

NetApp Hybrid Multicloud with VMware

NetApp Solutions

NetApp September 19, 2024

This PDF was generated from https://docs.netapp.com/us-en/netapp-solutions/ehc/ehc-overview.html on September 19, 2024. Always check docs.netapp.com for the latest.

Table of Contents

letApp Hybrid Multicloud with VMware Solutions	1
VMware for Public Cloud	1
VMware Hybrid Cloud Use Cases	120
NetApp for AWS / VMC	123
NetApp for Azure / AVS	276
NetApp for GCP / GCVE	363
BlueXP Disaster Recovery	456

NetApp Hybrid Multicloud with VMware Solutions

VMware for Public Cloud

Overview of NetApp Hybrid Multicloud with VMware

Most IT organizations follow the hybrid cloud-first approach. These organizations are in a transformation phase and customers are evaluating their current IT landscape and then migrating their workloads to the cloud based on the assessment and discovery exercise.

The factors for customers migrating to the cloud can include elasticity and burst, data center exit, data center consolidation, end-of-life scenarios, mergers, acquisitions, and so on. The reason for this migration can vary based on each organization and their respective business priorities. When moving to the hybrid cloud, choosing the right storage in the cloud is very important in order to unleash the power of cloud deployment and elasticity.

VMware Cloud options in Public Cloud

This section describes how each of the cloud providers support a VMware Software Defined Data Center (SDDC) and/or VMware Cloud Foundation (VCF) stack within their respective public cloud offerings.

Azure VMware Solution



Azure VMware Solution is a hybrid cloud service that allows for fully functioning VMware SDDCs within the Microsoft Azure public cloud. Azure VMware Solution is a first-party solution fully managed and supported by Microsoft, verified by VMware leveraging Azure infrastructure. This means that when Azure VMware Solution is deployed, customer's get VMware's 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.

VMware Cloud on AWS



VMware Cloud on AWS brings VMware's enterprise-class SDDC software to the AWS Cloud with optimized access to native AWS services. Powered by VMware Cloud Foundation, VMware Cloud on AWS integrates VMware's compute, storage, and network virtualization products (VMware vSphere, VMware vSAN, and VMware NSX) along with VMware vCenter Server management, optimized to run on dedicated, elastic, bare-metal AWS infrastructure.

Google Cloud VMware Engine



Google Cloud VMware Engine is an infrastructure-as-a-service (IaaS) offering built on Google Cloud's highly

performant scalable infrastructure and VMware Cloud Foundation stack – VMware vSphere, vCenter, vSAN, and NSX-T. This service enables a fast path to the cloud, seamlessly migrating or extending existing VMware workloads from on-premises environments to Google Cloud Platform without the cost, effort ,or risk of rearchitecting applications or retooling operations. It is a service sold and supported by Google, working closely with VMware.



SDDC private cloud and NetApp Cloud Volumes colocation provides the best performance with minimal network latency.

Did you know?

Regardless of the cloud used, when a VMware SDDC is deployed, the initial cluster includes the following products:

- VMware ESXi hosts for compute virtualization with a vCenter Server appliance for management
- VMware vSAN hyper-converged storage incorporating the physical storage assets of each ESXi host
- VMware NSX for virtual networking and security with an NSX Manager cluster for management

Storage configuration

For customers planning to host storage-intensive workloads and scale out on any cloud-hosted VMware solution, the default hyper-converged infrastructure dictates that the expansion should be on both the compute and storage resources.

By integrating with NetApp Cloud Volumes, such as Azure NetApp Files, Amazon FSx for NetApp ONTAP, Cloud Volumes ONTAP (available in all three major hyperscalers), and Cloud Volumes Service for Google Cloud, customers now have options to independently scale their storage separately, and only add compute nodes to the SDDC cluster as needed.

Notes:

- VMware does not recommend unbalanced cluster configurations, hence expanding storage means adding more hosts, which implies more TCO.
- Only one vSAN environment is possible. Therefore, all storage traffic will compete directly with production workloads.
- There is no option to provide multiple performance tiers to align application requirements, performance, and cost.
- It is very easy to reach the limits of storage capacity of vSAN built on top of the cluster hosts. Use NetApp Cloud Volumes to scale storage to either host active datasets or tier cooler data to persistent storage.

Azure NetApp Files, Amazon FSx for NetApp ONTAP, Cloud Volumes ONTAP (available in all three major hyperscalers), and Cloud Volumes Service for Google Cloud can be used in conjunction with guest VMs. This hybrid storage architecture consists of a vSAN datastore that holds the guest operating system and application binary data. The application data is attached to the VM through a guest-based iSCSI initiator or the NFS/SMB mounts that communicate directly with Amazon FSx for NetApp ONTAP, Cloud Volume ONTAP, Azure NetApp Files and Cloud Volumes Service for Google Cloud respectively. This configuration allows you to easily overcome challenges with storage capacity as with vSAN, the available free space depends on the slack space and storage policies used.

Let's consider a three-node SDDC cluster on VMware Cloud on AWS:

• The total raw capacity for a three-node SDDC = 31.1TB (roughly 10TB for each node).

- The slack space to be maintained before additional hosts are added = 25% = (.25 x 31.1TB) = 7.7TB.
- The usable raw capacity after slack space deduction = 23.4TB
- The effective free space available depends on the storage policy applied.

For example:

- RAID 0 = effective free space = 23.4TB (usable raw capacity/1)
- RAID 1 = effective free space = 11.7TB (usable raw capacity/2)
- RAID 5 = effective free space = 17.5TB (usable raw capacity/1.33)

Thus, using NetApp Cloud Volumes as guest-connected storage would help in expanding the storage and optimizing the TCO while meeting the performance and data protection requirements.



In-guest storage was the only available option at the time this document was written. As supplemental NFS datastore support becomes available, additional documentation will be available here.

Points to Remember

- In hybrid storage models, place tier 1 or high priority workloads on vSAN datastore to address any specific latency requirements because they are part of the host itself and within proximity. Use in-guest mechanisms for any workload VMs for which transactional latencies are acceptable.
- Use NetApp SnapMirror® technology to replicate the workload data from the on-premises ONTAP system to Cloud Volumes ONTAP or Amazon FSx for NetApp ONTAP to ease migration using block-level mechanisms. This does not apply to Azure NetApp Files and Cloud Volumes Services. For migrating data to Azure NetApp Files or Cloud Volumes Services, use NetApp XCP, BlueXP Copy and Sync, rysnc or robocopy depending on the file protocol used.
- Testing shows 2-4ms additional latency while accessing storage from the respective SDDCs. Factor this additional latency into the application requirements when mapping the storage.
- For mounting guest-connected storage during test failover and actual failover, make sure iSCSI initiators are reconfigured, DNS is updated for SMB shares, and NFS mount points are updated in fstab.
- Make sure that in-guest Microsoft Multipath I/O (MPIO), firewall, and disk timeout registry settings are configured properly inside the VM.



This applies to guest connected storage only.

Benefits of NetApp cloud storage

NetApp cloud storage offers the following benefits:

- Improves compute-to-storage density by scaling storage independently of compute.
- Allows you to reduce the host count, thus reducing the overall TCO.
- Compute node failure does not impact storage performance.
- The volume reshaping and dynamic service-level capability of Azure NetApp Files allows you to optimize cost by sizing for steady-state workloads, and thus preventing over provisioning.
- The storage efficiencies, cloud tiering, and instance-type modification capabilities of Cloud Volumes ONTAP allow optimal ways of adding and scaling storage.

- Prevents over provisioning storage resources are added only when needed.
- Efficient Snapshot copies and clones allow you to rapidly create copies without any performance impact.
- Helps address ransomware attacks by using quick recovery from Snapshot copies.
- Provides efficient incremental block transfer-based regional disaster recovery and integrated backup block level across regions provides better RPO and RTOs.

Assumptions

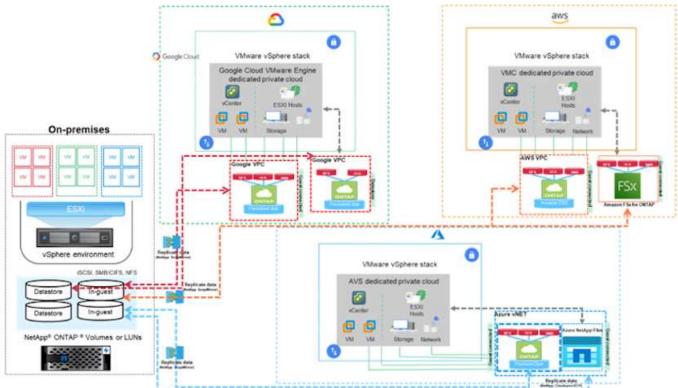
- SnapMirror technology or other relevant data migration mechanisms are enabled. There are many connectivity options, from on-premises to any hyperscaler cloud. Use the appropriate path and work with the relevant networking teams.
- · In-guest storage was the only available option at the time this document was written. As supplemental NFS datastore support becomes available, additional documentation will be available here.



Engage NetApp solution architects and respective hyperscaler cloud architects for planning and sizing of storage and the required number of hosts. NetApp recommends identifying the storage performance requirements before using the Cloud Volumes ONTAP sizer to finalize the storage instance type or the appropriate service level with the right throughput.

Detailed architecture

From a high-level perspective, this architecture (shown in the figure below) covers how to achieve hybrid Multicloud connectivity and app portability across multiple cloud providers using NetApp Cloud Volumes ONTAP, Cloud Volumes Service for Google Cloud and Azure NetApp Files as an additional in-guest storage option.



NetApp Solutions for VMware in Hyperscalers

Learn more about the capabilities that NetApp brings to the three (3) primary hyperscalers - from NetApp as a guest connected storage device or a supplemental NFS datastore to migrating workflows, extending/bursting to the cloud, backup/restore and disaster recovery.

Pick your cloud and let NetApp do the rest!



 (\mathbf{i})

To see the capabilities for a specific hyperscaler, click on the appropriate tab for that hyperscaler.

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

- VMware in the Hyperscalers Configuration
- NetApp Storage Options
- NetApp / VMware Cloud Solutions

VMware in the Hyperscalers Configuration

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

AWS / VMC

This section describes how to set up and manage VMware Cloud on AWS SDDC and use it in combination with the available options for connecting NetApp storage.



In-guest storage is the only supported method of connecting Cloud Volumes ONTAP to AWS VMC.

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

- Deploy and Configure VMware Cloud for AWS
- Connect VMware Cloud to FSx ONTAP

View the detailed configuration steps for VMC.

Azure / AVS

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



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

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

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

View the detailed configuration steps for AVS.

GCP / GCVE

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



In-guest storage is the only supported method of connecting Cloud Volumes ONTAP and Cloud Volumes Services to GCVE.

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

- · Deploy and Configure GCVE
- Enable Private Access to GCVE

View the detailed configuration steps for GCVE.

NetApp Storage Options

NetApp storage can be utilized in several ways - either as guest connected or as a supplemental NFS datastore - within each of the 3 major hyperscalers.

Please visit Supported NetApp Storage Options for more information.

AWS / VMC

AWS supports NetApp storage in the following configurations:

- FSx ONTAP as guest connected storage
- Cloud Volumes ONTAP (CVO) as guest connected storage
- FSx ONTAP as a supplemental NFS datastore

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

Azure / AVS

Azure supports NetApp storage in the following configurations:

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

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

GCP / GCVE

Google Cloud supports NetApp storage in the following configurations:

- Cloud Volumes ONTAP (CVO) as guest connected storage
- · Cloud Volumes Service (CVS) as guest connected storage
- · Cloud Volumes Service (CVS) as a supplemental NFS datastore

View the detailed guest connect storage options for GCVE.

Read more about NetApp Cloud Volumes Service datastore support for Google Cloud VMware Engine (NetApp blog) or How to use NetApp CVS as datastores for Google Cloud VMware Engine (Google blog)

NetApp / VMware Cloud Solutions

With NetApp and VMware cloud solutions, many use cases are simple to deploy in your hyperscaler of choice. VMware defines the primary cloud workload use-cases as:

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

AWS / VMC Browse the NetApp solutions for AWS / VMC
Azure / AVS Browse the NetApp solutions for Azure / AVS
GCP / GCVE Browse the NetApp solutions for Google Cloud Platform (GCP) / GCVE

Supported Configurations for NetApp Hybrid Multicloud with VMware

Understanding the combinations for NetApp storage support in the major hyperscalers.

	Guest Connected	Supplemental NFS Datastore
AWS	CVO FSx ONTAP Details	FSx ONTAP Details
Azur e	CVO ANF Details	ANF Details
GCP	CVO CVS Details	CVS Details

VMware in the Hyperscalers Configuration

Configuring the virtualization environment in the cloud provider

Details for how to configure the virtualization environment in each of the supported hyperscalers are covered here.

AWS / VMC

This section describes how to set up and manage VMware Cloud on AWS SDDC and use it in combination with the available options for connecting NetApp storage.



In-guest storage is the only supported method of connecting Cloud Volumes ONTAP to AWS VMC.

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

- Deploy and Configure VMware Cloud for AWS
- Connect VMware Cloud to FSx ONTAP

View the detailed configuration steps for VMC.

Azure / AVS

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



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

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

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

View the detailed configuration steps for AVS.

GCP / GCVE

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



In-guest storage is the only supported method of connecting Cloud Volumes ONTAP and Cloud Volumes Services to GCVE.

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

- Deploy and Configure GCVE
- Enable Private Access to GCVE

View the detailed configuration steps for GCVE.

Deploy and configure the Virtualization Environment on AWS

As with on-premises, planning VMware Cloud on AWS is critical for a successful production-ready environment for creating VMs and migration.

This section describes how to set up and manage VMware Cloud on AWS SDDC and use it in combination

with the available options for connecting NetApp storage.



In-guest storage is currently the only supported method of connecting Cloud Volumes ONTAP (CVO) to AWS VMC.

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

VMware Cloud on AWS provides for a cloud native experience for VMware based workloads in the AWS ecosystem. Each VMware Software-Defined Data Center (SDDC) runs in an Amazon Virtual Private Cloud (VPC) and provides a full VMware stack (including vCenter Server), NSX-T software-defined networking, vSAN software-defined storage, and one or more ESXi hosts that provide compute and storage resources to your workloads.

This section describes how to set up and manage VMware Cloud on AWS and use it in combination with Amazon FSx for NetApp ONTAP and/or Cloud Volumes ONTAP on AWS with in-guest storage.



In-guest storage is currently the only supported method of connecting Cloud Volumes ONTAP (CVO) to AWS VMC.

The setup process can be broken down into three parts:

Register for an AWS Account

Register for an Amazon Web Services Account.

You need an AWS account to get started, assuming there isn't one created already. New or existing, you need administrative privileges in the account for many steps in this procedure. See this link for more information regarding AWS credentials.

Register for a My VMware Account

Register for a My VMware account.

For access to VMware's cloud portfolio (including VMware Cloud on AWS), you need a VMware customer account or a My VMware account. If you have not already done so, create a VMware account here.

After the VMware account is configured and proper sizing is performed, deploying a Software-Defined Data Center is the obvious next step for using the VMware Cloud on AWS service. To create an SDDC, pick an AWS region to host it, give the SDDC a name, and specify how many ESXi hosts you want the SDDC to contain. If you don't already have an AWS account, you can still create a starter configuration SDDC that contains a single ESXi host.

1. Log into the VMware Cloud Console using your existing or newly created VMware credentials.

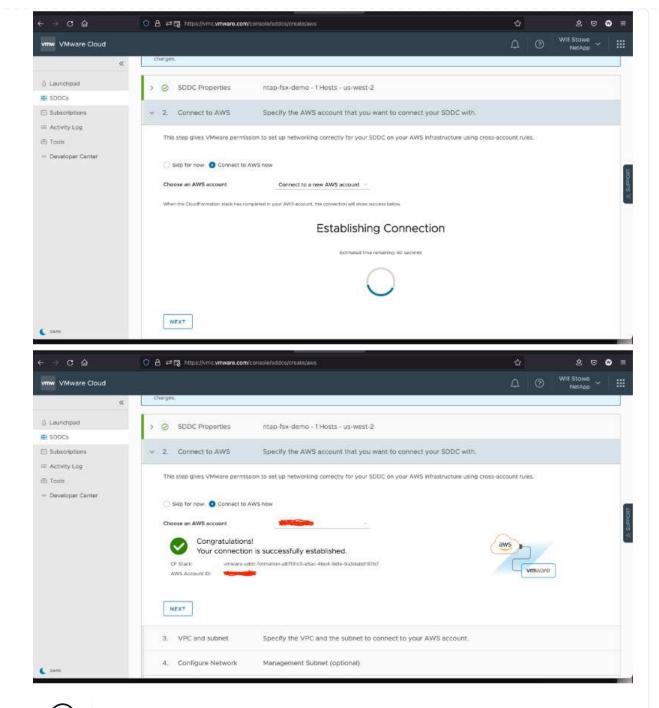
→ C @ O A https://console.cloud.vm	mware.com/csp/gatewasy/discovery?logout&skipLogout
Welcome	
Welcome to	
VMware Cloud Services	
Sign in with your VMware account	
Email address	
username@ensel.com	
HEST	
New to VMware Cloud?	
CREATE YOUR VMWARE ACCOUNT	
August 630, P. 170, do o Lucio Nation, a service de ministri 17	
ENGLISH	
6202I VMware, Inc. Terms Privacy California Privacy Rights	

2. Configure the AWS region, deployment, and host type and the SDDC name:

vmw VMware Cloud		A	0	Will Stown NetApp	
*	charges.				
å Launchped	v 1. SDDC Properties	Give your SDDC a name, choose a size, and specify the AWS region where it will be created.			
 Subscriptions Activity Log Tools Developer Center 	AWS Region Deployment Host Type SDDC Name Number of Hosts Host Capacity Total Capacity SHOW ADVANCED CONF	US West (Oregon)			
Dated	2. Connect to AWS	Specify the AWS account that you want to connect your SDDC with.			

3. Connect to the desired AWS account and execute the AWS Cloud Formation stack.

Quick cre	3 Stacks 3 Create stack
Template	
	eate stack
45 W20 - 240	
Template URL https://vmwar /mq5ijohtcliec	re-sddc.s3.us-west-2.amazonaws.com/1eb9d184-a706-4488-abb8-692aad0a25d0 h8l5b75ntegq%ccAbddd7lffq07m/7v16fk36
Stack descript This template	ion is created by VMware Cloud on AWS for SDDC deployment and maintenance. Please do not remove.
Stack name	e
Stack name	
	c-formation-a87f51c9-eSac-4bb4-9d1e-9a3dabd197b7 Include letters (A-Z and a-d, numbers (D-9), and dather (-).
Parameters are d	S Infined in your template and sllow you to input custom values when you create or update a stack.
ici. Englism (US). 🔻	6/2008 - 2021, Ansamn West Service, Ac. or In allitance All rights reasoned. Privacy Policy Terms of Use C
>Crû § Services▼	B. https://us-west-2.conaolo.aws.amazon.com/cloudformation/htcma?rsgionwus-west-2#istacka/quickcreate?stockNamew/mware-sdo: Q Search for services, fractures, marketplace products, and docs (Option+5) Q & 550-Administrator/WEStaweginetage.com @ doubleroes ♥ Oregon ♥
Stack name	
Stack name	
	c-formation-a82/51c9-e5ac-4bb4-9d1e-9a3dabd197b7 Indtude letter: (A-2 and a-st, numbers (D-9), and dathes (-).
Parameters are d	S lefined in your template and allow you to input custom values when you create or update a stack.
	No parameters There are no parameters defined in your template
Capabilities	
This temp Check tha	wing resource(s) require capabilities: [AWS::IAM::Role] Late contains identity and Access Management (IAM) resources that might provide entities access to make changes to your AWS account. Tyou want to create each of these resources and that they have the minimum required permissions. Learn more [2] owledge that AWS CloudFormation might create IAM resources.
aci, Englisti (US) 🔻	Cancel Create change set Create stack: 0.0005-2021, Ansam Web Sevilos, Mc. or Its 2016/10s, Mill rights vesarived. Privacy Policy Terms of Use C



Single-host configuration is used in this validation.

4. Select the desired AWS VPC to connect the VMC environment with.

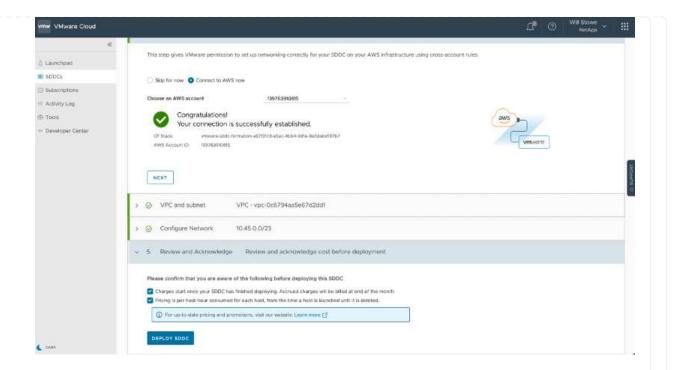
i

			2 🔍 🤇	
vmw VMware Cloud		û Ω	Will Stowe NetApp	
 kaunchpad SOOCs Subscriptions Activity Log Tools Developer Center 	the same availability zone to avoid cross AZ traffic charge.	Teer Assess Arrows Tour ANS TYC Arabacity Tour A ANS Schen 1 IC: Interser IC: Interser ANS Schen 1 IC: Interser ANS Schen 1 IC: Interser Arabacity for 2		

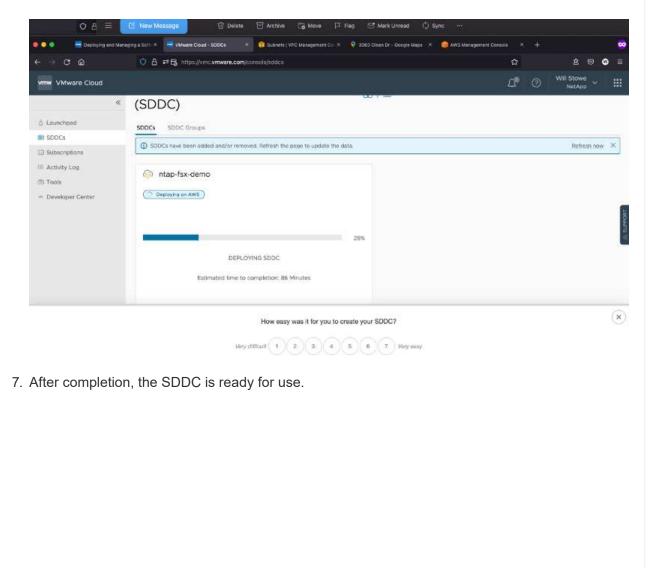
5. Configure the VMC Management Subnet; this subnet contains VMC-managed services like vCenter, NSX, and so on. Do not choose an overlapping address space with any other networks that need connectivity to the SDDC environment. Finally, follow the recommendations for CIDR size notated below.

⇒ C @	A # Https://vmc.vmware.com/console/sddcs/creats/aws	\$	2 🛛 🜑
w VMware Cloud		۵ ۵	③ Will Stowe ~
«	charges.		
Launchpad	SDDC Properties ntap-fsx-demo - 1 Hosts - us-west-2		
SODCs			
Subscriptions	> O Connect to AWS Aws Account ID 3a4ad01e-f5a7-3860-b	1a7-3bf4d70db1db	
Activity Log	VPC and subnet VPC - vpc-0c6794aa5e67d2dd1		
Developer Center	y even and sublet who i vpc-ocor and soes ruzudi		
Developer Center	~ 4. Configure Network Management Subnet (optional)		
	Specify a private subnet range (RFC 1918) to be used for vCenter Server, NSX A Choose a range that will not overlap with other networks or SDDC group memb Minimum CIDR sizes: /23 for up to 27 hosts, /26 for up to 25 hosts, /16 for up to Reserved CIDRs: 10.0.0.01/5, 172.310.0/h6. Menagement Subnet CIDR Intek Default: 10.3.0.016 NEXT	ers that connect to this SDDC.	
	5. Review and Acknowledge Review and acknowledge cost befor	re deployment	

6. Review and acknowledge the SDDC configuration, and then click deploy the SDDC.



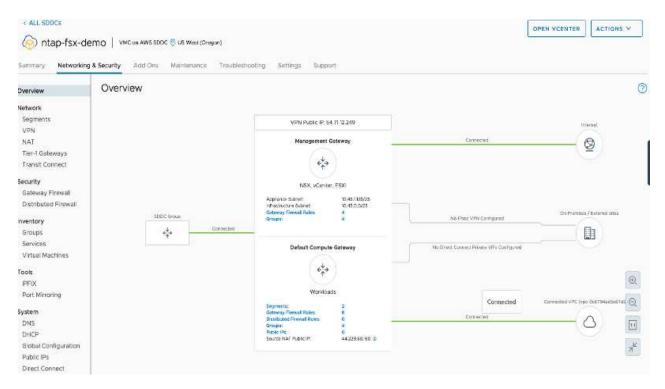
The deployment process typically takes approximately two hours to complete.



5 Laurchpad	Software-Defined Data Centers	881 =	CHEATE BODC ACTIONS
 500Cs Subscriptoms Activity Log Tools Developer Cardier 	(SDDC) SDDC Groups March 15x-demo March 1		
	VIEW DETAILS OPEN VOENTER ACTIONS Y	BACK TO TOP GO TO GRID VIEW	
L lane			

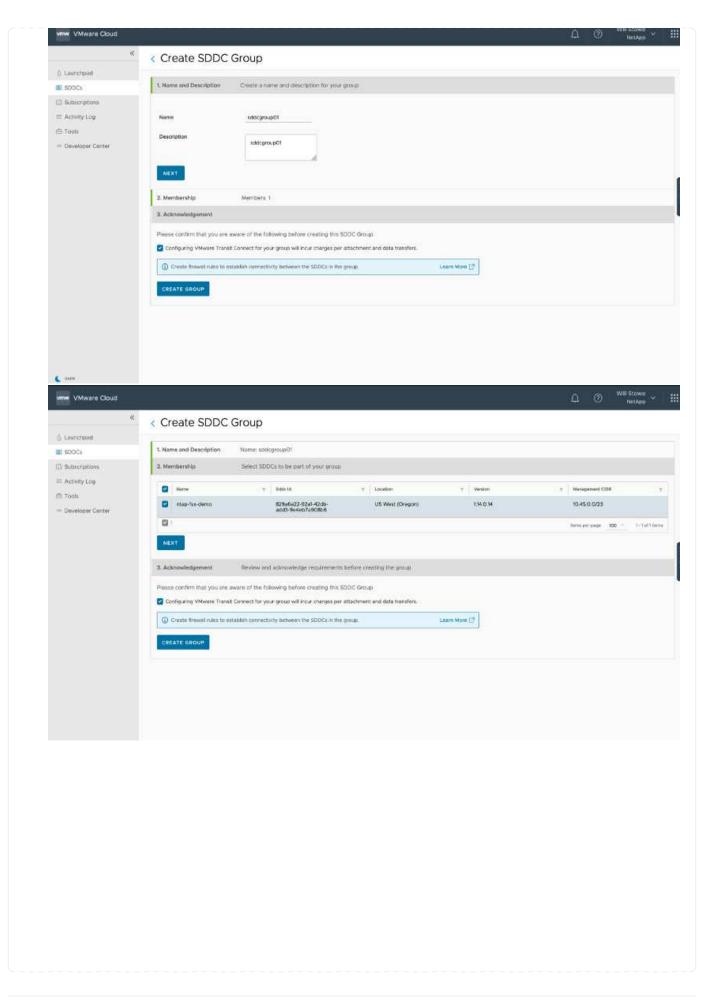
To connect VMware Cloud to FSx ONTAP, complete the following steps:

 With VMware Cloud deployment completed and connected to AWS VPC, you must deploy Amazon FSx for NetApp ONTAP into a new VPC rather than the original connected VPC (see the screenshot below). FSx (NFS and SMB floating IPs) is not accessible if it is deployed in the connected VPC. Keep in mind that ISCSI endpoints like Cloud Volumes ONTAP work just fine from the connected VPC.



2. Deploy an additional VPC in the same region, and then deploy Amazon FSx for NetApp ONTAP into the new VPC.

Configuration of an SDDC group in the VMware Cloud console enables the networking configuration options required to connect to the new VPC where FSx is deployed. In step 3, verify that "Configuring VMware Transit Connect for your group will incur charges per attachment and data transfers" is checked, and then choose Create Group. The process can take a few minutes to complete.



vmm VMware Cloud		Ω ③ ^{Will Stowe} ∽
6.	< Create SDDC Group	
6. Launchpad		
SDDC1	1. Name and Description Name: sddcgroup01	
C Subscriptions	2. Membership Members 1	
= Activity Log	3. Acknowledgement	
i Tools - Developer Center	Please confirm that you are aware of the following before creating this SDDC Group. Configuring VMwere Transit Connect for your group will incur charges per attachment and deta transfers.	
	🕞 Create frewst ruits to establish connectivity between the SDDCs in the group.	
	CREATE GROUP	
C DADA		

3. Attach the newly created VPC to the just created SDDC group. Select the External VPC tab and follow the instructions for attaching an External VPC to the group. This process can take 10 to 15 minutes to complete.

Kell SDDC Group Actions SSDCs Summary vCenter Linking Exect Connect External VPC External TBW Routing Support Subscriptions Activity Log Tools	ଟ ଲ	📀 🔒 🕫 https://vnc.umwate.com/corecte/vddcs/groups/Tec2c621-1cb1-68fo-a9bb-366e4012fc5e/vpc-connectivity	☆ 2020
Actions Actions Sobocs Summary Meantar Linking Elifect Connect External VPC External TGW Routing Support Support Subscriptions Actions Actions Actions Activity Log Add Account Instance Instance Instance Tools AMS Account Instance Instance Instance Instance	mw VMware Cloud		년 ① Wil Stowe NetAop ~
Subscription Accroined External VPC External VPC External TBW Routing Support Source provide Amp Account Internal VPC External VPC Extern		« ALL SDDC Graup	
Spoce Summary VCenter Linking Direct Connect External TVPC External TSW Boulting Burpont Selections Add Account Indenter Indenter Indenter Indenter Tools AVX5 Account D Indenter Name Index Index Index	Launchpad		ACTIONS ~
Sensempoons Activity Log Tools AWS Account D T Resource Share Name T Mate T WPC Status	SODCs		
TOOIS AVVS Account D + Resource Share Name + Mate + Mate	Subscriptions		
	Activity Log	ADD ACCOUNT / HEHRINE	
	Tools	AWS Account D = Resource Street Note = Mate	······································
	Developer Center		

< → C ⋒	🛇 🛱 🕫 https://ms. unwex.com /correcte/addox/groups/1e/2=621-1.tz/-6869965-356640/2/c5e/xpc-connectivity	<u> </u>
vmw VMware Cloud		CP () Wil Stowe NetApp
🖞 Launchpad	C ALL SDC Group Subport Subport Summary vCenter Linking Direct Connect External VPC External TOW Routing Support	ACTION
🕮 Subscriptions 🏛 Activity Log	ADD ACCOUNT REDEVE	
🗇 Tools	AVVS Acount ID 7 Resource Norm Name 7 State	 WPC Bistus
··· Developer Center	UWC-Group-dc4930De+587-4165-b016-966176516866 ASSCCIATED	

4. As part of the external VPC process, you are prompted through the AWS console to a new shared resource via the Resource Access Manager. The shared resource is the AWS Transit Gateway managed by VMware Transit Connect.

Services V	Q. Search for services, features, manifestplace products, and does (Diption+S)	ninistrutor/WillStowegInstapp.com @ cloushones • Oriscon • Support
Resource Access × Manager × Shared by me Resource shares	AWS Resource Access Manager Share AXY5 resources with other AXY5 accounts.	Start sharing your AWS resources with other accounts
Shared resources Principals • Shared with me Resource Stores Shared resources Principals	How it works	Pricing AWS RAM is offered at no additional charge. There are no setup fees or upfront commetments.
Permissions library New Settings	Jis S Revents Access Hauger Thus secons a street on y accounty of the Constrained by one that Digitation of Data Solid fy Hindball Solid Street Street Revents Street Solid fy Hindball Solid Street Street Solid fy Hindball Solid Street Street Revents Street	More resources 2 What is AWS Resource Access Managen? Getting started Documentation.
	Use cases Manage resources centrally in a multi-	Your AZ ID AZ IDs provides a consistent way of identifying the location of a resource across all your accounts. This makes it easier for you to provision resources centrally in a single account and share them across multiple

Resource Access X Manager	Resource Access Manager > Shared with me : VMC-Group-dc49300e-f			1e-4560-853f-e2939c	1856b0c)
ihared by me	Details and information relating to this resource				
lesource shares		and the second se			
hared resources	Reject resource share Accept resour	te shure			
vincipals					
ihared with me	Summary				
Resource shares (1m/1400)	Name	Owner	Invitation date	Status	
Pared resources	VMC-Group-dc49300a-f5e7-6fa5-b016-	645453501102	2021/10/14	Pending	
vincipals.	ae5176a1e8a6				
	ARN	Rezeiver			
ermissions library New .	amawsramus- west-2:645453501102:resource- share/051a6fc5-0a1e-4560-853f- e2939d855b0c	139763910815			

5. Create the Transit Gateway Attachment.

		ame M
Details		
Name tag - optional Creates a tag with the key set to Name and the value set to the specif	ed string.	
my-transit-gateway-attachment		
Transit gateway ID Info		
tgw-001646b36ce07a2cb		
Attachment type Info		
VPC		
VPC attachment		
Select and configure your VPC attachment		
DNS support Info		
IPv6 support Info		
VPC ID Select the VPC to actach to the transit cateway		
vpc-0d1c764bcc495e805 (vmcfsx2.vpc)	•	

6. Back on the VMC Console, Accept the VPC attachment. This process can take approximately 10 minutes to complete.

«	K ALL SDDC Brougs				1	
Laurchpad	sddcgroup01				ACTI	ions 🛩
5DOCs	Summary eCenter Linking Direct Connect External VF	C External TGW Routing Supp	ort			
Subscriptions Activity Log						
≌ Tools - Developer Center	AWS Account ID T AWS Account ID T Resource share name : VW State : ASSOCATED ACCEPT REWOYE	ີ - Group: ທ່ວ48300::- ເຮັດ?- 41a5 1:016-ຂອດ176aໃນ	eŝu 6			×
	VPC IS VPC-Odfic764bcc493	 VINC on AWS Begion Ψ StellOS US West (Crisgon) 	Treask Galeway Attachment ID y topw-antach-Q24863369122657/054	Reutes		, T

- 7. While in the External VPC tab, click the edit icon in the Routes column and add in the following required routes:
 - A route for the floating IP range for Amazon FSx for NetApp ONTAP floating IPs.
 - A route for the floating IP range for Cloud Volumes ONTAP (if applicable).
 - A route for the newly created external VPC address space.

I All SDDC Simular Sufficiency Vicenter Linking Direct Compact External VPC External TGW Routing Support IS Subscriptions Activity Log Activity Log Sufficiency Vicenter Linking Direct Compact External VPC External TGW Routing Support IT Subscriptions Activity Log Developer Center Activity Compact Sufficiency Vicenter Linking Support If Tools Activity Compact Sufficiency Vicenter Linking Support If Tools Activity Compact Sufficiency Vicenter Vicenter Sufficiency Vicenter Vicent Vicenter Vicenter Vicenter Vicent Vicenter	ctions ~
E SDOCs Surmary Venter Livieng Dirsch Connect External VPC External TGW Reuting Support Subscriptions ANS Account ID : ANS Account ID : A Rute : Associated in the Account ID : Ans Account ID	
E Activity tog E Activity tog E Tools Developer Center Developer Center Develop	
AVX5 Account ID : Marine A	
😰 spc. Odic/64bcc405e805 US West (Oregon) 19# attach-0548536982667664 W88.13.255.024 🧷 AwaLA	
	A.E.

8. Finally, allow bidirectional traffic firewall rules for access to FSx/CVO. Follow these detailed steps for compute gateway firewall rules for SDDC workload connectivity.

re Coud			
н С	sddcgroup01		
(1997) 1		Edit Routes ×	
		Set of routes pointing to this attachment	
		The profiles can be detinded by comma, space or a new line \$ 1004, 0 mild	
		CANCEL	

9. After the firewall groups are configured for both the Management and Compute gateway, the vCenter can be accessed as follows:

4	The SODC will expire	in 54 days.	LEARN	NORE							SCAL	LEVP
	< ALL SEDCa								Ī	OPEN VCENTER	ACTION	15 ~
	ntap-fsx-de	emo∣v⊮	K on AV	rs sooc 🦁 us west (Cregon)							
	Summery Networking	s & Security	Add	Oris Maintenanc	# Troubles	hootina Settinas	Support					
							and the second					
	Overview	Gatev	vay F	irewall								1
nter.	Network	Manager	mant Ga	neway Comput	e Gateway							
	Segments	and the start of the										
	VPN									95.9	18T	77/11.5
	NAT Tier-1 Gateways	+ ADD	RULE	(C) 86000 50	and in	DELETE			Filte	er by Name, Path and re	ore	. 7
	Transit Connect	1		Name	1D	Sources	Destinations	Services	Applied To	Action		
	Security	14	Ô	alow internet fro.	1019	#1 vmc-sddc	ADy	Any	All Uplinks	Alow -	•	9. TES.
	Gateway Firewall	1.1		C Real Charles and C	1710	22 vmc-addc-2			10000000000			r. (1995)
	Distributed Firewall	4	n	allow VMC to VPC	1017	mc-sade	Connecte .	Any	At uptres	· Alow -		1 22
	Inventory		1,47	and the second	1910	vmc-addc-2		100	1942	- Harn		相對化
	Groups Services	1	É.	allow VPC to VMC	10/6	Connecte.	www.eddc	Any	All Uplims	· Allow		107
	Virtual Machines	3:	<u> </u>	and which the state	iu ie	80,27777777	0.000 00000000	102	Contraction of the second	• 1001		1. 1997.
	Tools	1		allow to vmcha2	1022	TT vine-adde	83 vmdsx2.v.	Any	All Uplinies	 Allow – 		1 22
	IPEX					Uniterstate-2						
	Port Mirroring	-		all from vinctaic2	1023	12 vnctsv2.v.	📰 vmc-sddc-2	Any	At Uplinks	 Allow 		# 新祥
	System						83 vmc sddc					
	DN5	3		Default VTI Rule	1012	Any.	Ariy	Arty	VPN Tunnel In.	· Allow ·		# 四
	DHCP Clabel Cardin when	4		12121210102122		Any	Any	Any	Ali uphriks	n a Variancia I	-	
	Global Configuration Public IPs	1		Default Uples Ru.		AND STORES		208	An opened	• Drop -	00	
		-										

The next step is to verify that Amazon FSx ONTAP or Cloud Volumes ONTAP is configured depending on your requirements and that the volumes are provisioned to offload storage components from vSAN to optimize the deployment.

Deploy and configure the Virtualization Environment on Azure

As with on-premises, planning Azure VMware Solution is critical for a successful production-ready environment for creating VMs and migration.

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

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

To use Azure VMware Solution, first register the resource provider within the identified subscription:

- 1. Sign in to the Azure portal.
- 2. On the Azure portal menu, select All Services.
- 3. In the All Services dialog box, enter the subscription and then select Subscriptions.
- 4. To view, select the subscription from the subscription list.
- 5. Select Resource Providers and enter Microsoft.AVS into the search.
- 6. If the resource provider is not registered, select Register.

Home > Subscriptions >					
Subscriptions « NetApp (cloudcontrolproduction.com)	Subscription		Resource providers		×
+ Add 📋 Manage Policies	P Search (Ctrl+/)		< Register 🏷 Unregister 🕐 Refresh		
View list of subscriptions for which you have role-based access control (R8AC) permissions	(*) Resource groups	^	₽ AVS		×
to manage Azure resources. To view subscriptions for which you have billing	III Resources				
access, click here Showing subscriptions in NetApp directory.	Preview features		Provider	Status	
Don't see a subscription? Switch directories	🗮 Usage + quotas		Microsoft.AVS	Registering	
My role ① Status ③	Policies				
8 selected V 3 selected V	🐖 Management certificates				
Apply	A My permissions				
Showing 1 of 1 subscriptions global Show only subscriptions selected in the	SE Resource providers				
subscriptions filter ①	m Deployments				
P Search	Properties				
Subscription name 14	A Resource locks				
< Previous 1 V Next >	Support + troubleshooting	~			

Provider	Status
Microsoft.OperationsManagement	Registered
Microsoft.Compute	Registered
Microsoft.ContainerService	Registered
Microsoft.ManagedIdentity	🖉 Registered
Microsoft.AVS	Registered
Microsoft.OperationalInsights	🧿 Registered
Microsoft.GuestConfiguration	Registered

- 7. After the resource provider is registered, create an Azure VMware Solution private cloud by using the Azure portal.
- 8. Sign in to the Azure portal.
- 9. Select Create a New Resource.
- 10. In the Search the Marketplace text box, enter Azure VMware Solution and select it from the results.
- 11. On the Azure VMware Solution page, select Create.
- 12. From the Basics tab, enter the values in the fields and select Review + Create.

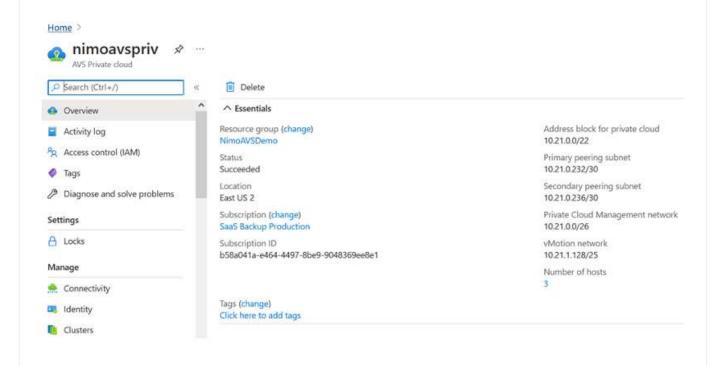
Notes:

- For a quick start, gather the required information during the planning phase.
- Select an existing resource group or create a new resource group for the private cloud. A resource group is a logical container in which the Azure resources are deployed and managed.
- Make sure the CIDR address is unique and does not overlap with other Azure Virtual Networks or onpremises networks. The CIDR represents the private cloud management network and is used for the cluster management services, such as vCenter Server and NSX-T Manager. NetApp recommends using a /22 address space. In this example, 10.21.0.0/22 is used.

Prerequisities "Basics Tags	Review and Create	
Project details		
Subscription * ②	SaaS Backup Production	×
Resource group * 💿	(New) NimoAVSDemo	~
	Create new	
Private cloud details		
Resource name * 💿	nimoaispriv	Ŷ
Location * 💿	(US) East US 2	~~
Size of host * 💿	AV36 Trial	~
Number of hosts * ③	0	3
	Find	out how many hosts you nee
	There is no metering for the selected subscript data to display.	ion, region, and SKU. No cost
CIDR address block		
	d for cluster management. Make sure these are unique tworks.	e and do not overlap with an
other Azure vnets or on-premise ne		

The provisioning process takes approximately 4–5 hours. After the process is complete, verify that the deployment was successful by accessing the private cloud from the Azure portal. A status of Succeeded is displayed when the deployment is complete.

An Azure VMware Solution private cloud requires an Azure Virtual Network. Because Azure VMware Solution doesn't support on-premises vCenter, additional steps are required to integrate with an existing on-premises environment. Setting up an ExpressRoute circuit and a virtual network gateway is also required. While waiting for the cluster provisioning to complete, create a new virtual network or use an existing one to connect to Azure VMware Solution.



To create a new Azure Virtual Network (VNet), select the Azure VNet Connect tab. Alternatively, you can create one manually from the Azure portal by using the Create Virtual Network wizard:

- 1. Go to Azure VMware Solution private cloud and access Connectivity under the Manage option.
- 2. Select Azure VNet Connect.
- 3. To create a new VNet, select the Create New option.

This feature allows a VNet to be connected to the Azure VMware Solution private cloud. The VNet enables communication between workloads in this virtual network by automatically creating required components (for example, jump box, shared services such as Azure NetApp Files, and Cloud Volume ONTAP) to the private cloud created in Azure VMware Solution over ExpressRoute.

Note: The VNet address space should not overlap with the private cloud CIDR.

₽ Search (Ctrl+/)	«	🖫 Save 🕐 Refresh			
Overview	^	Azure vNet connect Settings	ExpressRoute	Public IP	
Activity log					
Access control (IAM)		This is an optional feature that allows private cloud. A vNet enables the cor			
Tags		Jumpbox) to the private cloud create subnet 'GatewaySubnet' should be se	d in Azure VMware	Solution over ExpressRoute. Or	nly a vNet with a valid
Diagnose and solve problems		address space does not overlap with network.			
Settings		Virtual network			~
A Locks			Create new		
Manage		Address block for vnet	3K		
🌨 Connectivity		Address block for private cloud	10.21.0.0/2	22	C
Identity					
Clusters					

4. Provide or update the information for the new VNet and select OK.

Azur defa 172.1	e VMware Solution over a ult address range and sub 16.0.0/16), Step 2: Add a s	he communication between workloads in this virtual n an Express route. A default address range and a subne anet of this virtual network, follow these steps. Step 1: subnet under "Subnets" with the name as "GatewaySu re about virtual networks Cf	t is selected for this virtual network. For changing Change the "Address Range" to desired range (e.e.	the g.
Nam	ie *	nimoavspriv-vnet		
Add	ress space			
The	virtual network's address	space specified as one or more address prefixes in CIE	R notation (e.g. 10.0.0.0/16).	
	Address range	Addresses	Overlap	
	172.24.0.0/16	172.24.0.4 - 172.24.255.254 (65531 addresses)	None	Ē
		(0 Addresses)	None	
Sub	nets			
The:	subnet's address range in	CIDR notation (e.g. 10.0.0.0/24). It must be contained	by the address space of the virtual network.	
	Subnet name	Address range	Addresses	
	GatewaySubnet	172.24.0.0/24	172.24.0.4 - 172.24.0.254 (251 addresses)	Û
	영양 전 전 이상 방법 전 전 것 같은 것 같은 것			

The VNet with the provided address range and gateway subnet is created in the designated subscription and resource group.

If you create a VNet manually, create a virtual network gateway with the appropriate SKU and ExpressRoute as the gateway type. After the deployment is complete, connect the ExpressRoute connection to the virtual network gateway containing Azure VMware Solution private cloud using the authorization key. For more information, see Configure networking for your VMware private cloud in Azure.

 (\mathbf{i})

Validate the network connect and access to Azure VMware Solution private cloud

Azure VMware Solution does not allow you to manage a private cloud with on-premises VMware vCenter. Instead, jump host is required to connect to the Azure VMware Solution vCenter instance. Create a jump host in the designated resource group and sign in to the Azure VMware Solution vCenter. This jump host should be a Windows VM on the same virtual network that was created for connectivity and should provide access to both vCenter and the NSX Manager.

Creat	e a vi	rtual mad	chine					
Basics	Disks	Networking	Management	Advanced	Tags	Review + create		
image. C	omplete t		n Review + create			zure marketplace or us nachine with default par		
Project	details							
	e subscrip all your re		deployed resource	s and costs. Us	e resou	rce groups like folders	to organize	and
Subscrip	tion * 💿		SaaS Bad	kup Production				~
- 1	Resource	group * 🕕	NimoAV	Demo				\sim
	e details sachine na	ime * 🛈	nimA/\$8	н				~
Region *	• •		(US) East	US 2				~
vailabil	ity option:	0	No infra	structure redunc	iancy re	quired		~
mage *	0			- 15 F (+ F F F (+ F F F F F F F F F F F F	2 R2 Da	tacenter - Gen2		\sim
Azure Sp	pot instanc	0 N	See all imi	City.				
Size * (D.		The party of the second s		us, 8 Gi	8 memory (\$130.67/mo	nth)	~
			See all size	es .				

After the virtual machine is provisioned, use the Connect option to access RDP.

Virtual machine	st …
	▲ To improve security, enable just-in-time access on this VM, \rightarrow
Overview	
Activity log	RDP SSH BASTION
Access control (IAM)	Connect with RDP
	connect with KDP
Tags	To connect to your virtual machine via RDP, select an IP address, optionally change the port number, and download the
	To connect to your virtual machine via RDP, select an IP address, optionally change the port number, and download the RDP file.
Diagnose and solve problems	
Diagnose and solve problems	RDP file.
Diagnose and solve problems	RDP file. IP address *
 Diagnose and solve problems Settings Networking 	RDP file. IP address * Public IP address (52:138:103:135)
 Diagnose and solve problems Settings Networking 	RDP file. IP address * Public IP address (52:138.103.135) Port number *

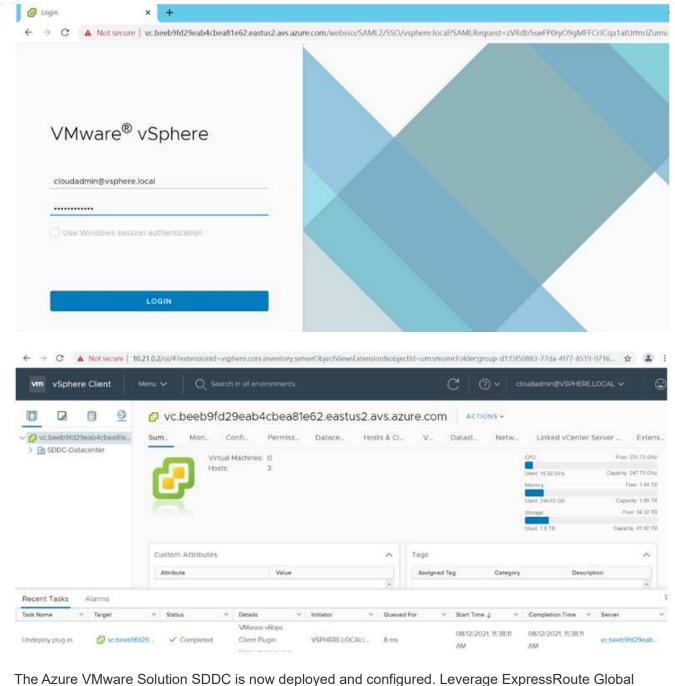
Sign in to vCenter from this newly created jump host virtual machine by using the cloud admin user . To access the credentials, go to the Azure portal and navigate to Identity (under the Manage option within the private cloud). The URLs and user credentials for the private cloud vCenter and NSX-T Manager can be copied from here.

Search (Ctrl+/)	« Login credentials		
Access control (IAM)	 vCenter credentials 		
🖉 Tags	Web client URL ①	https://10.21.0.2/	D
Diagnose and solve problems	Admin username ③	cloudadmin@vsphere.local	D
Settings	Admin password 🛈	D	
A Locks	Certificate thumbprint ①	AE26B15A5CE38DC069D35F045F088CA6343475EC	D
Manage	NSX-T Manager credentials		
nectivity	Web client URL ①	https://10.21.0.3/	D
💐 Identity	Admin username ①	admin	D
Clusters	Admin username ()	Land State of Control	чц
Placement policies (preview)	Admin password ③		
+ Add-ons	Certificate thumbprint ①	B2B722EA683958283EE159007246D5166D0509D3	Ð

In the Windows virtual machine, open a browser and navigate to the vCenter web client URL ("https://10.21.0.2/") and use the admin user name as **cloudadmin@vsphere.local** and paste the copied password. Similarly, NSX-T manager can also be accessed using the web client URL ("https://10.21.0.3/") and use the admin user name and paste the copied password to create new segments or modify the existing tier gateways.



The web client URLs are different for each SDDC provisioned.



The Azure VMware Solution SDDC is now deployed and configured. Leverage ExpressRoute Global Reach to connect the on-premises environment to Azure VMware Solution private cloud. For more information, see Peer on-premises environments to Azure VMware Solution.

Deploy and configure the Virtualization Environment on Google Cloud Platform (GCP)

As with on-premises, planning Google Cloud VMware Engine (GCVE) is critical for a successful production-ready environment for creating VMs and migration.

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

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

To configure a GCVE environment on GCP, login to the GCP console and access the VMware Engine portal.

Click on the "New Private Cloud" button and enter the desired configuration for the GCVE Private Cloud. On "Location", make sure to deploy the private cloud in the same Region/Zone where CVS/CVO is deployed, to ensure the best performance and lowest latency.

Pre-requisites:

- Setup VMware Engine Service Admin IAM role
- Enable VMWare Engine API access and node quota
- Make sure that the CIDR range doesn't overlap with any of your on-premises or cloud subnets. The CIDR range must be /27 or higher.

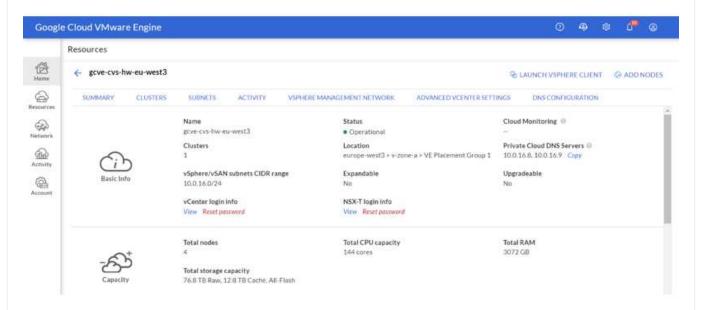
	 Create Private Cloud ① 	
Ê	Private Cloud name *	
Home	NiMoGCVE	
esources	Location *	
A	us-east4 > v-zone-a > VE Placement Group 2	•
4etwork	Node type *	
A	ve1-standard-72	
Activity (Q)	2x2.6 GHz, 36 Cores (72 HT), 768 GB RAM 19.2 TB Raw, 3.2 TB Cache (All-Flash)	
Account	Node count *	
	3	
	(3to3)	
	vSphere/vSAN subnets CIDR range *	
	192.168.100.0	/ 22 •
	IP Range: 192.168.100.0 - 192.168.103.255	
	HCX Deployment Network CIDR range	
	192.168.104.0	/ 26 •
	IP Range: 192.168.104.0 - 192.168.104.63	

Once the Private Cloud is provisioned, configure private access to the Private Cloud for high-throughput and low-latency data-path connection.

This will ensure that the VPC network where Cloud Volumes ONTAP instances are running is able to communicate with the GCVE Private Cloud. To do so, follow the GCP documentation. For the Cloud Volume Service, establish a connection between VMware Engine and Cloud Volumes Service by performing a one-time peering between the tenant host projects. For detailed steps, follow this link.

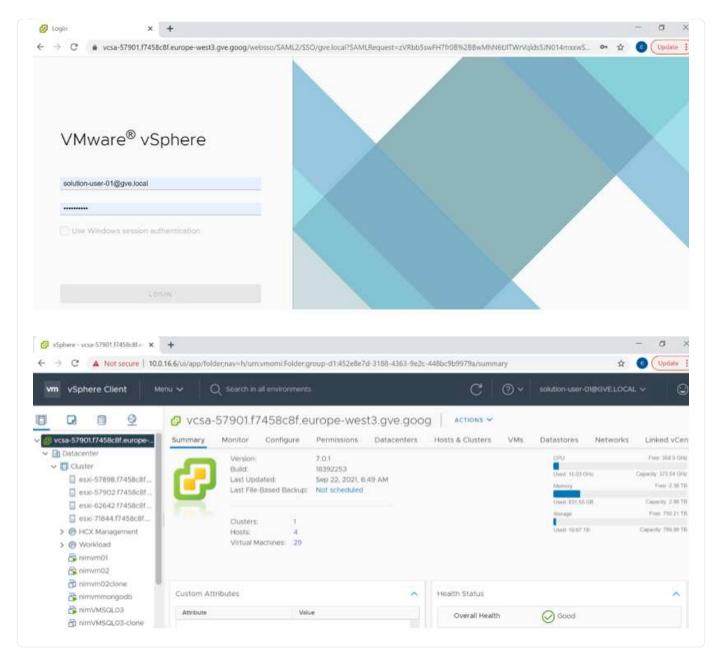
Tenant P 🕅 🗍 🖨	Service	÷	Region	$\frac{1}{2}$	Routing Mode	$\frac{d}{T}$	Peered Project ID 🌐	Peered VPC	÷,	VPC Peering Sta ≑	Region Status
ke841388caa56b	VPC Network		europe-west3		Global		cv-performance-te	cloud-volumes-vpc		 Active 	Connected
jbd729510b3ebbf	NetApp CVS		europe-west3		Global		y2b6c17202af6dc	netapp-tenant-vpc		Active	 Connected

Sign in to vcenter using the CloudOwner@gve.local user. To access the credentials, go to the VMware Engine portal, Go to Resources, and select the appropriate private cloud. In the Basic info section, click the View link for either vCenter login info (vCenter Server, HCX Manager) or NSX-T login info (NSX Manager).



In a Windows virtual machine, open a browser and navigate to the vCenter web client URL ("https://10.0.16.6/") and use the admin user name as CloudOwner@gve.local and paste the copied password. Similarly, NSX-T manager can also be accessed using the web client URL ("https://10.0.16.11/") and use the admin user name and paste the copied password to create new segments or modify the existing tier gateways.

For connecting from an on-premises network to VMware Engine private cloud, leverage cloud VPN or Cloud Interconnect for appropriate connectivity and make sure the required ports are open. For detailed steps, follow this link.



Deploy NetApp Cloud Volume Service supplemental datastore to GCVE

Refer Procedure to deploy supplemental NFS datastore with NetApp CVS to GCVE

NetApp Storage in Hyperscaler Clouds

NetApp Storage options for Public Cloud Providers

Explore the options for NetApp as storage in the three major hyperscalers.

AWS / VMC

AWS supports NetApp storage in the following configurations:

- FSx ONTAP as guest connected storage
- Cloud Volumes ONTAP (CVO) as guest connected storage
- FSx ONTAP as a supplemental NFS datastore

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

Azure / AVS

Azure supports NetApp storage in the following configurations:

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

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

GCP / GCVE

Google Cloud supports NetApp storage in the following configurations:

- Cloud Volumes ONTAP (CVO) as guest connected storage
- · Cloud Volumes Service (CVS) as guest connected storage
- · Cloud Volumes Service (CVS) as a supplemental NFS datastore

View the detailed guest connect storage options for GCVE.

Read more about NetApp Cloud Volumes Service datastore support for Google Cloud VMware Engine (NetApp blog) or How to use NetApp CVS as datastores for Google Cloud VMware Engine (Google blog)

TR-4938: Mount Amazon FSx for ONTAP as a NFS datastore with VMware Cloud on AWS

This document outlines how to mount Amazon FSx for ONTAP as a NFS datastore with VMware Cloud on AWS.

Niyaz Mohamed, NetApp

Introduction

Every successful organization is on a path of transformation and modernization. As part of this process, companies typically use their existing VMware investments to leverage cloud benefits and exploring how to migrate, burst, extend, and provide disaster recovery for processes as seamlessly as possible. Customers migrating to the cloud must evaluate the use cases for elasticity and burst, data-center exit, data-center consolidation, end-of-life scenarios, mergers, acquisitions, and so on.

Although VMware Cloud on AWS is the preferred option for the majority of the customers because it delivers unique hybrid capabilities to a customer, limited native storage options have restricted its usefulness for

organizations with storage-heavy workloads. Because storage is directly tied to hosts, the only way to scale storage is to add more hosts, which can increase costs by 35-40% or more for storage intensive workloads. These workloads need additional storage and segregated performance, not additional horsepower, but that means paying for additional hosts. This is where the recent integration of FSx for ONTAP comes in handy for storage and performance intensive workloads with VMware Cloud on AWS.

Let's consider the following scenario: a customer requires eight hosts for horsepower (vCPU/vMem), but they also have a substantial requirement for storage. Based on their assessment, they require 16 hosts to meet storage requirements. This increases the overall TCO because they must buy all that additional horsepower when all they really need is more storage. This is applicable for any use case, including migration, disaster recovery, bursting, dev/test, and so on.

This document walks you through the steps necessary to provision and attach FSx for ONTAP as a NFS datastore for VMware Cloud on AWS.



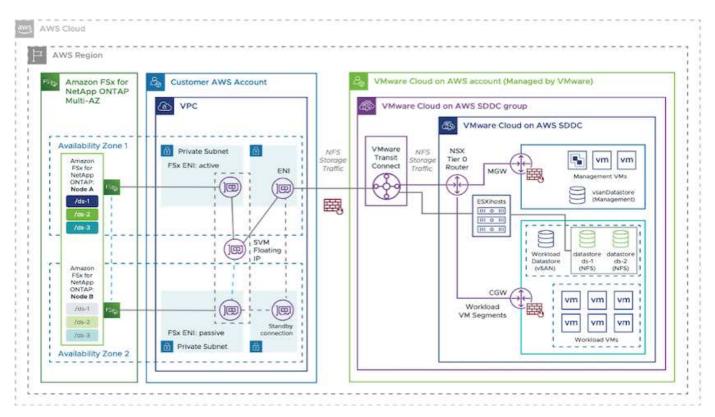
This solution is also available from VMware. Please visit the VMware Cloud Tech Zone for more information.

Connectivity options

 (\mathbf{i})

VMware Cloud on AWS supports both multi-AZ and single-AZ deployments of FSx for ONTAP.

This section describes the high-level connectivity architecture along with the steps needed to implement the solution to expand the storage in a SDDC cluster without the need for adding additional hosts.



The high-level deployment steps are as follows:

- 1. Create Amazon FSx for ONTAP in a new designated VPC.
- 2. Create an SDDC group.

- 3. Create VMware Transit Connect and a TGW attachment.
- 4. Configure routing (AWS VPC and SDDC) and security groups.
- 5. Attach an NFS volume as a datastore to the SDDC cluster.

Before you provision and attach FSx for ONTAP as a NFS datastore, you must first set up a VMware on Cloud SDDC environment or get an existing SDDC upgraded to v1.20 or above. For more information, see the Getting Started With VMware Cloud on AWS.



FSx for ONTAP is not currently supported with stretched clusters.

Conclusion

This document covers the steps necessary to configure Amazon FSx for ONTAP with VMware cloud on AWS. Amazon FSx for ONTAP provides excellent options to deploy and manage application workloads along with file services while reducing the TCO by making data requirements seamless to the application layer. Whatever the use case, choose VMware Cloud on AWS along with Amazon FSx for ONTAP for rapid realization of cloud benefits, consistent infrastructure, and operations from on-premises to AWS, bidirectional portability of workloads, and enterprise-grade capacity and performance. It is the same familiar process and procedures used to connect storage. Remember, it is just the position of the data that changed along with new names; the tools and processes all remain the same, and Amazon FSx for ONTAP helps to optimize the overall deployment.

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

Amazon FSX for Ontap VMware Cloud

NetApp Guest Connected Storage Options for AWS

AWS supports guest connected NetApp storage with the native FSx service (FSx ONTAP) or with Cloud Volumes ONTAP (CVO).

FSx ONTAP

Amazon FSx for NetApp ONTAP is a fully managed service that provides highly reliable, scalable, highperforming, and feature-rich file storage built on NetApp's popular ONTAP file system. FSx for ONTAP combines the familiar features, performance, capabilities, and API operations of NetApp file systems with the agility, scalability, and simplicity of a fully managed AWS service.

FSx for ONTAP provides feature-rich, fast, and flexible shared file storage that's broadly accessible from Linux, Windows, and macOS compute instances running in AWS or on premises. FSx for ONTAP offers high-performance solid state drive (SSD) storage with submillisecond latencies. With FSx for ONTAP, you can achieve SSD levels of performance for your workload while paying for SSD storage for only a small fraction of your data.

Managing your data with FSx for ONTAP is easier because you can snapshot, clone, and replicate your files with the click of a button. In addition, FSx for ONTAP automatically tiers your data to lower-cost, elastic storage, lessening the need for you to provision or manage capacity.

FSx for ONTAP also provides highly available and durable storage with fully managed backups and support for cross-Region disaster recovery. To make it easier to protect and secure your data, FSx for ONTAP supports popular data security and antivirus applications.

FSx ONTAP as guest connected storage

Configure Amazon FSx for NetApp ONTAP with VMware Cloud on AWS

Amazon FSx for NetApp ONTAP files shares and LUNs can be mounted from VMs that are created within the VMware SDDC environment at VMware Cloud at AWS. The volumes can also be mounted on the Linux client and mapped on the Windows client using the NFS or SMB protocol, and LUNS can be accessed on Linux or Windows clients as block devices when mounted over iSCSI. Amazon FSx for the NetApp ONTAP file system can be set up quickly with the following steps.



Amazon FSx for NetApp ONTAP and VMware Cloud on AWS must be in the same availability zone to achieve better performance and avoid data transfer charges between availability zones.

To create and mount Amazon FSx for NetApp ONTAP file system, complete the following steps:

- 1. Open the Amazon FSx console and choose Create file system to start the file system creation wizard.
- 2. On the Select File System Type page, choose Amazon FSx for NetApp ONTAP, and then choose Next. The Create File System page appears.

Step 1 Select file system type	Select file system type			^ (
Step 2 Specify file	File system options			
system details Step 3 Review and create	Amazon F5x for NetApp ONTAP	Amazon FSx for Windows File Server FSX Amazon FSx for Windows File Server	Amazon FSx for Lustre	
		Select file system type		

1. In the Networking section, for Virtual Private Cloud (VPC), choose the appropriate VPC and preferred subnets along with the route table. In this case, vmcfsx2.vpc is selected from the dropdown.

eation method	
 Quick create Use recommended best-practice configurations. Most configuration options can be changed after the file system is created. 	Standard create You set all of the configuration options, including specifying performance, networking, security, backups, and maintenance.

1. For the creation method, choose Standard Create. You can also choose Quick Create, but this document uses the Standard create option.

File system name - optional Info		
vmcfsxval2		
Maximum of 256 Unicode letters, whitespa	e, and numbers, plus + - = : /	
SSD storage capacity Info		
1024 0		
Minimum 1024 GB; Maximum 192 TB.		
Provisioned SSD IOPS Amazon FSx provides 3 IOPS per GB of stor needed.	ige capacity. You can also provision additional SSD IOPS a	5
 Automatic (3 IOPS per GB of SSD 	storage)	
User-provisioned		
Throughput capacity Info The sustained speed at which the file server burst to higher speeds for periods of time.	hosting your file system can serve data. The file server ca	n also

1. In the Networking section, for Virtual Private Cloud (VPC), choose the appropriate VPC and preferred subnets along with the route table. In this case, vmcfsx2.vpc is selected from the dropdown.

Virtual Private Cloud (VPC) Info Specify the VPC from which your file system is accessible.	
vmcfsx2.vpc vpc-0d1c764bcc495e805	
VPC Security Groups Info Specify VPC Security Groups to associate with your file system's network interface.	
Choose VPC security group(s)	
5g-018896ea218164ccb (default) ×	
Preferred subnet Info Specify the preferred subnet for your file system.	
subnet02.sn subnet-013675849a5b99b3c (us-west-2b)	
Standby subnet	
subnet01.sn subnet-0ef956cebf539f970 (us-west-2a)	
VPC route tables Specify the VPC route tables associated with your file system.	
VPC's default route table	
Select one or more VPC route tables	
Endpoint IP address range Specify the IP address range in which the endpoints to access your file system will be created	
No preference	
Select an IP address range	



In the Networking section, for Virtual Private Cloud (VPC), choose the appropriate VPC and preferred subnets along with the route table. In this case, vmcfsx2.vpc is selected from the dropdown.

1. In the Security & Encryption section, for the Encryption Key, choose the AWS Key Management Service (AWS KMS) encryption key that protects the file system's data at rest. For the File System Administrative Password, enter a secure password for the fsxadmin user.

ncryption key Info NS Key Management Service (KMS) encryption key that protects	your file system data at re	st.
aws/fsx (default)		•
Description	Account	KMS key ID
Default master key that protects my FSx resources when no other key is defined	139763910815	72745367-7bb0-499c- acc0-4f2c0a80e7c5
le system administrative password ssword for this file system's "fsxadmin" user, which you can use t	o access the ONTAP CLI o	r REST API.
le system administrative password issword for this file system's "fsxadmin" user, which you can use t Don't specify a password	to access the ONTAP CLI o	r REST API.
issword for this file system's "fsxadmin" user, which you can use t	o access the ONTAP CLI o	r REST API.
assword for this file system's "fsxadmin" user, which you can use t Don't specify a password	o access the ONTAP CLI o	r REST API.
 assword for this file system's "fsxadmin" user, which you can use to Don't specify a password Specify a password 	o access the ONTAP CLI o	r REST API.
assword for this file system's "fsxadmin" user, which you can use to Don't specify a password Specify a password assword	o access the ONTAP CLI o	r REST API.

 In virtual machine and specify the password to use with vsadmin for administering ONTAP using REST APIs or the CLI. If no password is specified, a fsxadmin user can be used for administering the SVM. In the Active Directory section, make sure to join Active Directory to the SVM for provisioning SMB shares. In the Default Storage Virtual Machine Configuration section, provide a name for the storage in this validation, SMB shares are provisioned using a self-managed Active Directory domain.

Storage virtual machine name	
vmcfsxval2svm	
SVM administrative password Password for this SVM's "vsadmin" user, which you can use to access the ONTAP CLI or REST API.	
O Don't specify a password	
O Specify a password	
Password	
•••••	
Confirm password	

Active Directory Joining an Active Directory enables access from Windows and MacOS clients over the SMB protocol.	
 Do not join an Active Directory 	
Join an Active Directory	

1. In the Default Volume Configuration section, specify the volume name and size. This is an NFS volume. For Storage Efficiency, choose Enabled to turn on the ONTAP storage efficiency features (compression, deduplication, and compaction) or Disabled to turn them off.

Volume name	
vol1	
Maximum of 203 alphanumeric characters, plus	
Junction path	
/vol1	
The location within your file system where your volume will be mounted.	
Volume size	
1024	0
Minimum 20 MiB; Maximum 104857600 MiB	
Storage efficiency Select whether you would like to enable ONTAP storage efficiencies on your volume: deduplicatio compression, and compaction.	n,
 Enabled (recommended) 	
O Disabled	
Capacity pool tiering policy You can optionally enable automatic tiering of your data to lower-cost capacity pool storage.	
Auto	v

- 1. Review the file system configuration shown on the Create File System page.
- 2. Click Create File System.

	FSx > File sys	stems						
File systems	File syste	ms (3)			C Attach	Actions ¥	Create file sys	tem
Backups	Q. Filter fi	le systems					< 1 >	0
ONTAP								
Storage virtual machines Volumes	File syst nam	em File syst	em ID 🔺	File system type ⊽	Status	v Deployment type	Storage	7
Windows File Server	O fsm	tapcifs 🗗	8399be9c1f9f	ONTAP	⊘ Available	Multi-AZ	SSD	
Lustre Data repository tasks		fs-040ea	cc5d0ac31017		0		521A1	
	O vmc	fsxval2	0447ebd6082aa	ONTAP	⊘ Available	Multi-AZ	SSD	
FSx on Service Quotas [2]	O fsxn	tapsql 🗗	944700008234	ONTAP	Available	Multi-AZ	SSD	
Network & security Ad	ministration	Storage virt	tual machines	Volu	imes Backi	ips Tags		
Storage virtual machir	nes (SVMs)	(2)	C	Acti	ons 🔻 🔽 Ci	eate storage vir	tual machin	e
Q Find storage virtual mac	hines					<	1 >	0
SVM name 🛛	SVM ID	V	Status 🔻	Crea	ation time	▲ Act	ive Directory	1 5
fsxsmbtesting01	svm-075dcfb	e2cfa2ece9	⊘ Created	202	1-10-19 15:17:08	SUTC FSX	TESTING.LO	CAL
				200	:00			
vmcfsxval2svm		76341561212	⊘ Created		1-10-15 15:16:54	ч итс		
Storage virtual machine xsmbtesting01	es 🗦 svm-075	dcfbe2cfa2ece9	Created	202 +01:	1-10-15 15:16:54	UTC -	Upd	ate
> Storage virtual machine	es 🗦 svm-075	dcfbe2cfa2ece9	Created	202 +01:	1-10-15 15:16:54	•	Upd	ate
Storage virtual machine xsmbtesting01	es 🗦 svm-075	dcfbe2cfa2ece9 75dcfbe Creation time	Created	202 +01: ce9)	1-10-15 15:16:54 :00 Active D	Delete	Upd	ate
Storage virtual machine xsmbtesting01 Summary	es 🗦 svm-075	dcfbe2cfa2ece9 75dcfbe	Created	202 +01: ce9)	1-10-15 15:16:54 :00 Active D	Delete	Upd	ate
Storage virtual machine SumbtestingO1 Summary SVM ID svm-075dcfbe2cfa2ece9	es 🗦 svm-075	dcfbe2cfa2ece9 75dcfbe Creation time	Created 2cfa2e	202 +01: ce9)	1-10-15 15:16:54 :00 Active D	Delete	Upd	ate
Storage virtual machine xsmbtesting01 Summary SVM ID svm-075dcfbe2cfa2ece9 SVM name	es 🗦 svm-075	dcfbe2cfa2ece9 75dcfbe Creation time 2021-10-19T1	Created 2cfa2e	202 +01: ce9)	1-10-15 15:16:54 :00 Active D FSXTES1 Net BIO:	Delete	Upd	ate
Storage virtual machine SumbtestingO1 Summary SVM ID svm-075dcfbe2cfa2ece9	es 🗦 svm-075	dcfbe2cfa2ece9 75dcfbe Creation time 2021-10-19T1 Lifecycle state ⓒ Created	Created 2cfa2e	202 +01: ce9)	1-10-15 15:16:54 :00 Active D FSXTEST Net BIO: FSXSMB	irectory 'ING.LOCAL S name TESTING01		ate
Storage virtual machine xsmbtesting01 Summary SVM ID svm-075dcfbe2cfa2ece9 I SVM name	es 🗦 svm-075	dcfbe2cfa2ece9 75dcfbe Creation time 2021-10-19T1 Lifecycle state	Created 2cfa2e	202 +01: ce9)	1-10-15 15:16:54 :00 Active D FSXTEST Net BIO: FSXSMB Fully qua	irectory 'ING.LOCAL		ate
Storage virtual machine Summary SVM ID Svm-075dcfbe2cfa2ece9 SVM name fsxsmbtesting01 UUID 4a50e659-30e7-11ec-ac4f-	es 🗦 svm-075	dcfbe2cfa2ece9 75dcfbe Creation time 2021-10-19T1 Lifecycle state ⊘ Created Subtype	Created 2cfa2e	202 +01: ce9)	1-10-15 15:16:54 :00 Active D FSXTEST Net BIO: FSXSMB Fully qua FSXTEST	irectory ING.LOCAL S name TESTING01 alified domain nam	me	ate
Storage virtual machine xsmbtestingO1 Summary SVM ID svm-075dcfbe2cfa2ece9 SVM name fsxsmbtesting01 UUID 4a50e659-30e7-11ec-ac4f- f3ad92a6a735	es 🗦 svm-075	dcfbe2cfa2ece9 75dcfbe Creation time 2021-10-19T1 Lifecycle state ⊘ Created Subtype	Created 2cfa2e	202 +01: ce9)	1-10-15 15:16:54 :00 Active D FSXTEST Net BIO: FSXSMB Fully qua FSXTEST	irectory TING.LOCAL S name TESTING01 allified domain nam TING.LOCAL	me	ate
Storage virtual machine Summary SVM ID Svm-075dcfbe2cfa2ece9 SVM name fsxsmbtesting01 UUID 4a50e659-30e7-11ec-ac4f-	es 🗦 svm-075	dcfbe2cfa2ece9 75dcfbe Creation time 2021-10-19T1 Lifecycle state ⊘ Created Subtype	Created 2cfa2e	202 +01: ce9)	1-10-15 15:16:54 :00 Active D FSXTEST Net BIO FSXSMB Fully qua FSXTEST Service a administ	irectory TING.LOCAL S name TESTING01 allified domain nam TING.LOCAL	me	

For more detailed information, see Getting started with Amazon FSx for NetApp ONTAP.

After the file system is created as above, create the volume with the required size and protocol.

- 1. Open the Amazon FSx console.
- 2. In the left navigation pane, choose File systems, and then choose the ONTAP file system that you want to create a volume for.
- 3. Select the Volumes tab.
- 4. Select the Create Volume tab.
- 5. The Create Volume dialog box appears.

For demo purposes, an NFS volume is created in this section that can be easily mounted on VMs running on VMware cloud on AWS. nfsdemovol01 is created as depicted below:

	2
File system	
fs-040eacc5d0ac31017 vmcfsxval2	
Storage virtual machine	
svm-095db076341561212 vmcfsxval2svm	
Volume name	
nfsdemovol01	
Maximum of 205 alphanumeric characters, plus	
Junction path	
/nfsdemovol01	
The location within your file system where your volume will be mounted.	
Volume size	
1024	(0
Minimum 20 MiB; Maximum 104857600 MiB	
실행 이 10 M <u>10</u> M 2010	a substant dark after that
Storage efficiency Select whether you would like to enable ONTAP storage efficiencies on yo compression, and compaction.	ur rouante, oeospinación,
Select whether you would like to enable ONTAP storage efficiencies on yo	ar source, coologication,
Select whether you would like to enable ONTAP storage efficiencies on yo compression, and compaction. C Enabled (recommended)	ar aquarre, cenagarcación,
Select whether you would like to enable ONTAP storage efficiencies on yo compression, and compaction.	

To mount the FSx ONTAP volume created in the previous step. from the Linux VMs within VMC on AWS SDDC, complete the following steps:

- 1. Connect to the designated Linux instance.
- 2. Open a terminal on the instance using Secure Shell (SSH) and log in with the appropriate credentials.
- 3. Make a directory for the volume's mount point with the following command:

```
$ sudo mkdir /fsx/nfsdemovol01
```

4. Mount the Amazon FSx for NetApp ONTAP NFS volume to the directory that is created in the previous step.

```
sudo mount -t nfs nfsvers=4.1,198.19.254.239:/nfsdemovol01
/fsx/nfsdemovol01
```

roat@ubuntu01:/fsx/nfsdemovol01# mount —t nfs 198.19.254.239:/nfsdemovol01 /fsx/nfsdemovol01

1. Once executed, run the df command to validate the mount.

Sphere - ubuntu01 - Summary ×	ubuntu01 ×	+	C
$\leftarrow \rightarrow \circ$	O A ≓ https://vcenter.sddc-52	2-37-127-104 vmwarevmc.com/ui/webconso	ie.html?vmid=vm-1003&vmName=ubuntu01&serv 🗠 🏠
📵 Getting Started 🛛 😑 EC2 Managem	nent Con 😸 New Tab		
ubuntu01			Enforce US Keyboard Layout View Fullscree
	root@ubuntu01:/fsk/n Filesystem tmofs /dev/mapper/ubuntu tmofs tmofs /dev/sda2. tmpfs 172.16.0.2:/nfsdemov 198.19.254.205/nfsd root@ubuntu01:/fsk/n nimewill.txt	IK-blocks Used Available 814396 1176 813220. vg-uBuntulv 15412168 3666428 10943132 4071960 0 4071950 5120 0 5120 4096 0 4096 993320 254956 675512 814392 4 814398 1951472 4241792 5719600 199616 512 95648 Hisdemovol01# cd /fs/ntsdemovol01/	25% / 0% //un/lock 0% //un/lock 0% //scgroup 2% //bock 1% //un/user/1000 4% //scv0testing01/nfgdemovo101

Mount FSx ONTAP volume on Linux client

To manage and map file shares on an Amazon FSx file system, the Shared Folders GUI must be used.

- 1. Open the Start menu and run fsmgmt.msc using Run As Administrator. Doing this opens the Shared Folders GUI tool.
- 2. Click Action > All tasks and choose Connect to Another Computer.
- 3. For Another Computer, enter the DNS name for the storage virtual machine (SVM). For example, FSXSMBTESTING01.FSXTESTING.LOCAL is used in this example.



Tp find the SVM's DNS name on the Amazon FSx console, choose Storage Virtual Machines, choose SVM, and then scroll down to Endpoints to find the SMB DNS name. Click OK. The Amazon FSx file system appears in the list for the Shared Folders.

Management IP address

198.19.254.9

198.19.254.9

SMB IP address

198.19.254.9

iSCSI IP addresses

10.222.2.224, 10.222.1.94

NFS IP address

Endpoints

Management DNS name

svm-075dcfbe2cfa2ece9.fs-040eacc5d0ac31017.fsx.us-

west-2.amazonaws.com

NFS DNS name

svm-075dcfbe2cfa2ece9.fs-040eacc5d0ac31017.fsx.us-

west-2.amazonaws.com

SMB DNS name

FSXSMBTESTING01.FSXTESTING.LOCAL

iSCSI DNS name

iscsi.svm-075dcfbe2cfa2ece9.fs-040eacc5d0ac31017.fsx.us-

west-2.amazonaws.com	D
	and the second s

1. In the Shared Folders tool, choose Shares in the left pane to see the active shares for the Amazon FSx file system.

🕈 🏟 📶 🙆 🕞 📓 🛅 就					
 Computer Management (FSXSMBTESTING01.FSXTESTING.LOCAL) System Tools Task Scheduler Event Viewer Shared Folders Shares Sessions Open Files Modulation of the session of the ses	Share Name	Folder Path C:\ C:\smbdernovol01 C:\testnimvol	Type Windows Windows Windows	# Client Connections 0 1 1 0	Descriptio
1. Now choose a new share and complete	the Create	a Shared Fol	der wizar	d.	
Create A Shared Folder Wizard				×	
Name, Description, and Settings Specify how people see and use this sha	re over the r	atuork		23	

Type information about the share for users. To modify how people use the content while offline, click Change.

hare path:	\\FSXSMBTESTING01.FSXTESTING.LOCAL\nimtestsm	b01
escription:		
ffine setting:	Selected files and programs available offline	Change
	-	

reate A Shared Folder Wizard		×
	Sharing was Successful	
	Status:	
22	You have successfully completed the Share a Folder Wizard.	0
	Summary:	
	You have selected the following share settings on \ \FSXSMBTESTING01.FSXTESTING.LOCAL: Folder path: C:\nimtestsmb01 Share name: nimtestsmb01 Share path: \FSXSMBTESTING01.FSXTESTING.LOCAL \nimtestsmb01	< >
	When I click Finish, run the wizard again to share and folder	ther
	To dose this wizard, dick Finish.	
	Finish	ncel

To learn more about creating and managing SMB shares on an Amazon FSx file system, see Creating SMB Shares.

1. After connectivity is in place, the SMB share can be attached and used for application data. To accomplish this, Copy the share path and use the Map Network Drive option to mount the volume on the VM running on VMware Cloud on the AWS SDDC.

← → C Q A == https://vcenter.addc-52-37-127- & Getting Started ■ EC2 Management Con New Tab	7-104 vmwarevmc.com/ui/webconsole.html?vmld=vm-10058.vmName=vmcdct 67% 🟠 🖸	ð 🛃
	[]o	ther Bookma
vmicdst1		terrar and protecting
	Enforce 10 Keyboard Layest New Fullstreen	Sand Chil+Alt+O
Do Anno the life	tanage undetwowed(2)(106/142548)(1)	- 0
Compute Management (FSRMITEITAGE) /SITESTINGLOCAL Share Name med lines	Cate modeled Type Size	
i of tax shadder	01 10/10/2011 315.84A File-future	ora Actions
w M Theres Folders M Developed a former for investors M Developed a former former for investors M Developed a former forme		mental.
al Seniore al Centere al Cen		ore Johann
> # Local Users and Goupe		
A Device Manager		
Window Serve Baltur		
/ Disk Maragement 5. Semine and Applications		

Connect a FSx for NetApp ONTAP LUN to a host using iSCSI

iSCSI traffic for FSx traverses the VMware Transit Connect/AWS Transit Gateway via the routes provided in the previous section. To configure a LUN in Amazon FSx for NetApp ONTAP, follow the documentation found here.

On Linux clients, make sure that the iSCSI daemon is running. After the LUNs are provisioned, refer to the detailed guidance on iSCSI configuration with Ubuntu (as an example) here.

In this paper, connecting the iSCSI LUN to a Windows host is depicted:

- 1. Access the NetApp ONTAP CLI using the management port of the FSx for the ONTAP file system.
- 2. Create the LUNs with the required size as indicated by the sizing output.

FsxId040eacc5d0ac31017::> lun create -vserver vmcfsxval2svm -volume
nimfsxscsivol -lun nimofsxlun01 -size 5gb -ostype windows -space
-reserve enabled

In this example, we created a LUN of size 5g (5368709120).

1. Create the necessary igroups to control which hosts have access to specific LUNs.

```
FsxId040eacc5d0ac31017::> igroup create -vserver vmcfsxval2svm -igroup
winIG -protocol iscsi -ostype windows -initiator ign.1991-
05.com.microsoft:vmcdc01.fsxtesting.local
FsxId040eacc5d0ac31017::> igroup show
Vserver
       Igroup Protocol OS Type Initiators
_____ ____
_____
vmcfsxval2svm
        ubuntu01 iscsi
                          linux iqn.2021-
10.com.ubuntu:01:initiator01
vmcfsxval2svm
        winIG
                   iscsi
                           windows iqn.1991-
05.com.microsoft:vmcdc01.fsxtesting.local
```

Two entries were displayed.

1. Map the LUNs to igroups using the following command:

	acc5d0ac31017::> lun map -vserve sxscsivol/nimofsxlun01 -igroup w		val2svm -	path
FsxId040e	acc5d0ac31017::> lun show			
Vserver Size	Path	State	Mapped	Туре
vmcfsxval	2svm			
5gb	/vol/blocktest01/lun01	online	mapped	linux
vmcfsxval	2svm			
5gb	/vol/nimfsxscsivol/nimofsxlun01	online	mapped	windows

Two entries were displayed.

1. Connect the newly provisioned LUN to a Windows VM:

To connect the new LUN tor a Windows host residing on VMware cloud on AWS SDDC, complete the following steps:

- a. RDP to the Windows VM hosted on the VMware Cloud on AWS SDDC.
- b. Navigate to Server Manager > Dashboard > Tools > iSCSI Initiator to open the iSCSI Initiator Properties dialog box.
- c. From the Discovery tab, click Discover Portal or Add Portal and then enter the IP address of the iSCSI target port.
- d. From the Targets tab, select the target discovered and then click Log On or Connect.
- e. Select Enable Multipath, and then select "Automatically Restore This Connection When the Computer Starts" or "Add This Connection to the List of Favorite Targets". Click Advanced.



The Windows host must have an iSCSI connection to each node in the cluster. The native DSM selects the best paths to use.

	New York and the second s			
Quick Conne	ect		Ştatus	
	r and log on to a target usin of the target and then dick		Quick Connect	3
Iarget:	10.222.2.221			tion at the IP address or DNS name that you targets are available, you need to connect
Discovered	targets		to each target individually.	
			Connections made here will be addee	to the list of Favorite Targets and an attempt
			to restore them will be made every t	ime this computer restarts.
Name		Sta	and the state of the second	
ign. 1992-0	08.com.netapp:sn.264efe8.	32dd911eca951d5f Cor	Discovered targets	
			Name	Status
			ign. 1992-08.com.netapp:sn.f0c90	Ref2dr611erar4f Connerted
		look a second and share		
To connect click Conne	using advanced options, se	lect a target and then	Progress report	
dick Conne	ct. ely disconnect a target, sele		Progress report Login Succeeded.	
dick Conne To complete then dick D For target ;	ct. ely disconnect a target, sele	ect the target and	NUMBER OF CONTRACTORS	

LUNs on the storage virtual machine (SVM) appear as disks to the Windows host. Any new disks that are added are not automatically discovered by the host. Trigger a manual rescan to discover the disks by completing the following steps:

- 1. Open the Windows Computer Management utility: Start > Administrative Tools > Computer Management.
- 2. Expand the Storage node in the navigation tree.
- 3. Click Disk Management.
- 4. Click Action > Rescan Disks.

	p				12000	-	-	12000			
1 C Task Scheduler	- (C) - New Volume (I - System Face) - System Face)	1 9-05,0V9(0)	Simple Ba Simple Ba	ic NTFS ic UDP	s) (Boha, Hoatty (Biol, Page File, Crail: Curry, Pareney PartBoot Heatty (Frinnay PartBoot) Heatty (Frinnay PartBoot) Heatty (System, Active, Primay PartBoot)	95.45 GB 9.98 GB 4.93 GB	9.95 GB 0 MB	5 Free 2015 2015 2015 2115		 	
	-Dia 1 Baic 8.55 GB Online	New Yohane S.H. (B.HTF) Healthy (Prim		i.							
	un Disk Basic 495.55 CB Oxfore	499.9t GB									2 MB Unaffect

When a new LUN is first accessed by the Windows host, it has no partition or file system. Initialize the LUN and, optionally, format the LUN with a file system by completing the following steps:

- 1. Start Windows Disk Management.
- 2. Right-click the LUN, and then select the required disk or partition type.
- 3. Follow the instructions in the wizard. In this example, drive F: is mounted.

$\leftarrow \rightarrow c$	OB	# https://vcenter.sddc-52-37-127-10	4.vmwarevmc.com/ui/webconsole.	html/hmld=vm-10058bm	Name+vmcdc0	87% 1	0	± ≡
Getting Started	EC2 Management Con	👹 New Tab					D Other B	ookmark
mcdc01					Enforce US3	leyboard Leyout View Fulls	creen Send Cal+	Alt + Delet
Firmalia Management File Actors: Vale - Vale								0 K
** * *** *	2 D							
Computer Management Local With Schemer Social Of Task Schemer	= (C) Serg = New Yolyne (C) Serg	Al Type File Tommer Dates	[Capacity] Prex Space] 5, Prex		- 0	х.	Artistan Dail Management Management	
Shared Folders	Personal success of the lot line and	A C T T T D I DUIC		ψe	Section Training	1		
- B Vindon lava facha P Vindon lava facha P Vid Mengement		 # Gard score # Golders (7) # Deama # Deama # Deama # Deama 	Dallie	Deuterte				
 By Service and Apphiations 		Decements / Decements	Marr.	Potente				
		- 10 Ten HC						
	HEAA 1 Sola 1 Sola 2 Sola 3 Sola 3 So		Bhill Onice (D) Sill, View Will, Dive UK, DVR Display The UK, DVR	New Yorker E.)			*	
	er Das Reni Scille (B. Scille (B. Colley	- Aetaon location (2)	NORMAL AND	á		118 Deducer		
	- Data 2 Balain All 2014 All Of NOTS Online Haufty Pressors						T.	

Cloud Volumes ONTAP (CVO)

Cloud volumes ONTAP, or CVO, is the industry-leading cloud data management solution built on NetApp's ONTAP storage software, available natively on Amazon Web Services (AWS), Microsoft Azure and Google Cloud Platform (GCP).

It is a software-defined version of ONTAP that consumes cloud-native storage, allowing you to have the same storage software in the cloud and on-premises, reducing the need to retrain you IT staff in all-new methods to

manage your data.

CVO gives customers the ability to seamlessly move data from the edge, to the data center, to the cloud and back, bringing your hybrid cloud together — all managed with a single-pane management console, NetApp Cloud Manager.

By design, CVO delivers extreme performance and advanced data management capabilities to satisfy even your most demanding applications in the cloud

Cloud Volumes ONTAP (CVO) as guest connected storage

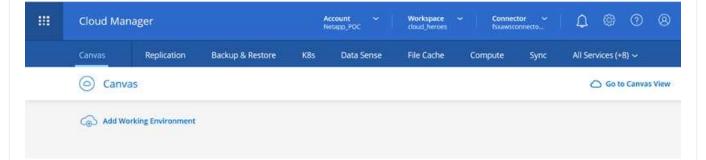
Cloud Volumes ONTAP shares and LUNs can be mounted from VMs that are created in the VMware Cloud on AWS SDDC environment. The volumes can also be mounted on native AWS VM Linux Windows clients, and LUNS can be accessed on Linux or Windows clients as block devices when mounted over iSCSI because Cloud Volumes ONTAP supports iSCSI, SMB, and NFS protocols. Cloud Volumes ONTAP volumes can be set up in a few simple steps.

To replicate volumes from an on-premises environment to the cloud for disaster recovery or migration purposes, establish network connectivity to AWS, either using a site-to-site VPN or DirectConnect. Replicating data from on-premises to Cloud Volumes ONTAP is outside the scope of this document. To replicate data between on-premises and Cloud Volumes ONTAP systems, see Setting up data replication between systems.



Use the Cloud Volumes ONTAP sizer to accurately size the Cloud Volumes ONTAP instances. Also, monitor on-premises performance to use as inputs in the Cloud Volumes ONTAP sizer.

1. Log into NetApp Cloud Central; the Fabric View screen is displayed. Locate the Cloud Volumes ONTAP tab and select Go to Cloud Manager. After you are logged in, the Canvas screen is displayed.



1. On the Cloud Manager home page, click Add a Working Environment and then select AWS as the cloud and the type of the system configuration.

 Cloud Ma	nager					Account Netapo Pr		Workspace cloud, herees		Connector Supervision	ř I L	1 💿	0	8
Canvas	Replication	Backup & Restore	KBS	Data Sense	File Cache	Compute	Sync	All Services (+8	u~					
Add Work	ing Environme	nt												×
					6									
			seft Azure	Amazon We	2011	Coogle Cloud Platform		On Premiers						
					Choose T	/pe								
			0		0		(
		Clou	d Volumes Ol	TAP	Cloud Volumes C	Access of the second	and the second second	Sx for ONTAP						
			EngleNode		CHERN Provides	-Har	sigh-	weilshilty						
														-
					Next	4							3	Ŀ

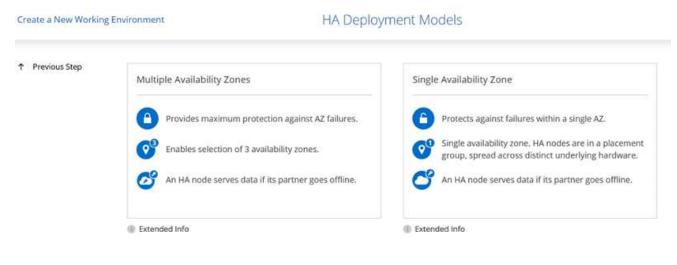
1. Provide the details of the environment to be created including the environment name and admin credentials. Click Continue.

Previous Step	Instance Profile 139763910815 Credential Name Account ID	netapp.com-cloud-volumes Marketplace Subscription	Edit Credentials
	Details	Credentials	
	Working Environment Name (Cluster Name)	User Name	
	fsxcvotesting01	admin	
		Password	
	Add Tags Optional Field Up to four tags	******	
		Confirm Password	

1. Select the add-on services for Cloud Volumes ONTAP deployment, including BlueXP Classification, BlueXP backup and recovery, and Cloud Insights. Click Continue.

Data Sense & Compliance	e	
Backup to Cloud		•
(III) Monitoring		-

1. On the HA Deployment Models page, choose the Multiple Availability Zones configuration.



1. On the Region & VPC page, enter the network information and then click Continue.

US West Oregon wpcdd1c/264bcc495e805. Use generated security group Image: Node 1: Image: Node 2: Image: Node 2: Image: Node 3: Image: Node 1: Image: Node 2: Image: Node 3: Image: Node 3: Image: Node 1: Image: Node 2: Image: Node 3: Image: Node 3: Image: Node 1: Image: Node 2: Image: Node 3: Image: Node 3: Image: Node 1: Image: Node 3: Image: Node 3: Image: Node 3: Image: Node 1: Image: Node 3: Image: Node 3: Image: Node 3: Image: Node 3: Node 5: Node 3: Image: Node 3: Node 3: Previous Step Image: Node 3: Image: Node 3: Image: Node 3: Image: Node 3: Previous Step Image: Node 3: Image: Node 3: Image: Node 3: Image: Node 3: Image: Node 3: Node 3: Image: Node 3: Image: Node 3: Image: Node 3: Image: Node 3: Node 3: Image: Node 3: Image: Node 3: Image: Node 3: Image: Node 3: Node 3: Image: Node 3: Image: Node 3: Image: Node 3: Image: Node 3: Node 3: Image: Nod 3:	Previous Step	AWS Region	6		VPC		Sei	curity group	
Availability Zone us-west-22 Subnet 10.2222.10/24 Continue Continue Continue Continue Continue Continue Continue Continue Continue Continue Continue Continue Continue Continue Previous Step Previous Step Previous Step Previous Step Previous Consectivity and Consectivity & SSH Authentication Mediator SSH Authentication Method Previous Step Previous Consectivity group Consectivity Bair Name Internet Connection Method Public IP address		US West	Oregon	•		805 -	•	Use a generated security group	•
Availability Zone us west 22 Subnet 10.2221.0/24 0 Continue		No.	de 1:		Node 2:			Mediator:	
usweit:2a usweit:2b usweit:2c isubnet Subnet 10222.10/24 usweit:2c isubnet 10222.10/24 usweit:2c isubnet 10222.30/24 isubnet Continue continue isubnet isubnet isubnet isubnet On the Connectivity and SSH Authentication page, choose connection methods for the HA pair and the mediator. continue isubnet <					ETTHO			*	
Submet 10.222.1.0/24 Submet 10.222.1.0/24 Incentive Continue On the Connectivity and SSH Authentication page, choose connection methods for the HA pair and the mediator. ate a New Working Environment Connectivity & SSH Authentication Previous Step Mediator SSH Authentication Method SSH Authentication Method Password Use a generated security group Key Pair Name Internet Connection Method Public IP address Internet Connection Method									
In 222.1.0/24 In 222.2.0/24 In the Connectivity and SSH Authentication page, choose connection methods for the HA pair and the mediator. ate a New Working Environment Connectivity & SSH Authentication Previous Step Image: Mediator SSH Authentication Method Image: Mediator SSH Authentication Method Image: Mediator Vise a generated security group Image: Method Image: Method Image: Method Image: Method <td></td> <td>us-west-</td> <td>2a</td> <td>· · ·</td> <td>us-west-2b</td> <td>(e</td> <td></td> <td>us-west-2c</td> <td>*</td>		us-west-	2a	· · ·	us-west-2b	(e		us-west-2c	*
Continue On the Connectivity and SSH Authentication page, choose connection methods for the HA pair and the mediator. ate a New Working Environment Connectivity & SSH Authentication Previous Step Previous Step Nodes SSH Authentication Method Password Nodes Internet Connection Method Public IP address		Subnet			Subnet			Subnet	
On the Connectivity and SSH Authentication page, choose connection methods for the HA pair and the mediator. Area a New Working Environment Previous Step Previous Step Nodes SSH Authentication Method Password Mediator Key Pair Name Internet Connection Method Public IP address		10.222.1	1.0/24		10.222.2.0/24	S.		10.222.3.0/24	•
Password Use a generated security group Key Pair Name nimokey Internet Connection Method Public IP address	ate a New Workin	g Environment			Connectivity 8	SSH Aut	nentica	tion	
Key Pair Name nimokey - Internet Connection Method Public IP address -			ACCOUNT OF A LOCAL OF A		Connectivity 8	-			
nimokey - Internet Connection Method Public IP address -			Nodes	on Method			Media		
Internet Connection Method Public IP address			SSH Authenticatio	on Method		Secur	Media ty Group	ator	
Public IP address -			SSH Authenticatio	on Method		Secur	Media ty Group a generate	ator	
			SSH Authenticatio	on Method		Secur Use Key P.	Media ty Group a generate air Name	ator	
Continue			SSH Authenticatio	on Method		Secur Use Key P. nim	Media ty Group a generate air Name okey	ator d security group	
			SSH Authenticatio	on Method		Secur Use Key P. nim	Media ty Group a generate air Name okey et Connecti	ator d security group ion Method	
	Previous Step		SSH Authentication Password			Secur Use Key P. nim Intern Pub	Media ty Group a generate air Name okey et Connecti	ator d security group ion Method	
	Previous Step		SSH Authentication Password		•	Secur Use Key P. nim Intern Pub	Media ty Group a generate air Name okey et Connecti	ator d security group ion Method	
	Previous Step		SSH Authentication Password		•	Secur Use Key P. nim Intern Pub	Media ty Group a generate air Name okey et Connecti	ator d security group ion Method	

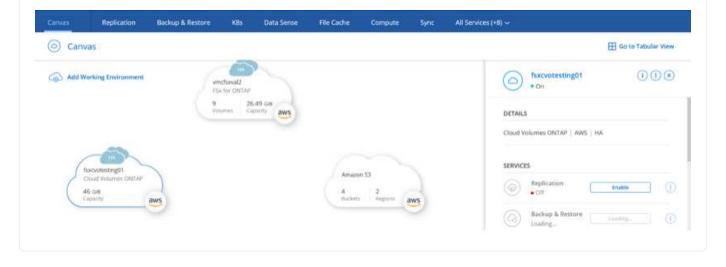
	Previous Step			Floating IPs		
Floating IP address for cluster management 122.16.0.1 Ploating IP address 1 for NFS and CFS data 122.16.0.2 Ploating IP address 2 for NFS and CFS data 122.16.0.3 Ploating IP address for SVM management (Optional) 122.16.0.4 Continue Previous Step Select the route tables to include routes to the floating IP addresses and then coll Continue Previous Step Select the route tables that should include routes to the floating IP addresses. This enables client access to the Cloud Volume pair. If you leave a route table unselected, clients that are associated with the route table cannot access the Hap a dditional information (************************************	NI 107446346345					
Image: state stat		You mu	ust specify IP addresses that are o	utside of the CIDR blocks for a	all VPCs in the selected AWS r	region.
Floating IP address 1 for NFS and CIFS data 172,16.0.2 Floating IP address 2 for NFS and CIFS data 172,16.0.3 Proting IP address for SVM management (Optional) 172,16.0.4 Continue 1. Select the appropriate route tables to include routes to the floating IP addresses and then clicontinue. reate a New Working Environment Route Tables * Previous Step Select the route tables that should include routes to the floating IP addresses. This enables client access to the Cloud Volume pair. If you leave a route table unselected, clients that are associated with the route table cannot access the HA pa Address are not table unselected, dients that are associated with the route table cannot access the HA pa Address multiple information IP Name Main Nassociate with Subnet 1 IV es rb-00b2d30c3f68fdbdd 0 Subnets 1 I Route Tables The main route table is the default for the VPC 1			Floating IP address for	cluster management		
172.16.0.2 Floating IP address 2 for NFS and CIFS data 172.16.0.3 Floating IP address for SVM management (Optional) 172.16.0.4 Continue 1. Select the appropriate route tables to include routes to the floating IP addresses and then clic Continue. treate a New Working Environment Route Tables * Previous Step Select the route tables that should include routes to the floating IP addresses. This enables client access to the Cloud Volume pair. If you leave a route table unselected, clients that are associated with the route table cannot access the HA pair. Additional information Name Main Ves robob2d30c3f68fdbdd 0 Subnets 1 Route Tables The main route table is the default for the VPC						
172.16.2 Floating IP address 2 for NFS and CIFS data 172.16.3 Floating IP address for SVM management (Optional) 172.16.0.4 Continue 18. Select the appropriate route tables to include routes to the floating IP addresses and then clic Continue. reate a New Working Environment Route Tables Previous Step Select the route tables that should include routes to the floating IP addresses. This enables client access to the Cloud Volume pair. If you leave a route table unselected, clients that are associated with the route table cannot access the the pair. If you leave a route table unselected, clients that are associated with the route table cannot access the the pair. Name Main ID Associate with Subnet Tables I Route Tables The main route table is the default for the VPC It Route Tables The main route table is the default for the VPC			Floating IP address 1 fo	r NFS and CIFS data		
172.16.0.3 Floating IP address for SVM management (Optional) 172.16.0.4 Continue 1. Select the appropriate route tables to include routes to the floating IP addresses and then cli Continue. reate a New Working Environment Previous Step Select the route tables that should include routes to the floating IP addresses. This enables client access to the Cloud Volume pair. If you leave a route table unselected, clients that are associated with the route table cannot access the HA pair. If you leave a route table unselected, clients that are associated with Subnet Tables Name Main Additional information It Route Tables The main route table is the default for the VPC 1						
172.16.0.3 Ploating IP address for SVM management (Optional) 172.16.0.4 Continue 1. Select the appropriate route tables to include routes to the floating IP addresses and then cli Continue. reate a New Working Environment Previous Step Select the route tables that should include routes to the floating IP addresses. This enables client access to the Cloud Volume pair. If you leave a route table unselected, clients that are associated with the route table cannot access the HA pair. If you leave a route table unselected, clients that are associated with Subnet Taper. Name Main Main Associate with Subnet Taper. It Route Tables The main route table is the default for the VPC It Route Tables The main route table is the default for the VPC			Floating IP address 2 fo	r NFS and CIFS data		
172.160.4 Continue 1. Select the appropriate route tables to include routes to the floating IP addresses and then old Continue. reate a New Working Environment Previous Step Select the route tables that should include routes to the floating IP addresses. This enables client access to the Cloud Volume pair. If you leave a route table unselected, clients that are associated with the route table cannot access the HA pair. Additional information Name Main 10 Associate with Subnet Takes I Route Tables The main route table is the default for the VPC 11						
172.160.4 Continue 1. Select the appropriate route tables to include routes to the floating IP addresses and then clicontinue. Greate a New Working Environment Previous Step Select the route tables that should include routes to the floating IP addresses. This enables client access to the Cloud Volume pair. If you leave a route table unselected, clients that are associated with the route table cannot access the HA pair. Additional information Name Main D Associate with Subnet Takes I Route Tables The main route table is the default for the VPC			Floating IP address for	SVM management (Optional)		
Continue 1. Select the appropriate route tables to include routes to the floating IP addresses and then old Continue. Greate a New Working Environment Previous Step Select the route tables that should include routes to the floating IP addresses. This enables client access to the Cloud Volume pair. If you leave a route table unselected, clients that are associated with the route table cannot access the HA pair. If you leave a route table unselected, clients that are associated with the route table cannot access the HA pair. If you leave a route table unselected, clients that are associated with Subnet Takes Name Main ID Associate with Subnet Takes Image: Tables The main route table is the default for the VPC 1 1			and a second			
Name Main ID Associate with Subnet Tape Image: Second secon	Previous Step					
Ves rtb-00b2d30c3f68fdbdd 0 Subnets 1 T			Ado	litional information 🏐		
Route Tables The main route table is the default for the VPC		Name	Main	ID	Associate with Subnet	Tags
			Yes	rtb-00b2d30c3f68fdbdd	0 Subnets	1 Tags
Continue		1 Route Tables The mai	n route table is the default for the	VPC		
Continue						
Continue						
			-			
1. On the Data Eneryntian page, chaose AWS managed eneryntian				Continue		
1. On the Data Encryption page, choose AWS-managed encryption.	1. On the Date	Energian name of		Section 20		
	1. On the Data	Encryption page, ch	oose AWS-managed	Section 20		
	1. On the Data	Encryption page, ch	oose AWS-managed	Section 20		

reate a New Working Envir	onment	Data Encryptic	n
 Previous Step 	AWS Man	aged Encryption	
		ele for data encryption and decryptic /S key management services.	n operations. Key management
	Default Master K	ey: aws/ebs	ar Change Key
 Select the license Pay-As-You-Go o 	e option: Pay-As-You-Go or BY0	Continue DL for using an existing I	icense. In this example, the
-	ronmentCloud Volumes ONTAP	Charging Methods &	NSS Account
· · · ·			
Cloud Volumes ONTAP C		NetApp Support Site	Account (Optional)
	harging Methods		Account <i>(Optional)</i> pp Support Site (NSS) accounts
Cloud Volumes ONTAP C	Charging Methods ging methods	Learn more about NetA	op Support Site (NSS) accounts
Cloud Volumes ONTAP C Learn more about our charg	Charging Methods ging methods o by the hour	Learn more about NetA To register this Cloud V should add NetApp Su Don't have a NetApp Su finish deploying this sy:	opp Support Site (NSS) accounts olumes ONTAP to support,you opport Site Account. upport Site account?Select go to stem.After its created,use the
Cloud Volumes ONTAP C Learn more about our charg	Charging Methods ging methods o by the hour	Learn more about NetA To register this Cloud V should add NetApp Su Don't have a NetApp Su finish deploying this sy:	opp Support Site (NSS) accounts olumes ONTAP to support,you oport Site Account.
Cloud Volumes ONTAP C Learn more about our charg O Pay-As-You-Go Bring your ow 1. Select between so deployed on the V	Charging Methods ging methods to by the hour m license co everal preconfigured packages /Ms running on the VMware clo	Learn more about NetA To register this Cloud V should add NetApp Su Don't have a NetApp Su finish deploying this sys Support Registration or ntinue available based on the to ud on AWS SDDC.	opp Support Site (NSS) accounts olumes ONTAP to support, you oport Site Account. upport Site account?Select go to stem.After its created, use the stion to create an NSS account
Cloud Volumes ONTAP C Learn more about our charg O Pay-As-You-Go O Bring your ow 1. Select between so deployed on the V Create a New Working Environ	Charging Methods ging methods to by the hour m license	Learn more about NetA To register this Cloud V should add NetApp Sup Don't have a NetApp Su finish deploying this sys Support Registration or ntinue available based on the to ud on AWS SDDC. Packages	olumes ONTAP to support, you oport Site Account. upport Site account?Select go to stem.After its created, use the otion to create an NSS account.
Cloud Volumes ONTAP C Learn more about our charg O Pay-As-You-Go O Bring your ow 1. Select between se deployed on the V Create a New Working Environ	Charging Methods ging methods to by the hour m license everal preconfigured packages /Ms running on the VMware clo ment Preconfigured lackages	Learn more about NetA To register this Cloud V should add NetApp Sup Don't have a NetApp Su finish deploying this sys Support Registration or ntinue available based on the to ud on AWS SDDC. Packages	opp Support Site (NSS) accounts olumes ONTAP to support, you opport Site Account. upport Site account?Select go to stem.After its created, use the otion to create an NSS account. ype of workload to be

1. On the Review & Approve page, review and confirm the selections. To create the Cloud Volumes ONTAP instance, click Go.

vevious Step TSXCvotesting us-west-2	на		Show /	API request
	TAP instance will be registered with NetApp support unde	r the NSS Account mchad.		
	Cloud Manager will allocate the appropriate AWS resources		e information >	
Overview	Networking Storage			
Overview	Networking Storage Cloud Volumes ONTAP HA	HA Deployment Model:	Multiple Availability Zones	
		HA Deployment Model: Encryption:	Multiple Availability Zones AWS Managed	

1. After Cloud Volumes ONTAP is provisioned, it is listed in the working environments on the Canvas page.



1. After the working environment is ready, make sure the CIFS server is configured with the appropriate DNS and Active Directory configuration parameters. This step is required before you can create the SMB volume.

Volumes HA Status Cost Replications			0	C	٩	*	Ξ
Create a CIFS server		+ Advanced					
DNS Primary IP Address	Active Directory Domain to join						
192.168.1.3	fsxtestinglocal						
DNS Secondary IP Address (Optional)	Credentials authorized to join the domain						
Example: 127.0.0.1	Username Pastword						

1. Select the CVO instance to create the volume and click the Create Volume option. Choose the appropriate size and cloud manager chooses the containing aggregate or use advanced allocation mechanism to place on a specific aggregate. For this demo, SMB is selected as the protocol.

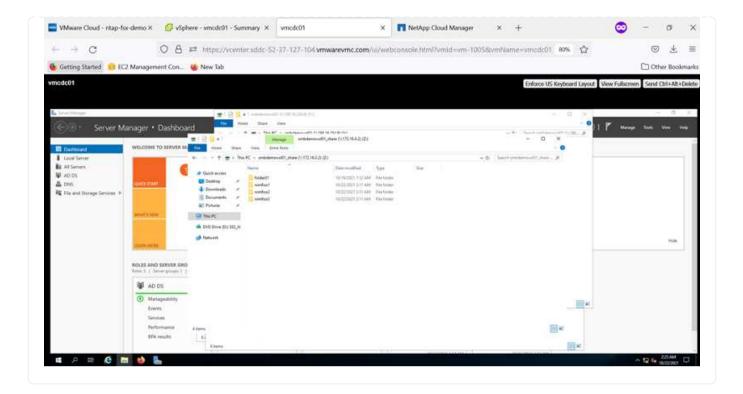
Details & Protection			Protocol		
Volume Name:	Size (G8):	0	NFS	CIFS	iSCSI
smbdemovol01	100	-			
			Share name:	Permissions	
Snapshot Policy:			smbdemovol01_share	Full Contro	• Io
default		-			
Default Policy			Users / Groups:		
			Everyone;		
			Valid users and groups separa	ted by a semicolon	

1. After the volume is provisioned, it is availabe under the Volumes pane. Because a CIFS share is provisioned, you should give your users or groups permission to the files and folders and verify that those users can access the share and create a file.

INFO		CAPACITY	
Disk Type	GP2		1.67 MB
Tiering Policy	None	10 GB	EBS Used
Backup	OFF	Allocated	

- 1. After the volume is created, use the mount command to connect to the share from the VM running on the VMware Cloud in AWS SDDC hosts.
- 2. Copy the following path and use the Map Network Drive option to mount the volume on the VM running on the VMware Cloud in AWS SDDC.

(HA) fsxcvotesting01 (Multiple AZs)	Aws 品 Aws
Volumes HA Status Cost Replications	S (U) (0)
Mount Volume smbdemovol01	
Access from inside the VPC using Floating IP	Access from outside the VPC using AWS Private IP
Auto failover between nodes	No auto failover between nodes
The IP address automatically migrates between nodes if failures occur	The IP address does not migrate between nodes if failures occur
Go to your machine and enter this command	To avoid traffic between nodes, mount the volume by using the primary node's IP address:
\\172.16.0.2\smbdemovol01_share	\\10.222.1.100\smbdemovo101_share
	If the primary node ones offline, mount the volume by using the HA partner's IP address:



Connect the LUN to a host

To connect the Cloud Volumes ONTAP LUN to a host, complete the following steps:

- 1. On the Cloud Manager Canvas page, double-click the Cloud Volumes ONTAP working environment to create and manage volumes.
- 2. Click Add Volume > New Volume, select iSCSI, and click Create Initiator Group. Click Continue.

	Det	tails & Pro	otection				P	rotocol			
	Volu	me Name:			Size (GB):	0		NFS	CIFS	iscs	1
	nîn	nofsxiscsicvo	01		500					What about I	UNs? 🕕
	Snat	shot Policy:					In	tiator Group 🛞			
		fault					۲	Map Existing Initi	ator Groups ု	Create Initiate	r Group
	() D	efault Policy					Op	perating System Typ	pe		_
								Windows			
							-				
							50	lect Initiator Group		1 (of 3) Groups
								winiG wine ign.1991-05.	dows .com.microsoft:vrr	cdc01.fsxtestir	here
		ere - vmcdc01 - 5 ==== https://vce		vmcdc01		1.354	rtApp Cloud N e.htmi?emid	Manager × +		3	- a © 4
Getting Started 🤐 EC2 Man nocc01 Interlineup Garage Server Manage	O A a	== https://vce New Tab	enter sidd:-52	-37-127-104.vm	warevmc.com//ai/	1.354	11447		Enforce US Keyboard Lag	2	Send Orf+W
Cetting Started Cetting Started Cetting Started Cetting Cetting Started Cetting Cetti	agement Con	new Tab	nter side-52	-37-127-104.vm	warevmc.com//u//	webconsole state state state state	11447		Syncdc01 80% C	7 vout View Fußiszeen	Send Orf+W
Conting Started Cocol	A a agement Con.	E https://vce Now Tab	nter side-52	-37-127-104.vm	warevmc.com/ui/ warevm	webconsole state state state state	e.html?vmid	svm-10058ivmName	Syncdc01 80% C	7 vout View Fußiszeen	©
Getting Started C EC2 Mark Getting Started EC2 Mark Getting Started Server Manage Server Manage A General A General	COME TO BASHDOAT COME TO BAS	E https://vce Now Tab	nter side-52	-37-127-104.vm	warevmc.com/ui/ warevm	webconsole state state state state	e.html?vmid	svm-10058ivmName	Syncdc01 80% C	7 vout View Fußiszeen	©
Getting Started C EC2 Mark Getting Started C EC2 Mark CdC01 Server Manage Server Manage Ad Server Ad Server Ad Server Ad Server Fre and Starge Servers C E	Construction Cons	E https://vce Now Tab	nter side-52	-37-127-104.vm	warevmc.com/ui/ warevm	webconsole state state state state	e.html?vmid	svm-10058ivmName	Syncdc01 80% C	View Fullaceer	©
Cetting Started Cetting Started Cetting Started Cetting Started Cetting Cetting Started Cetting Cetti	Construction C	E https://vce Now Tab	nter side-52	-37-127-104.vm	warevmc.com/ui/ warevm	webconsole state state state state	e.html?vmid	svm-10058ivmName	Enforce US Keyboard La Enforce US Keyboard La - 2 X - 2 X - 3 - 4 - 4 - 4 - 4 - 4 - 4 - 4 - 4	View Fullaceer	©

1. After the volume is provisioned, select the volume, and then click Target IQN. To copy the iSCSI Qualified Name (IQN), click Copy. Set up an iSCSI connection from the host to the LUN.

To accomplish the same for the host residing on the VMware Cloud on AWS SDDC, complete the following steps:

a. RDP to the VM hosted on VMware cloud on AWS.

- b. Open the iSCSI Initiator Properties dialog box: Server Manager > Dashboard > Tools > iSCSI Initiator.
- c. From the Discovery tab, click Discover Portal or Add Portal and then enter the IP address of the iSCSI target port.
- d. From the Targets tab, select the target discovered and then click Log On or Connect.
- e. Select Enable Multipath, and then select Automatically Restore This Connection When the Computer Starts or Add This Connection to the List of Favorite Targets. Click Advanced.



The Windows host must have an iSCSI connection to each node in the cluster. The native DSM selects the best paths to use.

	scovery Favorite Targets Volumes and Devices Ru	ADIUS Configuration
uid: Conn	[13] We share the second se Second second s Second second seco	
	r and log on to a target using a basic connection, type of the target and then click Quick Connect.	the IP address or
arget:	172.24.2.9	Quick Connect
scovered	targets	
		Refresh
lane	St	atus
	t using advanced options, select a target and then	Connect
ick Conne o complet		Connect
ick Conne o complet ien click (or target	ect. tely disconnect a target, select the target and	

LUNs from the SVM appear as disks to the Windows host. Any new disks that are added are not automatically discovered by the host. Trigger a manual rescan to discover the disks by completing the following steps:

- 1. Open the Windows Computer Management utility: Start > Administrative Tools > Computer Management.
- 2. Expand the Storage node in the navigation tree.
- 3. Click Disk Management.
- 4. Click Action > Rescan Disks.

Computer Management (Local	× 2 5 5 10.		Te	100.0	1.0		1000		Text
Comparison Management (Lata) Comparison Management (Lata) Comparison Management Comparison Management Comparis	Tree Yolame St.) System Reserved System Reserved	5,014(0) Sim	e Basic e Basic	NTEL	Status Hoathy Boot, Fage Roc, Crash Dung Healthy Grinney Particini Healthy Grinney Particini Healthy Grystein, Aston, Primary Batt		85.46 GB 9.92 GB	9.85 GB 0 MB	8 60% 300% 9%
	10.00 GE	ystem Tanarved 40 MB NTPS Healthy Cystem, A	tiye, Prin	nery Partition		IES 81.46 GB NTFS Healthy (Boot, 7s	ge File, Cra	h Durry, Por	Permary Paction)
	Basic 19000 GB Codine 	40 MB NTFS		nery Partition		25-46-GE NTRS	pe File, Cre	h Durry, Por	Persey Patien)

When a new LUN is first accessed by the Windows host, it has no partition or file system. Initialize the LUN; and optionally, format the LUN with a file system by completing the following steps:

- 1. Start Windows Disk Management.
- 2. Right-click the LUN, and then select the required disk or partition type.
- 3. Follow the instructions in the wizard. In this example, drive F: is mounted.

VMware Cloud Services - Log In X	Ø vSphere -	vmcdc01 - Summary	× vmodc01	× NetAp	p Cloud Manager	× +	0	(-)	a ×
C	0 8 ₽	https://wcenter.add	-52-37-127-104.vmwa	revmc.com/ui/webconsole.ht	mi?vmid=vm-10058e	mName+vmcdc)	aos 🏠	0	± =
Getting Started 🥫 EC2 Manager	nent Con. 🐞 I	New Tatz						C) Other	Bookmark
nodc01						Enforce US R	eyboard Layout View Fullic	seen Sent Oil	+AZ+Delet
Compatible Managements								-	8 ×
Di Computer Management Sciller (Holana		Fit bates	1	Coguetty [Ann Sports] 16. Anno				Artist	
· II Soler Sol. # C) · () Sek Schelute # Des Solere ()		P Q + TeaPC				- 0	×	Did Meageree	
El Los Yange Second Faller Second F	LR Dick (D.) Seconda .	the Lingdon Has				& last het		1000 6000	
A Deckarages A Deckarages w The Surveys			iden (7)						
· Britisten Sever Backer		Battana r	al Open	Dates	The Decement				
(), Service and Applications		Dunkak /	Durthash		10				
		Ritchen P	4	A Marc	Rear Prove				
		# DO Dive Do BLA	Total Volume						
-tia 1	;		vices and drives (4)					-	
Name Alter Car	Non Volume BJ		Careford Date	Del Dia dii Di Anni In C. Del	New Yoldward B.				
(Index	Healthy (Homary Partic		And Area (
- Disk			and and a second second)¢					
Annual Contract	401.04 28	- 14	ferrir locations (2) and demonster (2110) 19254 B (1)				148 Dateste		
=Da7	_		Contraction of the	×"					
Resist 4,10 (28	A REPORT OF A REPO								
	Healthy (Panary Fettis	Uners Theradeland					108	5	
a 🖉 induced 🖬 A									

On the Linux clients, ensure the iSCSI daemon is running. After the LUNs are provisioned, refer to the detailed guidance on iSCSI configuration for your Linux distribution. For example, Ubuntu iSCSI configuration can be found here. To verify, run lsblk cmd from the shell.

To mount the Cloud Volumes ONTAP (DIY) file system from VMs within VMC on AWS SDDC, complete the following steps:

- 1. Connect to the designated Linux instance.
- 2. Open a terminal on the instance using secure shell (SSH) and log in with the appropriate credentials.
- 3. Make a directory for the volume's mount point with the following command.

\$ sudo mkdir /fsxcvotesting01/nfsdemovol01

4. Mount the Amazon FSx for NetApp ONTAP NFS volume to the directory that is created in the previous step.

/fsxcvotes	z -t nfs nfsvers=4.1,172.16.0.2:/nfsdemovol01 sting01/nfsdemovol01	
root@ubuntu01:/fs	sx# mount -t nfs 172.16.0.2:/nfsdemovol01 /fsxcvotesting01/nfsdem	ovo101 <u>.</u>
😰 vSphere - ubuntu01 - Summary ×	ubuntu01 × +	0
$\leftarrow \rightarrow c$	O A # https://vcenter.sddc-52-37-127-104.vmwarevmc.com/ul/webconsole.html?vmld=vm-10038vmName=ubuntu018xerv	ŵ
Getting Started 🔒 EC2 Manager	ment Con 🗰 New Tab	
ubuntu01	Enforce US Keyboard Layout	liew Fullscree
	root@ubuntu01:/fsX/mfsdemovol01# df Filesystem tmpfs /dev/mapper/ubuntuvg-ubuntuiv 1541956 1176 813820 11 /run /dev/mapper/ubuntuvg-ubuntuiv 15412188 3666428 10943132 265 / tmpfs 4071950 0 4071950 0 37 /dev/shm	

Overview of ANF Datastore Solutions

Every successful organization is on a path of transformation and modernization. As part of this process, companies typically use their existing VMware investments while leveraging cloud benefits and exploring how to make migration, burst, extend, and disaster recovery processes as seamless as possible. Customers migrating to the cloud must evaluate the issues of elasticity and burst, data center exit, data center consolidation, end- of- life scenarios, mergers, acquisitions, and so on. The approach adopted by each organization can vary based on their respective business priorities. When choosing cloud-based operations, selecting a low- cost model with appropriate performance and minimal hindrance is a critical goal. Along with choosing the right platform, storage and workflow orchestration is particularly important to unleash the power of cloud deployment and elasticity.

Use Cases

Although the Azure VMware solution delivers unique hybrid capabilities to a customer, limited native storage options have restricted its usefulness for organizations with storage-heavy workloads. Because storage is directly tied to hosts, the only way to scale storage is to add more hosts, which can increase costs by 35-40% or more for storage intensive workloads. These workloads need additional storage, not additional horsepower, but that means paying for additional hosts.

Let's consider the following scenario; a customer requires six hosts for horsepower (vCPU/vMem), but they also have a substantial requirement for storage. Based on their assessment, they require 12 hosts to meet storage requirements. This increases the overall TCO because they must buy all that additional horsepower when all they really need is more storage. This is applicable for any use case, including migration, disaster recovery, bursting, dev/test, and so on.

Another common use case for Azure VMware Solution is disaster recovery (DR). Most organizations do not have a fool- proof DR strategy, or they might struggle to justify running a ghost datacenter just for DR. Administrators might explore zero- footprint DR options with a pilot- light cluster or an on-demand cluster. They could then scale the storage without adding additional hosts, potentially an attractive option.

So, to summarize, the use cases can be classified in two ways:

- · Scaling storage capacity using ANF datastores
- Using ANF datastores as a disaster recovery target for a cost- optimized recovery workflow from onpremises or within Azure regions between the software-defined datacenters (SDDCs). This guide provides insight into using Azure NetApp Files to provide optimized storage for datastores (currently in public preview) along with best-in-class data protection and DR capabilities in an Azure VMware solution, which enables you to offload storage capacity from vSAN storage.



Contact NetApp or Microsoft solution architects in your region for additional information on using ANF datastores.

VMware Cloud options in Azure

Azure VMware Solution

The Azure VMware Solution (AVS) is a hybrid cloud service that provides fully functioning 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.

Regardless of the cloud used, when a VMware SDDC is deployed, the initial cluster includes the following components:

- VMware ESXi hosts for compute virtualization with a vCenter server appliance for management.
- VMware vSAN hyper-converged storage incorporating the physical storage assets of each ESXi host.
- VMware NSX for virtual networking and security with an NSX Manager cluster for management.

Conclusion

Whether you are targeting all-cloud or hybrid cloud, Azure NetApp files provide excellent options to deploy and

manage the application workloads along with file services while reducing the TCO by making the data requirements seamless to the application layer. Whatever the use case, choose Azure VMware Solution along with Azure NetApp Files for rapid realization of cloud benefits, consistent infrastructure, and operations across on-premises and multiple clouds, bi-directional portability of workloads, and enterprise-grade capacity and performance. It is the same familiar process and procedures used to connect the storage. Remember, it is just the position of the data that changed along with new names; the tools and processes all remain the same, and Azure NetApp Files helps in optimizing the overall deployment.

Takeaways

The key points of this document include:

- You can now use Azure NetApp Files as a datastore on AVS SDDC.
- Boost the application response times and deliver higher availability to provide access workload data when and where it is needed.
- Simplify the overall complexity of the vSAN storage with simple and instant resizing capabilities.
- Guaranteed performance for mission-critical workloads using dynamic reshaping capabilities.
- If Azure VMware Solution Cloud is the destination, Azure NetApp Files is the right storage solution for optimized deployment.

Where to find additional information

To learn more about the information described in this document, refer to the following website links:

• Azure VMware Solution documentation

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

Azure NetApp Files documentation

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

• Attach Azure NetApp Files datastores to Azure VMware Solution hosts (Preview)

https://docs.microsoft.com/en-us/azure/azure-vmware/attach-azure-netapp-files-to-azure-vmware-solution-hosts?tabs=azure-portal/

NetApp Guest Connected Storage Options for Azure

Azure supports guest connected NetApp storage with the native Azure NetApp Files (ANF) service or with Cloud Volumes ONTAP (CVO).

Azure NetApp Files (ANF)

Azure netApp Files brings enterprise-grade data management and storage to Azure so you can manage your workloads and applications with ease. Migrate your workloads to the cloud and run them without sacrificing performance.

Azure netApp Files removes obstacles, so you can move all of your file-based applications to the cloud. For the first time, you do not

have to re-architect your applications, and you get persistent storage for your applications without complexity.

Because the service is delivered through the Microsoft Azure Portal, users experience a fully managed service

as part of their Microsoft enterprise Agreement. World-class support, managed by Microsoft, gives you complete peace of mind. This single solution enables you to quickly and easily add multiprotocol workloads. you can build and deploy both Windows and Linux file-based applications, even for legacy environments.

Azure NetApp Files (ANF) as guest connected storage

Configure Azure NetApp Files with Azure VMware Solution (AVS)

Azure NetApp Files shares can be mounted from VMs that are created in the Azure VMware Solution SDDC environment. The volumes can also be mounted on the Linux client and mapped on the Windows client because Azure NetApp Files supports SMB and NFS protocols. Azure NetApp Files volumes can be set up in five simple steps.

Azure NetApp Files and Azure VMware Solution must be in the same Azure region.

To create and mount Azure NetApp Files volumes, complete the following steps:

1. Log in to the Azure Portal and access Azure NetApp Files. Verify access to the Azure NetApp Files service and register the Azure NetApp Files Resource Provider by using the *az provider register --namespace Microsoft.NetApp –wait* command. After registration is complete, create a NetApp account.

For detailed steps, see Azure NetApp Files shares. This page will guide you through the step-by-step process.

Microsoft Azure 🔑 Search res	sources, services, and docs (G+/)		E.	Ð	P	۲	?	3
Home > Azure NetApp Files >								
Azure NetApp Files « etApp (cloudcontrolproduction.com)	New NetApp account							
🕂 Create 🛛 🕲 Manage view 🗸 …	Name *							
ilter for any field	nimoAVSANFdemo	~]					
lame 🗘	Subscription							
	SaaS Backup Production	~						
	Resource group *							
	NimoAVSDemo	~]					
	Create new							
NetApp accounts to display	Location *							
re NetApp Files makes it easy to migrate and	East US 2	~]					
complex, file-based applications with no code nge. With support for multiple protocols and rated data protection, storage management is simple, fast, and reliable.								
Create NetApp account								
Learn more of	Create Download a template for automation							

2. After the NetApp account is created, set up the capacity pools with the required service level and size.

For more information, see Set up a capacity pool.

Azure NetApp Files « NetApp (cloudcontrolpreduction.com)		mo				New capacity pool	×
+ Create 🔘 Manage view 🗸 …	,D Search (Ctrl+/)	-0C	+ Add pool	Refresh		nimcappool	4
Filter for any field.	Azure NetApp Files	^	P Search pool			Service level • 💿	
Name 1	Active Directory connections		Name	.†↓ Capacity	1. Service lev	Standard	V
m nimoAVSANFdemo ····	Storage service		You don't have	any capacity pools. Click	Add pool to get started	Size (TiB) * 🕜	
	Capacity pools					4	4 Tie
	🖳 Volumes					QoS type	14, 115
	Data protection					O Manual	
	Snapshot policies					 Auto 	
	Storage service add-ons						
	NetApp add-ons						
	Automation						
< Page 1 V of 1 >	🕌 Tasks (preview)					Create Discard	

3. Configure the delegated subnet for Azure NetApp Files and specify this subnet while creating the volumes. For detailed steps to create delegated subnet, see Delegate a subnet to Azure NetApp Files.

		Add subnet
nimoavspriv-vn Virtual network	et Subnets	Name *
Search (Ctrl+/)	« + Subnet -	name ~
Overview	Search subn	Subnet address range * ①
Activity log	Contraction of the second	172.24.3.0/28
Access control (IAM)	Name ↑↓	172.24.3.0 - 172.24.3.15 (11 + 5 Azure reserved address
🧳 Tags	GatewaySubne	Add IPv6 address space ③
Diagnose and solve problems	VMSubnet	NAT gateway 💿
	StorageSubnet	None
Settings	<	Network security group
Address space		None
Ø Connected devices		Route table
 Subnets 		None
ODoS protection		
🚭 Firewall		
Security		Save Cancel

4. Add an SMB volume by using the Volumes blade under the Capacity Pools blade. Make sure the Active Directory connector is configured prior to creating the SMB volume.

Azure NetApp Files « NetApp (cloudcontrolproduction.com)	NetApp account	Active Directory connections	Primary DNS * ③
+ Create 🔞 Manage view 🗸 …	C Search (Ctrl+/)	🖉 Join 🕐 Refresh	172.24.1.5
Filter for any field	Activity log	DNS 1 AD DNS Domai 1 SMB Server	Secondary DNS
Name 1.	Access control (IAM)	No currently joined Active Directories.	
nimoAVSANEdemo ····	Tags	<	AD DNS Domain Name * 💿
· · · · · · · · · · · · · · · · · · ·	• 1037	-	nimodemo.com
	Settings		AD Site Name ①
	D Quota		1
	III Properties		SMB Server (Computer Account) Prefix * 📀
	🔒 Locks		nimsmb
	Azure NetApp Files		Organizational Unit Path 💿
	Active Directory connections		
	Storage service		
< Page 1 V of 1 >	Capacity pools		Join

5. Click Review + Create to create the SMB volume.

If the application is SQL Server, then enable the SMB continuous availability.

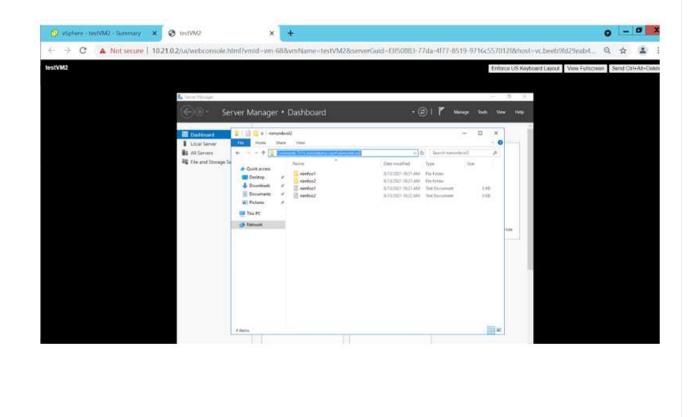
	mo	Volumes	. 6	Create a volume		>
,P Search (Ctrl+/)	*	+ Add volume 🕐 Refresh				
Azure NetApp Files	^	prigonal and a second	^	Basics Protocol Tags R	Review + create	
Active Directory connections		Search volumes Name 1 Quota			Azure NetApp Files volume in your subscriptio stwork. Learn more about Azure NetApp File	
Storage service		You don't have any volumes. Click	k Add vo	Volume details		
E Capacity pools		<	>			
		· · · · · · · · · · · · · · · · · · ·		Volume name *	nimvoltest1	~
🗟 Volumes	6			and the second second		~ 0
Volumes	f.			Capacity pool * 📀	nimcappool	~ ~
	1			and the second second		 410
Data protection	1			Capacity pool * 📀	nimcappool	

nimoAVSAN NetApp account	Fdemo	Volumes	359 359											
P Search (Ctrl+/)	e .	+ Add volume	0	Refresh										
Quota	^	. ^O Search volum	65 ::											
Properties		Name	\uparrow_{\downarrow}	Quota	÷ψ	Throughput	74	Protocol type	1	Mount path	14	Service level	14	Capacity
A Locks		nimsmbvo	12	100 GiB		1.6 Mi8/s		SMB		\\nimsmb-7c1c	nimode	Standard		nimcapp
		nimvoltest		100 GiB		1.6 Mi8/s		NFSv3		172.24.3.4:/nim		000104098		nimcapp

To learn more about Azure NetApp Files volume performance by size or quota, see Performance considerations for Azure NetApp Files.

6. After the connectivity is in place, the volume can be mounted and used for application data.

To accomplish this, from the Azure portal, click the Volumes blade, and then select the volume to mount and access the mount instructions. Copy the path and use the Map Network Drive option to mount the volume on the VM running on Azure VMware Solution SDDC.



E I I I I I I I I I I I I I I I I I I			-	- 0	~
🗧 🔶 👻 🛧 📜 🕅	nsmb-7c1c.nimodemo.com\nimsmbvol2	ۍ ~	Search nimsmbvo	12	م ر
10:1	Name	Date modified	Туре	Size	
A Quick access	nimfoo1	8/13/2021 10:21 AM	File folder		
Desktop 🖈	nimfoo2	8/13/2021 10:21 AM	File folder		
🕹 Downloads 🚿	nimfoo1	8/13/2021 10:21 AM	Text Document		0 KB
Documents #	in nimfoo2	8/13/2021 10:22 AM	Text Document		0 KB
This PC					
interview					

7. To mount NFS volumes on Linux VMs running on Azure VMware Solution SDDC, use this same process. Use volume reshaping or dynamic service level capability to meet the workload demands.

ilesystem	1K-blocks	Used	Available	Use%	Mounted on
dev	8168112	0	8168112	6%	/dev
npfs	1639548	1488	1638060	1%	/run
dev/sdaS	50824704	7902752	40310496	17%	1
npfs	8197728	0	8197728	6%	/dev/shn
npfs	5120	0	5120	0%	/run/lock
npfs	8197728		8197728	8%	/sys/fs/cgroup
dev/loop0	56832	56832	0	100%	/snap/core18/2128
dev/loop2	66688	66688	6	100%	/snap/gtk-common-the
es/1515					
dev/loop1	224256	224256	9	100%	/snap/gnome-3-34-18
/72					
dev/loop3	52224	52224	.0	100%	/snap/snap-store/54
dev/loop4	33152	33152	0	100%	/snap/snapd/12704
dev/sda1	523248	4	523244	1%	/boot/efi
npfs	1639544	52	1639492	1%	/run/user/1000
dev/sr0	54738	54738	9	100%	/media/nimoadmin/VM
re Tools					
72.24.3.4:/nimodemonfsv1	104857600	. 0	104857600	0%	/home/nimoadmin/nim

For more information, see Dynamically change the service level of a volume.

Cloud Volumes ONTAP (CVO)

Cloud volumes ONTAP, or CVO, is the industry-leading cloud data management solution built on NetApp's ONTAP storage software, available natively on Amazon Web Services (AWS), Microsoft Azure and Google Cloud Platform (GCP).

It is a software-defined version of ONTAP that consumes cloud-native storage, allowing you to have the same storage software in the cloud and on-premises, reducing the need to retrain you IT staff in all-new methods to manage your data.

CVO gives customers the ability to seamlessly move data from the edge, to the data center, to the cloud and back, bringing your hybrid cloud together — all managed with a single-pane management console, NetApp Cloud Manager.

By design, CVO delivers extreme performance and advanced data management capabilities to satisfy even your most demanding applications in the cloud

Cloud Volumes ONTAP (CVO) as guest connected storage

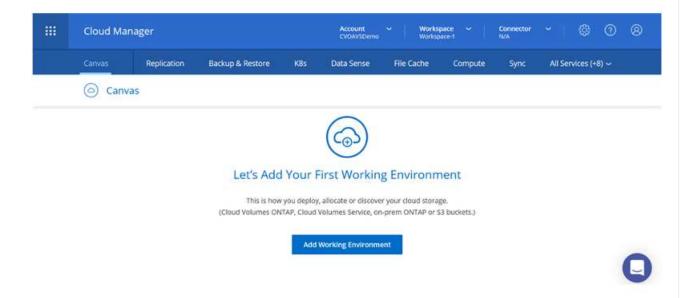
Cloud Volumes ONTAP shares and LUNs can be mounted from VMs that are created in the Azure VMware Solution SDDC environment. The volumes can also be mounted on the Linux client and on Windows client because Cloud Volumes ONTAP supports iSCSI, SMB, and NFS protocols. Cloud Volumes ONTAP volumes can be set up in a few simple steps.

To replicate volumes from an on-premises environment to the cloud for disaster recovery or migration purposes, establish network connectivity to Azure, either using a site-to-site VPN or ExpressRoute. Replicating data from on-premises to Cloud Volumes ONTAP is outside the scope of this document. To replicate data between on-premises and Cloud Volumes ONTAP systems, see Setting up data replication between systems.



Use Cloud Volumes ONTAP sizer to accurately size the Cloud Volumes ONTAP instances. Also monitor on-premises performance to use as inputs in the Cloud Volumes ONTAP sizer.

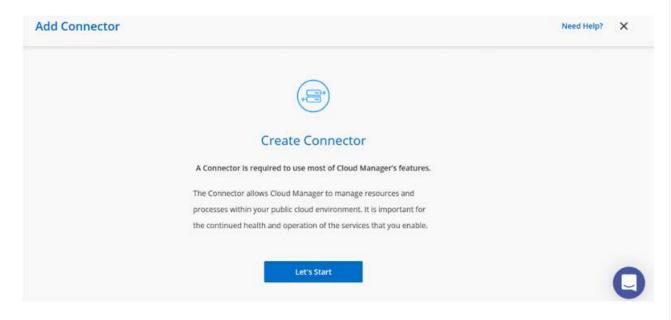
1. Log in to NetApp Cloud Central—the Fabric View screen is displayed. Locate the Cloud Volumes ONTAP tab and select Go to Cloud Manager. After you are logged in, the Canvas screen is displayed.



2. On the Cloud Manager home page, click Add a Working Environment and then select Microsoft Azure as the cloud and the type of the system configuration.

	Designation of		1/05		and the second second			ARCEN		
Canvas	Replication	Backup & Restore	K8s D	ata Sense I	File Cache	Compute	Sync	All Serv	vices (+8) 🛩	
Add New	Working Enviro	nment								×
		0								
			aws	0	<u>(</u>)					
	Mi	crostt Azure Ama	zon Web Services	Google Cloud	Platform	On-Premise	5			
	Choose	Туре								
		0	2							
		0		0		(III)				
				0		9				
	Clo	ud Volumes ONTAP	Cloud Volu	imes ONTAP HA	A	zure NetApp Files				6

3. When creating the first Cloud Volumes ONTAP working environment, Cloud Manager prompts you to deploy a Connector.



4. After the connector is created, update the Details and Credentials fields.

Managed Service Ide	SaaS Backup Prod	CMCVOSub	
Credential Name	Azure Subscription	Marketplace Subscription	Edit Credentials
Details		Credentials	
Working Environment Nam	e (Cluster Name)	User Name	
nimavsCVO	an den en de de de la	admin	
		Password	

5. Provide the details of the environment to be created including the environment name and admin credentials. Add resource group tags for the Azure environment as an optional parameter. After you are done, click Continue.

Details	Credentials
Working Environment Name (Cluster Name)	User Name
nimavsCVO	admin
	Password
Add Resource Group Tags Optional Field	••••••
	Confirm Password

6. Select the add-on services for Cloud Volumes ONTAP deployment, including BlueXP Classification, BlueXP backup and recovery, and Cloud Insights. Select the services and then click Continue.

Data Sense & Compliance	•
Backup to Cloud	-• ~
(ilii) Monitoring	-

7. Configure the Azure location and connectivity. Select the Azure Region, resource group, VNet, and subnet to be used.

Azure Region		Resource Group
East US 2		Create a new group Use an existing group
Availability Zone	(Optional)	Resource Group Name
Select in Availability Zone	•	nimassCVO-rg
Wet		
nimoavspriv-vnet NimoAVSDemo	*	Security Group
Subnet		Generated security group O Use existing security group
172.24.2.0/24	•	
		I have verified network connectivity between the Cloud Manager server and the selected Whiet.
	Con	tinue
	-	

Cloud Volumes ONTAP Charging Methods	NetApp Support Site Account (Optional)
earn more about our charging methods	Learn more about NetApp Support Site (NSS) accounts
Pay-As-You-Go by the hour	To register this Cloud Volumes ONTAP to support, you should add NetApp Support Site Account.
Bring your own license	Don't have a NetApp Support Site account?Select go to finish deploying this system.After its created,use the Support Registration option to create an NSS account

9. Select between several preconfigured packages available for the various types of workloads.

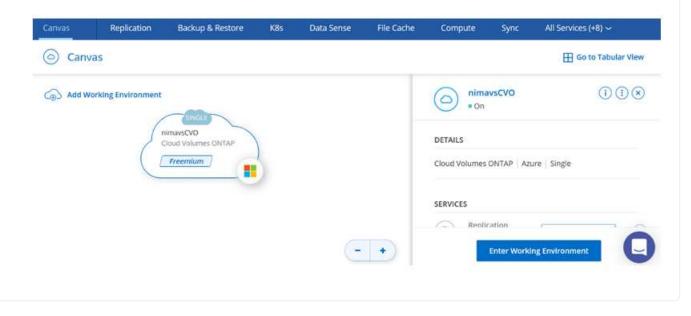
Create a New Working EnvironmentCloud Volumes ONTAP Charging Methods & NSS Account

Select a pre	configured Cloud Volumes ONTAP system that best Preconfigured settings can be n		onfiguration. Change Configuration
·•		\$0	.ę.
POC and small workloads Up to 500GB of storage	Database and application data production workloads	Cost effective DR	Highest performance production workloads

10. Accept the two agreements regarding activating support and allocation of Azure resources. To create the Cloud Volumes ONTAP instance, click Go.

1			
nimavsCVO Ature East US 2			
		out 1 must first conistor	r Claud Volumar CAITAD with Notana Alexa information
			r Cloud Volumes ONTAP with NetApp. More information >
I understand that	t Cloud Manager will alloc	cate the appropriate Azi	ure resources to comply with my above requirements. More information >
	Networking	Storage	

11. After Cloud Volumes ONTAP is provisioned, it is listed in the working environments on the Canvas page.



1. After the working environment is ready, make sure the CIFS server is configured with the appropriate DNS and Active Directory configuration parameters. This step is required before you can create the SMB volume.

Volumes Replications		0	\bigcirc	C	⊜	4	Ξ
Create a CIFS server	+ Advance	d					
DNS Primary IP Address	Active Directory Domain to join						
172.24.1.5	nimodemo.com						
DNS Secondary IP Address (Optional)	Credentials authorized to join the domain						
Example: 127.0.0.1	nimoadmin						

 Creating the SMB volume is an easy process. Select the CVO instance to create the volume and click the Create Volume option. Choose the appropriate size and cloud manager chooses the containing aggregate or use advanced allocation mechanism to place on a specific aggregate. For this demo, SMB is selected as the protocol.

Details & Protection			Protocol		
Volume Name:	Size (GB);	0	NFS	CIFS	iSCSI
nimavssmbvol1	50				
			Share name:	Permissions:	
Snapshot Policy:			nimavssmbvol1_share	Full Control	
default		•			
③ Default Policy			Users / Groups:		
			Everyone;		

3. After the volume is provisioned, it will be availabe under the Volumes pane. Because a CIFS share is provisioned, give your users or groups permission to the files and folders and verify that those users can access the share and create a file. This step is not required if the volume is replicated from an on-premises environment because the file and folder permissions are all retained as part of SnapMirror replication.

volumes			
Volume 50 GB Alloca	ited 1.74 MB Total Used	(1.74 MB in Disk, 0 KB in Blo	b)
	25 - 251		
erm nimavs	smbvol1		ONLINE
INFO		CAPACITY	
INFO		CAPACITY	
Disk Type	PREMIUM_LRS		1.74 MB
Tiering Policy	Auto	50 GB	Disk Used
		Allocated	
Backup	OFF		O GB Blob Used
			Diab Lizozi

- 4. After the volume is created, use the mount command to connect to the share from the VM running on the Azure VMware Solution SDDC hosts.
- 5. Copy the following path and use the Map Network Drive option to mount the volume on the VM running on Azure VMware Solution SDDC.

Moun o to your mac		er this com	mand					
\\172.24.2.	8\nimavssmb	bvol1_shar	e					
					Col	oy 👘		
					a and a second			
🖓 🧧 🖛 nimavssm	nbvoll share						- 0	>
File Home Share								Ŷ
- 🚽 × 🛧 💆 🕅	242.8\nimavombvol1_s	hate				~ 0	Search nimavssmbvoll_shar	e 9
	Name	0	Date modified	Туре	Size			
Quick access Desktop				This folder	is empty:			
Downloads					2019 - 2019 - 2019 - 2019 - 2019 - 2019 - 2019 - 2019 - 2019 - 2019 - 2019 - 2019 - 2019 - 2019 - 2019 - 2019 -			
🗿 Documents 👒								

Connect the LUN to a host

To connect the LUN to a host, complete the following steps:

- 1. On the Canvas page, double-click the Cloud Volumes ONTAP working environment to create and manage volumes.
- 2. Click Add Volume > New Volume and select iSCSI and click Create Initiator Group. Click Continue.

Details & Protection		Protocol		
Volume Name:	Size (GB):	NFS	CIFS	iscst
nimavsscsi1	500			What about LUNs? 🕕
Snapshot Policy:		Initiator Group 🚯		
default		Map Existing Init	iator Groups 🢽	Create Initiator Group
Default Policy		Initiator Group		
		avsvmlG		

3. After the volume is provisioned, select the volume, and then click Target IQN. To copy the iSCSI Qualified Name (IQN), click Copy. Set up an iSCSI connection from the host to the LUN.

To accomplish the same for the host residing on Azure VMware Solution SDDC:

- a. RDP to the VM hosted on Azure VMware Solution SDDC.
- b. Open the iSCSI Initiator Properties dialog box: Server Manager > Dashboard > Tools > iSCSI Initiator.
- c. From the Discovery tab, click Discover Portal or Add Portal and then enter the IP address of the iSCSI target port.
- d. From the Targets tab, select the target discovered and then click Log on or Connect.
- e. Select Enable multipath, and then select Automatically Restore This Connection When the Computer Starts or Add This Connection to the List of Favorite Targets. Click Advanced.

Note: The Windows host must have an iSCSI connection to each node in the cluster. The native DSM selects the best paths to use.

		g on to a target usin arget and then clock		ion, type the	IP address or
Target	172	1.24.2.9			Quick Connect.
Discove	ared targets	i.		-	
					Refresh
Nome				Status	10 C
ddx Co	onnect.	idvanced options, s			Omet
dick Co To con	onnect.	onnect a target, se			Correct Decorvect
dick Co To con then d	pletely disc ick Disconne get properti	onnect a target, se	ect the target and	e	

LUNs on storage virtual machine (SVM) appear as disks to the Windows host. Any new disks that are added are not automatically discovered by the host. Trigger a manual rescan to discover the disks by completing the following steps:

- 1. Open the Windows Computer Management utility: Start > Administrative Tools > Computer Management.
- 2. Expand the Storage node in the navigation tree.
- 3. Click Disk Management.
- 4. Click Action > Rescan Disks.

	Volume	Layout	Type	File System	Status		Capacity	Free Space	% Free	
System Tools	- (C)		Basic			rash Dump, Frimary Partition)		34.99 GB	63 %	
Task Scheduler	SSS_X64FREE_EN+4		Basic		Healthy (Primary Partition)		6.49 GB	0 MB	0%	
Event Vasver Shared Foldes Shared Foldes Local Users and Groups Orformance Device Manager Storage Windows Server Backup Disk Management Services and Applications	- System Reierved	Sample	Basic	NTFS	Healthy Gystern, Active, Pr	imary Partition)	500 M8	169 MB	345	
	40.00 G8	System Reserved 500 ME NTFS Healthy (System, Act	ive Frim	very Partition)	(ICJ 39.51 GB NTFS Healthy (Boot, Page Fide, C)	rash Dump,	Primary Parti	tion)	

When a new LUN is first accessed by the Windows host, it has no partition or file system. Initialize the LUN; and optionally, format the LUN with a file system by completing the following steps:

1. Start Windows Disk Management. 2. Right-click the LUN, and then select the required disk or partition type. 3. Follow the instructions in the wizard. In this example, drive E: is mounted Ecomputer Management File Action View Help 💠 🔿 🙇 📆 🖬 🖽 📼 S Computer Management (Local Volume Capacity Free Space % Free) 39.51 GB 23.95 GB 61 % 499.87 ... 499.73 GB 100 % 9.97 GB 9.91 GB 100 % 5.97 GB 9.91 GB 100 % Layout Type File System Status (C)
 OBdisk (E)
 OBDisk2 (F) Healthy (Boot, Page File, Crash Dump, Primary Partitio Healthy (Primary Partition) Healthy (Primary Partition) II System Tools NTES Simple Basic NTFS Simple Basic NTFS Simple Basic NTFS () Task Scheduler Event Viewer SSS_X64FREE_EN-US_DV9 (D) Simple Basic UDF Simple Basic NTFS Shared Folders Healthy (Primary Partition 6.49.GB 0 MB 0% Healthy (System, Active, Primary Partition) 500 MB 169 MB 34% Coal Oesi and Unoug
 Coal Oesi and -Disk 1 DBdisk (Ed Basic 499.88 GB 499.87 GE NTFS Online Healthy (Primary Partition) -Disk 2 Bai DROok2 (Fd 9.97 GB Online 9.97 GB NTES by (Prim ary Partition) 💻 | 🔄 📗 😴 | This PC × Computer 0 View - 🛧 🔜 🕨 This PC V & Search This PC p v Folders (6) ✓ ★ Quick access Desktop Desktop Documents Downloads Downloads B Documents Music Pictures Videos Fictures . 🛫 nimoavsdemosn 🖻 Devices and drives (4) > 🛄 This PC Local Disk (Cr) DBdisk (E) DVD Drive (D:) SSS_X64FREE_EN-US_DV9 > 🥩 Network 23.9 GB free of 39.5 GB 499 GB free of 499 GB 0 bytes free of 6.49 GB DBDisk2 (F;) 9.93 GB free of 9.96 GB Network locations (3) inviden oll_share nimodemofilvol1 (\\172.24.3.4) (2:) imoavsdemosmbv1 (\\172.24.3.5) (\\172.24.2.15) (X:) (m) 🗶 🦱

Google Cloud VMware Engine Supplemental NFS Datastore with NetApp Cloud Volume Service

Customers can expand storage capacity on Google Cloud VMware Engine using NFS supplemental datastore with NetApp Cloud Volume Service.

Overview

Authors: Suresh Thoppay, NetApp

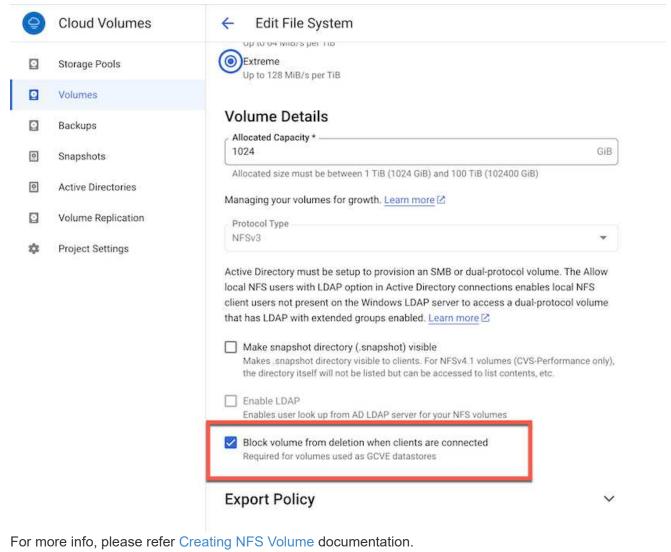
Customers that requires additional storage capacity on their Google Cloud VMware Engine (GCVE) environment can utilize Netapp Cloud Volume Service to mount as supplemental NFS datastore. Storing data on NetApp Cloud Volume Service allows customers to replicate between regions to protect from diaster.



Deployment steps to mount NFS datastore from NetApp CVS on GCVE

Provision CVS-Performance Volume

The NetApp Cloud Volume Service volume can be either provisioned by Using Google Cloud Console Using NetApp BlueXP portal or API To avoid accidental deletion of volume while VM is running, ensure the volume is marked as nondeletable as shown in screenshot below.



Ensure Private Connection on GCVE exists for NetApp CVS Tenant VPC.

To mount NFS Datastore, there should be a private connection exists between GCVE and NetApp CVS project.

For more info, please refer How to setup Private Service Access

Mount NFS datastore

For instructions on how to mount NFS datastore on GCVE, please refer How to create NFS datastore with NetApp CVS



As vSphere hosts are managed by Google, you don't have access to install NFS vSphere API for Array Integration (VAAI) vSphere Installation Bundle (VIB). If you need support for Virtual Volumes (vVol), please let us know.

If you like to use Jumbo Frames, please refer Maximum supported MTU sizes on GCP

Savings with NetApp Cloud Volume Service

To learn more about your potential saving with NetApp Cloud Volume Service for your storage demands on GCVE, please check NetApp ROI Calculator

Reference Links

- · Google Blog How to use NetApp CVS as datastores for Google Cloud VMware Engine
- NetApp Blog A better way to migrate your storage-rich apps to Google Cloud

NetApp Storage Options for GCP

GCP supports guest connected NetApp storage with Cloud Volumes ONTAP (CVO) or Cloud Volumes Service (CVS).

Cloud Volumes ONTAP (CVO)

Cloud volumes ONTAP, or CVO, is the industry-leading cloud data management solution built on NetApp's ONTAP storage software, available natively on Amazon Web Services (AWS), Microsoft Azure and Google Cloud Platform (GCP).

It is a software-defined version of ONTAP that consumes cloud-native storage, allowing you to have the same storage software in the cloud and on-premises, reducing the need to retrain you IT staff in all-new methods to manage your data.

CVO gives customers the ability to seamlessly move data from the edge, to the data center, to the cloud and back, bringing your hybrid cloud together — all managed with a single-pane management console, NetApp Cloud Manager.

By design, CVO delivers extreme performance and advanced data management capabilities to satisfy even your most demanding applications in the cloud

Cloud Volumes ONTAP (CVO) as guest connected storage

Cloud Volumes ONTAP shares and LUNs can be mounted from VMs that are created in the GCVE private cloud environment. The volumes can also be mounted on the Linux client and on Windows client and LUNS can be accessed on Linux or Windows clients as block devices when mounted over iSCSI because Cloud Volumes ONTAP supports iSCSI, SMB, and NFS protocols. Cloud Volumes ONTAP volumes can be set up in a few simple steps.

To replicate volumes from an on-premises environment to the cloud for disaster recovery or migration purposes, establish network connectivity to Google Cloud, either using a site-to-site VPN or Cloud Interconnect. Replicating data from on-premises to Cloud Volumes ONTAP is outside the scope of this document. To replicate data between on-premises and Cloud Volumes ONTAP systems, see xref:./ehc/Setting up data replication between systems.



Use Cloud Volumes ONTAP sizer to accurately size the Cloud Volumes ONTAP instances. Also monitor on-premises performance to use as inputs in the Cloud Volumes ONTAP sizer.

1. Log in to NetApp Cloud Central—the Fabric View screen is displayed. Locate the Cloud Volumes ONTAP tab and select Go to Cloud Manager. After you are logged in, the Canvas screen is displayed.

 Cloud Ma	nager			Account ~	Workspace cloud_heroes	 Connet fixawsc 	tor 👻 prinecto	
Canvas	Replication	Backup & Restore	K8s	Data Sense	File Cache	Compute	Sync	All Services (+8) ~
Canv	as							Go to Canvas View
🕝 Add W	orking Environment							

2. On the Cloud Manager Canvas tab, click Add a Working Environment and then select Google Cloud Platform as the cloud and the type of the system configuration. Then, click Next.

Canvas	Replication	Backup & Restore	KBS	Data Sense	File Cache	Compute	Sync	All Services (
Add Work	ling Environme	nt				_					×
		Microsoft Acure	Ana	aws on Web Services	Google Cloud Plat	O lorm	On-Premises				
				Choos	e Type						
		Cloud Volumes ON	ТАР	Cloud Volum	es ONTAP HA	Cloud Vol	() umes Service				
		Single Node			allability		waitability				

3. Provide the details of the environment to be created including the environment name and admin

reate a New Work	ing Environment	Details and Cr	edentials
Previous Step	CV-Performance-Testing Google Cloud Project	HCLMainBillingAccountSubs Marketplace Subscription	Edit Project
	Details		Credentials
	Working Environment Name	(Cluster Name)	User Name
	cvogcveva		admin
	Service Account		Password
	 Notice: A Google Cloud se to use two features: backing 	지 것은 물건 것이 있는 일정 등 것이 같이 많은 것이다.	Confirm Password
		Continue	

 Select or deselect the add-on services for Cloud Volumes ONTAP deployment, including Data Sense & Compliance or Backup to Cloud. Then, click Continue.

HINT: A verification pop-up message will be displayed when deactivating add-on services. Add-on services can be added/removed after CVO deployment, consider to deselect them if not needed from the beginning to avoid costs.

Data Sense & Compliance			Previous Step
Backup to Cloud	~	Data Sense & Compliance	
$\overline{\mathbf{Q}}$	~	Backup to Cloud	
WARNING:By turning off Backup to Cloud, future data recovery will not be possible in case of data corruption or los		WARNING:By turning off Backup to Cloud, future data recovery will not be possible in case of data corruption or loss	

5. Select a location, choose a firewall policy, and select the checkbox to confirm network connectivity to Google Cloud storage.

Previous Step	Location	Connectivity
	GCP Region	VPC
	europe-west3 •	cloud-volumes-vpc •
	GCP Zone	Subnet
	europe-west3-c •	10.0.6.0/24
		Firewall Policy
	I have verified connectivity between the target VPC and Google Cloud storage.	 Generated firewall policy Use existing firewall policy
reemium o	cense option: Pay-As-You-Go or BYOL for us ption is used. Then, click on Continue.	sing existing license. In this example, arging Methods & NSS Account
reemium o Create a New W	cense option: Pay-As-You-Go or BYOL for us ption is used. Then, click on Continue. forking Environment Cloud Volumes ONTAP Cha	sing existing license. In this example, arging Methods & NSS Account
Treemium o Create a New W	cense option: Pay-As-You-Go or BYOL for us ption is used. Then, click on Continue. forking Environment Cloud Volumes ONTAP Cha	sing existing license. In this example, arging Methods & NSS Account NetApp Support Site Account
Treemium o Create a New W	cense option: Pay-As-You-Go or BYOL for us ption is used. Then, click on Continue. forking Environment Cloud Volumes ONTAP Cha	sing existing license. In this example, arging Methods & NSS Account NetApp Support Site Account
Treemium o Create a New W	cense option: Pay-As-You-Go or BYOL for us ption is used. Then, click on Continue. forking Environment Cloud Volumes ONTAP Cha	sing existing license. In this example, arging Methods & NSS Account NetApp Support Site Account Learn more about NetApp Support Site (NSS) account: NetApp Support Site Account
reemium o Create a New W ↑ Previous Step	cense option: Pay-As-You-Go or BYOL for us ption is used. Then, click on Continue. forking Environment Cloud Volumes ONTAP Cha bud Volumes ONTAP Charging Methods	sing existing license. In this example, arging Methods & NSS Account NetApp Support Site Account Learn more about NetApp Support Site (NSS) account
reemium o Create a New W ↑ Previous Step	cense option: Pay-As-You-Go or BYOL for us ption is used. Then, click on Continue. forking Environment Cloud Volumes ONTAP Cha bud Volumes ONTAP Charging Methods	sing existing license. In this example, arging Methods & NSS Account NetApp Support Site Account Learn more about NetApp Support Site (NSS) account NetApp Support Site Account

7. Select between several preconfigured packages available based on the type of workload that will be deployed on the VMs running on VMware cloud on AWS SDDC.

HINT: Hoover your mouse over the tiles for details or customize CVO components and ONTAP version by clicking on Change Configuration.

Select a pre	econfigured Cloud Volumes ONTAP system that best Preconfigured settings can be n		onfiguration. Change Configuration
	5	\$0	
POC and small workloads Up to 500GB of storage	Database and application data production workloads	Cost effective DR	Highest performance production workloads

8. On the Review & Approve page, review and confirm the selections. To create the Cloud Volumes ONTAP instance, click Go.

Create a New Work	ng Environment	Review & Approve		
Previous Step CVOgCVEVal GCP europe-we	st3		5	how API request
	TAP instance will be registered with NetApp support of	inder the NS5 Account mchad.		
I understand that	Cloud Manager will allocate the appropriate GCP reso	irces to comply with my above requirements. More info	ormation >	
I understand that Overview	Cloud Manager will allocate the appropriate GCP reso Networking Storage	irces to comply with my above requirements. More inf	srmation >	
Overview		irces to comply with my above requirements. More info	n2-standard-4	
	Networking Storage			

9. After Cloud Volumes ONTAP is provisioned, it is listed in the working environments on the Canvas page.

#	Cloud Mar	iager				Account ~ Netapp_POC	Workspace cloud_herbe		Connector		۵	Ð	0	8
	Canvas	Replication	Backup & Restore	KBS	Data Sense	File Cache	Compute	Sync	All Service	es (+7) ~				
	Canvo	as :									E	Go to	Tabular	View
	Add Wo	rking Environment						Worki	ng Environn	nents				
	1	cvogcve01			DatacenterDude	-		0		id Volume 5 GiB: Prav				
		Cloud Volumes ONTA	۵. ۲		Azure NetApp Fi	ез		0		for ONTAP ovisioned (10.000		y)	
								Ē		re NetApp TiB Provisi		oarity		

1. After the working environment is ready, make sure the CIFS server is configured with the appropriate DNS and Active Directory configuration parameters. This step is required before you can create the SMB volume.

HINT: Click on the Menu Icon (°), select Advanced to display more options and select CIFS setup.

Volumes Replications		© ∪ ∪ ⊙ + Ξ
Create a CIFS server	+ Advanced	
DNS Primary IP Address	Active Directory Domain to join	
192.168.0.16	ningcveval.com	
DN5 Secondary IP Address (Optional)	Credentials authorized to join the domain	
Example: 127.0.0.1	administrator	

2. Creating the SMB volume is an easy process. At Canvas, double-click the Cloud Volumes ONTAP working environment to create and manage volumes and click on the Create Volume option. Choose the appropriate size and cloud manager chooses the containing aggregate or use advanced allocation mechanism to place on a specific aggregate. For this demo, CIFS/SMB is selected as the protocol.

Volume Name: Size (GB): NFS CIFS ISCSI cvogcvesmbvol01 10 Share name: Permissions: Snapshot Policy: • Cips Full Control default • Users / Groups: •	cvogcvesmbvol01 10 Snapshot Policy: Share name: default •
Share name: Permissions: Shapshot Policy: cvogcvesmbvol01_share default • Default Policy Users / Groups:	Snapshot Policy: cvogcvesmbvol01_share Full Control * default *
Snapshot Policy: cvogcvesmbvol01_share Full Control default • • Default Policy Users / Groups:	Snapshot Policy: cvogcvesmbvol01_share Full Control • default •
default	default -
Default Policy Users / Groups:	
	Sector and the sector
	Default Policy Users / Groups:
Everyone;	Everyone;
Valid users and groups separated by a semicolon	Valid users and groups separated by a semicolon

3. After the volume is provisioned, it will be availabe under the Volumes pane. Because a CIFS share is provisioned, give your users or groups permission to the files and folders and verify that those users can access the share and create a file. This step is not required if the volume is replicated from an on-premises environment because the file and folder permissions are all retained as part of SnapMirror replication.

HINT: Click on the volume menu (°) to display its options.

INFO		CAPACITY	
Disk Type	PD-SSD		■ 1.84 MB
Tiering Policy	None	10 GB Allocated	Disk Used

4. After the volume is created, use the mount command to display the volume connection instructions, then connect to the share from the VMs on Google Cloud VMware Engine.

Volu	mes Repl	ications				
	Nount Volun	ne cvogcvesmb	vol01			
o to yoi	ur machine and e	enter this command				
\\10.	0.6.251\cvogcv	esmbvol01_share		Ē	Сору	
py the nning o	on the Google C	and use the Map Ne loud VMware Engin	e.			rolume on the $lacksquare$
py the nning o pecify the	on the Google C		e.			rolume on the ∖
ppy the nning o pecify the rive:	on the Google C e drive letter for the c	loud VMware Engin	e.			rolume on the ∖
py the nning o pecify the rive:	on the Google C e drive letter for the c	loud VMware Engin onnection and the folder th v gcvesmbvol01_share	e. Nat you want to	onnect to:		rolume on the ∖
ppy the nning o pecify the rive:	e drive letter for the co Y: \\10.0.6.251\cvo	loud VMware Engin onnection and the folder th v gcvesmbvol01_share share	e. Nat you want to	onnect to:		rolume on the V
py the nning o	on the Google C e drive letter for the c Y: \\10.0.6.251\cvoj Example: \\server\ Reconnect at s	loud VMware Engin onnection and the folder th v gcvesmbvol01_share share	e. Nat you want to	onnect to:		rolume on the V
py the nning o pecify the rive:	e drive letter for the co Y: \\10.0.6.251\cvog Example: \\server Reconnect at s Connect using	loud VMware Engin onnection and the folder th consection and the folder th govesmbvol01_share share ign-in	e. Nat you want to	onnect to: Browse	ount the v	rolume on the ∖
py the ining o becify the	e drive letter for the co Y: \\10.0.6.251\cvog Example: \\server Reconnect at s Connect using	loud VMware Engin onnection and the folder th consection and the folder th govesmbvol01_share share ign-in different credentials	e. Nat you want to	onnect to: Browse	ount the v	rolume on the ∖

Once mapped, it can be easily accessed, and the NTFS permissions can be set accordingly. 💣 | 🛃 📗 = | Network - 🗆 X 🗌 👎 🛫 l 📴 📒 🖛 l cvogcvesmbvol01_share (\\10.0.6.251) (Y:) × 4 Home Share View 0 ÷ ↑ 👳 > This PC ⇒ cvogcvesmbvol01_share (\\10.0.6.251) (Y:) > ✓ Ŏ Search cvogcvesmbvol01_sha... , P 7 1 Net 6 Name Date modified Type Size # Quick access foo1 11/9/2021 10:59 AM File folder Desktop foo2 11/9/2021 10:59 AM File folder Downloads 1 Documents A Pictures 1 This PC

To connect the cloud volumes ONTAP LUN to a host, complete the following steps:

- 1. On the Canvas page, double-click the Cloud Volumes ONTAP working environment to create and manage volumes.
- 2. Click Add Volume > New Volume and select iSCSI and click Create Initiator Group. Click Continue.

Accold A form though A form though Constrained A form though A form though		a comp of ri	otection				Protocol			
Snapshot Policy: default Default Policy Mop Existing Initiator Group Miliator Group WinlG Operating System Type Windows VMeree Cloud - ritap-fracebras X © Viphere - windch1 - Summary X windows Continue VMeree Cloud - ritap-fracebras X © Viphere - windch1 - Summary X windows Continue VMeree Cloud - ritap-fracebras X © Viphere - windch1 - Summary X windows Continue VMeree Cloud - ritap-fracebras X © Viphere - windch1 - Summary X windows © Continue VMeree Cloud - ritap-fracebras X © Viphere - windch1 - Summary X windows © Continue Vision fracebras X © Viphere - windch1 - Summary X windows © Continue Vision fracebras X © Viphere - windch1 - Summary X windows © Continue Continue Vision fracebras X © Viphere - windch1 - Summary X windows © Continue		Volume Name:			Size (GB):	0	NFS	CIFS	iscsi	
Snapshot Policy: default Default Policy Map Existing Initiator Groups Initiator Group WindG Operating System Type Windows Continue VMwee Cloud - ntap-for-dem X @ vSphere - vmcdol1 - Summary X vmcdol1 X methods with a sphere		cvogcvescsilun	101		10				What about LUNs	
Map Existing Initiator Group I		Snapshot Policy:					Initiator Group 🎚			
WiniG Operating System Type Windows Continue Winese Cloud - intag-faz-demo X Vsphere - vmcdc01 - Summary X vmcdc01 x NetApp Cloud Manager x + Co -							Map Existing	Initiator Groups 🤅	Create Initiator Gro	up
Operating System Type Windows Continue VMessee Cloud - ntap-far-demox X Image: Second Lagority - Summary X Image: Second Lagority - Summary X Image: Second Lagority - Summary X Image: Second Lagority - Summary X Image: Second Lagority - Summary X Image: Second Lagority - Summary X Image: Second Lagority - Summary X Image: Second Lagority - Summary X Image: Second Lagority - Summary X Image: Second Lagority - Summary X Image: Second Lagority - Summary X Image: Second Lagority - Summary X Image: Second Lagority - Summary X Image: Second Lagority - Summary X Image: Second Lagority - Summary X Image: Second Lagority - Summary X Image: Second Lagority - Summary X Image: Second Lagority - Summary X Image: Second Lagority - Second La		Default Policy					Initiator Group			
Windows Continue VMware Cloud - ntap-fas-demo X vsphere - vmcdc01 - Summary X vmcdc01 x NetApp Cloud Manager x + Co - C C A = https://vcenter.sdddc-S2-37-127-104.vmwarevmc.com/uv/vebconsole.html/vmid=vm-1005&bomName=vmcdc01 00% Co Getting Stated EC2 Management Con. New Tab Co Coto Server Manager + Dashboard New Tab Co							WinlG			
Windows Continue Www.see Cloud - ntap-fas-demo X Voltore vmcdc01 - Summary X vmcdc01 x NetApp Cloud Manager x + Co										
VMwsre Cloud - ntap-far-demo X V vSphere + vincdc01 - Summary X vincdc01 x NetApp Cloud Manager X + CO - C <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td>Operating System</td> <td>Туре</td> <td></td> <td></td>							Operating System	Туре		
VMware Cloud - ntap-fas-demo X Vsphere + vmcdc01 - Summary X vmcdc01 x NetApp Cloud Manager x + Cold -							Windows			•
Control Visit COME TO DERVERT M None	ng Started 🥫 EC2			NET ADDL. 32.1	(-127-104 vmwan	evinc.com/u/ve	ebcansole.html?vmld=vm+100			C) Other Bo
A AD DDS AD DS AD DDS AD DS AD	ng Statted 🔋 EC2	Management Con.	New Tab	() () () () () () () () () ()	1201.762043-111 194		ebconsole.html?vmld=vm-100		eyboard Layout View Fullscreer	C) Other Bo
E hten f	ng Statted 😝 EC2	Management Con.	New Teb	e timerenaitie f	nor - Contractor The Second States Second States	8 49	ebcansole.html?vmld=vm-100	Enforce US K	eyboard Layout View Fullscreer	C) Other Bo
Model's Model.	ng Statted 💼 EC2	Management Con.	New Tab	name Paran Para name Para	No. 12 (1994) No. Sector Science (1997) No. 2 (1997) No.	n nine (historia takata) (digi ana musikikati / Tape ana kasata takata Masatata takata (historia		Enforce US K	eyboard Layout View Fullscreer	C) Other Bo
Walker 2.). Gener proceed (* 1	ng Statted 💼 EC2	Management Con.	New Tab New Tab Prove Tab	n m Para Para n m Para n m Para Para Para Para Para Para Para Para	No. 12 (1994) No. Sector Science (1997) No. 2 (1997) No.	n nine (historia takata) (digi ana musikikati / Tape ana kasata takata Masatata takata (historia		Enforce US K	eyboard Layout View Fullscreer	C Other Bc
Margadity	ng Statted 💼 EC2	Management Con.	New Tab New Tab Prove Tab	n m Para Para n m Para Na Para	No. 12 (1994) No. Sector Science (1997) No. 2 (1997) No.	n nine (historia takata) (digi ana musikikati / Tape ana kasata takata Masatata takata (historia		Enforce US K	eyboard Layout View Fullscreer	C) Other Bo
14970	ng Statted 💼 EC2	Management Con.	New Tab New Tab Prove Tab	n m Para Para n m Para Na Para	No. 12 (1994) No. Sector Science (1997) No. 2 (1997) No.	n nine (historia takata) (digi ana musikikati / Tape ana kasata takata Masatata takata (historia		Enforce US K	eycoard Layout Vow Fullscreen	C Other Bc
Services	ng Statted 💼 EC2	Management Con.	New Tab New Tab Prove Tab	n m Para Para n m Para Na Para	No. 12 (1994) No. Sector Science (1997) No. 2 (1997) No.	n nine (historia takata) (digi ana musikikati / Tape ana kasata takata Masatata takata (historia		Enforce US K	eycoard Layout Vow Fullscreen	Cother I

3. After the volume is provisioned, select the volume menu (°), and then click Target iQN. To copy the iSCSI Qualified Name (iQN), click Copy. Set up an iSCSI connection from the host to the LUN.

To accomplish the same for the host residing on Google Cloud VMware Engine:

- a. RDP to the VM hosted on Google Cloud VMware Engine.
- b. Open the iSCSI Initiator Properties dialog box: Server Manager > Dashboard > Tools > iSCSI Initiator.
- c. From the Discovery tab, click Discover Portal or Add Portal and then enter the IP address of the iSCSI target port.

- d. From the Targets tab, select the target discovered and then click Log on or Connect.
- e. Select Enable multipath, and then select Automatically Restore This Connection When the Computer Starts or Add This Connection to the List of Favorite Targets. Click Advanced.

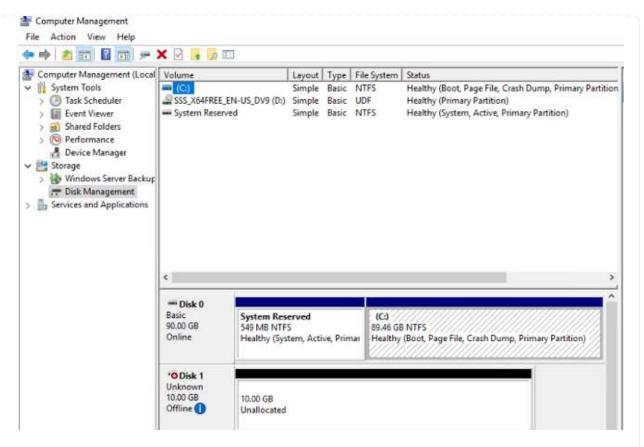


The Windows host must have an iSCSI connection to each node in the cluster. The native DSM selects the best paths to use.

€ 🕞 🔹 Ser	iSCSE Initiato	r Properties			0
Ser Ser		scovery Pavorite Targets Volumes and D	Devices RAD	0.5 Configuration	
Dashboard	Quick Conn To discove DNS name	ect r and log on to a target using a basic conne of the target and then click Quick Connect.	ection, type th	e ≫ address or	
Local Server	Target:	10.0.6.250		Quick Connect	I
AD DS	Discovered targets			Refresh	i
File and Storage Ser	Name		Statu	6	Ĩ.
	dick Conne	201		Carried	
	then dick (tely disconnect a target, select the target a Xisconnect.		Ownrect	1
	then dick For target select the For configu		ons,	Disconvect Properties - Devotes -	
	then dick For target select the For configu	Nsconnect, properties, including configuration of sesse target and click Properties. uration of devices associated with a target,	ons,	Properter	

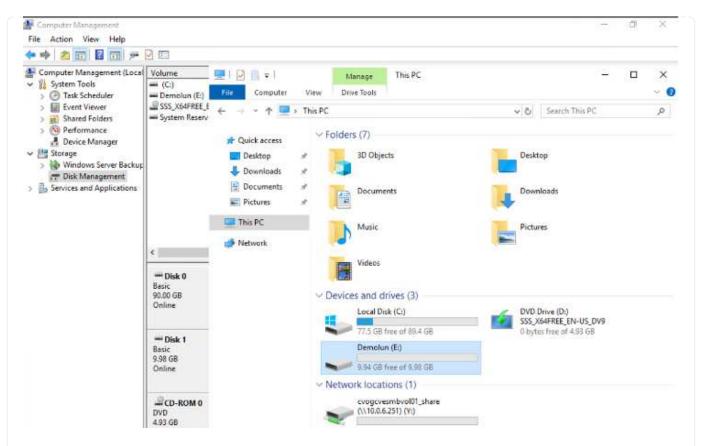
LUNs on storage virtual machine (SVM) appear as disks to the Windows host. Any new disks that are added are not automatically discovered by the host. Trigger a manual rescan to discover the disks by completing the following steps:

- 1. Open the Windows Computer Management utility: Start > Administrative Tools > Computer Management.
- 2. Expand the Storage node in the navigation tree.
- 3. Click Disk Management.
- 4. Click Action > Rescan Disks.



When a new LUN is first accessed by the Windows host, it has no partition or file system. Initialize the LUN; and optionally, format the LUN with a file system by completing the following steps:

- 5. Start Windows Disk Management.
- 6. Right-click the LUN, and then select the required disk or partition type.
- 7. Follow the instructions in the wizard. In this example, drive F: is mounted.



On the Linux clients, ensure the iSCSI daemon is running. Once the LUNs are provisioned, refer to the detailed guidance on iSCSI configuration with Ubuntu as an example here. To verify, run Isblk cmd from the shell.

	nimubulli	:-\$	LSDLK			
NAME	MAJ:MIN	RM	SIZE	RO	TYPE	MOUNTPOINT
loop0	7:0	0	55.4M	1	loop	/snap/core18/2128
Loop1	7:1	Θ	219M	1	loop	/snap/gnome-3-34-1804/72
Loopz	7:2		65.1M	1	loop	/snap/gtk-common-themes/1515
Loop3	7:3	0	51M			/snap/snap-store/547
Loop4	7:4	0	32.3M	1	loop	/snap/snapd/12704
Loop5	7:5	0	32.5M	1	loop	/snap/snapd/13640
loop6	7:6	0	55.5M	1	loop	/snap/core18/2246
Loop7	7:7	0	4K	1	loop	/snap/bare/5
Loop8	7:8	0	65.2M	1	loop	/snap/gtk-common-themes/1519
sda	8:0	0	16G	0	disk	
-sda1	8:1	0	512M	0	part	/boot/efi
-sda2	8:2	0	1K	0	part	
-sda5	8:5	e	15.5G	0	part	1
sdb	8:16	0	16	. 0	disk	

iyaz@ninubu0						
ilesystem	Size	Used	Avail		Mounted on	
idev	1.9G	0	1.96	0%	/dev	
mpfs	394M	1.5M	392M	1%	/run	
dev/sda5	16G	7.6G	6.9G	53%	/	
mpfs	2.0G	0	2.0G	0%	/dev/shm	
mpfs	5.0M	0	5.0M	0%	/run/lock	
mpfs	2.0G	0	2.06	0%	/sys/fs/cgroup	
dev/loop1	219M	219M	6		/snap/gnome-3-34-1804/72	
dev/loop2	66M	66M	8	166%	/snap/gtk-common-themes/1515	
dev/loop3	51M	51M	.0	100%	/snap/snap-store/547	
dev/loop0	56M	56M	0	100%	/snap/core18/2128	
dev/loop4	33M	33M	8	100%	/snap/snapd/12764	
dev/sda1	511M	4.0K	511M	1%	/boot/efi	
mpfs	394M	64K	394M	1%	/run/user/1000	
dev/loop5	33M	33M	0	100%	/snap/snapd/13640	
dev/loop6	56M	56M	8	100%	/snap/core18/2246	
dev/loop7	128K	128K	0	100%	/snap/bare/5	
dev/loop8	66M	66M	θ	100%	/snap/gtk-common-themes/1519	
dev/sdb	976M	2.6M	987M	1%	/mnt	

To mount the Cloud Volumes ONTAP (DIY) file system from VMs within Google Cloud VMware Engine, follow the below steps:

Provision the volume following the below steps

- 1. In the Volumes tab, click Create New Volume.
- 2. On the Create New Volume page, select a volume type:

	cvogcver	nfsvol01					
	INFO		CAPACITY	CAPACITY			
	Disk Type	PD-SSD		■ 6.08 GB			
	Tiering Policy	None	11.05 GB Allocated	Disk Used			
	ne Volumes tab, place Int Command.	e your mouse cursor o	over the volume, select the	e menu icon (º), and then clic			
	Volumes	Replications					
4	O Mount V	olume cvogc	venfsvol01				
G	o to your <mark>Linux m</mark> a	achine and enter t	his mount command				
	mount 10.0.6.2	51:/cvogcvenfsv	ol01 <dest_dir></dest_dir>	Сору			
4. Clicl	k Сору.						
	nect to the designate	d Linux instance.					
				n the appropriate credentials			

\$ sudo mkdir /cvogcvetst

root@nimubu01:~# sudo mkdir cvogcvetst

8. Mount the Cloud Volumes ONTAP NFS volume to the directory that is created in the previous step.

```
sudo mount 10.0.6.251:/cvogcvenfsvol01 /cvogcvetst
root@nimubu01:~# sudo mount -t nfs 10.0.6.251:/cvogcvenfsvol01 cvogcvetst
nimubu01
                                                                                        Enforce US Keyboard Layout View Fullscreen Send Ctrl+Alt+De
                                       Terminal *
                                                                   Nov 16 12:42
                                                                                                A # 0 .
                                                                 root@nimubu01: -
                                      oot@ninubu01:-# df
ilesysten
                                                               blocks
                                                                         Used
                                                                                        0%
1%
                                                                         1432
                                                                       7832332
                                                                               726804 201135
                                                                  5120
                                                                               201135
                                                               2011352
                                                                        12
5683
                                                                        56832
                                                                        6668
                                                                        52224
                                                                 52224
                                                                66816
                                                                        66816
                                                                                      100% /snap/gtk-co
                                                               33280 224256
                                                                       33280
                                                                                             ap/snapd/1364
                                                                523248
                                                             515010816
                                                                      42016812
                                                                                              e/nlyaz/cvs1
                                                                                          /snap/snapd/13831
                                                             43264
                                                                        43264
                                                                                      100N
                                                                       8577536
                                                                               4622016
                                                      afsvol01
```

Cloud Volumes Service (CVS)

Cloud Volumes Services (CVS) is a complete portfolio of data services to deliver advanced cloud solutions. Cloud Volumes Services supports multiple file access protocols for major cloud providers (NFS and SMB support).

Other benefits and features include: data protection and restore with Snapshot; special features to replicate, sync and migrate data destinations on-prem or in the cloud; and consistent high performance at the level of a dedicated flash storage system.

Cloud Volumes Service (CVS) as guest connected storage

Configure Cloud Volumes Service with VMware Engine

Cloud Volumes Service shares can be mounted from VMs that are created in the VMware Engine environment. The volumes can also be mounted on the Linux client and mapped on the Windows client because Cloud Volumes Service supports SMB and NFS protocols. Cloud Volumes Service volumes can be set up in simple steps.

Cloud Volume Service and Google Cloud VMware Engine private cloud must be in the same region.

To purchase, enable and configure NetApp Cloud Volumes Service for Google Cloud from the Google Cloud Marketplace, follow this detailed guide.

To create and mount NFS volumes, complete the following steps:

1. Access Cloud Volumes from Partner Solutions within the Google cloud console.

÷ -	C 🖬 console.cloud	google o	om/bome/dashboard?	project.»cv-performance-testing		🗞 🕁 😒 Incogn	ito (1) Upda	ti i
=	Google Cloud Platfo	erm i	CV-Performance-Te	sting 👻 🔍 9. Search products and resou		v 10 0	• 1 (0
ŧ.	Home	>	MMENDATIONS	_			CUSTOM	IZE
*	Pins appear here	×		Compute Engine		Google Cloud Platform status		-
PARTI	NER SOLUTIONS			CPU (N)	•	All services normal		
	Redis Enterprise Apache Kafka on Co				102%	→ Go to Cloud status dashboard		
8	Databricks				85%	-		
٨	DataStax Astra				40%	Billing Estimated charges	\$ USD \$0.00	
\$	Elasticsearch Service		Volumes	12:15 12:30 12:45 1.764	0	For the billing period starting Nov 1, 2021		
0	MongoDB Atlas		Backups Snapshots	Instance/cpu/utilization: 3.39%		View detailed charges		
0	Neo4j Aura Professi		Active Directories	→ Go to Compute Engine				
0	Cloud Volumes	>	Volume Replication			Monitoring	1	

2. In the Cloud Volumes Console, go to the Volumes page and click Create.

	Google Cloud Platform	s cv	Perfe	rmance Testing	۹.		ucts and reso				3.	0	۰	1	8
Ð	Cloud Volumes	Volur	mes	CREA	TE 🖀 DELE	TE									(
	Volumes	Quick r	efere	nce for Cloud Volum	es Private Servic	e Access 🖾 AP	I L2 Shared VPC	support 🖾 Granular permi	ssions 🗠						
	Backups	Ŧ	Filter	Search for volume	rs by name, 10, re	gion, etc.							0	ш	
Ð	Snapshots			ID	Name	Region	Zone	Zone Redundancy	Life Cycle	Billi	ng Label		State	e Detai	is .
	Active Directories Volume Replication		0	DacBaB3d- 03d8-c9db- 2aba-	testnfsds01	europe- west3			available				Avai	lable f	bř s
			0	189c7535445b 330f35e2- b0c6-98b3- ec7a- 8dd4ea7ba00e	gcpive-da4	europe- west3			available				Avai	lable f	Dri
			0	7d0a6f0d- 3e0a-50c3- 5295- 5152040681fc	gcp-ve-ds3	europe- west3			available				Avai	lable f	ors.
		0	0	8cae6850- 0919-4eaf- af42-	gcve-ds-2	europe- west3			available				Avai	lable f	ors

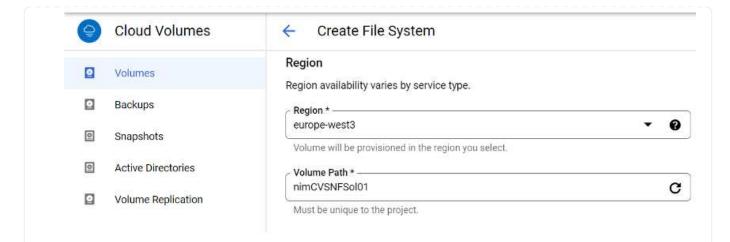
3. On the Create File System page, specify the volume name and billing labels as required for chargeback mechanisms.

Oloud Volumes	← Create File System
2 Volumes	
Backups	Volume Name
Snapshots	nimCVNFSvol01
Active Directories	A human readable name used for display purposes.
Volume Replication	Billing Labels
	Label your volumes for billing reports, queries. Supported with CVS-Performance service type; can be set with CVS service type but not available for billing at this time.
	+ ADD LABEL

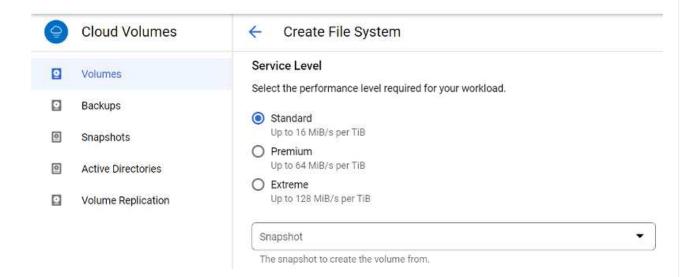
4. Select the appropriate service. For GCVE, choose CVS-Performance and desired service level for improved latency and higher performance based on the application workload requirements.

9	Cloud Volumes	← Create File System
0	Volumes	Service Type
2	Backups	Cloud Volumes Service is offered as two service types: CVS and CVS-Performance. Select the service type that matches your workload needs. Region availability 🖄 varies by
0	Snapshots	service type. Learn more 🖄
0	Active Directories	O CVS Offers volumes created with zonal high availability.
0	Volume Replication	 CVS-Performance Offers 3 performance levels and improved latency to address higher performance application requirements.
		Volume Replication
		Secondary Select to create volume as a destination target for volume replication. Applicable only to CVS-performance volumes.

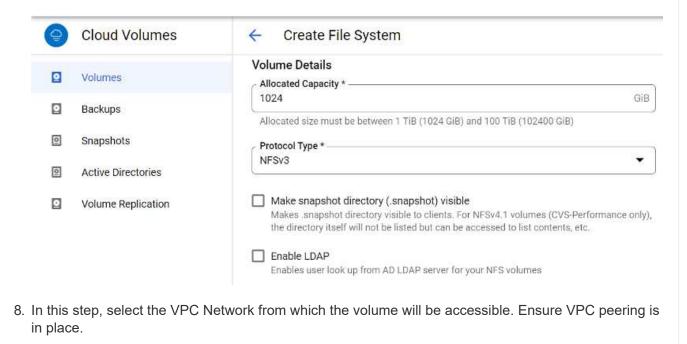
5. Specify the Google Cloud region for the volume and volume path (The volume path must be unique across all of cloud volumes in the project)



6. Select the level of performance for the volume.



7. Specify the size of the volume and the protocol type. In this testing, NFSv3 is used.

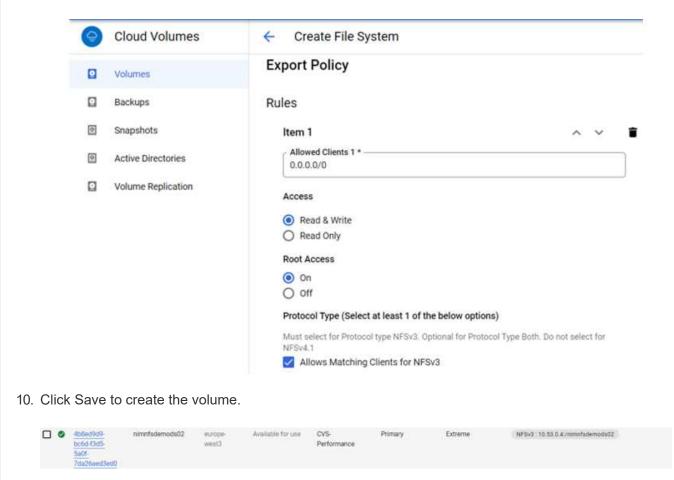


HINT: If VPC peering has not been done, a pop-up button will be displayed to guide you through the peering commands. Open a Cloud Shell session and execute the appropriate commands to peer your VPC with Cloud Volumes Service producer. In case you decide to prepare VPC peering in beforehand, refer to these instructions.

9	Cloud Volumes	← Create File System
	Volumes	Network Details
Ø	Backups	Provide the host project name when deploying in a shared VPC service project.
0	Snapshots	VPC Network Name *
0	Active Directories	Select the VPC Network from which the volume will be accessible. This cannot be changed later.
0	Volume Replication	Use Custom Address Range
		Reserved Address range netapp-addresses

9. Manage the Export policy rules by adding the appropriate rules and Select the checkbox for the corresponding NFS version.

Note: Access to NFS volumes won't be possible unless an export policy is added.



Before preparing to mount the NFS volume, ensure the peering status of private connection is listed as Active. Once status is Active, use the mount command.

To mount an NFS volume, do the following:

- 1. In the Cloud Console, go to Cloud Volumes > Volumes.
- 2. Go to the Volumes page
- 3. Click the NFS volume for which you want to mount NFS exports.
- 4. Scroll to the right, under Show More, click Mount Instructions.

To perform the mounting process from within the guest OS of the VMware VM, follow the below steps:

- 1. Use SSH client and SSH to the virtual machine.
- 2. Install the nfs client on the instance.
 - a. On Red Hat Enterprise Linux or SuSE Linux instance:

sudo yum install -y nfs-utils

b. On an Ubuntu or Debian instance:

sudo apt-get install nfs-common

3. Create a new directory on the instance, such as "/nimCVSNFSol01":

```
sudo mkdir /nimCVSNFSol01
```

Ubuntu-20.04-00		Enforce US Keyboard Layout	View Fullscreen	Send Ctr	+AR+Do
Activities 🖸 Terminal 🕶	Nov 3 06:22				4 6 C
IR Flodelnevni:-5 sudo ekdir /etmcvsNFSplei	floadmin@vm1: -				

4. Mount the volume using the appropriate command. Example command from the lab is below:

```
sudo mount -t nfs -o rw,hard,rsize=65536,wsize=65536,vers=3,tcp
10.53.0.4:/nimCVSNFSol01 /nimCVSNFSol01
```

Filesystem	1K-blocks	Used	Available	Use%	Mounted on
udev	16409952	6.00	16409952	0%	/dev
tnpfs	3288328	1580	3286748	1%	/run
/dev/sdb5	61145932	19231356	38778832	34%	1
tnpfs	16441628	6	16441628	8%	/dev/shm
tnpfs	5120	6	\$120	6%	/run/lock
tnpfs	16441628	a	16441628	0%	/sys/fs/cgroup
/dev/loop0	128	128	0	100%	/snap/bare/5
/dev/loop1	56832	56832	6	100%	/snap/core18/2128
/dev/loop2	66688	66688	6	100%	/snap/gtk-common-themes/1515
/dev/loop4	66816	66816	0	100%	/snap/gtk-connon-thenes/1519
/dev/loop3	52224	52224	0	100%	/snap/snap-store/S47
/dev/loop5	224256	224256	0	166%	/snap/gnone-3-34-1804/72
/dev/sdb1	523248	100-12	523244	1%	/boot/efi
tnpfs	3288324	28	3288296	1%	/run/user/1000
10.53.0.4:/gcve-ds-1	107374182400	1136086016	106238096384	2%	/base
/dev/mapper/nfsprdvg1-prod01	419155968	55384972	363778996	14%	/datastore1
/dev/loop8	33280	33280	0	100%	/snap/snapd/13270
/dev/loop6	33280	33280	0	100%	/snap/snapd/13640
/dev/loop7	56832	56832	0	100%	/snap/core18/2246
10.53.0.4:/n1mCV5NFSol01	107374182400	256	107374182144	1%	/nimCVSNFSol01
root@vml:-#					

For SMB volumes, make sure the Active Directory connections is configured prior to creating the SMB volume.

The a Windows Active Directory connection to your existing AD server. This is a prerequisite step before creating volumes with the SMB protocol type. Learn more (2) The search for Active Directory connections by ID, username, DNS, netBIOS, region, etc.	ctive	Directory cor	nections	+ CREATE	DELETE.						
	eate a	Windows Active D	rectory connection to yo	our existing AD se	rver. This is a prerequisite	step before creating vo	lumes with the SMB pro	tocol type. Learn	more (2		
		and the state of the state			a the american and a second	21				•	
	₹ F	Iter Search for A	ctive Directory connection	ons by ID, useman DNS Servers	ne, DNS, netBIOS, region, et NetBIOS Prefix	OU Path	AD Server Name	KDC IP	Region	O Sta	III tus

Once the AD connection is in place, create the volume with the desired service level. The steps are like creating NFS volume except selecting the appropriate protocol.

- 1. In the Cloud Volumes Console, go to the Volumes page and click Create.
- 2. On the Create File System page, specify the volume name and billing labels as required for chargeback mechanisms.



Volume Name

Name * ---

nimCVSMBvol01

A human readable name used for display purposes.

Billing Label

Label your volumes for billing reports, queries. Supported with CVS-Performance service type; can be set with CVS service type but not available for billing at this time.



3. Select the appropriate service. For GCVE, choose CVS-Performance and desired service level for improved latency and higher performance based on the workload requirements.

Create File System

Service Type

←

Cloud Volumes Service is offered as two service types: CVS and CVS-Performance. Select the service type that matches your workload needs. <u>Region availability</u> is varies by service type. Learn more is



Offers volumes created with zonal high availability.



Offers 3 performance levels and improved latency to address higher performance application requirements.

Volume Replication

Secondary

Select to create volume as a destination target for volume replication. Applicable only to CVS-performance volumes.

4. Specify the Google Cloud region for the volume and volume path (The volume path must be unique across all of cloud volumes in the project)



Region

Region availability varies by service type.

europe-west3	Ŧ	0
Volume will be provisioned in the region you select.		
Volume Path *		

C

nimCVSMBvol01

Must be unique to the project.

5. Select the level of performance for the volume.

0.0	rvice Level	
Sel	lect the performance level required for your workload.	
0	Standard Up to 16 MiB/s per TiB	
0	Premium Up to 64 MIB/s per TIB	
0	Extreme Up to 128 MiB/s per TiB	
s	inapshot 👻	
T	he snapshot to create the volume from.	
Зре	cify the size of the volume and the protocol type. In this testing, SMB is used.	
÷	Create File System	
Vo	lume Details	
A	llocated Capacity *	
(A)	Ilocated Capacity * 024 GiB	
(A)	llocated Capacity *	
	Ilocated Capacity *	
	Ilocated Capacity *	
Al Al SI	Ilocated Capacity * GiB Ilocated size must be between 1 TiB (1024 GiB) and 100 TiB (102400 GiB) rotocol Type * MB Make snapshot directory (.snapshot) visible Makes snapshot directory visible to clients. For NFSv4.1 volumes (CVS-Performance only), the directory itself will not be listed but can be accessed to list contents, etc. Enable SMB Encryption Enable this option only if you require encryption of your SMB data traffic.	
Al Al SI	Ilocated Capacity * 024 GiB Ilocated size must be between 1 TiB (1024 GiB) and 100 TiB (102400 GiB) rotocol Type * MB Make snapshot directory (.snapshot) visible Makes .snapshot directory visible to clients. For NFSv4.1 volumes (CVS-Performance only), the directory itself will not be listed but can be accessed to list contents, etc. Enable SMB Encryption	
Al Al SI	Ilocated Capacity *	

		PC configur e host projec		hen deployi	ng in a shar	ed VPC ser	vice project.	
1.1.1.1.1.1.1.1	C Network	Name * Nes-vpc						•
Sele		°C Network f	rom which	n the volum	e will be acc	essible. Th	is cannot be	changed
	Jse Cust	om Address	Range					
	erved Ad app-addi	dress range esses						
V SI	NOW SN	APSHOT PC	LICY					
SA		CANCEL						
	Save to	create the	volume.					
-						Primary	Standard	SM8 \\nimamb-3830.nimgcveval.com\nimCVSMBw

To mount the SMB volume, do the following:

- 1. In the Cloud Console, go to Cloud Volumes > Volumes.
- 2. Go to the Volumes page
- 3. Click the SMB volume for which you want to map an SMB share.
- 4. Scroll to the right, under Show More, click Mount Instructions.

To perform the mounting process from within the Windows guest OS of the VMware VM, follow the below steps:

- 1. Click the Start button and then click on Computer.
- 2. Click Map Network Drive.
- 3. In the Drive list, click any available drive letter.
- 4. In the folder box, type:

\\nimsmb-3830.nimgcveval.com\nimCVSMBvol01

VVIIdi II	etwork folder would you like to	map?				
Specify th	e drive letter for the connection and the f	older that you want to o	onnect to:			
Drive:	Z: ~					
Folder:	\\10.53.0.4\nimcvsmbvpl01	~	Browse			
	Example: \\server\share	1000				
	Reconnect at sign-in					
	Connect using different credential	s				
	Connect to a Web site that you can u	se to store your docum	ents and pictures			
		ur computor, solo	ct the Reco	nnect at sig	n-in che	eck box.
To conne Click Fin	ect every time you log on to yo ish.	ur computer, sere		J		
Click Fin		ui computer, sele		C		-

foo3 11/1/2021 7:38 AM File folder inimgcvevaltesting.bt 11/1/2021 7:38 AM Text Document 0 KB

11/1/2021 7:38 AM File folder

11/1/2021 7:38 AM File folder

Region Availability for Supplemental NFS datastores on AWS, Azure, and GCP

Learn more about the the Global Region support for supplemental NFS datastores on AWS, Azure and Google Cloud Platform (GCP).

AWS Region Availability

The availability of supplemental NFS datastores on AWS / VMC is defined by Amazon. First, you need to determine if both VMC and FSxN are available in a specified region. Next, you need to determine if the FSxN supplemental NFS datastore is supported in that region.

• Check the availability of VMC here.

foo1 foo2

- Amazon's pricing guide offers information on where FSxN (FSx ONTAP) is available. You can find that information here.
- Availability of the FSxN supplemental NFS datastore for VMC is coming soon.

While information is still being released, the following chart identifies the current support for VMC, FSxN and FSxN as a supplemental NFS datastore.

Americas

AWS Region	VMC Availability	FSx ONTAP Availability	NFS Datastore Availability
US East (Northern Virginia)	Yes	Yes	Yes
US East (Ohio)	Yes	Yes	Yes
US West (Northern California)	Yes	No	No
US West (Oregon)	Yes	Yes	Yes
GovCloud (US West)	Yes	Yes	Yes
Canada (Central)	Yes	Yes	Yes
South America (Sao Paulo)	Yes	Yes	Yes

Last updated on: June 2, 2022.

EMEA

AWS Region	VMC Availability	FSx ONTAP Availability	NFS Datastore Availability
Europe (Ireland)	Yes	Yes	Yes
Europe (London)	Yes	Yes	Yes
Europe (Frankfurt)	Yes	Yes	Yes
Europe (Paris)	Yes	Yes	Yes
Europe (Milan)	Yes	Yes	Yes
Europe (Stockholm)	Yes	Yes	Yes

Last updated on: June 2, 2022.

Asia Pacific

AWS Region	VMC Availability	FSx ONTAP Availability	NFS Datastore Availability
Asia Pacific (Sydney)	Yes	Yes	Yes
Asia Pacific (Tokyo)	Yes	Yes	Yes
Asia Pacific (Osaka)	Yes	No	No
Asia Pacific (Singapore)	Yes	Yes	Yes
Asia Pacific (Seoul)	Yes	Yes	Yes
Asia Pacific (Mumbai)	Yes	Yes	Yes
Asia Pacific (Jakarta)	No	No	No
Asia Pacific (Hong Kong)) Yes	Yes	Yes

Azure Region Availability

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

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

GCP Region Availability

GCP region availability will be released when GCP enters public availability.

Summary and Conclusion: Why NetApp Hybrid Multicloud with VMware

NetApp Cloud Volumes along with VMware solutions for the major hyperscalers provides great potential for organizations looking to leverage hybrid cloud. The rest of this section provides the use cases that show integrating NetApp Cloud Volumes enables true hybrid Multicloud capabilities.

Use case #1: Optimizing storage

When performing a sizing exercise using RVtools output, it is always evident that the horsepower (vCPU/vMem) scale is parallel with storage. Many times, organizations find themselves in a situation where the storage space requires drives the size of the cluster well beyond what is needed for horsepower.

By integrating NetApp Cloud Volumes, organizations can realize a vSphere-based cloud solution with a simple migration approach, with no re-platforming, no IP changes, and no architectural changes. Additionally, this optimization enables you to scale the storage footprint while keeping the host count to least amount required in vSphere, but no change to the storage hierarchy, security, or files made available. This allows you to optimize the deployment and reduce the overall TCO by 35–45%. This integration also enables you to scale storage from warm storage to production-level performance in seconds.

Use case #2: Cloud migration

Organizations are under pressure to migrate applications from on-premises data centers to the Public Cloud for multiple reasons: an upcoming lease expiration; a finance directive to move from capital expenditure (capex) spending to operational expenditures (opex) spending; or simply a top-down mandate to move everything to the cloud.

When speed is critical, only a streamlined migration approach is feasible because re-platforming and refactoring applications to adapt to the cloud's particular IaaS platform is slow and expensive, often taking months. By combining NetApp Cloud Volumes with the bandwidth-efficient SnapMirror replication for guest-connected storage (including RDMs in conjunction with application-consistent Snapshot copies and HCX, cloud specific migration (e.g. Azure Migrate), or third-party products for replicating VMs), this transition is even easier than relying on time-consuming I/O filters mechanisms.

Use case #3: Data center expansion

When a data center reaches capacity limits due to seasonal demand spikes or just steady organic growth,

moving to the cloud-hosted VMware along with NetApp Cloud Volumes is an easy solution. Leveraging NetApp Cloud Volumes allows storage creation, replication, and expansion very easily by providing high availability across availability zones and dynamic scaling capabilities. Leveraging NetApp Cloud Volumes helps in minimizing host cluster capacity by overcoming the need for stretch clusters.

Use case #4: Disaster recovery to the cloud

In a traditional approach, if a disaster occurs, the VMs replicated to the cloud would require conversion to the cloud's own hypervisor platform before they could be restored – not a task to be handled during a crisis.

By using NetApp Cloud Volumes for guest-connected storage using SnapCenter and SnapMirror replication from on-premises along with public cloud virtualization solutions, a better approach for disaster recovery can be devised allowing VM replicas to be recovered on fully consistent VMware SDDC infrastructure along with cloud specific recovery tools (e.g. Azure Site Recovery) or equivalent third-party tools such as Veeam. This approach also enables you to perform disaster recovery drills and recovery from ransomware quickly. This also enables you to scale to full production for testing or during a disaster by adding hosts on-demand.

Use case #5: Application modernization

After applications are in the public cloud, organizations will want to take advantage of the hundreds of powerful cloud services to modernize and extend them. With the use of NetApp Cloud Volumes, modernization is an easy process because the application data is not locked into vSAN and allows data mobility for a wide range of use cases, including Kubernetes.

Conclusion

Whether you are targeting an all-cloud or hybrid cloud, NetApp Cloud Volumes provides excellent options to deploy and manage the application workloads along with file services and block protocols while reducing the TCO by making the data requirements seamless to the application layer.

Whatever the use case, choose your favorite cloud/hyperscaler together with NetApp Cloud Volumes for rapid realization of cloud benefits, consistent infrastructure, and operations across on-premises and multiple clouds, bidirectional portability of workloads, and enterprise-grade capacity and performance.

It is the same familiar process and procedures that are used to connect the storage. Remember, it is just the position of the data that changed with new names; the tools and processes all remain the same and NetApp Cloud Volumes helps in optimizing the overall deployment.

VMware Hybrid Cloud Use Cases

Use Cases for NetApp Hybrid Multicloud with VMware

An overview of the use cases of importance to IT organization when planning hybridcloud or cloud-first deployments.

Popular Use Cases

Use cases include:

- · Disaster recovery,
- Hosting workloads during data center maintenance, * quick burst in which additional resources are required beyond what's provisioned in the local data center,

- VMware site expansion,
- Fast migration to the cloud,
- Dev/test, and
- Modernization of apps leveraging cloud supplemental technologies.

Throughout this documentation, cloud workload references will be detailed using the VMware use-cases. These use-cases are:

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

Inside the IT Journey

Most organizations are on a journey to transformation and modernization. As part of this process, companies are trying use their existing VMware investments while leveraging cloud benefits and exploring ways to make the migration process as seamless as possible. This approach would make their modernization efforts very easy because the data is already in the cloud.

The easiest answer to this scenario is VMware offerings in each hyperscaler. Like NetApp® Cloud Volumes, VMware provides a way to move or extend on-premises VMware environments to any cloud, allowing you to retain existing on-premises assets, skills, and tools while running workloads natively in the cloud. This reduces risk because there will be no service breaks or a need for IP changes and provides the IT team the ability to operate the way they do on-premises using existing skills and tools. This can lead to accelerated cloud migrations and a much smoother transition to a hybrid Multicloud architecture.

Understanding the Importance of Supplemental NFS Storage Options

While VMware in any cloud delivers unique hybrid capabilities to every customer, limited supplemental NFS storage options have restricted its usefulness for organizations with storage-heavy workloads. Because storage is directly tied to hosts, the only way to scale storage is to add more hosts—and that can increase costs by 35–40 percent or more for storage intensive workloads. These workloads just need additional storage, not additional horsepower. But that means paying for additional hosts.

Let's consider this scenario:

A customer requires just five hosts for CPU and memory, but has a lot of storage needs, and needs 12 hosts to meet the storage requirement. This requirement ends up really tipping the financial scale by having to buy the additional horsepower, when they only need to increment the storage.

When you're planning cloud adoption and migrations, it's always important to evaluate the best approach and take the easiest path that reduces total investments. The most common and easiest approach for any application migration is rehosting (also known as lift and shift) where there is no virtual machine (VM) or data conversion. Using NetApp Cloud Volumes with VMware software-defined data center (SDDC), while complementing vSAN, provides an easy lift-and-shift option.

NetApp Solutions for Amazon VMware Managed Cloud (VMC)

Learn more about the solutions that NetApp brings to AWS.

VMware defines the cloud workloads into one of three categories:

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

Browse the available solutions in the following sections.

Protect

- Disaster Recovery with VMC on AWS (guest connected)
- Veeam Backup & Restore in VMC with FSx for ONTAP
- Disaster Recovery (DRO) with FSx for ONTAP and VMC
- Using Veeam Replication and FSx for ONTAP for Disaster recovery to VMware Cloud on AWS

Migrate

• Migrate Workloads to FSxN datastore using VMware HCX

Extend

COMING SOON!!

NetApp Solutions for Azure VMware Solution (AVS)

Learn more about the solutions that NetApp brings to Azure.

VMware defines the cloud workloads into one of three categories:

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

Browse the available solutions in the following sections.

Protect

- Disaster Recovery with ANF and JetStream (supplemental NFS datastore)
- Disaster Recovery with ANF and CVO (guest connected storage)
- Disaster Recovery (DRO) with ANF and AVS
- Using Veeam Replication and Azure NetApp Files datastore for disaster recovery to Azure VMware Solution

Migrate

Migrate Workloads to Azure NetApp Files datastore using VMware HCX

Extend

COMING SOON!!

NetApp Solutions for Google Cloud VMware Engine (GCVE)

Learn more about the solutions that NetApp brings to GCP.

VMware defines the cloud workloads into one of three categories:

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

Browse the available solutions in the following sections.

Protect

- Application Disaster Recovery with SnapCenter, Cloud Volumes ONTAP and Veeam Replication
- Application Consistent Disaster Recovery with NetApp SnapCenter and Veeam Replication to NetApp CVS on GCVE

Migrate

- Workload Migration using VMware HCX to NetApp Cloud Volume Service NFS datastore
- VM Replication using Veeam to NetApp Cloud Volume Service NFS datastore

Extend COMING SOON!!

NetApp for AWS / VMC

NetApp Capabilities for AWS VMC

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

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

- Configuring VMC in AWS
- NetApp Storage Options for VMC
- NetApp / VMware Cloud Solutions

Configuring VMC in AWS

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

This section describes how to set up and manage VMware Cloud on AWS SDDC and use it in combination with the available options for connecting NetApp storage.



In-guest storage is the only supported method of connecting Cloud Volumes ONTAP to AWS VMC.

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

- Deploy and Configure VMware Cloud for AWS
- Connect VMware Cloud to FSx ONTAP

View the detailed configuration steps for VMC.

NetApp Storage Options for VMC

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

Please visit Supported NetApp Storage Options for more information.

AWS supports NetApp storage in the following configurations:

- FSx ONTAP as guest connected storage
- Cloud Volumes ONTAP (CVO) as guest connected storage
- FSx ONTAP as a supplemental NFS datastore

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

Solution Use Cases

With NetApp and VMware cloud solutions, many use cases are simple to deploy in your AWS VMC. Use cases are defined for each of the VMware defined cloud areas:

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

Browse the NetApp solutions for AWS VMC

Protecting Workloads on AWS / VMC

TR-4931: Disaster Recovery with VMware Cloud on Amazon Web Services and Guest Connect

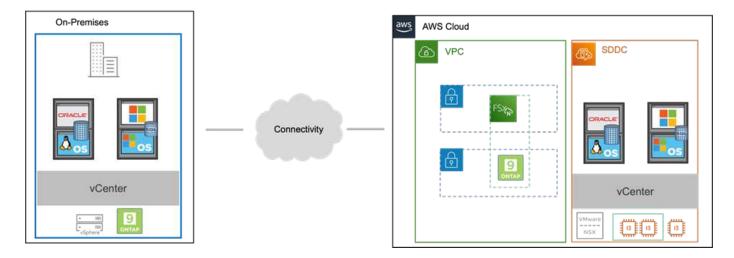
A proven disaster recovery (DR) environment and plan is critical for organizations to ensure that business-critical applications can be rapidly restored in the event of a major outage. This solution focuses on demonstrating DR use cases with a focus on VMware and NetApp technologies, both on-premises and with VMware Cloud on AWS.

Authors: Chris Reno, Josh Powell, and Suresh Thoppay - NetApp Solutions Engineering

Overview

NetApp has a long history of integration with VMware as evidenced by the tens of thousands of customers that have chosen NetApp as their storage partner for their virtualized environment. This integration continues with guest-connected options in the cloud and recent integrations with NFS datastores as well. This solution focuses on the use case commonly referred to as guest-connected storage.

In guest-connected storage, the guest VMDK is deployed on a VMware-provisioned datastore, and application data is housed on iSCSI or NFS and mapped directly to the VM. Oracle and MS SQL applications are used to demonstrate a DR scenario, as shown in the following figure.



Assumptions, pre-requisites and component overview

Before deploying this solution, review the overview of the components, the required pre-requisites to deploy the solution and assumptions made in documenting this solution.

DR Solution Requirements, Pre-requisities and Planning

Performing DR with SnapCenter

In this solution, SnapCenter provides application-consistent snapshots for SQL Server and Oracle application data. This configuration, together with SnapMirror technology, provides high-speed data replication between our on-premises AFF and FSx ONTAP cluster. Additionally, Veeam Backup & Replication provides backup and restore capabilities for our virtual machines.

In this section, we cover the configuration of SnapCenter, SnapMirror, and Veeam for both backup and restore.

The following sections cover configuration and the steps needed to complete a failover at the secondary site:

Configure SnapMirror relationships and retention schedules

SnapCenter can update SnapMirror relationships within the primary storage system (primary > mirror) and to secondary storage systems (primary > vault) for the purpose of long-term archiving and retention. To do so, you must establish and initialize a data replication relationship between a destination volume and a source volume using SnapMirror.

The source and destination ONTAP systems must be in networks that are peered using Amazon VPC peering, a transit gateway, AWS Direct Connect, or an AWS VPN.

The following steps are required for setting up SnapMirror relationships between an on-premises ONTAP

system and FSx ONTAP:



Refer to the FSx for ONTAP – ONTAP User Guide for more information on creating SnapMirror relationships with FSx.

Record the source and destination Intercluster logical interfaces

For the source ONTAP system residing on-premises, you can retrieve the inter-cluster LIF information from System Manager or from the CLI.

1. In ONTAP System Manager, navigate to the Network Overview page and retrieve the IP addresses of Type: Intercluster that are configured to communicate with the AWS VPC where FSx is installed.

Buckets												
Qtrees			-									
Quotes		Network Interfaces	Portsets									
Storage VMs		in south								Q Search 🔮 De	ownload 🕆 Filter 🕒 Show/H	
Tiers		+ Add								A pearon I be	MINDAU . 7 FILME	
NETWORK A		Name	Status	Storage VM	IPspace	Address ©	Current Node	Current Port	Portset	Protocols	Туре	73
Overview		veeam_repo	0	Backup	Default	10.61.181.179	E13A300_1	a0a-161		SMB/CIFS, NFS, S3	Data	
Ethernet Ports		CM01	0		Default	10.61.181.180	E13A300_1	101-101			Cluster/Node Mgmt	
FC Ports			50									1
EVENTS & JOBS		HC_NI	0		Default	10.61.181.183	E13A300_1	a0a-181			Intercluster,Cluster/Node Mgmt	
PROTECTION ~		HC_N2	0		Default	10.61.181.184	E13A300_2	1000-181			Intercluster, Cluster/Node Mgmt	1
Proficences >		lif_ora_svm_614	0	1	Default	10.61.181.185	E13A300_1	a0a-181		SMB/CIFS, NFS, FL	Data	÷.,
HOSTS V	2	es_ors_svol_614	0	ora_tvm	Detailut	10.01.181.192	E10/300_1	ava-181		awayura, NPS, PL.	Lorus .	

2. To retrieve the Intercluster IP addresses for FSx, log into the CLI and run the following command:

FSx-Dest::> network interface show -role intercluster

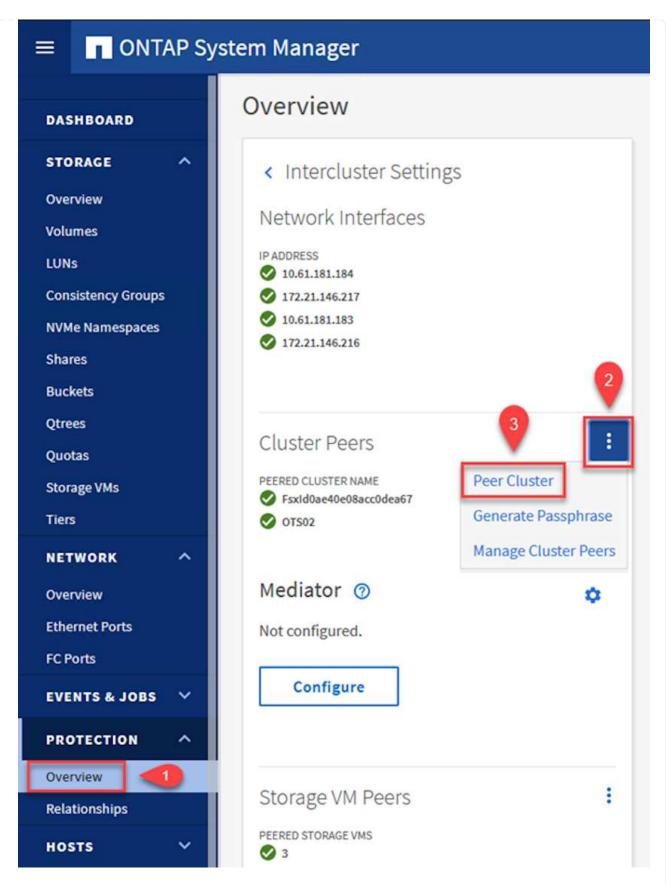
```
FsxId0ae40e08acc0dea67::> network interface show -role intercluster
                       Status
                                  Network
            Logical
                                                      Current
                                                                     Current Is
            Interface Admin/Oper Address/Mask
                                                      Node
/server
                                                                     Port
                                                                             Home
FsxId0ae40e08acc0dea67
                                  172.30.15.42/25
                                                      FsxId0ae40e08acc0dea67-01
            inter 1
                         up/up
                                                                     e0e
                                                                             true
            inter 2
                         up/up
                                  172.30.14.28/26
                                                      FsxId0ae40e08acc0dea67-02
                                                                     e0e
                                                                             true
 entries were displayed.
```

To establish cluster peering between ONTAP clusters, a unique passphrase entered at the initiating ONTAP cluster must be confirmed in the other peer cluster.

1. Set up peering on the destination FSx cluster using the cluster peer create command. When prompted, enter a unique passphrase that is used later on the source cluster to finalize the creation process.

```
FSx-Dest::> cluster peer create -address-family ipv4 -peer-addrs
source_intercluster_1, source_intercluster_2
Enter the passphrase:
Confirm the passphrase:
```

2. At the source cluster, you can establish the cluster peer relationship using either ONTAP System Manager or the CLI. From ONTAP System Manager, navigate to Protection > Overview and select Peer Cluster.



- 3. In the Peer Cluster dialog box, fill out the required information:
 - a. Enter the passphrase that was used to establish the peer cluster relationship on the destination FSx cluster.

- b. Select Yes to establish an encrypted relationship.
- c. Enter the intercluster LIF IP address(es) of the destination FSx cluster.
- d. Click Initiate Cluster Peering to finalize the process.

Peer Cluster

	PASSPHRASE 🕜	
STORAGE VM PERMISSIONS	 PASSPHRASE	
All storage VMs (incl ×	******	6
Storage VMs created in the future also will be permissions.	 It cannot be determined from the p this relationship was encrypted. Is encrypted? 2 Yes No	
	To generate passphrase, Laun	ich Remote Cluster
	Intercluster Network Interfaces	IP Addresses
	172.30.15.42	
	3 172.30.14.28	
		Cancel
4	+ Add	

4. Verify the status of the cluster peer relationship from the FSx cluster with the following command:

FSx-Dest::> cluster p	eer show		
FsxId0ae40e08acc0dea67::> Peer Cluster Name	cluster peer show Cluster Serial Number	Availability	Authentication
E13A300	1-80-000011	Available	ok

129

×

Establish SVM peering relationship

The next step is to set up an SVM relationship between the destination and source storage virtual machines that contain the volumes that will be in SnapMirror relationships.

1. From the source FSx cluster, use the following command from the CLI to create the SVM peer relationship:

```
FSx-Dest::> vserver peer create -vserver DestSVM -peer-vserver
Backup -peer-cluster OnPremSourceSVM -applications snapmirror
```

- 2. From the source ONTAP cluster, accept the peering relationship with either ONTAP System Manager or the CLI.
- 3. From ONTAP System Manager, go to Protection > Overview and select Peer Storage VMs under Storage VM Peers.



- 4. In the Peer Storage VM's dialog box, fill out the required fields:
 - The source storage VM
 - The destination cluster
 - The destination storage VM



5. Click Peer Storage VMs to complete the SVM peering process.

SnapCenter manages retention schedules for backups that exist as snapshot copies on the primary storage system. This is established when creating a policy in SnapCenter. SnapCenter does not manage retention policies for backups that are retained on secondary storage systems. These policies are managed separately through a SnapMirror policy created on the secondary FSx cluster and associated with the destination volumes that are in a SnapMirror relationship with the source volume.

When creating a SnapCenter policy, you have the option to specify a secondary policy label that is added to the SnapMirror label of each snapshot generated when a SnapCenter backup is taken.



On the secondary storage, these labels are matched to policy rules associated with the destination volume for the purpose of enforcing retention of snapshots.

The following example shows a SnapMirror label that is present on all snapshots generated as part of a policy used for daily backups of our SQL Server database and log volumes.

Select secondary replication options ()

Update SnapMirror after creating a local Snapshot copy.

✓ Update SnapVault after creating a local Snapshot copy.

Secondary policy label	Custom Label -	0
	sql-daily	
Error retry count	3 🗘 🚯	

For more information on creating SnapCenter policies for a SQL Server database, see the SnapCenter documentation.

You must first create a SnapMirror policy with rules that dictate the number of snapshot copies to retain.

1. Create the SnapMirror Policy on the FSx cluster.

FSx-Dest::> snapmirror policy create -vserver DestSVM -policy
PolicyName -type mirror-vault -restart always

2. Add rules to the policy with SnapMirror labels that match the secondary policy labels specified in the SnapCenter policies.

```
FSx-Dest::> snapmirror policy add-rule -vserver DestSVM -policy
PolicyName -snapmirror-label SnapMirrorLabelName -keep
#ofSnapshotsToRetain
```

The following script provides an example of a rule that could be added to a policy:

```
FSx-Dest::> snapmirror policy add-rule -vserver sql_svm_dest -policy
Async SnapCenter SQL -snapmirror-label sql-ondemand -keep 15
```



Create additional rules for each SnapMirror label and the number of snapshots to be retained (retention period).

Create destination volumes

To create a destination volume on FSx that will be the recipient of snapshot copies from our source volumes, run the following command on FSx ONTAP:

```
FSx-Dest::> volume create -vserver DestSVM -volume DestVolName
-aggregate DestAggrName -size VolSize -type DP
```

Create the SnapMirror relationships between source and destination volumes

To create a SnapMirror relationship between a source and destination volume, run the following command on FSx ONTAP:

```
FSx-Dest::> snapmirror create -source-path
OnPremSourceSVM:OnPremSourceVol -destination-path DestSVM:DestVol -type
XDP -policy PolicyName
```

Initialize the SnapMirror relationships

Initialize the SnapMirror relationship. This process initiates a new snapshot generated from the source volume and copies it to the destination volume.

FSx-Dest::> snapmirror initialize -destination-path DestSVM:DestVol

Deploy and configure Windows SnapCenter server on-premises.

Deploy Windows SnapCenter Server on premises

This solution uses NetApp SnapCenter to take application-consistent backups of SQL Server and Oracle databases. In conjunction with Veeam Backup & Replication for backing up virtual machine VMDKs, this provides a comprehensive disaster recovery solution for on-premises and cloud-based datacenters.

SnapCenter software is available from the NetApp support site and can be installed on Microsoft Windows systems that reside either in a domain or workgroup. A detailed planning guide and installation instructions can be found at the NetApp Documentation Center.

The SnapCenter software can be obtained at this link.

After it is installed, you can access the SnapCenter console from a web browser using *https://Virtual_Cluster_IP_or_FQDN:8146*.

After you log into the console, you must configure SnapCenter for backup SQL Server and Oracle databases.

To add storage controllers to SnapCenter, complete the following steps:

1. From the left menu, select Storage Systems and then click New to begin the process of adding your storage controllers to SnapCenter.

	letApp SnapCo	enter®	D			≅ 0 -	👤 scadmin 🛛 SnapC	CenterAdmin 🛛 🖡 Sign C
<		ONTAI	P Storage					
	Dashboard	Туре	ONTAP SVMs	• Search	n by Name			+ II New Date
0	Resources	ONTA	AP Storage Connectio	ns				
•	Monitor		Name 41	IP	Cluster Name	User Nan	ne Platform	Controller Licens
a 1	Reports		Backup	172.16.13.17	172.16.13.17		AFF	~
			<u>FS02</u>	172.16.13.17	172.16.13.17		AFF	~
*	Hosts		ora_svm	172.16.13.17	172.16.13.17		AFF	
1	Storage Systems		ora svm dest		172.30.15.42		AFF	Not applicable
=	Settings		<u>sql_svm</u>	172.16.13.17	172.16.13.17		AFF	~
	and the second s		sal sym_dest		172.30.15.42		AFF	Not applicable
▲	Alerts		svm HCApps		172.30.15.42		AFF	Not applicable

2. In the Add Storage System dialog box, add the management IP address for the local on-premises ONTAP cluster and the username and password. Then click Submit to begin discovery of the storage system.

Add Storage System	
Add Storage System	•
Storage System	10.61.181.180
Username	admin
Password	•••••
 Send AutoSuppor Log SnapCenter S 	System (EMS) & AutoSupport Settings It notification to storage system
Submit Cancel	atform, Protocol, Preferred IP etc
at the bottom of the Add Storag	FSx ONTAP system to SnapCenter. In this case, select More Options ge System window and click the check box for Secondary to designate ary storage system updated with SnapMirror copies or our primary

Platform	FAS	•	Secondary	9
Protocol	HTTPS			
Port	443			
Timeout	60	seconds	0	
Preferred IP	1			0

Add hosts to SnapCenter

The next step is adding host application servers to SnapCenter. The process is similar for both SQL Server and Oracle.

- 1. From the left menu, select Hosts and then click Add to begin the process of adding storage controllers to SnapCenter.
- 2. In the Add Hosts window, add the Host Type, Hostname, and the host system Credentials. Select the plug-in type. For SQL Server, select the Microsoft Windows and Microsoft SQL Server plug-in.

	etApp	• SnapCenter®					
>	Man	aged Hosts					
===	Se	arch by Name		Add Host			
I		Name	11	Host Type	Windows	•	
•		oraclesry_01.sddc.netapp.com		Host Name	sqlsrv-01.sddc.netapp.com		
		oraclesry_02.sddc.netapp.com		Credentials	sddc-jpowell	•	+
ណ៍		oraclesry_03.sddc.netapp.com			t		
A.		oraclesry 04.sddc.netapp.com		Select Plug-ins to In	stall SnapCenter Plug-ins Package 4.6 for Window	VS	
20		oraclesry_05.sddc.netapp.com			Microsoft Windows		
Anima di		oraclesry 06.sddc.netapp.com			Microsoft SQL Server		
**		oraclesry_07.sddc.netapp.com			Microsoft Exchange Server SAP HANA		
▲		oraclesry_08.sddc.netapp.com		More Options : P	ort, gMSA, Install Path, Custom Plug-Ins		
		oraclesry_09.sddc.netapp.com					
		oraclesry 10.sddc.netapp.com		Submit Cancel]		

3. For Oracle, fill out the required fields in the Add Host dialog box and select the check box for the Oracle Database plug-in. Then click Submit to begin the discovery process and to add the host to SnapCenter.

Host Type	Linux	•		
Host Name	oraclesrv_11.sddc.netapp.com			
			1	
Credentials Select Plug-ins to In:	root stall SnapCenter Plug-ins Package 4.6 for Linux Oracle Database	•	+	(
	• Tall SnapCenter Plug-ins Package 4.6 for Linux	•	+	•
Select Plug-ins to In:	stall SnapCenter Plug-ins Package 4.6 for Linux	•	+	

Policies establish the specific rules to be followed for a backup job. They include, but are not limited to, the backup schedule, replication type, and how SnapCenter handles backing up and truncating transaction logs.

You can access policies in the Settings section of the SnapCenter web client.

<			Policies	Users and Access	Roles	Credential	Software	
D	Dashboard	Microsoft SQL Server						
R	lesources	Search by Name	New Modify					
	Aonitor	Name	1E	Backup Type	Sche	dule Type	Re	plication
		SQL-Daily		Full and Log backup	Daily		Sna	apVault
M R	leports	SQL-Hourly		Full and Log backup	Hour	ly	Sna	apVault
H	losts	SQL-Hourly-Logs		Log backup	Hour	ly	Sna	apVault
- s	torage Systems	SQL-OnDemand		Full and Log backup	On d	emand	Sna	apVault
	ettings	SQL-Weekly		Full and Log backup	Week	dy	Sna	apVault
- s								

For complete information on creating policies for SQL Server backups, see the SnapCenter documentation.

For complete information on creating policies for Oracle backups, see the SnapCenter documentation.

Notes:

- As you progress through the policy creation wizard, take special note of the Replication section. In this section you stipulate the types of secondary SnapMirror copies that you want taken during the backups process.
- The "Update SnapMirror after creating a local Snapshot copy" setting refers to updating a SnapMirror relationship when that relationship exists between two storage virtual machines residing on the same cluster.
- The "Update SnapVault after creating a local SnapShot copy" setting is used to update a SnapMirror relationship that exists between two separate cluster and between an on-premises ONTAP system and Cloud Volumes ONTAP or FSxN.

The following image shows the preceding options and how they look in the backup policy wizard.

New SQL Serve	r Backup Policy						
1 Name	Select secondary replication options 🚯						
2 Backup Type	Update SnapMirror after creating a local Snapshot copy.						
3 Retention	Update SnapVault after creating a local Snapshot copy.						
4 Replication	Secondary policy label	Choose		÷.	0		
Alpheaton	Error retry count	з С	0				
5 Script							

Create SnapCenter Resource Groups

Resource Groups allow you to select the database resources you want to include in your backups and the policies followed for those resources.

- 1. Go to the Resources section in the left-hand menu.
- 2. At the top of the window, select the resource type to work with (In this case Microsoft SQL Server) and then click New Resource Group.

	letApp SnapC	enter®)		۰ 🖬 😔		lmin SnapCenterA	lmin 🛛 🗊 Sign Out	
<		Microsoft SQL Server -							
	Dashboard	View	Resource Group	•	search by name		2 H		
0	Resources	19	Name	Resource Count	Tags	Policies	Last Backup	Overall Status	
đ	Monitor		SQLSRV-01	1		SQL-Daily SQL-Hourly	05/11/2022	Completed	
M	Reports				OnDen	SQL- OnDemand SQL-Weekly			
h	Hosts								
1	Storage Systems		SQLSRV-02	1		SQL-Daily SQL-Hourly SQL-	03/28/2022	Failed	
=	Settings				OnDerr	OnDemand SQL-Weekly			
	Alerts		SQLSRV-03	1		SQL-Daily	05/11/2022	Completed	

The SnapCenter documentation covers step-by-step details for creating Resource Groups for both SQL Server and Oracle databases.

For backing up SQL resources, follow this link.

For Backing up Oracle resources, follow this link.

Deploy and configure Veeam Backup Server

Veeam Backup & Replication software is used in the solution to back up our application virtual machines and archive a copy of the backups to an Amazon S3 bucket using a Veeam scale-out backup repository (SOBR). Veeam is deployed on a Windows server in this solution. For specific guidance on deploying Veeam, see the Veeam help Center Technical documentation.

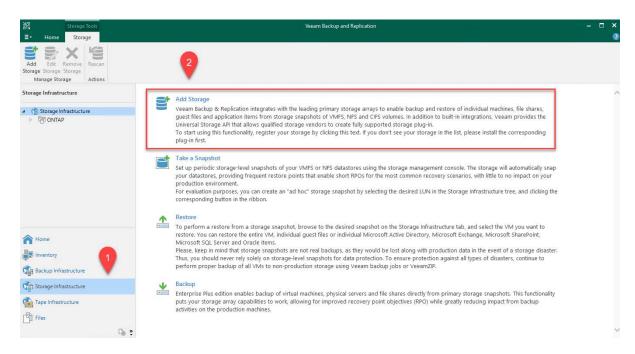
After you deploy and license the software, you can create a scale-out backup repository (SOBR) as target storage for backup jobs. You should also include an S3 bucket as a backup of VM data offsite for disaster recovery.

See the following prerequisites before getting started.

- 1. Create an SMB file share on your on-premises ONTAP system as the target storage for backups.
- 2. Create an Amazon S3 bucket to include in the SOBR. This is a repository for the offsite backups.

First, add the ONTAP storage cluster and associated SMB/NFS filesystem as storage infrastructure in Veeam.

1. Open the Veeam console and log in. Navigate to Storage Infrastructure and then select Add Storage.



- 2. In the Add Storage wizard, select NetApp as the storage vendor and then select Data ONTAP.
- 3. Enter the management IP address and check the NAS Filer box. Click Next.

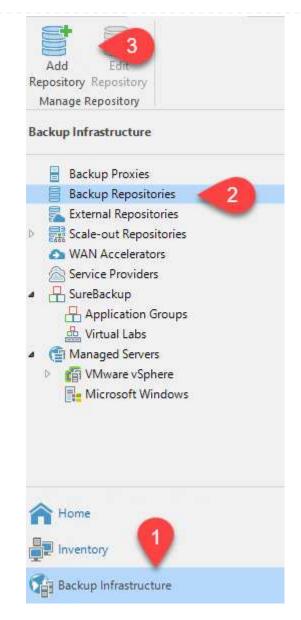
Name	Management server DNS name or IP address:
	10.61.181.180
Credentials	Description:
NAS Filer	Created by SDDC\jpowell at 5/17/2022 10:34 AM.
Apply	
Summary	Role:
	 Block or file storage for VMware vSphere Block storage for Microsoft Windows servers NAS filer
dd your credent	< Previous Next > Finish Cancer tials to access the ONTAP cluster.
New NetApp Data ONT/	tials to access the ONTAP cluster.
New NetApp Data ONT/ Credentials Specify acco	tials to access the ONTAP cluster.
New NetApp Data ONT/ Credentials Specify acco Name	tials to access the ONTAP cluster. AP Storage punt with storage administrator privileges.
New NetApp Data ONT/ Credentials Specify acco Name Credentials	tials to access the ONTAP cluster. AP Storage bount with storage administrator privileges. Credentials: McIEUC\Admin (HCIEUC\Admin, last edited: 98 days ago) Addorg Manage accounts
New NetApp Data ONT/ Credentials Specify acco Name	tials to access the ONTAP cluster.
New NetApp Data ONT/ Credentials Specify acco Name Credentials NAS Filer	tials to access the ONTAP cluster. AP Storage bount with storage administrator privileges. Credentials: McIEUC\Admin (HCIEUC\Admin, last edited: 98 days ago) Addorg Manage accounts
New NetApp Data ONT/ Credentials Specify acco Name Credentials NAS Filer Apply	tials to access the ONTAP cluster.
New NetApp Data ONT/ Credentials Specify acco Name Credentials NAS Filer Apply	tials to access the ONTAP cluster.
New NetApp Data ONT/ Credentials Specify acco Name Credentials NAS Filer Apply	tials to access the ONTAP cluster.
New NetApp Data ONTA Credentials Specify acco Name Credentials	tials to access the ONTAP cluster.
New NetApp Data ONTA Credentials Specify acco Name Credentials NAS Filer Apply	tials to access the ONTAP cluster.
New NetApp Data ONT/ Credentials Specify acco Name Credentials NAS Filer Apply	tials to access the ONTAP cluster.
New NetApp Data ONT/ Credentials Specify acco Name Credentials NAS Filer Apply	tials to access the ONTAP cluster.

New NetApp Data ONTAP Storag	e	×
NAS Filer Specify how this store	age can be accessed by file backup jobs.	
Name	Protocol to use:	
Credentials	□ NFS	
NAS Filer	Create required export rules automatically Volumes to scan:	
Apply	All volumes	Choose
Summary	Backup proxies to use:	
	Automatic selection	Choose
	< Previous Apply Finish	Cancel

6. Complete the Apply and Summary pages of the wizard and click Finish to begin the storage discovery process. After the scan completes, the ONTAP cluster is added along with the NAS filers as available resources.

Add Edit Remove Storage Storage Storage	Rescan
Manage Storage	Actions
Storage Infrastructure	
 ▲ G Storage Infrastructu ▲ □ ONTAP 	ire
器 E13A300	
▲ 器 OTS-HC-Clus	ter
Image: Svm_nfs-A	
⊿ 😐 svm0	
iscsi_D	atastore
▷ 🧧 sqdb_v	ol2
▷ 🥛 sqldb_v	vol1
▷ 🦰 svm0_n	oot

7. Create a backup repository using the newly discovered NAS shares. From Backup Infrastructure, select Backup Repositories and click the Add Repository menu item.



8. Follow all steps in the New Backup Repository Wizard to create the repository. For detailed information on creating Veeam Backup Repositories, see the Veeam documentation.

New Backup Repository

Share

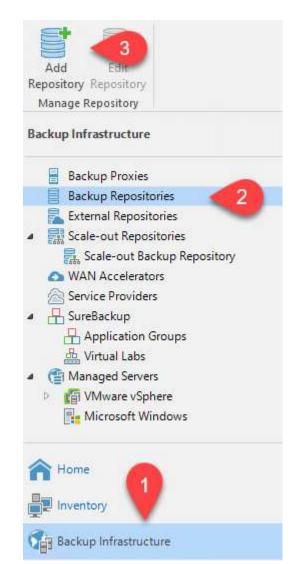
Type in UNC path to share (mapped drives are not supported), specify share access credentials and how backup jobs should write data to this share.

 \times

Name Share	Shared folder: \\172.21.162.181\VBRRepo Browse Use \\server\folder format
Repository Mount Server	This share requires access credentials: Sddc\administrator (sddc\administrator, last edited: 85 days ago) Manage accounts
Review Apply	Gateway server: Automatic selection The following server:
Summary	veeam.sddc.netapp.com (Backup server) Use this option to improve performance and reliability of backup to a NAS located in a remote site.
	< Previous Next > Finish Cancel

The next step is to add the Amazon S3 storage as a backup repository.

1. Navigate to Backup Infrastructure > Backup Repositories. Click Add Repository.



2. In the Add Backup Repository wizard, select Object Storage and then Amazon S3. This starts the New Object Storage Repository wizard.

Add Backup Repository

Select the type of backup repository you want to add.

=
3

Direct attached storage

Microsoft Windows or Linux server with internal or direct attached storage. This configuration enables data movers to run directly on the server, allowing for fastest performance.



Network attached storage

Network share on a file server or a NAS device. When backing up to a remote share, we recommend that you select a gateway server located in the same site with the share.



₿

Deduplicating storage appliance

Dell EMC Data Domain, ExaGrid, HPE StoreOnce or Quantum DXi. If you are unable to meet the requirements of advanced integration via native appliance API, use the network attached storage option instead.



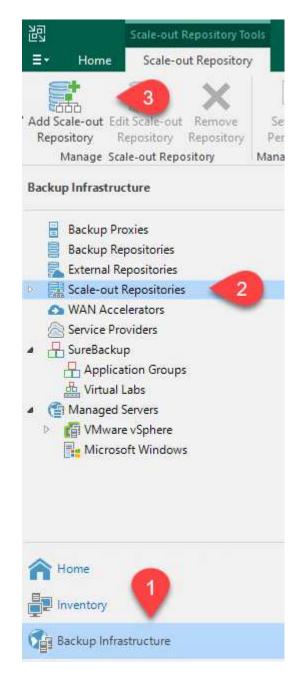
On-prem object storage system or a cloud object storage provider. Object storage can only be used as a Capacity Tier of scale-out backup repositories, backing up directly to object storage is not currently supported.

- 3. Provide a name for your object storage repository and click Next.
- 4. In the next section, provide your credentials. You need an AWS Access Key and Secret Key.

Name	Credentials:	
Account	💦 AKIAX4H43ZT557HXQT2W (last edited: 107 days ago) 🗸 🗸	Add
Bucket	AWS region:	
Summary	Global	
	Use the following gateway server:	
	Use the following gateway server: veeam.sddc.netapp.com (Backup server) Select a gateway server to proxy access to Amazon S3. If no gateway server is specified, all backup repository extents must have direct Internet access.	Il scale-(

Now that we have added our storage repositories to Veeam, we can create the SOBR to automatically tier backup copies to our offsite Amazon S3 object storage for disaster recovery.

1. From Backup Infrastructure, select Scale-out Repositories and then click the Add Scale-out Repository menu item.



- 2. In the New Scale-out Backup Repository provide a name for the SOBR and click Next.
- 3. For the Performance Tier, choose the backup repository that contains the SMB share residing on your local ONTAP cluster.

Performance Tier		
\square	ies to use as the landing zone and for the short-term retention.	
Name	Extents:	
Performance Tier	Name	Add
Placement Policy		Remove

- 4. For the Placement Policy, choose either Data Locality or Performance based your requirements. Select next.
- 5. For Capacity Tier we extend the SOBR with Amazon S3 object storage. For the purposes of disaster recovery, select Copy Backups to Object Storage as Soon as They are Created to ensure timely delivery of our secondary backups.

New Scale-out Backup Repositor	y	×	
	e to copy backups to for redundancy and DR purposes. Older backups can be moved to object storage long-term retention costs while preserving the ability to restore directly from offloaded backups.		
Name	Extend scale-out backup repository capacity with object storage:		
Performance Tier	Amazon S3 Repo V Add		
Placement Policy	Define time windows when uploading to capacity tier is allowed Window		
Capacity Tier	Copy backups to object storage as soon as they are created		
Archive Tier	Create additional copy of your backups for added redundancy by having all backups copied to the capacity tier as soon as they are created on the performance tier.		
Summary	Move backups to object storage as they age out of the operational restore window Reduce your long-term retention costs by moving older backups to object storage completely while preserving the ability to restore directly from offloaded backups.		
	Move backup files older than 14 🛓 days (your operational restore window) Override		
	Encrypt data uploaded to object storage Password:		
	< Previous Next > Finish Cancel		
6. Finally, select Apply and	d Finish to finalize creation of the SOBR.		

Create the scale-out backup repository jobs

The final step to configuring Veeam is to create backup jobs using the newly created SOBR as the backup destination. Creating backup jobs is a normal part of any storage administrator's repertoire and we do not cover the detailed steps here. For more complete information on creating backup jobs in Veeam, see the Veeam Help Center Technical Documentation.

BlueXP backup and recovery tools and configuration

To conduct a failover of application VMs and database volumes to VMware Cloud Volume services running in AWS, you must install and configure a running instance of both SnapCenter Server and Veeam Backup and Replication Server. After the failover is complete, you must also configure these tools to resume normal backup operations until a failback to the on-premises datacenter is planned and executed.

Deploy secondary Windows SnapCenter Server

SnapCenter Server is deployed in the VMware Cloud SDDC or installed on an EC2 instance residing in a VPC with network connectivity to the VMware Cloud environment.

SnapCenter software is available from the NetApp support site and can be installed on Microsoft Windows systems that reside either in a domain or workgroup. A detailed planning guide and installation instructions can be found at the NetApp documentation center.

You can find the SnapCenter software at this link.

Configure secondary Windows SnapCenter Server

To perform a restore of application data mirrored to FSx ONTAP, you must first perform a full restore of the on-premises SnapCenter database. After this process is complete, communication with the VMs is reestablished and application backups can now resume using FSx ONTAP as the primary storage.

To achieve this, you must complete the following items on the SnapCenter Server:

- 1. Configure the computer name to be identical to the original on-premises SnapCenter Server.
- 2. Configure networking to communicate with VMware Cloud and the FSx ONTAP instance.
- 3. Complete the procedure to restore the SnapCenter database.
- 4. Confirm that SnapCenter is in Disaster Recovery mode to make sure that FSx is now the primary storage for backups.
- 5. Confirm that communication is reestablished with the restored virtual machines.

Deploy secondary Veeam Backup & Replication server

You can install the Veeam Backup & Replication server on a Windows server in the VMware Cloud on AWS or on an EC2 instance. For detailed implementation guidance, see the Veeam Help Center Technical Documentation.

To perform a restore of virtual machines that have been backed up to Amazon S3 storage, you must install the Veeam Server on a Windows server and configure it to communicate with VMware Cloud, FSx ONTAP, and the S3 bucket that contains the original backup repository. It must also have a new backup repository configured on FSx ONTAP to conduct new backups of the VMs after they are restored.

To perform this process, the following items must be completed:

- 1. Configure networking to communicate with VMware Cloud, FSx ONTAP, and the S3 bucket containing the original backup repository.
- 2. Configure an SMB share on FSx ONTAP to be a new backup repository.
- 3. Mount the original S3 bucket that was used as part of the scale-out backup repository on premises.
- 4. After restoring the VM, establish new backup jobs to protect SQL and Oracle VMs.

For more information on restoring VMs using Veeam, see the section "Restore Application VMs with Veeam Full Restore".

SnapCenter database backup for disaster recovery

SnapCenter allows for the backup and recovery of its underlying MySQL database and configuration data for the purpose of recovering the SnapCenter server in the case of a disaster. For our solution, we recovered the SnapCenter database and configuration on an AWS EC2 instance residing in our VPC. For more information on this step, see this link.

SnapCenter backup prerequisites

The following prerequisites are required for SnapCenter backup:

- A volume and SMB share created on the on-premises ONTAP system to locate the backed-up database and configuration files.
- A SnapMirror relationship between the on-premises ONTAP system and FSx or CVO in the AWS account. This relationship is used for transporting the snapshot containing the backed-up SnapCenter database and configuration files.
- Windows Server installed in the cloud account, either on an EC2 instance or on a VM in the VMware Cloud SDDC.
- SnapCenter installed on the Windows EC2 instance or VM in VMware Cloud.

- Create a volume on the on-premises ONTAP system for hosting the backup db and config files.
- Set up a SnapMirror relationship between on-premises and FSx/CVO.
- Mount the SMB share.
- Retrieve the Swagger authorization token for performing API tasks.
- Start the db restore process.
- Use the xcopy utility to copy the db and config file local directory to the SMB share.
- On FSx, create a clone of the ONTAP volume (copied via SnapMirror from on-premises).
- Mount the SMB share from FSx to EC2/VMware Cloud.
- Copy the restore directory from the SMB share to a local directory.
- Run the SQL Server restore process from Swagger.

SnapCenter provides a web client interface for executing REST API commands. For information on accessing the REST APIs through Swagger, see the SnapCenter documentation at this link.

After you have navigated to the Swagger page, you must retrieve an authorization token to initiate the database restore process.

1. Access the SnapCenter Swagger API web page at *https://<SnapCenter Server IP>:8146/swagger/*.

SnapCenter A	PI [—]	
[Base URL: /api]		
https://snapcenter.sddc.netapp.com:814	6/Content/swagger/SnapCenter,yaml	
	sing the SnapCenter API. tion of "SnapCenter Plug-in for VMware vSphere" API's, please use t port}/api/swagger-ui.html	
Expand the Auth section a		,
expand the Auth section a	and click Try it Out.	
Auth	and click Try it Out. gin Service login ethod required to log in to the SnapCenter service. The login method re	eturns a token that is used to

3. In the UserOperationContext area, fill in the SnapCenter credentials and role and click Execute.

TokenNeverExpires	Token never expires	
boolean (query)		
(duery)	false ~	
UserOperationContext * re object	uired User credentials	
(body)	Edit Value Model	
	<pre>{ "UserOperationContext": { "User": { "Name": "localhost\\scadmin", "Passphrase": "NetApp321", "Rolename": "SnapCenterAdmin" } } }</pre>	
	Cancel	h.
	Parameter content type application/json	

4. In the Response body below, you can see the token. Copy the token text for authentication when executing the backup process.

200	Response body
	"PluginName": null,
	"HostId": 0,
	"RoleId": null,
	"JobIds": null
	ь
	"User": {
	"Token":
	"KlYxDg==tsV6EOdtdAmAYpe8q5SG6wcoGaSjwM26jrNy5CsY63HRD5LkoZLIESRNAhpGJJ0UUQynENdgtVGDZnvx+I/ZJZIn5M1NZrj6
	CLfGTApg1GscagT08bgb5bMTx07EcdrAidzAX00b3GyLGKtW0GdwKzSeOwKj3uVupnk1E31skK6PRBv9RS8j0qHQvo4v4RL0hhThhwFhV
	9/23nFeJVP/p1Ev4vrV/zeZVTUHFHUM069XRe5cuW9nwyj4b015Y5FN3XDkjQ
	"Name": "SCAdmin",
	"TokenHashed": null,
	"Туре": "",
	"TokenTime": "2022-03-22T14:21:57.3665661-07:00",
	"Id": "1",
	"FullName": "SCAdmin",
	"Host": null,
	"Author": null,
	"UserName": "",
	"Domain": "", Downie
	"Passphrase": "",

Next go to the Disaster Recovery area on the Swagger page to begin the SnapCenter backup process.

1. Expand the Disaster Recovery area by clicking it.

Disaster Recovery GET /4.6/disasterrecovery/server/backup Fetch all the existing SnapCenter Server DR Backups. POST /4.6/disasterrecovery/server/backup Starts the SnapCenter Server DR backup. DELETE /4.6/disasterrecovery/server/backup Deletes the existing Snapcenter DR backup. POST /4.6/disasterrecovery/server/backup Deletes the existing Snapcenter DR backup. POST /4.6/disasterrecovery/server/restore Starts SnapCenter Server Restore. POST /4.6/disasterrecovery/storage Enable or disable the storage disaster recovery.

2. Expand the /4.6/disasterrecovery/server/backup section and click Try it Out.

POST	/4.6/disasterrecovery/server/backup Starts the SnapCenter Server DR backup.
Starts and crea	ates a new SnapCenter Server DR backup.
Parameters	Try it out

3. In the SmDRBackupRequest section, add the correct local target path and select Execute to start the backup of the SnapCenter database and configuration.



The backup process does not allow backing up directly to an NFS or CIFS file share.

Name	Description
Token * required string	User authorization token
(header)	TUHFHUM069XRe5cuW9nwyj4b0I5Y5FN3XDkjQ==
SmDRBackupRequest * required object	Parameters to take Backup
(body)	Edit Value Model
	<pre>{ "TargetPath": "C:\\SnapCenter_Backups\\" }</pre>
	Cancel Parameter content type application/json
	Execute

Monitor the backup job from SnapCenter

Log into SnapCenter to review log files when starting the database restore process. Under the Monitor section, you can view the details of the SnapCenter server disaster recovery backup.

4	SnapCenter Server disaster recovery backup	^
~	Precheck validation	
~	Disaster recovery backup of 'oraclesrv_04.sddc.netapp.com'	
~	Disaster recovery backup of SnapCenter Server 'SnapCenter.sddc.netapp.com'	
~	Disaster recovery backup of 'oraclesrv_02.sddc.netapp.com'	
~	Disaster recovery backup of 'oraclesrv_03.sddc.netapp.com'	
~	Disaster recovery backup of 'oraclesrv_05.sddc.netapp.com'	
~	Disaster recovery backup of 'oraclesrv_07.sddc.netapp.com'	
4	Disaster recovery backup of 'sqlsrv-02.sddc.netapp.com'	
~	Disaster recovery backup of 'sqlsrv-03.sddc.netapp.com'	
~	Disaster recovery backup of 'oraclesrv_10.sddc.netapp.com'	
4	Disaster recovery backup of 'sqlsrv-04.sddc.netapp.com'	
~	Disaster recovery backup of 'sqlsrv-01.sddc.netapp.com'	
~	Disaster recovery backup of 'sqlsrv-05.sddc.netapp.com'	
4	Disaster recovery backup of 'oraclesrv_09.sddc.netapp.com'	
4	Disaster recovery backup of 'sqlsrv-06.sddc.netapp.com'	
~	Disaster recovery backup of 'sqlsrv-07.sddc.netapp.com'	~
) Tas	k Name: SnapCenter Server disaster recovery backup Start Time: 03/23/2022 10:27:11 AM End Time: 03/23/2 7 AM	2022

Next you must move the backup from the local drive on the SnapCenter server to the CIFS share that is used to SnapMirror copy the data to the secondary location located on the FSx instance in AWS. Use xcopy with specific options that retain the permissions of the files.

Open a command prompt as Administrator. From the command prompt, enter the following commands:

```
xcopy <Source_Path> \\<Destination_Server_IP>\<Folder_Path> /O /X
/E /H /K
xcopy c:\SC_Backups\SnapCenter_DR \\10.61.181.185\snapcenter_dr /O
/X /E /H /K
```

Failover

Disaster occurs at primary site

For a disaster that occurs at the primary on-premises datacenter, our scenario includes failover to a secondary site residing on Amazon Web Services infrastructure using VMware Cloud on AWS. We assume that the virtual machines and our on-premises ONTAP cluster are no longer accessible. In addition, both the SnapCenter and Veeam virtual machines are no longer accessible and must be rebuilt at our secondary site.

This section address failover of our infrastructure to the cloud, and we cover the following topics:

- SnapCenter database restore. After a new SnapCenter server has been established, restore the MySQL database and configuration files and toggle the database into disaster recovery mode in order to allow the secondary FSx storage to become the primary storage device.
- Restore the application virtual machines using Veeam Backup & Replication. Connect the S3 storage that contains the VM backups, import the backups, and restore them to VMware Cloud on AWS.
- Restore the SQL Server application data using SnapCenter.
- Restore the Oracle application data using SnapCenter.

SnapCenter supports disaster recovery scenarios by allowing the backup and restore of its MySQL database and configuration files. This allows an administrator to maintain regular backups of the SnapCenter database at the on-premises datacenter and later restore that database to a secondary SnapCenter database.

To access the SnapCenter backup files on the remote SnapCenter server, complete the following steps:

- 1. Break the SnapMirror relationship from the FSx cluster, which makes the volume read/write.
- 2. Create a CIFS server (if necessary) and create a CIFS share pointing to the junction path of the cloned volume.
- 3. Use xcopy to copy the backup files to a local directory on the secondary SnapCenter system.
- 4. Install SnapCenter v4.6.
- 5. Ensure that SnapCenter server has the same FQDN as the original server. This is required for the db restore to be successful.

To start the restore process, complete the following steps:

- 1. Navigate to the Swagger API web page for the secondary SnapCenter server and follow the previous instructions to obtain an authorization token.
- 2. Navigate to the Disaster Recovery section of the Swagger page, select /4.6/disasterrecovery/server/restore, and click Try it Out.

POST	/4.6/disasterrecovery/server/restore Starts SnapCenter Server Restore.
Starts SnapC	Center Server Restore.
Parameters	Try it out

3. Paste in your authorization token and, in the SmDRResterRequest section, paste in the name of the backup and the local directory on the secondary SnapCenter server.

Token * ^{required}	User authorization token
(header)	KIYxOg==rMXzS7EPIGRzTXjfton6Q+JoNGpueQt
SmDRRestoreRequest * require	Parameters to take for Restore
(body)	Edit Value Model
	<pre>{ "BackupName": "SnapCenter.sddc.netapp.com_03-23-2022_12.38.00.6713", "BackupPath": "C:\\SnapCenter\\" }</pre>

163

5. From SnapCenter, navigate to the Monitor section to view the progress of the restore job.

<	Jobs	Schedules	Events Logs
Dashboard	search	by name	
Resources	Jobs - F	ilter	
Monitor	ID	Status	Name
Reports	20482	*	SnapCenter Server Disaster Recovery
	20481	4	SnapCenter Server disaster recovery backup
Hosts	20480	×	SnapCenter Server disaster recovery backup
- Storage Systems	20475	~	Backup of Resource Group 'SQLSRV-09' with policy 'SQL-Hourly'
E Settings	20474	~	Backup of Resource Group 'SQLSRV-05' with policy 'SQL-Hourly'
	20473	2	Backup of Resource Group 'OracleSrv_06' with policy 'Oracle-Hourly'
Alerts	20472	×	SnapCenter Server disaster recovery backup

Job Details

SnapCenter Server Disaster Recovery

- SnapCenter Server Disaster Recovery
- Prepare for restore job
- Precheck validation
- Saving original server state
- Schedule restore
- Repository restore
- Config restore
- Reset MySQL password
- 6. To enable SQL Server restores from secondary storage, you must toggle the SnapCenter database into Disaster Recovery mode. This is performed as a separate operation and initiated on the Swagger API web page.
 - a. Navigate to the Disaster Recovery section and click /4.6/disasterrecovery/storage.
 - b. Paste in the user authorization token.
 - c. In the SmSetDisasterRecoverySettingsRequest section, change EnableDisasterRecover to true.
 - d. Click Execute to enable disaster recovery mode for SQL Server.

Name	Description
Token * required string	User authorization token
(header)	KIYxOg==rMXzS7EPIGRzTXjfton6Q+JoNGpueQt
SmSetDisasterRecoverySettingsRequest * required object	Parameters to enable or disable the DR mode
(body)	Edit Value Model
	<pre>{ "EnableDisasterRecovery": true }</pre>
See comments regarding addit	ional procedures
See comments regarding add	ional procedures.

Restore application VMs with Veeam full restore

From the secondary Veeam server, import the backups from S3 storage and restore the SQL Server and Oracle VMs to your VMware Cloud cluster.

To import the backups from the S3 object that was part of the on-premises scale-out backup repository, complete the following steps:

1. Go to Backup Repositories and click Add Repository in the top menu to launch the Add Backup Repository wizard. On the first page of the wizard, select Object Storage as the backup repository type.

	ackup Repository type of backup repository you want to add.	
	Direct attached storage Microsoft Windows or Linux server with internal or direct attached storage. This configuration enables data movers to run directly on the server, allowing for fastest performance.	
	Network attached storage Network share on a file server or a NAS device. When backing up to a remote share, we recommend that you select a gateway server located in the same site with the share.	
¥	Deduplicating storage appliance Dell EMC Data Domain, ExaGrid, HPE StoreOnce or Quantum DXi. If you are unable to meet the requirements of advanced integration via native appliance API, use the network attached storage option instead.	
	Object storage On-prem object storage system or a cloud object storage provider. Object storage can only be used as a Capacit Tier of scale-out backup repositories, backing up directly to object storage is not currently supported.	ty

2. Select Amazon S3 as the Object Storage type.

	Object Storage Select the type of object storage you want to use as a backup repository.
R	S3 Compatible Adds an on-premises object storage system or a cloud object storage provider.
aws	Amazon S3 Adds Amazon cloud object storage. Amazon S3, Amazon S3 Glacier (including Deep Archive) and Amazon Snowball Edge are supported
٥	Google Cloud Storage Adds Google Cloud storage. Both Standard and Nearline storage classes are supported.
	IBM Cloud Object Storage Adds IBM Cloud object storage. S3 compatible versions of both on-premises and IBM Cloud storage offerings are supported.
Δ	Microsoft Azure Storage Adds Microsoft Azure cloud object storage. Microsoft Azure Blob Storage, Microsoft Azure Archive Storage and Microsoft Azure Data Box are supported.

- Example the type of Amazon storage you want to use as a backup repository.
 Amazon S3 Adds Amazon S3 storage. Both Standard and Infrequent Access (IA) storage classes are supported.
 Amazon S3 Glacier Adds Amazon S3 Glacier storage. Both Amazon S3 Glacier and Glacier Deep Archive are supported.
 Amazon S3 Glacier Storage. Both Amazon S3 Glacier and Glacier Deep Archive are supported.
 Adds Amazon S3 Glacier storage. Both Amazon S3 Glacier and Glacier Deep Archive are supported.
- 4. Select your pre-entered credentials from the drop-down list or add a new credential for accessing the cloud storage resource. Click Next to continue.

×

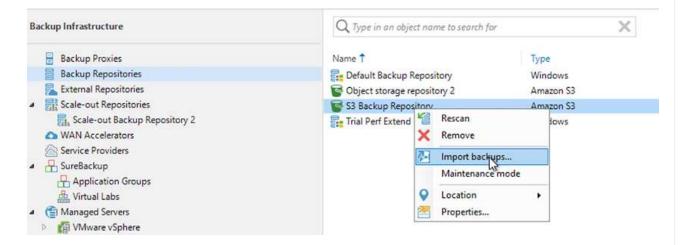
Specify AWS	account to use for connecting to Amazon S3 storage bucket.
Name	Credentials:
Account	🖗 AKIAX4H43ZT53YJXPY2Y (last edited: 33 days ago) 🗸 Add
ucket	Manage cloud accounts AWS region:
	Global
	Use the following gateway server:
	Use the following gateway server: EC2AMAZ-3POTKQV (Backup server)

5. On the Bucket page, enter the data center, bucket, folder, and any desired options. Click Apply.

Name	Data center:	
	US East (N. Virginia)	
Account	Bucket:	
Bucket	ehcveeamrepo	Browse
Summary	Folder:	
Summary	RTP	Browse
	 Limit object storage consumption to: 10 TB This is a soft limit to help control your object storage spend. If the specified lialready running backup offload tasks will be allowed to complete, but no new Make recent backups immutable for: 30 days Protects backups from modification or deletion by ransomware, hackers or new 	w tasks will be started

To import the backups from the S3 repository that was added in the previous section, complete the following steps.

1. From the S3 backup repository, select Import Backups to launch the Import Backups wizard.



2. After the database records for the import have been created, select Next and then Finish at the summary screen to start the import process.

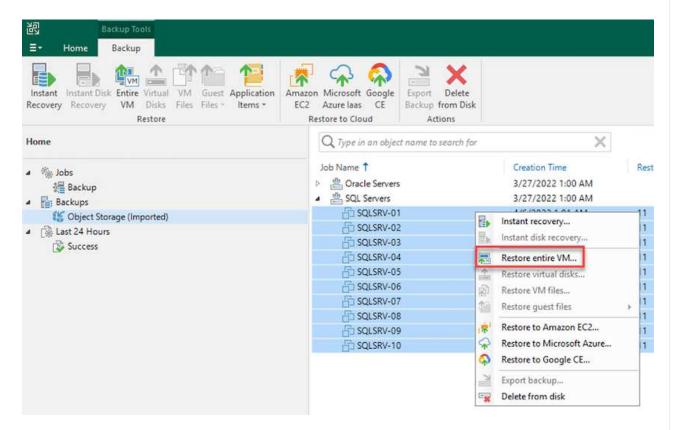
Import Backups Import Please wait v	while we're preparing object storage repository.	×
Import Summary	Message Starting infrastructure item update process	Duration 0:00:16
	Creating database records for repository	0:00:04
	< Previous	ext > Finish Cancel

3. After the import is complete, you can restore VMs into the VMware Cloud cluster.

Name: Action type:	Configuration Database Resynchr Configuration Resynchronize	Status: Start time:		
nitiated by:	EC2AMAZ-3POTKQV\vadmin	End time:	4/6/2022 3:04:57 PM	
Message				Duration
Starting l	backup repositories synchronization			
C Enumera	ting repositories			
Second 1	repository			
🕑 Processir	ng capacity tier extent of S3 Backup Repo	ository 2		0:03:23
💙 S3 Backu	p Repository: added 2 unencrypted			0:03:20
💟 Importin	g backup 2 out of 2			0:03:15
🕑 Backup r	epositories synchronization completed s	successfully		
				Close

To restore SQL and Oracle virtual machines to the VMware Cloud on AWS workload domain/cluster, complete the following steps.

1. From the Veeam Home page, select the object storage containing the imported backups, select the VMs to restore, and then right click and select Restore Entire VM.



2. On the first page of the Full VM Restore wizard, modify the VMs to backup if desired and select Next.

irtual Machines	Virtual machines to restor	151.1		_
Restore Mode	Name		Restore point	Add
ecure Restore	SQLSRV-04	62.7 GB	less than a day ago (1:03 AM	Point
ummary				Remove

3. On the Restore Mode page, select Restore to a New Location, or with Different Settings.

Full VM Restore	×
Restore Mode Specify whethe	e er selected VMs should be restored back to the original location, or to a new location or with different settings.
Virtual Machines Restore Mode	 Restore to the original location Quickly initiate the restore of selected VM to its original location, with the original name and settings. This option minimizes the chance of user input error.
Host Resource Pool	Restore to a new location, or with different settings Customize the restored VM location, and change its settings. The wizard will automatically populate all controls with the original VM settings as the defaults.
Datastore Folder	Staged restore Run the selected VM directly from backup files in the isolated DataLab to make changes to the guest OS or applications prior to placing the VM into production environment.
Network Secure Restore	Pick proxy to use
Summary	
	Quick rollback (restore changed blocks only) Allows for quick VM recovery in case of guest OS software problem, or user error. Do not use this option when recovering from disaster caused by hardware or storage issue, or power loss.
	< Previous Next > Finish Cancel

4. On the host page, select the Target ESXi host or cluster to restore the VM to.

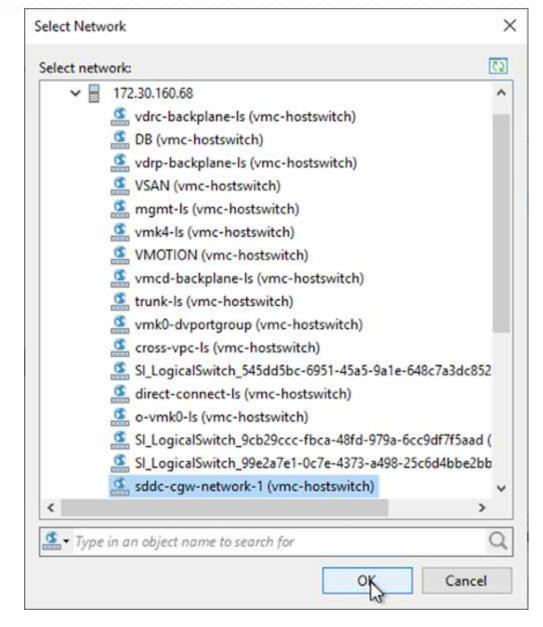
Host		-	
By default, origin Host. Use multi-s Virtual Machines	 ✓ (☐ Hosts ✓ (☑ vcenter.sddc-35-171-99-106.vmwarevmc.com) 	0	ting desired VM and clickir
Restore Mode	✓		st or cluster
Host			
Resource Pool			
Datastore			
Folder			
Network			
Secure Restore			
Summary			
	Type in an object name to search for	Q	Host
	ОК	Cancel	Finish Cancel

5. On the Datastores page, select the target datastore location for both the configuration files and hard disk.

Virtual Machines	Files location:			
Restore Mode	File Generation SQLSRV-04	Size	Datastore	Disk type
Host	Configuration files		WorkloadDatastore (VM	
1051	Hard disk 1 (SQLSR	100 GB	WorkloadDatastore (VM	Same as source
Resource Pool				
Datastore				
Folder				
Vetwork				
ecure Restore				
ummary				
	Select multiple VMs to apply sett	tings in hulk	D	atastore Disk Type.

6. On the Network page, map the original networks on the VM to the networks in the new target location.

Virtual Machines	Network connections:		
Restore Mode	Source	Target	
	4 🗄 SQLSRV-04		
Host	Management 181 (DSwitch) Bota - A - 3374 (DSwitch)	Not connected Not connected	
Resource Pool	S Data - B - 3375 (DSwitch)	Not connected	
	LEAST		
Datastore			
Folder			
Network			
Secure Restore			
Summary			



7. Select whether to scan the restored VM for malware, review the summary page, and click Finish to start the restore.

Restore SQL Server application data

The following process provides instructions on how to recover a SQL Server in VMware Cloud Services in AWS in the event of a disaster that renders the on-premises site inoperable.

The following prerequisites are assumed to be complete in order to continue with the recovery steps:

- 1. The Windows Server VM has been restored to the VMware Cloud SDDC using Veeam Full Restore.
- A secondary SnapCenter server has been established and SnapCenter database restore and configuration has been completed using the steps outlined in the section "SnapCenter backup and restore process summary."

After the restore of the VM is complete, you must configure networking and other items in preparation for rediscovering the host VM within SnapCenter.

- 1. Assign new IP addresses for Management and iSCSI or NFS.
- 2. Join the host to the Windows domain.
- 3. Add the hostnames to DNS or to the hosts file on the SnapCenter server.



If the SnapCenter plug-in was deployed using domain credentials different than the current domain, you must change the Log On account for the Plug-in for Windows Service on the SQL Server VM. After changing the Log On account, restart the SnapCenter SMCore, Plug-in for Windows, and Plug-in for SQL Server services.



To automatically rediscover the restored VMs in SnapCenter, the FQDN must be identical to the VM that was originally added to the SnapCenter on premises.

Configure FSx storage for SQL Server restore

To accomplish the disaster recovery restore process for a SQL Server VM, you must break the existing SnapMirror relationship from the FSx cluster and grant access to the volume. To do so, complete the following steps.

1. To break the existing SnapMirror relationship for the SQL Server database and log volumes, run the following command from the FSx CLI:

FSx-Dest::> snapmirror break -destination-path DestSVM:DestVolName

2. Grant access to the LUN by creating an initiator group containing the iSCSI IQN of the SQL Server Windows VM:

FSx-Dest::> igroup create -vserver DestSVM -igroup igroupName
-protocol iSCSI -ostype windows -initiator IQN

3. Finally, map the LUNs to the initiator group that you just created:

```
FSx-Dest::> lun mapping create -vserver DestSVM -path LUNPath igroup
igroupName
```

4. To find the path name, run the lun show command.

Set up the Windows VM for iSCSI access and discover the file systems

- 1. From the SQL Server VM, set up your iSCSI network adapter to communicate on the VMware Port Group that has been established with connectivity to the iSCSI target interfaces on your FSx instance.
- 2. Open the iSCSI Initiator Properties utility and clear out the old connectivity settings on the Discovery, Favorite Targets, and Targets tabs.
- 3. Locate the IP address(es) for accessing the iSCSI logical interface on the FSx instance/cluster. This can be found in the AWS console under Amazon FSx > ONTAP > Storage Virtual Machines.

Endpoints	
Management DNS name	Management IP address
svm-045c077375d3d9799.fs-0ae40e08acc0dea67.fsx.us-east-1.amazonaws.com	198.19.254.53
NFS DNS name	NFS IP address
svm-045c077375d3d9799.fs-0ae40e08acc0dea67.fsx.us-east-1.amazonaws.com	198.19.254.53
iSCSI DNS name	iSCSI IP addresses
iscsi.svm-045c077375d3d9799.fs-0ae40e08acc0dea67.fsx.us-east-1.amazonaws.com 日	172.30.15.101, 172.30.14.49

4. From the Discovery tab, click Discover Portal and enter the IP addresses for your FSx iSCSI targets.

	iator Proper				
argets	Discovery	Favorite Targets	Volumes and Devices	RADIUS	Configuration
Targe	t portals				
The s	system will lo	ok for Targets on fo	llowing portals:		Refresh
Addr	ress	Port	Adapter	I	P address
To D	dd <mark>a</mark> target p	ortal, <mark>click</mark> Discover	Portal.	Disco	over Portal
10 40	60	et portal, select the	address above and	1	Remove

Discover Target Portal	
Enter the IP address or DNS nar want to add.	me and port number of the portal you
To change the default settings o the Advanced button.	f the discovery of the target portal, dick
	f the discovery of the target portal, dick Port: (Default is 3260.)

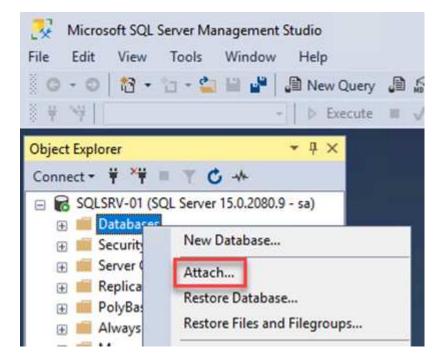
5. On the Target tab, click Connect, select Enable Multi-Path if appropriate for your configuration and then click OK to connect to the target.

argets	Discovery	Favorite Targets	Volumes and Devices	RADIUS	Configuration	
	Connect					
To disc	cover and log	g on to a target usin arget and then click	ng a basic connection, t Quick Connect.	ype the IP	address or	
Target	:			Q	ick Connect	1
Discove	ered targets					
					Refresh	
Name	5			Status]
ign, 19	992-08.com.	netapp:sn.5918b03	3f9ef411ecb007495	Inactive		
					0	
					1	
To con	nect using a	dvanced options, si	elect a target and then		1	,
	nect using a	dvanced options, se	elect a target and then		1 Connect]
dick Co	onnect.		elect a target and then		1	
dick Co			elect a target and then		1 Connect	
tick Co th Fo Ta	onnect.		elect a target and then		1	
dick Co To Co th Co	onnect. onnect To Ta arget name:	arget	elect a target and then Def411ecb0074956fb75	F45c:vs.6	1	
click Co To th Fo Ta Se 19 Fo	onnect. onnect To Ta arget name: 2-08.com.ne	arget tapp:sn.5918b03f9	9ef411ecb0074956fb75	f45c:vs.6	1	
click Co To th Fo Ta Se 19 Fo	onnect. onnect To Ta arget name: 2-08.com.ne Add this con	arget tapp:sn.5918b03f9 nection to the list o	ef411ecb0074956fb75 f Favorite Targets.		1	
dick Co To th Fo Ta Se 19 Fo th	onnect. onnect To Ta arget name: 2-08.com.ne Add this con This will mak	arget tapp:sn.5918b03f9 nection to the list o	ef411ecb0074956fb75 f Favorite Targets. natically attempt to rest		1	
dick Co To th Fo Ta Se Po th Se	onnect. onnect To Ta arget name: 2-08.com.ne Add this con This will mak connection e	arget tapp:sn.5918b03f9 nection to the list o the system auton every time this comp	ef411ecb0074956fb75 f Favorite Targets. natically attempt to rest		1	
dick Co To th Fo Ta Se Po th Se	onnect. onnect To Ta arget name: 2-08.com.ne Add this con This will mak	arget tapp:sn.5918b03f9 nection to the list o the system auton every time this comp	ef411ecb0074956fb75 f Favorite Targets. natically attempt to rest		1	
dick Co To th Co Fo Ta Se 19 Fo th Se 19 Fo Ta Se 19 Fo Ta Se 19 Fo Ta Se 19 Fo Ta Se 19 Fo Ta Se 19 Fo Ta Se 19 Fo Ta Se 19 Fo Ta Se 19 Fo Ta Se 19 Fo Ta Se 19 Fo Ta Se 19 Fo Ta Se 19 Fo Ta Se 19 Fo Ta Se 19 Fo Ta Se 19 Fo Ta Se 10 Ta Se Ta Ta Se Ta Ta Se Ta Ta Se Ta Ta Se Ta Ta Ta Ta Ta Ta Ta Ta Ta Ta	onnect. onnect To Ta arget name: 2-08.com.ne Add this con This will mak connection e Enable multi-	arget tapp:sn.5918b03f9 nection to the list o the system auton every time this comp	Pef411ecb0074956fb75 f Favorite Targets. natically attempt to rest puter restarts.	ore the		
dick Co To th Co Fo Ta Se 19 Fo th Se 19 Fo Ta Se 19 Fo Ta Se 19 Fo Ta Se 19 Fo Ta Se 19 Fo Ta Se 19 Fo Ta Se 19 Fo Ta Se 19 Fo Ta Se 19 Fo Ta Se 19 Fo Ta Se 19 Fo Ta Se 19 Fo Ta Se 19 Fo Ta Se 19 Fo Ta Se 19 Fo Ta Se 19 Fo Ta Se 10 Ta Se Ta Ta Se Ta Ta Se Ta Ta Se Ta Ta Se Ta Ta Ta Ta Ta Ta Ta Ta Ta Ta	onnect. onnect To Ta arget name: 2-08.com.ne Add this con This will mak connection e	arget tapp:sn.5918b03f9 nection to the list o the system auton every time this comp	ef411ecb0074956fb75 f Favorite Targets. natically attempt to rest	ore the	1	

6. Open the Computer Management utility and bring the disks online. Verify that they retain the same drive letters that they previously held.

Basic 579.98 GB Online	MSSQL_DATA (E:) 579.98 GB NTFS Healthy (Primary Partition)	
*O Disk 2 Basic		
99.98 GB Offline	Online	
	Properties	
CD-ROM	Help	Perf 11.

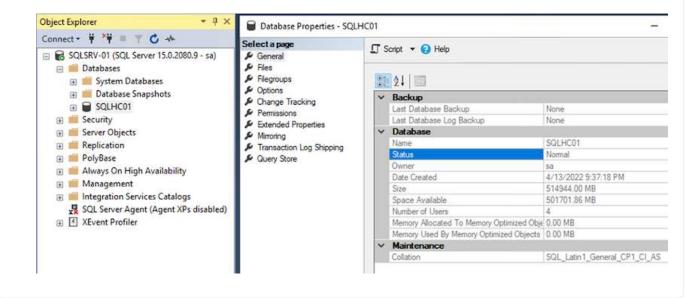
1. From the SQL Server VM, open Microsoft SQL Server Management Studio and select Attach to start the process of connecting to the database.



2. Click Add and navigate to the folder containing the SQL Server primary database file, select it, and click OK.

Locate Database Files - Si	QLSRV-01				\times
Database Data File location:	E:\MSSQL 2019	MSSQL15.MSSQLSERVE	F 🕐		P
C: SRECYCLE.BIN SRECYCLE.BIN MSSQL 2019 MSSQL15.MSS MSSQL DATA DATA System Volume Info	QLSERVER	SQLHC01_01.mdf			
File name: SQ	LHC01_01.mdf		Database Data F	iles(*.mdf)	~

- 3. If the transaction logs are on a separate drive, choose the folder that contains the transaction log.
- 4. When finished, click OK to attach the database.



With the SnapCenter database restored to its previous state, it automatically rediscovers the SQL Server hosts. For this to work correctly, keep in mind the following prerequisites:

- SnapCenter must be placed in Disaster Recover mode. This can be accomplished through the Swagger API or in Global Settings under Disaster Recovery.
- The FQDN of the SQL Server must be identical to the instance that was running in the on-premises datacenter.
- The original SnapMirror relationship must be broken.
- The LUNs containing the database must be mounted to the SQL Server instance and the database attached.

To confirm that SnapCenter is in Disaster Recovery mode, navigate to Settings from within the SnapCenter web client. Go to the Global Settings tab and then click Disaster Recovery. Make sure that the Enable Disaster Recovery checkbox is enabled.

	letApp Snap(Center®
<		Global Settings Policies Users and Access
	Dashboard	
0	Resources	Global Settings
•	Monitor	
m	Reports	Hypervisor Settings 🚯
A	Hosts	Notification Server Settings 🚯
ł	Storage Systems	Configuration Settings ()
***	Settings	Purge Jobs Settings
	Alerts	Domain Settings
		CA Certificate Settings 🕕
		Disaster Recovery
		Enable Disaster Recovery Apply

Restore Oracle application data

The following process provides instructions on how to recover Oracle application data in VMware Cloud Services in AWS in the event of a disaster that renders the on-premises site inoperable.

Complete the following prerequisites to continue with the recovery steps:

- 1. The Oracle Linux server VM has been restored to the VMware Cloud SDDC using Veeam Full Restore.
- 2. A secondary SnapCenter server has been established and the SnapCenter database and configuration files have been restored using the steps outlined in this section "SnapCenter backup and restore process summary."

To make the secondary storage volumes hosted on the FSxN instance accessible to the Oracle servers, you must first break the existing SnapMirror relationship.

1. After logging into the FSx CLI, run the following command to view the volumes filtered by the correct name.

```
FSx-Dest::> volume show -volume VolumeName*
FsxId0ae40e08acc0dea67::> volume show -volume oraclesrv 03*
Vserver
         Volume
                     Aggregate
                                  State
                                             Type
                                                       Size Available Used%
ora svm dest
         oraclesrv_03_u01_dest
                      aggrl
                                  online
                                             DP
                                                       100GB
                                                               93.12GB
                                                                          68
ora svm dest
         oraclesrv 03 u02 dest
                                             DP
                                                      200GB
                                                               34.98GB
                                                                         82%
                      aggrl
                                  online
ora svm dest
         oraclesrv 03 u03 dest
                                             DP
                                                       150GB
                                                               33.37GB
                                                                         778
                      aggrl
                                  online
3 entries were displayed.
FsxId0ae40e08acc0dea67::>
```

2. Run the following command to break the existing SnapMirror relationships.

FSx-Dest::> snapmirror break -destination-path DestSVM:DestVolName

FsxId0ae40e08acc0dea67::> snapmirror break -destination-path ora_svm_dest:oraclesrv_03_u02_dest Operation succeeded: snapmirror break for destination "ora_svm_dest:oraclesrv_03_u02_dest".

FsxId0ae40e08acc0dea67::> snapmirror break -destination-path ora_svm_dest:oraclesrv_03_u03_dest Operation succeeded: snapmirror break for destination "ora_svm_dest:oraclesrv_03_u03_dest".

3. Update the junction-path in the Amazon FSx web client:

FSx > Volumes > fsvol-01167370e9b7aefa0 oraclesrv_03_u01_dest (fsvol-01167370e9b7aefa0) Attach Actions 🔺 Update volume Summary Create backup Delete volume Volume ID Creation time SVM ID 2022-03-08T14:52:09-05:00 svm-02b2ad25c6b2e5bc2 fsvol-01167370e9b7aefa0 🗇 Lifecycle state Junction path Volume name ⊘ Created - 🗇 oraclesrv_03_u01_dest Volume type Tiering policy name UUID ONTAP SNAPSHOT_ONLY 3d7338ce-9f19-11ecb007-4956fb75f45c Size Tiering policy cooling period (days) 100.00 GB 🗇 2 File system ID fs-0ae40e08acc0dea67 Storage efficiency enabled Disabled Resource ARN arn:aws:fsx:useast-1:541696183547:volume/fs-0ae40e08acc0dea67/fsvol-01167370e9b7aefa0 🗇

4. Add the junction path name and click Update. Specify this junction path when mounting the NFS volume from the Oracle server.

Update volume

Junction path

/oraclesrv_03_u01_dest

The location within your file system where your volume will be mounted.

Volume size

102400

Minimum 20 MiB; Maximum 104857600 MiB

Storage efficiency

Select whether you would like to enable ONTAP storage efficiencies on your volume: deduplication, compression, and compaction.

Capacity pool tiering policy You can optionally enable automatic tiering of	your data to lower-cos	t capacity pool st	orage.
Snapshot Only			•

×

\$

In Cloud Manager, you can obtain the mount command with the correct NFS LIF IP address for mounting the NFS volumes that contain the Oracle database files and logs.

1. In Cloud Manager, access the list of volumes for your FSx cluster.

HCApps	Overview Volumes			
	50 Volumes Volume Name ÷	State ÷	Storage VM 💠	Disk Type
	oraclesrv_02_ u02_dest	• Online	ora_svm_dest	SSD
	oraclesrv_02_ u03_dest	• Online	ora_svm_dest	SSD
	oraclesrv_03_ u01_dest	• Online	ora_svm_dest	SSD

2. From the action menu, select Mount Command to view and copy the mount command to be used on our Oracle Linux server.

etApp	Information	or ~ nconn	
	Edit		
	Clone		
	Restore from Snapshot copy		
	Create a Snapshot copy		
Capacity Pool Us	Mount Command		
0 B	Change Tiering Policy		
0 B	Delete		
	Snapshot		
	Mount Volume NFS oraclesrv_03_u01_dest		
Go to your linux m	achine and enter this mount comn	nand	
Mount Command			
mount 109 10 2	54.180:/oraclesrv_03_u01_dest <d< td=""><td>est d</td><td>Copy</td></d<>	est d	Copy

- 3. Mount the NFS file system to the Oracle Linux Server. The directories for mounting the NFS share already exist on the Oracle Linux host.
- 4. From the Oracle Linux server, use the mount command to mount the NFS volumes.

FSx-Dest::> mount -t oracle server ip:/junction-path

Repeat this step for each volume associated with the Oracle databases.



To make the NFS mount persistent upon rebooting, edit the /etc/fstab file to include the mount commands.

5. Reboot the Oracle server. The Oracle databases should start up normally and be available for use.

Failback

Upon successful completion of the failover process outlined in this solution, SnapCenter and Veeam resume their backup functions running in AWS, and FSx for ONTAP is now designated as primary storage with no existing SnapMirror relationships with the original on-premises datacenter. After normal function has resumed on premises, you can use a process identical to the one outlined in this documentation to mirror data back to the on-premises ONTAP storage system.

As is also outlined in this documentation, you can configure SnapCenter to mirror the application data volumes from FSx for ONTAP to an ONTAP storage system residing on premises. Similarly, you can configure Veeam to replicate backup copies to Amazon S3 using a scale-out backup repository so that those backups are accessible to a Veeam backup server residing at the on-premises datacenter.

Failback is outside the scope of this documentation, but failback differs little from the detailed process outlined here.

Conclusion

The use case presented in this documentation focuses on proven disaster recovery technologies that highlight the integration between NetApp and VMware. NetApp ONTAP storage systems provide proven data-mirroring technologies that allow organizations to design disaster recovery solutions that span on-premises and ONTAP technologies residing with the leading cloud providers.

FSx for ONTAP on AWS is one such solution that allows for seamless integration with SnapCenter and SyncMirror for replicating application data to the cloud. Veeam Backup & Replication is another well-known technology that integrates well with NetApp ONTAP storage systems and can provide failover to vSphere-native storage.

This solution presented a disaster recovery solution using guest connect storage from an ONTAP system hosting SQL Server and Oracle application data. SnapCenter with SnapMirror provides an easy-to-manage solution for protecting application volumes on ONTAP systems and replicating them to FSx or CVO residing in the cloud. SnapCenter is a DR-enabled solution for failing over all application data to VMware Cloud on AWS.

Where to find additional information

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

• Links to solution documentation

NetApp Hybrid Multicloud with VMware Solutions

NetApp Solutions

Veeam Backup & Restore in VMware Cloud, with Amazon FSx for ONTAP

Veeam Backup & Replication is an effective and reliable solution for protecting data in VMware Cloud. This solution demonstrates the proper setup and configuration for using Veeam Backup and Replication to backup and restore application VMs residing on FSx for ONTAP NFS datastores in VMware Cloud.

Author: Josh Powell - NetApp Solutions Engineering

Overview

VMware Cloud (in AWS) supports the use of NFS datastores as supplemental storage, and FSx for NetApp ONTAP is a secure solution for customers who need to store large amounts of data for their cloud applications that can scale independent of the number of ESXi hosts in the SDDC cluster. This integrated AWS storage service offers highly efficient storage with all of the traditional NetApp ONTAP capabilities.

Use Cases

This solution addresses the following use cases:

- Backup and restore of Windows and Linux virtual machines hosted in VMC using FSx for NetApp ONTAP as a backup repository.
- Backup and restore of Microsoft SQL Server application data using FSx for NetApp ONTAP as a backup repository.
- Backup and restore of Oracle application data using FSx for Netapp ONTAP as a backup repository.

NFS Datastores Using Amazon FSx for ONTAP

All virtual machines in this solution reside on FSx for ONTAP supplemental NFS datastores. Using FSx for ONTAP as a supplemental NFS datastore has several benefits. For example, it allows you to:

- Create a scalable and highly available file system in the cloud without the need for complex setup and management.
- Integrate with your existing VMware environment, allowing you to use familiar tools and processes to manage your cloud resources.
- Benefit from the advanced data management features provided by ONTAP, such as snapshots and replication, to protect your data and ensure its availability.

This list provides the high level steps necessary to configure Veeam Backup & Replication, execute backup and restore jobs using FSx for ONTAP as a backup repository, and perform restores of SQL Server and Oracle VMs and databases:

- 1. Create the FSx for ONTAP file system to be used as iSCSI backup repository for Veeam Backup & Replication.
- 2. Deploy Veeam Proxy to distribute backup workloads and mount iSCSI backup repositories hosted on FSx for ONTAP.
- 3. Configure Veeam Backup Jobs to backup SQL Server, Oracle, Linux and Windows virtual machines.
- 4. Restore SQL Server virtual machines and individual databases.
- 5. Restore Oracle virtual machines and individual databases.

Prerequisites

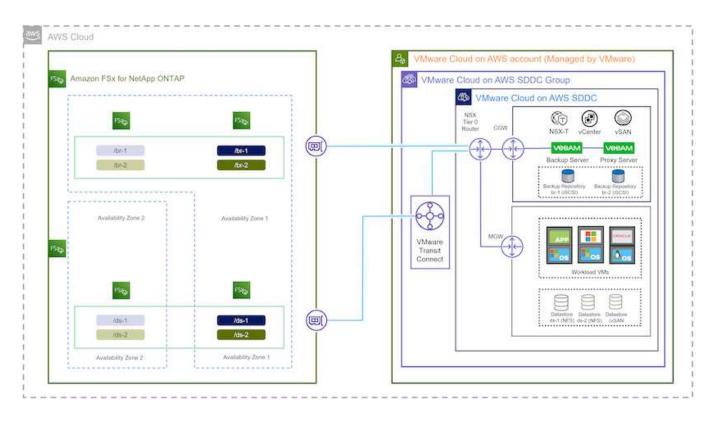
The purpose of this solution is to demonstrate data protection of virtual machines running in VMware Cloud and located on NFS Datastores hosted by FSx for NetApp ONTAP. This solution assumes the following components are configured and ready for use:

- 1. FSx for ONTAP filesystem with one or more NFS datastores connected to VMware Cloud.
- 2. Microsoft Windows Server VM with Veeam Backup & Replication software installed.
 - vCenter server has been discovered by the Veeam Backup & Replication server using their IP address or fully qualified domain name.
- 3. Microsoft Windows Server VM to be installed with Veeam Backup Proxy components during the solution deployment.
- 4. Microsoft SQL Server VMs with VMDKs and application data residing on FSx for ONTAP NFS datastores. For this solution we had two SQL databases on two separate VMDKs.
 - Note: As a best practice database and transaction log files are placed on separate drives as this will improve performance and reliability. This is in part due to the fact that transaction logs are written sequentially, whereas database files are written randomly.
- 5. Oracle Database VMs with VMDKs and application data residing on FSx for ONTAP NFS datastores.
- 6. Linux and Windows file server VMs with VMDKs residing on FSx for ONTAP NFS datastores.
- 7. Veeam requires specific TCP ports for communication between servers and components in the backup environment. On Veeam backup infrastructure components, the required firewall rules are automatically created.

For a full listing of the network port requirements refer to the Ports section of the Veeam Backup and Replication User Guide for VMware vSphere.

High Level Architecture

The testing / validation of this solution was performed in a lab that may or may not match the final deployment environment. For more information, please refer to the following sections.



Hardware / Software Components

The purpose of this solution is to demonstrate data protection of virtual machines running in VMware Cloud and located on NFS Datastores hosted by FSx for NetApp ONTAP. This solution assumes the following components are already configured and ready for use:

- Microsoft Windows VM's located on an FSx for ONTAP NFS Datastore
- · Linux (CentOS) VM's located on an FSx for ONTAP NFS Datastore
- Microsoft SQL Server VM's located on an FSx for ONTAP NFS Datastore
 - Two databases hosted on separate VMDK's
- Oracle VM's located on an FSx for ONTAP NFS Datastore

Solution Deployment

In this solution we provide detailed instructions for deploying and validating a solution utilizing Veeam Backup and Replication software to perform backup and recovery of SQL Server, Oracle, and Windows and Linux file server virtual machines in a VMware Cloud SDDC on AWS. The Virtual Machines in this solution reside on a supplemental NFS datastore hosted by FSx for ONTAP. In addition, a separate FSx for ONTAP file system is used to host iSCSI volumes that will be used for Veeam backup repositories.

We will go over FSx for ONTAP file system creation, mounting iSCSI volumes to be used as backup repositories, creating and running backup jobs, and performing VM and database restores.

For detailed information on FSx for NetApp ONTAP refer to the FSx for ONTAP User Guide.

For detailed information on Veeam Backup and Replication refer to the Veeam Help Center Technical Documentation site.

For considerations and limitations when using Veeam Backup and Replication with VMware Cloud on AWS, refer to VMware Cloud on AWS and VMware Cloud on Dell EMC Support. Considerations and Limitations.

Deploy Veeam Proxy server

A Veeam proxy server is a component of the Veeam Backup & Replication software that acts as an intermediary between the source and the backup or replication target. The proxy server helps to optimize and accelerate data transfer during backup jobs by processing data locally and can use different Transport Modes to access data using VMware vStorage APIs for Data Protection or through direct storage access.

When choosing a Veeam proxy server design it is important to consider the number of concurrent tasks and the transport mode or type of storage access desired.

For sizing the number of proxy servers, and for their system requirements, refer to the Veeam VMware vSphere Best Practice Guide.

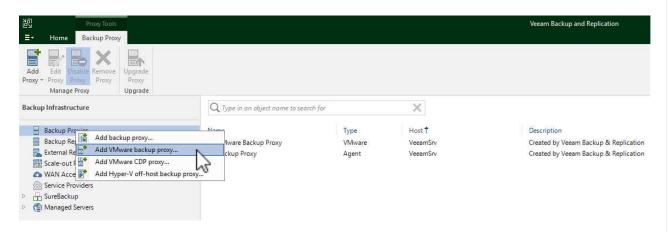
The Veeam Data Mover is a component of the Veeam Proxy Server and utilizes a Transport Mode as a method for obtaining VM data from the source and transferring it to the target. The transport mode is specified during the configuration of the backup job. It is possible to increase the efficiency backups from NFS datastores by using direct storage access.

For more information on Transport Modes refer to the Veeam Backup and Replication User Guide for VMware vSphere.

In the following step we cover deployment of the Veeam Proxy Server on a Windows VM in the VMware Cloud SDDC.

In this step the Veeam Proxy is deployed to an existing Windows VM. This allows backup jobs to be distributed between the primary Veeam Backup Server and the Veeam Proxy.

- 1. On the Veeam Backup and Replication server, open the administration console and select **Backup Infrastructure** in the lower left menu.
- 2. Right click on Backup Proxies and click on Add VMware backup proxy... to open the wizard.



3. In the Add VMware Proxy wizard click the Add New... button to add a new proxy server.

Server	Choose server:	
	VeeamSrv (Backup server)	Add Nev
Traffic Rules	Proxy description:	-
Apply	Created by VEEAMSRV\Administrator at 12/22/2022 9:11 PM.	
Summary		
unnary		
	Transport mode:	10.00
	Automatic selection	Choose
	Connected datastores:	
	Automatic detection (recommended)	Choose
		il shi
	Max concurrent tasks:	

198

- \circ Select an account to use for Credentials on the new system or add new credentials
- Review the components to be installed and then click on Apply to begin the deployment

Vame	Message	Duration
redentials	Starting infrastructure item update process	0:00:03
regenuals	Collecting hardware info	
eview	Detecting operating system	
	🖉 Detecting OS version	
Apply	🖉 Creating temporary folder	
Summary	Package VeeamTransport.msi has been uploaded	0:00:05
	Package VeeamGuestAgent_x86.msi has been uploaded	
	🖉 Package VeeamGuestAgent_x64.msi has been uploaded	
	🖉 Package VeeamLogBackupService_x86.msi has been uploaded	0:00:01
	Package VeeamLogBackupService_x64.msi has been uploaded	
	Installing package Transport	0:00:19

5. Back in the **New VMware Proxy** wizard, choose a Transport Mode. In our case we chose **Automatic Selection**.

Choose a se	Transport Mode	× ux servers added to the
Managed Se	Backup proxy transport mode:	lux servers added to the
erver Traffic Rules	Automatic selection Data retrieval mode is selected automatically by analyzing backup proxy configuration and reachable VMFS and NFS datastores. Transport modes allowing for direct storage access will be used whenever possible.	2/2022 9 ~ Add New.
Apply Summary	 Direct storage access Data is retrieved directly from shared storage, without impacting production hosts. For block storage, backup proxy server must be connected into SAN fabric via hardware or software HBA, and have VMFS volumes mounted. Virtual appliance Data is retrieved directly from storage through hypervisor I/O stack by hot adding backed up virtual disks to a backup proxy VM. Datastores containing protected VMs must be connected to a host running backup proxy VM. Network Data is retrieved from storage through hypervisor network stack using NBD protocol over host management interface. This mode has no special setup requirements. Recommended for 10 Gb Ethernet or faster. Options Failover to network mode if primary mode fails, or is unavailable Enable host to proxy traffic encryption in Network mode (NBDSSL) 	Choose

6. Select the Connected datastores that you want the VMware Proxy to have direct access to.

Server

Choose a server for VMware backup proxy. You can choose between any Microsoft Windows or Linux servers added to the Managed Servers which are not assigned a VMware backup proxy role already.

X

Server	Choose server:	
	veeamproxy.demozone.com (Created by VEEAMSRV\Administrator at 12/22/2022 9 $ \smallsetminus $	Add New.
Traffic Rules	Proxy description:	
Apply	Created by VEEAMSRV\Administrator at 12/22/2022 9:11 PM.	
c		
summary		
summary	Transport mode:	
summary	Transport mode: Direct storage access	Choose
Summary		Choose

200

	Select Objects	×	6
1	Select objects:	62	er
	 Hosts and Disks venter.sddc-52-34-17-99.vmwarevmc.com DS01 DS02)2:
	■ • Type in an object name to search for	Q	
	Type in an object name to search for	Cancel	Fine

7. Configure and apply any specific network traffic rules such as encryption or throttling that are desired. When complete click on the **Apply** button to complete the deployment.

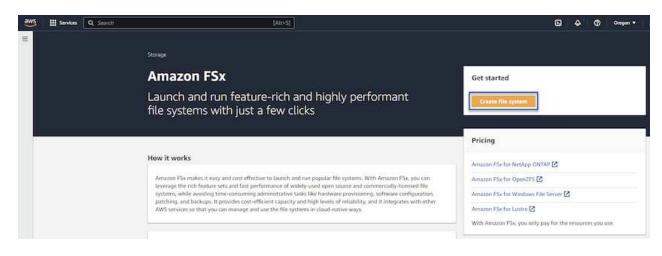
		with set bandwidth spl		network traffic bas ss all backup proxie	
Traffic Rules		ork traffic rules apply to			-
Apply	Name Internet	Encryption Enabled	Throttling Disabled	Time period	View
Summary					
	Manage network tra	ffic rules			

Configure storage and Backup Repositories

The primary Veeam Backup server and Veeam Proxy server have access to a backup repository in the form of direct connected storage. In this section we cover creating an FSx for ONTAP file system, mounting iSCSI LUNs to the Veeam servers and creating Backup Repositories.

Create an FSx for ONTAP file system that will be used to host the iSCSI volumes for the Veeam Backup Repositories.

1. In the AWS console, Go to FSx and then Create file system

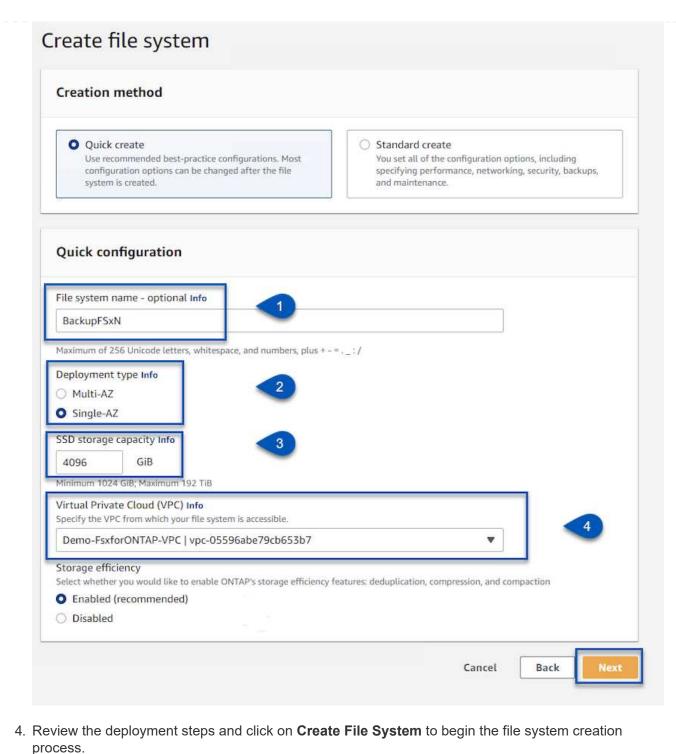


2. Select Amazon FSx for NetApp ONTAP and then Next to continue.

Select file system type

Amazon F5x for NetApp ONTAP	Amazon FSx for OpenZFS	Amazon FSx for Windows File Server	 Amazon FSx for Lustre
FSX	FSX _{z=}	FSx□	FSXa
Amazon FSx for NetApp ONTAP	Amazon FSx for OpenZFS	Amazon FSx for Windows File Server	Amazon FSx for Lustre
		storage built on NetApp's popular ONTAP file system an nning on AWS or on-premises) via industry-standard NF	
Broadly accessible from Linux, Windows, a Provides ONTAP's popular data managem	ind macOS compute instances and containers (nu	nning on AWS or on-premises) via industry-standard NF ata replication), FlexClone (for data cloning), and data co	5, SMB, and iSCSI protocols.
Broadly accessible from Linux, Windows, a Provides ONTAP's popular data managem Delivers hundreds of thousands of IOPS w Differs highly-available and highly-durable	ind macOS compute instances and containers (nu ent capabilities like Snapshots, SnapMirror (for d rith consistent sub-millisecond latencies, and up i e multi-AZ SSD storage with support for cross-ree	nning on AWS or on-premises) via industry-standard NF ata replication), FlexClone (for data cloning), and data co	5, 5MB, and ISCSI protocols. mpression / deduplication.

 Fill in the file system name, deployment type, SSD storage capacity and the VPC in which the FSx for ONTAP cluster will reside. This must be a VPC configured to communicate with the virtual machine network in VMware Cloud. Click on Next.



Create and configure the iSCSI LUNs on FSx for ONTAP and mount to the Veeam backup and proxy servers. These LUNs will later be used to create Veeam backup repositories.



Creating an iSCSI LUN on FSx for ONTAP is a multi-step process. The first step of creating the volumes can be accomplished in the Amazon FSx Console or with the NetApp ONTAP CLI.



For more information on using FSx for ONTAP, see the FSx for ONTAP User Guide.

1. From the NetApp ONTAP CLI create the initial volumes using the following command:

```
FSx-Backup::> volume create -vserver svm_name -volume vol_name
-aggregate aggregate_name -size vol_size -type RW
```

2. Create LUNs using the volumes created in the previous step:

```
FSx-Backup::> lun create -vserver svm_name -path
/vol/vol_name/lun_name -size size -ostype windows -space-allocation
enabled
```

3. Grant access to the LUNs by creating an initiator group containing the iSCSI IQN of the Veeam backup and proxy servers:

FSx-Backup::> igroup create -vserver svm_name -igroup igroup_name -protocol iSCSI -ostype windows -initiator IQN



To complete the preceding step you will need to first retrieve the IQN from the iSCSI initiator properties on the Windows servers.

4. Finally, map the LUNs to the initiator group that you just created:

```
FSx-Backup::> lun mapping create -vserver svm_name -path
/vol/vol_name/lun_name igroup igroup_name
```

5. To mount the iSCSI LUNs, log into the Veeam Backup & Replication Server and open iSCSI Initiator Properties. Go to the **Discover** tab and enter the iSCSI target IP address.

iscover Target Portal	×	nfiguration
inter the IP address or DNS name and port number of the port vant to add. o change the default settings of the discovery of the target po	10/1 1/48	resh
e Advanced button.		Idress
P address or DNS name: Port: (Default is 32	60.)	
10.49.0.154 3260		
Advanced QK	Cancel	Portal
then dick Remove.	Re	nove
iSNS servers		
iSNS servers The system is registered on the following iSNS servers:	Rei	fresh
	Re	fresh
The system is registered on the following iSNS servers:	Re	fresh
The system is registered on the following iSNS servers:		fresh erver

6. On the **Targets** tab, highlight the inactive LUN and click on **Connect**. Check the **Enable multi-path** box and click on **OK** to connect to the LUN.

argets	Discovery	Favorite Targets	Volumes and Devices	RADIUS	Configuration	
Quick C	onnect					
To disco DNS na	over and log me of the ta) on to a target usir arget and then dick	ng a basic connection, t Quick Connect.	/pe the IP	address or	
Target:				Qu	ick Connect	
Discove	red targets					
					Refresh	
Name		in in	No. No. Sta	Status		
0.625862	92-08.com.	netapp:sn.d9aad3c	d818011edbfcd87a	2222046		
iqn. 19	nect using a	7. 45	d818011edbfcd87a	2222046	Connect	
To conr click Co	nect using a	dvanced options, se	elect a target and then	2222046	Connect Disconnect	
To conr dick Co To com then di For targ	nect using a nnect. pletely disco ck Disconner get properti	dvanced options, so onnect a target, sel	elect a target and then	Inactive		

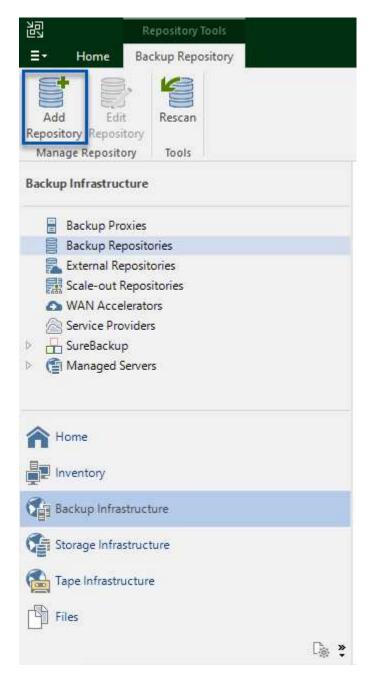
7. In the Disk Management utility initialize the new LUN and create a volume with the desired name and drive letter. Check the **Enable multi-path** box and click on **OK** to connect to the LUN.

🗢 🔿 🖄 📰 🔽 📷 🗩 🗹		[1+[T	Els Cartan	Chatan			
 System Tools Task Scheduler Event Viewer Shared Folders Local Users and Groups Performance Device Manager Storage Windows Server Backup Disk Management Services and Applications 	<	me Wizard on ther you war of format this at this volume e system: ocation unit s lume fabel: Perform a qu	tition, yo nt to form volume with th ize:	e following sett NTFS Default Backup_	it first. e, and if so, wha tings: Target	t settings you want to use.	×	hary Partitio

8. Repeat these steps to mount the iSCSI volumes on the Veeam Proxy server.

In the Veeam Backup and Replication console, create backup repositories for the Veeam Backup and Veeam Proxy servers. These repositories will be used as backup targets for the virtual machines backups.

1. In the Veeam Backup and Replication console click on **Backup Infrastructure** in the lower left and then select **Add Repository**



2. In the New Backup Repository wizard, enter a name for the repository and then select the server from the drop-down list and click on the **Populate** button to choose the NTFS volume that will be used.

Name	Repository server:			
Server	veeamproxy.demozone.com (Cre	ated by VEEAMSRV\Administrator at 12	/22/2022 9 🗸	Add New.
	Path	Capacity	Free	Populate
Repository		89.4 GB	74 GB	
Mount Server	⊂ E:\	1.9 TB	1.9 TB	
Review				
Apply				
Summary				

- 3. On the next page choose a Mount server that will be used to mount backups to when performing advanced restores. By default this is the same server that has the repository storage connected.
- 4. Review your selections and click on **Apply** to start the backup repository creation.

lame	the following components will be processed on service	/er veeamproxy.demozone.com:
	Component name	Status
erver	Transport	already exists
Repository	vPower NFS	will be installed
repository	Mount Server	will be installed
Mount Server		
lpply		
Apply Summary	Search the repository for existing backups and in	
	Search the repository for existing backups and in	

Configure Veeam backup jobs

Backup jobs should be created utilizing the the Backup Repositories in the previous section. Creating backup jobs is a normal part of any storage administrator's repertoire and we do not cover all of the steps here. For more complete information on creating backup jobs in Veeam, see the Veeam Help Center Technical Documentation.

In this solution separate backup jobs were created for:

- Microsoft Windows SQL Servers
- Oracle database servers
- · Windows file servers
- Linux file servers

- 1. Enable application-aware processing to create consistent backups and perform transaction log processing.
- 2. After enabling application-aware processing add the correct credentials with admin privileges to the application as this may be different than the guest OS credentials.

Specify	Oracle ac	count w	ith SYSDE	A privileges: 🄇		
🔧 Use	guest OS	creden	tials		~	Add
				Manage	accounts	
Archived	d logs:					
() Do n	ot delete	archive	d logs			
Dele	te logs ol	der thar	n: 24 📑	hours		
O Dele	te logs ov	/er:	10	GB		
🗌 Back	up logs e	every:	15	minutes		
Reta	in log ba	ckups:				
۱ ا	Intil the o	orrespo	nding im	age-level backu	ip is deleted	
OK	leep only	last 1	5 🌻 da	ys of log back	ıba	
Log	shipping	servers;				
Aut	omatic se	election				Choose

3. To manage the retention policy for the backup check the **Keep certain full backups longer for archival purposes** and click the **Configure...** button to configure the policy.

Con	figure GFS		×	
	Keep weekly full backups for: 15 🚔 weeks			10:3 ~
	If multiple full backups exist, use the one from:	Sunday	~	packup
\square	Keep monthly full backups for: 12 🚔 months			
	Use weekly full backup from the following week of a month:	First	~	Configure
	Keep yearly full backups for:			
	Use monthly full backup from the following month:	January	~	
				Ve recommend to m d off-site.
~	ve As Default OK	Canc	el	

Restore Application VMs with Veeam full restore

Performing a full restore with Veeam is the first step in performing an application restore. We validated that full restores of our VMs powered on and all services were running normally.

Restoring servers is a normal part of any storage administrator's repertoire and we do not cover all of the steps here. For more complete information on performing full restores in Veeam, see the Veeam Help Center Technical Documentation.

Restore SQL Server databases

Veeam Backup & Replication provides several options for restoring SQL Server databases. For this validation we used the Veeam Explorer for SQL Server with Instant Recovery to execute restores of our SQL Server databases. SQL Server Instant Recovery is a feature that allows you to quickly restore SQL Server databases without having to wait for a full database restore. This rapid recovery process minimizes downtime and ensures business continuity. Here's how it works:

- Veeam Explorer mounts the backup containing the SQL Server database to be restored.
- The software **publishes the database** directly from the mounted files, making it accessible as a temporary database on the target SQL Server instance.
- While the temporary database is in use, Veeam Explorer **redirects user queries** to this database, ensuring that users can continue to access and work with the data.
- In the background, Veeam **performs a full database restore**, transferring data from the temporary database to the original database location.
- Once the full database restore is complete, Veeam Explorer **switches user queries back to the original** database and removes the temporary database.

1. In the Veeam Backup and Replication console, navigate to the list of SQL Server backups, right click on a server and select **Restore application items** and then **Microsoft SQL Server databases...**.

Home Backup Instant Instant Disk Entire Virtual VM Guest Applica Recovery VM Disks Files - Beno Retore	ion Amazon Microsoft Google EC2 Azure Las CE Backup from Disk Bestore to Cloud				
Home	Q. Type in an object name to search for	×			
 Na Jobs Pan Backups 	Job Name 1 SOB Server Backups	Creation Time 1/10/2023 9:05 PM	Restore Points	Repository Repository - Veeam Server	Platform VMware
🖹 Disk > 🕼 Last 24 Hours	Instant recovery Instant recovery Instant disk recovery Restore entire VM Restore WM files Restore guest files	10/2023 9:44 PM 10/2023 9:45 PM 10/2023 9:47 PM	2		
	Restore application item Restore to Amazon EC2. Restore to Microsoft Aa Restore to Microsoft Aa Restore to Google CE	E S	rver databases		
	Export backup				

2. In the Microsoft SQL Server Database Restore Wizard select a restore point from the list and click on **Next**.

estore Point eason ummary	VM name: sql_srv_wkld_1 VM size: 43.9 GB O Restore from the latest available backup Restore from this restore point:	VM size: 43.9 GB O Restore from the latest available backup				
	Created	Туре	Backup			
	🕑 less than a day ago (9:44 PM Tuesday	Increment	SQL Server Backups			

3. Enter a **Restore reason** if desired and then, on the Summary page, click on the **Browse** button to launch Veeam Explorer for Microsoft SQL Server.

Microsoft SQL	Server	Database	Restore
---------------	--------	----------	---------

estore Point eason immary	Summary: MM name: sql_srv_wkld_1 Restore point: Current: sql_srv_wkld_1 less than a day ago (9:07 PM Tuesday 1/10/2023)
	< Previous Next > Browse Cancel

4. In Veeam Explorer expand the list of database instances, right click and select **Instant recovery** and then the specific restore point to recover to.

à ≣• Home	Databas				sql_	srv_wkld_1	as of less than a day ago (9:07 PM	Tuesday 1/10/2023) - Veeam Explorer for Microsoft SQL Server
Instant Recovery •	Publish Database •	Restore Database • Resto		Export Backup •	Export Files • Schemi Export			
Databases					Database I	nfo		
▲ 🔚 SQLSRV-0 ▲ 📴 Defaul	t instance				Name: Backup create	d:	DATA_01 1/10/2023 9:07 PM	
<mark>0</mark> D/ 0.	Instant re	an a	防 Instar			10.01	/2023, 9:07 PM to SQLSRV-01	
	Restore c	database 🔸			Available F	estore F	Period	
	Export ba	les 🔸			Database F Primary datab E:\MSSQL 201	ase file	5.MSSQLSERVER\MSSQL\DATA\DA	TA_01.mdf
					E:\MSSQL 201 E:\MSSQL 201	AMSSQL1 MSSQL1 MSSQL1	log files 5.MSSQLSERVER\MSSQL\LOGS\DA 5.MSSQLSERVER\MSSQL\DATA\DA 5.MSSQLSERVER\MSSQL\DATA\DA 5.MSSQLSERVER\MSSQL\DATA\DA	TA_02.ndf TA_03.ndf

5. In the Instant Recovery Wizard specify the switchover type. This can either be automatically with minimal downtime, manually, or at a specified time. Then click the **Recover** button to begin the

	1	Instant Recovery Wizard
Specify database	switchover s	scheduling options
Specify switchover typ	pe:	
Auto		
Switchover will be	e performed autor	matically with minimal possible downtime once the database is
ready.		
🔘 Manual		
Switchover can be	e performed manı	ually at any point in time after the database is ready.
Scheduled at:	1/10/	/2023 10:16 PM
 		Back Recover Cancel Ored from Veeam Explorer. Ex of less than a day ago (5407 PM Tuesday 1/10/2022) - Vesam Explorer for Microsoft SQL Server
Home Instant Recovery		red from Veeam Explorer.
Mone Instant Recovery		ared from Veeam Explorer.
Mane Instant Recovery	sql_erv_widd_1 as	ared from Veeam Explorer.
Home Instant Recovery	Instant Recovery Info Status SQL Seven	ered from Veeam Explorer. es of less than a day ago (807 PM Tuesdey 1/10/2023) - Veeam Explorer for Microsoft SQL Server Starting (restored) SQL SRV.01
Hone Instant Recovery	sal_en_okkd_1 as Instant Recovery Info Status	ared from Veeam Explorer. as of less than a day age (907 PM Tuesday 1/10/2023) - Veeam Explorer for Microsoft SQL Server Starting (restored)
Home Instant Recovery Control Control Control Instant Recovery Instant Recovery (1) DATA_01 SSR-01 SSR-01	Instant Recovery Info Status SQL Seven Target name: Target point in time Redore point:	starting (resorced)_ Starting
Hone Instant Recovery	Instant Recovery Info Sens SGI Seven Target name Target point in time:	starting (restored)
Home Instant Recovery	Instant Recovery Info Status SQL Seven Target name: Target point in time Redore point:	starting (resorced)_ Starting
Home Instant Recovery	Instant Recovery Info Sens SGL Seven Target name Target point in time Restore point Switchover mode	starting (resorced)_ Starting
Home Instant Recovery	Instant Recovery Info Status SQL Server: Target name: Target point infine Rectore point Softichorer mode: Database Files Status Pinnay ddatase file	ex cel feas shan a day age (807 PM Tuesday 1/10/2023) - Veeam Explorer for Microsoft SQL Server * cel feas shan a day age (807 PM Tuesday 1/10/2023) - Veeam Explorer for Microsoft SQL Server * Starting (restored)_ SQLSRV-01 DATA_01 * Un2/2023 S07 PM * sqLsrv_wild_1 Auto Persistent
Home Instant Recovery	Instant Recovery Info Satas SQL Sevee Target came Target point in time Redore point Switchover mode Database Files Sata Pimary database file EUMSSQL 2019/MSSQL 155/MS	st of less than a day ago (XX7 PM Tuesday 1/10/2023) - Veeam Explorer for Microsoft SOL Server st of less than a day ago (XX7 PM Tuesday 1/10/2023) - Veeam Explorer for Microsoft SOL Server st of less than a day ago (XX7 PM Tuesday 1/10/2023) - Veeam Explorer for Microsoft SOL Server st of less than a day ago (XX7 PM Tuesday 1/10/2023) - Veeam Explorer for Microsoft SOL Server st of less than a day ago (XX7 PM Tuesday 1/10/2023) - Veeam Explorer for Microsoft SOL Server st of less than a day ago (XX7 PM Tuesday 1/10/2023) - Veeam Explorer for Microsoft SOL Server st of less than a day ago (XX7 PM Tuesday 1/10/2023) - Veeam Explorer for Microsoft SOL Server st of less than a day ago (XX7 PM Tuesday 1/10/2023) - Veeam Explorer for Microsoft SOL Server st of less than a day ago (XX7 PM Tuesday 1/10/2023) - Veeam Explorer for Microsoft SOL Server st of less than a day ago (XX7 PM Tuesday 1/10/2023) - Veeam Explorer for Microsoft SOL Server st of less than a day ago (XX7 PM Tuesday 1/10/2023) - Veeam Explorer for Microsoft SOL Server st of less than a day ago (XX7 PM Tuesday 1/10/2023) - Veeam Explorer for Microsoft SOL Server st of less than a day ago (XX7 PM Tuesday 1/10/2023) - Veeam Explorer for Microsoft SOL Server st of less than a day ago (XX7 PM Tuesday 1/10/2023) - Veeam Explorer for Microsoft SOL Server st of less than a day ago (XX7 PM Tuesday 1/10/2023) - Veeam Explorer for Microsoft SOL Server st of less than a day ago (XX7 PM Tuesday 1/10/2023) - Veeam Explorer for Microsoft SOL Server st of less than a day ago (XX7 PM Tuesday 1/10/2023) - Veeam Explorer for Microsoft SOL Server st of less than a day ago (XX7 PM Tuesday 1/10/2023) - Veeam Explorer for Microsoft SOL Server st of less than a day ago (XX7 PM Tuesday 1/10/2023) - Veeam Explorer for Microsoft SOL Server st of less than a day ago (XX7 PM Tuesday 1/10/2023) - Veeam Explorer for Microsoft SOL Server st of less than a day ago (XX7 PM Tuesday 1/10/2023) - Veeam Explorer for Microsoft SOL Server st of less than a day ago (XX7
Home Instant Recovery	Instant Recovery Info Sense SQL Seven SQL Seven Target same Target point in time Recover mode Database Files Sets Database Files Sata Pinnay diabase file EVMSSQL 2019/MSSQL SMS EVMSSQL 2019/MSSQL SMS EVMSSQL 2019/MSSQL SMS	st of less than a day ago (XX7 PM Tuesday 1/10/2023) - Veeam Explorer for Microsoft SOL Server st of less than a day ago (XX7 PM Tuesday 1/10/2023) - Veeam Explorer for Microsoft SOL Server st of less than a day ago (XX7 PM Tuesday 1/10/2023) - Veeam Explorer for Microsoft SOL Server st of less than a day ago (XX7 PM Tuesday 1/10/2023) - Veeam Explorer for Microsoft SOL Server st of less than a day ago (XX7 PM Tuesday 1/10/2023) - Veeam Explorer for Microsoft SOL Server st of less than a day ago (XX7 PM Tuesday 1/10/2023) - Veeam Explorer for Microsoft SOL Server st of less than a day ago (XX7 PM Tuesday 1/10/2023) - Veeam Explorer for Microsoft SOL Server st of less than a day ago (XX7 PM Tuesday 1/10/2023) - Veeam Explorer for Microsoft SOL Server st of less than a day ago (XX7 PM Tuesday 1/10/2023) - Veeam Explorer for Microsoft SOL Server st of less than a day ago (XX7 PM Tuesday 1/10/2023) - Veeam Explorer for Microsoft SOL Server st of less than a day ago (XX7 PM Tuesday 1/10/2023) - Veeam Explorer for Microsoft SOL Server st of less than a day ago (XX7 PM Tuesday 1/10/2023) - Veeam Explorer for Microsoft SOL Server st of less than a day ago (XX7 PM Tuesday 1/10/2023) - Veeam Explorer for Microsoft SOL Server st of less than a day ago (XX7 PM Tuesday 1/10/2023) - Veeam Explorer for Microsoft SOL Server st of less than a day ago (XX7 PM Tuesday 1/10/2023) - Veeam Explorer for Microsoft SOL Server st of less than a day ago (XX7 PM Tuesday 1/10/2023) - Veeam Explorer for Microsoft SOL Server st of less than a day ago (XX7 PM Tuesday 1/10/2023) - Veeam Explorer for Microsoft SOL Server st of less than a day ago (XX7 PM Tuesday 1/10/2023) - Veeam Explorer for Microsoft SOL Server st of less than a day ago (XX7 PM Tuesday 1/10/2023) - Veeam Explorer for Microsoft SOL Server st of less than a day ago (XX7 PM Tuesday 1/10/2023) - Veeam Explorer for Microsoft SOL Server st of less than a day ago (XX7 PM Tuesday 1/10/2023) - Veeam Explorer for Microsoft SOL Server st of less than a day ago (XX7
Home Instant Recovery	Instant Recovery Info Satus SGL Seven Target name Target point in time Retore point Satus Satus Database Files Satus Pinnary database file E-MSSQL 2019/MSSQL 55MS E-MSSQL 2019/MSSQL 55MS E-MSSQL 2019/MSSQL 55MS E-MSSQL 2019/MSSQL 55MS E-MSSQL 2019/MSSQL 55MS	ered from Veeam Explorer. at of less than a day age (807 PM Tuesday 1/10/2023) - Veeam Explorer for Microsoft SQL Server at of less than a day age (807 PM Tuesday 1/10/2023) - Veeam Explorer for Microsoft SQL Server scalary age (setored) SQL SRV: Mill SQL SRV: Mill (1 Auto Perioderat Second SQL MATATATA, 01 and price.
Home Instant Recovery	Instant Recovery Info Setue Setue Setsee Setsee Setsee Insysteme Target point Setschover mode Database Files Setue Primay detabase file EVMSSQL 2019/MSSQL15MS EVMSSQL 2019/MSSQL15MS EVMSSQL 2019/MSSQL15MS EVMSSQL 2019/MSSQL15MS	And Constant and Ange and A
Home Instant Recovery	Instant Recovery Info Satus Status Status Status Status Status Networe mode Database Files Satus Database Files Satus Pinnay database file EVMSSQL 2019/MSSQL15MS EVMSSQL 2019/MSSQL15MS EVMSSQL 2019/MSSQL15MS EVMSSQL 2019/MSSQL15MS EVMSSQL 2019/MSSQL15MS EVMSSQL 2019/MSSQL15MS EVMSSQL 2019/MSSQL15MS EVMSSQL 2019/MSSQL15MS EVMSSQL 2019/MSSQL15MS	And Constant and Ange and A
Home Instant Recovery	Instant Recovery Info Setue SQL Seven SQL Seven Target name Target poset in time Recover point Settchover mode Database Files Setue Pinnary database file E-MSSQL 2019/MSSQL ISMS E-MSSQL 2019/MSSQL ISMS E-MSSQL 2019/MSSQL ISMS E-MSSQL 2019/MSSQL ISMS E-MSSQL 2019/MSSQL ISMS E-MSSQL 2019/MSSQL ISMS E-MSSQL 2019/MSSQL ISMS	ex of Vess share a day ago (307 PM Tuesday 1/10/2021) - Vesam Explorer for Microsoft SOL Serve:
Home Instant Recovery	Instant Recovery Info Satus SQL Seven Target name Target point in time Redore point Switchover mode Database Files Satus Primary database file EVMSQL 2019/MSQL 15MS EVMSQL 2019/MSQL 15MS	ex of Vess share a day ago (307 PM Tuesday 1/10/2021) - Vesam Explorer for Microsoft SOL Serve:

For more detailed information on performing SQL Server restore operations with Veeam Explorer refer to the Microsoft SQL Server section in the Veeam Explorers User Guide.

Restore Oracle databases with Veeam Explorer

Veeam Explorer for Oracle database provides the ability to perform a standard Oracle database restore or an uninterrupted restore using Instant Recovery. It also supports publishing databases for fast access, recovery of Data Guard databases and restores from RMAN backups.

For more detailed information on performing Oracle database restore operations with Veeam Explorer refer to the Oracle section in the Veeam Explorers User Guide.

In this section an Oracle database restore to a different server is covered using Veeam Explorer.

1. In the Veeam Backup and Replication console, navigate to the list of Oracle backups, right click on a server and select **Restore application items** and then **Oracle databases...**.

Backup Tools E - Home: Backup			Veeam Backup and Replication
Instant Instant Disk Entire Virtual VM Guest Application lecovery Recovery VM Disk Files Files * Inters * Restore	Amazon Microsoft Google EC2 Azure laas CEE Restore to Cloud		
lome	Q Type in an object name to search for	×	
The Jobs	Job Name 1	Creation Time Restore Po	ints Repository
호텔 Backup	Oracle Backups	1/20/2023 2:24 PM	Repository - Veeam Serve
Fel Backups	ara_srv_01	1/20/2023 6:00 PM 6	
Disk	ara_srv_02	1/20/2023 6:02 PM .4	
Last 24 Hours	ora_sry Instant recovery SQL Serve	* 20/2023 6:01 PM 5	
😰 Success	 SQL Servet III Instant recovery Instant disk recovery 	10/2023 9:05 PM	Repository - Veeam Serve
Warning Warning			
📸 Failed	Restore entire VM		
	Restore virtual disks		
	Restore VM files		
	Restore guest files	•	
	Restore application iter	ns → Fa Oracle databases	
	Restore to Amazon EC2	5	
	Restore to Microsoft Az		
	Restore to Google CE		
	Export backup		
	and		

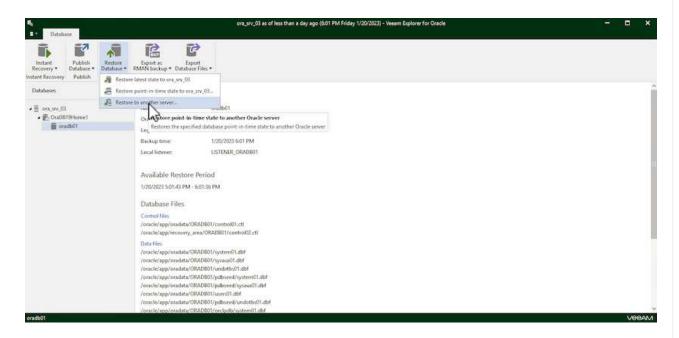
2. In the Oracle Database Restore Wizard select a restore point from the list and click on **Next**.

Restore Point Reason	VM name: ora_srv_03 VM size: 38.5 GB Restore from the latest available backup	Original ho	ost: vcenter.sddc-44-235-223-88.vm
Summary	O Restore from this restore point:		
	Created	Туре	Backup
	less than a day ago (6:01 PM Friday 1/ Iess than a day ago (5:01 PM Friday 1/	Increment	Oracle Backups
	(5) less than a day ago (3:01 PM Priday 1/ (5) less than a day ago (4:02 PM Friday 1/		Oracle Backups Oracle Backups
	Iss than a day ago (3:47 PM Friday 1/		Oracle Backups
	(less than a day ago (2:47 PM Friday 1/		Oracle Backups
	رق less than a day ago (2:47 PM Friday 1/	Full	Oracle Backups

3. Enter a **Restore reason** if desired and then, on the Summary page, click on the **Browse** button to launch Veeam Explorer for Oracle.

ry: ry: me: ora_srv_03 : point: ent: ora_srv_03 le					where you will be ab
ry: me: ora_srv_03 : point:					where you will be ab
me: ora_srv_03	:ss than a day	y ago (6:01 PM F	riday 1/20/202		
point:	ess than a day	y ago (6:01 PM F	riday 1/20/202		
ent: ora_srv_03 le	ess than a day	y ago (6:01 PM F	riday 1/20/202		
			11003 17 207 202.	3)	
		< Previous	Next>	Brows	se Cancel
			< Previous	< Previous	< Previous Next > Brows

4. In Veeam Explorer expand the list of database instances, click on the database to be restored and then from the **Restore Database** drop-down menu at the top select **Restore to another server...**



5. In the Restore Wizard specify the restore point to restore from and click Next.

Specify restore point				
Specify point in time you wa	nt to restore the data	base to:		
Restore to the point in till	me of the selected in	nage-level backup		
Restore to a specific poir	nt in time (requires re	do log backups)		
5:01 PM 1/20/2023				6:01 PM 1/20/2023
	Friday, Jar	uary 20, 2023 6:01	PM	
Perform restore to the	ne specific transactio	n		
	w major database tra nent in time right be			and restore the
🦺 To enable this fu	inctionality, specify t	he staging Oracle s	erver under Men	u > Options.

6. Specify the target server the database will be restored to and the account credentials and click **Next**.

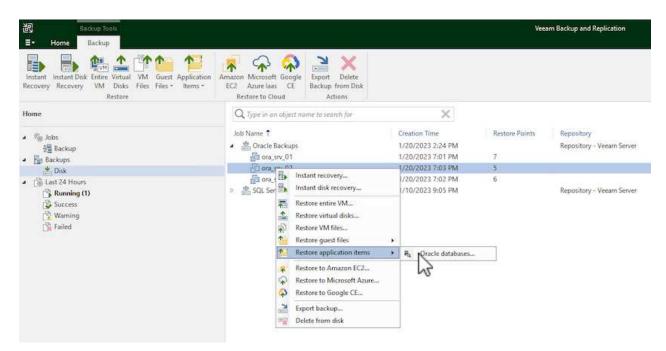
Advanced
1
Browse
Cancel

		 125
Control files		^
/oracle/app/oradata/oradb01/control01.ctl		_
/oracle/app/recovery_area/oradb01/contro	l02.ctl	11
Data files		
/oracle/app/oradata/oradb01/system01.db	f	
/oracle/app/oradata/oradb01/sysaux01.dbf		
/oracle/app/oradata/oradb01/undotbs01.d	bf	
/oracle/app/oradata/oradb01/pdbseed/sys		
/oracle/app/oradata/oradb01/pdbseed/sys		
/oracle/app/oradata/oradb01/users01.dbf		~

222

In this section a database is published to an alternate server for fast access without launching a full restore.

1. In the Veeam Backup and Replication console, navigate to the list of Oracle backups, right click on a server and select **Restore application items** and then **Oracle databases...**.



2. In the Oracle Database Restore Wizard select a restore point from the list and click on Next.

Restore Point Reason Summary	VM name: ora_srv_02 VM size: 38.1 GB Restore from the latest available backup Restore from this restore point:	Original ho	ost: vcenter.sddc-44-235-223-88.vm.
	Created	Туре	Backup
	🕒 less than a day ago (7:03 PM Friday 1/	Increment	Oracle Backups
	🕑 less than a day ago (6:02 PM Friday 1/	Increment	Oracle Backups
	less than a day ago (5:02 PM Friday 1/		Oracle Backups
	Iess than a day ago (4:03 PM Friday 1/ Iess than a day ago (3:49 PM Friday 1/	Increment Full	Oracle Backups Oracle Backups

- 3. Enter a **Restore reason** if desired and then, on the Summary page, click on the **Browse** button to launch Veeam Explorer for Oracle.
- 4. In Veeam Explorer expand the list of database instances, click on the database to be restored and then from the **Publish Database** drop-down menu at the top select **Publish to another server...**

Databa	se					
Instant Recovery •	Publish Database •	Restore Database •	Export a RMAN bac	IS	Export Database Files •	
nstant Recovery	Publis	h to another s	erver	Expo	rt	
Databases		1	Datab	ase In	fo	
a ora_srv_02			Name:		,	oradb01
OraDB			Oracle S	SID:		oradb01
ora 🖉	db01		Log mo	de:		ARCHIVELOG
			Backup	time:		1/20/2023 7:03 PM
			Local lis	tener:	1	LISTENER_ORADB01

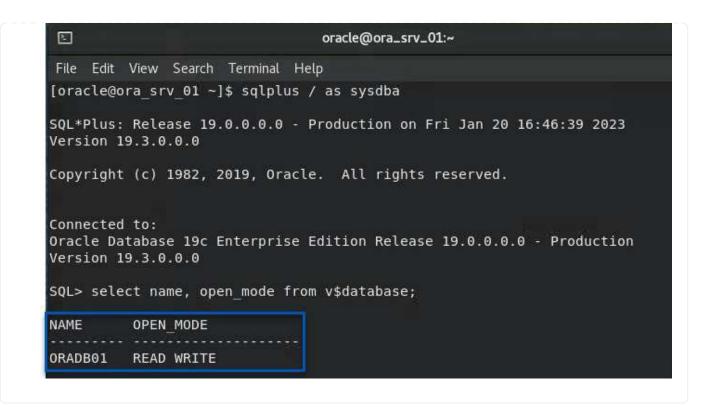
- 5. In the Publish wizard, specify the restore point at which to publish the database from and click **Next**.
- 6. Finally, specify the target linux file system location and click on **Publish** to begin the restore process.

	ocation	
lestore to a different lo	ocation:	
Dracle Home:	/oracle/app/product/19c	Browse
Global Database Name	oradb01.demozone.com	
Dracle SID:	oradb01	

7. Once the publish has completed log into the target server and run the following commands to ensure the database is running:

oracle@ora_srv_01> sqlplus / as sysdba

SQL> select name, open_mode from v\$database;



Conclusion

VMware Cloud is a powerful platform for running business-critical applications and storing sensitive data. A secure data protection solution is essential for businesses that rely on VMware Cloud to ensure business continuity and help protect against cyber threats and data loss. By choosing a reliable and robust data protection solution, businesses can be confident that their critical data is safe and secure, no matter what.

The use case presented in this documentation focuses on proven data protection technologies that highlight the integration between NetApp, VMware, and Veeam. FSx for ONTAP is supported as supplemental NFS datastores for VMware Cloud in AWS and is used for all virtual machine and application data. Veeam Backup & Replication is a comprehensive data protection solution designed to help businesses improve, automate, and streamline their backup and recovery processes. Veeam is used in conjunction with iSCSI backup target volumes, hosted on FSx for ONTAP, to provide a secure and easy to manage data protection solution for application data residing in VMware Cloud.

Additional Information

To learn more about the technologies presented in this solution refer to the following additional information.

- FSx for ONTAP User Guide
- Veeam Help Center Technical Documentation
- VMware Cloud on AWS Support. Considerations and Limitations

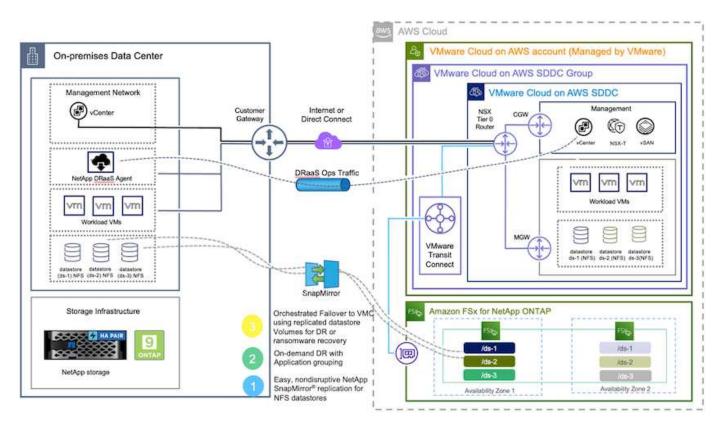
TR-4955: Disaster Recovery with FSx for ONTAP and VMC (AWS VMware Cloud)

Disaster Recovery Orchestrator (DRO; a scripted solution with UI) can be used to seamlessly recover workloads replicated from on-premises to FSx for ONTAP. DRO automates the recovery from the SnapMirror level, through VM registration to VMC, to network mappings directly on NSX-T. This feature is included with all VMC environments.

Overview

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). With NetApp SnapMirror technology, on-premises VMware workloads can be replicated to FSx for ONTAP running in AWS.

Disaster Recovery Orchestrator (DRO; a scripted solution with UI) can be used to seamlessly recover workloads replicated from on-premises to FSx for ONTAP. DRO automates the recovery from the SnapMirror level, through VM registration to VMC, to network mappings directly on NSX-T. This feature is included with all VMC environments.



Getting started

Deploy and configure VMware Cloud on AWS

VMware Cloud on AWS provides a cloud-native experience for VMware-based workloads in the AWS ecosystem. Each VMware Software-Defined Data Center (SDDC) runs in an Amazon Virtual Private Cloud (VPC) and provides a full VMware stack (including vCenter Server), NSX-T software-defined networking, vSAN software-defined storage, and one or more ESXi hosts that provide compute and storage resources to the workloads. To configure a VMC environment on AWS, follow the steps at this link. A pilot-light cluster can also be used for DR purposes.



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

Provision and configure FSx for ONTAP

Amazon FSx for NetApp ONTAP is a fully managed service that provides highly reliable, scalable, high-

performing, and feature-rich file storage built on the popular NetApp ONTAP file system. Follow the steps at this link to provision and configure FSx for ONTAP.

Deploy and configure SnapMirror to FSx for ONTAP

The next step is to use NetApp BlueXP and discover the provisioned FSx for ONTAP on AWS instance and replicate the desired datastore volumes from an on-premises environment to FSx for ONTAP with the appropriate frequency and NetApp Snapshot copy retention:

NetApp BlueXP	Account Y Workspace nimoleb nimbybridieb	
Canvas My Working Environments	My Opportunities	🖽 Go to Tabular View
+ Add Working Environment	Enable Services	(i)
PSA TOP ONTAP 7 13.01 THE	On-Premises ONTAP 131.27 TIB	DETAILS
at Votumes Capacity aws	Capacity	On-Premises ONTAP
		SERVICES
DemoFSxN FSx.For ONTAP	ANF Azumi NotApp Files	Blackup and recovery Enable • 1
5 Capacity aws	() Failed	Copy & sync 1,57 Till (1) # On Data Synced
		Tiering Loading.
Azure Blob Storage	Amazon 53	Classification Enable 3
Bhorager Accounts	Buckets aws -++	Enter Working Environment

Follow the steps in this link to configure BlueXP. You can also use the NetApp ONTAP CLI to schedule replication following this link.



A SnapMirror relationship is a prerequisite and must be created beforehand.

DRO installation

To get started with DRO, use the Ubuntu operating system on a designated EC2 instance or virtual machine to make sure you meet the prerequisites. Then install the package.

Prerequisites

- Make sure that connectivity to the source and destination vCenter and storage systems exists.
- DNS resolution should be in place if you are using DNS names. Otherwise, you should use IP addresses for the vCenter and storage systems.
- Create a user with root permissions. You can also use sudo with an EC2 instance.

OS requirements

- · Ubuntu 20.04 (LTS) with minimum of 2GB and 4 vCPUs
- The following packages must be installed on the designated agent VM:

- Docker
- Docker-compose
- ∘ Jq

Change permissions on docker.sock: sudo chmod 666 /var/run/docker.sock.



The deploy.sh script executes all the required prerequisites.

Install the package

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

git clone https://github.com/NetApp/DRO-AWS.git



The agent can be installed on-premises or within an AWS VPC.

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

tar xvf DRO-prereq.tar

3. Navigate to the directory and run the deploy script as follows:

```
sudo sh deploy.sh
```

4. Access the UI using:

```
https://<host-ip-address>
```

with the following default credentials:

Username: admin Password: admin

The password can be changed using the "Change Password" option.

NetApp	FSX _m
Disaster Recovery Orchestrator Lingung Industrie with DDP Username	I CAN'
Password	
Login	

DRO configuration

After FSx for ONTAP and VMC have been configured properly, you can begin configuring DRO to automate the recovery of on-premises workloads to VMC by using the read-only SnapMirror copies on FSx for ONTAP.

NetApp recommends deploying the DRO agent in AWS and also to the same VPC where FSx for ONTAP is deployed (it can be peer connected too), so that the DRO agent can communicate through the network with your on-premises components as well as with the FSx for ONTAP and VMC resources.

The first step is to discover and add the on-premises and cloud resources (both vCenter and storage) to DRO. Open DRO in a supported browser and use the default username and password (admin/admin) and Add Sites. Sites can also be added using the Discover option. Add the following platforms:

- On-premises
 - On-premises vCenter
 - ONTAP storage system
- Cloud
 - VMC vCenter
 - FSx for ONTAP

NetApp Disaster Recovery Orchestra	tor 💊 Dashboard Discover	Resource Groups Replication Plans Job Monitoring	≜ ∲* @ * @ *
Add New Site	1 Site Type 2 S	ite Details ③ vCenter Details ④ Storage Details	×
		Site Type	
	s	ource Destination	
		Continue	

C 2 Sites	2 vCenters	B 2 Storages	Site Type	(G) 1 Destination	Site Location	Cloud
2 Sites			Source		Unrien	Q O Add New Site
Site Name Cloud	C Site Type =	Location 😓 vCenter	r ¢ Storage ¢ VM	M List Discovery : • 44.23		⊙ Success ····
On Prem	Source	On Prem 1	1	View VM List • 172.21	.253.160	⊘ Success ····

Once added, DRO performs automatic discovery and displays the VMs that have corresponding SnapMirror replicas from the source storage to FSx for ONTAP. DRO automatically detects the networks and portgroups used by the VMs and populates them.

Back		VM List Site: On Prem J vCenter: 172.21	1253.160		
6 1	0 Hastories	219 Virtual Machines	VM Protection 3 Protected	0 Unpro	216 Instand
38 vive				٩	Create Resource Group
VM Name	C VM Status	₩ VM State (1)	⊕ DetaStore	C CPU	© Memory (MB) ©
#300-vcsa02	10 Not Protected	() Powered On	A300_NF5_D504	16	65538
PFSense	0 Not Protected	() Powered On	A300_NFS_DS04	4	8192
		() Powered On	A300_NFS_DS04	4	16384
PFSense260	0 Not Protected				
	Not Protected Not Protected	() Powered On	A300_NFS_DS04	4	8192
PFSense260		() Powered On () Powered On	A300_NFS_D504	4	8192

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

Resource groupings

After the platforms have been added, you can 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, complete the following steps:

- 1. Access Resource Groups, and click Create New Resource Group.
- 2. Under **New resource group**, select the source site from the dropdown and click **Create**.
- 3. Provide Resource Group Details and click Continue.
- 4. Select the appropriate VMs using the search option.
- 5. Select the boot order and boot delay (secs) for the selected VMs. Set the order of the power-on sequence by selecting each VM and setting up the priority for it. Three is the default value for all VMs.

Options are as follows:

- 1 The first virtual machine to power on
- 3 Default
- 5 The last virtual machine to power on
- 6. Click Create Resource Group.

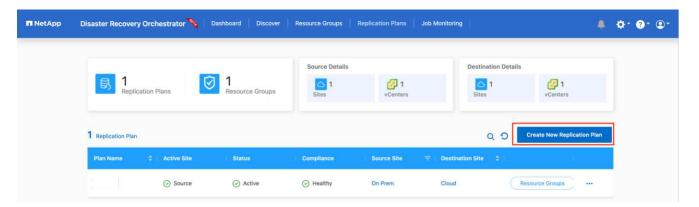
NetApp	Disaster Recovery Orchestrator 💊	Dashboard Discover	Resource Groups Replication Plans	Job Monitoring	å ¢· 0·
	Resource Group		1 P	1 3 vCenter Virtu	al Machines
	1 Resource Group			Q D Create)	lew Resource Group
	Resource Group Name	C Site Name		😇 💿 VM List	36 - C
	DemoRG1	On Prem	172.21.253.160	View VM List)

Replication plans

You need a plan to recover applications in the event of a disaster. Select the source and destination vCenter platforms from the drop down and pick the resource groups to be included in this plan, along with the grouping of how applications should be restored and powered on (for example, domain controllers, then tier-1, then tier-2, and so on). Such plans are sometimes also called blueprints. 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. Access Replication Plans, and click Create New Replication Plan.



2. Under **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.

Replication Plan Details Plan Name • Recovery Mapping Source Site • Select Source Site • Source vCenter • Select Source vCenter • Select Source vCenter • Select Source vCenter •	Create New Replication Plan	Replication Plan and Site Details Select Resource	Groups (3) Set Execution Order (4) Set VM D	Details
Recovery Mapping Source Site Destination Site Select Source Site Select Destination Site Source vCenter Destination vCenter		Replication	Plan Details	
Source Site Destination Site Select Source Site Select Destination Site Source vCenter Destination vCenter		Plan Name		0
Source Site Destination Site Select Source Site Select Destination Site Source vCenter Destination vCenter				
Select Source Site Select Destination Site Source vCenter Destination vCenter		Recovery	/ Mapping	
Source vCenter Destination vCenter				
		Pre-requisite - You must configure SnapMirror relat	ionships between the source site and target site to	×
Pre-requisite - You must configure SnapMirror relationships between the source site and target site to ×		Create successful replication plan		

3. After Recovery mapping is completed, select the cluster mapping.

Create New Replication Plan	Replication Plan and Site Details	2) Select Resource	Groups 3 Set Execution Order	Set VM Details	
		Replication	Plan Details		
	Plan Name			0	
	DemoRP				
		Recovery	/ Mapping		
	Source Site	0	Destination Site	0	
	On Prem	*	Cloud		
	Source vCenter	0	Destination vCenter	0	
	172.21.253.160	*	44.235.223.88		
		Cluster	Mapping		
	Source Site Resource	O Destinati	on Site Resource		
	TempCluster	· .	Cluster-1 ~	Add	
	Source Resource	Destination	Resource		
	A300-Cluster01	Cluster-1		Delete	

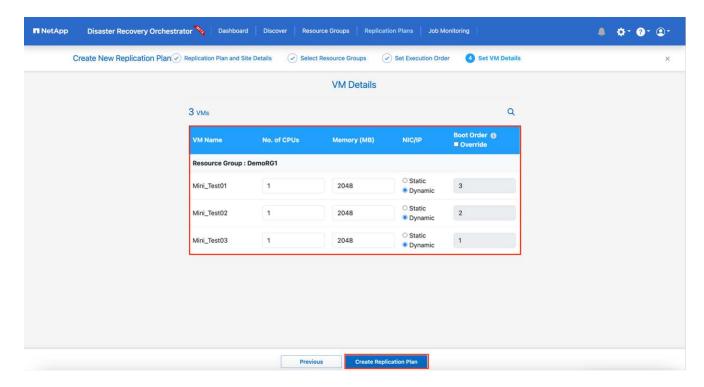
- 4. Select Resource Group Details and click Continue.
- 5. Set the execution order for the resource group. This option enables you to select the sequence of operations when multiple resource groups exist.
- 6. After you are done, select the network mapping to the appropriate segment. The segments should already be provisioned within VMC, so select the appropriate segment to map the VM.
- 7. Based on the selection of VMs, datastore mappings are automatically selected.



SnapMirror is at the volume level. Therefore, all VMs are replicated to the replication destination. Make sure to select all VMs that are part of the datastore. If they are not selected, only the VMs that are part of the replication plan are processed.

Create New Replication Plan	Replication Plan and Site Details	Select Resource Groups Set Execution Order (4) Set VM Da	Details
		Replication Plan Details	
		Select Execution Order	
	Resource Group Name	Execution Order 💿	
	DemoRG1	3	
	No more	Network Mapping Source/Destination network resources available for mapping	
	No more	12212/2010/01/2017/2017	
	Source Resource	e Source/Destination network resources available for mapping Destination Resource	
	Provide and the second second	P Source/Destination network resources available for mapping	
	Source Resource	e Source/Destination network resources available for mapping Destination Resource	
	Source Resource	e Source/Destination network resources available for mapping Destination Resource sddc-cgw-network-1 Delete	

8. Under the VM details, you can optionally resize the VM's CPU and RAM parameters; this can be very helpful when recovering large environments to smaller target clusters or for conducting DR tests without having to provision a one-to-one physical VMware infrastructure. Also, you can modify the boot order and boot delay (seconds) for all the selected VMs across the resource groups. There is an additional option to modify the boot order if there are any changes required from those selected during the resource-group boot-order selection. By default, the boot order selected during resource-group selection is used; however, any modifications can be performed at this stage.



9. Click Create Replication Plan.

			Source Details		Destination Details	Destination Details	
B 2 Replica	ation Plans	7 1 Resource Groups	Sites 1	Centers	Control 1 Sites	Centers	
					_		
2 Replication Plans					0.0	Create New Replication Plan	
2 Replication Plans	Active Site	Status	Compliance	Source Site	Q O	Create New Replication Plan	

After the replication plan is created, the failover option, the test-failover option, or the migrate option can be exercised depending on the requirements. During the failover and test-failover options, the most recent SnapMirror Snapshot copy is used, or a specific Snapshot copy can be selected from a point-in-time Snapshot copy (per the retention policy of SnapMirror). The point-in-time option can be very helpful if you are facing a corruption event like ransomware, where the most recent replicas are already compromised or encrypted. DRO shows all available points in time. To trigger failover or test failover with the configuration specified in the replication plan, you can click **Failover** or **Test failover**.

n NetApp	Disaster Recovery	Orchestrator 🔌 🛛	Dashboard Discover	Resource Groups	Replication Plans	Job Monitoring		.¢. Ø.	•
	B 2 Replica	ition Plans	1 Resource Groups	Source Details	Centers	Destination 1 Sites	n Details		
	2 Replication Plans	9				٩	Create New Replication	Plan	
	Plan Name	C Active Site	Status	Compliance	Source Site	😇 🛛 Destination Site 😂			
	DemoRP	 Source Source 	 Active Active 	 Healthy Healthy 	On Prem	Cloud	Resource Groups Plan Details Resource	•	
							Edit Plan Failover		
							Test Failover		
							Migrate Run Compliance	ce	
							Delete Plan		
	/er Deta e Snapsh	ils ot Details	7						>
	latest snap								
		snapshot ()							
Jele									
Jele									

The replication plan can be monitored in the task menu:

■ NetApp	Disaster Rec	overy Orchestrator Dashboard Discover Resource Groups Replication Plans Job Monito Failover Steps Replication Plan: DemoRP	pring	≜ ☆· @· @·
	~	Breaking SnapMirror relationships (in parallel)	Success	11.3 Seconds 🕢
	~	Mounting volumes and creating datastores (in parallel)	Success	34.7 Seconds 🛈
	~	Registering VMs (in parallel)	⊘ Success	13.2 Seconds 🕕
	~	Powering on VMs in protection group - DemoRG1 - in target	Success	95.8 Seconds 🕕
	~	Updating replication status	Success	0.5 Seconds ()

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

	2 Reserve Chapter	1 Automor Pie	219	Provented UNA	0 214 Uptiment	
Exchangements Contract Reservences Contract Reservences Contrac	B z Stronge freedommente De 22 Stronger	Septing Canada Define 112 21 20 100 112 21 20 100 112 21 20 100)(0aut 41252218 10-0-0 100	intention two ()	

Failback can be triggered at the replication-plan level. For a test failover, the tear-down option can be used to roll back the changes and remove the FlexClone relationship. Failback related to failover is a two-step process. Select the replication plan and select **Reverse data sync**.

Ref	plication Plans	1 Resource Groups	Source Details	vCenters		tination Details	P 1 vCenters	
2 Replication						4.0	ite New Replication Plan	
Plan Name DemoRP	Active Site O Destination	Status Running In Failover	Compliance	On Prem	Cloud		ce Groups 💮	
DemoRP	 Source 	 Active 	Healthy	On Prem	Cloud	Resource	Plan Details Ce Reverse Data Sync	
							Fallback	
tApp Disaster Recov	rery Orchestrator 🦄	Dashboard Discover	Resource Groups	Replication Plans	Job Monitoring		Fallback	¢- 0-
tApp Disaster Recov Back	rery Orchestrator 🗞	Dashboard Discover	Resource Groups Reverse Data Replication F	a Sync Steps	Job Monitoring		Fallback	¢* @`

Once completed, you can trigger failback to move back to original production site.

			Source Details		Destination Details	Destination Details		
B 2 Repl	ication Plans	Resource Groups	Sites 1	Centers	Sites 1	Centers 1		
2 Replication Pla	ins				Q 0	Create New Replication Pla		
2 Replication Pla	C Active Site	Status	Compliance	Source Site 👳		Create New Replication Pla		
			Compliance	Source Site 👳	Destination Site	Create New Replication Pl		

NetApp	Disaster Reco	overy Orchestrator 🗞 Dashboard Discover Resource Groups Replication Plans Job Monitoring		≜ ☆· @· ©·
	Back	Failback Steps Replication Plan: DemoRP		
	~	Powering off VMs in protection group - DemoRG1 - in target	C In progress	- 0
	~	Unregistering VMs in target (in parallel)	✓ Initialized	- @
	~	Unmounting volumes in target (in parallel)	✓ Initialized	- @
	~	Breaking reverse SnapMirror relationships (in parallel)	 Initialized 	- ©
	~	Updating VM networks (in parallel)	✓ Initialized	- ©
	~	Powering on VMs in protection group - DemoRG1 - in source	✓ Initialized	- ©
	~	Deleting reverse SnapMirror relationships (in parallel)	 Initialized 	- ①
	~	Resuming SnapMirror relationships to target (in parallel)	✓ Initialized	- ©

From NetApp BlueXP, we can see that replication health has broken off for the appropriate volumes (those that were mapped to VMC as read-write volumes). During test failover, DRO does not map the destination or replica volume. Instead, it makes a FlexClone copy of the required SnapMirror (or Snapshot) instance and exposes the FlexClone instance, which does not consume additional physical capacity for FSx for ONTAP. This process makes sure that the volume is not modified and replica jobs can continue even during DR tests or triage workflows. Additionally, this process makes sure that, if errors occur or corrupted data is recovered, the recovery can be cleaned up without the risk of the replica being destroyed.

Plans Protected Unprotected Environments Immersive View () Vorteter Summary Immersive View () Vorteter Summary Immersive View () Image Environments Image Environments Image Environments Image Environments Vorteter Summary Image Environments Image Environments	Plans Protected Environments Immensive View () Venter Summary Immensive View () Image: Custers 22 Custers 22 Image: Custers 22 Image: Custers 23 Image: Custers 45	2 Sites	1	8 2	a 219	Protected VMs	0 216	
Withual Environments Big 2 Storage Environments vCenter Summary Image: 22 Clusters Image: 3 Clusters Image: 22 Clusters Image: 23 Catastores Image: 23 Clusters Image: 23 Clusters Image: 24 Clusters	Verture Z winners Verture Summary W Market W Market W Market Mark	Sites	Resource Group	Hephcabon	VMs			
Virtual Environments Storage Environments vCenter Summary Image: Clusters Image: Clusters Image: Clusters	Virtual Environments Storage Environments vCenter Summary	Environments		Topology Canvas			Immersive View ()	
Image: Solutions Image: Solutions Image: Solutions Cloud Cloud Cloud 44.235.223.88 44.235.223.88 10.480.191 Image: Solution control in the solutin the soluti	Image: Securition Jobs Image: Securition Jobs Cool Cool <t< td=""><td></td><td></td><td></td><td></td><td></td><td></td><td></td></t<>							
Image: Solutions Image: Solutions Image: Solutions Cloud Cloud Cloud 44.235.223.88 44.235.223.88 10.480.191 Image: Solution control in the solutin the soluti	Image: Securition Jobs Image: Securition Jobs Cool A Image: Securition Jobs Image: Securition Jobs Securition Plans Image: Securition Jobs Image: Securition Plans Securition Plans Image: Securition Jobs Image: Securition Plans Securition Plans	vCenter Summary			<u>}</u>	aws		
Clusters Folders 172.21.253.180 44.235.223.88 172.21.254.210 10.480.191 2.3 2.45 Notworks	Clusters Folders 172.21.253.180 44.235.223.88 23 245 10.49.0.191 Execution Jobs Replication Plans 0 3 10		- 22			9		
Datastores Notworks	Datastores Notworks Execution Jobs Replication Plans 3 Replication Plan	Clusters	Folders	172.21.253.166		44.235.223.88		
Datastores Networks	Execution Jobs Replication Plans Oatastores Notworks 03 Replication Plan	a 23	o 45					
	O 3 Teplication Plan Active Site Status	Datastores	× Networks					
Execution Jobs Hepication Hans		Execution Jobs		Replication Plans				

Ransomware recovery

Recovering from ransomware can be a daunting task. Specifically, it can be hard for IT organizations to pinpoint where the safe point of return is and, once that is determined, to protect recovered workloads from reoccurring attacks from, for example, sleeping malware or vulnerable applications.

DRO addresses these concerns by enabling you to recover your system from any available point in time. You can also recover workloads to functional and yet isolated networks so that applications can function and communicate with each other in a location where they are not exposed to north-south traffic. This gives your security team a safe place to conduct forensics and make sure there is no hidden or sleeping malware.

Benefits

- Use of the efficient and resilient SnapMirror replication.
- Recovery to any available point in time with Snapshot copy retention.
- Full automation of all required steps to recover hundreds to thousands of VMs from the storage, compute, network, and application validation steps.
- Workload recovery with ONTAP FlexClone technology using a method that doesn't change the replicated volume.
 - Avoids risk of data corruption for volumes or Snapshot copies.
 - Avoids replication interruptions during DR test workflows.
 - Potential use of DR data with cloud computing resources for workflows beyond DR such as DevTest, security testing, patch or upgrade testing, and remediation testing.
- CPU and RAM optimization to help lower cloud costs by allowing recovery to smaller compute clusters.

Using Veeam Replication and FSx for ONTAP for Disaster recovery to VMware Cloud on AWS

Amazon FSx for NetApp ONTAP integration with VMware Cloud on AWS is an AWSmanaged external NFS datastore built on NetApp's ONTAP file system that can be attached to a cluster in the SDDC. It provides customers with flexible, high-performance virtualized storage infrastructure that scales independently of compute resources.

Author: Niyaz Mohamed - NetApp Solutions Engineering

Overview

For those customers looking to use VMware Cloud on AWS SDDC as the disaster recovery target, FSx for ONTAP datastores can be used to replicate data from on-premises using any validated third-party solution that provides VM replication capability. By adding FSx for ONTAP datastore, it will enable cost optimised deployment than building VMware cloud on AWS SDDC with enormous amount of ESXi hosts just to accommodate the storage.

This approach also helps customers to use pilot light cluster in VMC along with FSx for ONTAP datastores to host the VM replicas. The same process can also be extended as a migration option to VMware Cloud on AWS by gracefully failing over the replication plan.

Problem Statement

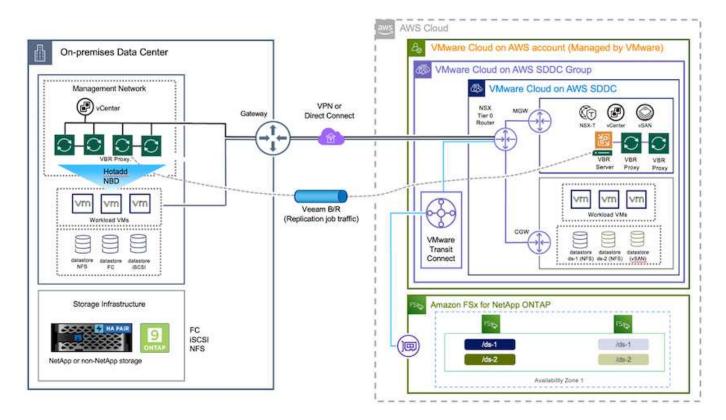
This document describes how to use FSx for ONTAP datastore and Veeam Backup and replication to set up disaster recovery for on-premises VMware VMs to VMware Cloud on AWS using the VM replication functionality.

Veeam Backup & Replication allows onsite and remote replication for disaster recovery (DR). When virtual machines are replicated, Veeam Backup & Replication creates an exact copy of the VMs in the native VMware vSphere format on the target VMware Cloud on AWS SDDC cluster and keeps the copy synchronized with the original VM.

Replication provides the best recovery time objective (RTO) values as there is a copy of a VM in the ready-tostart state. This replication mechanism ensures that the workloads can quickly start in VMware Cloud on AWS SDDC in 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, and compresses the replica traffic.

To prevent replication jobs from consuming the entire network bandwidth, WAN accelerators and network throttling rules can be put in place. The replication process in Veeam Backup & Replication is job driven which means replication is performed by configuring replication jobs. In 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. Fail over 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. In Veeam Backup & Replication, failover and failback are temporary intermediate step that should be further finalized. Veeam Backup & Replication offers multiple options to handle different disaster recovery scenarios.



Solution Deployment

High level steps

- 1. Veeam Backup and Replication software is running in on-premises environment with appropriate network connectivity.
- 2. Configure VMware Cloud on AWS, see the VMware Cloud Tech Zone article VMware Cloud on AWS integration with Amazon FSx for NetApp ONTAP Deployment Guide to deploy, configure VMware Cloud on

AWS SDDC and FSx for ONTAP as NFS datastore. (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 jobs 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 VMC and FSx for ONTAP datastores

- 1. Ensure Veeam Backup & Replication backup VM is connected to the source vCenter as well as the target VMware cloud on AWS SDDC clusters.
- 2. The backup server must be able to resolve short names and connect to source and target vCenters.
- 3. The target FSx for ONTAP 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 and during replication, Veeam Backup & Replication requests VMware vSphere to create a VM snapshot. The VM snapshot is the point-in-time copy of a VM that includes virtual disks, system state, configuration and so on. 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, select Replication Job > Virtual machine > VMware vSphere.
- 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 AWS has restricted bandwidth.
 - Select the Network remapping (for AWS VMC sites with different networks) check box if segments on VMware Cloud on AWS 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 AWS VMC site, select the Replica re-IP (for DR sites with different IP addressing scheme) check box.



4. Select the VMs that needs to be replicated to FSx for ONTAP datastore attached to VMware Cloud on AWS 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 replicated to FSx for ONTAP datastores. Click Add, then in the Add Object window select the necessary VMs or VM containers and click Add. Click Next.

Virtual Machines

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

	Name	Type	Size	^	Add
Virtual Machines	TestVeeam21	Virtual Machine	873 MB		Remove
Destination	TestVeeam22	Virtual Machine	890 MB		Nethaye
	TestVeeam23	Virtual Machine	883 MB		Total III and
Vetwork	TestVeeam24	Virtual Machine	879 MB		Exclusions
	TestVeeam25	Virtual Machine	885 MB		Source
ob Settings	TestVeeam26	Virtual Machine	883 MB		
Data Transfer	TestVeeam27	Virtual Machine	879 MB		
Jata Transfer	TestVeeam28	Virtual Machine	880 MB		🕈 Up
Suest Processing	TestVeeam29	Virtual Machine	878 MB		+ Down
j	TestVeeam30	Virtual Machine	876 MB		
Schedule	TestVeeam31	Virtual Machine	888 MB		
	TestVeeam32	Virtual Machine	881 MB		
Summary	TestVeeam33	Virtual Machine	877 MB		
	TestVeeam34	Virtual Machine	875 MB		-
	TestVeeam35	Virtual Machine	882 MB		Recalculate
	WinSQL401	Virtual Machine	20.3 GB		
	WinSQL405	Virtual Machine	24.2 GB		Total size:
	F2			*	120 GB

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

Virtual Machines Destination Resource pool: Resources Pick resource pool for selected replicas VM folder: VM folder: Vm	Vame	Host or cluster:	
Network Resources Choos Nob Settings VM folder: Choos Data Transfer vm Choos Guest Processing Datastore: Choos Schedule Veeam [5.6 TB free] Choos	/irtual Machines		Choose
Network Pick resource pool for selected replicas ob Settings VM folder: Data Transfer vm Souest Processing Pick VM folder for selected replicas Datastore:	Destination	Resource pool:	
Pick resource pool for selected replicas Nob Settings VM folder: Data Transfer Guest Processing Schedule Datastore:	Vetwork	Resources	Choose
Guest Processing Pick VM folder for selected replicas Datastore: Datastore: Choose Choose	ob Settings		
Datastore: Choose Choose Choo	Data Transfer	vm	Choose
ScheduleVeeam [5.6 TB free] Choose	Suest Processing		
Veeam [5.6 1B free]	chedule		
			Choose
Summary Pick datastore for selected virtual disks	jummary	Pick datastore for selected virtual disks	

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

Name	Network mapping:		
Virtual Machines Destination	Source network Source network VM_3508 (vDS-Switch0) Source vM_3510 (vDS-Switch0)	Target network SepSeg SegmentTemp	Add Edit
Network			Remove
Job Settings			
Data Transfer			
Guest Processing			
Schedule			
Summary			

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

Name Virtual Machines	Enable application-aware processing Detects and prepares applications for consistent backup, performs transaction logs configures the OS to perform required application restore steps upon first boot.	processing, and
Destination	Customize application handling options for individual machines and applications Guest interaction proxy:	Applications
Network	Automatic selection	Choose
lob Settings	Guest QS credentials:	
Data Transfer		Add
	Manage accounts	
Suest Processing	Customize guest OS credentials for individual machines and operating systems	Credentials
Schedule	Verify network connectivity and credentials for each machine included in the job	Test Now

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

acting Replication. CDP Backup Copy Restars Falls Initial Jobs - Policy Copy - Aile - Plan Primary folls Restars Falls - Plan Restars Falls	re Import Esport								
Name	$Q_{\rm c}$ (specified on the state τ moves to exactly	(m)	ж	T Atate					
a lighter	Name 7	Type	Chierts	Sinte	Last Run	Last Result	Mart Runt	Target	Description
Dispication a gill hepication	a ANF Japiob01 要 ANF Japiob01	Where Replication Where Replication	8	Stopped	2 days app 23 days app	Faled Second	and scheduled+	Outer1	General by VEAMBRPSR031Administrator at 2/16/202. Created by VEAMBRPSR031Administrator at 2/18/202.
So Ready So Active (1)	書 FSLAL_16VM_20230318 群 FSLAL_Replied01_20250313	Where Replication Where Replication	16	Shapped Shapped	Z days ago 6 days ago	Success Success	rect scheduled+ crut scheduled+	172.33.160.68	Overheit by VERAMBRISRVID Administrator et 1/16/202 Overheit by VERAMBRISRVID Administrator et 1/12/202
Falson Para (3) Last 24 Hours (3) Socrese (3) Falson (3) Falson									-

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

문 Home View Job					Ween Bockup a	nd Replication						- 8
Start Sup Kny Statistics Report Ede	Gene Dutile Delete											
Sob Control Details	Manage Joli											
Home	Q. Type in an object name to a	earth fur		\times								
- Se Jobs	Name	Type	Objects	Status	LestRun	Lent Result	NextRun	Target	Description	•		
38 Replication	操 AVS_Repict01	Whyare Replication	2	Stopped	19 days ago	Success	<not scheduled=""></not>	Ouster-1	Created by V	EEAMERPSRV03	Administrator at	2/16/2023 2:12 AN
e (j]] Replicas	谢 ANF,RepJob01	Weiware Replication	6	Slopped	6 days ago	Falled	<not scheduled=""></not>	Cluster-1				2/16/2023 T/27 AA
Seady	書 ISAN_Repticb01_20230313	Whyare Replication	5		3 days ago	Success	<not scheduled=""></not>	172.30.160.66				3/13/2023 2:53 AA
Failover Plans	(0) F54N 16VM4 20230316	Where Replication	16	Stopped	I days ago	Success	unot scheduled >	172.30.160.68				3/16/2023 6-57 AA
		MB/s Reed	topod	256 GB (100%) 256 GB 38.9 MB (+996	STATUS Success Warnings 0 Emote	Success 16 Warnings 0						Speed: 504 M
	Name S	when Action										Duration
				and the second								
			oceasing Test									08:13
			ocessing Test									07.09
	200000000000000000000000000000000000000	1100000	scessing Test									13.21
		Success no p.	scessing Test									09:05
												14.59
	En TestVeeam05	Success 🕐 py	ecessing Test									08.53
â llane	TestVeeam05	Success O p.	cessing Test	Veesm10								
	TestVeeam05) Success () Success (ecessing Test ecessing Test	Veesm10 Veesm11								15:47
	TestVeeam05	Success O p. Success O p. Success O p. Success O p.	cessing Test	Veesm10 Veesm11								08:45
T inventory	TestVecan05 TestVecan06 TestVecan07 TestVecan08 TestVecan08	Success O s. Success O s. Success O s. Success O s. Success O s.	ecessing Test ecessing Test	Veesm10 Veesm11 Veesm12								08:45 09:24
T inventory	TestVecon05 TestVecon07 TestVecon07 TestVecon08 TestVecon09 TestVecon09	Success O s. Success O s. Success O s. Success O s. Success O s. Success O s.	ocessing Test ocessing Test ocessing Test	Veeam10 Veeam11 Veeam12 Veeam13								08:45
T inventory	TestVecan05	Success () 5- Success () 5-	acessing Test acessing Test acessing Test acessing Test	Veesm10 Veesm11 Veesm12 Veesm13 Veesm14								08:45 09:24
aventory All Rackup Infrastructure Storage Infrastructure	TestVeeam05	Success O P. Success O P.	scessing Test scessing Test scessing Test scessing Test scessing Test	Veesm10 Veesm11 Veesm12 Veesm13 Veesm14 Veesm15								08:45 09:24 14:34
aventory All Rackup Infrastructure Storage Infrastructure	Test/veen05 Test/veen07 Test/veen07 Test/veen00 Test/veen00 Test/veen10 Test/veen11) Success () p.) Success () p.	acessing Test acessing Test acessing Test acessing Test acessing Test acessing Test	Veesm10 Veesm11 Veesm12 Veesm13 Veesm14 Veesm15	esting							08:45 09:24 14:34 16:16
and the second s	Test/ecen05 Test/ecen06 Test/ecen07 Test/ecen00 Test/ecen09 Test/ecen10 Test/ecen10 Test/ecen12	Success D	accessing Test accessing Test accessing Test accessing Test accessing Test accessing Test VMs have be	Veesm10 Veesm11 Veesm12 Veesm13 Veesm14 Veesm15 Veesm16		get 30%						08:45 09:24 14:34 16:16 17:21
None Image: Source Stratucture Source Stratucture Source Stratucture Tope Inflammeture Tope Source Stratucture Tope Source Stratucture	TestVecen05 TestVecen06 TestVecen00 TestVecen00 TestVecen10 TestVecen10 TestVecen10 TestVecen13 TestVecen13 TestVecen14	Success D	accessing Test accessing Test accessing Test accessing Test accessing Test accessing Test VMs have be	Veenm10 Veenm11 Veenm12 Veenm13 Veenm14 Veenm15 Veenm16 min.queueet for proc min.queueet for proc min.queueet for proc		get 30%						08:45 09:24 14:34 16:16 17:21

For additional information for Veeam replication, refer to 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, select Failover Plan > VMware vSphere.
- 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.

記 王・ Home		Veeam Backup and Replication	
Backup Replication COP Job - Job - Policy Primary Jobs	General	and description for this failover plan, and optionally specify scripts to trigger before and after the failover.	
Sobs Seplication Replicate Active (4) Fallover Plans Soccess Soccess Failed	General Virtual Machines Summary	Name: Failover_VMC_Demo! Description: Created by VEEAM8KPSRV05\Administrator at 8/15/2023 7:50 AM. Pre-failover script: Post-failover script:	
Home Home Storage Infrastructure Storage Infrastructure Tape Infrastructure Files		Remove Next > Cancel	

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

6666 U 8	X				
	Deleta				
Actions Details Manag	pe Rah				
Honve	🔍 Type in an object name to search far 🛛 🕺				
• 🐐 Jobs	Narie 1	Platom Statut Number of VML			
部:Replication • 回 Replicat	Edit Failover Plan (Failover, VMC, Demo)				
Ready Fallower Plant Tailower Plant Gast 24 Hours	Vertual Machines Add virtual machines to be failed over is a part of this plan. Use VM order and delays to ensure all application dependencies are net.				
Success	General	Virtual machines			
	Virtual Machines	Name Delay Replica state * Add VM			
	and the second	TestVecam02 U sec. 3 days ago (412 AM Finday 3/24/2023) TestVecam01 G sac. 3 days ago (411 AM Finday 3/24/2023)			
	Summary	TestViewm03 Dise: 3 days ago (416.434 Friday 3/24/2023)			
		TestVesem04 Disec 3 days ago (4.16 AM Finday 3/24/2023) TestVesem05 Disec 3 days ago (4.18 AM Finday 3/24/2023)			
		🔂 listVessm06 li sec 3 days aga (419 AM Friday 3/24/2023)			
		Testivecam07 Disco: 3 days ago (424 AM Finday \$724(2023) Testivecam08 Divec: 3 days ago (426 AM Finday \$724(2023)			
		TestVerent09 Disec 3 days ego (431 MM Fridey 3/24/2023)			
		TestVeenm10 0 sec 3 days ago (432 AM Friday 3/24/2022)			
		TestNesem11 0 sec 3 days ago (4.39 AM Friday 3/04/2023) TestNesem12 0 sec 3 days ago (4.39 AM Friday 1/24/2023)			
		Terrivesen13 Disc 3 days aga (641 AM Friday \$734/2021)			
		TestVecent14 Disec 3 days ago (A47 AM Friday 3/2A/2023)			
		TestVecem15 0 sec 3 days ago (451 AM Friday 3/24/2023) TestVecem16 0 sec 3 days ago (451 AM Friday 3/24/2023)			
		TWIN503401 2 late 1 days ago (1:50 AM Fiday 5/34/2021)			
A Hone					
and a sectory		< Brevious Apply Binish Cancel			
C Backup Inframacture					
🚰 Storage Infrastructure					
Carl Tope Infrastructure					
D Res					
G ₀ :					

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

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



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

To start the failover plan, simply click in **Failover Plans** tab and right click on the 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**.

ome	Q Type in an object name	to search for		\times		
🐐 Jobs	Name 1	Platform	Status	Number of VMs		
输 Replication	Failover_VMC_Demo	VMware	Ready	21		
E Replicas						
Ready						
() Active (1)						
Failover Plans						
Last 24 Hours						
Success						
🙀 Failed						
ecuting failover Plan: Failover_VMC_Demo						
Name: Failover_VMC_Demo	Sta	tus: In pro	gress			
		and the second	gress 023 11:53:59 PM			
Restore type: Failover Plan	Sta	and the second			Cancel sectors tack	
Restore type: Failover Plan	Sta	and the second			Cancel restore task	
Restore type: Failover Plan nitiated by: VEEAMBKPSRV05\Administrator	Sta	and the second			Cancel restore task	
Restore type: Failover Plan nitiated by: VEEAMBKPSRV05\Administrator VM name Status	Sta	and the second			· · · · · · · · · · · · · · · · · · ·	7 8
Restore type: Failover Plan Initiated by: VEEAMBKPSRV05\Administrator VM name Status TestVeeam02 () Processing	Sta	and the second			Cancel restore task Duration	
Restore type: Failover Plan Initiated by: VEEAMBKPSRV05\Administrator VM name Status TestVeeam02 (): Processing TestVeeam01 (): Processing	Sta Log Message () Processing VM: TestVeeam01	rt time: 3/23/2			· · · · · · · · · · · · · · · · · · ·	
Restore type: Failover Plan Initiated by: VEEAMBKPSRV05\Administrator VM name Status TestVeeam02 () Processing TestVeeam01 () Processing TestVeeam03 () Processing	Sta Log Message	rt time: 3/23/2			Duration	
Restore type: Failover Plan Initiated by: VEEAMBKPSRV05\Administrator VM name Status TestVeeam02 () Processing TestVeeam03 () Processing TestVeeam04 () Processing	Sta Log Message () Processing VM: TestVeeam01	rt time: 3/23/2			Duration	
Restore type: Failover Plan Initiated by: VEEAMBKPSRV05\Administrator VM name Status TestVeeam02 () Processing TestVeeam03 () Processing TestVeeam04 () Processing TestVeeam04 () Processing TestVeeam05 () Processing	Sta Log Message () Processing VM: TestVeeam01 () Waiting 0 sec before the next	rt time: 3/23/2 VM			Duration 0:00:23	
Restore type: Failover Plan Initiated by: VEEAMBKPSRV05\Administrator VM name Status TestVeeam02 () Processing TestVeeam03 () Processing TestVeeam04 () Processing TestVeeam05 () Processing TestVeeam05 () Processing TestVeeam06 () Processing	Sta Log Message ③ Processing VM: TestVeeam01 ③ Waiting 0 sec before the next ④ Processing VM: TestVeeam03	rt time: 3/23/2 VM			Duration 0:00:23	
Restore type: Failover Plan Initiated by: VEEAMBKPSRV05\Administrator VM name Status TestVeeam02 Processing TestVeeam03 Processing TestVeeam04 Processing TestVeeam05 Processing TestVeeam06 Processing TestVeeam07 Processing	Sta Log Message Processing VM: TestVeeam01 Waiting 0 sec before the next Processing VM: TestVeeam03 Waiting 0 sec before the next	rt time: 3/23/2 VM VM			Duration 0:00:23 0:00:23	,
Restore type: Failover Plan Initiated by: VEEAMBKPSRV05\Administrator VM name Status TestVeeam02 () Processing TestVeeam03 () Processing TestVeeam04 () Processing TestVeeam05 () Processing TestVeeam05 () Processing TestVeeam06 () Processing TestVeeam07 () Processing TestVeeam08 () Processing	Sta Log Message Processing VM: TestVeeam01 Waiting 0 sec before the next Processing VM: TestVeeam03 Waiting 0 sec before the next Processing VM: TestVeeam04	rt time: 3/23/2 VM VM			Duration 0:00:23 0:00:23	
Restore type: Failover Plan Initiated by: VEEAMBKPSRV05\Administrator VM name Status TestVeeam02 Processing TestVeeam03 Processing TestVeeam04 Processing TestVeeam05 Processing TestVeeam06 Processing TestVeeam07 Processing TestVeeam08 Processing TestVeeam09 Processing	Sta Log Message Processing VM: TestVeeam01 Waiting 0 sec before the next Processing VM: TestVeeam03 Waiting 0 sec before the next Processing VM: TestVeeam04 Waiting 0 sec before the next	vm vm			Duration 0:00:23 0:00:22	
Restore type: Failover Plan Initiated by: VEEAMBKPSRV05\Administrator VM name Status TestVeeam02 Processing TestVeeam03 Processing TestVeeam04 Processing TestVeeam05 Processing TestVeeam06 Processing TestVeeam07 Processing TestVeeam08 Processing TestVeeam09 Processing TestVeeam09 Processing TestVeeam09 Processing	Sta Log Message Processing VM: TestVeeam01 Waiting 0 sec before the next Processing VM: TestVeeam03 Waiting 0 sec before the next Processing VM: TestVeeam04 Waiting 0 sec before the next Processing VM: TestVeeam05	vm vm			Duration 0:00:23 0:00:22	
Restore type: Failover Plan Initiated by: VEEAMBKPSRV05\Administrator VM name Status TestVeeam02 Processing TestVeeam03 Processing TestVeeam04 Processing TestVeeam05 Processing TestVeeam06 Processing TestVeeam07 Processing TestVeeam08 Processing TestVeeam09 Processing TestVeeam09 Processing TestVeeam09 Processing TestVeeam09 Processing TestVeeam09 Processing TestVeeam09 Processing TestVeeam10 Processing	Sta Log Message Processing VM: TestVeeam01 © Waiting 0 sec before the next Processing VM: TestVeeam03 © Waiting 0 sec before the next Processing VM: TestVeeam04 © Waiting 0 sec before the next Processing VM: TestVeeam05 © Waiting 0 sec before the next	vt time: 3/23/2 vM vM vM vM			Duration 0:00:23 0:00:22 0:00:22 0:00:22	
Restore type: Failover Plan Initiated by: VEEAMBKPSRV05\Administrator VM name Status TestVeeam02 Processing TestVeeam03 Processing TestVeeam04 Processing TestVeeam05 Processing TestVeeam06 Processing TestVeeam07 Processing TestVeeam08 Processing TestVeeam09 Processing TestVeeam09 Processing TestVeeam09 Processing TestVeeam10 Processing TestVeeam10 Processing TestVeeam10 Processing	Sta Log Message Processing VM: TestVeeam01 Waiting 0 sec before the next Processing VM: TestVeeam03 Waiting 0 sec before the next Processing VM: TestVeeam04 Waiting 0 sec before the next Processing VM: TestVeeam05 Waiting 0 sec before the next Processing VM: TestVeeam05	vt time: 3/23/2 vM vM vM vM			Duration 0:00:23 0:00:22 0:00:22 0:00:22	
Restore type: Failover Plan Initiated by: VEEAMBKPSRV05\Administrator VM name Status TestVeeam02 Processing TestVeeam03 Processing TestVeeam04 Processing TestVeeam05 Processing TestVeeam06 Processing TestVeeam07 Processing TestVeeam08 Processing TestVeeam09 Processing TestVeeam09 Processing TestVeeam01 Processing TestVeeam02 Processing TestVeeam04 Processing TestVeeam05 Processing TestVeeam07 Processing TestVeeam08 Processing TestVeeam10 Processing TestVeeam11 Pending TestVeeam12 Pending TestVeeam13 Pending	Sta Log Message Processing VM: TestVeeam01 Waiting 0 sec before the next Processing VM: TestVeeam03 Waiting 0 sec before the next Processing VM: TestVeeam04 Waiting 0 sec before the next Processing VM: TestVeeam05 Waiting 0 sec before the next Processing VM: TestVeeam06 Waiting 0 sec before the next	vm vm vm vm vm vm			Duration 0.00:23 0:00:22 0:00:22 0:00:22	
Restore type: Failover Plan Initiated by: VEEAMBKPSRV05\Administrator TestVeeam02 Processing TestVeeam03 Processing TestVeeam04 Processing TestVeeam05 Processing TestVeeam06 Processing TestVeeam07 Processing TestVeeam08 Processing TestVeeam09 Processing TestVeeam09 Processing TestVeeam09 Processing TestVeeam10 Processing TestVeeam10 Processing TestVeeam10 Processing TestVeeam11 Pending TestVeeam11 Pending TestVeeam13 Pending TestVeeam14 Pending	Sta Log Message Processing VM: TestVeeam01 Waiting 0 sec before the next Processing VM: TestVeeam03 Waiting 0 sec before the next Processing VM: TestVeeam04 Waiting 0 sec before the next Processing VM: TestVeeam06 Waiting 0 sec before the next Processing VM: TestVeeam06 Waiting 0 sec before the next	vm vm vm vm vm vm			Duration 0.00:23 0:00:22 0:00:22 0:00:22	
Restore type: Failover Plan Initiated by: VEEAMBKPSRV05\Administrator VM name Status TestVeeam02 Processing TestVeeam03 Processing TestVeeam04 Processing TestVeeam05 Processing TestVeeam06 Processing TestVeeam07 Processing TestVeeam08 Processing TestVeeam09 Processing TestVeeam09 Processing TestVeeam09 Processing TestVeeam10 Processing TestVeeam11 Pending TestVeeam12 Pending TestVeeam13 Pending TestVeeam14 Pending TestVeeam15 Pending	Sta Log Message Processing VM: TestVeeam01 Waiting 0 sec before the next Processing VM: TestVeeam03 Waiting 0 sec before the next Processing VM: TestVeeam04 Waiting 0 sec before the next Processing VM: TestVeeam06 Waiting 0 sec before the next Processing VM: TestVeeam07 Waiting 0 sec before the next Processing VM: TestVeeam08	vm vm vm vm vm vm vm			Duration 0:00:23 0:00:22 0:00:22 0:00:22 0:00:22	
Restore type: Failover Plan Initiated by: VEEAMBKPSRV05\Administrator VM name Status TestVeeam02 Processing TestVeeam03 Processing TestVeeam04 Processing TestVeeam05 Processing TestVeeam06 Processing TestVeeam07 Processing TestVeeam08 Processing TestVeeam09 Processing TestVeeam09 Processing TestVeeam09 Processing TestVeeam10 Processing TestVeeam11 Pending TestVeeam12 Pending TestVeeam13 Pending TestVeeam14 Pending TestVeeam15 Pending TestVeeam16 Pending	Sta Log Message Processing VM: TestVeeam01 Waiting 0 sec before the next Processing VM: TestVeeam03 Waiting 0 sec before the next Processing VM: TestVeeam04 Waiting 0 sec before the next Processing VM: TestVeeam05 Waiting 0 sec before the next Processing VM: TestVeeam06 Waiting 0 sec before the next Processing VM: TestVeeam07 Waiting 0 sec before the next Processing VM: TestVeeam08 Waiting 0 sec before the next Processing VM: TestVeeam08 Waiting 0 sec before the next	vm vm vm vm vm vm vm			Duration 0:00:23 0:00:22 0:00:22 0:00:22 0:00:22	
Restore type: Failover Plan Initiated by: VEEAMBKPSRV05\Administrator VM name Status TestVeeam02 Processing TestVeeam03 Processing TestVeeam04 Processing TestVeeam05 Processing TestVeeam06 Processing TestVeeam07 Processing TestVeeam08 Processing TestVeeam09 Processing TestVeeam09 Processing TestVeeam09 Processing TestVeeam09 Processing TestVeeam09 Processing TestVeeam01 Processing TestVeeam10 Processing TestVeeam11 Pending TestVeeam13 Pending TestVeeam14 Pending TestVeeam15 Pending TestVeeam16 Pending WinSQL401 Pending	Sta Log Message Processing VM: TestVeeam01 Waiting 0 sec before the next Processing VM: TestVeeam03 Waiting 0 sec before the next Processing VM: TestVeeam04 Waiting 0 sec before the next Processing VM: TestVeeam05 Waiting 0 sec before the next Processing VM: TestVeeam07 Waiting 0 sec before the next Processing VM: TestVeeam07 Waiting 0 sec before the next Processing VM: TestVeeam08 Waiting 0 sec before the next Processing VM: TestVeeam08 Waiting 0 sec before the next Processing VM: TestVeeam08 Waiting 0 sec before the next Processing VM: TestVeeam08	vm vm vm vm vm vm vm vm vm vm			Duration 0:00:23 0:00:22 0:00:22 0:00:22 0:00:22 0:00:22	
Restore type: Failover Plan Initiated by: VEEAMBKPSRV05\Administrator VM name Status TestVeeam02 Processing TestVeeam03 Processing TestVeeam04 Processing TestVeeam05 Processing TestVeeam06 Processing TestVeeam07 Processing TestVeeam08 Processing TestVeeam09 Processing TestVeeam09 Processing TestVeeam09 Processing TestVeeam10 Processing TestVeeam11 Pending TestVeeam12 Pending TestVeeam13 Pending TestVeeam14 Pending TestVeeam15 Pending TestVeeam16 Pending	Sta Log Message Processing VM: TestVeeam01 Waiting 0 sec before the next Processing VM: TestVeeam03 Waiting 0 sec before the next Processing VM: TestVeeam04 Waiting 0 sec before the next Processing VM: TestVeeam05 Waiting 0 sec before the next Processing VM: TestVeeam07 Waiting 0 sec before the next Processing VM: TestVeeam07 Waiting 0 sec before the next Processing VM: TestVeeam08 Waiting 0 sec before the next	vm vm vm vm vm vm vm vm vm vm			Duration 0:00:23 0:00:22 0:00:22 0:00:22 0:00:22 0:00:22 0:00:22 0:00:22	
Restore type: Failover Plan Initiated by: VEEAMBKPSRV05\Administrator VM name Status TestVeeam02 Processing TestVeeam03 Processing TestVeeam04 Processing TestVeeam05 Processing TestVeeam06 Processing TestVeeam07 Processing TestVeeam08 Processing TestVeeam09 Processing TestVeeam09 Processing TestVeeam09 Processing TestVeeam09 Processing TestVeeam10 Processing TestVeeam11 Pending TestVeeam12 Pending TestVeeam13 Pending TestVeeam14 Pending TestVeeam15 Pending TestVeeam16 Pending TestVeeam16 Pending TestVeeam16 Pending	Sta Log Message Processing VM: TestVeeam01 Waiting 0 sec before the next Processing VM: TestVeeam03 Waiting 0 sec before the next Processing VM: TestVeeam04 Waiting 0 sec before the next Processing VM: TestVeeam05 Waiting 0 sec before the next Processing VM: TestVeeam06 Waiting 0 sec before the next Processing VM: TestVeeam07 Waiting 0 sec before the next Processing VM: TestVeeam08 Waiting 0 sec before the next Processing VM: TestVeeam08 Waiting 0 sec before the next Processing VM: TestVeeam09 Waiting 0 sec before the next Processing VM: TestVeeam09 Waiting 0 sec before the next Processing VM: TestVeeam09 Waiting 0 sec before the next Processing VM: TestVeeam09	vm vm vm vm vm vm vm vm vm vm			Duration 0:00:23 0:00:22 0:00:22 0:00:22 0:00:22 0:00:22	
Restore type: Failover Plan Initiated by: VEEAMBKPSRV05\Administrator VM name Status TestVeeam02 Processing TestVeeam03 Processing TestVeeam04 Processing TestVeeam04 Processing TestVeeam04 Processing TestVeeam04 Processing TestVeeam05 Processing TestVeeam06 Processing TestVeeam07 Processing TestVeeam08 Processing TestVeeam09 Processing TestVeeam10 Processing TestVeeam11 Pending TestVeeam13 Pending TestVeeam13 Pending TestVeeam13 Pending TestVeeam14 Pending TestVeeam15 Pending WinSQL401 Pending	Sta Log Message Processing VM: TestVeeam01 Waiting 0 sec before the next Processing VM: TestVeeam03 Waiting 0 sec before the next Processing VM: TestVeeam04 Waiting 0 sec before the next Processing VM: TestVeeam05 Waiting 0 sec before the next Processing VM: TestVeeam07 Waiting 0 sec before the next Processing VM: TestVeeam07 Waiting 0 sec before the next Processing VM: TestVeeam07 Waiting 0 sec before the next Processing VM: TestVeeam09 Waiting 0 sec before the next	vm vm vm vm vm vm vm vm vm vm			Duration 0.00.23 0.00.22 0.00.22 0.00.22 0.00.22 0.00.22 0.00.22 0.00.22 0.00.22	
Restore type: Failover Plan Initiated by: VEEAMBKPSRV05\Administrator VM name Status TestVeeam02 Processing TestVeeam03 Processing TestVeeam04 Processing TestVeeam05 Processing TestVeeam04 Processing TestVeeam05 Processing TestVeeam07 Processing TestVeeam07 Processing TestVeeam09 Processing TestVeeam04 Processing TestVeeam05 Processing TestVeeam07 Processing TestVeeam10 Processing TestVeeam11 Pending TestVeeam13 Pending TestVeeam14 Pending TestVeeam15 Pending TestVeeam16 Pending TestVeeam16 Pending WinSQL401 Pending WinSQL404 Pending	Sta Log Message Processing VM: TestVeeam01 Waiting 0 sec before the next Processing VM: TestVeeam03 Waiting 0 sec before the next Processing VM: TestVeeam04 Waiting 0 sec before the next Processing VM: TestVeeam05 Waiting 0 sec before the next Processing VM: TestVeeam07 Waiting 0 sec before the next Processing VM: TestVeeam07 Waiting 0 sec before the next Processing VM: TestVeeam08 Waiting 0 sec before the next Processing VM: TestVeeam09 Waiting 0 sec before the next Processing VM: TestVeeam10	vm vm vm vm vm vm vm vm vm vm vm vm			Duration 0:00:23 0:00:22 0:00:22 0:00:22 0:00:22 0:00:22 0:00:22 0:00:22	
Restore type: Failover Plan Initiated by: VEEAMBKPSRV05\Administrator VM name Status TestVeeam02 Processing TestVeeam03 Processing TestVeeam04 Processing TestVeeam05 Processing TestVeeam06 Processing TestVeeam07 Processing TestVeeam07 Processing TestVeeam07 Processing TestVeeam07 Processing TestVeeam07 Processing TestVeeam07 Processing TestVeeam01 Processing TestVeeam03 Processing TestVeeam04 Processing TestVeeam05 Processing TestVeeam01 Processing TestVeeam11 Pending TestVeeam13 Pending TestVeeam15 Pending TestVeeam16 Pending TestVeeam16 Pending TestVeeam16 Pending TestVeeam16 Pending TestVeeam16 Pending TestVeeam16 Pending TestVeeam1	Sta Log Message Processing VM: TestVeeam01 Waiting 0 sec before the next Processing VM: TestVeeam03 Waiting 0 sec before the next Processing VM: TestVeeam04 Waiting 0 sec before the next Processing VM: TestVeeam05 Waiting 0 sec before the next Processing VM: TestVeeam07 Waiting 0 sec before the next Processing VM: TestVeeam07 Waiting 0 sec before the next Processing VM: TestVeeam07 Waiting 0 sec before the next Processing VM: TestVeeam09 Waiting 0 sec before the next	vm vm vm vm vm vm vm vm vm vm vm vm vm v			Duration 0.00.23 0.00.22 0.00.22 0.00.22 0.00.22 0.00.22 0.00.22 0.00.22 0.00.22	

The state of the VM replica changes from Ready to Failover and VMs will start on the destination VMware Cloud on AWS SDDC cluster / host.

 O A ← r vSphere Client Q → r 	ne na serie de la 1934 de la companye de la company Reference de la companye de la company	VMs failed over to VMC vCenter Server
Ø 8 0	Cluster-1 Actions Summary Monitor Configure Permissions Hosts VMs	Datastores Networks Updates
	Cluster Details	Capacity and Usage Late contend at 133 PM CV 16.62 Grou was abcates Storage 3,352.09 Grow was abcates VVW 11418 UVW 11
(2) TestVesam0 (2) TestVesam1 (2) TestVesam12 (2) TestVesam15 (2) TestVesam15 (2) TestVesam15 (2) TestVesam15 (2) WeiSGL401 (2) WeiSGL402 (2) WeiSGL403 (2) WeiSGL403	Related Objects II vSphere HA Detacenter Dis Bit SOOC-Datacenter Dis HeartNewHA: Dis HeartNewHorking: Environment VM Montaining: VM	

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

-	Q (see in on object to	reg for union (A) flow	×						
5. Adv	Name T	Intel Televie	Type	Dates	Grantion Time	Kenne Pui.	Original Latation	Repfice Location	Plathere
(D Residention	Els DECT_cold/2	AVE BALLART	Saudie .	(altern	2/16/2023 2/15 AM	1	aloo-vess03.mes	172-30-558-25Gume-1	Wegen
S. Replice	fest/search1	4564,18VAL20230316	Reputer	Failure:	3/23/2023 11/13 PM	4	#200-vca#25.ehul	reamerado)-33-165-115-210 ameratemic cam/ 172.30.16068	Websare
S. Fesh	Test/www.02	F3vN_HEVM_20230314	Regular	Fallower	3/23/2023 11/15 PM	4	a200-mia#05.ehct	volation addo-35-145-115-210	Webware
Anther (27)	A Testiveen03	FE-N, 16VM, 25230316	Reputer	fallower	3/25/2023 13/13/PM	4	all00-resa01.evet.	scenter adds-35-165-115-210 immediating card 172.30.160.68	WANTER
2 Falcor Para	Test/eearo04	PS-N, 18VM, 20220318	Angular	Fallocar	3/21/2023 8:29 4M	3	abore theory only	vienter addi-35-185-115-210 ameetering.com/ 172.30.16068	Wheen
Ci Lan 24 Hours	the TestVeese03	45k/4_16VM_20230316	hepdar	failurer	3/21/2025 8:81 AM	3	a000a03-ehot	veentier adde-35-185-113-210 -means-inc.com/172.30.16058	Viduare
Success	Test/ward6	PSAN 16VM 20230318	Reputer	fallow	3/21/2023 8:32 AM	3	alton-coasts-basis-	viantes addc-33-185-115-210 omvaneutic cum/ 172.30.180.08	Wideare
(S failed	Tantiesant7	FSH1 18VM4 20230316	Regular	Falmer	3/21/2023 8:32 AM	1	aboo-waats med.	ventres adoc-35-185-115-210 venuentvine.com/,172.30.16048	Vidware
1	All Testionands	F544,16444,20230316	Repulse	Fallener	3/31/2023 6:32 AM		#300-wca#05-ehid	scenter add: 33-165-115-210maammer.com/172.30.160.66	Shhuare
	A Testiveenite	FEAN TRUM 20230316	Repulse	Failurer	3/21/2023 8:33 444	2	a300-vesal1 about	veneties adde-35-145-115-210 amagement cam/, 172, 52, 16046	Widward
	Test/esam10	Flate, 16VM-20220316	Reputer	Fallener	3/T1/2022 6 34 AM	3	aloo-veratil-	venetter adds-35-165-115-210 whereartwine.com/172.30.160/68	Widowert
	All Testiments	FILM, 19VM, 20230316	Regular	Failuret	3/21/2023 & 54 AM	¥.	a300-vesa01-met-	volenter adds-35-145-115-210 cm artenic cum/,172.30.16048	Weiners
	dia testitean12	FEWN 18VAA 20230316	Bappine	Failurer	3/21/2023 8:34 AM	1	#200-vci#05.#vci	+cartist adds-25-185-112-210 amount-inc.com/.072.30.160.08	Webser
	(a Sertimani)	F3vN, 18VM, 20230314	Angular	Palitical	3/21/2023 8:35 AM	1	allon-scalls.etest	visional addr-35-185-115-210	Viduate
	A Sectionantia	FEAN, NEVAN, 20230316	Regular	fallower	3/21/2023 0.34 AM	3	#300-read5.ehot	scenteradd-15-15-115-210 -meaning.com/172.30.10068	Ween
	A Sectionarit	45-N, 18VM 20220318	Angular	Failurer	3/21/2023 8-38 AM		aboo	vientes adde-15-185-113-210 emergence cam/ 172-30 160/8	(Sheers
	TextVesen18	PSivis_18VM_20230316	Regular	failurer	3/21/2023 8:37 AM	3	aboo-waathahod	veenterador 35-185-115-210 -mean-inc.com/172.30.16058	Videare
	- WH5QL401	Flicht, Republich, 20230315	Regular	Fallow	3/17/2023 3:58 AM	4	aborte folgen-006a	viantee addc-35-185-115-310 omeaneune cum/ 172.30.160.08	Webware
	12 WimSCE 402	FSell ReplobU1 20200313	Regular	falmer	3/17/2023 3:58 AM		aboo weath met.	veneries uppr-15-185-115-210 veneratives com/, 172.30.16068	Vidward
	10 Wit-00x403	F3x14, Replated1, 20230313	Repulse	Fallener	3/11/0023 4:05 AM	4	a300-ccas05.ehol.	scanlar adds-35-165-115-310 minutes res camil 172.30.160.68	Websare
	3 WinSCL404	Flath Replieb01 20220313	Bender	Eatment	3/117/2023 4:00 AM	*	allon-vessilt shut	venetine adde-35-145-115-210 wma are me cum/, 172.30.16008	Widward
	Win5CL405	Flaht Auguste01 20230313	Angular	fallow -	3/117/2025 4-02 AM		al00-read1abet.	valenter addr-35-165-115-210 one among care(172.30.140/68	Walanger
		of all Fa 'Ms verif		ove	r				

 (\mathbf{i})

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 to 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:

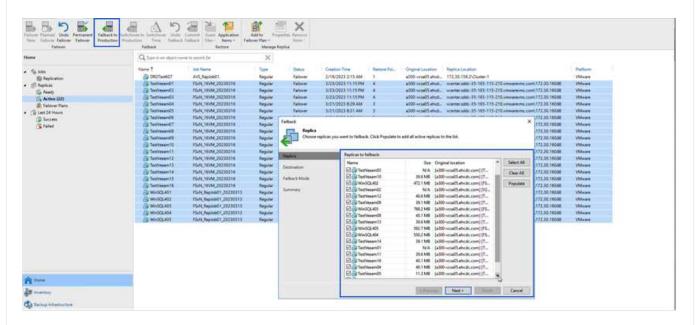
• Failback to production - switch back to the original VM and transfer all changes that took place while the VM replica was running to the original VM.



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.



E Later					Viewen Dathug an	Replication						
	Andrewski Andrewski Statuster Fridanski Statuster Fridanski	Control Cont Application Factors Determined	Add to denote Plan - Harage	×		6	VM: DnPre				ack t er Se	
late	Q 7pm in an object to	me to search for	×				and the	a.a.a.e.	Participant -	2022	-	-second second
 Bate Factoria Restance Restanc	New 7 ODDCmdDT ODDCmdDT Carlorised0 Carl	an fram ArS, Papison Pisk, 1944, 20001 Pisk, 1944, 200001 Pisk, 1944, 200000 Pisk, 1944, 200000 Pisk, 1944, 2000000 Pisk, 1944, 2000000 Pisk, 1944, 2000000 Pisk, 1944, 2000000 Pisk, 1944, 200000000000000000000000000000000000		Data Falce F	Distribution Diff. offer proce Production Clarick rolling Promet or	editesent) editesent1 editesent3 editesent3 editesent3 editesent3 editesent3 ist2(247)	Uscation Sign die soluction	TT2 301144	NOvemen 1 35:145:115-2 35:145:115-2 35:145:115-2 35:145:115-2 35:145:115-2 35:145:115-2	10 maarten 10 maarten 11 maarten 12 maarten 13 maarten 14 maarten	cs=4,173.30.160.68 zs=6,173.30.160.68 cs=6,173.30.160.68	Pathon What What What What What What What What
ñ ***					A. Replice V	M will be privers	d off for the duration of	failback,				
a manage							< Previous	(Charles)	Init	Cancel	11	
C Relacionation												

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.

And Andrews					Name Dailing at	Reptort			
	a 5	2 2 2	a =	×		"(Comn	nit Failback" to	complet
ner Flannark Under Fanzensent Fahlandelte Dark ner Fahlener Fahlener Fahlener Fre Fahlener	Chevier to Saddhasar 1 Deda	Failings First - Barry - Fo	Addite: Fright Annap Fan - Manapa Fapi	Trainer -				the Failback T	ask
-	Q fore is an algest nor	ne hi provin for	×						
fa her	Name T	Job Name	7,04	Tarius .	Dration Tree	Ramon Pol.	Original Casalian	Replice Location	Pattern
(2 Application	CR07##807	AVS, Rephoto1	Repular	Failurer	2/16/2023 2:13 AM	1	all00-yyaa05 ahut	172.35.154.25 Quiter 1	Village
ST Replicas	Ci fertieser01	FININ_18VM_20220216	Reparet	failers.	B/34/3023 1/36 AM	5.	#800-mia05 ahut	rearray abs. 35-185-115-210 cms are my comit/72.30.36048	MART
(C Kenty	Some Territory	F645,19767,20200218	Rep.fat	Tailack.	1/2A/2013 7.22 AH	1		1044104 AND 25-185-115-210 are my sum 172.30 2000	(Morean
Ci. Active (22)	Determine St.	PEACIEVA_30230316	Repaire	Failback	3/34/2023 523 484	5		114-Tax Add, 23, 123-113-210, cmcare.res.com/372.36.36006	Videore
D Falsport Plans	Settimen04	PD/H_18VM_20230318	Repaire	failurb.	A/24/2023 148 AM	A.		+camerate: 15-145-113-210mean mic cont. 172.35.16066	Videore
E Last 24 Moury	Deserver S	P5xH,18VM,20030316	Reputer	Faillerin	1/24/2223 1-89 AM			viamar adde .83-182-113-210 zumit/172.30.16008	Wheee
(S Autom	Satisments .	Plan, 19954, 20230314 Plan, 18954, 20230316	Ferpalar Repulse	FallerA FallerA	5/24/2023 1-24 AM	- 21		reamaradeb - 33-105-115-210	Villeam Villeam
(Warring	Testviserritit	PEAN, 18VM, 20230318 PEAN, 18VM, 20230316	Reporter	Tallack	1/24/2023 1/28 AM	-		reamar add; 201003-115-270 cmaarevers 2000-172.80 1608	Videore
Stated	Testimetrico	PSeN,16VM,20220318	Report	Failurs	8/14/2015 1.37 444	2		Transmissioner and 15-165-113-210 comparements count 172 30 16068	Wilson
	Terrissen12	FSirb, 16VM, 20220376	Report	Failurb	B-54/2023 1.27 884	- 28		scantar adds 25-165-115-210 unsure my card, 172 30 16068	Wheen
	Ca Testiment I	FERCHWA JEDOUTS	1000	Failura	1/24/2013 1-44 AM	- C		Towney and \$1.161 111 212	Witness
	Contention 12	FS/N, 18/44,00200316	Report	failure	ACCREDITION TOT AND			100 mm ann. 25-163-113-210. cm ann an camb 172-30-36568	Whene
	di feminanta	FLAC HEVAL DECENTIN	Reputer	Tallinia	1/34/2013 1/34 AM	8		104100 ADD 25-103-115-210-0000000000000000000000000000000	When
	S Internation	FEAL 18VA 20220218	Repulse	Faillant.	1/34/2023 1/30 AM	-		114114 AMR. 23-185-115-210	Villen
	Batteriesen15	APAK 18/44,00200318	Replie .	faller's	3/04/2023 1:21 AM	- A1	#100-++1401-#vm.	starter abs. 25-165-115-210.000 general cont 172.30 16066	Water
	E hotesants	FINN, 18VM, 20230218	Replie	Failleria.	B/24/2023 1/12 AM	40	#100-++1#05-#hell.	Name and 35-182-112-210 among cont.172.30 1606	Videore
	- Webblant	PS-N, Replied 1, 20230113	Repaire	Failback.	5/24/2023 1(87 AM	11		reams add: 35-165-115-210maxmmx.com 312.35.16568	Webser
	CQ WINDOLAD2	Plate Repland 1,20230213	Replie	Salback.	3/04/2023 1/29 AM	3	a300-wsa05.etus	10.000 alth-35-103-113-210	Whene
	WWWSDLAES	Plats Republit 20230113	Report	faithers.	1/24/2021 1 13 AM	2	a)00-yearst mus.	scarme add:-35-185-115-210 umuseum reaminf?2.3016068	Villeare
		#5x10, Repland 1, 20230813	and a later				The second second second	teranter alth: 25-165-115-210	Villager
	- WHOLEASA	Contraction of the second s	Reputer	Fallack	3/14/2010 1(53 AM	1	#300-research #holi		
	West Ats	Plan, September 20230113	Tagular Tagular	Fallers	3/34/2023 1/38.444	1		vianus adu, 21-188-115-210-manune, cont.172.30.1404	Manu
						1			
ckup Replication CDP Backup Copy Rettore I	Weiscatt								
coup Replication CDP Backup Copy Retore I dk+ Jok+ Poky Copy+Jok+ +	Weiscatt	Plan, Separat (2013) 11							
chup Replication (CDF) Bachup Copy Bachup F k* Mik* Pristy Copy* Ink* * * Primary Jobs Austiliang Jobs Rech me	WestCAADS	Plan, Separat (2013) 11	Report			and low			
chup Replication (CDF) Bachup Copy Bachup F k* Mik* Pristy Copy* Ink* * * Primary Jobs Austiliang Jobs Rech me	Allows Q. type in sedigint for	Plan, Separat (2013) 11	Napore X		104000118844				
Sog Feglication CDF Backup Copy Return 1 5* John - Parky Copy* Mit * * Fremeyrian Academyrian Return me Sg Anine Sg Replication	Allows Allows	Plan, Separat (2013) 11	Napise X	father)	Social tables	1/14/2023	200 AM		
Sog Feglication CDF Backup Copy Return 1 5° John Parky Copy Mat * * frameyride Academyride Return me \$\$ Anima John Statemyride Return Statemyride Return 1 \$\$ Anima John	Allows Allows	Plan, Separat (2013) 11	Napier X Series Test Cerrent failues	Pathers 2004 Sectors	Start Time 1 Scart Time 1	3/24/2023	200 AM 220 AM		
dag Englandra CUP Bulling Capy Fattering 1 1 July - Nation Capy Fattering 1 Network Nation Statement National	Weindowes	Plan, Separat (2013) 11	Napier X Second failback Connet failback Connet failback	falled Doto Screen Screen	3040003 108444	3/24/2023 3/24/2023 3/24/2023	200 AM 200 AM 200 AM 200 AM		
dag Espandon CDF Balang Capy Falence 1 r Alar Park Capy Take 1 remarket Alar Analysis Remarket Alar Analysis Remarket Alar Alar Alar Alar Alar Alar Alar Alar	Allows Allows	Plan, Separat (2013) 11	Teppine X Second Fallence Connect Fallence Connect Fallence	falled Dote: Surres Surres Surres	Start Time 1 Scart Time 1	3/24/2023 3/24/2023 3/24/2023 3/24/2023	206 AM 206 AM 206 AM 206 AM		
Say Espicialization CDP Backing Capy Restores 1 In Nair Fachy Capyrill Nair / New York Auditory Nets And Restored Same Restored Same Res	C type in an officer C type in a officer C type in	Plan, Separat (2013) 11	Neptie X Second Fallock Corrent Fallock Corrent Fallock Corrent Fallock	faitest 2000 Scene Scene Scene	30400031188444	3/34/2023 3/24/2023 3/24/2023 3/24/2023 3/24/2023	206 AM 206 AM 206 AM 206 AM 206 AM 206 AM		
Say Espicialization CDP Backing Capy Restores 1 In Nair Fachy Capyrill Nair / New York Auditory Nets And Restored Same Restored Same Res	Weindowski Weindowski Windowski	Plan, Separat (2013) 11	Napalan X Second Fallback Connot Fallback Connot Fallback Connot Fallback Connot Fallback	faited Street Terms Scens Scens Scens Scens	3040003 108444	3/34/2023 3/24/2023 3/24/2023 3/24/2023 3/24/2023 3/24/2023	200 AM 200 AM 200 AM 200 AM 200 AM 200 AM 200 AM 200 AM		
hop Englished CED Balling Capy Restore 1 to All Factor 1 Marrier Net Audited	C type in an official and a second and a sec	Plan, Separat (2013) 11	Negation Section Fore Connect Follows: Connect Follows: Connect Follows: Connect Follows: Connect Follows: Connect Follows:	feitert Deres Socen Socen Socen Socen	104/0031108.444	5/24/2023 5/24/2023 3/24/2023 3/24/2023 5/24/2023 5/24/2023 5/24/2023 5/24/2023	200 AM 200 AM 200 AM 200 AM 200 AM 200 AM 200 AM		
hop forgations CED taking Capy Reserve 1: to As Factor 2: New Print Assessment Ass Assessment Assessment Assessment Assessment Assessment Assessment Assessment Assessment Assessment Assessment As Assessment Assessment Assessment Assessment Assessment Assessment Assessment Assessment Assessment Assessment As Assessme	Weindoweds	Plan, Separat (2013) 11	Negation Section Targe Connect Failures Connect Failures Connect Failures Connect Failures Connect Failures Connect Failures	feitert 2006 Terrins Socras Socras Socras Socras Socras Socras	3040003 108444	5/24/2023 5/24/2023 3/24/2023 3/24/2023 5/24/2023 5/24/2023 5/24/2023 5/24/2023 5/24/2023	200		
The figures CD barries for to be figures (CD gay files) The file of the fil	C type in an official and a second	Plan, Separat (2013) 11	Ingular Section Fastless Connet Fastless Connet Fastless Connet Fastless Connet Fastless Connet Fastless Connet Fastless Connet Fastless Connet Fastless	Secon Secon Secon Secon Secon Secon Secon Secon Secon	10440001 108444	10000000000000000000000000000000000000	200 AM 206 AM		
Sap Englanden C.D. Barling Carp Rattern 1 Harris Nai - Rais (Carp Rattern 1 Harris Nai - Rais (Carp Rattern 1 Rattern 1 San Anton 1	Weindowski Weindowski Windowski	Plan, Separat (2013) 11	Negation X Section Farle Commit Fallwack Commit Fallwack Commit Fallwack Commit Fallwack Commit Fallwack Commit Fallwack Commit Fallwack Commit Fallwack	Terres Terres Socen Socen Socen Socen Socen Socen Socen	5040003 108444	 3/34/2023 3/24/2023 	206 AM 206 AM		
The figures CD barries for to be figures (CD gay files) The file of the fil	Weindowes	Plan, Separat (2013) 11	Register	faitheat Territors Socram Socram Socram Socram Socram Socram Socram Socram Socram	1040001 104444	3/34/2023 3/24/2023 3/24/2023 3/24/2023 3/24/2023 3/24/2023 3/24/2023 3/24/2023 3/24/2023 3/24/2023 3/24/2023 3/24/2023	200	Task succe	essful
The figures CD barries for to be figures (CD gay files) The file of the fil	Weindowski Weindowski Windowski	Plan, Separat (2013) 11	Inquire Sector Sector	Secon Secon Secon Secon Secon Secon Secon Secon Secon Secon Secon Secon Secon Secon Secon Secon	5040003 108444	5/24/2023 3/24/2023 3/24/2023 3/24/2023 3/24/2023 3/24/2023 3/24/2023 3/24/2023 3/24/2023 3/24/2023 3/24/2023 3/24/2023	200	Task succe	essful
Sap Englanden C.D. Barling Carp Rattern 1 Harris Nai - Rais (Carp Rattern 1 Harris Nai - Rais (Carp Rattern 1 Rattern 1 San Anton 1	Adams	Plan, Separat (2013) 11	Report Section Processing Section Processing Connect Follows Connect Follows	Tertest Terres Socen Socen Socen Socen Socen Socen Socen Socen Socen Socen Socen Socen Socen Socen Socen	304/0001 1084/44	1/24/2023 1/24/2023 1/24/2023 1/24/2023 1/24/2023 1/24/2023 1/24/2023 1/24/2023 1/24/2023 1/24/2023 1/24/2023 1/24/2023 1/24/2023 1/24/2023	200		essful
Sap Englanden C.D. Barling Carp Rattern 1 Harris Nai - Rais (Carp Rattern 1 Harris Nai - Rais (Carp Rattern 1 Rattern 1 San Anton 1	Weindowski	Plan, Separat (2013) 11	Inquire Sector Sector	Televit Seren Seren Secen Secen Secen Secen Secen Secen Secen Secen Secen Secen Secen Secen Secen	5040003 108444	1.104/2023 3/24/2023 3/24/2023 3/24/2023 3/24/2023 3/24/2023 3/24/2023 3/24/2023 3/24/2023 3/24/2023 3/24/2023 3/24/2023 3/24/2023 3/24/2023	200 AM 206 AM	Task succe	essful
Sile Faislands CDF Backing Capy Retries 1 Harris Nat - Role Capy Capy Retries 1 Newsy Inter Sile Antine (Net Sile Capy Retries Sile Capy Retries Sile Capital Sile Sile Capy Retries Sile Capital Sile Sile Capital Sile Sile Sile Sile Sile Sile Sile Sil	Allow Al	Plan, Separat (2013) 11	Report Section Version Connect Follows Connect Follows	Solar Socas Socas Socas Socas Socas Socas Socas Socas Socas Socas Socas Socas Socas Socas Socas Socas Socas Socas	Boot Time J Mide 1000 J 1000 Anno 1004 2003 3 001 An 1004 2003 3 001 An	1/24/2023 3/24/2023 3/24/2023 3/24/2023 3/24/2023 3/24/2023 3/24/2023 3/24/2023 3/24/2023 3/24/2023 3/24/2023 3/24/2023 3/24/2023 3/24/2023 3/24/2023	200	Task succe	essful
Copy Englishers COP Nation Copy Factors 1 1 Nation Copy Factors 1 Nation (New York Nation Copy Factors 1 Nation (New York Nation (New York	Average Action Average	Plan, Separat (2013) 11	Inspire Sector Sector	Autor Autor Secon	5040003 108444	1.154/2023 3.154/2023 3.154/2023 3.174/2023 3.174/2023 3.174/2023 3.174/2023 3.174/2023 3.174/2023 3.174/2023 3.174/2023 3.174/2023 3.174/2023 3.174/2023 3.174/2023 3.174/2023	200	Task succe	essful
Copy Englishers COP Nation Copy Factors 1 1 Nation Copy Factors 1 Nation (New York Nation Copy Factors 1 Nation (New York Nation (New York	Advances Advanc	Plan, Separat (2013) 11	Section 2014 Section 2014 Connect February Connect February	Televit Social	Start Time 1 Start	1.54/2023 3.54/2023 3.74/2023 3.74/2023 3.74/2023 3.74/2023 3.74/2023 3.74/2023 3.74/2023 3.74/2023 3.74/2023 3.74/2023 3.74/2023 3.74/2023 3.74/2023 3.74/2023	200	Task succe	essful
Sile Faislands CDF Backing Capy Retries 1 Harris Nat - Role Capy Capy Retries 1 Newsy Inter Sile Antine (Net Sile Capy Retries Sile Capy Retries Sile Capital Sile Sile Capy Retries Sile Capital Sile Sile Capital Sile Sile Sile Sile Sile Sile Sile Sil	Average Action Actions Action	Plan, Separat (2013) 11	Inspire Sector Sector	Autor Autor Secon	3040003 108444	5:24/2023 5:24/2023 5:24/2023 5:24/2023 5:24/2023 5:24/2023 5:24/2023 5:24/2023 5:24/2023 5:24/2023 5:24/2023 5:24/2023 5:24/2023 5:24/2023 5:24/2023	200	Task succe	essful
Sap Englanden C.D. Barling Carp Rattern 1 Harris Nai - Rais (Carp Rattern 1 Harris Nai - Rais (Carp Rattern 1 Rattern 1 San Anton 1	Weidquads W	Plan, Separat (2013) 11	Second Parks Second Parks Connell Fallers Connell Fallers	Televit Social S	3040 Time 1 3040 Time 1 3040 2000 2 407 AA 1040 2000 2 407 AA	5.04/2023 10/4/2023 10/4/2023 10/4/2023 10/4/2023 10/4/2023 10/4/2023 10/4/2023 10/4/2023 10/4/2023 10/4/2023 10/4/2023 10/4/2023	206 AM 206 AM	Task succe	essful
Sap Englanden C.D. Barling Carp Rattern 1 Harris Nai - Rais (Carp Rattern 1 Harris Nai - Rais (Carp Rattern 1 Rattern 1 San Anton 1	WeiddLABS	Plan, Separat (2013) 11	Inspire Sector Sector	Autoria Zurina Sacram Sacram Sacram Sacram Sacram Sacram Sacram Sacram Sacram Sacram Sacram Sacram Sacram Sacram Sacram Sacram Sacram Sacram	5040000 1108 AM	5:04/2023 3:04/2023 3:04/2023 3:04/2023 3:04/2023 3:04/2023 3:04/2023 3:04/2023 3:04/2023 3:04/2023 3:04/2023 3:04/2023 3:04/2023 3:04/2023 3:04/2023	200	Task succe	essful
Sap Englanden C.D. Barling Carp Rattern 1 Harris Nai - Rais (Carp Rattern 1 Harris Nai - Rais (Carp Rattern 1 Rattern 1 San Anton 1	Average Action Actions Action	Plan, Separat (2013) 11	Reputer	Autor Autor Secon	3040 Time 1 3040 Time 1 3040 Citer 2 3040 Ci	5:04/2023 3:04/2023 3:04/2023 3:04/2023 3:04/2023 3:04/2023 3:04/2023 3:04/2023 3:04/2023 3:04/2023 3:04/2023 3:04/2023 3:04/2023 3:04/2023 3:04/2023 3:04/2023 3:04/2023 3:04/2023 3:04/2023	206 AM 206 AM	Task succe	essful

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

	0 &	e na th e Notice on y la happenen			All	VN	ls r	ecove	red	386	© @ Q
😑 vSphere Client 🛛 🔾										C 3	
		🗈 Cluster05 🕅		AR 1987-02040-07	on C	n	Pre	m vCe	enter		
B B	· · · · · · · · · · · · · · · · · · ·	Total Process		ents vite Dalationes						1	Proc. 92.00 Canony, 194.00 Proc. 00.00 Canonity, 100.00 Proc. 00 Canonity, 10.00
(2) Test/vexamico (2) Test/vexamico (2) Test/vexamico (2) Test/vexamico (2) Test/vexamico		Related Objects Datacenter	推 A2	x0.0K05		Î	vSphare C Cluster Se				
(計 TestVesam06 (計 TestVesam07 (計 TestVesam08 (計 TestVesam08		Outline Cotsumers				÷	Custore A	0/Gules		Mar	
62 TestVeeen10 62 TestVeeen10 63 TestVeeen10 63 TestVeeen10 63 TestVeeen10 63 TestVeeen10		Tarja Autoret Tag	Computy	Decemen		•		ek Johnstonen Aufer Aufer Aufer	defuzióse)		
Tetriveants Sit tetriveants Sit tetriveants Sit windcusts Sit Windcusts Sit Windcusts Sit Windcusts		× III			No april 1	3 v 1999	ŧĸ.				1 harry
は WestGLADS 一部 WestGLADS		Outlet Resources				v					
 Recent Tasks Alarms 											
			Detats	• Hibelie	* Duniet *	Bat fire		Completion Time •	- The second second		
	WHISCALADI	Comparted Comparted		EHCDC COM(Administrator EHCDC COMAdministrator	4 mi	03/34/202	15907_	05/24/2023 159/07	abdo-ectaids etco abdo-ectaids etco		

Conclusion

FSx for ONTAP datastore capability enables Veeam or any validated third-party tool to provide low-cost DR solution using Pilot light cluster and without standing up large number of hosts in the cluster just to accommodate the VM replica copy. This provides a powerful solution to handle a tailored, customized disaster recovery plan and also allows to reuse existing backup products in house to meet the DR needs, thus enabling cloud-based disaster recovery by exiting DR datacentres on-premises. Failover can be done as planned failover or failover with a click of a button when disaster occurs, and decision is made to activate the DR site.

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

https://netapp.hosted.panopto.com/Panopto/Pages/Embed.aspx?id=15fed205-8614-4ef7-b2d0-b061015e925a

Migrating Workloads on AWS / VMC

TR 4942: Migrate Workloads to FSx ONTAP datastore using VMware HCX

A common use case for VMware Cloud (VMC) on Amazon Web Services (AWS), with its supplemental NFS datastore on Amazon FSx for NetApp ONTAP, is the migration of VMware workloads. VMware HCX is a preferred option and provides various migration methods to move on-premises virtual machines (VMs) and their data, running on any VMware supported datastores, to VMC datastores, which includes supplemental NFS datastores on FSx for ONTAP.

Author(s): NetApp Solutions Engineering

Overview: Migrating virtual machines with VMware HCX, FSx ONTAP supplemental datastores, and VMware Cloud

VMware HCX is primarily a mobility platform that is designed to simplify workload migration, workload

rebalancing, and business continuity across clouds. It is included as part of VMware Cloud on AWS and offers many ways to migrate workloads and can be used for disaster recovery (DR) operations.

This document provides step-by-step guidance for deploying and configuring VMware HCX, including all its main components, on-premises and on the cloud data center side, which enables various VM migration mechanisms.

For more information, see Introduction to HCX Deployments and Install Checklist B - HCX with a VMware Cloud on AWS SDDC Destination Environment.

High-level steps

This list provides the high-level steps to install and configure VMware HCX:

- 1. Activate HCX for the VMC software-defined data center (SDDC) through VMware Cloud Services Console.
- 2. Download and deploy the HCX Connector OVA installer in the on-premises vCenter Server.
- 3. Activate HCX with a license key.
- 4. Pair on-premises VMware HCX Connector with VMC HCX Cloud Manager.
- 5. Configure the network profile, compute profile, and service mesh.
- 6. (Optional) Perform Network Extension to extend the network and avoid re-IP.
- 7. Validate the appliance status and ensure that migration is possible.
- 8. Migrate the VM workloads.

Prerequisites

Before you begin, make sure the following prerequisites are met. For more information, see Preparing for HCX Installation. After the prerequisites are in place, including connectivity, configure and activate HCX by generating a license key from the VMware HCX Console at VMC. After HCX is activated, the vCenter Plug- in is deployed and can be accessed by using the vCenter Console for management.

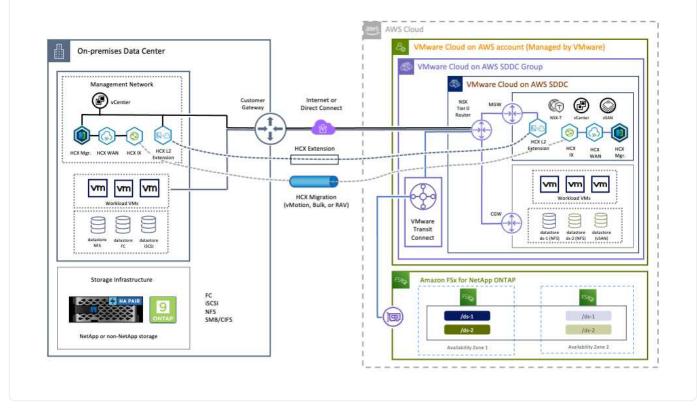
The following installation steps must be completed before proceeding with HCX activation and deployment:

- 1. Use an existing VMC SDDC or create a new SDDC following this NetApp link or this VMware link.
- 2. The network path from the on-premises vCenter environment to the VMC SDDC must support migration of VMs by using vMotion.
- 3. Make sure the required firewall rules and ports are allowed for vMotion traffic between the onpremises vCenter Server and the SDDC vCenter.
- 4. The FSx for ONTAP NFS volume should be mounted as a supplemental datastore in the VMC SDDC. To attach the NFS datastores to the appropriate cluster, follow the steps outlined in this NetApp link or this VMware link.

High Level Architecture

For testing purposes, the on-premises lab environment used for this validation was connected through a site-to-site VPN to AWS VPC, which allowed on-premises connectivity to AWS and to VMware cloud SDDC through External transit gateway. HCX migration and network extension traffic flows over the internet between on-premises and VMware cloud destination SDDC. This architecture can be modified to use Direct Connect private virtual interfaces.

The following image depicts the high-level architecture.



Solution Deployment

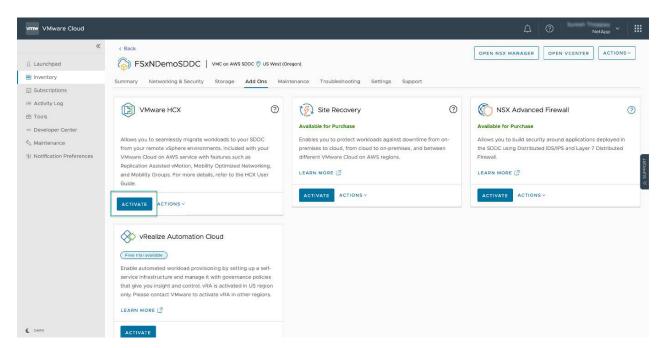
Follow the series of steps to complete the deployment of this solution:

To perform the installation, complete the following steps:

- 1. Log in to the VMC Console at vmc.vmware.com and access Inventory.
- 2. To select the appropriate SDDC and access Add- ons, click View Details on SDDC and select the Add Ons tab.
- 3. Click Activate for VMware HCX.



This step takes up to 25 minutes to complete.



- 4. After the deployment is complete, validate the deployment by confirming that HCX Manager and its associated plug-ins are available in vCenter Console.
- 5. Create the appropriate Management Gateway firewalls to open the ports necessary to access HCX Cloud Manager.HCX Cloud Manager is now ready for HCX operations.

For the on-premises Connector to communicate with the HCX Manager in VMC, make sure that the appropriate firewall ports are open in the on-premises environment.

- 1. From the VMC Console, navigate to the HCX Dashboard, go to Administration, and select the Systems Update tab. Click Request a Download Link for the HCX Connector OVA image.
- 2. With the HCX Connector downloaded, deploy the OVA in the on-premises vCenter Server. Right- click vSphere Cluster and select the Deploy OVF Template option.

😑 vSphere Client	Q	C 2 Ameritan Alexandra	₩~ © Ø>
	K III A300-Cluste	701 Excisions	_
- 👩 atoo veisot enco	Deploy OVF Template	Select an OVF template × select an OVF template from remote URL or local file system	
- El ANDO OMAGE - El ANDO OMAGE El ANDO GEN	Select an OVF template Select a name and forder	Enter a URL to download and install the OVF package from the internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.	Hire.
0 a000-es 0 a000-es 0 G ADE 40	3 Select a compute resource 4 Review details	Local file	
 O ANFORM O AVSAULT O HOLDE 	5 Select storage 6 Ready to complete	UPLOAD FILES VMware-HCK-Connector-4: ova	
(2 HO) (2 HO) (2 HO) (2 HO) (2 HO)			
ta rea. Ta reak		CANCEL	
	Photos 24	recence Powerst, C. Kernal Acros EDAR (JB 20 Mate 75 GB	x + 11 /4 2 X
A Recent Tasks	Alarma :		

- 3. Enter the required information in the Deploy OVF Template wizard, click Next and then Finish to deploy the VMware HCX Connector OVA.
- 4. Power on the virtual appliance manually.For step- by- step instructions, go to VMware HCX User Guide.

After you deploy the VMware HCX Connector OVA on-premises and start the appliance, complete the following steps to activate HCX Connector. Generate the license key from the VMware HCX Console at VMC and input the license during the VMware HCX Connector setup.

- 1. From the VMware Cloud Console, go to Inventory, select the SDDC, and click View Details. From the Add Ons tab, in the VMware HCX tile, click Open HCX.
- 2. From the Activation Keys tab, click Create Activation Key. Select the System Type as HCX Connector and click Confirm to generate the key. Copy the activation key.

bs	criptions Activation Keys	SDDCs						C DARI
cti	ivation Keys						- C	REATE ACTIVATION KEY
	Activation Key		Status v	Subscription	τ System Type τ	System Id	7	Created
	ABIEI	\$3	CONSUMED	VMware Cloud on AWS (HEX Connector	205	73	9/19/22, 9:24 AM
	9203	75	CONSUMED	VMware Cloud on AWS (HCK Cloud	201	>5321	9/16/22, 9:56 AM
	100	(846	DEACTIVATED	VMware Cloud on AWS	HCK Cloud	205	26	8/11/22, 12:23 PM



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

3. Log in to the on-premises VMware HCX Connector at "https://hcxconnectorIP:9443" using administrator credentials.



Use the password defined during the OVA deployment.

4. In the Licensing section, enter the activation key copied from step 2 and click Activate.



The on-premises HCX Connector must have internet access for the activation to complete successfully.

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



Use the FQDN to avoid communication issues later.

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



Enter the vCenter Server's IP address or FQDN.

- 10. Verify that the information is entered correctly and click Restart.
- 11. After complete, the vCenter Server is displayed as green. Both the vCenter Server and SSO must

have the correct configuration parameters, which should be the same as the previous page.



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

$\rightarrow \alpha$	O 🔓 https:/	//172.21.254.157:9443/hoc-m	nanager-ul/index.html#	//dashboard			<u>Ω</u>	2	9
m HCX Manager	Dashboard	Appliance Summary	Configuration	Administration			7221254157	Version: 4.410 Type : Connector	admir
0 VMware-HCX	-440				(CPU		Free 688 MHZ	67%
FODN:	VMware-HCX-440	ehcdc.com				Used 1407 MHZ		Capacity 2095 MHZ	
P Address:	172.2					Memory		Free 2316 MB	
Version:	4.4.1.0				(D			81%
Uptime:	20 days, 21 hours,					Used 9691 MB		Capacity 12008 MB	
Current Time:	Tuesday, 13 Septer	mber 2022 07:44:11 PM UT(C			Storage		Free 98G	23%
						D Used 29G		Capacity 1276	
NSX			vCenter			SSO			
			https://a300-vc	sa01.ehcdc.com		https://a300-vcsa01.eh	cdc.com		
MANAGE			MANAGE			MANAGE			
MANAGE			MANAGE			MANAGE			

Step 4: Pair on-premises VMware HCX Connector with VMC HCX Cloud Manager

1. To create a site pair between the on-premises vCenter Server and the VMC SDDC, log in to the onpremises vCenter Server and access the HCX vSphere Web Client Plug- in.

hortcuts											
iventories	B)	8	Ø			°%	п	Ŵ	(A	٢	
Hosts and Clusters	VMs and Templates	Storage	Setworking	Content Libraries	Global Inventory Lists	Workfoad Management	SnapCenter Plug-in for VMware vSphere	Cloud Provider Migration	Site Recovery	нсх	
Ionitoring											
圖		Æ	F		\sim						
Task Console	Event Console	VM Customization Specifications	VM Storage Policies	Host Profiles	Lifecycle Manager	ONTAP tools					
dministratio	n										

2. Under Infrastructure, click Add a Site Pairing. To authenticate the remote site, enter the VMC HCX Cloud Manager URL or IP address and the credentials for the CloudAdmin role.

	< Sit	te Pairing	
HCX C DayPoord Intrastructure			ADO A SITE PAIRING .
Bite Paring Marcannect Stanport Analytics		BHCX-loud - F5xNDemoSDDC Mass./702.3524.357.443 Massen Masse	
Antwork Extension Antwork Extension Migration Disaster Recovery	*	timesonectigi eart convection pisconnect	
yatan Administration © Secont	×.		

HCX information can be retrieved from the SDDC Settings page.

(i)

VMware Cloud					۵	O Suresh Th	AttAco
ĸ	e Back			OPEN	NSX MANAGER	OPEN VCENTER	ACTIONS-
& Launchood	FSxNDemoSDDC VAIC on ANS SDDC () US Week (Dregord)						
El Inventory	Summary Networking & Security Storage Add Ons Maintenan	ce Troubleshooting Setting	ge Skaport				
3 Subscriptions							
i Activity Log	SDDC						
h Tools	> Management Appliances (N/A)						
Developer Center Montenance	vCenter Information						
Notification Preferences	S Default vCenter User Account						
	3 vSphere Clant (HTML5)						
	> Center Server API Explorer						
	> PowerCLI Connect						
	> vCenter PGDN						
	HCX Information						
	inco Facel Mitgau/Thi	Anna Andrea Public IP - Tready	rabla from internet	Pare P	Province (* 172.30.16		80
	NSX Information						
	3 NSX Manager button default access						1
							(

HD Internet : Stratteriota Stratteriota - Schemenses Schemense	C ADD A SITE FAILURE STREAM C C C C C C C C C C C C C C C C C C C
A stream Concess A stream Concess A stream Concess Sector Concess A stream concess C frame	View Connect to Remote Site Image: State of the sta
 Meter table. Alores Meter P. Sope (* 1996) 	T Index T Index T Index T Index In T

3. To initiate the site pairing, click Connect.



VMware HCX Connector must be able to communicate with the HCX Cloud Manager IP over port 443.

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

The VMware HCX Interconnect (HCX-IX) appliance provides secure tunnel capabilities over the internet and private connections to the target site that enable replication and vMotion-based capabilities. The interconnect provides encryption, traffic engineering, and an SD-WAN. To create the HCI-IX Interconnect Appliance, complete the following steps:

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



Compute profiles contain the compute, storage, and network deployment parameters required to deploy an interconnect virtual appliance. They also specify which portion of the VMware data center will be accessible to the HCX service.

For detailed instructions, see Creating a Compute Profile.

e → C	08.=	# 0+ https://a300-vcsa01ahodc.com/ui/app/blu	ain/com.vmware.hybridity/com.vmware.ho	x/lybridConnect	Ŷ		. ∎
\equiv vSphere Client Q				C		٢	@ ~
HCX Dashboard Infrastructure Stee Pairing Infectormect Services Network Extension Migration Disaster Recovery	~	Interconnect Multi-State Service Mesh Computer Middliss Service Mesh Network P hcxdemo hcxdemo Host a000-ess/01 encot: comple host 2022	is in critical (red) table for service compute	rompute	Q C CREATE COM	PUTE PRC	DFILE
System & Administration	2	Serves Resultés Ga300-vosa01.ekcdc.com A300-Cluster01 SCC Services SCC Services S		Networks	Last al al an	EDIT	

- After the compute profile is created, create the network profile by selecting Multi-Site Service Mesh > Network Profiles > Create Network Profile.
- 3. The network profile defines a range of IP address and networks that will be used by HCX for its virtual appliances.



This will require two or more IP address. These IP addresses will be assigned from the management network to virtual appliances.

= vSphere Client Q							C a	Administrator@EHCO	с.сом 🛩	٢	0
HCX Dashboard Infrastructure Site Pairing interconnect Transport Analytics	~	Interconnect Multi-Site Senice Mesn Compute Profiles Senice Mesh	Notwork Profiles Ser	tinel Management				Q C C	REATE NETW	ORK PR	OFILE
Services Network Extension Migration Disaster Recovery System So Administration So Support	~	VM_3510 Network Details Decking VM_3510 show more	мти 9000		Ranges 0 - 172.21.254.95	IP Usage(Used/Total) 4/ 16	Prefix Length	Gateway 172.21.254.230			
		EDIT DELETE									

For detailed instructions, see Creating a Network Profile.



If you are connecting with an SD-WAN over the internet, you have to reserve public IPs under the Networking and Security section.

4. To create a service mesh, select the Service Mesh tab within the Interconnect option and select onpremises and VMC SDDC sites.

The service mesh establishes a local and remote compute and network profile pair.

vm VMware HCX		Ø- administrator-
Dashboard Infrastructure Site Paring Site Paring Site Paring Siterconnect L: Transport Analytics Services @ Network Extension	Interconnect Multi-Site Service Mesh Compute Profiles Service Mesh Network Profiles Bendinet Management	O. C. CREATE REMOCE MERH
Algration Oilaister Secovery Administration Is System Updates Troubleshooting Addit Logs Activity Logs Activity Logs Activity Logs Activity Logs Oile	100007 Ste Fairing WYsware-HCK-640 BAnapatane Readers Stateme Tot139-ECK COBINE RESTRE VIEW ARPLIANCES RESYNC EDIT DELETE MORE+	>



Part of this process involves deploying HCX appliances that will be automatically configured on both the source and target sites, creating a secure transport fabric.

5. Select the source and remote compute profiles and click Continue.

Create Service Mesh	1 2 12 4 5	
Select Compute Profiles		
Select one compute profile each in the source and remote pites for activiting hybridity services. The		
Select Source Compute Profile (ncxdemo)	Select Remote Compute Profile ComputeProfile(scemer)	
Hourt 4305 eccl01 anciec camilations 2252; is in critical (web) states for service compute More a305 eccl01 anciec camilations 2250; is in critical (rec) states for deployment compute		
(C) was any concernent residuals (M) is care but one is sholding residual residual		CONTINU

6. Select the service to be activated and click Continue.

Edit Service Mesh		1 2 3 4	5		×
Select Services to be activated					
OS Assisted Migration Service can't be SRM Integration Service cannot be set	e selected as one or both the compute profiles sele lected as they are not licensed with this HCK visital	icted in previous step doesn't have these services act altion.	overland .		
Hybrid Interconnect (Preside Types)		Coss-close WithomMaration ()) F2wiCounter Proceeding		Reportation Assisted vectors Migration () Etherbalanduserteinberer Picce Phone	Network Extension (1)
DissterRectivery () AppEdit Colorest		Di Austride Mayantin @			
	Paginer has not been actuated				CONTINUE



An HCX Enterprise license is required for Replication Assisted vMotion Migration, SRM Integration, and OS Assisted Migration.

7. Create a name for the service mesh and click Finish to begin the creation process. The deployment should take approximately 30 minutes to complete. After the service mesh is configured, the virtual infrastructure and networking required to migrate the workload VMs has been created.

≡ viphere Gent Q								C 2	
xa	- in	terconr	rect						
Openhant	2	som dae ben	tas linker						
of adruction O the fairing	. 5	Conjulation	w brokiwi issekhde. bette laspoet						
anterioroest		+ 1	ccoo7 ~						CON SERVICE HERE
10. Transport Analytics Services		Attains	BARRING CTURE						11
Cr ketwork potension			and Statement Strengton and Strengton						
C Mgratian			Applaint form	t a Assessed Type 1 of Address		funne inner	Darrente Versione	Average reserved	
© Disate Recovery System A elementation © Support	×	0.	CODDT-01-0 or 2159-091-0126-070-00220-002080 Annewsky ASSOC_0074-00 Browge ASSOC_0747_02020	112-24.00 (maximum) ((1944-490-1940)	•	642.0		
		0.3	COUT 48.0 as UTM-9 INVA-547-5487 MIRINGCICU Comman ADD-CUITED Temper ADD-AFE_DIDE Manager ADD-AFE_DIDE Manager Manager (DI) Manager Manager (DI)	Carlos and		۲	6420		
			0000114904 w 42417749/Mite-selfa-ambe-editional Ennances-2000/001000 Binnege-4000/071_01004	C all man out			1234	N/A	
									1.000
			es on hox.liebf3b0b76at4cc08e3t85.westeurope.a						for an ended
		-							4400
				NO 400 400 400 400 400 400 400 400 400 40	antenari (
		-00307 H	14	(0.001 Dia 10.000)					480.0
		K0001W	сн	Ci mai ort					7380

Step 6: Migrating Workloads

HCX provides bidirectional migration services between two or more distinct environments such as onpremises and VMC SDDCs. Application workloads can be migrated to and from HCX activated sites using a variety of migration technologies such as HCX bulk migration, HCX vMotion, HCX Cold migration, HCX Replication Assisted vMotion (available with HCX Enterprise edition), and HCX OS Assisted Migration (available with HCX Enterprise edition).

To learn more about available HCX migration technologies, see VMware HCX Migration Types

The HCX-IX appliance uses the Mobility Agent service to perform vMotion, Cold, and Replication Assisted vMotion (RAV) migrations.



The HCX-IX appliance adds the Mobility Agent service as a host object in the vCenter Server. The processor, memory, storage and networking resources displayed on this object do not represent actual consumption on the physical hypervisor hosting the IX appliance.

≡ vSphere Client Q	
<u>9</u> = 0	C 172.21.254.82 Actions Summary Monitor Configure Permissions VMs Resource Pools Datastores Networks Updates
	Wypervisor: VMware 62XX, 7.0.3, 20305777 Model: VMware Mobility Platform Processor Type: VMware Virtual Processor Logical Processors: 768 NiCi:: 8 Virtual Machines: 0 State: Connected Uptime: 29 days

VMware HCX vMotion

This section describes the HCX vMotion mechanism. This migration technology uses the VMware vMotion protocol to migrate a VM to VMC SDDC. The vMotion migration option is used for migrating the VM state of a single VM at a time. There is no service interruption during this migration method.



Network Extension should be in place (for the port group in which the VM is attached) in order to migrate the VM without the need to make an IP address change.

1. From the on-premises vSphere client, go to Inventory, right- click on the VM to be migrated, and select HCX Actions > Migrate to HCX Target Site.

≡ vSphere Clent Q, ∞	d Actions -HCX_Photon_34 Prover	5						C & Assessed and Concrete	· • 6
0 8 9 9	Guest OS Shapshots Coon Remote Console	2. 2	noton_14 > ontor Configure			Shiphots	updates		
- 📴 4300-Visiolationer - 🔝 4300-DataCenter - 🖾 4300-DataCenter	dit Migrate . Clone		Cont	et O'S sualbrilly wate Tools	VMeans Rooten OS (64-04) 8001 6.7 And later (M version M) Rooteng, version RDD (Cent Manapel)				O Hz
addo-eskild shodc.com	Fault TolerAnce	7		Name	work and procesor			a	B 20 MB
appo-execting encourceme	VM Policies		INSOLA	odresen.	172 21 255 17 VEW ALL 2 IP ADDRESSES 4000-exe01 shcds.com			-	718.61 MB
G ANFJHDC,Deno G ANFDeno	Template Compatibility	2	I COMPOCE O	61					
 Ø withing Ø withing 	Export System Logs					^	Nucles.		~
B HOUTHING H	4) Edit Settings.			10PU	00 88. 0.02.08 memory active		Custom Attributes		~
 (注) HCX(Photon_17-865000504387 (注) HCX(Photon_18) 	Move to folder Bename Edit Notes		Augster 1	2 08 VM_M	929 (convected)		Aminde	Ville	
 A HOLIMONUM A HOLIMONUM 	Tags & Custom Attributes	•	Tree 1	01000 4 MB	vector	5.1			
B HOUPHONGE B HOUPHONGE	Add Permission Alarms	2	•		e on the virtual machine PIG pus that prov et for the virtual machine communication (the terms to all addap
A HOLENDARY Recent Table Alarma	Annual Date Instituty Debug from 200			A505	oral Hardware				
His Name Total Terant Here foldor ED HCK_Pector_H_NK, HCM/gover Vitual Mach. @ HCK_Pector_N	vslan NetApp SnapCenter	ſ	Orien Orien Orien	rgei Site	-COC COM Administrative	Guenet T Far 3 ms 2 mi	Hust Tree J Compression Tree 08/13/2022 4.45.97.P 08/13/2022 09/13/2022 4.45.97.P 09/13/2022	e 45.37 P, a300-vesa01 ahooc care	
tove antities D. VMs moralad to con-	All Side Recovery actions HOX Actions	-	+protect to HCLT	iger sae	-COC COM Agriculture	4.758	09/13/2022 4:45:04 09/13/2022	a 45.04 a 300-vçaðt en coz.com	

2. In the Migrate Virtual Machine wizard, select the Remote Site Connection (target VMC SDDC).

 Select Connection (there are 2 records found) 				C Reload	Connectio
	D-vcsa01.ehcdc.com → Destination: (select)				
and the second se	vcepter.sddc-54-188-6-128.vmwarevmc.com				
Mbsr./172.30.156.9	/ VC 172.30.156.2				
✓ Transfer and Placement:					
	(Mandatory: Storage)		(Migration Profile)		
	Same format as source	~	(Optional: Switchover Schedule)		0
> Switchover:					
Extended Options: Edit Extended Options					
O selected				9	
VM for Migration	Disk / Memory / vCPU		Migration Info		
C Loading data					

3. Add a group name and under Transfer and Placement, update the mandatory fields (Cluster, Storage, and Destination Network), Click Validate.

> Ø Source: VMware-HCX-440 / VC → Ø Destination: HCX Cloud - FSxN	DemoSDDC / V	dc.com C vcenter.sddc-54-188-6-128.vmware	mc.com		C Deload Cornect
roup Name: vMotion-vm14-2/vmc			Batch size: 1vm	/ 2GB/ 2GB/ 1v	
 Transfer and Placement: 					
Compute-ResourcePool	2	DemoD\$01 (IE-4 GB/10 TB)		vMotion	~
Workloads		Same format as source	×	(Optional: Switchover Sched	ule) O
Switchover: Force Power-off VM		Remove Shapshots Force unmount ISO Images			
v Extended Ontions		Core announ do majes			
Extended Options: Edit Extended Options Relative	NC)				a
East Extended Options Reliais M	NC)	Disk / Memory / vCPU		Migration Info	β.
Edit Extended Options Retain M VM for Migration • HCX_Photon_14	<u>xc</u>) •	Disk / Memory / vCPU 2 GB / 2 GB / 1 vCPU			4
Edit Ectended Options Relative		Disk / Memory / vCPU		Migration Info	۹.

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



The vMotion transfer captures the VM active memory, its execution state, its IP address, and its MAC address. For more information about the requirements and limitations of HCX vMotion, see Understanding VMware HCX vMotion and Cold Migration.

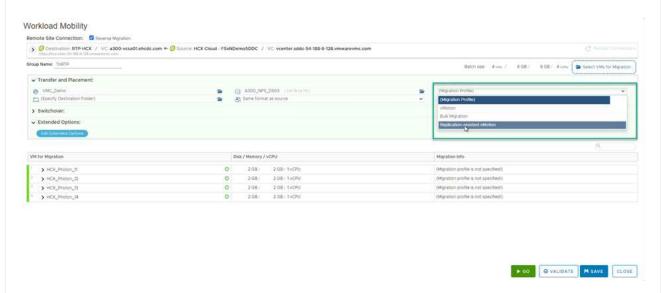
5. You can monitor the progress and completion of the vMotion from the HCX > Migration dashboard.

	٤.,	Migration								
NCX		A TANKA AND								
infrastructure	1322	= Tracking E Macagement	E [21 HO	FATE C	LCC.					
Site Parmy	Ť	Auror		au 201-1000 Mar-	est Disa	Б	Progress	Mart	Test.	(manual
A interconnect M Transport Analytics		 a 300-vcsa01 ehcdc.com 	1 A	Aller school 64	188-6-128 w	15	LESNIC A.	L million	11.025	L9MW.
Services		v vikilion entit 2 enc		t: 108-			00% New Sym. Golf I Highest	10	12	00
Natwork Estanaion Migration	-	0 Orrandet					Real (Distance)		Brenca saaraar	
Disaider Recovery System		1 D MICONNE,14	-	2 08	206.1	2		DA-SS He Data 12		Subdiview started
C hippint		Destanting Descention - Discount	ResourceMan	Duk Forma	e 1. 408, waking birt	APPENDED BY DEVELOP			110-46a3-9031-20193a71di	
₽ lupeort		Destination Desconder - Di 5000 Destination Fisiker - Di Voluki Myrellen Optime - Reden M	Ostacenter ods	0			10 Mainter	gatar Polle & Arking gatar Polle & Arking amar Waler & Math Name VMC C Events Dat Calester		
€ hoport		Destination Failur - Co Works Mayation Options - Chalain M	Ostacenter ods w.) (Remove IBC	0		ei -	18 Maintee Serife Settemer Einrie	Iguiter Polite (2) William umar Wesley (2) Pol Sch a Mark Name (VMC C Events		
₽ liseent		Destination Future - 🕑 Works Mignificat Optimes - Chalan M	Ostacenter ods w.) (Remove IBC	e) O DELMORE	5-3505-a0041a0	4C	18 Mainter Servic Sectorer Correle 1 militage	Iguiter Polite (2) William umar Wesley (2) Pol Sch a Mark Name (VMC C Events		
₽ liseent		Contraction Pattern (E) Works Magnitum Optimes (Citation M	Ostacenter ods w.) (Remove IBC	 101 (M) (M) 101 (M) (M) 	6-3505-4004140 8-08:- 4	4 	ja Mantu Sovie Sov	Iguiter Polite (2) William umar Wesley (2) Pol Sch a Mark Name (VMC C Events		
₽ liseent		Destination Future C Works Majoriter Optime C Reserve 2 Control 28 2 Well-49	Ostacenter ods w.) (Remove IBC	E) A tou 4 tou 4 tou	8 3505 40041 ad 8 08 - 4 8 08 - 4	4	ia Maine Sente Sente Sente Migratus Company Migratus Company Migratus Company	Iguiter Polite (2) William umar Wesley (2) Pol Sch a Mark Name (VMC C Events		
		Contraction Fundament Adaption Cottons (Index Of Science Of Science Of Science Of Science Of Science Of Science Of Science Of Science Of Scienc	Ostacenter ods w.) (Remove IBC	t 100 t 100 t 100 € C1217AN 360	8-08-4 8-08-4 8-08-4 2-08-1 2-08-1	4 4 4	a Marine Serie Serie Maystan Complete Maystan Complete Maystan Complete Maystan Complete	Iguiter Polite (2) William umar Wesley (2) Pol Sch a Mark Name (VMC C Events		
 Recent Taska Alarma 	T torus	Destination Fundare (E) 200444 Magnation Optimise (Entrine M) Contrib 20) VANNE JP) VANNE JP) 2022 05-12 20145 (EVVPO	Ostacenter ods w.) (Remove IBC	C 200 4 100 4 100 1 200 1	8 3505 400 81 40 8 08 4 8 08 5 2 08 5 2 08 7 2 08 1	4 4 4	IN Network Servic Servic 2 Martine Complete 2 Martine Complete	Iguiter Polite (2) William umar Wesley (2) Pol Sch a Mark Name (VMC C Events	ndunt ner te ditalte	
 Becent Tasks Alarms 	T tous	Contraction Fundare (1) 1999/44 Adjustion Cystown (1) Index M > Contract 20 > WebSite > 2002 01 12 20xet (1997 O - 2002 01 12 20xet (1997 O	Optioneter och an (hannen BC C VM(2002 + VM(2002 +	 P. 208 P. 208	8 3005 400 41 44 8 08 4 8 08 4 1 08 1 1 08 1 1 08 1 1 08 1 1 08 1		IN Network Servic Servic 2 Martine Complete 2 Martine Complete	gante Piolite di Materia una l'Indez El to Silo e Arabi Nace Ceventa Inat Calvesta I	ndunt Innere delatis	

VMware Replication Assisted vMotion

As you might have noticed from VMware documentation, VMware HCX Replication Assisted vMotion (RAV) combines the benefits of bulk migration and vMotion. Bulk migration uses vSphere Replication to migrate multiple VMs in parallel—the VM gets rebooted during switchover. HCX vMotion migrates with no downtime, but it is performed serially one VM at a time in a replication group. RAV replicates the VM in parallel and keeps it in sync until the switchover window. During the switchover process, it migrates one VM at a time with no downtime for the VM.

The following screenshot show the migration profile as Replication Assisted vMotion.



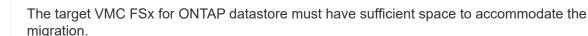
The duration of the replication might be longer compared to the vMotion of a small number of VMs. With RAV, only sync the deltas and include the memory contents. The following is a screenshot of the migration status—it shows how the start time of the migration is the same and the end time is different for each VM.

vSphere Client. (2														9	5	S chooledwide	Hickologi 🗸 🗌 🧯	<i>.</i> e
	<	Migratio	00																
CX .		1000000000			_			-											
Dishbord		(8,7)4	oling El Manag	enert	L C HOA	ATE] [(g 3 1.0											(mapping)	
shadruchare	~																		
O Ste Farmy		Barre				whit the	nyn/ Harri	erg/ CPUs		117					liari	Deal		liniar	
15 francourt Analytics		-	conter sidde-S44	88-6-128	mwarevm	ecom -		300 west	Otehcidic.com										
er si cen	~	~ 100	17				\$ 145	1.08	1	0	Agentium Co	-	N						00
Antwork Evenenic																			
Mgration *D Departer Recounty							110	100							1.20 m			Margher campiled	
			3 HCR, Photon, 12		-		1.00			0	Agradian Co	et planta			4-00	140		adding contrast	
Americani	~	10	3 HCR, Photon, 52		0		2.08	3.08	1	01	Againter Ca	-			0.20.84	83.54		Meator convolution	
Characteria		10	> HDK, Photos, 13		63		2.08	2.08	1	21		et prime			1.20 me n 31	03.6		Mpation completed	
		10	> HOL/Holder, H	5	-		208	210		01	No Hand Co	-			0.20 mil	83.5	S Par	Migrature completed	
		> 210	1.00.22 15:24 INTY				\$ 09	3.00		0	hy days in	-							
		·	centersiddc-54-1	88-6-128	mwarenm	c.com (- 44	300-vcsa	01.ehcdc.com										
		5 Free	9879			*	1.02	8.05	4	0	hy it in th	et giante	N.	1		-			
Fecers Tasks Alar	74																		
six Barre T. 5	e pet	•	Shelve		Deprin .		,	between		٠	fumet No	•	Stat Time	1.7	Constantion Time	*	Sever		
iebłe ietus machine 🛛 👌	2 -CX, Shaton, R, Shado	e.)	Q-Completed					VMCLO	AUM menshator		2.05		0%/ZM/2022.4	1004	06/23/2022. 4 111	U	vpantar sodo-54 8	ID-5-DE umaneuro	e.com
regiber orbat mattere	\$ HCK_Platin_1		Occumenter					VMCLO	au Valence en		2.00		29/25/2023 4	23.03	09/25/2022 4:03:0	19	venter solde-54 til	IS S OL INVITED	c.com
etrephysical machine x. {	# HCK_Photon_R		Companies .					VMCLO	ALC-Administrator		4.75		08/21/2022.4		09/35/0022.4 03 0	19.	stander abbi 54-5	ID-5 CE empresente	c.com
	3 HOL/Instan_5		 Completed 		Heating	Virtual Maid	héa ác	VHCLO	ALLASHING ALLAS		4.0%		-06/25/2022 #1	0.55	00/25/0022 #01/0	2.2%4	stanter add: 54.8	ID 4. C2 House and	4.49PP
	3 scoclassese		@-Companied					WCLO	ALM-environmentation		3.64		08/23/2022 31	0.47	00/35/0022.558.4	ė	vianter abdod4.8	ISA OL maxim	
Refresh host storage sys.	5 172 55 WIL258		@ Completing					WHICKON	a:\Administration		4.000		OW/25/2022. 81	HTTP.	00/03/2022 8581	1.0	vienter side-54 8	15-6-CH Lamoret	ciel in

For additional information about the HCX migration options and on how to migrate workloads from onpremises to VMware Cloud on AWS using HCX, see the VMware HCX User Guide.



VMware HCX vMotion requires 100Mbps or higher throughput capability.



Conclusion

Whether you are targeting all-cloud or hybrid cloud and data residing on any type/vendor storage in onpremises, Amazon FSx for NetApp ONTAP along with HCX provide excellent options to deploy and migrate the workloads while reducing the TCO by making the data requirements seamless to the application layer. Whatever the use case, choose VMC along with FSx for ONTAP datastore for rapid realization of cloud benefits, consistent infrastructure, and operations across on-premises and multiple clouds, bidirectional portability of workloads, and enterprise-grade capacity and performance. It is the same familiar process and procedures used to connect the storage and migrate VMs using VMware vSphere replication, VMware vMotion or even NFC copy.

Takeaways

The key points of this document include:

- You can now use Amazon FSx ONTAP as a datastore with VMC SDDC.
- You can easily migrate data from any on-premises datacenter to VMC running with FSx for ONTAP datastore
- You can easily grow and shrink the FSx ONTAP datastore to meet the capacity and performance requirements during migration activity.

Where to find additional information

To learn more about the information described in this document, refer to the following website links:

VMware Cloud documentation

https://docs.vmware.com/en/VMware-Cloud-on-AWS/

Amazon FSx for NetApp ONTAP documentation

https://docs.aws.amazon.com/fsx/latest/ONTAPGuide

VMware HCX User Guide

• https://docs.vmware.com/en/VMware-HCX/4.4/hcx-user-guide/GUID-BFD7E194-CFE5-4259-B74B-991B26A51758.html

Region Availability – Supplemental NFS datastore for VMC

Learn more about the the Global Region support for AWS, VMC and FSx ONTAP.



NFS datastore will be available in regions where both services (VMC and FSx ONTAP) are available.

The availability of supplemental NFS datastores on AWS / VMC is defined by Amazon. First, you need to

determine if both VMC and FSxN are available in a specified region. Next, you need to determine if the FSxN supplemental NFS datastore is supported in that region.

- Check the availability of VMC here.
- Amazon's pricing guide offers information on where FSxN (FSx ONTAP) is available. You can find that information here.
- Availability of the FSxN supplemental NFS datastore for VMC is coming soon.

While information is still being released, the following chart identifies the current support for VMC, FSxN and FSxN as a supplemental NFS datastore.

Americas

AWS Region	VMC Availability	FSx ONTAP Availability	NFS Datastore Availability
US East (Northern Virginia)	Yes	Yes	Yes
US East (Ohio)	Yes	Yes	Yes
US West (Northern California)	Yes	No	No
US West (Oregon)	Yes	Yes	Yes
GovCloud (US West)	Yes	Yes	Yes
Canada (Central)	Yes	Yes	Yes
South America (Sao Paulo)	Yes	Yes	Yes

Last updated on: June 2, 2022.

EMEA

AWS Region	VMC Availability	FSx ONTAP Availability	NFS Datastore Availability
Europe (Ireland)	Yes	Yes	Yes
Europe (London)	Yes	Yes	Yes
Europe (Frankfurt)	Yes	Yes	Yes
Europe (Paris)	Yes	Yes	Yes
Europe (Milan)	Yes	Yes	Yes
Europe (Stockholm)	Yes	Yes	Yes

Last updated on: June 2, 2022.

Asia Pacific

AWS Region	VMC Availability	FSx ONTAP Availability	NFS Datastore Availability
Asia Pacific (Sydney)	Yes	Yes	Yes
Asia Pacific (Tokyo)	Yes	Yes	Yes
Asia Pacific (Osaka)	Yes	No	No
Asia Pacific (Singapore)	Yes	Yes	Yes
Asia Pacific (Seoul)	Yes	Yes	Yes
Asia Pacific (Mumbai)	Yes	Yes	Yes
Asia Pacific (Jakarta)	No	No	No
Asia Pacific (Hong Kong) Yes	Yes	Yes

NetApp for Azure / AVS

NetApp Capabilities for Azure AVS

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

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

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

Configuring AVS in Azure

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

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



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

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

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

View the detailed configuration steps for AVS.

NetApp Storage Options for AVS

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

Please visit Supported NetApp Storage Options for more information.

Azure supports NetApp storage in the following configurations:

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

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

Solution Use Cases

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

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

Browse the NetApp solutions for Azure AVS

Protecting Workloads on Azure / AVS

Disaster Recovery with ANF and JetStream

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

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

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

- 1. Install JetStream DR software in the on-premises data center.
 - a. Download the JetStream DR software bundle from Azure Marketplace (ZIP) and deploy the JetStream DR MSA (OVA) in the designated cluster.
 - b. Configure the cluster with the I/O filter package (install JetStream VIB).
 - c. Provision Azure Blob (Azure Storage Account) in the same region as the DR AVS cluster.
 - d. Deploy DRVA appliances and assign replication log volumes (VMDK from existing datastore or shared iSCSI storage).
 - e. Create protected domains (groups of related VMs) and assign DRVAs and Azure Blob Storage/ANF.
 - f. Start protection.
- 2. Install JetStream DR software in the Azure VMware Solution private cloud.
 - a. Use the Run command to install and configure JetStream DR.
 - b. Add the same Azure Blob container and discover domains using the Scan Domains option.
 - c. Deploy required DRVA appliances.
 - d. Create replication log volumes using available vSAN or ANF datastores.
 - e. Import protected domains and configure RocVA (recovery VA) to use ANF datastore for VM placements.
 - f. Select the appropriate failover option and start continuous rehydration for near-zero RTO domains or VMs.
- 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 ② ~ Administrator@EHCDC.COM ~ (
☐ ☑ ◎ ☑ □ ○	Magazina A300-DataCent	Pr ACTIONS ~	8.
 A300-DataCenter A300-Cluster a300-esxi02.eh 	 More Alarm Definitions Scheduled Tasks 	Jet/Stiream DR Protected Domains Statistics Storage Sites Appliances Configurations Ta	ask Log
a300-esxi03.eh	Network Protocol Pr	Site Details	Alarm Settings
a300-esxi05.eh		vCenter Server Hostname 172 21 253 160	
ANFJSDR-MSA0		Management Appliance Hostname ANFJSDR-msa	
AuctionAppA0		Software Version 4.0.0.443	
🔂 AuctionAppA2		Subscription ID 0000000-0000-0000-0000-000000000000	1 Configure
AuctionAppA3		Tenant ID / Application ID - Configure	
🖧 AuctionAppB0		Application Secret + Configure	

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

ite Details							Alam	
/Center Server Hostname		172.21.253.160						
Management Appliance Hostname		SNC IODD						
Software Version	Configure	Clusters						
Subscription ID					-	٩		
fenant ID / Application ID				Select All	Clear All	, ~		
Application Secret	the second secon	ter Name 🔺		enter Name 🔺		^		
Configured Clusters	A300-	-Cluster	A300-	DataCenter				
Configure Cluster								C
Cluster Name 🔺						~	Host Details 🔺	
No cluster contigured				c	ancel 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 Applia	ince (DRVA)				Ê
DRVAs (DR Virtual Appliances)	1. General	2. DRVA VM 3. DRVA Netv	work 4. Summa	ry		
+ Deploy New DRVA DPgrade	Name	ANFdemo001		^		Q
Name 🔺	Description (Optional)				Details 🔺	
No DR Virtual Appliance configured.	Datacenter	A300-DataCenter				
	Cluster	A300-Cluster				
	Resource Pool (Optional)	-				
	VM Folder (Optional)	-				\sim
Replication Log Volume	Datastore	A300_NFS_DS04				
	Number Of CPUs	8		- 15		0
+ New Replication Log Volume	Memory Size	32GB				Q
Disk Path Name 🔺	Management Network	VM_187			Details 🔺	
No DRVA selected. Select a DRVA to vi	Host(iofilter) to DRVA Data Net	twork VM_187				
	Replication Network to Object	t Store VM_187				
	Replication Log Network	VM_187		\sim		\sim
		Cancel	Back Deple	by		

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.

elect Protected Domain: ANFPD001	Start Protection				reate 🛍 Delete	
ecoverable / Total VMs	Protection Mode for selected VMs Write-Back(VMDK)			q		Edit Detai
eplication Status	VM Name ▲		. Protection Mode	~	ANFDemoblobrepo AL (172.21.253.160)	1
emaining Background Data	1	×			0-DataCenter \ A300-Cluster	
urrent RPO	AuctionAppA1	1	Write-Back(VMDK) v	^	bled	
	AuctionAppB1	1	Write-Back(VMDK) V			
Protected VMs Settings Ala	AuctionDB1	2	Write-Back(VMDK) v			
	AuctionLB1	1	Write-Back(VMDK) V			
+ Start Protection	AuctionMSQ1	1	Write-Back(VMDK) V			Q
	AuctionNoSQL1	2	Write-Back(VMDK) v		increased Data Datalla	
VM Name 🔺	AuctionWebA1	1	Write-Back(VMDK) V		kground Dat Details	
No VM is protected.	AuctionWebB1	1	Write-Back(VMDK) V			
	Client1	1	Write-Back(VMDK) V	0		
		2	(•		
		1		~		

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+/)	🔿 Rehish 🔗 Feedback		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* ()
Clusters		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	
4 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
. MIR.			
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.

Site Details						Alerna Coll	11
Site Details						Alarm Set	un
vCenter Server Hostname	172.30.15	6.2					
Management Appliance Hostname	anfjsval-m	sa					
Software Version	4.0.2.450						
Subscription ID	- <u>Configu</u>	re					
Tenant ID / Application ID	- Configu	re					
Application Secret	- Configu	re					
Configure Cluster	Duconfigure	🛠 Resolv	e Configure I	ssue			(
Cluster Name	Datacenter I	Name 🔺	Status	Softwar	re Version 🔺	Host Details	
Cluster-1	SDDC-Datac	enter	🕝 Ok	4.0.2.13	2	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.

Protected Domain	Description	Recoverable V	VMs	Import		^
ANFPD000	Protected Domain Tile0	20	20	Import	^	188
ANFPD001	ŧ	20	20	Import		
ANFPD002	Protected Domain 02	20	20	Import		180
ANFPD003	Protected Domain Tile 03	20	20	Import	~	
<					>	185
						- 84
Si						
c						~

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.

Select Protected Domain: Continuous Failover Protected Domain									≡Mor	
le	•	•	•			•				Det
overable / Total VMs	1. General	2a. Failover Settings	2b. VM Settings	3. Reco	very VA	4. DR Settings	5. Summary	▲ reporec		
Protected Domain Name			ANFPD002			253.160)				
Datacenter				SDDC-Data	enter			1000		
	Cluster			Cluster-1	enter			1000		
		ool (Optional)		-				1000		
otected VMs Setti	VM Folder (-				1000		
	Datastore			ANFRecoDS	J002			1000		
	Internal Net	twork		DRSeg				1000		3
VM Name 🛦	External Re	plication Network		DRSeg				1.000	Details	
AuctionAppA2	Managemei	nt Network		DRSeg				1000	Details	
AuctionAppB2	Storage Site	9		ANFDemoble	breporec				Details	
AuctionDB2	DR Virtual A	ppliance		ANFRecDRV	A003				Details	
AuctionLB2	Doplication	l on Storano		idoviedh				¥	Details	
AuctionMSQ2					Cancel	Back	Continuous Failov	er	Details	

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

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

Protected Domains Statistics	Storag	je Sites A	ppliances	Configurat	ions	Task Log	_
Select Protected Domain: ANFPD	• 0000	View all		+ Create		Delete	■Mor
Mode		Imported	Configura	tions		O Restore	
Recoverable / Total VMs		20 / 20	Storage Sit	te	1	→ Failover	
			Owner Site	í.	RE	→ Continuo	us Failover
						→ Test Faild	over
Protected VMs Settings	Alarms						
VM Name 🔺		Protecti	on Status 🔺		Protectio	on Mode 🛦	Details
AuctionAppA0		Record	/erable		Write-Bac	:k(VMDK)	Details
AuctionAppB0		Record	(erable		Write-Bar	k(VMDK)	Details

Performing Failover / Failback

 (\mathbf{i})

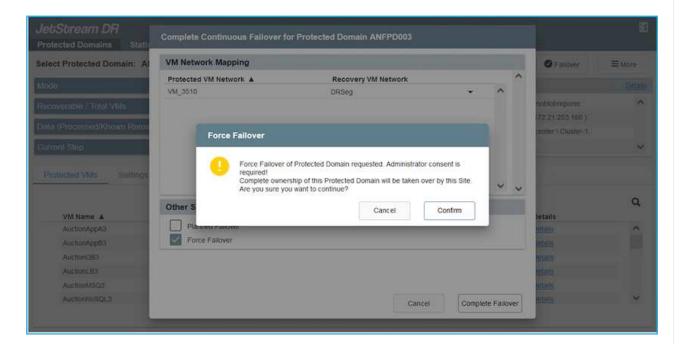
1. After a disaster occurs in the protected cluster of the on-premises environment (partial or full failure), trigger the failover.



÷

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

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



Protected Domains Statistics	Storage Sites Appliances Configurations Task Log	_		
Select Protected Domain: ANFPD00	3 👻 View all		+ Create	≡More
Mode	Task Steps			Detail
Recoverable / Total VMs	laan olepa		ANFDemobiobreporec	~
	Prerequisite checks	^	MOTE (172.21.253.160)	
Data (Processed/Known Remaining)	Prepare for rehydration	1	C-Datacenter \ Cluster-1	
Current Step	 Prepare Recovery VM ISOs 		ibled	~
	Recreate Protected Domain on DRVA.			
Protected VMs Settings Al	Prepare temporary Recovery VMs	- 10		
	 Power on and retrieve Recovery VMs' IPs 	- 11		
	Recover VMs' data from Storage Site	- 11		Q
VM Name 🔺	Take Protected Domain ownership Finalize rehydration		Details	
AuctionAppA3	Initialize DR Protection Mode	- 10	Details	^
AuctionAppB3	Clean up temporary Recovery VMs	- 11	Details	
Auction/DB3	Resume Protected Domain protection		Details	
AuctionLB3	Finalize recovered VMs		Details	
AuctionMSQ3	Apply DR resumption storage policy		Octails	
AuctionNoSQL3	A Everute runbook	~	Details	~

The task bar shows progress of failover activities.

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

letStream DR Protected Domains	f Stati	Continuous Rehydration Task Result					1
elect Protected Dor	nain: Al	Task Completed Successfully				Delete	≡ More
lode -						1	dt Detai
	-	Protected Domain	ANFPD003				^
ecoverable / Total VI	vis.	VMs Recovery Status	Success			nobiobreporec	^
eplication Status		Total VMs Recovered	20			2 30 156 2)	
		testFGP0 Status:				center \ Cluster-1	
emaining Backgroun	d Data	Pre-script Execution Status	Not defined				
urrent RPO		Runbook Execution Status	Success				~
		Post-script Execution Status	Not defined				
Protected VMs	Settings						
+ Start Protection	1 15kg P						۹
VM Name A						d D Details	
AuctionAppA3						Details	^
AuctionApp83						Details	
AuctionDB3						Details	
AuctionLB3						Details	
AuctionMSQ3					Dismiss	Details	
AuctionNoSQL3	-	IN ROCURCIALIO	u un	THE DULLYMUN	va	Details	×

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.

elect Protected Domai	Failback Prote	ected Domain						Delete	≡ More
lode	 General 	2a. Failback Settings	2b. VM Settings	3. Recovery VA	4. DR Settin	gs 5.	Summary		Edit Deta
ctive Site		1949-1957 - 1977 - 1977 - 1977 - 1977 - 1977 - 1977 - 1977 - 1977 - 1977 - 1977 - 1977 - 1977 - 1977 - 1977 - 1 1977 - 1977 - 1977 - 1977 - 1977 - 1977 - 1977 - 1977 - 1977 - 1977 - 1977 - 1977 - 1977 - 1977 - 1977 - 1977 -		534194959C 65 ⁴⁴ (2004)		Teol () (^ 100	1
ecoverable / Total VMs	Protected D	omain Name		ANFPD003				56.2)	
	Failback Dat	tacenter		A300-DataCenter					
	Failback Clu	uster		A300-Cluster				-	1
Protected VMs Se	Failback Re	source Pool		÷.					
Protected VMS Se	VM Folder (Optional)		8					
	Failback Dat	tastore		A300_NFS_DS02				- 200	Q
VM Name	Maximum D	elay After Stopping		60 Minutes					
AuctionAppA3	Internal Net	work		VM_187					^
AuctionAppB3	External Re	plication Network		VM_187					
Aller a	Managemer	nt Network		VM_187				~	
AuctionDB3									

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

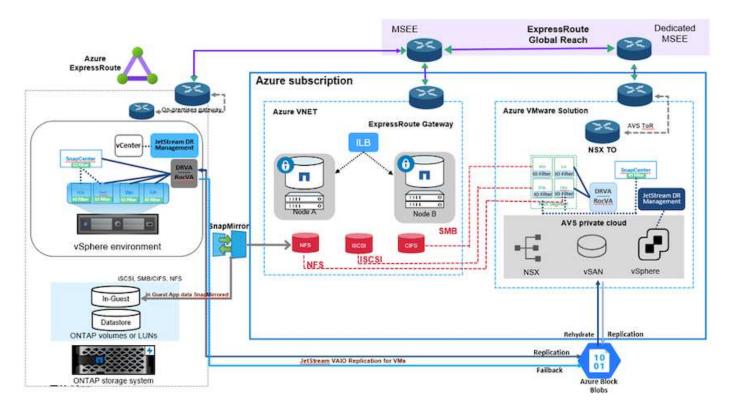
Disaster recovery to cloud is a resilient and cost-effective way of protecting workloads against site outages and data corruption events such as ransomware. With NetApp SnapMirror, on-premises VMware workloads that use guest-connected storage can be replicated to NetApp Cloud Volumes ONTAP running in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

Overview

Authors: Ravi BCB and Niyaz Mohamed, NetApp

This covers application data; however, what about the actual VMs themselves. Disaster recovery should cover all dependent components, including virtual machines, VMDKs, application data, and more. To accomplish this, SnapMirror along with Jetstream can be used to seamlessly recover workloads replicated from on-premises to Cloud Volumes ONTAP while using vSAN storage for VM VMDKs.

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



Assumptions

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



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

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



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

Deploying the DR Solution

Solution Deployment Overview

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

Deployment Details

Configure CVO on Azure and replicate volumes to CVO

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

Health Status 🕴	Source Volume	Target Volume =	Total Transfer Ti	me e	Status	Mirror State	Last Successful Transfer	(+
0	gcsdrsqldb_sc46 ntaphci-a300e9u25	gcsdrsqldb_sc46_copy ANFCVODRDemo	17 seconds		idle	snapmirrored	May 6, 2022, 11:43:18 AM 105.06 KiB	
\odot	gcsdrsqlhld_sc46_copy ANFCVODRDemo	gcsdrsqlhid_sc46 ntaphci-a300e9u25	7 seconds		idle.	snapmirrored	May 6, 2022, 11:42:20 AN 7.22 MiB	
\odot	gcsdrsqilog_sc46 ntaphci-a300e9u25	gcsdrsqilog_sc46_copy ANFCVODRDemo	16 seconds		idle	snapmirrored	May 6, 2022, 11:43:52 AN 130.69 KiB	

Configure AVS hosts and CVO data access

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

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

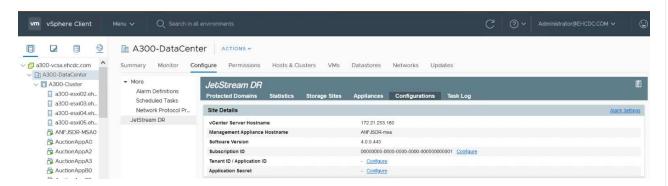
The most common deployed option is to have SDDC running in an always-on, pilot-light mode of operation. This option provides a small footprint of three hosts that are always available, and it also speeds up recovery operations by providing a running baseline for simulation activities and compliance checks,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

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

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

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

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



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

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

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

Storage Sites	Add Storage Site	
+ Add Storage Site Scan Donaun	Storage Site Type *	
Name A	Azure Blob Storage	
No Storage Site configured.		
	Access Type *	
	Key Access	
	Storage Site Name (Provide a name to identify this Site) *	
	ANFDemoblobrepo	
Storage Site Details Alarms		
	Azure Blob Storage Account Name.*	
No storage site selected. Select a storage		
The storage and selection ouncer a storage	Aqure Bob Storage Account Key *	
	······································	
	Cancel Add Storage Site	

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

(i)

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

JebSbream DR Protected Domains Statistics Storage Sites Applian	ces Configurations	Task Log			Ē
DRVAs (DR Virtual Appliances)					
+ Deprog New DRVA TUpgrade TUpgrade					٩
Name 🔺	Status 🔺	Child Alarm 🔺	Software Version 🔺	Details 🔺	
No DR Virtual Appliance configured.					
					ν.
Replication Log Volume					
+ New Replication Log Volume					a
Disk Path Name 🔺	Status	Child Alarm 🔺	Size (available/total)	Details 🔺	
No DRVA selected. Select a DRVA to view replication log volumes.					

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

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

Jet/Stream DR Protected Domains	Statistics	Storage Sites	Appliances	Configurations	Task Log			
DRVAs (DR Virtual A	ppliances)	L2						
+ Deploy New DRVA	* Courada	D Unconfigure						q
Name A				Status A	Child Alarm 🔺	Software Version	Details A	
GCSDRPD001				O Running	00	4.0.0.134	Detain	
+ New Replication Log		condure.						a
Disk Path Name A				Status.	Child Alarm	Size (available/total) 🔺	Details A	
idev/sco				O Ok	0 0	179 88 GB / 200 GB	Detats	
Replication Log Volu	ume Details							
the randomation ten uniter	a coloriari Galar	t a unknown to user dat	alla					

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 With			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 C.	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	10.1	
	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	tes Appliances Configuration	ons Task Log				Running Tasks	
elect Protected Domain: GCSDRPD_Demo01	<u>View all</u>				+ (Start Protection (GCS-DR-SCA) 509	i.
tecoverable / Total VMs		0/5	Configurations			Start Protection (GCS-DR-Win 50%	6
eplication Status		ок	Storage Site		ANFDRDe	Start Protection (GCS-DR-Lin 50%	
emaining Background Data		0 B	Owner Site Datacenter \ Cluste	ar.	LOCAL (172.2 A300-DataCen	Start Protection (GCS-DR-DC) 50%	
urrent RPO			Point-in-time Reco	very	Disabled	Start Protection (GCS-DR-SQ 50%	6
Protected VMs Settings Alarms						Configure VMDK Re Completed	
+ Start Protection							10
T Start Protection				52555 N 81 82581	Decision of Dec	ta 🔺 Details	
Start Protection William Stap Protection VM Name	Protection Status	Replication Sta	tus 🔺	Protection Mode	Background Dat		
Construction of the second s	Protection Status Protection Status Protection Status	Replication Sta	tus 🔺	Protection Mode Write-Back(VMDK)	-	Details	1
VM Name 🔺			tus 🛦				14
O VM Name ▲ O GCS-DR-DC	Initializing		tus 🔺	Write-Back(VMDK)		Details	18
VM Name GCS-DR-DC GCS-DR-LinVM01	Initializing Initializing	*	tus 🔺	Write-Back(VMDK) Write-Back(VMDK)	•	Details Details	

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

Jet/Stream 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	
lecoverable / Total VMs		5/5	Configurations			Edit Detail	
eplication Status		OK	Storage Site	ANFDRDemoFailo	ANFDRDemoFailoverSite		
		1.00	Owner Site	LOCAL (172 21 253 1	50)		
temaining Background Data		08	Datacenter \ Cluster	A300-DataCenter \ A30	00-DataCenter \ A300-Cluster		
Lurrent RPO		05	Point-in-time Recovery	Disabled	Disabled		
Distactort VMc Cattings Alarms							
Protected VMs Settings: Alarms Start Protection VM Name	Protection Status	Replication St	atus 🔺 Protection Mode 🔺	Background Data 🔺	Details	٩	
+ Start Protection		Replication St	atus 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)	0.8	Details	٩	
+ Start Protection VM Name GCS-DR-DC GCS-DR-LinVM01	Protection Status ▲ © Recoverable © Recoverable	o ok o 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.

(i)

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

Protected Domains Statistics Storage Sites Appliances Configurations Task Log			-				
Select Protected Domain: GCSDRPD_Demo01 View all		+ Create	Delete	≡ More			
Recoverable / Total VMs 5 / 5	Configurations			Edit Detail			
Replication Status OK	Storage Site	ANFDRDemoFailov	erSite	3			
	Owner Site LOCAL (172 21.253 160)						
Remaining Background Data 0 B	Datacenter \ Cluster A300-DataCenter \ A300-Cluster						
Current RPO 0s	Point-in-time Recovery	Disabled					
0 0							
Protected VMs Settings Alarms							
Failover Runbook Not Configured Configure							
Test Fallover Runbook Not Configured Configure							
Faliback Runbook 💭 Not Configured Configure							
Memory Setting Not Configured Configure							
GC Settings 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	E Celitte	≡ 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: GCSDRPD Demo					0				+ Create	Delete	1
	1. General	2. Select VM	5	3. Edit V	M Settings		4. Summa	ary .		1 MARCENT	
Recoverable // Total VMs	Retain MAC		Power Of	f VMs			O Reset	1 1			
Replication Status	VM Name	Boot Sequence	Root Delay	CPU	Memory	Script	NIC		DRDnmoFalloyn		
Remaining Background Data	GCS-DR-WinVM01	1↑↓	Os	32	64 GB	Config		22			
NAME OF COMPANY OF COMPANY	GCS-DR-SCA	21 1	Qs	4	16 GB	Contig	3				
Clateri RPO	GCS-DR-LinVM01	3↑ ↓	0s	2	4 GB	Config	View				
Protected Ville Settings Alarma	GCS-DR-SQL0	47 4	0s	4	8 GB	Config	View				
	GCS-DR-DC	51 4	0s.	4	16 GB	Config	View	÷.			
Concurrency Settings Not Configured Comburg.											
								_			

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

Label		Network Name	Key	PCI Slot #	IP	
245 Tak	cadapter 1	VM_3510	4000	192	Configure	aix
Re						
VM No						
GCS-E	Configur	e Static IP Address				
Cibunh						
GCSD GCS-E	IP Address *					
0-0	172.21.2	54.185			_	
.00	Subnet Mask	-				
	255.255.2					
	1100.001.000.000				_	
	Gateway *					
	172.21.2	54,1				
	DNS +					
	172.30.1	53.20				
	200000	52.73				
	DNS Suff	be .				
		Reset	Canc	el Confi	gure Im	
				5		
					Close	Next
bStream DR	Create Runt	oook Group				
Rector Department Subtraction	nur-og i service a		3. Edit VM Si	tüngs 4. Summ	+oun)	
	Group Na	me	GCSRecovery		•	
	Number o Retain VM	f VMs Fs MAC addresses	5 true		PERMIT PLANE	
	Power Of	VMs	false		And and I All Spice	
	Te Group	menganitig and boot sequence change will	be applied to both Fallover a	nd 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-PreflightJetDRInutal	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 ()
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.

JetStream DR Protected Domains Statistics Storage Sites	Available Protected	Domain(s) For Impor	t					Ē
Storage Sites + Add Storage Site Constant Storage Site	Protected Domain GCSDRPD_Demo01	Description Protection domain ANF	Recoverable V 5	VMs 5	Import Import	^		Q
Name A ANFDemobilotrepored							ee Blob Storage	^

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

Select Protected Domain: GCSDRPD_Demo01 View all			+ Create	Delete	■More
Mode	Imported	Configurations			Deta
Recoverable / Total VMs	5/5	Storage Site	ANFDemoblobrer	orec	
		Owner Site	-		
					c
VII Name	Protection Status	*	Protection Mode	Details	c
VM Name A GCS-DR-DC	Protection Status Protection Status	•	Protection Mode Write-Back(VMDK)	Details Details	
		•			
GCS-DR-DC	Recoverable	•	Write-Back(VMDK)	Details	c
GCS-DR-DC GCS-DR-LinVM01	Recoverable Recoverable	• •	Write-Back(VMDK) Write-Back(VMDK)	Details Details	

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

 (\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
đo	1. General	2a. Failover Settings	2b. VM Settings	1 Per	overy VA	4. DR Settings	5. Summary			Dela
coverable / Total VMs	1. General	za. ranover settings	zo, vin settings	s. Neu	overy w	4. Dr. astungs	o. ouninary	~ reporec		2
	Protected D	omain Name		ANFPD002				253,160)		
	Datacenter			SDDC-Data	center					
	Cluster			Cluster-1				1000		1
	Resource P	ool (Optional)		•				1000		
rotected VMs Setti	VM Folder (Optional)		÷.				1.000		
	Datastore			ANFRecoDS	0002			100		-
	Internal Net	work		DRSeg					-	C
VM Name A AuctionAppA2	External Re	plication Network		DRSeg					Details	1
AuctionAppB2	Managemer	nt Network		DRSeg				1000	Details	
AuctionDB2	Storage Site	•		ANFDemobi	obreporec			1000	Details	
AuctionLB2	DR Virtual A	ppliance		ANFRecDRV	/A003			~	Details	
AuctionMSQ2	Bonlightion	I an Ptorsea		Mouladh				_	Details	
AuctionNoSQL2					Cancel	Back	Continuous Failov	er	Details	- 3

()

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).

JebSbream DR Protected Domains Statistics Storage Sites Appliances	Configurations Task	Log			
Select Protected Domain: GCSDRPD_Demo01 👻 View all			+ Create	Delete	≡ More
Mode	Imported	Configurations		O Restore	
Recoverable / Total VMs	5/5	Storage Site	ANFDemoblobrepor	→ Failover	
		Owner Site	REMOTE (172.21.253.16	→ Continuous Fai	lover.
				→ Test Failover	0
Protected VMs Settings Alarms O O					
VM Name 🔺	Protection Status		Protection Mode 🔺	Details	
GCS-DR-DC	Recoverable		Write-Back(VMDK)	Details	
GCS-DR-LinVM01	Ø Recoverable		Write-Back(VMDK)	Details	
GCS-DR-SCA	C Recoverable		Write-Back(VMDK)	Details	
GCS-DR-SQL01	O Recoverable		Write-Back(VMDK)	Details	
GCS-DR-WinVM01	Recoverable		Write-Back(VMDK)	Details	

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

Failover and Failback

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

	Colume II	elationships	4.78 GIB Replicated Capacity	0 Currently Trans	sterring	3 Healthy	8 0 Failed	
	3 Volume Relationships							٩
	Health Status	Source Volume	Target Volume T	0—0 Total Transfer Time 1	Status	≅ Mirror State	Last Successful Transfer	0
	0	gcsdrsqldb_sc46 ntaphci-a300e9u25	gcsdrsqldb_sc46_copy ANFCVODRDemo	6 minutes 41 seconds	idle	snapmirrored	May 5, 2022, 12:08:34 Ph 33.66 Ki8	
	0	gcsdrsq/hid_sc46 ntaphci-a300e9u25	gcsdrsqlhld_sc46_copy ANFCVODRDemo	4 minutes 56 seconds	idle	snapmirrored	Information	
	ø	gcsdrsqlfog_sc46 ntaphci-a300e9u25	gcsdrsqllog_sc46_copy ANFCVODRDemo	10 minutes 18 seconds	idle	snapmirrored	Break Reverse Resync	
	¢		· · · ·				Edit Schedule	
							Edit Max Transfer Rate	
							Update	
							Update Delete	
rs Replication	e 3	Data Sense	File Cache Compute	Sync All Service		S Healthy		
	e 3	elationships	4.78 GIB Replicated Capacity Break Relationship	0 Currently Tran	sferring	Healthy	Delete	C
	J Volume R	relationships	4.78 GIB Replicated Capacity Break Relationship	€→ 0	sferring	Healthy	Delete	_
	Volume Relationships	relationships	4.78 GIB Replicated Capacity Break Relationship Are you sure that you want 1	0 Currently Tran	sferring ween 'gcsdrsqld	Healthy	Delete	¢
	3 Volume Relationships Health Status :	elationships	4.78 GIB Replicated Capacity Break Relationship Are you sure that you want 1	0 Currently Tran	sferring ween 'gcsdrsqld	Healthy	Delete Delete Delete Last Successful Transfer May 5, 2022, 12:08:34 PM	Q • •

(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_Demo01	View all		+ Create	O Freilover	≡ Mor
Mode	Continuous Rehydration in Progress	Configurations			Details
Recoverable / Total VMs	4/4	Storage Site		porec	^
		Owner Site	REMOTE (172.21.25	3.160)	
Data (Processed/Known Remaining)	329.01 GB / 6.19 GB	Datacenter \ Cluster	SDDC-Datacenter \ C	Cluster-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	
GCS-DR-SCA	Recoverable		Write-Back(VMDK)	Detaits	
GCS-DR-SQL01	Recoverable		Write-Back(VMDK)	Details	
	Recoverable		Write-Back(VMDK)	Details	

Protected VM Network	Recovery VM Network		3
VM_3510	DRStretchSeg +	^	
0 0		v	
Other Settings Planned Fallover Force Failover			
Some VM's quest credential are requi	ired because of network configuration: Configure		

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

Ð	Force Failover of Protected Dor required! Complete ownership of this Pro Site. Are you sure you want to contin	otected Domain will be t	
		Cancel	Confirm

/M Network Mapping			
Protected VM Network 🔺	Recovery VM Network		^
VM_3510	DRStretchSeg	•	^
0 0			v .
ther Settings			-
Planned Failover			
Force Failover			
Some VM's guest credential are requi	red because of network configuration: Con	figure	

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.

Protected Domains Statistics Stora	Continuous Rehydration Task Resu	alt		
Select Protected Domain: GCSDRPD002	Task Completed Successfully with	h warnings	+ Create	🛢 Dellata 🗮 More
ade -				Est Data
ecoverable / Total VMs	Protected Domain	GCSDRPD002	ANECVODR	
ecoverable r volati vics	VMs Recovery Status	Success with warnings	OCAL (172 30.1	56.2.)
	Total VMs Recovered	4	DBC-Datacente	
emaining Background Data	VM(s) with warning	2 <u>View</u>	esabled	
emaining background bata	GCSRecovery03 Status:		and a second	
	Pre-script Execution Status	Not defined		
	Runbook Execution Status	O Success		
Protected VMs Settings Alarms	Post-script Execution Status	Not defined		
+ Start Protection				c
VM Name A			ackground Data	A Details
GCS-DR-SC46		5	8	Detalla
GCS-DR-SQL03			0	Datals
GCSDR-W2K10-01			8	Detaits
UbuntuSrv001			8	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.

() () () () () () () () () () () () () (·	sc46.gcsdc.com ×	
		etApp。。	
BACK			
	SnapCente		
	Username	gcsdc\adri\jnnimo	
	Password	•••••	
		Sign In	

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

	NetApp SnapC	enter®						•	-	9-	L gcsdc\adminnimo	SnapCenterAdmin	Sign Out
<		Global Settings	Policies	Users and Access	Roles	Credential	Software						
	Dashboard												
9	Resources	Global Settings	0										
۲	Monitor												
мi	Reports	Hypervisor Settin	1gs 0										~
٨	Hosts	Notification Serv	er Settings	0		0.0	>						~
ł.	Storage Systems	Configuration Se	ttings 😗										~
華	Settings	Purge Jobs Settin	gs O										~
▲	Alerts	Domain Settings	0										~
		CA Certificate Se	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	9	O Currently Tran	sferring	©	3 Healthy		⊗ 0 Failed	
	3	3 Volume Relationships											9
	3	8 Volume Relationships Health Status 🔅	Source Volume	\$I.	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

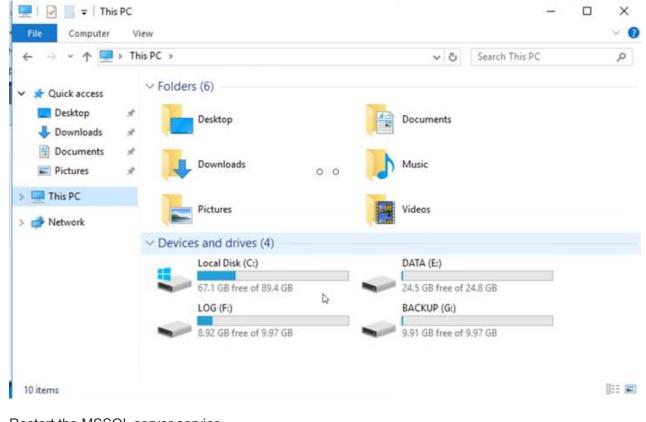
7. Attach the LUN from Cloud Volumes ONTAP to the recovered SQL guest VM with same drive letters.

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 %	
	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.

🐊 Services (Local)	Services (Local) SQL Server (MSSQLSERVER)	Name	Description	Status	Startup Type	Log
	Stop the service	SQL Full-text Filter Daemon	Service to la	Running	Manual	NT GCS
	Pause the service Restart the service Description: Provides storage, processing and controlled access of data, and rapid transaction processing.	SQL Server Agent (MSS) SQL Server Browser SQL Server CEIP service SQL Server CEIP service SQL Server Integration S SQL Server VSS Writer SSDP Discovery State Repository Service Still Image Acquisition E Storage Service Storage Tiers Managem Superfetch Sync Host df83a	Start Stop Pause ^{ooo} Resume Restart All Tasks Refresh Properties Help This service	ning ning ning ning ning ning ning	Automatic Automatic Automatic Automatic Automatic Automatic Manual Manual Manual Manual Manual Manual Automatic (D.,,	GCS Loc NT NT Loc Loc Loc Loc Loc Loc
		System Event Notification S	Monitors sy	Running	Automatic	Loc

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

the second se	w Query 월 & & & & & A & D & ? - ? - 원 Execute ■ ✔ \$? 클 🔲 \$? \$? 램 월 翩 관 3 🦉	- 🏓 - 🖅 🎫 😻 🖕
bject Explorer	SQLQuery1.sql-GDC\adminnimo(66)) + × /****** Script for SelectTopNRows command from ESELECT TOP (1000) [Id] ,[Name] ,[Price] FROM [CarDB].[dbo].[Cars]	SSMS *****/
📁 External Tables 💼 Graph Tables	100 % · · ·	
 ☐ dbo.Cars ⊕ Columns ⊕ Keys ⊕ Constraints ⊕ Triggers ⊕ Indexes ⊕ Statistics 	Id Name Price 1 1 Car-1 1000 Image: Car-2 Image: Car-2	

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	← Fallback	
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	uster		A300-Cluster				
Failback Re	source Pool						
VM Folder (Optional)						
Failback Da	tastore		A300_NFS_vMotion				
Maximum D	elay After Stopping		10 Minutes				
Internal Net	wo9k		VM_187				
External Re	plication Network		VM_187				
Managemen	it 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.

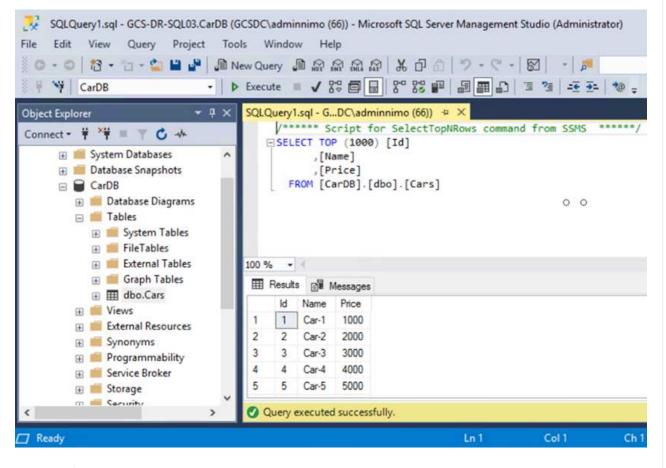
JetStream DR Protected Domains Statistics Storage	Failback Task Result			
Select Protected Domain: GCSDRPD002 💌	Task Completed Successfully			
Recoverable / Total VMs	Protected Domain	GCSDRPD002		
Replication Status	VMs Recovery Status	Success		
Remaining Background Data	Total VMs Recovered	4		
Containing Cooling Conta	GCSRecovery03 Status:			
Current RPO	Pre-script Execution Status	Not defined		
	Runbook Execution Status	Success		
Protected VMs Settings Alarms	Post-script Execution Status	Not defined	B	

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

\odot	gcsdrsqldb_sc46 ntaphci-a300e9u25	19	gcsdrsqldb_sc46_coj ANFCVODRDemo	py	6 minutes 41 seconds	idle	broken-off	May 5. 2022. 12:08:34 PN 33.66 KiB	•
\odot	gcsdrsqlhld_sc46 ntaphci-a300e9u25	19	gcsdrsqlhld_sc46_co ANFCVODRDemo	ру	4 minutes 56 seconds	idle	broken-off	Information	
0	gcsdrsqllog_sc46 ntaphci-a300e9u25		gcsdrsqllog_sc46_co ANFCVODRDemo	py •	10 minutes 18 seconds	idle	broken-off	Reverse Resync	
								Edit Schedule	
								Edit Max Transfer Rate	
								Delete	

B Volume Re	lationships	6.54 GiB Replicated Capacity	Currently Tran	sferring	Ø 3 Healthy	S O 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

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

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

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

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

Benefits of this solution

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

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

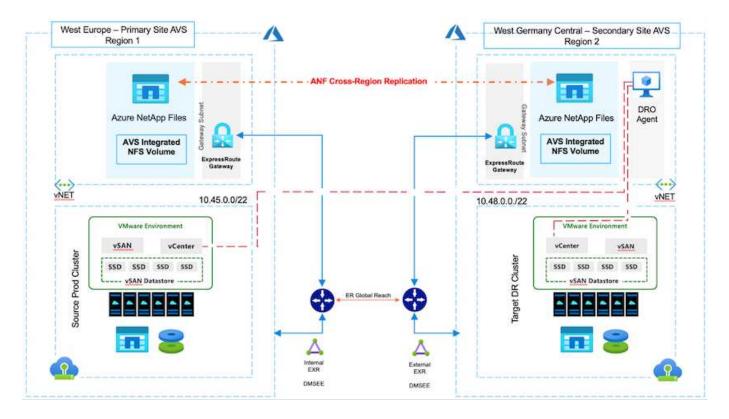
Disaster recovery using block-level replication between regions within the cloud is a resilient and cost-effective way of protecting the workloads against site outages and data corruption events (for example, ransomware).

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 xvf draas_package.tar
Navigate to the directory and run the deploy script as below:
sudo sh deploy.sh
```

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

■ NetApp	
Disaster Recovery Orchestrator Grind Educer with Gui Vername Password	
Loyin	

DRO configuration

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

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

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

To perform this operation, complete the following steps:

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

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

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

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

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

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

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

Resource Groups Replication Plans Job Monitoring	٥	?	۹
Add New Site 0 Site Type 2 Site Details 3 vCenter Details 3 storage Details			×
Site Type			
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 👍 S	Storage Details		
		Source AVS Private Cloud			
	Select Credentials	Azure Region 🕘 🖌	Azure Resource Group		
	DemoCred -	West Europe +	ANFAVSVal2 +		
	Add New Credential IS				
		AVS Details			
		Avo Details			
	Web Clien	URL	0		
		ANFDataClus	·		
	Username		0		
	cloudad	min@vsphere.local			
	Password				
		•••••			
		Accept self-signed certificates			
		Manager and a service of the service			

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	N Dashboard Docover R	escurce Groups Replication Plans Job	Monitoring		<u> </u>
Back VM List Site: DemoSRC vCenter: https://172.30.156.2/					
🔁 7	attores	128 Virtual Machines	VM Protection 2 Protected	126 Unprotecte	
128 vm				Q	Create Resource Group
VM Name	C VM Status		DetaStore	: i au	C Memory (MB)
HDSenth_2.5.1	0 Not Protected	() Powered On	vianDatastore		8192
hci-fio-datastore-13984-0-1	0 Not Protected	D Powered Off	HCRstDS	32	65536
ICCA2005-WO-R1	0 Not Protected	(1) Powered On	wanDatastone		14336
ICCA2005-NE-R1	0 Not Protected	() Powered On	vsanDatastore		3072
ICCA2005-01-81	() Not Protected	() Powered On	vianDatactore	8	3072
HCX_Demo_05	10 Not Protected	Powered 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 💊 📔 Deshi	board Discover Resource Groups Re	plication Plans Job Monitoring	. (¢ 0 4
	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 Disco		Replication Plans	Job Monitoring			• •	
Edit Resource Group		Resource Group Deta	ils 🕜 Select VMs	Boot order	and Delay			
			Boot order and	d Delay				
	VM Name	Boot Order 🚳		Boot Delay	(secs)			
	QALin1	3	12	0	12			
	QALin	3	10	0	[0]			

6. Click Create Resource Group.

Disaster Recovery Orchestrator 💊	Dashboard Discover Resource Groups	Replication Plans Job Monitoring	A :
Resource Group	C 1 Ste	C 1	P Virtual Machines
1 Resource Group			Q O Create New Resource Group
Resource 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	?	۹
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.

B 1 Replice	ation Plans	Resource Groups	Sites 1	vCenters	Sites 1		2 1 vCenters
1 Replication Plan						۹٥	Create New Replication Plan
Plan Name	C Active Site) Status	Compliance	Source Site	⇒ Destination Site	÷ 1) – j
DemoRP	Source	 Active 	A Partially Healthy	DemoSRC	DemoDest	Resour	ce Groups
							Plan Details
							Edit Plan
							Fallover
							Test Fallover

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

		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.

III NetApp	Disaster Recovery Orchestrat	tor 🔌 Decisional Discover	Resource Groups Replication	on Plans Job Monitoring			0 0 C
	C 2 Sites	1 Resource Group	B, 1 Replication	s Plan	128 Protected VMs	0 527 Ungentivected	
	Environments 2 Vortual Environments	2 Aver Storage Accounts	Topology Canvan			Immensive View (3	
	SDOC Summary	D 14 Feiders		A	DemoGest regis /110 75 6 2/		
	Dutastores						
	Execution Jobs		Replication Plans			1	
	🕑 1 Tintal solar	0 1 m Property	Replication Plan DemoRP	Active Site	Status		

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

			Source Details	-	Destination Details	1
Replic	ication Plans	Resource Groups	T Sites	vCenters	Sites 1	vCenters
1 Replication Plan					Q	Create New Replication Plan
1 Replication Plan Plan Name	≎ Active Site	Status	Compliance	Source Site →	Q · ·	Create New Replication Plan
	Active Site Operation	Status Running In Failover Mode 		Source Site ⊽ DemoSRC	Destination Site	Create New Replication Plan
Plan Name					Destination Site	1

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

🗖 NetApp	Disaster Recovery Orchestrator 💊 Dashboard Disco	ver Resource Groups Replication Plans Job Monitoring	A O O O
	Replication Plans	Source Details Destination Details urce Groups Image: Source Details Image: Source Details	
	1 Replication Plan Plan Name 0 Active Site Stat	Q O Create New Replication Hus Compliance Source Site ♥ Destination Site ↓	s Plan
	DemoRP © Destination ©	Active O Healthy DemoSRC DemoDest Resource Groups Ran Deals	
		Falback	
I NetApp	Disaster Recovery Orchestrator 💊 Decidenari Disc	cover Resource Groups Replication Plans Job Monitoring	• • •
	C 2 Sites 1 Resource	Group I Replication Plan I 28 VMa VMa Unproducted VMa VMa VMa	
	Environments 2 2 What Environments All Ecorporacions	Topology Cances Immensive View	*0
	SDDC Summary		
	Chutters 2 14 Folders	DemoSRC DemoSet https://112.30.156.2/ https://10.75.0.2/	
	12 Datastores		
	Execution Jobs	Replication Plans	
	Image: Second system Image: Second system Image: Second system Image: Second system	Repútation Plan Adves Site Status Drmolifi C) Source C) Adves	

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

Ransomware recovery

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

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

Conclusion

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

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

Where to find additional information

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

Create volume replication for Azure NetApp Files

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

Cross-region replication of Azure NetApp Files volumes

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

Azure VMware Solution

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

• Deploy and configure the Virtualization Environment on Azure

Setup AVS on Azure

• Deploy and configure Azure VMware Solution

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

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

Azure NetApp Files (ANF) datastores decouples storage from compute and unlocks the flexibility needed for any organisation to take their workloads to the cloud. It provides customers with flexible, high-performance storage infrastructure that scales independently of compute resources. Azure NetApp Files datastore's simplifies and

optimizes the deployment alongside Azure VMware Solution (AVS) as a disaster recovery site for on premises VMWare environments.

Author: Niyaz Mohamed - NetApp Solutions Engineering

Overview

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

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

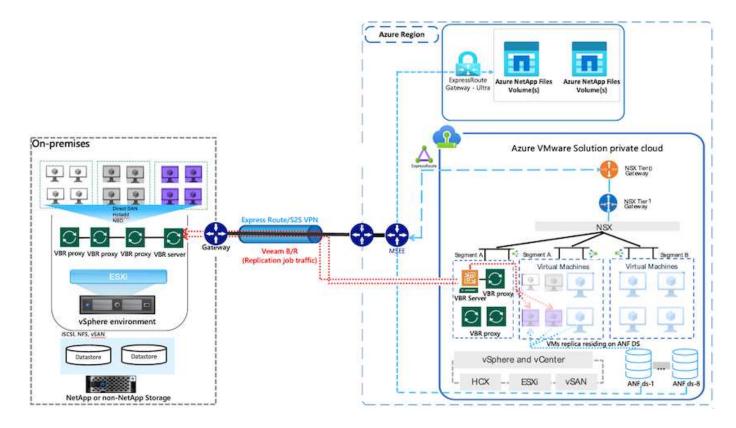
Purposes of this document

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

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

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

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



Solution Deployment

High level steps

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

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

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

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

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

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

Deployment Details

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

To replicate VMs, follow the below steps:

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

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

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

Name	Name:
irtual Machines	AVS_20230522_RepJob01
intual Machines	Description:
estination	Created by VEEAMBKPSRV05\Administrator at 5/21/2023 10:52 PM.
Network	
ob Settings	Show advanced controls:
ata Transfer	Replica seeding (for low bandwidth DR sites)
lata Transfer	Network remapping (for DR sites with different virtual networks)
juest Processing	Replica re-IP (for DR sites with different IP addressing scheme)
chedule	L
Summary	
	High priority
	Backup infrastructure resources are offered to high priority jobs first. Use this option for jobs sensitive to the start time, or jobs with strict RPO requirements.

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

Virtual Machines

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

	Name	Type	Size	^	Add
Virtual Machines	TestVeeam21	Virtual Machine	873 MB		Remove
Destination	TestVeeam22	Virtual Machine	890 MB		Nethaye
	TestVeeam23	Virtual Machine	883 MB		Total III and
Vetwork	TestVeeam24	Virtual Machine	879 MB		Exclusions
	TestVeeam25	Virtual Machine	885 MB		Source
ob Settings	TestVeeam26	Virtual Machine	883 MB		
Data Transfer	TestVeeam27	Virtual Machine	879 MB		
Jata Transfer	TestVeeam28	Virtual Machine	880 MB		🕈 Up
Suest Processing	TestVeeam29	Virtual Machine	878 MB		+ Down
j	TestVeeam30	Virtual Machine	876 MB		
Schedule	TestVeeam31	Virtual Machine	888 MB		
	TestVeeam32	Virtual Machine	881 MB		
Summary	TestVeeam33	Virtual Machine	877 MB		
	TestVeeam34	Virtual Machine	875 MB		-
	TestVeeam35	Virtual Machine	882 MB		Recalculate
	WinSQL401	Virtual Machine	20.3 GB		
	WinSQL405	Virtual Machine	24.2 GB		Total size:
	F2			*	120 GB

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

Edit Replication Job [AVS_2 Destination Specify where	replicas should be created in the DR site.	3
Name Virtual Machines	Host or cluster: Cluster-1	Choose
Destination	Resource pool:	
Network	Resources	Choose
Job Settings	Pick resource pool for selected replicas VM folder:	
Data Transfer	vm	Choose
Guest Processing	Pick VM folder for selected replicas	_
Schedule	Datastore: ds001 [152.6 GB free] ds001 is an ANF Datastore	Choose
Summary	Pick datastore for selected virtual disks	
	< Previous Next > Finish	Cancel

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

Name	Network mapping:		10.7
Virtual Machines	Source network Source network VM_3508 (vDS-Switch0) SVM_3510 (vDS-Switch0)	Target network SepSeg SegmentTemp	Add Edit
Destination Network		segment emp	Remove
Job Settings			
Data Transfer			
Guest Processing			
Schedule			
Summary			

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

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

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

Name	Run the job automatically	t			
Virtual Machines	Daily at this time:	10:00 PM	Everyday	~	Days
virtual machines	O Monthly at this time:	10:00 PM	Fourth 🗸	Saturday 🚽	Months
Destination	O Periodically every:	1	Hours	~	Schedule
Network	 After this job: 	Replication Jo	b 2 (Created by VEE/	AMBKPSRV05\Administ	trator at 6/6/
ob Settings	Automatic retry				
Data Transfer Guest Processing Schedule	Wait before each retry Backup window	•	0 💽 minutes		Window
Summary	If the job does not cor terminated to prevent	mplete within al	ocated backup wind		11114401914
		< P	revious Appl	V Finish	Cancel

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.

Name	Summary:	
	Name: AVS 20230522 RepJob01	-
Virtual Machines	Type: VMware Replication	
	Source items:	
Destination	TestVeeam21 (a300-vcsa05.ehcdc.com)	
	TestVeeam22 (a300-vcsa05.ehcdc.com)	
Network	TestVeeam23 (a300-vcsa05.ehcdc.com)	
Network	TestVeeam24 (a300-vcsa05.ehcdc.com)	
lob Settings	TestVeeam25 (a300-vcsa05.ehcdc.com)	
ob settings	TestVeeam26 (a300-vcsa05.ehcdc.com)	
Data Transfer	TestVeeam27 (a300-vcsa05.ehcdc.com)	
Data Transfer	TestVeeam28 (a300-vcsa05.ehcdc.com)	
	TestVeeam29 (a300-vcsa05.ehcdc.com)	
Guest Processing	TestVeeam30 (a300-vcsa05.ehcdc.com)	
	TestVeeam31 (a300-vcsa05.ehcdc.com)	
Schedule	TestVeeam32 (a300-vcsa05.ehcdc.com) TestVeeam33 (a300-vcsa05.ehcdc.com)	
175	TestVeeam34 (a300-vcsa05.ehcdc.com)	
Summary	TestVeeam35 (a300-vcsa05.ehcdc.com)	
	WinSQL401 (a300-vcsa05.ehcdc.com)	
	WinSQL405 (a300-vcsa05.ehcdc.com)	
	WinSQL404 (a300-vcsa05.ehcdc.com)	
	146-501 402 (-20005	`
	Run the job when I click Finish	

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

	S. Samer			T 100						
-	Statement Statement	-	-		e Hate			111	Service and the service of the servi	
	100				-					
		-	4144	10.000	1000	10	-			346.01.01
	Same -		100		1	1				
	1	-				17.	-			
		1 ion								1

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.

Backup Replication CDP B Job * Job * Policy C	ackup Copy Copy * Job * Auxiliary Jobs		oort Export kup Backup Actions				
Home		Q Type in an object r	ame to search	for		X T	All jobs
Jobs		Name 🕹	Тур	e e	Objects	Status	Last Run
猶 Replication		🔅 Replication Job 2	VM	ware Replication	1	Stopped	63 days ago
 Replicas Ready Active (4) Failover Plans 		僻 AVS_20230522_Rep	Job01 VM	lware Replication	20	Stopped	8 days ago

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

	ANF_AVS_FP01 Description: Created by VEEAMBKPSRV05\Administrator at 5/24/2023 9:08 AM.	irtual Machines
		ummary
	Pre-failover script:	
Browsen		
	Post-failover script:	
Browsen		

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

General Virtual Machines	Name	Delay	Realize state	121	
Virtual Machines	and the second		Replica state	^	Add VM
	TestVeeam21	2 sec	63 days ago (5:52 AM T		Remove
Summary	TestVeeam23	2 sec	7 days ago (10:12 AM T		Remove
Summary	TestVeeam24	2 sec	7 days ago (10:20 AM T		Set Delay
	TestVeeam22	2 sec	7 days ago (10:10 AM T		-
	WinSQL401	2 sec	7 days ago (3:52 AM Tu		
	WinSQL405	2 sec	8 days ago (4:05 PM Mo		
	TestVeeam25	2 sec	7 days ago (10:14 AM T		
	TestVeeam26	2 sec	7 days ago (10:17 AM T		
	TestVeeam27	2 sec	7 days ago (10:18 AM T		
	TestVeeam28	2 sec	7 days ago (10:14 AM T		
	TestVeeam29	2 sec	7 days ago (10:18 AM T		
	TestVeeam30	2 sec	7 days ago (10:15 AM T		
	TestVeeam31	2 sec	7 days ago (10:21 AM T		
	TestVeeam32	2 sec	7 days ago (10:13 AM T		
	TestVeeam33	2 sec	7 days ago (10:15 AM T		
	TestVeeam34	2 sec	7 days ago (10:14 AM T		✤ Up
	TestVeeam35	2 sec	7 days ago (10:20 AM T		+ Down

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



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

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

Start Start Retry Undo to Actions Details	Edit Delete			
Home	Q. Type in an obje	ect name to search for		×
🛚 🆓 Jobs	Name 1	Platform	Status	Number of VMs
續 Replication ■ 記 Replicas 認 Ready	ANF_AVS_FP01	VMware Start	Completed	20
Active (4)		🚯 Undo	_	
Last 24 Hours		Image: Statistics Statistics X Delete Image: Statistics Edit		

Name: ANF_AVS_FP01 Restore type: Failover Plan Initiated by: VEEAMBKPSRV05	\Adm	Status: In progress Start time: 8/9/2023 3:37:41 AM inistrator <u>Cancel res</u>	tore task
VM name Status	^	Log	
TestVeeam21 💿 Proce		Message	Duration ^
TestVeeam23 🜔 Proce		Waiting 2 sec before the next VM	0:00:02
TestVeeam24 🕑 Proce		Processing VM: TestVeeam22	0:00:13
TestVeeam22 🜔 Proce		Waiting 2 sec before the next VM	0:00:02
WinSQL401 () Proce		Processing VM: WinSQL401	0:00:10
WinSQL405 () Proce		S Waiting 2 sec before the next VM	0:00:02
TestVeeam25 🕑 Proce		Processing VM: WinSQL405	0:00:08
TestVeeam26 D Proce		S Waiting 2 sec before the next VM	0:00:02
TestVeeam27 🜔 Pendi		Processing VM: TestVeeam25	0:00:06
TestVeeam28 🜔 Pendi		S Waiting 2 sec before the next VM	0:00:02
TestVeeam29 🕑 Pendi		Processing VM: TestVeeam26	0:00:04
TestVeeam30 🕑 Pendi		S Waiting 2 sec before the next VM	0:00:02
TestVeeam31 () Pendi		Processing VM: TestVeeam27	0:00:02
TestVeeam32 🕑 Pendi		Waiting 2 sec before the next VM	0:00:02
🛅 TestVeeam33 🜔 Pendi	~		~

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

a Ølen	 In instag lapport las- 	baser & And	hada Alamittan P 🖉 iya	a team, high as 11. N	Ø ingen 👘 👻	() inge	· · · ·					0
	A ++	10		and the block	and she will make a	244						m 0 U.A.
espheredlere: Q		1.0									- <u>et</u>	C American Q
		< av	least Appleas Later								1	
0 11 10		have	my Monte Carlany Per	materia Report Article	VMs	power	red on A	1VS	SDDC	2		
a herbdelafalikelti oo	mount and adapt tom	-	and the second second			off	er failov	OF				
· B mochainm		and the second	and constrained on	-		an	er ranov	ei				
+ 28 (Sale-1												+ 10cl
	Collection (The PTE and the PTE and		64W	- 644	Bee	- Announcement	-their fame	-	v market	-		
	Contracting Fibli and incomparing		2 .B terment	Powerstoff	Noted	81158	10.49	1.4				
() (04.0007mm)	CARTONNAL SERVICE	0.00	i B televenti	Provenue dia	-7 16/16	10.05.0.0	01229-00	1.4	221.948			
> Children		0	a di termenta	However) (N	-/ 10/hd	10-07-03	1012-07 100	44	32149	110,014		
1 - LD Backing		0	- di terimente	Number Of Co.	1 10.000	10.00.08	8/9.37.465	2.6	221/148	101004	4	
A CR Mark Time		0	· . Ø fotmentt	Municipal Dis	< 10mg	8.010	475.75 100	-1-6	22110			
O More Journal			< # tutments	Parent In	-< mm	6.0118	070.29 #89	1.4	00.00			
D arrived		0.0	- B Turner P	Physical Div	1 martia	31-01-018	000-02-000	2.46	10.46			
@ automotivi		0	1 2 Televell	Restrict To	of Highed	10.04.08	0757348	1.4	10.44			
(T. Obi-reary		0	- 2 horizonte	finance in		10.01.00	112-0-140	1.00	. 22148			
(Freisbergel, (A)		0	 # Introduction 	Proverine (co	1 10000		675.64.745	1.4	00.00			
(B-140),Peales,33		9	/ @ Interact	flowered (1)	< 100 mg		1010	1.4	0.0			
B Noteriti		0	(E tutment)	Pureat 10	/ 8/14		100,04,040	14	31-10			
Of sChallen in m		0	· Distances	Purseal (n	1 10,000		072.01400	14				
IF COMMENT		0	· B hermanist	The set of		10.01.08	6733246 A150146					
d attaint with		0	A mean an	Recently in		10.0.0	1014-14	-	21.000			
and a second second		1.0	antiat					_		_		1014 MA . 8 . 4
Record Table Johns		_										
	- Terpi	iner-	1 Inste		- Internet	* 20 *	that the	1.7	Company Inc.		heren	
e is stud har te	-D weakers	4)-Companies	Disasting lab tim label late	a daine	visited March 10, Automation	0.000	11700 (1000 - 101 Add and		Antonio (10, 10, 10, 10, 10, 10, 10, 10, 10, 10,	- 10	or institution in the content of the second second second second	
infact intra tiachte	D WHERE	C-Louise	Decempony Office New	tion on particular hand	alabelite of the later surgery	0.000	1110203-014-04		terminaria, brim of a		or her bill induced in the second second second	
induct of the months	0 weakit	(Classifier)	 Incodigoing (1) of her 	ten or periodice and	10HH LUCA MANNER	2.00	100 0 0 0 0 0 0 0 0 0 m		1000001010-000404	-	of party state and the second state and the second state of the se	
column a state transme	B 10032412	() (insered	Amontopying 2014 Amon		CONTRACTOR (CONTRACTOR)	2.04	017802103.00040-04		dimension in the state		A REPORT AND CONTRACTOR OF ANY ANY	
e-2-stud tarbe	B WHEEKS	O Latence	Prosting or the test with		signation cook is presented.	2.04	Directory and in sec.		00000011 0 40 51 4		a before to the condition of an and not	
entiped of the market of	-B WHERE	- O Lansent	Reartpring 1154 Har		VIP-RTELDOLLIN-INSTR	2.49	2579(252), 1-15,83 AP		1000031-010-06.0		a beneration for a children and an and an	
er (h. dituk kapiten	- worker	() Competine	Proventing but the rate such		131627123100000	2.44	2179(200), in (8.1) and		00000333 208454		or perception and an internal sector of the sector of the	
infante of the Fachtie	O writher	() Campaine	Recentpulse incertex.		+3HERTOOLULUMARE	249	01/00/2011 0:00:01 4:44		CONTRACTOR NOT A DECIMAL		- METROPOLISHING WERE AN ADDRESS	
outplue output unitate	B W68405	CO Conserve	Increasing that he		Adverted for Advertised	2.44	15/80203. 8:09:29:00		00000023-000-22-0		 Section Contracting the Child Section on the Astronomy Contracting Contractin	
migure vehice manage	A 10052414	Clonated	Descriptions (1754 Her		VIP-BIELDUA (Assessment	2.046	STORES AND ADDRESS OF				and the state of t	
have while marked	B W45425	O Constitute O Constitute	Security or a Mar		VMMERED (CAL) Summer of	2.04	Division, social are		CONTRACTOR DESIGNATION		a permitta tarta a batteria per ante ante	
and an address of the state of	d weaks	O Companie	and desired in the part	the second of	VENERAL OCA, STRATEGICS	249	stracture and and and		includes and as		a bet hit was clearly and an are an are	
er in alle name	@ taronach	O Compariso	Page 19 and 19 and 19	a Barris	olithetite a DCA laboration	2.44	strapping lower and		entantis sources		- barbarbarbarbarbarbarbarbarbarbarbarbarb	
at its shad harden	dt fafementt	O Longend	Property in the last time		COMPANY OF A DESCRIPTION	1.04	COLUMN TWO IS NOT		summer passa.		a service water (Section and section and section)	
10 10 10 10 10 10 10 10 10 10 10 10 10 1	(B. Turbunarite	() Demand	Classing to Do Los VII.		VIPERATOR DRAMMER.	144	survey of the local division of the		stringer, passion		a harbert faith (half) and a star to see the	
or 22 while balling	di fatimati	Q Dorumet	Dissering to the late late		VIP-ITELCCL.Lturater.	1.04	20700001 8-08-00-04		errorente bite ca.		a barbarb facto (Barbi) and and and and out	Activity Weichows
stand shind markets	di Informatità	C targetet	Incidence of the National State		Vaheni LOOL Varianteen	2.04			Antonia and an		a last hits faither, the bit sector as an and out	

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

E Hone India					Vision Backup and Replicati				- 0
None Fallower Fallower	Autock to Descrive to tool Production Production T	ibuver Under Connet Hautz run Fallback Failback File-	Application Nerris - Restore	Fellover Plen *	Financias Sector				
lome	Q Type in an adjustment	taé in senirih fer	×						
The later	Alaria 🕈	Alla Marrie	Type	Status'	Crastion Time	Rative Ports	O-symul Location	Replica Location	Itation
- Replication	15 TestVetam22	AVS.20210322, Replat01	Rogular	Failovor	MA-6572023-353-AM	3	a200 vsso05 chick: cont/Oustor03	172.30 156 2\Quster 1	Whytware
ril Teolices	Test/eesm23	AV\$_20230522_Replo601	Regular	Failover	6/6/2023 5/52 AM	4	a300-vcsa05.ehcdc.com/Cluster05	172.30.156.25Ouster-1	Vistwore
(Reaty	Test/veeem24	AV5_20230522_Replot01	Septer	fellover	6/6/2025 3-32 AM	3	a300-vesa05 ehede.com/.Cluster05	172.30.156.250uster-1	Moree
Dis Active (19)	TestVecim27	AVE 20210522 Replet01	Rogetar	Fallovor	6/6/2023 7:48 AM	4	allo	172.30.156.2\Chister-3	VMware
a Falover Flans	TestVecon26	AV\$ 20230522_Replat01	Regular	Failover	6/6/2023 10:44 AM	1	a300-vcta05 shedt.com/Cluster05	172.30.156.2\Guster-1	Virtuare
Let 24 Hours	TextVecern27	AV5 20230522 Replot01	Regular	Fallover	6/6/2023 12:19 9%	3	a000-vesa05.ebcdc.com/Quster05	172.30.156.2\Guster-1	\$54tware
3 Success	Tan/Valuarin28	AV5 20210522 Repible1	Reppla	Fallows	6/6/2023 1.07 PM	3.	a500-www.5.ehidc.com/Duile03	172.30.156.2\Gusher-1	VMANCH
Warning	Testvecon20	AV5.20230522_Replat01	Rogular	Failovet	6/6/2023 1:16 PM	1	a300 vcsa05 ehodo.com/Cluster05	172.30.156.2\Cluster-1	VMMware
C. Manada	CENTextVeesm00	AV\$_20230522_Replot01	Regular	Tallover	6/6/2023 2:24 PM	1	a300-vcsa05.ehodc.com/Cluster05	172.30.156.2\Quster-1	Vilviere
	Tent Verentil 1	AVS 20230522 Eepleb01	Reputer	Falcer	7/31/2023 4-41 AM	1	a508-vcsa05 etcd: com/(Duster01	172.30.150.25Guster-1	Videore
	Tectivocore12	AVE 30330522 Replot01	Rogetar	Ealover	6/6/2028 8:31 PM	1	alide vesu05 shole confiduator03	172.20.156,210Juster 1	Vistoaro
	TestVetern23	AV\$ 20230522 Replot01	Regular	Failover	6/6/2023 3:31 PM	4	a300-vcsa05.ebcdc.com/Cluster05	172.00.156.2\Cluster-1	Vit-twore
	TextVeesm04	Av5.20230522 Replat01	Regular	Failover	6/6/2023 4:31 PM	4	a500-vcsa05.ehcdc.comt/Cluster05	172.30.156.2\Cluster-1	Where
	Tantwasm11	Avs. 20230522, Replat01	Regular	Failovet	6/6/2028 5:30 PM	8	at00 visia05 shodc.com//Dustar03	172.30.156.2\Gustar-1	VMaurie
	WinSQL401	AV5,20230522,Replat01	Regular	Failover	6/6/2023 6 52 AM	5	a300-vcsa05.ehodc.com//Cluster05	172.30.156.2\Cluster-1	Võdware
	WinSQL 102	AV5.20230522 Recleb01	Septier	Failover	6/7/2023 6:11 AM	3	a300-vesa05 ehede.com/Guster05	172.30.156.2\Guster-1	Vistware
A Home	WVSC/403	AVS 20210522 Replicid1	Fergilar	Failower	6/7/2023 12:28 AM	1	20m water and a constant of the	172.30 156.2 Cluster 7	Whener
C. Contract	1 Win908404	AVS 20210522 Replot01	Regular	Failover	6/6/2023 6:29 PM	3	a300 vcsa05 eticdc.com/Ouster05	172.30.156.2\Guster-1	VMwore
E Inventory	WinSOL405	AV5_20230522_Replot01	Regular	Fallover	6/6/2023 7:50 AM	3	a300-vcsa05 ehodo.com/Quster05	172.30.156.21Ouster-1	Sheware
🙀 Dackup left astructure									
Storage Infrastructure									
Tape Intracticuture									
(Pp inter									
10	6.2								



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:

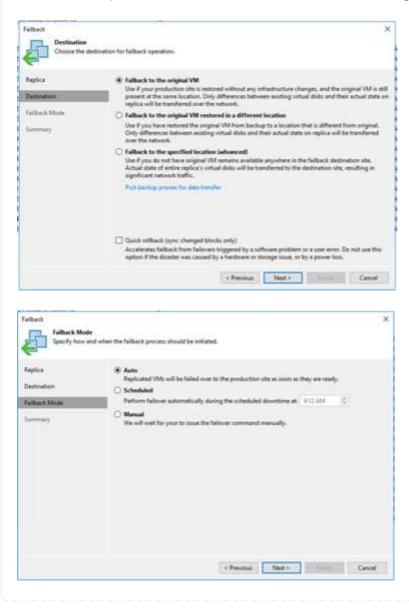
 Failback to production - switch back to the original VM and transfer all changes that took place while the VM replica was running to the original VM.



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.



Current offer	cas you want to faillack. Cick Populate t	a was as stored offic	and or the sta-		
Replice	Replices to failleck:				
	Name	Sor	Original location		Select All
Destination	E3 Testilean28	85.8 MB	(al00-vesal5 mide com) [7.	1	Clear All
Faillack Mode	TestVecarri23	\$2.3 MB	(al00-veza%.aheatc.com) (T.		CORE NO.
	Edina Testilanam22	75.4 MB	(a)00-yeard5 ahestc.com[[7.		Populate
Summary	Testileam30	86.8 MB 85.7 MB	(#XII-vesal5.ehodc.com) [7. (#XII-vesal5.ehodc.com] [7.		
	E WinSQL42	15.08	(a)00-vesal5.ehedc.com) (FS		
	12 / Testineen25	812MB	(a)00-ycaal5 ahctic.com) [T.		
	Statiseen14	81.7 M9	(a)00-vesal5.aheak.com) [7.		
	2 Testiesenil	96.43/0	(a300-vesall5.ehodc.com) [7.		
	ES WindQuido	1.6.08	(s000-vesa05.ehudc.com) [PS		
	E Testilepanili	88.3 MB	(a30)-veaal5-eheste.com[[7-		
	E for Testilesan 25	88.3 MB	(a)05-vesal5.ahcdc.com) [T.		
	Conwesters	14-08	(e300-vca#05.ehodc.com) [PS		
	E West And	13.08	(#100-ses#05.#hcdc.com) (PS		
	Contestiment39	81.2 MB 77.6 MB	(#300-ves#05.ehode.com) [7 (#300-ves#05.ehode.com) [7		
	Eline Testiveanili		(al05-vesal5-mote-com) [1-		
	Level and Level				
			Net		Carcel
ilback					
Summary	ck sattings, and click Fasids to start faillin	ch operation. You o	il be able to undo failback pro	icess if req	piek
Summary Review failth		ch apendico. You a	il be able to undo failback pro	ces il rea	pirel
Summary Review failth	Summary	ch aperation. You o	d be able to unde failback pri	sons if my	piret
Summary Review failts optics lettinution		ch operation. You e	if he able to unde failback pro	cess if rea	piret.
Summary Review failts optics lettinution	Summary \$131 name TettVesen28	ch operation. You u	il be able to unde faibleck pro	ices if req	pint
Summary Review failte Applica Jestinution sithack Mode	Summay SM name TetVesen21 VM name TetVesen21	ck operation. You u	il be able to unde failback pro	ces f re	pint
Summary Review failte Applica Jestinution sithack Mode	Summay Mit name: TettVesen21 Mit name: TettVesen21 Mit name: TettVesen22	ck operation. You u	il be able to unde failteck pro	oons if my	påed.
Summary Review failte Applica Jestinution sithack Mode	Summay: Mit rame TetVision21 Mit rame TetVision22 Mit rame TetVision22 Mit rame TetVision32	ck operation. You u	il be able to unde failtack pr	cons d'ma	pinel
Summary Review failte Applica Jestinution sithack Mode	Summary Mit rame: TettVeen21 Wit rame: TettVeen23 Wit rame: TettVeen22 Wit rame: TettVeen32 Wit rame: TettVeen32	ck operation. You o	il be able to unde failback pro	ices il reg	påes.
Summary Review failte Applica Jestinution sithack Mode	Summary Mit name: Tettiveen28 Wit name: Tettiveen28 Wit name: Tettiveen28 Wit name: Tettiveen28 Wit name: Tettiveen22 Wit name: Wit402,402	ck operation. You a	d be able to unde failback pr	nomo il reg	pare.
Summary Review failte Applica Jestinution sithack Mode	Summary BM name TetlVesen21 VM name TetlVesen22 VM name TetlVesen22 VM name TetlVesen22 VM name TetlVesen22 VM name TetlVesen23	ck operation. You a	d be able to unde failback pr	cass if my	pint
Summary Review failte Applica Jestinution sithack Mode	Summary Mit name: TettVesen21 Wit name: TettVesen22 Wit name: TettVesen22 Wit name: TettVesen22 Wit name: TettVesen22 Wit name: TettVesen23 Wit name: TettVesen23 Wit name: TettVesen24	ck operation. You u	il be able to unde failteck pr	ocess if reg	pint
Summary Review failte Inplice Institution satlack Mode	Summary Alt name TettVeen21 VM name TettVeen22 VM name TettVeen22 VM name TettVeen22 VM name TettVeen23 VM name TettVeen24 VM name TettVeen24 VM name TettVeen24		il be able to unde failback pr	cons if reg	p.es.
	Summary BM name: TettViseen28 VM name: TettViseen28 VM name: TettViseen20 VM name: TettViseen20 VM name: Visid24.42 VM name: TettViseen23 VM name: TettViseen24 VM name: TettViseen24 VM name: TettViseen24			cost if reg	pired.
Summary Review failte Inplice Institution satlack Mode	Summary Mit name: Tettiveen28 Wit name: Tettiveen28		n of failback.	cong if reg	Cancel

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.

And		Under Stations	unit Jalo	Martine and Plane - Transmission Martine - Transmission Martine - Transmission Martine - Transmission								
	Q Sar in an Hant nu	ren by page of the	X	8								
Sa bit B Reficience Sa Reality Sa Reality R relation from Sa Reality Particle from Sa Reality Sa Reality	Termination of the second seco	201 Turnet 4442 (2013)2323, Jegendel 7, 4442 (2013)2323, Jegendel 7, 4442 (2013)232, Jegendel 7, 4442 (2013)232, Jegendel 7, 4442 (2013)242, Jegendel 7, 4442 (2013)242, Jegendel 7, 4442 (2013)243, Jegendel 7, 4442 (2013)24, Jegendel 7, 4	Type Regular Angular	Data T Calays Calays Calays Solars Solars Calays Calays Calays Calays Calays Calays Calays Calays Calays Calays Calays Calays Calays Calays Calays Calays Calays	Content Time Entropics (BH+ AM R100023 (BH+ AM R10003 (BH+ AM R100023 (BH+ AM R10003 (BH+ AM R100023 (BH+ AM R10003 (B	Fame fain 4 4 4 4 4 4 4 4 4 4 4 4 4	Comparison (1) (and (1)) (Equipa Lagran 17.30 (19.4) Column (17.30 (1	Partiese Oberea	いる このの あまり	alone ton., general times., all to failure give which to production., arout failurd along gate failurd along gate failurd along gate failurd along failurd failurd along failurd failurd along failurd failurd along failurd failurd along failurd failurd along failurd alo	•
A men												
Tation information												
Through inflationation												
😰 tempeletationen Se Tempeletationen												

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

. 8 8 9	⁶ (2) VeelamTest (across Summary Monitor Configure		e Pools VMs						
 B 4300-ccu01-ehcit.com B 4300-0005 	Vistaal Hattories VH Terratal	in where							
 D Oumerth 	and the second s							A CONTRACT	
□ a000 exa01 efect com									
C abox exits share non		1 Bate	Dates	Poderedber	Used Space	Heat CPU	Multi Mere		
 G HOBerth DR0F 	() / // test/eeendt	Powered On	V horna		563.2 MS	0.014	408.140		
 Q HOBERS_0002 	C 11 / twinklar-32	Powersd On	 Normal 	16 GB	384 99 548	0.64	543 M8		
 O HOBerch 2003 	C) + (# TettWear23	Powersd On	 Normal 		378.89.148	0.46	34140		
- O Vecamiliest	C = D TestVetunde	Powered On	 Normal 		1274.4 563	010	340 MB		
(# Textomary21	City of terrors	Powerse On	V. Nortal		890.27 ME	019	237.648		
12 TextVetam22	C) / D TeitWear30	Plowing On	V Nortal	10-08	8763.45	0 Hz	2202 1405		
62 TextmeanIS	C = C Tectobeand?	Presented On	- Normal	16.08	874.45 MB	0.10	34290		
(B Testiveam34	Circ di testweetik	Powered On	 Nema 	10.08	875.12 HB	0.Hg	202.440		
di festiveani25	C / / // testveram20	Proveragi Dri	- Normal	16.08	873 54 MB	0.H2	340 MS		
(# Technologia	C A thickness	Powered On	V tonal	16 GB	87129 MB	0.142	300 MB		
(B Testsbeam2)	C) · · · (2 Testymeers3)	Rowersd On	U Normal	16:08	882,92.99	- Ó HR	343.66		
ill Testelearchi	C + C testverentz	Provend On	 Normal 	NO OIE	675.34 148	0.40	223 MB		
(D Testvieiam29)	C 1 If tertyteemild	Powered On	V Normal	10.08	872 07 ME	0.Hg	337 MB		
40 testviewambb	Ci + /# testveam34	Powersel On	V Normal	16.08	670.29 Mil	0102	300 MB		
(D Yestviewen))	CI = (# terryteam))	Powered On	V Normal	16:08	877.62 MB	ding	128.149		
dit Teatumaniza	CI + CP WYNSCARDI	Powered OT	· Normal	308.22.08	20.32.08	ONE	08		
(2. Sentreearn23	() 1.4 (b) WHOOLAGO	Powered Off	- Normal	308.22.08	20.63.08	0.0142	.08		
(2 Testimearc)4	C) / /2 WestQuest	Powered On	V Nortal	300.01.08	20.51 GB	85144	2.04.00		
(3 Testivearcil)	C (1 (P YM 50,404	Powered Off	- tarma	318.23.58	224268	0.40	0.8		
(2) Weinbla.eco	() + (0 mmou.ett	Powerst OT		208.22.08	24,24,00	010	0.0		
(B) Webbc.402	C) = (2 WW0.00	Powered On	V Normal		19.9.08	21434-0	W 00 00		
(2) Weisoukto (2) Weisoukto	Ci - G - Harden	- rame as well			10.7.100				
後 WHSOLION 後 WHSOLION 後 DATERSON 後 DATERSON 後 DATERSON 後 HCORPORT									
(2) HOBBERRE, DQA. (2) HOBBERRE, DQA.									
(2) Liendovideov									
ED Lastonimos	CI (COPORT)							Terris per pige	10 × 12
2A contraction	A CARDINE COMPANY								-

Conclusion

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

disaster occurs.

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

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

Migrating Workloads on Azure / AVS

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

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

Author(s): NetApp Solutions Engineering

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

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

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



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

High-level steps

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

- 1. Install HCX through the Azure portal.
- 2. Download and deploy the HCX Connector Open Virtualization Appliance (OVA) installer in the onpremises VMware vCenter Server.
- 3. Activate HCX with the license key.
- 4. Pair the on-premises VMware HCX Connector with Azure VMware Solution HCX Cloud Manager.
- 5. Configure the network profile, compute profile, and service mesh.
- 6. (Optional) Perform network extension to avoid re-IP during migrations.
- 7. Validate the appliance status and ensure that migration is possible.
- 8. Migrate the VM workloads.

Prerequisites

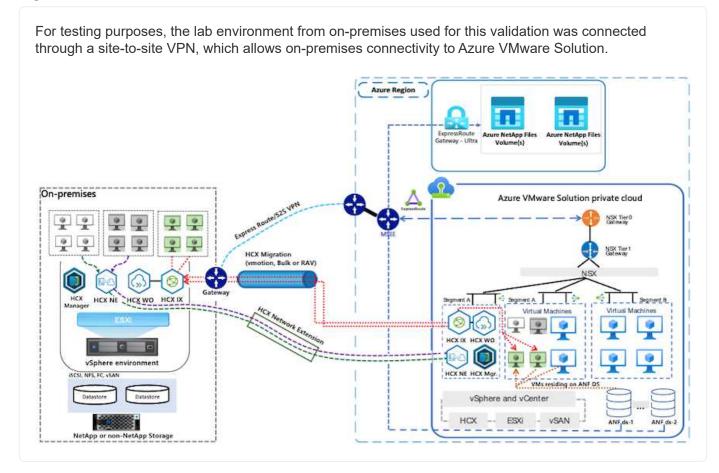
Before you begin, make sure the following prerequisites are met. For more information, see this link. After the prerequisites, including connectivity, are in place, configure and activate HCX by generating the license key from the Azure VMware Solution portal. After the OVA installer is downloaded, proceed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



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

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

High Level Architecture

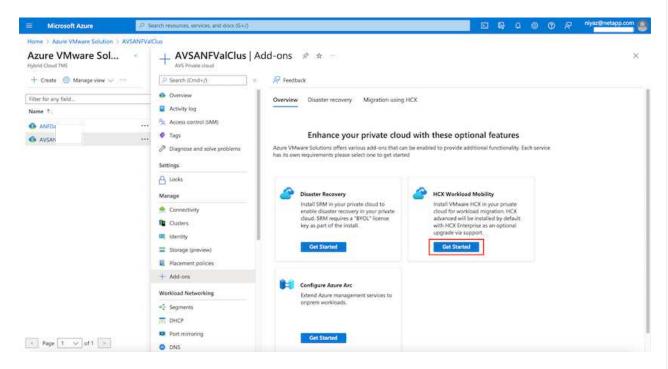


Solution Deployment

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

To perform the installation, complete the following steps:

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



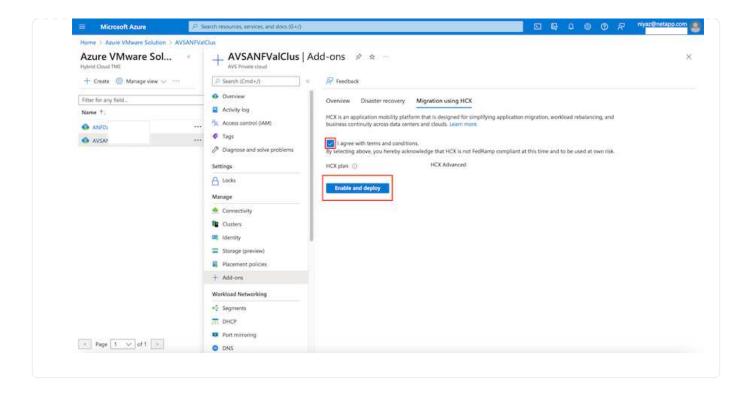
4. Select the I Agree with Terms and Conditions option and click Enable and Deploy.



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



The deployment takes approximately 25 to 30 minutes.



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

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

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



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

= Microsoft Azure	arch resources, services, and docs (G+/)	niyaz@netapp.com
Microsoft Azure Iome > Azure VMware Solution > A Azure VMware Solution > A Azure VMware Solution > A Azure VMware Solution + Create Manage view ··· Filter for any field Name ↑ ANF AVS ···	arch resources, services, and docs (G+r) Image Image </th <th>Nya2@netapp.com</th>	Nya2@netapp.com
< Page 1 v of 1 >	Test-440 FADE113ADA46490A8739C0E O Consumed ···· Segments testmig 40DD435C82F940EF641CF41 O Consumed ···· DHCP Port mirroring O Consumed ····	

2. After you access the HCX portal with cloudadmin@vsphere.local using the jumphost, navigate to Administration > System Updates and click Request Download Link.



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

→ C A Not secure Mile	ps //172h	hybridity/w/h	cs-client/index.html#/administra	6on/upgradeapp						iff 1	
vm VMware HCX									C	@~ =~	cloudadmi
O Dashboard Infrastructure O Site Paining S Interconnect Services C Compute Network Extension O Disaster Recovery	Pair your	EQUEST DOW	a center with VMware HCX								
Administration		urrent. fersion	System Name		2	Status	Info	System v Type	NSX Version T	VC Version T	Copy To Clipboard
Audit Logs	0 8	4330	hcx. Cloud	MV5.82	ure.co		0	HCX Ooud	312.0.017883600	7.0.3 19234570	G
Support	Remote	нсх			-					No. Physical Street Str	er of Applance
	Current 3	Version	System Name	τ Status		info		System Type	· ·	Copy To Clipboard	
						9					
										Number	inf Appliances (

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

😑 vSphere Client	Q	С 2 лонинализического - ©
	* IEI A300-Cluste	r01 Excisions
- 👩 at00-ves40140.co	Deploy OVF Template	Select an OVF template × Select an OVF template from remote UR, or local file system
- B ANDOMICH - D ANDONICH B ANDONI	Select an OVF template Select a name and folder	Enter a URL to download and install the OVF package from the internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive. O URL MID LINEL Press Leafer an enternit/Tetropress on Line
C acces C acces y G acces	3. Select a compute resource 4. Review details	Local Se Local Se VPWare-HCK-Connector-4: ova
 G ANSAN G HOLDE G HOLDE G HOLDE 	5. Select through 0. Ready to complete	
(3 HO) (3 HO) (3 HO) (3 HO) (3 HO)		
10 HOL.		CANCEL
	Photos_22	Policito Policito Policita Anton Discon 20 Mile / 19 Mile (19 Mile
A Recent Tasks	Alarms -	

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

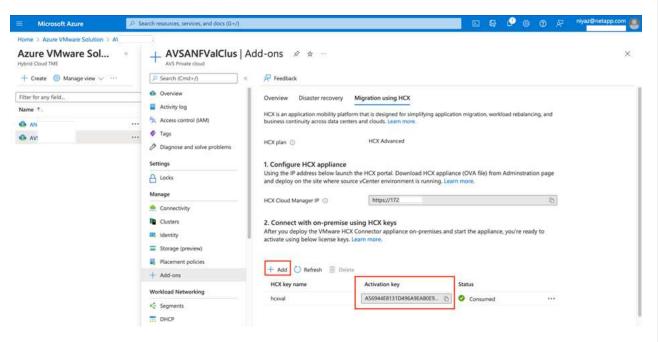


Power on the virtual appliance manually.

For step-by-step instructions, see the VMware HCX User Guide.

After you deploy the VMware HCX Connector OVA on-premises and start the appliance, complete the following steps to activate HCX Connector. Generate the license key from the Azure VMware Solution portal and activate it in VMware HCX Manager.

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





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

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



Use the password defined during the OVA deployment.

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



The on-premises HCX Connector should have internet access.

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



Use the FQDN to avoid connectivity issues later.

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

Continue.



Enter the VMware vCenter Server FQDN or IP address.

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



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

m HCX Manager	Dashboard	Appliance Summary	Configuration Administrati	on		ឆ	72.21.254.157	Version : 4.410 Type : Connector	admir
VMware-HCX FODN: IP Address: Version	K-440 VMware-HCX-440 172.2 4.4.1.0).ehcdc.com			()	CPU Used 1407 MHZ Memory		Free 688 MHZ Capacity 2095 MHZ Free 2316 MB	67%
Version: Uptime: Current Time:	20 days, 21 hours,	, 9 minutes mber 2022 07:44:11 PM UTi	c		0	Used 9691 MB Storage Used 296		Capacity 12008 MB Free 98G Capacity 127G	23%
NSX			vCenter		s	SO			
			https://a300-vcsa01.ehcdc.com	•	h	ttps://a300-vcsa01.ehcdc.com	n —		_
MANAGE			MANAGE			ANAGE			

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

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

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

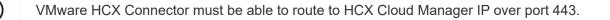
hortcuts ventories											
([])	ð		Ø	11		ంర్టం	п	Ŵ	I	٢	
Hosts and Clusters	VMs and Templates	Storage	Networking	Content Libraries	Global Inventory Lists	Workload Management	SnapCenter Plug-in for VMware VSphere	Cloud Provider Migration	Site Recovery	нсх	
Monitoring											
圁		Ċ.	E:	E.	\diamond	п					
Task Console	Event Console	VM Costomization Specifications	VM Storage Policies	Host Profiles	Lifecycle Manager	ONTAP tools					
Administratic	n										

1. Under Infrastructure, click Add a Site Pairing.



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

😑 vSphere Client 🛛 Q					.sitePairing	1 (24) K. (24)	an generation of	
 vispriere caent Q 						Q .0****	and a second s	9.0
CX Distributions therefore	* 3 *	Site Pairing					. C A00'A SI	TE DAUDUG
ol Editory Distanconnect In Transport Analytics envices		Ø By	Connect to F		×	ava azuro com-		
P Notissis Extension Migration Disaster Becowery		tine coit consectio	Remote HCX URL	https://172.	©			
ntem 3e Accessivation - 12 Support	×	Ø 🗣	Password		CONNECT			
		EDIT CONNECTOR						



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

	· · · ·	Site Pairi	ng			
Cashboard					C ADD A SITE PA	
astructure	~	-			C ADD A SITE /	AIRING
Site Pairing		ø	VMware-HCX-440	\rightarrow	6	
Interconnect		~	Ø https://172.21.254.157:443		hcx.8ebf3b0b7ddf4cc08e3f85.westeurope.avs.azure.com-	
Transport Analytics					cloud	
Network Extension	~					
Migration			1 interconnect(s)		V Protocology Sealers	
Disaster Recovery			a moles etcome etcome etcome			
item	~	EDIT CO	NNECTION DISCONNECT			
Administration				0.22	240-12-121	
C Support		Ø	VMware-HCX-440	\rightarrow	le HCX	
			& https://172.21.254.157.443 Raileigh		⊘ https ⊗ US W	
			1 Interconnect(s)			

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

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

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



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

← → 0	0 & ≓	P+ https://a300-vcsa01.ehcdc.com/ui/app/blug	pin/com.vmware.hybridity/com.vmware.ho	uhytiridConnect	公		0 8
\equiv vSphere Client Q				C	Administrator@EHCDC.COM ~	9	0
HCX Dashboard Infrastructure Site Paining Infection Transport Analytics Services Network Extension Megration	~	Interconnect Multi-Site Barvice Mesin Compute Profiles Sentinel Management Q C CREATE COMPU hcxdemo					OFILE
Disaster Recovery System & Administration Support	~	A Host a000-exa01 allocit conditioned 2007 Tent a000 exa01 allocit conditioned 2007 Enrota Resources Ba000-voca01 allocit conditioned 2007 A000-Cluster01 HCX Services C Services This Compute Profile is being used in 2 Service This Compute Profile is being used in 2 Service This Compute Profile is being used in 2 Service	Is in ordead (red) state for deployment container Orphyment Container (24300-voste01.ehcdc.com (roongude Nativorks @VM_3510 (Masagement) (v\$pnu Nativork Container (Nativork Externain A ⊯ VDS-Switch0 (Unlimited)	and a first state of the state	EDIT	

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

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



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

	<	Interconnect								
ICX Dashboard nfrastructure Ø Site Pairing	v	Multi-Site Service Mest	Network Profiles Sentin	vel Management						
Interconnect							Q C CR	EATE NETW	ORK PRO	DFIL
Services Network Extension Migration Disaster Recovery System	× •	VM_3510	MTU 9000	IP Pools IP Ranges	IP Usage(Used/Total)	Prefix Length	Gateway			
& Administration		EOIT DELETE		172.21.254.80 - 172.21.254.95	4/16	24	172.21.254.230			

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



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

$\leftarrow \ \rightarrow \ G$	08	Ov. https://x300-vcsa01.ehcdcccm/ui/app/plugin/com.vmware.hybridfty/com.vmware.hcs.hybridfConnect				⊚ ≡
\equiv vSphere Client	Q		C		9	0~
HCX Dashboard Infrastructure Site Pairing Inferconnect E: Transport Analytics Services	~	Interconnect Multi-Site Service Mesh Compute Profiles Service Mesh Network Profiles Sentinel Management ICC007			е мезн	L ĵ
Network Extension Network Extension Migration Disaster Recovery System & Administration @ Support		New version for service meth applances is available. Click on Update Applances to upgrade to latest. See Paring 		Serves	×	

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

S MARKAN AND SAL		_	_	_	_	_				I SCHOOL S		1000
vighere Glent Q										C 2**		
	12	nterconr	nect.									
read			ma liter									
inutive	<i>u</i> :	Countral	w Broatwer House Fides better Unigonet									
An Parrieg Management		Construction of the local division of the lo	(CC001 v								CON STREET	
hamport AAAAtsu	- 1										Con street	
*	8	"Training	BAppiances Class									5
arbeizik Bitariolen Algestian												
inarier Becovery					manut fund in the		Second Second	Summit Branco	Darrente Versione	Average result.		
n Januarian Jacon	×	0.1	CODET-de-4 er 1999/97-95-20-470-85-20-05-06-08-08-08-08-08-08-08-08-08-08-08-08-08-	45	0	(1) (1) (1) (1) (1) (1) (1) (1) (1) (1)		•	4422			
and .		9.3	COUT 48.0 is UNIX 9004-4014 UNIX 0001400 Consum 5000,012.000 Temper 4000,012.000 Temper 4001,012.000 Temper 400.010 Temper 400.010 Temper 400.010 Temper 400.000 Temper 400.0000 Temper 400.0000 Temper 400.0000 Temper 400.0000 Temper 400.0000 Temper 400.0000 Temper 400.0000 Temper 400.0000 Tempe 400.00000 Tempe 400.0000 Tempe 400.0000 Tempe 400.00000 Tempe 400.	6	iconter	722(2)+H		۲	6420	****		
			COULTING A w 64817747 Min Aska public Albanacitus Inneuro X300-Cultural Samage 2002/971,2004	G	Common Sta				1480	NA		
												-
		Applano	es on hix liebf.lb0b76df4cc08e3f85 westeurope.an	Licture			# Julium					
		00007-0			Approx						44.1	
					100	Crimania.	122147 (mm) 122147 (mm) 122147 (mm)					
		100007 H				COAD DIT	1230 78640 (mmg)repr					0.0
		100001-04	oin .		120	ci sus del					. 734	12

Step 6: Migrate workloads

Workloads can be migrated bidirectionally between on-premises and Azure SDDCs using various VMware HCX migration technologies. VMs can be moved to and from VMware HCX-activated entities using multiple migration technologies such as HCX bulk migration, HCX vMotion, HCX Cold migration, HCX Replication Assisted vMotion (available with HCX Enterprise edition), and HCX OS Assisted Migration (available with the HCX Enterprise edition).

To learn more about various HCX migration mechanisms, see VMware HCX Migration Types.

Bulk migration

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

To initiate bulk VM migrations, complete the following steps:

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

😑 vSphere Client 🛛 📿								C A	Aoministrator@EHC	оссом ч 🛛 🤅	0
ICX Disstribused	<	Migration	t 🗊	MIGRATE	c) (e				(Biddh)	
Ste Paring		Name	VMs/ S	torage/ Nem	ory/ CPUs		Progress	Start	End	Status	
S Transport Analytics											
ervices	~										
Network Extension											
Migration		Y a300-vcsa01.ehcdc.com	n 🔿 💿 1	72.30.156	2						
Disaster Recovery stem		> 2022-09-26 09:00 FLJVU	3	2.08	2.08	3	O Migration Complete	4	14		
& Administration		> 2022-09-26 08:35 8XMTM	1	2.68	2.69	1	Higration Complete				
@ Support	-	> 2022.09-18 16:21 ERC20	2	4.68	4.08	2	@ Draft	¥			
		> MG-18cbce94/Sep 16	ET9 5	10 GB	10 GB	6	Migration Complete	12.44 AU Sep 10			
		> MG-04abdee8 / Sep 16	1570	2.68	2.68	1	Stepation Complete	12.25 Add dag 16	2		
		> MG-ef7374dd / Sep 16	1000	2.GB	2.68	1	Migration Complete	12:11 Ass Bep 18	2		
		> MG-d2of93ef / Sep 14	1000 S	10 GB	10 08	5	O Migration Complete	02.05 ene Sep 1a	÷		
		> MG-69fecac8 / Sep 14	1000	2.09	2.08	.1	Migration Complete	11:02 AM	12. 1		
		> MG-548618cb / Sep 14	1000	2.08	2.08	1	Stagration Complete	10.04 AM Test 14	*		
			2	4:09/	4 GB		() Migration Complete	12.25 PM			

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

				Select VHs for Migration
 Transfer and Placement: 	This is migrating to ANF datastore			
Ouster-1	😦 📋 Datasheve2 ((11)(210)	9	Bok Migration	÷
C) (Seecity Destination Folder)	Same footiat as source	*	(Optional Switchover Schedule)	0
Switchover:				
 Extended Options: 				
and the second se				
Extended Options: (Seture MAC)				
and the second se				0
and the second sec	Opk/ Memory / vCPU		Migration Info	8
(Brian WAC)	098/ Memory / vCPU. Ø 2.08. 2.08. 1vCPU		Migration Info	ē.
Central Coversity (Central MAC)				9
(Brun MAC) (An Moralian) Demo_HCX_Buildol	0 2.08 2.08 1VCPU		Bulk Migration	(ā
(British MAC) (British MAC) M for Migradian) Demo, HOX, Buikd) Demo, HOX, Buikd	0 2.08 2.08 1.000 0 2.08 2.08 1.000		Bulk Migration Bulk Migration	ē.

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

 (\mathbf{i})

+ + C	0 & =	repaire 200	- spinistry	ehodo.tam////	entra patrices	man high inter		dan	patonia										4	0	*
😑 vSphere Client	Q																C		8 marine de la co ccon -	•	
CX Disabboard drastructure C Sta Parray Statesconvet St Interconvet St Transport Analytics		~		ation acking 5: Marating VM	Management	D rector				RO4	Progress				Start	e End			atie; ;	8	
P technology Externing		×.																			
Moraton Disaster Recovery				a100 vcs	a01.ehcdic.co	m → 🖕 172.	30.156.2														
Anterestration		×	01	Dono, HCK,			•	190	268	!	Highley.				2.91 PM 807 Sea 14				ettetteren allanteret		
Ca Administration			0	Dema, HCX.			•	3.08	2.68	ŧ.	Migrating	******			2.01 Ptr 801				Active stated		
			0		NA03		•	2.58	2.58	ŧ.	37% Same Survi				2-25 ANI 4277			5	analier (Ranfed)		
				100 million (1000)	14862			108	2.68	۰.	Ingrating.				201 (14 601			1	dishaver adjudied		
				Deno_HCK	by9-01			108	2.08	÷	Washing				205 (14 801			1	etchover stated		
			0	ALL ALL AND	Molaum		-	2.98	2.68	5	O Wandom Com				1102 Aut 421 7102 Aut 421 744 M	11.10 and 80 Bee-14	1 1-1	. 10	pullus completed		
V Recent Tasks	danna																				
an Nata Y	Target			Natur	-e ¥	Getala			subatur		*	Donund For	.*	Start Time		Completion Ter		۲	Server		,
ulk Migration	(D. Dens, HDC, J	ue:03	1		245.0	Trahider Starte	ed .		Americator	00	KODC COM	0.910		08/14/202	2.2.05 11 PM			_	hybridity-manager		
ula Migration	(D Demis HOK)	URD?			01-0	Transfer Starts	10		American	00-	KDC:COM	0.05		08/14/202	2.2.03 11 PM				hybrioty-manager		
all Mgradon	D Denie_HCK_B	UHD3			0.40	Transfer Starts	e)		American	041-	EDCCOM	0.00		00/14/202	17.20511944				syskisty-manager		
uk Migration	(2 Dene, HOL, 3	UACS.			53.0	Transfer Starts	18		Administrator	\$41-	KDC COM	0.945		09/14/202	2,2:0511244				hybridly-manaper		
tuk Migration	(D. Démis, HOK, B	WHOM I	1		275 0	Thanster Starts	nd .		Americhistor	00	KIDC COM	0.mil		08/14/202	2.20511PH				hybrioty-manager		

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

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

e + 0 0	A # month	interary determined Datastic	midates 2143	673e56e3-1000-4345	NU1-1151(524)	Noniciana -			\$	0	2 1
= vSphere Clent Q								c			
, 0 8 8 0	DatastoreO2 Across	Permissions Piles	Hosts VHs								
 Ø vc.bier3008.7outriccobidt. BE SODC-Datacenter 	Victure Nachines VM Templates VMs on ANF datastore after migra	tion							* 04	N. HOLM	
· · · · · · · · · · · · · · · · ·	and a second	Bon Shie t		Produced Space	Vetiges	net OV :	Had Mart		r <u>0</u> r	no.HCK.J	
vic beersook footbic cobers. E SOCC-Ontexenter Contexenter Contexenter Contexenter Contexenter	VMs on ANF datastore after migra	Contraction of the Contraction o	- State		Ved fpers 246.07.46	net OV	Head March /		+ <u>0</u>	no.HCK.H	
Vot bebradow fourth code of . B SODO-Detacenter Detailsong	VMs on ANF datastore after migra	State t		208					+ <u>0</u>	nu voruli	
v: berzock/osticcober: E SOCC-Determent Contentore0 Contentore0 Contentore0 Contentore0	VMs on ANF datastore after migra	State 1 Proversid On	V Nortal	3 G8	245.87 MB	0 HQ	244.66		* <u>0</u>	nu voul	
Contraction to the code of the code o	VMs on ANF datastore after migra	Proventil Cri Proventil Cri Proventil Cri	vi Nornal vi Nornal	2.08 3.08 3.08	748.87 MB 751.24 MB	0 HQ 0 HQ	264.MB 280.MB		, t <u>or</u>	10.100.1	

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

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

Workload Migration using HCX

Here is a screenshot of HCX vMotion option.

€ 0 C	O & at should	100-100	Clahobulom/sites/plag	-	main physical sec-	10.00	riputentit								\$	0	\$
😑 vSphere Client	٩													C		0	
KX 3 bestcord #testrature ⊘ tax Parrog		-	gration tracking 12 minut	met	(27 Million TE)							124-94	Rea		1007047	85	
A Hercenaut Ic. Transport Analytics			Э миритрим			thorage/	Wemerg/ CPUs	Propess				Sart	. Del	-	Taka		-
 Traducció d'alternation 	3																
Mgratus																	
Disaster Recovery			a allo vesatteh	605.00	m -> + 172.30.154												
Vatiens			> Denu HCK Vilabos			- 21	2.08	38% Sec. 1	int :	0.	TRI ad Arm	11.52 our spin-		_	Molton Plansfer In Progress		
Administration		C	Down HCk, Contings	10.00) C	20	06 2.06 (Onian	as Complete			TO DIS LAN ST."	NO TE SANGTE Des TE	10 mpc	Migration companies		
			transfer and the second		-	20	208 1	ONyst	Constele			1225 PH 801	1231 Paratel	12.000	Righter comprised		
		0	> MCX_Photor_47	8.A													
					-		8 218	Owne	et Corgana			12:25 Hic 807 Bell 17	1235-44807 Bei 10	.919	Righter property		
		c	NX, Peter, N	-	-		CB 2 CB 1	Contraction of the	et Complete			12.25 HILBOT	1235-44807		Nigotos constella		
		0	NX, Peen, 11		-	23		@ Mayor				12.25.44capt Bes 17	12.35.44.607 Bei 10 12.54.94.607	trie			
	Alarms.	0	 MX, Polin, N 			23	09 208	@ Mayor	es Complete			12.25 Holdst Bas 13 12.17 Holdst Bas 13 12.01 Holdst	1235-44407 Ber 10 1224-947020 Ser 10 1237-44407	trie	Nigration completed		
·· Becent Tasks	tiarms forget		 MX, Pollar, N 		e e oran	20	09 208	@ Mayor	es Complete			12.25 Holdst Bas 13 12.17 Holdst Bas 13 12.01 Holdst	1235-44407 Ber 10 1224-947020 Ser 10 1237-44407	7 mil	Nigration completed		
Pecent Tasks /			 Amountage Count MOL/Neter, 19 MOL/Neter, 15 MOL/Neter, 15 MOL/Neter, 28 MOL/Neter, 28 			20	CB 2 GB 1	© mitre	es Complete es Complete	Ť		1225 Hot 607 Ben 10 (217 Hot 807 (201 Hot 607 (201 Hot 607 Ben 10	12.35 Auto0 Ber 12 12.54 Per 22 Ber 13 12.55 Anto00 Ber 19	2 min	Ngalar sinskini Ngalar sinskini		
Recent Tasks /	faget		 Antoniosoglicitorii MCX, Penni, H MC		Drian.	20	00 2.00 1 00 2.00 1	C Marel	es Complete es Complete T Guerent Tur		Blat Type	1225 Hot 601 Bee 10 (2117 Hot 601 (2117 Hot 601) (2111 Hot 601) Bee 10 (2117 Hot 601) Het 10 (2117 Hot 601) Het 10 (2117 Hot 601) Het 10 (2117 Hot 601) (2117 Hot 601) (211	12:33-44.837 Ber 13 12:54-94.827 Ber 13 12:53-94.837 Set 13 Set 13 Set 13 Set 13	Tries Tries	Ngalar provided Ngalar provided		
< Recent Tasks A	farget (\$ Dama_HCK_VHotor		Annovation of the second		Drian.	20	00 2.00 1 00 2.00 1 edutor 0+CDC.COMA	C Mgraf C Mgraf Dreneti alter Streneti alter	es Complete es Complete T Ourseet Fair S mit		Blat Tese Olyma/2022	1225 He 807 He 11 (217 He 837 He 0 (211 He 8487 He 11 (10 57 H 1) (10 57 H 1) (10 59 H 1)	C235+64307 Nor-12 C255+944207 Nor-12 Sec-12 Companion Three C045442022, 50:20	7 min 7 min	Ngoslan completed Ngoslan completed T I foreign AXXX-scractl electric com		

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

HCX vMotion

i

Make sure sufficient bandwidth is available to handle the migration.

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

Conclusion

Whether you're targeting all-cloud or hybrid cloud and data residing on any type/vendor storage in onpremises, Azure NetApp Files and HCX provide excellent options to deploy and migrate the application workloads while reducing the TCO by making the data requirements seamless to the application layer. Whatever the use case, choose Azure VMware Solution along with Azure NetApp Files for rapid realization of cloud benefits, consistent infrastructure, and operations across on-premises and multiple clouds, bidirectional portability of workloads, and enterprise-grade capacity and performance. It is the same familiar process and procedures used to connect the storage and migrate VMs using VMware vSphere Replication, VMware vMotion, or even network file copy (NFC).

Takeaways

The key points of this document include:

- You can now use Azure NetApp Files as a datastore on Azure VMware Solution SDDC.
- You can easily migrate data from on-premises to Azure NetApp Files datastore.
- You can easily grow and shrink the Azure NetApp Files datastore to meet the capacity and performance requirements during migration activity.

Where to find additional information

To learn more about the information described in this document, refer to the following website links:

Azure VMware Solution documentation

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

Azure NetApp Files documentation

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

• VMware HCX User Guide

https://docs.vmware.com/en/VMware-HCX/4.4/hcx-user-guide/GUID-BFD7E194-CFE5-4259-B74B-991B26A51758.html

Region Availability – Supplemental NFS datastore for ANF

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



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

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

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

NetApp for GCP / GCVE

NetApp Capabilities for Google Cloud Platform GCVE

Learn more about the capabilities that NetApp brings to the Google Cloud Platform (GCP) Google Cloud VMware Engine (GCVE) - from NetApp as a guest connected storage

device or a supplemental NFS datastore to migrating workflows, extending/bursting to the cloud, backup/restore and disaster recovery.

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

- Configuring GCVE in GCP
- NetApp Storage Options for GCVE
- NetApp / VMware Cloud Solutions

Configuring GCVE in GCP

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

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



In-guest storage is the only supported method of connecting Cloud Volumes ONTAP and Cloud Volumes Services to GCVE.

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

- Deploy and Configure GCVE
- Enable Private Access to GCVE

View the detailed configuration steps for GCVE.

NetApp Storage Options for GCVE

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

Please visit Supported NetApp Storage Options for more information.

Google Cloud supports NetApp storage in the following configurations:

- Cloud Volumes ONTAP (CVO) as guest connected storage
- · Cloud Volumes Service (CVS) as guest connected storage
- · Cloud Volumes Service (CVS) as a supplemental NFS datastore

View the detailed guest connect storage options for GCVE.

Read more about NetApp Cloud Volumes Service datastore support for Google Cloud VMware Engine (NetApp blog) or How to use NetApp CVS as datastores for Google Cloud VMware Engine (Google blog)

Solution Use Cases

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

• Protect (includes both Disaster Recovery and Backup / Restore)

- Extend
- Migrate

Browse the NetApp solutions for Google Cloud GCVE

Protecting Workloads on GCP / GCVE

Application Consistent Disaster Recovery with NetApp SnapCenter and Veeam Replication

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 Google Cloud.

Authors: Suresh Thoppay, NetApp

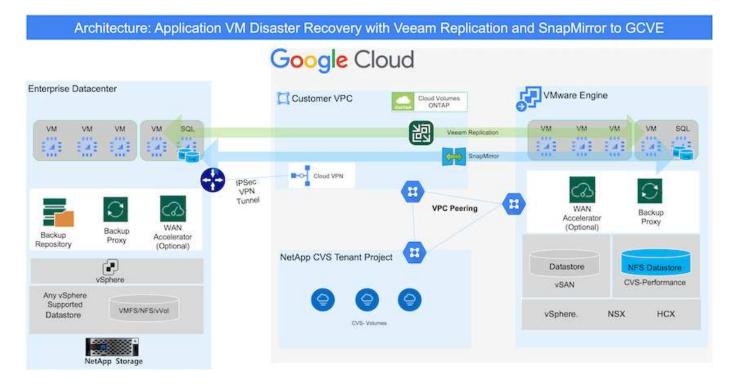
Overview

Many customers are looking for an effective disaster recovery solution for their application VMs hosted on VMware vSphere. Many of them use their existing backup solution to perform recovery during diaster. Many times that solution increase the RTO and doesn't meet their expectations. To reduce the RPO and RTO, Veeam VM replication can be utilized even from on-prem to GCVE as long as network connectivity and environemnt with appropriate permissions are available.

NOTE: Veeam VM Replication doesn't protect VM guest connected storage devices like iSCSI or NFS mounts inside the guest VM. Need to protect those seperately.

For application consistent replication for SQL VM and to reduce the RTO, we used SnapCenter to orchestrate snapmirror operations of SQL database and log volumes.

This document provides a step-by-step approach for setting up and performing disaster recovery that uses NetApp SnapMirror, Veeam, and the Google Cloud VMware Engine (GCVE).



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 Google Cloud network, use the connectivity options like dedicated interconnect or Cloud VPN. Segments should be created based on the on-premises VLAN design.



There are multiple options for connecting on-premises datacenters to Google Cloud, which prevents us from outlining a specific workflow in this document. Refer to the Google Cloud documentation for the appropriate on-premises-to-Google 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 BlueXP 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 Veeam software and start replicating virtual machines to Google Cloud VMware Engine instance.
- 4. During a disaster event, break the SnapMirror relationship using BlueXP and trigger failover of virtual machines with Veeam.
 - a. Reconnect the ISCSI LUNs and NFS mounts for the application VMs.
 - b. Bring up applications online.
- 5. Invoke failback to the protected site by reverse resyncing SnapMirror after the primary site has been recovered.

Deployment Details

The first step is to configure Cloud Volumes ONTAP on Google Cloud (cvo) and replicate the desired volumes to Cloud Volumes ONTAP with the desired frequencies and snapshot retentions.

Architecture: Cloud Ve oogle Cloud	blumes ONTAP comm	unication to GCVE	
VMware Engine	Custom		
	Connection	ONTAP	Compute engine
VSAN		Persistent disks	Cloud storage
vSphere NSX		Hot data	Cold data

For sample step-by-step instructions on setting up SnapCenter and replicating the data, Refer to Setup Replication with SnapCenter

Review of SQL VM protection with SnapCenter

Configure GCVE hosts and CVO data access

Two important factors to consider when deploying the SDDC are the size of the SDDC cluster in the GCVE 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.

NetApp Cloud Volume Service for NFS Datastore and Cloud Volumes ONTAP for SQL databases and log can be deployed to any VPC and GCVE should have private connection to that VPC to mount NFS datastore and have VM connect to iSCSI LUNs.

To configure GCVE SDDC, see Deploy and configure the Virtualization Environment on Google Cloud Platform (GCP). As a prerequisite, verify that the guest VMs residing on the GCVE hosts are able to consume data from Cloud Volumes ONTAP after connectivity has been established.

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

Based on deployment scenario, the Veeam backup server, backup repository and backup proxy that needs to be deployed. For this use case, there is no need to deploy object store for Veeam and Scale-out repository also not required.

Refer to the Veeam documentation for the installation procedure For additional information, please refer Migration with Veeam Replication

Setup VM Replication with Veeam

Both on-premises vCenter and GCVE vCenter needs to be registered with Veeam. Setup vSphere VM Replication Job At the Guest Processing step of wizard, select disable application processing as we will be utilizing SnapCenter for application aware backup and recovery.

https://netapp.hosted.panopto.com/Panopto/Pages/Embed.aspx?id=8b7e4a9b-7de1-4d48-a8e2-b01200f00692

Failover of Microsoft SQL Server VM

https://netapp.hosted.panopto.com/Panopto/Pages/Embed.aspx?id=9762dc99-081b-41a2-ac68-b01200f00ac0

Benefits of this solution

- Uses the efficient and resilient replication of SnapMirror.
- Recovers to any available points in time with ONTAP snapshot retention.
- Full automation is available for all required steps to recover hundreds to thousands of VMs, from the storage, compute, network, and application validation steps.
- SnapCenter uses cloning mechanisms that do not change the replicated volume.
 - This avoids the risk of data corruption for volumes and snapshots.
 - Avoids replication interruptions during DR test workflows.
 - Leverages the DR data for workflows beyond DR, such as dev/test, security testing, patch and upgrade testing, and remediation testing.
- Veeam Replication allows changing VM IP addresses on DR site.

Application Disaster Recovery with SnapCenter, Cloud Volumes ONTAP and Veeam Replication

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 Google Cloud.

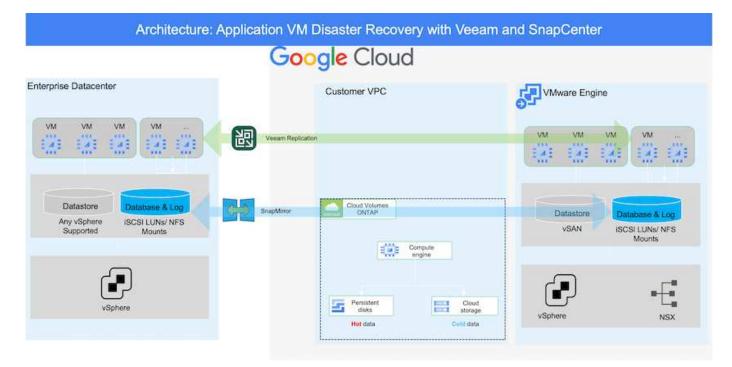
Authors: Suresh Thoppay, NetApp

Overview

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 Veeam 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, Veeam, and the Google Cloud VMware Engine (GCVE).



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 Google Cloud network, use the connectivity options like dedicated interconnect or Cloud VPN. Segments should be created based on the on-premises VLAN design.



There are multiple options for connecting on-premises datacenters to Google Cloud, which prevents us from outlining a specific workflow in this document. Refer to the Google Cloud documentation for the appropriate on-premises-to-Google 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 Veeam software and start replicating virtual machines to Google Cloud VMware Engine instance.
- 4. During a disaster event, break the SnapMirror relationship using Cloud Manager and trigger failover of virtual machines with Veeam.
 - a. Reconnect the ISCSI LUNs and NFS mounts for the application VMs.
 - b. Bring up applications online.
- 5. Invoke failback to the protected site by reverse resyncing SnapMirror after the primary site has been recovered.

Deployment Details

Configure CVO on Google Cloud and replicate volumes to CVO

The first step is to configure Cloud Volumes ONTAP on Google Cloud (cvo) and replicate the desired volumes to Cloud Volumes ONTAP with the desired frequencies and snapshot retentions.

ogle Cloud VMware Engine		Customer VP	с	
	Private Connection	-	Cloud Volumes	Compute engine
Datastore vSAN			Persistent disks Hot data	Cloud storage Cold data
vSphere NSX		L		

Replication with SnapCenter

Setup Replication with SnapCenter

Two important factors to consider when deploying the SDDC are the size of the SDDC cluster in the GCVE 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.

Cloud Volumes ONTAP can be deployed to any VPC and GCVE should have private connection to that VPC to have VM connect to iSCSI LUNs.

To configure GCVE SDDC, see Deploy and configure the Virtualization Environment on Google Cloud Platform (GCP). As a prerequisite, verify that the guest VMs residing on the GCVE hosts are able to consume data from Cloud Volumes ONTAP after connectivity has been established.

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

Install Veeam Components

Based on deployment scenario, the Veeam backup server, backup repository and backup proxy that needs to be deployed. For this use case, there is no need to deploy object store for Veeam and Scale-out repository also not required.

Refer to the Veeam documentation for the installation procedure

Setup VM Replication with Veeam

Both on-premises vCenter and GCVE vCenter needs to be registered with Veeam. Setup vSphere VM Replication Job At the Guest Processing step of wizard, select disable application processing as we will be utilizing SnapCenter for application aware backup and recovery.

Setup vSphere VM Replication Job

Failover of Microsoft SQL Server VM

Failover of Microsoft SQL Server VM

Benefits of this solution

- Uses the efficient and resilient replication of SnapMirror.
- Recovers to any available points in time with ONTAP snapshot retention.
- Full automation is available for all required steps to recover hundreds to thousands of VMs, from the storage, compute, network, and application validation steps.
- SnapCenter uses cloning mechanisms that do not change the replicated volume.
 - This avoids the risk of data corruption for volumes and snapshots.
 - Avoids replication interruptions during DR test workflows.

- Leverages the DR data for workflows beyond DR, such as dev/test, security testing, patch and upgrade testing, and remediation testing.
- Veeam Replication allows changing VM IP addresses on DR site.

Migrating Workloads on GCP / GCVE

Migrate workloads to NetApp Cloud Volume Service datastore on Google Cloud VMware Engine using VMware HCX - Quickstart guide

One of the most common use cases for the Google Cloud VMware Engine and Cloud Volume Service datastore is the migration of VMware workloads. VMware HCX is a preferred option and provides various migration mechanisms to move on-premises virtual machines (VMs) and its data to Cloud Volume Service NFS datastores.

Author(s): NetApp Solutions Engineering

Overview: Migrating virtual machines with VMware HCX, NetApp Cloud Volume Service datastores, and Google Cloud VMware Engine (GCVE)

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

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



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

High-level steps

This list provides the high-level steps necessary to pair & Migrate the VMs to HCX Cloud Manager on the Google Cloud VMware Engine side from HCX Connector on-premises:

- 1. Prepare HCX through the Google VMware Engine portal.
- 2. Download and deploy the HCX Connector Open Virtualization Appliance (OVA) installer in the onpremises VMware vCenter Server.
- 3. Activate HCX with the license key.
- 4. Pair the on-premises VMware HCX Connector with Google Cloud VMware Engine HCX Cloud Manager.
- 5. Configure the network profile, compute profile, and service mesh.
- 6. (Optional) Perform network extension to avoid re-IP during migrations.
- 7. Validate the appliance status and ensure that migration is possible.
- 8. Migrate the VM workloads.

Prerequisites

Before you begin, make sure the following prerequisites are met. For more information, see this link. After the prerequisites, including connectivity, are in place, download HCX license key from the Google Cloud VMware Engine portal. After the OVA installer is downloaded, proceed with the installation process as described below.

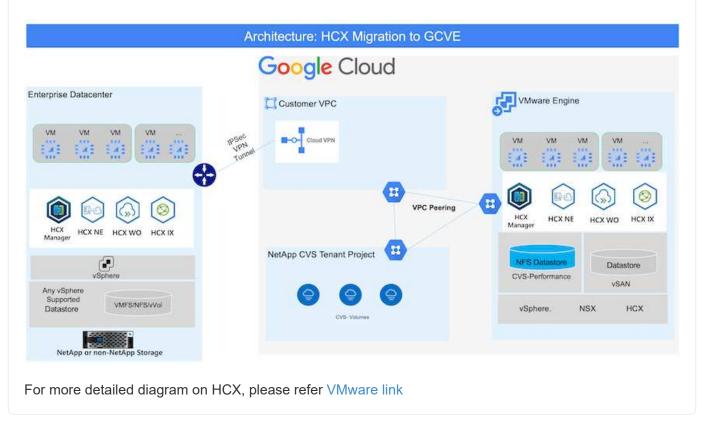


HCX advanced is the default option and VMware HCX Enterprise edition is also available through a support ticket and supported at no additional cost. Refer this link

- Use an existing Google Cloud VMware Engine software-defined data center (SDDC) or create a private cloud by using this NetApp link or this Google link.
- Migration of VMs and associated data from the on-premises VMware vSphere- enabled data center requires network connectivity from the data center to the SDDC environment. Before migrating workloads, set up a Cloud VPN or Cloud Interconnect connection between the on-premises environment and the respective private cloud.
- The network path from on-premises VMware vCenter Server environment to the Google Cloud VMware Engine private cloud must support the migration of VMs by using vMotion.
- Make sure the required firewall rules and ports are allowed for vMotion traffic between the onpremises vCenter Server and SDDC vCenter.
- Cloud Volume Service NFS volume should be mounted as a datastore in Google Cloud VMware Engine. Follow the steps detailed in this link to attach Cloud Volume Service datastores to Google Cloud VMware Engines hosts.

High Level Architecture

For testing purposes, the lab environment from on-premises used for this validation was connected through a Cloud VPN, which allows on-premises connectivity to Google Cloud VPC.



Solution Deployment

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

HCX Cloud Manager component automatically gets installed as you provision private cloud with VMware Engine. To prepare for site pairing, complete the following steps:

1. Log in to the Google VMware Engine Portal and sign-in to the HCX Cloud Manager.

You can login to HCX Console either by clicking on the HCX version link

	Resources			
5	 gove ovs hw eu west3 			S LAUNCH VERHERE CULOUT S ADD NOT
2	SUMMARY CUSTLES	BURNETS ACTIVITY VEHICLE MANAGEMENT NETWO	DEK ADVANCED VCENTUR SETTINGE DAS CONFIGURATION	
2		Name grave (vs.fex-ex-vent13	Status • Operational	Charters L
	Ś	Stratched No	Primary Location surges weit3 + s-tone a + VE Platement Group 1	Sevendary Location
	Basic Isra	Oned Monitaring (0	Private Cloud DNS Servers () 10.0.16.0, 10.0.16.9 Case	vSphere/vSAN subnets CIDR range 100, 16.0/24
		IP Plan Version 1	vCenter logis indu- Verv Relet primeral	NSX T high info View Rent provint
	1.000.000	Total nodes	Tetal CPU capacity 100 cores	Tetal RAM 2304 GB
	- Experience	Total storage capacity 57.6 TB Raw, 9.6 TB Cache, All Flash	2007 00/00	Konz zw.
		vSphere version 2.0x2	NSX-T Edition 74(3):/T Advanced	HCX Manager Cloud version

or clicking on HCX FQDN under vSphere Management Network tab.

	Resources					
8	← gove-ovs-hw-eu-west3				& DAUNCH VSPH	ERE CLIENT @ ADD NODE
2	SUMMARY CLUSTERS SUBNETS ACTIVITY	VEPHERE MANAGEMENT NETWORK	ADVANCED VCINTER SETTINGE DNS CONFIGURATION			
PAPER	da Drownland ar CSV	6)				dia determinante data
4	Type	Verslap	C IQON	5	IP Address	
~	(Center Server Appliance	10.2.18272205	nur 5790157458ultzunpr wirt3.gw.gmg		10,0.1A.6	
à,	NSX Marager	and the state of the	mer 13041/7458cltaurupt weilitigen gemp		10.0.16.11	
	HDC	-	Nor-StOK2/1450-Benner webling manuel		30-0-16-13	
	(9)	7.0.2.18836573	envi-57896.07458c0Taurice-week3.gun.goog		10.0.16.15	
	156	7.0.2.18856573	exel 715444/7456cdfaurope-went3.gve.goog		202.14.19	
	691	70.2.558565672	essi-57902/745bcittaurope-went5gve.goog		2003636	
	DNS.Servic 2		m2.67900/7453otteurope-weith.pvi.and		50.0.1K.V	
	DNS Server 1	-	ex1/5709977455cdf.numpe-weat3.gvit.gvit.gvit.gvit.gvit.gvit.gvit.gvit		20.0.16.8	

- 2. In HCX Cloud Manager, go to Administration > System Updates.
- 3. Click **Request download link** and download the OVA file.

Or DatAboard Whethwature Or Size Hanog Size Hanog Entroport Analytics Entroport Analytics Entroport Onework Network Extension Network Extension Network Extension	System Updates Par your remote data sense ##60001 complex complex Local MCX [complex row unitable]							
40 Disaster Recovery Administration	Current Version	System Name	* Data	100	Restore Type	* NEX Version	4 VEWeen	· Cies To Dateset
the Restmin Codates Troubleshooting Audit Logs	O # 4520	Non 5604277458x88 wompen	with pre-prop-cloud	Ø	HEXCOME	112 0 0106730 Watero	7.0.3 10272239	æ
Activity Logis Arets OCE Otec	Remote HCX							Normal di Kopi
	Carrent Version	Equilation (Section	 (a) Sinter 	1.6997		Rymen Tane	 Cepy Ta 	Dateri
	4520	HOLATE		G		HCX Contractor		Ċ.
								Names of Asses

4. Update HCX Cloud Manager to the latest version available from the HCX Cloud Manager UI.

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

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

- 1. Have the ova downloaded from the HCX Console on Google Cloud VMware Engine as stated in previous step.
- 2. After the OVA is downloaded, deploy it on to the on-premises VMware vSphere environment by using the **Deploy OVF Template** option.

Deploy OVF Template	Select an OVF template ×
1 Select an OVF template	Select an OVF template from remote URL or local file system Enter a URL to download and install the OVF package from the internet, or browse to a location accessible from your computer,
2 Select a name and folder	such as a local hard drive, a network share, or a CD/DVD drive. O URL
3 Select a compute resource	
4. Review details	Local file
5 Select storage	UPLOAD FILES VMware-HCX-Connector-4.5.2.0-20914338.ova
6 Ready to complete	
	CANCEL

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



Power on the virtual appliance manually.

For step-by-step instructions, see the VMware HCX User Guide.

After you deploy the VMware HCX Connector OVA on-premises and start the appliance, complete the following steps to activate HCX Connector. Generate the license key from the Google Cloud VMware Engine portal and activate it in VMware HCX Manager.

1. From the VMware Engine portal, Click on Resources, select the private cloud, and **click on download icon under HCX Manager Cloud Version**.

Resources			
🔶 gove ovs hw eu west3			Q, LAURICH VSPHERE CUIDHT 🛛 ADD NOT
SUMMARY CLUSTERS	JURNETS ACTIVITY VERMINE MANAGEMENT NETWO	IN ADVANCED VCINTUE SETTINGE ON CONFIGURATION	
	Name	Status	Charters
	give (vs fee ex west3	Operational	
6	Stratched No	Primary Location surops-weit3 > v-tone-a = VE Platement Group 1	Sevendary Socation
0	Could Monitoring G	Private Cloud DNS Servers ()	vSphere/vSAN subnets CIDR range
Basic Info		10.0.16.0.10.0.16.9 Carm	100,160/24
	IP Plan Version	vCenter logis livfu	NSX-T lingle info
	1	Vew Restances	View Rent provend
	Total nodes	Total CPU sequenty	Total RAM
	3	100 cores	2304 G8
-52	Total storage capacity		
Capacity	57.6 TB Rave, 9.6 TB Cache, All-Flanh		
	vSphera version	NEX-T Edition	HCX Manager Claud version
	3.022	343XT Advanced	422 📥 🖸

Open Downloaded file and copy the License Key String.

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



Use the hcxmanagerIP and password defined during the OVA deployment.

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



The on-premises HCX Connector should have internet access.

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



Use the FQDN to avoid connectivity issues later.

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



For Embedded PSC, Enter the VMware vCenter Server FQDN or IP address.

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

same as the previous page.



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

HCX-RTP			()	CPU	Free 1543 MHZ	26%
P Address:	172.21.254.155		0	Used 552 MHZ	Capacity 2095 MHZ	97655
Version:	4.5.2.0		\bigcirc	Memory	Free 2472 MB	79%
Jptime: Current Time:	13 days, 21 hours, 6 minutes Thursday, 16 February 2023 05:	59:00 PM UTC	0	Used 9535 MB	Capacity 12008 MB	1976
			0	Storage	Free 76G	
			(!)	Used 7.7G	Capacity 84G	9%
NSX		vCenter		so		
NSA						
		https://a300-vcsa01.ehcdc.com	• •	ttps://a300-vcsa01.ehcd	c.com	
MANAGE		MANAGE		ANAGE		
MANAGE		MANAGE	м	ANAGE		

Step 4: Pair on-premises VMware HCX Connector with Google Cloud VMware Engine HCX Cloud Manager

After HCX Connector is deployed and configured on on-premises vCenter, establish connection to Cloud Manager by adding the pairing. To configure the site pairing, complete the following steps:

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

vSphere C	Client Q							C	AdministratorgEHCDC.COM ~	0
Shortcuts										
Inventories									\frown	
	ð)		\otimes	11		000		(٢	
Hosts and Clusters	VMs and Templates	Storage	Networking	Content Libraries	Global Inventory Lists	Workload Management	ShapCenter Plug-in for VMware vSphere	Site Recovery	нск	
Monitoring										
		E.	R			\Diamond				
Task Console	Event Console	VM Customization Specifications	VM Storage Policies	Host Profiles	ONTAP tools	Lifecycle Manager				
Administratio	'n									
Q										
Licensing										

2. Under Infrastructure, click Add a Site Pairing.



Enter the Google Cloud VMware Engine HCX Cloud Manager URL or IP address and the credentials for user with Cloud-Owner-Role privileges for accessing the private cloud.

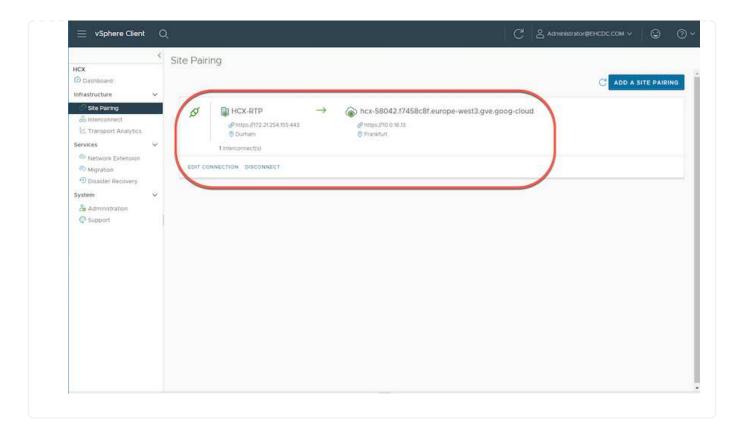
Connect to R	Remote Site	\times
Remote HCX URL	https://hcx-58042.f7458c8f.europe-west3.g	i
Username	cloudowner@gve.local	i
Password		
	CANCEL	CONNECT

3. Click Connect.



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

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



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

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

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



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

vSphere Client	Q	1077 N		
HCX Dashboard Infrastructure Ste Pairing Interconnect Transport Analytics	~	Interconnect Muti-Site Service Mesh Compute Profiles Service Mesh Network P	rofiles Sentinel Management	
Services Network Edension Migration Disaster Recovery System And Administration Support	×	HCX-CP Service Resources Ba300-Vesa01.ehcdc.com A300-Cluster01 HCK Services O	Deployment Container Ca300-vesa0t.eheddc.com A300-Cluster01 Datastore A300_NF5_D503 CoultAemory Reservations CoultAemory Reservations CoultAemory Reservations CoultAemory Reservations CoultAemory Reservations CoultAemory Reservations CoultAemory Reservations	Network WM_3510 Management (Schere Replication) (Uplink) (vitation) © EDIT Network Container (Network Extension Applance Limit) WDS-Switch0 (Unlimited)
		EDIT DELETE REVIEW CONNECTION B	utes	

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

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



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

	~	Interconnect							
Dashboard Dashboard nfrastructure	×	Muti-Site Service Mesh	Notwork Profiles Sertine	Management					
Interconnect							Q C CREAT	NETWORK PRO	offici
ervices	~	O VM_3510							
Migration Disaster Recovery		Network Detain Backing: VM_3510	мтці 1350	IP Pools IP Ranges	@ Usage(Used/Total)	Prefix Length	Gateway		
System	~	show more		172.21.254.81 - 172.21.254.95	2/15	24	172.21.254.231		
		EDIT DELETE							

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

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

	102			- A - 8 A
CX D Dashboard trestructure Ste Paining Sterconnect Transport Analytics	~	Interconnect Muti-Site Service Mesh Compute Profiles Service Mesh Network Profiles Sentinel Management	Q. C ^e create se	RVICE MESH
ervices	~	RTP-GCVE		
Network Extension Negration Disaster Recovery ystem & Administration © Support	÷	Ste Paring Charter Charter HCX-RTP Durinem HCX-CP Uprivis (Overndden) Q VM_2510 C MCX-MINE C		×
		VIEW APPLIANCES RESYNC EDIT DELETE MORE -		

(i)

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

	5	Intercon	mect						
t Danheourid		Math-Star for							
astructure		005-00-0	Annya Sauli						
Die Parry		Smbite P	Index Device Mark Andreas France Destine Management						
Interconnect		- 4-	RTP-OCVE v						EDIT SERVICE MESH
Tianaport Analytics		Atopie	oy BApplanon Etails						
Network Extension		Annilan	ices on NCX-RTP						
Mage groupe									C
Disaster Recovery									
ann, Ar generated and generated	12		Xaatavo Nene	1.2	Applanet Type	27.400000	Turnet Barne	Concern Version	
¹ filoport		0.7	ITTO-OCYSIAN w statutej-word-auto-ben-disperimenty fampure A300 Outseth Strange A300, VPL_2003		HCR WARLIN	122.2548 (Brogerer (James Balgarer) (James (1999 (Brogerer))		4520	
			0 >	WTV-0225-06-3 Mr 011521-6e4-4/m a-f10-estabilitation Compare 3200-3410_00001 Hereare Container, 420-540000 Estational Memories 1/9 00000		HOCHET CO.	0222348(<u></u>)	۲	4520
			10%-00-9 W0-0 ar 2051758-0% 470-088-088843-0004 Sampler ADO-Outed fromp ADO-Outed		G HOR WARK CIT			1210	
									8. Augustion of the
		Applan	ices on fick-\$8042.17458c8f.europe-west3.gvi	9909-tioud					
		Approve	a Marine	Augment for	P 5.00+1	0			Garrell Weather
		079-029	V5 (H-87	1800 HOR	walate 0.000	(newsprote (clares framew), some (3			4320
		1011-003	We want the	4	NAME OF TAXABLE PARTY.				7380

Step 6: Migrate workloads

Workloads can be migrated bidirectionally between on-premises and GCVE SDDCs using various VMware HCX migration technologies. VMs can be moved to and from VMware HCX-activated entities using multiple migration technologies such as HCX bulk migration, HCX vMotion, HCX Cold migration, HCX Replication Assisted vMotion (available with HCX Enterprise edition), and HCX OS Assisted Migration (available with the HCX Enterprise edition).

To learn more about various HCX migration mechanisms, see VMware HCX Migration Types.

The HCX-IX appliance uses the Mobility Agent service to perform vMotion, Cold, and Replication Assisted vMotion (RAV) migrations.



The HCX-IX appliance adds the Mobility Agent service as a host object in the vCenter Server. The processor, memory, storage and networking resources displayed on this object do not represent actual consumption on the physical hypervisor hosting the IX appliance.

HCX vMotion

This section describes the HCX vMotion mechanism. This migration technology uses the VMware vMotion protocol to migrate a VM to GCVE. The vMotion migration option is used for migrating the VM state of a single VM at a time. There is no service interruption during this migration method.



Network Extension should be in place (for the port group in which the VM is attached) in order to migrate the VM without the need to make an IP address change.

1. From the on-premises vSphere client, go to Inventory, right- click on the VM to be migrated, and select HCX Actions > Migrate to HCX Target Site.

	C JA Meson 202010	STOR 3	o to a lo (peries)							
80 (1) (2)			ure Permisione Detailores	VILLIAN CONTRACT VI	3232010					
	Surriary Monto	careg	ore: Herrisons Destroyes	WEIWOOKS SEGERATE 12	powiet .					
() countries	-	S	Gunt Ob VMware Photon 05-8	4.9-X					Switt	OH TO MEN VE
di constante a			Compatibility EDV-6.7 and later CVM	service 36					0	O Hz
() KCARCE-WOR			VMware Toma Romming, remain (122) Hone wire	(Guest Managett)						HEHDER UT
a zeu	D. Priveral Dr.		DNS follow photon-21 IF Advenues 1772 212 213 7						E	0.8
(B) and the Operation?	B Actions - MoveDSCVE		VIEW ALL 2 IF ADDRE							STOKAIE U
G Move2GCVE	Power	QP.	water additional and an and a	m						731.45 2
di amator	Guest 05	2	∆ 16							
Disease fi	Snapshota					With the				
母 nmation()	Queen menter carace				2	Notes				
(b anvasco	值 Mgrate		EPG66			2.3/ below				
(D) (+00+02430+000)	Cons	?	🔲 2 (38, 0 (38 mer	ory active		Costam Attribute	4			
@ INCOVERNE	Fault Tolerance	2	2.08			7 dmbar	20	View		
2 mint have been			VM_1000 (conver-	AND .		and the second second				
进 att-ocverial	VM Policies	2	Distributed		Sec. 1					
B annocisimen	Template	5	4 MEL							
2 am ocut work	compatibility	>		e metros PE pos tratanovires sus	port for the					
(B. Snapilli ())	Export System Logs			munulation interface						The berry to draw
@ trupCartin/Mean			Additional Hardwa	1		ter.				
C techania	∉ bak Sellings		EDO-6.7 and later	AN INCIDENTIAL						
(b. Tetriaren	serve to fulder					3ags.				
(D) Test-Terring	Relate					Antigrent Tag		Cempiny	Description	
th Territe-mint	Edit Notes.									
(\$ Test_the	Tags & Custon Attributes	*	A300-ChitNit							
D Territed	Add Permission .		100-eu001.e	kdcom.						
(2 Testerio)	Alleren		18 59C3059							
R			A300, NPR, 01		-					10.0010.000
Recent Tasks - Alwins					Latera d'arrest					
Name Target				1	100		Completion Time -			
er Christial martine (Brief	vsin		Planning on the new What	Syllars EHCDC COM/Administration		6/2028, 2180 ML.	03/6/2011 132.9 PM	a300-ecsio1anceccom a300-ecsio1anceccom		
	SartApp On/TAP tools ThenApp SnapCenter		Higrate to HCK Target	DACOC COMPANYAMINANA		6/0073 J 30 3J F.	03/6/3031 3 30 33 4	alcol-scall endocum		
empre entrainent: // H	GLAI Ste Recovery actors	-	502	EHCOC COM/Administration		M2001 21010 PM	-100402000-200300-	#300-coath #tubcom		
	HCX Actions	2 10	Protect to HCX Target							

2. In the Migrate Virtual Machine wizard, select the Remote Site Connection (target GCVE).

emote Site Connection: > ☐ Source: HCX-RTP / VC. a300-vcsa0 → ☐ Destination: hcx-58042.17458c8f.e https://to.036.0	1.ehcdc.com urope-west3.g	ve.goog-clou	d / V⊂ vcsa-57901.17458	c8f.europe-west3.g	gve.goog	C Relicati Connecti
 Transfer and Placement: 						
(Mandatory: Compute Container)	20) (Manda	tory: Storage)	-	(Migration Profile)	~
(Specify Destination Folder)	-	👸 Same fe	ormat as source	v	(Optional: Switchover Schedule)	0
> Switchover:						
 Extended Options: 						
Edit Extended Options						
						a

O VALIDATE

CLOSE

3. Update the mandatory fields (Cluster, Storage, and Destination Network), Click Validate.

Source: HCX-RTP / VC a300-vcs → Ø Destination: hcx-58042.17458c8 https://10.036.13	a01.ehcdc.com f.europe-west3.g	ve.goog-cloud / VC vcsa-57901,17458c8	f.europe-west3.	gve.goog	C Extend Conner
✓ Transfer and Placement:					
Workload	-	gcp-ve-4 (807.6387178)	2	vMotion	
(Specify Destination Folder)	-	Same format as source	Ŷ	(Optional: Switchover Schedule)	G
> Switchover:					
✓ Extended Options:					
(Edit Extended Options) (Retain MA					
					Q.
VM for Migration		Disk / Memory / vCPU		Migration Info	
1. V Move2GCVE	C	2 GB / 2 GB / 1 VCPU			
Workload	1	gcp-ve-4 (007.6-68/178)		vMotion	~
(Specify Destination Folder)	9	Same format as source	~		
Force Power-off VM					
. C Enable Seed Checkpoint					
Edit Extended Options Reten MA					
>	Network	adapter1 (VM_3509) → L2E_VM_350	9-3509-a0041a8	3d	2
				► GO Ø VALIDATE	CLO
				O VALIDATE	



The vMotion transfer captures the VM active memory, its execution state, its IP address, and its MAC address. For more information about the requirements and limitations of HCX vMotion, see Understanding VMware HCX vMotion and Cold Migration.

5. You can monitor the progress and completion of the vMotion from the HCX > Migration dashboard.

HCK Official	¢	Migra	tion									
Guernarz			(1) (1) (1) (1)									
		III Tra	cking		T2 MERALE] [[]	-de ANDIVE						a,
infrastructure												
Chite Faring			Migrating VM		State	gal Warnery/ CPUs	Program		Start	C	Tursa	
A electronic l		1			C. CONTRACTOR OF STREET	1977 C 1987 1111 (1979)						_
To transport Analytics		* 0	a300-vesa01ehcde	com 🕂	vcsa/67901/7458c8	Leurope-west3 gve.goog						
Services			Minw AGENE			2.00 2.00 1	O Mpietas Cargae		2Al Paget 254 Paget Paget	No. 227	 Mighton competed. 	
C faithers Echemon		-	Destrution Namiabile Prod	0		Delative III galant 4				20140145-0149-47914	an in the prior banks of	
Disatile Nerrowy			Destruter Date selec			Distant G fare he				1 Minima entre acma		
System			Marallel Californi						Abgratian Profil	a constant		
A Americana and			and the second							e 🖾 Not Schwitzer		
C happert					OW,399 + O U	N_VM_MOWINIDE-MOMINTEE			Delvice Mean Name	 Hot Australia 		
										CEASING		
								Jack Service Press		122.21	÷	
								1 mile April 1 mile April		 Collecting rearranties Residency (Casadian) 		
								P. Phone ages		Commis larger man		
								* 2 min apr		Reardsons serve		
								1 terringen	10	· Alter contervent	totik acquired	
								2 mm apr		 Recently units larged if 		
								a mer apr			Viel for endotion at the per state	
								1 militage		 Nativg records late 		
								t me ape		 Stacking vehicular basis (These level) 	an eres of the	
		0.	WINDOW TO MARKET COLOR		-	49.06 + 0.0 2	O Maraten Conare		TO SEAM BUT TT J	244 EET	Migration completes	
 Becent Tasks All 	arra											
	Teger	1.7	(mea.)			Notation .	T. David T	Batting 2. 7	Completion Treat	farmer		
Unregater virtue machine	(2 How 25CV)		Competer			EHCER CONSAMINATION	2.00	81/4/2021, 2:54 31 PM			108	
Behein ortual machine b.	CE MonitoCVS		Q Companies			Dictic contaction of	5.04	02/05/2023, 2 54 31 PM				
			Concentee	1	national Marinne pr	En-CIIC 20M-Arminetrator	3 ms		00/6/2023 23246V			
Period Are visitual machine	C Mundboys											

Conclusion

Whether you're targeting all-cloud or hybrid cloud and data residing on any type/vendor storage in onpremises, Cloud Volume Service and HCX provide excellent options to deploy and migrate the application workloads while reducing the TCO by making the data requirements seamless to the application layer. Whatever the use case, choose Google Cloud VMware Engine along with Cloud Volume Service for rapid realization of cloud benefits, consistent infrastructure, and operations across on-premises and multiple clouds, bidirectional portability of workloads, and enterprise-grade capacity and performance. It is the same familiar process and procedures used to connect the storage and migrate VMs using VMware vSphere Replication, VMware vMotion, or even network file copy (NFC).

Takeaways

The key points of this document include:

- You can now use Cloud Volume Service as a datastore on Google Cloud VMware Engine SDDC.
- You can easily migrate data from on-premises to Cloud Volume Service datastore.
- You can easily grow and shrink the Cloud Volume Service datastore to meet the capacity and performance requirements during migration activity.

Videos from Google and VMware for reference

From Google

- Deploy HCX Connector with GCVE
- Configure HCX ServiceMesh with GCVE
- Migrate VM with HCX to GCVE

From VMware

- HCX Connector deployment for GCVE
- HCX ServiceMesh configuration for GCVE
- HCX Workload Migration to GCVE

Where to find additional information

To learn more about the information described in this document, refer to the following website links:

• Google Cloud VMware Engine documentation

https://cloud.google.com/vmware-engine/docs/overview

Cloud Volume Service documentation

https://cloud.google.com/architecture/partners/netapp-cloud-volumes

• VMware HCX User Guide

https://docs.vmware.com/en/VMware-HCX/index.html

VM Migration to NetApp Cloud Volume Service NFS Datastore on Google Cloud VMware Engine using Veeam Replication feature

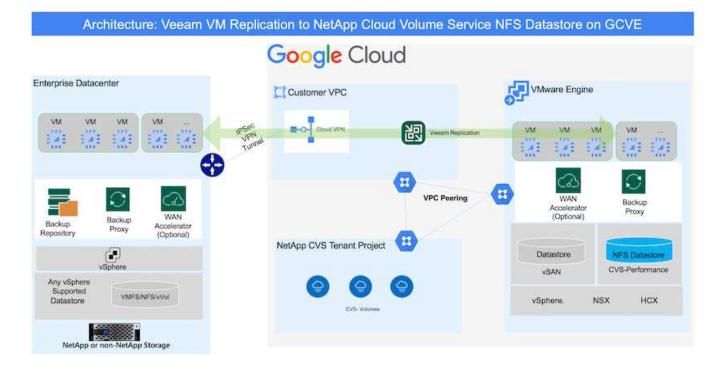
Customers who currently use Veeam for their data protection requirements continue using that solution to migrate the workloads to GCVE and enjoy the benefits of NetApp Cloud Volume Service NFS Datastores.

Overview

Authors: Suresh Thoppay, NetApp

VM Workloads running on VMware vSphere can be migrated to Google Cloud VMware Engine (GCVE) utilizing Veeam Replication feature.

This document provides a step-by-step approach for setting up and performing VM migration that uses NetApp Cloud Volume Service, Veeam, and the Google Cloud VMware Engine (GCVE).



Assumptions

This document assumes you have either Google Cloud VPN or Cloud Interconnect or other networking option in place to establish network connectivity from existing vSphere servers to Google Cloud VMware Engine.



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

Deploying the Migration Solution

Solution Deployment Overview

- 1. Make sure NFS datastore from NetApp Cloud Volume Service is mounted on GCVE vCenter.
- 2. Ensure Veeam Backup Recovery is deployed on existing VMware vSphere environment
- 3. Create Replication Job to start replicating virtual machines to Google Cloud VMware Engine instance.
- 4. Perform Failover of Veeam Replication Job.
- 5. Perform Permanent Failover on Veeam.

Deployment Details

Make sure NFS datastore from NetApp Cloud Volume Service is mounted on GCVE vCenter

Login to GCVE vCenter and ensure NFS datastore with sufficient space is available. If not, Please refer Mount NetApp CVS as NFS datastore on GCVE

Ensure Veeam Backup Recovery is deployed on existing VMware vSphere environment

Please refer Veeam Replication Components documentation to install required components.

Create Replication Job to start replicating virtual machines to Google Cloud VMware Engine instance.

Both on-premises vCenter and GCVE vCenter needs to be registered with Veeam. Setup vSphere VM Replication Job Here is a video explaining how to Configure Replication Job.



Replica VM can have different IP from the source VM and can also be connected to different port group. For more details, check the video above.

Perform Failover of Veeam Replication Job

To Migrate VMs, perform Perform Failover

Perform Permanent Failover on Veeam.

To treat GCVE as your new source environment, perform Permanent Failover

Benefits of this solution

- Existing Veeam backup infrastructure can be utilized for migration.
- Veeam Replication allows changing VM IP addresses on target site.
- Has ability to remap existing data replicated outside of Veeam (like replicated data from BlueXP)
- Has ability to specify different network portgroup on target site.
- Can specify the order of VMs to power on.
- Utilizes VMware Change Block Tracking to minimize the amount of data to send across WAN.
- · Capability to execute pre and post scripts for replication.
- · Capability to execute pre and post scripts for snapshots.

Region Availability – Supplemental NFS datastore for Google Cloud Platform (GCP)

Learn more about the the Global Region support for GCP, GCVE and CVS.



NFS datastore will be available in regions where both services (GCVE and CVS Performance) are available.

Supplemental NFS datastore for GCVE is supported with NetApp Cloud Volume Service.



Only CVS-Performance volumes can be used for GCVE NFS Datastore. For the available location, refer Global Region Map

Google Cloud VMware Engine is available at following locations:

asia-northeast1 > v-zone-a > VE Placement Group 1 asia-northeast1 > v-zone-a > VE Placement Group 2 asia-south1 > v-zone-a > VE Placement Group 2 asia-south1 > v-zone-a > VE Placement Group 1 asia-southeast1 > v-zone-a > VE Placement Group 1 asia-southeast1 > v-zone-a > VE Placement Group 2 australia-southeast1 > v-zone-b > VE Placement Group 1 australia-southeast1 > v-zone-a > VE Placement Group 1 australia-southeast1 > v-zone-b > VE Placement Group 2 australia-southeast1 > v-zone-a > VE Placement Group 2 europe-west2 > v-zone-a > VE Placement Group 2 europe-west2 > v-zone-a > VE Placement Group 1 europe-west3 > v-zone-b > VE Placement Group 2 europe-west3 > v-zone-a > VE Placement Group 3 europe-west3 > v-zone-a > VE Placement Group 4 europe-west3 > v-zone-b > VE Placement Group 1 europe-west3 > v-zone-a > VE Placement Group 2 europe-west3 > v-zone-a > VE Placement Group 1 europe-west4 > v-zone-a > VE Placement Group 2 europe-west4 > v-zone-a > VE Placement Group 1 europe-west6 > v-zone-a > VE Placement Group 1 europe-west8 > v-zone-a > VE Placement Group 1 northamerica-northeast1 > v-zone-a > VE Placement Group 1 northamerica-northeast1 > v-zone-a > VE Placement Group 2 northamerica-northeast2 > v-zone-a > VE Placement Group 2 northamerica-northeast2 > v-zone-a > VE Placement Group 1 southamerica-east1 > v-zone-a > VE Placement Group 1 southamerica-east1 > v-zone-a > VE Placement Group 2 us-central1 > v-zone-a > VE Placement Group 2 us-central1 > v-zone-a > VE Placement Group 5 us-central1 > v-zone-a > VE Placement Group 1 us-central1 > v-zone-a > VE Placement Group 3 us-east4 > v-zone-a > VE Placement Group 5 us-east4 > v-zone-a > VE Placement Group 10 us-east4 > v-zone-a > VE Placement Group 6 us-east4 > v-zone-a > VE Placement Group 3 us-east4 > v-zone-b > VE Placement Group 5 us-east4 > v-zone-a > VE Placement Group 1 us-east4 > v-zone-b > VE Placement Group 1 us-east4 > v-zone-a > VE Placement Group 4 us-east4 > v-zone-b > VE Placement Group 6 us-east4 > v-zone-a > VE Placement Group 2 us-west2 > v-zone-a > VE Placement Group 3 us-west2 > v-zone-a > VE Placement Group 4 us-west2 > v-zone-a > VE Placement Group 5 us-west2 > v-zone-a > VE Placement Group 2 us-west2 > v-zone-a > VE Placement Group 1 us-west2 > v-zone-a > VE Placement Group 6

To minimize latency, NetApp CVS Volume and GCVE where you intent to mount the volume should be in same availability zone.

Work with Google and NetApp Solution Architects for availability and TCO optimizations.

Security overview - NetApp Cloud Volumes Service (CVS) in Google Cloud

TR-4918: Security overview - NetApp Cloud Volumes Service in Google Cloud

Oliver Krause, Justin Parisi, NetApp

Security, particularly in the cloud where infrastructure is outside of the control of storage administrators, is paramount to trusting your data to service offerings provided by cloud providers. This document is an overview of the security offerings that NetApp Cloud Volumes Service provides in Google Cloud.

Intended audience

This document's intended audience includes, but is not limited to, the following roles:

- Cloud providers
- Storage administrators
- Storage architects
- · Field resources
- Business decision makers

If you have questions about the content of this technical report, see the section "Contact us."

Abbreviation	Definition
CVS-SW	Cloud Volumes Service, Service Type CVS
CVS-Performance	Cloud Volume Service, Service Type CVS- Performance
PSA	

How Cloud Volumes Service in Google Cloud secures your data

Cloud Volumes Service in Google Cloud provides a multitude of ways to natively secure your data.

Secure architecture and tenancy model

Cloud Volumes Service provides a secure architecture in Google Cloud by segmenting the service management (control plane) and the data access (data plane) across different endpoints so that neither can impact the other (see the section "Cloud Volumes Service architecture"). It uses Google's private services access (PSA) framework to provide the service. This framework distinguishes between the service producer, which is provided and operated by NetApp, and the service consumer, which is a Virtual Private Cloud (VPC) in a customer project, hosting the clients that want to access Cloud Volumes Service file shares.

In this architecture, tenants (see the section "Tenancy model") are defined as Google Cloud projects that are completely isolated from each other unless explicitly connected by the user. Tenants allow complete isolation of data volumes, external name services, and other essential pieces of the solution from other tenants using the Cloud Volumes Service volume platform. Because the Cloud Volumes Service platform is connected through VPC peering, that isolation applies to it also. You can enable sharing of Cloud Volumes Service volumes between multiple projects by using a shared-VPC (see the section "Shared VPCs"). You can apply access

controls to SMB shares and NFS exports to limit who or what can view or modify datasets.

Strong identity management for the control plane

In the control plane where Cloud Volumes Service configuration takes place, identity management is managed by using Identity Access Management (IAM). IAM is a standard service that enables you to control authentication (logins) and authorization (permissions) to Google Cloud project instances. All configuration is performed with Cloud Volumes Service APIs over a secure HTTPS transport using TLS 1.2 encryption, and authentication is performed by using JWT tokens for added security. The Google console UI for Cloud Volumes Service translates user input into Cloud Volumes Service API calls.

Security hardening - Limiting attack surfaces

Part of effective security is limiting the number of attack surfaces available in a service. Attack surfaces can include a variety of things, including data at-rest, in-flight transfers, logins, and the datasets themselves.

A managed service removes some of the attack surfaces inherently in its design. Infrastructure management, as described in the section "Service operation," is handled by a dedicated team and is automated to reduce the number of times a human actually touches configurations, which helps reduce the number of intentional and unintentional errors. Networking is fenced off so that only necessary services can access one another. Encryption is baked into the data storage and only the data plane needs security attention from Cloud Volumes Service administrators. By hiding most of the management behind an API interface, security is achieved by limiting the attack surfaces.

Zero Trust model

Historically, IT security philosophy has been to trust but verify, and manifested as relying solely on external mechanisms (such as firewalls and intrusion detection systems) to mitigate threats. However, attacks and breaches evolved to bypass the verification in environments through phishing, social engineering, insider threats and other methods that provide the verification to enter networks and wreak havoc.

Zero Trust has become a new methodology in security, with the current mantra being "trust nothing while still verifying everything." Therefore, nothing is allowed access by default. This mantra is enforced in a variety of ways, including standard firewalls and intrusion detection systems (IDS) and also with the following methods:

- Strong authentication methods (such as AES-encrypted Kerberos or JWT tokens)
- Single strong sources of identities (such as Windows Active Directory, Lightweight Directory Access Protocol (LDAP), and Google IAM)
- Network segmentation and secure multitenancy (only tenants are allowed access by default)
- · Granular access controls with Least Privileged Access policies
- · Small exclusive lists of dedicated, trusted administrators with digital audit and paper trails

Cloud Volumes Service running in Google Cloud adheres to the Zero Trust model by implementing the "trust nothing, verify everything" stance.

Encryption

Encrypt data at-rest (see the section "Data encryption at rest") by using XTS-AES-256 ciphers with NetApp Volume Encryption (NVE) and in-flight with "SMB encryption" or NFS Kerberos 5p support. Rest easy knowing cross-region replication transfers are protected by TLS 1.2 encryption (see the section "Cross-region replication"). In addition, Google networking also provides encrypted communications (see the section "Data encryption in transit") for an added layer of protection against attacks. For more information about transport encryption, see the section "Google Cloud network".

Data protection and backups

Security isn't just about the prevention of attacks. It is also about how we recover from attacks if or when they occur. This strategy includes data protection and backups. Cloud Volumes Service provides methods to replicate to other regions in case of outages (see the section "Cross-region replication") or if a dataset is affected by a ransomware attack. It can also perform asynchronous backups of data to locations outside of the Cloud Volumes Service instance by using Cloud Volumes Service backup. With regular backups, mitigation of security events can take less time and save money and angst for administrators.

Fast ransomware mitigation with industry leading Snapshot copies

In addition to data protection and backups, Cloud Volumes Service provides support for immutable Snapshot copies (see the section "Immutable Snapshot copies") of volumes that allow recovery from ransomware attacks (see the section "Service operation") within seconds of discovering the issue and with minimal disruption. Recovery time and effects depend on the Snapshot schedule, but you can create Snapshot copies that provide as little as one-hour deltas in ransomware attacks. Snapshot copies have a negligible effect on performance and capacity usage and are a low-risk, high-reward approach to protecting your datasets.

Security considerations and attack surfaces

The first step in understanding how to secure your data is identifying the risks and potential attack surfaces.

These include (but are not limited to) the following:

- Administration and logins
- Data at rest
- Data in flight
- Network and firewalls
- · Ransomware, malware, and viruses

Understanding attack surfaces can help you to better secure your environments. Cloud Volumes Service in Google Cloud already considers many of these topics and implements security functionality by default, without any administrative interaction.

Ensuring secure logins

When securing your critical infrastructure components, it is imperative to make sure that only approved users can log in and manage your environments. If bad actors breach your administrative credentials, then they have the keys to the castle and can do anything they want—change configurations, delete volumes and backups, create backdoors, or disable Snapshot schedules.

Cloud Volumes Service for Google Cloud provides protection against unauthorized administrative logins through the obfuscation of storage as a service (StaaS). Cloud Volumes Service is completely maintained by the cloud provider with no availability to login externally. All setup and configuration operations are fully automated, so a human administrator never has to interact with the systems except in very rare circumstances.

If login is required, Cloud Volumes Service in Google Cloud secures logins by maintaining a very short list of trusted administrators that have access to log in to the systems. This gatekeeping helps reduce the number of potential bad actors with access. Additionally, the Google Cloud networking hides the systems behind layers of network security and exposes only what is needed to the outside world. For information about the Google Cloud, Cloud Volumes Service architecture, see the section "Cloud Volumes Service architecture."

Cluster administration and upgrades

Two areas with potential security risks include cluster administration (what happens if a bad actor has admin access) and upgrades (what happens if a software image is compromised).

Storage administration protection

Storage provided as a service removes the added risk of exposure to administrators by removing that access to end users outside of the cloud data center. Instead, the only configuration done is for the data access plane by customers. Each tenant manages their own volumes, and no tenant can reach other Cloud Volumes Service instances. The service is managed by automation, with a very small list of trusted administrators given access to the systems through the processes covered in the section "Service operation."

The CVS-Performance service type offers cross-region replication as an option to provide data protection to a different region in the event of a region failure. In those cases, Cloud Volumes Service can be failed over to the unaffected region to maintain data access.

Service upgrades

Updates help protect vulnerable systems. Each update provides security enhancements and bug fixes that minimize attack surfaces. Software updates are downloaded from centralized repositories and are validated before the updates are allowed to verify that official images are used and that the upgrades are not compromised by bad actors.

With Cloud Volumes Service, updates are handled by the cloud provider teams, which removes risk exposure for administrator teams by providing experts well versed in configuration and upgrades that have automated and fully tested the process. Upgrades are nondisruptive, and Cloud Volumes Service maintains the latest updates for best overall results.

For information about the administrator team that performs these service upgrades, see the section "Service operation."

Securing data at-rest

Data-at-rest encryption is important to protect sensitive data in the event of a disk that is stolen, returned, or repurposed. Data in Cloud Volumes Service is protected at rest by using software-based encryption.

- · Google-generated keys are used for CVS-SW.
- For CVS-Performance, the per-volume keys are stored in a key manager built into Cloud Volumes Service, which uses NetApp ONTAP CryptoMod to generate AES-256 encryption keys. CryptoMod is listed on the CMVP FIPS 140-2 validated modules list. See FIPS 140-2 Cert #4144.

Starting in November 2021, preview Customer-managed Encryption (CMEK) functionality was made available for CVS-Performance. This functionality allows you to encrypt the per-volume keys with per-project, per-region master-keys that are hosted in Google Key Management Service (KMS). KMS enables you to attach external key managers.

For details about how to configure KMS for CVS-Performance, see the Cloud Volumes Service documentation.

For more information about architecture, see the section "Cloud Volumes Service architecture."

Securing data in-flight

In addition to securing data at rest, you must also be able to secure data when it is in flight between the Cloud Volumes Service instance and a client or replication target. Cloud Volumes Service provides encryption for in-

flight data over NAS protocols by using encryption methods such as SMB encryption using Kerberos, the signing/sealing of packets, and NFS Kerberos 5p for end-to-end encryption of data transfers.

Replication of Cloud Volumes Service volumes uses TLS 1.2, which takes advantage of AES-GCM encryption methods.

Most insecure in-flight protocols such as telnet, NDMP, and so on are disabled by default. DNS, however, is not encrypted by Cloud Volumes Service (no DNS Sec support) and should be encrypted by using external network encryption when possible. See the section "Data encryption in transit" for more information about securing data in-flight.

For information about NAS protocol encryption, see the section "NAS protocols."

Users and groups for NAS permissions

Part of securing your data in the cloud involves proper user and group authentication, where the users accessing the data are verified as real users in the environment and the groups contain valid users. These users and groups provide initial share and export access, as well as permission validation for files and folders in the storage system.

Cloud Volumes Service uses standard Active Directory-based Windows user and group authentication for SMB shares and Windows-style permissions. The service can also leverage UNIX identity providers such as LDAP for UNIX users and groups for NFS exports, NFSv4 ID validation, Kerberos authentication, and NFSv4 ACLs.



Currently only Active Directory LDAP is supported with Cloud Volumes Service for LDAP functionality.

Detection, prevention and mitigation of ransomware, malware, and viruses

Ransomware, malware, and viruses are a persistent threat to administrators, and detection, prevention, and mitigation of those threats are always top of mind for enterprise organizations. A single ransomware event on a critical dataset can potentially cost millions of dollars, so it is beneficial to do what you can to minimize the risk.

Although Cloud Volumes Service currently doesn't include native detection or prevention measures, such as antivirus protection or automatic ransomware detection, there are ways to quickly recover from a ransomware event by enabling regular Snapshot schedules. Snapshot copies are immutable and read only pointers to changed blocks in the file system, are near instantaneous, have minimal impact on performance, and only use up space when data is changed or deleted. You can set schedules for Snapshot copies to match your desired acceptable recovery point objective (RPO)/recovery time objective (RTO) and can keep up to 1,024 Snapshot copies per volume.

Snapshot support is included at no additional cost (beyond data storage charges for changed blocks/data retained by Snapshot copies) with Cloud Volumes Service and, in the event of a ransomware attack, can be used to roll back to a Snapshot copy before the attack occurred. Snapshot restores take just seconds to complete, and you then can get back to serving data as normal. For more information, see The NetApp Solution for Ransomware.

Preventing ransomware from affecting your business requires a multilayered approach that includes one or more of the following:

- Endpoint protection
- · Protection against external threats through network firewalls
- · Detection of data anomalies

- Multiple backups (onsite and offsite) of critical datasets
- · Regular restore tests of backups
- Immutable read-only NetApp Snapshot copies
- Multifactor authentication for critical infrastructure
- · Security audits of system logins

This list is far from exhaustive but is a good blueprint to follow when dealing with the potential of ransomware attacks. Cloud Volumes Service in Google Cloud provides several ways to protect against ransomware events and reduce their effects.

Immutable Snapshot copies

Cloud Volumes Service natively provides immutable read-only Snapshot copies that are taken on a customizable schedule for quick point-in-time recovery in the event of data deletion or if an entire volume has been victimized by a ransomware attack. Snapshot restores to previous good Snapshot copies are fast and minimize data loss based on the retention period of your Snapshot schedules and RTO/RPO. The performance effect with Snapshot technology is negligible.

Because Snapshot copies in Cloud Volumes Service are read-only, they cannot be infected by ransomware unless the ransomware has proliferated into the dataset unnoticed and Snapshot copies have been taken of the data infected by ransomware. This is why you must also consider ransomware detection based on data anomalies. Cloud Volumes Service does not currently provide detection natively, but you can use external monitoring software.

Backups and restores

Cloud Volumes Service provides standard NAS client backup capabilities (such as backups over NFS or SMB).

- CVS-Performance offers cross-region volume replication to other CVS-Performance volumes. For more information, see volume replication in the Cloud Volumes Service documentation.
- CVS-SW offers service-native volume backup/restore capabilities. For more information, see cloud backup in the Cloud Volumes Service documentation.

Volume replication provides an exact copy of the source volume for fast failover in the case of a disaster, including ransomware events.

Cross-region replication

CVS-Performance enables you to securely replicate volumes across Google Cloud regions for data protection and archive use cases by using TLS1.2 AES 256 GCM encryption on a NetApp-controlled backend service network using specific interfaces used for replication running on Google's network. A primary (source) volume contains the active production data and replicates to a secondary (destination) volume to provide an exact replica of the primary dataset.

Initial replication transfers all blocks, but updates only transmit the changed blocks in a primary volume. For instance, if a 1TB database that resides on a primary volume is replicated to the secondary volume, then 1TB of space is transferred on the initial replication. If that database has a few hundred rows (hypothetically, a few MB) that change between the initialization and the next update, only the blocks with the changed rows are replicated to the secondary (a few MB). This helps to make sure that the transfer times remain low and keeps replication charges down.

All permissions on files and folders are replicated to the secondary volume, but share access permissions

(such as export policies and rules or SMB shares and share ACLs) must be handled separately. In the case of a site failover, the destination site should leverage the same name services and Active Directory domain connections to provide consistent handling of user and group identities and permissions. You can use a secondary volume as a failover target in the event of a disaster by breaking the replication relationship, which converts the secondary volume to read-write.

Volume replicas are read-only, which provides an immutable copy of data offsite for quick recovery of data in instances where a virus has infected data or ransomware has encrypted the primary dataset. Read-only data won't be encrypted, but, if the primary volume is affected and replication occurs, the infected blocks also replicate. You can use older, non-affected Snapshot copies to recover, but SLAs might fall out of range of the promised RTO/RPO depending on how quickly an attack is detected.

In addition, you can prevent malicious administrative actions, such as volume deletions, Snapshot deletions, or Snapshot schedule changes, with cross-region replication (CRR) management in Google Cloud. This is done by creating custom roles that separate volume administrators, who can delete source volumes but not break mirrors and therefore cannot delete destination volumes, from CRR administrators, who cannot perform any volume operations. See Security Considerations in the Cloud Volumes Service documentation for permissions allowed by each administrator group.

Cloud Volumes Service backup

Although Cloud Volumes Service provides high data durability, external events can cause data loss. In the event of a security event such as a virus or ransomware, backups and restores become critical for resumption of data access in a timely manner. An administrator might accidentally delete a Cloud Volumes Service volume. Or users simply want to retain backup versions of their data for many months and keeping the extra Snapshot copy space inside the volume becomes a cost challenge. Although Snapshot copies should be the preferred way to keep backup versions for the last few weeks to restore lost data from them, they are sitting inside the volume and are lost if the volume goes away.

For all these reasons, NetApp Cloud Volumes Service offers backup services through Cloud Volumes Service backup.

Cloud Volumes Service backup generates a copy of the volume on Google Cloud Storage (GCS). It only backs up the actual data stored within the volume, not the free space. It works as incremental forever, meaning it transfers the volume content once and from there on continues backing up changed data only. Compared to classical backup concepts with multiple full backups, it saves large amounts of backup storage, reducing cost. Because the monthly price of backup space is lower compared to a volume, it is an ideal place to keep backup versions longer.

Users can use a Cloud Volumes Service backup to restore any backup version to the same or a different volume within the same region. If the source volume is deleted, the backup data is retained and needs to be managed (for example, deleted) independently.

Cloud Volumes Service backup is built into Cloud Volumes Service as option. Users can decide which volumes to protect by activating Cloud Volumes Service backup on a per-volume basis. See the Cloud Volumes Service backup documentation for information about backups, the number of maximum backup versions supported, scheduling, and pricing.

All backup data of a project is stored within a GCS bucket, which is managed by the service and not visible to the user. Each project uses a different bucket. Currently, the buckets are in same region as the Cloud Volumes Service volumes, but more options are being discussed. Consult the documentation for the latest status.

Data transport from a Cloud Volumes Service bucket to GCS uses service-internal Google networks with HTTPS and TLS1.2. Data is encrypted at-rest with Google-managed keys.

To manage Cloud Volumes Service backup (creating, deleting, and restoring backups), a user must have the roles/netappcloudvolumes.admin role.

Architecture

Overview

Part of trusting a cloud solution is understanding the architecture and how it is secured. This section calls out different aspects of the Cloud Volumes Service architecture in Google to help alleviate potential concerns about how data is secured, as well as call out areas where additional configuration steps might be required to obtain the most secure deployment.

The general architecture of Cloud Volumes Service can be broken down into two main components: the control plane and the data plane.

Control plane

The control plane in Cloud Volumes Service is the backend infrastructure managed by Cloud Volumes Service administrators and NetApp native automation software. This plane is completely transparent to end users and includes networking, storage hardware, software updates, and so on to help deliver value to a cloud-resident solution such as Cloud Volumes Service.

Data plane

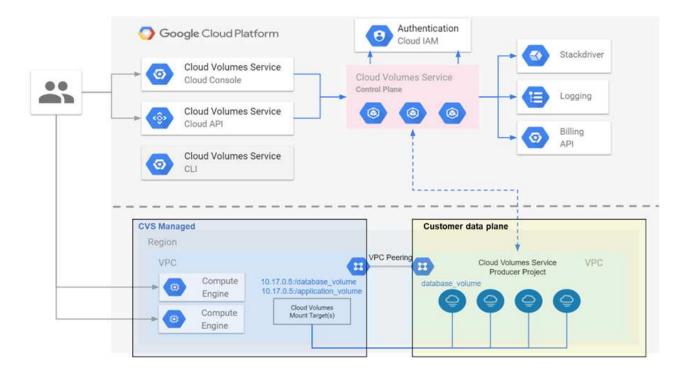
The data plane in Cloud Volumes Service includes the actual data volumes and the overall Cloud Volumes Service configuration (such as access control, Kerberos authentication, and so on). The data plane is entirely under the control of the end users and the consumers of the Cloud Volumes Service platform.

There are distinct differences in how each plane is secured and managed. The following sections cover these differences, starting with a Cloud Volumes Service architecture overview.

Cloud Volumes Service architecture

In a manner similar to other Google Cloud native services such as CloudSQL, Google Cloud VMware Engine (GCVE), and FileStore, Cloud Volumes Service uses Google PSA to deliver the service. In PSA, services are built inside a service producer project, which uses VPC network peering to connect to the service consumer. The service producer is provided and operated by NetApp, and the service consumer is a VPC in a customer project, hosting the clients that want to access Cloud Volumes Service file shares.

The following figure, referenced from the architecture section of the Cloud Volumes Service documentation, shows a high-level view.



The part above the dotted line shows the control plane of the service, which controls the volume lifecycle. The part below the dotted line shows the data plane. The left blue box depicts the user VPC (service consumer), the right blue box is the service producer provided by NetApp. Both are connected through VPC peering.

Tenancy model

In Cloud Volumes Service, individual projects are considered unique tenants. This means that manipulation of volumes, Snapshot copies, and so on are performed on a per- project basis. In other words, all volumes are owned by the project that they were created in and only that project can manage and access the data inside of them by default. This is considered the control plane view of the service.

Shared VPCs

On the data plane view, Cloud Volumes Service can connect to a shared VPC. You can create volumes in the hosting project or in one of the service projects connected to the shared VPC. All projects (host or service) connected to that shared VPC are able to reach the volumes at the network layer (TCP/IP). Because all clients with network connectivity on the shared- VPC can potentially access the data through NAS protocols, access control on the individual volume (such as user/group access control lists (ACLs) and hostnames/IP addresses for NFS exports) must be used to control who can access the data.

You can connect Cloud Volumes Service to up to five VPCs per customer project. On the control plane, the project enables you to manage all created volumes, no matter which VPC they are connected to. On the data plane, VPCs are isolated from one another, and each volume can only be connected to one VPC.

Access to the individual volumes is controlled by protocol specific (NFS/SMB) access control mechanisms.

In other words, on the network layer, all project s connected to the shared VPC are able to see the volume, while, on the management side, the control plane only allows the owner project to see the volume.

VPC Service Controls

VPC Service Controls establish an access control perimeter around Google Cloud services that are attached to

the internet and are accessible worldwide. These services provide access control through user identities but cannot restrict which network location requests originate from. VPC Service Controls close that gap by introducing the capabilities to restrict access to defined networks.

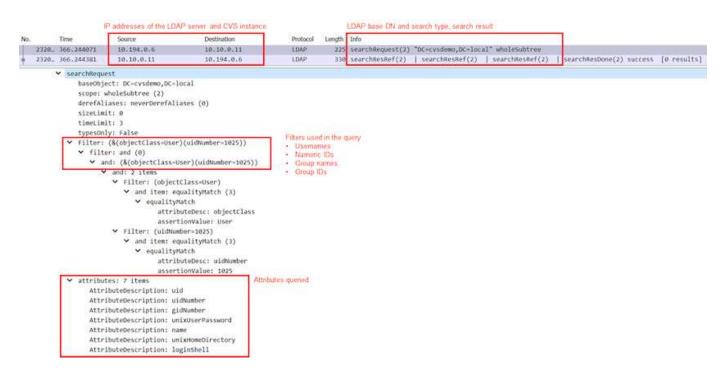
The Cloud Volumes Service data plane is not connected to the external internet but to private VPCs with welldefined network boundaries (perimeters). Within that network, each volume uses protocol-specific access control. Any external network connectivity is explicitly created by Google Cloud project administrators. The control plane, however, does not provide the same protections as the data plane and can be accessed by anyone from anywhere with valid credentials (JWT tokens).

In short, the Cloud Volumes Service data plane provides the capability of network access control, without the requirement to support VPC Service Controls and does not explicitly use VPC Service Controls.

Packet sniffing/trace considerations

Packet captures can be useful for troubleshooting network issues or other problems (such as NAS permissions, LDAP connectivity, and so on), but can also be used maliciously to gain information about network IP addresses, MAC addresses, user and group names, and what level of security is being used on endpoints. Because of the way Google Cloud networking, VPCs, and firewall rules are configured, unwanted access to network packets should be difficult to obtain without user login credentials or JWT tokens into the cloud instances. Packet captures are only possible on endpoints (such as virtual machines (VMs)) and only possible on endpoints internal to the VPC unless a shared VPC and/or external network tunnel/IP forwarding is in use to explicitly allow external traffic to endpoints. There is no way to sniff traffic outside of the clients.

When shared VPCs are used, in-flight encryption with NFS Kerberos and/or SMB encryption can mask much of the information gleaned from traces. However, some traffic is still sent in plaintext, such as DNS and LDAP queries. The following figure shows a packet capture from a plaintext LDAP query originating from Cloud Volumes Service and the potential identifying information that is exposed. LDAP queries in Cloud Volumes Service currently do not support encryption or LDAP over SSL. CVS-Performance support LDAP signing, if requested by Active Directory. CVS-SW does not support LDAP signing.





unixUserPassword is queried by LDAP and is not sent in plaintext but instead in a salted hash. By default, Windows LDAP does not populate the unixUserPassword fields. This field is only required if you need to leverage Windows LDAP for interactive logins through LDAP to clients. Cloud Volumes Service does not support interactive LDAP logins to the instances.

The following figure shows a packet capture from an NFS Kerberos conversation next to a capture of NFS over AUTH_SYS. Note how the information available in a trace differs between the two and how enabling in-flight encryption offers greater overall security for NAS traffic.

ernet II, Sr ernet Protoc nsmission Co	18014 10. 18480 10. 18641 10. 59035 10. bytes on wire 10. c: IntelCor_7f 10. ol Version 4, 4. ntrol Protocol 10.	ce 193.67.225 193.67.219 193.67.225 193.67.219 (3408 bits), 42 5:da:bc (90:e2:b Src: 10.193.67. ., Src Port: 204 Leply XID:0xef5e	pa:7f:da:bc), 219, Dst: 10. 19, Dst Port:	219 225 219 225 ured (3408 b Dst: VMware 193.67.225	_a0:2c:	346 426 370 458 2d (00		y (Call (Reply y (Call y (Call 00:2c:20	l In / In L In	380) 397)
381 9.2 382 9.2 397 9.3 me 381: 426 ernet II, Sr ernet Protoc nsmission Co ote Procedur	18480 10. 18641 10. 186935 10. bytes on wire 10. c: IntelCor_7f 10. ol Version 4, 10. ntrol Protocol 10.	193.67.219 193.67.225 193.67.219 (3408 bits), 42 ::da:bc (90:e2:b Src: 10.193.67. ., Src Port: 204	10.193.67. 10.193.67. 10.193.67. 26 bytes captu pa:7f:da:bc), 219, Dst: 10. 49, Dst Port:	225 219 225 Jred (3408 b Dst: VMware 193.67.225	NFS NFS NFS Dits) a_a0:2c:	426 370 458 2d (00	V4 Repl V4 Call V4 Repl :50:56:a	y (Call (Reply y (Call y (Call 00:2c:20	l In / In L In	380) 397)
382 9.2 397 9.3 me 381: 426 ernet II, Sr ernet Protoc nsmission Co ote Procedur	1864110.5903510.bytes on wirec: IntelCor_7fcl Version 4,ntrol Protocol	193.67.225 193.67.219 (3408 bits), 42 :da:bc (90:e2:b Src: 10.193.67. ., Src Port: 204	10.193.67. 10.193.67. 26 bytes captu ba:7f:da:bc), 219, Dst: 10. 19, Dst Port:	219 225 Jred (3408 b Dst: VMware 193.67.225	NFS NFS pits) 2_a0:2c:	426 370 458 2d (00	V4 Repl V4 Call V4 Repl :50:56:a	y (Call (Reply y (Call y (Call 00:2c:20	l In / In L In	380) 397)
382 9.2 397 9.3 me 381: 426 ernet II, Sr ernet Protoc nsmission Co ote Procedur	1864110.5903510.bytes on wirec: IntelCor_7fcl Version 4,ntrol Protocol	193.67.225 193.67.219 (3408 bits), 42 :da:bc (90:e2:b Src: 10.193.67. ., Src Port: 204	10.193.67. 10.193.67. 26 bytes captu ba:7f:da:bc), 219, Dst: 10. 19, Dst Port:	219 225 Jred (3408 b Dst: VMware 193.67.225	NFS NFS pits) 2_a0:2c:	370 458 2d (00	V4 Call V4 Repl :50:56:a	(Reply y (Call 0:2c:20	/ In L In	397)
397 9.30 me 381: 426 ernet II, Sr ernet Protoc nsmission Co ote Procedur	59035 10. bytes on wire c: IntelCor_7f ol Version 4, ntrol Protocol	193.67.219 (3408 bits), 42 :da:bc (90:e2:b Src: 10.193.67. ., Src Port: 204	10.193.67. 26 bytes captu ba:7f:da:bc), 219, Dst: 10. 19, Dst Port:	225 ured (3408 b Dst: VMware 193.67.225	NFS pits) e_a0:2c:	458 2d (00	V4 Repl	y (Call	l In	
me 381: 426 ernet II, Sr ernet Protoc nsmission Co ote Procedur	bytes on wire c: IntelCor_7f ol Version 4, ntrol Protocol	(3408 bits), 42 :da:bc (90:e2:b Src: 10.193.67. ., Src Port: 204	26 bytes captu ba:7f:da:bc), 219, Dst: 10. 49, Dst Port:	ured (3408 b Dst: VMware 193.67.225	oits) e_a0:2c:	2d (00	:50:56:a	0:2c:20		382)
ernet II, Sr ernet Protoc nsmission Co ote Procedur	c: IntelCor_7f ol Version 4, ntrol Protocol	da:bc (90:e2:b Src: 10.193.67. , Src Port: 204	pa:7f:da:bc), 219, Dst: 10. 19, Dst Port:	Dst: VMware 193.67.225	_a0:2c:				4)	
ernet Protoc nsmission Co ote Procedur	ol Version 4, ntrol Protocol	Src: 10.193.67. ., Src Port: 204	219, Dst: 10. 19, Dst Port:	193.67.225	-				4)	
nsmission Co ote Procedur	ntrol Protocol	, Src Port: 204	19, Dst Port:		305, Ac	k: 656	9, Len:	360		
ote Procedur		•	•	738, Seq: 6	305, Ac	k: 656	9, Len:	360		
	e Call, Type:R	eply XID:0xef5e	998d		-		-			
-Wrap										
				GSS wra	apped NFS c	alls/replies v	<i>i</i> ith no other id	entifying info	rmation	
ength: 300										
0	107ff00000000	000000000000013/5	1001d/3d208cf	3031						
-		000000000259134	5166104302980	12021.						
-										
-	-									
V4 Procedure	e: COMPOUND (1)]								
	IP addresses of the NFS	client and CVS instance		Detailed NES call type	a and file har	dle informati	on			
Time	Course	Destination		and the second						
33 0.958480	10.193.67.201	10.193.67.204	11111 AV	and the second	In 32) OP	EN Statel	D: 0x0481			
34 0.958784	10.193.67.204	10.193.67.201	12 COL					a		
35 8,959284	10 102 57 301	10.193.67.204	NFS 358	V4 Reply (Call	In 34) SE	TATTR				
	SS Data: 056 (rb5_blob: 05 work File Sy: Program Vers V4 Procedure 33 0.958480 34 0.958784	355 Data: 050407ff0000000 crb5_blob: 050407ff0000000 work File System [Program Version: 4] [V4 Procedure: COMPOUND (1 IP addresses of the NFS Time Source 33 0.958480 10.193.67.201 34 0.958784 10.193.67.204	335 Data: 050407ff00000000000000000000000000000000	35S Data: 050407ff00000000000000000000000000000000	Social	35S Data: 050407ff00000000000000000000000000000000	355 Data: 050407ff00000000000000000000000000000000	35S Data: 050407ff00000000000000000000000000000000	35S Data: 050407ff00000000000000000000000000000000	35S Data: 050407ff00000000000000000000000000000000

- Opcode: GETATTR (9)
 Status: NFS4_OK (0)
- Attr mask[0]: 0x0010011a (Type, Change, Size, FSID, FileId)

File ID

- > regd attr: Type (1)
- > reqd_attr: Change (3)
- > reqd_attr: Size (4)
- > reqd_attr: FSID (8)
- v reco_attr: FileId (20)
- Feco_attr: File1d (20) fileid: 9232254136597092620
- Attr mask[1]: 0x00b0a03a (Mode, NumLinks, Owner, Owner_Group, Space_Used, Time_Access, Time_Metadata, Time_Modify, Mounted_on_FileId)
- reco_attr: Mode (33)
 Permission information
 mode: 0644, Name: Unknown, Read permission for owner, Write permission for owner, Read permission for group, Read permission for others
 reco_attr: NumLinks (35)
 reco_attr: Owner (36)
 Owner and group ID strings
- > fattr4_owner: root@NTAP.LOCAL
 v reco_attr: Owner_Group (37)
- reco_attr: Owner_Group (37)
 fattr4_owner_group: root@NTAP.LOCAL
- reco_attr: Space_Used (45)
- > reco_attr: Time_Access (47)
- > reco_attr: Time_Metadata (52)
- > reco_attr: Time_Modify (53)
 > reco_attr: Mounted_on_FileId (55)
- > reco_attr: Mounted_on_FileId (55)

VM network interfaces

One trick attackers might attempt is to add a new network interface card (NIC) to a VM in promiscuous mode (port mirroring) or enable promiscuous mode on an existing NIC in order to sniff all traffic. In Google Cloud, adding a new NIC requires a VM to be shut down entirely, which creates alerts, so attackers cannot do this

unnoticed.

In addition, NICs cannot be set to promiscuous mode at all and will trigger alerts in Google Cloud.

Control plane architecture

All management actions to Cloud Volumes Service are done through API. Cloud Volumes Service management integrated into the GCP Cloud Console also uses the Cloud Volumes Service API.

Identity and Access Management

Identity and Access Management (IAM) is a standard service that enables you to control authentication (logins) and authorization (permissions) to Google Cloud project instances. Google IAM provides a full audit trail of permissions authorization and removal. Currently Cloud Volumes Service does not provide control plane auditing.

Authorization/permission overview

IAM offers built-in, granular permissions for Cloud Volumes Service. You can find a complete list of granular permissions here.

IAM also offers two predefined roles called netappcloudvolumes.admin and netappcloudvolumes.viewer. These roles can be assigned to specific users or service accounts.

Assign appropriate roles and permission to allow IAM users to manage Cloud Volumes Service.

Examples for using granular permissions include the following:

- Build a custom role with only get/list/create/update permissions so that users cannot delete volumes.
- Use a custom role with only snapshot.* permissions to create a service account that is used to build application- consistent Snapshot integration.
- Build a custom role to delegate volumereplication.* to specific users.

Service accounts

To make Cloud Volumes Service API calls through scripts or Terraform, you must create a service account with the roles/netappcloudvolumes.admin role. You can use this service account to generate the JWT tokens required to authenticate Cloud Volumes Service API requests in two different ways:

- Generate a JSON key and use Google APIs to derive a JWT token from it. This is the simplest approach, but it involves manual secrets (the JSON key) management.
- Use Service account impersonation with roles/iam.serviceAccountTokenCreator. The code (script, Terraform, and so on.) runs with Application Default Credentials and impersonates the service account to gain its permissions. This approach reflects Google security best practices.

See Creating your service account and private key in the Google cloud documentation for more information.

Cloud Volumes Service API

Cloud Volumes Service API uses a REST-based API by using HTTPS (TLSv1.2) as the underlying network transport. You can find the latest API definition here and information about how to use the API at Cloud

Volumes APIs in the Google cloud documentation.

The API endpoint is operated and secured by NetApp using standard HTTPS (TLSv1.2) functionality.

JWT tokens

Authentication to the API is performed with JWT bearer tokens (RFC-7519). Valid JWT tokens must be obtained by using Google Cloud IAM authentication. This must be done by fetching a token from IAM by providing a service account JSON key.

Audit logging

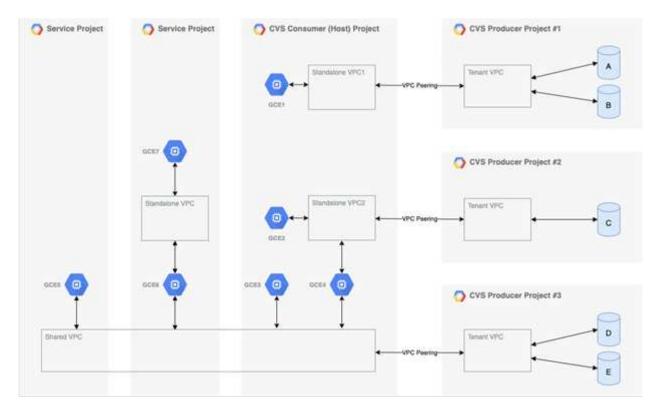
Currently, no user-accessible control plane audit logs are available.

Data plane architecture

Cloud Volumes Service for Google Cloud leverages the Google Cloud private services access framework. In this framework, users can connect to the Cloud Volumes Service. This framework uses Service Networking and VPC peering constructs like other Google Cloud services, ensuring complete isolation between tenants.

For an architecture overview of Cloud Volumes Service for Google Cloud, see Architecture for Cloud Volumes Service.

User VPCs (standalone or shared) are peered to VPCs within Cloud Volumes Service managed tenant projects, which hosts the volumes.



The preceding figure shows a project (the CVS consumer project in the middle) with three VPC networks connected to Cloud Volumes Service and multiple Compute Engine VMs (GCE1-7) sharing volumes:

• VPC1 allows GCE1 to access volumes A and B.

- VPC2 allows GCE2 and GCE4 to access volume C.
- The third VPC network is a shared VPC, shared with two service projects. It allows GCE3, GCE4, GCE5, and GCE6 to access volumes D and E. Shared VPC networks are only supported for volumes of the CVS-Performance service type.



GCE7 cannot access any volume.

Data can be encrypted both in-transit (using Kerberos and/or SMB encryption) and at-rest in Cloud Volumes Service.

Data encryption in transit

Data in transit can be encrypted at the NAS protocol layer, and the Google Cloud network itself is encrypted, as described in the following sections.

Google Cloud network

Google Cloud encrypts traffic on the network level as described in Encryption in transit in the Google documentation. As mentioned in the section "Cloud Volumes Services architecture," Cloud Volumes Service is delivered out of a NetApp-controlled PSA producer project.

In case of CVS-SW, the producer tenant runs Google VMs to provide the service. Traffic between user VMs and Cloud Volumes Service VMs is encrypted automatically by Google.

Although the data path for CVS-Performance isn't fully encrypted on the network layer, NetApp and Google use a combination of IEEE 802.1AE encryption (MACSec), encapsulation (data encryption), and physically restricted networks to protect data in transit between the Cloud Volumes Service CVS-Performance service type and Google Cloud.

NAS protocols

NFS and SMB NAS protocols provide optional transport encryption at the protocol layer.

SMB encryption

SMB encryption provides end-to-end encryption of SMB data and protects data from eavesdropping occurrences on untrusted networks. You can enable encryption for both the client/server data connection (only available to SMB3.x capable clients) and the server/domain controller authentication.

When SMB encryption is enabled, clients that do not support encryption cannot access the share.

Cloud Volumes Service supports RC4-HMAC, AES-128-CTS-HMAC-SHA1, and AES-256-CTS-HMAC-SHA1 security ciphers for SMB encryption. SMB negotiates to the highest supported encryption type by the server.

NFSv4.1 Kerberos

For NFSv4.1, CVS-Performance offers Kerberos authentication as described in RFC7530. You can enable Kerberos on a per-volume basis.

The current strongest available encryption type for Kerberos is AES-256-CTS-HMAC-SHA1. NetApp Cloud Volumes Service supports AES-256-CTS-HMAC-SHA1, AES-128-CTS-HMAC-SHA1, DES3, and DES for NFS. It also supports ARCFOUR-HMAC (RC4) for CIFS/SMB traffic, but not for NFS.

Kerberos provides three different security levels for NFS mounts that offer choices for how strong the Kerberos security should be.

As per RedHat's Common Mount Options documentation:

```
sec=krb5 uses Kerberos V5 instead of local UNIX UIDs and GIDs to
authenticate users.
sec=krb5i uses Kerberos V5 for user authentication and performs integrity
checking of NFS operations using secure checksums to prevent data
tampering.
sec=krb5p uses Kerberos V5 for user authentication, integrity checking,
and encrypts NFS traffic to prevent traffic sniffing. This is the most
secure setting, but it also involves the most performance overhead.
```

As a general rule, the more the Kerberos security level has to do, the worse the performance is, as the client and server spend time encrypting and decrypting NFS operations for each packet sent. Many clients and NFS servers provide support for AES-NI offloading to the CPUs for a better overall experience, but the performance impact of Kerberos 5p (full end-to-end encryption) is significantly greater than the impact of Kerberos 5 (user authentication).

Security level	Security	Performance
NFSv3—sys	 Least secure; plain text with numeric user IDs/group IDs 	Best for most cases
	 Able to view UID, GID, client IP addresses, export paths, file names, permissions in packet captures 	
NFSv4.x—sys	 More secure than NFSv3 (client IDs, name string/domain string matching) but still plain text 	 Good for sequential workloads (such as VMs, databases, large files)
	 Able to view UID, GID, client IP addresses, name strings, domain IDs, export paths, file names, permissions in packet captures 	 Bad with high file count/high metadata (30-50% worse)

The following table shows differences in what each level does for security and performance.

Security level	Security	Performance
NFS—krb5	 Kerberos encryption for credentials in every NFS packet—wraps UID/GID of users/groups in RPC calls in GSS wrapper User requesting access to mount needs a valid Kerberos ticket (either through username/password or manual key tab exchange); ticket expires after a specified time period and user must reauthenticate for access No encryption for NFS operations or ancillary protocols like mount/portmapper/nlm (can see export paths, IP addresses, file handles, permissions, file names, atime/mtime in packet captures) 	 Best in most cases for Kerberos; worse than AUTH_SYS
NFS—krb5i	 Kerberos encryption for credentials in every NFS packet—wraps UID/GID of users/groups in RPC calls in GSS wrapper User requesting access to mount needs a valid Kerberos ticket (either via username/password or manual key tab exchange); ticket expires after a specified time period and user must reauthenticate for access No encryption for NFS operations or ancillary protocols like mount/portmapper/nlm (can see export paths, IP addresses, file handles, permissions, file names, atime/mtime in packet captures) Kerberos GSS checksum is added to every packet to ensure nothing intercepts the packets. If checksums match, conversation is allowed. 	 Better than krb5p because the NFS payload is not encrypted; only added overhead compared to krb5 is the integrity checksum. Performance of krb5i won't be much worse than krb5 but will see some degradation.

Security level	Security	Performance
NFS – krb5p	 Kerberos encryption for credentials in every NFS packet—wraps UID/GID of users/groups in RPC calls in GSS wrapper User requesting access to mount needs a valid Kerberos ticket (either via username/password or manual keytab exchange); ticket expires after specified time period and user must reauthenticate for access 	 Worst performance of the security levels; krb5p has to encrypt/decrypt more. Better performance than krb5p with NFSv4.x for high file count workloads.
	 All of the NFS packet payloads are encrypted with the GSS wrapper (cannot see file handles, permissions, file names, atime/mtime in packet captures). 	
	 Includes integrity check. 	
	 NFS operation type is visible (FSINFO, ACCESS, GETATTR, and so on). 	
	 Ancillary protocols (mount, portmap, nlm, and so on) are not encrypted - (can see export paths, IP addresses) 	

In Cloud Volumes Service, a configured Active Directory server is used as Kerberos server and LDAP server (to lookup user identities from an RFC2307 compatible schema). No other Kerberos or LDAP servers are supported. NetApp highly recommends that you use LDAP for identity management in Cloud Volumes Service. For information on how NFS Kerberos is shown in packet captures, see the section "Packet sniffing/trace considerations."

Data encryption at rest

All volumes in Cloud Volumes Service are encrypted-at-rest using AES-256 encryption, which means all user data written to media is encrypted and can only be decrypted with a per-volume key.

- For CVS-SW, Google-generated keys are used.
- For CVS-Performance, the per-volume keys are stored in a key manager built into the Cloud Volumes Service.

Starting in November 2021, preview customer-managed encryption keys (CMEK) functionality was made available. This enables you to encrypt the per-volume keys with a per-project, per-region master key that is hosted in Google Key Management Service (KMS). KMS enables you to attach external key managers.

For information about configuring KMS for CVS-Performance, see Setting up customer-managed encryption keys.

Firewall

Cloud Volumes Service exposes multiple TCP ports to serve NFS and SMB shares:

- Ports required for NFS access
- Ports required for SMB access

Additionally, SMB, NFS with LDAP including Kerberos, and dual-protocol configurations require access to a Windows Active Directory domain. Active Directory connections must be configured on a per-region basis. Active Directory Domain controllers (DC) are identified by using DNS-based DC discovery using the specified DNS servers. Any of the DCs returned are used. The list of eligible DCs can be limited by specifying an Active Directory site.

Cloud Volumes Service reaches out with IP addresses from the CIDR range allocated with the gcloud compute address command while on-boarding the Cloud Volumes Service. You can use this CIDR as source addresses to configure inbound firewalls to your Active Directory domain controllers.

Active Directory Domain Controllers must expose ports to the Cloud Volumes Service CIDRs as mentioned here.

NAS protocols

NAS protocols overview

NAS protocols include NFS (v3 and v4.1) and SMB/CIFS (2.x and 3.x). These protocols are how CVS allows shared access to data across multiple NAS clients. In addition, Cloud Volumes Service can provide access to NFS and SMB/CIFS clients simultaneously (dual-protocol) while honoring all of the identity and permission settings on files and folders in the NAS shares. To maintain the highest possible data transfer security, Cloud Volumes Service supports protocol encryption in flight using SMB encryption and NFS Kerberos 5p.



Dual-protocol is available with CVS-Performance only.

Basics of NAS protocols

NAS protocols are ways for multiple clients on a network to access the same data on a storage system, such as Cloud Volumes Service on GCP. NFS and SMB are the defined NAS protocols and operate on a client/server basis where Cloud Volumes Service acts as the server. Clients send access, read, and write requests to the server, and the server is responsible for coordinating the locking mechanisms for files, storing permissions and handling identity and authentication requests.

For example, the following general process is followed if a NAS client wants to create a new file in a folder.

1. The client asks the server for information about the directory (permissions, owner, group, file ID, available space, and so on); the server responds with the information if the requesting client and user have the necessary permissions on the parent folder.

- 2. If the permissions on the directory allow access, the client then asks the server if the file name being created already exists in the file system. If the file name is already in use, creation fails. If the file name does not exist, the server lets the client know it can proceed.
- 3. The client issues a call to the server to create the file with the directory handle and file name and sets the access and modified times. The server issues a unique file ID to the file to make sure that no other files are created with the same file ID.
- 4. The client sends a call to check file attributes before the WRITE operation. If permissions allow it, the client then writes the new file. If locking is used by the protocol/application, the client asks the server for a lock to prevent other clients from accessing the file while locked to prevent data corruption.

NFS

NFS is a distributed file system protocol that is an open IETF standard defined in Request for Comments (RFC) that allows anyone to implement the protocol.

Volumes in Cloud Volumes Service are shared out to NFS clients by exporting a path that is accessible to a client or set of clients. Permissions to mount these exports are defined by export policies and rules, which are configurable by Cloud Volumes Service administrators.

The NetApp NFS implementation is considered a gold standard for the protocol and is used in countless enterprise NAS environments. The following sections cover NFS and specific security features available in Cloud Volumes Service and how they are implemented.

Default local UNIX users and groups

Cloud Volumes Service contains several default UNIX users and groups for various basic functionalities. These users and groups cannot currently be modified or deleted. New local users and groups cannot currently be added to Cloud Volumes Service. UNIX users and groups outside of the default users and groups need to be provided by an external LDAP name service.

The following table shows the default users and groups and their corresponding numeric IDs. NetApp recommends not creating new users or groups in LDAP or on the local clients that re-use these numeric IDs.

Default users: numeric IDs	Default groups: numeric IDs
• root:0	• root:0
• pcuser:65534	• daemon:1
• nobody:65535	• pcuser:65534
	• nobody:65535

i

When using NFSv4.1, the root user might display as nobody when running directory listing commands on NFS clients. This is due to the client's ID domain mapping configuration. See the section called NFSv4.1 and the nobody user/group for details on this issue and how to resolve it.

The root user

In Linux, the root account has access to all commands, files, and folders in a Linux-based file system. Because of the power of this account, security best practices often require the root user to be disabled or restricted in some fashion. In NFS exports, the power a root user has over the files and folders can be controlled in Cloud Volumes Service through export policies and rules and a concept known as root squash.

Root squashing ensures that the root user accessing an NFS mount is squashed to the anonymous numeric user 65534 (see the section "The anonymous user") and is currently only available when using CVS-Performance by selecting Off for root access during export policy rule creation. If the root user is squashed to the anonymous user, it no longer has access to run chown or setuid/setgid commands (the sticky bit) on files or folders in the NFS mount, and files or folders created by the root user show the anon UID as the owner/group. In addition, NFSv4 ACLs cannot be modified by the root user. However, the root user still has access to chmod and deleted files that it does not have explicit permissions for. If you want to limit access to a root user's file and folder permissions, consider using a volume with NTFS ACLs, creating a Windows user named root, and applying the desired permissions to the files or folders.

The anonymous user

The anonymous (anon) user ID specifies a UNIX user ID or username that is mapped to client requests that arrive without valid NFS credentials. This can include the root user when root squashing is used. The anon user in Cloud Volumes Service is 65534.

This UID is normally associated with the username nobody or nfsnobody in Linux environments. Cloud Volumes Service also uses 65534 as the local UNIX user' pcuser' (see the section "Default local UNIX users and groups"), which is also the default fallback user for Windows to UNIX name mappings when no valid matching UNIX user can be found in LDAP.

Because of the differences in usernames across Linux and Cloud Volumes Service for UID 65534, the name string for users mapped to 65534 might not match when using NFSv4.1. As a result, you might see nobody as the user on some files and folders. See the section "NFSv4.1 and the nobody user/group" for information about this issue and how to resolve it.

Access control/exports

Initial export/share access for NFS mounts is controlled through host- based export policy rules contained within an export policy. A host IP, host name, subnet, netgroup, or domain is defined to allow access to mount the NFS share and the level of access allowed to the host. Export policy rule configuration options depend on the Cloud Volumes Service level.

For CVS-SW, the following options are available for export-policy configuration:

- Client match. Comma-separated list of IP addresses, comma-separated list of hostnames, subnets, netgroups, domain names.
- **RO/RW access rules.** Select read/write or read only to control level of access to export.CVS-Performance provides the following options:
- Client match. Comma-separated list of IP addresses, comma-separated list of hostnames, subnets, netgroups, domain names.
- RO/RW access rules. Select read/write or read only to control level of access to export.
- Root access (on/off). Configures root squash (see the section "The root user" for details).
- **Protocol type.** This limits access to the NFS mount to a specific protocol version. When specifying both NFSv3 and NFSv4.1 for the volume, either leave both blank or check both boxes.
- Kerberos security level (when Enable Kerberos is selected). Provides the options of krb5, krb5i, and/or krb5p for read-only or read-write access.

Change ownership (chown) and change group (chgrp)

NFS on Cloud Volumes Service only allows the root user to run chown/chgrp on files and folders. Other users see an Operation not permitted error— even on files they own. If you use root squash (as covered in

the section "The root user"), the root is squashed to a nonroot user and is not allowed access to chown and chgrp. There are currently no workarounds in Cloud Volumes Service to allow chown and chgrp for non-root users. If ownership changes are required, consider using dual protocol volumes and set the security style to NTFS to control permissions from the Windows side.

Permission management

Cloud Volumes Service supports both mode bits (such as 644, 777, and so on for rwx) and NFSv4.1 ACLs to control permissions on NFS clients for volumes that use the UNIX security style. Standard permission management is used for these (such as chmod, chown, or nfs4_setfacl) and work with any Linux client that supports them.

Additionally, when using dual protocol volumes set to NTFS, NFS clients can leverage Cloud Volumes Service name mapping to Windows users, which then are used to resolve the NTFS permissions. This requires an LDAP connection to Cloud Volumes Service to provide numeric-ID-to- username translations because Cloud Volumes Service requires a valid UNIX username to map properly to a Windows username.

Providing granular ACLs for NFSv3

Mode bit permissions cover only owner, group, and everyone else in the semantics—meaning that there are no granular user access controls in place for basic NFSv3. Cloud Volumes Service does not support POSIX ACLs, nor extended attributes (such as chattr), so granular ACLs are only possible in the following scenarios with NFSv3:

- NTFS security style volumes (CIFS server required) with valid UNIX to Windows user mappings.
- NFSv4.1 ACLs applied using an admin client mounting NFSv4.1 to apply ACLs.

Both methods require an LDAP connection for UNIX identity management and a valid UNIX user and group information populated (see the section "LDAP") and are only available with CVS-Performance instances. To use NTFS security style volumes with NFS, you must use dual-protocol (SMB and NFSv3) or dual-protocol (SMB and NFSv4.1), even if no SMB connections are made. To use NFSv4.1 ACLs with NFSv3 mounts, you must select Both (NFSv3/NFSv4.1) as the protocol type.

Regular UNIX mode bits don't provide the same level of granularity in permissions that NTFS or NFSv4.x ACLs provide. The following table compares the permission granularity between NFSv3 mode bits and NFSv4.1 ACLs. For information about NFSv4.1 ACLs, see nfs4_acl - NFSv4 Access Control Lists.

NFSv3 mode bits	NFSv4.1 ACLs
 Set user ID on execution Set group ID on execution Save swapped text (not defined in POSIX) Read permission for owner Write permission for owner 	Access control entry (ACE) types (Allow/Deny/Audit) * Inheritance flags * directory-inherit * file-inherit * no-propagate-inherit * inherit-only Permissions
 Execute permission for owner on a file; or look up (search) permission for owner in directory Read permission for group Write permission for group 	 * read-data (files) / list-directory (directories) * write-data (files) / create-file (directories) * append-data (files) / create-subdirectory (directories) * execute (files) / change-directory (directories) * delete
 Execute permission for group on a file; or look up (search) permission for group in directory Read permission for others Write permission for others Execute permission for others on a file; or look up (search) permission for others in directory 	 * delete * delete-child * read-attributes * write-attributes * read-named-attributes * write-named-attributes * read-ACL * write-ACL * write-owner * Synchronize

Finally, NFS group membership (in both NFSv3 and NFSV4.x) is limited to a default maximum of 16 for AUTH_SYS as per the RPC packet limits. NFS Kerberos provides up to 32 groups and NFSv4 ACLs remove the limitation by way of granular user and group ACLs (up to 1024 entries per ACE).

Additionally, Cloud Volumes Service provides extended group support to extend the maximum supported groups up to 32. This requires an LDAP connection to an LDAP server that contains valid UNIX user and group identities. For more information about configuring this, see Creating and managing NFS volumes in the Google documentation.

NFSv3 user and group IDs

NFSv3 user and group IDs come across the wire as numeric IDs rather than names. Cloud Volumes Service does no username resolution for these numeric IDs with NFSv3, with UNIX security style volumes using just mode bits. When NFSv4.1 ACLs are present, a numeric ID lookup and/or name string lookup is needed to resolve the ACL properly—even when using NFSv3. With NTFS security style volumes, Cloud Volumes Service must resolve a numeric ID to a valid UNIX user and then map to a valid Windows user to negotiate access rights.

Security limitations of NFSv3 user and group IDs

With NFSv3, the client and server never have to confirm that the user attempting a read or write with a numeric ID is a valid user; it is just implicitly trusted. This opens the file system up to potential breaches simply by spoofing any numeric ID. To prevent security holes like this, there are a few options available to Cloud Volumes Service.

• Implementing Kerberos for NFS forces users to authenticate with a username and password or keytab file to get a Kerberos ticket to allow access into a mount. Kerberos is available with CVS-Performance instances and only with NFSv4.1.

- Limiting the list of hosts in your export policy rules limits which NFSv3 clients have access to the Cloud Volumes Service volume.
- Using dual-protocol volumes and applying NTFS ACLs to the volume forces NFSv3 clients to resolve numeric IDs to valid UNIX usernames to authenticate properly to access mounts. This requires enabling LDAP and configuring UNIX user and group identities.
- Squashing the root user limits the damage a root user can do to an NFS mount but does not completely remove risk. For more information, see the section "The root user."

Ultimately, NFS security is limited to what the protocol version you are using offers. NFSv3, while more performant in general than NFSv4.1, does not provide the same level of security.

NFSv4.1

NFSv4.1 provides greater security and reliability as compared to NFSv3, for the following reasons:

- · Integrated locking through a lease-based mechanism
- Stateful sessions
- All NFS functionality over a single port (2049)
- TCP only
- ID domain mapping
- Kerberos integration (NFSv3 can use Kerberos, but only for NFS, not for ancillary protocols such as NLM)

NFSv4.1 dependencies

Because of the additionally security features in NFSv4.1, there are some external dependencies involved that were not needed to use NFSv3 (similar to how SMB requires dependencies such as Active Directory).

NFSv4.1 ACLs

Cloud Volumes Service offers support for NFSv4.x ACLs, which deliver distinct advantages over normal POSIX-style permissions, such as the following:

- · Granular control of user access to files and directories
- Better NFS security
- · Improved interoperability with CIFS/SMB
- Removal of the NFS limitation of 16 groups per user with AUTH_SYS security
- ACLs bypass the need for group ID (GID) resolution, which effectively removes the GID limitNFSv4.1 ACLs are controlled from NFS clients—not from Cloud Volumes Service. To use NFSv4.1 ACLs, be sure your client's software version supports them and the proper NFS utilities are installed.

Compatibility between NFSv4.1 ACLs and SMB clients

NFSv4 ACLs are different from Windows file-level ACLs (NTFS ACLs) but carry similar functionality. However, in multiprotocol NAS environments, if NFSv4.1 ACLs are present and you are using dual-protocol access (NFS and SMB on the same datasets), clients using SMB2.0 and later won't be able to view or manage ACLs from Windows security tabs.

How NFSv4.1 ACLs work

For reference, the following terms are defined:

- · Access control list (ACL). A list of permissions entries.
- Access control entry (ACE). A permission entry in the list.

When a client sets an NFSv4.1 ACL on a file during a SETATTR operation, Cloud Volumes Service sets that ACL on the object, replacing any existing ACL. If there is no ACL on a file, then the mode permissions on the file are calculated from OWNER@, GROUP@, and EVERYONE@. If there are any existing SUID/SGID/STICKY bits on the file, they are not affected.

When a client gets an NFSv4.1 ACL on a file during the course of a GETATTR operation, Cloud Volumes Service reads the NFSv4.1 ACL associated with the object, constructs a list of ACEs, and returns the list to the client. If the file has an NT ACL or mode bits, then an ACL is constructed from mode bits and is returned to the client.

Access is denied if a DENY ACE is present in the ACL; access is granted if an ALLOW ACE exists. However, access is also denied if neither of the ACEs is present in the ACL.

A security descriptor consists of a security ACL (SACL) and a discretionary ACL (DACL). When NFSv4.1 interoperates with CIFS/SMB, the DACL is one-to-one mapped with NFSv4 and CIFS. The DACL consists of the ALLOW and the DENY ACEs.

If a basic chmod is run on a file or folder with NFSv4.1 ACLs set, existing user and group ACLs are preserved, but the default OWNER@, GROUP@, EVERYONE@ ACLs are modified.

A client using NFSv4.1 ACLs can set and view ACLs for files and directories on the system. When a new file or subdirectory is created in a directory that has an ACL, that object inherits all ACEs in the ACL that have been tagged with the appropriate inheritance flags.

If a file or directory has an NFSv4.1 ACL, that ACL is used to control access no matter which protocol is used to access the file or directory.

Files and directories inherit ACEs from NFSv4 ACLs on parent directories (possibly with appropriate modifications) as long as the ACEs have been tagged with the correct inheritance flags.

When a file or directory is created as the result of an NFSv4 request, the ACL on the resulting file or directory depends on whether the file creation request includes an ACL or only standard UNIX file access permissions. The ACL also depends on whether the parent directory has an ACL.

- If the request includes an ACL, that ACL is used.
- If the request includes only standard UNIX file access permissions and the parent directory does not have an ACL, the client file mode is used to set standard UNIX file access permissions.
- If the request includes only standard UNIX file access permissions and the parent directory has a noninheritable ACL, a default ACL based on the mode bits passed into the request is set on the new object.
- If the request includes only standard UNIX file access permissions but the parent directory has an ACL, the ACEs in the parent directory's ACL are inherited by the new file or directory as long as the ACEs have been tagged with the appropriate inheritance flags.

ACE permissions

NFSv4.1 ACLs permissions uses a series of upper- and lower-case letter values (such as rxtncy) to control access. For more information about these letter values, see HOW TO: Use NFSv4 ACL.

NFSv4.1 ACL behavior with umask and ACL inheritance

NFSv4 ACLs provide the ability to offer ACL inheritance. ACL inheritance means that files or folders created beneath objects with NFSv4.1 ACLs set can inherit the ACLs based on the configuration of the ACL inheritance flag.

Umask is used to control the permission level at which files and folders are created in a directory without administrator interaction. By default, Cloud Volumes Service allows umask to override inherited ACLs, which is expected behavior as per RFC 5661.

ACL formatting

NFSv4.1 ACLs have specific formatting. The following example is an ACE set on a file:

A::ldapuser@domain.netapp.com:rwatTnNcCy

The preceding example follows the ACL format guidelines of:

```
type:flags:principal:permissions
```

A type of A means "allow." The inherit flags are not set in this case, because the principal is not a group and does not include inheritance. Also, because the ACE is not an AUDIT entry, there is no need to set the audit flags. For more information about NFSv4.1 ACLs, see http://linux.die.net/man/5/nfs4_acl.

If the NFSv4.1 ACL is not set properly (or a name string cannot be resolved by the client and server), the ACL might not behave as expected, or the ACL change might fail to apply and throw an error.

Sample errors include:

```
Failed setxattr operation: Invalid argument
Scanning ACE string 'A:: user@rwaDxtTnNcCy' failed.
```

Explicit DENY

NFSv4.1 permissions can include explicit DENY attributes for OWNER, GROUP, and EVERYONE. That is because NFSv4.1 ACLs are default-deny, which means that if an ACL is not explicitly granted by an ACE, then it is denied. Explicit DENY attributes override any ACCESS ACEs, explicit or not.

DENY ACEs are set with an attribute tag of D.

In the example below, GROUP@ is allowed all read and execute permissions, but denied all write access.

```
sh-4.1$ nfs4_getfacl /mixed
A::ldapuser@domain.netapp.com:ratTnNcCy
A::OWNER@:rwaDxtTnNcCy
D::OWNER@:
A:g:GROUP@:rxtncy
D:g:GROUP@:waDTC
A::EVERYONE@:rxtncy
D::EVERYONE@:waDTC
```

DENY ACEs should be avoided whenever possible because they can be confusing and complicated; ALLOW ACLs that are not explicitly defined are implicitly denied. When DENY ACEs are set, users might be denied access when they expect to be granted access.

The preceding set of ACEs is equivalent to 755 in mode bits, which means:

- The owner has full rights.
- · Groups have read only.
- Others have read only.

However, even if permissions are adjusted to the 775 equivalent, access can be denied because of the explicit DENY set on EVERYONE.

NFSv4.1 ID domain mapping dependencies

NFSv4.1 leverages ID domain mapping logic as a security layer to help verify that a user attempting access to an NFSv4.1 mount is indeed who they claim to be. In these cases, the username and group name coming from the NFSv4.1 client appends a name string and sends it to the Cloud Volumes Service instance. If that username/group name and ID string combination does not match, then the user and/or group is squashed to the default nobody user specified in the /etc/idmapd.conf file on the client.

This ID string is a requirement for proper permission adherence, especially when NFSv4.1 ACLs and/or Kerberos are in use. As a result, name service server dependencies such as LDAP servers are necessary to ensure consistency across clients and Cloud Volumes Service for proper user and group name identity resolution.

Cloud Volumes Service uses a static default ID domain name value of defaultv4iddomain.com. NFS clients default to the DNS domain name for its ID domain name settings, but you can manually adjust the ID domain name in /etc/idmapd.conf.

If LDAP is enabled in Cloud Volumes Service, then Cloud Volumes Service automates the NFS ID domain to change to what is configured for the search domain in DNS and clients won't need to be modified unless they use different DNS domain search names.

When Cloud Volumes Service can resolve a username or group name in local files or LDAP, the domain string is used and non-matching domain IDs squash to nobody. If Cloud Volumes Service cannot find a username or group name in local files or LDAP, the numeric ID value is used and the NFS client resolves the name properly (this is similar to NFSv3 behavior).

Without changing the client's NFSv4.1 ID domain to match what the Cloud Volumes Service volume is using, you see the following behavior:

- UNIX users and groups with local entries in Cloud Volumes Service (such as root, as defined in local UNIX users and groups) are squashed to the nobody value.
- UNIX users and groups with entries in LDAP (if Cloud Volumes Service is configured to use LDAP) squashes to nobody if DNS domains are different between NFS clients and Cloud Volumes Service.
- UNIX users and groups with no local entries or LDAP entries use the numeric ID value and resolve to the name specified on the NFS client. If no name exists on the client, only the numeric ID is shown.

The following shows the results of the preceding scenario:

```
# ls -la /mnt/home/prof1/nfs4/
total 8
drwxr-xr-x 2 nobody nobody 4096 Feb 3 12:07 .
drwxrwxrwx 7 root root 4096 Feb 3 12:06 ..
-rw-r--r-- 1 9835 9835 0 Feb 3 12:07 client-user-no-name
-rw-r--r-- 1 nobody nobody 0 Feb 3 12:07 ldap-user-file
-rw-r--r-- 1 nobody nobody 0 Feb 3 12:06 root-user-file
```

When the client and server ID domains match, this is how the same file listing looks:

```
# ls -la
total 8
drwxr-xr-x 2 root
                                 4096 Feb 3 12:07 .
                   root
                                 4096 Feb 3 12:06 ..
drwxrwxrwx 7 root
                   root
-rw-r--r-- 1
              9835
                                   0 Feb 3 12:07 client-user-no-name
                            9835
-rw-r--r-- 1 apache apache-group
                                   0 Feb 3 12:07 ldap-user-file
                                    0 Feb 3 12:06 root-user-file
-rw-r--r-- 1 root
                   root
```

For more information about this issue and how to resolve it, see the section "NFSv4.1 and the nobody user/group."

Kerberos dependencies

If you plan to use Kerberos with NFS, you must have the following with Cloud Volumes Service:

- Active Directory domain for Kerberos Distribution Center services (KDC)
- Active Directory domain with user and group attributes populated with UNIX information for LDAP functionality (NFS Kerberos in Cloud Volumes Service requires a user SPN to UNIX user mapping for proper functionality.)
- · LDAP enabled on the Cloud Volumes Service instance
- · Active Directory domain for DNS services

NFSv4.1 and the nobody user/group

One of the most common issues seen with an NFSv4.1 configuration is when a file or folder is shown in a listing using 1s as being owned by the user:group combination of nobody:nobody.

For example:

```
sh-4.2$ ls -la | grep prof1-file
-rw-r--r-- 1 nobody nobody 0 Apr 24 13:25 prof1-file
```

And the numeric ID is 99.

```
sh-4.2$ ls -lan | grep prof1-file
-rw-r--r- 1 99 99 0 Apr 24 13:25 prof1-file
```

In some instances, the file might show the correct owner but nobody as the group.

```
sh-4.2$ ls -la | grep newfile1
-rw-r--r- 1 prof1 nobody 0 Oct 9 2019 newfile1
```

Who is nobody?

The nobody user in NFSv4.1 is different from the nfsnobody user. You can view how an NFS client sees each user by running the id command:

```
# id nobody
uid=99(nobody) gid=99(nobody) groups=99(nobody)
# id nfsnobody
uid=65534(nfsnobody) gid=65534(nfsnobody) groups=65534(nfsnobody)
```

With NFSv4.1, the nobody user is the default user defined by the idmapd.conf file and can be defined as any user you want to use.

```
# cat /etc/idmapd.conf | grep nobody
#Nobody-User = nobody
#Nobody-Group = nobody
```

Why does this happen?

Because security through name string mapping is a key tenet of NFSv4.1 operations, the default behavior when a name string does not match properly is to squash that user to one that won't normally have any access to files and folders owned by users and groups.

When you see nobody for the user and/or group in file listings, this generally means something in NFSv4.1 is misconfigured. Case sensitivity can come into play here.

For example, if user1@CVSDEMO.LOCAL (uid 1234, gid 1234) is accessing an export, then Cloud Volumes Service must be able to find user1@CVSDEMO.LOCAL (uid 1234, gid 1234). If the user in Cloud Volumes Service is USER1@CVSDEMO.LOCAL, then it won't match (uppercase USER1 versus lowercase user1). In

many cases, you can see the following in the messages file on the client:

May 19 13:14:29 centos7 nfsidmap[17481]: nss_getpwnam: name 'root@defaultv4iddomain.com' does not map into domain 'CVSDEMO.LOCAL' May 19 13:15:05 centos7 nfsidmap[17534]: nss_getpwnam: name 'nobody' does not map into domain 'CVSDEMO.LOCAL'

The client and server must both agree that a user is indeed who they are claiming to be, so you must check the following to ensure that the user that the client sees has the same information as the user that Cloud Volumes Service sees.

- NFSv4.x ID domain. Client: idmapd.conf file; Cloud Volumes Service uses defaultv4iddomain.com and cannot be changed manually. If using LDAP with NFSv4.1, Cloud Volumes Service changes the ID domain to what the DNS search domain is using, which is the same as the AD domain.
- User name and numeric IDs. This determines where the client is looking for user names and leverages the name service switch configuration—client: nsswitch.conf and/or local passwd and group files; Cloud Volumes Service does not allow modifications to this but automatically adds LDAP to the configuration when it is enabled.
- Group name and numeric IDs. This determines where the client is looking for group names and leverages the name service switch configuration—client: nsswitch.conf and/or local passwd and group files; Cloud Volumes Service does not allow modifications to this but automatically adds LDAP to the configuration when it is enabled.

In almost all cases, if you see nobody in user and group listings from clients, the issue is user or group name domain ID translation between Cloud Volumes Service and the NFS client. To avoid this scenario, use LDAP to resolve user and group information between clients and Cloud Volumes Service.

Viewing name ID strings for NFSv4.1 on clients

If you are using NFSv4.1, there is a name-string mapping that takes place during NFS operations, as previously described.

In addition to using /var/log/messages to find an issue with NFSv4 IDs, you can use the nfsidmap -l command on the NFS client to view which usernames have properly mapped to the NFSv4 domain.

For example, this is output of the command after a user that can be found by the client and Cloud Volumes Service accesses an NFSv4.x mount:

```
# nfsidmap -1
4 .id_resolver keys found:
    gid:daemon@CVSDEMO.LOCAL
    uid:nfs4@CVSDEMO.LOCAL
    gid:root@CVSDEMO.LOCAL
    uid:root@CVSDEMO.LOCAL
```

When a user that does not map properly into the NFSv4.1 ID domain (in this case, netapp-user) tries to access the same mount and touches a file, they are assigned nobody:nobody, as expected.

```
# su netapp-user
sh-4.2$ id
uid=482600012(netapp-user), 2000(secondary)
sh-4.2$ cd /mnt/nfs4/
sh-4.2$ touch newfile
sh-4.2$ ls -la
total 16
drwxrwxrwx 5 root root
                          4096 Jan 14 17:13 .
drwxr-xr-x. 8 root root
                          81 Jan 14 10:02 ..
-rw-r--r-- 1 nobody nobody
                             0 Jan 14 17:13 newfile
drwxrwxrwx 2 root root 4096 Jan 13 13:20 gtree1
drwxrwxrwx 2 root root 4096 Jan 13 13:13 qtree2
drwxr-xr-x 2 nfs4
                   daemon 4096 Jan 11 14:30 testdir
```

The nfsidmap -l output shows the user pcuser in the display but not netapp-user; this is the anonymous user in our export-policy rule (65534).

```
# nfsidmap -1
6 .id_resolver keys found:
    gid:pcuser@CVSDEMO.LOCAL
    uid:pcuser@CVSDEMO.LOCAL
    gid:daemon@CVSDEMO.LOCAL
    uid:nfs4@CVSDEMO.LOCAL
    gid:root@CVSDEMO.LOCAL
    uid:root@CVSDEMO.LOCAL
```

SMB

SMB is a network file sharing protocol developed by Microsoft that provides centralized user/group authentication, permissions, locking, and file sharing to multiple SMB clients over an Ethernet network. Files and folders are presented to clients by way of shares, which can be configured with a variety of share properties and offers access control through share-level permissions. SMB can be presented to any client that offers support for the protocol, including Windows, Apple, and Linux clients.

Cloud Volumes Service provides support for the SMB 2.1 and 3.x versions of the protocol.

Access control/SMB shares

- When a Windows username requests access to the Cloud Volumes Service volume, Cloud Volumes Service looks for a UNIX username using the methods configured by Cloud Volumes Service administrators.
- If an external UNIX identity provider (LDAP) is configured and Windows/UNIX usernames are identical, then Windows usernames will map 1:1 to UNIX usernames without any additional configuration needed. When LDAP is enabled, Active Directory is used to host those UNIX attributes for user and group objects.

- If Windows names and UNIX names do not match identically, then LDAP must be configured to allow Cloud Volumes Service to use the LDAP name mapping configuration (see the section "Using LDAP for asymmetric name mapping").
- If LDAP is not in use, then Windows SMB users map to a default local UNIX user named pcuser in Cloud Volumes Service. This means files written in Windows by users that map to the pcuser show UNIX ownership as pcuser in multiprotocol NAS environments. pcuser here is effectively the nobody user in Linux environments (UID 65534).

In deployments with SMB only, the pcuser mapping still occurs, but it won't matter, because Windows user and group ownership is correctly displayed and NFS access to the SMB-only volume is not allowed. In addition, SMB-only volumes do not support conversion to NFS or dual-protocol volumes after they are created.

Windows leverages Kerberos for username authentication with the Active Directory domain controllers, which requires a username/password exchange with the AD DCs, which is external to the Cloud Volumes Service instance. Kerberos authentication is used when the \\SERVERNAME UNC path is used by the SMB clients and the following is true:

- DNS A/AAAA entry exists for SERVERNAME
- A valid SPN for SMB/CIFS access exists for SERVERNAME

When a Cloud Volumes Service SMB volume is created, the machine account name is created as defined in the section "How Cloud Volumes Service shows up in Active Directory." That machine account name also becomes the SMB share access path because Cloud Volumes Service leverages Dynamic DNS (DDNS) to create the necessary A/AAAA and PTR entries in DNS and the necessary SPN entries on the machine account principal.



For PTR entries to be created, the reverse lookup zone for the Cloud Volumes Service instance IP address must exist on the DNS server.

For example, this Cloud Volumes Service volume uses the following UNC share path: \\cvs-east-433d.cvsdemo.local.

In Active Directory, these are the Cloud Volumes Service-generated SPN entries:

```
PS C:\> setspn /L CVS-EAST-433D
Registered ServicePrincipalNames for CN=CVS-EAST-433D,CN=Computers,DC=cvsdemo,DC=local:
HOST/cvs-east-433d.cvsdemo.local
HOST/CVS-EAST-433D
```

This is the DNS forward/reverse lookup result:

```
PS C:\> nslookup CVS-EAST-433D
Server: activedirectory. region. lab. internal
Address: 10. xx.0. xx
Name: CVS-EAST-433D.cvsdemo.local
Address: 10. xxx.0. x
PS C:\> nslookup 10. xxx.0. x
Server: activedirectory.region.lab.internal
Address: 10.xx.0.xx
Name: CVS-EAST-433D.CVSDEMO.LOCAL
Address: 10. xxx.0. x
```

Optionally, more access control can be applied by enabling/requiring SMB encryption for SMB shares in Cloud Volumes Service. If SMB encryption isn't supported by one of the endpoints, then access is not allowed.

Using SMB name aliases

In some cases, it might be a security concern for end users to know the machine account name in use for Cloud Volumes Service. In other cases, you might simply want to provide a simpler access path to your end users. In those cases, you can create SMB aliases.

If you want to create aliases for the SMB share path, you can leverage what is known as a CNAME record in DNS. For example, if you want to use the name \\CIFS to access shares instead of \\cvs-east-433d.cvsdemo.local, but you still want to use Kerberos authentication, a CNAME in DNS that points to the existing A/AAAA record and an additional SPN added to the existing machine account provides Kerberos access.

cifs Properties		?	×
Alias (CNAME) Security			
Alia <u>s</u> name (uses parent domain if left bl	ank):		
cifs			
Fully qualified domain name (FQDN):			
cifs.cvsdemo.local			
Fully qualified domain name (FQDN) for CVS-EAST-433D.CVSDEMO.LOCAL	arget host:	11-11-1	
CVS-EAST-435D.CVSDEINO.LOCAL		Browse.	
ОК	Cancel	Ap	olv

This is the resulting DNS forward lookup result after adding a CNAME:

PS C:\> nslookup cifs
Server: ok-activedirectory.us-east4-a.c.cv-solution-architect-
lab.internal
Address: 10. xx.0. xx
Name: CVS-EAST-433D.cvsdemo.local
Address: 10. xxx.0. x
Aliases: cifs.cvsdemo.local

This is the resulting SPN query after adding new SPNs:

PS C:\> setspn /L CVS-EAST-433D Registered ServicePrincipalNames for CN=CVS-EAST-433D,CN=Computers,DC=cvsdemo,DC=local: cifs/cifs.cvsdemo.local cifs/cifs HOST/cvs-east-433d.cvsdemo.local HOST/CVS-EAST-433D

In a packet capture, we can see the Session Setup Request using the SPN tied to the CNAME.

431 4.156722	SMB2	308 Negotiate Protocol Response
432 4.156785	SMB2	232 Negotiate Protocol Request
434 4.158108	SMB2	374 Negotiate Protocol Response
435 4.160977	SMB2	1978 Session Setup Request
437 4.166224	SMB2	322 Session Setup Response
438 4.166891	SMB2	152 Tree Connect Request Tree: \\cifs\IPC
439 4.168063	SMB2	138 Tree Connect Response

```
realm: CVSDEMO.LOCAL

sname
name-type: kRB5-NT-SRV-INST (2)

sname-string: 2 items
SNameString: cifs
SNameString: cifs
enc-part
etype: eTYPE-ARCFOUR-HMAC-MD5 (23)
```

SMB authentication dialects

Cloud Volumes Service supports the following dialects for SMB authentication:

- LM
- NTLM
- NTLMv2
- Kerberos

Kerberos authentication for SMB share access is the most secure level of authentication you can use. With AES and SMB encryption enabled, the security level is further increased.

Cloud Volumes Service also supports backward compatibility for LM and NTLM authentication. When Kerberos is misconfigured (such as when creating SMB aliases), share access falls back to weaker authentication methods (such as NTLMv2). Because these mechanisms are less secure, they are disabled in some Active Directory environments. If weaker authentication methods are disabled and Kerberos is not configured properly, share access fails because there is no valid authentication method to fall back to.

For information about configuring/viewing your supported authentication levels in Active Directory, see Network security: LAN Manager authentication level.

Permission models

NTFS/File permissions

NTFS permissions are the permissions applied to files and folders in file systems adhering to NTFS logic. You can apply NTFS permissions in Basic or Advanced and can be set to Allow or Deny for access control.

Basic permissions include the following:

- Full Control
- Modify
- Read & Execute
- Read
- Write

When you set permissions for a user or group, referred to as an ACE, it resides in an ACL. NTFS permissions use the same read/write/execute basics as UNIX mode bits, but they can also extend to more granular and extended access controls (also known as Special Permissions), such as Take Ownership, Create Folders/Append Data, Write Attributes, and more.

Standard UNIX mode bits do not provide the same level of granularity as NTFS permissions (such as being able to set permissions for individual user and group objects in an ACL or setting extended attributes). However, NFSv4.1 ACLs do provide the same functionality as NTFS ACLs.

NTFS permissions are more specific than share permissions and can be used in conjunction with share permissions. With NTFS permission structures, the most restrictive applies. As such, explicit denials to a user or group overrides even Full Control when defining access rights.

NTFS permissions are controlled from Windows SMB clients.

Share permissions

Share permissions are more general than NTFS permissions (Read/Change/Full Control only) and control the initial entry into an SMB share—similar to how NFS export policy rules work.

Although NFS export policy rules control access through host-based information such as IP addresses or host names, SMB share permissions can control access by using user and group ACEs in a share ACL. You can set share ACLs either from the Windows client or from the Cloud Volumes Service management UI.

By default, share ACLs and initial volume ACLs include Everyone with Full Control. The file ACLs should be changed but share permissions are overruled by the file permissions on objects in the share.

For instance, if a user is only allowed Read access to the Cloud Volumes Service volume file ACL, they are denied access to create files and folders even though the share ACL is set to Everyone with Full Control, as shown in the following figure.

eneral Publish Share	Permissions S	ecurity		General Publish Share Permissions Security	
group or user names:					
Everyone			1	Object name: //CVS-EAST-433D/ecstatic-angry-jonamar	
Lionano				Group or user names:	
				a cvs-svc	_
				Justin Parisi (parisi@cvsdemo.local)	
		Add	Remove	To change permissions, click Edit.	
ermissions for Everyone	1	Allow	Deny	Permissions for Justin Parisi Allow Deny	у
Full Control				Full control	
Change				Modify	
Read				Read & execute	
				List folder contents	
				↓ v	_
	ОК	Cancel	Apply	OK Cancel A	pp
→ • ↑ 👢 :			Apply tic-angry-jonarnar	OK Cancel ✓ 乙 Search ecstatic-angry-jonarna	
		> cifs > ecstat			ar
	> Network	> cifs > ecstat		✓ ひ Search ecstatic-angry-jonarna	ar
	> Network	> cifs > ecstat		✓ ひ Search ecstatic-angry-jonarna	ar
🖈 Quick access	> Network : Nam	> cifs > ecstat		✓ ひ Search ecstatic-angry-jonarna Date modified Type	ar
 Quick access Desktop Downloads 	Network	> cifs > ecstat		✓ ひ Search ecstatic-angry-jonarna Date modified Type This folder is empty.	ar
 Quick access Desktop Downloads Documents 	Network	> cifs > ecstat	tic-angry-jonarnar	✓ ひ Search ecstatic-angry-jonarna Date modified Type	ar
 Quick access Desktop Downloads Documents Pictures 	Network	 cifs > ecstat ne ation Folder Ac 	tic-angry-jonarnar	・ ひ Search ecstatic-angry-jonarna Date modified Type This folder is empty.	ar
 Quick access Desktop Downloads Documents 	Network	 cifs > ecstat ne ation Folder Ac 	tic-angry-jonarnar	・ ひ Search ecstatic-angry-jonarna Date modified Type This folder is empty.	ar
 Quick access Desktop Downloads Documents Pictures System32 	Network	 cifs > ecstat ne ation Folder Ac 	tic-angry-jonarnar	✓ ひ Search ecstatic-angry-jonarna Date modified Type This folder is empty. ✓ m this action	ar
 Quick access Desktop Downloads Documents Pictures 	Network	 cifs > ecstat ne ation Folder Ac 	tic-angry-jonarnar	✓ ひ Search ecstatic-angry-jonarna Date modified Type This folder is empty. ✓ m this action	ar
 Quick access Desktop Downloads Documents Pictures System32 This PC 	Network	 cifs > ecstat ne ation Folder Ac 	tic-angry-jonarnar	✓ ひ Search ecstatic-angry-jonarna Date modified Type This folder is empty. ✓ m this action	ar S

For best security results, do the following:

- Remove Everyone from the share and file ACLs and instead set share access for users or groups.
- Use groups for access control instead of individual users for ease of management and faster removal/addition of users to share ACLs through group management.
- Allow less restrictive, more general share access to the ACEs on the share permissions and lock down access to users and groups with file permissions for more granular access control.
- Avoid general use of explicit deny ACLs, because they override allow ACLs. Limit use of explicit deny ACLs for users or groups that need to be restricted from access to a file system quickly.
- Make sure that you pay attention to the ACL inheritance settings when modifying permissions; setting the inheritance flag at the top level of a directory or volume with high file counts means that each file below that

directory or volume has inherited permissions added to it, which can create unwanted behavior such as unintended access/denial and long churn of permission modification as each file is adjusted.

SMB share security features

Snapshot directory visible: Unchecked

When you first create a volume with SMB access in Cloud Volumes Service, you are presented with a series of choices for securing that volume.

Some of these choices depend on the Cloud Volumes Service level (Performance or Software) and choices include:

• Make snapshot directory visible (available for both CVS-Performance and CVS-SW). This option controls whether or not SMB clients can access the Snapshot directory in an SMB share (\\server\share\~snapshot and/or Previous Versions tab). The default setting is Not Checked, which means that the volume defaults to hiding and disallowing access to the ~snapshot directory, and no Snapshot copies appear in the Previous Versions tab for the volume.

cvs-parisi (\\CVS-EAS	T-C2DB) Properties	×	🜷 cvs-parisi (\\CVS-EAS	T-C2DB) Properties	>
General Previous Versions	Network Customize	Security Classification	General Previous Versions	Network Customize	Security Classification
	rsions come from shade natically to your compu			sions come from shad natically to your compu	
Eolder versions:	Date mo	dified	Eolder versions:	Date mo	dified
There are n	o previous versions a	available	✓ Today (1) € cvs-parisi	2/1/202	2 6:56 PM
	<u>O</u> pen	▼ Restore ▼		Open	▼ <u>R</u> estore ▼
	OK Can			OK Car	

Snapshot directory visible: Checked

Hiding Snapshot copies from end users might be desired for security reasons, performance reasons (hiding these folders from AV scans) or preference. Cloud Volumes Service Snapshots are read- only, so even if these Snapshots are visible, end users cannot delete or modify files in the Snapshot directory. File permissions on the files or folders at the time the Snapshot copy was taken apply. If a file or folder's permissions change between Snapshot copies, then the changes also apply to the files or folders in the Snapshot directory. Users and groups can gain access to these files or folders based on permissions. While deletes or modifications of files in the Snapshot directory are not possible, it is possible to copy files or folders out of the Snapshot

directory.

- Enable SMB encryption (available for both CVS-Performance and CVS-SW). SMB encryption is disabled on the SMB share by default (unchecked). Checking the box enables SMB encryption, which means traffic between the SMB client and server is encrypted in-flight with the highest supported encryption levels negotiated. Cloud Volumes Service supports up to AES-256 encryption for SMB. Enabling SMB encryption does carry a performance penalty that might or might not be noticeable to your SMB clients—roughly in the 10-20% range. NetApp strongly encourages testing to see if that performance penalty is acceptable.
- Hide SMB share (available for both CVS-Performance and CVS-SW). Setting this option hides the SMB share path from normal browsing. This means that clients that do not know the share path cannot see the shares when accessing the default UNC path (such as \\CVS-SMB). When the checkbox is selected, only clients that explicitly know the SMB share path or have the share path defined by a Group Policy Object can access it (security through obfuscation).
- Enable access-based enumeration (ABE) (CVS-SW only). This is similar to hiding the SMB share, except the shares or files are only hidden from users or groups that do not have permissions to access the objects. For instance, if Windows user joe is not allowed at least Read access through the permissions, then the Windows user joe cannot see the SMB share or files at all. This is disabled by default, and you can enable it by selecting the checkbox. For more information on ABE, see the NetApp Knowledge Base article How does Access Based Enumeration (ABE) work?
- Enable Continuously Available (CA) share support (CVS-Performance only). Continuously Available SMB shares provide a way to minimize application disruptions during failover events by replicating lock states across nodes in the Cloud Volumes Service backend system. This is not a security feature, but it does offer better overall resiliency. Currently, only SQL Server and FSLogix applications are supported for this functionality.

Default hidden shares

When an SMB server is created in Cloud Volumes Service, there are hidden administrative shares (using the \$ naming convention) that are created in addition to the data volume SMB share. These include C\$ (namespace access) and IPC\$ (sharing named pipes for communication between programs, such as the remote procedure calls (RPC) used for Microsoft Management Console (MMC) access).

The IPC\$ share contains no share ACLs and cannot be modified—it is strictly used for RPC calls and Windows disallows anonymous access to these shares by default.

The C\$ share allows BUILTIN/Administrators access by default, but Cloud Volumes Service automation removes the share ACL and does not allow access to anyone because access to the C\$ share allows visibility into all mounted volumes in the Cloud Volumes Service file systems. As a result, attempts to navigate to \\SERVER\C\$ fail.

Accounts with local/BUILTIN administrator/backup rights

Cloud Volumes Service SMB servers maintain similar functionality to regular Windows SMB servers in that there are local groups (such as BUILTIN\Administrators) that apply access rights to select domain users and groups.

When you specify a user to be added to Backup Users, the user is added to the BUILTIN\Backup Operators group in the Cloud Volumes Service instance that uses that Active Directory connection, which then gets the SeBackupPrivilege and SeRestorePrivilege.

When you add a user to Security Privilege Users, the user is given the SeSecurityPrivilege, which is useful in some application use cases, such as SQL Server on SMB shares.

Backup Users

Provide a comma separated list of domain users or a domain group name that require elevated privileges to access volumes created by Cloud Volumes Service.

Accountnames _____ administrator,cvs-svc

Security Privilege Users

Provide a list of comma separated domain user accounts that require elevated privileges to manage security log for the Active Directory associated with Cloud Volumes Service.

Accountnames administrator,cvs-svc

You can view Cloud Volumes Service local group memberships through the MMC with the proper privileges. The following figure shows users that have been added by using the Cloud Volumes Service console.

Backup Operator	s Properties	5		?	Х
General					
Backu	up Operators				
Description:	Backup O	perators group			
Members:					
CVSDEMC		Dr			
A <u>d</u> d	Remove		to a user's group fective until the ne on.		
	ОК	Cancel	Apply	He	əlp

The following table shows the list of default BUILTIN groups and what users/groups are added by default.

Local/BUILTIN group	Default members
BUILTIN\Administrators*	DOMAIN\Domain Admins
BUILTIN\Backup Operators*	None
BUILTIN\Guests	DOMAIN\Domain Guests
BUILTIN\Power Users	None
BUILTIN\Domain Users	DOMAIN\Domain Users

*Group membership controlled in Cloud Volumes Service Active Directory connection configuration.

You can view local users and groups (and group members) in the MMC window, but you cannot add or delete objects or change group memberships from this console. By default, only the Domain Admins group and Administrator are added to the BUILTIN\Administrators group in Cloud Volumes Service. Currently, you cannot modify this.

Computer Management (CVS-EAST-C2D8)	Name Full Name	Description Built-in administrator account	Computer Management (CVS-EAST-C2DB)	Name Administrators	Description Built-in Administrators group All users Built-in Guests Group Restricted administrative privileges Backup Operators group
Administrators	Properties		?	×	
General					-
Adn	ninistrators				
Description:	Built-in Adr	ministrators grou	p		
Members:					
Administr	ator 10\Domain Adm	nins			
		0		- 1 1 -	
A <u>d</u> d	Remove		o a user's group mer ective until the next t on.		
	OK	Cancel	Apply	Help	

MMC/Computer Management access

SMB access in Cloud Volumes Service provides connectivity to the Computer Management MMC, which allows you to view shares, manage share ACLs, ands view/manage SMB sessions and open files.

To use the MMC to view SMB shares and sessions in Cloud Volumes Service, the user logged in currently must be a domain administrator. Other users are allowed access to view or manage the SMB server from MMC and receive a You Do Not Have Permissions dialog box when attempting to view shares or sessions on the Cloud Volumes Service SMB instance.

To connect to the SMB server, open Computer Management, right click Computer Management and then select Connect To Another Computer. This opens the Select Computer dialog box where you can enter the SMB server name (found in the Cloud Volumes Service volume information).

When you view SMB shares with the proper permissions, you see all available shares in the Cloud Volumes Service instance that share the Active Directory connection. To control this behavior, set the Hide SMB Shares option on the Cloud Volumes Service volume instance.

🛃 Computer Management X File Action View Help 🗢 🄿 🙍 📅 🤷 📥 🚺 📷 💰 Computer Management (CVS-EAST-C2DB) Actions Share Name Folder Path Туре # Client Connections Description 👔 System Tools 1 c\$ C:\ Windows 0 Shares Task Scheduler 🕺 cvs-parisi C:\cvs-parisi Windows 1 More Actions ۲ Event Viewer 🕺 dgeyer-sm... C:\dgeyer-smb-test Windows 0 ✓ x Shared Folders 2 ipc\$ Windows 2 😥 Shares 🕫 Sessions 2 Open Files > 🛃 Local Users and Groups > 🔊 Performance 🔒 Device Manager Storage > Services and Applications >

Remember, only one Active Directory connection is allowed per region.

🕈 🔿 🙍 🗟 🖬 🚺 🛅							_
Computer Management (CVS-EAST-C2DB) System Tools System Tools System Tools Shared Folders Shares Sessions Copen Files Local Users and Groups Open Formance Device Manager Storage Storage Services and Applications	User Sparisi parisi	Computer ok-activedi ok-activedi.	# Open Files 2 3	Connected Time 01:19:15 01:01:08	Idle Tim 00:00:00 00:39:58	Actions Sessions More Actions	

The following table shows a list of supported/unsupported functionality for the MMC.

Supported functions	Unsupported functions
View shares	 Creating new local users/groups
 View active SMB sessions 	 Managing/viewing existing local user/groups
• View open files	 View events or performance logs
 View local users and groups 	Managing storage
 View local group memberships 	 Managing services and applications
 Enumerate the list of sessions, files, and tree connections in the system 	
 Close open files in the system 	
Close open sessions	
Create/manage shares	

SMB server security information

The SMB server in Cloud Volumes Service uses a series of options that define security policies for SMB connections, including things such as Kerberos clock skew, ticket age, encryption, and more.

The following table contains a list of those options, what they do, the default configurations, and if they can be modified with Cloud Volumes Service. Some options do not apply to Cloud Volumes Service.

Security option	What it does	Default value	Can change?
Maximum Kerberos Clock Skew (minutes)	Maximum time skew between Cloud Volumes Service and domain controllers. If the time skew exceeds 5 minutes, Kerberos authentication fails. This is set to the Active Directory default value.	5	No
Kerberos Ticket Lifetime (hours)	Maximum time a Kerberos ticket remains valid before requiring a renewal. If no renewal occurs before the 10 hours, you must obtain a new ticket. Cloud Volumes Service performs these renewals automatically. 10 hours is the Active Directory default value.	10	No
Maximum Kerberos Ticket Renewal (days)	Maximum number of days that a Kerberos ticket can be renewed before a new authorization request is needed. Cloud Volumes Service automatically renews tickets for SMB connections. Seven days is the Active Directory default value.	7	No
Kerberos KDC Connection Timeout (secs)	The number of seconds before a KDC connection times out.	3	No
Require Signing for Incoming SMB Traffic	Setting to require signing for SMB traffic. If set to true, clients that do not support signing fail connectivity.	False	
Require Password Complexity for Local User Accounts	Used for passwords on local SMB users. Cloud Volumes Service does not support local user creation, so this option does not apply to Cloud Volumes Service.	True	No

Security option	What it does	Default value	Can change?
Use start_tls for Active Directory LDAP Connections	Used to enable start TLS connections for Active Directory LDAP. Cloud Volumes Service does not currently support enabling this.	False	No
Is AES-128 and AES-256 Encryption for Kerberos Enabled	This controls whether AES encryption is used for Active Directory connections and is controlled with the Enable AES Encryption for Active Directory Authentication option when creating/modifying the Active Directory connection.	False	Yes
LM Compatibility Level	Level of supported authentication dialects for Active Directory connections. See the section "SMB authentication dialects" for more information.	ntlmv2-krb	No
Require SMB Encryption for Incoming CIFS Traffic	Requires SMB encryption for all shares. This is not used by Cloud Volumes Service; instead, set encryption on a per- volume basis (see the section "SMB share security features").	False	No
Client Session Security	Sets signing and/or sealing for LDAP communication. This is not currently set in Cloud Volumes Service but might be needed in future releases to address . Remediation for LDAP authentication issues due to the Windows patch is covered in the section "LDAP channel binding.".	None	No
SMB2 enable for DC connections	Uses SMB2 for DC connections. Enabled by default.	System-default	No

Security option	What it does	Default value	Can change?
LDAP Referral Chasing	When using multiple LDAP servers, referral chasing allows the client to refer to other LDAP servers in the list when an entry is not found in the first server. This is currently not supported by Cloud Volumes Service.	False	No
Use LDAPS for Secure Active Directory Connections	Enables the use of LDAP over SSL. Currently not supported by Cloud Volumes Service.	False	No
Encryption is required for DC Connection	Requires encryption for successful DC connections. Disabled by default in Cloud Volumes Service.	False	No

Dual-protocol/multiprotocol

Cloud Volumes Service offers the ability to share the same datasets to both SMB and NFS clients while maintaining proper access permissions (dual-protocol). This is done by coordinating identity mapping between protocols and using a centralized backend LDAP server to provide the UNIX identities to Cloud Volumes Service. You can use Windows Active Directory to provide both Windows and UNIX users for ease of use.

Access control

- Share access controls. Determine which clients and/or user and groups can access a NAS share. For NFS, export policies and rules control client access to exports. NFS exports are managed from the Cloud Volumes Service instance. SMB makes use of CIFS/SMB shares and share ACLs to provide more granular control at the user and group level. You can only configure share-level ACLs from SMB clients by using MMC/Computer Management with an account that has administrator rights on the Cloud Volumes Service instance (see the section "Accounts with local/BUILTIN administrator/backup rights.").
- File access controls. Control permissions at a file or folder level and are always managed from the NAS client. NFS clients can make use of traditional mode bits (rwx) or NFSv4 ACLs. SMB clients leverage NTFS permissions.

The access control for volumes that serve data to both NFS and SMB depends on the protocol in use. For information on permissions with dual protocol, see the section "Permission model."

User mapping

When a client accesses a volume, Cloud Volumes Service attempts to map the incoming user to a valid user in the opposite direction. This is necessary for proper access to be determined across protocols and to ensure that the user requesting access is indeed who they claim to be.

For example, if a Windows user named joe attempts access to a volume with UNIX permissions through SMB,

then Cloud Volumes Service performs a search to find a corresponding UNIX user named joe. If one exists, then files that are written to an SMB share as Windows user joe appears as UNIX user joe from NFS clients.

Alternately, if a UNIX user named joe attempts access to a Cloud Volumes Service volume with Windows permissions, then the UNIX user must be able to map to a valid Windows user. Otherwise, access to the volume is denied.

Currently, only Active Directory is supported for external UNIX identity management with LDAP. For more information about configuring access to this service, see Creating an AD connection.

Permission model

When using dual-protocol setups, Cloud Volumes Service makes use of security styles for volumes to determine the type of ACL. These security styles are set based on which NAS protocol is specified, or in the case of dual protocol, is a choice made at the time of Cloud Volumes Service volume creation.

- If you are only using NFS, Cloud Volumes Service volumes use UNIX permissions.
- If you are only using SMB, Cloud Volumes Service volumes use NTFS permissions.

If you are creating a dual-protocol volume, you can choose the ACL style at volume creation. This decision should be made based on the desired permissions management. If your users manage permissions from Windows/SMB clients, select NTFS. If your users prefer using NFS clients and chmod/chown, use UNIX security styles.

Considerations for creating Active Directory connections

Cloud Volumes Service provides the ability to connect your Cloud Volumes Service instance to an external Active Directory server for identity management for both SMB and UNIX users. Creating an Active Directory connection is required to use SMB in Cloud Volumes Service.

The configuration for this provides several options that require some consideration for security. The external Active Directory server can be an on-premises instance or cloud native. If you are using an on-premises Active Directory server, don't expose the domain to the external network (such as with a DMZ or an external IP address). Instead, use secure private tunnels or VPNs, one-way forest trusts, or dedicated network connections to the on-premises networks with Private Google Access. See the Google Cloud documentation for more information about best practices using Active Directory in Google Cloud.



CVS-SW requires Active Directory servers to be located in the same region. If a DC connection is attempted in CVS-SW to another region, the attempt fails. When using CVS-SW, be sure to create Active Directory sites that include the Active Directory DCs and then specify sites in Cloud Volumes Service to avoid cross-region DC connection attempts.

Active Directory credentials

When SMB or LDAP for NFS is enabled, Cloud Volumes Service interacts with the Active Directory controllers to create a machine account object to use for authentication. This is no different from how a Windows SMB client joins a domain and requires the same access rights to Organizational Units (OUs) in Active Directory.

In many cases, security groups do not allow the use of a Windows administrator account on external servers such as Cloud Volumes Service. In some cases, the Windows Administrator user is disabled entirely as a security best practice.

Permissions needed to create SMB machine accounts

To add Cloud Volumes Service machine objects to an Active Directory, an account that either has administrative rights to the domain or has delegated permissions to create and modify machine account objects to a specified OU is required. You can do this with the Delegation of Control Wizard in Active Directory by creating a custom task that provides a user access to creation/deletion of computer objects with the following access permissions provided:

- Read/Write
- Create/Delete All Child Objects
- Read/Write All Properties
- Change/Reset Password

Doing this automatically adds a security ACL for the defined user to the OU in Active Directory and minimizes the access to the Active Directory environment. After a user has been delegated, that username and password can be provided as Active Directory Credentials in this window.



The username and password that is passed to the Active Directory domain leverages Kerberos encryption during the machine account object query and creation for added security.

Active Directory connection details

The Active Directory Connection Details provide fields for administrators to give specific Active Directory schema information for machine account placement, such as the following:

- Active Directory Connection Type. Used to specify whether the Active Directory connection in a region is used for volumes of either Cloud Volumes Service or CVS-Performance service type. If this is set incorrectly on an existing connection, it might not work properly when used or edited.
- **Domain.** The Active Directory domain name.
- Site. Limits Active Directory servers to a specific site for security and performance considerations. This is necessary when multiple Active Directory servers span regions because Cloud Volumes Service does not currently support allowing Active Directory authentication requests to Active Directory servers in a different region than the Cloud Volumes Service instance. (For instance, the Active Directory domain controller is in a region that only CVS-Performance supports but you want an SMB share in a CVS-SW instance.)
- DNS servers. DNS servers to use in name lookups.
- NetBIOS name (optional). If desired, the NetBIOS name for the server. This what is used when new machine accounts are created using the Active Directory connection. For instance, if the NetBIOS name is set to CVS-EAST then the machine account names will be CVS-EAST-{1234}. See the section "How Cloud Volumes Service shows up in Active Directory" for more information.
- **Organizational Unit (OU).** The specific OU to create the computer account. This is useful if you're delegating control to a user for machine accounts to a specific OU.
- **AES Encryption.** You can also check or uncheck the Enable AES Encryption for AD Authentication checkbox. Enabling AES encryption for Active Directory authentication provides extra security for Cloud Volumes Service to Active Directory communication during user and group lookups. Before enabling this option, check with your domain administrator to confirm that the Active Directory domain controllers support AES authentication.

()

By default, most Windows servers do not disable weaker ciphers (such as DES or RC4-HMAC), but if you choose to disable weaker ciphers, confirm Cloud Volumes Service Active Directory connection has been configured to enable AES. Otherwise, authentication failures occur. Enabling AES encryption doesn't disable weaker ciphers but instead adds support for AES ciphers to the Cloud Volumes Service SMB machine account.

Kerberos realm details

This option does not apply to SMB servers. Rather, it is used when configuring NFS Kerberos for the Cloud Volumes Service system. When these details are populated, the NFS Kerberos realm is configured (similar to a krb5.conf file on Linux) and is used when NFS Kerberos is specified on the Cloud Volumes Service volume creation, as the Active Directory connection acts as the NFS Kerberos Distribution Center (KDC).



Non-Windows KDCs are currently unsupported for use with Cloud Volumes Service.

Region

A region enables you to specify the location where the Active Directory connection resides. This region must be the same region as the Cloud Volumes Service volume.

 Local NFS Users with LDAP. In this section, there is also an option to Allow Local NFS Users with LDAP. This option must be left unselected if you want to extend your UNIX user group membership support beyond the 16-group limitation of NFS (extended groups). However, using extended groups requires a configured LDAP server for UNIX identities. If you don't have an LDAP server, leave this option unselected. If you have an LDAP server and want to also use local UNIX users (such as root), select this option.

Backup users

This option enables you to specify Windows users that have backup permissions to the Cloud Volumes Service volume. Backup privileges (SeBackupPrivilege) are necessary for some applications to properly backup and restore data in NAS volumes. This user has a high level of access to data in the volume, so you should consider enabling auditing of that user access. After it is enabled, audit events display in Event Viewer > Windows Logs > Security.

🛃 Event Properties - Event 4674, S	ecurity-Auditing		×
General Details			
Friendly View <u>X</u> ML View	ew		
SubjectUserNam	le parisi		
SubjectDomain	Name CVSDEMO		
SubjectLogonId	0x31de4904		
ObjectServer	Security		
ObjectType	-		
ObjectName	±		-
Handleld	0x1174		
AccessMask	1048577		
PrivilegeList	SeBackupPrivilege		
ProcessId	0x498		
ProcessName	C:\Windows\System32\wbem\WmiPrvSE.exe	~	
Сору		<u>C</u> I	ose

Security privilege users

This option enables you to specify Windows users that have security modification permissions to the Cloud Volumes Service volume. Security privileges (SeSecurityPrivilege) are necessary for some applications (such as SQL Server) to properly set permissions during installation. This privilege is needed to manage the security log. Although this privilege is not as powerful as SeBackupPrivilege, NetApp recommends auditing user access of users with this privilege level if needed.

For more information, see Special privileges assigned to new logon.

How Cloud Volumes Service shows up in Active Directory

Cloud Volumes Service shows up in Active Directory as a normal machine account object. The naming conventions are as follows.

- CIFS/SMB and NFS Kerberos create separate machine account objects.
- NFS with LDAP enabled creates a machine account in Active Directory for Kerberos LDAP binds.
- Dual protocol volumes with LDAP share the CIFS/SMB machine account for LDAP and SMB.
- CIFS/SMB machine accounts use a naming convention of NAME-1234 (random four digit ID with hyphen appended to <10 character name) for the machine account. You can define NAME by the NetBIOS name setting on the Active Directory connection (see the section "Active Directory connection details").
- NFS Kerberos uses NFS-NAME-1234 as the naming convention (up to 15 characters). If more than 15 characters are used, the name is NFS-TRUNCATED-NAME-1234.

- NFS-only CVS-Performance instances with LDAP enabled create an SMB machine account for binding to the LDAP server with the same naming convention as CIFS/SMB instances.
- When an SMB machine account is created, default hidden admin shares (see the section "Default hidden shares") are also created (c\$, admin\$, ipc\$), but those shares have no ACLs assigned and are inaccessible.
- The machine account objects are placed in CN=Computers by default, but a you can specify a different OU when necessary. See the section "Permissions needed to create SMB machine accounts" for information about what access rights are needed to add/remove machine account objects for Cloud Volumes Service.

When Cloud Volumes Service adds the SMB machine account to Active Directory, the following fields are populated:

- cn (with the specified SMB server name)
- dNSHostName (with SMBserver.domain.com)
- msDS-SupportedEncryptionTypes (Allows DES_CBC_MD5, RC4_HMAC_MD5 if AES encryption is not enabled; if AES encryption is enabled, DES_CBC_MD5, RC4_HMAC_MD5, AES128_CTS_HMAC_SHA1_96, AES256_CTS_HMAC_SHA1_96 are allowed for Kerberos ticket exchange with the machine account for SMB)
- name (with the SMB server name)
- sAMAccountName (with SMBserver\$)
- servicePrincipalName (with host/smbserver.domain.com and host/smbserver SPNs for Kerberos)

If you want to disable weaker Kerberos encryption types (enctype) on the machine account, you can change the msDS-SupportedEncryptionTypes value on the machine account to one of the values in the following table to allow AES only.

msDS-SupportedEncryptionTypes value	Enctype enabled
2	DES_CBC_MD5
4	RC4_HMAC
8	AES128_CTS_HMAC_SHA1_96 only
16	AES256_CTS_HMAC_SHA1_96 only
24	AES128_CTS_HMAC_SHA1_96 and AES256_CTS_HMAC_SHA1_96
30	DES_CBC_MD5, RC4_HMAC, AES128_CTS_HMAC_SHA1_96 and AES256_CTS_HMAC_SHA1_96

To enable AES encryption for SMB machine accounts, click Enable AES Encryption for AD Authentication when creating the Active Directory connection.

To enable AES encryption for NFS Kerberos, see the Cloud Volumes Service documentation.

Other NAS Infrastructure service dependencies (KDC, LDAP, and DNS)

When using Cloud Volumes Service for NAS shares, there might be external dependencies required for proper functionality. These dependencies are in play under specific circumstances. The following table shows various configuration options and what,

if any, dependencies are required.

Configuration	Dependencies required
NFSv3 only	None
NFSv3 Kerberos only	Windows Active Directory: * KDC * DNS * LDAP
NFSv4.1 only	Client ID mapping configuration (/etc/idmap.conf)
NFSv4.1 Kerberos only	 Client ID mapping configuration (/etc/idmap.conf) Windows Active Directory: KDC DNS LDAP
SMB only	Active Directory: * KDC * DNS
Multiprotocol NAS (NFS and SMB)	 Client ID mapping configuration (NFSv4.1 only; /etc/idmap.conf) Windows Active Directory: KDC DNS LDAP

Kerberos keytab rotation/password resets for machine account objects

With SMB machine accounts, Cloud Volumes Service schedules periodic password resets for the SMB machine account. These password resets occur using Kerberos encryption and operate on a schedule of every fourth Sunday at a random time between 11PM and 1AM. These password resets change the Kerberos key versions, rotate the keytabs stored on the Cloud Volumes Service system, and help maintain a greater level of security for SMB servers running in Cloud Volumes Service. Machine account passwords are randomized and are not known to administrators.

For NFS Kerberos machine accounts, password resets take place only when a new keytab is created/exchanged with the KDC. Currently, this is not possible to do in Cloud Volumes Service.

Network ports for use with LDAP and Kerberos

When using LDAP and Kerberos, you should determine the network ports in use by these services. You can find a complete list of ports in use by Cloud Volumes Service in the Cloud Volumes Service documentation on security considerations.

LDAP

Cloud Volumes Service acts as an LDAP client and uses standard LDAP search queries for user and group lookups for UNIX identities. LDAP is necessary if you intend to use users and groups outside the standard default users provided by Cloud Volumes Service. LDAP is also necessary if you plan on using NFS Kerberos

with user principals (such as user1@domain.com). Currently, only LDAP using Microsoft Active Directory is supported.

To use Active Directory as a UNIX LDAP server, you must populate the necessary UNIX attributes on users and groups you intend to use for UNIX identities. Cloud Volumes Service uses a default LDAP schema template that queries attributes based on RFC-2307-bis. As a result, the following table shows the bare minimum necessary Active Directory attributes to populate for users and groups and what each attribute is used for.

For more information about setting LDAP attributes in Active Directory, see Managing dual-protocol access.

Attribute	What it does
uid*	Specifies the UNIX user name
uidNumber*	Specifies the UNIX user's numeric ID
gidNumber*	Specifies the UNIX user's primary group numeric ID
objectClass*	Specifies what type of object is being used; Cloud Volumes Service requires "user" to be included in the list of object classes (is included in most Active Directory deployments by default).
name	General information about the account (real name, phone number, and so on—also known as gecos)
unixUserPassword	No need to set this; not used in UNIX identity lookups for NAS authentication. Setting this puts the configured unixUserPassword value in plaintext.
unixHomeDirectory	Defines path to UNIX home directories when a user authenticates against LDAP from a Linux client. Set this if you want to use LDAP for UNIX home directory functionality.
loginShell	Defines path to the bash/profile shell for Linux clients when a user authenticates against LDAP.

*Denotes attribute is required for proper functionality with Cloud Volumes Service. Remaining attributes are for client-side use only.

Attribute	What it does
cn*	Specifies the UNIX group name. When using Active Directory for LDAP, this is set when the object is first created, but it can be changed later. This name cannot be the same as other objects. For instance, if your UNIX user named user1 belongs to a group named user1 on your Linux client, Windows doesn't allow two objects with the same cn attribute. To work around this, rename the Windows user to a unique name (such as user1-UNIX); LDAP in Cloud Volumes Service uses the uid attribute for UNIX user names.
gidNumber*	Specifies the UNIX group numeric ID.

Attribute	What it does
objectClass*	Specifies what type of object is being used; Cloud Volumes Service requires group to be included in the list of object classes (this attribute is included in most Active Directory deployments by default).
memberUid	Specifies which UNIX users are members of the UNIX group. With Active Directory LDAP in Cloud Volumes Service, this field is not necessary. The Cloud Volumes Service LDAP schema uses the Member field for group memberships.
Member*	Required for group memberships/secondary UNIX groups. This field is populated by adding Windows users to Windows groups. However, if the Windows groups don't have UNIX attributes populated, they are not included in the UNIX user's group membership lists. Any groups that need to be available in NFS must populate the required UNIX group attributes listed in this table.

*Denotes attribute is required for proper functionality with Cloud Volumes Service. Remaining attributes are for client-side use only.

LDAP bind information

To query users in LDAP, Cloud Volumes Service must bind (login) to the LDAP service. This login has readonly permissions and is used to query LDAP UNIX attributes for directory lookups. Currently, LDAP binds are possible only by using an SMB machine account.

You can only enable LDAP for CVS-Performance instances and use it for NFSv3, NFSv4.1, or dual-protocol volumes. An Active Directory connection must be established in the same region as the Cloud Volumes Service volume for successful deployment of the LDAP-enabled volume.

When LDAP is enabled, the following occurs in specific scenarios.

- If only NFSv3 or NFSv4.1 is used for the Cloud Volumes Service project, then a new machine account is created in the Active Directory domain controller, and the LDAP client in Cloud Volumes Service binds to Active Directory by using the machine account credentials. No SMB shares are created for the NFS volume and default hidden administrative shares (see the section "Default hidden shares") have share ACLs removed.
- If dual-protocol volumes are used for the Cloud Volumes Service project, then only the single machine account created for SMB access is used to bind the LDAP client in Cloud Volumes Service to Active Directory. No additional machine accounts are created.
- If dedicated SMB volumes are created separately (either before or after NFS volumes with LDAP are enabled), then the machine account for LDAP binds is shared with the SMB machine account.
- If NFS Kerberos is also enabled, two machine accounts are created—one for SMB shares and/or LDAP binds and one for NFS Kerberos authentication.

LDAP queries

Although LDAP binds are encrypted, LDAP queries are passed over the wire in plaintext by using the common LDAP port 389. This well-known port cannot currently be changed in Cloud Volumes Service. As a result,

someone with access to packet sniffing in the network can see user and group names, numeric IDs, and group memberships.

However, Google Cloud VMs cannot sniff other VM's unicast traffic. Only VMs actively participating in LDAP traffic (that is, being able to bind) can see traffic from the LDAP server. For more information about packet sniffing in Cloud Volumes Service, see the section "Packet sniffing/trace considerations."

LDAP client configuration defaults

When LDAP is enabled in a Cloud Volumes Service instance, an LDAP client configuration is created with specific configuration details by default. In some cases, options either do not apply to Cloud Volumes Service (not supported) or are not configurable.

LDAP client option	What it does	Default value	Can change?
LDAP Server List	Sets LDAP server names or IP addresses to use for queries. This is not used for Cloud Volumes Service. Instead, Active Directory Domain is used to define LDAP servers.	Not set	No
Active Directory Domain	Sets the Active Directory Domain to use for LDAP queries. Cloud Volumes Service leverages SRV records for LDAP in DNS to find LDAP servers in the domain.	Set to the Active Directory domain specified in the Active Directory connection.	No
Preferred Active Directory Servers	Sets the preferred Active Directory servers to use for LDAP. Not supported by Cloud Volumes Service. Instead, use Active Directory sites to control LDAP server selection.	Not set.	No
Bind using SMB Server Credentials	Binds to LDAP by using the SMB machine account. Currently, the only supported LDAP bind method in Cloud Volumes Service.	True	No
Schema Template	The schema template used for LDAP queries.	MS-AD-BIS	No
LDAP Server Port	The port number used for LDAP queries. Cloud Volumes Service currently uses only the standard LDAP port 389. LDAPS/port 636 is not currently supported.	389	No

LDAP client option	What it does	Default value	Can change?
Is LDAPS Enabled	Controls whether LDAP over Secure Sockets Layer (SSL) is used for queries and binds. Currently not supported by Cloud Volumes Service.	False	No
Query Timeout (sec)	Timeout for queries. If queries take longer than the specified value, queries fail.	3	No
Minimum Bind Authentication Level	The minimum supported bind level. Because Cloud Volumes Service uses machine accounts for LDAP binds and Active Directory does not support anonymous binds by default, this option does not come into play for security.	Anonymous	No
Bind DN	The user/distinguished name (DN) used for binds when simple bind is used. Cloud Volumes Service uses machine accounts for LDAP binds and does not currently support simple bind authentication.	Not set	No
Base DN	The base DN used for LDAP searches.	The Windows domain use for the Active Directory connection, in DN format (that is, DC=domain, DC=local).	No
Base search scope	The search scope for base DN searches. Values can include base, onelevel, or subtree. Cloud Volumes Service only supports subtree searches.	Subtree	No
User DN	Defines the DN where user searches start for LDAP queries. Currently not supported for Cloud Volumes Service, so all user searches start at the base DN.	Not set	No

LDAP client option	What it does	Default value	Can change?
User search scope	The search scope for user DN searches. Values can include base, onelevel, or subtree. Cloud Volumes Service does not support setting the user search scope.	Subtree	No
Group DN	Defines the DN where group searches start for LDAP queries. Currently not supported for Cloud Volumes Service, so all group searches start at the base DN.	Not set	No
Group search scope	The search scope for group DN searches. Values can include base, onelevel, or subtree. Cloud Volumes Service does not support setting the group search scope.	Subtree	No
Netgroup DN	Defines the DN where netgroup searches start for LDAP queries. Currently not supported for Cloud Volumes Service, so all netgroup searches start at the base DN.	Not set	No
Netgroup search scope	The search scope for netgroup DN searches. Values can include base, onelevel, or subtree. Cloud Volumes Service does not support setting the netgroup search scope.	Subtree	No
Use start_tls over LDAP	Leverages Start TLS for certificate based LDAP connections over port 389. Currently not supported by Cloud Volumes Service.	False	No
Enable netgroup-by-host lookup	Enables netgroup lookups by hostname rather than expanding netgroups to list all members. Currently not supported by Cloud Volumes Service.	False	No

LDAP client option	What it does	Default value	Can change?
Netgroup-by-host DN	Defines the DN where netgroup-by-host searches start for LDAP queries. Netgroup-by-host is currently not supported for Cloud Volumes Service.	Not set	No
Netgroup-by-host search scope	The search scope for netgroup-by-host DN searches. Values can include base, onelevel or subtree. Netgroup-by-host is currently not supported for Cloud Volumes Service.	Subtree	No
Client session security	Defines what level of session security is used by LDAP (sign, seal, or none). LDAP signing is supported by CVS- Performance, if requested by Active Directory. CVS- SW does not support LDAP signing. For both service types, sealing is currently not supported.	None	No
LDAP referral chasing	When using multiple LDAP servers, referral chasing allows the client to refer to other LDAP servers in the list when an entry is not found in the first server. This is currently not supported by Cloud Volumes Service.	False	No
Group membership filter	Provides a custom LDAP search filter to be used when looking up group membership from an LDAP server. Not currently supported with Cloud Volumes Service.	Not set	No

Using LDAP for asymmetric name mapping

Cloud Volumes Service, by default, maps Windows users and UNIX users with identical usernames bidirectionally without special configuration. As long as Cloud Volumes Service can find a valid UNIX user (with LDAP), then 1:1 name mapping occurs. For instance, if Windows user johnsmith is used, then, if Cloud Volumes Service can find a UNIX user named johnsmith in LDAP, name mapping succeeds for that user, all files/folders created by johnsmith show the correct user ownership, and all ACLs affecting johnsmith are

honored regardless of the NAS protocol in use. This is known as symmetric name mapping.

Asymmetric name mapping is when the Windows user and UNIX user identity don't match. For instance, if Windows user johnsmith has a UNIX identity of jsmith, Cloud Volumes Service needs a way to be told about the variation. Because Cloud Volumes Service currently doesn't support creation of static name mapping rules, LDAP must be used to look up the identity of the users for both Windows and UNIX identities to ensure proper ownership of files and folders and expected permissions.

By default, Cloud Volumes Service includes LDAP in the ns-switch of the instance for the name map database, so that to provide name mapping functionality by using LDAP for asymmetric names, you only need to modify some of the user/group attributes to reflect what Cloud Volumes Service looks for.

The following table shows what attributes must be populated in LDAP for asymmetric name mapping functionality. In most cases, Active Directory is already configured to do this.

Cloud Volumes Service attribute	What it does	Value used by Cloud Volumes Service for name mapping
Windows to UNIX objectClass	Specifies the type of object being used. (That is, user, group, posixAccount, and so on)	Must include user (can contain multiple other values, if desired.)
Windows to UNIX attribute	that defines the Windows username at creation. Cloud Volumes Service uses this for Windows to UNIX lookups.	No change needed here; sAMAccountName is the same as the Windows login name.
UID	Defines the UNIX username.	Desired UNIX username.

Cloud Volumes Service currently does not use domain prefixes in LDAP lookups, so multiple domain LDAP environments do not function properly with LDAP namemap lookups.

The following example shows a user with the Windows name asymmetric, the UNIX name unix-user, and the behavior it follows when writing files from both SMB and NFS.

The following figure shows how LDAP attributes look from the Windows server.

asymmetric Properties

Published (Certificates	Member Of	Passwor	d Replication	Dial-in	Object
Security	Er	vironment	Sess	ions	Remote c	ontrol
General	Address	Account	Profile	Telephones	Orga	nization
Remote	Desktop Se	ervices Profile	С	OM+	Attribute I	Editor

Attributes:

Attribute	Value	^
name	asymmetric	
objectCategory	CN=Person, CN=Schema, CN=Configuration,	
objectClass	top; person; organizationalPerson; user	
objectGUID	de489556-dd7b-43a3-98fa-2722f79d67ed	
objectSid	S-1-5-21-3552729481-4032800560-2279794	
primaryGroupID	513 = (GROUP_RID_USERS)	
pwdLastSet	1/19/2017 1:56:34 PM Eastern Standard Tim	
replPropertyMetaData	AttID Ver Loc.USN Org.DSA	
sAMAccountName	asymmetric	
sAMAccountType	805306368 = (NORMAL_USER_ACCOUN1	
uid	unix-user	
uidNumber	1207	

From an NFS client, you can query the UNIX name but not the Windows name:

```
# id unix-user
uid=1207(unix-user) gid=1220(sharedgroup) groups=1220(sharedgroup)
# id asymmetric
id: asymmetric: no such user
```

When a file is written from NFS as unix-user, the following is the result from the NFS client:

```
sh-4.2$ pwd
/mnt/home/ntfssh-4.2$ touch unix-user-file
sh-4.2$ ls -la | grep unix-user
-rwx----- 1 unix-user sharedgroup 0 Feb 28 12:37 unix-user-nfs
sh-4.2$ id
uid=1207(unix-user) gid=1220(sharedgroup) groups=1220(sharedgroup)
```

From a Windows client, you can see that the owner of the file is set to the proper Windows user:

```
PS C:\ > Get-Acl \\demo\home\ntfs\unix-user-nfs | select Owner
Owner
-----
NTAP\asymmetric
```

Conversely, files created by the Windows user asymmetric from an SMB client show the proper UNIX owner, as shown in the following text.

SMB:

PS Z:\ntfs> echo TEXT > asymmetric-user-smb.txt

NFS:

```
sh-4.2$ ls -la | grep asymmetric-user-smb.txt
-rwx----- 1 unix-user sharedgroup 14 Feb 28 12:43 asymmetric-
user-smb.txt
sh-4.2$ cat asymmetric-user-smb.txt
TEXT
```

LDAP channel binding

Because of a vulnerability with Windows Active Directory domain controllers, Microsoft Security Advisory ADV190023 changes how DCs allow LDAP binds.

The impact for Cloud Volumes Service is the same as for any LDAP client. Cloud Volumes Service does not currently support channel binding. Because Cloud Volumes Service supports LDAP signing by default through negotiation, LDAP channel binding should not be an issue. If you do have issues binding to LDAP with channel binding enabled, follow the remediation steps in ADV190023 to allow LDAP binds from Cloud Volumes Service to succeed.

DNS

Active Directory and Kerberos both have dependencies on DNS for host name to IP/IP to host name resolution. DNS requires port 53 to be open. Cloud Volumes Service does not make any modifications to DNS records, nor does it currently support the use of dynamic DNS on network interfaces.

You can configure Active Directory DNS to restrict which servers can update DNS records. For more information, see Secure Windows DNS.

Note that resources within a Google project default to using Google Cloud DNS, which isn't connected with Active Directory DNS. Clients using Cloud DNS cannot resolve UNC paths returned by Cloud Volumes Service. Windows clients joined to the Active Directory domain are configured to use Active Directory DNS and can resolve such UNC paths.

To join a client to Active Directory, you must configure its DNS configuration to use Active Directory DNS.

Optionally, you can configure Cloud DNS to forward requests to Active Directory DNS. See Why can't my client resolve the SMB NetBIOS name? for more information.



Cloud Volumes Service does not currently support DNSSEC and DNS queries are performed in plaintext.

File access auditing

Currently not supported for Cloud Volumes Service.

Antivirus protection

You must perform antivirus scanning in Cloud Volumes Service at the client to a NAS share. There is currently no native antivirus integration with Cloud Volumes Service.

Service operation

The Cloud Volumes Service team manages the backend services in Google Cloud and uses multiple strategies to secure the platform and prevent unwanted access.

Each customer gets their own unique subnet that has access fenced off from other customers by default, and every tenant in Cloud Volumes Service gets their own namespace and VLAN for total data isolation. After a user is authenticated, the Service Delivery Engine (SDE) can only read configuration data specific to that tenant.

Physical security

With proper preapproval, only onsite engineers and NetApp-badged Field Support Engineers (FSEs) have access to the cage and racks for physical work. Storage and network management is not permitted. Only these onsite resources are able to perform hardware maintenance tasks.

For onsite engineers, a ticket is raised for the statement of work (SOW) that includes the rack ID and device location (RU) and all other details are included in the ticket. For NetApp FSEs, a site visitation ticket must be raised with the COLO and the ticket includes the visitor's details, date, and time for auditing purposes. The SOW for the FSE is communicated internally to NetApp.

Operations team

The operations team for Cloud Volumes Service consists of Production Engineering and a Site Reliability Engineer (SRE) for Cloud Volume Services and NetApp Field Support Engineers and Partners for hardware. All operations team members are accredited for work in Google Cloud and detailed records of work are maintained for every ticket raised. In addition, there is a stringent change control and approval process in place to ensure each decision is appropriately scrutinized.

The SRE team manages the control plane and how the data is routed from UI requests to backend hardware and software in Cloud Volumes Service. The SRE team also manages system resources, such as volume and inode maximums. SREs are not allowed to interact with or have access to customer data. SREs also provide coordination with Return Material Authorizations (RMAs), such as new disk or memory replacement requests for the backend hardware.

Customer responsibilities

Customers of Cloud Volumes Service manage their organization's Active Directory and user role management as well as the volume and data operations. Customers can have administrative roles and can delegate permissions to other end users within the same Google Cloud project using the two predefined roles that NetApp and Google Cloud provide (Administrator and Viewer).

The administrator can peer any VPC within the customer project to Cloud Volumes Service that the customer determines to be appropriate. It is the responsibility of the customer to manage access to their Google Cloud marketplace subscription and to manage the VPCs that have access to the data plane.

Malicious SRE protection

One concern that could arise is how does Cloud Volumes Service protect against scenarios in which there is a malicious SRE or when SRE credentials have been compromised?

Access to the production environment is with a limited number of SRE individuals only. Administrative privileges are further restricted to a handful of experienced administrators. All actions performed by anyone in the Cloud Volumes Service production environment are logged and any anomalies to the baseline or suspicious activities are detected by our security information and event management (SIEM) threat intelligence platform. As a result, malicious actions can be tracked and mitigated before too much damage is done to the Cloud Volumes Service backend.

Volume life cycle

Cloud Volumes Service manages only the objects within the service—not the data within the volumes. Only clients accessing the volumes can manage the data, the ACLs, file owners, and so on. The data in these volumes is encrypted at rest and access is limited to tenants of the Cloud Volumes Service instance.

The volume lifecycle for Cloud Volumes Service is create-update-delete. Volumes retain Snapshot copies of volumes until the volumes are deleted, and only validated Cloud Volumes Service administrators can delete volumes in Cloud Volumes Service. When a volume deletion is requested by an administrator, an additional step of entering the volume name is required to verify the deletion. After a volume is deleted, the volume is gone and cannot be recovered.

In cases where a Cloud Volumes Service contract is terminated, NetApp marks volumes for deletion after a specific time period. Before that time period expires, you can recover volumes at the customer's request.

Certifications

Cloud Volumes Services for Google Cloud is currently certified to ISO/IEC 27001:2013 and ISO/IEC 27018:2019 standards. The service also recently received its SOC2 Type I attestation report. For information about the NetApp commitment to data security and privacy, see Compliance: Data security and data privacy.

GDPR

Our commitments to privacy and compliance with GDPR are available in a number of our customer contracts, such as our Customer Data Processing Addendum, which includes the Standard Contractual Clauses provided by the European Commission. We also make these commitments in our Privacy Policy, backed by the core values set out in our corporate Code of Conduct.

Additional information and contact information

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

· Google Cloud documentation for Cloud Volumes Service

https://cloud.google.com/architecture/partners/netapp-cloud-volumes/

· Google private service access

https://cloud.google.com/vpc/docs/private-services-access?hl=en_US

NetApp product documentation

https://www.netapp.com/support-and-training/documentation/

Cryptographic Validation Module Program—NetApp CryptoMod

https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/4144

• The NetApp Solution for Ransomware

https://www.netapp.com/pdf.html?item=/media/16716-sb-3938pdf.pdf&v=202093745

• TR-4616: NFS Kerberos in ONTAP

https://www.netapp.com/pdf.html?item=/media/19384-tr-4616.pdf

Contact us

Let us know how we can improve this technical report.

Contact us at doccomments@netapp.com. Include TECHNICAL REPORT 4918 in the subject line.

BlueXP Disaster Recovery

3-2-1 Data Protection for VMware with SnapCenter Plug-in and BlueXP backup and recovery for VMs

The 3-2-1 backup strategy is an industry accepted data protection method, providing a comprehensive approach to safeguarding valuable data. This strategy is reliable and ensures that even if some unexpected disaster strikes, there will still be a copy of the data available.

Author: Josh Powell - NetApp Solutions Engineering

Overview

The strategy is comprised of three fundamental rules:

- 1. Keep at least three copies of your data. This ensures that even if one copy is lost or corrupted, you still have at least two remaining copies to fall back on.
- 2. Store two backup copies on different storage media or devices. Diversifying storage media helps protect against device-specific or media-specific failures. If one device gets damaged or one type of media fails, the other backup copy remains unaffected.
- 3. Finally, ensure that at least one backup copy is offsite. Offsite storage serves as a fail-safe against localized disasters like fires or floods that could render onsite copies unusable.

This solution document covers a 3-2-1 backups solution using SnapCenter Plug-in for VMware vSphere (SCV) to create primary and secondary backups of our on-premises virtual machines and BlueXP backup and

recovery for virtual machines to backup a copy of our data to cloud storage or StorageGRID.

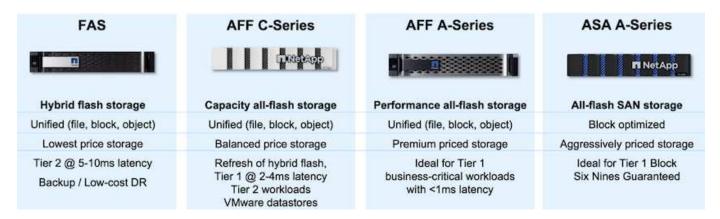
Use Cases

This solution addresses the following use cases:

- Backup and restore of on-premises virtual machines and datastores using using SnapCenter Plug-in for VMware vSphere.
- Backup and restore of on-premises virtual machines and datastores, hosted on ONTAP clusters, and backed up to object storage using BlueXP backup and recovery for virtual machines.

NetApp ONTAP Data Storage

ONTAP is NetApp's industry leading storage solution that offers unified storage whether you access over SAN or NAS protocols. The 3-2-1 backup strategy ensures on-premises data is protected on more than one media type and NetApp offers platforms ranging from high-speed flash to lower-cost media.



For more information on all of NetApp's hardware platform's check out NetApp Data Storage.

SnapCenter Plug-in for VMware vSphere

The SnapCenter Plugin for VMware vSphere is a data protection offering which is tightly integrated with VMware vSphere and allows easy management of backup and restores for virtual machines. As part of that solution, SnapMirror provides a fast and reliable method to create a second immutable backup copy of virtual machine data on a secondary ONTAP storage cluster. With this architecture in place, virtual machine restore operations can easily be initiated from either the primary or secondary backup locations.

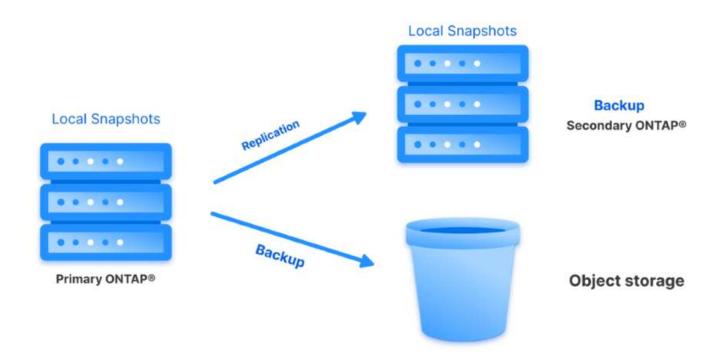
SCV is deployed as a linux virtual appliance using an OVA file. The plug-in now uses a remote plug-in architecture. The remote plug-in runs outside of the vCenter server and is hosted on the SCV virtual appliance.

For detailed information on SCV refer to SnapCenter Plug-in for VMware vSphere documentation.

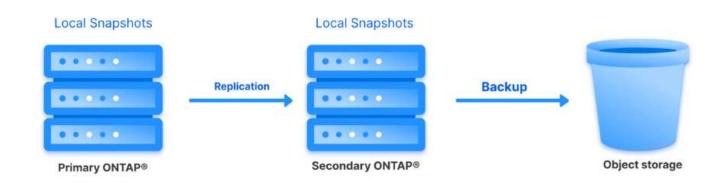
BlueXP backup and recovery for virtual machines

BlueXP backup and recovery is a cloud based tool for data management that provides a single control plane for a wide range of backup and recovery operations across both on-premises and cloud environments. Part of the NetApp BlueXP backup and recovery suite is a feature that integrates with the SnapCenter Plugin for VMware vSphere (on-premises) to extend a copy of the data to object storage in the cloud. This establishes a third copy of the data offsite that is sourced from the primary or secondary storage backups. BlueXP backup and recovery makes it easy to set up storage policies that transfer copies of your data from either of these two on-prem locations. Choosing between the primary and secondary backups as the source in BlueXP Backup and Recovery will result in one of two topologies being implemented:

Fan-out Topology – When a backup is initiated by the SnapCenter Plug-in for VMware vSphere, a local snapshot is immediately taken. SCV then initiates a SnapMirror operation that replicates the most recent snapshot to the Secondary ONTAP cluster. In BlueXP Backup and Recovery, a policy specifies the primary ONTAP cluster as the source for a snapshot copy of the data to be transferred to object storage in your cloud provider of choice.



Cascading Topology – Creating the primary and secondary data copies using SCV is identical to the fan-out topology mentioned above. However, this time a policy is created in BlueXP Backup and Recovery specifying that the backup to object storage will originate from the secondary ONTAP cluster.



BlueXP backup and recovery can create backup copies of on-premises ONTAP snapshots to AWS Glacier, Azure Blob, and GCP Archive storage.







AWS Glacier Azure GCP and Deep Glacier Blob Archive Archive Storage

In addition, you can use NetApp StorageGRID as the object storage backup target. For more on StorageGRID refer to the StorageGRID landing page.

Solution Deployment Overview

This list provides the high level steps necessary to configure this solution and execute backup and restore operations from SCV and BlueXP backup and recovery:

- 1. Configure SnapMirror relationship between the ONTAP clusters to be used for primary and secondary data copies.
- 2. Configure SnapCenter Plug-In for VMware vSphere.
 - a. Add Storage Systems
 - b. Create backup policies
 - c. Create resource groups
 - d. Run backup first backup jobs
- 3. Configure BlueXP backup and recovery for virtual machines
 - a. Add working environment
 - b. Discover SCV and vCenter appliances
 - c. Create backup policies
 - d. Activate backups
- 4. Restore virtual machines from primary and secondary storage using SCV.
- 5. Restore virtual machines from object storage using BlueXP backup and restore.

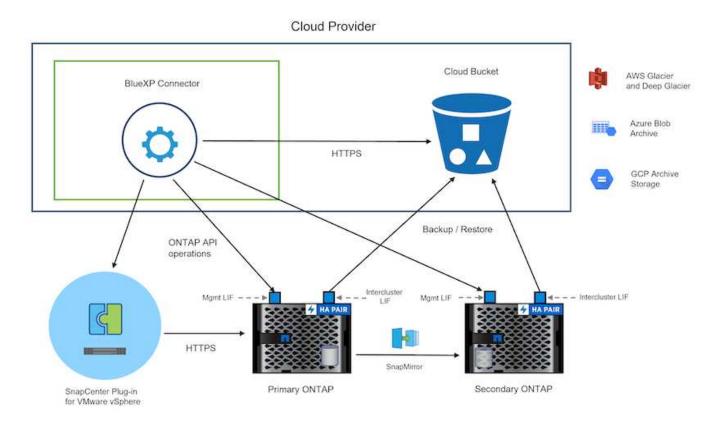
Prerequisites

The purpose of this solution is to demonstrate data protection of virtual machines running in VMware vSphere and located on NFS Datastores hosted by NetApp ONTAP. This solution assumes the following components are configured and ready for use:

- 1. ONTAP storage cluster with NFS or VMFS datastores connected to VMware vSphere. Both NFS and VMFS datastores are supported. NFS datastores were utilized for this solution.
- 2. Secondary ONTAP storage cluster with SnapMirror relationships established for volumes used for NFS datastores.
- 3. BlueXP connector installed for cloud provider used for object storage backups.
- 4. Virtual machines to be backed are on NFS datastores residing on the primary ONTAP storage cluster.
- 5. Network connectivity between the BlueXP connector and on-premises ONTAP storage cluster management interfaces.
- 6. Network connectivity between the BlueXP connector and on-premises SCV appliance VM and between the BlueXP connecter and vCenter.
- 7. Network connectivity between the on-premises ONTAP intercluster LIFs and the object storage service.
- 8. DNS configured for management SVM on primary and secondary ONTAP storage clusters. For more information refer to Configure DNS for host-name resolution.

High Level Architecture

The testing / validation of this solution was performed in a lab that may or may not match the final deployment environment.



460

Solution Deployment

In this solution, we provide detailed instructions for deploying and validating a solution that utilizes SnapCenter Plug-in for VMware vSphere, along with BlueXP backup and recovery, to perform the backup and recovery of Windows and Linux virtual machines within a VMware vSphere cluster located in an on-premises data center. The virtual machines in this setup are stored on NFS datastores hosted by an ONTAP A300 storage cluster. Additionally, a separate ONTAP A300 storage cluster serves as a secondary destination for volumes replicated using SnapMirror. Furthermore, object storage hosted on Amazon Web Services and Azure Blob were employed as targets for a third copy of the data.

We will go over creating SnapMirror relationships for secondary copies of our backups managed by SCV and configuration of backup jobs in both SCV and BlueXP backup and recovery.

For detailed information on SnapCenter Plug-in for VMware vSphere refer to the SnapCenter Plug-in for VMware vSphere documentation.

For detailed information on BlueXP backup and recovery refer to the BlueXP backup and recovery documentation.

Establish SnapMirror relationships between ONTAP Clusters

SnapCenter Plug-in for VMware vSphere uses ONTAP SnapMirror technology to manage the transport of secondary SnapMirror and/or SnapVault copies to a secondary ONTAP Cluster.

SCV backup policies have the option of using SnapMirror or SnapVault relationships. The primary difference is that when using the SnapMirror option, the retention schedule configured for backups in the policy will be the same at the primary and secondary locations. SnapVault is designed for archiving and when using this option a separate retention schedule can be established with the SnapMirror relationship for the snapshot copies on the secondary ONTAP storage cluster.

Setting up SnapMirror relationships can be done in BlueXP where many of the steps are automated, or it can be done using System Manager and the ONTAP CLI. All of these methods are discussed below.

Establish SnapMirror relationships with BlueXP

The following steps must be completed from the BlueXP web console:

Begin by logging into the BlueXP web console and navigating to the Canvas.

1. Drag and drop the source (primary) ONTAP storage system onto the destination (secondary) ONTAP storage system.

My working environments	My estate	
iment		
	ntaphd-a300e9u25 On-Premises ONTAP	
	NTAPSelect 173.74TIB On-Premises ONTAP Capacity	
	Capacity Ots-demo On-Premises ONTAP	
\sim	3 TIB Capacity	
E13A300 On-Premises ONTAP 75.21TiB		
Capacity		HA

2. From the menu that appears select **Replication**.



3. On the **Destination Peering Setup** page select the destination Intercluster LIFs to be used for the connection between storage systems.

Replication Setup		Destination	Peering Setup		
CVO_InterCluster_B	Replication requires	s an initial connection between the two v	uld like to use for cluster peering setup rorking environments which is called a clu tons, see Cloud Manager documentation. coneb-n2 pro	intercluster_node_1 intercl	intercluster_node_2 production (1) and (2) and (3) a
a0a-3510 172.21.254.212/24 up	a0a-3510 172.21.254.211/24 up	a0a-3484 172.21.228.21/24 up	a0a-3484 172.21.228.22/24 up	10.61.181.193/24 up	10.61.181.194/24 up

4. On the **Destination Volume Name** page, first select the source volume and then fill out the destination volume name and select the destination SVM and aggregate. Click on **Next** to continue.

E13A300		Select the volume that	you want to replicate
mes			
CDM01	Conline	Data	CONLINE
NFO Storage VM Name F502 Hering Policy None Volume Type RW	CAPACHY 206 GB Allocated Disk Used	INFO Storage VM Name PS02 Thering Policy None Volume Type RW	CAPACITY 512 GB Alliscated
Demo		Demo02_01	CNLINE
IFO Itorage VM Name zonea Iterling Policy None Italume Type RW	1.79 GB 250 GB Allocated	tHFO Storage VM Name Demo Tiering Policy None Volume Type RW	500 GB Allocated

Destination Volume Name

Destination Volume Name

Demo_copy

Destination Storage VM

EHC_NFS

Destination Aggregate

EHCAggr01

5. Choose the max transfer rate for replication to occur at.

	***	r rate. An unlimited rate	might
You should limi negatively impa			1000
	act the perfo	mance of other applica	1000

6. Choose the policy that will determine the retention schedule for secondary backups. This policy can be created beforehand (see the manual process below in the **Create a snapshot retention policy** step) or can be changed after the fact if desired.

• Previou	s Step	Default Policies Additional Policies	
	CloudBackupService-1674046623282	CloudBackupService-1674047424679	CloudBackupService-1674047718637
	Original Policy Name: CloudBackupService-1674046623282	Custom Policy - No Comment	Custom Policy - No Comment
	Creates a SnapVault relationship which replicates Snapshot copies with the following labels to the destination volume: hourly (12), adaly (15), weekly (4) (# of retained Snapshot copies in parenthesis)		colorin to sy the comment
		More info	More info

Replication Setup	Review & Approve						
↑ Previous Step			Review your selection and start	the replication process			
	Source	Destination	Source Volume Allocated Size:	250 GB	Destination Aggregate:	EHCAggr01	
			Source Volume Used Size:	1.79 GB	Destination Storage VM:	EHC_NFS	
	E13A300	ntaphci-a300e9u25	Source Thin Provisioning:	Yes	Max Transfer Rate:	100 MB/s	
	2	→ 🛢	Destination Volume Allocated Siz	e: 250 GB	SnapMirror Policy:	Mirror	
		→ U	Destination Thin Provisioning:	No	Replication Schedule:	One-time copy	
	Demo	Demo_copy					

Establish SnapMirror relationships with System Manager and ONTAP CLI

All required steps for establishing SnapMirror relationships can be accomplished with System Manager or the ONTAP CLI. The following section provides detailed information for both methods:

Record the source and destination Intercluster logical interfaces

For the source and destination ONTAP clusters, you can retrieve the inter-cluster LIF information from System Manager or from the CLI.

1. In ONTAP System Manager, navigate to the Network Overview page and retrieve the IP addresses of Type: Intercluster that are configured to communicate with the AWS VPC where FSx is installed.

Buckets											
Qtrees											
Quotes	Network Interfaces	Portsets									
Storage VMs	+ Add								Q Search 🔮 Do	ownload	
Tiers	- A00								Sealor ₹ 00	WINDED - PIDER SOOW / H	100 4
NETWORK	Name	Status	Storage VM	IPspace	Address 🤤	Current Node	Current Port	Portset	Protocols	Туре	Th
Overview	veeam_repo	0	Backup	Default	10.61.181.179	E13A300_1	a0a-181		SMB/CIPS, NFS, S3	Data	
Ethernet Ports	CM01	0		Default	10.61.181.180	E13A300_1	202-101			Cluster/Node Mgmt	
FC Ports		5.									1
EVENTS & JOBS	HC_N3	0		Default	10.61.181.183	E13A300_1	a0a-181			Intercluster,Cluster/Node Mgmt	
PROTECTION V	HC_N2	0		Default	10.61.181.184	E13A300_2	181-60c			Intercluster, Cluster/Node Mgmt	
Sectors Contraction	lif_ora_svm_614	٢	073_9970	Default	10.61.181.185	E13A300_1	a0a-181		SMB/CIFS, NFS, FL	Duta	

2. To retrieve the Intercluster IP addresses using the CLI run the following command:

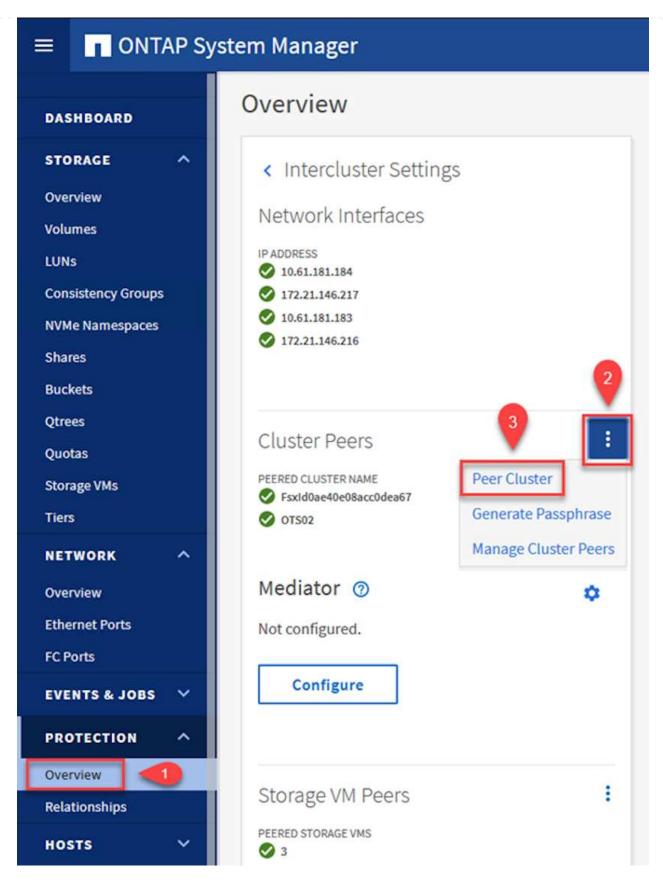
```
ONTAP-Dest::> network interface show -role intercluster
```

To establish cluster peering between ONTAP clusters, a unique passphrase entered at the initiating ONTAP cluster must be confirmed in the other peer cluster.

1. Set up peering on the destination ONTAP cluster using the cluster peer create command. When prompted, enter a unique passphrase that is used later on the source cluster to finalize the creation process.

```
ONTAP-Dest::> cluster peer create -address-family ipv4 -peer-addrs
source_intercluster_1, source_intercluster_2
Enter the passphrase:
Confirm the passphrase:
```

2. At the source cluster, you can establish the cluster peer relationship using either ONTAP System Manager or the CLI. From ONTAP System Manager, navigate to Protection > Overview and select Peer Cluster.



- 3. In the Peer Cluster dialog box, fill out the required information:
 - a. Enter the passphrase that was used to establish the peer cluster relationship on the destination ONTAP cluster.

- b. Select Yes to establish an encrypted relationship.
- c. Enter the intercluster LIF IP address(es) of the destination ONTAP cluster.
- d. Click Initiate Cluster Peering to finalize the process.

Peer Cluster

Local		Remo
STORAGE VM PERMISSIONS		PASSPHRASE 1
All storage VMs (incl ×		
Storage VMs created in the future also will be gi permissions.	ven 2	It cannot be determined from the passphrase whether this relationship was encrypted. Is the relationship encrypted?
		To generate passphrase, Launch Remote Cluster
		Intercluster Network Interfaces IP Addresses
		172.30.15.42
		172.30.14.28
		Cancel
4		+ Add
•		

4. Verify the status of the cluster peer relationship from the destination ONTAP cluster with the following command:

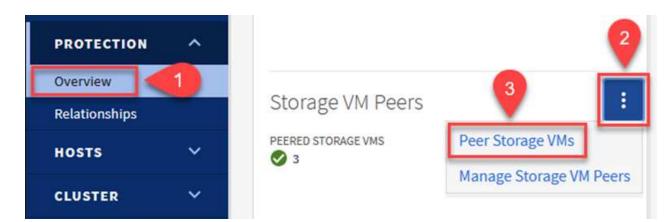


The next step is to set up an SVM relationship between the destination and source storage virtual machines that contain the volumes that will be in SnapMirror relationships.

1. From the destination ONTAP cluster, use the following command from the CLI to create the SVM peer relationship:

```
ONTAP-Dest::> vserver peer create -vserver DestSVM -peer-vserver
Backup -peer-cluster OnPremSourceSVM -applications snapmirror
```

- 2. From the source ONTAP cluster, accept the peering relationship with either ONTAP System Manager or the CLI.
- 3. From ONTAP System Manager, go to Protection > Overview and select Peer Storage VMs under Storage VM Peers.



- 4. In the Peer Storage VM's dialog box, fill out the required fields:
 - The source storage VM
 - The destination cluster
 - The destination storage VM



5. Click Peer Storage VMs to complete the SVM peering process.

SnapCenter manages retention schedules for backups that exist as snapshot copies on the primary storage system. This is established when creating a policy in SnapCenter. SnapCenter does not manage retention policies for backups that are retained on secondary storage systems. These policies are managed separately through a SnapMirror policy created on the secondary FSx cluster and associated with the destination volumes that are in a SnapMirror relationship with the source volume.

When creating a SnapCenter policy, you have the option to specify a secondary policy label that is added to the SnapMirror label of each snapshot generated when a SnapCenter backup is taken.



On the secondary storage, these labels are matched to policy rules associated with the destination volume for the purpose of enforcing retention of snapshots.

The following example shows a SnapMirror label that is present on all snapshots generated as part of a policy used for daily backups of our SQL Server database and log volumes.

Select secondary replication options ()

Update SnapMirror after creating a local Snapshot copy.

✓ Update SnapVault after creating a local Snapshot copy.

Secondary policy label	Custom Label -	0
	sql-daily	
Error retry count	3 🗘 🚯	

For more information on creating SnapCenter policies for a SQL Server database, see the SnapCenter documentation.

You must first create a SnapMirror policy with rules that dictate the number of snapshot copies to retain.

1. Create the SnapMirror Policy on the FSx cluster.

ONTAP-Dest::> snapmirror policy create -vserver DestSVM -policy PolicyName -type mirror-vault -restart always

2. Add rules to the policy with SnapMirror labels that match the secondary policy labels specified in the SnapCenter policies.

```
ONTAP-Dest::> snapmirror policy add-rule -vserver DestSVM -policy
PolicyName -snapmirror-label SnapMirrorLabelName -keep
#ofSnapshotsToRetain
```

The following script provides an example of a rule that could be added to a policy:

```
ONTAP-Dest::> snapmirror policy add-rule -vserver sql_svm_dest
-policy Async_SnapCenter_SQL -snapmirror-label sql-ondemand -keep 15
```



Create additional rules for each SnapMirror label and the number of snapshots to be retained (retention period).

Create destination volumes

To create a destination volume on ONTAP that will be the recipient of snapshot copies from our source volumes, run the following command on the destination ONTAP cluster:

```
ONTAP-Dest::> volume create -vserver DestSVM -volume DestVolName
-aggregate DestAggrName -size VolSize -type DP
```

Create the SnapMirror relationships between source and destination volumes

To create a SnapMirror relationship between a source and destination volume, run the following command on the destination ONTAP cluster:

```
ONTAP-Dest::> snapmirror create -source-path
OnPremSourceSVM:OnPremSourceVol -destination-path DestSVM:DestVol -type
XDP -policy PolicyName
```

Initialize the SnapMirror relationships

Initialize the SnapMirror relationship. This process initiates a new snapshot generated from the source volume and copies it to the destination volume.

To create a volume, run the following command on the destination ONTAP cluster:

ONTAP-Dest::> snapmirror initialize -destination-path DestSVM:DestVol

Configure the SnapCenter Plug-in for VMware vSphere

Once installed, the SnapCenter Plug-in for VMware vSphere can be accessed from the vCenter Server Appliance Management interface. SCV will manage backups for the NFS datastores mounted to the ESXi hosts and that contain the Windows and Linux VMs.

Review the Data protection workflow section of the SCV documentation for more information on the steps involved in configuring backups.

To configure backups of your virtual machines and datastores the following steps will need to be completed

from the plug-in interface.

Discover the ONTAP storage clusters to be used for both primary and secondary backups.

1. In the SnapCenter Plug-in for VMware vSphere navigate to **Storage Systems** in the left-hand menu and click on the **Add** button.

SnapCenter Plug-in for VMware vSphere INSTANCE 10.61.181.201:8080 ~

🔄 Dashboard	Storage Systems			
🝺 Settings	🛖 Add 🥒 Edit	🗙 Delete 🛛 🔂 Export		
🔃 Resource Groups	Name	Display Name		
🔏 Policies	E 10.61.181.180	E13A300		
Storage Systems	Anthos	Anthos		
100	Backup	Backup		
👩 Guest File Restore	Demo	Demo		
>>	172.21.146.131	FS02		
"	470 04440 466	070 0100		

2. Fill out the credentials and platform type for the primary ONTAP storage system and click on Add.

Add	Storage	System
-----	---------	--------

Platform	All Flash FAS	
Authentication Method	 Credentials 	O Certificate
Username	admin	
Password	•••••	
Protocol	HTTPS	
Port	443	
Timeout	60	Seconds
Preferred IP	Preferred IP	
Event Management Syste	em(EMS) & AutoSupport Settin	g
Log Snapcenter server	events to syslog	
	fication for failed operation to si	torage system

Policies specify the retention period, frequency and replication options for the backups managed by SCV.

Review the Create backup policies for VMs and datastores section of the documentation for more information.

To create backup policies complete the following steps:

1. In the SnapCenter Plug-in for VMware vSphere navigate to **Policies** in the left-hand menu and click on the **Create** button.

SnapCenter Plug-in for VMware vSphere INSTANCE 10.61.181.201:8080 v

🔄 Dashboard	Policies	
😰 Settings	🕂 Create 🥒 Edit 🗙 Remov	ve 🏳 Export
🔃 Resource Groups	<i>▲Name</i>	VM Co
Policies	Daily	No
Storage Systems	FCD	No
	Hourly	No
🔯 Guest File Restore	Monthly	No
	Or Demonstra	N1-

2. Specify a name for the policy, retention period, frequency and replication options, and snapshot label.

New Backup Policy

Name	Daily
Description	description
Retention	Days to keep 🔹 30 🖕 🕫
Frequency	Daily
Replication	🗌 Update SnapMirror after backup 🕧
	🗹 Update SnapVault after backup 🕧
	Snapshot label Daily
Advanced \vee	VM consistency ()
	 Include datastores with independent disks
	Scripts 🕦
	Enter script path

When creating a policy in the SnapCenter Plug-in you will see options for SnapMirror and SnapVault. If you choose SnapMirror, the retention schedule specified in the policy will be the same for both the primary and secondary snapshots. If you choose SnapVault, the retention schedule for the secondary snapshot will be based on a separate schedule implemented with the SnapMirror relationship. This is useful when you wish longer retention periods for secondary backups.

()

(;)

Snapshot labels are useful in that they can be used to enact policies with a specific retention period for the SnapVault copies replicated to the secondary ONTAP cluster. When SCV is used with BlueXP Backup and Restore, the Snapshot label field must either be blank or <u>match</u> the label specified in the BlueXP backup policy.

3. Repeat the procedure for each policy required. For example, separate policies for daily, weekly, and monthly backups.

Resource groups contain the datastores and virtual machines to be included in a backup job, along with the associated policy and backup schedule.

Review the Create resource groups section of the documentation for more information.

To create resource groups complete the following steps.

1. In the SnapCenter Plug-in for VMware vSphere navigate to **Resource Groups** in the left-hand menu and click on the **Create** button.

💁 Dashboard	Resource Groups	
👩 Settings	Create / Edit X Delete	Run Now
Resource Groups	Name	Des
8 Policies	SMBC	
Storage Systems	Oracle_Servers	
Curat File Destant	Demo	
👩 Guest File Restore	SQL_Servers_Weekly	

- 2. In the Create Resource Group wizard, enter a name and description for the group, as well as information required to receive notifications. Click on **Next**
- 3. On the next page select the datastores and virtual machines that wish to be included in the backup job and then click on **Next**.

Create Resource Group

 1. General info & notification 	Scope:	Datastores ~	•		
2. Resource	Datacenter:	Datastores			
3. Spanning disks	Datacemen	Virtual Machines			
4. Policies		Tags	ntity name		
5. Schedules	Available entiti	Folders			Selected entities
6. Summary	🗐 Demo				INFS_SCV
	🗐 DemoD	S			SVERT
	📒 destinat	ion			
	🗐 esxi7-ho	-01 Local			
	🗐 esxi7-ho	-02 Local		>	
	a esxi7-ho	-03 Local		<	
	-			«	

You have the option to select specific VMs or entire datastores. Regardless of which you choose, the entire volume (and datastore) is backed up since the backup is the result of taking a snapshot of the underlying volume. In most cases, it is easiest to choose the entire datastore. However, if you wish to limit the list of available VMs when restoring, you can choose only a subset of VMs for backup.

4. Choose options for spanning datastores for VMs with VMDKs that reside on multiple datastores and then click on **Next**.

Create Resource Group 1. General info & notification 2. Resource 3. Spanning disks 4. Policies 5. Schedules 6. Summary Manually select the spanning datastores to be included in this backup You will need to modify the list every time new VMs are added There are no spanned entities in the selected virtual entities list.



BlueXP backup and recovery does not currently support backing up VMs with VMDKs that span multiple datastores.

5. On the next page select the policies that will be associated with the resource group and click on **Next**.

1. General info & notification	+ Cre	ate			
2. Resource		Name	VM Consistent	Include independent di	Schedule
 3. Spanning disks 		Daily	No	No	Daily
4. Policies		FCD	No	Yes	On Demand Only
5. Schedules		Monthly	No	No	Monthly



When backing up SCV managed snapshots to object storage using BlueXP backup and recovery, each resource group can only be associated with a single policy.

6. Select a schedule that will determine at what times the backups will run. Click on **Next**.

Create Resource Grou	qu			
 1. General info & notification 				
 2. Resource 	Daily	•	Туре	Daily
 3. Spanning disks 			Every	1 Day(s)
 4. Policies 			Starting	06/23/2023
 Schedules 				
 6. Summary 			At	07 🗘 00 🌩 PM

7. Finally, review the summary page and then on **Finish** to complete the resource group creation.

Run a backup job

In this final step, run a backup job and monitor its progress. At least one backup job must be successfully completed in SCV before resources can be discovered from BlueXP backup and recovery.

- 1. In the SnapCenter Plug-in for VMware vSphere navigate to **Resource Groups** in the left-hand menu.
- 2. To initiate a backup job, select the desired resource group and click the **Run Now** button.

SnapCenter Plug-in for VMware vSphere INSTANCE 10.61.181.201:8080 ~

Dashboard	Resource Groups		
🔁 Settings	🕂 Create 🥒 Edit 🗙 Delete	🔘 Run N	Now 🔘 Suspend
Resource Groups	Name		Description
🥞 Policies	Win01		
Storage Systems	SMBC		
🔂 Guest File Restore	Oracle_Servers		
Ouest the Restore	Demo		
>	SQL_Servers_Dally		
	SQL_Servers_Weekly		

3. To monitor the backup job, navigate to **Dashboard** on the left hand menu. Under **Recent Job Activities** click on the Job ID number to monitor the job progress.

Job Details : 2614	Ċ ×
Validate Retention Settings	
Quiescing Applications	
🤣 Retrieving Metadata	
Creating Snapshot copy	
Onquiescing Applications	
Registering Backup	
Ø Backup Retention	
🤣 Clean Backup Cache	
🤣 Send EMS Messages	
(Job 2616)SnapVault Update	
Running, Start Time: 07/31/2023 07:24:40 PM.	~
	CLOSE DOWNLOAD JOB LOGS

Configure Backups to Object Storage in BlueXP backup and recovery

For BlueXP to manage the data infrastructure effectively, it requires the prior installation of a Connector. The Connector executes the actions involved in discovering resources and managing data operations.

For more information on the BlueXP Connector refer to Learn about Connectors in the BlueXP documentation.

Once the connector is installed for the cloud provider being utilized, a graphic representation of the object storage will be viewable from the Canvas.

To configure BlueXP backup and recovery to backup data managed by SCV on-premises, complete the following steps:

The first step is to add the on-premises ONTAP storage systems to BlueXP

1. From the Canvas select Add Working Environment to begin.

	n Ne	etAp	P BlueXP				
	-	(🛆 Canva	s My	/ working enviro	onments	
2.	U U Select On-	Premi				ne Discover button.	
			Microsoft Azure	aws Amazon Web Services	Google Cloud Platform	On-Premises	
		On-Premis	ses ONTAP			Discover	

3. Fill out the credentials for the ONTAP storage system and click the **Discover** button to add the working environment.

10.61.181.180		
User Name		
admin		
Password		
•••••	\odot	

To discover the on-premises datastore and virtual machine resources, add info for the SCV data broker and credentials for the vCenter management appliance.

1. From the BlueXP left-hand menu selection **Protection > Backup and recovery > Virtual Machines**

•	NetApp BlueXP		
8	Storage	•	ironment
ø	Health	•	
V	Protection	•	
	Backup and recovery	☆	Volumes Restore
	Disaster recovery (Beta)	☆	Applications
	Replication	☆	Virtual Machines
6	Governance	•	Kubernetes
0	Mobility	•	Job Monitoring
0 ⁰ 0	Extensions	•	Reports

2. From the Virtual Machines main screen access the **Settings** drop down menu and select **SnapCenter Plug-in for VMware vSphere**.

Settings ▼
SnapCenter Plug-in for VMware vSphere
Policies
Folicies

 Click on the **Register** button and then enter the IP address and port number for the SnapCenter Plugin appliance and the username and password for the vCenter management appliance. Click on the **Register** button to begin the discovery process.

	lug-in for VMware vSphere
SnapCenter Plug-in for VMware vSphere	Username
10.61.181.201	administrator@vsphere.local
Port	Password

4. The progress of jobs can be monitored from the Job Monitoring tab.

	,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,		rtual Resources fr Job Id: 559167ba-8876	5-45db-9131-b918a165d	-		
	Other Job Type	Jul 31 2 Start Tin	023, 9:18:22 pm ne	Jul 31 2023, 9:1 End Time	8:26 pm	Success Job Status	
b-Jobs(2)							Collapse All
Job Name		🗘 Job ID	\$ \$	start Time	End Time	Duration	÷ 🔂
Discover V	firtual Resources from SnapCente	er Plu 🗇 55916	7ba-8876-45db J	ul 31 2023, 9:18:22 pm	Jul 31 2023, 9:18	3:26 pm 4 Seconds	
Di	scovering Virtual Resources	D 99446	761-f997-4c80-8 J	ul 31 2023, 9:18:22 pm	Jul 31 2023, 9:14	3:24 pm 2 Seconds	
Re	gistering Datastores	D b7ab4	95-1ee5-40ff-9a J	ul 31 2023, 9:18:24 pm	Jul 31 2023, 9:11	3:26 pm 2 Seconds	

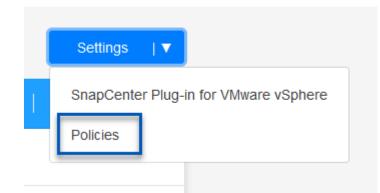
5. Once discovery is complete you will be able to view the datastores and virtual machines across all discovered SCV appliances.

	orking Environments	6 Datastores 14 Virtual Mac	hines Prote	
6 Datastores Filter By +			Q	VM View Setting
Datastore	0 Datastore Type	; vCenter ≎ Poli	cy Name 🔅 Prote	ection Status
NFS_SCV	NFS	vcsa7-hc.sddc.netapp.com	0	Unprotected ••••
OTS_DS01	NFS	172.21.254.160 1 Ye	ar Daily LTR 🥏	Protected
SCV_WKLD	NFS	vcsa7-hc.sddc.netapp.com 1 Ye	ar Daily LTR 🥏	Protected
NFS_SQL	NFS	vcsa7-hc.sddc.netapp.com 1 Ye	ar Daily LTR 🥏	Protected •••
NFS_SQL2	NFS	vcsa7-hc.sddc.netapp.com 1 Ye	ar Daily LTR 🥏	Protected
SCV_DEMO	NFS	vcsa7-hc.sddc.netapp.com	0	Unprotected

In BlueXP backup and recovery for virtual machines, create policies to specify the retention period, backup source and the archival policy.

For more information on creating policies refer to Create a policy to back up datastores.

1. From the BlueXP backup and recovery for virtual machines main page, access the **Settings** drop down menu and select **Policies**.



- 2. Click on Create Policy to access the Create Policy for Hybrid Backup window.
 - a. Add a name for the policy
 - b. Select the desired retention period
 - c. Select if backups will be sourced from the primary or secondary on-premises ONTAP storage system
 - d. Optionally, specify after what period of time backups will be tiered to archival storage for additional cost savings.

Policy Details	Policy Name	
	12 week - daily backups	
	U	
Retention 🚯		
	Daily	
	Backups to retain SnapMirror	Label
	84 Daily	
	Weekiy	Setup Refention Weekly
	Monthly	Setup Retention Monthly
Archival Policy	Backups reside in standard storage for frequently acc you can tier backups to archival storage for further co	
	 Tier Backups to Archival 	,
	Archival After (Davs)	
	Cancel Create	
The Snan	/lirror Label entered here is used to i	dentify which backups to apply
	The label name must match the labe	

The final step is to activate data protection for the individual datastores and virtual machines. The following steps outline how to activate backups to AWS.

For more information refer to Back up datastores to Amazon Web Services.

1. From the BlueXP backup and recovery for virtual machines main page, access the settings drop down for the datastore to be backed up and select **Activate Backup**.

6 Datastores						
Filter By +				C	Q 🕒 VM View	Settings ▼
Datastore	Datastore	Type 🗘 vCenter	0 Policy I	Name 🗘 Pr	rotection Status	1
NFS_SCV	NFS	vcsa7-hc.sddc	.netapp.com		Unprotected	
OTS_DS01	NFS	172.21.254.16	0 1 Year I	Daily LTR	Protected	w Details ivate Backup
SCV_WKLD	NFS	vcsa7-hc.sddc	.netapp.com 1 Year I	Daily LTR	Protected	
	1 Assign Policy	2 Add Working Environm	Assign Policy		gure Provider (5)	Review
21 Policies	olicy Name	SnapMirror Label	Retention Count	Backup Source	Archival Pc	licy
5	Year Daily LTR	daily	daily : 1830	Primary	Not Active	
5	Year Daily LTR	daily	daily : 1830	Primary	Not Active	

3. At the **Add Working Environments** page the datastore and working environment with a check mark should appear if the working environment has been previously discovered. If the working environment has not been previously discovered you can add it here. Click on **Next** to continue.

	Add Workin	ng Environments		
	rironment) details that you want Cloud Ma cluster. You will need to enter multiple wo	anager to discover. Working e		
SVM	Volume	Working Environ	nment	I.
EHC_NFS	NFS_SCV		kingEnvironment-6MzE27u1	Edit

4. At the Select Provider page click on AWS and then click on the Next button to continue.

Assign Policy	Add Working Environments	3 Select Provider (4) Configure	Provider 5 Review
	Sele	ct Provider	
aws		۵	StorageGRID
Amazon Web Services	Microsoft Azure	Google Cloud Platform	StorageGRID

5. Fill out the provider specific credential information for AWS including the AWS access key and secret key, region, and archival tier to be used. Also, select the ONTAP IP space for the on-premises ONTAP storage system. Click on **Next**.

Assign Policy	Add Working Environments	Select Provider	4 Configure Provider	5 Review
	Confi Cloud Manager needs the follow	gure Provider ing details to connect with the	ne cloud provider.	
Provi	ider Information		Location and Connectivity	
AWS Account		Region		
	•	US East (N	I. Virginia)	-
AWS Access Key			Environment kingEnvironment-6MzE27u1	
Enter AWS Access Key Required		Default		•
AWS Secret Key		Archival Tier	r.	
Enter AWS Secret Key Required		Glacier		•

6. Finally, review the backup job details and click on the **Activate Backup** button to initiate data protection of the datastore.

Assign Policy

 (\checkmark)

\frown	
(\checkmark)	Select Provider
· · /	OCICCUT TO MIGCI



 (\checkmark)

Review

-	
Rev	Iew/
1.00	

Policy		5 Year Daily LTR
SVM		EHC_NFS
Volumes		NFS_SCV
Working Environment		OnPremWorkingEnvironment-6MzE27u1
Backup Source		Primary
Cloud Service Provider		AWS
AWS Account		
AWS Access Key		
Region		US East (N. Virginia)
IP space		Default
Tier Backups to Archival		No
	Previous	Activate Backup
At this point data	transfer may not imr	nediately begin. BlueXP backup and recove

Restoring Virtual Machines in the case of data loss

Ensuring the safeguarding of your data is only one aspect of comprehensive data protection. Equally crucial is the ability to promptly restore data from any location in the event of data loss or a ransomware attack. This capability is vital for maintaining seamless business operations and meeting recovery point objectives.

NetApp offers a highly adaptable 3-2-1 strategy, providing customized control over retention schedules at the

primary, secondary, and object storage locations. This strategy provides the flexibility to tailor data protection approaches to specific needs.

This section provides an overview of the data restoration process from both the SnapCenter Plug-in for VMware vSphere and BlueXP backup and recovery for virtual machines.

Restoring Virtual Machines from SnapCenter Plug-in for VMware vSphere

For this solution virtual machines were restored to original and alternate locations. Not all aspects of SCV's data restoration capabilities will be covered in this solution. For in depth information on all that SCV has to offer refer to the Restore VMs from backups in the product documentation.

Complete the following steps to restore a virtual machine restore from primary or secondary storage.

- 1. From the vCenter client navigate to **Inventory > Storage** and click on the datastore that contains the virtual machines you wish to restore.
- 2. From the **Configure** tab click on **Backups** to access the list of available backups.

5 8 9	Summary Monitor Configure	r Permissions Paus Hosts VMs						
 Vosa7-te: sidic netappicom Ib betecenter Demo 	Alarm Defestions Scheduled Taxins Gametar	Backups	- G-Expert				(The	
DemoD5	Device Nacking	Name Salar	Locanora	Stat Tate	End Tree	Mourned	Policy	SM-spe Stappic
destination Cannectivity with Haids exol 3-bc-01 Local Hardware Acceleration	Currentwity with Husta	10x, mms, mily, 07.012023, 79.2430.0755. Compared	Pitmary & Secondary	101/2020 7 24.35 PM	2/19/2003 7:24 18 PM	No .	Dwly	Aui
	Hardware Acceleration	tox. deem. andy, 07-31 2021, 08 3800.00. Complete	Premary & Secondary	MA 0045 # 2000 AM	T19/2023 9 28:02 AM	No	Datly	No
essi7-to-02 Local	Capatility sets	10-, man, may (0110-2023, 0530.00 ft) Constant	Primary & Secondary	7/50/2022 9/29/00 AM	7130/2023 9/39/02 AM	110	Dwly	160
exo7 &c-03 Local	SnapCenter Plug in for Vitwa	10, mm, mm, 07-29-2023.09.080008. Complete	Premary & Secondary	P29/2023 8 39:00 AM	109/2023/9/29/02 AM	hap .	Daty	No
ess/7-hc-04 Local	Resource Getople	101, more, may, 07 28 2071, 26 28 00 8. Compariso	Primary & Secondary	1728/2023 9-39 00 AM	7/20/2023 9/38/02 AM	No	Dwy	No.
exv7-hc-05-Local	Báckupa	100,0000,000,01212023,3025.5016. Compariso	Primary & Secondary	1/2//2023 10:29:10 AM	7/27/2023 10:25:52 XM	No	Dwly	No.
essi7-bc-06 Local		are mine may \$5.77.2023 (\$1.57.29.06. Complete	Prenary & Secondary	7/77/20123 9/5/7.28 AM	727202395730 AM	No	Dety	Alto
🗐 iso		10.000 mm, may 07 27 2022-09 39 00 05. Complete	Primary & Secondary	1/27/2023 8:30:00 AM	WA 55/003 9 30/02 AM	tio	Dwy	.944
E NPS_SCV		are more may 01/27/2022 00/24 h bits Complete	Primary & Secondary	7/27/2023 8 34 71 644	7/27/2023 9:34 12 AM	No	Dwy	. 191

3. Click on a backup to access the list of VMs and then select a VM to restore. Click on Restore.

SCV_DEMO : A Summary Monitor Con	figure Permissions	Files Hosts	VMs					
Alarm Definitions Name: scv_demo_daily_07-31-2023_19.24.36.0755 Scheduled Tasks Time Stamp: Mon Jul 31 2023 19:24:36 GMT-0400 (Eastern Daylight Time) General Mounted: No Device Backing Policy: Dally Connectivity with Hosts Koman and the second and the sec								
Capability sets	The following entities are	The following entities are included in the backup:scv_demo_daily_07-31-2023_19.24.36.0755						
SnapCenter Plug-in for VMwa V Select an entity and click Restore to restore it.								
Resource Groups	RESTORE							
Backups	Entity Name	Quiesced	UUID	Location				
	SQLSRV-07	No	5032d1f2-2591-7f7b-46e3-8dbd4a6b2fb4	[SCV_DEMO] SQLSRV-07/SQLSRV-07.vmx				
	scv_restore_test	Yes	50323c8e-04a3-5acf-a2df-a6bc0ced0419	[SCV_DEMO] scv_restore_test/scv_restore_test.vmx				
	SQLSRV-06	No	50327515-8cce-5942-0f85-350ad39bce42	[SCV_DEMO] SQLSRV-06/SQLSRV-06.vmx				
	SQLSRV-08	No	5032b2a9-e1af-c56a-6923-6dbd0eeb6327	[SCV_DEMO] SQLSRV-08/SQLSRV-08.vmx				
	SQLSRV-05	No	50326625-dd29-af23-2fd5-fe04e0a57a69	[SCV_DEMO] SQLSRV-05/SQLSRV-05.vmx				
	SCV_DEMO	No	netfs://172.21.118.112///SCV_DEMO	SCV:/vol/SCV_DEMO				

4. From the Restore wizard select to restore the entire virtual machine or a specific VMDK. Select to install to the original location or alternate location, provide VM name after restore, and destination datastore. Click **Next**.

1. Select scope	Restore scope	Entire virtual machine
2. Select location	Restart VM	
3. Summary	Restore Location	Original Location
		(This will restore the entire VM to the original Hypervisor with the original
		settings. Existing VM will be unregistered and replaced with this VM.)
		Alternate Location
		(This will create a new VM on selected vCenter and Hypervisor with the customized settings.)
	Destination vCenter Server	10.61.181.210
	Destination ESXi host	esxi7-hc-04.sddc.netapp.com
	Network	Management 181
	VM name after restore	SQL_SRV_08_restored
	Select Datastore:	NFS_SCV
5. Choose to backup fro	om the primary or second	BACK NEXT FINISH CANCEL
5. Choose to backup fro Restore	om the primary or second	
Restore	Destination datastore Lo	ary storage location.
Restore 1. Select scope 	Destination datastore Lo SCV_DEMO (1	ary storage location.
 Restore 1. Select scope 2. Select location 	Destination datastore Lo SCV_DEMO (1	ary storage location. cations Primary) SCV:SCV_DEMO THRM: SCV SCV_DEMO
 Restore 1. Select scope 2. Select location 	Destination datastore Lo SCV_DEMO (1	ary storage location. cations Primary) SCV:SCV_DEMO THRM: SCV SCV_DEMO
 Restore 1. Select scope 2. Select location 	Destination datastore Lo SCV_DEMO (1	ary storage location. cations Primary) SCV:SCV_DEMO THRM: SCV SCV_DEMO
 Restore 1. Select scope 2. Select location 	Destination datastore Lo SCV_DEMO (1	ary storage location. cations Primary) SCV:SCV_DEMO THRM: SCV SCV_DEMO

Restoring Virtual Machines from BlueXP backup and recovery for virtual machines

BlueXP backup and recovery for virtual machines allows restores of virtual machines to their original location. Restore functions are accessed through the BlueXP web console.

For more information refer to Restore virtual machines data from the cloud.

To restore a virtual machine from BlueXP backup and recovery, complete the following steps.

1. Navigate to **Protection > Backup and recovery > Virtual Machines** and click on Virtual Machines to view the list of virtual machines available to be restored.

Backup and recovery	Volumes	Restore	Applications	Virtual Machines	Kubernetes	Job Monitoring	Reports
	0	4 Working Env	vironments	6 Datastores	đ	14 Virtual Machines	

2. Access the settings drop down menu for the VM to be restored and select

ter By +				Q (VM View	Settings
Virtual Machine	Oatastore Type	0 vCenter ~	Policy Name	Protection Status	Last Backup 🔅 🕴	
SQLSRV-08	NFS	vcsa7-hc.sddc.netap		Unprotected		
SQLSRV-04	NFS	vcsa7-hc.sddc.netap	1 Year Daily LTR	Protected	Jul 31, 2023, 7:2	•••

3. Select the backup to restore from and click on Next.

7 Backup	IS		
	Backup Name	≎ Backup Time	٥
⊘	SQL_Servers_Daily_07-31-2023_19.23.39.0938	Jul 31, 2023, 7:23:42 PM	
	SQL_Servers_Daily_07-31-2023_16.40.00.0661	Jul 31, 2023, 4:40:03 PM	
	SQL_Servers_Daily_07-30-2023_16.40.00.0690	Jul 30, 2023, 4:40:03 PM	

- 4. Review a summary of the backup job and click on **Restore** to start the restore process.
- 5. Monitor the progress of the restore job from the **Job Monitoring** tab.

estore 17 files fr	om Cloud		lame: Restore 17 files fr ld: ec567065-dcf4-4174-b7ef-b27			
	Restore Files Job Type	NFS_SQL Restore Content	17 Files Content Files	NFS_SQL Restore to) In Progress Job Status	
						Exp
5	Restore Content					^
aws	ots-demo Working Environment Name	NAS_VOLS SVM Name	NFS_SQL Volume Name	SQL_Servers_D Backup Name		ıl 31 2023, 7:24:03 pm ackup Time
5	Restore from					~
aws	AWS Provider	us-east-1 Region	982589175402 Account ID	netapp-backup Bucket/Contain	o-d56250b0-24ad her Name	

Conclusion

The 3-2-1 backup strategy, when implemented with SnapCenter Plug-in for VMware vSphere and BlueXP backup and recovery for virtual machines, offers a robust, reliable, and cost-effective solution for data protection. This strategy not only ensures data redundancy and accessibility but also provides the flexibility of restoring data from any location and from both on-premises ONTAP storage systems and cloud based object storage.

The use case presented in this documentation focuses on proven data protection technologies that highlight the integration between NetApp, VMware, and the leading cloud providers. The SnapCenter Plug-in for VMware vSphere provides seamless integration with VMware vSphere, allowing for efficient and centralized management of data protection operations. This integration streamlines the backup and recovery processes for virtual machines, enabling easy scheduling, monitoring, and flexible restore operations within the VMware ecosystem. BlueXP backup and recovery for virtual machines provides the one (1) in 3-2-1 by providing secure, air-gapped backups of virtual machine data to cloud based object storage. The intuitive interface and logical workflow provide a secure platform for long-term archival of critical data.

Additional Information

To learn more about the technologies presented in this solution refer to the following additional information.

- SnapCenter Plug-in for VMware vSphere documentation
- BlueXP documentation

DR using BlueXP DRaas

Overview

Disaster Recovery is foremost in the minds of every VMware administrator. Because VMware encapsulates entire servers into a series of files that make up the virtual

machine; administrators take advantage of block storage-based techniques such as clones, snapshots and replicas to protect these VMs. ONTAP arrays offer built-in replication to transfer volume data, and therefore the virtual machines residing on the designated datastore LUNs, from one site to another. BlueXP DRaaS integrates with vSphere and automates the entire workflow for seamless failover and failback in the event of disaster. By combining storage replication with intelligent automation, administrators now have a manageable way to not only configure, automate, and test disaster recovery plans, but the means to easily run them in the case of a disaster.

Most time-consuming parts of a DR failover in a VMware vSphere environment is the execution of the steps necessary to inventory, register, reconfigure, and power up VMs at the DR site. An ideal solution has both a low RPO (as measured in minutes) and a low RTO (measured in minutes to hours). One factor that is often overlooked in a DR solution is the ability to test the DR solution efficiently on a periodic interval.

To architect a DR solution, keep the following factors in mind:

- The recovery time objective (RTO). The RTO is how quickly a business can recover from a disaster, or, more specifically, how long it takes to execute the recovery process to make business services available again.
- The recovery point objective (RPO). The RPO is how old the recovered data is after it has been made available, relative to the time that the disaster occurred.
- Scalability and adaptability. This factor includes the ability to grow storage resources incrementally as demand increases.

For more technical information on the available solutions, please see:

- DR using BlueXP DRaaS for NFS Datastores
- DR using BlueXP DRaaS for VMFS Datastores

DR using BlueXP DRaaS for NFS Datastores

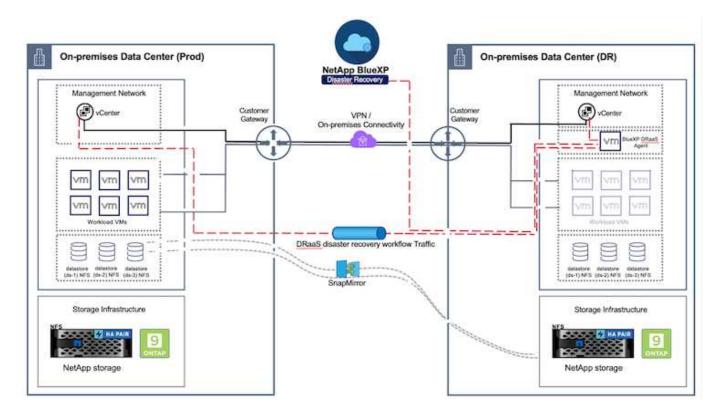
Implementing disaster recovery through block-level replication from the production site to the disaster recovery site is a resilient and cost-effective method for safeguarding workloads against site outages and data corruption events, such as ransomware attacks. Using NetApp SnapMirror replication, VMware workloads running on on-premises ONTAP systems with NFS datastore can be replicated to another ONTAP storage system located in a designated recovery datacenter where VMware is also deployed.

This section of the document describes the configuration of BlueXP DRaaS to set up disaster recovery for onpremises VMware VMs to another designated site. As part of this setup, the BlueXP account, BlueXP connector, the ONTAP arrays added within BlueXP workspace which is needed to enable communication from VMware vCenter to the ONTAP storage. In addition, this document details how to configure replication between sites and how to setup and test a recovery plan. The last section has instructions for performing a full site failover and how to failback when the primary site is recovered and bought online.

Utilizing the BlueXP disaster recovery service, integrated into the NetApp BlueXP console, companies can easily discover their on-premises VMware vCenters and ONTAP storage. Organizations can then create resource groupings, create a disaster recovery plan, associate it with resource groups, and test or execute failover and failback. SnapMirror provides storage-level block replication to keep the two sites up to date with incremental changes, resulting in a Recovery Point Objective (RPO) of up to 5 minutes. Additionally, it is

possible to simulate disaster recovery procedures without affecting production or incurring additional storage costs.

BlueXP disaster recovery leverages ONTAP's FlexClone technology to create a space-efficient copy of the NFS datastore from the last replicated Snapshot on the disaster recovery site. After completing the disaster recovery test, customers can easily delete the test environment without impacting actual replicated production resources. In case of an actual failover, the BlueXP disaster recovery service orchestrates all the necessary steps to automatically bring up the protected virtual machines on the designated disaster recovery site with just a few clicks. The service will also reverse the SnapMirror relationship to the primary site and replicate any changes from the secondary to the primary for a failback operation, when needed. All these capabilities come at a fraction of the cost compared to other well-known alternatives.



Getting started

To get started with BlueXP disaster recovery, use BlueXP console and then access the service.

- 1. Log in to BlueXP.
- 2. From the BlueXP left navigation, select Protection > Disaster recovery.
- 3. The BlueXP disaster recovery Dashboard appears.

			Account * Workspace	
A Storage	very Dashboard Sites Re	plication plans. Resource groups Job m	nhong	Free trial (55 days left) - View details 🔹
🗘 Health				
Protection -	s (2)	Replication plans (3)	Activ	vity
Backup and recovery	ja So ∆o tesue			Backup job for Replication Plan DemoRP004 14 align
Disaster recovery	Dashboard Shee		0	mitalus Backup of DemoRP004 for every 5 minutes Emispe
Replication 0	Replication plans	View plans		Eackup job for Replication Plan RPVMF503 3 m apr
Ransonware protection 🖄	Resource groups	21 👩 11	,	Witalize Backup of RPVWF503 for every 5 minutes 3 m app
Orvensece +	Job monitoring	Protected VMs Unpr	tected VMs	Backup job for Replication Plan (RFNF5001 30 m op
Mobility	em resource groups Verw	protected VMs		all jobs
🔹 Extensiona 🔸				
	1 Satovers.	ent fallowers	O Migrations	

Before configuring disaster recovery plan, ensure the following pre-requisites are met:

- BlueXP Connector is set up in NetApp BlueXP.
- BlueXP connector instance have connectivity to the source and destination vCenter and storage systems.
- NetApp Data ONTAP cluster to provide storage NFS datastores.
- On-premises NetApp storage systems hosting NFS datastores for VMware are added in BlueXP.
- DNS resolution should be in place when using DNS names. Otherwise, use IP addresses for the vCenter.
- SnapMirror replication is configured for the designated NFS based datastore volumes.
- Make sure that the environment has supported versions of vCenter Server and ESXi servers.

Once the connectivity is established between the source and destination sites, proceed with configuration steps, which should take couple of clicks and about 3 to 5 minutes.



NetApp recommends deploying the BlueXP connector in the destination site or in a third site, so that the BlueXP connector can communicate through the network with source and destination resources.

@) Disaster recovery	Dashboard	Sites Re	plication plans Report	arce groups Job monitoring	9 Free trial (68 days left)	- View details
	Sites (2)			Replication plan	is (2)	Activity	
	© 2 Runnling View sh	© 0 Down	▲ 0 Insue	⊘2 Ready View plan	© 0 Failed	Backup job for Replication Plan DemoRPVM/S03 In progress Sin progress products Backup of DemoRPVMPS03 for every 10 minutes 7 s age Discovery of resources in host 172.21166.100 sis age	
	Z Resource	ce groups	View prote	tected VMs	Unprotected VMs	Failback of resources using the replication plan. 'DemoR9VM/S03' It's says Discovery of resources in host 172.231.86.190 9 m app View all jobs	
			1 Failbacks	⊘ 1 Test fallowers	⊘ 0 Migrations		

BlueXP disaster recovery configuration

The first step in preparing for disaster recovery is to discover and add the on-premises vCenter and storage resources to BlueXP disaster recovery.

Open BlueXP console and select **Protection > Disaster Recovery** from left navigation. Select **Discover vCenter servers** or use top menu, Select **Sites > Add > Add vCenter**.

III No	etApp BlueXP	C. BlueXP Search Account ~ Workspace ~ BlueXPDR BlueXPDR BlueXPDR BlueXPDR-Wo	Connector ~ StagingConn01		0 B
	Disaster recovery	Dashboard Sites Replication plans Resource groups Job monitoring			
9	O sites		a 🗖	Add	
•	-				
÷		Add site			
		A site is a collection of vCenter servers, either on-premises or in the cloud.			
4		Site DemoSrc			
		Location			
		On-premi			
		AWS			
		Add Cancel			

Add the following platforms:

• Source. On-premises vCenter.

I Ne	tApp BlueXP	Q BlueXP Search	Account ~ Workspace ~ nimopisa nimopoce	Connector GISABLYPConn
	Oisaster recovery Dashb	tend Sites Implication plans Resour	ta groups	Free trial (55 days left) - View details +
	2 stee	Add vCenter server		Add;
¢ ø	minDemoSic	Enter connection details for the vCenter server Site	that is accessible from the BlueXP Connector. BlueXP Connector	(T) Serre
*		vCenter IP address 172.21.166.155		0
	nimDemoDe	vCenter user name administrator@hmcdc.local	vCenter password	1) Seren
		🛛 Use self-signed certificates 🌒		
		 	Add Cancel	

• **Destination**. VMC SDDC vCenter.

Dislaster recovery Deal	sboard Sites Repfication plans Resource groups Job monitoring	Free trial (55 days left) - View details
2 sites	Add vCenter server	Addic
📟 nimDemoSte	Enter connection details for the vCenter server that is accessible from the BlueXP Connector.	۲
572.233.306.3 O marty	Site BlueXP Connector nimDemoSrc	Senin
	vCenter IP address 172.21.108.190	
- nimDemoDe	vCenter user name vCenter password	0
() () () () () () () () () () () () () (administrator@hmcdc.local	Sann (1)
	C Use self-signed certificates	
	Add Cancel	

Once the vCenters are added, automated discovery is triggered.

Configuring Storage replication between source site array and destination site array

SnapMirror provides data replication in a NetApp environment. Built on NetApp Snapshot® technology, SnapMirror replication is extremely efficient because it replicates only the blocks that have been changed or added since the previous update. SnapMirror is easily configured by using either NetApp OnCommand® System Manager or the ONTAP CLI. BlueXP DRaaS also creates the SnapMirror relationship provided cluster and SVM peering is configured beforehand.

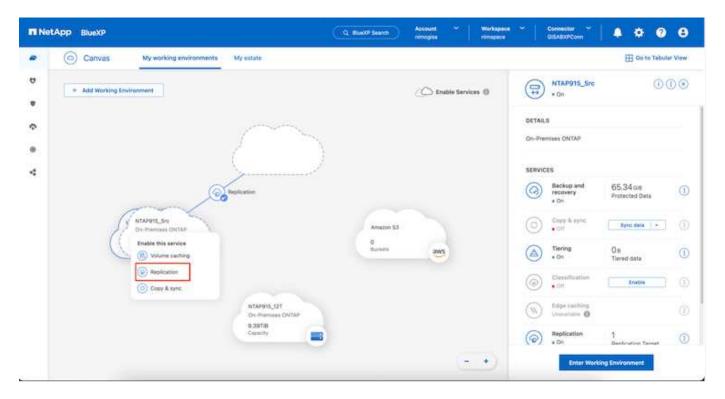
For cases in which the primary storage is not completely lost, SnapMirror provides an efficient means of resynchronizing the primary and DR sites. SnapMirror can resynchronize the two sites, transferring only changed or new data back to the primary site from the DR site by simply reversing the SnapMirror relationships. This means replication plans in BlueXP DRaaS can be resynchronized in either direction after a failover without recopying the entire volume. If a relationship is resynchronized in the reverse direction, only new data that was written since the last successful synchronization of the Snapshot copy is sent back to the destination.



If SnapMirror relationship is already configured for the volume via CLI or System Manager, BlueXP DRaaS picks up the relationship and continues with the rest of the workflow operations.

How to set it up for VMware Disaster Recovery

The process to create SnapMirror replication remains the same for any given application. The process can be manual or automated. The easiest way is to leverage BlueXP to configure SnapMirror replication by using simple drag & drop of the source ONTAP system in the environment onto the destination to trigger the wizard that guides through the rest of the process.



BlueXP DRaaS can also automate the same provided the following two criteria's are met:

- Source and destination clusters have a peer relationship.
- Source SVM and destination SVM have a peer relationship.

8	Add replication plan	🖉 vCenter servers 🕑 Applications 🚯 Resource mapping 🕘 Recurrence 💿 Review
ø		Fallover mappings Telst mappings
•		Compute resources ⊘ Mapped
Ф 8		Virtual networks 📀 Mapped
4		Virtual machines 📀 Mapped
		Datastores
		RPO for all datastores in minutes Retention count for all datastores 5 30
		Source datastore Target datastore Src_NFS_D503 (svm_NFS:Src_NFS_D503) Src_NFS_D503 (svm_ninfs:Src_NFS_D503 (svm_ninfs:Src_NFS_D503_CP) Transfer schedule(RP0) : hourly, async

(**i**)

If SnapMirror relationship is already configured for the volume via CLI, BlueXP DRaaS picks up the relationship and continues with the rest of the workflow operations.

What can BlueXP disaster recovery do for you?

After the source and destination sites are added, BlueXP disaster recovery performs automatic deep discovery and displays the VMs along with associated metadata. BlueXP disaster recovery also automatically detects the networks and port groups used by the VMs and populates them.

2 sites				Q	Add
Z stes				~	100
nimDemoSrc					1
172.21.186.155	72 VMs	13 Dutasteres	1 Hesource groups	GISABXPConn Currentiar	1
nimDemoDest					1
172.21.166.190 () Inactive	61 vhis	3 Datastures	0 Resource prodit	GISABXPConn Connector	1
			Resource		1

After the sites have been added, VMs can be grouped into resource groups. BlueXP disaster recovery

resource groups allow you to group a set of dependent VMs into logical groups that contain their boot orders and boot delays that can be executed upon recovery. To start creating resource groups, navigate to **Resource Groups** and click **Create New Resource Group**.

III Net	App BlueXP	Q: BlueXP Searc	Account ~ imogiaa	Workspace 🔪	Connector ~ GISABXPCenn	4 0 *	0 B
	Disaster recovery Das	Add resource group			The second se	51 days left) - View o	Setails (+
9	1 meauros grouge				۹ 🔳	7.666	
	Nonseries process	Name	vCenter			- E - N	
0	The state of the	DemoNFSDS03RQ	172.21.166.155			- 1 1	
·**	DemuR001						
0		Select virtual machines					
		Q NFS_DemoA	Selected VMs (5)				
~		VFS_DemoA_VM01	NFS_DemoA_VM01	×			
		VF5_DemoA_VM02	NFS_DemoA_VM02	×			
		NFS_DemoA_VM03	NFS_DemoA_VM03	×			
		MFS_DemoA_VM04	NFS_DemoA_VM04	×			
		NFS_DemoA_VM05	NFS_DemoA_VM05	×			
			Add	Cancel			

0	Disaster recovery Dashboard Si	tes Replication plans Resource groups	Job monitoring	Free trial (51 days left) - View details
	2 resource groups			Q Add
	Resource group	2 Course Ma	Source vCenter	÷ ()
	DemoRG01	nimDemoSrc	172.21.166.155	
	DemoNFSDSD3RG	nimDemoSco	172.21.166.155	

The resource group can also be created while creating a replication plan.

(i)

The boot order of the VMs can be defined or modified during the creation of resource groups by using simple drag and drop mechanism.

III Net	App BlueXP	Q BlackP Sea	roh Account ~ Workspace ~ nimogiaa nimopica	Connector 🖌 🛛 🍋 🌣 📀 😆
•• • • •	Disaster recovery Der 2 resource groupe DemuR003 DemuR011DB00RG	Edit resource group Name DemoNFSDS0380 Belect virtual machines Q Search All Datastares BICSLDemoCvm01 BICSLDemoCvm03 BICSLDemoCvm04 BICSLDemoCvm05 UburtuVM01		restance (St days left) - View details -
		Win2K19VM01	Save Cancel	

Once the resource groups are created, the next step is to create the execution blueprint or a plan to recover virtual machines and applications in the event of a disaster. As mentioned in the prerequisites, SnapMirror replication can be configured beforehand or DRaaS can configure it using the RPO and retention count specified during creation of the replication plan.

NetApp BlueXP O Cariyas My working environments My estate	Q BlueXP Search Account ~ Workspace nimopisa nimopisa nimopose	
 Add Working Environment Add Working Environment NTAP915_50 On-Premises ONTAP 2.0178 CaseOff Replication NTAP915_Destin On-Premises ONTAP 2.5878 CaseOff Satia Satia CaseOff Premises ONTAP Satia CaseOff Premises ONTAP Satia CaseOff Premises ONTAP Satia CaseOff CaseOff	C Enable Services ()	Working Environments Image: Solution of the s

0	Replication						
	Volume Relationships ((8)					9 C
	Health Status 🕴	Source Volume \$1	Target Volume	Total Transfer Time 🗘	Status 🔍 🛛	Mirror State 🗧 🗧	Last Successful Ber 39.3 Millio
	ø	Demo_TPS_DSD1 NTAP915_Src	Demo_TPS_DS01_Copy NTAP915_Desth	13 seconds	idie	snapmirrored	Aug 5, 2024, 6:15 386.63 MB
	Ø	Srt_256_Vol01 NTAP915_Src	Src_25G_Vol01_Copy NTAP915_Destn	4 seconds	idle	unapmirrored	Aug 16, 2024, 12= 79-23 MiB
	0	Src_NFS_DS03 NTAP915_Src	Src_NFS_DSD3_CP NTAP915_Destn	12 seconds	ide	snapmirrored	Aug 16, 2024, 12: 24.64 MB
	Θ	Src_NFS_DS04 NTAP915_Src	Src_NF5_0504_CP NTAP915_Destn	3 seconds	idie	snapmirrored	Aug 16, 2024, 12± 47.38 Mit
	0	Src_ISCSI_DS04 NTAP915_Src	Src_ISCSI_DS04_copy NTAP915_Destn	4 seconds	ide	snapmirrored	Aug 16, 2024, 12× 108.87 M8
	0	nimpra NTAP915_Src	nimpra_dest NTAP915_Destn	2 seconds	ide	snapmirrored	Aug 16, 2024, 12± 3.48 Kib

Configure the replication plan by selecting the source and destination vCenter platforms from the drop down and pick the resource groups to be included in the plan, along with the grouping of how applications should be restored and powered on and mapping of clusters and networks. To define the recovery plan, navigate to the **Replication Plan** tab and click **Add Plan**.

First, select the source vCenter and then select the destination vCenter.

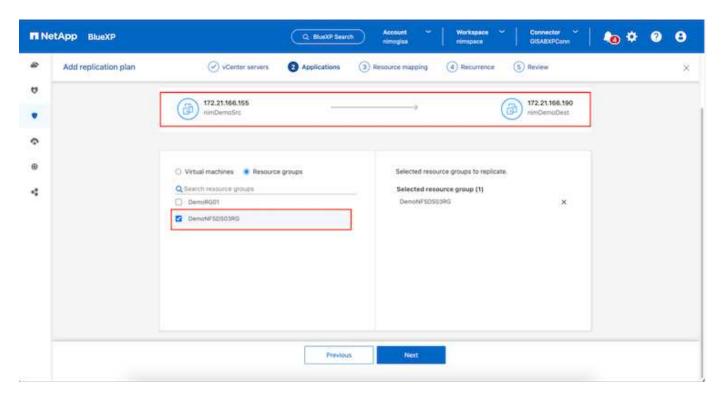
NetApp BlueXP	Q BlueXP Search Account " Workspace " Connector 🍋 🌣 📀 🔒
Add replication plan	1 vCenter servers 2 Applications 3 Resource mapping 4 Recurrence 5 Review X
Ē.	Replication plan name DemoN#SD503RP
	Select a source vCenter where your data exists, to replicate to the selected target vCenter.
	Source vCenter Target vCenter 122.21:86.155 *
	Cancel

The next step is to select existing resource groups. If no resource groups created, then the wizard helps to group the required virtual machines (basically create functional resource groups) based on the recovery objectives. This also helps define the operation sequence of how application virtual machines should be

restored.

÷.

i.



Resource group allows to set boot order using the drag and drop functionality. It can be used to easily modify the order in which the VMs would be powered on during the recovery process.

Each virtual machine within a resource group is started in sequence based on the order. Two resource groups are started in parallel.

The below screenshot shows the option to filter virtual machines or specific datastores based on organizational requirements if resource groups are not created beforehand.

min	tApp BlueXP		(Q. Black Second	Account *	Workspace 🗶	Connector ~ 015ABXPConn	• •	?	۲
	Add replication plan	Select the	Applications (3) Resource in Applications e applications on the source inCenter t Hypicorie Base Community	accing (1) Recurre	none (b) Review			•	3 ×
			Previous	Het .					

Once the resource groups are selected, create the failover mappings. In this step, specify how the resources from the source environment maps to the destination. This includes compute resources, virtual networks. IP customization, pre- and post-scripts, boot delays, application consistency and so on. For detailed information, refer to Create a replication plan.

Add replication plan	✓ vCenter server	vers 🕜 Applications	Resource mapping	(4) Recurrence	(5) Review	40 *	- 12	8 ×
	Use same mappings for fa	1. A	683					
	Fallover mappings	Test mappings						
	Compute resources							
	Source cluster		Target cluster					
	vvCSA8-Cluster01		wid	d04-Cluster01 👻				
	Virtual networks				^			
	Source virtual LAN		Target segment	ř.				
	VM_3420		VM	N_3422 *				
		Previo	s Matt					

By default, same mapping parameters are used for both test and failover operations. To set different mappings for test environment, select the Test mapping option after unchecking the checkbox as shown below:

(i)

Add replication plan	✓ vCenter s	ervers 🕑 Ap	plications C	Resource ma	apping ④ Recurre	nce (5) Review		
	Virtual machines						~	
	IP address type	Target IP		1				
	Static	* Same as	source) 👻]				
	Use the same cred	pentials for	s source nt from source					
	Q.	printran vi						
	Source VM	CPUs	RAM		Boot delay(mins between 0 and 10)	Create application consistent replicas		
	DemoNFSDS03RG							
	NFS_DemoA_VM01	2	4	GIB ~	0] 0		
	NFS_DemoA_VM02	2	4	GB ~	0			

Once the resource mapping is complete, click Next.

Add replication plan	VCenter set	vers 🕑 Applications 👩 Resource mapping ④	Recurrence (5) Review	
	172.21.166.155 nimDemoStc	·	172.21.168.190 nimDemoDest	
	Use same mappings for fi	allover and test mappings		
	Pailover mappings	Test mappings	÷	
	122200200200200	() Mapped		
	Virtual networks			

Select the recurrence type. In simple words, select Migrate (one time migration using failover) or recurring continuous replication option. In this walkthrough, Replicate option is selected.

IT Ne	tApp BlueXP	Q. BlueXP Search	Account " Workspace " Connector nimopise nimopice GISABLYPCenn	♠ ♥ ♥ ♥
	Add replication plan	⊘ vCenter servers ⊘ Applications (Resource mapping O Recurrence (5) Review	×
a				
٠		(m) 172.21.166.155	172.21.166.190	
Ŷ			0	
Θ				
*				
		Migrate	Replicate	
		Migrate application data one time from tourte to larget.		
			Next	
		Previous		

Once done, review the created mappings and then click on Add plan.

 (\mathbf{i})

VMs from different volumes and SVMs can be included in a replication plan. Depending on the VM placement (be it on same volume or separate volume within the same SVM, separate volumes on different SVMs), the BlueXP disaster recovery creates a Consistency Group Snapshot.

III N	etApp BlueXP		Q BueXP Search Account ~	Workspace Connector GISABXPConn	l 🍖 🌣 📀 😣
8	Add replication plan	VCenter servers	Applications	Recurrence B Review	×
a					
		(a) 172.21.166.155	\longrightarrow	(a) 172.21.106.190 nmDemoDest	1
¢			Replicate	0	1
0		Plan details	Fallover mapping	Virtual mochines	1
-:					
		Plan name	DemoNFSDS03RP		
		Recurrence	Replicate		
			Previous Add plan		

0						1	napika	Connector ~ GISA8XPCenn	•	
0	Disaster recov	ery Di	ishboard Sites	Replication p	Resource group	ps Job monitoring		Q,	(51 days left) - Vie A6d	w details
	Plan		Compliance check		Toblecouperate	Resource groups 🚊	Recurrence C	Failover site	*	
	Deni	WF\$D\$03RP	Healthy	@ Ready	rimDemoSrc	DemoNFSDS03RG	Replicate	rimDemoDest		

BlueXP DRaaS consists of the following workflows:

- Test failover (including periodic automated simulations)
- Cleanup failover test
- Failover
- Failback

Test failover

Test failover in BlueXP DRaaS is an operational procedure that allows VMware administrators to fully validate their recovery plans without disrupting their production environments.

2	Oisas	iter recovery D	ashboard Sites	Replication	plans Resource grou	Job monitoring		Free trial (51 days left) - View	details -
		1 plans						Q. Add:	
		Plan	Compliance check	Piero atabas	Protected alte	Resource groups ()	Recurrence ::	Fallower site	
		DemoNF\$D\$D3RP	Healthy	Ready	rimDemoSrc	DemoNFSD503RG	Replicate	r/mDemoDest	
								View plan details Run compliance check	
								Test fallover	
								Deat op falsoer test : Feil over	
								Fuel Stack	
								Edit schedules Take snapshot now	
								Disable	
								Institu	

BlueXP DRaaS incorporates the ability to select the snapshot as an optional capability in the test failover operation. This capability allows the VMware administrator to verify that any changes that were recently made in the environment are replicated to the destination site and thus are present during the test. Such changes include patches to the VM guest operating system

I NetA	op BlueXP	Q BlueXP Search Account " Workspace " Connector nimogisa immpace GISABXP Con	.č 4 ₀ ♦ ∅ ੳ
*	Disaster recovery	Test failover: DemoNFSDS03RP	rial (51 days lett) - View details 🛛 +
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	1 plans Part Demotyl SDS0344	 Warning: This test will create 5 VMs in the site nimDemoDest. The test won't affect the site nimDemoSrc. Snapshot copy for volume recovery a Take snapshot now Select Warning: The corresponding volume will be restored with the selected snapshot copy. All the changes made after this snapshot copy was created will be lost. I snapshot name Resource group DemoNFSDSD3RP_DemoNFSDSD3RG_8-16-202 DemoNFSDSD3RP_DemoNFSDSD3RG_8-16-202 	Add 2
		Enter Test fallover to confirm Test fallover Cancel Cancel	

When the VMware administrator runs a test failover operation, BlueXP DRaaS automates the following tasks:

• Triggering SnapMirror relationships to update storage at the destination site with any recent changes that were made at the production site.

- Creating NetApp FlexClone volumes of the FlexVol volumes on the DR storage array.
- Connecting the NFS datastores in the FlexClone volumes to the ESXi hosts at the DR site.
- Connecting the VM network adapters to the test network specified during the mapping.
- Reconfiguring the VM guest operating system network settings as defined for the network at the DR site.
- Executing any custom commands that have been stored in the replication plan.
- Powering on the VMs in the order that is defined in the replication plan.

🗊 💆 📋 🤇	Summa	c_NFS_DS03 3 Activ ry Monitor Configure	ons Permissions Piles Host					
Wisd04-DC01 O4Yest6ed_t IS00uma S00.NF5.DS	Det	Type	573.1	E Capacity and U Last updates at 654 a Storage	C 1. T. 1		71.22 GB base	(ĝ
E tempotel		Hoats Virtual machines VM terrigitates Server Folder Location	2 5 172.21366366 /fire_p4P5_0503_TEST ds:///mt/s/valumes/tb005 -le687464/			,	00 OB casecity	
✓ Recent Tasks Al	larms '			VIEW STATS REFER	(D4			
Tash Name 🛛 🛪	Target. •	Statua 🔫	Details T	istatur T	Gueund Y For	Start firse 🚽 🕈	Completion Time M	•
Pecconfigure virtual máchin e	@ MES Demok VM02	Completed		HMCDCLOCAL\Administrator	3 mi	06/16/2024, 6:53:59 A M	06/16/2024, 6:53 M	150 A
Degister Witual mechine	Ett asstos-ocot	Completed		System	6 ers.	08/16/2024. 6:53:58 A	08/16/2024.6-53	159 A
Register Vitual machine	1000-F06866_1[3	() Completed		System	2.85	08/16/2024, 6:53:58 A	06/16/2024, 6:53	139 A
Degister vitual machine	PB wisso4-pcpt	O Compiletera	Registering Virtual Machine o In definiation hoef	5ysteni	2 ms	06/10/2024/6/51968%: V		00 A

Cleanup failover test Operation

The cleanup failover test operation occurs after the replication plan test has been completed and the VMware administrator responds to the cleanup prompt.

6	Disaster recovery Dar	shboard Sites	Replication pla	ens Resource group	Job monitoring		Free trial (51 days	left) - View details -
	1 plans						Q Ad	
	Plan in i	Compliance check	Plen status 🗧	Protected after	Resource groups	Recurrence ()	Fallower site (
	DemioNFSDSD3RP	@ Healthy	Test failover	rimDemoSrc	DemoNFSD5038G	Replicate	nimDemoDest	
							View plan details Run compliance che	a
							Clean up failover tes	1
							Fait over	
							Fail back Edit schedules	
							Take snapshot now	
							Disable	

This action will reset the virtual machines (VMs) and the status of the replication plan to the ready state.

When the VMware administrator performs a recovery operation, BlueXP DRaaS completes the following process:

- 1. It powers off each recovered VM in the FlexClone copy that was used for testing.
- 2. It deletes the FlexClone volume that was used to present the recovered VMs during the test.

Planned Migration and Fail over

BlueXP DRaaS has two methods for performing a real failover: planned migration and fail over. The first method, planned migration, incorporates VM shutdown and storage replication synchronization into the process to recover or effectively move the VMs to the destination site. Planned migration requires access to the source site. The second method, failover, is an planned/unplanned failover in which the VMs are recovered at the destination site from the last storage replication interval that was able to complete. Depending on the RPO that was designed into the solution, some amount of data loss can be expected in the DR scenario.

O Disa	aster recovery D	ashboard Sites	Replication	plans Resource grou	ps Job monitoring		Free trial (51 days left) - Vi	ew details \mid -
	1 plans						Q. Add	1
	Plan (*	Compliance check	Pien status :	Protected alte	Resource groups ()	Recurrence (//Fellowerside	
	DemoNFSDSD3RP	Healthy	@ Ready	nimDemoSrc	DemoNFSD503RG	Replicate	nimDemoDest	
							View plan details Run compliance check Test fallover Dean up takewar test	
							Feil over	
							Follows Edit schedules Take snapshot now	
							Disable	

When the VMware administrator performs a failover operation, BlueXP DRaaS automates the following tasks:

- Break and fail over the NetApp SnapMirror relationships.
- Connect the replicated NFS datastores to the ESXi hosts at the DR site.
- Connect the VM network adapters to the appropriate destination site network.
- Reconfigure the VM guest operating system network settings as defined for the network at the destination site.
- Execute any custom commands (if any) that have been stored in the replication plan.
- Power on the VMs in the order that was defined in the replication plan.

		NFS_DS03 Actio	vs Permissions Files Hosts	VMs				
Weido4-vco1hmcdcl Weido4-vco1hmcdcl Weido4-vco1hmcdcl Weido4-0co1 O4TestBed_D55 IsODume ScoNe3.0500 Itempdel weido4_patru	ocal Details	t Type Hoets Varbuit machines	505.3 2 5	Capacity and Last underest at 7- Storage		43.06 100.08 c	C8 hee	0
		VM templates Server Folder Location	172.21386366 7/lvc_34P5_0503_SP 25L//vm54/vstunescaldStite Saca4S36/	55				
Recent Tasks Alia				VIEW STATE BE	FREDA			
	Target	Status 🔻	Details. T	Initiation	T Dursed T	Start Time + + Com	mulation firms	+
ower On virtual machine	(# MS Denick VM02	Completed	Powering on the new Virtual Machine	HMCDCLOCALVAdministrati	or 4 ms.	08/16/2024, 7:04:07 A 08/ M M	/16/2024, 7:0412 A	
oww. On virtual machine	@ NES Demok VM05	Completed	Powering on the new Virtual Machine	HMCDCLOCALMeniatrat	tor 3 ms	08/16/2024, 7:04:07 A 08/ M	/16/2024, 7:04:12 A	È
wer On virtual machine	(# NES Demos VHO)	O Completed		HMCDCLOCAL\Admenitrat	tor 2 me	Activite Windo	n6/2024, 7:04:07 /	Ă,
over On virtual martime	B NPS Demica VM03	(2) Comparind	Powering on the new Virtual	HMCDCLOCAL Methodality	2 mil	ouncrook tokol an lob		

Failback

A failback is an optional procedure that restores the original configuration of the source and destination sites after a recovery.

Oisast	er recovery	Dashboard Sites	Replication p	Resource gr	Job monitoring		Free trial (51 da	vys left) - View details 🍴
	1 plans						a 🗾 V	Ndd
	Plan in	Compliance check	Pien status 🗧	Protected alte	Besource groups	Recurrence C	Fallover site	
	DemoNFSDSD3RP	Healthy	G Falled over	nimDemoSrc	DemoNFSD503RG	Replicate	rimDemoDest	
							View plan details	_
							Run compliance c	heck
							Texclutiver	
							Dean up talever 1 Fail over	
							Fail back	
							Edit schedules	_
							Take snapshot no	w
							Disable	
							Druble	

VMware administrators can configure and run a failback procedure when they are ready to restore services to the original source site.

NOTE: BlueXP DRaaS replicates (resyncs) any changes back to the original source virtual machine before reversing the replication direction. This process starts from a relationship that has completed failing over to a

target and involves the following steps:

- Power off and unregister the virtual machines and volumes on the destination site are unmounted.
- Break the SnapMirror relationship on the original source is broken to make it read/write.
- Resynchronize the SnapMirror relationship to reverse the replication.
- Mount the volume on the source, power on and register the source virtual machines.

For more details about accessing and configuring BlueXP DRaaS, see the Learn about BlueXP Disaster Recovery for VMware.

Monitoring and Dashboard

From BlueXP or the ONTAP CLI, you can monitor the replication health status for the appropriate datastore volumes, and the status of a failover or test failover can be tracked via Job Monitoring.

Oisa	ster recovery Das	hboard Site	Replication	on plans Resource groups Job mon	itoring	Free trial (50	0 days left) - View details
	26515 jobs						Q
	10 (C)	States :	Workload) News 2) Alternative (Endaime C	
	🗇 d923e607-b2±2-401	() In pra_	Backup	Backup job for Replication Plan DemoNF	08/16/2024, 04:5		Cancel job?
	0 3549cc9c-aa4e-45e	G Succe	Backup	Initialize Backup of DemoNFSD503RP for	68/16/2024, 04:5	08/16/2024, 04:5	
	5cb01bcc-9ea6-4aft	Succe	Backup	Backup job for Replication Plan:DemoNF	08/16/2024, 04:4	08/16/2024, 04:5	
		Succe	Backup	Initialize Backup of DemoNESDS03RP for	06/16/2024, 04:4	08/16/2024, 04:4	
	0 2FBb44d4-4be2-46t	Succe	Compliance	Compliance check for Replication Plan: D.,	08/16/2024, 04:4	08/16/2024, 04:4	
	🖞 398bc6a3-ata8-45d	Succe	Compliance	Initialize Compliance of DemoNFSDSD3R	08/16/2024, 04:4	08/16/2024, 04:4	
	Ø 977dbed8-6177-459;	Succe	Backup	Backup job for Replication Plan:DemoNF	06/16/2024, 04:4_	08/16/2024, 04:4	
	C bifc015e-cx3a-409d	Succe	Backup	Initialize Backup of DemoNFSDS03RP for	08/16/2024, 04:4	08/16/2024, 04:4	
	O cde759a8-ebet-498i	Succe	Backup	Backup job for Replication Plan:DemoNF	08/16/2024, 04:3	08/16/2024, 04:4	
	🗇 a414daba-9630-4c5	Succe	Backup	Initialize Backup of DemoNFSDS03RP for	08/16/2024, 04:3	08/16/2024, 04:3	

(i)

If a job is currently in progress or queued, and you wish to stop it, there is an option to cancel it.

With the BlueXP disaster recovery dashboard, confidently evaluate the status of disaster recovery sites and replication plans. This enables administrators to swiftly identify healthy, disconnected, or degraded sites and plans.

(@) Disa	aster recovery	Dashboard	Sites Replica	tion plans Resou	rce groups Job monitoring	g Free trial (50 days left) - Vie	w details
	Sites (2)			Replication plan	s (1)	Activity	
	⊘ 2 Running	O Cown	C O Tessue	⊘.1 Ready	🛞 0 Failed	Backup job for Replication Plan.DemoNF505038P 1m app	
	View sit	tes.		View repli	cation plan	Initialize Backup of DemoNPSDS03RP for every 5 minutes 4 m ago	
						 Isstiating DR Icense compliance check film app 	
	E 2 Resc	urce groups	S Protecte		0 130 Unprotected VMs	Backup job for Replication Plan DemoNFS0S038P If maps	
	View resour	ce groups	View protected	VMa	View unprotected VMs	 Initialize Backup of DemoNFSDSD3RP for every 5 minutes B milliopi 	
						View all jobs	
	01		<mark>⊚</mark> 1	01	0		

This provides a powerful solution to handle a tailored and customized disaster recovery plan. Failover can be done as planned failover or failover with a click of a button when disaster occurs and decision is made to activate the DR site.

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

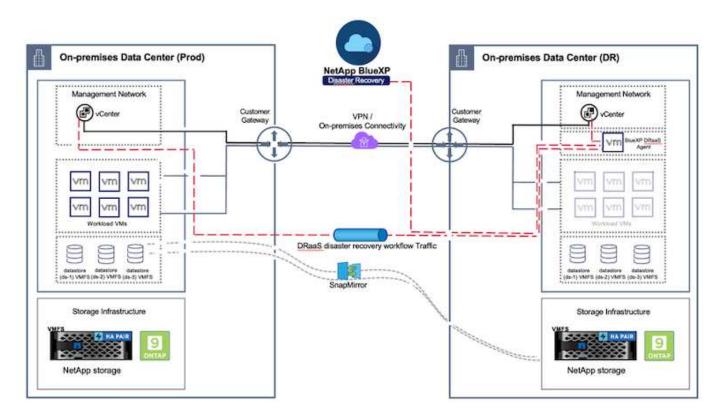
DR using BlueXP DRaaS for VMFS Datastores

Disaster recovery using block-level replication from production site to disaster recovery site is a resilient and cost-effective way of protecting the workloads against site outages and data corruption events, like ransomware attacks. With NetApp SnapMirror replication, VMware workloads running on-premises ONTAP systems using VMFS datastore can be replicated to another ONTAP storage system in a designated recovery datacenter where VMware resides

This section of the document describes the configuration of BlueXP DRaaS to set up disaster recovery for onpremises VMware VMs to another designated site. As part of this setup, the BlueXP account, BlueXP connector, the ONTAP arrays added within BlueXP workspace which is needed to enable communication from VMware vCenter to the ONTAP storage. In addition, this document details how to configure replication between sites and how to setup and test a recovery plan. The last section has instructions for performing a full site failover and how to failback when the primary site is recovered and bought online.

Using the BlueXP disaster recovery service, which is integrated into the NetApp BlueXP console, customers can discover their on-premises VMware vCenters along with ONTAP storage, create resource groupings, create a disaster recovery plan, associate it with resource groups, and test or execute failover and failback. SnapMirror provides storage-level block replication to keep the two sites up to date with incremental changes, resulting in a RPO of up to 5 minutes. It is also possible to simulate DR procedures as a regular drill without impacting the production and replicated datastores or incurring additional storage costs. BlueXP disaster recovery takes advantage of ONTAP's FlexClone technology to create a space-efficient copy of the VMFS datastore from the last replicated Snapshot on the DR site. Once the DR test is complete, customers can

simply delete the test environment, again without any impact to actual replicated production resources. When there is a need (planned or unplanned) for actual failover, with a few clicks, the BlueXP disaster recovery service will orchestrate all the steps needed to automatically bring up the protected virtual machines on designated disaster recovery site. The service will also reverse the SnapMirror relationship to the primary site and replicate any changes from secondary to primary for a failback operation, when needed. All of these can be achieved with a fraction of cost compared to other well-known alternatives.



Getting started

To get started with BlueXP disaster recovery, use BlueXP console and then access the service.

- 1. Log in to BlueXP.
- 2. From the BlueXP left navigation, select Protection > Disaster recovery.
- 3. The BlueXP disaster recovery Dashboard appears.

Storage	,	very Dashboard	Sites Replication plans	Resource groups	Job monitoring	Free trial (55 days left) - View details 🛛 +
Health		-				
Protection		s (2)		Replication plans (3)		Activity
Backup and recov	ey ≙	32 (S) 0	e	⊙1 Ready	() 2 Faired	Backup de for Replication Plan DemotPS04 M a sep
Disaster recovery] 🌣	Deshboard				Initiature Backup of DemoRP004 for every 5 Initiature
Replication.	ŵ	Replication plane		View plans		Backup job for Replication Plan RPVMF503 Secure
Ransomware prote	iction 🕁	Resource groups	21		117	 Invitative Backup of RPVN/FS03 for every 6 microtes 3mage
Oovernance		Job monitoring	Protected VM		Unprotected VMs	Backup job for Replication Plan RPNF5001 Stim igo
Mobility		ew resource groups	View protected VMs		ew unprotected VMs	View all jobs
Extensiona						
		1 Falovers	Palbacks	2 Test fallowers	O Migrations	

Before configuring disaster recovery plan, ensure the following pre-requisites are met:

- BlueXP Connector is set up in NetApp BlueXP. The connector should be deployed in AWS VPC.
- BlueXP connector instance have connectivity to the source and destination vCenter and storage systems.
- On-premises NetApp storage systems hosting VMFS datastores for VMware are added in BlueXP.
- DNS resolution should be in place when using DNS names. Otherwise, use IP addresses for the vCenter.
- SnapMirror replication is configured for the designated VMFS based datastore volumes.

Once the connectivity is established between the source and destination sites, proceed with configuration steps, which should take about 3 to 5 minutes.



NetApp recommends deploying the BlueXP connector in the disaster recovery site or in a third site, so that the BlueXP connector can communicate through the network with source and destination resources during real outages or natural disasters.

0) Disaster recovery	Dashboard	Sites Replication plans	Resource groups	Job monitoring	Free trial (68 days left) - View details
	Sites (2)		Replic	cation plans (2)		Activity
	© 2 Runnling View site Resou Resource	Down	A C C C C C C C C C C C C C C C C C C C		led VMs	Backup job for Replication Plan DemoRPVMFS03 is progress shitlatze Backup of DemoRPVMFS03 for every 10 minutes 7 is spo Discovery of resources in host 172-21160.190 et a spo Failback of resources using the replication plan 'DemoRPVMFS03' 68 is apic Discovery of resources in host 172-21.166.190 win apic
	Saliove	rs 🛛 🔊	1 Failbacks 0	st failovers	0 Migrations	View all jobs

Support for on-premises to on-premises VMFS datastores is in technology preview while writing this document. The capability is supported with both FC and ISCSI protocol based VMFS datastores.

BlueXP disaster recovery configuration

The first step in preparing for disaster recovery is to discover and add the on-premises vCenter and storage resources to BlueXP disaster recovery.



(i)

Ensure the ONTAP storage systems are added to the working environment within the canvas. Open BlueXP console and select **Protection > Disaster Recovery** from left navigation. Select **Discover vCenter servers** or use top menu, Select **Sites > Add > Add vCenter**.

II NetA	pp BlueXP CQ BueXP Search Account ~ Workspace ~ nimopilis	GISAEXPConn
	Disaster recovery Dashboard Sites Replication plans Resource groups Job robritoring	Free trial (55 days left) - View details 🔰 -
0 0	2 stas Add site	Q A55
• •	172_33,300,31 A site is a collection of vCenter servers, either on-premises or in the cloud. Site	Jenn (1)
	nimDemoDe Un-prem	(1)
	Add Cancel	0

Add the following platforms:

• **Source**. On-premises vCenter.

RetApp BlueXP		Connector GISAEXPConn
Oisaster recovery Dashbo	and Sites Replication plans Resource groups Job monitoring	Free trial (55 days left) - View details +
e 2 star	Add vCenter server	Add:
• mimDernoStc • 172,43,306,11 • 172,43,306,11 • 172,43,306,11	Enter connection details for the vCenter server that is accessible from the BlueXP Connector. Site BlueXP Connector InimDemoSrc	Conn (1)
nimQemoDe	vCenter IP address 172.21.166.155 vCenter user name administrator@hmcdc.local	() Seen
	Use self-signed certificates	

• Destination. VMC SDDC vCenter.

NetApp BlueXP	Q BlueXP Search Account ~ Workspace ~ mimopisk mimopisk	GISABXPCenn 🖌 🛵 🏟 😗 🖨
Oisaster recovery Dashb	oard Sites Bioplication plans Resource groups Job monitoring	Free trial (55 days left) - View details +
e 2 sites	Add vCenter server	Add (
• mimDemoSrc	Enter convection details for the vCenter server that is accessible from the BlueXP Connector. Site BlueXP Connector	•
• 172.23.306.0 •	vCenter IP address	Jenn (1)
- amDemoDe	vCenter user name vCenter password	٢
17221.106.11 () Inspire	administrator@hmcdc.local	Seren (3)
	C Use self-signed certificates	
	Add	

Once the vCenters are added, automated discovery is triggered.

Configuring Storage replication between source and destination site

SnapMirror makes use of ONTAP snapshots to manage the transfer of data from one location to another. Initially, a full copy based on a snapshot of the source volume is copied over to the destination to perform a baseline synchronization. As data changes occur at the source, a new snapshot is created and compared to the baseline snapshot. The blocks found to have changed are then replicated to the destination, with the newer snapshot becoming the current baseline, or newest common snapshot. This enables the process to be repeated and incremental updates to be sent to the destination.

When a SnapMirror relationship has been established, the destination volume is in an online read-only state, and so is still accessible. SnapMirror works with physical blocks of storage, rather than at a file or other logical level. This means that the destination volume is an identical replica of the source, including snapshots, volume settings, etc. If ONTAP space efficiency features, such as data compression and data deduplication, are being used by the source volume, the replicated volume will retain these optimizations.

Breaking the SnapMirror relationship makes the destination volume writable and would typically be used to perform a failover when SnapMirror is being used to synchronize data to a DR environment. SnapMirror is sophisticated enough to allow the data changed at the failover site to be efficiently resynchronized back to the primary system, should it later come back online, and then allow for the original SnapMirror relationship to be re-established.

How to set it up for VMware Disaster Recovery

The process to create SnapMirror replication remains the same for any given application. The process can be manual or automated. The easiest way is to leverage BlueXP to configure SnapMirror replication by using simple drag & drop of the source ONTAP system in the environment onto the destination to trigger the wizard that guides through the rest of the process.

RetApp BlueXP	CQ. Bueld Search Montagen	Connector ~ A O O O
Canvas My working environments My estate		🖽 Go to Tabular View
Currugs wy working environments wy estate Add Working Environment Add Working Envinter Add Working Environment Add Working Environment	Anazan 13 O Routine Services (0)	NTAP915_Src () () () () DETAILS On-Premises ON(AP DETAILS On-Premises ON(AP SERVICES () (a) Backup and recovery + On 65,34 om Protected Data () (a) Copy & sync + Of Bync data () (a) Copy & sync + Of Bync data () (a) Thering + On Os Thered data () (a) Copy Strate Thered data () (a) Copy Strate () ()
NTAPOIS_121 On-Premiers On/TAP 8.39178 Casety		Index stating Unavailable (i) (ii) Replication + On 1 Bankingtion Tames (iii) Emer Working Environment

BlueXP DRaaS can also automate the same provided the following two criteria's are met:

• Source and destination clusters have a peer relationship.

(i)

• Source SVM and destination SVM have a peer relationship.

III Ne	tApp BlueXP	Q Buegl' Search Account " Workspace " rimspice	Connector ~ OtSABURConn	0 O
8	Add replication plan	Venter servers V Applications S Resource mapping (a) Recurrence (b) Review		×
٥				
		Source cluster Target cluster vVCSA8-Cluster01 whtdD8-Cluster01		
¢				
		Virtual networks 🥥 Mapped	~	
4		Virtuel machines 📀 Mapped		2
		Datastores	~	
		RPO for all datastores in minutes Recention count for all datastores Required Source datastore Src_AFS_DS01 (svm_NFS-Src_AFS_Vol01) Sirc_NFS_DS01 (svm_nim_nfs_Src_AFS_DS01_co) Transfer scheduli	((RPD) ;;	
		Previous		

If SnapMirror relationship is already configured for the volume via CLI, BlueXP DRaaS picks up the relationship and continues with the rest of the workflow operations.



Apart from the above approaches, SnapMirror replication can also be created via ONTAP CLI or System Manager. Irrespective of the approach used to synchronize the data using SnapMirror, BlueXP DRaaS orchestrates the workflow for seamless and efficient disaster recovery operations.

What can BlueXP disaster recovery do for you?

After the source and destination sites are added, BlueXP disaster recovery performs automatic deep discovery and displays the VMs along with associated metadata. BlueXP disaster recovery also automatically detects the networks and port groups used by the VMs and populates them.

2 sites				۹ 🗖	Add
nimDemoSrc					1
172,21.186,155	72 1948	13 Datashires	1 Hesoarce groups	GISABXPConn Ceinecter	1
nimDemoDest					1
172.21.166.190 ② Headby	61 Vela	3 Datasteres	0 Resource groups	GISABXPConn Connector	1

After the sites have been added, VMs can be grouped into resource groups. BlueXP disaster recovery resource groups allow you to group a set of dependent VMs into logical groups that contain their boot orders and boot delays that can be executed upon recovery. To start creating resource groups, navigate to **Resource Groups** and click **Create New Resource Group**.

O Dis	aster recovery Dashboard	Sites Replication plans Resource grou	ps Job monitoring	Free trial (83 days left) - View details +
	2 resource groups			۹	Add
	Resource group	C Bource site	Source vCenter		3 N
	DemoR001	nimDemoSite	172.21.108.155		
	DemoRGVMF503	nimDemoSre	172.21.166.155		

The resource group can also be created while creating a replication plan.

(i)

The boot order of the VMs can be defined or modified during the creation of resource groups by using simple drag and drop mechanism.

NetApp Blu	юХР	Q BlueXP Searc	h Account " Workspace nimogisk nimspace	Connector GISABXPCon	.č 4₀ ≎ 0 0
e 💮 Dis	aster recovery Dear	Add resource group			n trial (B3 days left) - View details 📋 +
•	1 resource groups	Name DemoRGVMF503	vCenter 172.21.166.155 ==		a
9	DermiRGOT	Select virtual machines	Selected VMs (5)	_	
*		BCSI_DemoVM01 BCSI_DemoVM03 ISCSI_DemoVM03 ISCSI_DemoVM02	ISCSI_DemoVM01	×	
		iSCSLDemoVM04 iSCSLDemoVM05	ISCSI_DemoVM04	×	
			Use diag and drop term to modify the boot order		
			Add	Cancel	
			Add	Cancel	

Once the resource groups are created, the next step is to create the execution blueprint or a plan to recover virtual machines and applications in the event of a disaster. As mentioned in the prerequisites, SnapMirror replication can be configured beforehand or DRaaS can configure it using the RPO and retention count specified during creation of the replication plan.

P (a) Carivas My working environme	My estate	I Go to Tabular Vie
+ Add Working Environment	C Enable Services ()	Working Environments
	NTAP915_Brc On-Premiums ONTAP	3 On-Premises ONTAP 11.16 Till Provisioned Capacity
Real	201Ti8 CaseOy	Amazon 53 A Buckets
Repl	cation	
NTAP915_Destn On-Promises ONTAP 1.26T/8 Cepecity	Amazon S3	
Capacity	Buckets	
	NTAP915_127 On-Premises ONTAP	

Replication			ninogist	nimspace	GISABXPCo	nn 🍓 🕈 😗
6	Aume Relationships	495.27 GiB Replicated Capacity	O Currently Transfer	ing 🤇	6 Healthy	⊗ 0 Failed
Volume Relation	ships (6)					a C
Health Status	† Source Volume	C Target Volume	💲 🛛 Total Transfer Time 🗘	Status 1	F Mirror State	: Last Successfu
Ø	DRad5_arc NTAP915_Src	DRas5_src_copy NTAP915_Destn	5 seconds	ide	snapmirrored	Jul 15, 2024, 8:05:05 28:41 M/B
0	Src_NFS_D503 NTAP915_Src	Src_NFS_DS03_CP NTAP915_Destn	13 seconds	ide	snapmirrored	Jul 15, 2024, 8:07:13 183.41 MB
\odot	Src_NFS_DS04 NTAP915_Src	Src_NFS_DS04_CP NTAP915_Destn	6 seconds	ide	snapmirrored	Jul 15, 2024, 8:05:06 183.38 Mil
\odot	Srtt_NFS_Vol01 NTAP915_Src	Src_NFS_DS01_cp NTAP915_Destri	14 seconds	ide	snapmirrored	Jul 15, 2024, 8:43:22 546.23 MB
0	Src_JSCSI_DS01 NTAP915_Src	Src_ISCSI_DS01_cp NTAP915_Destri	20 seconds	idie	snapmirrored	Jul 12, 2024, 4:24:34 22:35 MiB
0	Sre_ISCSI_DS03 NTAP915_Src	Src_iSCSI_DS03_CP NTAP915_Destn	6 seconds	idle	snapmirrored	Jui 15, 2024, 8:05:06 254.89 MiB

Configure the replication plan by selecting the source and destination vCenter platforms from the drop down and pick the resource groups to be included in the plan, along with the grouping of how applications should be restored and powered on and mapping of clusters and networks. To define the recovery plan, navigate to the **Replication Plan** tab and click **Add Plan**.

First, select the source vCenter and then select the destination vCenter.

M Ne	tApp BlueXP		Q BlueXP See	ch Account ~	Workspace 😁 nimspace	Connector GISABXPConn	۰ 🐟	0 B	
	Add replication plan	1 vCenter servers	(2) Applications	3 Resource mapping	(4) Recurrence	3 Roview		×	
ø		-							Ĩ
٠		Replication plan name DemoRPVMES03							1
Ŷ		A second a second second second							
0									
-		 Select a source vCenter where y 	rour data exists, to repl	licate to the selected target vC	lecter,				
			5						
			ลี เ	Replicate	1				
			9	Targe	t vCenter				
		Source vCenter 172.21.166.155	-	Baie	act a target vCenter	*			
			1. J.	1 million 2	2.21.166.155 DemoSrc				
					221.166.190				4
			Cance	i i i i i i i i i i i i i i i i i i i	DemoDest				

The next step is to select existing resource groups. If no resource groups created, then the wizard helps to group the required virtual machines (basically create functional resource groups) based on the recovery objectives. This also helps define the operation sequence of how application virtual machines should be restored.

III Ne	etApp BlueXP	Q BueXP Search Account " Workspace " Connector " Q nimopisa nimopoce GISABXPConn " Q	•	0	θ
4 D • G 9	Add replication plan				×
3		Previous			

Resource group allows to set boot order using the drag and drop functionality. It can be used to easily modify the order in which the VMs would be powered on during the recovery process.

(;)



Each virtual machine within a resource group is started in sequence based on the order. Two resource groups are started in parallel.

The below screenshot shows the option to filter virtual machines or specific datastores based on organizational requirements if resource groups are not created beforehand.

ILING	tApp BlueXP		ccount 👋 Workspace 🎽 Connector 🎽 🌲 🍄 🥹 😆
	Add replication plan	🕑 vCenter servers 👩 Applications ③ Resource mapping	(Recurrence B Review X
ø		Applications Select the applications on the source v Center that you	
		station on additionation of our address of the bull	a man na ar taga pana.
¢		(a) 172.21.186.155	172.21.166.190 nimDenisDest
4		Datastare All datastores + Q. Sales & December Bissources	
		Previous	

Once the resource groups are selected, create the failover mappings. In this step, specify how the resources from the source environment maps to the destination. This includes compute resources, virtual networks. IP customization, pre- and post-scripts, boot delays, application consistency and so on. For detailed information, refer to Create a replication plan.

Add replication plan	0	VCenter servers	Applications	0	esource mapping	Recurrence	rview		
	Virtual machines							<u>^</u>	
	P address type	Target IP							
	Static	· Same as	source -						
	Use the same or	edentials for all VMs							
	Use the same sp	ript for all VMs							
	Q								
	Source VM	CPUs	RAM		Boot delay(mins between 0 and 10)	Create application consistent replicas	Scripts		
	DemoR001								
	50_DemoVM	2	34	Giß ~	0		None 🥜		
	\$0_DemoVM01	2	4	Gill ~	0	o	None 🖉		
	50_DemoVM02	2	4	Ga ~	0	0	None Ø		

By default, same mapping parameters are used for both test and failover operations. To apply different mappings for test environment, select the Test mapping option after unchecking the checkbox as shown below:

	Add replication plan	Ø vCenter server	s 🕑 Applications 📢	Besource mapping	(4) Recurrence	(6) Review	×
۵	Replication plan 3 Add plan						
٠				arce mapping			
¢			specty new resources	nap from the source to the	i urgit.		
0	((m) 172.21.186.156 AmDemoSirc	_			(m) 172.21.166.190	
-						U	
		Use same mappings for failover and tes					
		une serie megange for terowic and me	(mapping a				
		allover mappings Test mapp	ings -				

Once the resource mapping is complete, click Next.

(i)

Add replication plan	🔗 vCenter ser	vers 🕑 Applications 🔞 Resource	mapping (4) Recurrent	ar (5) Raview		
	172.21.166.165 nimDemoSirc			172.21.186.190 nimDemoDest		
	Use same mappings for fi	linear and test manuface			-	
	Service and the stage of the service	and and man mappings				
	Failover mappings	Test mappings				
				Ų		
	Failover mappings	Test mappings		- - 		

Select the recurrence type. In simple words, select Migrate (one time migration using failover) or recurring continuous replication option. In this walkthrough, Replicate option is selected.

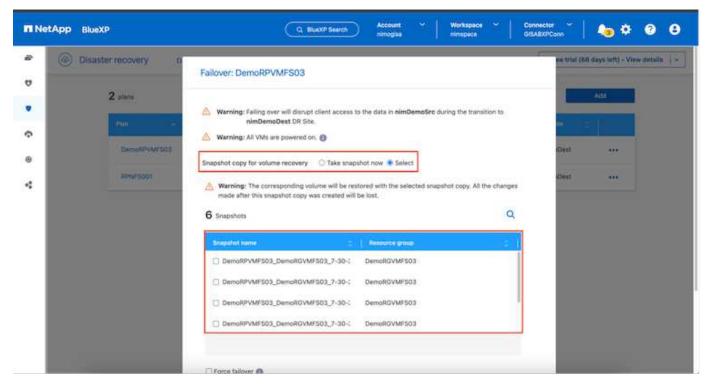
Add replication plan	🕑 sCentr	r servers 🕢 Application	ns 🕜 Resource map	ping Recurrence	5 Review		
	172.21.166.11 nim/DemoSirc	55		÷	172.21.166.190 niniDemaDest		
				6	-		
		Migrate Migrate application data one source to target	time them . Bepla	Replicate are application data to keep the ta sp-te-data with the source.	n (Jana)		

Once done, review the created mappings and then click on Add plan.

NetApp BlueXP	0.000	Q BlueXP Search Account rimopha	Workspace Connector nimpace GISAEXPConn	4 9 *	0 0
Add replication plan	VCenter servers	Applications Resource mapping	Recumunce Review		>
	172.21.106.155 nimDemoSirc		172.21.166.190 rimDemaDest	ň	
	Plan details	Fallover mapping	Virtual mechines		
	Plan name	DemoRPVMFS03			
	Recurrence	Replicate			
		Previous Add plan			

2 plans						۹	Add
Pan 🔹	Compliance check	Plan status	Protected alte	Resource groups	Recurrence :	Failurer site	2 () ()
OemoRPVMF503	Healthy	@ Ready	nimDemoSrc	Demo#GVMFS03	Replicate	nimDemoDest	
RPNES001	Healthy	Ready	nimDemoSrc	DemoRG01	Replicate	nimDemoDest	

Once the replication plan is created, failover can be performed depending on the requirements by selecting the failover option, test-failover option, or the migrate option. BlueXP disaster recovery ensures that the replication process is being executed according to the plan every 30 minutes. During the failover and test-failover options, you can use the most recent SnapMirror Snapshot copy, or you can select a specific Snapshot copy from a point-in-time Snapshot copy (per the retention policy of SnapMirror). The point-in-time option can be very helpful if there is a corruption event like ransomware, where the most recent replicas are already compromised or encrypted. BlueXP disaster recovery shows all available recovery points.



To trigger failover or test failover with the configuration specified in the replication plan, click on **Failover** or **Test failover**.

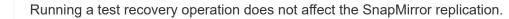
• 6	0.0	1	ishboard Sites		and the second second	n ye na ye han ba		Records	design and the second	aver re
	Disast Disast	ter recovery b	ishboard Sites	Replication p	alans Resource gro	ups Job monitoring		Free trial (68	days left) - View	details -
		2 plans						۹ 🗖	Add	
		Pan 🖉	Constance check	Plan status	Protected site	Resource groups	Recurrence	- Falcourabe		
		DemoRPVMF503	Healthy	Ready	nimDemoSrc	DemoRGVMFS03	Replicate	nimDemoDest.		
		RPNF5001	Healthy	🕑 Ready	nimDemoSrc	DemoRG01	Replicate	View plan detail ni Run compliance Test failover		
								Corrup false Fail over	CHAT:	
								Feit back Edit schedules		
								Take snapshot n Disable	ow	
								Drutte		

What happens during a failover or test failover operation?

During a test failover operation, BlueXP disaster recovery creates a FlexClone volume on the destination ONTAP storage system using the latest Snapshot copy or a selected snapshot of the destination volume.



A test failover operation creates a cloned volume on the destination ONTAP storage system.



(;

T Ne	tApp BlueXP		Connector GISABXPConn
	Disaster recovery Deat	board Silies Replication plans Resource groups Job monitoring	Pres trial (BB days left) - View details 🕴 -
۵			
	2 states	Test failover: DemoRPVMFS03	A00
¢	PSH		
	DecoRPyMF503	OR Test Fallover Update Mirror	oOust
4	Realition	SrapMirror relationship for volume :svm_ISCSI:Src_ISCSI_D503 Destination volume 'Src_ISCSI_D503_CP': size is less than source volume :'Src_ISCSI_D503': size SrapMirror relationship is healthy for volume :svm_ISCSI:Src_ISCSI_D503	eDest ***
		Destination storage environment found for volume :svm_JSCSISrc_JSCSI_0503 Take snapshot now option is not selected, primary backup & snapmirror update not performed.	
		OR Test Failover Target Start	
		Run in background	

During the process, BlueXP disaster recovery does not map the original target volume. Instead, it makes a new FlexClone volume from the selected Snapshot and a temporary datastore backing the FlexClone volume is mapped to the ESXi hosts.

m <u>9 3</u> 8	d la a enconnella	cal Factions Permissions Datacenters			Administration@HMCDCLC	ocal	@~ • ···
 Wkid04-vc01/hmcdc.local Wkid04-DC01 04TestBed_DS01 ISODump Wkid04_Dstn_DS01 	vCenter Details Version: Build: Last Updated: Last Fiel-Based Backup: Cluster: Heats: Virtual Machines:	8.0.2 22385739 May 20, 2024, 3121 AM Not schedung 1 2 61	Capacity and Usage Last updated at 31% AM CPU CU CU Software Storage Storage Storage	2	73.44 4 5859	E CHL chee CHL cheer CHL cheer	0
	Tags II	Custom Attributes		11	vCenter Health	ц	
V Recent Tasks Alarms							
Task Name y Tarpel	Y Statue Y	Detalo Y	isitiator y Ou	wind w	Start Time 🚽 🔻	Completion Time	- T - H
Rescan VMPS	O4-esyl/thmsd		HACDCLOCAL\Administrator 2 (mi.	07/30/2024, 3:22:47 A M	07/30/2024, 3:22-4 M	17.A WE
	O4-exc0.tmcd Completed		HMCDCLOCAL\Administrator 31	ns.	07/30/2024;222;47;4 W	01/09/2924, 3:22-4 M	and the second se

				Hosts &	Administrator BHMCDCLOCAL Kosts & Clusters VHs Detestores Networks Linked vCenter Serve Capacity and Usage Last votated at 323 AM CPU 72.06 GHz H LT9 GHz used 73.44 GHz case Memory 485.84 GH Storage 39.110 H Storage 39.110 H Storage 41.12 case			, () () () () () () () () () () () () ()
								0.1
	Tags	П	Custom Attributes			11	vCenter Health ^{II}	
Pecent Tasks Alarms								
Task Name Tarpel	T Statue	۲	Detale T	avhator -	τ Oue For	ved T	Blact Time 4 Y Completion Time	- T P
Register Virtual machine El	-	20% ()	Registering Virtual Hachine o In destination host	System	20	ns.	07/30/2024, 3:23:43 A M	***
Register untual machine 🛛 wkxd04-DCD	-	20%	Registering Virtual Machine o In destination hust	System	9.8	-	07/30/2025/347/5h6 Windows	

When the test failover operation completes, the cleanup operation can be triggered using "**Clean Up failover test**". During this operation, BlueXP disaster recovery destroys the FlexClone volume that was used in the operation.

In the event of real disaster event occurs, BlueXP disaster recovery performs the following steps:

- 1. Breaks the SnapMirror relationship between the sites.
- 2. Mounts the VMFS datastore volume after resignature for immediate use.
- 3. Register the VMs
- 4. Power on VMs

II NetAp	P BlueXP		Connector 🎽 👍 🌣 📀 🖨
*	Disaster recovery Dente	oard Sites Replication plans. Resource groupe Job monitoring	Free trial (0.0 days left) - View details 🕴 -
۳	a 1957		A00
	2 stars	Failover: DemoRPVMFS03	
Ŷ	Pin -	IR Failover Target Start	
	DeconPvM/503	Breaking SnapMirror relationship for volume - Src_ISCSI_DS03. Using anapshot id Baf61dab- 87cd-42b2-bdee-cbe91e8c9aa2	400att +++
4	Revenues	Mounting volume - Src_ISCSI_DS03 - In datastore - Src_ISCSI_D503	etDest +++
		Registering VM - ISCSI_DemoVM03	
		Registering VM - iSCSI_DemoVM04	
		 Registering VM - iSCSI_DemoVM01 	
		Registering VM - ISCSI_DemoVM05	
		Powering on VM - ISCSI_DemoVM03	
		Close	

Once the primary site is up and running, BlueXP disaster recovery enables reverse resync for SnapMirror and enables failback, which again can be performed with the click of a button.

	Q BueXP Search Account ~ Workspace ~ rimograa	Connector 🖌 👆 🦣 🌣 🧿 🔒
Disaster recovery Dust	ooand Silles Replication plans Resource groups Job monitoring	Free tital (Ibli days left) - View details 🕴 -
2 plans	Failover: DemoRPVMFS03	<u>A66</u>
•	 Powering off VM - ISCSL_DemoVM02 	
DecoliPvM/503	 Powering off VM - iSCSi_DemoVM04 	eCent •••
RP#/5001	Powering off VM - ISCSI_DemoVM05	eOest +++
	 Powering off VM - iSCSL_DamoVM01 	
	 Reversing SnapMirror relationship for volume – Src_ISCSI_DS03 	
	O DR Failover Control	
	 All resources in this resourcegroup DemoRGVMFS03 are in the same volume 	
	Close	

And if migrate option is chosen, it is considered as a planned failover event. In this case, an additional step is triggered which is to shut down the virtual machines at the source site. The rest of the steps remains the same as failover event.

From BlueXP or the ONTAP CLI, you can monitor the replication health status for the appropriate datastore volumes, and the status of a failover or test failover can be tracked via Job Monitoring.

NetApp	BlueXP			ogise Workspa nimspaci		🍐 💩 🍄 📀 🤤
•	Disaster recovery Dashbo	ard Sites Replicatio	n plans Resource groups	Job monitoring	Free trial	(68 days left) - View details -
,	Last 24 hours 🖤				C Last updated: July	y 30, 2024, 11:52 AM
•	O Jobs	0 Success	O In progress View jobs	0 III Queued	0 Warning	O Failed
	\bigcirc	A NEW TOTAL	A MERI DOM	Viewjobs	view jour	view jobs
	11102 jobs					Q
	10 (a) (a)	Status : Workhold :	Martin	a Sinth	ne) ; { Endlime	
	() 2963d7f3-7eb0-475d	Success Discovery	Discovery of resources in t	ost 172.21.166 07/30/2	1024, 11:52: 07/30/2024, 11	:52:
	() 17ea7c0c-90d8-49b2	Success DRFailback	Failback of resources using	the replication 07/30/2	024, 11:49: 07/30/2024, 11	
	1 47115c12-1e97/48ce-	Success Discovery	Discovery of resources in I	ost 172.21.166	024, 11:43: 07/30/2024, 11	.44

This provides a powerful solution to handle a tailored and customized disaster recovery plan. Failover can be done as planned failover or failover with a click of a button when disaster occurs and decision is made to activate the DR site.

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

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.