



## **NetApp for Azure / AVS**

NetApp Solutions

NetApp

August 15, 2023

# Table of Contents

NetApp Hybrid Multicloud Solutions for Azure / AVS .....	1
Protecting Workloads on Azure / AVS .....	1
Migrating Workloads on Azure / AVS .....	53
Region Availability – Supplemental NFS datastore for ANF .....	71

# **NetApp Hybrid Multicloud Solutions for Azure / AVS**

## **Protecting Workloads on Azure / AVS**

### **Disaster Recovery with ANF and JetStream**

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). Using the VMware VAAI framework, on-premises VMware workloads can be replicated to Azure Blob storage and recovered, enabling minimal or close to no data loss and near-zero RTO.

JetStream DR can be used to seamlessly recover the workloads replicated from on-premises to AVS and specifically to Azure NetApp Files. It enables cost-effective disaster recovery by using minimal resources at the DR site and cost-effective cloud storage. JetStream DR automates recovery to ANF datastores via Azure Blob Storage. JetStream DR recovers independent VMs or groups of related VMs into recovery site infrastructure according to network mapping and provides point-in-time recovery for ransomware protection.

This document provides an understanding of the JetStream DR principles of operations and its main components.

## Solution deployment overview

1. Install JetStream DR software in the on-premises data center.
  - a. Download the JetStream DR software bundle from Azure Marketplace (ZIP) and deploy the JetStream DR MSA (OVA) in the designated cluster.
  - b. Configure the cluster with the I/O filter package (install JetStream VIB).
  - c. Provision Azure Blob (Azure Storage Account) in the same region as the DR AVS cluster.
  - d. Deploy DRVA appliances and assign replication log volumes (VMDK from existing datastore or shared iSCSI storage).
  - e. Create protected domains (groups of related VMs) and assign DRVAs and Azure Blob Storage/ANF.
  - f. Start protection.
2. Install JetStream DR software in the Azure VMware Solution private cloud.
  - a. Use the Run command to install and configure JetStream DR.
  - b. Add the same Azure Blob container and discover domains using the Scan Domains option.
  - c. Deploy required DRVA appliances.
  - d. Create replication log volumes using available vSAN or ANF datastores.
  - e. Import protected domains and configure RocVA (recovery VA) to use ANF datastore for VM placements.
  - f. Select the appropriate failover option and start continuous rehydration for near-zero RTO domains or VMs.
3. During a disaster event, trigger failover to Azure NetApp Files datastores in the designated AVS DR site.
4. Invoke fallback to the protected site after the protected site has been recovered. Before starting, make sure that the prerequisites are met as indicated in this [link](#) and also run the Bandwidth Testing Tool (BWT) provided by JetStream Software to evaluate the potential performance of Azure Blob storage and its replication bandwidth when used with JetStream DR software. After the pre-requisites, including connectivity, are in place, set up and subscribe to JetStream DR for AVS from the [Azure Marketplace](#). After the software bundle is downloaded, proceed with the installation process described above.

When planning and starting protection for a large number of VMs (for example, 100+), use the Capacity Planning Tool (CPT) from the JetStream DR Automation Toolkit. Provide a list of VMs to be protected together with their RTO and recovery group preferences, and then run CPT.

CPT performs the following functions:

- Combining VMs into protection domains according to their RTO.
- Defining the optimal number of DRVAs and their resources.
- Estimating required replication bandwidth.
- Identifying replication log volume characteristics (capacity, bandwidth, and so on).
- Estimating required object storage capacity, and more.



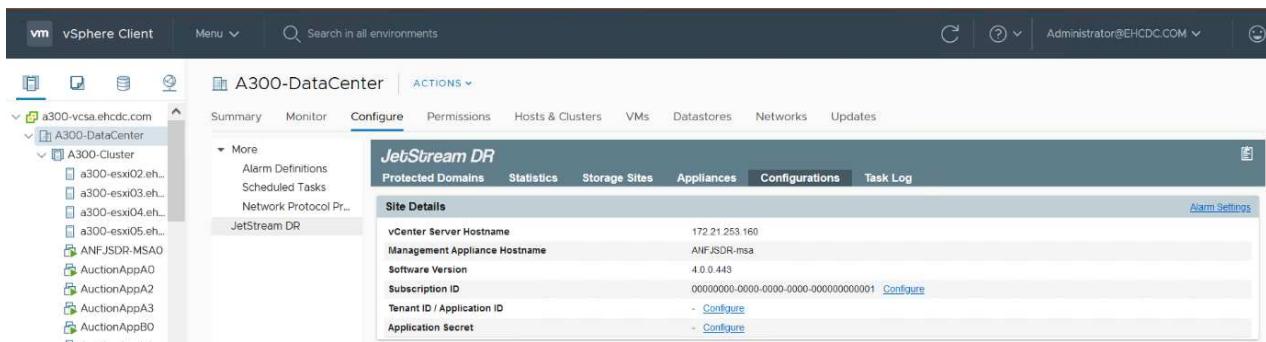
The number and content of domains prescribed depend upon various VM characteristics such as average IOPS, total capacity, priority (which defines failover order), RTO, and others.

## Install JetStream DR in On-Premises Datacenter

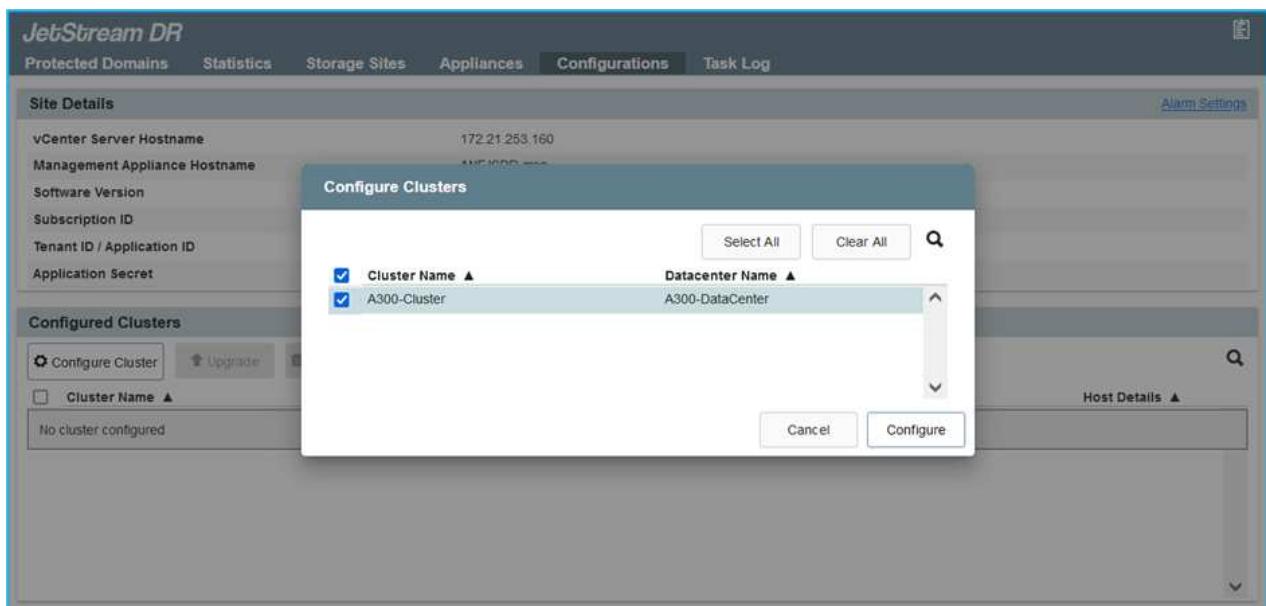
JetStream DR software consists of three major components: JetStream DR Management Server Virtual Appliance (MSA), DR Virtual Appliance (DRVA), and host components (I/O Filter packages). MSA is used to install and configure host components on the compute cluster and then to administer JetStream DR software. The following list provides a high-level description of the installation process:

## How to install JetStream DR for on-premises

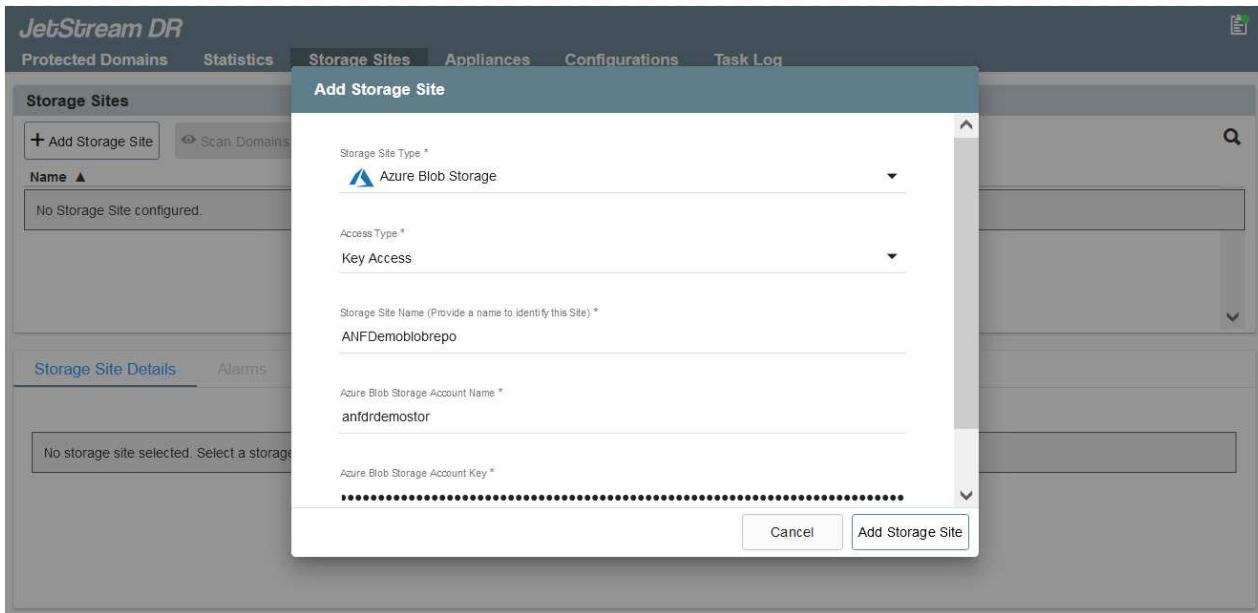
1. Check prerequisites.
2. Run the Capacity Planning Tool for resource and configuration recommendations (optional but recommended for proof-of-concept trials).
3. Deploy the JetStream DR MSA to a vSphere host in the designated cluster.
4. Launch the MSA using its DNS name in a browser.
5. Register the vCenter server with the MSA. To perform the installation, complete the following detailed steps:
6. After JetStream DR MSA has been deployed and the vCenter Server has been registered, access the JetStream DR plug-in using the vSphere Web Client. This can be done by navigating to Datacenter > Configure > JetStream DR.



7. From the JetStream DR interface, select the appropriate cluster.



8. Configure the cluster with the I/O filter package.

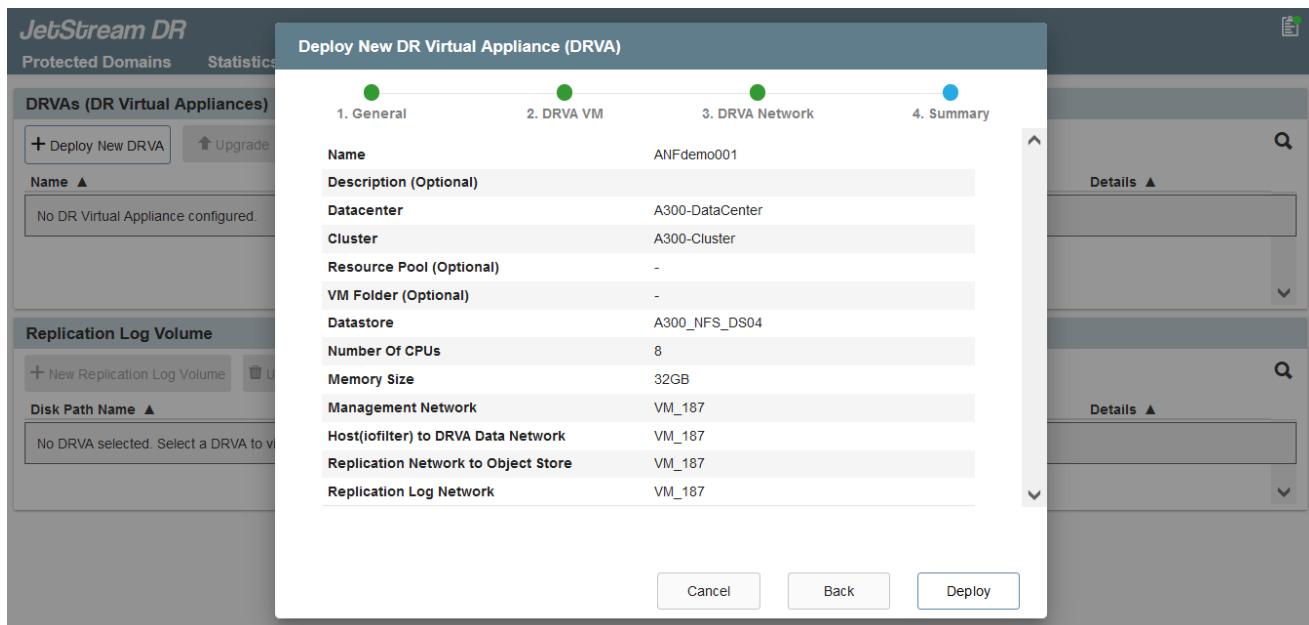


9. Add Azure Blob Storage located at the recovery site.
10. Deploy a DR Virtual Appliance (DRVA) from the Appliances tab.



DRVAs can be automatically created by CPT, but for POC trials we recommend configuring and running the DR cycle manually (start protection > failover > fallback).

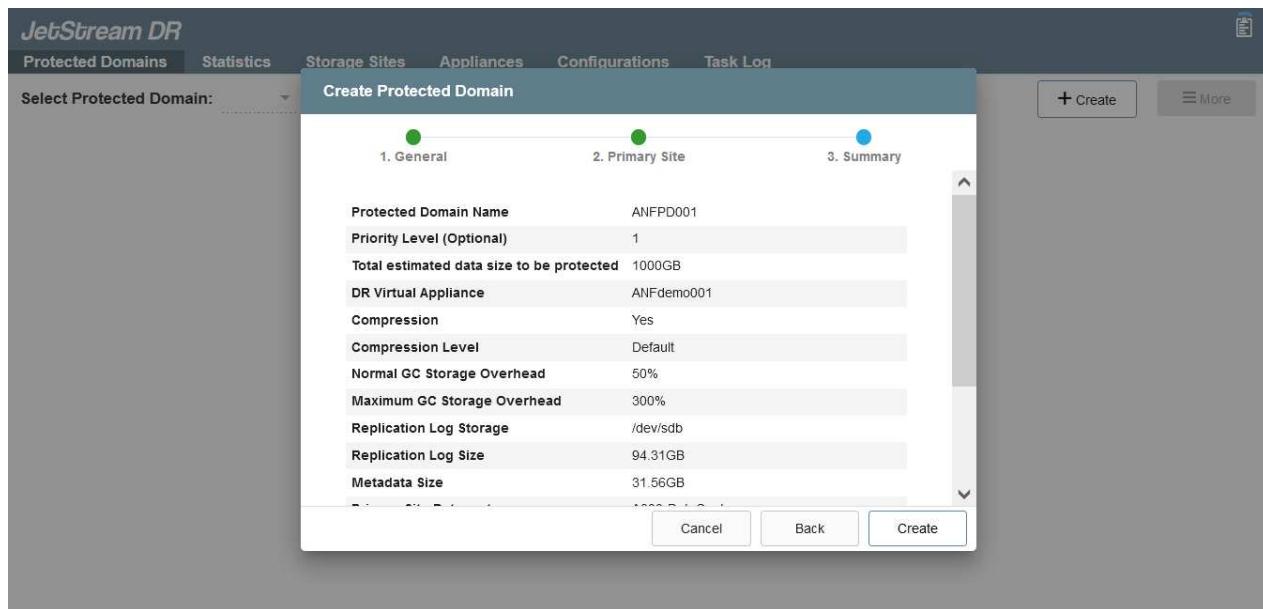
The JetStream DRVA is a virtual appliance that facilitates key functions in the data replication process. A protected cluster must contain at least one DRVA, and typically one DRVA is configured per host. Each DRVA can manage multiple protected domains.



In this example, four DRVA's were created for 80 virtual machines.

1. Create replication log volumes for each DRVA using VMDK from the datastores available or independent shared iSCSI storage pools.
2. From the Protected Domains tab, create the required number of protected domains using information

about the Azure Blob Storage site, DRVA instance, and replication log. A protected domain defines a specific VM or set of VMs within the cluster that are protected together and assigned a priority order for failover/failback operations.



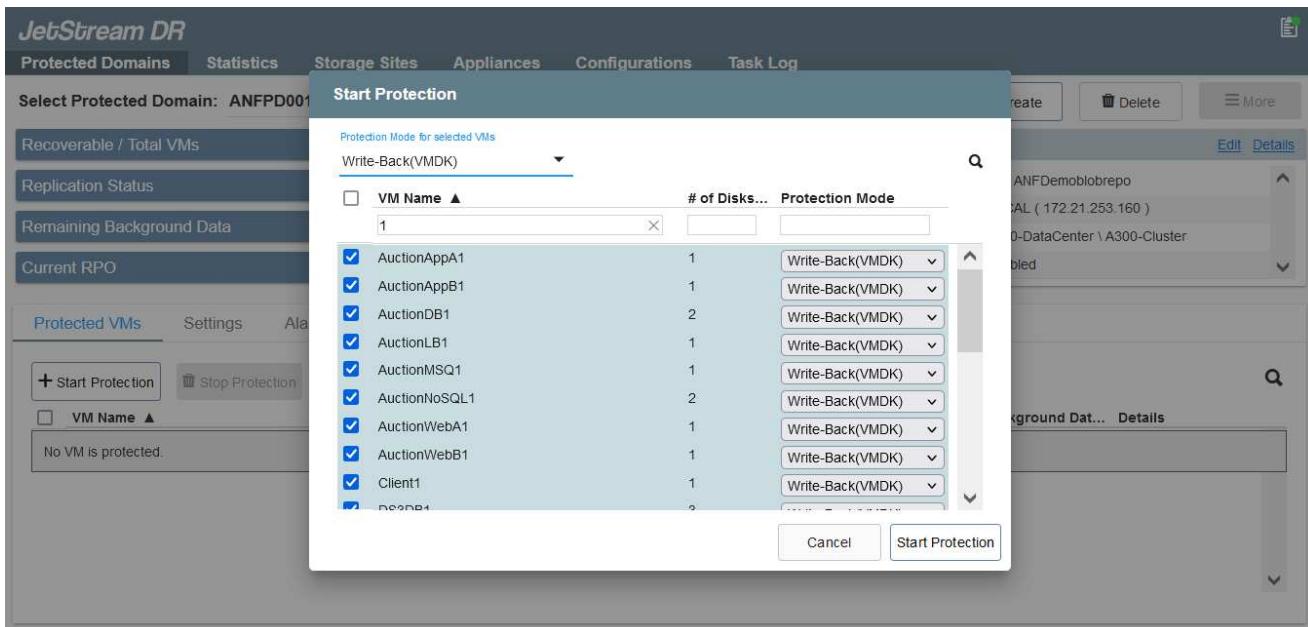
3. Select VMs you want to protect and start VM protection of the protected domain. This begins data replication to the designated Blob Store.



Verify that the same protection mode is used for all VMs in a protected domain.



Write- Back(VMDK) mode can offer higher performance.



Verify that replication log volumes are placed on high performance storage.



Failover run books can be configured to group the VMs (called Recovery Group), set boot order sequence, and modify the CPU/memory settings along with IP configurations.

## Install JetStream DR for AVS in an Azure VMware Solution private cloud using the Run command

A best practice for a recovery site (AVS) is to create a three-node pilot-light cluster in advance. This allows the recovery site infrastructure to be preconfigured, including the following items:

- Destination networking segments, firewalls, services like DHCP and DNS, and so on.
- Installation of JetStream DR for AVS
- Configuration of ANF volumes as datastores, and moreJetStream DR supports near-zero RTO mode for mission- critical domains. For these domains, destination storage should be preinstalled. ANF is a recommended storage type in this case.



Network configuration including segment creation should be configured on the AVS cluster to match on-premises requirements.

Depending on the SLA and RTO requirements, continuous failover or regular (standard) failover mode can be used. For near-zero RTO, continuous rehydration should be started at the recovery site.

## How to install JetStream DR for AVS in a private cloud

To install JetStream DR for AVS on an Azure VMware Solution private cloud, complete the following steps:

1. From the Azure portal, go to the Azure VMware solution, select the private cloud, and select Run command > Packages > JSDR.Configuration.



The default CloudAdmin user in Azure VMware Solution doesn't have sufficient privileges to install JetStream DR for AVS. Azure VMware Solution enables simplified and automated installation of JetStream DR by invoking the Azure VMware Solution Run command for JetStream DR.

The following screenshot shows installation using a DHCP-based IP address.

The screenshot shows the Microsoft Azure portal interface for running commands on an Azure VMware Solution private cloud named 'ANFDataClus'. The left sidebar shows various management options like Access control, Tags, Diagnose and solve problems, Settings, Manage, Workload Networking, and Operations. The main area is titled 'Run command - Install-JetDRWithDHCP' and displays a list of cmdlets under the 'JSDR.Configuration' package. The cmdlets listed are: Disable-JetDRForCluster, Enable-JetDRForCluster, Install-JetDRWithDHCP, Install-JetDRWithStaticIP, Invoke-PreflightJetDRInstall, Invoke-PreflightJetDRUninstall, and Uninstall-JetDR. The 'Install-JetDRWithDHCP' cmdlet is selected. On the right, there are detailed configuration fields for the command, including 'RegisterWithIp' set to 'True', 'ProtectedCluster' set to 'Cluster-1', 'Datastore' set to 'vsanDatastore', 'VMName' set to 'anfjpsval-msa', 'Cluster' set to 'Cluster-1', 'Credential' with 'Username' 'root' and 'Password' masked, 'HostName' set to 'anfjpsval-msa', 'Network' set to 'DRSeg', and 'Retain up to' set to '2 days'.

2. After JetStream DR for AVS installation is complete, refresh the browser. To access the JetStream DR UI, go to SDDC Datacenter > Configure > JetStream DR.

## JetStream DR

Protected Domains   Statistics   Storage Sites   Appliances   Configurations   Task Log

### Site Details

[Alarm Settings](#)

vCenter Server Hostname 172.30.156.2

Management Appliance Hostname anfjsval-msa

Software Version 4.0.2.450

Subscription ID - [Configure](#)

Tenant ID / Application ID - [Configure](#)

- [Configure](#)

#### Application Secret

[Configure Cluster](#)

[Upgrade](#)

[Unconfigure](#)

[Resolve Configure Issue](#)



Cluster Name ▲

Datacenter Name ▲

Status ▲

Software Version ▲

Host Details ▲

Cluster-1

SDDC-Datacenter

Ok

4.0.2.132

[Details](#)

- From the JetStream DR interface, add the Azure Blob Storage account that was used to protect the on-premises cluster as a storage site and then run the Scan Domains option.

Available Protected Domain(s) For Import

Protected Domain ...	Description	Recoverable V...	VMs ...	Import
ANFPD000	Protected Domain Tile0	20	20	<a href="#">Import</a>
ANFPD001	-	20	20	<a href="#">Import</a>
ANFPD002	Protected Domain 02	20	20	<a href="#">Import</a>
ANFPD003	Protected Domain Tile 03	20	20	<a href="#">Import</a>

[Close](#)

- After the protected domains are imported, deploy DRVA appliances. In this example, continuous rehydration is started manually from the recovery site using the JetStream DR UI.



These steps can also be automated using CPT created plans.

- Create replication log volumes using available vSAN or ANF datastores.
- Import the protected domains and configure the Recovery VA to use the ANF datastore for VM placements.



Make sure that DHCP is enabled on the selected segment and enough IPs are available. Dynamic IPs are temporarily used while domains are recovering. Each recovering VM (including continuous rehydration) requires an individual dynamic IP. After recovery is complete, the IP is released and can be reused.

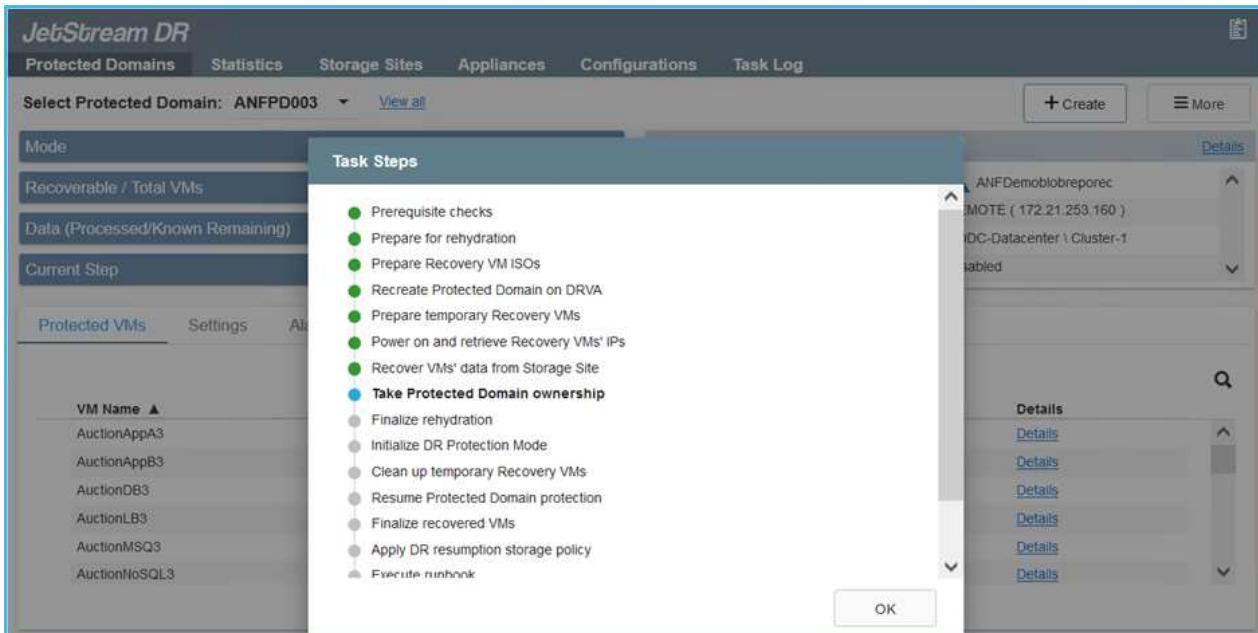
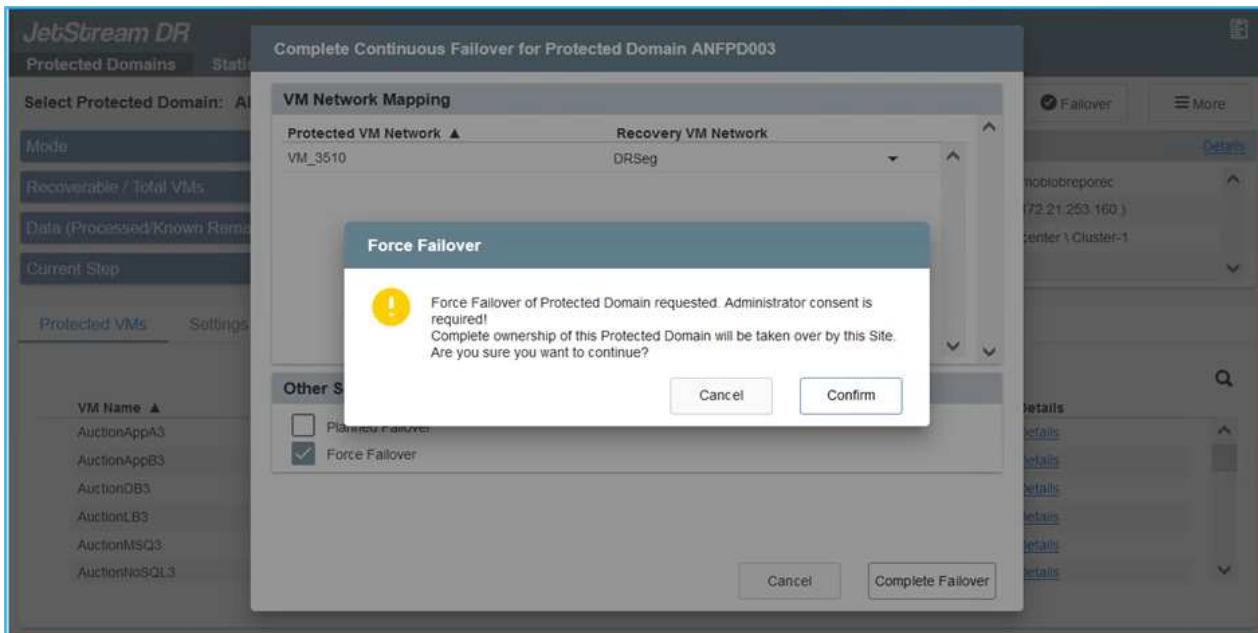
7. Select the appropriate failover option (continuous failover or failover). In this example, continuous rehydration (continuous failover) is selected.

## Performing Failover / Fallback

## How to perform a Failover / Failback

1. After a disaster occurs in the protected cluster of the on-premises environment (partial or full failure), trigger the failover.

- i CPT can be used to execute the failover plan to recover the VMs from Azure Blob Storage into the AVS cluster recovery site.
- i After failover (for continuous or standard rehydration) when the protected VMs have been started in AVS, protection is automatically resumed and JetStream DR continues to replicate their data into the appropriate/original containers in Azure Blob Storage.



The task bar shows progress of failover activities.

- When the task is complete, access the recovered VMs and business continues as normal.

**Protected Domains**   **Statistics**

**Continuous Rehydration Task Result**

**Select Protected Domain:** ANFPD003

**Mode**

**Recoverable / Total VMs**

**Replication Status**

**Remaining Background Data**

**Current RPO**

**Protected VMs**   **Settings**

**+ Start Protection**   **Stop Protection**

Protected Domain	
VM Name	ANFPD003
VMs Recovery Status	Success
Total VMs Recovered	20
testFGP0 Status:	
Pre-script Execution Status	Not defined
Runbook Execution Status	Success
Post-script Execution Status	Not defined

**Protected VMs**

- VM Name: AuctionAppA3, AuctionAppB3, AuctionDB3, AuctionLB3, AuctionMSQ3, AuctionNoSQL3

**Details**

**Dismiss**

After the primary site is up and running again, failback can be performed. VM protection is resumed and data consistency should be checked.

- Restore the on-premises environment. Depending upon the type of disaster incident, it might be necessary to restore and/or verify the configuration of the protected cluster. If necessary, JetStream DR software might need to be reinstalled.



Note: The `recovery_utility_prepare_failback` script provided in the Automation Toolkit can be used to help clean the original protected site of any obsolete VMs, domain information, and so on.

- Access the restored on-premises environment, go to the Jetstream DR UI, and select the appropriate protected domain. After the protected site is ready for failback, select the Failback option in the UI.

**Protected Domains**   **Statistics**   **Storage Sites**   **Appliances**   **Configurations**   **Task Log**

**Select Protected Domain:** ANFPD003   [View all](#)

**Mode**   **Running in Failover**

**Active Site**   **172.30.156.2**

**Recoverable / Total VMs**   **20 / 20**

**Protected VMs**   **Settings**   **Alarms**

**Configurations**

- Restore**
- Resume Continuous Rehydration**
- <-- Failback**

VM Name	Protection Status	Protection Mode	Details
AuctionAppA3	Recoverable	Write-Back(VMDK)	<a href="#">Details</a>
AuctionAppB3	Recoverable	Write-Back(VMDK)	<a href="#">Details</a>
AuctionDB3	Recoverable	Write-Back(VMDK)	<a href="#">Details</a>
AuctionLB3	Recoverable	Write-Back(VMDK)	<a href="#">Details</a>
AuctionMSQ3	Recoverable	Write-Back(VMDK)	<a href="#">Details</a>
AuctionNoSQL3	Recoverable	Write-Back(VMDK)	<a href="#">Details</a>



The CPT generated fallback plan can also be used to initiate the return of the VMs and their data from the object store back to the original VMware environment.



Specify the maximum delay after pausing VMs in the recovery site and restarting in the protected site. This time includes completing replication after stopping failover VMs, the time to clean recovery site, and the time to recreate VMs in protected site. The NetApp recommended value is 10 minutes.

Complete the fallback process, and then confirm the resumption of VM protection and data consistency.

## Ransomware Recovery

Recovering from ransomware can be a daunting task. Specifically, it can be hard for IT organizations to determine the safe point of return and, once determined, how to ensure that recovered workloads are safeguarded from the attacks reoccurring (from sleeping malware or through vulnerable applications).

JetStream DR for AVS together with Azure NetApp Files datastores can address these concerns by allowing organizations to recover from available points in time, so that workloads are recovered to a functional, isolated network if required. Recovery allows applications to function and communicate with each other while not exposing them to north-south traffic, thereby giving security teams a safe place to perform forensics and other necessary remediation.

The screenshot shows the JetStream DR interface with the following details:

- Protected Domains:** Fallback Protected Domain
- Mode:** Active Site
- Recoverable / Total VMs:** Protected VMs
- Protected Domain Name:** ANFPD003
- Fallback Datacenter:** A300-DataCenter
- Fallback Cluster:** A300-Cluster
- Fallback Resource Pool:** -
- VM Folder (Optional):** -
- Fallback Datastore:** A300\_NFS\_DS02
- Maximum Delay After Stopping:** 60 Minutes
- Internal Network:** VM\_187
- External Replication Network:** VM\_187
- Management Network:** VM\_187
- VM Name:** AuctionAppA3, AuctionAppB3, AuctionDB3, AuctionLB3, AuctionMSQ3, AuctionNoSQL3
- Status:** Recoverable (Write-Back(VMDK))

Buttons at the bottom include: Cancel, Back, and Fallback.

## Disaster Recovery with CVO and AVS (guest-connected storage)

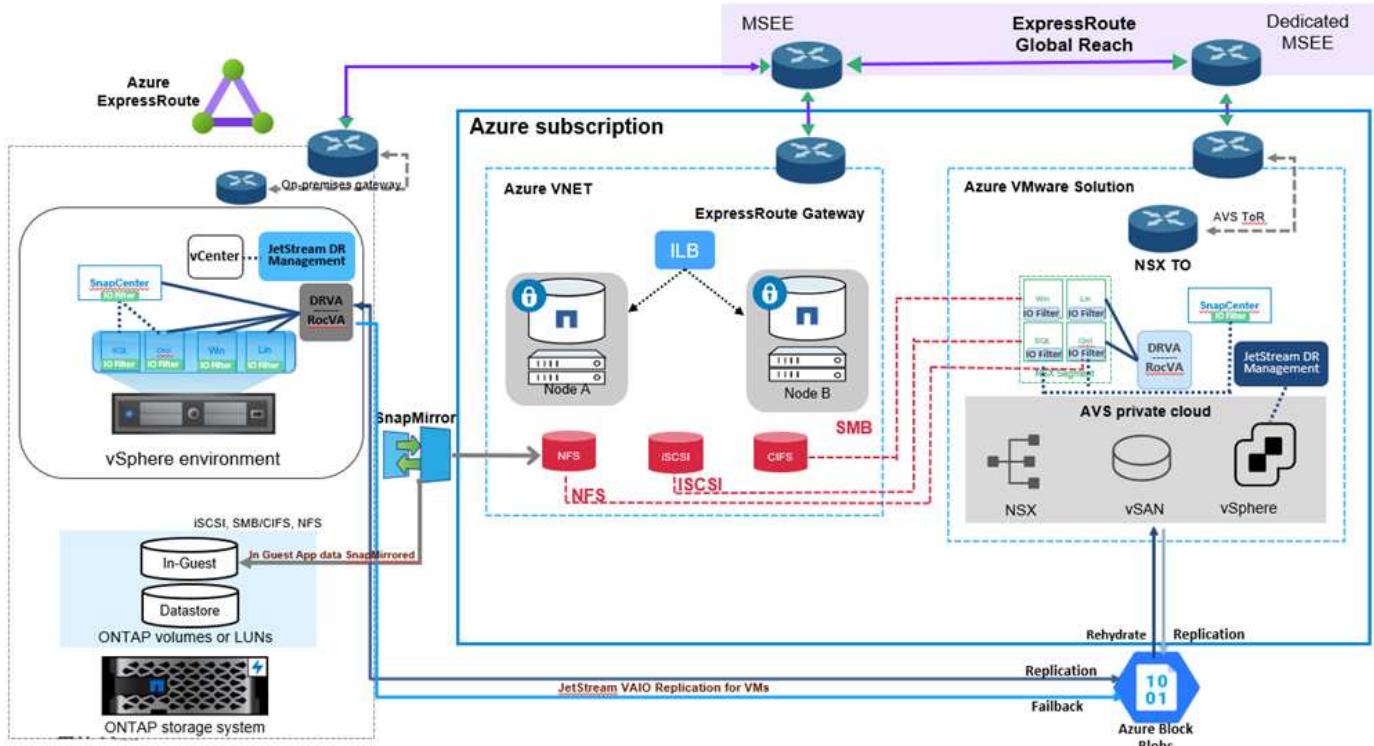
### Overview

Authors: Ravi BCB and Niyaz Mohamed, NetApp

Disaster recovery to cloud is a resilient and cost-effective way of protecting workloads against site outages and data corruption events such as ransomware. With NetApp SnapMirror, on-premises VMware workloads that use guest-connected storage can be replicated to NetApp Cloud Volumes ONTAP running in Azure. This covers application data; however, what about the actual VMs themselves. Disaster recovery should cover all dependent components, including virtual machines, VMDKs, application data, and more. To accomplish this,

SnapMirror along with Jetstream can be used to seamlessly recover workloads replicated from on-premises to Cloud Volumes ONTAP while using vSAN storage for VM VMDKs.

This document provides a step-by-step approach for setting up and performing disaster recovery that uses NetApp SnapMirror, JetStream, and the Azure VMware Solution (AVS).



## Assumptions

This document focuses on in-guest storage for application data (also known as guest connected), and we assume that the on-premises environment is using SnapCenter for application-consistent backups.

**i** This document applies to any third-party backup or recovery solution. Depending on the solution used in the environment, follow best practices to create backup policies that meet organizational SLAs.

For connectivity between the on-premises environment and the Azure virtual network, use the express route global reach or a virtual WAN with a VPN gateway. Segments should be created based on the on-premises VLAN design.

**i** There are multiple options for connecting on-premises datacenters to Azure, which prevents us from outlining a specific workflow in this document. Refer to the Azure documentation for the appropriate on-premises-to-Azure connectivity method.

## Deploying the DR Solution

### Solution Deployment Overview

1. Make sure that application data is backed up using SnapCenter with the necessary RPO requirements.

2. Provision Cloud Volumes ONTAP with the correct instance size using Cloud manager within the appropriate subscription and virtual network.
  - a. Configure SnapMirror for the relevant application volumes.
  - b. Update the backup policies in SnapCenter to trigger SnapMirror updates after the scheduled jobs.
3. Install the JetStream DR software in the on-premises data center and start protection for virtual machines.
4. Install JetStream DR software in the Azure VMware Solution private cloud.
5. During a disaster event, break the SnapMirror relationship using Cloud Manager and trigger failover of virtual machines to Azure NetApp Files or to vSAN datastores in the designated AVS DR site.
  - a. Reconnect the iSCSI LUNs and NFS mounts for the application VMs.
6. Invoke failback to the protected site by reverse resyncing SnapMirror after the primary site has been recovered.

## Deployment Details

### Configure CVO on Azure and replicate volumes to CVO

The first step is to configure Cloud Volumes ONTAP on Azure ([Link](#)) and replicate the desired volumes to Cloud Volumes ONTAP with the desired frequencies and snapshot retentions.

Health Status	Source Volume	Target Volume	Total Transfer Time	Status	Mirror State	Last Successful Transfer	...
✓	gcsdrsqldb_sc46_ntaphci-a300e9u25	gcsdrsqldb_sc46_copy_ANFCVODRDemo	17 seconds	idle	snapmirrored	May 6, 2022, 11:43:18 AM 105.06 KiB	...
✓	gcsdrsqlhld_sc46_copy_ANFCVODRDemo	gcsdrsqlhld_sc46_ntaphci-a300e9u25	7 seconds	idle	snapmirrored	May 6, 2022, 11:42:20 AM 7.22 MiB	...
✓	gcsdrsqllog_sc46_ntaphci-a300e9u25	gcsdrsqllog_sc46_copy_ANFCVODRDemo	16 seconds	idle	snapmirrored	May 6, 2022, 11:43:52 AM 130.69 KiB	...

## Configure AVS hosts and CVO data access

Two important factors to consider when deploying the SDDC are the size of the SDDC cluster in the Azure VMware solution and how long to keep the SDDC in service. These two key considerations for a disaster recovery solution help reduce the overall operational costs. The SDDC can be as small as three hosts, all the way up to a multi-host cluster in a full-scale deployment.

The decision to deploy an AVS cluster is primarily based on the RPO/RTO requirements. With the Azure VMware solution, the SDDC can be provisioned just in time in preparation for either testing or an actual disaster event. An SDDC deployed just in time saves on ESXi host costs when you are not dealing with a disaster. However, this form of deployment affects the RTO by a few of hours while SDDC is being provisioned.

The most common deployed option is to have SDDC running in an always-on, pilot-light mode of operation. This option provides a small footprint of three hosts that are always available, and it also speeds up recovery operations by providing a running baseline for simulation activities and compliance checks, thus avoiding the risk of operational drift between the production and DR sites. The pilot-light cluster can be scaled up quickly to the desired level when needed to handle an actual DR event.

To configure AVS SDDC (be it on-demand or in pilot-light mode), see [Deploy and configure the Virtualization Environment on Azure](#). As a prerequisite, verify that the guest VMs residing on the AVS hosts are able to consume data from Cloud Volumes ONTAP after connectivity has been established.

After Cloud Volumes ONTAP and AVS have been configured properly, begin configuring Jetstream to automate the recovery of on-premises workloads to AVS (VMs with application VMDKs and VMs with in-guest storage) by using the VAIO mechanism and by leveraging SnapMirror for application volumes copies to Cloud Volumes ONTAP.

## Install JetStream DR in on-premises datacenter

JetStream DR software consists of three major components: the JetStream DR Management Server Virtual Appliance (MSA), the DR Virtual Appliance (DRVA), and host components (I/O filter packages). The MSA is used to install and configure host components on the compute cluster and then to administer JetStream DR software. The installation process is as follows:

1. Check the prerequisites.
2. Run the Capacity Planning Tool for resource and configuration recommendations.
3. Deploy the JetStream DR MSA to each vSphere host in the designated cluster.
4. Launch the MSA using its DNS name in a browser.
5. Register the vCenter server with the MSA.
6. After JetStream DR MSA has been deployed and the vCenter Server has been registered, navigate to the JetStream DR plug-in with the vSphere Web Client. This can be done by navigating to Datacenter > Configure > JetStream DR.

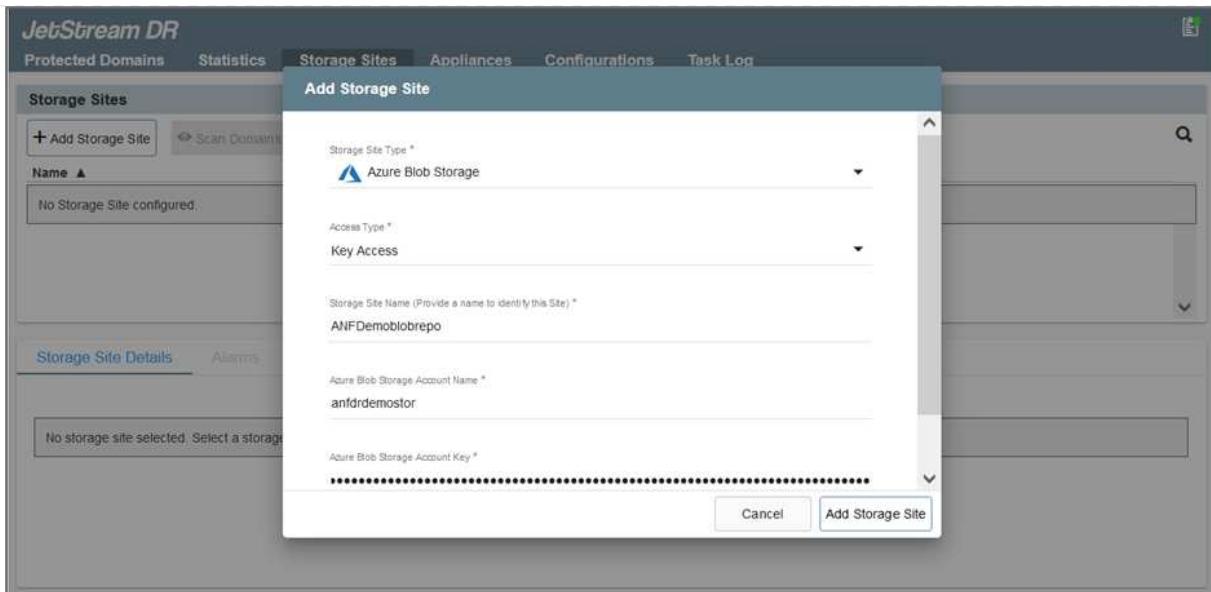
The screenshot shows the vSphere Client interface with the title bar "vSphere Client" and "Administrator@EHCDC.COM". The main navigation bar includes "Menu", "Search in all environments", and "Actions". Below the navigation bar, the left sidebar shows a tree structure with "a300-vcsa.ehcdc.com" expanded, revealing "A300-DataCenter" which further expands to "A300-Cluster" containing "a300-esxi02.eh...", "a300-esxi03.eh...", "a300-esxi04.eh...", "a300-esxi05.eh...", "ANFJSDR-MSA", "AuctionAppA0", "AuctionAppA2", "AuctionAppA3", and "AuctionAppB0". The main content area is titled "JetStream DR" and contains tabs for "Protected Domains", "Statistics", "Storage Sites", "Appliances", "Configurations", and "Task Log". The "Configurations" tab is selected. Under "Site Details", there are fields for "vCenter Server Hostname" (172.21.253.160), "Management Appliance Hostname" (ANFJSDR-msa), "Software Version" (4.0.0.443), "Subscription ID" (00000000-0000-0000-0000-000000000001), "Tenant ID / Application ID" (Configure), and "Application Secret" (Configure). An "Alarm Settings" link is also present.

7. From the JetStream DR interface, complete the following tasks:

- a. Configure the cluster with the I/O filter package.

The screenshot shows the JetStream DR Configuration interface with the "Configurations" tab selected. The main panel displays "Site Details" with the same information as the previous screenshot. Below it, the "Configured Clusters" section shows a table with one row: "Cluster Name" (A300-Cluster) and "Datacenter Name" (A300-DataCenter). A "Configure" button is visible at the bottom right of this section. A modal dialog box titled "Configure Clusters" is open over the main interface. It contains a table with two rows: "Cluster Name" (A300-Cluster) and "Datacenter Name" (A300-DataCenter). Both rows have checkboxes next to them, and the first row's checkbox is checked. At the bottom of the dialog are "Cancel" and "Configure" buttons.

- b. Add the Azure Blob storage located at the recovery site.



8. Deploy the required number of DR Virtual Appliances (DRVAs) from the Appliances tab.



Use the capacity planning tool to estimate the number of DRVAs required.

9. Create replication log volumes for each DRVA using the VMDK from the datastores available or the independent shared iSCSI storage pool.

The screenshot shows the JetStream DR interface with two main sections visible:

- DRVAs (DR Virtual Appliances):** A table listing one entry: GCSDRPD001. Columns include Name, Status (Running), Child Alarm (0), Software Version (4.0.0.134), and Details.
- Replication Log Volume:** A table listing one entry: /dev/sdb. Columns include Disk Path Name, Status (Ok), Child Alarm (0), Size (available/total) (179.88 GB / 200 GB), and Details.

- From the Protected Domains tab, create the required number of protected domains using information about the Azure Blob Storage site, the DRVA instance, and the replication log. A protected domain defines a specific VM or set of application VMs within the cluster that are protected together and assigned a priority order for failover/failback operations.

The screenshot shows the "Create Protected Domain" dialog box in Step 1: General. The form fields are as follows:

Protected Domain Name	GCSDRPD_Demo01
Priority Level (Optional)	-
Description	Protection domain ANF
Total estimated data size to be protected	1000GB
DR Virtual Appliance	GCSDRPD001
Compression	Yes
Compression Level	Default
Normal GC Storage Overhead	50%
Maximum GC Storage Overhead	300%
Replication Log Storage	/dev/sdb
Replication Log Size	4KB/R

The screenshot shows the "Create Protected Domain" dialog box in Step 2: Primary Site. The form fields are as follows:

Compression	Yes
Compression Level	Default
Normal GC Storage Overhead	50%
Maximum GC Storage Overhead	300%
Replication Log Storage	/dev/sdb
Replication Log Size	50GB
Metadata Size	31.56GB
Primary Site Datacenter	A300-DataCenter
Primary Site Cluster	A300-Cluster
Storage Site	ANFDRDemoFailoverSite
Enable PITR	No

- Select the VMs to be protected and group the VMs into applications groups based on dependency. Application definitions allow you to group sets of VMs into logical groups that contain their boot orders, boot delays, and optional application validations that can be executed upon recovery.



Make sure that the same protection mode is used for all VMs in a protected domain.



Write-Back(VMDK) mode offers higher performance.

The screenshot shows the 'Start Protection' dialog box from the JetStream DR interface. The 'Protection Mode for selected VMs' dropdown is set to 'Write-Through'. A list of VMs is shown with their protection modes: GCS-DR-DC, GCS-DR-LinVM01, GCS-DR-SCA, GCS-DR-SQL01, and GCS-DR-WinVM01 are all set to 'Write-Through'. Other VMs like ElasticWebA2, ElasticWebA3, etc., have 'Write-Through' as the default. The 'Start Protection' button at the bottom right is highlighted.

12. Make sure that replication log volumes are placed on high- performance storage.

The screenshot shows the 'Start Protection' dialog box from the JetStream DR interface. The 'Protection Mode for selected VMs' dropdown is set to 'Write-Back(VMDK)'. A list of VMs is shown with their protection modes: GCS-DR-DC, GCS-DR-LinVM01, GCS-DR-SCA, GCS-DR-SQL01, and GCS-DR-WinVM01 are all set to 'Write-Back(VMDK)'. Other VMs like ElasticWebA2, ElasticWebA3, etc., have 'Write-Through' as the default. The 'Start Protection' button at the bottom right is highlighted.

13. After you are done, click Start Protection for the protected domain. This starts data replication for the selected VMs to the designated Blob store.

14. After replication is completed, the VM protection status is marked as Recoverable.



Failover runbooks can be configured to group the VMs (called a recovery group), set the boot order sequence, and modify the CPU/memory settings along with the IP configurations.

15. Click Settings and then click the runbook Configure link to configure the runbook group.

16. Click the Create Group button to begin creating a new runbook group.



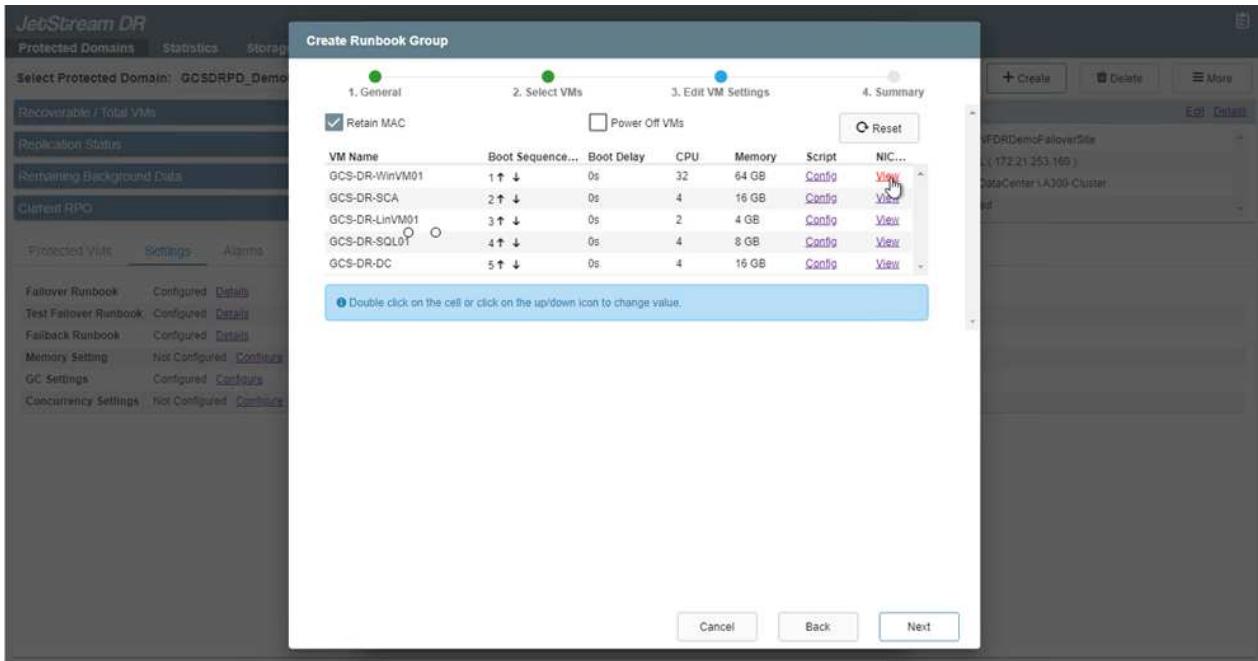
If needed, in the lower portion of the screen, apply custom pre-scripts and post-scripts to automatically run prior to and following operation of the runbook group. Make sure that the Runbook scripts are residing on the management server.

The screenshot shows the 'Failover Runbook Settings' page. On the left, there's a sidebar with 'Protected Domains' set to 'GCSDRPD\_Demo01'. The main area displays a table for 'Failover Runbook Settings' with two rows: 'Group Name' (with an edit icon) and 'Independent VMs' (with a delete icon). A tooltip 'Group Name' is shown over the first row. On the right, there's a panel for 'ANFDRDemoFailoverSite' showing its status as 'Disabled'.

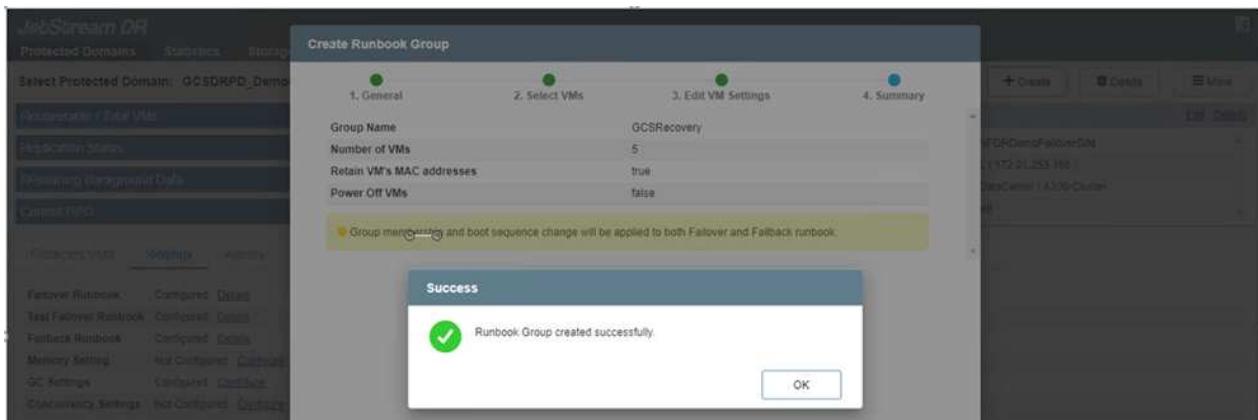
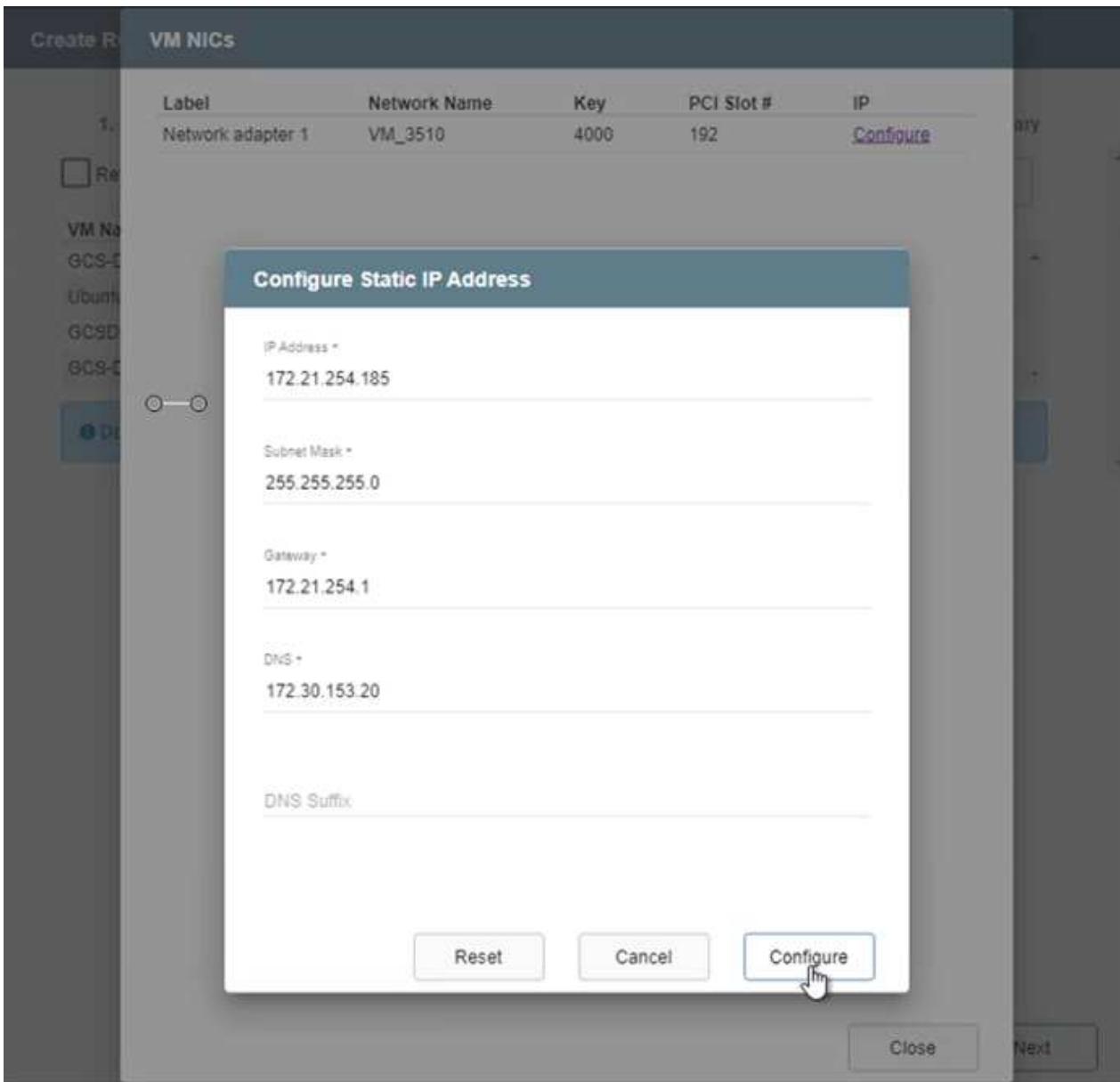
17. Edit the VM settings as required. Specify the parameters for recovering the VMs, including the boot sequence, the boot delay (specified in seconds), the number of CPUs, and the amount of memory to allocate. Change the boot sequence of the VMs by clicking the up or down arrows. Options are also provided to Retain MAC.

The screenshot shows the 'Create Runbook Group' wizard at step 3: 'Edit VM Settings'. It lists five VMs with their current settings: GCS-DR-WinVM01 (Boot Sequence: 1, Boot Delay: 0s, CPU: 32, Memory: 64 GB), GCS-DR-SCA (Boot Sequence: 2, Boot Delay: 0s, CPU: 4, Memory: 16 GB), GCS-DR-DC (Boot Sequence: 3, Boot Delay: 0s, CPU: 4, Memory: 16 GB), GCS-DR-LinVM01 (Boot Sequence: 4, Boot Delay: 0s, CPU: 2, Memory: 4 GB), and GCS-DR-SQL01 (Boot Sequence: 5, Boot Delay: 0s, CPU: 4, Memory: 8 GB). A tooltip 'Double click on the cell or click on the up/down icon to change value.' is visible. Buttons for 'Cancel', 'Back', and 'Next' are at the bottom.

18. Static IP addresses can be manually configured for the individual VMs of the group. Click the NIC View link of a VM to manually configure its IP address settings.



19. Click the Configure button to save NIC settings for the respective VMs.



The status of both the failover and fallback runbooks is now listed as Configured. Failover and fallback runbook groups are created in pairs using the same initial group of VMs and settings. If necessary, the settings of any runbook group can be individually customized by clicking its respective Details link and making changes.

## Install JetStream DR for AVS in private cloud

A best practice for a recovery site (AVS) is to create a three-node pilot-light cluster in advance. This allows the recovery site infrastructure to be preconfigured, including the following:

- Destination networking segments, firewalls, services like DHCP and DNS, and so on
- Installation of JetStream DR for AVS
- Configuration of ANF volumes as datastores and more

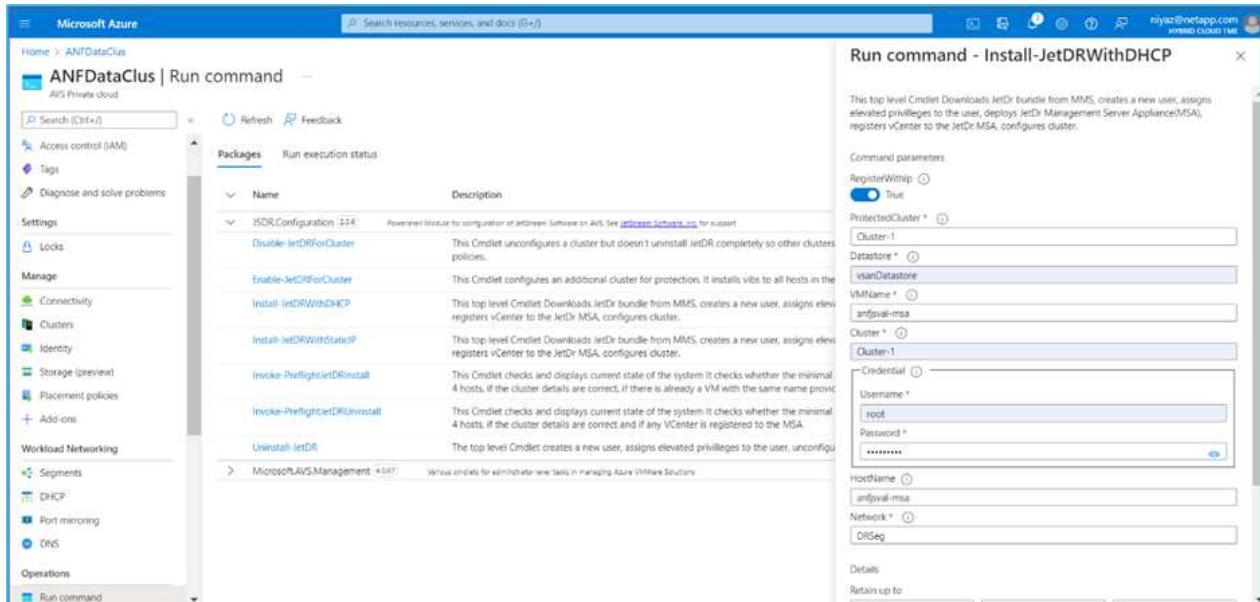
JetStream DR supports a near-zero RTO mode for mission-critical domains. For these domains, destination storage should be preinstalled. ANF is a recommended storage type in this case.

- i Network configuration including segment creation should be configured on the AVS cluster to match on-premises requirements.
- i Depending on the SLA and RTO requirements, you can use continuous failover or regular (standard) failover mode. For near-zero RTO, you should start continuous rehydration at the recovery site.

1. To install JetStream DR for AVS on an Azure VMware Solution private cloud, use the Run command. From the Azure portal, go to Azure VMware solution, select the private cloud, and select Run command > Packages > JSDR.Configuration.

- i The default CloudAdmin user of the Azure VMware Solution doesn't have sufficient privileges to install JetStream DR for AVS. The Azure VMware Solution enables simplified and automated installation of JetStream DR by invoking the Azure VMware Solution Run command for JetStream DR.

The following screenshot shows installation using a DHCP-based IP address.



2. After JetStream DR for AVS installation is complete, refresh the browser. To access the JetStream DR UI, go to SDDC Datacenter > Configure > JetStream DR.

## JetStream DR

Protected Domains   Statistics   Storage Sites   Appliances   Configurations   Task Log

### Site Details

[Alarm Settings](#)

vCenter Server Hostname 172.30.156.2

Management Appliance Hostname anfjsval-msa

Software Version 4.0.2.450

Subscription ID - [Configure](#)

Tenant ID / Application ID - [Configure](#)

Application Secret - [Configure](#)

[Configure Cluster](#)

[Upgrade](#)

[Unconfigure](#)

[Resolve Configure Issue](#)



Cluster Name ▲

Datacenter Name ▲

Status ▲

Software Version ▲

Host Details ▲

Cluster-1

SDDC-Datacenter

Ok

4.0.2.132

[Details](#)

- From the JetStream DR interface, complete the following tasks:

- Add the Azure Blob Storage account that was used to protect the on-premises cluster as a storage site and then run the Scan Domains option.
- In the pop-up dialog window that appears, select the protected domain to import and then click its Import link.

Protected Domain ...	Description	Recoverable V...	VMs ...	Import
GCSDRPD_Demo01	Protection domain ANF	5	5	<a href="#">Import</a>

- The domain is imported for recovery. Go to the Protected Domains tab and verify that the intended domain has been selected or choose the desired one from the Select Protected Domain menu. A list of the recoverable VMs in the protected domain is displayed.

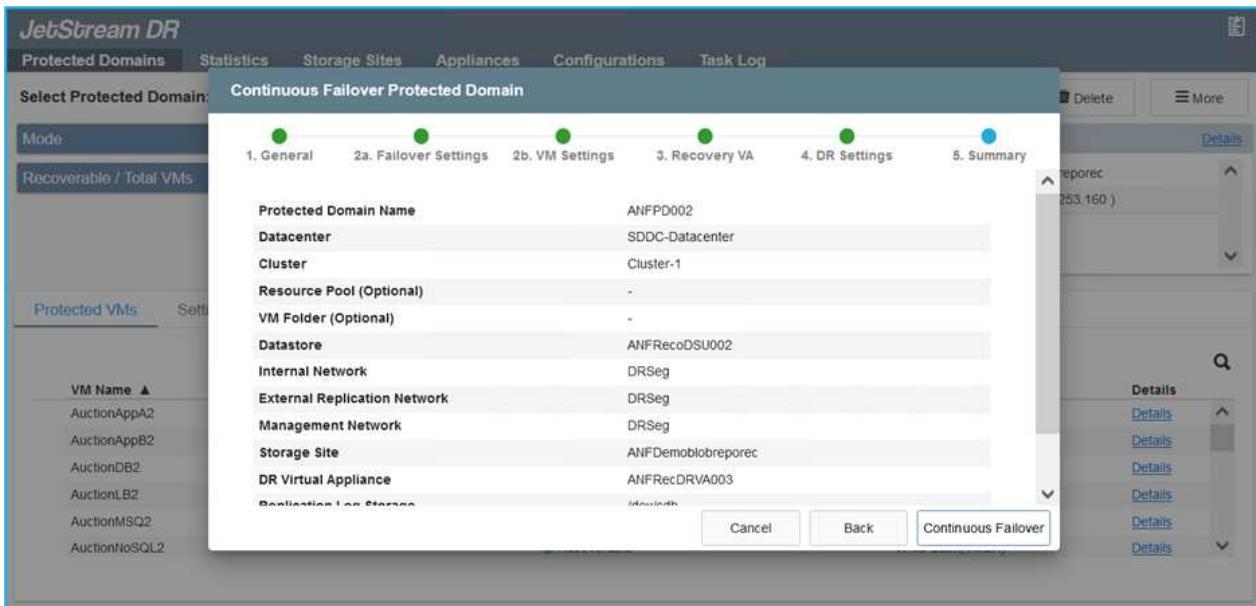
VM Name ▲	Protection Status ▲	Protection Mode ▲	Details
GCS-DR-DC	Recoverable	Write-Back(VMDK)	<a href="#">Details</a>
GCS-DR-LinVM01	Recoverable	Write-Back(VMDK)	<a href="#">Details</a>
GCS-DR-SCA	Recoverable	Write-Back(VMDK)	<a href="#">Details</a>
GCS-DR-SQL01	Recoverable	Write-Back(VMDK)	<a href="#">Details</a>
GCS-DR-WinVM01	Recoverable	Write-Back(VMDK)	<a href="#">Details</a>

- After the protected domains are imported, deploy DRVA appliances.



These steps can also be automated using CPT- created plans.

6. Create replication log volumes using available vSAN or ANF datastores.
7. Import the protected domains and configure the recovery VA to use an ANF datastore for VM placements.



Make sure that DHCP is enabled on the selected segment and that enough IPs are available. Dynamic IPs are temporarily used while domains are recovering. Each recovering VM (including continuous rehydration) requires an individual dynamic IP. After recovery is complete, the IP is released and can be reused.

8. Select the appropriate failover option (continuous failover or failover). In this example, continuous rehydration (continuous failover) is selected.



Although Continuous Failover and Failover modes differ on when configuration is performed, both failover modes are configured using the same steps. Failover steps are configured and performed together in response to a disaster event. Continuous failover can be configured at any time and then allowed to run in the background during normal system operation. After a disaster event has occurred, continuous failover is completed to immediately transfer ownership of the protected VMs to the recovery site (near-zero RTO).

**JetStream DR**

Protected Domains Statistics Storage Sites Appliances Configurations Task Log

Select Protected Domain: GCSDRPD\_Demo01 View all

Mode Imported

Recoverable / Total VMs 5 / 5

Configurations

Storage Site ANFDemoblobrepor  
Owner Site REMOTE ( 172.21.253.10 )

+ Create Delete More

Restore → Failover → Continuous Failover → Test Failover

Protected VMs Settings Alarms

VM Name	Protection Status	Protection Mode	Details
GCS-DR-DC	Recoverable	Write-Back(VMDDK)	Details
GCS-DR-LinVM01	Recoverable	Write-Back(VMDDK)	Details
GCS-DR-SCA	Recoverable	Write-Back(VMDDK)	Details
GCS-DR-SQL01	Recoverable	Write-Back(VMDDK)	Details
GCS-DR-WinVM01	Recoverable	Write-Back(VMDDK)	Details

The continuous failover process begins, and its progress can be monitored from the UI. Clicking the blue icon in the Current Step section exposes a pop-up window showing details of the current step of the failover process.

## Failover and Failback

- After a disaster occurs in the protected cluster of the on-premises environment (partial or complete failure), you can trigger the failover for VMs using Jetstream after breaking the SnapMirror relationship for the respective application volumes.

The screenshot shows the Jetstream UI for managing volume relationships. At the top, there are summary statistics: 3 Volume Relationships, 4.78 GiB Replicated Capacity, 0 Currently Transferring, 3 Healthy, and 0 Failed. Below this is a table titled "3 Volume Relationships" with columns: Health Status, Source Volume, Target Volume, Total Transfer Time, Status, Mirror State, and Last Successful Transfer. Three rows are listed, all in a "snapmirrored" state. The first row has a context menu open, showing options: Break (which is highlighted with a cursor), Reverse Resync, Edit Schedule, Edit Max Transfer Rate, Update, and Delete.

The screenshot shows the Jetstream UI with a "Break Relationship" dialog box. The dialog asks, "Are you sure that you want to break the relationship between "gcsdrsqldb\_sc46" and "gcsdrsqldb\_sc46\_copy"?". There are two buttons: "Break" (highlighted with a cursor) and "Cancel". In the background, the main interface shows the same volume relationships table as the previous screenshot, with the first row selected.



This step can easily be automated to facilitate the recovery process.

- Access the Jetstream UI on AVS SDDC (destination side) and trigger the failover option to complete failover. The task bar shows progress for failover activities.

In the dialog window that appears when completing failover, the failover task can be specified as planned or assumed to be forced.

**JetStream DR**

Protected Domains Statistics Storage Sites Appliances Configurations Task Log

Select Protected Domain: GCSDRPD\_Demo01 View all

Mode: Continuous Rehydration in Progress 4 / 4

Recoverable / Total VMs: 4 / 4

Data (Processed/Known Remaining): 329.01 GB / 6.19 GB

Current Step: Recover VMs' data from Storage Site

Configurations

Storage Site	ANFDemotlobreporec
Owner Site	REMOTE ( 172.21.253.160 )
Datacenter \ Cluster	SDDC-Datacenter \ Cluster-1
Point-in-time Recovery	Disabled

Protected VMs Settings Alarms

VM Name	Protection Status	Protection Mode	Details
GCS-DR-DC	Recoverable	Write-Back\MDK	<a href="#">Details</a>
GCS-DR-LinVM01	Recoverable	Write-Back\MDK	<a href="#">Details</a>
GCS-DR-SCA	Recoverable	Write-Back\MDK	<a href="#">Details</a>
GCS-DR-SQL01	Recoverable	Write-Back\MDK	<a href="#">Details</a>
GCS-DR-WinVM01	Recoverable	Write-Back\MDK	<a href="#">Details</a>

### Complete Continuous Failover for Protected Domain

**VM Network Mapping**

Protected VM Network	Recovery VM Network
VM_3510	DRStretchSeg

**Other Settings**

Planned Failover  
 Force Failover

Some VM's guest credential are required because of network configuration: [Configure](#)

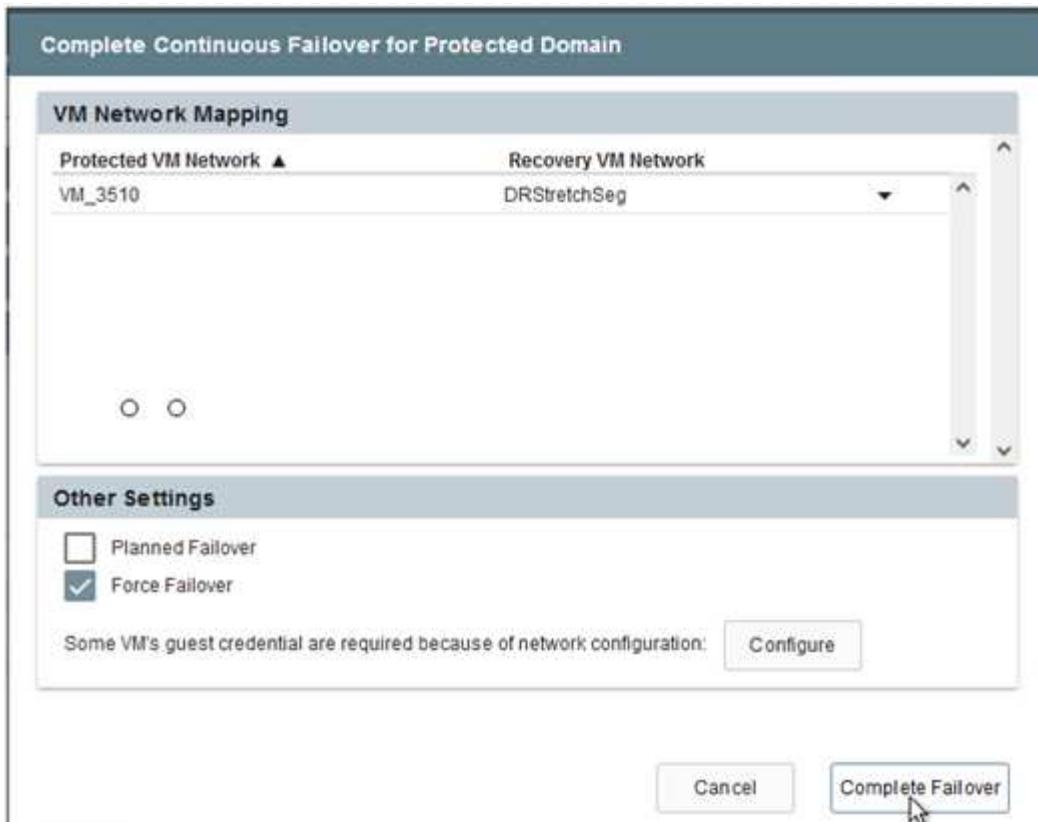
[Cancel](#) [Complete Failover](#)

Forced failover assumes the primary site is no longer accessible and ownership of the protected domain should be directly assumed by the recovery site.

### Force Failover

**!** Force Failover of Protected Domain requested. Administrator consent is required!  
 Complete ownership of this Protected Domain will be taken over by this Site.  
 Are you sure you want to continue?

[Cancel](#) [Confirm](#)



3. After continuous failover is complete, a message appears confirming completion of the task. When the task is complete, access the recovered VMs to configure iSCSI or NFS sessions.



The failover mode changes to Running in Failover and the VM status is Recoverable. All the VMs of the protected domain are now running at the recovery site in the state specified by the failover runbook settings.



To verify the failover configuration and infrastructure, JetStream DR can be operated in test mode (Test Failover option) to observe the recovery of virtual machines and their data from the object store into a test recovery environment. When a failover procedure is executed in test mode, its operation resembles an actual failover process.

4. After the virtual machines are recovered, use storage disaster recovery for in-guest storage. To demonstrate this process, SQL server is used in this example.
5. Log into the recovered SnapCenter VM on AVS SDDC and enable DR mode.
  - a. Access the SnapCenter UI using the browser.



- b. In the Settings page, navigate to Settings > Global Settings > Disaster Recovery.
- c. Select Enable Disaster Recovery.
- d. Click Apply.

- e. Verify whether the DR job is enabled by clicking Monitor > Jobs.



NetApp SnapCenter 4.6 or later should be used for storage disaster recovery. For previous versions, application-consistent snapshots (replicated using SnapMirror) should be used and manual recovery should be executed in case previous backups must be recovered in the disaster recovery site.

6. Make sure that the SnapMirror relationship is broken.

The screenshot shows the NetApp SnapCenter interface with the 'Replication' tab selected. At the top, there are summary statistics: 3 Volume Relationships, 4.78 GiB Replicated Capacity, 0 Currently Transferring, 3 Healthy, and 0 Failed. Below this is a table titled '3 Volume Relationships' with the following data:

Health Status	Source Volume	Target Volume	Total Transfer Time	Status	Mirror State	Last Successful Transfer
✓	gcsdrsqldb_sc46_ntaphci-a300e9u25	gcsdrsql ldb_sc46_copy ANFCVODRDemo	6 minutes 41 seconds	idle	broken-off	May 5, 2022, 12:08:34 PM 33.66 kB
✓	gcsdrsqlhld_sc46_ntaphci-a300e9u25	gcsdrsql hld_sc46_copy ANFCVODRDemo	4 minutes 56 seconds	idle	broken-off	May 5, 2022, 12:09:15 PM 69.84 kB
✓	gcsdrsqllog_sc46_ntaphci-a300e9u25	gcsdrsql log_sc46_copy ANFCVODRDemo	10 minutes 18 seconds	idle	broken-off	May 5, 2022, 12:08:34 PM 104.34 kB

7. Attach the LUN from Cloud Volumes ONTAP to the recovered SQL guest VM with same drive letters.

The screenshot shows the Windows Disk Management tool. The table below lists the volumes and their properties:

Volume	Layout	Type	File System	Status	Capacity	Free Spa...	% Free
---	Simple	Basic		Healthy (R...)	450 MB	450 MB	100 %
---	Simple	Basic		Healthy (E...)	99 MB	99 MB	100 %
-(C:)	Simple	Basic	NTFS	Healthy (B...)	89.45 GB	67.03 GB	75 %
-(BACKUP (G:)	Simple	Basic	NTFS	Healthy (P...)	9.97 GB	9.92 GB	99 %
-(DATA (E:)	Simple	Basic	NTFS	Healthy (P...)	24.88 GB	24.57 GB	99 %
-(LOG (F:)	Simple	Basic	NTFS	Healthy (P...)	9.97 GB	8.93 GB	90 %

8. Open iSCSI Initiator, clear the previous disconnected session and add the new target along with multipath for the replicated Cloud Volumes ONTAP volumes.

## iSCSI Initiator Properties

X

Targets Discovery Favorite Targets Volumes and Devices RADIUS Configuration

### Quick Connect

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

Target:

Quick Connect...

### Discovered targets

Refresh

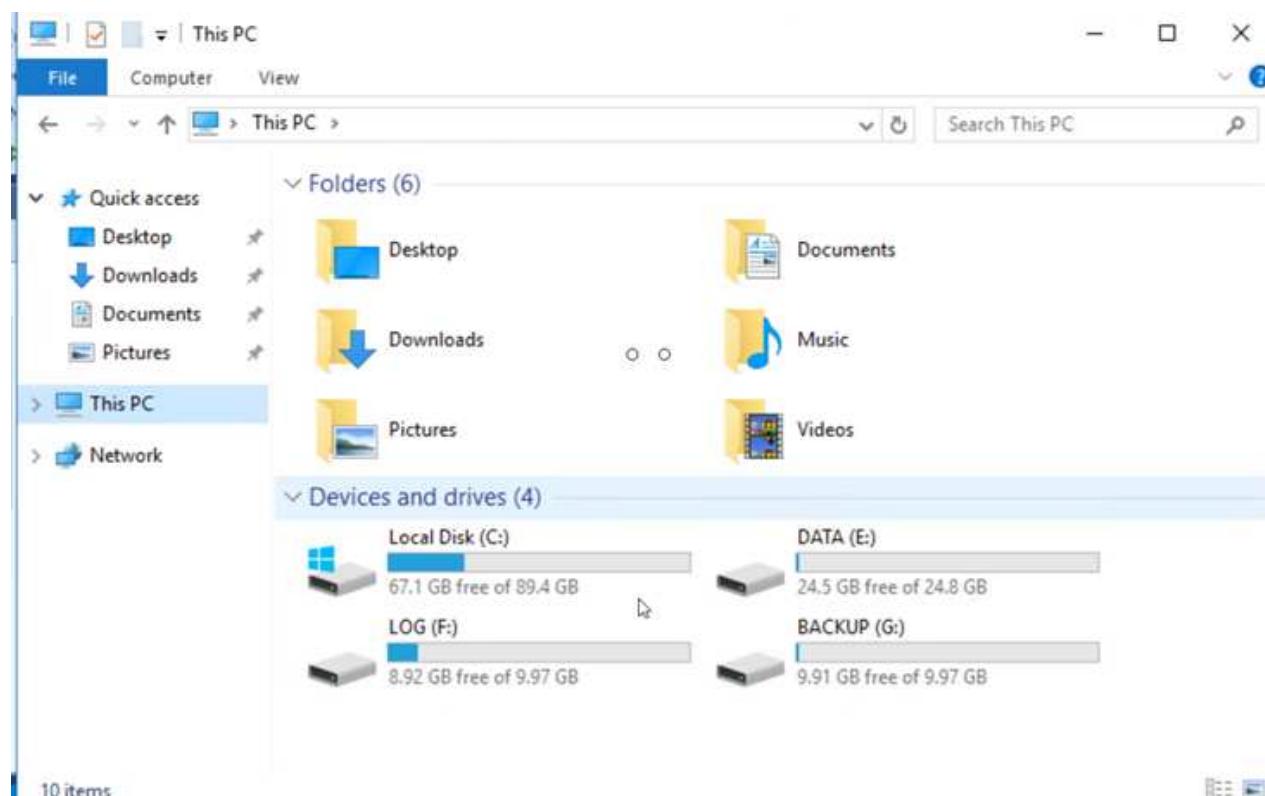
Name

Status

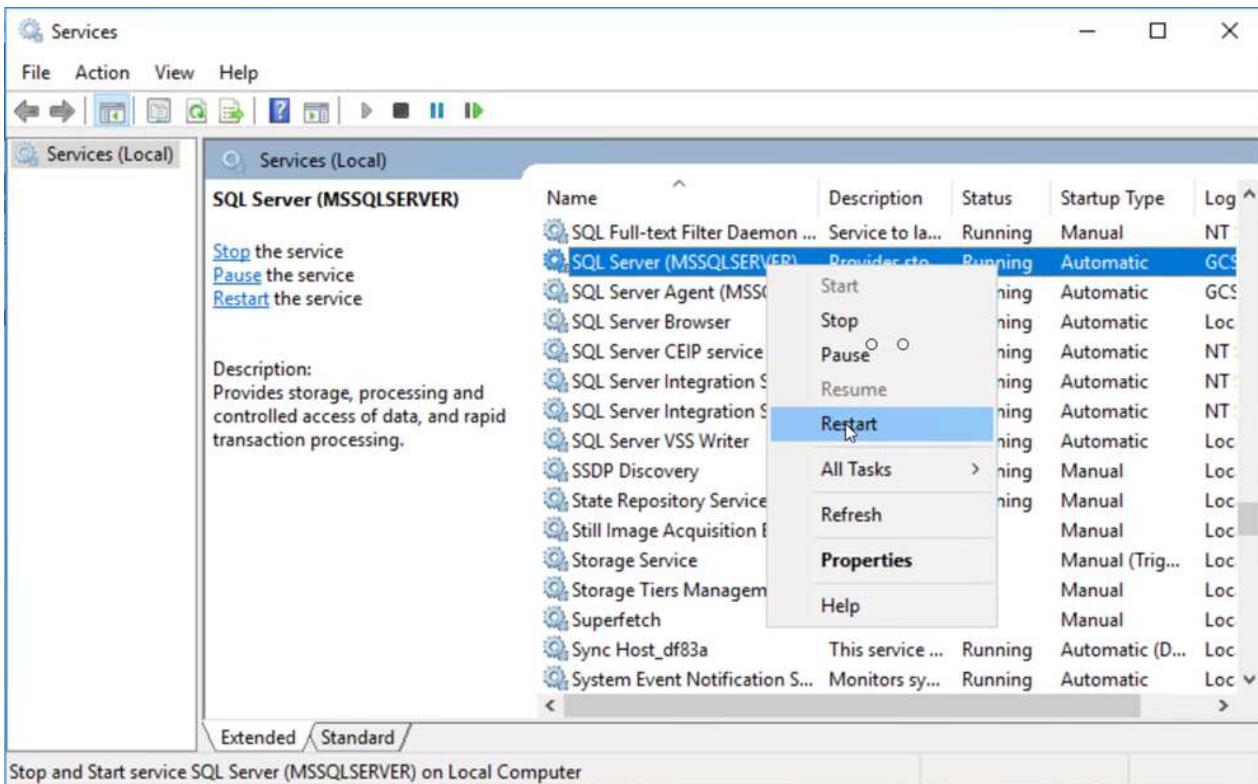
iqn.1992-08.com.netapp:sn.547772ccc47811ecbb62000... Connected

iqn.1992-08.com.netapp:sn.aeab78ab720011ec939800... Reconnecting...

9. Make sure that all the disks are connected using the same drive letters that were used prior to DR.



10. Restart the MSSQL server service.



11. Make sure that the SQL resources are back online.

The screenshot shows the Microsoft SQL Server Management Studio (SSMS) interface. The title bar reads 'SQLQuery1.sql - GCS-DR-SQL03.CarDB (GCSDC\adminnimo (66)) - Microsoft SQL Server Management Studio (Administrator)'. The Object Explorer on the left shows the database structure, including 'CarDB' and its tables. The central pane displays a query window with the following SQL script:

```

/*
***** Script for SelectTopNRows command from SSMS *****/
SELECT TOP (1000) [Id]
    ,[Name]
    ,[Price]
FROM [CarDB].[dbo].[Cars]

```

The 'Results' tab shows the execution output:

	Id	Name	Price
1	1	Car-1	1000
2	2	Car-2	2000
3	3	Car-3	3000
4	4	Car-4	4000
5	5	Car-5	5000

A message at the bottom of the results pane says 'Query executed successfully.'



In the case of NFS, attach the volumes using the mount command and update the /etc/fstab entries.

At this point, operations can be run and business continues normally.



On the NSX-T end, a separate dedicated tier-1 gateway can be created for simulating failover scenarios. This ensures that all workloads can communicate with each other but that no traffic can route in or out of the environment, so that any triage, containment, or hardening tasks can be performed without risk of cross-contamination. This operation is outside of the scope of this document, but it can easily be achieved for simulating isolation.

After the primary site is up and running again, you can perform failback. VM protection is resumed by Jetstream and the SnapMirror relationship must be reversed.

1. Restore the on-premises environment. Depending on the type of disaster incident, it might be necessary to restore and/or verify the configuration of the protected cluster. If necessary, JetStream DR software might need to be reinstalled.
2. Access the restored on-premises environment, go to the Jetstream DR UI, and select the appropriate protected domain. After the protected site is ready for failback, select the Failback option in the UI.



The CPT-generated failback plan can also be used to initiate the return of the VMs and their data from the object store back to the original VMware environment.



Specify the maximum delay after pausing the VMs in the recovery site and restarting them in the protected site. The time needed to complete this process includes the completion of replication after stopping failover VMs, the time needed to clean the recovery site, and the time needed to recreate VMs in the protected site. NetApp recommends 10 minutes.

## Fallback Protected Domain

1. General	2a. Fallback Settings	2b. VM Settings	3. Recovery VA	4. DR Settings	5. Summary
Fallback Datacenter			A300-DataCenter		
Fallback Cluster			A300-Cluster		
Fallback Resource Pool			-		
VM Folder (Optional)			-		
Fallback Datastore			A300_NFS_vMotion		
Maximum Delay After Stopping			10 Minutes		
Internal Network			VM_187		
External Replication Network			VM_187		
Management Network			VM_187		
Storage Site			ANFCVODR		
DR Virtual Appliance			GCSDRVA002		
Replication Log Storage			/dev/sdb		

Cancel

Back

Fallback

3. Complete the failback process and then confirm the resumption of VM protection and data consistency.

Protected Domain:		GCSDRPD002
Protected Domain	GCSDRPD002	
VMs Recovery Status	Success	
Total VMs Recovered	4	
GCSR03 Status:		
Pre-script Execution Status	Not defined	
Runbook Execution Status	Success	
Post-script Execution Status	Not defined	

4. After the VMs are recovered, disconnect the secondary storage from the host and connect to the primary storage.

Health Status	Source Volume	Target Volume	Total Transfer Time	Status	Mirror State	Last Successful Transfer	More Options
✓	gcsdrsqldb_sc46_ntaphcl-a300e9u25	gcsdrsqldb_sc46_copy_ANFCVODRDemo	6 minutes 41 seconds	idle	broken-off	May 5, 2022, 12:08:34 PM 33.66 kB	...
✓	gcsdrsqlhld_sc46_ntaphcl-a300e9u25	gcsdrsqlhld_sc46_copy_ANFCVODRDemo	4 minutes 56 seconds	idle	broken-off		Information
✓	gcsdrsqllog_sc46_ntaphcl-a300e9u25	gcsdrsqllog_sc46_copy_ANFCVODRDemo	10 minutes 18 seconds	idle	broken-off		Resync Reverse Resync Edit Schedule Edit Max Transfer Rate Delete

5. Restart the MSSQL server service.
6. Verify that the SQL resources are back online.

SQLQuery1.sql - GCS-DR-SQL03.CarDB (GCSDC\adminnimo (66)) - Microsoft SQL Server Management Studio (Administrator)

File Edit View Query Project Tools Window Help

New Query Execute

Object Explorer

System Databases Database Snapshots CarDB Database Diagrams Tables System Tables FileTables External Tables Graph Tables dbo.Cars Views External Resources Synonyms Programmability Service Broker Storage Security

SQLQuery1.sql - G...DC\adminnimo (66) ↗ X

```
===== Script for SelectTopNRows command from SSMS =====/
SELECT TOP (1000) [Id]
    ,[Name]
    ,[Price]
    FROM [CarDB].[dbo].[Cars]
```

Results Messages

	Id	Name	Price
1	1	Car-1	1000
2	2	Car-2	2000
3	3	Car-3	3000
4	4	Car-4	4000
5	5	Car-5	5000

Query executed successfully.



To failback to the primary storage, make sure that the relationship direction remains the same as it was before the failover by performing a reverse resync operation.



To retain the roles of primary and secondary storage after the reverse resync operation, perform the reverse resync operation again.

This process is applicable to other applications like Oracle, similar database flavors, and any other applications using guest-connected storage.

As always, test the steps involved for recovering the critical workloads before porting them into production.

## Benefits of this solution

- Uses the efficient and resilient replication of SnapMirror.
- Recovers to any available points in time with ONTAP snapshot retention.
- Full automation is available for all required steps to recover hundreds to thousands of VMs, from the storage, compute, network, and application validation steps.
- SnapCenter uses cloning mechanisms that do not change the replicated volume.
  - This avoids the risk of data corruption for volumes and snapshots.
  - Avoids replication interruptions during DR test workflows.
  - Leverages the DR data for workflows beyond DR, such as dev/test, security testing, patch and upgrade testing, and remediation testing.
- CPU and RAM optimization can help lower cloud costs by enabling recovery to smaller compute clusters.

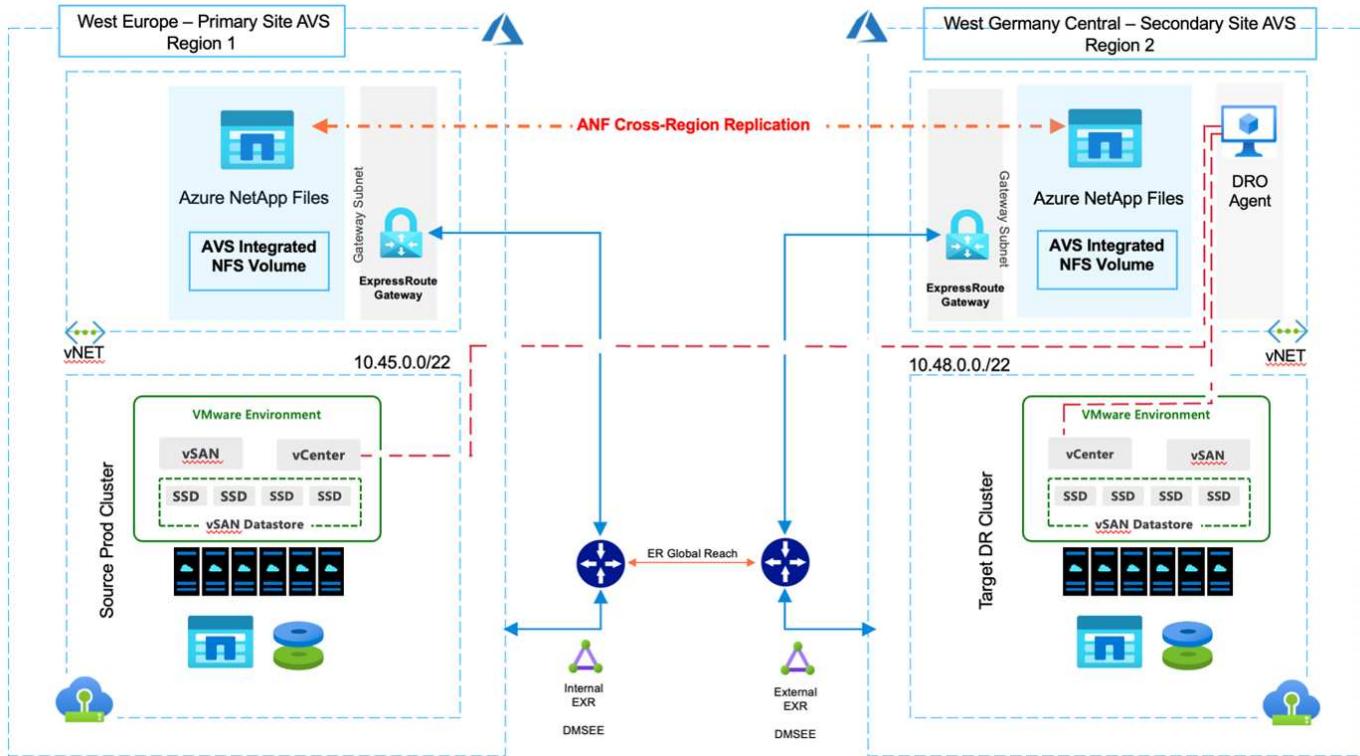
## TR-4955: Disaster Recovery with Azure NetApp Files (ANF) and Azure VMware Solution (AVS)

Author(s): Niyaz Mohamed, NetApp Solutions Engineering

### Overview

Disaster recovery using block-level replication between regions within the cloud is a resilient and cost-effective way of protecting the workloads against site outages and data corruption events (for example, ransomware). With Azure NetApp files (ANF) cross-region volume replication, VMware workloads running on an Azure VMware Solution (AVS) SDDC site using Azure NetApp files volumes as an NFS datastore on the primary AVS site can be replicated to a designated secondary AVS site in the target recovery region.

Disaster Recovery Orchestrator (DRO) (a scripted solution with a UI) can be used to seamlessly recover workloads replicated from one AVS SDDC to another. DRO automates recovery by breaking replication peering and then mounting the destination volume as a datastore, through VM registration to AVS, to network mappings directly on NSX-T (included with all AVS private clouds).



### Prerequisites and general recommendations

- Verify that you have enabled cross-region replication by creating replication peering. See [Create volume replication for Azure NetApp Files](#).
- You must configure ExpressRoute Global Reach between the source and target Azure VMware Solution private clouds.
- You must have a service principal that can access resources.
- The following topology is supported: primary AVS site to secondary AVS site.
- Configure the [replication](#) schedule for each volume appropriately based on business needs and the data-change rate.



Cascading and fan-in and fan-out topologies are not supported.

## Getting started

### Deploy Azure VMware Solution

The [Azure VMware Solution](#) (AVS) is a hybrid cloud service that provides fully functional VMware SDDCs within a Microsoft Azure public cloud. AVS is a first-party solution fully managed and supported by Microsoft and verified by VMware that uses Azure infrastructure. Therefore, customers get VMware ESXi for compute virtualization, vSAN for hyper-converged storage, and NSX for networking and security, all while taking advantage of Microsoft Azure's global presence, class-leading data-center facilities, and proximity to the rich ecosystem of native Azure services and solutions. A combination of Azure VMware Solution SDDC and Azure NetApp Files provides the best performance with minimal network latency.

To configure an AVS private cloud on Azure, follow the steps in this [link](#) for NetApp documentation and in this [link](#) for Microsoft documentation. A pilot-light environment set up with a minimal configuration can be used for DR purposes. This setup only contains core components to support critical applications, and it can scale out and spawn more hosts to take the bulk of the load if a failover occurs.



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

## Provision and configure Azure NetApp Files

Azure NetApp Files is a high-performance, enterprise-class, metered file- storage service. Follow the steps in this [link](#) to provision and configure Azure NetApp Files as a NFS datastore to optimize AVS private cloud deployments.

## Create volume replication for Azure NetApp Files-powered datastore volumes

The first step is to set up cross- region replication for the desired datastore volumes from the AVS primary site to the AVS secondary site with the appropriate frequencies and retentions.

The screenshot shows the Azure portal interface for managing Azure NetApp Files. The top navigation bar includes 'Home', 'Azure NetApp Files', 'WEANFAVSacct | Volumes', and 'testrepIdemo (WEANFAVSacct/testcap/testrepIdemo) | Replication'. The main content area displays the 'testrepIdemo' volume details. On the left, there's a sidebar with 'Search', 'Overview', 'Activity log', 'Access control (IAM)', and 'Tags'. The right side shows the 'Essentials' section with the following details:

End point type	: Source	Destination	: testrepIdemo_copy
Health status	: Healthy	Relationship status	: Idle
Mirror state	: Mirrored	Total progress	: 2.13 GiB

At the bottom right, there's a 'JSON View' link.

Follow the steps in this [link](#) to set up cross-region replication by creating replication peering. The service level for the destination capacity pool can match that of the source capacity pool. However, for this specific use case, you can select the standard service level and then [modify the service level](#) in the event of a real disaster or DR simulations.



A cross- region replication relationship is a prerequisite and must be created beforehand.

## DRO installation

To get started with DRO, use the Ubuntu operating system on the designated Azure virtual machine and make sure you meet the prerequisites. Then install the package.

### Prerequisites:

- Service principal that can access resources.
- Make sure that appropriate connectivity exists to the source and destination SDDC and Azure NetApp Files instances.
- DNS resolution should be in place if you are using DNS names. Otherwise, use IP addresses for vCenter.

### OS requirements:

- Ubuntu Focal 20.04 (LTS)The following packages must be installed on the designated agent virtual machine:
  - Docker
  - Docker- compose
  - JqChange docker.sock to this new permission: sudo chmod 666 /var/run/docker.sock.



The deploy.sh script executes all required prerequisites.

The steps are as follows:

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

```
git clone <link here>
```



The agent must be installed in the secondary AVS site region or in the primary AVS site region in a separate AZ than the SDDC.

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

```
tar xvf draas_package.tar
```

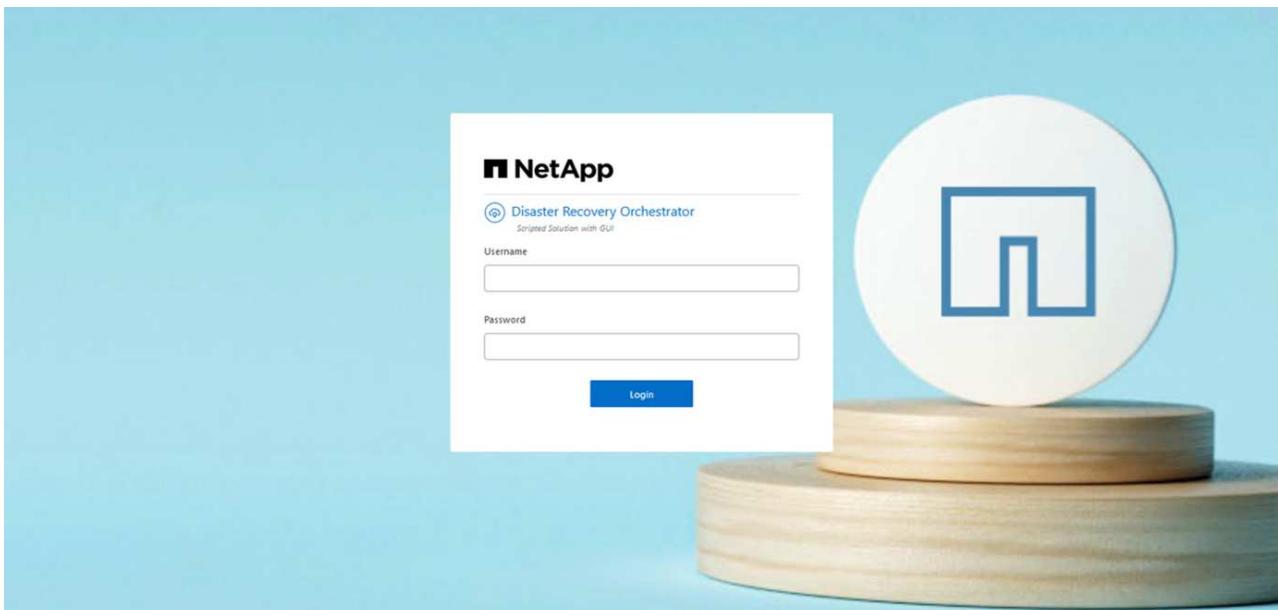
Navigate to the directory and run the deploy script as below:

```
sudo sh deploy.sh
```

3. Access the UI using the following credentials:

- ° Username: admin

- ° Password: admin



## DRO configuration

After Azure NetApp Files and AVS have been configured properly, you can begin configuring DRO to automate the recovery of workloads from the primary AVS site to the secondary AVS site. NetApp recommends deploying the DRO agent in the secondary AVS site and configuring the ExpressRoute gateway connection so that the DRO agent can communicate via the network with the appropriate AVS and Azure NetApp Files components.

The first step is to Add credentials. DRO requires permission to discover Azure NetApp Files and the Azure VMware Solution. You can grant the required permissions to an Azure account by creating and setting up an

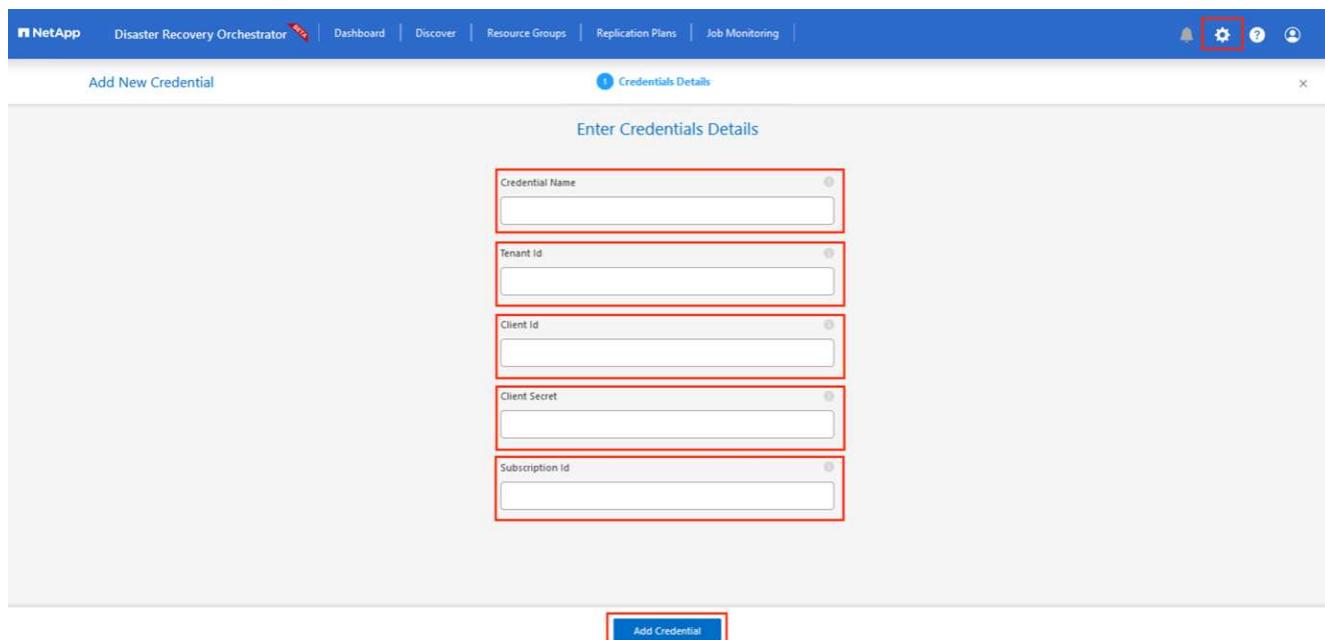
Azure Active Directory (AD) application and by obtaining the Azure credentials that DRO needs. You must bind the service principal to your Azure subscription and assign it a custom role that has the relevant required permissions. When you add source and destination environments, you are prompted to select the credentials associated with the service principal. You need to add these credentials to DRO before you can click Add New Site.

To perform this operation, complete the following steps:

1. Open DRO in a supported browser and use the default username and password (admin/admin). The password can be reset after the first login using the Change Password option.
2. In the upper right of the DRO console, click the **Settings** icon, and select **Credentials**.
3. Click Add New Credential and follow the steps in the wizard.
4. To define the credentials, enter information about the Azure Active Directory service principal that grants the required permissions:
  - Credential name
  - Tenant ID
  - Client ID
  - Client secret
  - Subscription ID

You should have captured this information when you created the AD application.

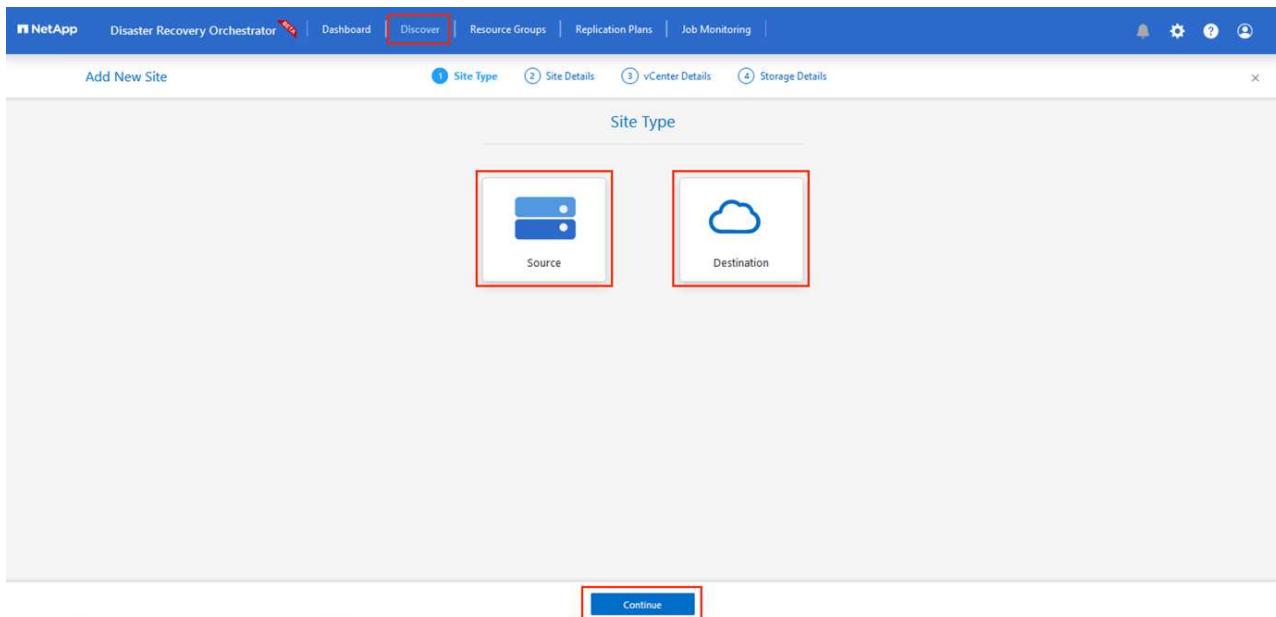
5. Confirm the details about the new credentials and click Add Credential.



After you add the credentials, it's time to discover and add the primary and secondary AVS sites (both vCenter and the Azure NetApp files storage account) to DRO. To add the source and destination site, complete the following steps:

6. Go to the **Discover** tab.
7. Click **Add New Site**.

8. Add the following primary AVS site (designated as **Source** in the console).
  - SDDC vCenter
  - Azure NetApp Files storage account
  
9. Add the following secondary AVS site (designated as **Destination** in the console).
  - SDDC vCenter
  - Azure NetApp Files storage account



10. Add site details by clicking **Source**, entering a friendly site name, and select the connector. Then click **Continue**.



For demonstration purposes, adding a source site is covered in this document.

11. Update the vCenter details. To do this, select the credentials, Azure region, and resource group from the dropdown for the primary AVS SDDC.
12. DRO lists all the available SDDCs within the region. Select the designated private cloud URL from the dropdown.
13. Enter the `cloudadmin@vsphere.local` user credentials. This can be accessed from Azure Portal. Follow the steps mentioned in this [link](#). Once done, click **Continue**.

14. Select the Source Storage details (ANF) by selecting the Azure Resource group and NetApp account.

15. Click **Create Site**.

Site Name	Site Type	Location	vCenter	Storage	VM List	Discovery Status
DemoDest	Destination	Cloud	1	1	<a href="#">View VM List</a>	<span>Success</span>
DemoSRC	Source	Cloud	1	1	<a href="#">View VM List</a>	<span>Success</span>

Once added, DRO performs automatic discovery and displays the VMs that have corresponding cross-region replicas from the source site to the destination site. DRO automatically detects the networks and segments used by the VMs and populates them.

**VM List**  
Site: DemoSRC | vCenter: <https://172.30.156.2/>

VM Name	VM Status	VM State	DataStore	CPU	Memory (MB)
HCI Bench_2.6.1	Not Protected	Powered On	vsanDatastore	8	8192
hci-flo-datastore-13984-0-1	Not Protected	Powered Off	HCItstDS	32	65536
ICCAz005-WO-R1	Not Protected	Powered On	vsanDatastore	8	14336
ICCAz005-NE-R1	Not Protected	Powered On	vsanDatastore	8	3072
ICCAz005-IX-R1	Not Protected	Powered On	vsanDatastore	8	3072
HCX_Demo_05	Not Protected	Powered Off	Demo002	1	2048
hci-nim-datastore-13984-0-1	Not Protected	Powered Off	HCItstDS	24	49152

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

### Resource groupings

After the platforms have been added, 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, click the **Create New Resource Group** menu item.

1. Access **Resource Groups** and click **\*Create New Resource Group**.

**Resource Groups**

**Create New Resource Group**

Resource Group Name: DemoRG | Site Name: DemoSRC | Source vCenter: https://172.30.156.2/

2. Under New Resource Group, select the source site from the dropdown and click **Create**.
3. Provide the resource group details and click **Continue**.
4. Select appropriate VMs using the search option.
5. Select the **Boot Order** and **Boot Delay (secs)** for all the selected VMs. Set the order of the power-on sequence by selecting each virtual machine and setting up the priority for it. The default value for all virtual machines is 3. The options are as follows:
  - The first virtual machine to power on
  - Default

- The last virtual machine to power on

VM Name	Boot Order	Boot Delay (secs)
QALin1	3	0
QALin	3	0

## 6. Click **Create Resource Group**.

Resource Group Name	Site Name	Source vCenter	VM List
DemoRG	DemoSRC	https://172.30.156.2/	<a href="#">View VM List</a>

## Replication plans

You must have a plan to recover applications in the event of a disaster. Select the source and destination vCenter platforms from the drop down, pick the resource groups to be included in this plan, and also include the grouping of how applications should be restored and powered on (for example, domain controllers, tier-1, tier-2, and so on). Plans are often called blueprints as well. 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. Navigate to **Replication Plans** and click **Create New Replication Plan**.

Plan Name	Active Site	Status	Compliance	Source Site	Destination Site	Resource Groups
DemoRP	Source	Active	Partially Healthy	DemoSRC	DemoDest	<a href="#">Resource Groups</a>

### 2. On the **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.

Plan Name  
DemoRP

**Recovery Mapping**

Source Site	Destination Site
DemoSRC	DemoDest

**Cluster Mapping**

Source Site Resource	Destination Site Resource
Cluster-1	Cluster-1

**Source Resource      Destination Resource**

No Mappings added!	
--------------------	--

**Continue**

3. After recovery mapping is complete, select the **Cluster Mapping**.

Plan Name  
DemoRP

**Recovery Mapping**

Source Site	Destination Site
DemoSRC	DemoDest

**Cluster Mapping**

No more Source/Destination cluster resources available for mapping

Source Resource	Destination Resource
Cluster-1	Cluster-1

**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. Once done, set network mapping to the appropriate segment. The segments should already be provisioned on the secondary AVS cluster, and, to map the VMs to those, select the appropriate segment.
7. Datastore mappings are automatically selected based on the selection of VMs.



Cross- region replication (CRR) is at the volume level. Therefore, all VMs residing on the respective volume are replicated to the CRR destination. Make sure to select all VMs that are part of the datastore, because only virtual machines that are part of the replication plan are processed.

8. Under VM details, you can optionally resize the VMs CPU and RAM parameters. This can be very helpful when you are recovering large environments to smaller target clusters or when you are conducting DR tests without having to provision a one-to-one physical VMware infrastructure. Also, modify the boot order and boot delay (secs) for all the selected VMs across the resource groups. There is an additional option to modify the boot order if any changes are required from what you selected during 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.

9. Click **Create Replication Plan**. After the replication plan is created, you can exercise the failover, test failover, or migrate options depending on your requirements.

The screenshot shows the DRO dashboard with the following details:

- Replication Plans:** 1
- Resource Groups:** 1
- Source Details:** 1 Site, 1 vCenter
- Destination Details:** 1 Site, 1 vCenter
- Replication Plan Summary:**
  - Plan Name:** DemoRP
  - Active Site:** Source (green)
  - Status:** Active
  - Compliance:** Partially Healthy
  - Source Site:** DemoSRC
  - Destination Site:** DemoDest
- Task Menu (Open):**
  - Plan Details
  - Edit Plan
  - Failover** (highlighted with a red box)
  - Test Failover
  - Migrate
  - Run Compliance
  - Delete Plan

During the failover and test failover options, the most recent snapshot is used, or a specific snapshot can be selected from a point-in-time snapshot. The point-in-time option can be very beneficial if you are facing a corruption event like ransomware, where the most recent replicas are already compromised or encrypted. DRO shows all available time points.

The screenshot shows the DRO dashboard with the following details:

- Replication Plans:** 1
- Resource Groups:** 1
- Source Details:** 1 Site, 1 vCenter
- Destination Details:** 1 Site, 1 vCenter
- Replication Plan Summary:**
  - Plan Name:** DemoRP
  - Active Site:** Source
- Testfailover Details Dialog:**
  - Options: Use latest snapshot (radio button), Select specific snapshot (radio button, selected).
  - Table: Shows a list of volumes and their corresponding snapshots. One row is highlighted with a blue background.
  - Buttons: Start Testfailover (blue button).

To trigger failover or test failover with the configuration specified in the replication plan, you can click **Failover** or **Test Failover**. You can monitor the replication plan in the task menu.

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

Failback can be triggered at the replication plan level. In case of test failover, the tear down option can be used to roll back the changes and remove the newly created volume. Failbacks related to failover are a two-step process. Select the replication plan and select **Reverse Data sync**.

After this step is complete, trigger failback to move back to the primary AVS site.

**Replication Plans**

Plan Name	Active Site	Status	Compliance	Source Site	Destination Site
DemoRP	Destination	Active	Healthy	DemoSRC	DemoDest

**Resource Groups**

**Topology Canvas**

**Replication Plans**

Replication Plan	Active Site	Status
DemoRP	Source	Active

From the Azure portal, we can see that the replication health has been broken off for the appropriate volumes that were mapped to the secondary site AVS SDDC as read/write volumes. During test failover, DRO does not map the destination or replica volume. Instead, it creates a new volume of the required cross-region replication snapshot and exposes the volume as a datastore, which consumes additional physical capacity from the capacity pool and ensures that the source volume is not modified. Notably, replication jobs can continue during DR tests or triage workflows. Additionally, this process makes sure that the recovery can be cleaned up without the risk of the replica being destroyed if errors occur or corrupted data is recovered.

### Ransomware recovery

Recovering from ransomware can be a daunting task. Specifically, it can be difficult for IT organizations to pinpoint what the safe point of return is, and, once that's determined, how to ensure that recovered workloads are safeguarded from the attacks reoccurring (for example, from sleeping malware or through vulnerable applications).

DRO addresses these concerns by allowing organizations to recover from any available point-in-time. Workloads are then recovered to functional and yet isolated networks, so that applications can function and communicate with each other but are not exposed to any north-south traffic. This process gives security teams

a safe place to conduct forensics and identify any hidden or sleeping malware.

## Conclusion

The Azure NetApp Files and Azure VMware disaster recovery solution provide you with the following benefits:

- Leverage efficient and resilient Azure NetApp Files cross- region replication.
- Recover to any available point-in-time with snapshot retention.
- Fully automate all required steps to recover hundreds to thousands of VMs from the storage, compute, network, and application validation steps.
- Workload recovery leverages the “Create new volumes from the most recent snapshots” process, which doesn’t manipulate the replicated volume.
- Avoid any risk of data corruption on the volumes or snapshots.
- Avoid replication interruptions during DR test workflows.
- Leverage DR data and cloud compute resources for workflows beyond DR, such as dev/test, security testing, patch and upgrade testing, and remediation testing.
- CPU and RAM optimization can help lower cloud costs by allowing recovery to smaller compute clusters.

## Where to find additional information

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

- Create volume replication for Azure NetApp Files

<https://learn.microsoft.com/en-us/azure/azure-netapp-files/cross-region-replication-create-peering>

- Cross-region replication of Azure NetApp Files volumes

<https://learn.microsoft.com/en-us/azure/azure-netapp-files/cross-region-replication-introduction#service-level-objectives>

- Azure VMware Solution

<https://learn.microsoft.com/en-us/azure/azure-vmware/introduction>

- Deploy and configure the Virtualization Environment on Azure

<https://docs.netapp.com/us-en/netapp-solutions/ehc/azure/azure-setup.html>

- Deploy and configure Azure VMware Solution

<https://learn.microsoft.com/en-us/azure/azure-vmware/deploy-azure-vmware-solution?tabs=azure-portal>

## Migrating Workloads on Azure / AVS

### TR-4940: Migrate workloads to Azure NetApp Files datastore using VMware HCX - Quickstart guide

Author(s): NetApp Solutions Engineering

## **Overview: Migrating virtual machines with VMware HCX, Azure NetApp Files datastores, and Azure VMware solution**

One of the most common use cases for the Azure VMware Solution and Azure NetApp Files datastore is the migration of VMware workloads. VMware HCX is a preferred option and provides various migration mechanisms to move on-premises virtual machines (VMs) and its data to Azure NetApp Files datastores.

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

This document provides step-by-step guidance for provisioning Azure NetApp Files datastore followed by downloading, deploying, and configuring VMware HCX, including all its main components in on-premises and the Azure VMware Solution side including Interconnect, Network Extension, and WAN optimization for enabling various VM migration mechanisms.

 VMware HCX works with any datastore type as the migration is at the VM level. Hence this document is applicable to existing NetApp customers and non-NetApp customers who are planning to deploy Azure NetApp Files with Azure VMware Solution for a cost-effective VMware cloud deployment.

### **High-level steps**

This list provides the high-level steps necessary to install and configure HCX Cloud Manager on the Azure cloud side and install HCX Connector on-premises:

1. Install HCX through the Azure portal.
2. Download and deploy the HCX Connector Open Virtualization Appliance (OVA) installer in the on-premises VMware vCenter Server.
3. Activate HCX with the license key.
4. Pair the on-premises VMware HCX Connector with Azure VMware Solution HCX Cloud Manager.
5. Configure the network profile, compute profile, and service mesh.
6. (Optional) Perform network extension to avoid re-IP during migrations.
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 this [link](#). After the prerequisites, including connectivity, are in place, configure and activate HCX by generating the license key from the Azure VMware Solution portal. After the OVA installer is downloaded, proceed with the installation process as described below.

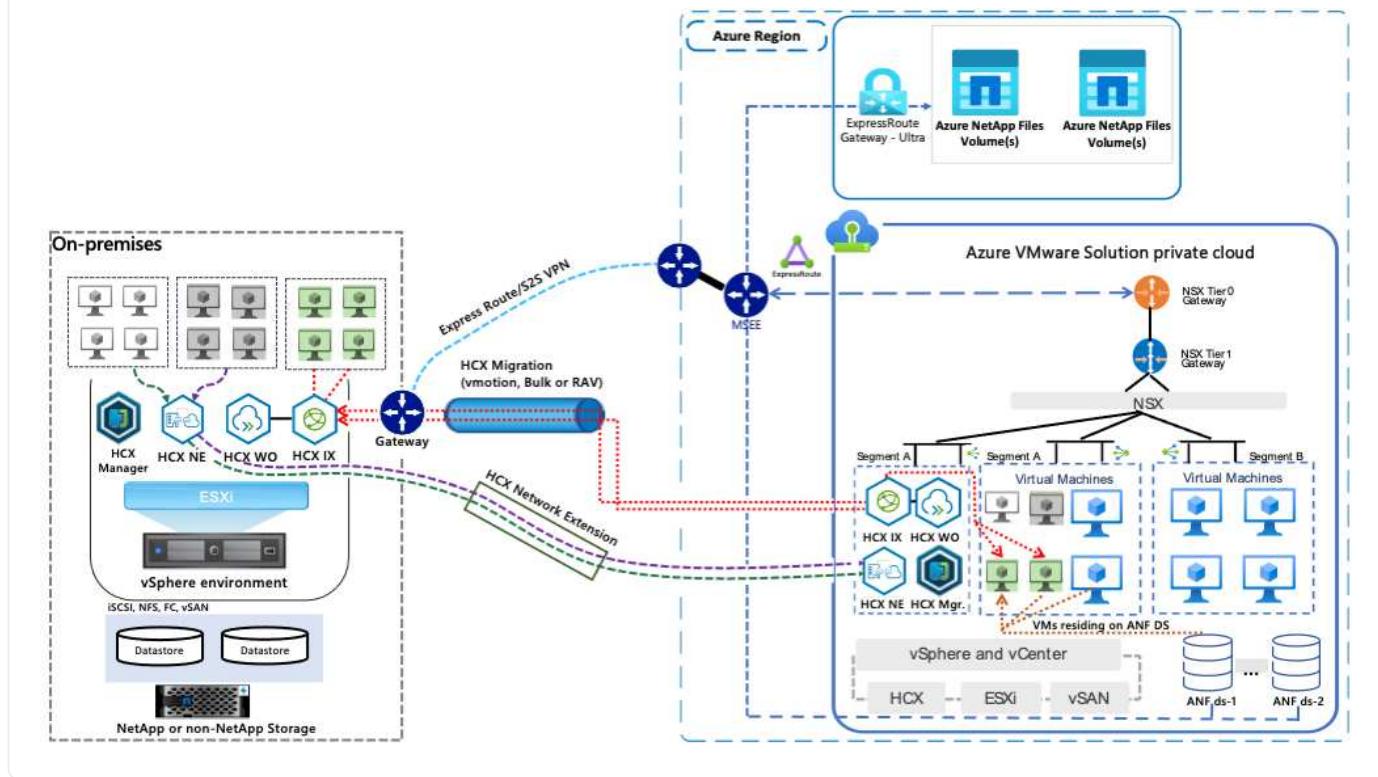


HCX advanced is the default option and VMware HCX Enterprise edition is also available through a support ticket and supported at no additional cost.

- Use an existing Azure VMware solution software-defined data center (SDDC) or create a private cloud by using this [NetApp link](#) or this [Microsoft link](#).
- Migration of VMs and associated data from the on-premises VMware vSphere- enabled data center requires network connectivity from the data center to the SDDC environment. Before migrating workloads, [set up a site-to-site VPN or Express route global reach connection](#) between the on-premises environment and the respective private cloud.
- The network path from on-premises VMware vCenter Server environment to the Azure VMware Solution private cloud must support the migration of VMs by using vMotion.
- Make sure the required [firewall rules and ports](#) are allowed for vMotion traffic between the on-premises vCenter Server and SDDC vCenter. On the private cloud, routing on the vMotion network is configured by default.
- Azure NetApp Files NFS volume should be mounted as a datastore in Azure VMware Solution. Follow the steps detailed in this [link](#) to attach Azure NetApp Files datastores to Azure VMware Solutions hosts.

## High Level Architecture

For testing purposes, the lab environment from on-premises used for this validation was connected through a site-to-site VPN, which allows on-premises connectivity to Azure VMware Solution.



## Solution Deployment

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

## Step 1: Install HCX through Azure Portal using the Add-ons option

To perform the installation, complete the following steps:

1. Log in to the Azure Portal and access the Azure VMware Solution private cloud.
2. Select the appropriate private cloud and access Add-ons. This can be done by navigating to **Manage > Add-ons**.
3. In the HCX Workload Mobility section, click **Get Started**.

The screenshot shows the Azure Portal interface. On the left, there's a sidebar for 'Azure VMware Sol...' with options like 'Create', 'Manage view', 'Add-ons', 'Overview', 'Activity log', 'Access control (IAM)', 'Tags', 'Diagnose and solve problems', 'Locks', 'Manage', 'Connectivity', 'Clusters', 'Identity', 'Storage (preview)', 'Placement policies', and 'Workload Networking'. The 'Add-ons' option is selected. On the right, the main content area is titled 'AVSANFValClus | Add-ons' and shows sections for 'Overview', 'Disaster recovery', and 'Migration using HCX'. A heading 'Enhance your private cloud with these optional features' is followed by three cards: 'Disaster Recovery' (with a 'Get Started' button), 'HCX Workload Mobility' (with a 'Get Started' button, which is highlighted with a red box), and 'Configure Azure Arc' (with a 'Get Started' button). At the bottom left of the main content area, there's a 'Page' navigation bar showing '1 of 1'.

1. Select the **I Agree with Terms and Conditions** option and click **Enable and Deploy**.

- i The default deployment is HCX Advanced. Open a support request to enable the Enterprise edition.
- i The deployment takes approximately 25 to 30 minutes.

The screenshot shows the Microsoft Azure portal interface for managing Azure VMware Solutions. The top navigation bar includes 'Microsoft Azure', a search bar, and user information ('niyaz@netapp.com'). The current page is 'Azure VMware Solution > AVSANFValClus'. On the left, a sidebar lists various management options like 'Create', 'Manage view', 'Search (Cmd +/)', 'Feedback', 'Overview', 'Activity log', 'Access control (IAM)', 'Tags', 'Diagnose and solve problems', 'Settings' (Locks), 'Manage' (Connectivity, Clusters, Identity, Storage (preview), Placement policies, Add-ons), and 'Workload Networking' (Segments, DHCP, Port mirroring, DNS). The 'Add-ons' section is currently selected. The main content area displays the 'AVSANFValClus | Add-ons' page for 'AVS Private cloud'. It features tabs for 'Overview', 'Disaster recovery', and 'Migration using HCX' (which is selected). A note states: 'HCX is an application mobility platform that is designed for simplifying application migration, workload rebalancing, and business continuity across data centers and clouds.' Below this is a checkbox for 'I agree with terms and conditions' (which is checked) followed by a note: 'By selecting above, you hereby acknowledge that HCX is not FedRamp compliant at this time and to be used at own risk.' At the bottom right of the main content area is a large blue 'Enable and deploy' button, which is also highlighted with a red box.

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

For the on-premises Connector to connect to the HCX Manager in Azure VMware Solution, make sure the appropriate firewall ports are open in the on-premises environment.

To download and install HCX Connector in the on-premises vCenter Server, complete the following steps:

- From the Azure portal, go to the Azure VMware Solution, select the private cloud, and select **Manage > Add-ons > Migration** using HCX and copy the HCX Cloud Manager portal to download the OVA file.



Use the default CloudAdmin user credentials to access the HCX portal.

The screenshot shows the Azure VMware Solution interface. On the left, there's a sidebar with options like 'Create', 'Manage view', 'Filter for any field...', 'Name', 'ANF', 'AVS.', 'Settings', 'Manage', 'Workload Networking', and 'Add-ons'. The 'Add-ons' section is currently selected. On the right, under 'Migration using HCX', it says 'HCX is an application mobility platform that is designed for simplifying application migration, workload rebalancing, and business continuity across data centers and clouds.' Below this, there's a section for 'HCX plan' with 'HCX Advanced' selected. Under '1. Configure HCX appliance', it says 'Using the IP address below launch the HCX portal. Download HCX appliance (OVA file) from Administration page and deploy on the site where source vCenter environment is running.' A red box highlights the 'HCX Cloud Manager IP' input field, which contains 'https://172...'. Below this, there's a table for 'HCX key name', 'Activation key', and 'Status'. It lists two entries: 'Test-440' with status 'Consumed' and 'testmig' with status 'Consumed'.

HCX key name	Activation key	Status
Test-440	FADE113ADA46490ABF39C0F...	Consumed
testmig	40DD435CB2F940EF841CF41...	Consumed

- After you access the HCX portal with [cloudadmin@vsphere.local](mailto:cloudadmin@vsphere.local) using the jumphost, navigate to **Administration > System Updates** and click **Request Download Link**.



Either download or copy the link to the OVA and paste it into a browser to begin the download process of the VMware HCX Connector OVA file to deploy on the on-premises vCenter Server.

The screenshot shows the VMware HCX web interface. On the left, there's a navigation sidebar with options like Dashboard, Infrastructure, Services, Administration, and System Updates (which is currently selected). The main area is titled 'System Updates' and contains a section for 'Local HCX'. It shows a table with one row: 'Current Version' (4.3.3.0), 'System Name' (hcx.cloud), 'Status' (av5.azure.co...), 'Info' (HCX Cloud), 'System Type' (3.1.2.0.0.17883600), 'NSX Version' (7.0.3.19234570), and a 'Copy To Clipboard' button. Below this is a 'Remote HCX' section with a table showing a single entry with a funnel icon.

- After the OVA is downloaded, deploy it on to the on-premises VMware vSphere environment by using the **Deploy OVF Template** option.

The screenshot shows the vSphere Client interface with a 'Deploy OVF Template' dialog open. The dialog has six steps: 1. Select an OVF template (radio button for Local file), 2. Select a name and folder, 3. Select a compute resource, 4. Review details, 5. Select storage, and 6. Ready to complete. Step 1 is highlighted with a red box around the 'UPLOAD FILES' field, which contains the path 'http://192.168.1.100:8225/filestore/VMware-HCX-Connector-4.3.3.0.ova'. The 'NEXT' button is at the bottom right of the dialog.

- Enter all the required information for the OVA deployment, click **Next**, and then click **Finish** to deploy the VMware HCX connector OVA.



Power on the virtual appliance manually.

For step-by-step instructions, see the [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 Azure VMware Solution portal and activate it in VMware HCX Manager.

1. From the Azure portal, go to the Azure VMware Solution, select the private cloud, and select **Manage > Add-ons > Migration using HCX**.
2. Under **Connect with on-premise Using HCX keys**, click **Add** and copy the activation key.

The screenshot shows the Azure portal interface. On the left, there's a sidebar for 'Azure VMware Sol...' with sections like 'Create', 'Manage view', 'Filter for any field...', 'Name', 'AN', and 'AV'. The main area is titled 'AVSANFValClus | Add-ons' under 'AVS Private cloud'. It has tabs for 'Overview', 'Activity log', 'Access control (IAM)', 'Tags', 'Diagnose and solve problems', 'Settings' (with 'Locks'), 'Manage' (with 'Connectivity', 'Clusters', 'Identity', 'Storage (preview)', 'Placement policies', and 'Add-ons'), 'Workload Networking' (with 'Segments' and 'DHCP'). The 'Add-ons' section is currently selected. Below it, there's a 'Feedback' section with tabs for 'Overview', 'Disaster recovery', and 'Migration using HCX'. The 'Migration using HCX' tab is active. It contains instructions for configuring the HCX appliance and connecting on-premises using HCX keys. A table lists an activation key: 'HCX key name: hcova' and 'Activation key: A56944E8131D496A9EA80E9...'. The 'Status' column shows a green checkmark and 'Consumed'.



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

1. Log into the on-premises VMware HCX Manager at <https://hcxmanagerIP:9443> using administrator credentials.



Use the password defined during the OVA deployment.

1. In the licensing, enter the key copied from step 3 and click **Activate**.



The on-premises HCX Connector should have internet access.

1. Under **Datacenter Location**, provide the nearest location for installing the VMware HCX Manager on-premises. Click **Continue**.
2. Under **System Name**, update the name and click **Continue**.
3. Click **Yes, Continue**.
4. Under **Connect your vCenter**, provide the fully qualified domain name (FQDN) or IP address of vCenter Server and the appropriate credentials and click **Continue**.



Use the FQDN to avoid connectivity issues later.

1. Under **Configure SSO/PSC**, provide the Platform Services Controller's FQDN or IP address and click **Continue**.



Enter the VMware vCenter Server FQDN or IP address.

1. Verify that the information entered is correct and click **Restart**.
2. After the services restart, vCenter Server is displayed as green on the page that appears. Both vCenter Server and SSO must have the appropriate configuration parameters, which should be the same as the previous page.



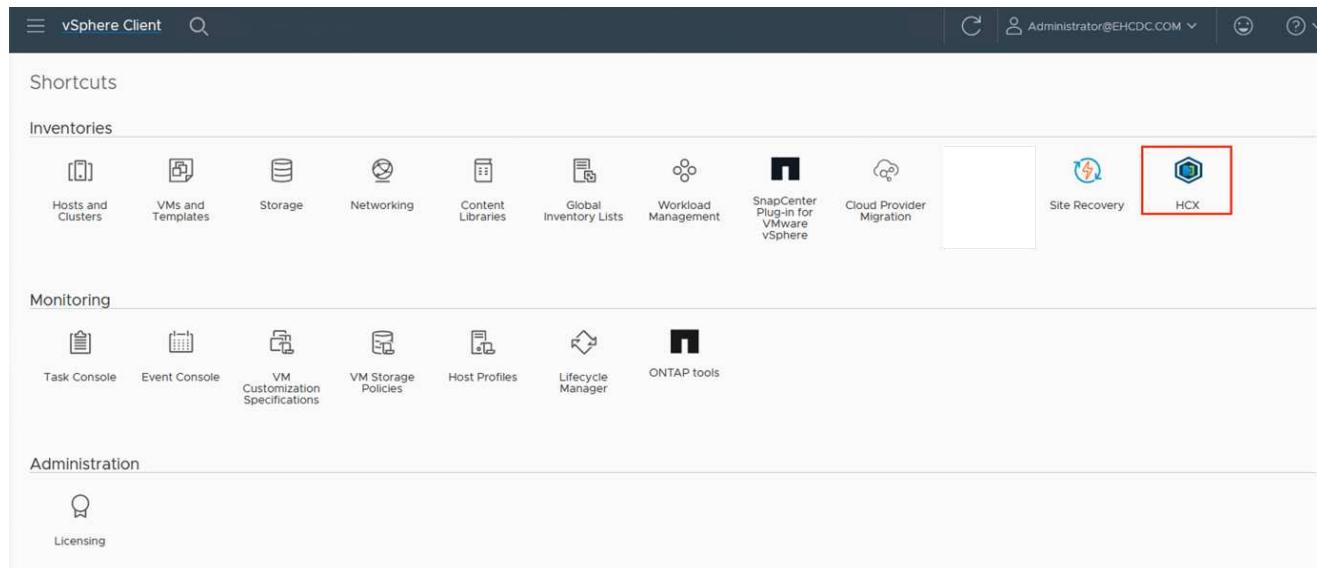
This process should take approximately 10 to 20 minutes and for the plug-in to be added to the vCenter Server.

The screenshot shows the HCX Manager UI dashboard. At the top, there are tabs for HCX Manager, Dashboard, Appliance Summary, Configuration, and Administration. The user is logged in as admin. Below the tabs, there is a summary for the appliance "VMware-HCX-440". It shows the FQDN as "VMware-HCX-440.ehcdc.com", IP Address as "172.2", Version as "4.4.1.0", Uptime as "20 days, 21 hours, 9 minutes", and Current Time as "Tuesday, 13 September 2022 07:44:11 PM UTC". To the right of this summary are three resource utilization bars: CPU (Free 688 MHZ, Used 1407 MHZ, Capacity 2095 MHZ, 67%), Memory (Free 2316 MB, Used 9691 MB, Capacity 12008 MB, 81%), and Storage (Free 98G, Used 29G, Capacity 127G, 23%). Below the summary, there are three cards: NSX, vCenter, and SSO. The vCenter card contains the URL "https://a300-vcsa01.ehcdc.com" and has a green status indicator. This URL is also highlighted with a red box. The SSO card contains the URL "https://a300-vcsa01.ehcdc.com" and has a grey status indicator. Both the vCenter and SSO cards have a "MANAGE" button below them.

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

After HCX Connector is installed in both on-premises and Azure VMware Solution, configure the on-premises VMware HCX Connector for Azure VMware Solution private cloud by adding the pairing. To configure the site pairing, complete the following steps:

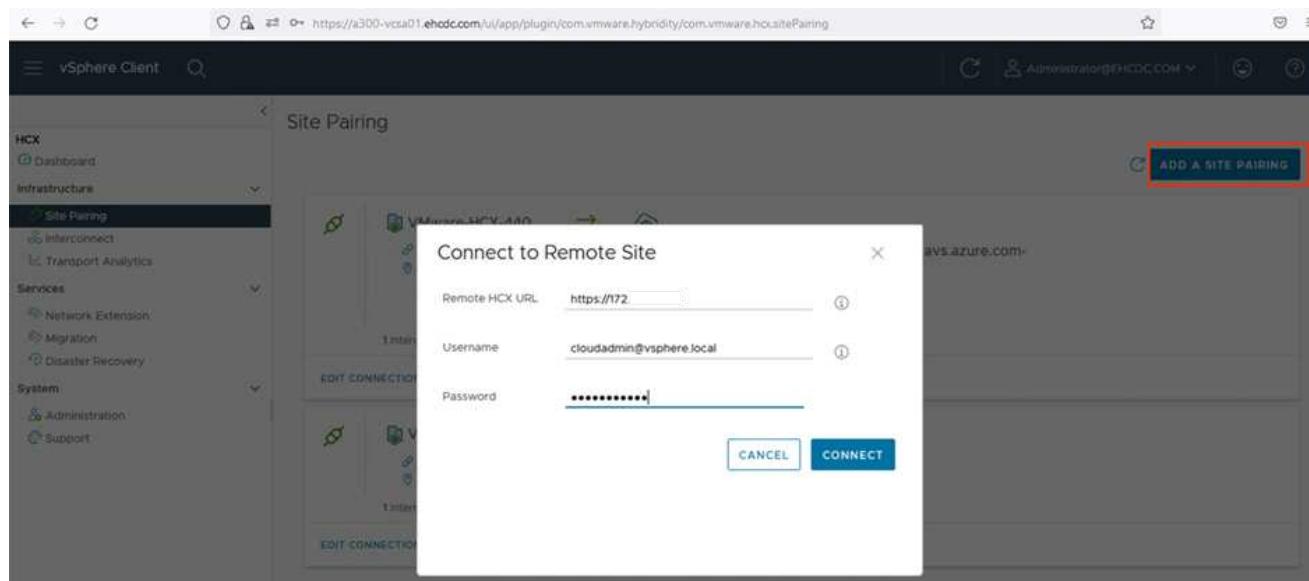
1. To create a site pair between the on-premises vCenter environment and Azure VMware Solution SDDC, log in to the on-premises vCenter Server and access the new HCX vSphere Web Client plug-in.



1. Under Infrastructure, click **Add a Site Pairing**.



Enter the Azure VMware Solution HCX Cloud Manager URL or IP address and the credentials for CloudAdmin role for accessing the private cloud.



1. Click **Connect**.



VMware HCX Connector must be able to route to HCX Cloud Manager IP over port 443.

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

The screenshot shows the vSphere Client interface with the HCX dashboard selected. The main pane displays the 'Site Pairing' section. Two site pairings are listed:

- VMware-HCX-440 → hcx.8ebf3b0b7ddf4cc08e3f85.westeurope.avs.azure.com-cloud**
  - Left Site: VMware-HCX-440 (https://172.21.254.157:443, Raleigh)
  - Right Site: hcx.8ebf3b0b7ddf4cc08e3f85.westeurope.avs.azure.com-cloud (https://172.30.156.9, Amsterdam)
  - Interconnects: 1 Interconnect(s)
  - Actions: EDIT CONNECTION, DISCONNECT
- VMware-HCX-440 → HCX**
  - Left Site: VMware-HCX-440 (https://172.21.254.157:443, Raleigh)
  - Right Site: HCX (https://, US W)
  - Interconnects: 1 Interconnect(s)
  - Actions: EDIT CONNECTION, DISCONNECT

A red box highlights the first site pairing entry.

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

The VMware HCX Interconnect service appliance provides replication and vMotion-based migration capabilities over the internet and private connections to the target site. The interconnect provides encryption, traffic engineering, and VM mobility. To create an Interconnect service appliance, complete the followings steps:

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



The compute profiles define the deployment parameters including the appliances that are deployed and which portion of the VMware data center are accessible to HCX service.

The screenshot shows the vSphere Client interface with the 'HCX' section selected in the sidebar. Under 'Multi-Site Service Mesh', the 'Compute Profiles' tab is active. A profile named 'hcxdemo' is displayed, showing its configuration details. The profile includes service resources (a300-vcsa01.ehcdc.com, A300-Cluster01), deployment containers (a300-vcsa01.ehcdc.com, A300-Cluster01), and networks (VM\_3510). It also lists a datastore (A300\_NFS\_D504) and CPU/Memory reservations (100% / 100%). A note indicates that this profile is used in 2 Service Mesh(es). A 'CREATE COMPUTE PROFILE' button is visible at the top right.

1. After the compute profile is created, create the network profiles by selecting **Multi-Site Service Mesh > Network Profiles > Create Network Profile**.

The network profile defines a range of IP address and networks that are used by HCX for its virtual appliances.



This step requires two or more IP addresses. These IP addresses are assigned from the management network to the Interconnect Appliances.

The screenshot shows the vSphere Client interface for HCX. The left sidebar has 'HCX' selected under 'Interconnect'. The main area is titled 'Interconnect' and 'Multi-Site Service Mesh'. A network profile named 'VM\_3510' is listed, showing its backing as 'VM\_3510'. Network details include MTU (9000), IP Pools (IP Ranges: 172.21.254.80 - 172.21.254.95, IP Usage: 4/16), Prefix Length (24), and Gateway (172.21.254.230). There are 'EDIT' and 'DELETE' buttons at the bottom.

1. At this time, the compute and network profiles have been successfully created.
2. Create the Service Mesh by selecting the **Service Mesh** tab within the **Interconnect** option and select the on-premises and Azure SDDC sites.
3. The Service Mesh specifies a local and remote compute and network profile pair.



As part of this process, the HCX appliances are deployed and automatically configured on both the source and target sites in order to create a secure transport fabric.

The screenshot shows the vSphere Client interface for HCX. The left sidebar has 'HCX' selected under 'Interconnect'. The main area is titled 'Interconnect' and 'Multi-Site Service Mesh'. A service mesh named 'ICC007' is listed, showing a site pairing between 'VMware-HCX-440' (Raleigh, Nodromo) and 'cloud' (Amsterdam, TNT93-HCX-COMPUTE-PROFILE). A message box says 'New version for service mesh appliances is available. Click on Update Appliances to upgrade to latest.' Below the pairing, there's a grid of icons representing HCX Services. Buttons at the bottom include 'VIEW APPLIANCES', 'RESYNC', 'EDIT', 'DELETE', 'UPDATE APPLIANCES', and 'MORE'.

1. This is the final step of configuration. This should take close to 30 minutes to complete the deployment. After the service mesh is configured, the environment is ready with the IPsec tunnels successfully created to migrate the workload VMs.

Screenshot of the vSphere Client interface showing the HCX Interconnect configuration for a multi-site tenant.

**Left Sidebar:**

- HCX
  - Dashboard
  - Infrastructure
  - Site Peering
  - Interconnect** (selected)
  - Transport Analytics
- Services
  - Network Extension
  - Migration
  - Disaster Recovery
- System
  - Administrator
  - Support

**Top Bar:**

- Address bar: https://a300-vctal01.ehdc.com/ui/app/plugin/com.vmware.hybridity/com.vmware.hcx/hybridConnect
- Battery icon: 67%
- User icon: Administrator@EHDCCOM

**Central Content:**

### Interconnect

Multi-Site Tenant

**ICX007**

**Appliances**

Appliance Name	Appliance Type	IP Address	Turner Status	Current Version	Available Version
ICX007-WO-A	HCI-WAN-01	172.21.254.30	Managed	4.4.0.0	4.4.1.0
ICX007-WO-B	HCI-NET-EXT	172.21.254.61	Managed	4.4.0.0	4.4.1.0
ICX007-WO-D	HCI-WAN-DPT		N/A		

**Bottom Content:**

Appliances on hcx.Bebf3b0b7dd4cc08e3f85.westeuropa.avs.azure.com-cloud

Appliance Name	Appliance Type	IP Address	Current Version
ICX007-WO-A	HCI-WAN-01	172.20.198.67 172.20.197.240 172.20.198.17 172.20.198.3	4.4.0.0
ICX007-WO-B	HCI-NET-EXT	172.20.198.64 172.20.198.2	4.4.0.0
ICX007-WO-D	HCI-WAN-DPT		7.3.9.0

## Step 6: Migrate workloads

Workloads can be migrated bidirectionally between on-premises and Azure SDDCs using various VMware HCX migration technologies. VMs can be moved to and from VMware HCX-activated entities using multiple 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 the HCX Enterprise edition).

To learn more about various HCX migration mechanisms, see [VMware HCX Migration Types](#).

### Bulk migration

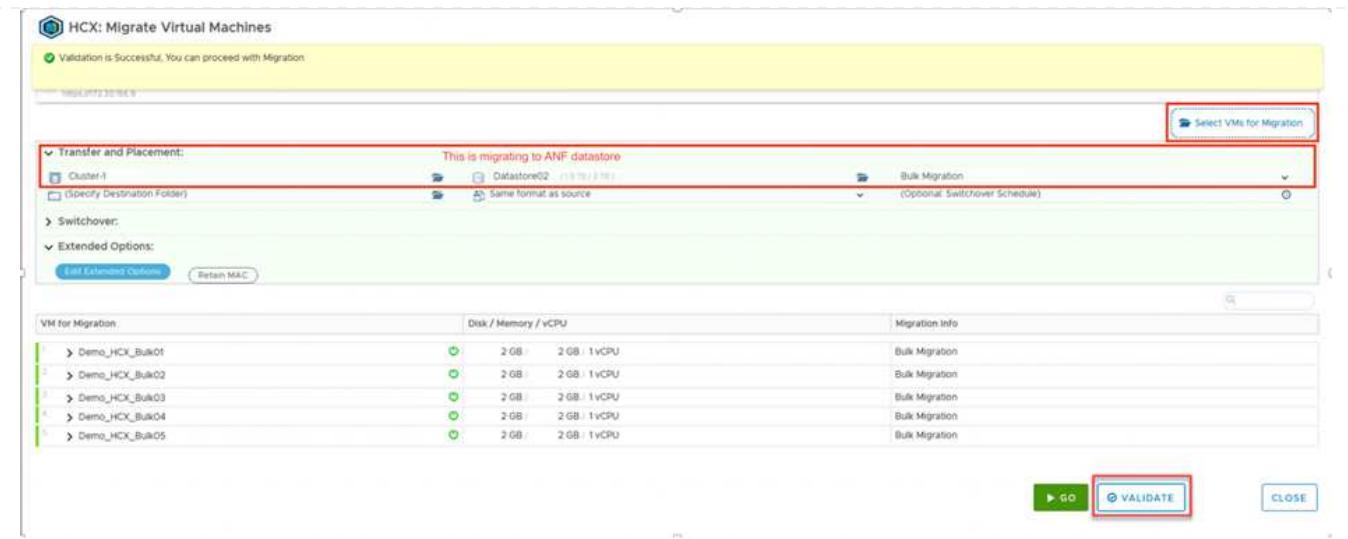
This section details the bulk migration mechanism. During a bulk migration, the bulk migration capability of HCX uses vSphere Replication to migrate disk files while recreating the VM on the destination vSphere HCX instance.

To initiate bulk VM migrations, complete the following steps:

1. Access the **Migrate** tab under **Services > Migration**.

Name	VMs / Storage / Memory / CPUs	Progress	Start	End	Status
2022-09-26 09:00 FLJVU	1 / 2 GB / 2 GB / 1	Migration Complete	-	-	
2022-09-26 08:35 BXMTM	1 / 2 GB / 2 GB / 1	Migration Complete	-	-	
2022-09-19 16:21 ERCZO	(DRAFT) 2 / 4 GB / 4 GB / 2	Draft	-	-	
MG-18cbce94 / Sep 16	Read Only	Migration Complete	12:44 AM Sep 16	-	
MG-04abdee8 / Sep 16	Read Only	Migration Complete	12:25 AM Sep 16	-	
MG-ef7374dd / Sep 16	Read Only	Migration Complete	12:11 AM Sep 16	-	
MG-d2ef93ef / Sep 14	Read Only	Migration Complete	02:05 PM Sep 14	-	
MG-99fecac8 / Sep 14	Read Only	Migration Complete	11:02 AM Sep 14	-	
MG-548618cb / Sep 14	Read Only	Migration Complete	10:04 AM Sep 14	-	
MG-dd475274 / Sep 12	Read Only	Migration Complete	12:25 PM	-	

1. Under **Remote Site Connection**, select the remote site connection and select the source and destination. In this example, the destination is Azure VMware Solution SDDC HCX endpoint.
2. Click **Select VMs for Migration**. This provides a list of all the on-premises VMs. Select the VMs based on the match:value expression and click **Add**.
3. In the **Transfer and Placement** section, update the mandatory fields (**Cluster**, **Storage**, **Destination**, and **Network**), including the migration profile, and click **Validate**.



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

The screenshot shows the vSphere Client interface with the 'Migration' tab selected in the sidebar. The main area displays a 'Migration' table with a single row for 'a300-vcsa01.ehcdc.com → 172.30.156.2'. This row lists six VMs: Demo\_HCX\_Bulk01 through Demo\_HCX\_Bulk05, all in 'Migrating...' status with progress bars. A red box highlights this row. Below the table is a 'Recent Tasks' table showing five completed 'Bulk Migration' tasks for the same VMs, each with a progress bar at 100% and a status of 'Transfer Completed'. A red box highlights this table.

i During this migration, a placeholder disk is created on the specified Azure NetApp Files datastore within the target vCenter to enable replication of the source VM disk's data to the placeholder disks. HBR is triggered for a full sync to the target, and after the baseline is complete, an incremental sync is performed based on the recovery point objective (RPO) cycle. After the full/incremental sync is complete, switchover is triggered automatically unless a specific schedule is set.

- After the migration is complete, validate the same by accessing the destination SDDC vCenter.

Name	Status	Provisioned Space	Used Space	Host CPU	Host Mem
Demo_HCX_Bulk01	Powered On	Normal 2 GB	748.87 MB	0 Hz	264 MB
Demo_HCX_Bulk04	Powered On	Normal 2 GB	751.24 MB	0 Hz	280 MB
Demo_HCX_Bulk02	Powered On	Normal 2 GB	755.46 MB	0 Hz	264 MB
Demo_HCX_Bulk05	Powered On	Normal 2 GB	781.22 MB	0 Hz	258 MB
Demo_HCX_Bulk03	Powered On	Normal 2 GB	755.92 MB	0 Hz	261 MB
Demo_HCX_Bulk06					

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

To learn more about this process, feel free to watch the following video:

### Workload Migration using HCX

Here is a screenshot of HCX vMotion option.

Migrating VM	Storage/ Memory/ CPU	Progress	Start	End	Status
a300-vcsa01.lehcoc.com → 172.30.156.2					
Demo_HCX_VMotion	2 GB 2 GB 1	30% save info Migrating	+101 sec ago Sec 14	11:02 min EST Sec 14	Migration In Progress
Demo_HCX_Catfish01	2 GB 2 GB 1	Migrated Complete	10:04 min EST Sec 14	10:19 min EST Sec 14	Migration completed
HCX_Probe_17	2 GB 2 GB 1	Migrated Complete	12:25 PM EST Sec 12	12:37 PM EST Sec 12	Migration completed
HCX_Probe_18	2 GB 2 GB 1	Migrated Complete	12:25 PM EST Sec 12	12:35 PM EST Sec 12	Migration completed
HCX_Probe_19	2 GB 2 GB 1	Migrated Complete	12:25 PM EST Sec 12	12:35 PM EST Sec 12	Migration completed
HCX_Probe_20	2 GB 2 GB 1	Migrated Complete	12:24 PM EST Sec 13	12:24 PM EST Sec 13	Migration completed
HCX_Demo_26	2 GB 2 GB 1	Migrated Complete	12:01 PM EST Sec 12	12:01 PM EST Sec 12	Migration completed

To learn more about this process, feel free to watch the following video:

### HCX vMotion



Make sure sufficient bandwidth is available to handle the migration.



The target ANF datastore should have sufficient space to handle the migration.

## Conclusion

Whether you're targeting all-cloud or hybrid cloud and data residing on any type/vendor storage in on-premises, Azure NetApp Files and HCX provide excellent options to deploy and migrate the application workloads while reducing the TCO by making the data requirements seamless to the application layer.

Whatever the use case, choose Azure VMware Solution along with Azure NetApp Files 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 network file copy (NFC).

## Takeaways

The key points of this document include:

- You can now use Azure NetApp Files as a datastore on Azure VMware Solution SDDC.
- You can easily migrate data from on-premises to Azure NetApp Files datastore.
- You can easily grow and shrink the Azure NetApp Files 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:

- Azure VMware Solution documentation

<https://docs.microsoft.com/en-us/azure/azure-vmware/>

- Azure NetApp Files documentation

<https://docs.microsoft.com/en-us/azure/azure-netapp-files/>

- 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 ANF

The availability of supplemental NFS datastores on Azure / AVS is defined by Microsoft. First, you need to determine if both AVS and ANF are available in a specific region. Next, you need to determine if the ANF supplemental NFS datastore is supported in that region.

- Check the availability of AVS and ANF [here](#).
- Check the availability of the ANF supplemental NFS datastore [here](#).

## **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.