



SnapCenter for databases

NetApp Solutions

NetApp
September 08, 2023

This PDF was generated from https://docs.netapp.com/us-en/netapp-solutions/databases/snapctr_svcs_ora_azure.html on September 08, 2023. Always check docs.netapp.com for the latest.

Table of Contents

SnapCenter for databases	1
TR-4977: Oracle Database backup, restore and clone with SnapCenter Services - Azure	1
TR-4964: Oracle Database backup, restore and clone with SnapCenter Services - AWS	35
Hybrid Cloud Database Solutions with SnapCenter	69

SnapCenter for databases

TR-4977: Oracle Database backup, restore and clone with SnapCenter Services - Azure

Allen Cao, Niyaz Mohamed, NetApp

Purpose

SnapCenter Services is the SaaS version of the classic SnapCenter database management UI tool that is available through the NetApp BlueXP cloud management console. It is an integral part of the NetApp cloud-backup, data-protection offering for databases such as Oracle and HANA running on Azure NetApp Files. This SaaS-based service simplifies traditional SnapCenter standalone server deployment that generally requires a Windows server operating in a Windows domain environment.

In this documentation, we demonstrate how you can set up SnapCenter Services to backup, restore, and clone Oracle databases deployed on Azure NetApp Files volumes and Azure compute instances. It is very easy to setup data protection for Oracle database deployed on Azure NetApp Files with web based BlueXP user interface.

This solution addresses the following use cases:

- Database backup with snapshots for Oracle databases hosted in Azure NetApp Files and Azure VMs
- Oracle database recovery in the case of a failure
- Fast cloning of primary databases for dev, test environments or other use cases

Audience

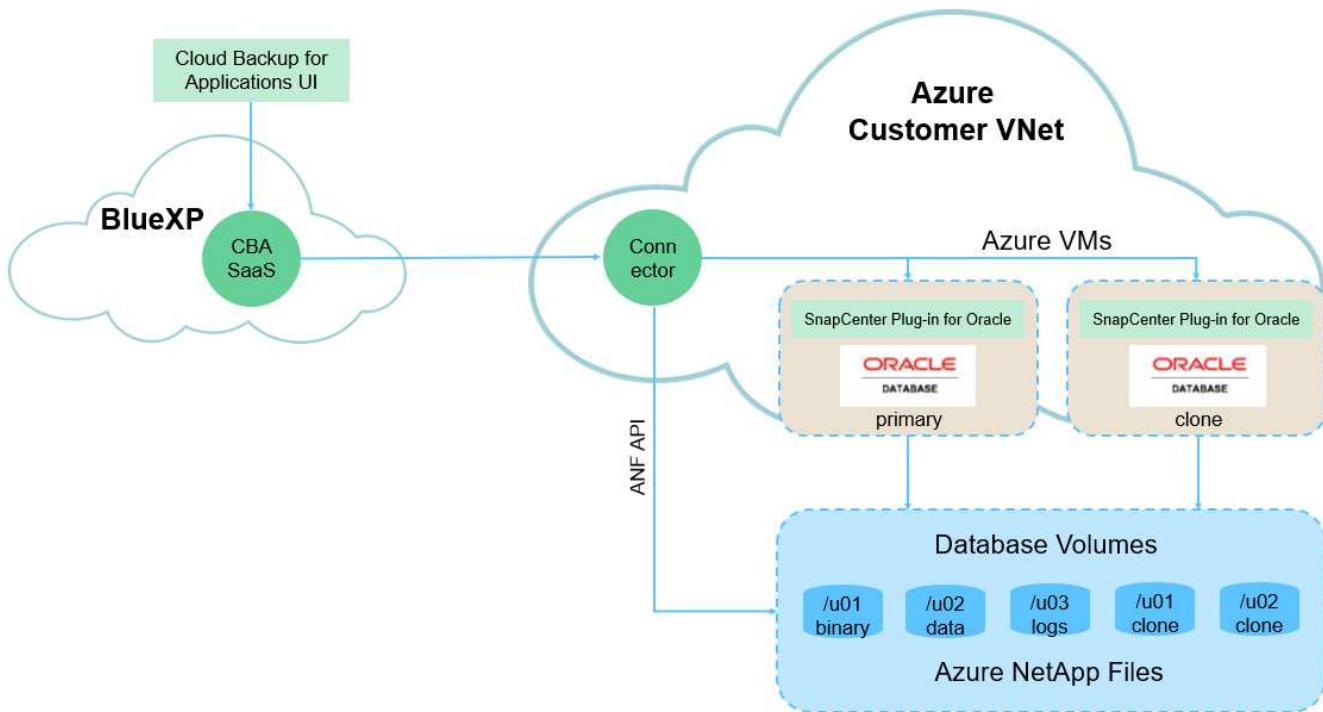
This solution is intended for the following audiences:

- The DBA who manages Oracle databases running on Azure NetApp Files storage
- The solution architect who is interested in testing Oracle database backup, restore, and clone in Azure
- The storage administrator who supports and manages the Azure NetApp Files storage
- The application owner who owns applications that are deployed to Azure NetApp Files storage and Azure VMs

Solution test and validation environment

The testing and validation of this solution was performed in a lab environment that might not match the final deployment environment. For more information, see the section [\[Key Factors for Deployment Consideration\]](#).

Architecture



This image provides a detailed picture of BlueXP backup and recovery for applications within the BlueXP console, including the UI, the connector, and the resources it manages.

Hardware and software components

Hardware

Azure NetApp Files storage	Premium Service level	Auto QoS type, and 4TB in storage capacity in testing
Azure instance for compute	Standard B4ms (4 vcpus, 16 GiB memory)	Two instances deployed, one as primary DB server and the other as clone DB server

Software

RedHat Linux	Red Hat Enterprise Linux 8.7 (LVM) - x64 Gen2	Deployed RedHat subscription for testing
Oracle Database	Version 19.18	Applied RU patch p34765931_190000_Linux-x86-64.zip
Oracle OPatch	Version 12.2.0.1.36	Latest patch p6880880_190000_Linux-x86-64.zip
SnapCenter Service	Version v2.5.0-2822	Agent Version v2.5.0-2822

Key factors for deployment consideration

- Connector to be deployed in the same virtual network / subnet as databases and Azure NetApp Files.** When possible, the connector should be deployed in the same Azure virtual networks and resource groups, which enables connectivity to the Azure NetApp Files storage and the Azure compute instances.

- **An Azure user account or Active Directory service principle created at Azure portal for SnapCenter connector.** Deploying a BlueXP Connector requires specific permissions to create and configure a virtual machine and other compute resources, to configure networking, and to get access to the Azure subscription. It also requires permissions to later create roles and permissions for the Connector to operate. Create a custom role in Azure with permissions and assign to the user account or service principle. Review the following link for details:[Set up Azure permissions](#).
- **A ssh key pair created in the Azure resource group.** The ssh key pair is assigned to the Azure VM user for logging into the connector host and also the database VM host for deploying and executing a plug-in. BlueXP console UI uses the ssh key to deploy SnapCenter service plugin to database host for one-step plugin installation and application host database discovery.
- **A credential added to the BlueXP console setting.** To add Azure NetApp Files storage to the BlueXP working environment, a credential that grants permissions to access Azure NetApp Files from the BlueXP console needs to be set up in the BlueXP console setting.
- **java-11-openjdk installed on the Azure VM database instance host.** SnapCenter service installation requires java version 11. It needs to be installed on application host before plugin deployment attempt.

Solution deployment

There is extensive NetApp documentation with a broader scope to help you protect your cloud-native application data. The goal of this documentation is to provide step-by-step procedures that cover SnapCenter Service deployment with the BlueXP console to protect your Oracle database deployed on an Azure NetApp Files storage and an Azure compute instance.

To get started, complete the following steps:

- Read the general instructions [Protect your cloud native applications data](#) and the sections related to Oracle and Azure NetApp Files.
- Watch the following video walkthrough

[Video of deployment of Oracle and ANF](#)

Prerequisites for SnapCenter service deployment

Deployment requires the following prerequisites.

1. A primary Oracle database server on an Azure VM instance with an Oracle database fully deployed and running.
2. An Azure NetApp Files storage service capacity pool deployed in Azure that has capacity to meet the database storage needs listed in hardware component section.
3. A secondary database server on an Azure VM instance that can be used for testing the cloning of an Oracle database to an alternate host for the purpose of supporting a dev/test workload or any use cases that requires a full data set of production Oracle database.
4. For additional information for Oracle database deployment on Azure NetApp Files and Azure compute instance, see [Oracle Database Deployment and Protection on Azure NetApp Files](#).

Onboarding to BlueXP preparation

1. Use the link [NetApp BlueXP](#) to sign up for BlueXP console access.
2. Create an Azure user account or an Active Directory service principle and grant permissions with role in Azure portal for Azure connector deployment.
3. To set up BlueXP to manage Azure resources, add a BlueXP credential with details of an Active Directory service principal that BlueXP can use to authenticate with Azure Active Directory (App client ID), a client secret for the service principal application (Client Secret), and the Active Directory ID for your organization (Tenant ID).
4. You also need the Azure virtual network, resources group, security group, an SSH key for VM access, etc. ready for connector provisioning and database plugin installation.

Deploy a connector for SnapCenter services

1. Login to the BlueXP console.

The screenshot shows the NetApp BlueXP console interface. At the top, there's a blue header bar with the NetApp BlueXP logo, a search bar labeled "BlueXP Search", and dropdown menus for "Account Automation-te...", "Workspace Azure-DB", "Connector N/A", and various system icons. Below the header is a navigation bar with tabs: "Canvas" (selected), "My working environments" (highlighted in blue), and "My estate". A button "+ Add Working Environment" is visible. On the left, there's a sidebar with several icons. The main canvas area displays two cloud storage resources: "Azure Blob Storage" (20 Storage Accounts) and "Amazon S3" (0 Buckets). To the right, a "Working Environments" section lists "Amazon S3" (0 Buckets) and "Azure Blob Storage" (20 Storage Accounts). At the bottom right, there are "Switch" and "Cancel" buttons.

2. Click on **Connector** drop down arrow and **Add Connector** to launch the connector provisioning workflow.

This screenshot shows the "Add Connector" step in the BlueXP console. The "Add Connector" tab is highlighted in red at the top of the right-hand sidebar. The sidebar also includes "Connectors" and "Manage Connectors" buttons. The main canvas area is dimmed, showing the same storage resources as the previous screenshot. The right sidebar contains a search bar "Search BlueXP Connectors" and a list of existing connectors: "acao-aws-connector" (AWS | us-east-1 | Inactive) and "AzureConnector" (Azure | southcentralus | Inactive). At the bottom right of the sidebar, there are "Switch" and "Cancel" buttons.

3. Choose your cloud provider (in this case, **Microsoft Azure**).

Add BlueXP Connector

X

Provider

Choose the cloud provider where you want to run the BlueXP Connector:



Microsoft Azure



Amazon Web Services



Google Cloud Platform

[Deploy the Connector on your premises](#)

Continue



4. Skip the **Permission**, **Authentication**, and **Networking** steps if you already have them set up in your Azure account. If not, you must configure these before proceeding. From here, you could also retrieve the permissions for the Azure policy that is referenced in the previous section "[Onboarding to BlueXP preparation](#)."

Deploying a BlueXP Connector

The BlueXP Connector is a crucial component for the day-to-day use of BlueXP.

It's used to connect BlueXP's services to your hybrid-cloud environments.

The BlueXP Connector can then manage the resources and processes within your public cloud environment.

Before you begin the deployment process, ensure that you have completed the required preparations. This guide will enable you to focus on the minimum requirements for BlueXP Connector installation.

Permissions

Ensure that the Azure user or service principal you've provided has sufficient permissions

Authentication

Choose between two methods: an [Azure user account](#) or an [Active Directory service principal](#)

Networking

Ensure that you have details on the VNet and subnet in which the BlueXP Connector will reside

[Skip to Deployment](#)

Previous

Continue



5. Click on **Skip to Deployment** to configure your connector **Virtual Machine Authentication**. Add the SSH key pair you have created in Azure resource group during onboarding to BlueXP preparation for connector OS authentication.

Add BlueXP Connector - Azure

More Information X

1 VM Authentication 2 Details 3 Network 4 Security Group 5 Review

Virtual Machine Authentication

You are logged in with Azure user: acao@netapp.com  Tenant: Hybrid Cloud TME 

Subscription: Hybrid Cloud TME Onprem

Location: South Central US

Resource Group: ANFAVSRG

Authentication Method: Public Key

User Name: azureuser

Enter SSH Public Key:  -----BEGIN RSA PRIVATE KEY----- MIIGSAIBAAKCA...

Previous Next 

6. Provide a name for the connector instance, select **Create** and accept default **Role Name** under **Details**, and choose the subscription for the Azure account.

Add BlueXP Connector - Azure

More Information X

VM Authentication Details Network Security Group Review

Details

Connector Instance Name: AzureConnector

Connector Role: Create

Add Tags to Connector Instance

Role Name: BlueXP Operator-5519248

Subscriptions to apply with the role: Hybrid Cloud TME Onprem

Previous Next



7. Configure networking with the proper **VNet**, **Subnet**, and disable **Public IP** but ensure that the connector has the internet access in your Azure environment.

Add BlueXP Connector - Azure

More Information X

VM Authentication Details Network Security Group Review

Network

<p>Connectivity</p> <p>VNet: ANFAVSVal</p> <p>Subnet: VM_Sub</p> <p>Public IP: Disable</p> <p><small>Notice: Ensure that the subnet has internet connectivity through a NAT device or proxy server so that the Connector can communicate with Azure services.</small></p>	<p>Proxy Configuration (Optional)</p> <p>HTTP Proxy: Example: http://172.16.254.1:8080</p> <p>Define Credentials for this Proxy</p> <p>Upload a root certificate</p>
--	---

Previous Next



8. Configure the **Security Group** for the connector that allows HTTP, HTTPS, and SSH access.

The screenshot shows the 'Add BlueXP Connector - Azure' interface at step 4: Security Group. The top navigation bar includes 'More Information' and a close button. Below it, tabs for 'VM Authentication', 'Details', 'Network', 'Security Group' (which is selected), and 'Review' are visible. The main area is titled 'Security Group' and contains instructions: 'The security group must allow inbound HTTP, HTTPS and SSH access.' A section titled 'Assign a security group:' offers two options: 'Create a new security group' (selected) and 'Select an existing security group'. Three panels define port configurations: 'HTTP (Port 80)', 'HTTPS (Port 443)', and 'SSH (Port 22)'. Each panel has a 'Source Type' dropdown set to 'Anywhere' and a 'Source (CIDR)' input field containing '0.0.0.0/0'. At the bottom are 'Previous' and 'Next' buttons, and a blue circular icon with a white envelope symbol.

9. Review the summary page and click **Add** to start connector creation. It generally takes about 10 mins to complete deployment. Once completed, the connector instance VM appears in the Azure portal.

Add BlueXP Connector - Azure

More Information X

VM Authentication ✓ Details ✓ Network ✓ Security Group 5 Review

Review

Code for Terraform Automation

BlueXP Connector Name	AzureConnector
Subscription	Hybrid Cloud TME Onprem
Location	South Central US
Resource Group	Existing - ANFAVSRG
Role	New - BlueXP Operator-5519248
Authentication Method	Password (user: azureuser)
VNet	ANFAVSVa1
Subnet	VM_Sub
Public IP	Enable
Proxy	None
Security Group	HTTP: 0.0.0.0/0, HTTPS: 0.0.0.0/0, SSH: 0.0.0.0/0

Previous Add



10. After the connector is deployed, the newly created connector appears under **Connector** drop-down.

NetApp BlueXP

Canvas My working environments My estate

+ Add Working Environment

Azure Blob Storage
20 Storage Accounts

Amazon S3
0 Buckets

Working Environments

Amazon S3
0 Buckets

Azure Blob Storage
20 Storage Accounts



Define a credential in BlueXP for Azure resources access

1. Click on setting icon on top right corner of BlueXP console to open **Account credentials** page, click **Add credentials** to start credential configuration workflow.

The screenshot shows the NetApp BlueXP interface. The top navigation bar includes 'NetApp BlueXP', 'BlueXP Search', 'Account Automation-team', 'Workspace Azure-DB', 'Connector AzureConnector', and various icons. On the left, there's a sidebar with icons for Cloud, Network, Compute, Storage, and Monitoring. The main content area is titled 'Credentials' with tabs for 'Account credentials' (selected), 'User credentials', and 'Add'. A message states: 'BlueXP and the Connector use account-level credentials to deploy and manage resources in your cloud environment.' Below this, there are three listed credentials:

- DemoFSxNCMCredentials**: Type: Assume Role | BlueXP, AWS Account ID: 982589175402, Role: DhruvCloudManagerRole
- shantanucreds**: Type: Assume Role | BlueXP, AWS Account ID: 210811600188, Role: nkarthik_kafka_nfs_role_FSSN
- Managed Service Identity**: Type: Managed Service Identity | Connector, Subscriptions: 1 View, Working Environments: 0

A red box highlights the 'Add' button at the bottom right of the credentials list. To the right, a sidebar titled 'Settings' shows sections for 'Connector Settings', 'Timeline', and 'Credentials' (which is also highlighted with a red box). Other sections include 'Software Update', 'HTTPS Setup', and 'Alerts and Notifications Settings'.

2. Choose credential location as - **Microsoft Azure - BlueXP**.

The screenshot shows the 'Add Credentials' wizard. The title bar says 'Add Credentials'. The first step, 'Choose Credentials Location', has two options: 'Microsoft Azure' (selected) and 'Amazon Web Services'. Below this, it says 'Choose how to associate the credentials' with two options: 'Connector' and 'BlueXP' (selected). A 'Next' button is at the bottom.

3. Define Azure credentials with proper **Client Secret**, **Client ID**, and **Tenant ID**, which should have been gathered during previous BlueXP onboarding process.

Add Credentials

Define Microsoft Azure Credentials

Credentials Name: Azure_Hybrid_TME

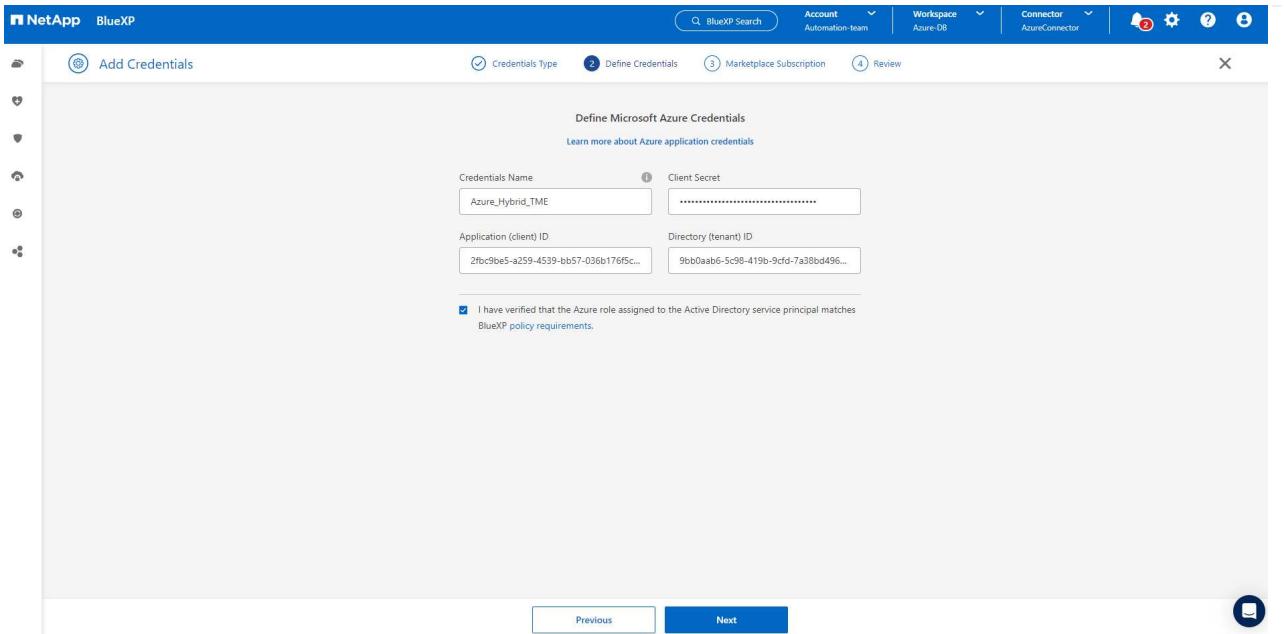
Client Secret:

Application (client) ID: 2fb9be5-a259-4539-bb57-036b176f5cc...

Directory (tenant) ID: 9bb0aab6-5c98-419b-9cf7-7a38bd496...

I have verified that the Azure role assigned to the Active Directory service principal matches BlueXP policy requirements.

Previous Next



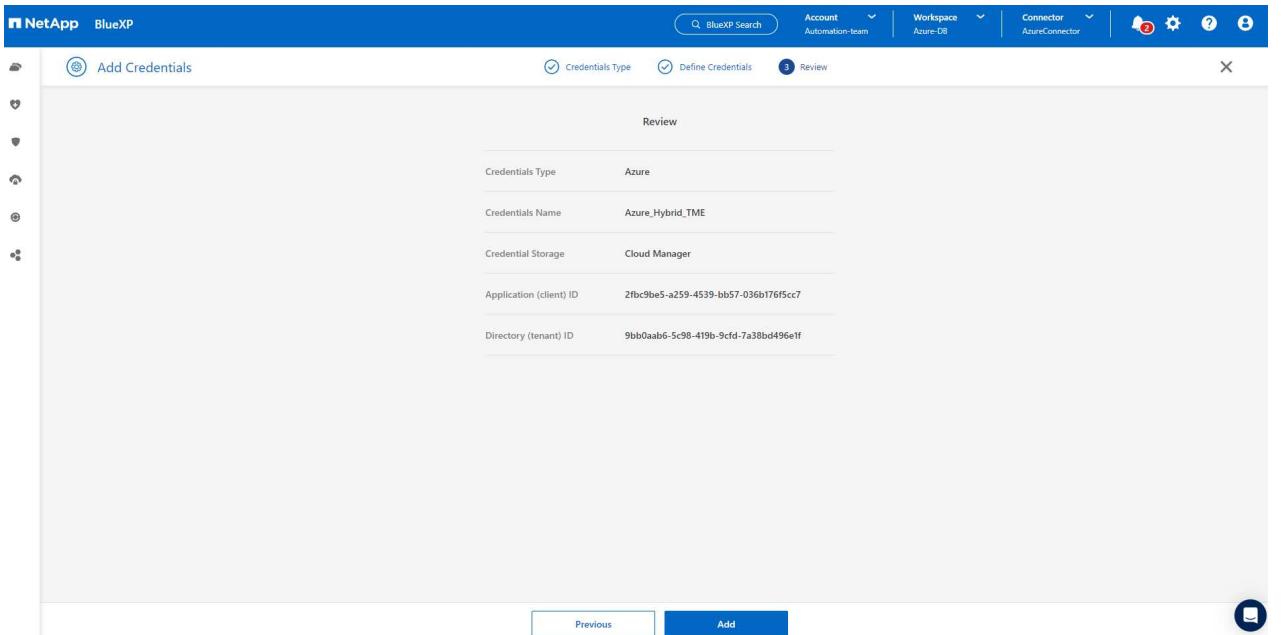
4. Review and Add.

Add Credentials

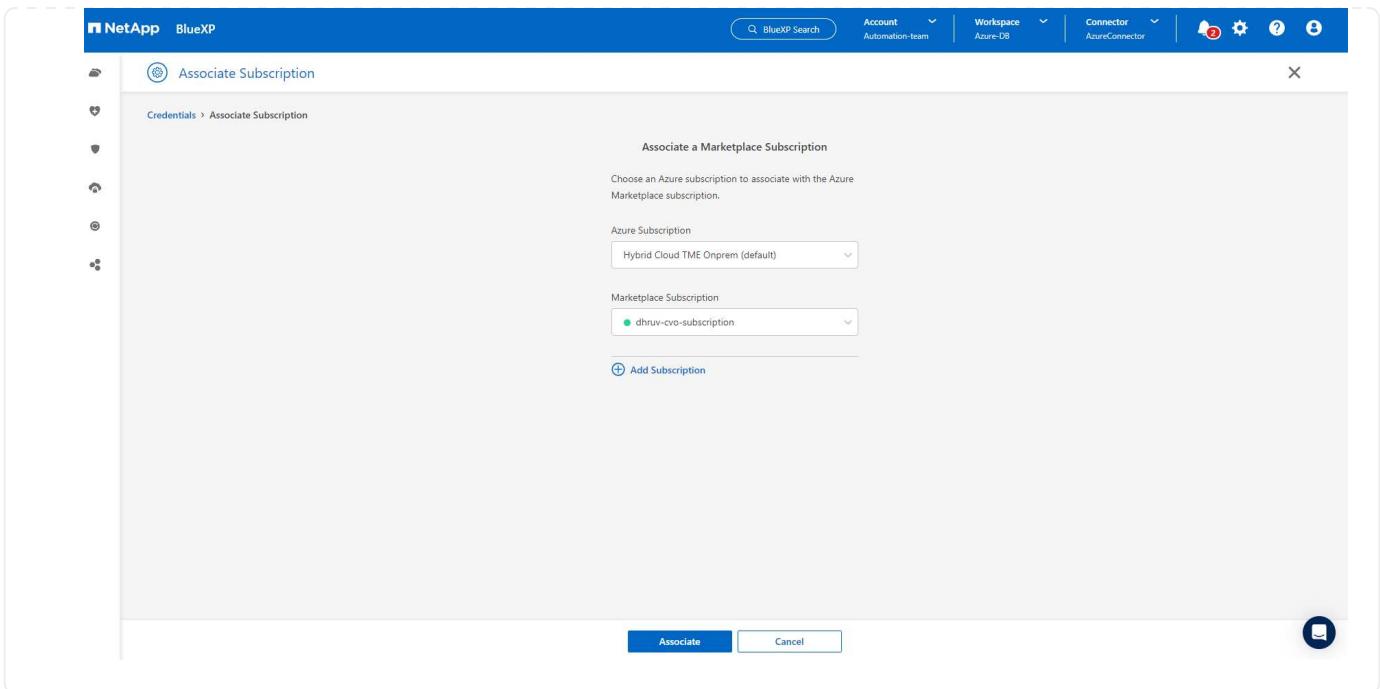
Review

Credentials Type	Azure
Credentials Name	Azure_Hybrid_TME
Credential Storage	Cloud Manager
Application (client) ID	2fb9be5-a259-4539-bb57-036b176f5cc7
Directory (tenant) ID	9bb0aab6-5c98-419b-9cf7-7a38bd496e1f

Previous Add



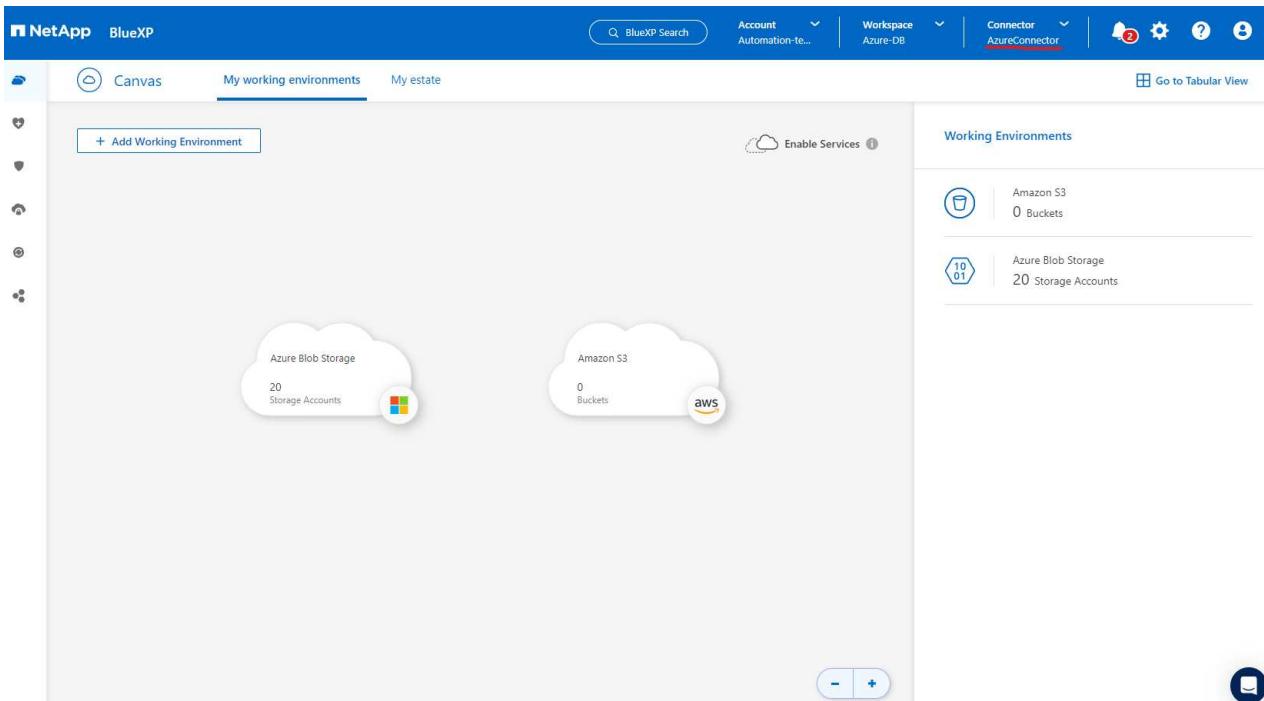
5. You may also need to associate a **Marketplace Subscription** with the credential.



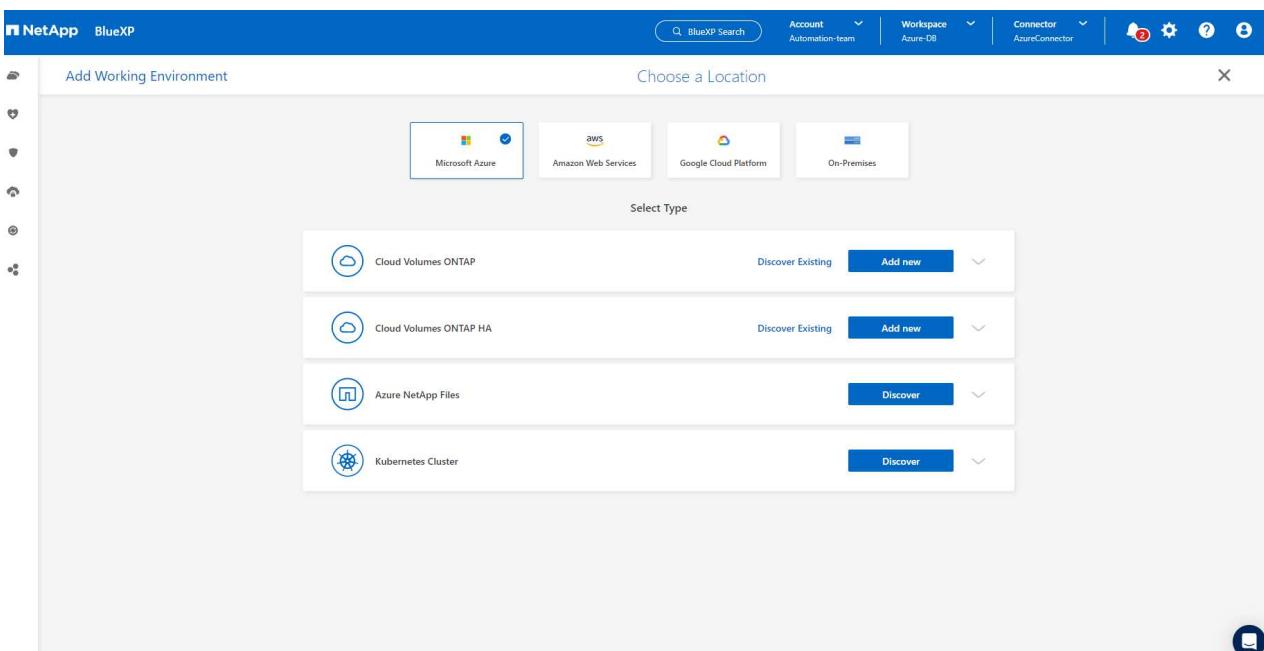
SnapCenter services setup

With the Azure credential configured, SnapCenter services can now be set up with the following procedures:

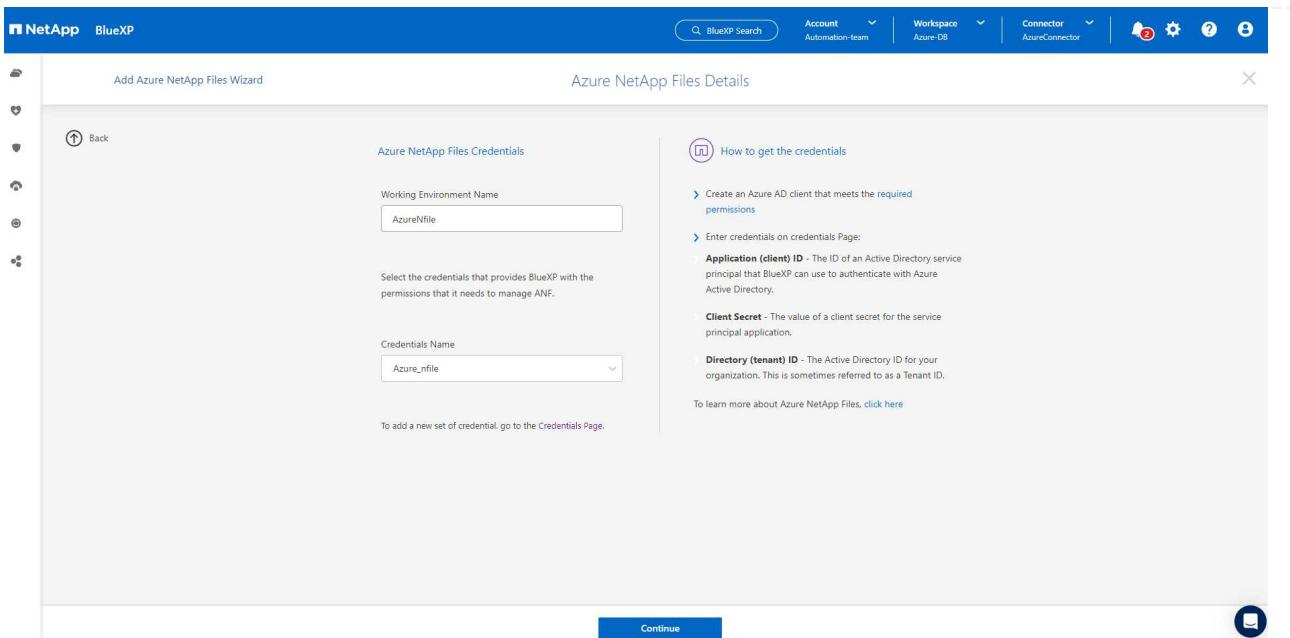
1. Back to Canvas page, from **My Working Environment** click **Add working Environment** to discover Azure NetApp Files deployed in Azure.



2. Choose **Microsoft Azure** as the location and click on **Discover**.



3. Name **Working Environment** and choose **Credential Name** created in previous section, and click **Continue**.



4. BlueXP console returns to **My working environments** and discovered Azure NetApp Files from Azure now appears on **Canvas**.

Canvas

My working environments

+ Add Working Environment

AzureNfile
Azure NetApp Files
16 Volumes | 7.08 TiB Capacity

Amazon S3
0 Buckets

Azure Blob Storage
20 Storage Accounts

Enable Services

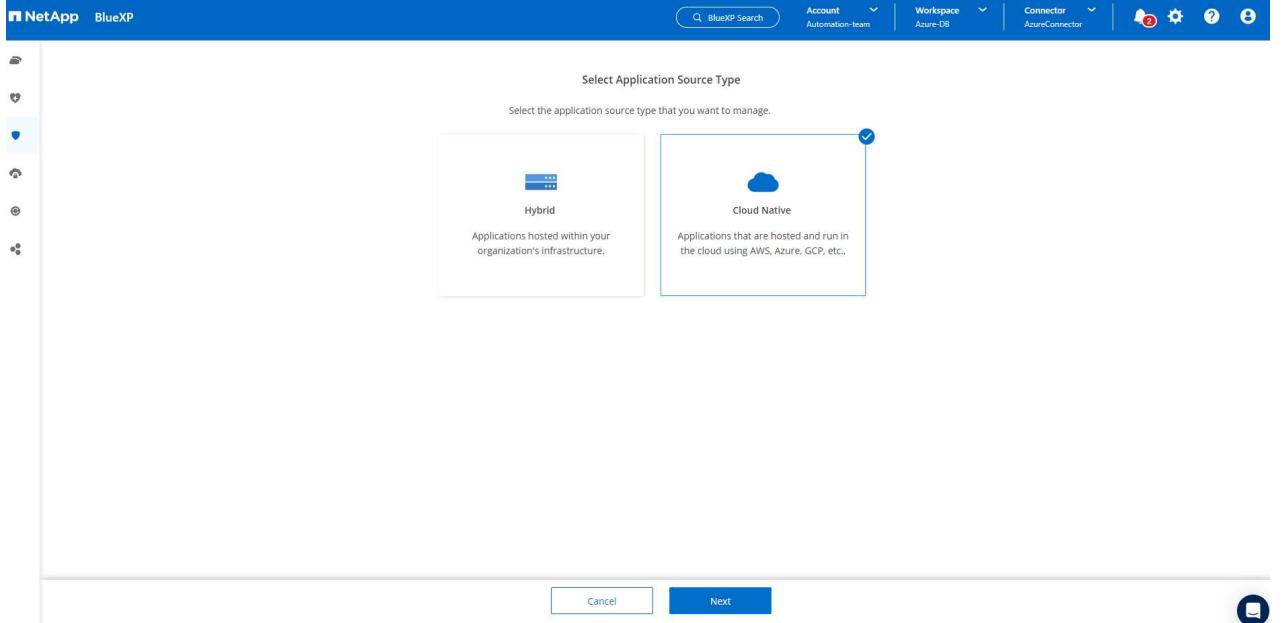
Working Environments

- 1 Azure NetApp Files
7.08 TiB Provisioned Capacity
- Amazon S3
0 Buckets
- Azure Blob Storage
20 Storage Accounts

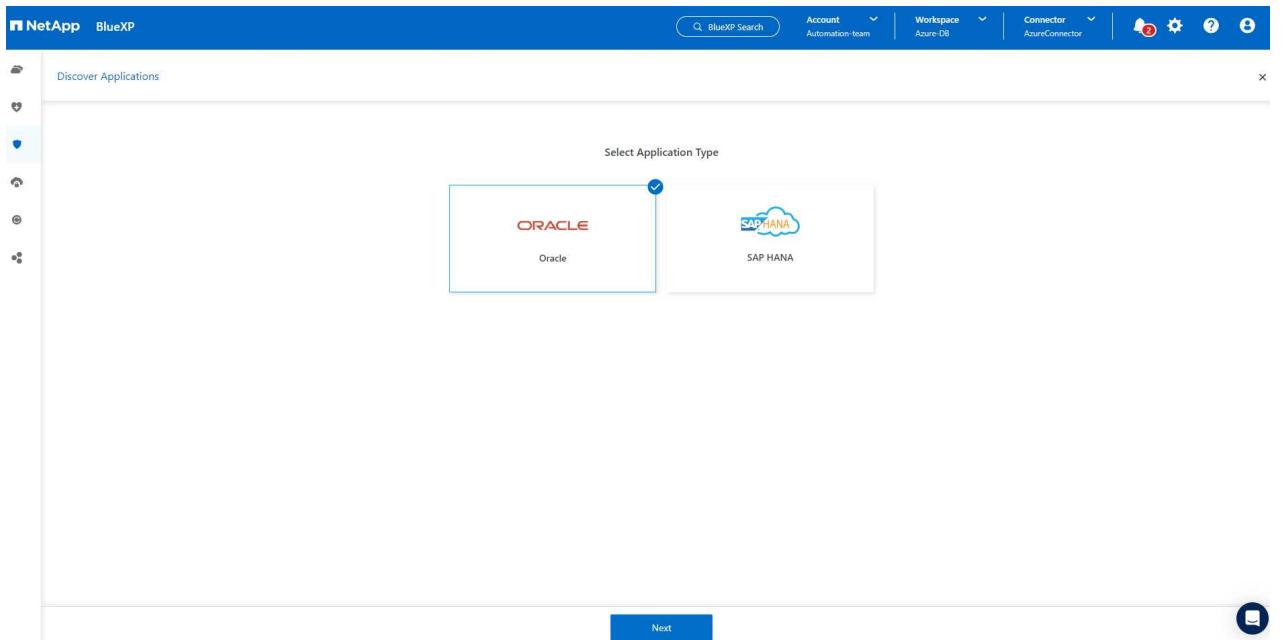
5. Click on **Azure NetApp Files** icon, then **Enter Working Environment** to view Oracle database volumes deployed in Azure NetApp Files storage.

- From the left-hand sidebar of the console, hover your mouse over the protection icon, and then click **Protection > Applications** to open the Applications launch page. Click **Discover Applications**.

- Select **Cloud Native** as the application source type.



8. Choose **Oracle** for the application type, click on **Next** to open host details page.



9. Select **Using SSH** and provide the Oracle Azure VM details such as **IP address**, **Connector**, Azure VM management **Username** such as azureuser. Click on **Add SSH Private Key** to paste in the SSH key pair that you used to deploy the Oracle Azure VM. You will also be prompted to confirm the fingerprint.

NetApp BlueXP

Discover Applications

Host Details Configuration Review

Select host type

Provide the following details to add host and discover applications

Host Installation Type Manual Using SSH

Host FQDN or IP: 172.30.137.142 Connector: AzureConnector

Username: azureuser

SSH Port: 22 Plug-in Port: 8145

Previous Next

Discover Applications

Host Details Configuration Review

Select host type

Provide the following details to add host and discover applications

Host Installation Type Manual Using SSH

Validate fingerprint

Algorithm: ssh-rsa

Fingerprint: AAAAE2VjZHNhLXN0YTltbmldHAYNTYAAAAbmldHAYNTYAAAB...

By proceeding further, I confirm that the above fingerprint for host is valid.

Proceed Cancel

Previous Next

10. Move on to next **Configuration** page to setup sudoer access on Oracle Azure VM.

Configuration

Follow the steps to make sure all the configuration expectations are met

1. Configure sudo access for "azureuser".
1. Log into the application host.
2. Create following file `/etc/sudoers.d/snapcenter` with the following content.

```
#  
# ======  
# ====== LINUX  
#===== #
```

I have configured sudo access for "azureuser" as per the above steps.

Previous Next

11. Review and click on **Discover Applications** to install a plugin on the Oracle Azure VM and discover Oracle database on the VM in one step.

Review

Follow the steps to make sure all the configuration expectations are met.

Host Details	Configurations
Host Installation Type	SSH
Host FQDN or IP	172.30.137.142
Connector	AzureConnector
User name (Sudo)	azureuser
Plug-in Port	8145
SSH Port	22
Fingerprint	AAAAAE2VjZHNhLXNoYTItbmIzdHayNTYAAAAlbmIzdH...
Key Type	ecdsa-sha2-nistp256

Previous Discover Applications

12. Discovered Oracle databases on Azure VM are added to **Applications**, and the **Applications** page lists the number of hosts and Oracle databases within the environment. The database **Protection Status** initially shows as **Unprotected**.

The screenshot shows the NetApp BlueXP application interface. At the top, there are navigation tabs: Backup and recovery, Volumes, Restore, Applications (which is selected), Virtual Machines, Kubernetes, Job Monitoring, and Reports. The top right includes search, account, workspace, and connector options. On the left, there's a sidebar with various icons. The main content area has dropdown filters for Cloud Native and Oracle. It displays three sections: Hosts (3), ORACLE (3), and Clone (0). Below this is an 'Application Protection' summary: 0 Protected and 3 Unprotected. A table titled '3 Databases' lists three entries: NTAP (Host Name: 172.30.137.142, Policy Name: Not Set, Protection Status: Unprotected), db1 (Host Name: 172.30.15.99, Policy Name: Not Set, Protection Status: Unprotected), and db1tst (Host Name: 172.30.15.124, Policy Name: Not Set, Protection Status: Unprotected). The table includes a search bar, a 'Manage Databases' button, and a settings dropdown.

This completes the initial setup of SnapCenter services for Oracle. The next three sections of this document describe Oracle database backup, restore, and clone operations.

Oracle database backup

1. Our test Oracle database in Azure VM is configured with three volumes with an aggregate total storage about 1.6 TiB. This gives context about the timing for the snapshot backup, restore, and clone of a database of this size.

```
[oracle@acao-ora01 ~]$ df -h
Filesystem           Size   Used  Avail Use% Mounted on
devtmpfs              7.9G    0    7.9G  0% /dev
tmpfs                 7.9G    0    7.9G  0% /dev/shm
tmpfs                 7.9G   17M  7.9G  1% /run
tmpfs                 7.9G    0    7.9G  0% /sys/fs/cgroup
/dev/mapper/rootvg-rootlv  40G   23G   15G  62% /
/dev/mapper/rootvg-usrlv  9.8G  1.6G   7.7G  18% /usr
/dev/sda2              496M  115M  381M  24% /boot
/dev/mapper/rootvg-varlv  7.9G  787M   6.7G  11% /var
/dev/mapper/rootvg-homelv 976M  323M  586M  36% /home
/dev/mapper/rootvg-optlv  2.0G  9.6M   1.8G  1% /opt
/dev/mapper/rootvg-tmplv  2.0G   22M   1.8G  2% /tmp
/dev/sdal               500M  6.8M  493M  2% /boot/efi
172.30.136.68:/ora01-u01 100G  23G   78G  23% /u01
172.30.136.68:/ora01-u03 500G  117G  384G  24% /u03
172.30.136.68:/ora01-u02 1000G 804G  197G  81% /u02
tmpfs                  1.6G    0    1.6G  0% /run/user/1000
[oracle@acao-ora01 ~]$
```

1. To protect database, click the three dots next to the database **Protection Status**, and then click **Assign Policy** to view the default preloaded or user defined database protection policies that can be applied to your Oracle databases. Under **Settings - Policies**, you have option to create your own policy with a customized backup frequency and backup data-retention window.

The screenshot shows the NetApp BlueXP interface under the Applications tab. It displays a summary of resources: 4 Hosts, 3 Oracle databases, and 0 Clones. In the Application Protection section, it shows 0 Protected and 3 Unprotected databases. Below this, a table lists three databases (NTAP, db1, db1tst) with their host names and current protection status (Unprotected). A context menu for the db1 database includes an option to 'Assign Policy'.

Name	Host Name	Policy Name	Protection Status
NTAP	172.30.137.142		Unprotected
db1	172.30.15.99		Unprotected
db1tst	172.30.15.124		Unprotected

- When you are happy with the policy configuration, you can then **Assign** your policy of choice to protect the database.

The screenshot shows the 'Assign Policy' dialog from the NetApp BlueXP Applications section. It lists four available policies for the database 'NTAP': 'Oracle Full Backup for Bronze', 'Oracle Full Backup for Gold', 'Oracle Full Backup for Silver', and 'my_full_bkup'. The 'my_full_bkup' policy is selected and highlighted with a checkmark. At the bottom, there are 'Cancel' and 'Assign' buttons.

Policy Name	Backup Type	Schedules
Oracle Full Backup for Bronze	FullBackup	Daily: Repeats Every 1 Day, Keeps 14 copies Weekly: Repeats Every Fri, Keeps 4 copies Monthly: Repeats Every 1st Day of Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, C
Oracle Full Backup for Gold	FullBackup	Hourly: Repeats Every 6 Hrs, Keeps 16 copies Daily: Repeats Every 1 Day, Keeps 30 copies Weekly: Repeats Every Fri, Keeps 4 copies Monthly: Repeats Every 1st Day of Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, C
Oracle Full Backup for Silver	FullBackup	Hourly: Repeats Every 12 Hrs, Keeps 6 copies Daily: Repeats Every 1 Day, Keeps 14 copies Weekly: Repeats Every Fri, Keeps 4 copies Monthly: Repeats Every 1st Day of Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, C
<input checked="" type="checkbox"/> my_full_bkup	FullBackup	Hourly: Repeats Every 6 Hrs, Keeps 3 Days

- After the policy is applied, the database protection status changed to **Protected** with a green check mark. BlueXP executes the snapshot backup according to the schedule defined. In addition, **ON-Demand Backup** is available from the three-dot drop down menu as shown below.

The screenshot shows the NetApp BlueXP interface with the Applications tab selected. In the top navigation bar, there are links for Volumes, Restore, Applications, Virtual Machines, Kubernetes, Job Monitoring, and Reports. The Applications section displays metrics for Cloud Native and Oracle environments. It shows 3 Hosts, 3 ORACLE databases, and 0 Clones. Under Application Protection, 1 database is Protected and 2 are Unprotected. Below this, a table lists three databases: NTAP, db1, and db1tst, along with their host names and protection status. A context menu is open for the db1 database, listing options like View Details, On-Demand Backup, Assign Policy, Un-assign Policy, and Restore.

- From **Job Monitoring** tab, backup job details can be viewed. Our test results showed that it took about 4 minutes to backup an Oracle database about 1.6 TiB.

The screenshot shows the NetApp BlueXP interface with the Job Monitoring tab selected. The top navigation bar includes links for Volumes, Restore, Applications, Virtual Machines, Kubernetes, Job Monitoring, and Reports. The Job Monitoring section displays a job history for a backup of the NTAP Oracle database. The job name is "Backup of NTAP oracle database on host 172.30.137.142 with policy my_full_bkup and schedule Hourly". The job ID is 61a12139-330e-4390-bca8-e7d15680869c. Below this, four summary icons are shown: Other Job Type, Start Time (Jul 11 2023, 2:17:53 pm), End Time (Jul 11 2023, 2:21:38 pm), and Success Job Status. A detailed table titled "Sub-Jobs(17)" lists the sub-jobs and their durations. One row, "Backup of NTAP oracle database on host 172.30...", has its duration of "4 Minutes" highlighted with a red box.

- From three-dot drop down menu **View Details**, you can view the backup sets created from snapshot backup.

The screenshot shows the NetApp BlueXP interface with the 'Applications' tab selected. In the top navigation bar, there are links for 'Cloud Native' and 'Oracle'. Below the navigation, there are summary counts for Hosts (4), ORACLE (3), and Clones (0). A 'Application Protection' box shows 2 Protected and 1 Unprotected databases. The main table lists three databases: NTAP, db1, and db1tst, each with its host name, policy name ('my_full_bkup'), and protection status (Protected or Unprotected). A context menu is open for the db1tst row, showing options like 'View Details', 'On-Demand Backup', 'Assign Policy', 'Un-assign Policy', and 'Restore'.

Name	Host Name	Policy Name	Protection Status
NTAP	172.30.137.142	my_full_bkup	Protected
db1	172.30.15.99	my_full_bkup	Protected
db1tst	172.30.15.124		Unprotected

6. Database backup details include the **Backup Name**, **Backup Type**, **SCN**, **RMAN Catalog**, and **Backup Time**. A backup set contains application-consistent snapshots for data volume and log volume respectively. A log volume snapshot takes place right after a database data volume snapshot. You could apply a filter if you are looking for a particular backup in the backup list.

The screenshot shows the 'Database Details' page for the NTAP database. It displays basic information such as the database name, protection status, policy names, host storage, connector ID, and RMAN catalog repository. Below this, a table lists 14 backups, showing columns for Backup Name, Backup Type, SCN, RMAN Catalog, and Backup Time. Each backup entry includes a 'Delete' link.

Backup Name	Backup Type	SCN	RMAN Catalog	Backup Time	Delete
my_full_bkup_Hourly_NTAP_2023_07_13_12_04_28_8376...	Log	29192187	Not Cataloged	Jul 13, 2023, 8:06:22 am	Delete
my_full_bkup_Hourly_NTAP_2023_07_13_12_03_07_4363...	Data	29192136	Not Cataloged	Jul 13, 2023, 8:03:40 am	Delete
my_full_bkup_Hourly_NTAP_2023_07_13_06_04_28_5618...	Log	29178022	Not Cataloged	Jul 13, 2023, 2:05:50 am	Delete
my_full_bkup_Hourly_NTAP_2023_07_13_06_03_03_6371...	Data	29177972	Not Cataloged	Jul 13, 2023, 2:03:43 am	Delete

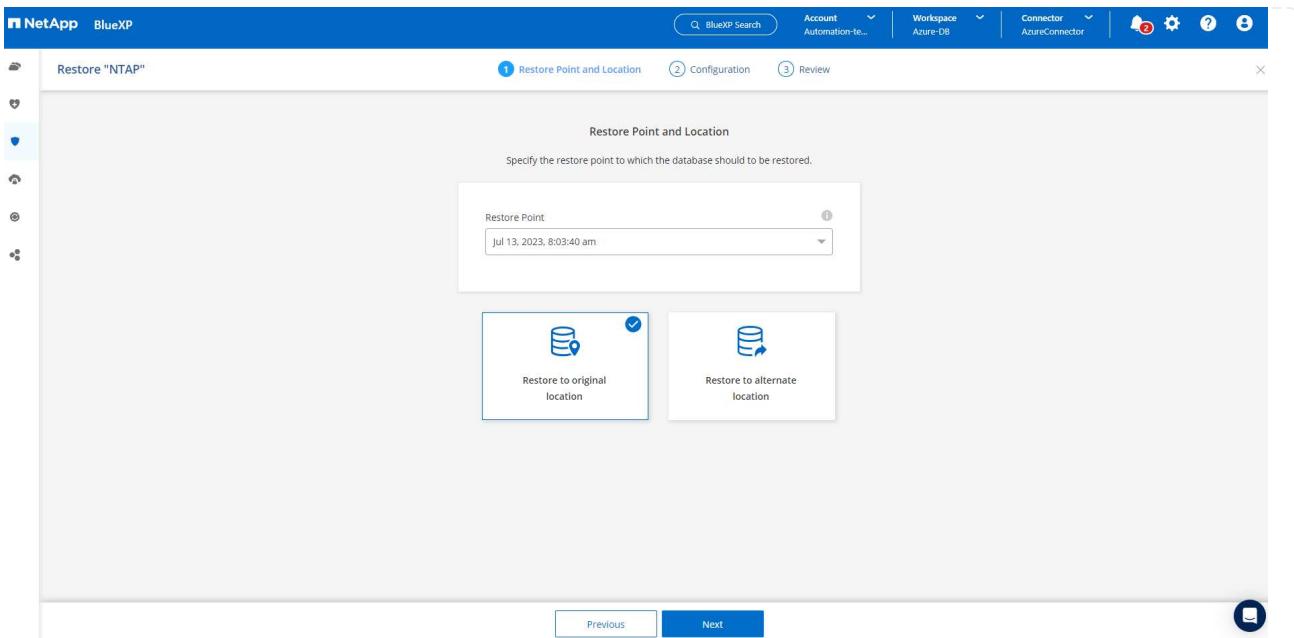
Oracle database restore and recovery

- For a database restore, click the three-dot drop down menu for the particular database to be restored in **Applications**, then click **Restore** to initiate database restore and recovery workflow.

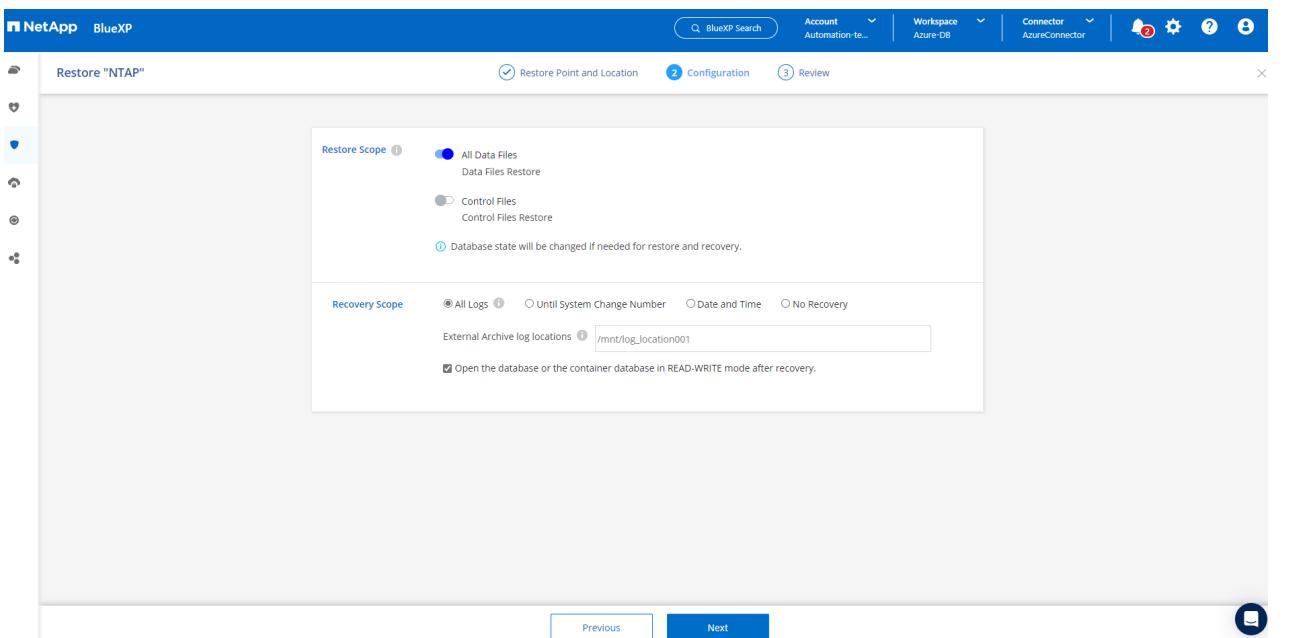
Name	Host Name	Policy Name	Protection Status
NTAP	172.30.137.142	my_full_bkup	Protected
db1	172.30.15.99	my_full_bkup	Protected
db1tst	172.30.15.124		Unprotected

- Choose your **Restore Point** by time stamp. Each time stamp in the list represents an available database backup set.

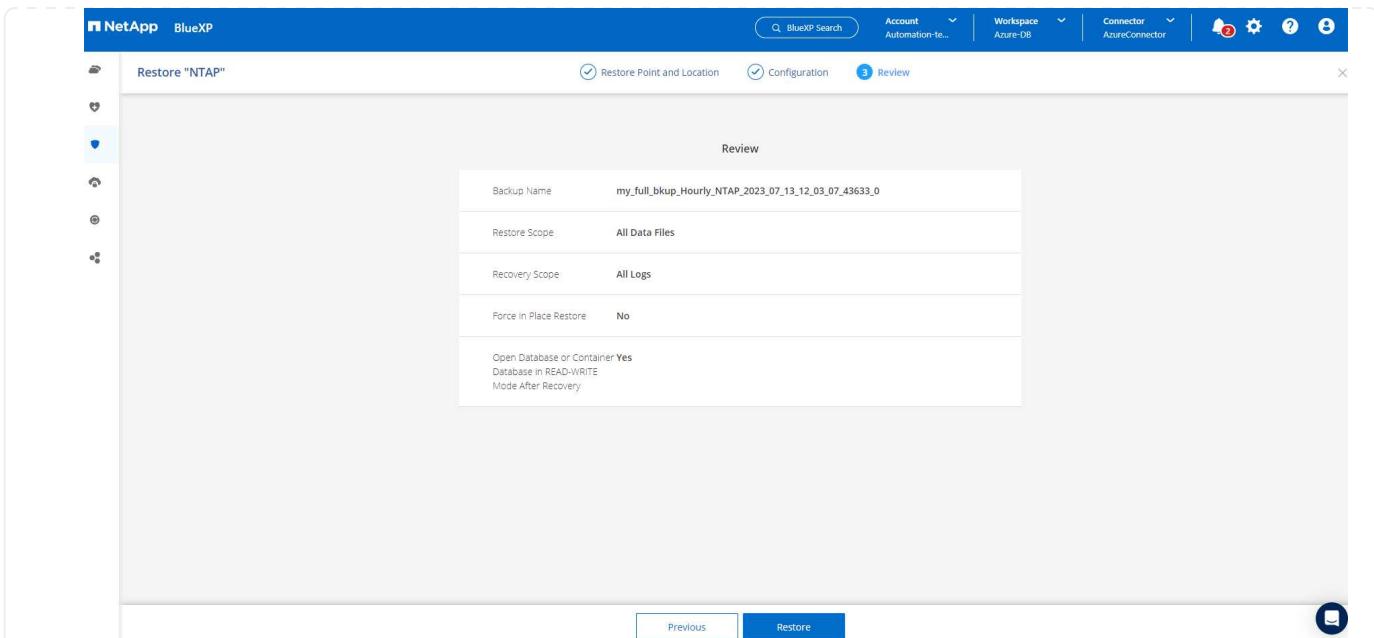
- Choose your **Restore Location** to **original location** for an Oracle database in place restore and recovery.



4. Define your **Restore Scope**, and **Recovery Scope**. All Logs mean a full recovery up to date including current logs.



5. Review and **Restore** to start database restore and recovery.



6. From the **Job Monitoring** tab, we observed that it took 2 minutes to run a full database restore and recovery up to date.

Job Name	Job ID	Start Time	End Time	Duration
Restore for Oracle Database NTAP using backup name my_full_bkup_Hourly_NTAP_2023_07_13_12_03_07_43633_0	80882740-952d-4acd-b868-9f279f830256	Jul 13 2023, 10:37:42 am	Jul 13 2023, 10:39:15 am	2 Minutes
Post Restore Cleanup	0533d58b-7750-40c1-a...	Jul 13 2023, 10:39:14 am	Jul 13 2023, 10:39:15 am	1 Second
Post Restore	64262431-041c-4c21-8d...	Jul 13 2023, 10:38:48 am	Jul 13 2023, 10:39:14 am	26 Seconds
Restore	918ad69-af04-417e-89...	Jul 13 2023, 10:38:24 am	Jul 13 2023, 10:38:48 am	24 Seconds

Oracle database clone

Database clone procedures are similar to restore but to an alternate Azure VM with identical Oracle software stack pre-installed and configured.



Ensure that your Azure NetApp File storage has sufficient capacity for a cloned database the same size as the primary database to be cloned. The alternate Azure VM has been added to **Applications**.

1. Click the three-dot drop down menu for the particular database to be cloned in **Applications**, then click **Restore** to initiate clone workflow.

The screenshot shows the NetApp BlueXP Applications interface. The top navigation bar includes Storage, Backup and recovery (selected), Volumes, Restore, Applications (selected), Virtual Machines, Kubernetes, Job Monitoring, and Reports. The left sidebar lists Health, Protection (selected), Backup and recovery, Governance, Mobility, and Extensions. The main content area displays Cloud Native and Oracle categories. Under Oracle, there are 4 Hosts, 3 ORACLE databases, and 0 Clones. An Application Protection summary shows 2 Protected and 1 Unprotected. Below this, a table lists 3 Databases: NTAP, db1, and db1tst, each with its host name, policy name (my_full_bkup), and protection status (Protected or Unprotected). A context menu is open for the db1tst database, with options for View Details, On-Demand Backup, Assign Policy, Un-assign Policy, and Restore. The 'Restore' option is highlighted in red.

2. Select the **Restore Point** and check the **Restore to alternate location**.

The screenshot shows the 'Restore "NTAP"' wizard, Step 1: Restore Point and Location. The top navigation bar includes a back arrow, Restore "NTAP", and three steps: 1. Restore Point and Location, 2. Configuration, 3. Review. The sidebar includes icons for Storage, Health, Protection, Backup and recovery, Governance, Mobility, and Extensions. The main content area is titled 'Restore Point and Location' and instructs to specify the restore point. A dropdown menu shows 'Jul 13, 2023, 8:03:40 am'. Below this, two options are shown: 'Restore to original location' and 'Restore to alternate location', with the latter being selected. At the bottom are 'Previous' and 'Next' buttons, and a feedback icon.

3. In the next **Configuration** page, set alternate **Host**, new database **SID**, and **Oracle Home** as configured at alternate Azure VM.

The screenshot shows the 'Configuration' step of a restore process. The 'Host' field is set to '172.30.137.147', the 'SID' field is 'NTAP1', and the 'Oracle Home' field is '/u01/app/oracle/product/19.0.0/clone'. There is an optional field for 'Maximum storage throughput (MiB/s)' with a placeholder 'Enter throughput (1-4500)'. Navigation buttons 'Previous' and 'Next' are at the bottom.

4. Review **General** page shows the details of cloned database such as SID, alternate host, data file locations, recovery scope etc.

General		Database parameters
Backup Name	my_full_bkup_Hourly_NTAP_2023_07_13_03_07_43633_0	
SID	NTAP1	
Host	172.30.137.147	
Datafile locations	/u02_NTAP1	
Control files	/u02_NTAP1/NTAP1/control/control01.ctl	
Redo logs	RedoGroup = 1 TotalSize = 1024 Path = /u02_NTAP1/NTAP1/redo redo01_01.log RedoGroup = 2 TotalSize = 1024 Path = /u02_NTAP1/NTAP1/redo redo02_01.log RedoGroup = 3 TotalSize = 1024 Path = /u02_NTAP1/NTAP1/redo redo03_01.log	
Recovery scope	Until cancel using selected backup's archive logs	
Recovery Point	Jul 13, 2023, 8:03:40 am	
Location	Alternate Location	

5. Review **Database parameters** page shows the details of cloned database configuration as well as some database parameters setting.

Restore "NTAP"

Review

General Database parameters

Database Credentials: None

Oracle home: /u01/app/oracle/product/19.0.0/clone

Oracle OS user: oracle

Oracle group: oinstall

DB parameters:

```

audit_file_dest = /u01/app/oracle/admin/NTAP/adump_NTAP1
audit_trail = DB
open_cursors = 300
pga_aggregate_target_in_mb = 512
processes = 320
remote_login_passwordfile = EXCLUSIVE
sga_target_in_mb = 9216
undo_tablespace = UNDOTBS1
  
```

Previous Restore

6. Monitor the cloning job status from the **Job Monitoring** tab, we observed that it took 8 minutes to clone a 1.6 TiB Oracle database.

Backup and recovery Volumes Restore Applications Virtual Machines Kubernetes Job Monitoring Reports

Job Name: Restore Oracle Database NTAP as NTAP1 on host 172.30.137.147 using backup my_full_bkup_Hourly_NTAP_2023_07_13_12_03_07_43633_0

Job Name: Restore Oracle Database NTAP as NTAP1 on host 172.30.137.147 using backup my_full_bkup_Hourly...

Job Id: 7a187d5a-7f7e-461a-83b3-48e37fbf890f

Other Job Type	Jul 13 2023, 1:05:02 pm Start Time	Jul 13 2023, 1:13:15 pm End Time	Success Job Status	
Sub-Jobs(6)				
Job Name	Job ID	Start Time	End Time	Duration
Restore Oracle Database NTAP as NTAP1 on ho...	7a187d5a-7f7e-461a-83...	Jul 13 2023, 1:05:02 pm	Jul 13 2023, 1:13:15 pm	8 Minutes
Collect the restore database job logs of...	abc9342a-5777-4262-b...	Jul 13 2023, 1:13:14 pm	Jul 13 2023, 1:13:14 pm	0 Second
Register the restored database metadata	15aefb90-b21b-418f-b0...	Jul 13 2023, 1:12:30 pm	Jul 13 2023, 1:12:30 pm	0 Second
Remove the temporary storage of the I...	cc106fb9-7555-46c8-9c...	Jul 13 2023, 1:12:30 pm	Jul 13 2023, 1:13:14 pm	44 Seconds

7. Validate the cloned database in BlueXP **Applications** page that showed the cloned database was immediately registered with BlueXP.

The screenshot shows the NetApp BlueXP interface with the Applications tab selected. A search bar at the top right contains 'BlueXP Search'. The main dashboard displays application protection statistics: 4 Hosts, 4 ORACLE, and 0 Clones. In the Application Protection section, 2 databases are Protected and 2 are Unprotected. Below this, a table lists four databases:

Name	Host Name	Policy Name	Protection Status
NTAP	172.30.137.142	my_full_bkup	Protected
NTAP1	172.30.137.147		Unprotected
db1	172.30.15.99	my_full_bkup	Protected
db1tst	172.30.15.124		Unprotected

Page navigation at the bottom indicates 1 - 4 of 4.

8. Validate the cloned database on the Oracle Azure VM that showed the cloned database was running as expected.

```
[oracle@acao-ora02 admin]$ cat /etc/oratab
#
#
# This file is used by ORACLE utilities. It is created by root.sh
# and updated by either Database Configuration Assistant while creating
# a database or ASM Configuration Assistant while creating ASM instance.
#
# A colon, ':', is used as the field terminator. A new line terminates
# the entry. Lines beginning with a pound sign, '#', are comments.
#
# Entries are of the form:
# $ORACLE_SID:$ORACLE_HOME:<N|Y>:
#
# The first and second fields are the system identifier and home
# directory of the database respectively. The third field indicates
# to the dbstart utility that the database should , "Y", or should not,
# "N", be brought up at system boot time.
#
# Multiple entries with the same $ORACLE_SID are not allowed.
#
#
# SnapCenter Plug-in for Oracle Database generated entry (DO NOT REMOVE THIS LINE)
NTAP1:/u01/app/oracle/product/19.0.0/clone:N
[oracle@acao-ora02 admin]$ export ORACLE_SID=NTAP1
[oracle@acao-ora02 admin]$ export ORACLE_HOME=/u01/app/oracle/product/19.0.0/clone
[oracle@acao-ora02 admin]$ export PATH=$PATH:$ORACLE_HOME/bin
[oracle@acao-ora02 admin]$ sqlplus / as sysdba

SQL*Plus: Release 19.0.0.0.0 - Production on Thu Jul 13 17:16:31 2023
Version 19.18.0.0.0

Copyright (c) 1982, 2022, Oracle. All rights reserved.

Connected to:
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.18.0.0.0

SQL> select name, open_mode, log_mode from v$database;

NAME        OPEN_MODE          LOG_MODE
-----  -----
NTAP1      READ WRITE        NOARCHIVELOG
```

This completes the demonstration of an Oracle database backup, restore, and clone in Azure with NetApp BlueXP console using SnapCenter Service.

Additional information

To learn more about the information that is described in this document, review the following documents and/or websites:

- Set up and administer BlueXP

<https://docs.netapp.com/us-en/cloud-manager-setup-admin/index.html>

- BlueXP backup and recovery documentation

<https://docs.netapp.com/us-en/cloud-manager-backup-restore/index.html>

- Azure NetApp Files

<https://azure.microsoft.com/en-us/products/netapp>

- Get started with Azure

<https://azure.microsoft.com/en-us/get-started/>

TR-4964: Oracle Database backup, restore and clone with SnapCenter Services - AWS

Allen Cao, Niyaz Mohamed, NetApp

Purpose

SnapCenter Services is the SaaS version of the classic SnapCenter database management UI tool that is available through the NetApp BlueXP cloud management console. It is an integral part of the NetApp cloud-backup, data-protection offering for databases such as Oracle and HANA running on NetApp cloud storage. This SaaS-based service simplifies traditional SnapCenter standalone server deployment that generally requires a Windows server operating in a Windows domain environment.

In this documentation, we demonstrate how you can set up SnapCenter Services to backup, restore, and clone Oracle databases deployed to Amazon FSx for ONTAP storage and EC2 compute instances. Although it is much easier to set up and use, SnapCenter Services deliver key functionalities that are available in the legacy SnapCenter UI tool.

This solution addresses the following use cases:

- Database backup with snapshots for Oracle databases hosted in Amazon FSx for ONTAP
- Oracle database recovery in the case of a failure
- Fast and storage-efficient cloning of primary databases for a dev/test environment or other use cases

Audience

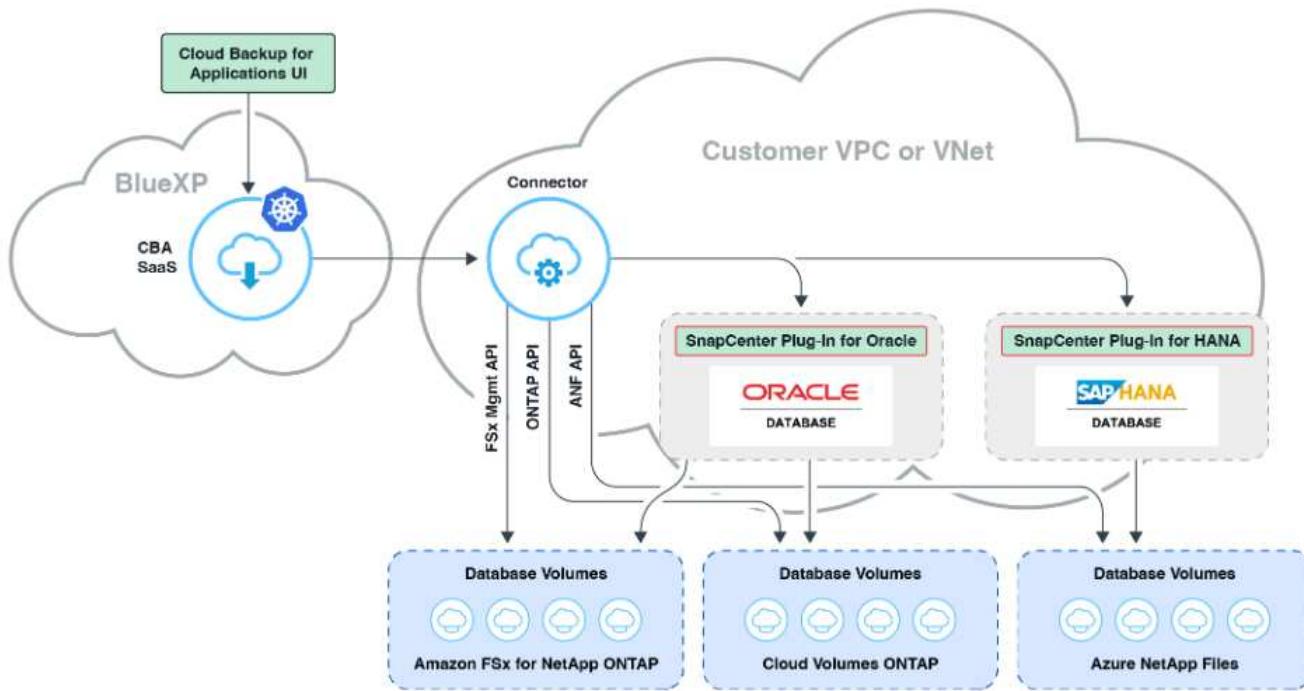
This solution is intended for the following audiences:

- The DBA who manages Oracle databases running on Amazon FSx for ONTAP storage
- The solution architect who is interested in testing Oracle database backup, restore, and clone in the public AWS cloud
- The storage administrator who supports and manages the Amazon FSx for ONTAP storage
- The application owner who owns applications that are deployed to Amazon FSx for ONTAP storage

Solution test and validation environment

The testing and validation of this solution was performed in an AWS FSx and EC2 environment that might not match the final deployment environment. For more information, see the section [\[Key Factors for Deployment Consideration\]](#).

Architecture



This image provides a detailed picture of BlueXP backup and recovery for applications within the BlueXP console, including the UI, the connector, and the resources it manages.

Hardware and software components

Hardware

FSx ONTAP storage	Current version offered by AWS	One FSx HA cluster in the same VPC and availability zone
EC2 instance for compute	t2.xlarge/4vCPU/16G	Two EC2 T2 large EC2 instances, one as primary DB server and the other as clone DB server

Software

RedHat Linux	RHEL-8.6.0_HVM-20220503-x86_64-2-Hourly2-GP2	Deployed RedHat subscription for testing
Oracle Grid Infrastructure	Version 19.18	Applied RU patch p34762026_190000_Linux-x86-64.zip
Oracle Database	Version 19.18	Applied RU patch p34765931_190000_Linux-x86-64.zip
Oracle OPatch	Version 12.2.0.1.36	Latest patch p6880880_190000_Linux-x86-64.zip
SnapCenter Service	Version	v2.3.1.2324

Key factors for deployment consideration

- **Connector to be deployed in the same VPC as database and FSx.** When possible, the connector should be deployed in the same AWS VPC, which enables connectivity to the FSx storage and the EC2 compute instance.
- **An AWS IAM policy created for SnapCenter connector.** The policy in JSON format is available in the detailed SnapCenter service documentation. When you launch connector deployment with the BlueXP console, you are also prompted to set up the prerequisites with details of required permission in JSON format. The policy should be assigned to the AWS user account that owns the connector.
- **The AWS account access key and the SSH key pair created in the AWS account.** The SSH key pair is assigned to the ec2-user for logging into the connector host and then deploying a database plug-in to the EC2 DB server host. The access key grants permission for provisioning the required connector with IAM policy above.
- **A credential added to the BlueXP console setting.** To add Amazon FSx for ONTAP to the BlueXP working environment, a credential that grants BlueXP permissions to access Amazon FSx for ONTAP is set up in the BlueXP console setting.
- **java-11-openjdk installed on the EC2 database instance host.** SnapCenter service installation requires java version 11. It needs to be installed on application host before plugin deployment attempt.

Solution deployment

There is extensive NetApp documentation with a broader scope to help you protect your cloud-native application data. The goal of this documentation is to provide step-by-step procedures that cover SnapCenter Service deployment with the BlueXP console to protect your Oracle database deployed to Amazon FSx for ONTAP and an EC2 compute instance. This document fills in certain details that might be missing from more general instructions.

To get started, complete the following steps:

- Read the general instructions [Protect your cloud native applications data](#) and the sections related to Oracle and Amazon FSx for ONTAP.
- Watch the following video walkthrough.

[Solution Deployment](#)

Prerequisites for SnapCenter service deployment

Deployment requires the following prerequisites.

1. A primary Oracle database server on an EC2 instance with an Oracle database fully deployed and running.
2. An Amazon FSx for ONTAP cluster deployed in AWS that is hosting the database volumes above.
3. An optional database server on an EC2 instance that can be used for testing the cloning of an Oracle database to an alternate host for the purpose of supporting a dev/test workload or any use cases that require a full data set of a production Oracle database.
4. If you need help to meet the above prerequisites for Oracle database deployment on Amazon FSx for ONTAP and EC2 compute instance, see [Oracle Database Deployment and Protection in AWS FSx/EC2 with iSCSI/ASM](#) or white paper [Oracle Database Deployment on EC2 and FSx Best Practices](#)
5. If you need help to meet the above prerequisites for Oracle database deployment on Amazon FSx for ONTAP and EC2 compute instance, see [Oracle Database Deployment and Protection in AWS FSx/EC2 with iSCSI/ASM](#) or white paper [Oracle Database Deployment on EC2 and FSx Best Practices](#)

Onboarding to BlueXP preparation

1. Use the link [NetApp BlueXP](#) to sign up for BlueXP console access.
2. Login to your AWS account to create an IAM policy with proper permissions and assign the policy to the AWS account that will be used for BlueXP connector deployment.

The screenshot shows the AWS IAM Policies Summary page. The left sidebar navigation includes: Dashboard, Access management (User groups, Users, Roles), Policies (Identity providers, Account settings), Access reports (Access analyzer, Archive rules, Analyzers, Settings), Credential report, Organization activity, and Service control policies (SCPs). A search bar for IAM is also present. The main content area shows a policy named "snapcenter" with the following details:

- Policy ARN:** arn:aws:iam::541696183547:policy/snapcenter
- Description:** Policy to grant snapcenter service permission to create connector in AWS.

The "Permissions" tab is selected, showing the JSON code for the policy:

```

1+ {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Action": [
7         "iam:CreateRole",
8         "iam:DeleteRole",
9         "iam:PutRolePolicy",
10        "iam:CreateInstanceProfile",
11        "iam:DeleteRolePolicy",
12        "iam:AddRoleToInstanceProfile",
13        "iam:RemoveRoleFromInstanceProfile",
14        "iam:DeleteInstanceProfile",
15        "iam:PassRole",
16        "iam>ListRoles",
17        "ec2:DescribeInstanceStatus",
18        "ec2:RunInstances",
19        "ec2:ModifyInstanceAttribute",
20        "ec2>CreateSecurityGroup",
21        "ec2:DeleteSecurityGroup",
22        "ec2:DescribeSecurityGroups",
23        "ec2:RevokeSecurityGroupEgress",
24        "ec2:AuthorizeSecurityGroupEgress",
25        "ec2:AuthorizeSecurityGroupIngress",
26        "ec2:RevokeSecurityGroupIngress",
27        "ec2>CreateNetworkInterface",
28        "ec2:DescribeNetworkInterface"
29      ]
30    }
31  ]
32}

```

The policy should be configured with a JSON string that is available in NetApp documentation. The JSON string can also be retrieved from the page when connector provisioning is launched and you are prompted for the prerequisites permissions assignment.

3. You also need the AWS VPC, subnet, security group, an AWS user account access key and secrets, an SSH key for ec2-user, and so on ready for connector provisioning.

Deploy a connector for SnapCenter services

1. Login to the BlueXP console. For a shared account, it is a best practice to create an individual workspace by clicking **Account > Manage Account > Workspace** to add a new workspace.

Manage Account: Automation-team

Overview Members Workspaces BlueXP Connector X

Manage the BlueXP connector Workspaces

+ Add New Workspace

Database	X Edit
Database-2	X Edit
sufians-k8	X Edit
Workspace-1	X Edit

2. Click **Add a Connector** to launch the connector provisioning workflow.

NetApp Cloud Manager

Account: Automation-team | Workspace: new-workspace | Connector: N/A | Notifications | Settings | Help | User

Backup & Restore Volumes Restore Applications Virtual Machines Kubernetes Job Monitoring

Backup & Restore

Fully integrated data protection for ONTAP anywhere

Cloud Backup dramatically reduces the complexity of backing up critical structured and unstructured data across your ONTAP hybrid cloud environments to cost-effective object storage. All you need to do is select the source, the target and the protection policy and you're protected

To start your Backup & Restore experience, please deploy our connector

Add a Connector

Simple & intuitive

No backup or cloud expertise required. Simply click the button above and follow the instructions

Hybrid Multicloud

Backup from On-premises or Cloud Volumes ONTAP to AWS, Azure, GCP or StorageGRID

Unmatched Efficiency

Combines incremental, block-level operation with storage efficiencies to reduce time and costs

1. Choose your cloud provider (in this case, **Amazon Web Services**).

Add Connector

X

Provider

Choose the cloud provider where you want to run the Connector:



Microsoft Azure



Amazon Web Services



Google Cloud Platform

Continue

Feedback

1. Skip the **Permission**, **Authentication**, and **Networking** steps if you already have them set up in your AWS account. If not, you must configure these before proceeding. From here, you could also retrieve the permissions for the AWS policy that is referenced in the previous section "[Onboarding to BlueXP preparation](#)."

Deploying a Connector

The Connector is a crucial component for the day-to-day use of Cloud Manager. It's used to connect Cloud Manager's services to your hybrid-cloud environments. The Connector can then manage the resources and processes within your public cloud environment.

Before you begin the deployment process, ensure that you have completed the required preparations. This guide will enable you to focus on the minimum requirements for Connector installation.

Permissions

Set up an IAM role with the required permissions

Authentication

Choose between two AWS authentication methods: AWS keys or assuming an IAM role

Networking

Obtain details about the VPC and subnet in which the Connector will reside

[Skip to Deployment](#)

[Previous](#)

[Continue](#)



1. Enter your AWS account authentication with **Access Key** and **Secret Key**.

[1 AWS Credentials](#)

[2 Details](#)

[3 Network](#)

[4 Security Group](#)

[5 Review](#)

AWS Authentication

Region

us-east-1 | US East (N. Virginia)

Select the Authentication Method:

Assume Role

AWS Keys

AWS Access Key

AKIA6JRXA6ZVGVFSHMO3

AWS Secret Key

.....

Want to launch an instance without AWS Credentials? ▾

[Previous](#)

[Next](#)



2. Name the connector instance and select **Create Role** under **Details**.

Add Connector - AWS

More Information 

1 AWS Credentials 2 Details 3 Network 4 Security Group 5 Review

Details

Connector Instance Name  SnapCenterSvs

Connector Role 
 Create Role Select an existing Role

Role Name  Cloud-Manager-Operator-VZzSSP9-SnapCenter

 AWS Managed Encryption 

Master Key: aws/ebs (default) [Change Key](#)

 Add Tags to Connector Instance

[Previous](#) [Next](#) 

1. Configure networking with the proper **VPC**, **Subnet**, and **SSH Key Pair** for connector access.

Add BlueXP Connector - AWS

More Information X

AWS Credentials Details Network Security Group Review

Network

Connectivity

VPC:

Subnet:

Key Pair:

Public IP:

Proxy Configuration (Optional)

HTTP Proxy:

Define Credentials for this Proxy:

Upload a root certificate:

Notice: Ensure that the subnet has internet connectivity through a NAT device or proxy server so that the Connector can communicate with AWS services.

Previous Next



2. Set the **Security Group** for the connector.

Add BlueXP Connector - AWS

More Information X

AWS Credentials Details Network Security Group Review

Security Group

The security group must allow inbound HTTP, HTTPS and SSH access.

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

Security Group Name	Description
default	default VPC security group

1 Security Group

Previous Next



3. Review the summary page and click **Add** to start connector creation. It generally takes about 10 mins to complete deployment. Once completed, the connector instance appears in the AWS EC2 dashboard.

Add BlueXP Connector - AWS

More Information X

AWS Credentials ✓ Details ✓ Network ✓ Security Group ✓ Review 5

Review

Code for Terraform Automation

BlueXP Connector Name	aws-snapctr-us-east
AWS Access Key	AKIAJ4H43ZT56IWWR3TI
Region	us-east-1
VPC	vpc-0b522d5e982a50ceb - 172.30.15.0/25
Subnet	172.30.15.0/25 priv-subnet-01
Key Pair	sufi_new
Public IP	Use subnet settings (Disable)
Proxy	None
Security Group	default

Previous Add S

Define a credential in BlueXP for AWS resources access

- First, from AWS EC2 console, create a role in **Identity and Access Management (IAM)** menu **Roles**, **Create role** to start role creation workflow.

The screenshot shows the AWS IAM Roles list page. The left sidebar includes sections for Access management (User groups, Users, Roles, Policies, Identity providers, Account settings) and Access reports (Access analyzer, Archive rules, Analyzers, Settings, Credential report, Organization activity, Service control policies (SCPs)). Below these are Related consoles for IAM Identity Center and AWS Organizations. The main content area displays a table of roles with columns for Role name, Trusted entities, Last activity, and a 'Create role' button at the top right. The table lists numerous roles, including AmazonEC2RoleForLaunchWizard, AmazonSSMRoleForInstancesQuickSetup, aws-controltower-AdministratorExecutionRole, and several AWS-Reserved-SSO roles.

- In **Select trusted entity** page, choose **AWS account**, **Another AWS account**, and paste in the BlueXP account ID, which can be retrieved from BlueXP console.

The screenshot shows the 'Select trusted entity' step in the IAM 'Create role' wizard. It has three steps: Step 1 (Select trusted entity), Step 2 (Add permissions), and Step 3 (Name, review, and create). The 'Trusted entity type' section shows four options: AWS service (selected), AWS account (selected), Web identity, and SAML 2.0 federation. The 'An AWS account' section shows 'This account (541696183547)' selected. The 'Options' section includes 'Require external ID' (selected), 'Require MFA' (unchecked), and 'Requires that the assuming entity use multi-factor authentication' (unchecked). At the bottom are 'Cancel' and 'Next' buttons.

- Filter permission policies by fsx and add **Permissions policies** to the role.

Step 1
Select trusted entity

Step 2
Add permissions

Step 3
Name, review, and create

Permissions policies (Selected 1/889) Choose one or more policies to attach to your new role.

Filter policies by property or policy name and press enter. 4 matches

Clear filters

Policy name	Type	Description
AmazonFSxReadOnlyAccess	AWS managed	Provides read only access to Amazon FSx.
AmazonFSxFullAccess	AWS managed	Provides full access to Amazon FSx and access to related AWS services.
AmazonFSxConsoleReadOnlyAccess	AWS managed	Provides read only access to Amazon FSx and access to related AWS services via the AWS Management Console.
AmazonFSxConsoleFullAccess	AWS managed	Provides full access to Amazon FSx and access to related AWS services via the AWS Management Console.

Set permissions boundary - optional Set a permissions boundary to control the maximum permissions this role can have. This is not a common setting, but you can use it to delegate permission management to others.

Cancel Previous Next

4. In **Role details** page, name the role, add a description, then click **Create role**.

Step 1
Select trusted entity

Step 2
Add permissions

Step 3
Name, review, and create

Name, review, and create

Role details

Role name
Enter a meaningful name to identify this role.
fsxn_bluexp

Maximum 64 characters. Use alphanumeric and '+-,._-' characters.

Description
Add a short explanation for this role.
Grant permission for BlueXP access to FSxN in AWS.

Maximum 1000 characters. Use alphanumeric and '+-,._-' characters.

Step 1: Select trusted entities

```

1 - [
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Action": "sts:AssumeRole",
7       "Principal": {
8         "AWS": "052013314444"
9       },
10      "Condition": {}
11    }
12  ]
13 ]

```

5. Back to BlueXP console, click on setting icon on top right corner of the console to open **Account credentials** page, click **Add credentials** to start credential configuration workflow.

NetApp BlueXP

Credentials Account credentials User credentials

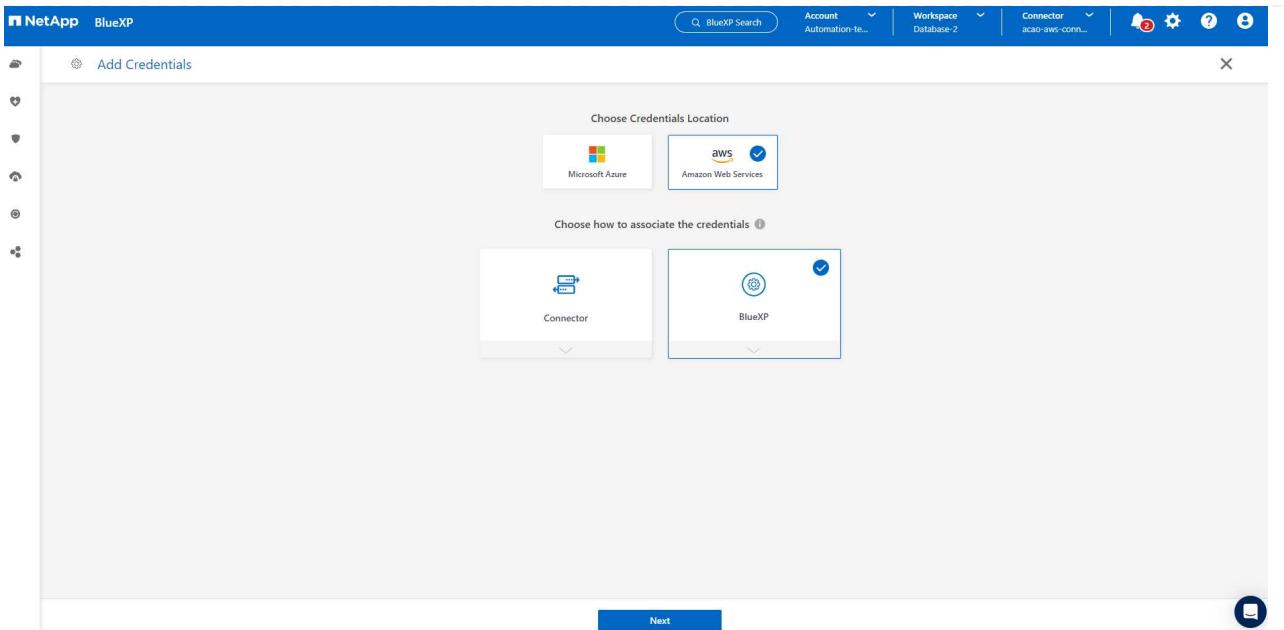
BlueXP and the Connector use account-level credentials to deploy and manage resources in your cloud environment.

5 Credentials

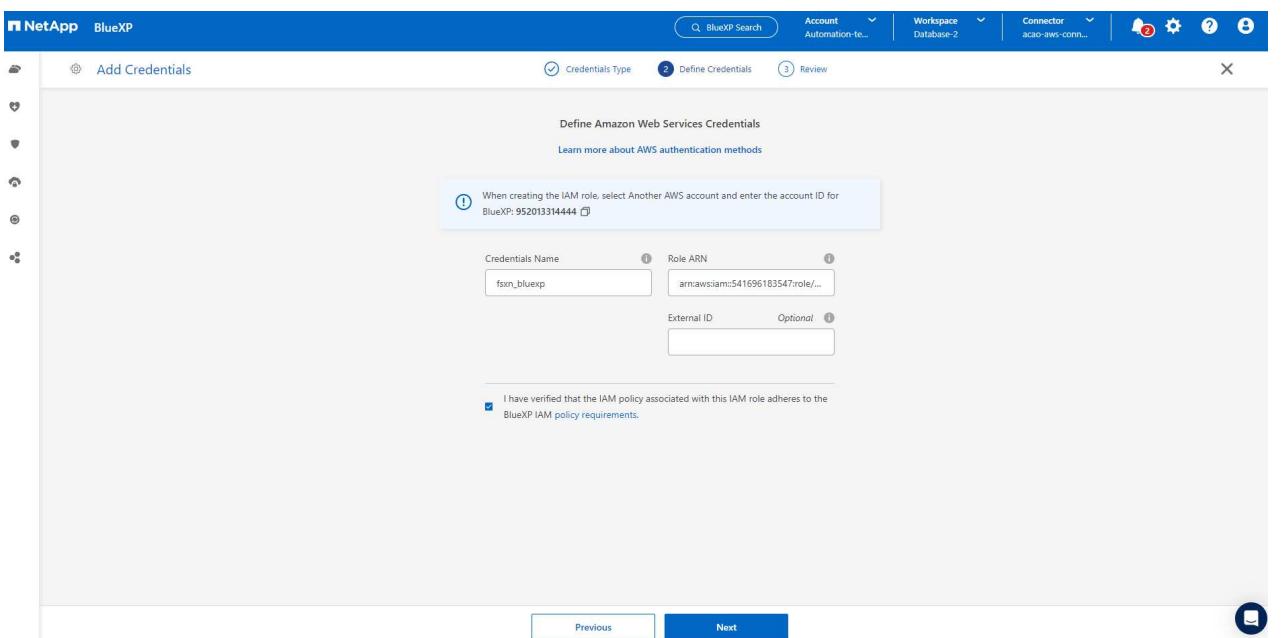
Add credentials

aws	shantanucreds	Type: Assume Role BlueXP	...
210811600188	nkarthik_kafka_mfs_role_FSxN	AWS Account ID	Assume Role

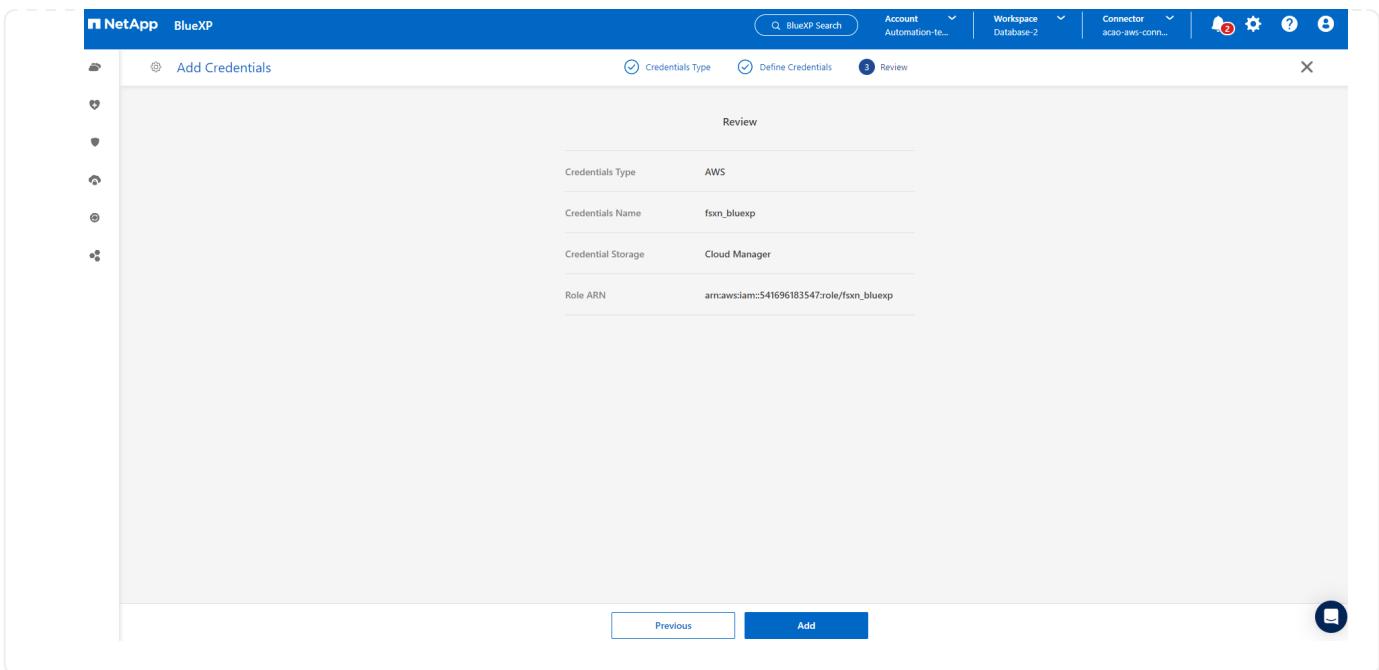
6. Choose credential location as - **Amazon Web Services - BlueXP**.



7. Define AWS credentials with proper **Role ARN**, which can be retrieved from AWS IAM role created in step one above. BlueXP **account ID**, which is used for creating AWS IAM role in step one.



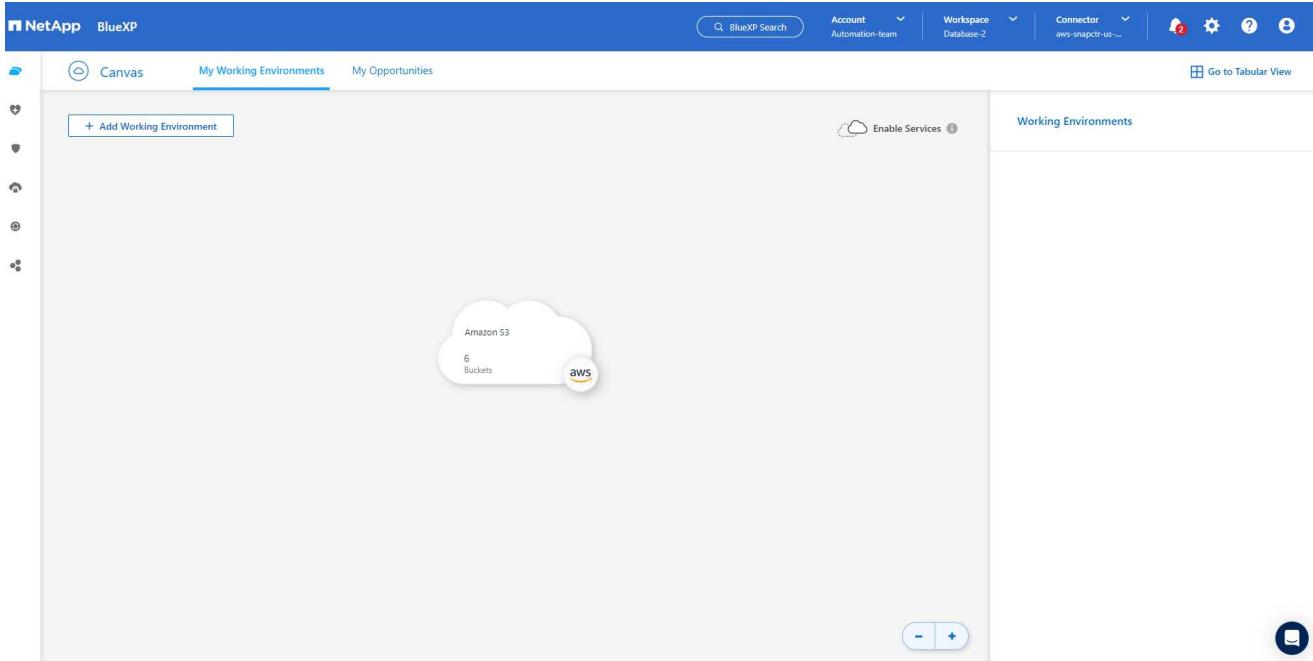
8. Review and Add.



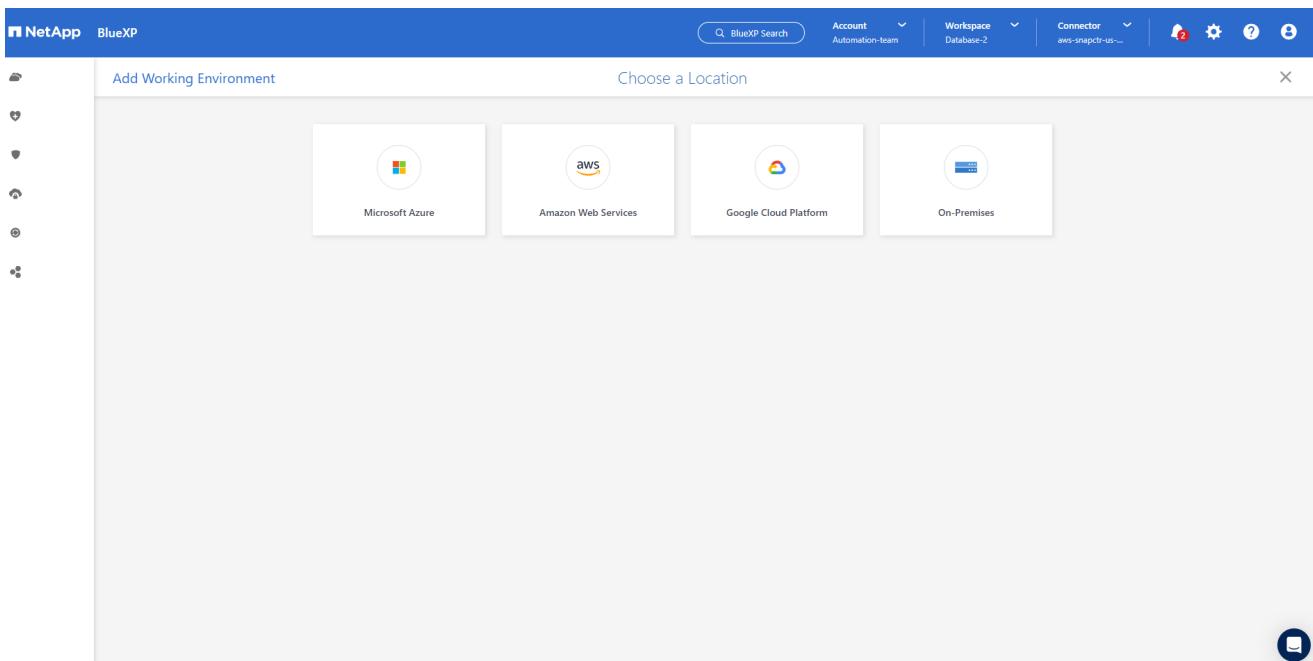
SnapCenter services setup

With the connector deployed and the credential added, SnapCenter services can now be set up with the following procedure:

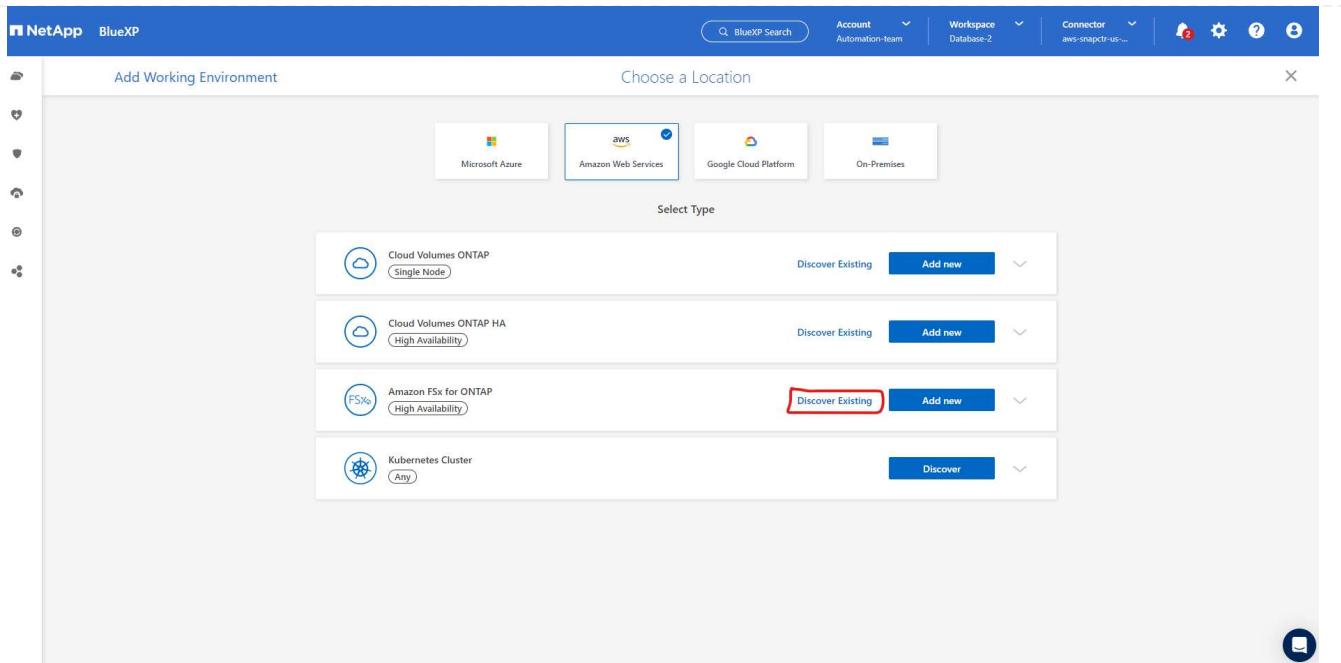
1. From **My Working Environment** click **Add working Environment** to discover FSx deployed in AWS.



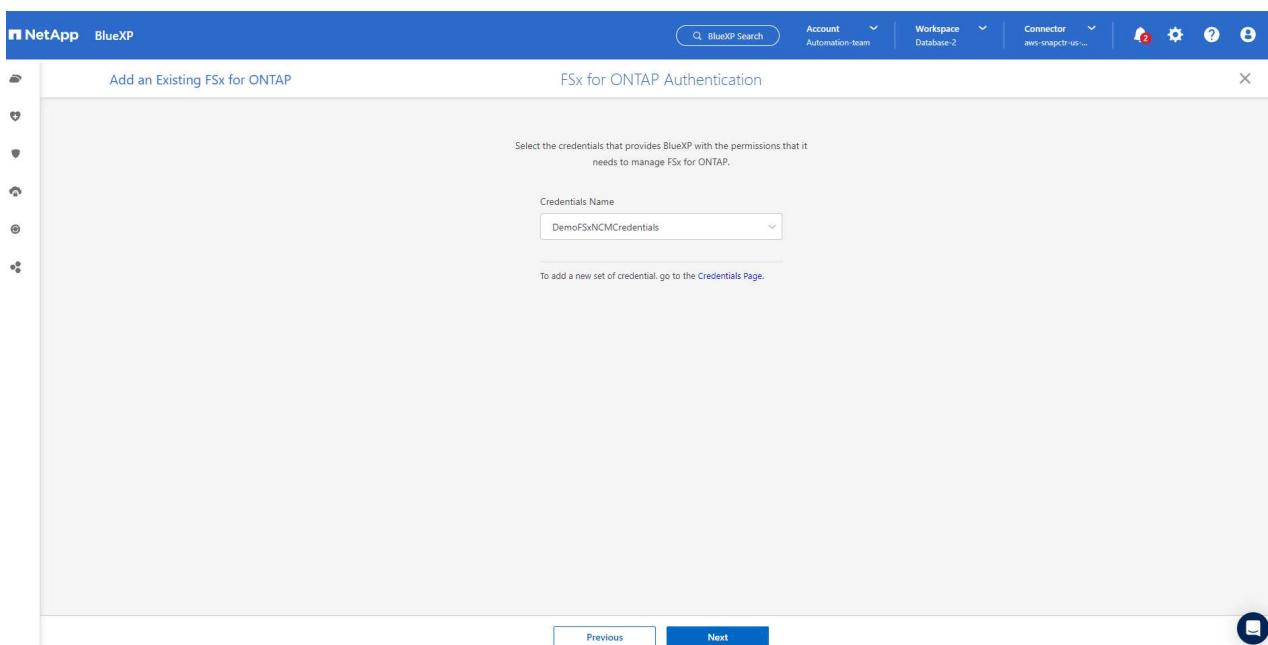
1. Choose **Amazon Web Services** as the location.



1. Click **Discover Existing** next to **Amazon FSx for ONTAP**.



1. Select the **Credentials Name** that you have created in previous section to grant BlueXP with the permissions that it needs to manage FSx for ONTAP. If you have not added credentials, you can add it from the **Settings** menu at the top right corner of the BlueXP console.



2. Choose the AWS region where Amazon FSx for ONTAP is deployed, select the FSx cluster that is hosting the Oracle database and click Add.

Add an Existing FSx for ONTAP

Select FSx for ONTAP

Choose an AWS region and then select the working environment that you want to add

Region: us-east-1 | US East (N. Virginia)

Name	File System ID	VPC ID	Subnet ID	Management Address	Deployment modal	Tags
fsx_01	fs-02ad7bf3476b741df	vpc-0b522d5e982a...	subnet-04f5fe7073ff...	management.fs-02ad7bf3476b741df.fsx.us-east...	Single Availability Zone	(4)

Previous Add

1. The discovered Amazon FSx for ONTAP instance now appears in the working environment.

Canvas My Working Environments My Opportunities

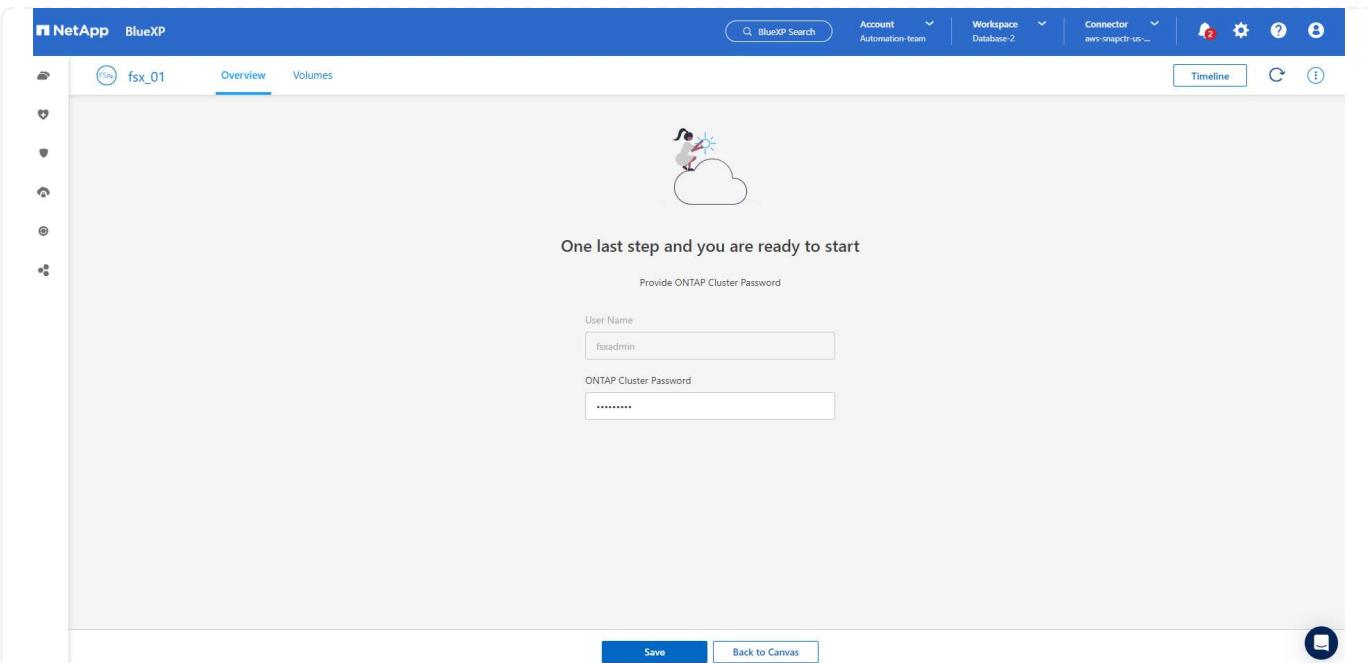
+ Add Working Environment

Enable Services

Working Environments

FSx 1 FSx for ONTAP (High-Availability)
250 GiB Provisioned Capacity

1. You can log into the FSx cluster with your fsxadmin account credentials.



1. After you log into Amazon FSx for ONTAP, review your database storage information (such as database volumes).

Volumes Summary

3 Volumes	250 GiB Provisioned Capacity	26.03 GiB SSD Used	0 GiB Capacity Pool Used
-----------	------------------------------	--------------------	--------------------------

3 Volumes

ora_01_data	ONLINE Manage Volume		
INFO	CAPACITY		
Disk Type	SSD	Provisioned	100 GiB
SVM Name	svm_ora	SSD Used	5.79 GiB
Tiering Policy	Snapshot Only	Capacity Pool Used	0 GiB

ora_01_logs	ONLINE Manage Volume		
INFO	CAPACITY		
Disk Type	SSD	Provisioned	100 GiB
SVM Name	svm_ora	SSD Used	1.14 GiB
Tiering Policy	Snapshot Only	Capacity Pool Used	0 GiB

ora_01_bin	ONLINE Manage Volume		
INFO	CAPACITY		
Disk Type	SSD	Provisioned	50 GiB
SVM Name	svm_ora	SSD Used	19.1 GiB
Tiering Policy	Snapshot Only	Capacity Pool Used	0 GiB

1. From the left-hand sidebar of the console, hover your mouse over the protection icon, and then click **Protection > Applications** to open the Applications launch page. Click **Discover Applications**.

Cloud Backup for Applications

Integrated Data Protection for ONTAP primary

Powered by SnapCenter, delivers application-consistent data protection on to Cloud Object Storage as well as on NetApp Cloud Storage. With proliferation of applications data on cloud, managing these data is challenging and complex. Cloud Backup for Applications offers simplified data management to smoother organizational IT operations and mitigates the risks associated with loss of application data.

Get started with Cloud Backup for Applications by discovering applications.

[Discover Applications](#)

1. Select **Cloud Native** as the application source type.

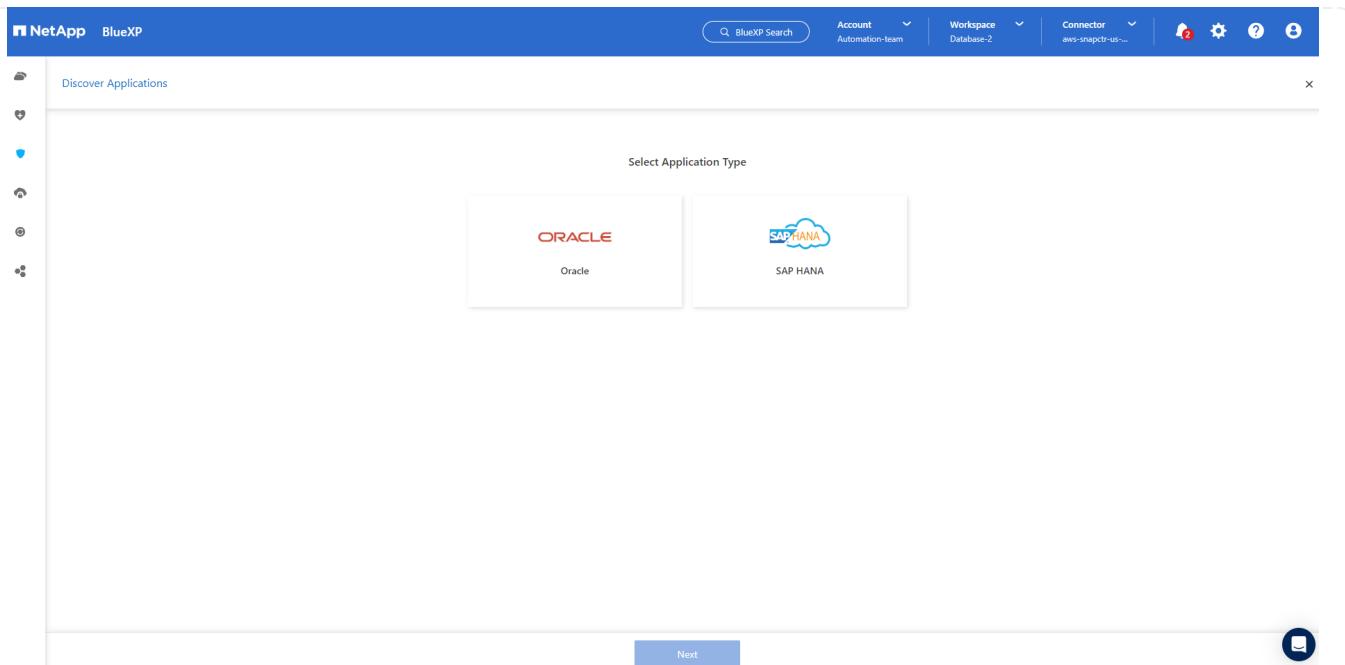
Select Application Source Type

Select the application source type that you want to manage.

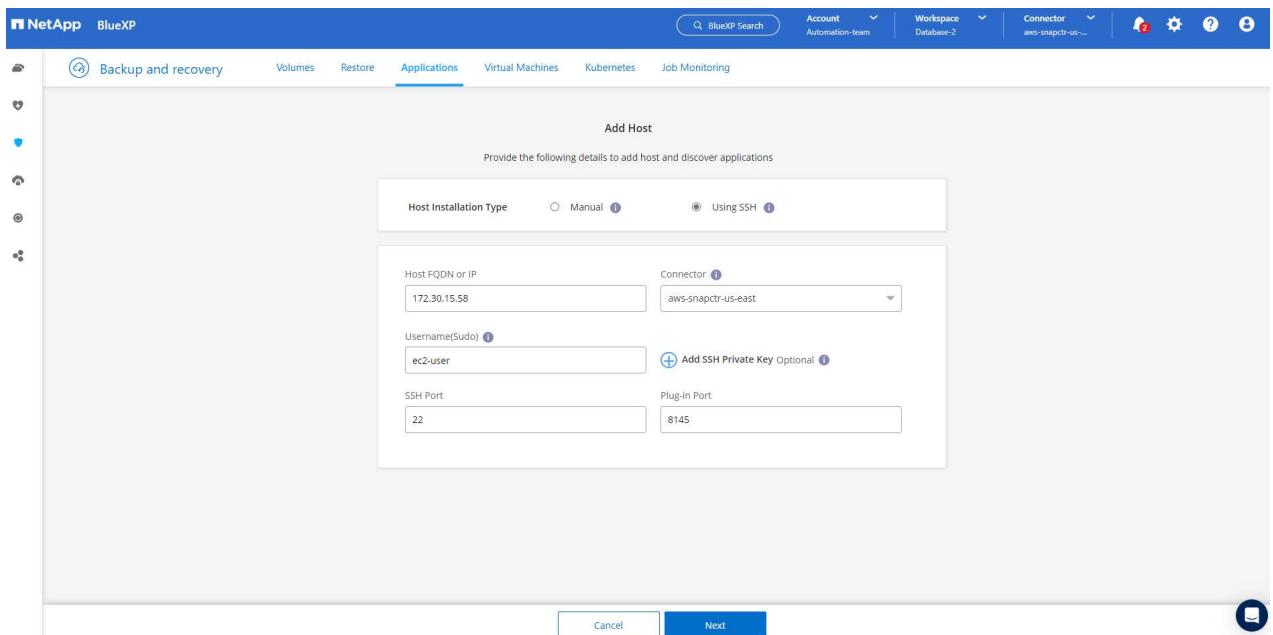
 Hybrid Applications hosted within your organization's infrastructure.	 Cloud Native Applications that are hosted and run in the cloud using AWS, Azure, GCP, etc.
--	---

[Cancel](#) [Next](#)

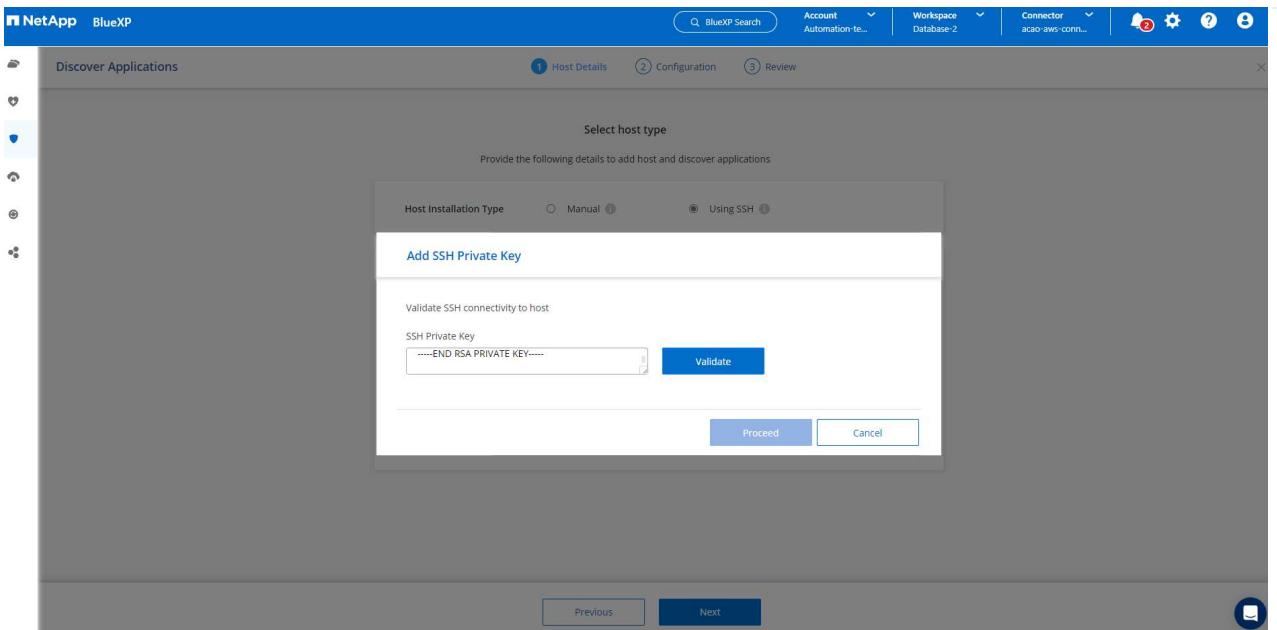
1. Choose **Oracle** for the application type.



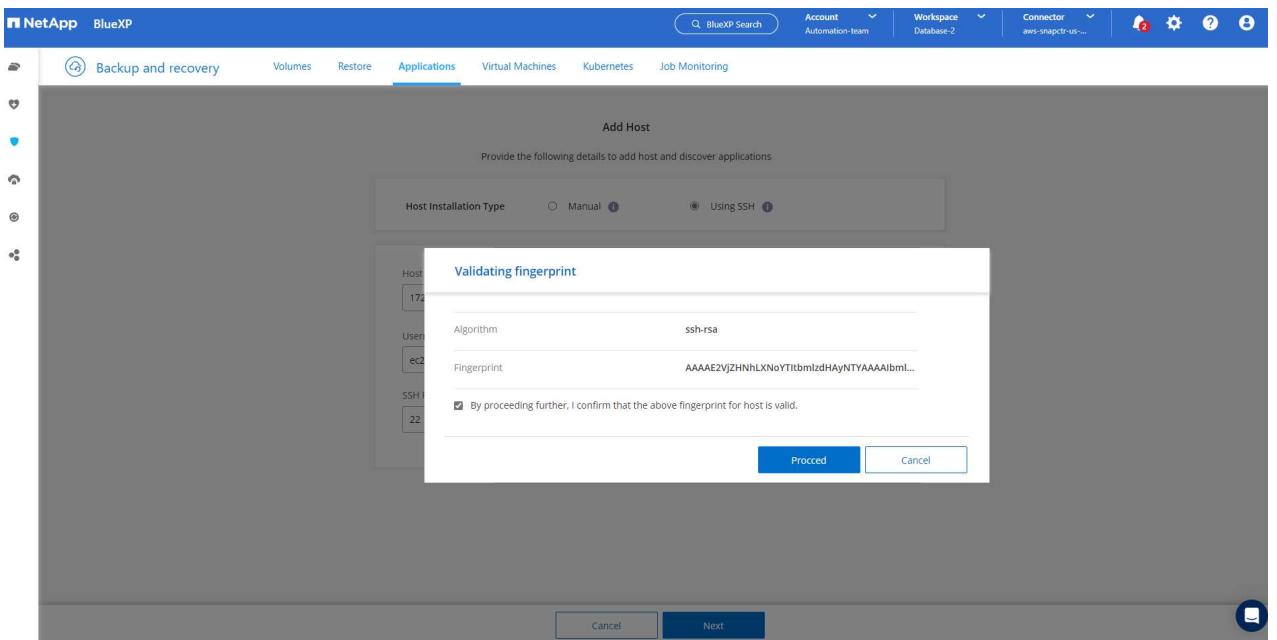
1. Fill in the AWS EC2 Oracle application host details. Choose **Using SSH as Host Installation Type** for one step plugin installation and database discovery. Then, click on **Add SSH Private Key**.



2. Paste in your ec2-user SSH key for the database EC2 host and click on **Validate** to proceed.



3. You will be prompted for **Validating fingerprint** to proceed.



4. Click on **Next** to install an Oracle database plugin and discover the Oracle databases on the EC2 host. Discovered databases are added to **Applications**. The database **Protection Status** shows as **Unprotected** when initially discovered.

The screenshot shows the NetApp BlueXP web interface. At the top, there are navigation tabs: Backup and recovery, Volumes, Restore, Applications (which is selected), Virtual Machines, Kubernetes, and Job Monitoring. The top right includes a search bar ('BlueXP Search'), account information ('Account Automation-team'), workspace ('Workspace Database-2'), connector ('Connector aws-snapctr-us-...'), and various system icons.

In the main content area, there's a summary section with counts for Hosts (1), ORACLE (1), and Clone (0). Below this is a table titled 'Application Protection' showing 0 Protected and 1 Unprotected items. The main table below lists 'Databases' with one entry:

Name	Host Name	Policy Name	Protection Status
db1	172.30.15.58		Unprotected

At the bottom of the table, it says '1 - 1 of 1' and has navigation arrows. A blue circular icon with a white square is located in the bottom right corner of the main content area.

This completes the initial setup of SnapCenter services for Oracle. The next three sections of this document describe Oracle database backup, restore, and clone operations.

Oracle database backup

- Click the three dots next to the database **Protection Status**, and then click **Polices** to view the default preloaded database protection policies that can be applied to protect your Oracle databases.

The screenshot shows the NetApp BlueXP interface under the Applications tab. It displays a summary of resources: 1 Host, 1 Oracle database, and 0 Clones. Below this, a table lists 1 Database named db1 with host 172.30.15.58. A context menu is open over the db1 row, with the 'Policies' option selected. The top navigation bar includes tabs for Backup and recovery, Volumes, Restore, Applications (selected), Virtual Machines, Kubernetes, and Job Monitoring. The right side of the interface has various status indicators and a search bar.

- You can also create your own policy with a customized backup frequency and backup data-retention window.

The screenshot shows the NetApp BlueXP interface under the Applications tab, specifically the Policies section. It lists four existing policies: 'Oracle Full Backup for Bronze', 'Oracle Full Backup for Gold', 'Oracle Full Backup for Silver', and 'my_full_bkup'. Each policy entry includes its name, backup type (FullBackup), and detailed scheduling and retention rules. A 'Create Policy' button is visible at the top right of the table. The top navigation bar is identical to the previous screenshot, showing tabs for Backup and recovery, Volumes, Restore, Applications (selected), Virtual Machines, Kubernetes, and Job Monitoring.

- When you are happy with the policy configuration, you can then assign your policy of choice to protect the database.

Cloud Native

Oracle

Hosts 1

ORACLE 1

Clone 0

Application Protection
Protected 0
Unprotected 1

1 Databases

Filter By +

Name	Host Name	Policy Name	Protection Status
db1	172.30.15.58		Unprotected

View Details

Assign Policy

1. Choose the policy to assign to the database.

Assign Policy

Assign a policy to start taking backups of the database "db1"

4 Policies

Policy Name	Backup Type	Schedules
Oracle Full Backup for Bronze	FullBackup	Daily: Repeats Every 1 Day, Keeps 14 copies Weekly: Repeats Every Fri, Keeps 4 copies Monthly: Repeats Every 1st Day of Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, C
Oracle Full Backup for Gold	FullBackup	Hourly: Repeats Every 6 Hrs, Keeps 16 copies Daily: Repeats Every 1 Day, Keeps 30 copies Weekly: Repeats Every Fri, Keeps 4 copies Monthly: Repeats Every 1st Day of Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, C
Oracle Full Backup for Silver	FullBackup	Hourly: Repeats Every 12 Hrs, Keeps 6 copies Daily: Repeats Every 1 Day, Keeps 14 copies Weekly: Repeats Every Fri, Keeps 4 copies Monthly: Repeats Every 1st Day of Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, C
my_full_bkup	FullBackup	Hourly: Repeats Every 1 Hr, Keeps 3 Days

1 - 4 of 4 << < 1 > >>

Cancel Assign

1. After the policy is applied, the database protection status changed to **Protected** with a green check mark.

The screenshot shows the NetApp BlueXP web interface. At the top, there's a navigation bar with tabs for Backup and recovery, Volumes, Restore, Applications (which is selected), Virtual Machines, Kubernetes, and Job Monitoring. Below the navigation bar, there are two dropdown menus: 'Cloud Native' and 'Oracle'. A summary box displays counts for Hosts (1), ORACLE (1), and Clone (0). To the right, an 'Application Protection' section shows 1 Protected and 0 Unprotected items. The main area is titled '1 Databases' and contains a table with one row. The table columns are Name, Host Name, Policy Name, and Protection Status. The single entry is db1, 172.30.15.58, my_full_bkup, and Protected. There are standard navigation buttons at the bottom of the table.

1. The database backup runs on a predefined schedule. You can also run a one-off on-demand backup as shown below.

This screenshot is similar to the first one but includes a context menu for the database entry 'db1'. The menu options are View Details, On-Demand Backup (which is underlined in red), Assign Policy, and Un-assign Policy. The rest of the interface is identical to the first screenshot, showing the same summary, application protection status, and database table.

1. The database backups details can be viewed by clicking **View Details** from the menu list. This includes the backup name, backup type, SCN, and backup date. A backup set covers a snapshot for both data volume and log volume. A log volume snapshot takes place right after a database volume snapshot. You can apply a filter if you are looking for a particular backup in a long list.

NetApp BlueXP

Backup and recovery Volumes Restore Applications Virtual Machines Kubernetes Job Monitoring

Applications > Database Details

Database Details

 db1 Database Name	 Protected Protection	Oracle Full Backup for Gold Policy Names	Database Type
172.30.15.58 Host Name	FSx Host Storage	Unreachable Database Version	bKed8yv2T19Bj0V5QyqvA... Agent Id
- Clones	- Parent Database		

8 Backups

Filter By +

Select Timeframe ▾

Backup Name	Backup Type	SCN	Backup Date	Action
Oracle_Full_Backup_for_Gold_Weekly_db1_2023_03_24_19_12_18_60900_1	Log	2589354	Mar 24, 2023, 3:12:34 pm	Delete
Oracle_Full_Backup_for_Gold_Weekly_db1_2023_03_24_19_11_51_51476_0	Data	2589306	Mar 24, 2023, 3:12:18 pm	***
Oracle_Full_Backup_for_Gold_Hourly_db1_2023_03_24_18_10_31_71953_1	Log	2586621	Mar 24, 2023, 2:10:45 pm	Delete
Oracle_Full_Backup_for_Gold_Hourly_db1_2023_03_24_18_10_03_70535_0	Data	2586557	Mar 24, 2023, 2:10:31 pm	***

Oracle database restore and recovery

- For a database restore, choose the right backup, either by the SCN or backup time. Click the three dots from the database data backup, and then click **Restore** to initiate database restore and recovery.

Database Details

db1 Database Name	Protected Protection	Oracle Full Backup for Gold Policy Names	Database Type
172.30.15.58 Host Name	FSX Host Storage	Unreachable Database Version	bKed8yv2T19Bj0V5QyqvA... Agent Id
Clones	Parent Database		

6 Backups

Backup Name	Backup Type	SCN	Backup Date	Action
Oracle_Full_Backup_for_Gold_Hourly_db1_2023_03_24_18_10_31_71953_1	Log	2586621	Mar 24, 2023, 2:10:45 pm	Delete
Oracle_Full_Backup_for_Gold_Hourly_db1_2023_03_24_18_10_03_70535_0	Data	2586557	Mar 24, 2023, 2:10:31 pm	Restore
Oracle_Full_Backup_for_Gold_Hourly_db1_2023_03_24_15_37_04_98851_1	Log	2580577	Mar 24, 2023, 11:37:1	Delete
Oracle_Full_Backup_for_Gold_Hourly_db1_2023_03_24_15_36_33_27205_0	Data	2580524	Mar 24, 2023, 11:37:0	Clone

- Choose your restore setting. If you are sure that nothing has changed in the physical database structure after the backup (such as the addition of a data file or a disk group), you can use the **Force in place restore** option, which is generally faster. Otherwise, do not check this box.

Restore Settings

Restore Scope

- All Data Files
Data Files Restore
- Control Files
Control Files Restore
- Force in place restore
In place restore will skip the foreign files(files which are not part of the database) validation check. The Oracle database and the ASM disk group will be restored to the point when the backup was created.
- Database state will be changed if needed for restore and recovery.

Recovery Scope

- All Logs
- Until System Change Number
- Date and Time
- No Recovery

Archive Log Files Locations: /mnt/log_location001
 Open the database or the container database in READ-WRITE mode after recovery.

Next

- Review and start database restore and recovery.

Restore "db1"

Review

Backup Name: Oracle_Full_Backup_for_Gold_Weekly_db1_2023_03_24_19_11_51_51476_0

Restore Scope: All Data Files

Recovery Scope: All Logs

Force In Place Restore: Yes

Open Database or Container: Yes

Database in READ-WRITE Mode After Recovery

Previous Restore

1. From the **Job Monitoring** tab, you can view the status of the restore job as well as any details while it is running.

Backup and recovery Volumes Restore Applications Virtual Machines Kubernetes Job Monitoring

Job Monitoring

Last Updated: March 24 2023, 15:25:33

Advanced Search & Filtering Timeframe: Last 24 Hours

Job ID	Type	Resource Name	Status	Job Name	Start Time
1fdca0bd-a9c8-45aa...	--	--	Success	Restore for Oracle Database db1 ...	Mar 24 2023, 3:16:28 pr
f6f4fe2d-3040-497f-...	--	--	Success	Backup of db1 oracle database o...	Mar 24 2023, 3:11:51 pr
5e3299f5-29db-4dcc...	--	--	Success	Backup of db1 oracle database o...	Mar 24 2023, 2:10:03 pr
6da5e51e-1a79-4e7e...	--	--	Success	Initialize FullBackup backup of po...	Mar 24 2023, 2:10:01 pr

The screenshot shows the NetApp BlueXP web interface. At the top, there are navigation links for 'Backup and recovery', 'Volumes', 'Restore', 'Applications', 'Virtual Machines', 'Kubernetes', and 'Job Monitoring'. The 'Job Monitoring' tab is currently selected. In the center, under 'Job Details', it shows a job with ID '1fdca0bd-a9c8-45aa-9d7a-05a07cb291f4'. Below this, a table lists 'Sub-Jobs(6)' with columns for Job Name, Job ID, Start Time, End Time, Duration, and a plus sign icon for adding more. The sub-jobs listed are:

Job Name	Job ID	Start Time	End Time	Duration
Restore for Oracle Database db1 using backup ...	1fdca0bd-a9c8-45aa-9d7a-05a07cb291f4	Mar 24 2023, 3:16:28 pm	Mar 24 2023, 3:23:33 pm	7 Minutes
Post Restore Cleanup	2096a8e4-889d-4b2a-9...	Mar 24 2023, 3:23:18 pm	Mar 24 2023, 3:23:32 pm	14 Seconds
Post Restore	fb7b1171-9f6f-4228-9e...	Mar 24 2023, 3:20:06 pm	Mar 24 2023, 3:23:19 pm	3 Minutes
Restore	0f4580d0-6598-458b-a7...	Mar 24 2023, 3:17:49 pm	Mar 24 2023, 3:20:07 pm	2 Minutes

Oracle database clone

To clone a database, launch the clone workflow from the same database backup details page.

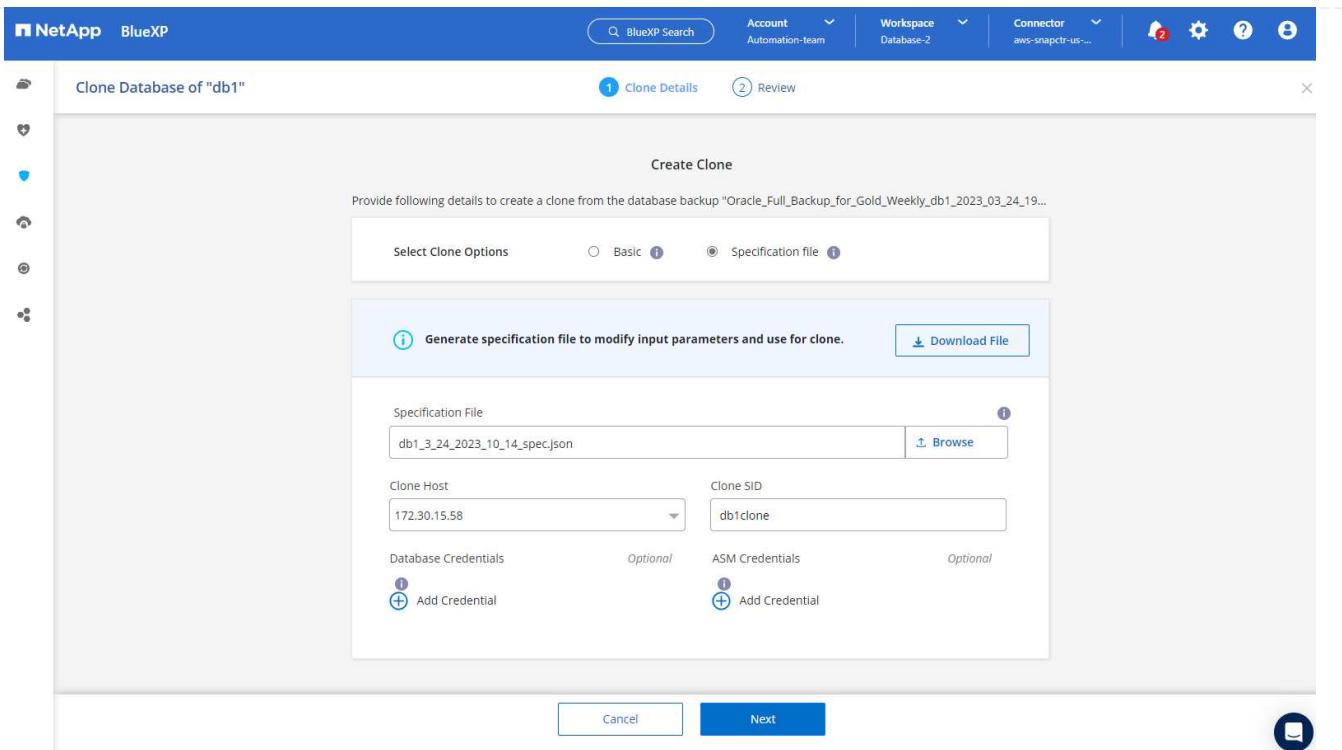
1. Select the right database backup copy, click the three dots to view the menu, and choose the **Clone** option.

The screenshot shows the BlueXP interface for managing databases. In the 'Database Details' section, a database named 'db1' is listed with its protection status as 'Protected'. Below it, host information like 'Host Name' and 'Host Storage' is shown, along with 'Unreachable' database version and 'Agent Id'. Under 'Clones', there is a link to the 'Parent Database'. In the 'Backups' section, two entries are listed: 'Oracle_Full_Backup_for_Gold_Hourly_db1_2023_03_24_13_34_41_30491_1' (Log type, SCN 2575607, Mar 24, 2023) and 'Oracle_Full_Backup_for_Gold_Hourly_db1_2023_03_24_13_34_07_26748_0' (Data type, SCN 2575555, Mar 24, 2023). A context menu is open over the second backup entry, with the 'Clone' option highlighted and circled in red.

1. Select the **Basic** option if you don't need to change any cloned database parameters.

The screenshot shows the 'Clone Database of "db1"' dialog. At the top, there are tabs for 'Clone Details' and 'Review'. The main area is titled 'Create Clone' and contains a sub-section 'Select Clone Options' with a radio button for 'Basic' (selected) and another for 'Specification file'. Below this, 'Clone Host' is set to '172.30.15.58', 'Clone SID' is 'db1 clone', 'Clone Naming Scheme' is 'Auto-generated', and 'Oracle Home' is '/u01/app/oracle/product/19.0.0/db1'. At the bottom, there are 'Cancel' and 'Next' buttons.

1. Alternatively, select **Specification file**, which gives you the option of downloading the current init file, making changes, and then uploading it back to the job.



1. Review and launch the job.

1. Monitor the cloning job status from the **Job Monitoring** tab.

The screenshot shows the NetApp BlueXP web interface. The top navigation bar includes links for Backup and recovery, Volumes, Restore, Applications, Virtual Machines, Kubernetes, and Job Monitoring. The Job Monitoring section is active, displaying a job ID: cd30abaf-fbe2-4052-a6db-4bf965a8d29b. Below this, the "Job Details" section is shown with the same job ID. A sub-job table lists three tasks: "Cloning Oracle Database db1 as db1clone on h...", "Running pre scripts", and "Validating clone request".

Job Name	Job ID	Start Time	End Time	Duration
Cloning Oracle Database db1 as db1clone on h...	cd30abaf-fbe2-4052-a6...	Mar 24 2023, 1:30:36 pm		--
Running pre scripts	5f1152c1-853a-4ec6-a4f...	Mar 24 2023, 1:30:41 pm	Mar 24 2023, 1:30:41 pm	0 Second
Validating clone request	f93a6c44-2eb2-4c5e-9f...	Mar 24 2023, 1:30:35 pm	Mar 24 2023, 1:30:42 pm	7 Seconds

1. Validate the cloned database on the EC2 instance host.

```

# Multiple entries with the same $ORACLE_SID are not allowed.
#
#+ASM:/u01/app/oracle/product/19.0.0/grid:N
db1:/u01/app/oracle/product/19.0.0/db1:N
# SnapCenter Plug-in for Oracle Database generated entry (DO NOT REMOVE THIS LINE)
dbiclone:/u01/app/oracle/product/19.0.0/db1:N
[oracle@ip-172-30-15-58 ~]$ crsctl stat res -t
-----
Name          Target  State       Server            State details
-----
Local Resources
-----
ora.DATA.dg      ONLINE  ONLINE    ip-172-30-15-58   STABLE
ora.DATA_DB1CLONE.dg      ONLINE  ONLINE    ip-172-30-15-58   STABLE
ora.LISTENER.lsnr      ONLINE  ONLINE    ip-172-30-15-58   STABLE
ora.LOGS.dg      ONLINE  ONLINE    ip-172-30-15-58   STABLE
ora.LOGS_SCO_2748138658.dg      ONLINE  ONLINE    ip-172-30-15-58   STABLE
ora.asm         ONLINE  ONLINE    ip-172-30-15-58   STABLE
ora.ons          OFFLINE OFFLINE   ip-172-30-15-58   Started,STABLE
-----
Cluster Resources
-----
ora.cssd        1      ONLINE  ONLINE    ip-172-30-15-58   STABLE
ora.db1.db       1      ONLINE  ONLINE    ip-172-30-15-58   Open,HOME=/u01/app/o
racle/product/19.0.0
/db1,STABLE
ora.db1clone.db 1      ONLINE  ONLINE    ip-172-30-15-58   Open,HOME=/u01/app/o
racle/product/19.0.0
/db1,STABLE
ora.diskmon      1      OFFLINE OFFLINE   STABLE
ora.driver.afd   1      ONLINE  ONLINE    ip-172-30-15-58   STABLE
ora.evmd         1      ONLINE  ONLINE    ip-172-30-15-58   STABLE
-----
[oracle@ip-172-30-15-58 ~]$ 

```

Additional information

To learn more about the information that is described in this document, review the following documents and/or websites:

- Set up and administer BlueXP

<https://docs.netapp.com/us-en/cloud-manager-setup-admin/index.html>

- BlueXP backup and recovery documentation

<https://docs.netapp.com/us-en/cloud-manager-backup-restore/index.html>

- Amazon FSx for NetApp ONTAP

<https://aws.amazon.com/fsx/netapp-ontap/>

- Amazon EC2

https://aws.amazon.com/pm/ec2/?trk=36c6da98-7b20-48fa-8225-4784bc9843&sc_channel=ps&s_kwcid=AL!4422!3!467723097970!e!!g!!aws%20ec2&ef_id=Cj0KCQiA54KfBhCKARIIsAJzSrdqwQrghn6I71jiWzSeaT9Uh1-vY-VfhJixF-xnv5rWwn2S7RqZOTQ0aAh7eEALw_wcB:G:s&s_kwcid=AL!4422!3!467723097970!e!!g!!aws%20ec2

Hybrid Cloud Database Solutions with SnapCenter

TR-4908: Hybrid Cloud Database Solutions with SnapCenter Overview

Alan Cao, Felix Melligan, NetApp

This solution provides NetApp field and customers with instructions and guidance for configuring, operating, and migrating databases to a hybrid cloud environment using the NetApp SnapCenter GUI-based tool and the NetApp storage service CVO in public clouds for the following use cases:

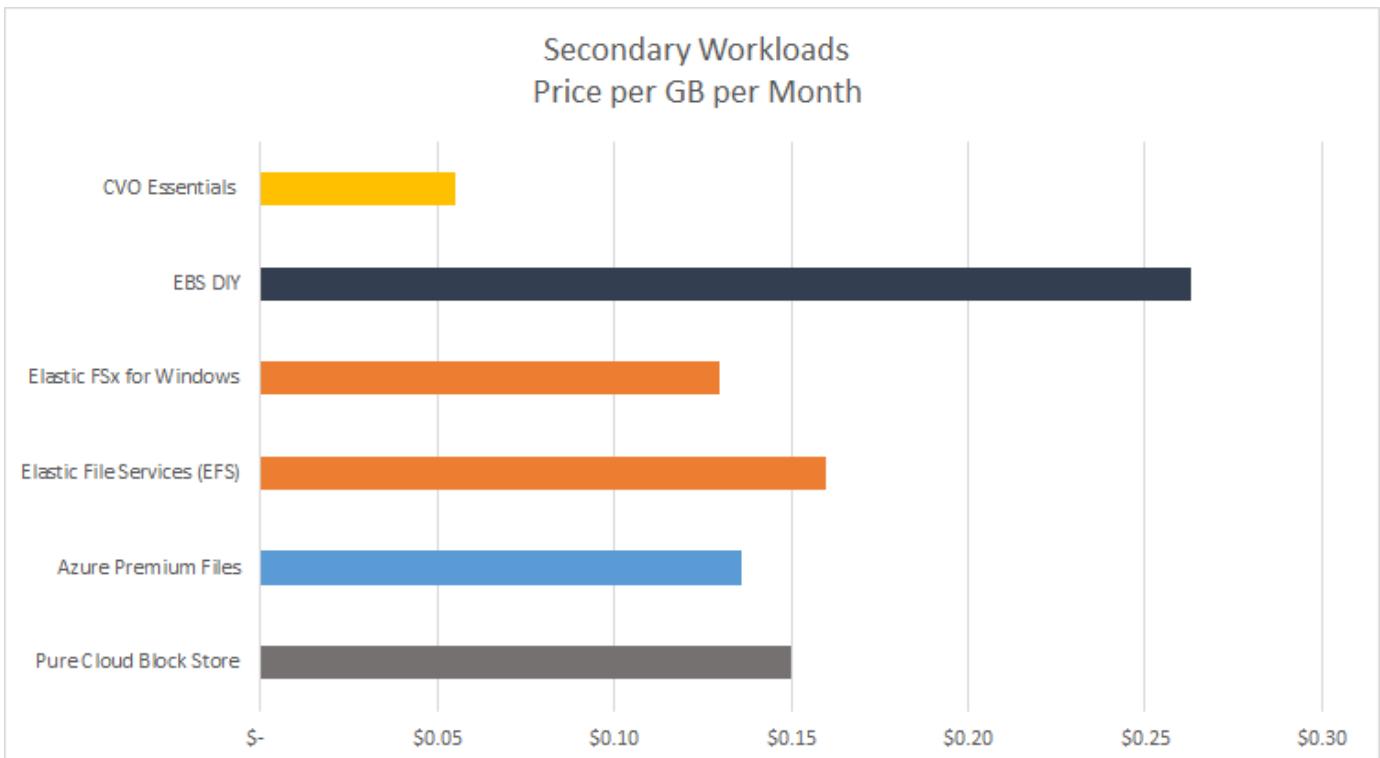
- Database dev/test operations in the hybrid cloud
- Database disaster recovery in the hybrid cloud

Today, many enterprise databases still reside in private corporate data centers for performance, security, and/or other reasons. This hybrid cloud database solution enables enterprises to operate their primary databases on site while using a public cloud for dev/test database operations as well as for disaster recovery to reduce licensing and operational costs.

Many enterprise databases, such as Oracle, SQL Server, SAP HANA, and so on, carry high licensing and operational costs. Many customers pay a one-time license fee as well as annual support costs based on the number of compute cores in their database environment, whether the cores are used for development, testing, production, or disaster recovery. Many of those environments might not be fully utilized throughout the application lifecycle.

The solutions provide an option for customers to potentially reduce their licensable cores count by moving their database environments devoted to development, testing, or disaster recovery to the cloud. By using public-cloud scale, redundancy, high availability, and a consumption-based billing model, the cost saving for licensing and operation can be substantial, while not sacrificing any application usability or availability.

Beyond potential database license-cost savings, the NetApp capacity-based CVO license model allows customers to save storage costs on a per-GB basis while empowering them with high level of database manageability that is not available from competing storage services. The following chart shows a storage cost comparison of popular storage services available in the public cloud.



This solution demonstrates that, by using the SnapCenter GUI-based software tool and NetApp SnapMirror technology, hybrid cloud database operations can be easily setup, implemented, and operated.

The following videos demonstrate SnapCenter in action:

- [Backup of an Oracle database across a Hybrid Cloud using SnapCenter](#)
- [SnapCenter- Clone DEV/TEST to AWS Cloud for an Oracle database](#)

Notably, although the illustrations throughout this document show CVO as a target storage instance in the public cloud, the solution is also fully validated for the new release of the FSx ONTAP storage engine for AWS.

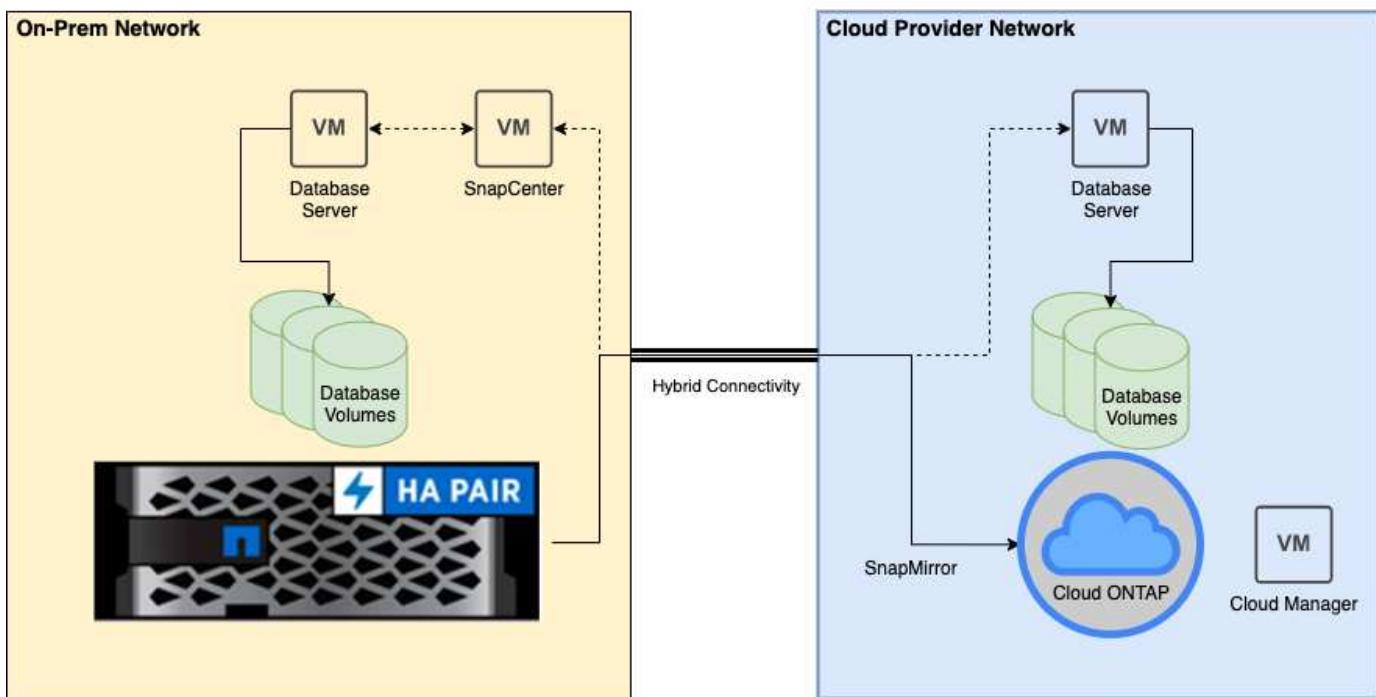
To test drive the solution and use cases for yourself, a NetApp Lab-on-Demand SL10680 can be requested at following xref:[./databases/ TL_AWS_004 HCoD: AWS - NW,SnapCenter\(OnPrem\)](#).

[Next: Solutions architecture.](#)

Solution Architecture

[Previous: Introduction.](#)

The following architecture diagram illustrates a typical implementation of enterprise database operation in a hybrid cloud for dev/test and disaster recovery operations.



In normal business operations, synchronized database volumes in the cloud can be cloned and mounted to dev/test database instances for applications development or testing. In the event of a failure, the synchronized database volumes in the cloud can then be activated for disaster recovery.

[Next: Solutions requirements.](#)

SnapCenter Requirements

[Previous: Solutions architecture.](#)

This solution is designed in a hybrid cloud setting to support on-premises production databases that can burst to all of the popular public clouds for dev/test and disaster recovery operations.

This solution supports all databases that are currently supported by SnapCenter, although only Oracle and SQL Server databases are demonstrated here. This solution is validated with virtualized database workloads, although bare-metal workloads are also supported.

We assume that production database servers are hosted on-premises with DB volumes presented to DB hosts from a ONTAP storage cluster. SnapCenter software is installed on-premises for database backup and data replication to the cloud. An Ansible controller is recommended but not required for database deployment automation or OS kernel and DB configuration syncing with a standby DR instance or dev/test instances in the public cloud.

Requirements

Environment	Requirements
On-premises	Any databases and versions supported by SnapCenter SnapCenter v4.4 or higher Ansible v2.09 or higher ONTAP cluster 9.x Intercluster LIFs configured Connectivity from on-premises to a cloud VPC (VPN, interconnect, and so on) Networking ports open - ssh 22 - tcp 8145, 8146, 10000, 11104, 11105
Cloud - AWS	Cloud Manager Connector Cloud Volumes ONTAP Matching DB OS EC2 instances to On-prem
Cloud - Azure	Cloud Manager Connector Cloud Volumes ONTAP Matching DB OS Azure Virtual Machines to On-prem
Cloud - GCP	Cloud Manager Connector Cloud Volumes ONTAP Matching DB OS Google Compute Engine instances to on-premises

[Next: Prerequisites configuration.](#)

Prerequisites configuration

[Previous: Solutions requirements.](#)

Certain prerequisites must be configured both on-premises and in the cloud before the execution of hybrid cloud database workloads. The following section provides a high-level summary of this process, and the following links provide further information about necessary system configuration.

On premises

- SnapCenter installation and configuration
- On-premises database server storage configuration
- Licensing requirements
- Networking and security
- Automation

Public cloud

- A NetApp Cloud Central login
- Network access from a web browser to several endpoints
- A network location for a connector
- Cloud provider permissions
- Networking for individual services

Important considerations:

1. Where to deploy the Cloud Manager Connector?
2. Cloud Volume ONTAP sizing and architecture
3. Single node or high availability?

The following links provide further details:

[On Premises](#)

[Public Cloud](#)

[Next: Prerequisites on-premises.](#)

Prerequisites on-premises

[Previous: Prerequisites configuration.](#)

The following tasks must be completed on-premises to prepare the SnapCenter hybrid-cloud database workload environment.

SnapCenter installation and configuration

The NetApp SnapCenter tool is a Windows-based application that typically runs in a Windows domain environment, although workgroup deployment is also possible. It is based on a multitiered architecture that includes a centralized management server (the SnapCenter server) and a SnapCenter plug-in on the database server hosts for database workloads. Here are a few key considerations for hybrid-cloud deployment.

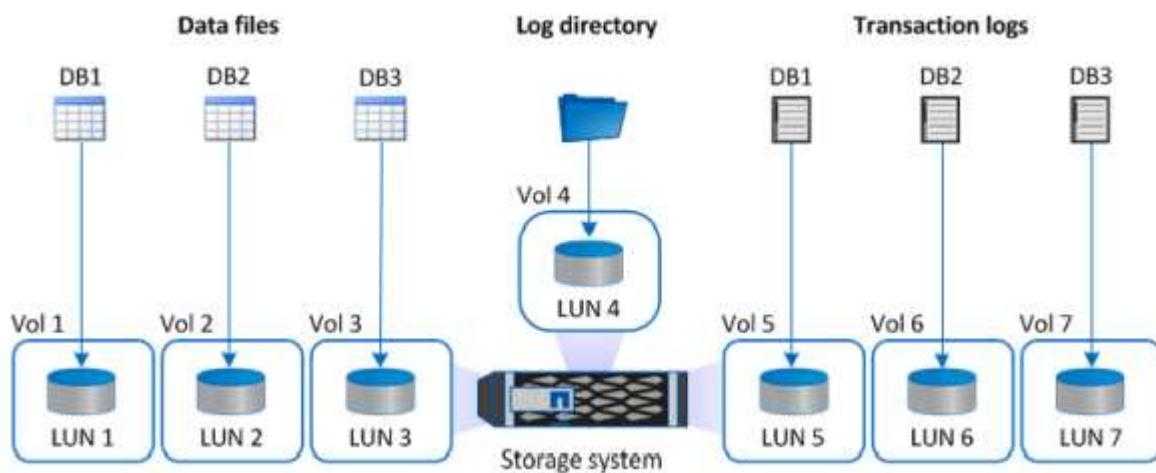
- **Single instance or HA deployment.** HA deployment provides redundancy in the case of a single SnapCenter instance server failure.
- **Name resolution.** DNS must be configured on the SnapCenter server to resolve all database hosts as well as on the storage SVM for forward and reverse lookup. DNS must also be configured on database servers to resolve the SnapCenter server and the storage SVM for both forward and reverse lookup.
- **Role-based access control (RBAC) configuration.** For mixed database workloads, you might want to use RBAC to segregate management responsibility for different DB platform such as an admin for Oracle database or an admin for SQL Server. Necessary permissions must be granted for the DB admin user.
- **Enable policy-based backup strategy.** To enforce backup consistency and reliability.
- **Open necessary network ports on the firewall.** For the on-premises SnapCenter server to communicate with agents installed in the cloud DB host.
- **Ports must be open to allow SnapMirror traffic between on-prem and public cloud.** The SnapCenter server relies on ONTAP SnapMirror to replicate onsite Snapshot backups to cloud CVO storage SVMs.

After careful pre-installation planning and consideration, click this [SnapCenter installation workflow](#) for details of SnapCenter installation and configuration.

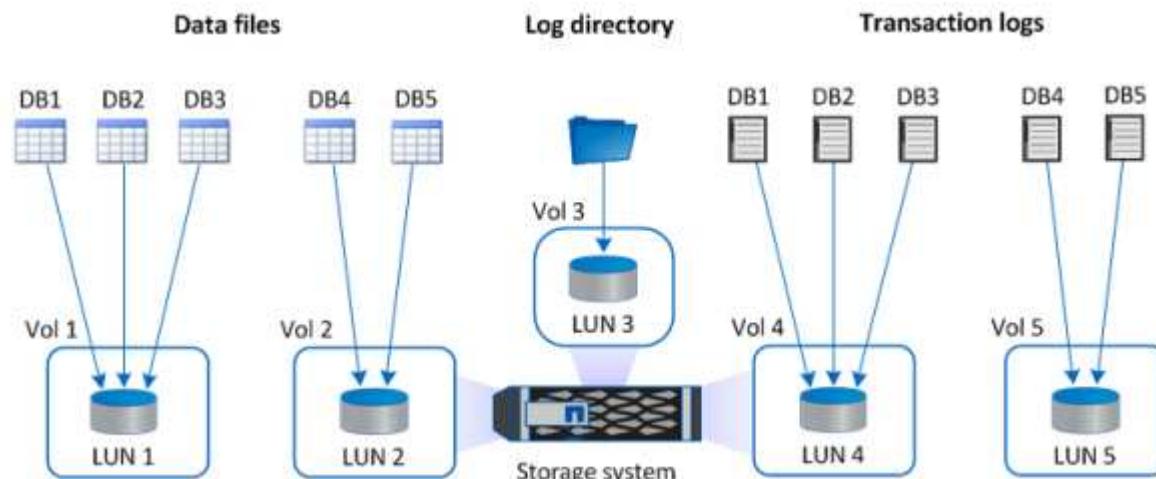
On-premises database server storage configuration

Storage performance plays an important role in the overall performance of databases and applications. A well-designed storage layout can not only improve DB performance but also make it easy to manage database backup and recovery. Several factors should be considered when defining your storage layout, including the size of the database, the rate of expected data change for the database, and the frequency with which you perform backups.

Directly attaching storage LUNs to the guest VM by either NFS or iSCSI for virtualized database workloads generally provides better performance than storage allocated via VMDK. NetApp recommends the storage layout for a large SQL Server database on LUNs depicted in the following figure.



The following figure shows the NetApp recommended storage layout for small or medium SQL Server database on LUNs.



The Log directory is dedicated to SnapCenter to perform transaction log rollup for database recovery. For an extra large database, multiple LUNs can be allocated to a volume for better performance.

For Oracle database workloads, SnapCenter supports database environments backed by ONTAP storage that

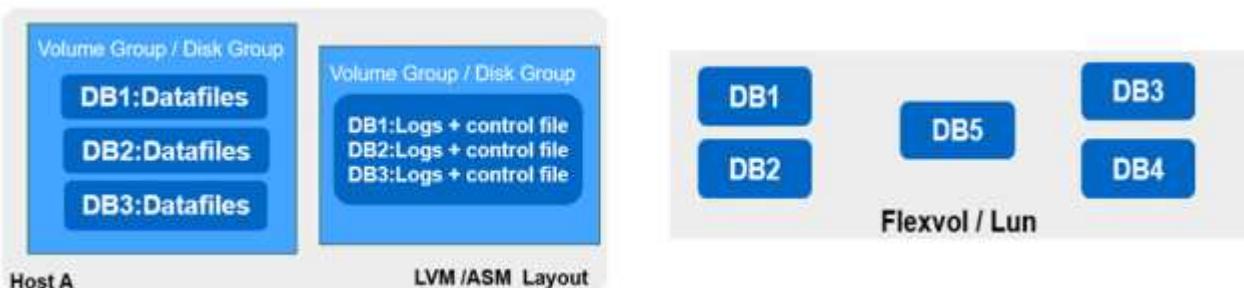
are mounted to the host as either physical or virtual devices. You can host the entire database on a single or multiple storage devices based on the criticality of the environment. Typically, customers isolate data files on dedicated storage from all other files such as control files, redo files, and archive log files. This helps administrators to quickly restore (ONTAP single-file SnapRestore) or clone a large critical database (petabyte scale) using Snapshot technology within few seconds to minutes.



For mission critical workloads that are sensitive to latency, a dedicated storage volume should be deployed to different types of Oracle files to achieve the best latency possible. For a large database, multiple LUNs (NetApp recommends up to eight) per volume should be allocated to data files.



For smaller Oracle databases, SnapCenter supports shared storage layouts in which you can host multiple databases or part of a database on the same storage volume or LUN. As an example of this layout, you can host data files for all the databases on a +DATA ASM disk group or a volume group. The remainder of the files (redo, archive log, and control files) can be hosted on another dedicated disk group or volume group (LVM). Such a deployment scenario is illustrated below.



To facilitate the relocation of Oracle databases, the Oracle binary should be installed on a separate LUN that is included in the regular backup policy. This ensures that in the case of database relocation to a new server host, the Oracle stack can be started for recovery without any potential issues due to an out-of-sync Oracle binary.

Licensing requirements

SnapCenter is licensed software from NetApp. It is generally included in an on-premises ONTAP license. However, for hybrid cloud deployment, a cloud license for SnapCenter is also required to add CVO to SnapCenter as a target data replication destination. Please review following links for SnapCenter standard capacity-based license for details:

[SnapCenter standard capacity-based licenses](#)

Networking and security

In a hybrid database operation that requires an on-premises production database that is burstable to cloud for dev/test and disaster recovery, networking and security is important factor to consider when setting up the environment and connecting to the public cloud from an on-premises data center.

Public clouds typically use a virtual private cloud (VPC) to isolate different users within a public-cloud platform. Within an individual VPC, security is controlled using measures such as security groups that are configurable based on user needs for the lockdown of a VPC.

The connectivity from the on-premises data center to the VPC can be secured through a VPN tunnel. On the VPN gateway, security can be hardened using NAT and firewall rules that block attempts to establish network connections from hosts on the internet to hosts inside the corporate data center.

For networking and security considerations, review the relevant inbound and outbound CVO rules for your public cloud of choice:

- [Security group rules for CVO - AWS](#)
- [Security group rules for CVO - Azure](#)
- [Firewall rules for CVO - GCP](#)

Using Ansible automation to sync DB instances between on-premises and the cloud - optional

To simplify management of a hybrid-cloud database environment, NetApp highly recommends but does not require that you deploy an Ansible controller to automate some management tasks, such as keeping compute instances on-premises and in the cloud in sync. This is particular important because an out-of-sync compute instance in the cloud might render the recovered database in the cloud error prone because of missing kernel packages and other issues.

The automation capability of an Ansible controller can also be used to augment SnapCenter for certain tasks, such as breaking up the SnapMirror instance to activate the DR data copy for production.

Follow these instruction to set up your Ansible control node for RedHat or CentOS machines: [RedHat/CentOS Ansible Controller Setup](#).

Follow these instruction to set up your Ansible control node for Ubuntu or Debian machines: [Ubuntu/Debian Ansible Controller Setup](#).

[Next: Public cloud.](#)

Prerequisites for the public cloud

[Previous: Prerequisites on-premises.](#)

Before we install the Cloud Manager connector and Cloud Volumes ONTAP and configure SnapMirror, we must perform some preparation for our cloud environment. This page describes the work that needs to be done as well as the considerations when deploying Cloud Volumes ONTAP.

Cloud Manager and Cloud Volumes ONTAP deployment prerequisites checklist

- A NetApp Cloud Central login
- Network access from a web browser to several endpoints

- A network location for a Connector
- Cloud provider permissions
- Networking for individual services

For more information about what you need to get started, visit our [cloud documentation](#).

Considerations

1. What is a Cloud Manager connector?

In most cases, a Cloud Central account admin must deploy a connector in your cloud or on-premises network. The connector enables Cloud Manager to manage resources and processes within your public cloud environment.

For more information about Connectors, visit our [cloud documentation](#).

2. Cloud Volumes ONTAP sizing and architecture

When deploying Cloud Volumes ONTAP, you are given the choice of either a predefined package or the creation of your own configuration. Although many of these values can be changed later on nondisruptively, there are some key decisions that need to be made before deployment based on the workloads to be deployed in the cloud.

Each cloud provider has different options for deployment and almost every workload has its own unique properties. NetApp has a [CVO sizing tool](#) that can help size deployments correctly based on capacity and performance, but it has been built around some basic concepts which are worth considering:

- Capacity required
- Network capability of the cloud virtual machine
- Performance characteristics of cloud storage

The key is to plan for a configuration that not only satisfies the current capacity and performance requirements, but also looks at future growth. This is generally known as capacity headroom and performance headroom.

If you would like further information, read the documentation about planning correctly for [AWS](#), [Azure](#), and [GCP](#).

3. Single node or high availability?

In all clouds, there is the option to deploy CVO in either a single node or in a clustered high availability pair with two nodes. Depending on the use case, you might wish to deploy a single node to save costs or an HA pair to provide further availability and redundancy.

For a DR use case or spinning up temporary storage for development and testing, single nodes are common since the impact of a sudden zonal or infrastructure outage is lower. However, for any production use case, when the data is in only a single location, or when the dataset must have more redundancy and availability, high availability is recommended.

For further information about the architecture of each cloud's version of high availability, visit the documentation for [AWS](#), [Azure](#) and [GCP](#).

[Next: Getting started overview.](#)

Getting started overview

[Previous: Prerequisites for the public cloud.](#)

This section provides a summary of the tasks that must be completed to meet the prerequisite requirements as outlined in previous section. The following section provide a high level tasks list for both on-premises and public cloud operations. The detailed processes and procedures can be accessed by clicking on the relevant links.

On-premises

- Setup database admin user in SnapCenter
- SnapCenter plugin installation prerequisites
- SnapCenter host plugin installation
- DB resource discovery
- Setup storage cluster peering and DB volume replication
- Add CVO database storage SVM to SnapCenter
- Setup database backup policy in SnapCenter
- Implement backup policy to protect database
- Validate backup

AWS public cloud

- Pre-flight check
- Steps to deploy Cloud Manager and Cloud Volumes ONTAP in AWS
- Deploy EC2 compute instance for database workload

Click the following links for details:

[On Premises, Public Cloud - AWS](#)

Getting started on premises

[Previous: Getting started overview.](#)

On Premises

1. Setup database admin user in SnapCenter

The NetApp SnapCenter tool uses role-based access control (RBAC) to manage user resources access and permission grants, and SnapCenter installation creates prepopulated roles. You can also create custom roles based on your needs or applications. It makes sense to have a dedicated admin user ID for each database platform supported by SnapCenter for database backup, restoration, and/or disaster recovery. You can also use a single ID to manage all databases. In our test cases and demonstration, we created a dedicated admin user for both Oracle and SQL Server, respectively.

Certain SnapCenter resources can only be provisioned with the SnapCenterAdmin role. Resources can then be assigned to other user IDs for access.

In a pre-installed and configured on-premises SnapCenter environment, the following tasks might have already been completed. If not, the following steps create a database admin user:

1. Add the admin user to Windows Active Directory.
2. Log into SnapCenter using an ID granted with the SnapCenterAdmin role.
3. Navigate to the Access tab under Settings and Users, and click Add to add a new user. The new user ID is linked to the admin user created in Windows Active Directory in step 1. . Assign the proper role to the user as needed. Assign resources to the admin user as applicable.

	Name	Type	Roles	Domain
<input type="checkbox"/>	administrator	User	SnapCenterAdmin	demo
<input type="checkbox"/>	oradba	User	App Backup and Clone Admin	demo
<input type="checkbox"/>	sqldba	User	App Backup and Clone Admin	demo

2. SnapCenter plugin installation prerequisites

SnapCenter performs backup, restore, clone, and other functions by using a plugin agent running on the DB hosts. It connects to the database host and database via credentials configured under the Setting and Credentials tab for plugin installation and other management functions. There are specific privilege requirements based on the target host type, such as Linux or Windows, as well as the type of database.

DB hosts credentials must be configured before SnapCenter plugin installation. Generally, you want to use an administrator user accounts on the DB host as your host connection credentials for plugin installation. You can also grant the same user ID for database access using OS-based authentication. On the other hand, you can also employ database authentication with different database user IDs for DB management access. If you decide to use OS-based authentication, the OS admin user ID must be granted DB access. For Windows domain-based SQL Server installation, a domain admin account can be used to manage all SQL Servers within the domain.

Windows host for SQL server:

1. If you are using Windows credentials for authentication, you must set up your credential before installing plugins.
2. If you are using a SQL Server instance for authentication, you must add the credentials after installing plugins.
3. If you have enabled SQL authentication while setting up the credentials, the discovered instance or database is shown with a red lock icon. If the lock icon appears, you must specify the instance or database credentials to successfully add the instance or database to a resource group.
4. You must assign the credential to a RBAC user without sysadmin access when the following conditions are met:
 - The credential is assigned to a SQL instance.
 - The SQL instance or host is assigned to an RBAC user.
 - The RBAC DB admin user must have both the resource group and backup privileges.

Unix host for Oracle:

1. You must have enabled the password-based SSH connection for the root or non-root user by editing sshd.conf and restarting the sshd service. Password-based SSH authentication on AWS instance is turned off by default.
2. Configure the sudo privileges for the non-root user to install and start the plugin process. After installing the plugin, the processes run as an effective root user.
3. Create credentials with the Linux authentication mode for the install user.
4. You must install Java 1.8.x (64-bit) on your Linux host.
5. Installation of the Oracle database plugin also installs the SnapCenter plugin for Unix.

3. SnapCenter host plugin installation



Before attempting to install SnapCenter plugins on cloud DB server instances, make sure that all configuration steps have been completed as listed in the relevant cloud section for compute instance deployment.

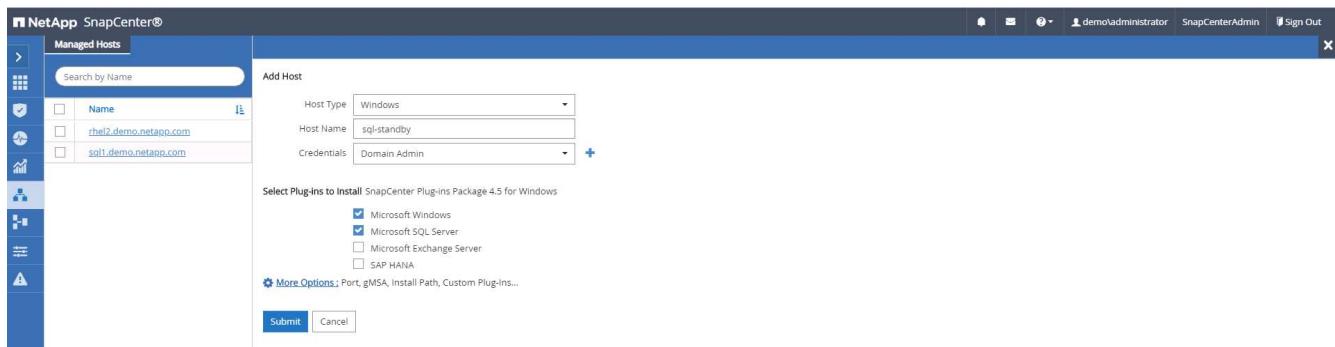
The following steps illustrate how a database host is added to SnapCenter while a SnapCenter plugin is installed on the host. The procedure applies to adding both on-premises hosts and cloud hosts. The following demonstration adds a Windows or a Linux host residing in AWS.

Configure SnapCenter VMware global settings

Navigate to Settings > Global Settings. Select "VMs have iSCSI direct attached disks or NFS for all the hosts" under Hypervisor Settings and click Update.

Add Windows host and installation of plugin on the host

1. Log into SnapCenter with a user ID with SnapCenterAdmin privileges.
2. Click the Hosts tab from the left-hand menu, and then click Add to open the Add Host workflow.
3. Choose Windows for Host Type; the Host Name can be either a host name or an IP address. The host name must be resolved to the correct host IP address from the SnapCenter host. Choose the host credentials created in step 2. Choose Microsoft Windows and Microsoft SQL Server as the plugin packages to be installed.

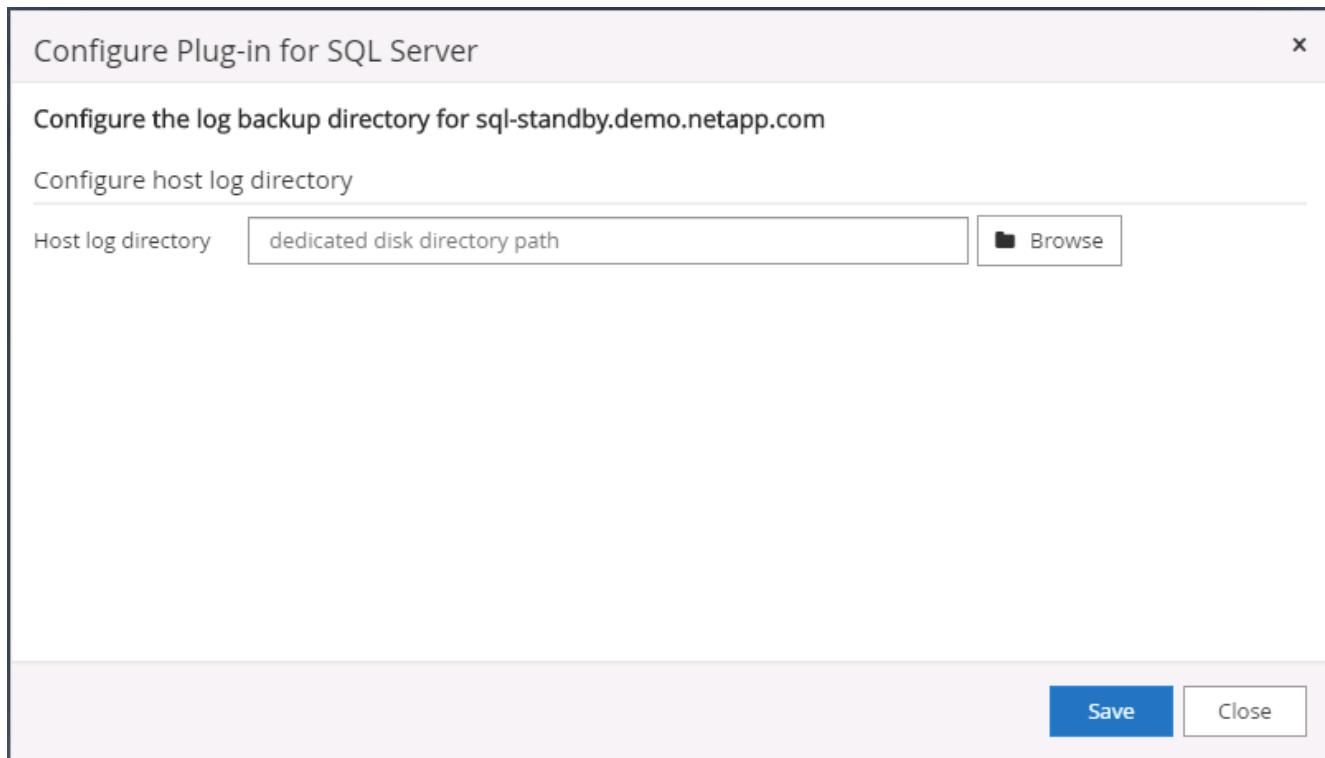


4. After the plugin is installed on a Windows host, its Overall Status is shown as "Configure log directory."

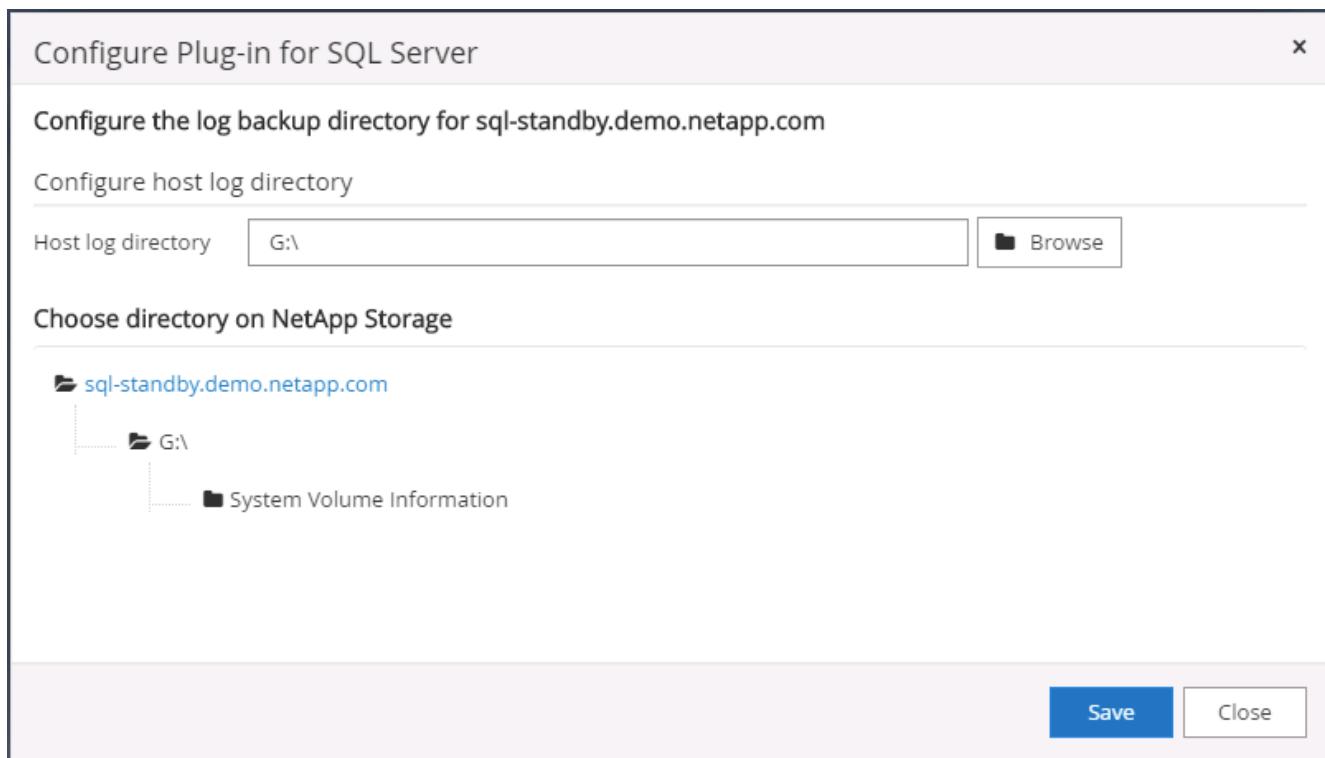
Name	Type	System	Plug-in	Version	Overall Status
rhel2.demo.netapp.com	Linux	Stand-alone	UNIX, Oracle Database	4.5	Running
sql1.demo.netapp.com	Windows	Stand-alone	Microsoft Windows Server, Microsoft SQL Server	4.5	Running
sql-standby.demo.netapp.com	Windows	Stand-alone	Microsoft Windows Server, Microsoft SQL Server	4.5	Configure log directory

5. Click the Host Name to open the SQL Server log directory configuration.

6. Click "Configure log directory" to open "Configure Plug-in for SQL Server."



7. Click Browse to discover NetApp storage so that a log directory can be set; SnapCenter uses this log directory to roll up the SQL server transaction log files. Then click Save.



For NetApp storage provisioned to a DB host to be discovered, the storage (on-prem or CVO) must be added to SnapCenter, as illustrated in step 6 for CVO as an example.

8. After the log directory is configured, the Windows host plugin Overall Status is changed to Running.

- To assign the host to the database management user ID, navigate to the Access tab under Settings and Users, click the database management user ID (in our case the sqldba that the host needs to be assigned to), and click Save to complete host resource assignment.

<input type="checkbox"/>	Asset Name
<input type="checkbox"/>	rhel2.demo.netapp.com
<input type="checkbox"/>	sql1.demo.netapp.com
<input checked="" type="checkbox"/>	sql-standby.demo.netapp.com

Add Unix host and installation of plugin on the host

- Log into SnapCenter with a user ID with SnapCenterAdmin privileges.
- Click the Hosts tab from left-hand menu, and click Add to open the Add Host workflow.
- Choose Linux as the Host Type. The Host Name can be either the host name or an IP address. However, the host name must be resolved to correct host IP address from SnapCenter host. Choose host credentials created in step 2. The host credentials require sudo privileges. Check Oracle Database as the plug-in to be installed, which installs both Oracle and Linux host plugins.

Add Host

Host Type: Linux

Host Name: ora-standby

Credentials: admin

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

- Oracle Database
- SAP HANA

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

Submit **Cancel**

- Click More Options and select "Skip preinstall checks." You are prompted to confirm the skipping of the preinstall check. Click Yes and then Save.

More Options

Port: 8145

Installation Path: /opt/NetApp/snapcenter

Skip preinstall checks

Add all hosts in the oracle RAC

Custom Plug-ins

Choose a File

Browse **Upload**

No plug-ins found.

Save **Cancel**

- Click Submit to start the plugin installation. You are prompted to Confirm Fingerprint as shown below.

Confirm Fingerprint

Authenticity of the host cannot be determined [i](#)

Host name	Fingerprint	Valid
ora-standby.demo.netapp.com	ssh-rsa 3072 5C:02:EF:6B:63:54:59:10:84:DF:4D:6B:AB:FB:61:67	

Confirm and Submit **Close**

6. SnapCenter performs host validation and registration, and then the plugin is installed on the Linux host. The status is changed from Installing Plugin to Running.

Name	Type	System	Plug-in	Version	Overall Status
ora-standby.demo.netapp.com	Linux	Stand-alone	UNIX, Oracle Database	4.5	Running
rhel2.demo.netapp.com	Linux	Stand-alone	UNIX, Oracle Database	4.5	Running
sql1.demo.netapp.com	Windows	Stand-alone	Microsoft Windows Server, Microsoft SQL Server	4.5	Running
sql-standby.demo.netapp.com	Windows	Stand-alone	Microsoft Windows Server, Microsoft SQL Server	4.5	Running

7. Assign the newly added host to the proper database management user ID (in our case, oradba).

User Name: oradba
Domain: demo
Roles: App Backup and Clone Admin

Assign Assets

Asset Name	Type	Asset Type
10.0.0.1	DataOnTapCluster	Storage Connection
192.168.0.101	DataOnTapCluster	Storage Connection
admin		Credentials
Linux Admin		Credentials
Oracle Archive Log Backup		Policy
Oracle Full Online Backup		Policy
rhel2.demo.netapp.com		hnnt

Asset Type: Host

Asset Name

<input checked="" type="checkbox"/>	ora-standby.demo.netapp.com
<input type="checkbox"/>	rhel2.demo.netapp.com
<input type="checkbox"/>	sql1.demo.netapp.com
<input type="checkbox"/>	sql-standby.demo.netapp.com

Save Close

4. Database resource discovery

With successful plugin installation, the database resources on the host can be immediately discovered. Click the Resources tab in the left-hand menu. Depending on the type of database platform, a number of views are

available, such as the database, resources group, and so on. You might need to click the Refresh Resources tab if the resources on the host are not discovered and displayed.

The screenshot shows the NetApp SnapCenter interface for an Oracle Database. The left sidebar has links for Dashboard, Resources (selected), Monitor, Reports, Hosts, Storage Systems, Settings, and Alerts. The main area shows a table with columns: Name, Oracle Database Type, Host/Cluster, Resource Group, Policies, Last Backup, and Overall Status. One row is visible for 'cdb2' with 'Single Instance (Multitenant)' type, 'rhel2.demo.netapp.com' host, and 'Not protected' status.

When the database is initially discovered, the Overall Status is shown as "Not protected." The previous screenshot shows an Oracle database not protected yet by a backup policy.

When a backup configuration or policy is set up and a backup has been executed, the Overall Status for the database shows the backup status as "Backup succeeded" and the timestamp of the last backup. The following screenshot shows the backup status of a SQL Server user database.

The screenshot shows the NetApp SnapCenter interface for Microsoft SQL Server. The left sidebar has links for Dashboard, Resources (selected), Monitor, Reports, Hosts, Storage Systems, Settings, and Alerts. The main area shows a table with columns: Name, Instance, Host, Last Backup, Overall Status, and Type. Several databases are listed, including 'tpcc' which has a timestamp in the 'Last Backup' column and 'Backup succeeded' in the 'Overall Status' column.

If database access credentials are not properly set up, a red lock button indicates that the database is not accessible. For example, if Windows credentials do not have sysadmin access to a database instance, then database credentials must be reconfigured to unlock the red lock.

The screenshot shows the NetApp SnapCenter interface for Microsoft SQL Server. The left sidebar has links for Dashboard, Resources (selected), Monitor, Reports, Hosts, Storage Systems, Settings, and Alerts. The main area shows a table with columns: Name, Host, Resource Groups, Policies, State, and Type. Two instances are listed: 'sql-standby' (with a red lock icon) and 'sql1'. Both are marked as 'Running' in the 'State' column and 'Standalone' in the 'Type' column.

The screenshot shows the NetApp SnapCenter interface for Microsoft SQL Server. The left sidebar has links for Dashboard, Resources (selected), Monitor, Reports, Hosts, Storage Systems, Settings, and Alerts. The main area shows a table titled 'Instance - Credentials' with columns: Name, Host, Resource Groups, Policies, State, and Type. It lists 'sql-standby' and 'sql1'. A note at the top says: 'The Microsoft SQL server or Windows credentials are necessary to unlock the selected instance. Click Refresh Resources to run a discovery with the associated Auth.' Below the table, there is a note: 'Not available for backup. DB is not on NetApp storage, auto-close is enabled or in recovery mode.'

After the appropriate credentials are configured either at the Windows level or the database level, the red lock disappears and SQL Server Type information is gathered and reviewed.

Name	Host	Resource Groups	Policies	State	Type
sql1	sql1.demo.netapp.com			Running	Standalone (15.0.2000)
sql-standby	sql-standby.demo.netapp.com			Running	Standalone (15.0.2000)

5. Setup storage cluster peering and DB volumes replication

To protect your on-premises database data using a public cloud as the target destination, on-premises ONTAP cluster database volumes are replicated to the cloud CVO using NetApp SnapMirror technology. The replicated target volumes can then be cloned for DEV/OPS or disaster recovery. The following high-level steps enable you to set up cluster peering and DB volumes replication.

1. Configure intercluster LIFs for cluster peering on both the on-premises cluster and the CVO cluster instance. This step can be performed with ONTAP System Manager. A default CVO deployment has inter-cluster LIFs configured automatically.

On-premises cluster:

Name	Status	Storage VM	IPspace	Address	Current Node	Current Port	Protocols	Type
onPrem-01_IC	green		Default	192.168.0.113	onPrem-01	e0b		Intercluster
onPrem-01_mgmt1	green		Default	192.168.0.111	onPrem-01	e0c		Cluster/Node Mgmt
cluster_mngt	green		Default	192.168.0.101	onPrem-01	e0a		Cluster/Node Mgmt

Target CVO cluster:

ONTAP System Manager Overview

IPspaces

Cluster	Broadcast Domains
Cluster	Cluster
Default	Storage VMs svm_hybridcvo Broadcast Domains Default

Broadcast Domains

Cluster	9000 MTU	IPSpace: Cluster hybridcvo-01 e0b hybridcvo-02 e0b
Default	9001 MTU	IPSpace: Default hybridcvo-01 e0a hybridcvo-02 e0a

Network Interfaces

Name	Status	Storage VM	IPspace	Address	Current Node	Current Port	Protocols	Type	Throughput (I)
hybridcvo-02_mgmt1	✓		Default	10.221.2.104	hybridcvo-02	e0a		Cluster/Node Mgmt	0
inter_1	✓		Default	10.221.1.180	hybridcvo-01	e0a		Intercluster,Cluster/Node Mgmt	0.02
inter_2	✓		Default	10.221.2.250	hybridcvo-02	e0a		Intercluster,Cluster/Node Mgmt	0.03
iscsi_1	✓	svm_hybridcvo	Default	10.221.1.5	hybridcvo-01	e0a	iSCSI	Data	0
iscsi_2	✓	svm_hybridcvo	Default	10.221.2.168	hybridcvo-02	e0a	iSCSI	Data	0

- With the intercluster LIFs configured, cluster peering and volume replication can be set up by using drag-and-drop in NetApp Cloud Manager. See "[Getting Started - AWS Public Cloud](#)" for details.

Alternatively, cluster peering and DB volume replication can be performed by using ONTAP System Manager as follows:

- Log into ONTAP System Manager. Navigate to Cluster > Settings and click Peer Cluster to set up cluster peering with the CVO instance in the cloud.

ONTAP System Manager Overview (Return to classic version)

UI Settings

- LOG LEVEL: DEBUG
- INACTIVITY TIMEOUT: 30 minutes

Intercluster Settings

Network Interfaces

IP ADDRESS: 192.168.0.113

Cluster Peers

PEERED CLUSTER NAME: hybridcvo

Peer Cluster (highlighted with a red box)
Generate Passphrase
Manage Cluster Peers

Storage VM Peers

PEERED STORAGE VMS: 1

- Go to the Volumes tab. Select the database volume to be replicated and click Protect.

Volumes

Protect (highlighted)

Name
onPrem_data
rhel2_u01
rhel2_u02
rhel2_u03
rhel2_u0309232119421203118
sql1_data
sql1_log
sql1_snapctr
svm_onPrem_root

rhel2_u03 Details

- STATUS:** Online
- STYLE:** FlexVol
- MOUNT PATH:** /rhel2_u03
- STORAGE VM:** svm_onPrem
- LOCAL TIER:** onPrem_01_SSD_1
- SNAPSHOT POLICY:** default
- QUOTA:** Off
- TYPE:** Read Write
- SPACE RESERVATION:**

Capacity
0 Bytes Available | 2.36 GB Used | 2.36 GB Overflow

Performance
Hour Day Week
Latency: 1.5, 1

- Set the protection policy to Asynchronous. Select the destination cluster and storage SVM.

Protect Volumes

PROTECTION POLICY: Asynchronous

Source:
CLUSTER: onPrem
STORAGE VM: svm_onPrem
SELECTED VOLUMES: rhel2_u03

Destination:
CLUSTER: hybridcvo
STORAGE VM: svm_hybridcvo

Destination Settings:
VOLUME NAME: vol_<SourceVolumeName>_dest
PREFIX: vol_
SUFFIX: _dest
 Override default storage service name

Configuration Details:
 Initialize relationship
 Enable FabricPool

Buttons: Save, Cancel

- Validate that the volume is synced between the source and target and that the replication relationship is healthy.

The screenshot shows the 'Volumes' section of the NetApp SnapCenter interface. A table lists volumes with columns for Name, Status, and more. One volume, 'rhe12_u03', is selected and highlighted in blue. Below the table, a tab bar includes 'Overview', 'Snapshot Copies', 'Clone Hierarchy', and 'SnapMirror (Local or Remote)', with 'SnapMirror (Local or Remote)' being the active tab. A detailed table below shows the relationship between the source volume 'svm_onPrem:rhe12_u03' and the destination volume 'svm_hybridcvo:rhe12_u03_dr'. The protection policy is 'MirrorAllSnapshots', and the status is 'Mirrored' with a lag of '12 seconds'.

6. Add CVO database storage SVM to SnapCenter

1. Log into SnapCenter with a user ID with SnapCenterAdmin privileges.
2. Click the Storage System tab from the menu, and then click New to add a CVO storage SVM that hosts replicated target database volumes to SnapCenter. Enter the cluster management IP in the Storage System field, and enter the appropriate username and password.

The screenshot shows the 'Add Storage System' dialog in the NetApp SnapCenter interface. It includes fields for 'Storage System' (IP address 10.0.0.1), 'Username' (admin), and 'Password' (redacted). Below these are 'Event Management System (EMS) & AutoSupport Settings' with checkboxes for 'Send AutoSupport notification to storage system' and 'Log SnapCenter Server events to syslog'. There is also a link to 'More Options'. At the bottom are 'Submit', 'Cancel', and 'Reset' buttons.

3. Click More Options to open additional storage configuration options. In the Platform field, select Cloud Volumes ONTAP, check Secondary, and then click Save.

The screenshot shows the 'More Options' configuration dialog. It contains fields for 'Platform' (Cloud Volumes ONTAP), 'Protocol' (HTTPS), 'Port' (443), 'Timeout' (60 seconds), and 'Preferred IP' (checkbox). A checkbox labeled 'Secondary' is checked. At the bottom are 'Save' and 'Cancel' buttons.

4. Assign the storage systems to SnapCenter database management user IDs as shown in [3. SnapCenter host plugin installation](#).

The screenshot shows the ONTAP Storage section of the NetApp SnapCenter interface. On the left is a navigation sidebar with options like Dashboard, Resources, Monitor, Reports, Hosts, Storage Systems (which is selected), Settings, and Alerts. The main area is titled 'ONTAP Storage' and shows 'ONTAP Storage Connections'. A table lists three connections: 'svm_hybridcvo' (IP: 10.0.0.1, Cluster Name: 10.0.0.1, User Name: [redacted], Platform: CVO, Controller License: crossed out) and 'svm_onPrem' (IP: 192.168.0.101, Cluster Name: [redacted], User Name: [redacted], Platform: CVO, Controller License: checked). There are 'New' and 'Delete' buttons at the top right.

7. Setup database backup policy in SnapCenter

The following procedures demonstrates how to create a full database or log file backup policy. The policy can then be implemented to protect databases resources. The recovery point objective (RPO) or recovery time objective (RTO) dictates the frequency of database and/or log backups.

Create a full database backup policy for Oracle

1. Log into SnapCenter as a database management user ID, click Settings, and then click Polices.

The screenshot shows the Policies section of the NetApp SnapCenter interface. The navigation sidebar includes Storage Systems (selected), Settings, and Alerts. The main area is titled 'Policies' and shows 'Oracle Database' backup policies. A table lists two policies: 'Oracle Archive Log Backup' (Backup Type: LOG, ONLINE, Schedule Type: Hourly, Replication: SnapMirror, Verification: [redacted]) and 'Oracle Full Online Backup' (Backup Type: FULL, ONLINE, Schedule Type: Daily, Replication: SnapMirror, Verification: [redacted]). There are 'New', 'Edit', 'Copy', 'Delete', 'Details', and 'Clone' buttons at the top right.

2. Click New to launch a new backup policy creation workflow or choose an existing policy for modification.

Modify Oracle Database Backup Policy x

1 Name

Provide a policy name

Policy name i

Details

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Previous Next

3. Select the backup type and schedule frequency.

Modify Oracle Database Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Select Oracle database backup options

Choose backup type

Online backup

Datafiles, control files, and archive logs

Datafiles and control files

Archive logs

Offline backup i

Mount i

Shutdown

Save state of PDBs i

Choose schedule frequency

Select how often you want the schedules to occur in the policy. The specific times are set at backup job creation enabling you to stagger your start times.

On demand

Hourly

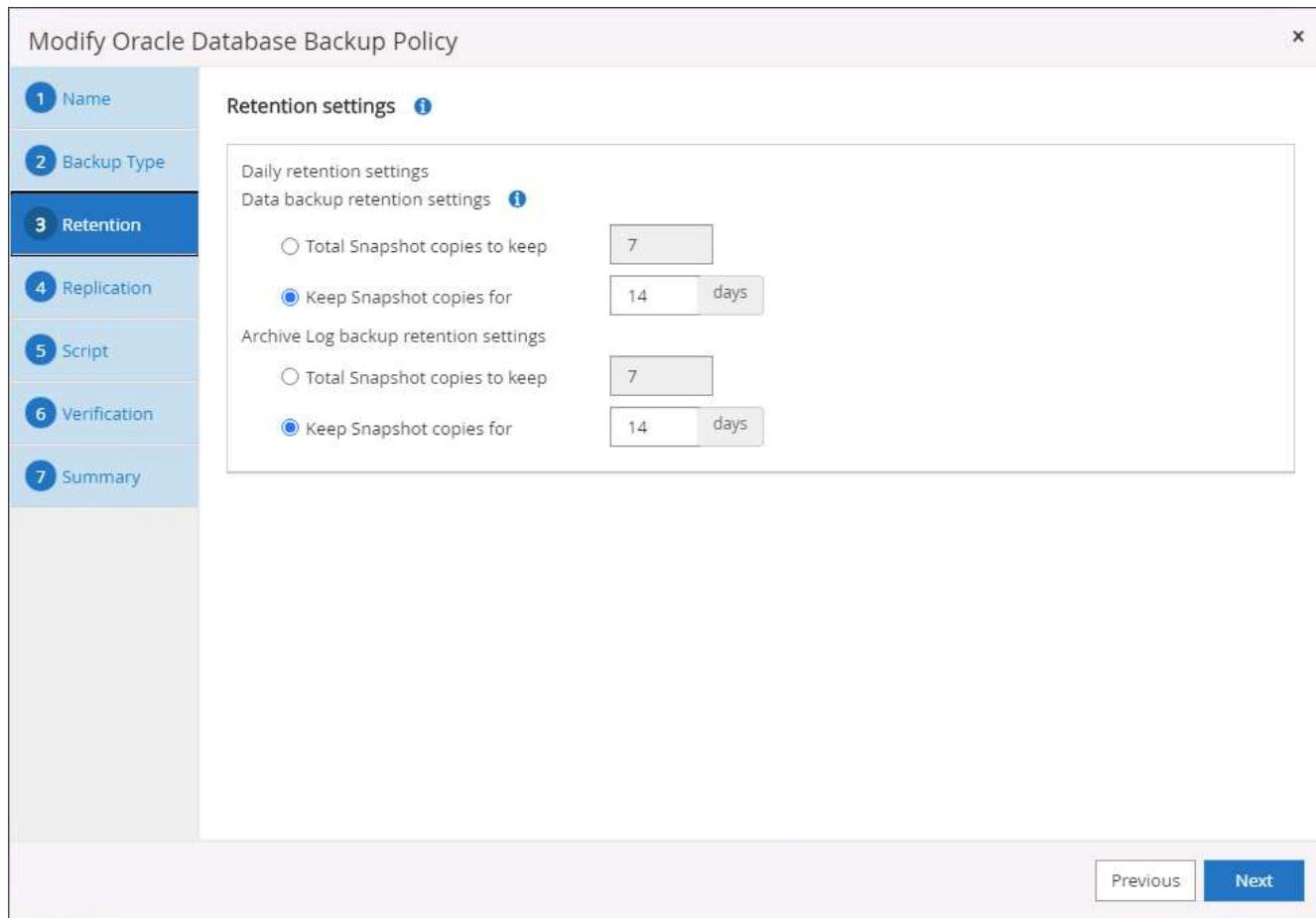
Daily

Previous

Next

This screenshot shows the 'Modify Oracle Database Backup Policy' wizard, specifically step 2: Backup Type. The left sidebar lists steps 1 through 7. Step 2 is currently active, indicated by a blue background. The main area is titled 'Select Oracle database backup options'. Under 'Choose backup type', 'Online backup' and 'Datafiles, control files, and archive logs' are selected. Other options like 'Datafiles and control files' and 'Archive logs' are available but not selected. Below that, 'Offline backup' is listed with a question mark icon, and 'Mount' is selected with a blue circle icon. 'Shutdown' is also listed. A checkbox for 'Save state of PDBs' is present but unchecked. Under 'Choose schedule frequency', 'Daily' is selected. At the bottom right are 'Previous' and 'Next' buttons.

- Set the backup retention setting. This defines how many full database backup copies to keep.



5. Select the secondary replication options to push local primary snapshots backups to be replicated to a secondary location in cloud.

Modify Oracle Database Backup Policy x

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Select secondary replication options i

Update SnapMirror after creating a local Snapshot copy.

Update SnapVault after creating a local Snapshot copy.

Secondary policy label Daily i

Error retry count 3 i

Previous Next

6. Specify any optional script to run before and after a backup run.

Modify Oracle Database Backup Policy X

Specify optional scripts to run before and after performing a backup job

1 Name	Prescript full path <input type="text" value="/var/opt/snapcenter/spl/scripts/"/> Enter Prescript path	
2 Backup Type	Prescript arguments <input type="text"/>	
3 Retention	Postscript full path <input type="text" value="/var/opt/snapcenter/spl/scripts/"/> Enter Postscript path	
4 Replication	Postscript arguments <input type="text"/>	
5 Script	Script timeout 60	secs
6 Verification		
7 Summary		

Previous **Next**

7. Run backup verification if desired.

Modify Oracle Database Backup Policy X

1 Name

Select the options to run backup verification

2 Backup Type

Run Verifications for following backup schedules

Select how often you want the schedules to occur in the policy. The specific verification times are set at backup job creation enabling you to stagger your verification start times.

Daily

3 Retention

4 Replication

5 Script

6 Verification

Verification script commands

Script timeout secs

Prescript full path Enter Prescript path

Prescript arguments

Postscript full path Enter Postscript path

Postscript arguments

7 Summary

Previous Next

8. Summary.

Modify Oracle Database Backup Policy

1 Name	Summary
2 Backup Type	Policy name: Oracle Full Online Backup Details: Backup all data and log files
3 Retention	Backup type: Online backup
4 Replication	Schedule type: Daily RMAN catalog backup: Disabled
5 Script	Archive log pruning: None On demand data backup retention: None
6 Verification	On demand archive log backup retention: None Hourly data backup retention: None Hourly archive log backup retention: None
7 Summary	Daily data backup retention: Delete Snapshot copies older than : 14 days Daily archive log backup retention: Delete Snapshot copies older than : 14 days Weekly data backup retention: None Weekly archive log backup retention: None Monthly data backup retention: None Monthly archive log backup retention: None Replication: SnapMirror enabled , Secondary policy label: Daily , Error retry count: 3

Previous Finish

Create a database log backup policy for Oracle

1. Log into SnapCenter with a database management user ID, click Settings, and then click Policies.
2. Click New to launch a new backup policy creation workflow, or choose an existing policy for modification.

New Oracle Database Backup Policy X

1 Name

Provide a policy name

Policy name i

Details

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Previous Next

The screenshot shows the 'New Oracle Database Backup Policy' wizard. The 'Name' step is active, with the policy name set to 'Oracle Archive Log Backup' and details indicating it's for 'Backup Oracle archive logs'. The sidebar lists steps 2 through 7: Backup Type, Retention, Replication, Script, Verification, and Summary. The bottom right has 'Previous' and 'Next' buttons.

3. Select the backup type and schedule frequency.

New Oracle Database Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Select Oracle database backup options

Choose backup type

Online backup

Datafiles, control files, and archive logs

Datafiles and control files

Archive logs

Offline backup i

Mount

Shutdown

Save state of PDBs i

Choose schedule frequency

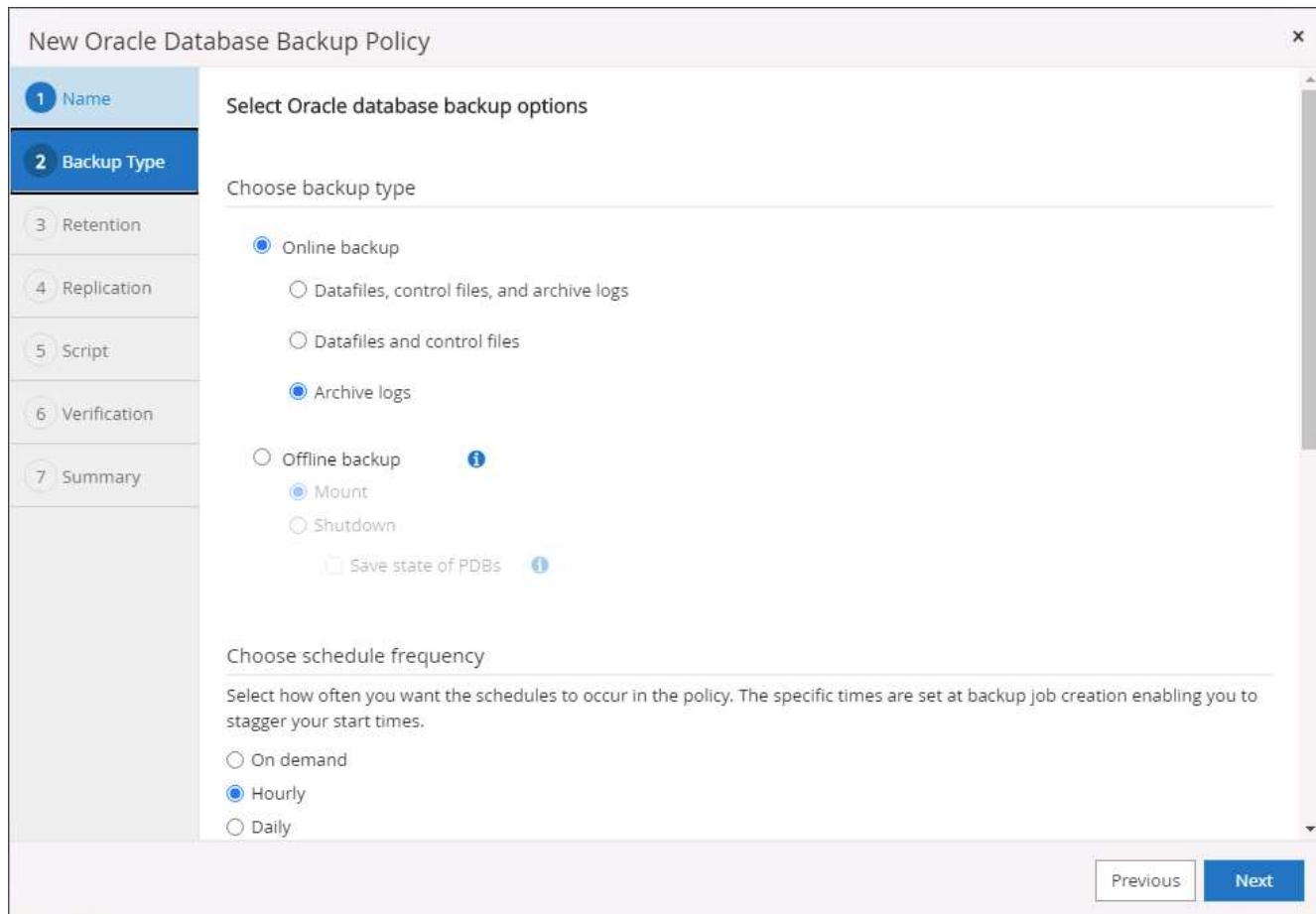
Select how often you want the schedules to occur in the policy. The specific times are set at backup job creation enabling you to stagger your start times.

On demand

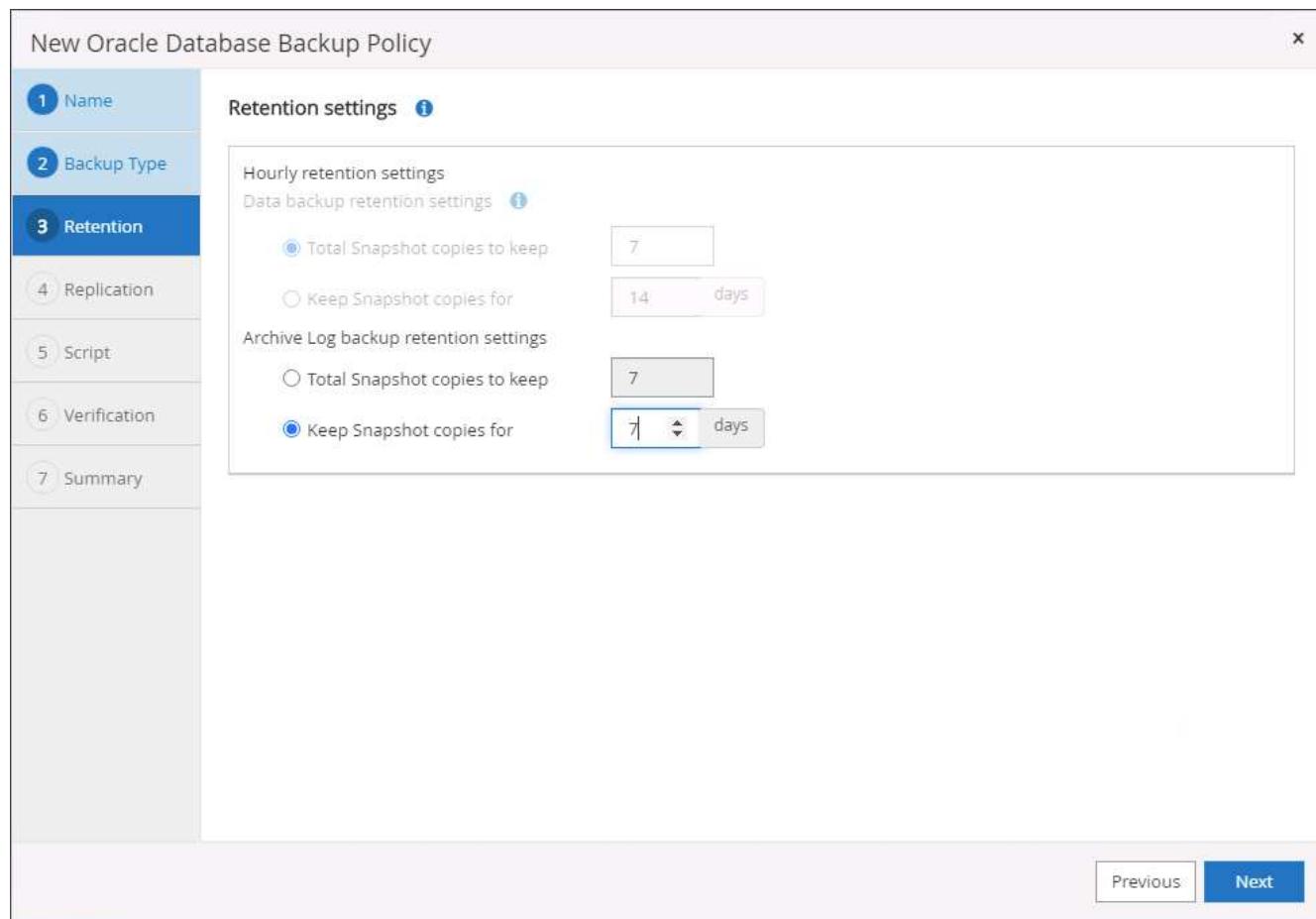
Hourly

Daily

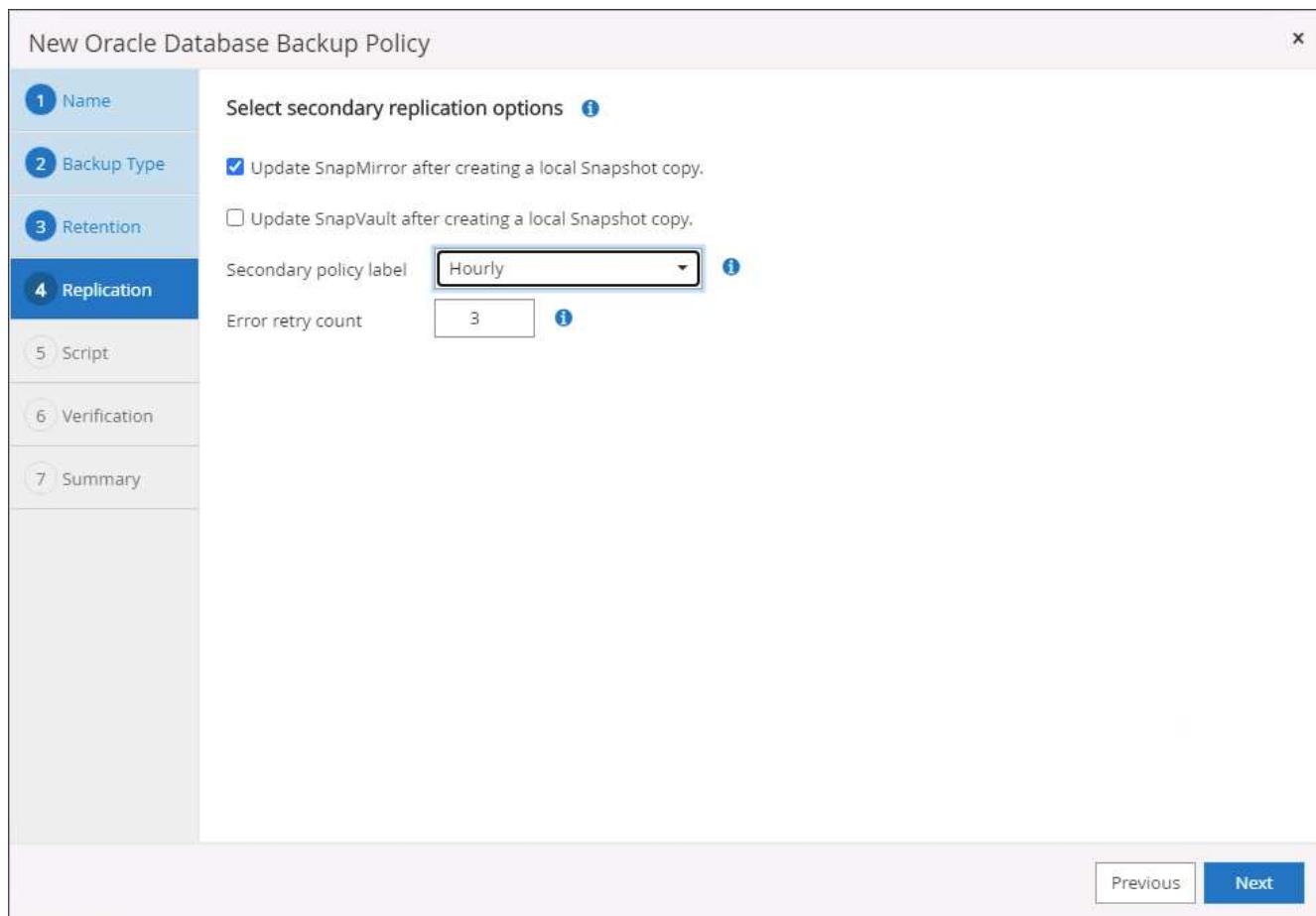
[Previous](#) [Next](#)



4. Set the log retention period.



5. Enable replication to a secondary location in the public cloud.



6. Specify any optional scripts to run before and after log backup.

New Oracle Database Backup Policy X

Specify optional scripts to run before and after performing a backup job

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Prescript full path: /var/opt/snapcenter/spl/scripts/ Enter Prescript path

Prescript arguments:

Postscript full path: /var/opt/snapcenter/spl/scripts/ Enter Postscript path

Postscript arguments:

Script timeout: 60 secs

Previous Next

7. Specify any backup verification scripts.

New Oracle Database Backup Policy X

1 Name
Select the options to run backup verification

2 Backup Type
Run Verifications for following backup schedules

3 Retention
Select how often you want the schedules to occur in the policy. The specific verification times are set at backup job creation enabling you to stagger your verification start times.

4 Replication

5 Script

6 Verification

7 Summary

Verification script commands

Script timeout 60 secs

Prescript full path /var/opt/snapcenter/spl/scripts/ Enter Prescript path

Prescript arguments Choose optional arguments...

Postscript full path /var/opt/snapcenter/spl/scripts/ Enter Postscript path

Postscript arguments Choose optional arguments...

[Previous](#) [Next](#)

8. Summary.

New Oracle Database Backup Policy

1 Name	Summary
2 Backup Type	Policy name: Oracle Archive Log Backup Details: Backup Oracle archive logs
3 Retention	Backup type: Online backup
4 Replication	Schedule type: Hourly RMAN catalog backup: Disabled
5 Script	Archive log pruning: None
6 Verification	On demand data backup retention: None
7 Summary	On demand archive log backup retention: None Hourly data backup retention: None Hourly archive log backup retention: Delete Snapshot copies older than : 7 days Daily data backup retention: None Daily archive log backup retention: None Weekly data backup retention: None Weekly archive log backup retention: None Monthly data backup retention: None Monthly archive log backup retention: None Replication: SnapMirror enabled , Secondary policy label: Hourly , Error retry count: 3
	Previous Finish

Create a full database backup policy for SQL

1. Log into SnapCenter with a database management user ID, click Settings, and then click Policies.

The screenshot shows the NetApp SnapCenter web interface. On the left is a navigation sidebar with links for Dashboard, Resources, Monitor, Reports, Hosts, Storage Systems, Settings (which is selected), and Alerts. The main content area has a header with 'NetApp SnapCenter®' and tabs for 'Policies' (selected) and 'Credential'. A dropdown menu shows 'Microsoft SQL Server'. Below this is a search bar with 'Search by Name'. The main table has columns for 'Name', 'Backup Type', 'Schedule Type', 'Replication', and 'Verification'. A message at the bottom of the table says 'There is no match for your search or data is not available.' To the right of the table are buttons for 'New', 'Modify', 'Copy', 'Details', and 'Delete'.

2. Click New to launch a new backup policy creation workflow, or choose an existing policy for modification.

New SQL Server Backup Policy

1 Name

Provide a policy name

Policy name: SQL Server Full Backup i

Details: Backup all data and log files

2 Backup Type

3 Retention

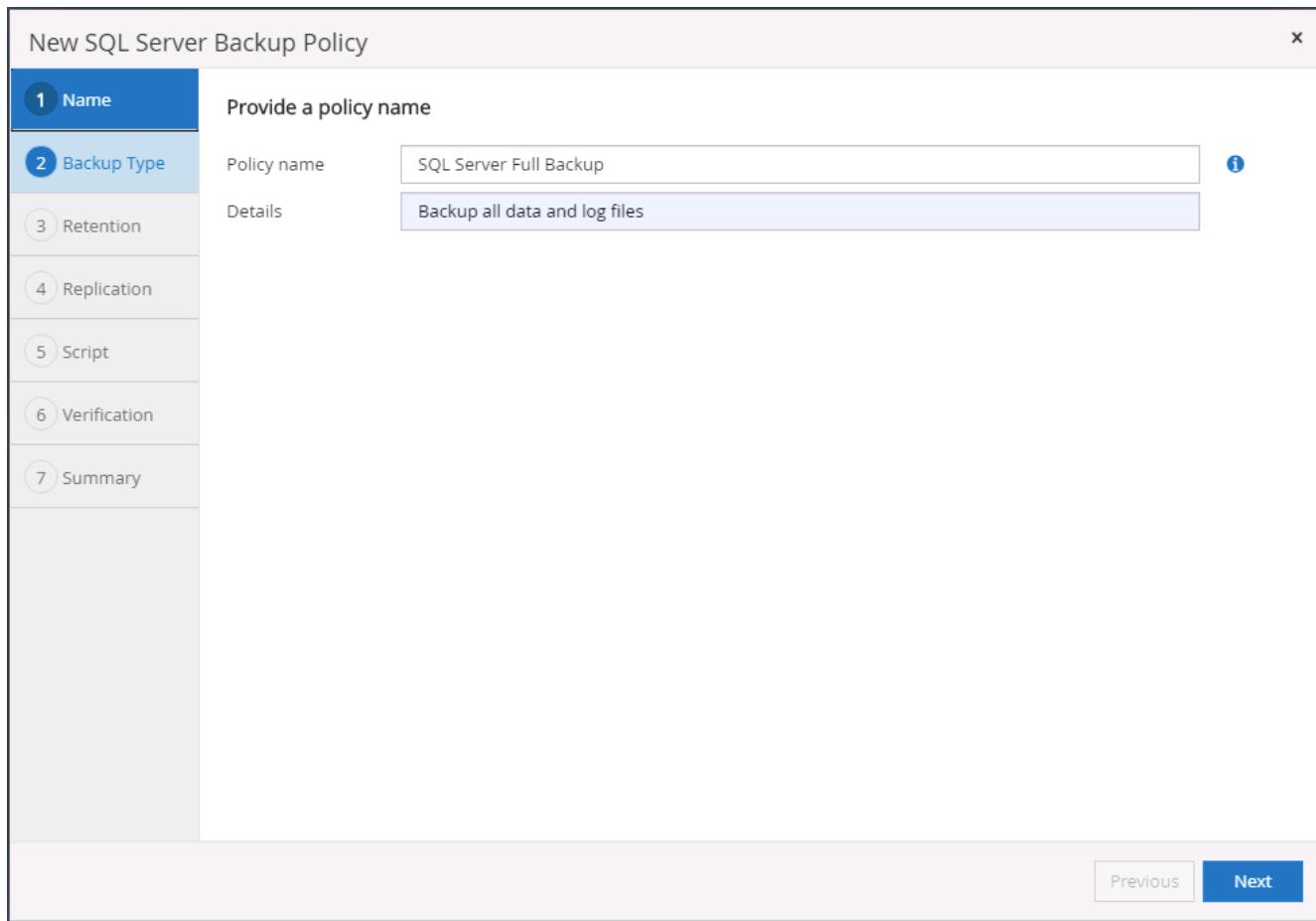
4 Replication

5 Script

6 Verification

7 Summary

Previous Next



3. Define the backup option and schedule frequency. For SQL Server configured with an availability group, a preferred backup replica can be set.

New SQL Server Backup Policy X

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Select SQL server backup options

Choose backup type

Full backup and log backup

Full backup

Log backup

Copy only backup i

Maximum databases backed up per Snapshot copy: 100 i

Availability Group Settings ▼

Schedule frequency

Select how often you want the schedules to occur in the policy. The specific times are set at backup job creation enabling you to stagger your start times.

On demand

Hourly

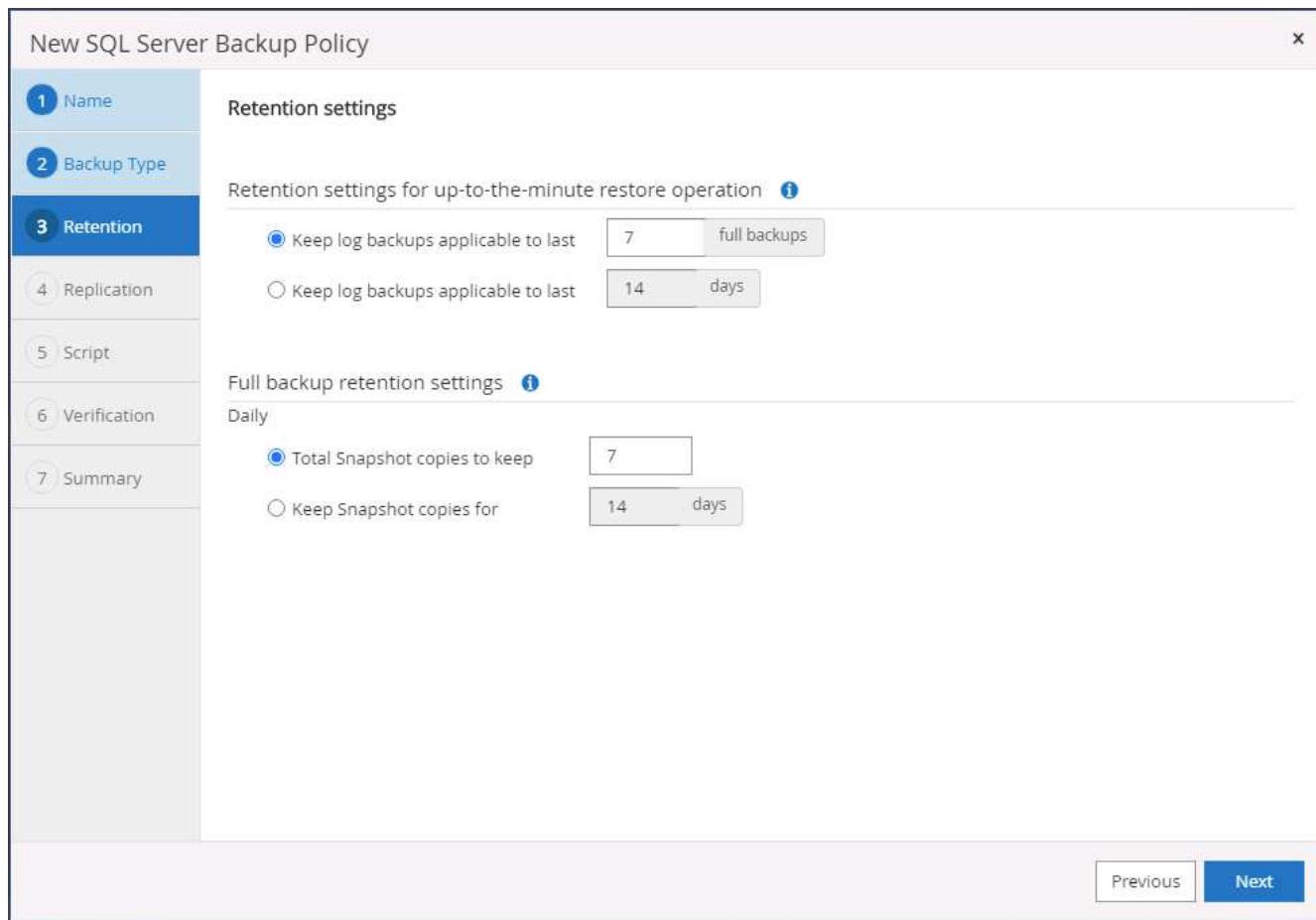
Daily

Weekly

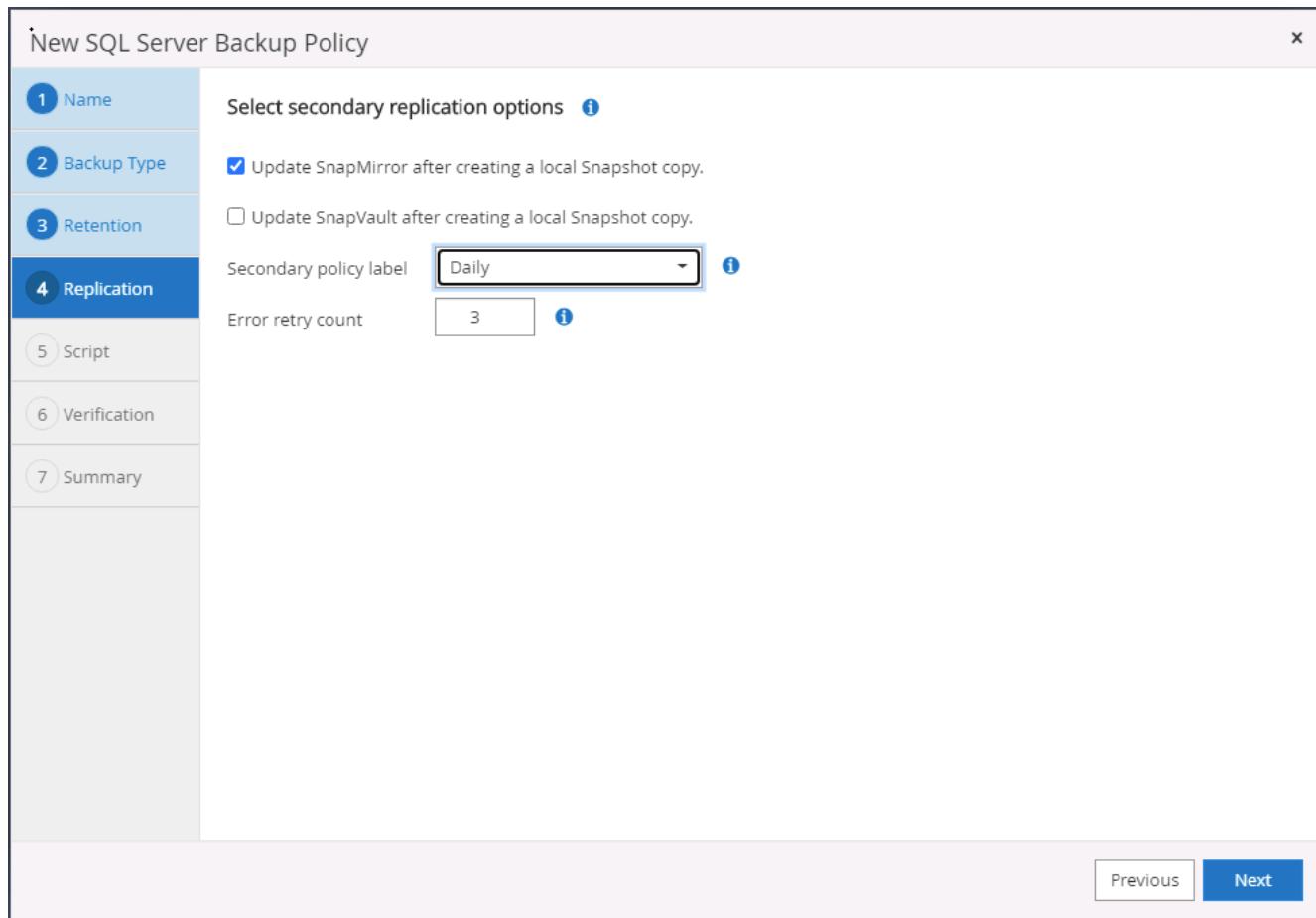
Monthly

Previous Next

4. Set the backup retention period.



5. Enable backup copy replication to a secondary location in cloud.



6. Specify any optional scripts to run before or after a backup job.

New SQL Server Backup Policy X

1 Name Specify optional scripts to run before performing a backup job

2 Backup Type Prescript full path

3 Retention Prescript arguments Choose optional arguments...

4 Replication

5 Script Specify optional scripts to run after performing a backup job

6 Verification Postscript full path

7 Summary Postscript arguments Choose optional arguments...

Script timeout secs

Previous Next

7. Specify the options to run backup verification.

New SQL Server Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Select the options to run backup verification

Run verifications for the following backup schedules

Select how often you want the schedules to occur in the policy. The specific verification times are set at backup job creation enabling you to stagger your verification start times.

Daily

Database consistency checks options

Limit the integrity structure to physical structure of the database (PHYSICAL_ONLY)

Suppress all information message (NO_INFOMSGS)

Display all reported error messages per object (ALL_ERRORMSGGS)

Do not check non-clustered indexes (NOINDEX)

Limit the checks and obtain the locks instead of using an internal database Snapshot copy (TABLOCK)

Log backup

Verify log backup. i

Verification script settings

Script timeout secs

Previous Next

8. Summary.

New SQL Server Backup Policy X

1	Name																										
2	Backup Type																										
3	Retention																										
4	Replication																										
5	Script																										
6	Verification																										
7	Summary																										
<p>Summary</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 15%;">Policy name</td> <td>SQL Server Full Backup</td> </tr> <tr> <td>Details</td> <td>Backup all data and log files</td> </tr> <tr> <td>Backup type</td> <td>Full backup and log backup</td> </tr> <tr> <td>Availability group settings</td> <td>Backup only on preferred backup replica</td> </tr> <tr> <td>Schedule Type</td> <td>Daily</td> </tr> <tr> <td>UTM retention</td> <td>Total backup copies to retain : 7</td> </tr> <tr> <td>Daily Full backup retention</td> <td>Total backup copies to retain : 7</td> </tr> <tr> <td>Replication</td> <td>SnapMirror enabled , Secondary policy label: Daily , Error retry count: 3</td> </tr> <tr> <td>Backup prescript settings</td> <td>undefined Prescript arguments:</td> </tr> <tr> <td>Backup postscript settings</td> <td>undefined Postscript arguments:</td> </tr> <tr> <td>Verification for backup schedule type</td> <td>none</td> </tr> <tr> <td>Verification prescript settings</td> <td>undefined Prescript arguments:</td> </tr> <tr> <td>Verification postscript settings</td> <td>undefined Postscript arguments:</td> </tr> </table>		Policy name	SQL Server Full Backup	Details	Backup all data and log files	Backup type	Full backup and log backup	Availability group settings	Backup only on preferred backup replica	Schedule Type	Daily	UTM retention	Total backup copies to retain : 7	Daily Full backup retention	Total backup copies to retain : 7	Replication	SnapMirror enabled , Secondary policy label: Daily , Error retry count: 3	Backup prescript settings	undefined Prescript arguments:	Backup postscript settings	undefined Postscript arguments:	Verification for backup schedule type	none	Verification prescript settings	undefined Prescript arguments:	Verification postscript settings	undefined Postscript arguments:
Policy name	SQL Server Full Backup																										
Details	Backup all data and log files																										
Backup type	Full backup and log backup																										
Availability group settings	Backup only on preferred backup replica																										
Schedule Type	Daily																										
UTM retention	Total backup copies to retain : 7																										
Daily Full backup retention	Total backup copies to retain : 7																										
Replication	SnapMirror enabled , Secondary policy label: Daily , Error retry count: 3																										
Backup prescript settings	undefined Prescript arguments:																										
Backup postscript settings	undefined Postscript arguments:																										
Verification for backup schedule type	none																										
Verification prescript settings	undefined Prescript arguments:																										
Verification postscript settings	undefined Postscript arguments:																										
Previous Finish																											

Create a database log backup policy for SQL.

1. Log into SnapCenter with a database management user ID, click Settings > Policies, and then New to launch a new policy creation workflow.

New SQL Server Backup Policy

1 Name

Provide a policy name

Policy name: SQL Server Log Backup

Details: Backup SQL server log

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Previous Next

The screenshot shows the 'New SQL Server Backup Policy' wizard. The 'Name' tab is active. The 'Policy name' field is set to 'SQL Server Log Backup'. The 'Details' field contains the text 'Backup SQL server log'. The sidebar on the left lists other tabs: 'Backup Type', 'Retention', 'Replication', 'Script', 'Verification', and 'Summary'. At the bottom right are 'Previous' and 'Next' buttons.

- Define the log backup option and schedule frequency. For SQL Server configured with a availability group, a preferred backup replica can be set.

New SQL Server Backup Policy X

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Select SQL server backup options

Choose backup type

Full backup and log backup
 Full backup
 Log backup
 Copy only backup i

Maximum databases backed up per Snapshot copy: 100 i

Availability Group Settings ▼

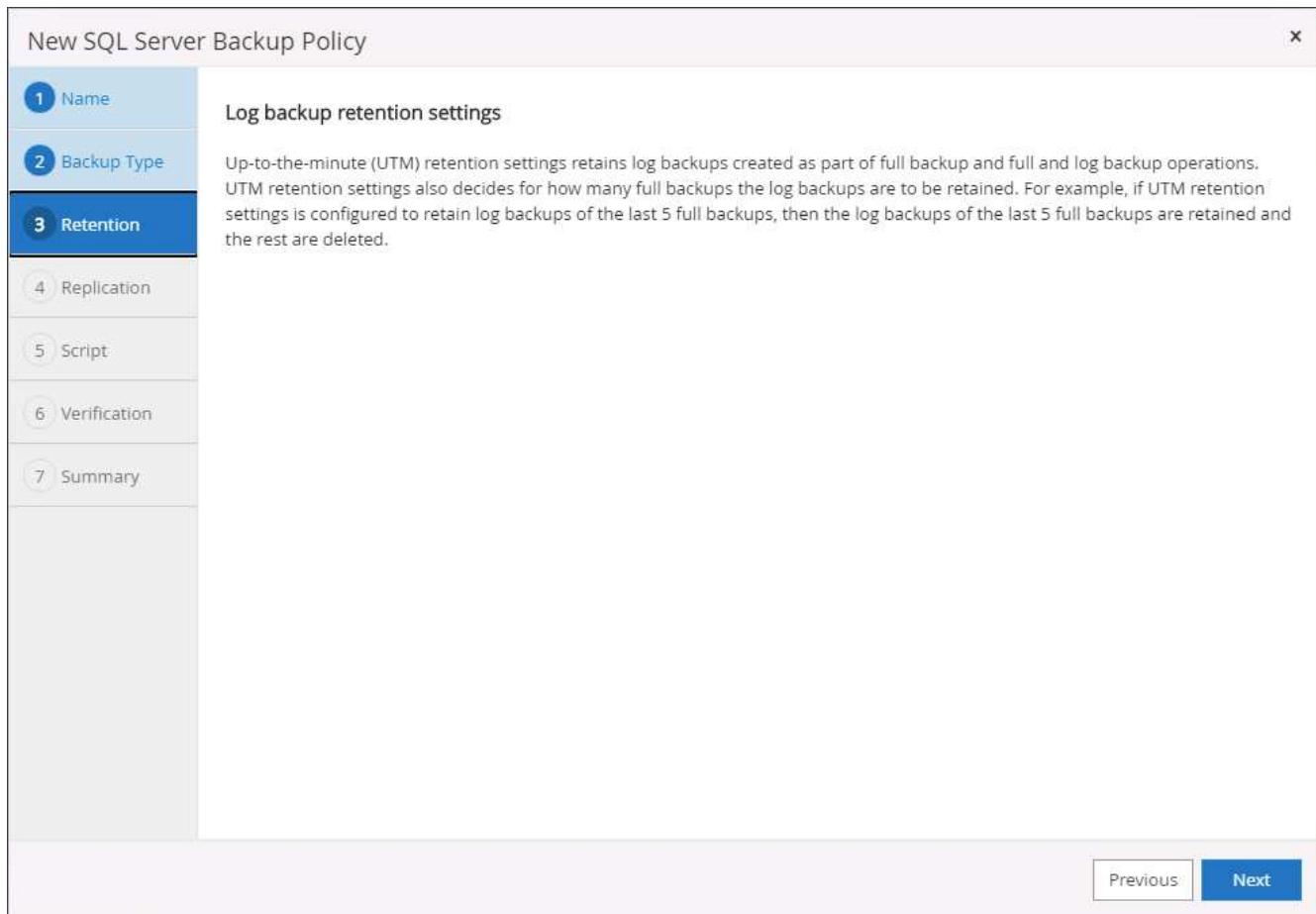
Schedule frequency

Select how often you want the schedules to occur in the policy. The specific times are set at backup job creation enabling you to stagger your start times.

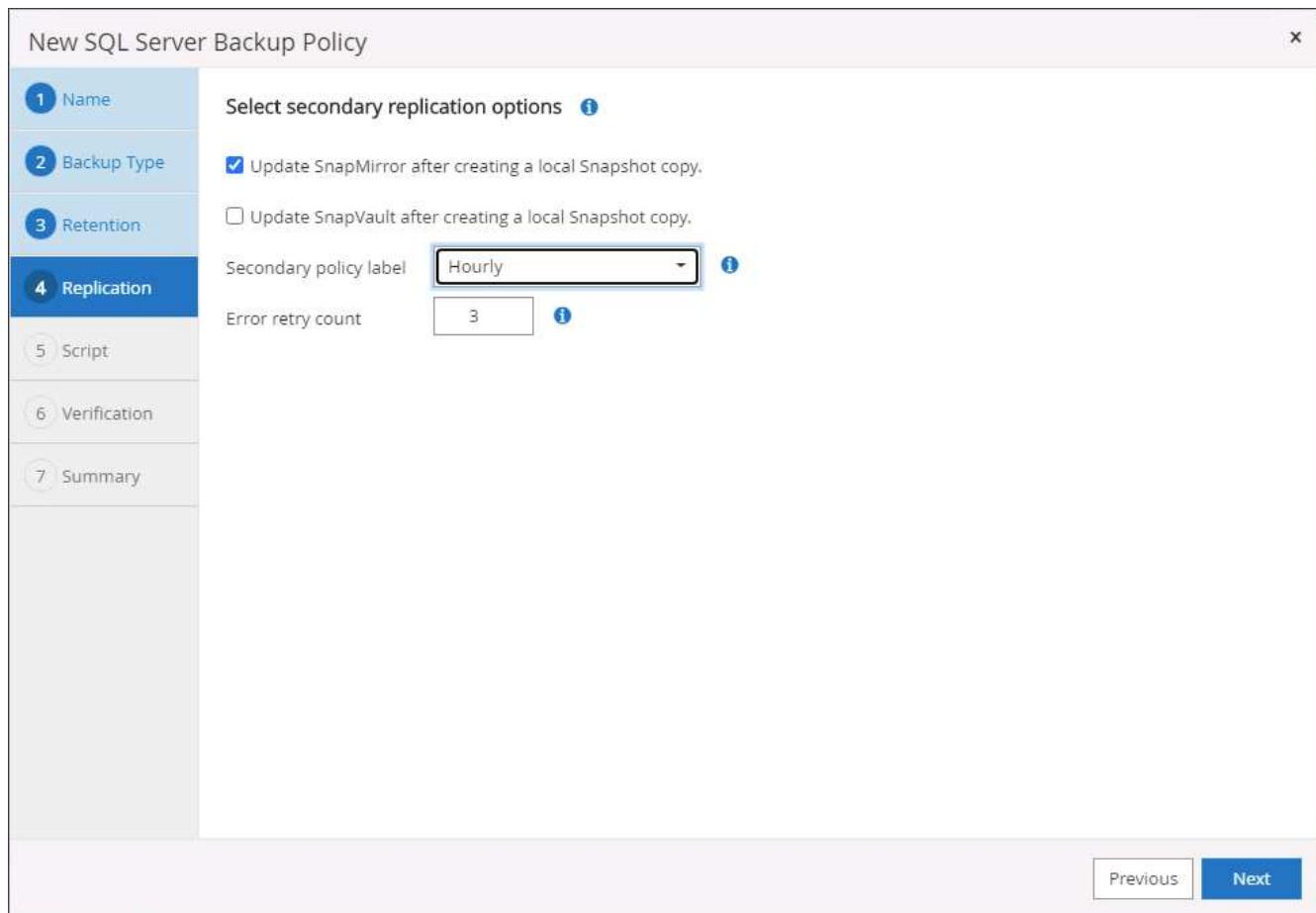
On demand
 Hourly
 Daily
 Weekly
 Monthly

Previous Next

3. SQL server data backup policy defines the log backup retention; accept the defaults here.



4. Enable log backup replication to secondary in the cloud.



5. Specify any optional scripts to run before or after a backup job.

New SQL Server Backup Policy X

1 Name Specify optional scripts to run before performing a backup job

2 Backup Type Prescript full path

3 Retention Prescript arguments Choose optional arguments...

4 Replication Specify optional scripts to run after performing a backup job

5 Script Postscript full path

Postscript arguments Choose optional arguments...

Script timeout 60 secs

6 Verification

7 Summary

Previous Next

6. Summary.

New SQL Server Backup Policy

Step	Summary
1 Name	Policy name: SQL Server Log Backup
2 Backup Type	Details: Backup SQL server log Backup type: Log transaction backup
3 Retention	Availability group settings: Backup only on preferred backup replica
4 Replication	Schedule Type: Hourly
5 Script	Replication: SnapMirror enabled, Secondary policy label: Hourly, Error retry count: 3
6 Verification	Backup prescript settings: undefined Prescript arguments: Backup postscript settings: undefined Postscript arguments:
7 Summary	Verification for backup schedule type: none Verification prescript settings: undefined Prescript arguments: Verification postscript settings: undefined Postscript arguments:

[Previous](#) [Finish](#)

8. Implement backup policy to protect database

SnapCenter uses a resource group to backup a database in a logical grouping of database resources, such as multiple databases hosted on a server, a database sharing the same storage volumes, multiple databases supporting a business application, and so on. Protecting a single database creates a resource group of its own. The following procedures demonstrate how to implement a backup policy created in section 7 to protect Oracle and SQL Server databases.

Create a resource group for full backup of Oracle

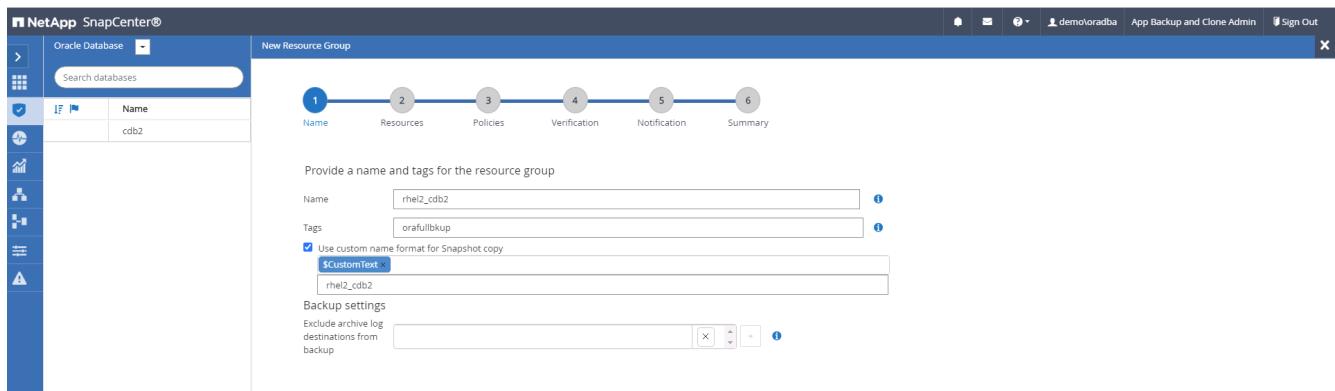
1. Log into SnapCenter with a database management user ID, and navigate to the Resources tab. In the View drop-down list, choose either Database or Resource Group to launch the resource group creation workflow.

The screenshot shows the NetApp SnapCenter interface. The top navigation bar includes links for Dashboard, Oracle Database, demotoradb, App Backup and Clone Admin, and Sign Out. The left sidebar has links for Resources, Monitor, Reports, Hosts, Storage Systems, Settings, and Alerts. The main content area is titled "Oracle Database" and shows a table with one row:

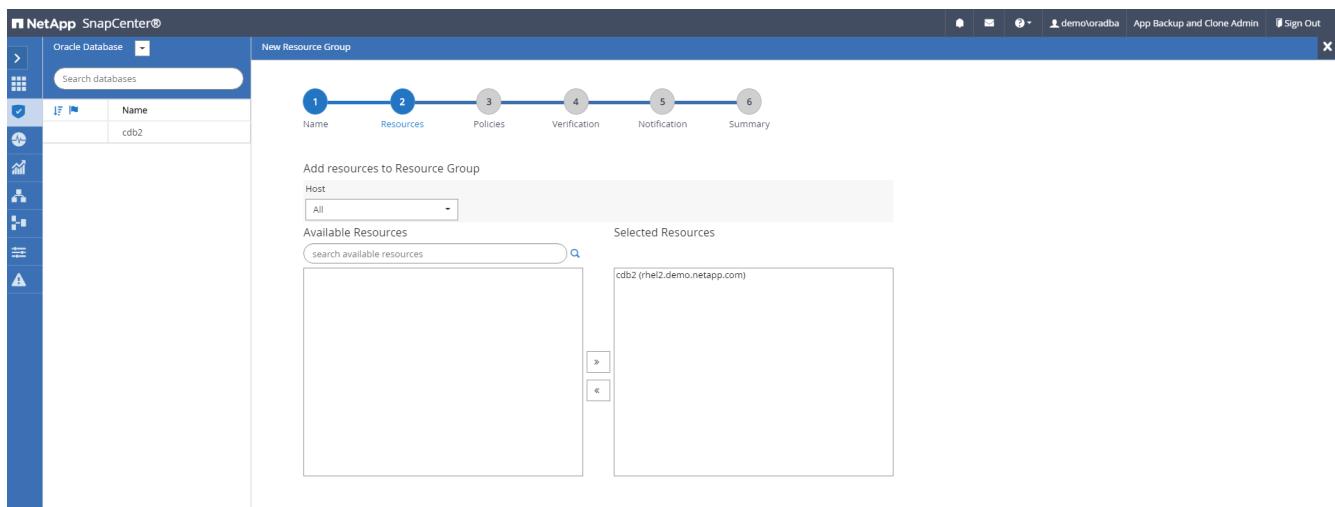
Name	Oracle Database Type	Host/Cluster	Resource Group	Policies	Last Backup	Overall Status
cdb2	Single Instance (Multitenant)	rhel2.demo.netapp.com				Not protected

Buttons at the bottom right include Refresh Resources and New Resource Group.

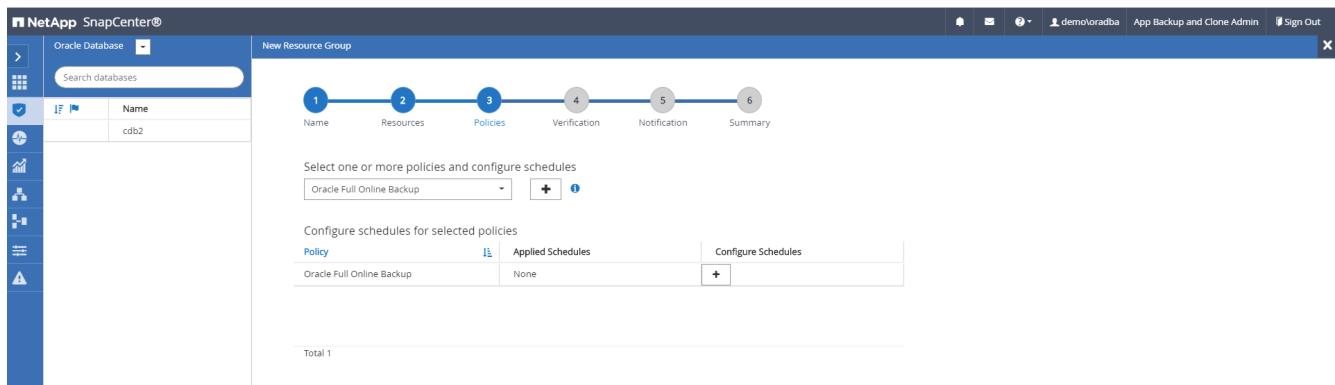
2. Provide a name and tags for the resource group. You can define a naming format for the Snapshot copy and bypass the redundant archive log destination if configured.



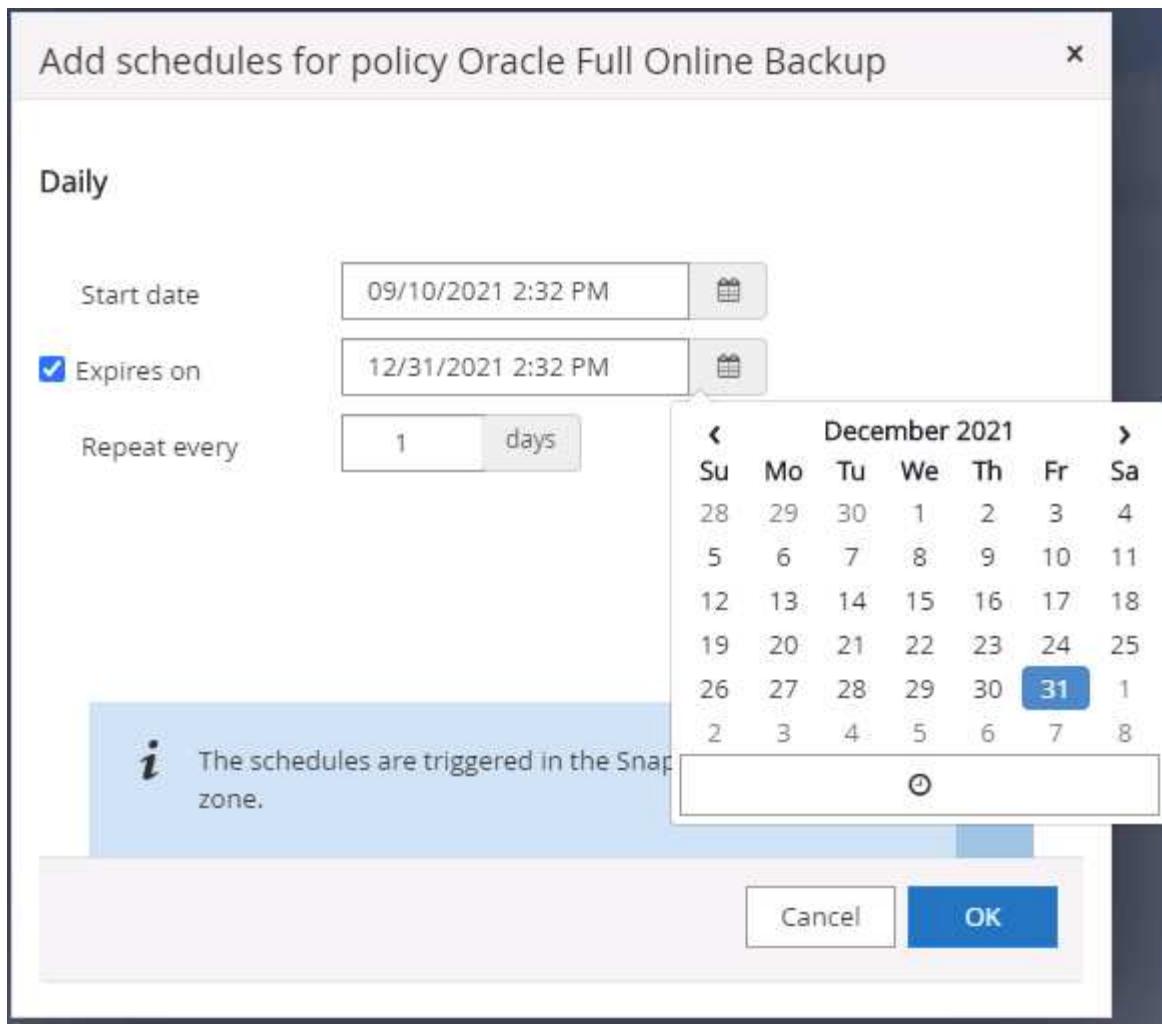
3. Add database resources to the resource group.



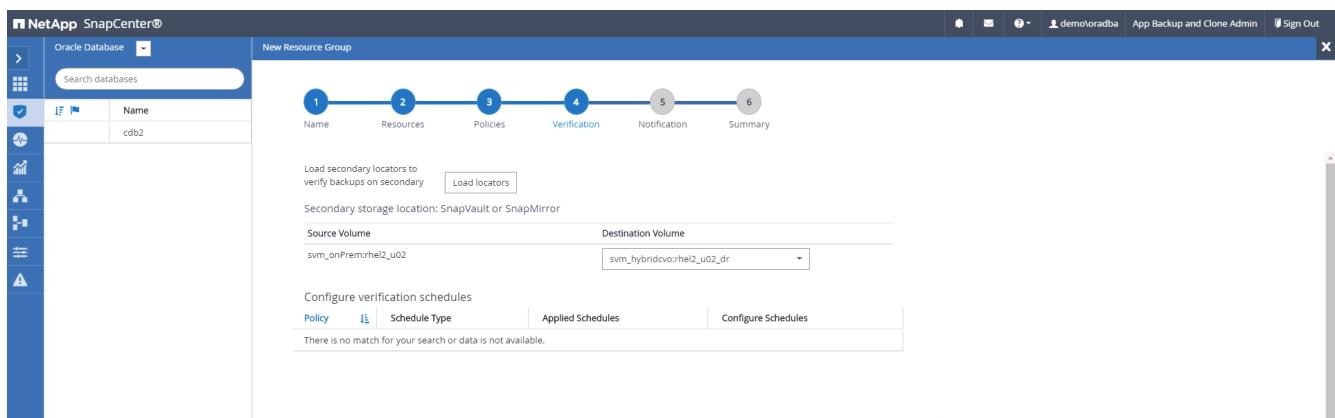
4. Select a full backup policy created in section 7 from the drop-down list.



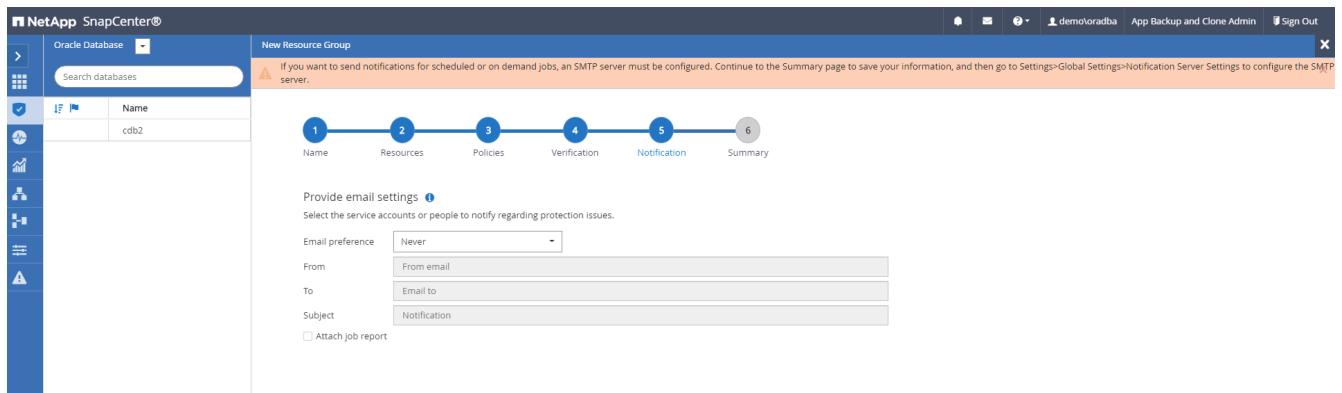
5. Click the (+) sign to configure the desired backup schedule.



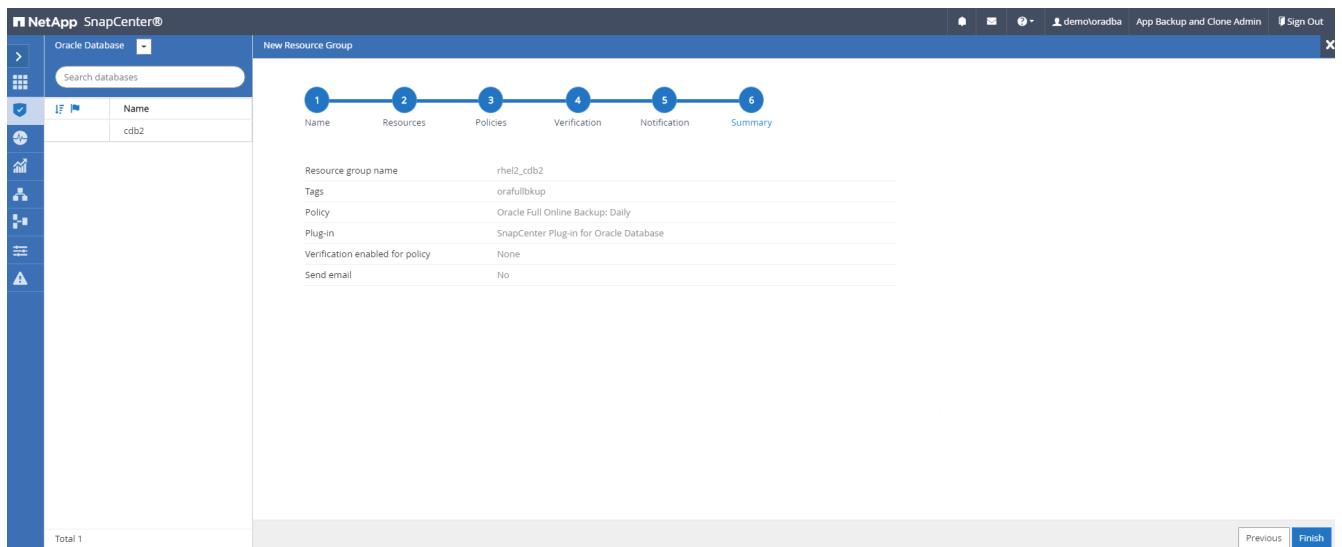
6. Click Load Locators to load the source and destination volume.



7. Configure the SMTP server for email notification if desired.

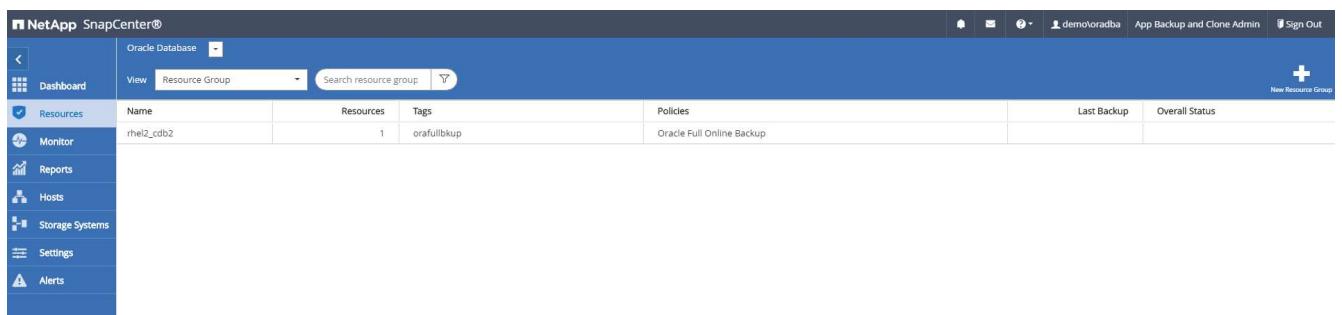


8. Summary.

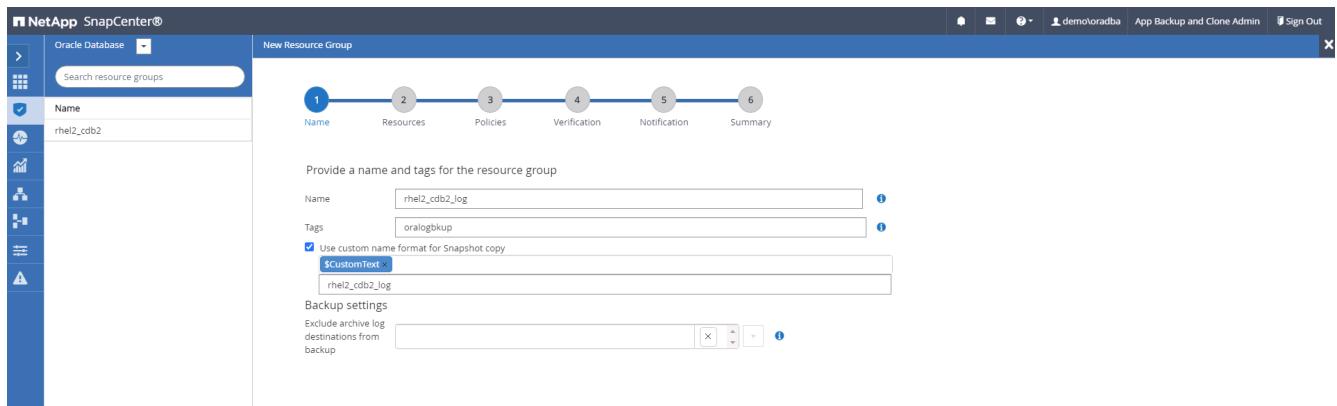


Create a resource group for log backup of Oracle

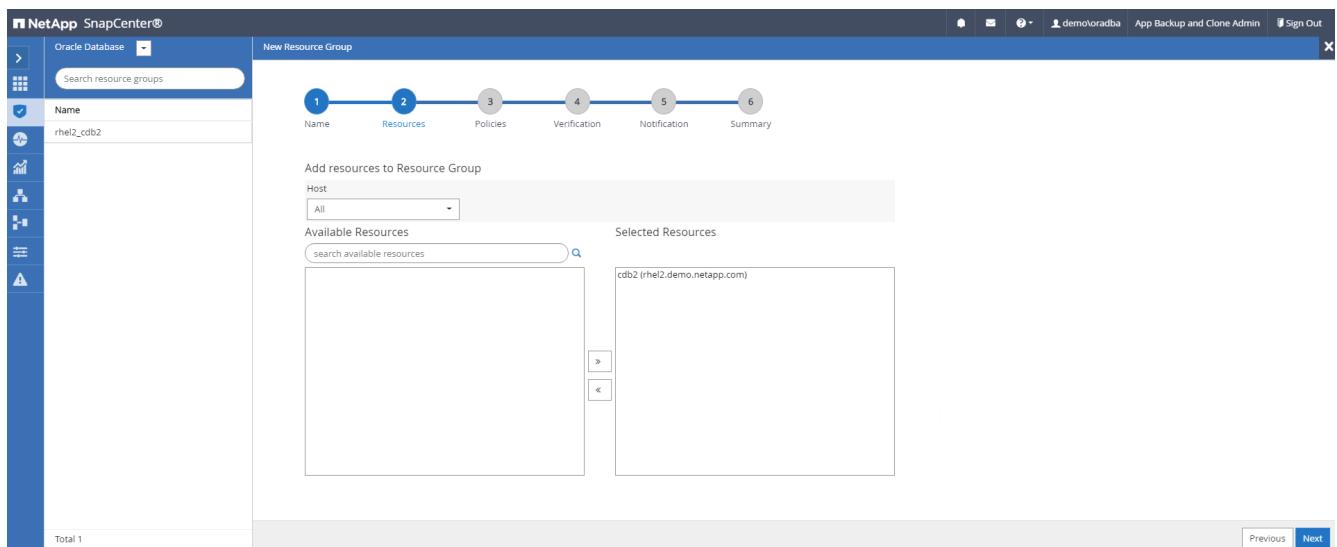
1. Log into SnapCenter with a database management user ID, and navigate to the Resources tab. In the View drop-down list, choose either Database or Resource Group to launch the resource group creation workflow.



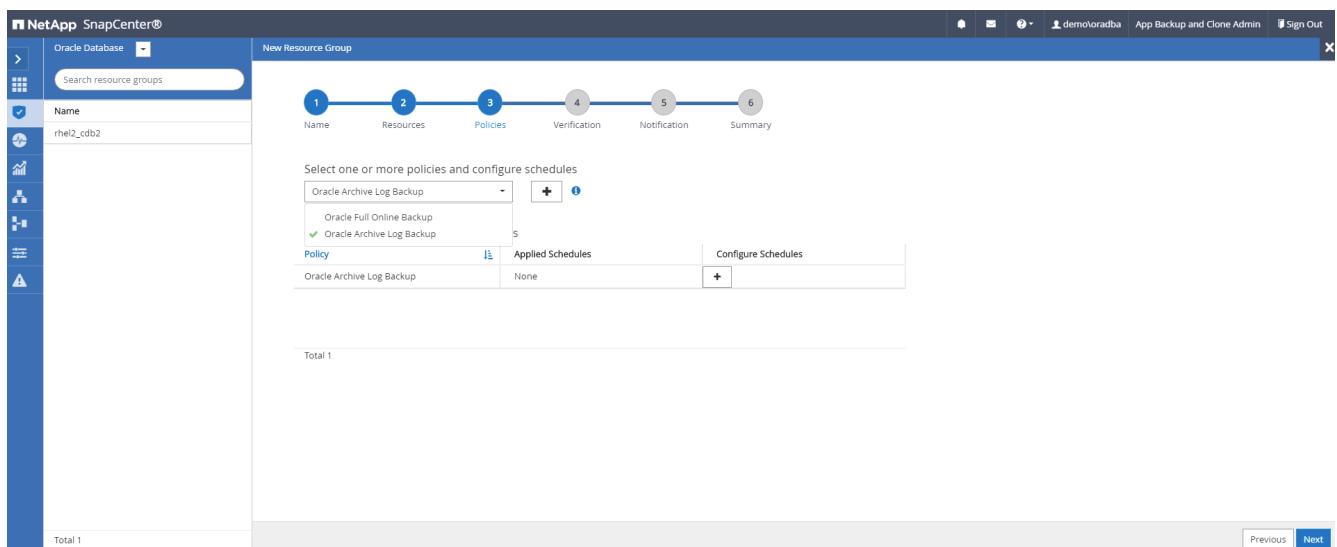
2. Provide a name and tags for the resource group. You can define a naming format for the Snapshot copy and bypass the redundant archive log destination if configured.



3. Add database resources to the resource group.



4. Select a log backup policy created in section 7 from the drop-down list.



5. Click on the (+) sign to configure the desired backup schedule.

Add schedules for policy Oracle Archive Log Backup x

Hourly

Start date

Expires on

Repeat every hours mins

i The schedules are triggered in the SnapCenter Server time zone. X

Cancel OK

6. If backup verification is configured, it displays here.

NetApp SnapCenter®

Oracle Database

New Resource Group

Name

Search resource groups

1 Name 2 Resources 3 Policies 4 Verification 5 Notification 6 Summary

Configure verification schedules

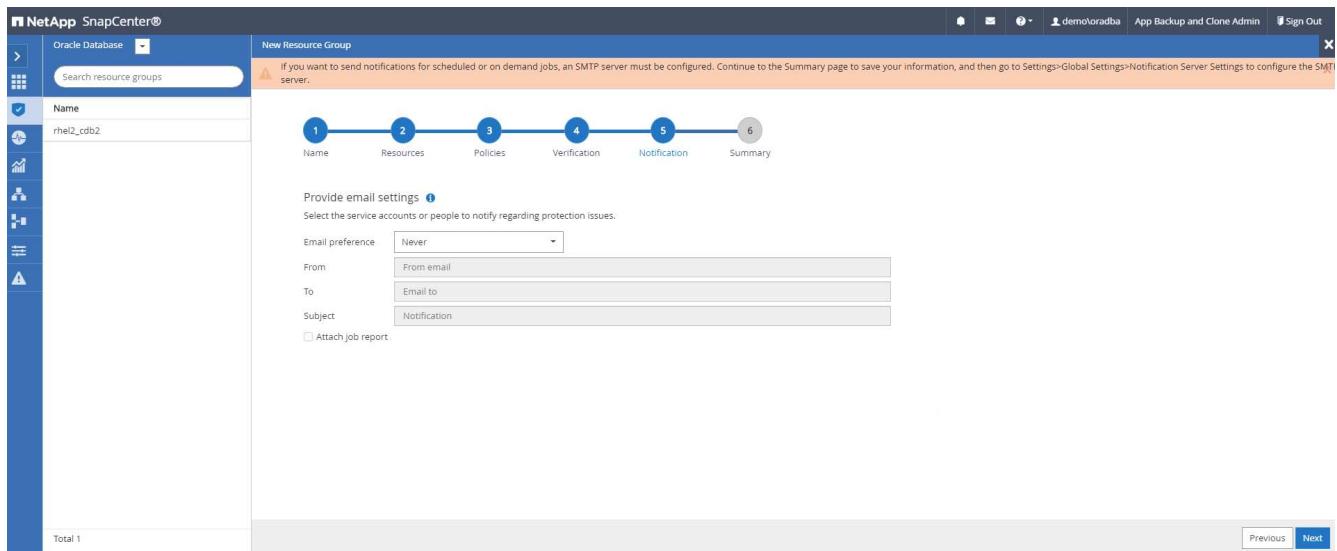
Policy Schedule Type Applied Schedules Configure Schedules

There is no match for your search or data is not available.

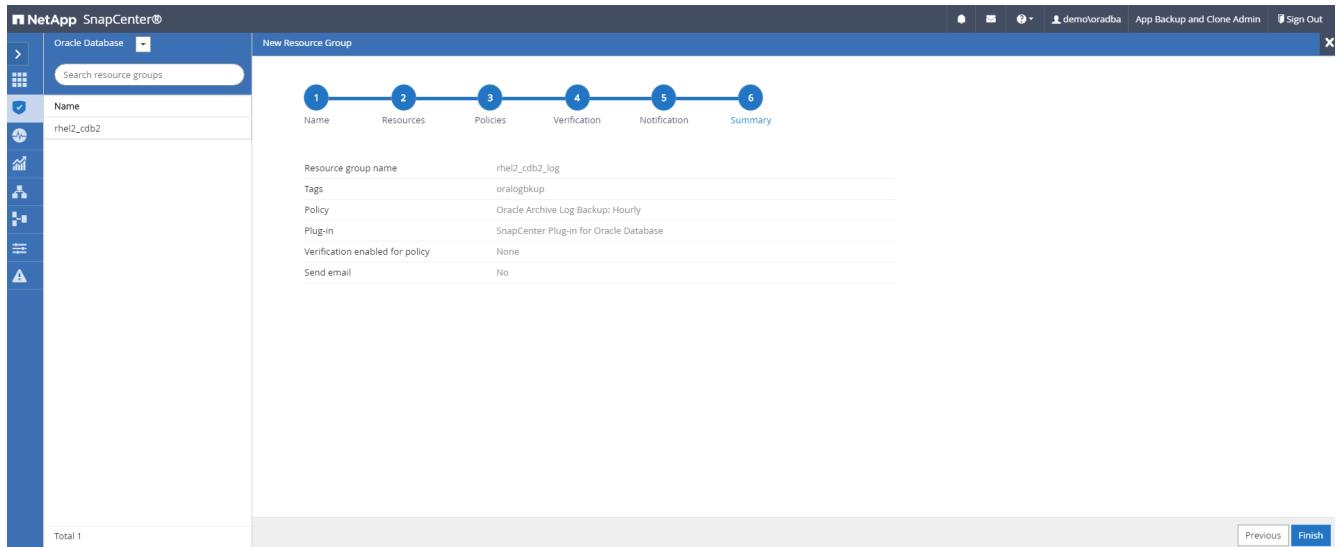
Total 0

Previous Next

7. Configure an SMTP server for email notification if desired.

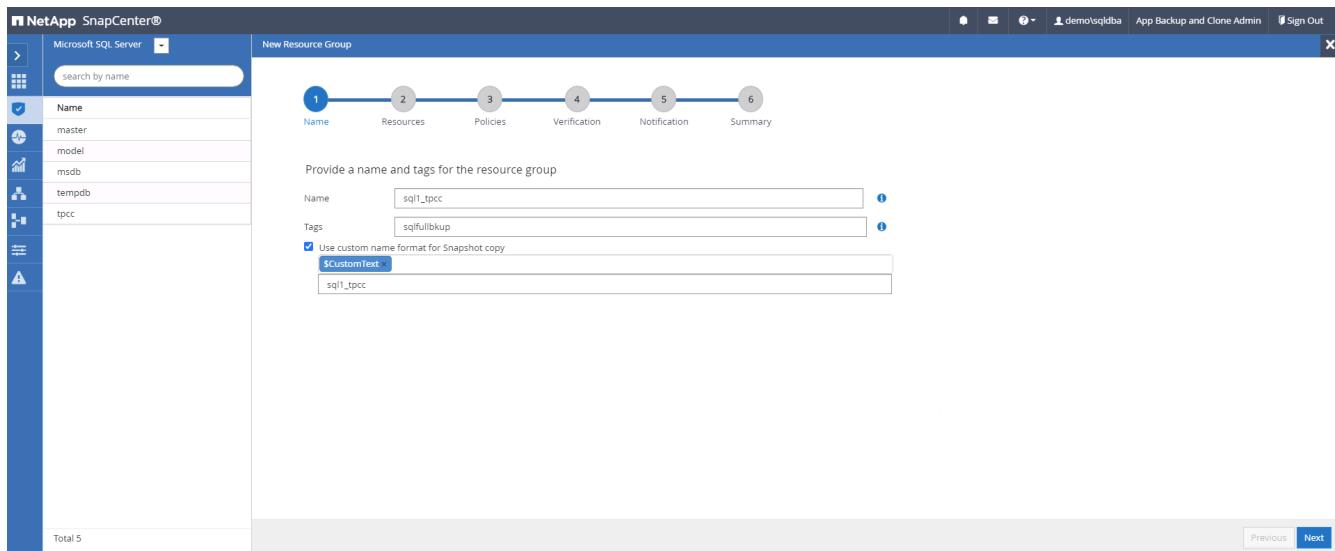


8. Summary.

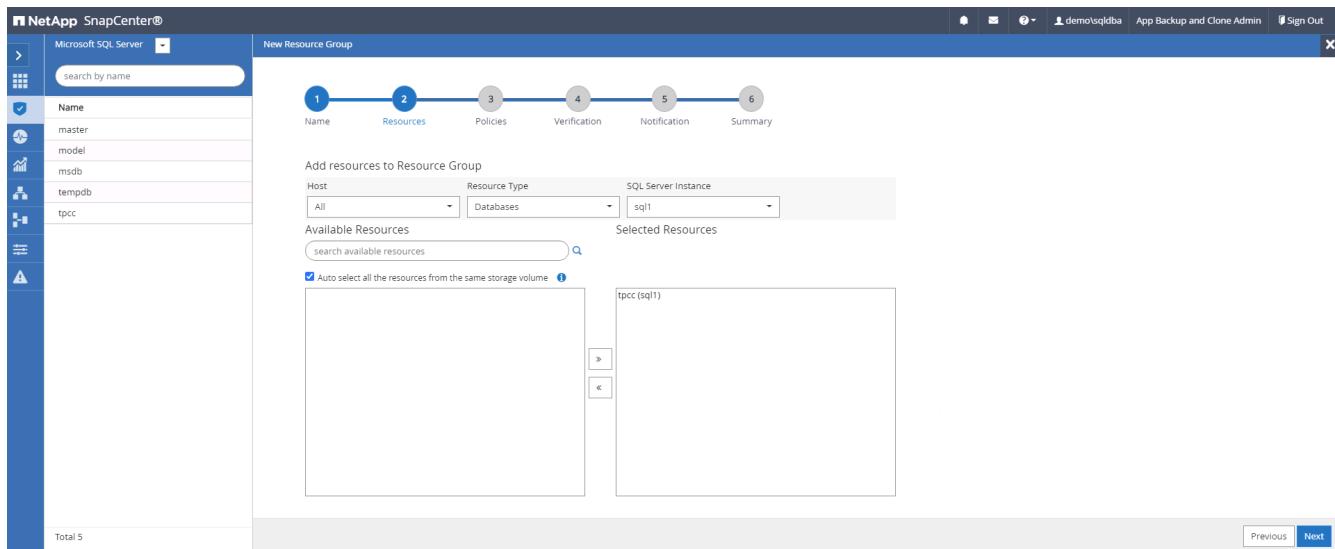


Create a resource group for full backup of SQL Server

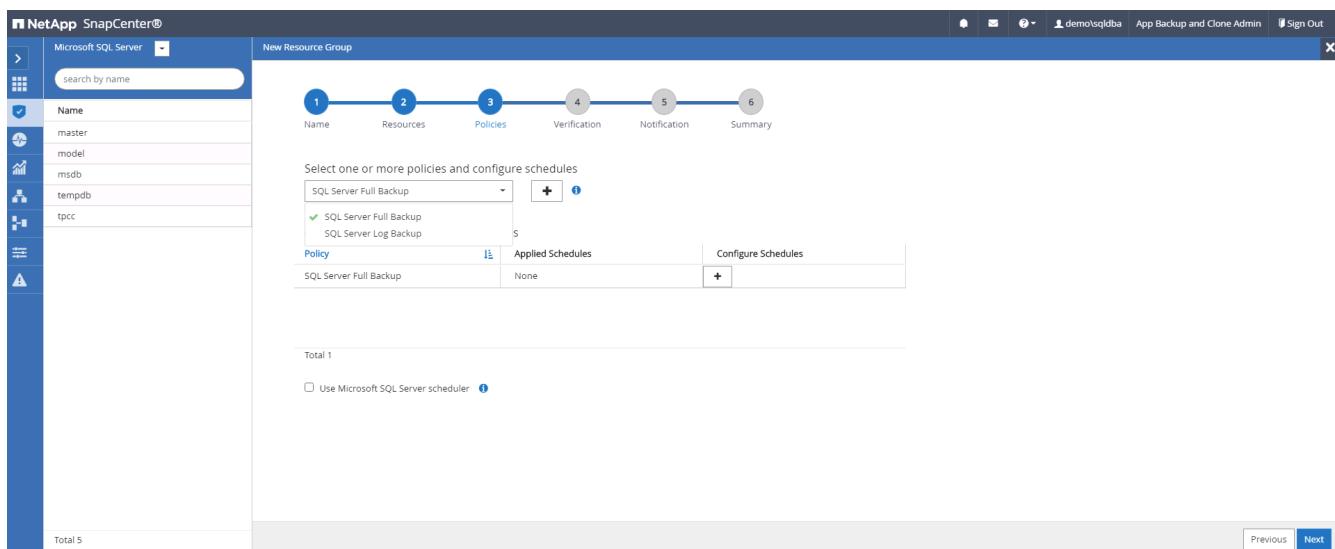
1. Log into SnapCenter with a database management user ID, and navigate to the Resources tab. In the View drop-down list, choose either a Database or Resource Group to launch the resource group creation workflow. Provide a name and tags for the resource group. You can define a naming format for the Snapshot copy.



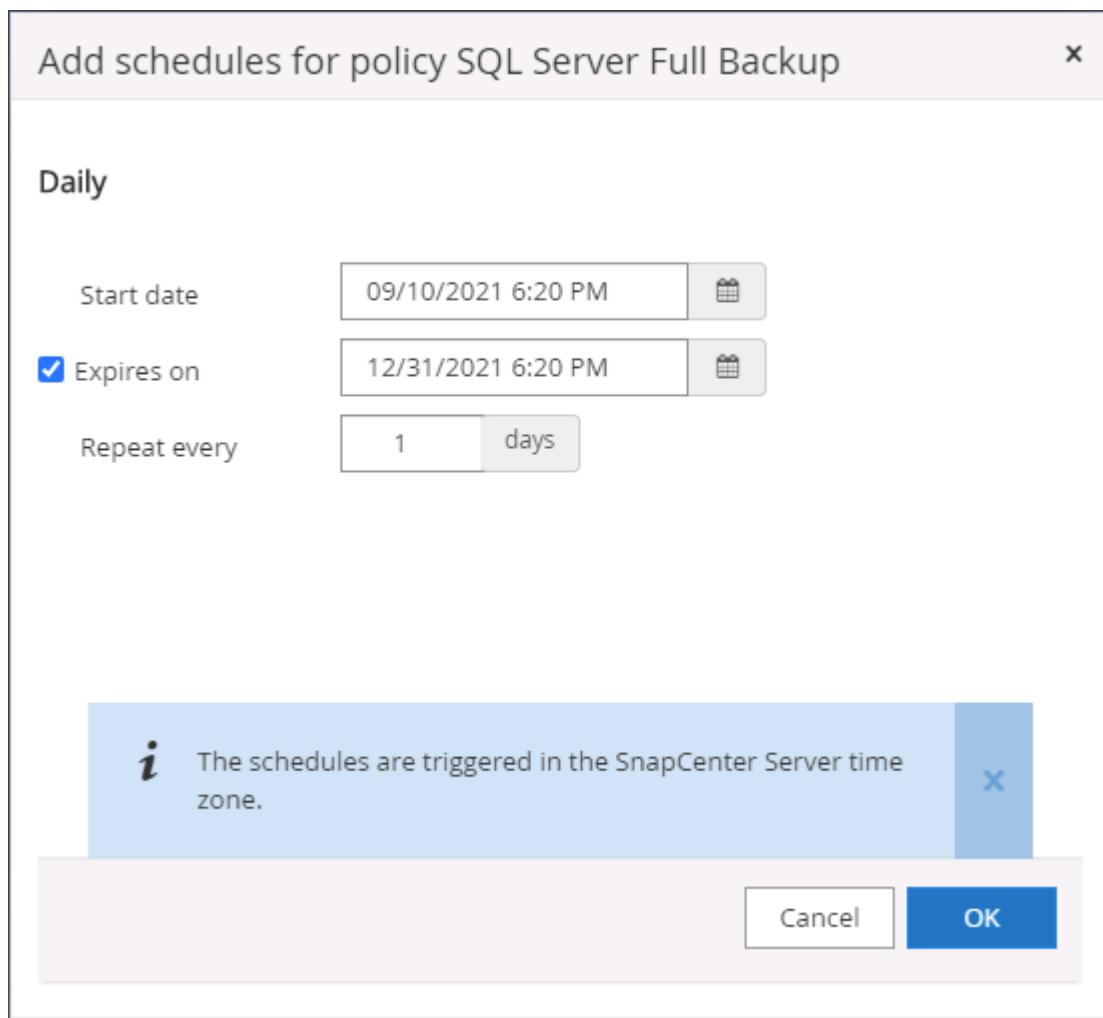
2. Select the database resources to be backed up.



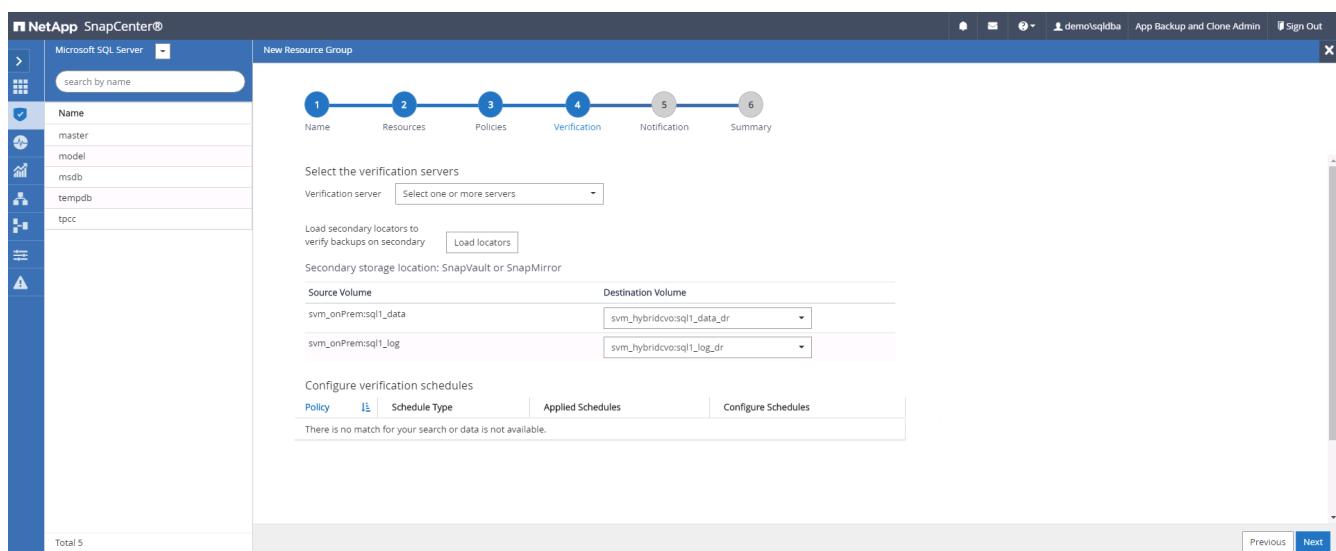
3. Select a full SQL backup policy created in section 7.



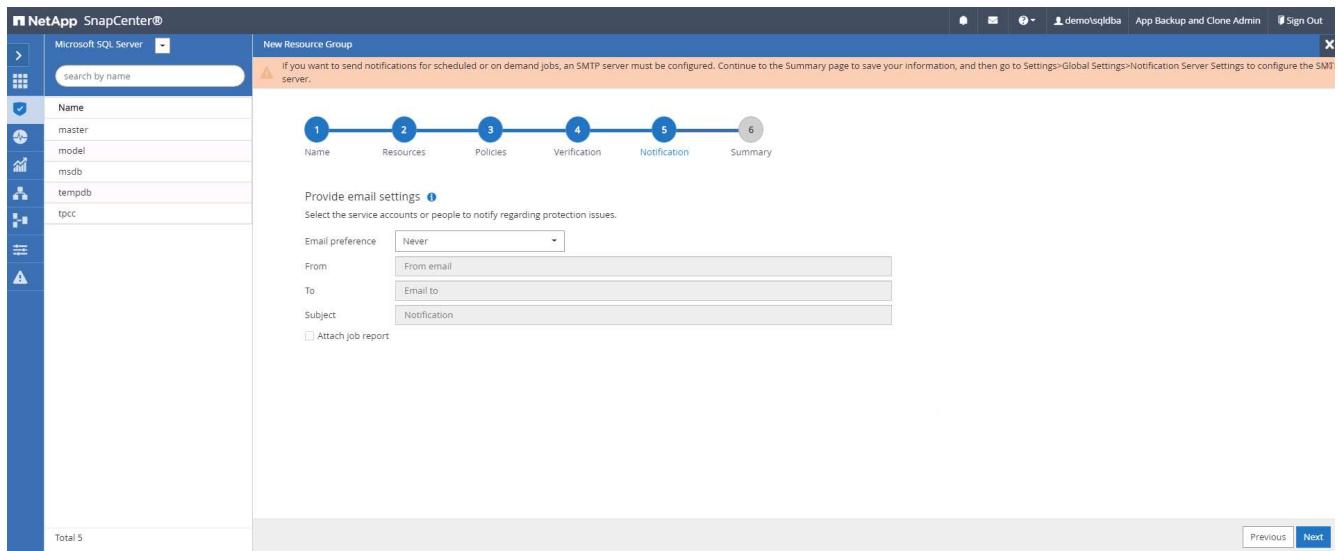
- Add exact timing for backups as well as the frequency.



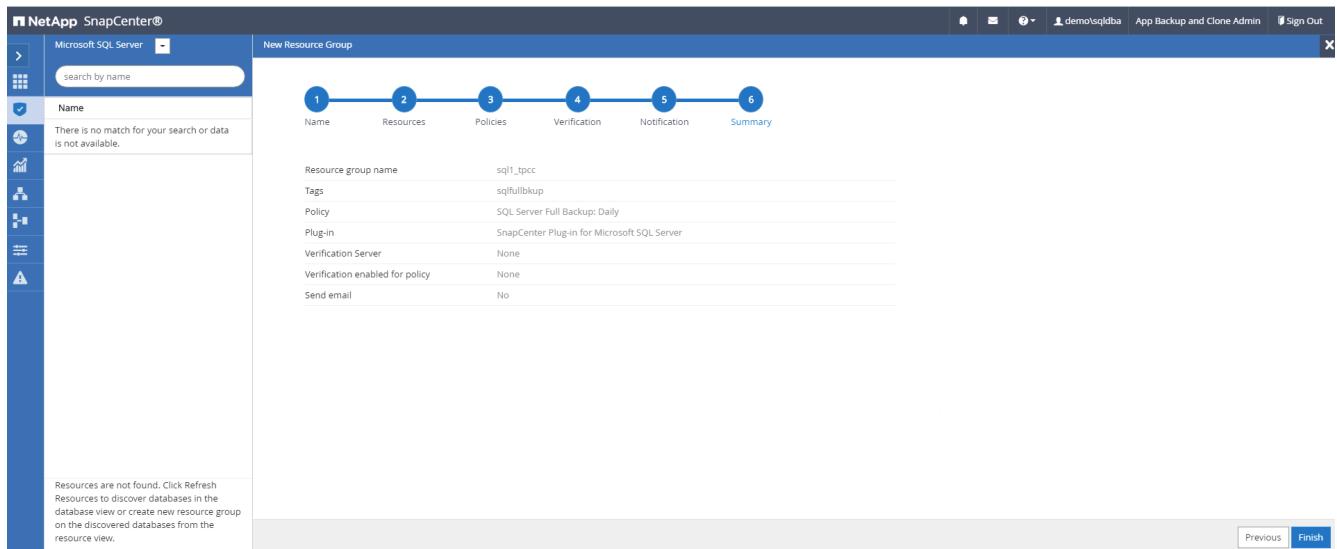
- Choose the verification server for the backup on secondary if backup verification is to be performed. Click Load Locator to populate the secondary storage location.



- Configure the SMTP server for email notification if desired.

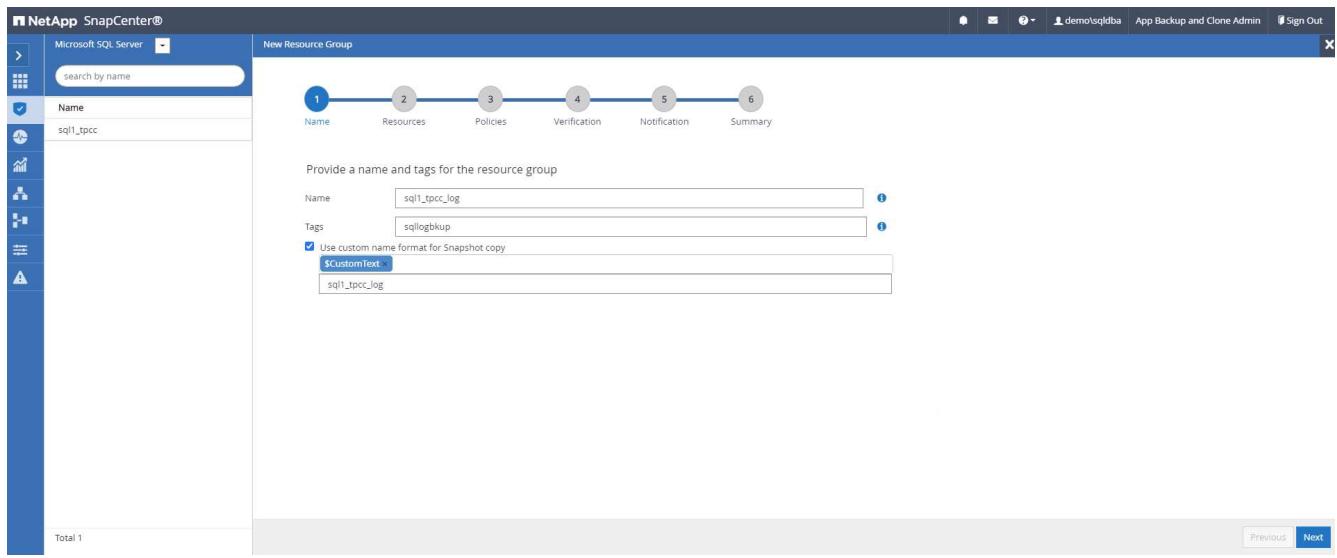


7. Summary.

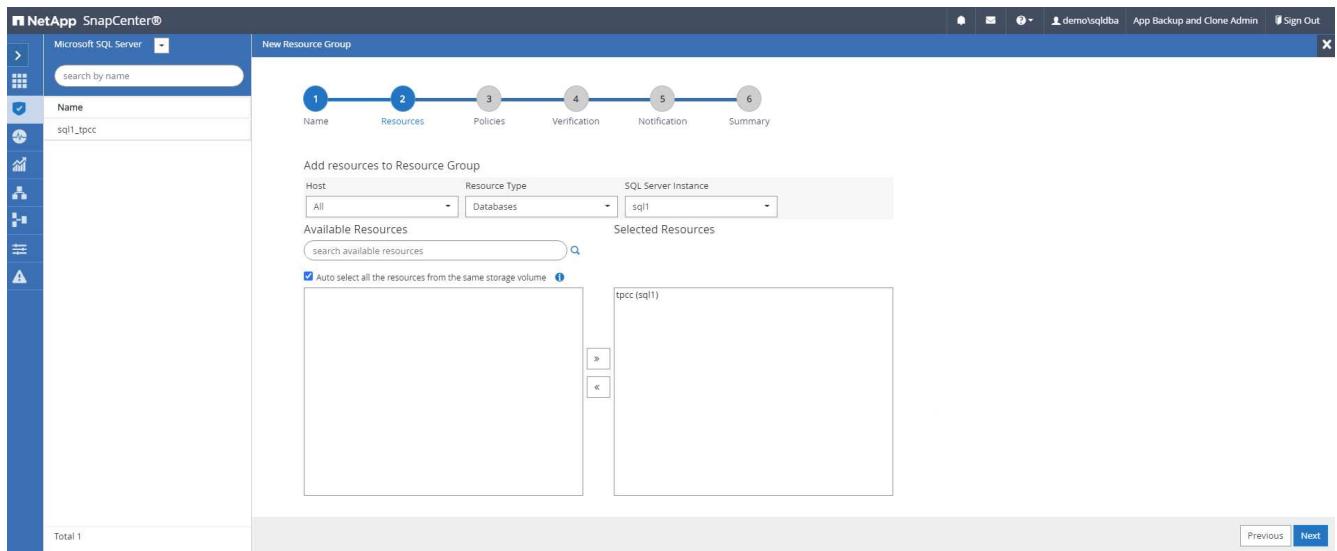


Create a resource group for log backup of SQL Server

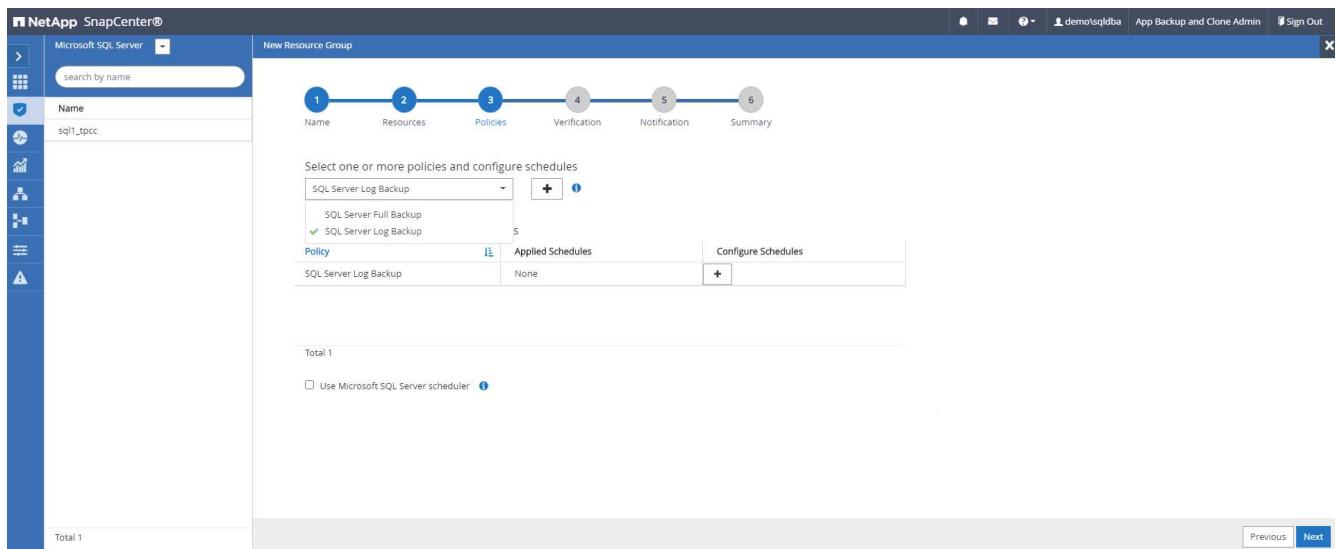
1. Log into SnapCenter with a database management user ID, and navigate to the Resources tab. In the View drop-down list, choose either a Database or Resource Group to launch the resource group creation workflow. Provide the name and tags for the resource group. You can define a naming format for the Snapshot copy.



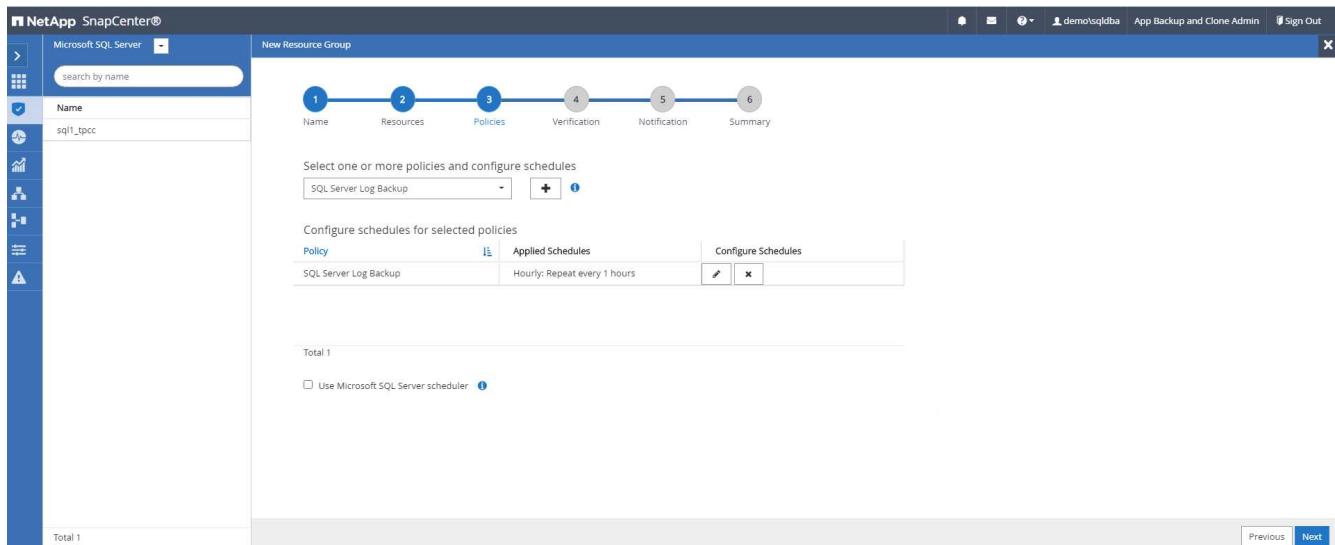
2. Select the database resources to be backed up.



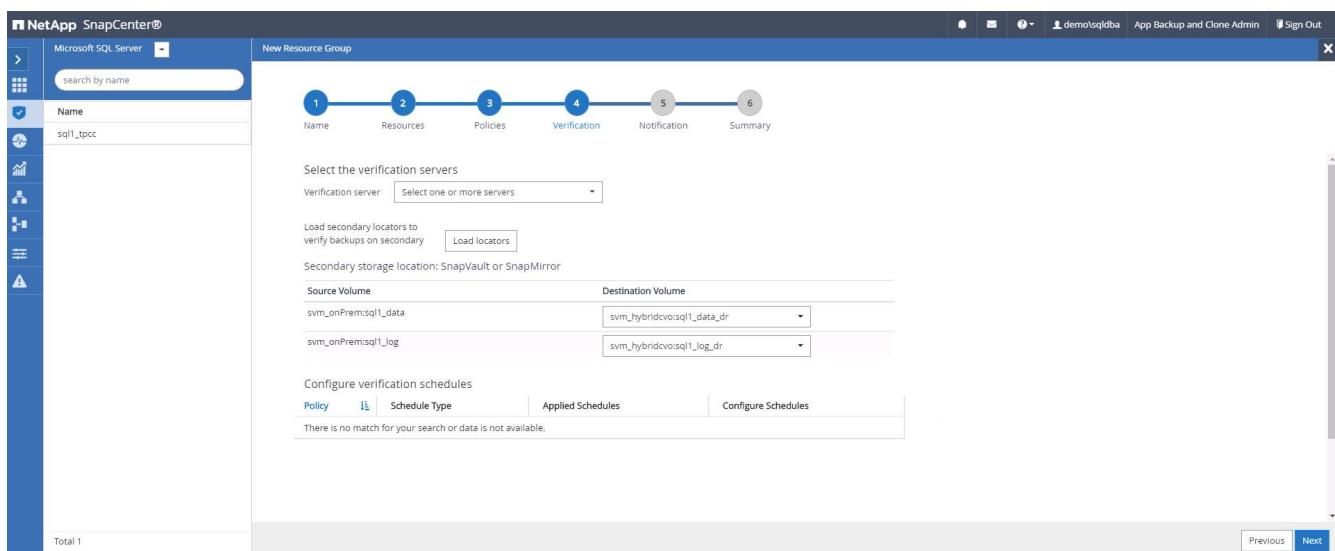
3. Select a SQL log backup policy created in section 7.



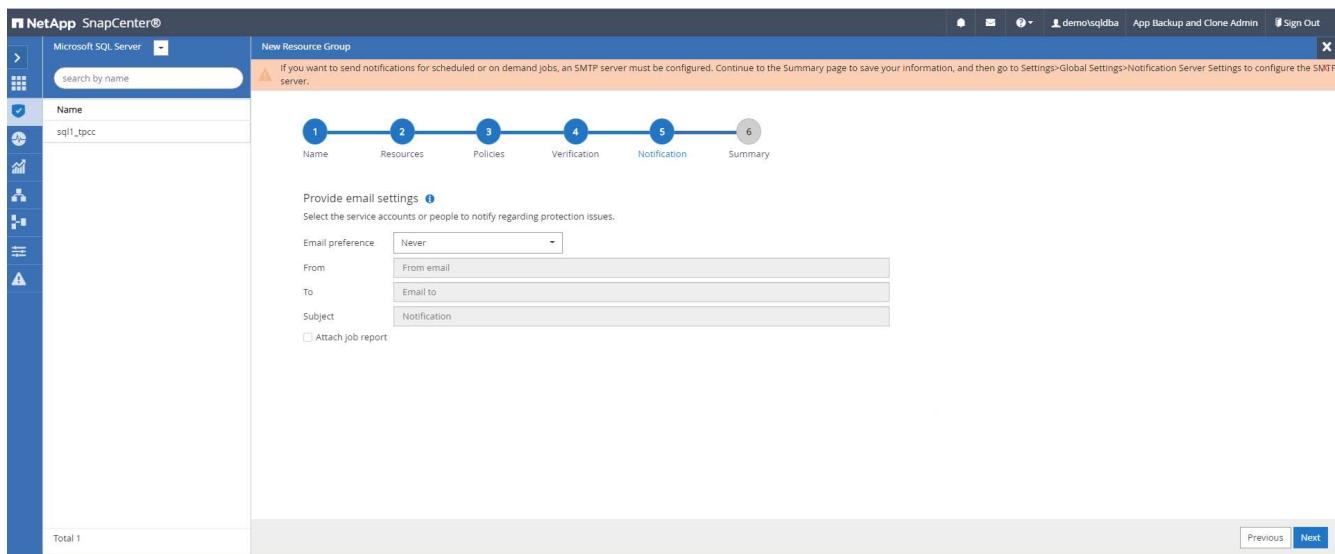
4. Add exact timing for the backup as well as the frequency.



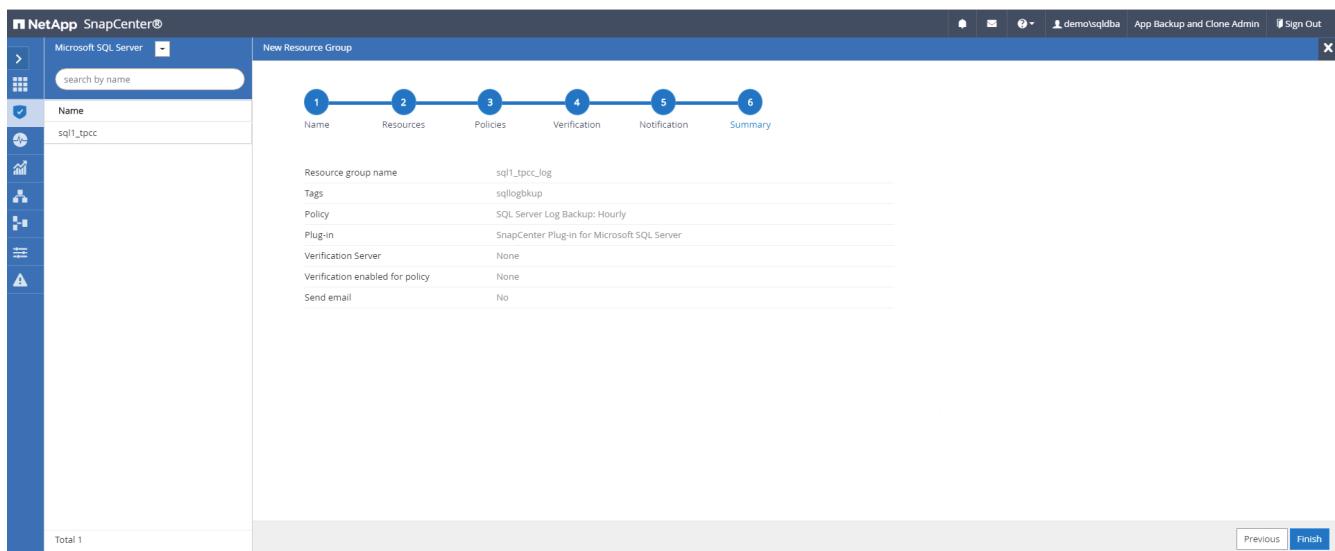
5. Choose the verification server for the backup on secondary if backup verification is to be performed. Click the Load Locator to populate the secondary storage location.



6. Configure the SMTP server for email notification if desired.



7. Summary.



9. Validate backup

After database backup resource groups are created to protect database resources, the backup jobs runs according to the predefined schedule. Check the job execution status under the Monitor tab.

Jobs							
Dashboard		Jobs - Filter		Logs			
Resources		ID	Status	Name	Start date	End date	Owner
Reports	532	✓	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/14/2021 8:35:01 PM	09/14/2021 8:37:10 PM	demo\sqldba	
Hosts	528	✓	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/14/2021 7:35:01 PM	09/14/2021 7:37:09 PM	demo\sqldba	
Storage Systems	524	✓	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/14/2021 6:35:01 PM	09/14/2021 6:37:08 PM	demo\sqldba	
Settings	521	✓	Backup of Resource Group 'sql1_tpcc' with policy 'SQL Server Full Backup'	09/14/2021 6:25:01 PM	09/14/2021 6:27:14 PM	demo\sqldba	
Alerts	517	✓	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/14/2021 5:35:01 PM	09/14/2021 5:37:09 PM	demo\sqldba	
	513	✓	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/14/2021 4:35:01 PM	09/14/2021 4:37:08 PM	demo\sqldba	
	509	✓	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/14/2021 3:35:01 PM	09/14/2021 3:37:09 PM	demo\sqldba	
	503	✓	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/14/2021 2:35:01 PM	09/14/2021 2:37:09 PM	demo\sqldba	

Go to the Resources tab, click the database name to view details of database backup, and toggle between Local copies and mirror copies to verify that Snapshot backups are replicated to a secondary location in the

public cloud.

The screenshot shows the NetApp SnapCenter interface for Oracle Database management. On the left, a sidebar lists databases: cdb2, cdb2dev, cdb2dr, cdb2dr2, and cdb2test. The main panel displays 'cdb2 Topology' with a summary card showing 394 Backups, 28 Data Backups, 366 Log Backups, and 3 Clones. It also shows 'Manage Copies' for 'Local copies' (197 Backups, 0 Clones) and 'Mirror copies' (197 Backups, 3 Clones). Below this is a table titled 'Primary Backup(s)' listing five backups with details like Count, Type, End Date, Verified, Mounted, RMAN Cataloged, and SCN.

Backup Name	Count	Type	End Date	Verified	Mounted	RMAN Cataloged	SCN
rhel2_cdb2_09-23-2021_14.35.03.3242_1	1	Log	09/23/2021 2:35:45 PM	Not Applicable	False	Not Cataloged	6872761
rhel2_cdb2_09-23-2021_14.35.03.3242_0	1	Data	09/23/2021 2:35:30 PM	Unverified	False	Not Cataloged	6872715
rhel2_cdb2_09-22-2021_14.35.02.0014_1	1	Log	09/22/2021 2:35:24 PM	Not Applicable	False	Not Cataloged	6737479
rhel2_cdb2_09-22-2021_14.35.02.0014_0	1	Data	09/22/2021 2:35:14 PM	Unverified	False	Not Cataloged	6737395
rhel2_cdb2_09-21-2021_14.35.02.1884_1	1	Log	09/21/2021 2:35:35 PM	Not Available	False	Not Cataloged	6598735

At this point, database backup copies in the cloud are ready to clone to run dev/test processes or for disaster recovery in the event of a primary failure.

Next: [Getting Started with AWS public cloud](#).

Getting Started with AWS public cloud

Previous: [Getting started on-premises](#).

AWS public cloud



To make things easier to follow, we have created this document based on a deployment in AWS. However, the process is very similar for Azure and GCP.

1. Pre-flight check

Before deployment, make sure that the infrastructure is in place to allow for the deployment in the next stage. This includes the following:

- AWS account
- VPC in your region of choice
- Subnet with access to the public internet
- Permissions to add IAM roles into your AWS account
- A secret key and access key for your AWS user

2. Steps to deploy Cloud Manager and Cloud Volumes ONTAP in AWS



There are many methods for deploying Cloud Manager and Cloud Volumes ONTAP; this method is the simplest but requires the most permissions. If this method is not appropriate for your AWS environment, please consult the [NetApp Cloud Documentation](#).

Deploy the Cloud Manager connector

1. Navigate to [NetApp Cloud Central](#) and log in or sign up.



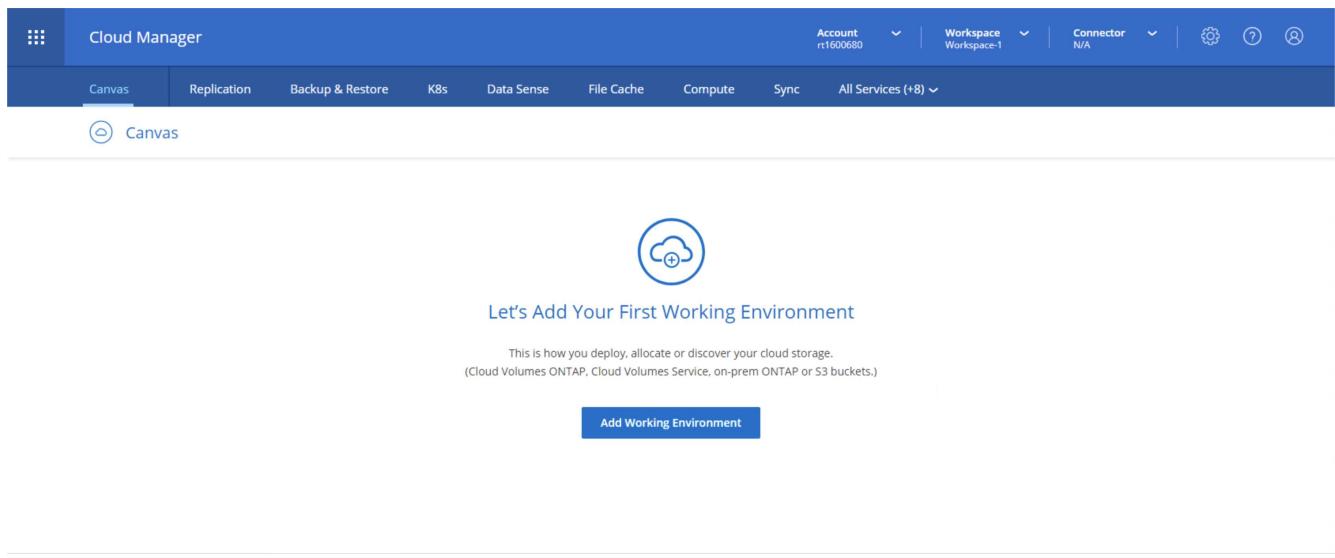
[Continue to Cloud Manager](#)

Log In to NetApp Cloud Central

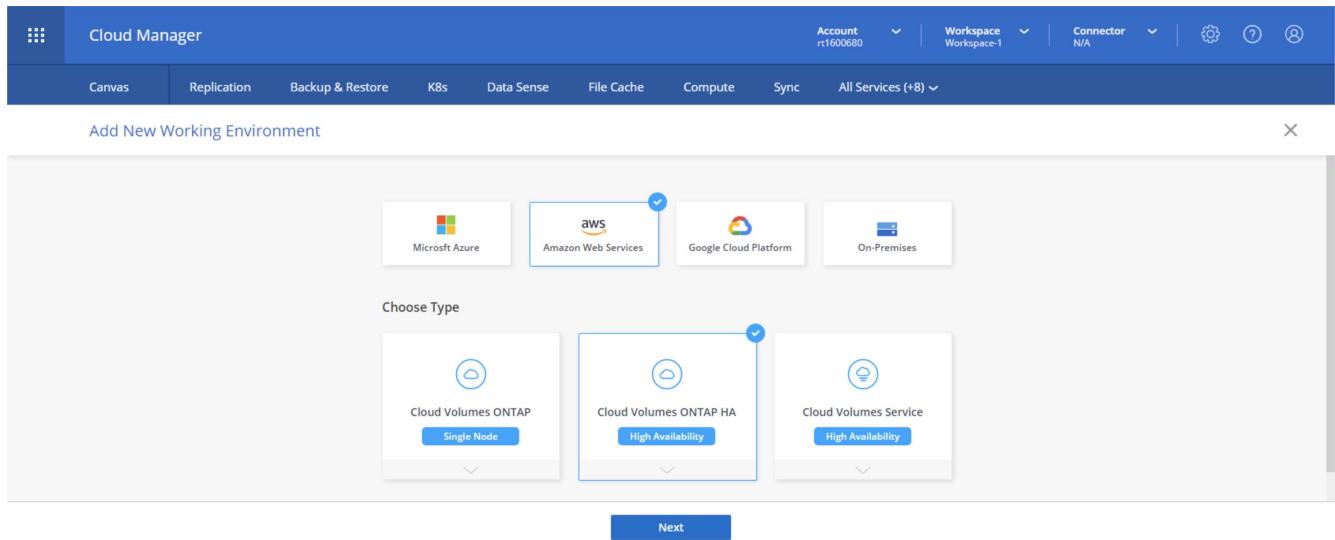
Don't have an account yet? [Sign Up](#)

[Forgot your password?](#)

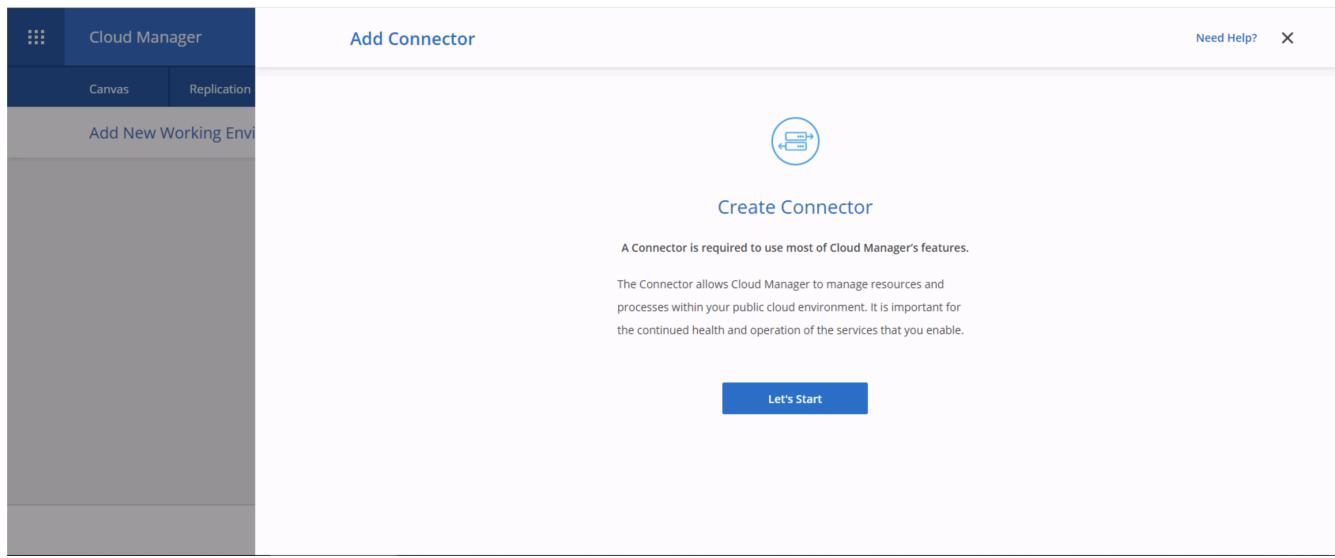
2. After you log in, you should be taken to the Canvas.



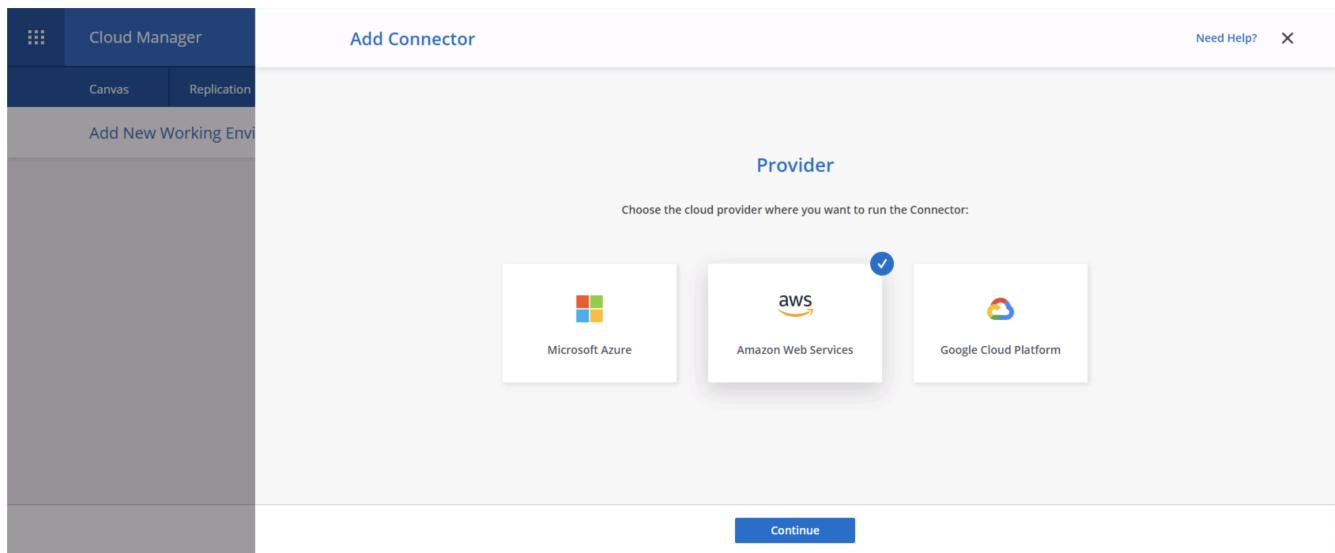
3. Click "Add Working Environment" and choose Cloud Volumes ONTAP in AWS. Here, you also choose whether you want to deploy a single node system or a high availability pair. I have chosen to deploy a high availability pair.



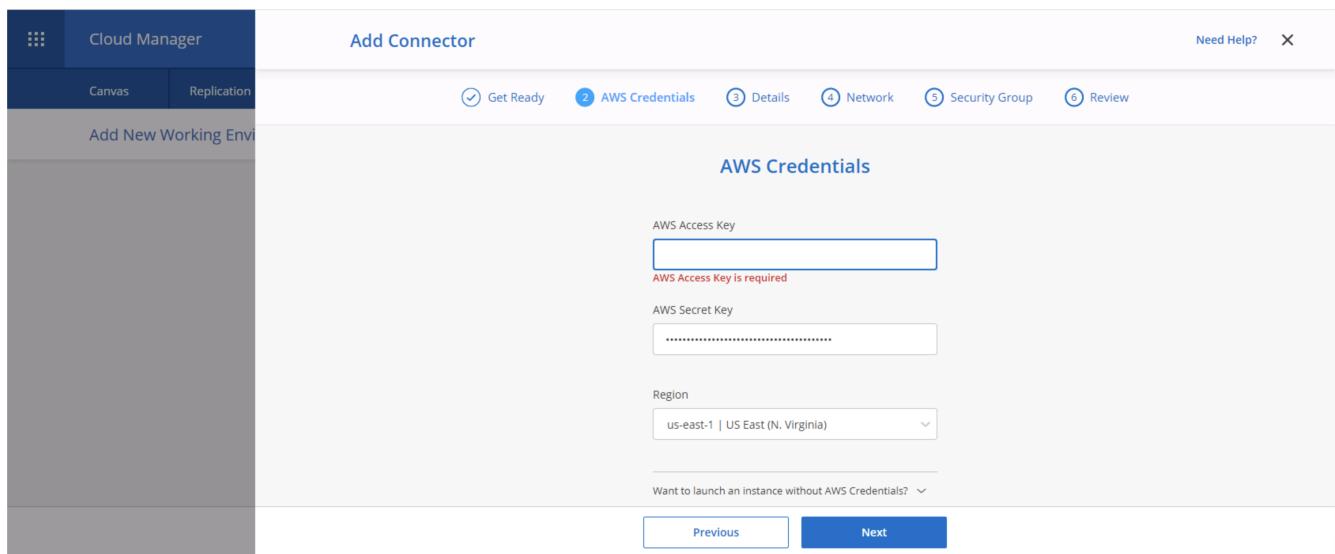
4. If no connector has been created, a pop-up appears asking you to create a connector.



5. Click Lets Start, and then choose AWS.



6. Enter your secret key and access key. Make sure that your user has the correct permissions outlined on the [NetApp policies page](#).



7. Give the connector a name and either use a predefined role as described on the [NetApp policies page](#) or ask Cloud Manager to create the role for you.

Cloud Manager

Add Connector

Get Ready AWS Credentials Details Network Security Group Review

Connector Instance Name: awscloudmanager

Connector Role:

- Create Role
- Select an existing Role

Role Name: Cloud-Manager-Operator-IBNt24

Add Tags to Connector Instance

Previous Next

8. Give the networking information needed to deploy the connector. Verify that outbound internet access is enabled by:
- Giving the connector a public IP address
 - Giving the connector a proxy to work through
 - Giving the connector a route to the public internet through an Internet Gateway

Cloud Manager

Add Connector

Get Ready AWS Credentials Details Network Security Group Review

Connectivity

VPC: vpc-083fcbd79f75dfb6e - 10.221.0.0/16

Subnet: 10.221.4.0/24 | publicSN_us-east-1a_rt1600...

Key Pair: rt1600680

Public IP: Enable

Proxy Configuration (Optional)

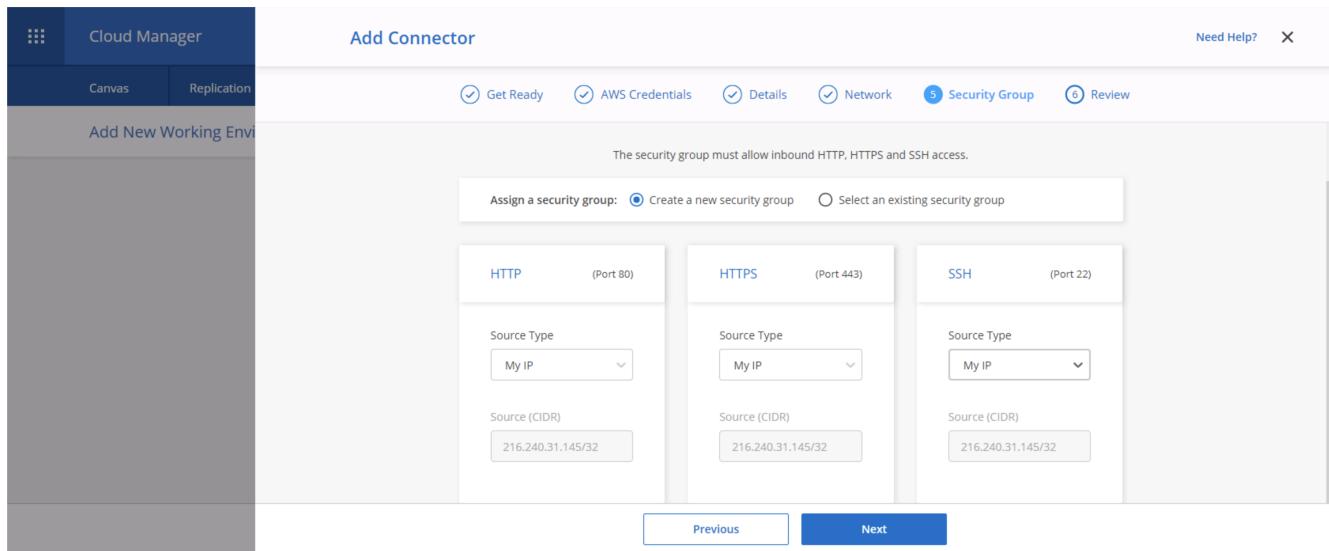
HTTP Proxy: Example: http://172.16.254.1:8080

Define Credentials for this Proxy

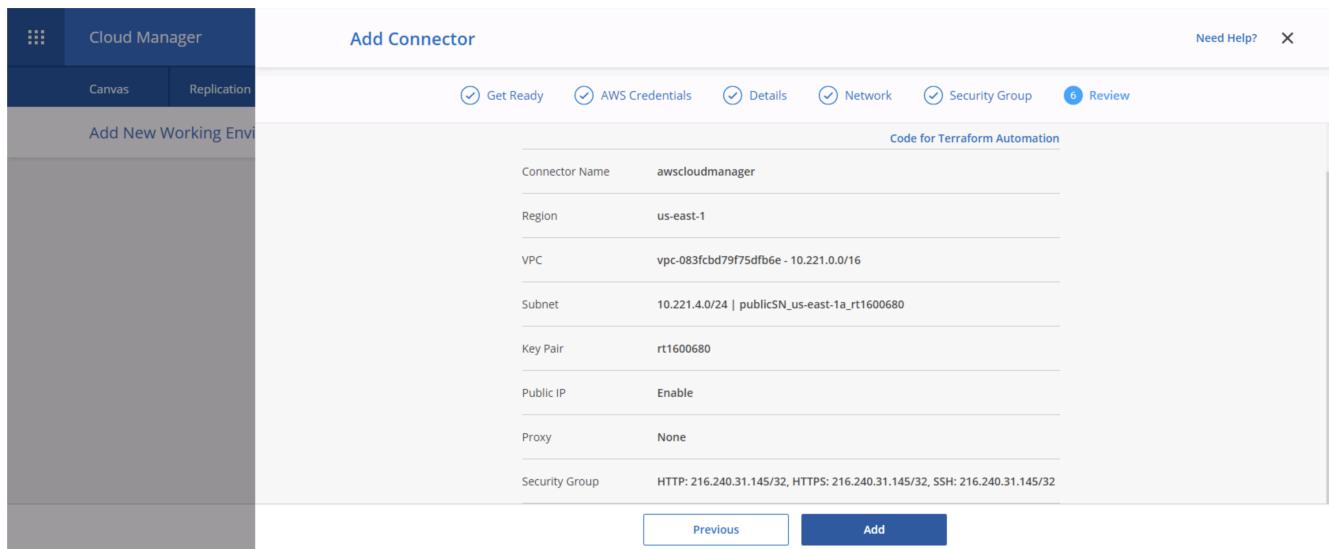
Upload a root certificate

Previous Next

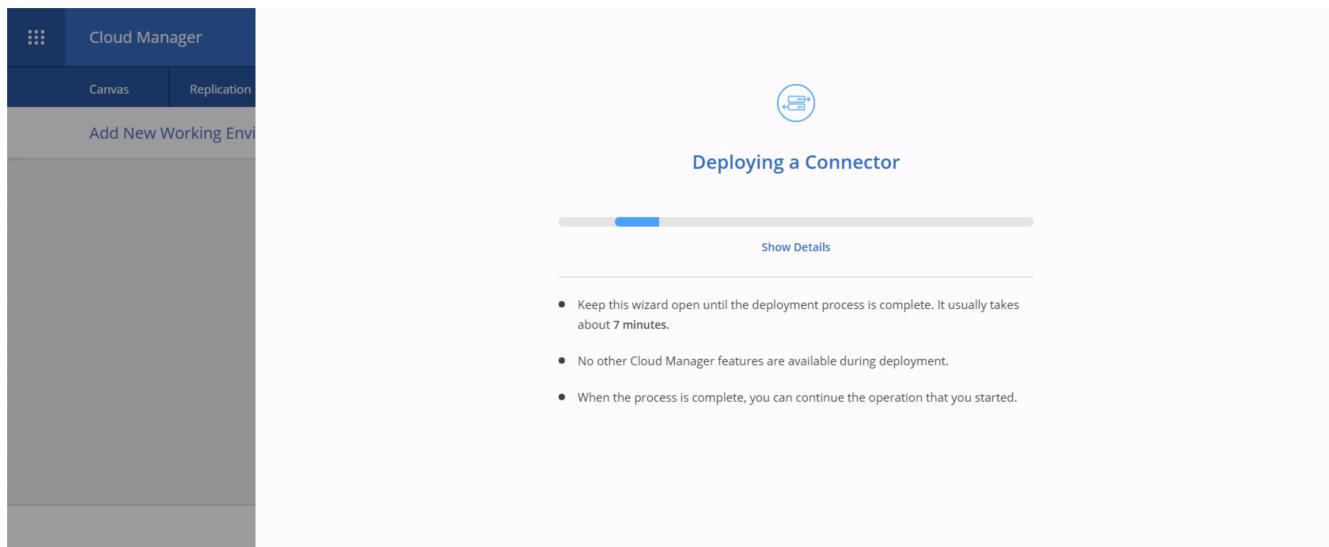
9. Provide communication with the connector via SSH, HTTP, and HTTPS by either providing a security group or creating a new security group. I have enabled access to the connector from my IP address only.



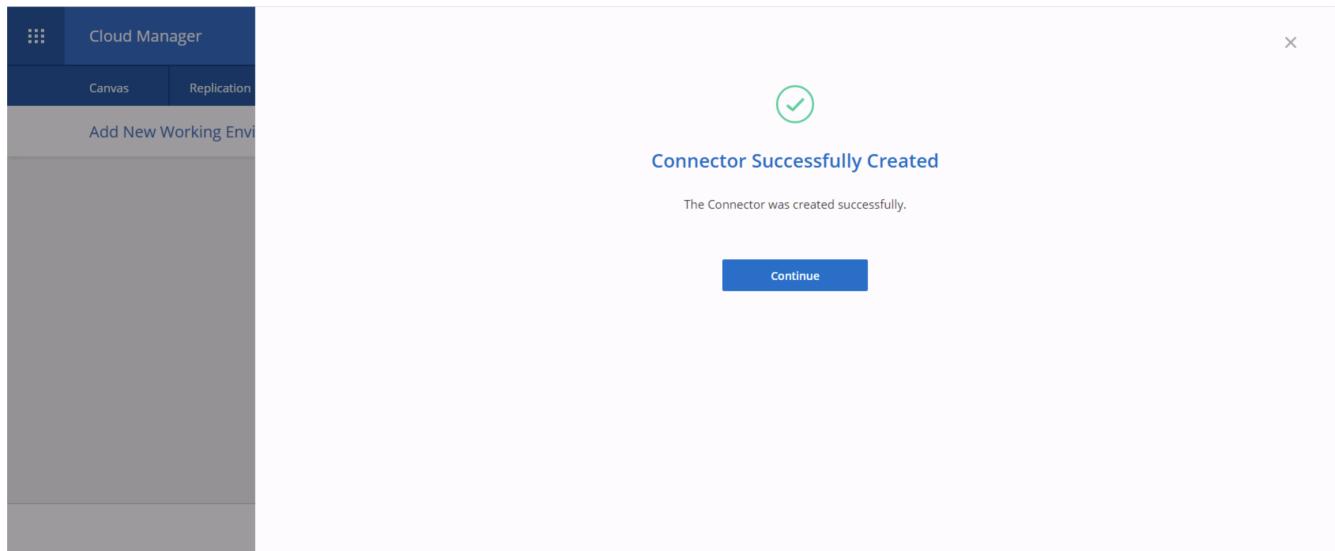
10. Review the information on the summary page and click Add to deploy the connector.



11. The connector now deploys using a cloud formation stack. You can monitor its progress from Cloud Manager or through AWS.

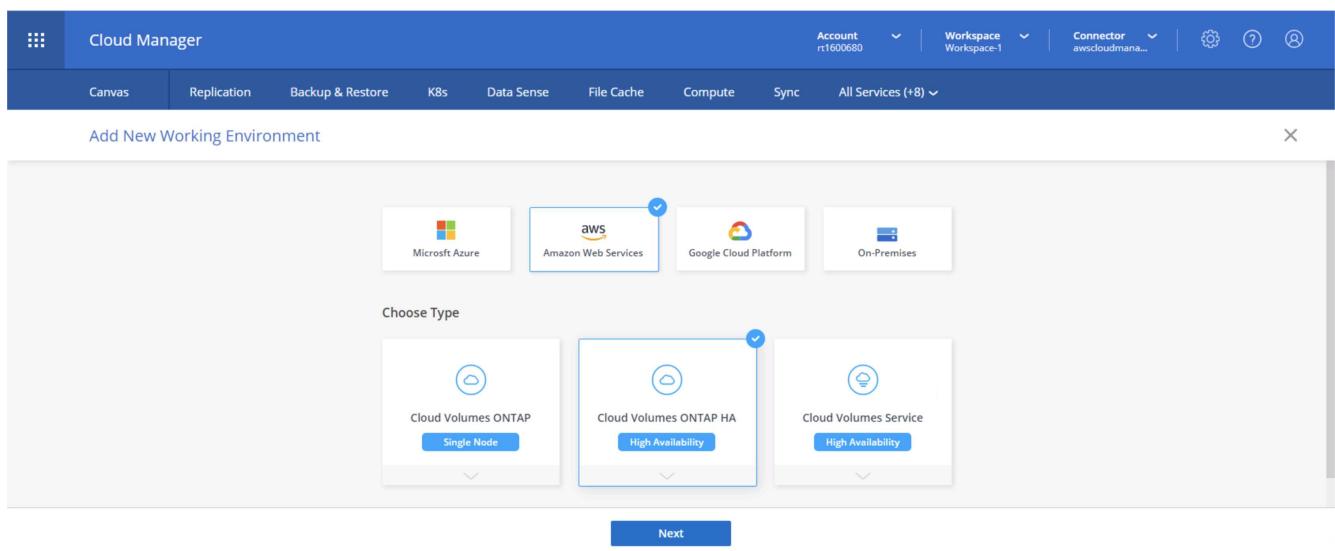


12. When the deployment is complete, a success page appears.



Deploy Cloud Volumes ONTAP

1. Select AWS and the type of deployment based on your requirements.



2. If no subscription has been assigned and you wish to purchase with PAYGO, choose Edit Credentials.

Create a New Working Environment

Details and Credentials

↑ Previous Step Instance Profile Credential Name Account ID No subscription is associated Marketplace Subscription Edit Credentials

Details Credentials

Working Environment Name (Cluster Name) User Name
Up to 40 characters admin

+ Add Tags Optional Field | Up to four tags Password

Confirm Password

Continue

Cloud Manager 3.9.9 Build: 0 Aug 18, 2021 04:13:35 am UTC

3. Choose Add Subscription.

Create a New Working Environment

Details and Credentials

↑ Previous Step Instance Profile Credential Name

Associate Subscription to Credentials ⓘ

Credentials Instance Profile | Account ID: 322944748816

Marketplace Subscription No subscription is associated with this credential

+ Add Subscription

Apply Cancel

Cloud Manager 3.9.9 Build: 0 Aug 18, 2021 04:13:35 am UTC

4. Choose the type of contract that you wish to subscribe to. I chose Pay-as-you-go.

Create a New Working Environment

Edit Credentials & Add Subscription

Select a subscription option and click Continue. The AWS Marketplace enables you to view pricing details and then subscribe.

Pay-Per-TiB - Annual Contract
Pay for Cloud Volumes ONTAP with an annual, upfront payment.

Pay-as-you-go
Pay for Cloud Volumes ONTAP at an hourly rate.

The next steps:

- ① AWS Marketplace
Subscribe and then click Set Up Your Account to configure your account.
- ② Cloud Manager
Save your subscription and associate the Marketplace subscription with your AWS credentials.

Continue Cancel

Cloud Manager 3.9.9 Build: 0 Aug 18, 2021 04:13:35 am UTC

5. You are redirected to AWS; choose Continue to Subscribe.

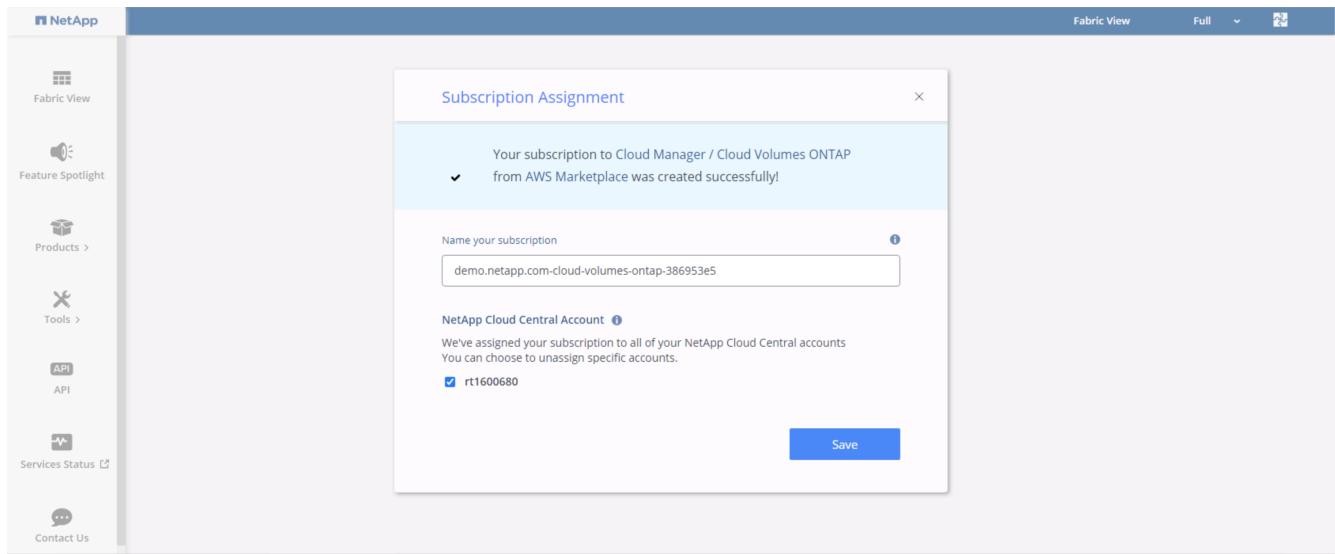
The screenshot shows the AWS Marketplace interface for the NetApp Cloud Manager product. The product title is 'Cloud Manager - Deploy & Manage NetApp Cloud Data Services'. It is sold by 'NetApp, Inc.'. Below the title, there is a brief description: 'Start here to deploy and manage Cloud Volumes ONTAP, Cloud Tiering, Cloud Data Sense, Cloud Backup and Cloud Volumes Service. Accelerate critical business apps with speed,' followed by a 'Show more' link. At the top right, there is a 'Continue to Subscribe' button and a 'Save to list' link. Below the main title, there are tabs for 'Overview', 'Pricing', 'Usage', 'Support', and 'Reviews'. The 'Overview' tab is selected. On the right side, there is a 'Highlights' section with a bulleted list:

- Streamline the deployment of all your NetApp Cloud Volumes ONTAP environments
- Centrally manage your NetApp based storage and replicate across availability zones or to and from your data center
- Enable your IT administrators to audit and track your cloud storage resource spend

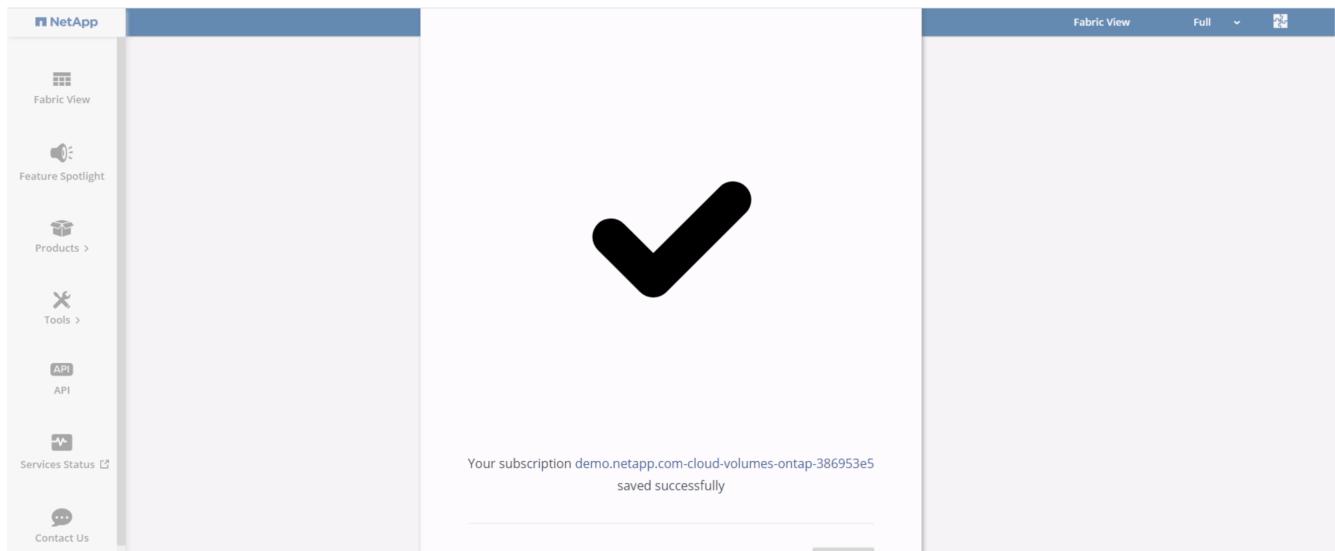
6. Subscribe and you are redirected back to NetApp Cloud Central. If you have already subscribed and don't get redirected, choose the "Click here" link.

The screenshot shows the AWS Marketplace confirmation page for the NetApp Cloud Manager subscription. It displays a message: 'You are extended multiple offers! Select an offer first and review the pricing information and EULA.' Below this, it shows the 'Offer name' as 'NetApp, Inc. for SaaS 2020-07-20- Private Offer - current subscription'. To the right, there is a note: 'You are subscribed to this offer. By: NetApp, Inc. Offer ID: offer-hmolsqhv7ii This offer is going to expire on August 1, 2022 UTC'. Below this, there is a box with a question mark icon and the text: 'Having issues signing up for your product? If you were unable to complete the set-up process for this software, please [click here](#) to be taken to the product's registration area.' To the right, there is a summary box: 'You Have Subscribed to a Private Offer' with the text: 'You have subscribed to this private offer on July 21, 2022 UTC. The private offer will expire on August 1, 2022 UTC. Your use of this product after the expiration date of your private offer will be billed at the then current public pricing, which can be found on this product's detail page.' At the bottom, there is a 'Subscribe' button and a note: 'By subscribing to this software, you agree to the pricing terms and the seller's [End User License Agreement \(EULA\)](#). You also agree and acknowledge that AWS may share information about this transaction.'

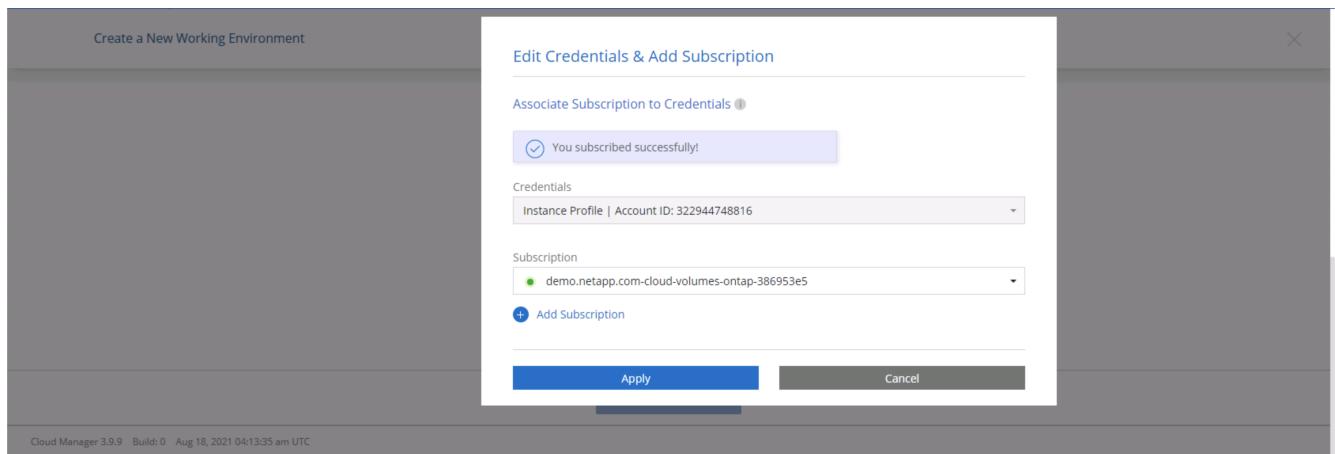
7. You are redirected to Cloud Central where you must name your subscription and assign it to your Cloud Central account.



- When successful, a check mark page appears. Navigate back to your Cloud Manager tab.



- The subscription now appears in Cloud Central. Click Apply to continue.



- Enter the working environment details such as:

- a. Cluster name

- b. Cluster password
- c. AWS tags (Optional)

The screenshot shows the 'Create a New Working Environment' interface in Cloud Manager. At the top, there are tabs for Canvas, Replication, Backup & Restore, K8s, Data Sense, File Cache, Compute, Sync, and All Services (+8). The 'Details and Credentials' tab is selected. On the left, there's a 'Previous Step' button and an 'Instance Profile' section with fields for '322944748816' and 'demo.netapp.com-cloud-vol...'. On the right, there's a 'Workspace' dropdown set to 'Workspace-1', a 'Connector' dropdown set to 'awscloudman...', and a 'Edit Credentials' button. Below these, there are two sections: 'Details' and 'Credentials'. The 'Details' section contains a 'Working Environment Name (Cluster Name)' field with 'hybridawscvo' entered. The 'Credentials' section contains fields for 'User Name' ('admin'), 'Password' (redacted), and 'Confirm Password' (redacted). A 'Continue' button is at the bottom.

11. Choose which additional services you would like to deploy. To discover more about these services, visit the [NetApp Cloud Homepage](#).

The screenshot shows the 'Services' configuration step in Cloud Manager. At the top, there are tabs for Canvas, Replication, Backup & Restore, K8s, Data Sense, File Cache, Compute, Sync, and All Services (+8). The 'Services' tab is selected. On the left, there's a 'Previous Step' button. The main area lists three services with toggle switches: 'Data Sense & Compliance' (on), 'Backup to Cloud' (on), and 'Monitoring' (on). A 'Continue' button is at the bottom.

12. Choose whether to deploy in multiple availability zones (requires three subnets, each in a different AZ), or a single availability zone. I chose multiple AZs.

The screenshot shows the Cloud Manager interface with the title "Cloud Manager" at the top. The top navigation bar includes "Account: rt1600680", "Workspace: Workspace-1", "Connector: awscloudman...", and icons for gear, help, and refresh. Below the top bar, there are tabs for "Canvas", "Replication", "Backup & Restore", "K8s", "Data Sense", "File Cache", "Compute", "Sync", and "All Services (+8)". A sub-header "Create a New Working Environment" is followed by "HA Deployment Models". Two comparison boxes are shown: "Multiple Availability Zones" and "Single Availability Zone".

- Multiple Availability Zones:**
 - Provides maximum protection against AZ failures.
 - Enables selection of 3 availability zones.
 - An HA node serves data if its partner goes offline.
- Single Availability Zone:**
 - Protects against failures within a single AZ.
 - Single availability zone. HA nodes are in a placement group, spread across distinct underlying hardware.
 - An HA node serves data if its partner goes offline.

At the bottom left, it says "Cloud Manager 3.9.9 Build: 0 Aug 18, 2021 04:13:35 am UTC".

13. Choose the region, VPC, and security group for the cluster to be deployed into. In this section, you also assign the availability zones per node (and mediator) as well as the subnets that they occupy.

The screenshot shows the Cloud Manager interface with the title "Cloud Manager" at the top. The top navigation bar includes "Account: rt1600680", "Workspace: Workspace-1", "Connector: awscloudman...", and icons for gear, help, and refresh. Below the top bar, there are tabs for "Canvas", "Replication", "Backup & Restore", "K8s", "Data Sense", "File Cache", "Compute", "Sync", and "All Services (+8)". A sub-header "Create a New Working Environment" is followed by "Region & VPC".

Configuration fields include:

- AWS Region: US East | N. Virginia
- VPC: vpc-083fcbd79f75dfb6e - 10.221.0.0/16
- Security group: Use a generated security group
- Node 1:
 - Availability Zone: us-east-1a
 - Subnet: 10.221.1.0/24
- Node 2:
 - Availability Zone: us-east-1b
 - Subnet: 10.221.2.0/24
- Mediator:
 - Availability Zone: us-east-1c
 - Subnet: 10.221.3.0/24

At the bottom left, it says "Cloud Manager 3.9.9 Build: 0 Aug 18, 2021 04:13:35 am UTC".

14. Choose the connection methods for the nodes as well as the mediator.

The screenshot shows the Cloud Manager interface with the title "Cloud Manager" at the top. The top navigation bar includes "Account: rt1600680", "Workspace: Workspace-1", "Connector: awscloudman...", and icons for gear, help, and refresh. Below the top bar, there are tabs for "Canvas", "Replication", "Backup & Restore", "K8s", "Data Sense", "File Cache", "Compute", "Sync", and "All Services (+8)". A sub-header "Create a New Working Environment" is followed by "Connectivity & SSH Authentication".

Configuration fields include:

- Nodes:
 - SSH Authentication Method: Password
- Mediator:
 - Security Group: Use a generated security group
 - Key Pair Name: rt1600680
 - Internet Connection Method: Public IP address

At the bottom left, it says "Cloud Manager 3.9.9 Build: 0 Aug 18, 2021 04:13:35 am UTC".



The mediator requires communication with the AWS APIs. A public IP address is not required so long as the APIs are reachable after the mediator EC2 instance has been deployed.

1. Floating IP addresses are used to allow access to the various IP addresses that Cloud Volumes ONTAP uses, including cluster management and data serving IPs. These must be addresses that are not already routable within your network and are added to route tables in your AWS environment. These are required to enable consistent IP addresses for an HA pair during failover. More information about floating IP addresses can be found in the [NetApp Cloud Documentation](#).

The screenshot shows the 'Cloud Manager' interface with the 'Floating IPs' step selected. The top navigation bar includes 'Account r1618549', 'Workspace Workspace-1', 'Connector awscloudman...', and icons for settings, help, and refresh. Below the navigation is a menu bar with 'Canvas', 'Replication', 'Backup & Restore', 'K8s', 'Data Sense', 'File Cache', 'Compute', 'Sync', and 'All Services (+8)'. A sub-menu 'Create a New Working Environment' is open. The main content area is titled 'Floating IPs' and contains instructions: 'Floating IP addresses are required for cluster and SVM access and for NFS and CIFS data access. These floating IPs can migrate between HA nodes if failures occur. To access the data from outside the VPC, you can set up an AWS transit gateway.' It also states 'You must specify IP addresses that are outside of the CIDR blocks for all VPCs in the selected AWS region.' There are four input fields: 'Floating IP address for cluster management' (10.222.0.200), 'Floating IP address 1 for NFS and CIFS data' (10.222.0.201), 'Floating IP address 2 for NFS and CIFS data' (10.222.0.202), and 'Floating IP address for SVM management (Optional)' (Enter Floating IP Address). A 'Continue' button is at the bottom.

2. Select which route tables the floating IP addresses are added to. These route tables are used by clients to communicate with Cloud Volumes ONTAP.

The screenshot shows the 'Cloud Manager' interface with the 'Route Tables' step selected. The top navigation bar and menu bar are identical to the previous screenshot. The main content area is titled 'Route Tables' and contains instructions: 'Select the route tables that should include routes to the floating IP addresses. This enables client access to the Cloud Volumes ONTAP HA pair. If you leave a route table unselected, clients that are associated with the route table cannot access the HA pair.' An 'Additional information' link is present. Below is a table showing route table details:

Name	Main	ID	Associate with Subnet	Tags
private_rt_rt1600680	No	rtb-08b4cb88f65c826a5	3 Subnets	1 Tags
public_rt_rt1600680	Yes	rtb-0e46720d0da10c593	1 Subnets	1 Tags

At the bottom, it says '2 Route Tables | The main route table is the default for the VPC'. A 'Continue' button is at the bottom.

3. Choose whether to enable AWS managed encryption or AWS KMS to encrypt the ONTAP root, boot, and data disks.

Cloud Manager

Account: rt1600680 | Workspace: Workspace-1 | Connector: awscloudman...

Canvas | Replication | Backup & Restore | K8s | Data Sense | File Cache | Compute | Sync | All Services (+8) | [Create a New Working Environment](#) | [Data Encryption](#) | [X](#)

↑ Previous Step | [AWS Managed Encryption](#)

AWS is responsible for data encryption and decryption operations. Key management is handled by AWS key management services.

Default Master Key: aws/ebs

[Continue](#)

Cloud Manager 3.9.9 Build: 0 Aug 18, 2021 04:13:35 am UTC

4. Choose your licensing model. If you don't know which to choose, contact your NetApp representative.

Cloud Manager

Account: rt1600680 | Workspace: Workspace-1 | Connector: awscloudman...

Canvas | Replication | Backup & Restore | K8s | Data Sense | File Cache | Compute | Sync | All Services (+8) | [Create a New Working Environment](#) | [Cloud Volumes ONTAP Charging Methods & NSS Account](#) | [X](#)

↑ Previous Step | [Cloud Volumes ONTAP Charging Methods](#)

Learn more about our charging methods

Pay-As-You-Go by the hour

Bring your own license

Freemium (Up to 500GB)

NetApp Support Site Account (*Optional*)

Learn more about NetApp Support Site (NSS) accounts

To register this Cloud Volumes ONTAP to support, you should add NetApp Support Site Account.

Don't have a NetApp Support Site account? Select go to finish deploying this system. After it's created, use the Support Registration option to create an NSS account.

[Add Netapp Support Site Account](#)

[Continue](#)

Cloud Manager 3.9.9 Build: 0 Aug 18, 2021 04:13:35 am UTC

5. Select which configuration best suits your use case. This is related to the sizing considerations covered in the prerequisites page.

Cloud Manager

Account: rt1600680 | Workspace: Workspace-1 | Connector: awscloudman...

Canvas | Replication | Backup & Restore | K8s | Data Sense | File Cache | Compute | Sync | All Services (+8) | [Create a New Working Environment](#) | [Preconfigured Packages](#) | [X](#)

↑ Previous Step | [Select a preconfigured Cloud Volumes ONTAP system that best matches your needs, or create your own configuration. Preconfigured settings can be modified at a later time.](#) | [Change Configuration](#)

 POC and small workloads
Up to 2TB of storage

 Database and application data production workloads
Up to 10TB of storage

 Cost effective DR
Up to 10TB of storage

 Highest performance production workloads
Up to 368TB of storage

[Continue](#)

Cloud Manager 3.9.9 Build: 0 Aug 18, 2021 04:13:35 am UTC

6. Optionally, create a volume. This is not required, because the next steps use SnapMirror, which creates the volumes for us.

Cloud Manager

Create a New Working Environment Create Volume

↑ Previous Step Details & Protection Protocol

Volume Name: Size (GB): Volume size

Snapshot Policy: default

Access Control: Custom export policy

Custom export policy: 10.221.0.0/16

Advanced options

Continue Skip

Cloud Manager 3.9.9 Build: 0 Aug 18, 2021 04:13:35 am UTC

7. Review the selections made and tick the boxes to verify that you understand that Cloud Manager deploys resources into your AWS environment. When ready, click Go.

Cloud Manager

Create a New Working Environment Review & Approve

↑ Previous Step hybridawsvco Show API request

AWS | us-east-1 | HA

I understand that in order to activate support, I must first register Cloud Volumes ONTAP with NetApp. [More information >](#)

I understand that Cloud Manager will allocate the appropriate AWS resources to comply with my above requirements. [More information >](#)

Overview Networking Storage

Storage System:	Cloud Volumes ONTAP HA	HA Deployment Model:	Multiple Availability Zones
License Type:	Cloud Volumes ONTAP Standard	Encryption:	AWS Managed
Capacity Limit:	10TB	Customer Master Key:	aws/ebs

Go

Cloud Manager 3.9.9 Build: 0 Aug 18, 2021 04:13:35 am UTC

8. Cloud Volumes ONTAP now starts its deployment process. Cloud Manager uses AWS APIs and cloud formation stacks to deploy Cloud Volumes ONTAP. It then configures the system to your specifications, giving you a ready-to-go system that can be instantly utilized. The timing for this process varies depending on the selections made.

The screenshot shows the Cloud Manager Canvas interface. At the top, there are tabs for Canvas, Replication, Backup & Restore, K8s, Data Sense, File Cache, Compute, Sync, and All Services (+8). The Canvas tab is selected. On the left, there's a "Add Working Environment" button and a "Canvas" section with a cloud icon labeled "hybridawscvo Cloud Volumes ONTAP" and "C Initializing". To its right is an "Amazon S3" icon showing 1 Bucket and 1 Region. On the right, a "Working environments" section lists "Cloud Volumes ONTAP (High-Availability)" and "Amazon S3". A zoom-in icon is at the bottom right.

9. You can monitor the progress by navigating to the Timeline.

The screenshot shows the Cloud Manager main dashboard. At the top, there are tabs for Canvas, Replication, Backup & Restore, K8s, Data Sense, File Cache, Compute, Sync, and All Services (+8). The Canvas tab is selected. Below the tabs, there are sections for "Resources" and "Services". The "Resources" section includes "Canvas", "Digital Wallet", and "Timeline". The "Services" section includes "Replication", "Backup & Restore", "K8s", "Data Sense", "Compliance", "Tiering", "Monitoring", "File Cache", "Compute", "Sync", "SnapCenter", and "Active IQ". A link "https://cloudmanager.netapp.com/timeline" is shown at the bottom left.

10. The Timeline acts as an audit of all actions performed in Cloud Manager. You can view all of the API calls that are made by Cloud Manager during setup to both AWS as well as the ONTAP cluster. This can also be effectively used to troubleshoot any issues that you face.

The screenshot shows the Cloud Manager interface with the 'Timeline' tab selected. At the top, there are filters for Time, Service, Action, Agent, Resource, User, and Status, with 'Agent (1)' currently selected. The timeline table lists three events:

Time	Action	Service	Agent	Resource	User	Status
Aug 18 2021, 9:42:32 pm	Check Connectivity	Cloud Manager	awscloudman...	hybridawscvo	Full Name	Success
Aug 18 2021, 9:42:00 pm	Create Aws Ha Working Environment	Cloud Manager	awscloudma...	hybridawscvo	Full Name	Pending
Aug 18 2021, 10:09:39 pm	Describe Operation Status					Success
Aug 19 2021, 10:00:20 pm	Describe Operation Status					Success

- After deployment is complete, the CVO cluster appears on the Canvas, which the current capacity. The ONTAP cluster in its current state is fully configured to allow a true, out-of-the-box experience.

The screenshot shows the Cloud Manager interface with the 'Canvas' tab selected. On the left, there's a cloud icon labeled 'Add Working Environment'. In the center, there are two clouds representing environments: one for 'Cloud Volumes ONTAP' (labeled 'hybridawscvo', 'Cloud Volumes ONTAP', '1 GiB Capacity', and 'aws') and one for 'Amazon S3' (labeled 'Amazon S3', '2 Buckets', '1 Region', and 'aws'). On the right, a sidebar titled 'Working environments' lists the resources:

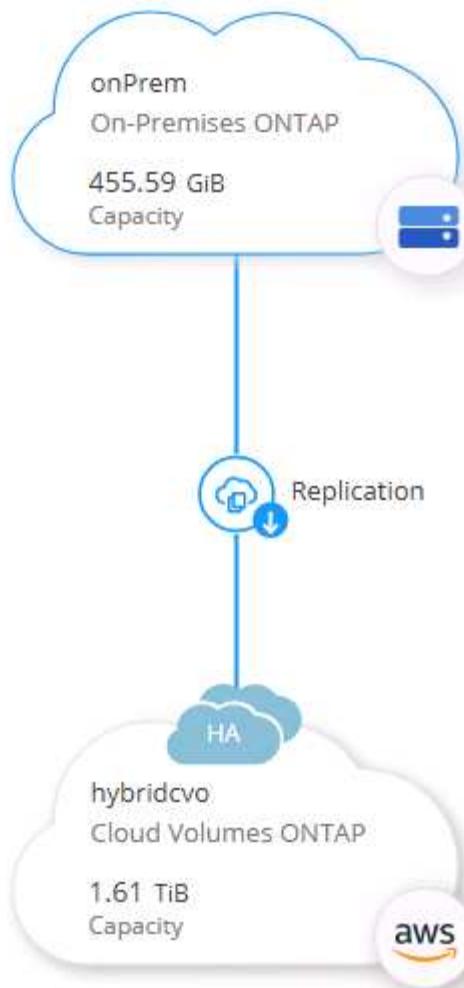
- 1 Cloud Volumes ONTAP (High-Availability)
1 GiB Allocated Capacity
- 1 Amazon S3
0 Buckets

Configure SnapMirror from on-premises to cloud

Now that you have a source ONTAP system and a destination ONTAP system deployed, you can replicate volumes containing database data into the cloud.

For a guide on compatible ONTAP versions for SnapMirror, see the [SnapMirror Compatibility Matrix](#).

- Click the source ONTAP system (on-premises) and either drag and drop it to the destination, select Replication > Enable, or select Replication > Menu > Replicate.



Select Enable.



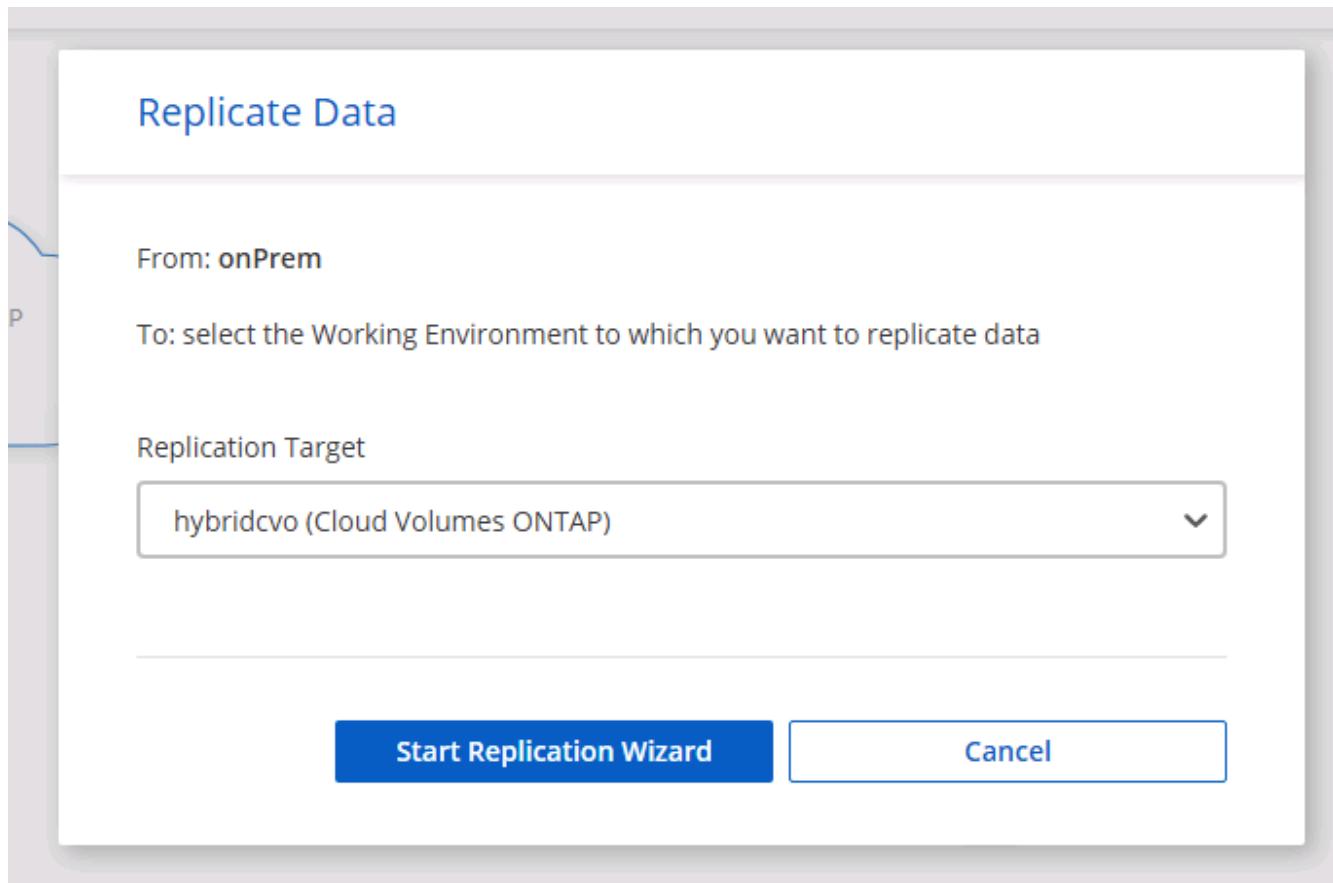
Or Options.

The screenshot shows the 'onPrem' cluster configuration in the NetApp ONTAP interface. At the top, there is a circular icon with two servers, followed by the text 'onPrem' and a green square indicating 'On'. To the right are three blue circular icons with symbols for information, more options, and delete. Below this, the word 'DETAILS' is in bold. Under 'DETAILS', the text 'On-PremisesONTAP' is displayed. In the 'SERVICES' section, there is another circular icon with a cloud and server, followed by the text 'Replication' and a green square indicating 'On'. To the right, it shows '1 Replication Target' with a blue circular icon containing three dots. A horizontal line separates this from the bottom section.

Replicate.

This screenshot is similar to the one above, showing the 'onPrem' cluster configuration. It includes the cluster icon, 'onPrem' name, and 'On' status. The 'DETAILS' section shows 'On-PremisesONTAP'. The 'SERVICES' section shows 'Replication' (On) with 1 Replication Target. A dropdown menu is open over the 'Replication' service entry, listing 'View Replications' and 'Replicate'.

2. If you did not drag and drop, choose the destination cluster to replicate to.



3. Choose the volume that you'd like to replicate. We replicated the data and all log volumes.

Source Volume Selection			
rhel2_u03 INFO Storage VM Name: svm_onPrem Tiering Policy: None Volume Type: RW CAPACITY 100 GB Allocated 7.29 GB Disk Used	rhel2_u03 INFO Storage VM Name: svm_onPrem Tiering Policy: None Volume Type: RW CAPACITY 100 GB Allocated 35.83 MB Disk Used	sql1_data INFO Storage VM Name: svm_onPrem Tiering Policy: None Volume Type: RW CAPACITY 53.37 GB Allocated 45.09 GB Disk Used	
sql1_log INFO Storage VM Name: svm_onPrem Tiering Policy: None Volume Type: RW CAPACITY 21.35 GB Allocated 18.16 GB Disk Used	sql1_snapctr INFO Storage VM Name: svm_onPrem Tiering Policy: None Volume Type: RW CAPACITY 24.87 GB Allocated 21.23 GB Disk Used		
Cloud Manager 3.9.10 Build: 2 Sep 12, 2021 06:47:41 am UTC			

4. Choose the destination disk type and tiering policy. For disaster recovery, we recommend an SSD as the disk type and to maintain data tiering. Data tiering tiers the mirrored data into low-cost object storage and saves you money on local disks. When you break the relationship or clone the volume, the data uses the fast, local storage.

[↑ Previous Step](#)

Destination Disk Type



S3 TIERING

[What are storage tiers?](#) Enabled DisabledNote: If you enable S3 tiering, thin provisioning must be enabled on volumes created in this aggregate.[Continue](#)

Cloud Manager 3.9.10 Build:2 Sep 12, 2021 06:47:41 am UTC

5. Select the destination volume name: we chose [source_volume_name]_dr.

Destination Volume Name

Destination Volume Name

sql1_data_dr

Destination Aggregate

Automatically select the best aggregate ▾

6. Select the maximum transfer rate for the replication. This enables you to save bandwidth if you have a low bandwidth connection to the cloud such as a VPN.

Max Transfer Rate

You should limit the transfer rate. An unlimited rate might negatively impact the performance of other applications and it might impact your Internet performance.

Limited to: MB/s

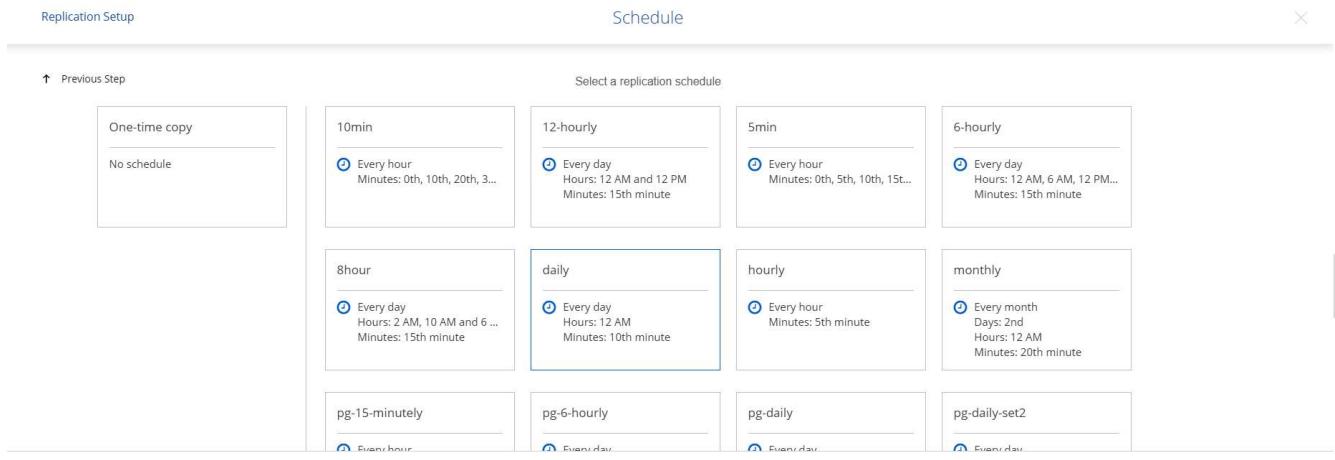
Unlimited (recommended for DR only machines)

7. Define the replication policy. We chose a Mirror, which takes the most recent dataset and replicates that into the destination volume. You could also choose a different policy based on your requirements.

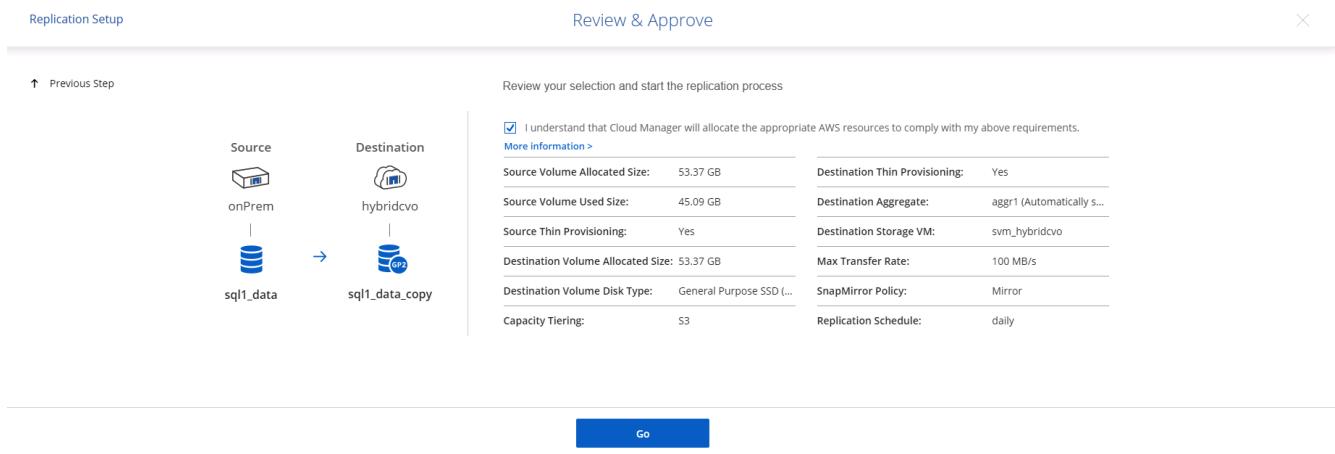
Replication Policy

Default Policies	Additional Policies
<p> Mirror</p> <p>Typically used for disaster recovery</p> <p>More info</p>	<p> Mirror and Backup (1 month retention)</p> <p>Configures disaster recovery and long-term retention of backups on the same destination volume</p> <p>More info</p>

8. Choose the schedule for triggering replication. NetApp recommends setting a "daily" schedule of for the data volume and an "hourly" schedule for the log volumes, although this can be changed based on requirements.



9. Review the information entered, click Go to trigger the cluster peer and SVM peer (if this is your first time replicating between the two clusters), and then implement and initialize the SnapMirror relationship.



10. Continue this process for data volumes and log volumes.

11. To check all of your relationships, navigate to the Replication tab inside Cloud Manager. Here you can manage your relationships and check on their status.

Health Status	Source Volume	Target Volume	Total Transfer Time	Status	Mirror State	Last Successful Transfer	Actions
✓	rhel2_u01 onPrem	rhel2_u01_dr hybridcvo	43 minutes 43 seconds	idle	snapmirrored	Sep 30, 2021, 12:12:50 AM 19.73 MiB	...
✓	rhel2_u02 onPrem	rhel2_u02_dr hybridcvo	1 hour 37 minutes 59 seconds	idle	snapmirrored	Sep 30, 2021, 2:37:08 PM 239.78 MiB	...
✓	rhel2_u03 onPrem	rhel2_u03_dr hybridcvo	16 hours 1 minute 9 seconds	idle	snapmirrored	Sep 30, 2021, 4:07:14 PM 225.37 KiB	...
✓	sql1_data onPrem	sql1_data_dr hybridcvo	1 hour 6 minutes 50 seconds	idle	snapmirrored	Sep 30, 2021, 12:12:28 AM 24.56 KiB	...

12. After all the volumes have been replicated, you are in a steady state and ready to move on to the disaster recovery and dev/test workflows.

3. Deploy EC2 compute instance for database workload

AWS has preconfigured EC2 compute instances for various workloads. The choice of instance type determines the number of CPU cores, memory capacity, storage type and capacity, and network performance. For the use cases, with the exception of the OS partition, the main storage to run database workload is allocated from CVO or the FSx ONTAP storage engine. Therefore, the main factors to consider are the choice of CPU cores, memory, and network performance level. Typical AWS EC2 instance types can be found here: [EC2 Instance Type](#).

Sizing the compute instance

1. Select the right instance type based on the required workload. Factors to consider include the number of business transactions to be supported, the number of concurrent users, data set sizing, and so on.
2. EC2 instance deployment can be launched through the EC2 Dashboard. The exact deployment procedures are beyond the scope of this solution. See [Amazon EC2](#) for details.

Linux instance configuration for Oracle workload

This section contain additional configuration steps after an EC2 Linux instance is deployed.

1. Add an Oracle standby instance to the DNS server for name resolution within the SnapCenter management domain.
2. Add a Linux management user ID as the SnapCenter OS credentials with sudo permissions without a password. Enable the ID with SSH password authentication on the EC2 instance. (By default, SSH password authentication and passwordless sudo is turned off on EC2 instances.)
3. Configure Oracle installation to match with on-premises Oracle installation such as OS patches, Oracle versions and patches, and so on.
4. NetApp Ansible DB automation roles can be leveraged to configure EC2 instances for database dev/test and disaster recovery use cases. The automation code can be download from the NetApp public GitHub site: [Oracle 19c Automated Deployment](#). The goal is to install and configure a database software stack on an EC2 instance to match on-premises OS and database configurations.

Windows instance configuration for SQL Server workload

This section lists additional configuration steps after an EC2 Windows instance is initially deployed.

1. Retrieve the Windows administrator password to log in to an instance via RDP.
2. Disable the Windows firewall, join the host to Windows SnapCenter domain, and add the instance to the DNS server for name resolution.
3. Provision a SnapCenter log volume to store SQL Server log files.
4. Configure iSCSI on the Windows host to mount the volume and format the disk drive.
5. Again, many of the previous tasks can be automated with the NetApp automation solution for SQL Server. Check the NetApp automation public GitHub site for newly published roles and solutions: [NetApp Automation](#).

Next: [Workflow for dev/test bursting to cloud](#).

Workflow for dev/test bursting to cloud

Previous: [Getting Started with AWS public cloud](#).

The agility of the public cloud, the time to value, and the cost savings are all meaningful value propositions for enterprises adopting the public cloud for database application development and testing effort. There is no better tool than SnapCenter to make this a reality. SnapCenter can not only protect your production database on-premises, but can also quickly clone a copy for application development or code testing in the public cloud while consuming very little extra storage. Following are details of the step-by-step processes for using this tool.

Clone an Oracle Database for dev/test from a replicated snapshot backup

1. Log into SnapCenter with a database management user ID for Oracle. Navigate to the Resources tab, which shows the Oracle databases being protected by SnapCenter.

Name	Oracle Database Type	Host/Cluster	Resource Group	Policies	Last Backup	Overall Status
cdb2	Single Instance (Multitenant)	rhel2.demo.netapp.com	rhel2_cdb2 rhel2_cdb2_log	Oracle Archive Log Backup Oracle Full Online Backup	09/17/2021 3:00:09 PM	Backup succeeded

2. Click the intended on-premises database name for the backup topology and the detailed view. If a secondary replicated location is enabled, it shows linked mirror backups.

Backup Name	Count	Type	End Date	Verified	Mounted	RMAN Cataloged	SCN
rhel2_cdb2_log_09-17-2021_15.00.01.1317_1	1	Log	09/17/2021 3:00:10 PM	Not Applicable	False	Not Cataloged	5980203
rhel2_cdb2_09-17-2021_14.35.01.4997_1	1	Log	09/17/2021 2:35:21 PM	Not Applicable	False	Not Cataloged	5980629
rhel2_cdb2_09-17-2021_14.35.01.4997_0	1	Data	09/17/2021 2:35:12 PM	Unverified	False	Not Cataloged	5980588
rhel2_cdb2_log_09-17-2021_14.00.01.1042_1	1	Log	09/17/2021 2:00:10 PM	Not Applicable	False	Not Cataloged	5978388
rhel2_cdb2_log_09-17-2021_13.00.01.7389_1	1	Log	09/17/2021 1:00:11 PM	Not Applicable	False	Not Cataloged	5975135
rhel2_cdb2_log_09-17-2021_12.00.01.1142_1	1	Log	09/17/2021 12:00:10 PM	Not Applicable	False	Not Cataloged	5971773
rhel2_cdb2_log_09-17-2021_11.00.01.0895_1	1	Log	09/17/2021 11:00:10 AM	Not	False	Not Cataloged	5968474

3. Toggled to the mirrored backups view by clicking mirrored backups. The secondary mirror backup(s) is then displayed.

NetApp SnapCenter®

Oracle Database ▾

Search databases

cdb2 Topology

Manage Copies

Local copies

Mirror copies

Summary Card

368 Backups

16 Data Backups

352 Log Backups

0 Clones

Backup Name

	Count	Type	IF	End Date	Verified	Mounted	RMAN Cataloged	SCN
rhel2_cdb2_log_09-17-2021_15.00.01.1317_1	1	Log		09/17/2021 3:00:10 PM	Not Applicable	False	Not Cataloged	5980203
rhel2_cdb2_09-17-2021_14.35.01.4997_1	1	Log		09/17/2021 2:35:21 PM	Not Applicable	False	Not Cataloged	5980629
rhel2_cdb2_09-17-2021_14.35.01.4997_0	1	Data		09/17/2021 2:35:12 PM	Unverified	False	Not Cataloged	5980588
rhel2_cdb2_log_09-17-2021_14.00.01.1042_1	1	Log		09/17/2021 2:00:10 PM	Not Applicable	False	Not Cataloged	5978388
rhel2_cdb2_log_09-17-2021_13.00.01.7389_1	1	Log		09/17/2021 1:00:11 PM	Not Applicable	False	Not Cataloged	5975135
rhel2_cdb2_log_09-17-2021_12.00.01.1142_1	1	Log		09/17/2021 12:00:10 PM	Not Applicable	False	Not Cataloged	5971773
rhel2_cdb2_log_09-17-2021_11.00.01.0895_1	1	Log		09/17/2021 11:00:10 AM	Not Applicable	False	Not Cataloged	5968474

Total 1

- Choose a mirrored secondary database backup copy to be cloned and determine a recovery point either by time and system change number or by SCN. Generally, the recovery point should be trailing the full database backup time or SCN to be cloned. After a recovery point is decided, the required log file backup must be mounted for recovery. The log file backup should be mounted to target DB server where the clone database is to be hosted.

Mount backups

Choose the host to mount the backup : ora-standby.demo.netapp.com

Mount path : /var/opt/snapcenter/sco/backup_mount/rhel2_cdb2_09-17-2021_14.35.01.4997_1/cdb2

Secondary storage location : Snap Vault / Snap Mirror

Source Volume	Destination Volume
svm_onPrem:rhel2_u03	svm_hybridcvo:rhel2_u03_dr

Mount Cancel

Backup Name	Count	Type	End Date	Verified	Mounted	RMAN Cataloged	SCN
rhel2_cdb2_log_09-17-2021_16.00.01.2156_1	1	Log	09/17/2021 4:00:10 PM	Not Applicable	False	Not Cataloged	5985272
rhel2_cdb2_log_09-17-2021_15.00.01.1317_1	1	Log	09/17/2021 3:00:10 PM	Not Applicable	False	Not Cataloged	5982003
rhel2_cdb2_09-17-2021_14.35.01.4997_1	1	Log	09/17/2021 2:35:21 PM	Not Applicable	True	Not Cataloged	5980629
rhel2_cdb2_09-17-2021_14.35.01.4997_0	1	Data	09/17/2021 2:35:12 PM	Unverified	False	Not Cataloged	5980588
rhel2_cdb2_log_09-17-2021_14.00.01.1042_1	1	Log	09/17/2021 2:00:10 PM	Not Applicable	False	Not Cataloged	5978388



If log pruning is enabled and the recovery point is extended beyond the last log pruning, multiple archive log backups might need to be mounted.

5. Highlight the full database backup copy to be cloned, and then click the clone button to start the DB clone Workflow.

Backup Name	Count	Type	End Date	Verified	Mounted	RMAN Cataloged	SCN
rhel2_cdb2_log_09-17-2021_16.00.01.2156_1	1	Log	09/17/2021 4:00:10 PM	Not Applicable	False	Not Cataloged	5985272
rhel2_cdb2_log_09-17-2021_15.00.01.1317_1	1	Log	09/17/2021 3:00:10 PM	Not Applicable	False	Not Cataloged	5982003
rhel2_cdb2_09-17-2021_14.35.01.4997_1	1	Log	09/17/2021 2:35:21 PM	Not Applicable	True	Not Cataloged	5980629
rhel2_cdb2_09-17-2021_14.35.01.4997_0	1	Data	09/17/2021 2:35:12 PM	Unverified	False	Not Cataloged	5980588
rhel2_cdb2_log_09-17-2021_14.00.01.1042_1	1	Log	09/17/2021 2:00:10 PM	Not Applicable	False	Not Cataloged	5978388

6. Choose a proper clone DB SID for a complete container database or CDB clone.

Clone from cdb2

1 Name

Complete Database Clone

Clone SID: cdb2test

Exclude PDBs: Type to find PDBs

PDB Clone

Secondary storage location : Snap Vault / Snap Mirror

Data

Source Volume	Destination Volume
svm_onPrem:rhel2_u02	svm_hybridcvo:rhel2_u02_dr

Logs

Source Volume	Destination Volume
svm_onPrem:rhel2_u03	svm_hybridcvo:rhel2_u03_dr

[Previous](#) [Next](#)

7. Select the target clone host in the cloud, and datafile, control file, and redo log directories are created by the clone workflow.

Clone from cdb2

1 Name

Select the host to create a clone

Clone host

2 Locations

3 Credentials

4 PreOps

5 PostOps

6 Notification

7 Summary

④ Datafile locations

/u02_cdb2test

⑤ Control files

/u02_cdb2test/cdb2test/control/control01.ctl
/u02_cdb2test/cdb2test/control/control02.ctl

⑥ Redo logs

Group	Size	Unit	Number of files
RedoGroup 1	200	MB	1
/u02_cdb2test/cdb2test/redolog redo03.log			
RedoGroup 2	200	MB	1

- The None credential name is used for OS-based authentication, which renders the database port irrelevant. Fill in the proper Oracle Home, Oracle OS User, and Oracle OS Group as configured in the target clone DB server.

Clone from cdb2

1 Name

2 Locations

3 Credentials

4 PreOps

5 PostOps

6 Notification

7 Summary

Database Credentials for the clone

Credential name for sys user + ?

Database port

Oracle Home Settings ?

Oracle Home

Oracle OS User

Oracle OS Group

Previous Next

The screenshot shows the 'Clone from cdb2' wizard in progress, specifically the 'Credentials' step (step 3). On the left, a vertical navigation bar lists steps 1 through 7. Step 3, 'Credentials', is highlighted with a blue background. The main area contains two sections: 'Database Credentials for the clone' and 'Oracle Home Settings'. Under 'Database Credentials', there is a dropdown menu for 'Credential name for sys user' set to 'None', a '+' button, and a help icon. A text input field for 'Database port' contains '1521'. Under 'Oracle Home Settings', three fields are shown: 'Oracle Home' with the path '/u01/app/oracle/product/19800/cdb2', 'Oracle OS User' with 'oracle', and 'Oracle OS Group' with 'oinstall'. At the bottom right are 'Previous' and 'Next' buttons.

9. Specify the scripts to run before clone operation. More importantly, the database instance parameter can be adjusted or defined here.

Clone from cdb2

Specify scripts to run before clone operation

Prescript full path	/var/opt/snapcenter/spl/scripts/	Enter Prescript path
Arguments		
Script timeout	60	secs

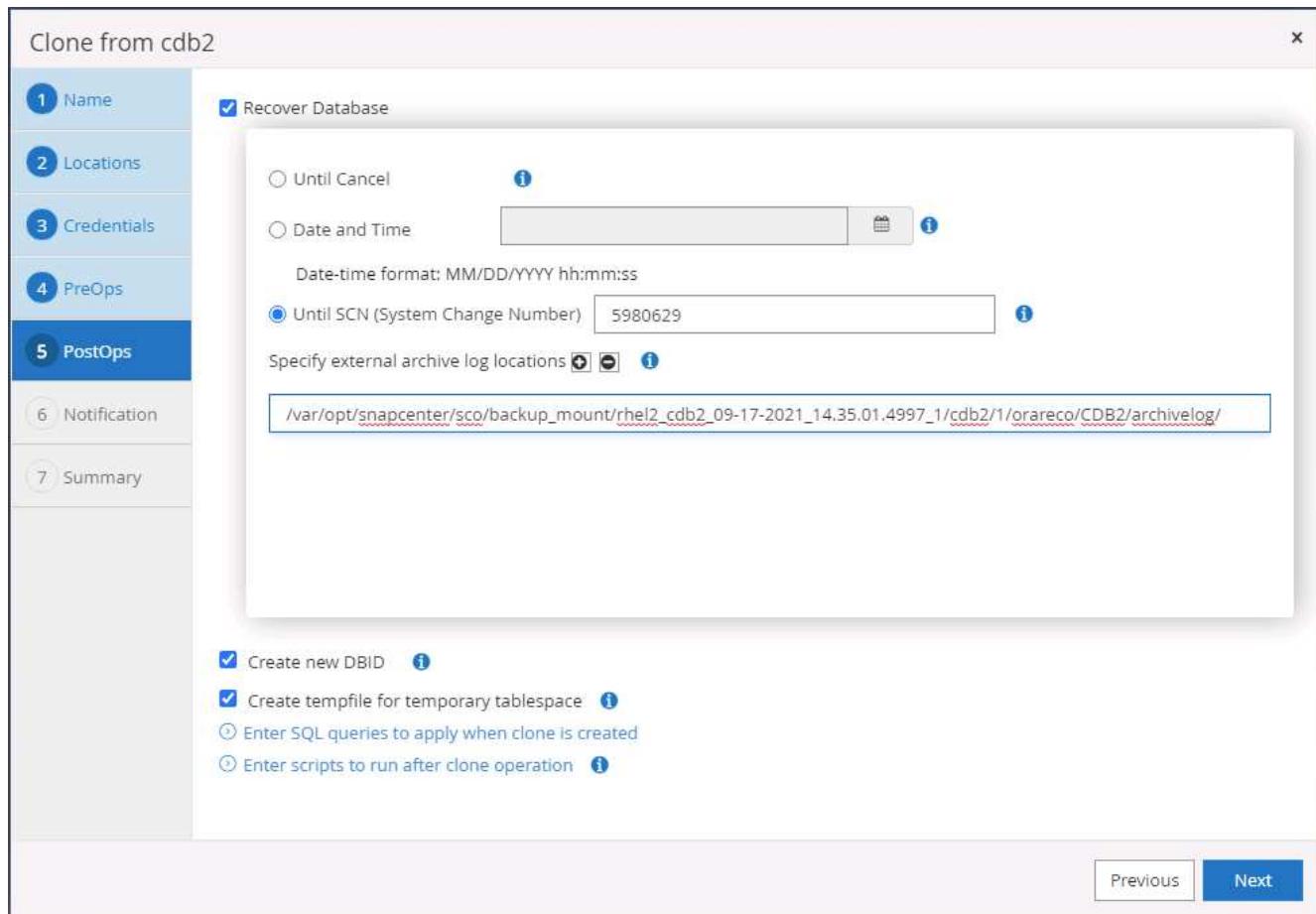
Database Parameter settings

processes	320	X
remote_login_passwordfile	EXCLUSIVE	X
sga_target	4311744512	X
undo_tablespace	UNDOTBS1	X

Buttons:

- Previous
- Next

- Specify the recovery point either by the date and time or SCN. Until Cancel recovers the database up to the available archive logs. Specify the external archive log location from the target host where the archive log volume is mounted. If target server Oracle owner is different from the on-premises production server, verify that the archive log directory is readable by the target server Oracle owner.



```
oracle@ora-standby:/tmp
[oracle@ora-standby tmp]$ ls /var/opt/snapcenter/sco/backup_mount/rhel2_cdb2_09-17-2021_14.35.01.4997_1/cdb2/1/orareco/CDB2/archivelog/
2021_08_26 2021_08_28 2021_08_30 2021_09_01 2021_09_03 2021_09_05 2021_09_07 2021_09_09 2021_09_11 2021_09_13 2021_09_15 2021_09_17
2021_08_27 2021_08_29 2021_08_31 2021_09_02 2021_09_04 2021_09_06 2021_09_08 2021_09_10 2021_09_12 2021_09_14 2021_09_16
[oracle@ora-standby tmp]$
```

11. Configure the SMTP server for email notification if desired.

Clone from cdb2

Provide email settings i

Email preference	Never
From	From email
To	Email to
Subject	Notification

Attach job report

⚠ If you want to send notifications for Clone jobs, an SMTP server must be configured. Continue to the Summary page to save your information, and then go to Settings>Global Settings>Notification Server Settings to configure the SMTP server.

[Previous](#) [Next](#)

12. Clone summary.

Clone from cdb2

1 Name	Summary
2 Locations	Clone from backup rhel2_cdb2_09-17-2021_14.35.01.4997_0
3 Credentials	Clone SID cdb2test
4 PreOps	Clone server ora-standby.demo.netapp.com
5 PostOps	Exclude PDBs none
6 Notification	Oracle home /u01/app/oracle/product/19800/cdb2
7 Summary	Oracle OS user oracle Oracle OS group oinstall Datafile mountpaths /u02_cdb2test Control files /u02_cdb2test/cdb2test/control/control01.ctl /u02_cdb2test/cdb2test/control/control02.ctl Redo groups RedoGroup =1 TotalSize =200 Path =/u02_cdb2test/cdb2test/redolog redo03.log RedoGroup =2 TotalSize =200 Path =/u02_cdb2test/cdb2test/redolog redo02.log RedoGroup =3 TotalSize =200 Path =/u02_cdb2test/cdb2test/redolog redo01.log Recovery scope Until SCN 5980629 Prescript full path none Prescript arguments Postscript full path none Postscript arguments

[Previous](#) [Finish](#)

13. You should validate after cloning to make sure that the cloned database is operational. Some additional tasks, such as starting up the listener or turning off the DB log archive mode, can be performed on the dev/test database.

```
oracle@ora-standby:/tmp
[oracle@ora-standby tmp]$ export ORACLE_SID=cdb2test
[oracle@ora-standby tmp]$ export ORACLE_HOME=/u01/app/oracle/product/19800/cdb2
[oracle@ora-standby tmp]$ export PATH=$PATH:$ORACLE_HOME/bin
[oracle@ora-standby tmp]$ sqlplus / as sysdba

SQL*Plus: Release 19.0.0.0.0 - Production on Fri Sep 17 17:49:29 2021
Version 19.3.0.0.0

Copyright (c) 1982, 2019, Oracle. All rights reserved.

Connected to:
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.3.0.0.0

SQL> select name, log_mode from v$database;
NAME      LOG_MODE
-----
cdb2test  ARCHIVELOG

SQL> select instance_name, host_name from v$instance;
INSTANCE_NAME
-----
HOST_NAME
-----
cdb2test
ora-standby.demo.netapp.com

SQL> show pdbs
CON_ID CON_NAME          OPEN MODE  RESTRICTED
----- -----
  2 PDB$SEED        READ ONLY NO
  3 CDB2_PDB1       READ WRITE NO
  4 CDB2_PDB2       READ WRITE NO
  5 CDB2_PDB3       READ WRITE NO

SQL>
```

Clone a SQL database for dev/test from a replicated Snapshot backup

1. Log into SnapCenter with a database management user ID for SQL Server. Navigate to the Resources tab, which shows the SQL Server user databases being protected by SnapCenter and a target standby SQL instance in the public cloud.

Name	Instance	Host	Last Backup	Overall Status	Type
master	sql1	sql1.demo.netapp.com		Not available for backup	System database
model	sql1	sql1.demo.netapp.com		Not available for backup	System database
msdb	sql1	sql1.demo.netapp.com		Not available for backup	System database
tempdb	sql1	sql1.demo.netapp.com		Not available for backup	System database
tpcc	sql1	sql1.demo.netapp.com	09/16/2021 7:35:05 PM	Backup succeeded	User database
master	sql1-standby	sql1-standby.demo.netapp.com		Not available for backup	System database
model	sql1-standby	sql1-standby.demo.netapp.com		Not available for backup	System database
msdb	sql1-standby	sql1-standby.demo.netapp.com		Not available for backup	System database
tempdb	sql1-standby	sql1-standby.demo.netapp.com		Not available for backup	System database

2. Click on the intended on-premises SQL Server user database name for the backups topology and detailed view. If a secondary replicated location is enabled, it shows linked mirror backups.

Backup Name	Count	Type	End Date	Verified
sql1_tpcc_09-16-2021_18.25.01.4024	1	Full backup	09/16/2021 6:25:05 PM	Unverified
sql1_tpcc_09-15-2021_18.25.01.4604	1	Full backup	09/15/2021 6:25:06 PM	Unverified
sql1_tpcc_09-14-2021_18.25.01.5233	1	Full backup	09/14/2021 6:25:05 PM	Unverified
sql1_tpcc_09-13-2021_18.25.01.4500	1	Full backup	09/13/2021 6:25:05 PM	Unverified
sql1_tpcc_09-12-2021_18.25.01.4016	1	Full backup	09/12/2021 6:25:05 PM	Unverified
sql1_tpcc_09-11-2021_18.25.01.3753	1	Full backup	09/11/2021 6:25:05 PM	Unverified
sql1_tpcc_09-10-2021_18.36.25.5430	1	Full backup	09/10/2021 6:36:29 PM	Unverified

3. Toggle to the Mirrored Backups view by clicking Mirrored Backups. Secondary Mirror Backup(s) are then displayed. Because SnapCenter backs up the SQL Server transaction log to a dedicated drive for recovery, only full database backups are displayed here.

Backup Name	Count	Type	End Date	Verified
sql1_tpcc_09-16-2021_18.25.01.4024	1	Full backup	09/16/2021 6:25:05 PM	Unverified
sql1_tpcc_09-15-2021_18.25.01.4604	1	Full backup	09/15/2021 6:25:06 PM	Unverified
sql1_tpcc_09-14-2021_18.25.01.5233	1	Full backup	09/14/2021 6:25:05 PM	Unverified
sql1_tpcc_09-13-2021_18.25.01.4500	1	Full backup	09/13/2021 6:25:05 PM	Unverified
sql1_tpcc_09-12-2021_18.25.01.4016	1	Full backup	09/12/2021 6:25:05 PM	Unverified
sql1_tpcc_09-11-2021_18.25.01.3753	1	Full backup	09/11/2021 6:25:05 PM	Unverified
sql1_tpcc_09-10-2021_18.36.25.5430	1	Full backup	09/10/2021 6:36:29 PM	Unverified

4. Choose a backup copy, and then click the Clone button to launch the Clone from Backup workflow.

Backup Name	Count	Type	End Date	Verified
sql1_tpcc_09-19-2021_18.25.01.4134	1	Full backup	09/19/2021 6:25:05 PM	Unverified
sql1_tpcc_09-18-2021_18.25.01.3963	1	Full backup	09/18/2021 6:25:05 PM	Unverified
sql1_tpcc_09-17-2021_18.25.01.4218	1	Full backup	09/17/2021 6:25:05 PM	Unverified
sql1_tpcc_09-16-2021_18.25.01.4024	1	Full backup	09/16/2021 6:25:05 PM	Unverified
sql1_tpcc_09-15-2021_18.25.01.4604	1	Full backup	09/15/2021 6:25:06 PM	Unverified
sql1_tpcc_09-14-2021_18.25.01.5233	1	Full backup	09/14/2021 6:25:05 PM	Unverified
sql1_tpcc_09-13-2021_18.25.01.4500	1	Full backup	09/13/2021 6:25:05 PM	Unverified

Clone from backup

1 Clone Options

Clone settings

Clone server: Choose

Clone instance: Nothing selected

Clone name: tpcc

Choose mount option

Auto assign mount point

Auto assign volume mount point under path: full file path

Secondary storage location : Snap Vault / Snap Mirror

Source Volume	Destination Volume
svm_onPrem:sql1_data	svm_hybridcvo:sql1_data_dr
svm_onPrem:sql1_log	svm_hybridcvo:sql1_log_dr

Next

5. Select a cloud server as the target clone server, clone instance name, and clone database name. Choose either an auto-assign mount point or a user-defined mount point path.

Clone from backup x

1 Clone Options

Clone settings

Clone server	sql-standby.demo.netapp.com	i
Clone instance	sql-standby	i
Clone name	tpcc_clone	

Choose mount option

Auto assign mount point i

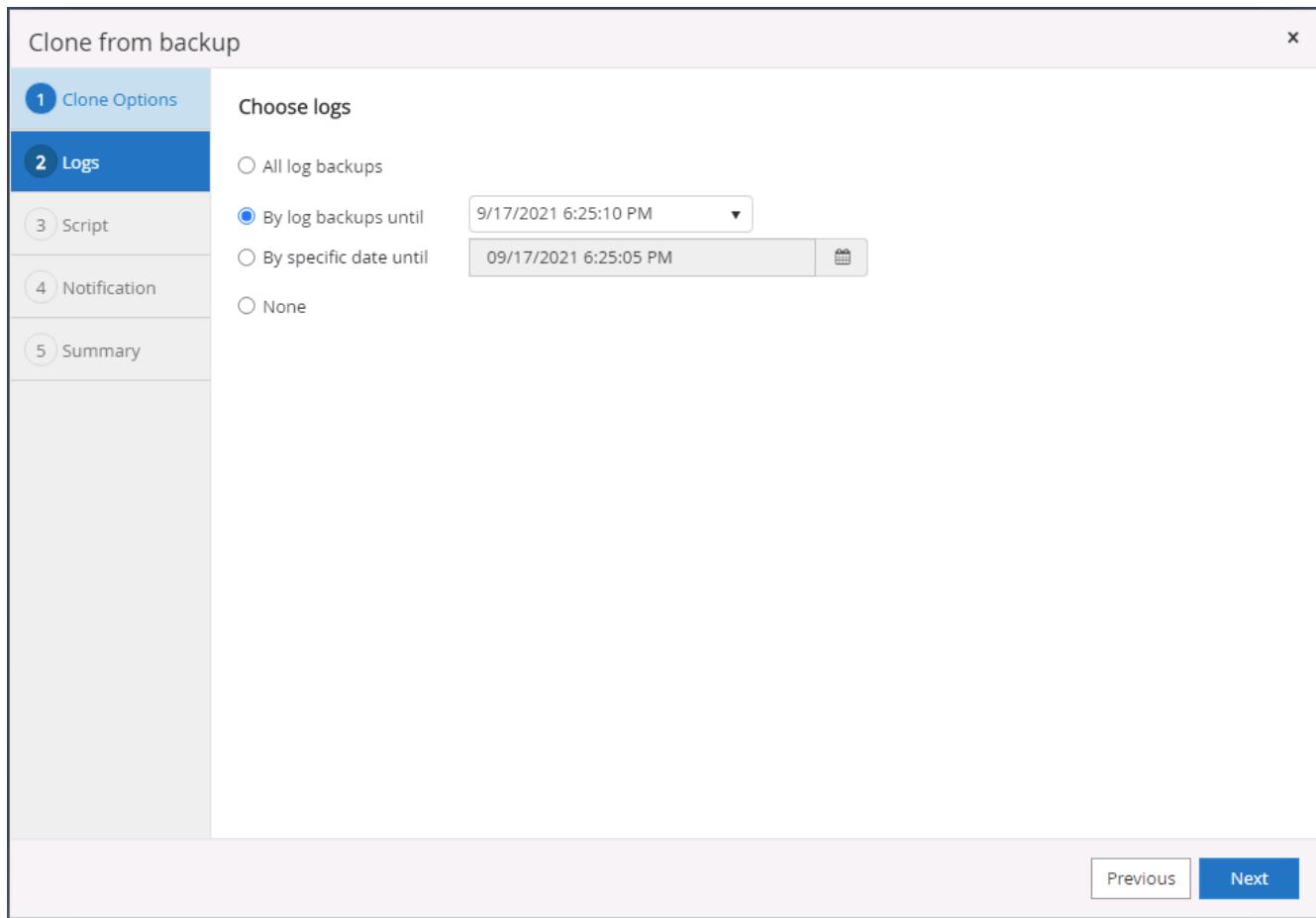
Auto assign volume mount point under path full file path i

Secondary storage location : Snap Vault / Snap Mirror

Source Volume	Destination Volume
svm_onPrem:sql1_data	svm_hybridcvo:sql1_data_dr
svm_onPrem:sql1_log	svm_hybridcvo:sql1_log_dr

Previous Next

6. Determine a recovery point either by a log backup time or by a specific date and time.



7. Specify optional scripts to run before and after the cloning operation.

Clone from backup x

1 Clone Options

2 Logs

3 Script

4 Notification

5 Summary

Specify optional scripts to run before and after performing a clone from backup job

Prescript full path

Prescript arguments Choose optional arguments...

Postscript full path

Postscript arguments Choose optional arguments...

Script timeout 60 secs

Previous Next

8. Configure an SMTP server if email notification is desired.

Clone from backup X

1 Clone Options

2 Logs

3 Script

4 Notification

5 Summary

Provide email settings i

Email preference	Never
From	From email
To	Email to
Subject	Notification

Attach Job Report

⚠ If you want to send notifications for Clone jobs, an SMTP server must be configured. Continue to the Summary page to save your information, and then go to Settings>Global Settings>Notification Server Settings to configure the SMTP server. X

Previous Next

9. Clone Summary.

Clone from backup

1 Clone Options

2 Logs

3 Script

4 Notification

5 Summary

Summary	
Clone server	sql-standby.demo.netapp.com
Clone instance	sql-standby
Clone name	tpcc_dev
Mount option	Auto assign volume mount point under custom path
Prescript full path	None
Prescript arguments	
Postscript full path	None
Postscript arguments	
Send email	No

[Previous](#) [Finish](#)

- Monitor the job status and validate that the intended user database has been attached to a target SQL instance in the cloud clone server.

ID	Status	Name	Start date	End date	Owner
766	✓	Clone from backup 'sql1_tpcc_09-16-2021_18:25:01.4024'	09/16/2021 8:05:25 PM	09/16/2021 8:06:17 PM	demo\sqldba
763	✓	Discover resources for all hosts	09/16/2021 7:56:49 PM	09/16/2021 7:56:54 PM	demo\sqldba
761	✓	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/16/2021 7:59:00 PM	09/16/2021 7:57:08 PM	demo\sqldba
760	⚠	Discover resources for all hosts	09/16/2021 7:19:05 PM	09/16/2021 7:19:09 PM	demo\sqldba
759	⚠	Discover resources for all hosts	09/16/2021 7:18:43 PM	09/16/2021 7:18:48 PM	demo\sqldba
756	⚠	Discover resources for all hosts	09/16/2021 6:59:51 PM	09/16/2021 6:59:56 PM	demo\sqldba
753	✓	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/16/2021 6:35:00 PM	09/16/2021 6:37:07 PM	demo\sqldba
750	✓	Backup of Resource Group 'sql1_tpcc' with policy 'SQL Server Full Backup'	09/16/2021 6:25:01 PM	09/16/2021 6:27:14 PM	demo\sqldba
749	✓	Discover resources for host 'sql-standby.demo.netapp.com'	09/16/2021 6:19:00 PM	09/16/2021 6:19:05 PM	Demo\administrator
745	✓	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/16/2021 5:35:00 PM	09/16/2021 5:37:08 PM	demo\sqldba

Post-clone configuration

- An Oracle production database on-premises is usually running in log archive mode. This mode is not necessary for a development or test database. To turn off log archive mode, log into the Oracle DB as sysdba, execute a log mode change command, and start the database for access.
- Configure an Oracle listener, or register the newly cloned DB with an existing listener for user access.
- For SQL Server, change the log mode from Full to Easy so that the SQL Server dev/test log file can be readily shrunk when it is filling up the log volume.

Refresh clone database

1. Drop cloned databases and clean up the cloud DB server environment. Then follow the previous procedures to clone a new DB with fresh data. It only takes few minutes to clone a new database.
2. Shutdown the clone database, run a clone refresh command by using the CLI. See the following SnapCenter documentation for details: [Refresh a clone](#).

Where to go for help?

If you need help with this solution and use cases, join the [NetApp Solution Automation community support Slack channel](#) and look for the solution-automation channel to post your questions or inquires.

Next: [Disaster recovery workflow](#).

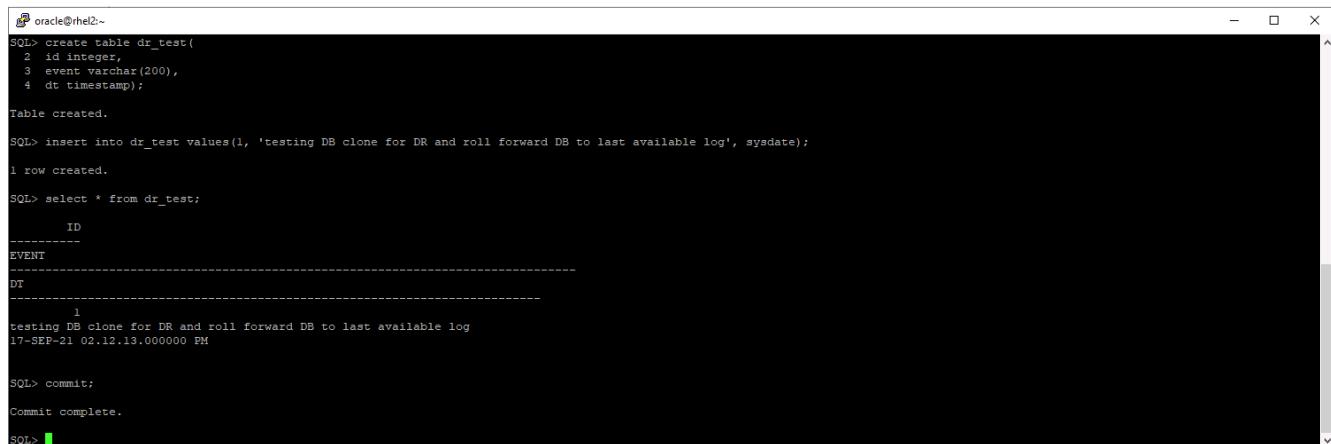
Disaster recovery workflow

Previous: [Workflow for dev/test bursting to cloud](#).

Enterprises have embraced the public cloud as a viable resource and destination for disaster recovery. SnapCenter makes this process as seamless as possible. This disaster recovery workflow is very similar to the clone workflow, but database recovery runs through the last available log that was replicated to cloud to recover all the business transactions possible. However, there are additional pre-configuration and post-configuration steps specific to disaster recovery.

Clone an on-premises Oracle production DB to cloud for DR

1. To validate that the clone recovery runs through last available log, we created a small test table and inserted a row. The test data would be recovered after a full recovery to last available log.



```
oracle@rhel2:~$ SQL> create table dr_test(
  2  id integer,
  3  event varchar(200),
  4  dt timestamp);
Table created.

SQL> insert into dr_test values(1, 'testing DB clone for DR and roll forward DB to last available log', sysdate);
1 row created.

SQL> select * from dr_test;
      ID
-----
EVENT
-----
DT
-----
      1
testing DB clone for DR and roll forward DB to last available log
17-SEP-21 02.12.13.000000 PM

SQL> commit;
Commit complete.

SQL>
```

2. Log into SnapCenter as a database management user ID for Oracle. Navigate to the Resources tab, which shows the Oracle databases being protected by SnapCenter.

The screenshot shows the NetApp SnapCenter interface. On the left, there's a sidebar with icons for Dashboard, Resources (selected), Monitor, Reports, Hosts, Storage Systems, Settings, and Alerts. The main area has a dropdown menu set to 'Oracle Database'. Below it, a search bar says 'Resource Group' and a search field contains 'rhe12_cdb2_log'. A table lists resources: 'rhe12_cdb2' (1 resource, orafullbkup tag, Oracle Full Online Backup policy, last backup 09/17/2021 2:38:16 PM, completed) and 'rhe12_cdb2_log' (1 resource, oralogbkup tag, Oracle Archive Log Backup policy, last backup 09/17/2021 6:02:13 PM, completed). A 'New Resource Group' button is in the top right.

3. Select the Oracle log resource group and click Backup Now to manually run an Oracle log backup to flush the latest transaction to the destination in the cloud. In a real DR scenario, the last transaction recoverable depends on the database log volume replication frequency to the cloud, which in turn depends on the RTO or RPO policy of the company.

This screenshot shows the 'rhe12_cdb2_log' resource group details. The sidebar and top navigation are identical to the previous screenshot. The main table now shows the details for 'rhe12_cdb2_log': Name (rhe12_cdb2), Resource Name (cdb2), Type (Oracle Database), and Host (rhe12.demo.netapp.com). Action buttons for Modify Resource Group, Back up Now, Maintenance, and Delete are at the top right.

A modal dialog box titled 'Backup' is displayed. It asks 'Create a backup for the selected resource group'. The 'Resource Group' field contains 'rhe12_cdb2_log'. The 'Policy' field is a dropdown set to 'Oracle Archive Log Backup', with an information icon next to it. At the bottom are 'Cancel' and 'Backup' buttons.



Asynchronous SnapMirror loses data that has not made it to the cloud destination in the database log backup interval in a disaster recovery scenario. To minimize data loss, more frequent log backup can be scheduled. However there is a limit to the log backup frequency that is technically achievable.

4. Select the last log backup on the Secondary Mirror Backup(s), and mount the log backup.

The screenshot shows the NetApp SnapCenter interface for Oracle Database management. On the left, a sidebar lists databases: cdb2, cdb2dev, and cdb2test. The main pane displays 'cdb2 Topology' with a diagram showing 'Local copies' (185 Backups, 0 Clones) connected to 'Mirror copies' (185 Backups, 2 Clones). A summary card on the right provides an overview of backups: 370 Backups, 16 Data Backups, 354 Log Backups, and 2 Clones. Below this, a table titled 'Secondary Mirror Backup(s)' lists three log backups:

Backup Name	Count	Type	End Date	Verified	Mounted	RMAN Cataloged	SCN
rhel2_cdb2_log_09-17-2021_18.20.04.1177_1	1	Log	09/17/2021 6:20:13 PM	Not Applicable	False	Not Cataloged	5994710
rhel2_cdb2_log_09-17-2021_18.00.01.2424_1	1	Log	09/17/2021 6:00:09 PM	Not Applicable	False	Not Cataloged	5992079
rhel2_cdb2_log_09-17-2021_17.00.01.1566_1	1	Log	09/17/2021 5:00:20 PM	Not Applicable	False	Not Cataloged	5988842

The dialog box is titled 'Mount backups'. It asks 'Choose the host to mount the backup' (set to 'ora-standby.demo.netapp.com') and specifies the 'Mount path' as '/var/opt/snapcenter/sco/backup_mount/rhel2_cdb2_log_09-17-2021_18.20.04.1177_1/cdb2'. It also shows the 'Secondary storage location : Snap Vault / Snap Mirror' section with 'Source Volume' set to 'svm_onPrem:rhel2_u03' and 'Destination Volume' set to 'svm_hybridcvo:rhel2_u03_dr'. At the bottom are 'Mount' and 'Cancel' buttons.

5. Select the last full database backup and click Clone to initiate the clone workflow.

Total 3

Backup Name	Count	Type	IF	End Date	Verified	Mounted	RMAN Cataloged	SCN
rhel2_cdb2_log_09-17-2021_18.20.04.1177_1	1	Log		09/17/2021 6:20:13 PM	Not Applicable	True	Not Cataloged	5994710
rhel2_cdb2_log_09-17-2021_18.00.01.2424_1	1	Log		09/17/2021 6:00:09 PM	Not Applicable	False	Not Cataloged	5992079
rhel2_cdb2_log_09-17-2021_17.00.01.1566_1	1	Log		09/17/2021 5:00:20 PM	Not Applicable	False	Not Cataloged	5988842
rhel2_cdb2_log_09-17-2021_16.00.01.2156_1	1	Log		09/17/2021 4:00:10 PM	Not Applicable	False	Not Cataloged	5985272
rhel2_cdb2_log_09-17-2021_15.00.01.1317_1	1	Log		09/17/2021 3:00:10 PM	Not Applicable	False	Not Cataloged	5982003
rhel2_cdb2_09-17-2021_14.35.01.4997_1	1	Log		09/17/2021 2:35:21 PM	Not Applicable	False	Not Cataloged	5980629
rhel2_cdb2_09-17-2021_14.35.01.4997_0	1	Data		09/17/2021 2:35:12 PM	Unverified	False	Not Cataloged	5980588

6. Select a unique clone DB ID on the host.

Clone from cdb2

1 Name

Complete Database Clone

Clone SID: **cdb2dr**

PDB Clone

Secondary storage location : Snap Vault / Snap Mirror

2 Locations

3 Credentials

4 PreOps

5 PostOps

6 Notification

7 Summary

Data

Source Volume	Destination Volume
svm_onPrem:rhel2_u02	svm_hybridcvo:rhel2_u02_dr

Logs

Source Volume	Destination Volume
svm_onPrem:rhel2_u03	svm_hybridcvo:rhel2_u03_dr

Previous **Next**

7. Provision a log volume and mount it to the target DR server for the Oracle flash recovery area and online logs.

The screenshot shows the ONTAP System Manager interface. On the left, there's a navigation sidebar with sections like DASHBOARD, STORAGE (Overview, Applications, Volumes), LUNs, Shares, Qtrees, Quotas, Storage VMs, Tiers, NETWORK, EVENTS & JOBS, PROTECTION, and HOSTS. The main area is titled 'Volumes' and lists several volumes: ora_standby_u01, rhel2_u01_dr, rhel2_u02_dr, rhel2_u02_dr09172116081193_60, rhel2_u02_dr09172117035348_63, rhel2_u03_dr, and rhel2_u03_dr09172118245747_75. A modal window titled 'Add Volume' is open, showing fields for NAME ('ora_standby_u03') and CAPACITY ('20 GB'). There are 'More Options' and 'Save' buttons at the bottom.

```

[ec2-user@ora-standby:tmp]$ sudo mkdir /u03_cdb2dr
[ec2-user@ora-standby tmp]$ chown oracle:oinstall /u03_cdb2dr
chown: changing ownership of '/u03_cdb2dr': Operation not permitted
[ec2-user@ora-standby tmp]$ sudo chown oracle:oinstall /u03_cdb2dr
[ec2-user@ora-standby tmp]$ sudo mount -t nfs 10.221.1.6:/ora_standby_u03 /u03_cdb2dr
[ec2-user@ora-standby tmp]$ df -h
Filesystem      Size  Used Avail Use% Mounted on
/dev/tmpfs       7.6G  0    7.6G  0% /dev
tmpfs           7.6G  0    7.6G  0% /dev/shm
tmpfs           7.6G  17M  7.6G  1% /run
tmpfs           7.6G  0    7.6G  0% /sys/fs/cgroup
/dev/nvme0nlp2   10G  9.0G  1.1G  90% /
10.221.1.6:/ora_standby_u01   31G  13G  18G  42% /u01
tmpfs           1.6G  0    1.6G  0% /run/user/1000
10.221.1.6:/Sc28182452-3fa8-448c-9e4a-c5a9e465f353 100G  3.1G  97G  4% /u02_cdb2dev
tmpfs           1.6G  0    1.6G  0% /run/user/54321
10.221.1.6:/Sc39c05df8-4b00-4b3a-853c-9d6d338e5df7 100G  3.7G  97G  4% /u02_cdb2test
10.221.1.6:/Scff88ea5c-3273-475e-ad97-472b2a8dccee 100G  3.8G  97G  4% /var/opt/snapcenter/sco/backup_mount/rhel2_cdb2_log_09-17-2021_18.20.04.1177_1/cdb2/1
10.221.1.6:/ora_standby_u03   21G  320K  20G  1% /u03_cdb2dr
[ec2-user@ora-standby tmp]$

```



The Oracle clone procedure does not create a log volume, which needs to be provisioned on the DR server before cloning.

8. Select the target clone host and location to place the data files, control files, and redo logs.

Clone from cdb2

1 Name

Select the host to create a clone

Clone host ora-standby.demo.netapp.com

2 Locations

Datafile locations /u02_cdb2dr

Control files /u02_cdb2dr/cdb2dr/control/control01.ctl
/u03_cdb2dr/cdb2dr/control/control02.ctl

Redo logs

Group	Size	Unit	Number of files
RedoGroup 1	200	MB	1
RedoGroup 2	200	MB	1

Previous Next

The screenshot shows the Oracle Database Clone wizard interface. The left sidebar lists steps 1 through 7. Step 2, 'Locations', is selected and active. The main area is titled 'Select the host to create a clone' and shows the 'Clone host' as 'ora-standby.demo.netapp.com'. Below this, under 'Datafile locations', the path '/u02_cdb2dr' is listed. Under 'Control files', two paths are listed: '/u02_cdb2dr/cdb2dr/control/control01.ctl' and '/u03_cdb2dr/cdb2dr/control/control02.ctl'. Under 'Redo logs', there is a table with three columns: Group, Size, and Unit. It contains two entries: 'RedoGroup 1' with size 200 MB and 1 file, and 'RedoGroup 2' with size 200 MB and 1 file. At the bottom right are 'Previous' and 'Next' buttons.

9. Select the credentials for the clone. Fill in the details of the Oracle home configuration on the target server.

Clone from cdb2

1 Name

2 Locations

3 Credentials

4 PreOps

5 PostOps

6 Notification

7 Summary

Database Credentials for the clone

Credential name for sys user + ?

Database port

Oracle Home Settings ?

Oracle Home

Oracle OS User

Oracle OS Group

Previous Next

The screenshot shows the Oracle Database Clone wizard interface. The left sidebar lists steps 1 through 7. Step 3, 'Credentials', is currently selected and highlighted in blue. The main panel shows 'Database Credentials for the clone' with a dropdown for 'Credential name for sys user' set to 'None'. Below it, the 'Database port' is set to '1521'. Under 'Oracle Home Settings', the 'Oracle Home' path is '/u01/app/oracle/product/19800/cdb2', and the 'Oracle OS User' and 'Oracle OS Group' are both 'oracle'. At the bottom right are 'Previous' and 'Next' buttons.

10. Specify the scripts to run before cloning. Database parameters can be adjusted if needed.

Clone from cdb2

Specify scripts to run before clone operation ⓘ

Prescript full path	/var/opt/snapcenter/spl/scripts/	Enter Prescript path
Arguments		
Script timeout	60	secs

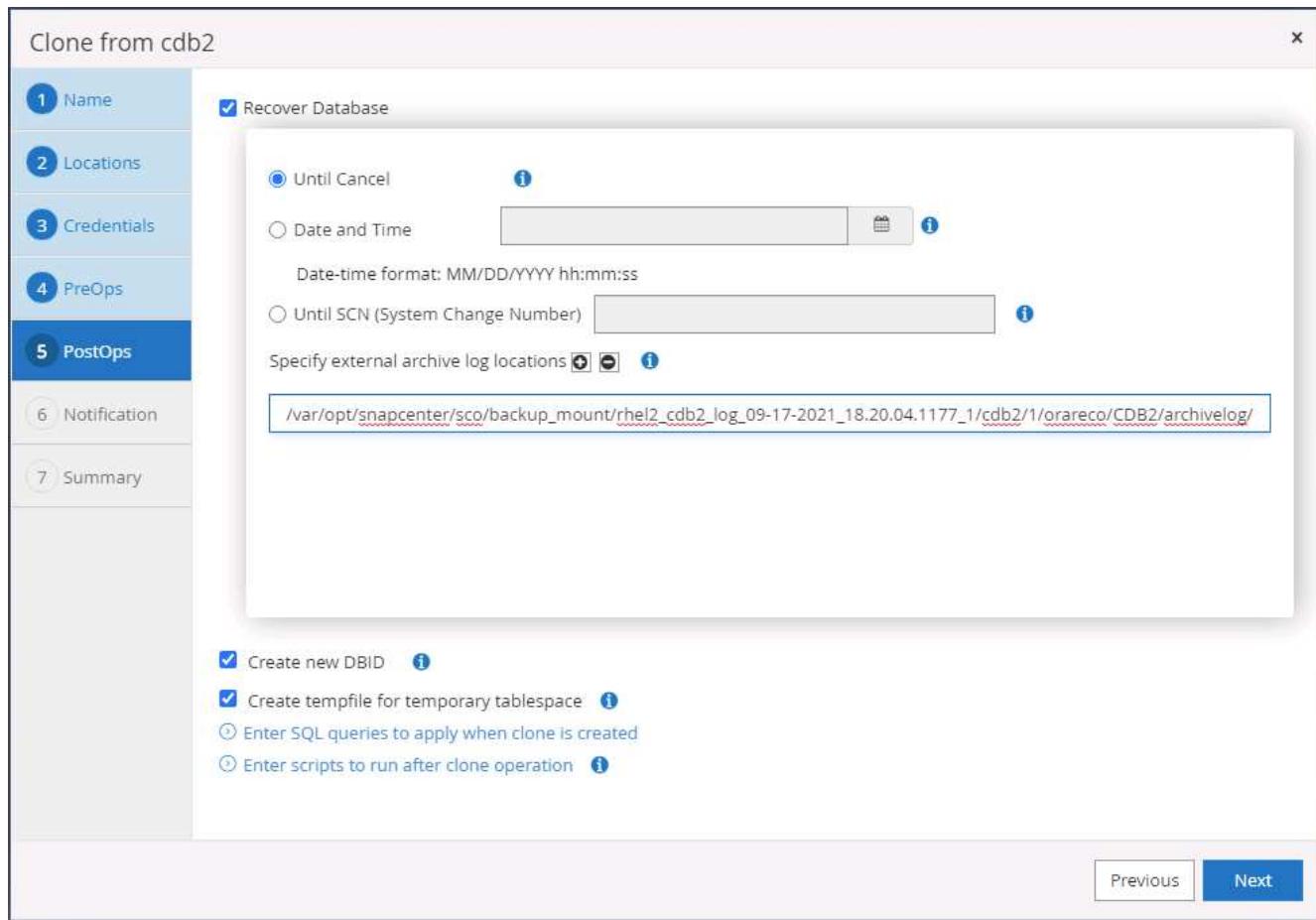
Database Parameter settings

audit_file_dest	/u01/app/oracle/admin/cdb2dr/adump	X
audit_trail	DB	X
open_cursors	300	X
pga_aggregate_target	1432354816	X

Buttons:

- Previous
- Next

- Select Until Cancel as the recovery option so that the recovery runs through all available archive logs to recoup the last transaction replicated to the secondary cloud location.



12. Configure the SMTP server for email notification if needed.

Clone from cdb2

Provide email settings i

Email preference	Never
From	From email
To	Email to
Subject	Notification

Attach job report

⚠ If you want to send notifications for Clone jobs, an SMTP server must be configured. Continue to the Summary page to save your information, and then go to Settings>Global Settings>Notification Server Settings to configure the SMTP server.

[Previous](#) [Next](#)

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

13. DR clone summary.

Clone from cdb2

1 Name	Summary
2 Locations	Clone from backup rhel2_cdb2_09-17-2021_14.35.01.4997_0
3 Credentials	Clone SID cdb2dr
4 PreOps	Clone server ora-standby.demo.netapp.com
5 PostOps	Exclude PDBs none
6 Notification	Oracle home /u01/app/oracle/product/19800/cdb2
7 Summary	Oracle OS user oracle
	Oracle OS group oinstall
	Datafile mountpaths /u02_cdb2dr
	Control files /u02_cdb2dr/cdb2dr/control/control01.ctl /u03_cdb2dr/cdb2dr/control/control02.ctl
	Redo groups RedoGroup =1 TotalSize =200 Path =/u03_cdb2dr/cdb2dr/redolog/redo03.log RedoGroup =2 TotalSize =200 Path =/u03_cdb2dr/cdb2dr/redolog/redo02.log RedoGroup =3 TotalSize =200 Path =/u03_cdb2dr/cdb2dr/redolog/redo01.log
	Recovery scope Until Cancel
	Prescript full path none
	Prescript arguments
	Postscript full path none
	Postscript arguments

[Previous](#) [Finish](#)

14. Cloned DBs are registered with SnapCenter immediately after clone completion and are then available for backup protection.

Oracle Database							
Resources		Name	Oracle Database Type	Host/Cluster	Resource Group	Policies	Last Backup
<input checked="" type="checkbox"/>		cdb2	Single Instance (Multitenant)	rhel2.demo.netapp.com	rhel2_cdb2 rhel2_cdb2_log	Oracle Archive Log Backup Oracle Full Online Backup	09/17/2021 7:00:10 PM
<input checked="" type="checkbox"/>		cdb2dev	Single Instance (Multitenant)	ora-standby.demo.netapp.com			Not protected
<input checked="" type="checkbox"/>		cdb2dr	Single Instance (Multitenant)	ora-standby.demo.netapp.com			Not protected
<input checked="" type="checkbox"/>		cdb2test	Single Instance (Multitenant)	ora-standby.demo.netapp.com			Not protected

Post DR clone validation and configuration for Oracle

1. Validate the last test transaction that has been flushed, replicated, and recovered at the DR location in the cloud.

```

oracle@ora-standby:/u01/app/oracle/product/19000/cdb2/dbs
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.3.0.0.0

SQL> set lin 200
SQL> select instance_name, host_name from v$instance;

INSTANCE_NAME      HOST_NAME
cdb2dr            ora-standby.demo.netapp.com

SQL> alter pluggable database cdb2_pdb1 open;
Pluggable database altered.

SQL> alter session set container=cdb2_pdb1;
Session altered.

SQL> select * from pdbadmin.dr_test;

ID
EVENT
DT
1
testing DB clone for DR and roll forward DB to last available log
17-SEP-21 02.12.13.000000 PM

SQL>

```

2. Configure the flash recovery area.

```

oracle@ora-standby:/u01/app/oracle/product/19000/cdb2/dbs
[oracle@ora-standby dbs]$ sqlplus / as sysdba

SQL*Plus: Release 19.0.0.0.0 - Production on Fri Sep 17 22:07:11 2021
Version 19.3.0.0.0

Copyright (c) 1982, 2019, Oracle. All rights reserved.

Connected to:
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.3.0.0.0

SQL> show parameter db_recovery_file_dest

NAME          TYPE        VALUE
-----
db_recovery_file_dest    string
db_recovery_file_dest_size  big integer 17208M
SQL> alter system set db_recovery_file_dest='/u03_cdb2dr/cdb2dr' scope=both;

System altered.

SQL> show parameter db_recovery_file_dest

NAME          TYPE        VALUE
-----
db_recovery_file_dest    string    /u03_cdb2dr/cdb2dr
db_recovery_file_dest_size  big integer 17208M
SQL>

```

3. Configure the Oracle listener for user access.

4. Split the cloned volume off of the replicated source volume.

5. Reverse replication from the cloud to on-premises and rebuild the failed on-premises database server.



Clone split may incur temporary storage space utilization that is much higher than normal operation. However, after the on-premises DB server is rebuilt, extra space can be released.

Clone an on-premises SQL production DB to cloud for DR

- Similarly, to validate that the SQL clone recovery ran through last available log, we created a small test table and inserted a row. The test data would be recovered after a full recovery to the last available log.

```

Administrator: Command Prompt - sqlcmd - SQLCMD
C:\Users\administrator.DEMO>sqlcmd
1> select host_name()
2> go

-----
SQL1

(1 rows affected)
1> use tpcc
2> go
Changed database context to 'tpcc'.
1> insert into snap_sync values ('test snap mirror DR for SQL', getdate())
2> go

(1 rows affected)
1> select * from snap_sync
2> go
event                                dt
test snap mirror DR for SQL          2021-09-20 14:23:04.533
(1 rows affected)
1> -

```

- Log into SnapCenter with a database management user ID for SQL Server. Navigate to the Resources tab, which shows the SQL Server protection resources group.

Name	Resource Name	Type	Host
sql1_tpcc	tpcc (sql1)	SQL Database	sql1.demo.netapp.com
sql1_tpcc_log			

- Manually run a log backup to flush the last transaction to be replicated to secondary storage in the public cloud.

Backup

Create a backup for the selected resource group

Resource Group: sql1_tpcc_log

Policy: SQL Server Log Backup

Cancel Backup

- Select the last full SQL Server backup for the clone.

Backup Name	Count	Type	End Date	Verified
sql1_tpcc_09-19-2021_18.25.01.4134	1	Full backup	09/19/2021 6:25:05 PM	Unverified
sql1_tpcc_09-18-2021_18.25.01.3963	1	Full backup	09/18/2021 6:25:05 PM	Unverified
sql1_tpcc_09-17-2021_18.25.01.4218	1	Full backup	09/17/2021 6:25:05 PM	Unverified

5. Set the clone setting such as the Clone Server, Clone Instance, Clone Name, and mount option. The secondary storage location where cloning is performed is auto-populated.

Clone from backup

1 Clone Options

Clone settings

Clone server: sql-standby.demo.netapp.com

Clone instance: sql-standby

Clone name: tpcc_dr

Choose mount option

Auto assign mount point

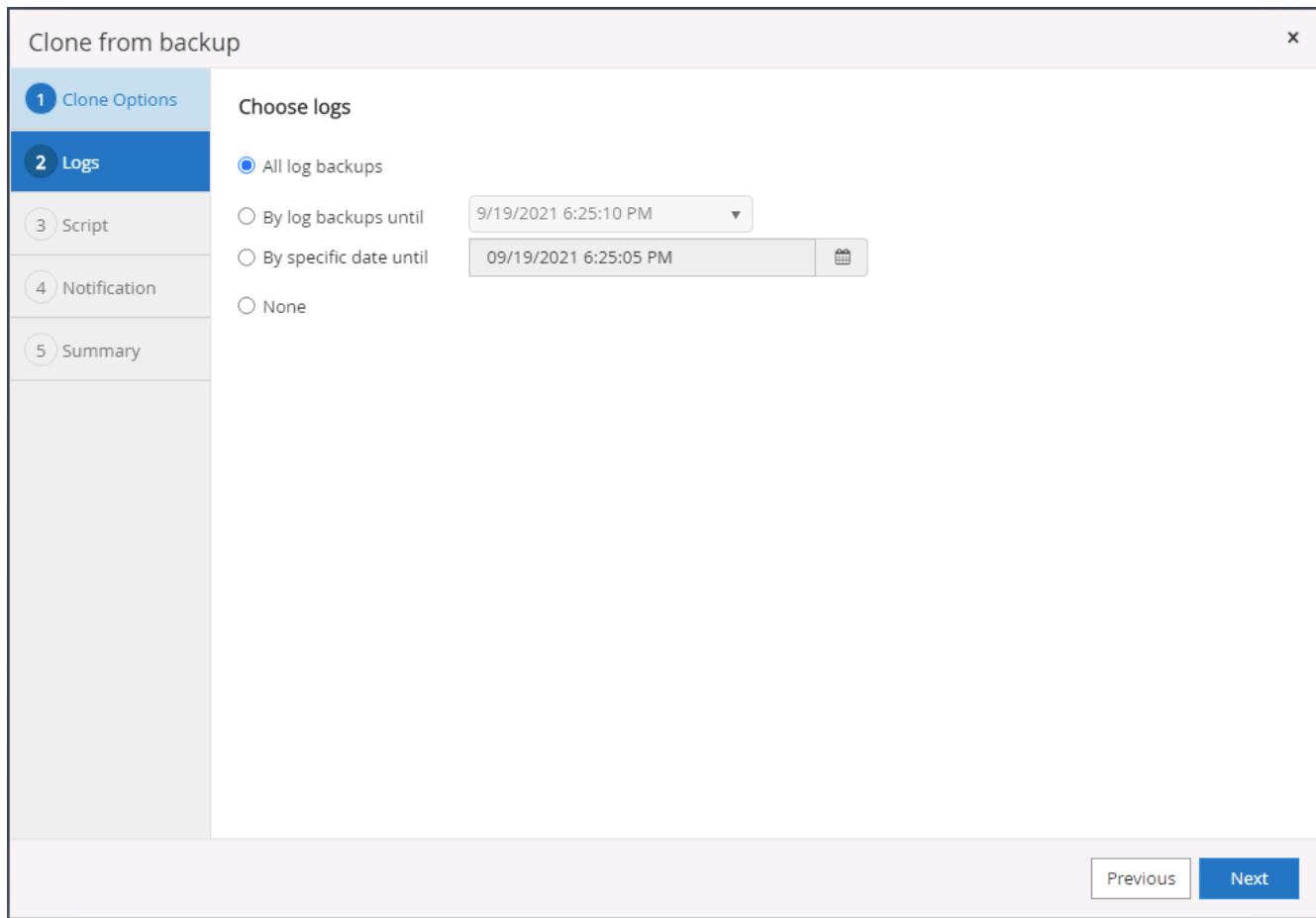
Auto assign volume mount point under path full file path

Secondary storage location : Snap Vault / Snap Mirror

Source Volume	Destination Volume
svm_onPrem:sql1_data	svm_hybridcvo:sql1_data_dr
svm_onPrem:sql1_log	svm_hybridcvo:sql1_log_dr

Next

6. Select all log backups to be applied.



7. Specify any optional scripts to run before or after cloning.

Clone from backup x

1 Clone Options

2 Logs

3 Script

4 Notification

5 Summary

Specify optional scripts to run before and after performing a clone from backup job

Prescript full path

Prescript arguments Choose optional arguments...

Postscript full path

Postscript arguments Choose optional arguments...

Script timeout 60 secs

Previous Next

8. Specify an SMTP server if email notification is desired.

Clone from backup

1 Clone Options

2 Logs

3 Script

4 Notification

5 Summary

Provide email settings i

Email preference: Never

From: From email

To: Email to

Subject: Notification

Attach Job Report

⚠ If you want to send notifications for Clone jobs, an SMTP server must be configured. Continue to the Summary page to save your information, and then go to Settings>Global Settings>Notification Server Settings to configure the SMTP server.

Previous

Next

The screenshot shows the 'Clone from backup' wizard in progress, specifically step 4: Notification. The left sidebar lists steps 1 through 5. Step 4 is highlighted in blue. The main area is titled 'Provide email settings' with an information icon. It contains four input fields: 'Email preference' set to 'Never', 'From' set to 'From email', 'To' set to 'Email to', and 'Subject' set to 'Notification'. Below these is a checkbox labeled 'Attach Job Report'. At the bottom, a note in an orange box states: '⚠ If you want to send notifications for Clone jobs, an SMTP server must be configured. Continue to the Summary page to save your information, and then go to Settings>Global Settings>Notification Server Settings to configure the SMTP server.' Navigation buttons 'Previous' and 'Next' are at the bottom right.

9. DR clone summary. Cloned databases are immediately registered with SnapCenter and available for backup protection.

Clone from backup

1 Clone Options

2 Logs

3 Script

4 Notification

5 Summary

Summary	
Clone server	sql-standby.demo.netapp.com
Clone instance	sql-standby
Clone name	tpcc_dr
Mount option	Auto Mount
Prescript full path	None
Prescript arguments	
Postscript full path	None
Postscript arguments	
Send email	No

[Previous](#) [Finish](#)

NetApp SnapCenter®

Microsoft SQL Server

Dashboard		View Database						
		Name	Instance	Host	Last Backup	Overall Status	Type	
✓ Resources	master	sql1	sql1.demo.netapp.com			Not available for backup	System database	
	model	sql1	sql1.demo.netapp.com			Not available for backup	System database	
	msdb	sql1	sql1.demo.netapp.com			Not available for backup	System database	
	tempdb	sql1	sql1.demo.netapp.com			Not available for backup	System database	
	tpcc	sql1	sql1.demo.netapp.com		09/22/2021 5:35:08 PM	Backup failed, Schedules on hold	User database	
		master	sql-standby	sql-standby.demo.netapp.com			Not available for backup	System database
		model	sql-standby	sql-standby.demo.netapp.com			Not available for backup	System database
		msdb	sql-standby	sql-standby.demo.netapp.com			Not available for backup	System database
		tempdb	sql-standby	sql-standby.demo.netapp.com			Not available for backup	System database
		tpcc_clone	sql-standby	sql-standby.demo.netapp.com			Not protected	User database
	tpcc_dlev	sql-standby	sql-standby.demo.netapp.com			Not protected	User database	
	tpcc_dr	sql-standby	sql-standby.demo.netapp.com			Not protected	User database	

[Refresh Resources](#) [New Resource Group](#)

Post DR clone validation and configuration for SQL

1. Monitor clone job status.

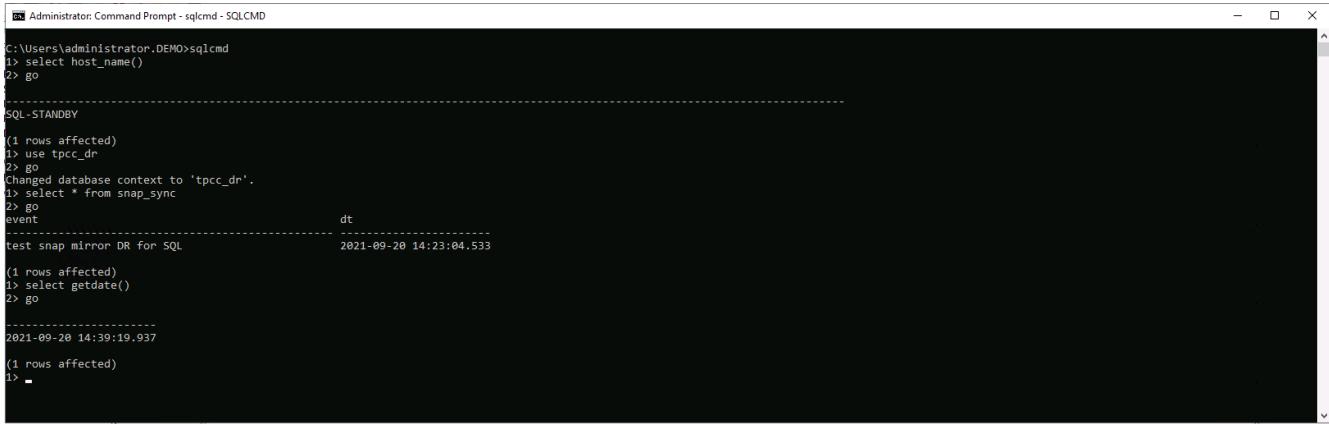
NetApp SnapCenter®

Jobs

Jobs		Schedules	Events	Logs		
		Search by name				
✓ Resources	ID	Status	Name			
	1052	✓	Clone from backup 'sql1_tpcc_09-19-2021_18.25.01.4134'	Start date: 09/20/2021 2:36:17 PM	End date: 09/20/2021 2:37:06 PM	Owner: demo\sqldba
	1047	✓	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/20/2021 2:35:01 PM	09/20/2021 2:37:08 PM	demo\sqldba
	1045	✓	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/20/2021 2:28:17 PM	09/20/2021 2:30:25 PM	demo\sqldba
	1044	✓	Clone from backup 'sql1_tpcc_09-17-2021_18.25.01.4218'	09/20/2021 1:39:24 PM	09/20/2021 1:40:09 PM	demo\sqldba
	1042	✓	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/20/2021 1:35:01 PM	09/20/2021 1:37:08 PM	demo\sqldba
	1040	✓	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/20/2021 1:25:01 PM	09/20/2021 1:27:08 PM	demo\sqldba

[Details](#) [Reports](#) [Download Logs](#) [Cancel Job](#)

2. Validate that last transaction has been replicated and recovered with all log file clones and recovery.



```
C:\Users\administrator.DEMO>sqlcmd
1> select host_name()
2> go
-----
SQL STANDBY
(1 rows affected)
1> use tpcc_dr
2> go
Changed database context to 'tpcc_dr'.
1> select * from snap_sync
2> go
event                                dt
test snap mirror DR for SQL          2021-09-20 14:23:04.533
(1 rows affected)
1> select getdate()
2> go
-----
2021-09-20 14:39:19.937
(1 rows affected)
1> -
```

3. Configure a new SnapCenter log directory on the DR server for SQL Server log backup.
4. Split the cloned volume off of the replicated source volume.
5. Reverse replication from the cloud to on-premises and rebuild the failed on-premises database server.

Where to go for help?

If you need help with this solution and use cases, please join the [NetApp Solution Automation community support Slack channel](#) and look for the solution-automation channel to post your questions or inquiries.

Copyright information

Copyright © 2023 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—with 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.