

Protecting Workloads on Azure / AVS

NetApp Solutions

NetApp May 17, 2024

This PDF was generated from https://docs.netapp.com/us-en/netapp-solutions/ehc/azure-native-dr-jetstream.html on May 17, 2024. Always check docs.netapp.com for the latest.

Table of Contents

Protecting Workloads on Azure / AVS	1
Disaster Recovery with ANF and JetStream	1
Disaster Recovery with CVO and AVS (guest-connected storage)	13
TR-4955: Disaster Recovery with Azure NetApp Files (ANF) and Azure VMware Solution (AVS)	39
Using Veeam Replication and Azure NetApp Files datastore for disaster recovery to Azure VMware	
Solution	53

Protecting Workloads on Azure / AVS

Disaster Recovery with ANF and JetStream

Disaster recovery to cloud is a resilient and cost-effective way of protecting the workloads against site outages and data corruption events (for example, ransomware). Using the VMware VAIO framework, on-premises VMware workloads can be replicated to Azure Blob storage and recovered, enabling minimal or close to no data loss and near-zero RTO.

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

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

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

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

CPT performs the following functions:

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



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

Install JetStream DR in On-Premises Datacenter

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

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

vm vSphere Client	Menu 🗸 🛛 🔍 Search in al	environments	C () × Administrator@EHCDC.COM × ()
Image: Constraint of the second sec	Magazia A300-DataCent	er ACTIONS figure 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 Configurations Task	(É
a300-esxi03.eh	Network Protocol Pr	Site Details	Alarm Settings
a300-esxi05.eh	JetStream DR	vCenter Server Hostname 172 21 253 160	
ANFJSDR-MSA0		Management Appliance Hostname ANFJSDR-msa	
AuctionAppA0		Software Version 4.0.0.443	
🔂 AuctionAppA2		Subscription ID 0000000-0000-0000-0000-00000000000 0	Configure
🔂 AuctionAppA3		Tenant ID / Application ID - Configure	
AuctionAppB0		Application Secret + Configure	

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

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

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

Protected Domains Statistics Storage Sites Add Storage Site Image Site Image Site Add Storage Site Image Site Image Add Storage Site Image Site Type * Image Site Type * No Storage Site configured. Access Type * Image Site Site Site Access Type * Key Access Image Site Site Site Site Site Site Site Sit	c
★ Add Storage Site Storage Site Type * Name ▲ ▲ No Storage Site configured ▲ Access Type * ▲ Key Access ▼ Storage Site Name (Provide a name to identify this Site) * ▲ ANFDemoblobrepo ▲	c
+ Add Storage Site	C
Name Azure Blob Storage No Storage Site configured. Access Type* Key Access Storage Site Name (Provide a name to identify this Site)* ANFDemoblobrepo ANFDemoblobrepo 	
Access Type * Key Access Storage Site Name (Provide a name to identify this Site) * ANFDemoblobrepo	
Key Access.	
ANFDemoblobrepo	
ANFDemoblobrepo	
AN ANY PRESS AND	
Storage Site Details Alarms	
Acure 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.

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

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

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

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

elect Protected Domain:	Create Protected Domain			+	Create E More
	•				
	1. General 2. Pri	imary Site 3	. Summary		
		111		^	
	Protected Domain Name	ANFPD001			
	Priority Level (Optional)	1			
	Total estimated data size to be protected	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	Create		

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.

Recoverable / Total VMs Protection Mode for seleded VMs Write-Back(VMDK) ✓ Q ANFDemobiobrepo ANFDemobiobrepo AL (172.21.253.160) 0-DataCenter \ A300-Cluster Current RPO Q AuctionAppB1	<u>Edit</u> Detai
WIN Name # of Disks Protection Mode ANFDemoblobrepo Current RPO 1 X D-DataCenter \ A300-Cluster	
Remaining Background Data 1 > 0-DataCenter \ A300-Cluster Current RPO AuctionAppA1 1 Write-Back(VMDK) >	
Current RPO	
✓ AuctionAppB1 1 Write-Back(VMDK) ✓	
Protected VMs Settings Ala AuctionDB1 2 Write-Back(VMDK) V	
AuctionLB1 1 Write-Back(VMDK) V	
+ Start Protection Stop Protection AuctionMSQ1 1 Write-Back(VMDK) V	Q
AuctionNoSQL1 2 Write-Back(VMDK) V	
VM Name A AuctionWebA1 1 Write-Back(VMDK) V	
No VM is protected. Virite-Back(VMDK) V	
Client1 1 Write-Back(VMDK)	

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



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

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

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

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



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

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

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

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



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

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

Microsoft Azure	30 Seathmeniden. a	verae, and door.15+A	EI E 🖓 🖓 🗇 🖓 niyazilmetapp.com
Home > ANFDataDus			Run command - Install-JetDRWithDHCP ×
ANFDataClus Ru	n command —		This top level Cristel Downloads JetCh bundle from MMS, creates a new user, assigns
P Search (Ch1+/)	🔿 Refrish 🔗 Foodback		elevated provideges to the user, deploys JetDr Management Server Appliance/MSA), registers vCenter to the JetDr MSA, configures cluster.
 Access control (UM) Tras 	Peckages Run execution status		Command parameters
 Diagnose and solve problems 	 Name 	Description	RegisterWorkp ()
Settings	V KOConfiguration 224 Research Marca	An endporter of Administration and Ad. Sec <u>address Schemening</u> for sumor	ProtectedCluster * ()
A Loda	Druttle-letORforChater	This Condiet unconfigures a cluster but doesn't uninstall JetDR completely so other doubers	Outer-1
D 1004		polos.	Datastore * (j)
Manage	Unable-JetDNI orCluster	This Cristlet configures an additional cluster for protection. It installs vibs to all hosts in the	viseCatastore
A Connectivity	Install-SetOff-MethDE4CP	This top level Gridlet Downloads JetDr bundle from MMS, creates a new user, assigns elevi	VMName* ()
Chatters		registers vCenter to the JetDr MSA, comfigures chaster.	antipival-msa Okuttw.* (C)
Identity	treature-sector/sectors.com	This top level Cristlet Downloads JerDr bundle from MMS, orestes a new user, assigns elevi- registers vCenter to the JerDr MSA, configures cluster:	Deare-1
Storage (perview)	Involve Prefight int DRmstall	This Creditet shedes and doplays current state of the system it checks whether the minimal	- Ordential (i)
Racement policies	mode rie appendistance	4 bots if the cluster details are correct, if there is already a VM with the same name provid	Osername *
+ Addions	Invole-Prefight/etDRUkinstall	This Critilet checks and displays current state of the system it checks whether the minimal	root
+ A00-018		4 hosts if the cluster details are correct and if any VCenter is registered to the MSA	Passwood *
Workload Networking	Universit ArtOR	The top level Ondlet creates a new user, assigns elevated privileges to the user, unconfigu	
🐇 Segments	> Microsoft/WS/Management 4147 www.	a chidata for administrator even lasks in managing Adves shriftees bouctures	HustName ()
DHCF			antoval-ma
Port manning			Network * ①
O DNS			DRSep
. Mar.			
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.

ite Details							Alarm Sett	+1.
							Aldini Sett	111
vCenter Server Hostname	172.30.15	6.2						
Management Appliance Hostname	anfjsval-m	sa						
Software Version	4.0.2.450							
Subscription ID	- Configu	ire						
Tenant ID / Application ID	- Configu	ire						
Application Secret	- Configu	ire						
Configure Cluster	Direction Unconfigure	🛠 Reso	ve Configure	Issue				1
Cluster Name	Datacenter	Name 🔺	Status	A	Software Versior	۱ 🔺	Host Details	
Cluster-1	SDDC-Datac	enter	🕝 Ok		4.0.2.132		Details	

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

000 001	Protected Domain Tile0	20	20	and the state of the		
001			20	Import	^	182
	5	20	20	Import		
002	Protected Domain 02	20	20	Import		
003	Protected Domain Tile 03	20	20	Import	~	
					>	122
						~
)	0003	0003 Protected Domain Tile 03	0003 Protected Domain Tile 03 20	0003 Protected Domain Tile 03 20 20		0003 Protected Domain Tile 03 20 20 Import

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



These steps can also be automated using CPT created plans.

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

ect Protected Domain:	Continuous Fa	ilover Protected Dom	ain					Delete	=	More
de	1. General	2a. Failover Settings	2b. VM Settings		overy VA	4. DR Settings	5. Summary			Det
coverable / Total VMs	I. General	za. Fallover settings	20. VM Settings	5. Rect	overy va	4. DR Settings	5. Summary	~ reporec		
	Protected Do	omain Name		ANFPD002				253.160)		
	Datacenter			SDDC-Datac	enter					
	Cluster			Cluster-1						
	Resource Po	ool (Optional)		2						
rotected VMs Setti	VM Folder (C	Optional)		-				1000		
	Datastore			ANFRecoDS	U002					
	Internal Netv	vork		DRSeg						0
VM Name	External Rep	lication Network		DRSeg					Details	
AuctionAppA2	Managemen	t Network		DRSeg				- 600	Details	- 1
AuctionAppB2 AuctionDB2	Storage Site			ANFDemoble	obreporec				Details Details	
AuctionLB2	DR Virtual Ap	opliance		ANFRecDRV	A003			~	Details	
AuctionMSQ2	Bonligation	on Storago		idoviedh				_	Details	
AuctionNoSQL2					Cancel	Back	Continuous Failov	er	Details	

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

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

Protected Domains Statistics	Storag	ge Sites	Appliances	Configurat	ions	Task Log	
Select Protected Domain: ANFPD00	0 🕶	View all		+ Create		Delete	■More
Mode		Imported	Configura	itions		O Restore	
Recoverable / Total VMs		20 / 20	Storage Si	te	1	→ Failover	
			Owner Site	•	RE	→ Continuo	us Failover
						→ Test Faild	over
Protected VMs Settings Ala	irms						
							c
VM Name 🔺		Protect	tion Status 🔺		Protectio	on Mode 🔺	Details
AuctionAppA0		🕝 Reco	overable		Write-Bac	k(VMDK)	Details
AuctionAppB0		Reco	overable		Write-Bac	k(VMDK)	Details

Performing Failover / Failback

(i)

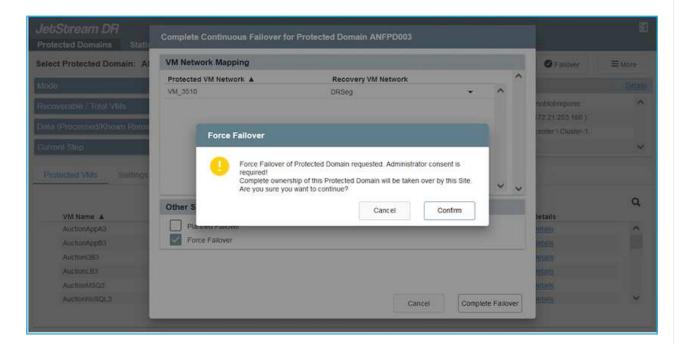
1. After a disaster occurs in the protected cluster of the on-premises environment (partial or full failure), trigger the failover.



÷

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

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



elect Protected Domain: ANFPD003			+ Create	≡More
lode	Task Steps			Details
tecoverable / Total VMs	lask Steps		ANEDemobiobreporec	^
	Prerequisite checks	^	MOTE (172.21.253.160)	
ata (Processed/Known Remaining)	Prepare for rehydration		DC-Datacenter \ Cluster-1	
urrent Step	Prepare Recovery VM ISOs		abled	~
Reviner no-Contractory	Recreate Protected Domain on DRVA			
Protected VMs Settings Al	Prepare temporary Recovery VMs			
	Power on and retrieve Recovery VMs' IPs			
	Recover VMs' data from Storage Site			Q
VM Name	Take Protected Domain ownership		Details	
AuctionAppA3	 Finalize rehydration 		Détaits	^
AuctionAppB3	Initialize DR Protection Mode		Details	
AuctionDB3	Clean up temporary Recovery VMs		Details	
AuctionLB3	 Resume Protected Domain protection Finalize recovered VMs 		Details	
AuctionMSQ3	Apply DR resumption storage policy		Octails.	
AuctionNoSQL3	Every on resumption storage pointy Every and the storage pointy	~	Details:	~

The task bar shows progress of failover activities.

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

IetSbream DR Protected Domains Str	Continuous Rehydration Task Result			E
elect Protected Domain:	Al Task Completed Successfully		Delet	te 🛛 🗏 More
lode				Edit Delan
Marca Shi Gulan (Shara) Shi Shi Marka	Protected Domain	ANFPD003		~ ^
tecoverable / Total VMs	VMs Recovery Status	Success	mobiobrepor	
teplication Status	Total VMs Recovered	20	230.156.2)	
10	testFGP0 Status:		center \ Clus	ter-1
emaining Background Data	Pre-script Execution Status	Not defined		
urrent RPO	Runbook Execution Status	Success		~
	Post-script Execution Status	Not defined		
Protected VMs Settin	35			
+ Start Protection	-			٩
VM Name A			d D Det	ails
AuctionAppA3			Det	
AuctionApp83			Det	ats
AuctionDB3			Deta	alls
AuctionLB3			Dets	aity.
AuctionMSQ3			Dismiss Deb	ada
AuctionNoSQL3	- Recording	TOR TROCORCE VINCES	Det	alls 🗸 🗸

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

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



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

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

Select Protected Domain: ANFPD003	View all		+ Create	Delete	≡ More
Mode	Running in Failover	Configurations		O Restore	
Active Site	172.30.156.2	Storage Site	ANF	O Resume Continu	Jous Rehýdratic
Recoverable / Total VMs	20 / 20	Owner Site	REMOT	← Failback	
Protected VMs Settings Alarma	ŝ				c
Protected VMs Settings Alarms	5 Protection Sta	tus 🔺 Protection Me	ode 🛦	Details	c
	*			Details Details	~
VM Name 🔺	Protection Sta	Write-Back(VM	DK)		
VM Name A AuctionAppA3	Protection Sta	Write-Back(VM Write-Back(VM	DK) DK)	Details	~
VM Name A AuctionAppA3 AuctionAppB3	Protection Sta @ Recoverable @ Recoverable	Write-Back(VM Write-Back(VM	DK) DK) DK)	Details Details	~
VM Name A AuctionAppA3 AuctionAppB3 AuctionDB3	Protection Sta © Recoverable © Recoverable © Recoverable	Write-Back(VM Write-Back(VM Write-Back(VM Write-Back(VM	DK) DK) DK)	Details Details Details	a



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.



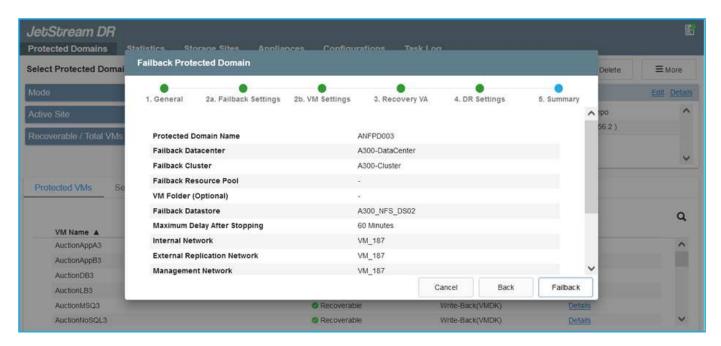
Specify the maximum delay after pausing VMs in the recovery site and restarting in the protected site. This time includes completing replication after stopping failover VMs, the time to clean recovery site, and the time to recreate VMs in protected site. The NetApp recommended value is 10 minutes.

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.



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

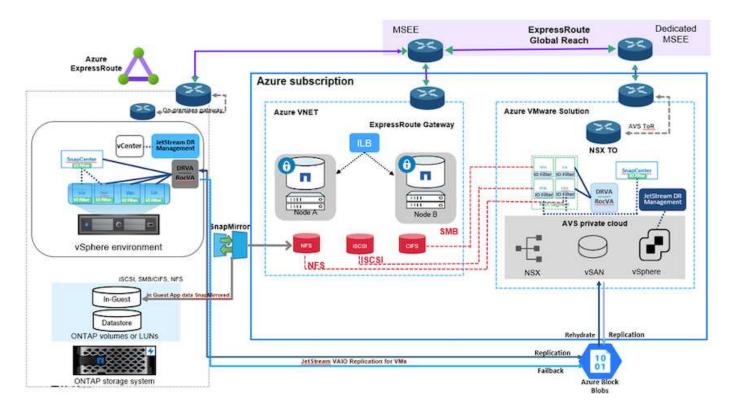
Disaster recovery to cloud is a resilient and cost-effective way of protecting workloads against site outages and data corruption events such as ransomware. With NetApp SnapMirror, on-premises VMware workloads that use guest-connected storage can be replicated to NetApp Cloud Volumes ONTAP running in 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 =		otal Transfer Time 👘	Status	Mirror State	Last Successful Transfer	(+
Ø	gcsdrsqidb_sc46 ntaphci-a300e9u25	gcsdrsqldb_sc46_copy ANFCVODRDemo		7 seconds	idle	snapmirrored	May 6, 2022, 11:43:18 AM 105.06 KiB	
0	gcsdrsqlhld_sc46_copy ANFCVODRDemo	gcsdrsqlhid_sc46 ntaphci-a300e9u25		seconds	idle	snapmirrored	May 6, 2022, 11:42:20 AN 7.22 MiB	
\odot	gcsdrsqilog_sc46 ntaphci-a300e9u25	gcsdrsqilog_sc46_copy ANFCVODRDemo	16	6 seconds	idle	snapmirrored	May 6, 2022, 11:43:52 AA 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.

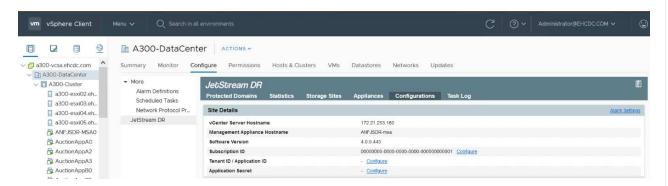
The most common deployed option is to have SDDC running in an always-on, pilot-light mode of operation. This option provides a small footprint of three hosts that are always available, and it also speeds up recovery operations by providing a running baseline for simulation activities and compliance checks, 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	00000000-0000-000	0-0000-00000000001 Configure		
Tenant ID / Application ID	- Configure			
Application Secret	- <u>Configure</u>			
Configured Clusters	Configure Clusters			
Configure Cluster 1 Upgrade Dunconfigure & Res		Select All Clear All	٩	٩
Cluster Name 🔺	Cluster Name A	Datacenter Name	sion 🔺	Host Details 🔺
No cluster configured	A300-Cluster	A300-DataCenter	*	
		2		
		Cancel Conf	figure	

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

Storage Sites	Add Storage Site	
+ Add Storage Site Scan Domain	Starage Sde Type *	
Name 🛦	Azure Blob Storage	
No Storage Site configured		
	Access Type * Key Access	
	Ney ALLess	
	Storage Site Name (Provide a name to identify this Site) *	
	ANFDemoblobrepo	
Storage Site Details Alarms	Acure Blob Storage Account Name *	
	Acure also storage Account name " anfordemostor	
No storage site selected. Select a storage		
	Aquire Bob Storage Account Key *	
	······································	

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

(i)

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

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

DRVAs (DR Virtual Appliances)	1. General 2. DRVA VM	3. DRVA Network 4. Summary	
+ Deploy New DRVA	Name	GCSDRPD001	
Name 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)	3.	
	VM Folder (Optional)		
Replication Log Volume	Datastore	A300_NFS_vMotion	
Statements and an other statements	Number Of CPUs	8	
+ New Replication Log Yourne 🗳 Encontigure	Memory Size	32GB	
Disk 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.

lebSbream DR Protected Domains Statistics Storage S	ites Appliances Configuration	ns Task Log			
DRVAs (DR Virtual Appliances)					
+ Deploy New DRVA Deploy New DRVA	10				C
Name 🔺	Status 🔺	Child Alarm 🔺	Software Version 🔺	Details 🔺	
OCSDRPD001	Running	00	4.0.0.134	Detain	
+ New Replication Log Volume					c
		AL 14 4	Size (available/total)	Details A	
Disk Path Name	Status	Child Alarm 🔺	ovce (avanauveriovar) 🔹		
	Status. O Ok	Child Alarm A	179 88 GE / 200 GB	Detata	
Disk Pam Name ▲ Idex/505 Replication Log Volume Details					

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

elect Protected Domain: • View all	Create Protected Domain				+ Create = At
	1. General 2. P	nimary Site	J. Summary	N	
	Protected Domain Name	GCSDRPD_Demo01			
	Priority Level (Optional)				
	Description	Protection domain ANF			
	Total estimated data size to be protected	1000GB			
	DR Virtual Appliance	GCSDRPD001			
	Compression	Yes			
	Compression Level	Default			
	Normal GC Storage Overhead	50%			
	Maximum GC Storage Overhead	300%			
	Replication Log Storage	/dev/sdb			
	Ranlication I on Size	50GR			
		Cancel	Back Creat	te	

Select Protected Domain: * View all	Create Protected Domain			+ Create
	1. General	2. Primary Site	3. Summary	
	Compression	Yes		
	Compression Level	Default		
	Normal GC Storage Overhead	50%		
	Maximum GC Storage Overhead	300%		
	Replication Log Storage	/dev/sdb		
	Replication Log Size	50GB		
	Metadata Size	31.56GB		
	Primary Site Datacenter	A300-DataCenter		
	Primary Site Cluster	A300-Cluster		
	Storage Site	ANFDRDemoFailoverSite		
	Enable PITR	No		
		Cancel Ba	ck Create	

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.

ebStream DR rotected Domains Statistics Storage Sites	s Appliances Configurations Task Lo				
elect Protected Domain: GCSDRPD_Demo01 -				_	+ Create Delata E blass
ecoverable / Total VMs	Start Protection			-	Est Det
epication Sianus	Protection Made for extended VMs ×			q	
emaining Background Data	VM Name	# of Disks	Protection Mode		LOCAL (177.21.253.160)
	EliziticWebA2	1		×. *	A303-BataCenter \ A300-Ouster
arrent RPO	ElasticWebA3	1		- 01 	Disabled
Protected VMs Settings Atarms	ElasticWebB0	.1	With-Through	¥.	
Protected VMs Settings Alarms	ElasticWebB1	t i			
+ Start Protection	EtasticWebB2	18			
	ElasticWebB3	0 5	Witte Through	14 jul	
VM Name 🔺	GCS-DR-DC	1	Write-Through	-	Background Data A Details
No VM is producted	GCS-DR-LinVM01	1	Write-Through	~ ~	
	GCS-DR-SCA	.1	Write-Through	~	
	GCS-DR-SQL01	1	Write-Through	~	
	GCS-DR-WeivM01	1	Write-Through	~	
	Bis-drva-OCSDRPD001	2		- X)-	
	PrimeClient Standby0	2		× .	
	Standbyt	1	Write-Through	- či n	
	Standby?				
	Standby3	1			
	Constraint and the second s	11			
	VMmark-Template01	1		M	

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

elect Protected Domain: GCSDRPD_Demo01 .	Start Protection				+ Creato Totete Totete
ecoverable / Total VMs	Persentent Work for selected Wile			1	Edi De
epication Status	Write-Back(VMDK) •			a	ANFDRDemoFalloverSite
emaining Background Data	U VM Name 🔺	# of Disks	Protection Mode		LOCAL (172.21.253.169.) A300-DataCenter (A300-Duster
arrent RPO	ElasticWebA2	31	Write Through:	×. *	Duatied
and the O	 ElasticWebA3 	1	Willie-Through	×	
Protected VMs Settings Atarms	ElasticWebB0	1	vinite-Through	¥.,	
Promiting with Statistics	ElasticWebB1	1	Write-Thiough	¥.,	
+ Start Protector	ElasticWeb82	1	Write-Through	¥.,	
	ElasticWebB3	1		9	
UM Name A	GCS-DR-DC	1	WITTE-Back(VMDK)	-	Bockground Data A Details
No VM is protected.	GCS-DR-LinVM01	3	Write-Back(VMDK)	~	
	GCS-DR-SCA	1	Write-Back(VMDK)	*	
	GCS-DR-SQL01	1	Write-Back(VMDK)	~	
	GCS-DR-WeVM01	1	Write-Back(VMDK)	~	
	jst-dva-GCSDRPD001	2		- M.S.	
	PrimeClient	2			
	Standby0	1	vente-Trenugh	×	
	Standby1	1		10 L	
	Standby2	1	White Treough	¥.,	
	Standby3	1	Write Through	10.0	
	VMmark-Template01	1		10.00	
			Cancel Sta	art Protection	
	N.		C SALAR CA	12	

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 Sit	es Appliances Configurati	ons Task Log			Running Tasks	
elect Protected Domain: GCSDRPD_Demo01	<u>View att</u>			+ (Start Protection (GCS-DR-SCA) 50%	8
Recoverable / Total VMs		0/5	Configurations		Start Protection (GCS-DR-Win 50%	ë
Replication Status		OK	Storage Site		Start Protection (GCS-DR-Lin 50%	ŝ
emaining Background Data		0 B	Owner Site Datacenter \ Cluster	LOCAL (172.2 A300-DataCen	Start Protection (GCS-DR-DC) 50%	1
Surrent RPO			Point-in-time Recovery	Disabled	Start Protection (GCS-DR-SQ. 50%	6
Protected VMs Settings Alarms					Configure VMDK Re Completed	
				1		ч
+ Start Protection						
+ Start Protection Stop Protection	Protection Status	Replication Stat	us 🔺 Protection Mode 🔺	Background Da	ta 🔺 Details	
	Protection Status Protecting	Replication Stat	us A Protection Mode A Write-Back(VMDK)	Background Da -	ta A Details Details	16
□ VM Name ▲						14
O VM Name ▲ O GCS-DR-DC	Initializing		Write-Back(VMDK)		Details	14
VM Name GCS-DR-DC GCS-DR-LinvW01	Initializing Initializing Initializing	*	Write-Back(VMDK) Write-Back(VMDK)		Details Details	18

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

IeUSUream DR Protected Domains Statistics Sto	rage Sites Appliances Configuration	ons Task Log				e
elect Protected Domain: GCSDRPD_De	emo01 👻 <u>View all</u>			+ Create	Delete	≡ More
ecoverable / Total VMs		5/5	Configurations			Edit Detail
teplication Status		OK	Storage Site	ANFDRDemoFailo	werSite	
			Owner Site	LOCAL (172.21.253.16	50)	
temaining Background Data		0 8	Datacenter \ Cluster	A300-DataCenter \ A30	0-Cluster	
urrent RPO		05	Point-in-time Recovery	Disabled		
Protected VMs Settings: Alarms Start Protection VM Name	Protection Status	Replication Sta	atus 🔺 Protection Mode 🔺	Background Data	Details	٩
+ Start Protection		Replication Sta	tus ▲ Protection Mode ▲ Write-Back(VMDK)	Background Data 🔺 0 B	Details Details	٩
+ Start Protection	Protection Status 🔺					٩
+ Start Protection VM Name GCS-DR-DC	Protection Status A	O OK	Write-Back(VMDK)	0 B	Details	٩
Start Protection Stop Protection VM Name GCS-DR-DC GCS-DR-LinVM01	Protection Status ▲ © Recoverable © Recoverable	0 OK	Write-Back(VMDK) Write-Back(VMDK)	0 B 0 B	Details Details	٩

()

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

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

	tatistics Storage Sites	Appliances	Configurations	Task Log			(C	0.0	1
select Protected Domain:	GCSDRPD_Demo01 *	View all					+ Create	Delete	≡ More
Recoverable / Total VMs				5/5	Configurations				Edit Detail
Replication Status				ок	Storage Site	A	VFDRDemoFailove	rSite	2
					Owner Site	LOCAL	L (172.21.253.160)	
Remaining Background Dat	ta			08	Datacenter \ Cluster	A300-0	DataCenter \ A300-	Cluster	
Current RPO				0s	Point-in-time Recovery	Disabi	eđ		
		0	0						
Protected VMs Settin	ngs Alarms								
Failover Runbook Not	Configured Configure								
Test Failover Runbook Not	Configured Configure								
Failback Runbook 👌 Not	Configured Configure								
Memory Setting Not	Configured Configure								
GC Settings Con	figured Configure								
Concurrency Settings Not	Configured Configure								

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

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

Select Protected Domain: GCSDRPD Demo01 *	V			+ Create Delete E More
Recoverable / Total VMs	T Create Group	# of VM Power Off	Retain MAC	Edi Deb
recoverable / Total Awa	Coroup Name Independent VMs			
		5 -	·*.	ANFDRDemoFalloverSite
Remaining Background Data				LOCAL (172:21:253:100)
Current RPO	-			A300-DataCenter (A300-Cluster Disabled
Protected VMs Settings Alarms	0 0			
Failover Runbook Configured Details				
Test Failover Runbook Configured Details				
Fallback Runbook Configured Details				
Memory Setting Not Configured Configured				
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	s	3. Edit V	M Settings		4. Summ	ary .	+ Create	Delitte	≡ Mon
economiale / Total VMs	Retain MAC		Power Off	f VMs			O Reset	1			
pleation Skillis	VM Name	Boot Sequence	Boot Delay	CPU	Memory	Script	NIC		DRDemoFillioverSi 172 21 253 165)		
chaning Background Clata	GCS-DR-WinVM01	17 4	0s	32	64 GB	Config	View	12			
irent RPO	GCS-DR-SCA	21 4	0s	4	16 GB	Config	View				
india H9-92	GCS-DR-DC	30	0s	4	16 GB	Config	View				
Protected Vills Settings Alarmo	GCS-DR-LinVM01	41 4	0s	2	4 GB	Contig	View				
	GCS-DR-SQL01	5† 4	05	4	8 GB	Config	View				
Annony Setting Not Configured Configure SC Settings Configured Configure											
C Settings Configured Configure											
C Settings Configured Configure											
C Settings Configured Configure											

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

 (\mathbf{i})

Select Protected Domain: GOSDRPD_Demo	1. General	2. Select VMs		3. Edit VI	9 M Settings		4. Summa	iry	+ Creala	Delatu	幕
Recoverable Filotal VMs	Retain MAC		Power Off	f VMs			O Reset	1 1			
Replication Status	VM Name	Boot Sequence	Boot Delay	CPU	Memory	Script	NIC		FDRDemoFalloy		
Remaining Background Data	GCS-DR-WinVM01	1↑↓	0s	32	64 GB	Config		*			
ENTERING CONTRACTOR	GCS-DR-SCA	2↑↓	Qs	4	16 GB	Contig	Č,				
Clatest RPO	GCS-DR-LinVM01	3↑↓	0s	2	4 GB	Config	View				
Protected Vite Settings Alarma	GCS-DR-SQLOP	47 4	0s	4	8 GB	Cantio	Mew				
Contraction of the second seco	GCS-DR-DC	5† 4	0s.	4	16 GB	Config	View	÷.			
GC Settings Configured Configured Configured Configured Configured Configured Configured Configured Configured											

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

	Label		Network Name	Key	PCI Slot #	IP	
-	Network a	dapter 1	VM_3510	4000	192	Configure	aity
Re							
VM Na							
GCS-E		Configur	e Static IP Address				
GCSD		IP Address *					
OCS-E	0 0	172.21.25	54.185				1
10 DL	0-0	Subnet Mask					
		255.255.2					
		Gateway * 172.21.25	34.1				
			1700.			_	
		DN/S +					
		172.30.15	53.20			_	
		DNS Suff	ic.			_	
			Reset	Cance	Confi	gure	
					~		
						Close	Next
	_						
		Create Runt	ook Group				
		nip 1. Gen		3. Edit VM Setti	ngs 4. Summ	+ count	
		Group Na Number o	r VMs	GCSRecovery 5		170FdbimcFoldureday	
		Power Off	's MAC addresses VMs	true Talse		Disconstructions	
		Security Croup	mangements and boot sequence change will	be applied to both Fallover and	Failback runbook.		
			Success				

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

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

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

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



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



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

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



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

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

Microsoft Azure	P. Search resour	ces, services, and docs (G+/)	📰 😂 🖉 🎯 🎯 🕫 hiyaz@netapp.com
Home 3: ANFOataClus			Run command - Install-JetDRWithDHCP
ANFDataClus Run	n command —		This top level Crititet 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 duater.
Access control (IAM)	Packages Run execution status		Command parameters
Diagnose and solve problems	v Name	Description	Register/Withip ① True
Settings	 SDRConfiguration 224 Assessed 	Manual for configuration of Arthouge Software on 205, See artificean Software, we for support	ProtectedOuster * ()
A Locks	Disatile-JetDRForCluster	This Cindlet unconfigures a cluster but doesn't uninstall JetDR completely so other clusters	Cluster-1
D 10003		policies.	Detastore * ()
Manage	Enable-JetORForCluster	This Cindlet configures an additional cluster for protection. It installs vibs to all hosts in the	vsanDatastore
Connectivity	Install-JetDRWithDHCP	This top level Cridlet Downloads JetDr bundle from MMS, owates a new user, assigns elev	VMName* ()
Custers	200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200	registers vCenter to the JetDr MSA, configures cluster.	antjsvei-msa
The second	Install-JetDRWittGtatidP	This top level Cmtilet Downloads JetDr bundle from MMS, creates a new user, assigns elevi	Cluster* ()
Identity		registers vCenter to the JetDr MSA, configures duster.	Outer-1
Storage (preview)	Invoke-PreflightJetDRInstall	This Cridlet checks and displays current state of the system it checks whether the minimal	Cridential ()
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/setDRUminstall	This Cindlet checks and displays current state of the system it checks whether the minimal 4 hosts, if the cluster details are correct and if any VCenter is registered to the MSA	root
			Persevord *
Workload Networking	Uninstall-JetDR	The top level Cmdlet creates a new user, assigns elevated privilleges to the user, unconfigu	
🔹 Segments	> MicrosoftAVSManagement +147	Venous condiets for estimative revertaixs in meneping Azure VMMere Sourcare	HoutMame ①
T DHOP			antipoal-ma
Port mirroring			Network*
O DNS			DRSeg
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.

MARCE MARKET CONTRACT								
Site Details							Alarm Set	tti
vCenter Server Hostna	me	172.30.15	56.2					
Management Applianc	e Hostname	anfjsval-n	nsa					
Software Version		4.0.2.450						
Subscription ID		- Config	ure					
Tenant ID / Application	ID	- Config	ure					
Application Secret		- Config	ure					
Configure Cluster	1 Upgrade	Duconfigure	* Resolv	e Configure I	ssue			
Cluster Name		Datacenter	Name 🔺	Status	Softwar	e Version 🔺	Host Details	5
Cluster-1		SDDC-Data	center	🕝 Ok	4.0.2.13	2	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.

Available Protected	l Domain(s) For Impoi	rt					Ē
				Import	12		
GCSDRPD_Demo01	Protection domain ANF	5	5	Imost	-		٩
						ra Blob Storage	~
	Protected Domain	Available Protected Domain(s) For Impor Protected Domain Description GCSDRPD_Demo01 Protection domain ANF	Protected Domain Description Recoverable V	Protected Domain Description Recoverable V VMs	Protected Domain Description Recoverable V VIIs Import GCSDRPD_Demo01 Protection domain ANF 5 5 Impgd	Protected Domain Description Recoverable V VIIs Import GCSDRPD_Demo01 Protection domain ANF 5 5 Import	Protected Domain Description Recoverable V VMs Import GCSDRPD_Demo01 Protection domain ANF 5 5 Import

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

Select Protected Domain: GCSDRPD_Demo01 👻 View all			+ Create	Delete	■More
/lode	Imported	Configurations			Deta
Recoverable / Total VMs	5/5	Storage Site	ANFDemoblobr	eporec	
		Owner Site			
Protected VMs Settings Alarms O O					
Protected VMs Settings Alarms O O					
Protected VMs Settings Alarms O O	Protection Status		Protection Mode	Details	c
	Protection Status	•	Protection Mode ▲ Write-Back(VMDK)	Details Details	
VM Name 🔺		•			
VM Name A GCS-DR-DC	Recoverable	•	Write-Back(VMDK)	Details	
VM Name ▲ GCS-DR-DC GCS-DR-LinVM01	Recoverable	• •	Write-Back(VMDK) Write-Back(VMDK)	Details Details	c

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

 (\mathbf{i})

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

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

ect Protected Domain	Continuous F	ailover Protected Dom	ain					Delete	=	More
đe	1. General	2a. Failover Settings	2b. VM Settings	1 Per	overy VA	4. DR Settings	5. Summary			Dela
coverable / Total VMs	i. General	za. ranover settings	zo, vin settings	s. neo	Stell in	4. Dr. betungs	o. Summary	~ reporec		2
	Protected D	omain Name		ANFPD002				253,160)		
	Datacenter			SDDC-Datad	enter			100		
	Cluster			Cluster-1				1000		3
	Resource P	ool (Optional)						- Balline		
rotected VMs Setti	VM Folder (Optional)		÷.				1000		
	Datastore			ANFRecoDS	U002			100		
N994100000000000000000000000000000000000	Internal Net	work		DRSeg				100		C
VM Name A	External Re	plication Network		DRSeg					Details	1
AuctionAppA2 AuctionAppB2	Managemer	nt Network		DRSeg				1000	Details Details	
AuctionDB2	Storage Site	•		ANFDemobio	obreporec			1000	ALC: NO.	
AuctionLB2	DR Virtual A	ppliance		ANFRecDRV	/A003			~	Details	
AuctionMSQ2	Bonligation	I on Ptorseo		Movindh			-	_	Details	
AuctionNoSQL2					Cancel	Back	Continuous Failov	er	Details Details	-



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

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



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

elect Protected Domain: GCSDRPD_Demo01 👻 View all			+ Create	Delete	≡ Mor
lode	Imported	Configurations		O Restore	
Recoverable / Total VMs	5/5	Storage Site	ANEDemoblobrepor	→ Failover	
		Owner Site	REMOTE (172.21.253.1)	→ Continuous Fail	OVAL.
				→ Test Failover	9
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	
GC3-DR-Citivillo 1					
GCS-DR-SCA	Recoverable		Write-Back(VMDK)	Details	
	© Recoverable © Recoverable		Write-Back(VMDK) Write-Back(VMDK)	Details Details	

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

Failover and Failback

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

	Volume R	elationships	4.78 GIB Replicated Capacity	Currently Tran	sterring	3 Healthy	O Falled	
	3 Volume Relationships							٩
	Health Status	Source Volume 1	Target Volume T	Total Transfer Time 1	Status	₩ Mirror State	Last Successful Transfer	•
	0	gcsdrsqldb_sc46 ntaphci-a300e9u25	gcsdrsqldb_sc46_copy ANECVODRDemo K >	6 minutes 41 seconds	idle	snapmirrored	May 5, 2022, 12:08:34 Ph 33.66 Ki8	œ
	0	gcsdrsqfhid_sc46 ntaphci-a300e9u25	gcsdrsqlhid_sc46_copy ANFCVODRDemo K	4 minutes 56 seconds	idle	snapmirrored	Information	
	0	gcsdrsqllog_sc46 ntaphci-a300e9u25	gcsdrsqllog_sc46_copy ANECVODRDemo	10 minutes 18 seconds	idle	snapmircored	Break Reverse Resync	
	¢						Edit Schedule	
							Edit Max Transfer Rate	
							Update	
							opuere	
							Delete	
Replication	on Backup & Restore	Data Sense I	ile Cache Compute	Sync All Service	is (+9) ~	_		
	a 3	Data Sense (relationships	The Cache Compute	Sync All Service		S Healthy		
	a 3	elationships	4.78 GIB	€→ 0			Delete	C
	J Volume R	elationships	4.78 GIB Replicated Capacity	0 Currently Tran	sferring	Healthy	Delete	
	B Volume Relationships	relationships	4.78 GIB Replicated Capacity Break Relationship Are you sure that you want t	0 Currently Tran	ssferring, ween "gcsdrsqld	Healthy	Delete	c
	B volume Relationships Health Status :	elationships	4.78 GIB Replicated Capacity Break Relationship Are you sure that you want t	0 Currently Tran	ssferring, ween "gcsdrsqld	Healthy	Delete Delete Delete	ę

(i)

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

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

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

elect Protected Domain: GCSDRPD_Demo	1 • View all		+ Create	O Freilover	≡ Mor
Mode	Continuous Rehydration in Progress	Configurations			Details
Recoverable / Total VMs	Total VMs 4/4			orec	1
			REMOTE (172.21.253.	160)	
Data (Processed/Known Remaining)	329.01 GB / 6.19 GB	Datacenter \ Cluster	SDDC-Datacenter \ Clu	uster-1	
Current Step	Recover VMs' data from Storage Site	Point-in-time Recovery	Disabled		~
VM Name	Protection Status		Protection Mode	Details	đ
GCS-DR-DC	© Recoverable		Write-Back(VMDK)	Details	^
GCS-DR-LinVM01	Recoverable		Write-Back(VMDK)	Details	
	Recoverable		Write-Back(VMDK)	Detaits	
GCS-DR-SCA			Write-Back(VMDK)	Details	
GCS-DR-SCA GCS-DR-SQL01	Recoverable				

Protected VM Network	Recovery VM Network		1
VM_3510	DRStretchSeg •	^	
0 0		Ŷ	
Other Settings Planned Failover GRy Force Failover			

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

Ð	Force Failover of Protected Domain required! Complete ownership of this Protect		
	Site. Are you sure you want to continue?		
		Cancel	Confirm

M Network Mapping			
Protected VM Network 🔺	Recovery VM Network		^
/M_3510	DRStretchSeg	•	^
0 0		2	× .
ther Settings			
Planned Failover			
 Force Failover 			
Some VM's guest credential are requi	red because of network configuration: Cor	ifigure	

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

 $\widehat{}$

i

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

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

Select Protected Domain: GCSDRPD002	Task Completed Successfully with	warnings	+ Create E Delate E More
Node	.		Est Das
CONTRACTOR AND A CONTRACTOR OF A CONTRACTOR AND A CONTRACTOR A	Protected Domain	GCSDRPD002	ANFEVODR
ecoveratile / Total VMs	VMs Recovery Status	Success with warnings	OC4L(17230.156.2)
	Total VMs Recovered	4	DDC-Datacenter \ Cluster-1
emaining Background Data	VM(s) with warning	2 <u>View</u>	esabled
	GCSRecovery03 Status:		
urrent RPO	Pre-script Execution Status	Not defined	
	Runbook Execution Status	O Success	P
Protected VMs Settings Alarms	Post-script Execution Status	Not defined	
+ Start Protection II State Protection			c
VM Name A		N	ackground Data 🔺 Details
GCS-DR-SC46		<i>₽</i>	8 Details
GCS-DR-SQL03			8 Details
GCSDR-W2K16-01			8 Detaits
UbuntuSrv001			B Details

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

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

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

	letApp SnapC	enter®						•	•	9-	SnapCenterAdmin	Sign Out
<		Global Settings	Policies	Users and Access	Roles	Credential	Software					
	Dashboard											
9	Resources	Global Settings	0									
۲	Monitor											
мi	Reports	Hypervisor Settin	gs O									~
٨	Hosts	Notification Serv	er Settings	0		0.0	>					~
ł.	Storage Systems	Configuration Se	ttings 😗									~
÷	Settings	Purge Jobs Settin	gs O									~
▲	Alerts	Domain Settings	0									~
		CA Certificate Set	ttings 🕕									~
		Disaster Recover	y o									
		🗹 Enable Disast	er Recoverv	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 Comput	e Sync	All Service	s (+9) ~					
Replication	ation												
		J Valume Re	lationships	ଚ	4.78 GIB Replicated Capacity	(O Currently Tran	sferring	©	3 Healthy		⊗ 0 Failed	
	3	3 Volume Relationships											9
	3	8 Volume Relationships Health Status 🔅	Source Volume	¥1	Target Volume	e Total T	⊖—© ransfer Time ÷	Status	(*]	Mirror State	新	Last Successful Transfer	
			Source Volume gcsdrsqldb_sc46 maphci-a300e9u25	3 	gcsdrsqldb_sc46_copy ANFCVODRDemo			Status	₹	Mirror State broken-off	Ħ	Last Successful Transfer May 5, 2022, 12:08:34 PM 33.66 KiB	Q (
		Health Status 🗧	gcsdrsqldb_sc46		gcsdrsqldb_sc46_copy ANFCVODRDemo gcsdrsqlhld_sc46_copy ANFCVODRDemo	6 minu >	ransfer Time 🗧		¥ .		#	May 5, 2022, 12:08:34 PM	0

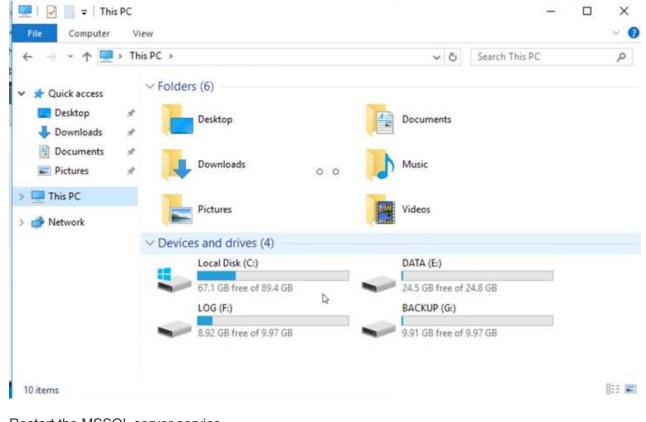
7. Attach the LUN from Cloud Volumes ONTAP to the recovered SQL guest VM with same drive letters.

Disk Manageme File Action View								
* * 🖬 👔	m 🗩 🗹 🛙							
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 %	
_ 200 (1)	surpre	BUSIC		ricensity (rin	0			

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

Targets	Discovery	Favorite Targets	Volumes and Devices	RADIUS	Configuration
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
Discove				Status	Refresh
Name		netapp:sn.547772c	cc47811ecbb62000	Status Connecte	

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



10. Restart the MSSQL server service.

	Q 🔒 🛛 🖬 🕨 🔲 🕪					
Services (Local)	Services (Local)			_		
	SQL Server (MSSQLSERVER)	Name	Description	Status	Startup Type	Log
	10 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	SQL Full-text Filter Daemon	Service to la	Running	Manual	NT
	Stop the service Pause the service	SQL Server (MSSQLSERVER)	Provider rto	Running	Automatic	GCS
	Restart the service	SQL Server Agent (MSS)	Start	ning	Automatic	GCS
		SQL Server Browser	Stop	ning	Automatic	Loc
	D	SQL Server CEIP service	Pause	ning	Automatic	NT
	Description: Provides storage, processing and	SQL Server Integration S	Resume	ning	Automatic	NT
	controlled access of data, and rapid	🗟 SQL Server Integration S	Restart	ning	Automatic	NT
	transaction processing.	🧠 SQL Server VSS Writer		ning	Automatic	Loc
		SSDP Discovery	All Tasks	> ning	Manual	Loc
		🧠 State Repository Service	Refresh	ning	Manual	Loc
		🖏 Still Image Acquisition E	nerresti		Manual	Loc
		Storage Service	Properties		Manual (Trig	Loc
		Storage Tiers Managem	Help		Manual	Loc
		Superfetch	0.00		Manual	Loc
		Sync Host_df83a	This service	-	Automatic (D	Loc
		System Event Notification S	Monitors sy	Running	Automatic	Loc
		<				>

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

	ols Window Help New Query 월요요요요요 사라라 ? - ♡ - ♡ - ♬ > Execute ■ ✔ \$? 클 🔒 \$? \$? 睅 녦 翩 요 ᆿ 弯 +존 존 ☜ =	
Object Explorer Image: Connect Image	SQLQuery1.sql - GDC\adminnimo (66)) + X /****** Script for SelectTopNRows command from SSMS ******/ ESELECT TOP (1000) [Id] ,[Name] ,[Price] FROM [CarDB].[dbo].[Cars] 0 0	
External Tables	100 % * 4	
🧰 Graph Tables	I Results I Messages	
 ☐ dbo.Cars ⊕ Columns ⊕ Keys ⊕ Constraints ⊕ Triggers ⊕ Indexes ⊕ Statistics 	Id Name Price 1 1 Car-1 1000 2 2 Car-2 2000 3 3 Car-3 3000 4 4 Car-4 4000 5 5 Car-5 5000	

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

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

(i)



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

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

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



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

Select Protected Domain: GCSDRPD_Demo01 🔻 View all			+ Create	🗴 Delete	More
Mode	Running in Failover	Configurations		O Restore	
Active Site	172.30.156.2	Storage Site	ANFCVODR	O Resume Continuous Rehy	vdratic
Recoverable / Total VMs	4/4	Owner Site	REMOTE (172.3	← Failback	
Testering With California Alarma					
VM Name 🔺	Protection Status		Protection Mode ▲	Details	
	Protection Status ▲ © Recoverable © Recoverable		Protection Mode ▲ Write-Back(VMDK) Write-Back(VMDK)	Details Details Details	
VM Name GCS-DR-DC	Recoverable		Write-Back(VMDK)	Details	
VM Name ▲ GCS-DR-DC GCS-DR-LinVM01	 Recoverable Recoverable 		Write-Back(VMDK) Write-Back(VMDK)	<u>Details</u> Details	(

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

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

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

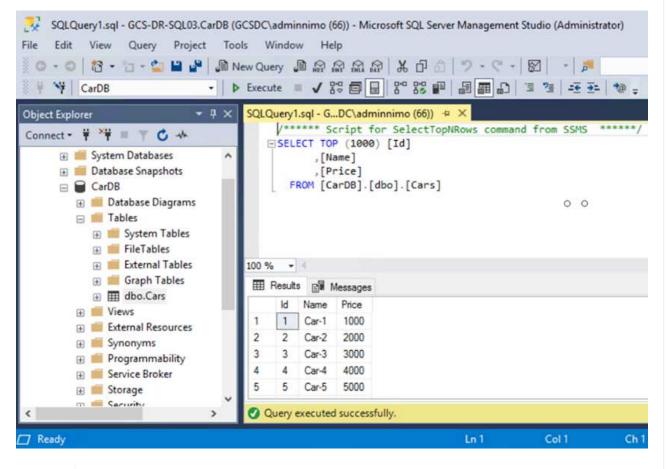
JetStream DR Protected Domains Statistics Storage S	Failback Task Result			
Select Protected Domain: GCSDRPD002 *	Task Completed Successfully			
Recoverable / Total VMs	Protected Domain	GCSDRPD002		
Replication Status	VMs Recovery Status	Success		
Remaining Background Data	Total VMs Recovered	4		
remaining causground caus	GCSRecovery03 Status:			
Current RPO	Pre-script Execution Status	Not defined		
	Runbook Execution Status	Success		
Protected VMs Settlings Alarms	Post-script Execution Status	Not defined	6	

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

\odot	gcsdrsqldb_sc46 ntaphci-a300e9u25	10	gcsdrsqldb_sc46_copy ANFCVODRDemo	•	6 minutes 41 seconds	idle	broken-off	May 5. 2022, 12:08:34 PN 33,66 KiB	-
\odot	gcsdrsqlhld_sc46 ntaphci-a300e9u25		gcsdrsqlhld_sc46_copy ANFCVODRDemo	•	4 minutes 56 seconds	idle	broken-off	Information	
\odot	gcsdrsqllog_sc46 ntaphci-a300e9u25		gcsdrsqllog_sc46_copy ANFCVODRDemo		10 minutes 18 seconds	idle	broken-off	Resync	
								Edit Schedule	
								Edit Max Transfer Rate	
								Delete	

Volume Re	lationships	6.54 GiB Replicated Capacity	Currently Tran	sferring	Ø 3 Healthy	⊗ 0 Failed	
/olume Relationships			0 0				Q
Health Status 🗧	Source Volume 🕴	Target Volume +	Total Transfer Time 🕴	Status	■ Mirror State ■	+ Last Successful Transfer	e
\odot	gcsdrsqldb_sc46 ntaphci-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)

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)

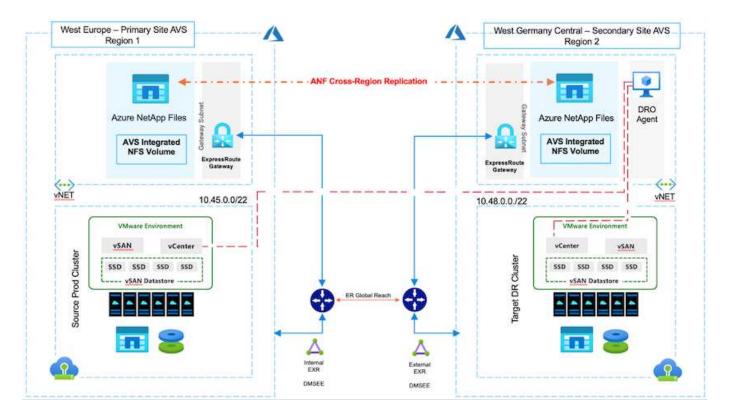
Disaster recovery using block-level replication between regions within the cloud is a resilient and cost-effective way of protecting the workloads against site outages and data corruption events (for example, ransomware).

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.



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 x	vſ	draa	is_pa	ackage.tar								
Navio	gate	to	the	directory	and	run	the	deploy	script	as	below:	
sudo	sh	depl	oy.s	sh								

- 3. Access the UI using the following credentials:
 - Username: admin
 - Password: admin

	■ NetApp		
	Disaster Recovery Orchestrator Impled Intermediate Journame		
	fersonerd.		
	boyin (_
		-	

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 🗘 Q 😩
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

Resource Groups Replication Plans Job Monitoring Discover Resource Groups Replication Plans Job Monitoring	٠	3	9
Add New Site 0 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 🔞 vCenter Details 🕘 !	Storage Details	
		Source AVS Private Cloud		
	Select Credentials	Azure Region	Azure Resource Group	
	DemoCred -	West Europe	ANFAVSVal2 +	
	Add New Credential IS			
		AVS Details		
		Avo Detalis		
	Web Client	URL	0	
		ANFDataClus	*	
	Username		0	
	cloudad	min@vsphere.local		
	Password		0	
		•••••		
		Accept self-signed certificates		
		- recept an agriculture		

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

15. Click Create Site.

Disaster Recovery Orchestrator 💊	Dashboard Discover Resource Group	ps Replication Plans Job Monitoring		4
		Site Type	Site Location	
C 2 C	vCenters 2 Storages	1 Source Destination	0 On Prem	2 Cloud
2 Sites				Q O Add New Site
2 Sites Site Name	○ Site Type = 〒 Location	n	Discovery Status	Q O Add New Site
	≎ Site type = ∀ Location Destination Cloud	n ⇒ vCenter ≎ Storage ≎ VM.List 1 1		Q O Add New Site

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

Disaster Recovery Orchestrator	Na Dashboard Docover R	escurce Groups Replication Plans Job	Monitoring		<u> </u>
Back		VM List Site: DemoSRC vCenter: https://17	2.30.156.2/		
🔁 7	attores	128 Virtual Machines	VM Protection 2 Protected	126 Understenter	
128 vm				Q	Create Resource Group
VM Name	211 VM Status		DuteStore	0 I. ON	C Memory (MB)
HDSenth_2.5.1	0 Not Protected	() Powered On	vianDatastore	8	8192
hci-fio-datastore-13964-0-1	0 Not Protected	D Powered Off	HERstDS	12	65536
ICCA2005-WO-R1	O Not Protected	(1) Powered On	wanDatastone	8	34336
ICCA2005-NE-R1	0 Not Protected	() Powered On	vsanDataitore	1	3072
ICCA2005-81-81	0 Not Protected	() Powered On	vianDatactore	5	3072
HCK_Demo_05	0 Not Protected	Dewered Dff	Demo002	1	2048

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

Resource groupings

After the platforms have been added, group the VMs you want to recover into resource groups. DRO resource groups allow you to group a set of dependent VMs into logical groups that contain their boot orders, boot delays, and optional application validations that can be executed upon recovery.

To start creating resource groups, click the Create New Resource Group menu item.

1. Access Resource Grou*ps and click *Create New Resource Group.

NetApp	Disaster Recovery Orchestrator 💊 📔 Dashi	poard Discover Resource Groups Re	plication Plans Job Monitoring	A 3	¢ 0 9
	Resource Group	☐ 1 Site	P 1	2 Virtual Machines	
	1 Resource Group			Q 🕤 Create New Resource Group	
	Resource Group Name	\$ Site Name	⇒ Source vCenter	⇒ VM List	
	DemoRG	DemoSRC	https://172.30.156.2/	View VM List	

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

• The last virtual machine to power on

NetApp Disaster Recovery Orchestrator	Dashboard Disc		Replication Plans	Job Monitoring			•	?
Edit Resource Group		Resource Group Det	ails 🕜 Select VMs	Boot order	and Delay			
			Boot order and	d Delay				
	VM Name	Boot Order 🕘		Boot Delay	(secs)			
	QALin1	3	0	0	12			
	QALin	3	10	0	[0]			

6. Click Create Resource Group.

Disaster Recovery Orchestrator 💊 🕴	Dashboard Discover Resource Groups F	eplication Plans Job Monitoring	4
Resource Group	C 1 Site	Center	2 Virtual Machines
1 Resource Group			Q O Create New Resource Group
Résource Group Name	Site Name	≂ Source vCenter	≂ VM List
DemoRG	DemoSRC	https://172.30.156.2/	(View VM List)

Replication plans

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

To start creating a replication plan, complete the following steps:

1. Navigate to Replication Plans and click Create New Replication Plan.

Image: Source Details Image: Source Details Image: Source Details Image: Source Groups Image: Source Groups Image: Source Groups Image: Source Groups Image: Source Groups Image: Source Groups Image: Source Groups Image: Source Groups Image: Source Groups Image: Source Groups Image: Source Groups Image: Source Groups Image: Source Groups Image: Source Groups Image: Source Groups Image: Source Groups Image: Source Groups Image: Source Groups Image: Source Groups Image: Source Groups Image: Source Groups Image: Source Groups Image: Source Groups Image: Source Groups Image: Source Groups Image: Source Groups Image: Source Groups Image: Source Groups Image: Source Groups Image: Source Groups Image: Source Groups Image: Source Groups Image: Source Groups Image: Source Groups Image: Source Groups Image: Source Groups Image: Source Groups Image: Source Groups Image: Source Groups Image: Source Groups Image: Source Groups Image: Source Groups Image: Source Groups Image: Source Groups Image: Source Groups	1 1 1 1 1 1 Replication Plans 1 1 1 1 1	App Disaster Recovery Orchestrator 💊 Dashboard Discover Resource	Groups Replication Plans	Job Monitoring		
Replication Plan Q Create New Replication Plan	1 Replication Plan Q Q Create New Replication Plan		Source Details		Destination Details	
		Replication Plans	Sites 1	—	Sites 1	
	Plan Name C Active Site Status Compliance Source Site 🐨 Destination Site C					Create New Replication Plan

2. On the **New Replication Plan**, provide a name for the plan and add recovery mappings by selecting the Source Site, associated vCenter, Destination Site, and associated vCenter.

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

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

NetApp Disaster Recovery Orchestrator	Dashboard Discover Resource Gro	ups Replication Pla	ins Job Monitoring		۵	٠	?	9
Create New Replication Plan	Replication Plan and Site Details	Select Resource G	iroups 3 Set Execution Order 4 Set VM Details					×
		Replication	Plan Details					
	Plan Name			0				
	DemoRP							
		Recovery	Mapping					
	Source Site	0	Destination Site	0				
	DemoSRC	· · ·	DemoDest	*				
	Source vCenter	0	Destination vCenter	0				
	https://172.30.156.2/	*	https://10.75.0.2/	*				
		Cluster I	Mapping					
	No more Si	ource/Destination clust	er resources available for mapping					
	Source Resource	Destination Re	source					
	Cluster-1	Cluster-1	Delete					
		Con	tinue					

- 4. Select **Resource Group Details** and click **Continue**.
- 5. Set the execution order for the resource group. This option enables you to select the sequence of operations when multiple resource groups exist.
- 6. Once done, set network mapping to the appropriate segment. The segments should already be provisioned on the secondary AVS cluster, and, to map the VMs to those, select the appropriate segment.
- 7. Datastore mappings are automatically selected based on the selection of VMs.



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

NetApp Disaster Recovery Orchestrator	Dashboard Discover Resource	Groups Replication Plans Job 1	Monitoring	A 🔅 🤅	•
Create New Replication Plan	Replication Plan and Site Details	Select Resource Groups 3	Set Execution Order (4) Set VM Details		×
		Replication Plan Det	ails		
		Select Execution Orde	er		
	Resource Group Name		Execution Order 👔		
	DemoRG		3 🕄		
		Network Mapping			
	No more	Source/Destination network resource	s available for mapping		
	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 and	Site Details 🕢 Select Resour	ce Groups 🕢 Set Exec	ution Order	Set VM Details			
		V	M Details					
	2 VMs					۹		
	VM Name	No. of CPUs	Memory (MB)	NIC/IP	Boot Order) Override			
	Resource Group : DemoR	G						
	QALin1	1 3	1024 [0]	 Static Dynamic 	3	0		
	QALin	4 8	1024 [0]	 Static Dynamic 	3	1		

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.

1 Replication Plan Q. O. Create New Replication Plan Name ↓ Active Site ↓ Status Compliance ↓ Source Site ♥ Destination Site ↓ DemoRP ⓒ Source ⓒ Active ▲ Partially Healthy DemoSRC DemoDest Resource Groups	Ran Create Now Replication Plan	 [3] [3]	lication Plans	2 1 Resource Groups	Source Details	1	Destination) Details	6 1
Plan Name \$ Active Site \$ Status Compliance \$ Source Site \$ Destination Site \$ DemoRP © Source © Active ▲ Partially Healthy DemoSRC DemoDest Resource Groups	C Active Site I I I O Source O Active Active I I Image: Source O Active Image: Source Site Image: Source				Sites	vCenters	Sites		vcenters
Plan Name ○ Active Site Status Compliance Source Site ♥ Destination Site ○ DemoRP ③ Source ③ Active ▲ Partially Healthy DemoSRC DemoDest Resource Groups		1 Replication Plan						9 9	Create New Replication Plan
Pan Details Edit Pan	Pan Details Edit Pan Fallover		C Active Site	Status	Compliance	Source Site		-)
Ede Pan	Edit Pan Fallover	DemoRP	⊘ Source	⊘ Active	A Partially Healthy	DemoSRC	DemoDest	Resour	ce Groups
	Fallover								Plan Details
Fallow									Edit Plan
	Test Fallover								Fallover
Test Falove									Test Fallover
Migrate	Migran								
	Run Compliance								

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

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

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

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 ①

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

C 2 Stes	1 Resource Group	128 Replication Plan	Protected VMs	0 127 Unprotected
Environments Virtual Environments	2 Allef Storage Accounts	Topology Cerves		Immensive View (3
SDDC Summary	14 Falders	DemuSRC teps.//172.38.156.29	Devisiblest Regis ITE 75.6.29	
12 Dutastores	12 Networks			

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

B 1 🖸 1	Source Details	Destination Deta	oits
Replication Plans Resource Gi		enters Sites	vCenters
1 Replication Plan			Q O Create New Replication Plan
Plan Name C Active Site Status	Compliance Source	e Site \mp Destination Site :	i i l
DemoRP ODestination () Runnin	ng In Failover Modi 🥥 Healthy Demo	SRC DemoDest	Resource Groups

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

			Source Details		Destin	ation Details		
B 1 Repli	ation Plans	1 Resource Groups	Sites 1	2 1 vCenters	Site		2 1 vCenters	
1 Replication Plan						Q 9	Create New Replication Plan	
Plan Name	C Active Site	Status	Compliance	Source Site	⇒ Destination Site	÷ 1	() ()	
DemoRP	© Destination	⊘ Active	Healthy	DemoSRC	DemoDest	Res		
-							Pian Details	<u> </u>
							Falback	
APP Disaster Recovery O	chestrator 🌯 Deshimani	Discover Resource Gros	ugis Replication Plans	Job Monitoring				• •
						Protected VMs		1
	es 😥	1 Tessur(e Group	别 1 Replication Plan	B	128	Protected VMs	0 127 Unprotected	1
	ei	1 Lesseurce Group	3 1 Replication Plan	B	128	0 1		
Environments	tes 🛛	1 Fassburge Groups Topplogy		8	128 \\\\	0 1		ļ
	B 2	Topology		B	128 VMs	0 1	Umprotected	
Environmenti 1992 2	a 2	Topology		B	128 VMs	0 1	Umprotected	
Environmenti 1992 2	a 2	Topology			128 VMs	0 1	Umprotected	
Environments 2 2 Vitriai Environm SDDC Summary	eta 🗧 2	Topology	Cances			• 1 Pretrotore	Umprotected	
Environments	eta 🗧 2	Topółogy	Canvas		128 VMs	© 1 Protection	Umprotected	
Environments 2012 Environm SDDC Summary	eta 🗧 2	Topółogy	Canual	.2	Demotes	© 1 Protection	Umprotected	
Invitormenti 2 2 Virtual Lennoun SDDC Summary Cluster 12	ets E 2 Att Storage Accord P 14 Fold	onts	Canual	<u>ل</u>	Demotes	© 1 Protection	Umprotected	
Environments 2 virtual between SDDC Summary Charter	ets E 2 Att Storage Accord P 14 Fold	onts	Canual		Demotes	© 1 Protection	Umprotected	
Invironmenti 2 Virtual Evenuenti SDDC Summary Cluster 2 Cluster	ets E 2 Att Storage Accord P 14 Fold	onts	rCanvas LennoSRC Nega./1172.20.150	e.2	Demotes	© 1 Protection	Umprotected	

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.

[dr veeam anf image1]

Solution Deployment

High level steps

- 1. Veeam Backup and Replication software is running in an on-premises environment with appropriate network connectivity.
- 2. Deploy Azure VMware Solution (AVS) private cloud and attach Azure NetApp Files datastores to Azure VMware Solution hosts.

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

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

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

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

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

Deployment Details

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

To replicate VMs, follow the below steps:

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

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

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

[dr veeam anf image2]

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

[dr veeam anf image3]

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

[dr veeam anf image4]

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

[dr veeam anf image5]

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

[dr veeam anf image6]

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

[dr veeam anf image7]

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

[dr veeam anf image8]

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

[dr veeam anf image9]

For additional information for Veeam replication, refer How Replication Works

Step 2: Create a failover plan

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

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



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



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



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

To create the Failover Plan, do the following:

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

[dr veeam anf image10]

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

[dr veeam anf image11]

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

[dr veeam anf image12]

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

Step 3: Run the failover plan

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



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

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

[dr veeam anf image13]

[dr veeam anf image14]

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

[dr veeam anf image15]

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

[dr veeam anf image16]



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

For detailed information about failover plans, refer Failover Plans.

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

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



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

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

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

[dr veeam anf image17]

[dr veeam anf image18]

[dr veeam anf image19]

[dr veeam anf image20]

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

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

[dr veeam anf image21]

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

[dr veeam anf image22]

Conclusion

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

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

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

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.