



## **NetApp for AWS / VMC**

### NetApp Solutions

NetApp  
February 20, 2023

# Table of Contents

|  |     |
|--|-----|
| NetApp Hybrid Multicloud Solutions for AWS / VMC .....         | 1   |
| Protecting Workloads .....                                     | 1   |
| Migrating Workloads .....                                      | 84  |
| Region Availability – Supplemental NFS datastore for VMC ..... | 102 |

# NetApp Hybrid Multicloud Solutions for AWS / VMC

## Protecting Workloads

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

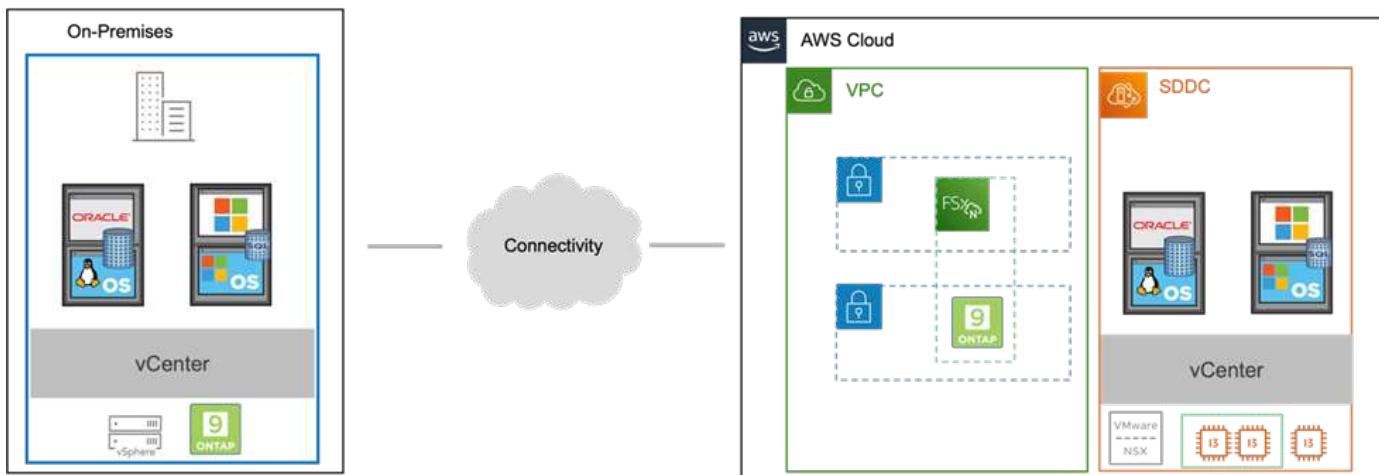
Authors: Chris Reno, Josh Powell, and Suresh Thoppay - NetApp Solutions Engineering

#### 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                           | Thru |
|-----------------|--------|------------|---------|---------------|--------------|--------------|---------|--------------------|--------------------------------|------|
| 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_svm_614 | ✓      | ora_svm    | 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
      Logical      Status      Network          Current      Current Is
Vserver     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-addrs  
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.

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 1
- 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

2

### Cluster Peers

PEERED CLUSTER NAME

- ✓ Fsxl0ae40e08acc0dea67
- ✓ OTS02

3

Peer Cluster

Generate Passphrase

Manage Cluster Peers

Mediator ②

Not configured.

Configure

Storage VM Peers

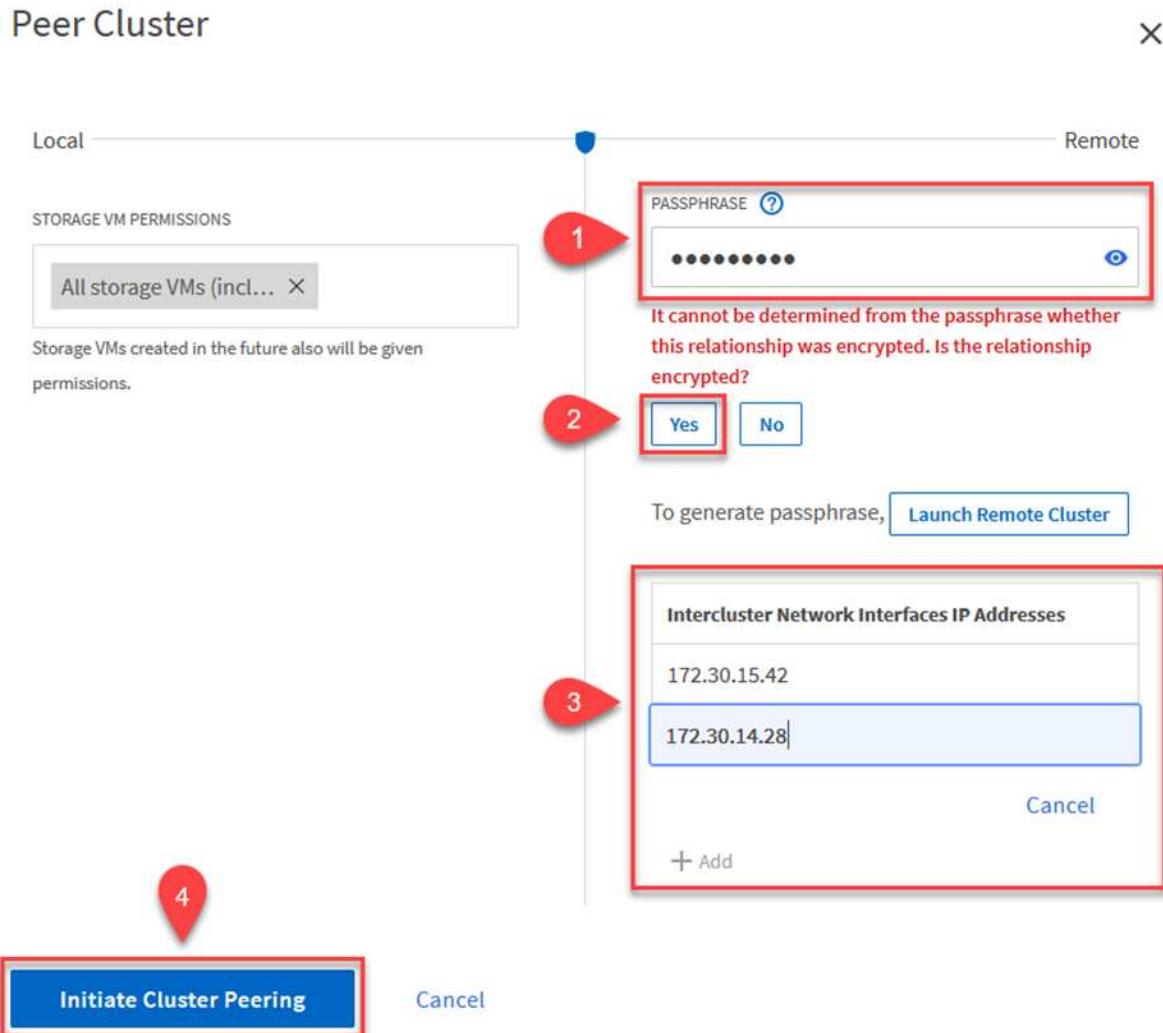
PEERED STORAGE VMs

3

3. In the Peer Cluster dialog box, fill out the required information:

- Enter the passphrase that was used to establish the peer cluster relationship on the destination FSx cluster.
- Select Yes to establish an encrypted relationship.
- Enter the intercluster LIF IP address(es) of the destination FSx cluster.

- d. Click Initiate Cluster Peering to finalize the process.



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
-----
```

| Peer Cluster Name | Cluster Serial Number | Availability | Authentication |
|-------------------|-----------------------|--------------|----------------|
| E13A300           | 1-80-000011           | Available    | ok             |

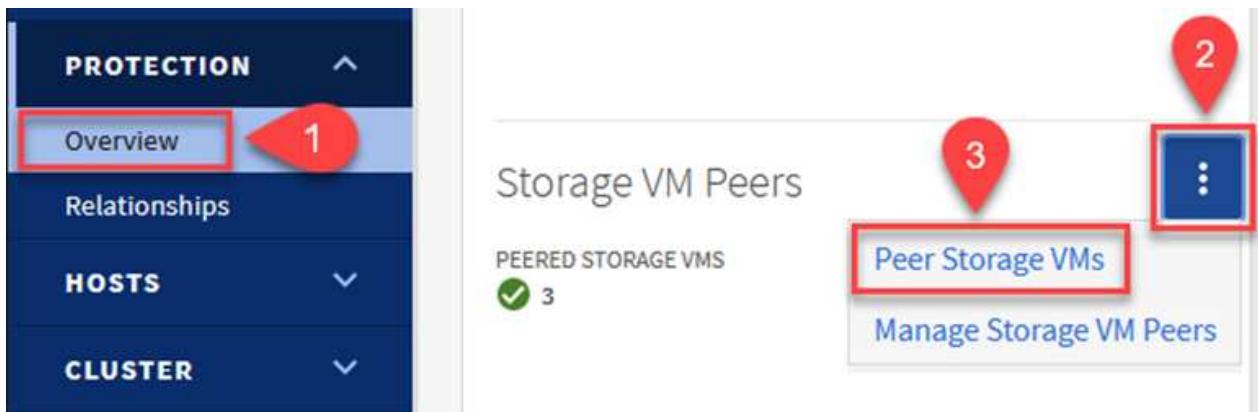
## Establish SVM peering relationship

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.

To create a volume, run the following command on FSx ONTAP:

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

## 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 interface. On the left is a navigation sidebar with icons for Dashboard, Resources, Monitor, Reports, Hosts, Storage Systems (which is selected), Settings, and Alerts. The main content area is titled 'ONTAP Storage' and shows 'ONTAP Storage Connections'. A dropdown menu indicates the type is 'ONTAP SVMs'. There is a search bar labeled 'Search by Name'. In the top right, there are icons for notifications, email, help, user scadmin, and sign out. A prominent red box highlights the 'New' button, which has a blue plus sign icon. Below the header is a table with columns: Name, IP, Cluster Name, User Name, Platform, and Controller License. The table lists several SVM connections, each with a checkbox in the first column and a link in the 'Name' column.

|                          | Name                         | IP           | Cluster Name | User Name | Platform | Controller License |
|--------------------------|------------------------------|--------------|--------------|-----------|----------|--------------------|
| <input type="checkbox"/> | <a href="#">Backup</a>       | 172.16.13.17 | 172.16.13.17 |           | AFF      | ✓                  |
| <input type="checkbox"/> | <a href="#">FS02</a>         | 172.16.13.17 | 172.16.13.17 |           | AFF      | ✓                  |
| <input type="checkbox"/> | <a href="#">ora_svm</a>      | 172.16.13.17 | 172.16.13.17 |           | AFF      | ✓                  |
| <input type="checkbox"/> | <a href="#">ora_svm_dest</a> |              | 172.30.15.42 |           | AFF      | Not applicable     |
| <input type="checkbox"/> | <a href="#">sql_svm</a>      | 172.16.13.17 | 172.16.13.17 |           | AFF      | ✓                  |
| <input type="checkbox"/> | <a href="#">sql_svm_dest</a> |              | 172.30.15.42 |           | AFF      | Not applicable     |
| <input type="checkbox"/> | <a href="#">svm_HCapps</a>   |              | 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 i

Storage System

Username

Password

#### Event Management System (EMS) & AutoSupport Settings

Send AutoSupport notification to storage system

Log SnapCenter Server events to syslog

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

**Submit**

**Cancel**

**Reset**

3. 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

X

|                                       |                |  |
|---------------------------------------|----------------|--|
| Platform                              | FAS            | <input checked="" type="checkbox"/> Secondary <span>i</span> |
| Protocol                              | HTTPS          |  |
| Port                                  | 443            |  |
| Timeout                               | 60             | seconds <span>i</span>                                       |
| <input type="checkbox"/> Preferred IP | <span>i</span> |  |

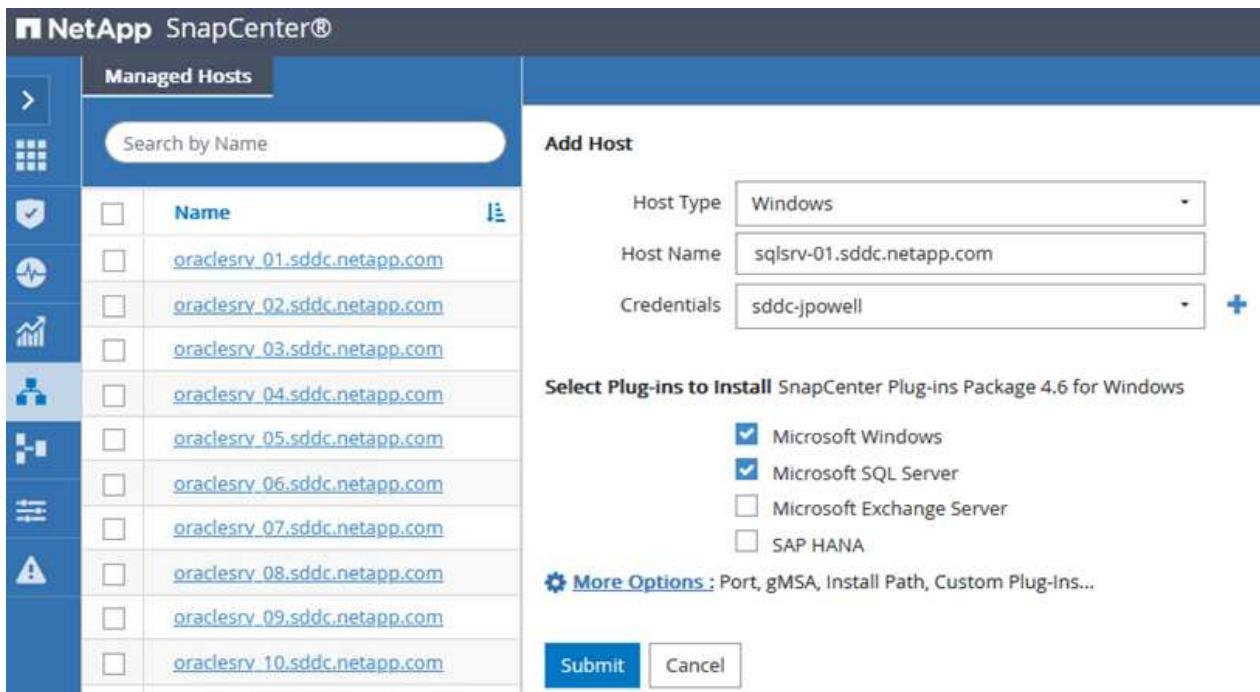
Save Cancel

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.



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.



| Name            | Backup Type         | Schedule Type | Replication |
|-----------------|---------------------|---------------|-------------|
| SQL-Daily       | Full and Log backup | Daily         | SnapVault   |
| SQL-Hourly      | Full and Log backup | Hourly        | SnapVault   |
| SQL-Hourly-Logs | Log backup          | Hourly        | SnapVault   |
| SQL-OnDemand    | Full and Log backup | On demand     | SnapVault   |
| SQL-Weekly      | Full and Log backup | Weekly        | SnapVault   |

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 i

Update SnapMirror after creating a local Snapshot copy.

Update SnapVault after creating a local Snapshot copy.

Secondary policy label

Choose i

Error retry count

3 i

## 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.

The screenshot shows the NetApp SnapCenter interface. On the left, a sidebar lists navigation options: Dashboard, Resources (which is selected and highlighted in blue), Monitor, Reports, Hosts, Storage Systems, Settings, and Alerts. The main content area has a header with 'Microsoft SQL Server' and a dropdown menu, with a red box and the number '1' highlighting the dropdown. Below the header is a search bar labeled 'search by name'. To the right of the search bar is a large red box with the number '2' containing a blue '+' icon and the text 'New Resource Group'. The main table displays three resource groups: SQLSRV-01, SQLSRV-02, and SQLSRV-03. Each row includes columns for Name, Resource Count, Tags, Policies, Last Backup, and Overall Status. The data for each row is as follows:

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

X

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

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

< Previous **Next >** Finish Cancel

4. Add your credentials to access the ONTAP cluster.

## New NetApp Data ONTAP Storage

X

**Credentials**  
Specify account with storage administrator privileges.

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

< Previous **Next >** Finish Cancel

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

## New NetApp Data ONTAP Storage

X


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

|                  |   |  |   |   |
|------------------|---|--|---|---|
| Name             | Protocol to use:  |  |   |   |
|                  | <input checked="" type="checkbox"/> SMB<br><input type="checkbox"/> NFS<br><input checked="" type="checkbox"/> Create required export rules automatically               |  |   |   |
| Credentials      |   |  |   |   |
| <b>NAS Filer</b> |   |  |   |   |
| Apply            |   |  |   |   |
| Summary          |   |  |   |   |
|                  | Volumes to scan:<br><input type="text" value="All volumes"/> <span style="border: 1px solid #ccc; padding: 2px 10px; margin-left: 10px;">Choose...</span>               |  |   |   |
|                  | Backup proxies to use:<br><input type="text" value="Automatic selection"/> <span style="border: 1px solid #ccc; padding: 2px 10px; margin-left: 10px;">Choose...</span> |  |   |   |
|                  | <a href="#" style="border: 1px solid #ccc; padding: 2px 10px;">&lt; Previous</a>  | <a href="#" style="border: 1px solid #0070C0; background-color: #0070C0; color: white; padding: 2px 10px;">Apply</a> | <a href="#" style="border: 1px solid #ccc; padding: 2px 10px;">Finish</a> | <a href="#" style="border: 1px solid #ccc; padding: 2px 10px;">Cancel</a> |

6. 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.



7. 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

X



### 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:<br><input type="text" value="\\172.21.162.181\VBRRepo"/> <a href="#">Browse...</a>  |
| Share        | <input checked="" type="checkbox"/> This share requires access credentials:<br><input type="button" value="sddc\administrator (sddc\administrator, last edited: 85 days ago)"/> <a href="#">Add...</a> <a href="#">Manage accounts</a> |
| Repository   | Gateway server:  |
| Mount Server | <input checked="" type="radio"/> Automatic selection   |
| Review       | <input type="radio"/> The following server:<br><input type="button" value="veeam.sddc.netapp.com (Backup 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:<br>AKIAJX4H4ZT557HXQT2W (last edited: 107 days ago) <input type="button" value="Add..."/> <a href="#">Manage cloud accounts</a>                       |
| Account | AWS region:<br><input type="button" value="Global"/>   |
| Bucket  | <input type="checkbox"/> Use the following gateway server:<br><input type="button" value="veeam.sddc.netapp.com (Backup server)"/>                                 |
| Summary | 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. |

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 | <input type="button" value="Add..."/> <input type="button" value="Remove"/> |
| Name             |   |      |          |   |
| VBRRepo2         |   |      |          |   |
| Placement Policy |   |      |          |   |

4. For the Placement Policy, choose either Data Locality or Performance based your requirements. Select next.
5. 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                 | Extend scale-out backup repository capacity with object storage:<br>Amazon S3 Repo  | Add...                                   |
|----------------------|---|--|
| Performance Tier     |   |  |
| Placement Policy     |   | <input type="button" value="Window..."/> |
| <b>Capacity Tier</b> | <input checked="" type="checkbox"/> Copy backups to object storage as soon as they are created<br>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.                        |  |
| Archive Tier         | <input checked="" type="checkbox"/> Move backups to object storage as they age out of the operational restore window<br>Reduce your long-term retention costs by moving older backups to object storage completely while preserving the ability to restore directly from offloaded backups. |  |
| Summary              | Move backup files older than <input type="text" value="14"/> days (your operational restore window) <input type="button" value="Override..."/>  |  |
|                      | <input type="checkbox"/> Encrypt data uploaded to object storage<br>Password: <input type="password"/><br><input type="button" value="Add..."/> <input type="button" value="Manage passwords"/>   |  |

6. 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](#).

## Cloud backup 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/>.



## SnapCenter API

[ Base URL: /api ]

<https://snapcentersddc.netapp.com:8146/Content/swagger/SnapCenter.yaml>

Manage your SnapCenter Server using the SnapCenter API.

To access the swagger documentation of "SnapCenter Plug-in for VMware vSphere" API's, please use  
[https://{{SCV\\_hostname}}:{{SCV\\_host\\_port}}/api/swagger-ui.html](https://{{SCV_hostname}}:{{SCV_host_port}}/api/swagger-ui.html)

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

### Auth

POST

/4.6/auth/login Service login

The login endpoint exposes the method required to log in to the SnapCenter service. The login method returns a token that is used to authenticate subsequent requests.

Parameters

Try it out

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

| Name  | Description  |
|---|--|
| TokenNeverExpires<br>boolean<br>(query)             | <input type="text" value="false"/>   |
| UserOperationContext * required<br>object<br>(body) | <p>User credentials</p> <p><a href="#">Edit Value</a>   <a href="#">Model</a></p> <pre>{   "UserOperationContext": {     "User": {       "Name": "localhost\\scadmin",       "Passphrase": "NetApp321",       "Rolename": "SnapCenterAdmin"     }   } }</pre> <p><a href="#">Cancel</a></p> <p>Parameter content type<br/><input type="text" value="application/json"/></p> <p><a href="#">Execute</a></p> |

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

```

{
  "User": {
    "Token": "K1YxOg==tsV6EOdtAmAYpe8q5SG6wcoGaSjwME6jrNy5CsY63HKQ5LkoZLIESRNhpGJJ0UUQynEndgtVGDZnvx+I/ZJZIn5M1Nzrj6
CLfGTApq1GmcagT08bqb5bMfx07EcdrAidzAXUDb3GyLOKtW0GdwKzSeUwKj3uVupnk1E3lskK6PRBv9RS8j0qHQvo4v4RL0hhThhwPhV
9/23nFeJVP/p1Ev4vrV/zeZVTUHFHUM069XRe5cuW9nwyj4b0I5Y5FN3XDkjO==",
    "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   |
|---|---|
| <b>Token</b> * required<br>string<br>(header)           | User authorization token<br><br>TUHFHUM069XRe5cuW9nwyj4b0l5Y5FN3XDkjQ==   |
| <b>SmDRBackupRequest</b> * required<br>object<br>(body) | Parameters to take Backup<br><br><a href="#">Edit Value</a>   <a href="#">Model</a><br><br>{<br>"TargetPath": "C:\\SnapCenter_Backups\\\\"<br>} |

[Cancel](#)

Parameter content type  
[application/json](#) ▾

[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'

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.

The screenshot shows the 'Try it out' interface for the `/4.6/disasterrecovery/server/restore` endpoint. The top bar indicates a POST method and the endpoint URL. Below the URL, a description states 'Starts SnapCenter Server Restore.' A 'Parameters' section is present, and a 'Try it out' button is located on the right.

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

The screenshot shows the 'Try it out' interface for the `/4.6/disasterrecovery/server/restore` endpoint. The 'Parameters' section contains:  
- **Token** (required, type string, header): KIYxOg==rMXzS7EPIGrzTXjfton6Q+JoNGpueQt  
- **SmDRRestRequest** (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\\\\" }  
The 'Edit Value' and 'Model' buttons are visible next to the SmDRRestRequest input field.

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.

| 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   |
|---|---|
| <b>Token</b> <small>* required</small><br>string<br>(header)                              | User authorization token<br><br>KIYxOg==rMXzS7EPIGRzTXjfton6Q+JoNGpueQi   |
| <b>SmSetDisasterRecoverySettingsRequest</b> <small>* required</small><br>object<br>(body) | Parameters to enable or disable the DR mode<br><br>Edit Value   Model<br><br>{<br>"EnableDisasterRecovery": true<br>} |



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.

- 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.

- 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.



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

### New Object Storage Repository

X



#### Bucket

Specify Amazon S3 bucket to use.

Name

Data center:

US East (N. Virginia)

Account

Bucket:

ehcveeamrepo

Browse...

Bucket

Summary

Folder:

RTP

Browse...

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.

Make recent backups immutable for: 30 days

Protects backups from modification or deletion by ransomware, hackers or malicious insiders using native object storage capabilities.

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.

Store backups in a single availability zone (even lower price per GB, reduced resilience)

< Previous

Apply

Finish

Cancel

- 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.



## 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.

Full VM Restore

**Virtual Machines**  
Select virtual machines to be restored. You can add individual virtual machines from backup files, or containers from live environment (containers will be automatically expanded into plain VM list).

**Virtual Machines**

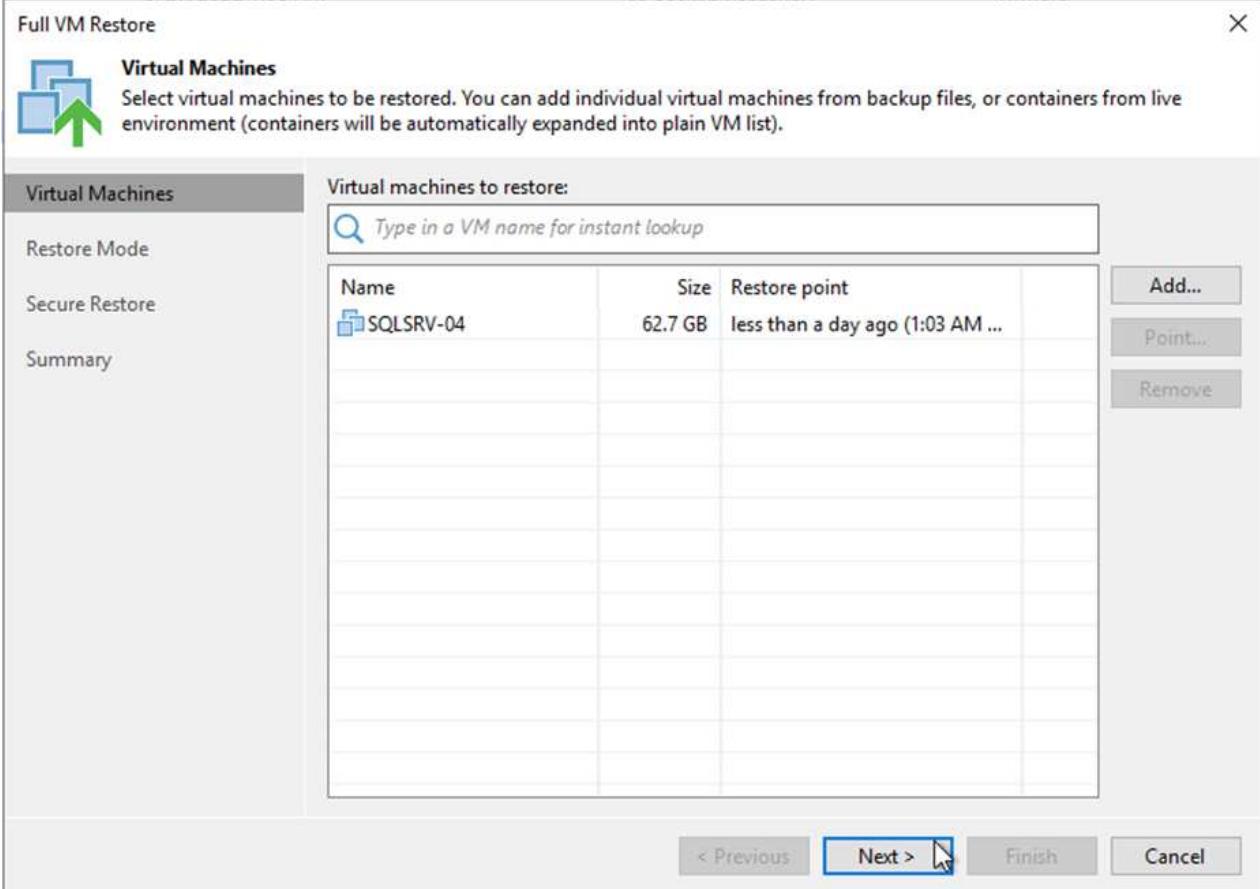
Restore Mode  
Secure Restore  
Summary

**Virtual machines to restore:**

| Name      | Size    | Restore point                     |
|-----------|---------|-----------------------------------|
| SQLSRV-04 | 62.7 GB | less than a day ago (1:03 AM ...) |

Add...  
Point...  
Remove

< Previous **Next >** Finish Cancel



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**  **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.

**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.

**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](#)

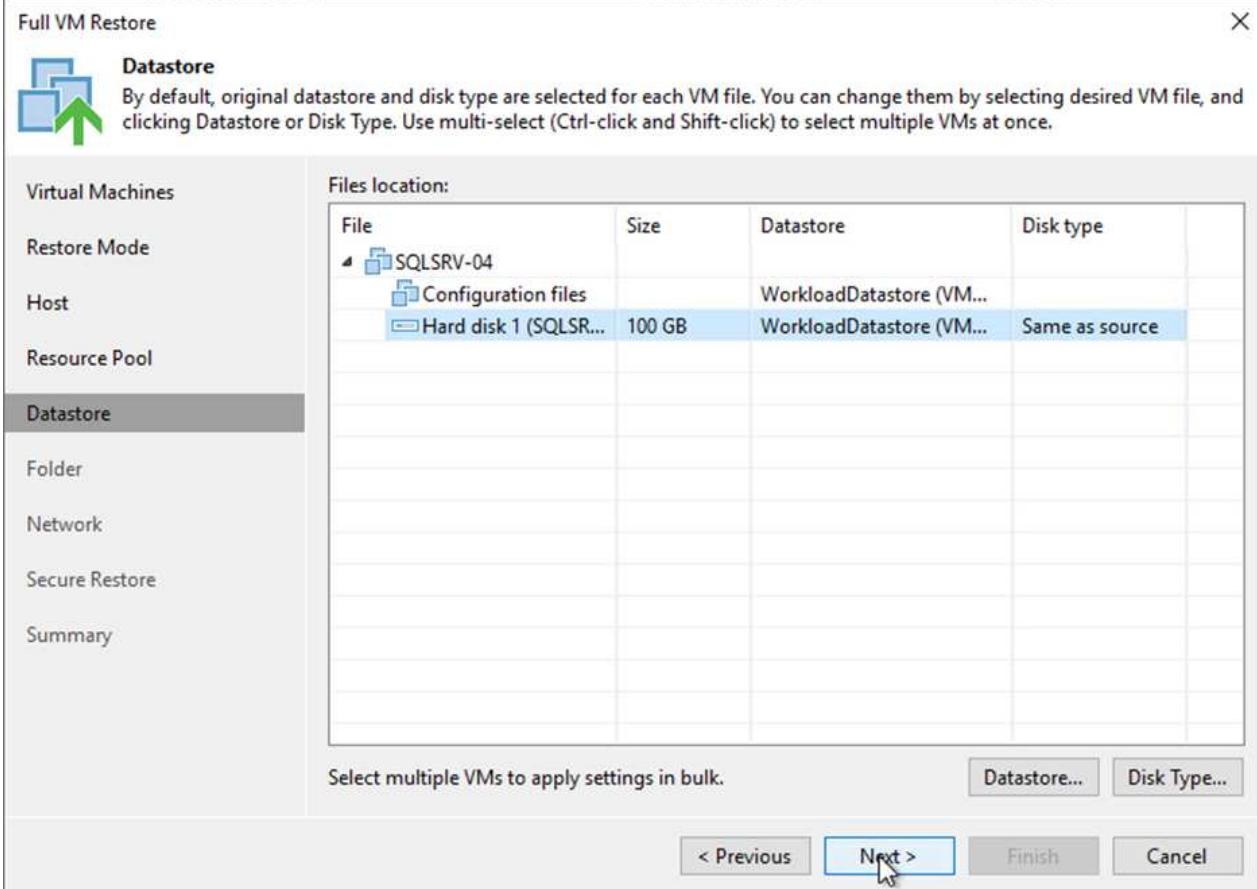
**Quick rollback (restore changed blocks only)**  
Allows for quick VM recovery in case of guest OS software problem, or user error. Do not use this option when recovering from disaster caused by hardware or storage issue, or power loss.

[< 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.



6. On the Network page, map the original networks on the VM to the networks in the new target location.

Full VM Restore

**Network**

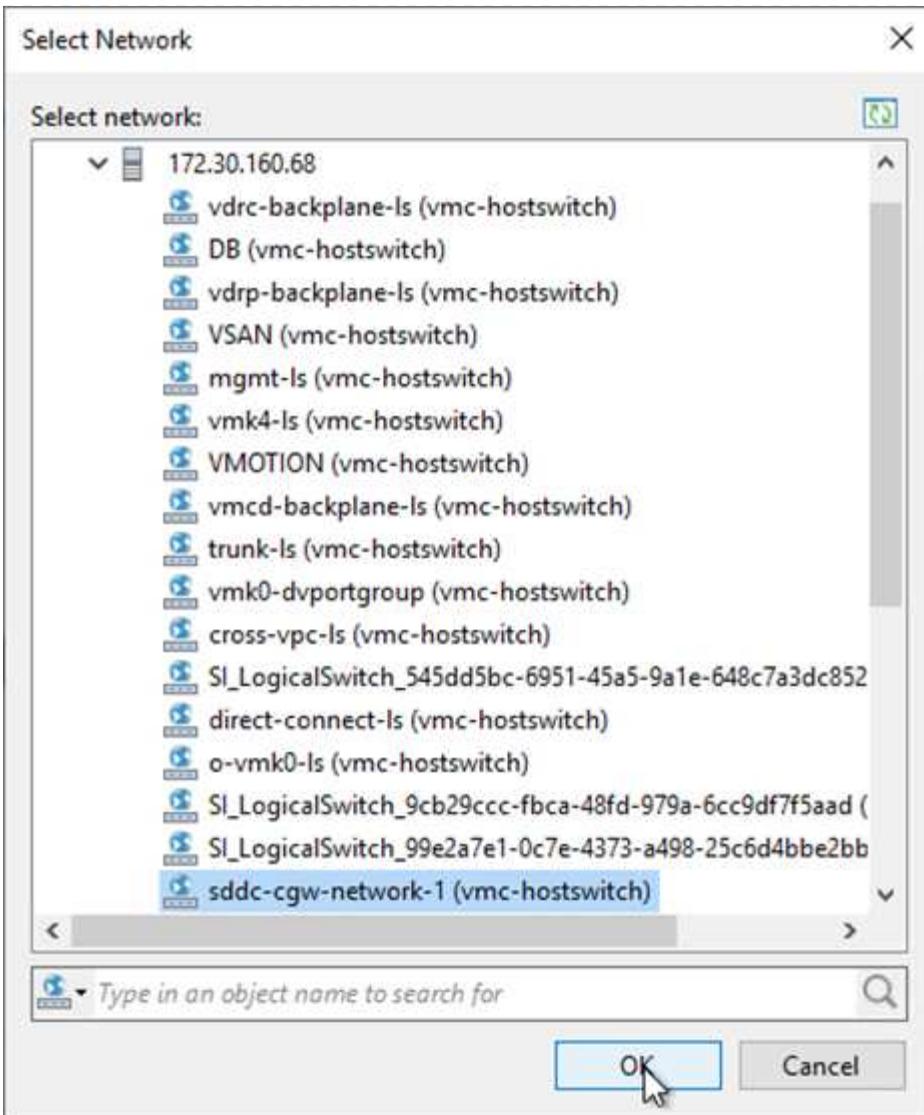
By default, we will connect the restored VM to the same virtual networks as the original VM. If you are restoring to a different location, specify how networks map between original and new locations.

| Virtual Machines | Network connections:      |               |
|------------------|---------------------------|---------------|
|                  | Source                    | Target        |
| Restore Mode     | SQLSRV-04                 |               |
| Host             | Management 181 (DSwitch)  | Not connected |
| Resource Pool    | Data - A - 3374 (DSwitch) | Not connected |
| Datastore        | Data - B - 3375 (DSwitch) | Not connected |
| Folder           |                           |               |
| <b>Network</b>   |                           |               |
| Secure Restore   |                           |               |
| Summary          |                           |               |

Select multiple VMs to apply settings change in bulk.

Network... Disconnect

< Previous Next > Finish 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:::> igrup create -vserver DestSVM -igroup igrupNome  
-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 igrup  
igroupNome
```

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

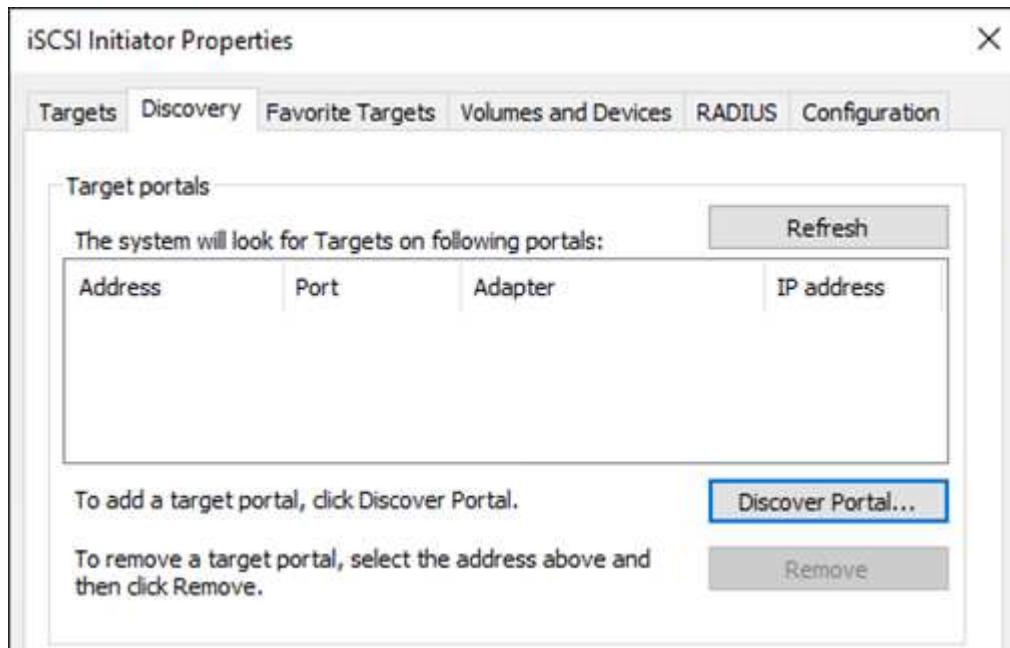
## Set up the Windows VM for iSCSI access and discover the file systems

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  | Management IP address       |
| svm-045c077375d3d9799.fs-0ae40e08acc0dea67.fsx.us-east-1.amazonaws.com       | 198.19.254.53               |
| NFS DNS name   | NFS IP address              |
| svm-045c077375d3d9799.fs-0ae40e08acc0dea67.fsx.us-east-1.amazonaws.com       | 198.19.254.53               |
| iSCSI DNS name   | iSCSI IP addresses          |
| iscsi.svm-045c077375d3d9799.fs-0ae40e08acc0dea67.fsx.us-east-1.amazonaws.com | 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.



## 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.

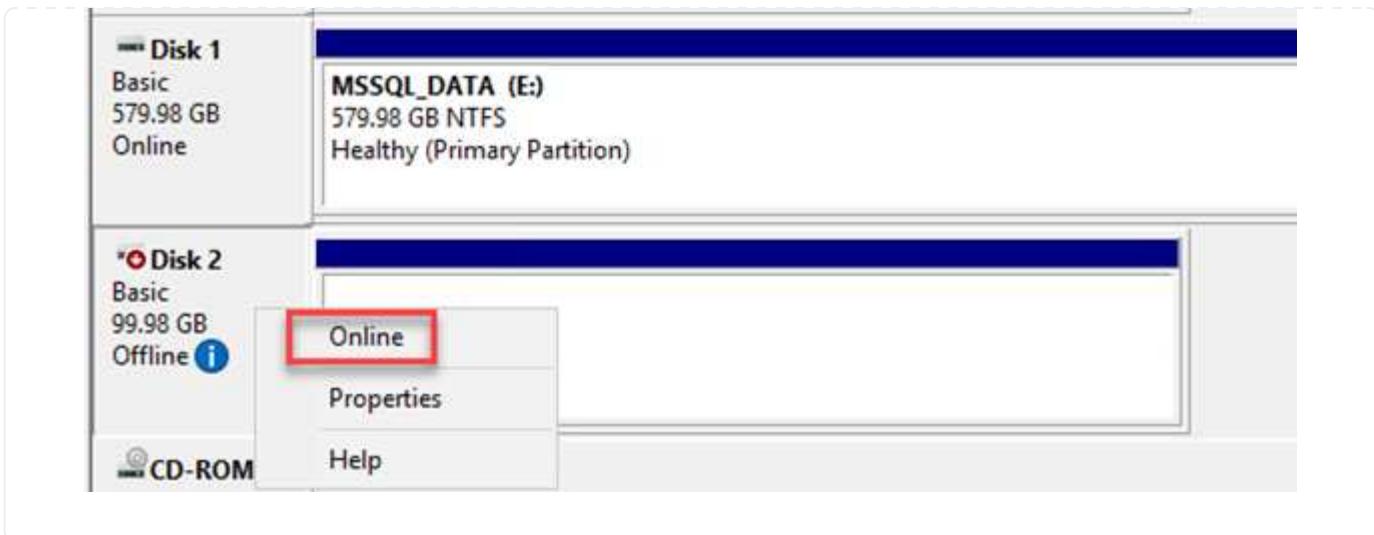
IP address or DNS name:

Port: (Default is 3260.)

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.

Object Explorer

Connect ▾

SQLSRV-01 (SQL Server 15.0.2080.9 - sa)

Databases

System Databases

Database Snapshots

SQLHC01

Security

Server Objects

Replication

PolyBase

Always On High Availability

Management

Integration Services Catalogs

SQL Server Agent (Agent XPs disabled)

XEvent Profiler

Select a page

General

Files

Filegroups

Options

Change Tracking

Permissions

Extended Properties

Monitoring

Transaction Log Shipping

Query Store

Script Help

Backup

Last Database Backup: None

Last Database Log Backup: None

Database

Name: SQLHC01

Status: Normal

Owner: sa

Date Created: 4/13/2022 9:37:18 PM

Size: 514944.00 MB

Space Available: 501701.86 MB

Number of Users: 4

Memory Allocated To Memory Optimized Objects: 0.00 MB

Memory Used By Memory Optimized Objects: 0.00 MB

Maintenance

Collation: SQL\_Latin1\_General\_CI\_AS

## 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.

The screenshot shows the NetApp SnapCenter web interface. The left sidebar has navigation links: Dashboard, Resources, Monitor, Reports, Hosts, Storage Systems, Settings (which is selected), and Alerts. The main content area has tabs: Global Settings (selected), Policies, and Users and Access. Under Global Settings, there are several sections: Hypervisor Settings, Notification Server Settings, Configuration Settings, Purge Jobs Settings, Domain Settings, and CA Certificate Settings. Below these is the Disaster Recovery section, which is highlighted with a blue background. Inside this section, the 'Enable Disaster Recovery' checkbox is checked, and there is an 'Apply' button. The overall theme is blue and white, typical of enterprise software interfaces.

## **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-01167370e9b7aefaa0)

Actions ▾

- Attach
- Update volume**
- Create backup
- Delete volume

**Summary**

|   |  |                                      |
|---|--|--------------------------------------|
| Volume ID   | Creation time                              | SVM ID                               |
| fsvol-01167370e9b7aefaa0  | 2022-03-08T14:52:09-05:00                  | svm-02b2ad25c6b2e5bc2                |
| Volume name   | Lifecycle state                            | Junction path                        |
| oraclesrv_03_u01_dest   | <span style="color: green;">Created</span> | -                                    |
| UUID  | Volume type                                | Tiering policy name                  |
| 3d7338ce-9f19-11ec-b007-4956fb75f45c  | ONTAP                                      | SNAPSHOT_ONLY                        |
| File system ID  | Size                                       | Tiering policy cooling period (days) |
| fs-0ae40e08acc0dea67  | 100.00 GB                                  | 2                                    |
| Resource ARN  |  | Storage efficiency enabled           |
| arn:aws:fsx:us-east-1:541696183547:volume/fs-0ae40e08acc0dea67/fsvol-01167370e9b7aefaa0 |  | 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

X

### 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



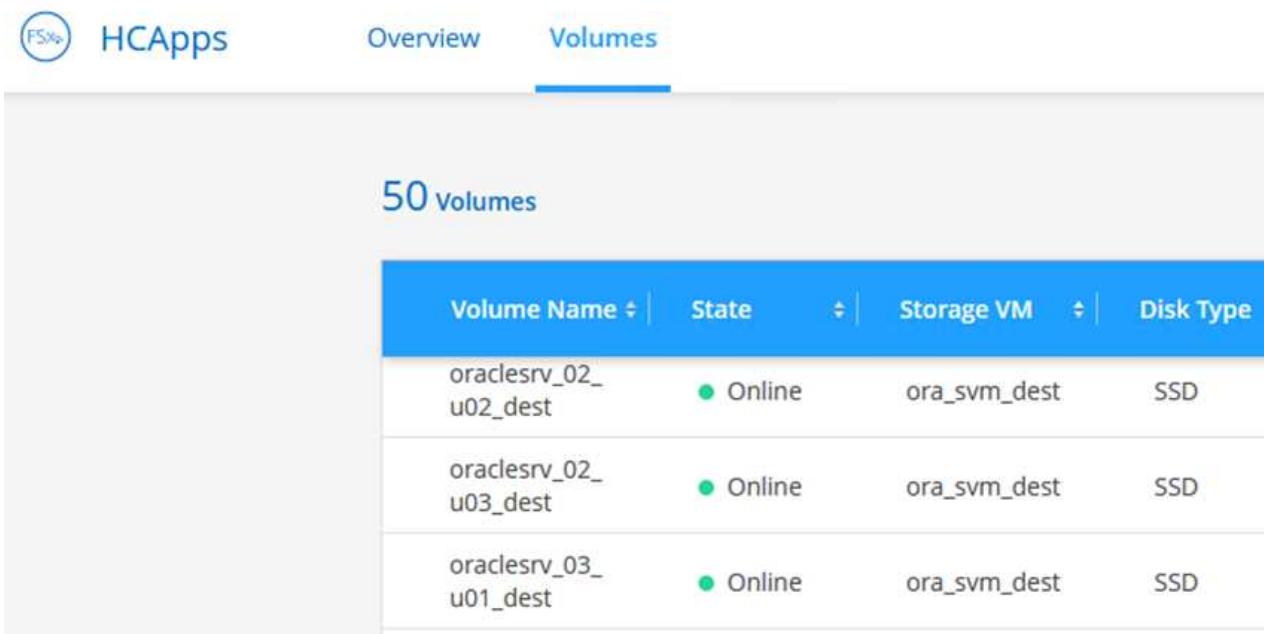
Cancel

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.



The screenshot shows the Cloud Manager interface with the 'Volumes' tab selected. The title bar includes icons for FSx, HCApps, Overview, and Volumes. Below the title bar, it says '50 Volumes'. A table lists three volumes:

| 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.

## Fallback

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](#)

[NetApp Solutions](#)

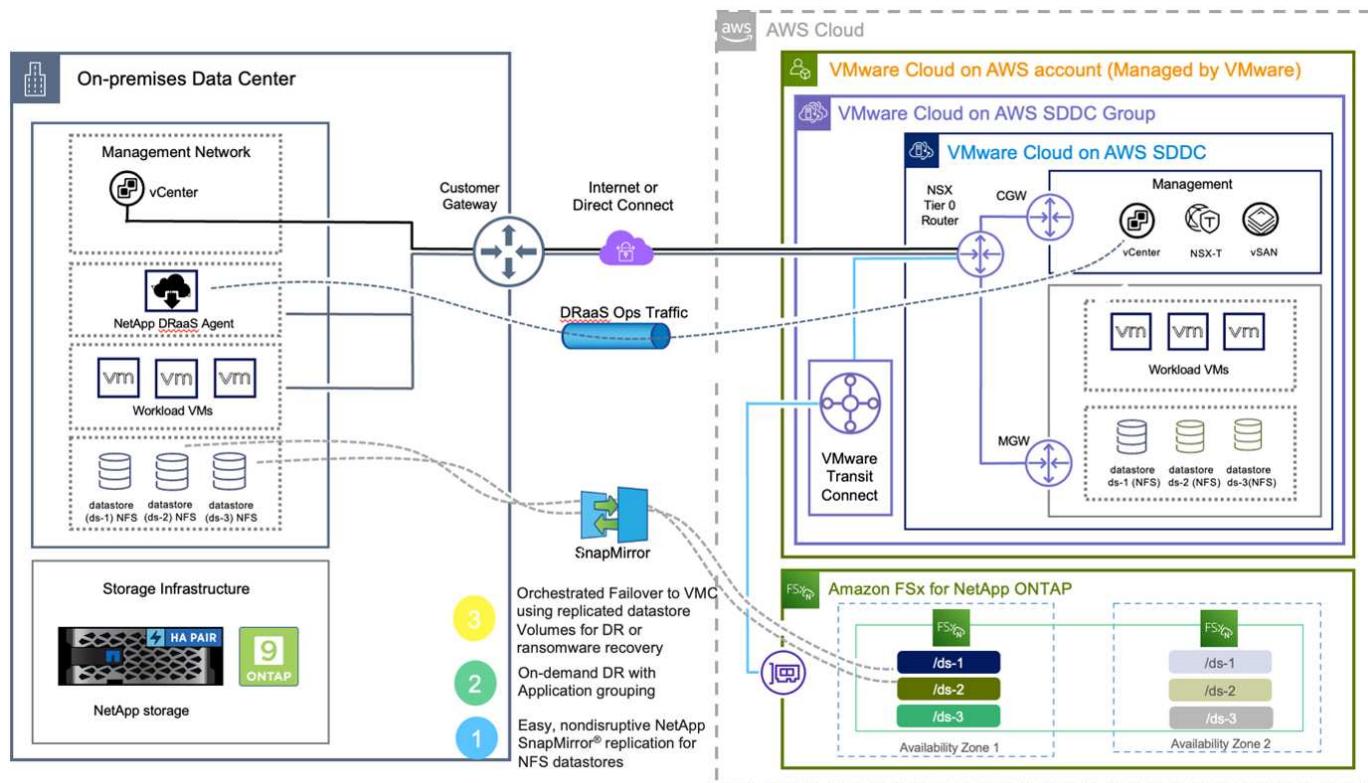
# TR-4955: Disaster Recovery with FSx for ONTAP and VMC (AWS VMware Cloud)

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:

The screenshot shows the NetApp BlueXP interface. At the top, there's a header with 'NetApp BlueXP' logo, account information ('nimolab'), workspace ('nimhybridlab'), connector ('AWSConnCM'), and various navigation icons. Below the header, there are tabs for 'Canvas' (selected), 'My Working Environments' (highlighted in blue), 'My Opportunities', and a 'New' button. The main canvas displays several cloud environments: 'nimfsx FSx for ONTAP' (7 volumes, 13.01 TiB capacity), 'ntaphci-a300e9u25 On-Premises ONTAP' (131.27 TiB capacity), 'DemoFSxN FSx for ONTAP' (5 volumes, 4.74 TiB capacity), and 'ANF Azure NetApp Files' (status 'Failed'). Below these are 'Azure Blob Storage' (0 storage accounts) and 'Amazon S3' (6 buckets). On the right side, there's a detailed view for 'ntaphci-a300e9u25' showing 'DETAILS' (On-Premises ONTAP) and 'SERVICES' (Backup and recovery, Copy & sync, Tiering, Classification). A large 'Enter Working Environment' button is at the bottom right.

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:

```
https://github.com/NetApp-Automation/DRO.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:

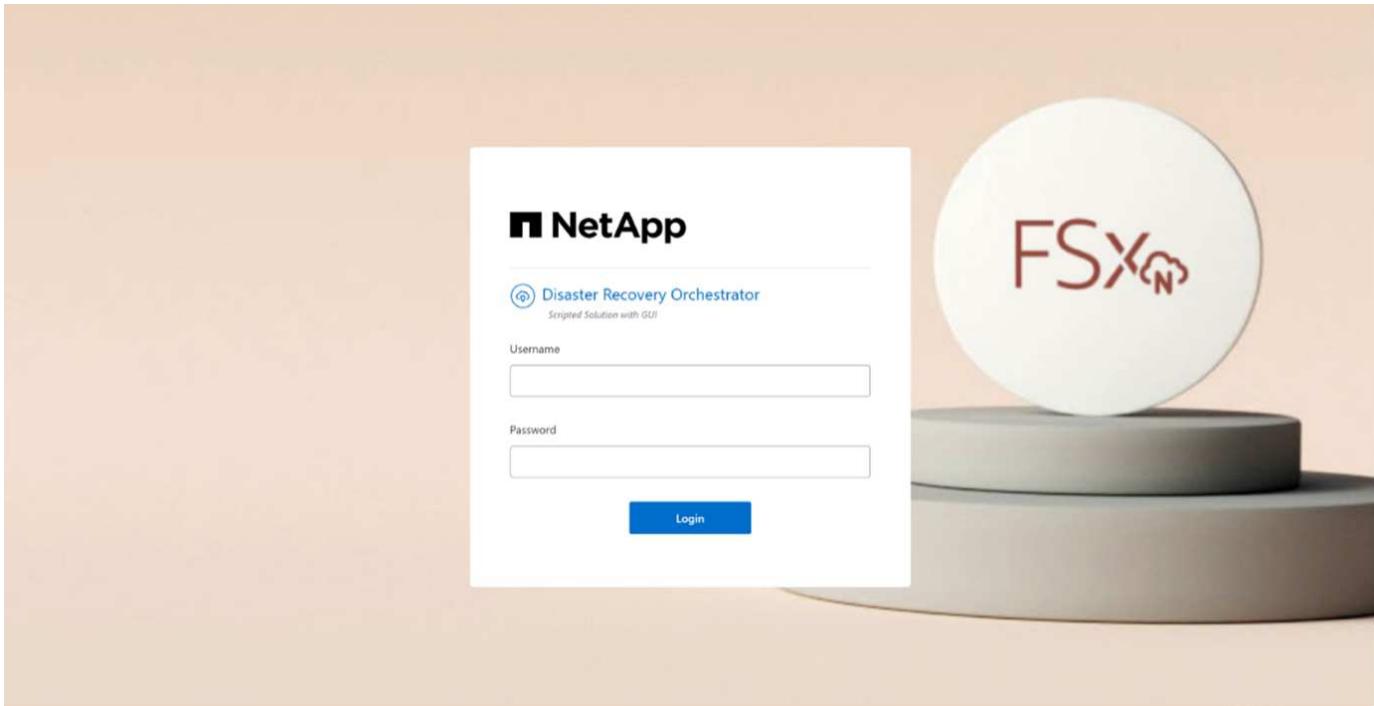
```
https://<host-ip-address>
```

with the following default credentials:

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



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



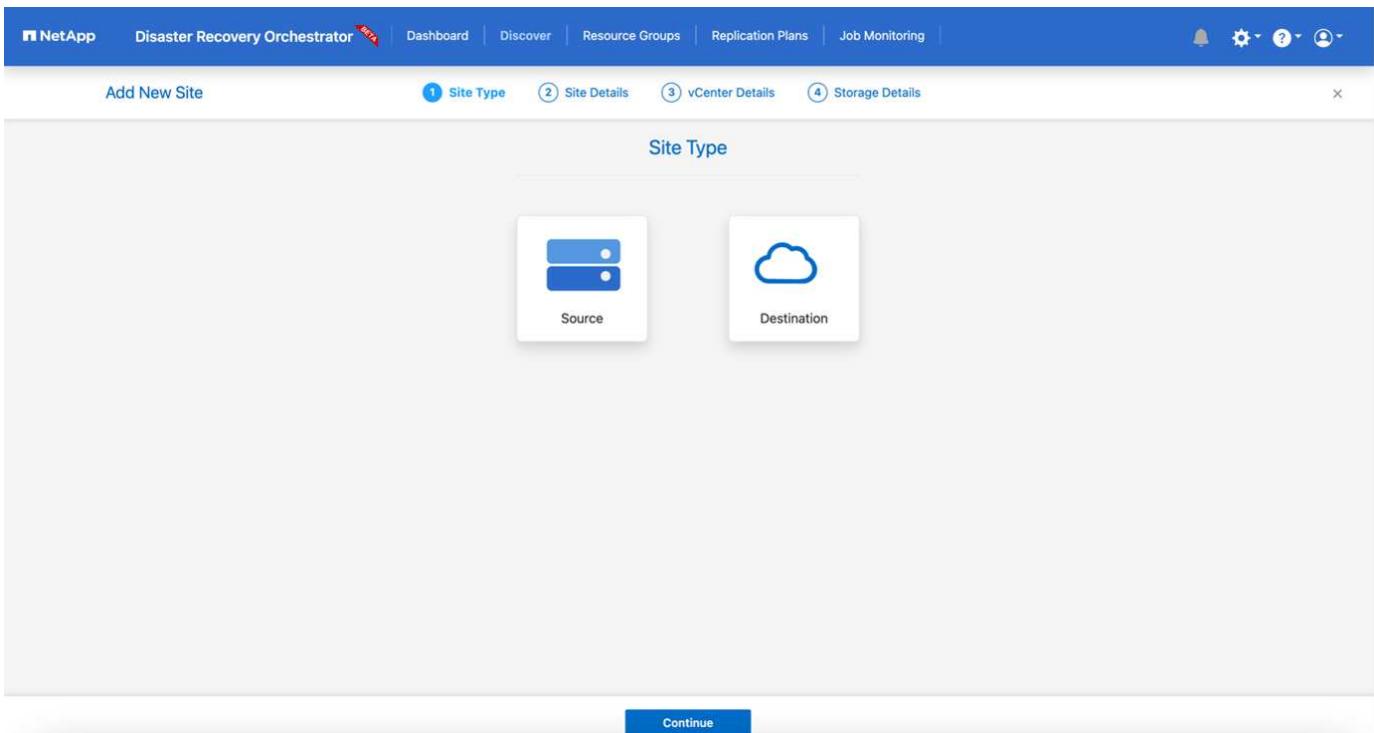
## DRO configuration

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



The screenshot shows the 'Site Summary' page in the NetApp Disaster Recovery Orchestrator. It displays summary statistics for 2 Sites, 2 vCenters, and 2 Storages. Below this, there is a table showing two sites:

| Site Name | Site Type   | Location | vCenter | Storage | VM List                      | Discovery Status            | Actions |
|-----------|-------------|----------|---------|---------|------------------------------|-----------------------------|---------|
| Cloud     | Destination | Cloud    | 1       | 1       | <a href="#">View VM List</a> | • 44.235.223.88<br>Success  | ...     |
| On Prem   | Source      | On Prem  | 1       | 1       | <a href="#">View VM List</a> | • 172.21.253.160<br>Success | ...     |

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.

**VM List**  
Site: On Prem | vCenter: 172.21.253.160

| 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        |
| jhRBhoja-187 | Not Protected | Powered On   | A300_NFS_DS04 | 4   | 16384       |
| jhNimo-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**.

The screenshot shows the NetApp Disaster Recovery Orchestrator interface. At the top, there are four summary cards: '1 Resource Group', '1 Site', '1 vCenter', and '3 Virtual Machines'. Below these are two tabs: 'Resource Groups' (which is highlighted with a red box) and 'Replication Plans'. The main content area displays a table for 'Resource Group Name' with one entry: 'DemoRG1'. It also shows 'Site Name' (On Prem), 'Source vCenter' (172.21.253.160), and a 'VM List' button. A 'Create New Resource Group' button is located at the bottom right of this section, also highlighted with a red box.

## 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**.

The screenshot shows the NetApp Disaster Recovery Orchestrator interface. At the top, there are four summary cards: '1 Replication Plans', '1 Resource Groups', 'Source Details' (1 Sites, 1 vCenters), and 'Destination Details' (1 Sites, 1 vCenters). Below these are two tabs: 'Replication Plans' (which is highlighted with a red box) and 'Job Monitoring'. The main content area displays a table for 'Plan Name' with one entry: 'DemoRP1'. It also shows 'Active Site' (Source, Active, Healthy), 'Status' (Compliance, On Prem, Cloud), and buttons for 'Resource Groups' and '...'. A 'Create New Replication Plan' button is located at the bottom right of this section, also highlighted with a red box.

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

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

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: DemoRP

**Recovery Mapping**

Source Site: On Prem   Destination Site: Cloud

Source vCenter: 172.21.253.160   Destination vCenter: 44.235.223.88

**Cluster Mapping**

Source Site Resource: TempCluster   Destination Site Resource: Cluster-1

**Add**

| Source Resource | Destination Resource |               |
|-----------------|----------------------|---------------|
| A300-Cluster01  | Cluster-1            | <b>Delete</b> |

**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.

The screenshot shows the 'Create New Replication Plan' wizard at step 4: 'Set Execution Order'. It displays a table with one row: 'DemoRG1' in the Resource Group Name column and '3' in the Execution Order column. Below this is a section titled 'Network Mapping' which states 'No more Source/Destination network resources available for mapping'. Under 'DataStore Mapping', there is a table with one row: 'VLAN 3375' in the Source Resource column and 'sddc-cgw-network-1' in the Destination Resource column. A 'Delete' link is also present. At the bottom are 'Previous' and 'Continue' buttons.

8. 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.

The screenshot shows the 'Create New Replication Plan' wizard at step 5: 'Set VM Details'. It displays a table for three VMs: Mini\_Test01, Mini\_Test02, and Mini\_Test03. The table includes columns for VM Name, No. of CPUs, Memory (MB), NIC/IP, and Boot Order. For each VM, the 'Dynamic' radio button is selected under Boot Order. The 'Override' checkbox is checked. The 'Resource Group : DemoRG1' is listed above the table. At the bottom are 'Previous' and 'Create Replication Plan' buttons, with 'Create Replication Plan' highlighted in red.

## 9. Click Create Replication Plan.

The screenshot shows the DRO interface with the 'Replication Plans' tab selected. The main area displays summary statistics: 2 Replication Plans, 1 Resource Groups, and details for Source and Destination sites. Below this, a table lists two replication plans named 'DemoRP'. The table columns include Plan Name, Active Site, Status, Compliance, Source Site, and Destination Site. The 'Create New Replication Plan' button is highlighted with a red box.

| Plan Name | Active Site | Status | Compliance    | Source Site | Destination Site |
|-----------|-------------|--------|---------------|-------------|------------------|
| DemoRP    | Source      | Active | Not Available | On Prem     | Cloud            |
| DemoRP    | Source      | Active | Healthy       | On Prem     | Cloud            |

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**.

The screenshot shows the DRO interface with the 'Replication Plans' tab selected. The main area displays summary statistics: 2 Replication Plans, 1 Resource Groups, and details for Source and Destination sites. Below this, a table lists two replication plans named 'DemoRP'. The table columns include Plan Name, Active Site, Status, Compliance, Source Site, and Destination Site. A context menu is open over the second 'DemoRP' entry, showing options like 'Edit Plan', 'Failover' (which is highlighted with a red box), 'Test Failover', 'Migrate', 'Run Compliance', and 'Delete Plan'.

## Failover Details



### Volume Snapshot Details

- Use latest snapshot (i)
- Select specific snapshot (i)

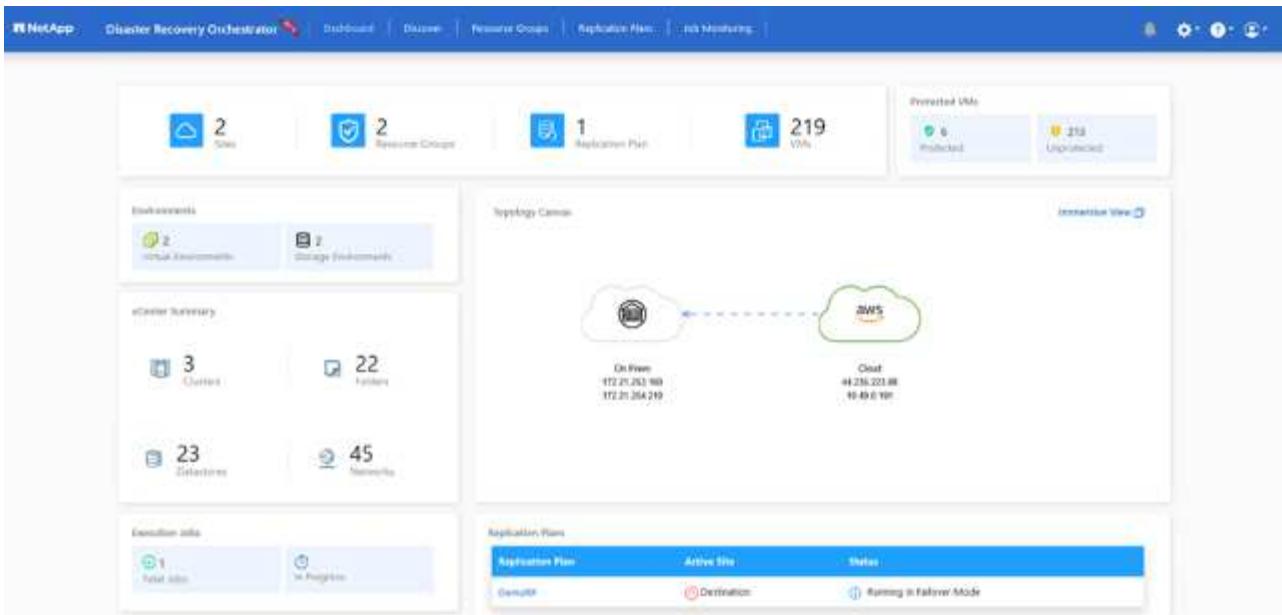
**Start Failover**

The replication plan can be monitored in the task menu:

The screenshot shows the NetApp Disaster Recovery Orchestrator interface. The top navigation bar includes 'NetApp' and 'Disaster Recovery Orchestrator' with a red alert icon, followed by 'Dashboard', 'Discover', 'Resource Groups', 'Replication Plans', and 'Job Monitoring'. A red box highlights the 'Job Monitoring' tab. Below the navigation is a toolbar with icons for bell, gear, help, and user. The main content area has a 'Back' link and a 'Failover Steps' section. A red box highlights the 'Failover Steps' header. Underneath it, the 'Replication Plan: DemoRP' is listed. The failover steps are as follows:

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

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**.

The interface shows the following details for the two replication plans:

| Plan Name | Active Site | Status                   | Compliance | Source Site | Destination Site |
|-----------|-------------|--------------------------|------------|-------------|------------------|
| DemoRP    | Destination | Running In Failover Mode | Healthy    | On Prem     | Cloud            |
| DemoRP    | Source      | Active                   | Healthy    | On Prem     | Cloud            |

A modal window titled "Plan Details" is open for the "DemoRP" plan, showing the "Resource Groups" tab selected. The "Reverse Data Sync" option is highlighted with a red box.

The "Reverse Data Sync Steps" page displays the following steps for the "DemoRP" replication plan:

- Powering off VMs in protection group - DemoRG1 - in source (In progress)
- Reversing SnapMirror relationships (in parallel) (Initialized)

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

The screenshot shows the DRO dashboard with the following key metrics:

- Replication Plans:** 2
- Resource Groups:** 1
- Source Details:** 1 Site, 1 vCenter
- Destination Details:** 1 Site, 1 vCenter

The main table lists two replication plans:

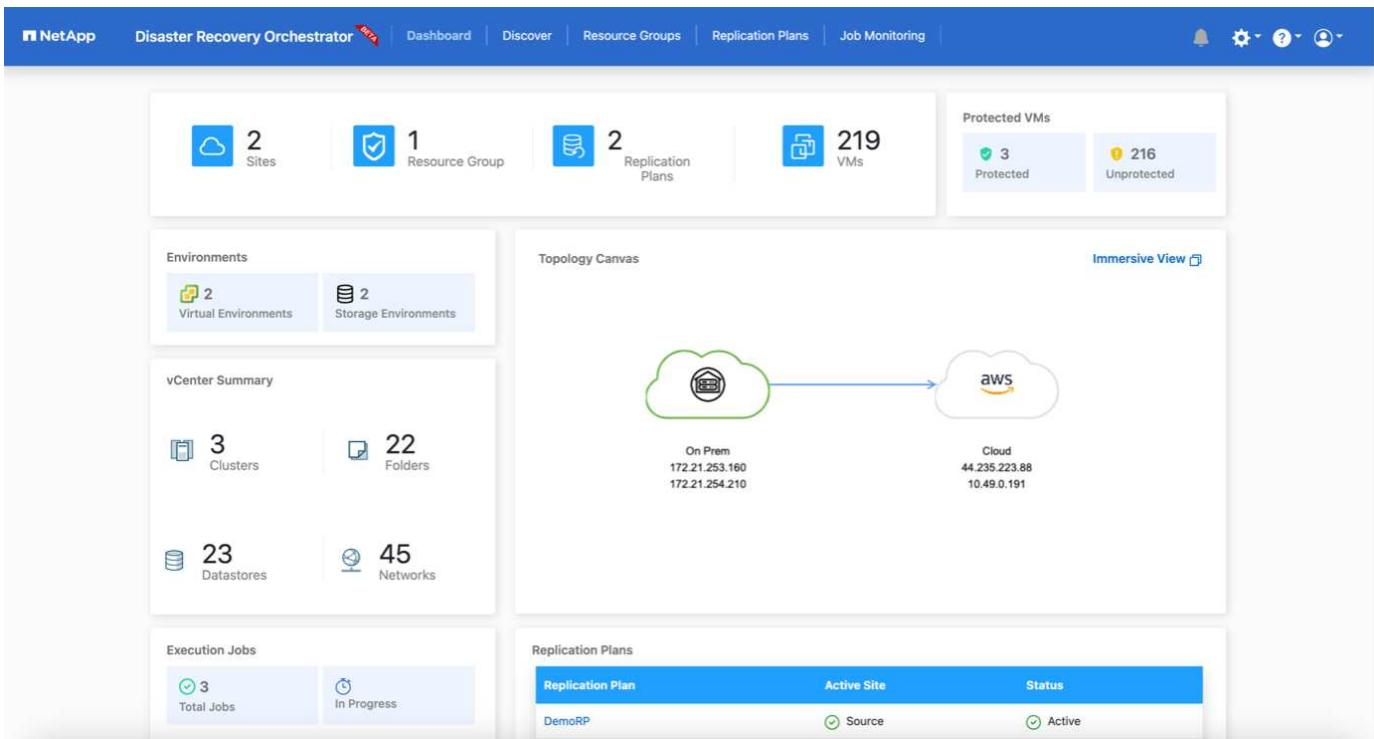
| Plan Name | Active Site | Status | Compliance | Source Site | Destination Site | Actions                         |
|-----------|-------------|--------|------------|-------------|------------------|---------------------------------|
| DemoRP    | Destination | Active | Healthy    | On Prem     | Cloud            | <a href="#">Resource Groups</a> |
| DemoRP    | Source      | Active | Healthy    | On Prem     | Cloud            | <a href="#">Resource</a>        |

A tooltip for the "Resource" link in the second row indicates "Plan Details" and "Fallback".

The screenshot shows the "Fallback Steps" page for the "DemoRP" replication plan. It lists the following steps:

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

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 Dev/Test, 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.

## Migrating Workloads

# TR 4942: Migrate Workloads to FSx ONTAP datastore using VMware HCX

Author(s): NetApp Solutions Engineering

## Overview: Migrating virtual machines with VMware HCX, FSx ONTAP supplemental datastores, and VMware Cloud

A common use case for VMware Cloud (VMC) on Amazon Web Services (AWS), with its supplemental NFS datastore on Amazon FSx for NetApp ONTAP, is the migration of VMware workloads. VMware HCX is a preferred option and provides various migration methods to move on-premises virtual machines (VMs) and their data, running on any VMware supported datastores, to VMC datastores, which includes supplemental NFS datastores on FSx for ONTAP.

VMware HCX is primarily a mobility platform that is designed to simplify workload migration, workload rebalancing, and business continuity across clouds. It is included as part of VMware Cloud on AWS and offers many ways to migrate workloads and can be used for disaster recovery (DR) operations.

This document provides step-by-step guidance for deploying and configuring VMware HCX, including all its main components, on-premises and on the cloud data center side, which enables various VM migration mechanisms.

For more information, see [Introduction to HCX Deployments](#) and [Install Checklist B - HCX with a VMware Cloud on AWS SDDC Destination Environment](#).

## High-level steps

This list provides the high-level steps to install and configure VMware HCX:

1. Activate HCX for the VMC software-defined data center (SDDC) through VMware Cloud Services Console.
2. Download and deploy the HCX Connector OVA installer in the on-premises vCenter Server.
3. Activate HCX with a license key.
4. Pair on-premises VMware HCX Connector with VMC HCX Cloud Manager.
5. Configure the network profile, compute profile, and service mesh.
6. (Optional) Perform Network Extension to extend the network and avoid re-IP.
7. Validate the appliance status and ensure that migration is possible.
8. Migrate the VM workloads.

## Prerequisites

Before you begin, make sure the following prerequisites are met. For more information, see [Preparing for HCX Installation](#). After the prerequisites are in place, including connectivity, configure and activate HCX by generating a license key from the VMware HCX Console at VMC. After HCX is activated, the vCenter Plug-in is deployed and can be accessed by using the vCenter Console for management.

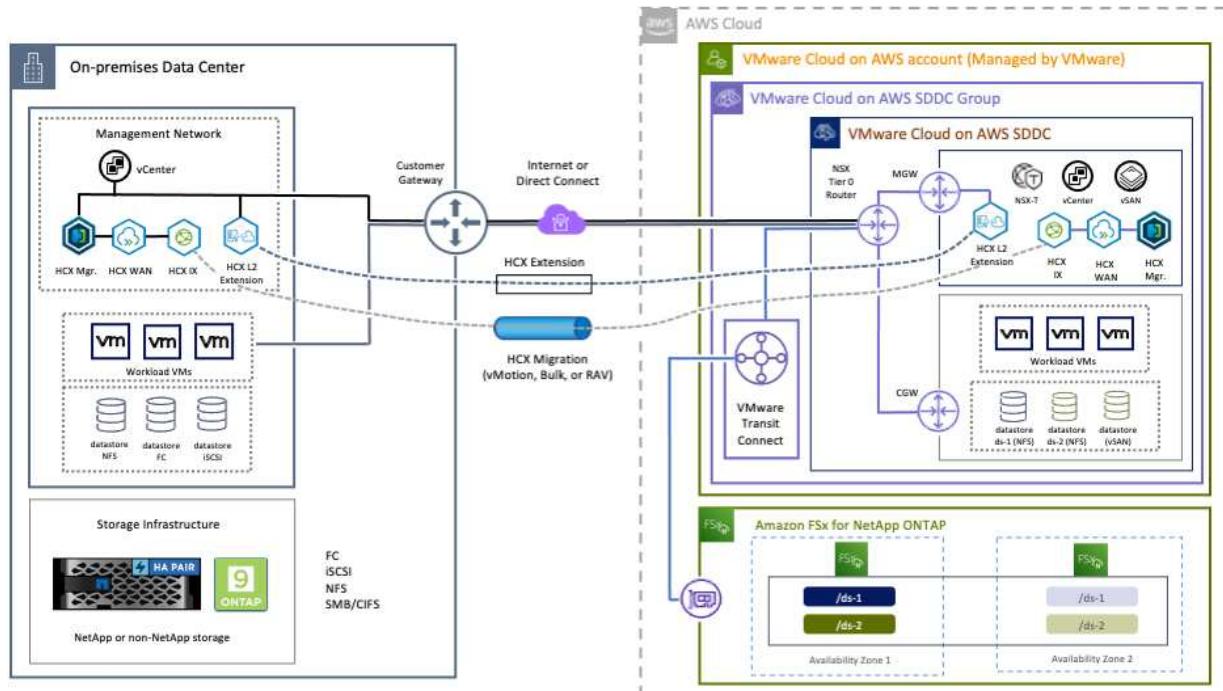
The following installation steps must be completed before proceeding with HCX activation and deployment:

1. Use an existing VMC SDDC or create a new SDDC following this [NetApp link](#) or this [VMware link](#).
2. The network path from the on-premises vCenter environment to the VMC SDDC must support migration of VMs by using vMotion.
3. Make sure the required [firewall rules and ports](#) are allowed for vMotion traffic between the on-premises vCenter Server and the SDDC vCenter.
4. The FSx for ONTAP NFS volume should be mounted as a supplemental datastore in the VMC SDDC. To attach the NFS datastores to the appropriate cluster, follow the steps outlined in this [NetApp link](#) or this [VMware link](#).

## High Level Architecture

For testing purposes, the on-premises lab environment used for this validation was connected through a site-to-site VPN to AWS VPC, which allowed on-premises connectivity to AWS and to VMware cloud SDDC through External transit gateway. HCX migration and network extension traffic flows over the internet between on-premises and VMware cloud destination SDDC. This architecture can be modified to use Direct Connect private virtual interfaces.

The following image depicts the high-level architecture.



## Solution Deployment

Follow the series of steps to complete the deployment of this solution:

### Step 1: Activate HCX through VMC SDDC using the Add-ons option

To perform the installation, complete the following steps:

1. Log in to the VMC Console at [vmc.vmware.com](https://vmc.vmware.com) and access Inventory.
2. To select the appropriate SDDC and access Add-ons, click View Details on SDDC and select the Add Ons tab.
3. Click Activate for VMware HCX.



This step takes up to 25 minutes to complete.

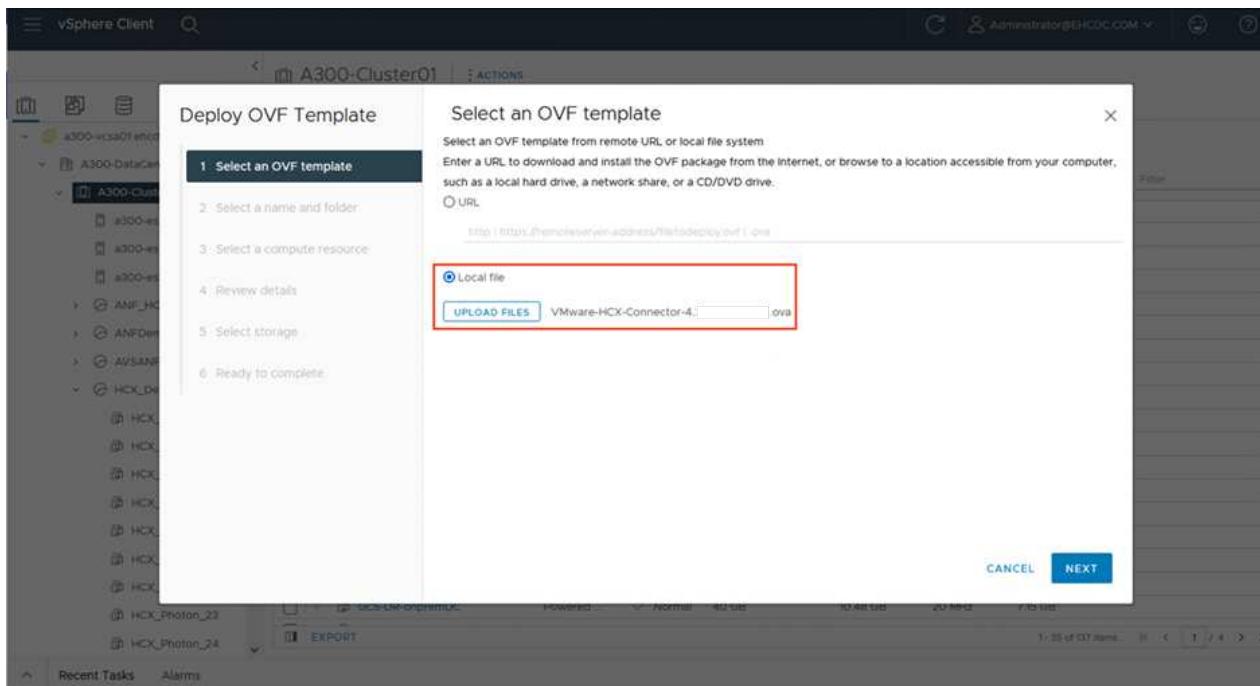
The screenshot shows the VMC SDDC Add-ons page for the FSxDemoSDDC. The VMware HCX section is highlighted, showing its description and an 'ACTIVATE' button. A tooltip indicates that this step takes up to 25 minutes to complete. Other add-ons like Site Recovery and NSX Advanced Firewall are also listed.

4. After the deployment is complete, validate the deployment by confirming that HCX Manager and its associated plug-ins are available in vCenter Console.
5. Create the appropriate Management Gateway firewalls to open the ports necessary to access HCX Cloud Manager. HCX Cloud Manager is now ready for HCX operations.

## Step 2: Deploy the installer OVA in the on-premises vCenter Server

For the on-premises Connector to communicate with the HCX Manager in VMC, make sure that the appropriate firewall ports are open in the on-premises environment.

1. From the VMC Console, navigate to the HCX Dashboard, go to Administration, and select the Systems Update tab. Click Request a Download Link for the HCX Connector OVA image.
2. With the HCX Connector downloaded, deploy the OVA in the on-premises vCenter Server. Right-click vSphere Cluster and select the Deploy OVF Template option.



3. Enter the required information in the Deploy OVF Template wizard, click Next and then Finish to deploy the VMware HCX Connector OVA.
4. Power on the virtual appliance manually. For step-by-step instructions, go to [VMware HCX User Guide](#).

### Step 3: Activate HCX Connector with the license key

After you deploy the VMware HCX Connector OVA on-premises and start the appliance, complete the following steps to activate HCX Connector. Generate the license key from the VMware HCX Console at VMC and input the license during the VMware HCX Connector setup.

1. From the VMware Cloud Console, go to Inventory, select the SDDC, and click View Details. From the Add Ons tab, in the VMware HCX tile, click Open HCX.
2. From the Activation Keys tab, click Create Activation Key. Select the System Type as HCX Connector and click Confirm to generate the key. Copy the activation key.

The screenshot shows the 'Activation Keys' tab in the VMware HCX interface. It displays a table with columns: Activation Key, Status, Subscription, System Type, System Id, and Created. Three entries are shown:

| Activation Key | Status      | Subscription        | System Type   | System Id | Created                |
|----------------|-------------|---------------------|---------------|-----------|------------------------|
| ABIE1          | CONSUMED    | VMware Cloud on AWS | HCX Connector | 202       | 73 9/19/22, 9:24 AM    |
| 92C1           | CONSUMED    | VMware Cloud on AWS | HCX Cloud     | 201       | 15321 9/16/22, 9:56 AM |
| 101            | DEACTIVATED | VMware Cloud on AWS | HCX Cloud     | 202       | 126 8/11/22, 12:23 PM  |

A blue button labeled 'CREATE ACTIVATION KEY' is visible in the top right corner of the table area.



A separate key is required for each HCX Connector deployed on-premises.

3. Log in to the on-premises VMware HCX Connector at <https://hcxconnectorIP:9443> using administrator credentials.



Use the password defined during the OVA deployment.

4. In the Licensing section, enter the activation key copied from step 2 and click Activate.



The on-premises HCX Connector must have internet access for the activation to complete successfully.

5. Under Datacenter Location, provide the desired location for installing the VMware HCX Manager on-premises. Click Continue.
6. Under System Name, update the name and click Continue.
7. Select Yes and then Continue.
8. Under Connect Your vCenter, provide the IP address or fully qualified domain name (FQDN) and the credentials for the vCenter Server and click Continue.



Use the FQDN to avoid communication issues later.

9. Under Configure SSO/PSC, provide the Platform Services Controller's FQDN or IP address and click Continue.
10. Enter the vCenter Server's IP address or FQDN.
11. Verify that the information is entered correctly and click Restart.
12. After complete, the vCenter Server is displayed as green. Both the vCenter Server and SSO must

have the correct configuration parameters, which should be the same as the previous page.



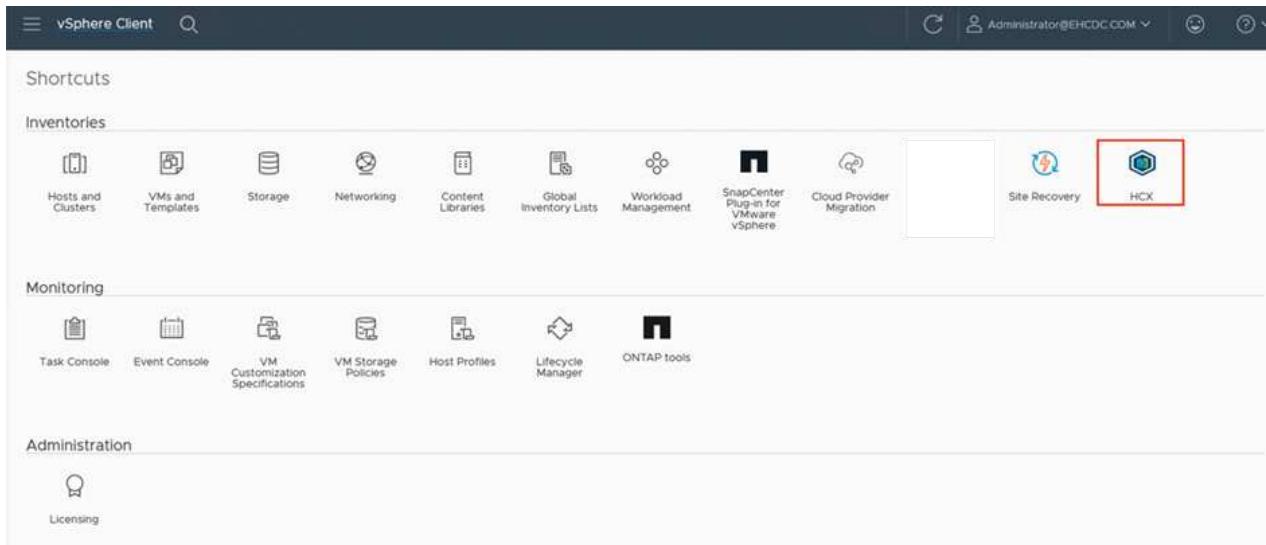
This process should take approximately 10–20 minutes and for the plug-in to be added to the vCenter Server.

The screenshot shows the HCX Manager dashboard for the appliance VMware-HCX-440. The top navigation bar includes links for HCX Manager, Dashboard, Appliance Summary, Configuration, and Administration, along with system information (IP: 172.21.254.157, Version: 4.4.1.0, Type: Connector) and a user account (admin). The main content area displays the following information:

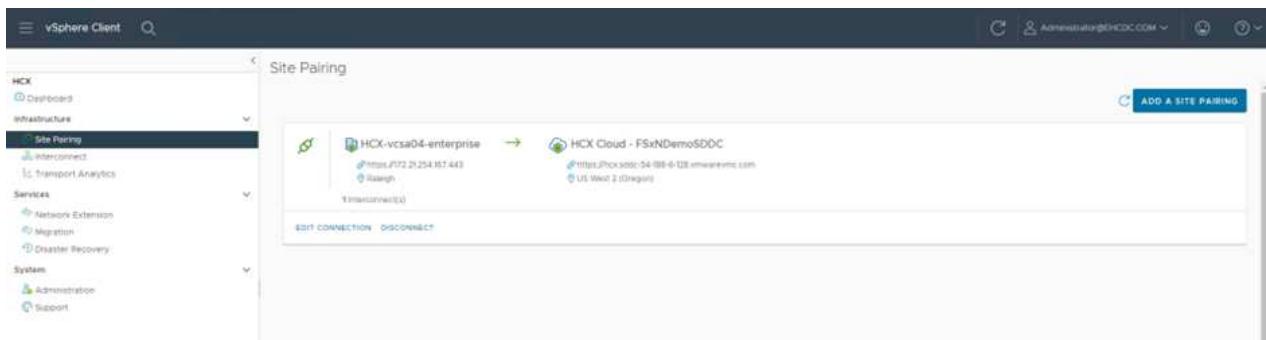
- VMware-HCX-440** summary:
  - FQDN: VMware-HCX-440.ehcde.com
  - IP Address: 172.21.254.157
  - Version: 4.4.1.0
  - Uptime: 20 days, 21 hours, 9 minutes
  - Current Time: Tuesday, 13 September 2022 07:44:11 PM UTC
- Resource Usage**: CPU (Used 1407 MHz, Free 688 MHz, 67% capacity), Memory (Used 9691 MB, Free 2316 MB, 81% capacity), Storage (Used 29G, Free 98G, 23% capacity).
- Connectivity**:
  - vCenter: https://a300-vcsa01.ehcde.com (highlighted with a red box)
  - SSO: https://a300-vcsa01.ehcde.com (highlighted with a red box)
- Management**: Buttons for NSX, vCenter, and SSO management.

## Step 4: Pair on-premises VMware HCX Connector with VMC HCX Cloud Manager

1. To create a site pair between the on-premises vCenter Server and the VMC SDDC, log in to the on-premises vCenter Server and access the HCX vSphere Web Client Plug-in.



2. Under Infrastructure, click Add a Site Pairing. To authenticate the remote site, enter the VMC HCX Cloud Manager URL or IP address and the credentials for the CloudAdmin role.



HCX information can be retrieved from the SDDC Settings page.

The screenshot shows the VMware Cloud SDDC Settings page. The left sidebar includes options like Launchpad, Inventory, Subscriptions, Activity Log, Tools, Developer Center, Maintenance, and Notification Preferences. The main content area has tabs for Summary, Networking & Security, Storage, Add Ons, Maintenance, Troubleshooting, Settings (selected), and Support. Under the Settings tab, there are three main sections: SDDC (Management Appliances), vCenter Information (Default vCenter User Account, vSphere Client (HTML5), vCenter Server API Explorer, PowerCLI Connect, vCenter FQDN), and HCX Information (HCX FQDN, NSX Manager button default access, NSX Manager URLs). The HCX FQDN section shows details for 'hcx' with Public IP '172.30.161.215'.

The screenshot shows the vSphere Client Site Pairing dialog box. It displays two sites: RTP-HCX (IP: 192.168.20.254 port 443) and hcx (IP: 192.168.20.30 port 443). The 'Connect to Remote Site' dialog box is open, showing the 'Remote HCX URL' as 'http://hcx', 'Username' as 'cloudadmin@vmc.local', and a password field. The 'CONNECT' button is highlighted.

- To initiate the site pairing, click Connect.



VMware HCX Connector must be able to communicate with the HCX Cloud Manager IP over port 443.

- After the pairing is created, the newly configured site pairing is available on the HCX Dashboard.

## Step 5: Configure the network profile, compute profile, and service mesh

The VMware HCX Interconnect (HCX-IX) appliance provides secure tunnel capabilities over the internet and private connections to the target site that enable replication and vMotion-based capabilities. The interconnect provides encryption, traffic engineering, and an SD-WAN. To create the HCI-IX Interconnect Appliance, complete the following steps:

1. Under Infrastructure, select Interconnect > Multi-Site Service Mesh > Compute Profiles > Create Compute Profile.



Compute profiles contain the compute, storage, and network deployment parameters required to deploy an interconnect virtual appliance. They also specify which portion of the VMware data center will be accessible to the HCX service.

For detailed instructions, see [Creating a Compute Profile](#).

The screenshot shows the vSphere Client interface with the URL <https://a300-vcsa01.ehcdc.com/ui/app/plugin/com.vmware.hybridity/com.vmware.hcx.hciConnect>. The left sidebar is expanded to show the HCX section, specifically the Interconnect category. The main content area displays a 'hcxdemo' compute profile. It lists service resources (a300-vcsa01.ehcdc.com, A300-Cluster01), deployment containers (VM\_3510), and datastores (A300\_NFS\_DS04). Network settings include VM\_3510 (Management, vSphere Replication, Uplink, vMotion) and vDS-Switch0 (Unlimited). A note indicates that the profile is used in 2 Service Mesh(es). At the bottom are 'EDIT', 'DELETE', and 'REVIEW CONNECTION RULES' buttons.

2. After the compute profile is created, create the network profile by selecting Multi-Site Service Mesh > Network Profiles > Create Network Profile.
3. The network profile defines a range of IP address and networks that will be used by HCX for its virtual appliances.



This will require two or more IP address. These IP addresses will be assigned from the management network to virtual appliances.

The screenshot shows the vSphere Client interface for HCX. The left sidebar has sections for Site Pairing, Infrastructure, Services, and System. The 'Interconnect' section is selected. Under 'Interconnect', there are tabs for Compute Profiles, Service Mesh, Network Profiles, and Sentinel Management. The 'Service Mesh' tab is active. A specific network profile, 'VM\_3510', is listed. Its details include Backing: VM\_3510, MTU: 9000, IP Pools (IP Range: 172.21.254.80 - 172.21.254.95, IP Usage: 4/16, Prefix Length: 24, Gateway: 172.21.254.230). There are 'EDIT' and 'DELETE' buttons at the bottom.

For detailed instructions, see [Creating a Network Profile](#).



If you are connecting with an SD-WAN over the internet, you have to reserve public IPs under the Networking and Security section.

4. To create a service mesh, select the Service Mesh tab within the Interconnect option and select on-premises and VMC SDDC sites.

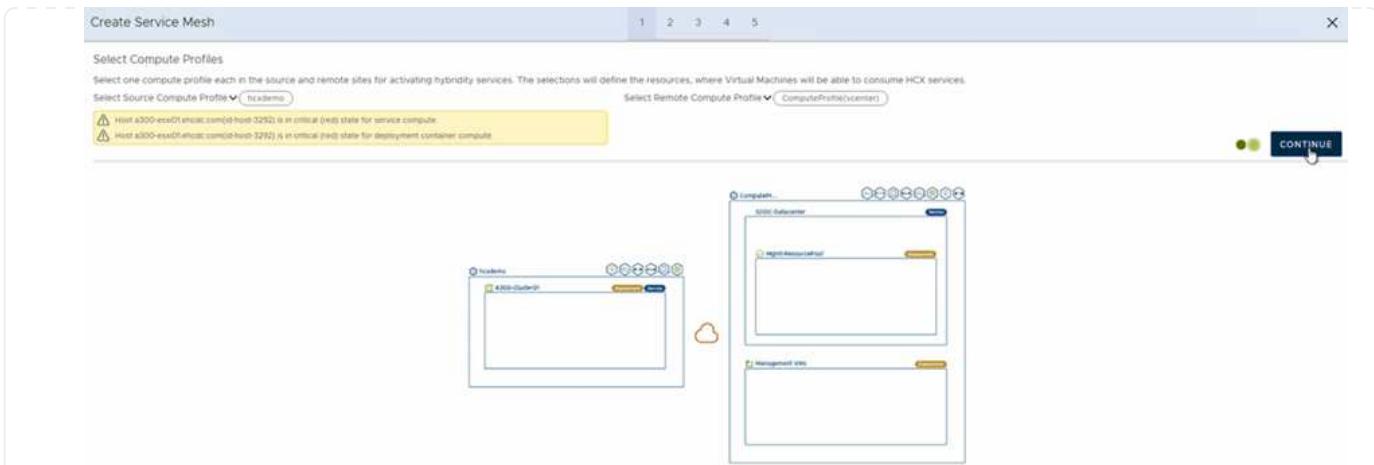
The service mesh establishes a local and remote compute and network profile pair.

The screenshot shows the VMware HCX interface. The left sidebar includes sections for Dashboard, Infrastructure, Site Pairing, Interconnect (selected), Transport Analytics, Services, Administration, and DICE. The 'Interconnect' section has tabs for Compute Profiles, Service Mesh, Network Profiles, and Sentinel Management. The 'Service Mesh' tab is active. A list of service mesh pairs is shown, with one entry named 'ICCO07'. It lists the source appliance as 'VMware-HCX-440' and the target as 'hcx.firebaseio.com'. Below the list are buttons for 'VIEW APPLIANCES', 'RESYNC', 'EDIT', 'DELETE', and 'MORE...'. At the top right, there is a 'CREATE SERVICE MESH' button.

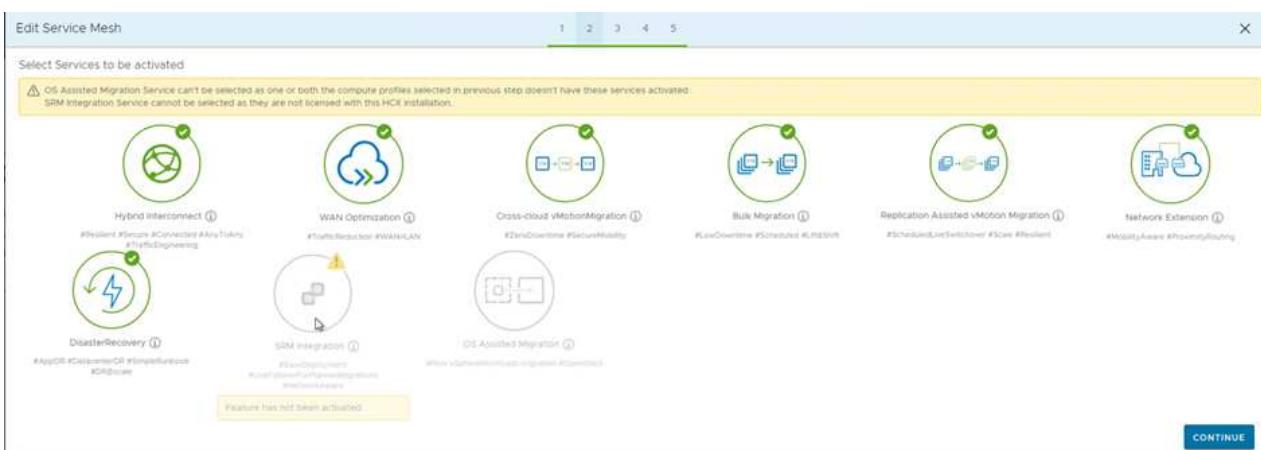


Part of this process involves deploying HCX appliances that will be automatically configured on both the source and target sites, creating a secure transport fabric.

5. Select the source and remote compute profiles and click Continue.



#### 6. Select the service to be activated and click Continue.



An HCX Enterprise license is required for Replication Assisted vMotion Migration, SRM Integration, and OS Assisted Migration.

#### 7. Create a name for the service mesh and click Finish to begin the creation process. The deployment should take approximately 30 minutes to complete. After the service mesh is configured, the virtual infrastructure and networking required to migrate the workload VMs has been created.

vsphere Client

https://a300-vcsa01.hcd.com/ui/app/plugin/com.vmware.hybridity/com.vmware.hcx.hybridConnect

67% Admin@vcsa01.hcd.com

### Interconnect

Multi-Site Service Mesh

Compte Profil Services Mesh Network Profil Sémantique management

**ICCO07**

Appliances Tasks

Topology Appliances

Créer Appliance Changer mot de passe Renommer appliance Mise à jour appliance

| Assistance Name | Assistance Type | IP Address    | Tunnel Status                    | Current Version | Available Version |
|-----------------|-----------------|---------------|----------------------------------|-----------------|-------------------|
| ICCO07-WO-H     | HDX WAN-OC      | IT2.21.254.89 | Transparent > Remote Replication | 4.4.0.0         | A.41.0            |
| ICCO07-AE-H     | HDX-NET-EXT     | IT2.21.254.89 | Transparent > Remote Replication | 4.4.0.0         | A.41.0            |
| ICCO07-WO-B     | HDX-WAN-OPT     |               |                                  | N/A             |                   |

8 Appliances

Appliances on hcx.Bebf3b0b7d0f4cc09e3f85.westeuropew.avs.azure.com-cloud

| Assistance Name | Assistance Type | IP Address    | Current Version |
|-----------------|-----------------|---------------|-----------------|
| ICCO07-WO-B     | HDX-WAN-OC      | IT2.30.198.17 | 4.4.0.0         |
| ICCO07-AE-B     | HDX-NET-EXT     | IT2.30.198.89 | 4.4.0.0         |
| ICCO07-WO-B     | HDX-WAN-OPT     |               | 7.3.0           |

## Step 6: Migrating Workloads

HCX provides bidirectional migration services between two or more distinct environments such as on-premises and VMC SDDCs. Application workloads can be migrated to and from HCX activated sites using a variety of migration technologies such as HCX bulk migration, HCX vMotion, HCX Cold migration, HCX Replication Assisted vMotion (available with HCX Enterprise edition), and HCX OS Assisted Migration (available with HCX Enterprise edition).

To learn more about available HCX migration technologies, see [VMware HCX Migration Types](#)

The HCX-IX appliance uses the Mobility Agent service to perform vMotion, Cold, and Replication Assisted vMotion (RAV) migrations.



The HCX-IX appliance adds the Mobility Agent service as a host object in the vCenter Server. The processor, memory, storage and networking resources displayed on this object do not represent actual consumption on the physical hypervisor hosting the IX appliance.

The screenshot shows the vSphere Client interface. On the left, the navigation tree displays a hierarchy: a300-vctaa01.ehcddc.com > A300-DataCenter > A300-Cluster01 > TempCluster > 172.21.254.80 > 172.21.254.82. The host 172.21.254.82 is currently selected. The main pane shows the host summary for 172.21.254.82. The host details are as follows:

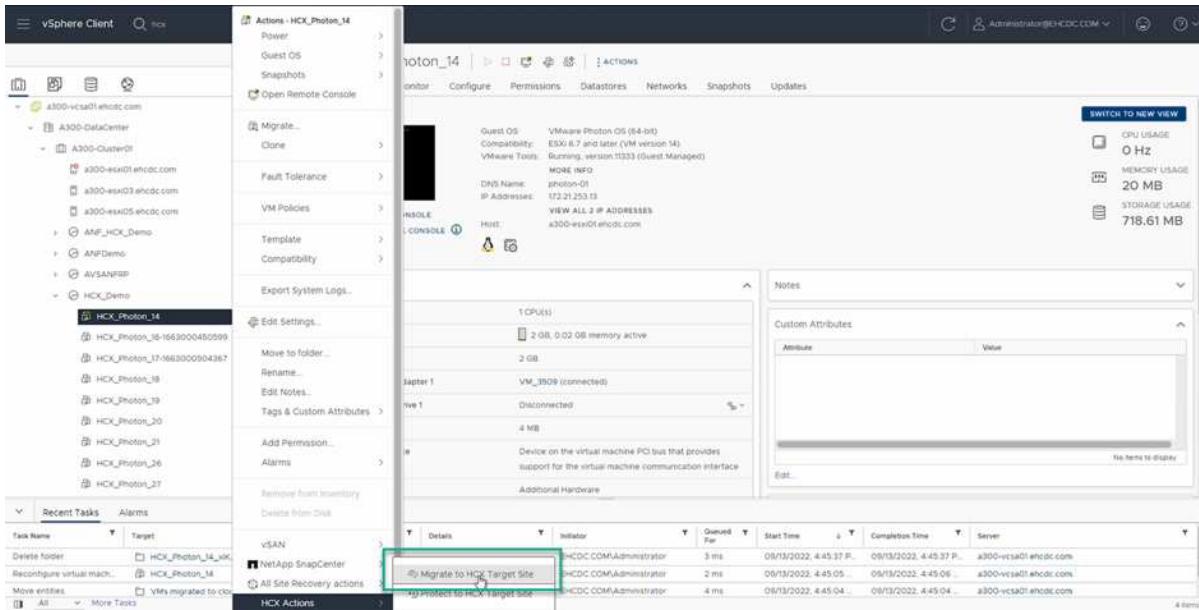
| Host Details       | Value                        |
|--------------------|------------------------------|
| Hypervisor         | VMware ESXi, 7.0.3, 20305777 |
| Model              | VMware Mobility Platform     |
| Processor Type     | VMware Virtual Processor     |
| Logical Processors | 768                          |
| NICs               | 8                            |
| Virtual Machines   | 0                            |
| State              | Connected                    |
| Uptime             | 29 days                      |

## VMware HCX vMotion

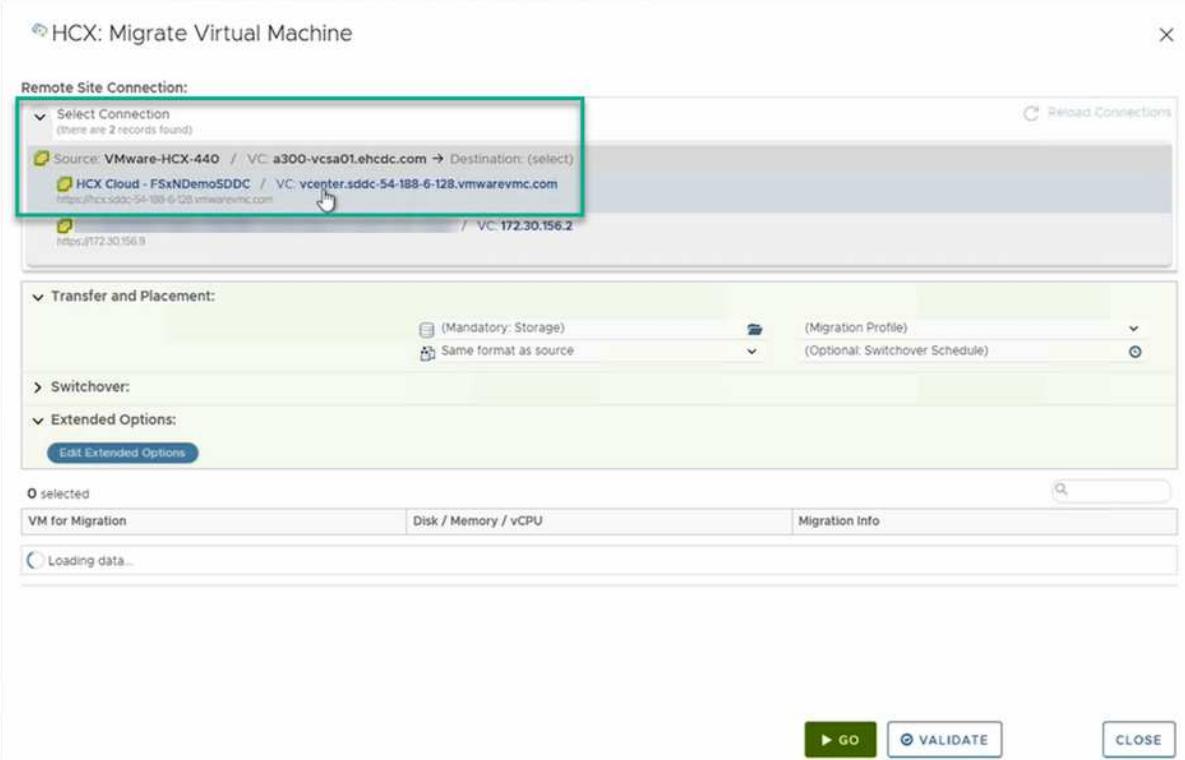
This section describes the HCX vMotion mechanism. This migration technology uses the VMware vMotion protocol to migrate a VM to VMC SDDC. The vMotion migration option is used for migrating the VM state of a single VM at a time. There is no service interruption during this migration method.

-  Network Extension should be in place (for the port group in which the VM is attached) in order to migrate the VM without the need to make an IP address change.

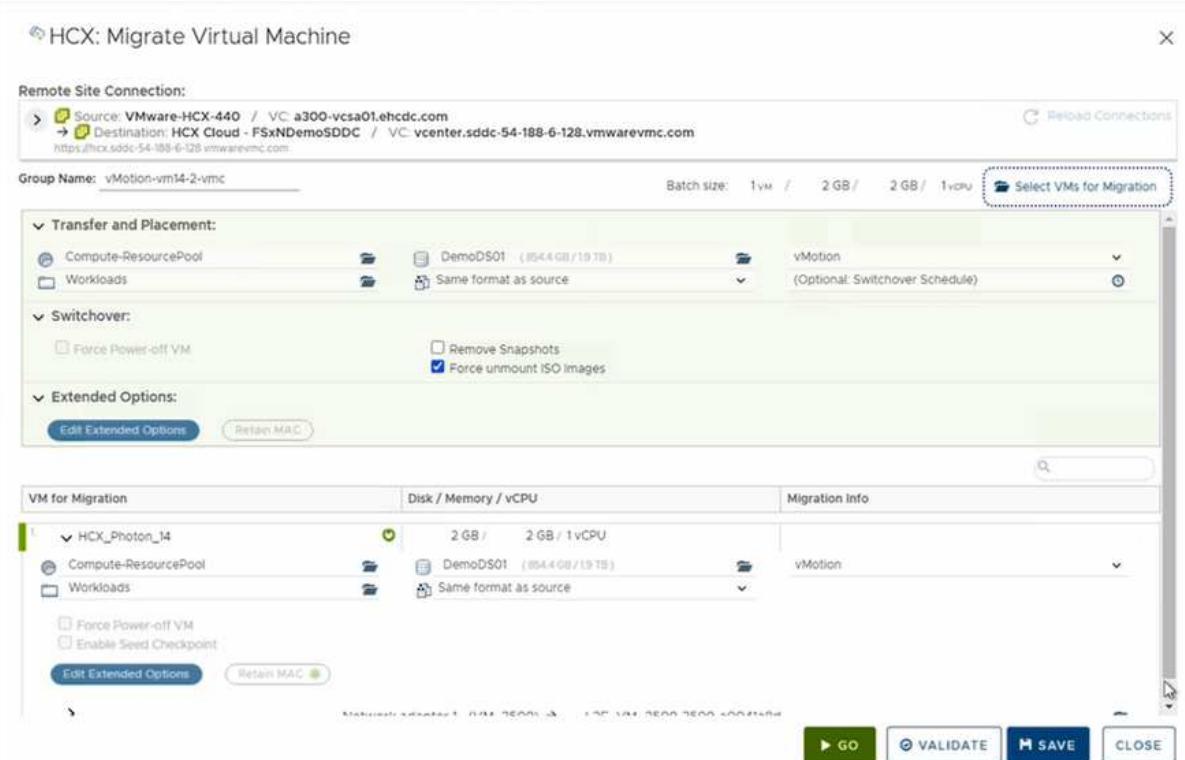
1. From the on-premises vSphere client, go to Inventory, right- click on the VM to be migrated, and select HCX Actions > Migrate to HCX Target Site.



2. In the Migrate Virtual Machine wizard, select the Remote Site Connection (target VMC SDDC).



3. Add a group name and under Transfer and Placement, update the mandatory fields (Cluster, Storage, and Destination Network), Click Validate.



4. After the validation checks are complete, click Go to initiate the migration.



The vMotion transfer captures the VM active memory, its execution state, its IP address, and its MAC address. For more information about the requirements and limitations of HCX vMotion, see [Understanding VMware HCX vMotion and Cold Migration](#).

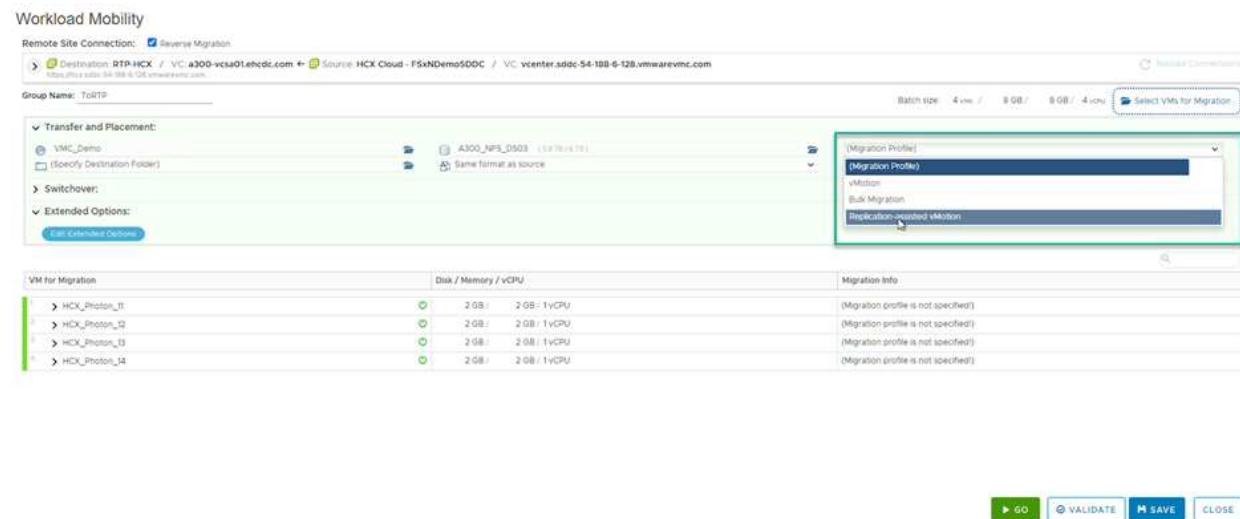
5. You can monitor the progress and completion of the vMotion from the HCX > Migration dashboard.

| Task Name                  | Target        | Status    | Details                         | Initiator               | Quiesce For | Start Time             | Completion Time        | Server               |
|----------------------------|---------------|-----------|---------------------------------|-------------------------|-------------|------------------------|------------------------|----------------------|
| Renocate virtual machine   | HCX_Photon_14 | 100%      | Migrating Virtual Machine ac... | EHCDC.COM\Administrator | 3 ms        | 09/03/2022, 4:39:08 .. | 09/03/2022, 4:39:08 .. | a300-vcsa01.hcdc.com |
| Refresh host storage sys.. | 172.21.254.82 | Completed |                                 | EHCDC.COM\Administrator | 3 ms        | 09/03/2022, 4:57:43 .. | 09/03/2022, 4:57:43 .. | a300-vcsa01.hcdc.com |

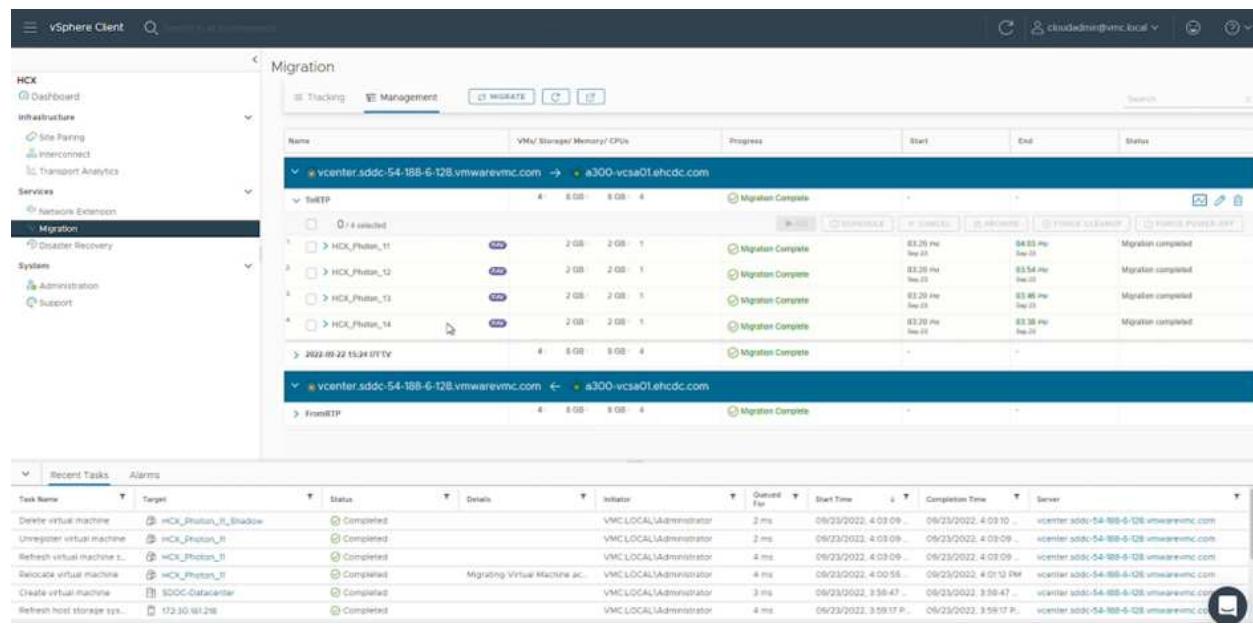
## VMware Replication Assisted vMotion

As you might have noticed from VMware documentation, VMware HCX Replication Assisted vMotion (RAV) combines the benefits of bulk migration and vMotion. Bulk migration uses vSphere Replication to migrate multiple VMs in parallel—the VM gets rebooted during switchover. HCX vMotion migrates with no downtime, but it is performed serially one VM at a time in a replication group. RAV replicates the VM in parallel and keeps it in sync until the switchover window. During the switchover process, it migrates one VM at a time with no downtime for the VM.

The following screenshot shows the migration profile as Replication Assisted vMotion.



The duration of the replication might be longer compared to the vMotion of a small number of VMs. With RAV, only sync the deltas and include the memory contents. The following is a screenshot of the migration status—it shows how the start time of the migration is the same and the end time is different for each VM.



For additional information about the HCX migration options and on how to migrate workloads from on-premises to VMware Cloud on AWS using HCX, see the [VMware HCX User Guide](#).



VMware HCX vMotion requires 100Mbps or higher throughput capability.



The target VMC FSx for ONTAP datastore must have sufficient space to accommodate the migration.

## Conclusion

Whether you are targeting all-cloud or hybrid cloud and data residing on any type/vendor storage in on-premises, Amazon FSx for NetApp ONTAP along with HCX provide excellent options to deploy and migrate the workloads while reducing the TCO by making the data requirements seamless to the application layer. Whatever the use case, choose VMC along with FSx for ONTAP datastore for rapid realization of cloud benefits, consistent infrastructure, and operations across on-premises and multiple clouds, bidirectional portability of workloads, and enterprise-grade capacity and performance. It is the same familiar process and procedures used to connect the storage and migrate VMs using VMware vSphere replication, VMware vMotion or even NFC copy.

## Takeaways

The key points of this document include:

- You can now use Amazon FSx ONTAP as a datastore with VMC SDDC.
- You can easily migrate data from any on-premises datacenter to VMC running with FSx for ONTAP datastore
- You can easily grow and shrink the FSx ONTAP datastore to meet the capacity and performance requirements during migration activity.

## Where to find additional information

To learn more about the information described in this document, refer to the following website links:

- VMware Cloud documentation

<https://docs.vmware.com/en/VMware-Cloud-on-AWS/>

- Amazon FSx for NetApp ONTAP documentation

<https://docs.aws.amazon.com/fsx/latest/ONTAPGuide>

VMware HCX User Guide

- <https://docs.vmware.com/en/VMware-HCX/4.4/hcx-user-guide/GUID-BFD7E194-CFE5-4259-B74B-991B26A51758.html>

## Region Availability – Supplemental NFS datastore for VMC

The availability of supplemental NFS datastores on AWS / VMC is defined by Amazon. First, you need to determine if both VMC and FSxN are available in a specified region. Next, you need to determine if the FSxN supplemental NFS datastore is supported in that region.

- Check the availability of VMC [here](#).
- Amazon's pricing guide offers information on where FSxN (FSx ONTAP) is available. You can find that information [here](#).
- Availability of the FSxN supplemental NFS datastore for VMC is coming soon.

While information is still being released, the following chart identifies the current support for VMC, FSxN and FSxN as a supplemental NFS datastore.

## Americas

| AWS Region                    | VMC Availability | FSx ONTAP Availability | NFS Datastore Availability |
|-------------------------------|------------------|------------------------|----------------------------|
| US East (Northern Virginia)   | Yes              | Yes                    | Yes                        |
| US East (Ohio)                | Yes              | Yes                    | Yes                        |
| US West (Northern California) | Yes              | No                     | No                         |
| US West (Oregon)              | Yes              | Yes                    | Yes                        |
| GovCloud (US West)            | Yes              | Yes                    | Yes                        |
| Canada (Central)              | Yes              | Yes                    | Yes                        |
| South America (Sao Paulo)     | Yes              | Yes                    | Yes                        |

Last updated on: June 2, 2022.

## EMEA

| AWS Region         | VMC Availability | FSx ONTAP Availability | NFS Datastore Availability |
|--------------------|------------------|------------------------|----------------------------|
| Europe (Ireland)   | Yes              | Yes                    | Yes                        |
| Europe (London)    | Yes              | Yes                    | Yes                        |
| Europe (Frankfurt) | Yes              | Yes                    | Yes                        |
| Europe (Paris)     | Yes              | Yes                    | Yes                        |
| Europe (Milan)     | Yes              | Yes                    | Yes                        |
| Europe (Stockholm) | Yes              | Yes                    | Yes                        |

Last updated on: June 2, 2022.

## Asia Pacific

| AWS Region               | VMC Availability | FSx ONTAP Availability | NFS Datastore Availability |
|--------------------------|------------------|------------------------|----------------------------|
| Asia Pacific (Sydney)    | Yes              | Yes                    | Yes                        |
| Asia Pacific (Tokyo)     | Yes              | Yes                    | Yes                        |
| Asia Pacific (Osaka)     | Yes              | No                     | No                         |
| Asia Pacific (Singapore) | Yes              | Yes                    | Yes                        |
| Asia Pacific (Seoul)     | Yes              | Yes                    | Yes                        |
| Asia Pacific (Mumbai)    | Yes              | Yes                    | Yes                        |
| Asia Pacific (Jakarta)   | No               | No                     | No                         |
| Asia Pacific (Hong Kong) | Yes              | Yes                    | Yes                        |

Last updated on: September 28, 2022.

## **Copyright information**

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

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

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

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

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

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

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

## **Trademark information**

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