



Protecting Workloads on AWS / VMC

NetApp Solutions

NetApp
March 19, 2024

This PDF was generated from <https://docs.netapp.com/us-en/netapp-solutions/ehc/aws-guest-dr-solution-overview.html> on March 19, 2024. Always check docs.netapp.com for the latest.

Table of Contents

- Protecting Workloads on AWS / VMC 1
 - TR-4931: Disaster Recovery with VMware Cloud on Amazon Web Services and Guest Connect 1
 - Veeam Backup & Restore in VMware Cloud, with Amazon FSx for ONTAP 70
 - TR-4955: Disaster Recovery with FSx for ONTAP and VMC (AWS VMware Cloud). 102
 - Using Veeam Replication and FSx for ONTAP for Disaster recovery to VMware Cloud on AWS 117

Protecting Workloads on AWS / VMC

TR-4931: Disaster Recovery with VMware Cloud on Amazon Web Services and Guest Connect

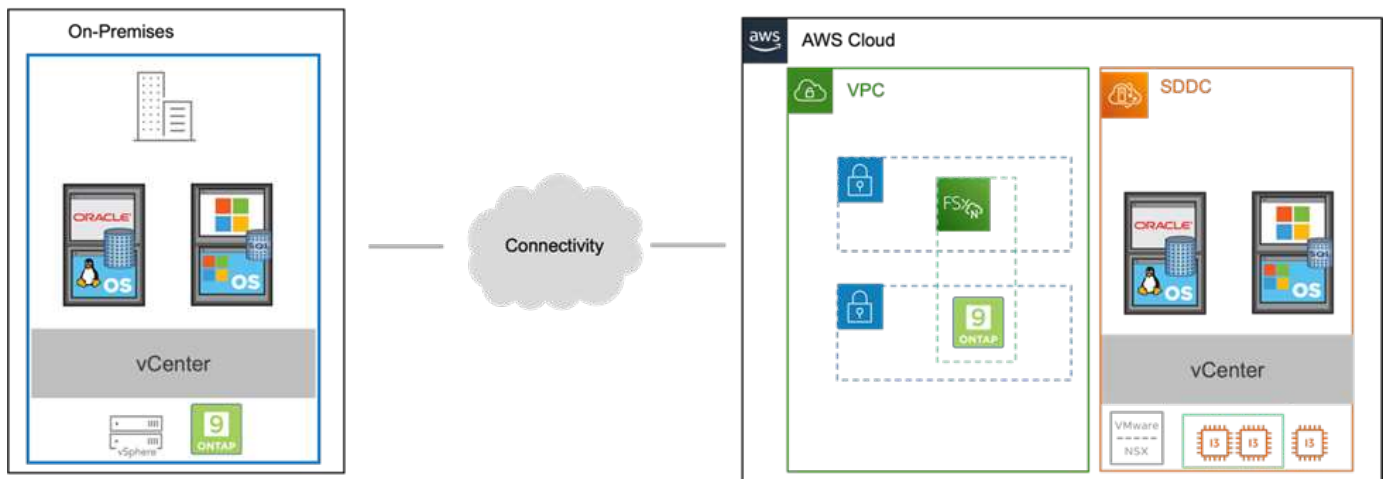
Authors: Chris Reno, Josh Powell, and Suresh Thoppay - NetApp Solutions Engineering

Overview

A proven disaster recovery (DR) environment and plan is critical for organizations to ensure that business-critical applications can be rapidly restored in the event of a major outage. This solution focuses on demonstrating DR use cases with a focus on VMware and NetApp technologies, both on-premises and with VMware Cloud on AWS.

NetApp has a long history of integration with VMware as evidenced by the tens of thousands of customers that have chosen NetApp as their storage partner for their virtualized environment. This integration continues with guest-connected options in the cloud and recent integrations with NFS datastores as well. This solution focuses on the use case commonly referred to as guest-connected storage.

In guest-connected storage, the guest VMDK is deployed on a VMware-provisioned datastore, and application data is housed on iSCSI or NFS and mapped directly to the VM. Oracle and MS SQL applications are used to demonstrate a DR scenario, as shown in the following figure.



Assumptions, pre-requisites and component overview

Before deploying this solution, review the overview of the components, the required pre-requisites to deploy the solution and assumptions made in documenting this solution.

[DR Solution Requirements, Pre-requisites and Planning](#)

Performing DR with SnapCenter

In this solution, SnapCenter provides application-consistent snapshots for SQL Server and Oracle application data. This configuration, together with SnapMirror technology, provides high-speed data replication between our on-premises AFF and FSx ONTAP cluster. Additionally, Veeam Backup & Replication provides backup and restore capabilities for our virtual machines.

In this section, we cover the configuration of SnapCenter, SnapMirror, and Veeam for both backup and restore.

The following sections cover configuration and the steps needed to complete a failover at the secondary site:

Configure SnapMirror relationships and retention schedules

SnapCenter can update SnapMirror relationships within the primary storage system (primary > mirror) and to secondary storage systems (primary > vault) for the purpose of long-term archiving and retention. To do so, you must establish and initialize a data replication relationship between a destination volume and a source volume using SnapMirror.

The source and destination ONTAP systems must be in networks that are peered using Amazon VPC peering, a transit gateway, AWS Direct Connect, or an AWS VPN.

The following steps are required for setting up SnapMirror relationships between an on-premises ONTAP system and FSx ONTAP:



Refer to the [FSx for ONTAP – ONTAP User Guide](#) for more information on creating SnapMirror relationships with FSx.

Record the source and destination Intercluster logical interfaces

For the source ONTAP system residing on-premises, you can retrieve the inter-cluster LIF information from System Manager or from the CLI.

1. In ONTAP System Manager, navigate to the Network Overview page and retrieve the IP addresses of Type: Intercluster that are configured to communicate with the AWS VPC where FSx is installed.

Name	Status	Storage VM	IPspace	Address	Current Node	Current Port	Portset	Protocols	Type	Thr
veeam_repo	✓	Backup	Default	10.61.181.179	E13A300_1	a0a-181		SMB/CIFS, NFS, S3	Data	0
CM01	✓		Default	10.61.181.180	E13A300_1	a0a-181			Cluster/Node Mgmt	0
HC_N1	✓		Default	10.61.181.183	E13A300_1	a0a-181			Intercluster, Cluster/Node Mgmt	0
HC_N2	✓		Default	10.61.181.184	E13A300_2	a0a-181			Intercluster, Cluster/Node Mgmt	0
lif_ora_vvm_614	✓	ora_vvm	Default	10.61.181.185	E13A300_1	a0a-181		SMB/CIFS, NFS, FL...	Data	0

2. To retrieve the Intercluster IP addresses for FSx, log into the CLI and run the following command:

```
FSx-Dest::> network interface show -role intercluster
```

```
FsxId0ae40e08acc0dea67::> network interface show -role intercluster
Vserver      Logical   Status   Network   Current   Current   Is
Interface    Admin/Oper Address/Mask Node       Port      Home
-----
FsxId0ae40e08acc0dea67
inter_1      up/up    172.30.15.42/25 FsxId0ae40e08acc0dea67-01
                                     e0e      true
inter_2      up/up    172.30.14.28/26 FsxId0ae40e08acc0dea67-02
                                     e0e      true
2 entries were displayed.
```

Establish cluster peering between ONTAP and FSx

To establish cluster peering between ONTAP clusters, a unique passphrase entered at the initiating ONTAP cluster must be confirmed in the other peer cluster.

1. Set up peering on the destination FSx cluster using the `cluster peer create` command. When prompted, enter a unique passphrase that is used later on the source cluster to finalize the creation process.

```
FSx-Dest::> cluster peer create -address-family ipv4 -peer-addr  
source_intercluster_1, source_intercluster_2  
Enter the passphrase:  
Confirm the passphrase:
```

2. At the source cluster, you can establish the cluster peer relationship using either ONTAP System Manager or the CLI. From ONTAP System Manager, navigate to Protection > Overview and select Peer Cluster.

ONTAP System Manager

DASHBOARD

STORAGE

- Overview
- Volumes
- LUNs
- Consistency Groups
- NVMe Namespaces
- Shares
- Buckets
- Qtrees
- Quotas
- Storage VMs
- Tiers

NETWORK

- Overview
- Ethernet Ports
- FC Ports

EVENTS & JOBS

PROTECTION

- Overview
- Relationships

HOSTS

Overview

< Intercluster Settings

Network Interfaces

IP ADDRESS

- ✓ 10.61.181.184
- ✓ 172.21.146.217
- ✓ 10.61.181.183
- ✓ 172.21.146.216

Cluster Peers

PEERED CLUSTER NAME

- ✓ FsxId0ae40e08acc0dea67
- ✓ OTS02

Peer Cluster

Generate Passphrase

Manage Cluster Peers

Mediator ?

Not configured.

Configure

Storage VM Peers

PEERED STORAGE VMS

- ✓ 3

3. In the Peer Cluster dialog box, fill out the required information:
 - a. Enter the passphrase that was used to establish the peer cluster relationship on the destination FSx cluster.

- b. Select **Yes** to establish an encrypted relationship.
- c. Enter the intercluster LIF IP address(es) of the destination FSx cluster.
- d. Click **Initiate Cluster Peering** to finalize the process.

Peer Cluster ✕

Local
Remote

STORAGE VM PERMISSIONS

All storage VMs (incl... ✕

Storage VMs created in the future also will be given permissions.

PASSPHRASE ?

.....

It cannot be determined from the passphrase whether this relationship was encrypted. Is the relationship encrypted?

Yes
No

To generate passphrase, Launch Remote Cluster

Intercluster Network Interfaces IP Addresses

172.30.15.42

172.30.14.28

Cancel

+ Add

Initiate Cluster Peering

Cancel

4. Verify the status of the cluster peer relationship from the FSx cluster with the following command:

```
FSx-Dest::> cluster peer show
```

```

FsxId0ae40e08acc0dea67::> cluster peer show
Peer Cluster Name      Cluster Serial Number Availability  Authentication
-----
E13A300                1-80-000011    Available   ok

```

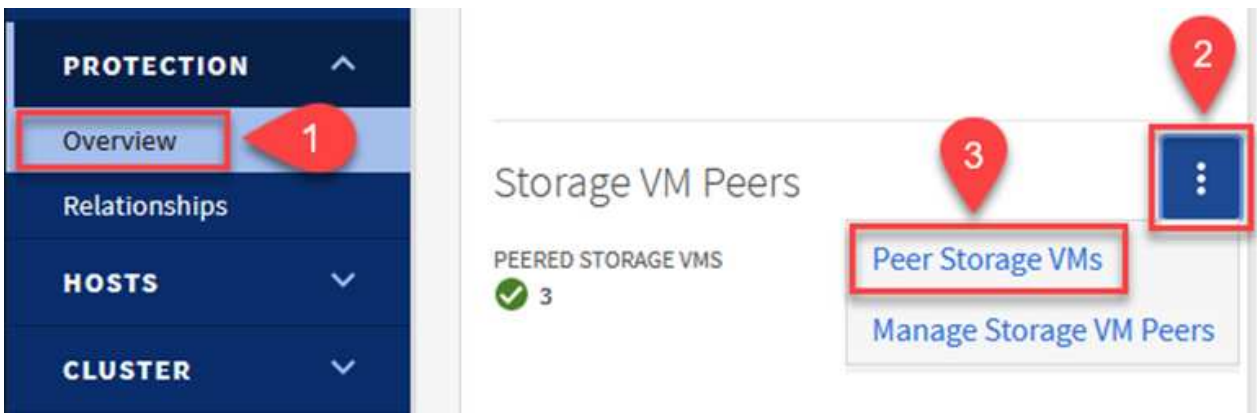
Establish SVM peering relationship

The next step is to set up an SVM relationship between the destination and source storage virtual machines that contain the volumes that will be in SnapMirror relationships.

1. From the source FSx cluster, use the following command from the CLI to create the SVM peer relationship:

```
FSx-Dest::> vserver peer create -vserver DestSVM -peer-vserver Backup -peer-cluster OnPremSourceSVM -applications snapmirror
```

2. From the source ONTAP cluster, accept the peering relationship with either ONTAP System Manager or the CLI.
3. From ONTAP System Manager, go to Protection > Overview and select Peer Storage VMs under Storage VM Peers.



4. In the Peer Storage VM's dialog box, fill out the required fields:
 - The source storage VM
 - The destination cluster
 - The destination storage VM



5. Click Peer Storage VMs to complete the SVM peering process.

Create a snapshot retention policy

SnapCenter manages retention schedules for backups that exist as snapshot copies on the primary storage system. This is established when creating a policy in SnapCenter. SnapCenter does not manage retention policies for backups that are retained on secondary storage systems. These policies are managed separately through a SnapMirror policy created on the secondary FSx cluster and associated with the destination volumes that are in a SnapMirror relationship with the source volume.

When creating a SnapCenter policy, you have the option to specify a secondary policy label that is added to the SnapMirror label of each snapshot generated when a SnapCenter backup is taken.



On the secondary storage, these labels are matched to policy rules associated with the destination volume for the purpose of enforcing retention of snapshots.

The following example shows a SnapMirror label that is present on all snapshots generated as part of a policy used for daily backups of our SQL Server database and log volumes.

Select secondary replication options ⓘ

☐ Update SnapMirror after creating a local Snapshot copy.

☒ Update SnapVault after creating a local Snapshot copy.

Secondary policy label

Custom Label ⓘ

sql-daily

Error retry count

3 ⓘ

For more information on creating SnapCenter policies for a SQL Server database, see the [SnapCenter documentation](#).

You must first create a SnapMirror policy with rules that dictate the number of snapshot copies to retain.

1. Create the SnapMirror Policy on the FSx cluster.

```
FSx-Dest::> snapmirror policy create -vserver DestSVM -policy  
PolicyName -type mirror-vault -restart always
```

2. Add rules to the policy with SnapMirror labels that match the secondary policy labels specified in the SnapCenter policies.

```
FSx-Dest::> snapmirror policy add-rule -vserver DestSVM -policy  
PolicyName -snapmirror-label SnapMirrorLabelName -keep  
#ofSnapshotsToRetain
```

The following script provides an example of a rule that could be added to a policy:

```
FSx-Dest::> snapmirror policy add-rule -vserver sql_svm_dest -policy Async_SnapCenter_SQL -snapmirror-label sql-ondemand -keep 15
```



Create additional rules for each SnapMirror label and the number of snapshots to be retained (retention period).

Create destination volumes

To create a destination volume on FSx that will be the recipient of snapshot copies from our source volumes, run the following command on FSx ONTAP:

```
FSx-Dest::> volume create -vserver DestSVM -volume DestVolName  
-aggregate DestAggrName -size VolSize -type DP
```

Create the SnapMirror relationships between source and destination volumes

To create a SnapMirror relationship between a source and destination volume, run the following command on FSx ONTAP:

```
FSx-Dest::> snapmirror create -source-path  
OnPremSourceSVM:OnPremSourceVol -destination-path DestSVM:DestVol -type  
XDP -policy PolicyName
```

Initialize the SnapMirror relationships

Initialize the SnapMirror relationship. This process initiates a new snapshot generated from the source volume and copies it to the destination volume.

```
FSx-Dest::> snapmirror initialize -destination-path DestSVM:DestVol
```

Deploy and configure Windows SnapCenter server on-premises.

Deploy Windows SnapCenter Server on premises

This solution uses NetApp SnapCenter to take application-consistent backups of SQL Server and Oracle databases. In conjunction with Veeam Backup & Replication for backing up virtual machine VMDKs, this provides a comprehensive disaster recovery solution for on-premises and cloud-based datacenters.

SnapCenter software is available from the NetApp support site and can be installed on Microsoft Windows systems that reside either in a domain or workgroup. A detailed planning guide and installation instructions can be found at the [NetApp Documentation Center](#).

The SnapCenter software can be obtained at [this link](#).

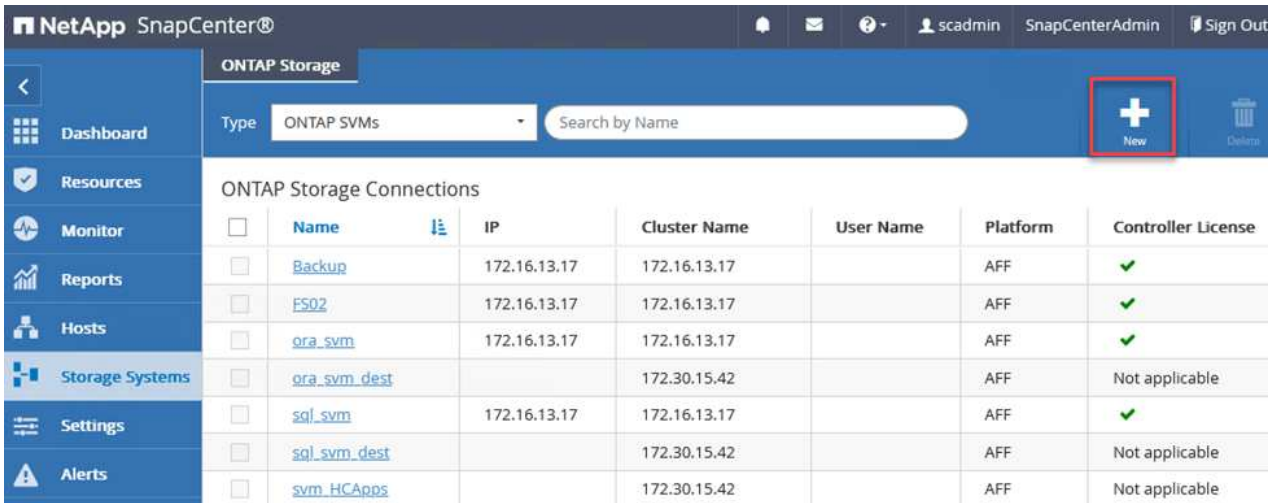
After it is installed, you can access the SnapCenter console from a web browser using *https://Virtual_Cluster_IP_or_FQDN:8146*.

After you log into the console, you must configure SnapCenter for backup SQL Server and Oracle databases.

Add storage controllers to SnapCenter

To add storage controllers to SnapCenter, complete the following steps:

1. From the left menu, select Storage Systems and then click New to begin the process of adding your storage controllers to SnapCenter.



The screenshot shows the NetApp SnapCenter web interface. The left sidebar contains a navigation menu with options: Dashboard, Resources, Monitor, Reports, Hosts, Storage Systems (selected), Settings, and Alerts. The main content area is titled 'ONTAP Storage' and includes a 'Type' dropdown set to 'ONTAP SVMs' and a 'Search by Name' input field. A red box highlights the '+ New' button in the top right corner of the main content area. Below this, there is a table titled 'ONTAP Storage Connections' with columns: Name, IP, Cluster Name, User Name, Platform, and Controller License. The table lists several storage systems, including 'Backup', 'FS02', 'ora_svm', 'ora_svm_dest', 'sql_svm', 'sql_svm_dest', and 'svm_HCAppls'.

	Name	IP	Cluster Name	User Name	Platform	Controller License
<input type="checkbox"/>	Backup	172.16.13.17	172.16.13.17		AFF	✓
<input type="checkbox"/>	FS02	172.16.13.17	172.16.13.17		AFF	✓
<input type="checkbox"/>	ora_svm	172.16.13.17	172.16.13.17		AFF	✓
<input type="checkbox"/>	ora_svm_dest		172.30.15.42		AFF	Not applicable
<input type="checkbox"/>	sql_svm	172.16.13.17	172.16.13.17		AFF	✓
<input type="checkbox"/>	sql_svm_dest		172.30.15.42		AFF	Not applicable
<input type="checkbox"/>	svm_HCAppls		172.30.15.42		AFF	Not applicable


2. In the Add Storage System dialog box, add the management IP address for the local on-premises ONTAP cluster and the username and password. Then click Submit to begin discovery of the storage system.

Add Storage System

Add Storage System

Storage System	<input type="text" value="10.61.181.180"/>
Username	<input type="text" value="admin"/>
Password	<input type="password" value="••••••••"/>

Event Management System (EMS) & AutoSupport Settings

- ☒ Send AutoSupport notification to storage system
- ☒ Log SnapCenter Server events to syslog
-  **More Options** : Platform, Protocol, Preferred IP etc..

- Repeat this process to add the FSx ONTAP system to SnapCenter. In this case, select More Options at the bottom of the Add Storage System window and click the check box for Secondary to designate the FSx system as the secondary storage system updated with SnapMirror copies or our primary backup snapshots.

More Options




Platform

☒ Secondary 

Protocol

Port

Timeout 

☐ Preferred IP 

Save

Cancel

For more information related to adding storage systems to SnapCenter, see the documentation at [this link](#).

Add hosts to SnapCenter

The next step is adding host application servers to SnapCenter. The process is similar for both SQL Server and Oracle.

1. From the left menu, select Hosts and then click Add to begin the process of adding storage controllers to SnapCenter.
2. In the Add Hosts window, add the Host Type, Hostname, and the host system Credentials. Select the plug-in type. For SQL Server, select the Microsoft Windows and Microsoft SQL Server plug-in.

NetApp SnapCenter®

Managed Hosts

Search by Name

<input type="checkbox"/>	Name
<input type="checkbox"/>	oraclesrv_01.sddc.netapp.com
<input type="checkbox"/>	oraclesrv_02.sddc.netapp.com
<input type="checkbox"/>	oraclesrv_03.sddc.netapp.com
<input type="checkbox"/>	oraclesrv_04.sddc.netapp.com
<input type="checkbox"/>	oraclesrv_05.sddc.netapp.com
<input type="checkbox"/>	oraclesrv_06.sddc.netapp.com
<input type="checkbox"/>	oraclesrv_07.sddc.netapp.com
<input type="checkbox"/>	oraclesrv_08.sddc.netapp.com
<input type="checkbox"/>	oraclesrv_09.sddc.netapp.com
<input type="checkbox"/>	oraclesrv_10.sddc.netapp.com

Add Host

Host Type:

Host Name:

Credentials:

Select Plug-ins to Install SnapCenter Plug-ins Package 4.6 for Windows

- ☒ Microsoft Windows
- ☒ Microsoft SQL Server
- ☐ Microsoft Exchange Server
- ☐ SAP HANA

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

3. For Oracle, fill out the required fields in the Add Host dialog box and select the check box for the Oracle Database plug-in. Then click Submit to begin the discovery process and to add the host to SnapCenter.

Add Host

Host Type Linux ▾

Host Name oraclesrv_11.sddc.netapp.com

Credentials root ▾



Select Plug-ins to Install SnapCenter Plug-ins Package 4.6 for Linux

☒ Oracle Database

☐ SAP HANA

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

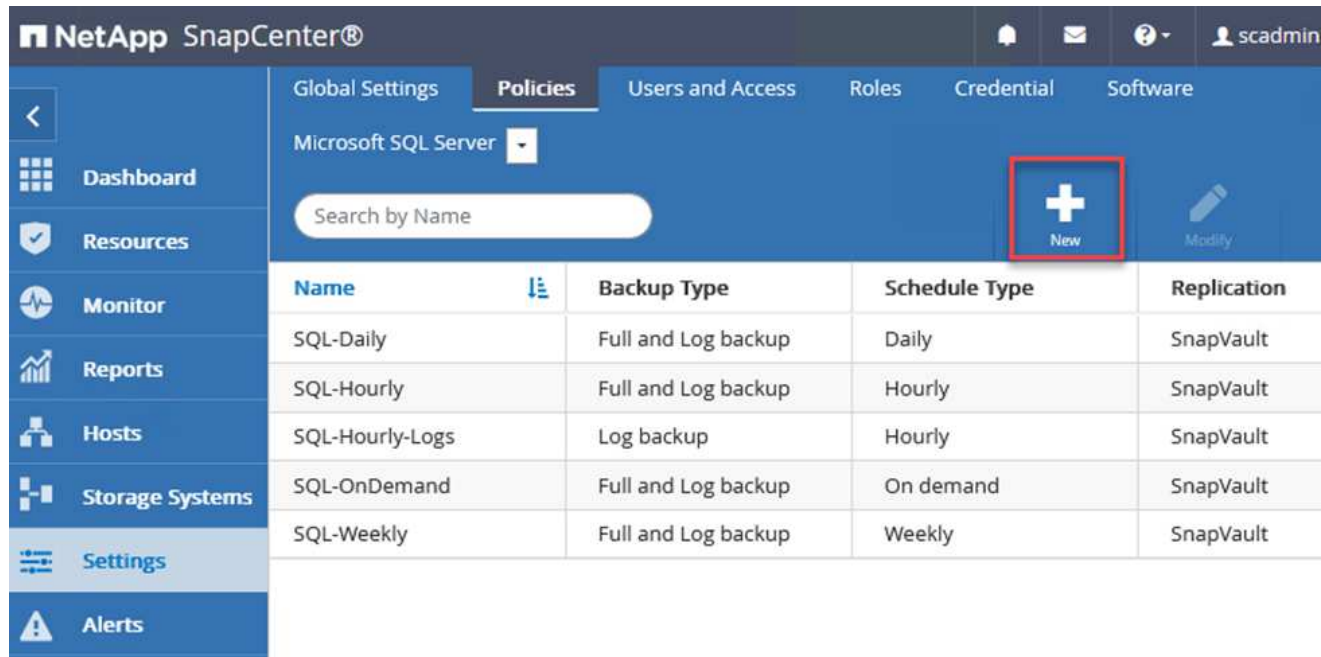
Submit

Cancel

Create SnapCenter policies

Policies establish the specific rules to be followed for a backup job. They include, but are not limited to, the backup schedule, replication type, and how SnapCenter handles backing up and truncating transaction logs.

You can access policies in the Settings section of the SnapCenter web client.



For complete information on creating policies for SQL Server backups, see the [SnapCenter documentation](#).

For complete information on creating policies for Oracle backups, see the [SnapCenter documentation](#).

Notes:

- As you progress through the policy creation wizard, take special note of the Replication section. In this section you stipulate the types of secondary SnapMirror copies that you want taken during the backups process.
- The “Update SnapMirror after creating a local Snapshot copy” setting refers to updating a SnapMirror relationship when that relationship exists between two storage virtual machines residing on the same cluster.
- The “Update SnapVault after creating a local SnapShot copy” setting is used to update a SnapMirror relationship that exists between two separate cluster and between an on-premises ONTAP system and Cloud Volumes ONTAP or FSxN.

The following image shows the preceding options and how they look in the backup policy wizard.

New SQL Server Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

Select secondary replication options ⓘ

☐ Update SnapMirror after creating a local Snapshot copy.

☐ Update SnapVault after creating a local Snapshot copy.

Secondary policy label

Choose

Error retry count

3

Create SnapCenter Resource Groups

Resource Groups allow you to select the database resources you want to include in your backups and the policies followed for those resources.

1. Go to the Resources section in the left-hand menu.
2. At the top of the window, select the resource type to work with (In this case Microsoft SQL Server) and then click New Resource Group.

Name	Resource Count	Tags	Policies	Last Backup	Overall Status
SQLSRV-01	1		SQL-Daily SQL-Hourly SQL-OnDemand SQL-Weekly	05/11/2022 ...	Completed
SQLSRV-02	1		SQL-Daily SQL-Hourly SQL-OnDemand SQL-Weekly	03/28/2022 ...	Failed
SQLSRV-03	1		SQL-Daily SQL-Hourly	05/11/2022 ...	Completed

The SnapCenter documentation covers step-by-step details for creating Resource Groups for both SQL Server and Oracle databases.

For backing up SQL resources, follow [this link](#).

For Backing up Oracle resources, follow [this link](#).

Deploy and configure Veeam Backup Server

Veeam Backup & Replication software is used in the solution to back up our application virtual machines and archive a copy of the backups to an Amazon S3 bucket using a Veeam scale-out backup repository (SOBR). Veeam is deployed on a Windows server in this solution. For specific guidance on deploying Veeam, see the [Veeam help Center Technical documentation](#).

Configure Veeam scale-out backup repository

After you deploy and license the software, you can create a scale-out backup repository (SOBR) as target storage for backup jobs. You should also include an S3 bucket as a backup of VM data offsite for disaster recovery.

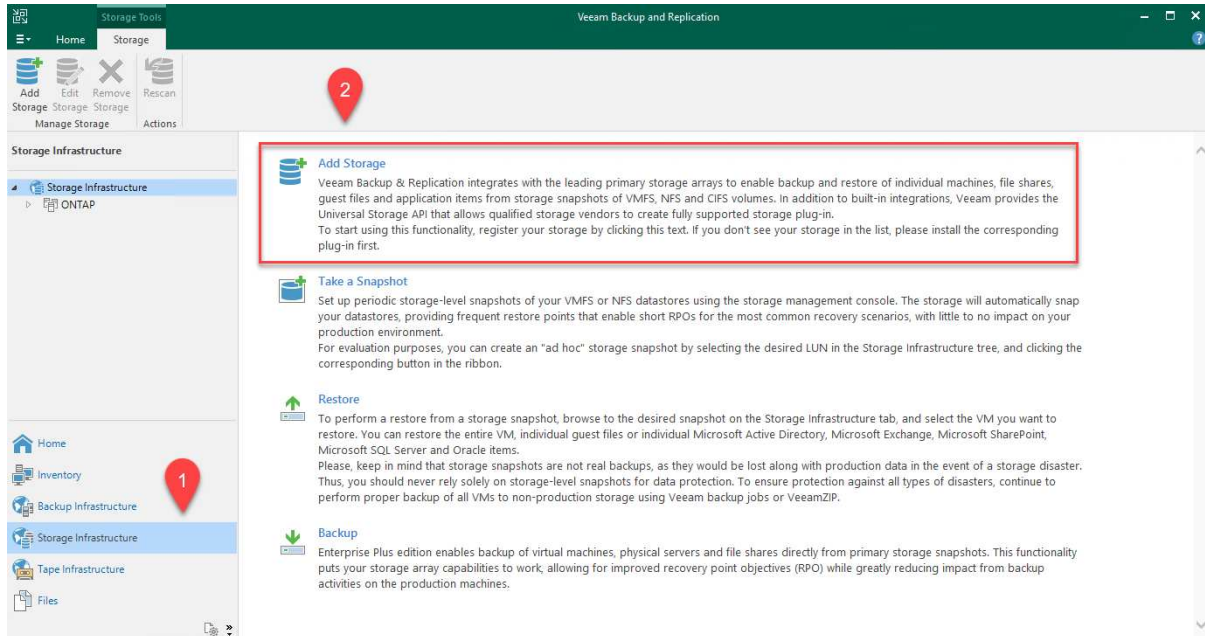
See the following prerequisites before getting started.

1. Create an SMB file share on your on-premises ONTAP system as the target storage for backups.
2. Create an Amazon S3 bucket to include in the SOBR. This is a repository for the offsite backups.

Add ONTAP Storage to Veeam

First, add the ONTAP storage cluster and associated SMB/NFS filesystem as storage infrastructure in Veeam.

1. Open the Veeam console and log in. Navigate to Storage Infrastructure and then select Add Storage.



2. In the Add Storage wizard, select NetApp as the storage vendor and then select Data ONTAP.
3. Enter the management IP address and check the NAS Filer box. Click Next.

New NetApp Data ONTAP Storage



Name

Register NetApp Data ONTAP storage by specifying DNS name or IP address.

Name	Management server DNS name or IP address: <input type="text" value="10.61.181.180"/>
Credentials	Description: <input type="text" value="Created by SDDC\jpowell at 5/17/2022 10:34 AM."/>
NAS Filer	Role: <input type="checkbox"/> Block or file storage for VMware vSphere <input type="checkbox"/> Block storage for Microsoft Windows servers <input checked="" type="checkbox"/> NAS filer
Apply	
Summary	

4. Add your credentials to access the ONTAP cluster.

New NetApp Data ONTAP Storage



Credentials

Specify account with storage administrator privileges.

Name	Credentials: <input type="text" value="HCIEUC\Admin (HCIEUC\Admin, last edited: 98 days ago)"/>	<input type="button" value="Add..."/>
Credentials	Manage accounts	
NAS Filer	Protocol: <input type="text" value="HTTPS"/>	
Apply	Port: <input type="text" value="443"/>	
Summary		

5. On the NAS Filer page choose the desired protocols to scan and select Next.

New NetApp Data ONTAP Storage ✕

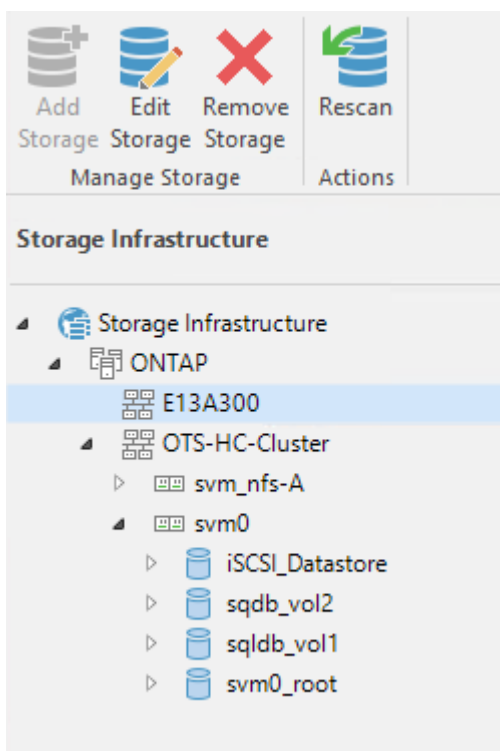
NAS Filer

Specify how this storage can be accessed by file backup jobs.

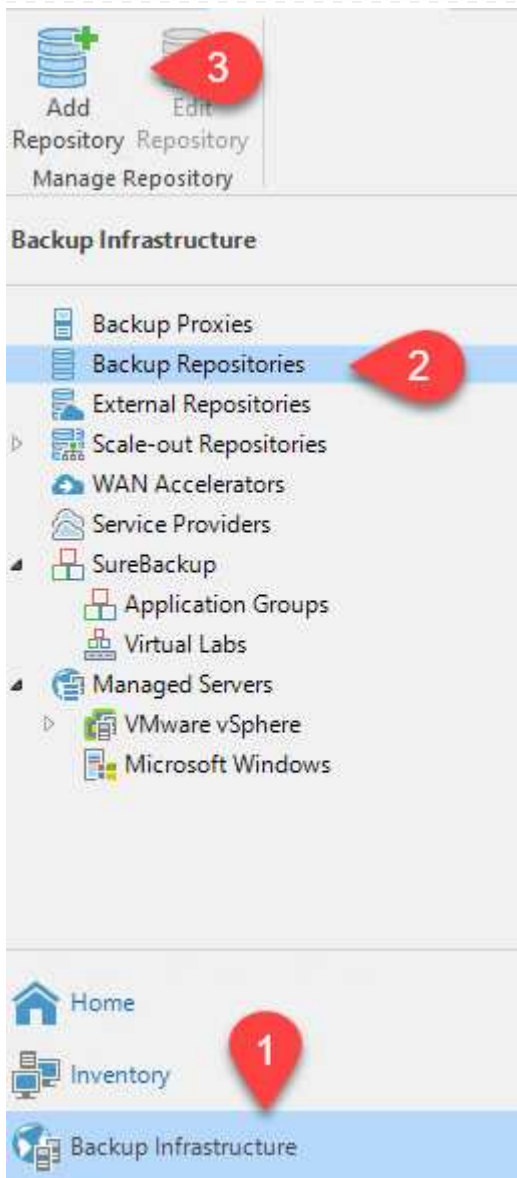
Name	Protocol to use:
Credentials	<input checked="" type="checkbox"/> SMB
NAS Filer	<input type="checkbox"/> NFS
Apply	<input checked="" type="checkbox"/> Create required export rules automatically
Summary	Volumes to scan:
	<input style="width: 100%;" type="text" value="All volumes"/> Choose...
	Backup proxies to use:
	<input style="width: 100%;" type="text" value="Automatic selection"/> Choose...

< Previous
Apply
Finish
Cancel

- Complete the Apply and Summary pages of the wizard and click Finish to begin the storage discovery process. After the scan completes, the ONTAP cluster is added along with the NAS filers as available resources.



- Create a backup repository using the newly discovered NAS shares. From Backup Infrastructure, select Backup Repositories and click the Add Repository menu item.



8. Follow all steps in the New Backup Repository Wizard to create the repository. For detailed information on creating Veeam Backup Repositories, see the [Veeam documentation](#).

New Backup Repository

**Share**

Type in UNC path to share (mapped drives are not supported), specify share access credentials and how backup jobs should write data to this share.

Name

Shared folder:

[Browse...](#)

Share

Use \\server\folder format

Repository

☒ This share requires access credentials:

sddc\administrator (sddc\administrator, last edited: 85 days ago)

[Add...](#)

Mount Server

[Manage accounts](#)

Review

Gateway server:

☒ Automatic selection☐ The following server:

Apply

Use this option to improve performance and reliability of backup to a NAS located in a remote site.

Summary

< Previous

Next >

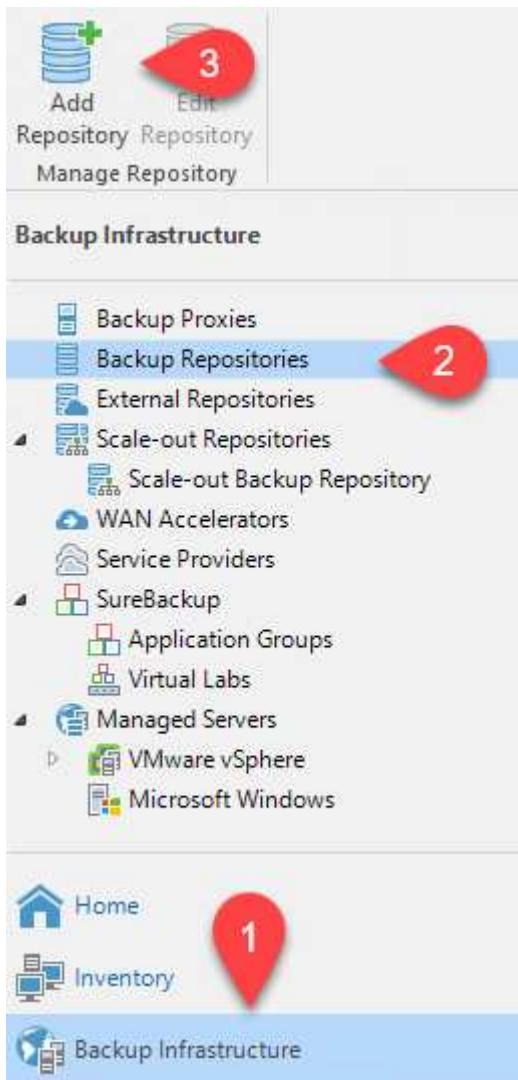
Finish

Cancel

Add the Amazon S3 bucket as a backup repository

The next step is to add the Amazon S3 storage as a backup repository.

1. Navigate to Backup Infrastructure > Backup Repositories. Click Add Repository.



2. In the Add Backup Repository wizard, select Object Storage and then Amazon S3. This starts the New Object Storage Repository wizard.

Add Backup Repository

Select the type of backup repository you want to add.



Direct attached storage

Microsoft Windows or Linux server with internal or direct attached storage. This configuration enables data movers to run directly on the server, allowing for fastest performance.



Network attached storage

Network share on a file server or a NAS device. When backing up to a remote share, we recommend that you select a gateway server located in the same site with the share.



Deduplicating storage appliance

Dell EMC Data Domain, ExaGrid, HPE StoreOnce or Quantum DXi. If you are unable to meet the requirements of advanced integration via native appliance API, use the network attached storage option instead.



Object storage

On-prem object storage system or a cloud object storage provider. Object storage can only be used as a Capacity Tier of scale-out backup repositories, backing up directly to object storage is not currently supported.

3. Provide a name for your object storage repository and click Next.
4. In the next section, provide your credentials. You need an AWS Access Key and Secret Key.

New Object Storage Repository



Account

Specify AWS account to use for connecting to Amazon S3 storage bucket.

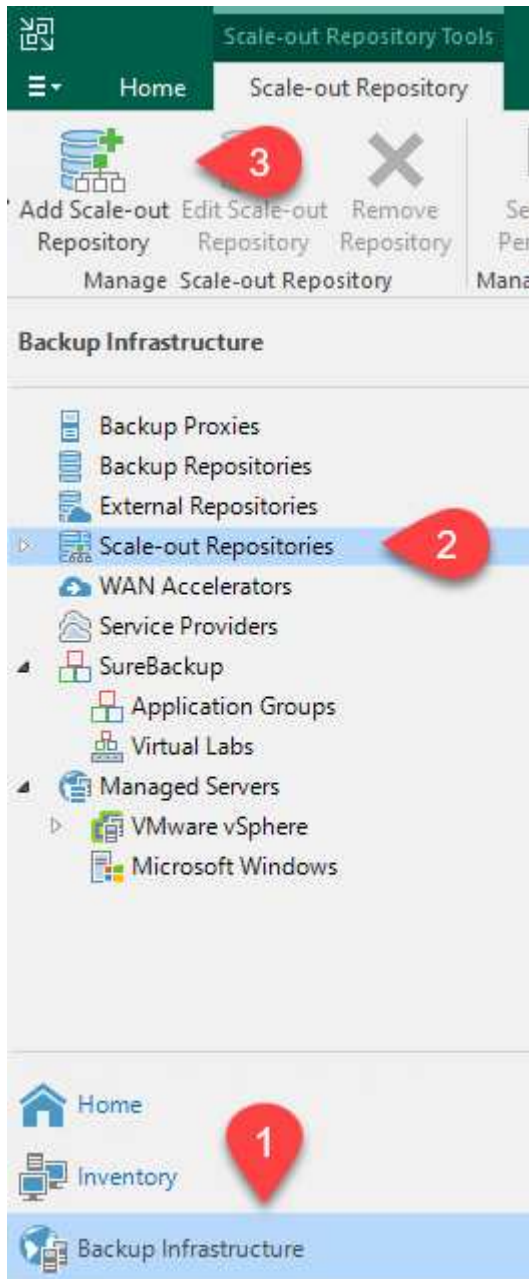
Name	Credentials:
Account	<input type="text" value="AKIAH4H43ZT557HXQT2W (last edited: 107 days ago)"/> Add...
	Manage cloud accounts
Bucket	AWS region:
Summary	<input type="text" value="Global"/>
	<input type="checkbox"/> Use the following gateway server:
	<input type="text" value="veeam.sddc.netapp.com (Backup server)"/>
	Select a gateway server to proxy access to Amazon S3. If no gateway server is specified, all scale-out backup repository extents must have direct Internet access.
	<input type="button" value=" < Previous"/> <input type="button" value=" Next > "/> <input type="button" value=" Finish "/> <input type="button" value=" Cancel "/>

5. After the Amazon configuration loads, choose your datacenter, bucket, and folder and click Apply. Finally, click Finish to close out the wizard.

Create scale-out backup repository

Now that we have added our storage repositories to Veeam, we can create the SOBR to automatically tier backup copies to our offsite Amazon S3 object storage for disaster recovery.

1. From Backup Infrastructure, select Scale-out Repositories and then click the Add Scale-out Repository menu item.



2. In the New Scale-out Backup Repository provide a name for the SOBR and click Next.
3. For the Performance Tier, choose the backup repository that contains the SMB share residing on your local ONTAP cluster.

New Scale-out Backup Repository



Performance Tier

Select backup repositories to use as the landing zone and for the short-term retention.

Name	Extents:		
Performance Tier	<table border="1"> <thead> <tr> <th>Name</th> </tr> </thead> <tbody> <tr> <td>VBRRepo2</td> </tr> </tbody> </table>	Name	VBRRepo2
Name			
VBRRepo2			
Placement Policy	<div>Add...</div> <div>Remove</div>		

- For the Placement Policy, choose either Data Locality or Performance based your requirements. Select next.
- For Capacity Tier we extend the SOBR with Amazon S3 object storage. For the purposes of disaster recovery, select Copy Backups to Object Storage as Soon as They are Created to ensure timely delivery of our secondary backups.

New Scale-out Backup Repository



Capacity Tier

Specify object storage to copy backups to for redundancy and DR purposes. Older backups can be moved to object storage completely to reduce long-term retention costs while preserving the ability to restore directly from offloaded backups.

Name	Extents:
Performance Tier	
Placement Policy	
Capacity Tier	<div> <input checked="" type="checkbox"/> Extend scale-out backup repository capacity with object storage: <div> <div>Amazon S3 Repo</div> <div>Add...</div> </div> </div>
Archive Tier	<div>Define time windows when uploading to capacity tier is allowed</div> <div>Window...</div>
Summary	<div> <input checked="" type="checkbox"/> Copy backups to object storage as soon as they are created Create additional copy of your backups for added redundancy by having all backups copied to the capacity tier as soon as they are created on the performance tier. </div> <div> <input checked="" type="checkbox"/> Move backups to object storage as they age out of the operational restore window Reduce your long-term retention costs by moving older backups to object storage completely while preserving the ability to restore directly from offloaded backups. </div> <div> Move backup files older than <input type="text" value="14"/> days (your operational restore window) <div>Override...</div> </div> <div> <input type="checkbox"/> Encrypt data uploaded to object storage Password: <div>Add...</div> <div>Manage passwords</div> </div>

< Previous

Next >

Finish

Cancel

- Finally, select Apply and Finish to finalize creation of the SOBR.

Create the scale-out backup repository jobs

The final step to configuring Veeam is to create backup jobs using the newly created SOBR as the backup destination. Creating backup jobs is a normal part of any storage administrator's repertoire and we do not cover the detailed steps here. For more complete information on creating backup jobs in Veeam, see the [Veeam Help Center Technical Documentation](#).

BlueXP backup and recovery tools and configuration

To conduct a failover of application VMs and database volumes to VMware Cloud Volume services running in AWS, you must install and configure a running instance of both SnapCenter Server and Veeam Backup and Replication Server. After the failover is complete, you must also configure these tools to resume normal backup operations until a failback to the on-premises datacenter is planned and executed.

Deploy secondary Windows SnapCenter Server

SnapCenter Server is deployed in the VMware Cloud SDDC or installed on an EC2 instance residing in a VPC with network connectivity to the VMware Cloud environment.

SnapCenter software is available from the NetApp support site and can be installed on Microsoft Windows systems that reside either in a domain or workgroup. A detailed planning guide and installation instructions can be found at the [NetApp documentation center](#).

You can find the SnapCenter software at [this link](#).

Configure secondary Windows SnapCenter Server

To perform a restore of application data mirrored to FSx ONTAP, you must first perform a full restore of the on-premises SnapCenter database. After this process is complete, communication with the VMs is reestablished and application backups can now resume using FSx ONTAP as the primary storage.

To achieve this, you must complete the following items on the SnapCenter Server:

1. Configure the computer name to be identical to the original on-premises SnapCenter Server.
2. Configure networking to communicate with VMware Cloud and the FSx ONTAP instance.
3. Complete the procedure to restore the SnapCenter database.
4. Confirm that SnapCenter is in Disaster Recovery mode to make sure that FSx is now the primary storage for backups.
5. Confirm that communication is reestablished with the restored virtual machines.

For more information on completing these steps, see to section "[SnapCenter database Restore Process](#)".

Deploy secondary Veeam Backup & Replication server

You can install the Veeam Backup & Replication server on a Windows server in the VMware Cloud on AWS or on an EC2 instance. For detailed implementation guidance, see the [Veeam Help Center Technical Documentation](#).

Configure secondary Veeam Backup & Replication server

To perform a restore of virtual machines that have been backed up to Amazon S3 storage, you must install the Veeam Server on a Windows server and configure it to communicate with VMware Cloud, FSx ONTAP, and the S3 bucket that contains the original backup repository. It must also have a new backup repository configured on FSx ONTAP to conduct new backups of the VMs after they are restored.

To perform this process, the following items must be completed:

1. Configure networking to communicate with VMware Cloud, FSx ONTAP, and the S3 bucket containing the original backup repository.
2. Configure an SMB share on FSx ONTAP to be a new backup repository.
3. Mount the original S3 bucket that was used as part of the scale-out backup repository on premises.
4. After restoring the VM, establish new backup jobs to protect SQL and Oracle VMs.

For more information on restoring VMs using Veeam, see the section ["Restore Application VMs with Veeam Full Restore"](#).

SnapCenter database backup for disaster recovery

SnapCenter allows for the backup and recovery of its underlying MySQL database and configuration data for the purpose of recovering the SnapCenter server in the case of a disaster. For our solution, we recovered the SnapCenter database and configuration on an AWS EC2 instance residing in our VPC. For more information on this step, see [this link](#).

SnapCenter backup prerequisites

The following prerequisites are required for SnapCenter backup:

- A volume and SMB share created on the on-premises ONTAP system to locate the backed-up database and configuration files.
- A SnapMirror relationship between the on-premises ONTAP system and FSx or CVO in the AWS account. This relationship is used for transporting the snapshot containing the backed-up SnapCenter database and configuration files.
- Windows Server installed in the cloud account, either on an EC2 instance or on a VM in the VMware Cloud SDDC.
- SnapCenter installed on the Windows EC2 instance or VM in VMware Cloud.

SnapCenter backup and restore process summary

- Create a volume on the on-premises ONTAP system for hosting the backup db and config files.
- Set up a SnapMirror relationship between on-premises and FSx/CVO.
- Mount the SMB share.
- Retrieve the Swagger authorization token for performing API tasks.
- Start the db restore process.
- Use the xcopy utility to copy the db and config file local directory to the SMB share.
- On FSx, create a clone of the ONTAP volume (copied via SnapMirror from on-premises).
- Mount the SMB share from FSx to EC2/VMware Cloud.
- Copy the restore directory from the SMB share to a local directory.
- Run the SQL Server restore process from Swagger.

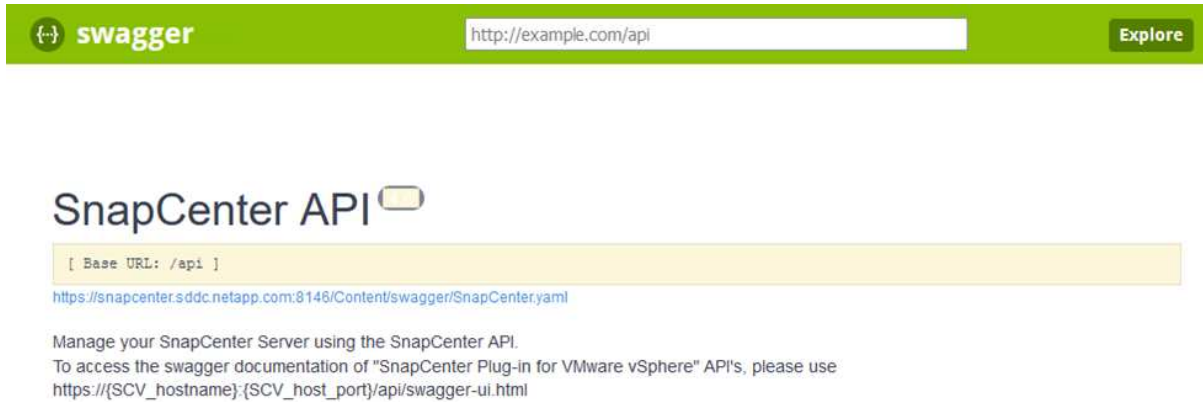
Back up the SnapCenter database and configuration

SnapCenter provides a web client interface for executing REST API commands. For information on accessing the REST APIs through Swagger, see the SnapCenter documentation at [this link](#).

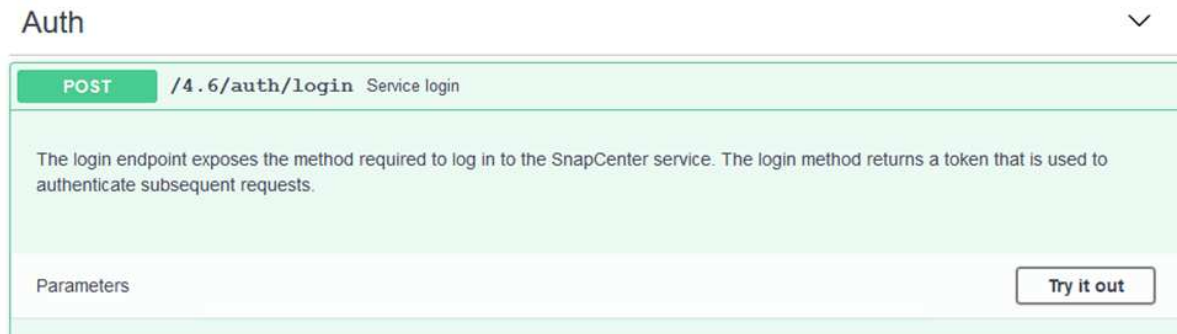
Log into Swagger and obtain authorization token

After you have navigated to the Swagger page, you must retrieve an authorization token to initiate the database restore process.

1. Access the SnapCenter Swagger API web page at *https://<SnapCenter Server IP>:8146/swagger/*.



2. Expand the Auth section and click Try it Out.



3. In the UserOperationContext area, fill in the SnapCenter credentials and role and click Execute.

Name	Description
TokenNeverExpires	Token never expires
boolean (query)	<div>false</div>
UserOperationContext * required	User credentials
object (body)	<div>Edit Value Model</div> <pre>{ "UserOperationContext": { "User": { "Name": "localhost\\scadmin", "Passphrase": "NetApp321", "Rolename": "SnapCenterAdmin" } } }</pre> <div>Cancel</div> <div>Parameter content type</div> <div>application/json</div> <div>Execute</div>

4. In the Response body below, you can see the token. Copy the token text for authentication when executing the backup process.

200

Response body


```
{
  "PluginName": null,
  "HostId": 0,
  "RoleId": null,
  "JobIds": null
},
{
  "User": {
    "Token": "KlYxOg==tsV6EOdtdAmAYpe8q5SG6wcoGaSjwME6jrlNy5CsY63HQ5LkoZLIESRNAhpGJJ0UQUynENdgtVGDZnvx+I/ZJZIn5M1NZrj6CLfGTApp1GacagT08bqb5bMTx07BodrAidzAXUDb3GyLOKtW0GdwKzSeUwKj3uVupnk1E3lskK6PRBv9RS8j0qHQvo4v4RL0hhThhwFhV9/23nFeJVP/p1Ev4vrV/zeZVTUHFHUM069XRe5cuW9mwyj4b0I5Y5FN3XDkjqQ=",
    "Name": "SCAdmin",
    "TokenHashed": null,
    "Type": "",
    "TokenTime": "2022-03-22T14:21:57.3665661-07:00",
    "Id": "1",
    "FullName": "SCAdmin",
    "Host": null,
    "Author": null,
    "UserName": "",
    "Domain": "",
    "Passphrase": ""
  }
}
```

Download

Perform a SnapCenter database backup

Next go to the Disaster Recovery area on the Swagger page to begin the SnapCenter backup process.

1. Expand the Disaster Recovery area by clicking it.

Disaster Recovery 

GET

/4.6/disasterrecovery/server/backup

Fetch all the existing SnapCenter Server DR Backups.

POST

/4.6/disasterrecovery/server/backup

Starts the SnapCenter Server DR backup.

DELETE

/4.6/disasterrecovery/server/backup

Deletes the existing Snapcenter DR backup.

POST

/4.6/disasterrecovery/server/restore

Starts SnapCenter Server Restore.

POST

/4.6/disasterrecovery/storage

Enable or disable the storage disaster recovery.

2. Expand the /4.6/disasterrecovery/server/backup section and click Try it Out.

POST

/4.6/disasterrecovery/server/backup

Starts the SnapCenter Server DR backup.

Starts and creates a new SnapCenter Server DR backup.

Parameters

Try it out

3. In the SmDRBackupRequest section, add the correct local target path and select Execute to start the backup of the SnapCenter database and configuration.



The backup process does not allow backing up directly to an NFS or CIFS file share.

Name	Description
Token * required string (header)	User authorization token <div>TUHFHUM069XRe5cuW9nwyj4b0l5Y5FN3XDkjQ==</div>
SmDRBackupRequest * required object (body)	Parameters to take Backup <div><div>Edit Value Model</div><div><pre>{ "TargetPath": "C:\\\\SnapCenter_Backups\\\\" }</pre></div></div> <div>Cancel</div> <div>Parameter content type application/json</div>

Execute

Monitor the backup job from SnapCenter

Log into SnapCenter to review log files when starting the database restore process. Under the Monitor section, you can view the details of the SnapCenter server disaster recovery backup.

Job Details

SnapCenter Server disaster recovery backup

- ✓ ▾ SnapCenter Server disaster recovery backup
 - ✓ ▶ Precheck validation
 - ✓ ▶ Disaster recovery backup of 'oraclesrv_04.sddc.netapp.com'
 - ✓ ▶ Disaster recovery backup of SnapCenter Server 'SnapCenter.sddc.netapp.com'
 - ✓ ▶ Disaster recovery backup of 'oraclesrv_02.sddc.netapp.com'
 - ✓ ▶ Disaster recovery backup of 'oraclesrv_03.sddc.netapp.com'
 - ✓ ▶ Disaster recovery backup of 'oraclesrv_05.sddc.netapp.com'
 - ✓ ▶ Disaster recovery backup of 'oraclesrv_07.sddc.netapp.com'
 - ✓ ▶ Disaster recovery backup of 'sqlsrv-02.sddc.netapp.com'
 - ✓ ▶ Disaster recovery backup of 'sqlsrv-03.sddc.netapp.com'
 - ✓ ▶ Disaster recovery backup of 'oraclesrv_10.sddc.netapp.com'
 - ✓ ▶ Disaster recovery backup of 'sqlsrv-04.sddc.netapp.com'
 - ✓ ▶ Disaster recovery backup of 'sqlsrv-01.sddc.netapp.com'
 - ✓ ▶ Disaster recovery backup of 'sqlsrv-05.sddc.netapp.com'
 - ✓ ▶ Disaster recovery backup of 'oraclesrv_09.sddc.netapp.com'
 - ✓ ▶ Disaster recovery backup of 'sqlsrv-06.sddc.netapp.com'
 - ✓ ▶ Disaster recovery backup of 'sqlsrv-07.sddc.netapp.com'

i Task Name: SnapCenter Server disaster recovery backup Start Time: 03/23/2022 10:27:11 AM End Time: 03/23/2022 10:27:47 AM

[View Logs](#)[Cancel Job](#)[Close](#)

Use XCOPY utility to copy the database backup file to the SMB share

Next you must move the backup from the local drive on the SnapCenter server to the CIFS share that is used to SnapMirror copy the data to the secondary location located on the FSx instance in AWS. Use xcopy with specific options that retain the permissions of the files.

Open a command prompt as Administrator. From the command prompt, enter the following commands:

```
xcopy <Source_Path> \\<Destination_Server_IP>\<Folder_Path> /O /X  
/E /H /K  
xcopy c:\SC_Backups\SnapCenter_DR \\10.61.181.185\snapcenter_dr /O  
/X /E /H /K
```

Failover

Disaster occurs at primary site

For a disaster that occurs at the primary on-premises datacenter, our scenario includes failover to a secondary site residing on Amazon Web Services infrastructure using VMware Cloud on AWS. We assume that the virtual machines and our on-premises ONTAP cluster are no longer accessible. In addition, both the SnapCenter and Veeam virtual machines are no longer accessible and must be rebuilt at our secondary site.

This section address failover of our infrastructure to the cloud, and we cover the following topics:

- SnapCenter database restore. After a new SnapCenter server has been established, restore the MySQL database and configuration files and toggle the database into disaster recovery mode in order to allow the secondary FSx storage to become the primary storage device.
- Restore the application virtual machines using Veeam Backup & Replication. Connect the S3 storage that contains the VM backups, import the backups, and restore them to VMware Cloud on AWS.
- Restore the SQL Server application data using SnapCenter.
- Restore the Oracle application data using SnapCenter.

SnapCenter database restore process

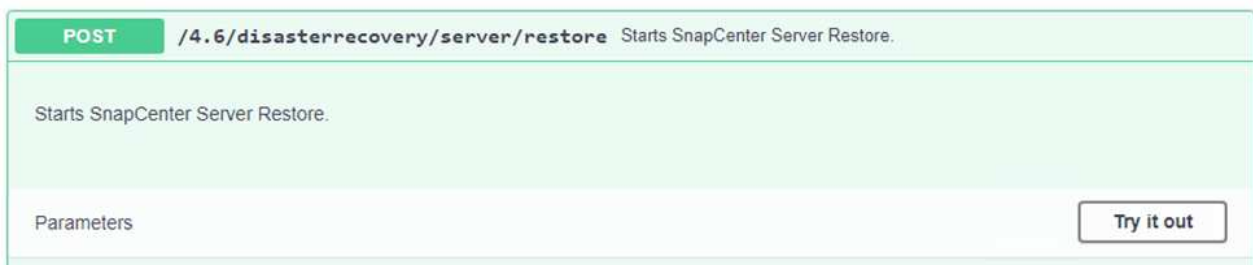
SnapCenter supports disaster recovery scenarios by allowing the backup and restore of its MySQL database and configuration files. This allows an administrator to maintain regular backups of the SnapCenter database at the on-premises datacenter and later restore that database to a secondary SnapCenter database.

To access the SnapCenter backup files on the remote SnapCenter server, complete the following steps:

1. Break the SnapMirror relationship from the FSx cluster, which makes the volume read/write.
2. Create a CIFS server (if necessary) and create a CIFS share pointing to the junction path of the cloned volume.
3. Use xcopy to copy the backup files to a local directory on the secondary SnapCenter system.
4. Install SnapCenter v4.6.
5. Ensure that SnapCenter server has the same FQDN as the original server. This is required for the db restore to be successful.

To start the restore process, complete the following steps:

1. Navigate to the Swagger API web page for the secondary SnapCenter server and follow the previous instructions to obtain an authorization token.
2. Navigate to the Disaster Recovery section of the Swagger page, select `/4.6/disasterrecovery/server/restore`, and click Try it Out.

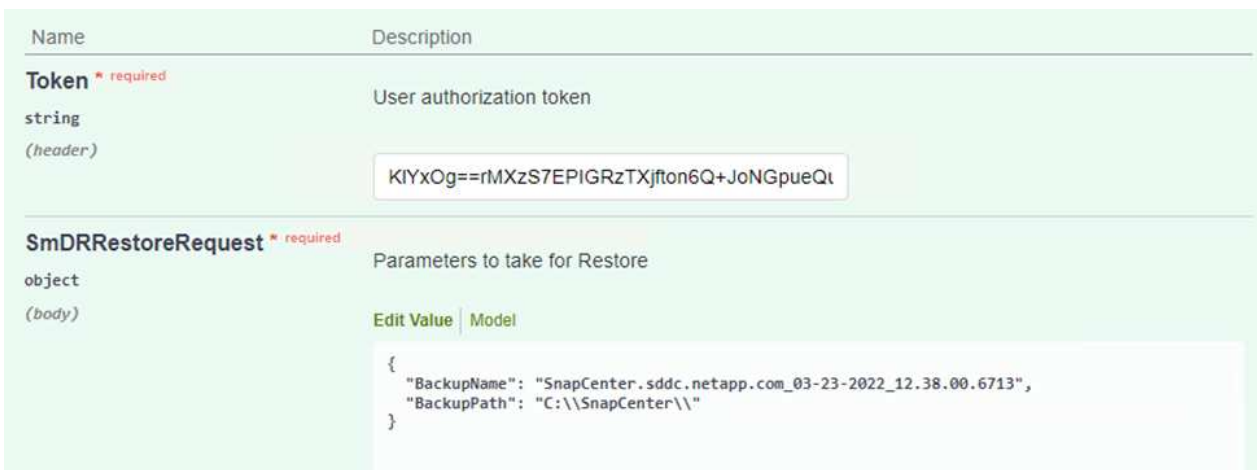


POST `/4.6/disasterrecovery/server/restore` Starts SnapCenter Server Restore.

Starts SnapCenter Server Restore.

Parameters Try it out

3. Paste in your authorization token and, in the SmDRResterRequest section, paste in the name of the backup and the local directory on the secondary SnapCenter server.



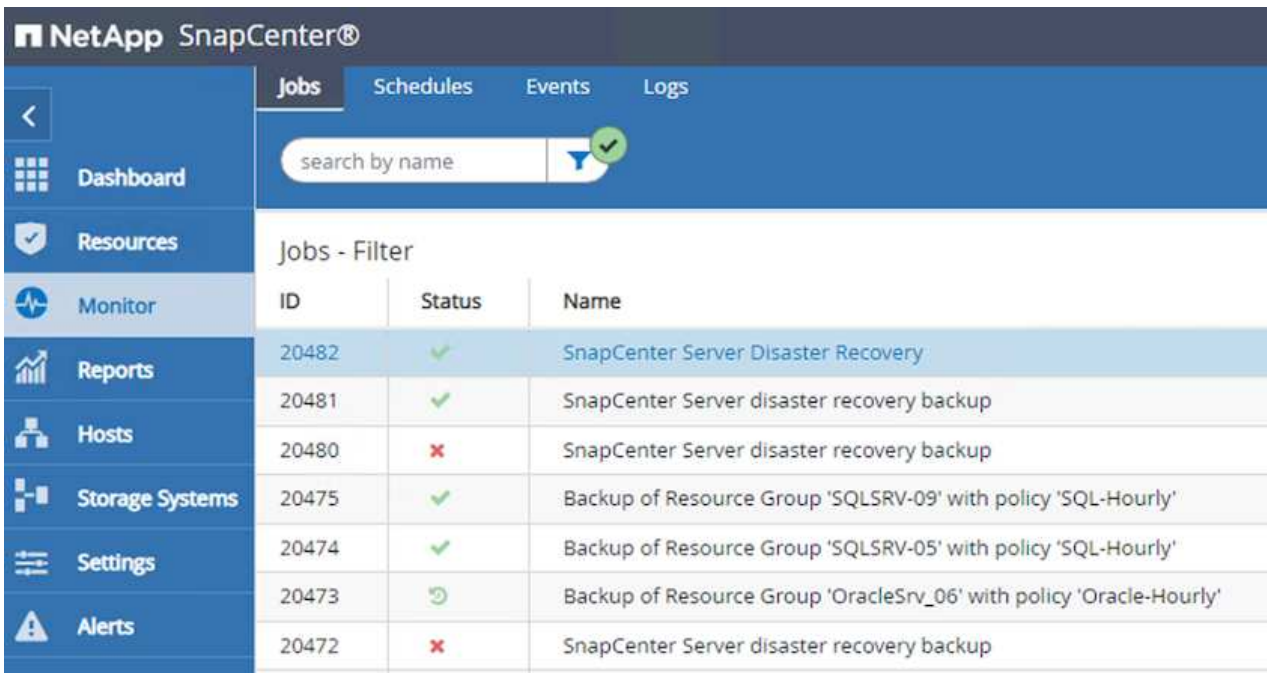
Name	Description
Token * required string (header)	User authorization token
SmDRResterRequest * required object (body)	Parameters to take for Restore

[Edit Value](#) [Model](#)

```
{
  "BackupName": "SnapCenter.sddc.netapp.com_03-23-2022_12.38.00.6713",
  "BackupPath": "C:\\SnapCenter\\"
}
```

4. Select the Execute button to start the restore process.

5. From SnapCenter, navigate to the Monitor section to view the progress of the restore job.



The screenshot shows the NetApp SnapCenter web interface. The left sidebar contains navigation links: Dashboard, Resources, Monitor (selected), Reports, Hosts, Storage Systems, Settings, and Alerts. The top navigation bar includes tabs for Jobs, Schedules, Events, and Logs. A search bar is present with the text 'search by name' and a green checkmark icon. Below the navigation, a 'Jobs - Filter' table is displayed with columns for ID, Status, and Name.

ID	Status	Name
20482	✓	SnapCenter Server Disaster Recovery
20481	✓	SnapCenter Server disaster recovery backup
20480	✗	SnapCenter Server disaster recovery backup
20475	✓	Backup of Resource Group 'SQLSRV-09' with policy 'SQL-Hourly'
20474	✓	Backup of Resource Group 'SQLSRV-05' with policy 'SQL-Hourly'
20473	⌚	Backup of Resource Group 'OracleSrv_06' with policy 'Oracle-Hourly'
20472	✗	SnapCenter Server disaster recovery backup

Job Details

SnapCenter Server Disaster Recovery

- ✓ ▼ SnapCenter Server Disaster Recovery
- ✓ ▼ Prepare for restore job
- ✓ ▼ Precheck validation
- ✓ ▼ Saving original server state
- ✓ ▼ Schedule restore
- ✓ ▼ Repository restore
- ✓ ▼ Config restore
- ✓ ▼ Reset MySQL password

6. To enable SQL Server restores from secondary storage, you must toggle the SnapCenter database into Disaster Recovery mode. This is performed as a separate operation and initiated on the Swagger API web page.
- Navigate to the Disaster Recovery section and click `/4.6/disasterrecovery/storage`.
 - Paste in the user authorization token.
 - In the `SmSetDisasterRecoverySettingsRequest` section, change `EnableDisasterRecover` to `true`.
 - Click Execute to enable disaster recovery mode for SQL Server.

Name	Description
Token * required string (header)	User authorization token <div>KlYxOg==rMXzS7EPIGRzTXjfton6Q+JoNGpueQt</div>
SmSetDisasterRecoverySettingsRequest * required object (body)	Parameters to enable or disable the DR mode <div> Edit Value Model <pre>{ "EnableDisasterRecovery": true }</pre> </div>



See comments regarding additional procedures.

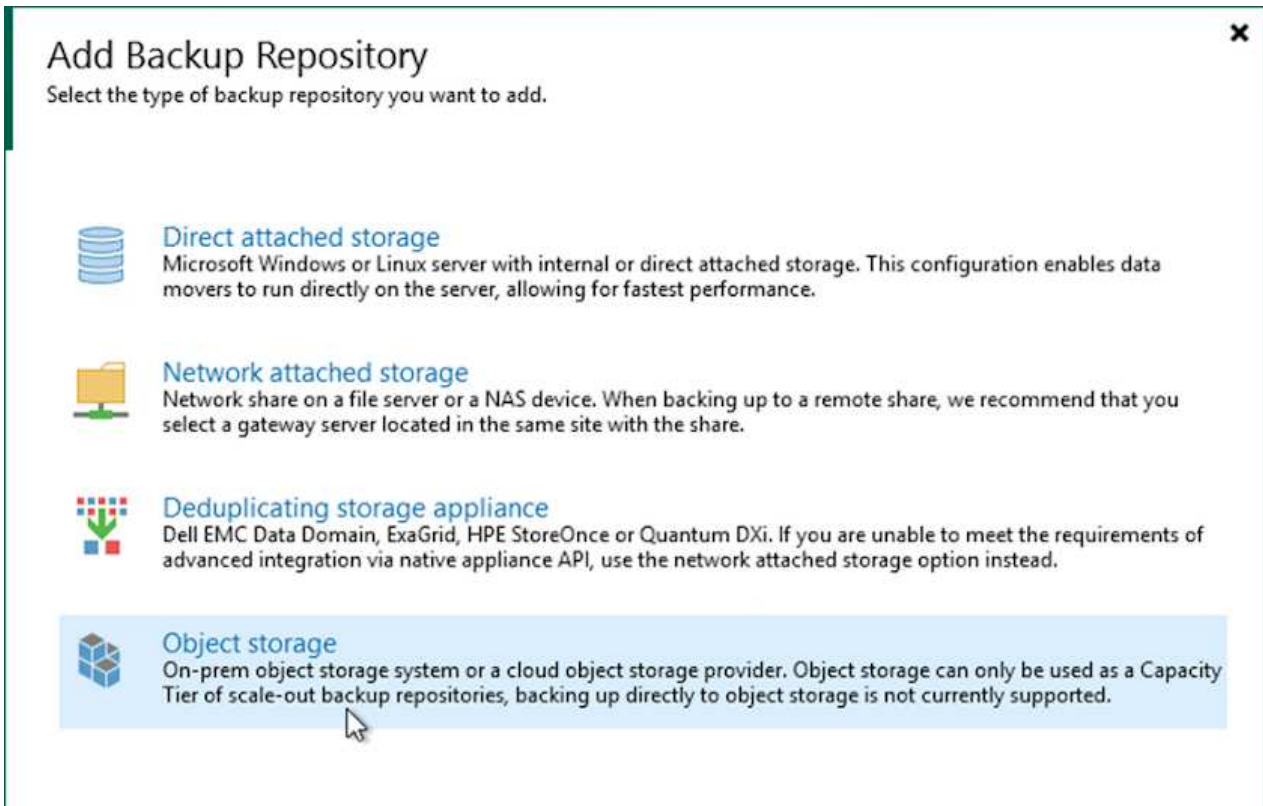
Restore application VMs with Veeam full restore

Create a backup repository and import backups from S3


From the secondary Veeam server, import the backups from S3 storage and restore the SQL Server and Oracle VMs to your VMware Cloud cluster.

To import the backups from the S3 object that was part of the on-premises scale-out backup repository, complete the following steps:

1. Go to Backup Repositories and click Add Repository in the top menu to launch the Add Backup Repository wizard. On the first page of the wizard, select Object Storage as the backup repository type.




2. Select Amazon S3 as the Object Storage type.




Object Storage


Select the type of object storage you want to use as a backup repository.




S3 Compatible
Adds an on-premises object storage system or a cloud object storage provider.




Amazon S3
Adds Amazon cloud object storage. Amazon S3, Amazon S3 Glacier (including Deep Archive) and Amazon Snowball Edge are supported.



Google Cloud Storage
Adds Google Cloud storage. Both Standard and Nearline storage classes are supported.




IBM Cloud Object Storage
Adds IBM Cloud object storage. S3 compatible versions of both on-premises and IBM Cloud storage offerings are supported.




Microsoft Azure Storage
Adds Microsoft Azure cloud object storage. Microsoft Azure Blob Storage, Microsoft Azure Archive Storage and Microsoft Azure Data Box are supported.

3. From the list of Amazon Cloud Storage Services, select Amazon S3.




Amazon Cloud Storage Services


Select the type of Amazon storage you want to use as a backup repository.



Amazon S3
Adds Amazon S3 storage. Both Standard and Infrequent Access (IA) storage classes are supported.




Amazon S3 Glacier
Adds Amazon S3 Glacier storage. Both Amazon S3 Glacier and Glacier Deep Archive are supported.








AWS Snowball Edge
Adds AWS Snowball Edge appliance to enable seeding of backups into Amazon S3 object storage.

4. Select your pre-entered credentials from the drop-down list or add a new credential for accessing the cloud storage resource. Click Next to continue.

New Object Storage Repository


 **Account**
Specify AWS account to use for connecting to Amazon S3 storage bucket.

Name	Credentials:
Account	 AKIA4H43ZT53YJXPY2Y (last edited: 33 days ago)  
Bucket	Manage cloud accounts
Summary	AWS region: Global 
	<input type="checkbox"/> Use the following gateway server: EC2AMAZ-3POTKQV (Backup server)  Select a gateway server to proxy access to Amazon S3. If no gateway server is specified, all scale-out backup repository extents must have direct Internet access.

< Previous **Next >** Finish Cancel

5. On the Bucket page, enter the data center, bucket, folder, and any desired options. Click Apply.

New Object Storage Repository ✕

 **Bucket**
Specify Amazon S3 bucket to use.

Name	Data center: US East (N. Virginia) ▼
Account	Bucket: ehcveeamrepo Browse...
Bucket	Folder: RTP Browse...
Summary	<p><input type="checkbox"/> Limit object storage consumption to: 10 ▼ TB ▼ This is a soft limit to help control your object storage spend. If the specified limit is exceeded, already running backup offload tasks will be allowed to complete, but no new tasks will be started.</p> <p><input type="checkbox"/> Make recent backups immutable for: 30 ▼ days Protects backups from modification or deletion by ransomware, hackers or malicious insiders using native object storage capabilities.</p> <p><input type="checkbox"/> Use infrequent access storage class (may result in higher costs) With lower price per GB but higher retrieval and early deletion fees, this storage class is best suited for long-term storage of GFS full backups. Avoid using it for short-term storage of recent backups.</p> <p><input type="checkbox"/> Store backups in a single availability zone (even lower price per GB, reduced resilience)</p>

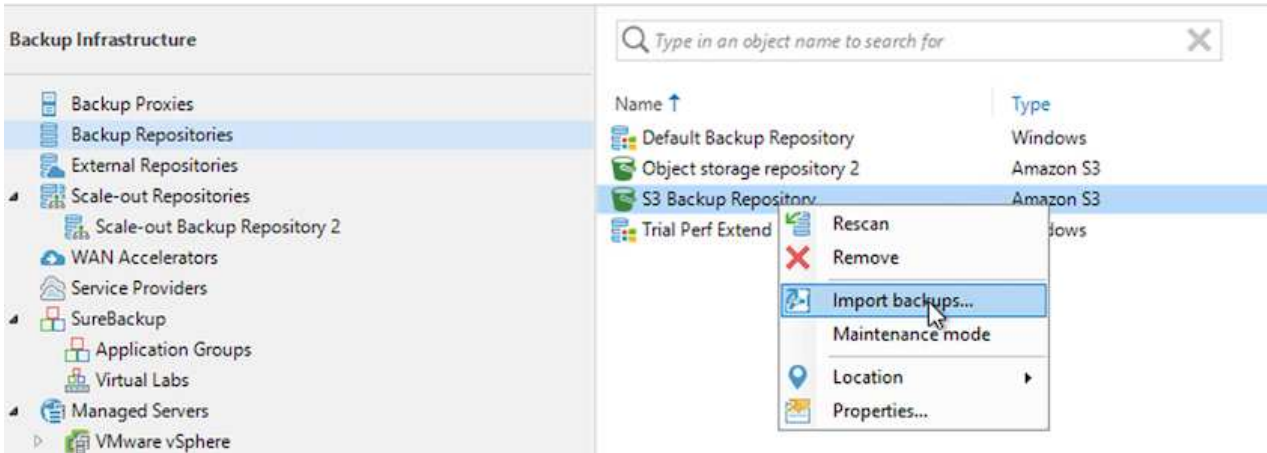
< Previous Apply Finish Cancel

6. Finally, select Finish to complete the process and add the repository.

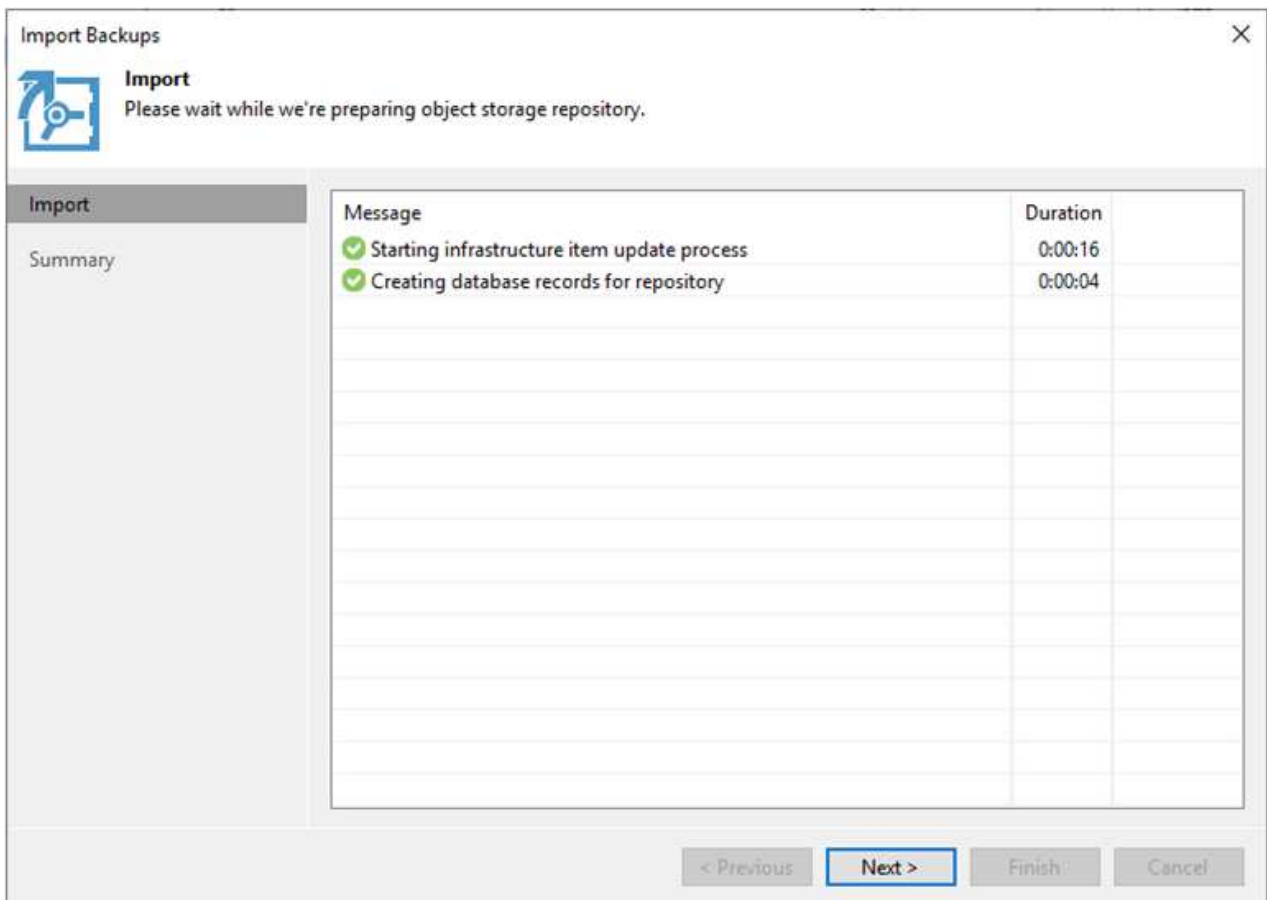
Import backups from S3 object storage

To import the backups from the S3 repository that was added in the previous section, complete the following steps.

1. From the S3 backup repository, select Import Backups to launch the Import Backups wizard.



2. After the database records for the import have been created, select Next and then Finish at the summary screen to start the import process.



3. After the import is complete, you can restore VMs into the VMware Cloud cluster.

System



Name: **Configuration Database Resynchr...** Status: **Success**
Action type: Configuration Resynchronize Start time: 4/6/2022 3:01:30 PM
Initiated by: EC2AMAZ-3POTKQV\vdadmin End time: 4/6/2022 3:04:57 PM

Log

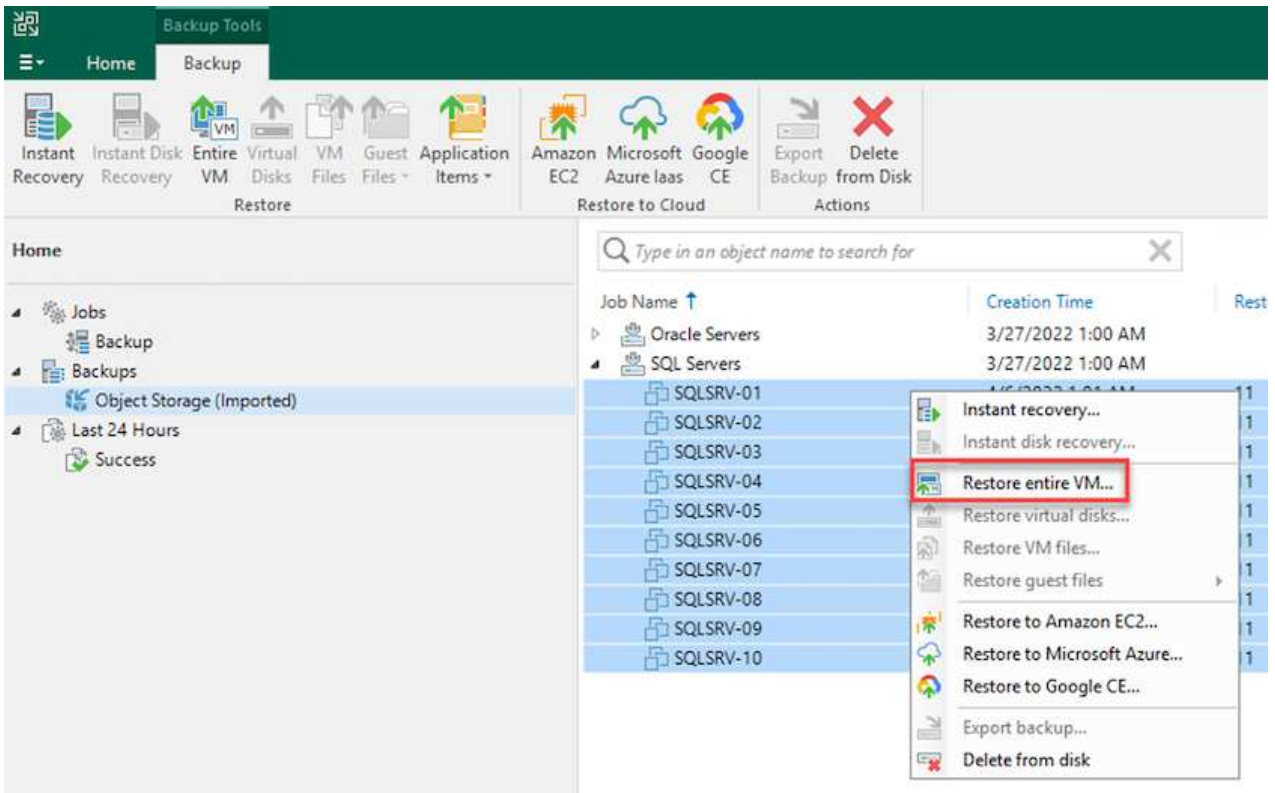
Message	Duration
✓ Starting backup repositories synchronization	
✓ Enumerating repositories	
✓ Found 1 repository	
✓ Processing capacity tier extent of S3 Backup Repository 2	0:03:23
✓ S3 Backup Repository: added 2 unencrypted	0:03:20
✓ Importing backup 2 out of 2	0:03:15
✓ Backup repositories synchronization completed successfully	

Close

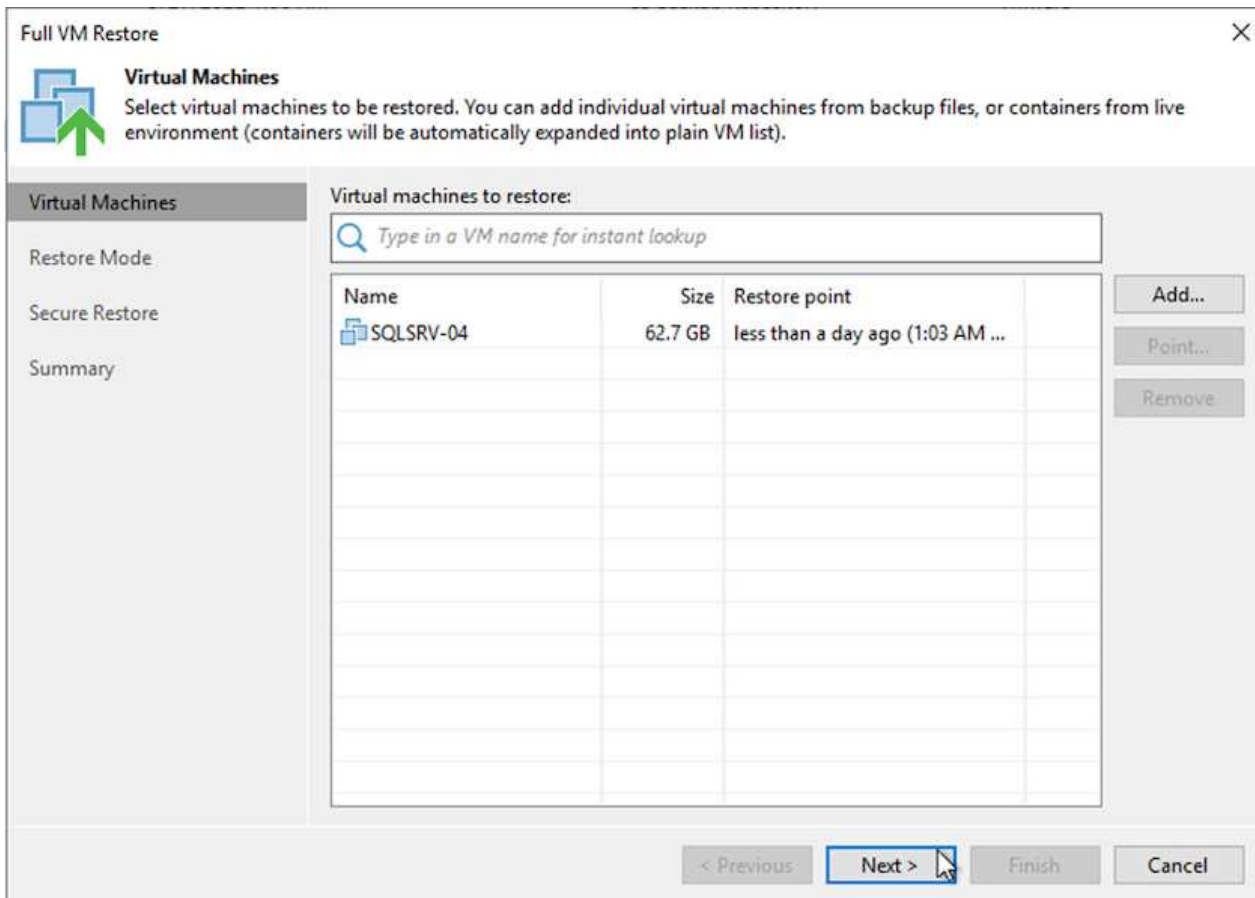
Restore application VMs with Veeam full restore to VMware Cloud

To restore SQL and Oracle virtual machines to the VMware Cloud on AWS workload domain/cluster, complete the following steps.

1. From the Veeam Home page, select the object storage containing the imported backups, select the VMs to restore, and then right click and select Restore Entire VM.




2. On the first page of the Full VM Restore wizard, modify the VMs to backup if desired and select Next.



3. On the Restore Mode page, select Restore to a New Location, or with Different Settings.

Full VM Restore



Restore Mode

Specify whether selected VMs should be restored back to the original location, or to a new location or with different settings.

Virtual Machines

Restore Mode

Host

Resource Pool

Datastore

Folder

Network

Secure Restore

Summary

☐ Restore to the original location

Quickly initiate the restore of selected VM to its original location, with the original name and settings. This option minimizes the chance of user input error.

☒ Restore to a new location, or with different settings

Customize the restored VM location, and change its settings. The wizard will automatically populate all controls with the original VM settings as the defaults.

☐ Staged restore

Run the selected VM directly from backup files in the isolated DataLab to make changes to the guest OS or applications prior to placing the VM into production environment.

[Pick proxy to use](#)

☐ Quick rollback (restore changed blocks only)

Allows for quick VM recovery in case of guest OS software problem, or user error. Do not use this option when recovering from disaster caused by hardware or storage issue, or power loss.

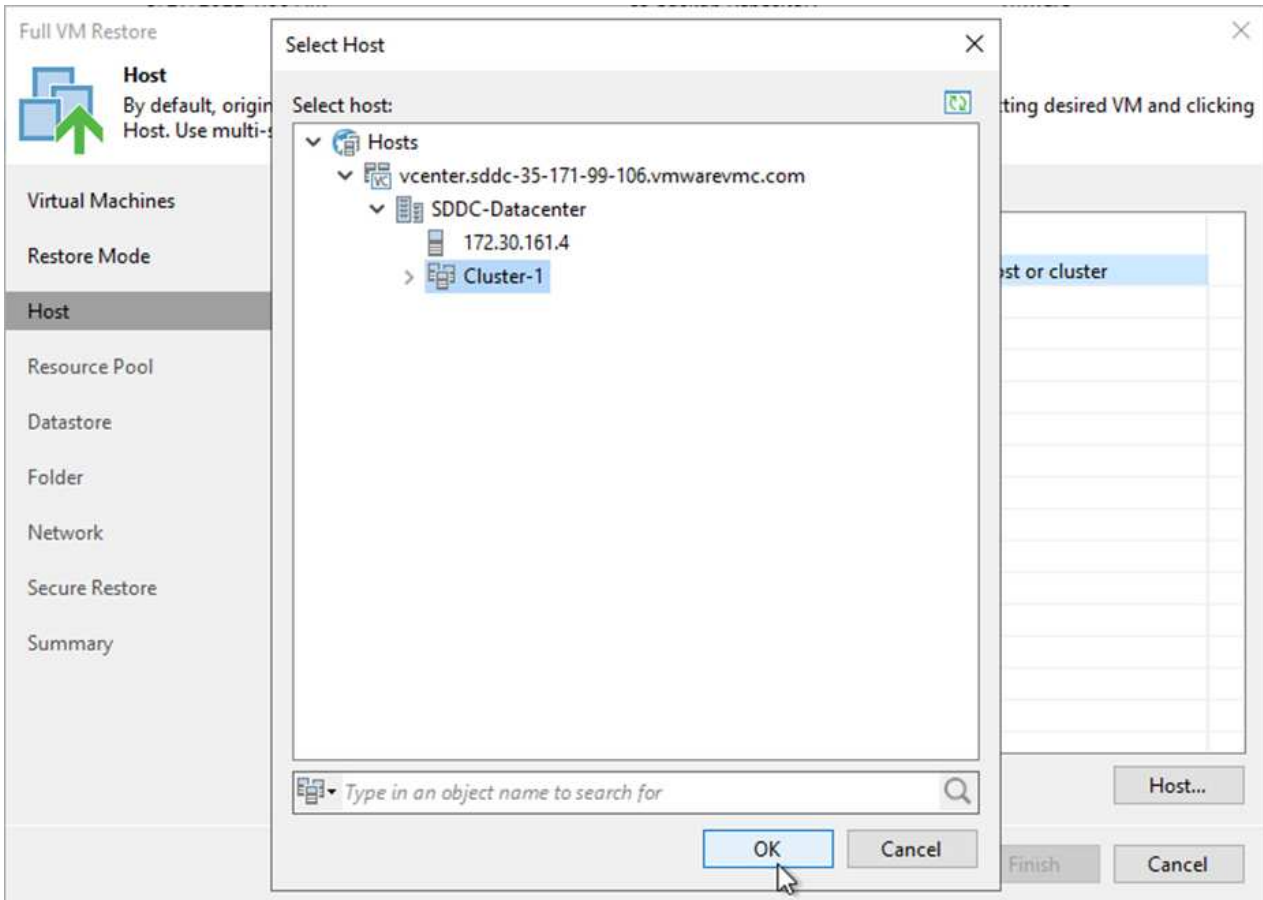
< Previous

Next >

Finish

Cancel

4. On the host page, select the Target ESXi host or cluster to restore the VM to.



5. On the Datastores page, select the target datastore location for both the configuration files and hard disk.

×

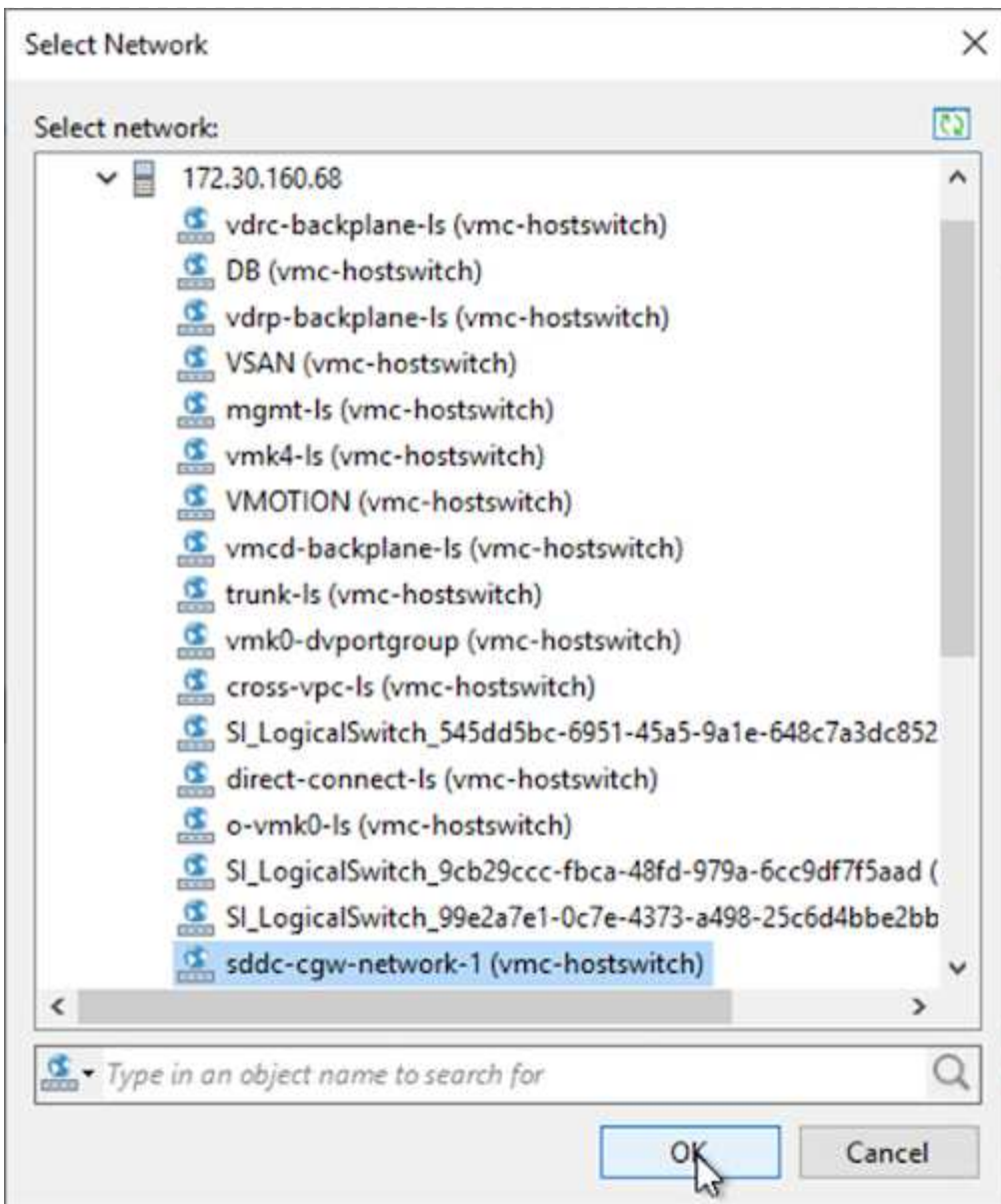


By default, we will connect the restored VM to the same virtual networks as the original VM. If you are restoring to a different location, specify how networks map between original and new locations.

Summary

Source	Target
SQLSRV-04	
Management 181 (DSwitch)	Not connected
Data - A - 3374 (DSwitch)	Not connected
Data - B - 3375 (DSwitch)	Not connected

Cancel



7. Select whether to scan the restored VM for malware, review the summary page, and click Finish to start the restore.

Restore SQL Server application data

The following process provides instructions on how to recover a SQL Server in VMware Cloud Services in AWS in the event of a disaster that renders the on-premises site inoperable.

The following prerequisites are assumed to be complete in order to continue with the recovery steps:

1. The Windows Server VM has been restored to the VMware Cloud SDDC using Veeam Full Restore.
2. A secondary SnapCenter server has been established and SnapCenter database restore and configuration has been completed using the steps outlined in the section "[SnapCenter backup and restore process summary](#)."

VM: Post restore configuration for SQL Server VM

After the restore of the VM is complete, you must configure networking and other items in preparation for rediscovering the host VM within SnapCenter.

1. Assign new IP addresses for Management and iSCSI or NFS.
2. Join the host to the Windows domain.
3. Add the hostnames to DNS or to the hosts file on the SnapCenter server.



If the SnapCenter plug-in was deployed using domain credentials different than the current domain, you must change the Log On account for the Plug-in for Windows Service on the SQL Server VM. After changing the Log On account, restart the SnapCenter SMCORE, Plug-in for Windows, and Plug-in for SQL Server services.



To automatically rediscover the restored VMs in SnapCenter, the FQDN must be identical to the VM that was originally added to the SnapCenter on premises.

Configure FSx storage for SQL Server restore

To accomplish the disaster recovery restore process for a SQL Server VM, you must break the existing SnapMirror relationship from the FSx cluster and grant access to the volume. To do so, complete the following steps.

1. To break the existing SnapMirror relationship for the SQL Server database and log volumes, run the following command from the FSx CLI:

```
FSx-Dest::> snapmirror break -destination-path DestSVM:DestVolName
```

2. Grant access to the LUN by creating an initiator group containing the iSCSI IQN of the SQL Server Windows VM:

```
FSx-Dest::> igroup create -vserver DestSVM -igroup igroupName  
-protocol iSCSI -ostype windows -initiator IQN
```

3. Finally, map the LUNs to the initiator group that you just created:

```
FSx-Dest::> lun mapping create -vserver DestSVM -path LUNPath igroup  
igroupName
```

4. To find the path name, run the `lun show` command.

Set up the Windows VM for iSCSI access and discover the file systems

1. From the SQL Server VM, set up your iSCSI network adapter to communicate on the VMware Port Group that has been established with connectivity to the iSCSI target interfaces on your FSx instance.
2. Open the iSCSI Initiator Properties utility and clear out the old connectivity settings on the Discovery, Favorite Targets, and Targets tabs.
3. Locate the IP address(es) for accessing the iSCSI logical interface on the FSx instance/cluster. This can be found in the AWS console under Amazon FSx > ONTAP > Storage Virtual Machines.

Endpoints

Management DNS name

svm-045c077375d3d9799.fs-0ae40e08acc0dea67.fsx.us-east-1.amazonaws.com

NFS DNS name

svm-045c077375d3d9799.fs-0ae40e08acc0dea67.fsx.us-east-1.amazonaws.com

iSCSI DNS name

iscsi.svm-045c077375d3d9799.fs-0ae40e08acc0dea67.fsx.us-east-1.amazonaws.com

Management IP address

198.19.254.53

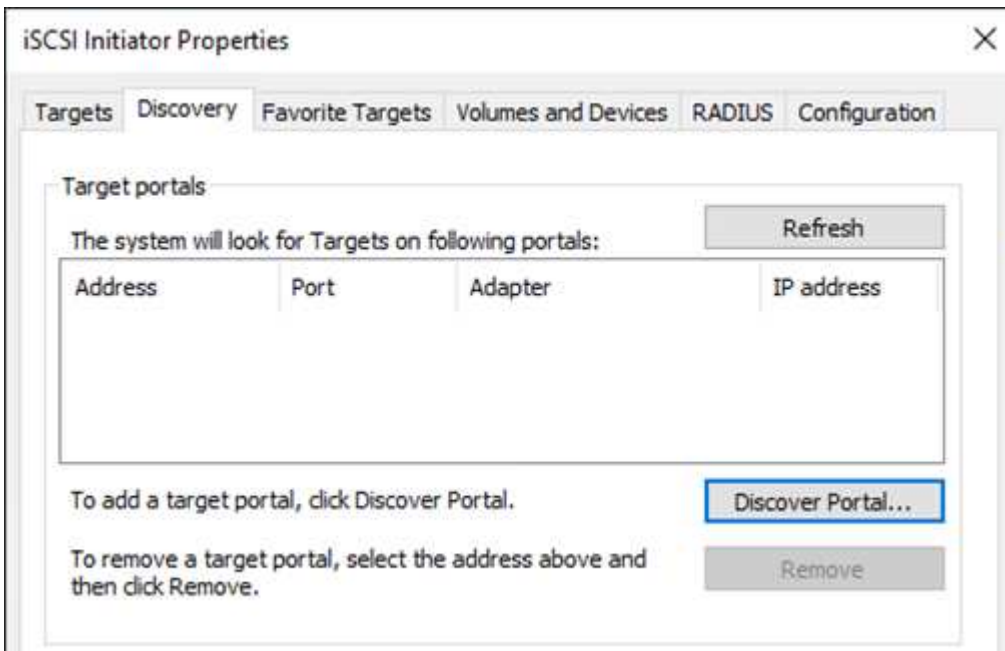
NFS IP address

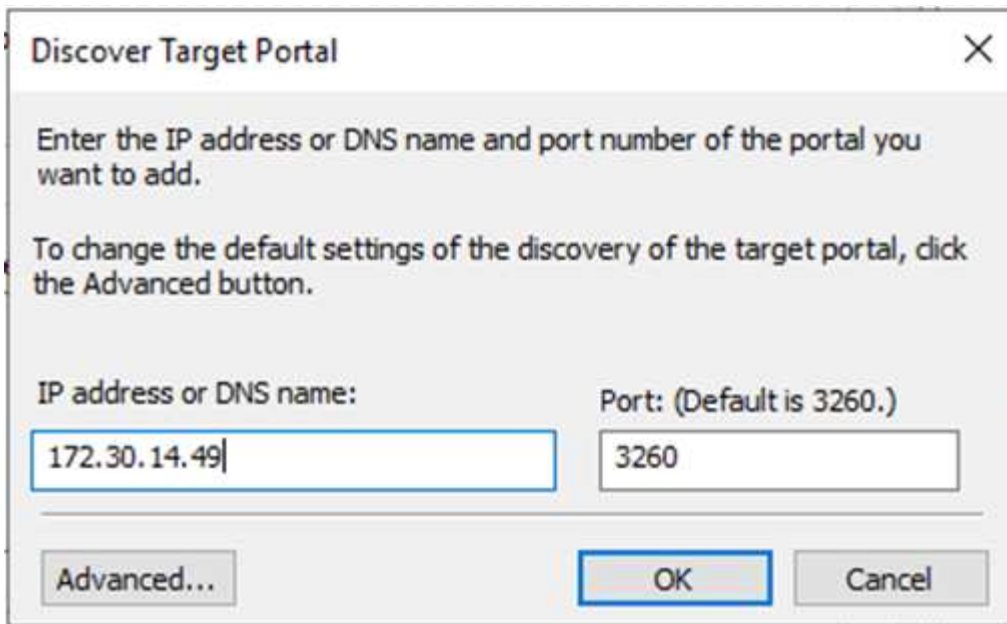
198.19.254.53

iSCSI IP addresses

172.30.15.101, 172.30.14.49

4. From the Discovery tab, click Discover Portal and enter the IP addresses for your FSx iSCSI targets.





The image shows a 'Discover Target Portal' dialog box. It has a title bar with a close button (X). The main area contains two paragraphs of text: 'Enter the IP address or DNS name and port number of the portal you want to add.' and 'To change the default settings of the discovery of the target portal, click the Advanced button.' Below the text are two input fields. The first is labeled 'IP address or DNS name:' and contains the text '172.30.14.49'. The second is labeled 'Port: (Default is 3260.)' and contains the text '3260'. At the bottom of the dialog are three buttons: 'Advanced...', 'OK', and 'Cancel'. The 'OK' button is highlighted with a blue border.

Discover Target Portal

Enter the IP address or DNS name and port number of the portal you want to add.

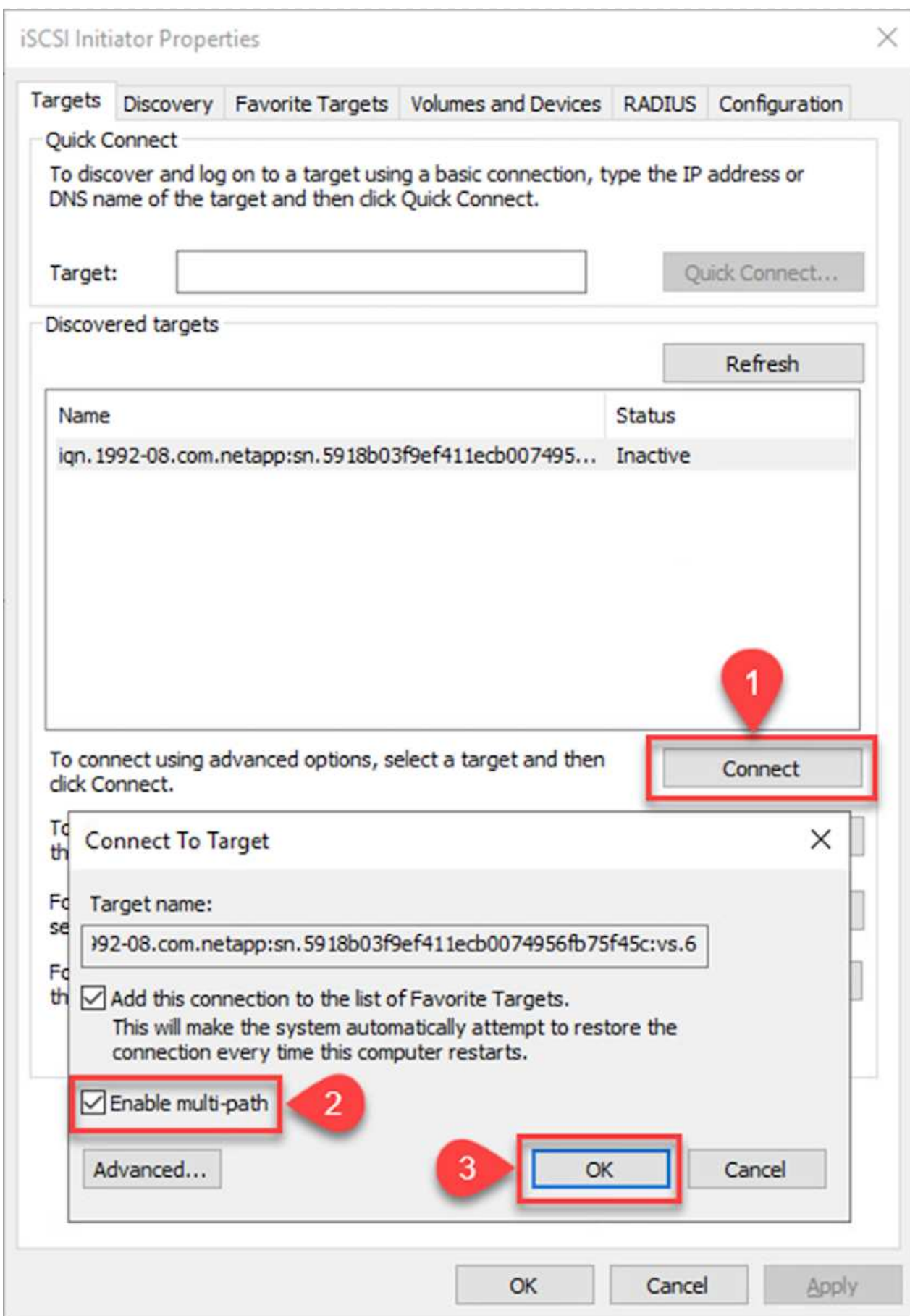
To change the default settings of the discovery of the target portal, click the Advanced button.

IP address or DNS name: 172.30.14.49

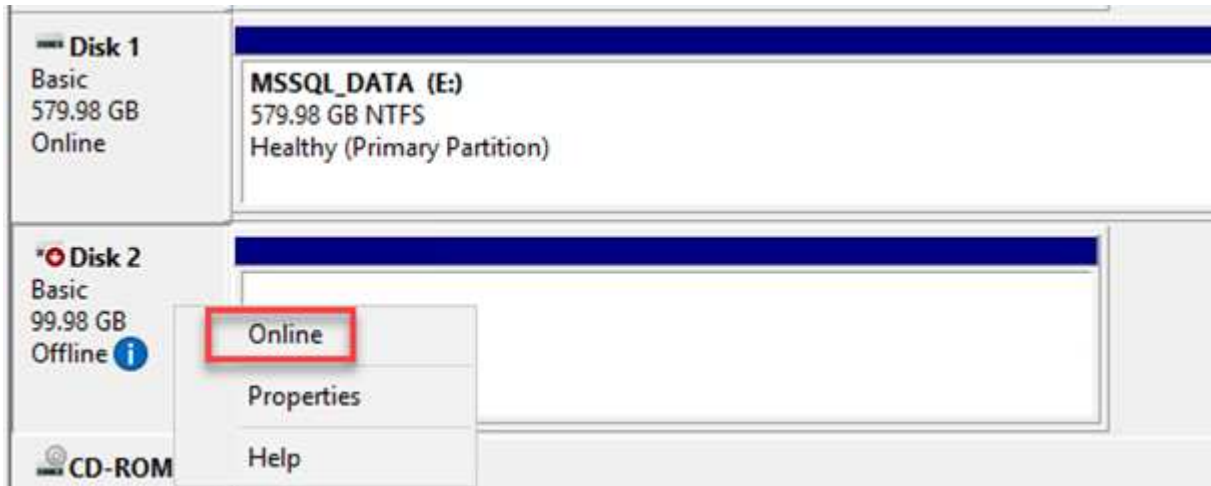
Port: (Default is 3260.) 3260

Advanced... OK Cancel

5. On the Target tab, click Connect, select Enable Multi-Path if appropriate for your configuration and then click OK to connect to the target.

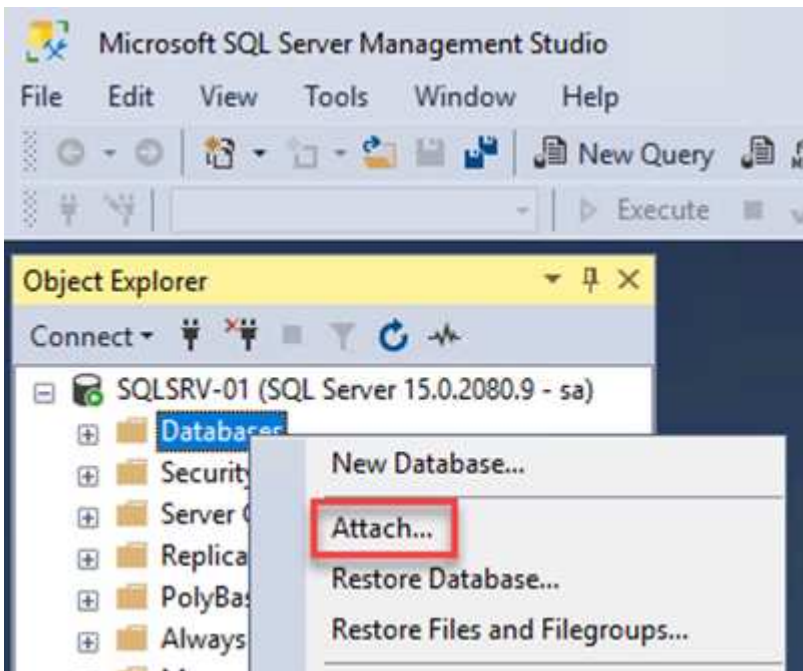


6. Open the Computer Management utility and bring the disks online. Verify that they retain the same drive letters that they previously held.

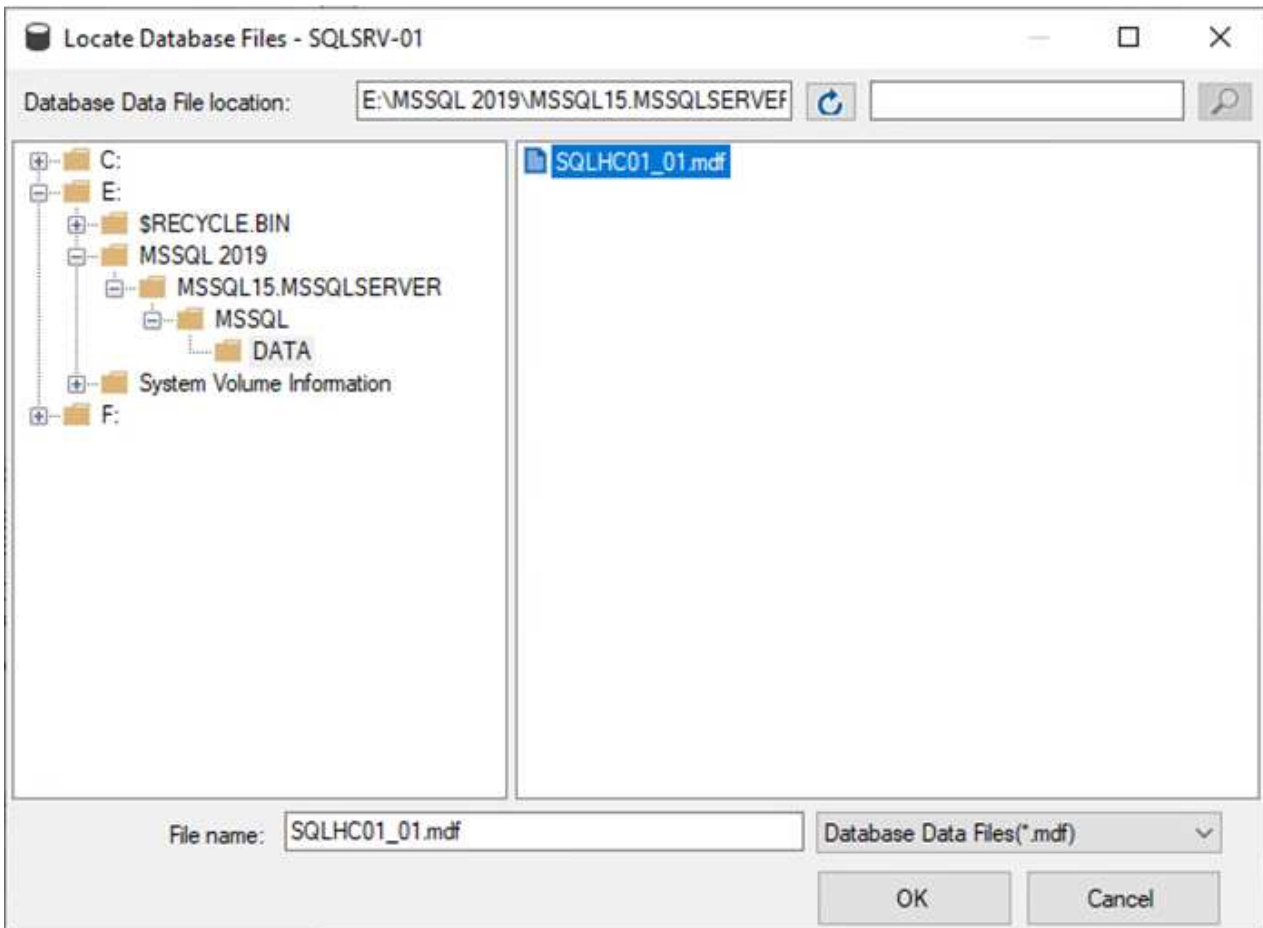


Attach the SQL Server databases

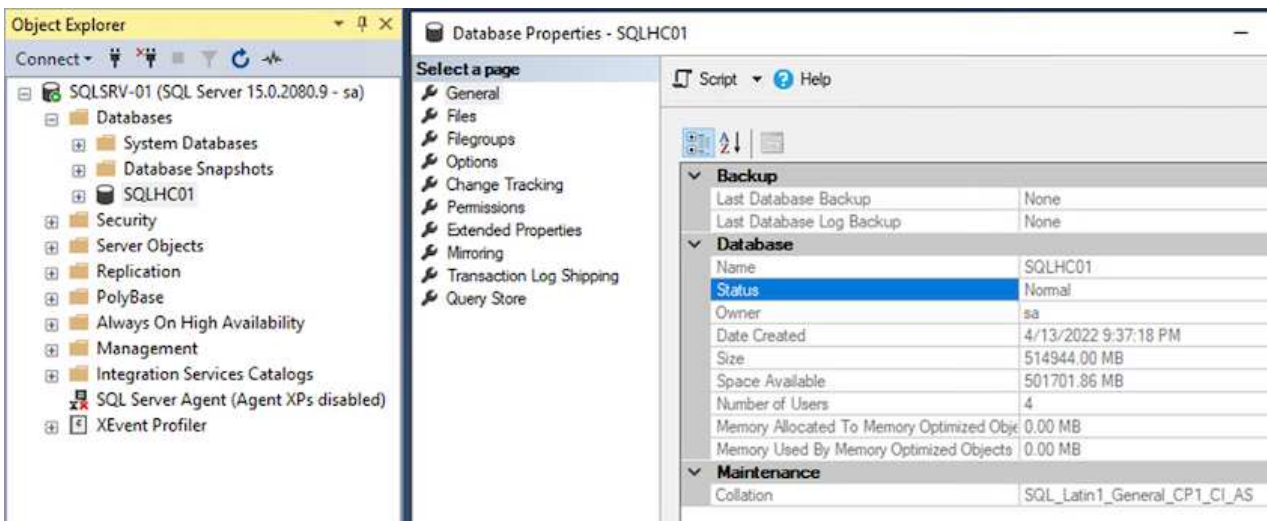
1. From the SQL Server VM, open Microsoft SQL Server Management Studio and select Attach to start the process of connecting to the database.



2. Click Add and navigate to the folder containing the SQL Server primary database file, select it, and click OK.



3. If the transaction logs are on a separate drive, choose the folder that contains the transaction log.
4. When finished, click OK to attach the database.

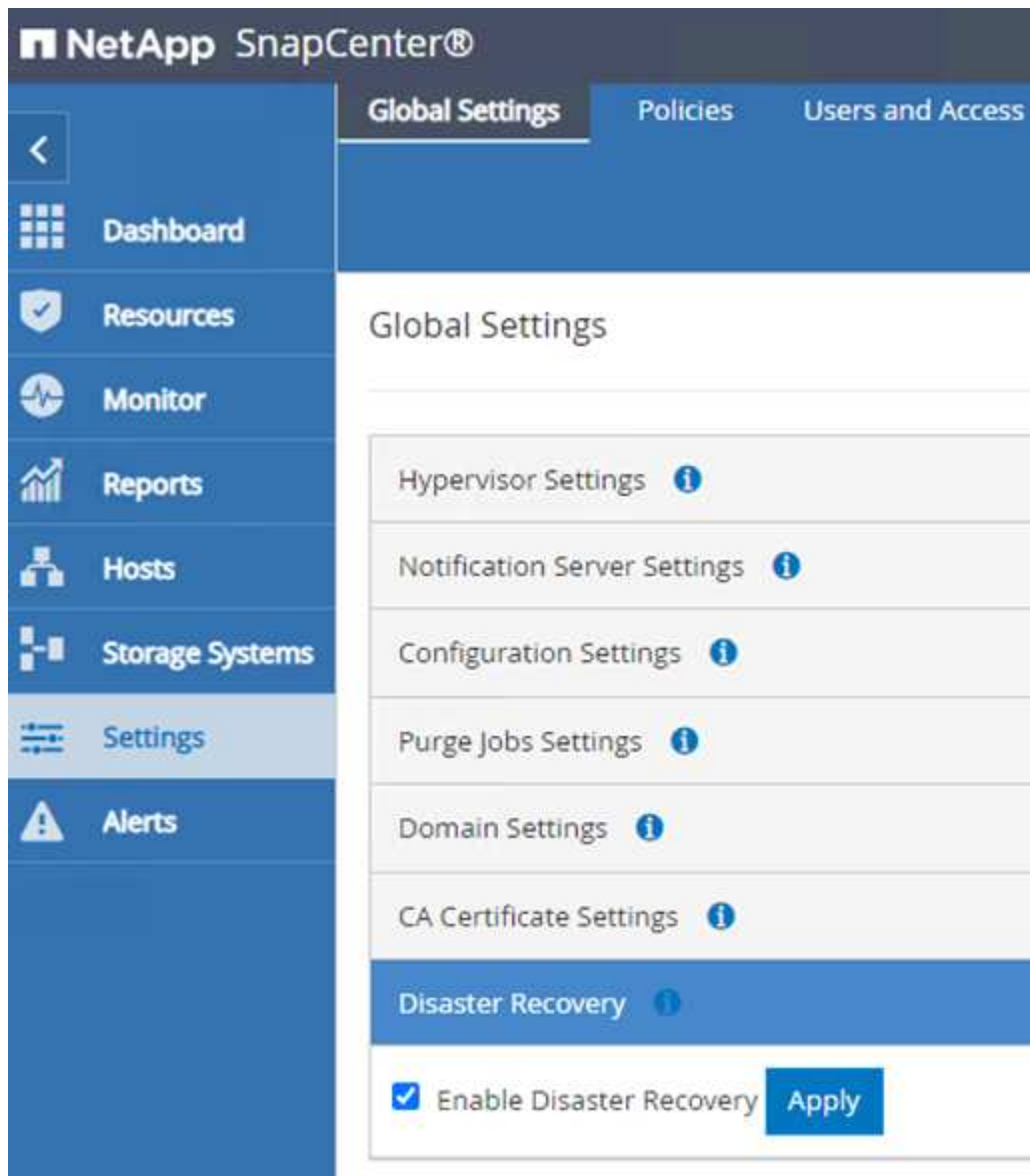


Confirm SnapCenter communication with SQL Server Plug-in

With the SnapCenter database restored to its previous state, it automatically rediscovers the SQL Server hosts. For this to work correctly, keep in mind the following prerequisites:

- SnapCenter must be placed in Disaster Recover mode. This can be accomplished through the Swagger API or in Global Settings under Disaster Recovery.
- The FQDN of the SQL Server must be identical to the instance that was running in the on-premises datacenter.
- The original SnapMirror relationship must be broken.
- The LUNs containing the database must be mounted to the SQL Server instance and the database attached.

To confirm that SnapCenter is in Disaster Recovery mode, navigate to Settings from within the SnapCenter web client. Go to the Global Settings tab and then click Disaster Recovery. Make sure that the Enable Disaster Recovery checkbox is enabled.



Restore Oracle application data

The following process provides instructions on how to recover Oracle application data in VMware Cloud Services in AWS in the event of a disaster that renders the on-premises site inoperable.

Complete the following prerequisites to continue with the recovery steps:

1. The Oracle Linux server VM has been restored to the VMware Cloud SDDC using Veeam Full Restore.
2. A secondary SnapCenter server has been established and the SnapCenter database and configuration files have been restored using the steps outlined in this section ["SnapCenter backup and restore process summary."](#)

Configure FSx for Oracle restore – Break the SnapMirror relationship

To make the secondary storage volumes hosted on the FSxN instance accessible to the Oracle servers, you must first break the existing SnapMirror relationship.

1. After logging into the FSx CLI, run the following command to view the volumes filtered by the correct name.

```
FSx-Dest::> volume show -volume VolumeName*
```

```
FSxId0ae40e08acc0dea67::> volume show -volume oraclesrv_03*
Vserver    Volume                Aggregate    State    Type    Size    Available    Used%
-----
ora_svm_dest
             oraclesrv_03_u01_dest
                   aggr1         online    DP        100GB    93.12GB     6%
ora_svm_dest
             oraclesrv_03_u02_dest
                   aggr1         online    DP        200GB    34.98GB    82%
ora_svm_dest
             oraclesrv_03_u03_dest
                   aggr1         online    DP        150GB    33.37GB    77%
3 entries were displayed.

FSxId0ae40e08acc0dea67::> █
```

2. Run the following command to break the existing SnapMirror relationships.

```
FSx-Dest::> snapmirror break -destination-path DestSVM:DestVolName
```

```
FSxId0ae40e08acc0dea67::> snapmirror break -destination-path ora_svm_dest:oraclesrv_03_u02_dest
Operation succeeded: snapmirror break for destination "ora_svm_dest:oraclesrv_03_u02_dest".

FSxId0ae40e08acc0dea67::> snapmirror break -destination-path ora_svm_dest:oraclesrv_03_u03_dest
Operation succeeded: snapmirror break for destination "ora_svm_dest:oraclesrv_03_u03_dest".
```

3. Update the junction-path in the Amazon FSx web client:

oraclesrv_03_u01_dest (fsvol-01167370e9b7aefa0)

Attach

Actions ▲

Update volume

Create backup


Delete volume

Summary

Volume ID

fsvol-01167370e9b7aefa0 

Volume name

oraclesrv_03_u01_dest 


UUID

3d7338ce-9f19-11ec-
b007-4956fb75f45c

File system ID

fs-0ae40e08acc0dea67 

Resource ARN

arn:aws:fsx:us-
east-1:541696183547:volume/fs-
0ae40e08acc0dea67/fsvol-
01167370e9b7aefa0 

Creation time

2022-03-08T14:52:09-05:00

Lifecycle state

 Created

Volume type

ONTAP

Size

100.00 GB 

SVM ID

svm-02b2ad25c6b2e5bc2

Junction path

- 

Tiering policy name

SNAPSHOT_ONLY

Tiering policy cooling period (days)

2

Storage efficiency enabled

Disabled

4. Add the junction path name and click Update. Specify this junction path when mounting the NFS volume from the Oracle server.

Update volume



Junction path

/oraclesrv_03_u01_dest

The location within your file system where your volume will be mounted.

Volume size

102400



Minimum 20 MiB; Maximum 104857600 MiB

Storage efficiency

Select whether you would like to enable ONTAP storage efficiencies on your volume: deduplication, compression, and compaction.

- ☐ Enabled (recommended)
- ☒ Disabled

Capacity pool tiering policy

You can optionally enable automatic tiering of your data to lower-cost capacity pool storage.

Snapshot Only



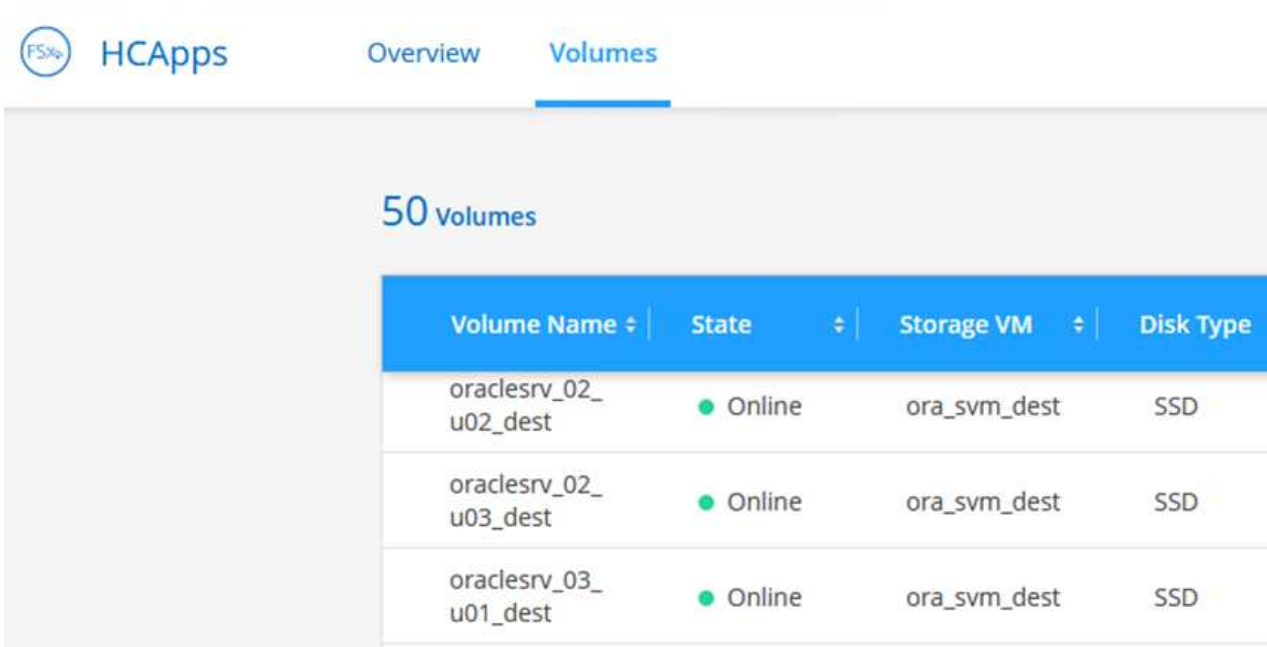
Cancel

Update

Mount NFS volumes on Oracle Server

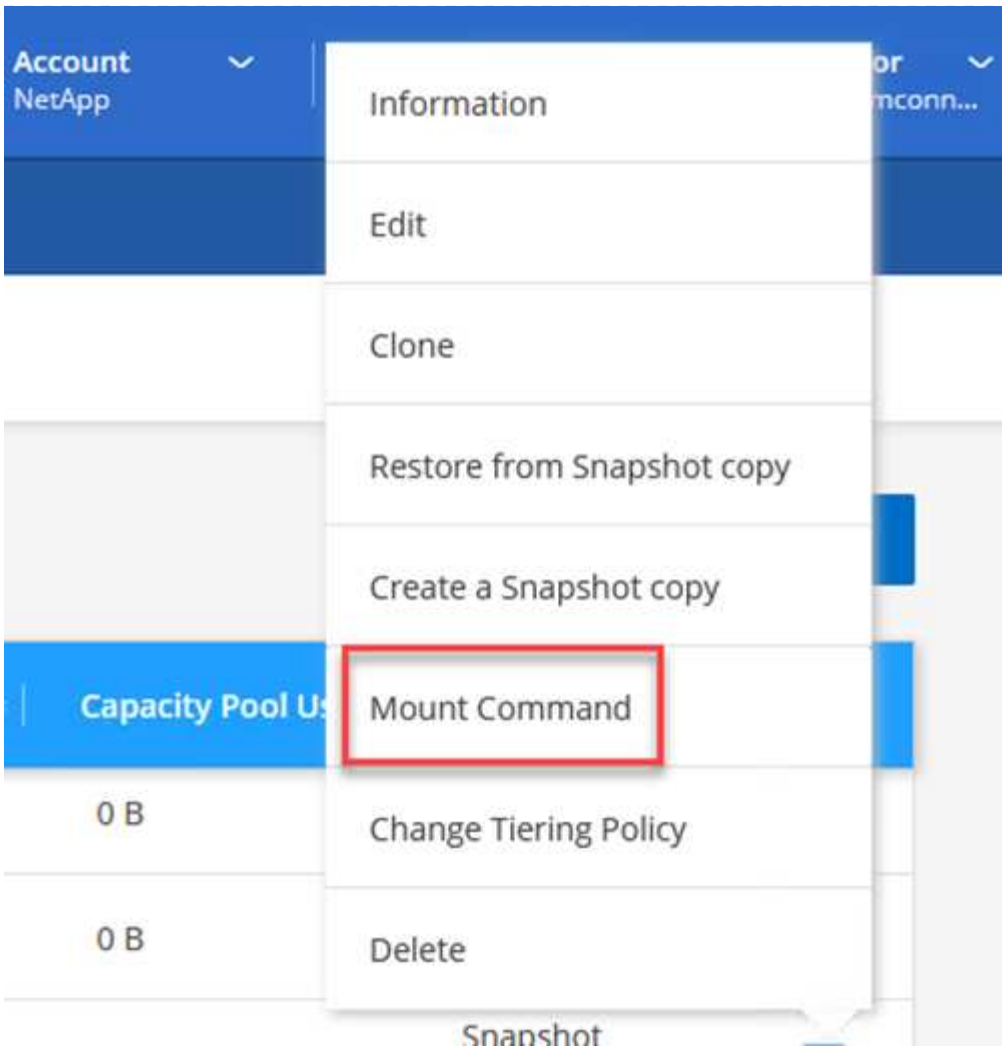
In Cloud Manager, you can obtain the mount command with the correct NFS LIF IP address for mounting the NFS volumes that contain the Oracle database files and logs.

1. In Cloud Manager, access the list of volumes for your FSx cluster.



Volume Name ↕	State ↕	Storage VM ↕	Disk Type
oraclesrv_02_u02_dest	● Online	ora_svm_dest	SSD
oraclesrv_02_u03_dest	● Online	ora_svm_dest	SSD
oraclesrv_03_u01_dest	● Online	ora_svm_dest	SSD

2. From the action menu, select Mount Command to view and copy the mount command to be used on our Oracle Linux server.



Mount Volume NFS

oraclesrv_03_u01_dest

Go to your linux machine and enter this mount command

Mount Command

```
mount 198.19.254.180:/oraclesrv_03_u01_dest <dest_d...
```

Copy

3. Mount the NFS file system to the Oracle Linux Server. The directories for mounting the NFS share already exist on the Oracle Linux host.
4. From the Oracle Linux server, use the mount command to mount the NFS volumes.

```
FSx-Dest::> mount -t oracle_server_ip:/junction-path
```

Repeat this step for each volume associated with the Oracle databases.



To make the NFS mount persistent upon rebooting, edit the `/etc/fstab` file to include the mount commands.

5. Reboot the Oracle server. The Oracle databases should start up normally and be available for use.

Failback

Upon successful completion of the failover process outlined in this solution, SnapCenter and Veeam resume their backup functions running in AWS, and FSx for ONTAP is now designated as primary storage with no existing SnapMirror relationships with the original on-premises datacenter. After normal function has resumed on premises, you can use a process identical to the one outlined in this documentation to mirror data back to the on-premises ONTAP storage system.

As is also outlined in this documentation, you can configure SnapCenter to mirror the application data volumes from FSx for ONTAP to an ONTAP storage system residing on premises. Similarly, you can configure Veeam to replicate backup copies to Amazon S3 using a scale-out backup repository so that those backups are accessible to a Veeam backup server residing at the on-premises datacenter.

Failback is outside the scope of this documentation, but failback differs little from the detailed process outlined here.

Conclusion

The use case presented in this documentation focuses on proven disaster recovery technologies that highlight the integration between NetApp and VMware. NetApp ONTAP storage systems provide proven data-mirroring technologies that allow organizations to design disaster recovery solutions that span on-premises and ONTAP technologies residing with the leading cloud providers.

FSx for ONTAP on AWS is one such solution that allows for seamless integration with SnapCenter and SyncMirror for replicating application data to the cloud. Veeam Backup & Replication is another well-known technology that integrates well with NetApp ONTAP storage systems and can provide failover to vSphere-native storage.

This solution presented a disaster recovery solution using guest connect storage from an ONTAP system hosting SQL Server and Oracle application data. SnapCenter with SnapMirror provides an easy-to-manage solution for protecting application volumes on ONTAP systems and replicating them to FSx or CVO residing in the cloud. SnapCenter is a DR-enabled solution for failing over all application data to VMware Cloud on AWS.

Where to find additional information

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

- [Links to solution documentation](#)

[NetApp Hybrid Multicloud with VMware Solutions](#)

Veeam Backup & Restore in VMware Cloud, with Amazon FSx for ONTAP

Author: Josh Powell - NetApp Solutions Engineering

Overview

Veeam Backup & Replication is an effective and reliable solution for protecting data in VMware Cloud. This solution demonstrates the proper setup and configuration for using Veeam Backup and Replication to backup and restore application VMs residing on FSx for ONTAP NFS datastores in VMware Cloud.

VMware Cloud (in AWS) supports the use of NFS datastores as supplemental storage, and FSx for NetApp ONTAP is a secure solution for customers who need to store large amounts of data for their cloud applications that can scale independent of the number of ESXi hosts in the SDDC cluster. This integrated AWS storage service offers highly efficient storage with all of the traditional NetApp ONTAP capabilities.

Use Cases

This solution addresses the following use cases:

- Backup and restore of Windows and Linux virtual machines hosted in VMC using FSx for NetApp ONTAP as a backup repository.
- Backup and restore of Microsoft SQL Server application data using FSx for NetApp ONTAP as a backup repository.
- Backup and restore of Oracle application data using FSx for Netapp ONTAP as a backup repository.

NFS Datastores Using Amazon FSx for ONTAP

All virtual machines in this solution reside on FSx for ONTAP supplemental NFS datastores. Using FSx for ONTAP as a supplemental NFS datastore has several benefits. For example, it allows you to:

- Create a scalable and highly available file system in the cloud without the need for complex setup and management.
- Integrate with your existing VMware environment, allowing you to use familiar tools and processes to manage your cloud resources.
- Benefit from the advanced data management features provided by ONTAP, such as snapshots and replication, to protect your data and ensure its availability.

Solution Deployment Overview

This list provides the high level steps necessary to configure Veeam Backup & Replication, execute backup and restore jobs using FSx for ONTAP as a backup repository, and perform restores of SQL Server and Oracle VMs and databases:

1. Create the FSx for ONTAP file system to be used as iSCSI backup repository for Veeam Backup & Replication.
2. Deploy Veeam Proxy to distribute backup workloads and mount iSCSI backup repositories hosted on FSx for ONTAP.
3. Configure Veeam Backup Jobs to backup SQL Server, Oracle, Linux and Windows virtual machines.
4. Restore SQL Server virtual machines and individual databases.
5. Restore Oracle virtual machines and individual databases.

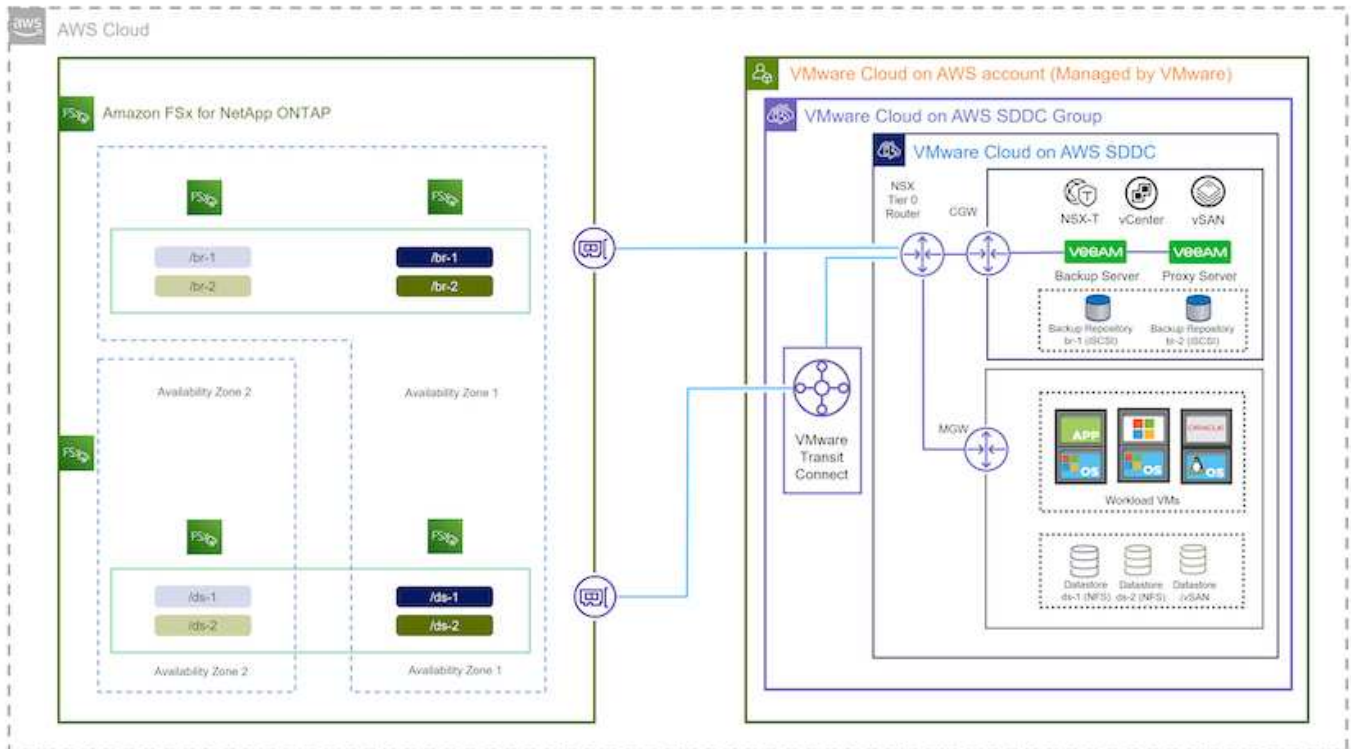
Prerequisites

The purpose of this solution is to demonstrate data protection of virtual machines running in VMware Cloud and located on NFS Datastores hosted by FSx for NetApp ONTAP. This solution assumes the following components are configured and ready for use:

1. FSx for ONTAP filesystem with one or more NFS datastores connected to VMware Cloud.
2. Microsoft Windows Server VM with Veeam Backup & Replication software installed.
 - vCenter server has been discovered by the Veeam Backup & Replication server using their IP address or fully qualified domain name.
3. Microsoft Windows Server VM to be installed with Veeam Backup Proxy components during the solution deployment.
4. Microsoft SQL Server VMs with VMDKs and application data residing on FSx for ONTAP NFS datastores. For this solution we had two SQL databases on two separate VMDKs.
 - Note: As a best practice database and transaction log files are placed on separate drives as this will improve performance and reliability. This is in part due to the fact that transaction logs are written sequentially, whereas database files are written randomly.
5. Oracle Database VMs with VMDKs and application data residing on FSx for ONTAP NFS datastores.
6. Linux and Windows file server VMs with VMDKs residing on FSx for ONTAP NFS datastores.
7. Veeam requires specific TCP ports for communication between servers and components in the backup environment. On Veeam backup infrastructure components, the required firewall rules are automatically created.
For a full listing of the network port requirements refer to the Ports section of the [Veeam Backup and Replication User Guide for VMware vSphere](#).

High Level Architecture

The testing / validation of this solution was performed in a lab that may or may not match the final deployment environment. For more information, please refer to the following sections.



Hardware / Software Components

The purpose of this solution is to demonstrate data protection of virtual machines running in VMware Cloud and located on NFS Datastores hosted by FSx for NetApp ONTAP. This solution assumes the following components are already configured and ready for use:

- Microsoft Windows VM's located on an FSx for ONTAP NFS Datastore
- Linux (CentOS) VM's located on an FSx for ONTAP NFS Datastore
- Microsoft SQL Server VM's located on an FSx for ONTAP NFS Datastore
 - Two databases hosted on separate VMDK's
- Oracle VM's located on an FSx for ONTAP NFS Datastore

Solution Deployment

In this solution we provide detailed instructions for deploying and validating a solution utilizing Veeam Backup and Replication software to perform backup and recovery of SQL Server, Oracle, and Windows and Linux file server virtual machines in a VMware Cloud SDDC on AWS. The Virtual Machines in this solution reside on a supplemental NFS datastore hosted by FSx for ONTAP. In addition, a separate FSx for ONTAP file system is used to host iSCSI volumes that will be used for Veeam backup repositories.

We will go over FSx for ONTAP file system creation, mounting iSCSI volumes to be used as backup repositories, creating and running backup jobs, and performing VM and database restores.

For detailed information on FSx for NetApp ONTAP refer to the [FSx for ONTAP User Guide](#).

For detailed information on Veeam Backup and Replication refer to the [Veeam Help Center Technical Documentation](#) site.

For considerations and limitations when using Veeam Backup and Replication with VMware Cloud on AWS, refer to [VMware Cloud on AWS and VMware Cloud on Dell EMC Support. Considerations and Limitations](#).

Deploy Veeam Proxy server

A Veeam proxy server is a component of the Veeam Backup & Replication software that acts as an intermediary between the source and the backup or replication target. The proxy server helps to optimize and accelerate data transfer during backup jobs by processing data locally and can use different Transport Modes to access data using VMware vStorage APIs for Data Protection or through direct storage access.

When choosing a Veeam proxy server design it is important to consider the number of concurrent tasks and the transport mode or type of storage access desired.

For sizing the number of proxy servers, and for their system requirements, refer to the [Veeam VMware vSphere Best Practice Guide](#).

The Veeam Data Mover is a component of the Veeam Proxy Server and utilizes a Transport Mode as a method for obtaining VM data from the source and transferring it to the target. The transport mode is specified during the configuration of the backup job. It is possible to increase the efficiency backups from NFS datastores by using direct storage access.

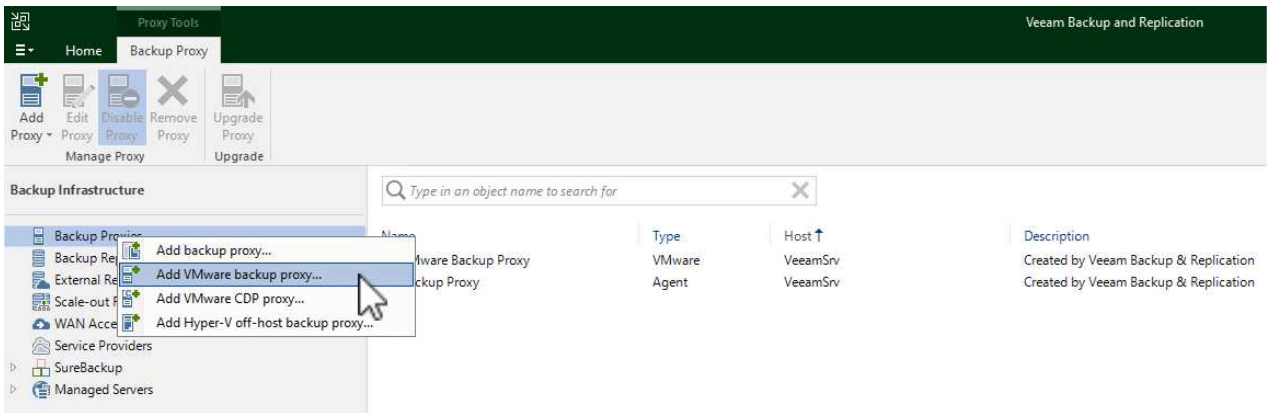
For more information on Transport Modes refer to the [Veeam Backup and Replication User Guide for VMware vSphere](#).

In the following step we cover deployment of the Veeam Proxy Server on a Windows VM in the VMware Cloud SDDC.

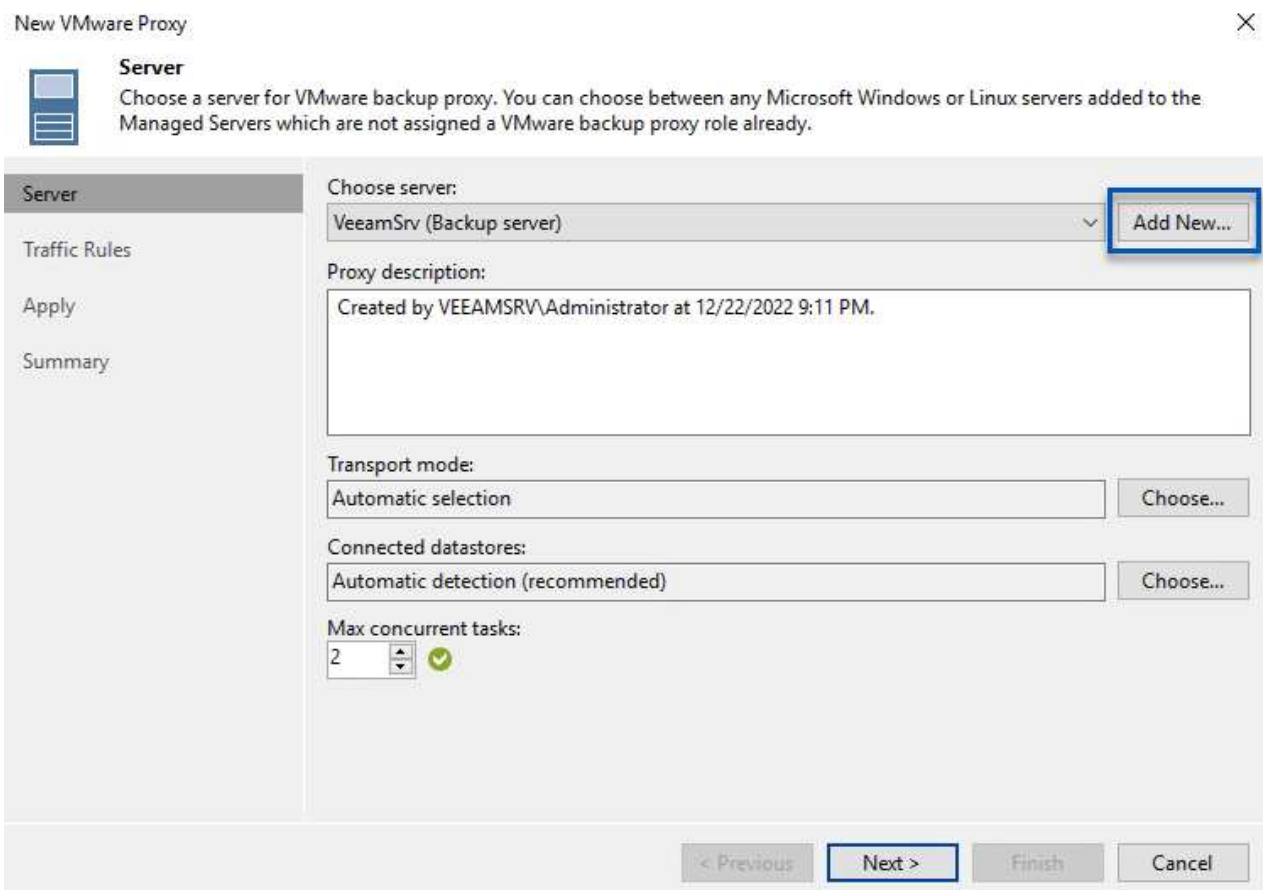
Deploy Veeam Proxy to distribute backup workloads

In this step the Veeam Proxy is deployed to an existing Windows VM. This allows backup jobs to be distributed between the primary Veeam Backup Server and the Veeam Proxy.

1. On the Veeam Backup and Replication server, open the administration console and select **Backup Infrastructure** in the lower left menu.
2. Right click on **Backup Proxies** and click on **Add VMware backup proxy...** to open the wizard.

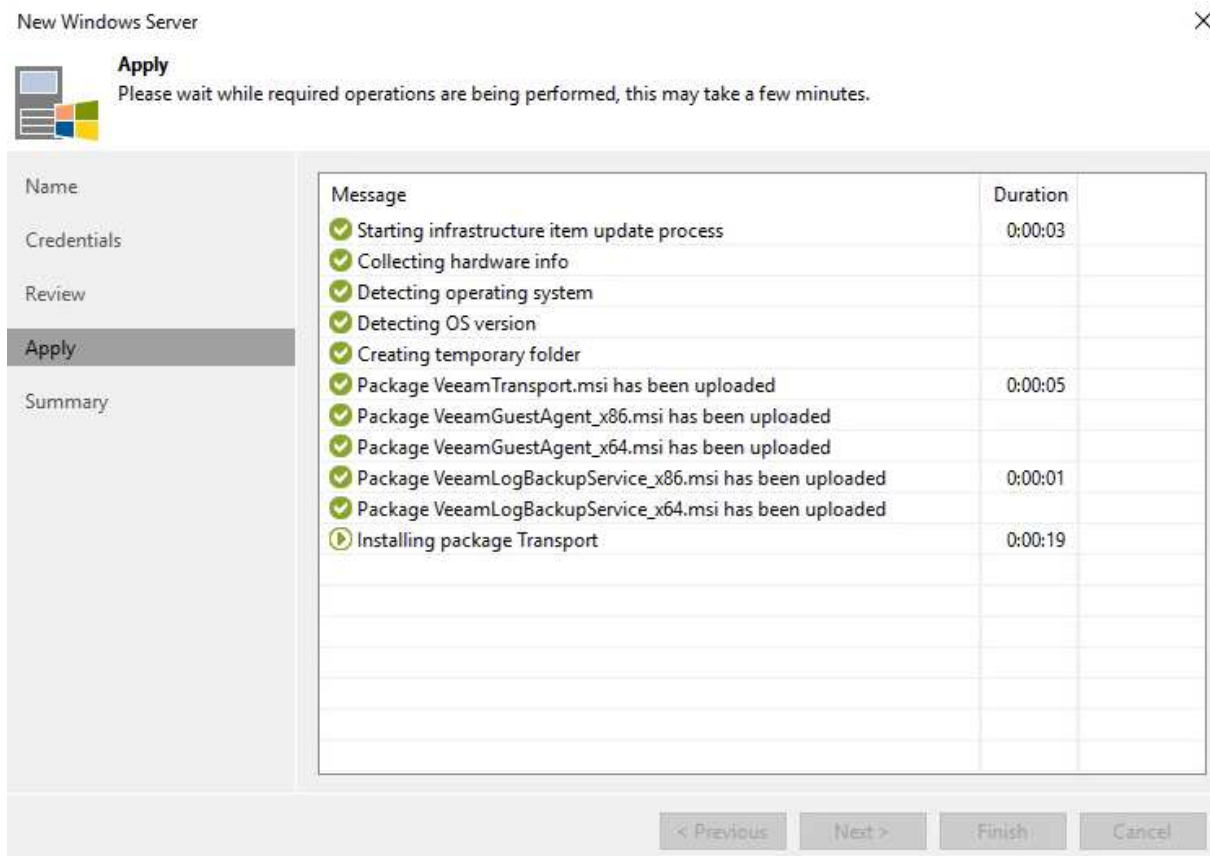


3. In the **Add VMware Proxy** wizard click the **Add New...** button to add a new proxy server.

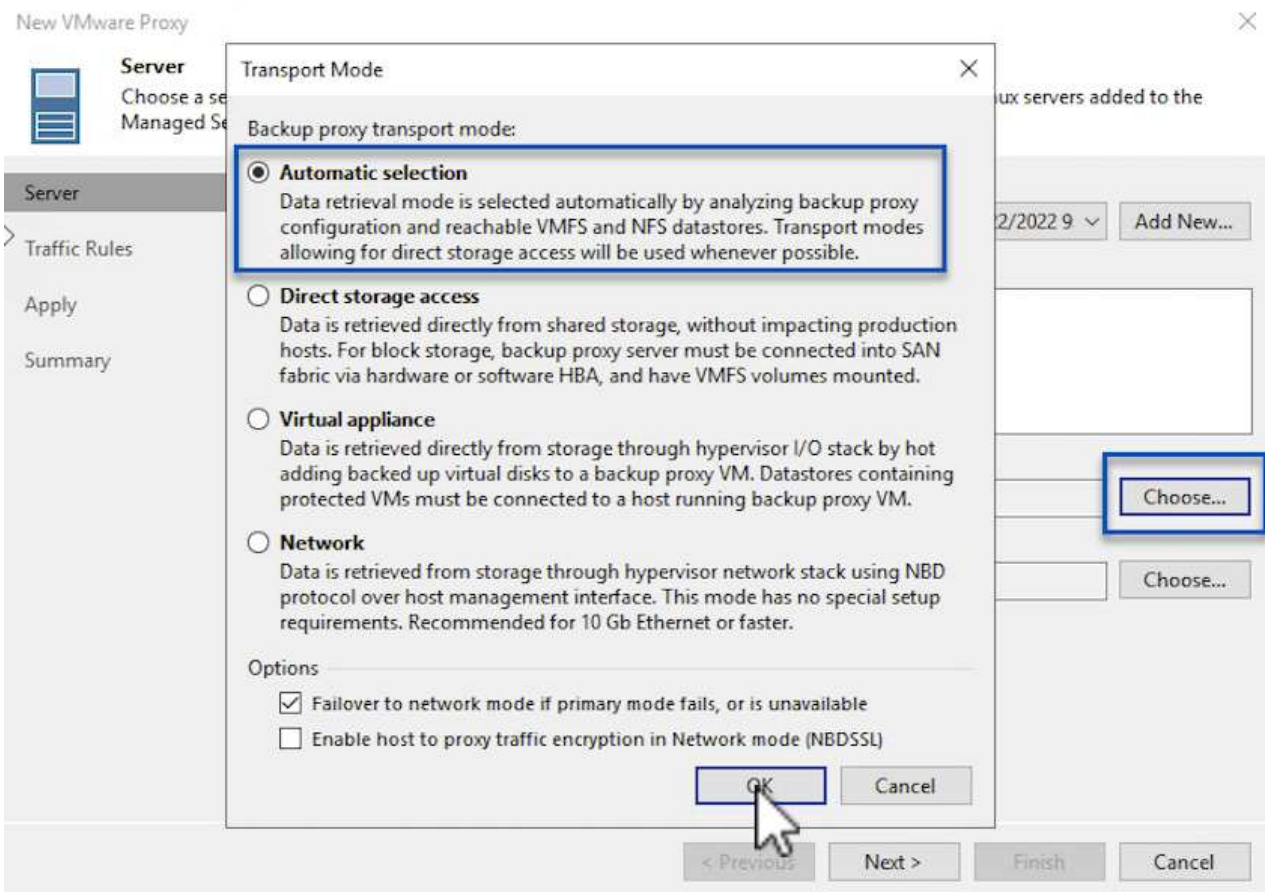


4. Select to add Microsoft Windows and follow the prompts to add the server:
 - Fill out the DNS name or IP address

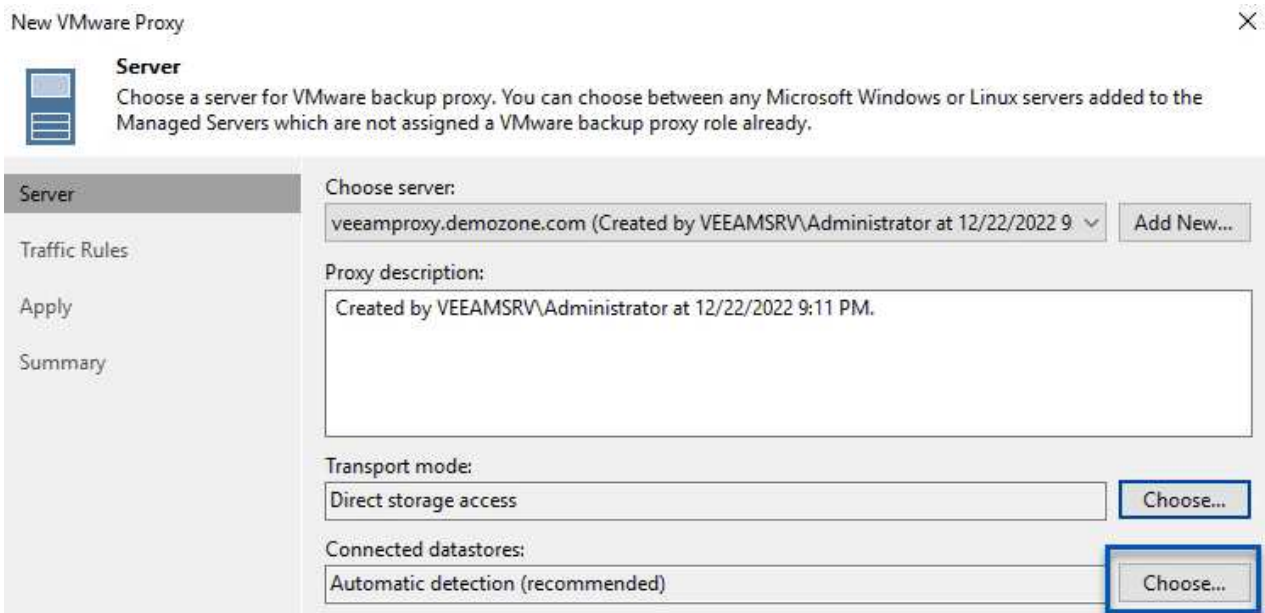
- Select an account to use for Credentials on the new system or add new credentials
- Review the components to be installed and then click on **Apply** to begin the deployment

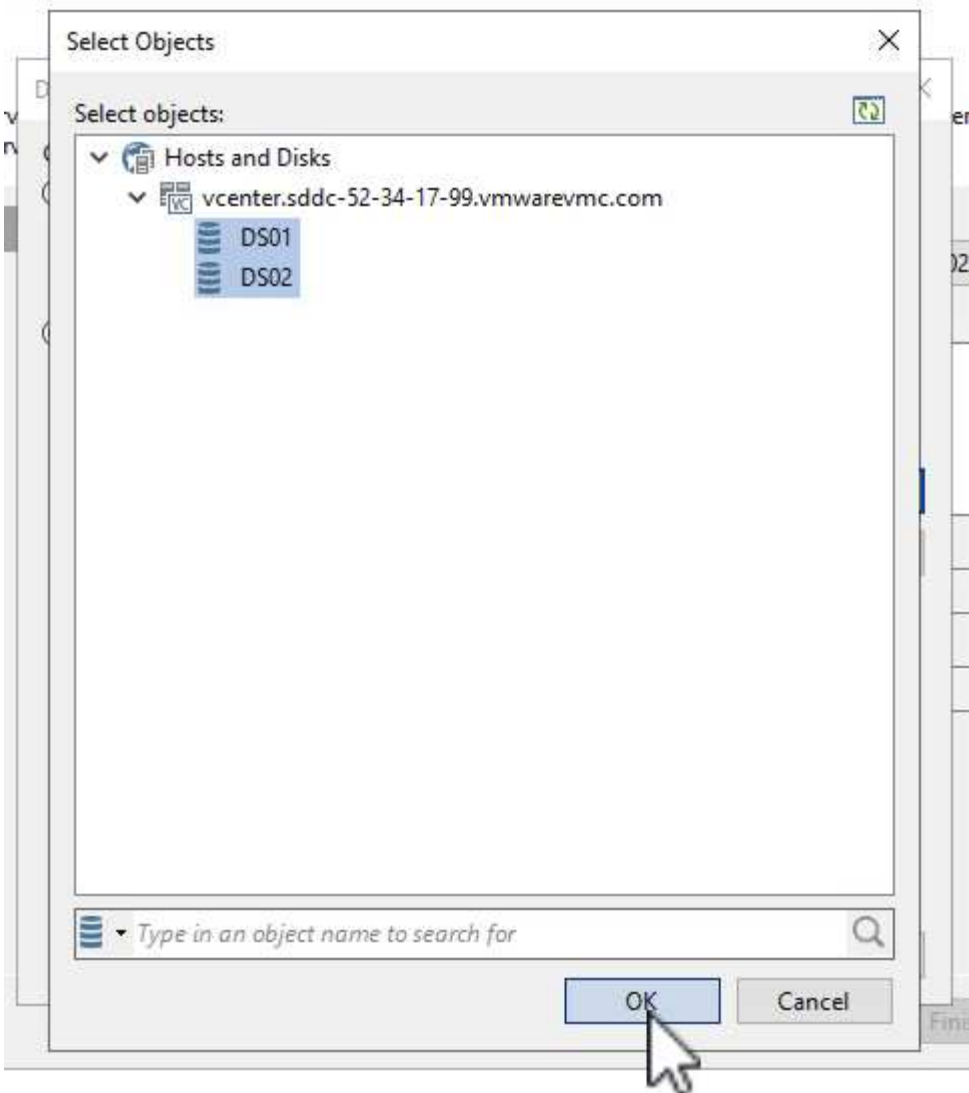


5. Back in the **New VMware Proxy** wizard, choose a Transport Mode. In our case we chose **Automatic Selection**.



6. Select the Connected datastores that you want the VMware Proxy to have direct access to.





7. Configure and apply any specific network traffic rules such as encryption or throttling that are desired. When complete click on the **Apply** button to complete the deployment.

New VMware Proxy

Traffic Rules

Review network traffic encryption and throttling rules which apply to this backup proxy.

Server

Traffic Rules

Apply

Summary

Network traffic rules control encryption and throttling of network traffic based on the destination. Throttling is global, with set bandwidth split equally across all backup proxies falling into the rule.

The following network traffic rules apply to this proxy:

Name	Encryption	Throttling	Time period	
Internet	Enabled	Disabled		

Manage network traffic rules

View

< Previous

Apply

Finish

Cancel

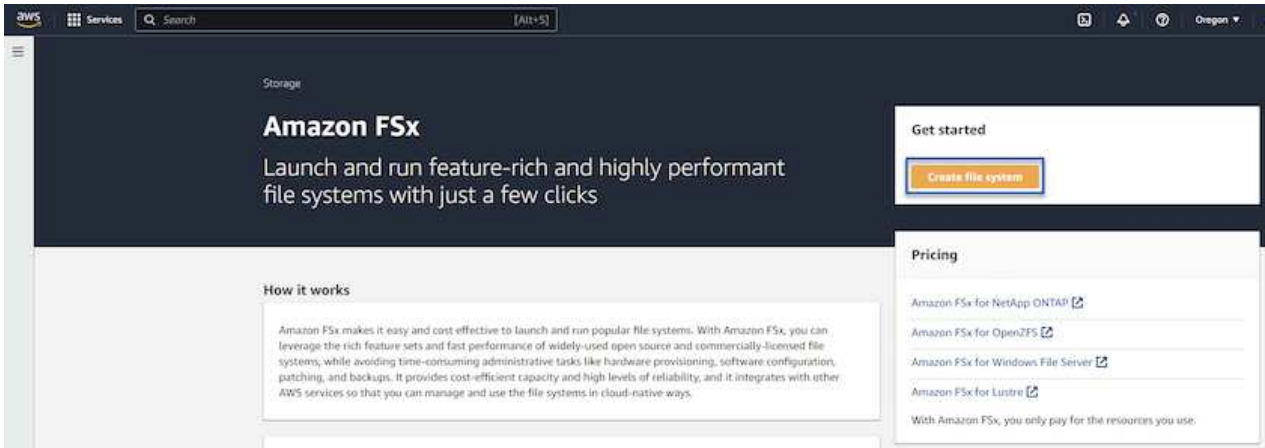
Configure storage and Backup Repositories

The primary Veeam Backup server and Veeam Proxy server have access to a backup repository in the form of direct connected storage. In this section we cover creating an FSx for ONTAP file system, mounting iSCSI LUNs to the Veeam servers and creating Backup Repositories.

Create FSx for ONTAP file system

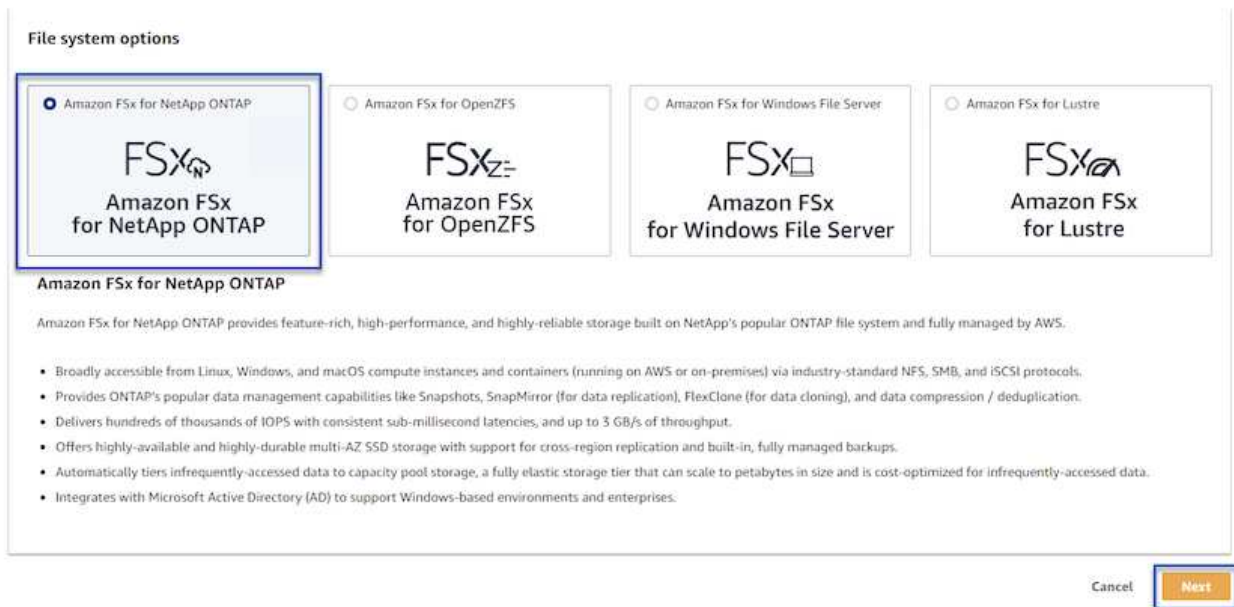
Create an FSx for ONTAP file system that will be used to host the iSCSI volumes for the Veeam Backup Repositories.

1. In the AWS console, Go to FSx and then **Create file system**



2. Select **Amazon FSx for NetApp ONTAP** and then **Next** to continue.

Select file system type



3. Fill in the file system name, deployment type, SSD storage capacity and the VPC in which the FSx for ONTAP cluster will reside. This must be a VPC configured to communicate with the virtual machine network in VMware Cloud. Click on **Next**.

Create file system

Creation method

☒ Quick create

Use recommended best-practice configurations. Most configuration options can be changed after the file system is created.

☐ Standard create

You set all of the configuration options, including specifying performance, networking, security, backups, and maintenance.

Quick configuration

File system name - optional info

BackupFSxN

1

Maximum of 256 Unicode letters, whitespace, and numbers, plus + - = . _ : /

Deployment type info

☐ Multi-AZ

☒ Single-AZ

2

SSD storage capacity info

4096

GiB

3

Minimum 1024 GiB; Maximum 192 TiB

Virtual Private Cloud (VPC) info

Specify the VPC from which your file system is accessible.

Demo-FsxforONTAP-VPC | vpc-05596abe79cb653b7

4

Storage efficiency

Select whether you would like to enable ONTAP's storage efficiency features: deduplication, compression, and compaction

☒ Enabled (recommended)

☐ Disabled

Cancel

Back

Next

4. Review the deployment steps and click on **Create File System** to begin the file system creation process.

Configure and mount iSCSI LUNs

Create and configure the iSCSI LUNs on FSx for ONTAP and mount to the Veeam backup and proxy servers. These LUNs will later be used to create Veeam backup repositories.



Creating an iSCSI LUN on FSx for ONTAP is a multi-step process. The first step of creating the volumes can be accomplished in the Amazon FSx Console or with the NetApp ONTAP CLI.



For more information on using FSx for ONTAP, see the [FSx for ONTAP User Guide](#).

1. From the NetApp ONTAP CLI create the initial volumes using the following command:

```
FSx-Backup::> volume create -vserver svm_name -volume vol_name  
-aggregate aggregate_name -size vol_size -type RW
```

2. Create LUNs using the volumes created in the previous step:

```
FSx-Backup::> lun create -vserver svm_name -path  
/vol/vol_name/lun_name -size size -ostype windows -space-allocation  
enabled
```

3. Grant access to the LUNs by creating an initiator group containing the iSCSI IQN of the Veeam backup and proxy servers:

```
FSx-Backup::> igroup create -vserver svm_name -igroup igroup_name  
-protocol iSCSI -ostype windows -initiator IQN
```

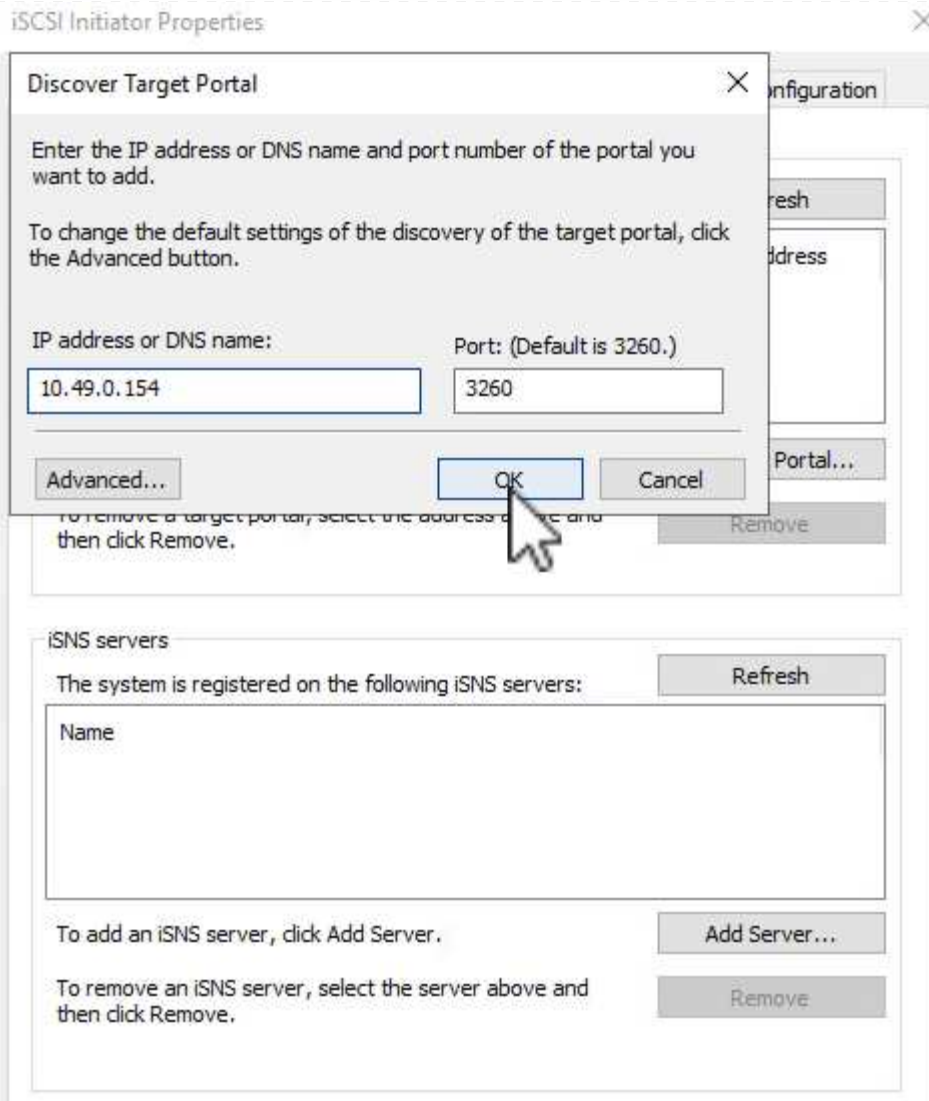


To complete the preceding step you will need to first retrieve the IQN from the iSCSI initiator properties on the Windows servers.

4. Finally, map the LUNs to the initiator group that you just created:

```
FSx-Backup::> lun mapping create -vserver svm_name -path  
/vol/vol_name/lun_name igroup igroup_name
```

5. To mount the iSCSI LUNs, log into the Veeam Backup & Replication Server and open iSCSI Initiator Properties. Go to the **Discover** tab and enter the iSCSI target IP address.



6. On the **Targets** tab, highlight the inactive LUN and click on **Connect**. Check the **Enable multi-path** box and click on **OK** to connect to the LUN.

Targets Discovery Favorite Targets Volumes and Devices RADIUS Configuration

Quick Connect
To discover and log on to a target using a basic connection, type the IP address or DNS name of the target and then click Quick Connect.

Target:

Discovered targets

Name	Status
iqn.1992-08.com.netapp:sn.d9aad3cd818011edbfcd87a...	Inactive

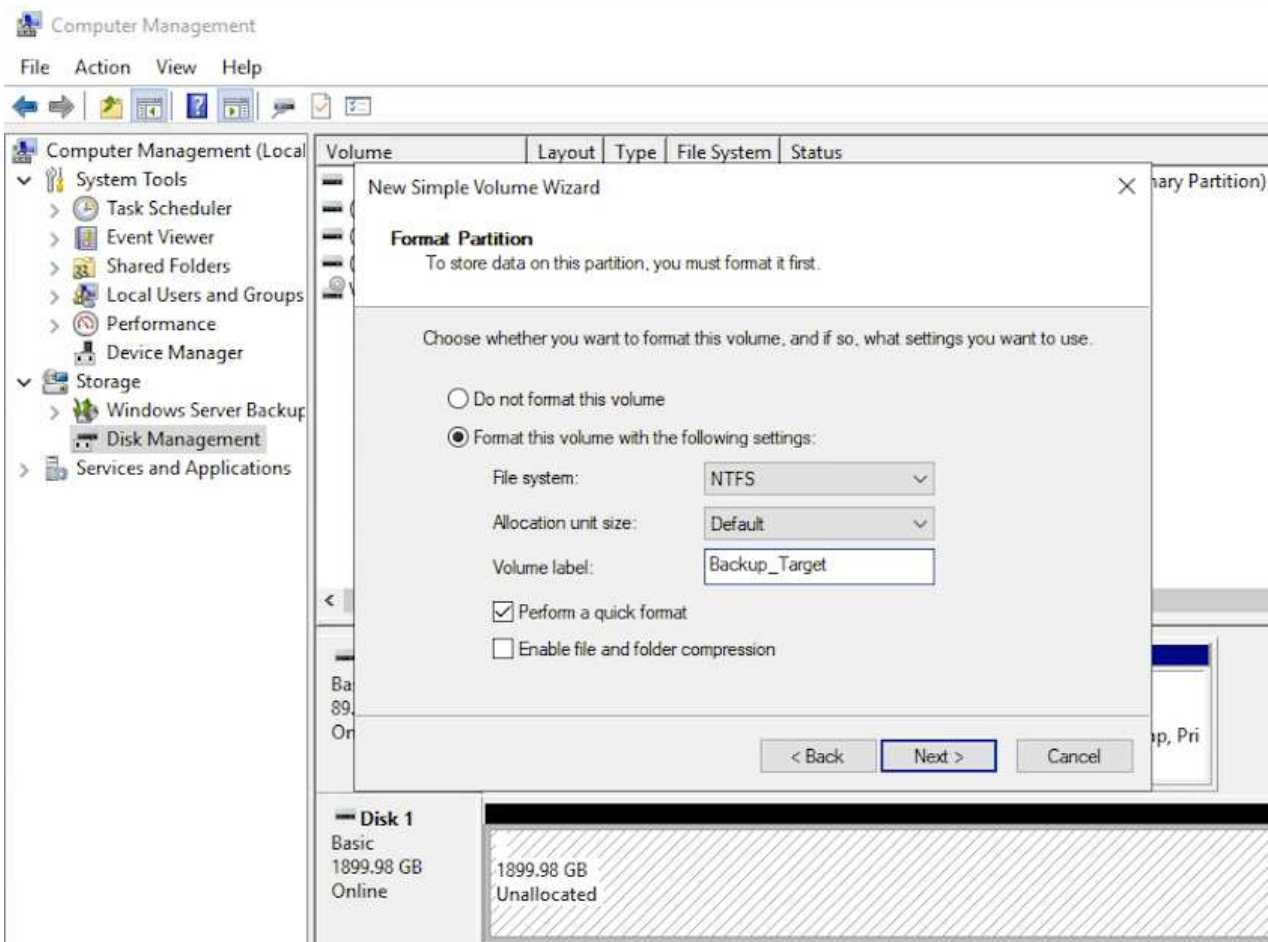
To connect using advanced options, select a target and then click Connect.

To completely disconnect a target, select the target and then click Disconnect.

For target properties, including configuration of sessions, select the target and click Properties...

For configuration of devices associated with a target, select the target and then click Devices...

7. In the Disk Management utility initialize the new LUN and create a volume with the desired name and drive letter. Check the **Enable multi-path** box and click on **OK** to connect to the LUN.

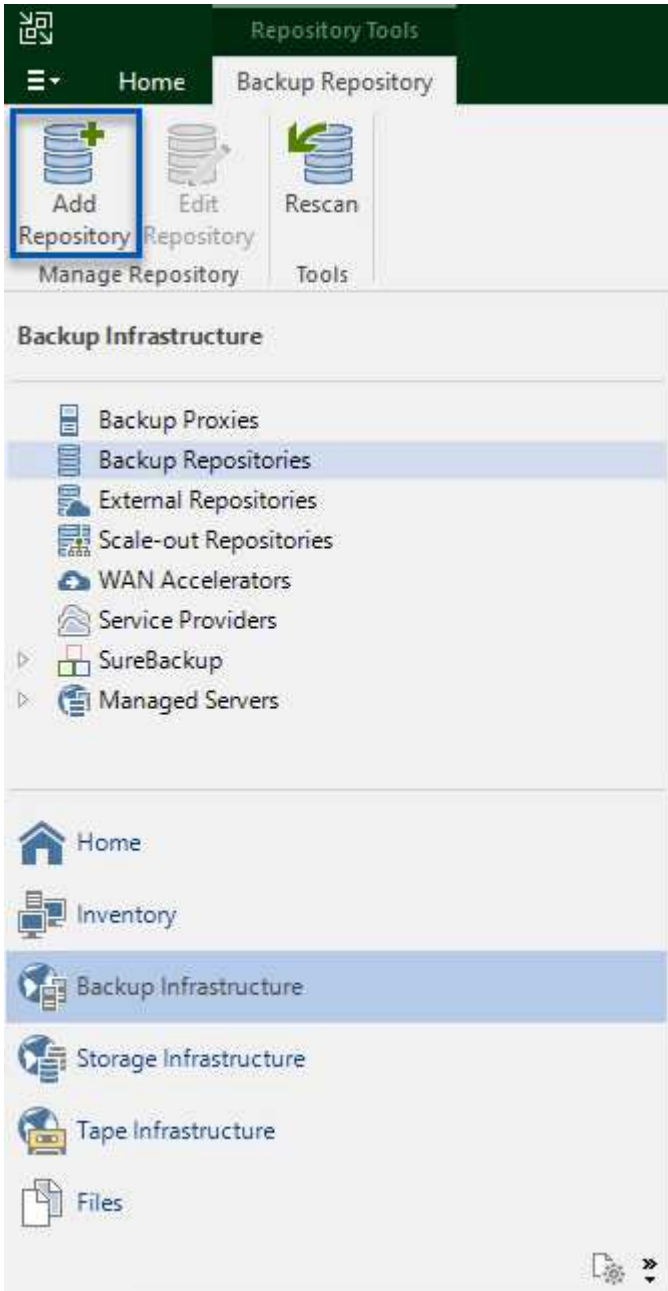


8. Repeat these steps to mount the iSCSI volumes on the Veeam Proxy server.

Create Veeam Backup Repositories


In the Veeam Backup and Replication console, create backup repositories for the Veeam Backup and Veeam Proxy servers. These repositories will be used as backup targets for the virtual machines backups.

1. In the Veeam Backup and Replication console click on **Backup Infrastructure** in the lower left and then select **Add Repository**



2. In the New Backup Repository wizard, enter a name for the repository and then select the server from the drop-down list and click on the **Populate** button to choose the NTFS volume that will be used.

New Backup Repository



Review
Please review the settings, and click Apply to continue.

Name

Server

Repository

Mount Server

Review

Apply

Summary

The following components will be processed on server veeamproxy.demozone.com:

Component name	Status
Transport	already exists
vPower NFS	will be installed
Mount Server	will be installed

☐ Search the repository for existing backups and import them automatically
☐ Import guest file system index data to the catalog

< Previous

Apply

Finish

Cancel

5. Repeat these steps for any additional proxy servers.

Configure Veeam backup jobs

Backup jobs should be created utilizing the the Backup Repositories in the previous section. Creating backup jobs is a normal part of any storage administrator's repertoire and we do not cover all of the steps here. For more complete information on creating backup jobs in Veeam, see the [Veeam Help Center Technical Documentation](#).

In this solution separate backup jobs were created for:

- Microsoft Windows SQL Servers
- Oracle database servers
- Windows file servers
- Linux file servers

General considerations when configuring Veeam backup jobs

1. Enable application-aware processing to create consistent backups and perform transaction log processing.
2. After enabling application-aware processing add the correct credentials with admin privileges to the application as this may be different than the guest OS credentials.

Processing Settings ✕

General SQL Oracle Exclusions Scripts

Specify Oracle account with SYSDBA privileges: i

🔑 Use guest OS credentials ▼ Add...

[Manage accounts](#)

Archived logs:

☐ Do not delete archived logs

☒ Delete logs older than: hours

☐ Delete logs over: GB

☐ Backup logs every: minutes

Retain log backups:

☒ Until the corresponding image-level backup is deleted

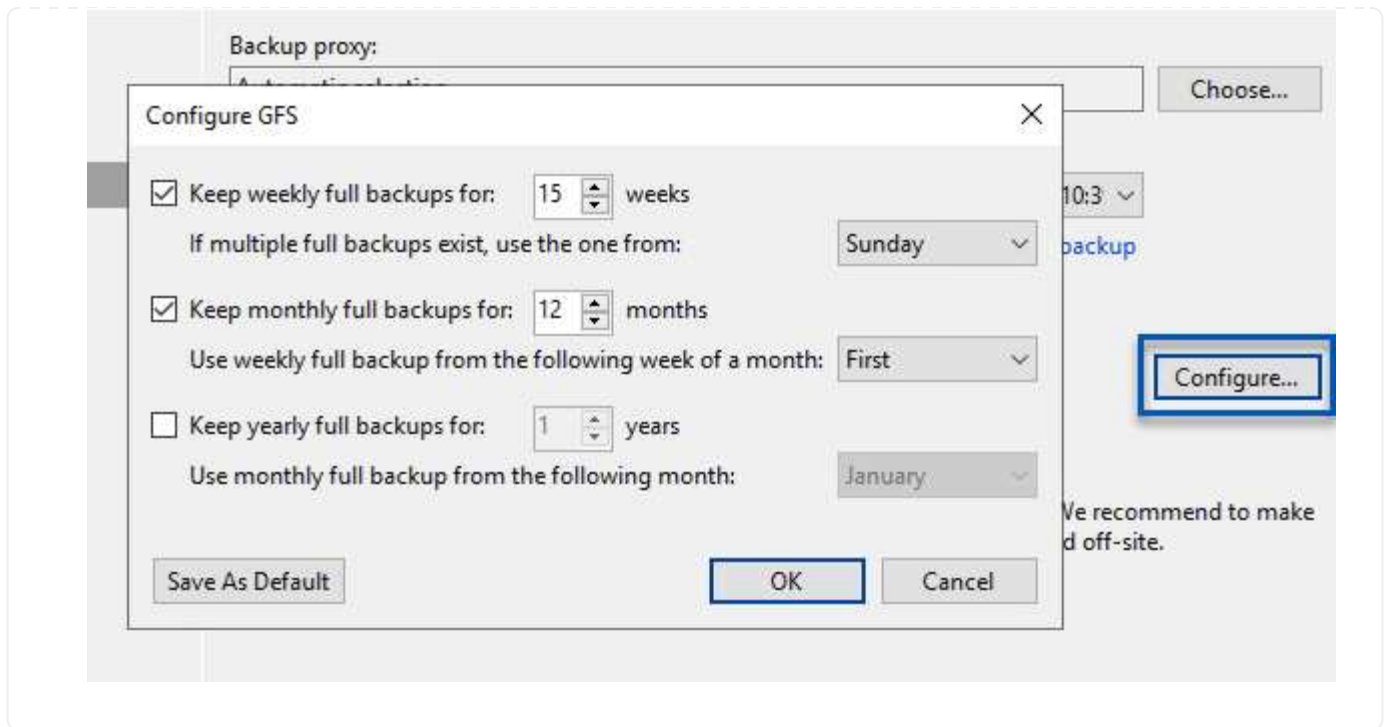
☐ Keep only last days of log backups

Log shipping servers:

Choose...

OK Cancel

3. To manage the retention policy for the backup check the **Keep certain full backups longer for archival purposes** and click the **Configure...** button to configure the policy.



Restore Application VMs with Veeam full restore

Performing a full restore with Veeam is the first step in performing an application restore. We validated that full restores of our VMs powered on and all services were running normally.

Restoring servers is a normal part of any storage administrator's repertoire and we do not cover all of the steps here. For more complete information on performing full restores in Veeam, see the [Veeam Help Center Technical Documentation](#).

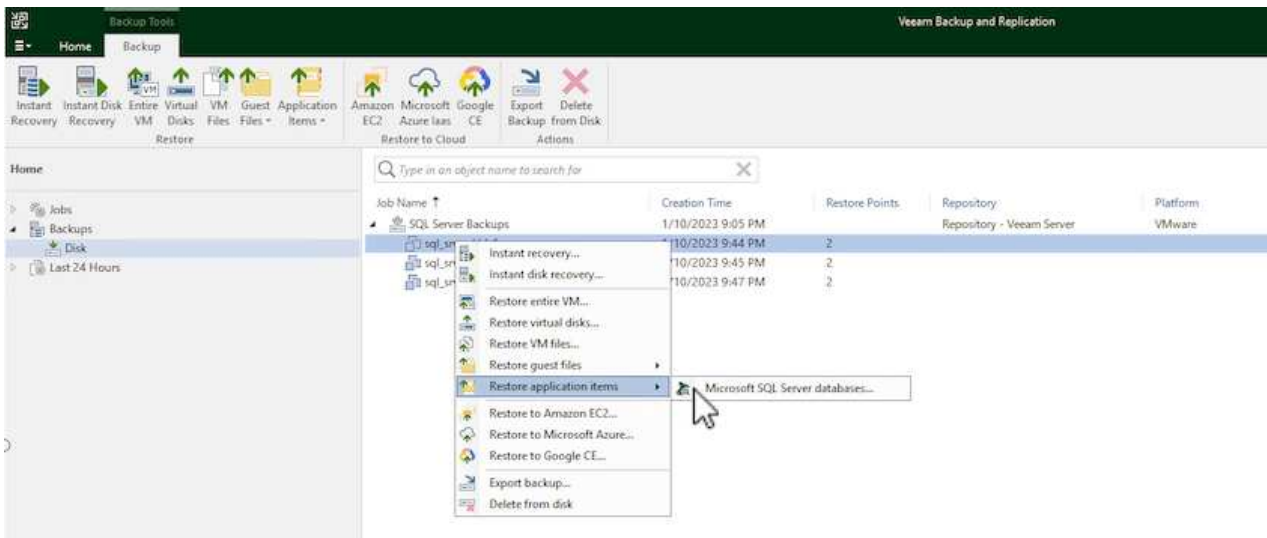
Restore SQL Server databases

Veeam Backup & Replication provides several options for restoring SQL Server databases. For this validation we used the Veeam Explorer for SQL Server with Instant Recovery to execute restores of our SQL Server databases. SQL Server Instant Recovery is a feature that allows you to quickly restore SQL Server databases without having to wait for a full database restore. This rapid recovery process minimizes downtime and ensures business continuity. Here's how it works:

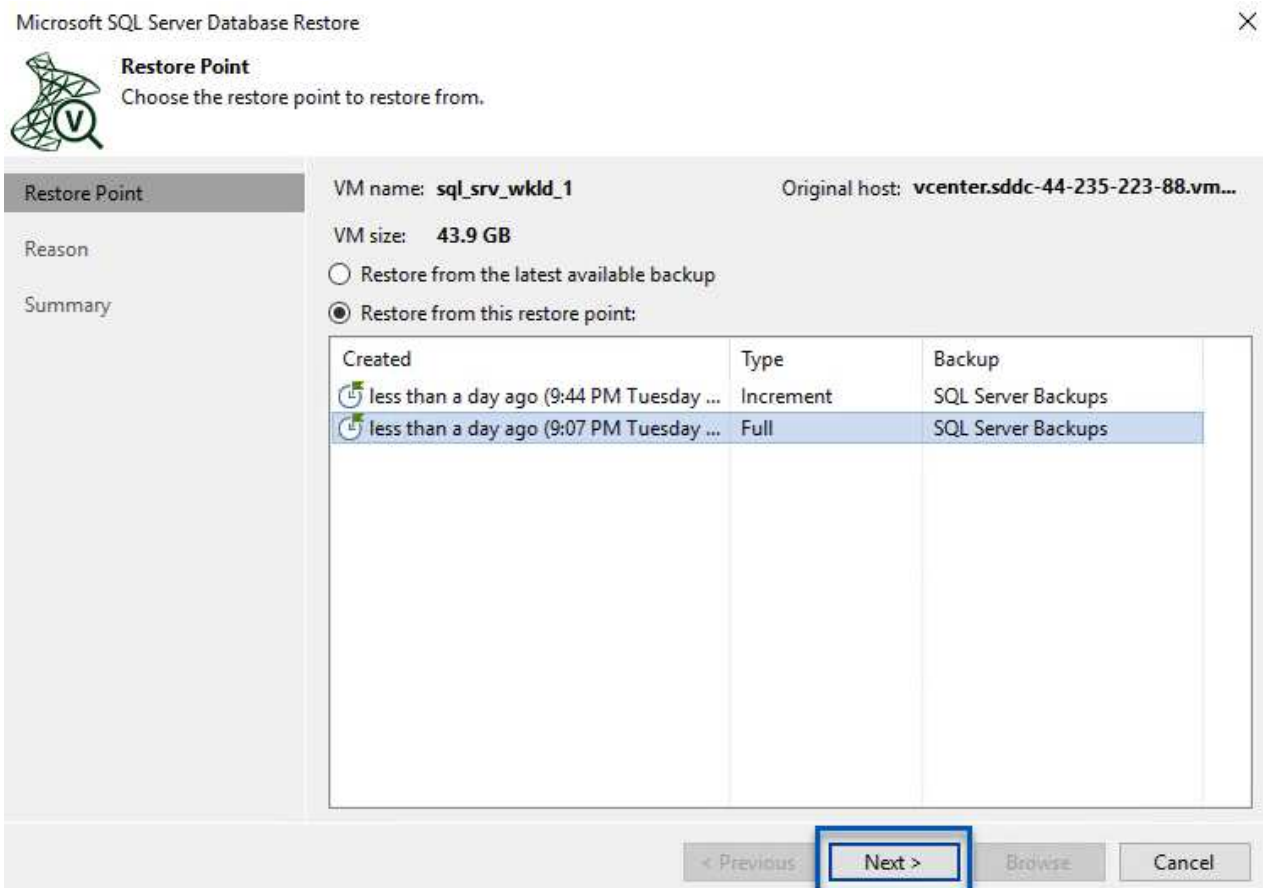
- Veeam Explorer **mounts the backup** containing the SQL Server database to be restored.
- The software **publishes the database** directly from the mounted files, making it accessible as a temporary database on the target SQL Server instance.
- While the temporary database is in use, Veeam Explorer **redirects user queries** to this database, ensuring that users can continue to access and work with the data.
- In the background, Veeam **performs a full database restore**, transferring data from the temporary database to the original database location.
- Once the full database restore is complete, Veeam Explorer **switches user queries back to the original** database and removes the temporary database.

Restore SQL Server database with Veeam Explorer Instant Recovery

1. In the Veeam Backup and Replication console, navigate to the list of SQL Server backups, right click on a server and select **Restore application items** and then **Microsoft SQL Server databases....**



2. In the Microsoft SQL Server Database Restore Wizard select a restore point from the list and click on **Next**.



3. Enter a **Restore reason** if desired and then, on the Summary page, click on the **Browse** button to launch Veeam Explorer for Microsoft SQL Server.

**Summary**

Review the restore settings, and click Browse to exit the wizard and open Veeam Explorer for SQL Server, where you will select databases to restore.

Restore Point

Reason

Summary

Summary:

VM name: sql_srv_wkld_1

Restore point:

Current: sql_srv_wkld_1 less than a day ago (9:07 PM Tuesday 1/10/2023)

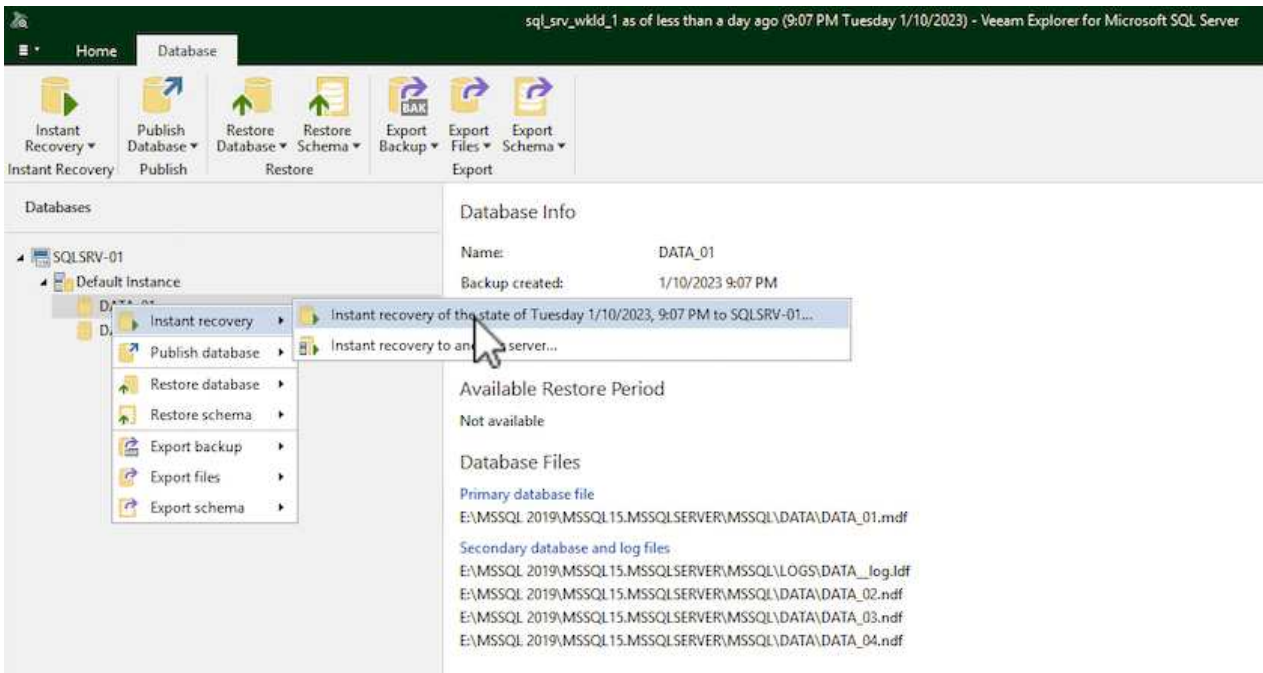
< Previous

Next >

Browse

Cancel

4. In Veeam Explorer expand the list of database instances, right click and select **Instant recovery** and then the specific restore point to recover to.



5. In the Instant Recovery Wizard specify the switchover type. This can either be automatically with minimal downtime, manually, or at a specified time. Then click the **Recover** button to begin the restore process.

Instant Recovery Wizard
✕

Specify database switchover scheduling options

Specify switchover type:

☒ **Auto**
Switchover will be performed automatically with minimal possible downtime once the database is ready.

☐ **Manual**
Switchover can be performed manually at any point in time after the database is ready.

☐ **Scheduled at:**

Back
Recover
Cancel

6. The recovery process can be monitored from Veeam Explorer.

The screenshot shows the Veeam Explorer for Microsoft SQL Server interface. The 'Instant Recovery' tab is active, displaying the progress of the recovery process for the 'DATA_01' database. The 'Instant Recovery Info' section shows the status as 'Starting (restored)...', the SQL Server as 'SQLSRV-01', the target name as 'DATA_01', the target point in time as '1/10/2023 9:07 PM', the restore point as 'sql_srv_wkld_1', and the switchover mode as 'Auto'. The 'Database Files' section lists the primary database file and secondary database and log files. The 'Action' table shows the progress of the recovery process, including publishing the database, copying target files, synchronizing files, and detaching the database.

Action	Duration
Instant Recovery started at 1/10/2023 10:12:06 PM	
Publishing database	00:35
Copying target files	08:28
Database published at 1/10/2023 10:12:42 PM	
Synchronizing files	
Ready for switchover	
Detaching database	
Detach database files with permissions	

For more detailed information on performing SQL Server restore operations with Veeam Explorer refer to the Microsoft SQL Server section in the [Veeam Explorers User Guide](#).

Restore Oracle databases with Veeam Explorer

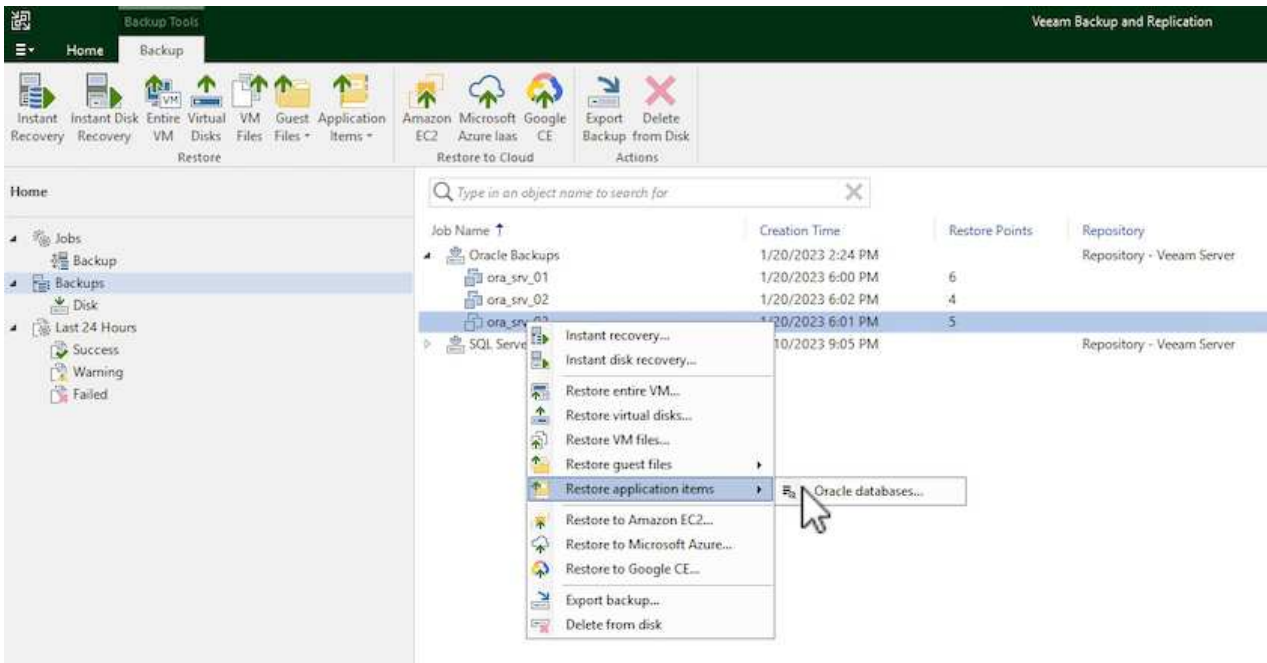
Veeam Explorer for Oracle database provides the ability to perform a standard Oracle database restore or an uninterrupted restore using Instant Recovery. It also supports publishing databases for fast access, recovery of Data Guard databases and restores from RMAN backups.

For more detailed information on performing Oracle database restore operations with Veeam Explorer refer to the Oracle section in the [Veeam Explorers User Guide](#).

Restore Oracle database with Veeam Explorer

In this section an Oracle database restore to a different server is covered using Veeam Explorer.

1. In the Veeam Backup and Replication console, navigate to the list of Oracle backups, right click on a server and select **Restore application items** and then **Oracle databases....**



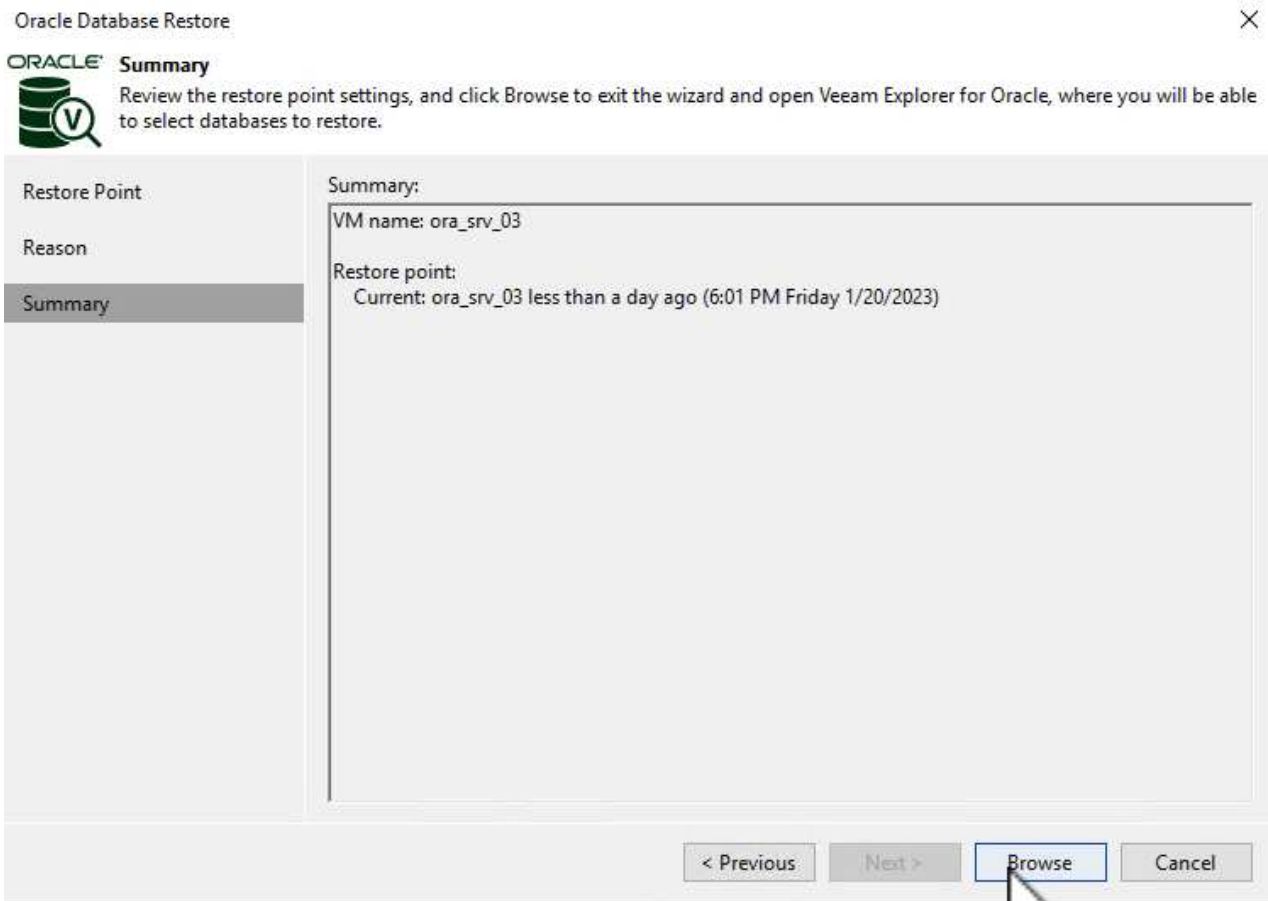
2. In the Oracle Database Restore Wizard select a restore point from the list and click on **Next**.

**Restore Point**

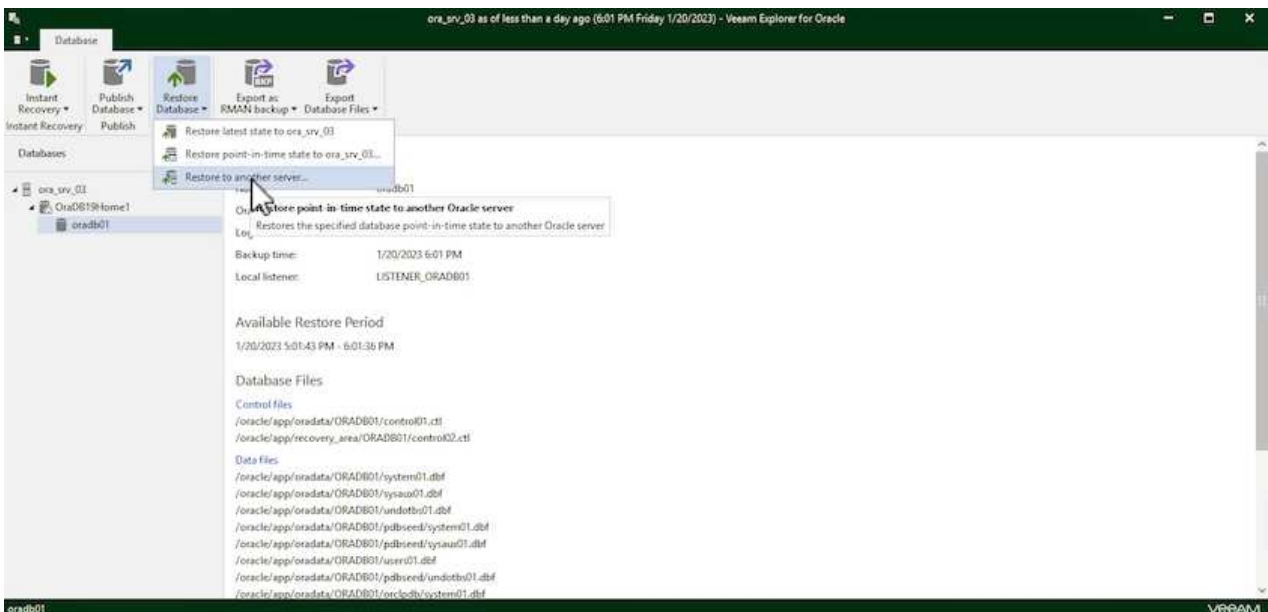
Choose the restore point to restore from.

Restore Point	VM name: ora_srv_03	Original host: vcenter.sddc-44-235-223-88.vm...																		
Reason	VM size: 38.5 GB																			
Summary	<input checked="" type="radio"/> Restore from the latest available backup <input type="radio"/> Restore from this restore point:																			
	<table border="1"><thead><tr><th>Created</th><th>Type</th><th>Backup</th></tr></thead><tbody><tr><td> less than a day ago (6:01 PM Friday 1/...</td><td>Increment</td><td>Oracle Backups</td></tr><tr><td> less than a day ago (5:01 PM Friday 1/...</td><td>Increment</td><td>Oracle Backups</td></tr><tr><td> less than a day ago (4:02 PM Friday 1/...</td><td>Increment</td><td>Oracle Backups</td></tr><tr><td> less than a day ago (3:47 PM Friday 1/...</td><td>Increment</td><td>Oracle Backups</td></tr><tr><td> less than a day ago (2:47 PM Friday 1/...</td><td>Full</td><td>Oracle Backups</td></tr></tbody></table>	Created	Type	Backup	less than a day ago (6:01 PM Friday 1/...	Increment	Oracle Backups	less than a day ago (5:01 PM Friday 1/...	Increment	Oracle Backups	less than a day ago (4:02 PM Friday 1/...	Increment	Oracle Backups	less than a day ago (3:47 PM Friday 1/...	Increment	Oracle Backups	less than a day ago (2:47 PM Friday 1/...	Full	Oracle Backups	
Created	Type	Backup																		
less than a day ago (6:01 PM Friday 1/...	Increment	Oracle Backups																		
less than a day ago (5:01 PM Friday 1/...	Increment	Oracle Backups																		
less than a day ago (4:02 PM Friday 1/...	Increment	Oracle Backups																		
less than a day ago (3:47 PM Friday 1/...	Increment	Oracle Backups																		
less than a day ago (2:47 PM Friday 1/...	Full	Oracle Backups																		
<div>< Previous Next > Browse Cancel</div>																				

3. Enter a **Restore reason** if desired and then, on the Summary page, click on the **Browse** button to launch Veeam Explorer for Oracle.



4. In Veeam Explorer expand the list of database instances, click on the database to be restored and then from the **Restore Database** drop-down menu at the top select **Restore to another server....**



5. In the Restore Wizard specify the restore point to restore from and click **Next**.

Restore Wizard

Specify restore point

Specify point in time you want to restore the database to:

☒ Restore to the point in time of the selected image-level backup

☐ Restore to a specific point in time (requires redo log backups)

5:01 PM
1/20/2023

6:01 PM
1/20/2023

Friday, January 20, 2023 6:01 PM

☐ Perform restore to the specific transaction

Enables you to review major database transactions around the selected time, and restore the database to the moment in time right before the unwanted change.

!

 To enable this functionality, specify the staging Oracle server under Menu > Options.

Back

Next

Cancel

6. Specify the target server the database will be restored to and the account credentials and click **Next**.

Restore Wizard

Specify target Linux server connection credentials

Server: ora_srv_01 SSH port: 22

Account: oracle Advanced...

Password: [Click here to change the password]

☐ Private key is required for this connection

Private key: Browse...

Passphrase:

Back

Next

Cancel

7. Finally, specify the database files target location and click the **Restore** button to start the restore process.

Specify database files target location

Control files

/oracle/app/oradata/oradb01/control01.ctl
/oracle/app/recovery_area/oradb01/control02.ctl

Data files

/oracle/app/oradata/oradb01/system01.dbf
/oracle/app/oradata/oradb01/sysaux01.dbf
/oracle/app/oradata/oradb01/undotbs01.dbf
/oracle/app/oradata/oradb01/pdbseed/system01.dbf
/oracle/app/oradata/oradb01/pdbseed/sysaux01.dbf
/oracle/app/oradata/oradb01/users01.dbf

Back

Restore

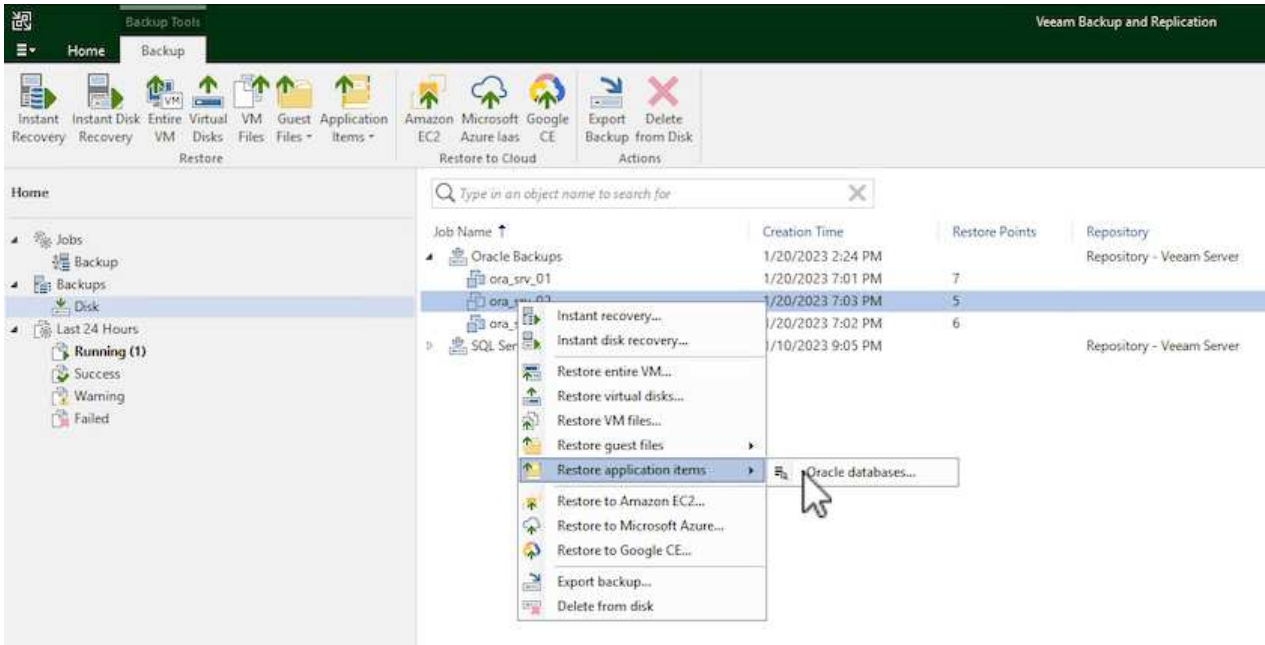
Cancel

8. Once the database recovery is complete check that the Oracle database starts properly on the server.

Publish Oracle database to alternate server

In this section a database is published to an alternate server for fast access without launching a full restore.

1. In the Veeam Backup and Replication console, navigate to the list of Oracle backups, right click on a server and select **Restore application items** and then **Oracle databases....**



2. In the Oracle Database Restore Wizard select a restore point from the list and click on **Next**.

Oracle Database Restore

ORACLE® Restore Point
Choose the restore point to restore from.

Restore Point

Reason

Summary

VM name: **ora_srv_02** Original host: **vcenter.sddc-44-235-223-88.vm...**

VM size: **38.1 GB**

☒ Restore from the latest available backup

☐ Restore from this restore point:

Created	Type	Backup
less than a day ago (7:03 PM Friday 1/...	Increment	Oracle Backups
less than a day ago (6:02 PM Friday 1/...	Increment	Oracle Backups
less than a day ago (5:02 PM Friday 1/...	Increment	Oracle Backups
less than a day ago (4:03 PM Friday 1/...	Increment	Oracle Backups
less than a day ago (3:49 PM Friday 1/...	Full	Oracle Backups

< Previous **Next >** Browse Cancel

- Enter a **Restore reason** if desired and then, on the Summary page, click on the **Browse** button to launch Veeam Explorer for Oracle.
- In Veeam Explorer expand the list of database instances, click on the database to be restored and then from the **Publish Database** drop-down menu at the top select **Publish to another server....**

Database

Instant Recovery

Publish Database

Restore Database

Export as RMAN backup

Export Database Files

Instant Recovery

Publish to another server...

Export

Databases

ora_srv_02

OraDB19Home1

oradb01

Database Info

Name: oradb01

Oracle SID: oradb01

Log mode: ARCHIVELOG

Backup time: 1/20/2023 7:03 PM

Local listener: LISTENER_ORADB01

- In the Publish wizard, specify the restore point at which to publish the database from and click **Next**.
- Finally, specify the target linux file system location and click on **Publish** to begin the restore process.

Specify Oracle settings

☒ Restore to the original location☐ Restore to a different location:

Oracle Home: /oracle/app/product/19c

Browse...

Global Database Name: oradb01.demozone.com

Oracle SID: oradb01

Back

Publish

Cancel

7. Once the publish has completed log into the target server and run the following commands to ensure the database is running:

```
oracle@ora_srv_01> sqlplus / as sysdba
```

```
SQL> select name, open_mode from v$database;
```

```
oracle@ora_srv_01:~  
File Edit View Search Terminal Help  
[oracle@ora_srv_01 ~]$ sqlplus / as sysdba  
  
SQL*Plus: Release 19.0.0.0.0 - Production on Fri Jan 20 16:46:39 2023  
Version 19.3.0.0.0  
  
Copyright (c) 1982, 2019, Oracle. All rights reserved.  
  
Connected to:  
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production  
Version 19.3.0.0.0  
  
SQL> select name, open_mode from v$database;  


| NAME    | OPEN_MODE  |
|---------|------------|
| ORADB01 | READ WRITE |


```

Conclusion

VMware Cloud is a powerful platform for running business-critical applications and storing sensitive data. A secure data protection solution is essential for businesses that rely on VMware Cloud to ensure business continuity and help protect against cyber threats and data loss. By choosing a reliable and robust data protection solution, businesses can be confident that their critical data is safe and secure, no matter what.

The use case presented in this documentation focuses on proven data protection technologies that highlight the integration between NetApp, VMware, and Veeam. FSx for ONTAP is supported as supplemental NFS datastores for VMware Cloud in AWS and is used for all virtual machine and application data. Veeam Backup & Replication is a comprehensive data protection solution designed to help businesses improve, automate, and streamline their backup and recovery processes. Veeam is used in conjunction with iSCSI backup target volumes, hosted on FSx for ONTAP, to provide a secure and easy to manage data protection solution for application data residing in VMware Cloud.

Additional Information

To learn more about the technologies presented in this solution refer to the following additional information.

- [FSx for ONTAP User Guide](#)
- [Veeam Help Center Technical Documentation](#)
- [VMware Cloud on AWS Support. Considerations and Limitations](#)

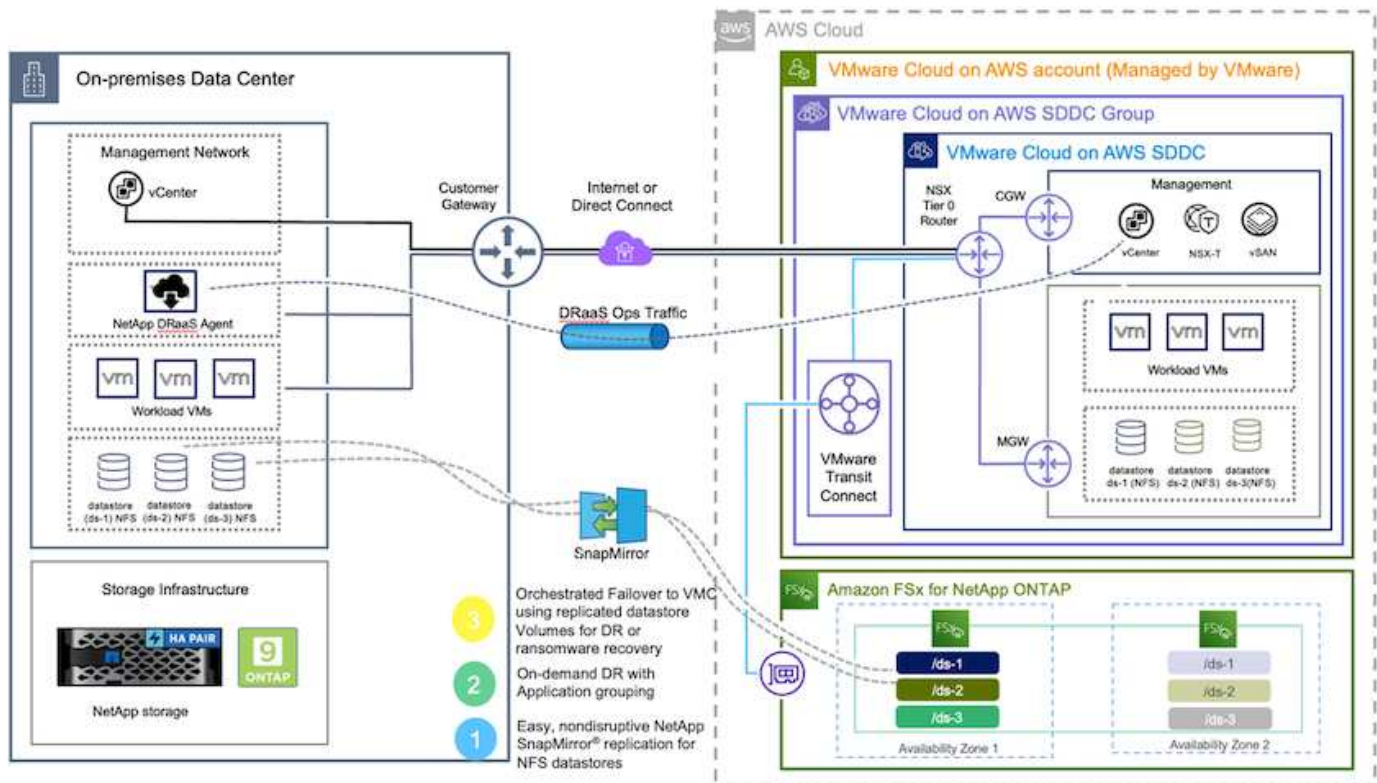
TR-4955: Disaster Recovery with FSx for ONTAP and VMC (AWS VMware Cloud)

Niyaz Mohamed, NetApp

Overview

Disaster recovery to cloud is a resilient and cost-effective way of protecting the workloads against site outages and data corruption events (for example, ransomware). With NetApp SnapMirror technology, on-premises VMware workloads can be replicated to FSx for ONTAP running in AWS.

Disaster Recovery Orchestrator (DRO; a scripted solution with UI) can be used to seamlessly recover workloads replicated from on-premises to FSx for ONTAP. DRO automates the recovery from the SnapMirror level, through VM registration to VMC, to network mappings directly on NSX-T. This feature is included with all VMC environments.



Getting started

Deploy and configure VMware Cloud on AWS

VMware Cloud on AWS provides a cloud-native experience for VMware-based workloads in the AWS ecosystem. Each VMware Software-Defined Data Center (SDDC) runs in an Amazon Virtual Private Cloud (VPC) and provides a full VMware stack (including vCenter Server), NSX-T software-defined networking, vSAN software-defined storage, and one or more ESXi hosts that provide compute and storage resources to the workloads. To configure a VMC environment on AWS, follow the steps at this [link](#). A pilot-light cluster can also be used for DR purposes.



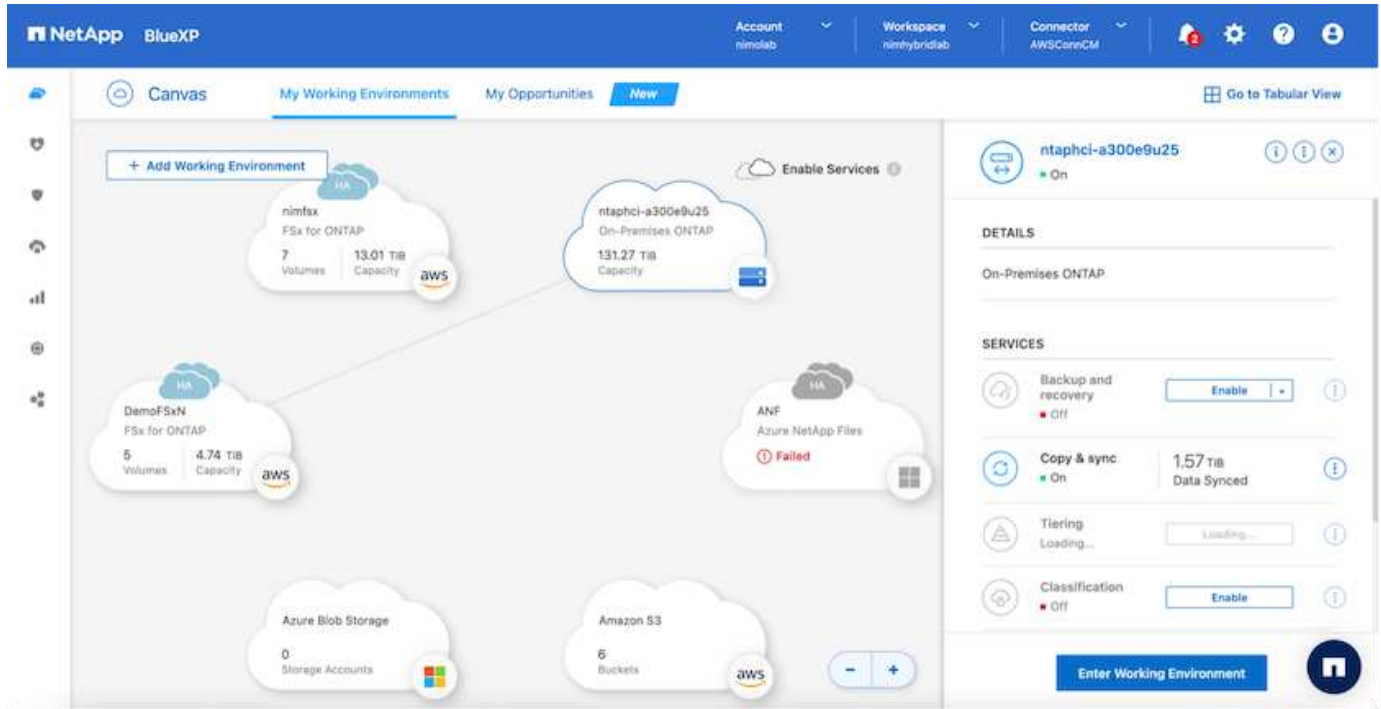
In the initial release, DRO supports an existing pilot-light cluster. On-demand SDDC creation will be available in an upcoming release.

Provision and configure FSx for ONTAP

Amazon FSx for NetApp ONTAP is a fully managed service that provides highly reliable, scalable, high-performing, and feature-rich file storage built on the popular NetApp ONTAP file system. Follow the steps at this [link](#) to provision and configure FSx for ONTAP.

Deploy and configure SnapMirror to FSx for ONTAP

The next step is to use NetApp BlueXP and discover the provisioned FSx for ONTAP on AWS instance and replicate the desired datastore volumes from an on-premises environment to FSx for ONTAP with the appropriate frequency and NetApp Snapshot copy retention:



Follow the steps in this link to configure BlueXP. You can also use the NetApp ONTAP CLI to schedule replication following this link.



A SnapMirror relationship is a prerequisite and must be created beforehand.

DRO installation

To get started with DRO, use the Ubuntu operating system on a designated EC2 instance or virtual machine to make sure you meet the prerequisites. Then install the package.

Prerequisites

- Make sure that connectivity to the source and destination vCenter and storage systems exists.
- DNS resolution should be in place if you are using DNS names. Otherwise, you should use IP addresses for the vCenter and storage systems.
- Create a user with root permissions. You can also use sudo with an EC2 instance.

OS requirements

- Ubuntu 20.04 (LTS) with minimum of 2GB and 4 vCPUs
- The following packages must be installed on the designated agent VM:
 - Docker
 - Docker-compose

- Jq

Change permissions on `docker.sock`: `sudo chmod 666 /var/run/docker.sock`.



The `deploy.sh` script executes all the required prerequisites.

Install the package

1. Download the installation package on the designated virtual machine:

```
git clone https://github.com/NetApp/DRO-AWS.git
```



The agent can be installed on-premises or within an AWS VPC.

2. Unzip the package, run the deployment script, and enter the host IP (for example, 10.10.10.10).

```
tar xvf DRO-prereq.tar
```

3. Navigate to the directory and run the deploy script as follows:

```
sudo sh deploy.sh
```

4. Access the UI using:

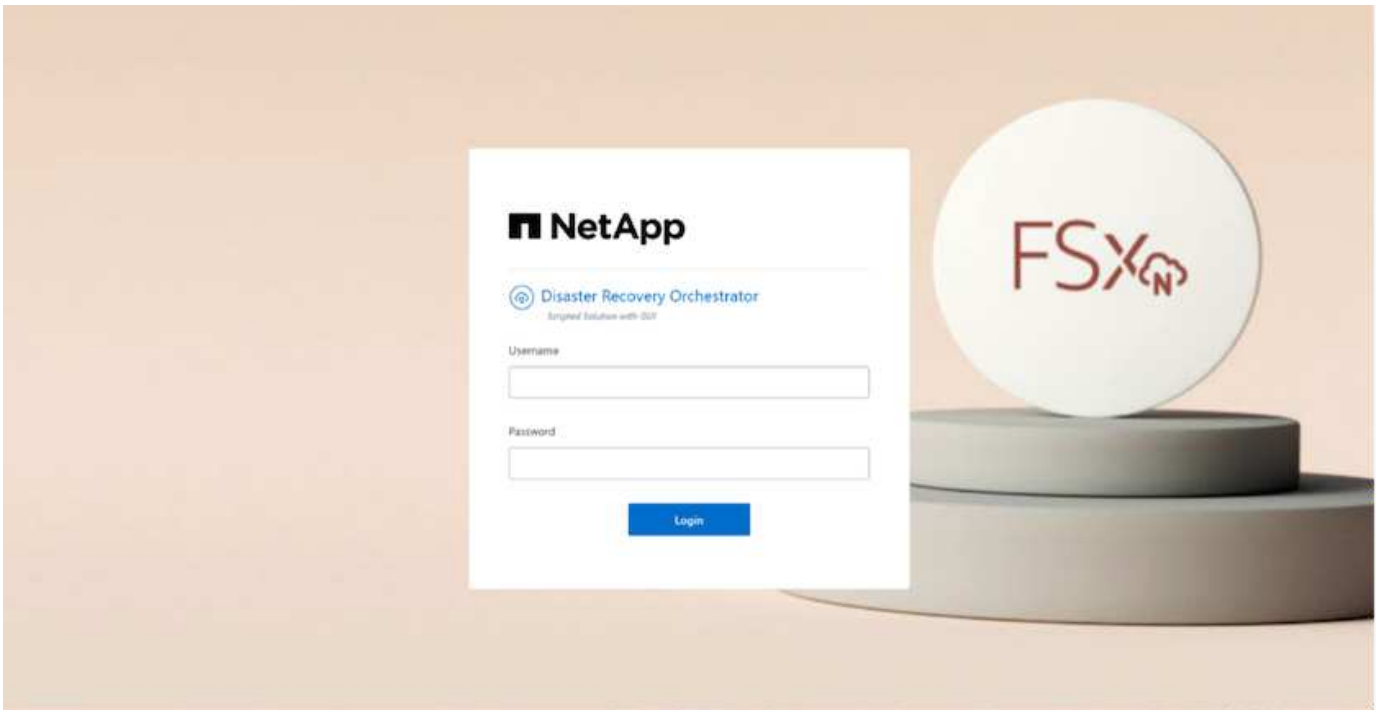
```
https://<host-ip-address>
```

with the following default credentials:

```
Username: admin  
Password: admin
```



The password can be changed using the "Change Password" option.



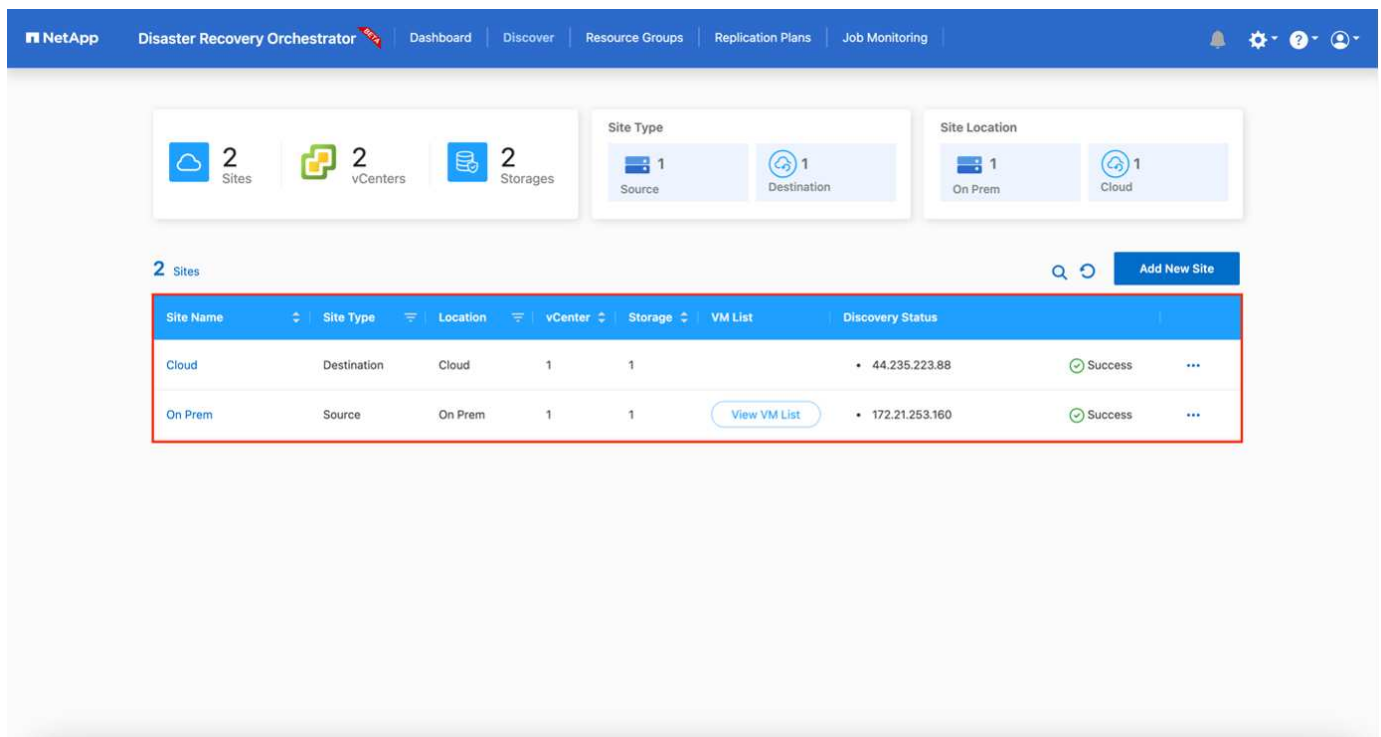
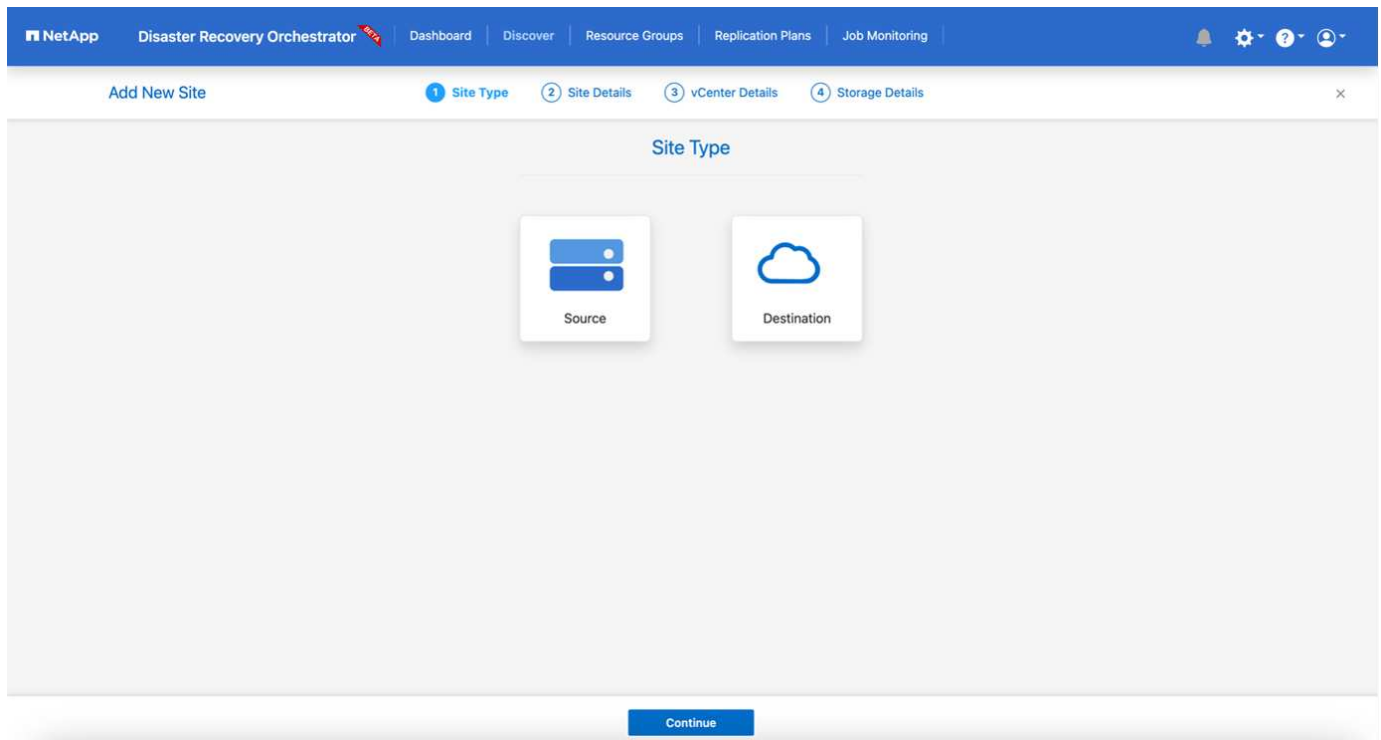
DRO configuration

After FSx for ONTAP and VMC have been configured properly, you can begin configuring DRO to automate the recovery of on-premises workloads to VMC by using the read-only SnapMirror copies on FSx for ONTAP.

NetApp recommends deploying the DRO agent in AWS and also to the same VPC where FSx for ONTAP is deployed (it can be peer connected too), so that the DRO agent can communicate through the network with your on-premises components as well as with the FSx for ONTAP and VMC resources.

The first step is to discover and add the on-premises and cloud resources (both vCenter and storage) to DRO. Open DRO in a supported browser and use the default username and password (admin/admin) and Add Sites. Sites can also be added using the Discover option. Add the following platforms:

- On-premises
 - On-premises vCenter
 - ONTAP storage system
- Cloud
 - VMC vCenter
 - FSx for ONTAP



Once added, DRO performs automatic discovery and displays the VMs that have corresponding SnapMirror replicas from the source storage to FSx for ONTAP. DRO automatically detects the networks and portgroups used by the VMs and populates them.

NetApp Disaster Recovery Orchestrator Dashboard Discover Resource Groups Replication Plans Job Monitoring

Back VM List Site: On Prem | vCenter: 172.21.253.160

10 Datastores 219 Virtual Machines

VM Protection 3 Protected 216 Unprotected

38 VMs Create Resource Group

VM Name	VM Status	VM State (1)	DataStore	CPU	Memory (MB)
a300-vcsa02	Not Protected	Powered On	A300_NFS_DS04	16	65536
PFSense	Not Protected	Powered On	A300_NFS_DS04	4	8192
PFSense260	Not Protected	Powered On	A300_NFS_DS04	4	16384
NimDC02	Not Protected	Powered On	A300_NFS_DS04	4	8192
jRBhoja-187	Not Protected	Powered On	A300_NFS_DS04	4	16384
jNimo-187	Not Protected	Powered On	A300_NFS_DS04	4	16384
NimMSDesktop	Not Protected	Powered On	A300_NFS_DS04	8	12288

The next step is to group the required VMs into functional groups to serve as resource groups.

Resource groupings

After the platforms have been added, you can group the VMs you want to recover into resource groups. DRO resource groups allow you to group a set of dependent VMs into logical groups that contain their boot orders, boot delays, and optional application validations that can be executed upon recovery.

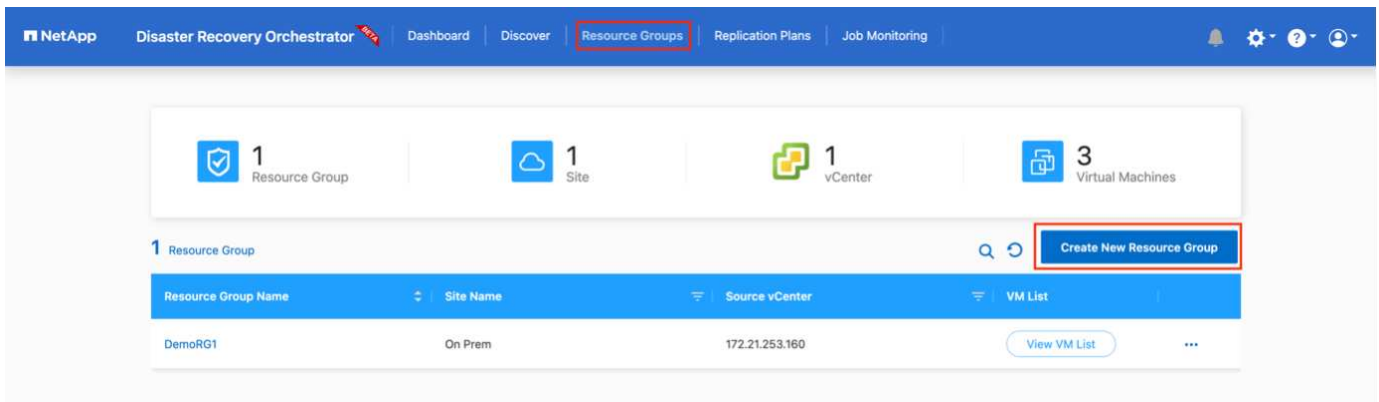
To start creating resource groups, complete the following steps:

1. Access **Resource Groups**, and click **Create New Resource Group**.
2. Under **New resource group**, select the source site from the dropdown and click **Create**.
3. Provide **Resource Group Details** and click **Continue**.
4. Select the appropriate VMs using the search option.
5. Select the boot order and boot delay (secs) for the selected VMs. Set the order of the power-on sequence by selecting each VM and setting up the priority for it. Three is the default value for all VMs.

Options are as follows:

- 1 – The first virtual machine to power on
- 3 – Default
- 5 – The last virtual machine to power on

6. Click **Create Resource Group**.

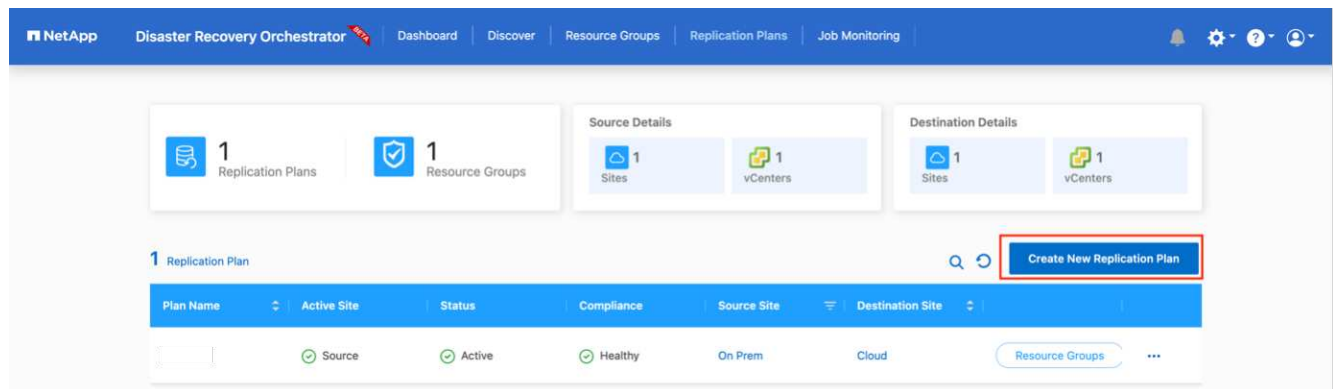


Replication plans

You need a plan to recover applications in the event of a disaster. Select the source and destination vCenter platforms from the drop down and pick the resource groups to be included in this plan, along with the grouping of how applications should be restored and powered on (for example, domain controllers, then tier-1, then tier-2, and so on). Such plans are sometimes also called blueprints. To define the recovery plan, navigate to the **Replication Plan** tab and click **New Replication Plan**.

To start creating a replication plan, complete the following steps:

1. Access **Replication Plans**, and click **Create New Replication Plan**.



2. Under **New Replication Plan**, provide a name for the plan and add recovery mappings by selecting the source site, associated vCenter, destination site, and associated vCenter.

NetApp Disaster Recovery Orchestrator | Dashboard | Discover | Resource Groups | **Replication Plans** | Job Monitoring

Create New Replication Plan | 1 Replication Plan and Site Details | 2 Select Resource Groups | 3 Set Execution Order | 4 Set VM Details

Replication Plan Details

Plan Name

Recovery Mapping

Source Site Destination Site

Source vCenter Destination vCenter

! Pre-requisite - You must configure SnapMirror relationships between the source site and target site to create successful replication plan

[Continue](#)

3. After Recovery mapping is completed, select the cluster mapping.

NetApp Disaster Recovery Orchestrator | Dashboard | Discover | Resource Groups | **Replication Plans** | Job Monitoring

Create New Replication Plan | 1 Replication Plan and Site Details | 2 Select Resource Groups | 3 Set Execution Order | 4 Set VM Details

Replication Plan Details

Plan Name

Recovery Mapping

Source Site Destination Site

Source vCenter Destination vCenter

Cluster Mapping

Source Site Resource Destination Site Resource [Add](#)

Source Resource	Destination Resource	
A300-Cluster01	Cluster-1	Delete

[Continue](#)

4. Select **Resource Group Details** and click **Continue**.
5. Set the execution order for the resource group. This option enables you to select the sequence of operations when multiple resource groups exist.
6. After you are done, select the network mapping to the appropriate segment. The segments should already be provisioned within VMC, so select the appropriate segment to map the VM.
7. Based on the selection of VMs, datastore mappings are automatically selected.



SnapMirror is at the volume level. Therefore, all VMs are replicated to the replication destination. Make sure to select all VMs that are part of the datastore. If they are not selected, only the VMs that are part of the replication plan are processed.

NetApp Disaster Recovery Orchestrator

Create New Replication Plan

Replication Plan and Site Details

Select Resource Groups

Set Execution Order

Set VM Details

Replication Plan Details

Select Execution Order

Resource Group Name	Execution Order
DemoRG1	3

Network Mapping

No more Source/Destination network resources available for mapping

Source Resource	Destination Resource	
VLAN 3375	sddc-cgw-network-1	Delete

DataStore Mapping

Source DataStore	Destination Volume
DRO_Mini	DRO_Mini_copy

Previous Continue

- Under the VM details, you can optionally resize the VM's CPU and RAM parameters; this can be very helpful when recovering large environments to smaller target clusters or for conducting DR tests without having to provision a one-to-one physical VMware infrastructure. Also, you can modify the boot order and boot delay (seconds) for all the selected VMs across the resource groups. There is an additional option to modify the boot order if there are any changes required from those selected during the resource-group boot-order selection. By default, the boot order selected during resource-group selection is used; however, any modifications can be performed at this stage.

NetApp Disaster Recovery Orchestrator

Create New Replication Plan

Replication Plan and Site Details

Select Resource Groups

Set Execution Order

Set VM Details

VM Details

3 VMs

VM Name	No. of CPUs	Memory (MB)	NIC/IP	Boot Order	Override
Resource Group : DemoRG1					
Mini_Test01	1	2048	<input type="radio"/> Static <input checked="" type="radio"/> Dynamic	3	
Mini_Test02	1	2048	<input type="radio"/> Static <input checked="" type="radio"/> Dynamic	2	
Mini_Test03	1	2048	<input type="radio"/> Static <input checked="" type="radio"/> Dynamic	1	

Previous Create Replication Plan

9. Click **Create Replication Plan**.

NetApp Disaster Recovery Orchestrator

Dashboard Discover Resource Groups **Replication Plans** Job Monitoring

2 Replication Plans 1 Resource Groups

Source Details: 1 Sites 1 vCenters

Destination Details: 1 Sites 1 vCenters

2 Replication Plans

Plan Name	Active Site	Status	Compliance	Source Site	Destination Site	
DemoRP	Source	Active	Not Available	On Prem	Cloud	Resource Groups ...
DemoRP	Source	Active	Healthy	On Prem	Cloud	Resource Groups ...

After the replication plan is created, the failover option, the test-failover option, or the migrate option can be exercised depending on the requirements. During the failover and test-failover options, the most recent SnapMirror Snapshot copy is used, or a specific Snapshot copy can be selected from a point-in-time Snapshot copy (per the retention policy of SnapMirror). The point-in-time option can be very helpful if you are facing a corruption event like ransomware, where the most recent replicas are already compromised or encrypted. DRO shows all available points in time. To trigger failover or test failover with the configuration specified in the replication plan, you can click **Failover** or **Test failover**.

NetApp Disaster Recovery Orchestrator

Dashboard Discover Resource Groups Replication Plans Job Monitoring

2 Replication Plans 1 Resource Groups

Source Details: 1 Sites 1 vCenters

Destination Details: 1 Sites 1 vCenters

2 Replication Plans

Plan Name	Active Site	Status	Compliance	Source Site	Destination Site	
DemoRP	Source	Active	Healthy	On Prem	Cloud	Resource Groups ...
DemoRP	Source	Active	Healthy	On Prem	Cloud	Resource Groups ...

- Plan Details
- Edit Plan
- Failover**
- Test Failover
- Migrate
- Run Compliance
- Delete Plan

Failover Details



Volume Snapshot Details

- ☒ Use latest snapshot ⓘ
- ☐ Select specific snapshot ⓘ

Start Failover

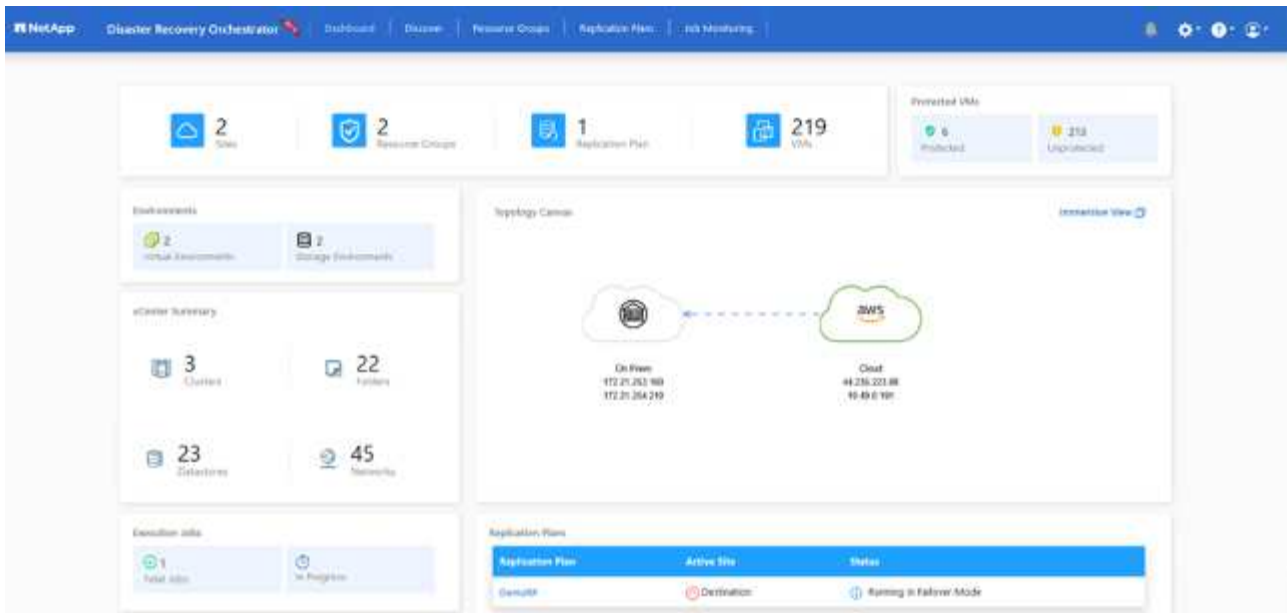
The replication plan can be monitored in the task menu:

The screenshot shows the NetApp Disaster Recovery Orchestrator interface. The top navigation bar includes the NetApp logo, the title "Disaster Recovery Orchestrator", and several menu items: Dashboard, Discover, Resource Groups, Replication Plans, and Job Monitoring (which is highlighted with a red box). On the right side of the navigation bar are icons for notifications, settings, help, and user profile.

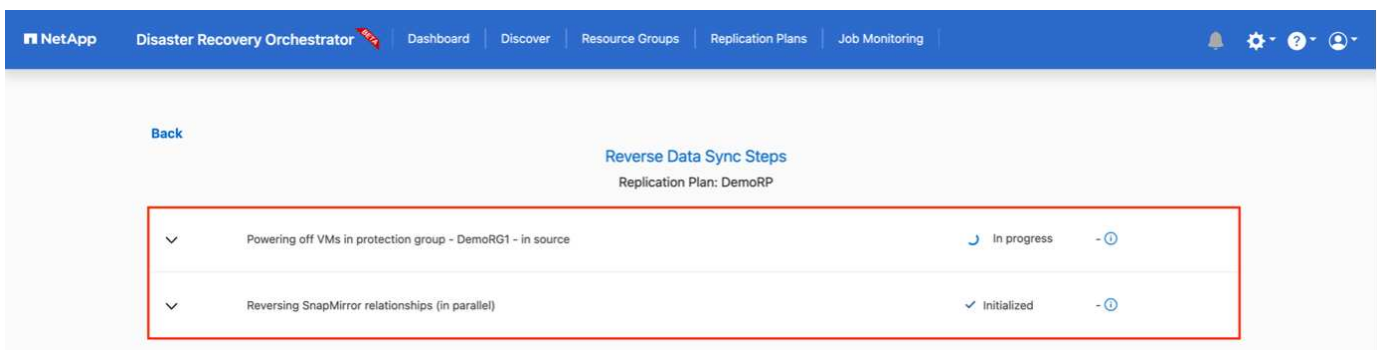
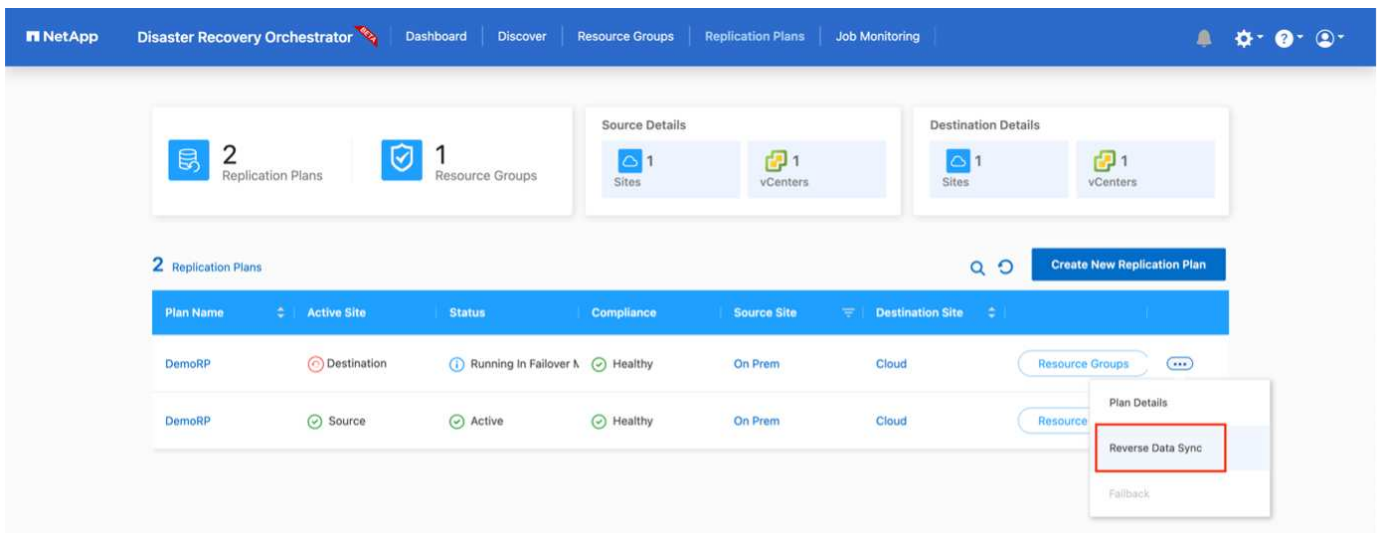
Below the navigation bar, the main content area displays the "Failover Steps" for "Replication Plan: DemoRP". A "Back" link is visible on the left. The steps are listed in a table with expandable rows (indicated by a downward arrow icon on the left of each row). Each row shows the step name, its status (all are "Success" with a green checkmark icon), and the duration. A red box highlights the "Failover Steps" header and the "Replication Plan: DemoRP" text.

Step	Status	Duration
Breaking SnapMirror relationships (in parallel)	Success	11.3 Seconds ⓘ
Mounting volumes and creating datastores (in parallel)	Success	34.7 Seconds ⓘ
Registering VMs (in parallel)	Success	13.2 Seconds ⓘ
Powering on VMs in protection group - DemoRG1 - in target	Success	95.8 Seconds ⓘ
Updating replication status	Success	0.5 Seconds ⓘ

After failover is triggered, the recovered items can be seen in the VMC vCenter (VMs, networks, datastores). By default, the VMs are recovered to the Workload folder.



Failback can be triggered at the replication-plan level. For a test failover, the tear-down option can be used to roll back the changes and remove the FlexClone relationship. Failback related to failover is a two-step process. Select the replication plan and select **Reverse data sync**.



Once completed, you can trigger failback to move back to original production site.

NetApp Disaster Recovery Orchestrator

Dashboard | Discover | Resource Groups | Replication Plans | Job Monitoring

2 Replication Plans

1 Resource Groups

Source Details: 1 Sites, 1 vCenters

Destination Details: 1 Sites, 1 vCenters

Plan Name	Active Site	Status	Compliance	Source Site	Destination Site
DemoRP	Destination	Active	Healthy	On Prem	Cloud
DemoRP	Source	Active	Healthy	On Prem	Cloud

Failback

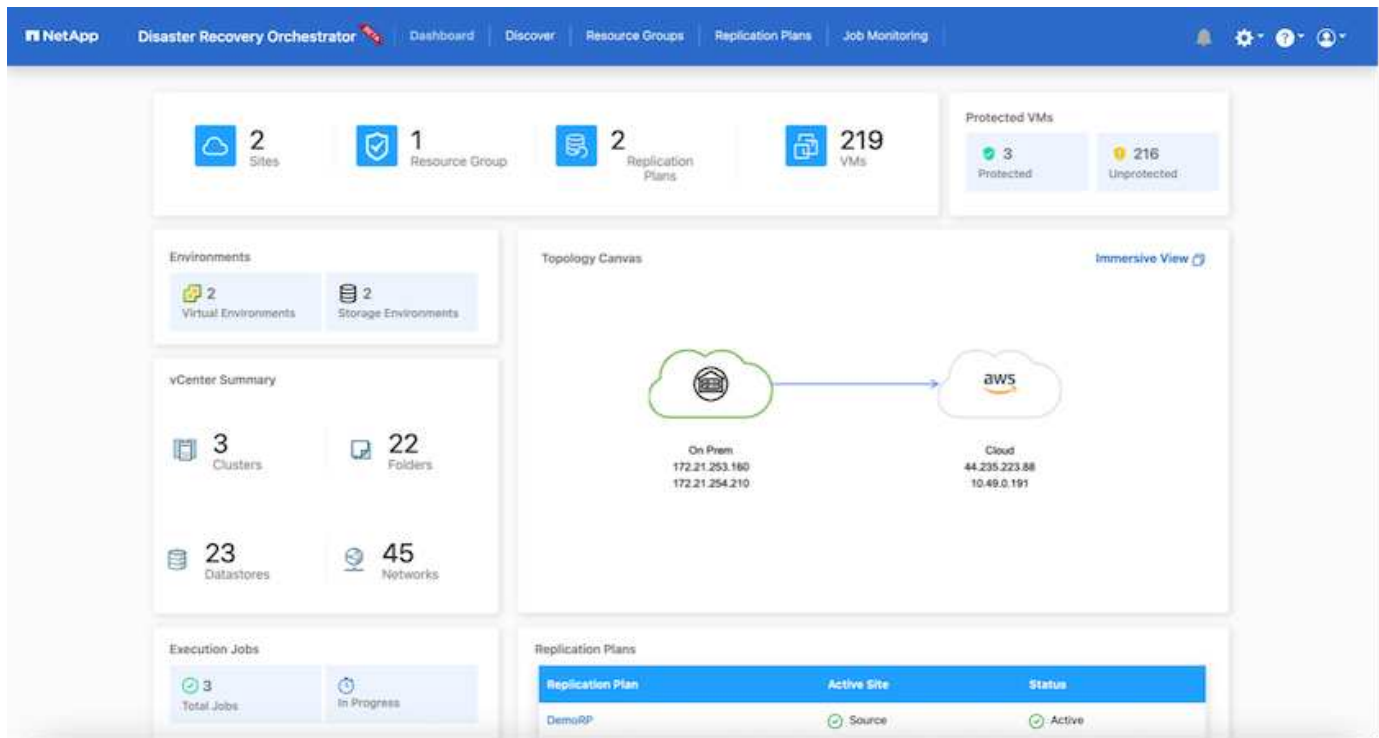
Back

Failback Steps

Replication Plan: DemoRP

Powering off VMs in protection group - DemoRG1 - in target	In progress	- ①
Unregistering VMs in target (in parallel)	Initialized	- ①
Unmounting volumes in target (in parallel)	Initialized	- ①
Breaking reverse SnapMirror relationships (in parallel)	Initialized	- ①
Updating VM networks (in parallel)	Initialized	- ①
Powering on VMs in protection group - DemoRG1 - in source	Initialized	- ①
Deleting reverse SnapMirror relationships (in parallel)	Initialized	- ①
Resuming SnapMirror relationships to target (in parallel)	Initialized	- ①

From NetApp BlueXP, we can see that replication health has broken off for the appropriate volumes (those that were mapped to VMC as read-write volumes). During test failover, DRO does not map the destination or replica volume. Instead, it makes a FlexClone copy of the required SnapMirror (or Snapshot) instance and exposes the FlexClone instance, which does not consume additional physical capacity for FSx for ONTAP. This process makes sure that the volume is not modified and replica jobs can continue even during DR tests or triage workflows. Additionally, this process makes sure that, if errors occur or corrupted data is recovered, the recovery can be cleaned up without the risk of the replica being destroyed.



Ransomware recovery

Recovering from ransomware can be a daunting task. Specifically, it can be hard for IT organizations to pinpoint where the safe point of return is and, once that is determined, to protect recovered workloads from reoccurring attacks from, for example, sleeping malware or vulnerable applications.

DRO addresses these concerns by enabling you to recover your system from any available point in time. You can also recover workloads to functional and yet isolated networks so that applications can function and communicate with each other in a location where they are not exposed to north-south traffic. This gives your security team a safe place to conduct forensics and make sure there is no hidden or sleeping malware.

Benefits

- Use of the efficient and resilient SnapMirror replication.
- Recovery to any available point in time with Snapshot copy retention.
- Full automation of all required steps to recover hundreds to thousands of VMs from the storage, compute, network, and application validation steps.
- Workload recovery with ONTAP FlexClone technology using a method that doesn't change the replicated volume.
 - Avoids risk of data corruption for volumes or Snapshot copies.
 - Avoids replication interruptions during DR test workflows.
 - Potential use of DR data with cloud computing resources for workflows beyond DR such as DevTest, security testing, patch or upgrade testing, and remediation testing.
- CPU and RAM optimization to help lower cloud costs by allowing recovery to smaller compute clusters.

Using Veeam Replication and FSx for ONTAP for Disaster recovery to VMware Cloud on AWS

Author: Niyaz Mohamed - NetApp Solutions Engineering

Overview

Amazon FSx for NetApp ONTAP integration with VMware Cloud on AWS is an AWS-managed external NFS datastore built on NetApp's ONTAP file system that can be attached to a cluster in the SDDC. It provides customers with flexible, high-performance virtualized storage infrastructure that scales independently of compute resources.

For those customers looking to use VMware Cloud on AWS SDDC as the disaster recovery target, FSx for ONTAP datastores can be used to replicate data from on-premises using any validated third-party solution that provides VM replication capability. By adding FSx for ONTAP datastore, it will enable cost optimised deployment than building VMware cloud on AWS SDDC with enormous amount of ESXi hosts just to accommodate the storage.

This approach also helps customers to use pilot light cluster in VMC along with FSx for ONTAP datastores to host the VM replicas. The same process can also be extended as a migration option to VMware Cloud on AWS by gracefully failing over the replication plan.

Problem Statement

This document describes how to use FSx for ONTAP datastore and Veeam Backup and replication to set up disaster recovery for on-premises VMware VMs to VMware Cloud on AWS using the VM replication functionality.

Veeam Backup & Replication allows onsite and remote replication for disaster recovery (DR). When virtual machines are replicated, Veeam Backup & Replication creates an exact copy of the VMs in the native VMware vSphere format on the target VMware Cloud on AWS SDDC cluster and keeps the copy synchronized with the original VM.

Replication provides the best recovery time objective (RTO) values as there is a copy of a VM in the ready-to-start state. This replication mechanism ensures that the workloads can quickly start in VMware Cloud on AWS SDDC in case of a disaster event. The Veeam Backup & Replication software also optimizes traffic transmission for replication over WAN and slow connections. In addition, it also filters out duplicate data blocks, zero data blocks, swap files and excluded VM guest OS files, and compresses the replica traffic.

To prevent replication jobs from consuming the entire network bandwidth, WAN accelerators and network throttling rules can be put in place. The replication process in Veeam Backup & Replication is job driven which means replication is performed by configuring replication jobs. In case of a disaster event, failover can be triggered to recover the VMs by failing over to its replica copy.

When failover is performed, a replicated VM takes over the role of the original VM. Fail over can be performed to the latest state of a replica or to any of its good known restore points. This enables ransomware recovery or isolated testing as needed. In Veeam Backup & Replication, failover and failback are temporary intermediate step that should be further finalized. Veeam Backup & Replication offers multiple options to handle different disaster recovery scenarios.

[Diagram of DR scenario using Veeam Replication and FSx ONTAP for VMC]

Solution Deployment

High level steps

1. Veeam Backup and Replication software is running in on-premises environment with appropriate network connectivity.
2. Configure VMware Cloud on AWS, see the VMware Cloud Tech Zone article [VMware Cloud on AWS integration with Amazon FSx for NetApp ONTAP Deployment Guide](#) to deploy, configure VMware Cloud on AWS SDDC and FSx for ONTAP as NFS datastore. (A pilot-light environment set up with a minimal configuration can be used for DR purposes. VMs will fail over to this cluster in the event of an incident, and additional nodes can be added).
3. Set up replication jobs to create VM replicas using Veeam Backup and Replication.
4. Create failover plan and perform failover.
5. Switch back to production VMs once the disaster event is complete and primary site is Up.

Pre-requisites for Veeam VM Replication to VMC and FSx for ONTAP datastores

1. Ensure Veeam Backup & Replication backup VM is connected to the source vCenter as well as the target VMware cloud on AWS SDDC clusters.
2. The backup server must be able to resolve short names and connect to source and target vCenters.
3. The target FSx for ONTAP datastore must have enough free space to store VMDKs of replicated VMs

For additional information, refer to "Considerations and Limitations" covered [here](#).

Deployment Details

Step 1: Replicate VMs

Veeam Backup & Replication leverages VMware vSphere snapshot capabilities and during replication, Veeam Backup & Replication requests VMware vSphere to create a VM snapshot. The VM snapshot is the point-in-time copy of a VM that includes virtual disks, system state, configuration and so on. Veeam Backup & Replication uses the snapshot as a source of data for replication.

To replicate VMs, follow the below steps:

1. Open the Veeam Backup & Replication Console.
2. On the Home view, select Replication Job > Virtual machine > VMware vSphere.
3. Specify a job name and select the appropriate advanced control checkbox. Click Next.
 - Select the Replica seeding check box if connectivity between on-premises and AWS has restricted bandwidth.
 - Select the Network remapping (for AWS VMC sites with different networks) check box if segments on VMware Cloud on AWS SDDC do not match that of on-premises site networks.
 - If the IP addressing scheme in on-premises production site differs from the scheme in the AWS VMC site, select the Replica re-IP (for DR sites with different IP addressing scheme) check box.

[dr veeam fsx image2] | *dr-veeam-fsx-image2.png*

4. Select the VMs that need to be replicated to FSx for ONTAP datastore attached to VMware Cloud on AWS SDDC in the **Virtual Machines** step. The Virtual machines can be placed on vSAN to fill the available vSAN datastore capacity. In a pilot light cluster, the usable capacity of a 3-node cluster will be limited. The rest of the data can be replicated to FSx for ONTAP datastores. Click **Add**, then in the **Add Object** window select the necessary VMs or VM containers and click **Add**. Click **Next**.

[dr veeam fsx image3] | *dr-veeam-fsx-image3.png*

5. After that, select the destination as VMware Cloud on AWS SDDC cluster / host and the appropriate resource pool, VM folder and FSx for ONTAP datastore for VM replicas. Then Click **Next**.

[dr veeam fsx image4] | *dr-veeam-fsx-image4.png*

6. In the next step, create the mapping between source and destination virtual network as needed.

[dr veeam fsx image5] | *dr-veeam-fsx-image5.png*

7. In the **Job Settings** step, specify the backup repository that will store metadata for VM replicas, retention policy and so on.
8. Update the **Source** and **Target** proxy servers in the **Data Transfer** step and leave **Automatic** selection (default) and keep **Direct** option selected and click **Next**.
9. At the **Guest Processing** step, select **Enable application-aware processing** option as needed. Click **Next**.

[dr veeam fsx image6] | *dr-veeam-fsx-image6.png*

10. Choose the replication schedule to run the replication job to run on a regular basis.
11. At the **Summary** step of the wizard, review details of the replication job. To start the job right after the wizard is closed, select the **Run the job when I click Finish** check box, otherwise leave the check box unselected. Then click **Finish** to close the wizard.

[dr veeam fsx image7] | *dr-veeam-fsx-image7.png*

Once the replication job starts, the VMs with the suffix specified will be populated on the destination VMC SDDC cluster / host.

[dr veeam fsx image8] | *dr-veeam-fsx-image8.png*

For additional information for Veeam replication, refer to [How Replication Works](#).

Step 2: Create a failover plan

When the initial replication or seeding is complete, create the failover plan. Failover plan helps in performing failover for dependent VMs one by one or as a group automatically. Failover plan is the blueprint for the order in which the VMs are processed including the boot delays. The failover plan also helps to ensure that critical dependant VMs are already running.

To create the plan, navigate to the new sub section called Replicas and select Failover Plan. Choose the appropriate VMs. Veeam Backup & Replication will look for the closest restore points to this point in time and use them to start VM replicas.



The failover plan can only be added once the initial replication is complete and the VM replicas are in Ready state.



The maximum number of VMs that can be started simultaneously when running a failover plan is 10.



During the failover process, the source VMs will not be powered off.

To create the **Failover Plan**, do the following:

1. On the Home view, select **Failover Plan > VMware vSphere**.
2. Next, provide a name and a description to the plan. Pre and Post-failover script can be added as required. For instance, run a script to shutdown VMs before starting the replicated VMs.

[dr veeam fsx image9] | *dr-veeam-fsx-image9.png*

3. Add the VMs to the plan and modify the VM boot order and boot delays to meet the application dependencies.

[dr veeam fsx image10] | *dr-veeam-fsx-image10.png*

For additional information for creating replication jobs, refer [Creating Replication Jobs](#).

Step 3: Run the failover plan

During failover, the source VM in the production site is switched over to its replica at the disaster recovery site. As part of the failover process, Veeam Backup & Replication restores the VM replica to the required restore point and moves all I/O activities from the source VM to its replica. Replicas can be used not only in case of a disaster, but also to simulate DR drills. During failover simulation, the source VM remains running. Once all the necessary tests have been conducted, you can undo the failover and return to normal operations.



Make sure network segmentation is in place to avoid IP conflicts during DR drills.

To start the failover plan, simply click in **Failover Plans** tab and right click on the failover plan. Select **Start**. This will failover using the latest restore points of VM replicas. To fail over to specific restore points of VM replicas, select **Start to**.

[dr veeam fsx image11] | *dr-veeam-fsx-image11.png*

[dr veeam fsx image12] | *dr-veeam-fsx-image12.png*

The state of the VM replica changes from Ready to Failover and VMs will start on the destination VMware Cloud on AWS SDDC cluster / host.

[dr veeam fsx image13] | *dr-veeam-fsx-image13.png*

Once the failover is complete, the status of the VMs will change to “Failover”.

[dr veeam fsx image14] | *dr-veeam-fsx-image14.png*



Veeam Backup & Replication stops all replication activities for the source VM until its replica is returned to the Ready state.

For detailed information about failover plans, refer to [Failover Plans](#).

Step 4: Failback to the Production site

When the failover plan is running, it is considered as an intermediate step and needs to be finalized based on the requirement. The options include the following:

- **Failback to production** - switch back to the original VM and transfer all changes that took place while the VM replica was running to the original VM.



When you perform failback, changes are only transferred but not published. Choose **Commit failback** (once the original VM is confirmed to work as expected) or **Undo failback** to get back to the VM replica If the original VM is not working as expected.

- **Undo failover** - switch back to the original VM and discard all changes made to the VM replica while it was running.
- **Permanent Failover** - permanently switch from the original VM to a VM replica and use this replica as the original VM.

In this demo, Failback to production was chosen. Failback to the original VM was selected during the Destination step of the wizard and “Power on VM after restoring” check box was enabled.

[dr veeam fsx image15] | *dr-veeam-fsx-image15.png*

[dr veeam fsx image16] | *dr-veeam-fsx-image16.png*

Failback commit is one of the ways to finalize failback operation. When failback is committed, it confirms that the changes sent to the VM which is failed back (the production VM) are working as expected. After the commit operation, Veeam Backup & Replication resumes replication activities for the production VM.

For detailed information about the failback process, refer Veeam documentation for [Failover and Failback for replication](#).

[dr veeam fsx image17] | *dr-veeam-fsx-image17.png*

[dr veeam fsx image18] | *dr-veeam-fsx-image18.png*

After failback to production is successful, the VMs are all restored back to the original production site.

[dr veeam fsx image19] | *dr-veeam-fsx-image19.png*

Conclusion

FSx for ONTAP datastore capability enables Veeam or any validated third-party tool to provide low-cost DR solution using Pilot light cluster and without standing up large number of hosts in the cluster just to accommodate the VM replica copy. This provides a powerful solution to handle a tailored, customized disaster recovery plan and also allows to reuse existing backup products in house to meet the DR needs, thus enabling cloud-based disaster recovery by exiting DR datacentres on-premises. Failover can be done as planned failover or failover with a click of a button when disaster occurs, and decision is made to activate the DR site.

To learn more about this process, feel free to follow the detailed walkthrough video.

<https://netapp.hosted.panopto.com/Panopto/Pages/Embed.aspx?id=15fed205-8614-4ef7-b2d0-b061015e925a>

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.