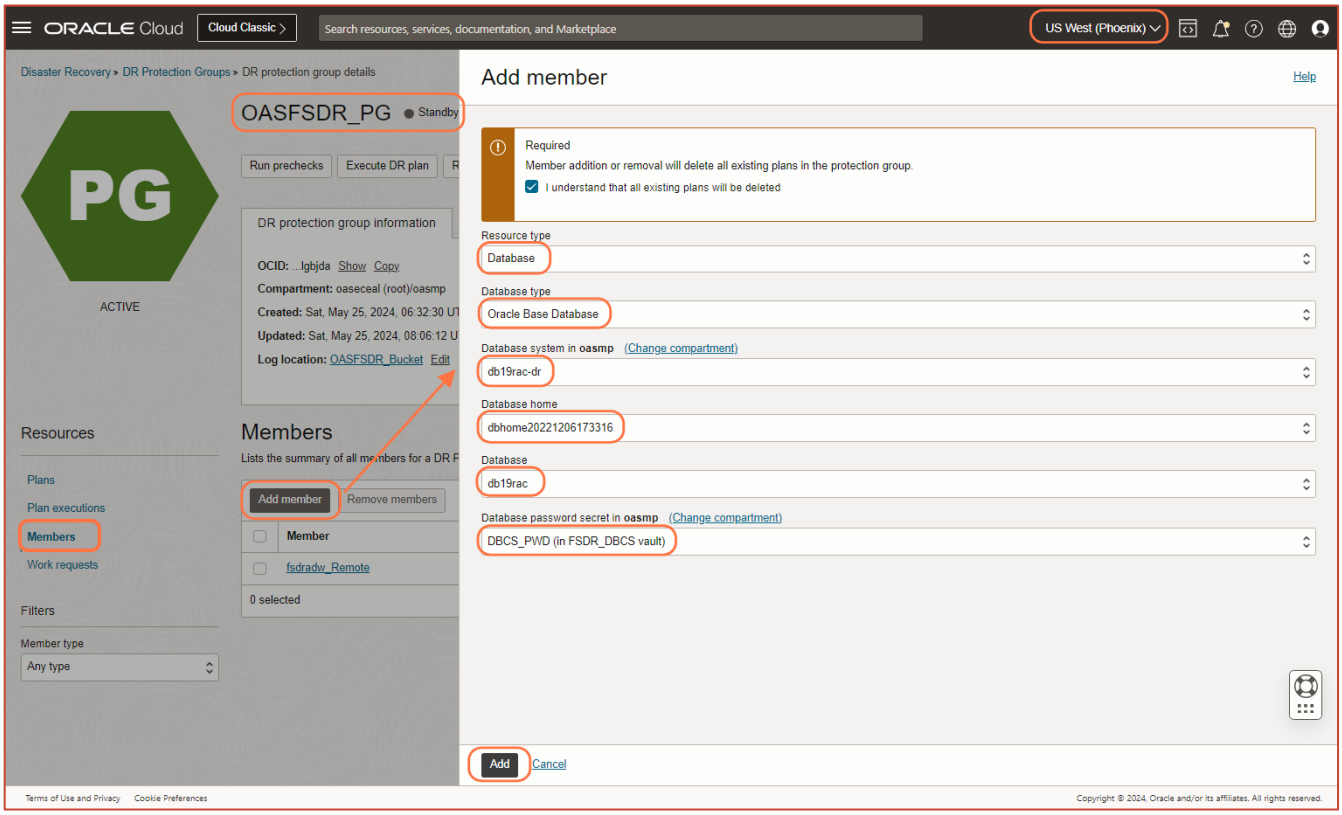


Add DBCS primary Instance to the primary DR Protection Group

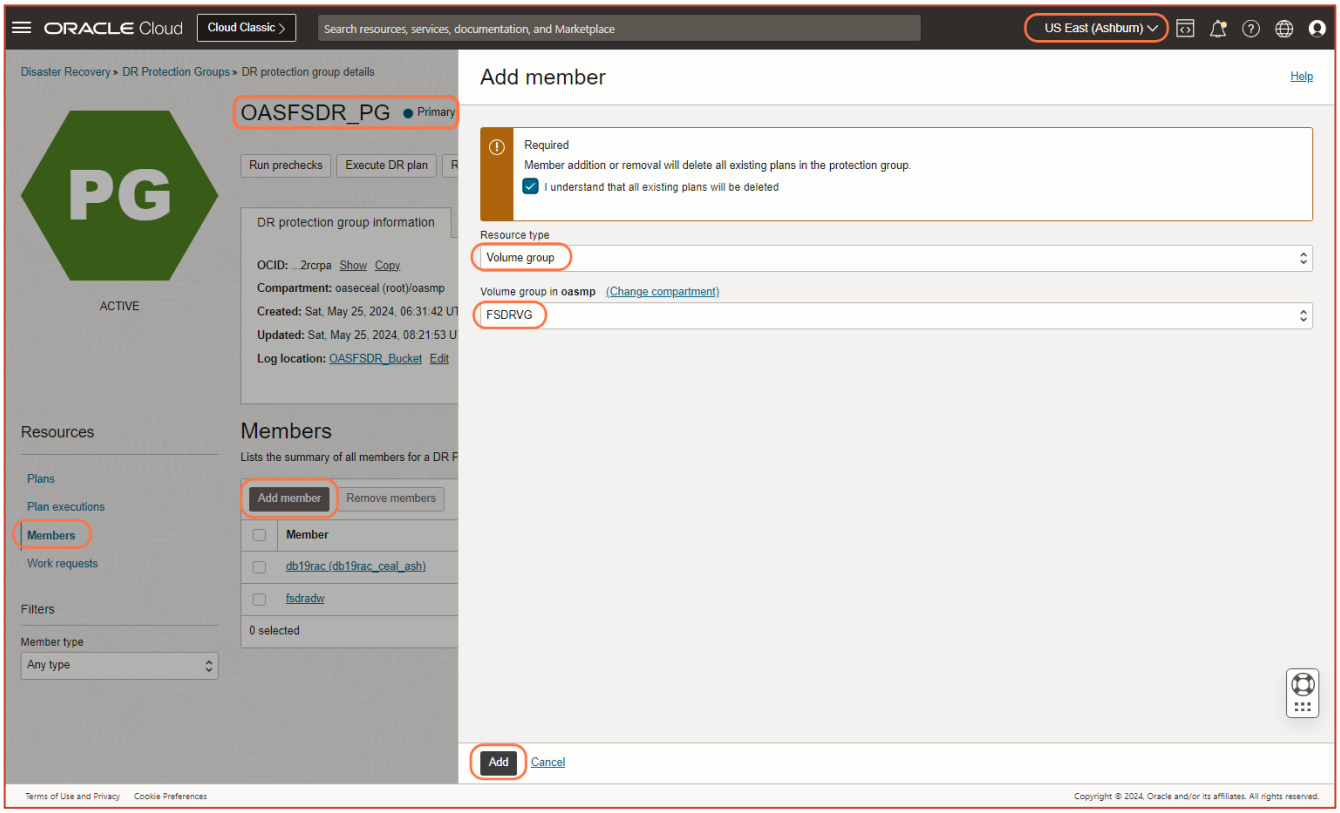


Select the DBCS admin password created in the Vault.

Add DBCS standby Instance to the standby DR Protection Group

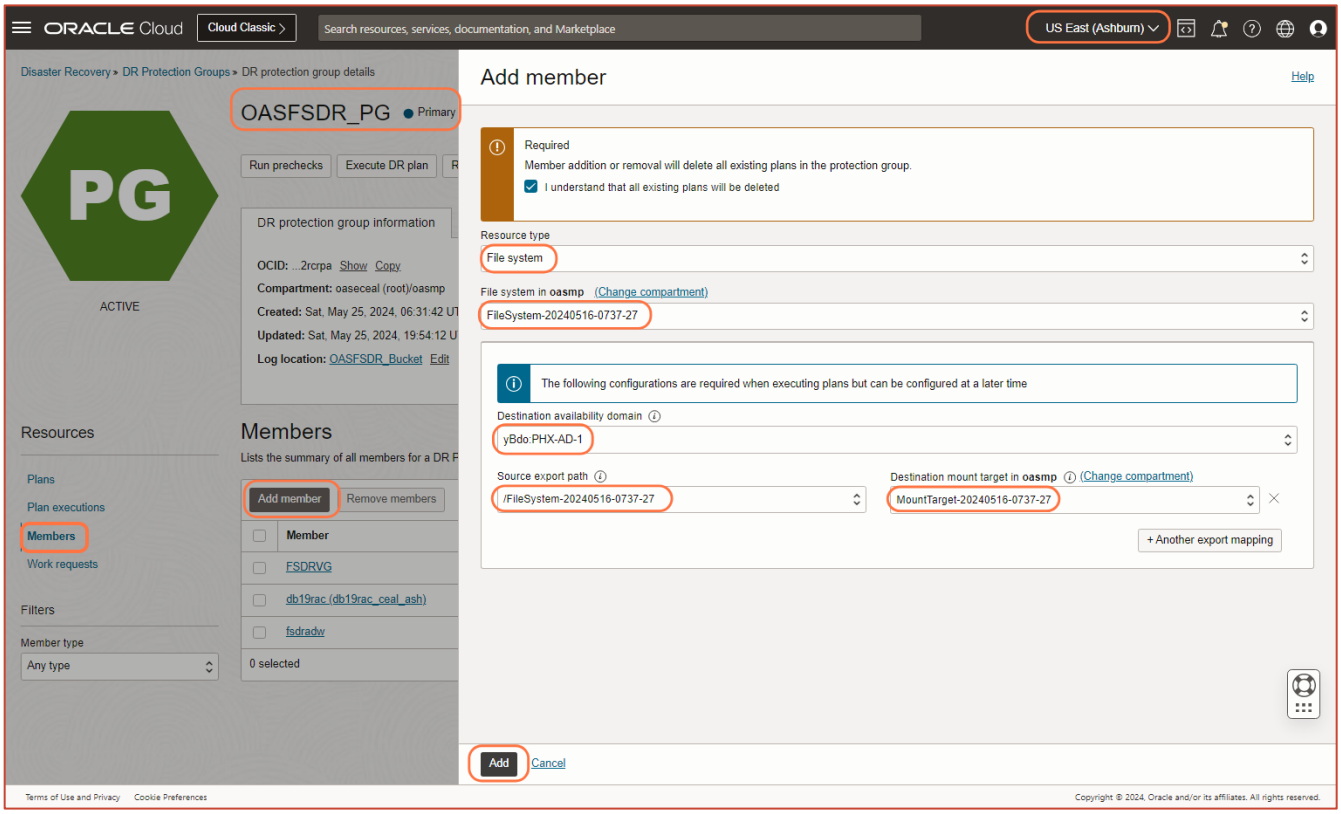


Add Volume Group to the primary DR Protection Group



For the moving instance scenario, a Volume Group is not needed in the Secondary (DR) OCI region. The Primary Volume Group replica will be used in the DR region during the switchover/failover.

Add File System to the primary DR Protection Group



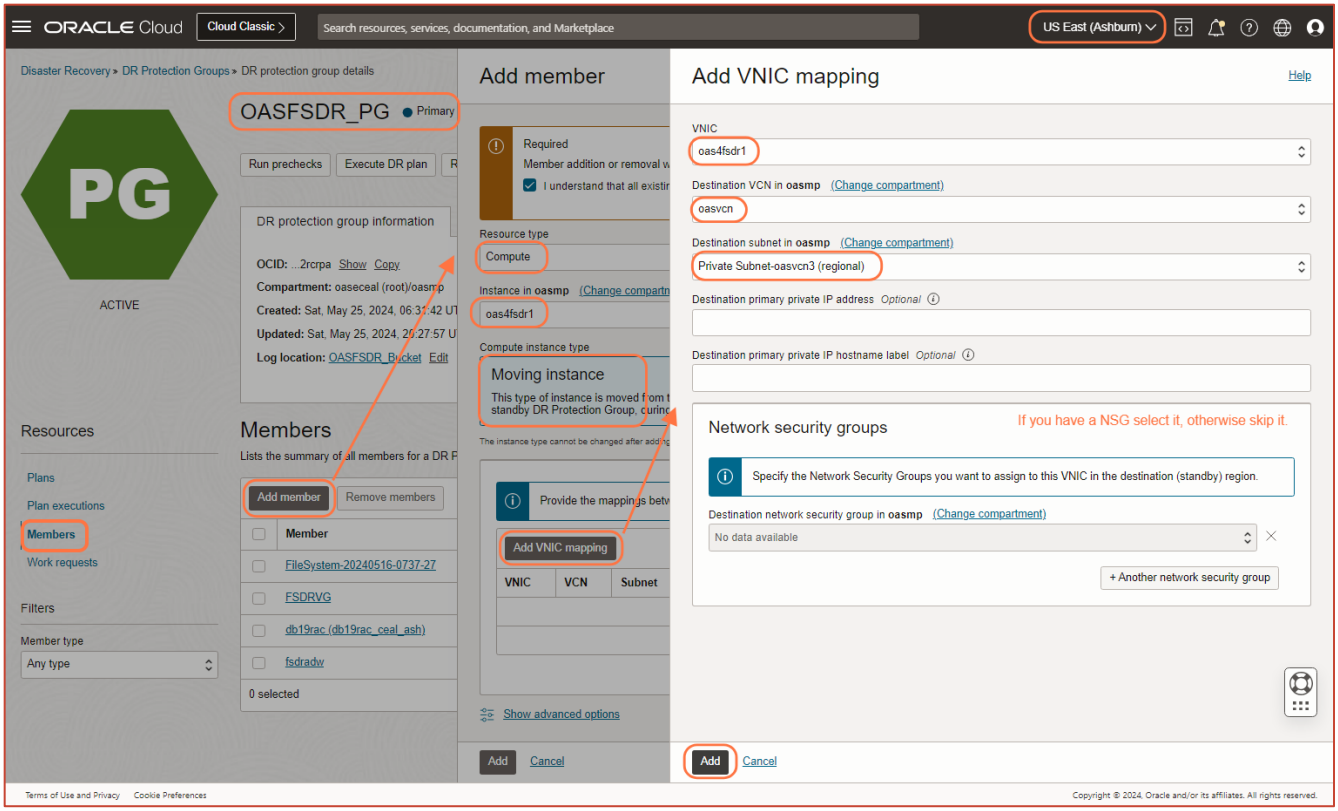
Add OAS compute instances to the primary DR Protection Group

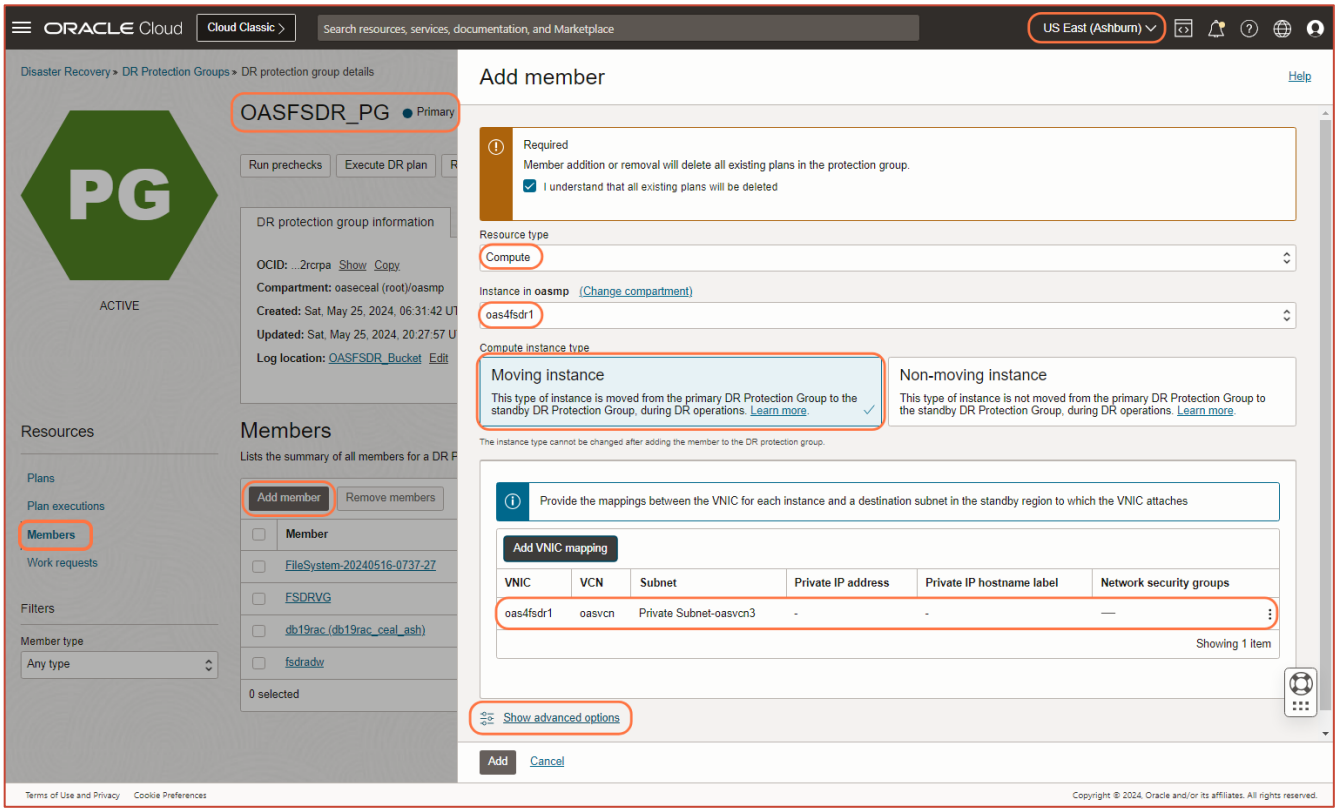
In a non-moving compute instance type, the OAS compute instances with the same hostnames are expected to be pre-created in the secondary (DR) OCI region before the DR plan execution like an active-passive DR architecture.

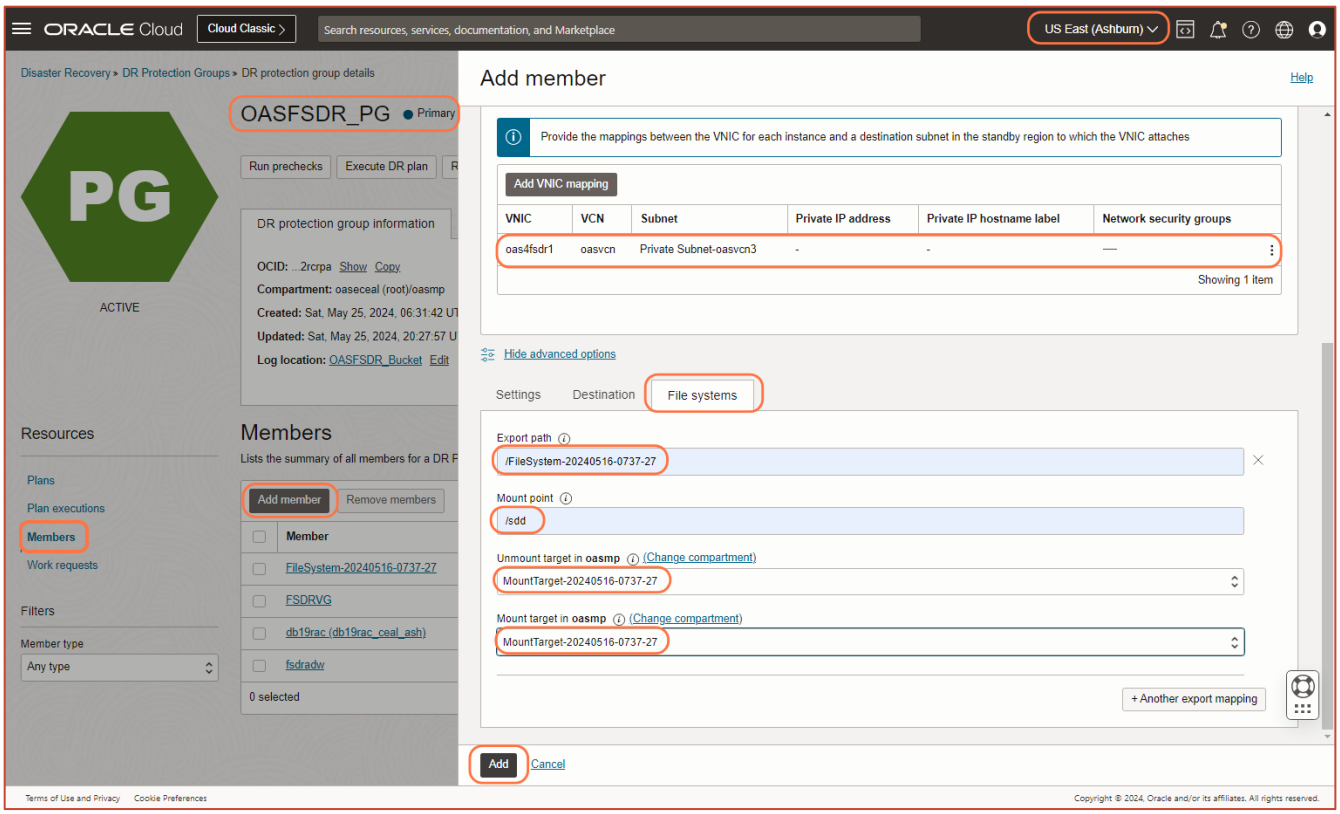
The OAS compute instances exist only in the primary OCI region in a moving compute instance type. When the switchover/failover happens due to DR plan execution, these compute instances are moved to the secondary (DR) OCI region.

In a moving compute instance type, you can select a private IP and hostname if required. However, for the OAS, you don't need to specify a private IP and hostname as we use non-overlapping CIDR ranges between the private subnets of the primary and secondary OCI regions.

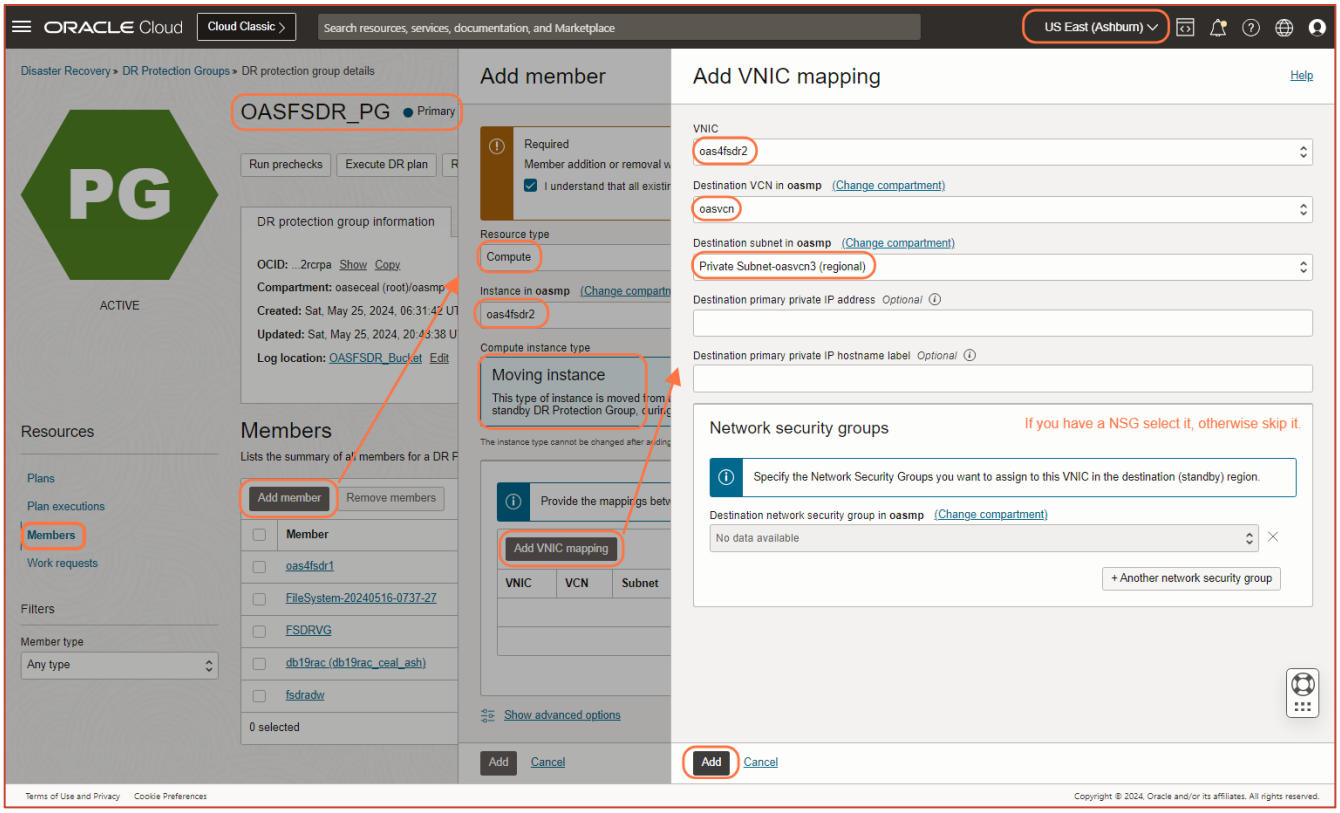
Since the private subnet used for OAS compute instances has labels like "e.g., oase," you will have the same domain name between the primary and secondary compute instances, which results in the same hostnames across regions.

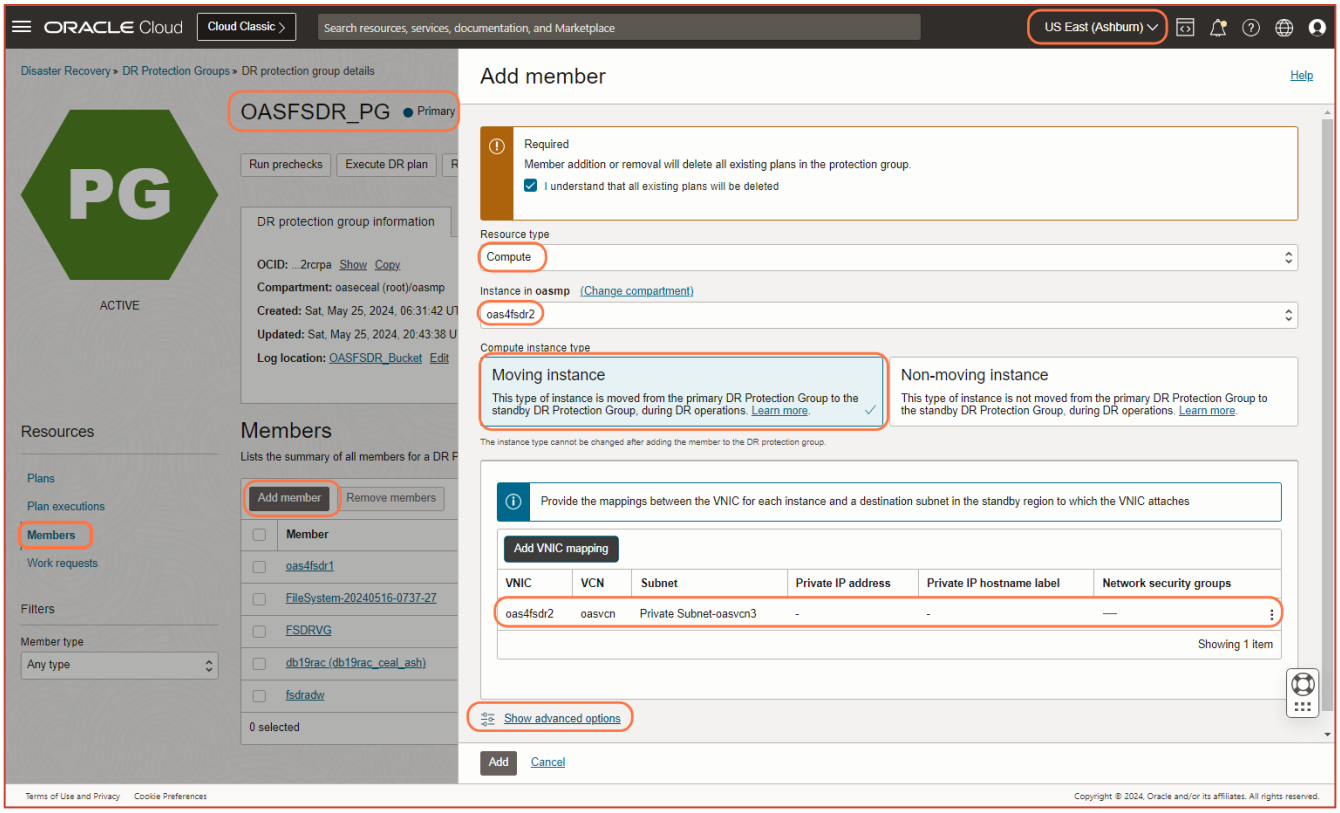


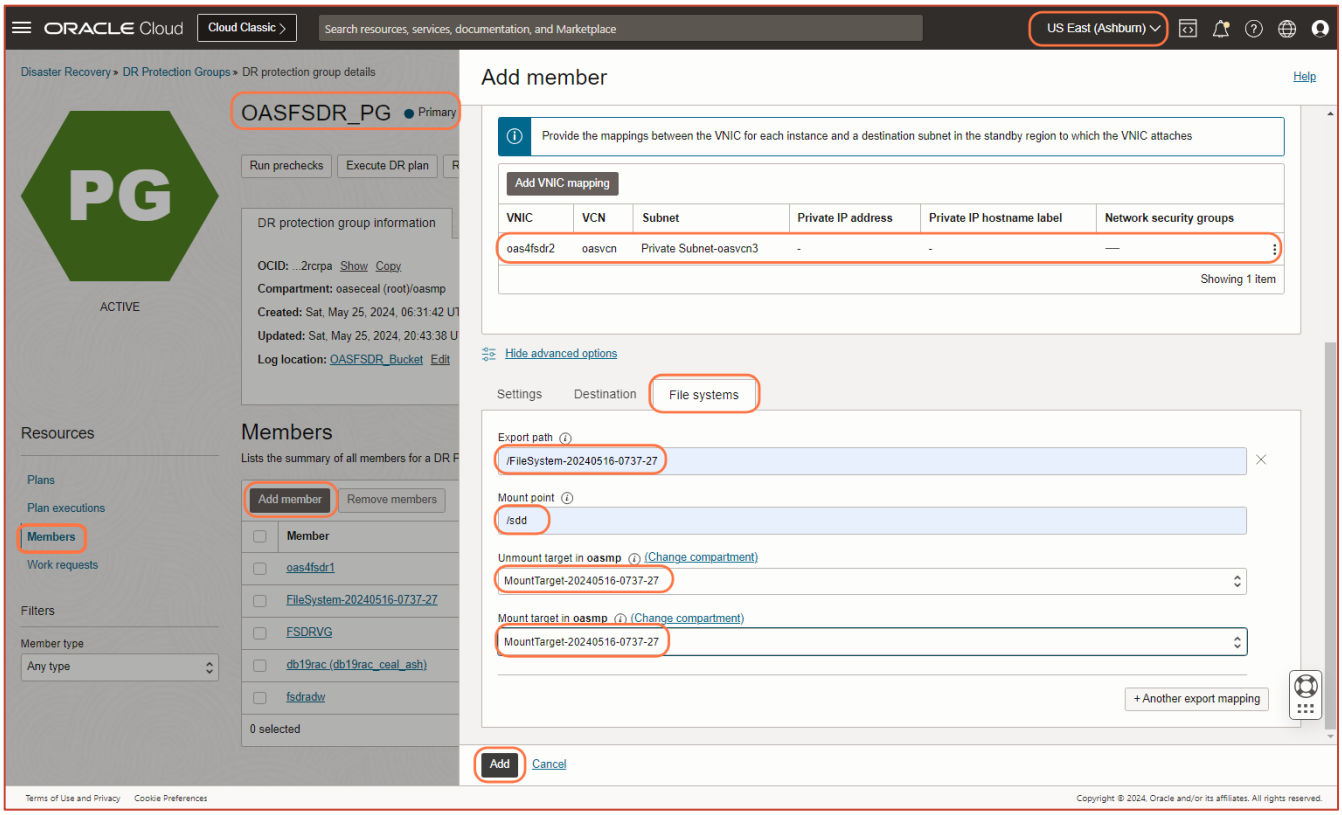




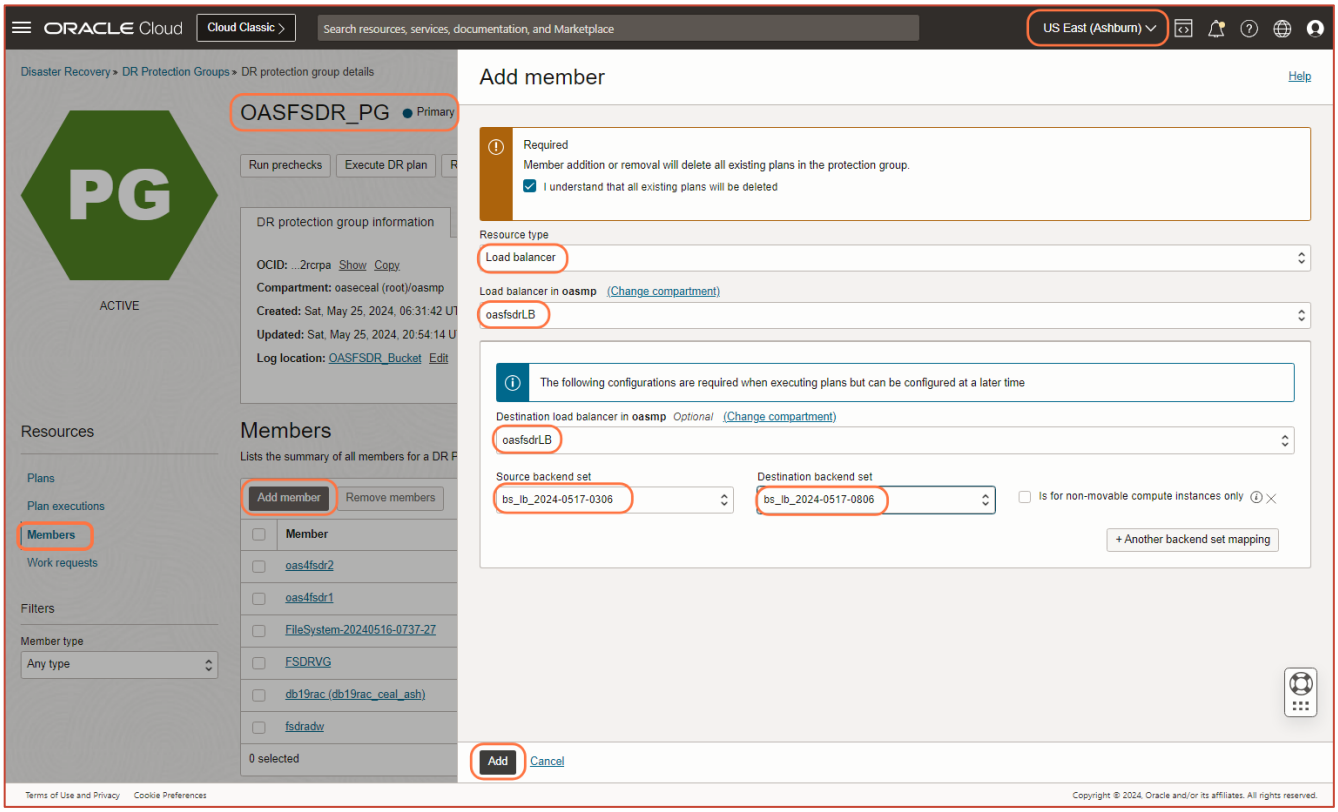
Similarly, add all the OAS nodes that are part of the Cluster.



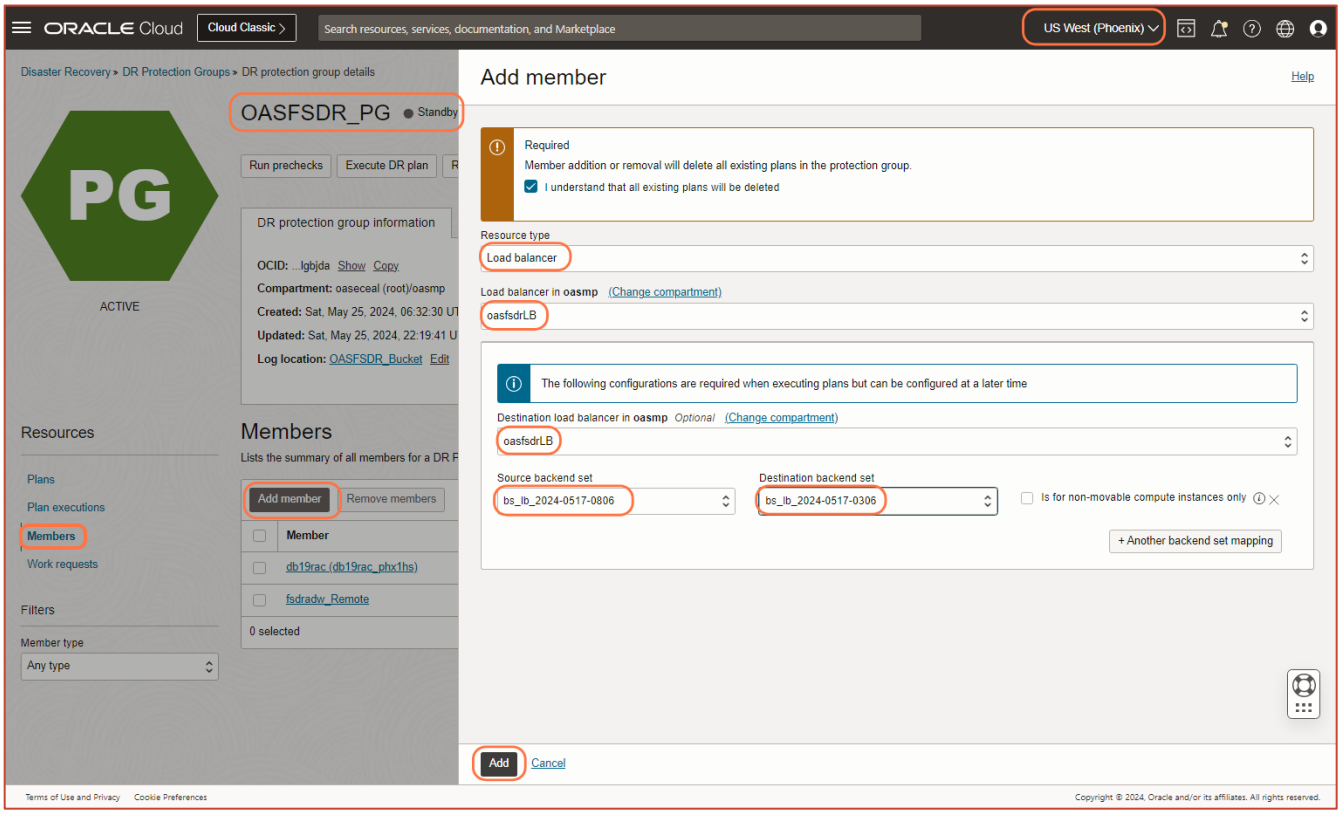


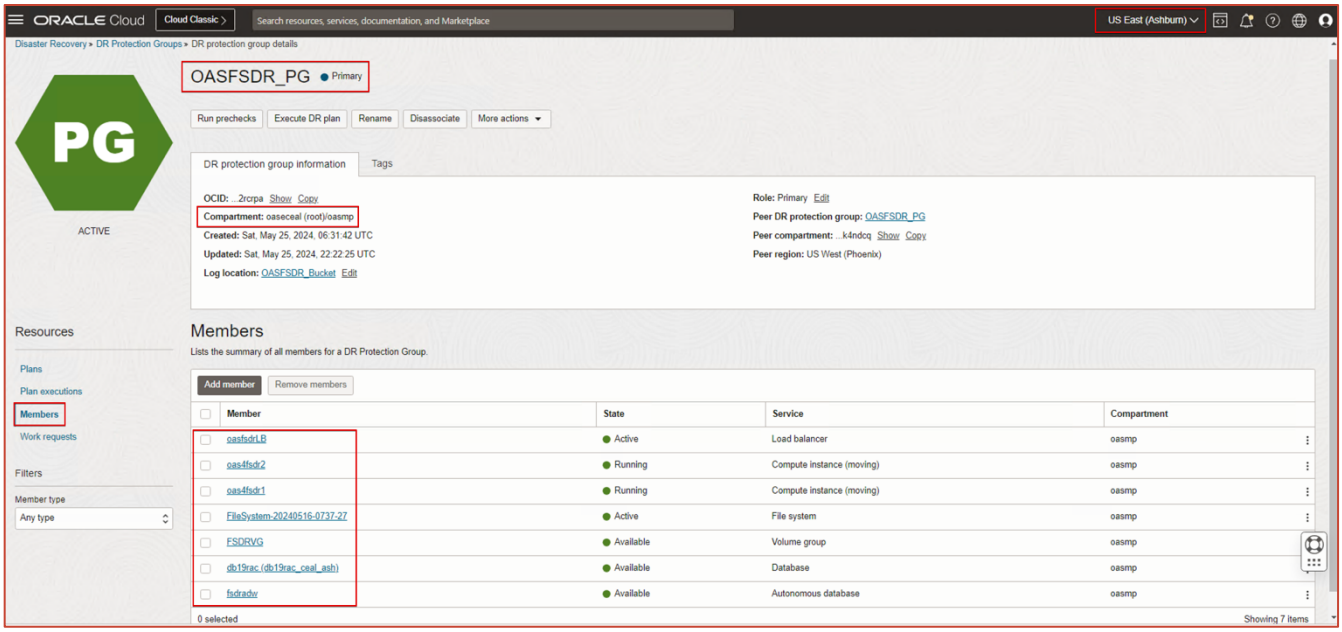


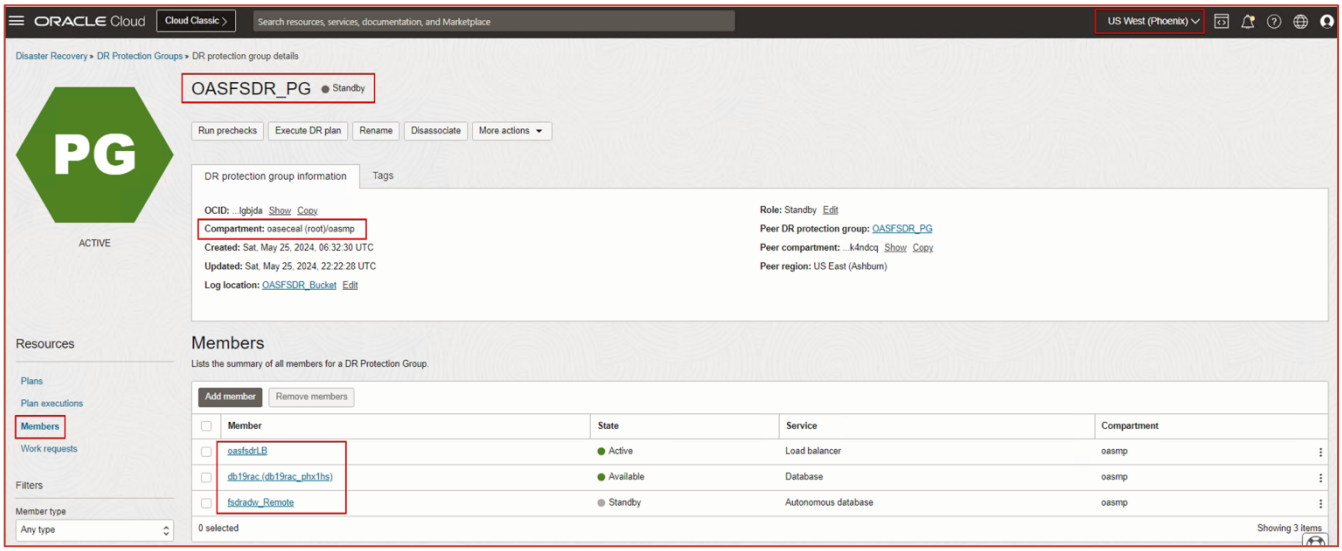
Add the OCI primary region Load Balancer to the primary DR Protection Group



Add the OCI secondary (DR) region Load Balancer to the standby DR Protection Group







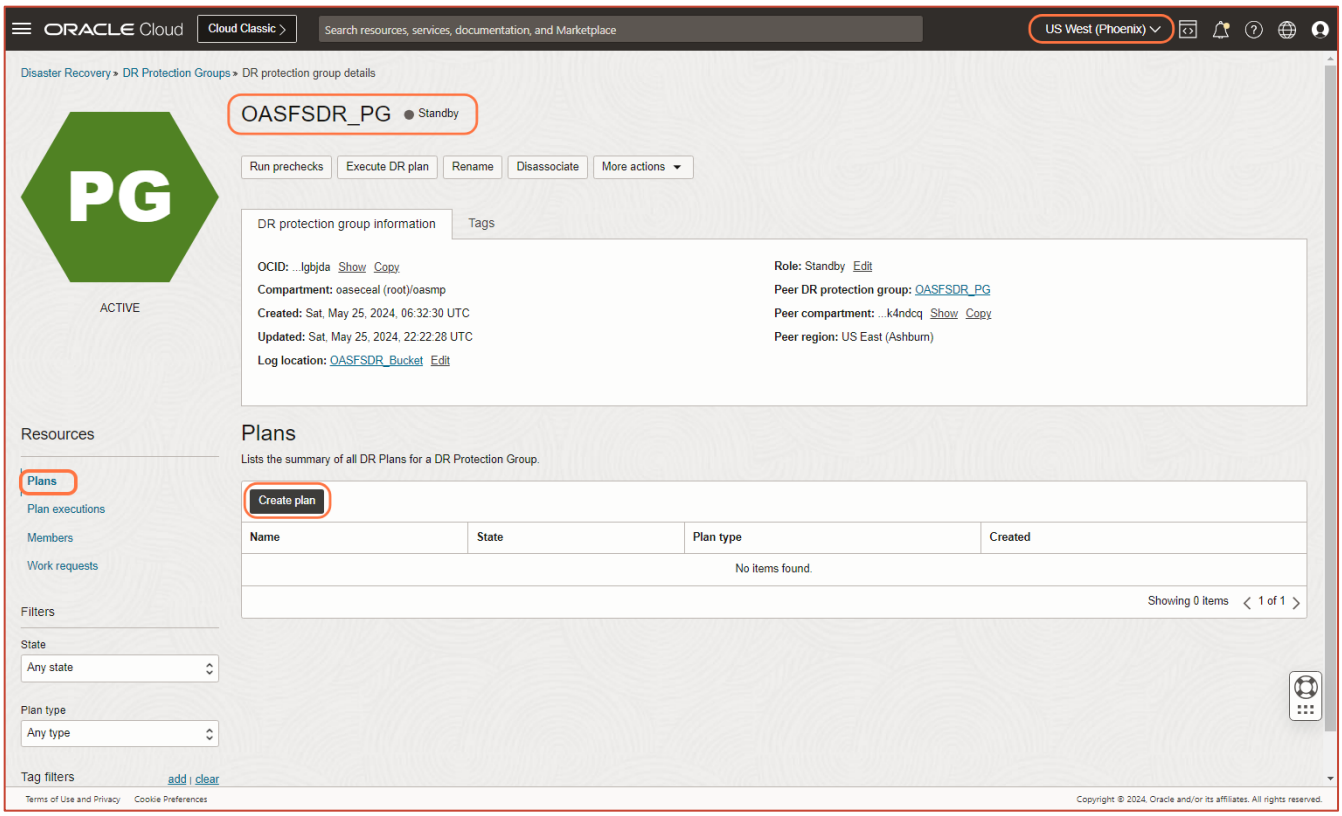
All the components involved in the OAS primary environment are added as members of the DR Protection Group.

Create a Switchover Plan

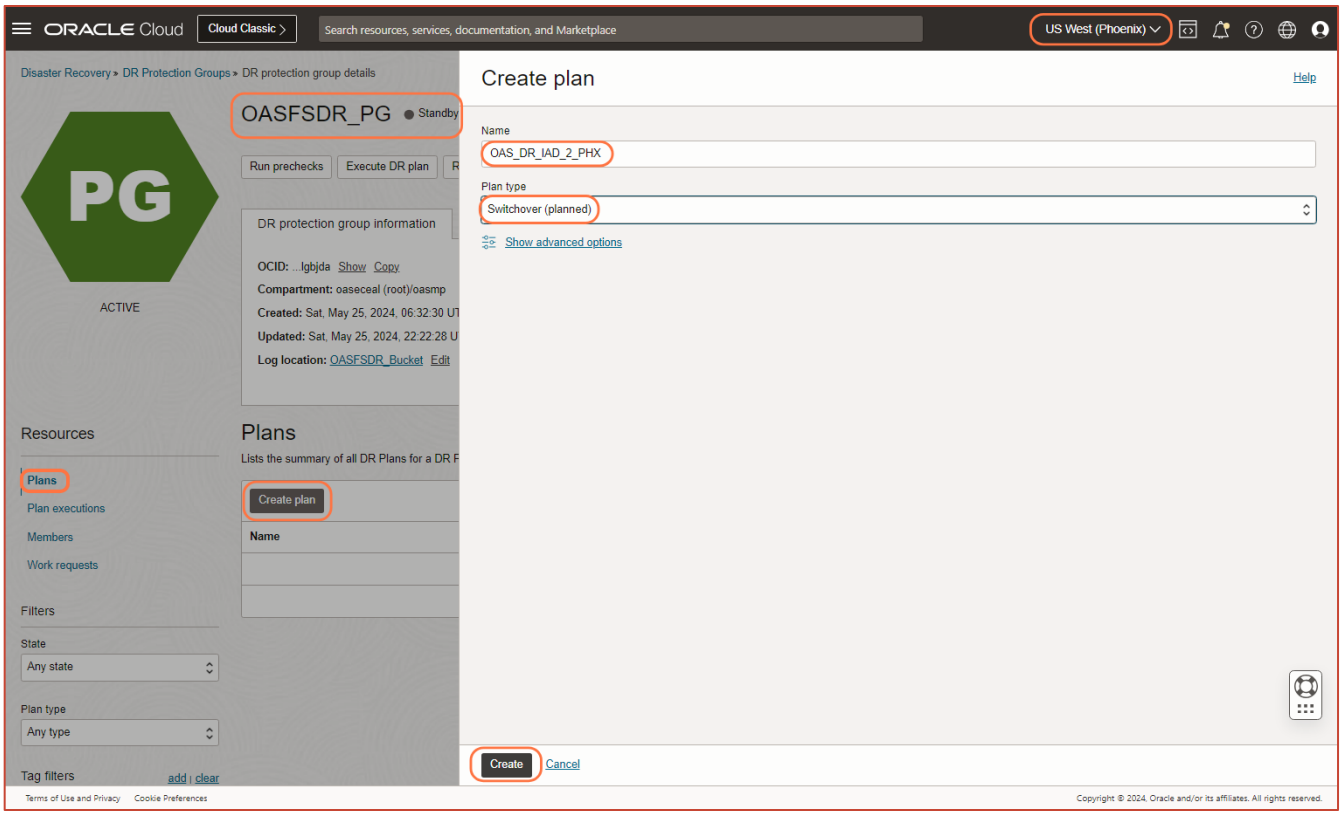
When switching from primary to secondary, always create the DR Plan and execute it from the secondary OCI region.

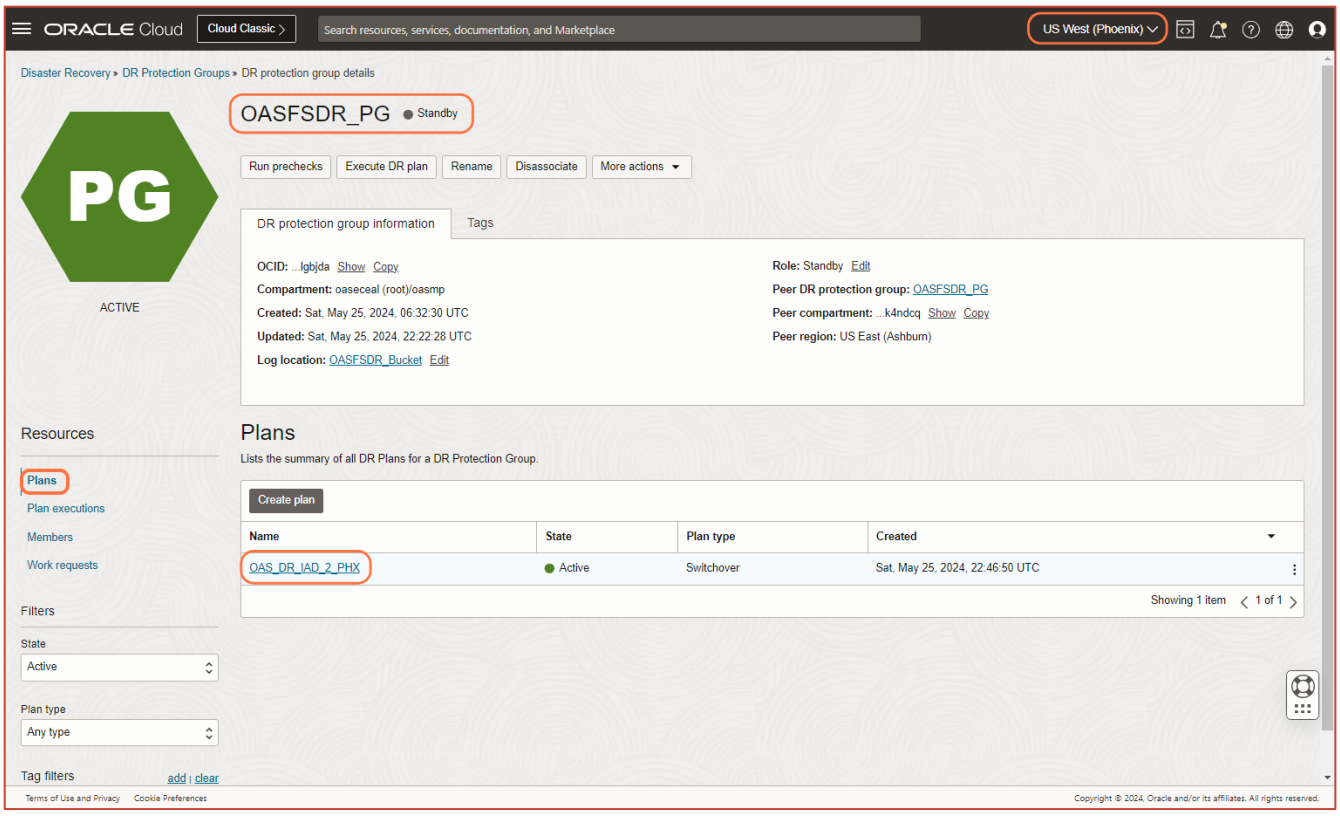
When falling back from secondary to primary, always create the DR Plan and execute it from the primary OCI region.

Create a switchover plan

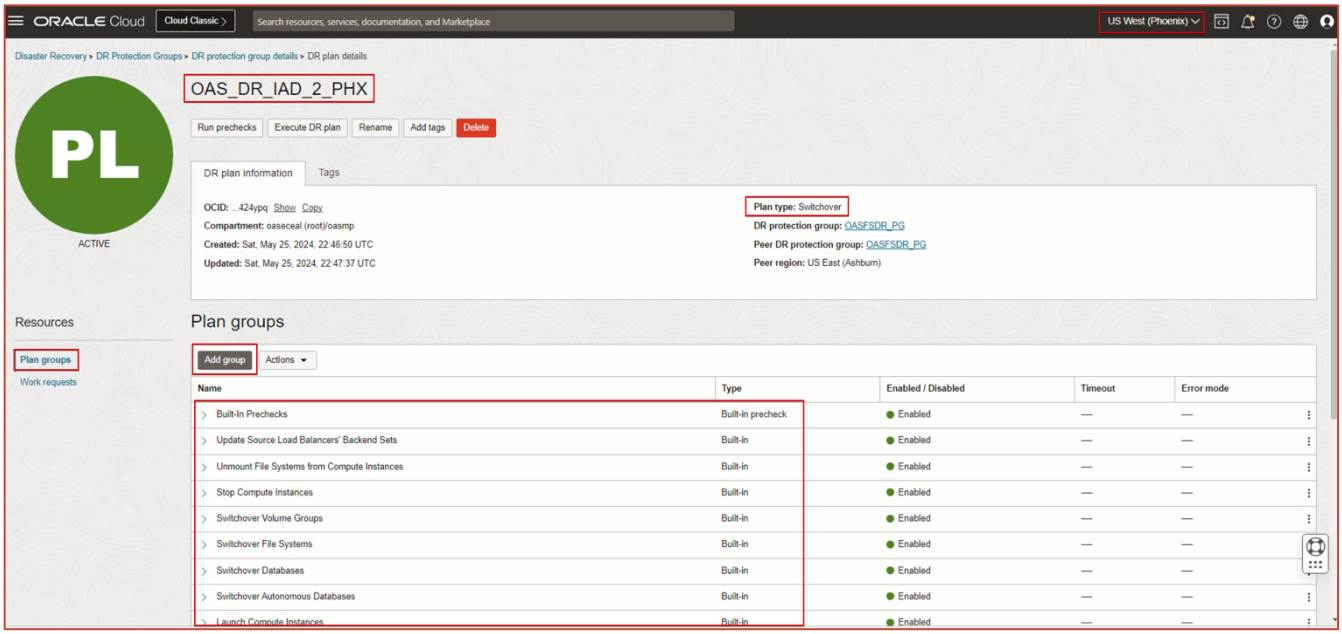


Can create multiple plans parallelly.





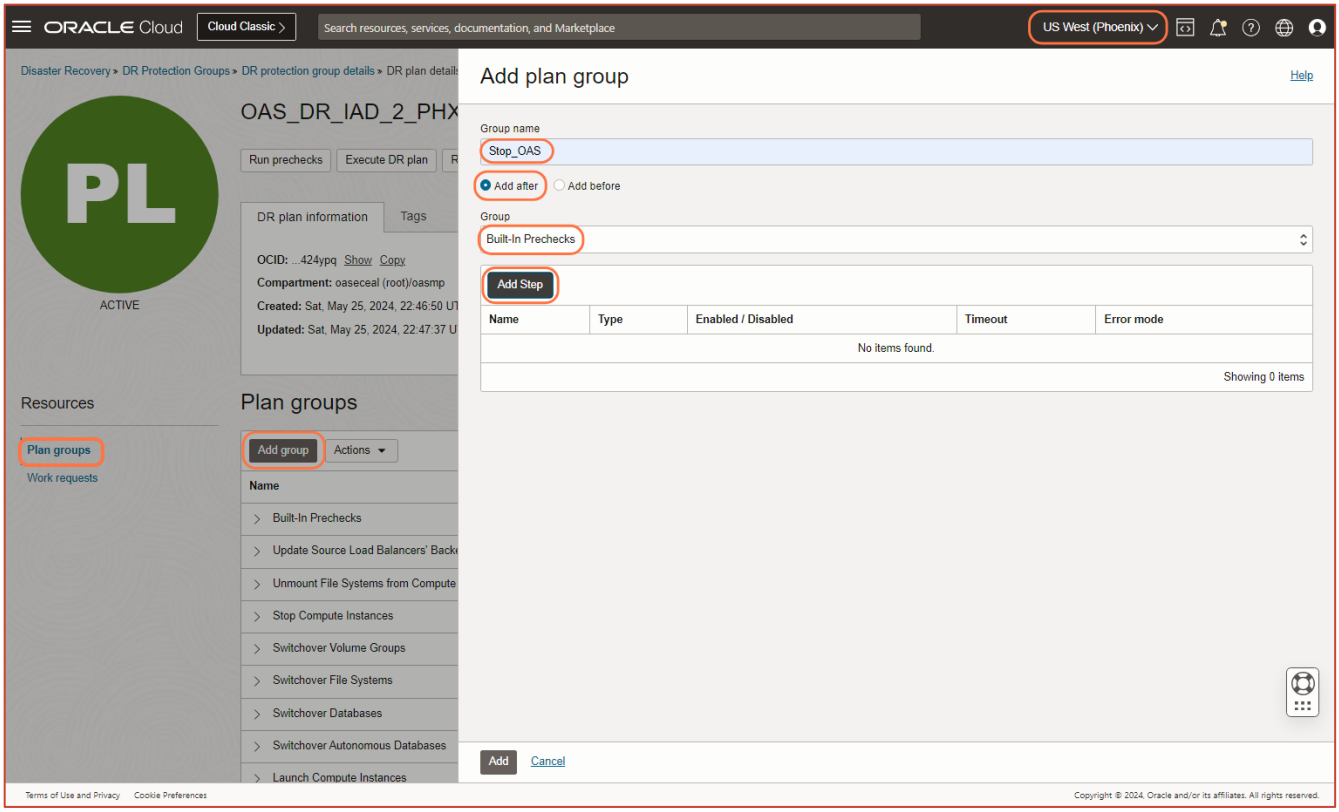
Click on the Plan created.

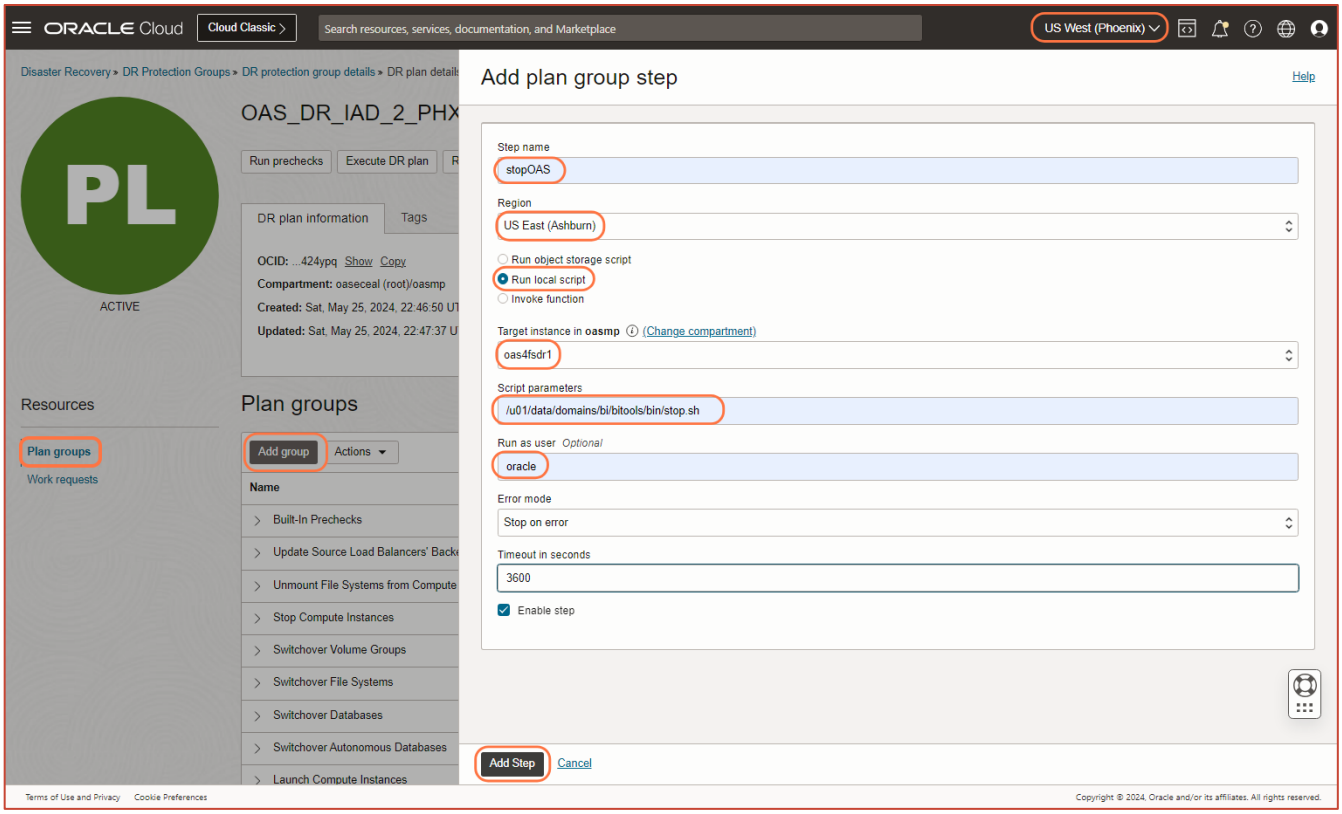


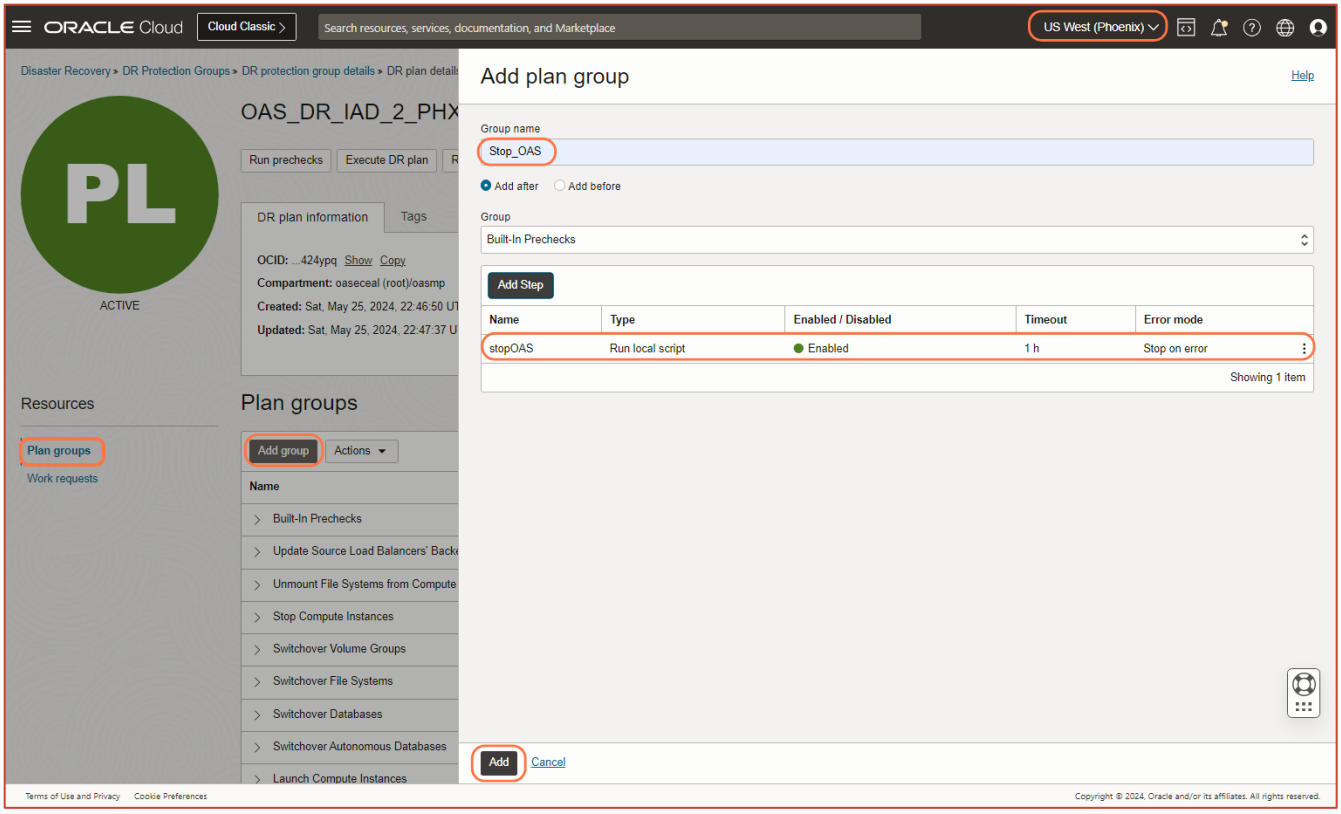
Observe the Built-in groups created. The process starts by stopping the primary compute instances in the primary region and starting the secondary compute instances in the secondary region.

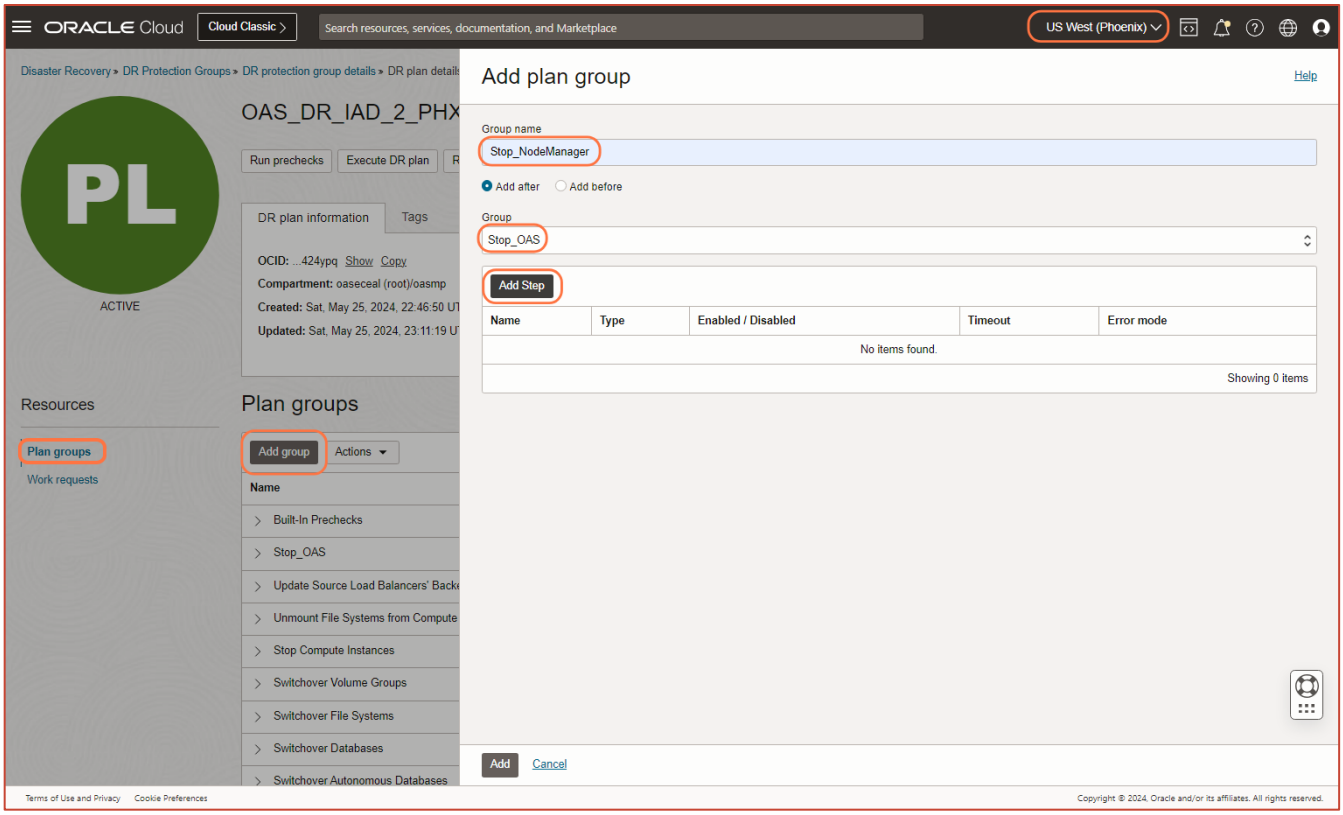
While doing such actions, it's always suggested to stop OAS services safely on the primary OAS compute instances and start OAS services on the secondary OAS compute instances.

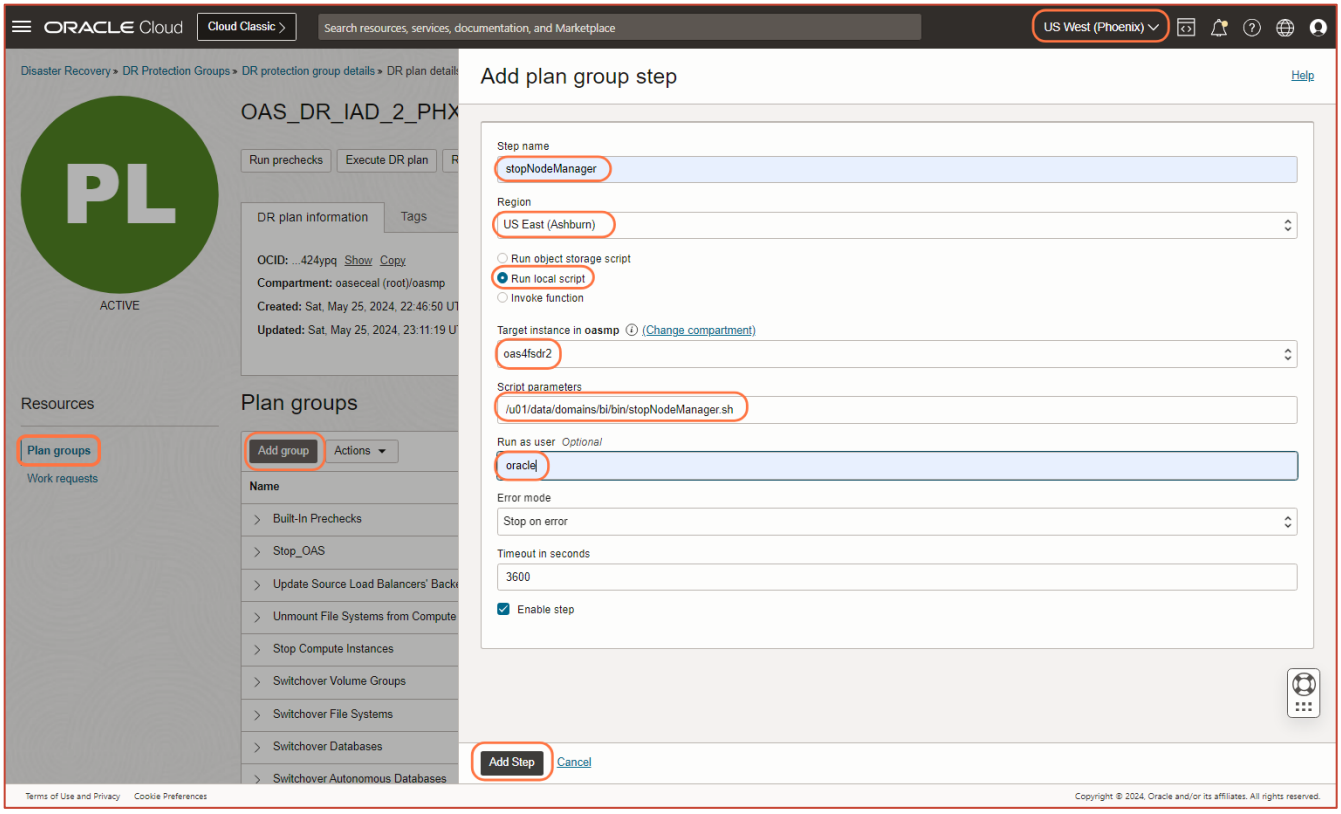
Add User-Defined Groups to include calls to stop OAS Services, stop Node Manager, etc.

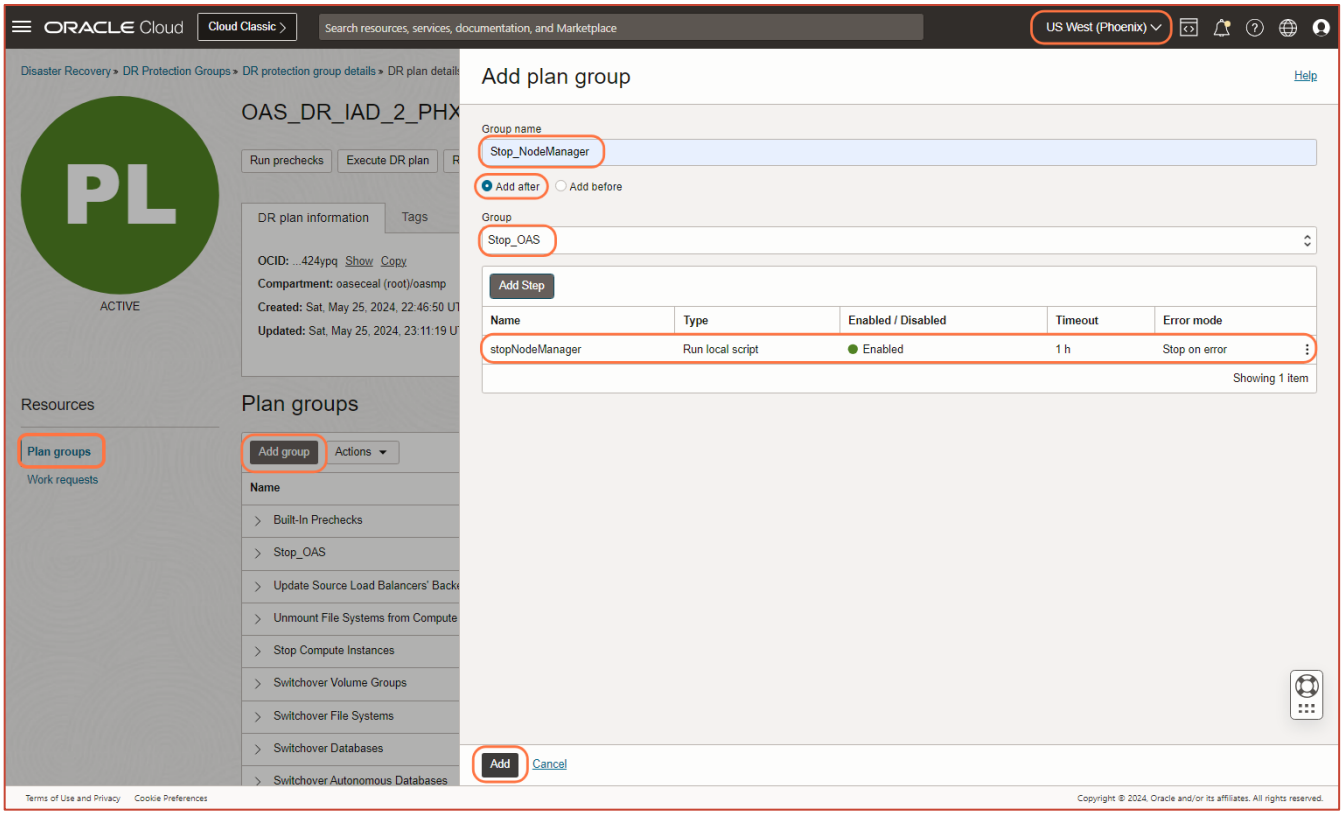




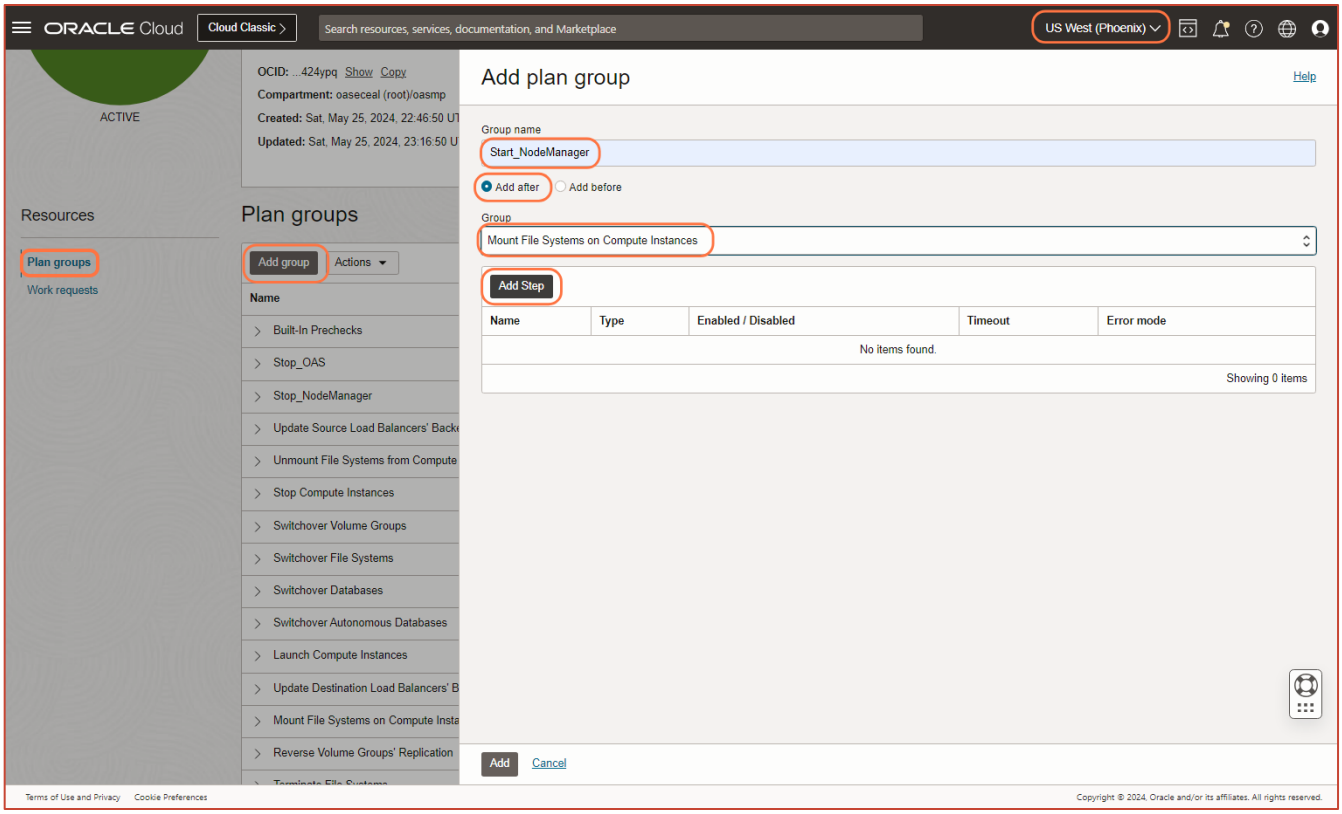








Similarly, add groups to start Node Manager and start OAS Services.



Start NodeManager task should be run on the secondary nodes of the OAS cluster, e.g., oas4fsdr2. Do not run on the AdminServer node.

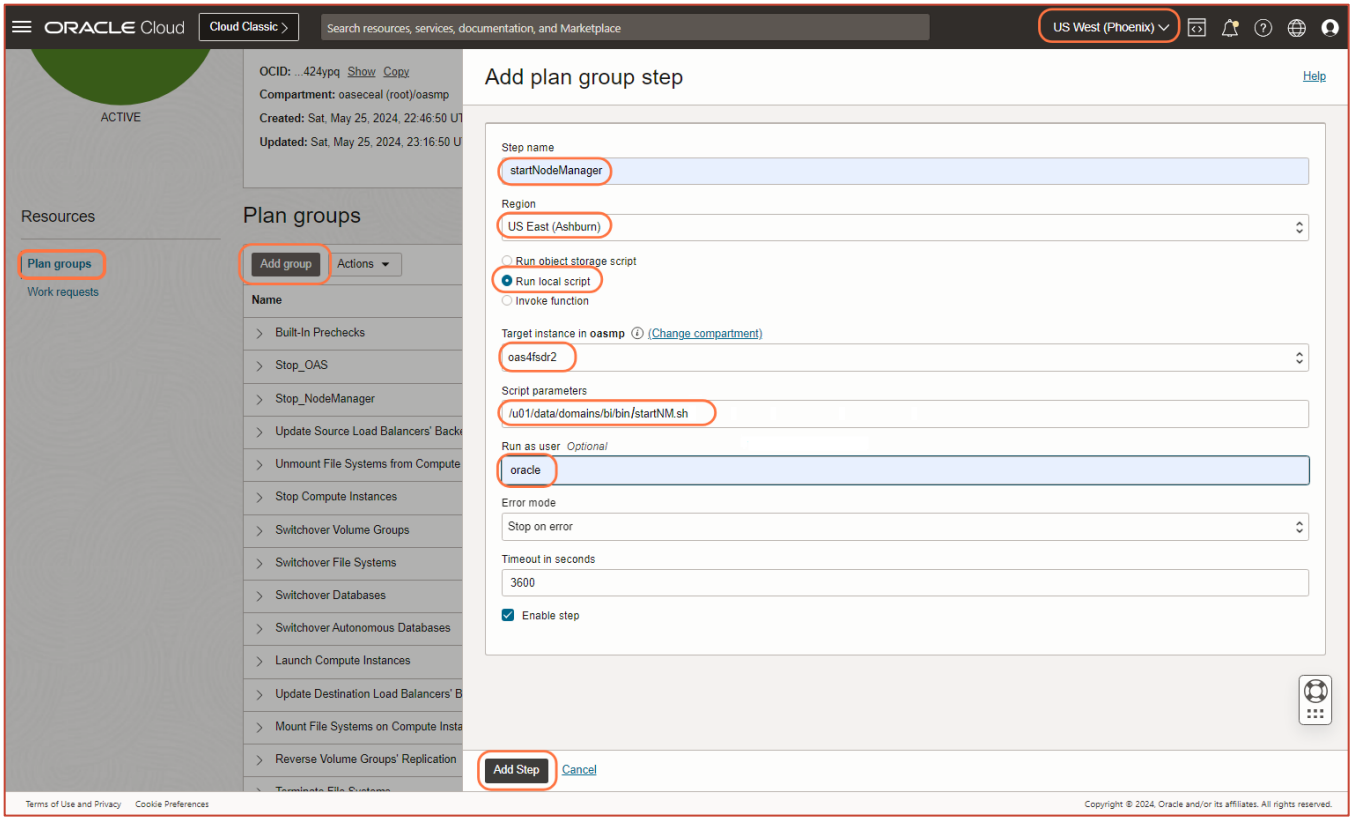
Create a script startNM.sh (`/u01/data/domains/bi/bin/startNM.sh`) with the below commands in all the secondary nodes of the OAS cluster.

startNM.sh

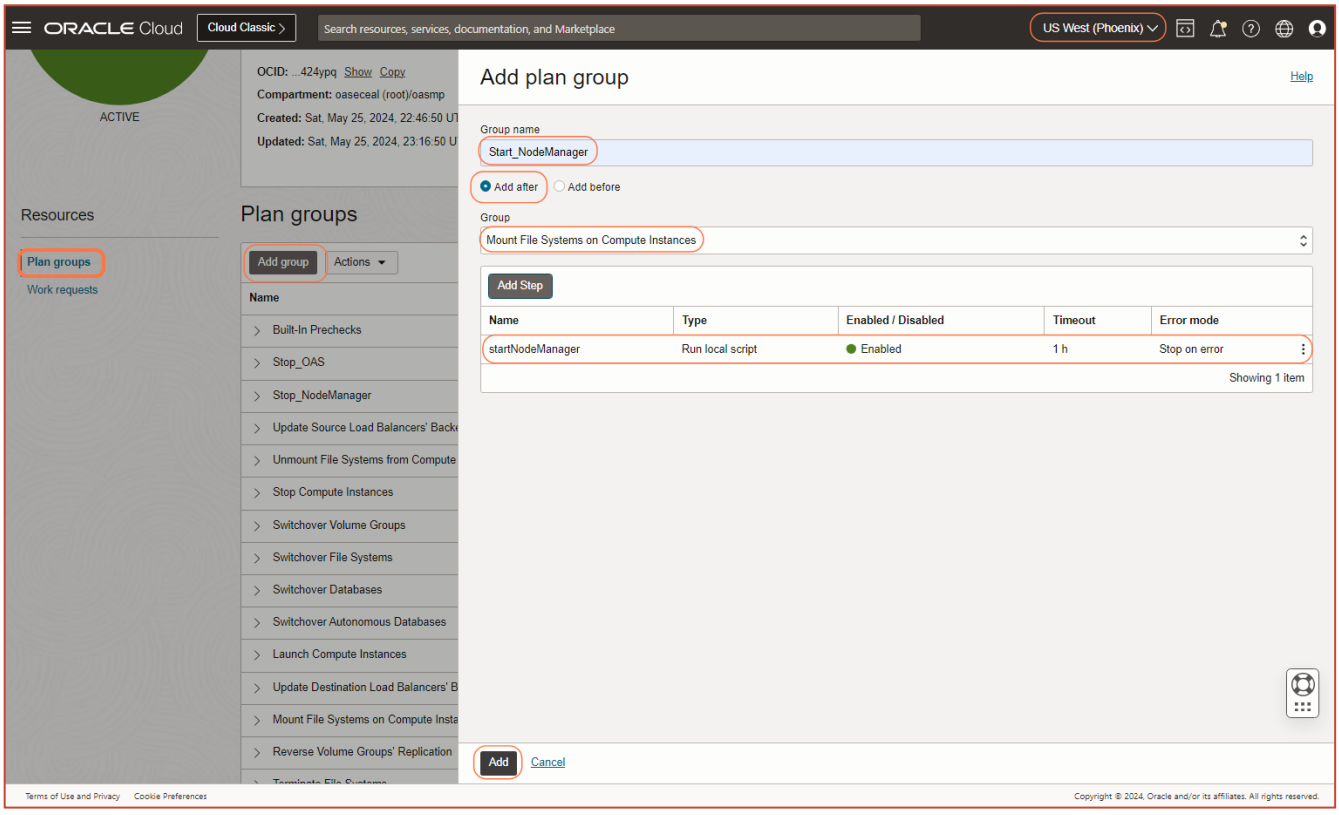
```
----------------------------------------
#!/bin/bash
cd /u01/data/domains/bi/bin
./stopNodeManager.sh
cd /u01/data/domains/bi/bin
nohup ./startNodeManager.sh &
----------------------------------------
```

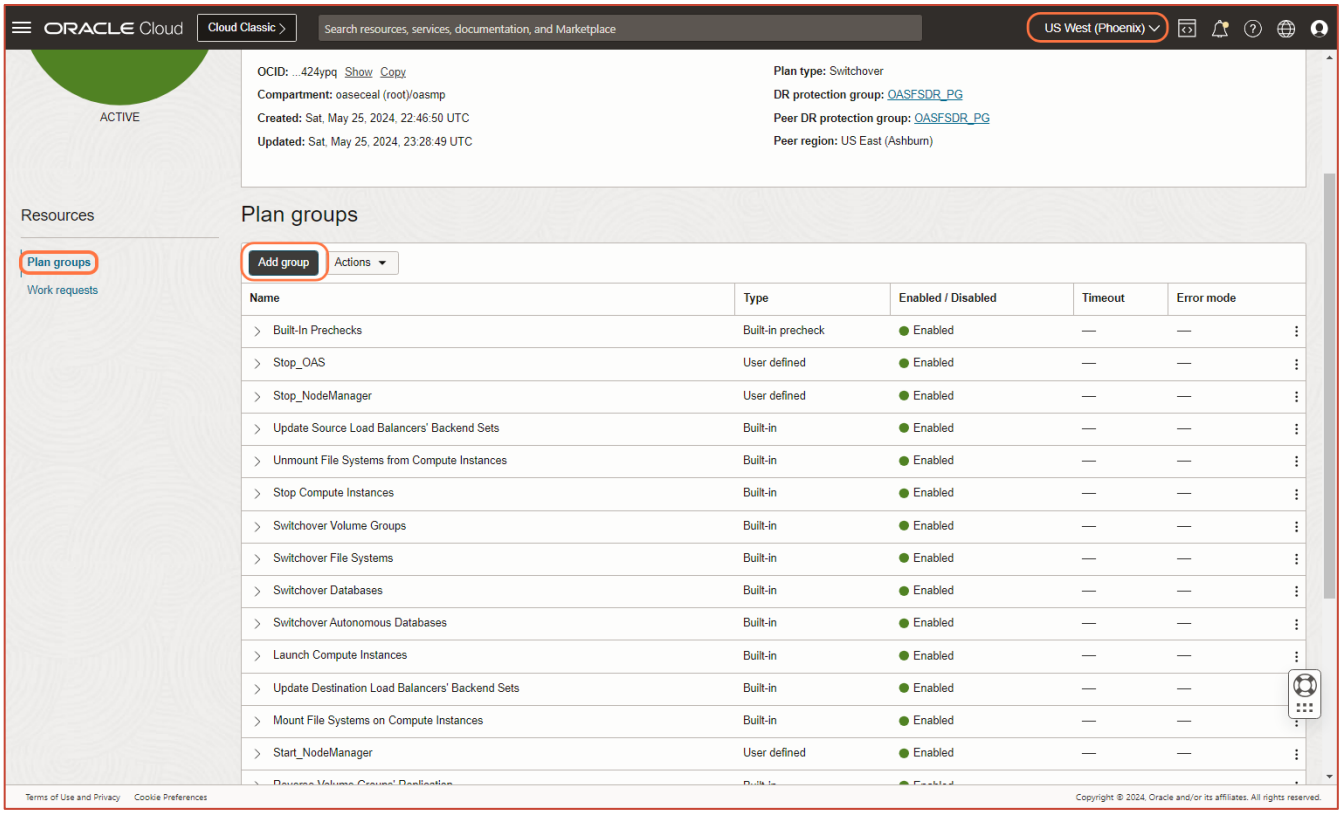
The Full Stack DR requires a script that can exit after execution for a user-defined group. The startNodemanager.sh script exits, but upon exit, the Node Manager will stop.

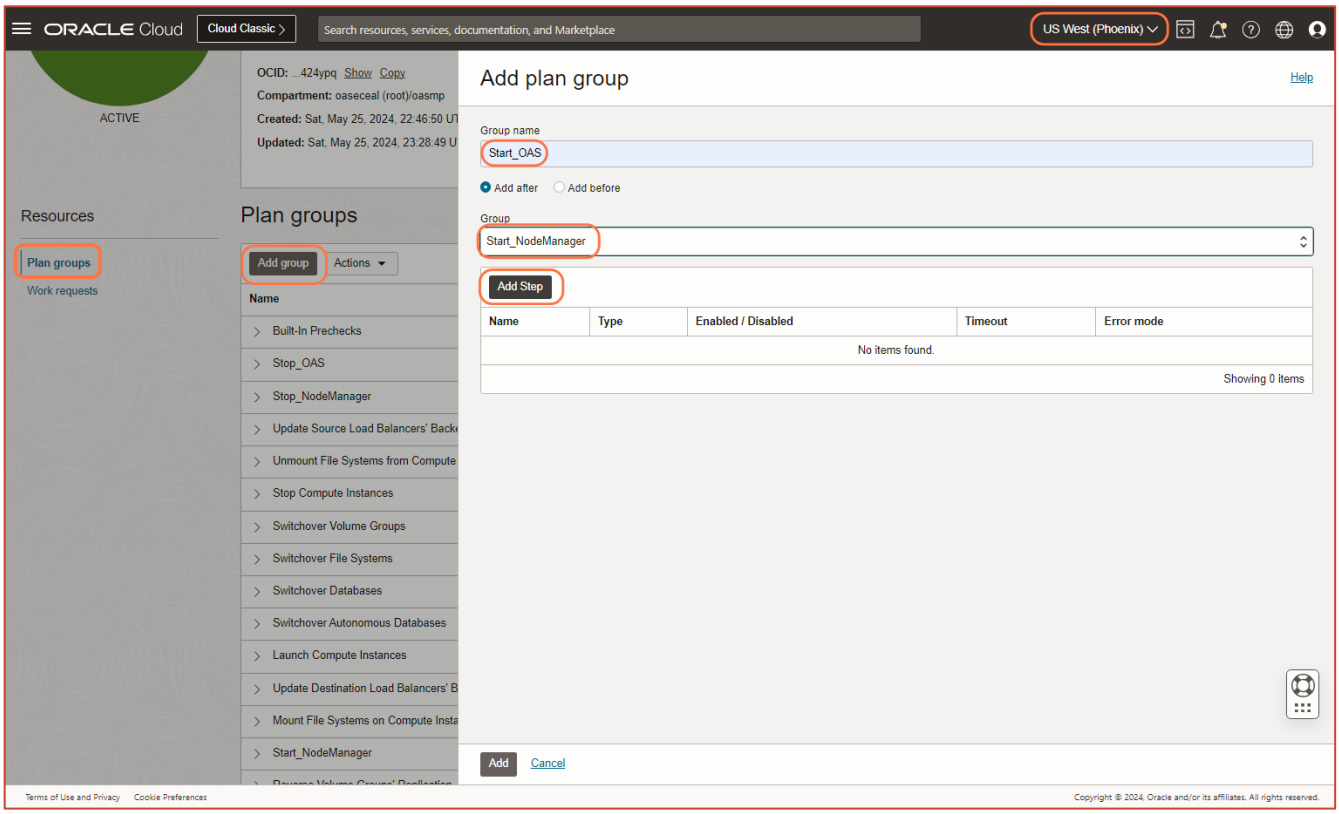
Either create the startNodeManager.sh as a service on the secondary nodes of the OAS cluster and call the *`systemctl start node-manager.service`* command in the user-defined group or create a different script `startNM.sh` as above and call it in the user-defined group.

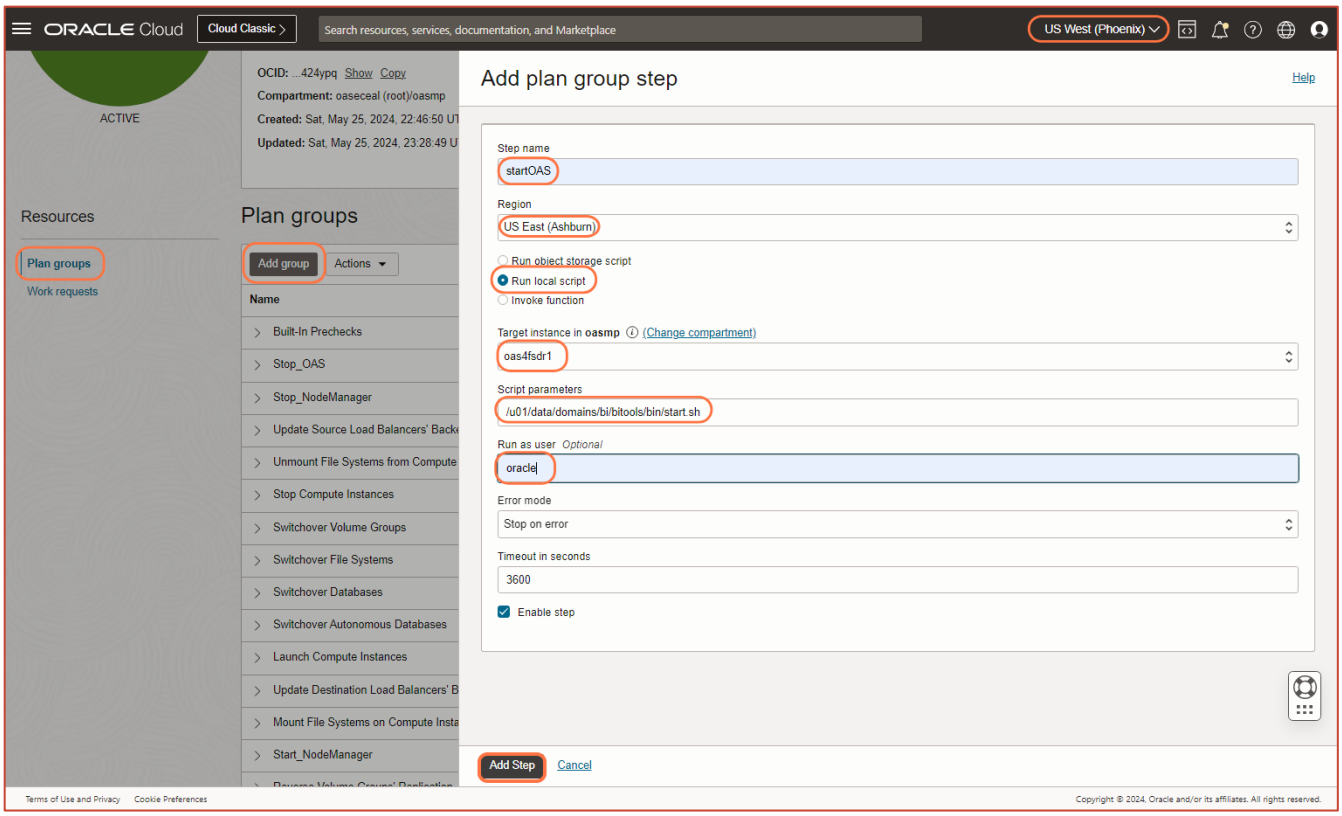


While adding the `startNM.sh` script as a user-defined group, the OAS computes in the secondary region have yet to be available, so we must select the region value as the primary OCI region. Full Stack DR manages it at runtime to execute on the OAS computes in the secondary OCI region.

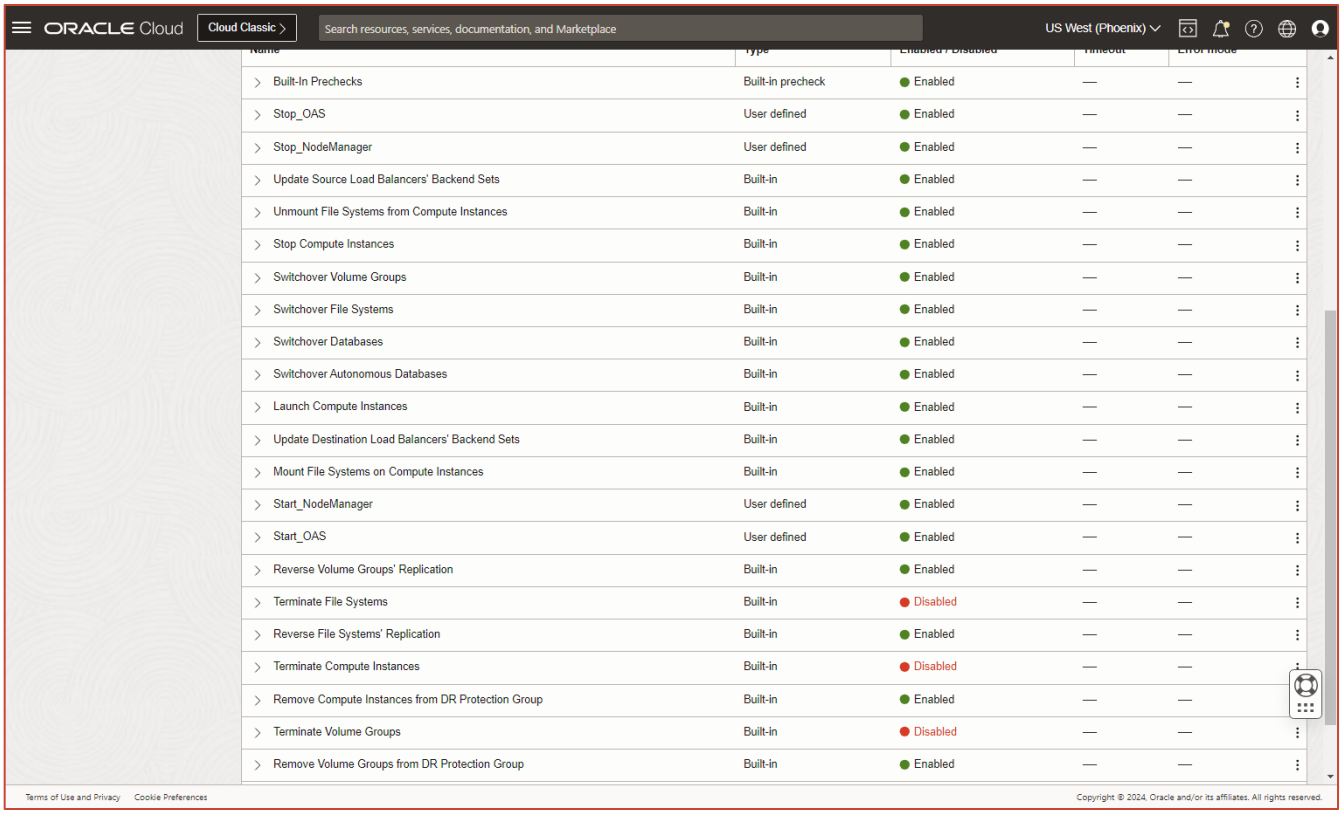






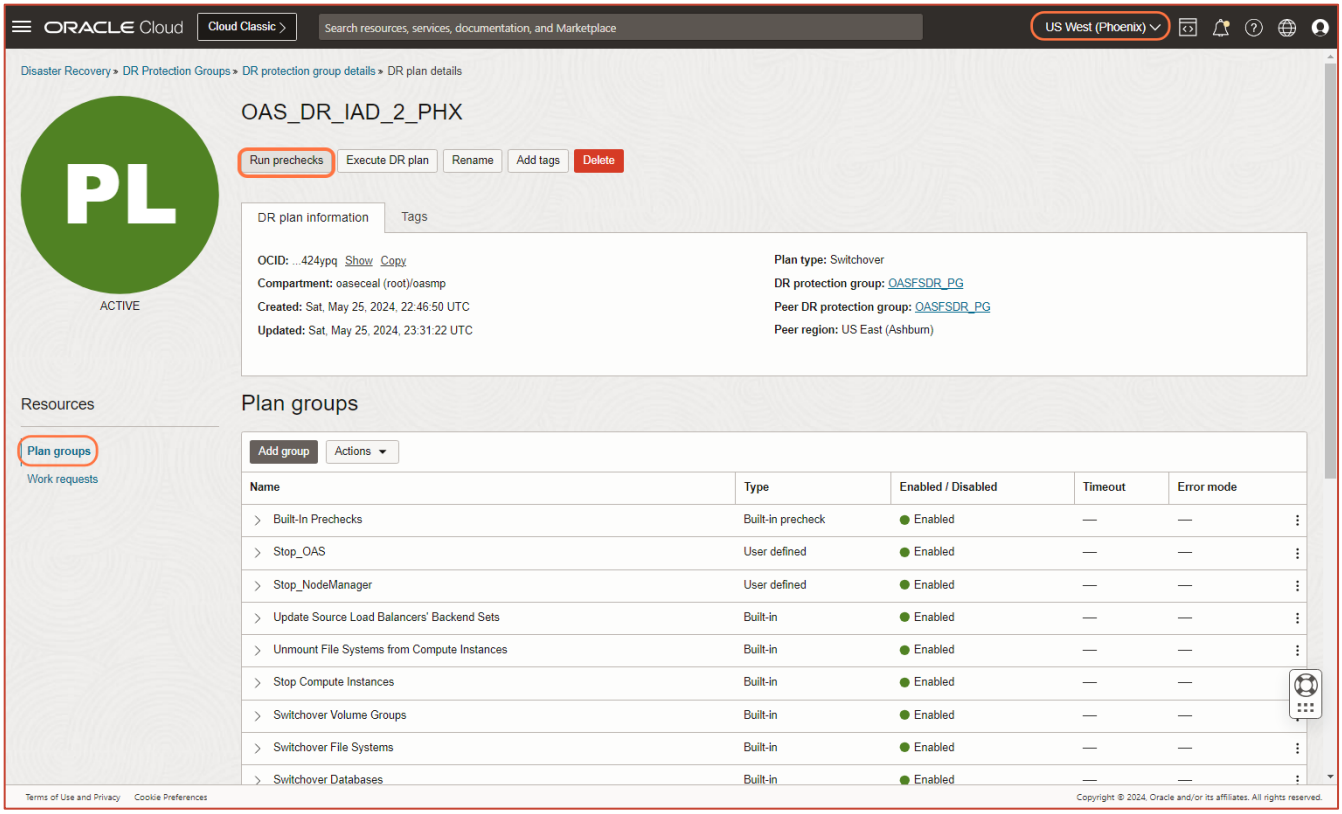


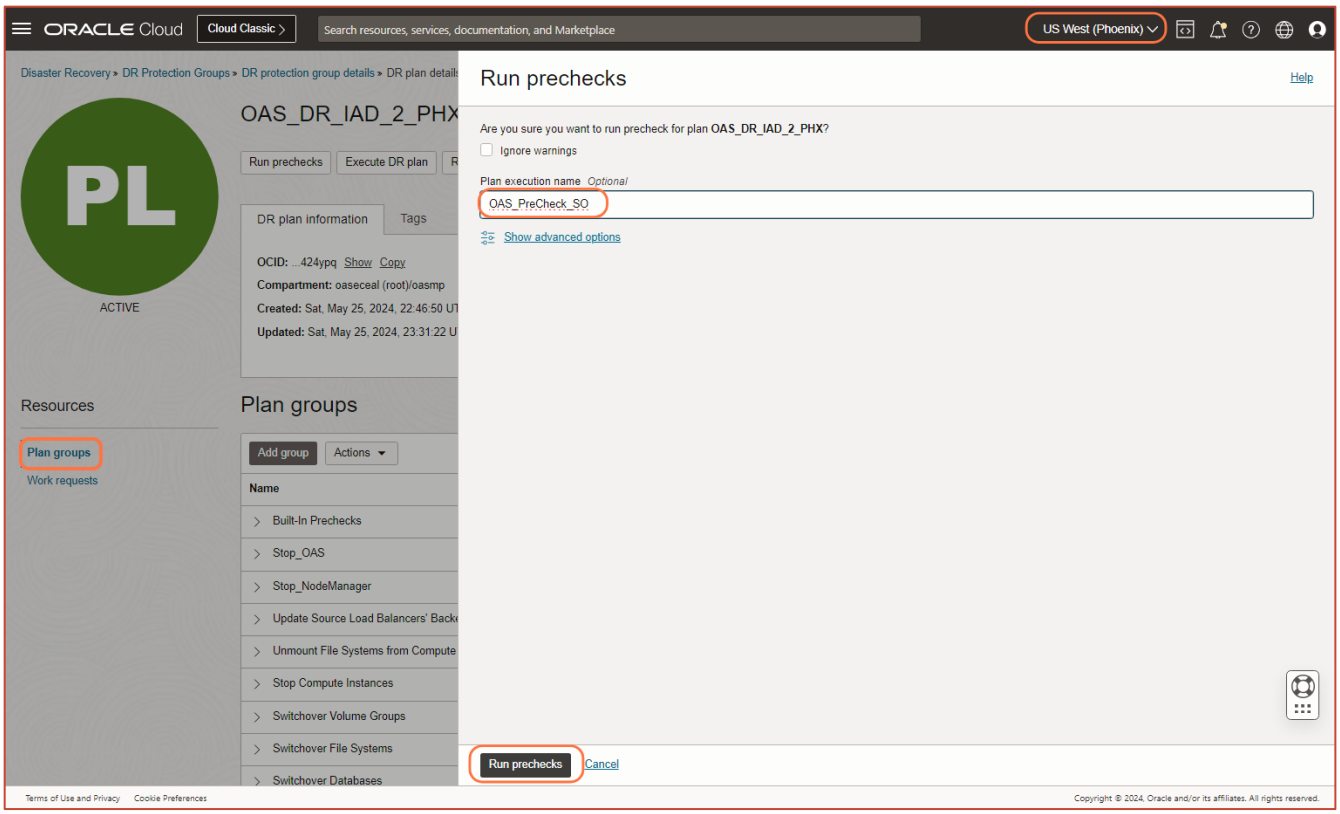
While adding the `start.sh` script as a user-defined group, the OAS computes in the secondary region have yet to be available, so we need to select the region value as the primary OCI region. Full Stack DR manages it at runtime to execute on the OAS computes in the secondary OCI region.



Enable the Disabled Groups. If you don't follow these steps, you may need to do housekeeping for the resource while falling back.

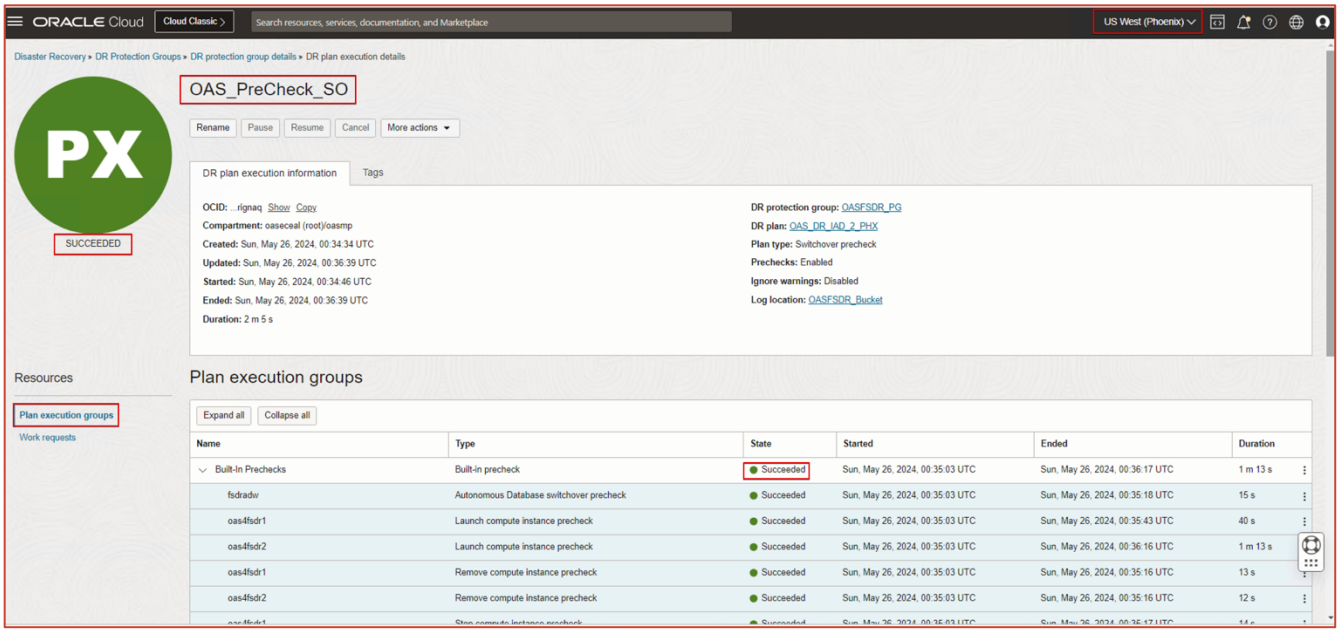
Run prechecks





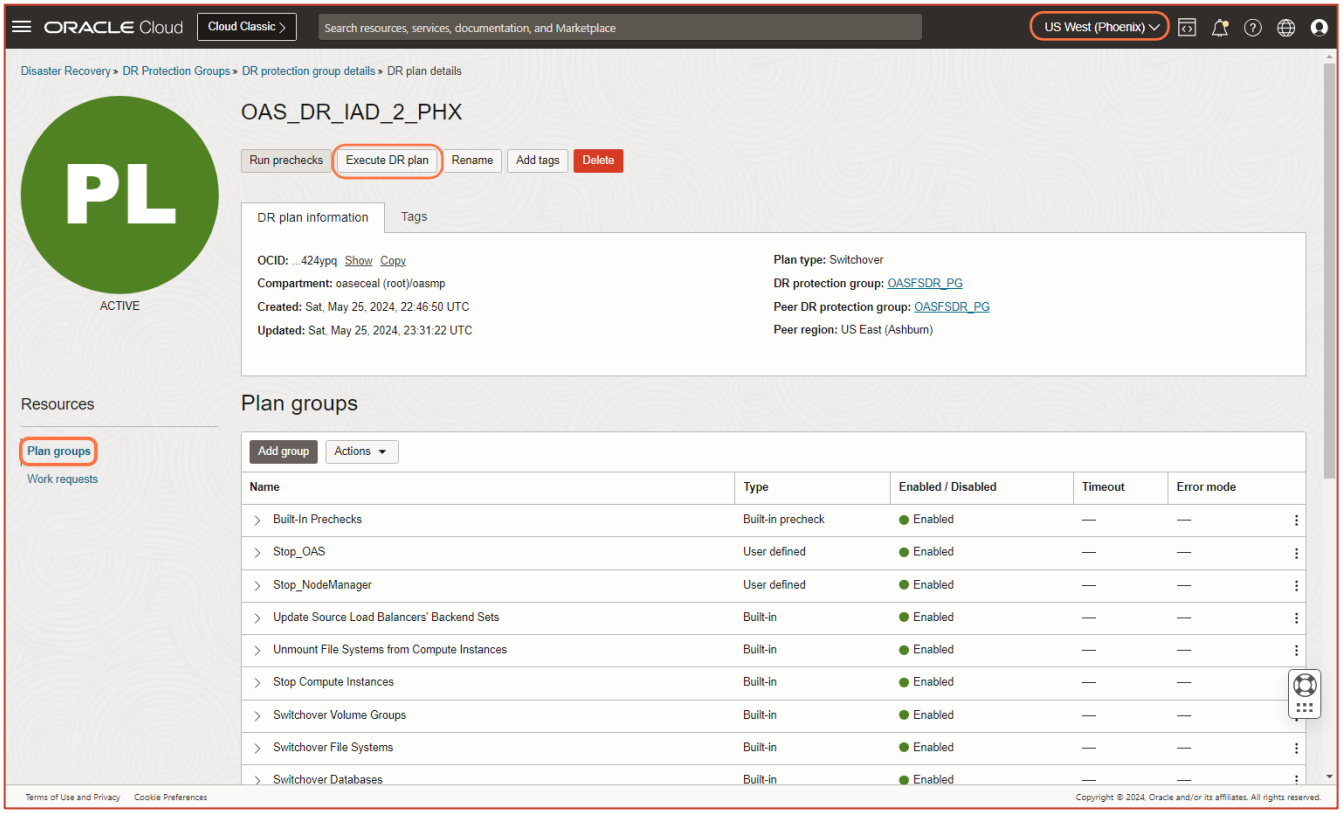
The precheck should be successful. If it fails, troubleshoot and fix the issues based on the information displayed in the precheck execution or the logs stored in the object storage bucket.

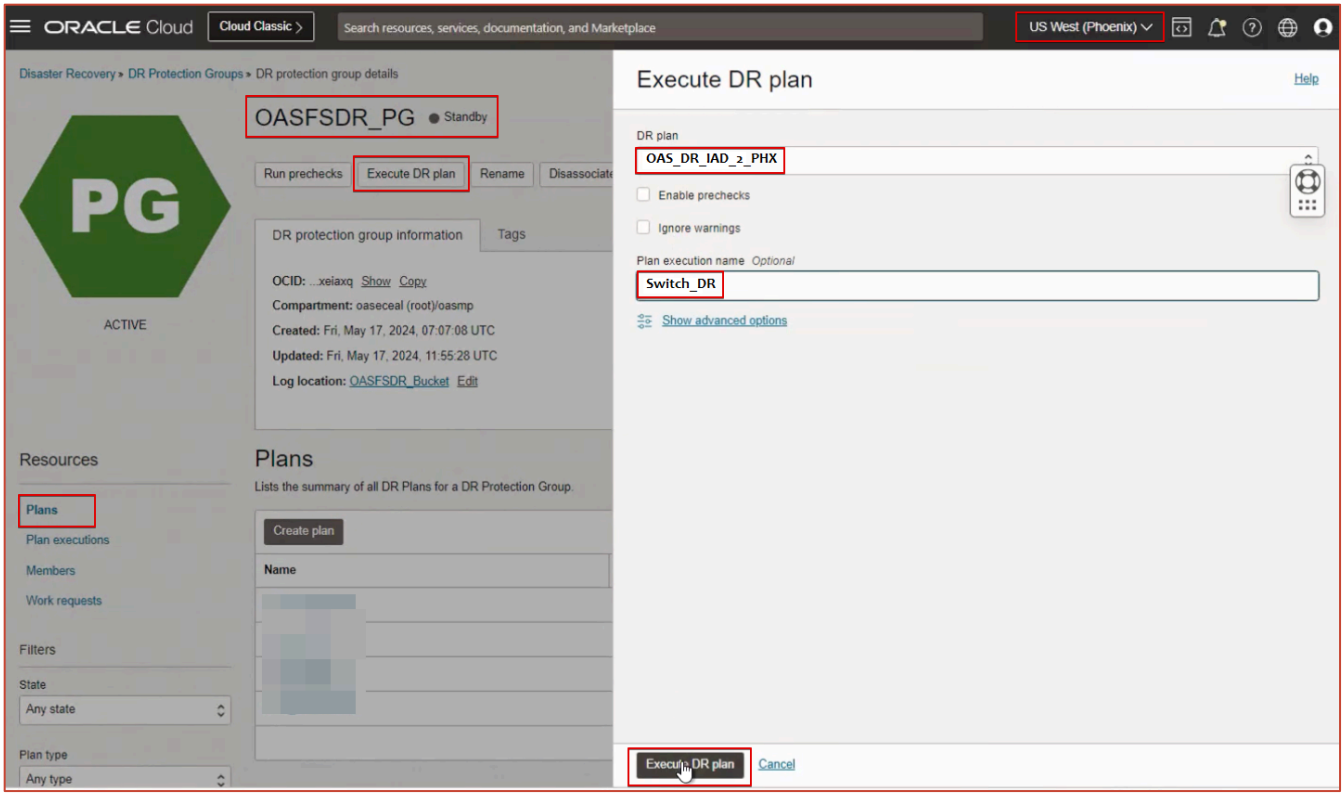
Once the precheck is successful, create a switchover plan and execute it.



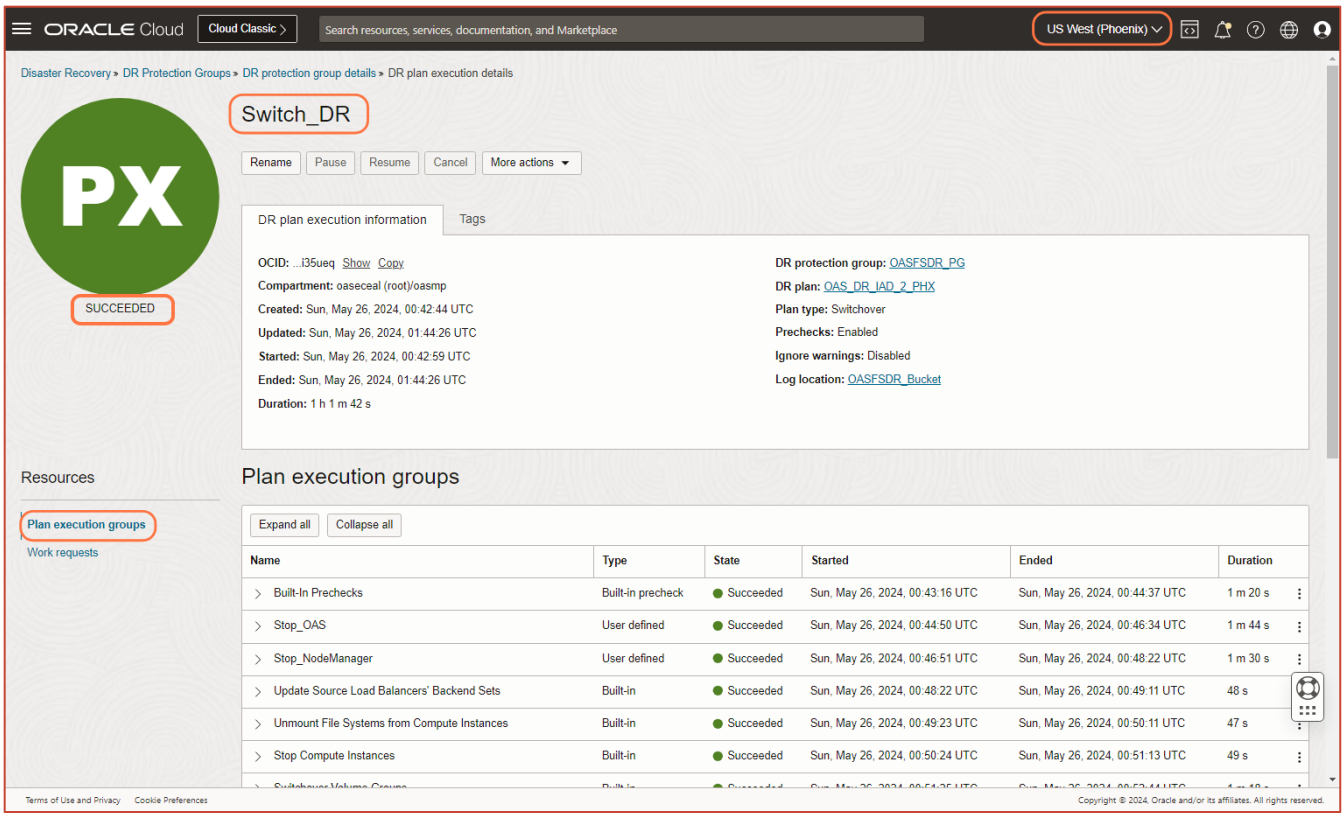
Note: You can create any Plan like (Failover, Switchover, DRDrill, etc).

Here, create a switchover plan and execute it.





The DR Plan should be successful.



During the DR Plan Execution, the following are the tasks performed by the Full Stack DR

1. User-defined task: Runs the stop OAS services command on the OAS compute instance.
2. User-defined task: Stops the Node Manager on the managed servers of the OAS cluster compute instances.
3. Unmounts the volumes and file system from the primary OAS compute instances.
4. Stops the OAS compute instances in the primary region.
5. Switchover the ADW from primary to standby instance.
6. Switchover the DBCS from primary to standby instance.
7. Using the Volume Group replication, creates the volumes added to the Volume Group.
8. Using the File System replication creates a File System in the secondary region.
9. Enable the plan group to terminate a compute instance, Volume Group, and File System, Full Stack DR will delete them in the primary region as they are redundant. By default, Full Stack DR shows them as Disabled; you can enable them.
10. Creates the OAS compute instances in the secondary region.
11. Mounts the volumes and file system in the secondary OAS compute instances.
12. User-defined: Starts the Node Manager on the managed servers of the OAS cluster compute instances.
13. User-defined: Starts the OAS services on the admin server of the OAS cluster compute instances.
14. Removes the Backends from the Backendset of the primary Load Balancer.

15. Adds the OAS compute instances in the secondary region as backends of the Backendset in the secondary Load Balancer.

After executing the Full Stack DR DR plan, you need to map the secondary region Load Balancer IP Address to the required DNS Name in your DNS Domain Management portal, such as GoDaddy.

If you have delegated your DNS domain to the OCI Zone, you can use the scripts with OCI CLI or SDKs to manage the DNS Name mapping within the OCI Zone.

What happens to the Full Stack DR Protection Group and its DR Plans?

The DR Protection Group is still active, but the DR Plan state will be inactive.

All the members added to the primary region's DR Protection Group will now be visible in the secondary region's DR Protection Group as the members like Volume Group, File System, and Compute instances are moved to the secondary region.

Now, the secondary region's OAS environment has become the primary.

The DR Protection Group in the primary OCI region, Ashburn, will now include ADW, DBCS, and Load Balancer without the Backends as members.

Fallback OAS to the primary OCI region

Considering the moved OAS environment in the secondary OCI region, e.g., Phoenix, as the primary OAS environment, create the DR Switchover Plan in the primary OCI region, i.e., Ashburn, and execute it so that the OAS and its dependencies move to the primary OCI region.

If you need to fall back your OAS environment to the primary OCI region, you need to create the DR Plan in the DR Protection Group existing in the primary OCI region and execute it using the same approach that we used to move to the secondary region.

Summary

You have understood the Full Stack Disaster Recovery feature of OCI and how to use it to orchestrate the disaster recovery of the OAS compute instances and their dependency resources, such as ADW, DBCS, Load Balancer, Block Volumes, Boot Volumes, File System, etc. Create the DR Plan type that suits your requirements and perform the DR.

The DR Plan types available in Full Stack DR include Switchover, Failover, and DR drill. The DR Drill is a simulated test case that tests all the configurations in a DR Plan instead of executing the plan on the OCI resources.

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