

Getting started overview

NetApp Solutions

NetApp July 31, 2024

This PDF was generated from https://docs.netapp.com/us-en/netappsolutions/databases/hybrid_dbops_snapcenter_getting_started_onprem.html on July 31, 2024. Always check docs.netapp.com for the latest.

Table of Contents

Setting 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

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

On-premises

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

AWS public cloud

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

Click the following links for details:

On Premises, Public Cloud - AWS

Getting started on premises

The NetApp SnapCenter tool uses role based access control (RBAC) to manage user resources access and permission grants, and SnapCenter installation creates prepopulated roles. You can also create custom roles based on your needs or applications.

On Premises

1. Setup database admin user in SnapCenter

It makes sense to have a dedicated admin user ID for each database platform supported by SnapCenter for database backup, restoration, and/or disaster recovery. You can also use a single ID to manage all databases. In our test cases and demonstration, we created a dedicated admin user for both Oracle and SQL Server, respectively.

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

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

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

п	NetApp Snap(Center®								•	8 9	- L demo\administrator	SnapCenterAdmin	🖡 Sign Out
<		Global Settir	igs Policies	Users and Access	Roles	Credential	Software							
	Dashboard	Search by	Name					Type All	.				Add	
	Resources		Name		1	🛓 Туре		Roles					Domain	
	Monitor		administrator			User		SnapCenterAdmin					demo	
			oradba			User		App Backup and Clone Admin					demo	
ŝ	Reports		<u>sqldba</u>			User		App Backup and Clone Admin					demo	
A	Hosts													
h	Storage Systems													
	Settings													
	Alerts													

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.
- 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.
- $\circ\,$ The RBAC DB admin user must have both the resource group and backup privileges.

Unix host for Oracle:

- 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.

	NetApp Snap(enter®		٠		8 -	L demo\administrator	SnapCenterAdmin	🖡 Sign Out	
<		Global Settings Policies Users and Access Roles Cree	iential Software							
	Dashboard									
V	Resources	Global Settings								
	Monitor									
ŝ	Reports	ervisor Settings 👔								
*	Hosts	VMs have ISCSI direct attached disks or NFS for all the hosts Update	ite							
ł۹	Storage Systems	Notification Server Settings 0							~	
	Settings	Configuration Settings ()							~	
A	Alerts	Purge Jobs Settings ()							~	
		Domain Settings 1							~	
		CA Certificate Settings 1							~	

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."

	NetApp Snap	Center	r®					٠		0-	1 den	10\administrato	r SnapCenterAdmir	🛙 🖡 Sign Out
<		Mana	aged Hosts Disks Shares Initiator Groups it											
	Dashboard	Sea	arch by Name 🛛 🗸									Add		More
ę	Resources		Name	15	Туре	System	Plug-in		Ven	sion	¢	overall Status		
9	Monitor		rhel2.demo.netapp.com		Linux	Stand-alone	UNIX, Oracle Database		4.5		1	Running		
			sgl1.demo.netapp.com		Windows	Stand-alone	Microsoft Windows Server, Microsoft SQL Server		4.5		2	Running		
ŵ	Reports		sql-standby.demo.netapp.com		Windows	Stand-alone	Microsoft Windows Server, Microsoft SQL Server		4.5			Configure lo	g directory	
2	Hosts													
ł	Storage Systems													
#	E Settings													
4	Alerts													

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

n Ne	tApp	SnapCenter®					٠	8-	1 demo\administrator	SnapCenterAdmin	🖡 Sign Out
>	Mana	ged Hosts									
	Sea	rch by Name		Host Details							
		Name	臣	Host Name	sql-standby.demo.netapp.com	Alorte					
		rhel2.demo.netapp.com		Host IP	10.221.2.56	Alerts					
		sgi1.demo.netapp.com		Overall Status	Configure log directory	No Alerts					
<i>~</i>		sgl-standby.demo.netapp.com		Host Type	Windows						
Δ.,				System	Stand-alone						
} •				Credentials	Domain Admin 🖋						
幸				Plug-ins	SnapCenter Plug-ins package 4.5.0.6123 for Windows						
▲					Microsoft Windows Microsoft SQL Server <u>Remove Configure log directory</u>						
				More Options : P	ort, gMSA, Install Path, Add Plug-Ins						
				Submit Cancel	Reset						

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

Configure Plug-	in for SQL Server		×
Configure the log l	backup directory for sql-standby.demo.netapp.com		
Configure host log	directory		
Host log directory	dedicated disk directory path	Browse	
		Save	Close

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

Configure Plug-in for SQL Server	×										
Configure the log backup directory for sql-standby.demo.netapp.com											
Configure host log directory											
Host log directory G:\	Browse										
Choose directory on NetApp Storage											
 sql-standby.demo.netapp.com G:\ System Volume Information 											
	Save Close										

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.

i

п	NetApp Snap	Center@	B							٠	•	0-	▲ demo\administrator	SnapCenterAdmin	🗊 Sign Out
<		Manag	ed Hosts Disks	Shares	Initiator Groups										
	Dashboard	Searc	ch by Name	V									Add		More
9	Resources		Name			IL.	Туре	System	Plug-in				Version	Overall Status	
-	Monitor		rhel2.demo.neta	app.com			Linux	Stand-alone	UNIX, Oracle Database				4.5	Running	
			sql1.demo.netap	<u>op.com</u>			Windows	Stand-alone	Microsoft Windows Server, Microsoft SQL Server				4.5	Running	
â	Reports		sql-standby.dem	no.netapp.com			Windows	Stand-alone	Microsoft Windows Server, Microsoft SQL Server				4.5	Running	
A	Hosts														
÷	Storage Systems														
霊	Settings														
▲	Alerts														

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

NetApp Sna	pCenter®					●	L demo\administrato	SnapCenterAdmin	Sign Out
/	Global Setting	gs Policies Users and Access Roles Credential	Software						
Dathboard	Search by N	lame		Type All	-			-	
Dashboard		Name [1]	Туре	Roles			D	Add omain	Remove
		administrator	User	SnapCenterAdmin			de	emo	
Monitor		oradba	User	App Backup and Clone Admin			de	emo	
Reports		soldba	User	App Backup and Clone Admin			de	emo	
Hosts									
Storage System	s								
Settings									
Alerts									
Assig	gn Ass	sets							×
_									_
Accet -	Turne	Llost	-		conreb				
Asset	Type	HOSE	•		Search				
	Accet	Name							15
	Asset	Name							1E
	rhel2	.demo.netapp.com							
	sql1.0	demo.netapp.com							
	sql-st	andby.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.

					٠		L demo\administrator	SnapCenterAdmin	🖡 Sign Out
									×
Add Host									
Host Type	Linux]							
Host Name	ora-standby								
Credentials	admin 👻	+ 0							
Select Plug-ins to Inst	all SnapCenter Plug-ins Package 4.5 for Linux								
	Oracle Database SAP HANA								
More Options : Po	rt, 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 Installation Path	8145 /opt/NetApp/snapcenter Skip preinstall checks Add all bosts in the oracle RAC	0
Custom Plug-ins —	Choose a File Upload No plug-ins found.	*
	Save	ncel

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 de	termined 🕕	
Host name 타	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.

п	NetApp Snap	1 demo\administrator	SnapCenterAdmin	🖡 Sign Out							
<		Manag	ed Hosts Disks Shares Initiator Groups i	SCSI Session							
	Dashboard	Searc	ch by Name 🛛 🍸						+ 		More
	Resources		Name	45	Туре	System	Plug-in		Version	Overall Status	
•	Monitor		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	
â	Reports		sgl1.demo.netapp.com		Windows	Stand-alone	Microsoft Windows Server, Microsoft SQL Server		4.5	Running	
A	Hosts		sql-standby.demo.netapp.com		Windows	Stand-alone	Microsoft Windows Server, Microsoft SQL Server		4.5	Running	
ł	Storage Systems										
=	Settings										
A	Alerts										

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

	etApp SnapCenter®				♠ ≅ ⊖-	L demo\administrator SnapCenterAdmin	🖡 Sign Out
	Users and Access	Users/Groups Details					
	Search by Name						
	Nama	User Name or	radba				
V	administrator	Roles	Ann Backun and Clone Admin				
*	oradba	Noico C					
âÂ	Soldba	Accian Accets					
A.		100051100000				+ Assign	Unassign
34		Asset Name		15	Туре	Asset Type	S. I.O.S. I.G.
		10.0.0.1			DataOntapCluster	Storage Connection	
Δ		192.168.0.10	n		DataOntapCluster	Storage Connection	
-		admin				Credentials	
		Linux Admin				Credentials	-
		Oracle Archiv	ve Log Backup			Policy	
		Oracle Full O	nine Backup			Policy	-
		Submit Cancel					
		Submit					
							~
1	Assign Assets						×
	0						
1							
	Asset Type Host	t	•	seard	ch		
1							
1	Asset Name						11
	ora-standby	.demo.netan	p.com				
	rhel2 demo	netann com					
		incupp.com					
1	sal1 demo	netann com					
	sqn.uenio.i	ictapp.com					
	sal_standby	domo notan	n com				
	sqrstanuby	.uemo.netap	p.com				
1							
1							
1							
						Save Close	2

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.

	NetApp Snap(Center	B		•		 🧘 demo\oradba	App Backup and Clo	ne Admin	🖡 Sign Out		
<		Oracle	Database -									
	Dashboard	View	Database	Search databa	ases V					Refre	ah Resources	New Resource Group
Ø	Resources	- The	Name	Oracle Database Type	Host/Cluster	Resource Group	Policie	es		Last Backup	Overall !	Status
	Monitor		cdb2	Single Instance (Multitenant)	rhel2.demo.netapp.com						Not prof	tected
<i>i</i> ii	Reports											
٨	Hosts											
ł	Storage Systems											
ŧ	Settings											
	Alerts											

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.

п	NetApp Snap	Center®	👤 demo\sqldba	App Backup a	and Clone Admin	🗊 Sign Out							
<			SQL Server 👻										
	Dashboard	View D	atabase • search by name	V								Refresh Resources	New Resource Group
0	Resources	12.10	Name	Instance	Host	Last Backup	Ov	erall Sta	atus		Туре		
•	Monitor		master	sql1	sql1.demo.netapp.com		No	t availa	ble for b	ackup	System	database	
			model	sql1	sql1.demo.netapp.com		No	t availa	ble for b	lackup	System	database	
â	Reports		msdb	sql1	sql1.demo.netapp.com		No	t availa	ble for b	ackup	System	database	
-	Hosts		tempdb	sql1	sql1.demo.netapp.com		No	t availa	ble for b	lackup	System	database	
÷	Storage Systems		tpcc	sql1	sql1.demo.netapp.com	09/14/2021 2:35:07 PM 🛱	Ba	ckup su	cceeded	i .	User da	atabase	
=	Settings												

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.

	NetApp SnapC	Center®						٠		8-	👤 demo\sqldba	App Backup and Clone Admin	🖡 Sign Out
			QL Server										
	Dashboard	View Inst	tance 🝷	search by name	V							Refresh Resources	New Resource Group
	Resources	12.14	Name		Host	Resource Groups	Policies	Sta	ate			Туре	
٠	Monitor	â	sql-standby		sql-standby.demo.netapp.com			Ru	inning			Standalone ()	
14	Penorte		sql1		sql1.demo.netapp.com			Ru	inning			Standalone (15.0.2000)	
	Reports												
•	Hosts												
50	Storage Systems												
橆	Settings												
A	Alerts												
_	latter Coast	-antar@							-	0-	• demolandaller	And Dealure and Chara Admin	Ec- ot
	Microroft SOLS			Instance Credentials					-		L demo-sqiuba	лрр васкир ани сюпе липш	o sign out
>	microsoft SQL 3			instance - credendals									
=	search by nar	me											Add Credential
0	Name			i The Microsoft SQL ser	rver or Windows credentials are neccessary to	unlock the selected instance. Click Refresh Re-	sources to run a discovery with the associated	l Auth.					×
۲	sql-standby			Name		sql-standby							
M	sql1			Resource Group		None							
ant				Policy		None							
A				Selectable		🖱 Not available for backup. DB is	not on NetApp storage, auto-close is enabled	l or in r	ecovery	mode.			
10													
華													
A													

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.

	letApp SnapCenter® • 🖬 😔 😔 1 demolsalidaa App Backup												
<		Microsoft S	QL Server 🗧										
	Dashboard	View Ins	tance • search by name	V								Refresh Resources	New Resource Group
۵	Resources	15 (m	Name	Host	Resource Groups	Policies	Stat	e			Туре		
۲	Monitor		sql1 sql1.demo.netapp.com								Standa	lone (15.0.2000)	
12	Benorte	sql-standby sql-standby.demo.netapp.com					Run	ining			Standa	lone (15.0.2000)	
-	Reports												
ň	Hosts												
20	Storage Systems												
靀	Settings												
▲	Alerts												

5. Setup storage cluster peering and DB volumes replication

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

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

On-premises cluster:

≡ 🔲 ONTAP Sy	vstem Manager (Return to class	sic version)				ages Q			? <	> -	. 8
DASHBOARD	Overview										
STORAGE 🗸	IPspaces			+	Broadcast Domains					+	
Overview	Cluster	Broadcast Domains Cluster			Cluster	9000 MTU IP	space: Cluster				
Ethernet Ports FC Ports	Default	Storage VMs			Default	1500 MTU IP or	space: Default Prem-01 e0a e0b e0c e0d e0i	e eOf eOg eOh eOg-100 eOe-20	0 e0f-201		
EVENTS & JOBS V		Broadcast Domains Default									
Overview									-		
Relationships	Network Interfaces	Statur 着	Storage VM	IBrnaco	Addrore	Current Node	Current Port	Brotocole	+	₹ Filte	ž.
SAN Initiator Groups NVMe Subsystem	onPrem-01_IC		JUIAGE VIII	Default	192.168.0.113	onPrem-01	e0b	Protocols	Intercluster		
	onPrem-01_mgmt1	0		Default	192.168.0.111	onPrem-01	e0c		Cluster/Node Mgn	nt	
Overview	cluster_mgmt	0		Default	192.168.0.101	onPrem-01	e0a		Cluster/Node Mgn	nt	

Target CVO cluster:

≡	ONTAP Sy	stem Manager				Search act	ions, objects, and p	oages Q				? <>	± #
DAS	HBOARD	Overview											ч
STO	RAGE 🗸												
NET	WORK ^	IPspaces			+		Broadcast Do	omains					
Over Ethe	view rnet Ports	Cluster	Broadcast Domains Cluster				Cluster	9000 M	TU IPspace: Cluster hybridcvo-01 e0b				
EVE	NTS & JOBS 💙	Default	Storage VMs				5-6-14	2001 14	The second particular				
PRO	TECTION V		svm_hybridevo Broadcast Domains				Delautt	9001 M	hybridevo-01 e0a				
но	its 🗸		Default						nybridcvo-uz eua				
CLU	ster ~	Network Interfaces								+ Q Search	➡ Download	how/Hide 🥆	
		Name ≑	Status	Storage VM	IPspace	Add	ress	Current Node	Current Port	Protocols	Туре	Through	put (I
		hybridcvo-02_mgmt1	0		Default	10.2	21.2.104	hybridcvo-02	e0a		Cluster/Node Mgmt		0
		inter_1	0		Default	10.2	21.1.180	hybridevo-01	e0a		Intercluster,Cluster/Node Mgmt		0.02
		inter_2	0		Default	10.2	21.2.250	hybridcvo-02	e0a		Intercluster,Cluster/Node Mgmt		0.03
		iscsi_1	0	svm_hybridcvo	Default	10.2	21.1.5	hybridcvo-01	e0a	ISCSI	Data		0
		iscsi_2	0	svm_hybridcvo	Default	10.2	21.2.168	hybridcvo-02	e0a	ISCSI	Data		0

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

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

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

≡ ∎ ONTAP Sy	ystem Manager (Return to classic version)				ects, and pages Q
Overview Applications Volumes LUNs NVMe Namespaces Shares Qtrees Quotas Storage VMs Tiers NETWORK	UI Settings Log Level Debug INACTIVITY TIMEOUT 30 minutes	,			
Overview Ethernet Ports FC Ports	Intercluster Settings				
EVENTS & JOBS × PROTECTION ^ Overview Relationships HOSTS × CLUSTER ^ Overview Settings	Network Interfaces	+	Cluster Peers PEERED CLUSTER NAME Mybridevo Genera Manag	i Cluster ate Passphrase ge Cluster Peers	Storage VM Peers PEERED STORAGE VMS

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

≡ ■ ONTAP S	/stem Manager (Return to classic version)					۹	
DASHBOARD	Volumes						
STORAGE ^	+ Add Tolete Protect	More					
Overview	Name	rhel2 u03 All Volumes					
Applications Volumes	onPrem_data						
LUNs	rhel2_u01	Overview Snap	oshot Copies Clo	one Hierarchy	SnapMirror (Local or Ren	note)	
NVMe Namespaces	rhel2_u02						
Shares Qtrees	rhel2_u03	STATUS		Capacity			
Quotas	rhel2_u030923211942120311 8	Online					
Storage VMs		FlexVol		00/ 100/	2004 2004	4004	500/
	squ_uata	MOUNT PATH			2070 3070	4070	50%
NETWORK A	sql1_log	STOPACE NM		0 Bytes Available	2.36 GB Used 2.36 GB O	verflow	
Overview Ethernet Ports	sql1_snapctr	svm_onPrem					
FC Ports	svm_onPrem_root	LOCAL TIER					
EVENTS & JOBS 🗸		onPrem_01_SSD_1					
		default		Performance			
		QUOTA		Hour	Day		Week
HOSTS V		Off		Latency			
CLUSTER V		Read Write		1.5			
		SPACE RESERVATION		1			

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

ONTAP System Manager (Return to classic vi	Asion) Search actions, objects, and pages Q
DASHBOARD	Protect Volumes ×
STORAGE ^	PROTECTION POLICY Asynchronous
Applications Volumes	Source Destination
LUNs NVMe Namespaces	cLUSTER CLUSTER onPrem hybridcvo ~
Shares Qtrees	STORAGE VM SVM_ON/Prem STORAGE VM SVM_ON/Prem STORAGE VM SVM_hybridevo
Quotas Storage VMs Tiers	rhel2_u03 Destination Settings
NETWORK ^	VOLUME NAME PREFIX SUFFIX
Ethernet Ports	vol_ <sourcevolumename> _dest</sourcevolumename>
EVENTS & JOBS Y	Override default storage service name Configuration Details
PROTECTION V HOSTS V	✓ Initialize relationship ⑦
CLUSTER V	Save Cancel

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

Volum	ies							
+ Add	Delete Protect IN	fore						⊤ Filter
•	Name	rhel2_u03 All Volumes					/ E	dit i More
	onPrem_data							
	rhel2_u01	Overview Snapshot	Copies Clone Hierarchy	SnapMirror (Local or Remote)				
	rhel2_u02							
	rhel2 u03	Source	Destination	Protection Policy	Relationship Health	Relationship Status	Lag	
-	rhel2_0030923211942120311	svm_onPrem:rhel2_u03	svm_hybridcvo:rhel2_u03_dr	MirrorAllSnapshots	🕑 Healthy	Mirrored	12 seconds	
	8							

6. Add CVO database storage SVM to SnapCenter

- 1. 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.

n Ne	tApp S	SnapCenter®					•	••	1 demo\administrator	SnapCenterAdmin	🖡 Sign Out
<u> </u>	ONTAP S	Storage		Add Storage System							×
				Add Storage System 1	•						
V	ONTAR	Storage Connections		Storage System	10.0.0.1]					
٠		Name	Æ	Username	admin]					
<i>.</i>		svm hybridcvo		Password]					
		svm_onPrem									
•				Event Management Sy	ystem (EMS) & AutoSupport Settings						
20 A				Send AutoSuppor	t notification to storage system						
莘	Log SnapCenter Server events to syslog Amore Options : Platform, Protocol, Preferred IP etc										
▲											
				Submit Cancel	Reset						

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

More Options		×
Platform	Cloud Volumes ON 👻 Secondary 🚺	
Protocol	HTTPS 🔻	
Port	443	
Timeout	60 seconds ()	
Preferred IP		0
Save Cance	•1	

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

п	n NetApp SnapCenter® 🔹 🗗 🕹 t demokudministrator SnapCenterAdmin 🖡 Sign									🖡 Sign Out	
<		ONTAP	Storage								
	Dashboard	Туре	ONTAP SVMs								
V	Resources	ONTAP Storage Connections									
-	Monitor		Name IL	IP	Cluster Name	User Name		Plat	orm Cont	roller License	
11	Reports		svm hybridevo		10.0.0.1			CVO	0		
	Hosts		svm_onPrem		192.168.0.101			CVO	~		
þ	Storage Systems										
	Settings										
	Alerts										

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.

	n NetApp SnapCenter® • 🖬 🕫 🗘 demokerad								adba App Backup and Clone Admin 🖡 Sign Ou			🛿 Sign Out
		Policies Credential										
	Dashboard	Oracle Database										100
Ę	Resources	Search by Name						New	Modify	Capy	Dessis	Determ
4	Monitor	Name 11	Backup Type	Schedule Type	Replication				Verificatio	n		
	8 -	Oracle Archive Log Backup	LOG, ONLINE	Hourly	SnapMirror							
â	Reports	Oracle Full Online Backup	FULL, ONLINE	Daily	SnapMirror							
ł	Hosts											
\$	Storage Systems											
-1-7	Ξ Settings											
4	Alerts											

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

Modify Oracle Database Backup Policy							
1 Name	Provide a policy na	Provide a policy name					
2 Backup Type	Policy name	Oracle Full Online Backup	0				
3 Retention	Details	Backup all data and log files					
4 Replication							
5 Script							
6 Verification							
7 Summary							
		Previous	Next				

3. Select the backup type and schedule frequency.

Modify Oracle	Database Backup Policy	×
1 Name	Select Oracle database backup options	-
2 Backup Type	Choose backup type	
3 Retention	Online backup	
4 Replication	Datafiles, control files, and archive logs	
5 Script	○ Datafiles and control files	
6 Verification	○ Archive logs	
7 Summary	O Offline backup 🚯	
	◯ Shutdown	
	Save state of PDBs 🕕	
	Choose schedule frequency	
	Select how often you want the schedules to occur in the policy. The specific times are set at backup job creation enabling you to stagger your start times.	
	🔿 On demand	
	⊖ Hourly	
	Daily	*
	Previous Next	

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

Modify Oracle I	Database Backup Policy					×
1 Name	Retention settings ()					
2 Backup Type	Daily retention settings					
3 Retention	 Total Snapshot copies to keep 	7				
4 Replication	Keep Snapshot copies for	14	days			
5 Script	Archive Log backup retention settings	7				
6 Verification	Keep Snapshot copies for	14	days			
7 Summary						
					Previous N	lext

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	×
1 Name	Select secondary replication options 1	
2 Backup Type	☑ Update SnapMirror after creating a local Snapshot copy.	
3 Retention	Update SnapVault after creating a local Snapshot copy.	
4 Replication 5 Script	Secondary policy label Daily Error retry count 3	
6 Verification		
7 Summary		
	Previou:	s Next

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

Modify Oracle [Database Backup	Policy			×					
1 Name	Name Specify optional scripts to run before and after performing a backup job									
2 Backup Type	Prescript full path	/var/opt/snapcen	/var/opt/snapcenter/spl/scripts/ Enter Prescript path							
3 Retention	Prescript arguments									
4 Replication	Postscript full path	/var/opt/snapcen	ter/spl/scripts/	Enter Postscript path						
5 Script	Postscript arguments									
	Script timeout	60 se	ecs							
6 Verification										
7 Summary										
					Previous Next					

7. Run backup verification if desired.

Modify Oracle I	Database Backup	Policy			×					
1 Name	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.									
A Replication	ation Daily									
5 Script	5 Script Verification script commands									
6 Verification	Script timeout	60	secs							
	Prescript full path Prescript arguments	/var/opt/sna	pcenter/spl/scripts/	Enter Prescript path						
3 Summary		Choose optional arguments								
	Postscript full path	/var/opt/snapcenter/spl/scripts/		Enter Postscript path						
	Postscript	'ostscript choose optional arguments								
				Previous	ext					

8. Summary.

	• (198)	
Name	Summary	
Backup Type	Policy name	Oracle Full Online Backup
Detection	Details	Backup all data and log files
Retention	Backup type	Online backup
Replication	Schedule type	Daily
	RMAN catalog backup	Disabled
Script	Archive log pruning	None
Verification	On demand data backup retention	None
	On demand archive log backup retentio	n None
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

Create a database log backup policy for Oracle

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

New Oracle Database Backup Policy							
1 Name	Provide a policy na	ame					
2 Backup Type	Policy name	Oracle Archive Log Backup	1				
3 Retention	Details	Backup Oracle archive logs					
4 Replication							
5 Script							
6 Verification							
7 Summary							
		Previous	Next				

3. Select the backup type and schedule frequency.

New Oracle Da	atabase Backup Policy	×
1 Name	Select Oracle database backup options	-
2 Backup Type	Choose backup type	
3 Retention	Online backup	
4 Replication	O Datafiles, control files, and archive logs	
5 Script	O Datafiles and control files	
6 Verification	Archive logs	
7 Summary	O Offline backup	
	◯ Shutdown	
	Save state of PDBs 0	
	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.	
	O On demand	
	Hourly	
	O Daily	*
	Previous Next	

4. Set the log retention period.

New Oracle Da	atabase Backup Policy			×
1 Name	Retention settings ()			
2 Backup Type	Hourly retention settings Data backup retention settings			
3 Retention	Total Snapshot copies to keep	7		
4 Replication	🔿 Keep Snapshot copies for	14	days	
5 Script	Archive Log backup retention settings	7		
6 Verification	Keep Snapshot copies for	, ⊅ ≑	days	
7 Summary				
				Previous Next

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

New Oracle Dat	tabase Backup Policy	×
1 Name	Select secondary replication options 🚯	
2 Backup Type	☑ Update SnapMirror after creating a local Snapshot copy.	
3 Retention	Update SnapVault after creating a local Snapshot copy.	
4 Replication	Secondary policy label Hourly Error retry count	
6 Verification		
7 Summary		
	Previous	Next

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

New Oracle Dat	New Oracle Database Backup Policy ×							
1 Name	Specify optional so	ripts to run before and after performing	g a backup job					
2 Backup Type	Prescript full path	/var/opt/snapcenter/spl/scripts/	Enter Prescript path					
3 Retention	Prescript arguments							
4 Replication	Postscript full path Postscript	/var/opt/snapcenter/spl/scripts/	Enter Postscript path					
5 Script	arguments							
6 Verification	Script timeout	60 secs						
7 Summary								
				Previous Next				

7. Specify any backup verification scripts.

New Oracle Dat	tabase Backup Po	licy		×					
1 Name	Select the options to run backup verification								
2 Backup Type	Run Verifications f	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	Verification script	commands							
6 Verification	Prescript full path	/var/opt/snapcenter/spl/scripts/	/var/opt/snapcenter/spl/scripts/						
7 Summary	Prescript arguments	Choose optional arguments							
	Postscript full path	/var/opt/snapcenter/spl/scripts/	Enter Postscript path						
	Postscript	Choose optional arguments							
			Previo	ous Next					

8. Summary.

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

Create a full database backup policy for SQL

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

	NetApp Snap	etApp SnapCenter®						👤 demo\	sqldba Apj	o Backup and Cl	one Admin	🖡 Sign Out
	<	Policies Credential										
	Dashboard	Microsoft SQL Server 👻						_				
	Resources	Search by Name						New				Deleter
4	Manitor	Name IL	Backup Type	Schedule Type	Replication				Verification	on		
	Reports	There is no match for your search or data is not availabl	е.									
	Hosts											
	 Storage Systems 											
	- Settings											
	A Alerts											

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

New SQL Serve	r Backup Policy		×
1 Name	Provide a policy na	ame	
2 Backup Type	Policy name	SQL Server Full Backup	1
3 Retention	Details	Backup all data and log files	
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 Serve	r Backup Policy ×
1 Name	Select SQL server backup options
2 Backup Type	Choose backup type
3 Retention	Full backup and log backup
4 Replication	 ○ Full backup ○ Log backup
5 Script	Copy only backup
6 Verification	Maximum databases backed up per Snapshot copy: 100
7 Summary	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
	O Weekly
	○ Monthly
	Previous Next

4. Set the backup retention period.

New SQL Serve	er Backup Policy	×
1 Name	Retention settings	
2 Backup Type	Retention settings for up-to-the-minute restore operation ()	
3 Retention	Keep log backups applicable to last 7 full backups	
(4) Replication	O Keep log backups applicable to last 14 days	
5 Script		
6 Verification	Full backup retention settings 🚯 Daily	
7 Summary	Total Snapshot copies to keep 7 Keep Snapshot copies for 14 days	
	Previous	Next

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

New SQL Serve	r Backup Policy	×
1 Name	Select secondary replication options 1	
2 Backup Type	✔ Update SnapMirror after creating a local Snapshot copy.	
3 Retention	Update SnapVault after creating a local Snapshot copy.	
 A Replication 5 Script 6 Verification 7 Summary 	Secondary policy label Daily Error retry count 3	
	Previous	ext

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

New SQL Serve	r Backup Policy								×
1 Name	Specify optional se	cripts to run be	fore pe	rforming a	backup job	1			
2 Backup Type	Prescript full path								
3 Retention	Prescript arguments	Choose optiona	al argum	ents					
4 Replication	Specify optional se	cripts to run aft	er perf	orming a b	ackup job				
C Contrat	Postscript full path								
5 Script	Postscript arguments	Choose optiona	al argum	ents					
6 Verification	Script timeout	60	secs						
7 Summary									
							Prev	ious	Next

7. Specify the options to run backup verification.

New SQL Serve	r Backup Policy	×
1 Name	Select the options to run backup verification	Â
2 Backup Type	Run verifications for the 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.	1
4 Replication	Daily	1
5 Script	Database consistency checks options	1
6 Verification	 Limit the integrity structure to physical structure of the database (PHYSICAL_ONLY) Suppress all information message (NO_INFOMSGS) 	1
7 Summary	Display all reported error messages per object (ALL_ERRORMSGS)	
	 Do not check non-clustered indexes (NOINDEX) Limit the checks and obtain the locks instead of using an internal database Snapshot copy (TABLOCK) 	1
	Log backup	1
	🗌 Verify log backup. 🚯	1
	Verification script settings	
	Script timeout 60 secs	
	Previous Next	

8. Summary.
New SQL Serve	r Backup Policy		×
1 Name	Summary		
2 Backup Type	Policy name	SQL Server Full Backup	
Detection	Details	Backup all data and log files	
3 Retention	Backup type	Full backup and log backup	
4 Replication	Availability group settings	Backup only on preferred backup replica	
	Schedule Type	Daily	
5 Script	UTM retention	Total backup copies to retain : 7	
6 Verification	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 Finis	h

Create a database log backup policy for SQL.

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

New SQL Serve	r Backup Policy		×
1 Name	Provide a policy na	ame	
2 Backup Type	Policy name	SQL Server Log Backup	•
3 Retention	Details	Backup SQL server log]
4 Replication			
5 Script			
6 Verification			
7 Summary			
		Previous	Next

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

New SQL Serve	r Backup Policy ×
1 Name	Select SQL server backup options
2 Backup Type	Choose backup type
3 Retention	○ Full backup and log backup
4 Replication	Full backup
5 Script	Copy only backup 1
6 Verification	Maximum databases backed up per Snapshot copy: 100
7 Summary	
	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
	O Daily
	O Weekly
	O Monthly
	Previous Next

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

New SQL Serve	r Backup Policy ×
1 Name	Log backup retention settings
2 Backup Type	Up-to-the-minute (UTM) retention settings retains log backups created as part of full backup and full and log backup operations.
3 Retention	settings is configured to retain log backups of the last 5 full backups, then the log backups of the last 5 full backups are retained and the rest are deleted.
4 Replication	
5 Script	
6 Verification	
7 Summary	
	Previous Next

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

New SQL Serve	r Backup Policy	×
1 Name	Select secondary replication options 1	
2 Backup Type	🛿 Update SnapMirror after creating a local Snapshot copy.	
3 Retention	Update SnapVault after creating a local Snapshot copy.	
4 Replication	Secondary policy label Hourly Error retry count 3	
6 Verification		
7 Summary		
		Previous Next

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

New SQL Serve	r Backup Policy		×
1 Name	Specify optional so	ripts to run before performing a backup job	
2 Backup Type	Prescript full path		
3 Retention	Prescript arguments	Choose optional arguments	
4 Replication	Specify optional so	ripts to run after performing a backup job	
	Postscript full path		
5 Script	Postscript arguments	Choose optional arguments	
6 Verification	Script timeout	60 secs	
7 Summary			
		Previous	Next

6. Summary.

New SQL Serve	r Backup Policy		×
1 Name	Summary		
2 Backup Type	Policy name	SQL Server Log Backup	
O Patrotica	Details	Backup SQL server log	
3 Retention	Backup type	Log transaction backup	
4 Replication	Availability group settings	Backup only on preferred backup replica	
	Schedule Type	Hourly	
5 Script	Replication	SnapMirror enabled , Secondary policy label: Hourly , Error retry count: 3	
6 Verification	Backup prescript settings	undefined Prescript arguments:	
7 Summary	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 Finis	h

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.

n	NetApp Snap	Center	®				٠	2	9 -	L demo\oradba	App Backup an	d Clone Admin	🖡 Sign Out
<		Oracle	Database 🔸										
	Dashboard		Database	- Search databases	V							Refresh Resources	New Resource Group
ę	Resources	18m	Name	Oracle Database Type	Host/Cluster	Resource Group	Policies				Last Backup	Overall Sta	tus
-	Monitor		cdb2	Single Instance (Multitenant)	rhel2.demo.netapp.com							Not protec	ted
â	Reports												
2	Hosts												
÷	Storage Systems												
#	E Settings												
4	Alerts												

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.

п	Net/	App Snap	oCenter®								٠	2	8 -	👤 demo\oradba	App Backup and Clone Admin	🖡 Sign O	Jt
>		Oracle Datab	ase 👻	New Resource Group													×
		Search data	abases														
U		të le	Name	0	2	3	4	5	6								
•			cdb2	Name H	Resources	Policies	Verification	Notification	Summary								
аĩ				Provide a name	e and tags for t	he resource g	roup										
٨				Name	rhel2_cdb2					0							
÷,				Tags	orafullbkup					 0							
幸				Use custom nan	me format for Snap	pshot copy											
A				\$CustomText × rhel2_cdb2	< Contract of the second se					_							
				Backup settings	5												
				Exclude archive log destinations from backup					< ÷ + 6								

3. Add database resources to the resource group.

n N	letApp S	napCenter®		🌲 📓 🥹 🖌 🛓 demo\oradba App Backup and Clone Admin 🛛 🖡 Sign Out
>		atabase 👻	New Resource Group	×
	Search	n databases		
	15 M	Name		
٠		cdb2	Name Resources Policies Vernication Notification Summary	
.			Add resources to Resource Group	
A			Host	
24				
=			Available Resources Selected Resources	
•			cdb2 (rhel2.demo.netapp.com)	
			<u>«</u>	

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

n Ne	etApp SnapCenter®			i (9	🔹 👤 demo\oradba	App Backup and Clone Admin	🖡 Sign Out
、	Oracle Database 👻	New Resource Group					×
	Search databases						
U	l ≣ I™ Name						
	cdb2	Name Resources Policies Verification Notification Summary					
íí		Select one or more policies and configure schedules					
*		Oracle Full Online Backup					
-		Configure schedules for selected policies					
詞		Policy Li Applied Schedules Configure Schedules					
A		Oracle Full Online Backup None +					
		Total 1					

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

Daily									
Start date	date 09/10/2021 2:32 PM		#)					
2 Expires on 12/31/2021 2:32 PM									
Report even	1	days	<		Dece	mber	2021		,
Repeatevery			Su	Mo	Tu	We	Th	Fr	S
			28	29	30	1	2	З	č
			5	б	7	8	9	10	1
			12	13	14	15	16	17	1
			19	20	21	22	23	24	2
			26	27	28	29	30	31	1
		and the state of the	2	3	4	5	6	7	Ę
zone.	oules are un	ggered in the S				0			
zone.						U			

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

	etApp Sna	pCenter®								٠	۰0	👤 demo\oradba	App Backup and Clone Admin	🖡 Sign O	ut
>	Oracle Data	base 👻	New Resource Group												×
	Search da	tabases													
♥ ☆ ☆ ↓ ↓ ↓ ↓ ↓ ↓	12 Ma	Name cdb2	Load secondary verify backups o Secondary sto Source Volume svm_onPremch Configure ver Policy I <u>i</u> There is no mate	Resources	apVault or Sna ules	Venification	stination Volume	6 Summary 2_u02_df Configure Schedu	- les						

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

ΠN	etApp Si	napCenter®									٠		0 -	👤 demo\oradba	App Backup and Clone Admin	🖡 Sign Out
•		atabase 👻	New Reso	ource Group												×
	Search	databases	A If you serve	u want to send i er.	notifications for schee	duled or on deman	d jobs, an SMTP serv	er must be configure	d. Continue to the S	ummary page to save	our information, an	d then go	to Settir	ngs>Global Settings>	Notification Server Settings to co	infigure the SMTP
U	17.19	Name		_	_		-									
2		cdb2		0—				6	6							
a il				Name	Resources	Policies	Verification	Notification	Summary							
Å				Provide em	ail settings 🚯											
÷٩.				Select the serv	vice accounts or peopl	e to notify regardin	g protection issues.									
橆				Email preferen	nce Never		-									
•				From	From email											
-				То	Email to											
				Subject	Notification											
				🗌 Attach job r	report											

8. Summary.

II Ne	tApp Sn	apCenter®					♦ ⊠ Ø	demo\oradba	App Backup and Clone Admin	🖡 Sign Out
>		abase 👻	New Resource Group							×
	Search d	latabases								
U	17 PM	Name	0-2-	4	5	6				
٠		cdb2	Name Resources	Policies Verification	Notification	Summary				
- 			Perource group pame	rhal2 cdb2						
*			Tags	orafullbkup						
34			Policy	Oracle Full Online Backup: D	aily					
			Plug-in	SnapCenter Plug-in for Oracl	le Database					
			Verification enabled for policy	None						
4										
	Total 1								Prev	ious Finish

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.

NetApp Snap	Center®		• =	€ + L demo\oradba	App Backup and Clone Admin	🖡 Sign Out	
	Oracle Database 👻						
Dashboard	View Resource Group	Search resource g	roup				New Resource Group
Resources	Name	Resources	Tags	Policies	Last Backup	Overall Status	
& Monitor	rhel2_cdb2	1	orafullbkup	Oracle Full Online Backup			
縮 Reports							
📥 Hosts							
Storage Systems							
🚍 Settings							
Alerts							

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.

n Ne	tApp SnapCenter®								٠	9-	👤 demo\oradba	App Backup and Clone Admin	🖡 Sign Out
>	Oracle Database 💌	New Resource Group											×
	Search resource groups												
0	Name		2 3	4	5	6							
۲	rhel2_cdb2	Name Re:	ources Policies	Ventication	Notification	Summary							
ай –		Provide a name a	ind tags for the resource g	roup									
Α.		Name	rhel2_cdb2_log					0					
80 - E		Tags	oralogbkup					0					
幸		Use custom name	format for Snapshot copy										
A		\$CustomText × rhel2 cdb2 log						_					
		Backup settings											
		Exclude archive log destinations from backup			×	÷ +	Ð						

3. Add database resources to the resource group.

	etApp SnapCenter®		• ≥	😢 🔹 👤 demo\oradba	App Backup and Clone Admin	🖡 Sign Out
>	Oracle Database 👻	New Resource Group				×
	Search resource groups					
0	Name					
•	rhel2_cdb2	Name Resources Policies Verification Notification Summary				
<i></i>		Add resources to Resource Group				
~		Host				
24						
=		AVailable Resources Selected Resources				
A		cdb2 (rhel2.demo.netapp.com)				
		>				
		¢				
	Total 1				Pre	vious Next

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

	NetApp SnapCenter®		🏟 🖾 😝 🔹 demo\oradba App Backup and Clone Admin 🖡 Sign Out
>	Oracle Database 👻	New Resource Group	
	Search resource groups		
0	Name	1 0 0 0 0 0 0 0 0 0 0	
•	rhel2_cdb2	Name Resources Policies Verification Notification Summary	
a il		Select one or more policies and configure schedules	
٨		Oracle Archive Log Backup -	
÷.		Oracle Full Online Backup	
幸		Policy IL Applied Schedules Configure Schedules	
A		Oracle Archive Log Backup None +	
		Total 1	
	Total 1		Previous Next

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

Add schedules for policy Oracle Archive Log Backup ×									
0/2021 3:00 PM									
1/2021 3:00 PM									
hours 0 mins									
triggered in the SnapCenter Server time									
Cancel OK									
11(1) (3)									

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

ΠN	etApp SnapCenter®		٠	۰.	👤 demo\oradba	App Backup and Clone Admin	🖡 Sign Out
>	Oracle Database 👻	New Resource Group					×
	Search resource groups						
	Name						
	rhel2_cdb2	Name Resources Policies Verification Notification Summary					
ай							
*		Configure verification schedules					
54		Policy Lie Schedule Type Applied Schedules Configure Schedules					
		There is no match for your search or data is not available.					
===							
4							
		7.010					
		lotal U					
	Total 1					Pre	vious Next

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

n N	etApp SnapCenter®	🌲 😆 🚱 - 1 demotoradba App Backup and Clone Admin	🗊 Sign Out
	Oracle Database 👻	New Resource Group	×
	Search resource groups	If you want to send notifications for scheduled or on demand jobs, an SMTP server must be configured. Continue to the Summary page to save your information, and then go to Settings-Giobal Settings-Notification Server Settings to conf server.	igure the SMTI
U	Name		
	rhel2_cdb2		
M		Name Resources Policies Verification Notification Summary	
Δ.		Provide email settings 🕐	
\$4.		Select the service accounts or people to notify regarding protection issues.	
=		Email preference Never -	
A		From From email	
		To Email to	
		Subject Notification	
		attach joo ieport.	
	Total 1	Previo	us Next

8. Summary.

ΠN	etApp SnapCenter®					•	≅ 0	demo\oradba	App Backup and Clone Admin	🖡 Sign Out
	Oracle Database 👻	New Resource Group								×
	Search resource groups									
	Name	0		5						
۲	rhel2_cdb2	Name Resources	Policies Verification	Notification	Summary					
		Resource group name	rhel2_cdb2_log							
٨		Tags	oralogbkup							
34		Policy	Oracle Archive Log Backup: Hou	urly						
-		Plug-in	SnapCenter Plug-in for Oracle E	Database						
		Verification enabled for policy	None							
	Total 1								Prev	ious Finish

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.

II N	tApp SnapCenter®				٠	≅ 0	- 👤 demo\sqldba	App Backup and Clone Admin	🖡 Sign Out
>	Microsoft SQL Server 👻	New Resource Group							×
	search by name								
U	Name		2 3 4 5 6						
٠	master	Name	Resources Policies Verification Notification Summary						
~1	model	Descride e es							
	msdb	Provide a ria	me and tags for the resource group						
<u> </u>	tocc	Name	sql1_tpcc	0					
24		Tags	sqlfullbkup	6					
莘		Use custom	name format for Snapshot copy						
▲		sql1_tpcc							
	Total 5							Pre	evious Next

2. Select the database resources to be backed up.

ΠN	letApp SnapCenter®		
>	Microsoft SQL Server 👻	New Resource Group	
	search by name		
	Name	1 2 3 4 5 6	
	master	Name Resources Policies Verification Notification Summary	
~	model		
aïi	msdb	Add resources to Resource Group	
A	tempdb	Host Resource Type SQL Server Instance	
34	tpcc	All Databases Sql1	
-		Available Resources Selected Resources	
#		search available resources	
A		Auto select all the resources from the same storage volume 🚯	
		tpcc (sql1)	
		< contract of the second secon	
	Total 5		Previous Next

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

II N	etApp SnapCenter®		🌲 📓 😧 🔹 demo\sqldba App Backup and Clone Admin 🖡 Sign Out
>	Microsoft SQL Server	New Resource Group	
	search by name		
	Name		
2	master	Name Resources Policies Verification Notification Summary	
~	model		
ini	msdb	Select one or more policies and configure schedules	
Δ.	tempdb	SQL Server Full Backup	
30 L	tpcc	SQL Server Full Backup	
		SQL Server Log Backup S Policy I: Applied Schedules Configure Schedules	
		SQL Server Sull Parkun None	
		Total 1 Use Microsoft SQL Server scheduler	
	Total 5		Previous

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

Add schedules for policy SQL Server Full Backup							
Daily							
Start date	09/10/2021 6:20 PM						
Z Expires on	12/31/2021 6:20 PM						
Repeat every	1 days						
i The schedu zone.	les are triggered in the SnapCenter Server time	×					
	Cancel	ок					

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

II Ne	etApp SnapCenter®		🌲 🗃 🥹 🛨 demo\sqldba App Backup and Clone Admin 🗊	Sign
>	Microsoft SQL Server	New Resource Group		
	search by name			
U	Name			
•	master	Name Resources Policies Verification Notification Summary		
~	model			
iii	msdb	Select the verification servers		
*	tempdb	Verification server Select one or more servers		
54	tpcc	Load secondary locators to		
₩		Secondary storage location: SnapMirror Secondary storage location: SnapMirror Source Volume svm_onPremsql1_data svm_hybridovosql1_data_dr svm_hybridovosql1_log_dr		
		Configure verification schedules		
		Policy LE Schedule Type Applied Schedules Configure Schedules		
		There is no match for your search or data is not available.		
	Total 5		Previous	N

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

II Ne	tApp SnapCenter®	🌒 🔤 🥹 🕶 1 demoisqidba App Backup and Clone Admin 🖉 Sg	n Out
	Microsoft SQL Server 👻	New Resource Group	×
	search by name	If you want to send notifications for scheduled or on demand jobs, an SMTP server must be configured. Continue to the Summary page to save your information, and then go to Settings-Global Settings-Notification Server Settings to configure	he SMT
U	Name		
	master		
	model	Name Resources Policies Verification Notification Summary	
â	msdb		
Δ.	tempdb	Provide email settings 👔	
34	tpcc	Select the service accounts or people to notify regarding protection issues.	
		Email preference Never -	
		From From email	
A		To Email to	
		Subject Notification	
		Attach job report	
	Total 5	Previous	Next

7. Summary.

							•			
n Ne	tApp SnapCenter®					• •	6.	⊥ demo\sqldba	App Backup and Clone Admin	🛡 Sign Ou
>	Microsoft SQL Server	New Resource Group								
	search by name									
		00								
•	Name	Name Resources	Policies Verification	Notification	Summary					
�	There is no match for your search or data is not available.	Hume Headerees	Fonces vernearon		Samay					
ай –		Resource group name	sql1_tpcc							
*		Tags	sqlfullbkup							
54		Policy	SQL Server Full Backup: Daily	y						
•		Plug-in	SnapCenter Plug-in for Micro	osoft SQL Server						
##		Verification Server	None							
A		Verification enabled for policy	None							
		Send email	No							
	Resources are not found. Click Refresh									
	Resources to discover databases in the database view or create new resource group									
	on the discovered databases from the								-	in a second
	resource view.								Prev	ious Finish

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.

II Ne	tApp SnapCenter®			• =	i 0-	👤 demo\sqldba	App Backup and Clone Admin	🖡 Sign Out
>	Microsoft SQL Server	New Resource Group						×
	search by name							
U	Name							
-	sql1_tpcc	Name Resources Policies Vernication Notification Summary						
a ii		Provide a name and tags for the resource group						
٨		Name sql1_tpcc_log	0					
89		Tags sqilogbkup	0					
1 2		Use custom name format for Snapshot copy						
▲		sql1_tpcc_log						
	Total 1							vious Next

2. Select the database resources to be backed up.

п	NetApp SnapCenter®		🌲 📓 🚱 🔹 💄 demo\sqldba App Backup and Clone Admin 🛛 🖉 Sign Out
>	Microsoft SQL Server	New Resource Group	×
	search by name		
U	Name		
-	sql1_tpcc	Name Resources Policies Verification Notification Summary	
a		Add resources to Resource Group	
A		Host Resource Type SQL Server Instance	
54		All • Databases • sql1 •	
		Available Resources Selected Resources	
*		search available resources	
▲		Auto select all the resources from the same storage volume	
		tpcc (sql1)	
		×	
	Total 1		Previous Next

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

II Ne	tApp SnapCenter®		🌲 🗃 🚱 🕶 🎍 demo\sqldba App Backup and Clone Admin 🛿 Sign Out
>	Microsoft SQL Server 🚽	New Resource Group	
	search by name		
U	Name		
	sql1_tpcc	Name Resources Policies Verification Notification Summary	
ណ៍		Select one or more policies and configure schedules	
A		SQL Server Log Backup 👻 🕇 🚯	
24		SQL Server Full Backup ✓ SQL Server Log Backup S	
韢		Policy Ii Applied Schedules Configure Schedules	
A		SQL Server Log Backup None +	
		Total 1 Use Microsoft SQL Server scheduler	
	Total 1		Previous Next

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.

	Net	App SnapCenter®		۰	-	0-	👤 demo\sqldba	App Backup and Clone Admin	🖡 Sign C	Dut
>		Microsoft SQL Server 🚽	New Resource Group							×
		search by name								
C		Name								
2		sql1_tpcc	Name Resources Policies Verification Notification Summary							
*	2		Select the verification servers							
2			Verification server Select one or more servers -							
			Load secondary locators to							
*	=		verify backups on secondary Load locators							
-			Secondary storage location: SnapVault or SnapMirror							
4	•		Source Volume Destination Volume							
			svm_onPrem:sql1_data svm_hybridcvo:sql1_data_dr •							
			svm_onPrem:sql1_log svm_hybridcvo:sql1_log_dr							
			Configure verification schedules							
			Policy I ¹ Schedule Type Applied Schedules Configure Schedules							
			There is no match for your search or data is not available.							
										- 1
		Total 1						Pre	vious N	ext

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

ΠN	etApp SnapCenter®	🌲 🗷 😲 - 💄 demoisqidba 🛛 App Backup and Clone Admin	🗊 Sign Out
	Microsoft SQL Server 🚽	New Resource Group	×
-	search by name	1 you want to send notifications for scheduled or on demand jobs, an SMTP server must be configured. Continue to the Summary page to save your information, and then go to Settings-Global Settings-Notification Server Settings to con-	figure the SMTF
U	Name		
٠	sql1_tpcc		
a i		Name Resources Policies Verification Notification Summary	
٨		Provide email settings 🚯	
20		Select the service accounts or people to notify regarding protection issues.	
=		Email preference Never -	
A		From From email	
		To Email to	
		Subject Notification	
		Attach job report	
	Total 1	Pren	ous Next

7. Summary.

	letApp SnapCenter®			٠	= 0	• 1 demo\sqldba	App Backup and Clone Admin	🖡 Sign Out
>	Microsoft SQL Server 🚽	New Resource Group						2
	search by name							
	Name							
	sql1_tpcc	Name Resources Policies	Verification Notification Summary					
~7								
-		Resource group name sql1	_tpcc_log					
^		lags sqli	Septer Lee Backup House					
84.		Plug-in Sna	pCenter Plug-In for Microsoft SOL Server					
譕		Verification Server Nor	le					
A		Verification enabled for policy Nor	le la					
		Send email No						
	Total 1						Prev	ious Finish

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.

п	NetApp Snap	Center®			•	i I	-	8-	L demo\sqldba	Арр Ва	ackup and O	Elone Admin	🖡 Sign Out
<		Jobs	Schedules										
	Dashboard	search	n by name	- - ?									Carcerijots
	Resources	Jobs - I	ilter										
•	Monitor	ID	Status	Name	Start date				E	ind date	Owne	er ,	
a ii	Reports	532	~	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/14/2021 8:35:01 PM 🗎				09/14/2021 8:37:10	PM 🛱	demo	\sqldba	
A	Hosts	528	~	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/14/2021 7:35:01 PM 🛱				09/14/2021 7:37:09	PM 🛱	demo	\sqldba	
		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	B PM 🛱	demo	\sqldba	
24	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	1 PM 🛱	demo	\sqldba	
筆	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	
Δ	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	B PM 🛱	demo	\sqldba	
20	, and the	509	~	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/14/2021 3:35:01 PM 🛱				09/14/2021 3:37:10	PM 🛱	demo	\sqldba	
		503	~	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/14/2021 2:35:01 PM 🛱				09/14/2021 2:37:09	PM 🛱	demo	\sqldba	

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

III Ne	tApp SnapC	:enter®				•	n ≅ 0-	👤 demo\oradba	App Backup and Clone A	dmin 🛛 🗊 Sign Out	
	Oracle Databas	e 📕	cdb2 Topology								×
	Search databa	ases							Database Settings F	rotect Refresh	
U	17 19	Name	Manage Copies								1
		cdb2	197 Backups					C	Cond.		1
	盾	cdb2dev	197 Backups 3 Clones				Summary Card				1
â		cdb2dr	Mirror copies				394 Backups				1
A	rin 🖌	cdb2dr2	Local copies				28 Data Backups 366 Log Backups				1
24	rii i	cdb2test						3 Clone	is		1
₩ #			Primary Backup(s)					Caratego Reco	t File 41 4	a a a	
			Backup Name	Count	Туре	17 End Date	Verified	Mounted	RMAN Cataloged	SCN	1
			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	í
			rhel2_cdb2_09-23-2021_14.35.03.3242_0	1	Data	09/23/2021 2:35:30 PM 🛱	Unverified	False	Not Cataloged	6872715	1
			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	l
			rhel2_cdb2_09-22-2021_14.35.02.0014_0	1	Data	09/22/2021 2:35:14 PM 🛱	Unverified	False	Not Cataloged	6737395	
			rhel2_cdb2_09-21-2021_14.35.02.1884_1	1	Log	09/21/2021 2:35:35 PM 🗎	Not	False	Not Cataloged	6598735	

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

Getting Started with AWS public cloud

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

AWS public cloud



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

1. Pre-flight check

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

- ☐ AWS account
- □ VPC in your region of choice
- □ Subnet with access to the public internet
- Permissions to add IAM roles into your AWS account
- $\hfill\square$ 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.

Log In to NetApp Cloud Central	
Don't have an account yet? Sign Up	
rt1600680@demo.netapp.com	
LOGIN	

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.

 Cloud Ma	nager							Account ~	Workspace Workspace 1	~ Com	sector ~	0	0	0
Canvas	Replication	Backup & Restore	KBs	Data Sense	File Cache	Compute	Sync	All Services (+8)	~					
Add New	Working Enviro	onment												×
					aws	0	L.							
			Microsoft Ap	rr	usin Web Services	Seeger Court	Sactorm	Co-Premises						
		Cho	oose Type		_									
			(0	6	6		\bigcirc						
			Cloud Volu	mes ONTAP	Cloud Volum	IES ONTAP HA	c	loud Volumes Service						
			- Prof	Note	High A	ontaking -		High Asselution						
						vext/								

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.

	Cloud Manager	Add Connector				Need Help?	×
_	Conves Replication						
			Choose th	Provider e cloud provider where you want to run the	e Connector:		
				aws	Control Harling		
			THE LOOP PLATE	ANALAN REC JECKES	adage Lood Philipin		
				Continue			

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

 Cloud Manager	Add Connector	Need Help? X
Canves Replication	🔗 Get Ready 👩 AWS Credentials 🚯 Details 🚯 Network 🚯 Security Group 🛞 Review	
Add New Working Envi	AWS Credentials	
	AWS Access Key AWS Access Key AWS Access Key AWS Access Key AWS Secret Key AWS Access Key AWS Ac	
	Previous Nexs	

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 Mar	nager	Add Connector	Need Help7	×
(Canvas)	Replication	🔗 Get Ready 🕑 AWS Credentials 🏮 Details ③ Network 🕥 Security Group 🙆 Review		
Add New \	Working Envi	Details		
		Connector Role		
		Add Tags to Connector Instance Cloud-Manager-Operator-IBNt24)		
		Previous		

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

-	Cloud Manager	Add Connector	Need Help? X
	Canvas Replication	🔗 Get Ready 🔗 AWS Credentials 🔗 Details 👩 Network 🚯 Security Group 🚳 Review	
	Add New Working Envi	Connectivity Proxy Configuration (Optional) VPC HTTP Proxy vpc:083fcbd79f75dfb6e-10.221.0.0/16 Europe: ImpultI22.06.256.1mm Subnet Define Credentials for this Proxy 10.221.4.0/24.1 publicSR_us-elast-1a_rT1500 Upload a root certificate ~ Key Pair	
		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.

Cloud Manager	Add Connector	Need Help? X
Canvas Replication	⊘ Get Ready ⊘ AWS Credentials 🕜 Details ⊘ Network 🔕 Security Group 🗿 Review	
Add New Working Envi	The secontry group must allow inbound HTTP. HTTPS and SSH access.	
	Assign a security group: Create a new security group Select an existing security group 	
	HTTP (Port Str) HTTPS (Port 443) SSH (Port 22)	
	Source Type Source Type Source Type	
	My IP ~ My IP ~	
	Source (CDP) Source (CDPI) Source (CDPI)	
	21624031.14502 21624031.54502 21624031.54502	
	Previous Next	

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

Cloud Manager	Add Connector	Need Help? X
Canvas Replication	🧭 Get Ready 🕑 AWS Credentials ⊘ Details ⊘ Network 🕑 Security Group 🔇 Review	
Add New Working Envi	Code for Terraform Automation	
	Connector Name awscloudmanager	i
	Region us-east-1	
	VPC vpc.083fcbd79f75dfb6e - 10.221.0.0/16	
	Subnet 10.221.4.0/24 publicSN_us-east-1a_rt1600680	
	Key Pair rt1600680	
	Public IP Enable	
	Proxy None	
	Security Group. HTTP: 216/240/31.145/32, HTTPS: 216/240/31.145/32, SSH: 216/240/31.145/32	
	Previous Add	

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

 Cloud Mana	ger	
Canvas	Replication	
Add New W	orking Envi	Deploying a Connector
		Show Details
		 Keep this wizard open until the deployment process is complete. It usually takes about 7 minutes.
		 No other Cloud Manager features are available during deployment.
		When the process is complete, you can continue the operation that you started.

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

 Cloud Manager		×
Clouid Manager Carwas Replication Add New Working Env	Connector Successfully Created The Connector was created successfully.	×

Deploy Cloud Volumes ONTAP

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

 Cloud Mar	nager					Account +1500880	- Workspace	(*	Connector ~	@ (98
Canvas	Replication	Backup & Restore X	8s Data Sense	File Cache	Compute	ync All Servici	es (+8) 🗸				
Add New	Working Enviro	nment									×
				aws	0		3				
		Mice	osit Azure Am	azon Web Services	Google Cloud Place	On Pre	nites				
		Choose 1	Гуре								
			0	0	~	0					
		Clou	d Volumes ONTAP	Cloud Volum	es ONTAP HA	Cloud Volumes 5	ervice				
			Single Note	E Man Ro	and the second second	High Asselution					
				N	lext						

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

	Cloud Ma	nager							Account Vorkspace r1505880 Vorkspace1	• Connector • •	0	0
	Canvas	Replication	Backup & Restore	KBs	Data Sense	File Cache	Compute	Sync	All Services (+8) 🗸			
	Create a Ne	w Working Environ	iment		D	etails ar	nd Credentia	Is				
	Previous	Step .	Instance Profil Credential Nar	le Ne	322944748816 Account ID		• Ne subscription Marketplace Subscr	in terms lared	Edit Credentials			
			Details Working Enviro	unment film	ne (Christer Name)		Cred	oritials				
			Up to 40 cha	racters.	re (crush), reacted)		adm	in				
			😗 Add Tags	Op	Gonal Vield Up to flag	r tags	Pasia	ord				
							Confi	m Password	1			
							ononve					
Coud M	inge 159 Built	5 Aug 10, 2021 (AU) 10	ani lata									

3. Choose Add Subscription.

	Cloud Ma	nager							Account		Workspace Workspace 1	Connector avectoration	9 (0 0
	Canvas	Replication	Backup & Restore	KBs	Data Sense	File Cache	Compute	Sync	All Se	sivices (+8)	~			
	Create a No	w Working Enviro	amant		_	Details and	i Credentia	5						
	 Prisitaliz 	Step .	Instance Profil Credential Nam	e. 14	Edit Cre	dentials & Ad	ld Subscripti	n	-		R Contercarts			
			Details Working Enviro	rotond Nam	Credentials	Profile Account It	0: 322944746816							
			 Add Tags 		Mackets O Most O Add Sk	lace Subscription	slated with the st	ntectur						
-		(n er fre			Apply	Ca	ucel						

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

 Cloud Mar	nager							Account ~	Workspace Workspace 1		Connector	6	0	
Canyas	Replication	Backup & Restore	Kās	Data Sense	File Cache	Compute	Sync	All Services (+8	0~					
Greate a Ne	w Working Environ	munt		Eart Cr	epentiais & A	aa suosenpt	on							
				Select a si details an	ubscription option id then subscribe.	and click Continue	The AWS M	farketplace enables	you to view pricing					
				C Pay Pay wit	y-Per-Till - Annual (y for Cloud Volumi h an annual, upfro	Contract es ONTAP ont payment.	۲	Pay-as-you-go Pay for Cloud Volur an hourly rate.	nes ONTAP at	1				
				The next	t steps:									
				(1) AV	S Marketplace scribe and then clic	k Set Up Your Act	ount to cont	figure your account.						
				(2) CBA Save	ud Manager e your subscription	and associate the	Marketplaci	e subscription with y	our AWS credenti	Res:				
 langer 1.5.5 . Babbi S	Aug 16, 2011 A418 21	ar (15)					- 70	Continue	Cancel					

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



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.

💭 aws marke	tplace					Q			Halla, rt1600	9680 -
out - Categories	- Delivery Methods -	Solutions -	AWS IQ =	Resources -	Your Saved List		Partners	Sell in AWS Marketplace	Amazon Web Services Home	н
		You are ex Offer name (NetApp, in	lanager + tended multi c. for SaaS 2	Deploy &	Manage NetApp Cloud Data ct an offer first and review the prices informate the Offer - current subscription >}	I Services Ifon and EULA You are subscribed to this offer. by Network of the Network Vice Vice Vice Vice Vice Vice Vice Vice				
		You are corre- utage at the artemation of	end of your in on the right. Harvining its if you were o please click	ed to this produc ext billing cycle, sures, signifi nable to comple here to be take	t and will be charged for your accumulated hased on the costs liabed in Pricing g up for your product? te the set up process for this software, to the product's registration area.	You have subscribed to a Privat You have subscribed to mis private offer on a 2020 UTC. This private offer will expire on A 5022 UTC. You use of this product after the care of your private offer will be billed at the t current public promo, which can be found on products detain page. To avoid being changed for use beyond the e- tate of mis offer, you can cancel your subscr- time product by August 1, 2022 UTC. Prese e- vendor directly with any questions regarding	e Offer luly 21, ogust 1, expitation hen this this xpration to contact the this offer			
						Subscribe: Its subscribes to the software, you agree to the pricing to softwar from Units Contrate Software and A. You also as	erres and the			

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

T NetApp		Faderic view	Füll	•	않
III Esteric view	Subscription Assignment *				
∎©: Feature Spatlight	Your subscription to Cloud Manager / Cloud Volumes ONTAP From AWS Marketplace was created successfully1				
tradactis (Name your subscription				
×.	NetApp Cloud Central Account: 0				
ED An	We've assgned your subscription to all or your YeeApp cloud Central accounts. You can choose to unassign specific accounts. ☑ rt1600680				
tervices Status, 12	Sive				
Contact Us					

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

II NetApp		Falaric View	Full +	8
TTT Fahric View				
i∰: Feature spottight				
Stradecti i				
X Junit -				
500 Art				
Services Status 12	Your subscription demo.netapp.com-cloud-volumes-ontap-386953e5 saved successfully			
ContactUs				

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

Croate a New Working Environment	Edit Credentials & Add Subscription		
	Associate Subscription to Credentials		
	Tou autocribed successfully		
	Credentials		
	Instance Profile Account ID: 322944748816		
	Subscription	_	
	 demo.netapp.com-cloud-volumes-ontap-386953e5 		
	Add Subscription		
		_	
	Apply Cancel		
Contractory Mathematical Academic States and State			

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

b. Cluster password

c. AWS tags (Optional)

	Cloud Ma	nager						Account v Workspace v r1500880 VWorkspace 1	Connector ~	@ @) @
	Canvas	Replication	Backup & Restore	K8s Data Sense	File Cache	Compute	Sync	All Services (+8) ~			
	Create a Ne	ew Working Enviror	nment		Details ar	nd Credentia	ls				
	Previous	Step	Instance Profil Credential Nat	e 32294474 e Account IC	8816	demo.netapp.com Marketplace Subscr	cloud-vol iption	Edit Credentials			
			Details			Cred	ontials				
			Working Erwino hybridawsew	nment Name (Cluster Nam)	e):	user i adm	Name Nin				
			🕒 Add Tags	Optional Vield Up	to four tags	Passor	brow				
						Confi	rm Password	a			
						Continue					
Coud M	inge 359 Suit	5 Aug 18, 2021 (AU 31)	s en lata								

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

	Cloud Ma	inager							Account		Workspace Workspace	•	Consector avecdademana.	۲	0	8
	Canvas	Replication	Backup & Restore	KBs	Data Sente	File Cache	Compute	Sync	All Servi	ces (+8) 🗸						
	Create a N	ew Working Enviro	oment			Se	rvices									
	T Previour	s Step														
			💮 Da	ta Sense 8	Compliance						-	~				
			(3) Ва	ckup to Cl	oud						-0	Ŷ				
			(iii) Mo	nitoring							-	~				
						Co	ntinue									
Condi	langa 159 Bult	a Aug 10,2021 (ALT))	5 का धारत			C.	ntinue									

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

Cloud Ma	nager					1	Account ~		forkspace forkspace (Connector avoidourimenta	٢	0	
Canvas	Replication	Backup & Restore	K8s Data	Sense File Cache	Compute	Sync	All Services	(+8) 🗸						
Create a No	ew Working Enviror	oment		HA Deplo	yment Mod	els								
† Previous	Step	Multiple Availabi	lity Zones aximum protection ention of 3 availabilit e serves data if its po	against AZ failures. ty zones. artner goes offline.	Single A	vailability Z(rotects again ingle availabil rooup, spread n HA node se t infis	ano at failures within ity zone. HA no neross distanct i rves data if its p	n æsingli ides are i underlyk partner g	: AZ n a placeme g hardware ces offline.	nt				

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 Ma	nager							Account York	space 🛩	Connector evolutionmena.	® 0	
	Canvas	Replication	Backup & Restore	X8s	Data Sense	Ele Cache	Compute	Syn	c All Services (+8) 🗸				
	Create a Ne	w Working Enviro	oment			Regio	n & VPC						
_	↑ Previous	Step	AWS Region US East N. Virgini	à	÷	VPC vpc-063ft/bd79f75c 10.221/0.0716	No6e -	÷	Security group Use a generated security groo	p •			
			Node 1:			Node 2:			Mediator:				
			Availability Zone us-east-1a			Availability Zone us-east-1b		•	Availability Zone us-east-1c				
			Subnet			Subnet			Subnet	-			
			- Constant - Constant			1012211220124			10.44.12.01.44				
						Co	ntinue						
Couth	houge 1.5.9 Suite	■ Aug 18, 2021 04,133	S en litte										

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

**	Cloud Ma	nager							Account		Worksp Worksp	ace ~	2	onnedor ochudroma.	۵ (0	0
	Canvas	Replication	Backup & Restore	K8s	Data Sense	File Cache	Compute	Sync	All Se	ivices (+B)	~						
	Create a N	ew Working Environ	nment		Conr	nectivity & S	SH Auther	tication									
	 Previou 	s Step	No.	des			<u>a a</u>	Mediator									
			SSH Authe	ntication M	ethod		Security Gr	oup.									
			Passwor	d		•	Use a ge	verated secu	uty group		•						
							Key Pair Na	inie.			- 0	÷					
							rt160068	0									
							internet Co	nnection Me	thod		0	8					
							Public IP	address			•						
						Cor	tinue										
						_											



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.

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

Cloud Man	ager								Account rτ1618549		Workspace Workspace-1		Connector awscloudmana		Ĺ)		0	
Canvas	Replication	Backup & Restore	K8s	Data Sense	File Cache	Compute	Sync	All Services (+8) 🗸										
Create a Nev	v Working Environ	ment				Floa	ting IPs											
↑ Previous S	tep		Floating IP	addresses are requ HA nodes if failu You must spec	uired for cluster an ures occur. To acce ify IP addresses th	d SVM access and iss the data from at are outside of	d for NFS and outside the Vi the CIDR bloci	CIFS data access. These f PC, you can set up an AW ks for all VPCs in the sele	loating IPs can I <mark>S transit gatev</mark> cted AWS regio	migrate b <mark>/ay.</mark> m.	etween							
					Floating IP add 10.222.0.200	ress for cluster m	ianagement											
					Floating IP add	ress 1 for NFS an	d CIFS data											
					Floating IP add	ress 2 for NFS an	d CIFS data											
					Floating IP add	ress for SVM mar	nagement (Op	tional)										
					Enter Floatin	g IP Address												
	Cloud Man Carvas Create a New Previous S	Cloud Manager Canvas Replication Create a New Working Environ Previous Step	Cloud Manager Annual An	Cloud Manager Canvas Replication Backup & Restore K8 Create a New Working Environment Previous Step Floating IP	Cloud Manager Canvas Replication Backup & Restore K8s Data Sense Create a New Working Environment Floating IP addresses are req HA nodes if fail Vou must spect	Cloud Manager Annotes Replication Replica	Cloud Manager Annoas Replication Backup & Restore K8s Data Sense File Cache Compute File Create a New Working Environment File File File File File File File File	Cloud Manager Canvas Replication Backup & Restore K8s Data Sense File Cache Compute Sync Create a New Working Environment Floating IP addresses are required for cluster and SVM access and for NFS and HA nodes if failures occur. To access the data from outside the VI You must specify IP addresses that are outside of the CIDR block * * * Floating IP addresses that are outside of the CIDR block Floating IP address for duster management 10:222.0200 Floating IP address of for NFS and CIPS data 10:222.0.200 Floating IP address of soft management (OPI Enter Floating IP Address for SVM	Cloud Manager Canvas Replication Backup & Restore K8s Data Sense File Cache Compute Sync All Services (+8) ~ Create a New Working Environment Floating IP Environment Floating IPs * Previous Step Floating IP addresses are required for duster and SVM access and for NFS and CIFS data access. These for HA nodes if failures occur. To access the data from outside the VPC, you can set up an AW You must specify IP addresses that are outside of the CIDR blocks for all VPCs in the selection of the VPC. you can set up an AW You must specify IP addresses for Cluster management 10.222.0200 Incess for IVPS and CIFS data Floating IP address 1 for NFS and CIFS data 10.222.0200 Incess for SVM management (Optional) Incers for SVM management (Optional) Floating IP address for SVM management (Optional) Enter Floating IP Address Incers for SVM management (Optional)	Cloud Marger Replication Backup & Restore KBs Data Sense File Cache Compute Sync All Services (+8) ✓ Create a New Working Environment Floating IP addresses are required for cluster and SVM access and for NFS and CIFS data access. These floating IPs can HA nodes if failures occur. To access the data from outside the VPC, you can set up an AVX5 transit gater Nout specify IP addresses are required for cluster and SVM access and for NFS and CIFS data access. These floating IPs can HA nodes if failures occur. To access the data from outside the VPC, you can set up an AVX5 transit gater Vou must specify IP addresses for cluster management 10:222.020 Floating IP address 1 for NFS and CIFS data 10:222.020 Floating IP address for SVM management (Optional) Enter Floating IP Address	Cloud Marger Replication Backup & Restore KBs Data Sense File Cache Compute Sync All Services (18) × Create a New Working Environment Floating IP addresses are required for cluster and SVM access and for NFS and CIFS data access. These floating IPs can migrate b HA nodes if failures occur. To access the data from outside the VPC, you can set up an AVS transfit gateway. Previous Step Floating IP addresses that are outside of the CIDR blocks for all VPCs in the selected AWS region. Floating IP addresses for SVM access for SVM access for SVM anagement 10.2220.200 Floating IP address 2 for NFS and CIFS data Cacce.2002 Floating IP address 2 for NFS and CIFS data Data SVM access for SVM management (Optional) Enter Floating IP Address	Cloud Margare Replication Backup & Restore K8 Data Sense File Cache Comput Sync All Services (+8) × Create a New Working Environment 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. Vor must specify 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. Vor must specify IP addresses that are outside of the CIDR blocks for all VPCs in the selected AWS region. floating IP address 1 for NFS and CIFS data 10.222.0.201 Integrating IP address 2 for NFS and CIFS data 10.222.0.201 Integrating IP address for SVM management (Optional) Inter Floating IP Address Inter Floating IP Address for SVM management (Optional) Inter Floating IP Address Inter Floating IP Address	Cloud Marce Count Count	Cloud Account Control Account Control Markages Control Control	Cloud Notice of Machine Notice of Machine Notice of Machine Notice of Machine Clouds Replication Backup & Restore Kis Data Sense File Cache Compute Sense All Services (14) Create a low Urking Environment Floating IP addresses are required for cluster and SVM access and for NFS and CIFS data access. These floating IPs can migrate between 14 nodes if failures occur. To access the data from outside the VPC, you can set up an AVS trapingt IPs can migrate between 14 nodes if failures occur. To access the data from outside the VPC, you can set up an AVS trapingt IPs can migrate between 14 nodes if failures occur. To access the data from outside the VPC, you can set up an AVS trapingt IPs can migrate between 14 nodes if failures occur. To access the data from outside the VPC, you can set up an AVS trapingt IPs can migrate between 14 nodes if failures occur. To access the data from outside of the CIDR blocks for all VPCs in the selected AVS region. Floating IP address of fuster management 10220.020 Inatage IP address of for SVM management (Dptional) Inter IP Dating IP Address of for SVM management (Optional) Inter Floating IP Address Inter Floating IP Address	Cloud Nervee Reduction Reduction </td <td>Cloud Notice Notice Notice Notice Notice Notice Notice Notice</td> <td>Cloud Lorse Notice Notice<</td>	Cloud Notice Notice Notice Notice Notice Notice Notice Notice	Cloud Lorse Notice Notice<

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.

Canvas	Replication	Backup & Restore	K8s	Data Sense	File Ca	iche Compute	Sync All Services (+	8) 🗸	
Create a Ne	w Working Environ	ment			R	loute Tables	1		
1 Previous	Step	Select the routs pair.	tables that sl if you leave a	iould include routes route table unselect	i to the flow ted. clients Add	iting IP addresses. This ena that are associated with th Storial information @	bles client access to the Cloud e route table cannot access th	l Volumes ONTAP HA le HA pair.	
		Name Name			Main	ID	Associate with Subnet	t Tags	
		😧 private_	1_111600680		No	rtb-08b4cb68f65c826a5	3 Subnets	1 Tags	
		Public_r	_rt1600680		Ves	rtb-0e46720d0da10c59	1 Subnets	1 Tags	
		2 Route Tables	The main ro	ute table is the defai	ult for the	VPC			
					111				

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

 Cloud Ma	inager							Account +1600680		Workspace Workspace 1	Connector ~ wodoutment.	® (୭ (Э
Canvas	Replication	Backup & Restore	K8s	Data Sense	Ble Cache	Compute	Sync	All Servi	ices (+8) 🗸	*				
Create a N	ew Working Enviro	oment			Data E	ncryption								
1 Previour	s Step		AW ist De	3 AWS Managed 75 is responsible for andled by AWS key fault Master Key: an	Encryption data encryption a management sen	nd decryption op rices.	erations. Key	macagemen	ŧ.,					
					Co	ntinue								

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

	Cloud Ma	nager							Account +1600680		Workspace Workspace		Const	ector ~	¢ (0	
	Canvas	Replication	Backup & Restore	K8s	Data Sense	File Cache	Compute	Sync	All Sen	vices (+8) •	<i>.</i>						
	Create a No	ew Working Enviro	oment	Cloud	d Volumes (ONTAP Cha	rging Meth	ods & N	ISS Acco	ount							
	1 Previous	Step	Cloud Volumes ONTAP Learn more about our chu © Pay-As-You-	Charging metho Go by the b	Methods our		Net. Lear Ta n shou Dan finis Supp	App Suppor n more abou sgister this C dd add NetAr t have a Net n deploying t sort Registrat	rt Site Acco It NetApp Su loud Volume op Support 5 App Support his system.4 tion option t	unt (Optie pport Site) is ONTAP to Site Accoun Site accou dier its create an	nal) NSS) accour support yo t tri?Select go triduse the NSS accoun	ts 2 to					
			Freemium (Up to SOOG8	83		ntinue	Add Netapp :	Support Site	Account							
Churth	ange 153 file	0 Avg 18,2021 04-133	15 arr 176														

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

Canvas	Replication	Backup & Restore	Kās	Data Sense	File Cache	Compute	Sync	All Services (+8)				
Create a Ne	w Working Environ	ment			Preconfigu	red Packag	es					
↑ Previous	Step	Select a proc	onligured (Cloud Volumes O Preconfi	NTAP system the gured settings ca	t best matches n be modified at	rour needs, or a later timo	créaté your own c	onfiguration.	a	uange Config	uratio
		÷.		IN O			\$0			. 9 .		
	POC and s Up to 3	mall workloads 18 of storage	D	atabase and applic production wor Up to 10TR of at	cation data kloads torage		Cost effective	DR rage	Highes	t performance production workloads up to 3687B of storage		
					Cor	otinue						

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

	Cloud Ma	nager							Account ~	Workspace		Connector ~	۲	0	0
	Canvas	Replication	Backup & Restore	K8s	Data Sense	File Cache	Compute	Sync	All Services (+8) ~					
	Create a N	ew Working Enviror	nment			Create	Volume								
	Previous	i Step	Details & Pro	tection			Protoco	(
			Volume Name:		Size (0	101 (D	NE	s	CIFS	(5C5)					
			1.		Volu	athe size	Arrest Con	track.							
			Snapshot Policy:				Custom e	xport policy	8		÷.				
			default												
			IDefault Policy				Custom exp	ort policy							
							10.221.0/	0/16							
							Advanced	options			~				
						· Continue	Ski	þ]						
Court M	anapar 100 Burlan	9 Aug 18 2027 64 53 5	h and lotty												

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.

8	Cloud Mar	nager					Account re16006	s ~	Workspace 1		Connector evolvedment.	٢	0	
	Canvas	Replication Back	up & Restore	K8s Data Sense	File Cache	Compute Sy	mc All	Services (+8)	÷					
	Create a New	w Working Environment			Review 8	& Approve								
	1 Previous	step hybridawscvo								Sh	ow API request			
		us-east-1	HA											
		Useast-1	HA n order to activate su	pport. I must first register	Cloud Volumes ONT	AP with NetApp. More in	formation >							
		Understand that of	HA n order to activate su Doud Manager will all	pport, I must first register locate the appropriate AW	Cloud Volumes ONT 5 resources to comp	AP with NetApp. More in ily with my above require	formation > miteritis, More	isformation *						
		Useast-1 Useast-1	HA n order to activate so Dood Manager will all Networking	pport. I must first register locate the appropriate AV Storage	Cloud Volumes ONT 5 resources to comp	AP with NetApp. More in ly with my above require	formation = mineritis, More	information *						
		I understand that it I understand that it Overview Storage System:	HA n order to activate so Doud Manager will all Networking Cloud Volu	pport, I must first register locate the appropriate AV Storage	Coud Volumes ONT 5 resources to comp	AP with NetApp. Mere in Iy with my above require HA Deployment 1	formation = mments, More Model:	information * Multiple A	valiability Zones					
		Iunderstand that in Overview Storage System: License Type:	HA n order to activite su Doud Manager will all Networking Cloud Volu Cloud Volu	pport. I must first register locate the appropriate AV Storage mes Oritae HA enes Oritae HA	Cloud Volumes ONT 5 resources to comp	AP with NetApp. Merein ly with my above require HA Deployment I Encryption:	formation = mments. More Model:	information * Multiple A AVICS Manu	valiability Zones					

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



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

	Cloud Ma	inager					A.	ccount ~	Workspace ~	Connector eventbookmana*	• • •
	Canvas	Replication	Backup & Restore	Käs	Data Sense	File Cache Compute	Sync	All Services (+)	n~		
		Resources Canvas Review C	10. CyS, ANT & Dri Premises	*	6	Digital Wallet View & Manage Digital Wallet	#	*	Timeline View Activity & Events		
		Services Replicati Data Rep	on Icabori	*	6	Backup & Restore Data Protection for CvO and On-Premi	10	۲	Kits Cloud Native Development		
		Data Ser Data Goy	sse ernance & Compilance	*	0	Compliance Prhacy & Compliance Controls	A.		Tiering Lift and DOWT shift	#	
		(the Monitori Monitor	ing Optimize and Secure	2	(1)	File Cache Convolidate your Data into the Cloud	1	\bigcirc	Compute Optimize your clinic speed	 *	
https://doi.att	arage weightion	Sync Automati	nd Data Synchronization	*	6	SnapCenter Application Data Management	#	*	Active IQ Digital Advisor	1	

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.

 Cloud Mana	iger			A10	50550 ~ (Norkspace Norkspace 1	Conn	nter Somme	۲	0	8
Canvas	Replication Backup & Rest	vre KBs Data Sense File	Cache Comput	e Sync	All Services (+8) ~						
(Timelin	ne										
	₩ Filters:										
	Time(0) Service	Action Agent (1) Resource	e User [Status Res	et.		c	t t			
	Time 🖕	Action :	Service :	O April :	O Resource :	User (:	Status :	•			
	> Aug 18 2021, 9:42:32 pm	Check Connectivity	Cloud Manager	avodoudman	hybridawscvo	Full Name	Success				
	✓ Aug 18 2021, 9:42:00 pm	Create Aws Ha Working Environment	Cloud Manager	awsclosidma	hybridawscvo	full Name) Pendinj	•			
	Aug 18 2021, 10/08:39 pm	Describe Operation Status					• Success				
	100.48.3031.10.00.83 em	Percenta Describer It in a					. Com				

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



Configure SnapMirror from on-premises to cloud

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

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

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


Select Enable.

ര	Replication	Enable] (:

Or Options.

onPrem • On	
DETAILS	
On-Premises ONTAP	
SERVICES	

Replicate.

onPres • On	m (<u>]</u> () (×
DETAILS		
On-Premises ON	TAP	
SERVICES		
SERVICES Replica On	tion 1 Replication Targe	et 🤇
SERVICES Replica On Backup Compli	tion 1 Replication Targe	et ons

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

From: onPrem	
To: select the Working Environment to which you w	ant to replicate data
Replication Target	
hybridcvo (Cloud Volumes ONTAP)	``
Start Replication Wizard	Cancel

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

Replication Setup		Source Vo	olume Selection		
Frhel2_u03		rhel2_u030923211942120	3118 • Online	sql1_data	ONLINE
INFO	CAPACITY	INFO	CAPACITY	INFO	CAPACITY
Storage VM Name svm_onPrem Tiering Policy None Volume Type RW	100 GB Allocated	Storage VM Name svm_onPrem Tiering Policy None Volume Type RW	100 GB Allocated	Storage VM Name svm_onPr Tiering Policy None Volume Type RW	em 53.37 GB Allocated Lisk Used
sql1_log	ONLINE	sql1_snapctr	ONLINE		
INFO	CAPACITY	INFO	САРАСПУ		
Tiering Policy None	18.16 GB Disk Used Allocated	Tiering Policy None	24.87 GB Allocated		
Volume Tune PIM	resources	Volume Tune PM	Chinese Chinese		

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

Replication Setup	Des	tination Disk Type and Ti	ering	
↑ Previous Step	Destination Disk Type	General Purpose SSD - Dynamic Performance	Throughput Optimized HDD	
	S3 Tiering S3 Tiering Enabled Disabled Note: If you enable S3 tiering, thin provisi	oning must be enabled on volumes created	What are storage tiers? 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.

74

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.

-	1	
 Limited to: 	100	MB/s

Unlimited (recommended for DR only machines)

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

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

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

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

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

Replication Setup			Review & Ap	oprove			
↑ Previous Step			Review your selection and start	the replication process	ate AWS resources to comply with m	y above requirements.	
	Source	Destination (in) hybridcvo	More information > Source Volume Allocated Size: Source Volume Used Size:	53.37 GB 45.09 GB	Destination Thin Provisioning: Destination Aggregate:	Yes aggr1 (Automatically s	
	sal1 data		Source Thin Provisioning: — — — — — — — — — — — — —	Yes e: 53.37 GB General Purpose SSD (Destination Storage VM: Max Transfer Rate: SnapMirror Policy:	svm_hybridcvo 100 MB/s Mirror	
	sqri_uata	sqir_uata_topy	Capacity Tiering:	53	Replication Schedule:	daily	
			6				

- 10. Continue this process for data volumes and log volumes.
- 11. To check all of your relationships, navigate to the Replication tab inside Cloud Manager. Here you can manage your relationships and check on their status.

Replication												
	Volume R	elationships	ø	153.32 GIB Replicated Capacity		O Currently Transl	erring	0	7 Healthy		⊗ 0 _{Failed}	
	7 Volume Relationships											Q C
	Health Status 💠	Source Volume	•	Target Volume).	Total Transfer Time 💠	Status	≡∣	Mirror State	٥	Last Successful Transfer	Đ
	\odot	rhel2_u01 onPrem		rhel2_u01_dr hybridcvo		43 minutes 43 seconds	idle		snapmirrored		Sep 30, 2021, 12:12:50 Af 19.73 MiB	
	\odot	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	
	\odot	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	
	\odot	sql1_data onPrem		sql1_data_dr hybridcvo		1 hour 6 minutes 50 seconds	idle		snapmirrored		Sep 30, 2021, 12:12:28 Af 24.56 KiB	-

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

×

3. Deploy EC2 compute instance for database workload

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

Sizing the compute instance

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

Linux instance configuration for Oracle workload

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

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

Windows instance configuration for SQL Server workload

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

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

Copyright information

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

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

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

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

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

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.