

NetApp for Azure / AVS

NetApp Solutions

NetApp April 26, 2024

This PDF was generated from https://docs.netapp.com/us-en/netapp-solutions/ehc/azure-native-dr-jetstream.html on April 26, 2024. Always check docs.netapp.com for the latest.

Table of Contents

NetApp Hybrid Multicloud with VMware Solutions	 '	1
Protecting Workloads on Azure / AVS	 '	1
Migrating Workloads on Azure / AVS	 . 60	0
Region Availability – Supplemental NFS datastore for ANF.	 . 7	7

NetApp Hybrid Multicloud with VMware Solutions

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 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.

- 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.
- 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:

- 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:
- 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.

vm vSphere Client	Menu 🗸 🛛 🔍 Search in all	environments	C 💿 v Administrator®EHCDC.COM v 😳
□ □ □ ○ ♀ ~ ⊕ a300-vcsa.ehcdc.com	A300-DataCent Summary Monitor Co	ACTIONS - figure Permissions Hosts & Clusters VMs Datastores Networks U	Updates
 A300-Datacenter A300-Cluster a300-esxi02.eh 	 More Alarm Definitions Scheduled Tasks 	JetiSbream DR Protected Domains Statistics Storage Sites Appliances Configurations	的 Task Log
a300-esxi03.en	Network Protocol Pr	Site Details	Alarm Settings
a300-esxi05.eh	JetStream DR	vCenter Server Hostname 172.21.253.160	
ANFJSDR-MSA0		Management Appliance Hostname ANFJSDR-msa	
AuctionAppA0		Software Version 4.0.0.443	
🔓 AuctionAppA2		Subscription ID 0000000-0000-0000-0000-0000-0000-000	00000001 Configure
🖧 AuctionAppA3		Tenant ID / Application ID - Configure	
AuctionAppB0		Application Secret - Configure	

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

ite Details						Alarm Se
vCenter Server Hostname	172.21.253	160				
Management Appliance Hostname Software Version	Configure Clusters	**				
Subscription ID Tenant ID / Application ID			Select All	Clear All	٩	
Application Secret	Cluster Name	Datacente	er Name 🔺			
Configured Clusters	A300-Citister	ASU0-Date	Geniei			
Configure Cluster						
Cluster Name 🔺					~	Host Details 🔺
No cluster configured			Can	cel Co	nfigure	

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

JetStream DR		1
Protected Domains Statistics	Storage Sites Appliances Configurations Task Log	
Storage Sites	Add Storage Site	
+ Add Storage Site Scan Domains	Shrane StaTine *	(
Name 🛦	▲ Azure Blob Storage	
No Storage Site configured.		
	Access Type * Key Access	
	Sinzana Sile Nama (Brovide a name in identify this Sile) *	
	ANFDemoblobrepo	
Storage Site Details Alarms		
	anfdrdemostor	
No storage site selected. Select a storage		
	Azure Blob Storage Account Key *	
	Cancel Add Storage Site	

- 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.

Jet:Stream DR Protected Domains Statistics	Deploy New DR Virtual	Appliance (DRVA)					
DRVAs (DR Virtual Appliances)	1. General	2. DRVA VM	3. DRVA Network	4. Summary	- 1		
+ Deploy New DRVA	Name		ANFdemo001		^		Q
Name 🔺	Description (Optional)					Details 🔺	
No DR Virtual Appliance configured.	Datacenter		A300-DataCenter				
	Cluster		A300-Cluster				
	Resource Pool (Option	ial)	-				
	VM Folder (Optional)		-				\checkmark
Replication Log Volume	Datastore		A300_NFS_DS04				
	Number Of CPUs		8				0
+ New Replication Log Volume	Memory Size		32GB				q
Disk Path Name 🔺	Management Network		VM_187			Details 🔺	
No DRVA selected. Select a DRVA to v	Host(iofilter) to DRVA	Data Network	VM_187				
	Replication Network to	Object Store	VM_187				
	Replication Log Netwo	rk	VM_187		\sim		\sim
			Cancel Bac	ck Deploy]		

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.

ect Protected Domain:	Create Protected Domain			+ ci	reate E Mor
	•	•	•	<u></u>	
	1. General 2	2. Primary Site	3. Summary	0	
	Protected Domain Name	ANEPD001			
	Priority Level (Optional)	1			
	Total estimated data size to be protec	ted 1000GB			
	DR Virtual Appliance	ANFdemo001			
	Compression	Yes			
	Compression Level	Default			
	Normal GC Storage Overhead	50%			
	Maximum GC Storage Overhead	300%			
	Replication Log Storage	/dev/sdb			
	Replication Log Size	94.31GB			
	Metadata Size	31.56GB		~	
				-	

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.

Select Protected Domain: ANFPD001	Star	t Protection					reate	
Recoverable / Total VMs	Protec Writ	ction Mode for selected VMs e-Back(VMDK)				٩		Edit Details
Replication Status		VM Name 🔺		# of Disks	Protection Mode		ANFDemoblobrepo	^
Remaining Background Data		1	×				AL (172.21.253.160)	
Current RPO		AuctionAppA1		1	Write-Back(VMDK) v	^	bled	~
		AuctionAppB1		1	Write-Back(VMDK) v			
Protected VMs Settings Ala		AuctionDB1		2	Write-Back(VMDK) v			
		AuctionLB1		1	Write-Back(VMDK) V			
+ Start Protection		AuctionMSQ1		1	Write-Back(VMDK) V			Q
		AuctionNoSQL1		2	Write-Back(VMDK) v			
U VM Name ▲		AuctionWebA1		1	Write-Back(VMDK) V		kground Dat Details	
No VM is protected.		AuctionWebB1		1	Write-Back(VMDK) V			
		Client1		1	Write-Back(VMDK) V			
		000004		0	(~		
					Cancel Start Pr	otection		

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.

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.

Microsoft Azure	P. Search revolution, services, and door 15 vi	10	El G 🤌 🛛 🖓 niyazilhetapp.com 🤮
Home > ANFOataClus			Run command - Install-JetDRWithDHCP ×
ANFDataClus Ru	command -		This top level Cristlet Downloads JerDI burdle from MMS, creates a new uses assiste
P Seirch (Chit+))	🔘 Rehisti 🖉 Feedback		elevated prolifeges to the user, deploys JetDr Management Server ApplianceOUS(A), registers vCenter to the JetDr MSA, configures cluster.
Access control (AM)	Peckages Fun execution status		Command parameters
 Diagnose and solve problems 	 Name Description 		AngathiWento ()
Settings	 BDRConfiguration 204 Research Marketor interfacement at active 	er laftener af dels for jefferen faftener ing for samer	Protecte@Custer*
A toda	Duable-letDRiceCuster This Crediet unconfi	pares a cluster but doesn't unrestall JerDR completely so other clusters.	Outer-1
	polos.		Datastore * (j)
Manage	Usable-JetDN/orCluster This Cristlet configu	res an additional cluster for protection. It installs vibs to all hosts in the	vserCatactore
🔶 Connectivity	Install-Set065WebDHCP This top level Gridle	Downloads JetDr bundle from MMS, creates a new user, assigns elev-	VMName* ()
Clusters	registers vCenter to	the JetDr MSA, configures cluster.	artjwał-msa
Identity	Instati-IntDRW/Industrial This top level Cristle registers vCenter to	t Downloads JerDr bundle from MMS, orestes a new user, assigns elev- the JerDr MSA, configures cluster.	Outer* () Outer1
Storage (printew)	Invite PrefightietDSmital Dis Credit checks	ind doplays current state of the system it checks whether the minimal	r- Credential 🕥
Placement policies	4 houts if the chuster	details are correct, if there is already a VM with the same name provid	Otername 50
+ Addiens	Invole-Prefight/etDRUkinstall This Crediet checks	and displays current state of the system it checks whether the minimal	root
I the set	4 hosts if the cluster	details are correct and if any VCenter is registered to the MSA.	Password *
Workload Networking	Univital JetON The top level Ondie	connectes a new user, assigns elevated privilleges to the user, unconfigu	
Segments	> Microsoft,AVS,Management 40.01 whole choice advectation	evel laski in managing klune vinitikee bourtuna	L. HistName ()
DHCF			anfpoal-maa
Port manusing			Network* ()
0 DNS			DRSeg
Operation			Details
			Retain up to
and activities and			

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.

tito Dotaile						Alarm Sott	+
						Additi Oct	un
vCenter Server Hostname	172.30.15	6.2					
Management Appliance Hostname	anfjsval-m	sa					
Software Version	4.0.2.450						
Subscription ID	- <u>Configu</u>	ire					
Tenant ID / Application ID	- Configu	ire					
Application Secret	- Configu	ire					
Configure Cluster	Duconfigure	🛠 Resol	ve Configure	Issue			
Cluster Name	Datacenter I	Name 🔺	Status	A	Software Version	Host Details	
Cluster-1	SDDC-Datac	enter	📀 Ok		4.0.2.132	Details	

3. 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.

letStre	Available Protected	Domain(s) For Import						Ê
	Protected Domain	Description	Recoverable V	VMs	Import		^	
storage Sit	ANFPD000	Protected Domain Tile0	20	20	Import	^	6	
dd Stora	ANFPD001	-	20	20	Import			Q
	ANFPD002	Protected Domain 02	20	20	Import			
noble	ANFPD003	Protected Domain Tile 03	20	20	Import		r	^
	<					>		
								~
rage Si								
age Ac							~	
SL								
Space					Clo	se		
Snace A	larm	Disabled Configure	Marm					

4. 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.

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

ect Protected Domain:	Continuous F	ailover Protected Dom	ain					🖬 Delete		More
le	•	•	•			•				De
overable / Total VMs	1. General	2a. Failover Settings	2b. VM Settings	3. Reco	very VA	4. DR Settings	5. Summary	reporec		
	Protected D	omain Name						253.160)		
	Datacenter	omani Name		SDDC-Datar	enter			1000		
	Cluster			Cluster-1	enter			1000		
	Resource P	ool (Optional)		-				1000		
otected VMs Setti	VM Folder (Optional)		-				1000		
	Datastore			ANFRecoDS	J002			1000		
	Internal Net	work		DRSeg				1000		- 3
VM Name 🔺	External Re	plication Network		DRSeg				1.000	Details	
AuctionAppA2	Managemer	nt Network		DRSeg				1000	Details	
AuctionAppB2	Storage Site	•		ANFDemoble	breporec				Details	
AuctionDB2	DR Virtual A	ppliance		ANFRecDRV	A003				Details	
AuctionLB2	Donligation	l on Storano		idoviedh				~	Details	
AuctionMSQ2					Cancel	Back	Continuous Failov	er	Details	

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.

Protected Domains Statistics	Storage Sites	Appliances	Configurati	ons	Task Log	
Select Protected Domain: ANFPD0	00 - View all		+ Create		Delete	■Mor
Mode	Imported	Configura	itions		O Restore	
Recoverable / Total VMs	20 / 20	Storage Si	te	1	→ Failover	
		Owner Site	•	RE	→ Continuo	us Failove
					→ Test Faild	over
Protected VMs Settings A	larms					
						(
VM Name 🔺	Protec	tion Status 🔺		Protectio	on Mode 🔺	Details
AuctionAppA0	🙆 Rec	overable		Write-Bac	k(VMDK)	Details
AuctionAppB0	Ø Rec	overable		Write-Bac	k(VMDK)	Details

Performing Failover / Failback

 (\mathbf{i})

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.



elect Protected Domain: ANFPD003	✓ Ymm all		+ Create	≡ More
Node	Task Stans			Detail
Recoverable / Total VMs	laak olepa		ANFDemobiobreporec	^
	Prerequisite checks	^	MOTE (172.21.253.160)	
Data (Processed/Known Remaining)	Prepare for rehydration		OC-Datacenter \ Cluster-1	
Surrent Step	 Prepare Recovery VM ISOs 		abled	
	 Recreate Protected Domain on DRVA 			
Protected VMs Settings Ali	 Prepare temporary Recovery VMs 			
	 Power on and retrieve Recovery VMs' IPs 			
	Recover VMs' data from Storage Site			Q
VM Name 🔺	Take Protected Domain ownership		Details	
AuctionAppA3	Initiatize renyonation		Details	^
AuctionAppB3	Clean un temporary Recovery VMs		Details	
Auction/DB3	Resume Protected Domain protection		Details	
AuctionLB3	Finalize recovered VMs		Details	
Auction/MSQ3	Apply DR resumption storage policy		Octails	
AuctionNoSOL3	Everute authook	~	Details	V

The task bar shows progress of failover activities.

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

Protected Domains	Stati	Continuous Rehydration Task Result					. U
elect Protected Dom	nain: Al	Task Completed Successfully				Delete	≡ More
lode						1	dt Detai
		Protected Domain	ANFPD003				
Recoverable / Total VN	lis.	VMs Recovery Status	Success			nobiobreporec	
Replication Status		Total VMs Recovered	20			2 30 106 2)	
	NAME OF COLUMN	testFGP0 Status:				tenter \ Gluster-1	
Remaining Backgroun	d Data	Pre-script Execution Status	Not defined				
urrent RPO		Runbook Execution Status	Success				
		Post-script Execution Status	0 Not defined				
Protected VMs	Settings						
+ Start Protection	0 Stop Pr						q
UM Name A						d D Details	
AuctionAppA3						Details	^
AuctionApp83						Details	
AuctionDB3						Details	
AuctionLB3						Details	
AuctionMSQ3					Dismiss	Details	
AuctionNoSQL3	-	IN RECORCIANT	g UK	THE DOLLEYMEN		Details	Y

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.

4. 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.

Select Protected Domain: ANFPD003	View all		+ Create	Delete	■More
Mode	Running in Failover	Configurations		O Restore	
Active Site	172.30.156.2	Storage Site	🔥 ANF	O Resume Continu	ibus Rehydrati
Recoverable / Total VMs	20 / 20	Owner Site	REMOT	← Failback	
Protected VMs Settings Alarm	S Protection Sta	tus A Protection M	ode A	Details	(
AuctionAppA3	Secoverable	Write-Back(VM	DK)	Details	
AuctionAppB3	Recoverable	Write-Back(VM	DK)	Details	
AuctionDB3	Recoverable	Write-Back(VM	DK)	Details	
AuctionLB3	Recoverable	Write-Back(VM	DK)	Details	
AuctionMSQ3	Recoverable	Write-Back(VM	DK)	Details	



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.

Ransomeware 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.

JetStream DR Protected Domains	tatistics St	orage Sites - Apolia	oces Configu	rations Task I	00.				ß
Select Protected Domai	Failback Prote	ected Domain						Delete	≡ More
Mode	0 1. General	2a. Fallback Settings	2b. VM Settings	3. Recovery VA	4. DR	Settings	5. Summary		Edit Details
Active Site								∧ :po	^
Recoverable / Total VMs	Protected D	omain Name		ANFPD003				56.2)	
	Failback Da	tacenter		A300-DataCenter					
	Failback Clu	uster		A300-Cluster					N.
Destinational Address Con	Failback Re	source Pool		2					
Piotected VMS De	VM Folder (Optional)		×					
	Failback Da	tastore		A300_NFS_DS02				- 200	0
VIII Name A	Maximum D	elay After Stopping		60 Minutes					4
AuctionAppA3	Internal Net	work		VM_187					^
AuctionAppB3	External Re	plication Network		VM_187					
Auction/DB3	Managemer	nt Network		VM_187				~	
AuctionLB3					Cancel	Back	Failback		
AuctionMSQ3			Recoverat	le	Write-Back	K(VMDK)	Deta	105	
AuctionNoSQL3			 Recoverat 	le	Write-Bac	K(VMDK)	Deta	ills	~

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	e
Ø	gcsdrsqidb_sc46 ntaphci-a300e9u25	gcsdrsqldb_sc46_copy ANFCVODRDemo	17 seconds	idle	snapmirrored	May 6, 2022, 11:43:18 AN 105.06 KiB	
⊘	gcsdrsqlhld_sc46_copy ANFCVODRDemo	gcsdrsqlhld_sc46 ntaphci-a300e9u25	7 seconds	idle.	snapmirrored	May 6, 2022, 11:42:20 AN 7.22 MiB	
\odot	gcsdrsqilog_sc46 ntaphci-a300e9u25	gcsdrsqilog_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 inguest storage) by using the VAIO mechanism and by leveraging SnapMirror for application volumes copies to Cloud Volumes ONTAP.

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.
- 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.

JetStream DR				
Protected Domains Statistics Storage Sites A	ppliances Configurations	Task Log		
Site Details				Alarm Settings
vCenter Server Hostname	172.21.253.160			
Management Appliance Hostname	ANFJSDR-msa			
Software Version	4.0.0.443			
Subscription ID	00000000-0000-0000	0-0000-000000000001 Configure		
Tenant ID / Application ID	- <u>Configure</u>			
Application Secret	- <u>Configure</u>			
Configured Clusters	Configure Clusters			
Configure Cluster 1 Upprade D Unconfigure & Res		Select All Clear All	۹	٩
Cluster Name 🔺	Cluster Name 🔺	Datacenter Name	sion 🔺	Host Details 🔺
No cluster configured	A300-Cluster	A300-DataCenter	*	
		l≽		
		Cancel	gure	

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

Storage Sites	Add Storage Site	
+ Add Storage Site Scan Domain	- Stores Site Tune *	
Name 🛦	Azure Blob Storage	
No Storage Site configured		
	Actess Type *	
	ney Access	
	Storage Ste Name (Provide a name to identity this Site) *	
	ANFDemoblobrepo	
Storage Site Details Alarms		
	Acure todo Storage Account valme " anfdrdemostor	
No storage site selected. Select a storage		
	Azure Bob Storage Account Key *	
	······································	

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

(i)

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

Protected Domains Statistics Storage Sites A	ppliances Configurations	Task Log			
DRVAs (DR Virtual Appliances)					
+ Deproy New DRVA DIgrade Di Unconfigure					Q
Name 🔺	Status 🔺	Child Alarm 🔺	Software Version 🔺	Details 🔺	
No DR Virtual Appliance configured.					
Replication Log Volume					
+ New Replication Log Volume					Q
	Status	Child Alarm 🔺	Size (available/total)	Details 🔺	
Disk Path Name 🔺					

JebSbream DR	Statistics	Storage Sites	Deploy New DR Virtua	I Appliance (DRVA)					Ē
DRVAs (DR Virtual A	ppliances)		1. General	2. DRVA VM	3. DRVA Network	4. Summary			
+ Deploy New DRVA	t Uppuda	th Uncontigura	Name		GCSDRPD001		1		Q
Name A			Description (Optional))	Protected Domain for VMs with	ANF and JS		Details A	
No DR Virtual Appliance	configured		Datacenter		A300-DataCenter				
	100001		Cluster		A300-Cluster				
			Resource Pool (Optio	nal)					
			VM Folder (Optional)		(e).				
Replication Los Volu	me		Datastore		A300_NFS_vMotion				
replication cog vole		-	Number Of CPUs		8				
+ MH= Replication Log	vourne 😫 bri	iconfigure	Memory Size		32GB				đ
Disk Path Name			Management Network		VM_187			Details 🔺	
No DRVA selected. Sele	ct a DRVA to via	w reolication loo volum	Host(iofilter) to DRVA	Data Network	VM_187				
			Replication Network b	o Object Store	VM_187				
			Replication Log Netwo	ork	VM_187				
					Cancel Back	Dillelon			

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

Protected Domains Statistics Storage Sites	Appliances Configurations	Task Log			
DRVAs (DR Virtual Appliances)					
+ Deploy New DRVA					C
Name 🔺	Status 🔺	Child Alarm 🔺	Software Version	Details 🔺	
OCSDRPD001	Running	00	4.0.0.134	Detain	
A time Bastating Las Malana River antique					C
L team Mabicandu roð Admus					
Disk Path Name	Status	Child Alarm 🔺	Size (available/total) 🔺	Details A	
Disk Path Name A	Status.	Child Alarm 🔺	Size (available/total) ▲ 179 88 G6 / 200 G8	Details ▲	
Disk Path Name A	Status. Ok	Child Alarm 🔺	Size (available/total) ▲ 179 88 GB / 200 GB	Details ▲	
Preminipation Log Volume Details	Status © Ok	Child Alarm ▲	Size (avvilablentotal) ▲ 179 88 GB / 200 GB	Details ▲ Details	

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.

ect Protected Domain: - Viswall	Create Protected Domain				+ Create = 14
	1. General 2. P	nimary Site	J. Summary		
	Protected Domain Name	GCSDRPD_Demo01		Ĩ	
	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			
	Panlication I on Siza	50GR			
		Cancel	Back Creat	te	

Select Protected Domain: * View all	Create Protected Domain			+ Create
	1. General	2. Primary Site	3. Summary	
	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		
		Concol Do	ek Orento	

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.

JebStream DR Protected Domains Statistics Storage Site	s Apoliances Configurations Task L	00				
Select Protected Domain: GCSDRPD_Demo01	Vit Start Protection				+ Create	lere .
Recoverable / Total VMs				1	14	Detar
	Protection Mode for selected VMs 💌			Q		
Remaining Background Data	VM Name 🔺	# of Disks	Protection Mode		LOCAL (177 21 253 166)	
	ElasticWebA2	1			A300-DetaCenter \A500-Ouster	
Mitteni RPD	ElasticWebA3	1		V	Turaded	
Print and a state of the second state of the s	ElasticWebB0	. 1	with Through	¥.		
erolected vies secolgs ovallitis	ElasticWebB1	it.		- V.,		
+ Start Bastantan Raman	ElasticWebB2	18	Vorie Treologh	10 C		Q
T SHELEWINGSON	ElasticWebB3	17	Write Through	9 -		1525
VM Name A	GCS-DR-DC	1	Write-Through	- N	Background Data A Details	
No VM is producted	GCS-DR-LieVM01	4	Write-Through	×		
	GCS-DR-SCA	1	Write-Through	*		
	GCS-DR-SQL01	.4	Write-Through	~		
	GCS-DR-WeVM01	1	Write-Through	¥		
	Bs-dva-GCSDRPD001	2		20		
	PrimeCkent	2		N 1		
	Standby0	1	with Transfe	1.1		
	Standby1	1				
	C Standby2	1				
	Standbys		Witte Through			
	Valentarik (remplated)			N. 18		
			Cincial Ch	att Destaution		

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

elect Protected Domain: GCSDRPD_Demo01 .	Start Protection				+ Creato
ecoverable / Total VMs				1	Eat Data
epication Status	Write-Back(VMDK)			۹	ANFORDemoFalloverSite
emaining Background Data	VM Name 🔺	# of Disks	Protection Mode		LOCAL (172,21,253,160)
	ElasticWebA2	1	Write-Through		Tournad
	ElasticWebA3	1	Willie-Through 🗸		
And a second second	ElasticWebB0	1	vinite-Through Y		
HURRELEG, VARS BEIDOGE MALAITE	ElasticWebS1	1	Witte-Through		
Laurence Management	ElasticWebB2	1	With-Through		0
T START PRODUCTION	ElasticWeb63	1	With-Through		
VM Name A	GCS-DR-DC	1	(Write-Back(VMDK) V	é .	Background Data A Details
No VM is protected.	GCS-DR-LivVM01	1	Write-Back(VMDK) V		
	C GCS-DR-SCA	1	Write-Back(VMDK) ¥		
	GCS-DR-SQL01	1	Write-Back(VMDK) V		
	GCS-DR-WeVM01	1	Write-Back(VMDK) V		
	jttl-dtva-GCSDRPD001	2	Witte-Trycogt 🗸 🗸		
	PrimeClient	2	With-Through 🗸		
	Standby0	1	with Trengts 🗸 🗸		
	Standby1	1	Wmi-Through 🛶	11 H	
	Standby2	1	White-Through 😪		
	Standby3	-1	Write-Through 🗠	1 II.	
	VMmark-Template01	1	Wills-Through 🗠	- E	
			Cancel Start De	Harting	
			Ganter	Nectory 1	

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.

Protected Domains Statistics Stora	ge Sites Appliances Configurations	Task Log			Running Tasks	
elect Protected Domain: GCSDRPD_Dem	o01 ▼ <u>View all</u>			+ (Start Protection (GCS-DR-SCA)	50%
ecoverable / Total VMs		0/5	Configurations		Start Protection (GCS-DR-Win	50%
eplication Status		ок	Storage Site	ANFDRDe	Start Protection (GCS-DR-Lin	50%
			Owner Site	LOCAL (172.2		-
emaining Background Data		0 B	Datacenter \ Cluster	A300-DataCen	Start Protection (GCS-DK-DC)	50%
urrent RPO			Point-in-time Recovery	Disabled	Start Protection (GCS-DR-SQ	50%
Protected VMs Settings Alarms					Configure VMDK Re Completed	~
Protected VMs Settings Alarms + Start Protection					Configure VMDK Re Completed	
Protected VMs Settings Alarms Start Protection VM Name	Protection Status	Replication Sta	atus 🔺 Protection Mode 🔺	Background Da	Configure VMDK Re _ Completed Close	
Protected VMs Settings Alarms Start Protection VM Name GCS-DR-DC	Protection Status ▲ Initializing	Replication Sta	atus ▲ Protection Mode ▲ Write-Back(VMDK)	Background Da	Configure VMDK Re _ Completed Close Ita A Details Details	
	Protection Status O Initializing O Initializing	Replication Sta	atus ▲ Protection Mode ▲ Write-Back(VMDK) Write-Back(VMDK)	Background Da -	Configure VMDK Re _ Completed Close ta Details Details Details	
	Protection Status ▲ O InitialZing O InitialZing O InitialZing	Replication Sta	atus Protection Mode Write-Back(VMDK) Write-Back(VMDK) Write-Back(VMDK)	Beckground De - -	Configure VMDK Re _ Completed Ctose ta A Details Details Details Details Details	
Protected VMs Settings Alarms	Protection Status ▲ Initializing Initializing Initializing Initializing 	Replication St.	atus Protection Mode A Write-Back(VMDK) Write-Back(VMDK) Write-Back(VMDK) Write-Back(VMDK)	Background Da - - -	Configure VMDK Re _ Completed Close ta A Details Details Details Details Details Details	

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

Protected Domains Statistics Sto	rage Sites Appliances Configurat	ions Task Log				e
elect Protected Domain: GCSDRPD_De	emo01 👻 <u>View all</u>			+ Create	Delete	≡ More
ecoverable / Total VMs		5/5	Configurations			Edit Detail
eplication Status		OK	Storage Site	ANFDRDemoFailo	verSite	
			Owner Site	LOCAL (172.21.253.16	50)	
temaining Background Data		0 B	Datacenter \ Cluster	A300-DataCenter \ A30	0-Cluster	
turrent RPO		05	Point-in-time Recovery	Disabled		
Destacted Vite Cottinge Algeme						
Protected VMs Settings: Alarms Start Protection VM Name	Protection Status	Replication Sta	stus 🔺 Protection Mode 🔺	Background Data 🔺	Details	٩
Protected VMs Settings: Alarms Start Protection VM Name GCS-DR-DC	Protection Status 🔺	Replication Sta	tus Protection Mode Write-Back(VMDK)	Background Data 🔺 0 B	Details Details	٩
Protected VMs Settings Alarms Start Protection VM Name GCS-DR-DC GCS-DR-LinVM01	Protection Status Protection Status	Replication Sta OK OK	tus Protection Mode Write-Back(VMDK) Write-Back(VMDK)	Background Data 🔺 0 B 0 B	Details Details Details	٩
Protected VMs Settings Alarms Start Protection VM Name GCS-DR-DC GCS-DR-DC GCS-DR-SCA	Protection Status Protection Status Recoverable Recoverable Recoverable	Replication Sta	tus Protection Mode Write-Back(VMDK) Write-Back(VMDK) Write-Back(VMDK)	Background Data ▲ 0 B 0 B 0 B	Details Details Details Details	٩
VM S Settings Alarms + Start Protection It Stop Protection ∨ VM Name ▲ GCS-DR-DC GCS-DR-DC GCS-DR-SCA GCS-DR-SCA GCS-DR-SOL01	Protection Status Recoverable Recoverable Recoverable Recoverable Recoverable	Replication Sta	tus ▲ Protection Mode ▲ Write-Back(VMDK) Write-Back(VMDK) Write-Back(VMDK) Write-Back(VMDK)	Background Data ▲ 0 B 0 B 0 B 0 B	Details Details Details Details Details	٩

()

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.

		Bit I strainboard		And a second			C 7		r
select Protected Domain:	GCSDRPD_Demo01 •	View all					+ Create	Delete	≡ More
Recoverable / Total VMs				5/5	Configurations				Edit Detail
Replication Status				ок	Storage Site	A	NFDRDemoFailove	rSite	2
				200	Owner Site	LOCAL	L (172.21.253.160)	
Remaining Background Dat	a			08	Datacenter \ Cluster	A300-I	DataCenter \ A300-	Cluster	
Current RPO				0s	Point-in-time Recovery	Disabi	eđ		
		0	0						
Protected VMs Settin	igs Alarms								
Failover Runbook Not	Configured Configure								
Test Failover Runbook Not	Configured Configure								
Fallback Runbook 👌 Not	Configured Configure								
Memory Setting Not	Configured Configure								
GC Settings Con	figured 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.

Jet/Stream DR Protected Domains Statistics Storage Sites	Failover Runbook Settings				卣
Select Protected Domain: GCSDRPD_Demo01 *	+ Create Group	Delete Group		+ Create Delete	≡ More
Recoverable / Total VMs	O Sroup Name	# of VM Power Off	Retain MAC		Edd Details
Replication Status	O 🗌 Independent VMs	5 -	•	ANFDRDemoFalloverSite	1
Remaining Background Data				LOCAL (172:21.253.160) A300-DataCenter (A300-Cluster	
Current RPO				Disabled	× .
Protected VMs Settings Alarms	0 0				
Failover Runbook Configured Details					
Test Failover Runbook Configured Details					
Fallback Runbook Configured Datality					
Memory Setting Not Configured Contigured					
GC Settings Configured Configure					
Concurrency Settings Not Configured Configures					

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.

JebSbream DR Protected Domains Statistics Storag	Create Runbook Group										劁
Select Protected Domain: GCSDRPD_Demo	1. General	2. Select VM	s	3. Edit V	M Settings		4. Summ	ary	+ Create	Delitte	■ More
Recoverable / Total VMs	Retain MAC		Power Of	f VMs			O Reset		^		
Replacion Status	VM Name	Boot Sequence	Boot Delay	CPU	Memory	Script	NIC		IFORDerniiFallove	rSite .	
Rephining Background Linta	GCS-DR-WinVM01	17 4	0s	32	64 GB	Config	View	-	1 1/2 2 1 293 199		
Concert DDO	GCS-DR-SCA	21 4	0s	4	16 GB	Config	View				
Content to 20	GCS-DR-DC	3 11m+	0s	4	16 GB	Config	View		· · · · · · · · · · · · · · · · · · ·		
Protected VUIs Settlens Alarma	GCS-DR-LinVM01	41 4	0s	2	4 G8	Config	View				
Change in the me	GCS-DR-SQL01	5† 4	0s	4	8 GB	Config	View	-			
Memory Setting Not Configured Cootburds GC Settings Configured Configured Concurrency Settings Not Configured Continues				Ca	incel	Back		Next			

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.

 (\mathbf{i})

Select Protected Don	nain: GCSDRP	D Demo					9				+ Create	Delete	≡ More
			1. General	2. Select VMs	5	3. Edit VI	A Settings		4. Summa	ry			
		_	Retain MAC		Power Off	VMs			O Reset		* 100 mm - 100		
			VM Name	Poot Seguence	Root Delay	COU	Mamoni	Ecript	NIC		VED EDENNOF #	Novar Gille	
			GCS-DR-WinVM01	1 + L	Os	32	64 GB	Config	View	*	L(172-21-253		
			GCS-DR-SCA	27 4	Ds	4	16 GB	Config	CEN		DataGenters A	300-Cluster:	
			GCS-DR-LinVM01	37 1	0s	2	4 GB	Config	View				
			GCS-DR-SQL0	47 4	0s	4	8 GB	Config	View				
		anna:	GCS-DR-DC	514	ÜS.	4	16 GB	Contia	View				
Memory Setting GC Settings	Not Cotificated	Conflicture.											
Memory Setting GC Settings Concurrency Settings	Not Cottigured Configured Car Not Configured	Configuration Southans											
Menory Setting GC Settings Concurrency Settings	Not Configured Configured Car Not Configured	Continues Souths Committee											
Memory Setting GC Settings Concurrency Settings	Not Configured Configured Car Not Configured	Continues Iours Continues											
Menary Setting GC Settings Concurrency Settings	Not Configured Configured Car Not Configured	Continues Fours Communes											
Memory Settings GC Settings Concurrency Settings	Not Configured Configured Case Not Configured	Continue Fours Continue											
Methory Settings GC Settings Concurrency Settings	Net Configured Configured Soci	Continue South											

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

	Label		Network Name	Key	PCI Slot #	IP	
1.	Network a	dapter 1	VM_3510	4000	192	Configure	ally.
Re							
VM No							
Ubum		Configur	e Static IP Address				
GCSD		IP Address *					
609-6	0 0	172.21.25	54.185				
10 Di	0_0	C. Annu Marci	-				
		255.255.2	255.0				
		Gateway *	4.1				
		176.6.1.6.1				_	
		DN/S +					
		172.30.15	53.20			_	
		DNS Suff	is.				
						_	
			Reset	Cance	Conf	gure	
		_			~		
						Close	Next
	_						
NGStream DR Inductor Comains	Section: No	Create Runt	ook Group				
		no 1. Gen	eral Z. Select VMs	3. Edit VM Setti	ngs 4. Summ	ey + Own	
		Group Nat Number o	me f VMs	GCSRecovery 5			
		Retain VM Power Off	's MAC addresses VMs	true faise		Disconstitution	
		Secur	manguinting and boot sequence change will	be applied to both Fallover and	Failbaca runbook.		
			Success				

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.

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.

 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.

= Microsoft Azure	,P Search resources, services, and docs (6+7).	DI DE 🤌 🗇 🗇 🕫 niyazênetapp.com
Home > ANFDataClus	command –	Run command - Install-JetDRWithDHCP ×
P Search (Citrl+/)	🔘 Refresh 🖉 Feedback	This top level Crindre Downloads JeCP trunkle from MMS, contaits a new user, assigns elevated prelifieges to the user, degloss, setth Intergeneems Server Appliance(MSA), registers vCenter to the JeCP, MSA, configures duster.
Access control (IAM) Tags	Packages Run execution status	Command parameters
Diagnose and solve problems	V Name Description	The
Settings	SDR.Configuration 324 Powener Values to conjustor at attorner Solvers or 245 ter gal Disable-letDRForChaster This Condist unconfigures a duster but doe	Initiative as we want to be a second and the second as a second as
Manage	policies. Enable-JetOliforDuster This Cridlet configures an additional duste	for protection. It installs vibs to all hosts in the samOutlastore
Connectivity	Install-JetDRWithDHCP This top level Condiet Downloads JetDr bun registers vCenter to the JetDr MSA; cooligu	Be from MMX5, creates a new user, assigns ellevi ex chatter.
Identity	Instalt-JetDRWitt/StaticIP This top level Cmtilet Downloads JetDr bun registers VCenter to the JetDr MSA, configu	Be from MMS; creates a new user, assigns elevi el duster.1
Storage (preview)	Invoke-PreflightletDRinstall This Conditit checks and displays current sta 4 hosts. If the cluster details are correct, if the	e of the system it checks whether the minimal ere is already a VM with the same name provid Username *
+ Add-ons	Invoke-PreflightLetDRUPrinstall This Circlet checks and displays current sta 4 hosts. If the cluster details are correct and	e of the system it checks whether the minimal if any VCenter is registered to the MSA
Workload Networking	Uninstall-letDR The top level Origins on area a new user, as	kgris elevated privitleges to the user, unconfigu
🔹 Segments	> MicrosoftAVSManagement +107 Whose ondets for epinishetic leve taxs in managing Asive	Mean Sectors Hotelsame ()
T DHOP		anfpvalima
Port mirroring		Network*
O DNS		DRSeg
Operations		Details
E Run command		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.

WART THE COLOR									
Site Details								Alarm Set	ti
vCenter Server Hostna	ime	172.30.15	56.2						
Management Applianc	e Hostname	anfjsval-n	nsa						
Software Version		4.0.2.450							
Subscription ID		- Config	ure						
Tenant ID / Application	ID	- Config	ure						
Application Secret		- Config	ure						
Configure Cluster	1 Upgrade	Duconfigure	* Resol	ve Configure	Issue				
Cluster Name		Datacenter	Name 🔺	Status		Software Version	A	Host Details	5
Cluster-1		SDDC-Data	center	🕝 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	Available Protected Domain(s) For Import	Ű
Storage Sites + Add Storage Site Scan Domains Remove Name A Add Storage Site Participation Site Site Participation Site P	Protected Domain Description Recoverable V VMs Import GCSDRPD_Demo01 Protection domain ANF 5 5 Import	٩
AlfDemoblobreporec		re Blob Storage ^

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.

Select Protected Domain: GCSDRPD_Demo01 🔻 View all			+0	Create 🛢 Delete	≡Mor
Node	Imported	Configurations			De
Recoverable / Total VMs	515 Storage Site			noblobreporec	
		Owner Site	-		
Protected VMs Settings Alarms O O					
Protected VMs Settings Alarms O O					
Protected VMs Settings Alarms O O	Protection Status		Protection Mode 🔺	Detai	ils.
Protected VMs Settings Alarms ○ ○	Protection Status	•	Protection Mode A	Detai Detai	ils Ils
Protected VMs Settings Alarms O O VM Name ▲ GCS-DR-DC GCS-DR-LinvM01	Protection Status Recoverable Recoverable		Protection Mode ▲ Write-Back(VMDK) Write-Back(VMDK)	Detai Detai Detai	45 1 <u>5</u>
Protected VMs Settings Alarms O O VM Name GCS-DR-DC GCS-DR-Lin/M01 GCS-DR-SCA	Protection Status © Recoverable © Recoverable © Recoverable	•	Protection Mode A Write-Back(VMDK) Write-Back(VMDK) Write-Back(VMDK)	Detai Detai Detai	is 15 12
Protected VMs Settings Alarms O O VII Name GCS-DR-DC GCS-DR-Lin/VM01 GCS-DR-SCA GCS-DR-ScL0	Protection Status © Recoverable © Recoverable © Recoverable © Recoverable	•	Protection Mode Write-Back(VMDK) Write-Back(VMDK) Write-Back(VMDK) Write-Back(VMDK)	Detai Detai Detai Detai	85 113 113 113

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

 (\mathbf{i})

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.

ect Protected Domain:	Continuous F	ailover Protected Dom	iain					Delete	=	More
đo	1 Ceneral	23 Esilouar Sattings	Oh VM Sattings	1 Per	Divary VA	A DR Settings	5 Summany			Dela
coverable / Total VMs	1. General	za. ranover settings	zo. vin settings	s. neu	Stell in	4. Dr. astungs	5. Summary	~ reporec		1
	Protected D	omain Name		ANFPD002				253,160)		
	Datacenter			SDDC-Data	enter					
	Cluster			Cluster-1				1000		1
	Resource P	ool (Optional)		•				1000		
rotected VMs Sett	VM Folder (Optional)		÷.				1.000		
	Datastore			ANFRecoDS	U002			100		
	Internal Net	work		DRSeg					-	ం
VM Name A	External Re	plication Network		DRSeg					Details	1
AuctionAppA2	Managemer	nt Network		DRSeg				1000	Dataile	
AuctionDB3	Storage Site	•		ANFDemobil	obreporec			1000	Dutaile	
Auction B2	DR Virtual A	ppliance		ANFRecDRV	/A003				Detaile	
AuctionLD2	Donligation	I an Biarana		Moundaile				<u> </u>	Dutaile	
Auctioninisedz					Cancel	Back	Continuous Failov	er	Littlelity.	

()

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).

elect Protected Domain: GCSDRPD_Demo01 👻 View all	······································		+ Create	Delete	≡ Mor
Node	Imported	Configurations		O Restore	
Recoverable / Total VMs	5/5	Storage Site	ANFDemoblobrepor	→ Failover	
		Owner Site	REMOTE (172.21.253.1)	+ Continuous Fail	over.
				Tast Callman	C
Protected VMs Settings Alarms O O					
198 Manua -	Destantion Status		Destantion Model -	Detaile	
GCS-DR-DC	@ Recoverable		Write-Back(VMDK)	Details	
GCS-DR-LinVM01	@ Recoverable		Write-Back(VMDK)	Details	
	Recoverable		Write-Back(VMDK)	Details	
GCS-DR-SCA	C. COOLONGING				
GCS-DR-SCA GCS-DR-SOL01	© 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.

	Volume II	elationships	4.78 GIB Replicated Capacity	0 Currently Tran	sterring	⊘ 3 Healthy	O Failted	
	3 Volume Relationships							٩
	Health Status	Source Volume :	Target Volume T	Total Transfer Time :	Status	E Mirror State	Last Successful Transfer	0
	0	gcsdrsqldb_sc46 ntaphci-a300e9u25	gcsdrsqldb_sc46_copy ANECVODRDemo K >	6 minutes 41 seconds	idle	shapmirrored	May 5, 2022, 12:08:34 Ph 33.66 Ki8	œ
	0	gcsdrsqfhid_sc46 ntaphci-a300e9u25	gcsdrsqlhid_sc46_copy ANFCVODRDemo	4 minutes 56 seconds	idle	snapmirrored	Information	
	0	gcsdrsqllog_sc46 ntaphci-a300e9u25	gcsdrsqilog_sc46_copy ANECVODRDemo	10 minutes 18 seconds	idle	snapmirrored	Reverse Resync	
	¢						Edit Schedule	
							Edit Max Transfer Rate	
							Update	
							Delete	
s Replication	on Backup & Restore	Data Sense F	ile Cache Compute	Sync All Service	s (+9) 🗸		Delete	
s Replication	on Backup & Restore	Data Sense F elationships	Ile Cache Compute	Sync All Service	≤ (+9) ~ sferring	⊙ 3 Healthy	Delete 0 Failed	
s Replication	m Backup & Restore	Data Sense F elationships	The Cache Compute	Sync All Service	s (+9) ~ sferring	⊙ 3 Healthy	Delete 0 railed	0
s Replication	Backup & Restore Backup & Restore 3 Volume Relationships Health Status	Data Sense F elationships	ile Cache Compute 4.78 GIB Replicated Capacity Break Relationship Are you sure that you want 1 "gcsdrsqldb_sc46_copy"?	Syric All Service	s (+9) ~ sferring ween "gcsdrsqldb	Sc46" and	Delete Delete E E E E Last Successful Transfer	
s Replication	m Backup & Restore 3 Volume Relationships Health Status :	Data Sense F elationships Source Volume gesdrsqldb_sc46 ntaphci-a300e9u25	The Cache Compute	Sync All Service	s (+9) ~ sferring ween "gcsdrsqldb	Scoff" and	Delete Delete 0 Failed Last Successful Transfer May 5, 2022, 12:08:34 Ph 33:66 KlB	0
s Replication	m Backup & Restore 3 Volume Relationships Health Status : ©	elationships	The Cache Compute	Sync All Service	s (+9) ~ sferring ween "gcsdrsqldb	Scafe" and d neel	Delete: Delete: 0 E Last Successful Transfer May 5, 2022, 12:08:34 PM 33:66 KlB May 5, 2022, 12:09:15 PM 69.84 KlB	C

(i)

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.

elect Protected Domain: GCSDRPD_Demo0	1 View all		+ Create	O Freilover	■Mor
Mode	Continuous Rehydration in Progress	Configurations			Details
Recoverable / Total VMs	Total VMs 4/4			porec	-
a (Dimensional Strength CB / 6 19 CB		Owner Site	REMOTE (172.21.25	3.160)	
Data (Processed/Known Remaining)	329.01 GB / 6.19 GB	Datacenter \ Cluster	SDDC-Datacenter \ C	luster-1	
Current Step	Recover VMs' data from Storage Site()	Point-in-time Recovery	Disabled		~
VM Name	Protection Status		Protection Mode	Details	a
GCS-DR-DC	© Recoverable		Write-Back(VMDK)	Details	^
GCS-DR-LinVM01	Recoverable		Write-Back(VMDK)	Details	
GCS-DR-SCA	Recoverable		Write-Back(VMDK)	Detaits	
GCS-DR-SQL01	Recoverable		Write-Back(VMDK)	Details	

Protected VM Network	Recovery VM Network		3
VM_3510	DRStretchSeg	. ^	
0 0		v	
Other Settings Planned Fallover Force Fallover			

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

Ð	Force Failover of Protected Dom required! Complete ownership of this Prot	ain requested. Adminis ected Domain will be ta	trator consent is aken over by this
	Site. Are you sure you want to continu	e?	
		Cancel	Confirm

otected VM Network C3510 DRStretchSeg O O O O O O Planned Failover Force Failover	A Network Mapping				
I_3510 DRStretchSeg ↓ ↓ O O O Planned Failover Force Failover	rotected VM Network 🔺	Recovery VM Network		^	1
O O her Settings Planned Failover Force Failover	J_3510	DRStretchSeg	•	^	
her Settings Planned Failover Force Failover	0 0			× .	
Planned Failover Force Failover	ther Settings				Į.
Force Failover	Planned Failover				
	Force Failover				
ome VM's guest credential are required because of network configuration. Configure	ome VM's guest credential are requi	red because of network configuration: Configuration	lgure		

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.

 $\widehat{}$

i

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.

Select Protected Domain: GCSDRPD002	Task Completed Successfully with	warnings	+ Create Dellate	I More
Node	*			Edit Data
OCCULIANTICS PROVIDENT	Protected Domain	GCSDRPD002	ANECYODR	
eecoverable r socal vites	VMs Recovery Status	Success with warnings	OCAL:(172:30.156.2.)	
	Total VMs Recovered	4	DDC-Datacenter \ Cluster-1	
Instalment Barkerment Data	VM(s) with warning	2 Ylew	esabled	
	GCSRecovery03 Status:			
Arrent RPO	Pre-script Execution Status	Not defined		
	Runbook Execution Status	O Success		
Protected VMs Settings Atarms	Post-script Execution Status	Not defined		
+ Start Protection				c
VM Name A		N	ackground Data 🔺 Details	
GCS-DR-SC46		14	B Details	3
GCS-DR-SQL03			B Datails	
GCSDR-W2K16-01			8 Details	
UbuntuSrv001			B Detuin	

- 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.

ک) اللہ https://gcs-dr-sc46.gcsdc.com:8146/ ک	- ≞× O gcs-dr-	sc46.gcsdc.com ×	
		etApp。。	
	SnapCente	r°	
	Username	gcsdc\adminnimo	
	Password	•••••	
		Sign In	

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

G	🐵 🖪 https://gcs-	r-sc45.gcsdc.com/8145/Administ D + 🗎 C 📑 SnapCenter 🛛 🖈	5 @ @
	NetApp Snap(enter® 🗴 😌 🕶 😫 😌 🛨 gcsdcLadminnimo SnapCenterAdmin 🗊 Sa	gn Out
<		Clobal Settings Policies Users and Access Roles Credential Software	
=	Dashboard		
۲	Resources	Global Settings	
۲	Monitor		
a	Reports	Hypervisor Settings 0	~
*	Hosts	Notification Server Settings 0 0 0	~
20	Storage Systems	Configuration Settings	~
#	Settings	Purge Jobs Settings 0	~
▲	Alerts	Domain Settings 0	~
		CA Certificate Settings 0	~
		Disaster Recovery	~
		Enable Disaster Recovery 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.

Canvas	Replication	Backup & Restore	Data Sense	File Cache	Compute	Sync All Servi	ces (+9) ~			
Repli	cation									
		B Volume Re	lationships	9 4.78 Replicate	GIB ed Capacity	Currently Tr	ansferring	S Healthy	⊗ 0 _{Falled}	
		3 Volume Relationships				0-0				90
		Health Status 🗧	Source Volume	s Target V	olume a	Total Transfer Time	e Status	■ Mirror State	+ Last Successful Transfer	0
		Ø	gcsdrsqldb_sc46 ntaphci-a300e9u25	gcsdrsql ANFCVO	db_sc46_copy DRDemo	6 minutes 41 seconds	idle	broken-off	May 5, 2022, 12:08:34 PN 33.66 KIB	
		\odot	gcsdrsqlhld_sc46 ntaphci-a300e9u25	gcsdrsql ANFCVO	hld_sc46_copy DRDemo	4 minutes 56 seconds	idle	broken-off	May 5, 2022, 12:09:15 PM 69.84 KiB	
		9	gcsdrsqllog_sc46	gcsdrsql	log_sc46_copy	10 minutes 18	idle	broken-off	May 5. 2022, 12:08:34 PN	1000

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

📅 Disk Manageme	nt						0 7-1 8	×
File Action View	v Help							
🗢 🏟 🗖 🚺	m 🗩 🖓 (\$ =1						
Volume	Layout	Туре	File System	Status	Capacity	Free Spa	% Free	
-	Simple	Basic	1 contract of a contract	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 %	
					0	0		

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

Targets	Discovery	Favorite Targets	Volumes and Devices	RADIUS	Configuration
Quick C To disc DNS na	Connect cover and log ame of the ta	on to a target usin arget and then click	g a basic connection, t Quick Connect.	ype the IP	address or
Target	:			Q	uick Connect
Discove	ered targets				Refresh
Discove	ered targets			Status	Refresh
Name	ered targets	netapp:sn.547772c	cc47811ecbb62000	Status Connecte	Refresh d

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

← → ~ ↑ 🛄	> This PC >			v Ö	Search This PC		Q
Quick access Control Desktop Downloads Documents Control Cont	- Folde	Desktop Downloads		Documents			
This PC	- Devi	Pictures ces and drives (4)		Videos			
	1	Local Disk (C:) 67.1 GB free of 89.4 GB LOG (F:) 8.92 GB free of 9.97 GB	A V	DATA (E:) 24.5 GB free of 2 BACKUP (G:) 9.91 GB free of 9	24.8 GB 9.97 GB	1	
							Rec

10. Restart the MSSQL server service.
| ile Action View | Help | | | | | |
|------------------|--|-----------------------------|---------------|---------|--------------|-------|
| • • 🛅 🔛 🖄 | | | | | | |
| Services (Local) | Services (Local) | | | | | |
| | SQL Server (MSSQLSERVER) | Name | Description | Status | Startup Type | Log ^ |
| | 11 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 | SQL Full-text Filter Daemon | Service to la | Running | Manual | NT |
| | Stop the service | SQL Server (MSSQLSERVER) | Provider rto | Running | Automatic | GCS |
| | Restart the service | Q SQL Server Agent (MSS | Start | ning | Automatic | GCS |
| | | SQL Server Browser | Stop | ning | Automatic | Loc |
| | 0 | SQL Server CEIP service | Pause | ning | Automatic | NT |
| | Provides storage processing and | SQL Server Integration S | Resume | ning | Automatic | NT |
| | controlled access of data, and rapid | Q SQL Server Integration S | Restart | ning | Automatic | NT |
| | transaction processing. | SQL Server VSS Writer | | ning | Automatic | Loc |
| | | SSDP Discovery | All Tasks | > ning | Manual | Loc |
| | | State Repository Service | Refresh | ning | Manual | Loc |
| | | Still Image Acquisition E | | | Manual | Loc |
| | | Storage Service | Properties | | Manual (Trig | Loc |
| | | Storage Tiers Managem | Help | | Manual | Loc |
| | | Superfetch | | | Manual | Loc |
| | | Sync Host_df83a | This service | Running | Automatic (D | Loc |
| | | System Event Notification S | Monitors sy | Running | Automatic | Loc V |
| | <u> </u> | | | | | - |

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

iie Edit View Query Project loc 이 - 이 영 - 업 - 업 월 월 / @ N 부 '북 CarDB - ▷	is Window Help ew Query 島岡岡岡岡岡太日台(ツ・ペ・図) Execute ■ ✔ 路回日 路路副国田(国 3	- 5
Object Explorer • • • • • • • • • • • • • • • •	SQLQuery1.sql-GDC\adminnimo (66)) + X /****** Script for SelectTopNRows command fro ESELECT TOP (1000) [Id] ,[Name] ,[Price] FROM [CarDB].[dbo].[Cars]	© 0
External Tables	100 % + 4	
🧰 Graph Tables	I 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	

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.

(i)



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.

Select Protected Domain: GCSDRPD_Demo01 🔻 View all			+ Create	🗑 Delete 📃 🚍	More
Mode	Running in Failover	Configurations		C Restore	
Active Site	172.30.156.2	Storage Site	ANFCVODR	O Resume Continuous Rehy	vdratio
Recoverable / Total VMs	4/4	Owner Site	REMOTE (172.3	← Failback	
Testected Villa Cottingen Alarman					
rotected VMs Settings Alarms O O	Destanting Chains		Destaction Hada a	Details	0
rotected VMs Settings Alarms O O	Protection Status ▲		Protection Mode ▲	Details Details	¢
VM Name ▲ GCS-DR-DC GCS-DR-LinvM01	Protection Status ▲ © Recoverable © Recoverable		Protection Mode ▲ Write-Back(VMDK) Write-Back(VMDK)	Details Details Details	(
rotected VMs Settings Alarms O O O VM Name ▲ GCS-DR-DC GCS-DR-LinVM01 GCS-DR-SCA	Protection Status ▲ © Recoverable © Recoverable @ Recoverable		Protection Mode ▲ Write-Back(VMDK) Write-Back(VMDK) Write-Back(VMDK)	Details Ostails Ostails Ostails	(
Protected VMs Settings Alarms O O O VM Name ▲ GCS-DR-DC GCS-DR-LinVM01 GCS-DR-SCA GCS-DR-SOL01	Protection Status ▲ © Recoverable © Recoverable © Recoverable © Recoverable		Protection Mode ▲ Wirte-Back(VMDK) Wirte-Back(VMDK) Wirte-Back(VMDK) Wirte-Back(VMDK)	Details Details Details Qetails 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.

•	•	•	•			0
. General	2a. Failback Settings	2b. VM Settings	3. Recovery VA	4. DR	Settings	5. Summary
Failback Da	tacenter		A300-DataCenter			
Failback Clu	ister		A300-Cluster			
Failback Re	source Pool					
VM Folder (Optional)					
Failback Da	lastore		A300_NFS_vMotion			
Maximum D	elay After Stopping		10 Minutes			
Internal Net	work		VM_187			
External Re	olication Network		VM_187			
Managemen	t Network		VM_187			
Storage Site			ANFCVODR			
DR Virtual A	ppliance		GCSDRVA002			
Replication	Log Storage		/dev/sdb			

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

JebSbream DR Protected Domains Statistics Storage Si	Failback Task Result	1
Select Protected Domain: GCSDRPD002 *	Task Completed Successfully	
Recoverable / Total VMs	Protected Domain	GCSDRPD002
Replication Status	VMs Recovery Status	Success
Remaining Background Data	Total VMs Recovered	4
	GCSRecovery03 Status:	
Current RPO	Pre-script Execution Status	Not defined
	Runbook Execution Status	O Success
Protected VMs Settings Alarms	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.

\odot	gcsdrsqldb_sc46 ntaphci-a300e9u25	10	gcsdrsqldb_sc46_copy ANFCVODRDemo	6 minutes 41 seconds	idle	broken-off	May 5. 2022. 12:08:34 PN 33,66 KiB
0	gcsdrsqlhld_sc46 ntaphci-a300e9u25		gcsdrsqlhld_sc46_copy ANFCVODRDemo	4 minutes 56 seconds	idle	broken-off	Information
9	gcsdrsqllog_sc46 ntaphci-a300e9u25	19	scsdrsqllog_sc46_copy	10 minutes 18 seconds	idle	broken-off	Resync
							Edit Schedule
							Edit Max Transfer Rate
							Delete

Volume Re	lationships	6.54 GiB Replicated Capacity	Currently Tran	sferring	S Healthy	S O Failed	
Volume Relationships			0 0				Q (
Health Status 🔹	Source Volume 🔹	Target Volume +	Total Transfer Time 🗧	Status		+ Last Successful Transfer	•
\odot	gcsdrsqldb_sc46 ntaphcl-a300e9u25	gcsdrsqldb_sc46_copy ANFCVODRDemo	19 seconds	idle	snapmirrored	May 6. 2022, 11:03:00AN 5.73 MiB	
0	gcsdrsqlhld_sc46_copy ANFCVODRDemo	gcsdrsqlhld_sc46 ntaphci-a300e9u25	1 minute 46 seconds	idle	snapmirrored	May 6, 2022, 11:01:39 AN 800.76 MiB	
\odot	gcsdrsqllog_sc46 ntaphcl-a300e9u25	gcsdrsqllog_sc46_copy ANFCVODRDemo	51 seconds	idle	snapmirrored	May 6, 2022, 11:03:15 AN 785.8 MiB	

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



(i)

i

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.
 - $\circ\,$ 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 datachange 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.



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 https://github.com/NetApp/DRO-Azure.git
```



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

NetApp	
Disaster Recovery Orchestrator Graded Salester with Gur Verraare Passeprid Login	

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.

NetApp Disaster Recovery Orchestrator 🂊 Dashboard	Discover Resource Groups Replication Plans Job Mo	nitoring	a 🗘 3 a
Add New Credential	Credentials Details		×
	Enter Credentials Deta	ils	
	Credential Name		
	Tenant id	•	
	Client Id	•	
	Client Secret	0	
	Subscription Id	•	
	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

NetApp Disaster Recovery Orchestrator A Dashboard Discover Resource Groups Replication Plans Job Monitoring	۰	?	9
Add New Site Octavits (3) vCenter Details (3) vCenter Details			×
Site Type			

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**.

Add New Site	⊘ Site Type () Site Details (3) vCenter Details (4) !	Storage Details	
		Source AVS Private Cloud		
	Select Credentials	Azure Region 🔘	Azure Resource Group	
	DemoCred -	West Europe	ANFAVSVal2 +	
	Add New Credential 😆			
		AV/S Details		
		Avo Detalis		
	Web Client	URL	0	
		ANFDataClus	*	
	Username			
	cloudad	min@vsphere.local		
	Password		0	
		•••••		
		Accent self-signed certificates		
		- recept an agriculture		

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

15. Click Create Site.

Disaster Recovery Orchestrator 💊 📔	Dashboard Discover Resource Group	ps Replication Plans Job Monitoring		4
		Site Type	Site Location	
	2 Centers 2 Storages	1 Source Destination	On Prem	2 Cloud
2 Sites				Q D Add New Site
2 sites Site Name	○ Site Type = 〒 Location	⇒ vCenter ≎ Storage ≎ VM-List	Discovery Status	Q O Add New Site
2 Sites Site Name DemoDest	≎ Site type	 ⇒ vCenter ≎ Storage ≎ VM List. 1 	Discovery Status + https://10.75.0.2/	Q O Add New Site

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.

tApp Disa	ster Recovery Orchestrate	e 🐴 Dashboard Docover Res	ource Groups Replication Plans Job	Monitoring		A & (
Ba	ick					
			VM List Site: DemoSRC vCenter: https://172	30.156.2/		
	271			VM Postection		
		itaitores	128 Virtual Machines	2 Postected	0 126 Unprotented	
12	28 vm				٩	Create Resource Group
	VM Name	2 VM Status	1 MM State	DetaStore	51, 6 0	C Memory (Mt)
	HDőenth,2.5.1	O Not Protected	() Powered On	vianDatastore	8	8192
0	hci-fio-datastore-13984-0-1	0 Not Protected	D Powered Off	HCtstD5	22	65538
1	ICCA2005-WID-R1	O Not Protected	(b) Powerrd On	vianDataitore	3	14336
	ICCA2005-NE-R1	0 Not Protected	() Powered On	vsanDatastore	1	3072
	ICCA2005-01-81	0 Not Protected	() Powered On	vianDatastore	5	3072
	HCX_Demo_05	10 Not Protected	Dewered Dff	Demo002	1	2048
	hci-nim-datastore-13964-0-1	0 Not Protected	() Fowered Off	HCRVIDS	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 Grou*ps and click *Create New Resource Group.

NetApp	Disaster Recovery Orchestrator 💊 📔	Dashboard Discover Resource Groups Re	plication Plans Job Monitoring	٨	¢? 2
	-				
	Resource Group	C 1 Site	Center 1	P Virtual Machines	
	1 Resource Group			Q D Create New Resource Group	
	Resource Group Name				
	DemoRG	DemoSRC	https://172.30.156.2/	View VM List	

- 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

n NetApp	Disaster Recovery Orchestrator 💊	Dashboard Discove	er Resource Groups R	eplication Plans Job	Monitoring			٠	?	
	Edit Resource Group		Resource Group Details	Select VMs	Boot order and	Delay				
			Bo	oot order and De	alay					
		VM Name	Boot Order 🕘		Boot Delay (see	s)				
		QALin1	3	12	0	10				
		QALin	3	101	0	[0]				

6. Click Create Resource Group.

P	Disaster Recovery Orchestrator 💊 🛛 Dask	hboard Discover Resource Groups Re	eplication Plans Job Monitoring	4 O
	☑ 1	☐ 1	P 1	
	1 Resource Group	Site	vuenter	Q O Create New Resource Group
	Resource Group Name			≂ VM List
	DemoRG	DemoSRC	https://172.30.156.2/	View VM List

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.

tApp	Disaster Recovery O	Drchestrator 💊 📔 Dashi	board Discover Resource G	Sroups Replication Plans	Job Monitoring			4	•	•
	R 1		I	Source Details	1	Destination	Details	Ø 1		
	Rep	lication Plans	Resource Groups	Sites	vCenters	Sites		vCenters		
	1 Replication Plan						م ی	Create New Replication Plan		
	Plan Name	C Active Site	Status	Compliance	Source Site	🐨 📔 Destination Site	91			
	DemoRP	 Source 	 Active 	Partially Healthy	DemoSRC	DemoDest	Resource	e Groups		

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.

NetApp Disaster Recovery Orchestrator	Dashboard Discover Resource Groups Replica	tion Plans Job Monitoring	4 🌣 3 🕰
Create New Replication Plan	Replication Plan and Site Details (2) Select Res	ource Groups ③ Set Execution Order ④ Set VM Details	×
	Replica	ion Plan Details	
	Plan Name		0
	DemoRP		
	Reco	very Mapping	
	Source Site	Destination Site	0
	DemoSRC	- DemoDest	*
	Source vCenter	Destination vCenter	0
	https://172.30.156.2/	+ https://10.75.0.2/	•
	Clu	ster Mapping	
	Source Site Resource Dest	nation Site Resource	
	Cluster-1 *	Cluster-1 + Add	
	Source Resource De	tination Resource	•
	No M	tappings added!	
		Continue	

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

NetApp Disaster Recovery Orchestrator	Dashboard Discover Resource Gro	oups Replication Pla	ins Job Monitoring			٠	?	۹
Create New Replication Plan	(1) Replication Plan and Site Details	Select Resource G	iroups ③ Set Execution Order ④ Set VM Details					×
		Replication	Plan Details					
	Plan Name			0				
	DemoRP							
		Recovery	Mapping					
	Source Site	0	Destination Site	0				
	DemoSRC		DemoDest	*				
	Source vCenter	0	Destination vCenter	.0				
	https://172.30.156.2/	*	https://10.75.0.2/	*				
		Cluster	Mapping		N			
	No more S	ource/Destination clust	er resources available for mapping					
	Source Resource	Destination Re	source					
	Cluster-1	Cluster-1	Delete					
		Con	tinue					

- 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.

NetApp Disaster Recovery Orchestrator	Dashboard Discover Resource	Groups Replication Plans Job M	Monitoring			۵ ۵	?	۹
Create New Replication Plan	Replication Plan and Site Details	Select Resource Groups (3)	Set Execution Order	(4) Set VM Details				×
		Replication Plan Det	ails					
		Select Execution Orde	er					
	Resource Group Name		Execution Order					
	DemoRG		3					
		Network Manning			1			
	No more	Source/Destination network resources	available for mapping					
	Source Resource	Destination Resource						
	SepSeg	SegDR		Delete				
		DataStore Mapping						
	Source DataStore	Destination Volume						
	TestSrc01	gwc_ntap_acct/gwc_DRO_cp/testsrc	01copy					
		Previous Conti	nue					

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.

NetApp	Disaster Recovery Orchestrator 💊	Dashboard Discover Resource	Groups Replication F	Plans Job Monitoring	Ы. П			۵	٥	?	9
	Create New Replication Plan	Replication Plan and Site Details	Select Resource	Groups 🕜 Set Execu	tion Order	🔕 Set VM Details					×
			VM	Details							
		2 VMs					٩				
		VM Name	No. of CPUs	Memory (MB)	NIC/IP	Boot Order 🔮 🔳 Override					
		Resource Group : DemoRG									
		QALin1	1 🗐	1024 🔯	 Static Dynamic 	3	0				
		QALin	4 0	1024 [0]	 Static Dynamic 	3	\$				
			Previous	Create Replication Plan							

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.

NetApp Disast	ter Recovery Orchestrat	tor 💊 Dashboard	Discover Resource Group	os Replication Plans	Job Monitoring			19	•	ł ?	۹
	Replication Pla	ans	1 Resource Groups	Source Details	1 vCenters	Destination De	tails VCenters				
1 R	Replication Plan						Q O Create N	ew Replication Pla	n		
PL	lan Name 🗢 🗧	Active Site	Status	Compliance	Source Site 🔫 🗧	Destination Site	÷1				
De	(emoRP	⊘ Source	 Active 	A Partially Healthy	DemoSRC	DemoDest	Retource Groups	Plan Details Edit Plan Fallover Test Fallover Migrate Run Compliance			

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.

		Source Details		Destination Details	
Replication Plans	Resource Groups	Sites	vCenters	1 Sites	vCenters
	Testfailover Details			×	
1 Replication Plan	 Use latest snapshot () Select specific snapshot () 	5		^ Q	Create New Replication Plan
Plan Name C Active Site	Volume	e.	Snapshot	÷.	l,
DemoRP 🥥 Source	WEANFAVSacct/testcap/test	src01	Belect Snapshot		Resource Groups
			2023-04-28		
			2023-04-28T11:31:55.000Z - gwc_ntap		
			2023-04-28T11:21:54.000Z - gwc_ntap		

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.

ACK	Tast Failovas Stans		
	Replication Plan: DemoRP		
~	Cloning volumes for test (in parallel)	⊘ Success	0.7 Seconds 🛈
~	Mounting cloned volumes and creating datastores (in parallel)	⊙ Success	0.9 Seconds 🕚
~	Registering VMs (in parallel)	⊙ Success	0.1 Seconds 🕕
~	Powering on VMs in protection group - DemoRG - in target (in parallel)	Success	0.1 Seconds ()

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.

C 2 Stes	1 Resource Group	Replication Plan	Instanting	0 127 Unprotected
Environments Virtual Environments	2 Allef Storage Accounts	Topology Cerves		Immensive View (3
SDDC Summary	14 Falders	DemuSRC Hyps.//172.38.156.29	Devisiblest Regis ITE 75.6.29	
12 Dutastores	12 Networks			

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**.

NetApp	Disaster Recovery Orchestrator 💊 🕴 Dashboard 🏻	Discover Resource Groups	Replication Plans	Job Monitoring		4 Ø	? 9
	B 1 Replication Plans	1 Resource Groups	Source Details	2 1 vCenters	Destination Details	i vCenters	
	1 Replication Plan	Status	Compliance	Source Site	QO	Create New Replication Plan	
	Plan Name - Active Site						
	DemoRP The Destination	 Running In Failover Mode 	 Healthy 	DemoSRC De	moDest Reso		
	Plan Name C A Cive Site DemoRP O Destination	 Running In Failover Mods 	⊙ Healthy	DemoSRC De	moDest Reso	Purce Groups	
	Plan Name C A Crive Site DemoRP O Destination	 Running In Failover Mod- 	⊙ Healthy	DemoSRC De	moDest Reso	Plan Details	1

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

🗖 NetApp	Disaster Recovery Orchestrato	or 💊 Dashboard	Discover Resource Grou	aps Replication Plans	Job Monitoring			4	¢ 0 ©
	B 1 Replication Pla	ns	1 Resource Groups	Source Details	vCenters	Desti Site	nation Details	VCenters	
	1 Replication Plan	Artius Site	1 Status	Compliance	Course Site	👳 丨 Destination Site	QÐ	Create New Replication Plan	
	DemoRP	© Destination	Active	Healthy	DemoSRC	DemoDest	Reso	Pian Details	
								Falback	
NetApp	Disaster Recovery Orchestrat	or 💊 🛛 Dashburd	Distance Resource Gr	mups Replication Plan	ns 🕴 Job Monitoring 🔡			4	• • •
	2	1		a 1	a	128	Protected VMs	1 127	
	Invironments	, in the second se	Issurce Group	Replication Plan		VMs	Protected	Unprotected	
	2 Vitual Evolutionents	E 2 ANF Storage Access	4)		~		_		
	SDDC Summary	D 14			<u> </u>				
	Charters	Fooder	1	Nega //172.30	156.21	https://10.75	i û 2/		
	12 Datastores	12 Network	is .						
	Execution Jobs	01	Replicati	on Plans		chep Sete	Status		
	Tertus Judes	in Prograts	Demos	φ.	e) Source	() Atter		

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-setup.html

Deploy and configure Azure VMware Solution

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

Using Veeam Replication and Azure NetApp Files datastore for disaster recovery to Azure VMware Solution

Author: Niyaz Mohamed - NetApp Solutions Engineering

Overview

Azure NetApp Files (ANF) datastores decouples storage from compute and unlocks the flexibility needed for any organisation to take their workloads to the cloud. It provides customers with flexible, high-performance storage infrastructure that scales independently of compute resources. Azure NetApp Files datastore's simplifies and optimizes the deployment alongside Azure VMware Solution (AVS) as a disaster recovery site for on premises VMWare environments.

Azure NetApp Files (ANF) volume based NFS datastores can be used to replicate data from on-premises using any validated third-party solution that provides VM replication capability. By adding Azure NetApp Files datastores, it will enable cost optimised deployment vs building an Azure VMware Solution SDDC with enormous amount of ESXi hosts to accommodate the storage. This approach is called a "Pilot Light Cluster". A pilot light cluster is a minimal AVS host configuration (3 x AVS nodes) along with Azure NetApp Files Datastore capacity.

The objective is to maintain a low-cost infrastructure with all the core components to handle a failover. A pilot light cluster can scale out and provision more AVS hosts if a failover does occur. And once the failover is complete and normal operations are restored, the pilot light cluster can scale back down to low-cost mode of operations.

Purposes of this document

This article describes how to use Azure NetApp Files datastore with Veeam Backup and replication to set up disaster recovery for on-premises VMware VMs to (AVS) using the Veeam VM replication software functionality.

Veeam Backup & Replication is a backup and replication application for virtual environments. When virtual machines are replicated, Veeam Backup & Replication is replicated from on AVS, the software will create an exact copy of the VMs in the native VMware vSphere format on the target AVS SDDC cluster. Veeam Backup & Replication will keep the copy synchronized with the original VM. Replication provides the best recovery time objective (RTO) as there is a mounted copy of a VM at the DR site in a ready-to-start state.

This replication mechanism ensures that the workloads can quickly start in a AVS SDDC in the case of a disaster event. The Veeam Backup & Replication software also optimizes traffic transmission for replication over WAN and slow connections. In addition, it also filters out duplicate data blocks, zero data blocks, swap files, and "excluded VM guest OS files". The software will also compress the replica traffic. To prevent replication jobs from consuming the entire network bandwidth, WAN accelerators and network throttling rules can be utilized.

The replication process in Veeam Backup & Replication is job driven which means replication is performed by configuring replication jobs. In the case of a disaster event, failover can be triggered to recover the VMs by failing over to its replica copy. When failover is performed, a replicated VM takes over the role of the original VM. Failover can be performed to the latest state of a replica or to any of its good known restore points. This enables ransomware recovery or isolated testing as needed. Veeam Backup & Replication offers multiple options to handle different disaster recovery scenarios.

[dr veeam anf image1]

Solution Deployment

High level steps

1. Veeam Backup and Replication software is running in an on-premises environment with appropriate network connectivity.

 Deploy Azure VMware Solution (AVS) private cloud and attach Azure NetApp Files datastores to Azure VMware Solution hosts.

A pilot-light environment set up with a minimal configuration can be used for DR purposes. VMs will fail over to this cluster in the event of an incident, and additional nodes can be added).

- 3. Set up replication job to create VM replicas using Veeam Backup and Replication.
- 4. Create failover plan and perform failover.
- 5. Switch back to production VMs once the disaster event is complete and primary site is Up.

Pre-requisites for Veeam VM Replication to AVS and ANF datastores

- 1. Ensure the Veeam Backup & Replication backup VM is connected to the source as well as the target AVS SDDC clusters.
- 2. The backup server must be able to resolve short names and connect to source and target vCenters.
- 3. The target Azure NetApp Files datastore must have enough free space to store VMDKs of replicated VMs.

For additional information, refer to "Considerations and Limitations" covered here.

Deployment Details

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

To replicate VMs, follow the below steps:

- 1. Open the Veeam Backup & Replication Console.
- 2. On the Home view. Right click the jobs node and select Replication Job > Virtual machine.
- 3. Specify a job name and select the appropriate advanced control checkbox. Click Next.
 - Select the Replica seeding check box if connectivity between on-premises and Azure has restricted bandwidth.

*Select the Network remapping (for AVS SDDC sites with different networks) check box if segments on Azure VMware Solution SDDC do not match that of on-premises site networks.

• If the IP addressing scheme in on-premises production site differs from the scheme in the target AVS site, select the Replica re-IP (for DR sites with different IP addressing scheme) check box.

[dr veeam anf image2]

4. Select the VMs to be replicated to Azure NetApp Files datastore attached to a Azure VMware Solution SDDC in the Virtual Machines* step. The Virtual machines can be placed on vSAN to fill the available vSAN datastore capacity. In a pilot light cluster, the usable capacity of a 3-node cluster will be limited. The rest of the data can be easily placed on Azure NetApp Files datastores so that the VMs can recovered, and cluster can be expanded to meet the CPU/mem requirements. Click Add, then in the Add Object window select the necessary VMs or VM containers and click Add. Click Next.

[dr veeam anf image3]

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

[dr veeam anf image4]

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

[dr veeam anf image5]

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

[dr veeam anf image6]

10. Choose the replication schedule to run the replication job to run on a regular basis.

[dr veeam anf image7]

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

[dr veeam anf image8]

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

[dr veeam anf image9]

For additional information for Veeam replication, refer How Replication Works

Step 2: Create a failover plan

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

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



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



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



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

To create the Failover Plan, do the following:

1. On the Home view. Right click the Replicas node and select Failover Plans > Failover Plan > VMware vSphere.

[dr veeam anf image10]

2. Next provide a name and a description to the plan. Pre and Post-failover script can be added as required. For instance, run a script to shutdown VMs before starting the replicated VMs.

[dr veeam anf image11]

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

[dr veeam anf image12]

For additional information for creating replication jobs, refer Creating Replication Jobs.

Step 3: Run the failover plan

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



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

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

[dr veeam anf image13]

[dr veeam anf image14]

The state of the VM replica changes from Ready to Failover and VMs will start on the destination Azure VMware Solution (AVS) SDDC cluster / host.

[dr veeam anf image15]

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

[dr veeam anf image16]



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

For detailed information about failover plans, refer Failover Plans.

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

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



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

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

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

[dr veeam anf image17]

[dr veeam anf image18]

[dr veeam anf image19]

[dr veeam anf image20]

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

For detailed information about the failback process, refer Veeam documentation for Failover and Failback for replication.

[dr veeam anf image21]

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

[dr veeam anf image22]

Conclusion

Azure NetApp Files datastore capability enables Veeam or any validated third-party tool to provide a low-cost DR solution by leveraging Pilot light clusters instead of standing up a large cluster only to accommodate VM replicas. This provides an efficacious way to handle a tailored, customized disaster recovery plan and to reuse existing backup products in house for DR, enabling cloud-based disaster recovery by exiting on-premises DR datacenters. It is possible to failover by clicking a button in case of disaster or to failover automatically if a disaster occurs.

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

https://netapp.hosted.panopto.com/Panopto/Pages/Embed.aspx?id=2855e0d5-97e7-430f-944a-b061015e9278

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 onpremises 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 onpremises 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



Solution Deployment

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

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.



1. 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.



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.



1. After you access the HCX portal with 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.

vm VMware HCX							C	⊘~ =	cloudadmin
Dashboard Infrastructure Site Pairing Sinterconnect Services Compute Network Extension Migration Disaster Recovery	System Upd Pair your remote da REDUEST DOT LOCAL HCX CHECK FOR UPDATE	ates							
Administration Administration Administration Administration Troubleshooting	Current Version	System Name	7	Status	Info	System T Type	NSX Version T	VC Version T	Copy To Clipboard
Audit Logs	○ ℝ4330	hex. cloud	WS-azure.co.		٩	HCX Ooud	312.0017883600	7.0.3 10234570	ß
DICE Support								Numb	er of Applance
	* ERROTE HCX								
	Current Version	System Name	τ Status	info		System Type	7	Copy To Clipboard	
				8					
								0000	///////////////////////////////////////

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

😑 vSphere Client	Q	C & Annual Concerns	⊪× © ⊘s
	R A300-Cluste	r01 Excisions	-
	Deploy OVF Template	Select an OVF template × Select an OVF template from remote URL or local file system	
- B ADDOMACH	1 Select an OVF template	Enter a URL to download and install the OVF package from the Internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.	The
0 4000-es	3 Select a compute resource	Nets Childra 2 Version bis Marker and Article Congress, part 1 Januar	
© 4305-41 → © 47#_HC	4 . Review details	Local file UPLOAD FILES VMware-HCX-Connector-4: ova	
1 G ANFORM	 Select starage Ready to complete 		
(2 HOL (2 HOL			
la Hox. B Hox.			
(B HOL (B HOL		RANCEL NEXT	
(3) HOX. (3) HOX3	Protoc_23	NEEDE Powersd V Numer 42168 30 42 68 20 Mile / 10 68	
A Recent Tarks	Histor_34 CIL EXPORT		N 4.11.04.2 H

1. 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.

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.

Microsoft Azure	🖓 Search resources; services; and docs (G+/) 📰 😵 🖉 🛞 🕐 🦗	niyaz@netapp.com
Microsoft Azure Home > Azure VMware Solution > A Azure VMware Solution > A Hybrid Cloud TME Create ③ Manage view $\lor \cdots$ Fitter for any field Name 1. AN AN AN AN	✓ Search recourse: service: and docs (G+/) ✓ AVSANFValClus Add-ons ★ ★ ← ✓ AVSANFValClus Add-ons ★ ★ ← ✓ Avs hnate cload ✓ Feedback ✓ ✓ Overview © Search (Cmd x/) ✓ ✓ ▲ Activity log ✓ ✓ ✓ ▲ Activity log ✓ ✓ ✓ ✓ Tags ✓ ✓ ✓ ✓ Diagnose and solve problems HCX plan ○ HCX Advanced Incofigure HCX appliance 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. Learn more. HCX plan Intops://III ✓ ✓ Connectivity Cloude and yelpoy the VMware HCX contextor appliance on-premises and start the appliance, you're ready to activate using below likense keys. Learn mole. ✓ Add-ons ✓ Activation key Status Workload Networking Nosel Exercise Status	niyaz@netapp.com ★
	Workload Networking HCX key name Activation key Status <	



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 onpremises. 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.

vm HCX Manager	Dashboard	Appliance Summary	Configuration	Administration				7221254357	Version 4.410 Type : Connector	admin
VMware-HCX FOON: IP Address: Version: Uptime: Current Time:	-440 VMware-HCX-440 172.2 4.4.1.0 20 days, 21 hours, Tuesday, 13 Septe).ehcdc.com 9 minutes mber 2022 07:44:11 PM UT0	:			() () ()	CPU Used 1407 MHZ Memory Used 9691 MB Storage Used 296		Free 688 MHZ Capacity 2095 MHZ Free 2316 MB Capacity 12008 MB Free 980 Capacity 1270	67% 81% 23%
NSX			vCenter https://a300-vc	sa01.ehcdc.com	•	S	SO ttps://a300-vcsa01.eh	dc.com		
MANAGE			MANAGE			м	IANAGE			

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 onpremises VMware HCX Connector for Azure VMware Solution private cloud by adding the pairing. To configure the site pairing, complete the following steps:

 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.

😑 vSphere (Client Q								C 8	Administrator@EHC	ос.coм ~	9
Shortcuts												
Inventories	ß		Ø	Ē		ංදිං	n	Ŵ		(٢	
Hosts and Clusters	VMs and Templates	Storage	Networking	Content Libraries	Giobal Inventory Lists	Workload Management	SnapCenter Plug-in for VMware VSphere	Cloud Provider Migration		Site Recovery	нсх]
Monitoring												
會		Ċ,	52	Ep.	\otimes							
Task Console	Event Console	VM Costomization Specifications	VM Storage Policies	Host Profiles	Lifecycle Manager	ONTAP tools						
Administratio	n											
Q												
Licensing												

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.

😑 vSphere Client (Q)							
VSphere Client	< Site	e Pairing	Connect to R Remote HCK URL Username Password	Permote Site https://72. cloudadmin@vsphere.local	Х @ NCEL <u>CONNECT</u>	Va azuro.com-	TRANSPORT

1. Click Connect.

i i

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.

	<	Site Pairi	ng				
X Dashboard						CI ADD A SITE	DAIDING
rastructure	~	-				C ADD A SITE	PAIRING
Site Pairing		Ø	VMware-HCX-440	\rightarrow	6		
biterconnect		~	Phitps://172.21.254.157.443		hcx.8ebf3b0b7ddf4cc08e3f85.westeurope.avs.azure.c	.om-	
Transport Analytics			👳 Raleigh		cloud		
rvices	×				@ https://172.30.156.9		
Network Extension			1 International (1)		Analysia man		
Disaster Recovery			a multi-comment(s)				
stem	~	EDIT CO	NNECTION DISCONNECT				
Administration		1			22011911001		
Support		Ø	VMware-HCX-440	\rightarrow	(a) HCX		
			Paleunh		Phttps PLIS W		
			A Interconnect/a)		0.054		
			1 interconnect(s)				
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.

← → Ø		ittps://a300-vcsa01.ehcdc.com/ui/app/blug	in/com.vmware.hybridity/com.vmware.ho	uhybridConnect	合		0 8
\equiv vSphere Client Q				C		9	0
HCX Dashboard Infrastructure Ste Paining Infrastructure Infrastructure Infrasport Analytics Services Network Extension Infrastruct	< Inte	erconnect II-Site Dervice Mesin Impute Hollies Service Mesin Network Pr O hoxdemo	roffies Sentinel Management		Q C CREATE COM	PUTE PR	OFILE
Megration Disaster Recovery System Administration Support	~	Hold a000-ecu/01 encod: com/of hold: 2020) Hold a000-ecu/01 encod: com/of hold: 2020) Find a000-ecu/01 encod: com/of hold: 2020 Modo-voca/01.ehc/dc.com Modo-voca/01.ehc/dc.com	In in critical (red) state for service compute Is in critical (red) state for deployment container Ceptoyment Container Ceptoyment Container Castoner C	compute Nativoiss ©VM_3510 (Management) (vgpn Nativois Container (Nativois Extension) © VDS-Switch0 (Untimited)	erre Beolication) (Upline) (whotion) @	EDIT	

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.

	<	Interconnect								
icx Dashboard nfrastructure Ø Site Pakring	×	Muth-Site Service Mesh Compute Profiles Service Mesh	Notwork Profiles Sent	sel Management						
Transport Analytics							Q C O	REATE NETW	ORK PR	OFIL
Services Network Extension Migration Disaster Recovery System So Administration	* *	VM_3510 Network Details backing: VM_3510 show more	ыти 9000	IP Pools IP Ranges 172.21.254.80 - 172.21.254.95	IP Usage(Used/Total) 4/ 16	Prefix Length	Gateway 172.21.254.230			
Support		EDIT DELETE								

- 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.

$\leftarrow \ \rightarrow \ G$	0 8	Ov. https://a300-vcia01.ehodc.com/ui/app/plugin/com/vmware.hybridity/com/vmware.hcc.hybridConnect		Ŷ		⊚ ≡
\equiv vSphere Client	Q		C		3	0~
HCX Dashboard Infrastructure Site Pairing Interconnect E: Transport Analytics Services	~	Interconnect Muts-Site Senice Mesh Compute Profiles Senice Mesh Network Profiles Sentinel Management ICC007			E MESH	L î
 Network Extension Migration Disaster Recovery System Administration Support	×	New version for service mesh explances is aveilable. Click on Update Appliances to Upgrade to latest. See Paing VMware- HCX-440 @ Raingh bcxdemo TNTI35-HCX-COMPUTE-PROFILE		Servees	×	

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.

		_	_					_				035
vignere Gent - Q										C 24m	numerical energies and a	
		interconn	nect									
and the second se												
utre												
he Parriej		Carrysie Port	e Berneline inset folle. Demolikaspeet									
teruinnest.		+ 1	(v) 10000								CON SERVIC	
#1807 AVA/711	e10	Attemp	BARRIANCES CTAINS									
ebearle godanision												
tipation.			Andered Same	2 4447	and first	*****		funnet Ballio	Darrente Versione	Annan man		
n Antonination Antonination	×	0.1	CODET and an 2019/09/10:20-0021-0021 STUDNeSS1056 Internative XXXX-2012.00200 Manager XXXX.2012.00200	80		112-204.80 (mm) -		۲	443.0			
		0.2	COUT 46.0 as UPAN NAMEAN AND ART NETWORKSCHOOL Demann KOOLOUWER Demann Konstan (25.5 millio) Herman Research DR	-63	-contract	722/348 <mark>(</mark>	(III) (I	۲	6420	****		
			000011-W0+0 w 44810749/Mile-exists-edition-distance/float Entering A200_2010_0000 Minespe 2002_2010_0004	0	-CE MAN OF				1234	NA		
												1.000
		Applano	es on hox.liebf.lb0b7ddf4cc0lie3185 westeurope.am	Likžurinic	om-cloud							
			Marka .		-		d' Address				Date	
		00007-0			80	Cidadia	12.22.28.20 (************************************				-	10
		100007 H	14		-	Civer D.T.	12.30 mil				444	1.Q
		10000114	0#		0	ci sia cet					. 734	10.

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.

$\leftrightarrow \rightarrow 0$	08 =	https://a300-vcsa01.ehodc.com/ui/app	/plogin/eam:	vmware.hybridit	y/com.vinv	vare, he	xmigrationold		ŵ	-	⊚ ± =
\equiv vSphere Client C	2							CA	Administrator@EHCD0		9 0
HCX Deshboard Infrastructure	×	Migration	ent	D MIGRATE	C (e				BEARD Doct	
oo interconnect		Name	VM	s/ Storage/ Mam	ory/ CPUs		Progress	Start	End	Status	
C Transport Analytics											
A Network Extension											
Migration		🛩 🍙 a300-vcsa01.ehcdc.co	om → (172.30.156	2						
*D Disaster Recovery		> 2022-09-26 09:00 FLJVU		1 208	2.08	1	Migration Complete	2			
& Administration		> 2022-09-26 08:35 8XMTM		1 2.68	2.69	1	Higration Complete	0	7		
@ Support		> 2022-09-18 16:21 ERCZO		2 4 68	4.08	ž	@ Draft	¥	÷.		
		> MG-18cbce94/Sep 16	enter#	5 10 GB	10 GB	6	Migration Complete	12.44 Au Sec 10	3		
		> MG-04abdeell / Sep 16		1 2.68	2.69	1	Migration Complete	12.25 Abi Bag 16	5		
		> MG-ef7374dd / Sep 10	1079	1 2.GB	2.68	1	Migration Complete	12:11 Att	8		
		> MG-d2of93et / Sep 14	1-27	5 10.08	10 08	5	O Mgration Complete	02.05 ma	4		
		> MG-99Recad81 Sep 14		1 2.09	2.08	t.	Migration Complete	11:02 AM	×		
		> MG-548618cb / Sep 14	we (58))	1 2.08	2.08	1	Stigration Complete	10.04 AM	2		
		> MG-dd475274 / Sep 12	aur Colly)	2 4.69	4 GB	2	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**.

			Select VMs for Migration
 Transfer and Placement: 	This is migrating to ANF datastore		
Ouster-1	Cataster002 ((115(210))	Bok Mgradion	÷
C) (Soecity Destination Fotoer)	Same format as source	 Kostona: Switchover Sche 	ouer O
> Switchover:			
 Extended Options: 			
v Extended Options:			
Extended Options: (Seture MAC)			
Extended Options:			<u>a</u> .
V Extended Options:	Disk / Memory / vCPU.	Migration Into	0
Extended Options: (Brigs MAC) (Brigs MAC)	Oph / Memory / vCPU. O 2/08 : 2/08 : 1/0PU	Migration Into Bulk Migration	0
Extended Options: Onlyne MAC	Opti/ Memory / vOPU O 208 208 1vOPU O 208 208 1vOPU	Migration Info Bull Migration Bulk Migration	Q.:
Extended Options: (Brain MAC) Affor Migration Oemo, HOX, Buik01 Oemo, HOX, Buik01 Oemo, HOX, Buik01 Oemo, HOX, Buik01	Otal / Hemory / vCPU O 2 GB 2 GB 1 vCPU	Migration toto Bull Migration Bull Migration Bull Migration	
Extended Options: (Brain MAE) M1 for Migrassee Soeno_HCX_Blak01 Demo_HCX_Blak02 Soeno_HCX_Blak03 Soeno_HCX_Blak03	Otak / Memory / vCPU D 2.08 2.08 1vCPU O 2.08 2.08 1vCPU	Migration Info Buil Migration Built Migration Built Migration Built Migration	3

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

 (\mathbf{i})

+ + C	0 & # musical	Simplify whether any la	Section and the section of		marchio	and a second									\$		0	土 昭
😑 vSphere Cle	mt Q													C	& American American Color	₩~	۹	•
HCX Deshboard Infrastructure C Site Darry	•	Migration	E Maragement M	() HERATE	Stereor (H	E) (#2	acia	Progress		_	2	Start	. Int		Status .	ł	Ļ	
E: transport Analytic Services P Technology Dolemon Morphon	а.																	
Disaster Recovery System & Administration	÷		se01 ehodis co Jakas photo ane Jakos	m → • 172.30. ⊂	1562 20 30	0 200	н 1	Highling.				2.91 PU AUT 544 14 2.91 PU AUT			Deltcherer starter			
. C. ardonat		Deno, HCR	gendol don (fubit) gendol don	-	30	0 2.58	٠	37% Same Surve		******		2-25 Add RDT Stag 14			Transfer (Rated			
		Demo_HO topology topology	Judoz (si-col con Judot (si-col con	-	10	0 200 0 200	e E	Warshop,		******		200 PM 827 Bag 14 200 PM 827 Bag 14			Deltchover stated			
		D > Detta_HCX	SMotive 64-424.20H	-	19	0 2.08	1	O Wgraten Cor	nglike		_	11.02 Aut 82.1 The 14	11.10 AM 857 Bap 14	3 10	Migration comprehent			
v Recent Tasks	Alarma																	
Tau Nate	Y Target	Y Matus	-e ¥	Generalia	*	saladur		۰.	Dokuré : Eur	Y Stat	e tana	. 4	Completion Time		Y Server			- 1
Bulk Migration	(D. Dens, HDC, BLADS	1000	245.0	Trahater Started		Azmestrato	00	KODC COM	0.01	09/	rw/2000	1.12.05 TI PSH			hybrisity-manager			
Buik Migration	(D Dens, HOK, BARDI		0.40	Transfer Started		Amesicals	00	KDC:00M	0.ms	09/	14/2023	2.20311.994			hybrioty-manager			
Bak Mgration	D Dens, HCX, SUHD2		0.40	Transfer Starten		American	00	CDC:COM	0.00	-00/	14/2033	7,20511944			myGridd(y-manager			
Bulk Migration	(2 DINE, HOL, BARS		5% Q	Transfer Martell		Administrato	\$6	KOC COM	0.995	-09/	14/2022	2,2:0511266			trybratty-manager			
Bulk Migration	D Dema HDK Builde	1000	225 0	Thatater Starled		Ameutrato	00	KODC COM	0.00	-06/	14/2022	2.205TEPH			hybrioty-manager			

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.

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

e + 0 (Q A ≠ monit electrical	enni olesenillentimidates B	4347345663-1000-434	0401-4054/05240	Changing and			\$	0 ±
😑 vSphere Clent 🛛 Q							C & 100		© 0
, 9 <u>0</u> 80	DatastoreO2 Across	Permission files mosts VM	-						
· B SCOC-Datacenter	Victure Machines. VM Templates								52
B SODC-Detacenter Decentration	Victual Restances VM Templates VMs on ANF datastore after migra	Son		- third lines	(and PRA)	1 Mark Marcold		* Dem	URUE I
B SODC-Datacenter Datastorecz G excel	Victors Matchines VM Templates VMs on ANF datastore after migra UMs on ANF datastore after migra	Son Net 1 Sole	Produced laws	Ved Spece	Prest OPU	First Mars		.* Own	uraul
B SOCCONSERVER Construction Construction Construction Construction	Victual National VM Templates VMs on ANF datastore after migra VMs on ANF datastore after migra to there I = 0 Cemu, ICC, Subdit I = 0 Cemu, ICC, Subdit I = 0 Cemu, ICC, Subdit	Son Sole 1 Bole Posend On V Apro	Produced laws	Ved Ipeer 748.87 MB 75124 MB	0 HQ	Head Marin 2014 Mill 2010 Mill		, ¥ _ Own	CHOCH
B: SOCCOstorenter Consultations Consultations mentations mentations vaseOstatione	Victure Matchines VMs on ANF datastone after migral I mene I = @ Owner, HCR, Baddi I = @ Owner, HCR, B	Don Poparel On ✓ Ages Poparel On ✓ Ages Poparel On ✓ Vor	Produced Spece # 2 08 # 3 08 # 3 08	246,87 MB 246,87 MB 75124 MB 755,46 MB	0 Hg 0 Hg 0 Hg	Huad Mass 264 MB 200 MB 264 MB		r Den	wood
B SODC-Datacenter BradinatoreD GradinatoreD me-ds-12851:35-(M. ViseOstantore	Victual Industrial VM Templates VMs on AVF datastore sher migra I new I d Complete back I d Complete back I d Complete back I d Complete back I d Complete back	Don Note f Boles Possenal On V Note Possenal On V Note Possenal On V Note	Produced Spein a 2 08 a 3 08 a 3 08 a 3 08 a 3 08	Viel Stee 248,87 MB 75124 MB 75124 MB 755.46 MB 76122 MB	0 H4 0 H4 0 H4 0 H4 0 H4	Host Mass 264 HB 200 HB 205 HB 255 HB		v Den	wood

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.

+ + C	0 & # =	hini alton-	sid) and com/side	a de la compañía de l	وم المارك الرقاية		hipstenh.	0							\$	e	*
😑 vSphere Client	٩													C		0	
HCK Destcored Inflastructures		с м 	figration	lå agement	(1. milester)	<u>_</u>	D (20	aces	a]]				(A	_		8	
C the Parry A interconnect Is: Transport Analytics			Hereich A.		-	through/ h	Amary/ ONA		Program			- Start	, bil		Taka		_
Dervices Distance Echergion Microbiol		~				- 251											
Vitem			a300-vesa	01.ehcdc.co	1 -> 1 12 30 19	12					(A. 110-11)						
de Admensionten			· Atoma and the				49 2.00	<u> </u>	CONTRACTOR NAME		C) + III AR	Bug ta			AND THE PROPERTY OF THE PROPER		
Chargert			Done BCC Co	Contraction (Contraction)		24	28 2.06	4	Switzmen	-piate		12/24 AM 827 Deg 14	ROTE AND DR. Dec 14	18.00	Migration (completed		
			C > MCX. Photon, 4	P	•	20	2.08	1	O Myratum Cor	stele		7225 Pec 807 Ins 52	0231+48807 349 13	12.000	Migration compreted		
			D > 103, Person, 1	4 Conc. Intere	•	- 71	8 218	۰.	OWNER	- annual		12:25 PACED? Basi 13	1235-H4807 Bea 12		Northe property		
			D > NOLPHONE	5	-	23	200	31	C Maritein Cor	-ciele		1217 House	12,24 (% #27) 940 10	trie	Nigodur completed		
			D > HO, belle, 3	00.004	9	24	2.00	×.	@ Migration Opr	-sinte		12.01 mic.42.0 (mar.10	12:07 Hanstoff Sec 19	7.600	Migration completed		
· Recent Tasks A	larms																
Tash Rame T	farget		t said	+ 30	D-Cell	*	adutor .		*	Gurund	e itari t	*	Comparison Type	5.5	* beine		
Receipter virtal nach.	(D Dens, HOK, VI	Autors.	Comparied		Recordports Vytual	Marin.	EHCOC COM	have	ristialur	5.85	09/14	/3022.1015717	09/4/2022 101	10.55 AM	A000-vector/Lefture pum		
Arower entral inactions ()	(B Darro, HCK, VA	Attion	Comparison				EHEDCION	1.55%	rist also	4.004	09/14	/3003,1039/58	294/54/2023.303	10:58 AM	e300-or saidt etuite, dam		
Bellesh vyhai machine s.	Dete, KCk, VA	Aningen	Completed.				EHCOC COM	1.8.4	restrator	6.046	09/54	2002.00333.	06/4/2022 110	2.23 AM	a000-uppel0terter.com		
geman not this by its.	G 07221254 00		Congreted				EHEOCCOM	15	hiddator.	3.94	09/74	2022,1104.33	06/4/2022,110	433.MI	6300-scsatt atust; cum		

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 onpremises, 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

Unresolved directive in ehc/azure-regions.adoc - include::../../_include/azure-regionsupport.adoc[]

Copyright information

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

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

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

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

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

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

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

Trademark information

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