



# Oracle Database Deployment on AWS EC2 and FSx Best Practices

NetApp Solutions

NetApp  
July 31, 2024

# Table of Contents

- Oracle Database Deployment on AWS EC2 and FSx Best Practices ..... 1
  - WP-7357: Oracle Database Deployment on EC2 and FSx Best Practices Introduction ..... 1
  - Solution architecture ..... 1
  - Factors to consider for Oracle database deployment ..... 2
  - Step-by-Step Oracle Deployment Procedures on AWS EC2 and FSx ..... 5
  - EC2 and FSx Oracle database management ..... 30
  - Database migration from on-prem to public cloud ..... 54

# Oracle Database Deployment on AWS EC2 and FSx Best Practices

## WP-7357: Oracle Database Deployment on EC2 and FSx Best Practices Introduction

Allen Cao, Niyaz Mohamed, Jeffrey Steiner, NetApp

Many mission-critical enterprise Oracle databases are still hosted on-premises, and many enterprises are looking to migrate these Oracle databases to a public cloud. Often, these Oracle databases are application centric and thus require user-specific configurations, a capability that is missing from many database-as-a-service public-cloud offerings.

Therefore, the current database landscape calls for a public-cloud-based Oracle database solution built from a high-performance, scalable compute and storage service that can accommodate unique requirements. AWS EC2 compute instances and the AWS FSx storage service might be the missing pieces of this puzzle that you can leverage to build and migrate your mission critical Oracle database workloads to a public cloud.

Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides secure, resizable compute capacity in the cloud. It is designed to make web-scale cloud computing easier for enterprises. The simple Amazon EC2 web-service interface allows you to obtain and configure capacity with minimal friction. It provides you with complete control of your computing resources and lets you run on Amazon's proven computing environment.

Amazon FSx for ONTAP is an AWS storage service that uses industry-leading NetApp ONTAP block and file storage, which exposes NFS, SMB, and iSCSI. With such a powerful storage engine, it has never been easier to relocate mission-critical Oracle database apps to AWS with sub-millisecond response times, multiple GBps of throughput, and 100,000+ IOPS per database instance. Better yet, the FSx storage service comes with native replication capability that allows you to easily migrate your on-premises Oracle database to AWS or to replicate your mission critical Oracle database to a secondary AWS availability zone for HA or DR.

The goal of this documentation is to provide step-by-step processes, procedures, and best-practice guidance on how to deploy and configure an Oracle database with FSx storage and an EC2 instance that delivers performance similar to an on-premises system. NetApp also provides an automation toolkit that automates most of the tasks that are required for the deployment, configuration, and management of your Oracle database workload in the AWS public cloud.

To learn more about the solution and use case, take a look at following overview video:

[Modernize your Oracle database with hybrid cloud in AWS and FSx ONTAP, Part1 - Use case and solution architecture](#)

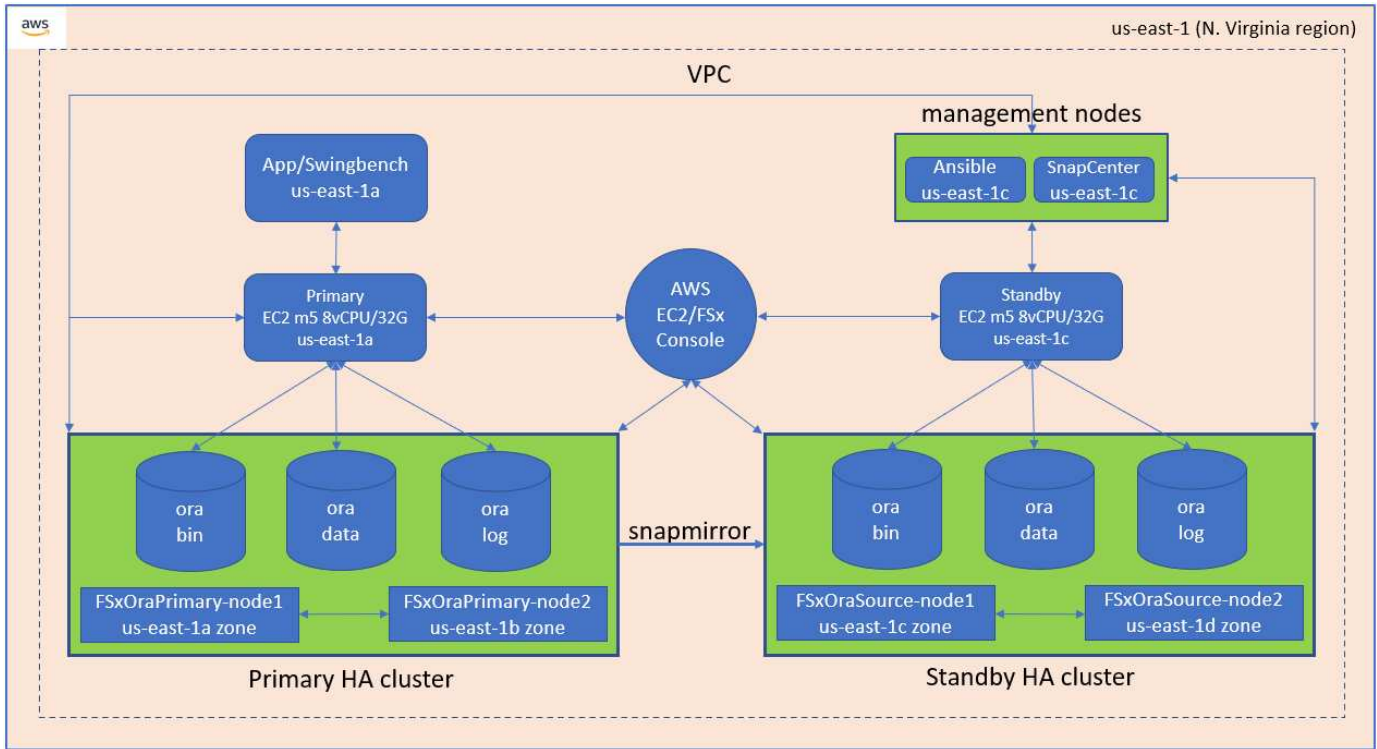
## Solution architecture

The following architecture diagram illustrates a highly available Oracle database deployment on an AWS EC2 instance with the FSx storage service. A similar deployment scheme but with the standby in a different region can be set up for disaster recovery.

Within the environment, the Oracle compute instance is deployed via an AWS EC2 instance console. There

are multiple EC2 instance types available from the console. NetApp recommends deploying a database-oriented EC2 instance type such as an m5 Ami image with RedHat enterprise Linux 8 and up to 10Gbps of network bandwidth.

Oracle database storage on FSx volumes on the other hand is deployed with the AWS FSx console or CLI. The Oracle binary, data, or log volumes are subsequently presented and mounted on an EC2 instance Linux host. Each data or log volume can have multiple LUNs allocated depending on the underlying storage protocol employed.



An FSx storage cluster is designed with double redundancy, so that both the primary and standby storage clusters are deployed in two different availability zones. Database volumes are replicated from a primary FSx cluster to a standby FSx cluster at a user-configurable interval for all Oracle binary, data, and log volumes.

This high availability Oracle environment is managed with an Ansible controller node and a SnapCenter backup server and UI tool. Oracle installation, configuration, and replication are automated using Ansible playbook-based tool kits. Any update to the Oracle EC2 instance kernel operating system or Oracle patching can be executed in parallel to keep the primary and standby in sync. In fact, the initial automation setup can be easily expanded to perform some repeating daily Oracle tasks if needed.

SnapCenter provides workflows for Oracle database point-in-time recovery or for database cloning at either the primary or standby zones if needed. Through the SnapCenter UI, you can configure Oracle database backup and replication to standby FSx storage for high availability or disaster recovery based on your RTO or RPO objectives.

The solution provides an alternative process that delivers capabilities similar to those available from Oracle RAC and Data Guard deployment.

## Factors to consider for Oracle database deployment

A public cloud provides many choices for compute and storage, and using the correct type of compute instance and storage engine is a good place to start for database

deployment. You should also select compute and storage configurations that are optimized for Oracle databases.

The following sections describe the key considerations when deploying Oracle database in an AWS public cloud on an EC2 instance with FSx storage.

## VM performance

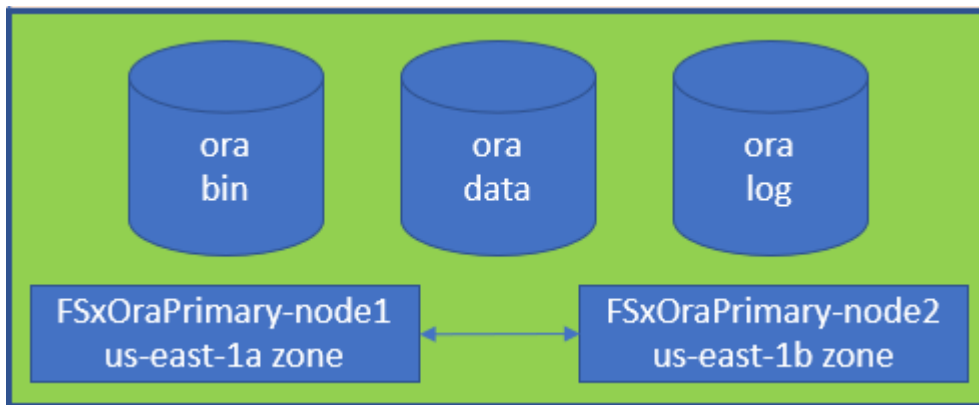
Selecting the right VM size is important for optimal performance of a relational database in a public cloud. For better performance, NetApp recommends using an EC2 M5 Series instance for Oracle deployment, which is optimized for database workloads. The same instance type is also used to power a RDS instance for Oracle by AWS.

- Choose the correct vCPU and RAM combination based on workload characteristics.
- Add swap space to a VM. The default EC2 instance deployment does not create a swap space, which is not optimal for a database.

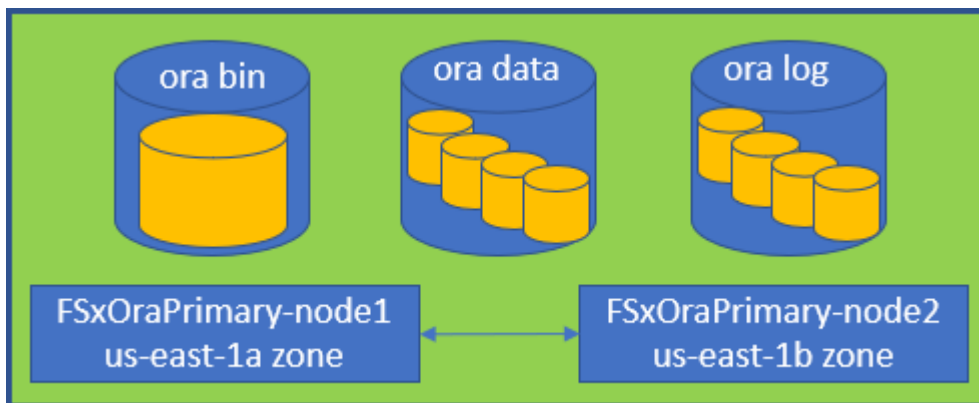
## Storage layout and settings

NetApp recommends the following storage layout:

- For NFS storage, the recommended volume layout is three volumes: one for the Oracle binary; one for Oracle data and a duplicate control file; and one for the Oracle active log, archived log, and control file.



- For iSCSI storage, the recommended volume layout is three volumes: one for the Oracle binary; one for Oracle data and a duplicate control file; and one for the Oracle active log, archived log, and control file. However, each data and log volume ideally should contain four LUNs. The LUNs are ideally balanced on the HA cluster nodes.



- For storage IOPS and throughput, you can choose the threshold for provisioned IOPS and throughput for the FSx storage cluster, and these parameters can be adjusted on the fly anytime the workload changes.
  - The auto IOPS setting is three IOPS per GiB of allocated storage capacity or user defined storage up to 80,000.
  - The throughput level is incremented as follow: 128, 256, 512, 1024, 2045 MBps.

Review the [Amazon FSx for NetApp ONTAP performance](#) documentation when sizing throughput and IOPS.

## NFS configuration

Linux, the most common operating system, includes native NFS capabilities. Oracle offers the direct NFS (dNFS) client natively integrated into Oracle. Oracle has supported NFSv3 for over 20 years. dNFS is supported with NFSv3 with all versions of Oracle. NFSv4 is supported with all OS's that follow the NFSv4 standard. dNFS support for NFSv4 requires Oracle 12.1.0.2 or higher. NFSv4.1 requires specific OS support. Consult the NetApp Interoperability Matrix Tool (IMT) for supported OS's. dNFS support for NFSv4.1 requires Oracle version 19.3.0.0 or higher.

Automated Oracle deployment using the NetApp automation toolkit automatically configures dNFS on NFSv3.

Other factors to consider:

- TCP slot tables are the NFS equivalent of host-bus-adapter (HBA) queue depth. These tables control the number of NFS operations that can be outstanding at any one time. The default value is usually 16, which is far too low for optimum performance. The opposite problem occurs on newer Linux kernels, which can automatically increase the TCP slot table limit to a level that saturates the NFS server with requests.

For optimum performance and to prevent performance problems, adjust the kernel parameters that control the TCP slot tables to 128.

```
sysctl -a | grep tcp.*.slot_table
```

- The following table provides recommended NFS mount options for Linux NFSv3 - single instance.

| File Type  | Mount Options   |
|--|---|
| <ul style="list-style-type: none"> <li>• Control files</li> <li>• Data files</li> <li>• Redo logs</li> </ul> | <code>rw,bg,hard,vers=3,proto=tcp,timeo=600,rsize=65536,wsiz=65536</code> |
| <ul style="list-style-type: none"> <li>• ORACLE_HOME</li> <li>• ORACLE_BASE</li> </ul>                       | <code>rw,bg,hard,vers=3,proto=tcp,timeo=600,rsize=65536,wsiz=65536</code> |



Before using dNFS, verify that the patches described in Oracle Doc 1495104.1 are installed. The NetApp Support matrix for NFSv3 and NFSv4 do not include specific operating systems. All OSs that obey the RFC are supported. When searching the online IMT for NFSv3 or NFSv4 support, do not select a specific OS because no matches will be displayed. All OSs are implicitly supported by the general policy.

## High availability

As indicated in the solution architecture, HA is built on storage-level replication. Therefore, the startup and availability of Oracle is contingent on how quickly the compute and storage can be brought up and recovered. See the following key factors:

- Have a standby compute instance ready and synced up with the primary through Ansible parallel update to both hosts.
- Replicate the binary volume from the primary for standby purposes so that you do not need to install Oracle at the last minute and figure out what needs to be installed and patched.
- Replication frequency dictates how fast the Oracle database can be recovered to make service available. There is a trade off between the replication frequency and storage consumption.
- Leverage automation to make recovery and switch over to standby quick and free of human error. NetApp provides an automation toolkit for this purpose.

## Step-by-Step Oracle Deployment Procedures on AWS EC2 and FSx

This section describes the deployment procedures of deploying Oracle RDS custom database with FSx storage.

### Deploy an EC2 Linux instance for Oracle via EC2 console

If you are new to AWS, you first need to set up an AWS environment. The documentation tab at the AWS website landing page provides EC2 instruction links on how to deploy a Linux EC2 instance that can be used to host your Oracle database via the AWS EC2 console. The following section is a summary of these steps. For details, see the linked AWS EC2-specific documentation.

#### Setting up your AWS EC2 environment

You must create an AWS account to provision the necessary resources to run your Oracle environment on the EC2 and FSx service. The following AWS documentation provides the necessary details:

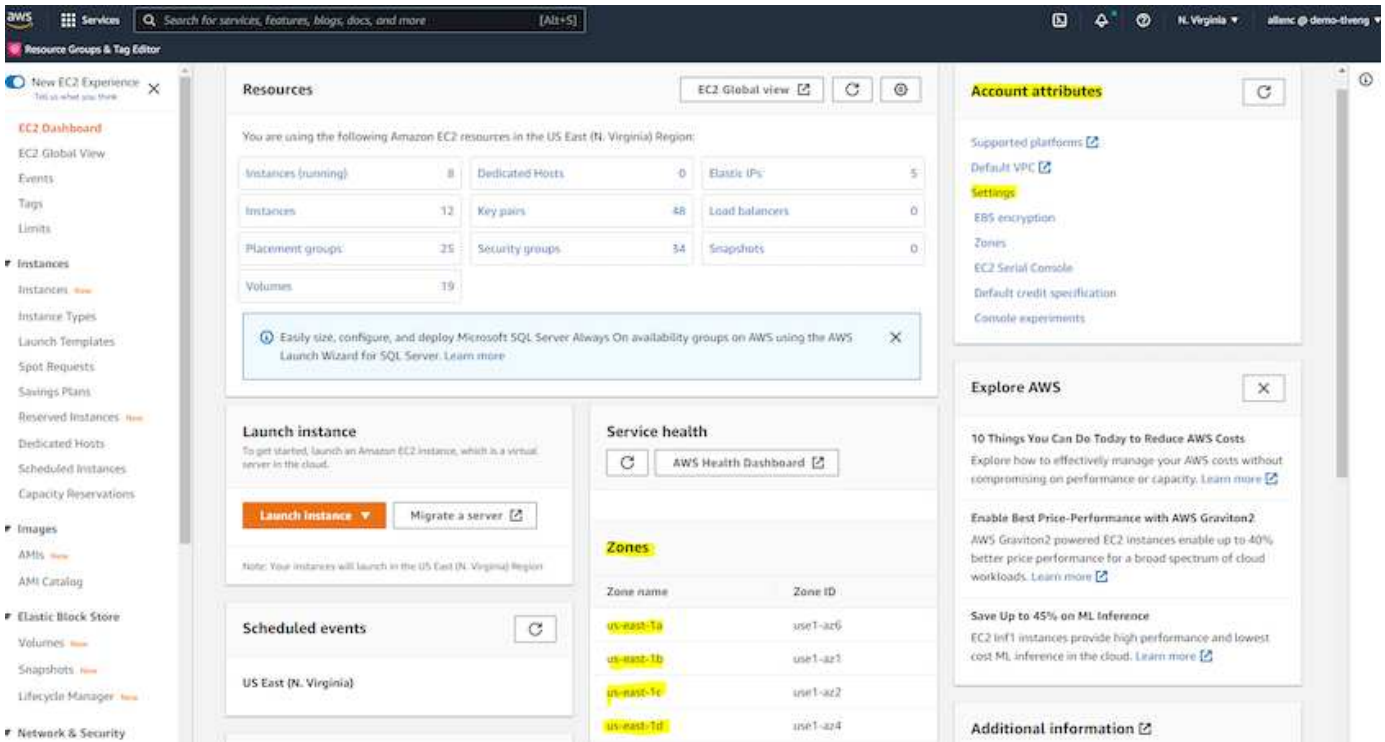
- [Set up to use Amazon EC2](#)

Key topics:

- Sign up for AWS.
- Create a key pair.
- Create a security group.

#### Enabling multiple availability zones in AWS account attributes

For an Oracle high availability configuration as demonstrated in the architecture diagram, you must enable at least four availability zones in a region. The multiple availability zones can also be situated in different regions to meet the required distances for disaster recovery.



## Creating and connecting to an EC2 instance for hosting Oracle database

See the tutorial [Get started with Amazon EC2 Linux instances](#) for step-by-step deployment procedures and best practices.

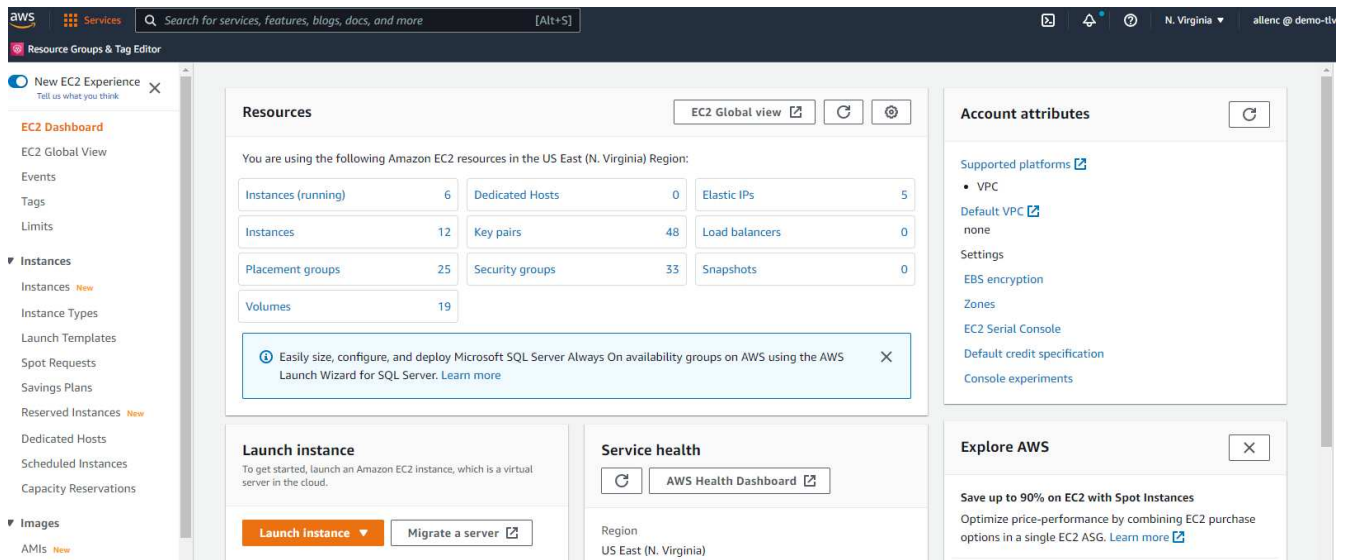
Key topics:

- Overview.
- Prerequisites.
- Step 1: Launch an instance.
- Step 2: Connect to your instance.
- Step 3: Clean up your instance.

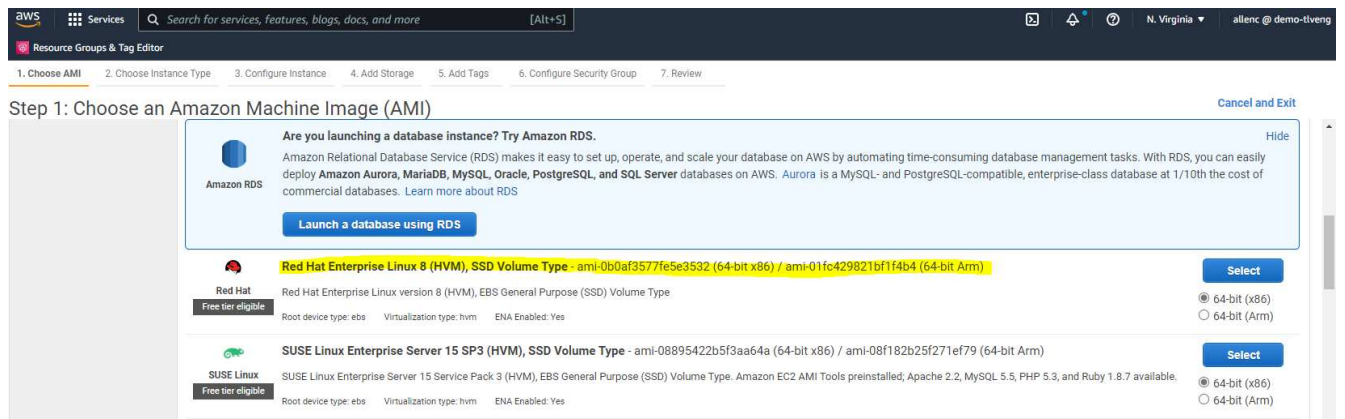
The following screen shots demonstrate the deployment of an m5-type Linux instance with the EC2 console for running Oracle.

1. From the EC2 dashboard, click the yellow Launch Instance button to start the EC2 instance deployment workflow.

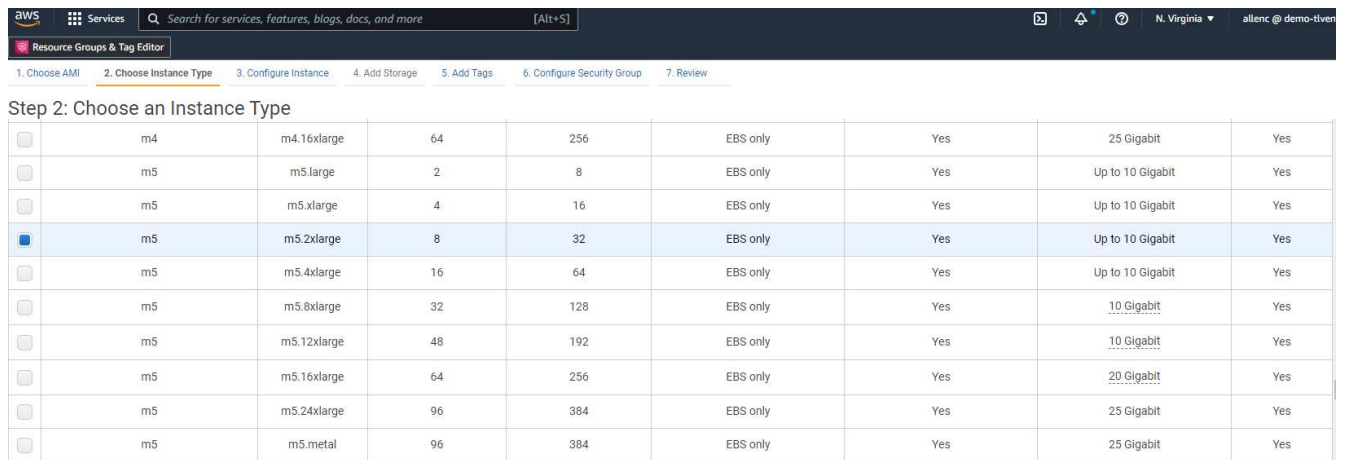




2. In Step 1, select "Red Hat Enterprise Linux 8 (HVM), SSD Volume Type - ami-0b0af3577fe5e3532 (64-bit x86) / ami-01fc429821bf1f4b4 (64-bit Arm)."



3. In Step 2, select an m5 instance type with the appropriate CPU and memory allocation based on your Oracle database workload. Click "Next: Configure Instance Details."



4. In Step 3, choose the VPC and subnet where the instance should be placed and enable public IP assignment. Click "Next: Add Storage."

Step 3: Configure Instance Details

No default VPC found. Select another VPC, or create a new default VPC.

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of instances: 1 [Launch into Auto Scaling Group](#)

Purchasing option:  Request Spot instances

Network: **vpc-0474064fc537e5182** [Create new VPC](#)  
No default VPC found. Create a new default VPC.

Subnet: **subnet-08c952541f4ab282d | us-east-1a** [Create new subnet](#)  
250 IP Addresses available

Auto-assign Public IP: **Enable**

Hostname type: Use subnet setting (IP name)

DNS Hostname:  Enable IP name IPv4 (A record) DNS requests  
 Enable resource-based IPv4 (A record) DNS requests  
 Enable resource-based IPv6 (AAAA record) DNS requests

Placement group:  Add instance to placement group

Capacity Reservation: Open

Domain join directory: No directory [Create new directory](#)

IAM role: None [Create new IAM role](#)

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Add Storage](#)

- In Step 4, allocate enough space for the root disk. You may need the space to add a swap. By default, EC2 instance assign zero swap space, which is not optimal for running Oracle.

Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. [Learn more about storage options in Amazon EC2.](#)

| Volume Type | Device    | Snapshot               | Size (GiB) | Volume Type               | IOPS       | Throughput (MB/s) | Delete on Termination               | Encryption    |
|-------------|-----------|------------------------|------------|---------------------------|------------|-------------------|-------------------------------------|---------------|
| Root        | /dev/sda1 | snap-03a3ad00558b4d17c | 50         | General Purpose SSD (gp2) | 150 / 3000 | N/A               | <input checked="" type="checkbox"/> | Not Encrypted |

[Add New Volume](#)

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. [Learn more](#) about free usage tier eligibility and usage restrictions.

Shared file systems

You currently don't have any file systems on this instance. Select "Add file system" button below to add a file system.

[Add file system](#)

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Add Tags](#)

- In Step 5, add a tag for instance identification if needed.

aws Services Search for services, features, blogs, docs, and more [Alt+S]

Resource Groups & Tag Editor

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

### Step 5: Add Tags

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webservers.  
A copy of a tag can be applied to volumes, instances or both.  
Tags will be applied to all instances and volumes. [Learn more](#) about tagging your Amazon EC2 resources.

Key (128 characters maximum) Value (256 characters maximum) Instances Volumes Network Interfaces

This resource currently has no tags.

Choose the Add tag button or click to add a Name tag.  
Make sure your IAM policy includes permissions to create tags.

Add Tag (Up to 50 tags maximum)

Cancel Previous Review and Launch Next: Configure Security Group

7. In Step 6, select an existing security group or create a new one with the desired inbound and outbound policy for the instance.

aws Services Search for services, features, blogs, docs, and more [Alt+S]

Resource Groups & Tag Editor

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

### Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more](#) about Amazon EC2 security groups.

Assign a security group:  Create a new security group  
 Select an existing security group

| Security Group ID  | Name  | Description  | Actions     |
|--|---|--|-------------|
| <input type="checkbox"/> sg-0d746a908b897c48             | AviOCCM03112021OCCM1635951256631-OCCMSecurityGroup-B3QFHUJRUUVW | NetApp OCCM Instance External Security Group                 | Copy to new |
| <input type="checkbox"/> sg-07b0625cd544aee16            | AviOCCM0311OCCM1635943382952-OCCMSecurityGroup-1L8D4QX2S945     | NetApp OCCM Instance External Security Group                 | Copy to new |
| <input type="checkbox"/> sg-0618122caef6c50e9            | AviOCCM1103OCCM1635944222133-OCCMSecurityGroup-DX5PHX6CKVKC     | NetApp OCCM Instance External Security Group                 | Copy to new |
| <input type="checkbox"/> sg-0d63ea8c78987e660            | AviOCCM1209OCCM1631452667252-OCCMSecurityGroup-T5KVZ1Q4SH48     | NetApp OCCM Instance External Security Group                 | Copy to new |
| <input type="checkbox"/> sg-0aed9f8836b48c52d            | AviOCCMFSXOCCM1638110371156-OCCMSecurityGroup-N0ENZJW3TVYB      | NetApp OCCM Instance External Security Group                 | Copy to new |
| <input type="checkbox"/> sg-083a6ea5cba912375            | connector01OCCM1631455604110-OCCMSecurityGroup-1790QV45PH32W    | NetApp OCCM Instance External Security Group                 | Copy to new |
| <input checked="" type="checkbox"/> sg-08148ca915189ac87 | default   | default VPC security group                                   | Copy to new |
| <input type="checkbox"/> sg-07f6c527620e3bb22            | fsx02OCCM1633339531669-OCCMSecurityGroup-1XZYC5WM15NP7          | NetApp OCCM Instance External Security Group                 | Copy to new |
| <input type="checkbox"/> sg-0f359d2ba38db749f            | SG-Version10-0CEc6MES-NetAppExternalSecurityGroup-N8B50GKTK58U  | ONTAP Cloud firewall rules for management and data interface | Copy to new |

Inbound rules for sg-08148ca915189ac87 (Selected security groups: sg-08148ca915189ac87)

| Type        | Protocol | Port Range | Source                         | Description |
|-------------|----------|------------|--------------------------------|-------------|
| All traffic | All      | All        | 192.168.1.0/24                 |             |
| All traffic | All      | All        | sg-08148ca915189ac87 (default) |             |

Cancel Previous Review and Launch

8. In Step 7, review the instance configuration summary, and click Launch to start instance deployment. You are prompted to create a key pair or select a key pair for access to the instance.

Step 7: Review Instance Launch

Please review your instance launch details. You can go back to edit changes for each section. Click **Launch** to assign a key pair to your instance and complete the launch process.

AMI Details Edit AMI

**Red Hat Enterprise Linux 8 (HVM), SSD Volume Type - ami-0b0af3577fe5e3532**  
 Free tier eligible Red Hat Enterprise Linux version 8 (HVM), EBS General Purpose (SSD) Volume Type  
 Root Device Type: ebs Virtualization type: hvm

Instance Type Edit instance type

| Instance Type | ECUs | vCPUs | Memory (GiB) | Instance Storage (GB) | EBS-Optimized Available | Network Performance |
|---------------|------|-------|--------------|-----------------------|-------------------------|---------------------|
| m5.2xlarge    | -    | 8     | 32           | EBS only              | Yes                     | Up to 10 Gigabit    |

Security Groups Edit security groups

| Security Group ID    | Name    | Description                |
|----------------------|---------|----------------------------|
| sg-08148ca915189ac87 | default | default VPC security group |

All selected security groups inbound rules

| Type        | Protocol | Port Range | Source                         | Description |
|-------------|----------|------------|--------------------------------|-------------|
| All traffic | All      | All        | 192.168.1.0/24                 |             |
| All traffic | All      | All        | sg-08148ca915189ac87 (default) |             |

Instance Details Edit instance details

Storage Edit storage

Cancel Previous **Launch**

### Select an existing key pair or create a new key pair

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance. Amazon EC2 supports ED25519 and RSA key pair types.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about [removing existing key pairs from a public AMI](#).

Choose an existing key pair

**Select a key pair**

accesststkey | RSA

I acknowledge that I have access to the corresponding private key file, and that without this file, I won't be able to log into my instance.

Cancel **Launch Instances**

- Log into EC2 instance using an SSH key pair. Make changes to your key name and instance IP address as appropriate.

```
ssh -i ora-db1v2.pem ec2-user@54.80.114.77
```

You need to create two EC2 instances as primary and standby Oracle servers in their designated availability

zone as demonstrated in the architecture diagram.

## Provision FSx for ONTAP file systems for Oracle database storage

EC2 instance deployment allocates an EBS root volume for the OS. FSx for ONTAP file systems provides Oracle database storage volumes, including the Oracle binary, data, and log volumes. The FSx storage NFS volumes can be either provisioned from the AWS FSx console or from Oracle installation, and configuration automation that allocates the volumes as the user configures in a automation parameter file.

### Creating FSx for ONTAP file systems

Referred to this documentation [Managing FSx for ONTAP file systems](#) for creating FSx for ONTAP file systems.

Key considerations:

- SSD storage capacity. Minimum 1024 GiB, maximum 192 TiB.
- Provisioned SSD IOPS. Based on workload requirements, a maximum of 80,000 SSD IOPS per file system.
- Throughput capacity.
- Set administrator fsxadmin/vsadmin password. Required for FSx configuration automation.
- Backup and maintenance. Disable automatic daily backups; database storage backup is executed through SnapCenter scheduling.
- Retrieve the SVM management IP address as well as protocol-specific access addresses from SVM details page. Required for FSx configuration automation.

The screenshot displays the AWS Management Console interface for an Amazon FSx for ONTAP file system. The console shows the following details:

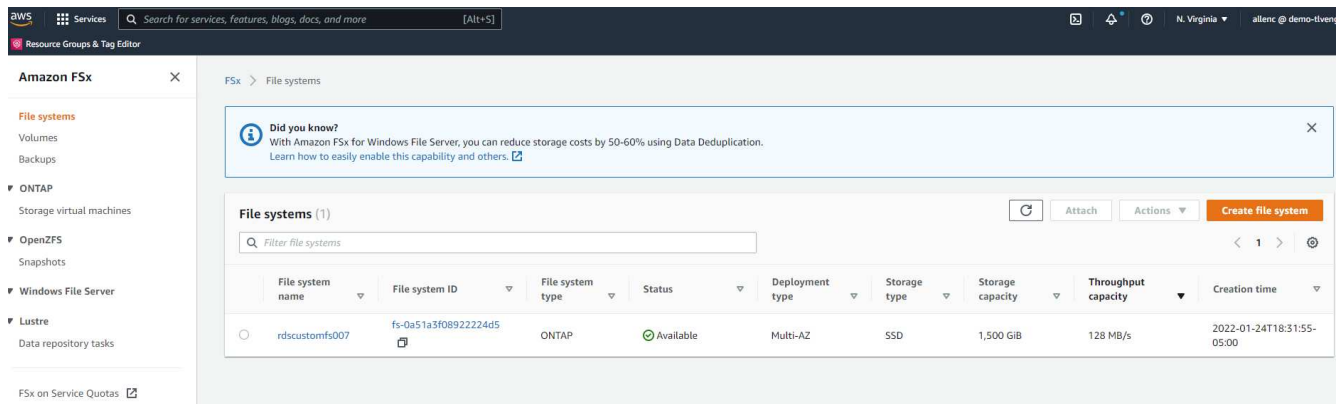
| Summary        |   |                           |
|----------------|---|---------------------------|
| SVM ID         | svm-005c6edf027866ca4   | Creation time             |
| SVM name       | fsx   | 2022-01-24T18:02:24-05:00 |
| UUID           | 1a07ea1f-7d6e-11ec-97a9-7df96ee2a64a  | Lifecycle state           |
| File system ID | fs-0a51a3f08922224d5  | Created                   |
| Resource ARN   | arn:aws:fsx:us-east-1:759995470648:storage-virtual-machine/fs-0a51a3f08922224d5/svm-005c6edf027866ca4 | Subtype                   |
|                |   | DEFAULT                   |

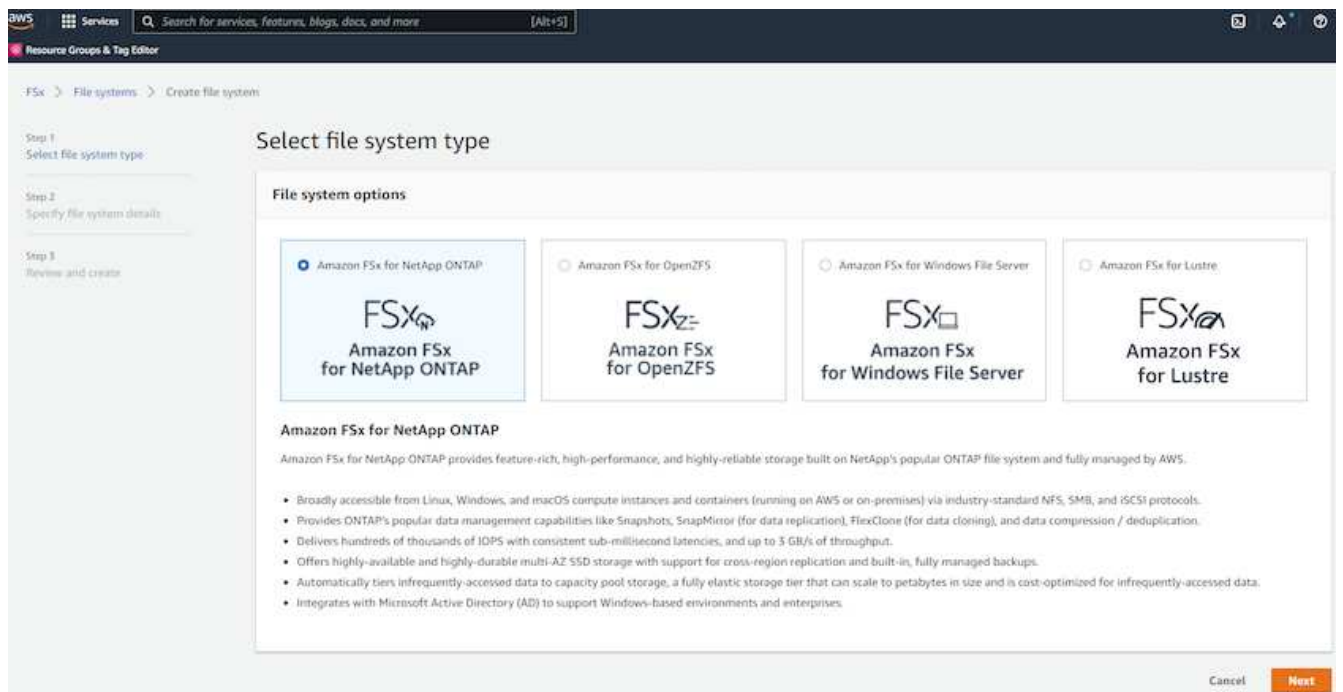
| Endpoints             |  |
|-----------------------|--|
| Management DNS name   | svm-005c6edf027866ca4.fs-0a51a3f08922224d5.fsx.us-east-1.amazonaws.com       |
| Management IP address | 198.19.255.68  |
| NFS DNS name          | svm-005c6edf027866ca4.fs-0a51a3f08922224d5.fsx.us-east-1.amazonaws.com       |
| NFS IP address        | 198.19.255.68  |
| iSCSI DNS name        | iscsi.svm-005c6edf027866ca4.fs-0a51a3f08922224d5.fsx.us-east-1.amazonaws.com |
| iSCSI IP addresses    | 10.0.1.200, 10.0.0.86  |

See the following step-by-step procedures for setting up either a primary or standby HA FSx cluster.

1. From the FSx console, click Create File System to start the FSx provision workflow.



2. Select Amazon FSx for NetApp ONTAP. Then click Next.



3. Select Standard Create and, in File System Details, name your file system, Multi-AZ HA. Based on your database workload, choose either Automatic or User-Provisioned IOPS up to 80,000 SSD IOPS. FSx storage comes with up to 2TiB NVMe caching at the backend that can deliver even higher measured IOPS.

## File system details

File system name - optional [Info](#)

Maximum of 256 Unicode letters, whitespace, and numbers, plus + - = . \_ : /

Deployment type [Info](#)

Multi-AZ

Single-AZ

SSD storage capacity [Info](#)

Minimum 1024 GiB; Maximum 192 TiB.

Provisioned SSD IOPS

Amazon FSx provides 3 IOPS per GiB of storage capacity. You can also provision additional SSD IOPS as needed.

Automatic (3 IOPS per GiB of SSD storage)

User-provisioned

Maximum 80,000 IOPS

Throughput capacity [Info](#)

The sustained speed at which the file server hosting your file system can serve data. The file server can also burst to higher speeds for periods of time.

Recommended throughput capacity

128 MB/s

Specify throughput capacity

Throughput capacity

4. In the Network & Security section, select the VPC, security group, and subnets. These should be created before FSx deployment. Based on the role of the FSx cluster (primary or standby), place the FSx storage nodes in the appropriate zones.

## Network & security

### Virtual Private Cloud (VPC) [Info](#)

Specify the VPC from which your file system is accessible.

vpc-0474064fc537e5182

### VPC Security Groups [Info](#)

Specify VPC Security Groups to associate with your file system's network interfaces.

Choose VPC security group(s)

sg-08148ca915189ac87 (default) X

### Preferred subnet [Info](#)

Specify the preferred subnet for your file system.

subnet-08c952541f4ab282d (us-east-1a)

### Standby subnet

subnet-0a84d6eeeb0f4e5c0 (us-east-1b)

### VPC route tables

Specify the VPC route tables associated with your file system.

- VPC's default route table
- Select one or more VPC route tables

### Endpoint IP address range

Specify the IP address range in which the endpoints to access your file system will be created

- No preference
- Select an IP address range

5. In the Security & Encryption section, accept the default, and enter the fsxadmin password.

## Security & encryption

### Encryption key [Info](#)

AWS Key Management Service (KMS) encryption key that protects your file system data at rest.

aws/fsx (default)

| Description  | Account      | KMS key ID                           |
|--|--------------|--------------------------------------|
| Default master key that protects my FSx resources when no other key is defined | 759995470648 | 5b31feff-6759-4306-a852-9c99a743982a |

### File system administrative password

Password for this file system's "fsxadmin" user, which you can use to access the ONTAP CLI or REST API.

- Don't specify a password
- Specify a password

Password

Confirm password



6. Enter the SVM name and the vsadmin password.

### Default storage virtual machine configuration

Storage virtual machine name

SVM administrative password  
Password for this SVM's "vsadmin" user, which you can use to access the ONTAP CLI or REST API.

Don't specify a password

Specify a password

Password

Confirm password

Active Directory  
Joining an Active Directory enables access from Windows and MacOS clients over the SMB protocol.

Do not join an Active Directory

Join an Active Directory

7. Leave the volume configuration blank; you do not need to create a volume at this point.

**Default volume configuration**

Volume name  
  
Maximum of 203 alphanumeric characters, plus \_.

Junction path  
  
The location within your file system where your volume will be mounted.

Volume size  
  
Minimum 20 MiB; Maximum 104857600 MiB

Storage efficiency  
Select whether you would like to enable ONTAP storage efficiencies on your volume: deduplication, compression, and compaction.

Enabled (recommended)  
 Disabled

Capacity pool tiering policy  
You can optionally enable automatic tiering of your data to lower-cost capacity pool storage.

► Backup and maintenance - *optional*

► Tags - *optional*

Cancel

8. Review the Summary page, and click Create File System to complete FSx file system provision.

aws Services Search for services, features, blogs, docs, and more [Alt+S]

Resource Groups & Tag Editor

Step 1 Select file system type

Step 2 Specify file system details

Step 3 Review and create

## Create file system

**Summary**  
Verify the following attributes before proceeding

| Attribute                     | Value   | Editable after creation |
|-------------------------------|---|-------------------------|
| File system type              | Amazon FSx for NetApp ONTAP   |                         |
| File system name              | aws_ora_prod  | ✓                       |
| Deployment type               | Multi-AZ  |                         |
| Storage type                  | SSD   |                         |
| SSD storage capacity          | 1,024 GiB   | ✓                       |
| Minimum SSD IOPS              | 40000 IOPS  | ✓                       |
| Throughput capacity           | 512 MB/s  | ✓                       |
| Virtual Private Cloud (VPC)   | vpc-0474064fc537e5182   |                         |
| VPC Security Groups           | sg-08148ca915189ac87  | ✓                       |
| Preferred subnet              | subnet-08c952541f4ab282d  |                         |
| Standby subnet                | subnet-0a84d6eeeb0f4e5c0  |                         |
| VPC route tables              | VPC's default route table   |                         |
| Endpoint IP address range     | No preference   |                         |
| KMS key ID                    | arn:aws:kms:us-east-1:759995470648:key/5b31feff-6759-4306-a852-9c99a743982a |                         |
| Daily automatic backup window | No preference   | ✓                       |
| Automatic backup              | 7 day(s)  | ✓                       |

## Provisioning of database volumes for Oracle database

See [Managing FSx for ONTAP volumes - creating a volume](#) for details.

Key considerations:

- Sizing the database volumes appropriately.
- Disabling capacity pool tiering policy for performance configuration.
- Enabling Oracle dNFS for NFS storage volumes.
- Setting up multipath for iSCSI storage volumes.

### Create database volume from FSx console

From the AWS FSx console, you can create three volumes for Oracle database file storage: one for the Oracle binary, one for the Oracle data, and one for the Oracle log. Make sure that volume naming matches the Oracle host name (defined in the hosts file in the automation toolkit) for proper identification. In this example, we use db1 as the EC2 Oracle host name instead of a typical IP-address-based host name for an EC2 instance.

## Create volume



### File system

ONTAP | fs-0a51a3f08922224d5 | rdscustomfs007



### Storage virtual machine

svm-005c6edf027866ca4 | fsx



### Volume name

db1\_bin

Maximum of 203 alphanumeric characters, plus \_.

### Junction path

/db1\_bin

The location within your file system where your volume will be mounted.

### Volume size

51200

Minimum 20 MiB; Maximum 104857600 MiB

### Storage efficiency

Select whether you would like to enable ONTAP storage efficiencies on your volume: deduplication, compression, and compaction.

- Enabled (recommended)
- Disabled

### Capacity pool tiering policy

You can optionally enable automatic tiering of your data to lower-cost capacity pool storage.

None



Cancel

Confirm

## Create volume



### File system

ONTAP | fs-0a51a3f08922224d5 | rdscustomfs007



### Storage virtual machine

svm-005c6edf027866ca4 | fsx



### Volume name

db1\_data

Maximum of 203 alphanumeric characters, plus \_ .

### Junction path

/db1\_data

The location within your file system where your volume will be mounted.

### Volume size

512000

Minimum 20 MiB; Maximum 104857600 MiB

### Storage efficiency

Select whether you would like to enable ONTAP storage efficiencies on your volume: deduplication, compression, and compaction.

- Enabled (recommended)
- Disabled

### Capacity pool tiering policy

You can optionally enable automatic tiering of your data to lower-cost capacity pool storage.

None



Cancel

Confirm

**Create volume**
✕

---

**File system**

ONTAP | fs-0a51a3f08922224d5 | rdscustomfs007 ▼

**Storage virtual machine**

svm-005c6edf027866ca4 | fsx ▼

**Volume name**

db1\_log

Maximum of 203 alphanumeric characters, plus \_.

**Junction path**

/db1\_log

The location within your file system where your volume will be mounted.

**Volume size**

256000

Minimum 20 MiB; Maximum 104857600 MiB

**Storage efficiency**

Select whether you would like to enable ONTAP storage efficiencies on your volume: deduplication, compression, and compaction.

Enabled (recommended)
   
 Disabled

**Capacity pool tiering policy**

You can optionally enable automatic tiering of your data to lower-cost capacity pool storage.

None ▼

Cancel
Confirm



Creating iSCSI LUNs is not currently supported by the FSx console. For iSCSI LUNs deployment for Oracle, the volumes and LUNs can be created by using automation for ONTAP with the NetApp Automation Toolkit.

## Install and configure Oracle on an EC2 instance with FSx database volumes

The NetApp automation team provide an automation kit to run Oracle installation and configuration on EC2 instances according to best practices. The current version of the automation kit supports Oracle 19c on NFS with the default RU patch 19.8. The automation kit can be easily adapted for other RU patches if needed.

## Prepare a Ansible controller to run automation

Follow the instruction in the section "[Creating and connecting to an EC2 instance for hosting Oracle database](#)" to provision a small EC2 Linux instance to run the Ansible controller. Rather than using RedHat, Amazon Linux t2.large with 2vCPU and 8G RAM should be sufficient.

## Retrieve NetApp Oracle deployment automation toolkit

Log into the EC2 Ansible controller instance provisioned from step 1 as ec2-user and from the ec2-user home directory, execute the `git clone` command to clone a copy of the automation code.

```
git clone https://github.com/NetApp-Automation/na_oracle19c_deploy.git
```

```
git clone https://github.com/NetApp-Automation/na_rds_fsx_oranfs_config.git
```

## Execute automated Oracle 19c deployment using automation toolkit

See these detailed instruction [CLI deployment Oracle 19c Database](#) to deploy Oracle 19c with CLI automation. There is a small change in command syntax for playbook execution because you are using an SSH key pair instead of a password for host access authentication. The following list is a high level summary:

1. By default, an EC2 instance uses an SSH key pair for access authentication. From Ansible controller automation root directories `/home/ec2-user/na_oracle19c_deploy`, and `/home/ec2-user/na_rds_fsx_oranfs_config`, make a copy of the SSH key `accesststkey.pem` for the Oracle host deployed in the step "[Creating and connecting to an EC2 instance for hosting Oracle database](#)."
2. Log into the EC2 instance DB host as `ec2-user`, and install the `python3` library.

```
sudo yum install python3
```

3. Create a 16G swap space from the root disk drive. By default, an EC2 instance creates zero swap space. Follow this AWS documentation: [How do I allocate memory to work as swap space in an Amazon EC2 instance by using a swap file?](#)
4. Return to the Ansible controller (`cd /home/ec2-user/na_rds_fsx_oranfs_config`), and execute the `preclone` playbook with the appropriate requirements and `linux_config` tags.

```
ansible-playbook -i hosts rds_preclone_config.yml -u ec2-user --private-key accesststkey.pem -e @vars/fsx_vars.yml -t requirements_config
```

```
ansible-playbook -i hosts rds_preclone_config.yml -u ec2-user --private-key accesststkey.pem -e @vars/fsx_vars.yml -t linux_config
```

5. Switch to the `/home/ec2-user/na_oracle19c_deploy-master` directory, read the `README` file, and populate the `global_vars.yml` file with the relevant global parameters.

6. Populate the `host_name.yml` file with the relevant parameters in the `host_vars` directory.
7. Execute the playbook for Linux, and press Enter when prompted for the `vsadmin` password.

```
ansible-playbook -i hosts all_playbook.yml -u ec2-user --private-key
accesststkey.pem -t linux_config -e @vars/vars.yml
```

8. Execute the playbook for Oracle, and press enter when prompted for the `vsadmin` password.

```
ansible-playbook -i hosts all_playbook.yml -u ec2-user --private-key
accesststkey.pem -t oracle_config -e @vars/vars.yml
```

Change the permission bit on the SSH key file to 400 if needed. Change the Oracle host (`ansible_host` in the `host_vars` file) IP address to your EC2 instance public address.

## Setting up SnapMirror between primary and standby FSx HA cluster

For high availability and disaster recovery, you can set up SnapMirror replication between the primary and standby FSx storage cluster. Unlike other cloud storage services, FSx enables a user to control and manage storage replication at a desired frequency and replication throughput. It also enables users to test HA/DR without any effect on availability.

The following steps show how to set up replication between a primary and standby FSx storage cluster.

1. Setup primary and standby cluster peering. Log into the primary cluster as the `fsxadmin` user and execute the following command. This reciprocal create process executes the `create` command on both the primary cluster and the standby cluster. Replace `standby_cluster_name` with the appropriate name for your environment.

```
cluster peer create -peer-addr
standby_cluster_name,inter_cluster_ip_address -username fsxadmin
-initial-allowed-vserver-peers *
```

2. Set up vServer peering between the primary and standby cluster. Log into the primary cluster as the `vsadmin` user and execute the following command. Replace `primary_vserver_name`, `standby_vserver_name`, `standby_cluster_name` with the appropriate names for your environment.

```
vserver peer create -vserver primary_vserver_name -peer-vserver
standby_vserver_name -peer-cluster standby_cluster_name -applications
snapmirror
```

3. Verify that the cluster and vserver peerings are set up correctly.



```

FsxId00164454fac5591e6::> cluster peer show
Peer Cluster Name          Cluster Serial Number Availability Authentication
-----
FsxId0b6a95149d07aa82e    1-80-000011             Available         ok

FsxId00164454fac5591e6::> vserver peer show
Vserver      Peer      Peer      Peering      Remote
Vserver      Vserver   State     Peer Cluster Applications Vserver
-----
svm_FSxOraSource
svm_FSxOraTarget
peered       FsxId0b6a95149d07aa82e
snapmirror   svm_FSxOraTarget

FsxId00164454fac5591e6::>

```

4. Create target NFS volumes at the standby FSx cluster for each source volume at the primary FSx cluster. Replace the volume name as appropriate for your environment.

```

vol create -volume dr_db1_bin -aggregate aggr1 -size 50G -state online
-policy default -type DP

```

```

vol create -volume dr_db1_data -aggregate aggr1 -size 500G -state online
-policy default -type DP

```

```

vol create -volume dr_db1_log -aggregate aggr1 -size 250G -state online
-policy default -type DP

```

5. You can also create iSCSI volumes and LUNs for the Oracle binary, Oracle data, and the Oracle log if the iSCSI protocol is employed for data access. Leave approximately 10% free space in the volumes for snapshots.

```

vol create -volume dr_db1_bin -aggregate aggr1 -size 50G -state online
-policy default -unix-permissions ---rwxr-xr-x -type RW

```

```

lun create -path /vol/dr_db1_bin/dr_db1_bin_01 -size 45G -ostype linux

```

```

vol create -volume dr_db1_data -aggregate aggr1 -size 500G -state online
-policy default -unix-permissions ---rwxr-xr-x -type RW

```

```

lun create -path /vol/dr_db1_data/dr_db1_data_01 -size 100G -ostype
linux

```

```
lun create -path /vol/dr_db1_data/dr_db1_data_02 -size 100G -ostype linux
```

```
lun create -path /vol/dr_db1_data/dr_db1_data_03 -size 100G -ostype linux
```

```
lun create -path /vol/dr_db1_data/dr_db1_data_04 -size 100G -ostype linux
```

```
vol create -volume dr_db1_log -aggregate aggr1 -size 250G -state online -policy default -unix-permissions ---rwxr-xr-x -type RW
```

```
lun create -path /vol/dr_db1_log/dr_db1_log_01 -size 45G -ostype linux
```

```
lun create -path /vol/dr_db1_log/dr_db1_log_02 -size 45G -ostype linux
```

```
lun create -path /vol/dr_db1_log/dr_db1_log_03 -size 45G -ostype linux
```

```
lun create -path /vol/dr_db1_log/dr_db1_log_04 -size 45G -ostype linux
```

6. For iSCSI LUNs, create mapping for the Oracle host initiator for each LUN, using the binary LUN as an example. Replace the igroup with an appropriate name for your environment, and increment the lun-id for each additional LUN.

```
lun mapping create -path /vol/dr_db1_bin/dr_db1_bin_01 -igroup ip-10-0-1-136 -lun-id 0
```

```
lun mapping create -path /vol/dr_db1_data/dr_db1_data_01 -igroup ip-10-0-1-136 -lun-id 1
```

7. Create a SnapMirror relationship between the primary and standby database volumes. Replace the appropriate SVM name for your environment.s

```
snapmirror create -source-path svm_FSxOraSource:db1_bin -destination  
-path svm_FSxOraTarget:dr_db1_bin -vserver svm_FSxOraTarget -throttle  
unlimited -identity-preserve false -policy MirrorAllSnapshots -type DP
```

```
snapmirror create -source-path svm_FSxOraSource:db1_data -destination  
-path svm_FSxOraTarget:dr_db1_data -vserver svm_FSxOraTarget -throttle  
unlimited -identity-preserve false -policy MirrorAllSnapshots -type DP
```

```
snapmirror create -source-path svm_FSxOraSource:db1_log -destination  
-path svm_FSxOraTarget:dr_db1_log -vserver svm_FSxOraTarget -throttle  
unlimited -identity-preserve false -policy MirrorAllSnapshots -type DP
```

This SnapMirror setup can be automated with a NetApp Automation Toolkit for NFS database volumes. The toolkit is available for download from the NetApp public GitHub site.

```
git clone https://github.com/NetApp-  
Automation/na_ora_hadr_failover_resync.git
```

Read the README instructions carefully before attempting setup and failover testing.



Replicating the Oracle binary from the primary to a standby cluster might have Oracle license implications. Contact your Oracle license representative for clarification. The alternative is to have Oracle installed and configured at the time of recovery and failover.

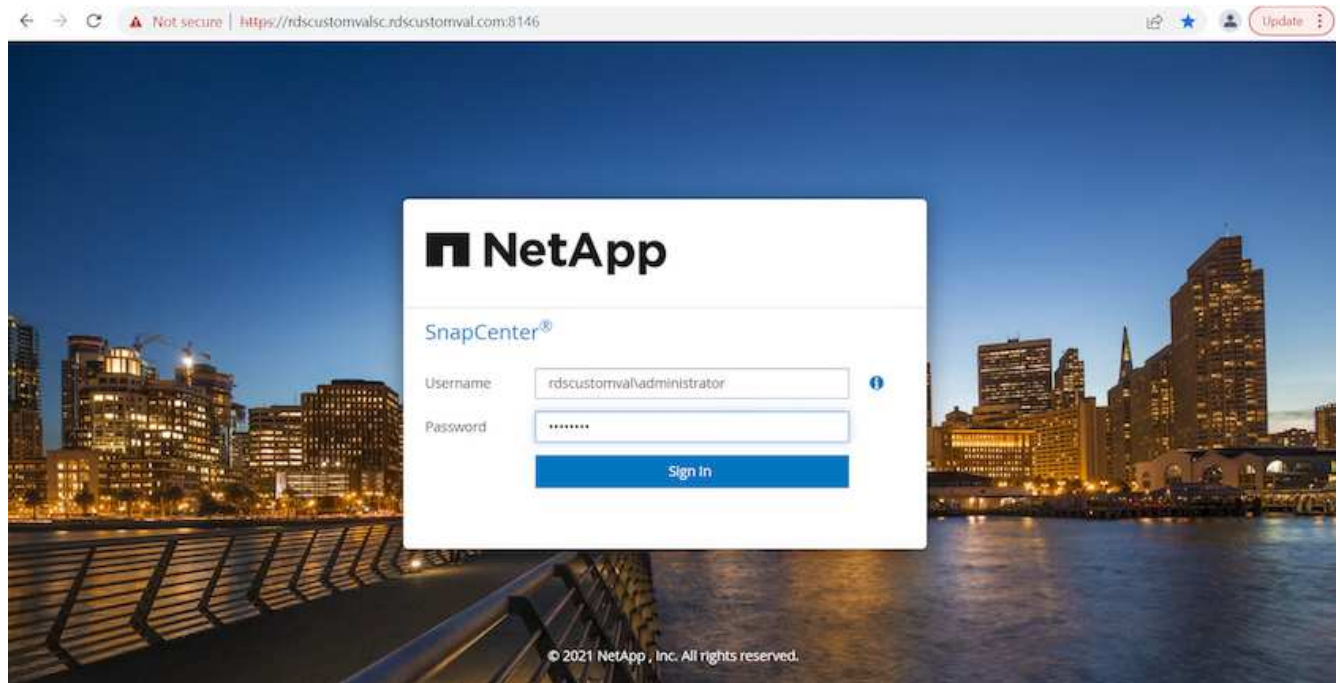
## SnapCenter Deployment

### SnapCenter installation

Follow [Installing the SnapCenter Server](#) to install SnapCenter server. This documentation covers how to install a standalone SnapCenter server. A SaaS version of SnapCenter is in beta review and could be available shortly. Check with your NetApp representative for availability if needed.

### Configure SnapCenter plugin for EC2 Oracle host

1. After automated SnapCenter installation, log into SnapCenter as an administrative user for the Window host on which the SnapCenter server is installed.



- From the left-side menu, click Settings, and then Credential and New to add ec2-user credentials for SnapCenter plugin installation.

| Credential Name | Authentication Mode | Details                           |
|-----------------|---------------------|-----------------------------------|
| 244rdscustomdb  | SQL                 | UserId:admin                      |
| 42rdscustomdb   | SQL                 | UserId:admin                      |
| admin           | SQL                 | UserId:admin                      |
| administrator   | Windows             | UserId:administrator              |
| ec2-user        | Linux               | UserId:ec2-user                   |
| onpremSQL       | Windows             | UserId:rdscustomval/administrator |
| rdsdb2          | Windows             | UserId:administrator              |
| rdsdb244        | Windows             | UserId:administrator              |
| rdsSQL          | Windows             | UserId:administrator              |
| tst244          | SQL                 | UserId:admin                      |
| tstcredfordemo  | Windows             | UserId:administrator              |

- Reset the ec2-user password and enable password SSH authentication by editing the `/etc/ssh/sshd_config` file on the EC2 instance host.
- Verify that the "Use sudo privileges" checkbox is selected. You just reset the ec2-user password in the previous step.

### Credential ✕

Credential Name

Authentication Mode  ▼

Username  i

Password

Use sudo privileges i

5. Add the SnapCenter server name and the IP address to the EC2 instance host file for name resolution.

```

[ec2-user@ip-10-0-0-151 ~]$ sudo vi /etc/hosts
[ec2-user@ip-10-0-0-151 ~]$ cat /etc/hosts
127.0.0.1    localhost localhost.localdomain localhost4
localhost4.localhostdomain4
::1        localhost localhost.localdomain localhost6
localhost6.localhostdomain6
10.0.1.233  rdscustomvalsc.rdscustomval.com rdscustomvalsc
```

6. On the SnapCenter server Windows host, add the EC2 instance host IP address to the Windows host file C:\Windows\System32\drivers\etc\hosts.

```

10.0.0.151    ip-10-0-0-151.ec2.internal
```

7. In the left-side menu, select Hosts > Managed Hosts, and then click Add to add the EC2 instance host to SnapCenter.

NetApp SnapCenter®

Managed Hosts | Disks | Shares | Initiator Groups | iSCSI Session

Search by Name

| Name   | Type    | System      | Plug-in  | Version | Overall Status |
|--|---------|-------------|--|---------|----------------|
| <a href="#">RDSAMAZ-VJ0DQK0</a>                  | Windows | Stand-alone | Microsoft Windows Server, Microsoft SQL Server | 4.5     | Host down      |
| <a href="#">rdscustommssql1.rdscustomval.com</a> | Windows | Stand-alone | Microsoft Windows Server, Microsoft SQL Server | 4.5     | Running        |

Dashboard | Resources | Monitor | Reports | Hosts | Storage Systems | Settings | Alerts

Check Oracle Database, and, before you submit, click More Options.

rdscustomval\administrator | SnapCenterAdmin | Sign Out

**Add Host**

Host Type: Linux

Host Name: 10.0.0.151

Credentials: ec2-user

Select Plug-ins to Install SnapCenter Plug-ins Package 4.5 P2 for Linux

Oracle Database

SAP HANA

[More Options](#): Port, Install Path, Custom Plug-Ins...

Submit | Cancel

Check Skip Preinstall Checks. Confirm Skipping Preinstall Checks, and then click Submit After Save.

### More Options ✕

Port  i

Installation Path  i

Skip preinstall checks

Custom Plug-ins \_\_\_\_\_

Choose a File

No plug-ins found.

You are prompted with Confirm Fingerprint, and then click Confirm and Submit.

### Confirm Fingerprint ✕

Authenticity of the host cannot be determined i

| Host name                  | Fingerprint  | Valid |
|----------------------------|--|-------|
| ip-10-0-0-151.ec2.internal | ssh-rsa 2048 97:6F:3C:7D:38:42:F6:54:B7:AF:E3:61:61:BA:2E:6F |       |

After successful plugin configuration, the managed host's overall status show as Running.

| Managed Hosts            |                            |        |       |                  |                       |               |  |
|--------------------------|----------------------------|--------|-------|------------------|-----------------------|---------------|--|
| Disks                    |                            | Shares |       | Initiator Groups |                       | iSCSI Session |  |
| Search by Name           |                            |        |       |                  |                       |               |  |
|                          |                            |        |       |                  |                       |               |  |
| <input type="checkbox"/> | Name                       | i      | Type  | System           | Plug-in               | Version       | Overall Status                               |
| <input type="checkbox"/> | ip-10-0-0-151.ec2.internal |        | Linux | Stand-alone      | UNIX, Oracle Database | 4.5           | <span style="color: green;">●</span> Running |

### Configure backup policy for Oracle database

Refer to this section [Setup database backup policy in SnapCenter](#) for details on configuring the Oracle database backup policy.

Generally you need create a policy for the full snapshot Oracle database backup and a policy for the Oracle archive-log-only snapshot backup.



You can enable Oracle archive log pruning in the backup policy to control log-archive space. Check "Update SnapMirror after creating a local Snapshot copy" in "Select secondary replication option" as you need to replicate to a standby location for HA or DR.

## Configure Oracle database backup and scheduling

Database backup in SnapCenter is user configurable and can be set up either individually or as a group in a resource group. The backup interval depends on the RTO and RPO objectives. NetApp recommends that you run a full database backup every few hours and archive the log backup at a higher frequency such as 10-15 mins for quick recovery.

Refer to the Oracle section of [Implement backup policy to protect database](#) for a detailed step-by-step processes for implementing the backup policy created in the section [Configure backup policy for Oracle database](#) and for backup job scheduling.

The following image provides an example of the resources groups that are set up to back up an Oracle database.



| Name | Oracle Database Type | Host/Cluster             | Resource Group                      | Policies                                | Last Backup           | Overall Status   |
|------|----------------------|--------------------------|-------------------------------------|---|-----------------------|------------------|
| ORCL | Single Instance      | ip-10-0-151-ec2.internal | orcl_full_backup<br>orcl_log_backup | Oracle full backup<br>Oracle log backup | 03/24/2022 8:40:08 PM | Backup succeeded |

## EC2 and FSx Oracle database management

In addition to the AWS EC2 and FSx management console, the Ansible control node and the SnapCenter UI tool are deployed for database management in this Oracle environment.

An Ansible control node can be used to manage Oracle environment configuration, with parallel updates that keep primary and standby instances in sync for kernel or patch updates. Failover, resync, and failback can be automated with the NetApp Automation Toolkit to archive fast application recovery and availability with Ansible. Some repeatable database management tasks can be executed using a playbook to reduce human errors.

The SnapCenter UI tool can perform database snapshot backup, point-in-time recovery, database cloning, and so on with the SnapCenter plugin for Oracle databases. For more information about Oracle plugin features, see the [SnapCenter Plug-in for Oracle Database overview](#).

The following sections provide details on how key functions of Oracle database management are fulfilled with the SnapCenter UI:

- Database snapshot backups
- Database point-in-time restore
- Database clone creation

Database cloning creates a replica of a primary database on a separate EC2 host for data recovery in the event of logical data error or corruption, and clones can also be used for application testing, debugging, patch



validation, and so on.

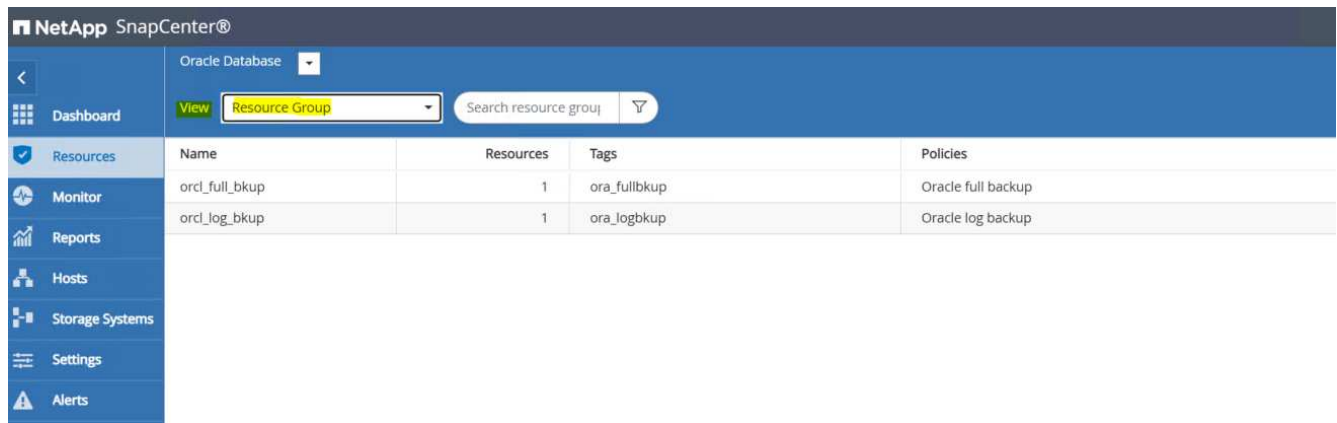
## Taking a snapshot

An EC2/FSx Oracle database is regularly backed up at intervals configured by the user. A user can also take a one-off snapshot backup at any time. This applies to both full-database snapshot backups as well as archive-log-only snapshot backups.

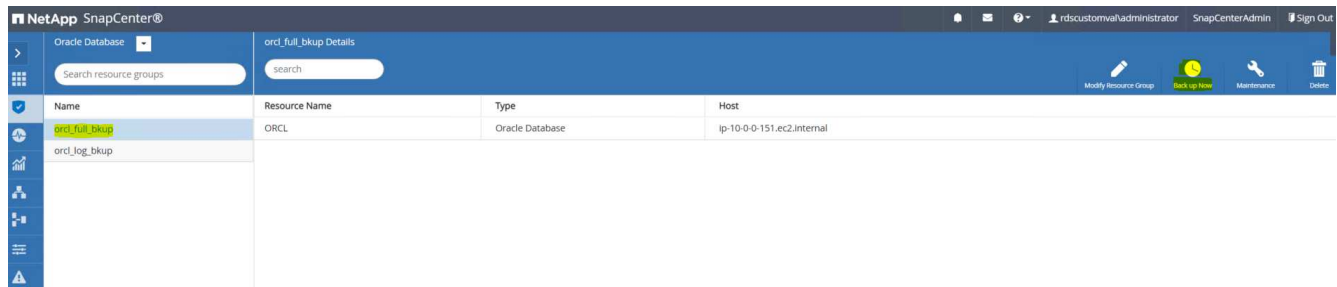
### Taking a full database snapshot

A full database snapshot includes all Oracle files, including data files, control files, and archive log files.

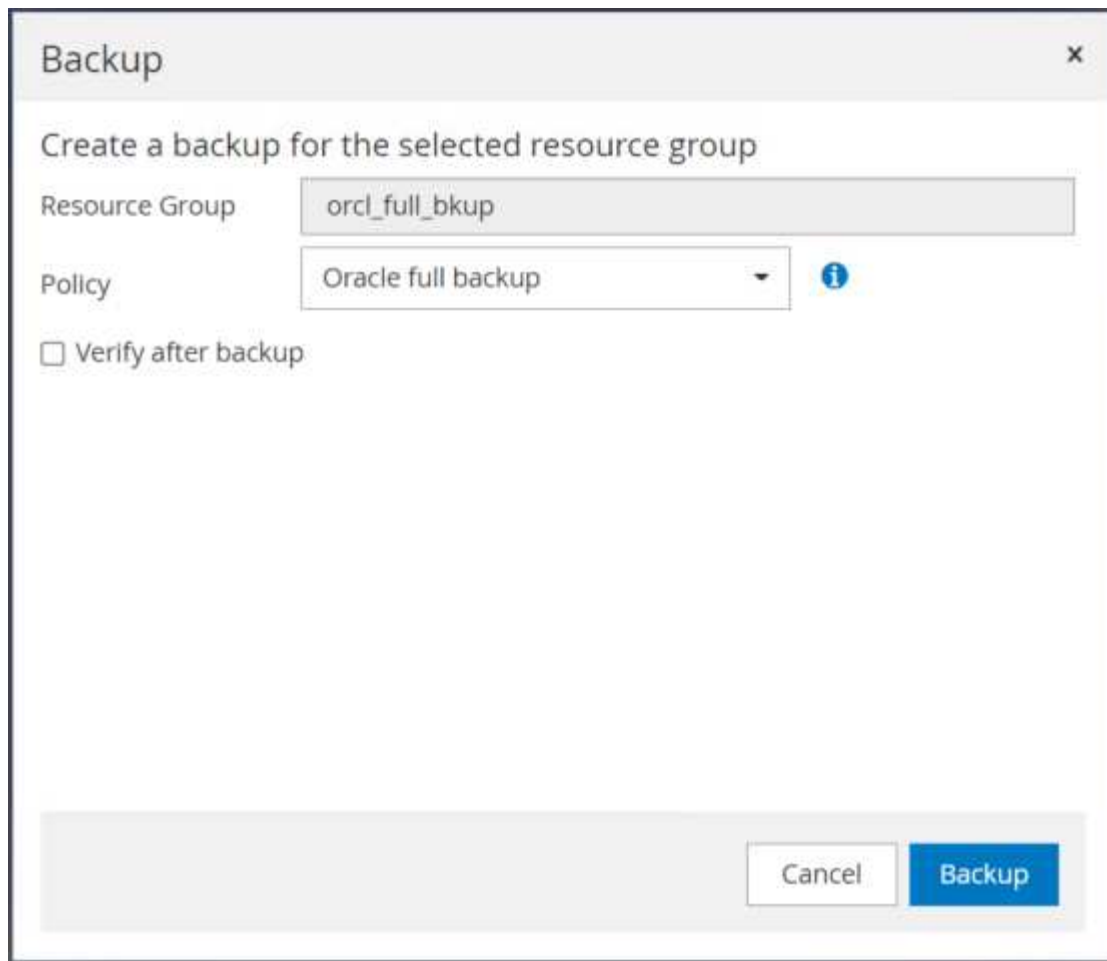
1. Log into the SnapCenter UI and click Resources in the left-side menu. From the View dropdown, change to the Resource Group view.



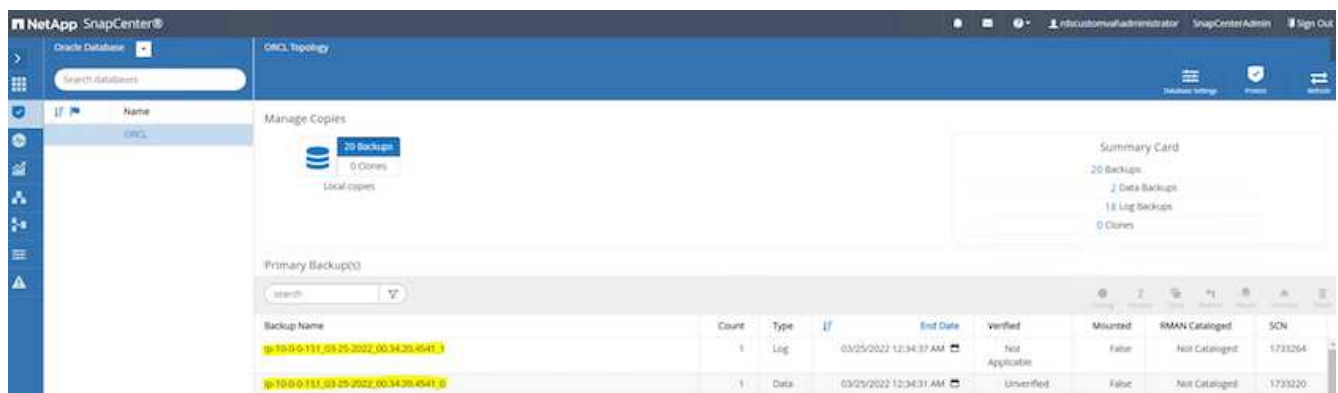
2. Click the full backup resource name, and then click the Backup Now icon to initiate an add-hoc backup.



3. Click Backup and then confirm the backup to start a full database backup.



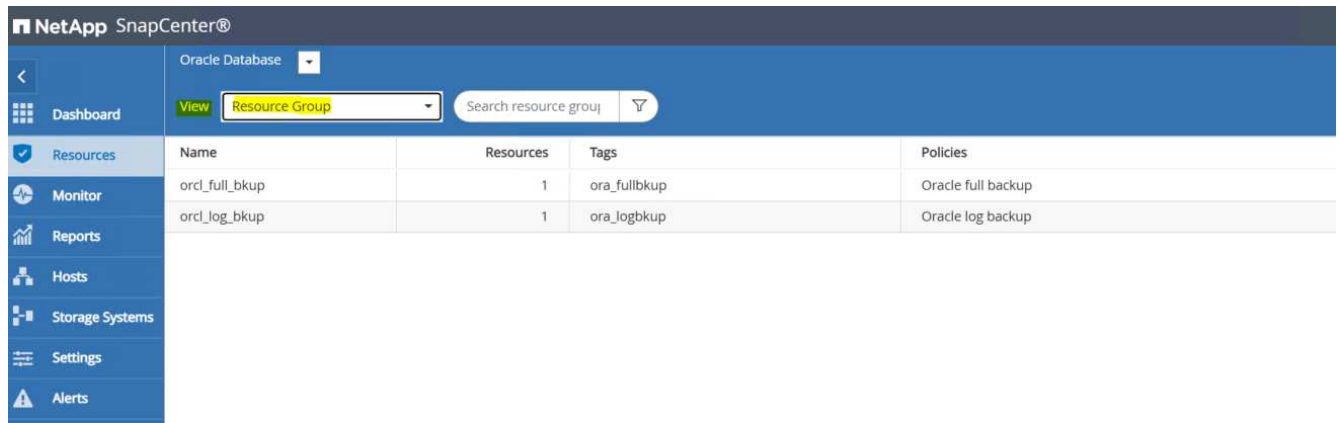
From the Resource view for the database, open the database Managed Backup Copies page to verify that the one-off backup completed successfully. A full database backup creates two snapshots: one for the data volume and one for the log volume.



## Taking an archive log snapshot

An archive log snapshot is only taken for the Oracle archive log volume.

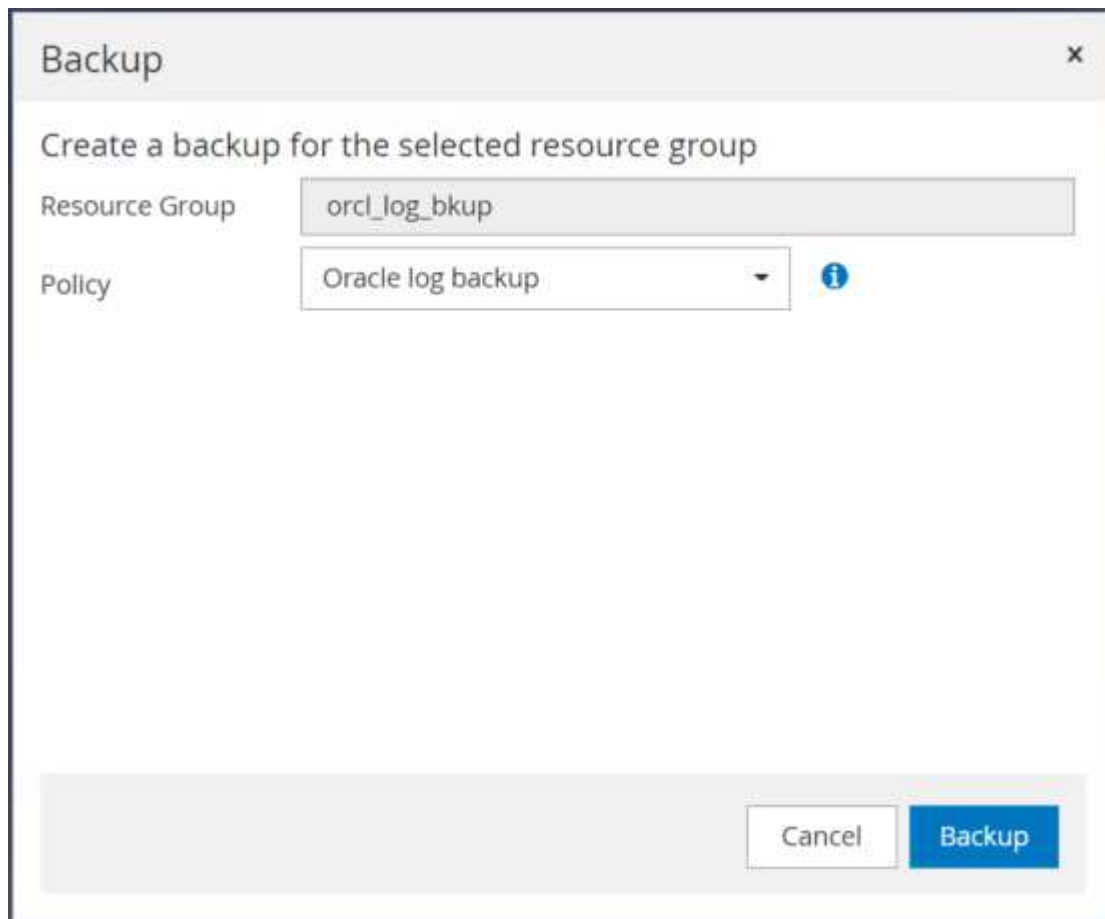
1. Log into the SnapCenter UI and click the Resources tab in the left-side menu bar. From the View dropdown, change to the Resource Group view.



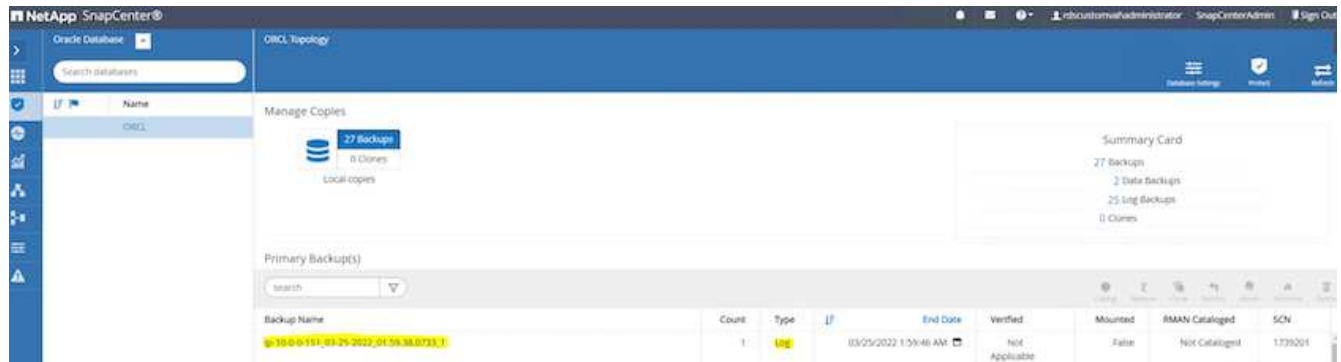
- Click the log backup resource name, and then click the Backup Now icon to initiate an add-hoc backup for archive logs.



- Click Backup and then confirm the backup to start an archive log backup.



From the Resource view for the database, open the database Managed Backup Copies page to verify that the one-off archive log backup completed successfully. An archive log backup creates one snapshot for the log volume.



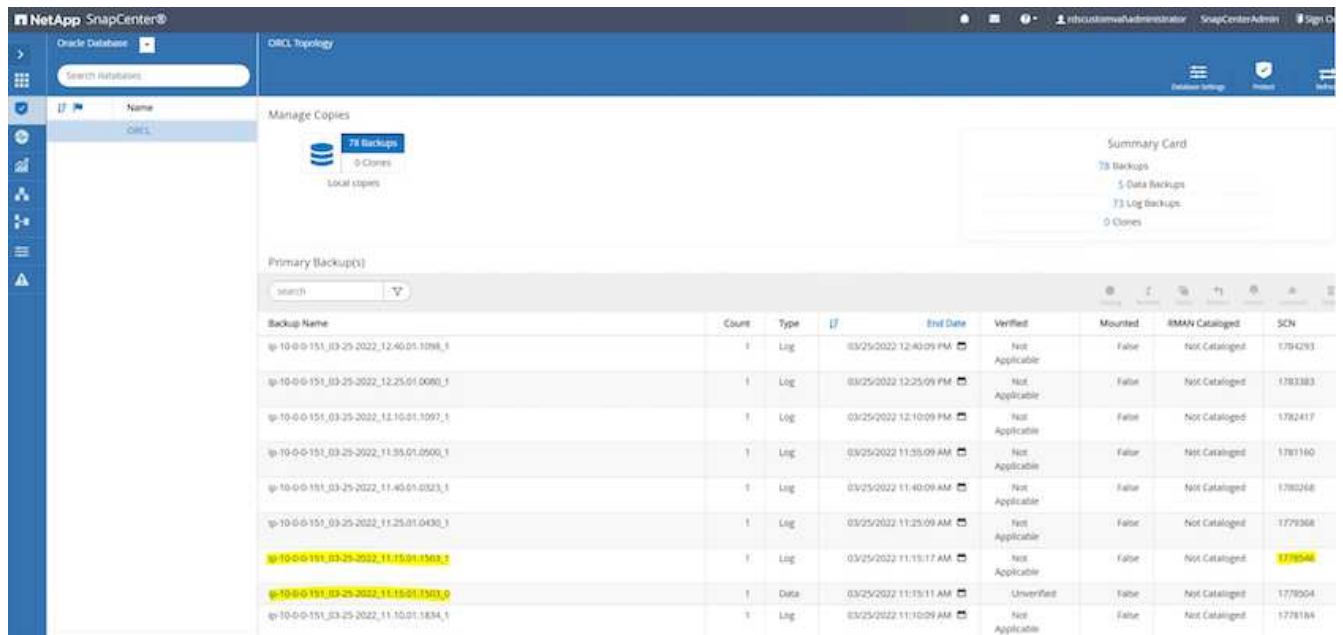
## Restoring to a point in time

SnapCenter-based restore to a point in time is executed on the same EC2 instance host. Complete the following steps to perform the restore:

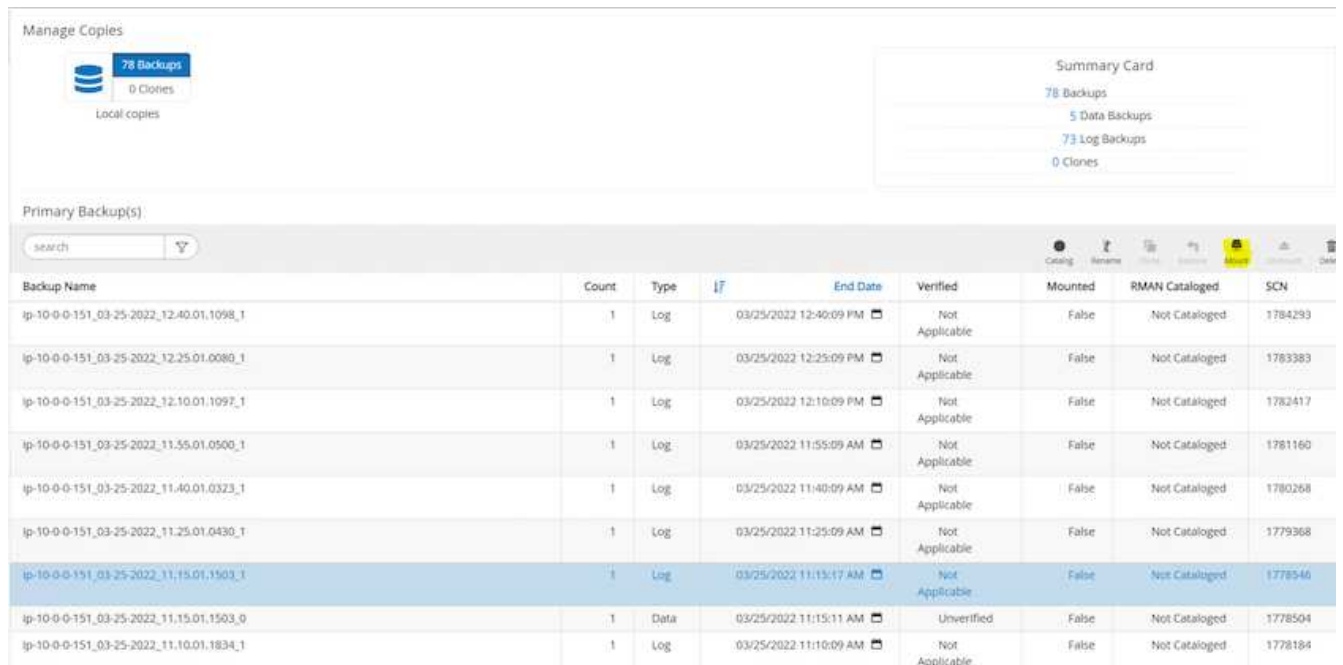
1. From the SnapCenter Resources tab > Database view, click the database name to open the database backup.



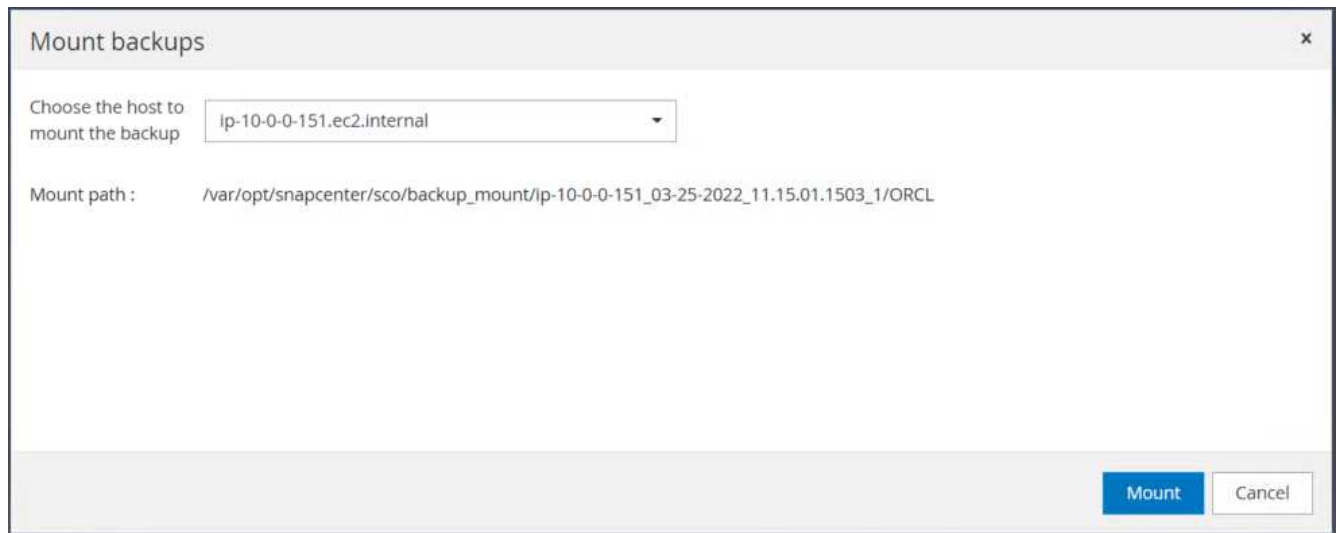
2. Select the database backup copy and the desired point in time to be restored. Also mark down the corresponding SCN number for the point in time. The point-in-time restore can be performed using either the time or the SCN.



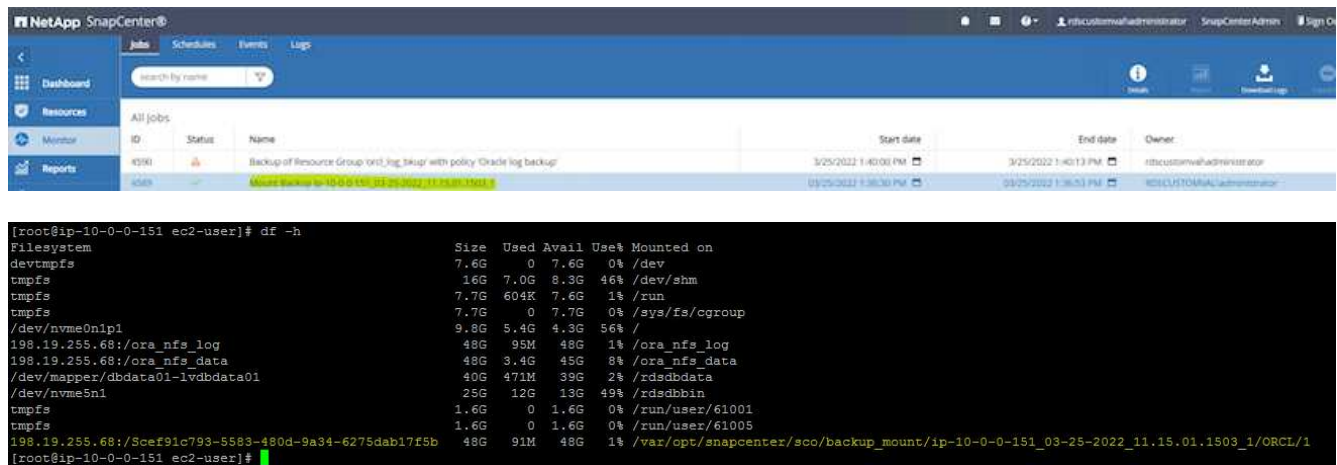
3. Highlight the log volume snapshot and click the Mount button to mount the volume.



4. Choose the primary EC2 instance to mount the log volume.



- Verify that the mount job completes successfully. Also check on the EC2 instance host to see that log volume mounted and also the mount point path.



- Copy the archive logs from the mounted log volume to the current archive log directory.

```
[ec2-user@ip-10-0-0-151 ~]$ cp /var/opt/snapcenter/sco/backup_mount/ip-10-0-0-151_03-25-2022_11.15.01.1503_1/ORCL/1/db/ORCL_A/arch/*.arc /ora_nfs_log/db/ORCL_A/arch/
```

- Return to the SnapCenter Resource tab > database backup page, highlight the data snapshot copy, and click the Restore button to start the database restore workflow.

Manage Copies

**80 Backups**

0 Clones

Local copies

**Summary Card**

80 Backups

5 Data Backups

75 Log Backups

0 Clones

Primary Backup(s)

| Backup Name                              | Count | Type | End Date               | Verified       | Mounted | RMAN Cataloged | SCN     |
|--|-------|------|------------------------|----------------|---------|----------------|---------|
| lp-10-0-0-151_03-25-2022_12.10.01.1097_1 | 1     | Log  | 03/25/2022 12:10:09 PM | Not Applicable | False   | Not Cataloged  | 1782417 |
| lp-10-0-0-151_03-25-2022_11.55.01.0500_1 | 1     | Log  | 03/25/2022 11:55:09 AM | Not Applicable | False   | Not Cataloged  | 1781160 |
| lp-10-0-0-151_03-25-2022_11.40.01.0323_1 | 1     | Log  | 03/25/2022 11:40:09 AM | Not Applicable | False   | Not Cataloged  | 1780268 |
| lp-10-0-0-151_03-25-2022_11.25.01.0430_1 | 1     | Log  | 03/25/2022 11:25:09 AM | Not Applicable | False   | Not Cataloged  | 1779368 |
| lp-10-0-0-151_03-25-2022_11.15.01.1503_1 | 1     | Log  | 03/25/2022 11:15:17 AM | Not Applicable | True    | Not Cataloged  | 1778546 |
| lp-10-0-0-151_03-25-2022_11.15.01.1503_0 | 1     | Data | 03/25/2022 11:15:11 AM | Unverified     | False   | Not Cataloged  | 1778504 |
| lp-10-0-0-151_03-25-2022_11.10.01.1834_1 | 1     | Log  | 03/25/2022 11:10:09 AM | Not Applicable | False   | Not Cataloged  | 1778184 |

8. Check "All Datafiles" and "Change database state if needed for restore and recovery", and click Next.

### Restore ORCL

**1 Restore Scope**

2 Recovery Scope

3 PreOps

4 PostOps

5 Notification

6 Summary

**Restore Scope**

All Datafiles

Tablespaces

Control files

**Database State**

Change database state if needed for restore and recovery

**Restore Mode**

Force in place restore

If this check box is not selected and if any of the in place restore criteria is not met, restore will be performed using the connect and copy method. The connect and copy restore method might take time based on the files being restored.

Previous **Next**

9. Choose a desired recovery scope using either SCN or time. Rather than copying the mounted archive logs to the current log directory as demonstrated in step 6, the mounted archive log path can be listed in

"Specify external archive log files locations" for recovery.

The screenshot shows a window titled "Restore ORCL" with a close button (x) in the top right corner. On the left is a vertical sidebar with six steps: 1 Restore Scope, 2 Recovery Scope (highlighted in blue), 3 PreOps, 4 PostOps, 5 Notification, and 6 Summary. The main content area is titled "Choose Recovery Scope" and contains the following options:

- All Logs (with an information icon)
- Until SCN (System Change Number)
  - SCN:  (with an information icon)
- Date and Time
- No recovery

Below these options is a section titled "Specify external archive log files locations" with a plus icon, a minus icon, and an information icon. Underneath is a large, empty text input field.

At the bottom right of the window are two buttons: "Previous" and "Next".

10. Specify an optional prescript to run if necessary.



Restore ORCL x

**1** Restore Scope  
**2** Recovery Scope  
**3** PreOps  
4 PostOps  
5 Notification  
6 Summary

**Specify optional scripts to run before performing a restore job** ⓘ

Prescript full path

Arguments

Script timeout

11. Specify an optional afterscript to run if necessary. Check the open database after recovery.

Restore ORCL x

**1** Restore Scope

**2** Recovery Scope

**3** PreOps

**4** PostOps

5 Notification

6 Summary

**Specify optional scripts to run after performing a restore job** ⓘ

Postscript full path

Arguments

Open the database or container database in READ-WRITE mode after recovery

12. Provide an SMTP server and email address if a job notification is needed.

Restore ORCL x

- 1 Restore Scope
- 2 Recovery Scope
- 3 PreOps
- 4 PostOps
- 5 Notification**
- 6 Summary

**Provide email settings** ⓘ

Email preference:

From:

To:

Subject:

Attach job report

13. Restore the job summary. Click finish to launch the restore job.

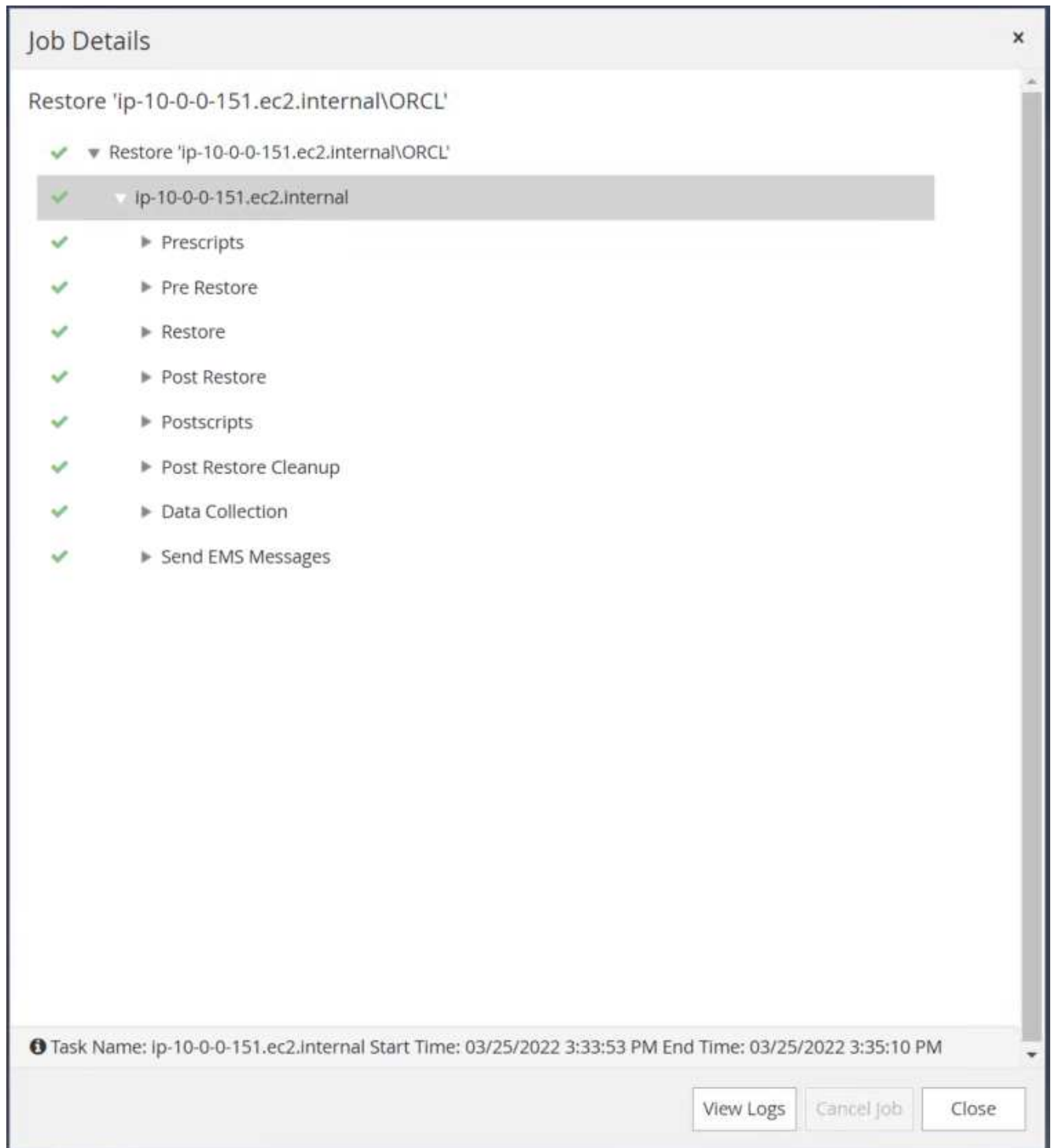
Restore ORCL x

- 1 Restore Scope
- 2 Recovery Scope
- 3 PreOps
- 4 PostOps
- 5 Notification
- 6 Summary**

### Summary

|                       |  |
|-----------------------|--|
| Backup name           | ip-10-0-0-151_03-25-2022_11.15.01.1503_0   |
| Backup date           | 03/25/2022 11:15:11 AM   |
| Restore scope         | All DataFiles  |
| Recovery scope        | Until SCN 1778546  |
| Auxiliary destination |  |
| Options               | Change database state if necessary , Open the database or container database in READ-WRITE mode after recovery |
| Prescript full path   | None   |
| Prescript arguments   |  |
| Postscript full path  | None   |
| Postscript arguments  |  |
| Send email            | No   |

14. Validate the restore from SnapCenter.



15. Validate the restore from the EC2 instance host.

```

-bash-4.2$ sqlplus / as sysdba

SQL*Plus: Release 19.0.0.0.0 - Production on Fri Mar 25 15:44:08 2022
Version 19.8.0.0.0

Copyright (c) 1982, 2020, Oracle. All rights reserved.

Connected to:
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.8.0.0.0

SQL> select name, RESETLOGS_CHANGE#, RESETLOGS_TIME, open_mode from v$database;

NAME          RESETLOGS_CHANGE# RESETLOGS_TIME OPEN_MODE
-----
ORCL          1778547 25-MAR-22 READ WRITE

SQL>

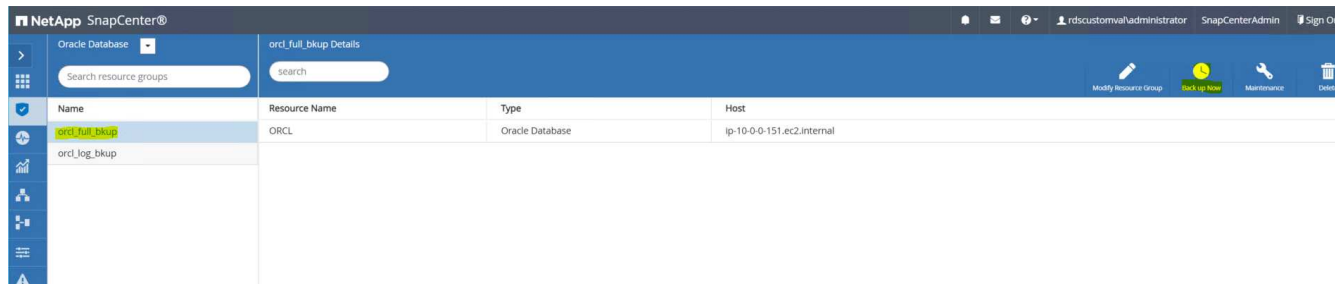
```

16. To unmount the restore log volume, reverse the steps in step 4.

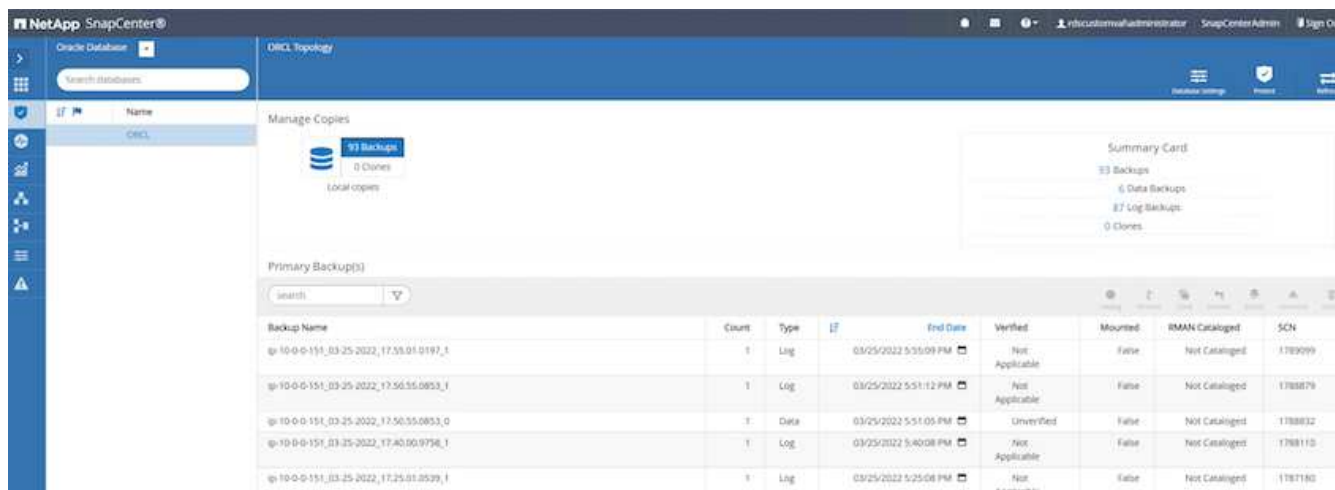
## Creating a database clone

The following section demonstrates how to use the SnapCenter clone workflow to create a database clone from a primary database to a standby EC2 instance.

1. Take a full snapshot backup of the primary database from SnapCenter using the full backup resource group.



2. From the SnapCenter Resource tab > Database view, open the Database Backup Management page for the primary database that the replica is to be created from.



3. Mount the log volume snapshot taken in step 4 to the standby EC2 instance host.

ORCL Topology

Manage Copies

95 Backups  
0 Clones  
Local copies

Summary Card

95 Backups  
6 Data Backups  
89 Log Backups  
0 Clones

Primary Backup(s)

| Backup Name                              | Count | Type | End Date              | Verified       | Mounted | RMAN Cataloged | SCN     |
|--|-------|------|-----------------------|----------------|---------|----------------|---------|
| ip-10-0-0-151_03-25-2022_18.55.01.0309_1 | 1     | Log  | 03/25/2022 6:55:09 PM | Not Applicable | False   | Not Cataloged  | 1892563 |
| ip-10-0-0-151_03-25-2022_18.40.00.9602_1 | 1     | Log  | 03/25/2022 6:40:23 PM | Not Applicable | False   | Not Cataloged  | 1891375 |
| ip-10-0-0-151_03-25-2022_17.55.01.0197_1 | 1     | Log  | 03/25/2022 5:55:09 PM | Not Applicable | False   | Not Cataloged  | 1789099 |
| ip-10-0-0-151_03-25-2022_17.50.55.0853_1 | 1     | Log  | 03/25/2022 5:51:12 PM | Not Applicable | False   | Not Cataloged  | 1788879 |
| ip-10-0-0-151_03-25-2022_17.50.55.0853_0 | 1     | Data | 03/25/2022 5:51:05 PM | Unverified     | False   | Not Cataloged  | 1788832 |
| ip-10-0-0-151_03-25-2022_17.40.00.9758_1 | 1     | Log  | 03/25/2022 5:40:08 PM | Not Applicable | False   | Not Cataloged  | 1788110 |

Mount backups

Choose the host to mount the backup: ip-10-0-0-47.ec2.internal

Mount path: /var/opt/snapcenter/sco/backup\_mount/ip-10-0-0-151\_03-25-2022\_17.50.55.0853\_1/ORCL

Mount Cancel

- Highlight the snapshot copy to be cloned for the replica, and click the Clone button to start the clone procedure.

ORCL Topology

Manage Copies

93 Backups  
0 Clones  
Local copies

Summary Card

93 Backups  
6 Data Backups  
87 Log Backups  
0 Clones

Primary Backup(s)

| Backup Name                              | Count | Type | End Date              | Verified       | Mounted | RMAN Cataloged | SCN     |
|--|-------|------|-----------------------|----------------|---------|----------------|---------|
| ip-10-0-0-151_03-25-2022_17.55.01.0197_1 | 1     | Log  | 03/25/2022 5:55:09 PM | Not Applicable | False   | Not Cataloged  | 1789099 |
| ip-10-0-0-151_03-25-2022_17.50.55.0853_1 | 1     | Log  | 03/25/2022 5:51:12 PM | Not Applicable | False   | Not Cataloged  | 1788879 |
| ip-10-0-0-151_03-25-2022_17.50.55.0853_0 | 1     | Data | 03/25/2022 5:51:05 PM | Unverified     | False   | Not Cataloged  | 1788832 |
| ip-10-0-0-151_03-25-2022_17.40.00.9758_1 | 1     | Log  | 03/25/2022 5:40:08 PM | Not Applicable | False   | Not Cataloged  | 1788110 |
| ip-10-0-0-151_03-25-2022_17.25.01.0539_1 | 1     | Log  | 03/25/2022 5:25:08 PM | Not Applicable | False   | Not Cataloged  | 1787180 |

5. Change the replica copy name so that it is different from the primary database name. Click Next.

The screenshot shows a wizard window titled "Clone from ORCL" with a close button (x) in the top right corner. On the left, there is a vertical sidebar with seven steps: 1 Name (highlighted in blue), 2 Locations, 3 Credentials, 4 PreOps, 5 PostOps, 6 Notification, and 7 Summary. The main area is titled "Provide clone database SID" and contains a "Clone SID" label followed by a text input field containing the value "ORCLREAD". At the bottom right, there are two buttons: "Previous" (disabled) and "Next" (active/highlighted in blue).

6. Change the clone host to the standby EC2 host, accept the default naming, and click Next.



Clone from ORCL
✕

- 1 Name
- 2 Locations
- 3 Credentials
- 4 PreOps
- 5 PostOps
- 6 Notification
- 7 Summary

### Select the host to create a clone

Clone host

Datafile locations ⓘ

Control files ⓘ

Redo logs ⓘ

| Group  | Size | Unit | Number of files |
|--|------|------|-----------------|
| <input checked="" type="checkbox"/> RedoGroup 1 <input type="button" value="✕"/>                                 | 128  | MB   | 1               |
| <input type="text" value="/ora_nfs_data_ORCLREAD/ORCLREAD/redolog/redo04.log"/> <input type="button" value="✕"/> |      |      |                 |
| <input type="checkbox"/> RedoGroup 2 <input type="button" value="✕"/>  | 128  | MB   | 1               |

7. Change your Oracle home settings to match those configured for the target Oracle server host, and click Next.

Clone from ORCL

1 Name

2 Locations

3 Credentials

4 PreOps

5 PostOps

6 Notification

7 Summary

### Database Credentials for the clone

Credential name for sys user: None + i

Database port: 1521

### Oracle Home Settings i

Oracle Home: /rdsdbbin/oracle

Oracle OS User: rdsdb

Oracle OS Group: database

Previous Next

8. Specify a recovery point using either time or the SCN and mounted archive log path.

### Clone from ORCL

- 1 Name
- 2 Locations
- 3 Credentials
- 4 PreOps
- 5 PostOps**
- 6 Notification
- 7 Summary

Recover Database

Until Cancel ?

Date and Time  ?

Date-time format: MM/DD/YYYY hh:mm:ss

Until SCN (System Change Number)  ?

Specify external archive log locations ?

Create new DBID ?

Create tempfile for temporary tablespace ?

Enter SQL queries to apply when clone is created

Enter scripts to run after clone operation ?

Previous **Next**

9. Send the SMTP email settings if needed.

Clone from ORCL x

- 1 Name
- 2 Locations
- 3 Credentials
- 4 PreOps
- 5 PostOps
- 6 Notification**
- 7 Summary

**Provide email settings** ⓘ

Email preference:

From:

To:

Subject:

Attach job report

10. Clone the job summary, and click Finish to launch the clone job.

Clone from ORCL

1 Name

2 Locations

3 Credentials

4 PreOps

5 PostOps

6 Notification

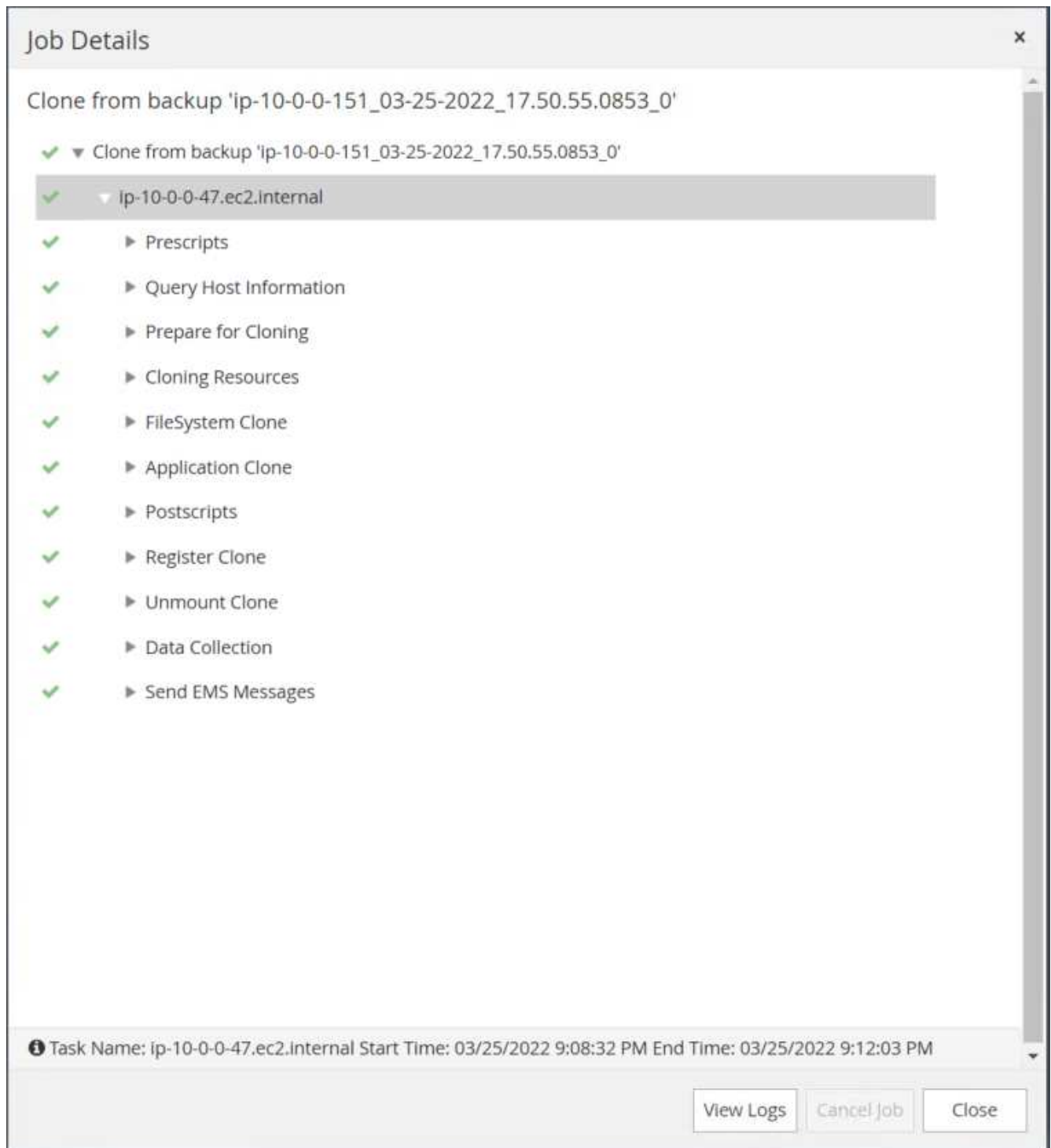
7 Summary

**Summary**

|                      |  |
|----------------------|--|
| Clone from backup    | ip-10-0-0-151_03-25-2022_17.50.55.0853_0   |
| Clone SID            | ORCLREAD   |
| Clone server         | ip-10-0-0-47.ec2.internal  |
| Oracle home          | /rdsdbbin/oracle   |
| Oracle OS user       | rdsdb  |
| Oracle OS group      | database   |
| Datafile mountpaths  | /ora_nfs_data_ORCLREAD   |
| Control files        | /ora_nfs_data_ORCLREAD/ORCLREAD/control/control01.ctl  |
| Redo groups          | RedoGroup =1 TotalSize =128 Path =/ora_nfs_data_ORCLREAD/ORCLREAD/redolog/redo04.log<br>RedoGroup =2 TotalSize =128 Path =/ora_nfs_data_ORCLREAD/ORCLREAD/redolog/redo03.log<br>RedoGroup =3 TotalSize =128 Path =/ora_nfs_data_ORCLREAD/ORCLREAD/redolog/redo02.log<br>RedoGroup =4 TotalSize =128 Path =/ora_nfs_data_ORCLREAD/ORCLREAD/redolog/redo01.log |
| Recovery scope       | Until SCN 1788879  |
| Prescript full path  | none   |
| Prescript arguments  |  |
| Postscript full path | none   |
| Postscript arguments |  |
| Send email           | No   |

Previous Finish

11. Validate the replica clone by reviewing the clone job log.



The cloned database is registered in SnapCenter immediately.

| Name     | Oracle Database Type | Host/Cluster               | Resource Group                      | Policies                                | Last Backup           | Overall Status   |
|----------|----------------------|----------------------------|-------------------------------------|---|-----------------------|------------------|
| ORCL     | Single Instance      | ip-10-0-0-151.ec2.internal | orcl_full_backup<br>orcl_log_backup | Oracle full backup<br>Oracle log backup | 03/25/2022 9:10:09 PM | Backup succeeded |
| ORCLREAD | Single Instance      | ip-10-0-0-47.ec2.internal  |                                     |   |                       | Not protected    |

12. Turn off Oracle archive log mode. Log into the EC2 instance as oracle user and execute following command:

```
sqlplus / as sysdba
```

```
shutdown immediate;
```

```
startup mount;
```

```
alter database noarchivelog;
```

```
alter database open;
```



Instead primary Oracle backup copies, a clone can also be created from replicated secondary backup copies on target FSx cluster with same procedures.

## HA failover to standby and resync

The standby Oracle HA cluster provides high availability in the event of failure in the primary site, either in the compute layer or in the storage layer. One significant benefit of the solution is that a user can test and validate the infrastructure at any time or with any frequency. Failover can be user simulated or triggered by real failure. The failover processes are identical and can be automated for fast application recovery.

See the following list of failover procedures:

1. For a simulated failover, run a log snapshot backup to flush the latest transactions to the standby site, as demonstrated in the section [Taking an archive log snapshot](#). For a failover triggered by an actual failure, the last recoverable data is replicated to the standby site with the last successful scheduled log volume backup.
2. Break the SnapMirror between primary and standby FSx cluster.
3. Mount the replicated standby database volumes at the standby EC2 instance host.
4. Relink the Oracle binary if the replicated Oracle binary is used for Oracle recovery.
5. Recover the standby Oracle database to the last available archive log.
6. Open the standby Oracle database for application and user access.
7. For an actual primary site failure, the standby Oracle database now takes the role of the new primary site and database volumes can be used to rebuild the failed primary site as a new standby site with the reverse SnapMirror method.
8. For a simulated primary site failure for testing or validation, shut down the standby Oracle database after the completion of testing exercises. Then unmount the standby database volumes from the standby EC2 instance host and resync replication from the primary site to the standby site.

These procedures can be performed with the NetApp Automation Toolkit available for download at the public NetApp GitHub site.

```
git clone https://github.com/NetApp-  
Automation/na_ora_hadr_failover_resync.git
```

Read the README instruction carefully before attempting setup and failover testing.

## Database migration from on-prem to public cloud

Database migration is a challenging endeavor by any means. Migrating an Oracle database from on-premises to the cloud is no exception.

The following sections provide key factors to consider when migrating Oracle databases to the AWS public cloud with the AWS EC2 compute and FSx storage platform.

### ONTAP storage is available on-premises

If the on-premises Oracle database is sitting on an ONTAP storage array, then it is easier to set up replication for database migration using the NetApp SnapMirror technology that is built into AWS FSx ONTAP storage. The migration process can be orchestrated using NetApp BlueXP console.

1. Build a target compute EC2 instance that matches the on-premises instance.
2. Provision matching, equally sized database volumes from FSx console.
3. Mount the FSx database volumes to the EC2 instance.
4. Set up SnapMirror replication between the on-premises database volumes to the target FSx database volumes. The initial sync might take some time to move the primary source data, but any following incremental updates are much quicker.
5. At the time of switchover, shut down the primary application to stop all transactions. From the Oracle sqlplus CLI interface, execute an Oracle online log switch and allow SnapMirror sync to push the last archived log to the target volume.
6. Break up the mirrored volumes, run Oracle recovery at the target, and bring up the database for service.
7. Point applications to the Oracle database in the cloud.

The following video demonstrates how to migrate an Oracle database from on-premises to AWS FSx/EC2 using the NetApp BlueXP console and SnapMirror replication.

[Migrate on-prem Oracle DB to AWS](#)

### ONTAP storage is not available on premises

If the on-premises Oracle database is hosted on third-party storage other than ONTAP, database migration is based on the restore of a Oracle database backup copy. You must play the archive log to make it current before switching over.

AWS S3 can be used as a staging storage area for database move and migration. See the following high level steps for this method:



1. Provision a new, matching EC2 instance that is comparable with the on-premises instance.
2. Provision equal database volumes from FSx storage and mount the volumes to the EC2 instance.
3. Create a disk-level Oracle backup copy.
4. Move the backup copy to AWS S3 storage.
5. Recreate the Oracle control file and restore and recover the database by pulling data and the archive log from S3 storage.
6. Sync the target Oracle database with the on-premises source database.
7. At switchover, shut down the application and source Oracle database. Copy the last few archive logs and apply them to the target Oracle database to bring it up to date.
8. Start up the target database for user access.
9. Redirect application to the target database to complete the switchover.

## Migrate on-premises Oracle databases to AWS FSx/EC2 using PDB relocation with maximum availability

This migration approach is best suited to Oracle databases that are already deployed in PDB/CDB multitenant model, and ONTAP storage is not available on-premises. The PDB relocation method utilizes Oracle PDB hot clone technology to move PDBs between a source CDB and a target CDB while minimizing service interruption.

First, create CDB in the AWS FSx/EC2 with sufficient storage to host PDBs to be migrated from on-premises. Multiple on-premises PDBs can be relocated one at a time.

1. If the on-premises database is deployed in a single instance rather than in the multitenant PDB/CDB model, follow the instructions in [Converting a single instance non-CDB to a PDB in a multitenant CDB](#) to convert the single instance to multitenant PDB/CDB. Then follow the next step to migrate the converted PDB to CDB in AWS FSx/EC2.
2. If the on-premises database is already deployed in the multitenant PDB/CDB model, follow the instructions in [Migrate on-premises Oracle databases to cloud with PDB relocation](#) to perform the migration.

The following video demonstrates how an Oracle database (PDB) can be migrated to FSx/EC2 using PDB relocation with maximum availability.

### [Migrate on-prem Oracle PDB to AWS CDB with max availability](#)



Although the instructions in step 1 and 2 are illustrated in the context of Azure public cloud, the procedures are applicable to AWS cloud without any changes.

The NetApp Solutions Automation team provides a migration toolkit that can facilitate Oracle database migration from on-premises to the AWS cloud. Use following command to download the Oracle database migration toolkit for PDB relocation.

```
git clone https://github.com/NetApp-Automation/na_ora_aws_migration.git
```

## Copyright information

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

## Trademark information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.