



SnapCenter for databases

NetApp Solutions

NetApp
April 18, 2023

This PDF was generated from https://docs.netapp.com/us-en/netapp-solutions/databases/snapctr_svcs_ora.html on April 18, 2023. Always check docs.netapp.com for the latest.

Table of Contents

SnapCenter for databases	1
TR-4964: Oracle Database backup, restore and clone with SnapCenter Services	1
Hybrid Cloud Database Solutions with SnapCenter	29

SnapCenter for databases

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

Allen Cao, Niyaz Mohamed, NetApp

Purpose

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

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

This solution addresses the following use cases:

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

Audience

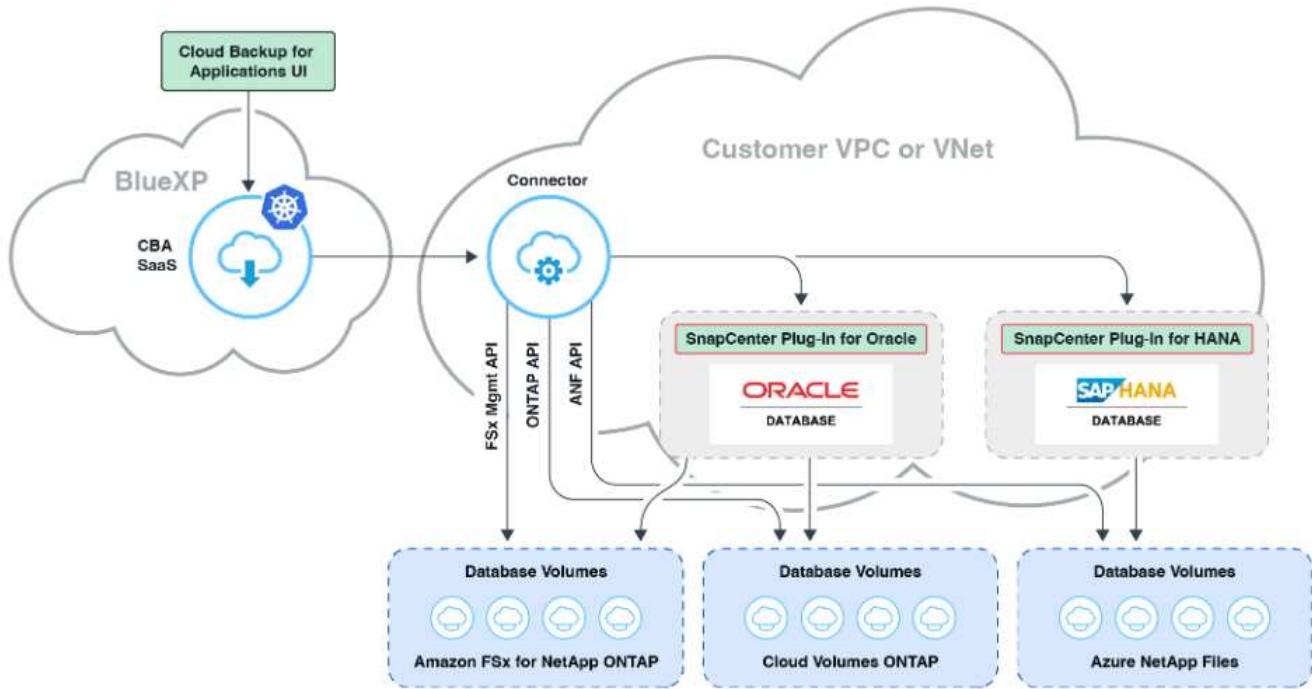
This solution is intended for the following audiences:

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

Solution test and validation environment

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

Architecture



This image provides a detailed picture of Cloud Backup for Application within the BlueXP console, including the UI, the connector, and the resources it manages.

Hardware and software components

Hardware		
FSx ONTAP storage	Current version offered by AWS	One FSx HA cluster in the same VPC and availability zone
EC2 instance for compute	t2.xlarge/4vCPU/16G	Two EC2 T2 xlarge EC2 instances, one as primary DB server and the other as clone DB server
Software		
RedHat Linux	RHEL-8.6.0_HVM-20220503-x86_64-2-Hourly2-GP2	Deployed RedHat subscription for testing
Oracle Grid Infrastructure	Version 19.18	Applied RU patch p34762026_190000_Linux-x86-64.zip
Oracle Database	Version 19.18	Applied RU patch p34765931_190000_Linux-x86-64.zip
Oracle OPatch	Version 12.2.0.1.36	Latest patch p6880880_190000_Linux-x86-64.zip
SnapCenter Service	Version	v2.3.1.2324

Key factors for deployment consideration

- **Connector to be deployed in the same VPC as database and FSx.** When possible, the connector should be deployed in the same AWS VPC, which enables connectivity to the FSx storage and the EC2 compute instance.

- **An AWS IAM policy created for SnapCenter connector.** The policy in JSON format is available in the detailed SnapCenter service documentation. When you launch connector deployment with the BlueXP console, you are prompted to set up the prerequisites. The policy should be assigned to the AWS user account that owns the connector.
- **The AWS account access key and the SSH key pair created in the AWS account.** The SSH key pair is assigned to the ec2-user for logging into the connector host and then deploying a database plug-in to the EC2 DB server host. The access key grants permission for provisioning the required connector.
- **A credential added to the BlueXP console setting.** To add Amazon FSx for ONTAP to the BlueXP working environment, a credential that grants permissions to access Amazon FSx for ONTAP from the BlueXP console is set up in the BlueXP console setting.
- **SnapCenter plug-in deployed to the EC2 database instance host.** SnapCenter services make API calls that are executed by the SnapCenter plug-in on the EC2 database instance host. You must deploy it before setting up the services.

Solution deployment

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

To get started, complete the following steps:

- Read the general instructions [Protect your cloud native applications data](#) and the sections related to Oracle and Amazon FSx for ONTAP.
- Watch the following video walkthrough.
 - ▶ <https://docs.netapp.com/us-en/netapp-solutions/media/oracle-aws-fsx-part4c-bkup-restore->

Prerequisites for SnapCenter service deployment

Deployment requires the following prerequisites.

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

Onboarding to BlueXP preparation

1. Use the link [NetApp BlueXP](#) to sign up for BlueXP console access.
2. To set up BlueXP to manage AWS cloud resources such as Amazon FSx for ONTAP, you should already have an AWS account set up. You can then log into your AWS account to create an IAM policy for granting SnapCenter service access to an AWS account to use for connector deployment.

The screenshot shows the AWS Identity and Access Management (IAM) console. The left sidebar is collapsed, showing the main navigation menu. The main area displays the 'Summary' tab for a policy named 'snapcenter'. The policy ARN is listed as 'arn:aws:iam::541696183547:policy/snapcenter'. The description is 'Policy to grant snapcenter service permission to create connector in AWS.' Below this, there are tabs for 'Permissions', 'Policy usage', 'Tags', 'Policy versions', and 'Access Advisor'. The 'Permissions' tab is selected, showing the JSON policy document:

```

1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Effect": "Allow",  
6       "Action": [  
7         "iam:CreateRole",  
8         "iam:DeleteRole",  
9         "iam:PutRolePolicy",  
10        "iam:CreateInstanceProfile",  
11        "iam:DeleteRolePolicy",  
12        "iam:AddRoleToInstanceProfile",  
13        "iam:RemoveRoleFromInstanceProfile",  
14        "iam:DeleteInstanceProfile",  
15        "iam:PassRole",  
16        "iam>ListRoles",  
17        "ec2:DescribeInstanceStatus",  
18        "ec2:RunInstances",  
19        "ec2:ModifyInstanceAttribute",  
20        "ec2>CreateSecurityGroup",  
21        "ec2>DeleteSecurityGroup",  
22        "ec2:DescribeSecurityGroups",  
23        "ec2:RevokeSecurityGroupEgress",  
24        "ec2:AuthorizeSecurityGroupEgress",  
25        "ec2:AuthorizeSecurityGroupIngress",  
26        "ec2:RevokeSecurityGroupIngress",  
27        "ec2>CreateNetworkInterface",  
28        "ec2:DescribeNetworkInterface"  
29      ]  
30    }  
31  ]  
32}  
33

```

The policy should be configured with a JSON string that is available when connector provisioning is launched and you are prompted as a reminder that an IAM policy has been created and granted to an AWS account that is used for connector deployment.

3. You also need the AWS VPC, a key and secrets for your AWS account, an SSH key for EC2 access, a security group, and so on ready for connector provisioning.

Deploy a connector for SnapCenter services

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

Manage Account: Automation-team

Overview Members Workspaces BlueXP Connector X

Manage the BlueXP connector Workspaces

+ Add New Workspace

Workspace Name	Action
Database	Edit Delete
Database-2	Edit Delete
sufians-k8	Edit Delete
Workspace-1	Edit Delete

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

NetApp Cloud Manager

Account Automation-team Workspace new-workspace Connector N/A

Backup & Restore Volumes Restore Applications Virtual Machines Kubernetes Job Monitoring

Backup & Restore
Fully integrated data protection for ONTAP anywhere

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

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

Add a Connector

Performance Metrics Status

Protection Environments	Volumes	Total Capacity
12	2,011	112.25 TB

2,011 datasets

Source	Destination	Last Sync	Protection	Status
Source, Volume_1	Dest, Volume_1	May 22, 2020, 08:00 AM	0.00 TB Imported	Green
Source, Volume_2	Dest, Volume_2	May 22, 2020, 08:00 AM	200TB Imported	Yellow
Source, Volume_3	Dest, Volume_3	May 22, 2020, 08:00 AM	1.71 TB Imported	Green
Source, Volume_4	Dest, Volume_4	May 22, 2020, 08:00 AM	0.00 TB Imported	Green
Source, Volume_5	Dest, Volume_5	May 22, 2020, 08:00 AM	27.96 TB Imported	Green

27.96 TB 15 1.71 TB 124 26.25 TB

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

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

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

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

Add Connector X

Provider

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



Microsoft Azure



Amazon Web Services



Google Cloud Platform

Continue Back

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

Add Connector - AWS

Deploying a Connector

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

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

Permissions Set up an IAM role with the required permissions	Authentication Choose between two AWS authentication methods: AWS keys or assuming an IAM role	Networking Obtain details about the VPC and subnet in which the Connector will reside
--	--	---

[Skip to Deployment](#)

[Previous](#) [Continue](#)



5. Enter your AWS account authentication access key and secret key.

Add Connector - AWS

[More Information](#) [X](#)

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

AWS Authentication

Region

Select the Authentication Method: Assume Role AWS Keys

AWS Access Key

AWS Secret Key

Want to launch an instance without AWS Credentials? [▼](#)

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



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

The screenshot shows the 'Add Connector - AWS' interface. At the top, there are five tabs: 'AWS Credentials' (selected), 'Details' (highlighted in blue), 'Network', 'Security Group', and 'Review'. Below the tabs, the 'Details' section is titled 'Details'. It contains fields for 'Connector Instance Name' (set to 'SnapCenterSvs'), 'Connector Role' (radio button selected for 'Create Role'), 'Role Name' (set to 'Cloud-Manager-Operator-VZzSSP9-SnapCenter'), and an 'AWS Managed Encryption' toggle switch (disabled). A note below the role name says 'Master Key: aws/ebs (default)' and has a 'Change Key' link. At the bottom of the section are 'Previous' and 'Next' buttons, with the 'Next' button being blue.

7. Configure networking with the proper VPC, subnet, and SSH key pair for EC2 access.

Add BlueXP Connector - AWS

More Information X

AWS Credentials Details Network Security Group Review

Network

Connectivity

VPC:

Subnet:

Key Pair:

Public IP:

Proxy Configuration (Optional)

HTTP Proxy:

Define Credentials for this Proxy:

Upload a root certificate:

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

Previous Next



8. Set the security group for the connector.

Add BlueXP Connector - AWS

More Information X

AWS Credentials Details Network Security Group Review

Security Group

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

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

Security Group Name	Description
default	default VPC security group

1 Security Group

Previous Next



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

The screenshot shows the 'Review' step of the 'Add BlueXP Connector - AWS' wizard. The configuration details listed are:

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

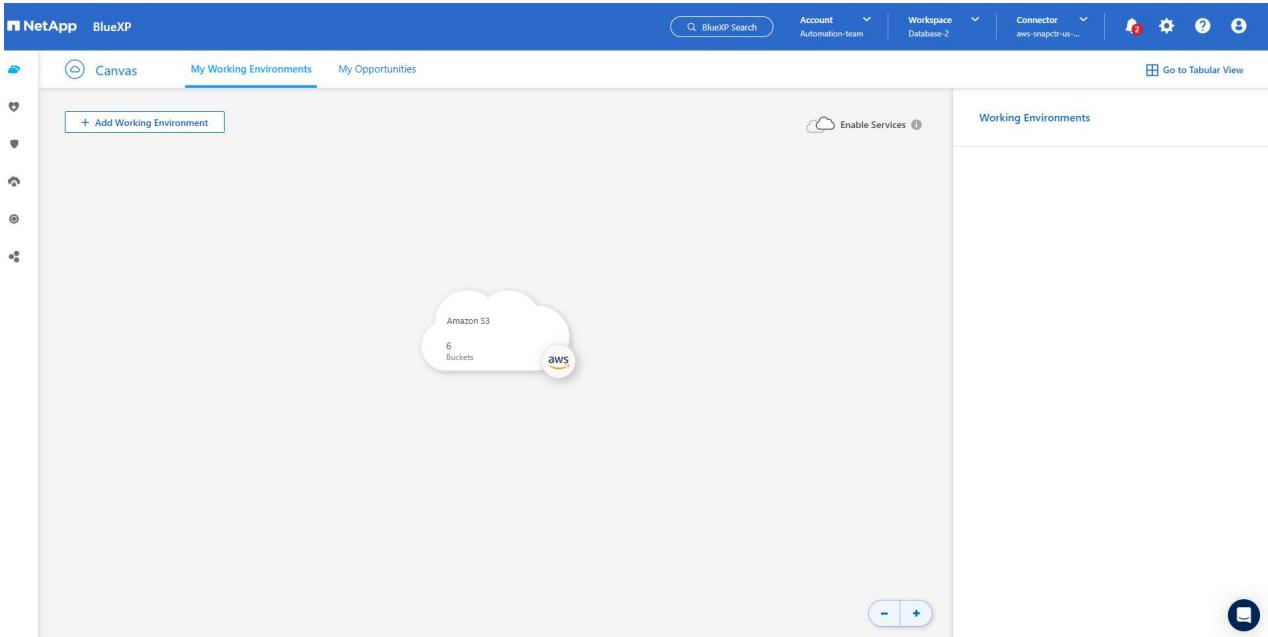
At the bottom of the screen, there are two buttons: 'Previous' and 'Add'. To the right of the buttons is a help icon (a blue circle with a white question mark).

10. After the connector is deployed, log into the connector EC2 host as the ec2-user with an SSH key to install the SnapCenter plug-in following these instructions: [Deploy the plug-in using script and add host from UI using manual option](#).

SnapCenter services setup

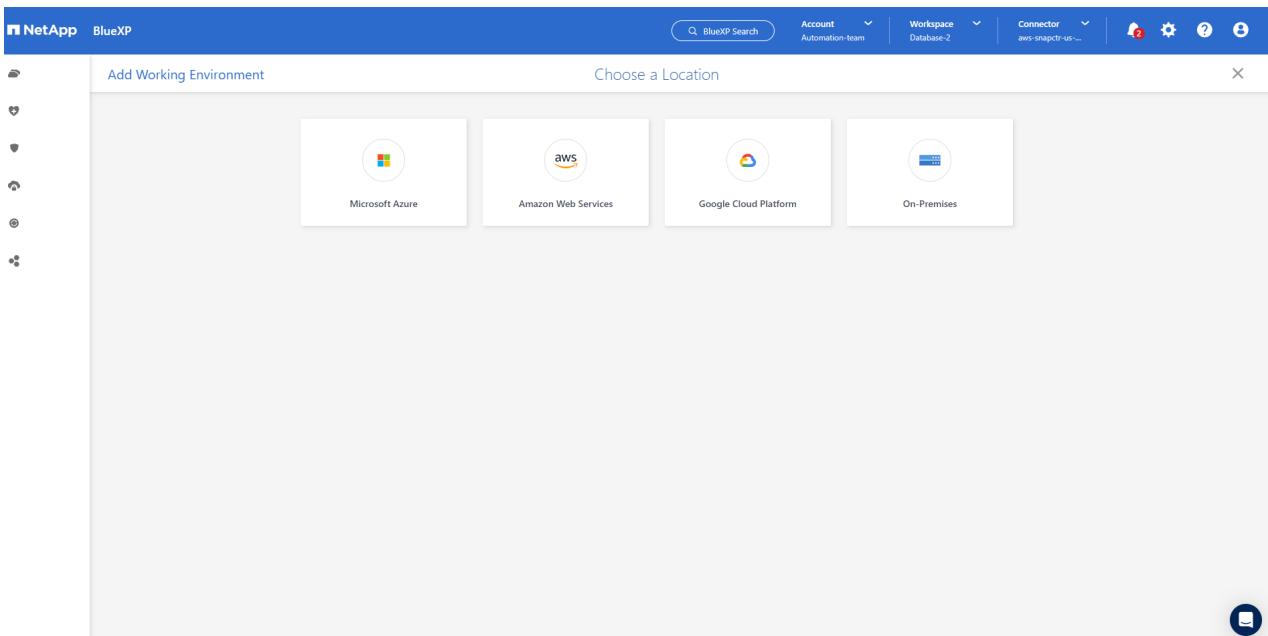
With the connector deployed, SnapCenter services can now be set up with the following procedure:

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



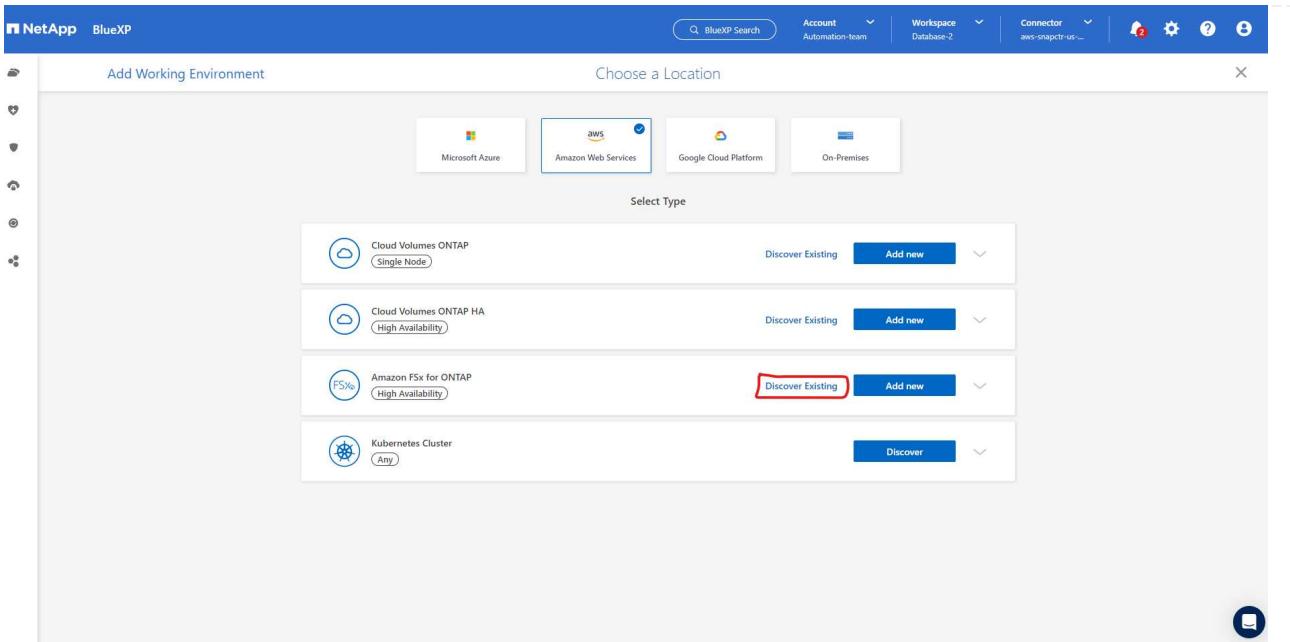
The screenshot shows the NetApp BlueXP web interface. At the top, there's a blue header bar with the NetApp logo, the word "BlueXP", and various navigation links like "Account", "Workspace", and "Connector". Below the header, there are three main tabs: "Canvas", "My Working Environments" (which is currently selected), and "My Opportunities". On the left side, there's a sidebar with several icons. The main content area features a large, stylized white cloud icon with the "aws" logo at the bottom right. Inside the cloud, it says "Amazon S3" and "6 Buckets". To the right of the cloud icon, there's a button labeled "+ Add Working Environment". At the bottom right of the main content area, there are "- +" buttons and a small circular icon with a speech bubble. The overall theme is light blue and white.

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

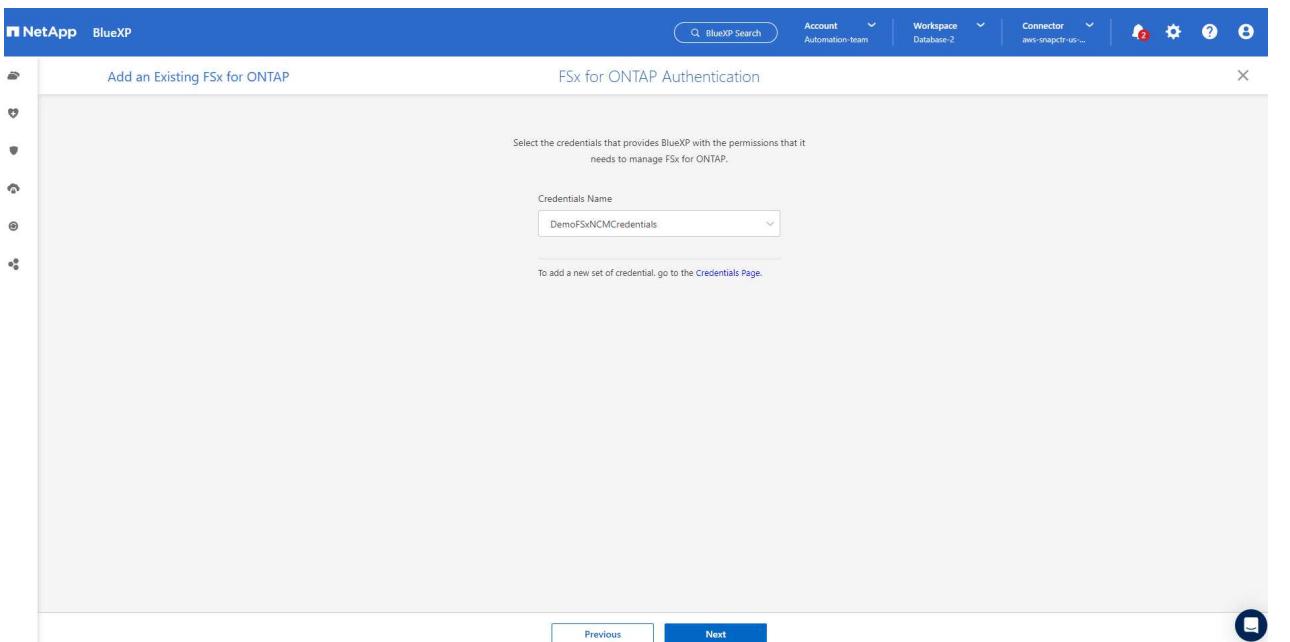


The screenshot shows a modal dialog box titled "Add Working Environment" with the sub-section "Choose a Location". The dialog has a light gray background. At the top right is a close button ("X"). The main area contains four square buttons, each representing a different cloud provider or location type. The second button from the left, which has the "aws" logo, is highlighted with a thin blue border, indicating it is selected. The other three buttons are for "Microsoft Azure", "Google Cloud Platform", and "On-Premises". The overall design is clean and modern, using a white background with blue and gray accents.

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



4. Select the credentials that provides BlueXP with the permissions that it needs to manage FSx for ONTAP. If you have not added credentials, you can add it from the **Settings** menu at the top right corner of the BlueXP console.



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

Add an Existing FSx for ONTAP

Select FSx for ONTAP

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

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

Name	File System ID	VPC ID	Subnet ID	Management Address	Deployment modal	Tags
fsx_01	fs-02ad7bf3476b741df	vpc-0b522d5e982a...	subnet-04f5fe7073ff5...	management.fs-02ad7bf3476b741df.fsx.us-east...	Single Availability Zone	(4)

Previous Add

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

Canvas My Working Environments My Opportunities

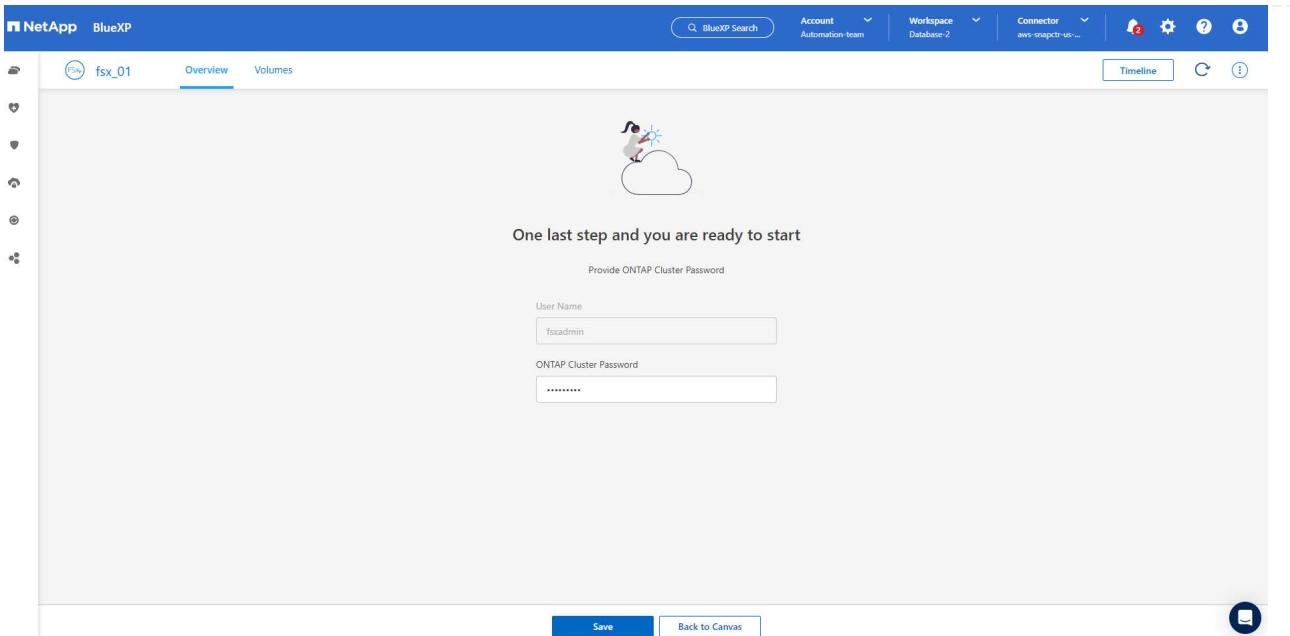
+ Add Working Environment

Enable Services

Working Environments

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

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



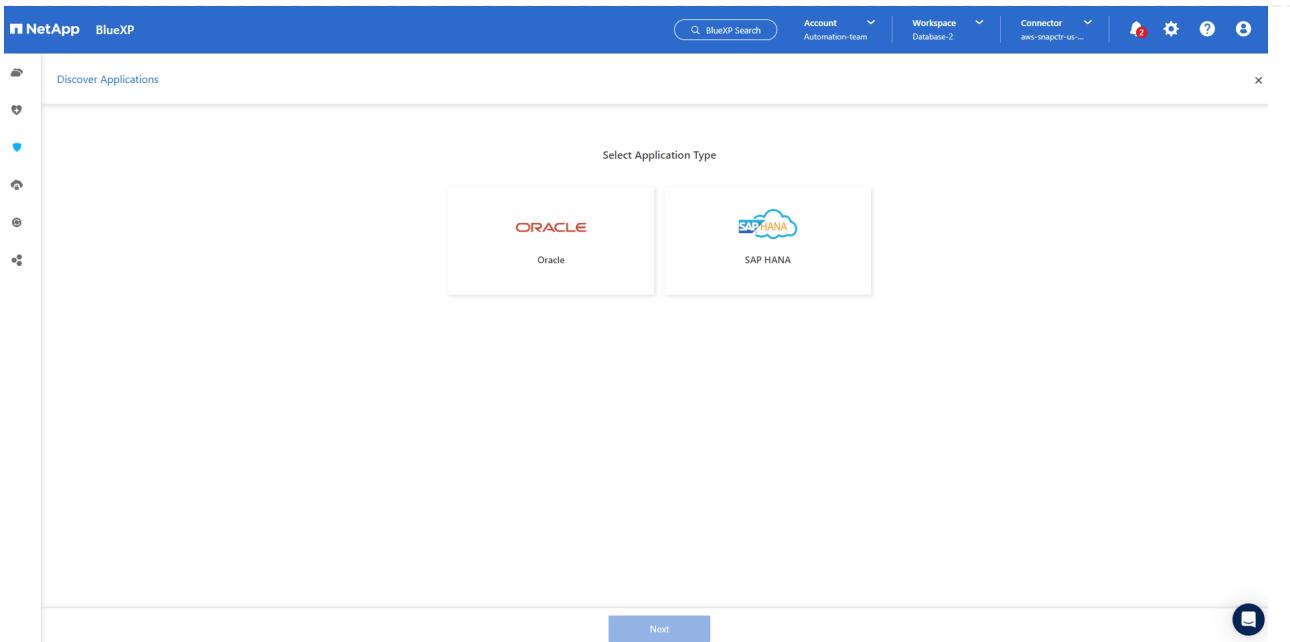
8. After you log into Amazon FSx for ONTAP, review your database storage information (such as database volumes).

Volume	INFO	CAPACITY
ora_01_data	Disk Type: SSD SVM Name: svm_ora Tiering Policy: Snapshot Only	Provisioned: 100 GiB SSD Used: 5.79 GiB Capacity Pool Used: 0 GiB
ora_01_logs	Disk Type: SSD SVM Name: svm_ora Tiering Policy: Snapshot Only	Provisioned: 100 GiB SSD Used: 1.14 GiB Capacity Pool Used: 0 GiB
ora_01_bin	Disk Type: SSD SVM Name: svm_ora Tiering Policy: Snapshot Only	Provisioned: 50 GiB SSD Used: 19.1 GiB Capacity Pool Used: 0 GiB

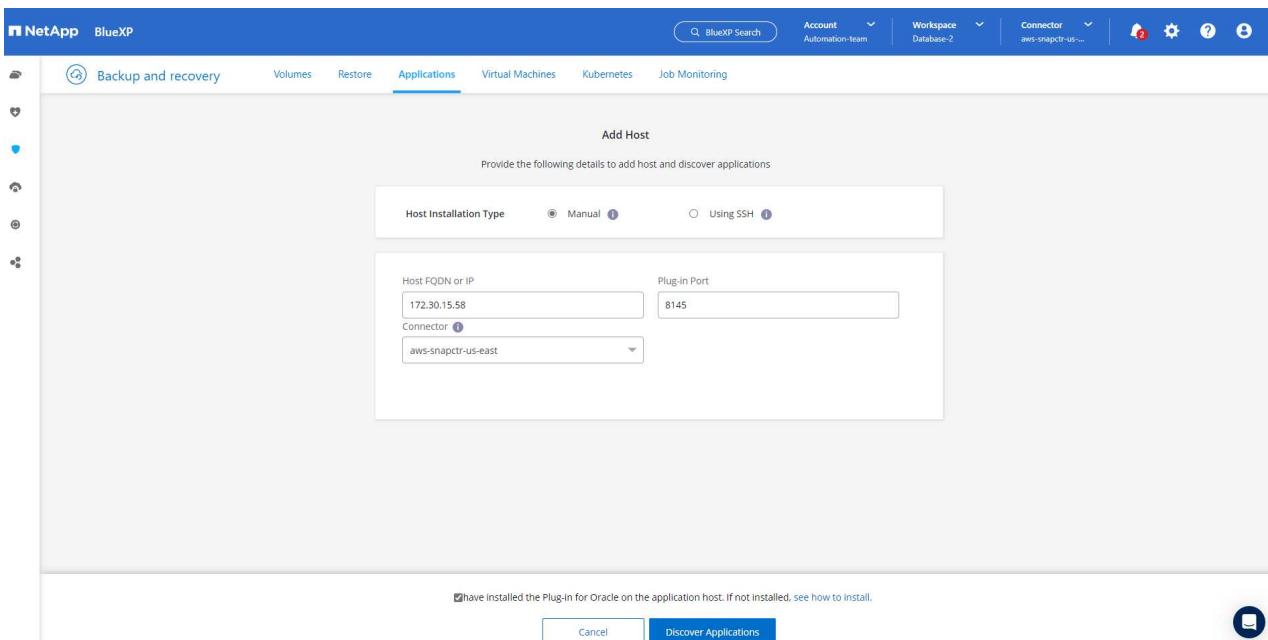
9. From the left-hand sidebar of the console, hover your mouse over the protection icon, and then click **Protection > Applications** to open the Applications launch page. Click **Discover Applications**.

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

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



12. Provide the Oracle EC2 instance host details to add a host. Check the box to confirm that the plug-in for Oracle on the host has been installed, because you deploy the plug-in after the connector is provisioned.



13. Discover the Oracle EC2 host and add it to **Applications**, and any databases on the host are discovered and displayed on the page as well. The database **Protection Status** shows as **Unprotected**.

The screenshot shows the NetApp BlueXP web interface. At the top, there are navigation tabs: Backup and recovery, Volumes, Restore, Applications (which is selected), Virtual Machines, Kubernetes, and Job Monitoring. The top right includes search, account, workspace, connector, and notification icons. Below the tabs, there's a summary section with counts for Hosts (1), ORACLE (1), and Clone (0). A 'Cloud Native' dropdown is set to Oracle. To the right is an 'Application Protection' box showing 0 Protected and 1 Unprotected. The main area displays a table titled '1 Databases' with one entry: db1, Host Name 172.30.15.58, Policy Name (empty), Protection Status Unprotected. There are buttons for 'Manage Databases' and 'Settings'.

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

Oracle database backup

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

The screenshot shows the NetApp BlueXP interface with the Applications tab selected. In the top navigation bar, the account is set to 'Automation-team' and the workspace is 'Database-2'. The left sidebar has icons for Cloud Native, Oracle, Kubernetes, and Job Monitoring. The main content area displays application protection statistics: 1 Host, 1 Oracle, and 0 Clones. Below this, a table lists 1 database named 'db1' with host '172.30.15.58'. The 'Protection Status' column shows 'Unprotected'. A context menu is open over the 'db1' row, with options like 'Policies', 'About', and 'Hosts'. The bottom right corner of the table has a blue circular icon with a white envelope.

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

The screenshot shows the NetApp BlueXP Applications > Policies page. The top navigation bar includes 'BlueXP Search', 'Account Automation-team', 'Workspace Database-2', and 'Connector aws-snapctr-us...'. The left sidebar shows 'Cloud Native' and 'Oracle'. The main content area displays four policies: 'Oracle Full Backup for Bronze', 'Oracle Full Backup for Gold', 'Oracle Full Backup for Silver', and 'my_full_bkup'. Each policy is associated with a 'Backup Type' (FullBackup) and a 'Schedules and Retention' section. The 'my_full_bkup' policy has a 'Create Policy' button above it. The bottom right corner of the table has a blue circular icon with a white envelope.

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

Cloud Native

Oracle

Application Protection

Hosts: 1

ORACLE: 1

Clone: 0

Protected: 0

Unprotected: 1

Databases: 1

Name: db1

Host Name: 172.30.15.58

Policy Name:

Protection Status: Unprotected

Assign Policy

4. Choose the policy to assign to the database.

Assign Policy

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

Policies

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

1 - 4 of 4

Cancel Assign

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

The screenshot shows the NetApp BlueXP web interface. At the top, there are navigation tabs: Backup and recovery (selected), Volumes, Restore, Applications, Virtual Machines, Kubernetes, and Job Monitoring. The Applications tab is highlighted in blue. Below the tabs, there are two dropdown menus: 'Cloud Native' and 'Oracle'. A summary box displays counts for Hosts (1), ORACLE (1), and Clone (0). An 'Application Protection' section shows 1 Protected and 0 Unprotected items. The main content area is titled '1 Databases' and includes a search bar, filter button, and 'Manage Databases' and 'Settings' buttons. A table lists one database entry: db1, Host Name 172.30.15.58, Policy Name my_full_bkup, and Protection Status Protected. A small '...' icon is next to the row.

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

This screenshot is similar to the previous one but shows a context menu for the database entry 'db1'. The menu is titled 'View Details' and includes options: 'On-Demand Backup' (which is highlighted with a red border), 'Assign Policy', and 'Un-assign Policy'. The rest of the interface is identical to the first screenshot, showing the same summary, protection status, and table of database details.

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

The screenshot shows the NetApp BlueXP interface. The top navigation bar includes 'NetApp BlueXP' logo, 'BlueXP Search' search bar, 'Account Automation-team', 'Workspace Database-2', 'Connector aws-snapctr-us...', and various system icons.

The main menu has tabs: 'Backup and recovery' (selected), 'Volumes', 'Restore', 'Applications' (selected), 'Virtual Machines', 'Kubernetes', and 'Job Monitoring'.

The 'Database Details' section for 'db1' displays the following information:

db1	Protected Protection	Oracle Full Backup for Gold Policy Names	Database Type
Database Name			
172.30.15.58	FSx	Unreachable	bKed8yv2T19BJ0V5QyqvA...
Host Name	Host Storage	Database Version	Agent Id
-	-		
Clones	Parent Database		

Below this, there is a section titled '8 Backups' with a table:

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

Oracle database restore and recovery

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

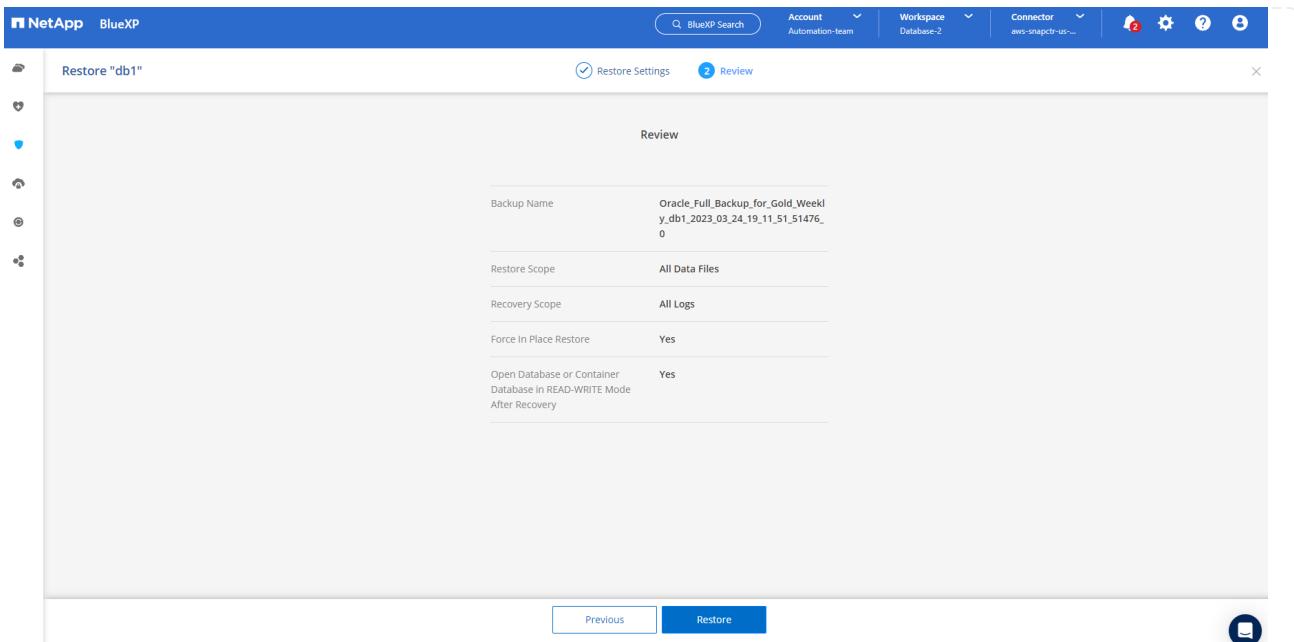
The screenshot shows the 'Database Details' section for a database named 'db1'. It displays various configuration details such as Protection, Host Name, Host Storage, and Database Type. Below this, a table lists four backups. The third backup, 'Oracle_Full_Backup_for_Gold_Hourly_db1_2023_03_24_18_10_31_71953_1', has a context menu open with a red box highlighting the 'Restore' option.

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

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

The screenshot shows the 'Restore Settings' dialog for restoring database 'db1'. Under 'Restore Scope', the 'All Data Files' option is selected. The 'Force in place restore' checkbox is checked, with a note explaining it will skip validation checks for foreign files. Under 'Recovery Scope', 'All Logs' is selected. The 'Archive Log Files Locations' field is set to '/mnt/log_location001'. A note at the bottom of the dialog states: 'Open the database or the container database in READ-WRITE mode after recovery.'

- Review and start database restore and recovery.



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

Backup and recovery Volumes Restore Applications Virtual Machines Kubernetes Job Monitoring

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

Advanced Search & Filtering Timeframe: Last 24 Hours

Jobs(30)

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

The screenshot shows the NetApp BlueXP web interface. At the top, there are navigation links for Backup and recovery, Volumes, Restore, Applications, Virtual Machines, Kubernetes, and Job Monitoring. The Job Monitoring link is currently selected, indicated by an underline. Below this, a breadcrumb trail shows 'Job Monitoring > Job Id: 1fdca0bd-a9c8-45aa-9d7a-05a07cb291f4'. The main content area is titled 'Job Details' and displays a table of 'Sub-Jobs(6)'. The table has columns for Job Name, Job ID, Start Time, End Time, Duration, and a '+' button for adding new jobs. The data in the table is as follows:

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

Oracle database clone

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

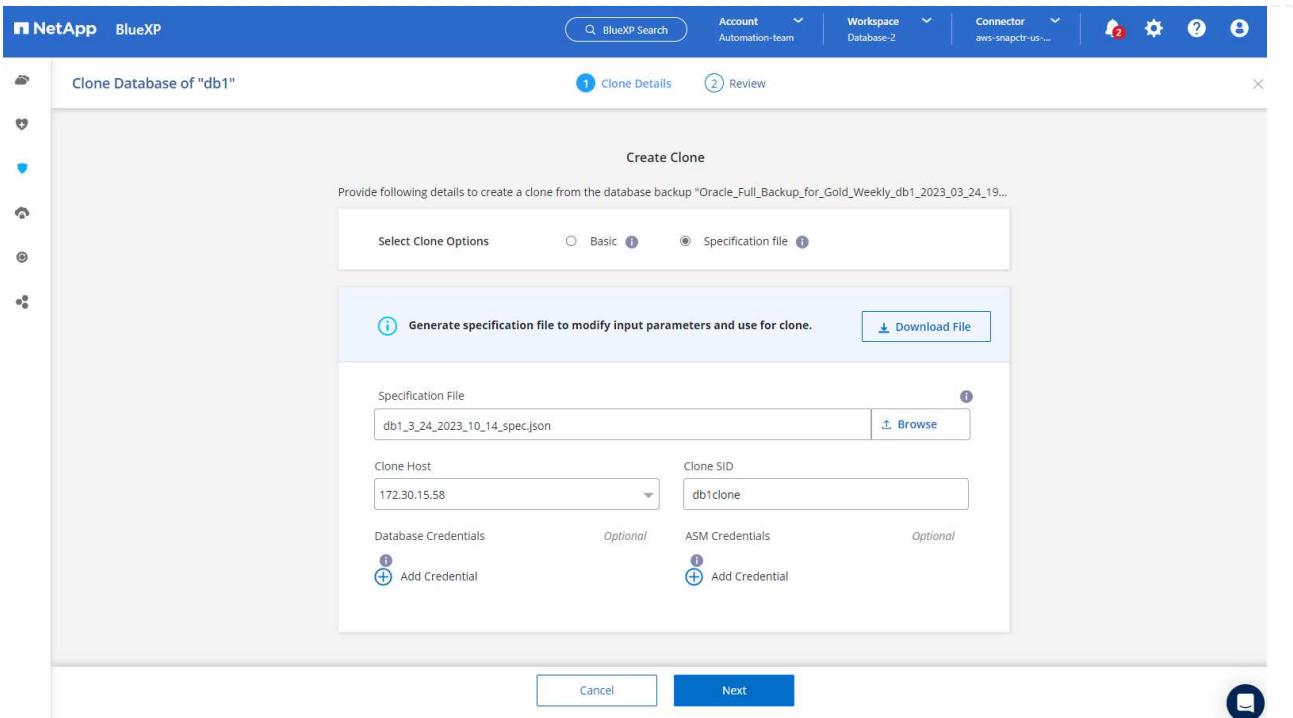
1. Select the right database backup copy, click the three dots to view the menu, and choose the **Clone** option.

The screenshot shows the 'Database Details' section of the NetApp BlueXP interface. It displays a table with columns: Database Name, Protection Status, Oracle Full Backup for Gold Policy Names, and Database Type. Below this is a table for Host Name, Storage Type, Database Version, and Agent ID. At the bottom, there's a 'Clones' section and a 'Parent Database' entry. Below these tables is a 'Backups' section with a table showing two entries: 'Oracle_Full_Backup_for_Gold_Hourly_db1_2023_03_24_13_34_41_30491_1' (Log, Mar 24, 2023, 9:34:55 am) and 'Oracle_Full_Backup_for_Gold_Hourly_db1_2023_03_24_13_34_07_26748_0' (Data, Mar 24, 2023, 9:34:41 am). A context menu is open over the second backup entry, with the 'Clone' option highlighted by a red box.

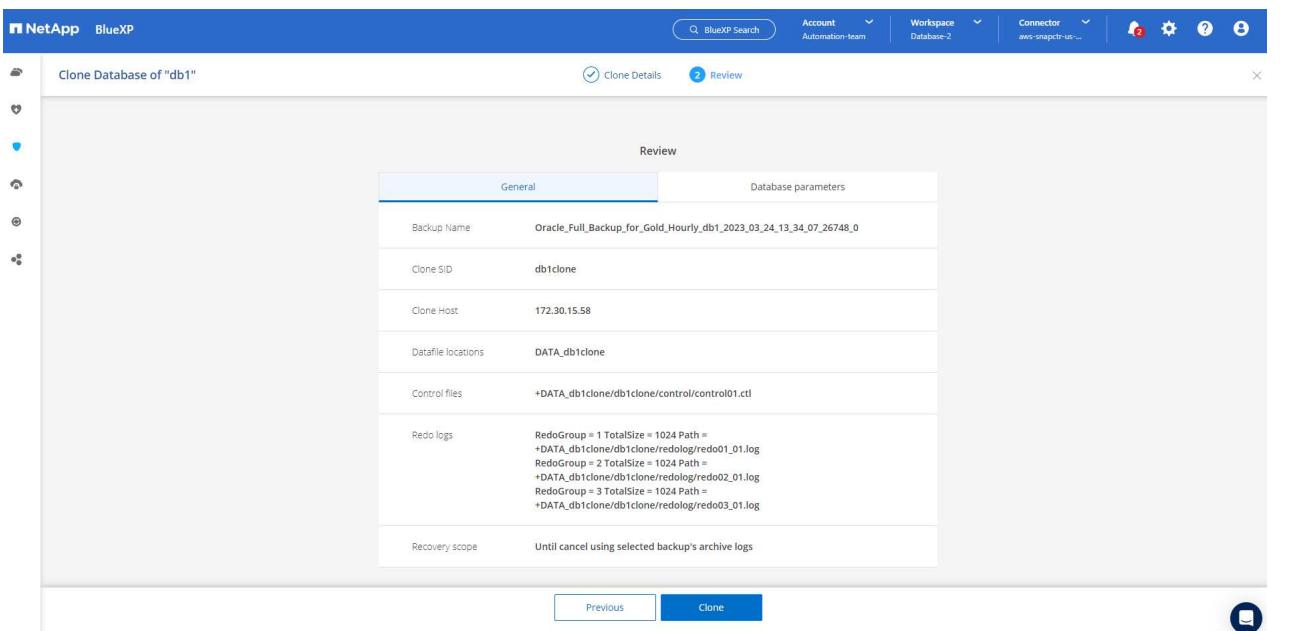
2. Select the **Basic** option if you don't need to change any cloned database parameters.

The screenshot shows the 'Create Clone' wizard step. It has two tabs at the top: 'Clone Details' (selected) and 'Review'. The main area is titled 'Create Clone' and contains instructions: 'Provide following details to create a clone from the database backup "Oracle_Full_Backup_for_Gold_Hourly_db1_2023_03_24_13_...".' Below this is a 'Select Clone Options' section with a radio button for 'Basic' (selected) and 'Specification file'. The 'Clone Host' field is set to '172.30.15.58' and the 'Clone SID' is 'db1clone'. The 'Clone Naming Scheme' is 'Auto-generated' and the 'Oracle Home' path is '/u01/app/oracle/product/19.0.0/db1'. Under 'Database Credentials', there are 'Optional' fields for 'Add Credential' (with a plus sign icon).

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



4. Review and launch the job.



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

The screenshot shows the NetApp BlueXP interface with the 'Job Monitoring' tab selected. A specific job is being tracked, with its ID visible in the URL. The interface displays the 'Job Details' for this job, which includes a table of sub-jobs. The sub-jobs listed are:

Job Name	Job ID	Start Time	End Time	Duration
Cloning Oracle Database db1 as db1clone on h...	cd30abaf-fbe2-4052-a6db-4bf965a8d29b	Mar 24 2023, 1:30:36 pm	--	--
Running pre scripts	5ff152c1-853a-4ec6-a4f...	Mar 24 2023, 1:30:41 pm	Mar 24 2023, 1:30:41 pm	0 Second
Validating clone request	f93a6cc4-2eb2-4c5e-9f...	Mar 24 2023, 1:30:35 pm	Mar 24 2023, 1:30:42 pm	7 Seconds

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

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

```

[oracle@ip-172-30-15-58 ~]$ export ORACLE_HOME=/u01/app/oracle/product/19.0.0/db1
[oracle@ip-172-30-15-58 ~]$ export ORACLE_SID=db1clone
[oracle@ip-172-30-15-58 ~]$ export PATH=$ORACLE_HOME/bin:$PATH
[oracle@ip-172-30-15-58 ~]$ sqlplus / as sysdba

SQL*Plus: Release 19.0.0.0.0 - Production on Fri Mar 24 18:32:21 2023
Version 19.18.0.0.0

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

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

SQL> select name, open_mode from v$database;

NAME      OPEN_MODE
----- -----
DB1CLONE  READ WRITE

SQL>

```

Additional information

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

- Set up and administer BlueXP

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

- Cloud Backup documentation

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

- Amazon FSx for NetApp ONTAP

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

- Amazon EC2

https://aws.amazon.com/pm/ec2/?trk=36c6da98-7b20-48fa-8225-4784bc9843&sc_channel=ps&s_kwcid=AL!4422!3!467723097970!e!!g!!aws%20ec2&ef_id=Cj0KCQiA54KfBhCKARIzAJzSrdqwQrghn6I71jiWzSeaT9Uh1-vY-VfhJixFxnv5rWwn2S7RqZOTQ0aAh7eEALw_wcB:G:s&s_kwcid=AL!4422!3!467723097970!e!!g!!aws%20ec2

Hybrid Cloud Database Solutions with SnapCenter

TR-4908: Hybrid Cloud Database Solutions with SnapCenter Overview

Alan Cao, Felix Melligan, NetApp

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

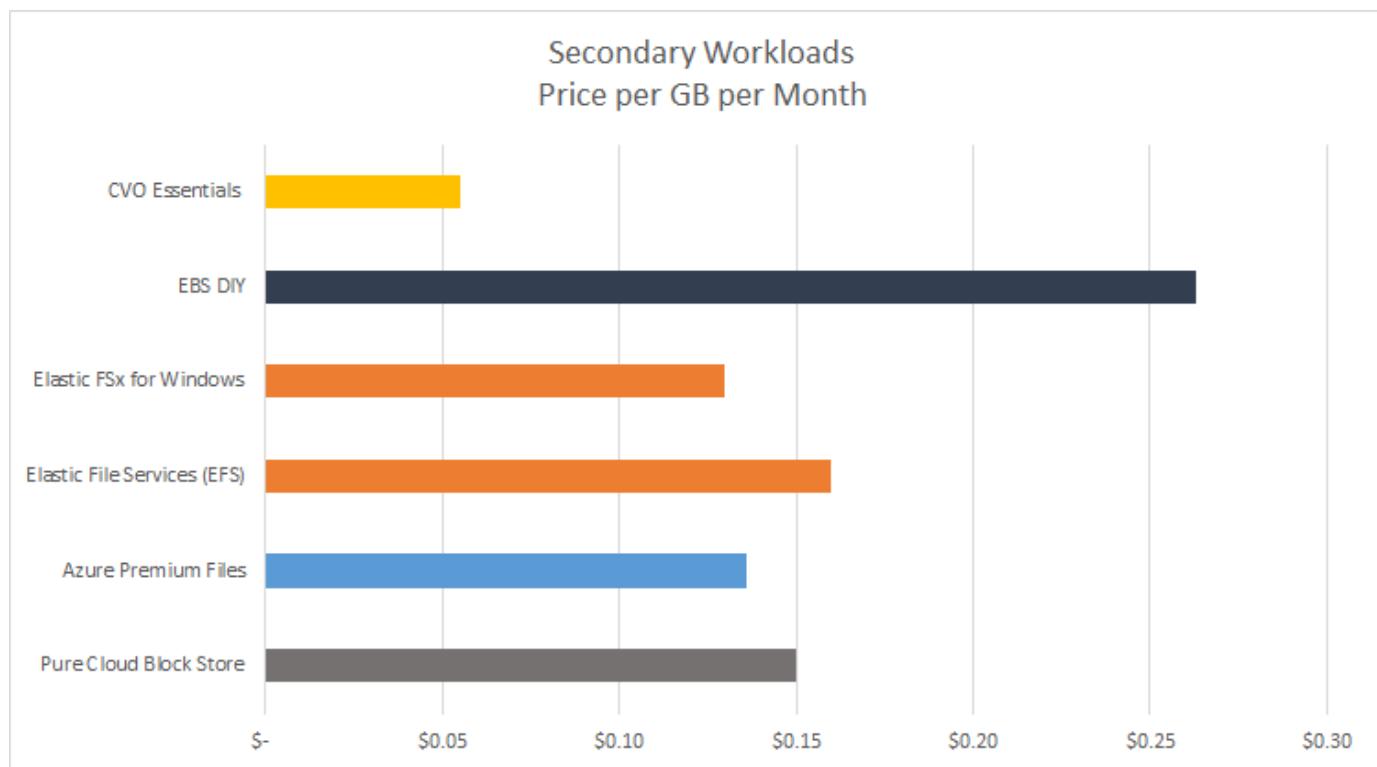
- Database dev/test operations in the hybrid cloud
- Database disaster recovery in the hybrid cloud

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

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

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

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



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

The following videos demonstrate SnapCenter in action:

- [Backup of an Oracle database across a Hybrid Cloud using SnapCenter](#)

- SnapCenter- Clone DEV/TEST to AWS Cloud for an Oracle database

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

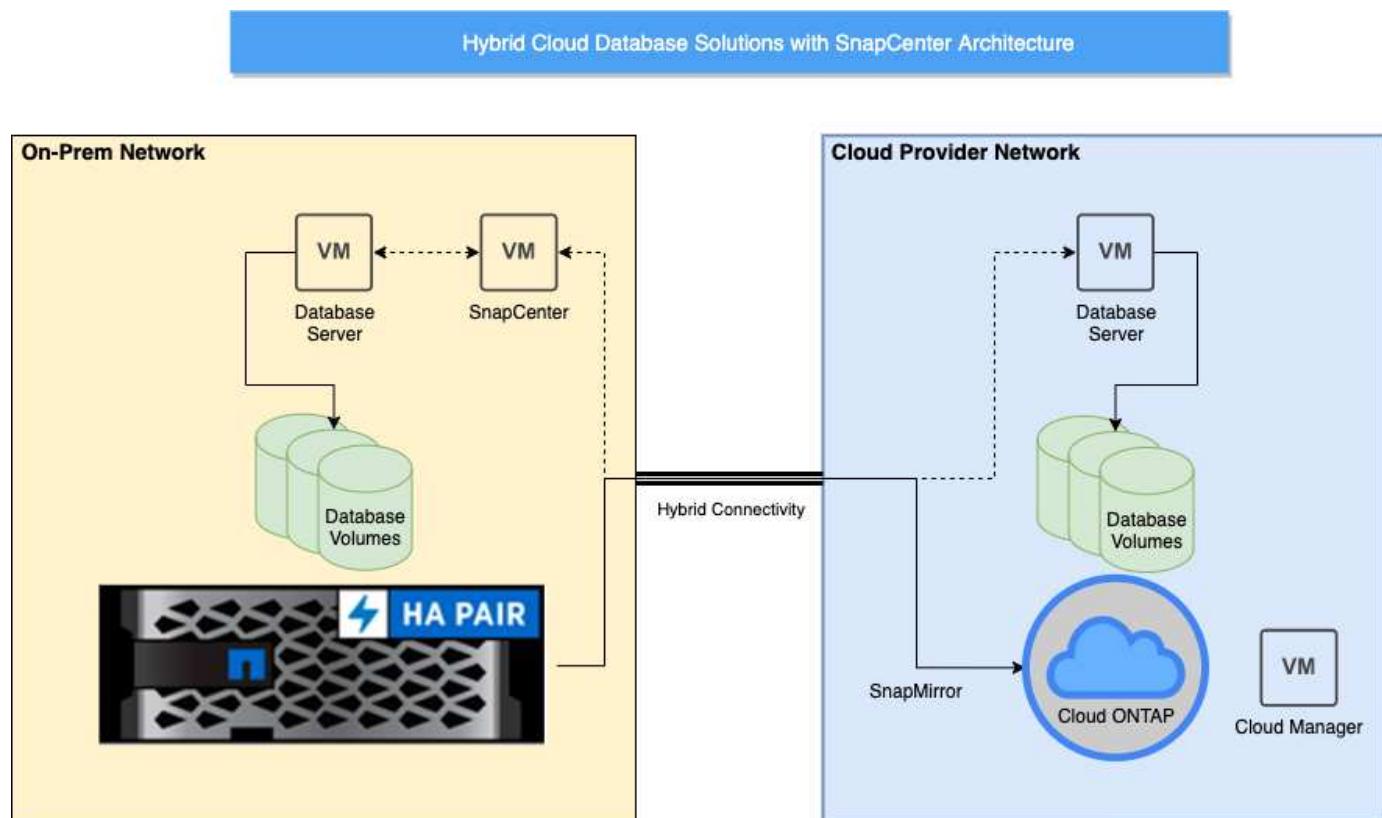
To test drive the solution and use cases for yourself, a NetApp Lab-on-Demand SL10680 can be requested at following xref:./databases/ [TL_AWS_004 HCoD: AWS - NW,SnapCenter\(OnPrem\)](#).

[Next: Solutions architecture.](#)

Solution Architecture

[Previous: Introduction.](#)

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



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

[Next: Solutions requirements.](#)

SnapCenter Requirements

[Previous: Solutions architecture.](#)

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

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

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

Requirements

Environment	Requirements
On-premises	<p>Any databases and versions supported by SnapCenter</p> <p>SnapCenter v4.4 or higher</p> <p>Ansible v2.09 or higher</p> <p>ONTAP cluster 9.x</p> <p>Intercluster LIFs configured</p> <p>Connectivity from on-premises to a cloud VPC (VPN, interconnect, and so on)</p> <p>Networking ports open</p> <ul style="list-style-type: none">- ssh 22- tcp 8145, 8146, 10000, 11104, 11105
Cloud - AWS	<p>Cloud Manager Connector</p> <p>Cloud Volumes ONTAP</p> <p>Matching DB OS EC2 instances to On-prem</p>
Cloud - Azure	<p>Cloud Manager Connector</p> <p>Cloud Volumes ONTAP</p> <p>Matching DB OS Azure Virtual Machines to On-prem</p>
Cloud - GCP	<p>Cloud Manager Connector</p> <p>Cloud Volumes ONTAP</p> <p>Matching DB OS Google Compute Engine instances to on-premises</p>

[Next: Prerequisites configuration.](#)

Prerequisites configuration

[Previous: Solutions requirements.](#)

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

On premises

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

Public cloud

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

Important considerations:

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

The following links provide further details:

[On Premises](#)

[Public Cloud](#)

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

Prerequisites on-premises

[Previous: Prerequisites configuration.](#)

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

SnapCenter installation and configuration

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

- **Single instance or HA deployment.** HA deployment provides redundancy in the case of a single SnapCenter instance server failure.
- **Name resolution.** DNS must be configured on the SnapCenter server to resolve all database hosts as well as on the storage SVM for forward and reverse lookup. DNS must also be configured on database servers to resolve the SnapCenter server and the storage SVM for both forward and reverse lookup.

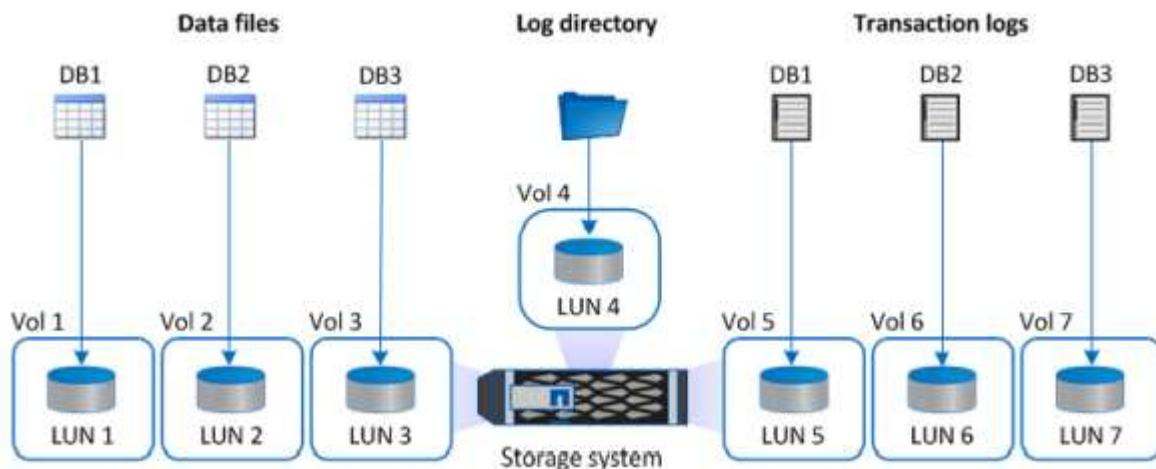
- **Role-based access control (RBAC) configuration.** For mixed database workloads, you might want to use RBAC to segregate management responsibility for different DB platform such as an admin for Oracle database or an admin for SQL Server. Necessary permissions must be granted for the DB admin user.
- **Enable policy-based backup strategy.** To enforce backup consistency and reliability.
- **Open necessary network ports on the firewall.** For the on-premises SnapCenter server to communicate with agents installed in the cloud DB host.
- **Ports must be open to allow SnapMirror traffic between on-prem and public cloud.** The SnapCenter server relies on ONTAP SnapMirror to replicate onsite Snapshot backups to cloud CVO storage SVMs.

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

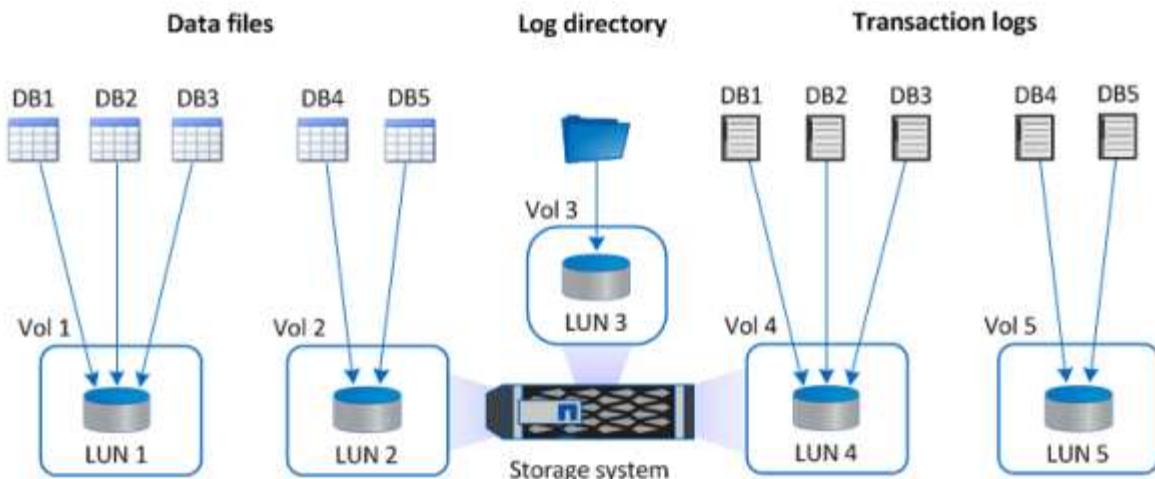
On-premises database server storage configuration

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

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



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



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

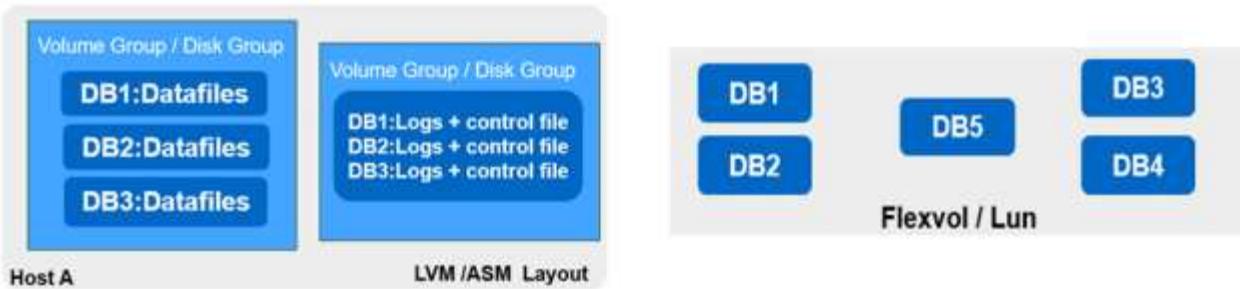
For Oracle database workloads, SnapCenter supports database environments backed by ONTAP storage that are mounted to the host as either physical or virtual devices. You can host the entire database on a single or multiple storage devices based on the criticality of the environment. Typically, customers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



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



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



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

Licensing requirements

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

[SnapCenter standard capacity-based licenses](#)

Networking and security

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

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

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

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

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

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

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

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

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

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

Next: Public cloud.

Prerequisites for the public cloud

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

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

Cloud Manager and Cloud Volumes ONTAP deployment prerequisites checklist

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

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

Considerations

1. What is a Cloud Manager connector?

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

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

2. Cloud Volumes ONTAP sizing and architecture

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

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

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

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

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

3. Single node or high availability?

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

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

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

[Next: Getting started overview.](#)

Getting started overview

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

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

On-premises

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

AWS public cloud

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

Click the following links for details:

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

Getting started on premises

Previous: [Getting started overview.](#)

On Premises

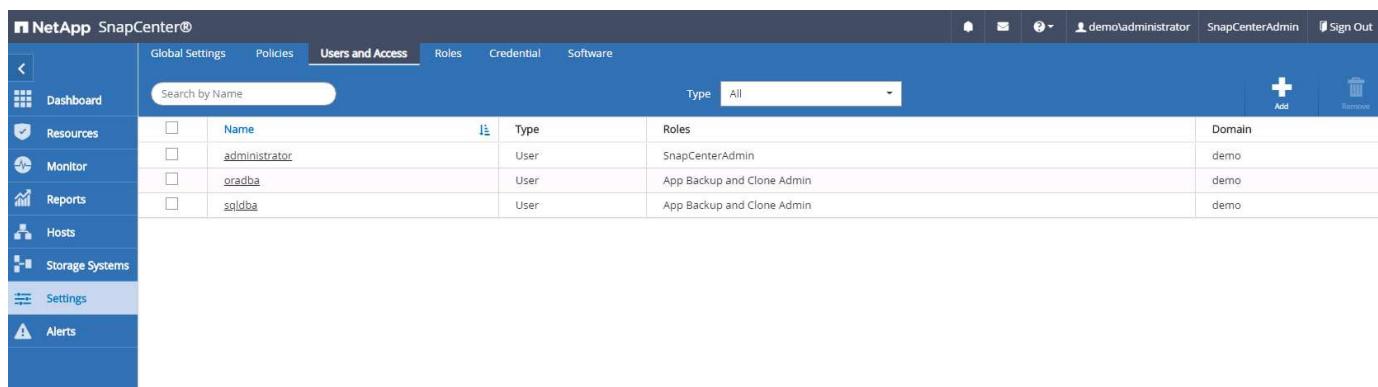
1. Setup database admin user in SnapCenter

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

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

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

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



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

2. SnapCenter plugin installation prerequisites

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

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

Windows host for SQL server:

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

Unix host for Oracle:

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

3. SnapCenter host plugin installation



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

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

Configure SnapCenter VMware global settings

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

Add Windows host and installation of plugin on the host

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

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

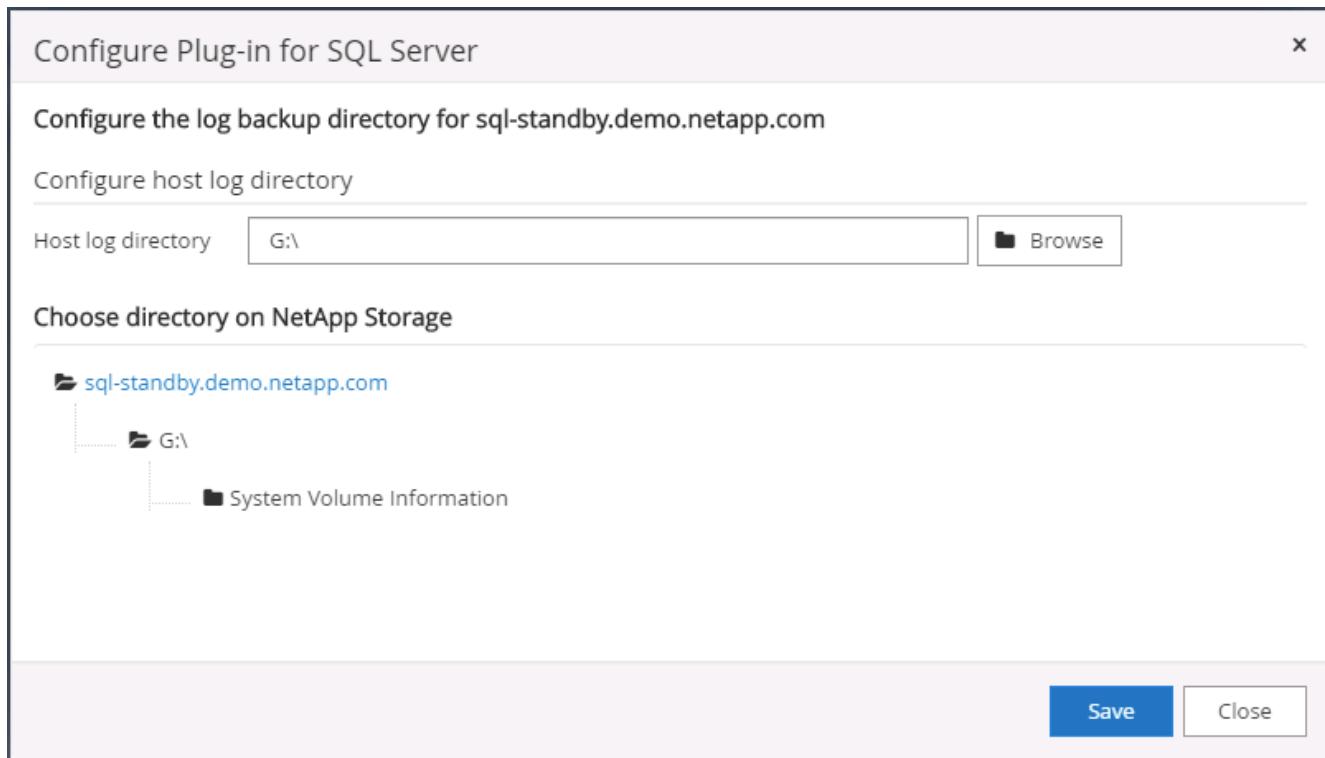
5. Click the Host Name to open the SQL Server log directory configuration.

The screenshot shows the NetApp SnapCenter interface. On the left, there's a sidebar with icons for hosts, storage, and logs. The main area has a title bar "NetApp SnapCenter®" and tabs "Managed Hosts" and "Alerts". Under "Managed Hosts", there's a search bar "Search by Name" and a list of hosts: "Name" (checkbox), "Host IP" (checkbox), "Overall Status" (checkbox), "Host Type" (checkbox), "System" (checkbox), "Credentials" (checkbox), and "Plug-ins" (checkbox). The host "sql-standby.demo.netapp.com" is selected and highlighted in blue. To the right, the "Host Details" panel shows the host name as "sql-standby.demo.netapp.com", host IP as "10.221.2.56", overall status as "Configure log directory", host type as "Windows", system as "Stand-alone", credentials as "Domain Admin", and plug-ins as "SnapCenter Plug-ins package 4.5.0.6123 for Windows" (Microsoft Windows, Microsoft SQL Server). At the bottom are buttons for "Submit", "Cancel", and "Reset".

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

The screenshot shows the "Configure Plug-in for SQL Server" dialog box. The title is "Configure Plug-in for SQL Server" with a close button. The main heading is "Configure the log backup directory for sql-standby.demo.netapp.com". Below it, a section titled "Configure host log directory" contains a "Host log directory" label and a "dedicated disk directory path" input field with a "Browse" button. At the bottom right are "Save" and "Close" buttons.

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



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

- 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

- 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.

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

search

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

Save **Close**

Add Unix host and installation of plugin on the host

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

Add Host

Host Type: Linux

Host Name: ora-standby

Credentials: admin

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

Oracle Database
 SAP HANA

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

Submit **Cancel**

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

More Options

Port	8145	i
Installation Path	/opt/NetApp/snapcenter	i
<input checked="" type="checkbox"/> Skip preinstall checks <input checked="" type="checkbox"/> Add all hosts in the oracle RAC		
Custom Plug-ins		
Choose a File Browse Upload		
No plug-ins found.		
Save Cancel		

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

Confirm Fingerprint

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

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

[Confirm and Submit](#) [Close](#)

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

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

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

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.

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)

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

Name	Host	Resource Groups	Policies	State	Type
sql-standby	sql-standby.demo.netapp.com	None	None	Not available for backup. DB is not on NetApp storage, auto-close is enabled or in recovery mode.	Standalone ()
sql1	sql1.demo.netapp.com				Standalone (15.0.2000)

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

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

5. Setup storage cluster peering and DB volumes replication

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

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

On-premises cluster:

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

Target CVO cluster:

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

The screenshot shows the ONTAP System Manager interface. The left sidebar is collapsed. The main area has a header "ONTAP System Manager" with a link to "Return to classic version". A search bar at the top right says "Search actions, objects, and pages".

- UI Settings:** LOG LEVEL is set to DEBUG. INACTIVITY TIMEOUT is set to 30 minutes.
- Intercluster Settings:**
 - Network Interfaces:** IP ADDRESS is 192.168.0.113.
 - Cluster Peers:** PEERED CLUSTER NAME is hybridcvo. A dropdown menu is open over this section, with "Peer Cluster" highlighted with a red box. Other options include "Generate Passphrase" and "Manage Cluster Peers".
 - Storage VM Peers:** PEERED STORAGE VMS is 1.

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

The screenshot shows the ONTAP System Manager interface with the Volumes tab selected in the left sidebar. The main area displays a list of volumes and detailed information for a selected volume.

- Volumes List:**
 - + Add
 - Delete
 - Protect** (highlighted with a red box)
 - More

	Name
<input type="checkbox"/>	onPrem_data
<input type="checkbox"/>	rhel2_u01
<input type="checkbox"/>	rhel2_u02
<input checked="" type="checkbox"/>	rhel2_u03
<input type="checkbox"/>	rhel2_u030923211942120311
<input type="checkbox"/>	8
<input type="checkbox"/>	sql1_data
<input type="checkbox"/>	sql1_log
<input type="checkbox"/>	sql1_snapctr
<input type="checkbox"/>	svm_onPrem_root
- Detailed Volume Information for rhel2_u03:**
 - Overview:** STATUS is Online. MOUNT PATH is /rhel2_u03. STORAGE VM is svm_onPrem. LOCAL TIER is onPrem_01_SSD_1. SNAPSHOT POLICY is default. QUOTA is Off. TYPE is Read Write. SPACE RESERVATION is 1.
 - Capacity:** Capacity bar chart showing usage from 0% to 50%. Snapshot capacity is 0 Bytes Available | 2.36 GB Used | 2.36 GB Overflow.
 - Performance:** Performance metrics for Hour, Day, and Week. Latency chart shows values of 1.5 and 1.

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

The screenshot shows the 'Protect Volumes' dialog in the ONTAP System Manager. The 'PROTECTION POLICY' dropdown is set to 'Asynchronous'. Under 'Source', 'CLUSTER' is 'onPrem' and 'SELECTED VOLUMES' is 'rhel2_u03'. Under 'Destination', 'CLUSTER' is 'hybridcvo' and 'STORAGE VM' is 'svm_hybridcvo'. In the 'Destination Settings' section, there are two matching labels. The 'VOLUME NAME' field has a prefix 'vol_' and a suffix '_dest'. Under 'Configuration Details', the 'Initialize relationship' checkbox is checked, while 'Enable FabricPool' is unchecked.

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

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

- Log into SnapCenter with a user ID with SnapCenterAdmin privileges.
- 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.

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 TM	<input checked="" type="checkbox"/> Secondary
Protocol	HTTPS	
Port	443	
Timeout	60	seconds
<input type="checkbox"/> Preferred IP		

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

Name	IP	Cluster Name	User Name	Platform	Controller License
svm_hybridcvo	10.0.0.1			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 Policies.

The screenshot shows the NetApp SnapCenter interface. The left sidebar has links for Dashboard, Resources, Monitor, Reports, Hosts, Storage Systems, Settings (which is selected), and Alerts. The main area is titled 'Policies' and shows 'Oracle Database'. A search bar says 'Search by Name'. Below is a table with columns: Name, Backup Type, Schedule Type, Replication, and Verification. Two policies are listed:

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

At the top right are buttons for New (+), Modify, Copy, Details, and Delete.

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

The dialog box is titled 'Modify Oracle Database Backup Policy' with a close button 'x' in the top right. On the left is a vertical navigation bar with steps 1 through 7: 1. Name, 2. Backup Type, 3. Retention, 4. Replication, 5. Script, 6. Verification, 7. Summary. Step 1 is highlighted in blue. The main area is titled 'Provide a policy name' and contains two fields: 'Policy name' with the value 'Oracle Full Online Backup' and 'Details' with the value 'Backup all data and log files'. In the bottom right corner are 'Previous' and 'Next' buttons.

3. Select the backup type and schedule frequency.

Modify Oracle Database Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Select Oracle database backup options

Choose backup type

Online backup

Datafiles, control files, and archive logs

Datafiles and control files

Archive logs

Offline backup i

Mount i

Shutdown

Save state of PDBs i

Choose schedule frequency

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

On demand

Hourly

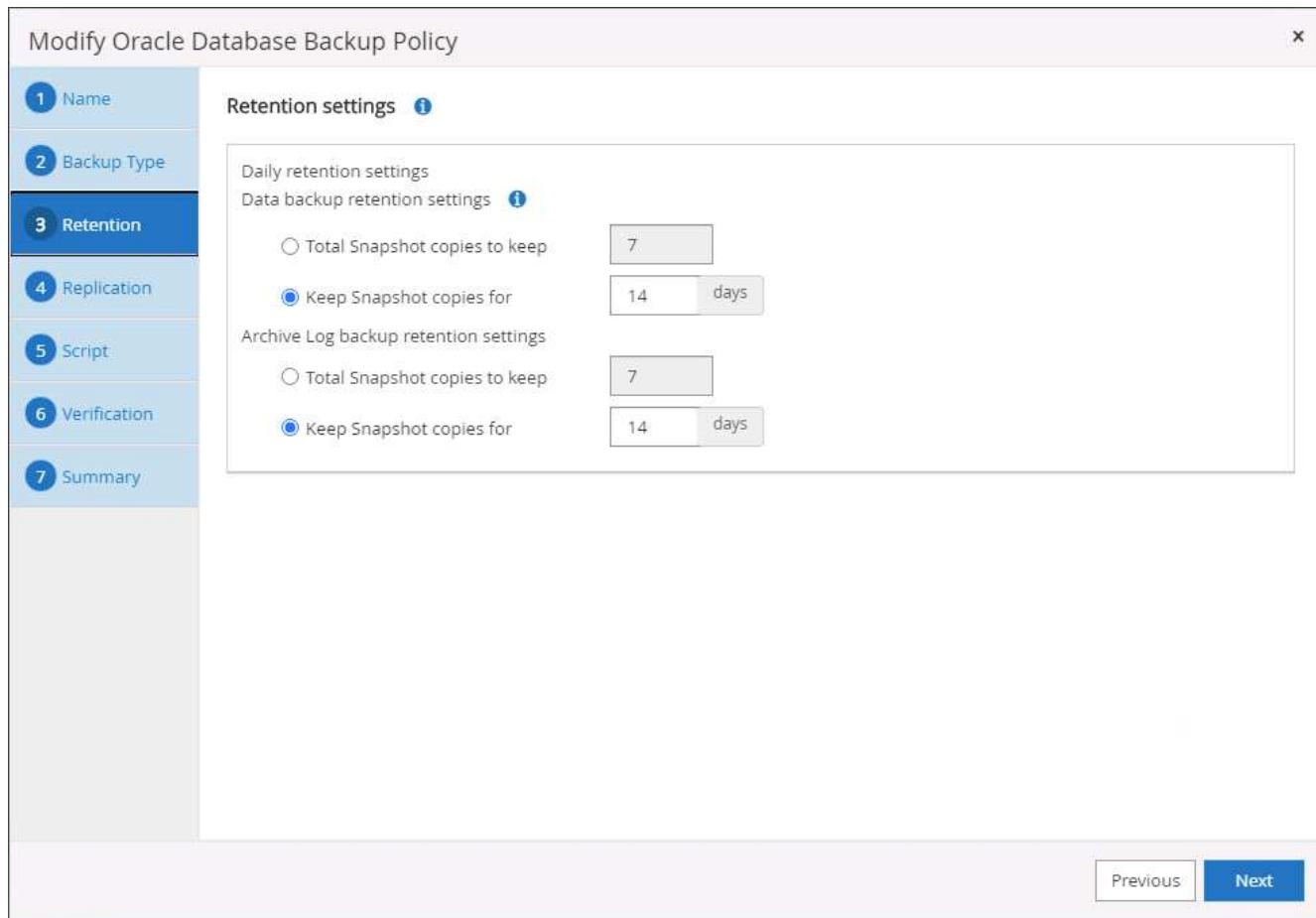
Daily

Previous

Next

This screenshot shows the 'Modify Oracle Database Backup Policy' wizard, specifically step 2: Backup Type. The left sidebar lists steps 1 through 7. Step 2 is currently active, indicated by a blue background. The main area is titled 'Select Oracle database backup options'. Under 'Choose backup type', 'Online backup' and 'Datafiles, control files, and archive logs' are selected. Other options like 'Datafiles and control files' and 'Archive logs' are available but not selected. Below this, under 'Choose schedule frequency', 'Daily' is selected. A note below the frequency section states: '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.' At the bottom right are 'Previous' and 'Next' buttons.

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



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

Modify Oracle Database Backup Policy x

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Select secondary replication options i

Update SnapMirror after creating a local Snapshot copy.

Update SnapVault after creating a local Snapshot copy.

Secondary policy label Daily i

Error retry count 3 i

Previous Next

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

Modify Oracle Database Backup Policy X

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

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

Previous **Next**

7. Run backup verification if desired.

Modify Oracle Database Backup Policy X

1 Name

Select the options to run backup verification

2 Backup Type

Run Verifications for following backup schedules

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

Daily

3 Retention

4 Replication

5 Script

6 Verification

Verification script commands

Script timeout secs

Prescript full path Enter Prescript path

Prescript arguments

Postscript full path Enter Postscript path

Postscript arguments

7 Summary

Previous Next

8. Summary.

Modify Oracle Database Backup Policy

1 Name	Summary
2 Backup Type	Policy name: Oracle Full Online Backup Details: Backup all data and log files
3 Retention	Backup type: Online backup
4 Replication	Schedule type: Daily RMAN catalog backup: Disabled
5 Script	Archive log pruning: None
6 Verification	On demand data backup retention: None On demand archive log backup retention: None
7 Summary	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

[Previous](#)
Finish

Create a database log backup policy for Oracle

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

New Oracle Database Backup Policy X

1 Name

Provide a policy name

Policy name i

Details

2 Backup Type

3 Retention

4 Replication

5 Script

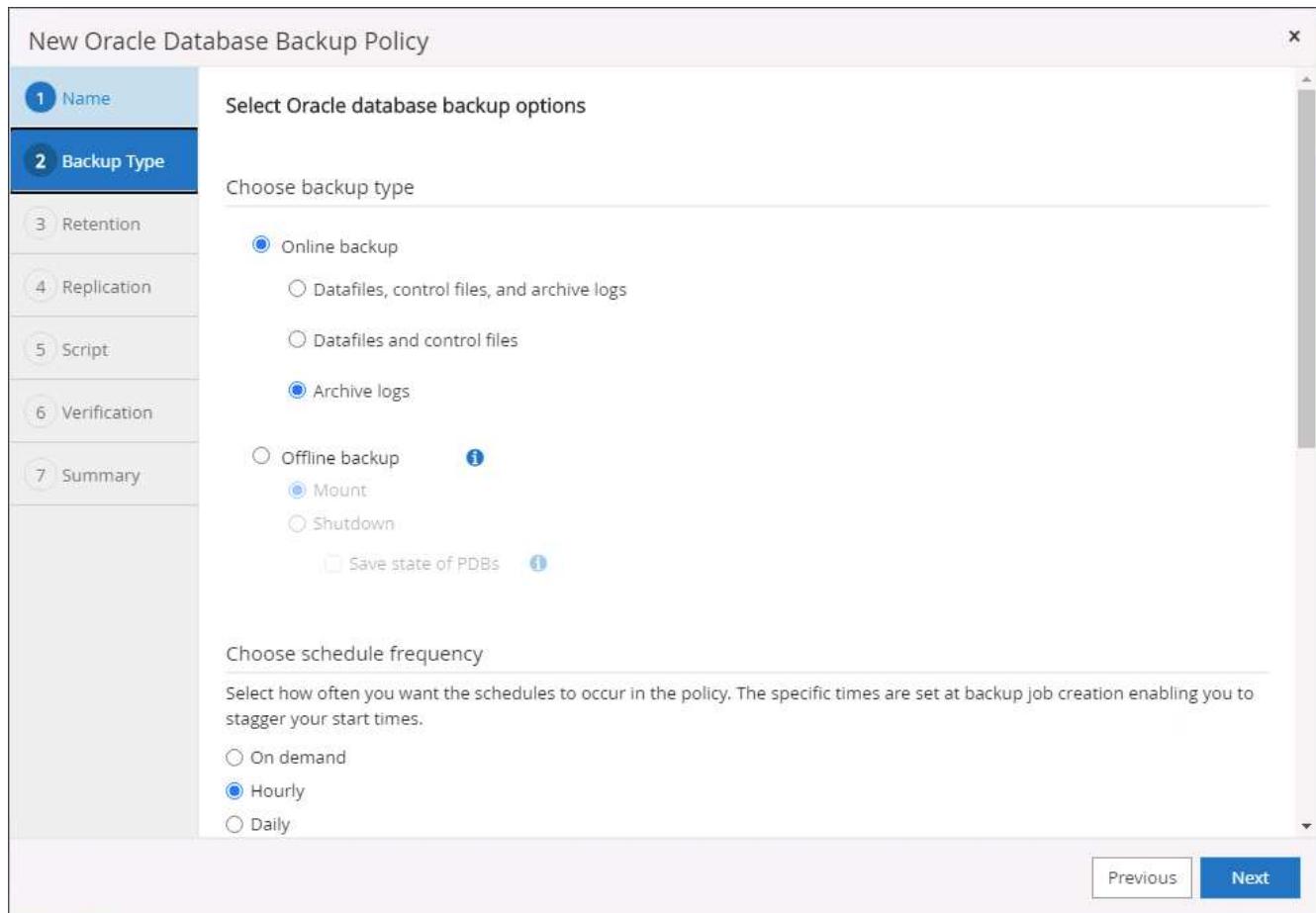
6 Verification

7 Summary

Previous Next

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

3. Select the backup type and schedule frequency.



4. Set the log retention period.

New Oracle Database Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Retention settings i

Hourly retention settings

Data backup retention settings i

Total Snapshot copies to keep

Keep Snapshot copies for days

Archive Log backup retention settings

Total Snapshot copies to keep

Keep Snapshot copies for days

Previous Next

The screenshot shows the 'New Oracle Database Backup Policy' wizard at step 3: Retention. The left sidebar lists steps 1 through 7. Step 3 is highlighted. The main area displays 'Retention settings' with two sections: 'Data backup retention settings' and 'Archive Log backup retention settings'. Both sections have two options: 'Total Snapshot copies to keep' (radio button) and 'Keep Snapshot copies for' (radio button). In both cases, the 'Keep Snapshot copies for' option is selected, and the value is set to 7 days. At the bottom right, there are 'Previous' and 'Next' buttons.

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

New Oracle Database Backup Policy

1 Name

Select secondary replication options [i](#)

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Secondary policy label [i](#)

Error retry count [i](#)

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

The screenshot shows the 'New Oracle Database Backup Policy' dialog box. The 'Replication' tab is selected. Under 'Select secondary replication options', there are two checkboxes: 'Update SnapMirror after creating a local Snapshot copy.' (which is checked) and 'Update SnapVault after creating a local Snapshot copy.' Below these are two input fields: 'Secondary policy label' with a dropdown menu showing 'Hourly' and an information icon, and 'Error retry count' with a text input field containing '3' and an information icon. At the bottom right are 'Previous' and 'Next' buttons.

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

New Oracle Database Backup Policy X

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

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

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

Prescript arguments:

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

Postscript arguments:

Script timeout: 60 secs

Previous Next

7. Specify any backup verification scripts.

New Oracle Database Backup Policy X

1 Name Select the options to run backup verification

2 Backup Type Run Verifications for following backup schedules

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

4 Replication

5 Script

6 Verification Verification script commands

Script timeout 60 secs

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

Prescript arguments Choose optional arguments...

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

Postscript arguments Choose optional arguments...

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

8. Summary.

New Oracle Database Backup Policy

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

Create a full database backup policy for SQL

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

The screenshot shows the NetApp SnapCenter interface. On the left, there's a sidebar with icons for Dashboard, Resources, Monitor, Reports, Hosts, Storage Systems, Settings (which is selected), and Alerts. The main area has a header with 'NetApp SnapCenter®', 'Policies' (selected), 'Credential' (set to 'Microsoft SQL Server'), and user info ('demo@sqldba'). Below the header is a search bar and a message: 'There is no match for your search or data is not available.' To the right are buttons for 'New', 'Modify', 'Copy', 'Details', and 'Delete'.

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

New SQL Server Backup Policy

1 Name

Provide a policy name

Policy name: SQL Server Full Backup i

Details: Backup all data and log files

2 Backup Type

3 Retention

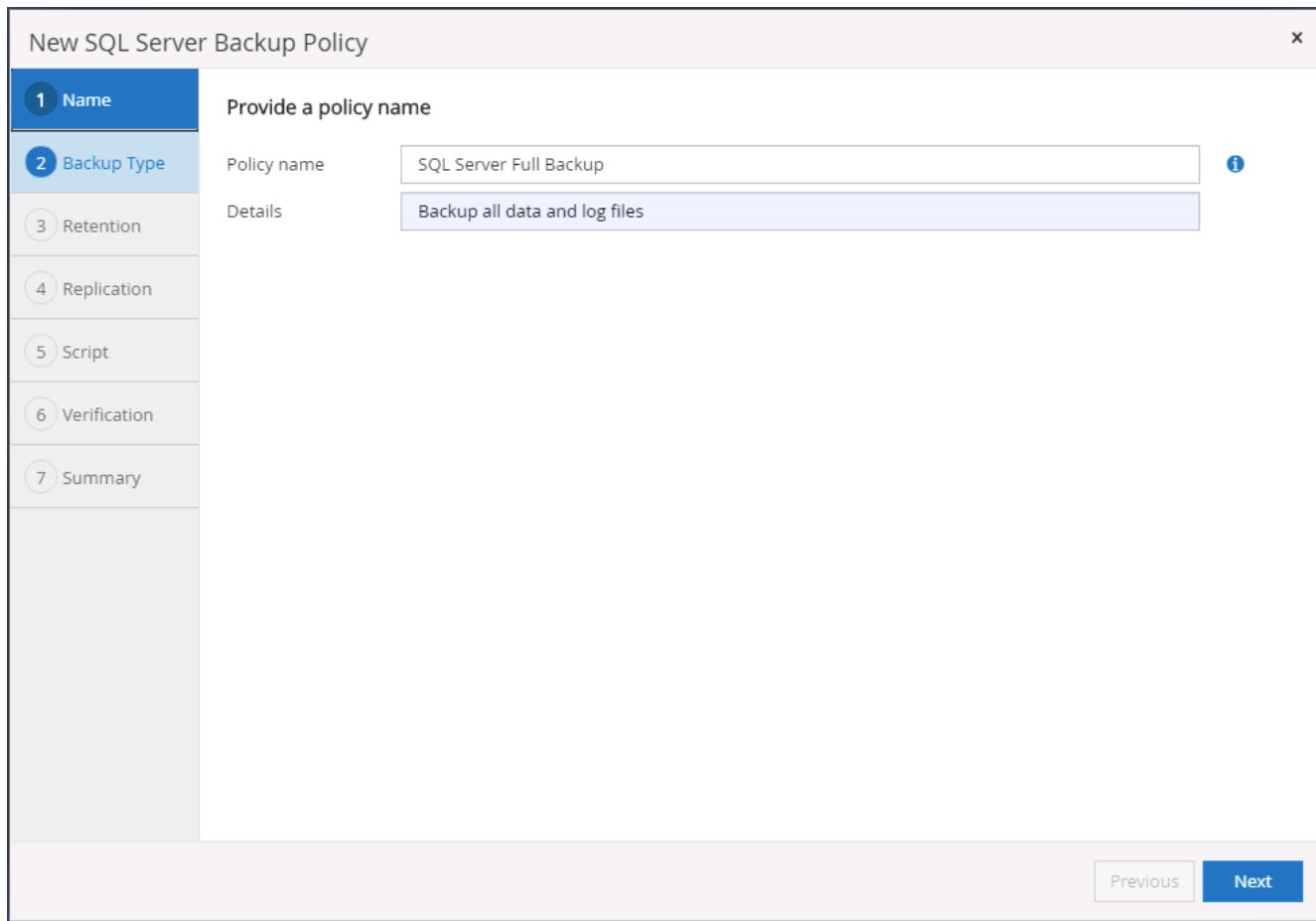
4 Replication

5 Script

6 Verification

7 Summary

Previous Next



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

New SQL Server Backup Policy X

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Select SQL server backup options

Choose backup type

Full backup and log backup

Full backup

Log backup

Copy only backup i

Maximum databases backed up per Snapshot copy: 100 i

Availability Group Settings ▼

Schedule frequency

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

On demand

Hourly

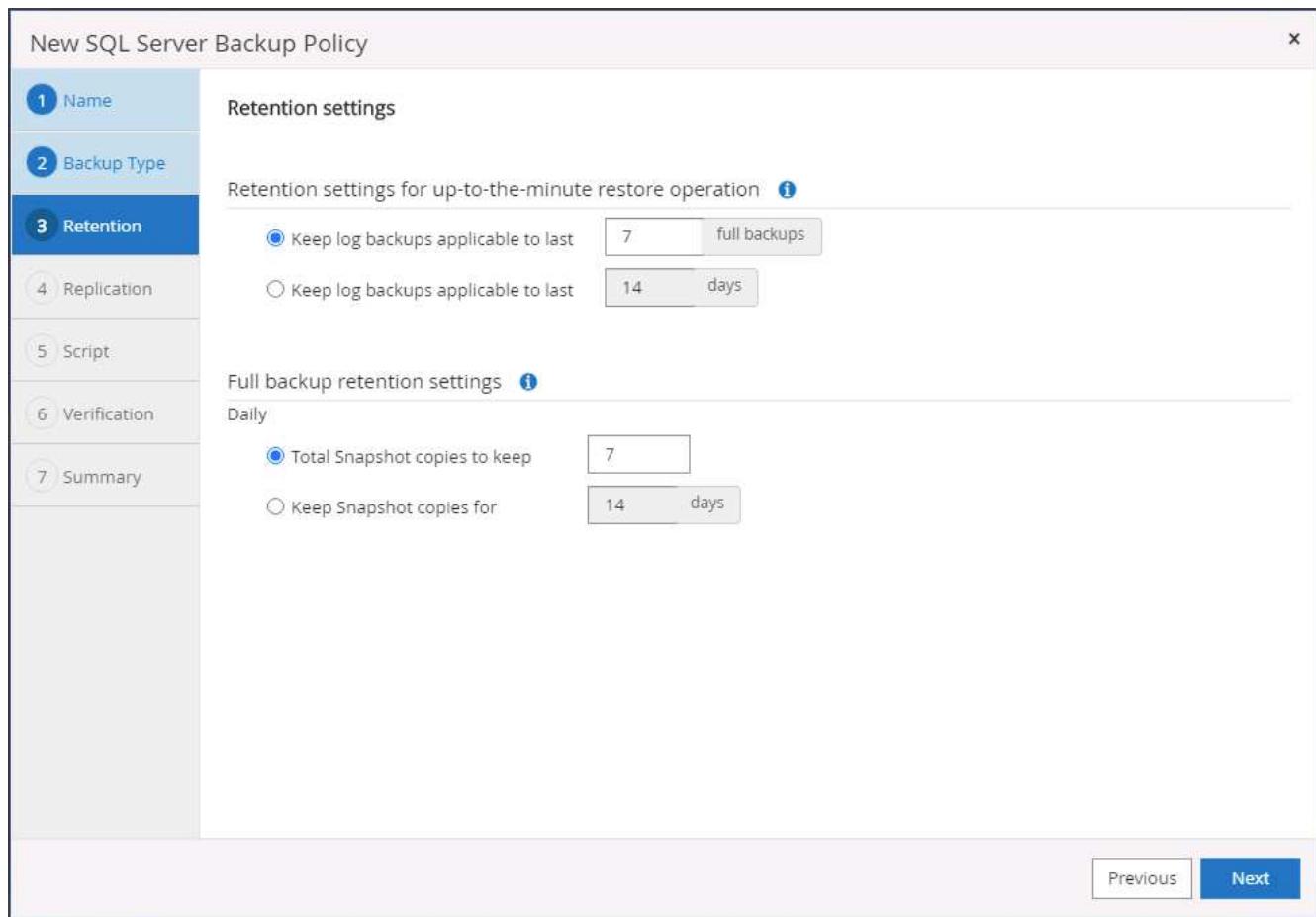
Daily

Weekly

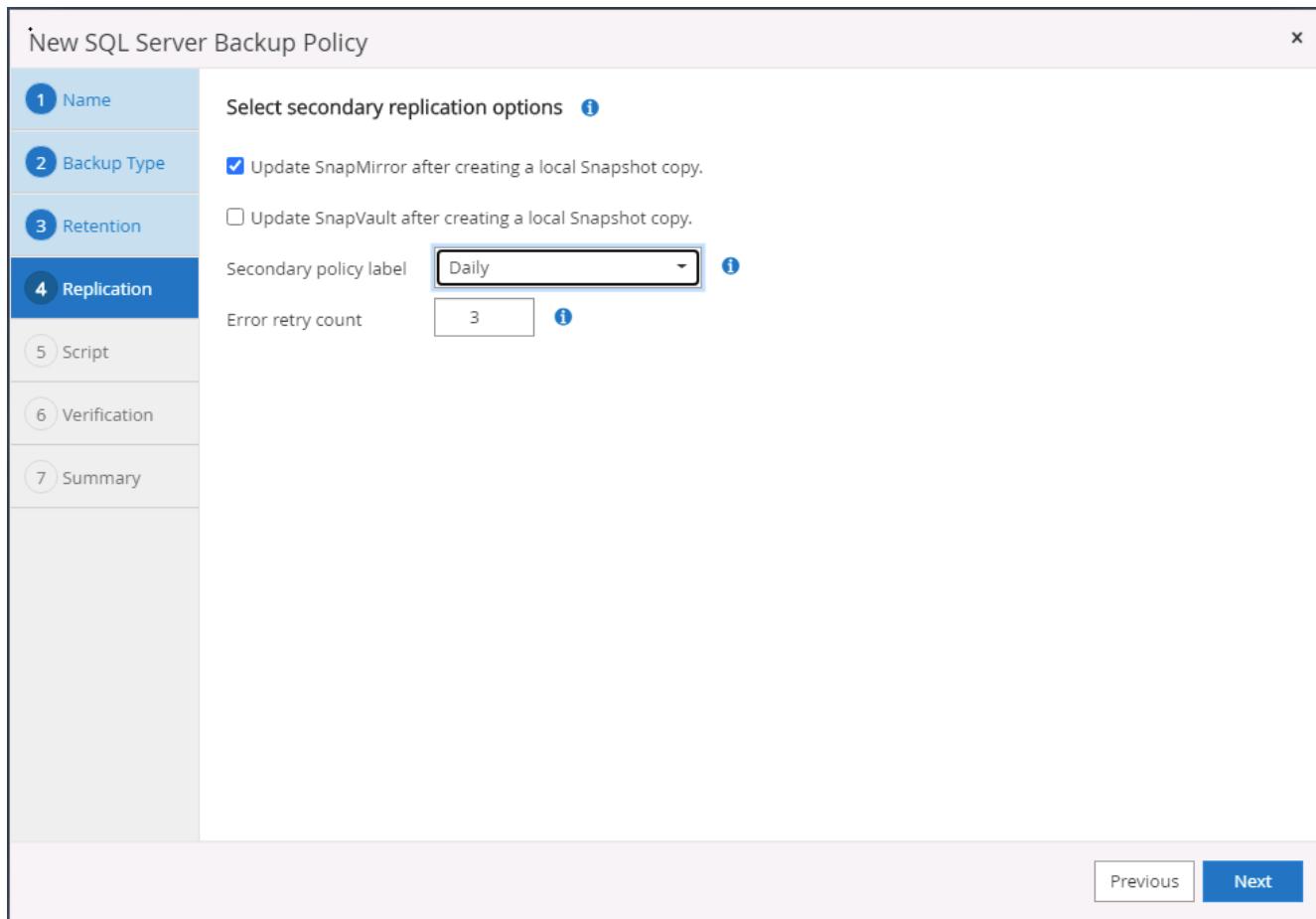
Monthly

Previous Next

4. Set the backup retention period.



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



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

New SQL Server Backup Policy X

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

2 Backup Type Prescript full path

3 Retention Prescript arguments Choose optional arguments...

4 Replication

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

6 Verification Postscript full path

7 Summary Postscript arguments Choose optional arguments...

Script timeout secs

Previous Next

7. Specify the options to run backup verification.

New SQL Server Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Select the options to run backup verification

Run verifications for the following backup schedules

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

Daily

Database consistency checks options

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

Suppress all information message (NO_INFOMSGS)

Display all reported error messages per object (ALL_ERRORMSGGS)

Do not check non-clustered indexes (NOINDEX)

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

Log backup

Verify log backup. i

Verification script settings

Script timeout secs

Previous **Next**

8. Summary.

New SQL Server Backup Policy X

1 Name	Summary
2 Backup Type	Policy name: SQL Server Full Backup
3 Retention	Details: Backup all data and log files
4 Replication	Backup type: Full backup and log backup
5 Script	Availability group settings: Backup only on preferred backup replica
6 Verification	Schedule Type: Daily 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
7 Summary	Backup prescript settings: undefined Prescript arguments: Backup postscript settings: undefined Postscript arguments: Verification for backup schedule type: none Verification prescript settings: undefined Prescript arguments: Verification postscript settings: undefined Postscript arguments:
Previous Finish	

Create a database log backup policy for SQL.

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

New SQL Server Backup Policy

1 Name

Provide a policy name

Policy name: SQL Server Log Backup

Details: Backup SQL server log

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Previous Next

The screenshot shows the 'New SQL Server Backup Policy' wizard. The 'Name' step is active. The 'Policy name' is set to 'SQL Server Log Backup'. The 'Details' field contains 'Backup SQL server log'. The 'Next' button is visible at the bottom right.

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

New SQL Server Backup Policy X

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Select SQL server backup options

Choose backup type

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

Maximum databases backed up per Snapshot copy: 100 i

Availability Group Settings ▼

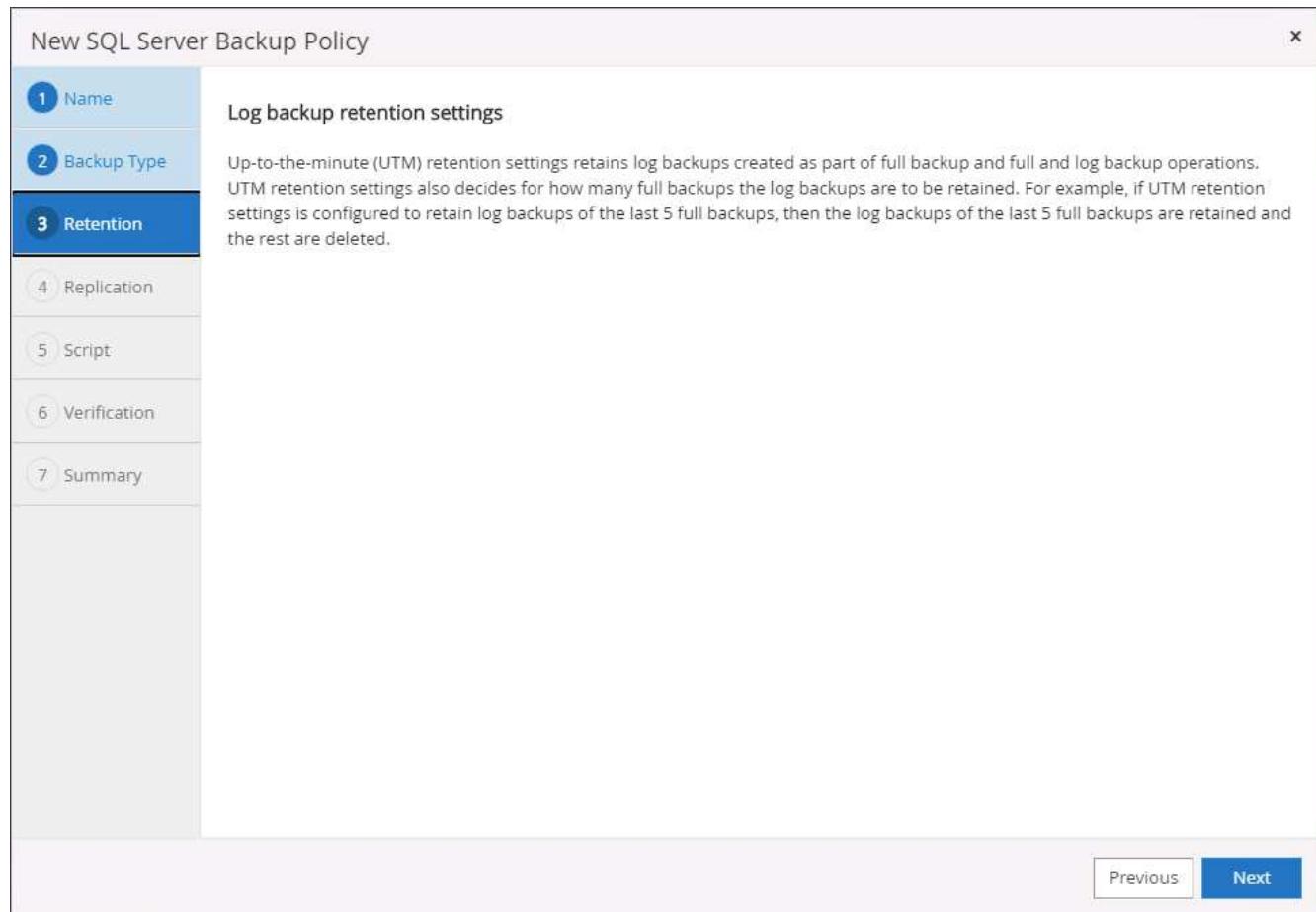
Schedule frequency

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

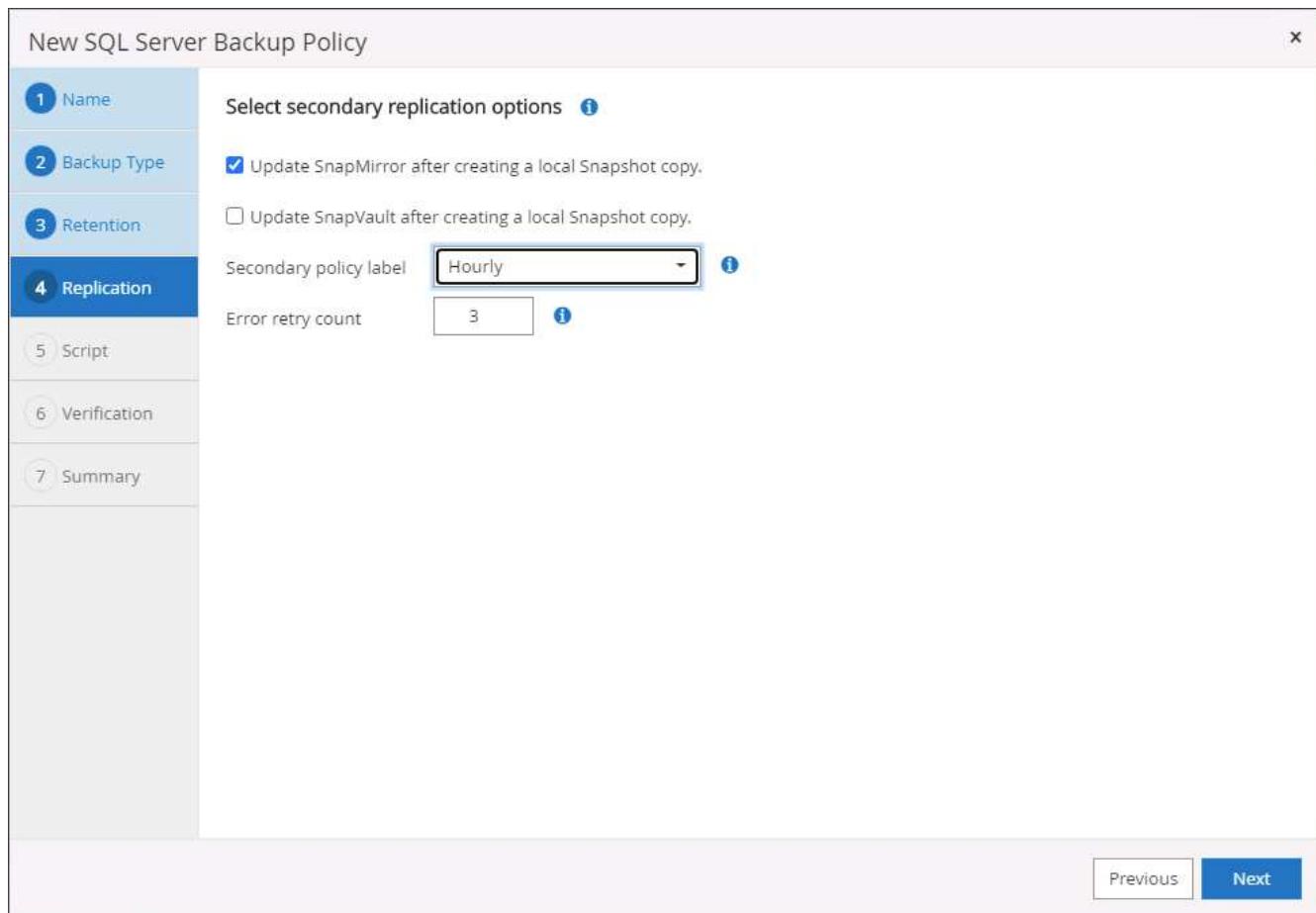
On demand
 Hourly
 Daily
 Weekly
 Monthly

Previous Next

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



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



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

New SQL Server Backup Policy X

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

2 Backup Type Prescript full path

3 Retention Prescript arguments Choose optional arguments...

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

5 Script Postscript full path

Postscript arguments Choose optional arguments...

Script timeout 60 secs

6 Verification

7 Summary

Previous Next

6. Summary.

New SQL Server Backup Policy

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

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

8. Implement backup policy to protect database

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

Create a resource group for full backup of Oracle

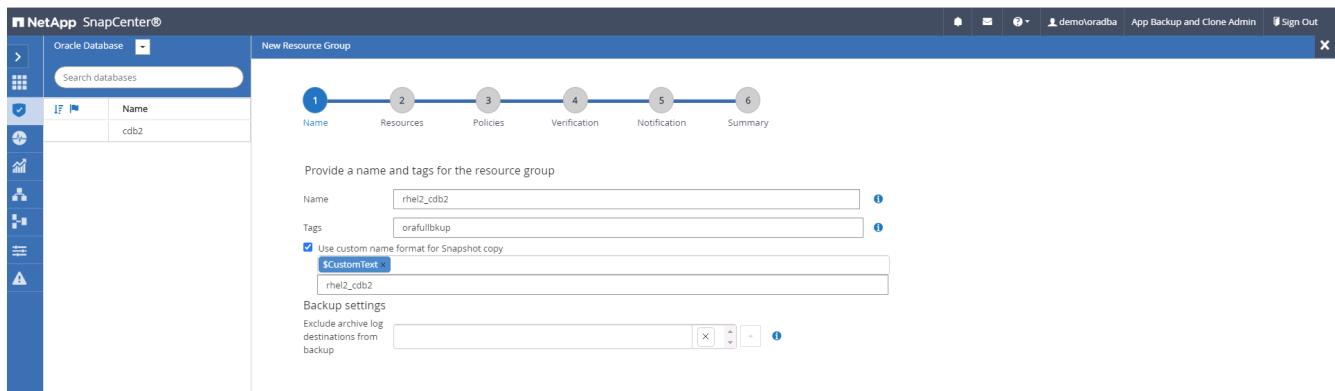
1. Log into SnapCenter with a database management user ID, and navigate to the Resources tab. In the View drop-down list, choose either Database or Resource Group to launch the resource group creation workflow.

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

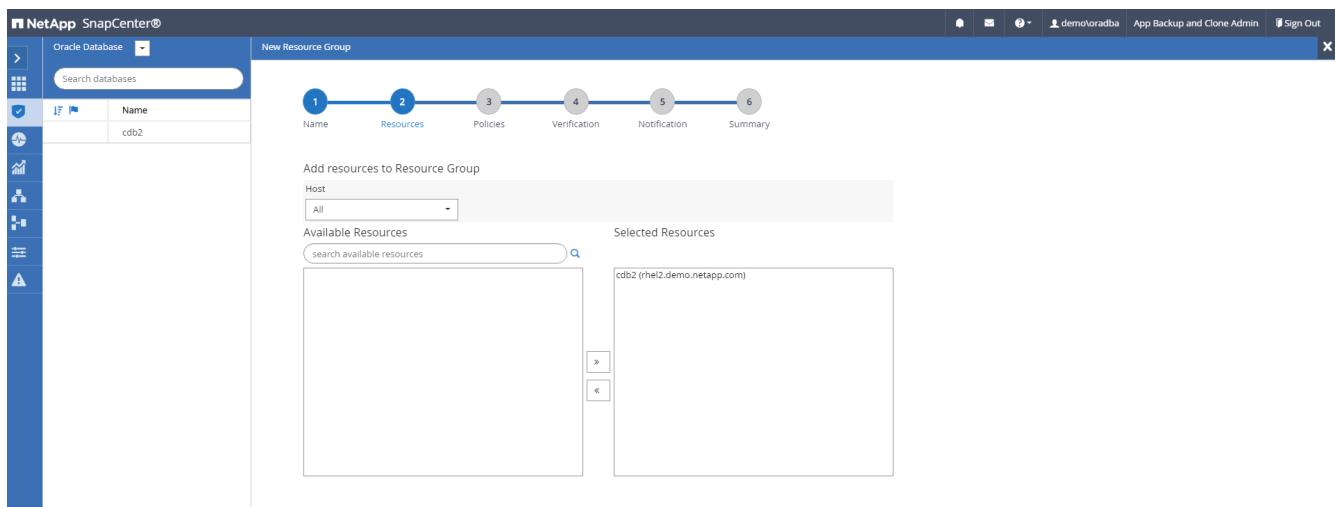
Name	Oracle Database Type	Host/Cluster	Resource Group	Policies	Last Backup	Overall Status
cdb2	Single Instance (Multitenant)	rhel2.demo.netapp.com				Not protected

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

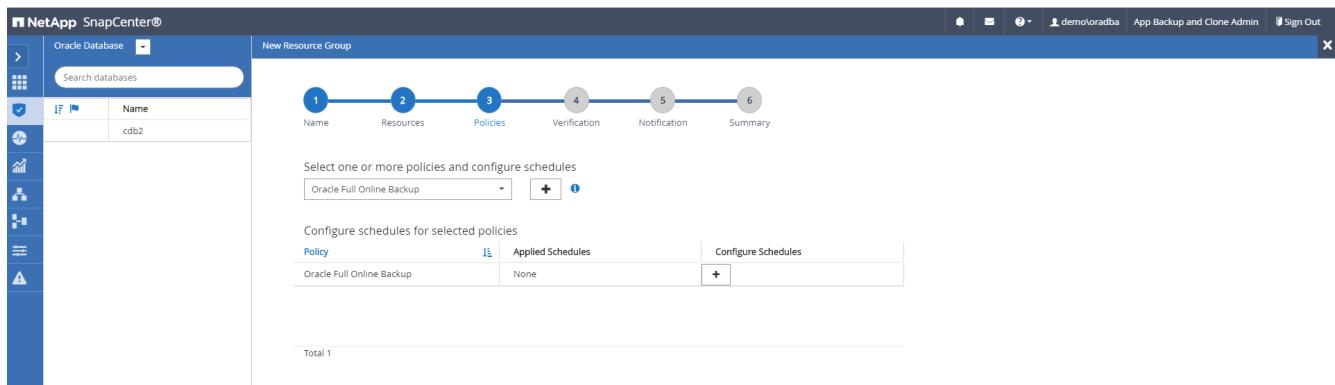
2. Provide a name and tags for the resource group. You can define a naming format for the Snapshot copy and bypass the redundant archive log destination if configured.



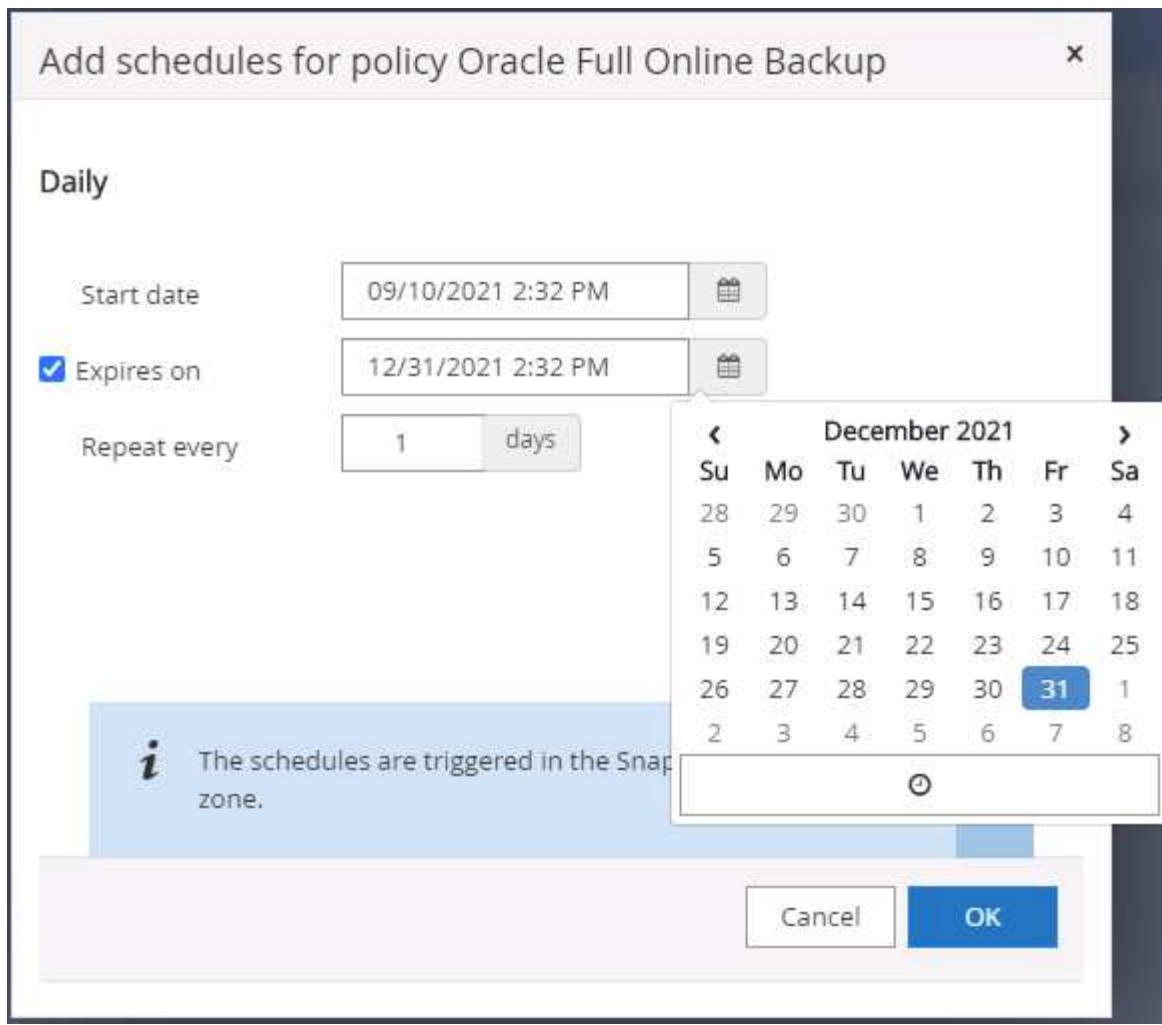
3. Add database resources to the resource group.



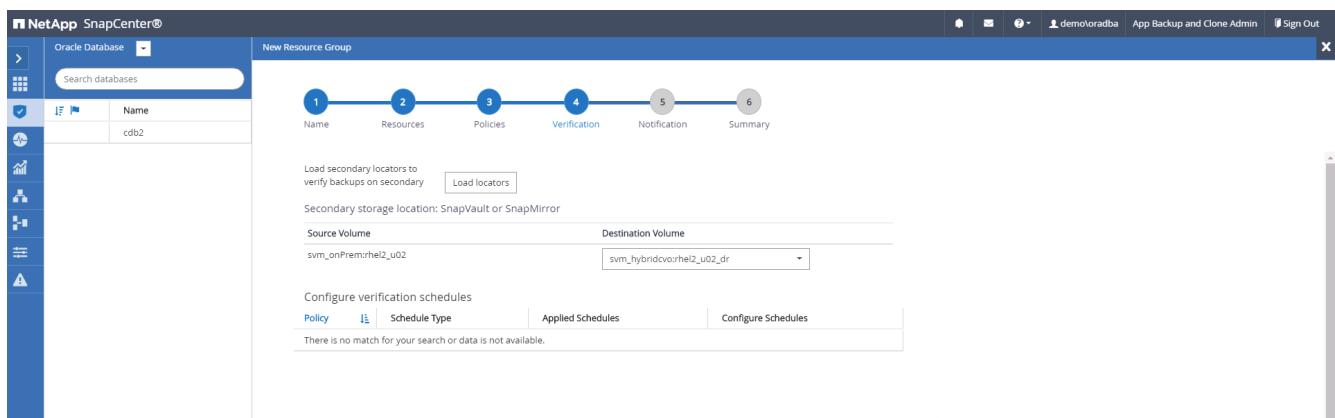
4. Select a full backup policy created in section 7 from the drop-down list.



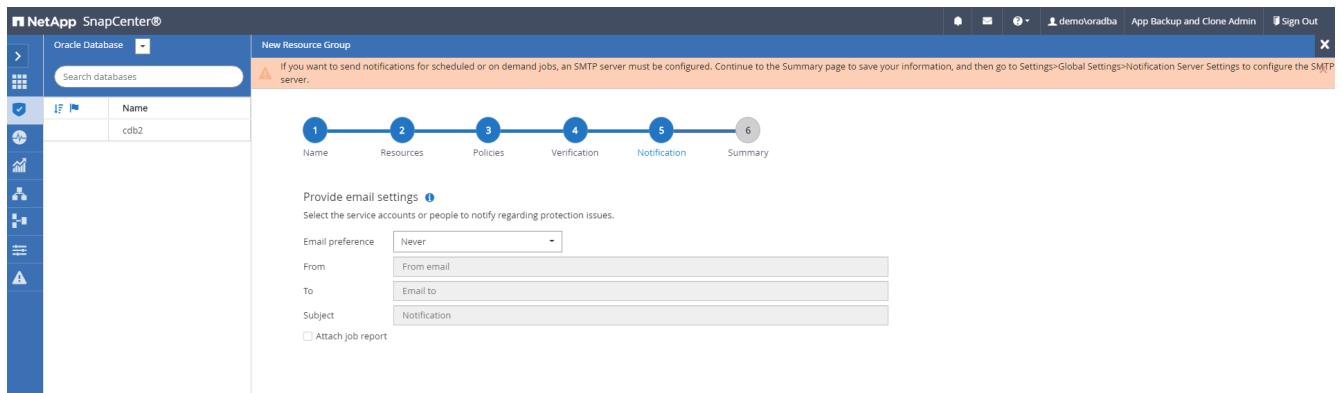
5. Click the (+) sign to configure the desired backup schedule.



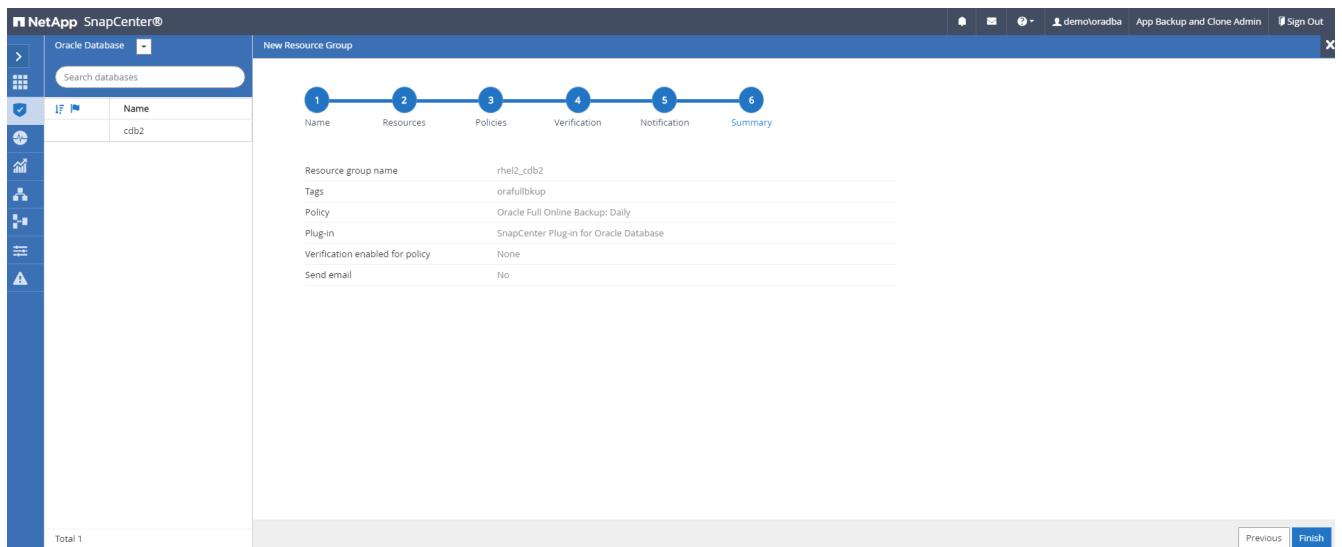
6. Click Load Locators to load the source and destination volume.



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

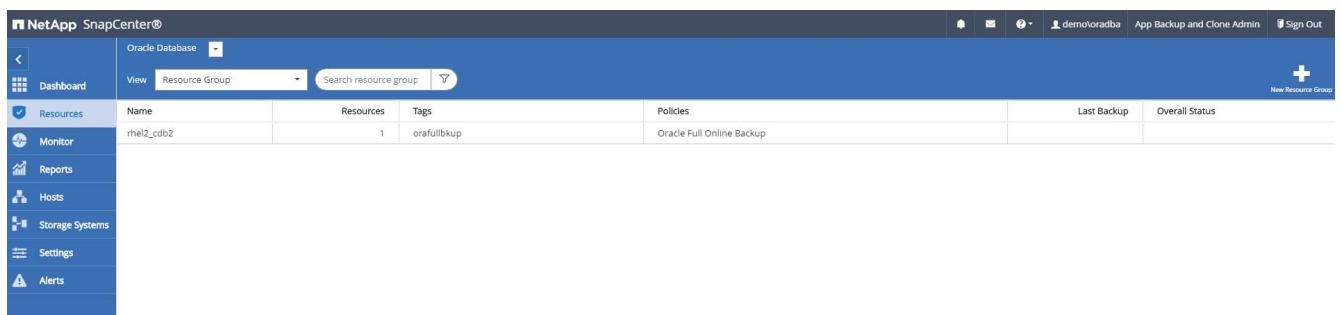


8. Summary.

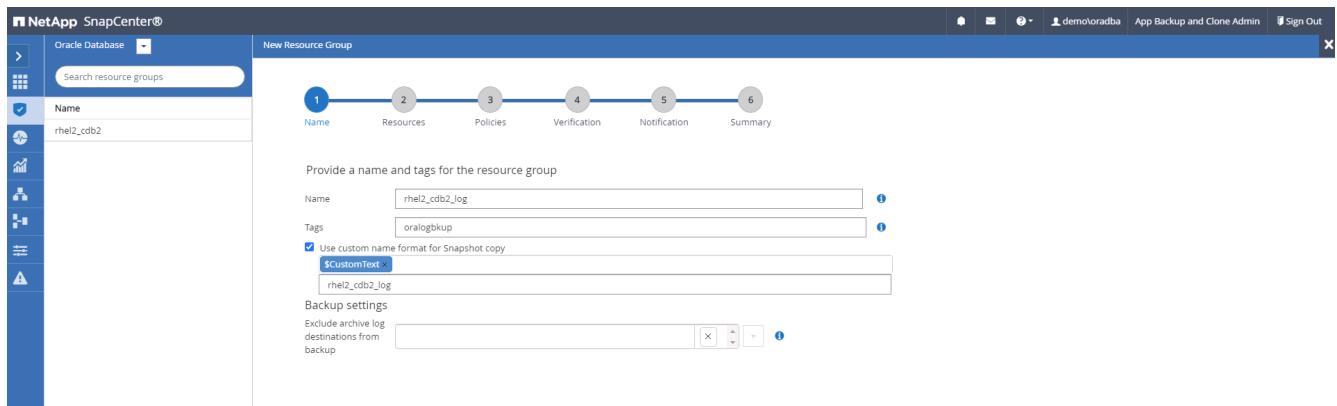


Create a resource group for log backup of Oracle

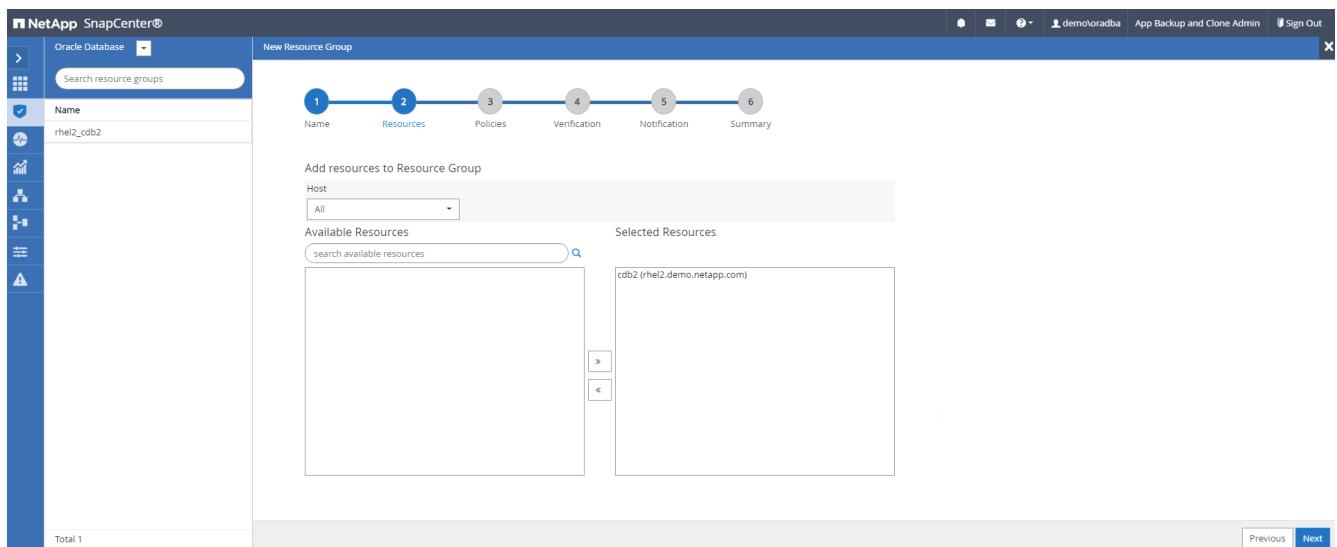
1. Log into SnapCenter with a database management user ID, and navigate to the Resources tab. In the View drop-down list, choose either Database or Resource Group to launch the resource group creation workflow.



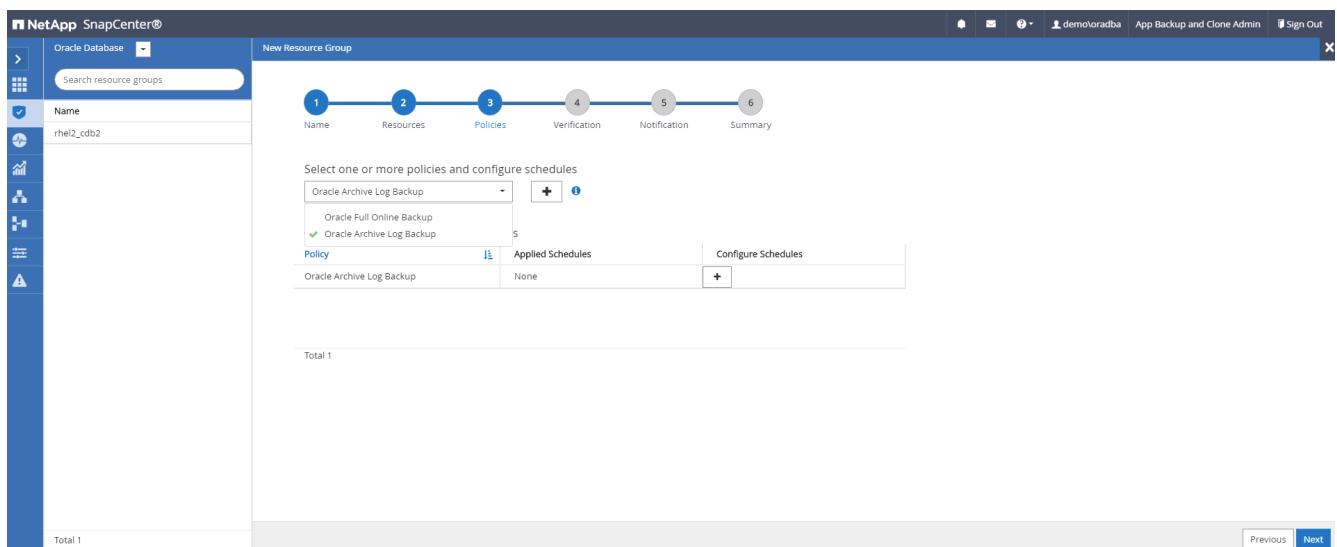
2. Provide a name and tags for the resource group. You can define a naming format for the Snapshot copy and bypass the redundant archive log destination if configured.



3. Add database resources to the resource group.



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



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

Add schedules for policy Oracle Archive Log Backup x

Hourly

Start date

Expires on

Repeat every hours mins

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

Cancel OK

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

NetApp SnapCenter®

Oracle Database

New Resource Group

Name

Search resource groups

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

Configure verification schedules

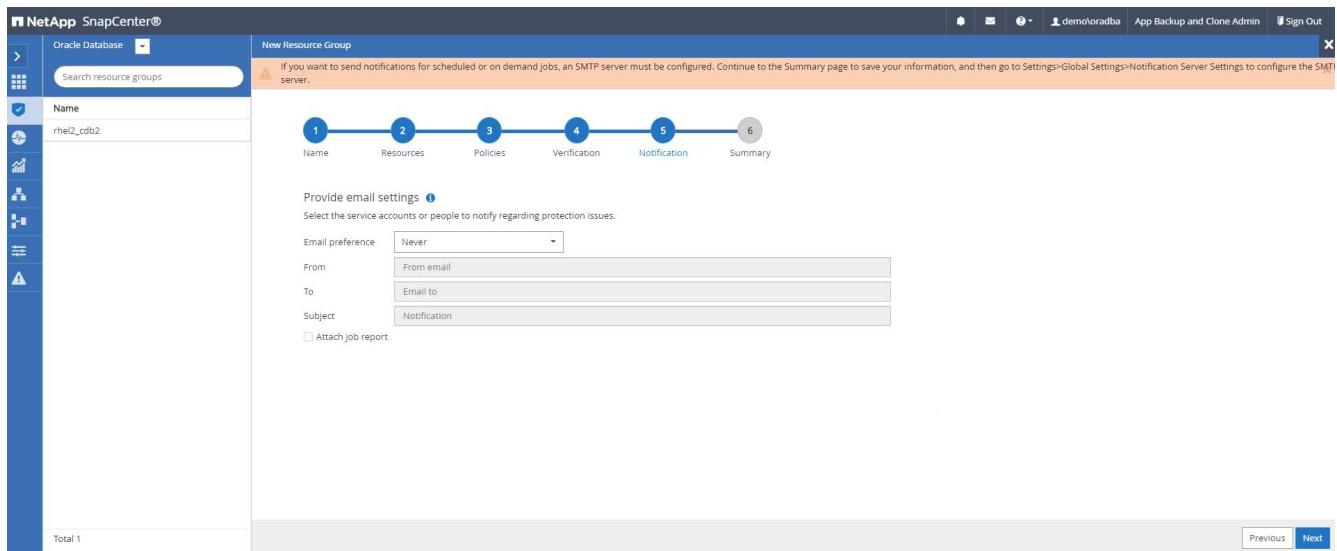
Policy Schedule Type Applied Schedules Configure Schedules

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

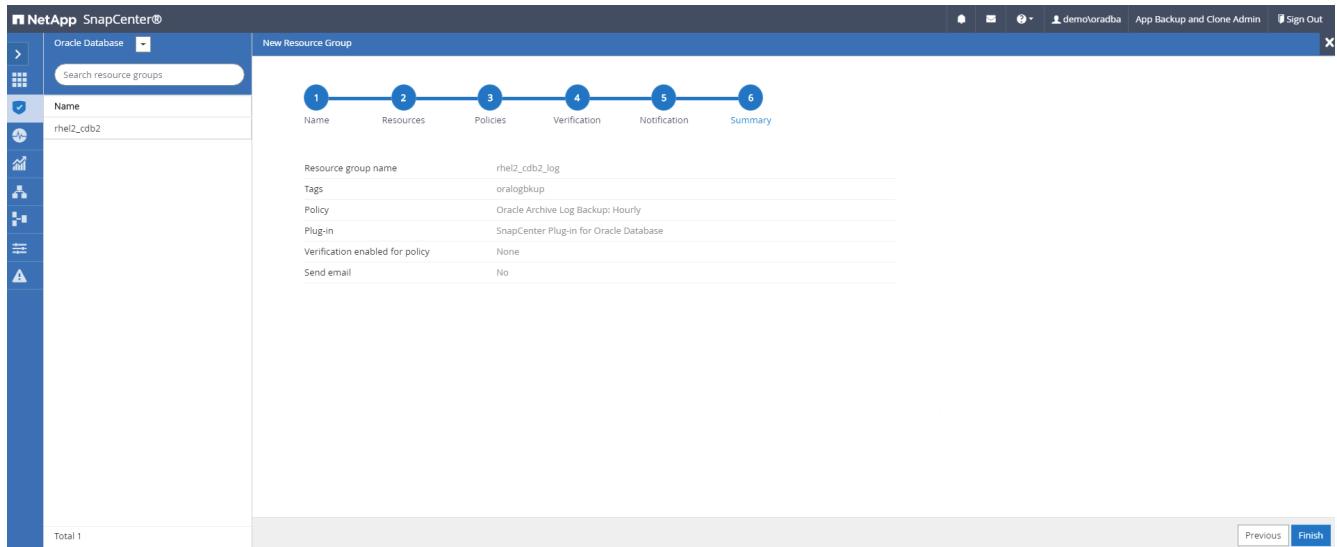
Total 0

Previous Next

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

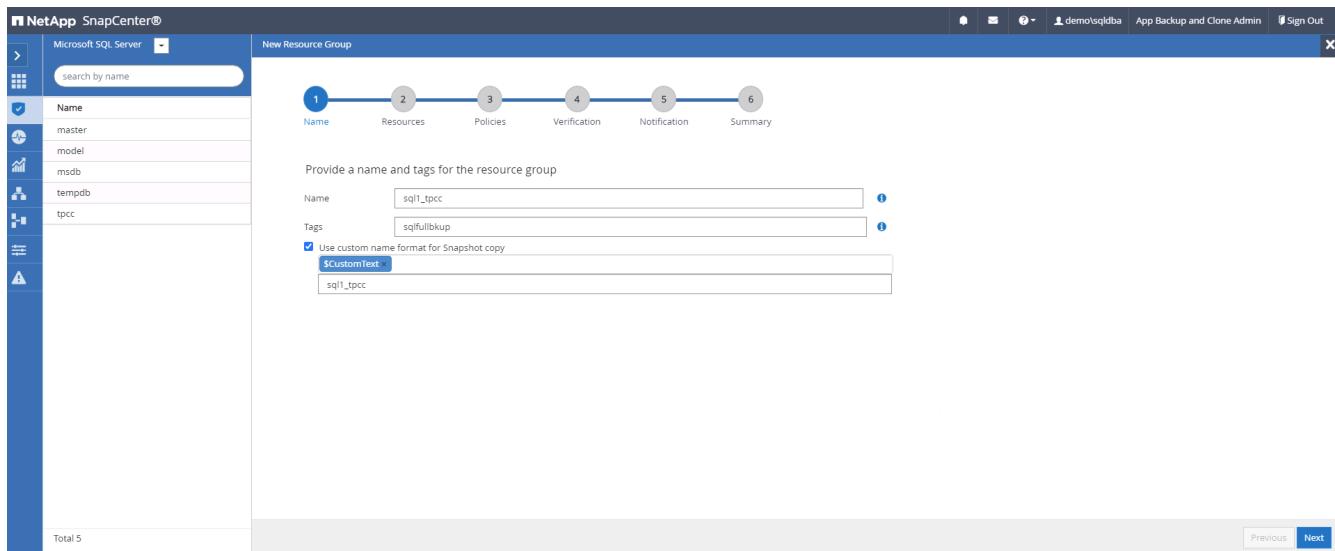


8. Summary.

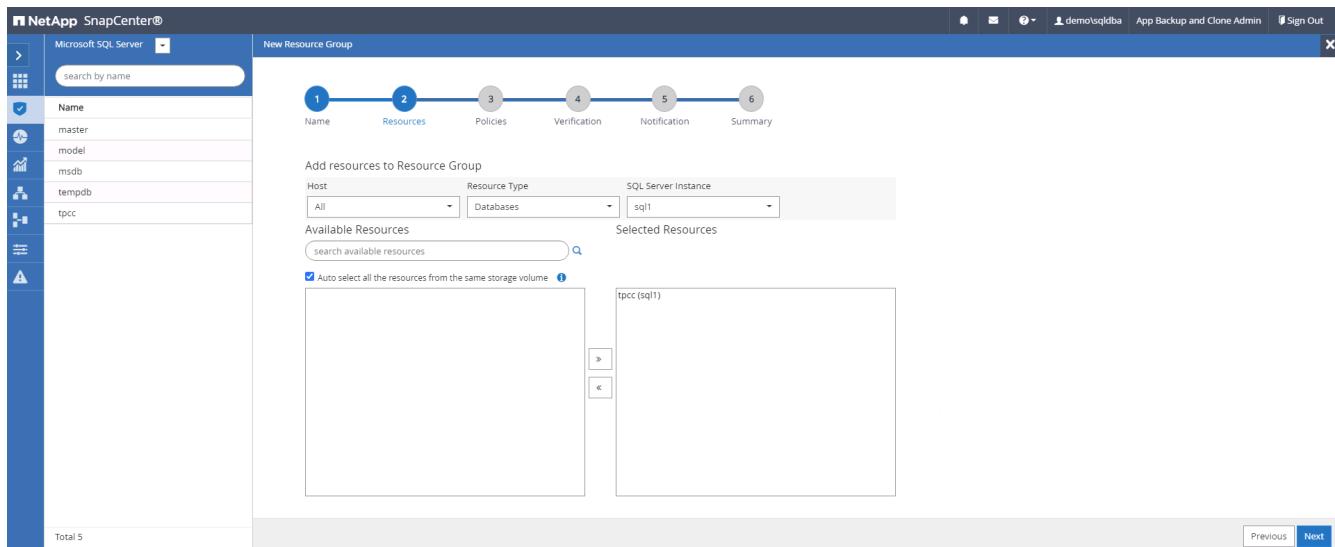


Create a resource group for full backup of SQL Server

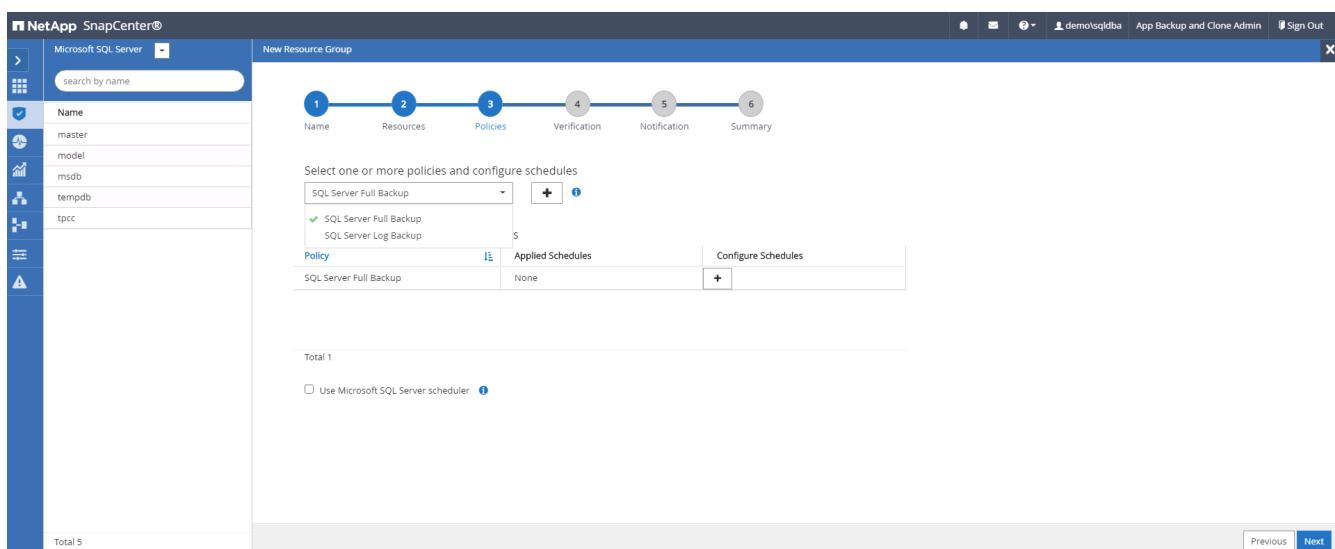
1. Log into SnapCenter with a database management user ID, and navigate to the Resources tab. In the View drop-down list, choose either a Database or Resource Group to launch the resource group creation workflow. Provide a name and tags for the resource group. You can define a naming format for the Snapshot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



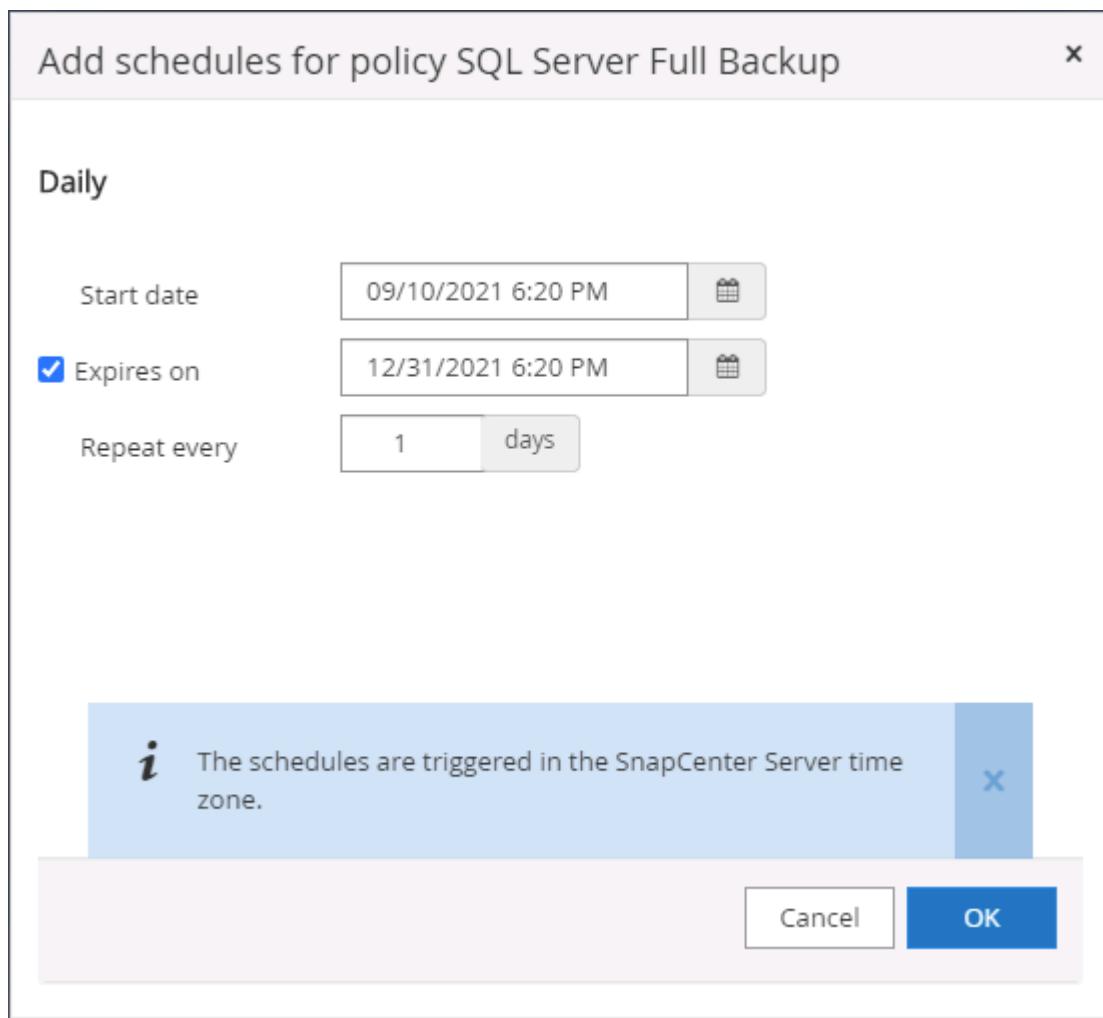
2. Select the database resources to be backed up.



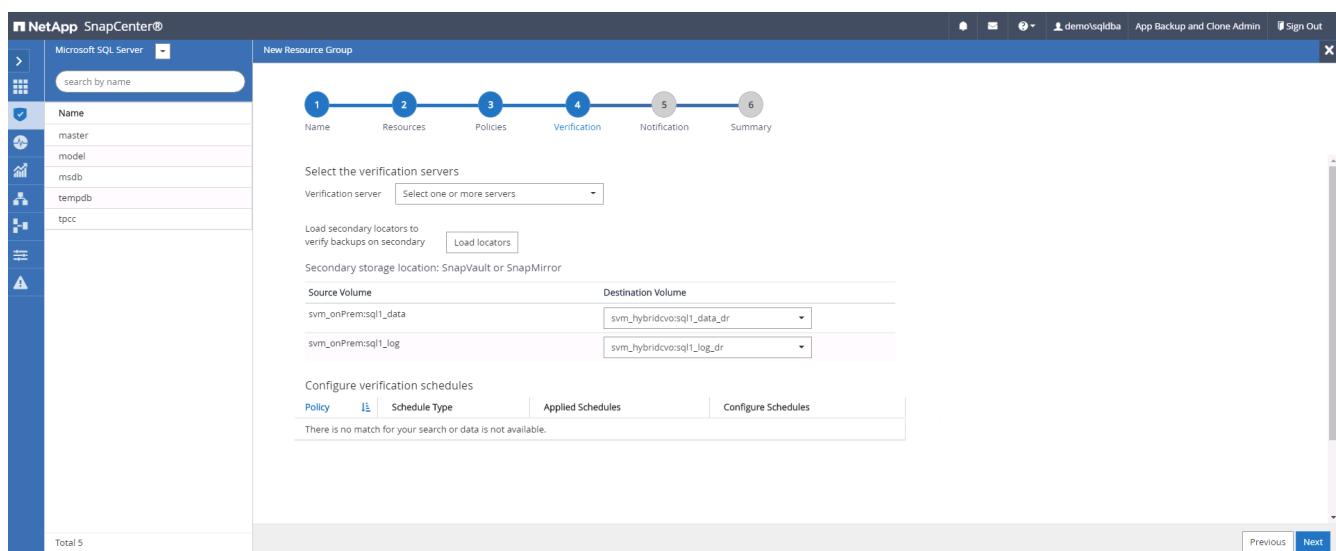
3. Select a full SQL backup policy created in section 7.



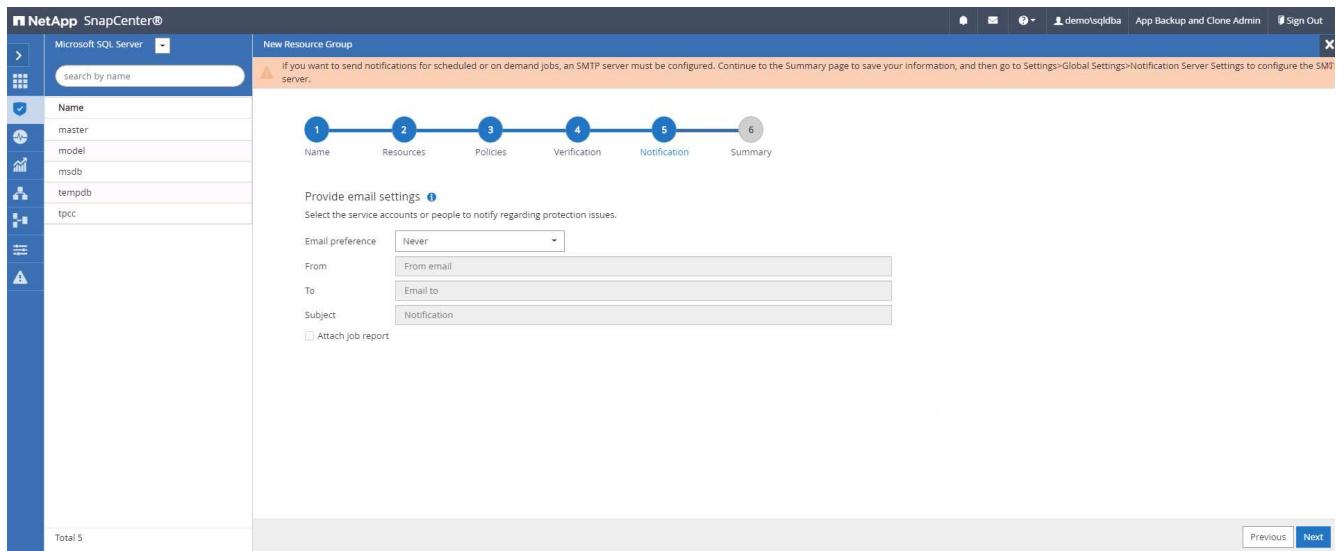
- Add exact timing for backups as well as the frequency.



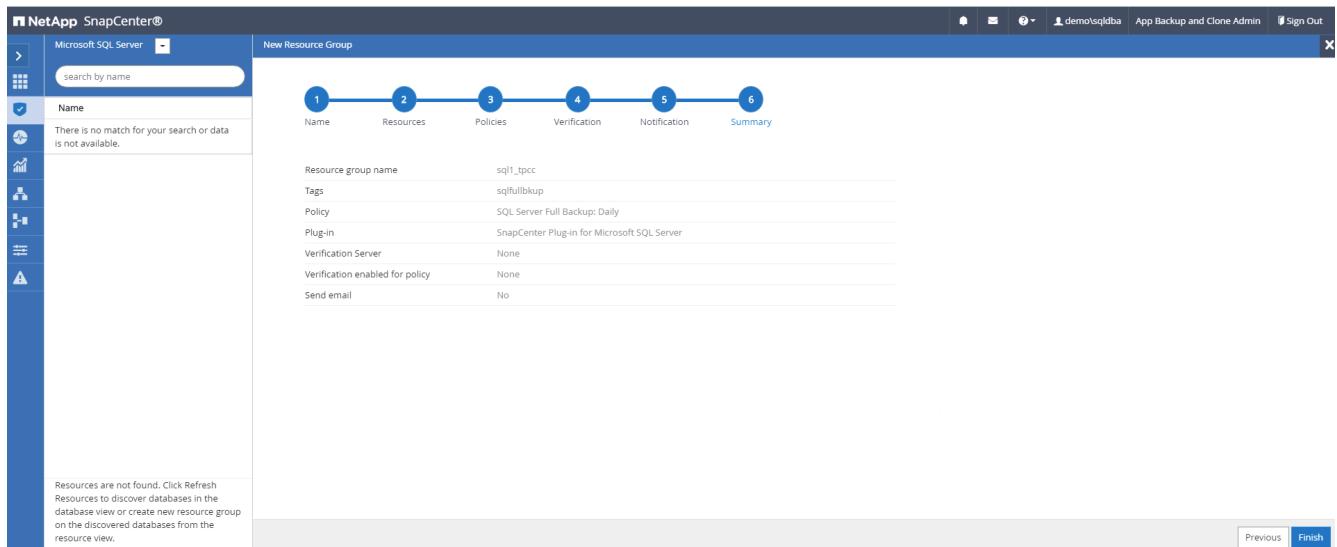
- Choose the verification server for the backup on secondary if backup verification is to be performed. Click Load Locator to populate the secondary storage location.



- Configure the SMTP server for email notification if desired.

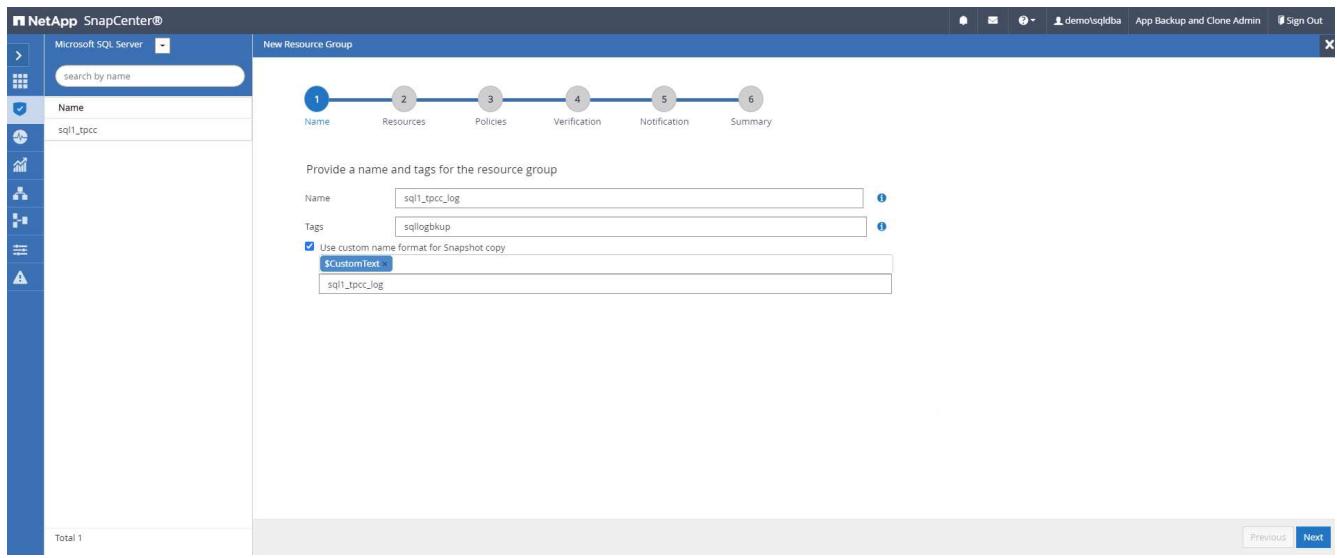


7. Summary.

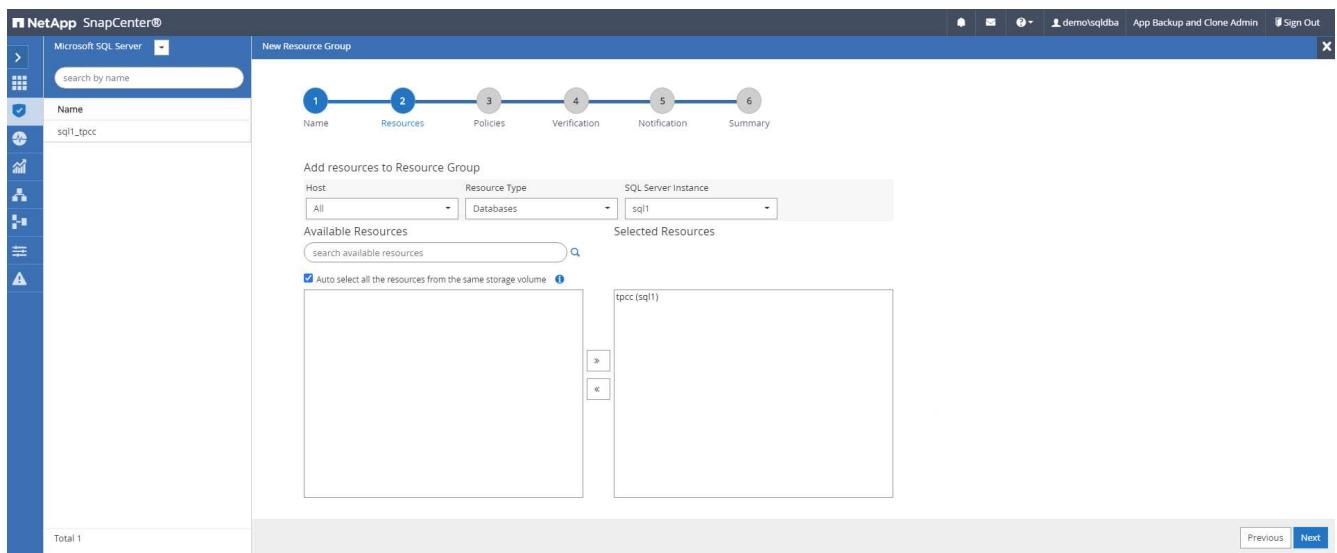


Create a resource group for log backup of SQL Server

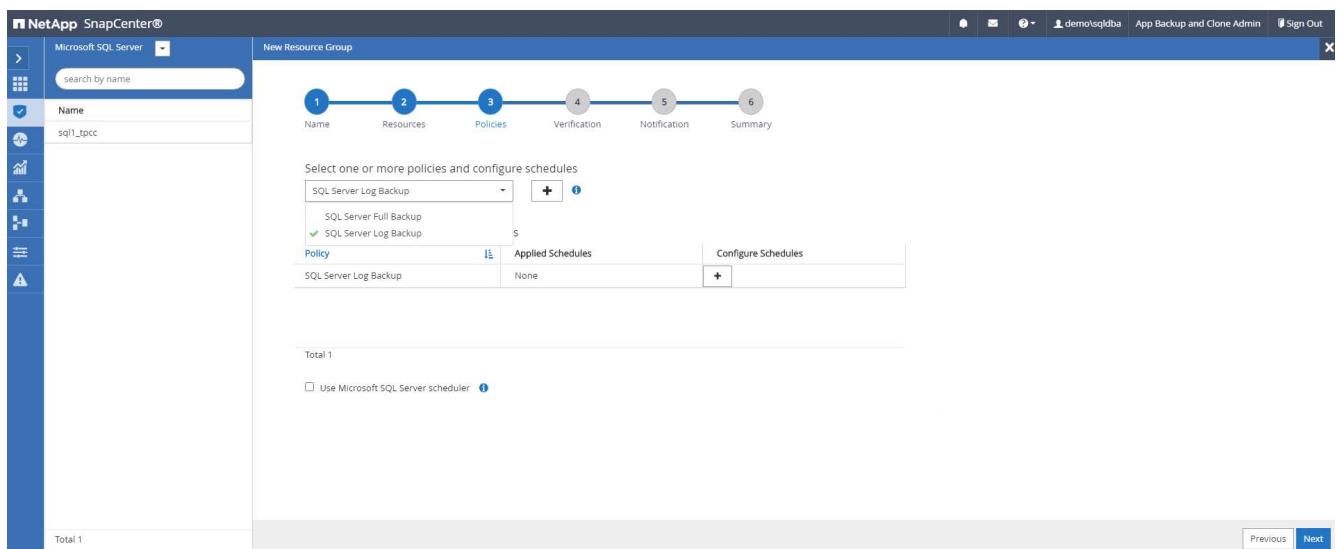
1. Log into SnapCenter with a database management user ID, and navigate to the Resources tab. In the View drop-down list, choose either a Database or Resource Group to launch the resource group creation workflow. Provide the name and tags for the resource group. You can define a naming format for the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



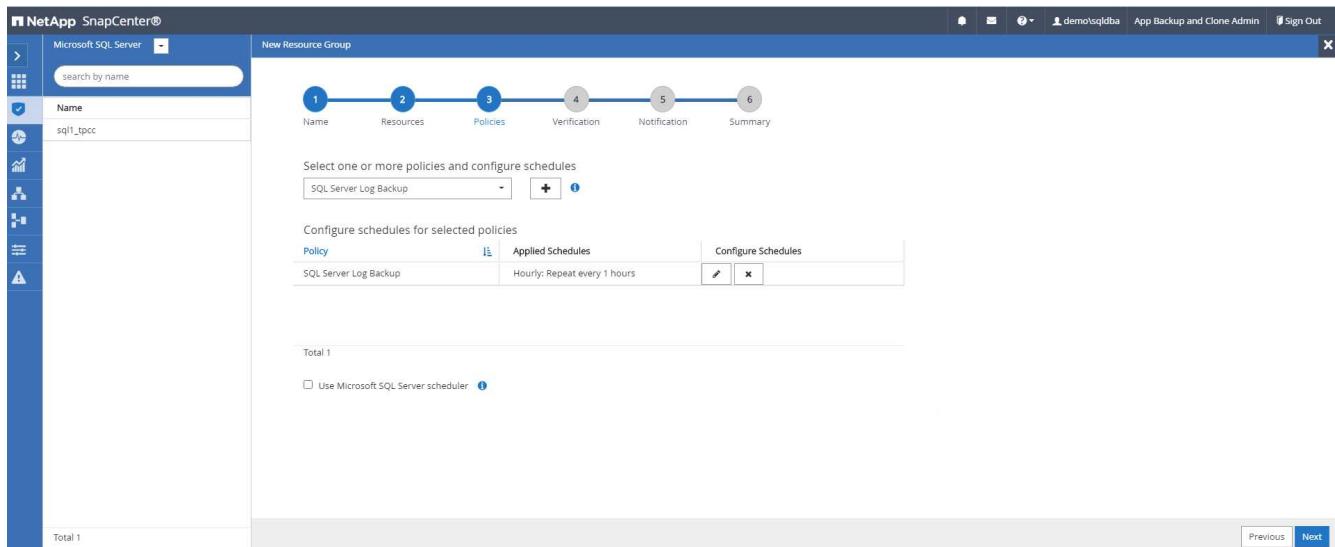
2. Select the database resources to be backed up.



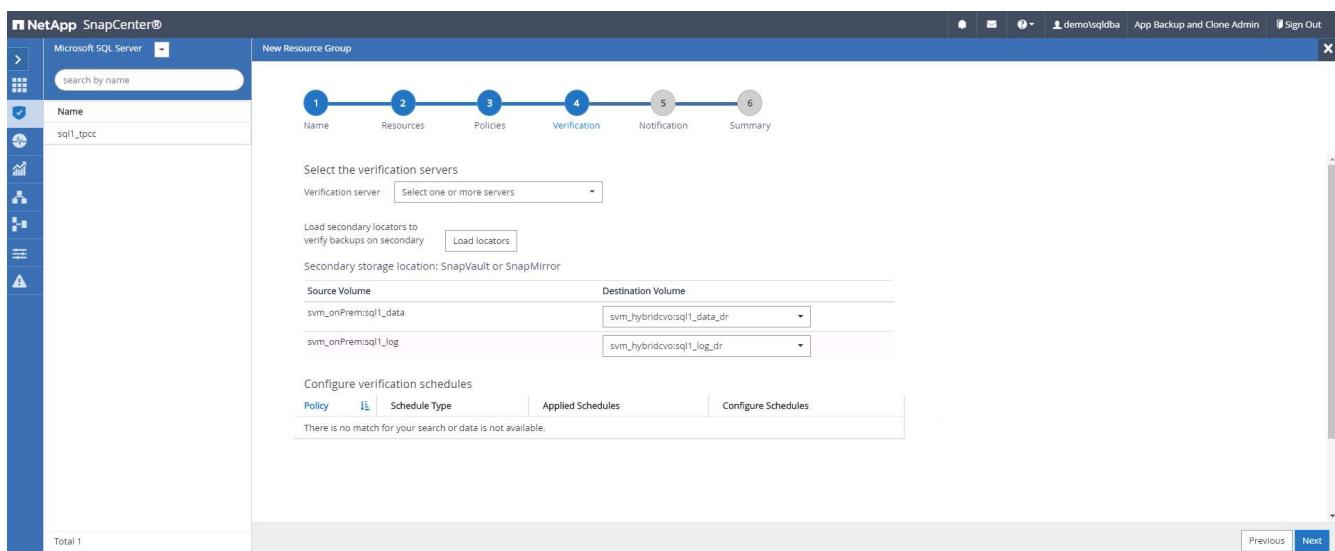
3. Select a SQL log backup policy created in section 7.



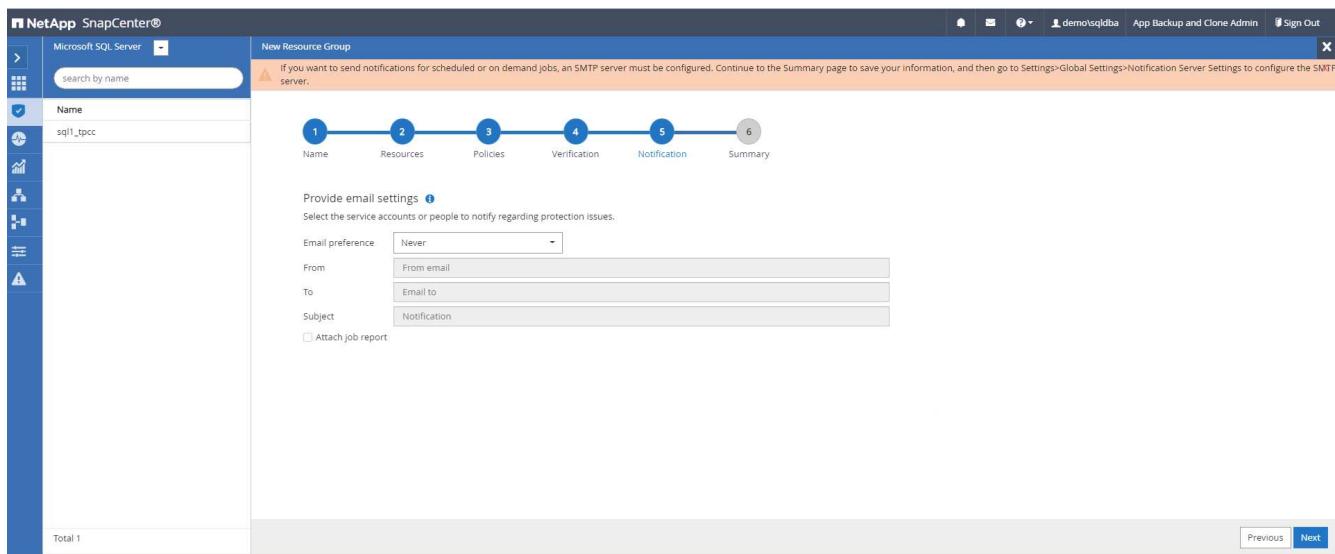
4. Add exact timing for the backup as well as the frequency.



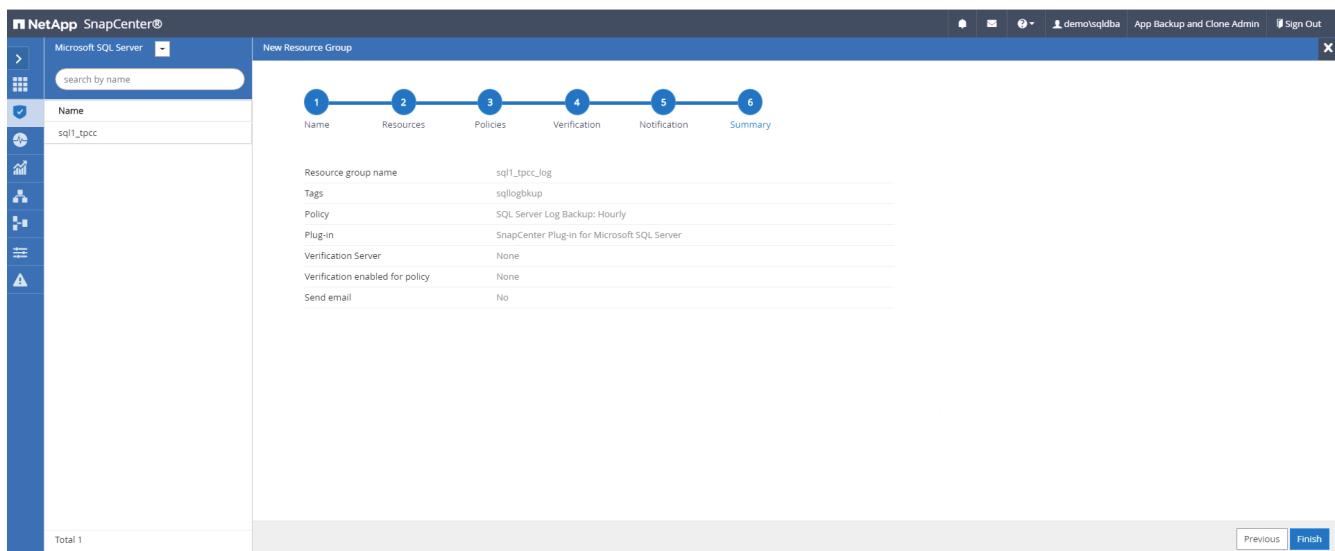
5. Choose the verification server for the backup on secondary if backup verification is to be performed. Click the Load Locator to populate the secondary storage location.



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



7. Summary.



9. Validate backup

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

Jobs						
	Jobs	Schedules	Events	Logs		
	Dashboard	<input type="text" value="search by name"/>				
	Resources	Jobs - Filter				
	ID	Status	Name		Start date	End date
	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
	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
	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
	521		Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Full Backup'		09/14/2021 6:25:01 PM	09/14/2021 6:27:14 PM
	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
	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
	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
	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

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

public cloud.

The screenshot shows the NetApp SnapCenter interface for Oracle Database management. On the left, a sidebar lists databases: cdb2, cdb2dev, cdb2dr, cdb2dr2, and cdb2test. The main panel displays the 'cdb2 Topology' section, which includes a 'Manage Copies' section showing 'Local copies' (197 Backups, 0 Clones) and 'Mirror copies' (197 Backups, 3 Clones). To the right is a 'Summary Card' showing statistics: 394 Backups, 28 Data Backups, 366 Log Backups, and 3 Clones. Below these sections is a table titled 'Primary Backup(s)' listing five backup entries with columns for Backup Name, Count, Type, End Date, Verified, Mounted, RMAN Cataloged, and SCN.

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

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

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

Getting Started with AWS public cloud

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

AWS public cloud



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

1. Pre-flight check

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

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

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



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

Deploy the Cloud Manager connector

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



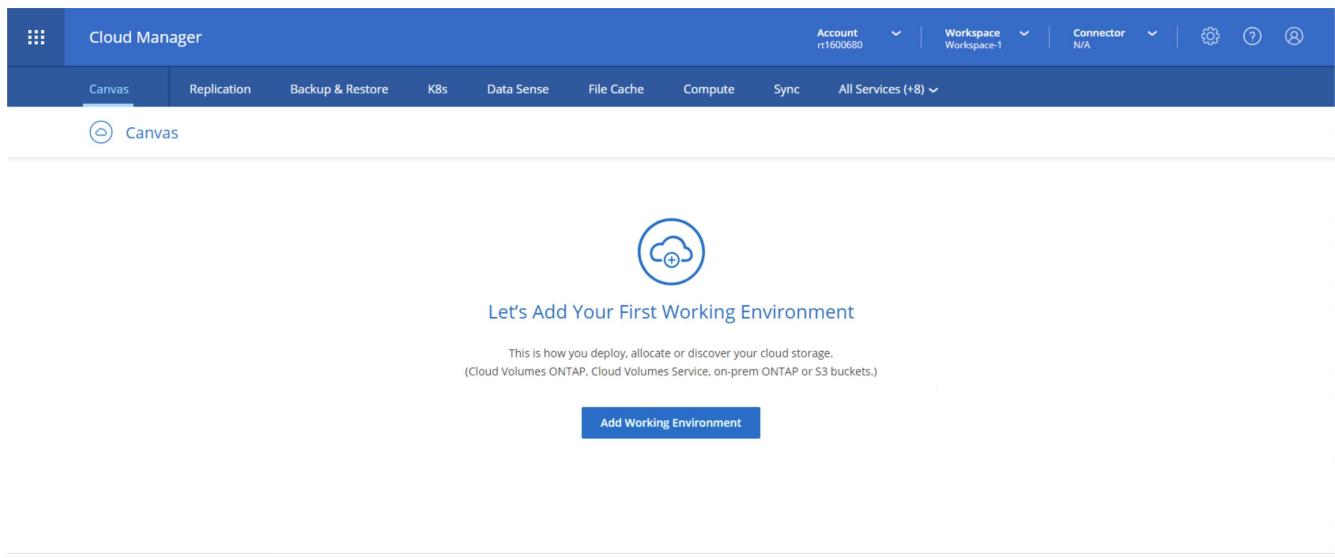
[Continue to Cloud Manager](#)

Log In to NetApp Cloud Central

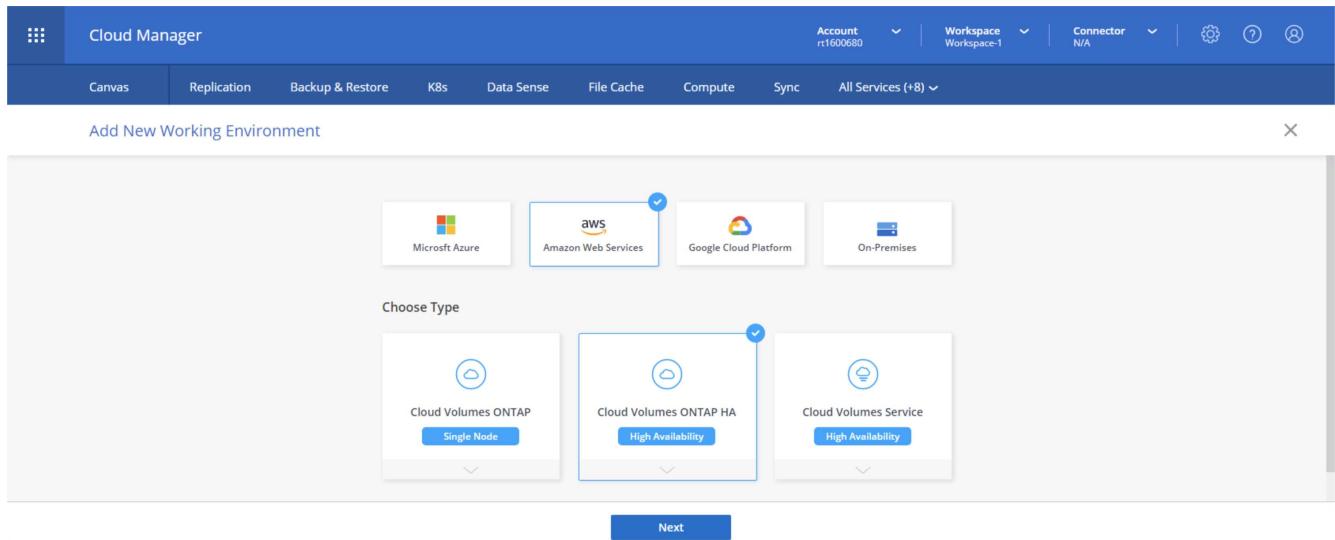
Don't have an account yet? [Sign Up](#)

[Forgot your password?](#)

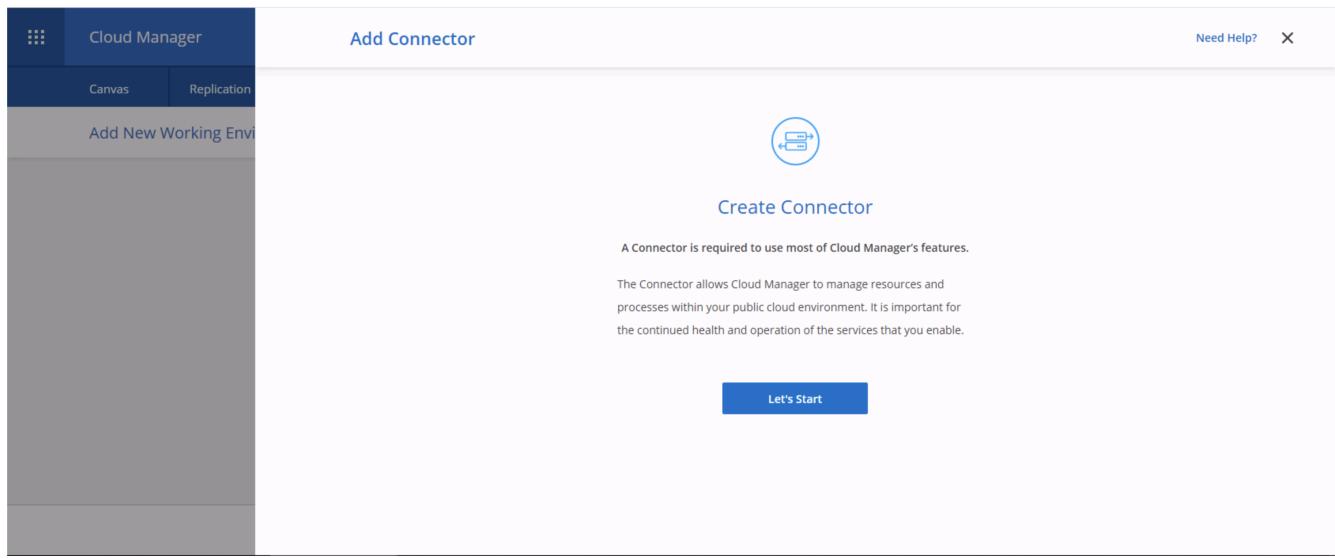
2. After you log in, you should be taken to the Canvas.



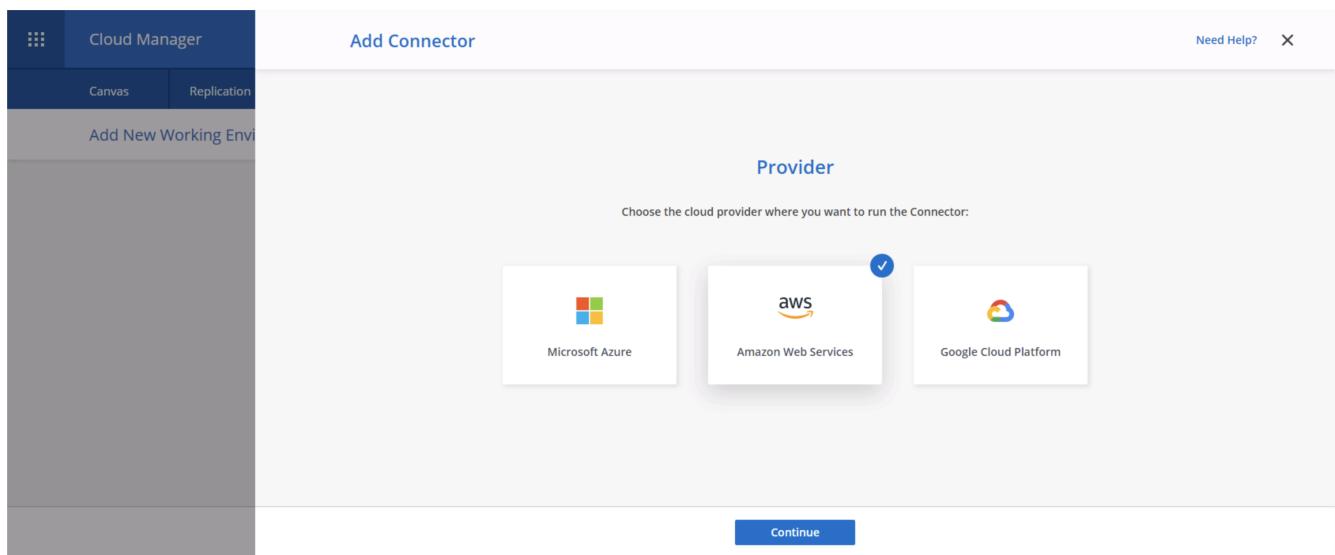
3. Click "Add Working Environment" and choose Cloud Volumes ONTAP in AWS. Here, you also choose whether you want to deploy a single node system or a high availability pair. I have chosen to deploy a high availability pair.



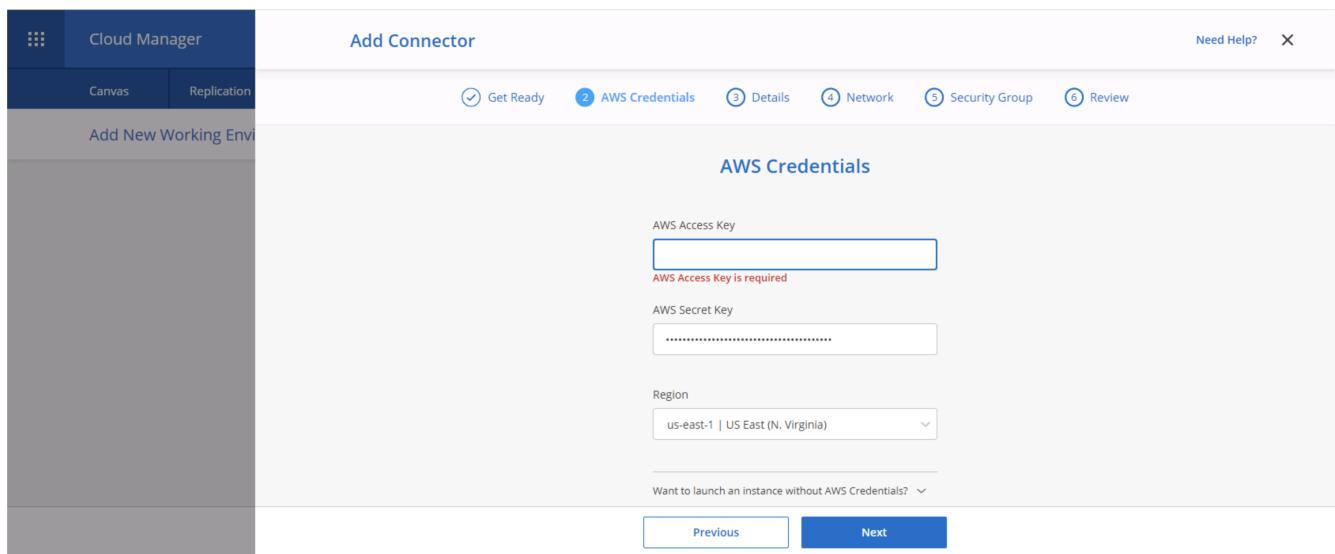
4. If no connector has been created, a pop-up appears asking you to create a connector.



5. Click Lets Start, and then choose AWS.



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



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

Cloud Manager

Add Connector

Get Ready AWS Credentials Details Network Security Group Review

Connector Instance Name: awscloudmanager

Connector Role:

- Create Role
- Select an existing Role

Role Name: Cloud-Manager-Operator-IBNt24

Add Tags to Connector Instance

Previous Next

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

Cloud Manager

Add Connector

Get Ready AWS Credentials Details Network Security Group Review

Connectivity

VPC: vpc-083fcbd79f75dfb6e - 10.221.0.0/16

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

Key Pair: rt1600680

Public IP: Enable

Proxy Configuration (Optional)

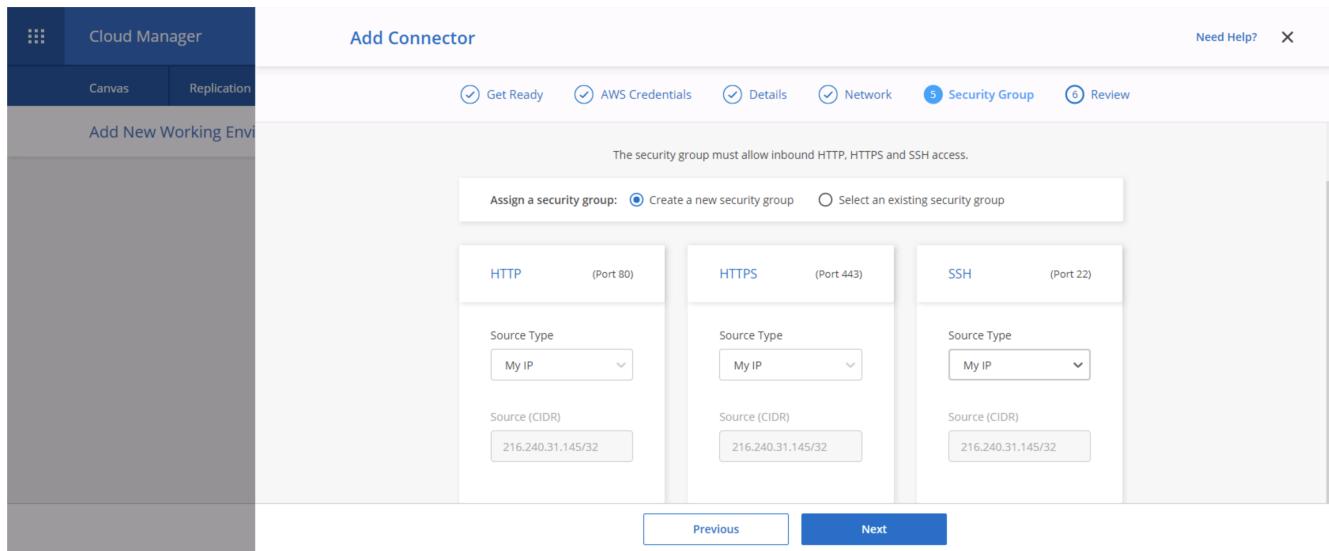
HTTP Proxy: Example: http://172.16.254.1:8080

Define Credentials for this Proxy

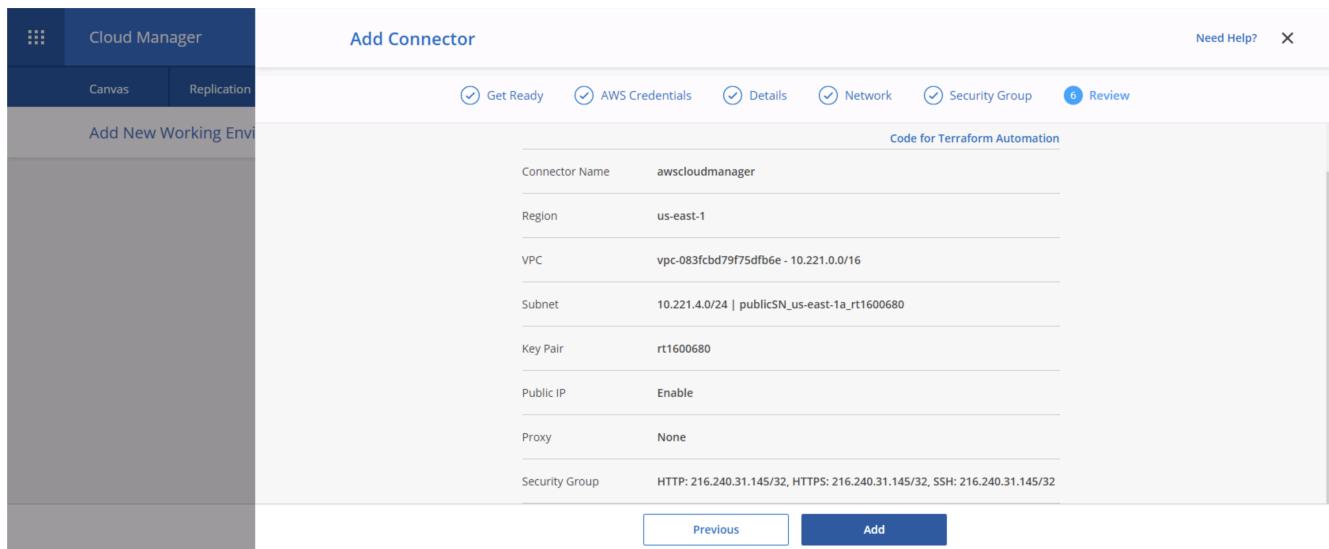
Upload a root certificate

Previous Next

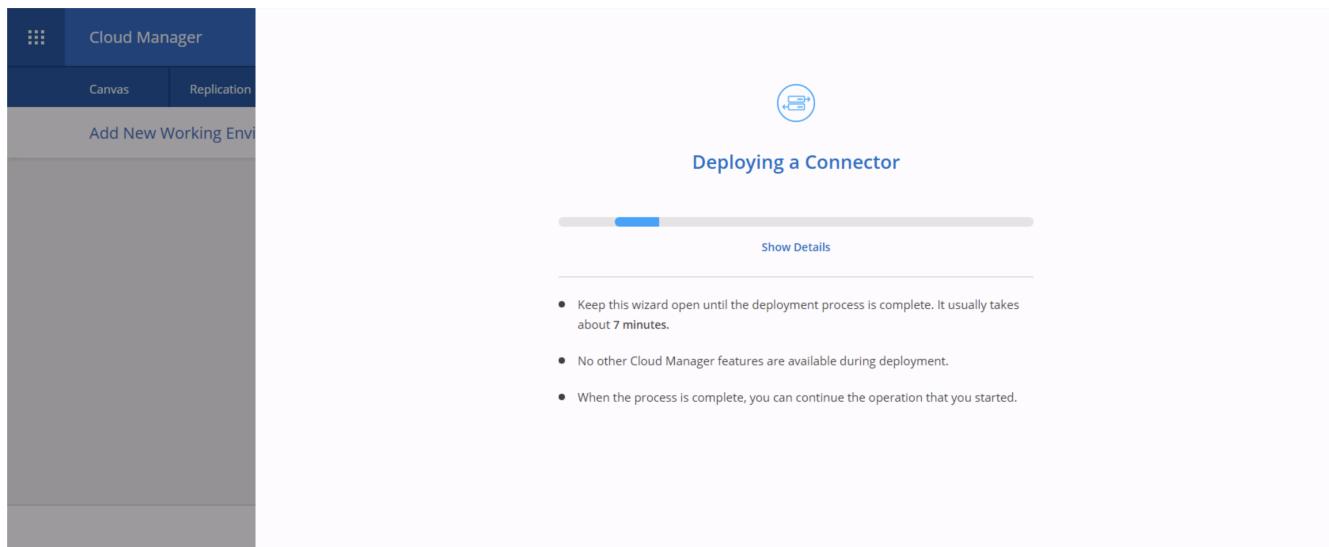
9. Provide communication with the connector via SSH, HTTP, and HTTPS by either providing a security group or creating a new security group. I have enabled access to the connector from my IP address only.



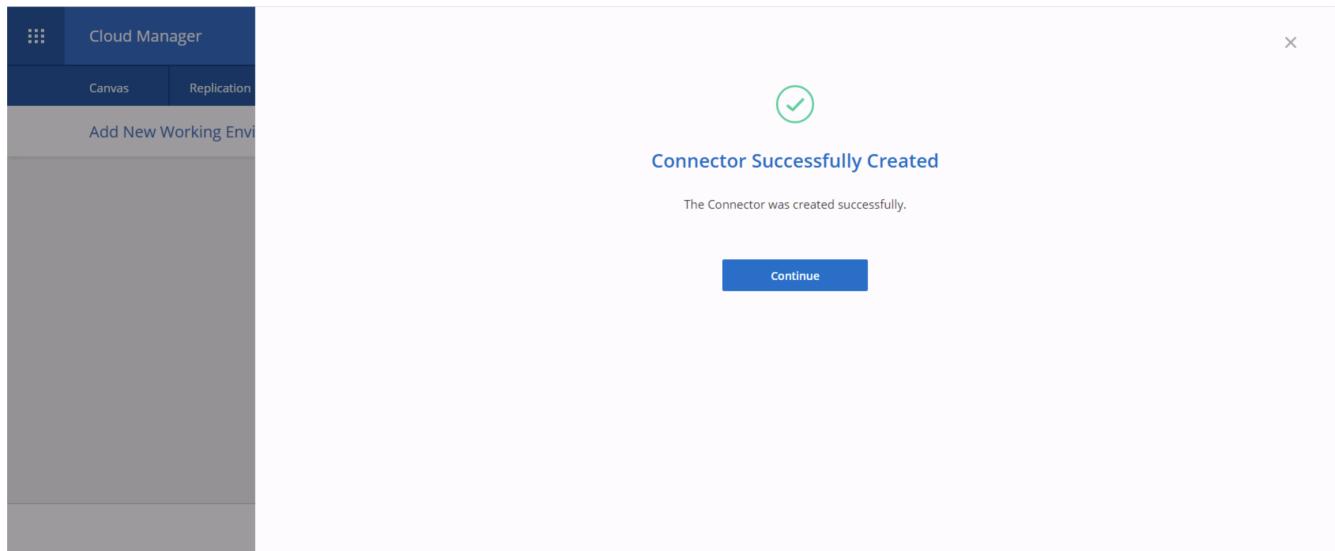
10. Review the information on the summary page and click Add to deploy the connector.



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

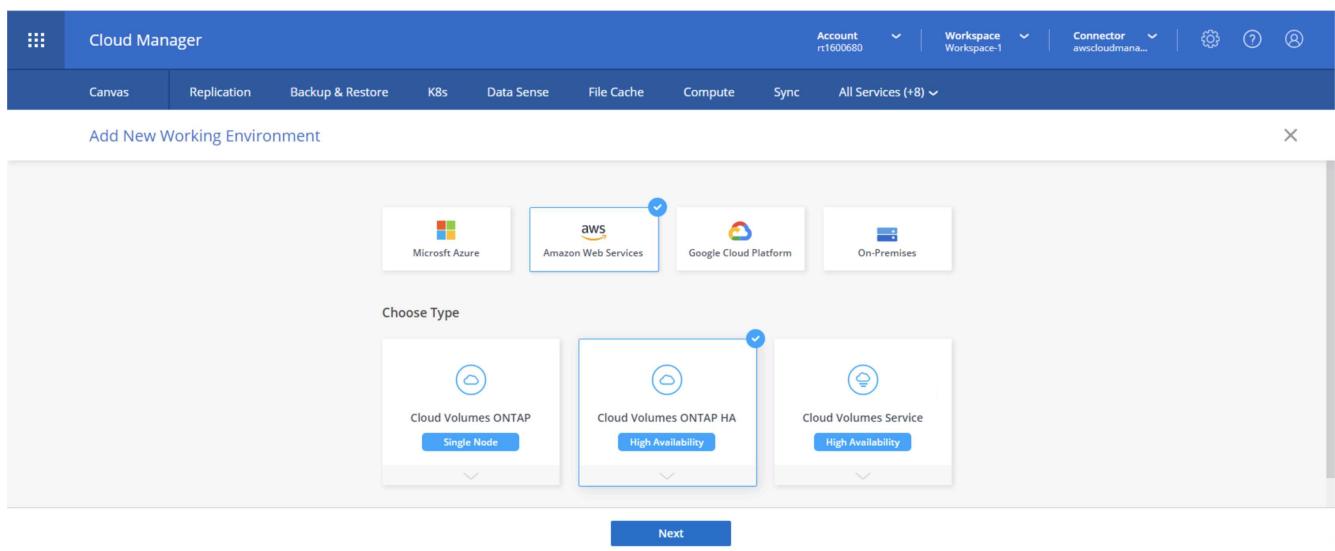


12. When the deployment is complete, a success page appears.



Deploy Cloud Volumes ONTAP

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



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

Create a New Working Environment

Details and Credentials

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

Details Credentials

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

+ Add Tags Optional Field | Up to four tags Password

Confirm Password

Continue

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

3. Choose Add Subscription.

Create a New Working Environment

Details and Credentials

↑ Previous Step Instance Profile Credential Name

Associate Subscription to Credentials ⓘ

Credentials Instance Profile | Account ID: 322944748816

Marketplace Subscription No subscription is associated with this credential

+ Add Subscription

Apply Cancel

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

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

Create a New Working Environment

Edit Credentials & Add Subscription

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

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

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

The next steps:

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

Continue Cancel

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

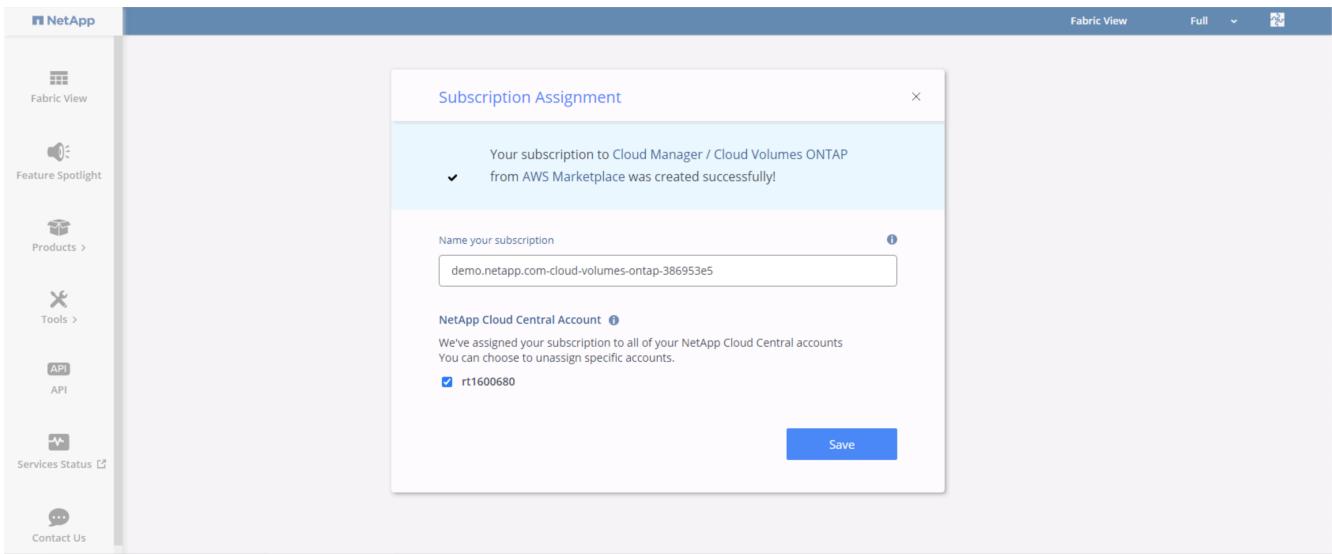
5. You are redirected to AWS; choose Continue to Subscribe.

The screenshot shows the AWS Marketplace interface for the NetApp Cloud Manager product. The product title is 'Cloud Manager - Deploy & Manage NetApp Cloud Data Services'. It is sold by 'NetApp, Inc.'. A 'Continue to Subscribe' button is visible at the top right. Below the title, there is a brief description of the product's features and a 'Show more' link. The 'Overview' tab is selected, showing a 'Product Overview' section with a list of features and a 'Highlights' section with bullet points. Other tabs include 'Pricing', 'Usage', 'Support', and 'Reviews'.

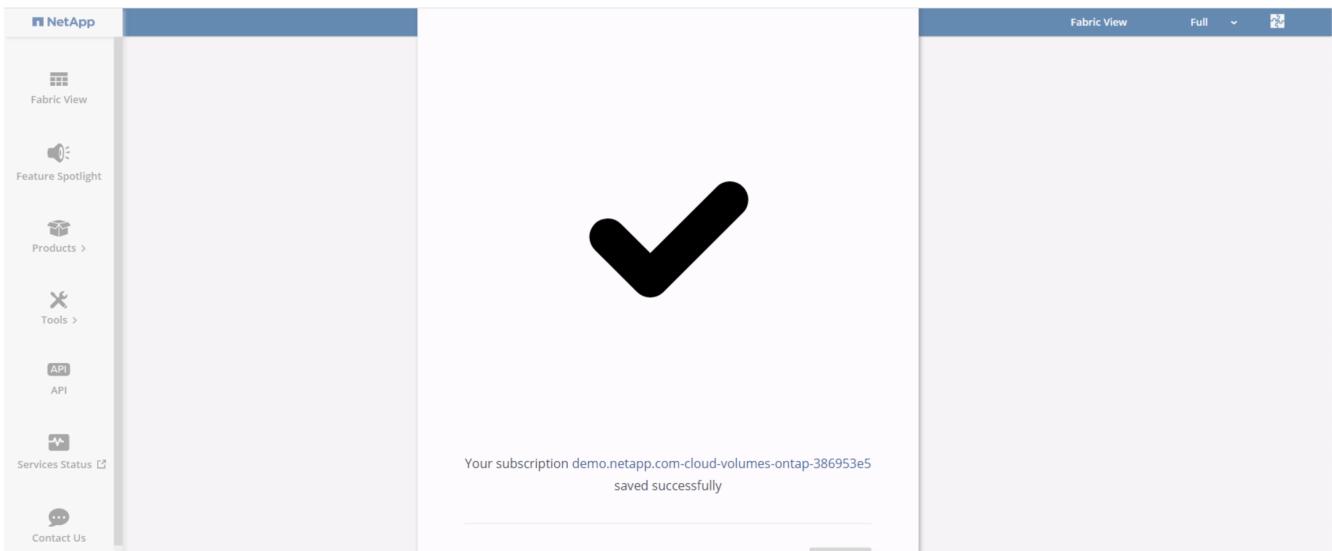
6. Subscribe and you are redirected back to NetApp Cloud Central. If you have already subscribed and don't get redirected, choose the "Click here" link.

The screenshot shows the AWS Marketplace interface for the NetApp Cloud Manager product. A message at the top states 'You are extended multiple offers! Select an offer first and review the pricing information and EULA.' Below this, there is a dropdown menu for 'Offer name' set to 'NetApp, Inc. for SaaS 2020-07-20- Private Offer - current subscription'. To the right, a box titled 'You Are Subscribed to This Offer' provides details about the offer, including the vendor, offer ID, and expiration date. Another box titled 'You Have Subscribed to a Private Offer' explains the private offer status and the date it will expire. At the bottom, there is a 'Subscribe' button and a note about agreeing to the EULA and terms.

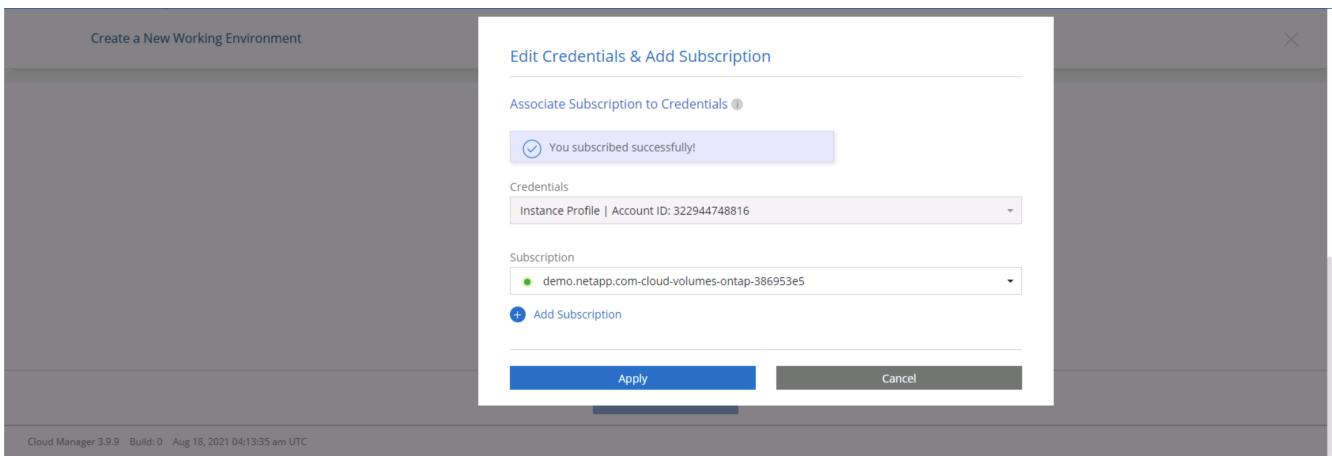
7. You are redirected to Cloud Central where you must name your subscription and assign it to your Cloud Central account.



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



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



- Enter the working environment details such as:

- Cluster name

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

The screenshot shows the 'Create a New Working Environment' interface in Cloud Manager. At the top, there are tabs for Canvas, Replication, Backup & Restore, K8s, Data Sense, File Cache, Compute, Sync, and All Services (+8). The 'Details and Credentials' tab is selected. On the left, there's a 'Previous Step' button and an 'Instance Profile' section with fields for '322944748816' and 'demo.netapp.com-cloud-vol...'. To the right, there's a 'Credential Name' field with 'Account ID' and 'Marketplace Subscription' dropdowns, and a 'Edit Credentials' button. Below these, the 'Details' section contains a 'Working Environment Name (Cluster Name)' input field with 'hybridawscvo'. The 'Credentials' section includes 'User Name' ('admin'), 'Password' ('*****'), and 'Confirm Password' ('*****'). A 'Continue' button is at the bottom.

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

The screenshot shows the 'Services' configuration step in Cloud Manager. It lists three services: 'Data Sense & Compliance', 'Backup to Cloud', and 'Monitoring', each with a toggle switch. All three switches are turned on. A 'Continue' button is at the bottom.

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

The screenshot shows the Cloud Manager interface with the title "Create a New Working Environment" and "HA Deployment Models". It compares "Multiple Availability Zones" and "Single Availability Zone".

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

Both sections have "Extended Info" links at the bottom.

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

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

The screenshot shows the Cloud Manager interface with the title "Region & VPC". It includes fields for AWS Region (US East | N. Virginia), VPC (vpc-083fcbd79f75dfb6e - 10.221.0.0/16), and Security group (Use a generated security group).

Below these fields are three sections for "Node 1", "Node 2", and "Mediator", each with "Availability Zone" and "Subnet" dropdowns. The "Subnet" dropdown for the "Mediator" section is highlighted.

A "Continue" button is at the bottom.

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

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

The screenshot shows the Cloud Manager interface with the title "Connectivity & SSH Authentication". It includes sections for "Nodes" and "Mediator".

Nodes: SSH Authentication Method is set to "Password".

Mediator: Security Group is set to "Use a generated security group", Key Pair Name is "rt1600680", and Internet Connection Method is "Public IP address".

A "Continue" button is at the bottom.

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



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

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

The screenshot shows the 'Cloud Manager' interface with the 'Floating IPs' step selected. It includes fields for entering floating IP addresses for cluster management, NFS/CIFS data, SVM management, and an optional floating IP address. A note explains that floating IPs can migrate between HA nodes if failures occur, and it's recommended to set up an AWS transit gateway. A 'Continue' button is at the bottom.

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

The screenshot shows the 'Cloud Manager' interface with the 'Route Tables' step selected. It lists two route tables: 'private_rt_rt1600680' and 'public_rt_rt1600680'. Both are checked. A note states that selecting route tables enables client access to the HA pair. An 'Additional Information' link is available. A 'Continue' button is at the bottom.

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

Cloud Manager

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

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

Create a New Working Environment Data Encryption X

↑ Previous Step AWS Managed Encryption

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

Default Master Key: aws/ebs

Continue

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

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

Cloud Manager

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

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

Create a New Working Environment Cloud Volumes ONTAP Charging Methods & NSS Account X

↑ Previous Step Cloud Volumes ONTAP Charging Methods

Learn more about our charging methods

Pay-As-You-Go by the hour

Bring your own license

Freemium (Up to 500GB)

NetApp Support Site Account (Optional)

Learn more about NetApp Support Site (NSS) accounts

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

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

Add Netapp Support Site Account

Continue

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

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

Cloud Manager

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

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

Create a New Working Environment Preconfigured Packages X

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

POC and small workloads Up to 2TB of storage

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

Cost effective DR Up to 10TB of storage

Highest performance production workloads Up to 368TB of storage

Continue

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

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

Cloud Manager

Create a New Working Environment Create Volume

↑ Previous Step Details & Protection Protocol

Volume Name: Size (GB): Volume size

Snapshot Policy: default

Access Control: Custom export policy

Custom export policy: 10.221.0.0/16

Advanced options

Continue Skip

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

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

Cloud Manager

Create a New Working Environment Review & Approve

↑ Previous Step hybridawscvo Show API request

AWS | us-east-1 | HA

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

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

Overview Networking Storage

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

Go

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

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

Cloud Manager

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

Account rt1600680 Workspace Workspace-1 Connector awscloudman...

Go to Tabular View

Add Working Environment

Working environments

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

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

Cloud Manager

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

Account rt1600680 Workspace Workspace-1 Connector awscloudman...

Resources

- Canvas Review CVO, CVS, ANF & On-Premises
- Digital Wallet View & Manage Digital Wallet
- Timeline** View Activity & Events

Services

Service	Description	Status
Replication	Data Replication	Green
Backup & Restore	Data Protection for CVO and On-Premises	Green
K8s	Cloud Native Development	Green
Data Sense	Data Governance & Compliance	Green
Compliance	Privacy & Compliance Controls	Green
Tiering	Lift and DON'T shift	Green
Monitoring	Monitor, Optimize and Secure	Green
File Cache	Consolidate your Data into the Cloud	Green
Compute	Optimize your cloud spend	Green
Sync	Automated Data Synchronization	Green
SnapCenter	Application Data Management	Green
Active IQ	Digital Advisor	Green

<https://cloudmanager.netapp.com/timeline>

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

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

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

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

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

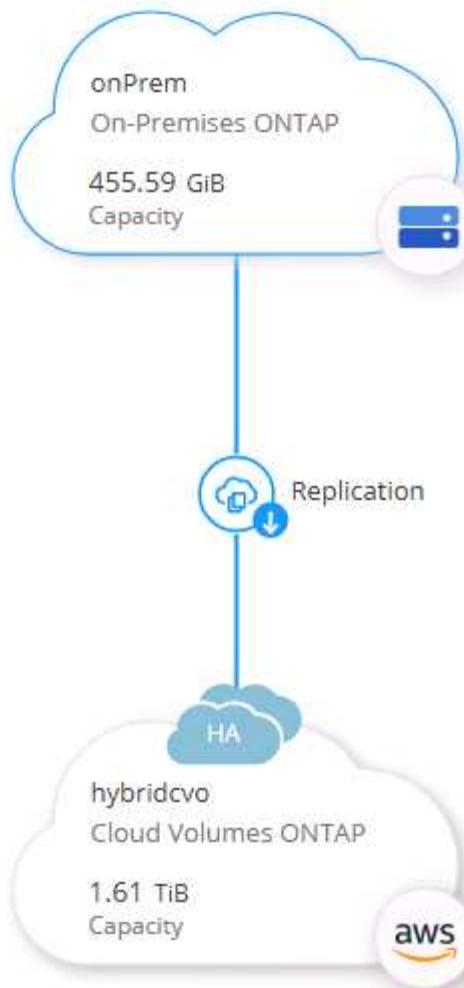
- 1 Cloud Volumes ONTAP (High-Availability)
1 GiB Allocated Capacity
- 1 Amazon S3
0 Buckets

Configure SnapMirror from on-premises to cloud

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

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

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



Select Enable.



Or Options.

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

onPrem
■ On

DETAILS

On-PremisesONTAP

SERVICES

Replication
■ On

1 Replication Target

Replicate.

This screenshot is similar to the first one but includes a dropdown menu for the 'Replication' service. The 'Replication' section shows '1 Replication Target'. A blue arrow points down to a dropdown menu with two items: 'View Replications' and 'Replicate'. The 'Replicate' item is highlighted with a blue border.

onPrem
■ On

DETAILS

On-PremisesONTAP

SERVICES

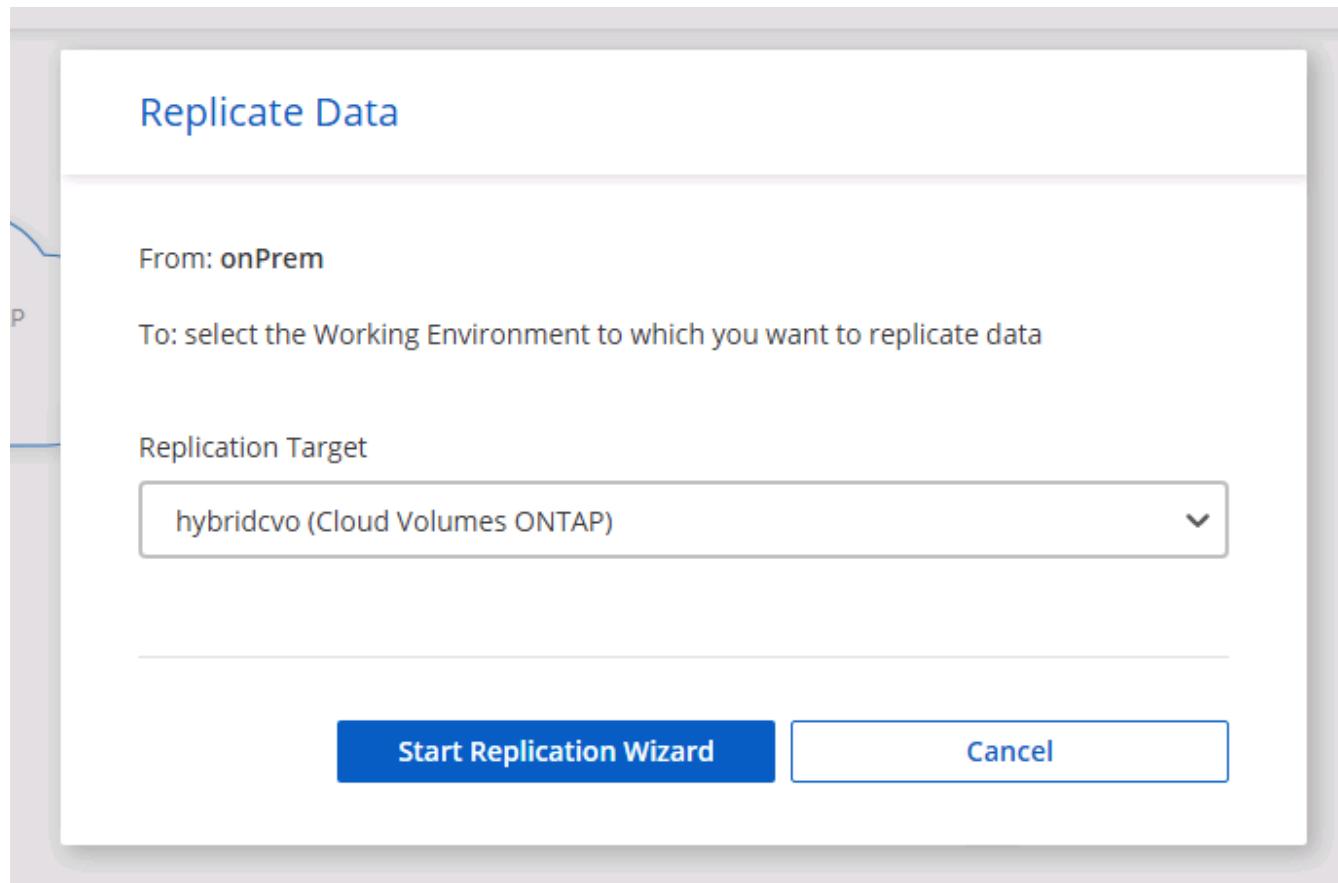
Replication
■ On

1 Replication Target

View Replications

Replicate

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



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

Source Volume Selection			
rhel2_u03 INFO Storage VM Name: svm_onPrem Tiering Policy: None Volume Type: RW CAPACITY 100 GB Allocated 7.29 GB Disk Used	rhel2_u03 INFO Storage VM Name: svm_onPrem Tiering Policy: None Volume Type: RW CAPACITY 100 GB Allocated 35.83 MB Disk Used	sql1_data INFO Storage VM Name: svm_onPrem Tiering Policy: None Volume Type: RW CAPACITY 53.37 GB Allocated 45.09 GB Disk Used	
sql1_log INFO Storage VM Name: svm_onPrem Tiering Policy: None Volume Type: RW CAPACITY 21.35 GB Allocated 18.16 GB Disk Used	sql1_snapctr INFO Storage VM Name: svm_onPrem Tiering Policy: None Volume Type: RW CAPACITY 24.87 GB Allocated 21.23 GB Disk Used		

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

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

[↑ Previous Step](#)

Destination Disk Type



S3 TIERING

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

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

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

Destination Volume Name

Destination Volume Name

sql1_data_dr

Destination Aggregate

Automatically select the best aggregate ▾

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

Max Transfer Rate

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

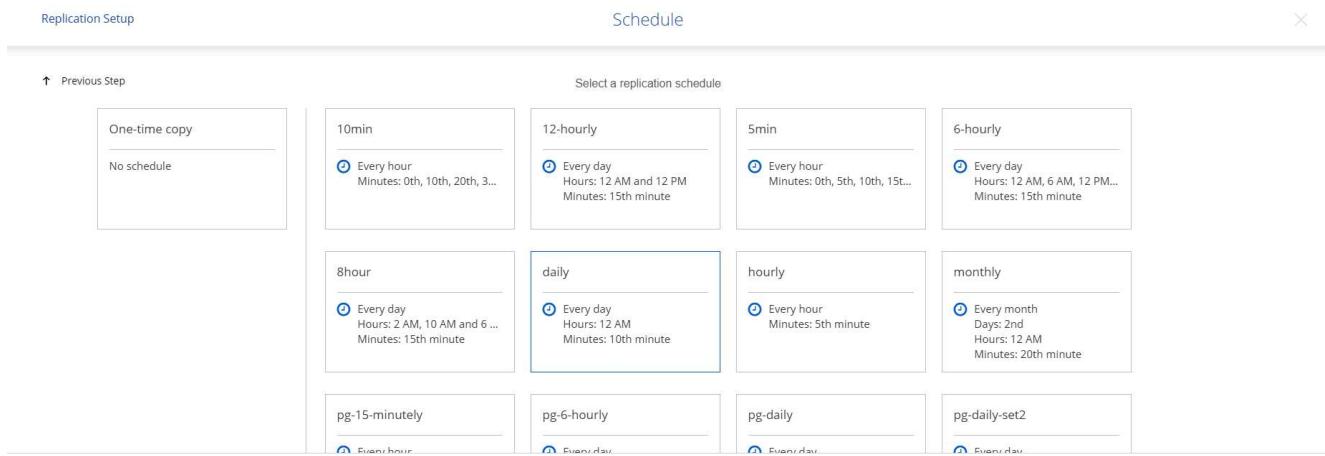
- Limited to: MB/s
- Unlimited (recommended for DR only machines)

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

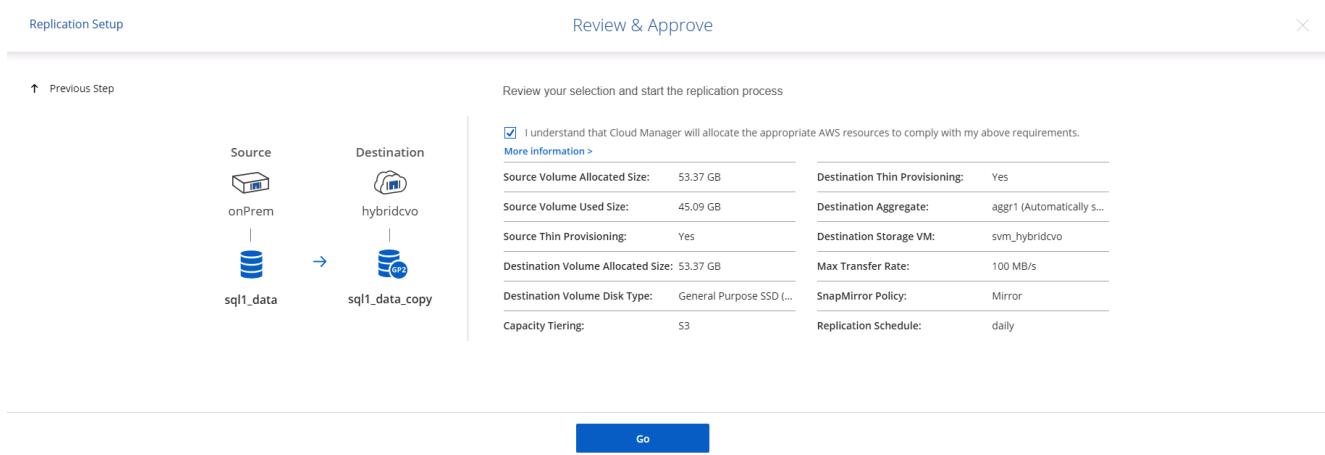
Replication Policy

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

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



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



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

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

Health Status	Source Volume	Target Volume	Total Transfer Time	Status	Mirror State	Last Successful Transfer
✓	rhel2_u01 onPrem	rhel2_u01_dr hybridcvo	43 minutes 43 seconds	idle	snapmirrored	Sep 30, 2021, 12:12:50 AM 19.73 MiB
✓	rhel2_u02 onPrem	rhel2_u02_dr hybridcvo	1 hour 37 minutes 59 seconds	idle	snapmirrored	Sep 30, 2021, 2:37:08 PM 239.78 MiB
✓	rhel2_u03 onPrem	rhel2_u03_dr hybridcvo	16 hours 1 minute 9 seconds	idle	snapmirrored	Sep 30, 2021, 4:07:14 PM 225.37 KiB
✓	sql1_data onPrem	sql1_data_dr hybridcvo	1 hour 6 minutes 50 seconds	idle	snapmirrored	Sep 30, 2021, 12:12:28 AM 24.56 KiB
✓	rhel2_u04 onPrem	rhel2_u04_dr hybridcvo	1 hour 1 minute 40 seconds	idle	snapmirrored	Sep 30, 2021, 12:12:30 AM 24.56 KiB
✓	rhel2_u05 onPrem	rhel2_u05_dr hybridcvo	1 hour 1 minute 40 seconds	idle	snapmirrored	Sep 30, 2021, 12:12:30 AM 24.56 KiB
✓	rhel2_u06 onPrem	rhel2_u06_dr hybridcvo	1 hour 1 minute 40 seconds	idle	snapmirrored	Sep 30, 2021, 12:12:30 AM 24.56 KiB

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

3. Deploy EC2 compute instance for database workload

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

Sizing the compute instance

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

Linux instance configuration for Oracle workload

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

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

Windows instance configuration for SQL Server workload

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

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

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

Workflow for dev/test bursting to cloud

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

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

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

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

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

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

Backup Name	Count	Type	End Date	Verified	Mounted	RMAN Cataloged	SCN
rhe12_cdb2_log_09-17-2021_15.00.01.1317_1	1	Log	09/17/2021 3:00:10 PM	Not Applicable	False	Not Cataloged	5982003
rhe12_cdb2_09-17-2021_14.35.01.4997_1	1	Log	09/17/2021 2:35:21 PM	Not Applicable	False	Not Cataloged	5980629
rhe12_cdb2_09-17-2021_14.35.01.4997_0	1	Data	09/17/2021 2:35:12 PM	Unverified	False	Not Cataloged	5980588
rhe12_cdb2_log_09-17-2021_14.00.01.1042_1	1	Log	09/17/2021 2:00:10 PM	Not Applicable	False	Not Cataloged	5978388
rhe12_cdb2_log_09-17-2021_13.00.01.7389_1	1	Log	09/17/2021 1:00:11 PM	Not Applicable	False	Not Cataloged	5971535
rhe12_cdb2_log_09-17-2021_12.00.01.1142_1	1	Log	09/17/2021 12:00:10 PM	Not Applicable	False	Not Cataloged	5971773
rhe12_cdb2_log_09-17-2021_11.00.01.0895_1	1	Log	09/17/2021 11:00:10 AM	Not Applicable	False	Not Cataloged	5968474

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

NetApp SnapCenter®

Oracle Database ▾

Search databases

cdb2 Topology

Manage Copies

Local copies

Mirror copies

Summary Card

368 Backups

16 Data Backups

352 Log Backups

0 Clones

Backup Name

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

Total 1

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

Mount backups

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

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

Secondary storage location : Snap Vault / Snap Mirror

Source Volume	Destination Volume
svm_onPrem:rhel2_u03	svm_hybridcvo:rhel2_u03_dr

Mount Cancel

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



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

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

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

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

Clone from cdb2

1 Name

Complete Database Clone

Clone SID: cdb2test

Exclude PDBs: Type to find PDBs

PDB Clone

Secondary storage location : Snap Vault / Snap Mirror

Data

Source Volume	Destination Volume
svm_onPrem:rhel2_u02	svm_hybridcvo:rhel2_u02_dr

Logs

Source Volume	Destination Volume
svm_onPrem:rhel2_u03	svm_hybridcvo:rhel2_u03_dr

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

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

Clone from cdb2

1 Name

Select the host to create a clone

Clone host

2 Locations

3 Credentials

4 PreOps

5 PostOps

6 Notification

7 Summary

④ Datafile locations

/u02_cdb2test

⑤ Control files

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

⑥ Redo logs

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

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

Clone from cdb2

1 Name

2 Locations

3 Credentials

4 PreOps

5 PostOps

6 Notification

7 Summary

Database Credentials for the clone

Credential name for sys user + ?

Database port

Oracle Home Settings ?

Oracle Home

Oracle OS User

Oracle OS Group

Previous Next

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

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

Clone from cdb2

Specify scripts to run before clone operation

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

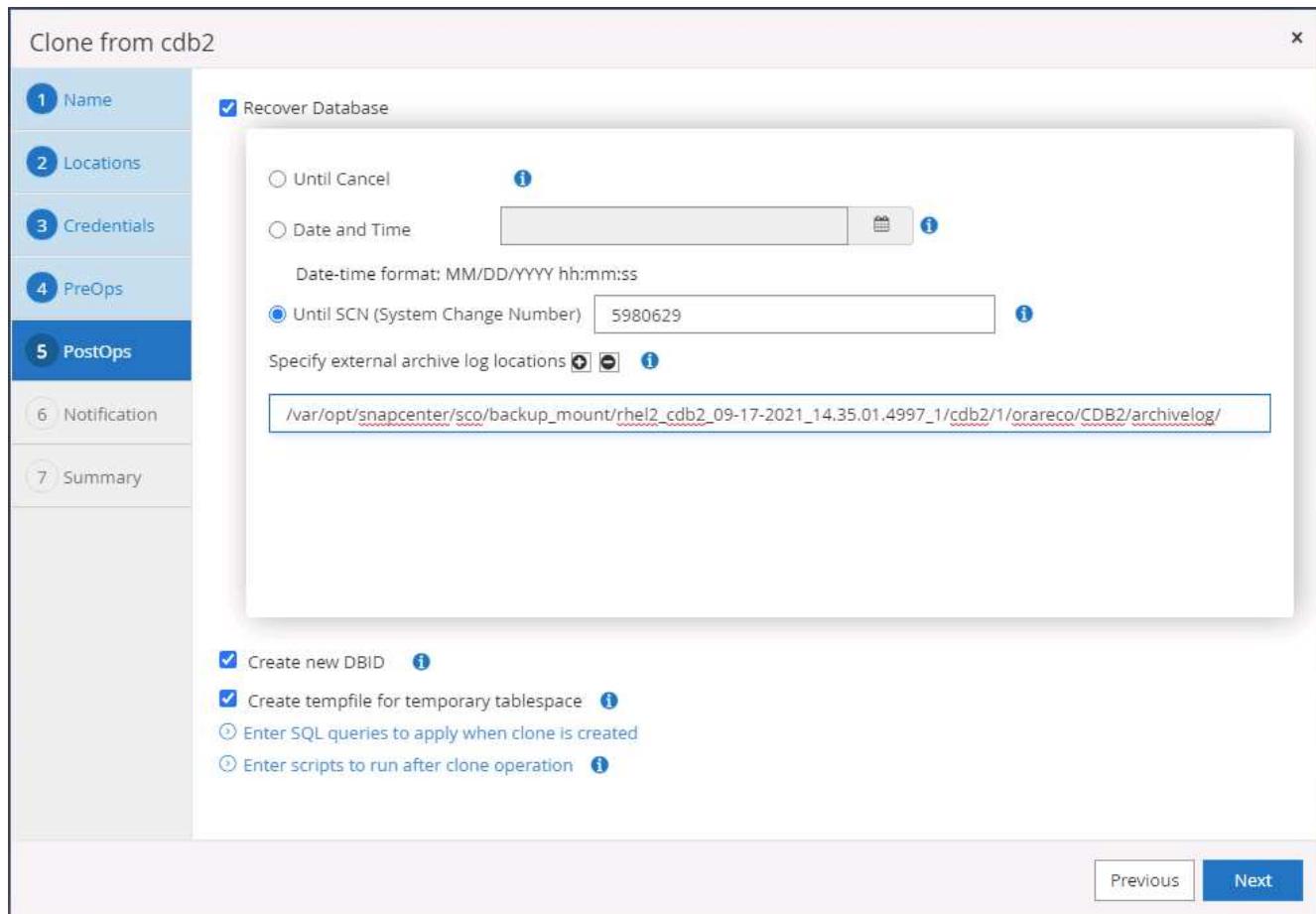
Database Parameter settings

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

Buttons:

- Previous
- Next

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



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

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

Clone from cdb2

Provide email settings i

Email preference	Never
From	From email
To	Email to
Subject	Notification

Attach job report

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

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

12. Clone summary.

Clone from cdb2

1 Name

2 Locations

3 Credentials

4 PreOps

5 PostOps

6 Notification

7 Summary

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

Previous **Finish**

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

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

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

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

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

SQL> select name, log_mode from v$database;
NAME      LOG MODE
-----
CDB2TEST  ARCHIVELOG

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

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

SQL>
```

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

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

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

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

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

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

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

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

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

Clone Options

Clone settings

- Clone server: Choose
- Clone instance: Nothing selected
- Clone name: tpcc

Choose mount option

- Auto assign mount point
- Auto assign volume mount point under path

Secondary storage location : Snap Vault / Snap Mirror

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

Next

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

Clone from backup X

1 Clone Options

Clone settings

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

Choose mount option

Auto assign mount point i

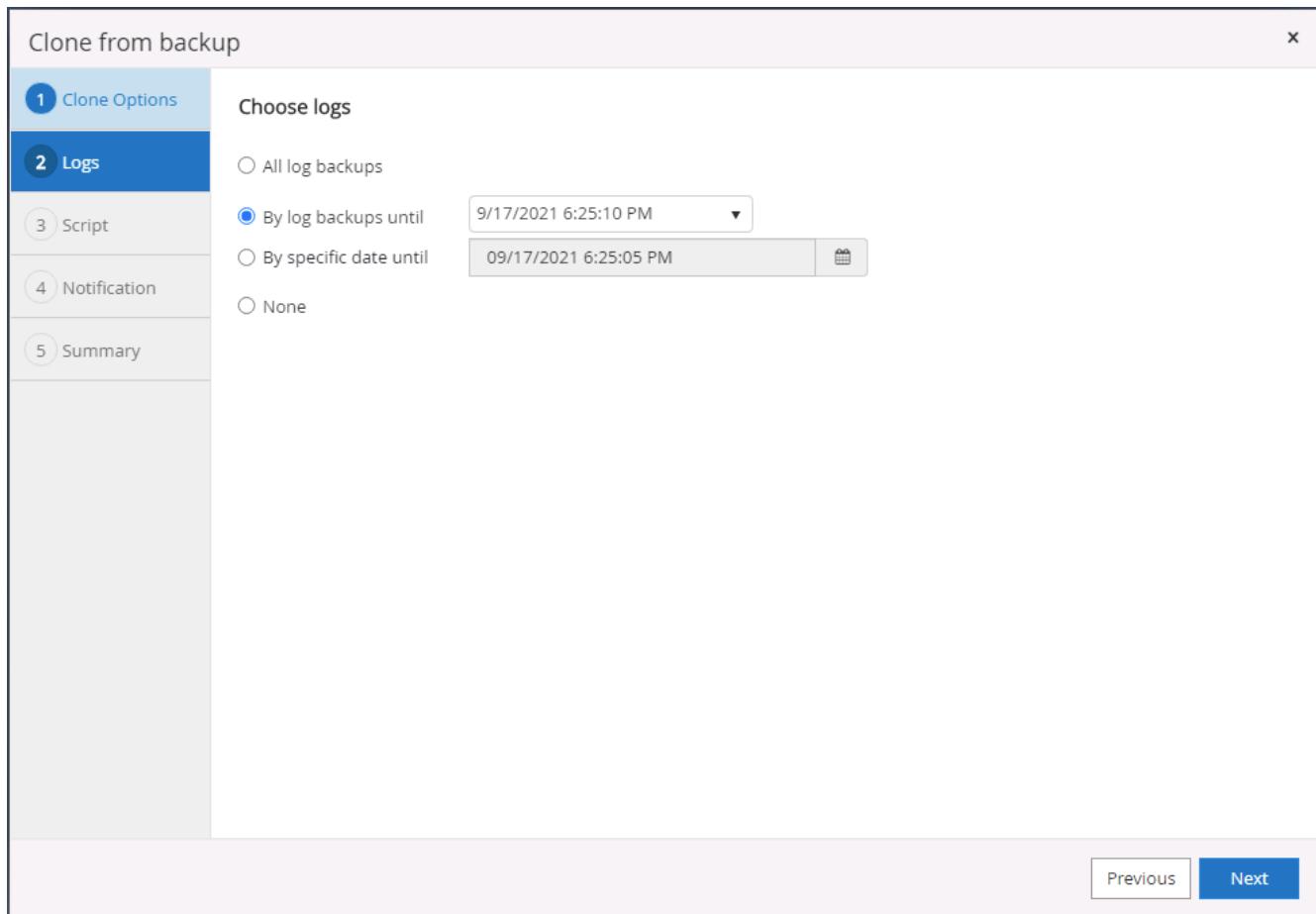
Auto assign volume mount point under path full file path i

Secondary storage location : Snap Vault / Snap Mirror

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

Previous Next

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



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

Clone from backup

X

1 Clone Options

2 Logs

3 Script

4 Notification

5 Summary

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

Prescript full path

Prescript arguments Choose optional arguments...

Postscript full path

Postscript arguments Choose optional arguments...

Script timeout 60 secs

Previous Next

This screenshot shows the 'Clone from backup' configuration interface. The 'Script' tab is active, allowing users to specify optional scripts for before and after the cloning process. Fields include Prescript and Postscript full paths, their respective argument inputs, and a script timeout of 60 seconds. Navigation buttons 'Previous' and 'Next' are at the bottom.

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

Clone from backup X

1 Clone Options

2 Logs

3 Script

4 Notification

5 Summary

Provide email settings i

Email preference	Never
From	From email
To	Email to
Subject	Notification

Attach Job Report

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

Previous Next

9. Clone Summary.

Clone from backup

1 Clone Options

2 Logs

3 Script

4 Notification

5 Summary

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

Previous **Finish**

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

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

Post-clone configuration

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

Refresh clone database

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

Where to go for help?

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

Next: [Disaster recovery workflow](#).

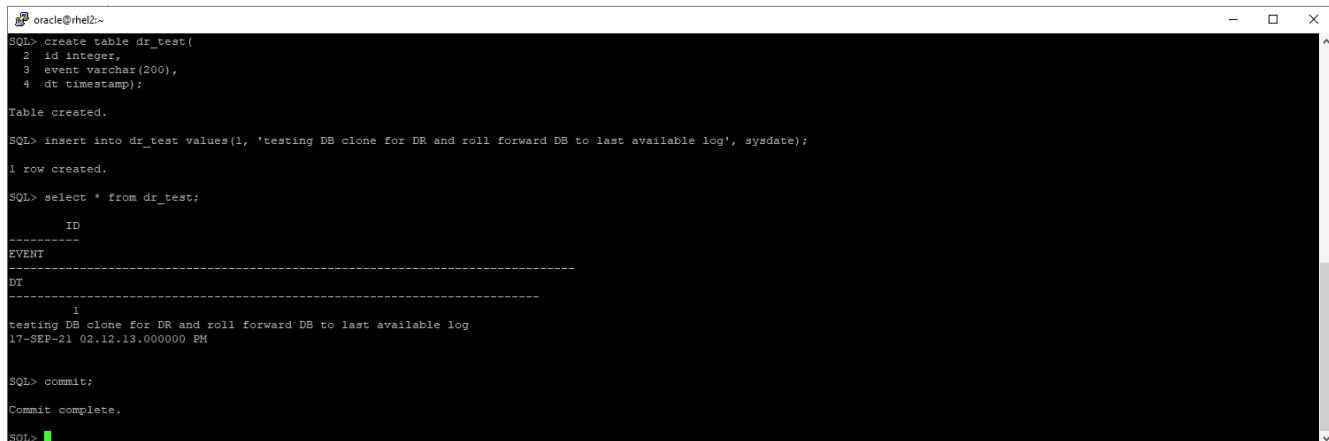
Disaster recovery workflow

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

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

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

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



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

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

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

SQL> commit;
Commit complete.

SQL>
```

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

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

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

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

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



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

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

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

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

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

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

The screenshot shows the NetApp SnapCenter interface for managing Oracle databases. The top navigation bar includes links for Database Settings, Protect, and Refresh. The main area displays the 'cdb2 Topology' for the 'cdb2' database. It shows 'Manage Copies' with 'Local copies' (185 Backups, 0 Clones) and 'Mirror copies' (185 Backups, 2 Clones). A 'Summary Card' provides a quick overview of backup statistics: 370 Backups, 16 Data Backups, 354 Log Backups, and 2 Clones. Below this, a table lists 'Secondary Mirror Backup(s)' with columns for Backup Name, Count, Type, End Date, Verified, Mounted, RMAN Cataloged, and SCN. The table contains six entries, all of which are Log type backups.

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

The screenshot shows the 'Clone from cdb2' wizard in progress. The current step is '1 Name'. The 'Complete Database Clone' option is selected. The 'Clone SID' field is populated with 'cdb2dr'. The sidebar on the left lists the following steps:

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

Secondary storage location : Snap Vault / Snap Mirror

Data

Source Volume	Destination Volume
svm_onPrem:rhel2_u02	svm_hybridcvo:rhel2_u02_dr

Logs

Source Volume	Destination Volume
svm_onPrem:rhel2_u03	svm_hybridcvo:rhel2_u03_dr

Buttons at the bottom:

- Previous
- Next

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

The screenshot shows the ONTAP System Manager interface. On the left, there's a navigation sidebar with sections like DASHBOARD, STORAGE (Overview, Applications, Volumes), LUNs, Shares, Qtrees, Quotas, Storage VMs, Tiers, NETWORK, EVENTS & JOBS, PROTECTION, and HOSTS. The main area is titled 'Volumes' and lists several volumes: ora_standby_u01, rhel2_u01_dr, rhel2_u02_dr, rhel2_u02_dr09172116081193_60, rhel2_u02_dr0917211703548_63, rhel2_u03_dr, and rhel2_u03_dr09172118245747_75. A modal window titled 'Add Volume' is open, prompting for a 'NAME' (set to 'ora_standby_u03') and 'CAPACITY' (set to '20 GB'). There are 'More Options' and 'Save' buttons.

```

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

```



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

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

Clone from cdb2

1 Name

Select the host to create a clone

Clone host ora-standby.demo.netapp.com

2 Locations

Datafile locations /u02_cdb2dr

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

Redo logs

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

Previous Next

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

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

Clone from cdb2

1 Name

2 Locations

3 Credentials

4 PreOps

5 PostOps

6 Notification

7 Summary

Database Credentials for the clone

Credential name for sys user + ?

Database port

Oracle Home Settings ?

Oracle Home

Oracle OS User

Oracle OS Group

Previous Next

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

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

Clone from cdb2

Specify scripts to run before clone operation

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

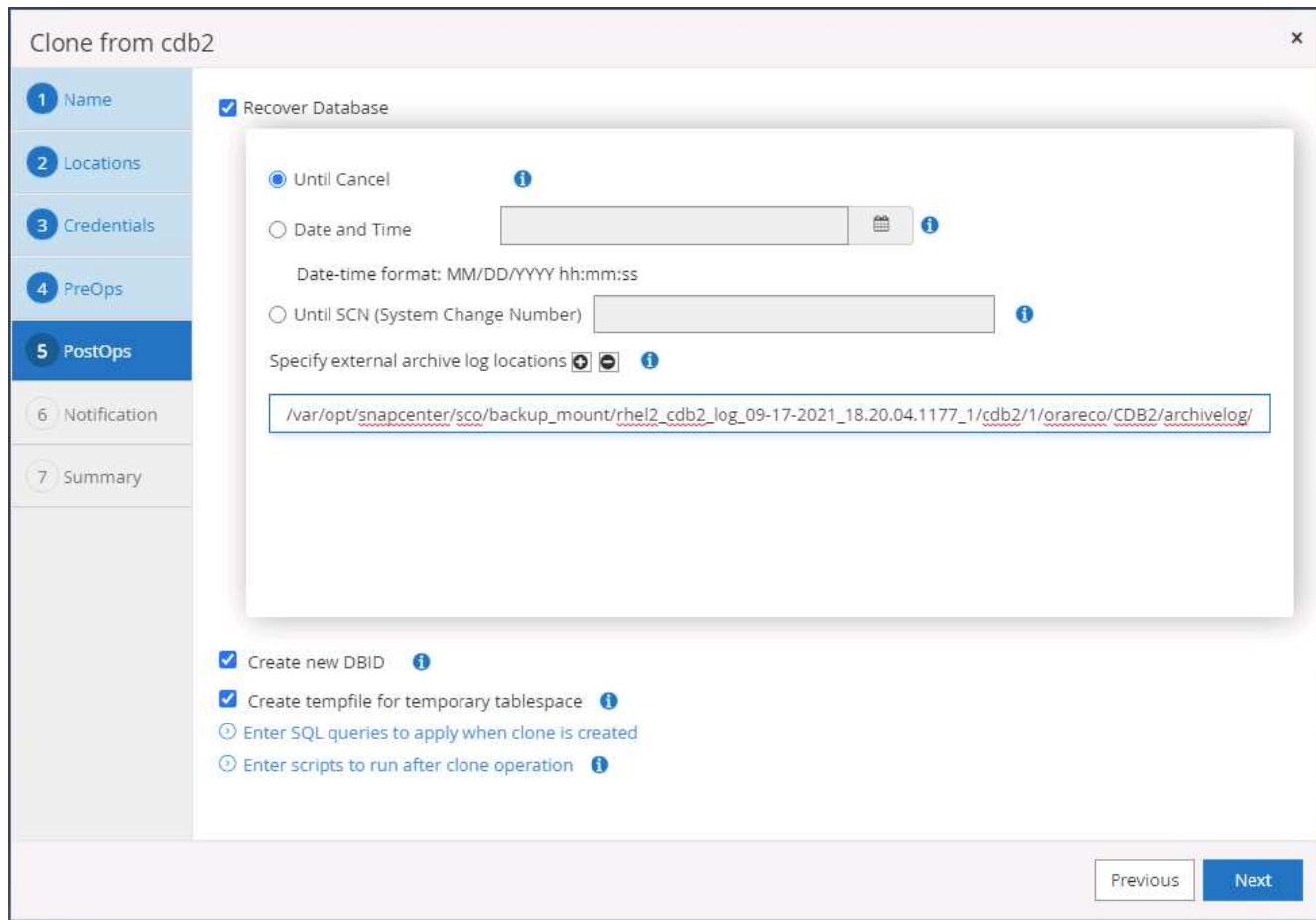
Database Parameter settings

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

Buttons:

- Previous
- Next

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



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

Clone from cdb2

Provide email settings i

Email preference	Never
From	From email
To	Email to
Subject	Notification

Attach job report

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

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

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

13. DR clone summary.

Clone from cdb2

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

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

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

NetApp SnapCenter							
		Oracle Database					
		View	Database	Search databases			
	Dashboard						
	Resources		cdb2	Single Instance (Multitenant)	rhel2.demo.netapp.com	rhel2_cdb2 rhel2_cdb2_log	Policies Oracle Archive Log Backup Last Backup 09/17/2021 7:00:10 PM Overall Status Backup succeeded
	Monitor		cdb2dev	Single Instance (Multitenant)	ora-standby.demo.netapp.com		
	Reports		cdb2dr	Single Instance (Multitenant)	ora-standby.demo.netapp.com		
	Hosts		cdb2test	Single Instance (Multitenant)	ora-standby.demo.netapp.com		
	Storage Systems						
	Settings						
	Alerts						

Post DR clone validation and configuration for Oracle

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

```

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

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

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

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

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

SQL> select * from pdbadmin.dr_test;

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

SQL>

```

2. Configure the flash recovery area.

```

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

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

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

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

SQL> show parameter db_recovery_file_dest

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

System altered.

SQL> show parameter db_recovery_file_dest

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

```

3. Configure the Oracle listener for user access.

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

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



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

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

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

```

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

-----
SQL1

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

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

```

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

Name	Resource Name	Type	Host
sql1_tpcc	tpcc (sq1)	SQL Database	sq1.demo.netapp.com
sql1_tpcc_log			

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

Backup

Create a backup for the selected resource group

Resource Group: sql1_tpcc_log

Policy: SQL Server Log Backup

Cancel Backup

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

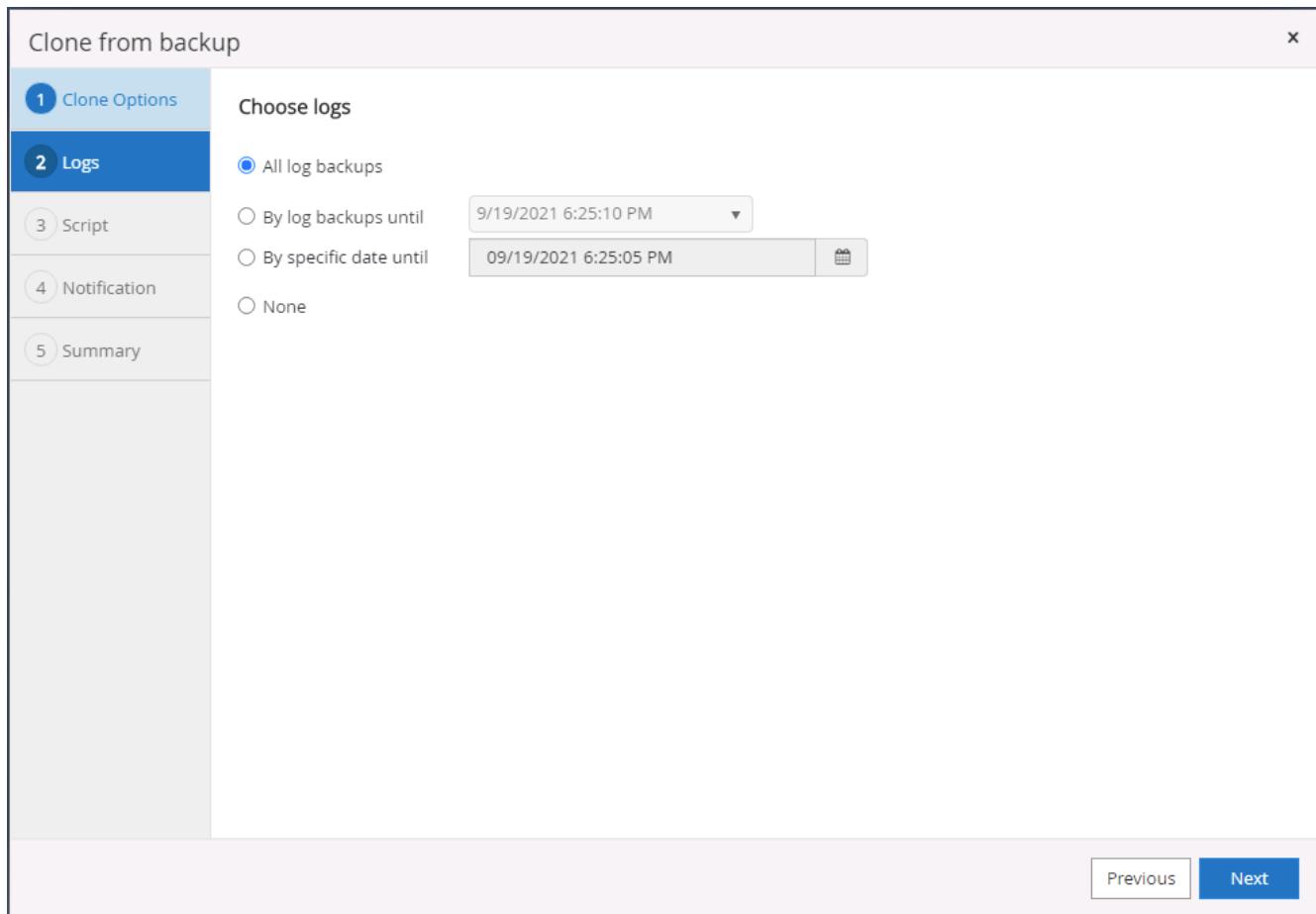
The screenshot shows the NetApp SnapCenter interface for managing a Microsoft SQL Server topology named 'tpcc (sql11)'. On the left, a sidebar lists database names: master, model, msdb, tempdb, tpcc, master, model, msdb, tempdb, tpcc_clone, and tpcc_dev. The 'tpcc' entry is selected. The main pane displays 'Manage Copies' with a diagram showing 'Local copies' (7 Backups, 0 Clones) connected to 'Mirror copies' (7 Backups, 2 Clones). Below this is a table for 'Secondary Mirror Backup(s)' with three entries:

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

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

The screenshot shows the 'Clone from backup' wizard, Step 1: Clone Options. The left sidebar shows steps 1 through 5. The main area is titled 'Clone settings' and includes fields for 'Clone server' (sql-standby.demo.netapp.com), 'Clone instance' (sql-standby), and 'Clone name' (tpcc_dr). Below this is a section titled 'Choose mount option' with two radio button options: 'Auto assign mount point' (selected) and 'Auto assign volume mount point under path' (full file path). The next section, 'Secondary storage location : Snap Vault / Snap Mirror', shows mappings between source volumes (svm_onPrem:sql1_data and svm_onPrem:sql1_log) and destination volumes (svm_hybridcvo:sql1_data_dr and svm_hybridcvo:sql1_log_dr). At the bottom are 'Previous' and 'Next' buttons.

- Select all log backups to be applied.



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

Clone from backup x

1 Clone Options

2 Logs

3 Script

4 Notification

5 Summary

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

Prescript full path

Prescript arguments Choose optional arguments...

Postscript full path

Postscript arguments Choose optional arguments...

Script timeout 60 secs

Previous Next

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

Clone from backup

Provide email settings i

Email preference	Never
From	From email
To	Email to
Subject	Notification

Attach Job Report

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

Previous Next

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

Clone from backup

1 Clone Options

2 Logs

3 Script

4 Notification

5 Summary

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

Previous **Finish**

NetApp SnapCenter®

Microsoft SQL Server

View Database search by name

Refresh Resources New Resource Group

Resources	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		09/22/2021 5:35:08 PM	Backup failed, Schedules on hold	User database
master	sql-standby	sql-standby.demo.netapp.com			Not available for backup	System database
model	sql-standby	sql-standby.demo.netapp.com			Not available for backup	System database
msdb	sql-standby	sql-standby.demo.netapp.com			Not available for backup	System database
tempdb	sql-standby	sql-standby.demo.netapp.com			Not available for backup	System database
tpcc_clone	sql-standby	sql-standby.demo.netapp.com			Not protected	User database
tpcc_dlev	sql-standby	sql-standby.demo.netapp.com			Not protected	User database
tpcc_dr	sql-standby	sql-standby.demo.netapp.com			Not protected	User database

Post DR clone validation and configuration for SQL

1. Monitor clone job status.

NetApp SnapCenter®

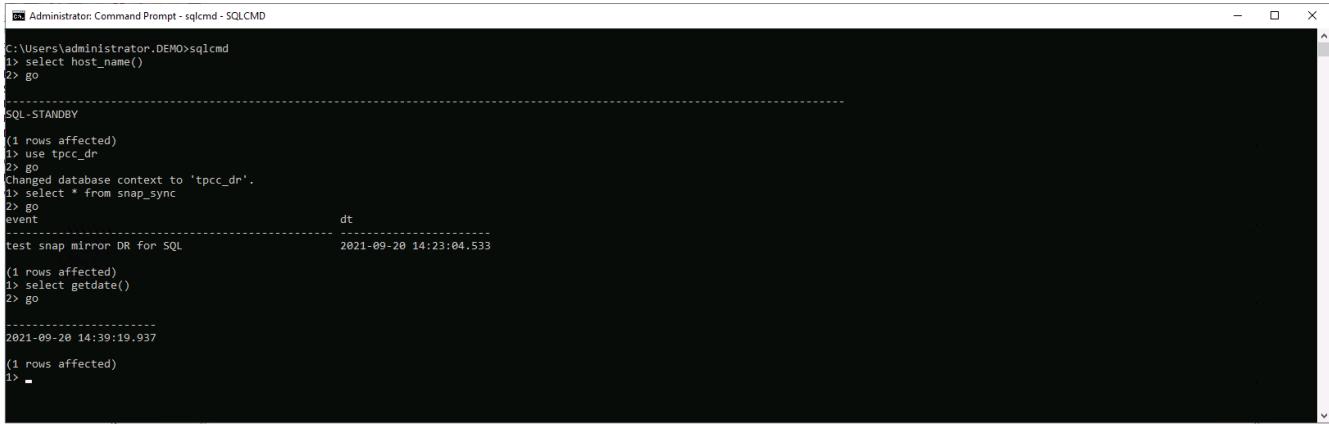
Jobs Schedules Events Logs

Search by name

Details Reports Download Logs Cancel All

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

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



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

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

Where to go for help?

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

Copyright information

Copyright © 2023 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—with prior written permission of the copyright owner.

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

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

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

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

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

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

Trademark information

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