Getting started overview

NetApp Solutions

NetApp
July 31, 2024

Table of Contents

Getting started overview

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

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.

On Premises

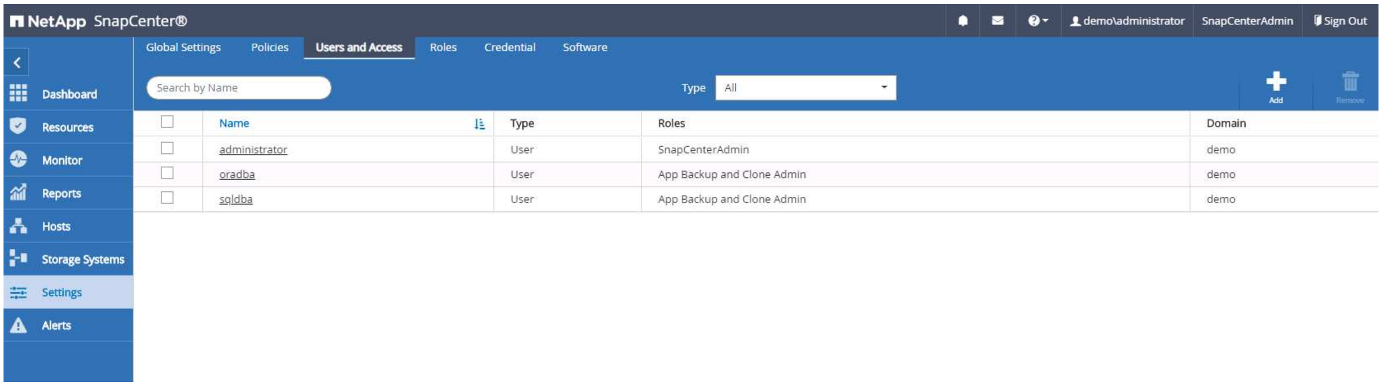
1. Setup database admin user in SnapCenter

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
administrator	User	SnapCenterAdmin	demo
oradba	User	App Backup and Clone Admin	demo
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.

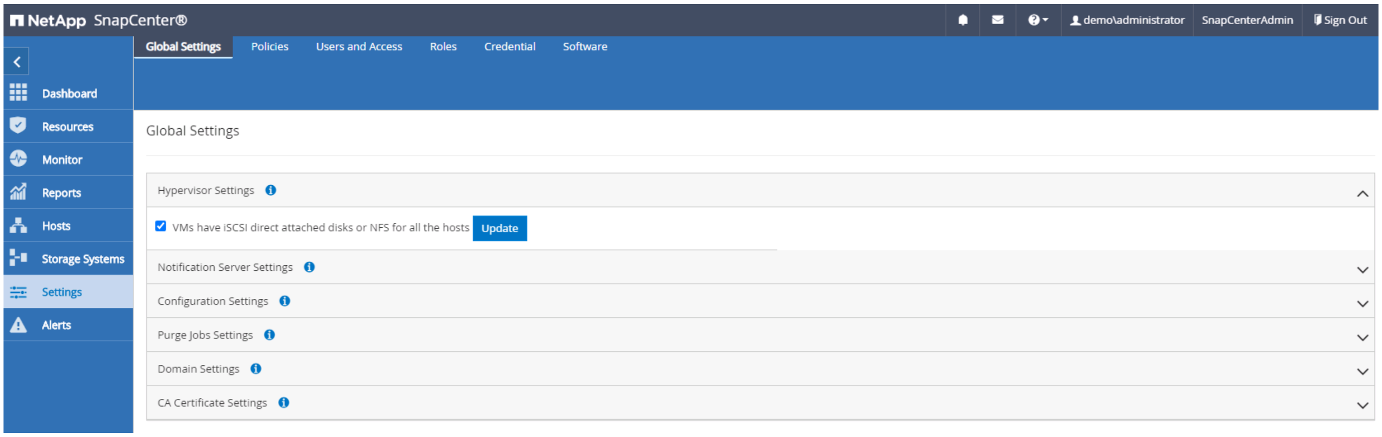
3. SnapCenter host plugin installation

> 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.



Global Settings

Hypervisor Settings

☑ VMs have iSCSI direct attached disks or NFS for all the hosts

Notification Server Settings

Configuration Settings

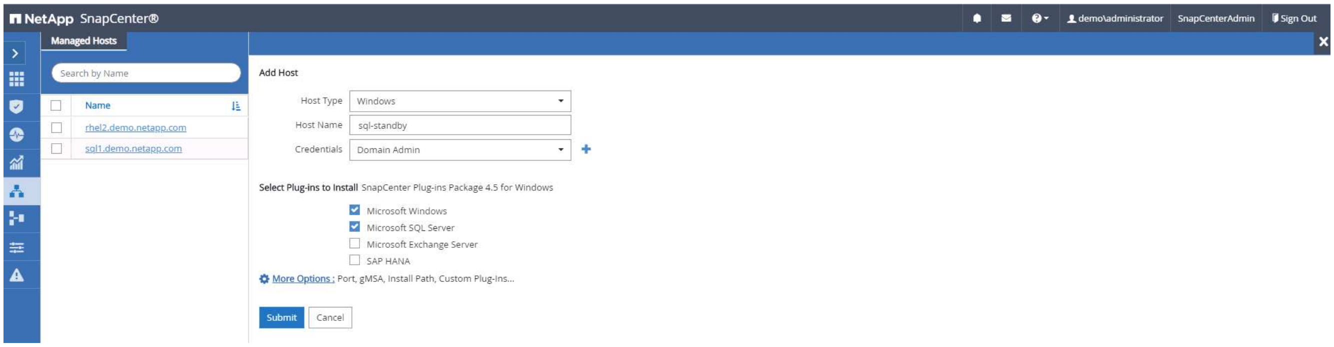
Purge Jobs Settings

Domain Settings

CA Certificate Settings

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.



□	Name
□	rhel2.demo.netapp.com
□	sql1.demo.netapp.com

Add Host

Host Type: Windows

Host Name: sql-standby

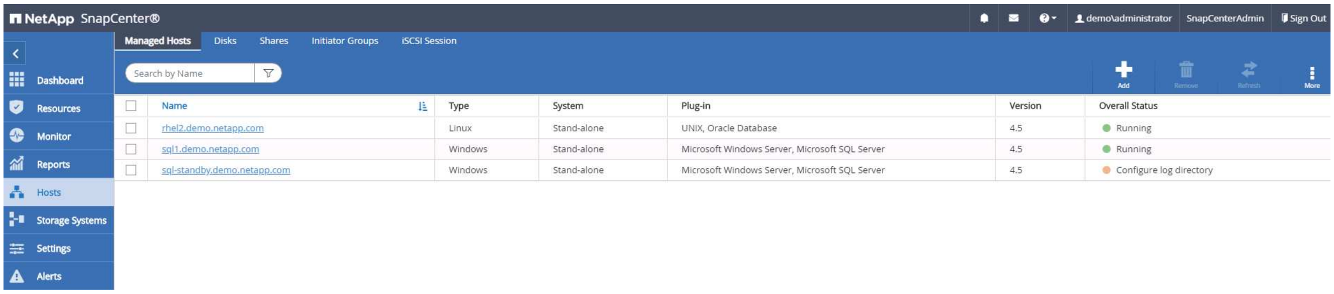
Credentials: Domain Admin

Select Plug-ins to Install SnapCenter Plug-ins Package 4.5 for Windows

☑ Microsoft Windows
☑ Microsoft SQL Server
□ Microsoft Exchange Server
□ SAP HANA

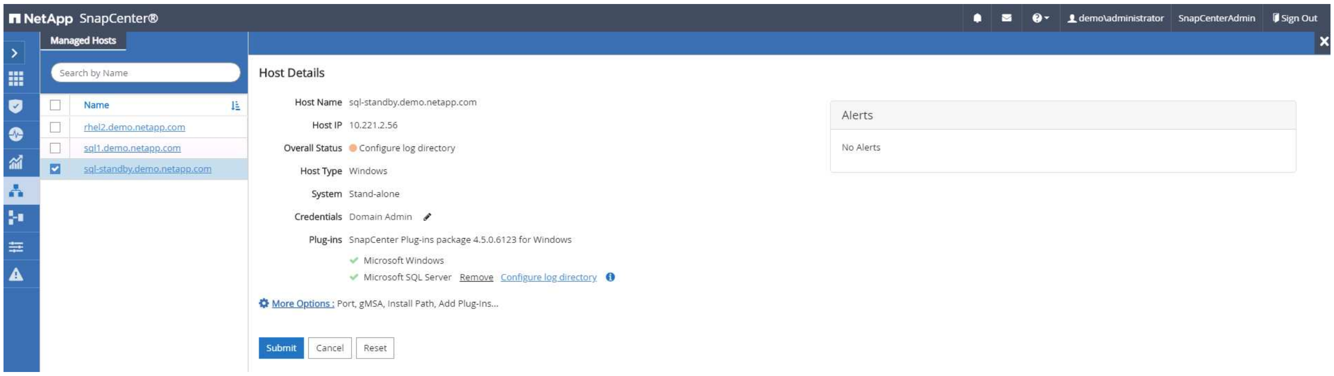
More Options : Port, gMSA, Install Path, Custom Plug-Ins...

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.



□	Name
□	rhel2.demo.netapp.com
□	sql1.demo.netapp.com
☑	sql-standby.demo.netapp.com

Host Details

Host Name: sql-standby.demo.netapp.com

Host IP: 10.221.2.56

Overall Status: ● Configure log directory

Host Type: Windows

System: Stand-alone

Credentials: Domain Admin

Plug-ins: SnapCenter Plug-ins package 4.5.0.6123 for Windows

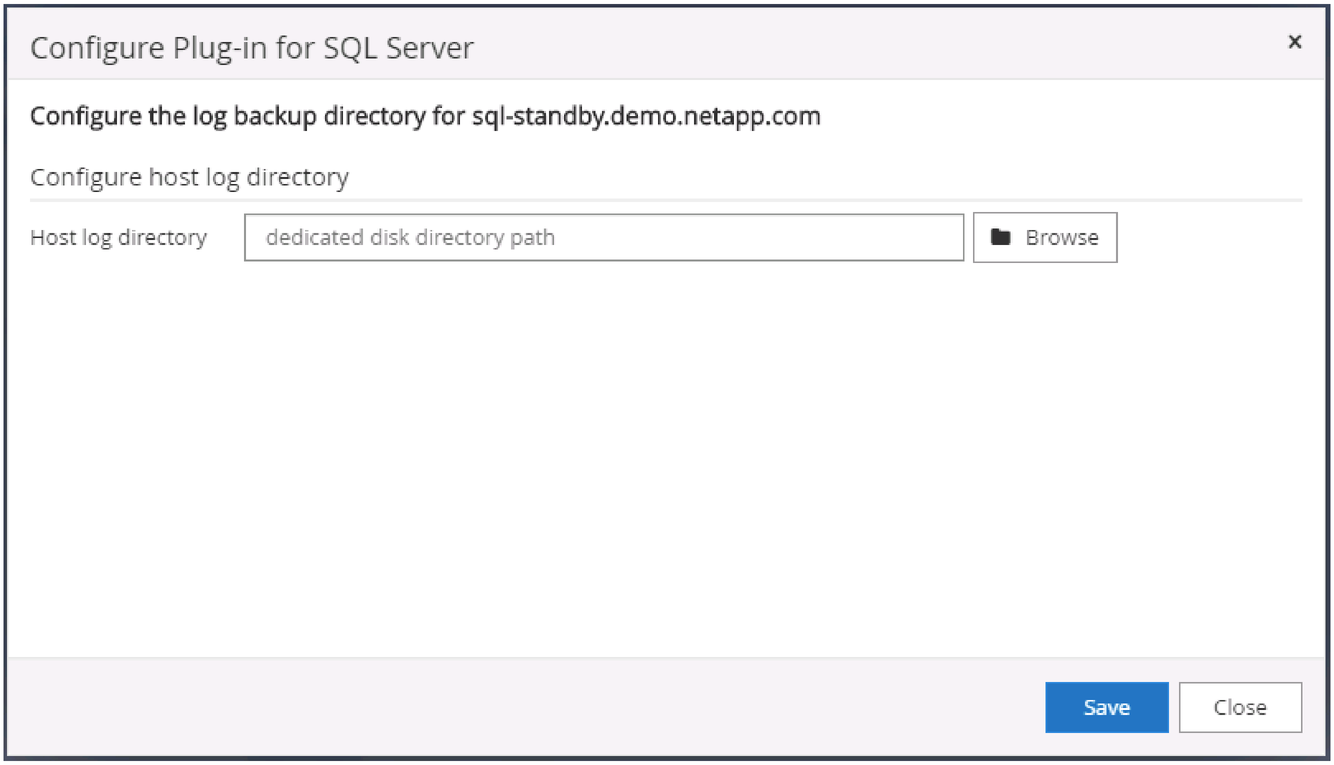
✓ Microsoft Windows
✓ Microsoft SQL Server Remove Configure log directory

More Options : Port, gMSA, Install Path, Add Plug-ins...

Alerts

No Alerts

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



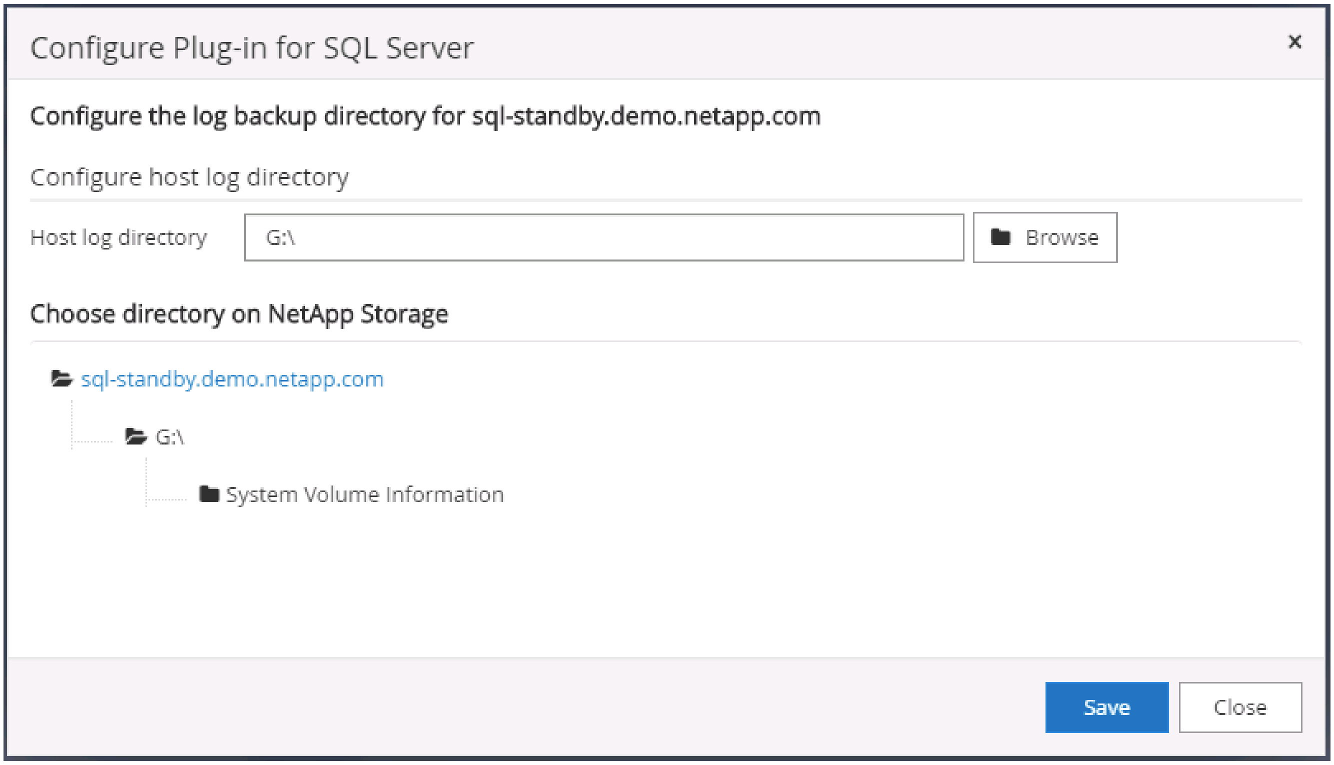
Configure Plug-in for SQL Server

Configure the log backup directory for sql-standby.demo.netapp.com

Configure host log directory

Host log directory: dedicated disk directory path

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.



Configure Plug-in for SQL Server

Configure the log backup directory for sql-standby.demo.netapp.com

Configure host log directory

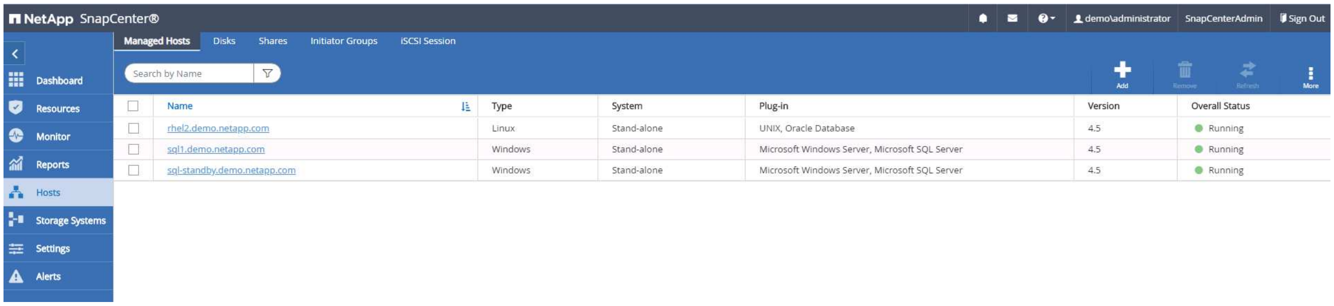
Host log directory: G:\

Choose directory on NetApp Storage

sql-standby.demo.netapp.com
G:\
System Volume Information

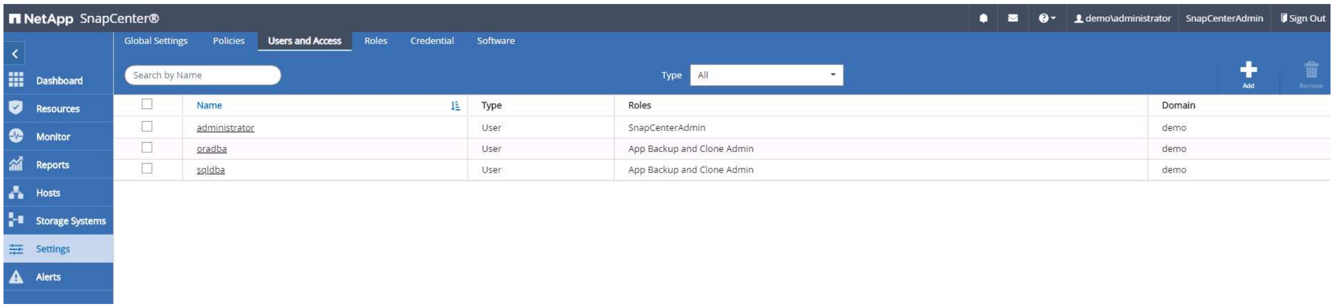
For NetApp storage provisioned to a DB host to be discovered, the storage (on-prem or CVO) must be added to SnapCenter, as illustrated in step 6 for CVO as an example.

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



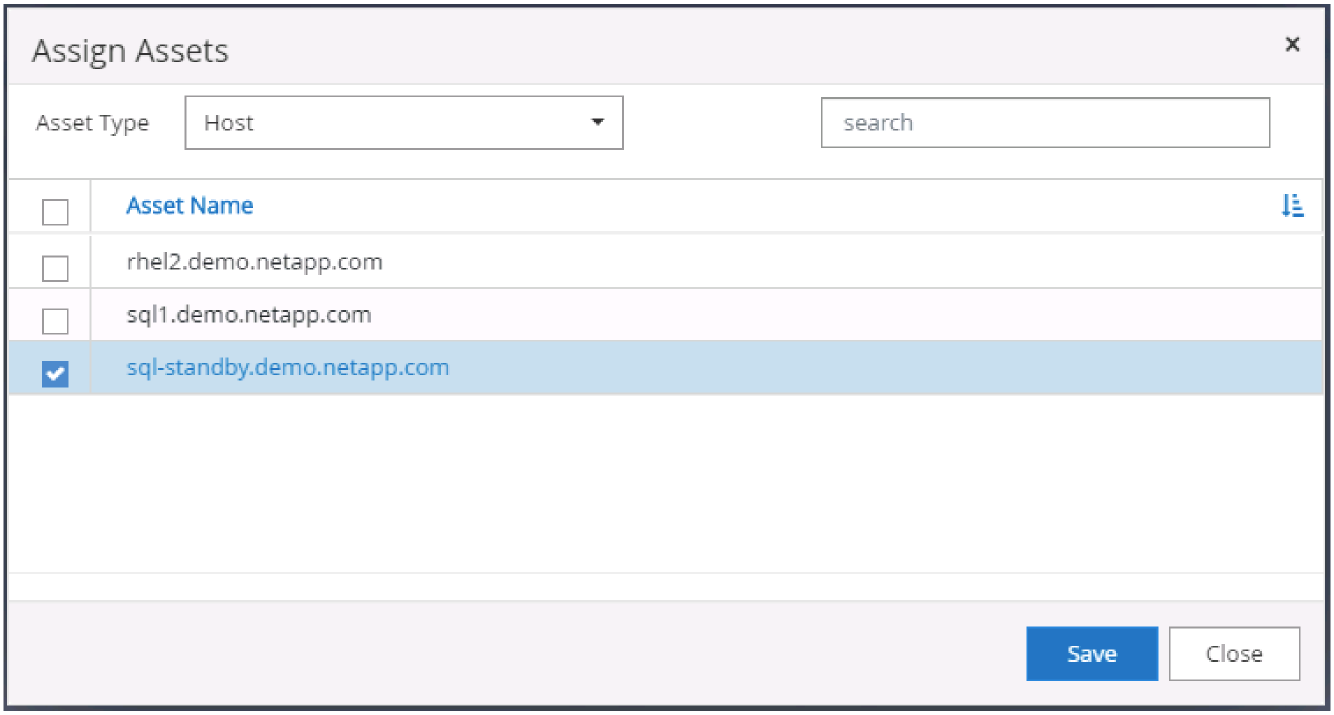
	Name	Type	System	Plug-in	Version	Overall Status
□	rhel2.demo.netapp.com	Linux	Stand-alone	UNIX, Oracle Database	4.5	● Running
□	sql1.demo.netapp.com	Windows	Stand-alone	Microsoft Windows Server, Microsoft SQL Server	4.5	● Running
□	sql-standby.demo.netapp.com	Windows	Stand-alone	Microsoft Windows Server,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



Type: All

	Name	Type	Roles	Domain
□	administrator	User	SnapCenterAdmin	demo
□	oradba	User	App Backup and Clone Admin	demo
□	sqldba	User	App Backup and Clone Admin	demo



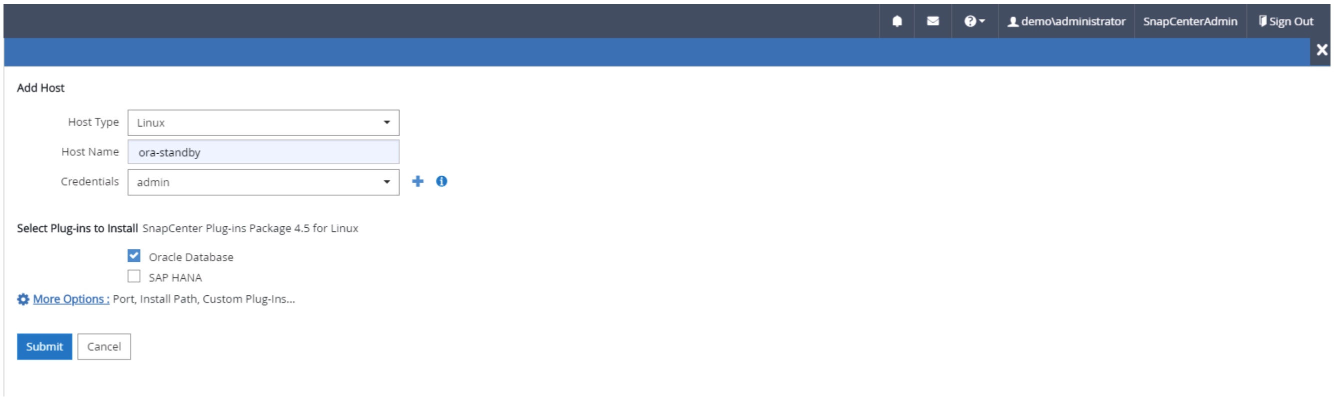
Assign Assets

Asset Type: Host

	Asset Name
□	rhel2.demo.netapp.com
□	sql1.demo.netapp.com
☑	sql-standby.demo.netapp.com

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

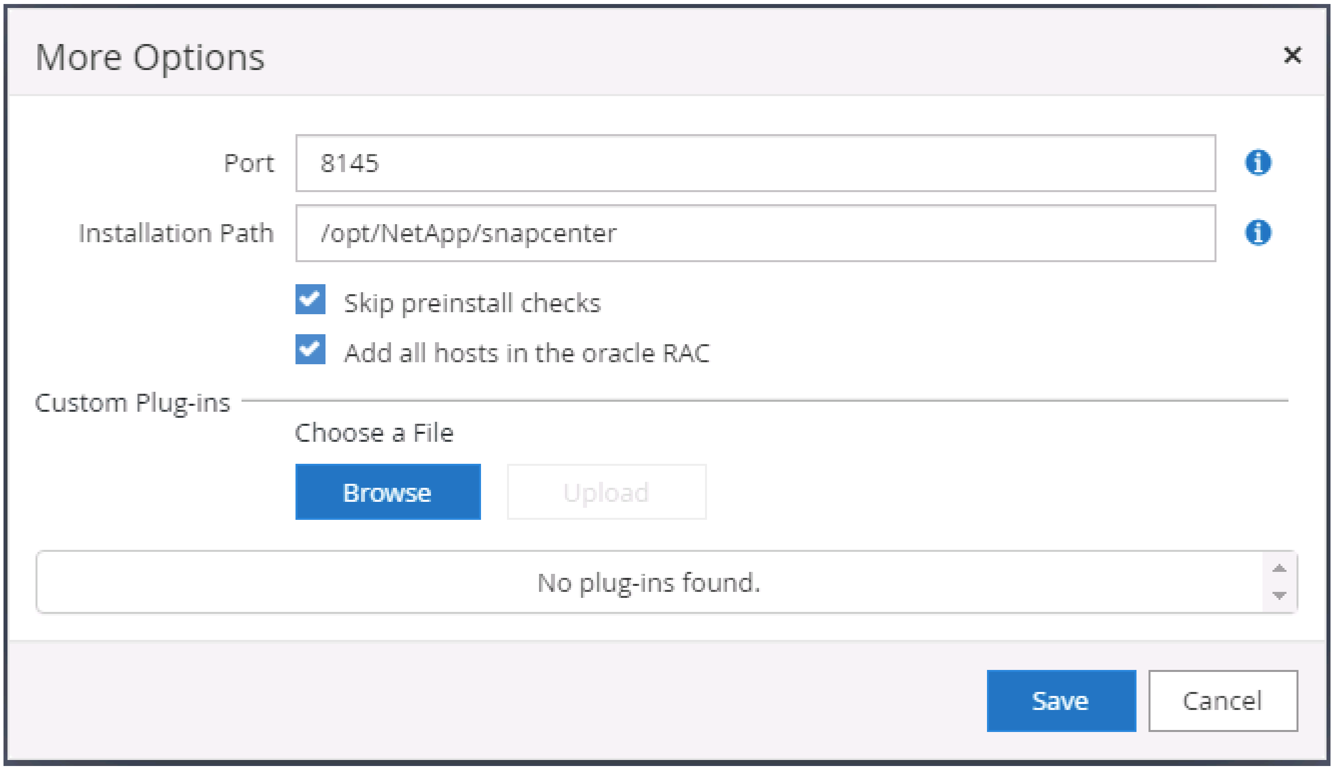
Select Plug-ins to Install SnapCenter Plug-ins Package 4.5 for Linux

☑ Oracle Database

□ SAP HANA

More Options : Port, Install Path, Custom Plug-ins...

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

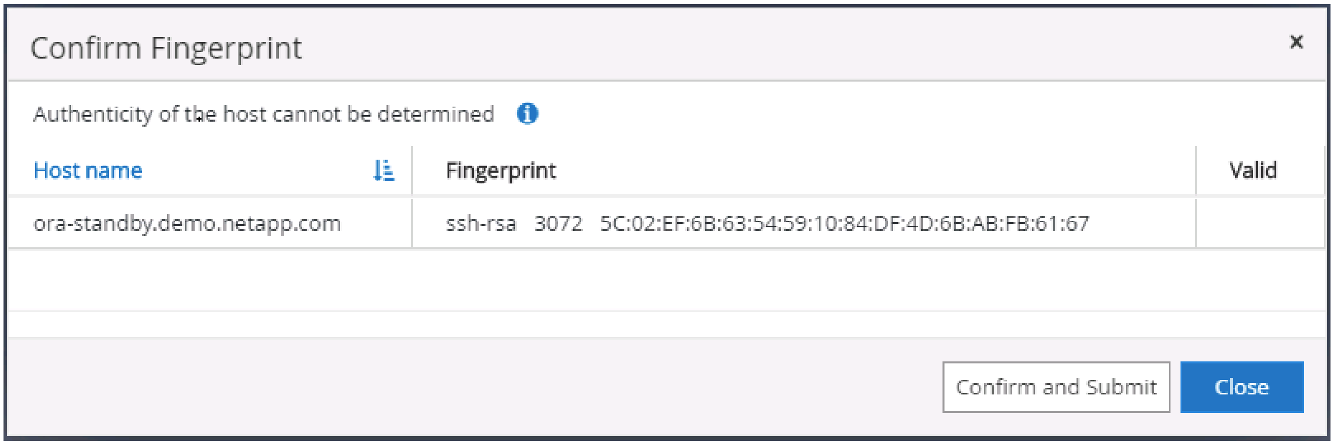
☑ Add all hosts in the oracle RAC

Custom Plug-ins

Choose a File

No plug-ins found.

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

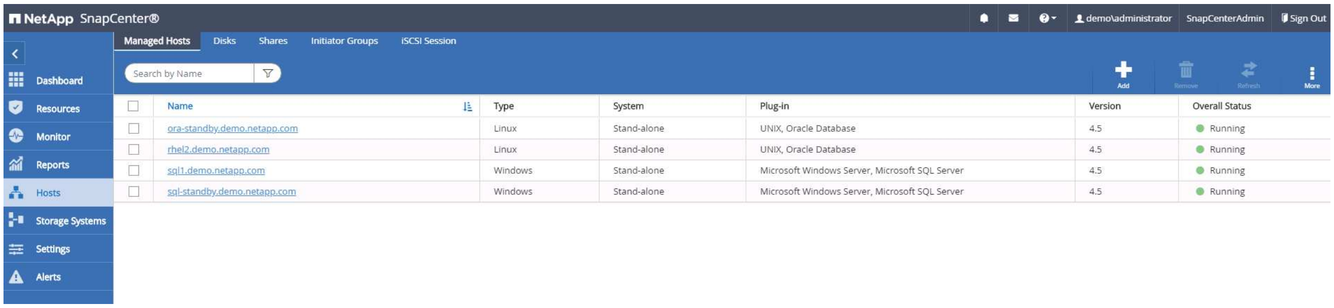


Confirm Fingerprint

Authenticity of the host cannot be determined

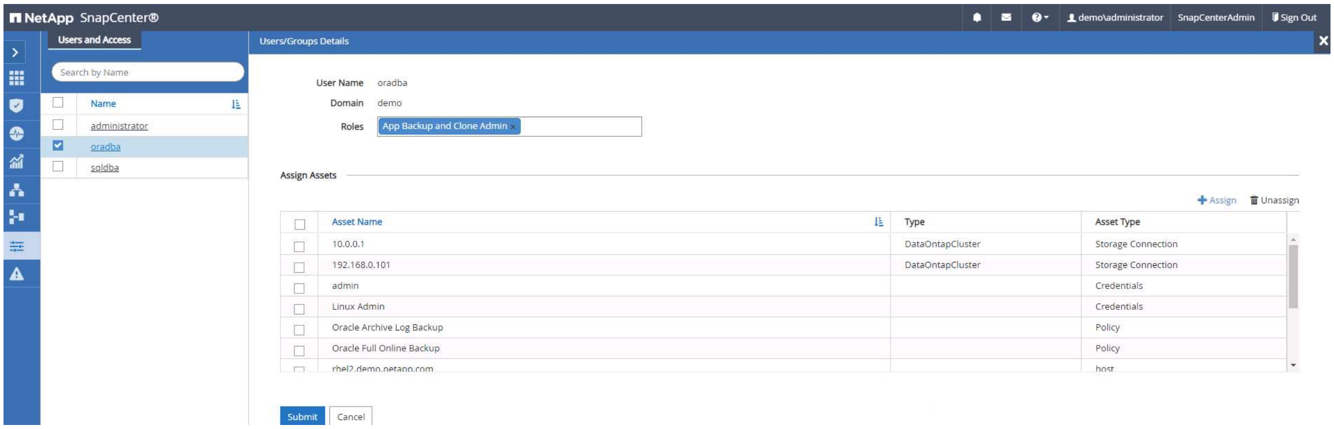
Host name	Fingerprint	Valid
ora-standby.demo.netapp.com	ssh-rsa 3072 5C:02:EF:6B:63:54:59:10:84:DF:4D:6B:AB:FB:61:67	

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).



☐	Name
☐	administrator
☑	oradba
☐	sqldba

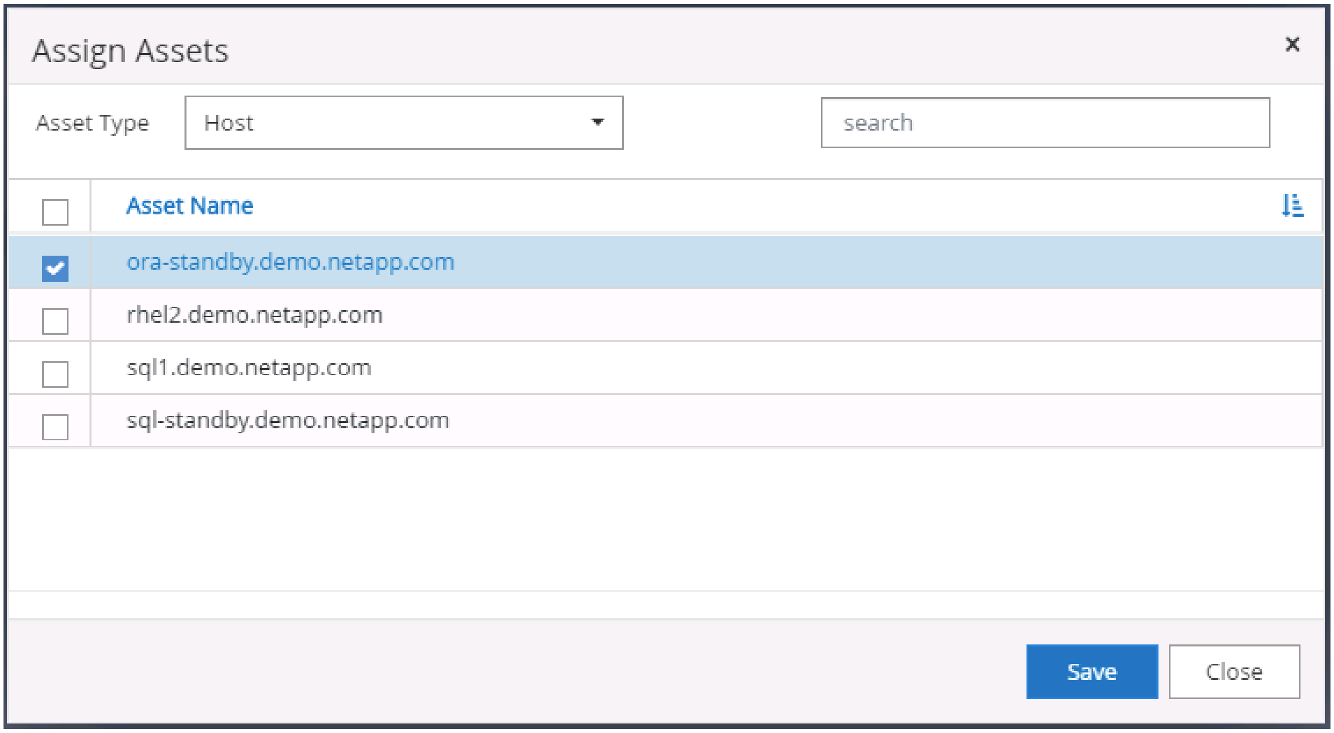
User Name oradba

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		host



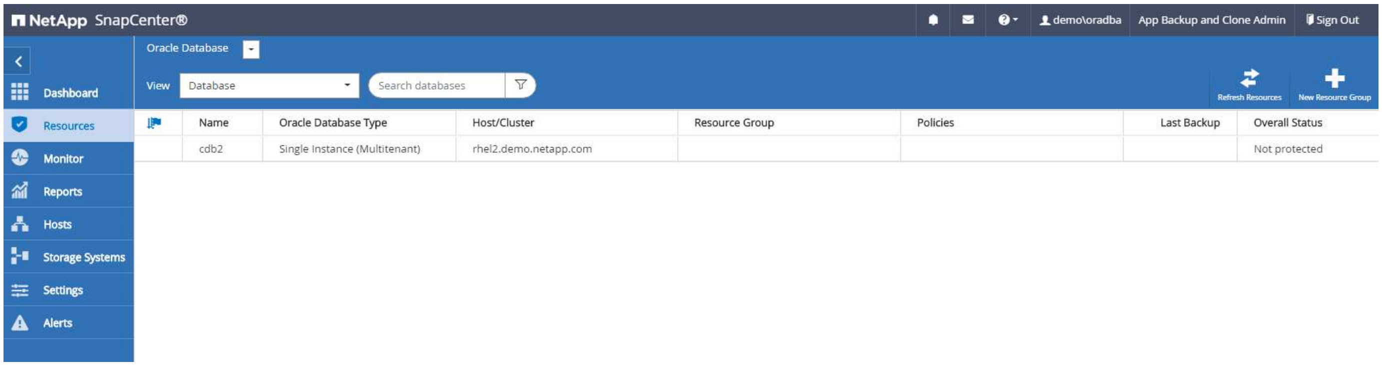
Asset Type Host

search

☐	Asset Name
☑	ora-standby.demo.netapp.com
☐	rhel2.demo.netapp.com
☐	sql1.demo.netapp.com
☐	sql-standby.demo.netapp.com

4. Database resource discovery

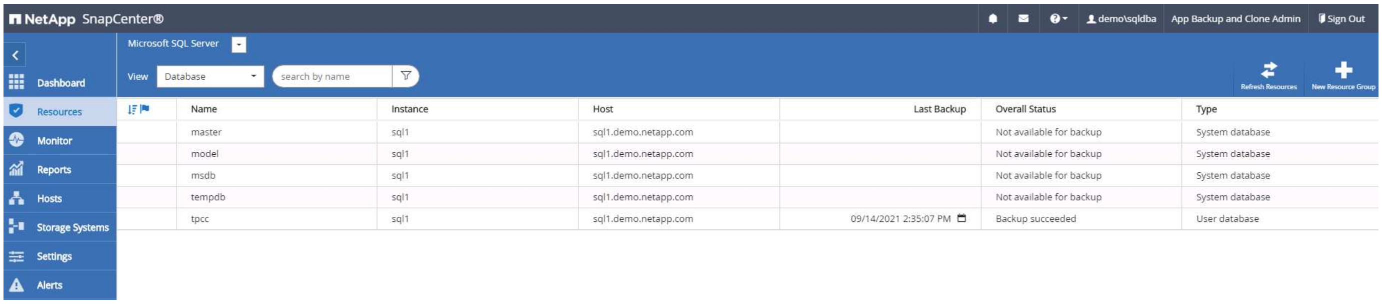
With successful plugin installation, the database resources on the host can be immediately discovered. Click the Resources tab in the left-hand menu. Depending on the type of database platform, a number of views are available, such as the database, resources group, and so on. You might need to click 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
cdb2	Single Instance (Multitenant)	rhel2.demo.netapp.com				Not protected

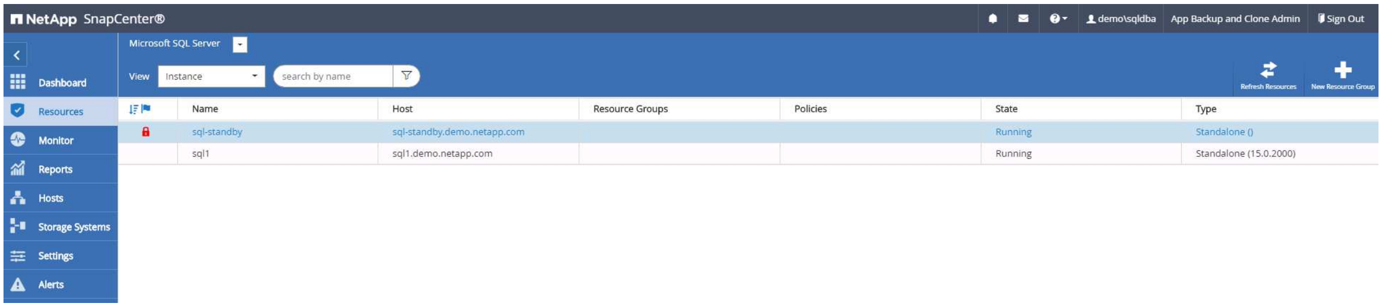
When the database is initially discovered, the Overall Status is shown as "Not protected." The previous screenshot shows an Oracle database not protected yet by a backup policy.

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.

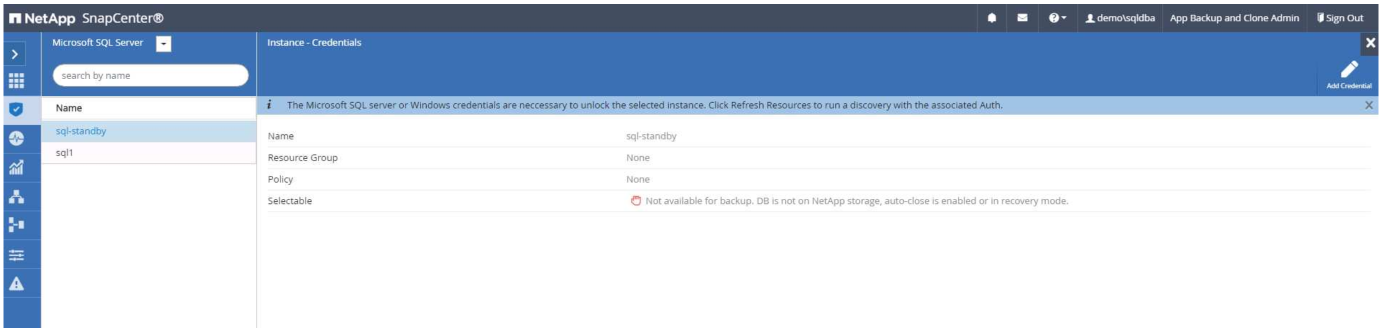


Name	Instance	Host	Last Backup	Overall Status	Type
master	sql1	sql1.demo.netapp.com		Not available for backup	System database
model	sql1	sql1.demo.netapp.com		Not available for backup	System database
msdb	sql1	sql1.demo.netapp.com		Not available for backup	System database
tempdb	sql1	sql1.demo.netapp.com		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)

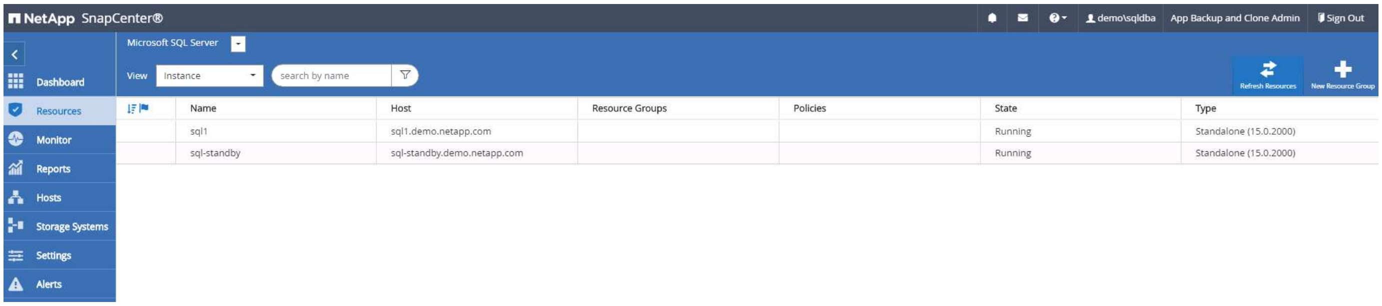


Name
sql-standby
sql1

The Microsoft SQL server or Windows credentials are neccessary to unlock the selected instance. Click Refresh Resources to run a discovery with the associated Auth.

Name	sql-standby
Resource Group	None
Policy	None
Selectable	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.



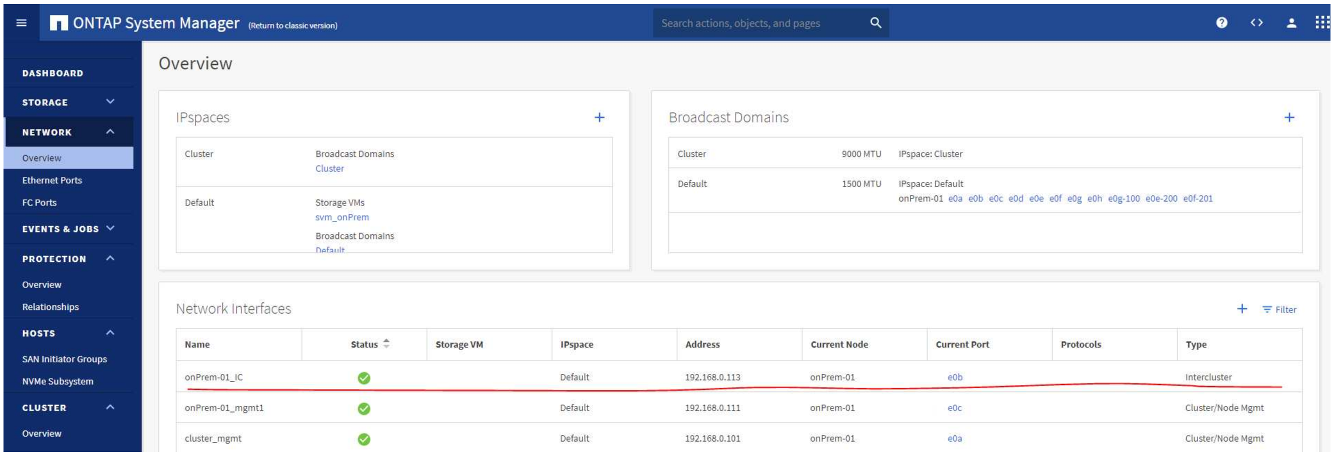
Name	Host	Resource Groups	Policies	State	Type
sql1	sql1.demo.netapp.com			Running	Standalone (15.0.2000)
sql-standby	sql-standby.demo.netapp.com			Running	Standalone (15.0.2000)

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 Manger. A default CVO deployment has inter-cluster LIFs configured automatically.

   On-premises cluster:



IPspaces

Cluster	Broadcast Domains Cluster
Default	Storage VMs svm_onPrem Broadcast Domains Default

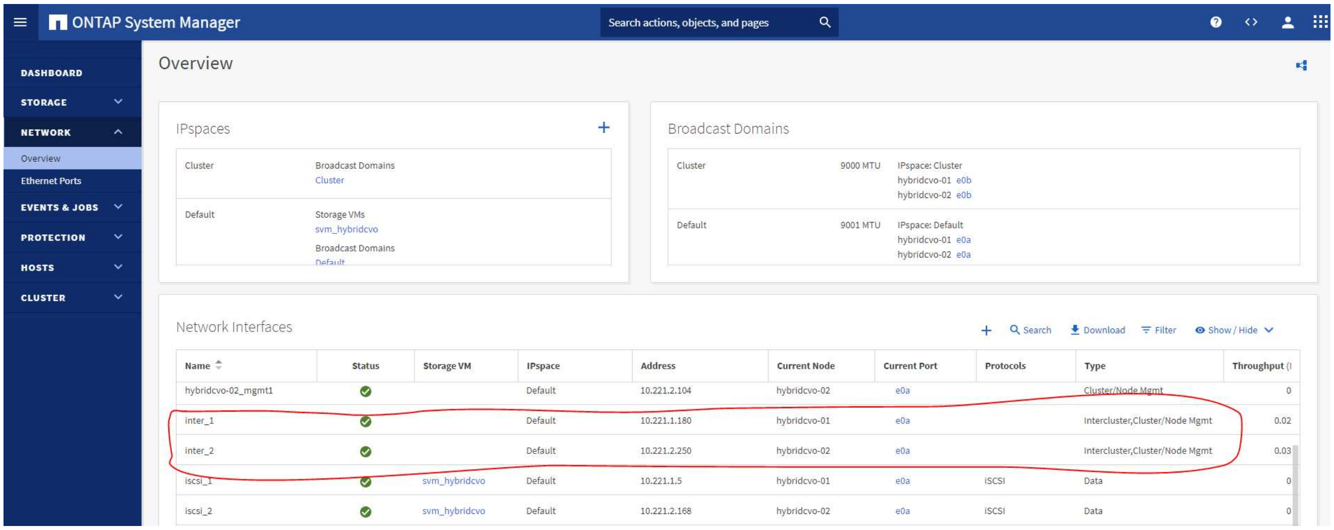
Broadcast Domains

Cluster	9000 MTU	IPspace: Cluster
Default	1500 MTU	IPspace: Default onPrem-01 e0a e0b e0c e0d e0e e0f e0g e0h e0g-100 e0e-200 e0f-201

Network Interfaces

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

   Target CVO cluster:



Overview

IPspaces

Cluster	Broadcast Domains 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

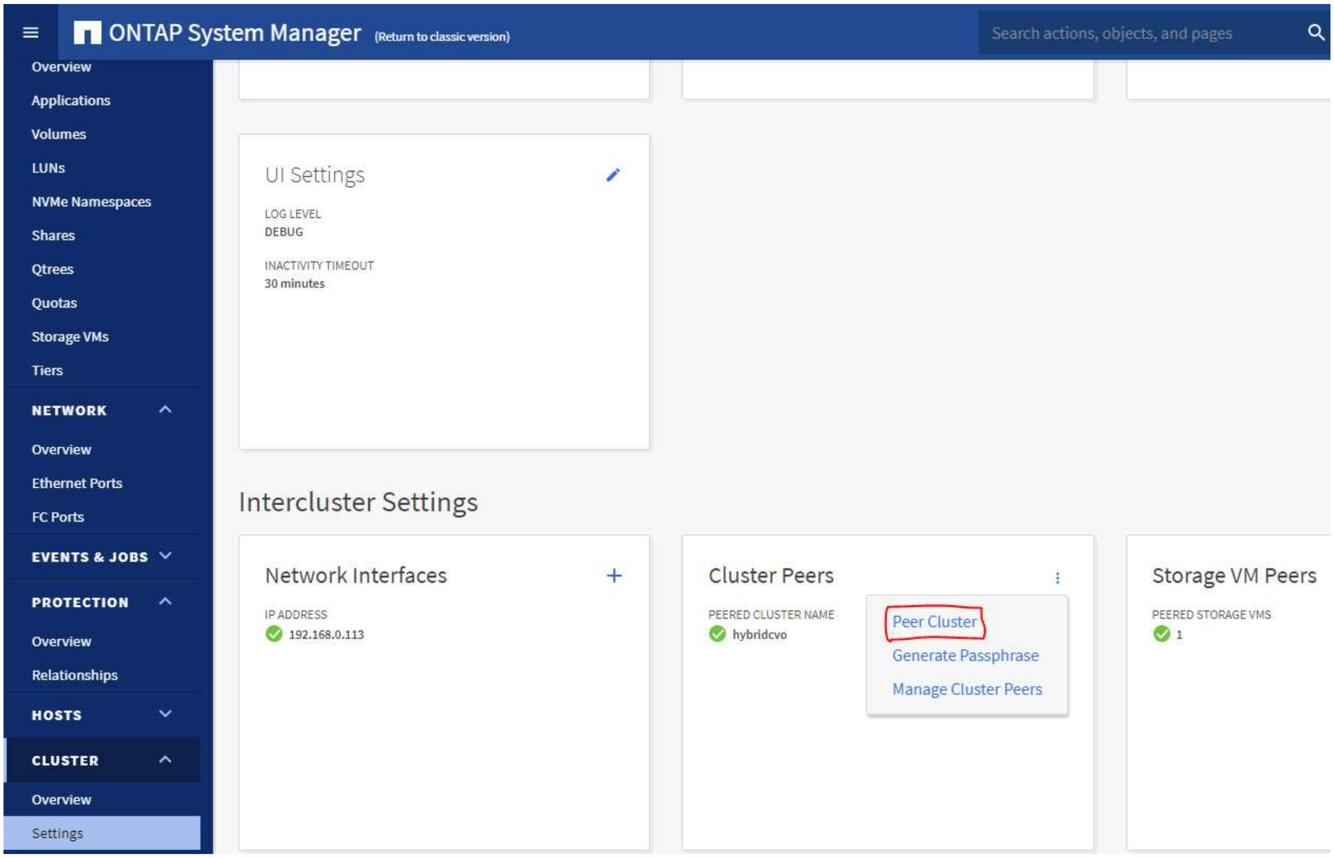
Network Interfaces

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.



UI Settings

LOG LEVEL
DEBUG

INACTIVITY TIMEOUT
30 minutes

Intercluster Settings

Network Interfaces

IP ADDRESS
✓ 192.168.0.113

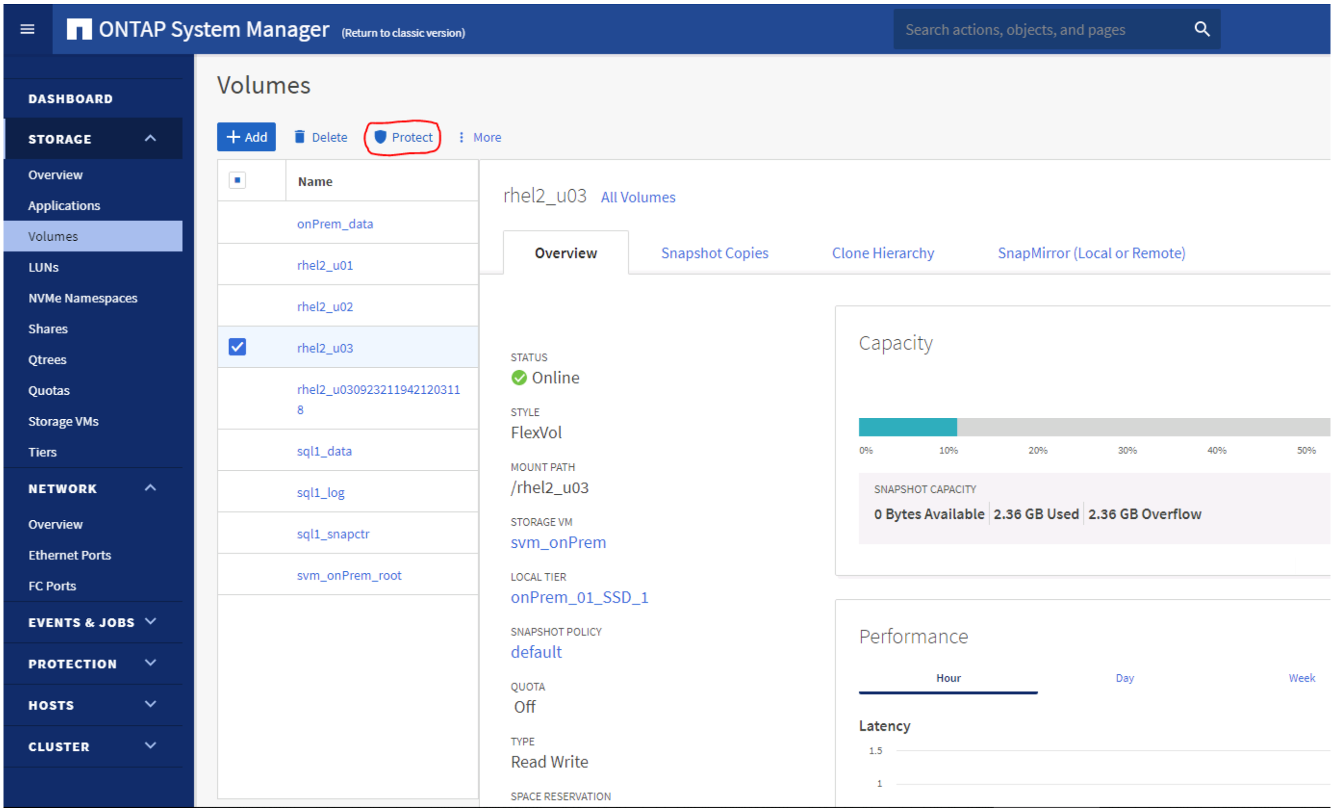
Cluster Peers

PEERED CLUSTER NAME
✓ hybridcvo

Storage VM Peers

PEERED STORAGE VMS
✓ 1

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



Volumes

	Name
	onPrem_data
	rhel2_u01
	rhel2_u02
☑	rhel2_u03
	rhel2_u030923211942120311 8
	sql1_data
	sql1_log
	sql1_snapctr
	svm_onPrem_root

rhel2_u03 All Volumes

STATUS
Online

STYLE
FlexVol

MOUNT PATH
/rhel2_u03

STORAGE VM
svm_onPrem

LOCAL TIER
onPrem_01_SSD_1

SNAPSHOT POLICY
default

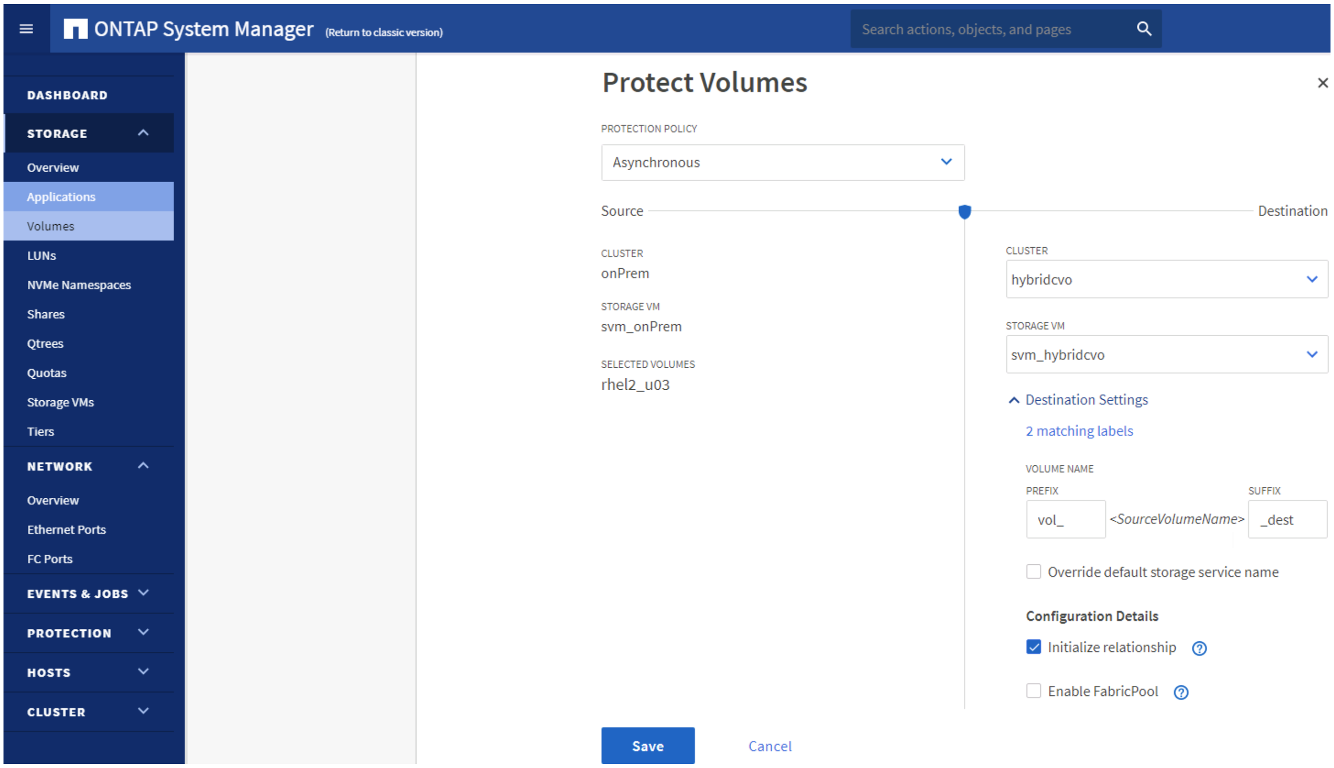
QUOTA
Off

TYPE
Read Write

SPACE RESERVATION

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

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



Protect Volumes

PROTECTION POLICY
Asynchronous

Source — Destination

CLUSTER
onPrem

STORAGE VM
svm_onPrem

SELECTED VOLUMES
rhel2_u03

CLUSTER
hybridcvo

STORAGE VM
svm_hybridcvo

Destination Settings

2 matching labels

VOLUME NAME

PREFIX vol_ <SourceVolumeName> SUFFIX _dest

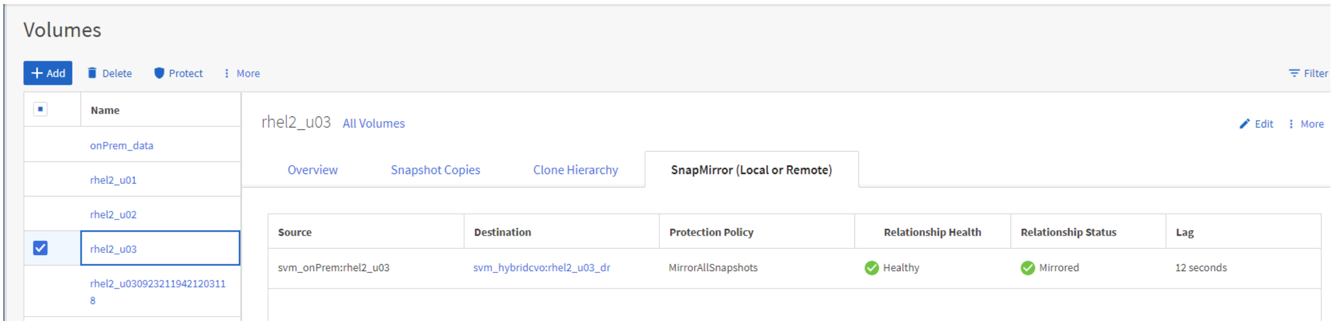
□ Override default storage service name

Configuration Details

☑ Initialize relationship

□ Enable FabricPool

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



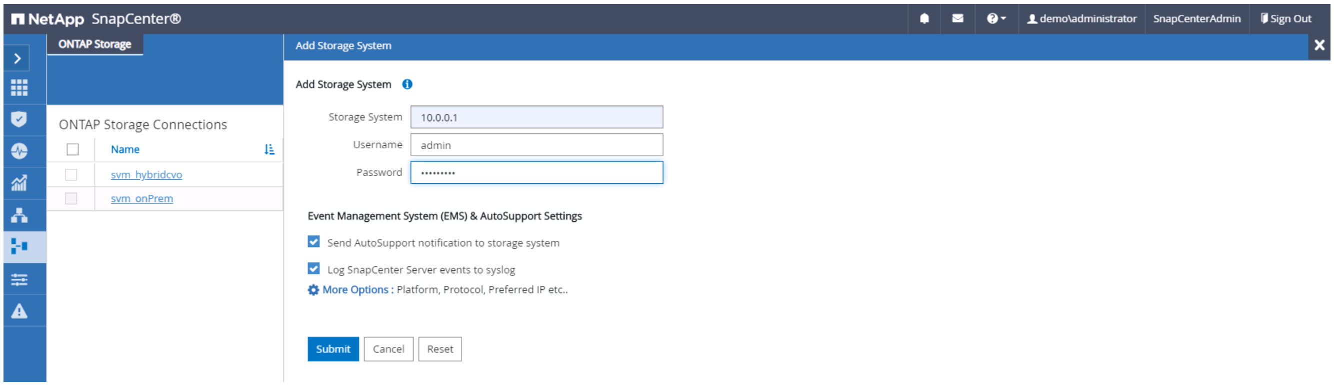
Name
onPrem_data
rhel2_u01
rhel2_u02
☑ rhel2_u03
rhel2_u0309232119421203118

rhel2_u03 All Volumes

Source	Destination	Protection Policy	Relationship Health	Relationship Status	Lag
svm_onPrem:rhel2_u03	svm_hybridcvo:rhel2_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.



□	Name
□	svm_hybridcvo
□	svm_onPrem

Add Storage System

Storage System: 10.0.0.1

Username: admin

Password: ••••••••••

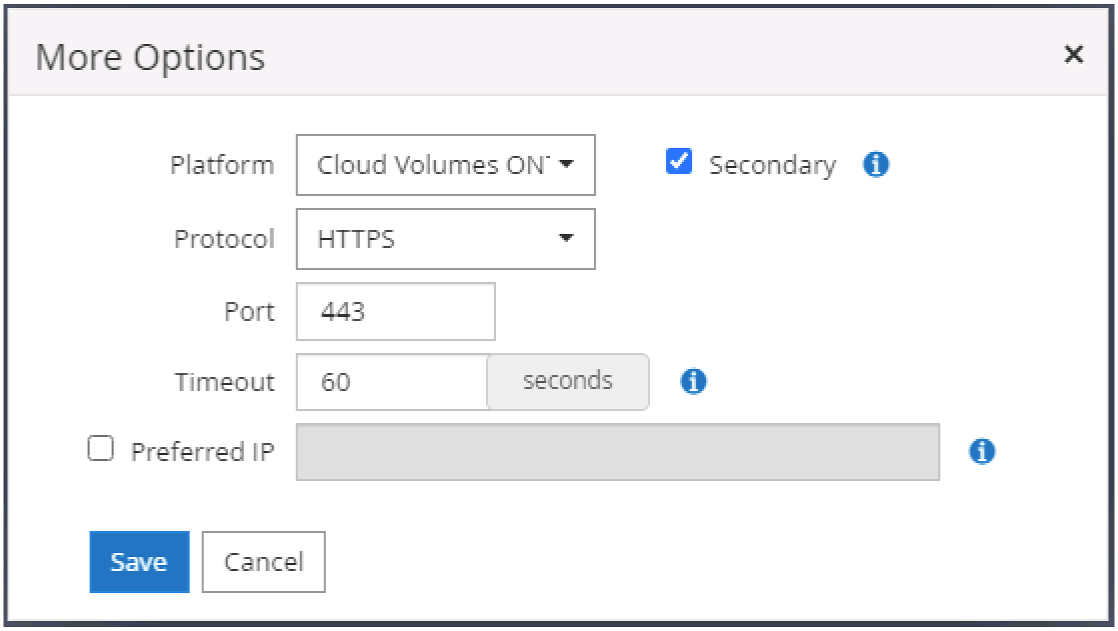
Event Management System (EMS) & AutoSupport Settings

☑ Send AutoSupport notification to storage system

☑ Log SnapCenter Server events to syslog

More Options : Platform, Protocol, Preferred IP etc..

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



Platform: Cloud Volumes ON˙ ☑ Secondary

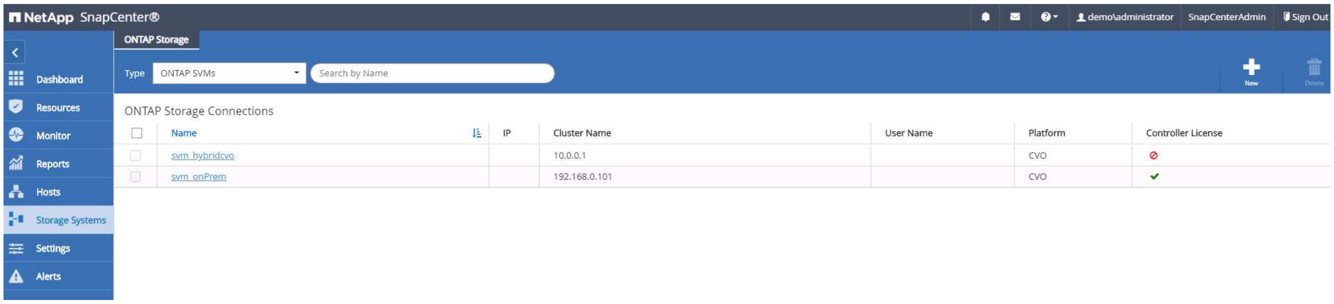
Protocol: HTTPS

Port: 443

Timeout: 60 seconds

□ Preferred IP

4. Assign the storage systems to SnapCenter database management user IDs as shown in 3. SnapCenter host plugin installation.



ONTAP Storage Connections

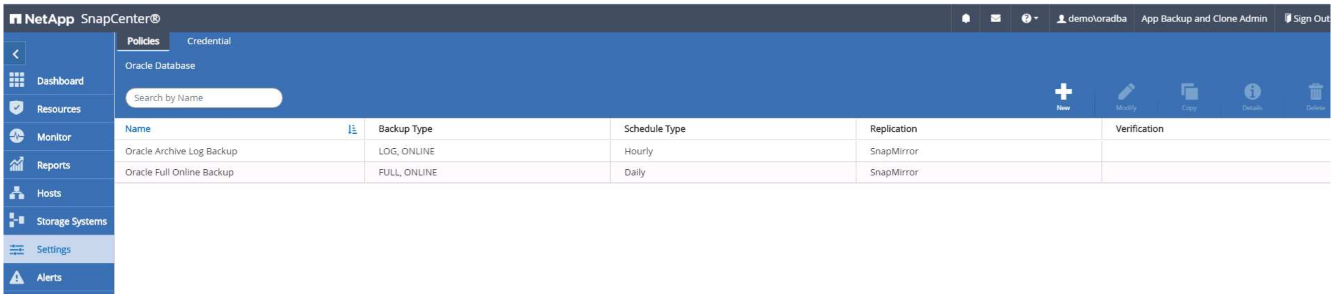
	Name	IP	Cluster Name	User Name	Platform	Controller License
□	svm_hybridcvo		10.0.0.1		CVO	⊘
□	svm_onPrem		192.168.0.101		CVO	✓

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

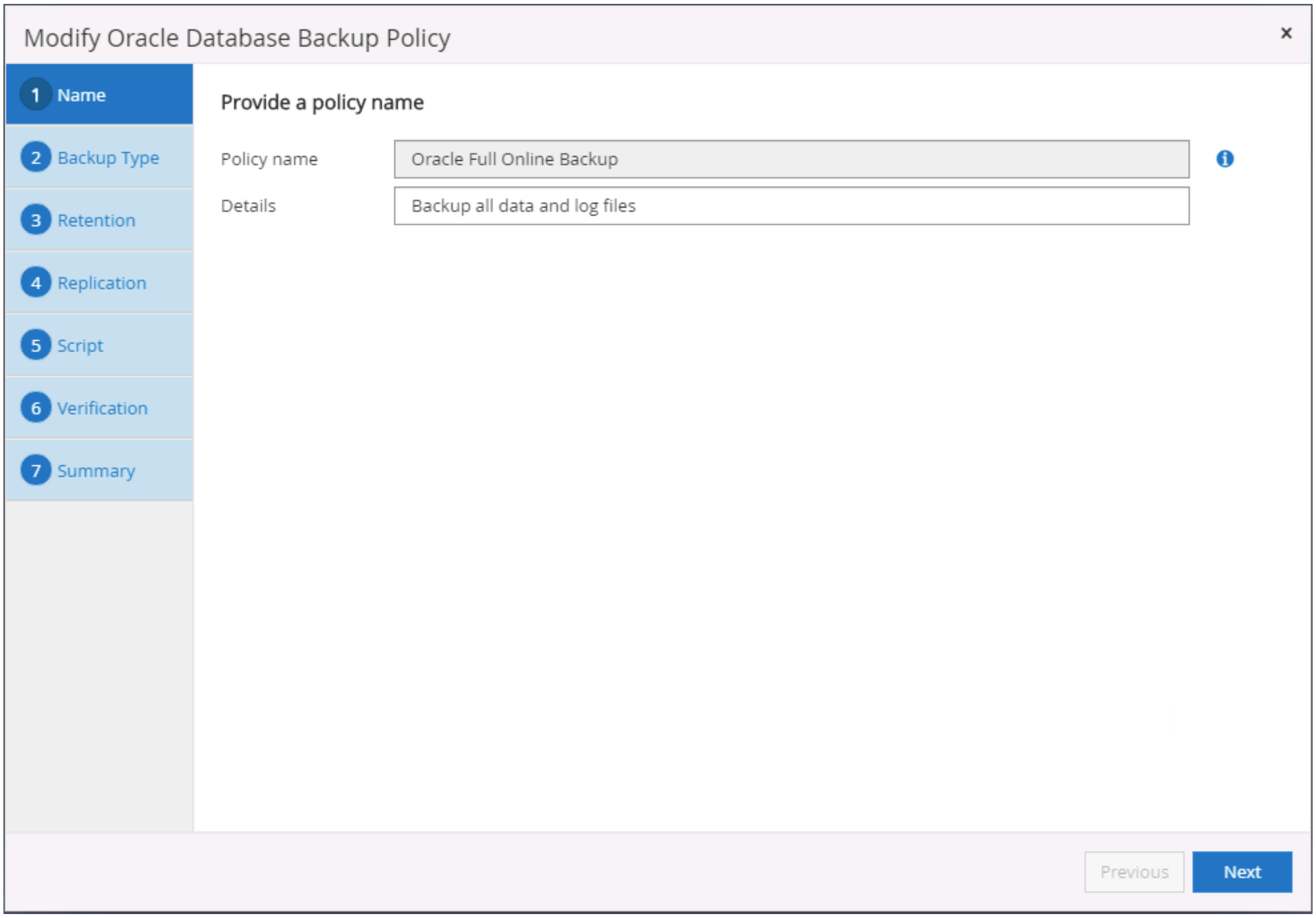
1. Log into SnapCenter as a database management user ID, click Settings, and then click Polices.



Oracle Database

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.



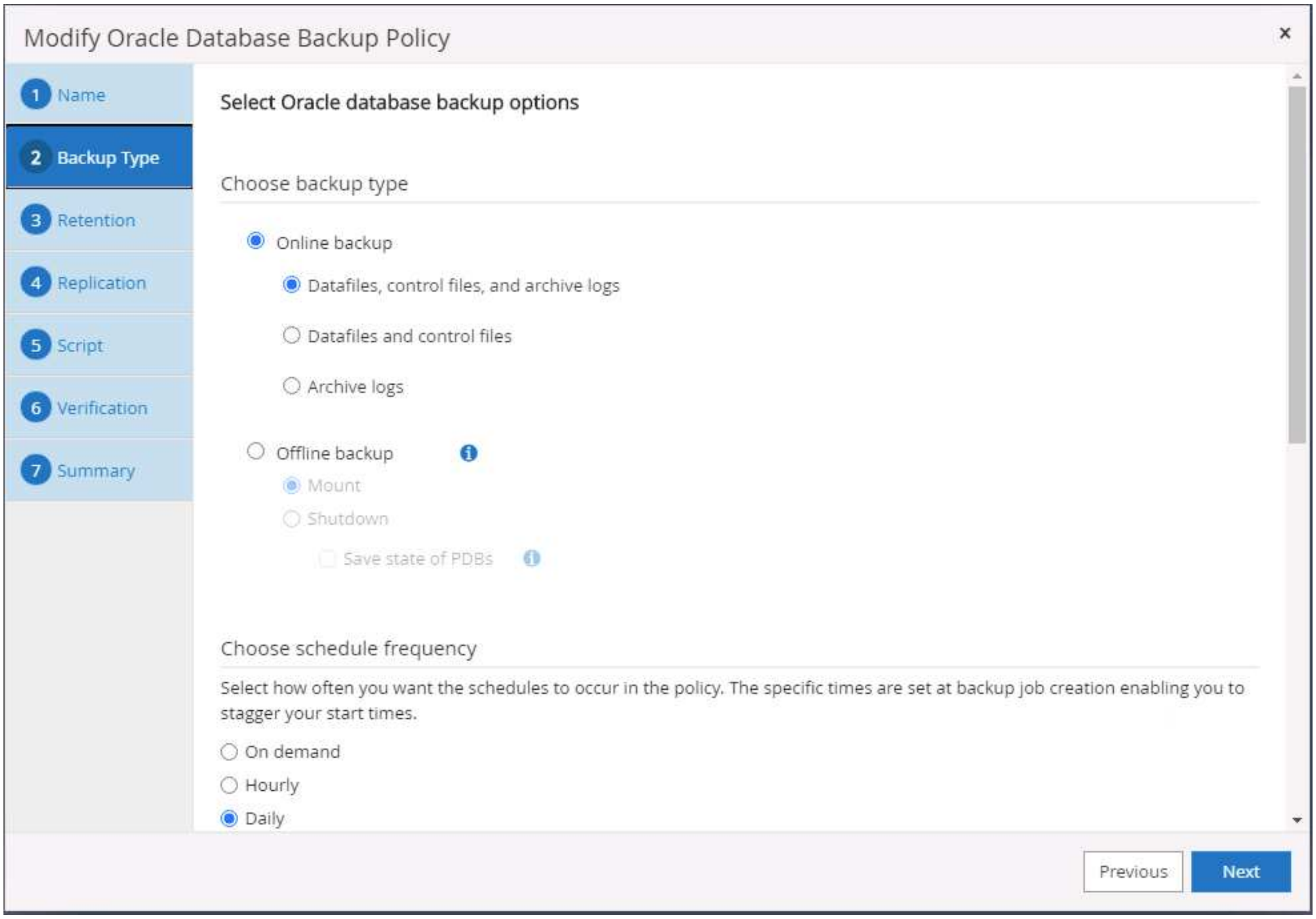
Modify Oracle Database Backup Policy

Provide a policy name

Policy name: Oracle Full Online Backup

Details: Backup all data and log files

3. Select the backup type and schedule frequency.



Modify Oracle Database Backup Policy

Select Oracle database backup options

Choose backup type

● Online backup

● Datafiles, control files, and archive logs

○ Datafiles and control files

○ Archive logs

○ Offline backup

● Mount

○ Shutdown

□ Save state of PDBs

Choose schedule frequency

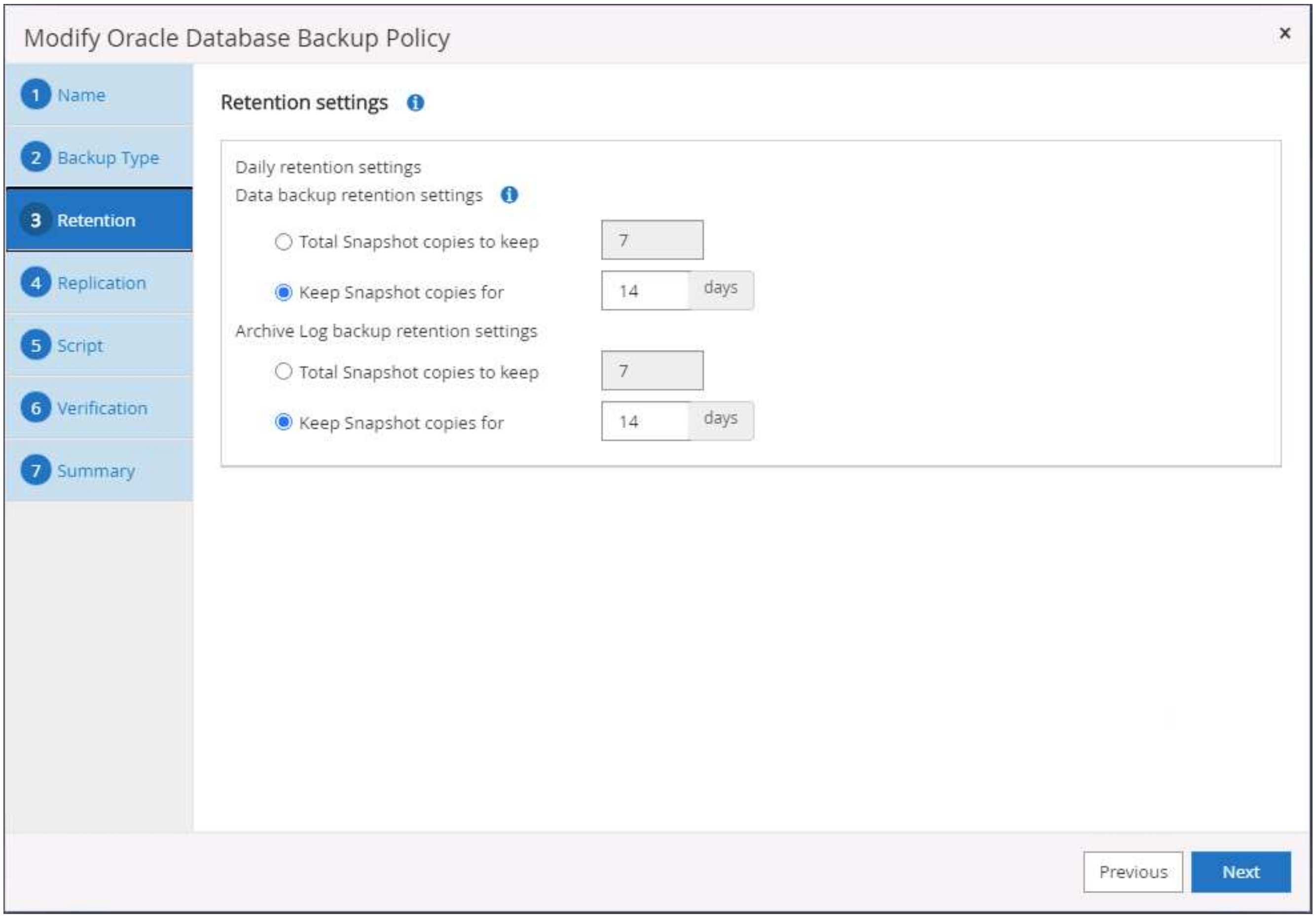
Select how often you want the schedules to occur in the policy. The specific times are set at backup job creation enabling you to stagger your start times.

○ On demand

○ Hourly

● Daily

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


Modify Oracle Database Backup Policy

Retention settings

Daily retention settings

Data backup retention settings

○ Total Snapshot copies to keep 7

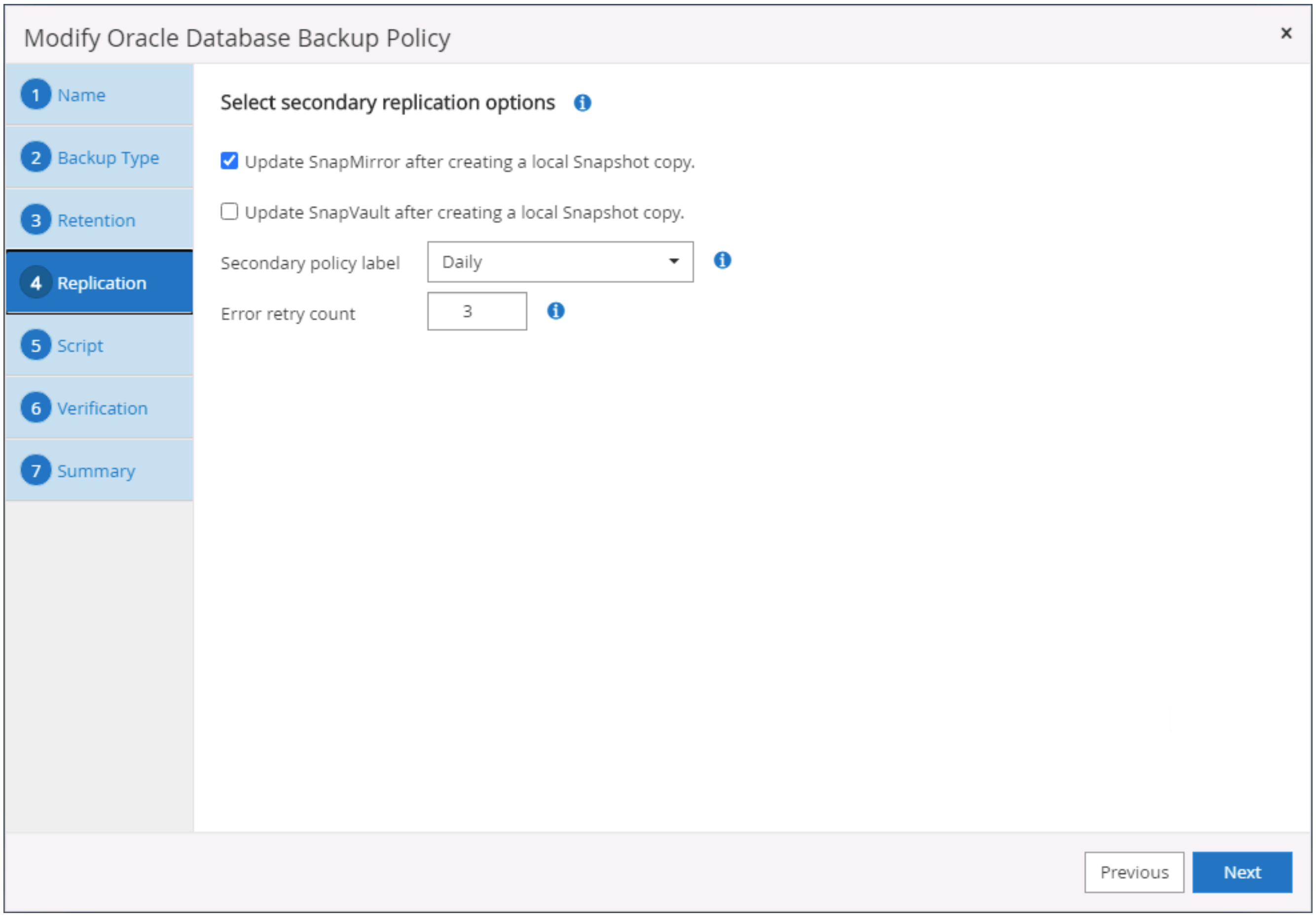
● Keep Snapshot copies for 14 days

Archive Log backup retention settings

○ Total Snapshot copies to keep 7

● Keep Snapshot copies for 14 days

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

Select secondary replication options

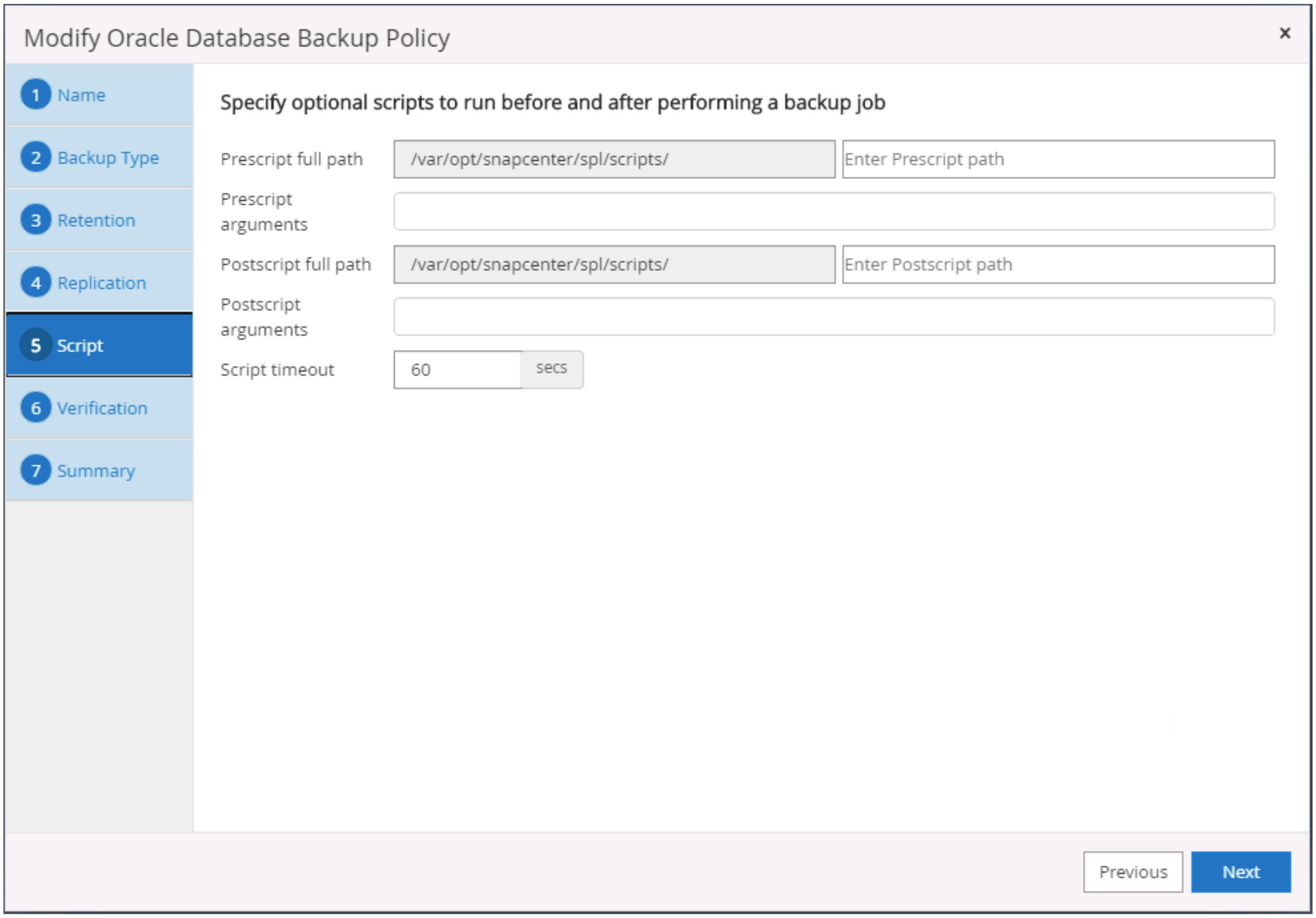
☑ Update SnapMirror after creating a local Snapshot copy.

□ Update SnapVault after creating a local Snapshot copy.

Secondary policy label: Daily

Error retry count: 3

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



Modify Oracle Database Backup Policy

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

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

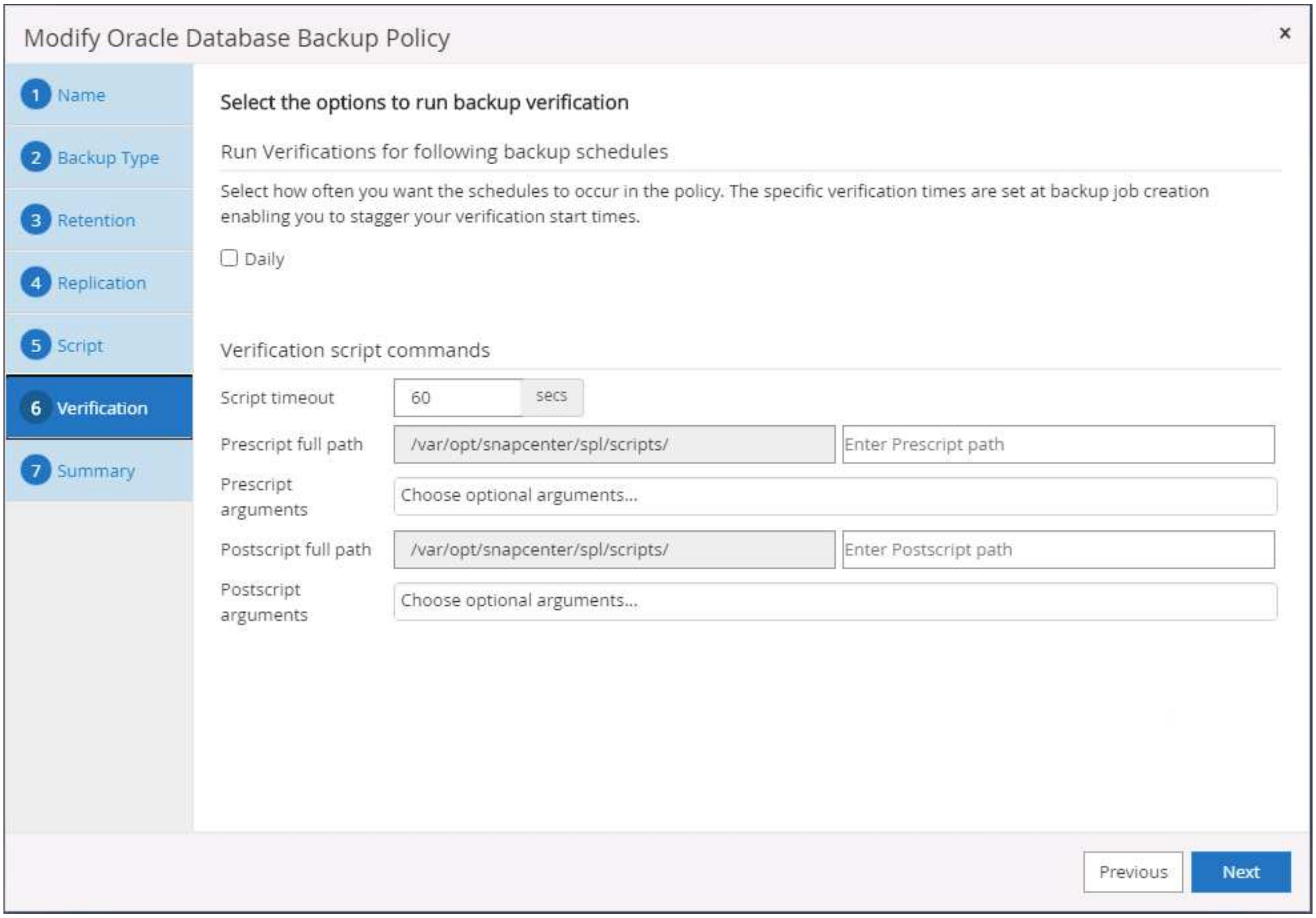
Prescript arguments:

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

Postscript arguments:

Script timeout: 60 secs

7. Run backup verification if desired.


Modify Oracle Database Backup Policy

Select the options to run backup verification

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

Verification script commands

Script timeout: 60 secs

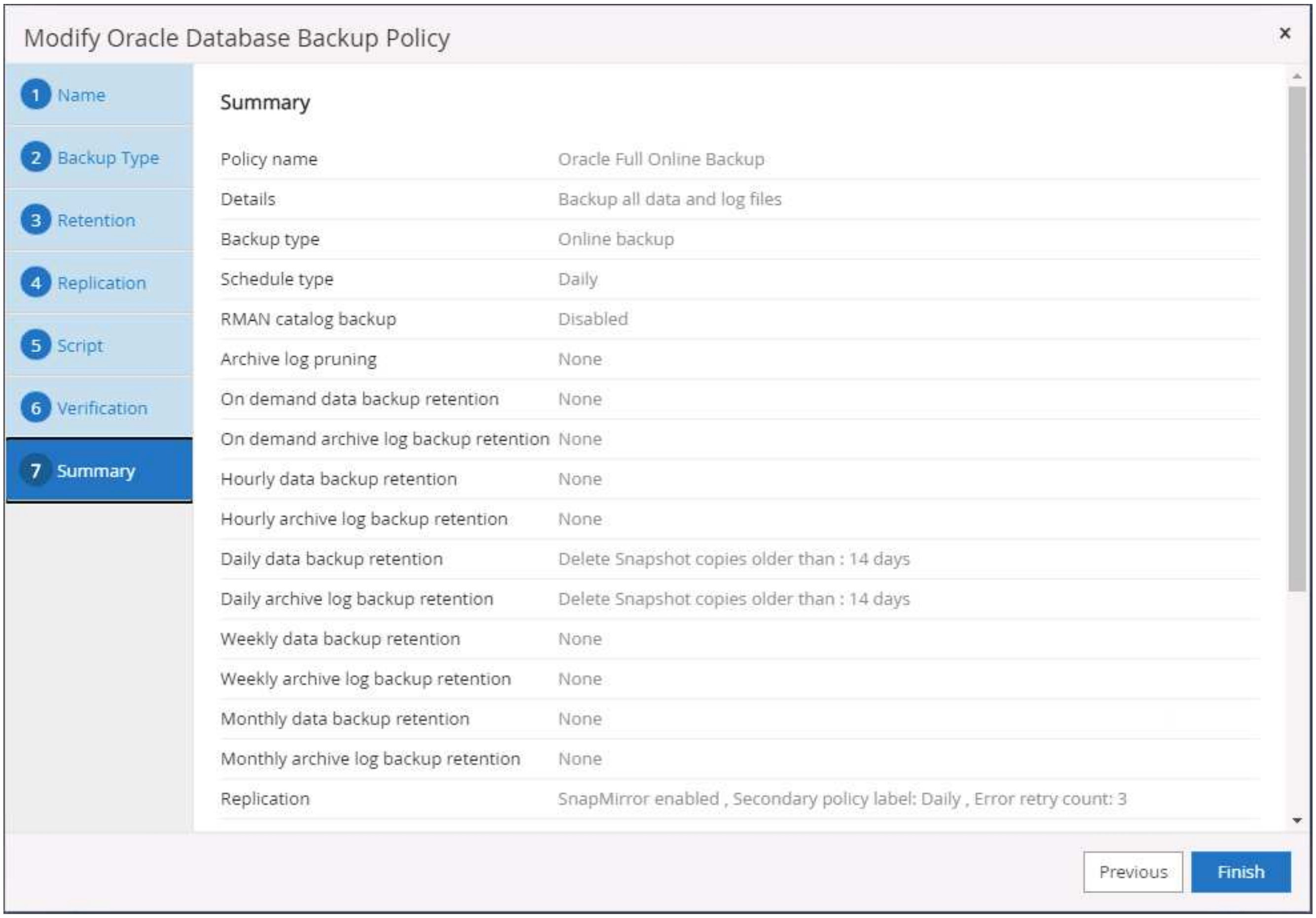
Prescript full path: /var/opt/snapcenter/spl/scripts/ Enter Prescript path

Prescript arguments: Choose optional arguments...

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

Postscript arguments: Choose optional arguments...

8. Summary.

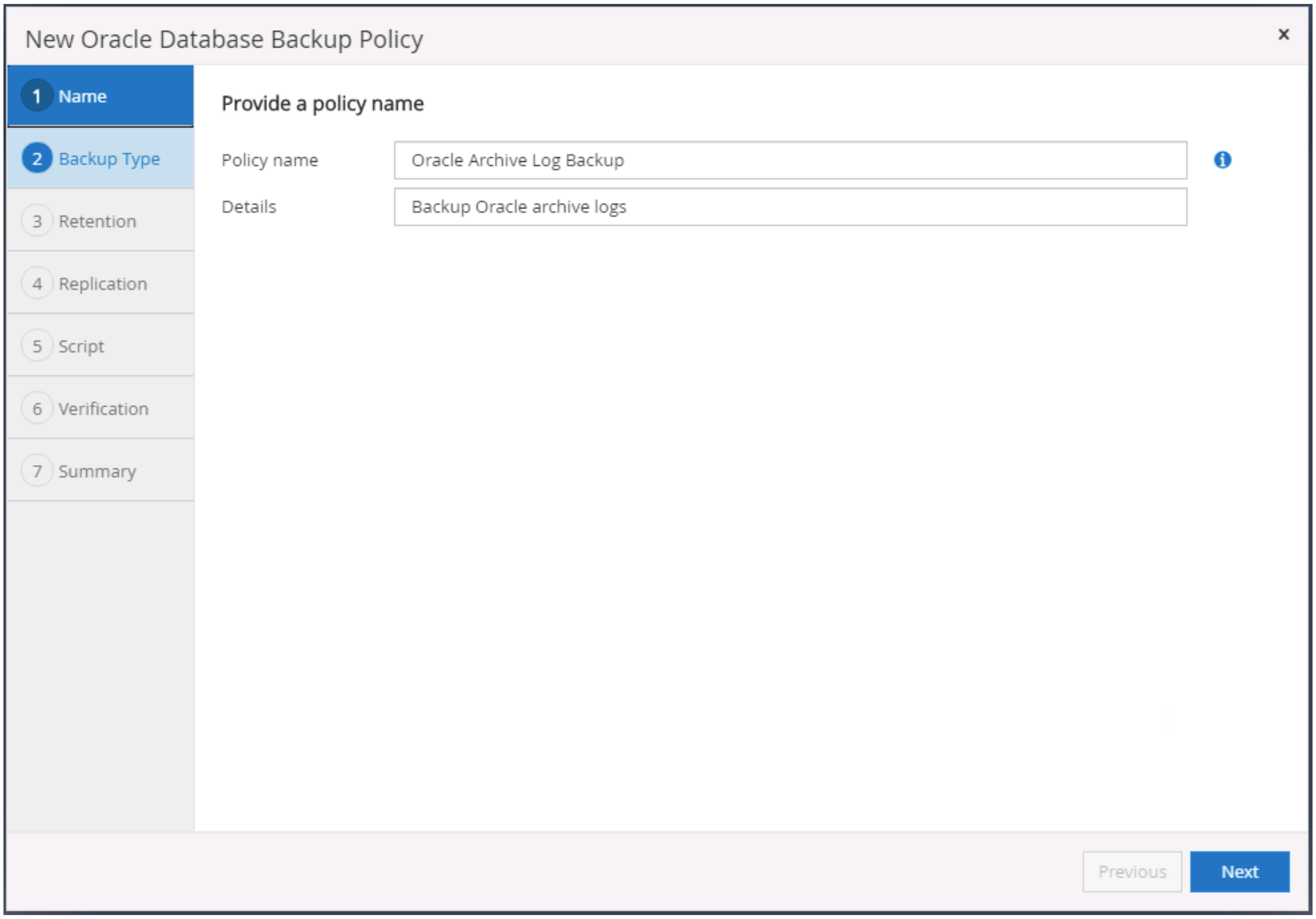


Summary

Policy name	Oracle Full Online Backup
Details	Backup all data and log files
Backup type	Online backup
Schedule type	Daily
RMAN catalog backup	Disabled
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

Create a database log backup policy for Oracle

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



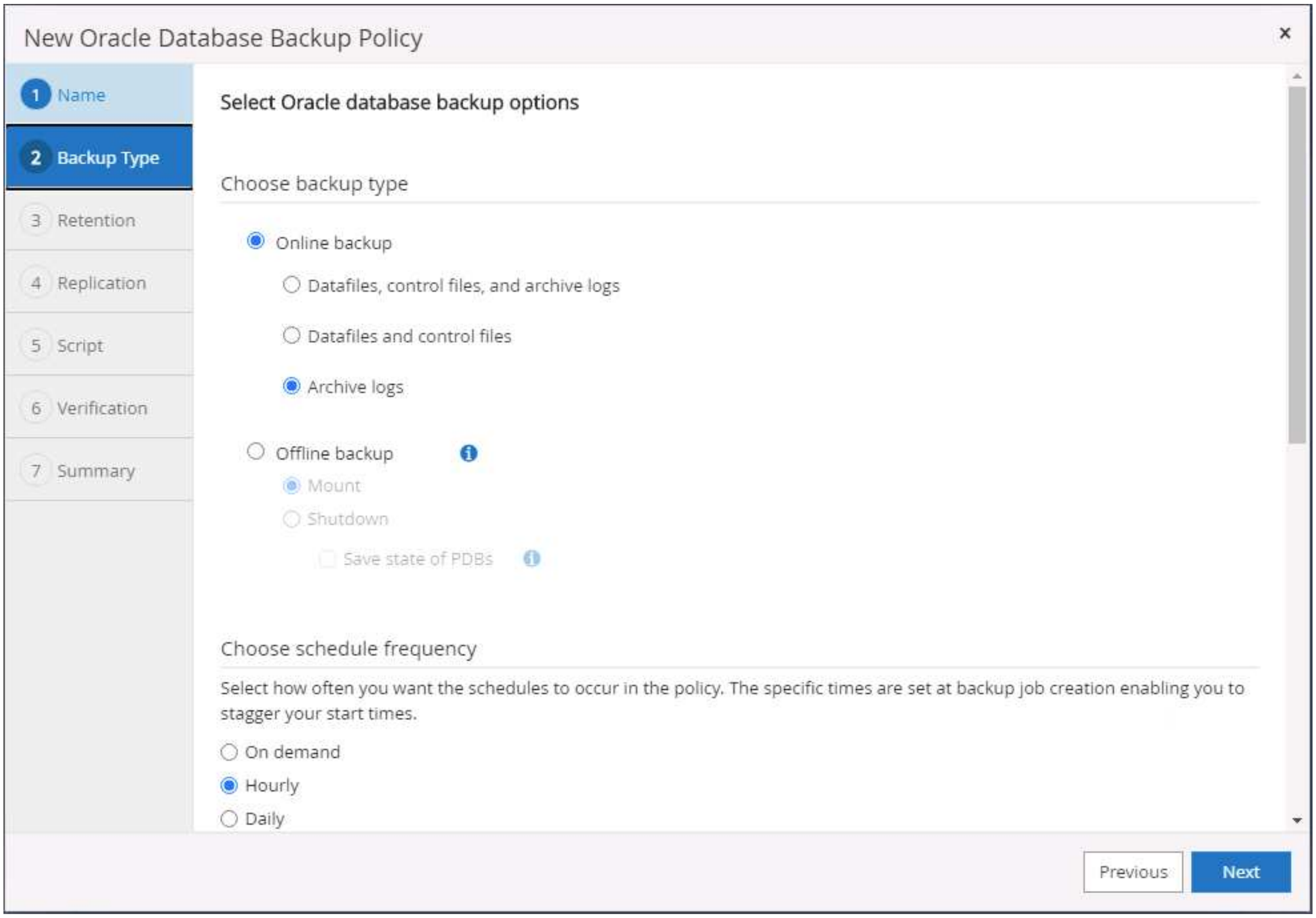
New Oracle Database Backup Policy

Provide a policy name

Policy name: Oracle Archive Log Backup

Details: Backup Oracle archive logs

3. Select the backup type and schedule frequency.



New Oracle Database Backup Policy

Select Oracle database backup options

Choose backup type

● Online backup

○ Datafiles, control files, and archive logs

○ Datafiles and control files

● Archive logs

○ Offline backup

● Mount

○ Shutdown

□ Save state of PDBs

Choose schedule frequency

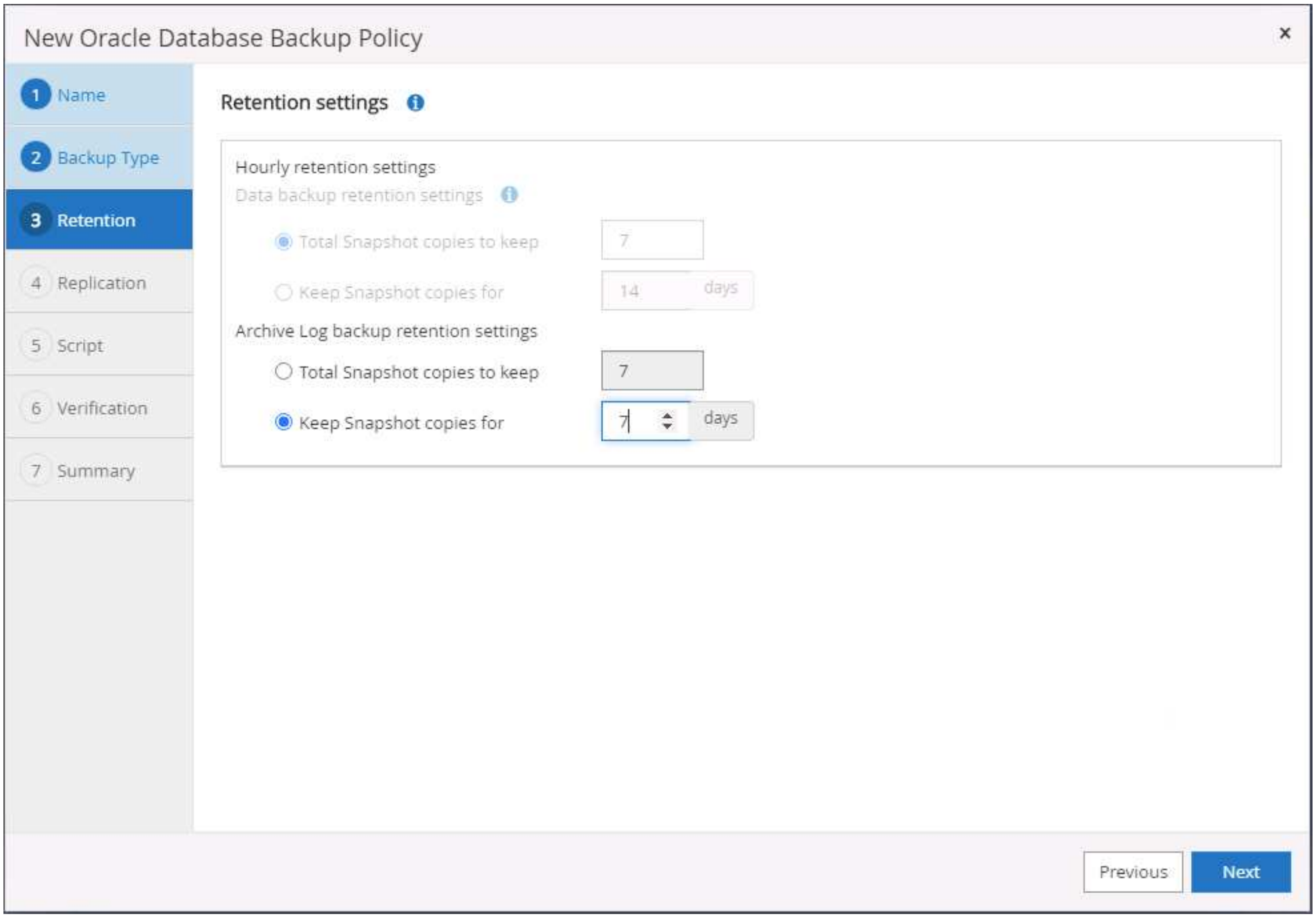
Select how often you want the schedules to occur in the policy. The specific times are set at backup job creation enabling you to stagger your start times.

○ On demand

● Hourly

○ Daily

4. Set the log retention period.


New Oracle Database Backup Policy

Retention settings

Hourly retention settings

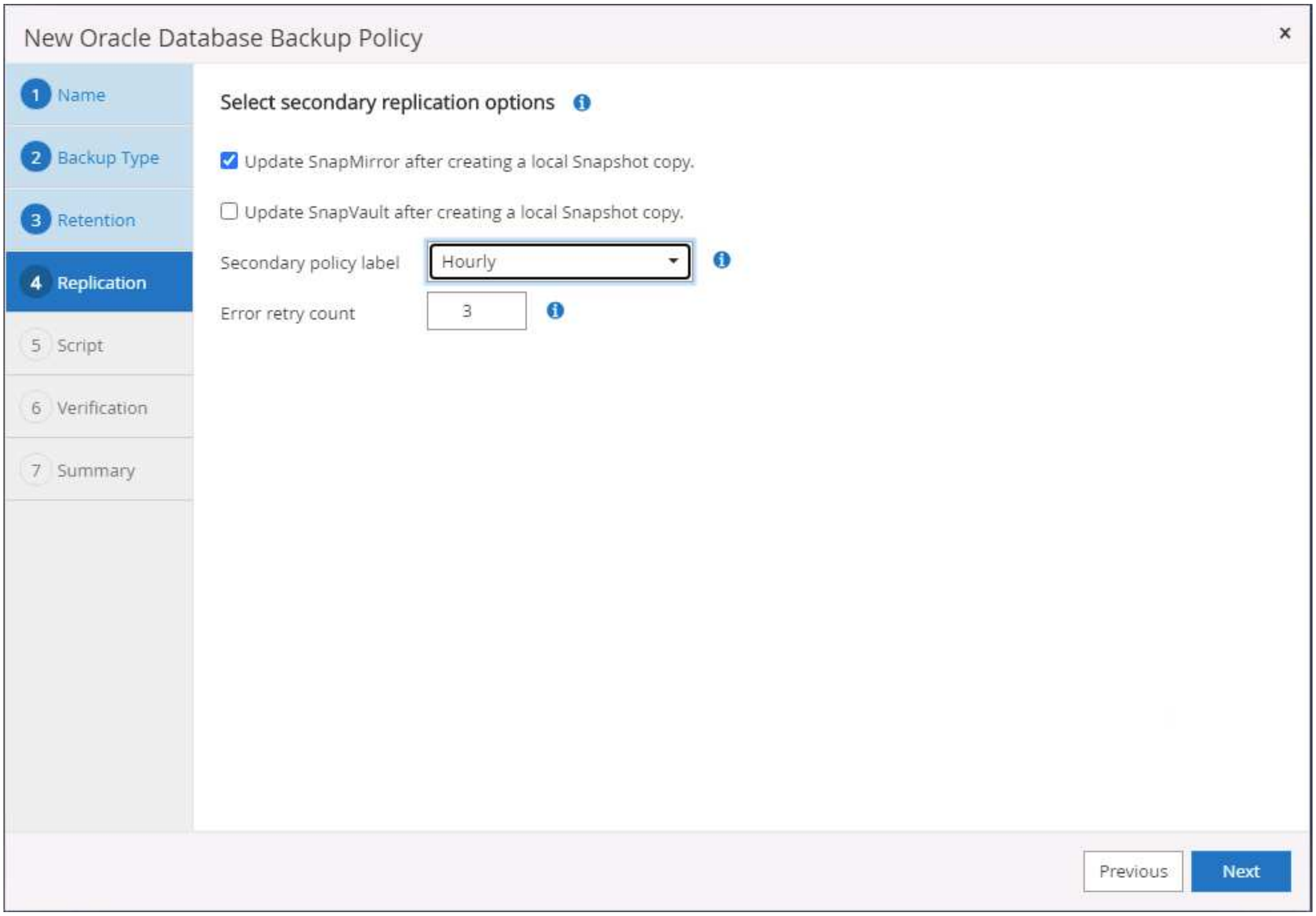
Data backup retention settings

- ● Total Snapshot copies to keep: 7
- ○ Keep Snapshot copies for: 14 days

Archive Log backup retention settings

- ○ Total Snapshot copies to keep: 7
- ● Keep Snapshot copies for: 7 days

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



New Oracle Database Backup Policy

Select secondary replication options

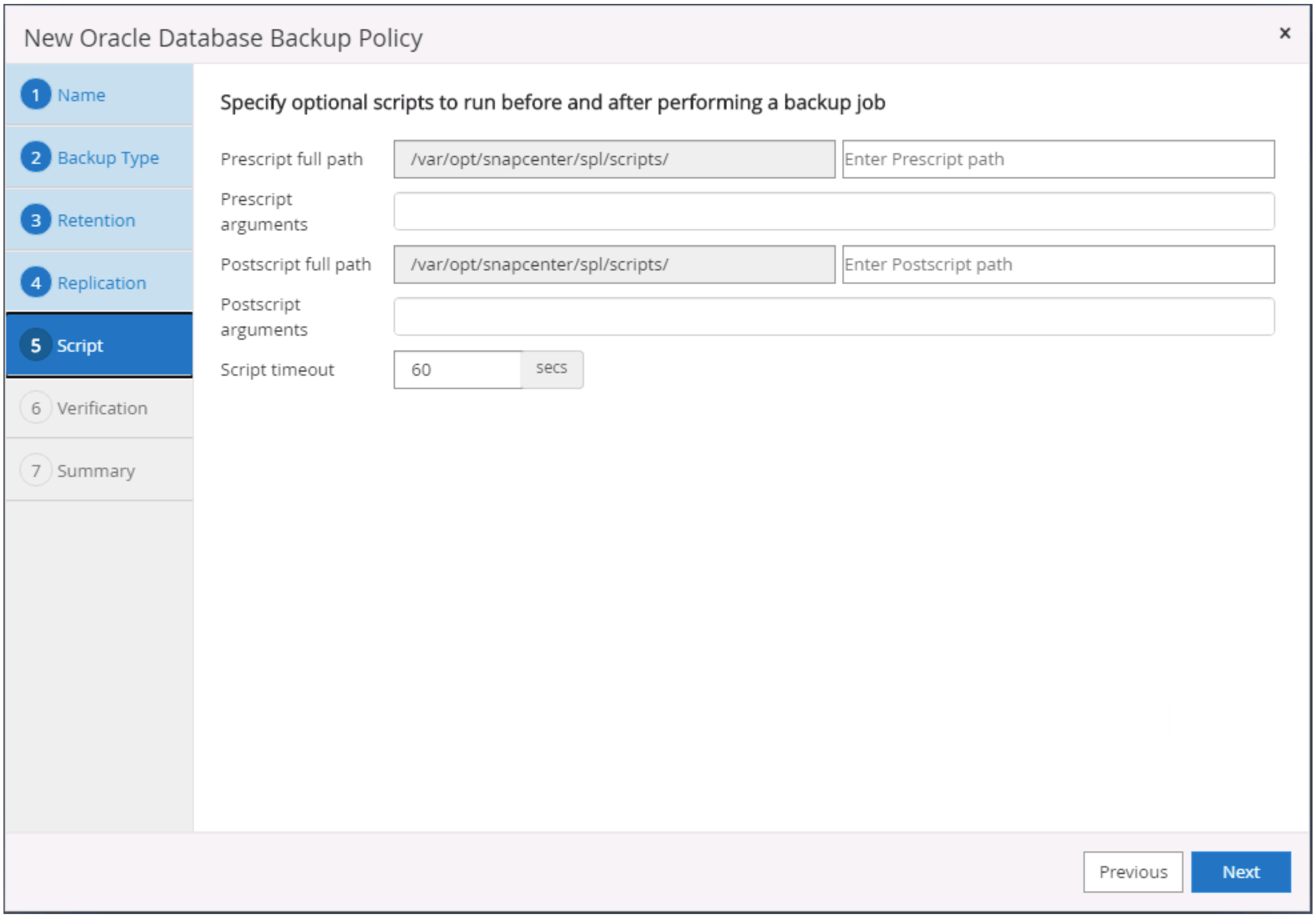
☑ Update SnapMirror after creating a local Snapshot copy.

□ Update SnapVault after creating a local Snapshot copy.

Secondary policy label: Hourly

Error retry count: 3

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



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

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

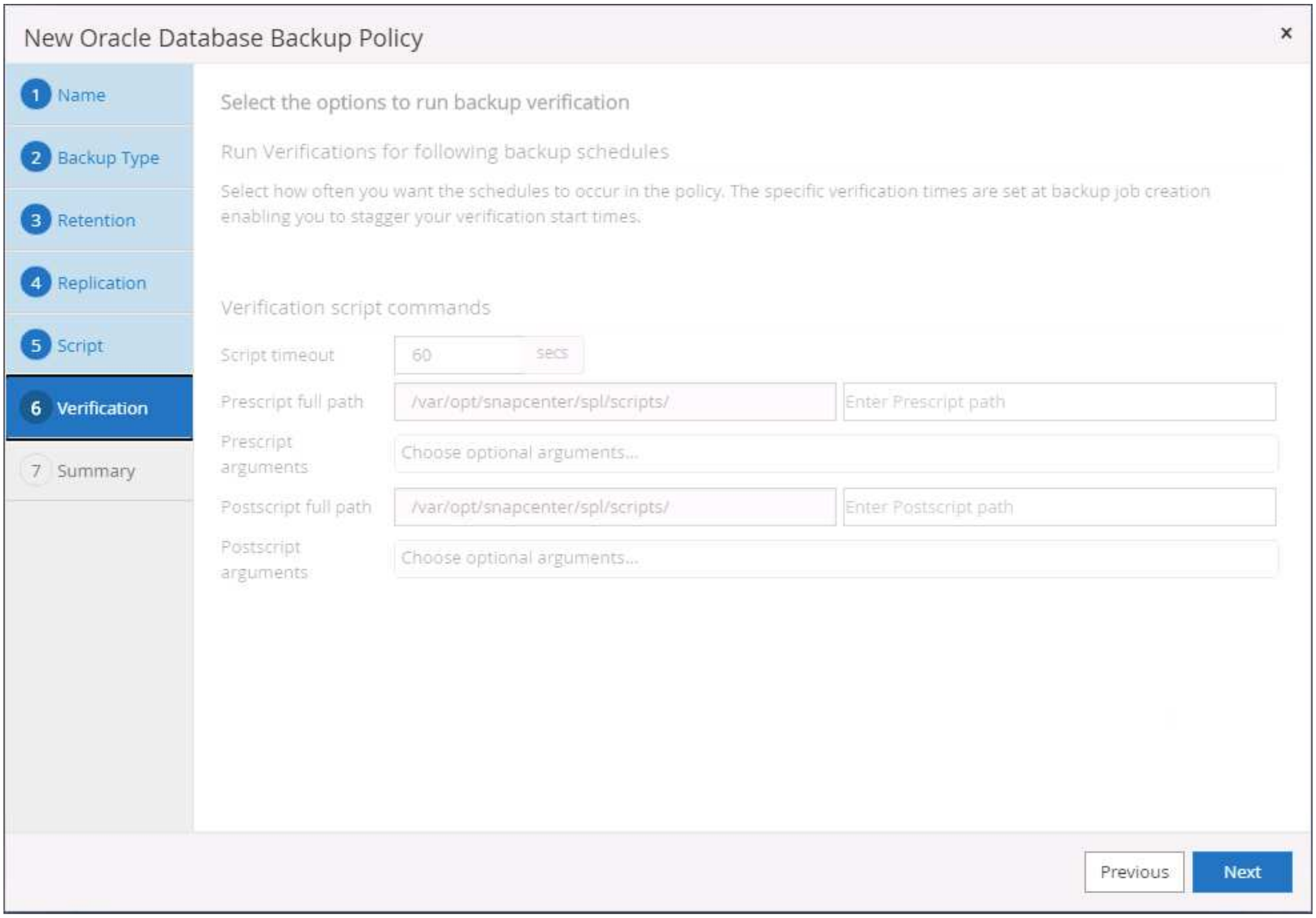
Prescript arguments

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

Postscript arguments

Script timeout 60 secs

7. Specify any backup verification scripts.



New Oracle Database Backup Policy

Select the options to run backup verification

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.

Verification script commands

Script timeout: 60 secs

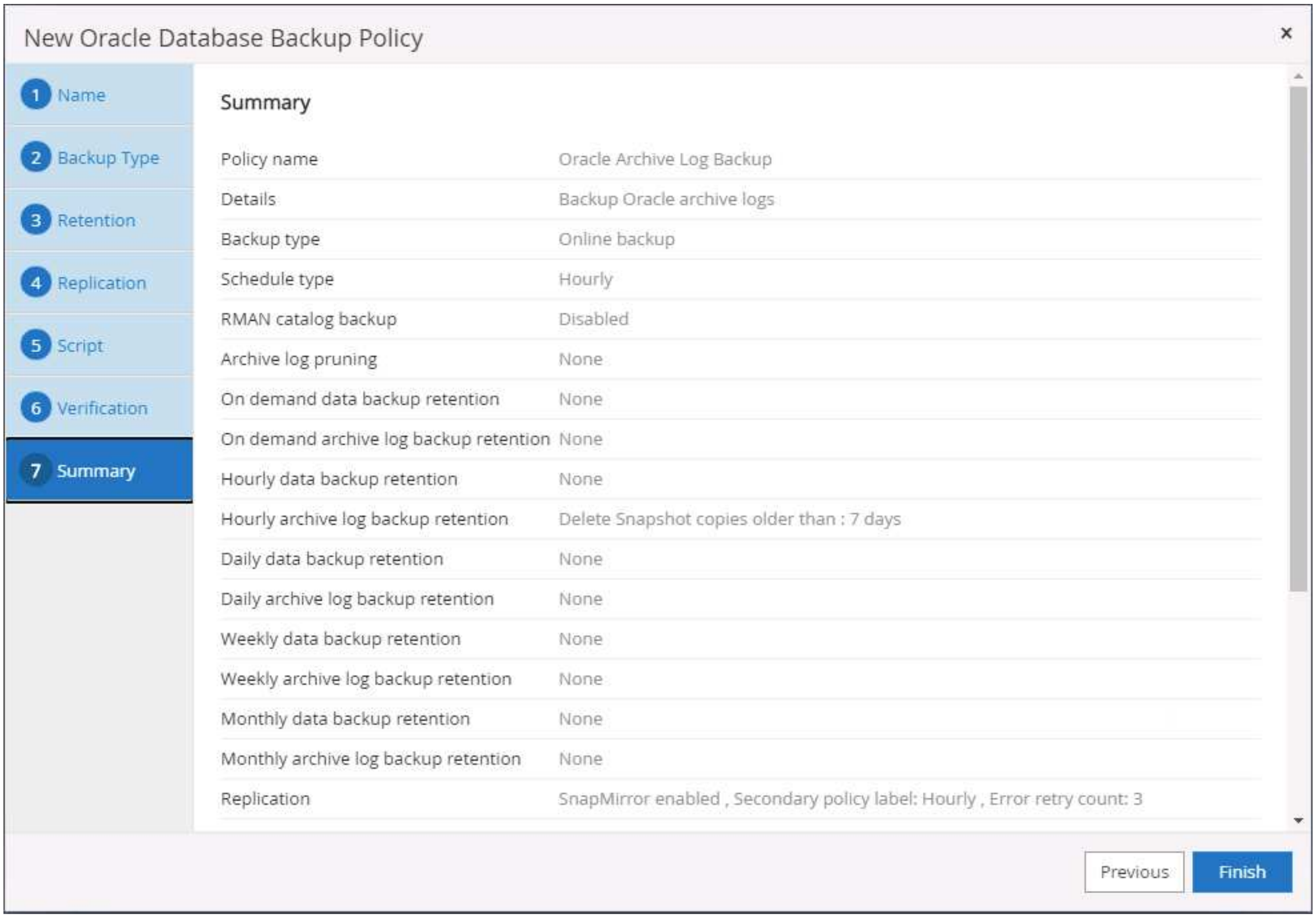
Prescript full path: /var/opt/snapcenter/spl/scripts/ Enter Prescript path

Prescript arguments: Choose optional arguments...

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

Postscript arguments: Choose optional arguments...

8. Summary.

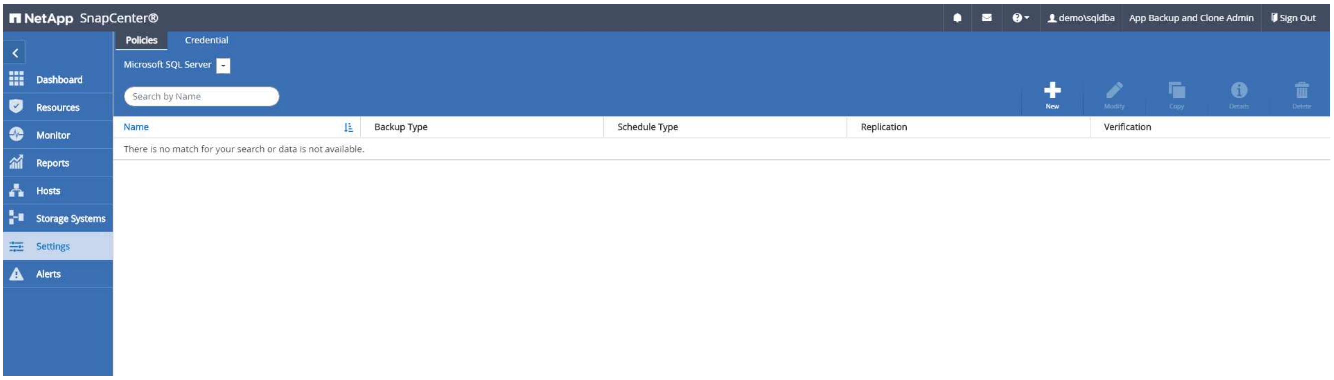


Summary

Policy name	Oracle Archive Log Backup
Details	Backup Oracle archive logs
Backup type	Online backup
Schedule type	Hourly
RMAN catalog backup	Disabled
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

Create a full database backup policy for SQL

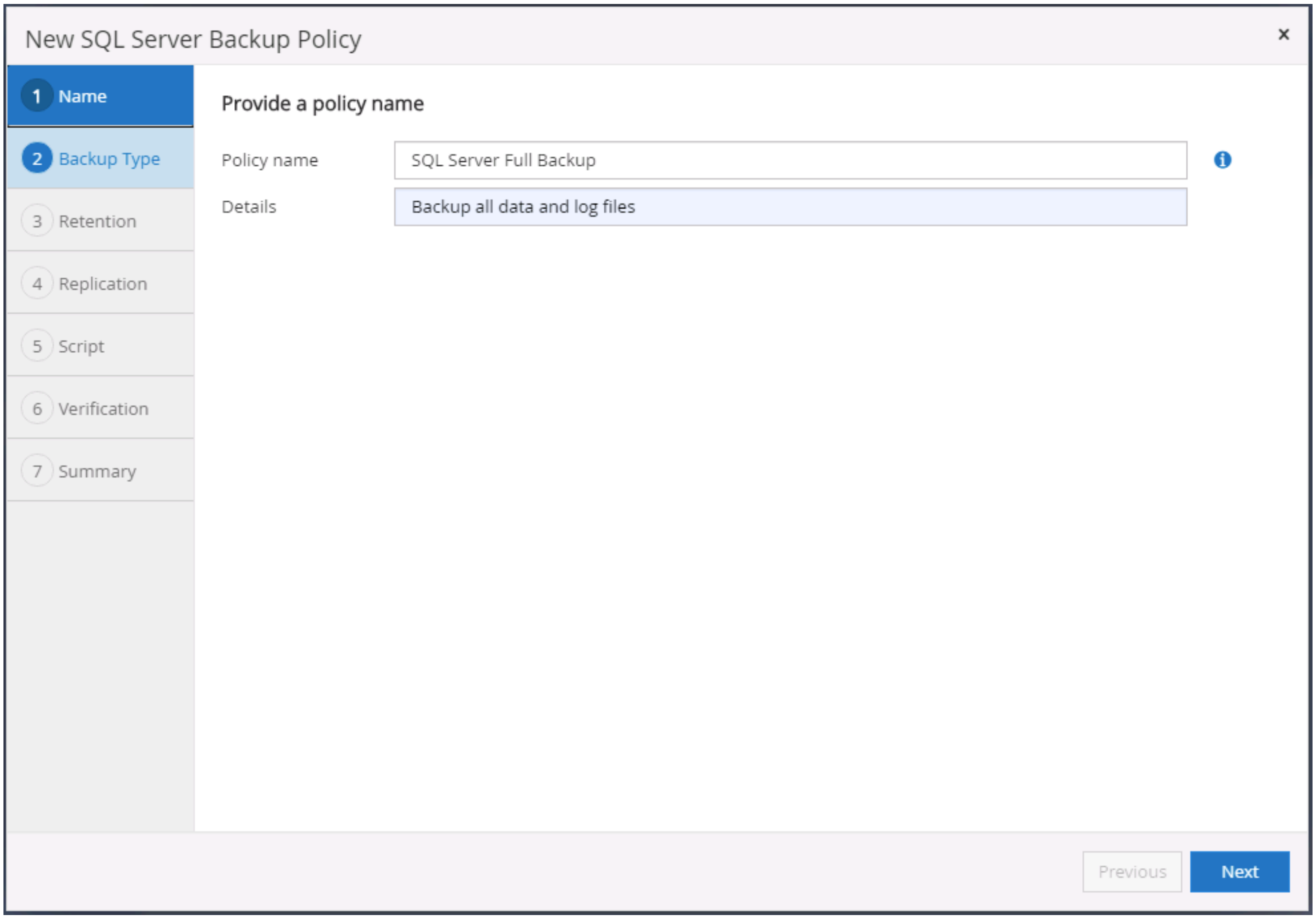
1. Log into SnapCenter with a database management user ID, click Settings, and then click Polices.



Name	Backup Type	Schedule Type	Replication	Verification

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.

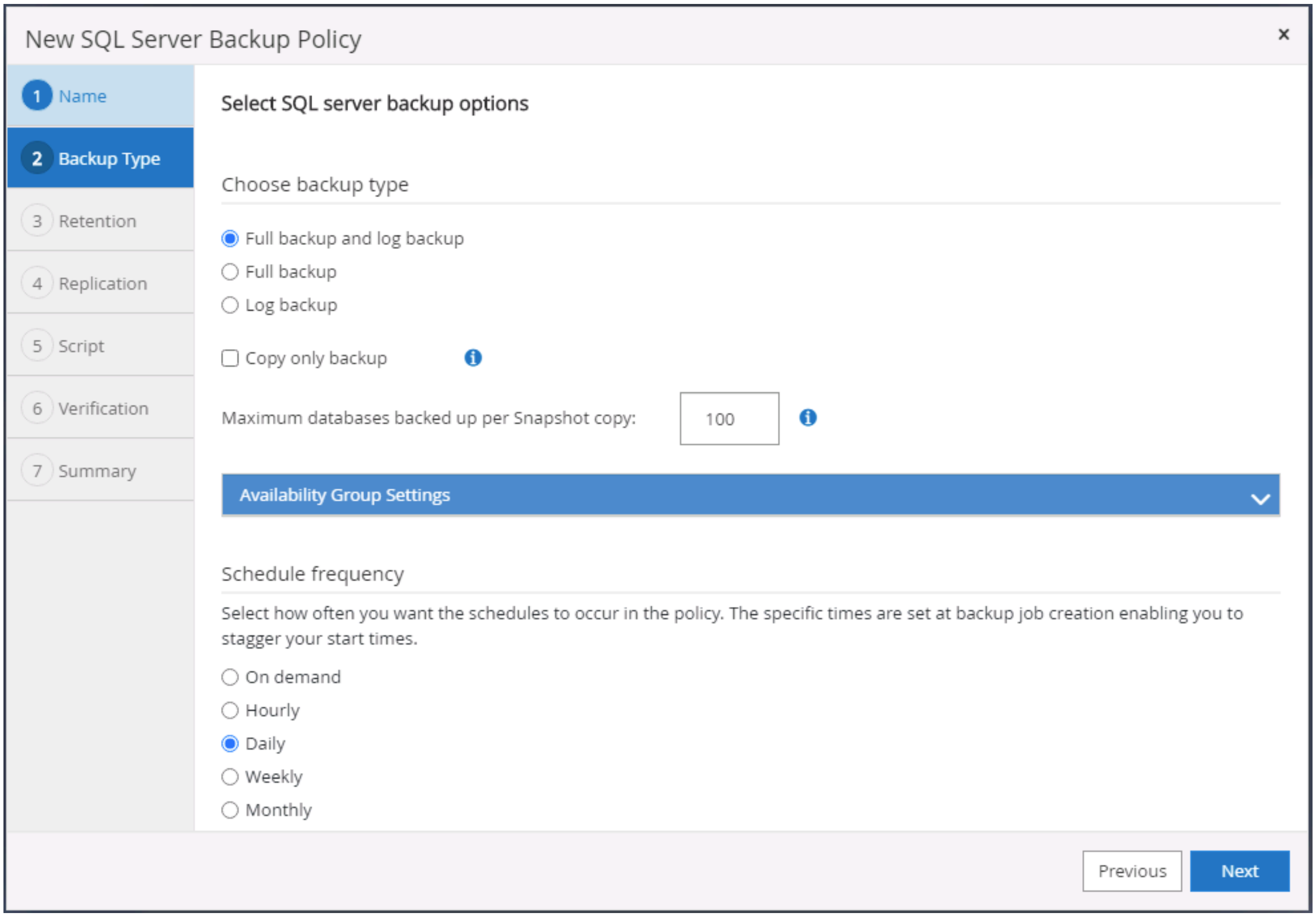


Provide a policy name

Policy name: SQL Server Full Backup

Details: Backup all data and log files

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

Select SQL server backup options

Choose backup type

● Full backup and log backup
○ Full backup
○ Log backup

□ Copy only backup

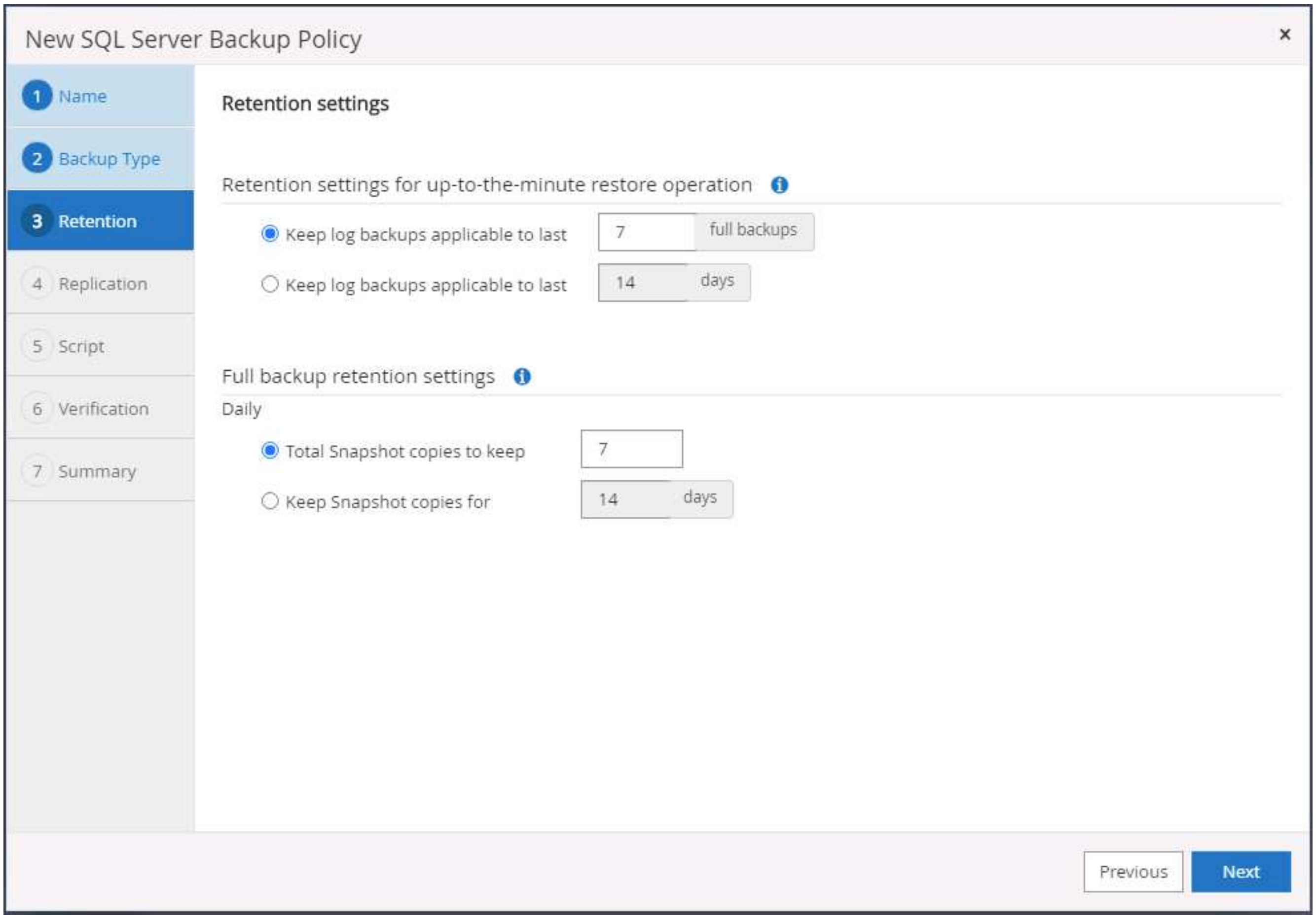
Maximum databases backed up per Snapshot copy: 100

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

4. Set the backup retention period.



New SQL Server Backup Policy

Retention settings

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

● Keep log backups applicable to last 7 full backups

○ Keep log backups applicable to last 14 days

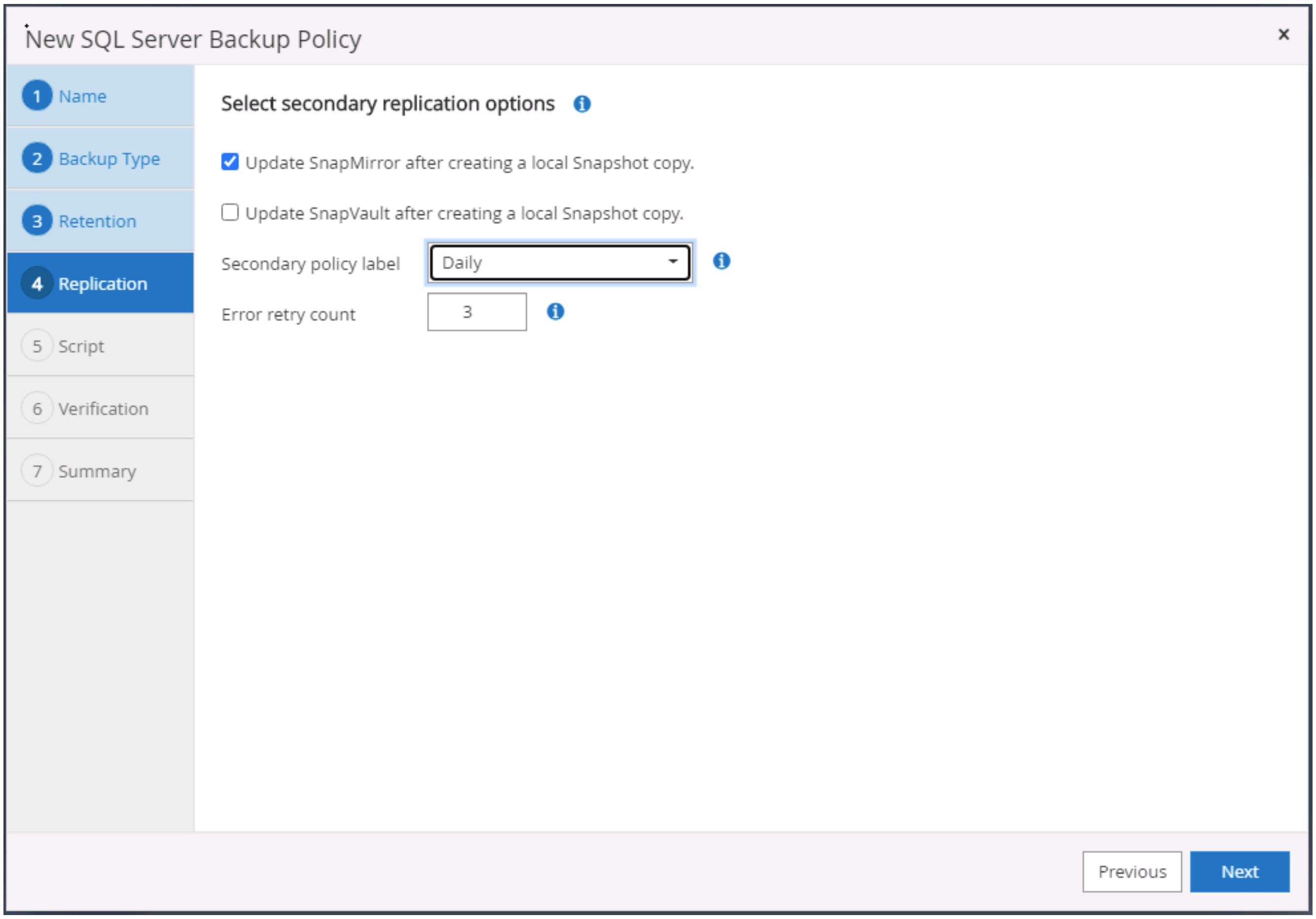
Full backup retention settings

Daily

● Total Snapshot copies to keep 7

○ Keep Snapshot copies for 14 days

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



New SQL Server Backup Policy

Select secondary replication options

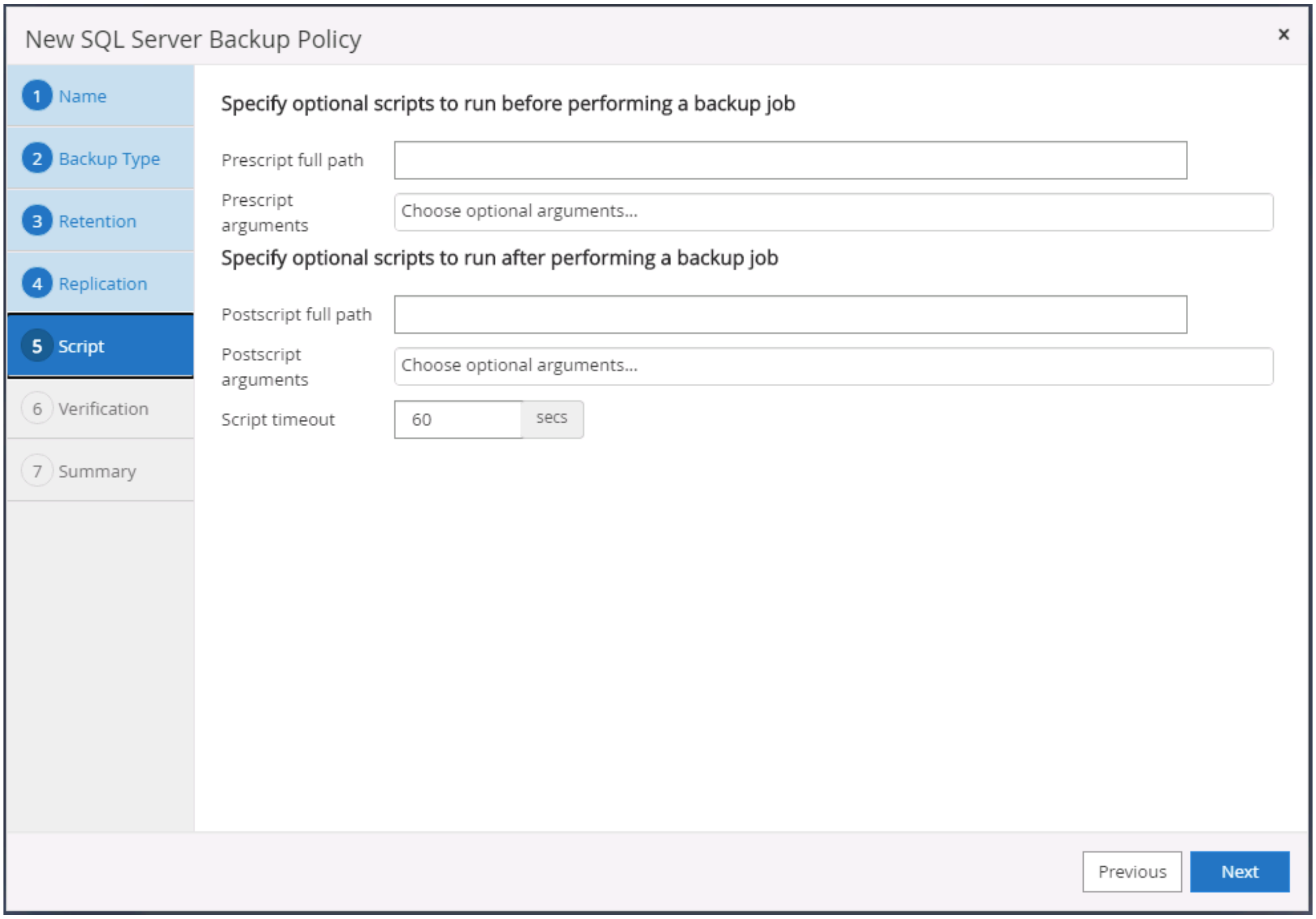
☑ Update SnapMirror after creating a local Snapshot copy.

□ Update SnapVault after creating a local Snapshot copy.

Secondary policy label: Daily

Error retry count: 3

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



New SQL Server Backup Policy

Specify optional scripts to run before performing a backup job

Prescript full path

Prescript arguments: Choose optional arguments...

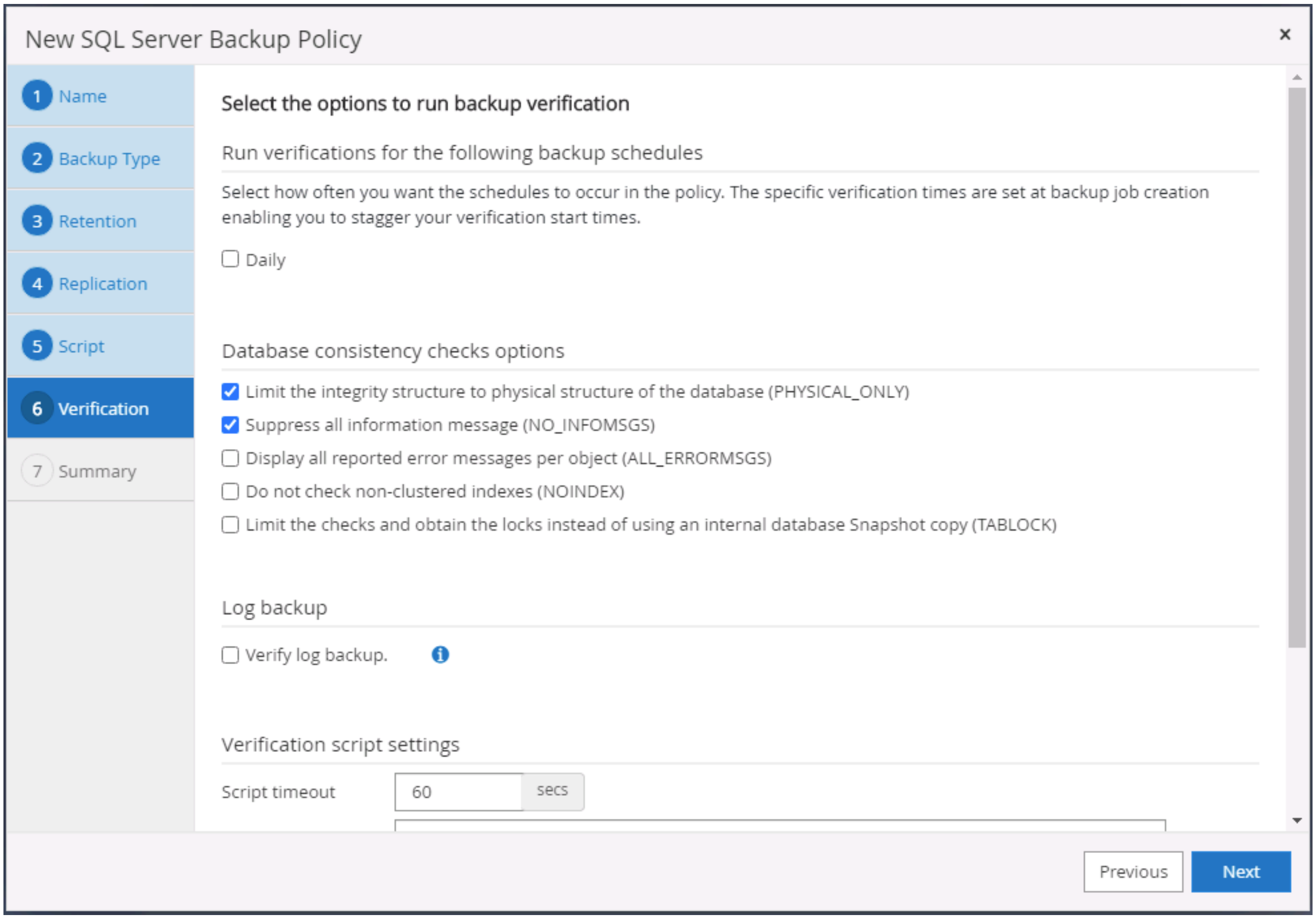
Specify optional scripts to run after performing a backup job

Postscript full path

Postscript arguments: Choose optional arguments...

Script timeout: 60 secs

7. Specify the options to run backup verification.



New SQL Server Backup Policy

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_ERRORMSGS)

☐ Do not check non-clustered indexes (NOINDEX)

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

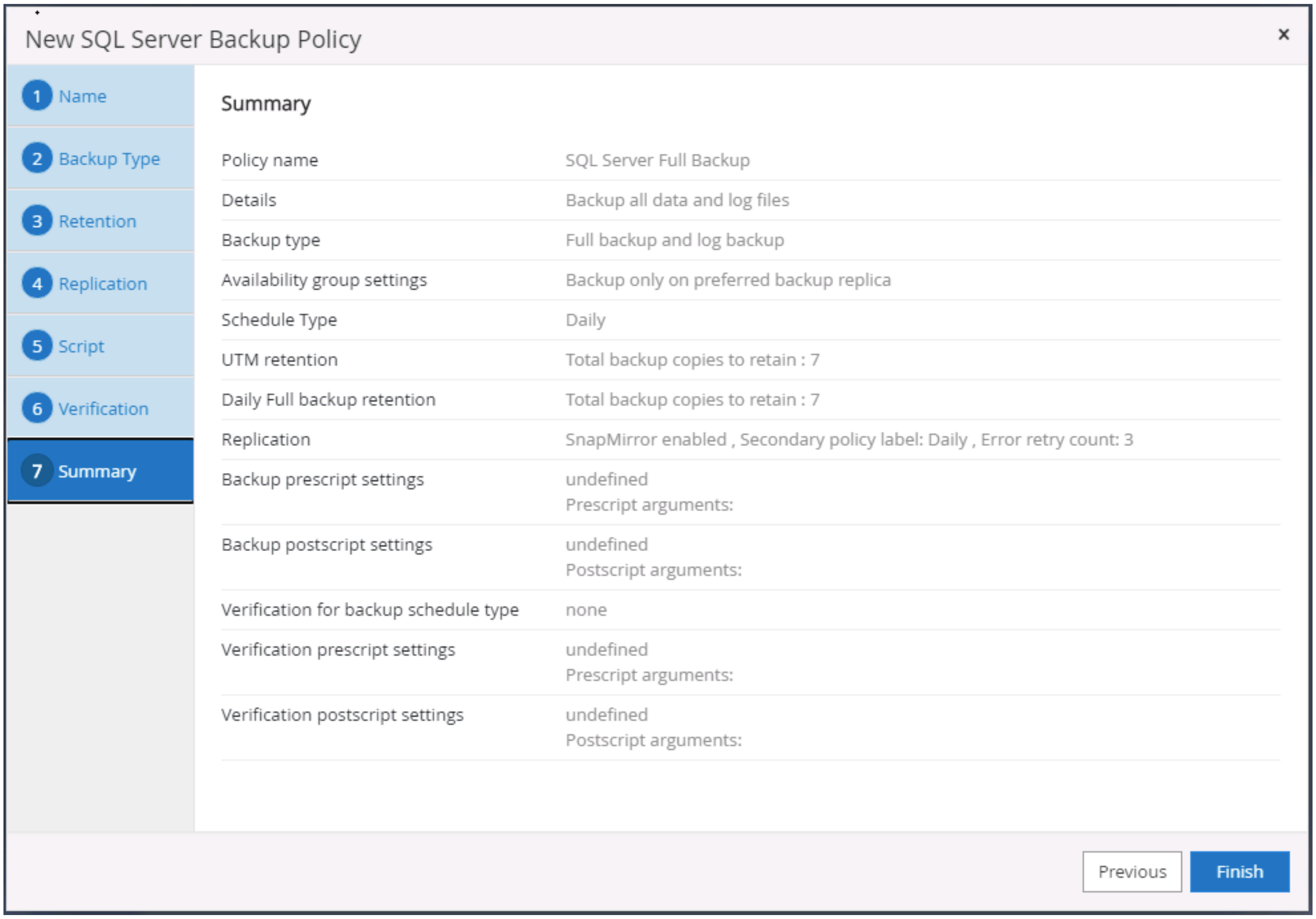
Log backup

☐ Verify log backup.

Verification script settings

Script timeout 60 secs

8. Summary.



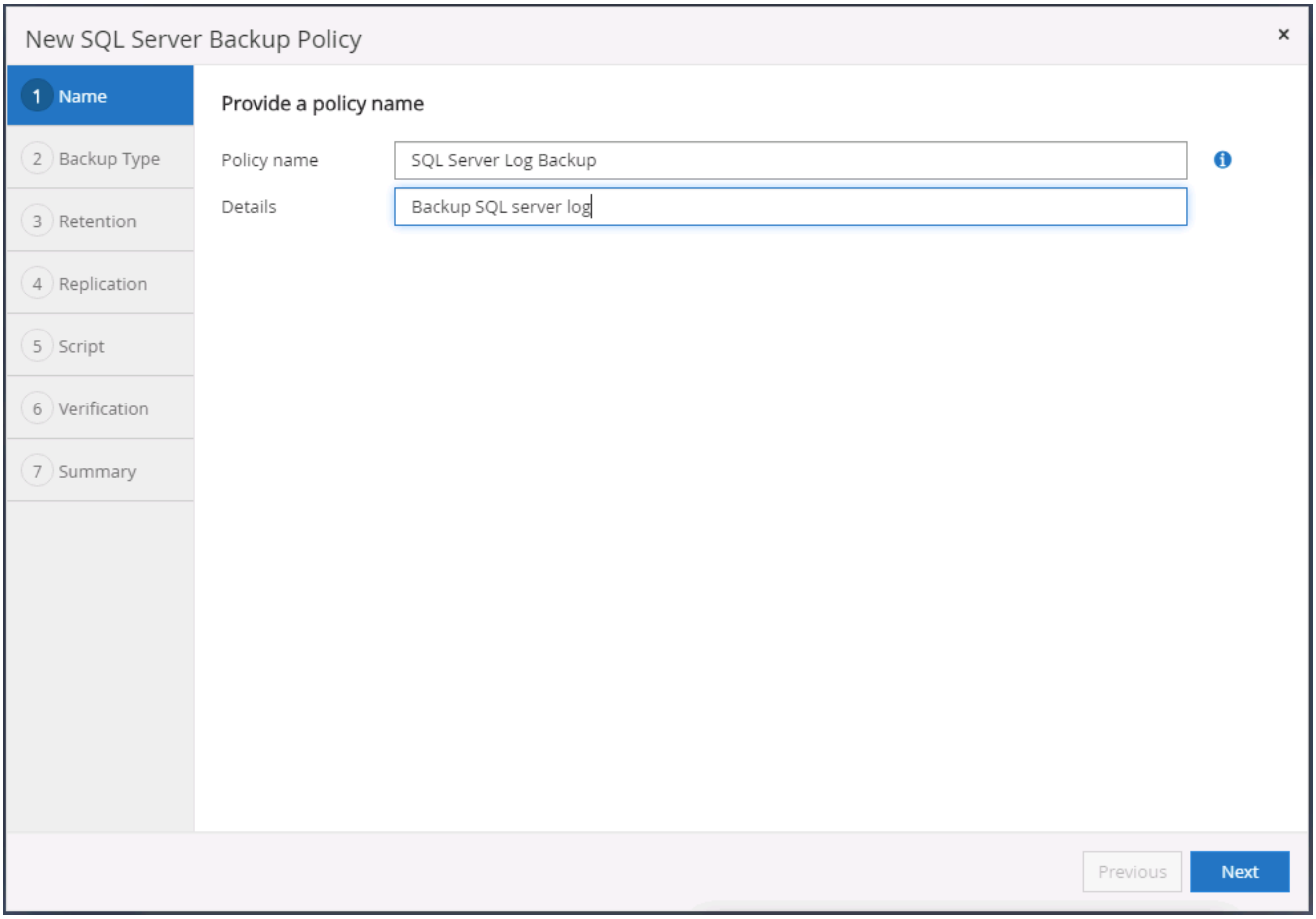
New SQL Server Backup Policy

Summary

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:

Create a database log backup policy for SQL.

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



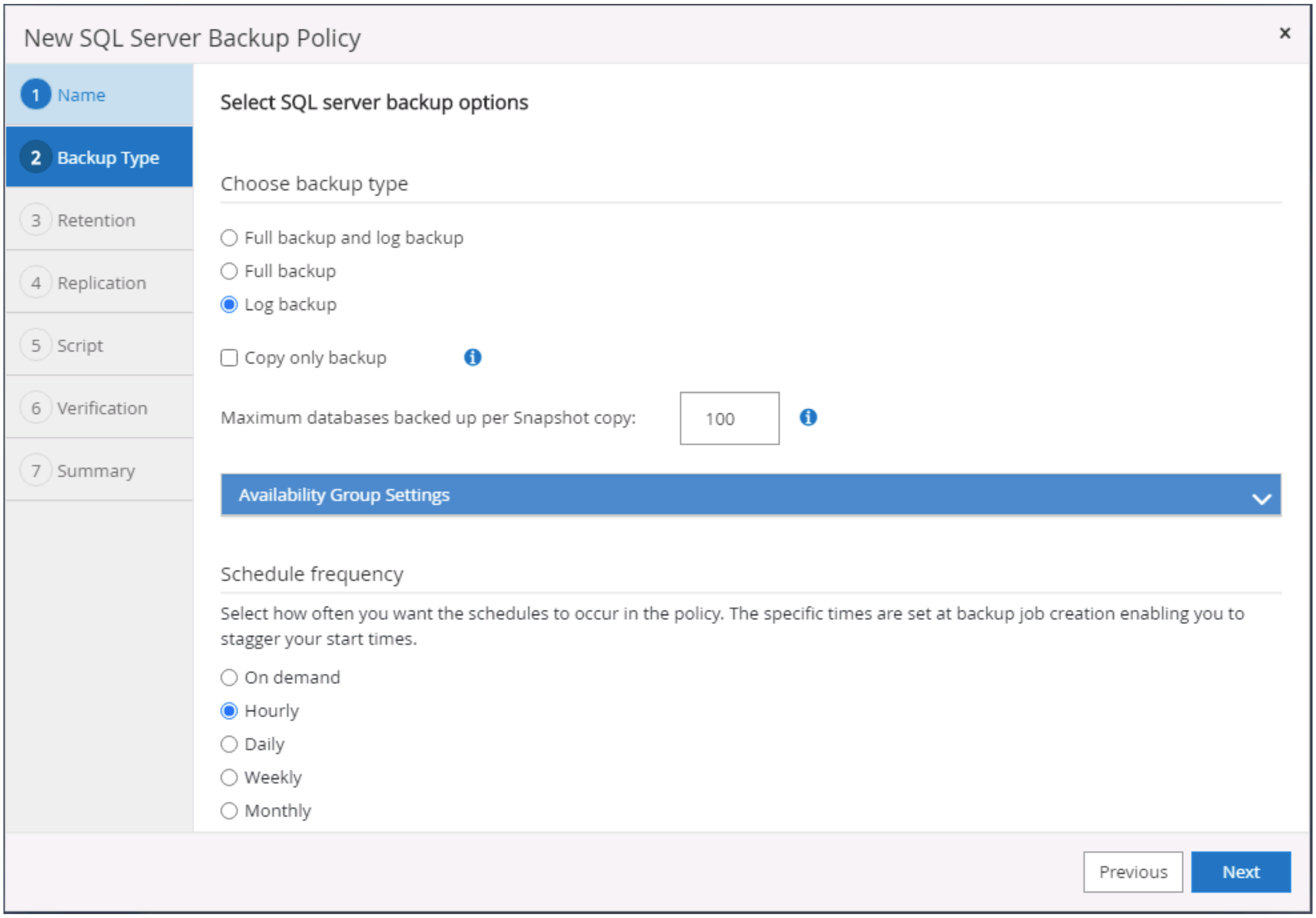
New SQL Server Backup Policy

Provide a policy name

Policy name: SQL Server Log Backup

Details: Backup SQL server log

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

Select SQL server backup options

Choose backup type

○ Full backup and log backup
○ Full backup
● Log backup

□ Copy only backup

Maximum databases backed up per Snapshot copy: 100

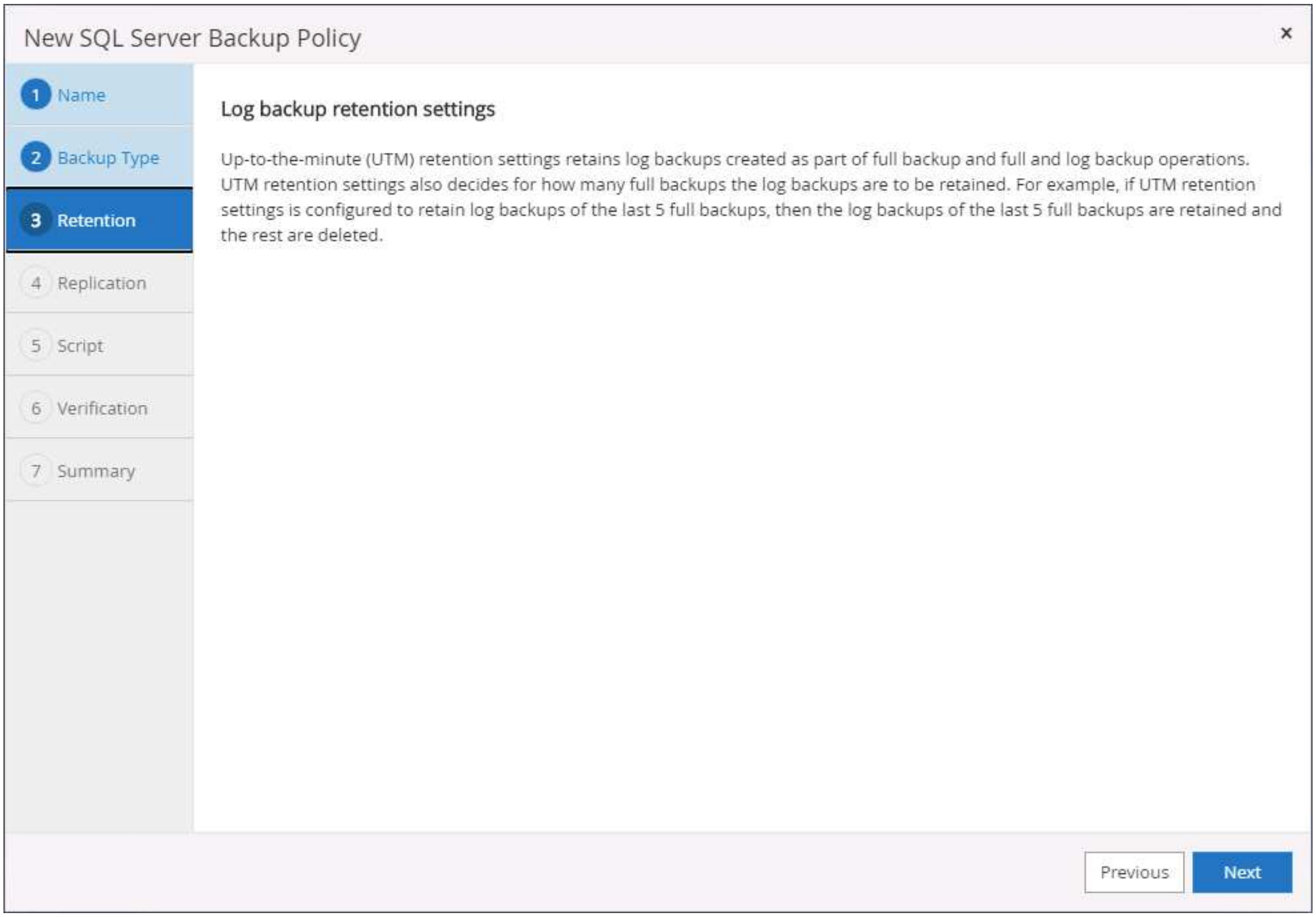
Availability Group Settings

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

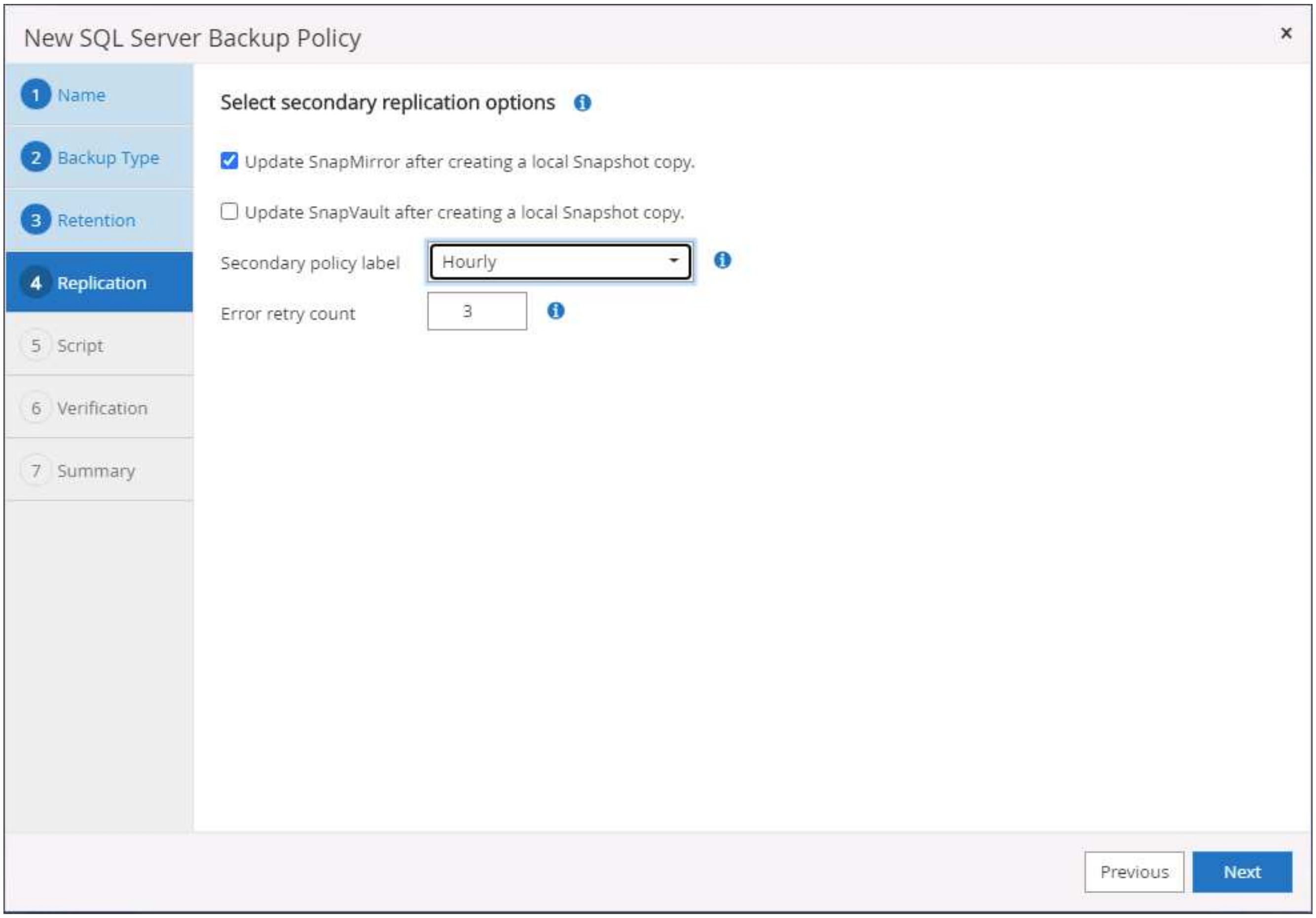
3. SQL server data backup policy defines the log backup retention; accept the defaults here.



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.

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



New SQL Server Backup Policy

Select secondary replication options

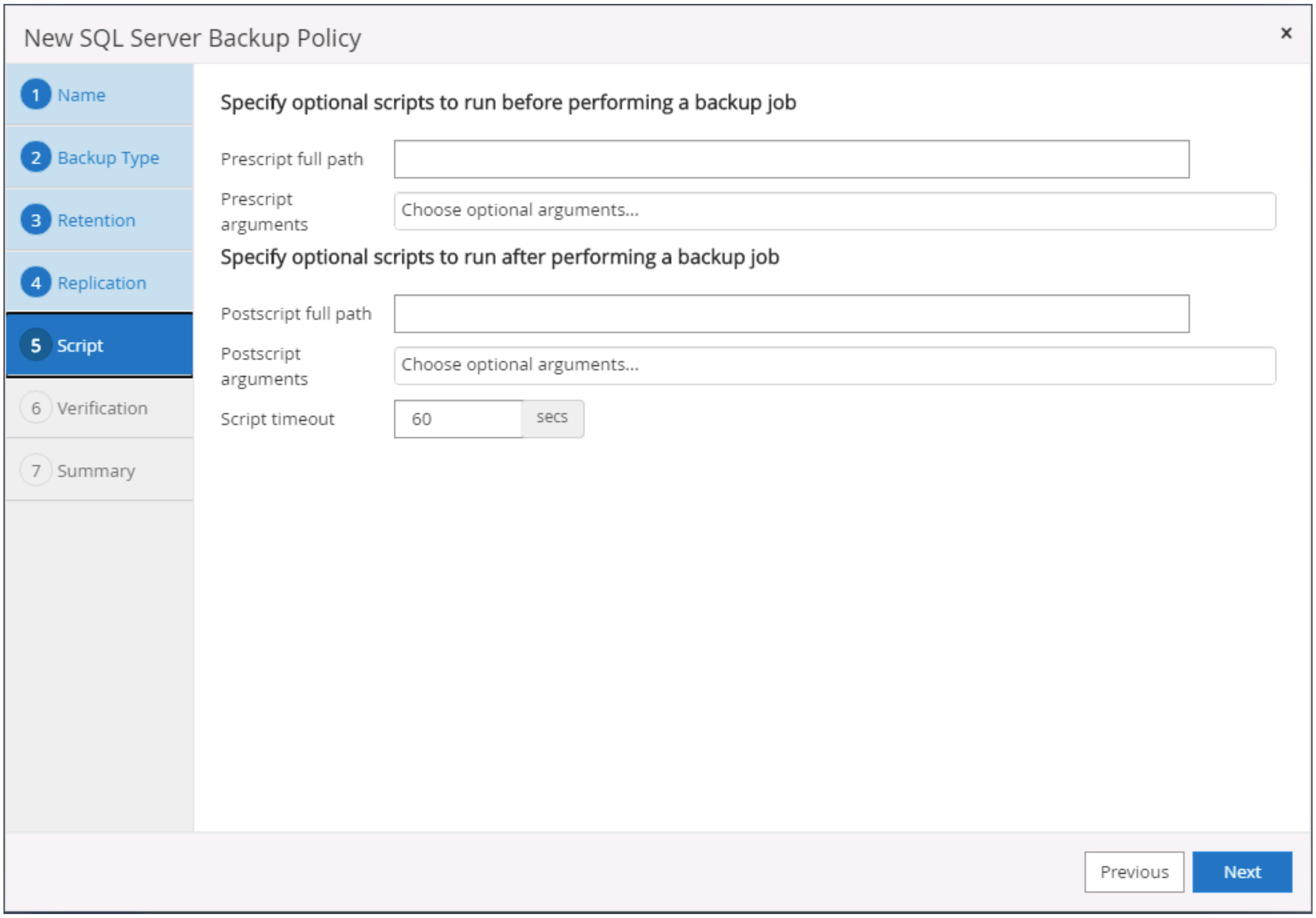
☑ Update SnapMirror after creating a local Snapshot copy.

□ Update SnapVault after creating a local Snapshot copy.

Secondary policy label: Hourly

Error retry count: 3

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



New SQL Server Backup Policy

Specify optional scripts to run before performing a backup job

Prescript full path

Prescript arguments: Choose optional arguments...

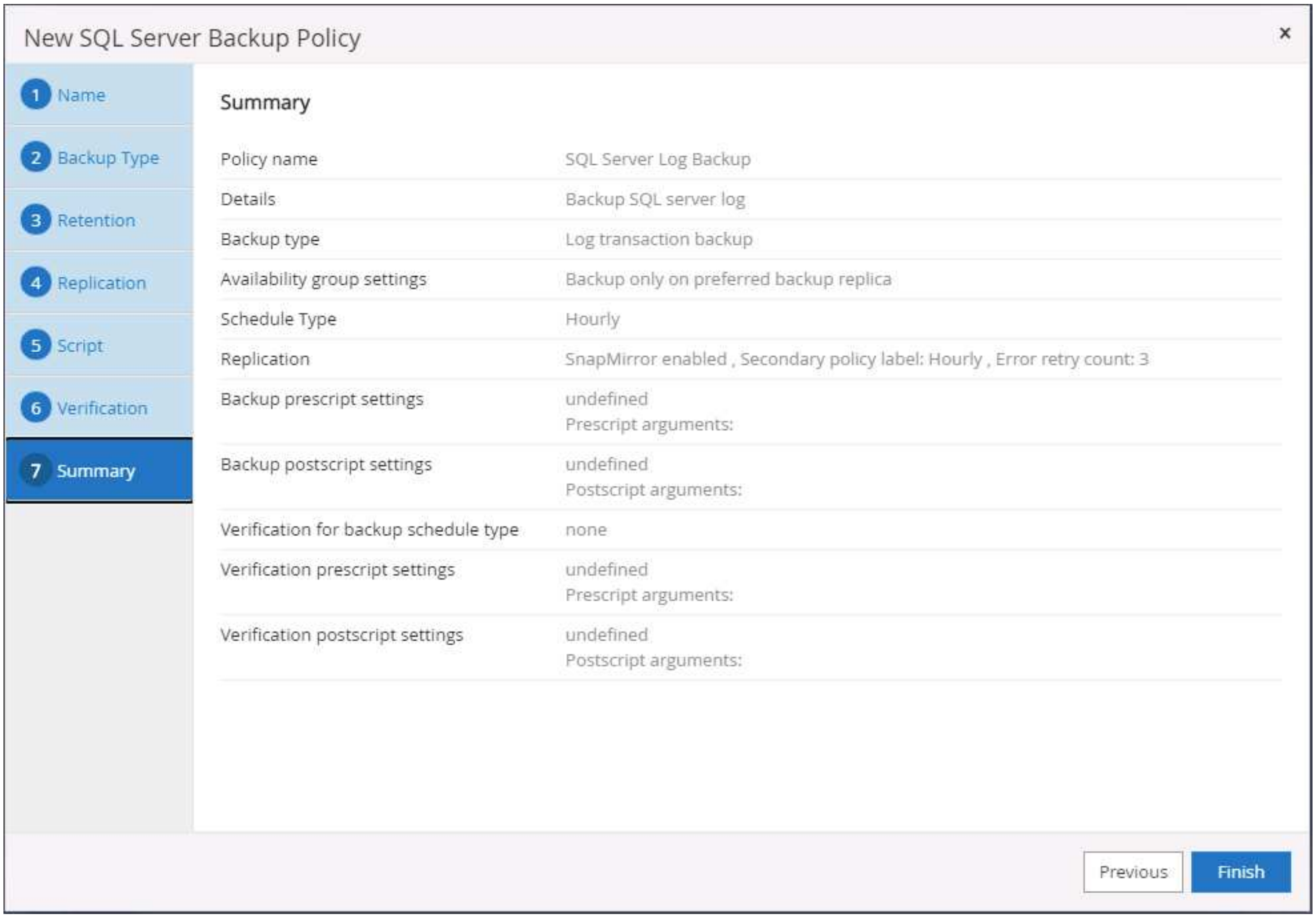
Specify optional scripts to run after performing a backup job

Postscript full path

Postscript arguments: Choose optional arguments...

Script timeout: 60 secs

6. Summary.



Summary

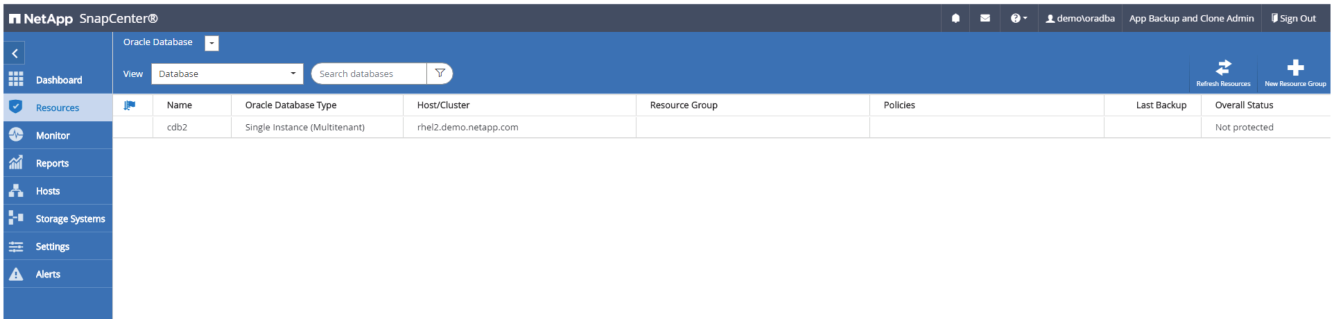
Policy name	SQL Server Log Backup
Details	Backup SQL server log
Backup type	Log transaction backup
Availability group settings	Backup only on preferred backup replica
Schedule Type	Hourly
Replication	SnapMirror enabled , Secondary policy label: Hourly , Error retry count: 3
Backup prescript settings	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:

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.

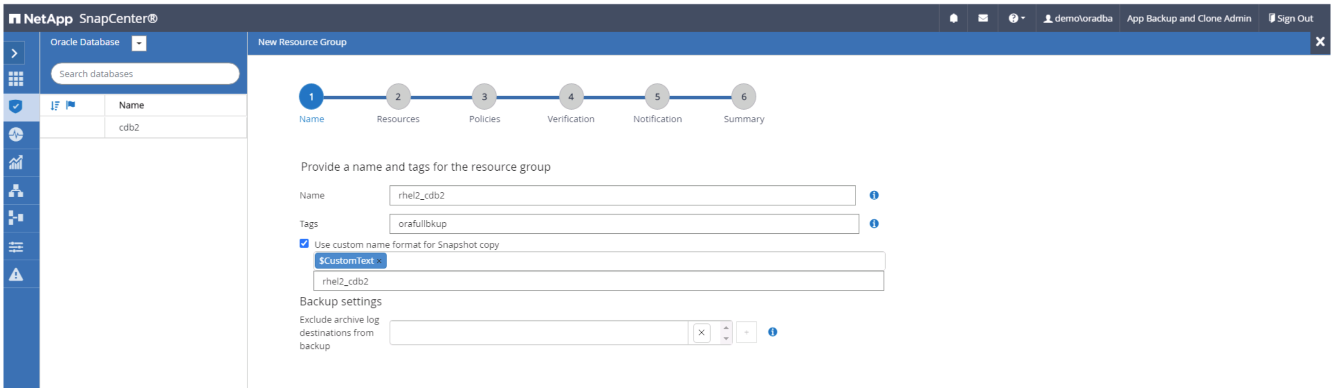
Create a resource group for full backup of Oracle

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.



Provide a name and tags for the resource group

Name: rhel2_cdb2

Tags: orafullbkup

☑ Use custom name format for Snapshot copy

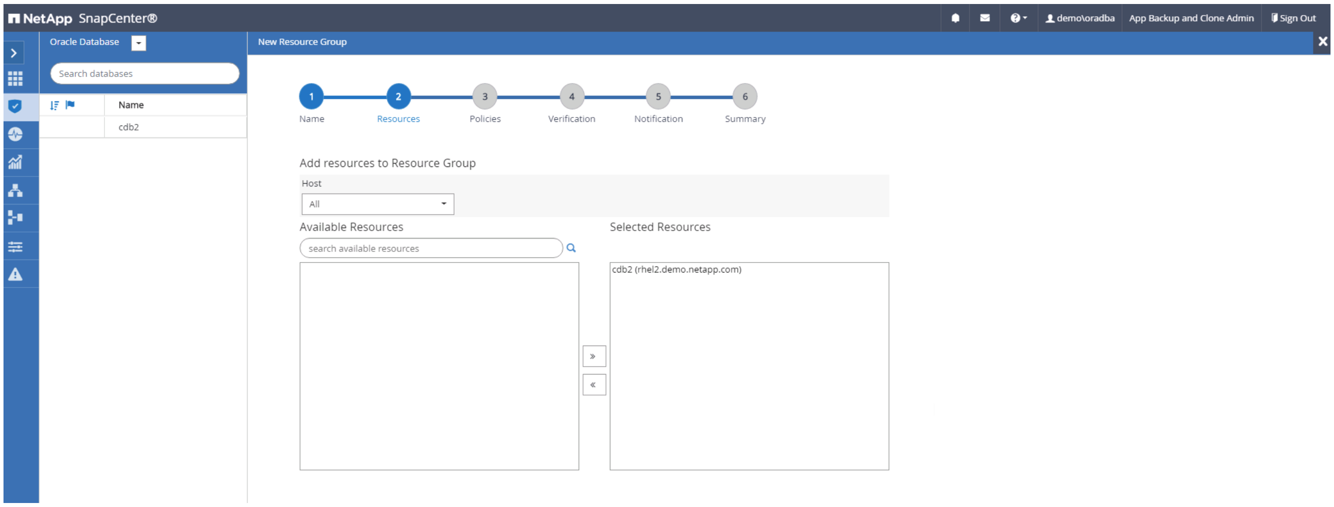
$CustomText

rhel2_cdb2

Backup settings

Exclude archive log destinations from backup

3. Add database resources to the resource group.



Add resources to Resource Group

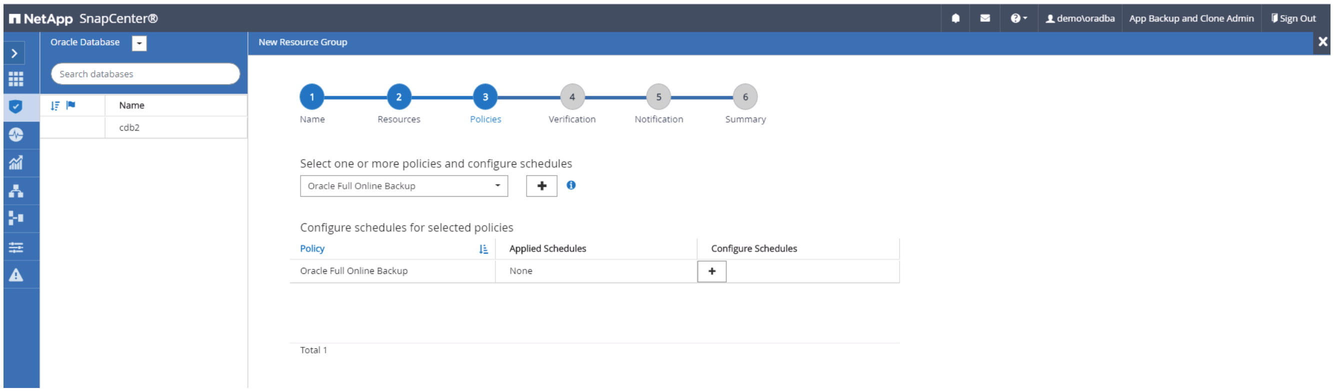
Host: All

Available Resources

Selected Resources

cdb2 (rhel2.demo.netapp.com)

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



Select one or more policies and configure schedules

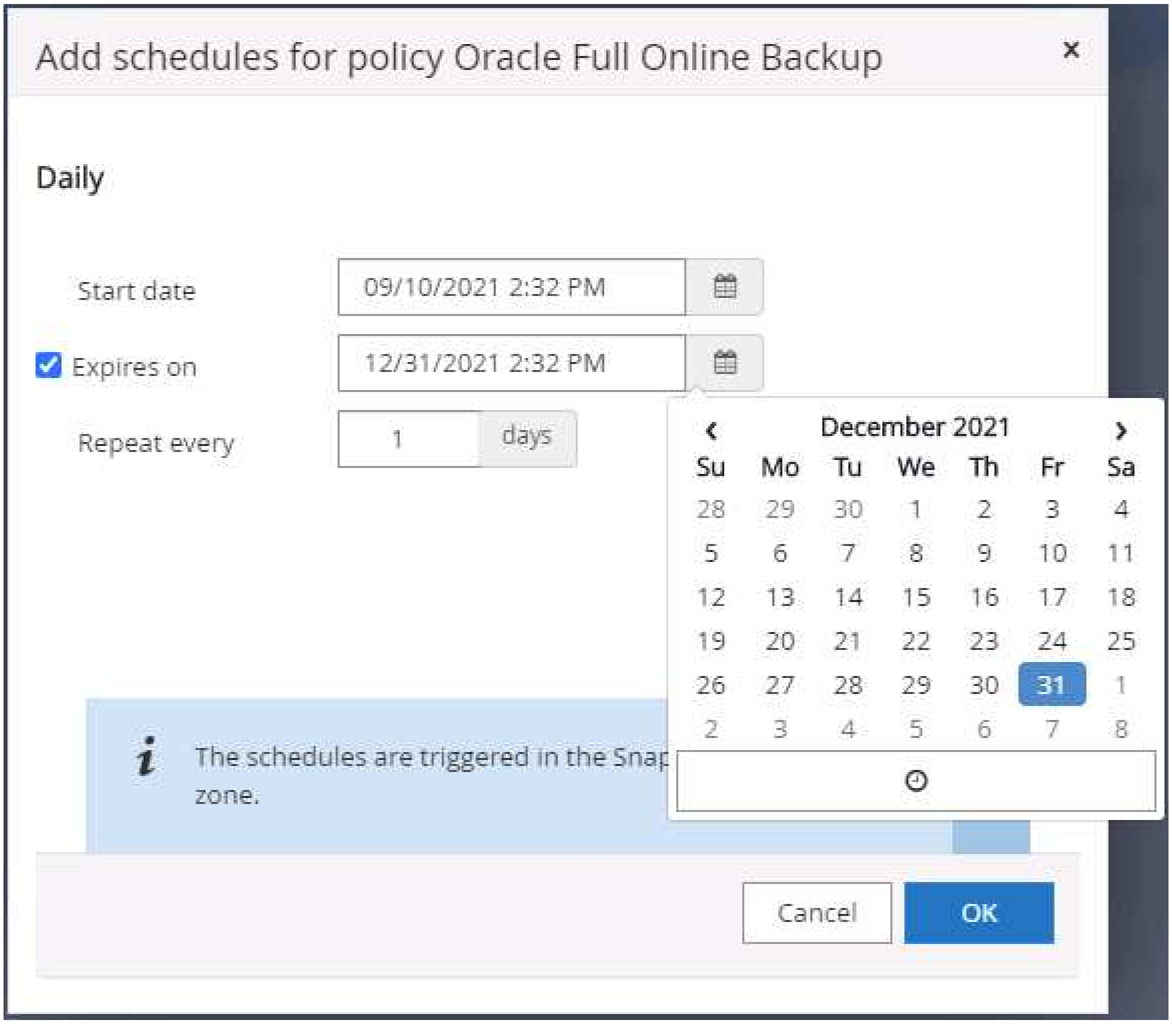
Oracle Full Online Backup

Configure schedules for selected policies

Policy	Applied Schedules	Configure Schedules
Oracle Full Online Backup	None	+

Total 1

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



Add schedules for policy Oracle Full Online Backup

Daily

Start date 09/10/2021 2:32 PM

☑ Expires on 12/31/2021 2:32 PM

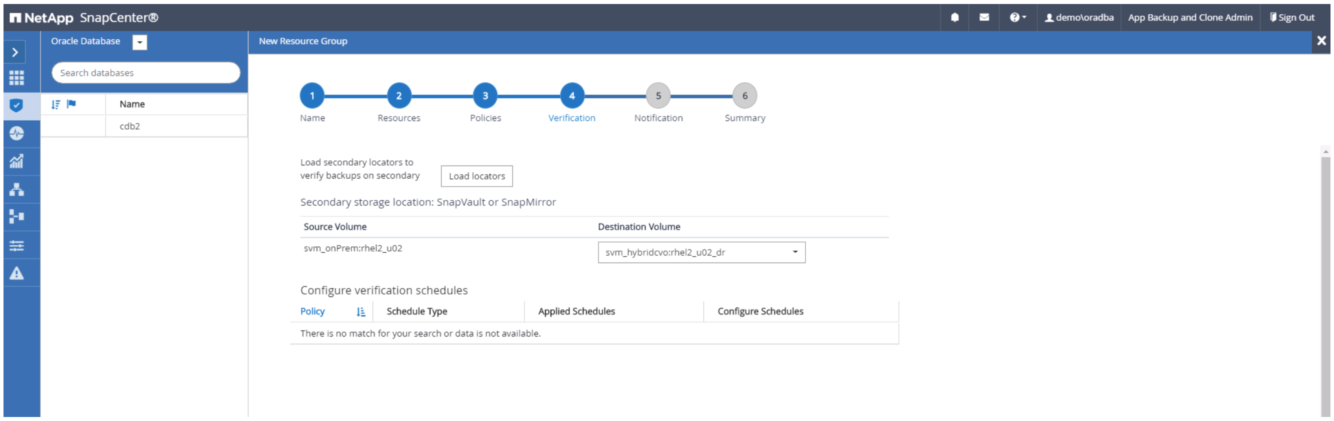
Repeat every 1 days

December 2021

Su	Mo	Tu	We	Th	Fr	Sa
28	29	30	1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	1
2	3	4	5	6	7	8

The schedules are triggered in the Snap zone.

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



Load secondary locators to verify backups on secondary [Load locators]

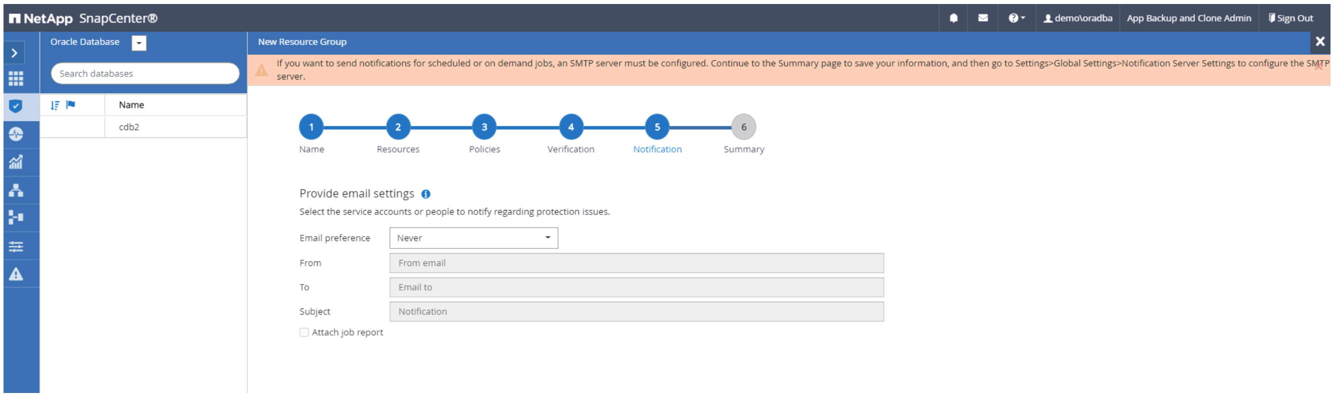
Secondary storage location: SnapVault or SnapMirror

Source Volume	Destination Volume
svm_onPrem:rhel2_u02	svm_hybridcvo:rhel2_u02_dr

Configure verification schedules

Policy	Schedule Type	Applied Schedules	Configure Schedules
There is no match for your search or data is not available.			

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



If you want to send notifications for scheduled or on demand 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.

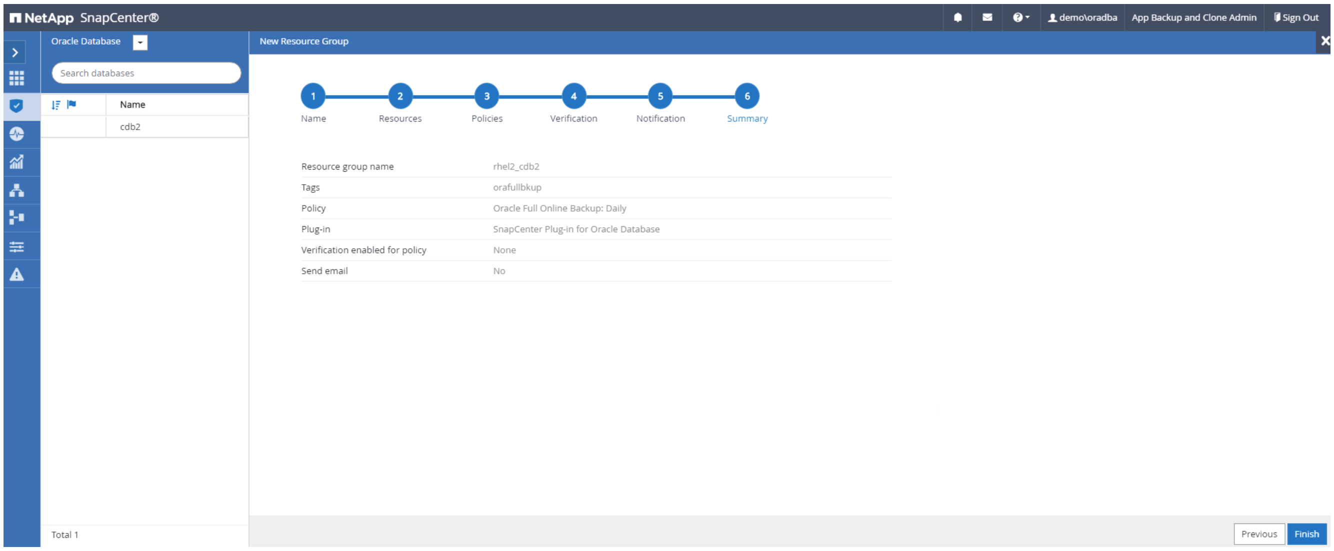
Provide email settings

Select the service accounts or people to notify regarding protection issues.

Email preference	Never
From	From email
To	Email to
Subject	Notification

□ Attach job report

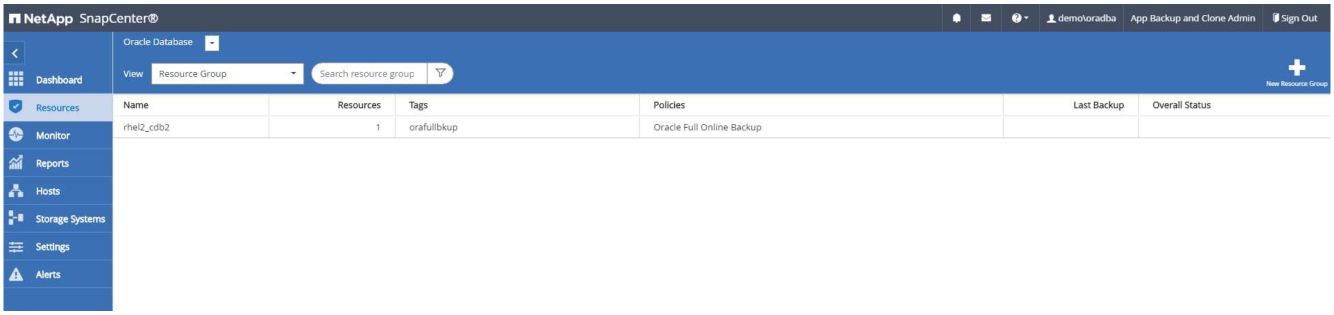
8. Summary.



Resource group name	rhel2_cdb2
Tags	orafullbkup
Policy	Oracle Full Online Backup: Daily
Plug-in	SnapCenter Plug-in for Oracle Database
Verification enabled for policy	None
Send email	No

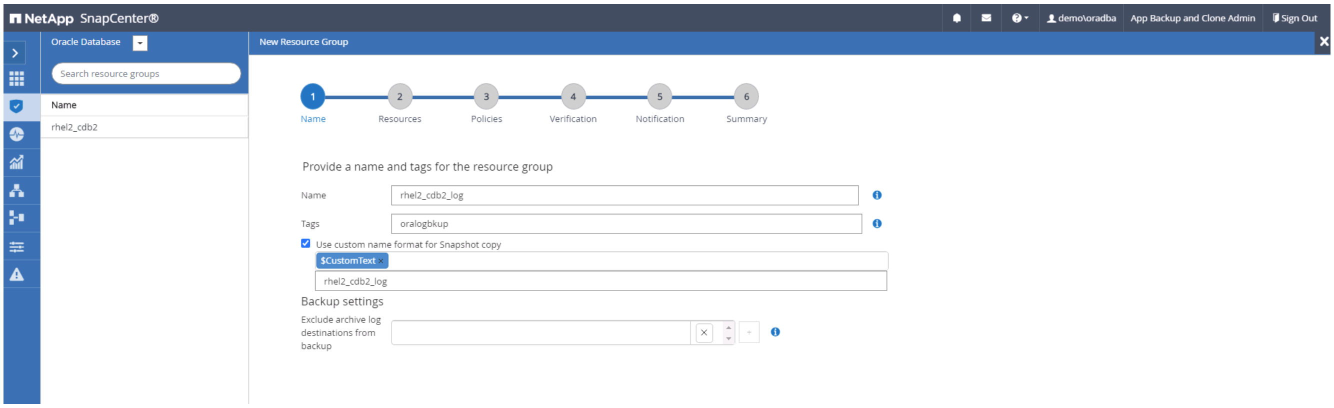
Create a resource group for log backup of Oracle

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.



Name	Resources	Tags	Policies	Last Backup	Overall Status
rhel2_cdb2	1	orafullbkup	Oracle Full Online Backup		

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.



Name
rhel2_cdb2

Provide a name and tags for the resource group

Name: rhel2_cdb2_log

Tags: oralogbkup

☑ Use custom name format for Snapshot copy

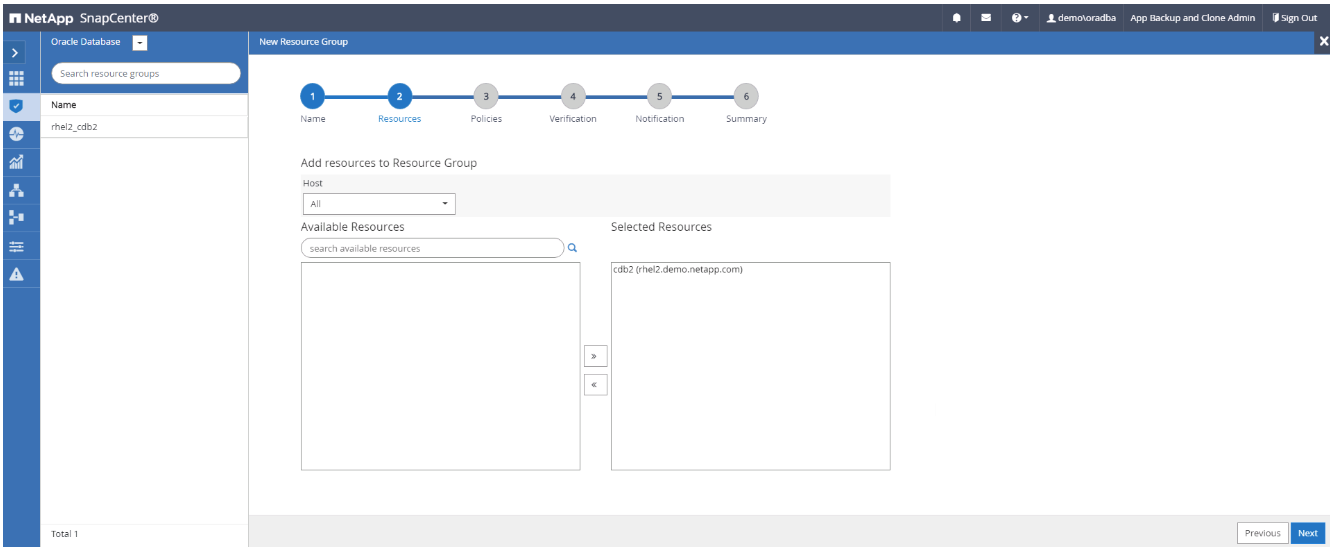
$CustomText

rhel2_cdb2_log

Backup settings

Exclude archive log destinations from backup

3. Add database resources to the resource group.



Name
rhel2_cdb2

Total 1

Add resources to Resource Group

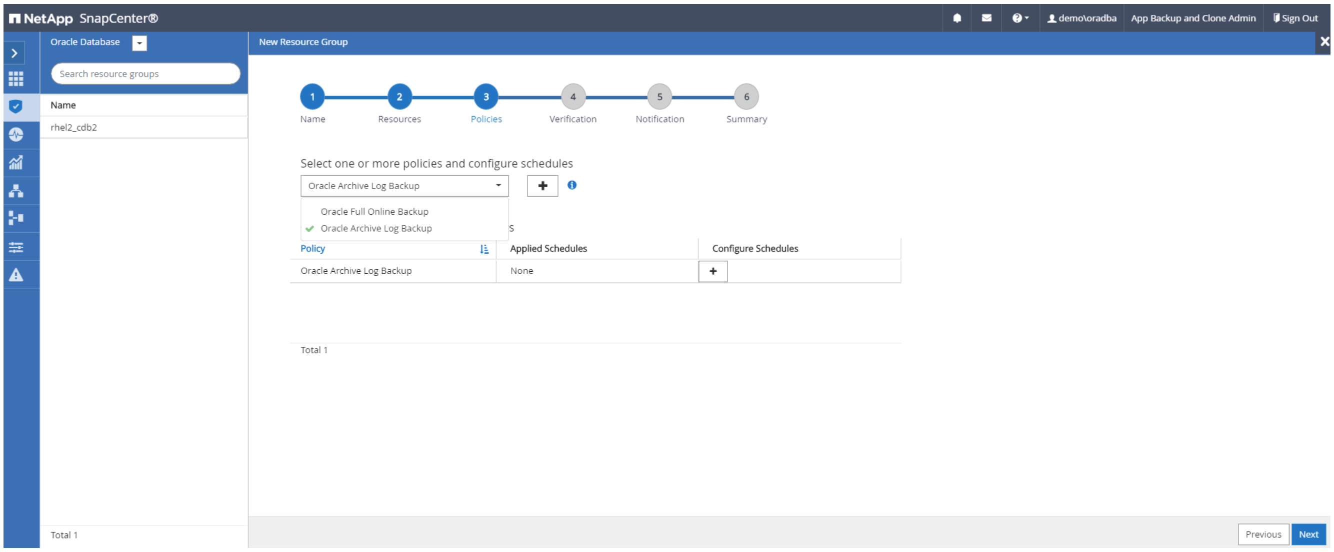
Host: All

Available Resources

Selected Resources

cdb2 (rhel2.demo.netapp.com)

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



Name
rhel2_cdb2

Total 1

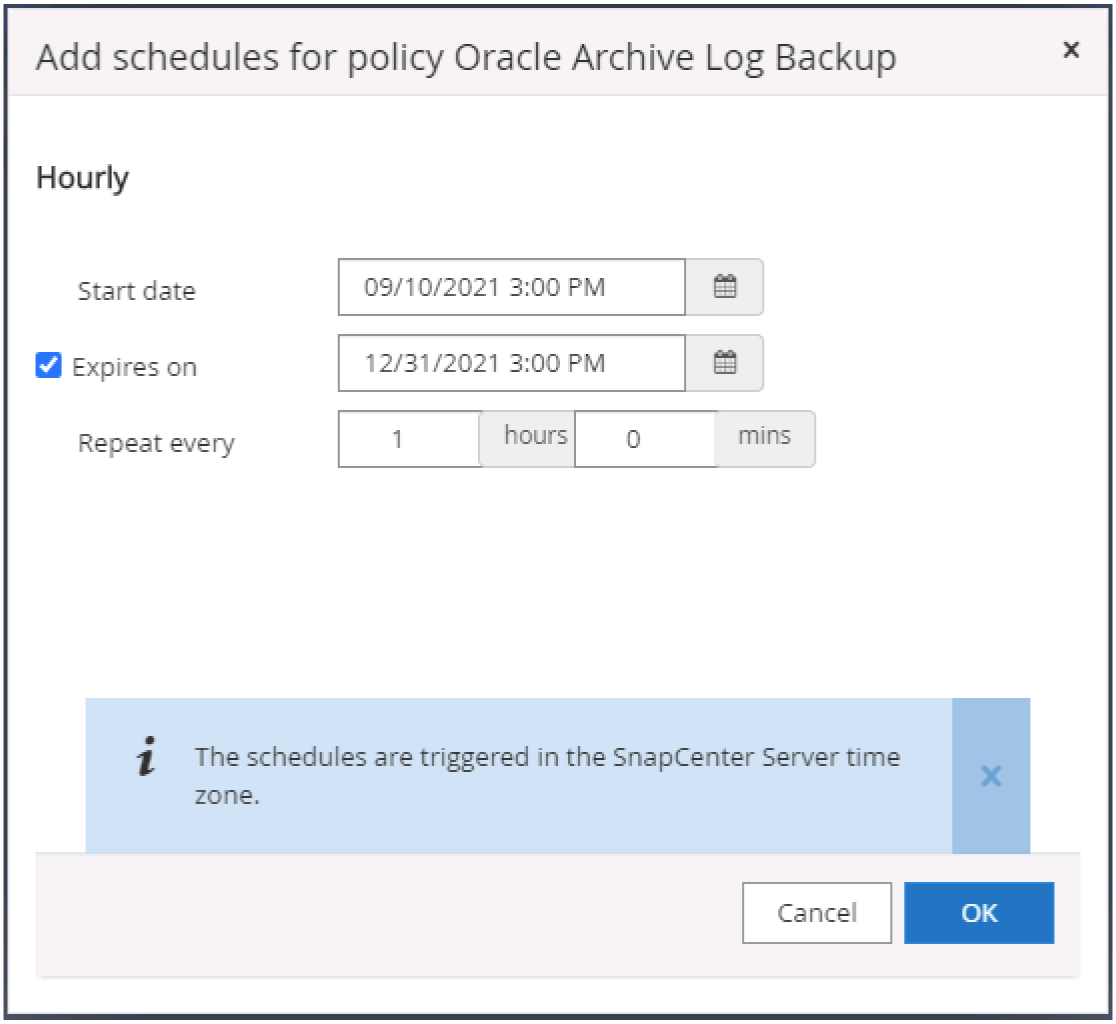
Select one or more policies and configure schedules

Oracle Archive Log Backup

Policy	Applied Schedules	Configure Schedules
Oracle Archive Log Backup	None	+

Total 1

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



Add schedules for policy Oracle Archive Log Backup

Hourly

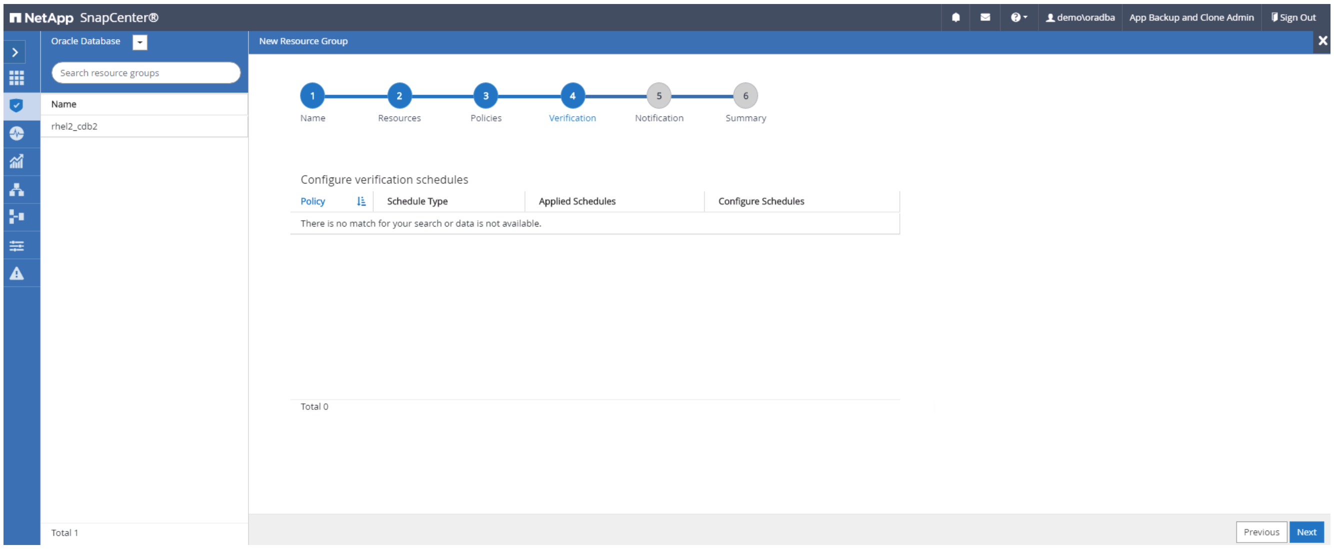
Start date: 09/10/2021 3:00 PM

☑ Expires on: 12/31/2021 3:00 PM

Repeat every: 1 hours 0 mins

The schedules are triggered in the SnapCenter Server time zone.

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

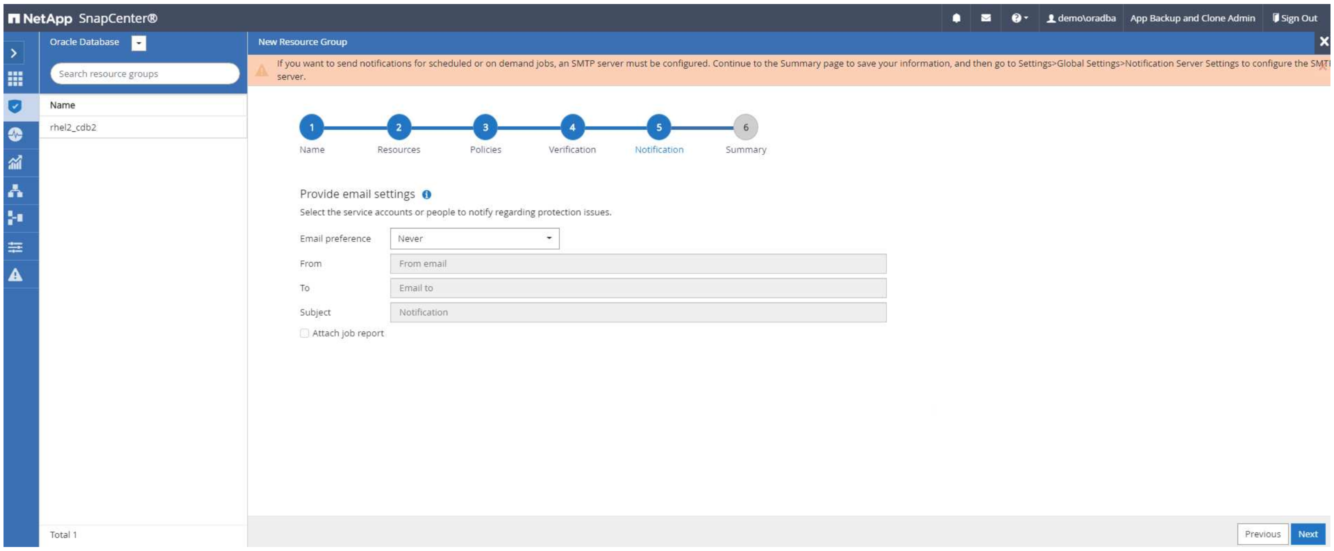


Configure verification schedules

Policy	Schedule Type	Applied Schedules	Configure Schedules
There is no match for your search or data is not available.			

Total 0

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



If you want to send notifications for scheduled or on demand 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 SMTI server.

Provide email settings

Select the service accounts or people to notify regarding protection issues.

Email preference: Never

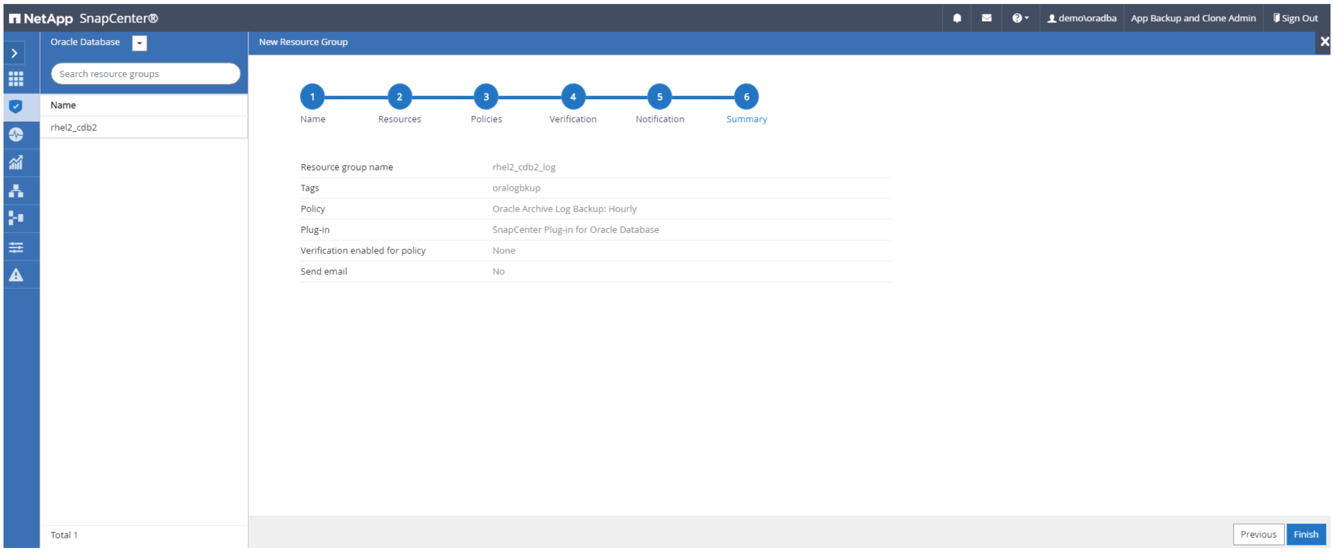
From: From email

To: Email to

Subject: Notification

□ Attach job report

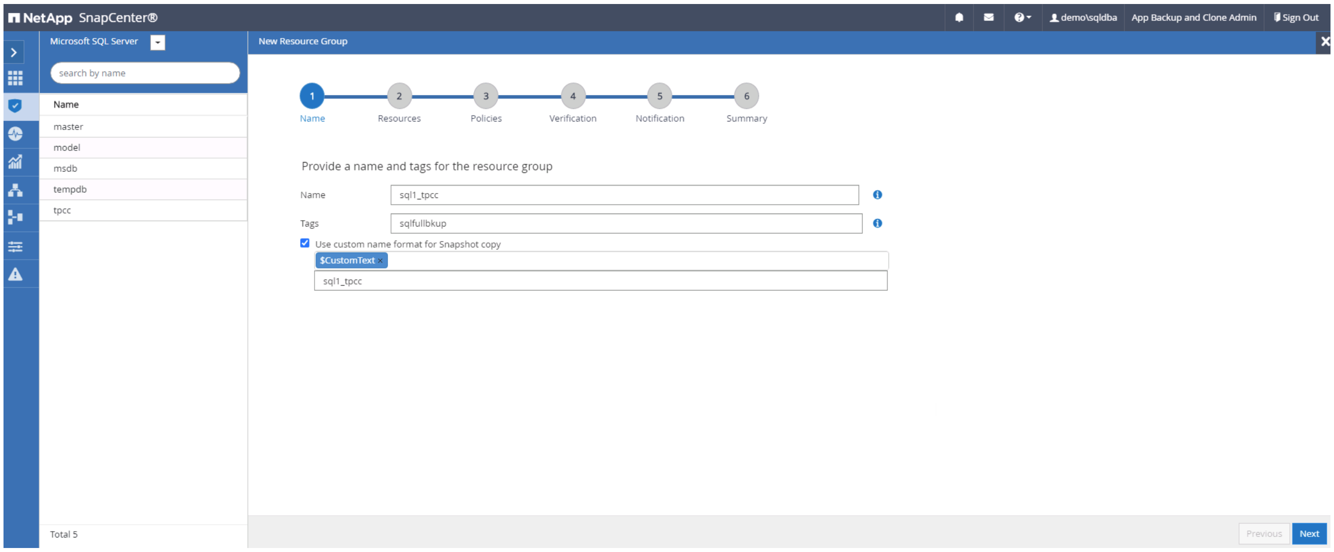
8. Summary.



Resource group name	rhel2_cdb2_log
Tags	oralogbkup
Policy	Oracle Archive Log Backup: Hourly
Plug-in	SnapCenter Plug-in for Oracle Database
Verification enabled for policy	None
Send email	No

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.



Provide a name and tags for the resource group

Name: sql1_tpcc

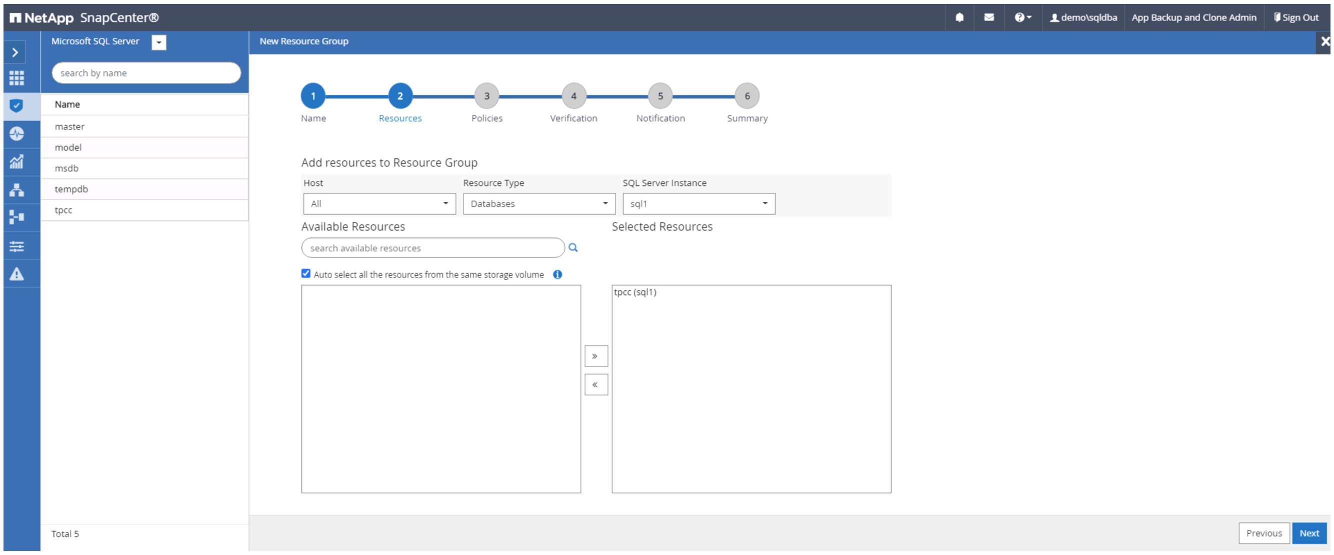
Tags: sqlfullbkup

☑ Use custom name format for Snapshot copy

$CustomText

sql1_tpcc

2. Select the database resources to be backed up.



Add resources to Resource Group

Host: All

Resource Type: Databases

SQL Server Instance: sql1

Available Resources

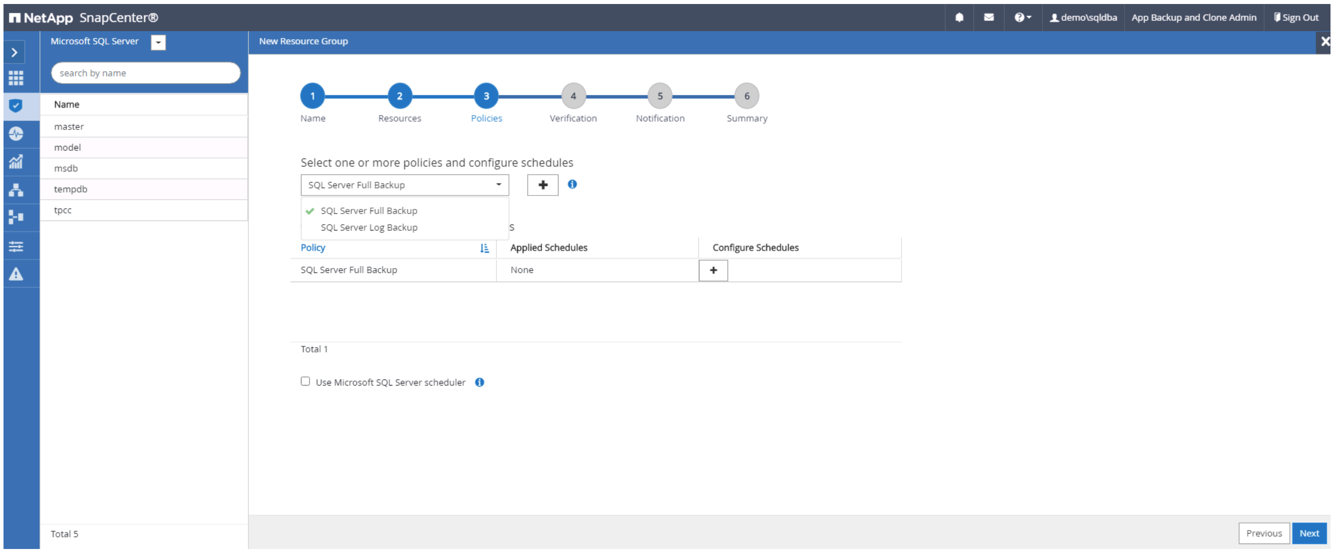
search available resources

☑ Auto select all the resources from the same storage volume

Selected Resources

tpcc (sql1)

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



Select one or more policies and configure schedules

SQL Server Full Backup

✓ SQL Server Full Backup

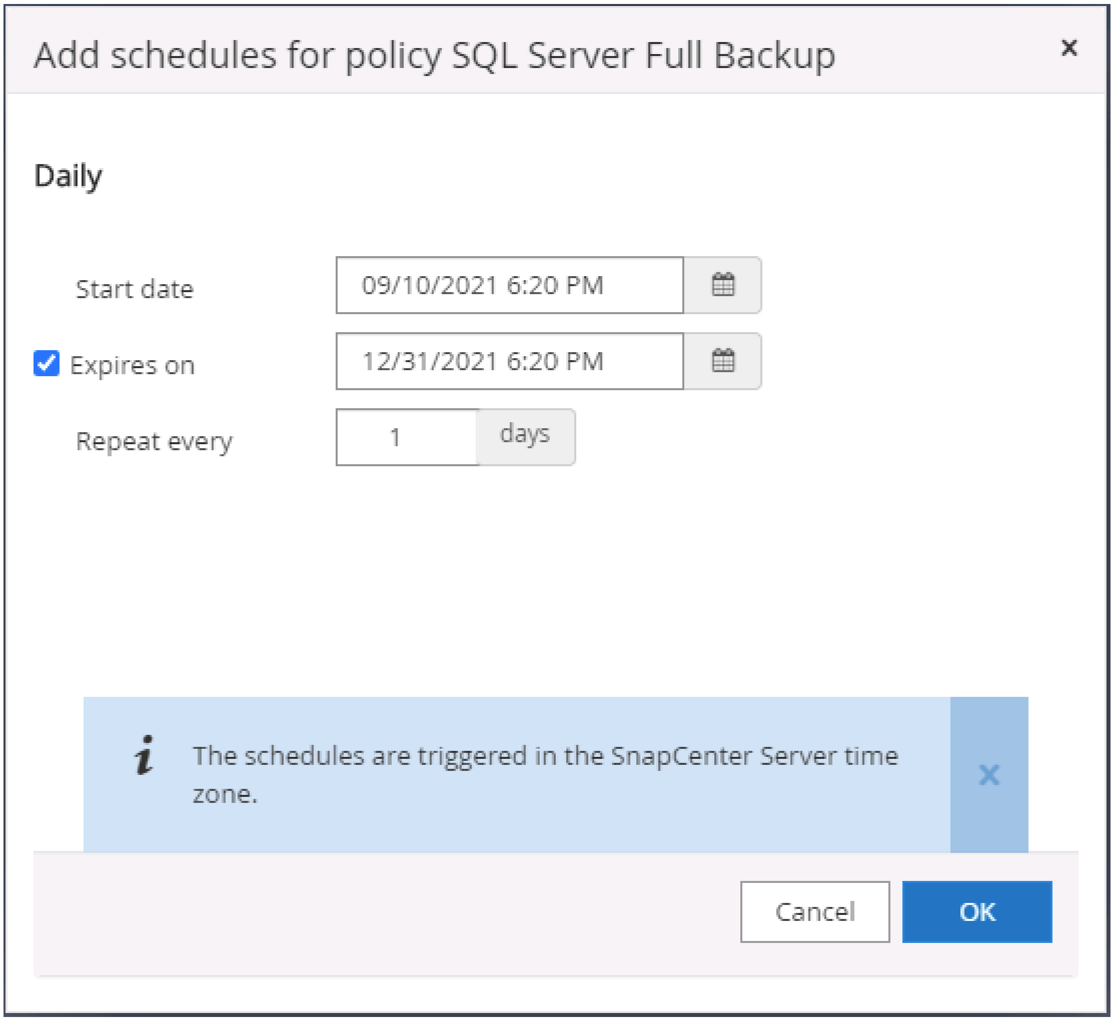
SQL Server Log Backup

Policy	Applied Schedules	Configure Schedules
SQL Server Full Backup	None	+

Total 1

☐ Use Microsoft SQL Server scheduler

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



Add schedules for policy SQL Server Full Backup

Daily

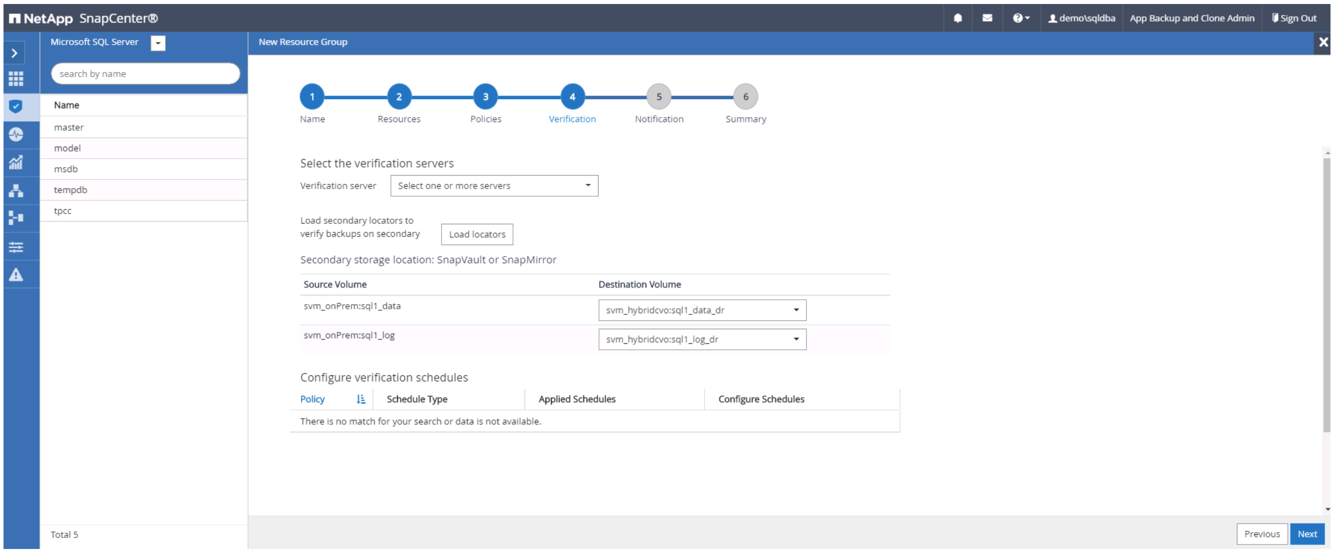
Start date: 09/10/2021 6:20 PM

☑ Expires on: 12/31/2021 6:20 PM

Repeat every: 1 days

The schedules are triggered in the SnapCenter Server time zone.

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.



New Resource Group

Microsoft SQL Server

Name
master
model
msdb
tempdb
tpcc

Total 5

Select the verification servers

Verification server: Select one or more servers

Load secondary locators to verify backups on secondary

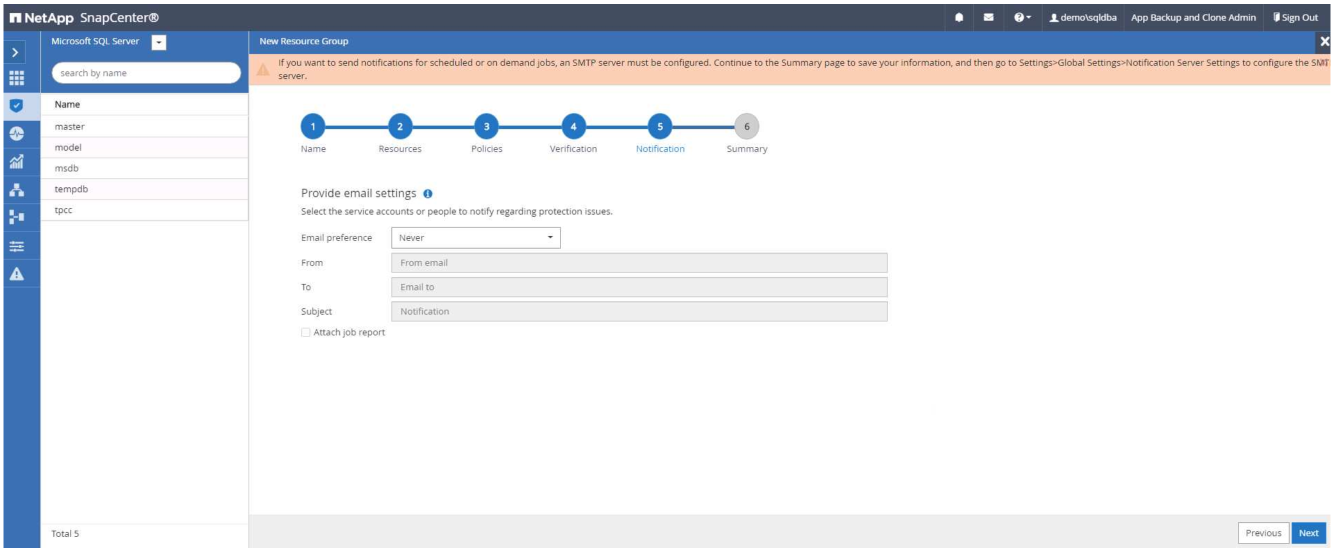
Secondary storage location: SnapVault or SnapMirror

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

Configure verification schedules

Policy	Schedule Type	Applied Schedules	Configure Schedules
There is no match for your search or data is not available.			

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



If you want to send notifications for scheduled or on demand 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 SMT server.

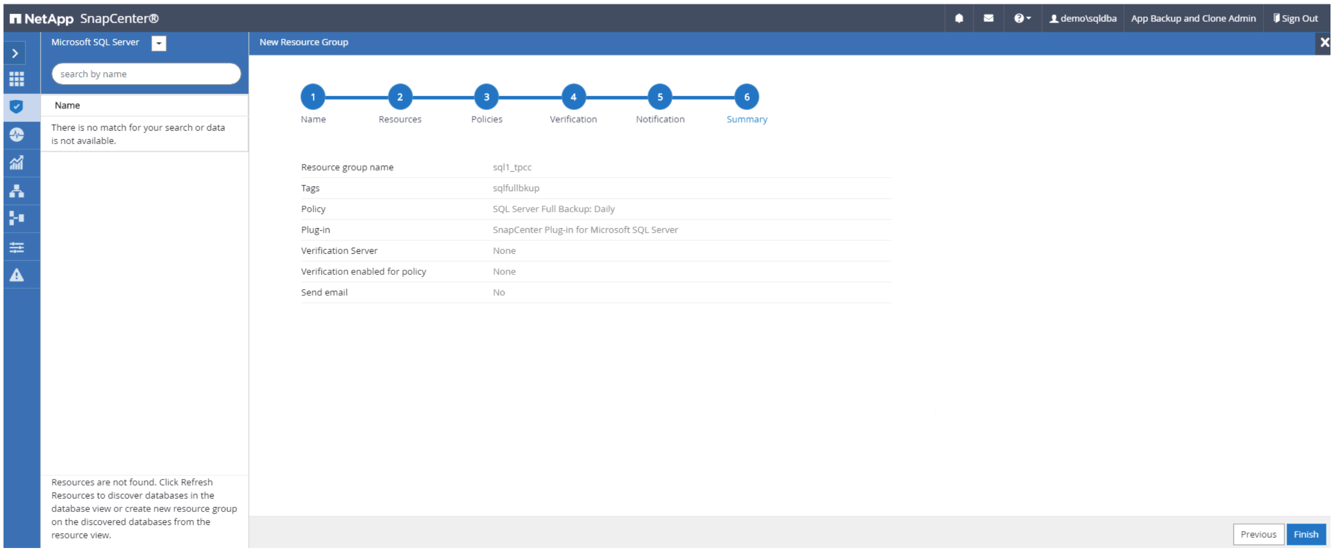
Provide email settings

Select the service accounts or people to notify regarding protection issues.

Email preference	Never
From	From email
To	Email to
Subject	Notification

□ Attach job report

7. Summary.



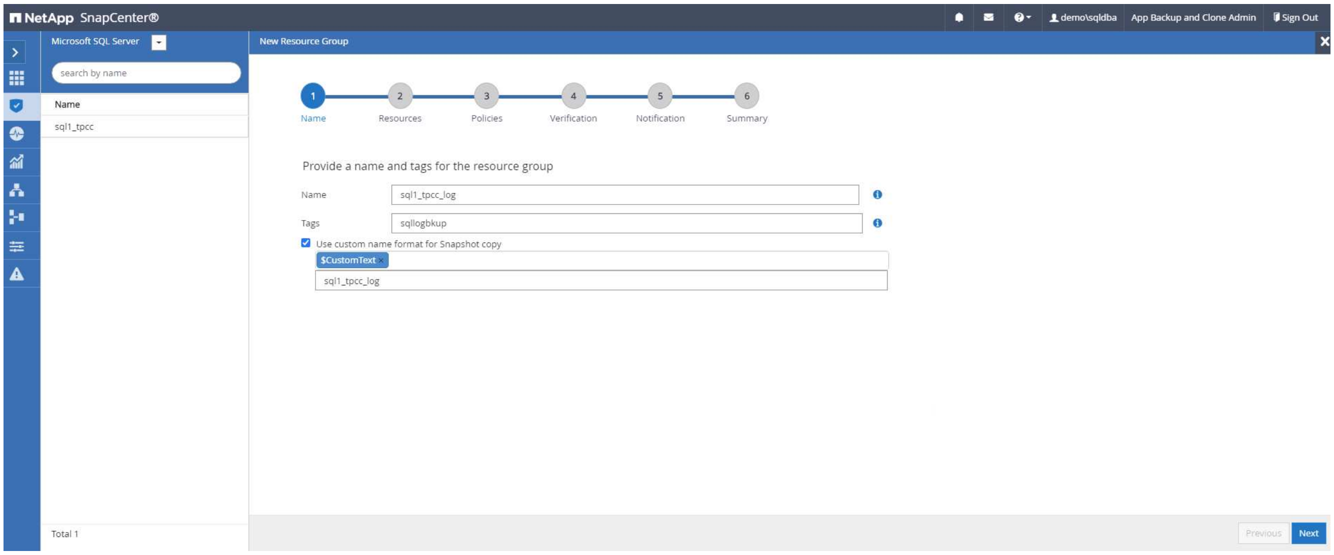
There is no match for your search or data is not available.

Resources are not found. Click Refresh Resources to discover databases in the database view or create new resource group on the discovered databases from the resource view.

Resource group name	sql1_tpcc
Tags	sqlfullbkup
Policy	SQL Server Full Backup: Daily
Plug-in	SnapCenter Plug-in for Microsoft SQL Server
Verification Server	None
Verification enabled for policy	None
Send email	No

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.



Provide a name and tags for the resource group

Name: sql1_tpcc_log

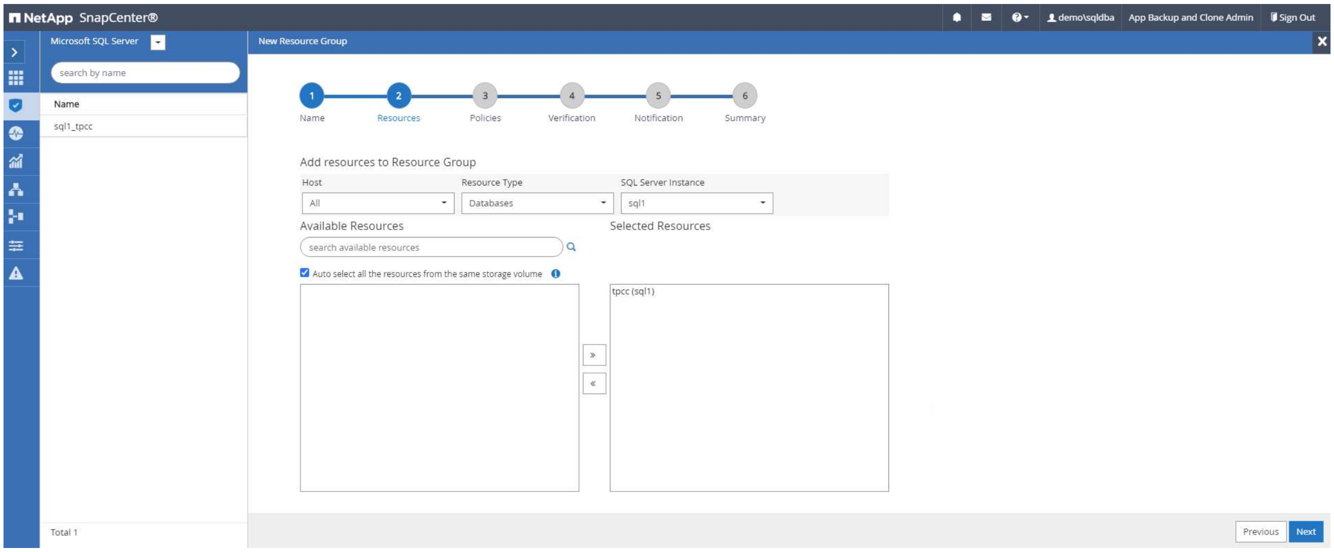
Tags: sqllogbkup

☑ Use custom name format for Snapshot copy

$CustomText

sql1_tpcc_log

2. Select the database resources to be backed up.



Add resources to Resource Group

Host: All

Resource Type: Databases

SQL Server Instance: sql1

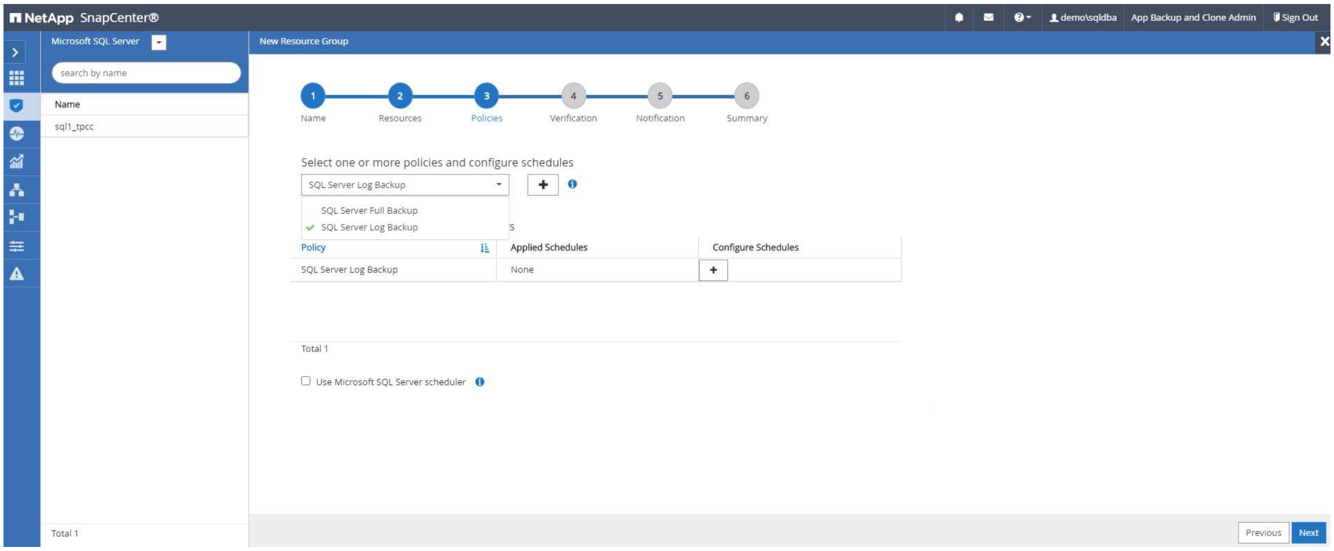
Available Resources

Selected Resources

☑ Auto select all the resources from the same storage volume

tpcc (sql1)

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



Select one or more policies and configure schedules

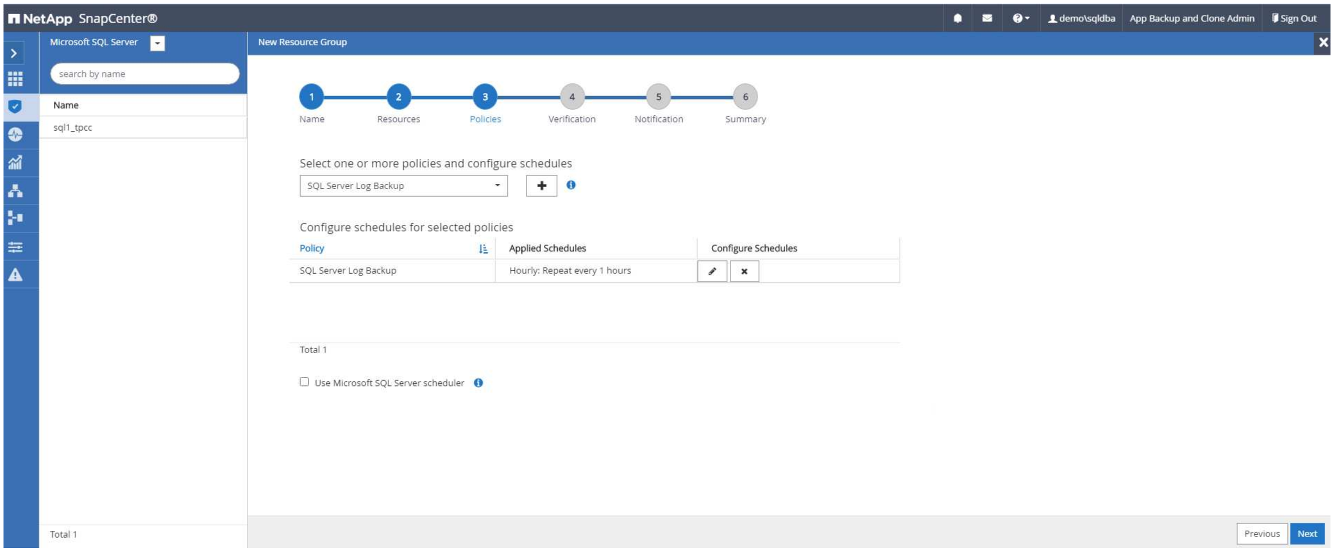
SQL Server Log Backup

Policy	Applied Schedules	Configure Schedules
SQL Server Log Backup	None	+

Total 1

☐ Use Microsoft SQL Server scheduler

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



Select one or more policies and configure schedules

SQL Server Log Backup

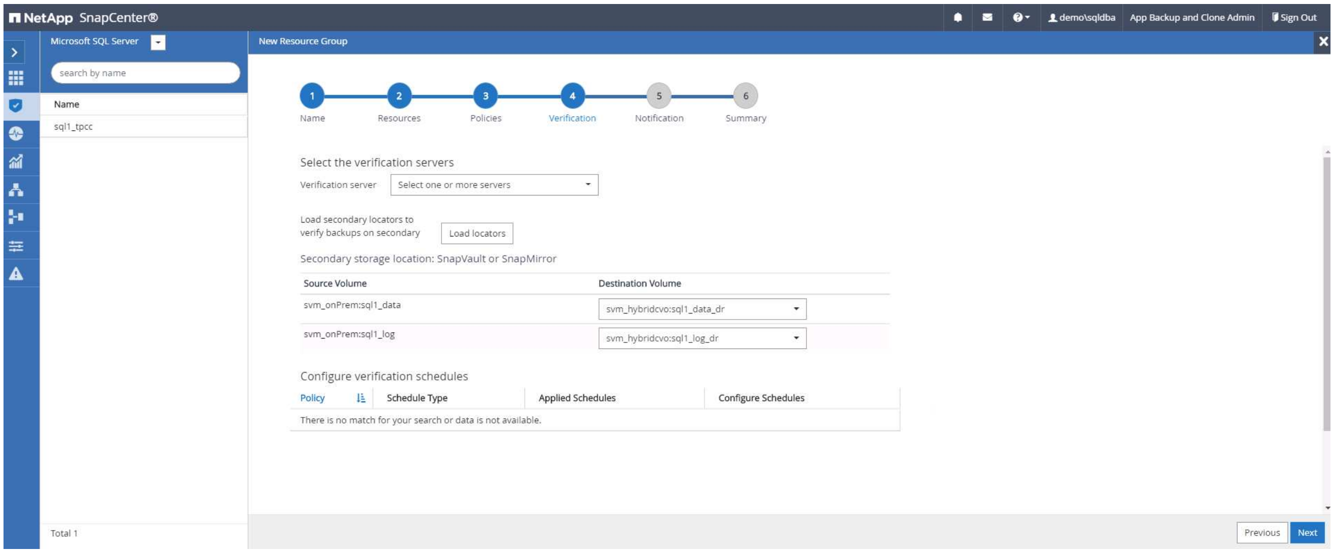
Configure schedules for selected policies

Policy	Applied Schedules	Configure Schedules
SQL Server Log Backup	Hourly: Repeat every 1 hours	

Total 1

☐ Use Microsoft SQL Server scheduler

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.



Select the verification servers

Verification server: Select one or more servers

Load secondary locators to verify backups on secondary

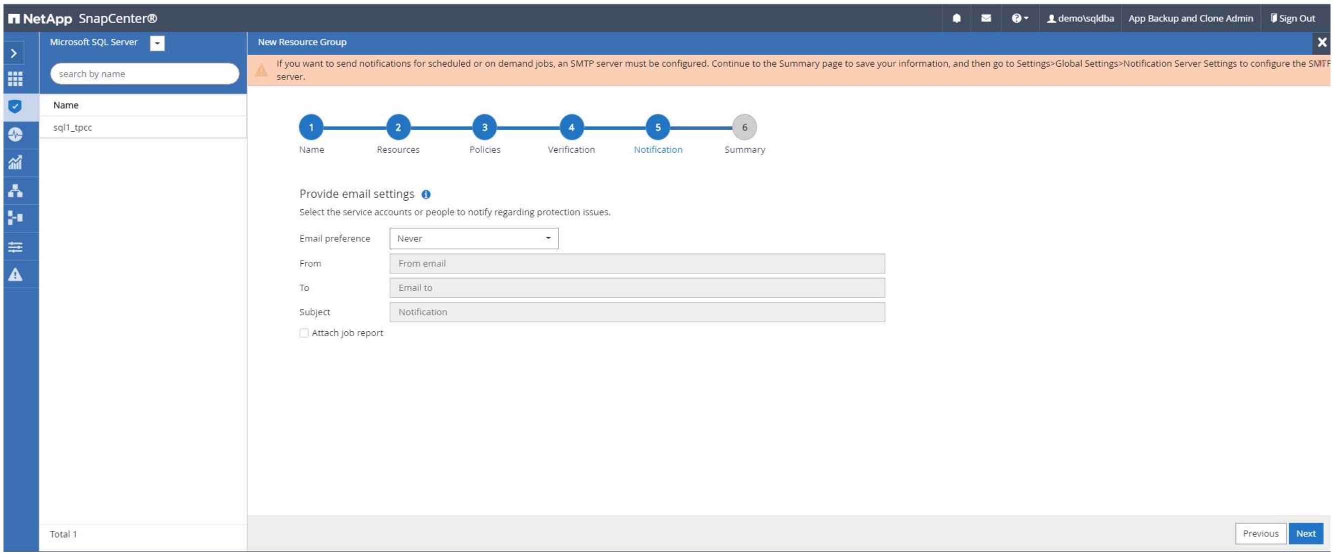
Secondary storage location: SnapVault or SnapMirror

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

Configure verification schedules

Policy	Schedule Type	Applied Schedules	Configure Schedules
There is no match for your search or data is not available.			

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



If you want to send notifications for scheduled or on demand 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.

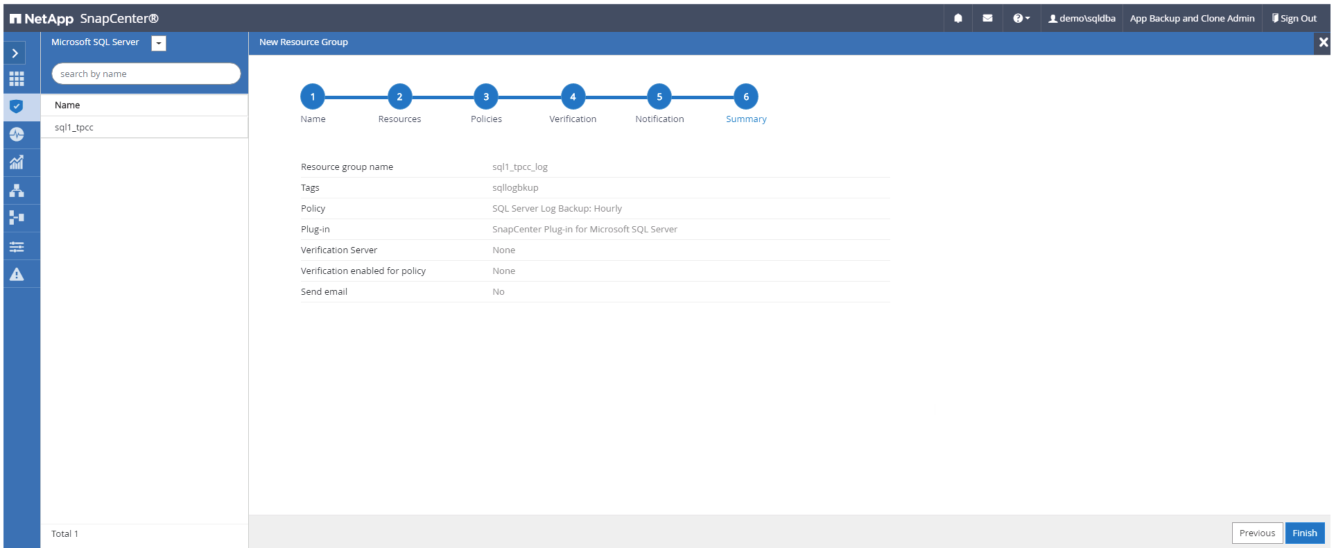
Provide email settings

Select the service accounts or people to notify regarding protection issues.

Email preference	Never
From	From email
To	Email to
Subject	Notification

□ Attach job report

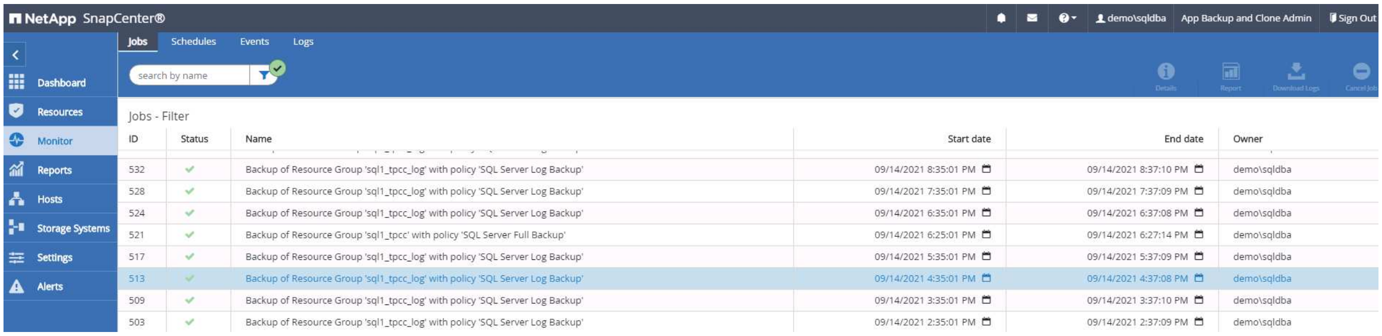
7. Summary.



Resource group name	sql1_tpcc_log
Tags	sqllogbkup
Policy	SQL Server Log Backup: Hourly
Plug-in	SnapCenter Plug-in for Microsoft SQL Server
Verification Server	None
Verification enabled for policy	None
Send email	No

9. Validate backup

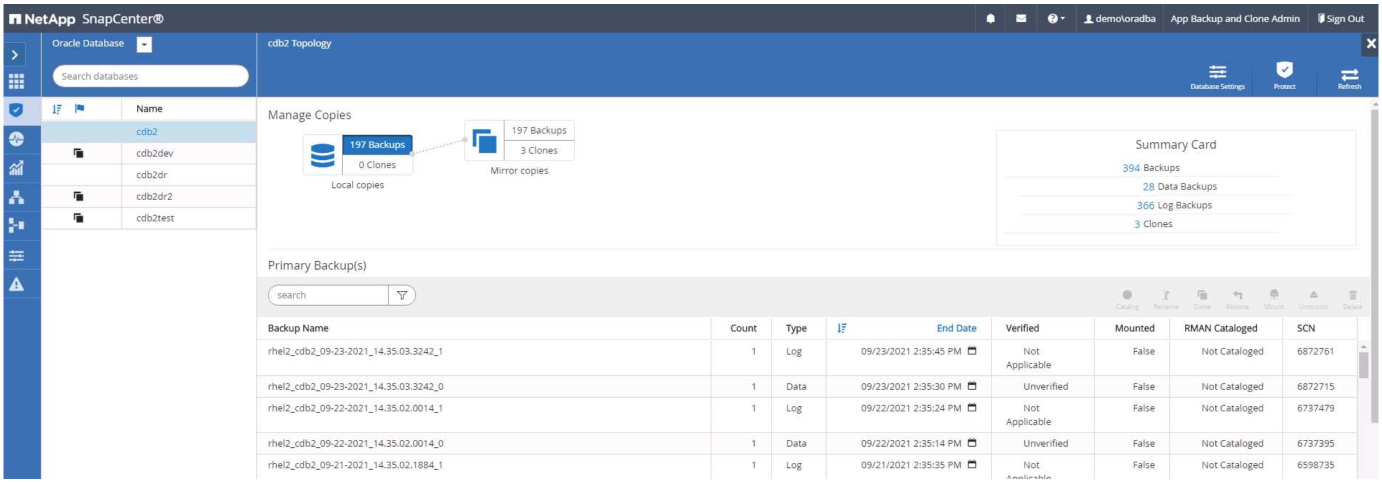
After database backup resource groups are created to protect database resources, the backup jobs runs according to the predefined schedule. Check the job execution status under the Monitor tab.



Jobs - Filter

ID	Status	Name	Start date	End date	Owner
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
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
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
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
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 3:37:10 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.



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	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.

Getting Started with AWS public cloud

This section describes the process of deploying Cloud Manager and Cloud Volumes ONTAP in AWS.

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:

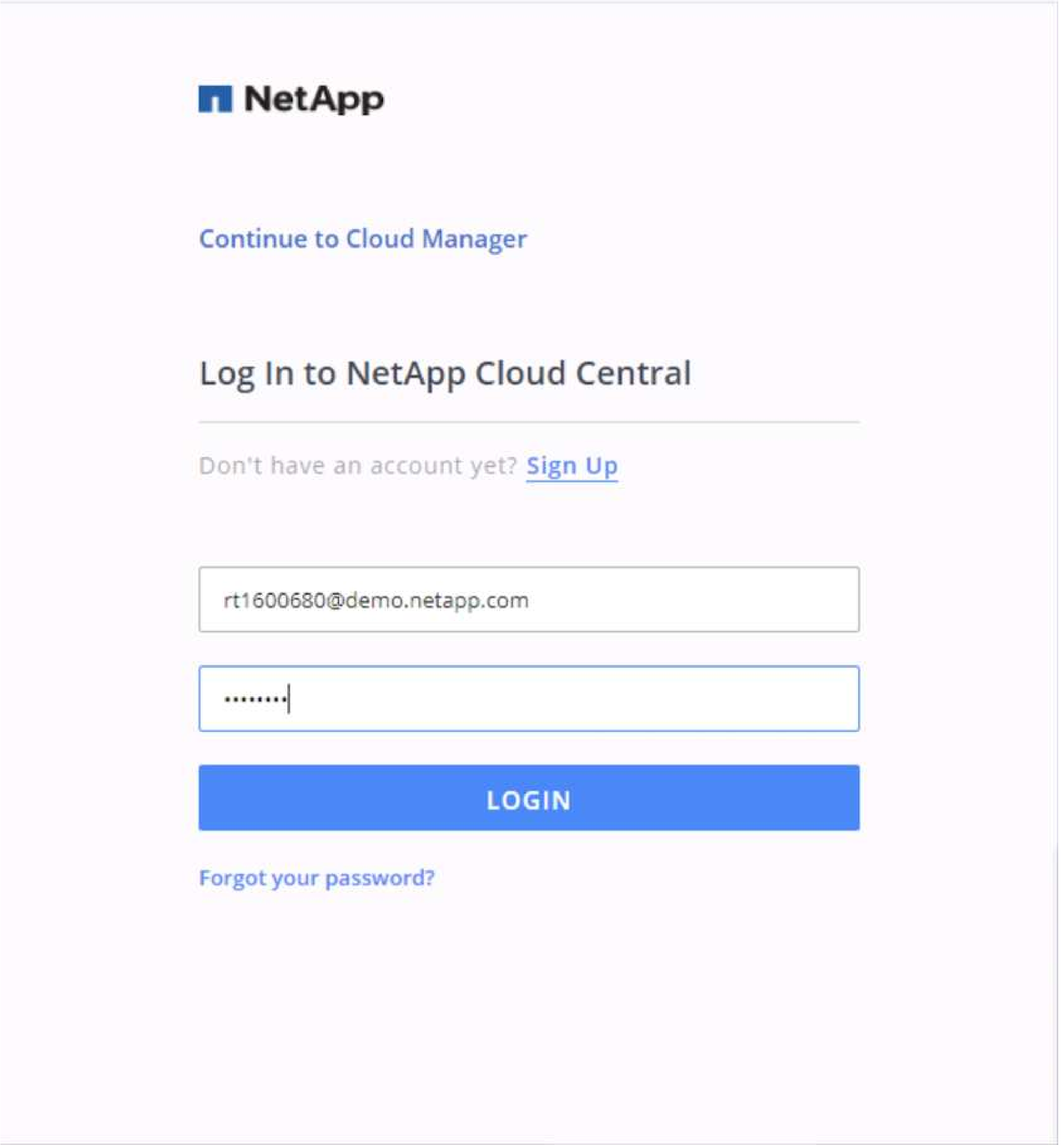
- □ AWS account
- □ VPC in your region of choice
- □ Subnet with access to the public internet
- □ Permissions to add IAM roles into your AWS account
- □ A secret key and access key for your AWS user

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

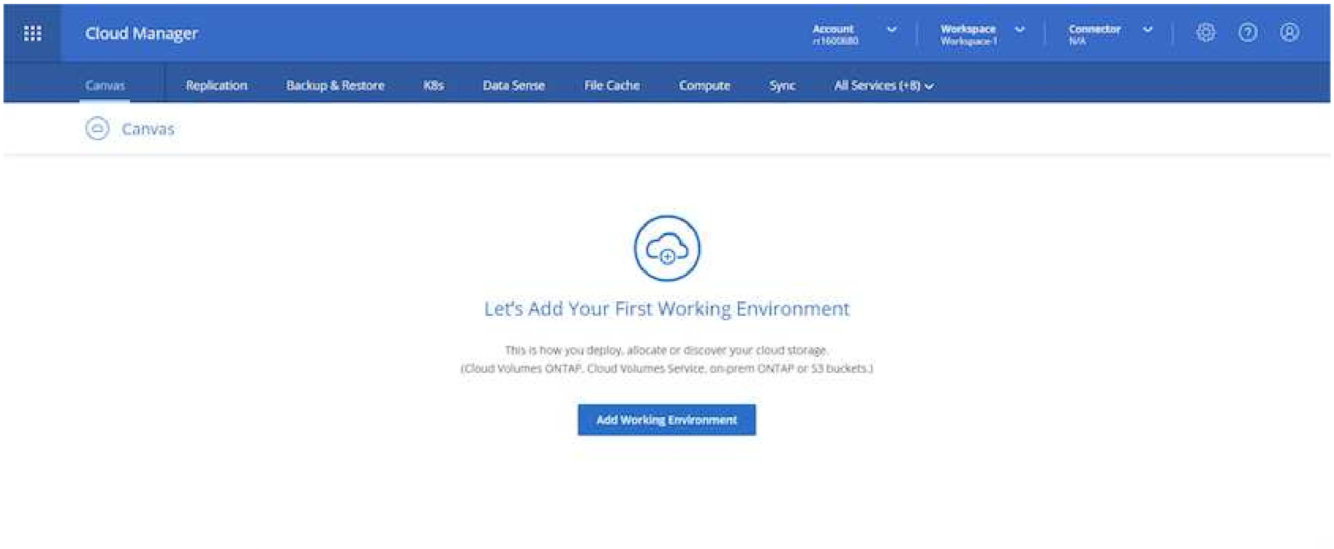
Log In to NetApp Cloud Central

Don't have an account yet? Sign Up

rt1600680@demo.netapp.com

••••••••

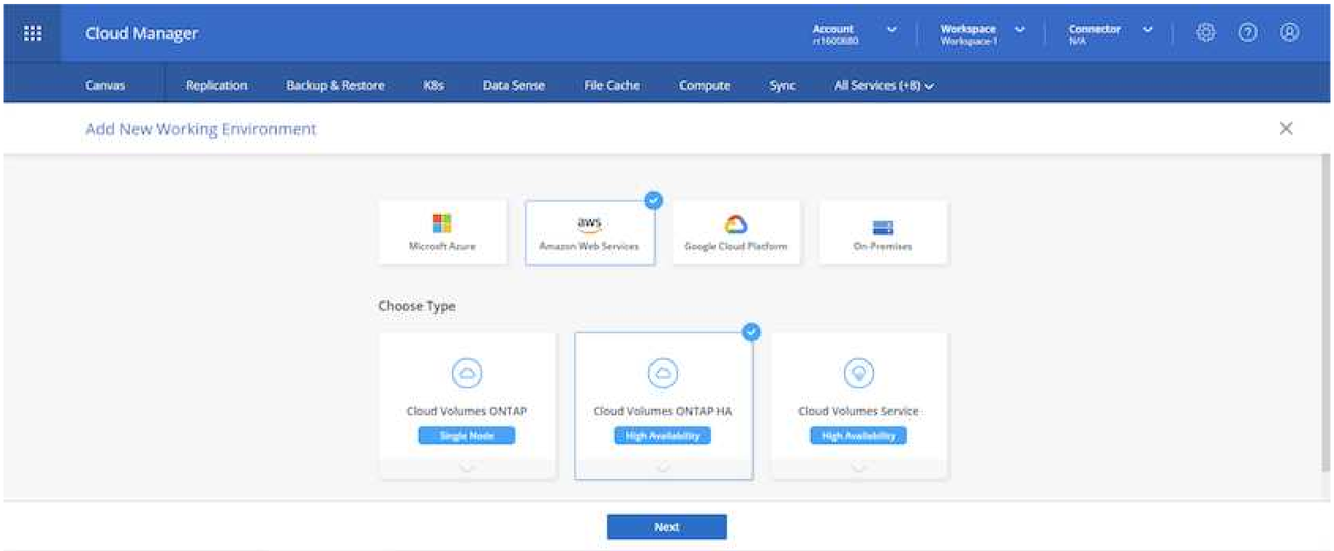
2. After you log in, you should be taken to the Canvas.



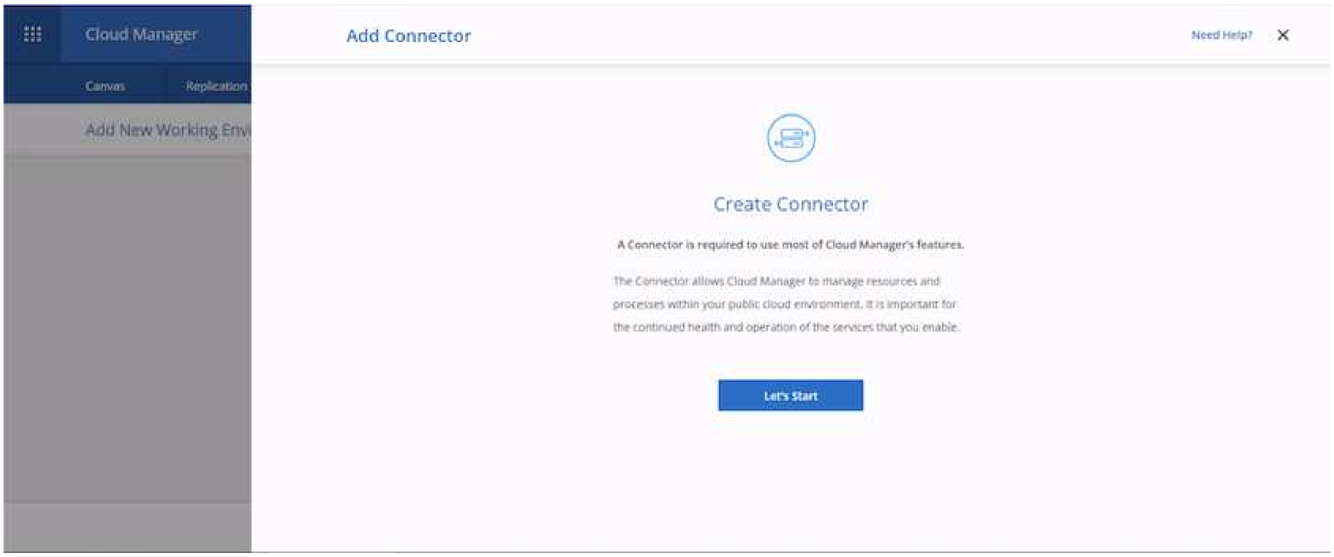
Let's Add Your First Working Environment

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

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.

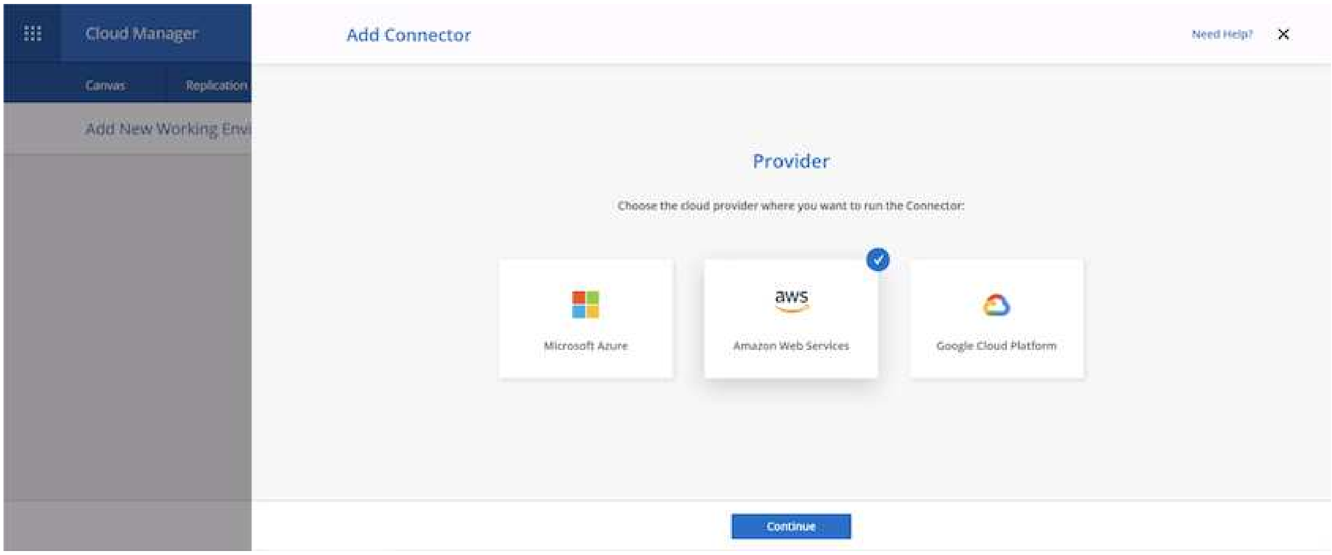


Create Connector

A Connector is required to use most of Cloud Manager's features.

The Connector allows Cloud Manager to manage resources and processes within your public cloud environment. It is important for the continued health and operation of the services that you enable.

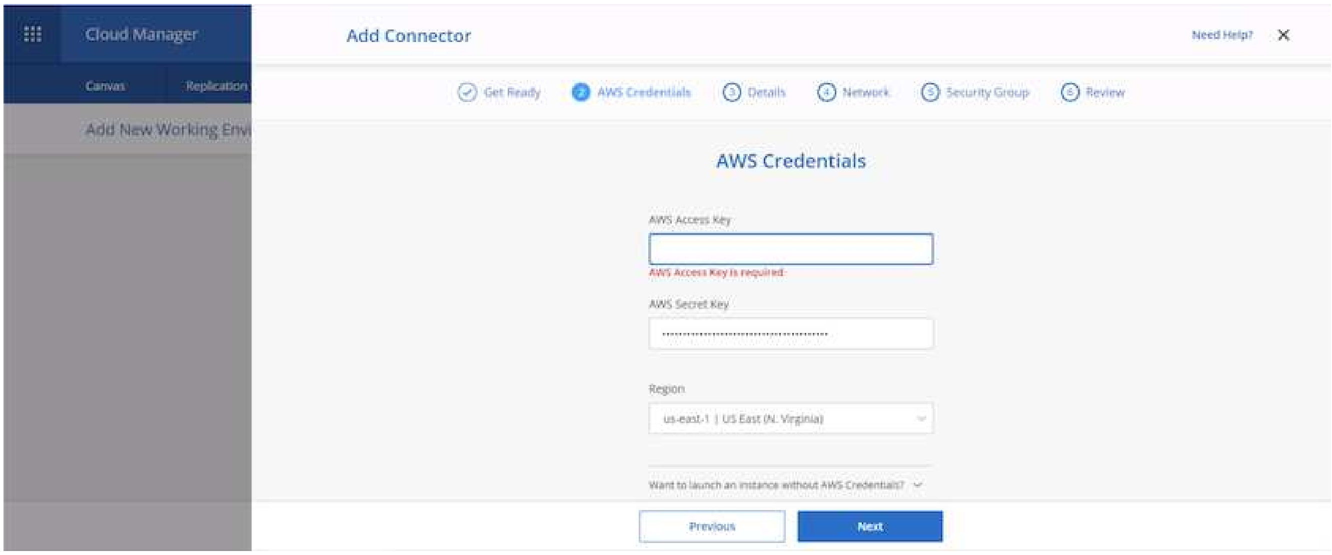
5. Click Lets Start, and then choose AWS.



Provider

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

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



AWS Credentials

AWS Access Key

AWS Access Key is required

AWS Secret Key

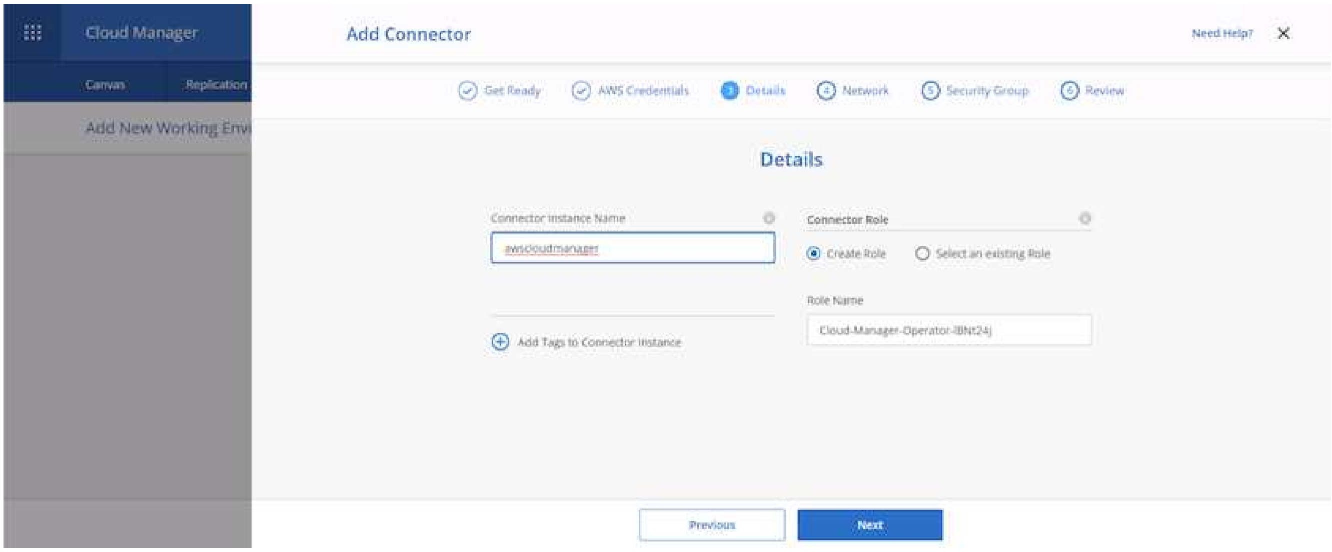
••

Region

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

Want to launch an instance without AWS Credentials?

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.



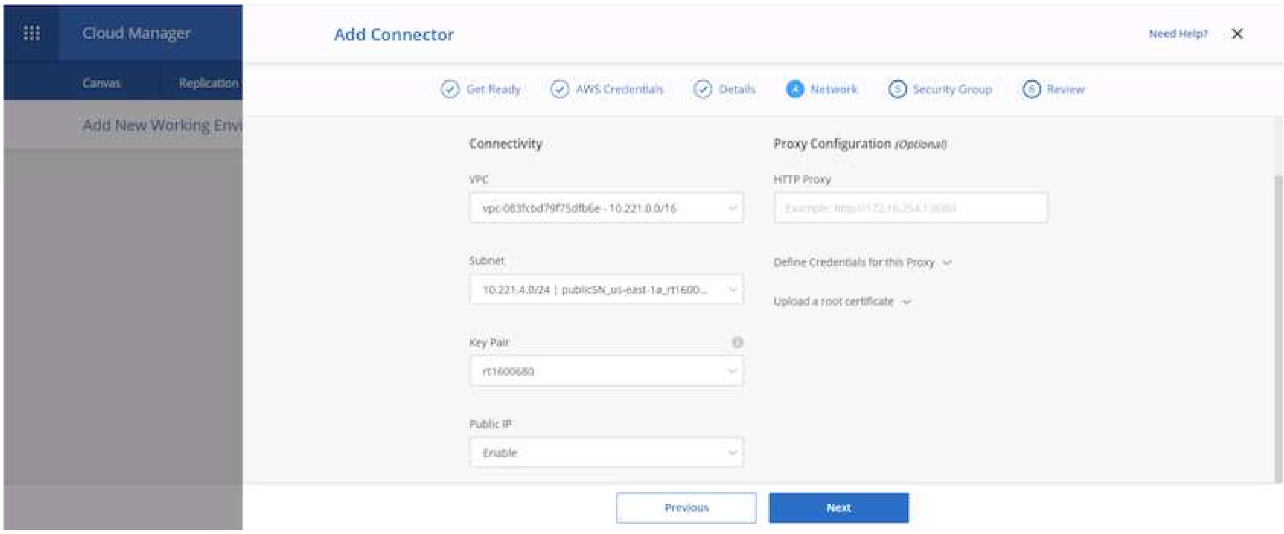
Details

Connector Instance Name: awscloudmanager

Connector Role: ● Create Role ○ Select an existing Role

Role Name: Cloud-Manager-Operator-IBNt24j

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



Connectivity

VPC: vpc-083fcbd79f75dfb6e - 10.221.0.0/16

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

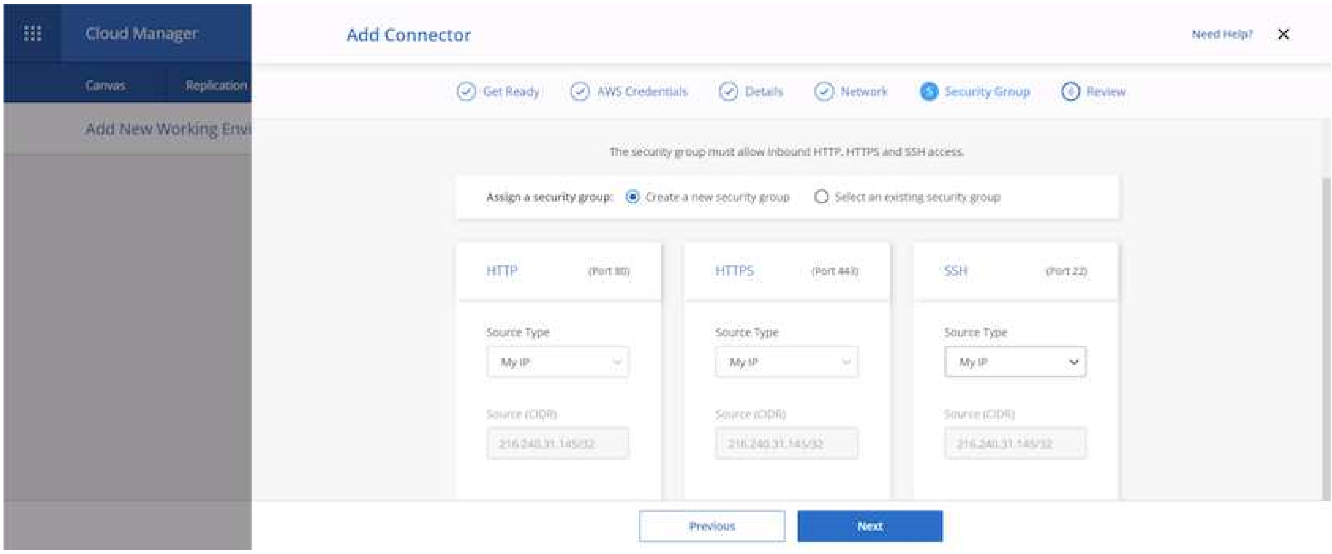
Key Pair: rt1600680

Public IP: Enable

Proxy Configuration *(Optional)*

HTTP Proxy

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.

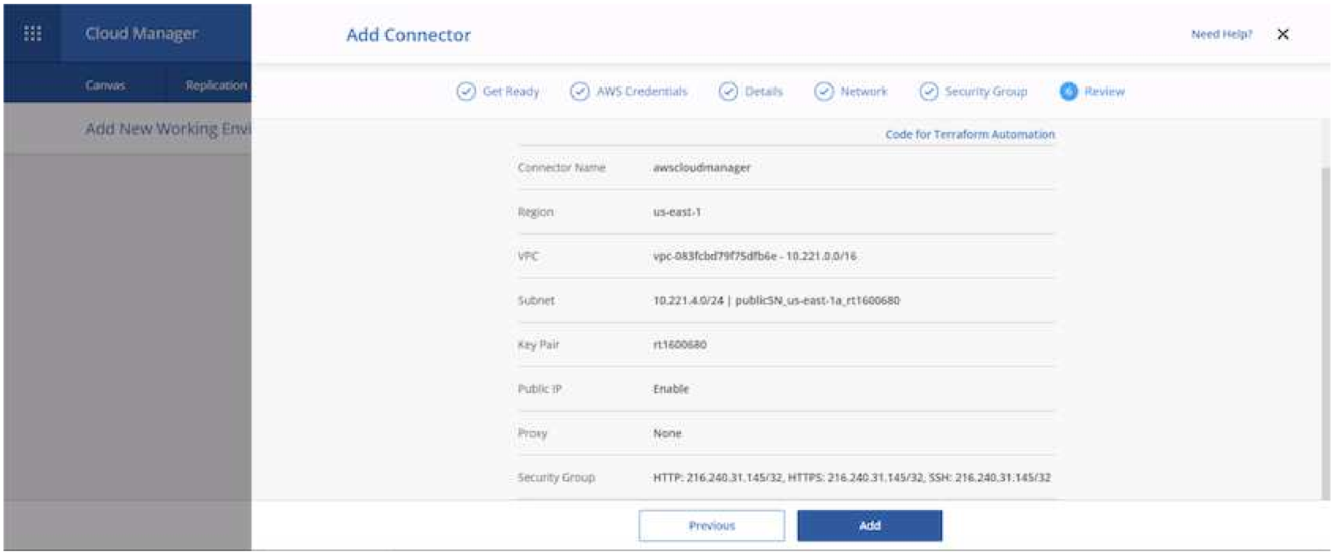


The security group must allow inbound HTTP, HTTPS and SSH access.

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

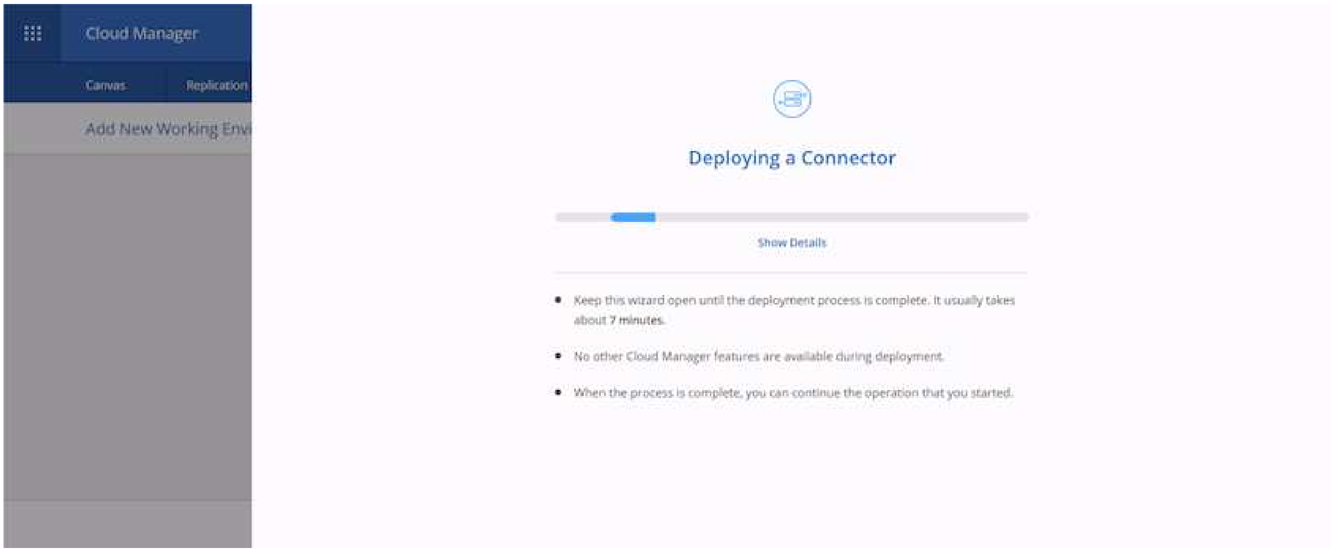
HTTP (Port 80)	HTTPS (Port 443)	SSH (Port 22)
Source Type: My IP	Source Type: My IP	Source Type: My IP
Source (CIDR): 216.240.31.145/32	Source (CIDR): 216.240.31.145/32	Source (CIDR): 216.240.31.145/32

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



Connector Name	awscloudmanager
Region	us-east-1
VPC	vpc-083fcbd79f75dfb6e - 10.221.0.0/16
Subnet	10.221.4.0/24 | publicSN_us-east-1a_rt1600680
Key Pair	rt1600680
Public IP	Enable
Proxy	None
Security Group	HTTP: 216.240.31.145/32, HTTPS: 216.240.31.145/32, SSH: 216.240.31.145/32

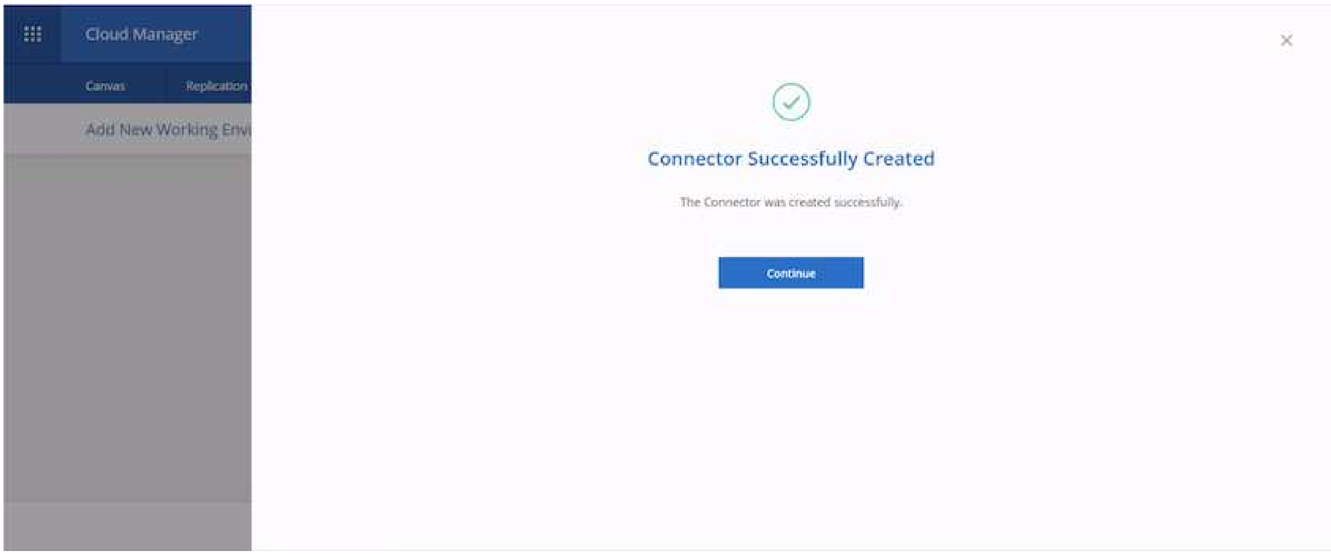
11. The connector now deploys using a cloud formation stack. You can monitor its progress from Cloud Manager or through AWS.



Deploying a Connector

- Keep this wizard open until the deployment process is complete. It usually takes about 7 minutes.
- No other Cloud Manager features are available during deployment.
- When the process is complete, you can continue the operation that you started.

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

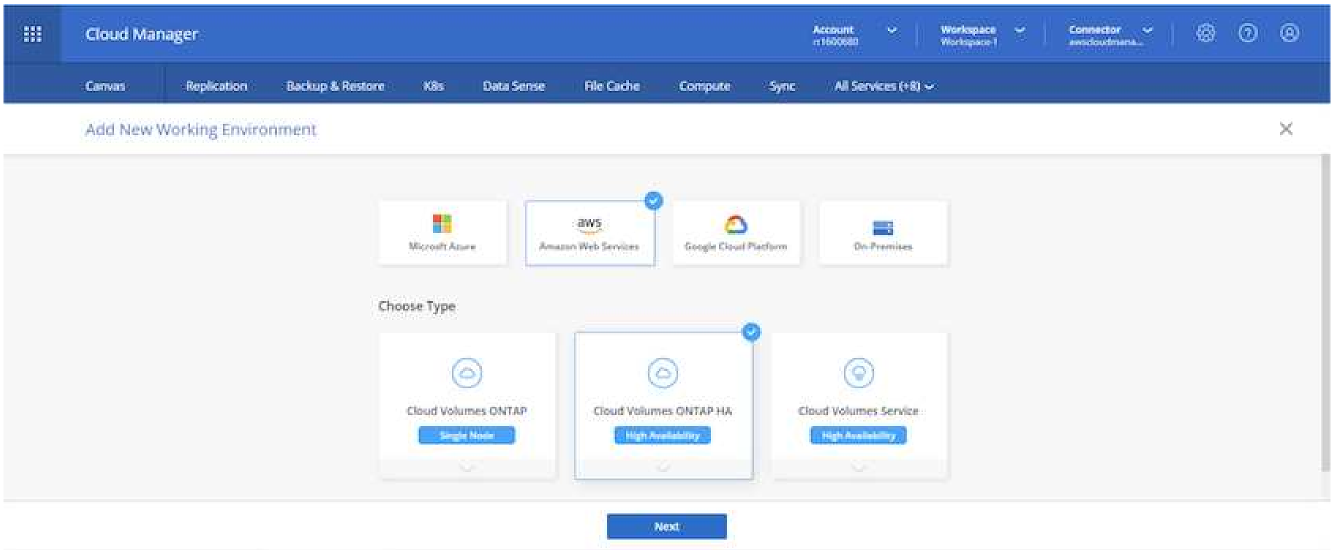


Connector Successfully Created

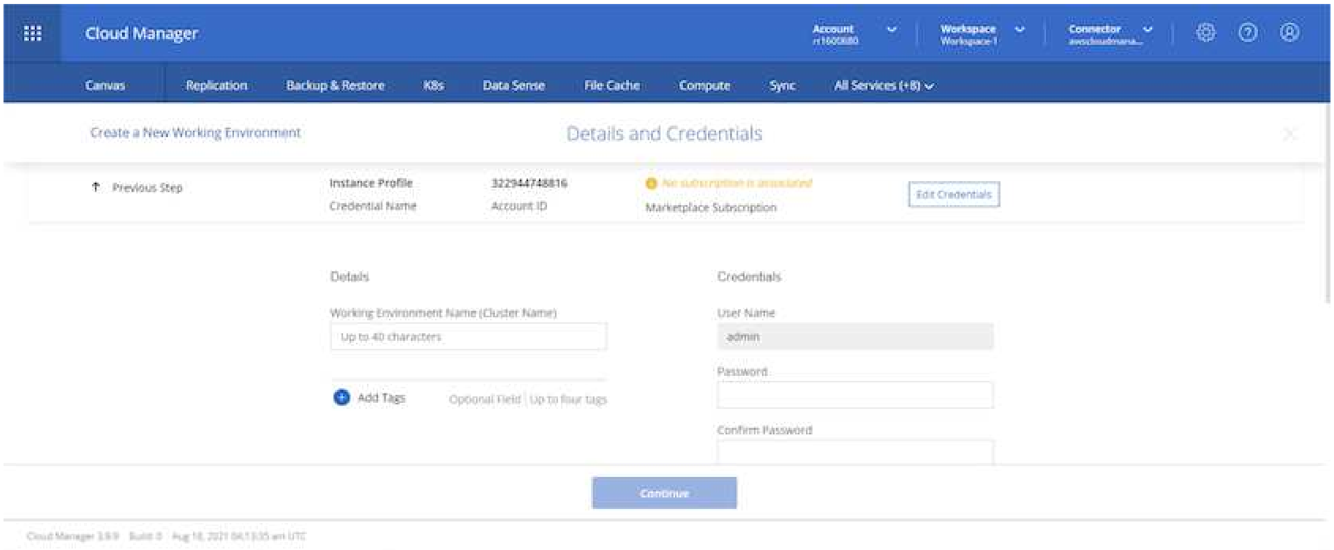
The Connector was created successfully.

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

Instance Profile
Credential Name

322944748816
Account ID

Marketplace Subscription

Details

Working Environment Name (Cluster Name)
Up to 40 characters

Optional Field | Up to four tags

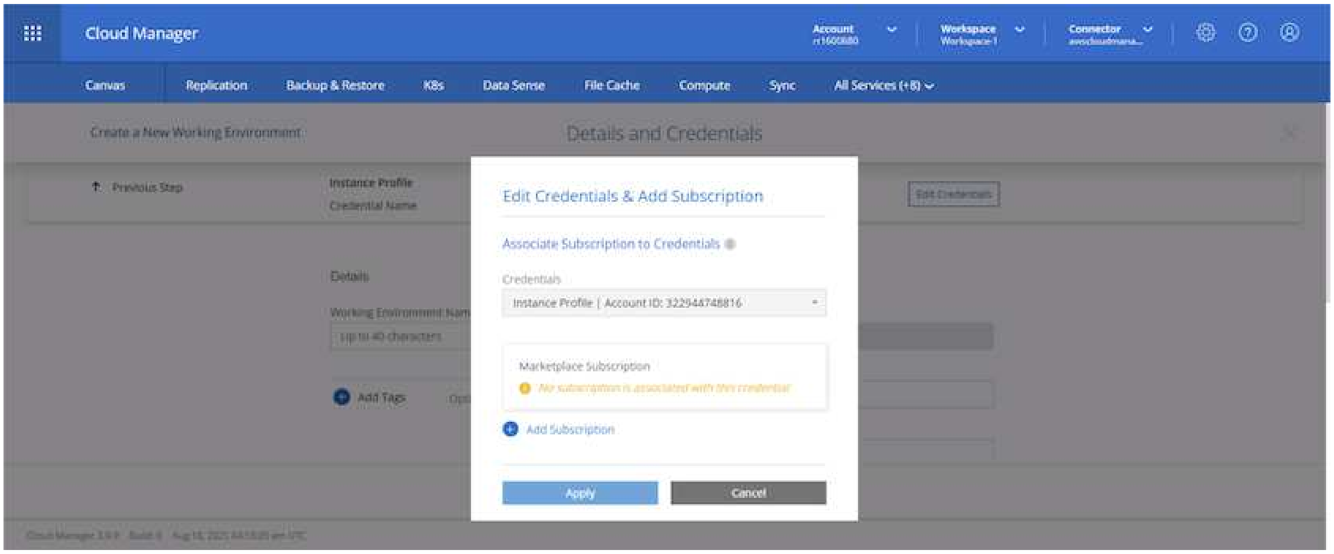
Credentials

User Name
admin

Password

Confirm Password

3. Choose Add Subscription.



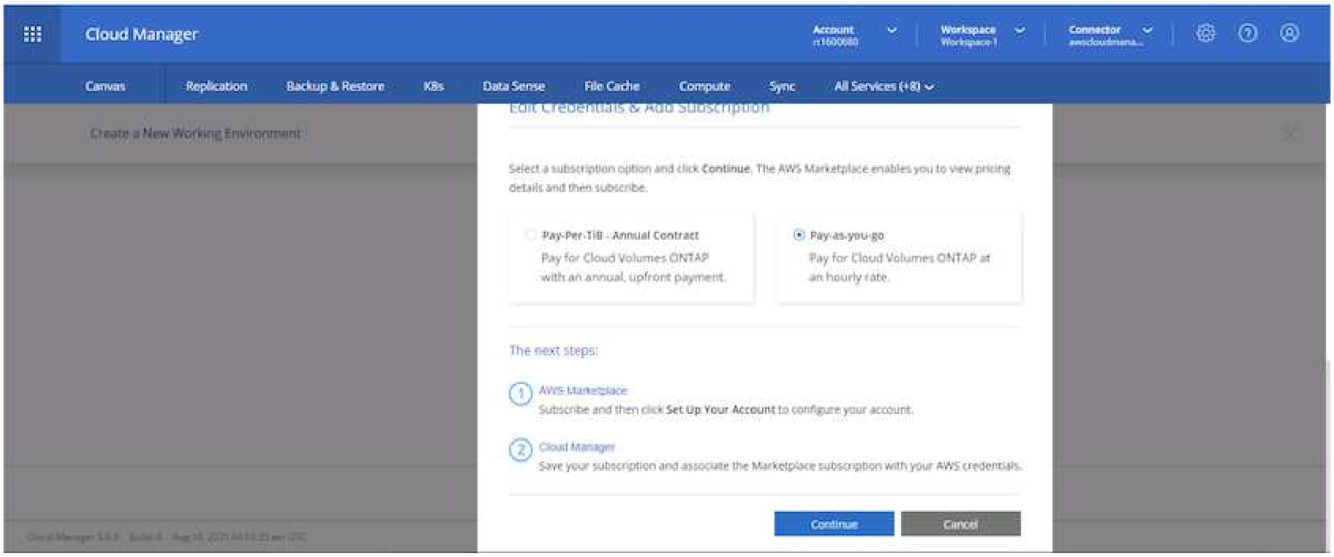
Edit Credentials & Add Subscription

Associate Subscription to Credentials

Credentials
Instance Profile | Account ID: 322944748816

Marketplace Subscription
No subscription is associated with this credential

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.

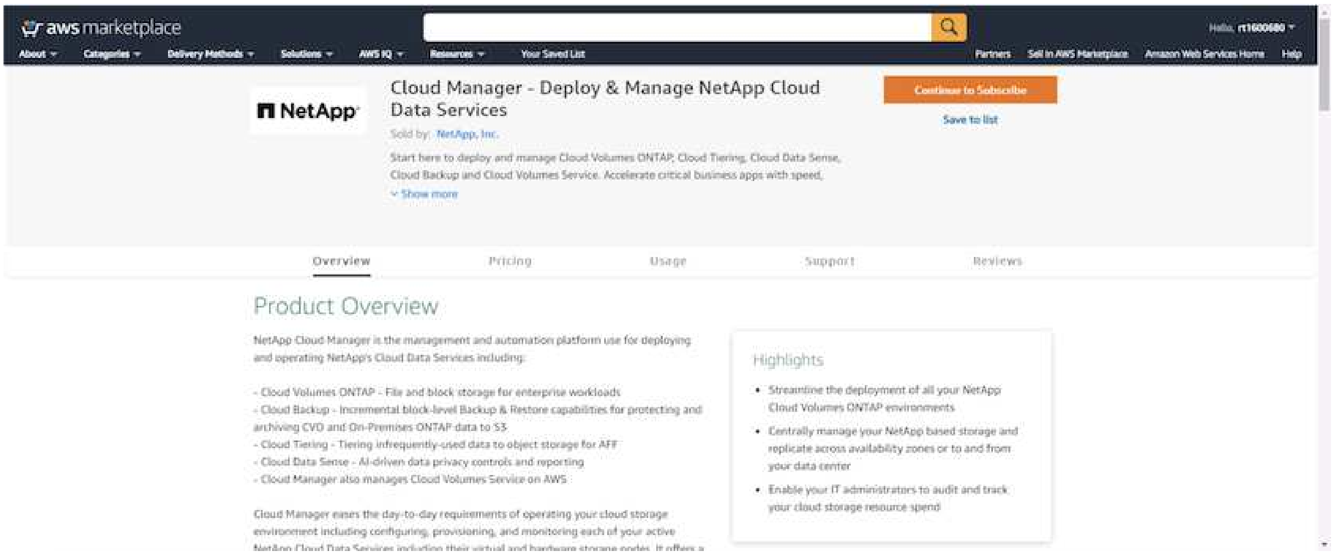
● Pay-as-you-go
Pay for Cloud Volumes ONTAP at an hourly rate.

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.

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,

Product Overview

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

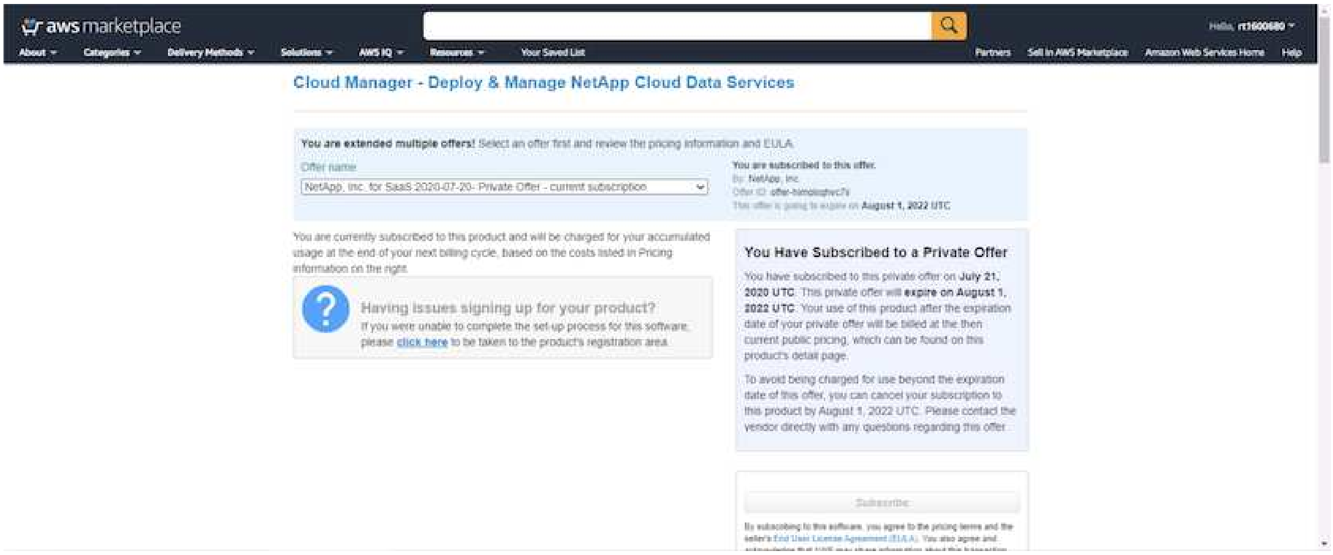
- Cloud Volumes ONTAP - File and block storage for enterprise workloads
- Cloud Backup - Incremental block-level Backup & Restore capabilities for protecting and archiving CVO and On-Premises ONTAP data to S3
- Cloud Tiering - Tiering infrequently-used data to object storage for AFF
- Cloud Data Sense - 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.



Cloud Manager - Deploy & Manage NetApp Cloud Data Services

You are extended multiple offers! Select an offer first and review the pricing information and EULA.

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

You are subscribed to this offer.
By: NetApp, Inc
Offer ID: offer-bimolqhvc7s
This offer is going to expire on **August 1, 2022 UTC**

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.

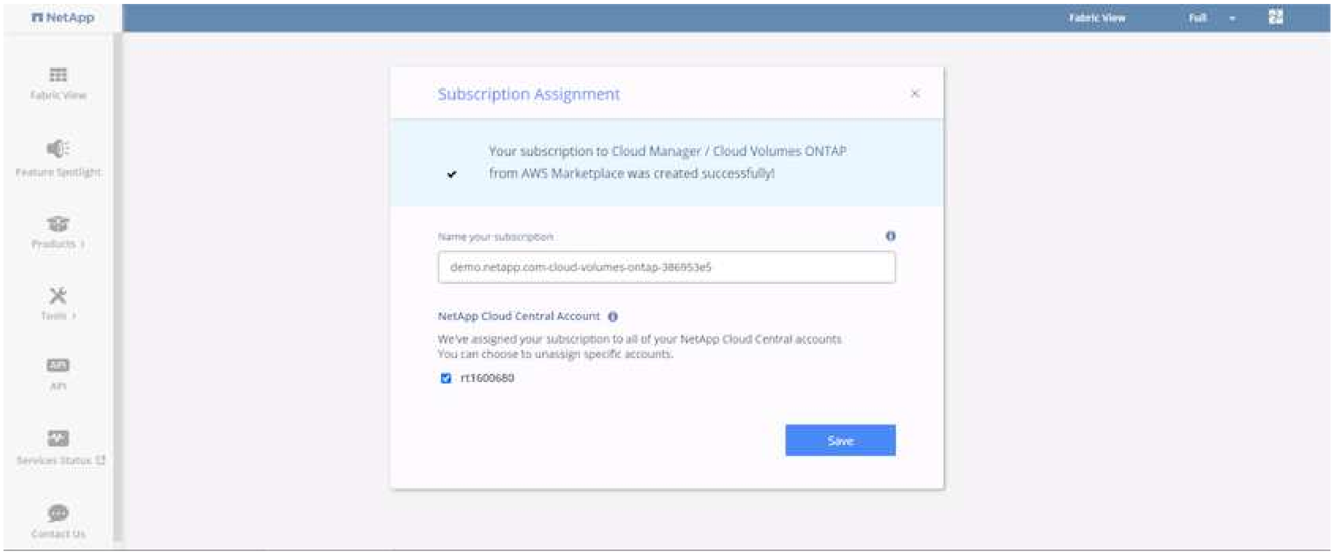
You Have Subscribed to a Private Offer

You have subscribed to this private offer on **July 21, 2020 UTC**. This 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.

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.



Subscription Assignment

✓ Your subscription to Cloud Manager / Cloud Volumes ONTAP from AWS Marketplace was created successfully!

Name your subscription

demo.netapp.com-cloud-volumes-ontap-386953e5

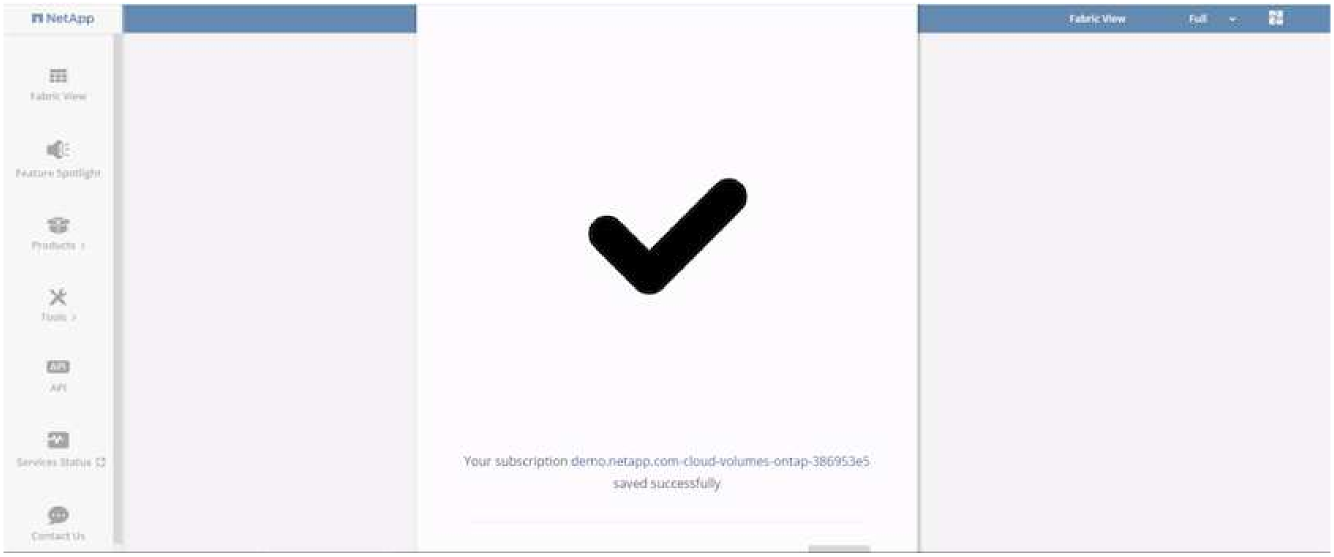
NetApp Cloud Central Account

We've assigned your subscription to all of your NetApp Cloud Central accounts. You can choose to unassign specific accounts.

☑ rt1600680

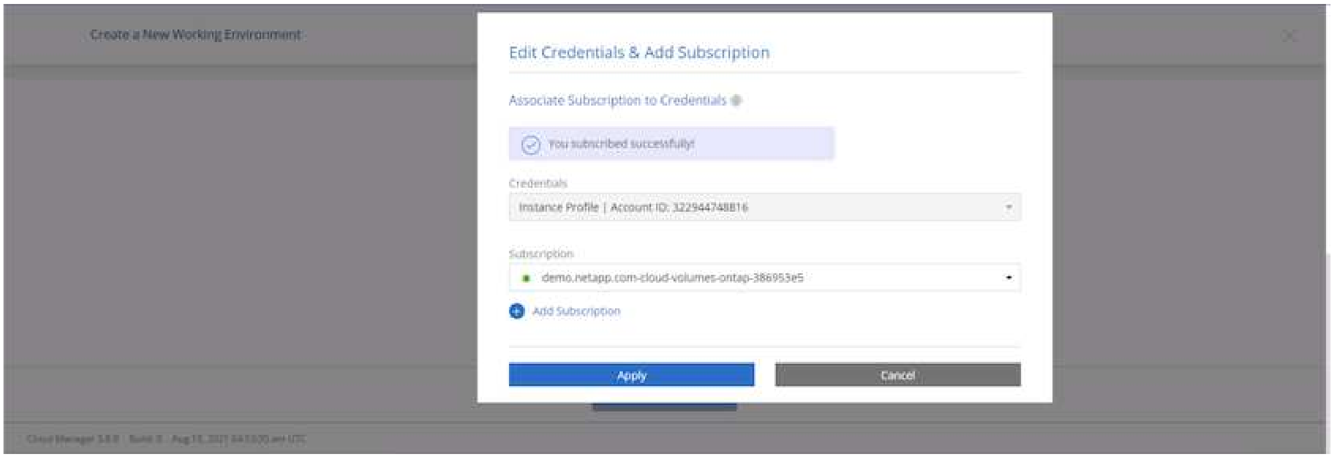
Save

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



Your subscription demo.netapp.com-cloud-volumes-ontap-386953e5 saved successfully

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



Edit Credentials & Add Subscription

Associate Subscription to Credentials

You subscribed successfully!

Credentials

Instance Profile | Account ID: 322944748816

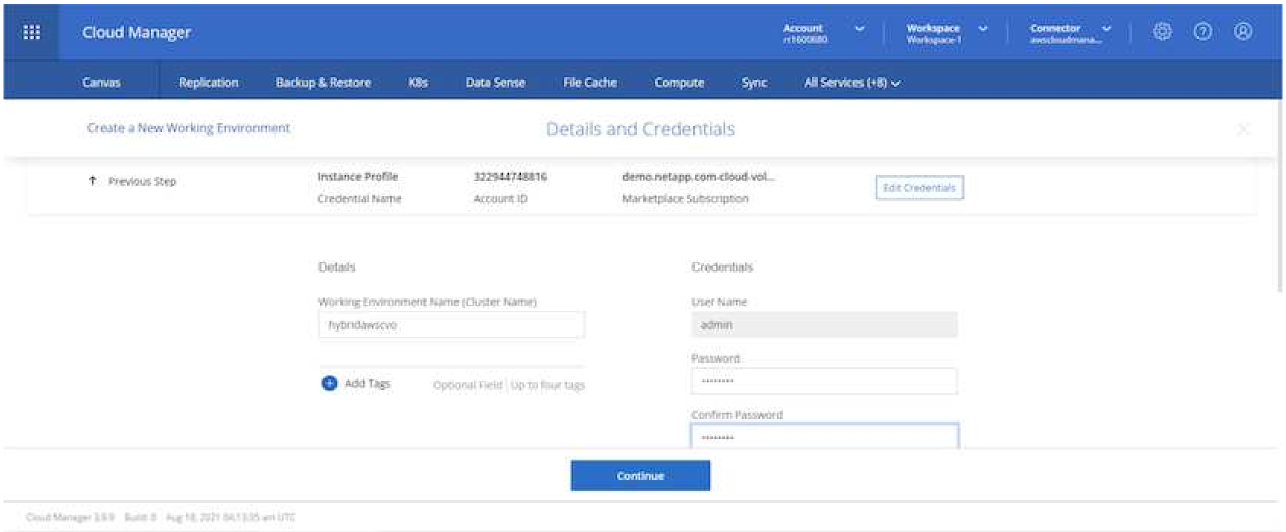
Subscription

demo.netapp.com-cloud-volumes-ontap-386953e5

10. Enter the working environment details such as:
    a. Cluster name

b. Cluster password

c. AWS tags (Optional)



Details and Credentials

Instance Profile — Credential Name

322944748816 — Account ID

demo.netapp.com-cloud-vol... — Marketplace Subscription

Details

Working Environment Name (Cluster Name): hybridawscvo

Add Tags — Optional Field | Up to four tags

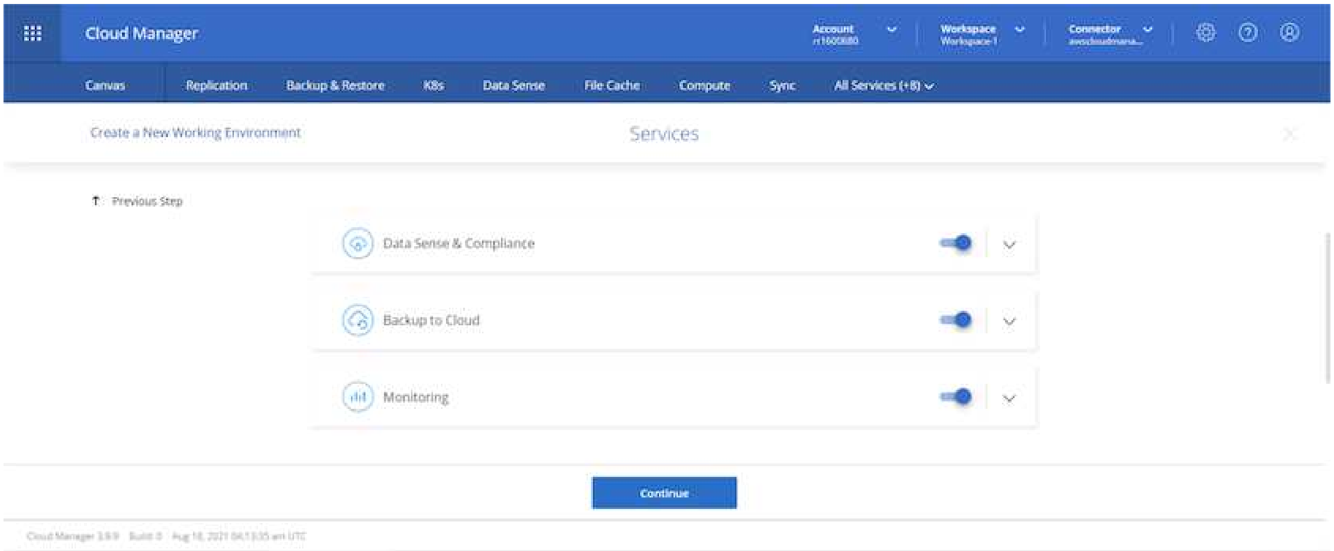
Credentials

User Name: admin

Password: ••••••••

Confirm Password: ••••••••

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



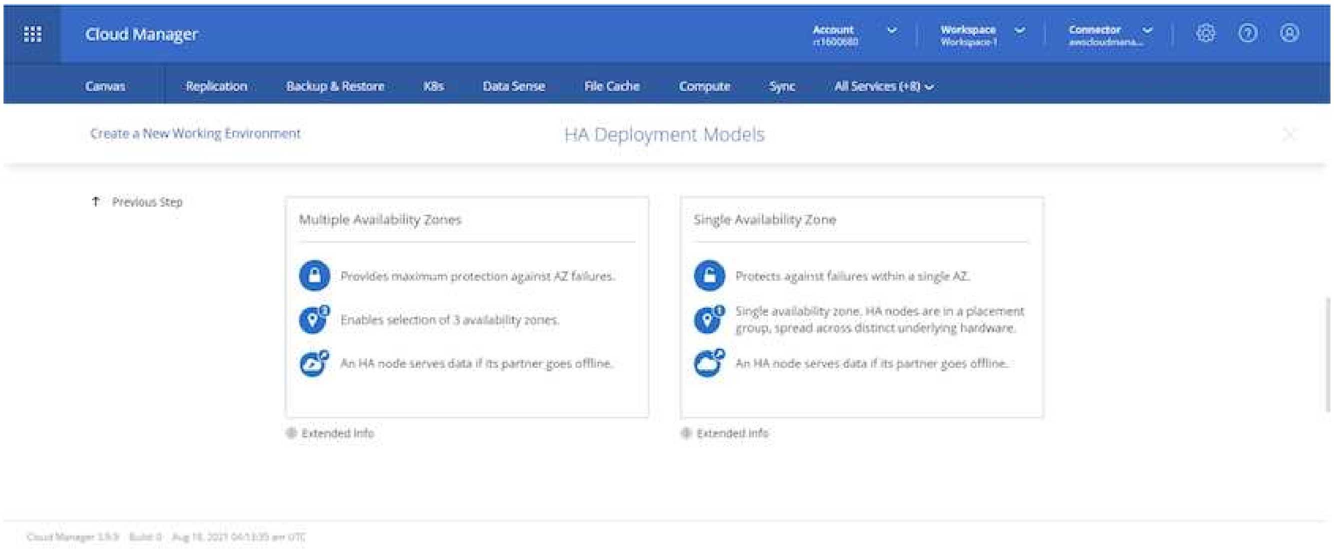
Services

Data Sense & Compliance ●

Backup to Cloud ●

Monitoring ●

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



HA Deployment Models

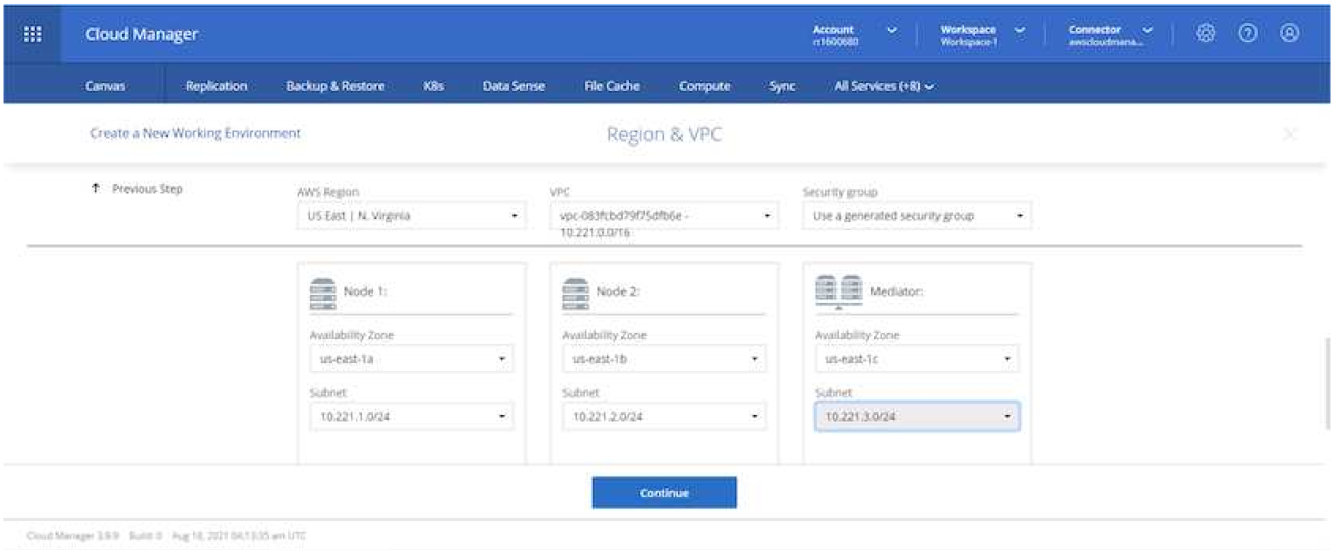
Multiple Availability Zones

- 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.

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.



Region & VPC

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

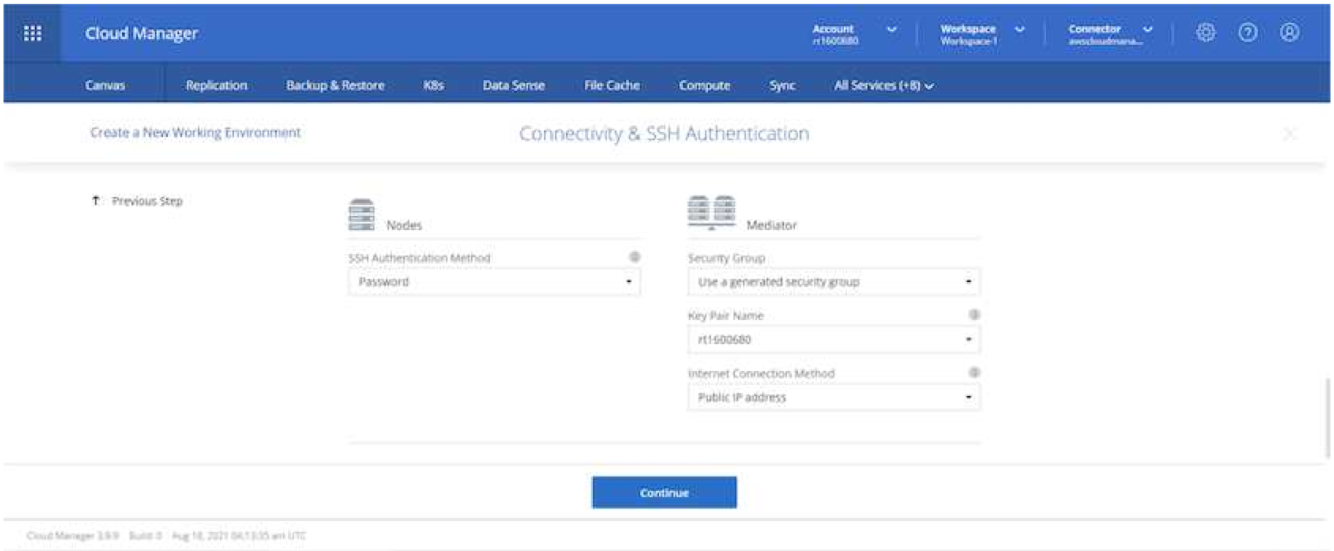
Subnet: 10.221.2.0/24

Mediator:

Availability Zone: us-east-1c

Subnet: 10.221.3.0/24

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



Connectivity & SSH Authentication

Nodes

SSH Authentication Method: Password

Mediator

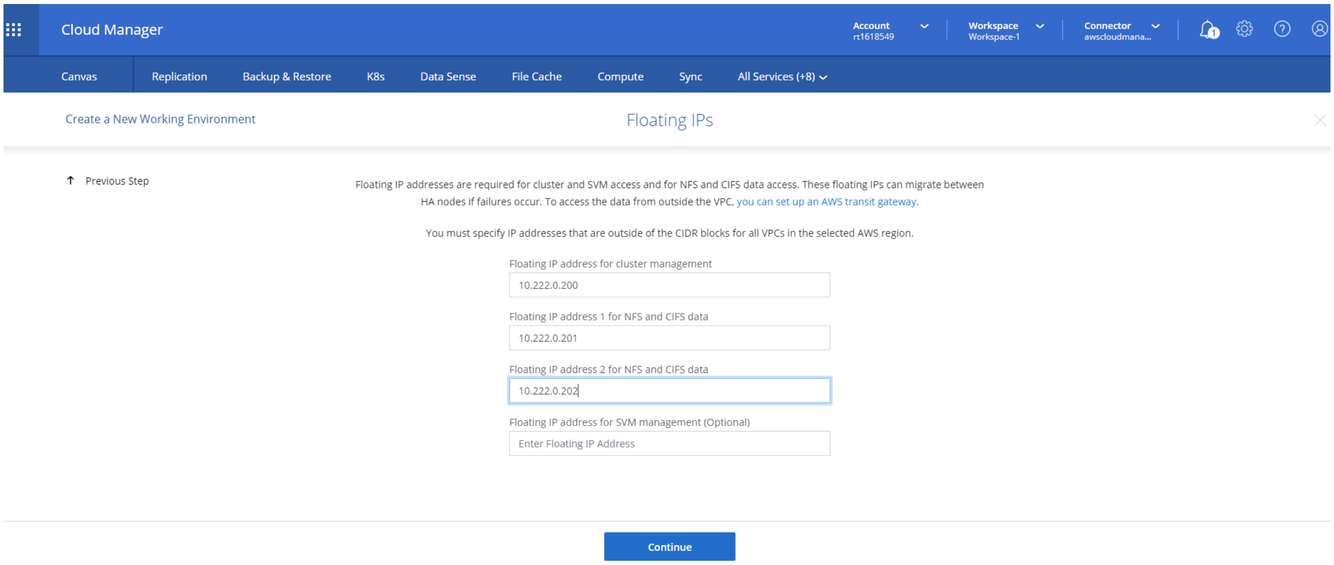
Security Group: Use a generated security group

Key Pair Name: rt1600680

Internet Connection Method: Public IP address

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 Documenation.



Floating IPs

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.

You must specify IP addresses that are outside of the CIDR blocks for all VPCs in the selected AWS region.

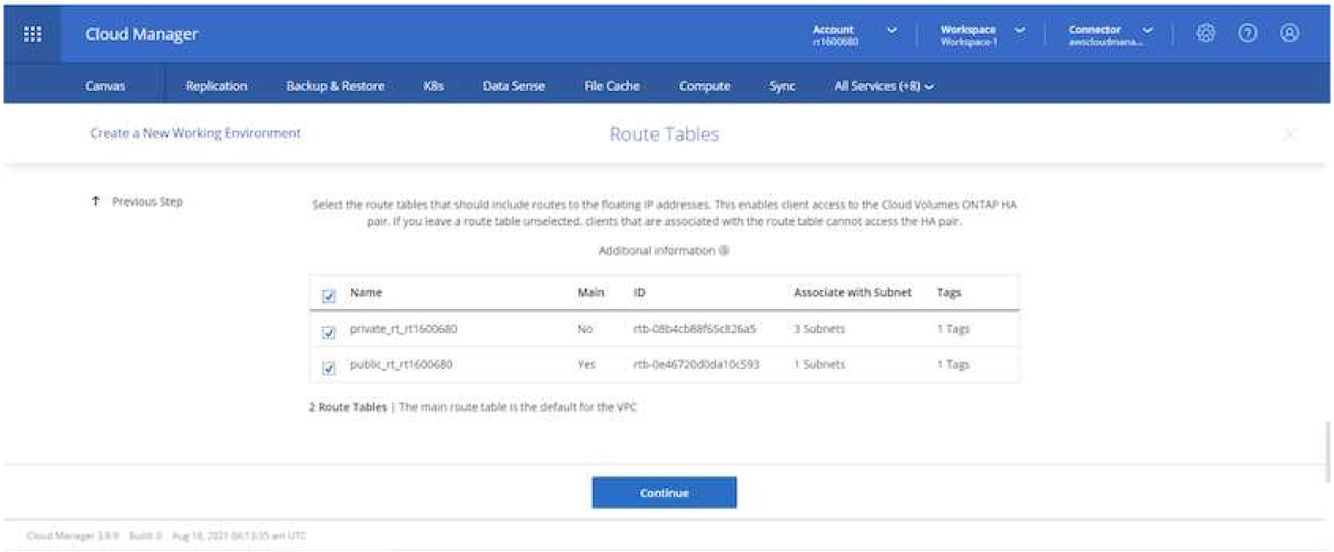
Floating IP address for cluster management: 10.222.0.200

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

Floating IP address for SVM management (Optional): Enter Floating IP Address

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.



Route Tables

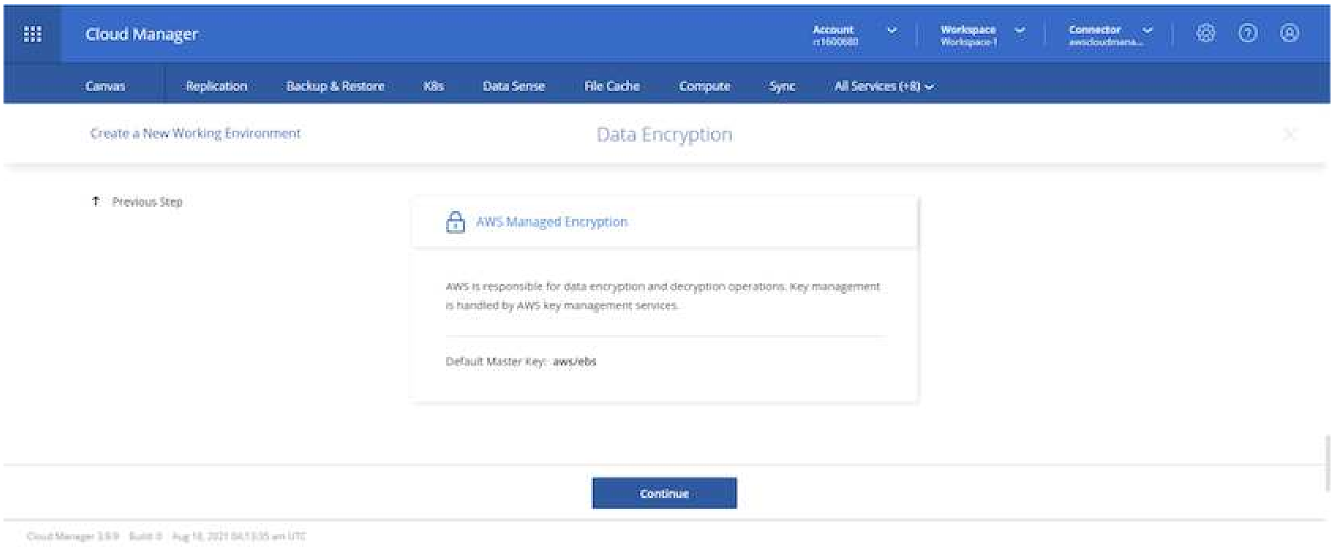
Select the route tables that should include routes to the floating IP addresses. This enables client access to the Cloud Volumes ONTAP HA pair. If you leave a route table unselected, clients that are associated with the route table cannot access the HA pair.

Additional information

☑	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

2 Route Tables | The main route table is the default for the VPC

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



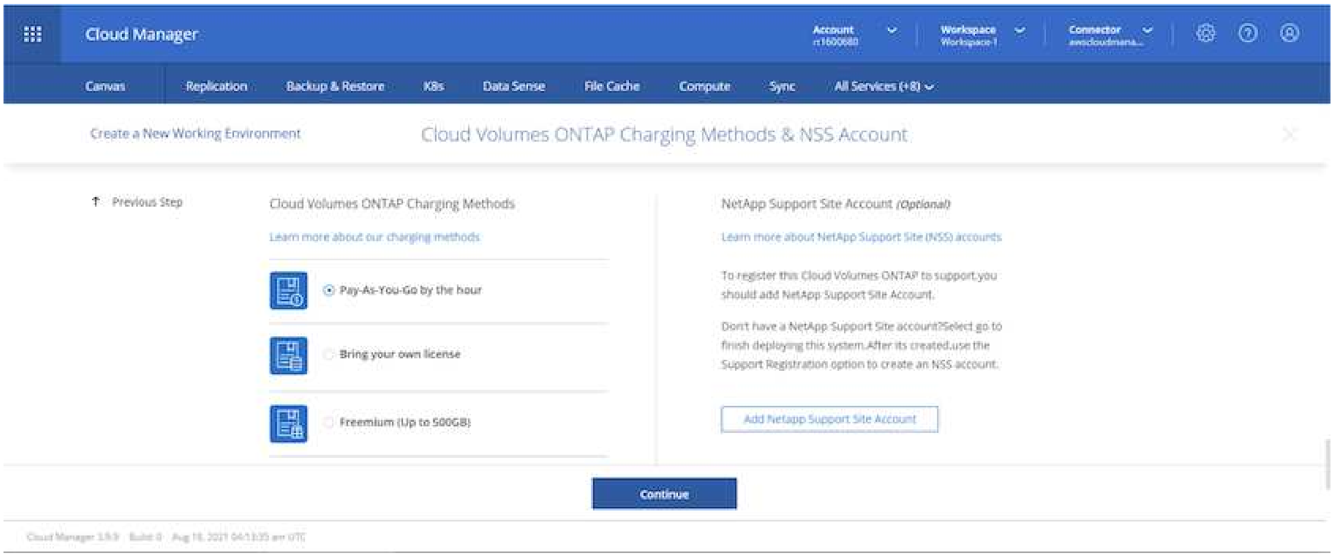
Data Encryption

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

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 awscloudmana...
Canvas
Replication
Backup & Restore
K8s
Data Sense
File Cache
Compute
Sync
All Services (+8)
Create a New Working Environment
Previous Step
Learn more about our charging methods
Learn more about NetApp Support Site (NSS) accounts
Add Netapp Support Site Account
Continue
Cloud Manager 3.9.9 Build 0 Aug 18, 2021 04:13:35 am UTC

Cloud Volumes ONTAP Charging Methods & NSS Account

Cloud Volumes ONTAP Charging Methods

● Pay-As-You-Go by the hour

○ Bring your own license

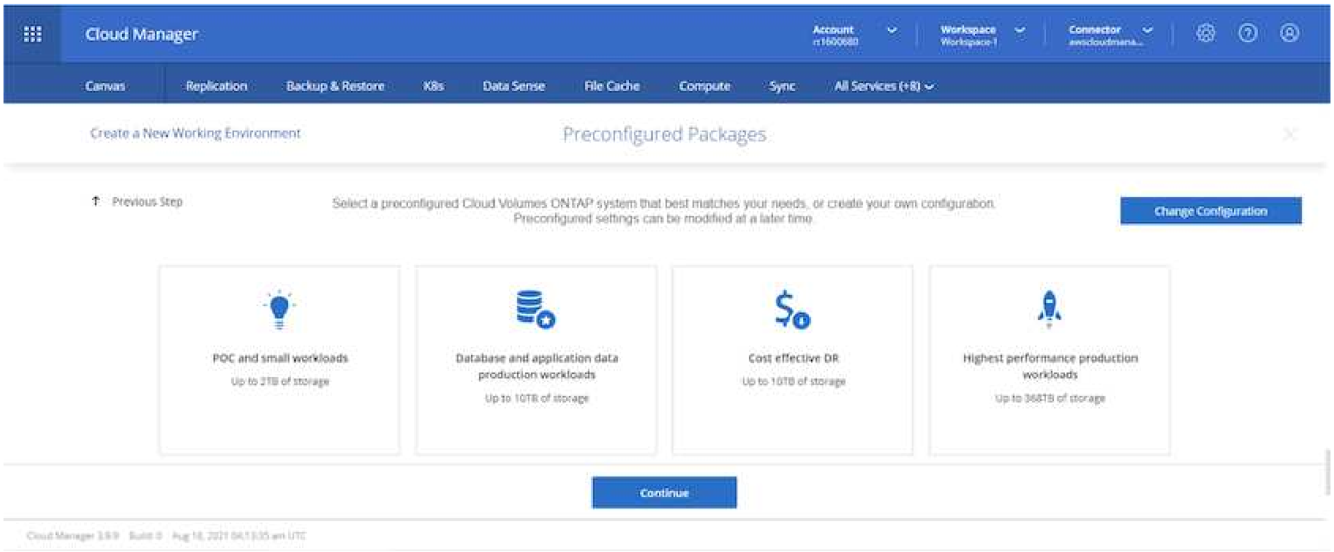
○ Freemium (Up to 500GB)

NetApp Support Site Account *(Optional)*

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 its created,use the Support Registration option to create an NSS account.

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



Preconfigured Packages

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.

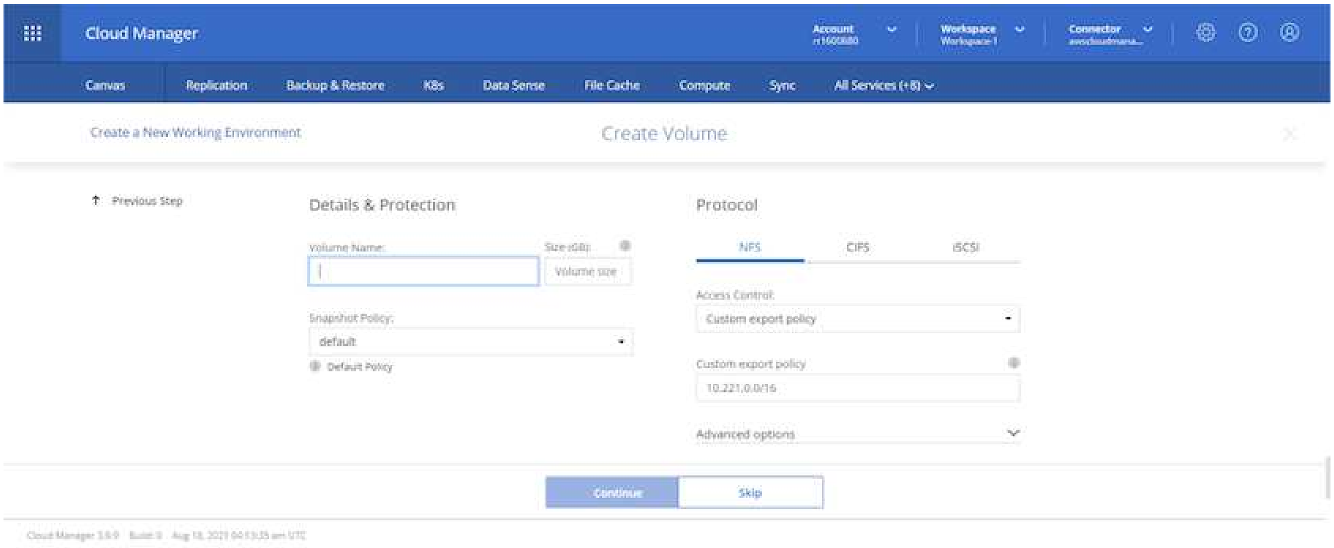
POC and small workloads
Up to 2TB of storage

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

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



Create Volume

Details & Protection

Volume Name:

Size (GB): Volume size

Snapshot Policy: default

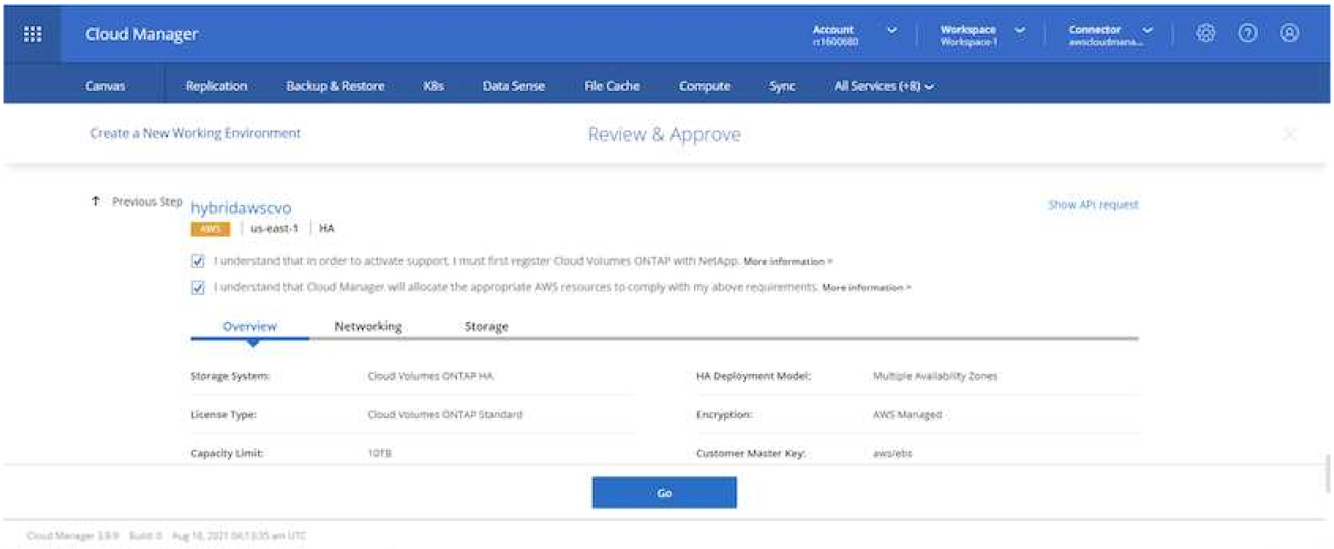
Default Policy

Protocol

Access Control: Custom export policy

Custom export policy: 10.221.0.0/16

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.



Review & Approve

hybridawscvo

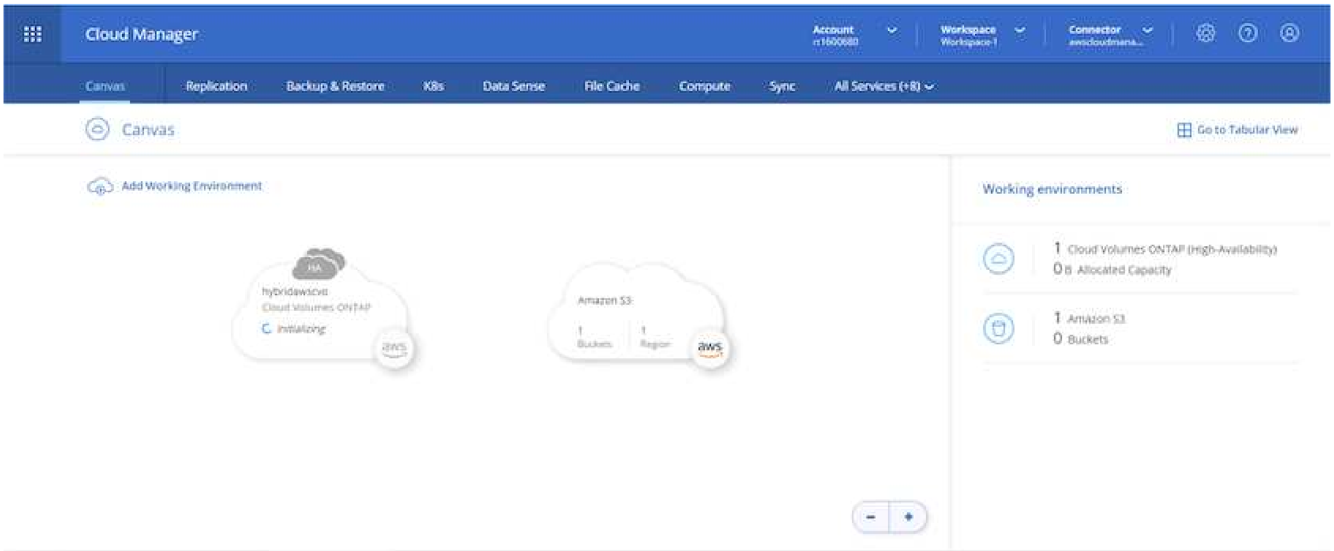
AWS | us-east-1 | HA

☑ I understand that in order to activate support, I must first register Cloud Volumes ONTAP with NetApp. More information »

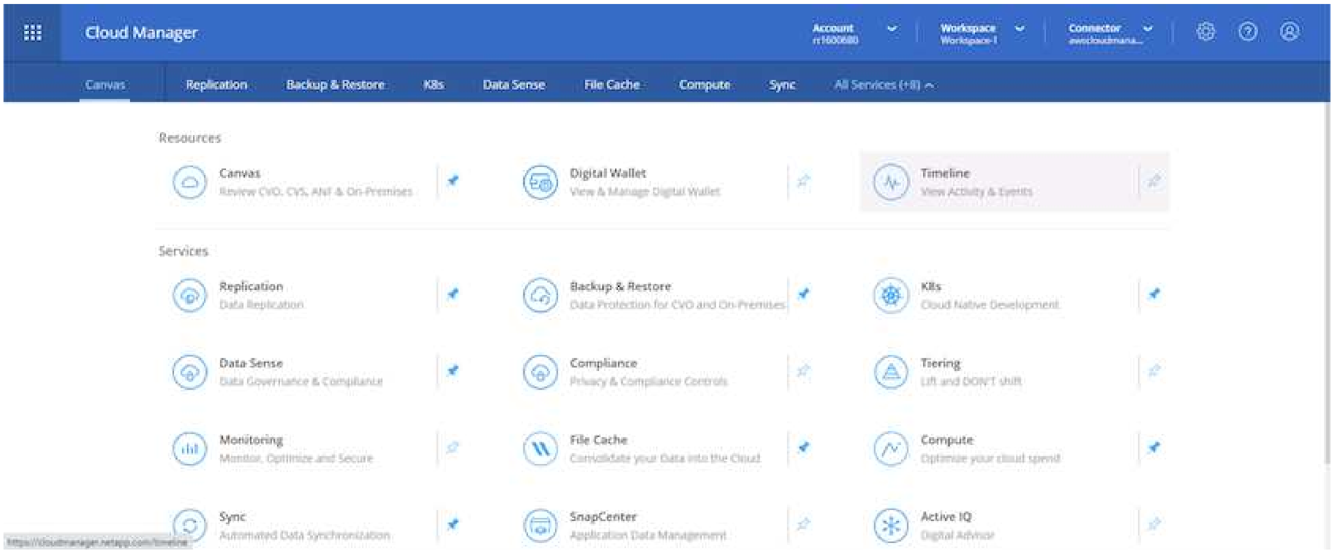
☑ I understand that Cloud Manager will allocate the appropriate AWS resources to comply with my above requirements. More information »

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

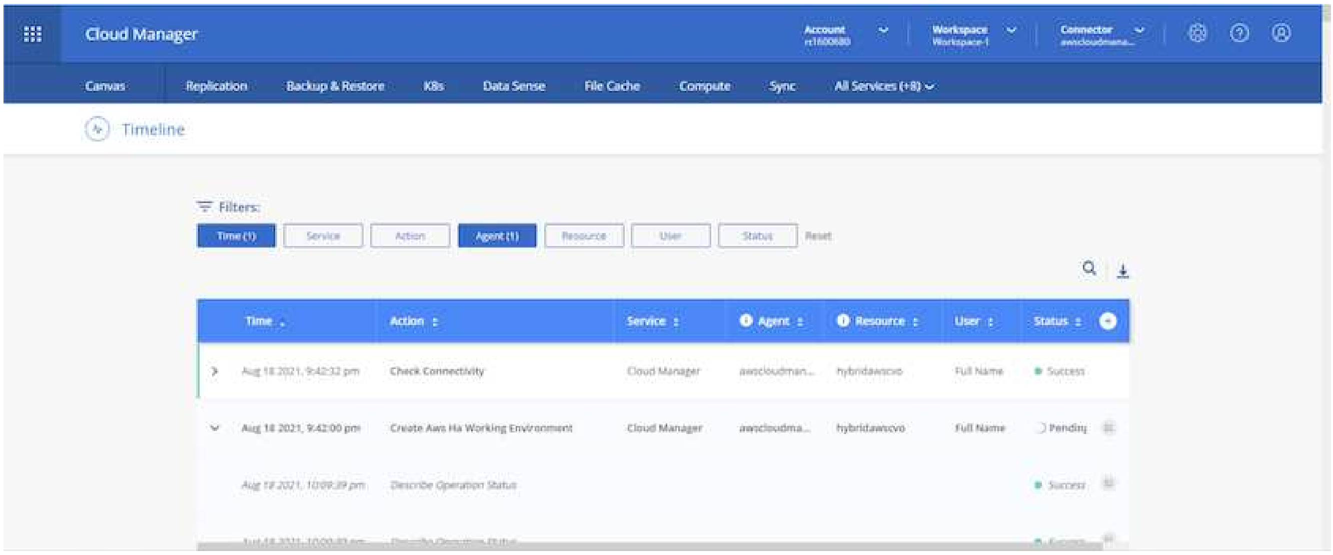
8. Cloud Volumes ONTAP now starts its deployment process. Cloud Manager uses AWS APIs and cloud formation stacks to deploy Cloud Volumes ONTAP. It then configures the system to your specifications, giving you a ready-to-go system that can be instantly utilized. The timing for this process varies depending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



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

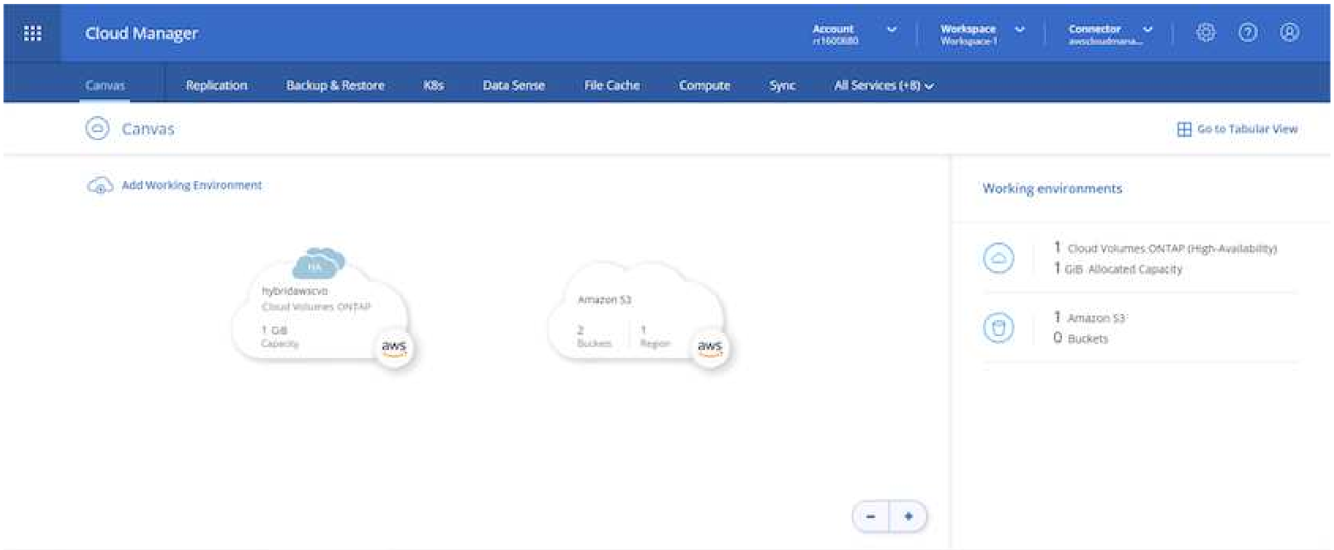


10. The Timeline acts as an audit of all actions performed in Cloud Manager. You can view all of the API calls that are made by Cloud Manager during setup to both AWS as well as the ONTAP cluster. This can also be effectively used to troubleshoot any issues that you face.



	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

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.

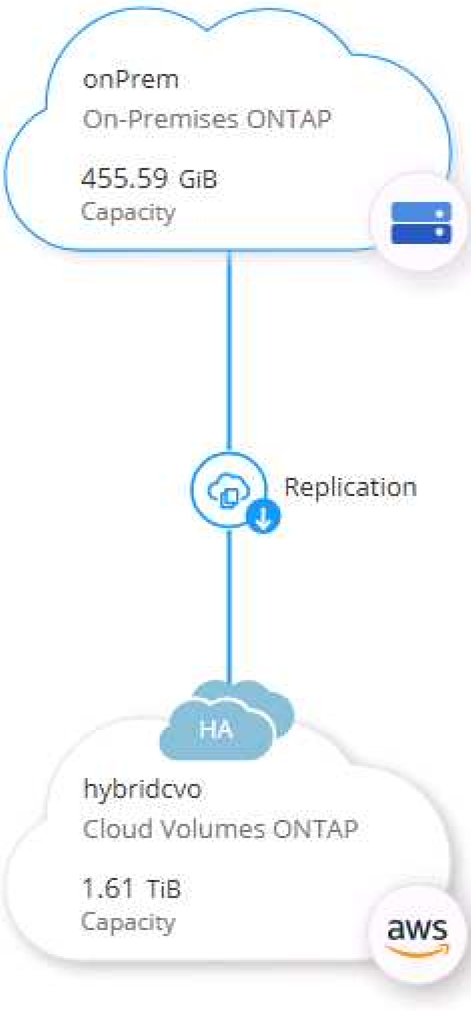


Configure SnapMirror from on-premises to cloud

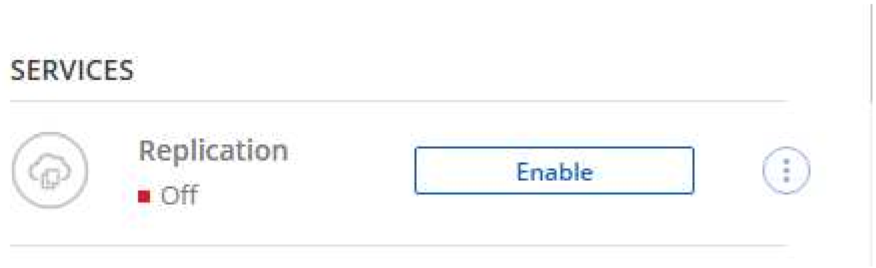
Now that you have a source ONTAP system and a destination ONTAP system deployed, you can replicate volumes containing database data into the cloud.

For a guide on compatible ONTAP versions for SnapMirror, see the SnapMirror Compatibility Matrix.

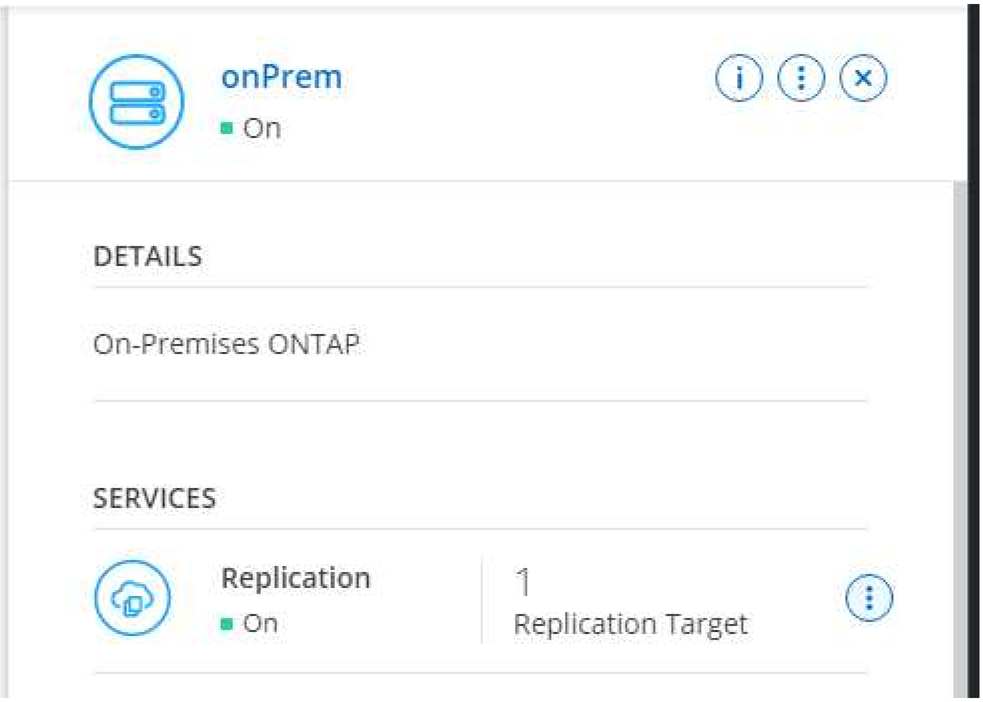
1. Click the source ONTAP system (on-premises) and either drag and drop it to the destination, select Replication > Enable, or select Replication > Menu > Replicate.



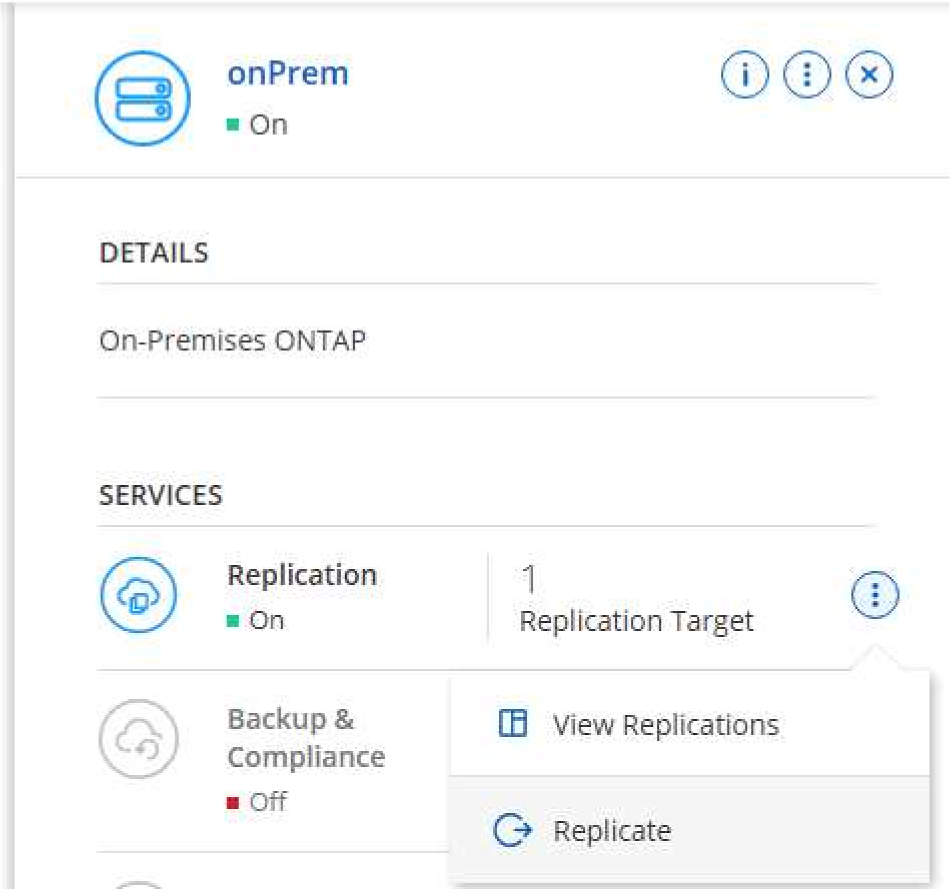
Select Enable.



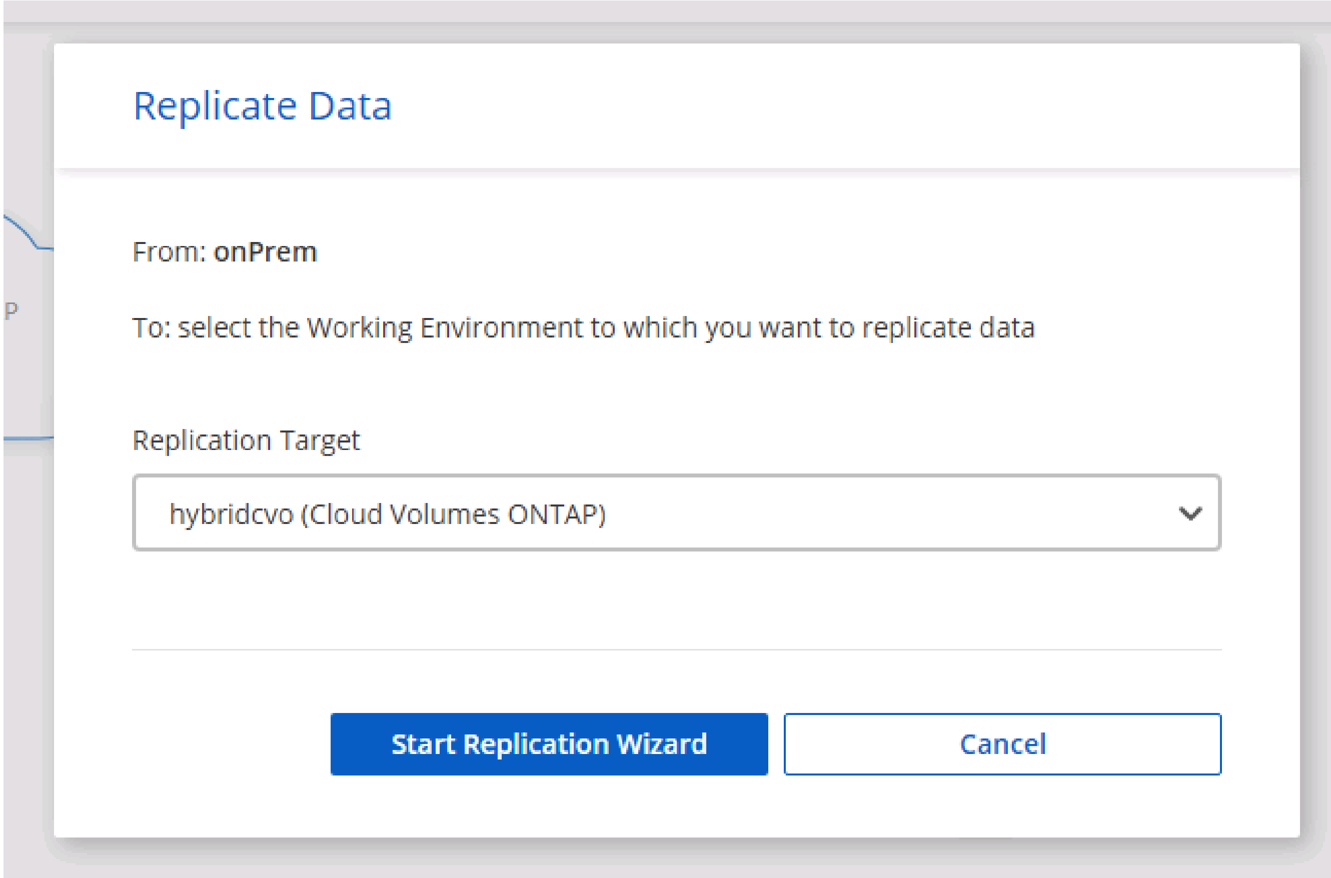
Or Options.



Replicate.



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



Replicate Data

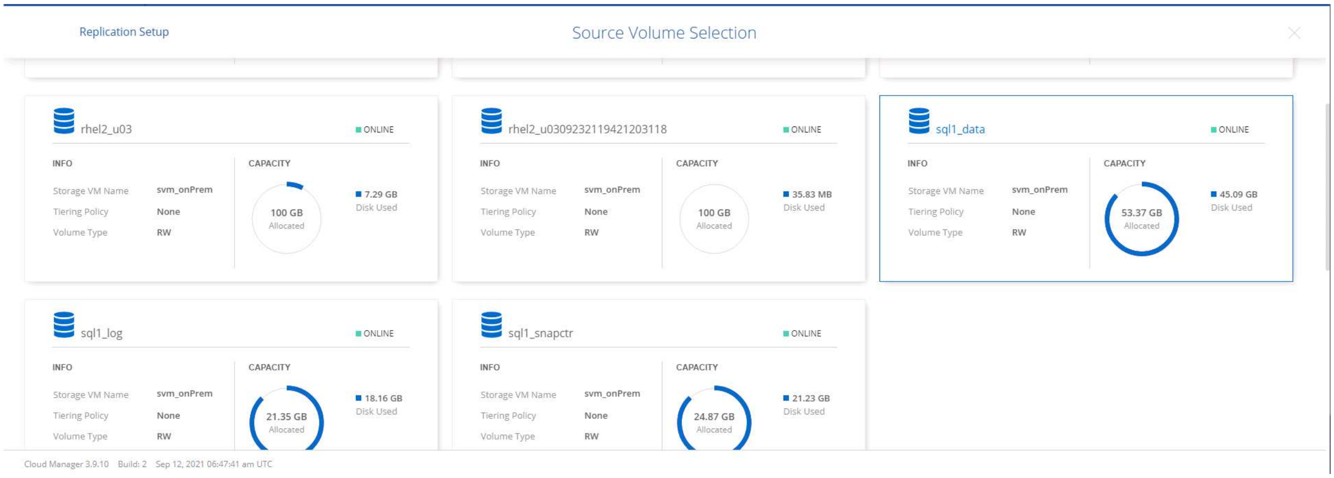
From: onPrem

To: select the Working Environment to which you want to replicate data

Replication Target

hybridcvo (Cloud Volumes ONTAP)

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



rhel2_u03 — ONLINE
INFO: Storage VM Name svm_onPrem; Tiering Policy None; Volume Type RW
CAPACITY: 100 GB Allocated; 7.29 GB Disk Used

rhel2_u0309232119421203118 — ONLINE
INFO: Storage VM Name svm_onPrem; Tiering Policy None; Volume Type RW
CAPACITY: 100 GB Allocated; 35.83 MB Disk Used

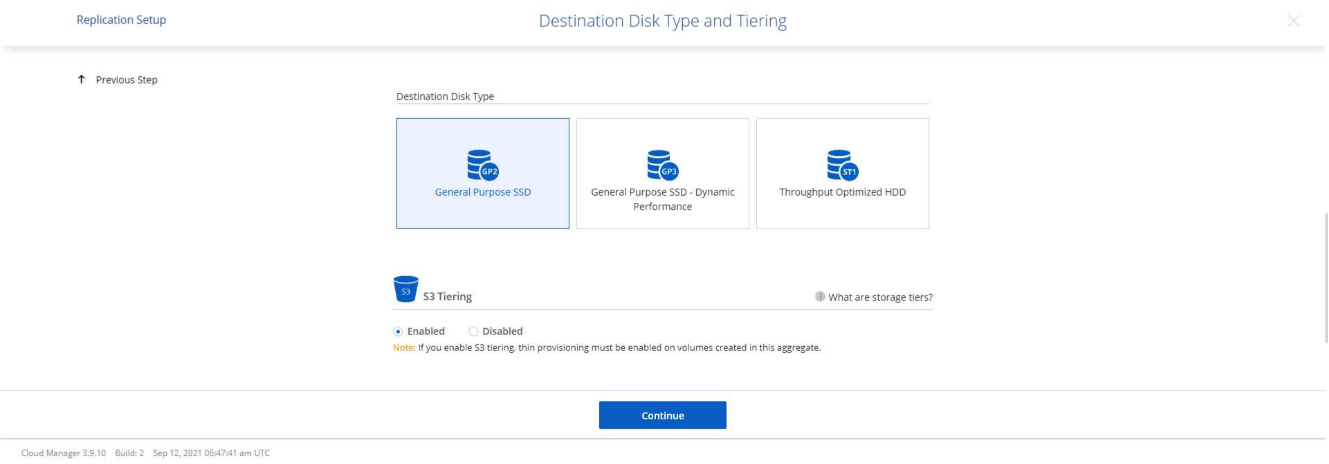
sql1_data — ONLINE
INFO: Storage VM Name svm_onPrem; Tiering Policy None; Volume Type RW
CAPACITY: 53.37 GB Allocated; 45.09 GB Disk Used

sql1_log — ONLINE
INFO: Storage VM Name svm_onPrem; Tiering Policy None; Volume Type RW
CAPACITY: 21.35 GB Allocated; 18.16 GB Disk Used

sql1_snapctr — ONLINE
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.



Replication Setup

Destination Disk Type and Tiering

Destination Disk Type

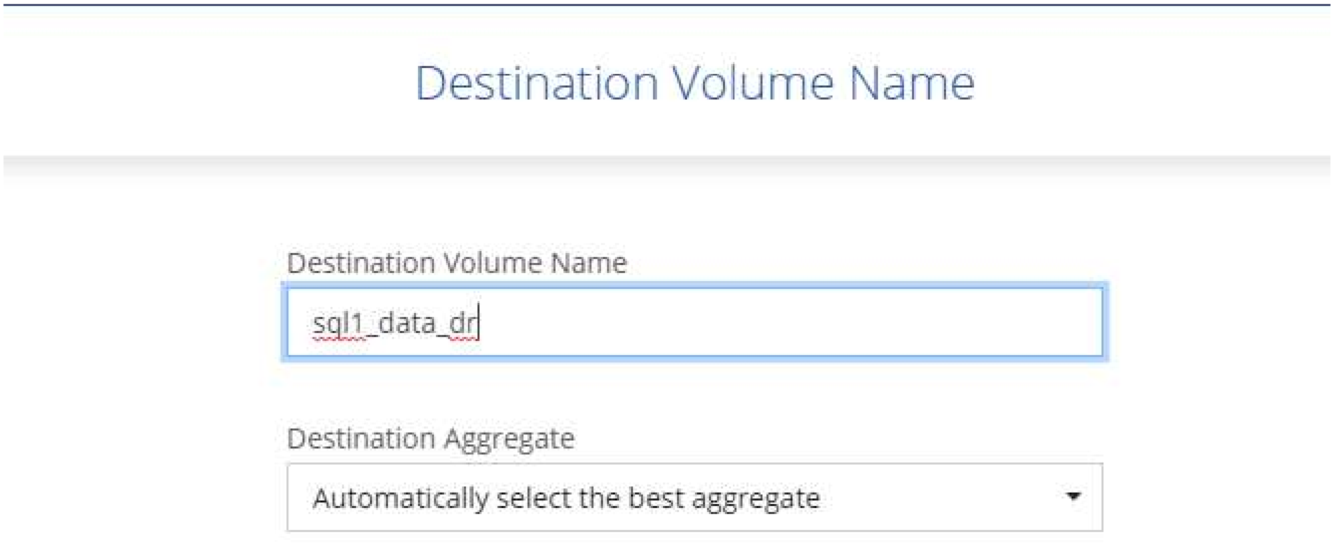
S3 Tiering

● Enabled ○ Disabled

Note: If you enable S3 tiering, thin provisioning must be enabled on volumes created in this aggregate.

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`.

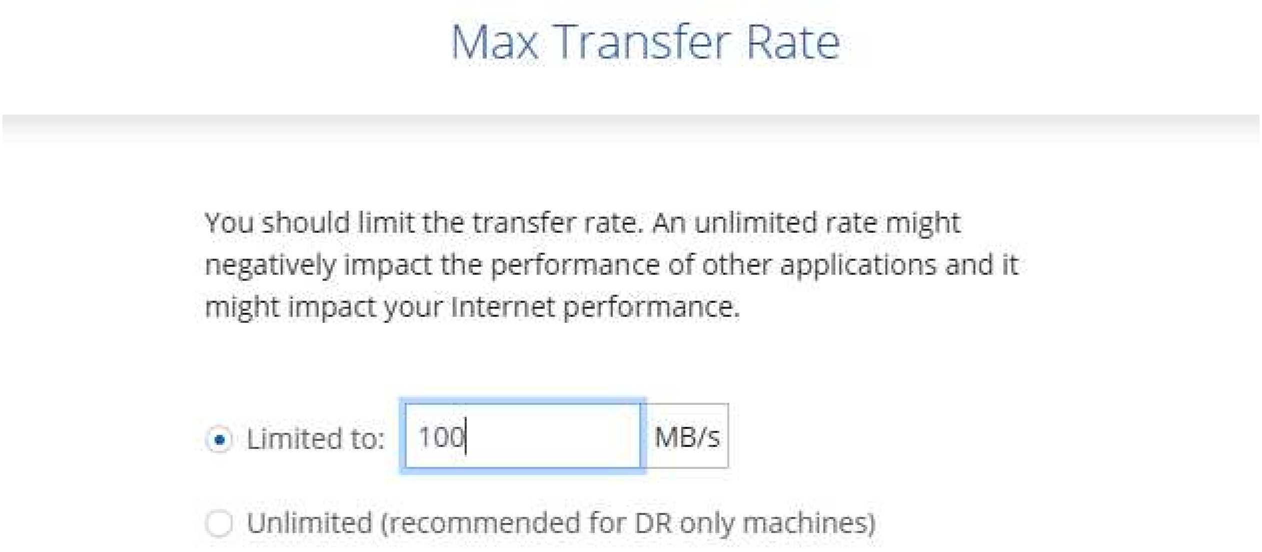


Destination Volume Name

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.



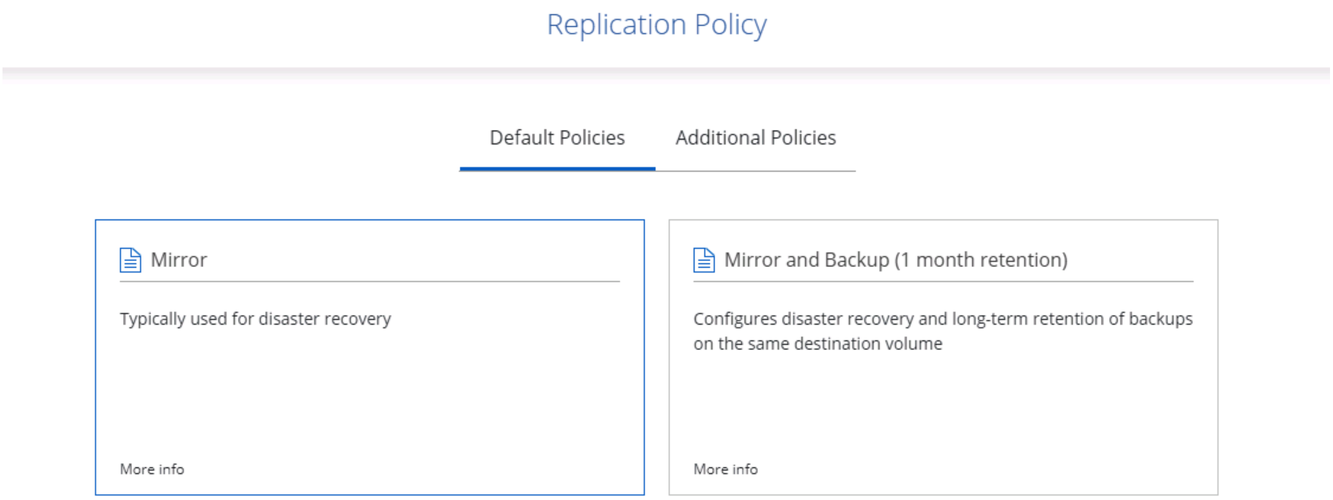
Max Transfer Rate

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

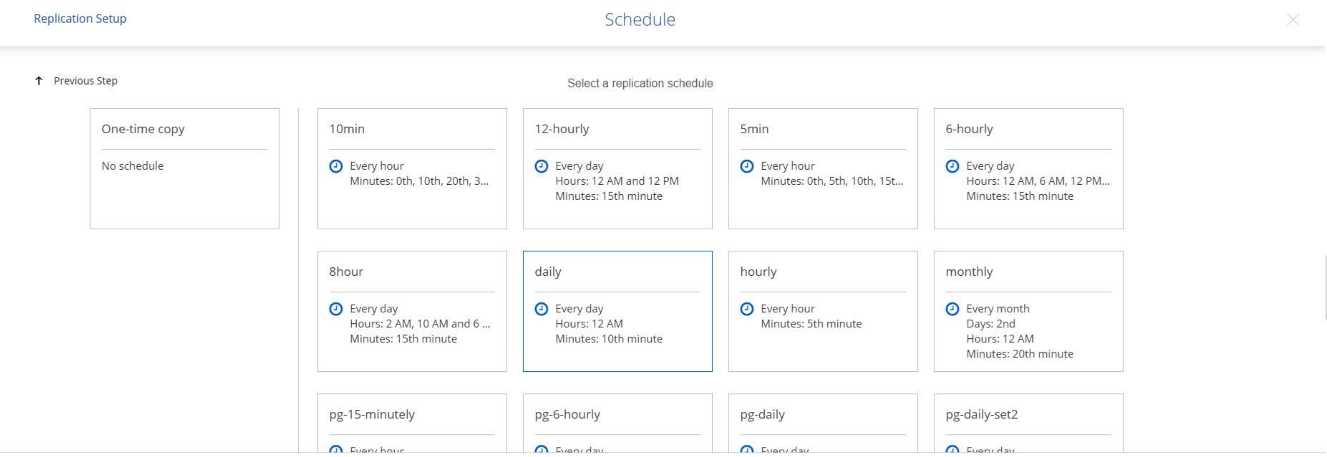
More info

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.



Replication Setup

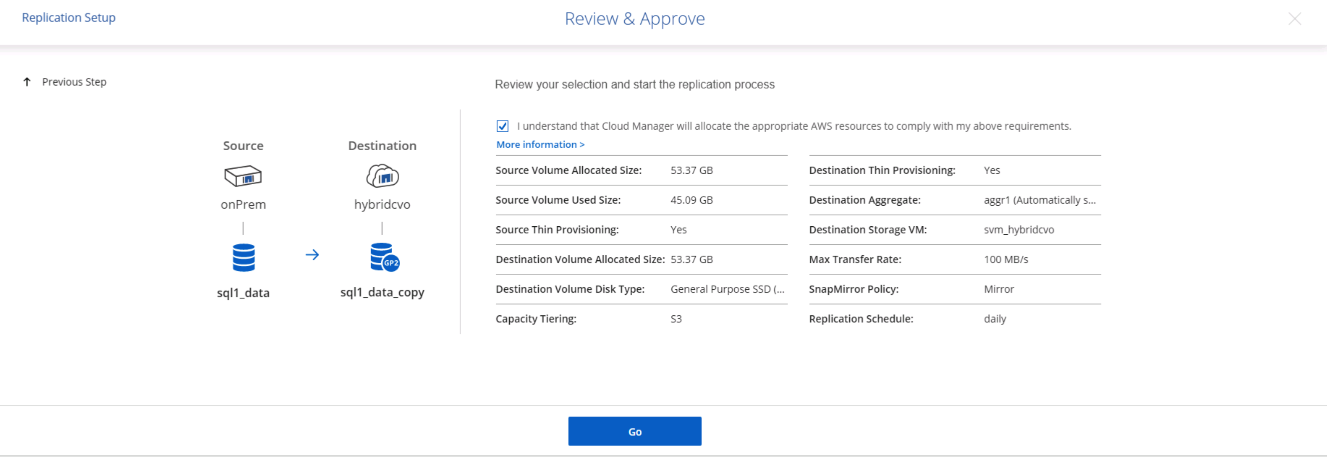
Schedule

↑ Previous Step

Select a replication schedule

One-time copy No schedule	10min Every hour Minutes: 0th, 10th, 20th, 3...	12-hourly Every day Hours: 12 AM and 12 PM Minutes: 15th minute	5min Every hour Minutes: 0th, 5th, 10th, 15t...	6-hourly Every day Hours: 12 AM, 6 AM, 12 PM... Minutes: 15th minute
	8hour Every day Hours: 2 AM, 10 AM and 6 ... Minutes: 15th minute	daily Every day Hours: 12 AM Minutes: 10th minute	hourly Every hour Minutes: 5th minute	monthly Every month Days: 2nd Hours: 12 AM Minutes: 20th minute
	pg-15-minutely Every hour	pg-6-hourly Every day	pg-daily Every day	pg-daily-set2 Every day

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.



Replication Setup

Review & Approve

↑ Previous Step

Review your selection and start the replication process

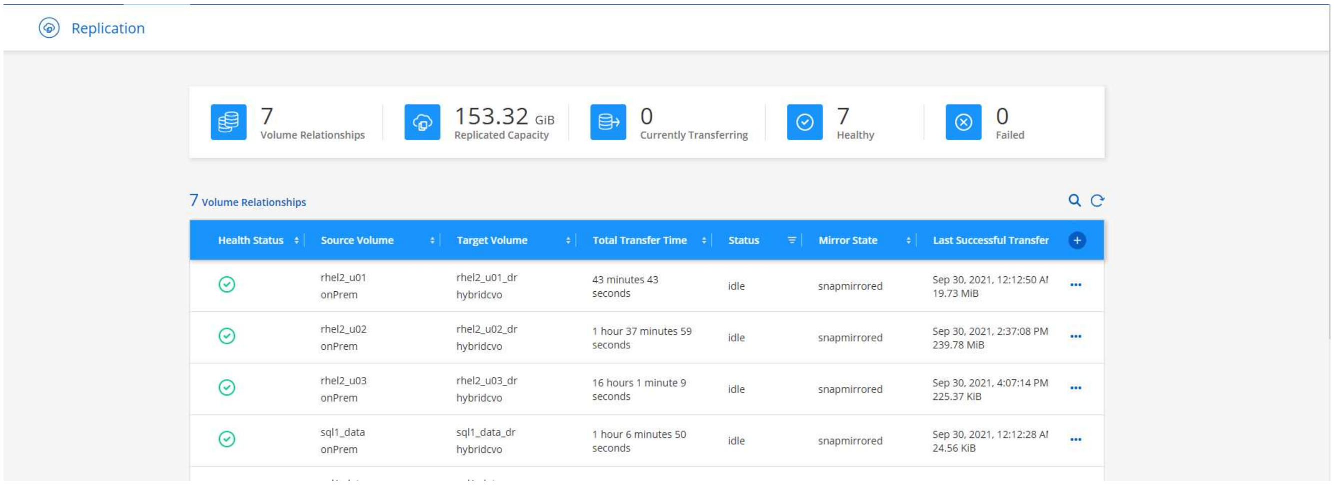
☑ I understand that Cloud Manager will allocate the appropriate AWS resources to comply with my above requirements.
More information >

Source Volume Allocated Size:	53.37 GB	Destination Thin Provisioning:	Yes
Source Volume Used Size:	45.09 GB	Destination Aggregate:	aggr1 (Automatically s...
Source Thin Provisioning:	Yes	Destination Storage VM:	svm_hybridcvo
Destination Volume Allocated Size:	53.37 GB	Max Transfer Rate:	100 MB/s
Destination Volume Disk Type:	General Purpose SSD (...	SnapMirror Policy:	Mirror
Capacity Tiering:	S3	Replication Schedule:	daily

Go

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.



Replication

7 Volume Relationships | 153.32 GiB Replicated Capacity | 0 Currently Transferring | 7 Healthy | 0 Failed

7 Volume Relationships

Health Status	Source Volume	Target Volume	Total Transfer Time	Status	Mirror State	Last Successful Transfer
✓	rhel2_u01 onPrem	rhel2_u01_dr hybridcvo	43 minutes 43 seconds	idle	snapmirrored	Sep 30, 2021, 12:12:50 AI 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 AI 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.

Copyright information

Trademark information