



Getting started overview

NetApp Solutions

NetApp
June 09, 2023

This PDF was generated from https://docs.netapp.com/us-en/netapp-solutions/databases/hybrid_dbops_snapcenter_getting_started_onprem.html on June 09, 2023. Always check docs.netapp.com for the latest.

Table of Contents

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

Getting started overview

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

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

On-premises

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

AWS public cloud

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

Click the following links for details:

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

Getting started on premises

Previous: [Getting started overview.](#)

On Premises

1. Setup database admin user in SnapCenter

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

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

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

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

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

2. SnapCenter plugin installation prerequisites

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

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

Windows host for SQL server:

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

- The SQL instance or host is assigned to an RBAC user.
- The RBAC DB admin user must have both the resource group and backup privileges.

Unix host for Oracle:

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

3. SnapCenter host plugin installation



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

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

Configure SnapCenter VMware global settings

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

Add Windows host and installation of plugin on the host

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

Host Type: Windows
Host Name: sql-standby
Credentials: Domain Admin

Select Plug-ins to Install: Microsoft Windows, Microsoft SQL Server, SAP HANA

Submit Cancel

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

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

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

Host Name: sql-standby.demo.netapp.com
Host IP: 10.221.2.56
Overall Status: Configure log directory
Host Type: Windows
System: Stand-alone
Credentials: Domain Admin

Plug-ins: Microsoft Windows, Microsoft SQL Server

Configure log directory

Alerts: No Alerts

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



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



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

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

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

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

Save Close

Add Unix host and installation of plugin on the host

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

Add Host

Host Type: Linux

Host Name: ora-standby

Credentials: admin

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

- Oracle Database
- SAP HANA

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

Submit **Cancel**

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

More Options

Port: 8145

Installation Path: /opt/NetApp/snapcenter

Skip preinstall checks

Add all hosts in the oracle RAC

Custom Plug-ins

Choose a File

Browse **Upload**

No plug-ins found.

Save **Cancel**

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

Confirm Fingerprint

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

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

Confirm and Submit **Close**

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

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

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

User Name	Domain	Roles
oradba	demo	App Backup and Clone Admin

Assign Assets

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

Asset Type: Host

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

Save Close

4. Database resource discovery

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

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

The screenshot shows the NetApp SnapCenter interface for Oracle Database. The left sidebar includes options like Dashboard, Resources (selected), Monitor, Reports, Hosts, Storage Systems, Settings, and Alerts. The main content area displays a table for Oracle Database resources:

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

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

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

The screenshot shows the NetApp SnapCenter interface for Microsoft SQL Server. The left sidebar includes options like Dashboard, Resources (selected), Monitor, Reports, Hosts, Storage Systems, Settings, and Alerts. The main content area displays a table for Microsoft SQL Server databases:

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.

The screenshot shows the NetApp SnapCenter interface for Microsoft SQL Server. The left sidebar includes options like Dashboard, Resources (selected), Monitor, Reports, Hosts, Storage Systems, Settings, and Alerts. The main content area displays a table for Microsoft SQL Server instances:

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 screenshot shows the NetApp SnapCenter interface for Instance - Credentials for Microsoft SQL Server. The left sidebar includes options like Dashboard, Resources (selected), Monitor, Reports, Hosts, Storage Systems, Settings, and Alerts. The main content area displays a table for Instance - Credentials:

Name	Description
sql-standby	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.
sql1	Name: sql-standby Resource Group: None Policy: None Selectable: Not available for backup. DB is not on NetApp storage, auto-close is enabled or in recovery mode.

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

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

5. Setup storage cluster peering and DB volumes replication

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

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

On-premises cluster:

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

Target CVO cluster:

ONTAP System Manager Overview

IPspaces

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

Broadcast Domains

Cluster	9000 MTU	IPSpace: Cluster
hybridcvo-01	e0b	hybridcvo-01 e0b
hybridcvo-02	e0b	hybridcvo-02 e0b

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

Network Interfaces

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

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

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

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

ONTAP System Manager Overview (Return to classic version)

UI Settings

LOG LEVEL: DEBUG
INACTIVITY TIMEOUT: 30 minutes

Intercluster Settings

Network Interfaces

IP ADDRESS: 192.168.0.113

Cluster Peers

PEERED CLUSTER NAME: hybridcvo

Peer Cluster (highlighted)
Generate Passphrase
Manage Cluster Peers

Storage VM Peers

PEERED STORAGE VMS: 1

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

Volumes

Protect (highlighted)

Name
onPrem_data
rhel2_u01
rhel2_u02
rhel2_u03
rhel2_u0309232119421203118
sql1_data
sql1_log
sql1_snapctr
svm_onPrem_root

rhel2_u03 All Volumes

Overview (selected)

Snapshot Copies **Clone Hierarchy** **SnapMirror (Local or Remote)**

Capacity

0% 10% 20% 30% 40% 50%

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

Performance

Hour Day Week

Latency
1.5
1

rhel2_u03 Details

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

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

Protect Volumes

PROTECTION POLICY: Asynchronous

Source

CLUSTER: onPrem
STORAGE VM: svm_onPrem
SELECTED VOLUMES: rhel2_u03

Destination

CLUSTER: hybridcvo
STORAGE VM: svm_hybridcvo

Destination Settings: 2 matching labels

VOLUME NAME: vol_<SourceVolumeName>_dest

PREFIX: vol_ SUFFIX: _dest

Override default storage service name

Configuration Details

Initialize relationship (?)

Enable FabricPool (?)

Save **Cancel**

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

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

6. Add CVO database storage SVM to SnapCenter

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

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

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

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

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

The screenshot shows the ONTAP Storage section of the NetApp SnapCenter interface. On the left is a navigation sidebar with options like Dashboard, Resources, Monitor, Reports, Hosts, Storage Systems, Settings, and Alerts. The main area displays a table titled 'ONTAP Storage Connections' with the following data:

Name	IP	Cluster Name	User Name	Platform	Controller License
sym_hybridcvo		10.0.0.1		CVO	✗
sym_onPrem		192.168.0.101		CVO	✓

7. Setup database backup policy in SnapCenter

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

Create a full database backup policy for Oracle

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

The screenshot shows the Policies section of the NetApp SnapCenter interface. The main area displays a table titled 'Oracle Database' with the following data:

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

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

Modify Oracle Database Backup Policy x

1 Name Provide a policy name

2 Backup Type Policy name: Oracle Full Online Backup i

3 Retention Details: Backup all data and log files

4 Replication

5 Script

6 Verification

7 Summary

Previous Next

The screenshot shows a step-by-step configuration interface for an Oracle Database Backup Policy. The current step is 'Name'. The policy name is 'Oracle Full Online Backup' and the details are 'Backup all data and log files'. The 'Next' button is highlighted in blue.

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. The main area is titled 'Select Oracle database backup options' and contains a section for 'Choose backup type'. Under 'Online backup', 'Datafiles, control files, and archive logs' is selected. There are also options for 'Datafiles and control files' and 'Archive logs'. Below this is another section for 'Choose schedule frequency' with 'Daily' selected. At the bottom right are 'Previous' and 'Next' buttons.

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

Modify Oracle Database Backup Policy

Retention settings

Daily retention settings
Data backup retention settings

Total Snapshot copies to keep

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 'Retention settings' section of the Oracle Database Backup Policy modification interface. It includes fields for daily data backup retention (14 days) and archive log retention (14 days). The 'Keep Snapshot copies for' option is selected for both.

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

Modify Oracle Database Backup Policy x

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Select secondary replication options i

Update SnapMirror after creating a local Snapshot copy.

Update SnapVault after creating a local Snapshot copy.

Secondary policy label Daily i

Error retry count 3 i

Previous Next

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

Modify Oracle Database Backup Policy X

1 Name

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

2 Backup Type

Prescript full path Enter Prescript path

3 Retention

Prescript arguments

4 Replication

Postscript full path Enter Postscript path

Postscript arguments

5 Script

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

[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

3. Select the backup type and schedule frequency.

New Oracle Database Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Select Oracle database backup options

Choose backup type

Online backup

Datafiles, control files, and archive logs

Datafiles and control files

Archive logs

Offline backup i

Mount

Shutdown

Save state of PDBs i

Choose schedule frequency

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

On demand

Hourly

Daily

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

The screenshot shows the 'New Oracle Database Backup Policy' configuration interface. The left sidebar lists steps 1 through 7. Step 2, 'Backup Type', is currently active. Under 'Choose backup type', 'Archive logs' is selected. Below it, 'Mount' is also selected under 'Choose schedule frequency'. Navigation buttons 'Previous' and 'Next' are at the bottom right.

4. Set the log retention period.



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

7 Summary

Verification script commands

Script timeout 60 secs

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

Prescript arguments Choose optional arguments...

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

Postscript arguments Choose optional arguments...

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

8. Summary.

New Oracle Database Backup Policy

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

Create a full database backup policy for SQL

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

The screenshot shows the NetApp SnapCenter web interface. On the left is a navigation sidebar with links for Dashboard, Resources, Monitor, Reports, Hosts, Storage Systems, Settings, and Alerts. The main area is titled "Policies" under the "Microsoft SQL Server" credential. It features a search bar labeled "Search by Name". Below the search bar are four filter dropdowns: "Name", "Backup Type", "Schedule Type", and "Replication". A message "There is no match for your search or data is not available." is displayed. At the bottom right of the main area are buttons for "New", "Modify", "Copy", "Details", and "Delete". The top right of the screen shows the user's name "demo\sqldba", their role "App Backup and Clone Admin", and "Sign Out".

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.

New SQL Server Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Retention settings

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

Keep log backups applicable to last full backups

Keep log backups applicable to last days

Full backup retention settings i

Daily

Total Snapshot copies to keep

Keep Snapshot copies for days

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

The screenshot shows the 'New SQL Server Backup Policy' wizard. The 'Retention' tab is selected. Under 'Retention settings', it specifies 'Keep log backups applicable to last 7 full backups'. Under 'Full backup retention settings', it specifies 'Total Snapshot copies to keep 7' daily. Navigation buttons 'Previous' and 'Next' are at the bottom.

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

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Prescript full path

Prescript arguments Choose optional arguments...

Postscript full path

Postscript arguments Choose optional arguments...

Script timeout 60 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

Prescript full path

Prescript arguments Choose optional arguments...

2 Backup Type

3 Retention

4 Replication

5 Script

Specify optional scripts to run after performing a backup job

Postscript full path

Postscript arguments Choose optional arguments...

Script timeout 60 secs

6 Verification

7 Summary

Previous Next

6. Summary.

New SQL Server Backup Policy

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

8. Implement backup policy to protect database

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

Create a resource group for full backup of Oracle

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

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

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



3. Add database resources to the resource group.



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



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



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



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



8. Summary.



Create a resource group for log backup of Oracle

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



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



3. Add database resources to the resource group.



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



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

Add schedules for policy Oracle Archive Log Backup x

Hourly

Start date

Expires on

Repeat every hours mins

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

Cancel OK

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

NetApp SnapCenter®

Oracle Database

New Resource Group

Name

Search resource groups

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

Configure verification schedules

Policy Schedule Type Applied Schedules Configure Schedules

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

Total 0

Previous Next

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



8. Summary.



Create a resource group for full backup of SQL Server

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

New Resource Group

Provide a name and tags for the resource group

Name	sql1_tpcc
Tags	sqfullbkup
<input checked="" type="checkbox"/> Use custom name format for Snapshot copy \$CustomText	
sql1_tpcc	

Total 5

Previous Next

2. Select the database resources to be backed up.

New Resource Group

Add resources to Resource Group

Host	Resource Type	SQL Server Instance
All	Databases	sql1

Available Resources

Selected Resources

search available resources

Auto select all the resources from the same storage volume

tpcc (sql1)

Total 5

Previous Next

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

New Resource Group

Select one or more policies and configure schedules

Policy	Applied Schedules	Configure Schedules
SQL Server Full Backup	None	+

Total 1

Use Microsoft SQL Server scheduler

Total 5

Previous Next

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



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



- Configure the SMTP server for email notification if desired.



7. Summary.



Create a resource group for log backup of SQL Server

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



2. Select the database resources to be backed up.



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



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



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



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



7. Summary.



9. Validate backup

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

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

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

public cloud.

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

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

The screenshot shows the 'Log In to NetApp Cloud Central' page. At the top, the NetApp logo is displayed. Below it, a blue link reads 'Continue to Cloud Manager'. The main title 'Log In to NetApp Cloud Central' is centered above two input fields. The first field contains the email address 'rt1600680@demo.netapp.com'. The second field is a password input field, indicated by a series of dots ('.....'). A large blue 'LOGIN' button is positioned below the inputs. At the bottom left, a link 'Forgot your password?' is visible.

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



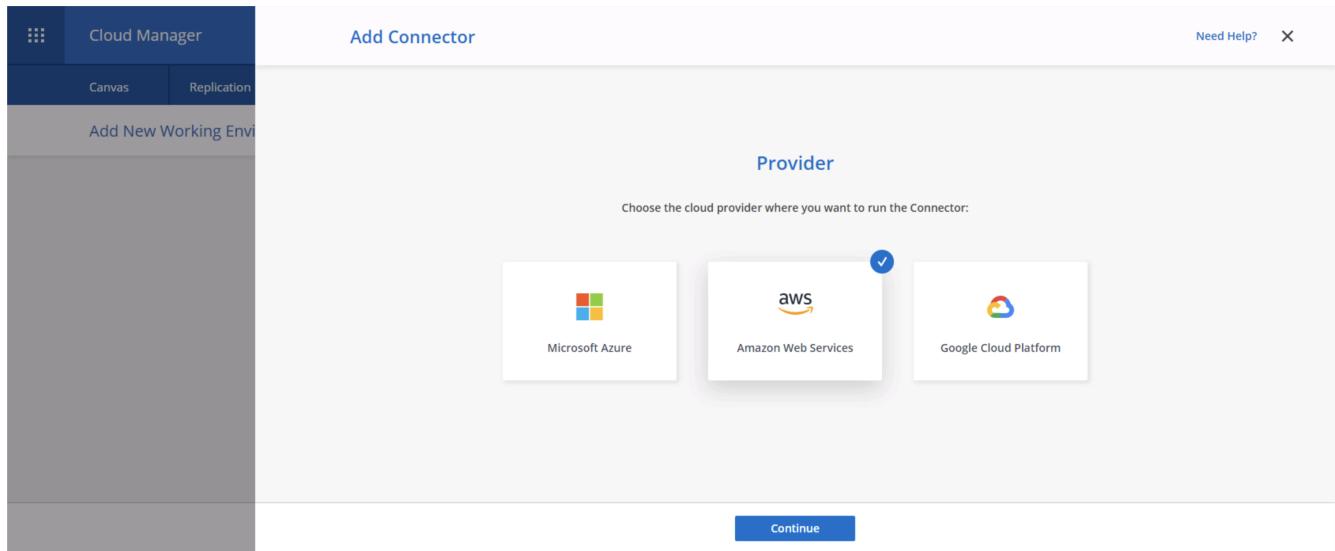
3. Click "Add Working Environment" and choose Cloud Volumes ONTAP in AWS. Here, you also choose whether you want to deploy a single node system or a high availability pair. I have chosen to deploy a high availability pair.



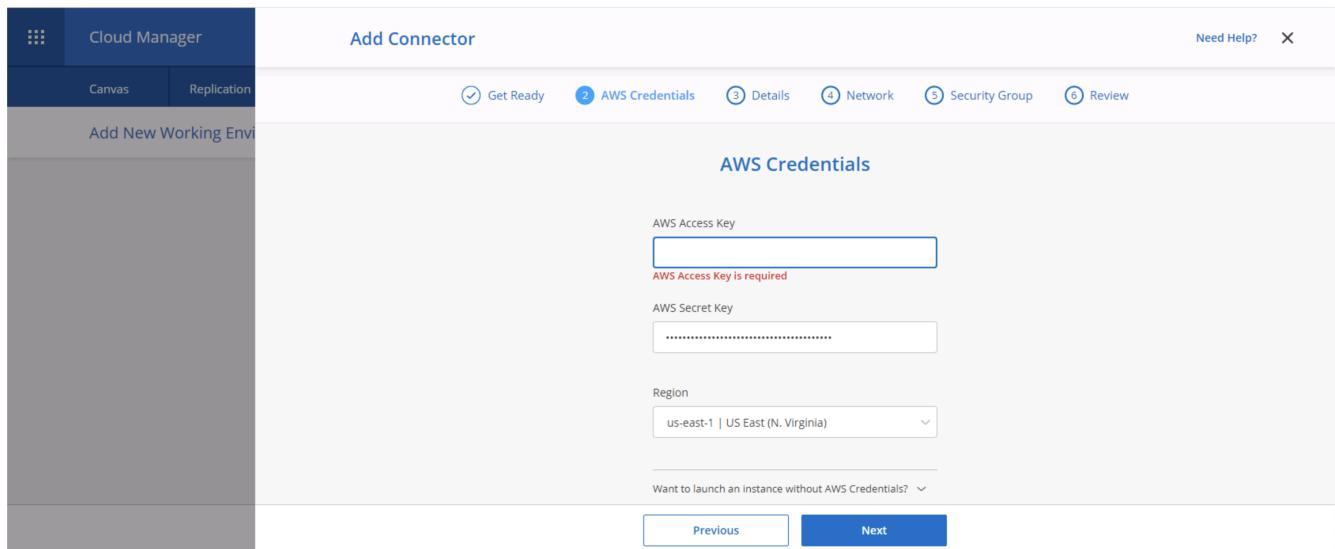
4. If no connector has been created, a pop-up appears asking you to create a connector.



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.

The screenshot shows the 'Add Connector' interface in Cloud Manager. The title bar says 'Add Connector'. Below it, a navigation bar has tabs: 'Get Ready' (checked), 'AWS Credentials' (checked), 'Details' (selected), 'Network', 'Security Group', and 'Review'. The main area is titled 'Details' and contains the following fields:

- Connector Instance Name:** awscloudmanager
- Connector Role:** Create Role (radio button selected)
- Role Name:** Cloud-Manager-Operator-IBNt24

At the bottom are 'Previous' and 'Next' buttons.

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

The screenshot shows the 'Add Connector' interface in Cloud Manager, specifically the 'Network' step. The title bar says 'Add Connector'. Below it, a navigation bar has tabs: 'Get Ready' (checked), 'AWS Credentials' (checked), 'Details' (checked), 'Network' (selected), 'Security Group', and 'Review'. The main area is titled 'Connectivity' and contains the following fields:

- 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

On the right side, there is a section for 'Proxy Configuration (Optional)' with a field for 'HTTP Proxy' (Example: http://172.16.254.1:8080).

At the bottom are 'Previous' and 'Next' buttons.

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.

The screenshot shows the Cloud Manager interface with the title 'Cloud Manager' at the top. The main navigation bar includes 'Canvas', 'Replication', 'Backup & Restore', 'K8s', 'Data Sense', 'File Cache', 'Compute', 'Sync', and 'All Services (+8)'. On the right, account information (Account: rt1600680, Workspace: Workspace-1, Connector: awscloudman...), settings, and help icons are visible. The central area is titled 'Create a New Working Environment' and 'Details and Credentials'. It shows an 'Instance Profile' section with 'Credential Name' set to '322944748816' and 'Account ID' set to 'Marketplace Subscription'. A button 'Edit Credentials' is present. Below this, there are two columns: 'Details' (Working Environment Name: 'Up to 40 characters') and 'Credentials' (User Name: 'admin', Password: empty, Confirm Password: empty). A 'Continue' button is at the bottom.

3. Choose Add Subscription.

The screenshot shows the 'Edit Credentials & Add Subscription' dialog box. It has a header 'Edit Credentials & Add Subscription' and a sub-header 'Associate Subscription to Credentials'. It displays a 'Credentials' section with 'Instance Profile | Account ID: 322944748816'. Below it is a 'Marketplace Subscription' section with a note 'No subscription is associated with this credential'. A 'Add Subscription' button is available. At the bottom are 'Apply' and 'Cancel' buttons.

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

The screenshot shows the 'Edit Credentials & Add Subscription' dialog box again, this time with a note: 'Select a subscription option and click Continue. The AWS Marketplace enables you to view pricing details and then subscribe.' Two options are shown: 'Pay-Per-TiB - Annual Contract' (radio button not selected) and 'Pay-as-you-go' (radio button selected). Below the options, a section 'The next steps:' lists: '1 AWS Marketplace' (Subscribe and then click Set Up Your Account to configure your account.) and '2 Cloud Manager' (Save your subscription and associate the Marketplace subscription with your AWS credentials.). At the bottom are 'Continue' and 'Cancel' buttons.

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

The screenshot shows the AWS Marketplace product page for 'Cloud Manager - Deploy & Manage NetApp Cloud Data Services' by NetApp, Inc. The page includes a search bar, navigation links (About, Categories, Delivery Methods, Solutions, AWS IQ, Resources, Your Saved List), and a user profile (Hello, rt1600680). The main content area displays the product title, vendor information, a brief description, and a 'Continue to Subscribe' button. Below the main content are tabs for Overview, Pricing, Usage, Support, and Reviews. A 'Product Overview' section details the platform's features, including Cloud Volumes ONTAP, Cloud Backup, Cloud Tiering, Cloud Data Sense, and Cloud Manager. A 'Highlights' section lists benefits such as streamlining deployment and centralizing management. A note at the bottom states that the product is offered as NetApp Cloud Data Services including their virtual and hardware storage nodes.

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 subscription confirmation page for the same product. It displays a message about being subscribed to multiple offers and provides a dropdown menu to select a specific offer. A callout box asks if there are issues signing up and provides a link to the registration area. To the right, a summary box titled 'You Have Subscribed to a Private Offer' details the subscription status, including the offer ID, expiration date (August 1, 2022 UTC), and billing information. A 'Subscribe' button and a note about accepting the EULA are also present.

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



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



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



- Enter the working environment details such as:

- a. Cluster name

b. Cluster password

c. AWS tags (Optional)

The screenshot shows the 'Cloud Manager' interface with the title 'Create a New Working Environment'. The top navigation bar includes 'Account: rt1600680', 'Workspace: Workspace-1', 'Connector: awscloudman...', and various icons. Below the title, there are tabs for 'Canvas', 'Replication', 'Backup & Restore', 'K8s', 'Data Sense', 'File Cache', 'Compute', 'Sync', and 'All Services (+8)'. The main form is titled 'Details and Credentials'. It contains fields for 'Instance Profile' (322944748816), 'Credential Name' (demo.netapp.com-cloud-vol...), 'Account ID' (rt1600680), and 'Marketplace Subscription'. A 'Edit Credentials' button is present. The 'Details' section has a 'Working Environment Name (Cluster Name)' field containing 'hybridawsco'. 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 'Cloud Manager' interface with the title 'Create a New Working Environment'. The top navigation bar includes 'Account: rt1600680', 'Workspace: Workspace-1', 'Connector: awscloudman...', and various icons. Below the title, there are tabs for 'Canvas', 'Replication', 'Backup & Restore', 'K8s', 'Data Sense', 'File Cache', 'Compute', 'Sync', and 'All Services (+8)'. The main form is titled 'Services'. It contains three service options with toggle switches: 'Data Sense & Compliance' (on), 'Backup to Cloud' (on), and 'Monitoring' (on). A 'Continue' button is at the bottom.

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

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 HA Deployment Models X

↑ Previous Step

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.

Extended Info

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.

Extended Info

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

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

Cloud Manager

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 Region & VPC X

↑ Previous Step

AWS Region: US East | N. Virginia

VPC: vpc-083fcbd79f75dfb6e - 10.221.0.0/16

Security group: Use a generated security group

Node 1:	Node 2:	Mediator:
Availability Zone: us-east-1a	Availability Zone: us-east-1b	Availability Zone: us-east-1c
Subnet: 10.221.1.0/24	Subnet: 10.221.2.0/24	Subnet: 10.221.3.0/24

Continue

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

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

Cloud Manager

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 Connectivity & SSH Authentication X

↑ Previous Step

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

Continue

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



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

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

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

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

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

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

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

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

Cloud Manager

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

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

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

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

Default Master Key: aws/ebs

[Continue](#)

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

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

Cloud Manager

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

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

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

[Learn more about our charging methods](#)

Pay-As-You-Go by the hour

Bring your own license

Freemium (Up to 500GB)

NetApp Support Site Account (*Optional*)

[Learn more about NetApp Support Site \(NSS\) accounts](#)

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

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

[Add Netapp Support Site Account](#)

[Continue](#)

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

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

Cloud Manager

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

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

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

 POC and small workloads
Up to 2TB of storage

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

 Cost effective DR
Up to 10TB of storage

 Highest performance production workloads
Up to 368TB of storage

[Continue](#)

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

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

Cloud Manager

Create a New Working Environment Create Volume

↑ Previous Step Details & Protection Protocol

Volume Name: Size (GB): Volume size

Snapshot Policy: default

Access Control: Custom export policy

Custom export policy: 10.221.0.0/16

Advanced options

Continue Skip

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

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

Cloud Manager

Create a New Working Environment Review & Approve

↑ Previous Step 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.

The screenshot shows the Cloud Manager Canvas interface. At the top, there are tabs for Canvas, Replication, Backup & Restore, K8s, Data Sense, File Cache, Compute, Sync, and All Services (+8). The Canvas tab is selected. In the center, there's a diagram of a hybrid cluster setup. On the left, a cloud icon labeled 'hybridawsenv' contains 'Cloud Volumes ONTAP' and 'Initializing'. On the right, another cloud icon labeled 'Amazon S3' shows '1 Buckets' and '1 Region'. Below the diagram are 'Add Working Environment' and 'Working environments' sections. The 'Working environments' section lists '1 Cloud Volumes ONTAP (High-Availability)' and '0 B Allocated Capacity' under a cloud icon, and '1 Amazon S3' with '0 Buckets' under a trash bin icon. A zoom-in and zoom-out button is at the bottom right.

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

The screenshot shows the Cloud Manager main dashboard. At the top, there are tabs for Canvas, Replication, Backup & Restore, K8s, Data Sense, File Cache, Compute, Sync, and All Services (+8). The Canvas tab is selected. Below the tabs, there are sections for 'Resources' and 'Services'. The 'Resources' section includes 'Canvas' (Review CVO, CVS, ANF & On-Premises), 'Digital Wallet' (View & Manage Digital Wallet), and 'Timeline' (View Activity & Events). The 'Services' section includes 'Replication' (Data Replication), 'Backup & Restore' (Data Protection for CVO and On-Premises), 'K8s' (Cloud Native Development), 'Data Sense' (Data Governance & Compliance), 'Compliance' (Privacy & Compliance Controls), 'Tiering' (Lift and DON'T shift), 'Monitoring' (Monitor, Optimize and Secure), 'File Cache' (Consolidate your Data into the Cloud), 'Compute' (Optimize your cloud spend), 'Sync' (Automated Data Synchronization), 'SnapCenter' (Application Data Management), and 'Active IQ' (Digital Advisor). A link to the Timeline at <https://cloudmanager.netapp.com/timeline> is also present.

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 tabs for Canvas, Replication, Backup & Restore, K8s, Data Sense, File Cache, Compute, Sync, and All Services (+8). The Timeline section has a filter bar with options: Time (1), Service, Action, Agent (1), Resource, User, Status, and Reset. Below the filter is a table with columns: Time, Action, Service, Agent, Resource, User, and Status. The table contains three rows of log entries:

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. At the top, there are tabs for Canvas, Replication, Backup & Restore, K8s, Data Sense, File Cache, Compute, Sync, and All Services (+8). The main area displays a cloud diagram representing a hybrid environment. On the left, a cloud icon labeled 'hybridawscvo' contains 'Cloud Volumes ONTAP' and '1 GiB Capacity'. On the right, another cloud icon labeled 'aws' contains 'Amazon S3' and '2 Buckets | 1 Region'. To the right of the diagram is a sidebar titled 'Working environments' listing:

- 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.

SERVICES



Replication

■ Off

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 bottom section.

Replicate.

This screenshot is similar to the one above but includes a dropdown menu. The 'Replication' service section has a blue arrow pointing down to a box containing two items: 'View Replications' and 'Replicate'. Both items have blue circular icons to their left. The rest of the interface is identical to the first screenshot.

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



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

Replication Setup				Source Volume Selection			
rhel2_u03	INFO Storage VM Name: svm_onPrem Tiering Policy: None Volume Type: RW	CAPACITY 100 GB Allocated / 7.29 GB Disk Used	ONLINE	rhel2_u03 09232119421203118	INFO Storage VM Name: svm_onPrem Tiering Policy: None Volume Type: RW	CAPACITY 100 GB Allocated / 35.83 MB Disk Used	ONLINE
sql1_data	INFO Storage VM Name: svm_onPrem Tiering Policy: None Volume Type: RW	CAPACITY 53.37 GB Allocated / 45.09 GB Disk Used	ONLINE	sql1_log	INFO Storage VM Name: svm_onPrem Tiering Policy: None Volume Type: RW	CAPACITY 21.35 GB Allocated / 18.16 GB Disk Used	ONLINE
sql1_snapctr	INFO Storage VM Name: svm_onPrem Tiering Policy: None Volume Type: RW	CAPACITY 24.87 GB Allocated / 21.23 GB Disk Used	ONLINE				

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

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

3. Deploy EC2 compute instance for database workload

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

Sizing the compute instance

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

Linux instance configuration for Oracle workload

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

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

Windows instance configuration for SQL Server workload

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

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

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

Copyright information

Copyright © 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.