



## **Getting started overview**

NetApp Solutions

NetApp  
March 11, 2022

This PDF was generated from [https://docs.netapp.com/us-en/netapp-solutions/ent-apps-db/hybrid\\_dbops\\_snapcenter\\_getting\\_started\\_onprem.html](https://docs.netapp.com/us-en/netapp-solutions/ent-apps-db/hybrid_dbops_snapcenter_getting_started_onprem.html) on March 11, 2022. Always check [docs.netapp.com](https://docs.netapp.com) for the latest.

# Table of Contents

Getting started overview .....	1
On-premises .....	1
AWS public cloud .....	1
Getting started on premises .....	1
Getting Started with AWS public cloud .....	54

# 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

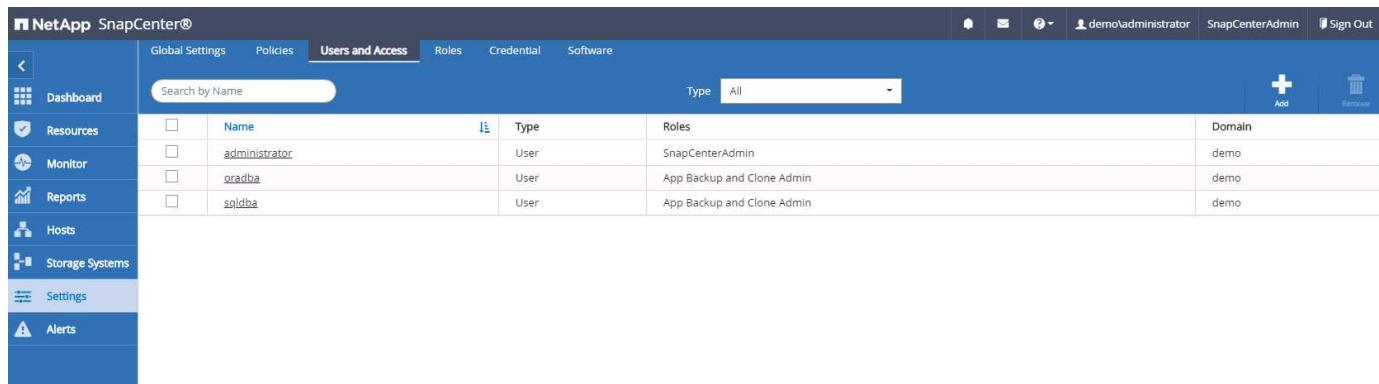
The NetApp SnapCenter tool uses role-based access control (RBAC) to manage user resources access and permission grants, and SnapCenter installation creates prepopulated roles. You can also create custom roles based on your needs or applications. It makes sense to have a dedicated admin user ID for each 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 have 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.

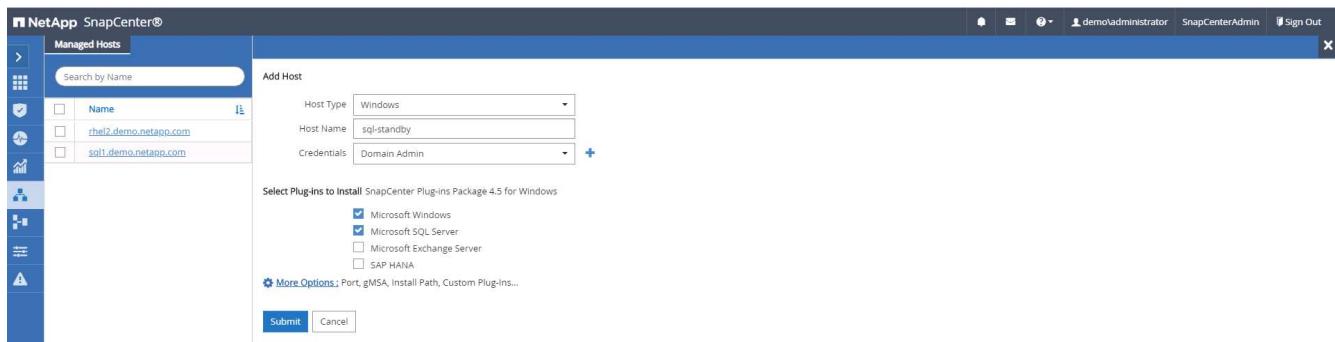
The following steps illustrate how a database host is added to SnapCenter while a SnapCenter plugin is installed on the host. The procedure applies to adding both on-premises hosts and cloud hosts. The following demonstration adds a Windows or a Linux host residing in AWS.

#### 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

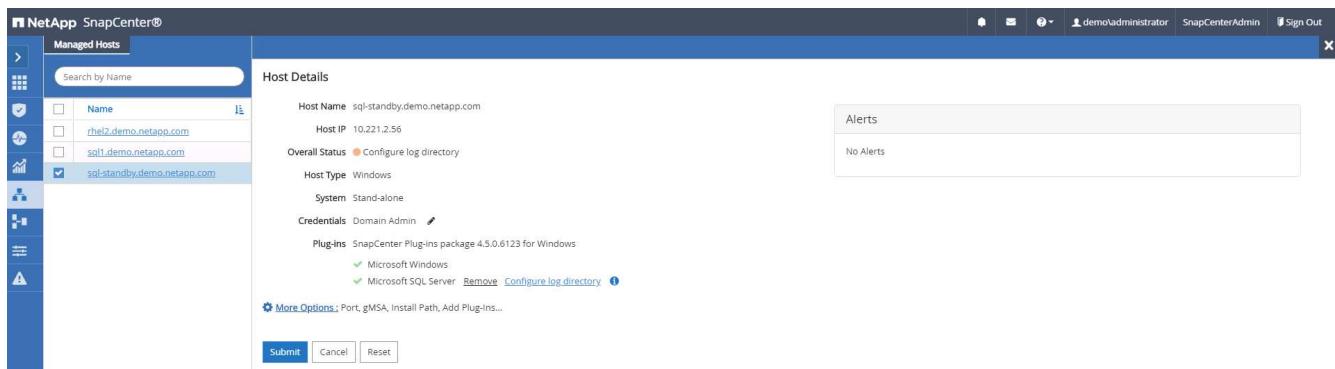
1. Log into SnapCenter with a user ID with SnapCenterAdmin privileges.
2. Click the Hosts tab from the left-hand menu, and then click Add to open the Add Host workflow.
3. Choose Windows for Host Type; the Host Name can be either a host name or an IP address. The host name must be resolved to the correct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



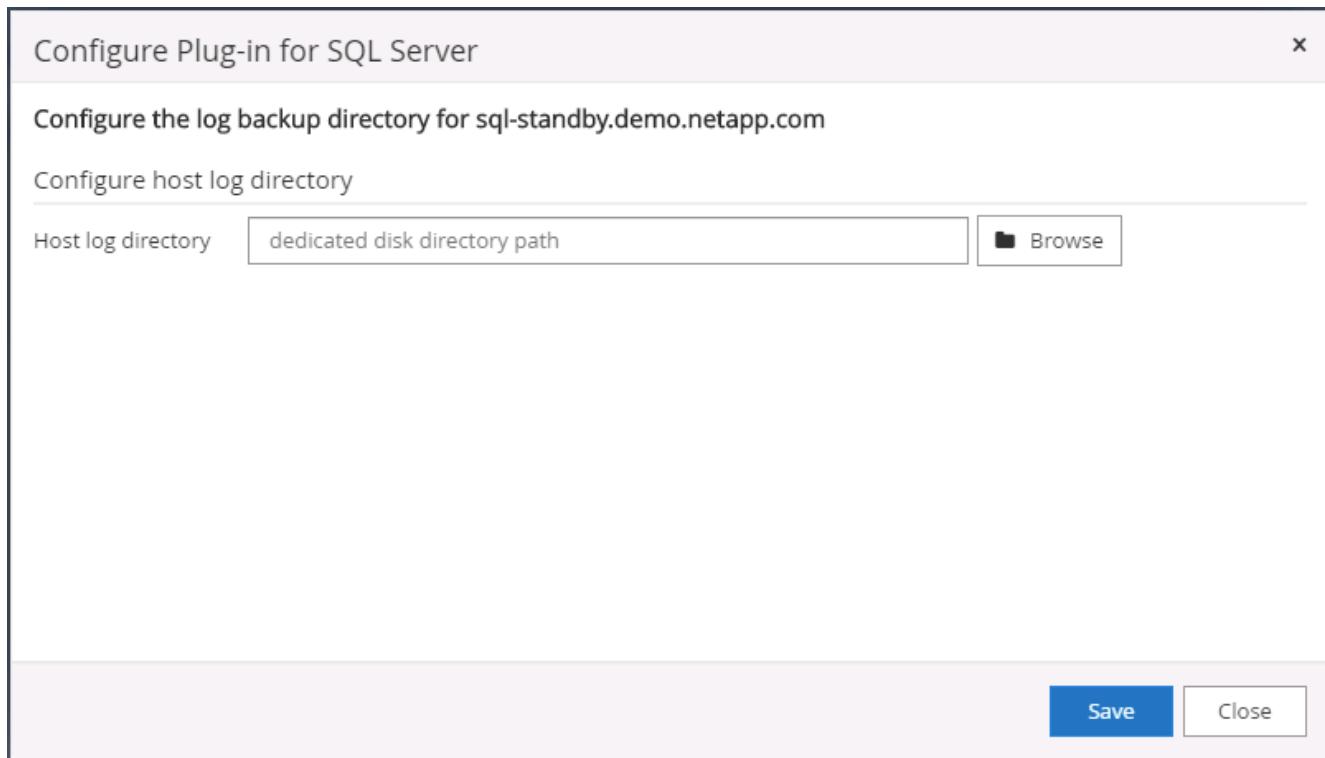
4. After the plugin is installed on a Windows host, its Overall Status is shown as "Configure log directory."

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

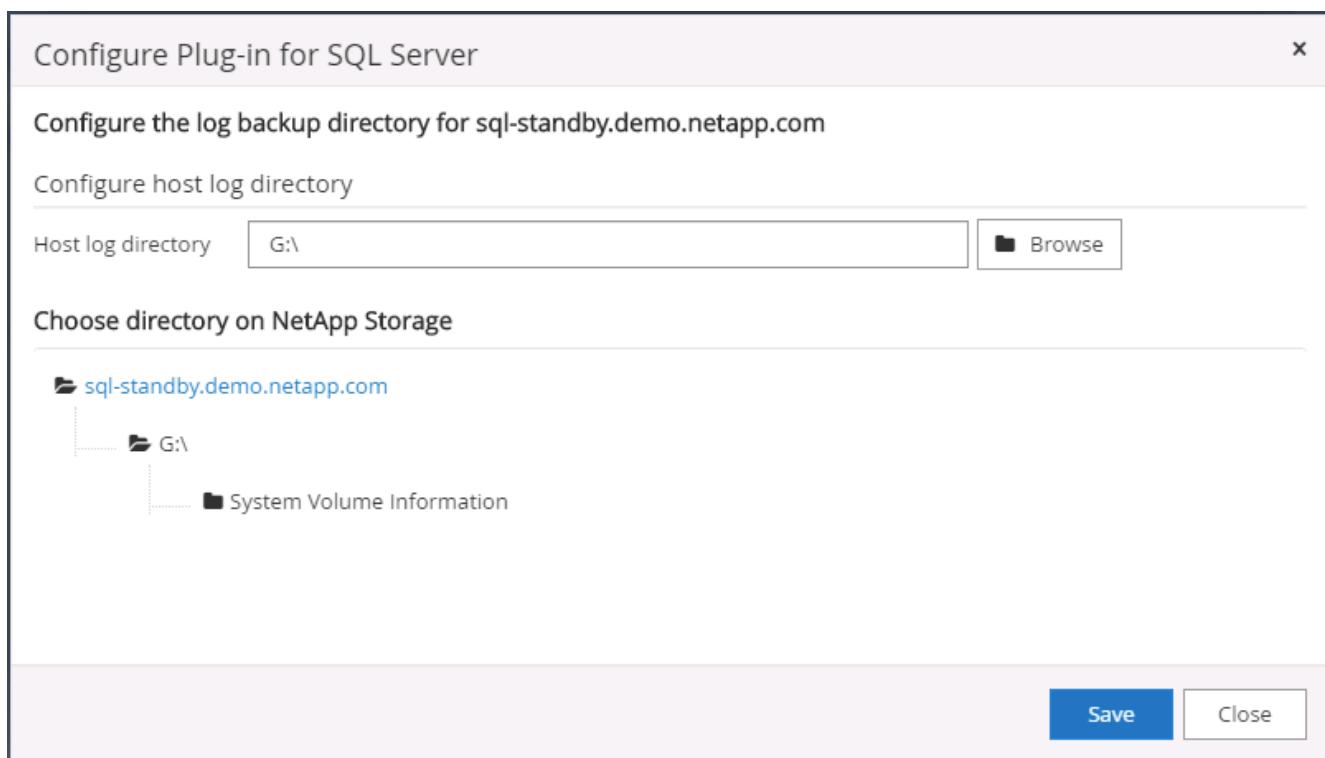
5. Click the Host Name to open the SQL Server log directory configuration.



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.

9. 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.

#### Add Unix 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 left-hand menu, and click Add to open the Add Host workflow.
3. 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**

4. 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**

5. 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	<b>i</b>	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.

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

#### 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.

Name	Oracle Database Type	Host/Cluster	Resource Group	Policies	Last Backup	Overall Status
cldb2	Single Instance (Multitenant)	rhel2.demo.netapp.com				Not protected

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.

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	09/14/2021 2:35:07 PM	Backup succeeded	User database

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.

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

Name	Name	Resource Group	Policy	Selectable
sql-standby	sql-standby	None	None	
sql1	sql1			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.

The screenshot shows the NetApp SnapCenter interface. The top navigation bar includes 'NetApp SnapCenter®', 'Microsoft SQL Server', 'View: Instance', 'Search by name', and user information 'demo\sqldba', 'App Backup and Clone Admin', and 'Sign Out'. The left sidebar has links for 'Dashboard', 'Resources', 'Monitor', 'Reports', 'Hosts', 'Storage Systems', 'Settings', and 'Alerts'. The main content area displays two instances: 'sql1' (Host: sql1.demo.netapp.com, State: Running, Type: Standalone (15.0.2000)) and 'sql-standby' (Host: sql-standby.demo.netapp.com, State: Running, Type: 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:

The screenshot shows the ONTAP System Manager interface under the 'NETWORK' tab. The left sidebar includes 'DASHBOARD', 'STORAGE', 'NETWORK', 'EVENTS & JOBS', 'PROTECTION', 'HOSTS', and 'CLUSTER'. The 'NETWORK' tab is selected. The main area shows 'IPSpaces' and 'Broadcast Domains' sections. In the 'Network Interfaces' section, three interfaces are listed: 'onPrem-01\_IC' (Status: green, Storage VM: Default, IPspace: Default, Address: 192.168.0.113, Current Node: onPrem-01, Current Port: e0b, Protocols: Cluster/Node Mgmt, Type: Intercluster), 'onPrem-01\_mgmt1' (Status: green, Storage VM: Default, IPspace: Default, Address: 192.168.0.111, Current Node: onPrem-01, Current Port: e0c, Protocols: Cluster/Node Mgmt, Type: Cluster/Node Mgmt), and 'cluster\_mgmt' (Status: green, Storage VM: Default, IPspace: Default, Address: 192.168.0.101, Current Node: onPrem-01, Current Port: e0a, Protocols: Cluster/Node Mgmt, Type: 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

2. 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:

3. 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

Applications

Volumes

LUNs

NVMe Namespaces

Shares

Qtrees

Quotas

Storage VMs

Tiers

**NETWORK**

Overview

Ethernet Ports

FC Ports

**EVENTS & JOBS**

**PROTECTION**

Overview

Relationships

**HOSTS**

**CLUSTER**

Overview

Settings

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  
Generate Passphrase  
Manage Cluster Peers

Storage VM Peers

PEERED STORAGE VMs  
✓ 1

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

ONTAP System Manager (Return to classic version)

Search actions, objects, and pages

Volumes

+ Add Delete Protect More

	Name
	rhel2_u03 All Volumes
	onPrem_data
	rhel2_u01
	rhel2_u02
<input checked="" type="checkbox"/>	<b>rhel2_u03</b>
	rhel2_u0309232119421203118
	sql1_data
	sql1_log
	sql1_snapctr
	svm_onPrem_root

Overview Snapshot Copies Clone Hierarchy SnapMirror (Local or Remote)

rhel2\_u03

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% 10% 20% 30% 40% 50%

SNAPSHOT CAPACITY: 0 Bytes Available | 2.36 GB Used | 2.36 GB Overflow

Performance

Hour Day Week

Latency

1.5 1

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

ONTAP System Manager (Return to classic version)

Search actions, objects, and pages

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

2 matching labels

VOLUME NAME

PREFIX: vol\_ <SourceVolumeName> \_dest

SUFFIX:

Override default storage service name

Configuration Details

Initialize relationship

Enable FabricPool

Save Cancel

6. 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. On the left, a list of volumes is shown with columns for Name and Status. A volume named 'rhe12\_u03' is selected. On the right, a detailed view for 'rhe12\_u03' is displayed under the 'SnapMirror (Local or Remote)' tab. It shows a table with columns for Source, Destination, Protection Policy, Relationship Health, Relationship Status, and Lag. The table data is as follows:

Source	Destination	Protection Policy	Relationship Health	Relationship Status	Lag
svm_onPrem:rhe12_u03	svm_hybridcvo:rhe12_u03_dr	MirrorAllSnapshots	Healthy	Mirrored	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. The 'Storage System' field is set to '10.0.0.1', 'Username' is 'admin', and 'Password' is '\*\*\*\*\*'. Below the fields are 'Event Management System (EMS) & AutoSupport Settings' with checkboxes for 'Send AutoSupport notification to storage system' and 'Log SnapCenter Server events to syslog'. A 'More Options' link is also present. 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. The 'Platform' dropdown is set to 'Cloud Volumes ONTAP'. The 'Secondary' checkbox is checked. The 'Protocol' dropdown is set to 'HTTPS', 'Port' is '443', and 'Timeout' is '60 seconds'. The 'Preferred IP' field is empty. 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](#).

Name	IP	Cluster Name	User Name	Platform	Controller License
svm_hybridcvo	10.0.0.1	10.0.0.1		CVO	No
svm_onPrem	192.168.0.101	192.168.0.101		CVO	Yes

## 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.

Name	Backup Type	Schedule Type	Replication	Verification
Oracle Archive Log Backup	LOG, ONLINE	Hourly	SnapMirror	
Oracle Full Online Backup	FULL, ONLINE	Daily	SnapMirror	

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

**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

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.

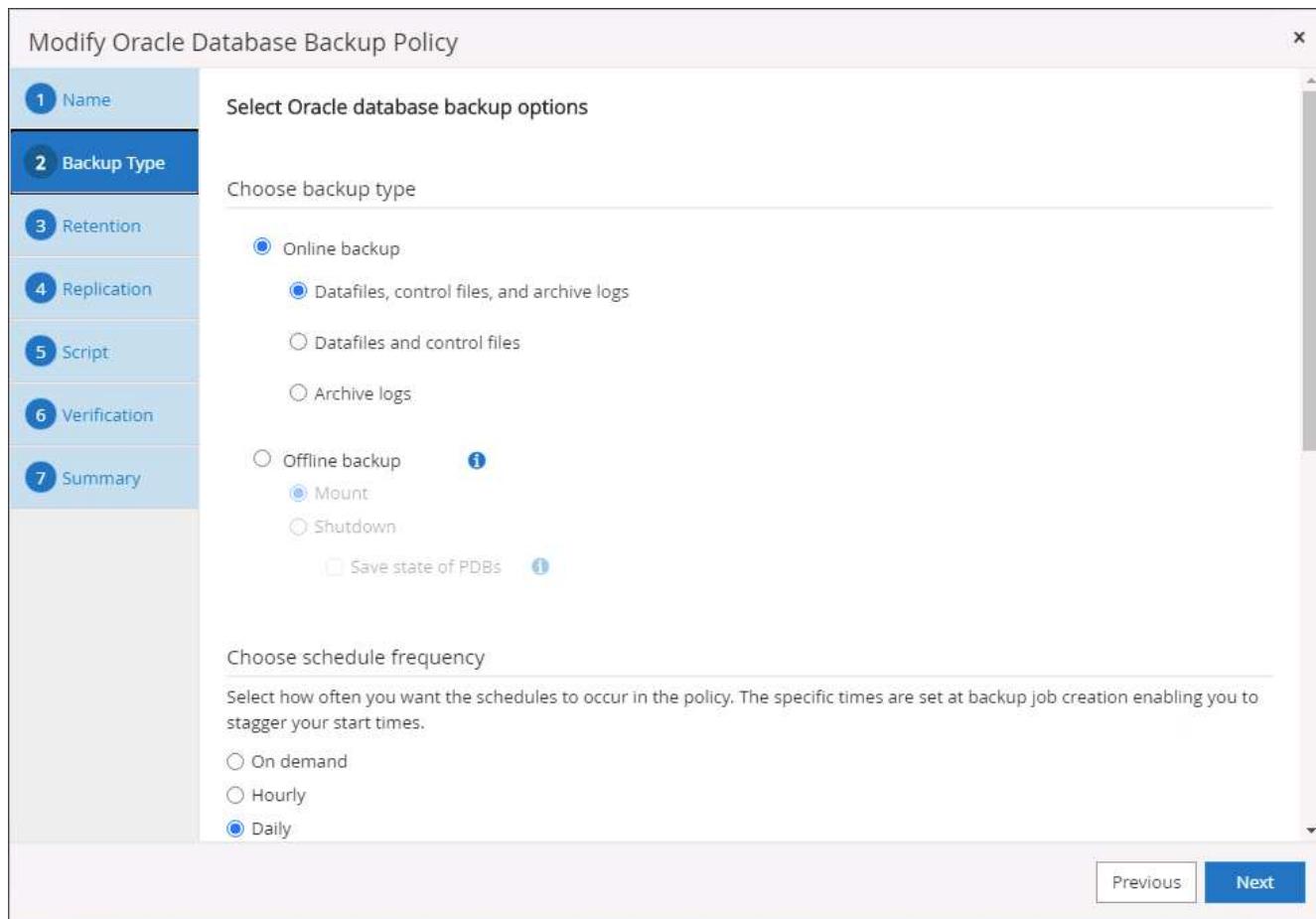
On demand

Hourly

Daily

Previous

Next



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

Modify Oracle Database Backup Policy

**1 Name**

**2 Backup Type**

**3 Retention**

**4 Replication**

**5 Script**

**6 Verification**

**7 Summary**

Retention settings i

Daily retention settings

Data backup retention settings i

Total Snapshot copies to keep

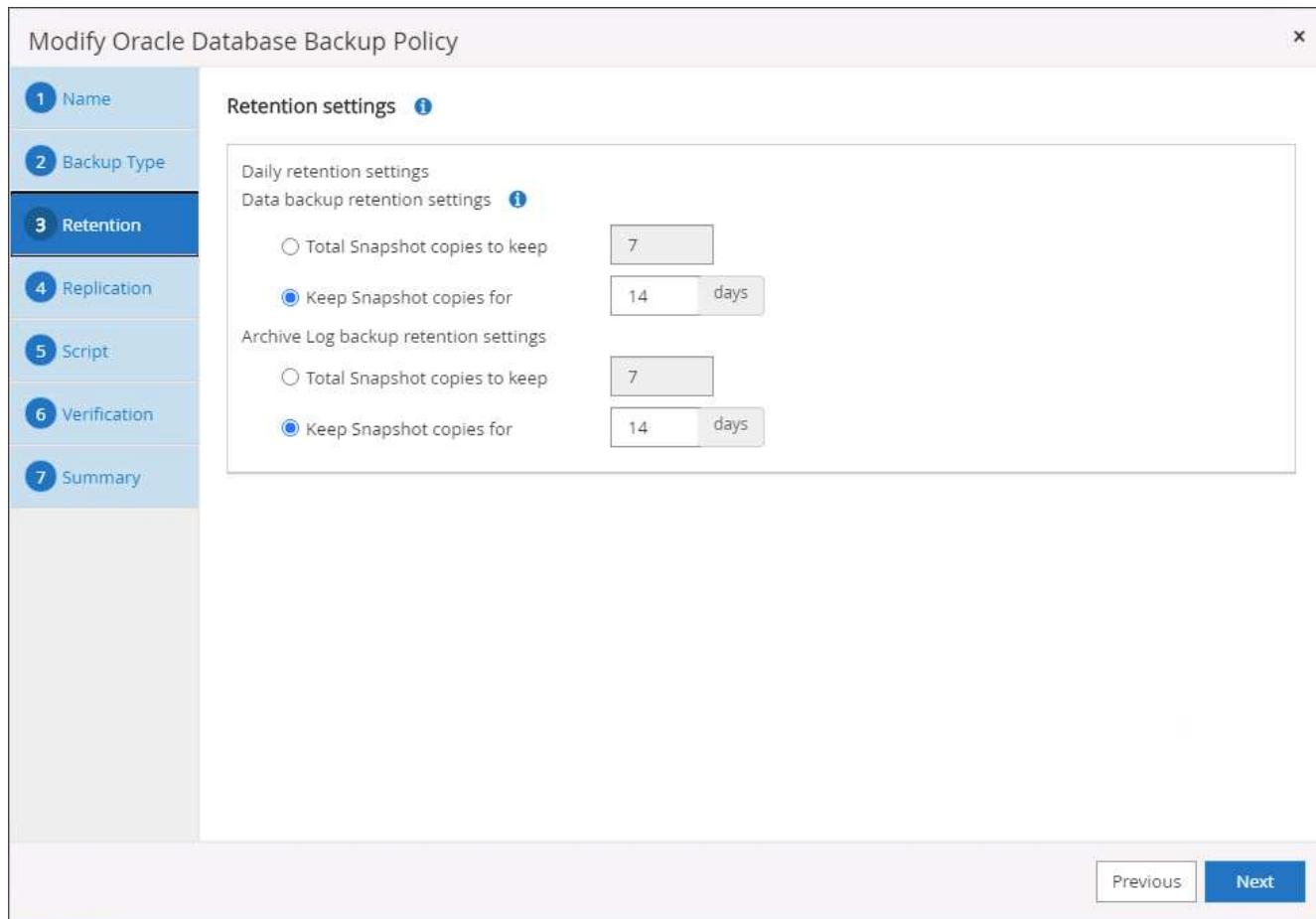
Keep Snapshot copies for  days

Archive Log backup retention settings

Total Snapshot copies to keep

Keep Snapshot copies for  days

Previous Next



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

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

2 Backup Type Prescript full path  Enter Prescript path

3 Retention Prescript arguments

4 Replication Postscript full path  Enter Postscript path

5 Script Postscript arguments

6 Verification Script timeout  secs

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

**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.

Daily

**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.

Modify Oracle Database Backup Policy X

1 Name	Summary
2 Backup Type	Policy name: Oracle Full Online Backup
3 Retention	Details: Backup all data and log files
4 Replication	Backup type: Online backup
5 Script	Schedule type: Daily
6 Verification	RMAN catalog backup: Disabled
7 Summary	Archive log pruning: None On demand data backup retention: None On demand archive log backup retention: None Hourly data backup retention: None Hourly archive log backup retention: None 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
<a href="#" style="border: 1px solid #ccc; padding: 2px 10px;">Previous</a> <span style="background-color: #0070C0; color: white; border: 1px solid #ccc; padding: 2px 10px; text-decoration: none; font-weight: bold;">Finish</span>	

#### 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**

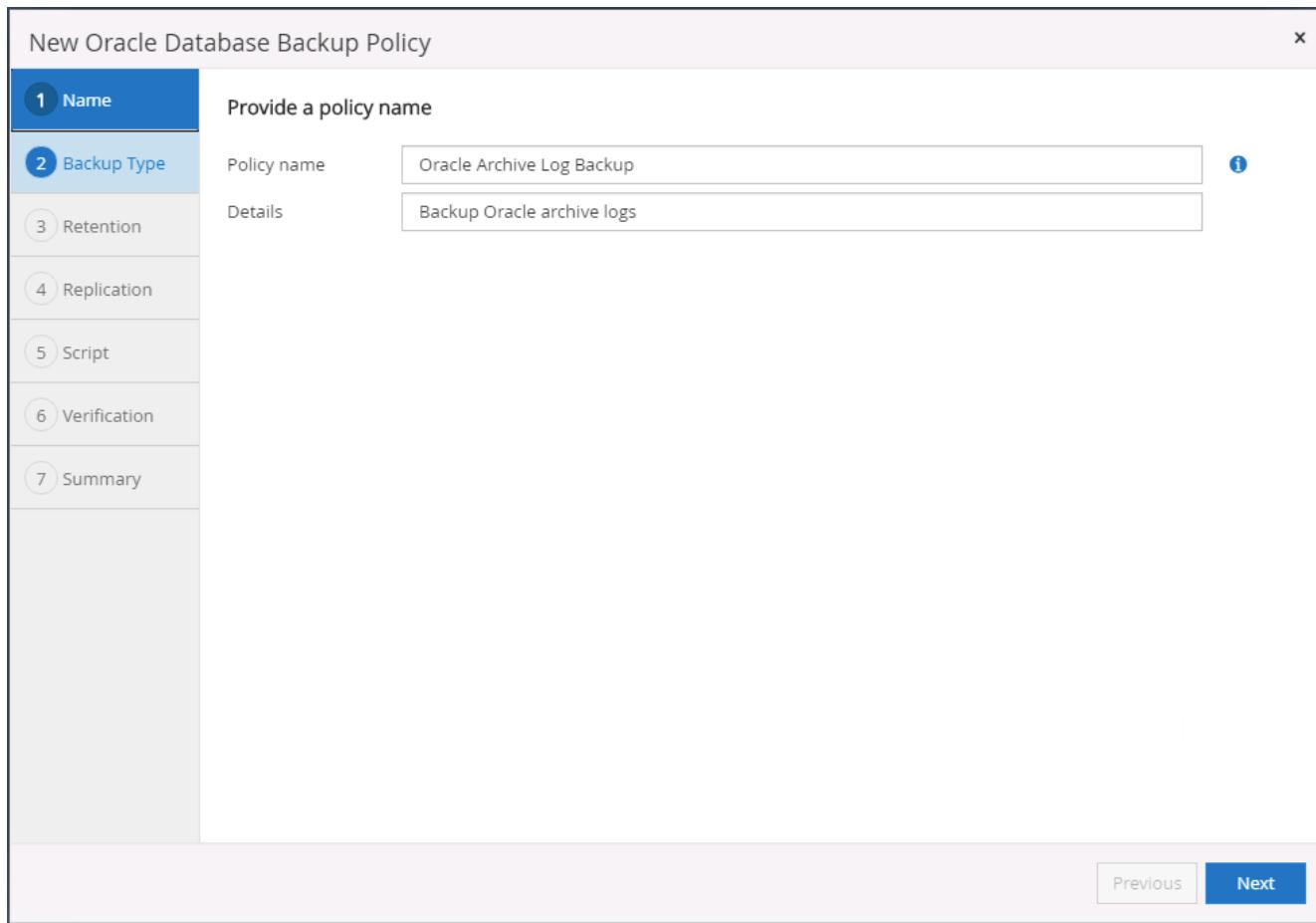
**4 Replication**

**5 Script**

**6 Verification**

**7 Summary**

Previous Next



3. Select the backup type and schedule frequency.

New Oracle Database Backup Policy X

**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.

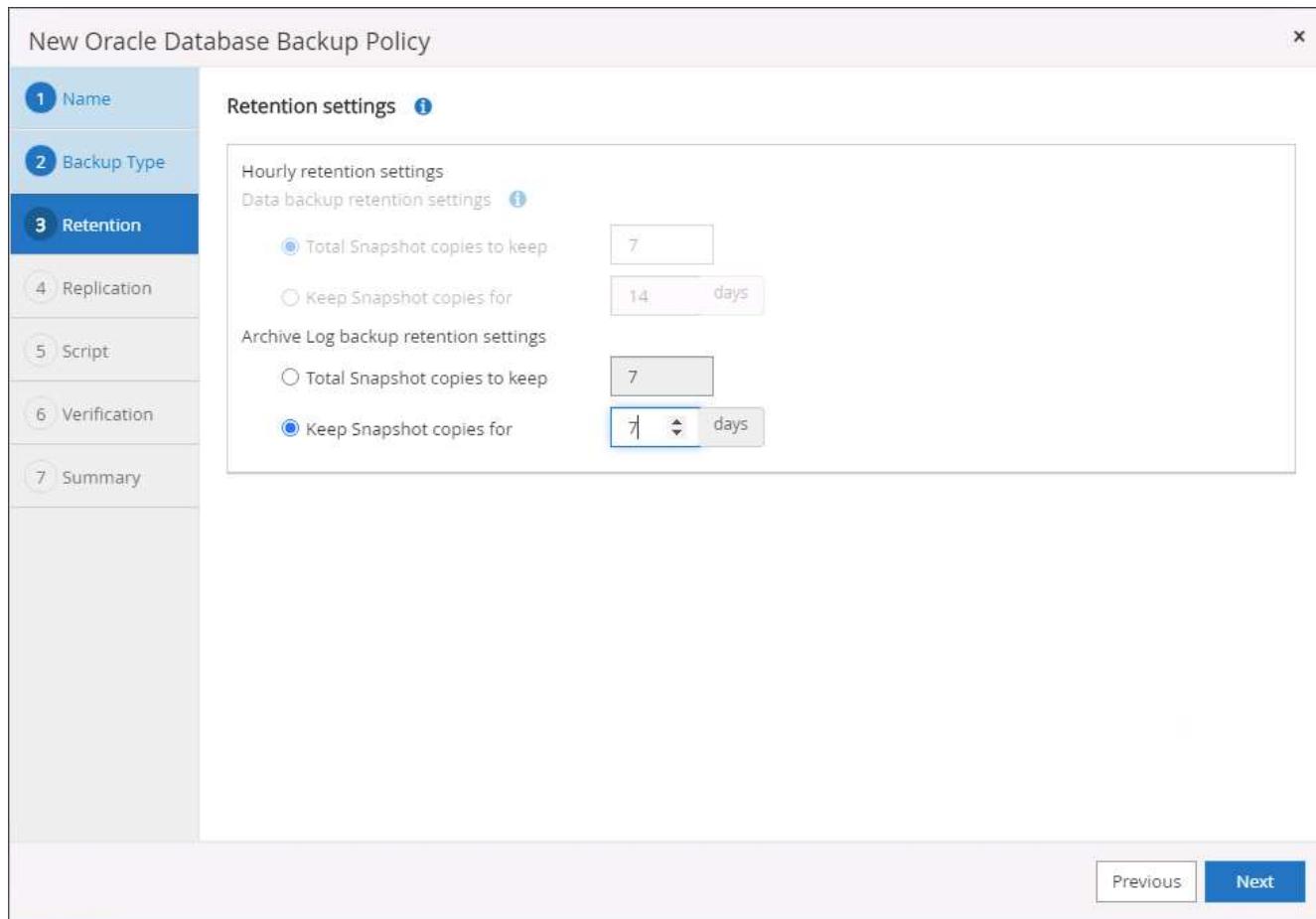
On demand

Hourly

Daily

Previous Next

4. Set the log retention period.



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

New Oracle Database Backup Policy

**1 Name**

**2 Backup Type**

**3 Retention**

**4 Replication**

**5 Script**

**6 Verification**

**7 Summary**

Select secondary replication options [i](#)

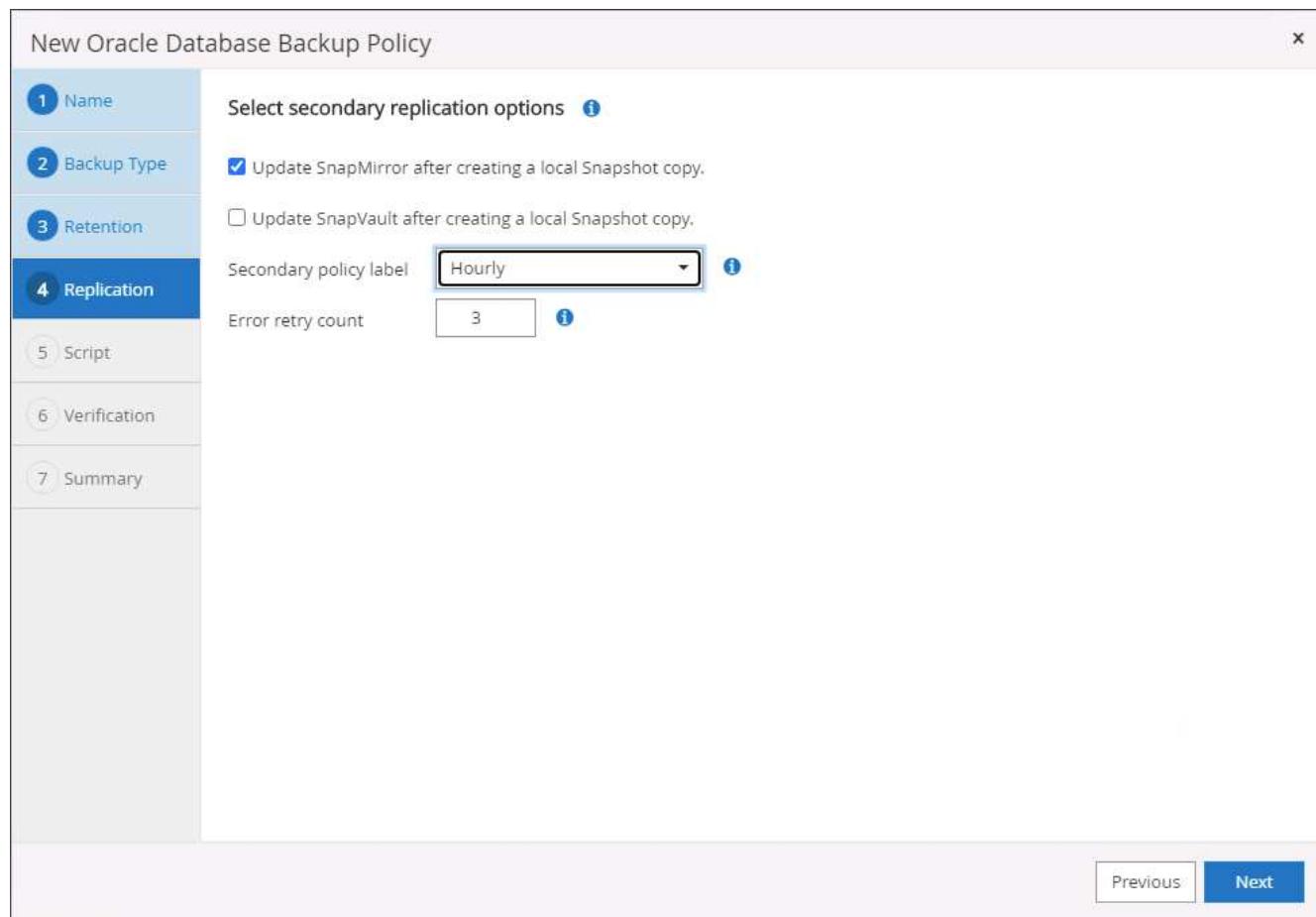
Update SnapMirror after creating a local Snapshot copy.

Update SnapVault after creating a local Snapshot copy.

Secondary policy label  [i](#)

Error retry count  [i](#)

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



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

New Oracle Database Backup Policy X

**1 Name**

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

**2 Backup Type**

Prescript full path  Enter Prescript path

**3 Retention**

Prescript arguments

**4 Replication**

Postscript full path  Enter Postscript path

**5 Script**

Postscript arguments

Script timeout  secs

**6 Verification**

**7 Summary**

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** Verification script commands

Script timeout 60 secs

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

Prescript arguments Choose optional arguments...

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

Postscript arguments Choose optional arguments...

8. Summary.

New Oracle Database Backup Policy

1 Name	Summary
2 Backup Type	Policy name: Oracle Archive Log Backup
3 Retention	Details: Backup Oracle archive logs
4 Replication	Backup type: Online backup
5 Script	Schedule type: Hourly
6 Verification	RMAN catalog backup: Disabled
7 Summary	Archive log pruning: None On demand data backup retention: None 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
<a href="#">Previous</a> <a href="#">Finish</a>	

### Create a full database backup policy for SQL

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

Name	Backup Type	Schedule Type	Replication
There is no match for your search or data is not available.			

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

New SQL Server Backup Policy X

**1 Name** Provide a policy name

**2 Backup Type**

**3 Retention**

**4 Replication**

**5 Script**

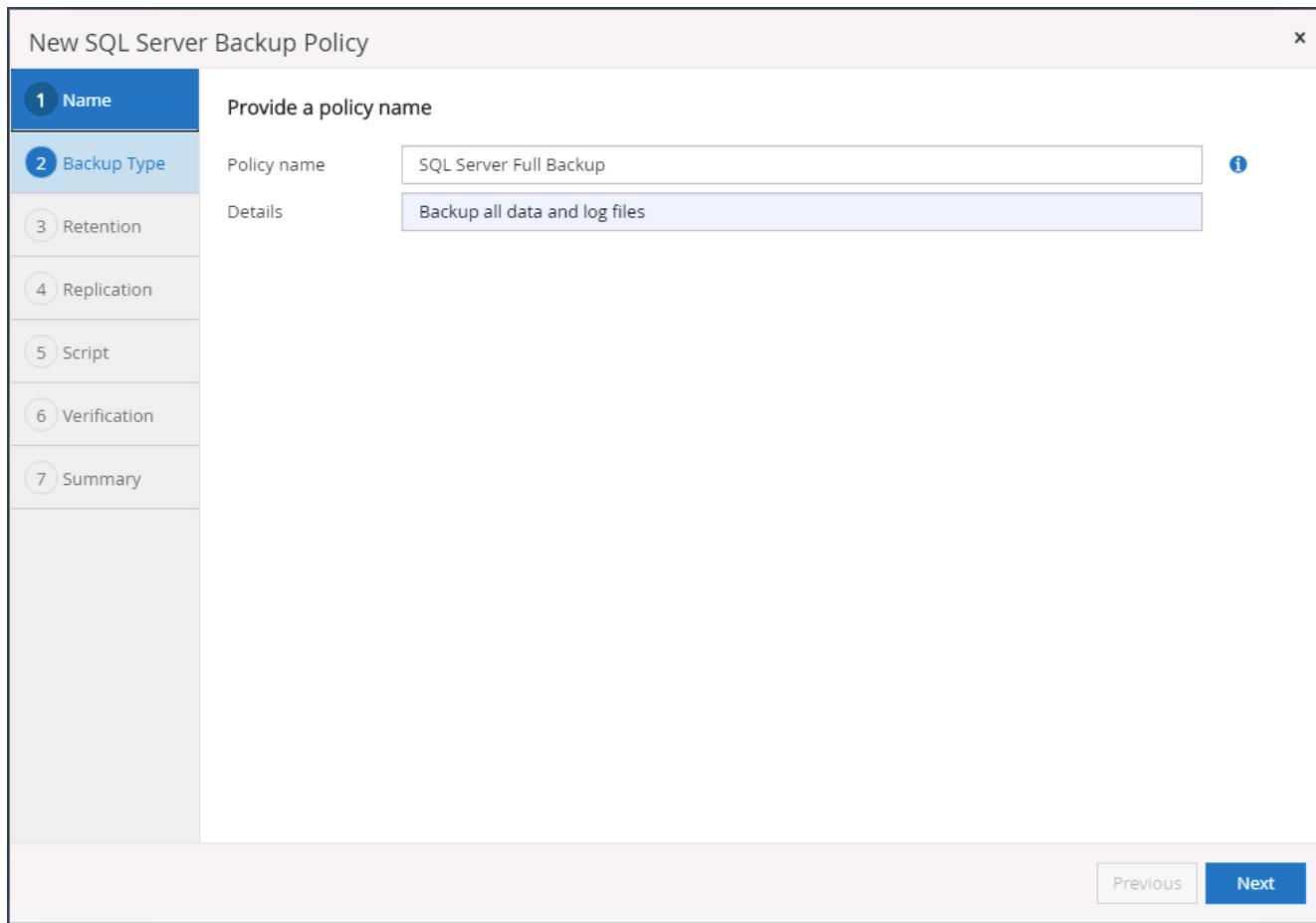
**6 Verification**

**7 Summary**

Policy name: SQL Server Full Backup i

Details: Backup all data and log files

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.

New SQL Server Backup Policy X

**1 Name**

**2 Backup Type**

**3 Retention** (selected)

**4 Replication**

**5 Script**

**6 Verification**

**7 Summary**

**Retention settings**

Retention settings for up-to-the-minute restore operation i

Keep log backups applicable to last 7 full backups

Keep log backups applicable to last 14 days

**Full backup retention settings** i

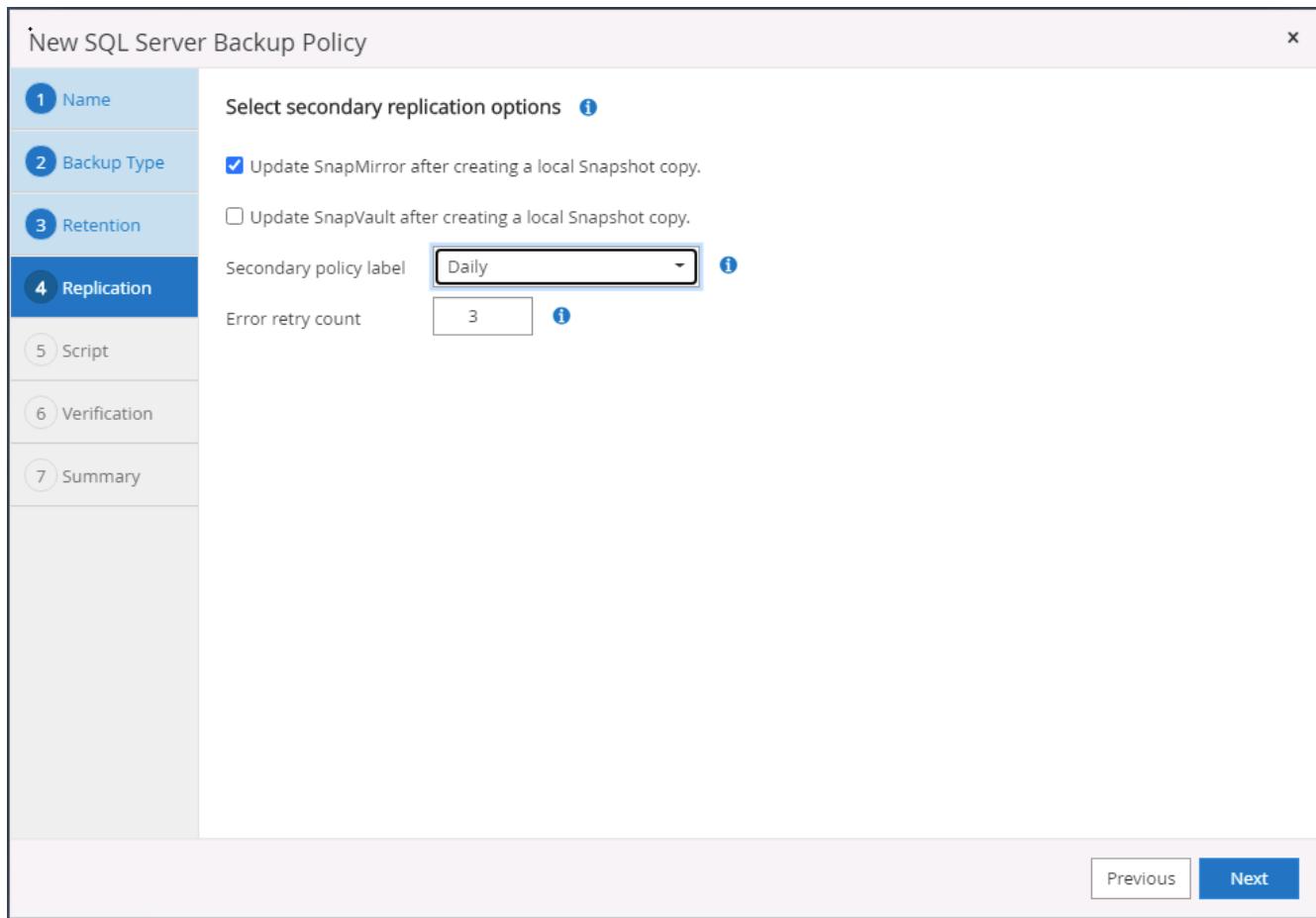
Daily

Total Snapshot copies to keep 7

Keep Snapshot copies for 14 days

Previous Next

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

Postscript full path

Postscript arguments  Choose optional arguments...

Script timeout  60  secs

**6 Verification**

**7 Summary**

Previous Next

7. Specify the options to run backup verification.

New SQL Server Backup Policy X

**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\_ERRORMSG)

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 60 secs

Previous Next

## 8. Summary.

New SQL Server Backup Policy
X

1 Name
Summary

2 Backup Type
Policy name: SQL Server Full Backup

3 Retention
Details: Backup all data and log files

4 Replication
Backup type: Full backup and log backup

5 Script
Availability group settings: Backup only on preferred backup replica

6 Verification
Schedule Type: Daily

7 Summary
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 X

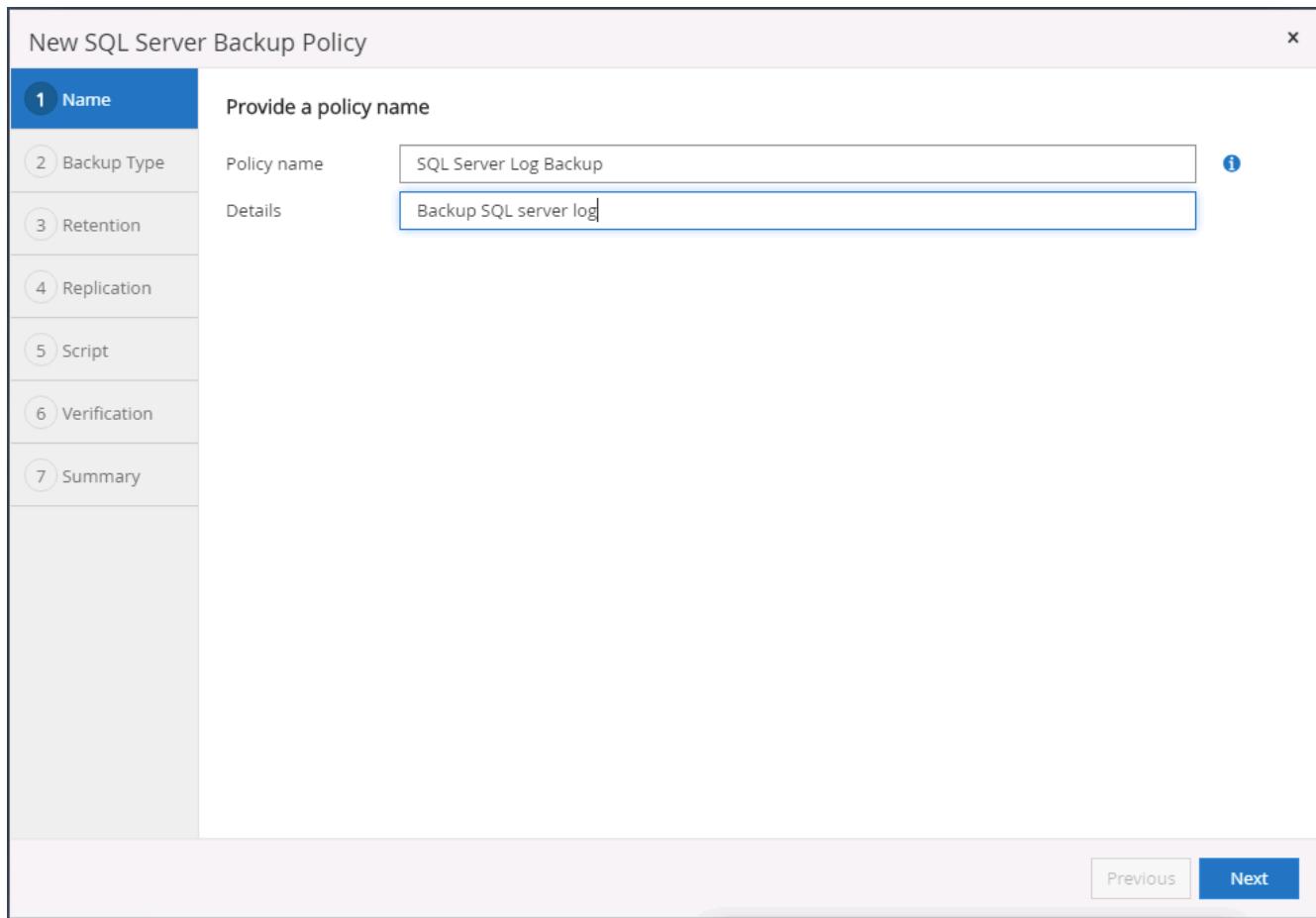
1 Name 2 Backup Type 3 Retention 4 Replication 5 Script 6 Verification 7 Summary

Provide a policy name

Policy name: SQL Server Log Backup i

Details: Backup SQL server log

Previous Next



2. 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.

New SQL Server Backup Policy X

**1 Name**

**2 Backup Type**

**3 Retention**

**4 Replication**

**5 Script**

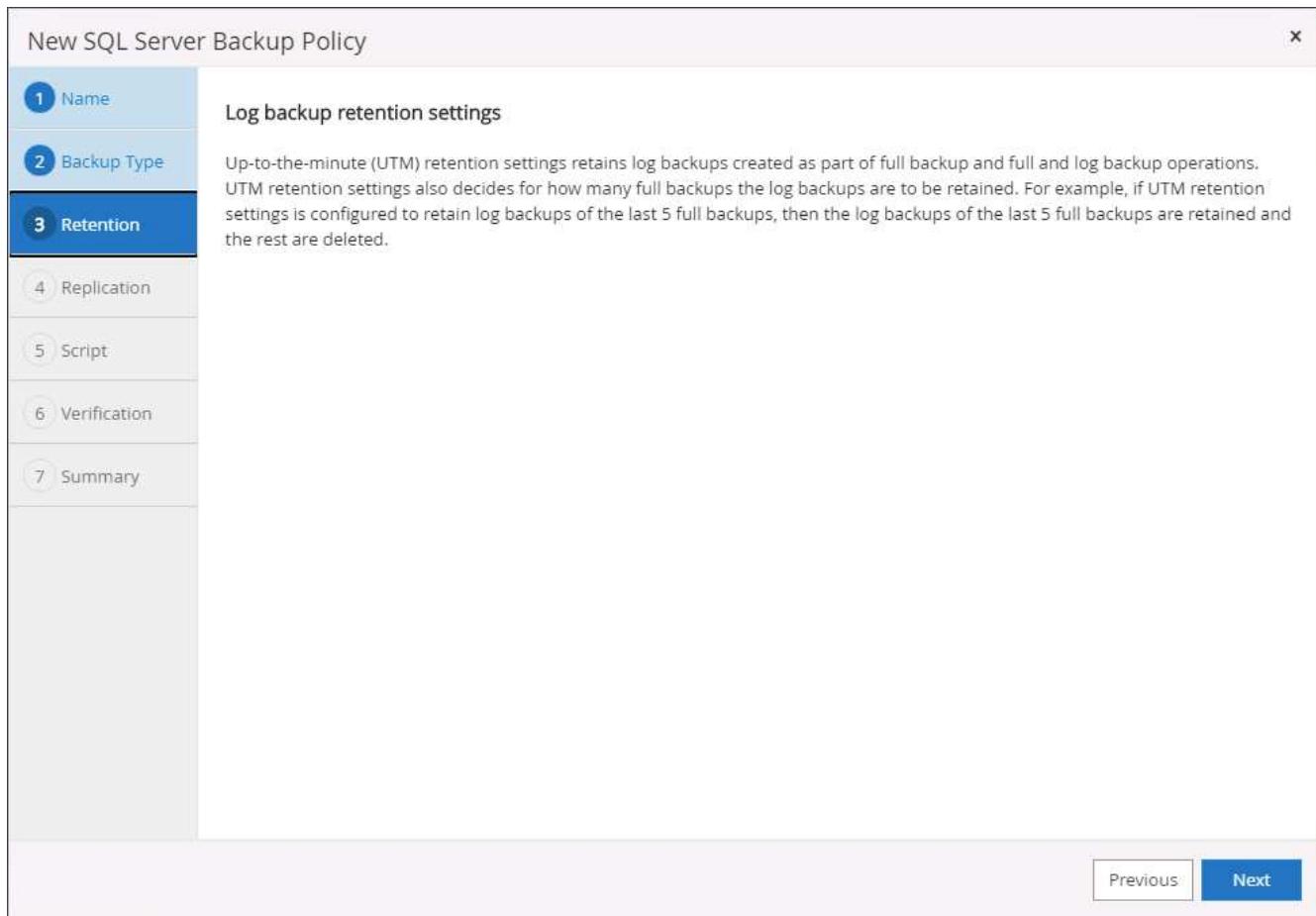
**6 Verification**

**7 Summary**

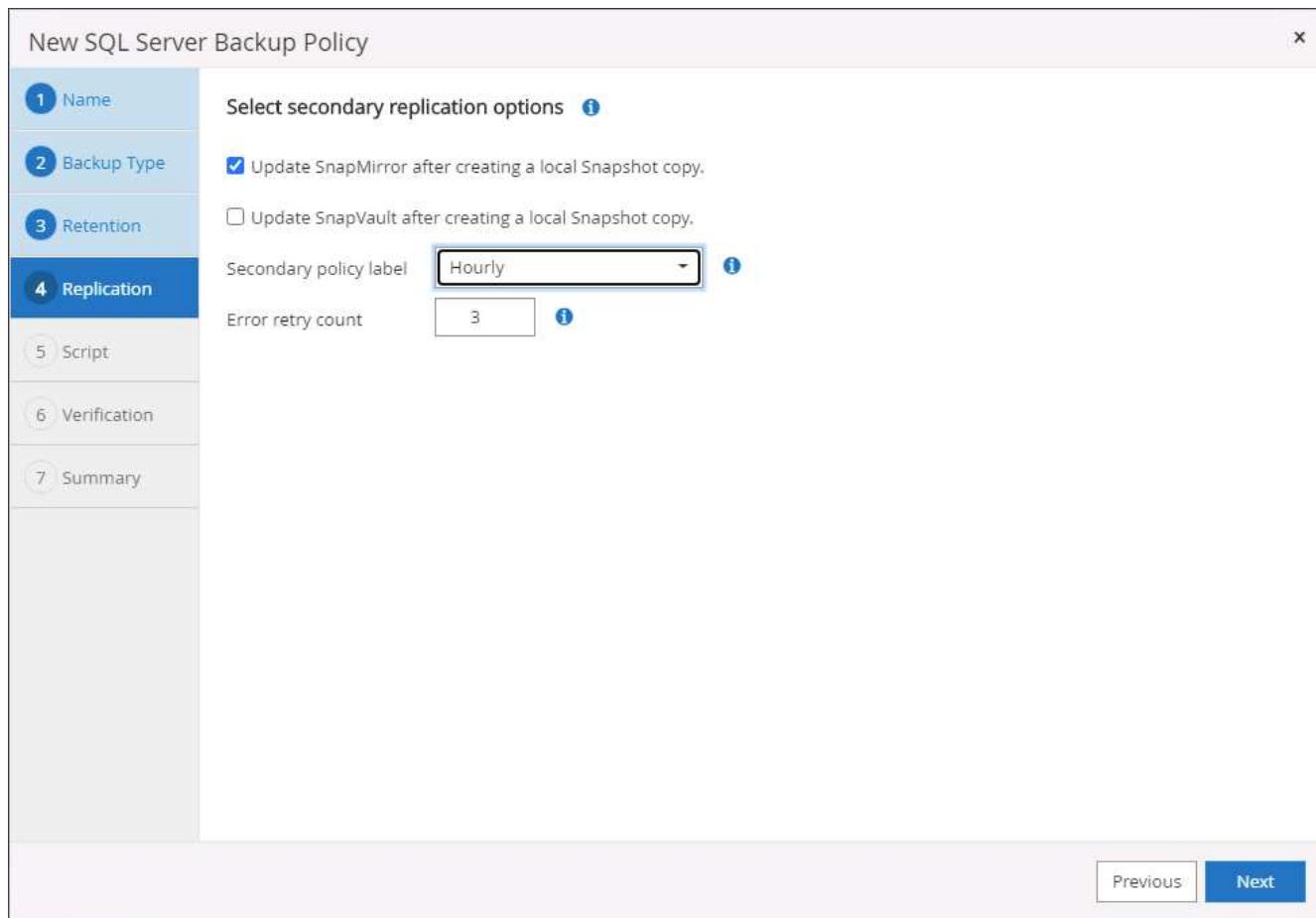
**Log backup retention settings**

Up-to-the-minute (UTM) retention settings retains log backups created as part of full backup and full and log backup operations. UTM retention settings also decides for how many full backups the log backups are to be retained. For example, if UTM retention settings is configured to retain log backups of the last 5 full backups, then the log backups of the last 5 full backups are retained and the rest are deleted.

Previous Next



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

1 Name	Summary
2 Backup Type	Policy name: SQL Server Log Backup
3 Retention	Details: Backup SQL server log
4 Replication	Backup type: Log transaction backup
5 Script	Availability group settings: Backup only on preferred backup replica
6 Verification	Schedule Type: Hourly
7 Summary	Replication: SnapMirror enabled, Secondary policy label: Hourly, 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

## 8. Implement backup policy to protect database

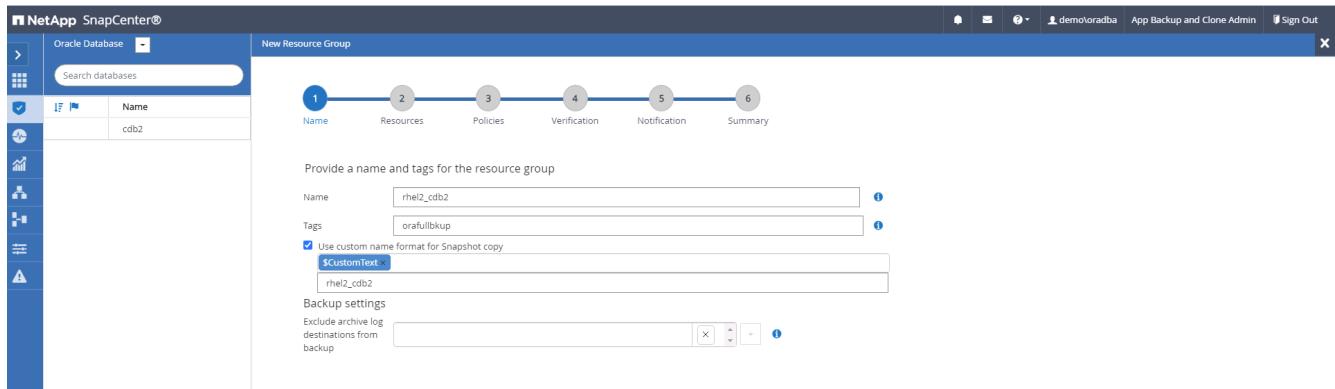
SnapCenter uses a resource group to backup a database in a logical grouping of database resources, such as multiple databases hosted on a server, a database sharing the same storage volumes, multiple databases supporting a business application, and so on. Protecting a single database creates a resource 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

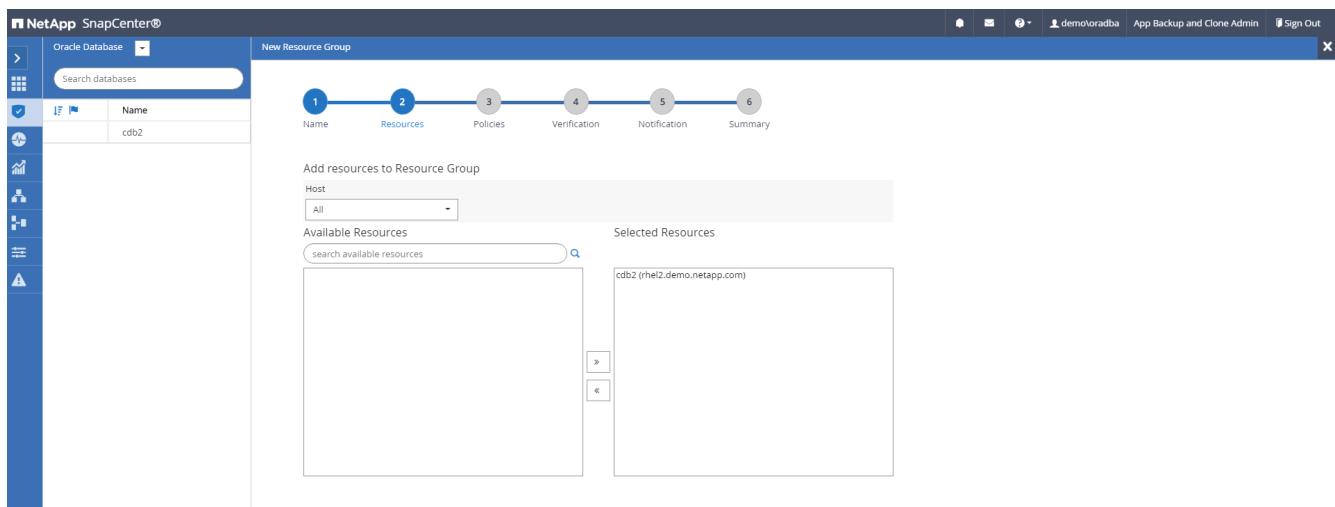
1. Log into SnapCenter with a database management user ID, and navigate to the Resources tab. In the View drop-down list, choose either Database or Resource Group to launch the resource group creation workflow.

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

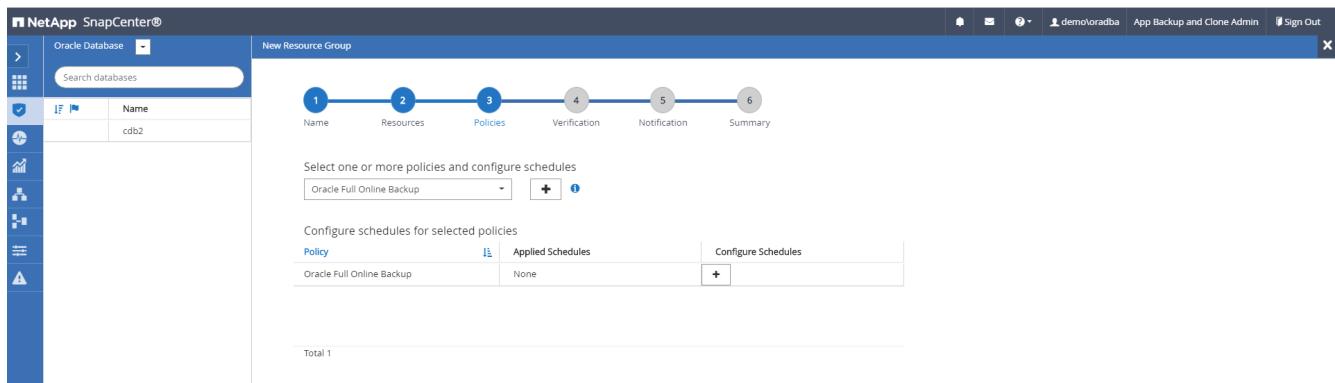
2. Provide a name and tags for the resource group. You can define a naming format for the Snapshot copy and bypass the redundant archive log destination if configured.



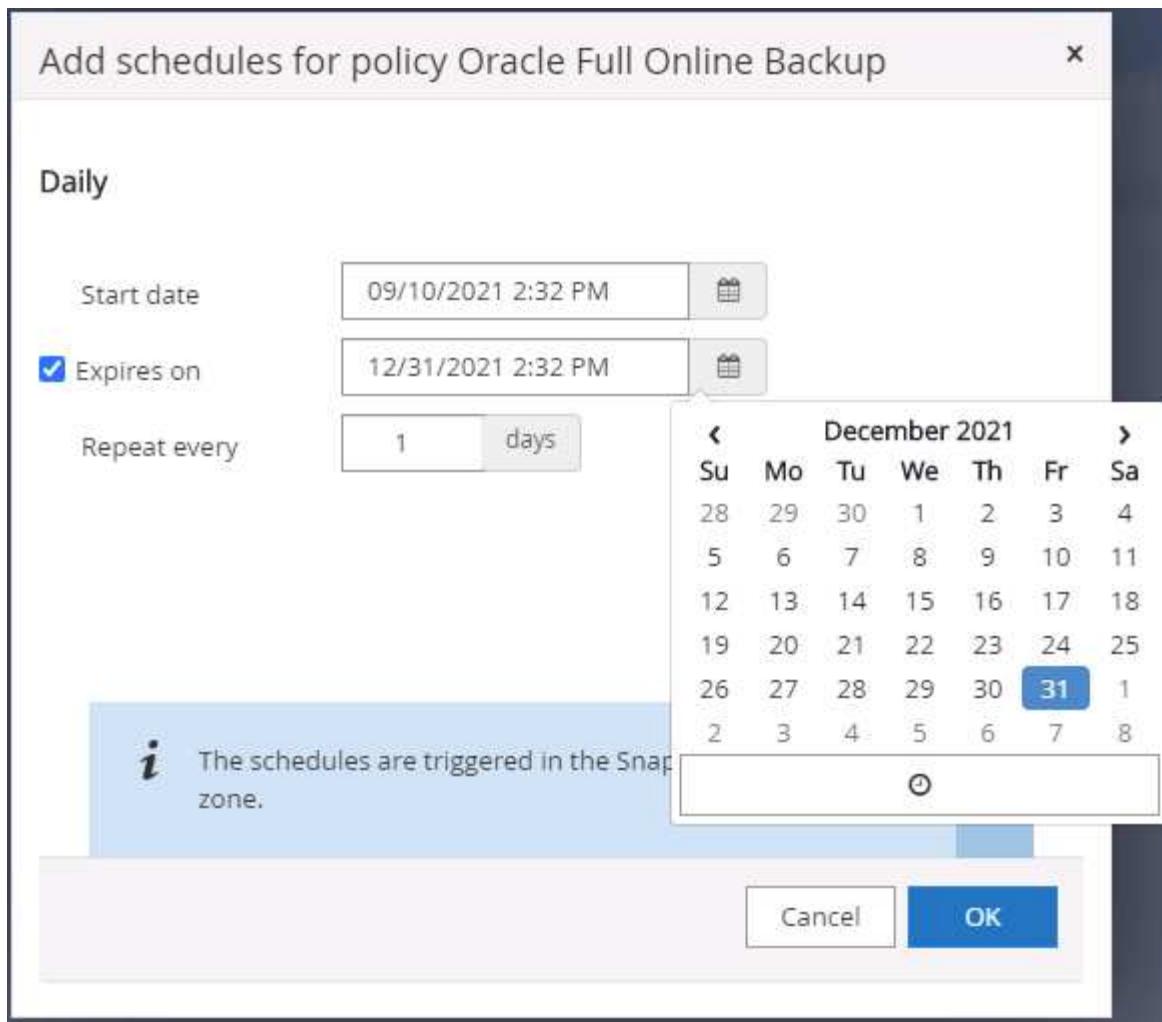
### 3. Add database resources to the resource group.



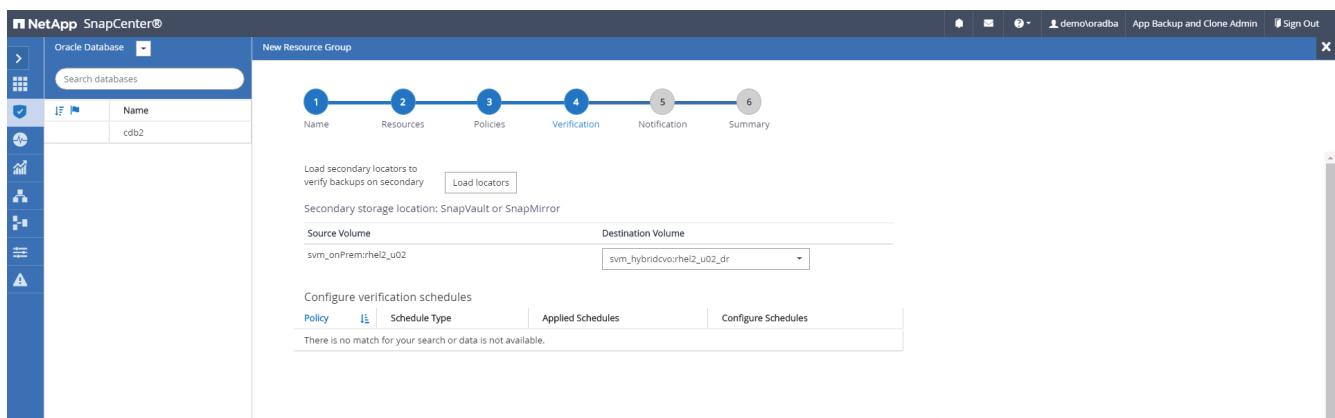
### 4. Select a full backup policy created in section 7 from the drop-down list.



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



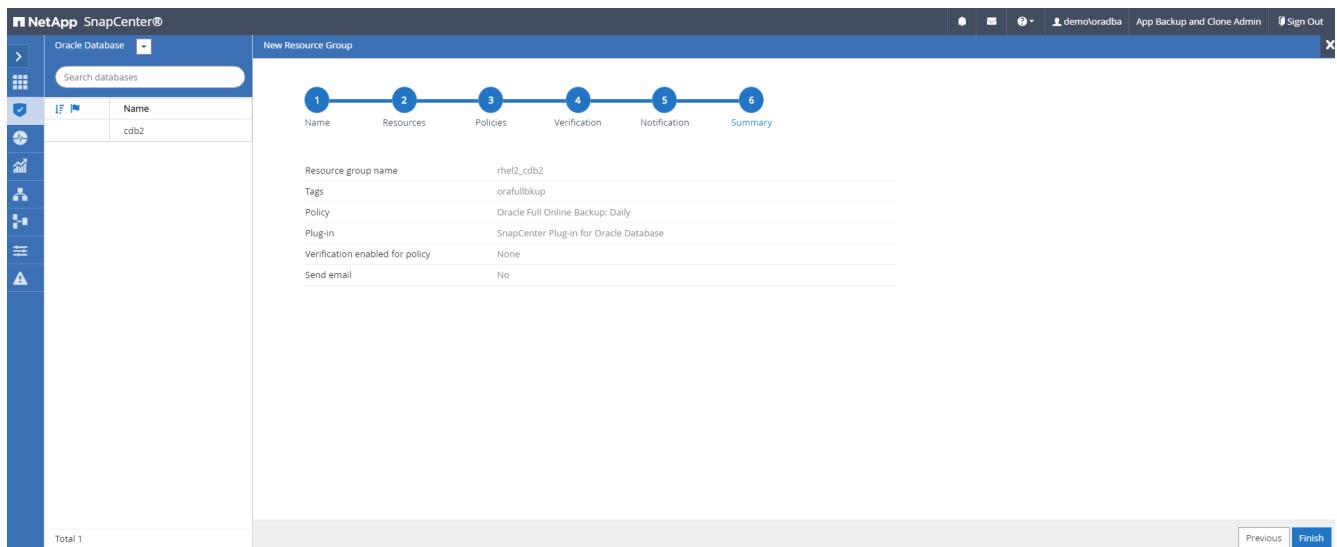
6. Click Load Locators to load the source and destination volume.



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

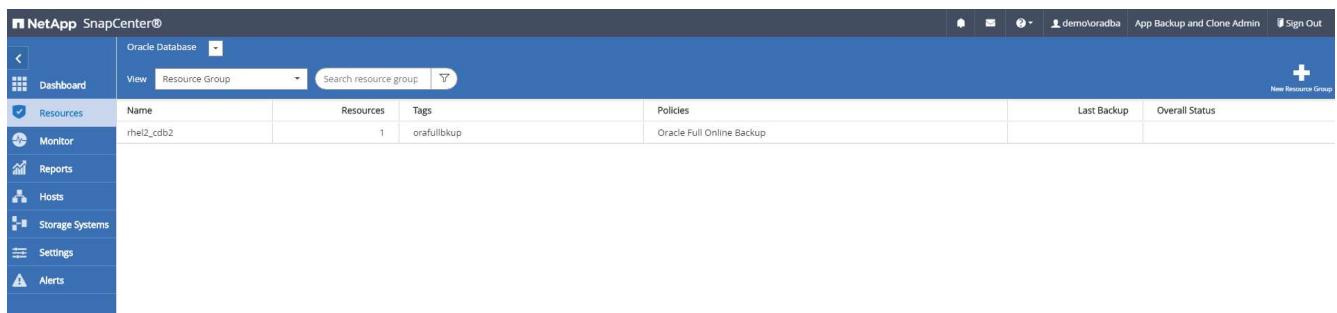


## 8. Summary.

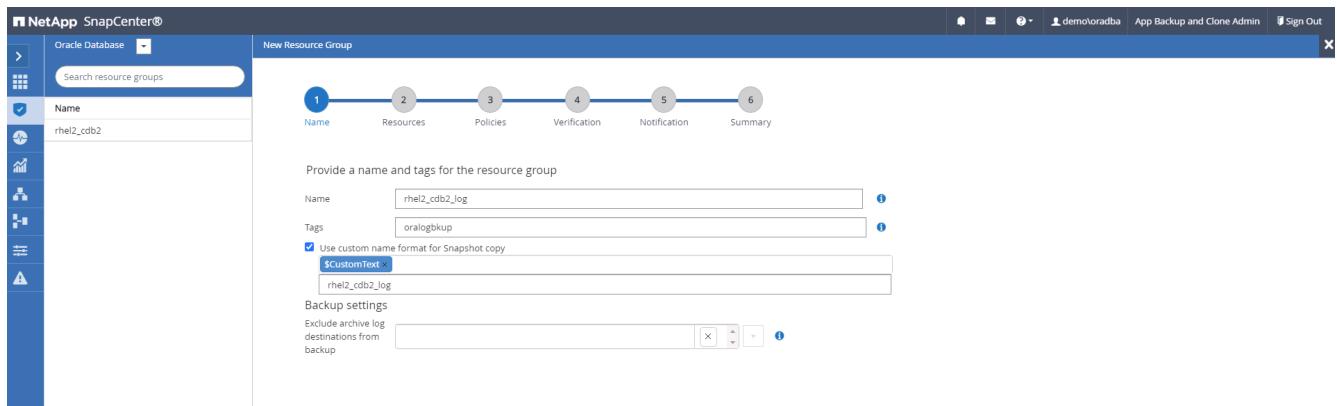


### Create a resource group for log backup of Oracle

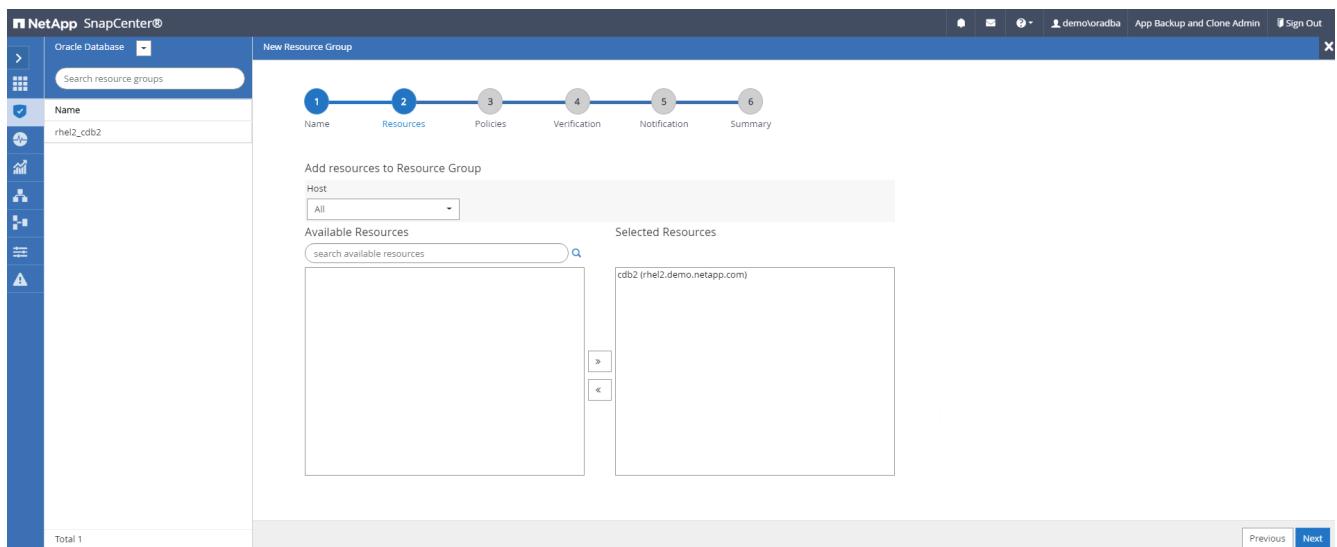
1. Log into SnapCenter with a database management user ID, and navigate to the Resources tab. In the View drop-down list, choose either Database or Resource Group to launch the resource group creation workflow.



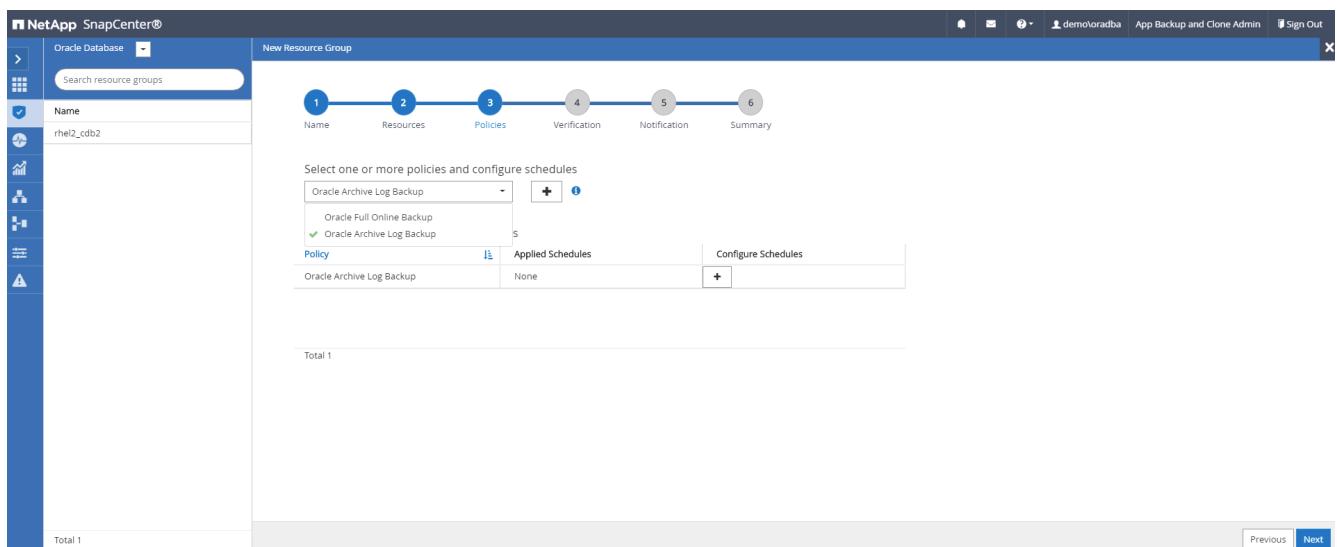
2. Provide a name and tags for the resource group. You can define a naming format for the Snapshot copy and bypass the redundant archive log destination if configured.



### 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

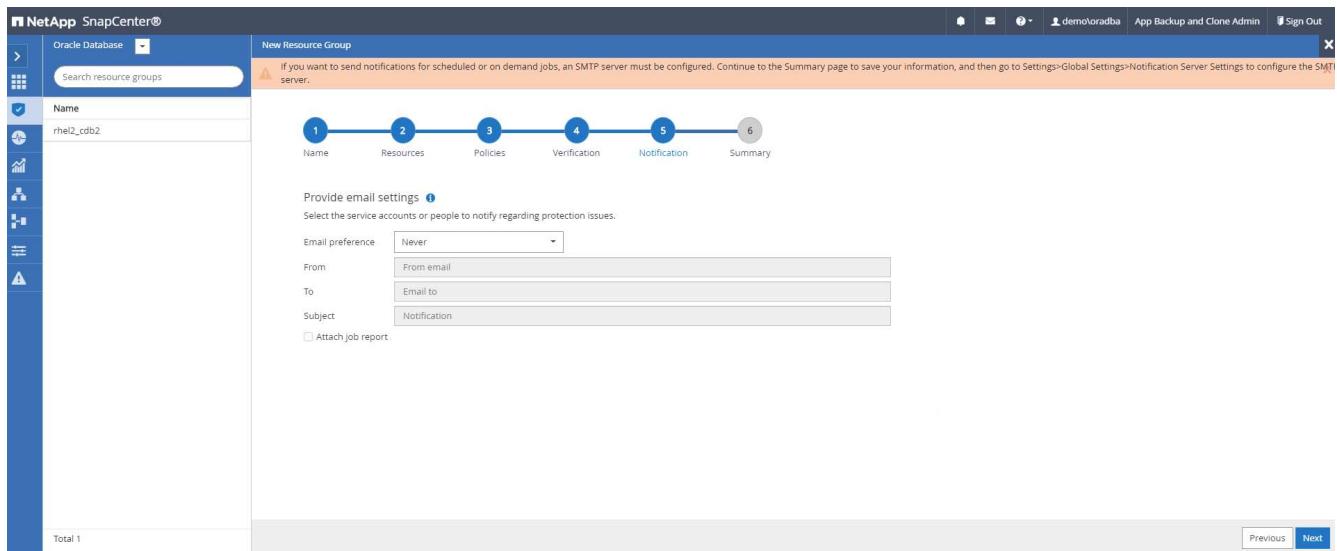
Policy   Schedule Type   Applied Schedules   Configure Schedules

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

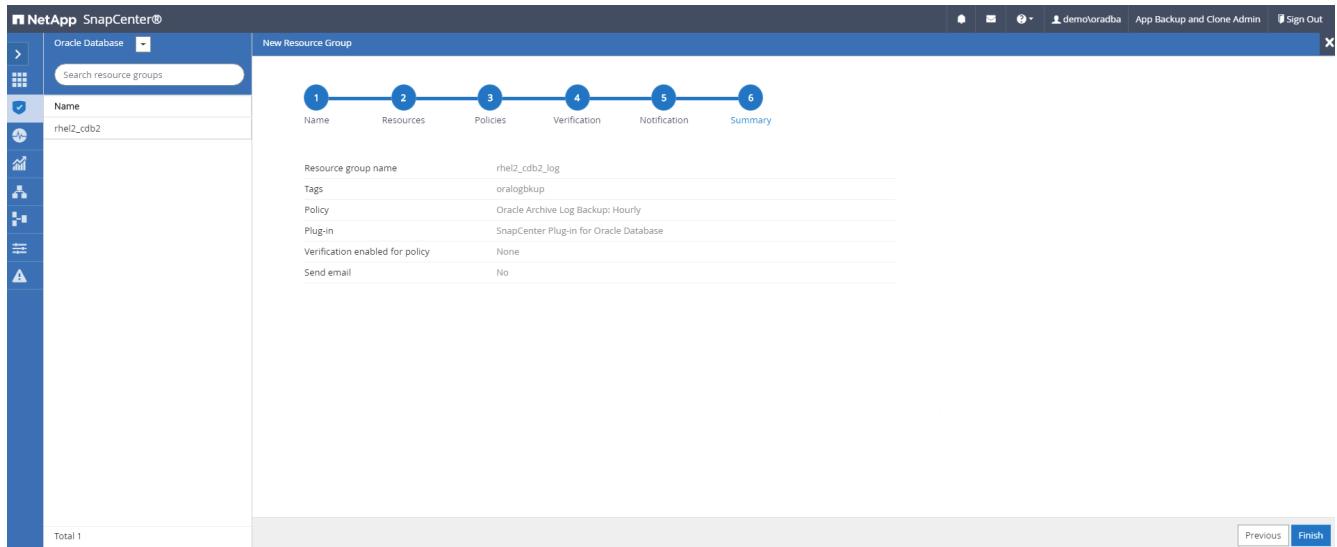
Total 0

Previous Next

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

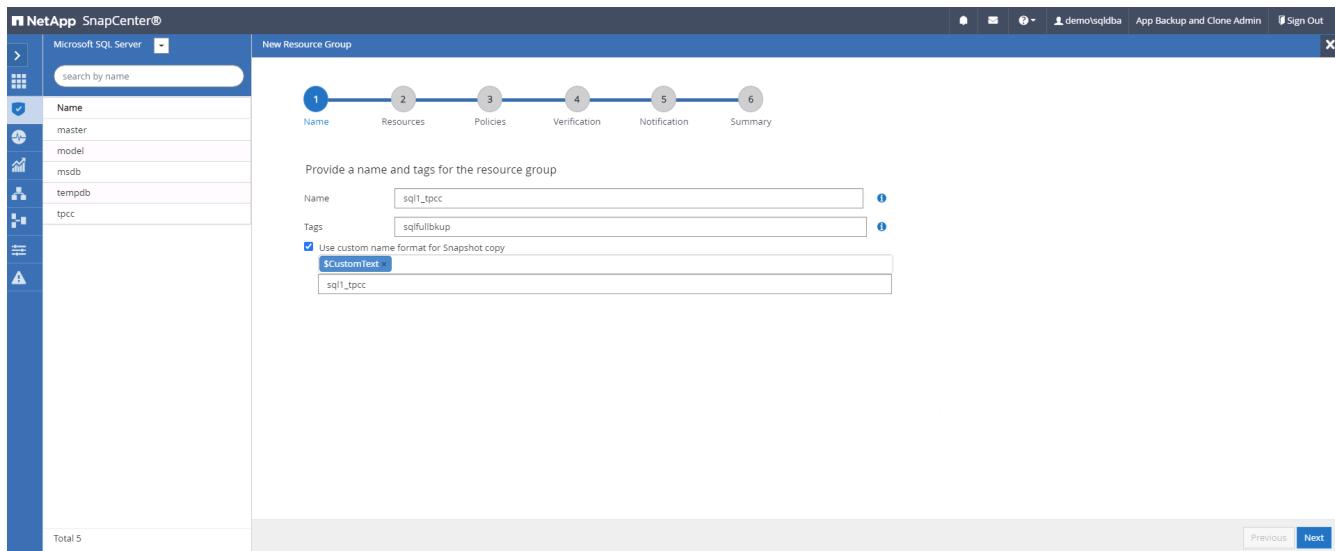


## 8. Summary.



## 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.



NetApp SnapCenter®

Microsoft SQL Server

search by name

Name

master

model

msdb

tempdb

tpcc

Total 5

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

Provide a name and tags for the resource group

Name: sql1\_tpcc

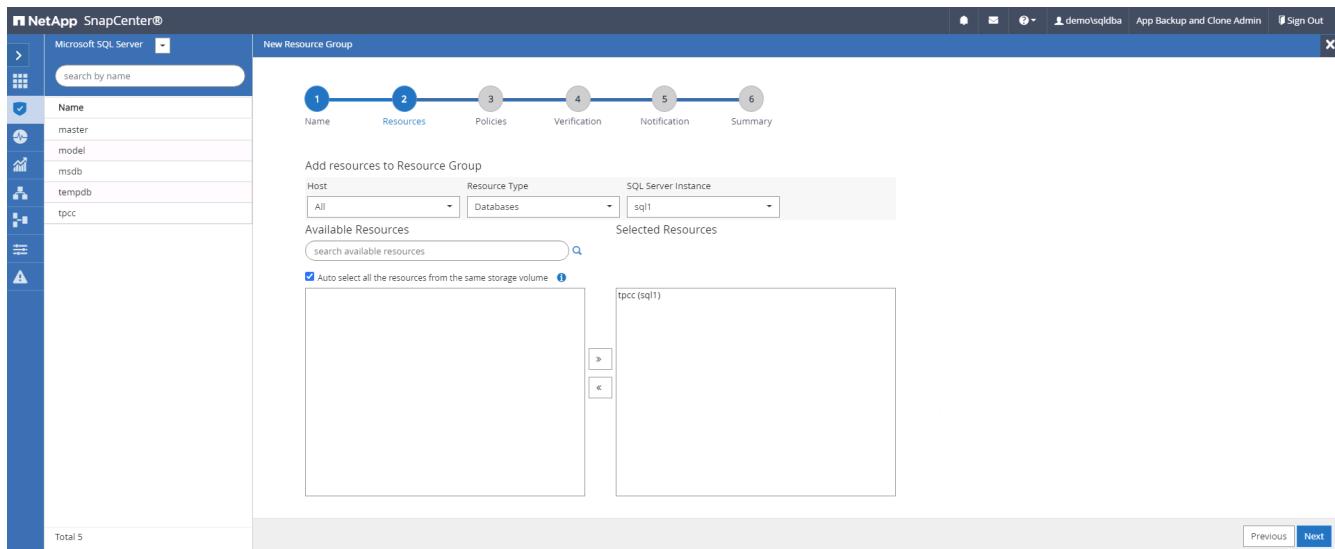
Tags: sqfullbkup

Use custom name format for Snapshot copy

\$CustomText: \$sql1\_tpcc

Previous Next

## 2. Select the database resources to be backed up.



NetApp SnapCenter®

Microsoft SQL Server

search by name

Name

master

model

msdb

tempdb

tpcc

Total 5

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

Add resources to Resource Group

Host: All Resource Type: Databases SQL Server Instance: sql1

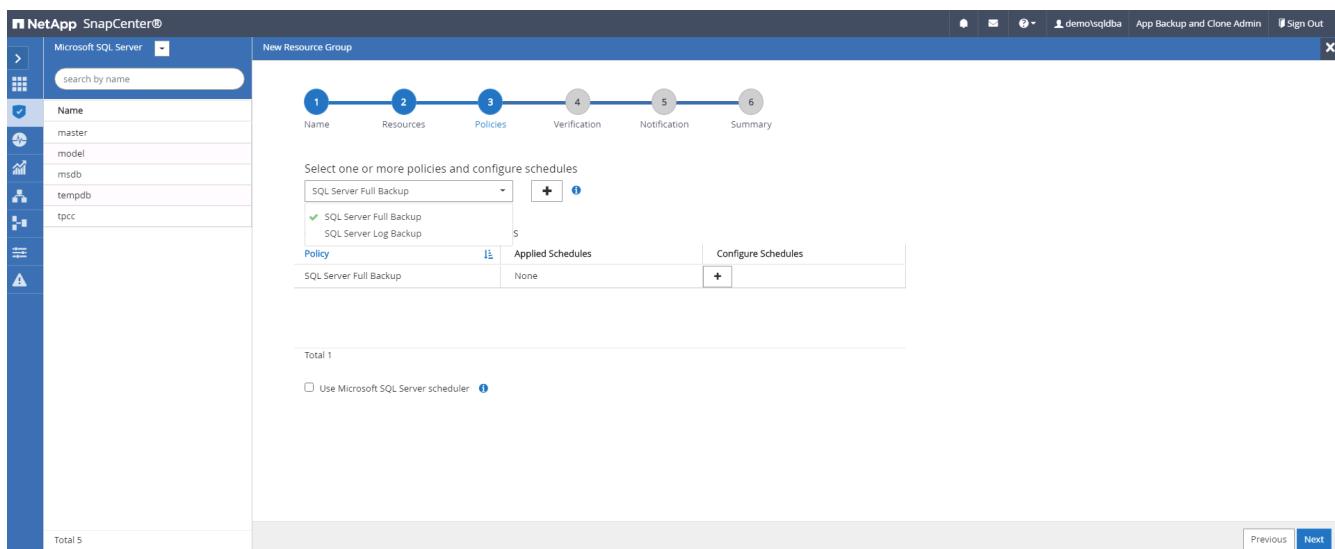
Available Resources: search available resources

Selected Resources: tpcc (sql1)

Auto select all the resources from the same storage volume

Previous Next

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



NetApp SnapCenter®

Microsoft SQL Server

search by name

Name

master

model

msdb

tempdb

tpcc

Total 5

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

Select one or more policies and configure schedules

SQL Server Full Backup

SQL Server Full Backup

SQL Server Log Backup

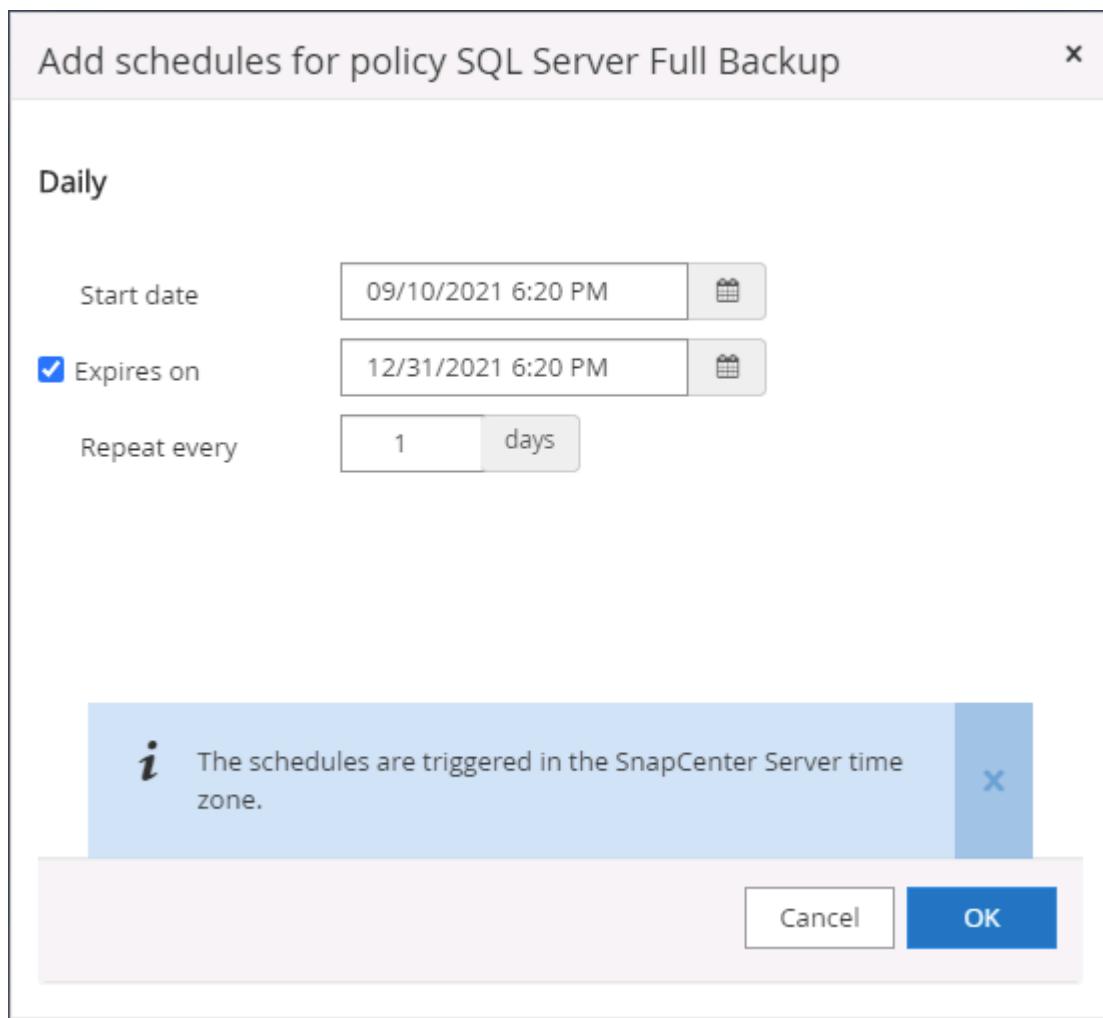
Policy	Applied Schedules	Configure Schedules
SQL Server Full Backup	None	<input type="button" value="+"/>

Total 1

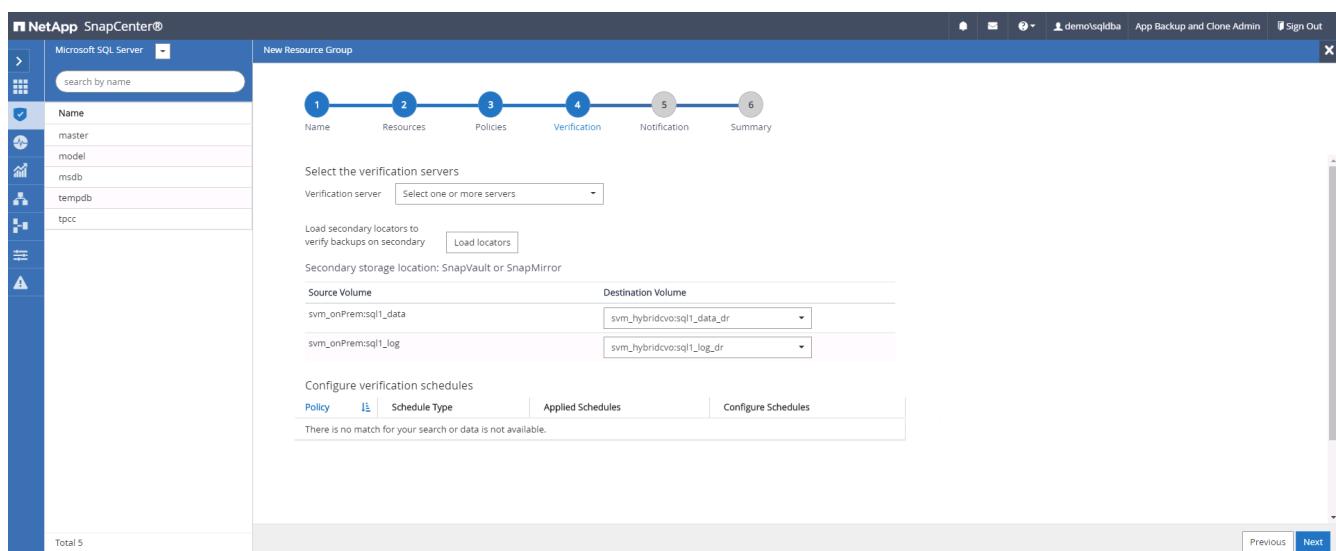
Use Microsoft SQL Server scheduler

Previous Next

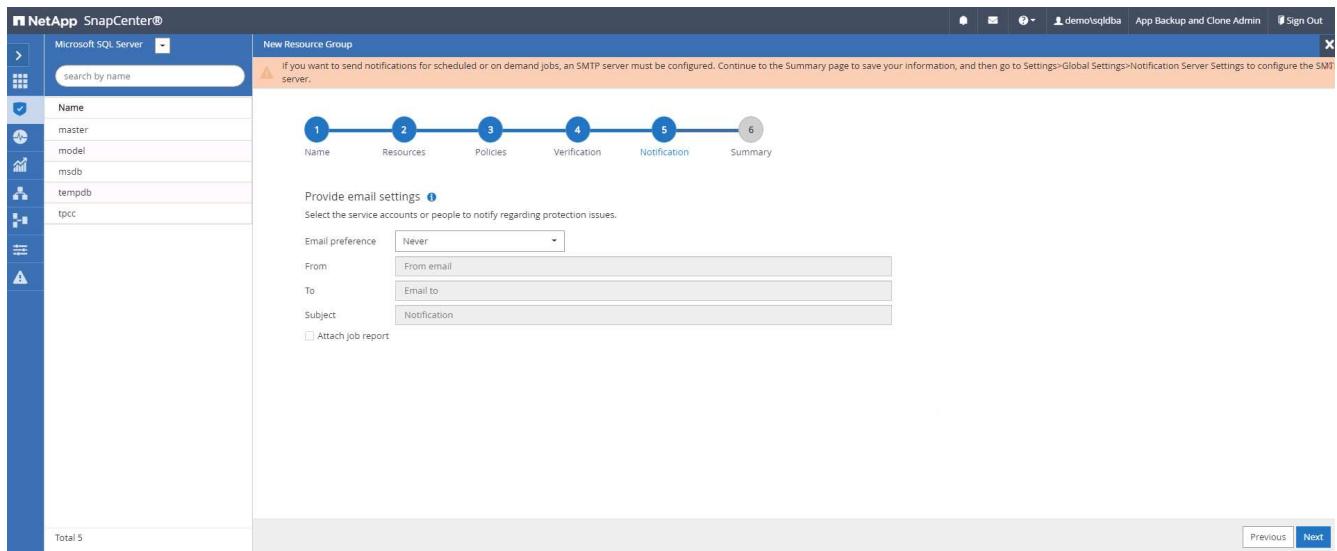
4. Add exact timing for backups as well as the frequency.



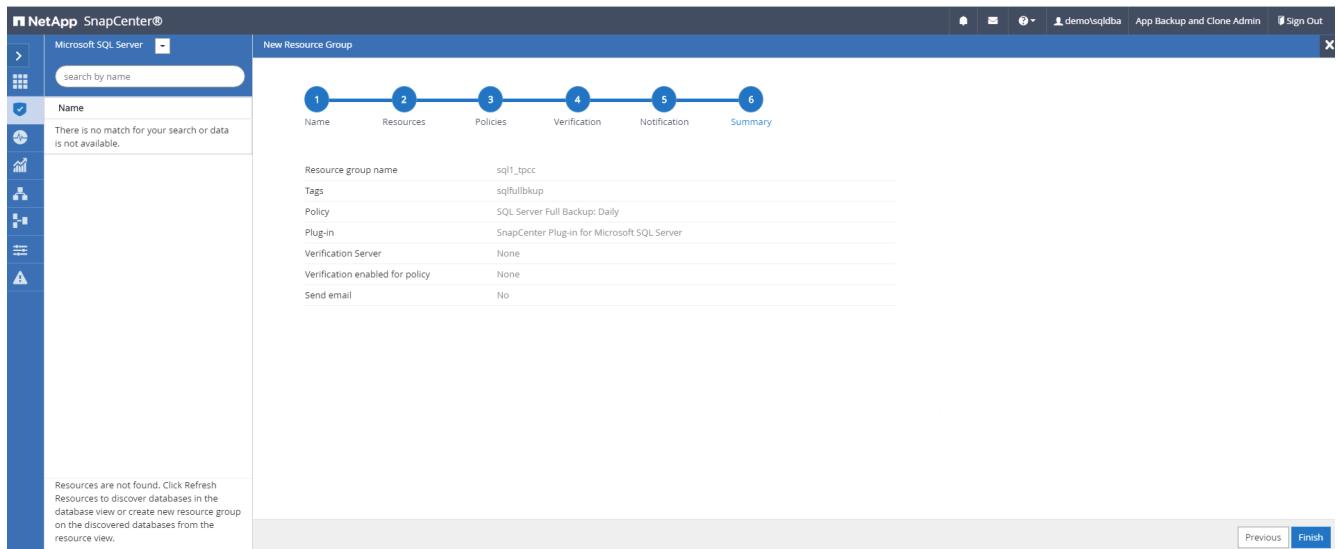
5. Choose the verification server for the backup on secondary if backup verification is to be performed. Click Load Locator to populate the secondary storage location.



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

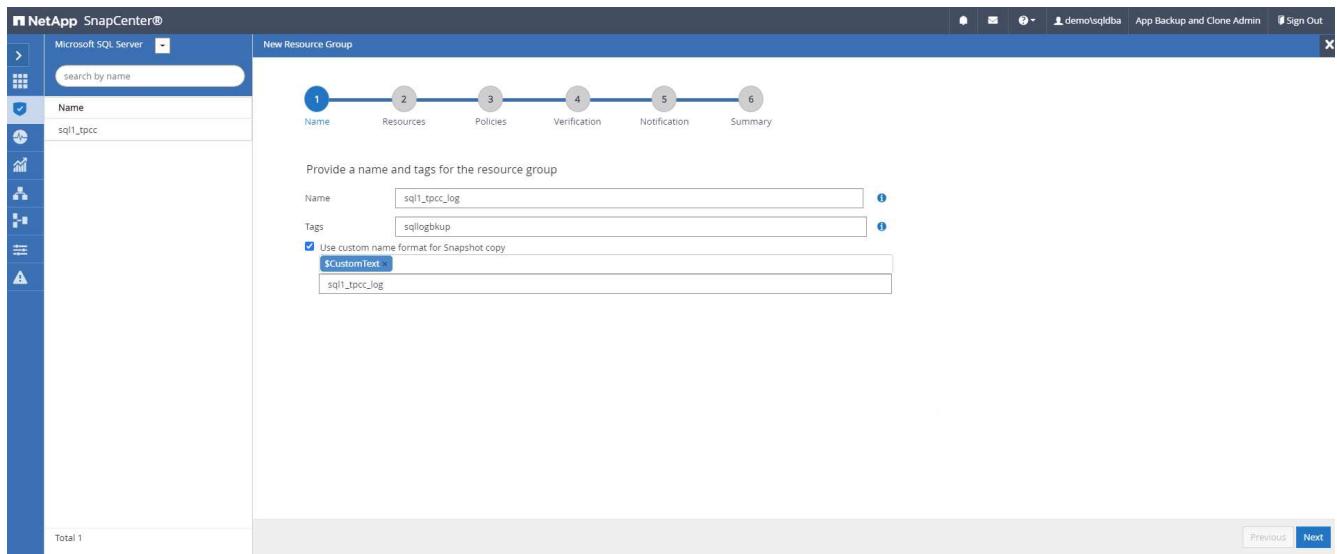


## 7. Summary.

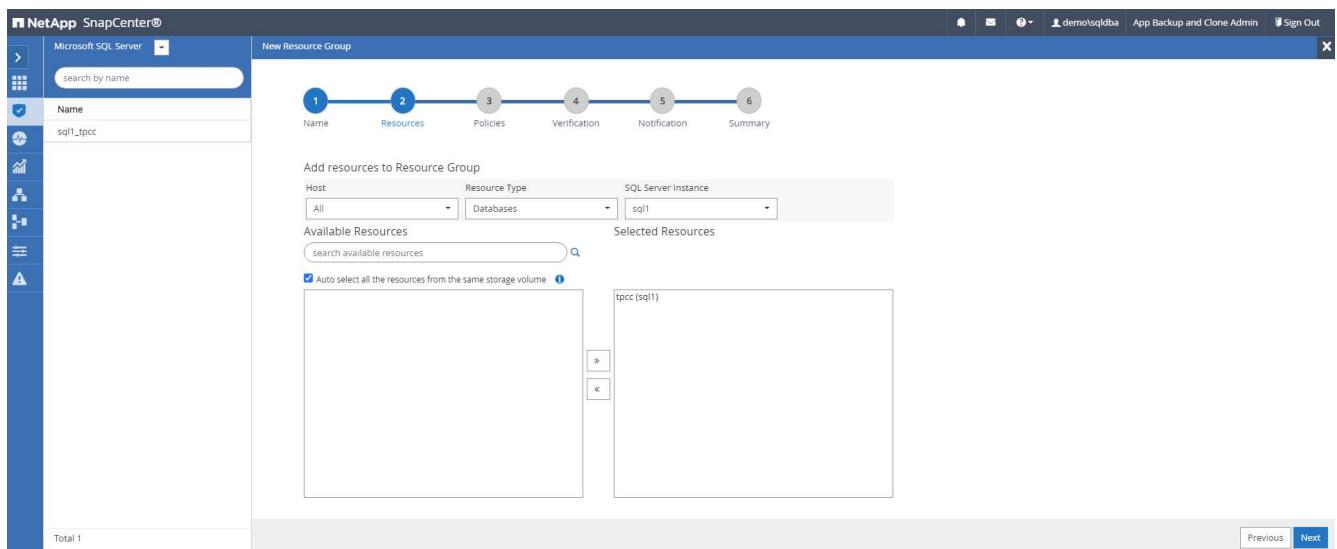


### Create a resource group for log backup of SQL Server

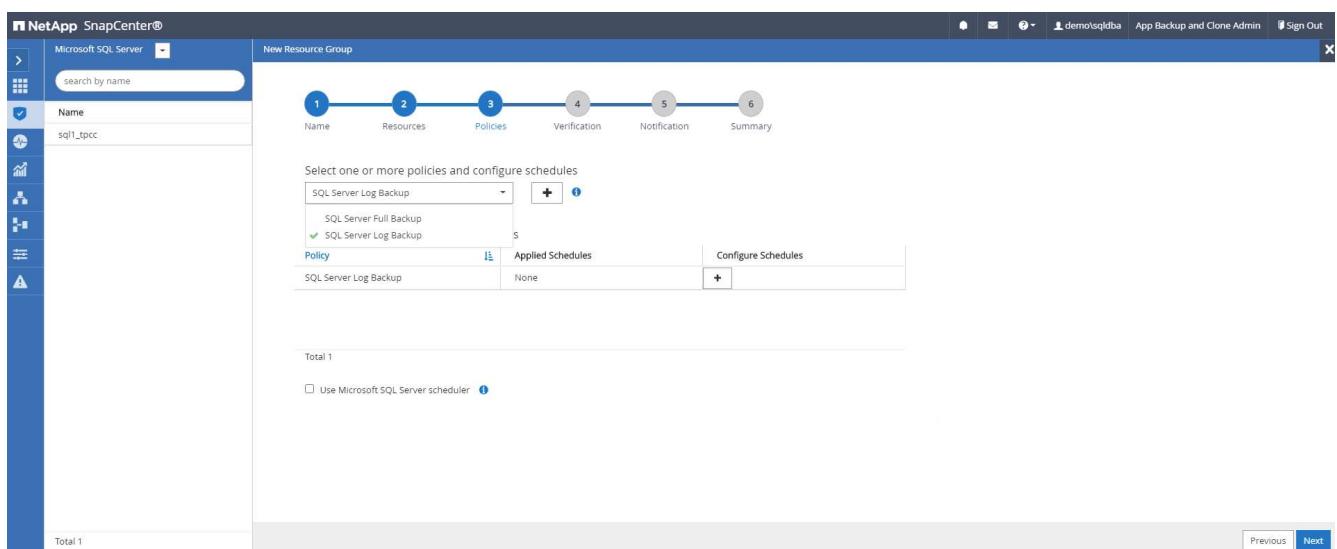
1. Log into SnapCenter with a database management user ID, and navigate to the Resources tab. In the View drop-down list, choose either a Database or Resource Group to launch the resource group creation workflow. Provide the name and tags for the resource group. You can define a naming format for the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



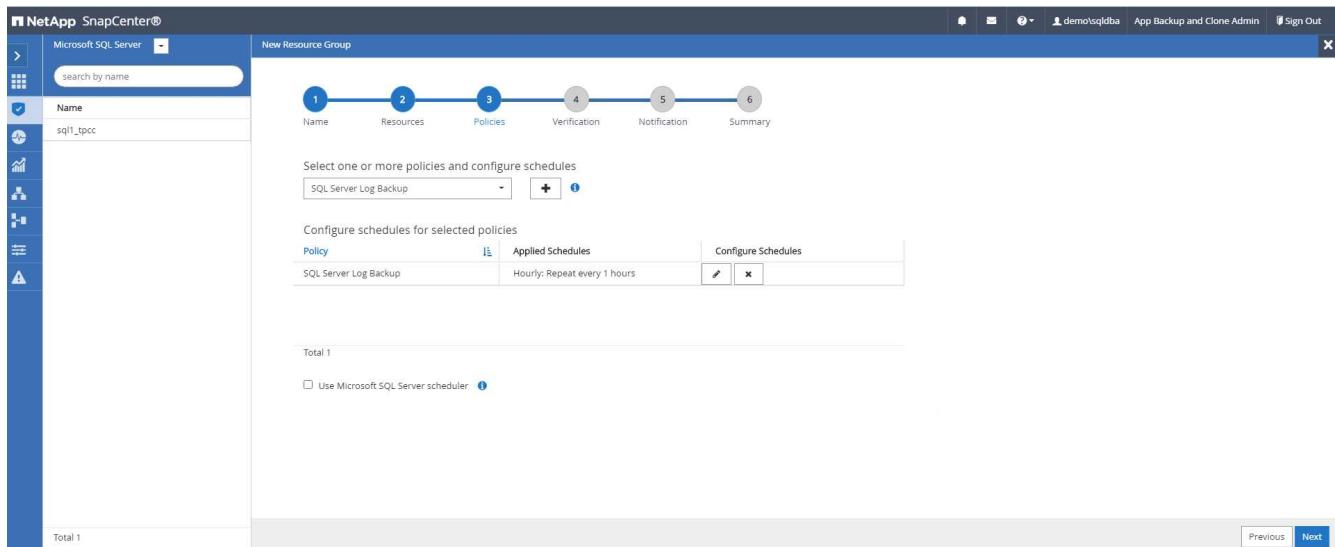
## 2. Select the database resources to be backed up.



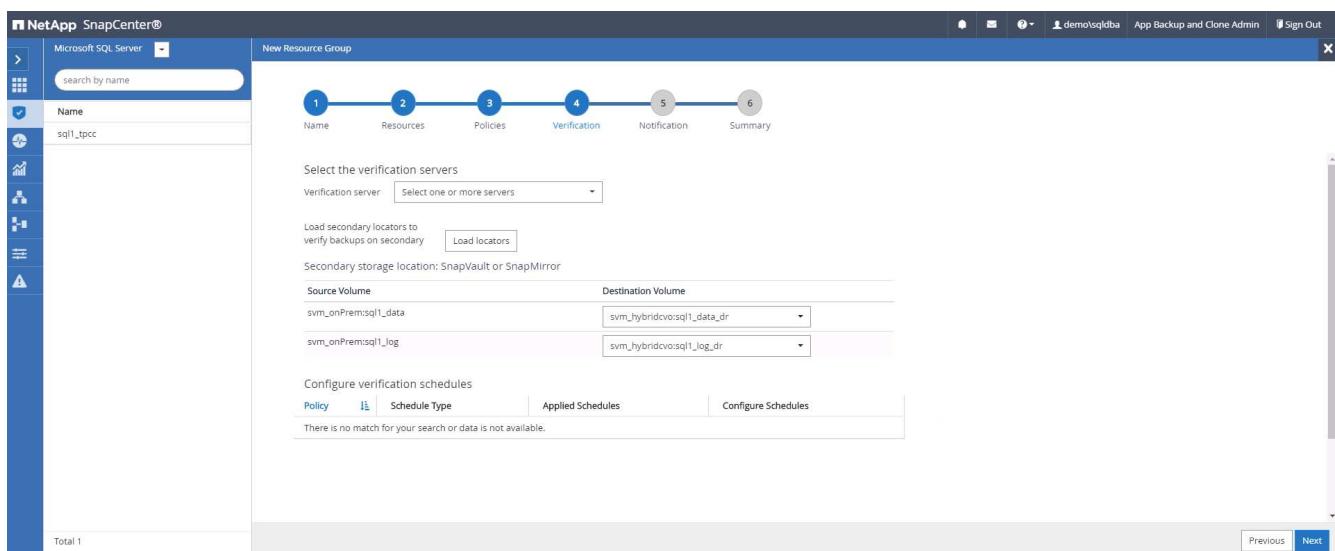
## 3. Select a SQL log backup policy created in section 7.



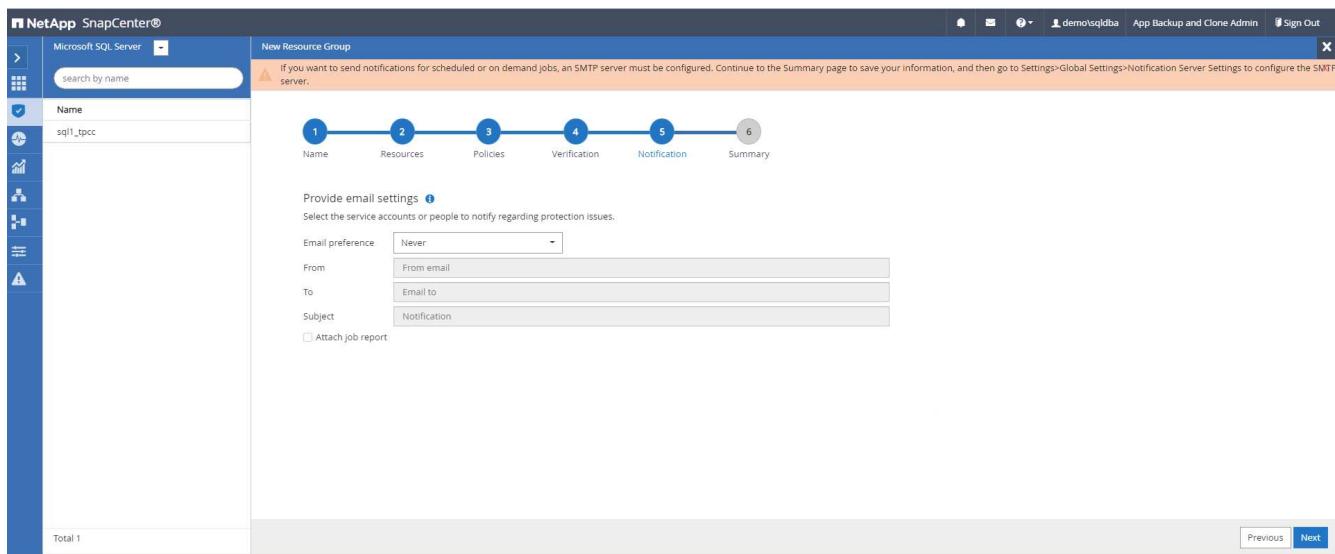
4. Add exact timing for the backup as well as the frequency.



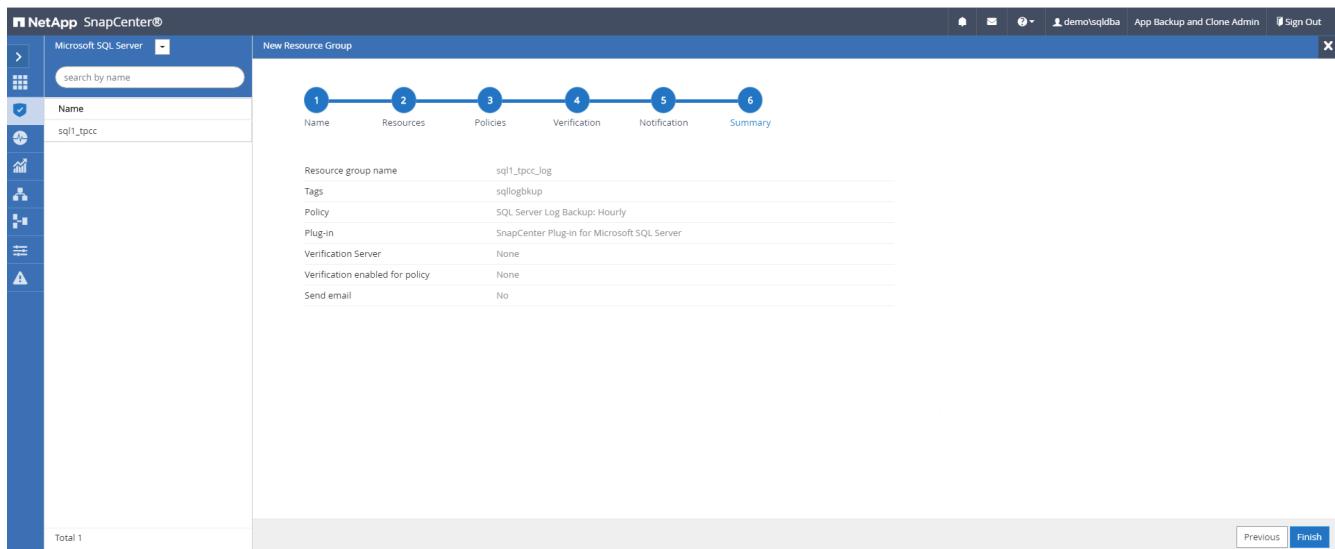
5. Choose the verification server for the backup on secondary if backup verification is to be performed. Click the Load Locator to populate the secondary storage location.



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

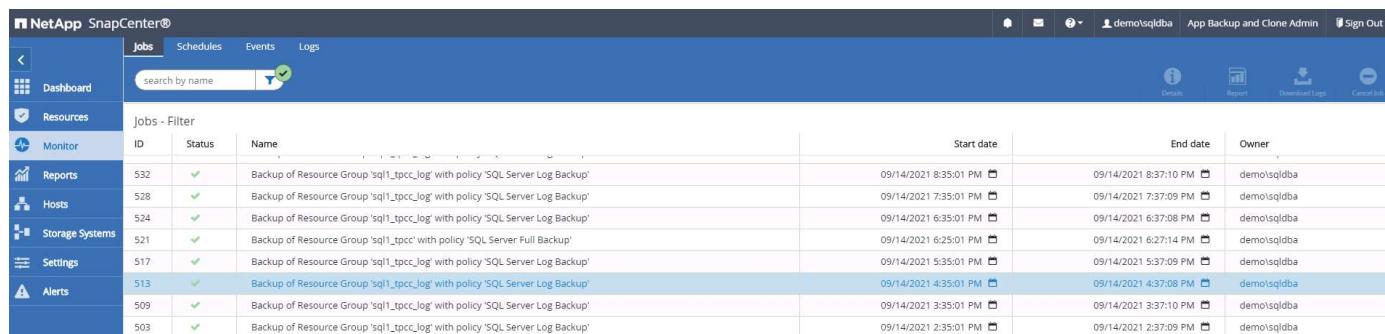


## 7. Summary.



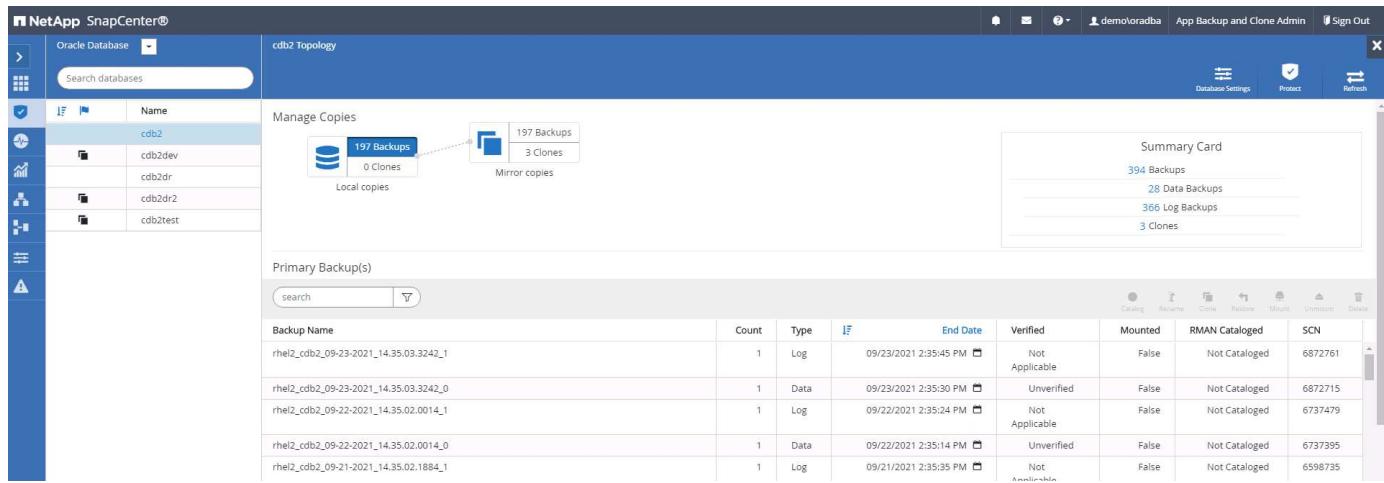
## 9. Validate backup

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.



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. The left sidebar lists databases: cdb2, cdb2dev, cdb2dr, cdb2dr2, and cdb2test. The main area displays the 'cdb2 Topology' with a 'Manage Copies' section showing '197 Backups' and '0 Clones' under 'Local copies', and '197 Backups' and '3 Clones' under 'Mirror copies'. A 'Summary Card' on the right shows statistics: 394 Backups, 28 Data Backups, 366 Log Backups, and 3 Clones. Below these are sections for 'Primary Backup(s)' and 'Secondary Backup(s)', each listing multiple backup entries with columns for Count, Type, End Date, Verified, Mounted, RMAN Cataloged, and SCN.

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](#)

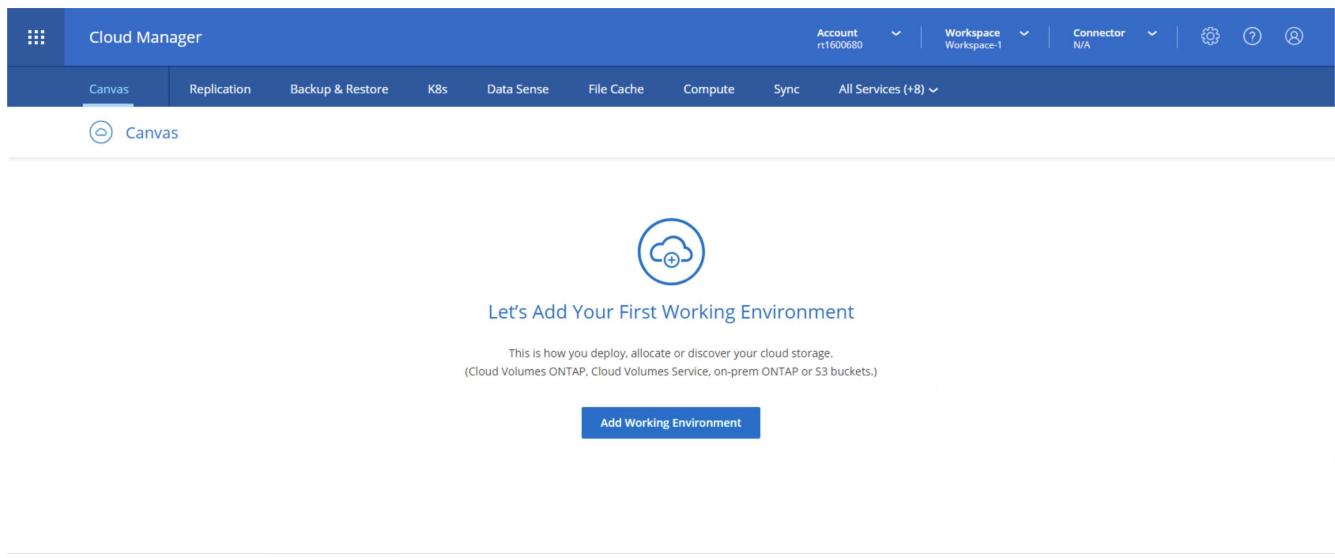
### Log In to NetApp Cloud Central

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

A text input field containing the email address "rt1600680@demo.netapp.com".A password input field showing five dots as a placeholder.A large blue rectangular button with the word "LOGIN" in white capital letters.

[Forgot your password?](#)

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



Cloud Manager

Account: rt1600680 | Workspace: Workspace-1 | Connector: N/A

Canvas Replication Backup & Restore K8s Data Sense File Cache Compute Sync All Services (+8) ▾

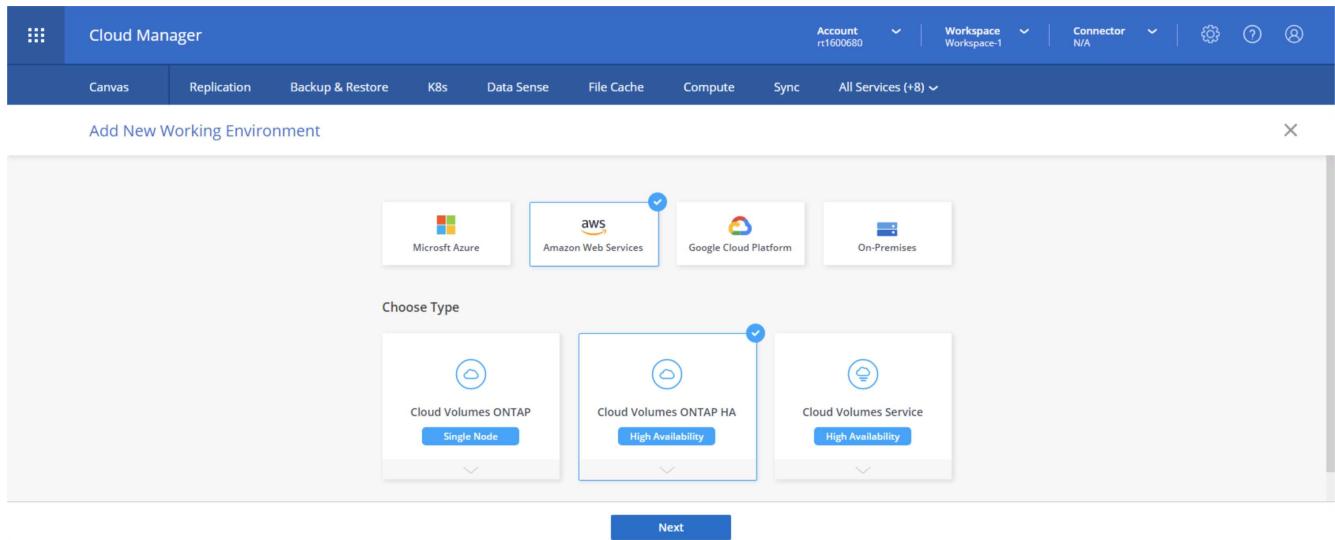
Canvas

Let's Add Your First Working Environment

This is how you deploy, allocate or discover your cloud storage.  
(Cloud Volumes ONTAP, Cloud Volumes Service, on-prem ONTAP or S3 buckets.)

Add Working Environment

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.



Cloud Manager

Account: rt1600680 | Workspace: Workspace-1 | Connector: N/A

Canvas Replication Backup & Restore K8s Data Sense File Cache Compute Sync All Services (+8) ▾

Add New Working Environment

Microsoft Azure

Amazon Web Services

Google Cloud Platform

On-Premises

Choose Type

Cloud Volumes ONTAP

Single Node

Cloud Volumes ONTAP HA

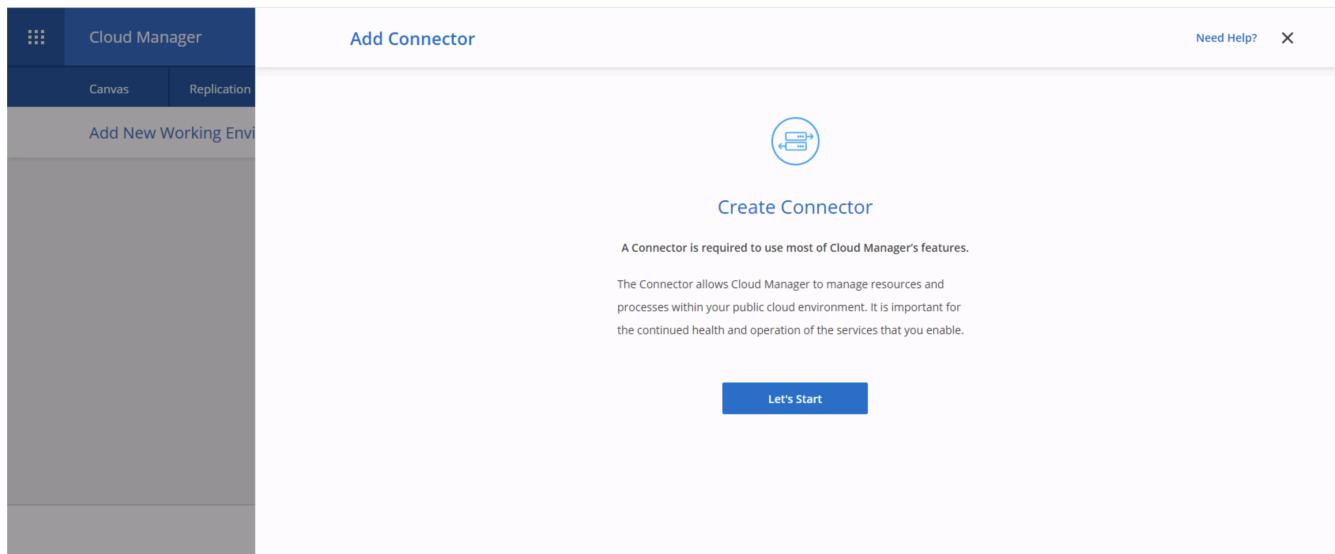
High Availability

Cloud Volumes Service

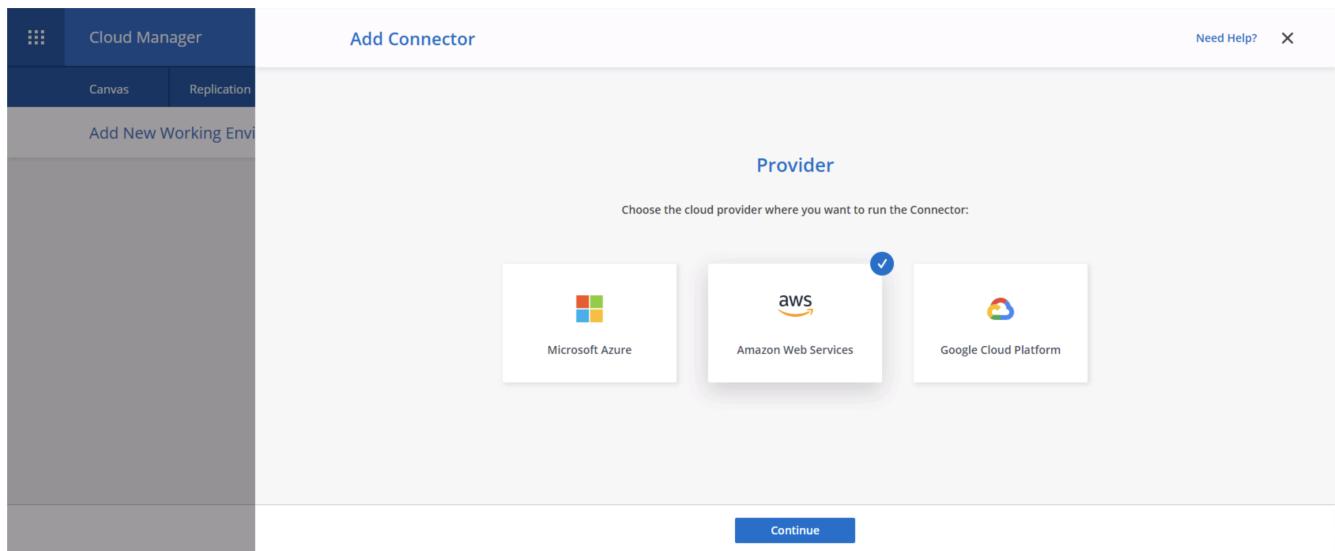
High Availability

Next

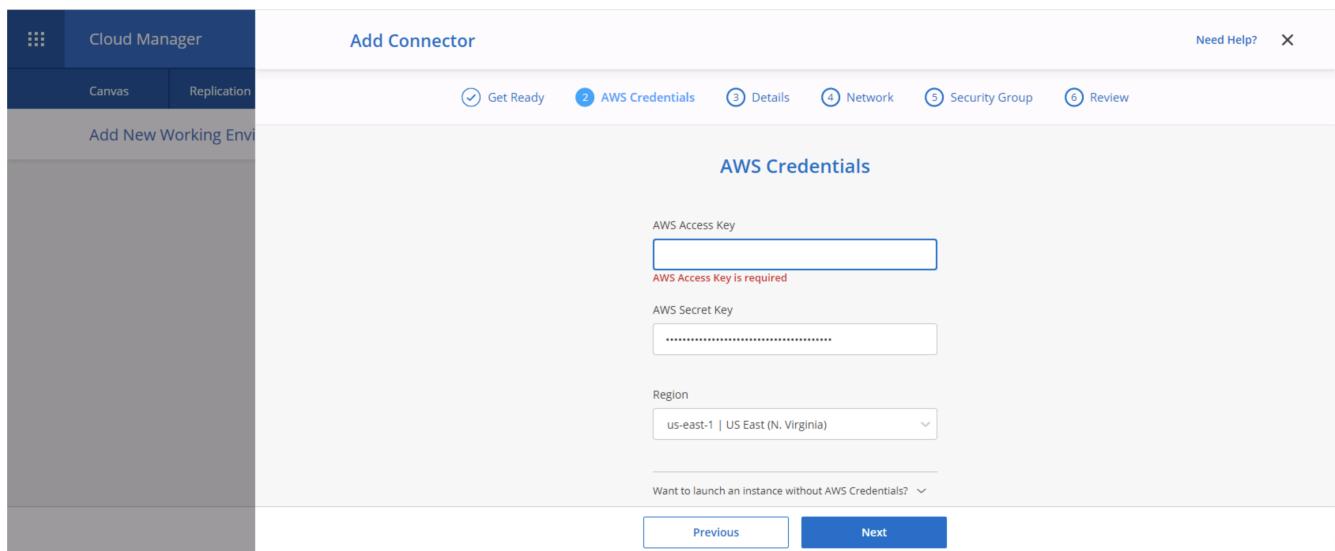
4. If no connector has been created, a pop-up appears asking you to create a connector.



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

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

Proxy Configuration (Optional)

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

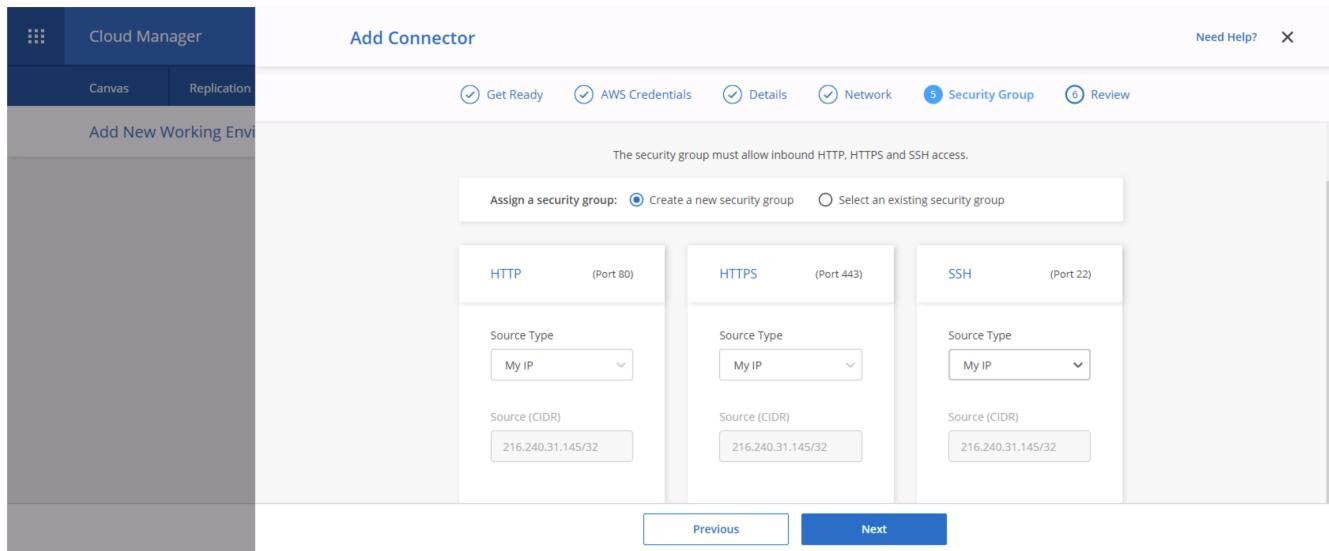
Define Credentials for this Proxy

Upload a root certificate

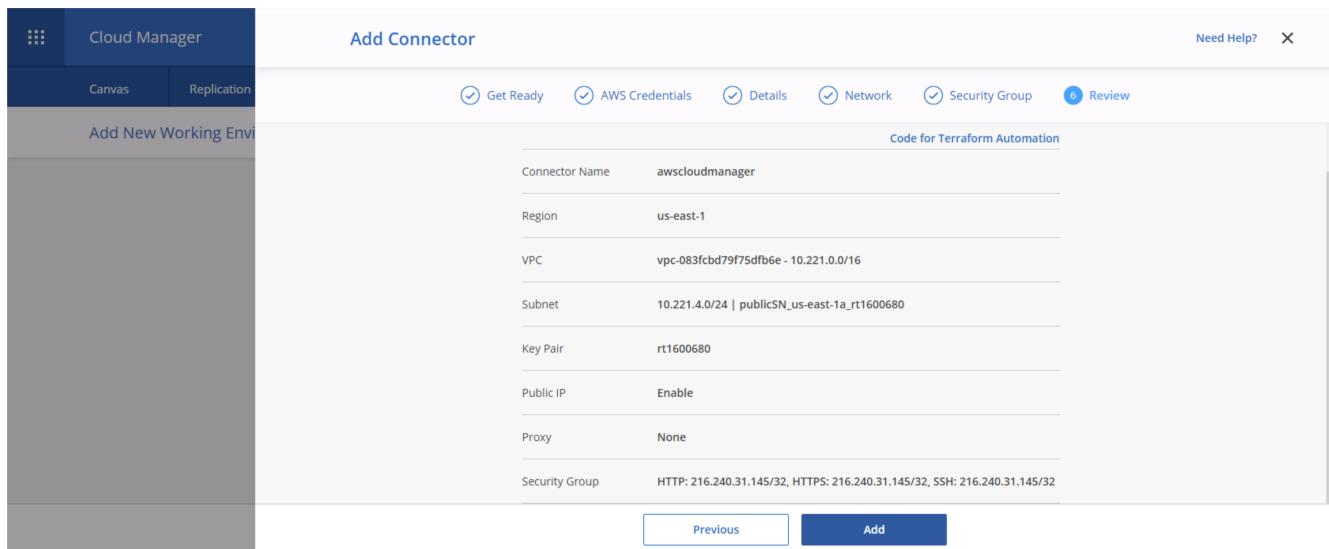
Public IP: Enable

Previous Next

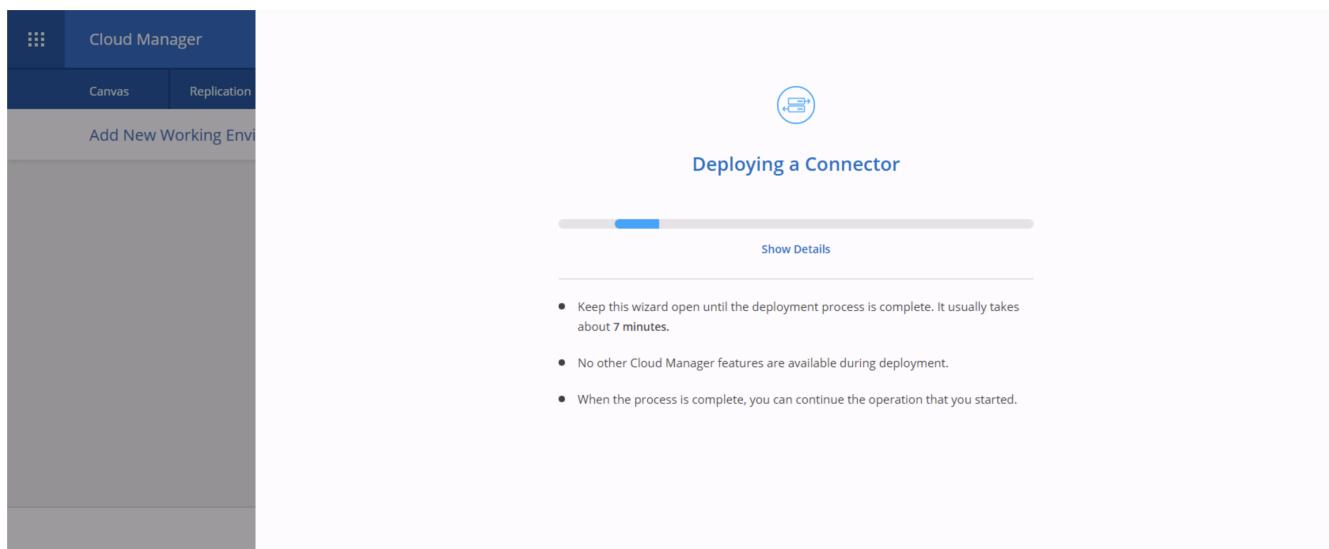
9. Provide communication with the connector via SSH, HTTP, and HTTPS by either providing a security group or creating a new security group. I have enabled access to the connector from my IP address only.



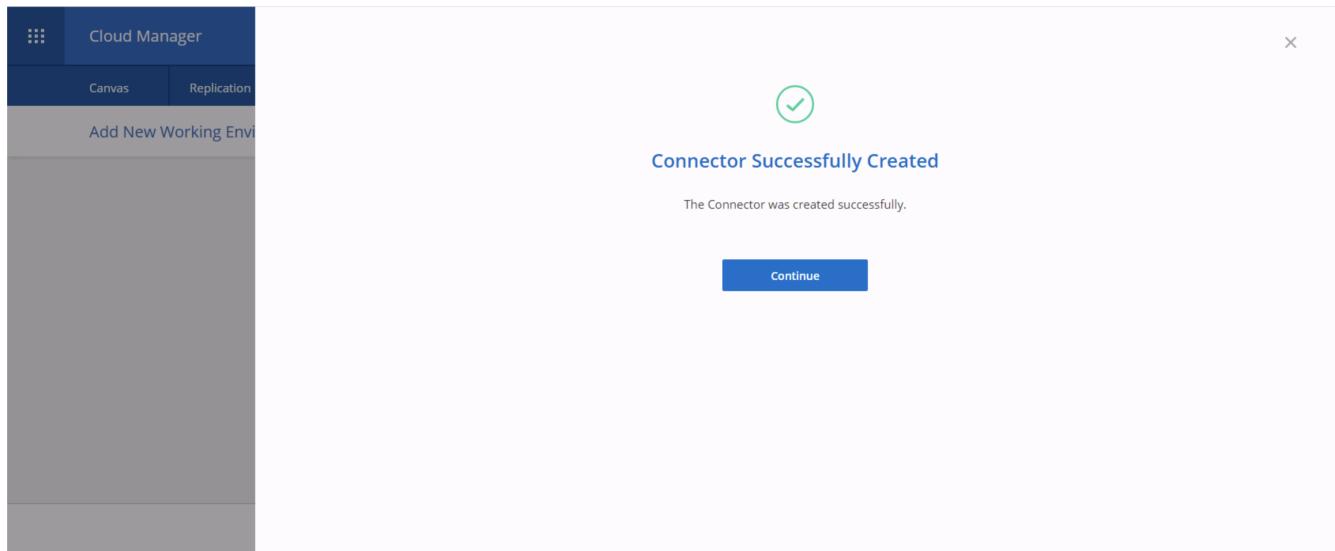
10. Review the information on the summary page and click Add to deploy the connector.



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

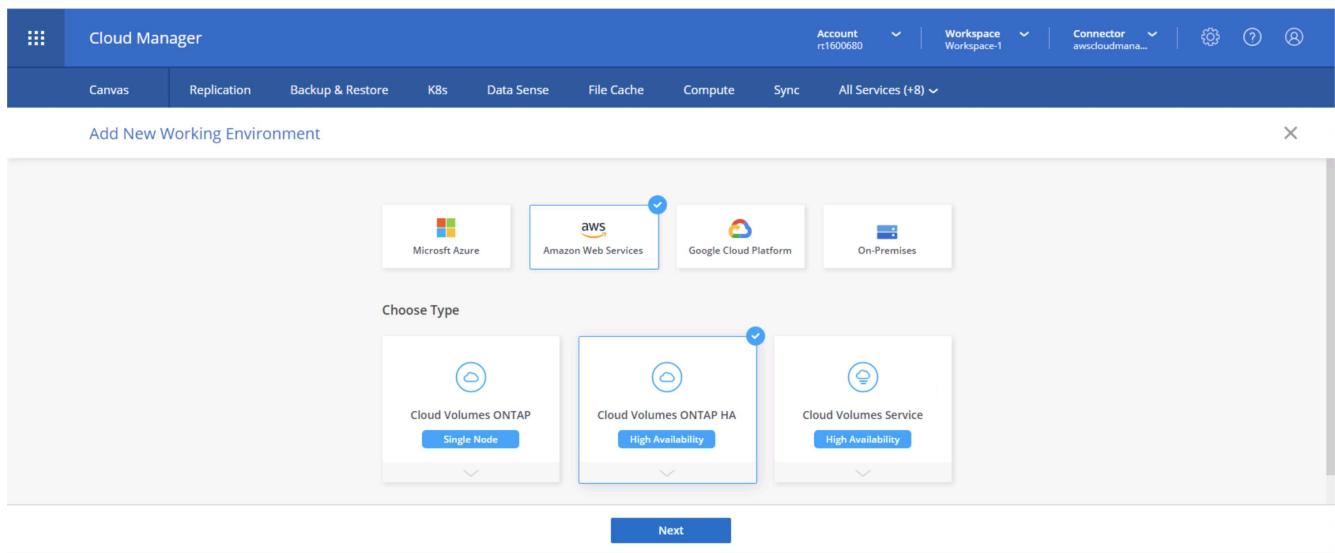


12. When the deployment is complete, a success page appears.



## 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.

Cloud Manager

Canvas Replication Backup & Restore K8s Data Sense File Cache Compute Sync All Services (+8)

Create a New Working Environment

Details and Credentials

↑ Previous Step Instance Profile 322944748816 Account ID 322944748816  
Credential Name Marketplace Subscription [Edit Credentials](#)

Details

Working Environment Name (Cluster Name)  
Up to 40 characters

Add Tags Optional Field Up to four tags

Credentials

User Name admin

Password

Confirm Password

Continue

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

### 3. Choose Add Subscription.

Cloud Manager

Canvas Replication Backup & Restore K8s Data Sense File Cache Compute Sync All Services (+8)

Create a New Working Environment

Details and Credentials

↑ Previous Step Instance Profile 322944748816 Account ID 322944748816  
Credential Name Marketplace Subscription [Edit Credentials](#)

Associate Subscription to Credentials ⓘ

Credentials

Instance Profile | Account ID: 322944748816

Marketplace Subscription [Edit Credentials](#)

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.

Cloud Manager

Canvas Replication Backup & Restore K8s Data Sense File Cache Compute Sync All Services (+8)

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.

Cloud Manager - Deploy & Manage NetApp Cloud Data Services

Sold by: NetApp, Inc.

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, [▼ Show more](#)

**Overview**    Pricing    Usage    Support    Reviews

**Product Overview**

NetApp Cloud Manager is the management and automation platform used for deploying and operating NetApp's Cloud Data Services including:

- Cloud Volumes ONTAP - File and block storage for enterprise workloads
- Cloud Backup - Incremental block-level Backup & Restore capabilities for protecting and archiving CVO and On-Premises ONTAP data to S3
- Cloud Tiering - Tiering infrequently-used data to object storage for AFF
- Cloud Data Sense - AI-driven data privacy controls and reporting
- Cloud Manager also manages Cloud Volumes Service on AWS

Cloud Manager eases the day-to-day requirements of operating your cloud storage environment including configuring, provisioning, and monitoring each of your active NetApp Cloud Data Services including their virtual and hardware storage nodes. It offers a

**Highlights**

- 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.

You are subscribed to this offer.

Offer name: NetApp, Inc. for SaaS 2020-07-20- Private Offer - current subscription

You are currently subscribed to this product and will be charged for your accumulated usage at the end of your next billing cycle, based on the costs listed in Pricing information on the right.

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.

You Have Subscribed to a Private Offer

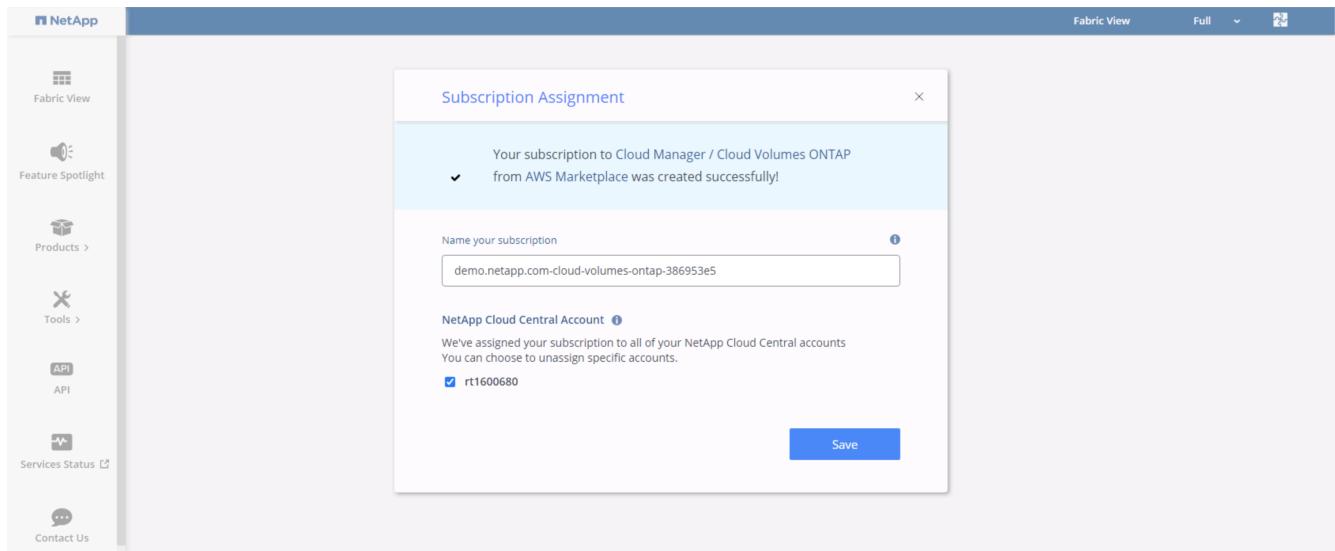
You have subscribed to this private offer on **July 21, 2020 UTC**. The private offer will **expire on August 1, 2022 UTC**. Your use of this product after the expiration date of your private offer will be billed at the then current public pricing, which can be found on this product's detail page.

To avoid being charged for use beyond the expiration date of this offer, you can cancel your subscription to this product by August 1, 2022 UTC. Please contact the vendor directly with any questions regarding this offer.

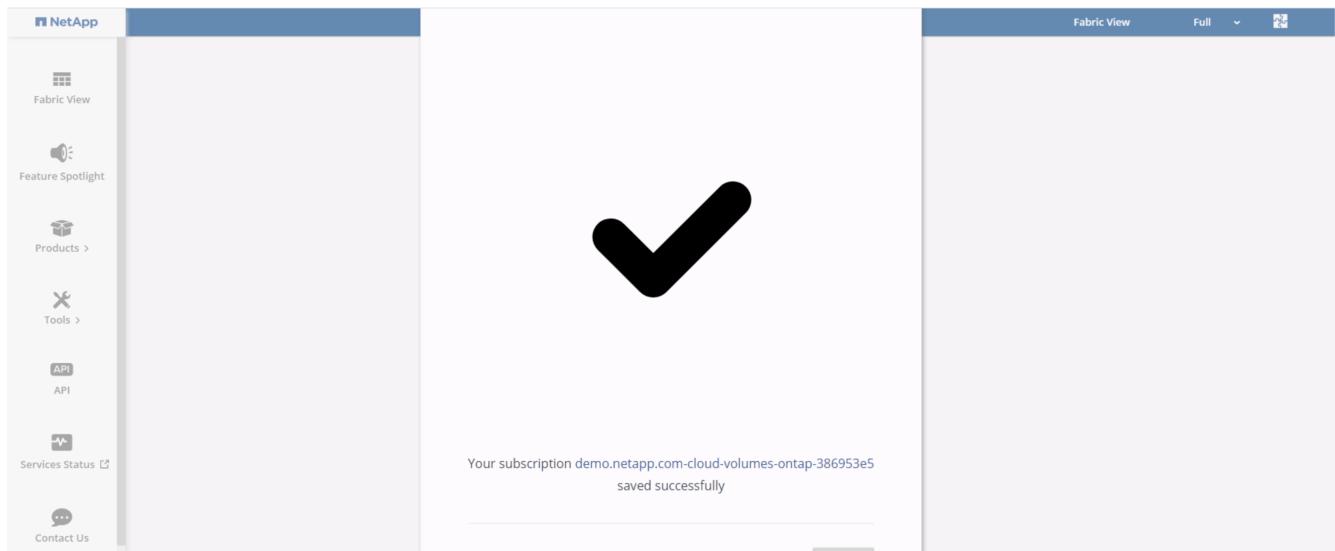
[Subscribe](#)

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.

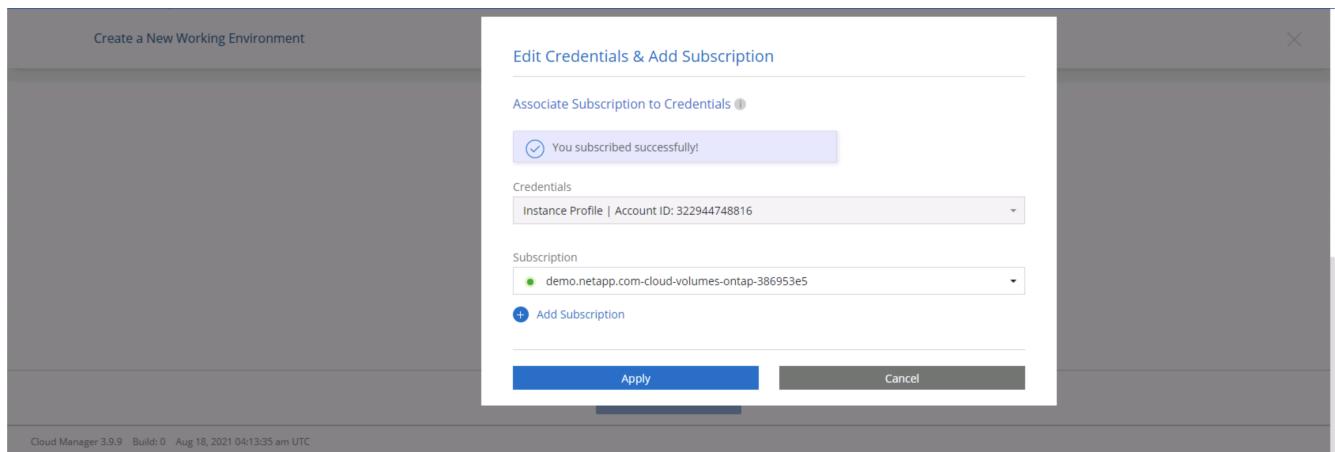
7. You are redirected to Cloud Central where you must name your subscription and assign it to your Cloud Central account.



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



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



10. Enter the working environment details such as:

- a. Cluster name

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

Cloud Manager

Canvas Replication Backup & Restore K8s Data Sense File Cache Compute Sync All Services (+8) ▾

Create a New Working Environment Details and Credentials

↑ Previous Step Instance Profile 322944748816 Credential Name demo.netapp.com-cloud-vol... Account ID Account rt1600680 Workspace Workspace-1 Connector awscloudman...

Edit Credentials

Details

Working Environment Name (Cluster Name)  
hybridawscvo

Credentials

User Name admin

Password \*\*\*\*\*

Confirm Password \*\*\*\*\*

Add Tags Optional Field Up to four tags

Continue

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

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

Cloud Manager

Canvas Replication Backup & Restore K8s Data Sense File Cache Compute Sync All Services (+8) ▾

Create a New Working Environment Services

↑ Previous Step

Data Sense & Compliance

Backup to Cloud

Monitoring

Continue

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

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.

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.

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

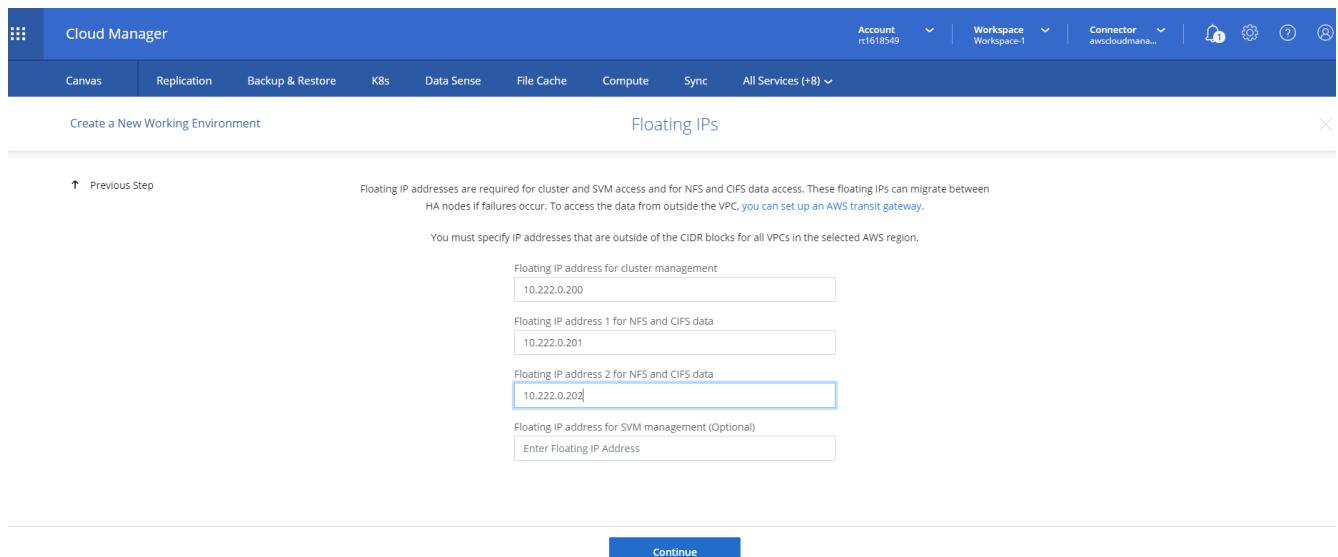
14. Choose the connection methods for the nodes as well as the mediator.

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



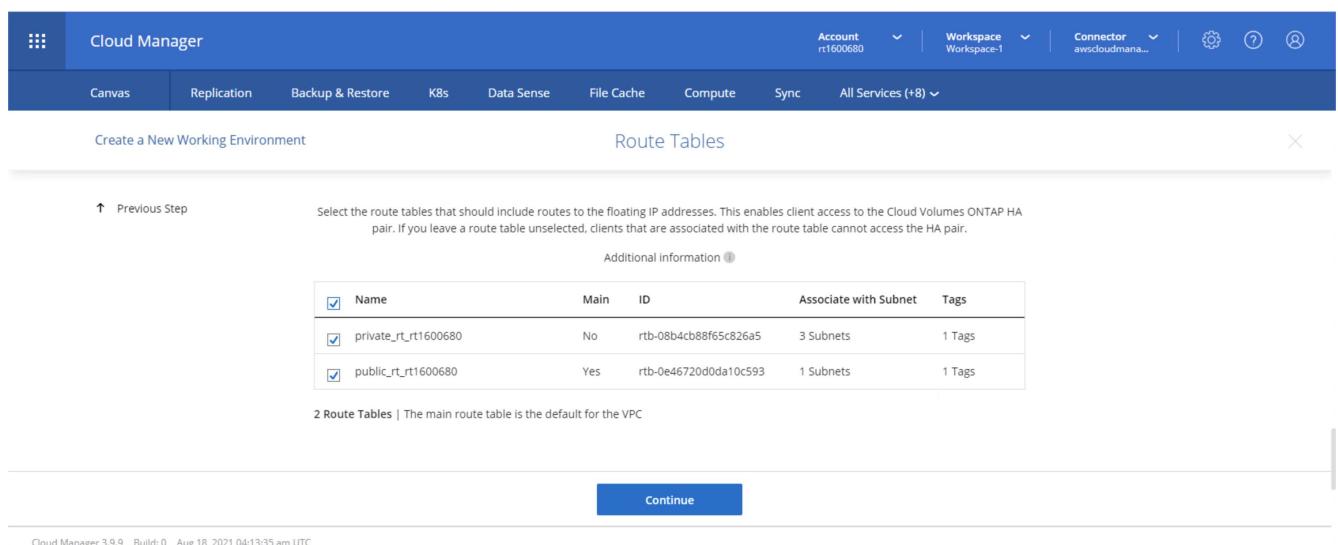
The mediator requires communication with the AWS APIs. A public IP address is not required so long as the APIs are reachable after the mediator EC2 instance has been deployed.

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' configuration step. The top navigation bar includes 'Account r11618549', 'Workspace Workspace-1', 'Connector awscloudman...', and various icons. The main content area is titled 'Create a New Working Environment' and 'Floating IPs'. It contains fields for 'Floating IP address for cluster management' (10.222.0.200), 'Floating IP address 1 for NFS and CIFS data' (10.222.0.201), and 'Floating IP address 2 for NFS and CIFS data' (10.222.0.202, highlighted with a blue border). There is also a field for 'Floating IP address for SVM management (Optional)' with the placeholder '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' configuration step. The top navigation bar is identical to the previous screenshot. The main content area is titled 'Create a New Working Environment' and 'Route Tables'. It contains a note: '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.' Below this is an 'Additional information' link. A table lists two route tables: 'private\_rt\_rt1600680' (Main: No, ID: rtb-08b4cb88f65c826a5, Associate with Subnet: 3 Subnets, Tags: 1 Tag) and 'public\_rt\_rt1600680' (Main: Yes, ID: rtb-0e46720d0da10c593, Associate with Subnet: 1 Subnets, Tags: 1 Tag). A note at the bottom states '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 | Database and application data production workloads | Cost effective DR | Highest performance production workloads

Up to 2TB of storage | Up to 10TB of storage | Up to 10TB of storage | 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

NFS

CIFS

iSCSI

Volume Name:

Size (GB):  Volume size

Snapshot Policy:  default

Access Control:  Custom export policy

Custom export policy: 10.221.0.0/16

Default Policy

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 hybridawscvo  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.

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

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 Timeline page. At the top, there are tabs for Canvas, Replication, Backup & Restore, K8s, Data Sense, File Cache, Compute, Sync, and All Services (+8). The Timeline tab is selected. Below the tabs is a filter bar with options: Time (1), Service, Action, Agent (1), Resource, User, Status, and a Reset button. The main area displays a table of deployment logs:

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

11. 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 Canvas page. 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 is a 'Add Working Environment' button and a 'Go to Tabular View' link. The main area displays two cloud icons representing working environments:

- Cloud Volumes ONTAP (High-Availability)**: Shows 'hybridawscvo' and 'Cloud Volumes ONTAP'. It has '1 GiB Capacity' and is marked with an 'aws' icon.
- Amazon S3**: Shows 'Amazon S3', '2 Buckets', and '1 Region'. It is marked with an 'aws' icon.

On the right, there is a 'Working environments' section with a table:

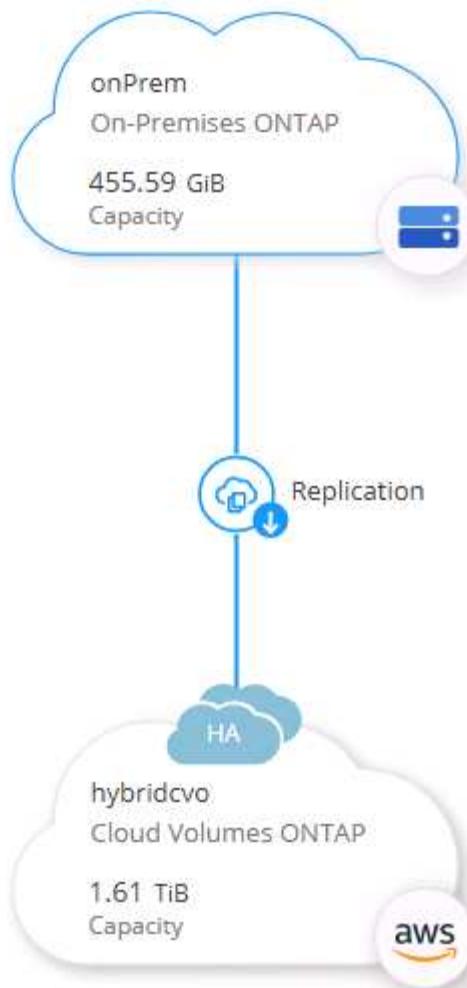
Environment	Capacity
Cloud Volumes ONTAP (High-Availability)	1 GiB Allocated Capacity
Amazon S3	0 Buckets

#### 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](#).

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

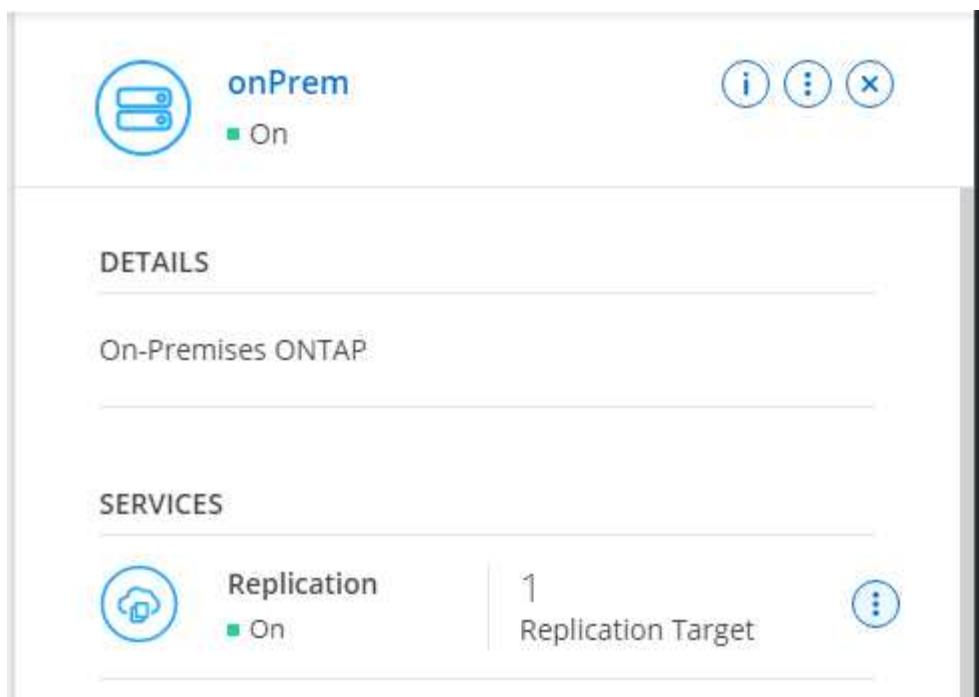


---

Select Enable.



Or Options.



onPrem

On

DETAILS

On-Premises ONTAP

SERVICES

Replication

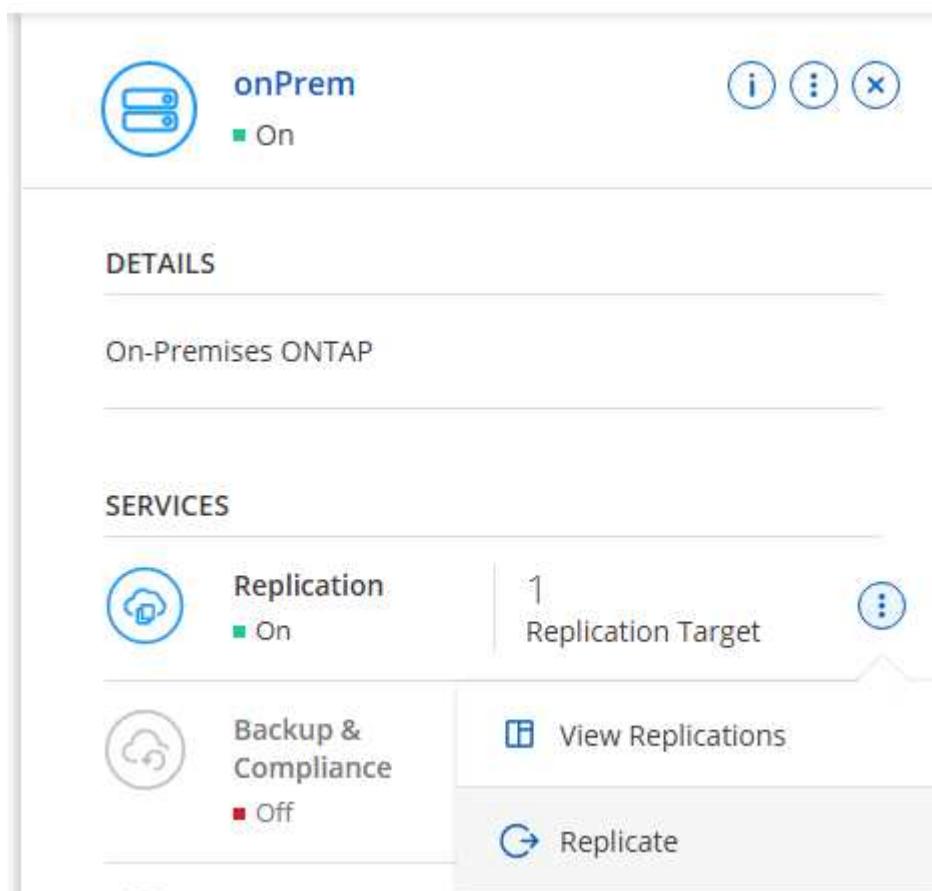
On

1

Replication Target

⋮

Replicate.



onPrem

On

DETAILS

On-Premises ONTAP

SERVICES

Replication

On

1

Replication Target

⋮

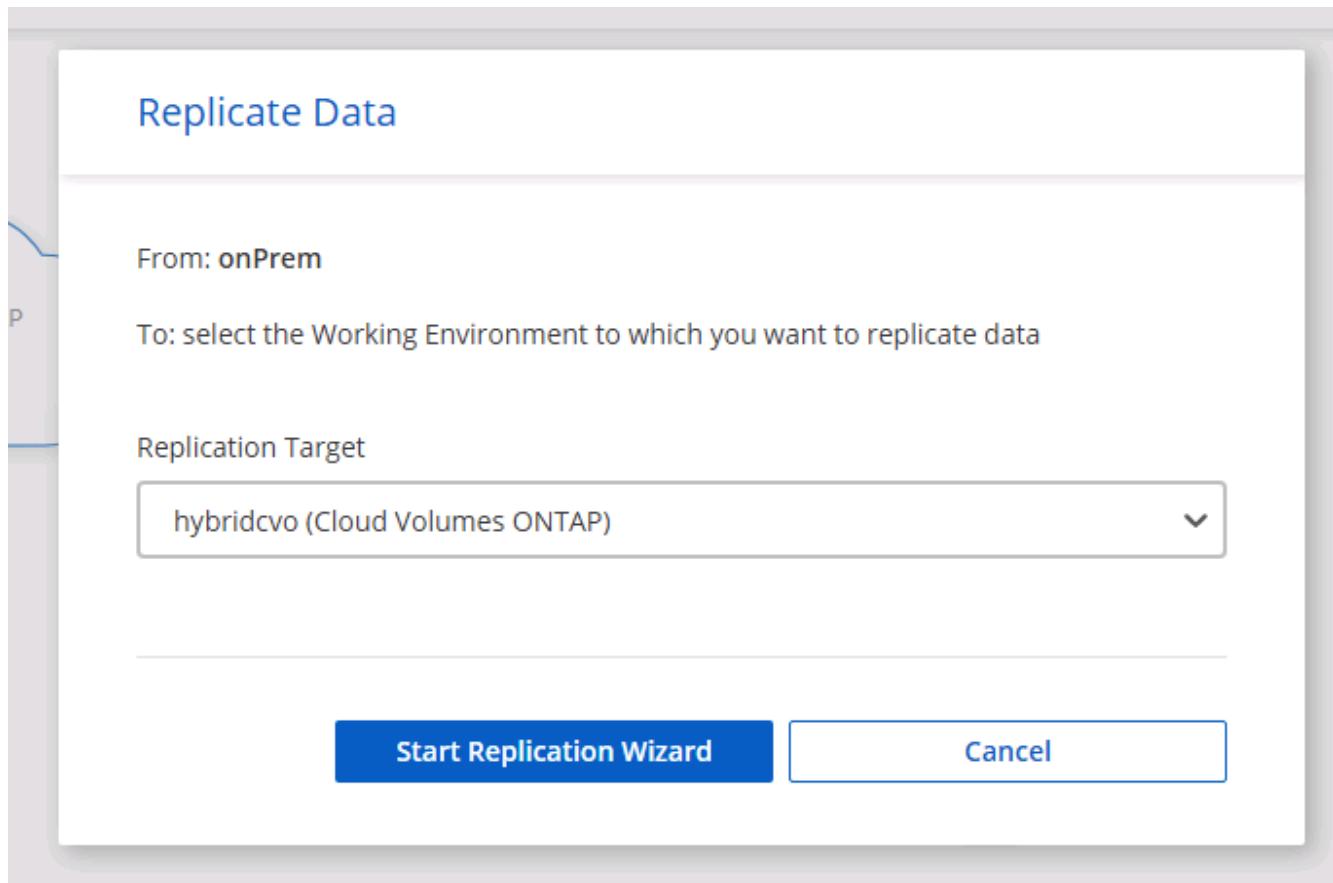
Backup & Compliance

Off

View Replications

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.

Replication Setup				Source Volume Selection			
<b>rhel2_u03</b>	INFO	Storage VM Name: <b>svm_onPrem</b>	CAPACITY	<b>rhel2_u0309232119421203118</b>	INFO	Storage VM Name: <b>svm_onPrem</b>	CAPACITY
INFO	Tiering Policy: <b>None</b>	Volume Type: <b>RW</b>	100 GB Allocated 7.29 GB Disk Used	INFO	Tiering Policy: <b>None</b>	Volume Type: <b>RW</b>	100 GB Allocated 35.83 MB Disk Used
INFO	Tiering Policy: <b>None</b>	Volume Type: <b>RW</b>	21.35 GB Allocated 18.16 GB Disk Used	INFO	Tiering Policy: <b>None</b>	Volume Type: <b>RW</b>	53.37 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:

100

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

#### Mirror

Typically used for disaster recovery

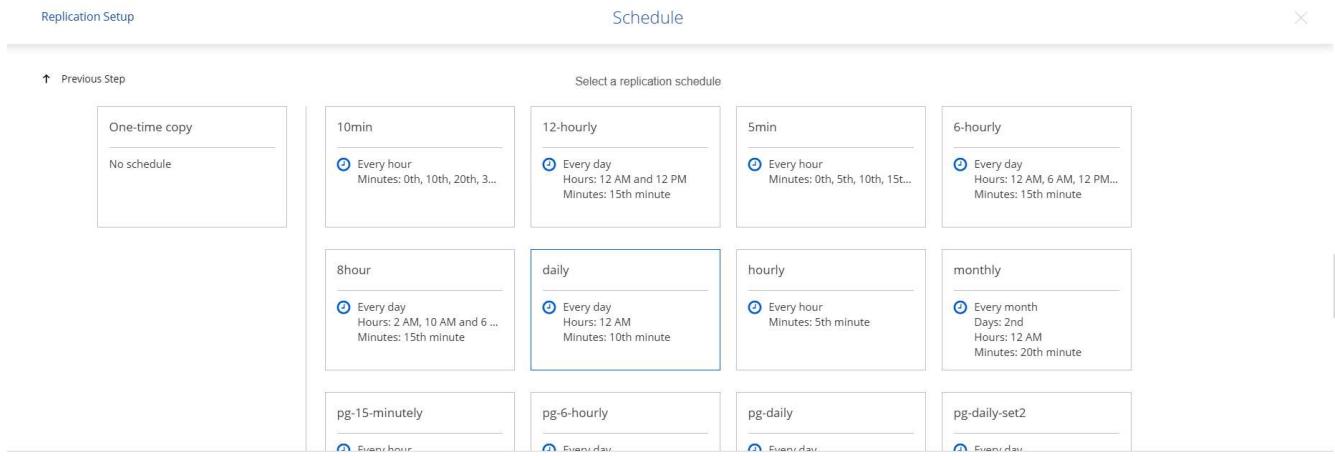
[More info](#)

#### Mirror and Backup (1 month retention)

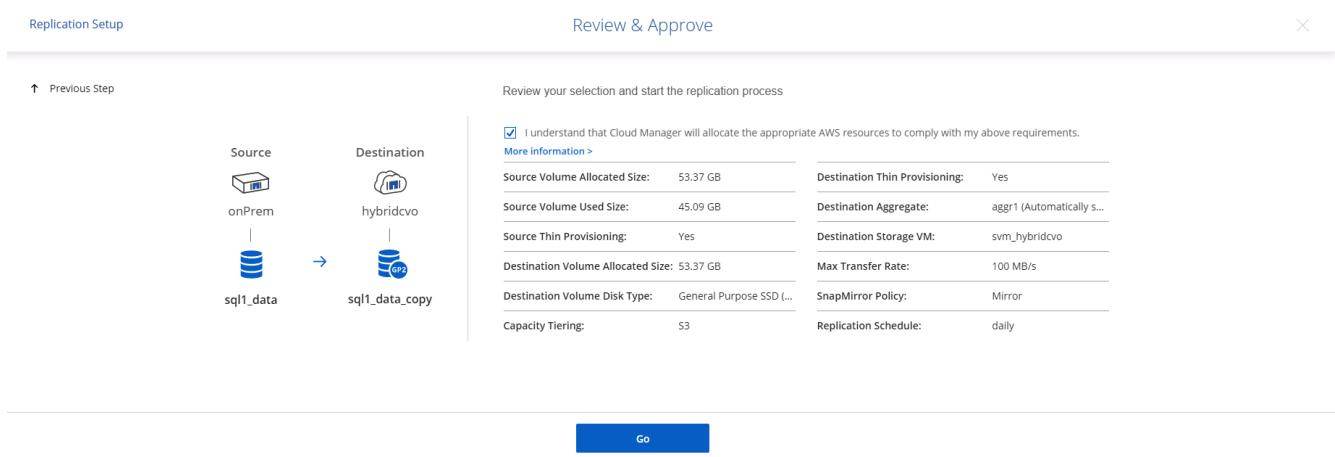
Configures disaster recovery and long-term retention of backups on the same destination volume

[More info](#)

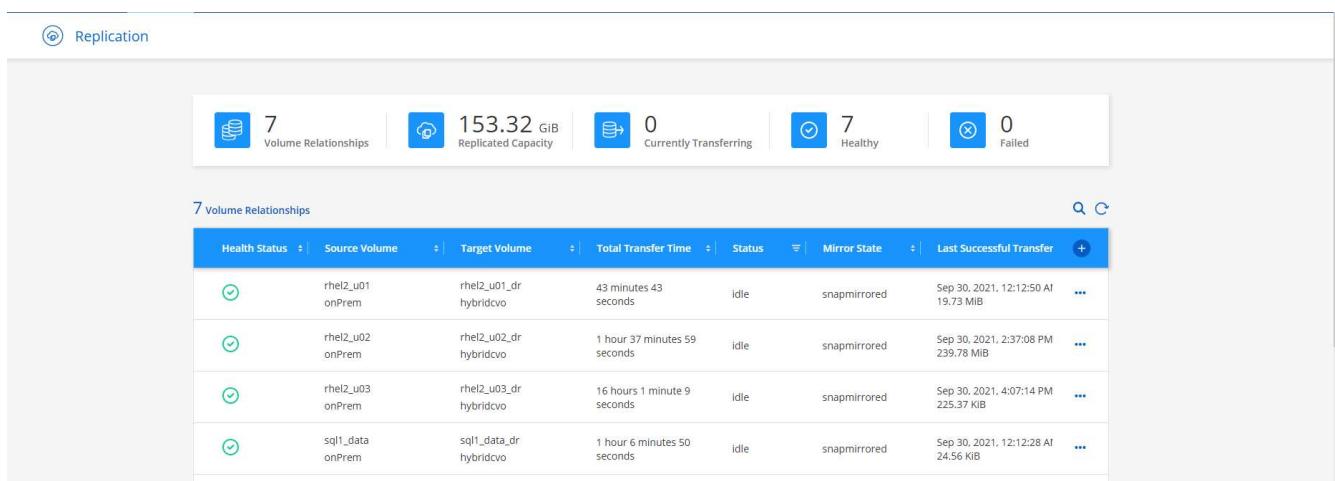
8. Choose the schedule for triggering replication. NetApp recommends setting a "daily" schedule of for the data volume and an "hourly" schedule for the log volumes, although this can be changed based on requirements.



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.



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](#).

## Copyright Information

Copyright © 2022 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means-graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system-without prior written permission of the copyright owner.

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

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

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

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

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

## 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.