

NetApp for Azure / AVS

NetApp Solutions

NetApp July 31, 2024

This PDF was generated from https://docs.netapp.com/us-en/netapp-solutions/ehc/azure-native-dr-jetstream.html on July 31, 2024. Always check docs.netapp.com for the latest.

Table of Contents

NetApp Capabilities for Azure AVS	
Configuring AVS in Azure	
NetApp Storage Options for AVS	
Solution Use Cases	
Protecting Workloads on Azure / AVS	
Migrating Workloads on Azure / AVS	
Region Availability – Supplemental NFS datastore for ANF.	

NetApp Capabilities for Azure AVS

Learn more about the capabilities that NetApp brings to the Azure VMware Solution (AVS) - from NetApp as a guest connected storage device or a supplemental NFS datastore to migrating workflows, extending/bursting to the cloud, backup/restore and disaster recovery.

Jump to the section for the desired content by selecting from the following options:

- Configuring AVS in Azure
- NetApp Storage Options for AVS
- NetApp / VMware Cloud Solutions

Configuring AVS in Azure

As with on-premises, planning a cloud based virtualization environment is critical for a successful productionready environment for creating VMs and migration.

This section describes how to set up and manage Azure VMware Solution and use it in combination with the available options for connecting NetApp storage.



In-guest storage is the only supported method of connecting Cloud Volumes ONTAP to Azure VMware Solution.

The setup process can be broken down into the following steps:

- · Register the resource provider and create a private cloud
- Connect to a new or existing ExpressRoute virtual network gateway
- · Validate the network connectivity and access the private cloud

View the detailed configuration steps for AVS.

NetApp Storage Options for AVS

NetApp storage can be utilized in several ways - either as guess connected or as a supplemental NFS datastore - within Azure AVS.

Please visit Supported NetApp Storage Options for more information.

Azure supports NetApp storage in the following configurations:

- Azure NetApp Files (ANF) as guest connected storage
- Cloud Volumes ONTAP (CVO) as guest connected storage
- Azure NetApp Files (ANF) as a supplemental NFS datastore

View the detailed guest connect storage options for AVS. View the detailed supplemental NFS datastore options for AVS.

Solution Use Cases

With NetApp and VMware cloud solutions, many use cases are simple to deploy in Azure AVS. se cases are defined for each of the VMware defined cloud areas:

- Protect (includes both Disaster Recovery and Backup / Restore)
- Extend
- Migrate

Browse the NetApp solutions for Azure AVS

Protecting Workloads on Azure / AVS

Disaster Recovery with ANF and JetStream

Disaster recovery to cloud is a resilient and cost-effective way of protecting the workloads against site outages and data corruption events (for example, ransomware). Using the VMware 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.
- 3. During a disaster event, trigger failover to Azure NetApp Files datastores in the designated AVS DR site.
- 4. Invoke failback to the protected site after the protected site has been recovered.Before starting, make sure that the prerequisites are met as indicated in this link and also run the Bandwidth Testing Tool (BWT) provided by JetStream Software to evaluate the potential performance of Azure Blob storage and its replication bandwidth when used with JetStream DR software. After the pre-requisites, including connectivity, are in place, set up and subscribe to JetStream DR for AVS from the Azure Marketplace. After the software bundle is downloaded, proceed with the installation process described above.

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

CPT performs the following functions:

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



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

Install JetStream DR in On-Premises Datacenter

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

- 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 a	environments	C ⑦ ~ Administrator@EHCDC.COM ~
a300-vcsa.ehcdc.com	A300-DataCent	er ACTIONS ~ ACTIONS ~ Permissions Hosts & Clusters VMs Datastores	Networks Updates
 A300-DataCenter A300-Cluster a300-esxi02.eh 	 More Alarm Definitions Scheduled Tasks 	JebSbream DR Protected Domains Statistics Storage Sites Appliances	E Configurations Task Log
a300-esxi03.eh	Network Protocol Pr	Site Details	Alarm Setting
a300-esxi05.eh	JetStream DR	vCenter Server Hostname 172 21 253.	160
ANFJSDR-MSA0		Management Appliance Hostname ANFJSDR-m	158
AuctionAppA0		Software Version 4.0.0.443	
AuctionAppA2		Subscription ID 0000000-0	000-0000-0000-00000000001 Configure
🖧 AuctionAppA3		Tenant ID / Application ID - Configure	2
🖧 AuctionAppB0		Application Secret - Configure	

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

Site Details				Alarm Setter
vCenter Server Hostname	172.21.253.160			
Management Appliance Hostname	AUC MOD			
Software Version	Configure Clusters			
Subscription ID			All Q	
Tenant ID / Application ID		Select All Clear	r All	
Application Secret	Cluster Name 🔺	Datacenter Name 🔺	1.1	
Configured Clusters	A300-Cluster	A300-DataCenter	^	
O Configure Cluster				
Cluster Name			~	Host Details 🔺
No cluster contigured		Cancel	Configure	
		100		

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

Storage Sites	Add Storage Site
+ Add Storage Site	^
Name A	Storage Site Type * Azure Blob Storage
No Storage Site configured.	Access Type *
	Key Access
	Storage Site Name (Provide a name to identify this Site) *
	ANFDemoblobrepo
Storage Site Details Alarms	
	Azure Blob Storage Account Name * 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.

JetStream DR Protected Domains Statistics	Deploy New DR Virtual A	oppliance (DRVA)					
DRVAs (DR Virtual Appliances)	1. General	2. DRVA VM	3. DRVA Networl	k 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 (Optiona	1)	-				
	VM Folder (Optional)		-				~
Replication Log Volume	Datastore		A300_NFS_DS04				
	Number Of CPUs		8				
+ New Replication Log Volume	Memory Size		32GB				Q
Disk Path Name 🔺	Management Network		VM_187			Details 🔺	
No DRVA selected. Select a DRVA to vi	Host(iofilter) to DRVA Da	ita Network	VM_187				
	Replication Network to 0	Object Store	VM_187				
	Replication Log Network	< Comparison of the second sec	VM_187		\sim		\sim
			Cancel	Back 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.

elect Protected Domai	in: 🗸 Ci	reate Protected Domain				+ Create	
				•			
		1. General	2. Primary Site	3. Summary			
					^		
		Protected Domain Name	ANFPD001				
		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		~		
			Cancel	Back Crea			

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.

elect Protected Domain: ANFPD001	Start	Protection						reate	Delete	
ecoverable / Total VMs		tion Mode for selected VMs	-				a			Edit Detai
eplication Status		e-Back(VMDK)	-	# of Disks	Protection Mode		ų	ANFDem	M.	1
emaining Background Data		1	×					and the second sec	21.253.160) nter \ A300-Cluster	
irrent RPO		AuctionAppA1		1	Write-Back(VMDK)	v !	^	bled	nter (A500-Gluster	
		AuctionAppB1		1	Write-Back(VMDK)	~				
Protected VMs Settings Ala		AuctionDB1		2	Write-Back(VMDK)	~				
		AuctionLB1		1	Write-Back(VMDK)	~				
Start Protection		AuctionMSQ1		1	Write-Back(VMDK)	~				q
VM Name		AuctionNoSQL1		2	Write-Back(VMDK)	~		design and the	Data Dataila	
		AuctionWebA1		1	Write-Back(VMDK)	~		kground	Dat Details	
No VM is protected.		AuctionWebB1		1	Write-Back(VMDK)	~				
		Client1		1	Write-Back(VMDK)	~ ,				
				0	····· - · · · · · · · ·		•			
					Cancel Star	rt Prote	ction			

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



i

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	D. Seath revi	uncers, services, and door.15+i)	📰 🖓 🕒 🖓 🖓 🖓 🖓 🖓 👘 miyazilinetapp.com
Home > ANFOataOut			Run command - Install-JetDRWithDHCP
ANFDataClus Ru	in command —		This top level Cristlet Desweipuds JetCh bunctle from MMS, creates a new user, assigns
JP Seieth (ChT+/)	< 🔘 Refresh 📯 Feedback		elevated privileges to the user, deploys JetDr Management Server Appliance/MSA), registers vCenter to the JetDr MSA, configures cluster.
Access control (AMA)	Packages Run execution status		Command parameters
 Tops Diagnose and solve problems 	 Name 	Description	RegisterWorkp 🕤
Settings	v ISDRConfiguration 224 Proven	et Mussie for configuration of addresses Software on Add Ser and organ Saftware, ing for suscept	ProtectedCuster*
A Looks	Disible-letDRiceCuster	This Crediet unconfigures a cluster but doesn't unestall JetDR completely so other clusters	Outer-1
-		polices.	Datastore * 💮
Nanage	Drable-JetON orCluster	This Cristlet configures an edictional cluster for protection. It installs vibs to all hosts in the	vserCatestore
Chinectivity	Install-SetDRWINDERCP	This top level Cindlet Downloads JetDr bundle from MMS, creates a new user, assigns elevi	VMName 1 🕤
Chaters		registers vCenter to the JetDr MSA, configures chater.	ahtjoval-trisa
dentity	Install-SetDRWAttGascaP	This top level Cristlet Downloads JerDr bundle from MMS, creates a new user, assigns elev-	Ouster * ③
		registers vCenter to the JetDr MSA, configures cluster.	Deter-1
Stocage (preview)	Involve PreflightJetDRimital	This Crediet checks and doplays current state of the system it checks whether the minimal 4 hosts, if the cluster details are correct, if there is already a VM with the same name provid	- Credential ()
Placement policies	a standard to all standards and		Ctername*
+ Add-ons	Invoke-Prefight/etDRUkimball	This Emdlet checks and displays current state of the system it checks whether the minimal 4 hosts, if the cluster details are correct and if any VCenter is registered to the MGA	root
Workload Networking	Lowersk werst	The top level Ondiet creates a new user, assignt elevated privileges to the user, unconfigu	Passwoled 1
Segments	> Microsoft/WS/Management 4-List	winder on debit für administration einer baka im managing Adaes VMMeet Dourforts	HostName 🕥
TI DHCF			anĝoval-mua
Port manoring			Network* (j)
DNS C			DRSep
51775)			10/02
Operation			Detain
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.

Protected Domains	Statistics	Storage Site	es Ap	pliances (Configurations	Task Log		
Site Details							Alarm Setti	ing
vCenter Server Hostna	ame	172.30.1	56.2					
Management Appliance	e Hostname	anfjsval-r	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	🛠 Resolv	ve Configure Issu	le			C
Cluster Name		Datacenter	Name 🔺	Status 🔺	Software Vers	sion 🔺	Host Details	
Cluster-1		SDDC-Data	center	🕝 Ok	4.0.2.132		Details	1

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.

	^		Import	VMs	Recoverable V	Description	Protected Domain
		^	Import	20	20	Protected Domain Tile0	ANFPD000
c			Import	20	20	÷	ANFPD001
			Import	20	20	Protected Domain 02	ANFPD002
		~	Import	20	20	Protected Domain Tile 03	ANFPD003
		>					<

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.

otected Domains Stat	istics Storage Sites Appliances Con Continuous Failover Protected Domain	figurations Task Log		
ect Protected Domain.			Delete =	More
de	• • •	• • •		Deta
coverable / Total VMs	1. General 2a. Failover Settings 2b. VM Sett	ings 3. Recovery VA 4. DR Settings 5. Summary	reporec	
			253.160)	
	Protected Domain Name	ANFPD002		
	Datacenter	SDDC-Datacenter		
	Cluster	Cluster-1		
	Resource Pool (Optional)	-		
rotected VMs Setti	VM Folder (Optional)			
	Datastore	ANFRecoDSU002		
	Internal Network	DRSeg		C
VM Name 🔺	External Replication Network	DRSeg	Details	
AuctionAppA2	Management Network	DRSeg	Details	1
AuctionAppB2			Details	
AuctionDB2	Storage Site	ANFDemoblobreporec	Details	
AuctionLB2	DR Virtual Appliance	ANFRecDRVA003	✓ Details	
AuctionMSQ2	Banlingtion I on Storage	/dou/adb	Details	
AuctionNoSQL2		Cancel Back Continuous Failo	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	Configuratio	ons	Task Log	_
Select Protected Domain: ANFPD	000 - View all		+ Create	Ŵ	Delete	■More
Mode	Imported	Configura	ations		O Restore	
Recoverable / Total VMs	20 / 20	Storage Si	te	1	→ Failover	
		Owner Site	3	RE	→ Continuo	us Failover
					→ Test Faild	over
Protected VMs Settings	Alarms					
						c
VM Name 🔺	Protect	tion Status 🔺	F	rotectio	n Mode 🔺	Details
AuctionAppA0	Reco	verable	v	Vrite-Bac	k(VMDK)	Details '
AuctionAppB0	O Pace	verable	Ŵ	Vrito Bar	k(VMDK)	Details

Performing Failover / Failback

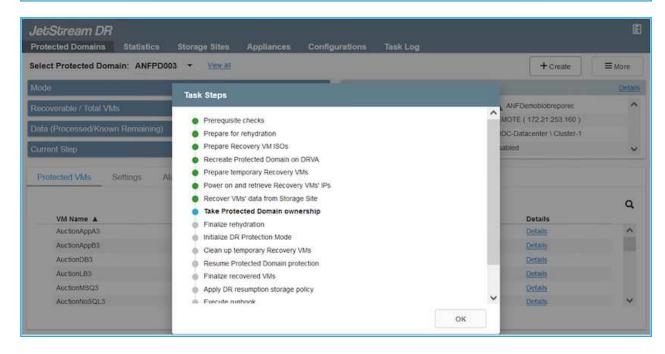
1. After a disaster occurs in the protected cluster of the on-premises environment (partial or full failure), trigger the failover.



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

After failover (for continuous or standard rehydration) when the protected VMs have been started in AVS, protection is automatically resumed and JetStream DR continues to replicate their data into the appropriate/original containers in Azure Blob Storage.

JebSbream DR Protected Domains Statis	Complete Continuous Fallover	for Protected Domain ANFPD003		8
Select Protected Domain: Al	VM Network Mapping			Ø Fallover ≣ More
	Protected VM Network	Recovery VM Network	^	
110001	VM_3510	DRSeg	· ^	(Settern)
Receiverable / Total VMs				100500000000 A
Data (Processed/Khown Roma	Force Failover			penter \ Cluster-1
Current Step			-	
Protoclad VMs Settings	required! Complete own	er of Protected Domain requested. Administrator consent is nership of this Protected Domain will be taken over by this Site you want to continue?	~ ~	
VM Name A	Other S	Cancel Confirm		Q
AuctonAppA3	Planama manarete			Hans A
AuctionAbpE3	Force Failover			
Auction/083				
AuctionLB3				Rists
Auction125G27				
Auction/10SQL3		Cancel	mplete Fallover	Han Y



The task bar shows progress of failover activities.

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

IetiStream DR Protected Domains St	Continuous Rehydration Task Resul		
elect Protected Domain:	AI Task Completed Successfully		Delete E More
Mode -			Edt Detai
	Protected Domain	ANFPD003	nobiobreporec
Recoverable / Total VMs	VMs Recovery Status	Success	2.30.156.2.)
	Total VMs Recovered	20	center \ Cluster-1
	testFGP0 Status:		tenter / Guster- i
temaining Background Dat	Pre-script Execution Status	Not defined	
urrent RPO	Runbook Execution Status	Success	
	Post-script Execution Status	Not defined	
Protected VMs Settin	<u>os</u>		
+ Start Protection	12		٩
VM Name A			d D Details
AuctionAppA3			Details
AuctionApp83			Detans
AuctionDB3			Details
AuctionLB3			Details
AuctionMSQ3			Dismiss Details
AuctionNoSQL3	U POCUTCIALO	won mec-paulyment	Details V

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

3. 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 Contin	nubus. Rehýdratio
Recoverable / Total VMs	20 / 20	Owner Site	REMOT	+ Failback	
					•
Protected VMs Settings Alarms					
Protected VMs Settings Alarms	Protection Stat	tus 🔺 Protection Mc	de 🛦	Details	٩
	Protection Stat	tus A Protection Mc Write-Back(VM		Details Details	9
VM Name			DK)		
VM Name A AuctionAppA3	Recoverable	Write-Back(VM	рк) рк)	Details	
VM Name A AuctionAppA3 AuctionAppB3	 Recoverable Recoverable 	Write-Back(VM Write-Back(VM	DK) DK)	Details Details	
VM Name A AuctionAppA3 AuctionAppB3 AuctionDB3	Recoverable Recoverable Recoverable	Write-Back(VM Write-Back(VM Write-Back(VM	DK) DK) DK) DK)	Details Details 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.

lect Protected Domai	Failback Prote	ected Domain						Delete	≡ More
ode	0 1. General	2a. Fallback Settings	2b. VM Settings	3. Recovery VA	4. DR Sett	ings	5. Summary		Edit Detai
tive Site								^ spo	1
acoverable / Total VMs	Protected D	omain Name		ANFPD003				56.2)	
	Failback Da	tacenter		A300-DataCenter					
	Failback Clu	uster		A300-Cluster					1
Protected VMs Se	Failback Re	source Pool		2				1000	
Protected VMS Se	VM Folder (Optional)		×				1.000	
	Failback Da	tastore		A300_NFS_DS02				- 200	Q
VM Name 🔺	Maximum D	elay After Stopping		60 Minutes					4
AuctionAppA3	Internal Net	work		VM_187					^
AuctionAppB3	External Re	plication Network		VM_187					
AuctionDB3	Managemen	nt Network		VM_187				~	
A CONTRACTOR OF A CONTRACTOR O					Cancel	Back	Failback		

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

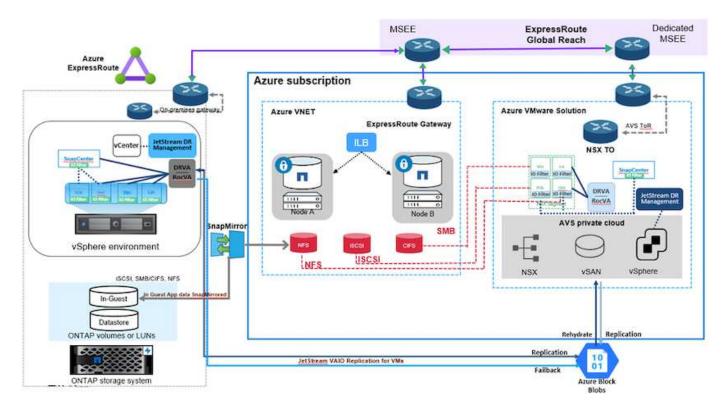
Disaster recovery to cloud is a resilient and cost-effective way of protecting workloads against site outages and data corruption events such as ransomware. With NetApp SnapMirror, on-premises VMware workloads that use guest-connected storage can be replicated to NetApp Cloud Volumes ONTAP running in Azure.

Overview

Authors: Ravi BCB and Niyaz Mohamed, NetApp

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	(+
0	gcsdrsqidb_sc46 ntaphci-a300e9u25	gcsdrsqidb_sc46_copy ANFCVODRDemo	17 seconds	idle	snapmirrored	May 6, 2022, 11:43:18 AN 105.06 KiB	
0	gcsdrsqlhld_sc46_copy ANFCVODRDemo	gcsdrsqlhld_sc46 ntaphci-a300e9u25	7 seconds	idle	snapmirrored	May 6, 2022, 11:42:20 AM 7.22 MiB	
\odot	gcsdrsqllog_sc46 ntaphci-a300e9u25	gcsdrsqilog_sc46_copy ANFCVODRDemo	16 seconds	idle	snapmirrored	May 6, 2022, 11:43:52 AN 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.

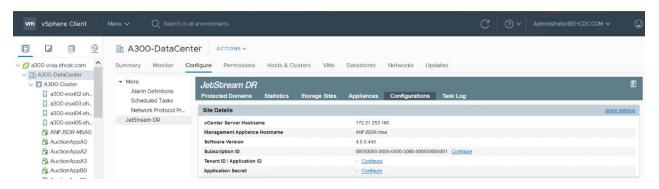
The most common deployed option is to have SDDC running in an always-on, pilot-light mode of operation. This option provides a small footprint of three hosts that are always available, and it also speeds up recovery operations by providing a running baseline for simulation activities and compliance checks, 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	-0000-000000000001 Configure			
Tenant ID / Application ID	- <u>Configure</u>				
Application Secret	- <u>Configure</u>				
Configured Clusters	Configure Clusters				
Configure Cluster Dupgrade Dunconfigure # Res		Select All	Clear All Q		٩
Cluster Name 🔺	Cluster Name 🔺	Datacenter Name		sion 🔺	Host Details 🔺
No cluster configured	A300-Cluster	A300-DataCenter			
		3	*		
		Cancel	Configure		

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

Storage Sites	Add Storage Site	
+ Add Storage Site Scan Domains	Storage Ste Type *	
Name A	Azure Blob Storage	
No Storage Site configured.		
	Access Type *	
	Key Access	
	Storage Site Name (Provide a name to identify this Site) *	
	ANFDemoblobrepo	
Storage Site Details Alarmy		
	Acure Biob Storage Account Name * anfdrdemostor	
No storage site selected. Select a storage		
no surage sile selected, select a surage	Adure Bob Storage Account Key *	
	······································	
	Cancel Add Storage Site	

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.

Jet/Stream DR Protected Domains Statistics Storage Sites Appliance	es Configurations	Task Log			Ē
DRVAs (DR Virtual Appliances)					
+ Desroy New DRVA	Status 🔺	Child Alarm	Software Version	Details	٩
No DR Virtuel Appliance configured.					
Replication Log Volume					
+ New Replication Log Volume 🛛 Unconfigure					Q
Disk Path Name 🔺	Status	Child Alarm	Size (available/total)	Details 🔺	
No DRVA selected. Select a DRVA to view replication log volumes.					

RVAs (DR Virtual Appliances)	1. General 2. DRVA VM	3. DRVA Network 4. Summary	
+ Deptoy New DRVA	Name	GCSDRPD001	Ĩ
fame A	Description (Optional)	Protected Domain for VMs with ANF and JS	Details 🔺
No DR Virtual Appliance configured	Datacenter	A300-DataCenter	
	Cluster	A300-Cluster	
	Resource Pool (Optional)		
	VM Folder (Optional)		
eplication Log Volume	Datastore	A300_NFS_vMotion	
The second se	Number Of CPUs	8	
Here Replication Log Volume 🗳 Unconfigure	Memory Size	32GB	
Nsk Path Name	Management Network	VM_187	Details 🔺
No DRVA selected. Select a DRVA to view replication log volum	Host(iofilter) to DRVA Data Network	VM_187	
	Replication Network to Object Store	VM_187	
	Replication Log Network	VM_187 .	

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

let/Stream DR Protected Domains	Statistics	Storage Sites	Appliances	Configurations	Task Log			
DRVAs (DR Virtual A	ppliances)	Ha						
+ Deploy New DRVA	* Copyrade	Dunconfigure						C
Name A				Status 🔺	Child Alarm 🔺	Software Version	Details A	
OCSDRPD001				O Running	00	4.0.0.134	Detain	
+ New Replication Log		canadrone.						c
Disk Path Name 🔺				Status	Child Alarm	Size (available/total) 🔺	Details A	
idev/sdb				O Ok	0 0	179.88 GB / 200 GB	Details	
Replication Log Volu	ime Details							
solovino substance and solovino second								

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.

JetStream DR Protected Domains Statistics Storage Sites Select Protected Domain: - <u>Viewall</u>	Appliances Confinuations Task Loc Create Protected Domain				+ Create # Morrs
	1. General 2. Pr	vimary Site	J. Summary	4	
	Protected Domain Name	GCSDRPD_Demo01		28- X	
	Priority Level (Optional)	2			
	Description	Protection domain ANF			
	Total estimated data size to be protected	1000GB			
	DR Virtual Appliance	GCSDRPD001			
	Compression	Yes			
	Compression Level	Default		88	
	Normal GC Storage Overhead	50%			
	Maximum GC Storage Overhead	300%			
	Replication Log Storage	/dev/sdb			
	Panlication I on Size	50GR			
		Cancel 6	Back Create		

elect 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		-	
		Cancel	Back Crea		

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.

ebSbream DR rotected Domains Statistics Storage Sites	Appliances Configurations Task Lo					
lect Protected Domain: GCSDRPD_Demo01 -	Start Protection				+ Create Deinte	E Mare
epication Siatun	Protection Mode for principal VMs 🔹				ANFOHDemoFalloverSite	5.00 141
44070293910500				a.	LOCAL (172 21 253 160)	
maining Background Data	VM Name 🔺	# of Disks Pr	otection Mode	12	A303-DataCenter 1A300-Ouster	
itrent RPO	ElasticWebA2	1	ine Through 🛛 😒		Duabled	
	ElasticWebA3		him Through 🗸			
rotected VMs Settings Alarms	ElasticWebB0		nite-Through 🔶			
	ElasticWebB1		ville-Theouph 🛛 👻 -			
+ Start Protection C Stree Presection	ElasticWeb82		ómi Through 🖌 🖌 .			
VM Name A	ElasticWebB3 GCS-DR-DC	144	Alle Through 🖌 👻		Background Data A Details	
No VM is producted	GCS-DR-UrVM01		hite-Through 👻			
Jaho Ano in Burtine and	C OCS-DR-SCA		inte-Through 🗸			
	GCS-DR-SQL01	1.4	inte-Through 👻			
	GCS-DR-WmVM01		inte-Through			
	ss-drva-GCSDRPD001		ime Through St			
	PrimeClent		nte-Through 💉 .			
	Standby0		nte-Through			
	Standby1		me-through 📿	1		
	Standby2		offertreach 😪			
	Standby3	1 V	Atte Through 😪			
	VMmark-Template01	18 19	Timougn 🗸 🗸	a 🛛		

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

ect Protected Domain: GCSDRPD_Demo01	Start Protection				+ Creato E Dotete E Man
coverable / Total VMs				1	Edi De
pication Status	Prevention Water for several VVV Write-Back(VMDK)			q	ANFORDemoFalloverSite
maining Background Data	VM Name 🔺	# of Disks	Protection Mode	1.4811	LOCAL (172.21.253.160.) A300-DataCenter (A300-Cluster
ment RPO	ElasticWebA2	1	Write Through	v. *	Distoled
100.020	ElasticWebA3	1	White-Through	×.	
Totalched VMs Settings Atarms	ElasticWebB0	1	white-Through		
TORELICO VALSI DELLOGI OVALITI	ElesticWebB1	-1	White-Through	- V.	
Start Protector	ElasticWebB2	1	With Through	¥.	
	ElasticWebB3	1	Write-Tracegit	14 m	
VM Name 🔺	GCS-DR-DC	1	Write-Back(VMDK)	~	Bockground Data A Details
No VM is protected.	GCS-DR-LinVM01	3	Write-Back(VMDK)	v	
	GCS-DR-SCA	1	Write-Back(VMDK)	*	
	GCS-DR-SQL01	1	Write-Back(VMDK)	~	
	GCS-DR-WeVM01	31	Write-Back(VMDK)	~	
	jss-dva-GCSDRPD001	2			
	PrimeClient	2		. v .	
	Standby0	1	Write-Trenugh	÷.,	
	Standby1	1		10	
	Standby2	1	White-Through	14. I	
	Standby3	1	Write Through	10	
	VMmark-Template01	1		10.00	
			Cancel Sta	rt Protection	

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 Storage Site	s Appliances Configuration:	s Task Log				Running Tasks	
elect Protected Domain: GCSDRPD_Demo01	• View all				+ (Start Protection (GCS-DR-SCA) 50	Y%s
Recoverable / Total VMs		0/5	Configuration	5		Start Protection (GCS-DR-Win 50	196
replication Status		ок	Storage Site			Start Protection (GCS-DR-Lin 50	196
emaining Background Data		0 B	Owner Site Datacenter \ Clu	ster	LOCAL (172.2 A300-DataCen	Start Protection (GCS-DR-DC) 50	196
urrent RPO			Point-in-time Re	covery	Disabled	Start Protection (GCS-DR-SQ. 50	196
Protected VMs Settings Alarms						Configure VMDK Re _ Completed	-
+ Start Protection							c
VM Name	Protection Status	Replication St	atus 🔺	Protection Mode 🔺	Background Dat	ta ▲ Details	
VM Name A				Write-Back(VMDK)		Details	1
GCS-DR-DC	Initializing					Details	
	Initializing Initializing	+		Write-Back(VMDK)		PUZEGIIS .	
GCS-DR-DC	Contraction of the second s	*		Write-Back(VMDK) Write-Back(VMDK)		Details	
GCS-DR-DC GCS-DR-LinVM01	O Initializing				•		

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

select Protected Domain: GCSDRPD_Demo	01 👻 <u>View all</u>			+ Create	Delete	≡ More
lecoverable / Total VMs		5/5	Configurations			Edit Deta
teplication Status		OK	Storage Site	ANFDRDemoFallo	verSite	
			Owner Site	LOCAL (172.21.253.16	(0	
emaining Background Data		08	Datacenter \ Cluster	A300-DataCenter \ A30	0-Cluster	
urrent RPO		05	Point-in-time Recovery	Disabled		
Protected VMs Settings Alarms						
+ Start Protection	Brotection Status	Replication Stat	tris + Drotection Mode +	Background Data	Datails	٩
	Protection Status ▲	Replication Stat	tus Protection Mode Write-Back(VMDK)	Background Data ▲ 0 B	Details Details	٩
+ Start Protection VM Name						
+ Start Protection VM Name GCS-DR-DC	Recoverable	O OK	Write-Back(VMDK)	0 B	Deteils	
+ Start Protection VM Name GCS-DR-DC GCS-DR-LinVM01	 Recoverable Recoverable 	0 0K 0 0K	Write-Back(VMDK) Write-Back(VMDK)	08	Details Details	

()

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

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

Select Protected Domain: GCSDRPD_Demo01 View all				+ Create	Delete	≡ More
Recoverable / Total VMs	5/5	Configurations				Edit Deta
Replication Status	ОК	Storage Site	AN	FDRDemoFailove	Site	
		Owner Site	LOCAL	(172.21.253.160)	
Remaining Background Data	0 B	Datacenter \ Cluster	A300-D	ataCenter \ A300-0	Cluster	
Current RPO	0s	Point-in-time Recovery	Disable	đ		
Protected VMs Settings Alarms						
Failover Runbook Not Configured Configure						
Test Failover Runbook Not Configured Configure						
Fallback Runbook 😓 Not Configured Configure						
Memory Setting Not Configured Configure						
GC Settings Configured Configure						
de settings compared somethie						

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.

 (\mathbf{i})

JetStream DR Protected Domains Statistics Storage Sit	es / Failover Runbook Settings				
Select Protected Domain: GCSDRPD_Demo01	- Ver + Create Group	Delete Group		+ Create Delete	≡ More
Recoverable / Total VMs	O Group Name	# of VM Power Off	Retain MAC		Edit Detail
Replication Status	O 🗌 Independent VMs	5		ANFDRDemoFalloverSite	9
				LOCAL (172 21 253 160)	
Remaining Background Data				A300-DataCenter \ A300-Cluster	
Current RPO				Disabled	
Protected VMs Settings Alarms	0 0		- 11		
Failover Runbook Configured Defails					
Test Failover Runbook Configured Details					
Failback Runbook Configured Details					
Memory Setting Not Configured Configure					
GC Settings Configured Configure					
Concurrency Settings Not Configured Configure					

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.

elect Protected Domain: GCSDRPD_Demo	1. General	2. Select VM	5		M Settings		4. Summ		Create	III Cielitte	≡ More
	Retain MAC		Power Of	f VMs			O Reset	1			
	VM Name	Boot Sequence	Boot Delay	CPU	Memory	Script	NIC		HernoFladoverS 21 253 165 1		
	GCS-DR-WinVM01	17 4	0s	32	64 GB	Config	View	A DESCRIPTION OF THE OWNER OWNER OF THE OWNER OWNER OF THE OWNER			
	GCS-DR-SCA	21 4	0s	4	16 GB	Config	View				
	GCS-DR-DC	3 B	0s	4	16 GB	Config	View				
	GCS-DR-LinVM01	41 4	0s	2	4 GB	Config	View				
	GCS-DR-SQL01	5 7 4	0s	4	8 G8	Config	View	*			
GC Settings Configured <u>Configures</u> Concurrency Settings Not Configured <u>Configures</u>											

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.

Select Protected Domain: GCSDRPD_Demo	1. General	2. Select VM:		1 5 40 10	M Settings		4. Summa	in.	+ Creale	Dente	1
Recoverable / Total VMI		2. Select vini			w settings		4. Summ	ny 👘			
Replication stams	Retain MAC		Power Off	VMs			O Reset		FORDEmoFallov		
Repiration status	VM Name	Boot Sequence	Boot Delay	CPU	Memory	Script	NIC				
Remaining Background Data	GCS-DR-WinVM01	1† ↓	0s	32	64 GB	Config	25	*			
Clatest RPO	GCS-DR-SCA	2↑↓	Qs	4	16 GB	Contig					
Comment of the	GCS-DR-LinVM01	3↑ ↓	0s	2	4 GB	Config	View				
Protected Villa Settings Alarma	GCS-DR-SQL0	47 4	0s	4	8 GB	Config	View				
	GCS-DR-DC	5† ↓	0s.	4	16 GB	Config	View	*			
GC Settings Configured Configured Configured Configured Configured Configured Configured											

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

Create R	VM NICs					
	Label	Network Name	Key	PCI Slot #	IP	
	Network adapte	r 1 VM_3510	4000	192	Contigure	ary
VM Na GCS-E Libunti GCSD		nfigure Static IP Addre	55			1
GCS-E		ddress * 2.21.254.185				
	25 Gar	met Mask = 5.255.255.0 wway = 2.21.254.1				
		2.30.153.20 IS Suffix Reset	Canc	el Confi	gure	
JobStream DR Protected Domains		sate Runbook Group			Close	Next
Benet Protected Domain Protected Control Protection States Research Protection Protection States Testion Ratiosactics Testion Ratiosactics	Allan Allan Allan	1. General 2. Select VI Group Name Number of VMs Retain VMs MAC addresses Power Off VMs Group manganings and boot sequence change Success	GCSRecovery 5 true faise		* Could * Copport atoms in Copport atoms in C	

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.

and the second sec			E & C & C P hijker@netapp.com
Home > ANFDataClus			Run command - Install-JetDRWithDHCP
ANFDataClus Run ArS Private clood	n command —		This top level Criticit Downloads JetDr bundle from MMS, creates a new user, assigns
P Seatch (Ctrl+/) =	C) Refresh 🛱 Feedback		elevated privilleges to the user, deploys JetDr Management Server Appliance(MSA), registers vCenter to the JetDr MSA, configures cluster.
 Access control (IAM) Tags 	Packages Run execution status		Command parameters
			RegisterWithip ()
Diagnose and solve problems	 Name 	Description	True True
Settings	V SOR Configuration 204 Powers	er Manuae for sampuration at lettheore Softwore on 205. See Jettineon Softwore, mo for support	ProtectedCluster * ()
A Locks	Disatile-letDRForCluster	This Cindlet unconfigures a cluster but doesn't uninstall JetDR completely so other clusters	Cluster-1
2 6004		policies.	Detastore * ()
fanage	Enable-JetORForCluster	This Cmdlet configures an additional cluster for protection. It installs vibs to all hosts in the	vsanDatastore
Connectivity	Install-JetDRW/thDHCP	This top level Critiet Downloads JetDr bundle from MMS, cwates a new user, assigns view	VMName* ()
Custers	The second second second second	registers vCenter to the JetDr MSA cooligures cluster.	anfjordi-msa
Construction of the second s	Install-JetDRW/(th6tallc)P	This top level Cristlet Downloads JetDr bundle from MMS, cristes a neur user, assigns elevi	Cluster* ()
I Identity		registers vCenter to the JetDr MSA, configures duster.	Outer-1
Storage (preview)	Invoke-PreflightJetDRIvataB	This Cridlet checks and displays current state of the system it checks whether the minimal	Credential 💿
Placement policies		4 hosts, if the cluster details are correct, if there is already a VM with the same name provid	Username *
Add-oni	Invoke-Preflight/etDRUminstall	This Ciriclet checks and displays current state of the system it checks whether the minimal	root
	a million of the second s	4 hosts, if the cluster details are correct and if any VCenter is registered to the MSA	Persword *
Workload Networking	Uninstal-letDR	The top level Gmdlet creates a new user, assigns elevated privilleges to the user, unconfigu	
Segments	> MicrosoftAVSManagement +147	Version and lats for eliminate larve takis in managing Azara VMMies Southans	HostName ()
DHOP			anfpoal-ma
Port minoring			Network* (i)
			DRSeg
O DNS			
Operations			Details
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.

Site Details							Alarm Set	ti
vCenter Server Hostna	me	172.30.15	56.2					
Management Appliance	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	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.

Protected Domain Description	Recoverable V VMs				
GCSDRPD_Demo01 Protection domain	in ANF 5 5	Imoget	_		٩
				en Filob Storage	~
				re Blob Storage	
		Protected Domain Description recoverable V Vita GCSDRPD_Demo01 Protection domain ANF 5 5 5	GCSDRPD_Demo01 Protection domain ANF 5 5 Imond	GCSDRPD_Demo01 Protection domain ANF 5 5 Imogd	GCSDRPD_Demo01 Protection domain ANF 5 5 Imond

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			+ Create	Delete	≡More
Mode	Imported	Configurations			Det
Recoverable / Total VMs	5/5	Storage Site	ANFDemoblobre	porec	
		Owner Site			
				2000	c
VM Name 🔺	Protection Status	•	Protection Mode	Details	
GCS-DR-DC	O Recoverable	•	Write-Back(VMDK)	Details	
GCS-DR-DC GCS-DR-LinVM01	Recoverable Recoverable	•	Write-Back(VMDK) Write-Back(VMDK)	Details Details	
GCS-DR-DC GCS-DR-Lin/M01 GCS-DR-SCA	© Recoverable © Recoverable © Recoverable	•	Write-Back(VMDK) Write-Back(VMDK) Write-Back(VMDK)	<u>Details</u> Details Details	c
GCS-DR-DC GCS-DR-LinVM01	Recoverable Recoverable	•	Write-Back(VMDK) Write-Back(VMDK)	Details Details	

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

- 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 Failover Protected Don	nain			Delete	Ξ×	More
de	1. General 2a. Failover Settings	2b. VM Settings 3. Reco	very VA 4. DR Settings	5. Summary			Detai
coverable / Total VMs	i, General 2a, Failover Settings	20. Yill Settings 5. Reco	very viel a lon betangs	5. Summary	reporec		1
	Protected Domain Name	ANFPD002			253,160)		
	Datacenter	SDDC-Datac	enter				
	Cluster	Cluster-1			100		1
	Resource Pool (Optional)	•					
rotected VMs Setti	VM Folder (Optional)						
	Datastore	ANFRecoDSI	1002				
	Internal Network	DRSeg					q
VM Name 🛦	External Replication Network	DRSeg			1	etails	
AuctionAppA2	Management Network	DRSeg			-	etaits	^
AuctionAppB2	Storage Site	ANFDemobio	breporec			etaits	
AuctionDB2	DR Virtual Appliance	ANFRecDRV	4003			etais	
AuctionLB2	are recourted to permitte				Image: Display in the second secon	etalis:	

1

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.



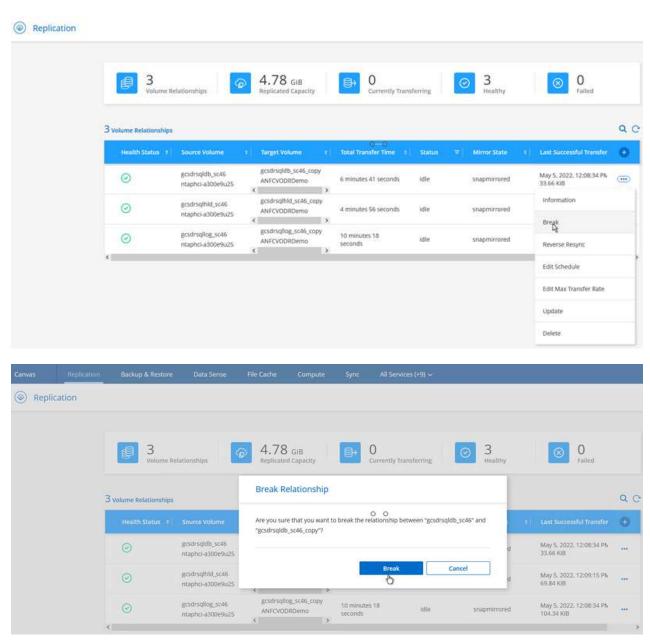
Although Continuous Failover and Failover modes differ on when configuration is performed, both failover modes are configured using the same steps. Failover steps are configured and performed together in response to a disaster event. Continuous failover can be configured at any time and then allowed 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	■More
Mode	Imported	Configurations		O Restore	
tecoverable / Total VMs	5/5	Storage Site	ANFDemoblobrepor	→ Failover	
	10.00	Owner Site	REMOTE (172.21.253.1)	+ Continuous Fail	louar.
				→ Test Failover	G
Protected VMs Settings Alarms O O					
VM Name	Protection Status		Protection Mode	Details	
GCS-DR-DC	@ Recoverable		Write-Back(VMDK)	Details	
GCS-DR-LinVM01	Recoverable		Write-Back(VMDK)	Details	
GCS-DR-SCA	Recoverable		Write-Back(VMDK)	Details	
GCS-DR-SQL01	O 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.



 (\mathbf{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.

lect Protected Domain: GCSDRPD_Demo01	 View all 			+ Create	O Feilover	■Mor
ode	Continuous Rehydration in Progress	Configurations				Details
coverable / Total VMs	4/4	Storage Site			orec	^
	58/1M	Owner Site		REMOTE (172.21.253		
ata (Processed/Known Remaining)	329.01 GB / 6.19 GB	Datacenter \ Cluster	SDDC-Datacenter \ Cluster-1			
irrent Step	Recover VMs' data from Storage Site	Point-in-time Recovery		Disabled		v
Protected VMs Settings Alarms	0 0					
						٩
VM Name 🔺	Protection Status A		Protection M		Details	^
GCS-DR-DC	Recoverable		Write-Back(VI		Details	^
GCS-DR-LinVM01	© Recoverable		Write-Back(VI		<u>Details</u>	
GCS-DR-SCA GCS-DR-SOL01	Recoverable Recoverable		Write-Back(VI Write-Back(VI		Details Details	
GCS-DR-SGL01	© Recoverable		Write-Back(VI		Details	
VM Network Mapping Protected VM Network VM_3510	Recovery VM Network DRStretchSeg	•	^			
0 0			v .,			
Other Settings						
Planned Failover	required because of network configuration:	Configure				

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 Domain re required! Complete ownership of this Protected Site.	CNV250 VA02220 M000	
	Are you sure you want to continue?		
		Cancel	Confirm

M Network Mapping			
Protected VM Network 🔺	Recovery VM Network		^
VM_3510	DRStretchSeg	• ^	•
0 0			
Other Settings			
Planned Failover			
Force Failover			
Some VM's guest credential are requir	ed because of network configuration: Cor	ifigure	
	The second se		

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

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

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

Select Protected D	Domain: GCSDRPD002	Task Completed Successfully with	warnings		+ Greate	2 Deltata	# More
Mode		×.					Edit Data
Social and the second	1970	Protected Domain	GCSDRPD082		ANECVODR		
Recoverable / Total	YM5	VMs Recovery Status	Success with warnings		DCAL (172 30 156 2	800	
		Total VMs Recovered	4		DOC-Datacenter \ Cit		
Remaining Backgros	und Data	VM(s) with warning	2 <u>View</u>		esabled		
centaliting backgrou	onu bala	GCSRecovery03 Status:			1000000		
Corrent RPO)	Pre-script Execution Status	Not defined				
		Runbook Execution Status	O Success				
Protected VMs	Settings Alarms	Post-script Execution Status	Not defined				
+ Start Protection	O Dese Prete chose						c
VM Name A				N	ackground Data 🔺	Details	
GCS-DR-SC45				ES.	8	Details	
GCS-DR-SOLO	13				8	Details	
GCSDR-W2K1	6-01				8	Detaits	
UbuntuStv001					8	Details	

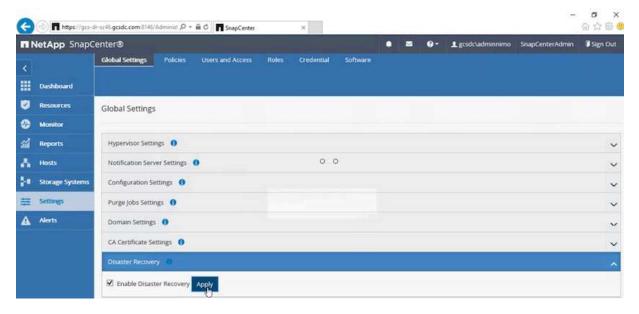
4. After the virtual machines are recovered, use storage disaster recovery for in-guest storage. To

 (\mathbf{i})

i

demonstrate this process, SQL server is us	ed in this ex	ample.	
5. Log into the recovered SnapCenter VM on A	AVS SDDC	and enable DR mode.	
a. Access the SnapCenter UI using the bro	owserN.		
(AX O acced	-sc46.acsdc.com ×	
		- Chagodocom	
		etApp。。	
		• • 0 0	
	SnapCent	er®	
	Username	gcsdc\adminnimo	
	Password	•••••	
a de hadene "reider de		Sign In	

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



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



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

6. Make sure that the SnapMirror relationship is broken.

Canvas	Replication	Backup & Restore	Data Sense	File Cache	Compute	Sync All Service	es (+9) 🛩			
Replication	ation									
		3 Volume Re	lationships		8 GIB Ited Capacity	0 Currently Tran	nsterring	⊘ 3 _{Healthy}	8 Pailed	
		3 Volume Relationships								9
		3 Volume Relationships Health Status	Source Volume	s Target	Volume a	ा—्) Total Transfer Time	: Status =	Mirror State	e Last Successful Transfer	Q (
			Source Volume gcsdrsqldb_sc46 ntaphci-a300e9u25	gcsdrs	Volume : gldb_sc46_copy ODRDemo >		i Status 😨	Mirror-State broken-off	t Last Successful Transfer May 5, 2022, 12:08:34 Ph 33.66 KIB	
		Health Status 🗧	gcsdrsqldb_sc46	gcsdrs ANFCV ¢ gcsdrs	qldb_sc46_copy ODRDemo	Total Transfer Time ÷			May 5, 2022, 12:08:34 PM	0

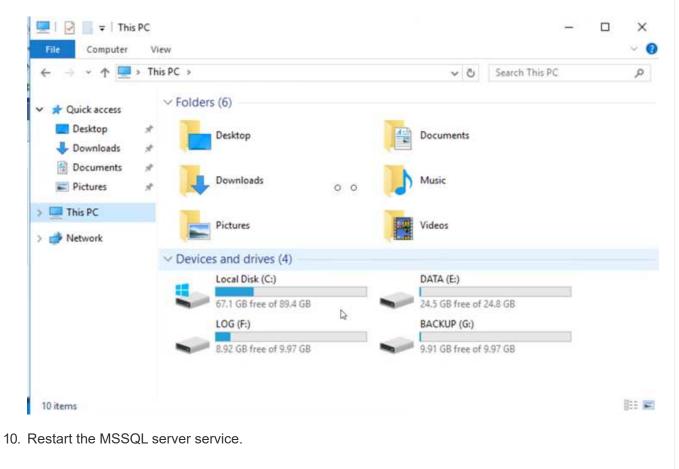
7. Attach the LUN from Cloud Volumes ONTAP to the recovered SQL guest VM with same drive letters.

📅 Disk Manageme	nt						- 	X
File Action Vie	w Help							
(= =) 🖬 🕅	🖬 🗩 🗹 ((H)						
Volume	Layout	Туре	File System	Status	Capacity	Free Spa	% Free	
	Simple	Basic	-	Healthy (R	450 MB	450 MB	100 %	
-	Simple	Basic		Healthy (E	99 MB	99 MB	100 %	
- (C:)	Simple	Basic	NTFS	Healthy (B	89.45 GB	67.03 GB	75 %	
BACKUP (G:)	Simple	Basic	NTFS	Healthy (P	9.97 GB	9.92 GB	99 %	
DATA (E:)	Simple	Basic	NTFS	Healthy (P	24.88 GB	24.57 GB	99 %	
- LOG (F:)	Simple	Basic	NTFS	Healthy (P	9.97 GB	8.93 GB	90 %	
10000000000000000000000000000000000000	•				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.

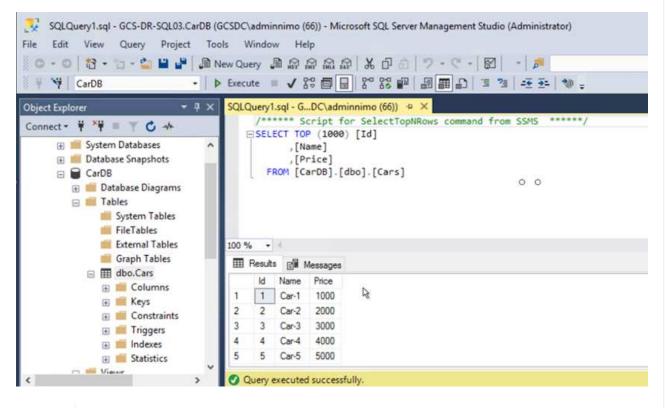
	iator Proper				
l'argets	Discovery	Favorite Targets	Volumes and Devices	RADIUS	Configuration
To disc		on to a target usin arget and then dick	g a basic connection, t Quick Connect.	ype the IP	address or
Target				Q	uick Connect
Discove	ered targets			_	
					Refresh
Name				Status	
Name		netapp:sn.547772c	cc47811ecbb62000	Status Connecte	d

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



(= -> 💼 🖼 🛛	a 🔒 🛛 🖬 🕨 🔳 🕪 🖬					
Services (Local)	Services (Local) SQL Server (MSSQLSERVER)	Name	Description	Status	Startup Type	Log '
	Stop the service	SQL Full-text Filter Daemon	Service to la	Running	Manual	NT
	Pause the service Restart the service Description: Provides storage, processing and controlled access of data, and rapid transaction processing.	SQL Server (MSSQLSERVER) SQL Server Agent (MSSC SQL Server Browser SQL Server CEIP service SQL Server Integration S SQL Server Integration S SQL Server VSS Writer SSDP Discovery State Repository Service Still Image Acquisition E Storage Service Storage Tiers Managem Superfetch Sync Host_df83a System Event Notification S	Provider sto Start Stop Pause ^{ooo} Resume Reftart All Tasks Refresh Properties Help This service Monitors sy	-	Automatic Automatic Automatic Automatic Automatic Automatic Automatic Manual Manual Manual Manual Manual Automatic (D Automatic	GCS GCS Loc NT NT Loc Loc Loc Loc Loc Loc Loc

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



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

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

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.

Jet/Stream DR Protected Domains Statistics Storage Sites Appliances Config	urations Task Log		[
Select Protected Domain: GCSDRPD_Demo01 View all		+ Create	Delete 🗮 More
Mode Ri	Inning in Failover Configurations		O Restore
Active Site	172.30.156.2 Storage Site	ANFCVODR	O Resume Continuous Rehydration
Recoverable / Total VMs	4/4 Owner Site	REMOTE (172.3	+ Fallback
Protected VMs Settings Alarms O O			
VM Name	Protection Status	Protection Mode	Details
GCS-DR-DC	Recoverable	Write-Back(VMDK)	Details
GCS-DR-LinVM01	Ø Recoverable	Write-Back(VMDK)	Details
GCS-DR-SCA	Recoverable	Write-Back(VMDK)	Details
GCS-DR-SQL01	Recoverable	Write-Back(VMDK)	Details
GCS-DR-WinVII01	Recoverable	Write-Back(VMDK)	Details



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

•	•	•	•		•	0
. General	2a. Failback Settings	2b. VM Settings	3. Recovery VA	4. DR	Settings	5. Summary
Failback Da	tacenter		A300-DataCenter			
Failback Cl	uster		A300-Cluster			
Failback Re	source Pool					
VM Folder (Optional)					
Failback Da	tastore		A300_NFS_vMotion			
Maximum D	elay After Stopping		10 Minutes			
Internal Net	wolk		VM_187			
External Re	plication Network		VM_187			
Managemer	nt Network		VM_187			
Storage Site	e		ANFCVODR			
DR Virtual A	Appliance		GCSDRVA002			
Replication	Log Storage		/dev/sdb			

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

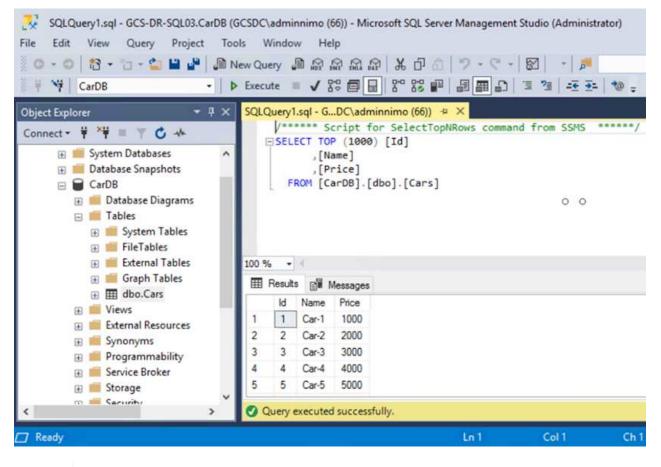
JetStream DR Protected Domains Statistics Storage Si	Failback Task Result			
Select Protected Domain: GCSDRPD002 *	Task Completed Successfully			
Recoverable / Total VMs	Protected Domain	GCSDRPD002		
Replication Status	VMs Recovery Status	Success		
Remaining Background Data	Total VMs Recovered	4		
Containing charge chara course	GC SRecovery03 Status:			
Current RPO	Pre-script Execution Status	Not defined		
	Runbook Execution Status	Success		
Protected VMs Settings Alarms	Post-script Execution Status	Not defined	B	

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

\odot	gcsdrsqldb_sc46 ntaphci-a300e9u25		gcsdrsqldb_sc46_copy ANFCVODRDemo		6 minutes 41 seconds	idle	broken-off		May 5. 2022. 12:08:34 PN 33.66 KiB	
	ntapht+a500e9025	4		•					Information	
\odot	gcsdrsqlhld_sc46 ntaphci-a300e9u25		gcsdrsqlhld_sc46_copy ANFCVODRDemo		4 minutes 56 seconds	idle	broken-off		mormation	
	10 1265 C.N.	(4)	gcsdrsqllog_sc46_copy	Þ.:					Resync	
\odot	gcsdrsqllog_sc46 ntaphci-a300e9u25		ANFCVODRDemo		10 minutes 18 seconds	idle	broken-off		Reverse Resync	
		. 4		6				_		
									Edit Schedule	
									Edit Max Transfer Rate	
									Delete	

Volume Re	lationships	6.54 GIB Replicated Capacity	O Currently Tran	sferring	Ø 3 Healthy	S O Failed	
/olume Relationships	1		0 0				Q
Health Status 🗧	Source Volume +	Target Volume +	Total Transfer Time 💠	Status	■ Mirror State ■	Last Successful Transfer	ŧ
0	gcsdrsqldb_sc46 ntaphcl-a300e9u25	gcsdrsqldb_sc46_copy ANFCVODRDemo	19 seconds	idle	snapmirrored	May 6, 2022, 11:03:000A 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 ntaphci-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.

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)

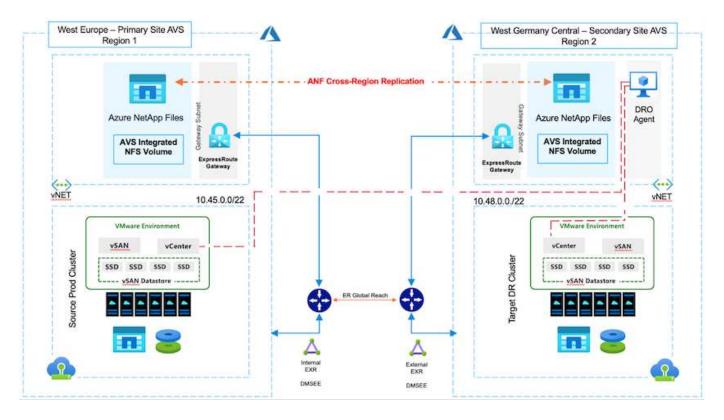
Disaster recovery using block-level replication between regions within the cloud is a resilient and cost-effective way of protecting the workloads against site outages and data corruption events (for example, ransomware).

Author(s): Niyaz Mohamed, NetApp Solutions Engineering

Overview

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.

Ho		Volumes > testrepidemo (WEANFAVSacct/testcap/testrepidemo)			
»	testrepidemo (WEAN	IFAVSacct/testcap/testrepIdemo) Replication * ···			×
	🔎 Search	🕐 Refresh			
	Cverview	↑ Essentials			JSON View
	Activity log	End point type : Source	Destination	: testrepidemo.copy	
3	Access control (IAM)	Health status : Healthy	Relationship status	: Idle	
•	🔷 Tags	Mirror state : Mirrored	Total progress	: 2.13 GiB	

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 Drame Lawrence with Guil Veemane	
	Passourd	
	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 Monitoring	4 * 0 ©
Add New Credential	Credentials Details	×
	Enter Credentials Details	
	Credential Name	
	Tenant Id	
	Client Id	
	Client Secret	
	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 🔌 Dashboard Discover Resource Groups Replication Plans Job Monitoring	٠	?	9
Add New Site Of Site Type (2) Site Details (3) vCenter Details (3) storage Details			×
Site Type			
Source Destination			
Continue			

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 v	
	Add New Credential D			
		AVS Details		
	Web Clie	nt URL	0	
		ANFDataClus	·	
	Usernam		0	
	cloud	idmin@vsphere.local		
	Password		0	
		•••••		
		Accept self-signed certificates		
		Meteps sen-signed cerunicates		

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

15. Click Create Site.

P Disaster Recovery C	Orchestrator 🗞 🕴 Dæ	shboard Di	icover	Resource Group:	s Replication Plar	s Job Monit	ning			\$	¢
					Site Type			Site Location			
C 2 Sites	2 vCer	nters	B 2	orages	💁 1 Source	(2) Desti		On Prem	Cloud 2		
									9.0	Add New Site	1
2 Sites									40	- Andrew Construction	_
2 Sites		¢ i s	te Type	⇒ Location	≂) vCenter ≎	Storage © N	M List	Discovery Status	4.0	1	
			ite Type estination		vCenter ≎	Storage ‡ \	M List	Discovery Status • https://10.75.0.2/	© Success	1	

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.

Back					
		VM List Site: DemoSRC vCenter: https://17	2.30.156.2/		
			VM Protection		
Contas Datas	itares	128 Virtual Machines	🦁 2. Protected	0 126 Unprotected	
128 vm				Q	Create Resource Group
VM Name	C VM Status	1 WM SDME	DuteStore	5 I. OU	2 Memory (MB)
HDBench,2.5.1	O Not Protected	() Powered On	vianDatastore	5	8192
hci-fio-datastore-13984-0-1	0 Not Protected	Powered Off	HOtstDS	32	65538
ICCA2005-WO-R1	Not Protected	() Powered On	wanDatastore	8	14336
	0 Not Protected	() Powered On	vianDataitore	1	3072
ICCA2005-NE-R1					
100A2005-NE-R1 100A2005-01-R1	Q Not Protected	🕐 Powered On	vianDatactore	-5	3072

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.

tApp	Disaster Recovery Orchestrator 🔌 🛛 Di	ashboard Discover	Resource Groups Re	plication Plans J	b Monitoring			٩	٠	?	2
	3 1 Resource Group		1 Site		P 1	ð	2 Virtual Machines				
	1 Resource Group					Q 9	Create New Resource	e Group			
	Resource Group Name DemoRG	Site Name DemoSRC		(E)	Source vCenter https://172.30.156.2/	≂ I VML	ist iew 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

NetApp Disaster Recovery Orchestrator	Dashboard Dis		Replication Plans	Job Monitoring			¢ 0	9
Edit Resource Group		Resource Group Deta	ils 🕜 Select VMs	3 Boot order	r and Delay			
			Boot order an	d Delay				
	VM Name	Boot Order 💿		Boot Delay	(secs)			
	QALin1	3	10	0	121			
	QALin	3	10	0	[0]			

6. Click Create Resource Group.

Арр	Disaster Recovery Orchestrator 💊 🛛 🕻	Dashboard Discover Resource Groups Re	eplication Plans Job Monitoring	* 0
	D 1 Resource Group	□ 1 Ste	Center	P Virtual Machines
	1 Resource Group Resource Group Name	0 Site Name	≂ Source vCenter	Q D Create New Resource Group
	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.

Source Details Image: Replication Plans Image: Resource Groups Source Details Image: Replication Plans Source Details Image: Replication Plans Source Details Image: Replication Plans Source Details Image: Replication Plans Image: Replication Plans		p Disaster Recovery Orchestrator 💊 Dashboard Discover R	esource Groups Replication Plans Job Monitoring		
Replication Plans Resource Groups Sites vCenters Sites vCenters	Replication Plans Resource Groups Sites vCenters 1 Replication Plan Q O Create New Replication Plan		Source Details	Destination Details	
		Replication Plans	ps 1 22 1 Sites vCenters		
					Rapitation Dise

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 Group	s Replication P	lans Job Monitoring		۹	٥	?	9
Create New Replication Plan	Replication Plan and Site Details	 Select Resource 	Groups 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 I	Mapping					
	Source Site Resource	O Destination	n Site Resource					
	Cluster-1	•	Cluster-1 *	Add				
	Source Resource	Destinat	ion Resource					
		No Mappi	ngs added!					
			ntinue					

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

NetApp Disaster Recovery Orchestrator	Dashboard Discover Resource Gro	oups Replication Pla	ns Job Monitoring			٠	?	۹
Create New Replication Plan	(1) Replication Plan and Site Details	2 Select Resource G	roups 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 I	Mapping					
	No more S	ource/Destination clust	er resources available for mapping					
	Source Resource	Destination Re	source					
	Cluster-1	Cluster-1	Delete					
		Cont	tinae -					

- 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	Sroups Replication Plans Job 1	Monitoring	¢ 6	•
Create New Replication Plan	Replication Plan and Site Details	Select Resource Groups 3	Set Execution Order ④ Set VM Details		×
		Replication Plan Det	tails		
		Select Execution Orde	er		
	Resource Group Name		Execution Order 🜒		
	DemoRG		3 [0]		
		Network Mapping			
	No more	Source/Destination network resource			
	Source Resource	Destination Resource			
	SepSeg	SegDR	Delete		
		DataStore Mapping			
	Source DataStore	Destination Volume			
	TestSrc01	gwc_ntap_acct/gwc_DRO_cp/testsrc	О1сору		
		Previous	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.

Create New Replication Plan	Replication Plan an	d Site Details 🕢 Select Resou	rce Groups 🕢 Set Exec	ution Order	Set VM Details		
		v	M Details				
	2 vms				٩		
	VM Name	No. of CPUs	Memory (MB)	NIC/IP	Boot Order 🕢 E Override		
	Resource Group : Demo	RG		-			
	QALin1	1	0 1024 (d)	 Static Dynamic 	3 0		
	QALin	4	0 1024 0	 Static Dynamic 	3 0		

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.

Replication Plans	Sites 1	1 vCenters Sites	
1 Replication Plan			Q O Create New Replication Plan
Plan Name C Active Site Status DemoRP O Source O Active		emoSRC DemoDest	e I I I Resource Groups
			Plan Details Edit Plan
			Fallover
			Test Fallover

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.

🖪 NetApp	Disaster Recovery Orc	hestrator 💊 🛛 Das	hboard Discover Resource (Groups Replication Pla	ins Job Monitoring					¢	0 3
				Source Details		Destination De	talis				
	B 1 Replica	ation Plans	Resource Groups	Sites	vCenters	Sites 1		vCenters			
			Testfailover Details			×					
	1 Replication Plan		 Use latest snapshot Select specific snapshot 	0		^	Q 9	Create New Replication Pla	in		
	Plan Name	Calify Active Site	Volume	•	Snapshot	- 1					
	DemoRP	⊘ Source	WEANFAVSacct/testcap/te	stsrc01	Select Snapshot	-	Reso	urce Groups			
					2023-04-28						
					2023-04-28T11:31:55.000Z - gwc_ntap	h					
					2023-04-28T11:21:54.000Z - gwc_ntap	···· 🗸					
				Start Te:	stfailover						
						<i>1</i> 1					

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.

Back			
	Test Failover Steps 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 🕕

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.

Enderonmenta 2 2 Vortual Environ SDOC Summery		Topology Carvas		Immenaliye View (3
Const		DemoSHC teque /172.38.156.	Devision of the second	
12 Dated	ores 212 Networks			
Execution Jobs		Replication Plans		

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**.

		Source Details		Destination Details	
Replication Plans	Resource Groups	Sites 1	vCenters	Sites 1	vCenters
1 Replication Plan				QĐ	Create New Replication Plan
				2.5.7.5	
Plan Name C Active S					
DemoRP	stination O Running In Faile	wer Mode (Healthy	DemoSRC	DemoDest R	esource Groups)
DemoRP 📀 Des	stination () Running In Failo	over Modi 🕝 Healthy	DemoSRC	DemoDest (R	esource Groups

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

民 1	cation Plans	1 Resource Groups	Source Details	7 1		stination Details	2 1	
Repli	cation Plans	Resource Groups	Sites	vCenters		lites	vCenters	
1 Replication Plan						Q 9	Create New Replication Pl	lan
Plan Name	0 Active Site	Status	Compliance	Source Site	😤 Destination S		li l	
DemoRP	© Destination	⊙ Active	 Healthy 	DemoSRC	DemoDest			
Demoke	Opestination	() ACIVE	() Healthy	DEMOSKC	DemoDest	C He	Plan Details	
							Fallback	_
APP Disaster Recovery C	rchestrator 💊 🛛 Dashimani	Discover Résource Gros	gis Replication Plans	Job Monitoring				
			Warding 1916 - Steeling		(U)			
						Descended VMA		
	2	1	a. 1	-	128	Protected VMs	0 127	
0	2 Sites	1 Resource Group	3 1 Replication Plan	đ	128	Protected VMs 1 Protected	0 127 Unproducted	
	2 Sites	Hestorie Group		B	128 VMs	01	Unprotected	
Invitormenti		1 Resolucce Groups Topology		8	128 vita	01		2
	82	Topology		8	128 vMa	01	Unprotected	2
Environments 2 2 Virtual Environm	82	Topology	Canvas		128 VMs	01	Unprotected	2
Environmenti	82	Topology)	128 VMs	01	Unprotected	9
Environments 2 2 Virtual Environment SDDC Summary	ents Alter Storage Acces	Topology	Cences)	VMs	Devt	Unprotected	9
Environments 2 2 Virtual Environment SDDC Summary	ents Alter Storage Acces	Topology	Ceness	*3		Devt	Unprotected	9
Environments 2 vintual Environments SEDIC Summary Cluster	enta E 2 Attri filosope Acces D 14 Fold	ers	Cences	₽	VMs	Devt	Unprotected	9
Environments 2 2 Virtual Environment SDDC Summary	enta E 2 ANY Stronger Accord	ers	Cences	*3	VMs	Devt	Unprotected	9
Environments 2 2 Virtual Environment SDDC Summary	ents Alter Storage Acces	Topology	Cences	*3	VMs	Devt	Unprotected	9
Environmenti 2 2 Ventual Environmenti SDDC Summery Cluster 12	enta E 2 ANY Stronger Accord	ers	Cences	*3	VMs	Devt	Unprotected	9

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

Setup AVS on Azure

• 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

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.

Author: Niyaz Mohamed - NetApp Solutions Engineering

Overview

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.

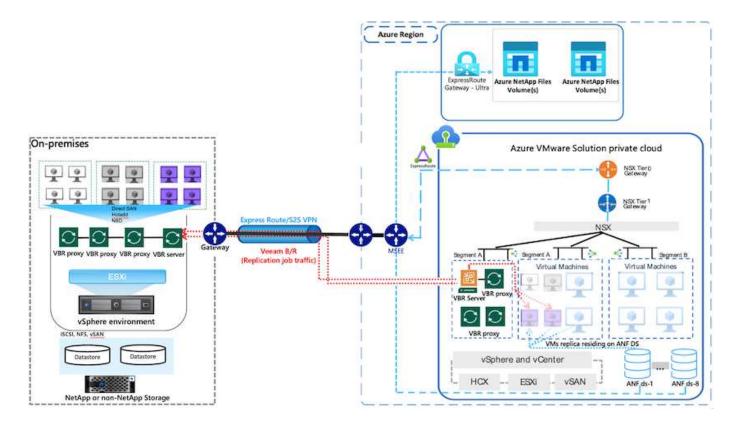
Purposes of this document

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.



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.

Name	Name:
/irtual Machines	AVS_20230522_RepJob01
in coor moenines	Description:
Destination	Created by VEEAMBKPSRV05\Administrator at 5/21/2023 10:52 PM.
Network	
lob Settings	Show advanced controls:
Data Transfer	Replica seeding (for low bandwidth DR sites)
Jata Iransfer	Network remapping (for DR sites with different virtual networks)
Guest Processing	Replica re-IP (for DR sites with different IP addressing scheme)
Schedule	
Summary	
	✓ High priority
	Backup infrastructure resources are offered to high priority jobs first. Use this option for jobs

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.

Virtual Machines

Select one or more VMs to replicate. Use exclusion settings to exclude specific VMs and virtual disks from replication.

	Name	Туре	Size	^	Add
Virtual Machines	TestVeeam21	Virtual Machine	873 MB		Remove
Destination	TestVeeam22	Virtual Machine	890 MB		Nethinke
o constituin	TestVeeam23	Virtual Machine	883 MB		
Network	TestVeeam24	Virtual Machine	879 MB		Exclusions
	TestVeeam25	Virtual Machine	885 MB		Source
lob Settings	TestVeeam26	Virtual Machine	883 MB		
	TestVeeam27	Virtual Machine	879 MB		
Data Transfer	TestVeeam28	Virtual Machine	880 MB		🕈 Up
Guest Processing	TestVeeam29	Virtual Machine	878 MB		+ Down
outservotessing	TestVeeam30	Virtual Machine	876 MB		
Schedule	TestVeeam31	Virtual Machine	888 MB		
	TestVeeam32	Virtual Machine	881 MB		
Summary	TestVeeam33	Virtual Machine	877 MB		
	TestVeeam34	Virtual Machine	875 MB		
	TestVeeam35	Virtual Machine	882 MB		Recalculate
	WinSQL401	Virtual Machine	20.3 GB		
	WinSQL405	Virtual Machine	24.2 GB		Total size:
	Phone course			Y	120 GB

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**.

Name	Host or cluster:	
/irtual Machines	Cluster-1	Choose
Destination	Resource pool:	
Network	Resources	Choose
ob Settings	Pick resource pool for selected replicas VM folder:	
Data Transfer	vm	Choose
Guest Processing	Pick VM folder for selected replicas	
Schedule	Datastore: ds001 [152.6 GB free] ds001 is an ANF Datastore	Choose
Summary	Pick datastore for selected virtual disks	1

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

Name	Network mapping:		i
Virtual Machines	Source network Source Number of Source	Target network SepSeg SegmentTemp	Add Edit
Destination Network	The state (vos-switche)	segment emp	Remove
Job Settings Data Transfer Guest Processing Schedule Summary			

- 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**.

lame irtual Machines	Enable application-aware processing Detects and prepares applications for consistent backup, performs transaction logs configures the OS to perform required application restore steps upon first boot.	processing, and
estination	Customize application handling options for individual machines and applications Guest interaction proxy:	Applications
letwork	Automatic selection	Choose
ob Settings	Guest OS credentials:	
ata Transfer	v	Add
	Manage accounts	
uest Processing	Customize guest OS credentials for individual machines and operating systems	Credentials
chedule	Verify network connectivity and credentials for each machine included in the job	Test Now
ummary		

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

Name	Run the job automatically	r					
Virtual Machines	Daily at this time:	10:00 PM	•	Everyday		~	Days
	O Monthly at this time:	10:00 PM	*	Fourth \vee	Saturday	~	Months
Destination	O Periodically every:	1	s.	Hours		\sim	Schedule
Network	O After this job:	Replication	Job	2 (Created by VEEA	MBKPSRV05\A	dministr	ator at 6/6/
Data Transfer Guest Processing Schedule Summary	 Retry failed items proc Wait before each retry Backup window Terminate job if it exce If the job does not cor terminated to prevent 	attempt for: eeds allowed I	alloc	ated backup wind			Window

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.

1	- 1
	-1
	i.

Summary

The job's settings have been saved successfully. Click Finish to exit the wizard.

Name	Summary:	
	Name: AVS_20230522_RepJob01	^
/irtual Machines	Type: VMware Replication	
	Source items:	
Destination	TestVeeam21 (a300-vcsa05.ehcdc.com)	
	TestVeeam22 (a300-vcsa05.ehcdc.com)	
Network	TestVeeam23 (a300-vcsa05.ehcdc.com)	
VELWOIK	TestVeeam24 (a300-vcsa05.ehcdc.com)	
1.6.11	TestVeeam25 (a300-vcsa05.ehcdc.com)	
ob Settings	TestVeeam26 (a300-vcsa05.ehcdc.com)	
	TestVeeam27 (a300-vcsa05.ehcdc.com)	
ata Transfer	TestVeeam28 (a300-vcsa05.ehcdc.com)	
	TestVeeam29 (a300-vcsa05.ehcdc.com)	
Suest Processing	TestVeeam30 (a300-vcsa05.ehcdc.com)	
	TestVeeam31 (a300-vcsa05.ehcdc.com)	
chedule	TestVeeam32 (a300-vcsa05.ehcdc.com)	
	TestVeeam33 (a300-vcsa05.ehcdc.com)	
ummary	TestVeeam34 (a300-vcsa05.ehcdc.com)	
	TestVeeam35 (a300-vcsa05.ehcdc.com)	
	WinSQL401 (a300-vcsa05.ehcdc.com)	
	WinSQL405 (a300-vcsa05.ehcdc.com)	
	WinSQL404 (a300-vcsa05.ehcdc.com)	~
	Run the job when I click Finish	

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

	S. Second			T. 1 mg					
tran Brann Brann Brann Brann Brann Brann Brann Brann Brann Brann	Anna anna an A		a talan	-	e Fatera		 11	Service Control of the service of th	
		111	:] ;]		Hh	1			
	7	1.1							

For additional information for Veeam replication, refer How Replication Works

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.

Backup Replication CDP B Job * Job * Policy C	ackup Copy opy * Job * Auxiliary Jobs	Restore Failover Plan • Restore Acti	Backup			
Home		Q. Type in an object name	🗙 🍸 All jobs			
Jobs		Name 🗸	Туре	Objects	Status	Last Run
猶 Replication		🔅 Replication Job 2	VMware Replication	1	Stopped	63 days ago
Replicas Ready Active (4)		AVS_20230522_RepJob0	1 VMware Replication	20	Stopped	8 days ago

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.

ieneral	Name: ANF_AVS_FP01	
Virtual Machines	Description:	
Summary	Created by VEEAMBKPSRV05\Administrator at 5/24/2023 9:08 AM.	
	Pre-failover script:	
		owsear
	Post-failover script:	
	Bo	owsen

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

e vm ^{met.}					
General	Virtual machines:				N I COMPANY
Virtual Machines	Name	Delay	Replica state	<u>^</u>	Add VM
virtual Machines	TestVeeam21	2 sec	63 days ago (5:52 AM T		Remove
iummary	TestVeeam23	2 sec	7 days ago (10:12 AM T		Hemore
	TestVeeam24	2 sec	7 days ago (10:20 AM T		Set Delay
	TestVeeam22	2 sec	7 days ago (10:10 AM T		
	WinSQL401	2 sec	7 days ago (3:52 AM Tu		
	WinSQL405	2 sec	8 days ago (4:05 PM Mo		
	TestVeeam25	2 sec	7 days ago (10:14 AM T		
	TestVeeam26	2 sec	7 days ago (10:17 AM T		
	TestVeeam27	2 sec	7 days ago (10:18 AM T		
	TestVeeam28	2 sec	7 days ago (10:14 AM T		
	TestVeeam29	2 sec	7 days ago (10:18 AM T		
	TestVeeam30	2 sec	7 days ago (10:15 AM T		
	TestVeeam31	2 sec	7 days ago (10:21 AM T		
	TestVeeam32	2 sec	7 days ago (10:13 AM T		
	TestVeeam33	2 sec	7 days ago (10:15 AM T		
	TestVeeam34	2 sec	7 days ago (10:14 AM T		✿ Up
	TestVeeam35	2 sec	7 days ago (10:20 AM T	~	✤ Down

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

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**.

Start Start Retry Undo to Actions Details	Edit Delete Manage Plan					
Home	Q, Type in an object	name to search for	ř.	×		
🛚 🖓 Jobs	Name 1	Platform	Status	Number of VMs		
緧 Replication	ANF_AVS_FP01	VMware	Completed	20		
Replicas		Start				
Ready		Start to				
Active (4)		S Undo				
Failover Plans	-	III Statistics				
Last 24 Hours	12		-			
Success	1	Delete				
	3	Edit				

Name: ANF_AVS_FP01 Restore type: Failover Plan Initiated by: VEEAMBKPSRV05	Start time:	In progress 8/9/2023 3:37:41 AM <u>Cancel restore task</u>	
VM name Status	Log		
TestVeeam21 🜔 Proce	Message	Durat	tion ^
TestVeeam23 🜔 Proce	🕲 Waiting 2 sec before the next \	/M 0:00	0:02
TestVeeam24 🕑 Proce	Processing VM: TestVeeam22	0:00	0:13
TestVeeam22 🜔 Proce	Waiting 2 sec before the next \	/M 0:00	0:02
WinSQL401 () Proce	Processing VM: WinSQL401	0:00):10
WinSQL405 () Proce	Waiting 2 sec before the next \	/M 0:00	0:02
TestVeeam25 🜔 Proce	Processing VM: WinSQL405	0:00):08
TestVeeam26 Deroce	Waiting 2 sec before the next \	/M 0:00):02
TestVeeam27 () Pendi	Processing VM: TestVeeam25	0:00):06
TestVeeam28 🜔 Pendi	🔮 Waiting 2 sec before the next \	/M 0:00):02
TestVeeam29 🜔 Pendi	Processing VM: TestVeeam26	0:00):04
TestVeeam30 🕑 Pendi	🖉 Waiting 2 sec before the next \	/M 0:00):02
TestVeeam31 () Pendi	Processing VM: TestVeeam27	0:00):02
TestVeeam32 Dendi	() Waiting 2 sec before the next \	/M 0:00):02
TestVeeam33 🜔 Pendi			~

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.

• Step	· Distaini Support las	-baser a Alate	litelite Manufithan P 🖉 Apres In	mitakan tir ti	a solar a	() Logo						8
C	0 & ++	ildz:		- International In	and have been as a second	and a						+ 0 U ± 1
visitee Clere CD,		-										C ammendita Q (
		(a)	Verant Replicat									
	mout as also me		tery Mode Sellers Person Research	in Intervisi Paris	🚊 VMs	a construction of the second	red on A er failov		SDDC			
 IB BDC falaiana- IB Date-1 						an	er ranov	CI				4.100
	1, 1, 1 d day, 1 de 1 (1, 1000), 1 o d				844	And in case of the local division of		-	- market	-		
	Contracting FB1 and include parts		2 B Serveral 2	*********	-C. Notes	8258	10.69	4.4				
(2 (24,28)7m)		0	· If terments	terminal (1)	-7 162104	10-05-118	075125-000	-1-15	221148			
> Conten		0	- B Normanits	ture a) (hi	-/ 1974	10-07-02	1012.47 446	-2-16		mage data		
1 - O baselos		0	- di Testimorda	weet 24	1 1000	10.04.08	873.37.465	- 216		11100	<	
A CO Mark Pres		0		terminel Dr.	< 10ml		675,29.40	- 1-1	224.46			
Co Means, Human.			and the second se	termed for	-2 minut		076.24 #8	1.4	08.00			
D arrival		0		100000	1 martia		1010-01-000	216	00.00			
0 waterengist		0		teach-date The	v' Norted		0751346	1.00	10.44			
Of Chieveney				teactured for		10.01.03	172.044	1.4	22.00			
(Freisbergr, 14)		.0		ware in	1 10010		671-68-145	1.4	10.48			
B NO(Point)				inversed (10		10.00.00	1010	1.4				
di matematici				urana) (i)	/ 8/44		100,04,040	14	31-10			
Country or my				used (>	1 10,000		172 21-40	14				
IF COARD AF IP			the second se	terment (c)	- 100 March 1		67232 HB	1.4				
C ACLASSIC WILLIN		8			1 1000	10.01.03	and a loss	10	21.44			
(Farman and the second		1.3	anner .					_				100-0 mg - 8 - 4
Receil Table Astron			(S1)									
r three	Too Served	and a	T Deale	1	idear.	* 200 T	that this	17	Company Inte		him -	
e-10-21-4-14/114	0 weakers	Q-Companies	Presenting lut time taken lating lide		vigh-dild a 22 da i shaaladhoo	0.000	11/10/2012 0-14-84-84		arrent and a local data		a better bein in the cline of the sector in the sector in the	
infacto of car function	D WHERE	- C-Louise	Decempency (1), a Nuclei o		visited by colors, including on	0.000	21/2020 204 44 m		terminaria, brite of A		of the Party of th	
induced with the latest	D WELLE	C Constant	 Neurigang Hud Refine r 		volution (CA) does not the	2.00	100000.000.000.00		straining non-state		to be the family family fields we want to be a set of	
10000	B webbert	() (in second	Neuripung Disa Nation I		CEREMIT COLUMNIES.	2.04	007802503, 9:04 40-04		CONTRACTOR DOTATION		in the first have also be an an and an	
e in studios testes	B weather	O Calasteet	Charactery on the loss of the day		statements in COA, is presented in	2.04	providence a da la ser		University based in an		a before the state of the sector as an extent	
entigent of full manifold	@ webbaik	() Conserved	Rearliping Ofue Inclue o		vighting a prophosisment.	2.49	21/10/2020, 11/10/20 AM		Internet, Park Mar		a before fare (Belli anne in an ann an	
er (h. 4154 Alective	- worker	42 Corporation	Proverting for the rate of the life		vitre of a local strength	1.04	217903033, 8-18, 52 mil		1000000033 \$100-41 A		a ben brit falle pieces an east of	
Infant vital rachte	O WHILE'S	4) Comprise	Recordpoing - Incel Nacione of		+3HOE1COLUMBER	249	01/02/2010 02012 408		OTTOM DE LA DE DE A		a benefit a factor and an an and an	
supplier oppressions	E weated	42 Consume	Secretary musices a		Advectation revealed	2.44	11/10/2010 11/10/21 00		0.0010102 9:09 22 10		 Section and an annual sector sector sector sector sector 	
million of his market	B W/62.414	O Despañse	Security of the first of		VIPER STREET	2.04	DATE NAMES AND ADDRESS OF TAXABLE PARTY.		CONTRACTOR STATES AND ADDRESS OF ADDRESS ADDRE		 And the first of the first sector of the sect	
infante of his market	B WASHES	4) Considered	Becompany Once Markey of Becompany Visio Bachey of		Variable 1004 Scholaster	2.44	Annahanan belelah asa		CONTRACTOR & CO. (5. 4		a perfect to be the first sector of a sector of	
al manual	d weaks	() Canadenee			VENERAL CONTRACTOR	244	surgeon bisition		instanting a bit to a		- best both factor, clin (M) estimates an area over	
in the name	@ farmenth	O familie	Property of the fact stream in		oldheitig a DOA h framework	2.44	strates are a		contacted in the car is		- testing into a local second second second	
an in stat to be	de fariements	O Longent	Property of Tanlas' Street Be		owned to be a summer	1.00	surgery house and		summing some a		of the local distance with the party of the local distance of the	
and the structure of the	(B. Turbunarité	Q Derested	Disease in the last little little		VPERIOR INCOME.	144	straining house and		striken at how the		a barber het internet at and or	
and the state has been as	a laterally	Q Dereman	Financia in the last little for		Variation of the Advancement	1.04	and subscript in the sub-sub-		error 100 h 100 kit h		a barbara tanta (Barbi) antisatan an anal are	Activity Working
		O famores	Incontraction (This Name of						Annual sciences			
white high a state of the	- Defensetti				watered LOOK standards	2.04	1010203-0003-04				to been borth fragment (Bec(M)) used and and any productory	

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

E- Hower Teplca					Vision Backup and Replicati				
Non Falson Falson Falson	Addaction Production To Faddaction Production To Faddaction	theory Under Conurst Hautz rese Fallback Failback Files -	Application Remit 7	Failover Plan *	Properties Access Section 1				
lome	Q Type in an adjustmen	ne in which for	×						
The later	Alaria 🕈	30b hiana	Type	Status'	Crastion Time	Eastore Founda	Gigmil Location	Replica Location	Italloom
- Septication	15 1estVetam22	AVS.20220522, Replot01	Rogular	Fallovor	6/6/2023 3:53 AM	3	a300 vcso75 chods.com/Ouster03	172.30.156.2\Cluster 1	Stativate
ril Teolices	Test/eesm23	AV\$_20230522_Replo601	Regular	Failover	6/6/2023 5/52 AM	4	a300-vcsa05.ehcdc.com/Cluster05	172.30.156.25Ouster-1	V8-twore
C Reaty	TextVeen M	Av5 20230522 Replat01	Sepaler	Failover	6/6/2025 3-32 AM	3	a300-vcsa05 ehedc.com/.Cluster05	172.30.156.2\Quster-1	Whene
Active (19)	Testivecum21	AVE 20210527 Replet01	Rogetar	Fallovat	6/6/2023 7:45 AM	4	2000 eccels shots confiduated	172.30.156.250aster-1	VMware
Falover Flans	Testveran26	AVE.20230522_Replot01	Regular	Fallover	6/6/2023 10,44 AM	1	a500-sesa05 ehods.com/cluster05	172.30.156.2\Quster 1	VMware
Let 24 Hours	TextVicearn27	AV5 20230522 Replob01	Regular	Fallover	6/6/2023 12:19 PM	3	a300-vesa05.ebcds.com/Quster05	172.30.156.2\Guster-1	V8-fivere
3 Success	Tan/Vasiani28	AV5 20210522 Repible1	Reputer	Fallows	6/6/2023 1.07 PM	3	a500-www.5.ehidc.com/Duile03	172.30.156.2\Gusher-1	Webwer
Warning	Testveeun20	AVS_20230522_Replot01	Regular	Failover	6/6/2023 1:16 PM	1	a500 vcsa05 ehods com/Cluster05	172.30.156.2\Cluster-1	VMware
C. Manage	TextVeesm00	AV\$_20230522_Replot01	Segular	Talover	6/6/2023 2:34 PM	3	a300-vcsa05.ehodo.com//Cluster05	172.30.156.2\Quster-1	VMware
	TentVerani31	AVS 76230522 Replob01	Repulse	Falcent	2/31/2023 4-41 AM	1	a500-scsa05 abod: com//Duster01.	172.30.150.25Gaster-1	Videore
	Tactiviscon J2	AVE JUJ20522 Replotert	Rogular	Fallover	6/6/2028 £31 PM	1	ali00-vesu05 official confiduation	172.20.158.2 (Duster 1	VMwarp
	TestVeesm23	AVS 20230522 Replot01	Regular	Failover	6/6/2023 3:31 PM	4	a300-vcsa05.ebcdc.com/Cluster05	172.00.156.2\Ouster-1	Vittania
	TextVeesm04	AV5 20230522 Replat01	Regular	Failover	6/6/2023 4-31 PM	4	a500-vcsa05.ekcdc.comt/Duster05	172.30.156.2\Cluster-1	Victoria
	Tellwayn11	Avs 20230322 Replat01	Regular	Failowet	6/6/2028 5:30 PM	5	a500-vision afrode com//Oustat03	172.30.156.2 (dustar-1	Videore
	S WinSQL401	AVS 20230522 Reolpt01	Segular	Failover	6/6/2023 6 52 AM	5	a300-vcsa05.ehodc.com//Cluster05	172.30.156.2\Cluster-1	Vôdware
	WinSOL/102	AV5 20230522 Replat01	Repular	Failover	6/7/2023 6:11 AM	3	a300-vesa05 ehede.com/Guster05	172.30.156.2\Guster-1	VMware
A Home	WVSC/401	AVS 20210522 Replicit@1	Fergilar	Fallows	6/7/2023 12:28 AM	1	20m water and a constant of the	172.30.156.25Cluster-1	Webser
T	WinSCk404	AVS 20220522 Replot01	Regular	Failover	6/6/2023 6 29 PM	3	a300 visia05 effects com/Ouster05	172.20.156.2\Guster-1	VMware
E Inventory	WinSOL405	AV5_20230522_Replot01	Regular	Fallover	6/6/2023 7:50 AM	3	a300-vçsa05 ehodo.com/Quster05	172.30.156.2\Custer-1	Stidwore
🔮 Backup leftactructure									
Storage Infrastructure									
Tape Infractigueture									
(P) Hits									
D ₆									



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:

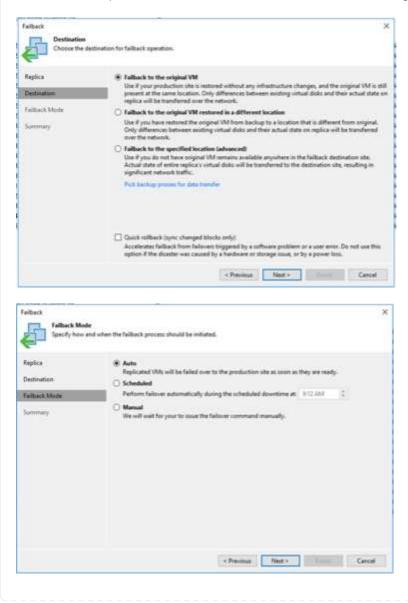
 Failback to production - switch back to the original VM and transfer all changes that took place while the VM replica was running to the original VM.



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.



Replice	Replices to failback								
	Name	See	Orig	inal location		(A)	Select All		
Destination:	[3. Tetherada	EST MR		events make	_TIIma				
Faillack Mode	TertVeens23	012140		0-separation about co			Clear All		
PRODUCT, MADDA	Contestineer22	75.4 MB	(#70	0-year/05 afterfic o	am]]T_		Populate		
Sammary	Testileam 30	06.8.149	(+30						
	E Testiesamil	857MB	15.748 [a30-vesa05.ehods.com]{7., 1.5.68 [a300-vesa05.ehods.com][Fs.,						
	E WinSQL42								
	Contestineer 25	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	81.2 MB (a00-vca85 ahotic.com) (T_						
	E Pastikeenski	\$1.7 MB		0-veskl5.ehesk.o					
	E in Test lesamil	96.4 MB		0-vesilit.eholo.o					
	E West Att	1.8.08		0-vesal5.ehude.o					
	E Terfilesamili	85.3 MB		D-vesal3 etcals.c					
	Contenant Convertexes	88.3 MB 1.6-58		E-vesal5.ahodc.o					
	Con WebGLAD	13.08	10.00	0-ves#05.ehede.o 0-ves#05.ehede.o					
	Entimen 3	812MB		e-results incode a E-results incode a					
	El Tettisean27	77.6 MB		0-vcs#05.ehcdc.o					
	2 Testiveanit			0-vesal5 medice					
Summary		1000		Net	in the second		Cancel		
Summary	it settings, and click Finish to start failly	ch operation. You o			back proces	s f m			
Summary Review failtai		ch operation. You o	-114		tack proce	ss # re			
Summary Review failting	ik settings, and click Finish to start failler Summary: Bill name TatVinsen21	al operation. You o	-		Lack proce	u f re			
Summary Review failbat opfica	Summary	al spectro. Yes			tack proce	st # re			
Summary Review failten optica estimation	Summary: \$14 name TettVreen28	ek spendion. Two			tack proce	a f re			
spica estinution sback Mode	Summary: BM name: TetVision28 VM name: TetVision23	ck spectro. To a	dbe		lack price	st # rm	2		
Summary Revee failter aptica lestinution alback Mode	Summay Still name: TettVesan21 VM name: TettVesan21 VM name: TettVesan21	ch spectro. To u	dbe		tack proce	as if re			
Summary Revee failter aptica lestinution alback Mode	Summary Stit name: TettVisian21 VM name: TettVisian21 VM name: TettVisian21 VM name: TettVisian21 VM name: TettVisian21	ch spectro. Too o	al be		tack proces	s i re	2		
Summary Revee failter aptica lestinution alback Mode	Summary Dit rame TetlVean21 Wit rame TetlVean21 Wit rame TetlVean22 Wit rame TetlVean30 Wit rame TetlVean32	ek specifics. You	dbe		teck proce	55 # re	2		
Summary Revee failter aptica lestinution alback Mode	Summary Oth name: TettVision28 VM name: TettVision28 VM name: TettVision28 VM name: TettVision28 VM name: TettVision282 VM name: WisSC2.822	et spection. You	dbe		teck proce		2		
Summary Revee failter Applica Jestinution alback Mode	Summary Mit name: TettVeeen28 Wit name: TettVeeen28 Wit name: TettVeeen20 Wit name: TettVeeen20 Wit name: TettVeeen22 Wit name: TettVeeen23	ek spection. You	dbe		teck proce	11. F 19	2		
Summary Revee failter Applica Jestinution alback Mode	Summary Mit name: TettVesen20 Wit name: TettVesen20 Wit name: TettVesen20 Wit name: TettVesen20 Wit name: TettVesen22 Wit name: TettVesen23 Wit name: TettVesen24	ek operation. You u	off be		teck proce	15 F 19	2		
	Summary PM name: TettVesen20 VM name: TettVesen20 VM name: TettVesen20 VM name: TettVesen22 VM name: TettVesen22 VM name: TettVesen23 VM name: TettVesen24 VM name: TettVesen24 VM name: TettVesen24		dbe		teck proce	5 F 10	2		

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.

Andrew Parlies		Solar Consult Indust Tables	ation J	All for an and a second								
and a second	Q been in on shired re-	net by particular for	X									
Se Me ∰ Replace ∰ Replace Service Facebook ∰ Replace ∰ Replace ∰ Service ∰ Serv	Tarret	201 Turon 447, 201322, Japaniol 7, 447, 20132, Japaniol 7, 447, 20142, Japani 7, 447, 20142, Japaniol 7, 447, 2014	Tere Repub R	Status 7 Calasis Calasis Calasis Salasis Salasis Calasis Calasis Calasis Calasis Calasis Calasis Calasis Calasis Calasis Calasis Calasis Calasis Calasis Calasis Calasis Calasis Calasis Calasis Calasis	Container Time Bint Groups (Bint Alak) Bint Groups (Bint Alak) Bint Groups (Bint Alak) Bint Groups (Bint Bink) Bint Groups (Bink) Bint Group	Party Flore 	Corporations in a constraint of the second s	Equipa Location 173.55 (1942) Orami-1 173.55 (1942) Orami-1	Partiese Oblasse	日本 二日の 二日日	Allow ins., Parent lines, Allow to geodotine, Convert folked Soft fallers Definition Return good file; Return good file; Return good file; Return good file; Anone good file; Anone good file; Anone good file; Anone good file; Anone fil	•

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

	4 (2) VeeamTest (acros Summay Monitor Configur		e Pools VMs						
 S a000-ecuel1.atex.com B a000-0001 Comerciti 	Victual Machines Viel Familian	na interes						Sector 1	
a000-esx09 mode cum	D) I was	2011 Marc	Bielos .	history	Unit fame -	Heir O'U	Intel New 1		
alloo-existo enullication	C) / /D text/rearch	Powered On	V horna	16-08	560.2 MS	010	408.140		
 (2) HOBERT, 2001 (3) HOBERT, 2002 	1 1 1 1 1 two manuars 22.	Powered On	V North	16.58	1014 103 548	0.40	543146		
 O HOBERD_DOCE O HOBERD_D001 	C) + (# TestVeen23	Powersd On	V Normal	N CE	878.89.148	070	341 HB		
O Vecanite	C = (2 TestVeeun34	Powered On	V Normal	10.08	874.4348	010	340 MB		
(if Textmeterizt	O 1 Y d Testveurs3	Powerse On	V.Wetter	10.0E	890.27 ME	019	337.648		
12 Testivetari22	C) : (2 terrveenot	Powerad On	V Normal	16-Q8	876.8 MS	0 Pit	338 Hell		
68 Testimeart23	C + d techeardt	Powersd O1	- Normal	16.08	874.45 MB	010	342.948		
(B Testiverani34	C) + dt textwoards	Powered On	V Nortal	10.08	875.12 HB	0.42	202.440		
(2 featureari2)	C) / (2 Serverance)	Powered Dis	- Normal	16.08	87254 MB	0.10	340 MS		
(# Technologia	C) / C Testuman00	Powered On	V tional	16.08	87129 MB	0.142	300 MB		
20 Textrolears27	C) - (2 Testymental)	Powerad On	U Normal	16.08	882.02 MB	- Ó Fill	343.66		
12 Testviniari28	C) / (2 testilevent2	Powered O6	V Normal	NO COR	\$75.34 HE	0.40	123 MB		
(D Textylearn29)	C 1 3 tertviewenth	Powered On	V Normal	No Gill	872 07 ME	0.Hg	227 640		
(# testveeenbb	Ci + (2 testveam34	Powered On	V. Normal	16.08	670.35 ME	010	200.040		
(2) Yestveeen20	CLUE (# Settlement)	Powered Dh	V Normal	16:08	877.62 MB	0 mg	228.160		
in Textuments	C + D WINGLASS	Powered OT	- Nortal		20.82.08	O HU	0.8		
(2. fest/maril)	() + (0 WY90x402	Powered Off	- Normal	308.22.08	20.43.08	0.0142	.08		
12 Textheored4	C) / (2 West 0.403	Powered On		300.01.08	20,51 GB	031400	2.04.08		
(2 Testivearcili	C (1, 1) 10-10,004	President Off	- Normal		2242.08	OHD	0.8		
(2) Wellox.4co	() + (0 mmo.ett	Powersd OT	V Norma		34.34.00	010	0.0		
(# Westx.402 (# Westx.403	C) = (2 WW0.000	Powered On	V Normal		19.9 08	214 1410	W 88 (A)		
B WessCubb B WessCubb B WessCubb d WessCubb d texture d									
10 Lastavinos 10 Lastavinos									
28 California	U Cercer							paula tau teleta 🛛 📰	1.1

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

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.

Author(s): NetApp Solutions Engineering

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

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

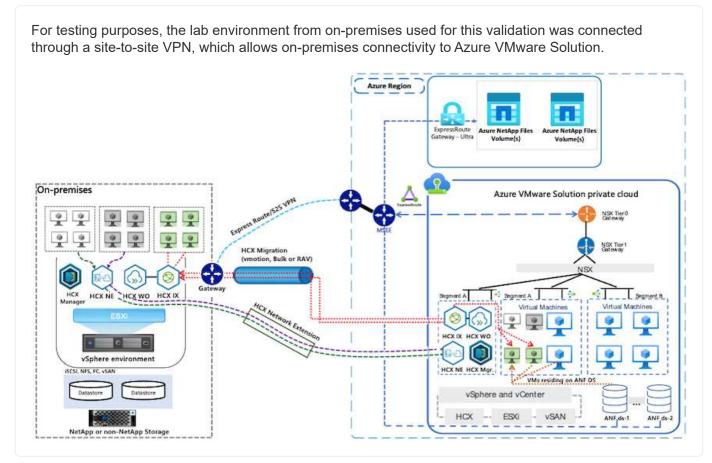
Before you begin, make sure the following prerequisites are met. For more information, see this link. After the prerequisites, including connectivity, are in place, configure and activate HCX by generating the license key from the Azure VMware Solution portal. After the OVA installer is downloaded, proceed 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

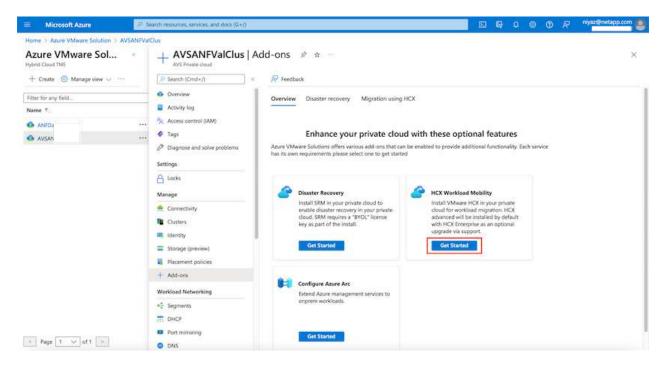


Solution Deployment

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.



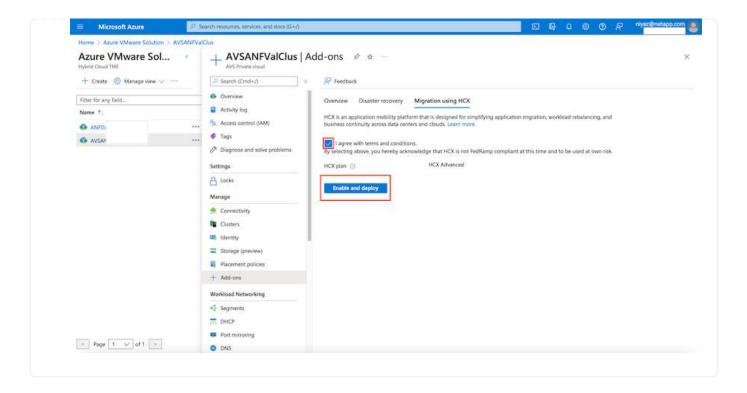
4. Select the I Agree with Terms and Conditions option and click Enable and Deploy.



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



The deployment takes approximately 25 to 30 minutes.



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.

E Microsoft Azure	earch resources, services, and docs (G+/)				9 @ 0 R	niyaz@netapp.com
 Microsoft Azure Home > Azure VMware Solution > A Azure VMware Solution > A Hybrid Goud TM + Create @ Manage view < ··· Filter for any field Name 1. @ AM# ··· @ AW\$ ··· 	ANFDataClus Add-or AVS Private doud Search (Cmd+/) Coverview Activity log Access control (IAM) Tags Connectivity Clusters I Identity Storage (preview) Storage (preview) Placement policies Add-ors Workload Networking	Feedback Overview Disaster recovery HCX is an application mobility platfor business continuity across data center HCX plan: 1. Configure HCX appliance Using the IP address below launch and deploy on the site where source HCX Cloud Manager IP: 2. Connect with on-premise u	HCX Advanced the HCX portal. Download HCX applian ce vCenter environment is running. Lear https://172 using HCX keys : Connector appliance on-premises and Learn more.	ion migration, workload nce (OVA file) from Ad	f rebalancing, and, ininstration page	niyaz@netapp.com
< Page 1 v of 1 >	Segments T DHCP Port mirroring	testmig	40DD435CB2F940EF841CF41	Consumed		

2. 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 onpremises vCenter Server.

							đ	18 1 6	
m VMware HCX							C	@~ =~	cloudadmi
Dashboard Infrastructure Site Pairing Sinterconnect Services Compute Network Extension Migration Disaster Recovery	System Upp Pair your remote di Code HCX Code CC Pair Pair Pair Pair Pair Pair Pair Pair	ata center with VMware HCX-							
Administration	Current. Version	System Name	τ.	Status	Info	System т Type	NSX Version T	VC Version T	Copy To Clipboard
Audit Logs Activity Logs DICE	○ E4330	hcx. Cloud	WS BILLING CO.		3	HCX Ooud	312.0.017883600	7.0.3 19234570	9
© Support								Nunt	or of Applance
	+ III Remote HCX								
	Current Version	System Name	τ Status	info		System Type	7	Copy To Clipboard	
				8					
								Number	inf Appliances (

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

	MI A300-Cluste	erOI Excesses	-
	Deploy OVF Template	Select an OVF template ×	
- B AND-ONICH	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.	HTM.
12 4300 er	 Select a name and folder Select a compute resource 	O URL	
∏ #300-ex > G #3#_Hc	4 - Review details	Local file	
1 G ANFON	5. Select storage	UPLOAD FILES VMWare-HCX-Connector-4: ova	
 G AVSANF G HOLDH 	 Ready to complete : 		
(2 HO). (2 HO).			
(B ++0), (B ++0),			
(2 HO); (5 HO);			
(D HOX		CANCEL NEXT	
(B HOUS /B HOUS	The second		8 4 1 1 14

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

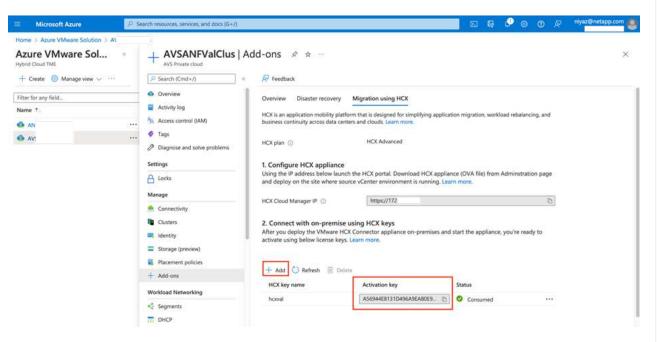


Power on the virtual appliance manually.

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.





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

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



Use the password defined during the OVA deployment.

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



The on-premises HCX Connector should have internet access.

- 5. Under **Datacenter Location**, provide the nearest location for installing the VMware HCX Manager onpremises. Click **Continue**.
- 6. Under System Name, update the name and click Continue.
- 7. Click Yes, Continue.
- 8. Under **Connect your vCenter**, provide the fully qualified domain name (FQDN) or IP address of vCenter Server and the appropriate credentials and click **Continue**.



Use the FQDN to avoid connectivity issues later.

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

Continue.



Enter the VMware vCenter Server FQDN or IP address.

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



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

vm HCX Manager	Dashboard	e//172.21.254.157:9443/hcc-n Appliance Summary	Configuration	Administration			ប់ 7221254157	Version: 4410	admin
• VMware-HCX FODN: IP Address: Version: Uptime: Current Time:	VMware-HCX-440 172.2 4.4.1.0 20 days, 21 hours		c		0 0	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-vcs	a01.ehcdc.com	0.04	SO ttps://a300-vcsa01.ehcdc.c	om		
MANAGE			MANAGE		1	ANAGE			

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.

ventories											
([])	圈		Ø	11		ంర్రం	п	Þ	1	٢	
Hosts and Clusters	VMs and Templates	Storage	Networking	Content Libraries	Global Inventory Lists	Workload Management	SnapCenter Plug-in for VMware VSphere	Cloud Provider Migration	Site Recovery	нсх	
Monitoring											
圁		Ē.	R	Es	\diamond	п					
Task Console	Event Console	VM Customization 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.

e → Q	08=0	▶ https://ø300-vcsa01	ehcdc.com/ui/hpp/blugi	/com.vmware.hybridity/com.vmware.hcv	sitePairing		合	0 1
⊒ vSphere Client (
HCX Contractions	< s	Site Pairing					C ADD A SIT	DAUDROS
C Sch Paines Si stereoscent Is Transport America Services Notivore Extension Magazilon Di Disatter Secowry System	~	St Diver	Connect to F Remote HCX URL Username	https://172. cloudadmin@vsphere.local	× © ©	avs.asuro.com-		
de Armenstration O fuccion		Carl Constant	Password	CANC	EL CONNECT			

1. Click Connect.

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 Pai	ing .				
~ <u> </u>					TE PAIRING
×	VMware-HCX-440 Phttps://72.21254.157.443 Rateigh 1 Interconnect(5)	→	<pre> hcx.8ebf3b0b7ddf4cc08e3f85.westeurope.avs.azure cloud</pre>	.com-	
v EDIT C	ONNECTION DISCONNECT	÷	HCX Ø nttps Ø us w		
	× EDIT C	✓ VMware-HCX-440 Øntps://172.21254.157.443 ©Raleign 1interconnect(s) EDIT CONNECTION DISCONNECT Ø WMware-HCX-440 @https://172.21254.157.443	✓ VMware-HCX-440 →	 ✓ VMware-HCX-440 → ^O https://172.21254.157.443 ^O Raieigh ^O Raieigh ^O https://172.30.156.9 ^O Amsterdam ^O https://172.30.156.9 ^O Amsterdam ^O https://172.21.254.157.443 ^O Amsterdam ^O https://172.21.254.157.443 ^O Amsterdam ^O https://172.21.254.157.443 ^O Amsterdam ^O https://172.21.254.157.443 ^O https://172.41.257.457 ^O https://172.41.254.157.443 ^O https://172.41.257.457	 ✓ VMware-HCX-440 → ^(a) https://172.21254.157.443 https://172.30.3156.9 ^(b) Amsterdiam. Interconnect(s) EDIT CONNECTION DISCONNECT Ø https://172.21254.157.443 Ø https ^(b) HCX ^(b) HCX ^(b) HCX ^(b) HCX ^(b) Raleigh Ø https.//172.21254.157.443 Ø https

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	08=	3 0+ https://a300-vcsa01.ehodc.com/ui/app/blug	in/com.vmware.hybridity/com.vmware.hc	x/lybridConnect	Ŷ		. ₪
$\equiv~$ vSphere Client $~$ Q				C	S Administrator@EHCDC.COM >	٢	0
HCX Dashboard Infrastructure Ste Paining Interconnect C Transport Analytics Services Network Extension Service Seturator Receivery	~	Interconnect Multi-State Dervice Mean Compute Profiles Service Mean Network P hcxdemo hcxdemo Host a000-ess/01 ancid: com/do frost 20202 Host a000-ess/01 ancid: com/do frost 20202 Host a000-ess/01 ancid: com/do frost 2020	in in critical (red) state for service compute		Q. C CREATE COMP	PUTE PRO	DFILE
System	*	A300-VELAG Lehods.com A300-VELAG Lehods.com A300-Cluster01 HCK Senters (a) (a) (a) (a) (a) (a) (a) (a) (a) (a)	Ceptoynees Container Ca300-vosa01.ehcdc.com Ca4300-Cluster01 Detestore CauMomory Reservations CauMomory Reservations CauMomory Reservations CauMomory Reservations CauMomory Reservations CauMomory Reservations	Networks ØVM_3510 (Management) (Some Network Container (Network Entension A) @ VDS-Switch0 (Unternited)	es la	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 Site Pairing	~	Multi-Site Service Mesh	Network Profiles Senti	net Management						
E 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	ыты 9000	IP Pools IP Ranges 172.21.254.80 - 172.21.254.95	IP Usage(UseduTotal) 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 =	Por. https://s300-vcsa01.ehodc.com/ui/app/plugin/com/vmware.hybridity/com/vmware.hcs.hybridConnect		\$	1	⊚ ≡
\equiv vSphere Client (<u>م</u>		C	Administrator@EHCDC.COM ≻	٢	0.
HCX Dashboard Intrastructure Stite Pairing Interconnect E Transport Analytics	*	Interconnect Multi-Ste Service Mesh Compute Profiles Service Mesh Network Profiles Service Management			E MESH	Ŷ
Services Potencial Content Potencial Content Pot	*	INccoo7 New version for service meth applances is available: Click on Update Applances to Upgrade to latest. Size Paring IV VM wave- HCX-440 Cloud Rainigh IV VM wave- HCX-440 Cloud Rainigh IV VM wave- View APPLIANCES Reserved VIEW APPLIANCES Resynce EDIT DELETE UPDATE APPLIANCES MORE -	Q	X Server	×	

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.

CONTRACTOR			v//a300-vcsa01. ehcdc.com /ui/app/plugin/com.vmv						Contract of the second		
viphere Client Q									C 2		
efficient Invities		iterconr santese									
An Parried Reserved	-		· · · · · · · · · · · · · · · · · · ·							CON SERVICE	
Tampert Arwytice		Atamp									_
ati ativo's Extension	1 I I I		of Contained Contractories (Contained and								5
Agention			Applete Series 1. 1	Assessed Type: 1			Turnet Ballio	Darrest Wester	A service revealed		
isader Recovery m Annocatalian Lagarri	*	0.1	00007-0-6 w 1959-99-0-026-470-0000 00006-66008e homework 42000_07F1_00004	80 -Cr 0000			۲	443.0	4410		
		0.2	COUT HE // we UPINE NOT-SATE ALL'ENTERCONCE Commany: ADD/COUTEON Temper, ADD/AFL_2004 Methianic (Instance' -05-SH100) Entermain Methianica (Int	€9 ≪เส⊺¢∂	722.0+K		۲	6428	**** 100		
			COOST MID-6 W_ 0405774D-056-Assis ambriedDatesc/Dot Kinneys X200_0775_0004 Miness X200_075_0004	(a) -compose				1110	NA .		
											y name
		Applano Applano			ne 7 der TCI dagi in	er Julium 172 Million IV (annum ann) 172 Million Jack (annum 1				6400	
		60007 H	1.0		ICONT DIT					48.0	ņ
		XCODOT W								22.61	

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**.

e → C	V La	https://a300-vcsa01.ehodc.com/ui/app	1 pring / 1/3300	and a second	ang sounds		and the second sec	_	습		⊚ ±
\equiv vSphere Client C	٤.							C A	Administrator@EHK		9 (
CX Dashboard Infrastructure	<	Migration		12 MIGRATE		(e)				(Selection	
elo interconnect.		Name	VI	Ma/ Storage/ N	tempry/ CPU	5	Progress	Start	End	Status	
C Transport Analytics											
Phetwork Extension	~										
Migration Disaster Recovery		✓ ■a300-vcsa01.ehcdc.c	om →	2	N9830						
ystem		> 2022-09-26 09:00 FLJVU		1 20			O Migration Complete	2	÷.		
& Administration		> 2022-09-26 08:35 EXMTM		1 20	8 2.69	1	Migration Complete		2		
@ Support		> 2022-09-18 16:21 ERC20	B 1000	2 40	8 408	2	@ Draft	S.	- K		
		> MG-18cbce94/Sep 16	and (Self)	5 10 0	8 10 GB	.6	Migration Complete	12:44 Au Sec 10	2		
		> MG-04abdeell / Sep 16	THE DAY	1 20	8 2.69	1	Migration Complete	12.25.468 Beg 10	5		
		> MG-ef7374dd / Sep 16	<u>-</u> 103	1 20	8 2.68	1	Migration Complete	12:11 Axs Bep 18	8		
		> MG-d2of93ef / Sep 14		5 100	8 10 08	5	O lagration Complete	02.05 mm Sep 14	÷		
		> MG-99fecac8 / Sep 14	tax corp	1 20	8/ 208	1	() Migration Complète	11.02 AM Sep 14	×		
		> MG-548618cb / Sep 14	teer Coly	1 20	8 2.08	1	Stagration Complete	10.04 AM Sec 14	*		
		> MG-dd475274 / Sep 12	aut Only)	2 40	9/ 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			- <u>P</u>
Ouster-1	Datasbur02 (((1)(1)(1)))	9	Bok Migration	÷
C) (Soecity Destination Follow)	Same format as source	÷.	(Cobonal Switchover Schedule)	Ø
Switchover:				
 Extended Options: 				
Statement and a statement				
(Providence) (Providence)				
Gen Dimond Darmer (Serium MAC)				
Constitution	Opik / Memory / vCPU		Migration linto	0
Constitution	014 / Memory / vCPU		Migration Info	<u>a</u> .
/W for Higration				<u>e</u> .
M for Migration 3 Demo, HCX, BulkOl	0 2.08 2.08 1V0PU		Bulk Migration	ē.
M for Migration 3 Demo_HCX_Build1 3 Demo_HCX_Build2	0 2.08 2.08 1VCPU 0 2.08 2.08 1VCPU		Bulk Migration Bulk Migration	ð

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

+ + C	0.6	A st report	105 mil	in sheddam/	Applitup-Jam.	mage spirities	n ermane hi	or granter	de :								位	0	*
😑 vSphere Client	Q															C	& American American Contraction	- @	۲
Vapare Can Con Vapare Can Vapare Can Vapare Can Vapare Can Vapare Vapare Can Vapare Vapare Can Vapare Vapare		 Hispating alj00.v Parrie H Parrie H Parrie H 	csa01 ehcdic co K, Selots galectic cov galectic cov galectic cov	(7 HEIXX11 m → - + 172.30	30mpc	68)	2 GB 1 2 GB 1 2 GB 1 2 GB 1	NYE Rogense Magning Magning Magning Magning Magning				Start	e End		Safus ; ;	8			
			50 50	Demo_HC	-96-00.004 -96-00.004			68	2 GB 4 2 GB 1 2 GB 3	Warstong				544 14 2:05 PM 627 Big 14 2:05 PM 627 Big 14 TT 62 AM 621	11.12 AM 831		belchover started belchover started Agridian competed		
v Becent Tasks	Jarma		L	A C Associate	ARRING TON									The 14	Big N				_
	Target		÷	Status		Getals		ninte		÷	Donund For	× .	lat line	. *	Completion Time		Server		,
hik Mgrabon	(D. Dens,	HOC BLADS -		1.0	245.0	Traisler Started		Ame	strator (10	HODGIOOM	0.01	0	0/14/2022	1.2.05 TLPM			hybristy-manager		
luis Migration	(D. Dente	HOK,BARD			01.0	Transfer Started		Admir	00000	HODGOOM	0.755	10	\$654/2022	2.0311.994			hybrioty-manager		
luk Mgration	D Denis	HCK_BUHCE			0.40	Transfer Started		Ame	11110101010	HEDCION	0.710	- 18	0/14/2022	20511944			hybridity-manager		
luk Migration	(2 cane	HCK_BAROS			55.0	Transfer Martell		Admin	sealarpe	HERE COM	0.946	4	9/14/2022	2.2511264			hybridly-manager		
Buik Migration	(D. Dens	HOK BARDE		-	225 0	Transfer Started		Ame	abilities (BK)	HODC COM	0.00	-	W/W/2022	2011294			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.

(i)

e + 0 0	A # House	interna spartnerski Daladi	endetatory 2543	673x56k3-1000-4345	NO1-0540524	Weingtone -			\$	0	2 1
= vSphere Clent Q								c			
, 0 8 8 0	DatastoreO2 Action	Permissions Files	Hosts VHs								
 Velaversecutionnic colorer. 	Victor Hathing VM Templates]									
 O vc.betratos.fouri/ccdbetr. EE sobc-betacenter 	Victual Hackines VM Templates VMs on AMF datastore after might	J.	_						× <u>0</u>	NO. HOR. H	
O ve bestable fastile cobets O ve bestable fastile cobets O ve bestable fastile cobets	Hale was a set of the	J.		Produced Space	Unit Raws	must CPU	Paul Mars /		. <u></u>	11.10X.1	
vic betracos/outliceobyor. El socio-betranere ordenoseco el anor	VMs on ANF datastore after might	ation	- Steen		Unit Name 246,87 MB	Peet ON 0 HQ	Head March /		* <u>0</u> *	no.HCK.J	
Vot bebrittottut fauthik cobkott B SODO-Detacenter Detamotreco	VMs on ANF datastore after mign	ation stee	and the second se	2.08					+ <u>0</u>	n.HOLI	
vic betracos/outliceobyor. El socio-betranere ordenoseco el anor	VMs on ANF datastore after mign	3 alton 8 Mile Powerket On	V Nortal	3 G8	245.87 MB	0 14	264.940		* <u>0</u>	nu ocul	
Ore of the second service of the second service of the second service of the second seco	VMs on ANF datastore after regn	J ation	v Nornal v Nornal	2.08 3.08 3.08	746.87 MB 751.24 MB	0 HQ 0 HQ	264.MB 280.MB		, t <u>or</u>	ne, HOLI	

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 6 =	https://www.	Of an advances of the second sec	-	enal a hybridget and	114414-000	reputered	0							\$		\$ 1
😑 🛛 vSphere Client	à													C		0	
KX 3 bankows ntastratus ⊘ tas Farrej & therminat		-	gration Tracking Elistanus 3 Milliotecover	emart	27 Million P		tt. C	ARC	ns.] Pagess			Start	. Del	-	Tabu	31	
IC: Transport Analytics analogs		~															
 balance Echeropol Morabah 																	
19 Disaster Recovery			 a300-vesa01el bena HCK VMater 	-	m -> 172.30.1	-	03 2.0		Mark Room States		0 +1m as see	11.52 ++ 10*		_	Addrest Transfer bi Program		
de Admentistion			Down NCK Could				Ci 20		O My share Car			They be TO DO AN UP !!	1215 444 827		Margare revenue		
Chargeort		1.1	4.V. et an and a second se	200	-							Deg 74	San 14				
		1	> MCX_Photos_47	and in the	-	-	09 2.0	1	O Myrahen Dirf	27ele		1223 PR(807 Inc 12	12:31 Person (hep-to)	12.000	logation completed		
		1	S HOL PROBE IN		-		15 80	1.1	OMpatien Cor	and a		12.25 Pec 807	1235-44807 Ber 12		Notice comprise		
			. MX.75080.15		-		0 20	1.1	C) Mightein Com	ciele .		1217 10221	12.54 Parent	Print 1	Maratim proprietad -		
												940-0	944.72				
		1	3 > #0,0000.38	-	6	e	68) 2.0		@ Mgratios Opr	Crew .		12.01 (Heat) (Heat 1)	12:57 Hantstill Sec 19	7.400	Wardon completed		
Recent Tasks	larms																
	farget		5564	+ 10	prom-	*	adutor.		*	Gueses . *	Start Type		Comparison Type		tener		
nik Rummi 🛛 🐨			Comparied	Excentiguing Vytual Marts.				wistialur	5.85	09/14/2022 10:5717				AM ADD-vctactietunc.com			
	(D Dame HCK)	VMattalan	Construction and	C Comparied								28/54/2023, 30 59 58 AM					
configure vertail mach.	(B Dens, HCK, (B Dens, HCK,						EHEDC CO	10.55	nonisit) altern	4.764	09/54/20	03,103958	28/56/2022.30.31	158 AM	allog-witable animit down		
est Rame *		Witten					EHEDC CO			6766		02, 10 3 8 58 02, 11 13 33 .	06/4/2022 ±03		e300-visadi etuzi com a00-visadi etuzi com		

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

HCX vMotion

i.

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

Learn more about the the Global Region support for Azure, AVS and ANF.



NFS datastore will be available in regions where both services (AVS and ANF) are available.

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

- Check the availability of AVS and ANF here.
- Check the availability of the ANF supplemental NFS datastore here.

Copyright information

Copyright © 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.