



NetApp for Azure / AVS

NetApp Solutions

NetApp
February 21, 2023

Table of Contents

- NetApp Hybrid Multicloud Solutions for Azure / AVS 1
 - Protecting Workloads 1
 - Migrating Workloads 39
 - Region Availability – Supplemental NFS datastore for ANF 56

NetApp Hybrid Multicloud Solutions for Azure / AVS

Protecting Workloads

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 VAIO 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 failback 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.



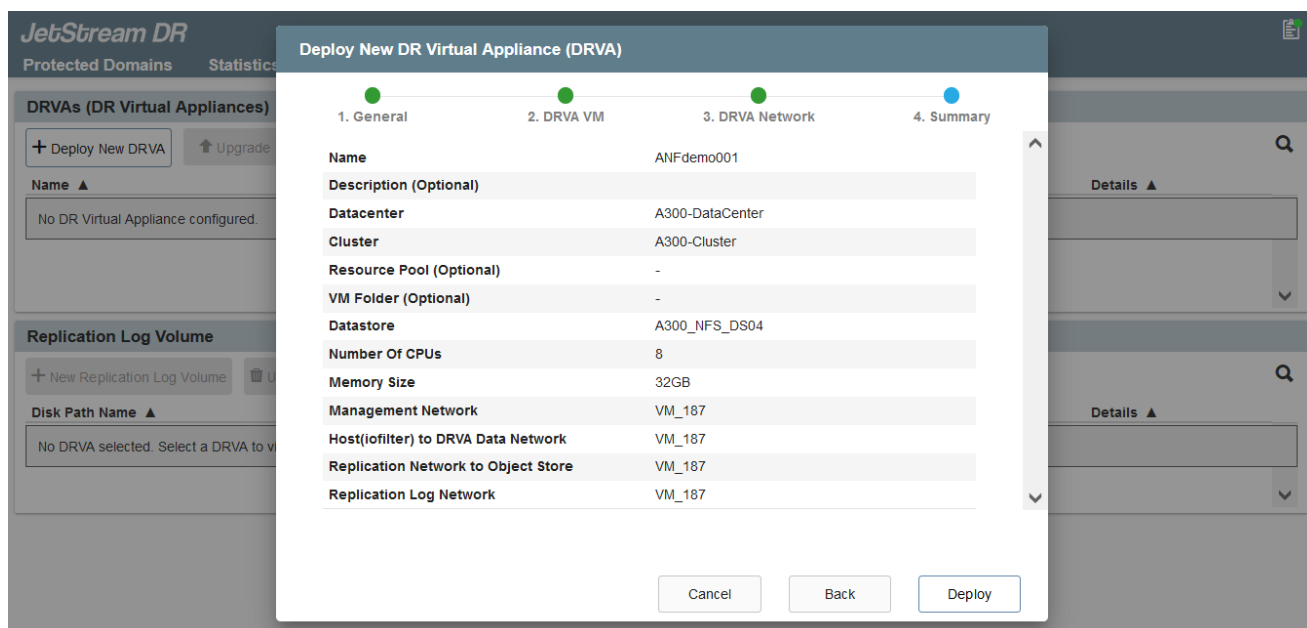
9. Add Azure Blob Storage located at the recovery site.

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 > failback).

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 displays the Microsoft Azure portal interface. On the left, the navigation pane shows the 'Run command' option under the 'Operations' section. The main area shows the 'Run command' window for the 'ANFDataClus' private cloud. The 'Packages' tab is selected, showing a list of available commands. The 'Install-JetDRWithDHCP' command is highlighted. The right pane shows the configuration details for this command, including command parameters, protected cluster, datastore, VM name, cluster, and credentials.

Name	Description
JSDR.Configuration (2.0.6)	Powershell Module for configuration of Jetstream Software on AVS. See Jetstream Software for support
Disable-JetDRForCluster	This Cmdlet unconfigures a cluster but doesn't uninstall JetDR completely so other clusters policies.
Enable-JetDRForCluster	This Cmdlet configures an additional cluster for protection. It installs vibs to all hosts in the cluster.
Install-JetDRWithDHCP	This top level Cmdlet Downloads JetDr bundle from MMS, creates a new user, assigns elevated privileges to the user, registers vCenter to the JetDr MSA, configures cluster.
Install-JetDRWithStaticIP	This top level Cmdlet Downloads JetDr bundle from MMS, creates a new user, assigns elevated privileges to the user, registers vCenter to the JetDr MSA, configures cluster.
Invoke-PreflightJetDRInstall	This Cmdlet checks and displays current state of the system It checks whether the minimal 4 hosts, if the cluster details are correct, if there is already a VM with the same name provisioned.
Invoke-PreflightJetDRUninstall	This Cmdlet checks and displays current state of the system It checks whether the minimal 4 hosts, if the cluster details are correct and if any vCenter is registered to the MSA.
Uninstall-JetDR	The top level Cmdlet creates a new user, assigns elevated privileges to the user, unconfigures cluster.

Run command - Install-JetDRWithDHCP

This top level Cmdlet Downloads JetDr bundle from MMS, creates a new user, assigns elevated privileges to the user, registers vCenter to the JetDr MSA, configures cluster.

Command parameters

RegisterWithDHCP ☒

ProtectedCluster *

Datastore *

VMName *

Cluster *

Credential *

Username *

Password *

HostName

Network *

Details

Retain up to

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 anfsval-msa

Software Version 4.0.2.450

Subscription ID - [Configure](#)

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

Application Secret - [Configure](#)

<input type="checkbox"/> Cluster Name ▲	Datacenter Name ▲	Status ▲	Software Version ▲	Host Details ▲
<input type="checkbox"/> 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.

JetStream DR

Protected Domains

Storage Sites

+ Add Storage Site

Name ▲

ANFDemob...

Available Protected Domain(s) For Import

Protected Domain ...	Description	Recoverable V...	VMs ...	Import
ANFPD000	Protected Domain Tile0	20	20	Import
ANFPD001	-	20	20	Import
ANFPD002	Protected Domain 02	20	20	Import
ANFPD003	Protected Domain Tile 03	20	20	Import

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 / Failback

How to perform a Failover / Failback

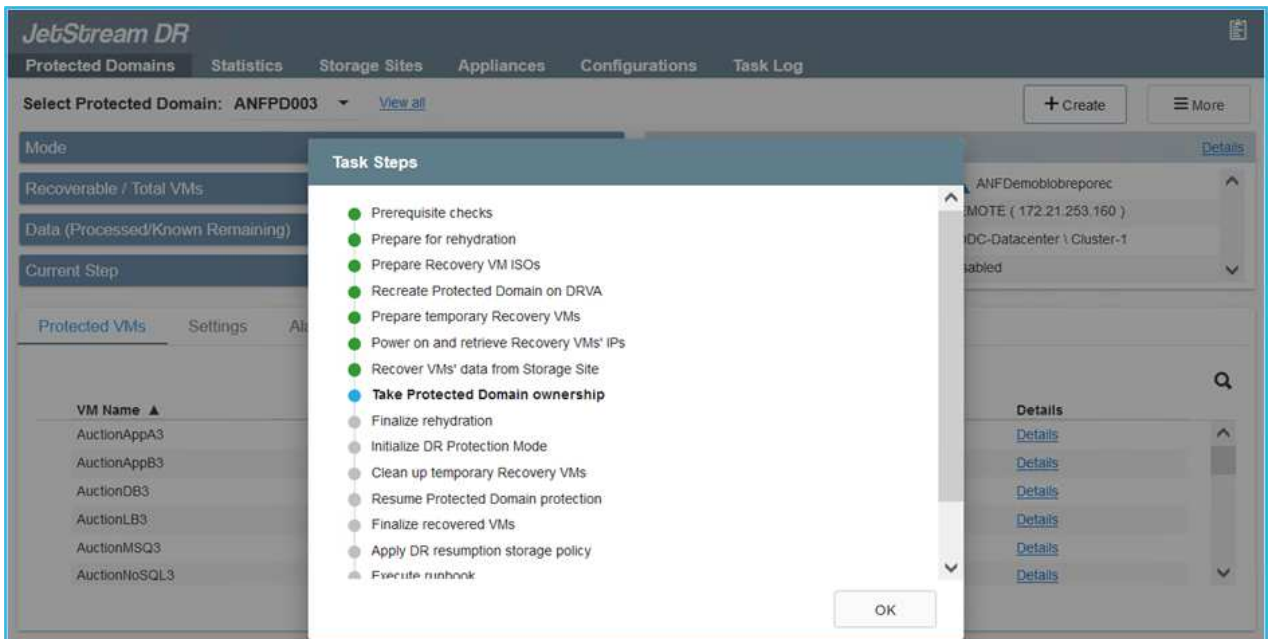
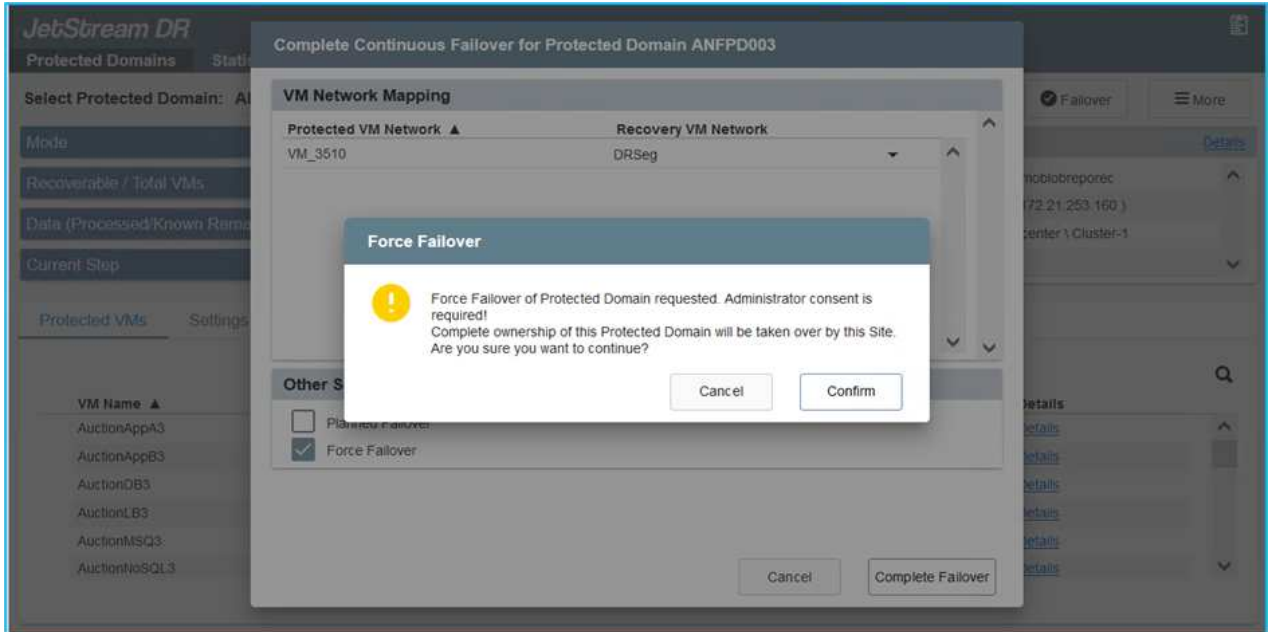
1. After a disaster occurs in the protected cluster of the on-premises environment (partial or full failure), trigger the failover.



CPT can be used to execute the failover plan to recover the VMs from Azure Blob Storage into the AVS cluster recovery site.



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.



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.





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.



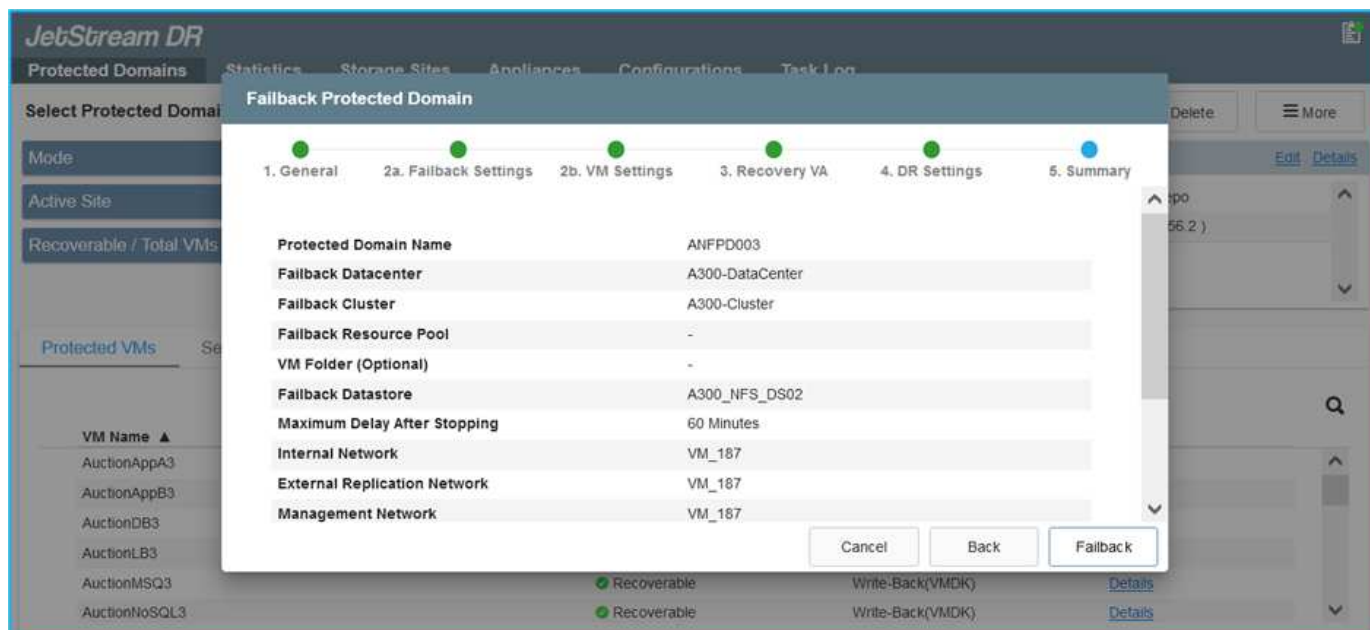
Specify the maximum delay after pausing VMs in the recovery site and restarting in the protected site. This time includes completing replication after stopping failover VMs, the time to clean recovery site, and the time to recreate VMs in protected site. The NetApp recommended value is 10 minutes.

Complete the failback 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.



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.



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.



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	...
	gcsdrsqhld_sc46_copy ANFCVODRDemo	gcsdrsqhld_sc46 ntaphci-a300e9u25	7 seconds	idle	snapmirrored	May 6, 2022, 11:42:20 AM 7.22 MiB	...
	gcsdrsqlog_sc46 ntaphci-a300e9u25	gcsdrsqlog_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.



7. From the JetStream DR interface, complete the following tasks:
 - a. Configure the cluster with the I/O filter package.



- 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.



10. 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.



11. 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.



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



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.

JetStream DR

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

Select Protected Domain: GCSDRPD_Demo01 [View all](#)

Recoverable / Total VMs: 0 / 5

Replication Status: OK

Remaining Background Data: 0 B

Current RPO: -

Configurations

- Storage Site: ANFDRD
- Owner Site: LOCAL (172.2)
- Datacenter \ Cluster: A300-DataCen
- Point-in-time Recovery: Disabled

Running Tasks

- Start Protection (GCS-DR-SCA) 50%
- Start Protection (GCS-DR-Win...) 50%
- Start Protection (GCS-DR-Lin...) 50%
- Start Protection (GCS-DR-DC) 50%
- Start Protection (GCS-DR-SQ...) 50%
- Configure VMDK Re... Completed

Protected VMs | Settings | Alarms

+ Start Protection | Stop Protection

VM Name	Protection Status	Replication Status	Protection Mode	Background Data	Details
GCS-DR-DC	Initializing	-	Write-Back(VMDK)	-	Details
GCS-DR-LinVM01	Initializing	-	Write-Back(VMDK)	-	Details
GCS-DR-SCA	Initializing	-	Write-Back(VMDK)	-	Details
GCS-DR-SQL01	Initializing	-	Write-Back(VMDK)	-	Details
GCS-DR-WinVM01	Initializing	-	Write-Back(VMDK)	-	Details

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

JetStream DR

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

Select Protected Domain: GCSDRPD_Demo01 [View all](#)

Recoverable / Total VMs: 5 / 5

Replication Status: OK

Remaining Background Data: 0 B

Current RPO: 0s

Configurations

- Storage Site: ANFDRDdemoFailoverSite
- Owner Site: LOCAL (172.21.253.160)
- Datacenter \ Cluster: A300-DataCenter \ A300-Cluster
- Point-in-time Recovery: Disabled

Protected VMs | Settings | Alarms

+ Start Protection | Stop Protection

VM Name	Protection Status	Replication Status	Protection Mode	Background Data	Details
GCS-DR-DC	Recoverable	OK	Write-Back(VMDK)	0 B	Details
GCS-DR-LinVM01	Recoverable	OK	Write-Back(VMDK)	0 B	Details
GCS-DR-SCA	Recoverable	OK	Write-Back(VMDK)	0 B	Details
GCS-DR-SQL01	Recoverable	OK	Write-Back(VMDK)	0 B	Details
GCS-DR-WinVM01	Recoverable	OK	Write-Back(VMDK)	0 B	Details



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.

JetStream DR

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

Select Protected Domain: GCSDRPD_Demo01 [View all](#)

Recoverable / Total VMs: 5 / 5

Replication Status: OK

Remaining Background Data: 0 B

Current RPO: 0s

Configurations

- Storage Site: ANFDRDdemoFailoverSite
- Owner Site: LOCAL (172.21.253.160)
- Datacenter \ Cluster: A300-DataCenter \ A300-Cluster
- Point-in-time Recovery: Disabled

Protected VMs | **Settings** | Alarms

+ Create | Delete | More

Failover Runbook	Not Configured	Configure
Test Failover Runbook	Not Configured	Configure
Failback Runbook	Not Configured	Configure
Memory Setting	Not Configured	Configure
GC Settings	Configured	Configure
Concurrency Settings	Not Configured	Configure

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.



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.



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 failback runbooks is now listed as Configured. Failover and failback 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.



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



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.



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: anjfsval-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](#)

<input type="checkbox"/> Cluster Name ▲	Datacenter Name ▲	Status ▲	Software Version ▲	Host Details ▲
<input type="checkbox"/> Cluster-1	SDDC-Datacenter	Ok	4.0.2.132	Details

3. From the JetStream DR interface, complete the following tasks:
 - a. 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.
 - b. In the pop-up dialog window that appears, select the protected domain to import and then click its Import link.

JetStream DR

Protected Domains Statistics **Storage Sites**

[Add Storage Site](#) [Scan Domains](#) [Remove](#)

Name ▲: ANJFDemo01breporec

Available Protected Domain(s) For Import

Protected Domain ...	Description	Recoverable V...	VMs ...	Import
GCSDRPD_Demo01	Protection domain ANF	5	5	Import

4. 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.

JetStream DR

Protected Domains Statistics Storage Sites Appliances Configurations Task Log

Select Protected Domain: GCSDRPD_Demo01 [View all](#)

[+ Create](#) [Delete](#) [More](#)

Mode Imported

Recoverable / Total VMs 5 / 5

Configurations [Details](#)

Storage Site: ANJFDemo01breporec

Owner Site: -

Protected VMs Settings Alarms

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

5. 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.

JetStream DR

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

Select Protected Domain: **Continuous Failover Protected Domain**

Mode: Recoverable / Total VMs

Protected VMs: AuctionAppA2, AuctionAppB2, AuctionDB2, AuctionLB2, AuctionMSQ2, AuctionNoSQL2

Protected Domain Name: ANFPD002

Datacenter: SDDC-Datacenter

Cluster: Cluster-1

Resource Pool (Optional): -

VM Folder (Optional): -

Datastore: ANFRecoDSU002

Internal Network: DRSeg

External Replication Network: DRSeg

Management Network: DRSeg

Storage Site: ANFDemoblobreporec

DR Virtual Appliance: ANFRecDRVA003

Replication Log Storage: (blank)

Buttons: Cancel, Back, Continuous Failover



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: GCDRDP_Demo01 [View all](#)

+ Create | Delete | More

Mode Imported

Recoverable / Total VMs 5 / 5

Configurations

Storage Site ANFDemoblobrepor

Owner Site REMOTE (172.21.253.11)

Restore

→ Failover

→ Continuous Failover

→ Test Failover

Protected VMs | Settings | Alarms

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

1. 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 displays the 'Replication' section of a management console. At the top, a summary bar shows: 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. The table lists three relationships, all with a 'snapmirrored' mirror state. A context menu is open for the first row, showing options: Information, Break, Reverse Resync, Edit Schedule, Edit Max Transfer Rate, Update, and Delete. The 'Break' option is highlighted. Below the table, a 'Break Relationship' dialog box is shown, asking: 'Are you sure that you want to break the relationship between "gcsdrsqldb_sc46" and "gcsdrsqldb_sc46_copy"?' with 'Break' and 'Cancel' buttons.

Health Status	Source Volume	Target Volume	Total Transfer Time	Status	Mirror State	Last Successful Transfer
✓	gcsdrsqldb_sc46 ntaphci-a300e9u25	gcsdrsqldb_sc46_copy ANFCVODRDemo	6 minutes 41 seconds	idle	snapmirrored	May 5, 2022, 12:08:34 PM 33.66 KiB
✓	gcsdrsqhld_sc46 ntaphci-a300e9u25	gcsdrsqhld_sc46_copy ANFCVODRDemo	4 minutes 56 seconds	idle	snapmirrored	May 5, 2022, 12:09:15 PM 69.84 KiB
✓	gcsdrsqlog_sc46 ntaphci-a300e9u25	gcsdrsqlog_sc46_copy ANFCVODRDemo	10 minutes 18 seconds	idle	snapmirrored	May 5, 2022, 12:08:34 PM 104.34 KiB



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

2. 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

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	ANFDemo01breporec
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(VMDK)	Details
GCS-DR-LinVM01	Recoverable	Write-Back(VMDK)	Details
GCS-DR-SCA	Recoverable	Write-Back(VMDK)	Details
GCS-DR-SQL01	Recoverable	Write-Back(VMDK)	Details
GCS-DR-WinVM01	Recoverable	Write-Back(VMDK)	Details

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](#)

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](#)

- 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.

JetStream DR

Protected Domains | Statistics | Storage

Select Protected Domain: GCSDRPD002

Mode

Recoverable / Total VMs

Replication Status

Remaining Background Data

Current RPO

Protected VMs | Settings | Alarms

+ Start Protection | Stop Protection

- ☐ VM Name ▲
- ☐ GCS-DR-SC46
- ☐ GCS-DR-SQL03
- ☐ GCS-DR-W2K16-01
- ☐ UbuntuSn001

Continuous Rehydration Task Result

Task Completed Successfully with warnings

Protected Domain	GCSDRPD002
VMs Recovery Status	Success with warnings
Total VMs Recovered	4
VM(s) with warning	2 View
GCSRecovery03 Status:	
Pre-script Execution Status	Not defined
Runbook Execution Status	Success
Post-script Execution Status	Not defined

+ Create | Delete | More

ANFCVODR

OCAL (172.30.156.2)

DDC-Datcenter\Cluster-1

disabled

Background Data | Details

B | Details

B | Details

B | Details

B | Details

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 browserN.



- 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.

3 Volume Relationships

Health Status	Source Volume	Target Volume	Total Transfer Time	Status	Mirror State	Last Successful Transfer
✓	gcsdrsqldb_sc46 ntaphci-a300e9u25	gcsdrsqldb_sc46_copy ANFCVODRDemo	6 minutes 41 seconds	idle	broken-off	May 5, 2022, 12:08:34 PM 33.66 KiB
✓	gcsdrsqhld_sc46 ntaphci-a300e9u25	gcsdrsqhld_sc46_copy ANFCVODRDemo	4 minutes 56 seconds	idle	broken-off	May 5, 2022, 12:09:15 PM 69.84 KiB
✓	gcsdrsqlog_sc46 ntaphci-a300e9u25	gcsdrsqlog_sc46_copy ANFCVODRDemo	10 minutes 18 seconds	idle	broken-off	May 5, 2022, 12:08:34 PM 104.34 KiB

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

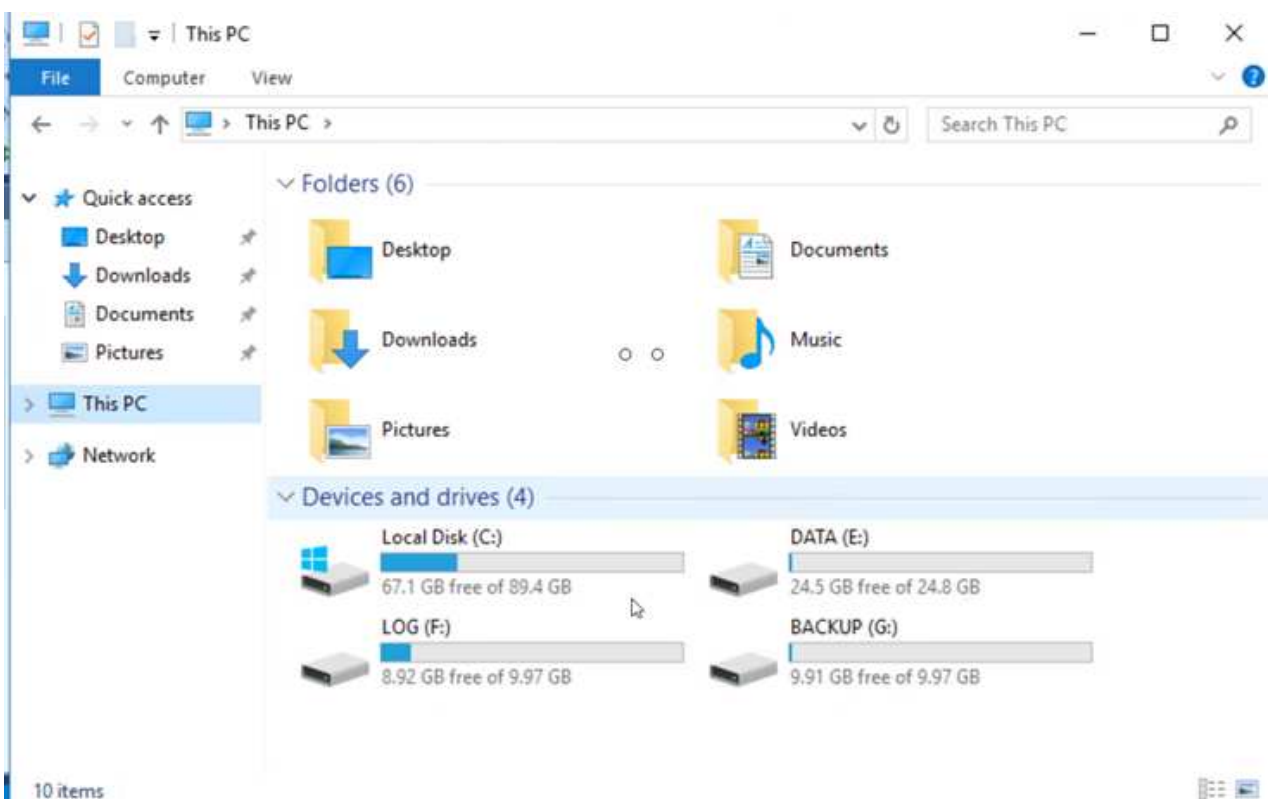
Disk Management

Volume	Layout	Type	File System	Status	Capacity	Free Space	% Free
(C:)	Simple	Basic		Healthy (R...)	450 MB	450 MB	100 %
(D:)	Simple	Basic		Healthy (E...)	99 MB	99 MB	100 %
(E:)	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.



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.



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.

JetStream DR

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

Select Protected Domain: GCSDRPD_Demo01 [View all](#)

Mode: Running in Failover

Active Site: 172.30.156.2

Recoverable / Total VMs: 4 / 4

Configurations

Storage Site	ANFCVODR
Owner Site	REMOTE (172.30.156.2)

Protected VMs | Settings | Alarms

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



Specify the maximum delay after pausing the VMs in the recovery site and restarting them in the protected site. The time need 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.

Failback Protected Domain

1. General 2a. Failback Settings 2b. VM Settings 3. Recovery VA 4. DR Settings 5. Summary

Failback Datacenter	A300-DataCenter
Failback Cluster	A300-Cluster
Failback Resource Pool	-
VM Folder (Optional)	-
Failback 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 Failback

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

JetStream DR

Protected Domains Statistics Storage S...

Select Protected Domain: GCSDRPD002

Recoverable / Total VMs

Replication Status

Remaining Background Data

Current RPO

Protected VMs Settings Alarms

Failback Task Result

✓ Task Completed Successfully

Protected Domain	GCSDRPD002
VMs Recovery Status	✓ Success
Total VMs Recovered	4
GCSRecovery03 Status:	
Pre-script Execution Status	ⓘ Not defined
Runbook Execution Status	✓ Success
Post-script Execution Status	ⓘ Not defined

- 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
✓	gcsdrsqldb_sc46 ntaphci-a300e9u25	gcsdrsqldb_sc46_copy ANFCVODRDemo	6 minutes 41 seconds	idle	broken-off	May 5, 2022, 12:08:34 PM 33.66 KiB
✓	gcsdrsqhld_sc46 ntaphci-a300e9u25	gcsdrsqhld_sc46_copy ANFCVODRDemo	4 minutes 56 seconds	idle	broken-off	
✓	gcsdrsqlog_sc46 ntaphci-a300e9u25	gcsdrsqlog_sc46_copy ANFCVODRDemo	10 minutes 18 seconds	idle	broken-off	

Information

Resync

Reverse Resync

Edit Schedule

Edit Max Transfer Rate

Delete



3

Volume Relationships



6.54 GiB

Replicated Capacity



0

Currently Transferring



3




Healthy



0

Failed

3 Volume Relationships

Health Status	Source Volume	Target Volume	Total Transfer Time	Status	Mirror State	Last Successful Transfer	
	gcsdrsqldb_sc46 ntaphci-a300e9u25	gcsdrsqldb_sc46_copy ANFCVODRDemo	19 seconds	idle	snapmirrored	May 6, 2022, 11:03:09 AM 5.73 MiB	
	gcsdrsqhld_sc46_copy ANFCVODRDemo	gcsdrsqhld_sc46 ntaphci-a300e9u25	1 minute 46 seconds	idle	snapmirrored	May 6, 2022, 11:01:39 AM 800.76 MiB	
	gcsdrsqlog_sc46 ntaphci-a300e9u25	gcsdrsqlog_sc46_copy ANFCVODRDemo	51 seconds	idle	snapmirrored	May 6, 2022, 11:03:15 AM 785.8 MiB	

- Restart the MSSQL server service.
- 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

CarDB

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))

```

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

```

Results

	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.

Ready Ln 1 Col 1 Ch 1

- 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.

Migrating Workloads

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**.



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



The default deployment is HCX Advanced. Open a support request to enable the Enterprise edition.



The deployment takes approximately 25 to 30 minutes.

Microsoft Azure

Search resources, services, and docs (G+/I)

niyaz@netapp.com

Home > Azure VMware Solution > AVSANFValClus

Azure VMware Sol...

Hybrid Cloud TME

Create

Manage view

Filter for any field...

Name

ANFD

AVSA

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Locks

Manage

Connectivity

Clusters

Identity

Storage (preview)

Placement policies

Add-ons

Workload Networking

Segments

DHCP

Port mirroring

DNS

AVSANFValClus | Add-ons

AVS Private cloud

Feedback

Overview Disaster recovery Migration using HCX

HCX is an application mobility platform that is designed for simplifying application migration, workload rebalancing, and business continuity across data centers and clouds. [Learn more.](#)

☒ I agree with terms and conditions.
By selecting above, you hereby acknowledge that HCX is not FedRamp compliant at this time and to be used at own risk.

HCX plan HCX Advanced

Enable and deploy

Page 1 of 1

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:

1. 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.



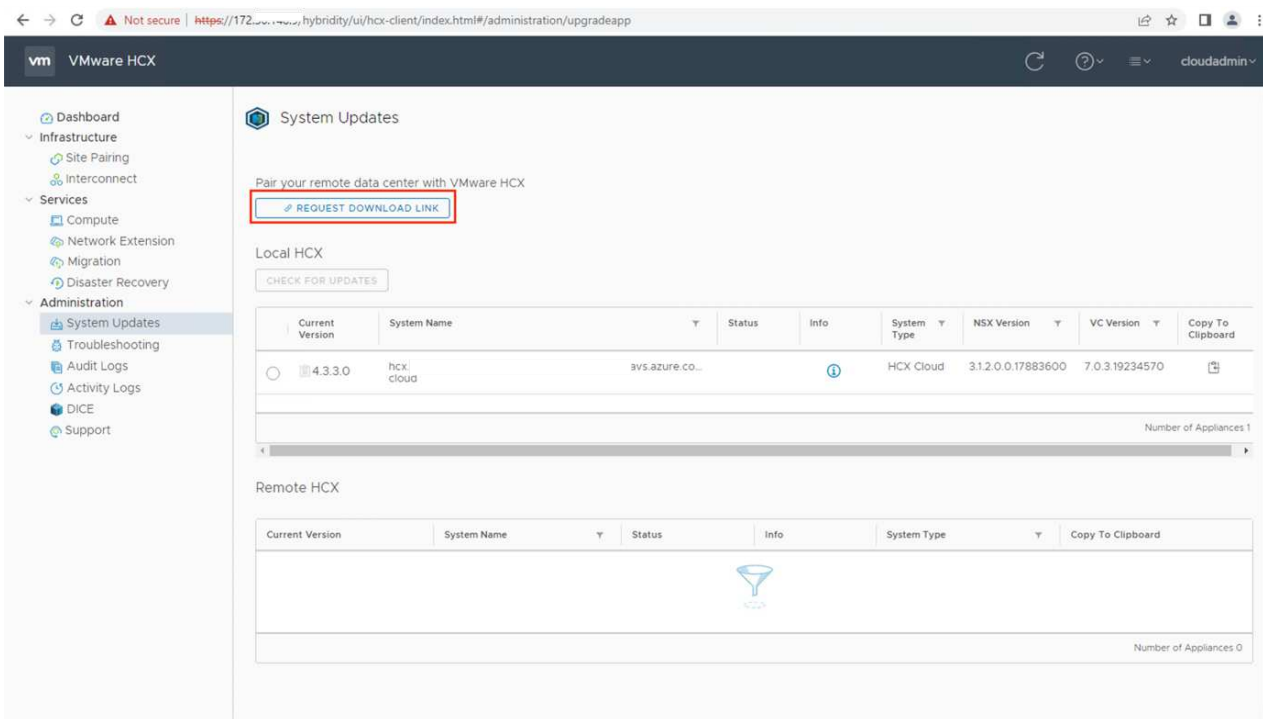
Use the default CloudAdmin user credentials to access the HCX portal.



2. After you access the HCX portal with `cloudadmin@vsphere.local` using the jump host, 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.



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



- 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.



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

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



Use the password defined during the OVA deployment.

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



The on-premises HCX Connector should have internet access.

5. Under **Datacenter Location**, provide the nearest location for installing the VMware HCX Manager on-premises. Click **Continue**.
6. Under **System Name**, update the name and click **Continue**.
7. Click **Yes, Continue**.
8. 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.

9. 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.

10. Verify that the information entered is correct and click **Restart**.
11. 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 VMware HCX Manager dashboard for a device named VMware-HCX-440. The dashboard includes a top navigation bar with tabs for Dashboard, Appliance Summary, Configuration, and Administration. The main content area displays the device's configuration and resource usage.

Device Configuration:

- NAME: VMware-HCX-440
- FQDN: VMware-HCX-440.ehcdc.com
- IP Address: 172.2
- Version: 4.4.1.0
- Uptime: 20 days, 21 hours, 9 minutes
- Current Time: Tuesday, 13 September 2022 07:44:11 PM UTC

Resource Usage:

- CPU:** Free 688 MHz, Used 1407 MHz, Capacity 2095 MHz (67% used)
- Memory:** Free 2316 MB, Used 9691 MB, Capacity 12008 MB (81% used)
- Storage:** Free 98G, Used 29G, Capacity 127G (23% used)

Service Status:

Service	URL	Status	Action
NSX			MANAGE
vCenter	https://a300-vcasa01.ehcdc.com	Green dot (Online)	MANAGE
SSO	https://a300-vcasa01.ehcdc.com		MANAGE

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 plugin.



2. 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.



3. Click **Connect**.



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

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



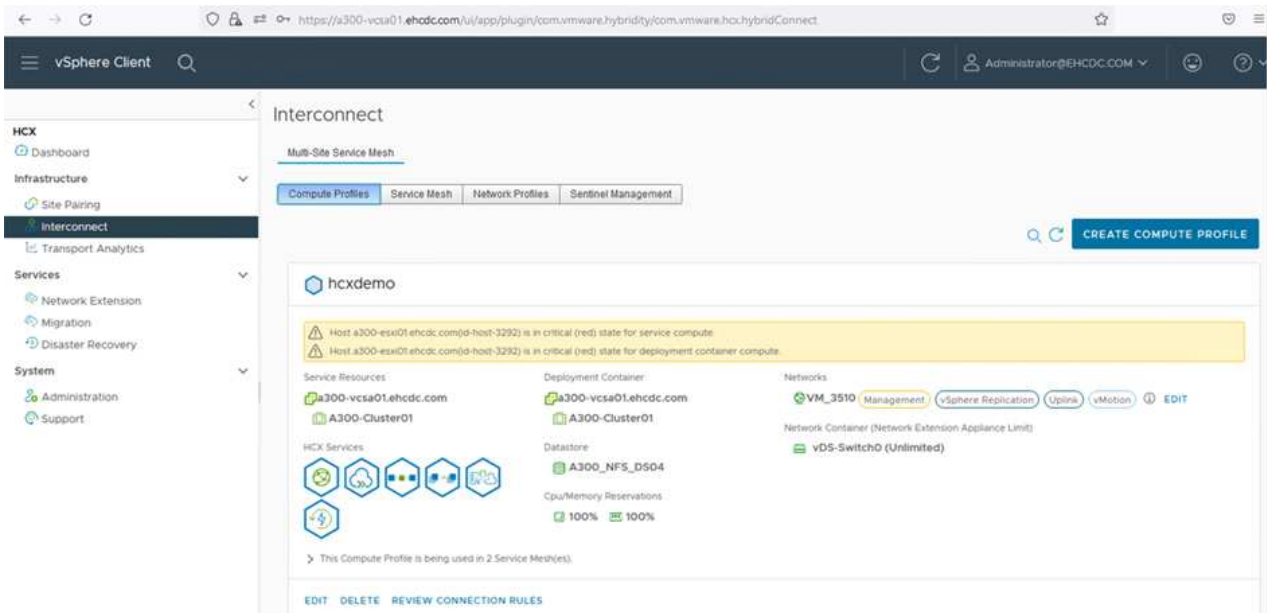
Step 5: Configure the network profile, compute profile, and service mesh

The VMware HCX Interconnect 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.



2. 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.



3. At this time, the compute and network profiles have been successfully created.
4. Create the Service Mesh by selecting the **Service Mesh** tab within the **Interconnect** option and select the on-premises and Azure SDDC sites.
5. 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.



6. 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.

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
▼ a300-vcsa01.ehcdc.com → 172.30.156.2					
> 2022-09-26 09:00 FLJVVU	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	2 4 GB / 4 GB / 2	Draft	-	-	
> MG-18cbce94 / Sep 16	5 10 GB / 10 GB / 5	✓ Migration Complete	12:44 AM Sep 16	-	
> MG-04abdee8 / Sep 16	1 2 GB / 2 GB / 1	✓ Migration Complete	12:25 AM Sep 16	-	
> MG-ef7374dd / Sep 16	1 2 GB / 2 GB / 1	✓ Migration Complete	12:11 AM Sep 16	-	
> MG-d2ef93ef / Sep 14	5 10 GB / 10 GB / 5	✓ Migration Complete	02:05 PM Sep 14	-	
> MG-99fecac8 / Sep 14	1 2 GB / 2 GB / 1	✓ Migration Complete	11:02 AM Sep 14	-	
> MG-548618cb / Sep 14	1 2 GB / 2 GB / 1	✓ Migration Complete	10:04 AM Sep 14	-	
> MG-d6475274 / Sep 12	2 4 GB / 4 GB / 2	✓ Migration Complete	12:25 PM	-	

2. 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.
3. 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**.
4. In the **Transfer and Placement** section, update the mandatory fields (**Cluster**, **Storage**, **Destination**, and **Network**), including the migration profile, and click **Validate**.



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



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.

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



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 follow the detailed walkthrough video:

► https://docs.netapp.com/us-en/netapp-solutions/media/Migration_HCX_AVS_ANF_Bulk.mp4 (video)

Here is a screenshot of HCX vMotion option.



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

► https://docs.netapp.com/us-en/netapp-solutions/media/Migration_HCX_AVS_ANF_VMotion.mp4

(video)



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—without prior written permission of the copyright owner.

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

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

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

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

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

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

Trademark information

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