



# **NetApp Hybrid Multicloud with VMware**

## NetApp Solutions

NetApp  
August 05, 2022

# Table of Contents

NetApp Hybrid Multicloud with VMware Solutions . . . . .	1
VMware for Public Cloud . . . . .	1
VMware Hybrid Cloud Use Cases . . . . .	136
NetApp Hybrid Multicloud Solutions for AWS / VMC . . . . .	138
NetApp Hybrid Multicloud Solutions for Azure / AVS . . . . .	220
NetApp Hybrid Multicloud Solutions for GCP / GCVE . . . . .	263

# 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

##### 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.

NOTE:

NetApp storage as a datastore is currently available as Public preview for AWS/VMC and Azure/AVS and Private preview for GCP/GSVE. Please visit the following links for more information.

AWS press release for FSx ONTAP as a native datastore COMING SOON!

[Azure NetApp Files \(ANF\) as a native datastore for Azure](#)  
[Cloud Volumes Service \(CVS\) as a native datastore for GCP](#)

#### 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, Cloud 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.

### NOTE:

NetApp storage as a datastore is currently available as Public preview for AWS/VMC and Azure/AVS and Private preview for GCP/GSVE. Please visit the following links for more information.

AWS press release for FSx ONTAP as a native datastore COMING SOON!

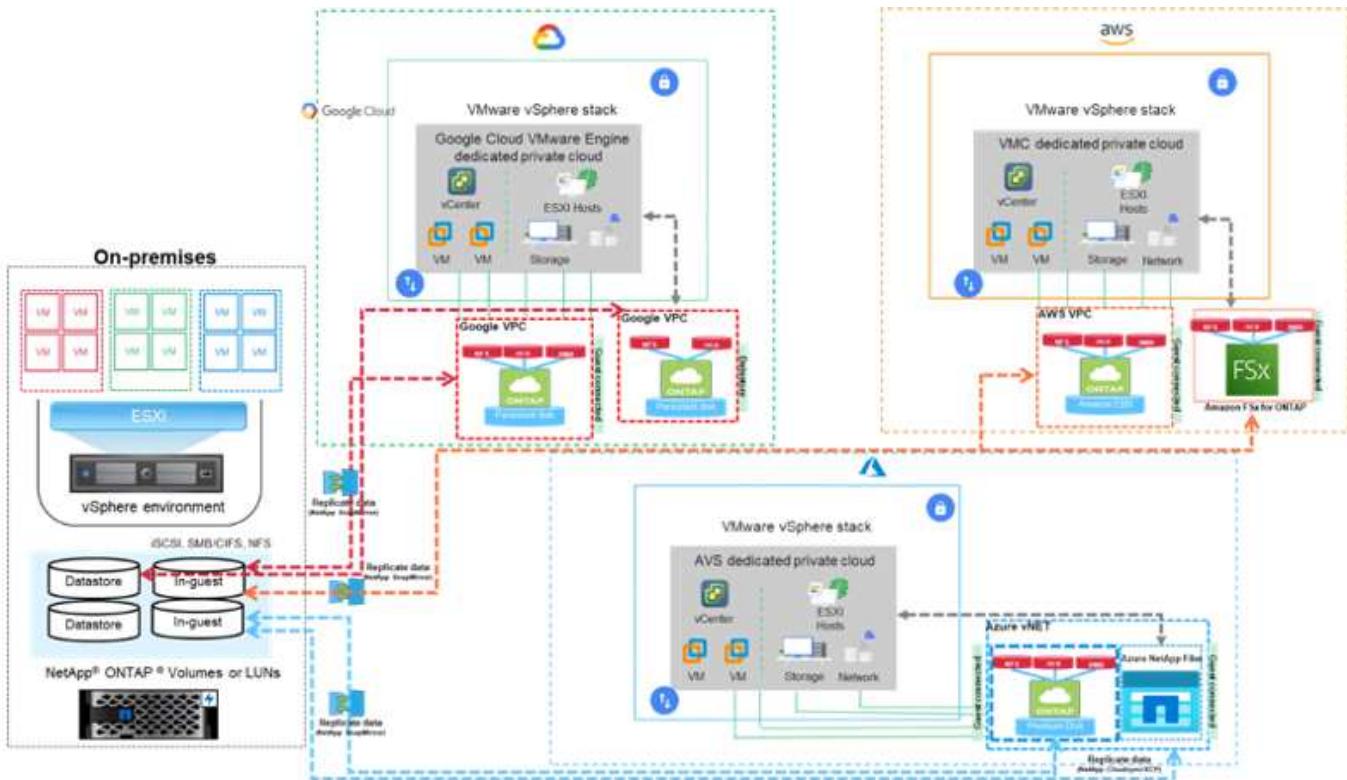
[Azure NetApp Files \(ANF\) as a native datastore for Azure](#)  
[Cloud Volumes Service \(CVS\) as a native datastore for GCP](#)



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 native datastore to migrating workflows, extending/bursting to the cloud, backup/restore and disaster recovery.

Pick your cloud and let NetApp do the rest!



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 production-ready 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 FSx ONTAP and 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 Azure NetApp Files and 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 native 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 native datastore<sup>1</sup>

View the detailed [guest connect storage options for VMC](#).



1 - FSxN for VMC is currently in IA (Initial Availability). Contact your NetApp sales representative for more information.

## 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 native datastore<sup>1</sup>

View the detailed [guest connect storage options for AVS](#).



1 - ANF as a native datastore for AVS is currently in Public Preview. Read more about it [here](#).

## 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 native datastore<sup>1</sup>

View the detailed [guest connect storage options for GCVE](#).

Read more about [Cloud Volumes Service \(CVS\) as a native datastore<sup>1</sup>](#).



1 - Currently in Private Preview

## 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.

	<b>Guest Connected</b>	<b>Native Datastore</b>
<b>AWS</b>	CVO FSx ONTAP <a href="#">Details</a>	FSx ONTAP Information coming soon! <sup>1</sup>
<b>Azure</b>	CVO ANF <a href="#">Details</a>	ANF <a href="#">Details</a> <sup>2</sup>
<b>GCP</b>	CVO CVS <a href="#">Details</a>	CVS <a href="#">Details</a> <sup>3</sup>

NOTE:

1 - Currently in Initial Availability (IA)

2 - Currently in Public Preview

3 - Currently in Private Preview

## 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 FSx ONTAP and 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 Azure NetApp Files and 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 FSx ONTAP and Cloud Volumes ONTAP to AWS VMC.

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

## Deploy and configure VMware Cloud for AWS

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 the only supported method of connecting Amazon FSx for NetApp ONTAP and Cloud Volumes ONTAP to VMware Cloud on AWS.

The setup process can be broken down into three parts:

### Register for an AWS Account

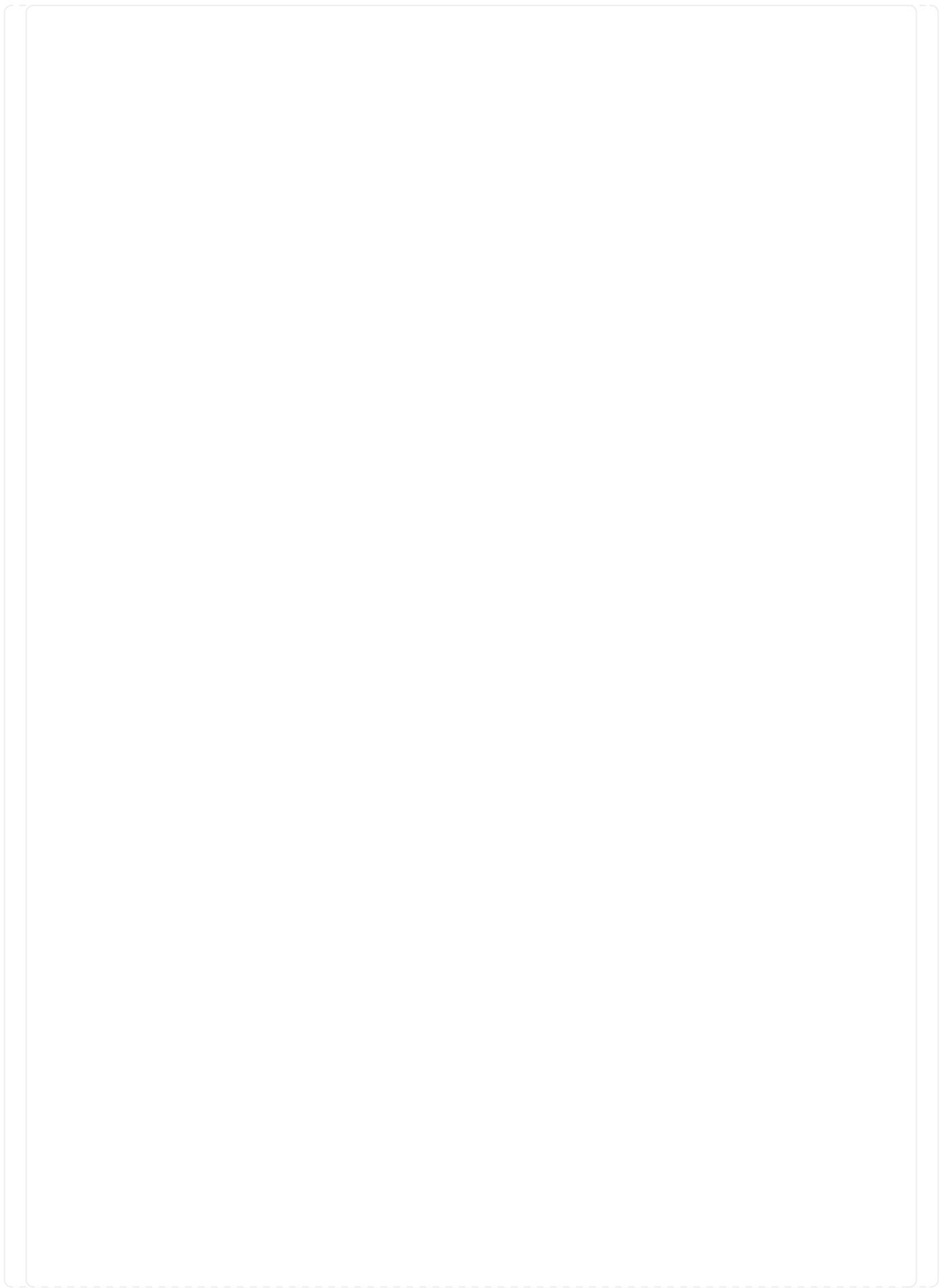
Register for an [Amazon Web Services Account](#).

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.

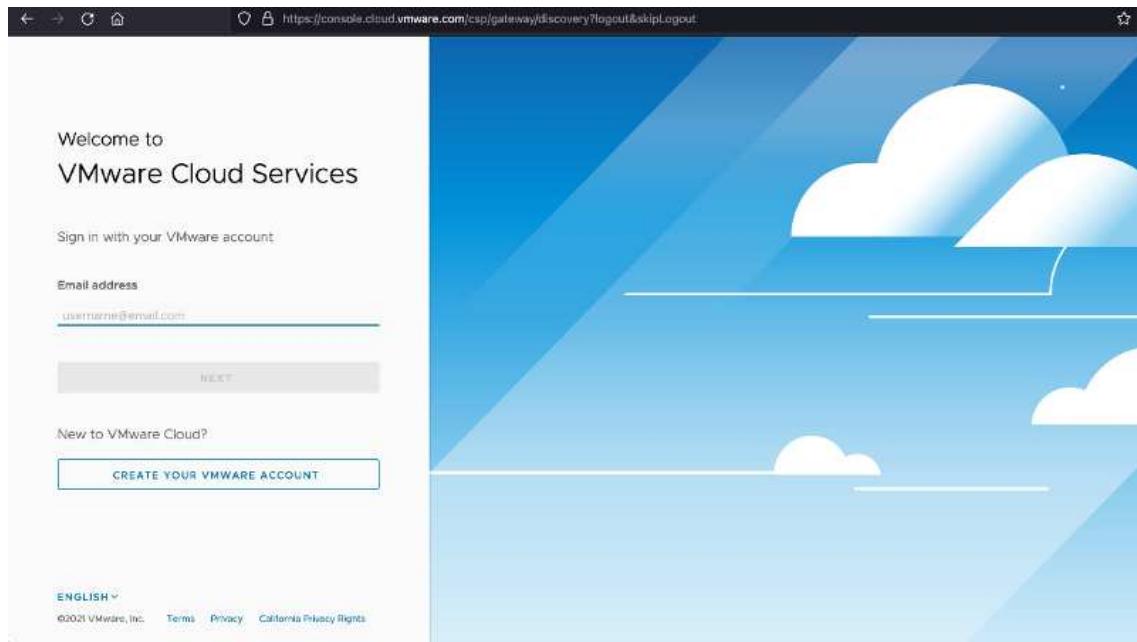
For access to VMware's cloud portfolio (including VMware Cloud on AWS), you need a VMware customer account or a My VMware account. If you have not already done so, create a VMware account [here](#).



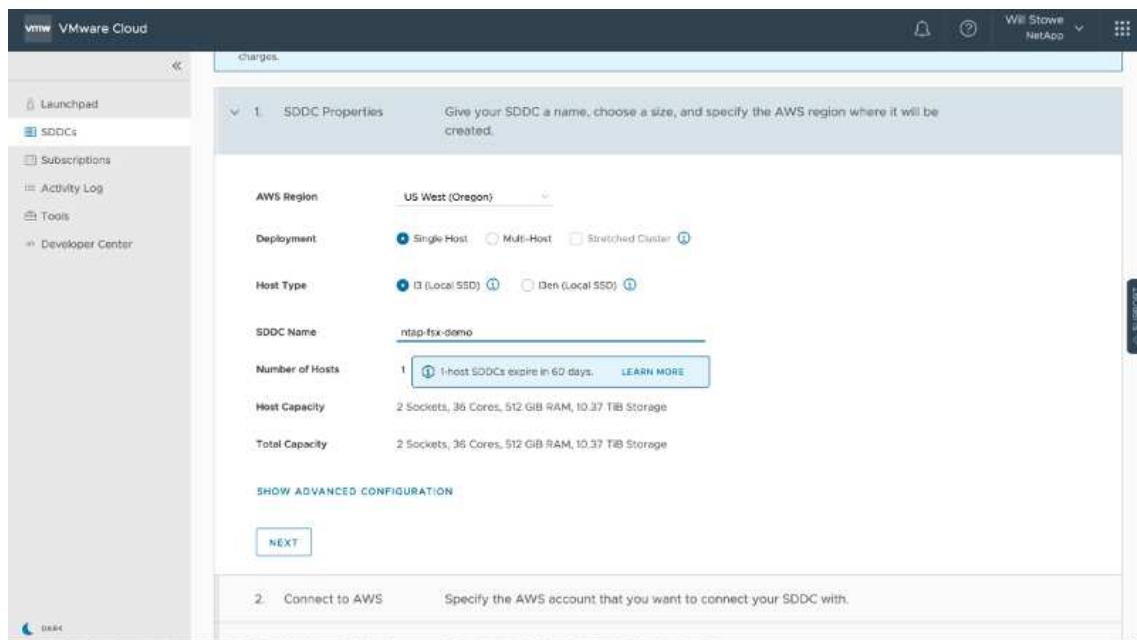
## Provision SDDC in VMware Cloud

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.



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



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

CloudFormation > Stacks > Create stack

## Quick create stack

**Template**

Template URL: <https://vmware-sddc.s3.us-west-2.amazonaws.com/1eb9d184-a706-4489-abb8-692aad0e25d0/mq5ijphtleoh85b75tegq9icc4bddd7ifq07nv716fk36>

Stack description: This template is created by VMware Cloud on AWS for SDDC deployment and maintenance. Please do not remove.

**Stack name**

Stack name: vmware-sddc-formation-a87f51c9-e5ac-4bb4-9d1e-9a3dahd197b7

Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-).

**Parameters**

Parameters are defined in your template and allow you to input custom values when you create or update a stack.

**Stack name**

Stack name: vmware-sddc-formation-a87f51c9-e5ac-4bb4-9d1e-9a3dahd197b7

Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-).

**Parameters**

Parameters are defined 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

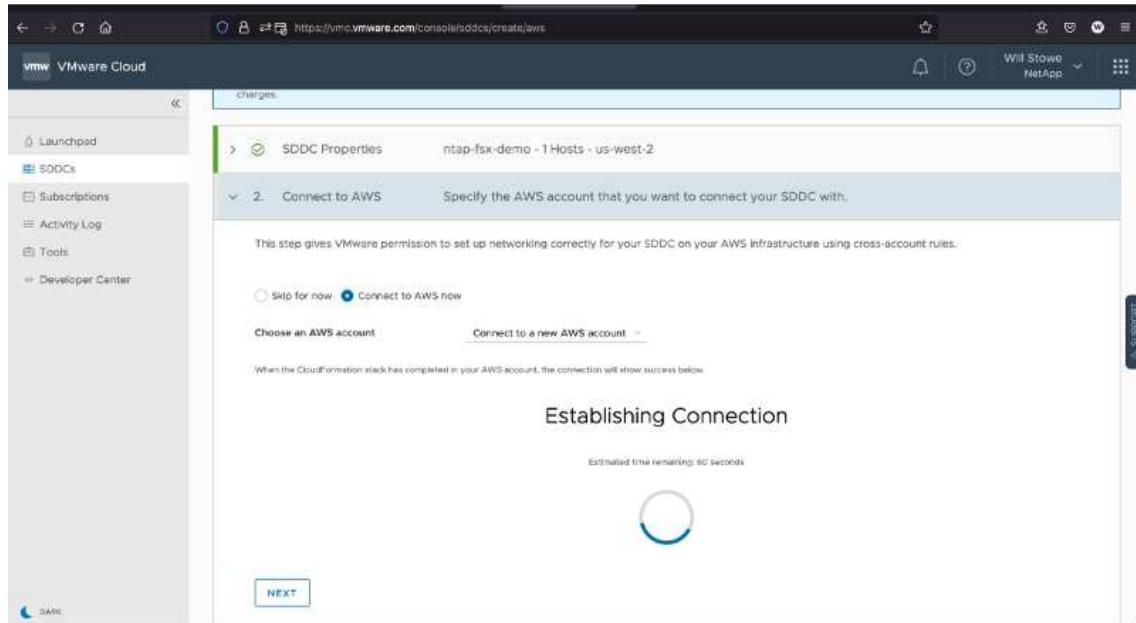
**Capabilities**

**ⓘ The following resource(s) require capabilities: [AWS::IAM::Role]**

This template contains Identity and Access Management (IAM) resources that might provide entities access to make changes to your AWS account. Check that you want to create each of these resources and that they have the minimum required permissions. [Learn more](#)

I acknowledge that AWS CloudFormation might create IAM resources.

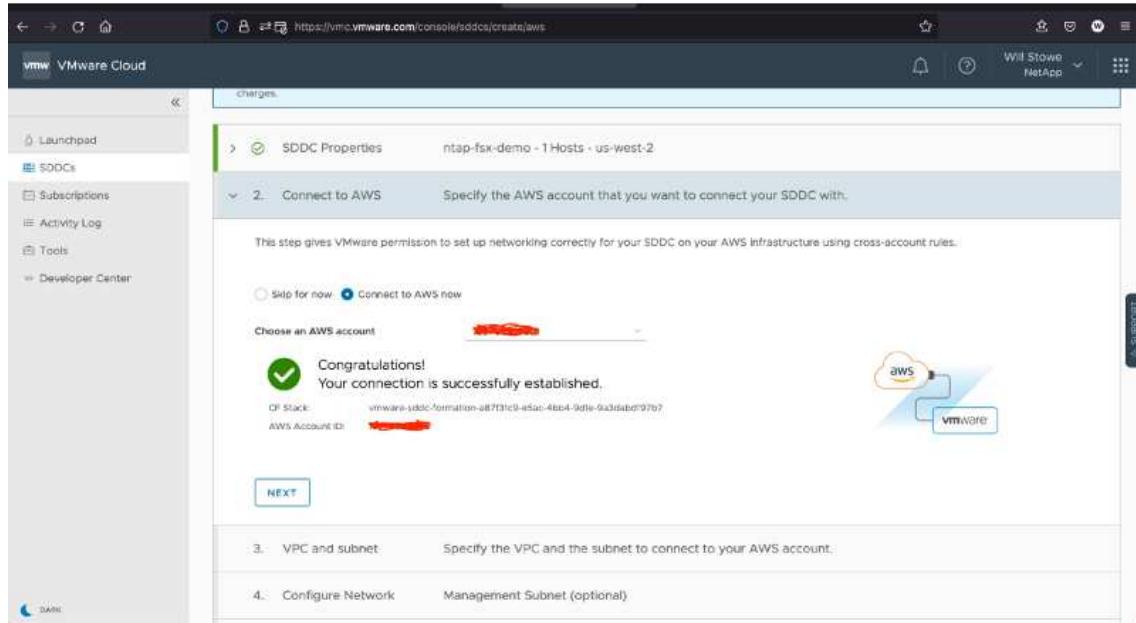
[Cancel](#) [Create change set](#) [Create stack](#)



Establishing Connection

Estimated time remaining: 60 seconds

**NEXT**



Congratulations!  
Your connection is successfully established.

OF Stack: vmware-iddc-formation-a87731c9-e5ac-4bb4-9dfc-9a3dab097b7  
AWS Account ID: [REDACTED]

**NEXT**

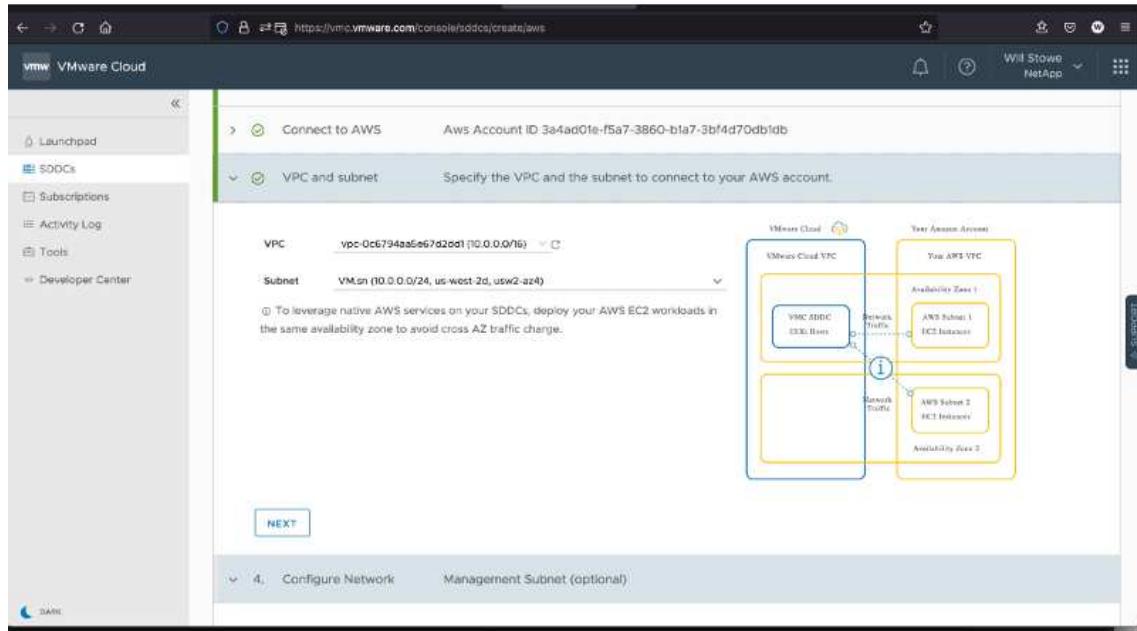
3. VPC and subnet: Specify the VPC and the subnet to connect to your AWS account.

4. Configure Network: Management Subnet (optional)

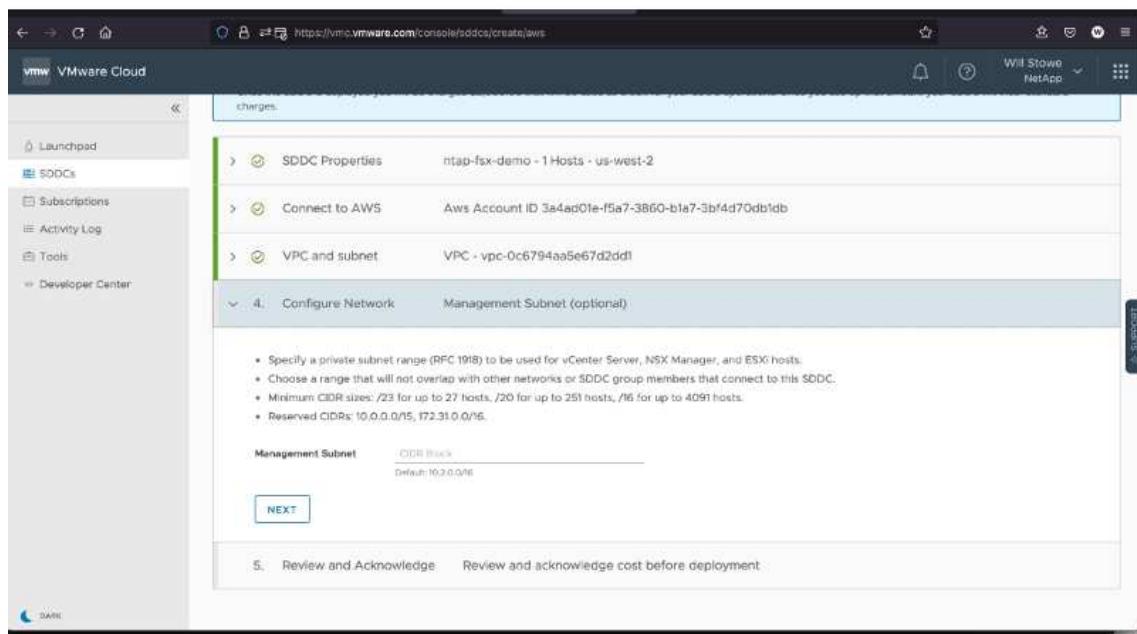


Single-host configuration is used in this validation.

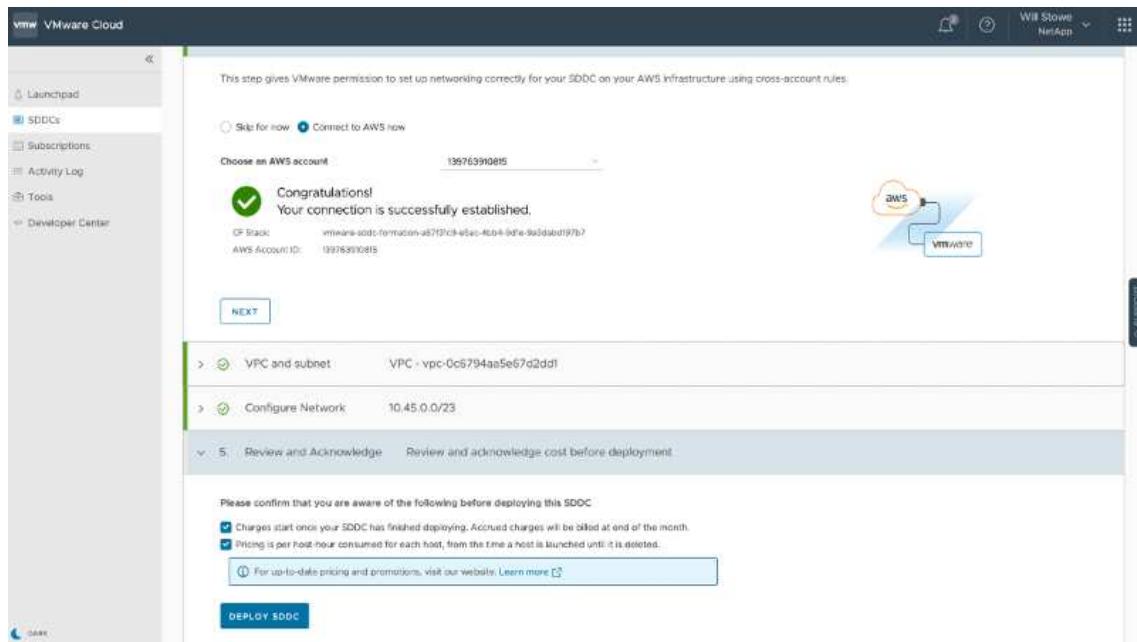
4. Select the desired AWS VPC to connect the VMC environment with.



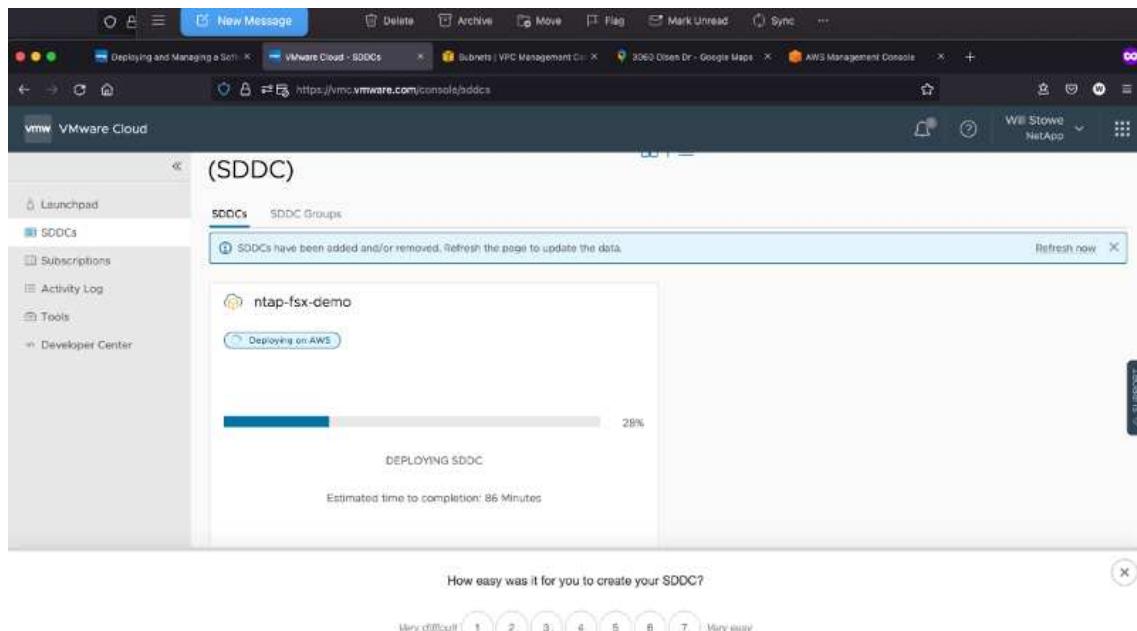
5. Configure the VMC Management Subnet; this subnet contains VMC-managed services like vCenter, NSX, and so on. Do not choose an overlapping address space with any other networks that need connectivity to the SDDC environment. Finally, follow the recommendations for CIDR size notated below.



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



The deployment process typically takes approximately two hours to complete.



7. After completion, the SDDC is ready for use.

Software-Defined Data Centers (SDDC)

ntap-fsx-demo

Ready | Expires in 60 days

Region	US West (Oregon)	Clusters	1
Type	VMC on AWS SDDC	Hosts	1
Availability Zones	us-west-2a, us-west-2b, us-west-2c	VMs	36

CPU	Memory	Storage
82.8 GHz	512 GiB	10.37 TiB

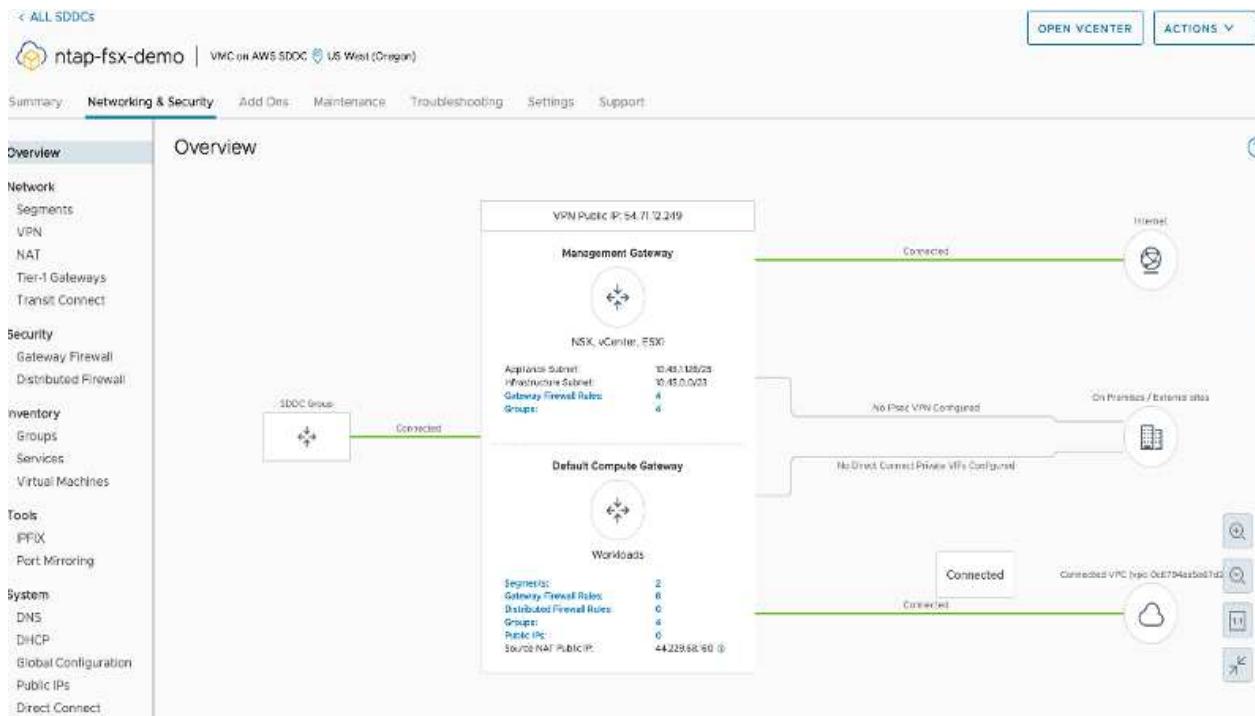
VIEW DETAILS | OPEN VCENTER | ACTIONS

For a step-by-step guide on SDDC deployment, see [Deploy an SDDC from the VMC Console](#).

## Connect VMware Cloud to FSx ONTAP

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

1. 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.

VMware Cloud

Create SDDC Group

1. Name and Description

Name: sddcgroup01

Description: sddcgroup01

**NEXT**

2. Membership

Members: 1

3. Acknowledgement

Please confirm that you are aware of the following before creating this SDDC Group.

Configuring VMware Transit Connect for your group will incur charges per attachment and data transfers.

Create firewall rules to establish connectivity between the SDDCs in the group. [Learn More](#)

**CREATE GROUP**

VMware Cloud

Create SDDC Group

1. Name and Description

Name: sddcgroup01

2. Membership

Select SDDCs to be part of your group.

Name	UUID	Location	Version	Management CIDR
intap-px-demo	829a6e22-92a1-42db-ad03-9e4eb7a908b6	US West (Oregon)	1.14.0.14	10.45.0.0/23
1				

**NEXT**

3. Acknowledgement

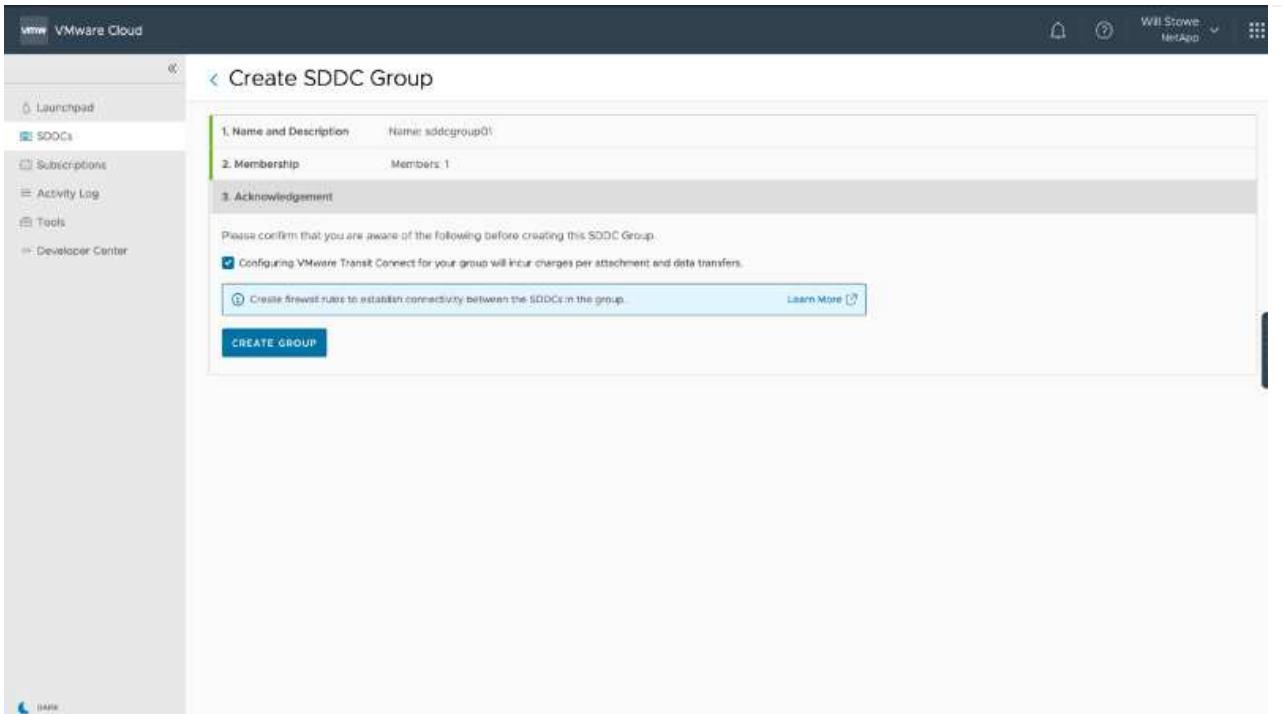
Review and acknowledge requirements before creating the group.

Please confirm that you are aware of the following before creating this SDDC Group.

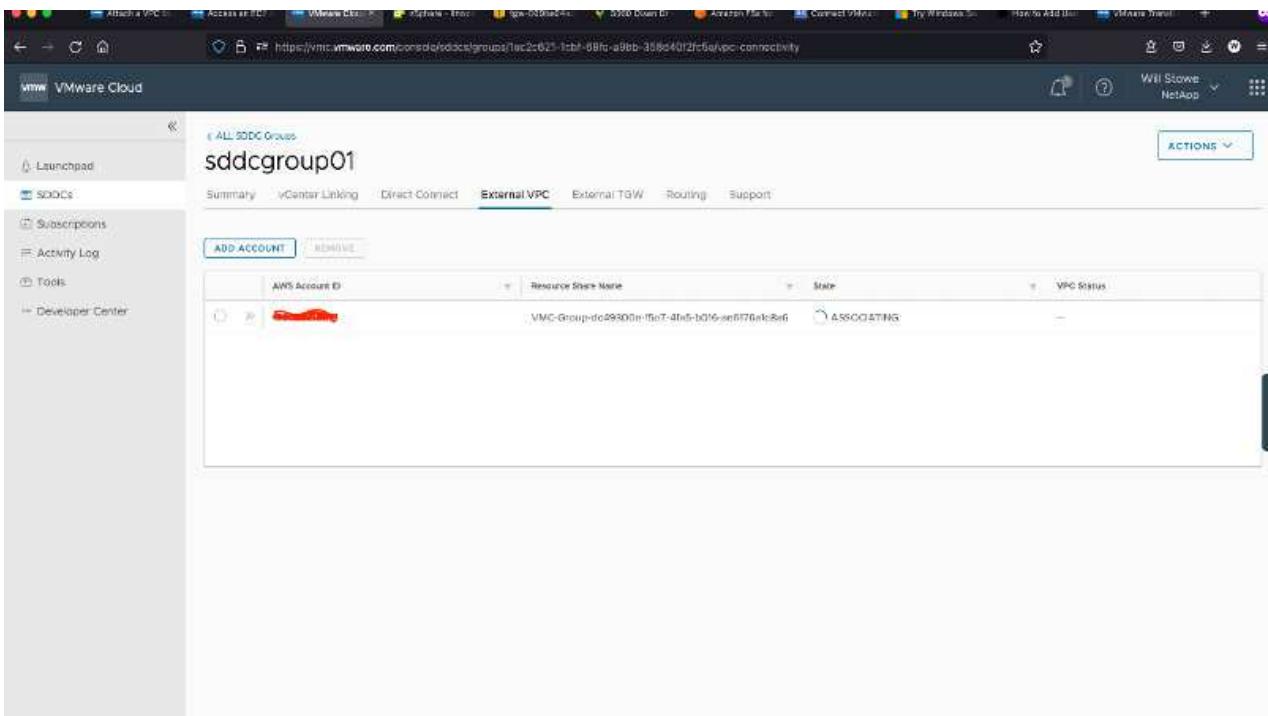
Configuring VMware Transit Connect for your group will incur charges per attachment and data transfers.

Create firewall rules to establish connectivity between the SDDCs in the group. [Learn More](#)

**CREATE GROUP**



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.



The screenshot shows the VMware Cloud interface with the URL <https://mc.vmware.com/core/sddc/groups/fe2c2c621-1cb1-80fc-a9bb-350a402f5a5c/connectivity>. The page title is "VMware Cloud". The main content area is titled "ALL SDDC Groups" and shows a group named "sddcgroup01". The "External VPC" tab is selected. A table lists an AWS Account ID (redacted) and its Resource Share Name (VMC-Group-), with a status of "ASSOCIATED".

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.

The screenshot shows the AWS Resource Access Manager (RAM) console with the URL <https://us-west-2.console.aws.amazon.com/ram/home?region=us-west-2#home>. The left sidebar shows "Shared by me" and "Shared with me" sections, with "Resource shares" selected under "Shared with me". The main content area is titled "AWS Resource Access Manager" and shows a diagram of the process: "AWS Resource Access Manager" (with a note: "Share resources across AWS accounts or AWS Organizations by creating a Resource Share") → "Select Resources" (with a note: "Select the resource(s) that you would like to add to a Resource Share") → "Specify Principals" (with a note: "Specify account ID, ARN, or Organization ID that can access the resources in the Resource Share") → "Share Resources" (with a note: "The specified principals will now have access to resources in the Resource Share"). To the right, there are sections for "Start sharing your AWS resources with other accounts" (with a "Create a resource share" button), "Pricing" (note: "RAM is offered at no additional charge. There are no setup fees or upfront commitments."), "More resources" (links to "What is AWS Resource Access Manager?", "Getting started", and "Documentation"), and "Your AZ ID" (note: "AZ IDs provide 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 accounts").

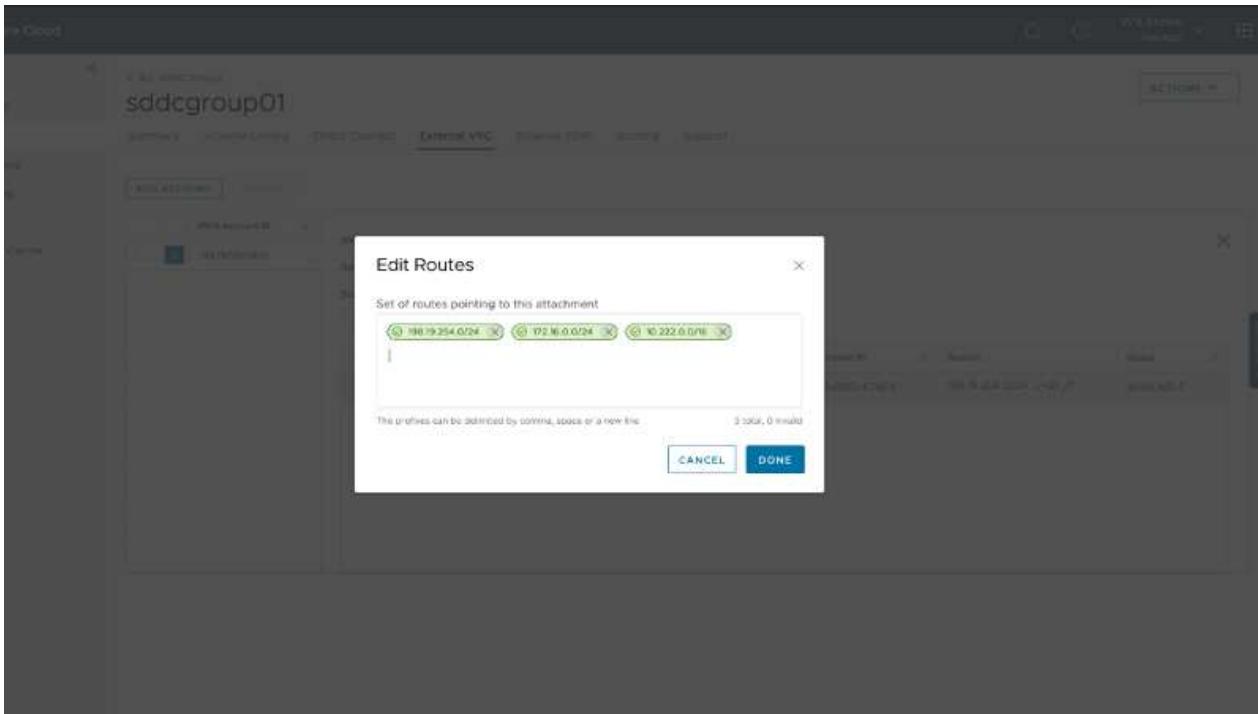
## 5. Create the Transit Gateway Attachment.

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

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.

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.



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

ID	Name	Sources	Destinations	Services	Applied To	Action
1019	allow Internet traffic	vmc-addc, vmc-addc-2	Any	Any	All Uplinks	Allow
1017	allow VMC to VPC	vmc-addc, vmc-addc-2	vmc-addc, vmc-addc-2	Any	All Uplinks	Allow
1016	allow VPC to VMC	vmc-addc	vmc-addc	Any	All Uplinks	Allow
1022	allow to vmch2...	vmc-addc, vmc-addc-2	vmch2.v...	Any	All Uplinks	Allow
1023	all from vmch2...	vmch2.v...	vmc-addc-2, vmc-addc	Any	All Uplinks	Allow
1012	Default VTI Rule	Any	Any	Any	VPN Tunnel In...	Allow
1011	Default Uplink Rule	Any	Any	Any	All Uplinks	Drop

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.



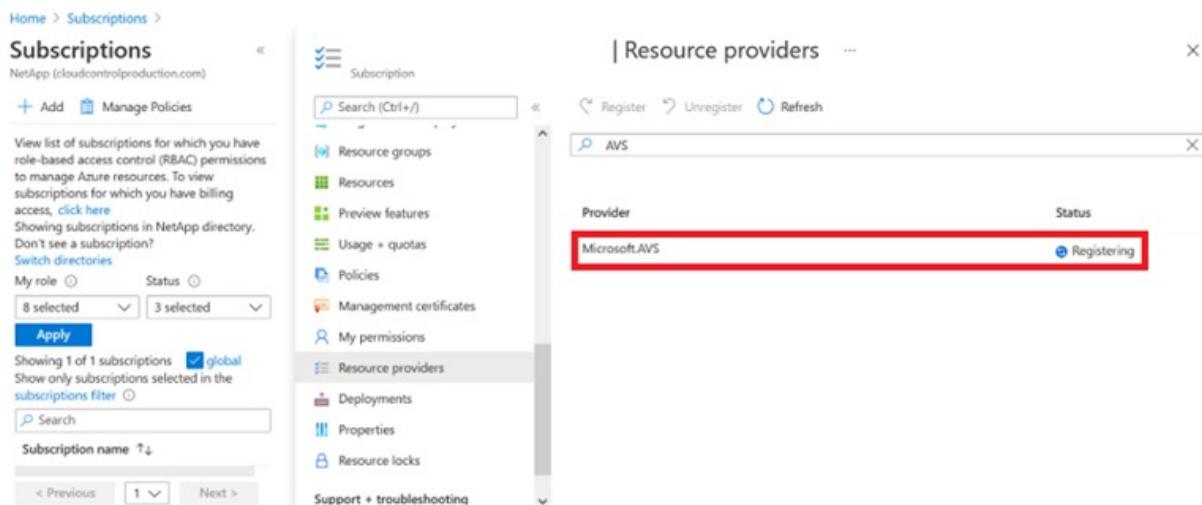
In-guest storage is the only supported method of connecting Azure NetApp Files and Cloud Volumes ONTAP to Azure VMware Solution.

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

## Register the resource provider and create a private cloud

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.



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 on-premises 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.

## Create a private cloud

Prerequisites   **Basics**   Tags   Review and Create

**Project details**

Subscription \* **SaaS Backup Production**  
Resource group \* **(New) NimoAVSDemo**  
Create new

**Private cloud details**

Resource name \* **nimoavsppriv**  
Location \* **(US) East US 2**  
Size of host \* **AV36 Trial**  
Number of hosts \* **3**  
Find out how many hosts you need

There is no metering for the selected subscription, region, and SKU. No cost data to display.

**CIDR address block**

Provide IP address for private cloud for cluster management. Make sure these are unique and do not overlap with any other Azure vnets or on-premise networks.

Address block for private cloud \* **10.21.0.0/22**

**Review and Create**   Previous   Next : Tags >

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.

Home >

**nimoavsppriv** AVS Private cloud

Search (Ctrl+ /) Delete

**Overview**

**Activity log**

**Access control (IAM)**

**Tags**

**Diagnose and solve problems**

**Settings**

**Locks**

**Manage**

**Connectivity**

**Identity**

**Clusters**

**Essentials**

Resource group (change) <b>NimoAVSDemo</b>	Address block for private cloud <b>10.21.0.0/22</b>
Status <b>Succeeded</b>	Primary peering subnet <b>10.21.0.232/30</b>
Location <b>East US 2</b>	Secondary peering subnet <b>10.21.0.236/30</b>
Subscription (change) <b>SaaS Backup Production</b>	Private Cloud Management network <b>10.21.0.0/26</b>
Subscription ID <b>b58a041a-e464-4497-8be9-9048369ee8e1</b>	vMotion network <b>10.21.1.128/25</b>
Tags (change) <b>Click here to add tags</b>	Number of hosts <b>3</b>

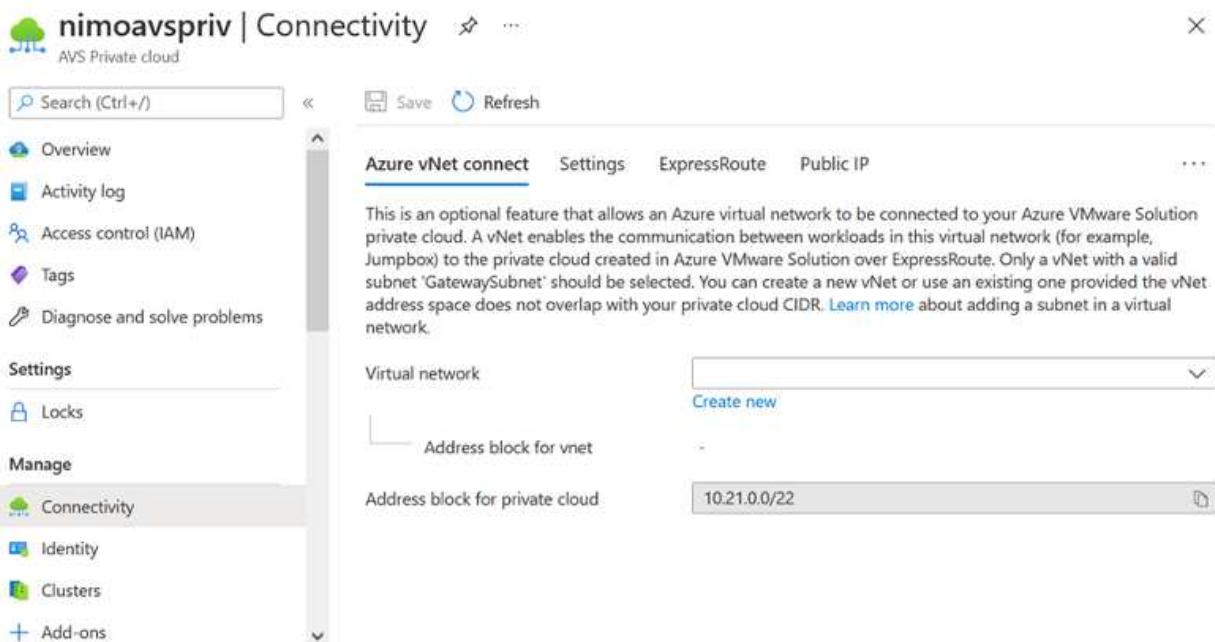
## Connect to a new or existing ExpressRoute virtual network gateway

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.



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

## Create virtual network

X

This virtual network enables the communication between workloads in this virtual network (e.g. a Jumphost) to the private cloud created in Azure VMware Solution over an Express route. A default address range and a subnet is selected for this virtual network. For changing the default address range and subnet of this virtual network, follow these steps: Step 1: Change the "Address Range" to desired range (e.g. 172.16.0.0/16). Step 2: Add a subnet under "Subnets" with the name as "GatewaySubnet" and provide subnet's address range in CIDR notation (e.g. 172.16.1.0/24). [Learn more about virtual networks](#)

Name \*

nimoavspiv-vnet

### Address space

The virtual network's address space specified as one or more address prefixes in CIDR notation (e.g. 10.0.0.0/16).

<input type="checkbox"/> Address range	Addresses	Overlap	
<input type="checkbox"/> 172.24.0.0/16	172.24.0.4 - 172.24.255.254 (65531 addresses)	None	
	(0 Addresses)	None	

### Subnets

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.

<input type="checkbox"/> Subnet name	Address range	Addresses	
<input type="checkbox"/> GatewaySubnet	172.24.0.0/24	172.24.0.4 - 172.24.0.254 (251 addresses)	
		(0 Addresses)	

**OK**

**Discard**

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](#).

## 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.

### Create a virtual machine

Basics Disks Networking Management Advanced Tags Review + create

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization. [Learn more](#)

**Project details**

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription \*  SaaS Backup Production

Resource group \*  NimoAVSDemo [Create new](#)

**Instance details**

Virtual machine name \*  nimAVSRH

Region \*  (US) East US 2

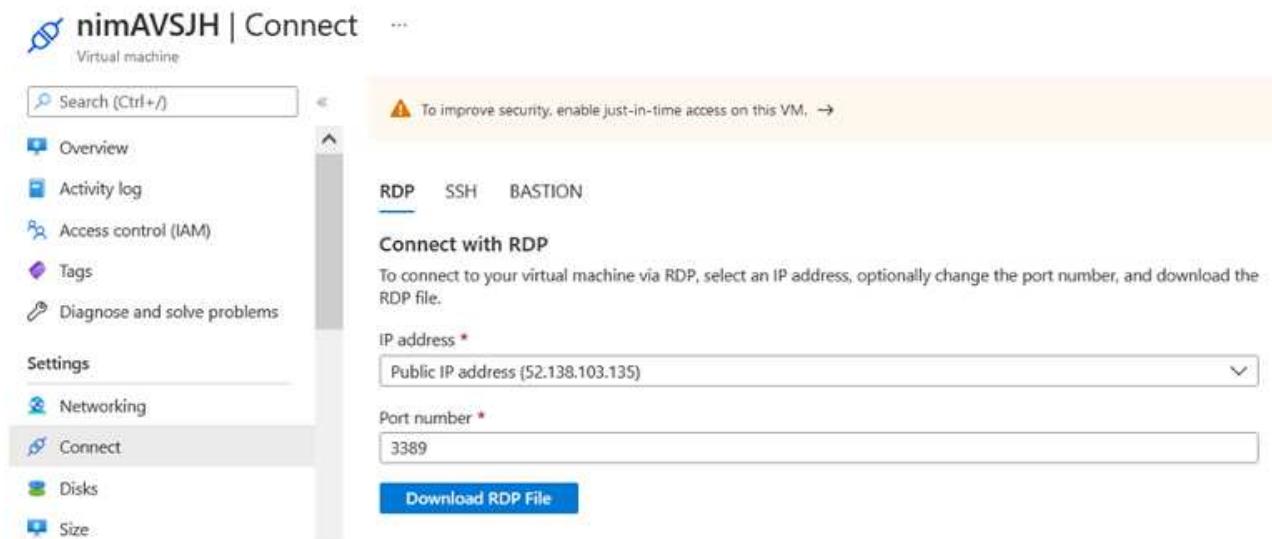
Availability options  No infrastructure redundancy required

Image \*  Windows Server 2012 R2 Datacenter - Gen2 [See all images](#)

Azure Spot instance

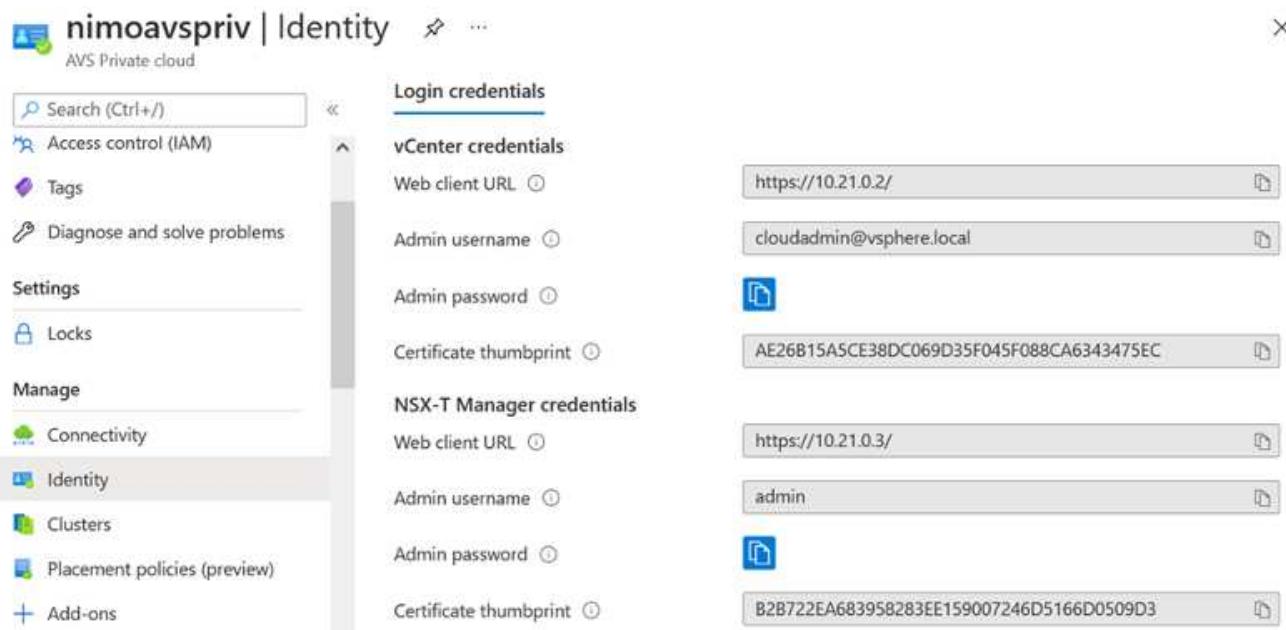
Size \*  Standard\_D2s\_v3 - 2 vcpus, 8 GiB memory (\$130.67/month) [See all sizes](#)

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



The screenshot shows the Azure portal interface for a virtual machine named 'nimAVSJH'. The left sidebar contains navigation links: Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings, Networking, Connect (which is selected), Disks, and Size. The main content area is titled 'nimAVSJH | Connect' and shows the 'Virtual machine' tab. A search bar at the top has 'Search (Ctrl+I)' placeholder text. A warning message at the top right says 'To improve security, enable just-in-time access on this VM.' Below this, there are tabs for RDP, SSH, and BASTION, with RDP selected. The 'Connect with RDP' section contains fields for 'IP address' (set to 'Public IP address (52.138.103.135)') and 'Port number' (set to '3389'), and a 'Download RDP File' button.

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.



The screenshot shows the Azure portal interface for an AVS Private cloud named 'nimoavsppriv'. The left sidebar contains navigation links: Access control (IAM), Tags, Diagnose and solve problems, Settings, Locks, Manage, Connectivity (which is selected), Identity (selected), Clusters, Placement policies (preview), and Add-ons. The main content area is titled 'nimoavsppriv | Identity' and shows the 'AVS Private cloud' section. A search bar at the top has 'Search (Ctrl+I)' placeholder text. The 'Login credentials' section is expanded, showing 'vCenter credentials' with fields for 'Web client URL' (set to 'https://10.21.0.2/'), 'Admin username' (set to 'cloudadmin@vsphere.local'), and 'Admin password' (with a copy icon). It also shows 'NSX-T Manager credentials' with fields for 'Web client URL' (set to 'https://10.21.0.3/'), 'Admin username' (set to 'admin'), and 'Admin password' (with a copy icon). Certificate thumbprint fields are also present for both.

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 screenshot shows two windows side-by-side. The left window is the 'Login' screen for 'VMware vSphere', with fields for 'Email' (clouadmin@vsphere.local), 'Password', and 'Use Windows session authentication'. The right window is the 'vSphere Client' interface for the 'vc.beeb9fd29eab4cbea81e62.eastus2.avs.azure.com' host. It displays summary statistics: 0 virtual machines, 3 hosts, and resource usage for CPU, Memory, and Storage. Below this is a table of recent tasks, showing an 'Undeploy plug-in' task completed successfully.

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.



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:

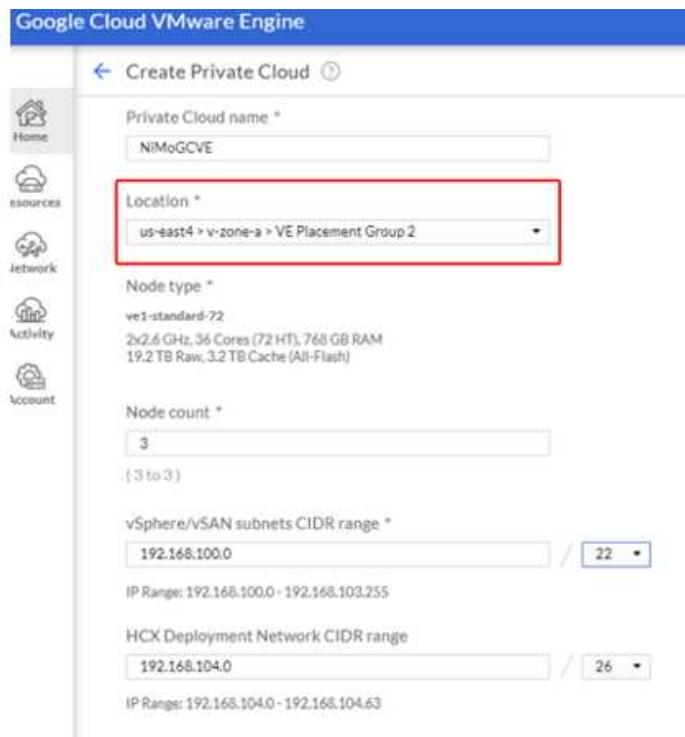
## Deploy and configure GCVE

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.



Google Cloud VMware Engine

← Create Private Cloud

Private Cloud name \*

NIMoGCVE

Location \*

us-east4 > v-zone-a > VE Placement Group 2

Node type \*

ve1-standard-72  
2x2.6 GHz, 36 Cores (72 HT), 768 GB RAM  
19.2 TB Raw, 3.2 TB Cache (All-Flash)

Node count \*

3  
(3 to 3)

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

Note: Private cloud creation can take between 30 minutes to 2 hours.

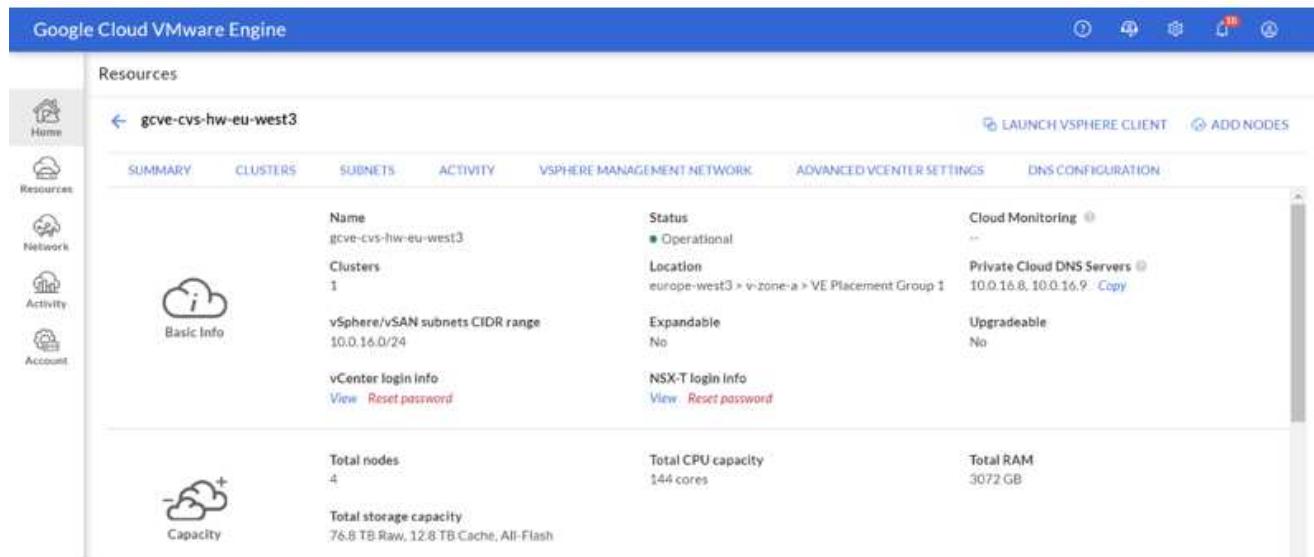
## Enable Private Access to GCVE

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 Project	Service	Region	Routing Mode	Peered Project ID	Peered VPC	VPC Peering Status	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).



The screenshot shows the Google Cloud VMware Engine vCenter interface. The left sidebar has navigation links: Home, Resources, Network, Activity, and Account. The main content area is titled 'gcve-cvs-hw-eu-west3'. It has tabs for SUMMARY, CLUSTERS, SUBNETS, ACTIVITY, VS SPHERE MANAGEMENT NETWORK, ADVANCED VCENTER SETTINGS, and DNS CONFIGURATION. The SUMMARY tab is selected. It displays basic information: Name (gcve-cvs-hw-eu-west3), Status (● Operational), Location (europe-west3 > v-zone-a > VE Placement Group 1), Cloud Monitoring (●), and Private Cloud DNS Servers (10.0.16.8, 10.0.16.9). It also shows vSphere/vSAN subnets CIDR range (10.0.16.0/24), Expandable (No), and Upgradeable (No). The 'Basic Info' section includes 'vCenter login info' (View, Reset password) and 'NSX-T login info' (View, Reset password). The 'Capacity' section shows Total nodes (4), Total CPU capacity (144 cores), Total RAM (3072 GB), and Total storage capacity (76.8 TB Raw, 12.8 TB Cache, All-Flash).

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](#).

The image shows two screenshots of the VMware vSphere interface. The top screenshot is the 'Login' screen, which includes fields for 'solution-user-01@gve.local', a password, and a checkbox for 'Use Windows session authentication'. The bottom screenshot is the 'vSphere Client' interface for the datacenter 'vcsa-57901.f7458c8f.europe-west3.gve.goog'. The 'Summary' tab is selected, displaying details such as Version: 7.0.1, Build: 18392253, Last Updated: Sep 22, 2021, 6:49 AM, and Last File-Based Backup: Not scheduled. It also shows resource usage for CPU, Memory, and Storage. The left sidebar lists clusters (esxi-57898, esxi-57902, esxi-62642, esxi-71844) and workloads (nimvmm01, nimvmm02, nimvmm02clone, nimvmmongodb, nimVMSQL03, nimVMSQL03-clone).

## 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 native datastore<sup>1</sup>

View the detailed [guest connect storage options for VMC](#).



1 - FSxN for VMC is currently in IA (Initial Availability). Contact your NetApp sales representative for more information.

## 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 native datastore<sup>1</sup>

View the detailed [guest connect storage options for AVS](#).



1 - ANF as a native datastore for AVS is currently in Public Preview. Read more about it [here](#).

## 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 native datastore<sup>1</sup>

View the detailed [guest connect storage options for GCVE](#).

Read more about [Cloud Volumes Service \(CVS\) as a native datastore<sup>1</sup>](#).



1 - Currently in Private Preview

## 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, high-performing, 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.



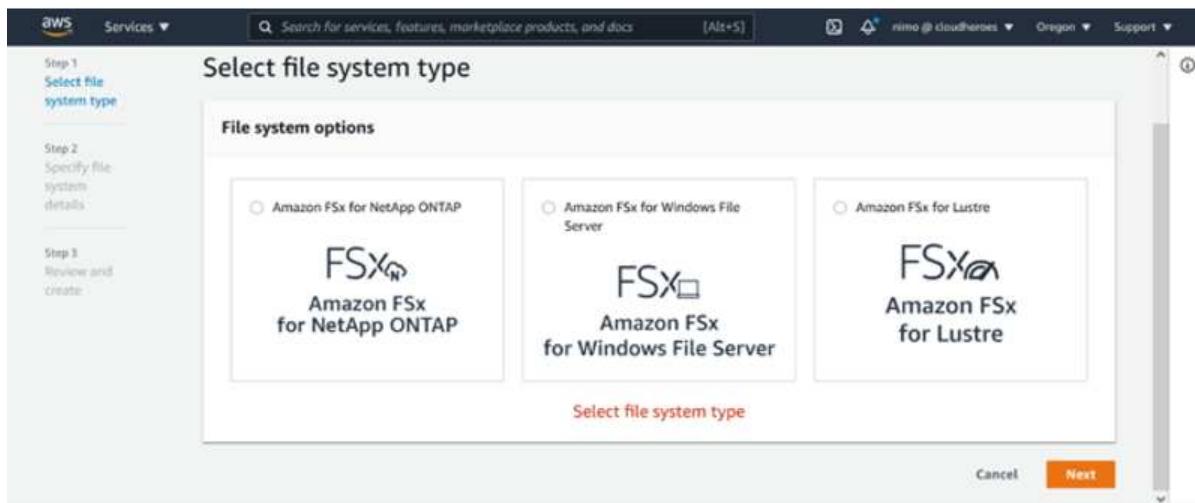
Amazon FSx for NetApp ONTAP and VMware Cloud on AWS must be in the same availability zone to achieve better performance and avoid data transfer charges between availability zones.



## Create and mount Amazon FSx for ONTAP volumes

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.



3. 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.

## Create file system

### Creation 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.

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

## File system details

File system name - optional [Info](#)

vmcfsxval2

Maximum of 256 Unicode letters, whitespace, and numbers, plus + - = . \_ : /

SSD storage capacity [Info](#)

1024

Minimum 1024 GB; Maximum 192 TB.

Provisioned SSD IOPS

Amazon FSx provides 3 IOPS per GB of storage capacity. You can also provision additional SSD IOPS as needed.

Automatic (3 IOPS per GB of SSD storage)

User-provisioned

Throughput capacity [Info](#)

The sustained speed at which the file server hosting your file system can serve data. The file server can also burst to higher speeds for periods of time.

512 MB/s (Recommended)

5. 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.

## Network & security

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)

sg-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.

6. 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.

## Security & encryption

### Encryption key [Info](#)

AWS Key Management Service (KMS) encryption key that protects your file system data at rest.

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

### File system administrative password

Password for this file system's "fsxadmin" user, which you can use to access the ONTAP CLI or REST API.

- Don't specify a password  
 Specify a password

Password

\*\*\*\*\*

Confirm password

\*\*\*\*\*

7. 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.

## Default storage virtual machine configuration

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.

- Don't specify a password
- 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

8. 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.

## Default volume configuration

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



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.

- Enabled (recommended)
- Disabled

Capacity pool tiering policy

You can optionally enable automatic tiering of your data to lower-cost capacity pool storage.

Auto



9. Review the file system configuration shown on the Create File System page.

10. Click Create File System.

Screenshot of the AWS FSx console showing the creation of a Storage virtual machine (SVM).

**File systems** (3)

File system name	File system ID	File system type	Status	Deployment type	Storage type	Size
fsxntapcifs	fs-014c28399be9c1f9f	ONTAP	Available	Multi-AZ	SSD	1.00 TB
vmcfsxval2	fs-040eacc5d0ac31017	ONTAP	Available	Multi-AZ	SSD	1.00 TB
fsxntapsql	fs-0ab4b447ebd6082aa	ONTAP	Available	Multi-AZ	SSD	2.00 TB

**Storage virtual machines (SVMs) (2)**

SVM name	SVM ID	Status	Creation time	Active Directory
fsxsmbtesting01	svm-075dcfbe2cfa2ece9	Created	2021-10-19 15:17:08 UTC +01:00	FSXTESTING.LOCAL
vmcfsxval2svm	svm-095db076341561212	Created	2021-10-15 15:16:54 UTC +01:00	-

**fsxsmbtesting01 (svm-075dcfbe2cfa2ece9)**

**Summary**

SVM ID svm-075dcfbe2cfa2ece9	Creation time 2021-10-19T15:17:08+01:00	Active Directory FSXTESTING.LOCAL
SVM name fsxsmbtesting01	Lifecycle state Created	Net BIOS name FSXSMBTESTING01
UUID 4a50e659-30e7-11ec-ac4f-f3ad92a6a735	Subtype DEFAULT	Fully qualified domain name FSXTESTING.LOCAL
File system ID fs-040eacc5d0ac31017		Service account username administrator
		Organizational unit distinguished name CN=Computers

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:



## Mount FSx ONTAP volume on Linux client

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:

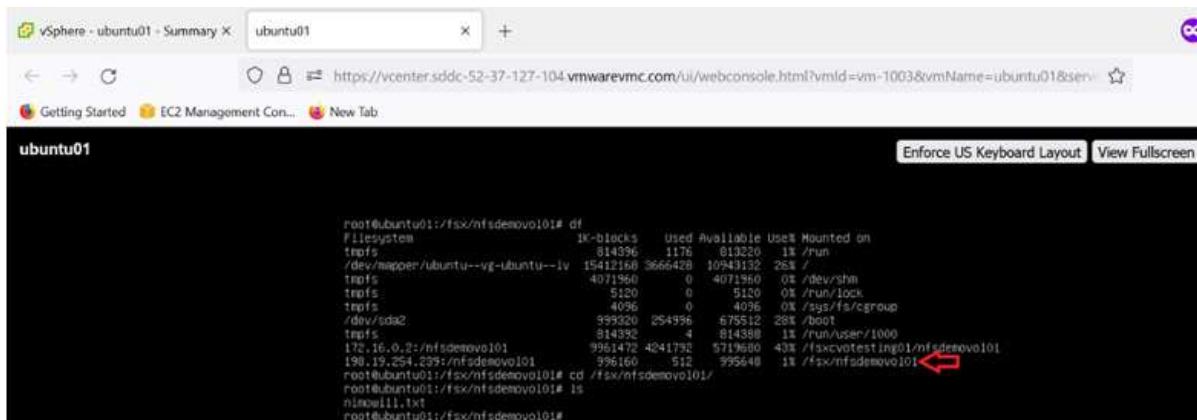
```
$ sudo mkdir /fsx/nfsdemovol01
```

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
```

```
root@ubuntu01:/fsx/nfsdemovol01# mount -t nfs 198.19.254.239:/nfsdemovol01 /fsx/nfsdemovol01
```

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



```
root@ubuntu01:/fsx/nfsdemovol01# df  
Filesystem 1K-blocks Used Available Use% Mounted on  
tmpfs 814396 1176 813220 1% /run  
/dev/mapper/ubuntu--vg-ubuntu--lv 15412160 3666428 10943132 26% /  
tmpfs 4071960 0 4071960 0% /dev/shm  
tmpfs 5120 0 5120 0% /run/lock  
tmpfs 4096 0 4096 0% /sys/fs/cgroup  
/dev/sda2 599320 254996 675512 28% /boot  
tmpfs 814392 4 814388 1% /run/user/1000  
172.16.0.2:/nfsdemovol01 9961472 4241732 5719680 43% /fsx/cvtest01/nfsdemovol01  
root@ubuntu01:/fsx/nfsdemovol01# cd /fsx/nfsdemovol01/  
root@ubuntu01:/fsx/nfsdemovol01# ls  
nfsnull1.txt  
root@ubuntu01:/fsx/nfsdemovol01#
```

► [https://docs.netapp.com/us-en/netapp-solutions/media/vmc\\_linux\\_vm\\_nfs.mp4](https://docs.netapp.com/us-en/netapp-solutions/media/vmc_linux_vm_nfs.mp4) (video)



## Attach FSx ONTAP volumes to Microsoft Windows clients

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.



To 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.

### Endpoints

Management DNS name	Management IP address
svm-075dcfbe2cfa2ece9.fs-040eacc5d0ac31017.fsx.us-west-2.amazonaws.com	198.19.254.9
NFS DNS name	NFS IP address
svm-075dcfbe2cfa2ece9.fs-040eacc5d0ac31017.fsx.us-west-2.amazonaws.com	198.19.254.9
SMB DNS name	SMB IP address
FSXSMBTESTING01.FSXTESTING.LOCAL	198.19.254.9
iSCSI DNS name	iSCSI IP addresses
iscsi.svm-075dcfbe2cfa2ece9.fs-040eacc5d0ac31017.fsx.us-west-2.amazonaws.com	10.222.2.224, 10.222.1.94

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

Computer Management

File Action View Help

Computer Management (FSXMBTESTING01.FSXTESTING.LOCAL)

- System Tools
  - Task Scheduler
  - Event Viewer
  - Shared Folders
    - Shares
    - Sessions
    - Open Files
  - Local Users and Groups
  - Performance
  - Device Manager
- Storage
  - Windows Server Backup
  - Disk Management
- Services and Applications

Share Name	Folder Path	Type	# Client Connections	Description
c\$	C:\	Windows	0	
ipc\$		Windows	1	
smbdemo...	C:\smbdemovol01	Windows	1	
testnimvol	C:\testnimvol	Windows	0	

5. Now choose a new share and complete the Create a Shared Folder wizard.

Create A Shared Folder Wizard

**Name, Description, and Settings**

Specify how people see and use this share over the network.

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

Share name:

Share path:

Description:

Offline setting:

< Back  Cancel

## Create A Shared Folder Wizard



### Sharing was Successful

#### Status:

You have successfully completed the Share a Folder Wizard.

#### 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 another folder

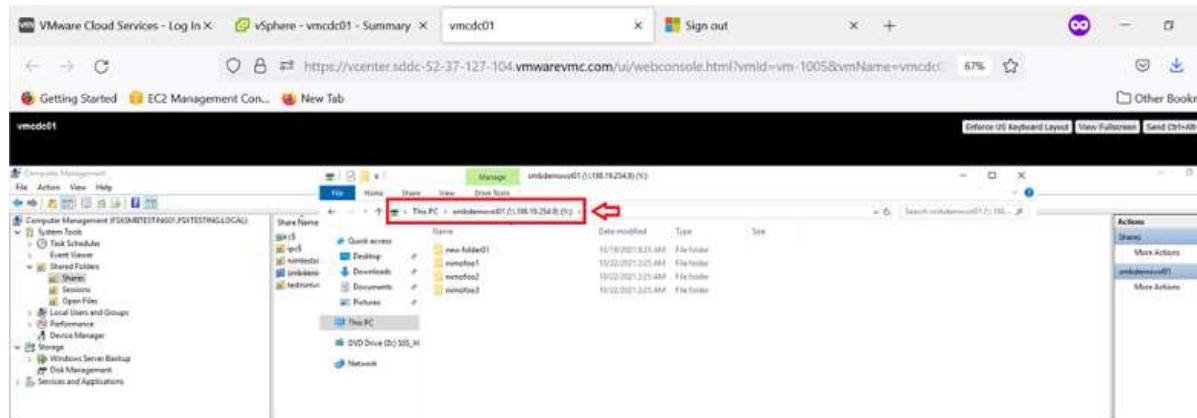
To close this wizard, click Finish.

**Finish**

**Cancel**

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

6. 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.



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

- ▶ [https://docs.netapp.com/us-en/netapp-solutions/media/vmc\\_windows\\_vm\\_iscsi.mp4](https://docs.netapp.com/us-en/netapp-solutions/media/vmc_windows_vm_iscsi.mp4) (video)

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:



## Provision a LUN in FSx for NetApp ONTAP:

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).

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

```
FsxId040eacc5d0ac31017::> igrup create -vserver vmcfsxval2svm  
-igroup winIG -protocol iscsi -ostype windows -initiator  
iqn.1991-05.com.microsoft:vmcdc01.fsxtesting.local
```

```
FsxId040eacc5d0ac31017::> igrup show
```

Vserver	Igroup	Protocol	OS	Type	Initiators
---------	--------	----------	----	------	------------

-----  
-----

vmcfssxval2sym

```
ubuntu01      iscsi      linux      iqn.2021-  
10.com.ubuntu:01:initiator01
```

vmcfssxval2sym

```
winIG      iscsi      windows  iqn.1991-05.com.microsoft:vmcdc01.fsxtesting.local
```

Two entries were displayed.

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

```

FsxId040eacc5d0ac31017::> lun map -vserver vmcfsxval2svm -path
/vol/nimfsxscsivol/nimofsxlun01 -igroup winIG

FsxId040eacc5d0ac31017::> lun show

Vserver      Path          State   Mapped   Type
Size

-----
-----
vmcfsxval2svm

/vol/blocktest01/lun01      online   mapped   linux
5GB

vmcfsxval2svm

/vol/nimfsxscsivol/nimofsxlun01 online   mapped
windows      5GB

```

Two entries were displayed.

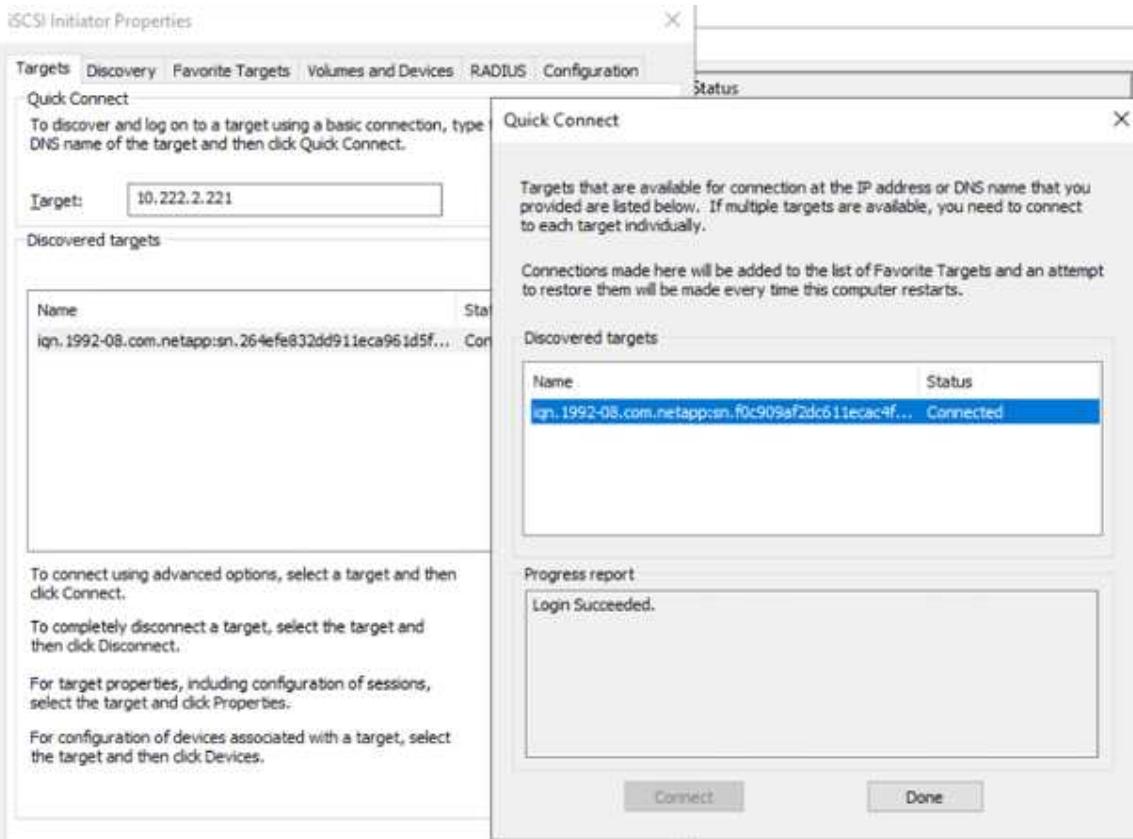
##### 5. Connect the newly provisioned LUN to a Windows VM:

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

- RDP to the Windows VM hosted on the VMware Cloud on AWS SDDC.
- Navigate to Server Manager > Dashboard > Tools > iSCSI Initiator to open the iSCSI Initiator Properties dialog box.
- From the Discovery tab, click Discover Portal or Add Portal and then enter the IP address of the iSCSI target port.
- From the Targets tab, select the target discovered and then click Log On or Connect.
- 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.

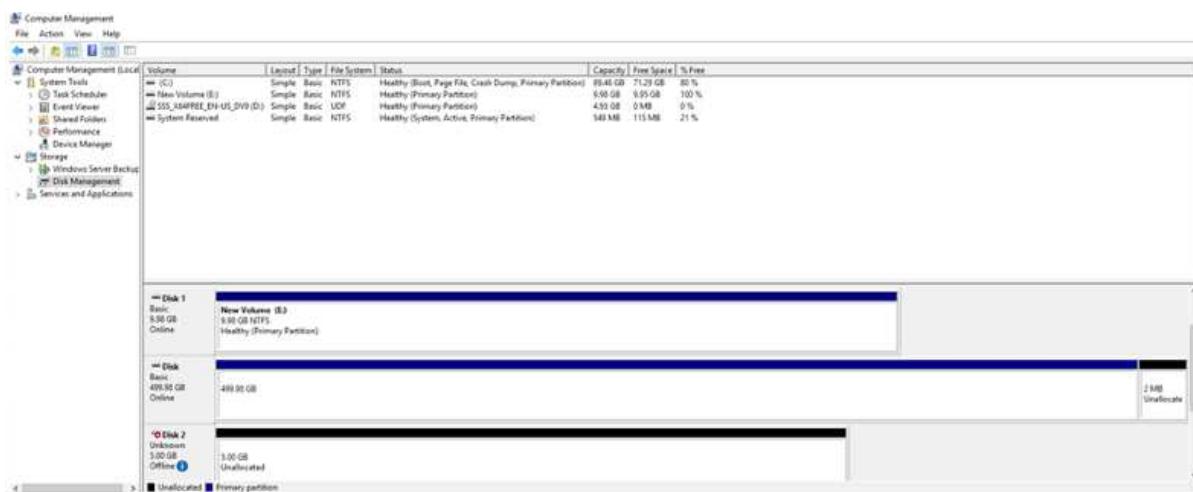


The Windows host must have an iSCSI connection to each node in the cluster. The native DSM selects the best paths to use.



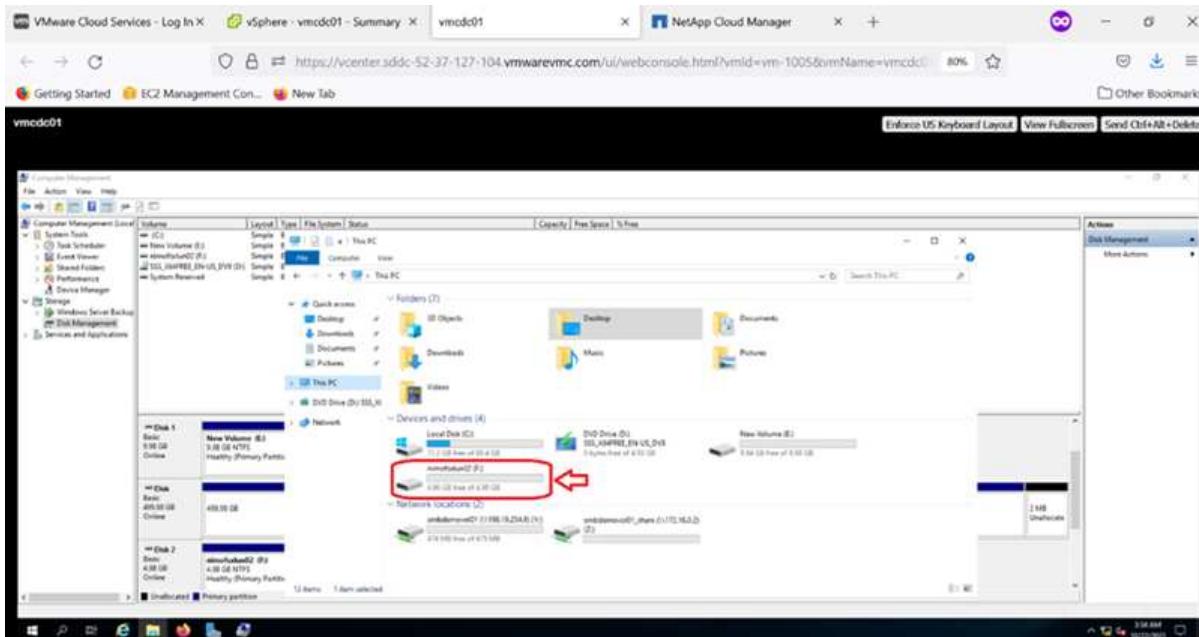
LUNs on the storage virtual machine (SVM) appear as disks to the Windows host. Any new disks that are added are not automatically discovered by the host. Trigger a manual rescan to discover the disks by completing the following steps:

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.



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.



## 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 your 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



## Deploy new Cloud Volumes ONTAP instance in AWS (do it yourself)

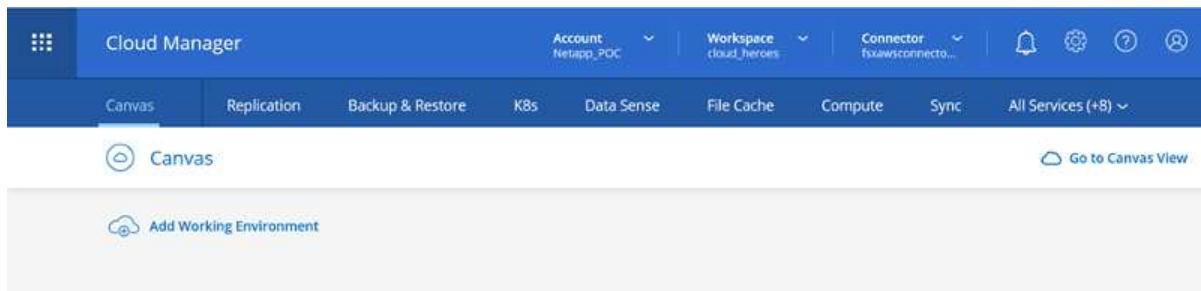
Cloud Volumes ONTAP shares and LUNs can be mounted from VMs that are created in the VMware Cloud on AWS SDDC environment. The volumes can also be mounted on native AWS VM Linux Windows clients, and LUNs can be accessed on Linux or Windows clients as block devices when mounted over iSCSI because Cloud 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](#).

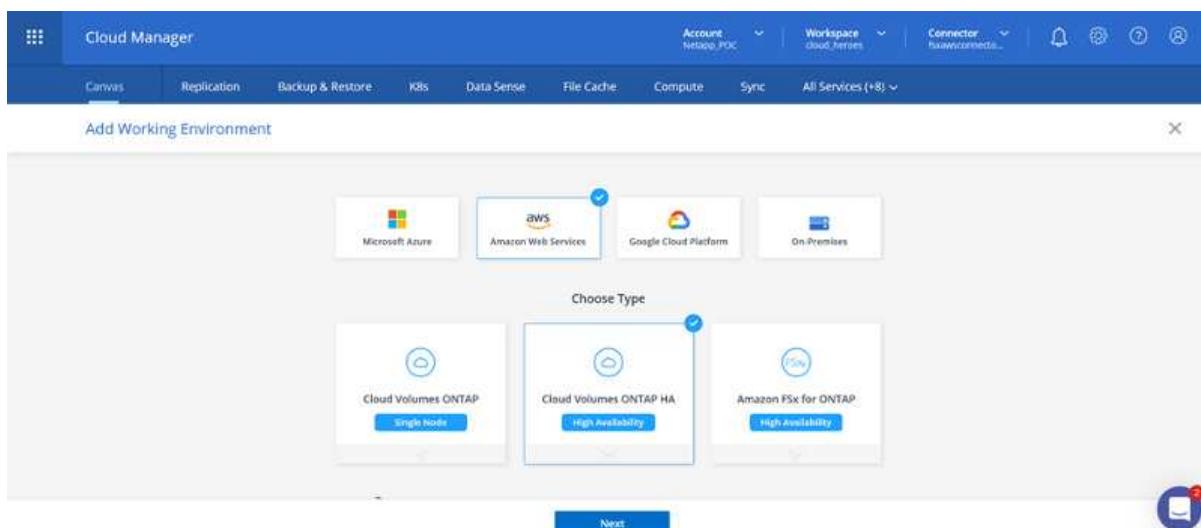


Use the [Cloud Volumes ONTAP sizer](#) to accurately size the Cloud Volumes ONTAP instances. Also, monitor on-premises performance to use as inputs in the Cloud Volumes ONTAP sizer.

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.



2. 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.



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

↑ Previous Step	Instance Profile Credential Name	139763910815 Account ID	netapp.com-cloud-volumes-... Marketplace Subscription	<a href="#">Edit Credentials</a>
<p>Details</p> <p>Working Environment Name (Cluster Name) fsxvcvtesting01</p> <p><a href="#">Add Tags</a>    Optional Field   Up to four tags</p>		<p>Credentials</p> <p>User Name admin</p> <p>Password *****</p> <p>Confirm Password *****</p>		
<a href="#">Continue</a>				

4. Select the add-on services for Cloud Volumes ONTAP deployment, including Cloud Data Sense, Cloud Backup, and Cloud Insights. Click Continue.

 Data Sense & Compliance	<input checked="" type="checkbox"/>	<a href="#">More Info</a>
 Backup to Cloud	<input checked="" type="checkbox"/>	<a href="#">More Info</a>
 Monitoring	<input checked="" type="checkbox"/>	<a href="#">More Info</a>
<a href="#">Continue</a>		

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

↑ Previous Step	<p>Multiple Availability Zones</p> <ul style="list-style-type: none"> <li> Provides maximum protection against AZ failures.</li> <li> Enables selection of 3 availability zones.</li> <li> An HA node serves data if its partner goes offline.</li> </ul> <p><a href="#">Extended Info</a></p>	<p>Single Availability Zone</p> <ul style="list-style-type: none"> <li> Protects against failures within a single AZ.</li> <li> Single availability zone. HA nodes are in a placement group, spread across distinct underlying hardware.</li> <li> An HA node serves data if its partner goes offline.</li> </ul> <p><a href="#">Extended Info</a></p>
<a href="#">Continue</a>		

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

↑ Previous Step

AWS Region	VPC	Security group															
US West   Oregon	vpc-0d1c764bcc495e805 - 10.222.0.0/16	Use a generated security group															
<table border="1"> <tr> <td> Node 1:</td> <td> Node 2:</td> <td> Mediator:</td> </tr> <tr> <td>Availability Zone</td> <td>Availability Zone</td> <td>Availability Zone</td> </tr> <tr> <td>us-west-2a</td> <td>us-west-2b</td> <td>us-west-2c</td> </tr> <tr> <td>Subnet</td> <td>Subnet</td> <td>Subnet</td> </tr> <tr> <td>10.222.1.0/24</td> <td>10.222.2.0/24</td> <td>10.222.3.0/24</td> </tr> </table>			Node 1:	Node 2:	Mediator:	Availability Zone	Availability Zone	Availability Zone	us-west-2a	us-west-2b	us-west-2c	Subnet	Subnet	Subnet	10.222.1.0/24	10.222.2.0/24	10.222.3.0/24
Node 1:	Node 2:	Mediator:															
Availability Zone	Availability Zone	Availability Zone															
us-west-2a	us-west-2b	us-west-2c															
Subnet	Subnet	Subnet															
10.222.1.0/24	10.222.2.0/24	10.222.3.0/24															

**Continue**

7. On the Connectivity and SSH Authentication page, choose connection methods for the HA pair and the mediator.

↑ Previous Step

Nodes	Mediator
SSH Authentication Method	Security Group
Password	Use a generated security group
Key Pair Name	
nimokey	
Internet Connection Method	
Public IP address	

**Continue**

8. Specify the floating IP addresses and then click Continue.

↑ Previous Step

Floating IP addresses are required for cluster and SVM access and for NFS and CIFS data access. These floating IPs can migrate between HA nodes if failures occur. To access the data from outside the VPC, [you can set up an AWS transit gateway](#).

You must specify IP addresses that are outside of the CIDR blocks for all VPCs in the selected AWS region.

Floating IP address for cluster management	172.16.0.1
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
Floating IP address for SVM management (Optional)	172.16.0.4

**Continue**

9. Select the appropriate route tables to include routes to the floating IP addresses and then click Continue.

Create 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 Volumes ONTAP HA 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	ID	Associate with Subnet	Tags
<input checked="" type="checkbox"/>	Yes	rtb-00b2d30c3f68fdbdd	0 Subnets	1 Tags

1 Route Tables | The main route table is the default for the VPC

Continue

10. On the Data Encryption page, choose AWS-managed encryption.

Create a New Working Environment

Data Encryption

↑ Previous Step

 AWS Managed Encryption

AWS is responsible for data encryption and decryption operations. Key management is handled by AWS key management services.

Default Master Key: aws/ebs

Change Key

Continue

11. Select the license option: Pay-As-You-Go or BYOL for using an existing license. In this example, the Pay-As-You-Go option is used.

Cloud Volumes ONTAP Charging Methods

Learn more about our charging methods

Pay-As-You-Go by the hour

Bring your own license

NetApp Support Site Account (Optional)

Learn more about NetApp Support Site (NSS) accounts

To register this Cloud Volumes ONTAP to support, you should add NetApp Support Site Account.

Don't have a NetApp Support Site account? Select go to finish deploying this system. After it's created, use the Support Registration option to create an NSS account.

**Continue**

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

Create a New Working Environment

Preconfigured Packages

Select a preconfigured Cloud Volumes ONTAP system that best matches your needs, or create your own configuration. Preconfigured settings can be modified at a later time.

**Change Configuration**

POC and small workloads  
Up to 500GB of storage

Database and application data production workloads

Cost effective DR  
Up to 500GB of storage

Highest performance production workloads

**Continue**

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

Create a New Working Environment

Review & Approve

Previous Step [tsxcvotesting](#)

AWS: us-west-2 | HA

Show API request

This Cloud Volumes ONTAP instance will be registered with NetApp support under the NSS Account mchad.

I understand that Cloud Manager will allocate the appropriate AWS resources to comply with my above requirements. [More information >](#)

**Overview** **Networking** **Storage**

Storage System:	Cloud Volumes ONTAP HA	HA Deployment Model:	Multiple Availability Zones
License Type:	Cloud Volumes ONTAP Explore	Encryption:	AWS Managed
Capacity Limit:	2TB	Customer Master Key:	aws/ebs

**Go**

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

Canvas Replication Backup & Restore K8s Data Sense File Cache Compute Sync All Services (+8) ▾

Canvas Go to Tabular View

Add Working Environment

vmhseval2  
15a for ONTAP

9 Volumes 26.49 GB Capacity AWS

fsxvotesting01  
Cloud Volumes ONTAP

46.08 Capacity AWS

Amazon S3

4 Buckets 2 Regions AWS

fsxvotesting01

Cloud Volumes ONTAP

On

DETAILS

Cloud Volumes ONTAP | AWS | HA

SERVICES

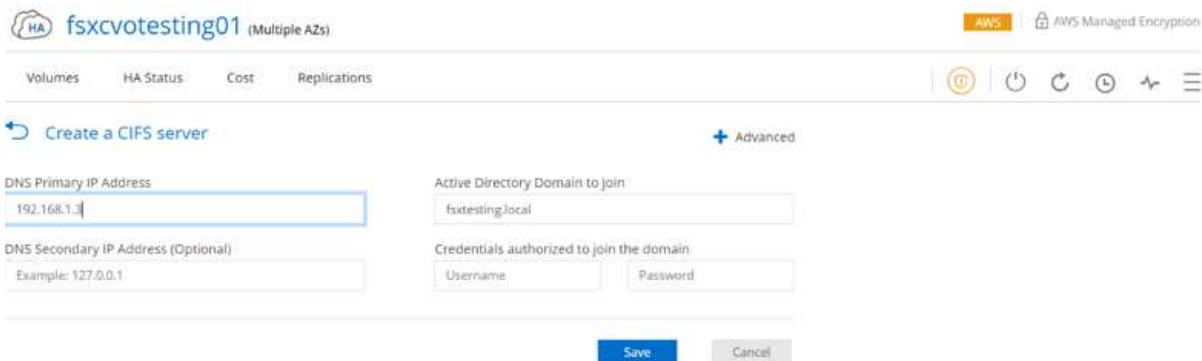
Replication Off Enable

Backup & Restore Loading...



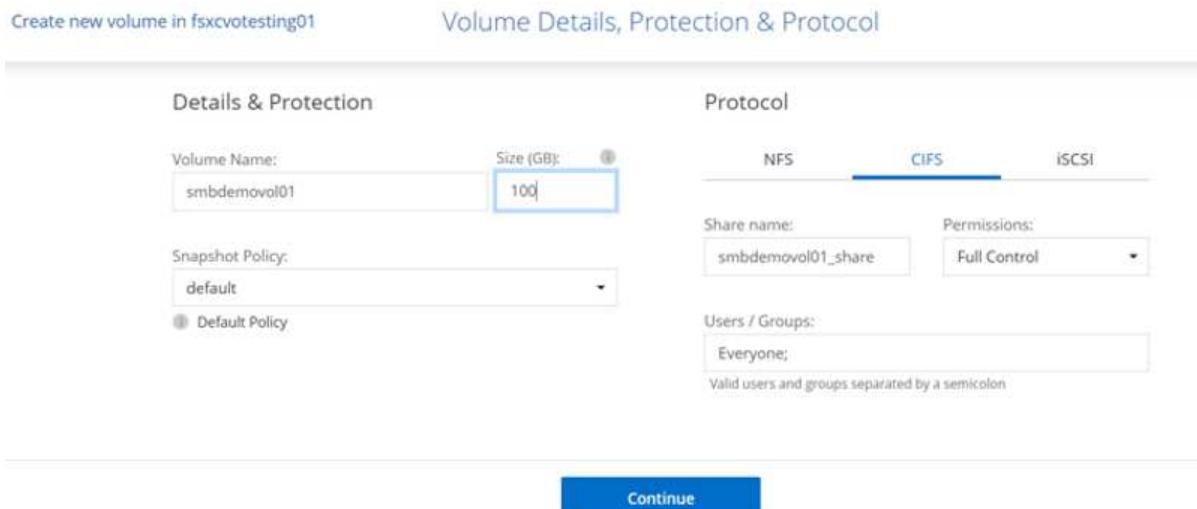
## Additional configurations for SMB volumes

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.



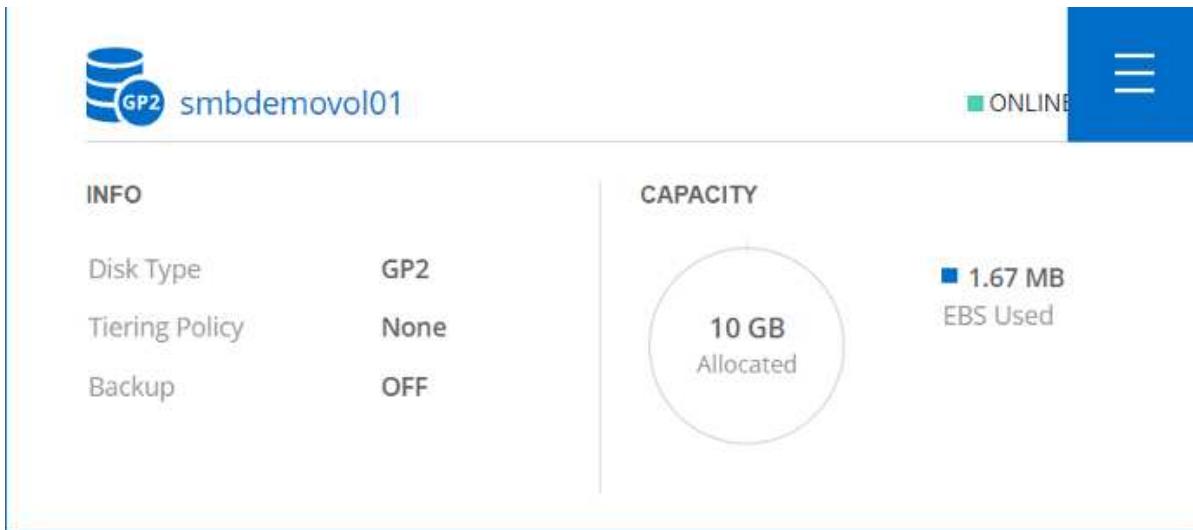
The screenshot shows the 'Create a CIFS server' configuration page within the AWS CloudFormation console. The stack name is 'fsxvotesting01' (Multiple AZs). The 'DNS Primary IP Address' is set to '192.168.1.3'. The 'Active Directory Domain to join' is 'fsxtesting.local'. The 'DNS Secondary IP Address (Optional)' field contains 'Example: 127.0.0.1'. The 'Credentials authorized to join the domain' section shows 'Username' and 'Password' fields. At the bottom are 'Save' and 'Cancel' buttons.

2. 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.



The screenshot shows the 'Create new volume in fsxvotesting01' wizard at the 'Volume Details, Protection & Protocol' step. The 'Volume Name' is 'smbdemovol01', the 'Size (GB)' is '100', and the 'Snapshot Policy' is 'default'. In the 'Protocol' section, 'CIFS' is selected. The 'Share name' is 'smbdemovol01\_share' and 'Permissions' are set to 'Full Control'. The 'Users / Groups' field contains 'Everyone'. A note at the bottom states 'Valid users and groups separated by a semicolon'. A 'Continue' button is at the bottom.

3. After the volume is provisioned, it is available 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.



4. 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.
5. 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.

fsxvotesting01 (Multiple AZs)

Mount Volume smbdemovol01

Access from inside the VPC using Floating IP

Access from outside the VPC using AWS Private IP

Auto failover between nodes

The IP address automatically migrates between nodes if failures occur

No auto failover between nodes

The IP address does not migrate between nodes if failures occur

Go to your machine and enter this command

\\172.16.0.2\smbdemovol01\_share

\\10.222.1.100\smbdemovol01\_share

If the primary node goes offline, mount the volume by using the HA partner's IP address: \\10.222.1.100\smbdemovol01\_share

VMware Cloud - ntap-fsx-demo

vsphere - vmcd01 - Summary

vmcd01

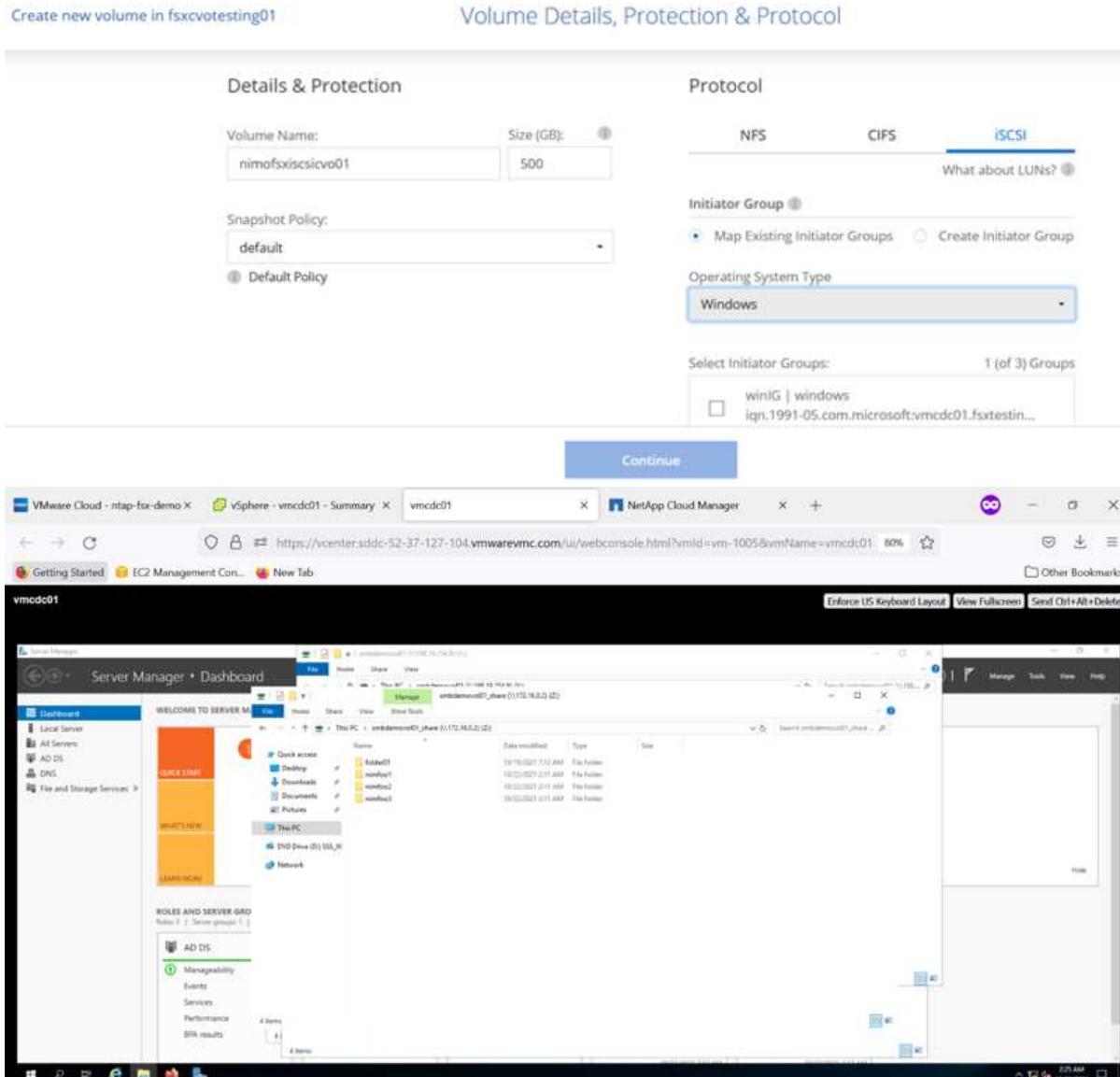
NetApp Cloud Manager



## 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.



The screenshot shows the 'Create new volume in fsxvotesting01' interface in NetApp Cloud Manager. The 'Protocol' tab is selected for iSCSI. In the 'Initiator Group' section, 'Map Existing Initiator Groups' is selected. The 'Operating System Type' is set to 'Windows'. The 'Select Initiator Groups' dropdown shows 'winIG | windows' and 'iqn.1991-05.com.microsoft:vmcd01.fsxtesting01'. A 'Continue' button is visible. Below the interface, a screenshot of a Windows Server Manager dashboard shows a file share named 'vmcd01' on the local machine.

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 the VMware Cloud on AWS SDDC, complete the following steps:

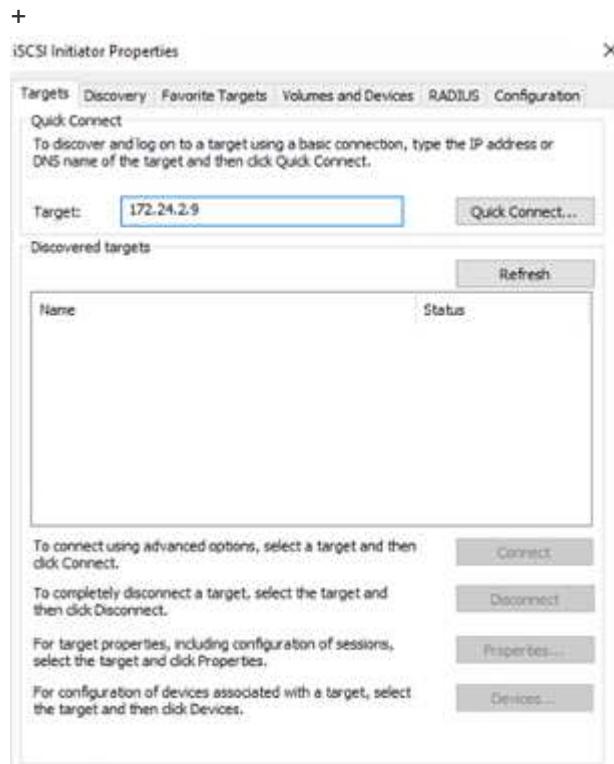
- a. RDP to the VM hosted on VMware cloud on AWS.
- b. Open the iSCSI Initiator Properties dialog box: Server Manager > Dashboard > Tools > iSCSI Initiator.
- c. From the Discovery tab, click Discover Portal or Add Portal and then enter the IP address of the

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.

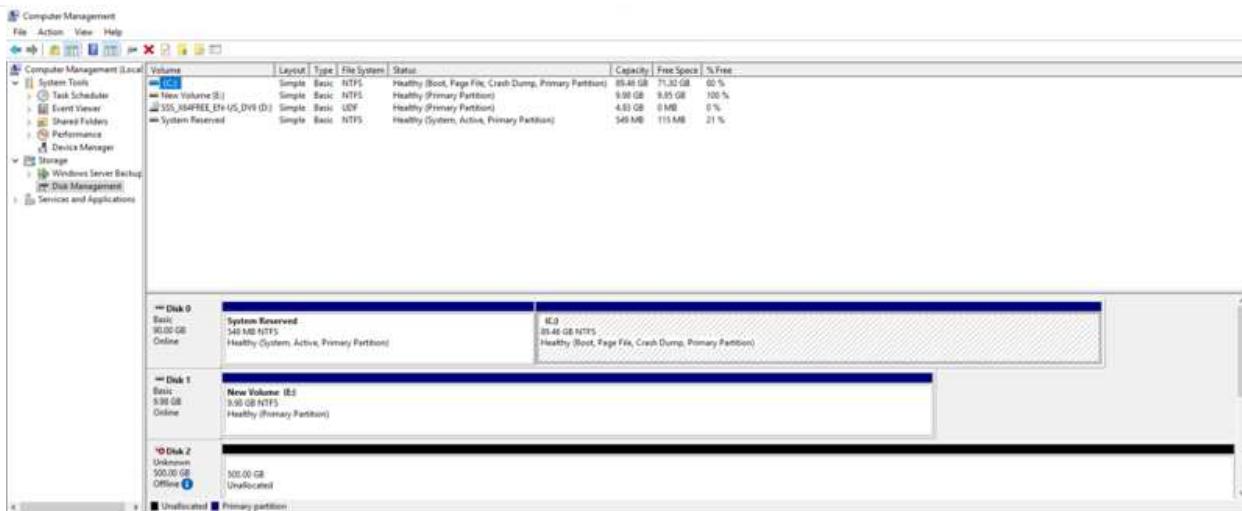


The Windows host must have an iSCSI connection to each node in the cluster. The native DSM selects the best paths to use.



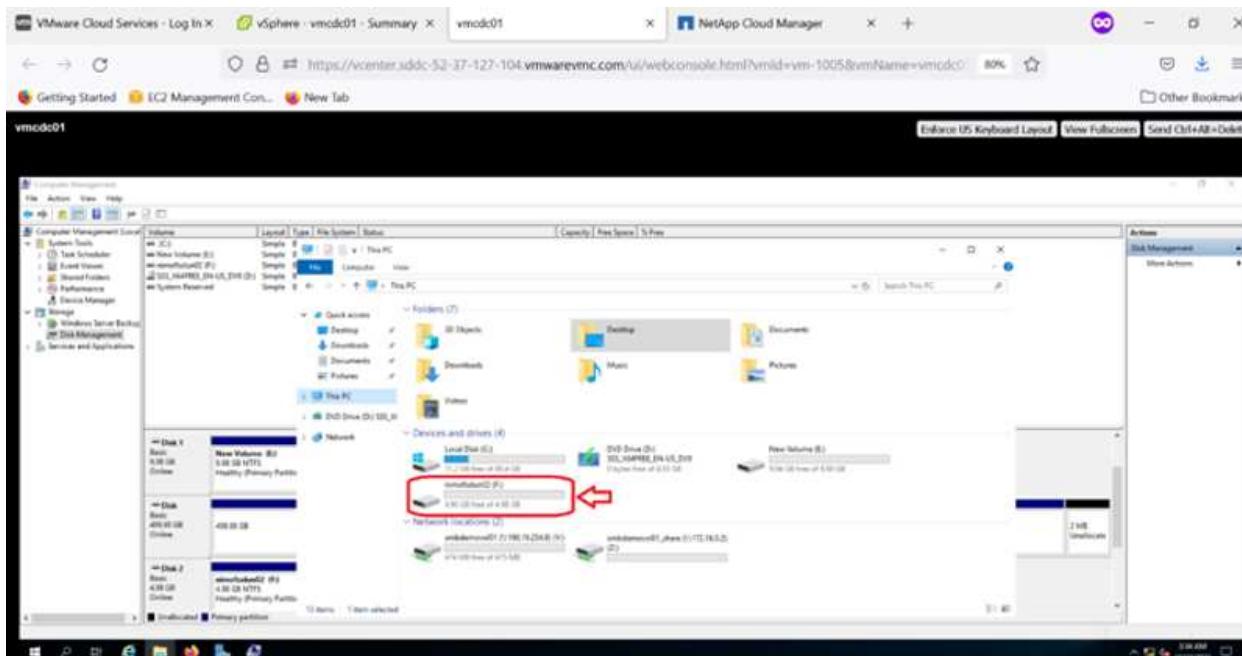
LUNs from the SVM appear as disks to the Windows host. Any new disks that are added are not automatically discovered by the host. Trigger a manual rescan to discover the disks by completing the following steps:

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.



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.



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.

## Mount Cloud Volumes ONTAP NFS volume on Linux client

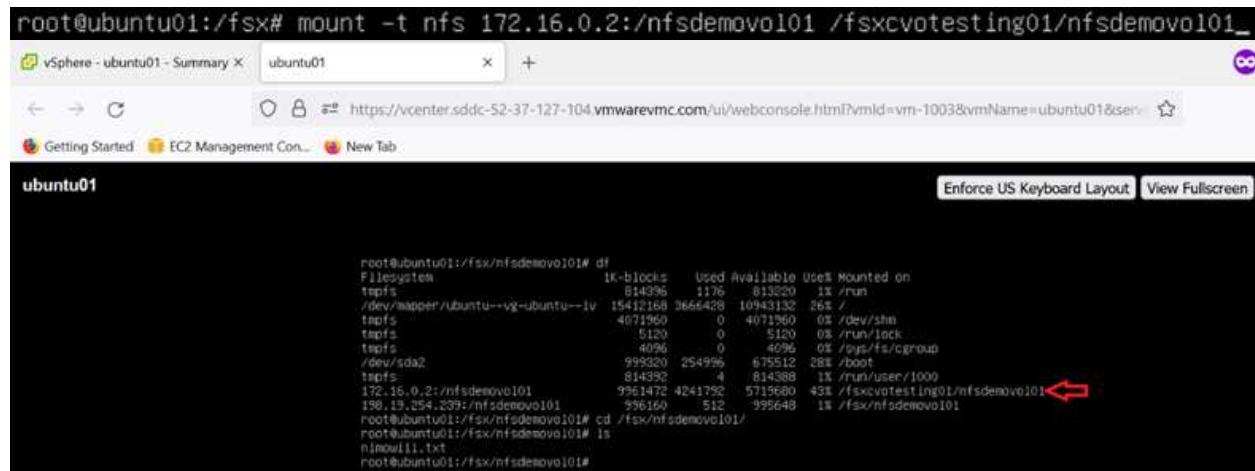
To mount the Cloud Volumes ONTAP (DIY) file system from VMs within VMC on AWS SDDC, complete the following steps:

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.

```
sudo mount -t nfs nfsvers=4.1,172.16.0.2:/nfsdemovol01  
/fsxcvotesting01/nfsdemovol01
```



```
root@ubuntu01:/fsx# mount -t nfs 172.16.0.2:/nfsdemovol01 /fsxcvotesting01/nfsdemovol01_
ubuntu01 x + https://vcenter.sddc-52-37-127-104.vmwarevmc.com/ui/webconsole.html?vmId=vm-1003&vmName=ubuntu01&ser
ubuntu01 Getting Started EC2 Management Con... New Tab
Enforce US Keyboard Layout View Fullscreen

root@ubuntu01:/fsx/nfsdemovol01# df
Filesystem      1K-blocks   Used   Available  Use%   Mounted on
tmpfs            814396   1176   813220  1%   /run
/dev/mapper/ubuntu--vg-ubuntu--1V 15412168 3666428 10943132 26% /
tmpfs            4071960   0   4071960  0%   /dev/shm
tmpfs            5120   0   5120  0%   /run/lock
tmpfs            4096   0   4096  0%   /sys/fs/cgroup
/dev/sda2        999320 254996  675512 28%   /boot
tmpfs            814392   4   814388  1%   /run/user/1000
172.16.0.2:/nfsdemovol01 7951472 4241792  5195680 43%   /fsxcvotesting01/nfsdemovol01
198.19.254.239:/nfsdemovol01 536160   512   995648  1%   /fsx/nfsdemovol01
root@ubuntu01:/fsx/nfsdemovol01# cd /fsx/nfsdemovol01/
root@ubuntu01:/fsx/nfsdemovol01# ls
n1now111.txt
root@ubuntu01:/fsx/nfsdemovol01#
```

## 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 on-premises 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.



The Azure NetApp Files datastore capability is currently in public preview. Contact NetApp or Microsoft solution architects in your region for additional information.

### 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/>
- Integrate Azure NetApp Files with Azure VMware Solution  
<https://docs.microsoft.com/en-us/azure/azure-vmware/netapp-files-with-azure-vmware-solution>

## 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.

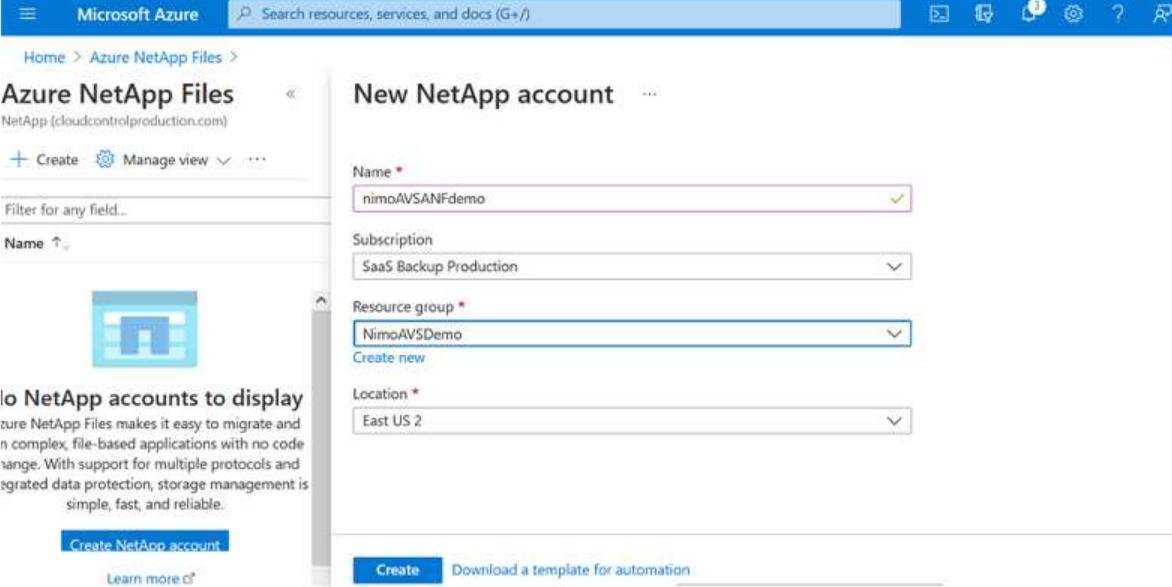


## Create and mount Azure NetApp Files volumes

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.



The screenshot shows the 'New NetApp account' creation page in the Azure portal. The 'Name' field is filled with 'nimoAVSANFDemo'. The 'Subscription' is set to 'SaaS Backup Production'. The 'Resource group' is 'NimoAVSDemo'. The 'Location' is 'East US 2'. At the bottom, there is a 'Create' button and a link to '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](#).

The screenshot shows the Azure NetApp Files portal. The left sidebar lists 'Azure NetApp Files' and 'nimoAVSANFdemo'. The main area shows the 'Capacity pools' blade for the 'nimoAVSANFdemo' account. A 'New capacity pool' dialog box is open, asking for a name (nimpool), service level (Standard), size (4 TiB), and QoS type (Auto). The 'Create' button is visible at the bottom of the dialog.

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](#).

The screenshot shows the Azure portal. The left sidebar lists 'Virtual network' and 'nimoavspriv-vnet'. The main area shows the 'Subnets' blade for the 'nimoavspriv-vnet' virtual network. A 'Add subnet' dialog box is open, asking for a name (anfdel), subnet address range (172.24.3.0/28), and other settings like NAT gateway and Network security group. The 'Save' button is visible at the bottom of the dialog.

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.

Join Active Directory

Primary DNS \* 172.24.1.5

Secondary DNS

AD DNS Domain Name \* nimodemo.com

AD Site Name

SMB Server (Computer Account) Prefix \* nim smb

Organizational Unit Path

Join

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

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

Basics Protocol Tags Review + create

This page will help you create an Azure NetApp Files volume in your subscription and enable you to access the volume from within your virtual network. [Learn more about Azure NetApp Files](#)

Volume details

Volume name \* nimvoltest1

Capacity pool \* nimcappool

Available quota (GiB) 4096 4 TiB

Quota (GiB) \* 100 100 GiB

Review + create < Previous Next : Protocol >

Home > Azure NetApp Files > nimoAVSANFdemo

nimoAVSANFdemo | Volumes

NetApp account

Search (Ctrl +/)

Add volume Refresh

Quota

Properties

Locks

Azure NetApp Files

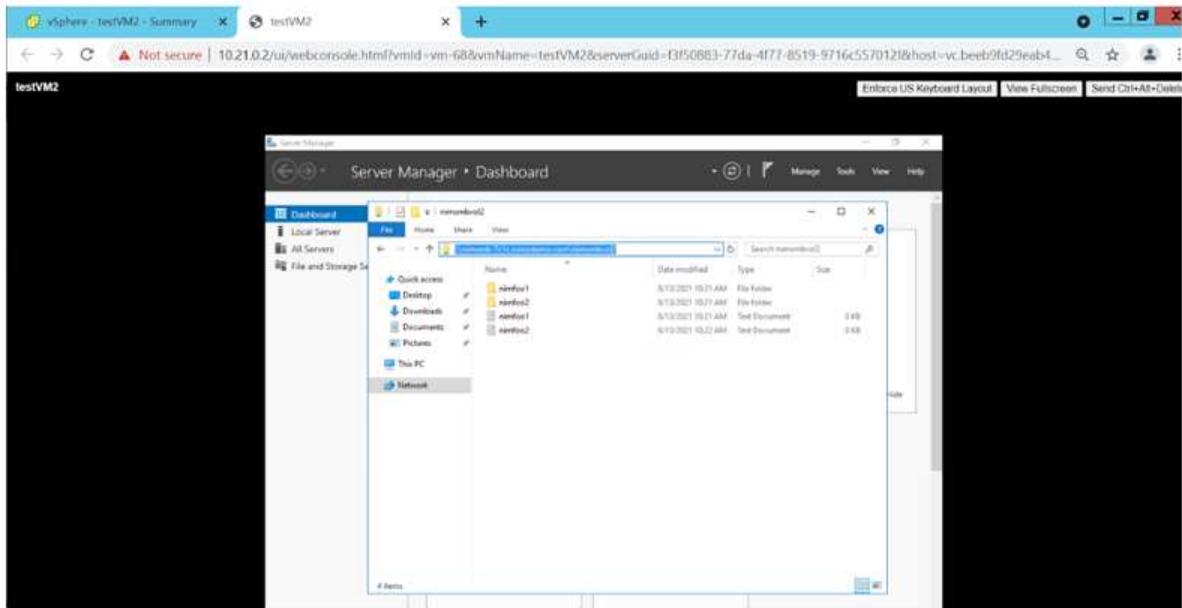
Active Directory connections

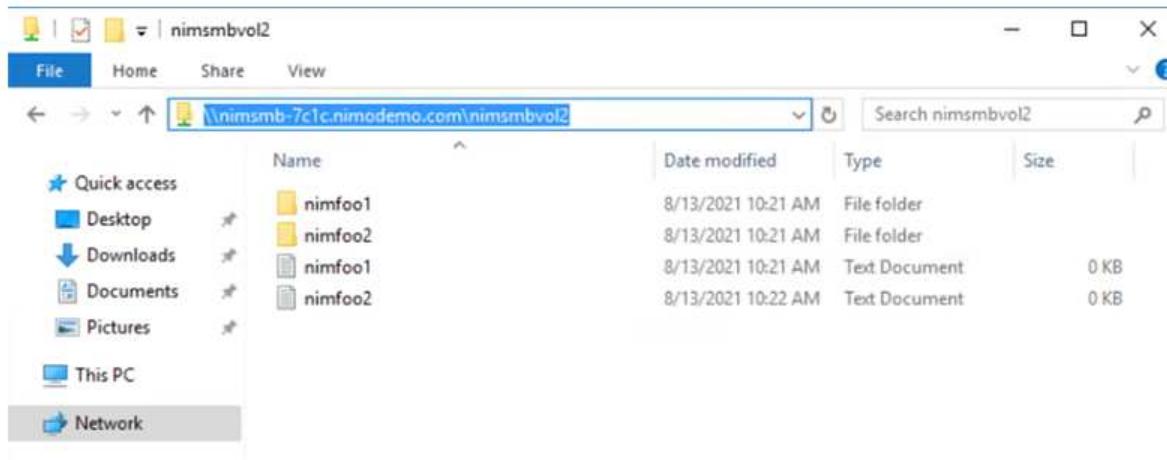
Name	Quota	Throughput	Protocol type	Mount path	Service level	Capacity pc
nimsmbvol2	100 GiB	1.6 MiB/s	SMB	\\\nimsmb-7c1c.nimodr	Standard	nimcapp00
nimvoltest1	100 GiB	1.6 MiB/s	NFSv3	172.24.3.4/nimvoltest1	Standard	nimcapp00

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.





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.

```

nimoadmin@nimoadmin-virtual-machine:~$ sudo mount -t nfs -o rw,hard,tcp 172.24.3.4:/nimodemofsv1 /home/nimoadmin/nimodemo11
nimoadmin@nimoadmin-virtual-machine:~$ df
Filesystem      1K-blocks    Used Available Use% Mounted on
udev             8168112      0  8168112   0% /dev
tmpfs            1639548   1488  1638060   1% /run
/dev/sda5      50824704 7902752 40310496  17% /
tmpfs            8197728      0  8197728   0% /dev/shm
tmpfs             5120       0   5120    0% /run/lock
tmpfs            8197728      0  8197728   0% /sys/fs/cgroup
/dev/loop0        56832    56832      0 100% /snap/core18/2128
/dev/loop2        66688    66688      0 100% /snap/gtk-common-themes/1515
/dev/loop1        224256   224256      0 100% /snap/gnome-3-34-1804/72
/dev/loop3        52224    52224      0 100% /snap/snap-store/547
/dev/loop4        33152    33152      0 100% /snap/snapd/12704
/dev/sda1        523248       4  523244   1% /boot/efi
tmpfs            1639544    52       1639492   1% /run/user/1000
/dev/sr0           54738    54738      0 100% /media/nimoadmin/VMware Tools
172.24.3.4:/nimodemofsv1 104857600      0 104857600   0% /home/nimoadmin/nimodemo11
nimoadmin@nimoadmin-virtual-machine:~$
```

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 your 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**



## Deploy new Cloud Volumes ONTAP in Azure

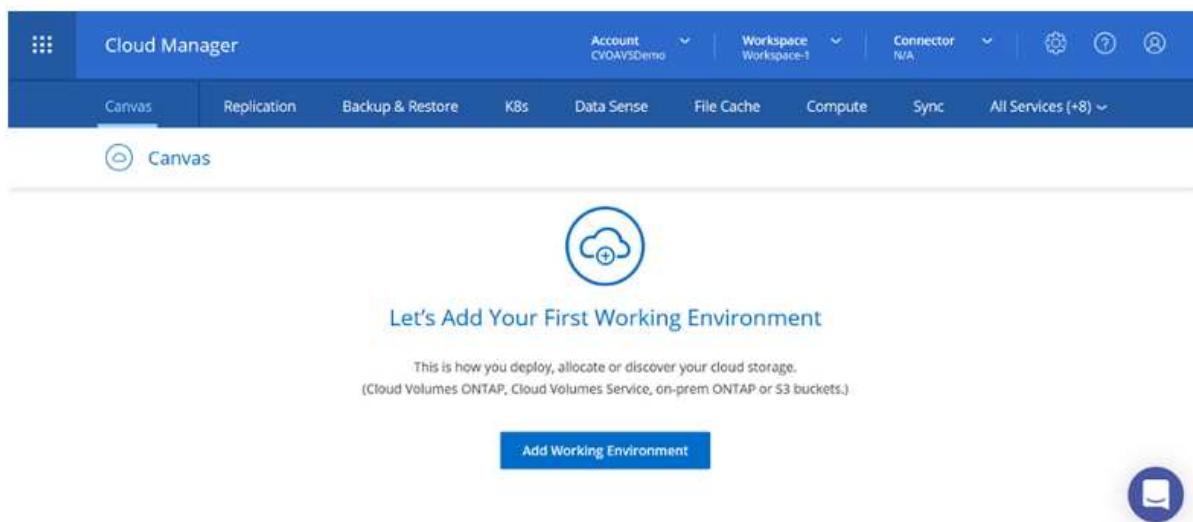
Cloud Volumes ONTAP shares and LUNs can be mounted from VMs that are created in the Azure VMware Solution SDDC environment. The volumes can also be mounted on the Linux client and on Windows client because Cloud Volumes ONTAP supports iSCSI, SMB, and NFS protocols. Cloud Volumes ONTAP volumes can be 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](#).

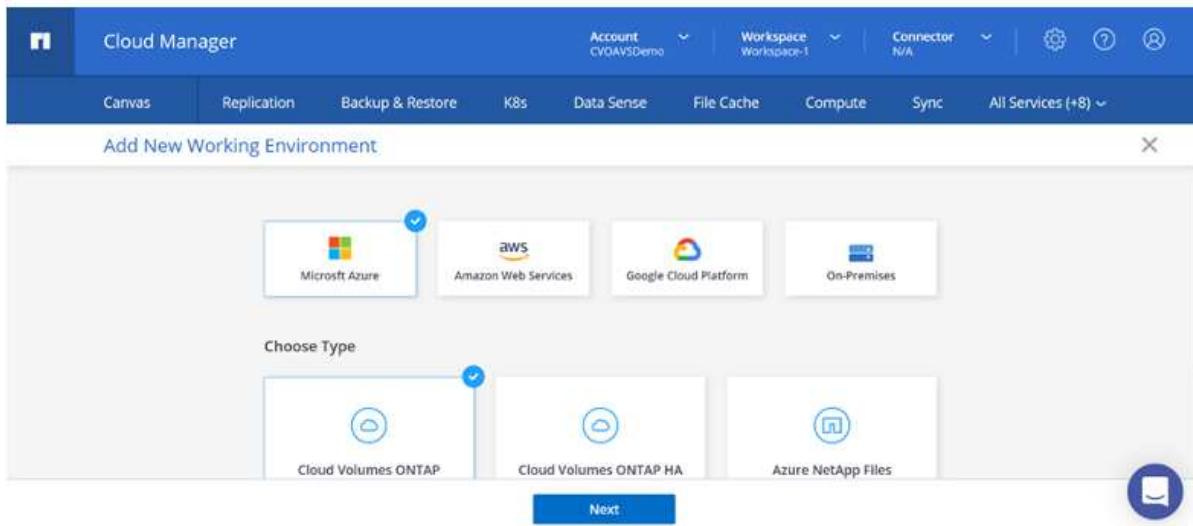


Use [Cloud Volumes ONTAP sizer](#) to accurately size the Cloud Volumes ONTAP instances. Also monitor on-premises performance to use as inputs in the Cloud Volumes ONTAP sizer.

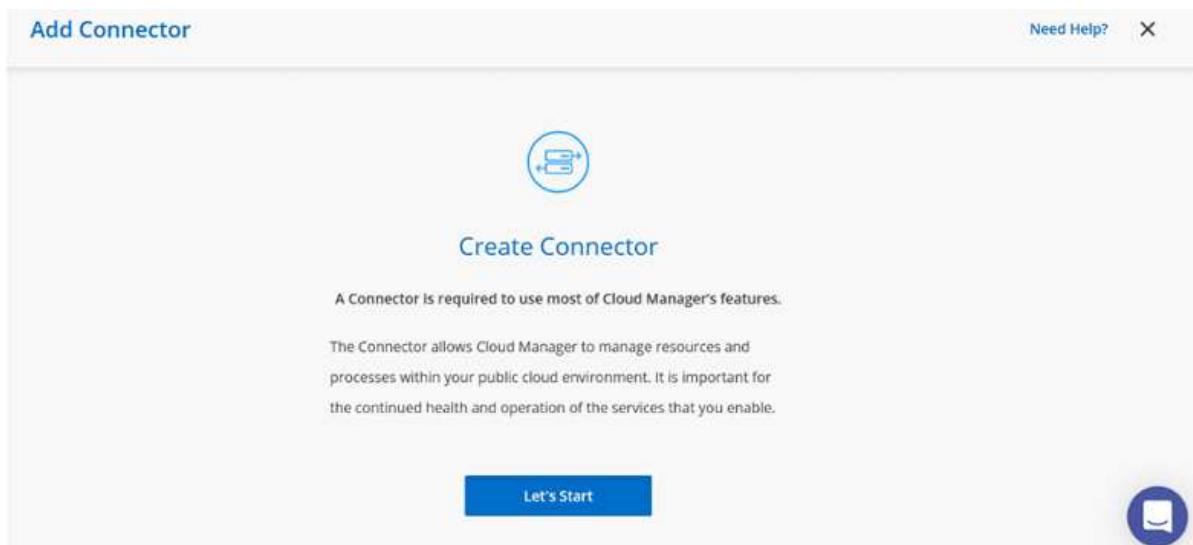
1. Log in to NetApp Cloud Central—the Fabric View screen is displayed. Locate the Cloud Volumes ONTAP tab and select Go to Cloud Manager. After you are logged in, the Canvas screen is displayed.



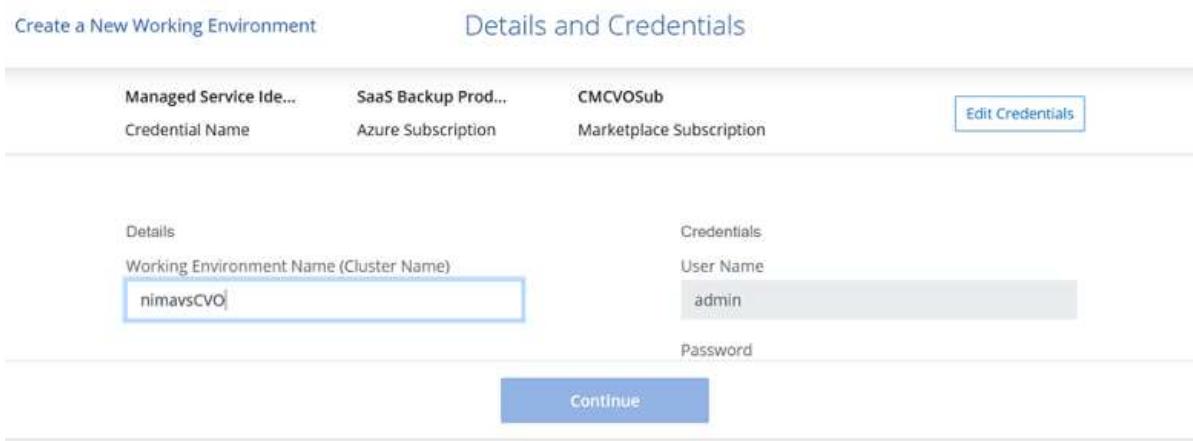
2. On the Cloud Manager home page, click Add a Working Environment and then select Microsoft Azure as the cloud and the type of the system configuration.



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.



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.

Create a New Working Environment      Details and Credentials

Working Environment Name (Cluster Name)	User Name
nimavsCVO	admin
Add Resource Group Tags      Optional Field	
<input type="button" value="Continue"/>	

6. Select the add-on services for Cloud Volumes ONTAP deployment, including Cloud Data Sense, Cloud Backup, and Cloud Insights. Select the services and then click Continue.

Create a New Working Environment      Services

Data Sense & Compliance	<input checked="" type="checkbox"/>
Backup to Cloud	<input checked="" type="checkbox"/>
Monitoring	<input checked="" type="checkbox"/>
<input type="button" value="Continue"/>	

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

Create a New Working Environment      Location & Connectivity

Azure Region	East US 2	Resource Group
Availability Zone	(Optional)	<input checked="" type="radio"/> Create a new group <input type="radio"/> Use an existing group
Select an Availability Zone		Resource Group Name
VNet	nimoavspriv-vnet   NimoAVSDemo	Security Group
Subnet	172.24.2.0/24	<input checked="" type="checkbox"/> I have verified network connectivity between the Cloud Manager server and the selected VNet.
<input type="button" value="Continue"/>		

8. Select the license option: Pay-As-You-Go or BYOL for using existing license. In this example, Pay-As-You-Go option is used.

## Create a New Working Environment Cloud Volumes ONTAP Charging Methods & NSS Account

### Cloud Volumes ONTAP Charging Methods

[Learn more about our charging methods](#)



Pay-As-You-Go by the hour



Bring your own license

### NetApp Support Site Account (Optional)

[Learn more about NetApp Support Site \(NSS\) accounts](#)

To register this Cloud Volumes ONTAP to support, you should add NetApp Support Site Account.

Don't have a NetApp Support Site account? Select go to finish deploying this system. After it's created, use the [Support Registration option](#) to create an NSS account.

[Continue](#)

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

## Create a New Working Environment

### Preconfigured Packages



Select a preconfigured Cloud Volumes ONTAP system that best matches your needs, or create your own configuration. Preconfigured settings can be modified at a later time.

[Change Configuration](#)



POC and small workloads  
Up to 500GB of storage



Database and application data production workloads



Cost effective DR  
Up to 500GB of storage



Highest performance production workloads

[Continue](#)

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

## Create a New Working Environment

### Review & Approve



**nimavscVO**

Azure | East US 2

- I understand that in order to activate support, I must first register Cloud Volumes ONTAP with NetApp. [More information](#) >
- I understand that Cloud Manager will allocate the appropriate Azure resources to comply with my above requirements. [More information](#) >

[Overview](#)

[Networking](#)

[Storage](#)

[Go](#)

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

[Canvas](#)[Go to Tabular View](#)[Add Working Environment](#)[nimavscvo](#)  
On[i](#) [⋮](#) [x](#)

## DETAILS

Cloud Volumes ONTAP | Azure | Single

## SERVICES

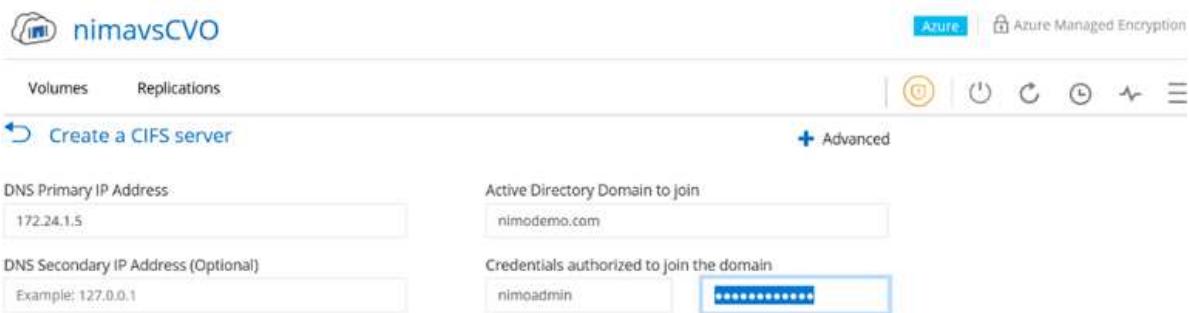
Replication

[Enter Working Environment](#)[-](#) [+](#)

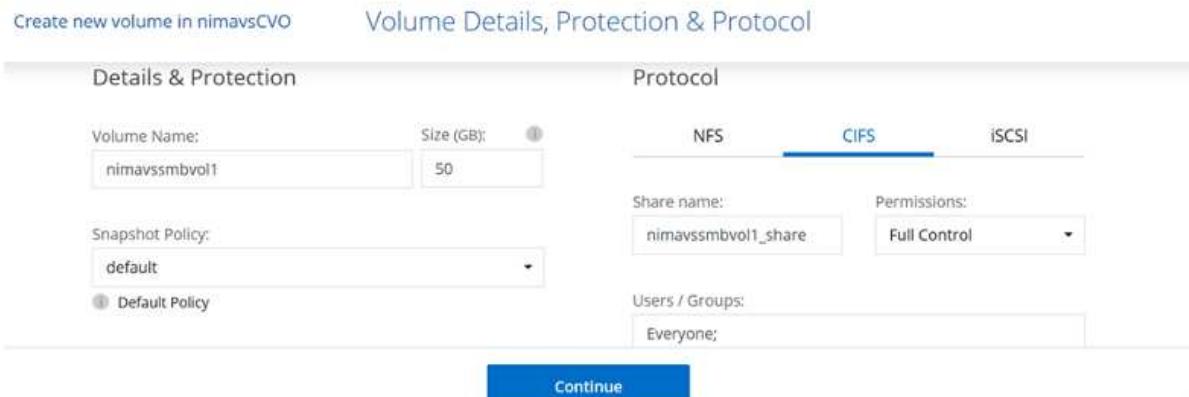


## Additional configurations for SMB volumes

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.



2. 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.



3. After the volume is provisioned, it will be available 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 Replications

Volumes

1 Volume | 50 GB Allocated | 1.74 MB Total Used (1.74 MB In Disk, 0 KB In Blob)

nimavssmbvol1

ONLINE

INFO

Disk Type: PREMIUM\_LRS

Tiering Policy: Auto

Backup: OFF

CAPACITY

1.74 MB Disk Used

0 GB Blob Used

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.

Volumes Replications

Mount Volume nimavssmbvol1

Go to your machine and enter this command

```
\\172.24.2.8\vimavssmbvol1_share
```

\\172.24.2.8\vimavssmbvol1\_share

File Home Share View

Search vimavssmbvol1\_share

Quick access

Desktop

Downloads

Documents

Pictures

This PC

Network



## 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: nimavsscsi1

Size (GB): 500

Snapshot Policy: default

Initiator Group: avsvmlIG

What about LUNs?

Map Existing Initiator Groups  Create Initiator Group

Continue

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:

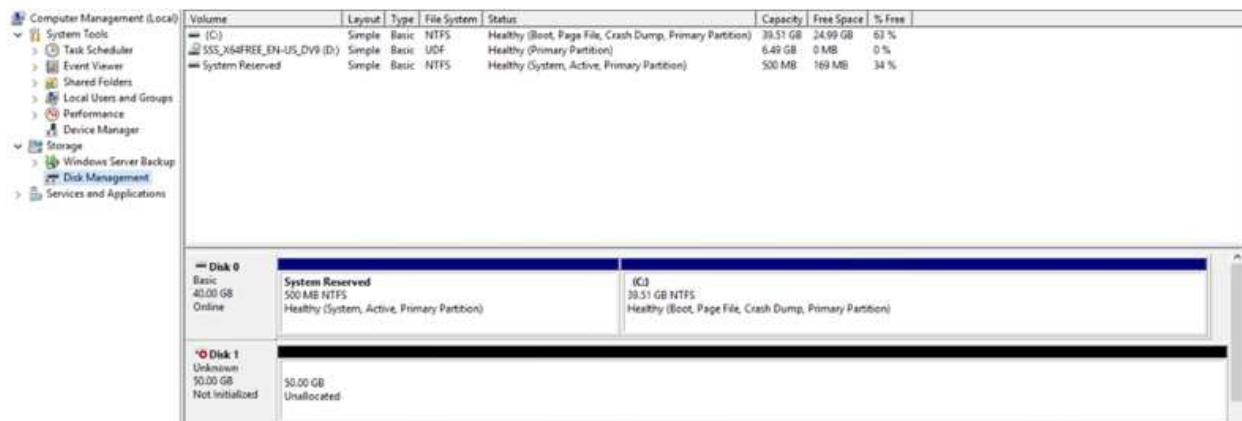
- a. RDP to the VM hosted on Azure VMware Solution SDDC.
- b. Open the iSCSI Initiator Properties dialog box: Server Manager > Dashboard > Tools > iSCSI Initiator.
- c. From the Discovery tab, click Discover Portal or Add Portal and then enter the IP address of the iSCSI target port.
- d. From the Targets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



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:

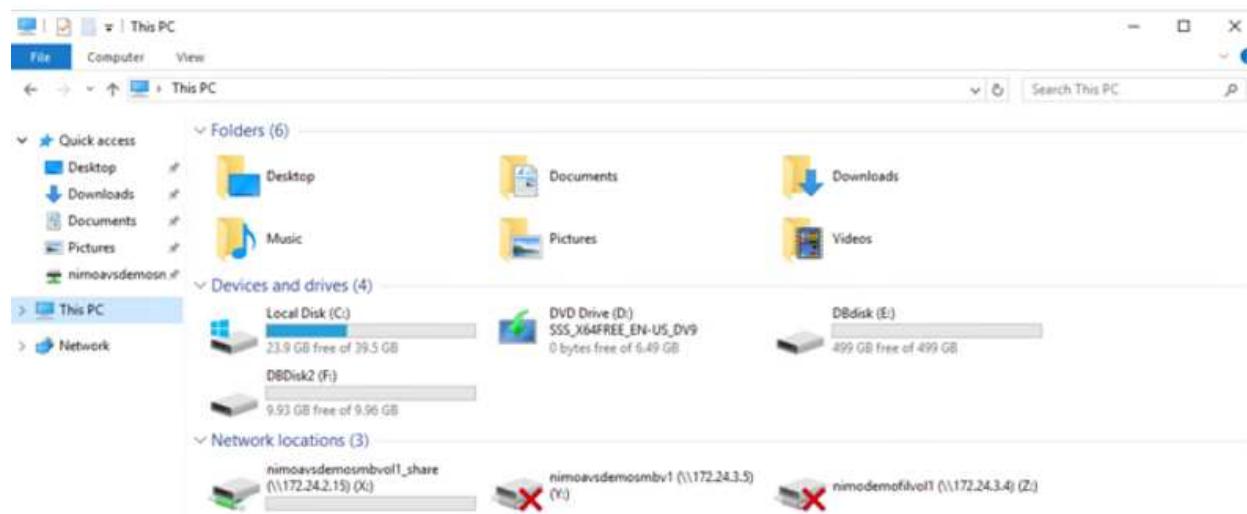
1. Open the Windows Computer Management utility: Start > Administrative Tools > Computer Management.
2. Expand the Storage node in the navigation tree.
3. Click Disk Management.
4. Click Action > Rescan Disks.



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:

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



## 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 your 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**



## Deploy Cloud Volumes ONTAP in Google Cloud (Do It Yourself)

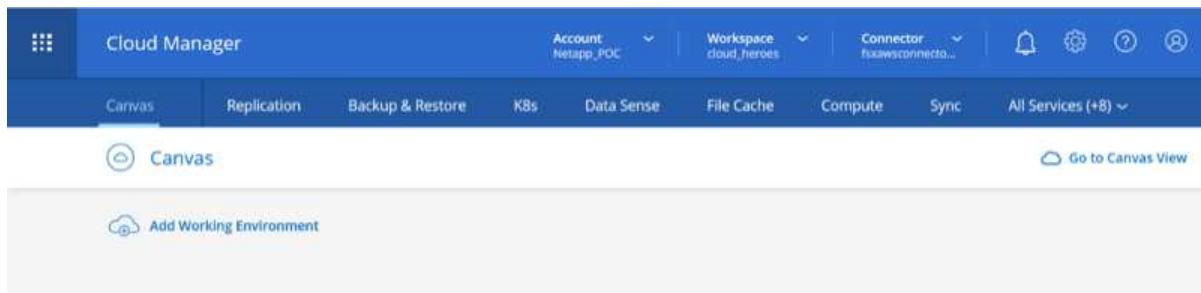
Cloud Volumes ONTAP shares and LUNs can be mounted from VMs that are created in the GCVE private cloud environment. The volumes can also be mounted on the Linux client and on Windows client and LUNs can be accessed on Linux or Windows clients as block devices when mounted over iSCSI because Cloud Volumes 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/gcp/Setting up data replication between systems](#).

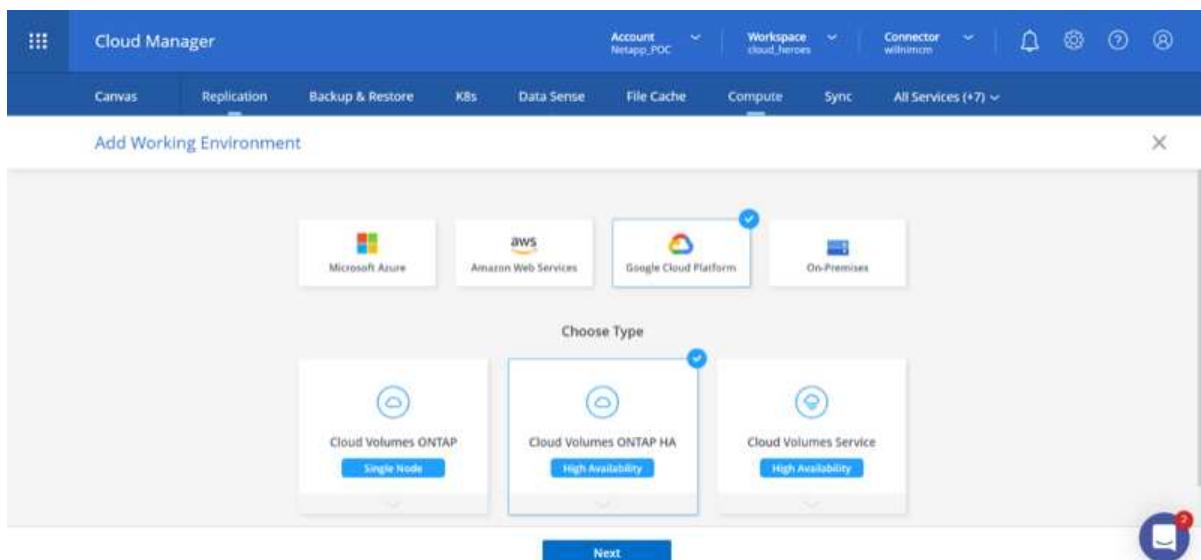


Use [Cloud Volumes ONTAP sizer](#) to accurately size the Cloud Volumes ONTAP instances. Also monitor on-premises performance to use as inputs in the Cloud Volumes ONTAP sizer.

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 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.



3. Provide the details of the environment to be created including the environment name and admin credentials. After you are done, click Continue.

[↑ Previous Step](#)

CV-Performance-Testing

Google Cloud Project

HCLMainBillingAccountSubs...

Marketplace Subscription

[Edit Project](#)

## Details

Working Environment Name (Cluster Name)

cvogcveva

## Service Account



! **Notice:** A Google Cloud service account is required to use two features: backing up data using Backup

## Credentials

User Name

admin

Password

.....

Confirm Password

.....

[Continue](#)

4. 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.

[↑ Previous Step](#)

Data Sense &amp; Compliance



Backup to Cloud



⚠ **WARNING:** By turning off Backup to Cloud, future data recovery will not be possible in case of data corruption or loss

[Continue](#)

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

[↑ Previous Step](#) Location

GCP Region

europe-west3

Connectivity

VPC

cloud-volumes-vpc

GCP Zone

europe-west3-c

Subnet

10.0.6.0/24

I have verified connectivity between the target VPC and Google Cloud storage.

Firewall Policy

 Generated firewall policy Use existing firewall policy[Continue](#)

6. Select the license option: Pay-As-You-Go or BYOL for using existing license. In this example, Freemium option is used. Then, click on Continue.

[↑ Previous Step](#)

Cloud Volumes ONTAP Charging Methods

[Learn more about our charging methods](#) Pay-As-You-Go by the hour Bring your own license Freemium (Up to 500GB)

NetApp Support Site Account

[Learn more about NetApp Support Site \(NSS\) accounts](#)

NetApp Support Site Account

mchad

To add a new NetApp Support Site account, go to the Support - NSS Management tab.

[Continue](#)

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 preconfigured Cloud Volumes ONTAP system that best matches your needs, or create your own configuration.  
Preconfigured settings can be modified at a later time.

[Change Configuration](#)

POC and small workloads

Up to 500GB of storage



Database and application data production workloads



Cost effective DR

Up to 500GB of storage



Highest performance production workloads

[Continue](#)

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

Create a New Working Environment

Review & Approve

Previous Step [cvogcveval](#)

GCP | europe-west3

This Cloud Volumes ONTAP instance will be registered with NetApp support under the NSS Account **mchad**.

I understand that Cloud Manager will allocate the appropriate GCP resources to comply with my above requirements. [More information >](#)

Overview Networking Storage

Storage System: Cloud Volumes ONTAP Cloud Volumes ONTAP runs on: n2-standard-4

License Type: Cloud Volumes ONTAP Freemium Encryption: Google Cloud Managed

Capacity Limit: 500GB Write Speed: Normal

**Go**

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

Cloud Manager

Canvas Replication Backup & Restore K8s Data Sense File Cache Compute Sync All Services (+7) ▾

Canvas Add Working Environment

Working Environments

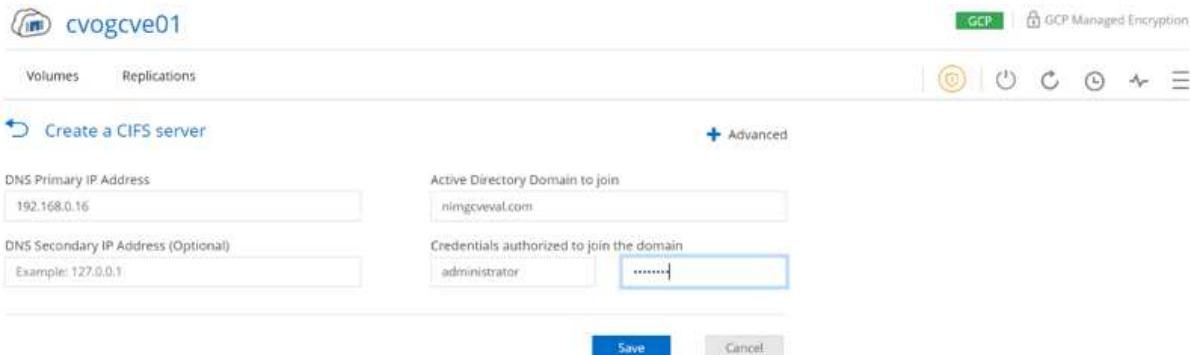
- cvogcveval Cloud Volumes ONTAP 43.05 GiB Provisioned Capacity
- DatacenterDude Azure NetApp Files 9.71 TiB Provisioned Capacity
- FSx for ONTAP (High-Availability) 0 B Provisioned Capacity
- Azure NetApp Files 9.71 TiB Provisioned Capacity



## Additional configurations for SMB volumes

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.



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.

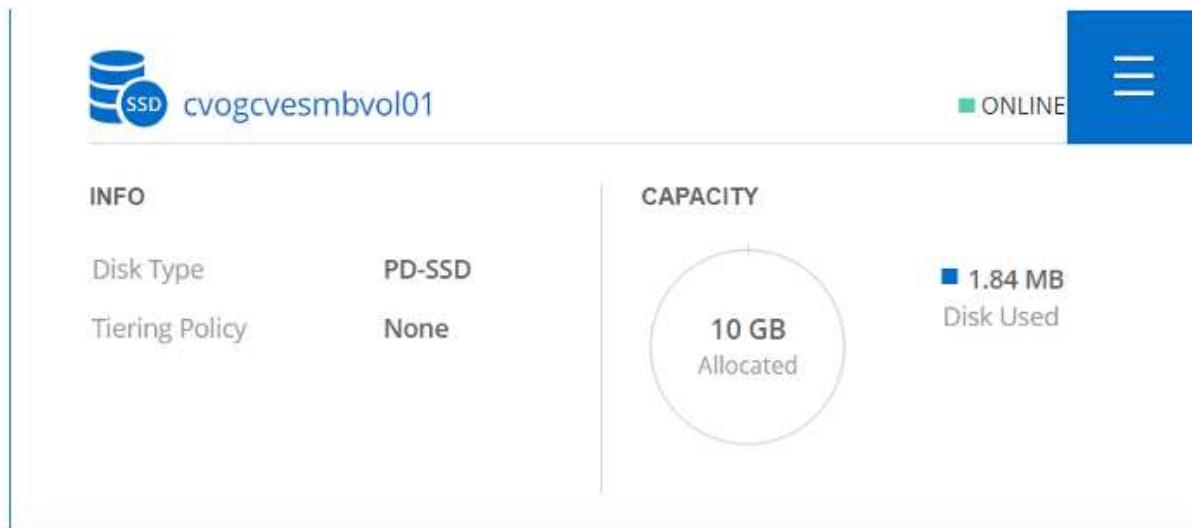
Create new volume in cvogcve01      Volume Details, Protection & Protocol

Details & Protection		Protocol
Volume Name: cvogcvesmbvol01	Size (GB): 10	<input checked="" type="radio"/> NFS <input type="radio"/> CIFS <input type="radio"/> iSCSI
Snapshot Policy: default		Share name: cvogcvesmbvol01_share    Permissions: Full Control
<input checked="" type="radio"/> Default Policy		Users / Groups: Everyone;    Valid users and groups separated by a semicolon

**Continue**

3. After the volume is provisioned, it will be available 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.



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.



Volumes Replications

#### Mount Volume cvogcvesmbvol01

Go to your machine and enter this command

\\10.0.6.251\cvogcvesmbvol01\_share

Copy

5. Copy the following path and use the Map Network Drive option to mount the volume on the VM running on the Google Cloud VMware Engine.

Specify the drive letter for the connection and the folder that you want to connect to:

Drive: Y:

Folder: \\10.0.6.251\cvogcvesmbvol01\_share

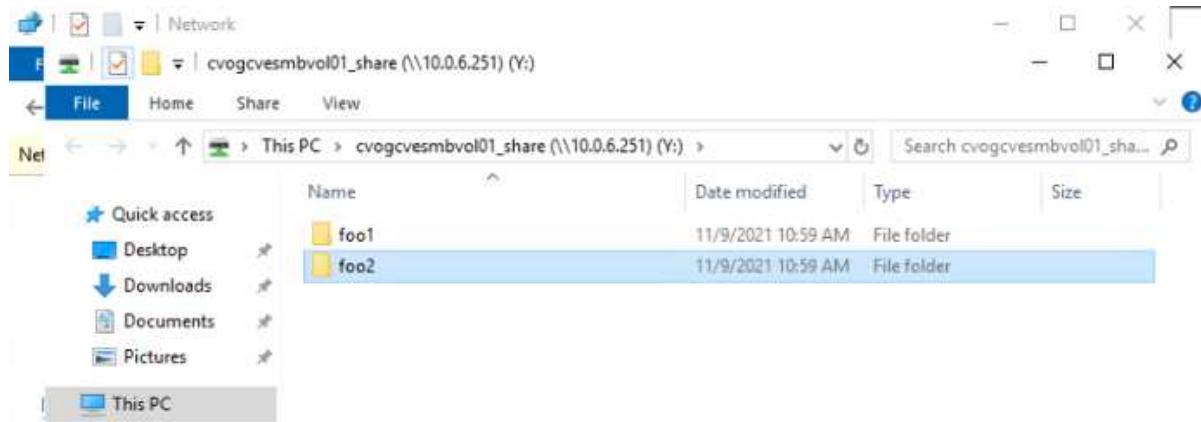
Example: \\server\share

Reconnect at sign-in

Connect using different credentials

[Connect to a Web site that you can use to store your documents and pictures.](#)

Once mapped, it can be easily accessed, and the NTFS permissions can be set accordingly.





## Connect the LUN on Cloud Volumes ONTAP to a host

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.

The image shows two screenshots. The top screenshot is a 'Create new volume in cvogcve01' dialog titled 'Volume Details, Protection & Protocol'. It has two tabs: 'Details & Protection' and 'Protocol'. Under 'Protocol', 'iSCSI' is selected. A sub-section 'Initiator Group' shows 'WinIG' selected. The bottom screenshot is a 'vmcd01' Server Manager dashboard showing a file list with three entries: 'Analyze01', 'analog01', and 'analog02'.

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.

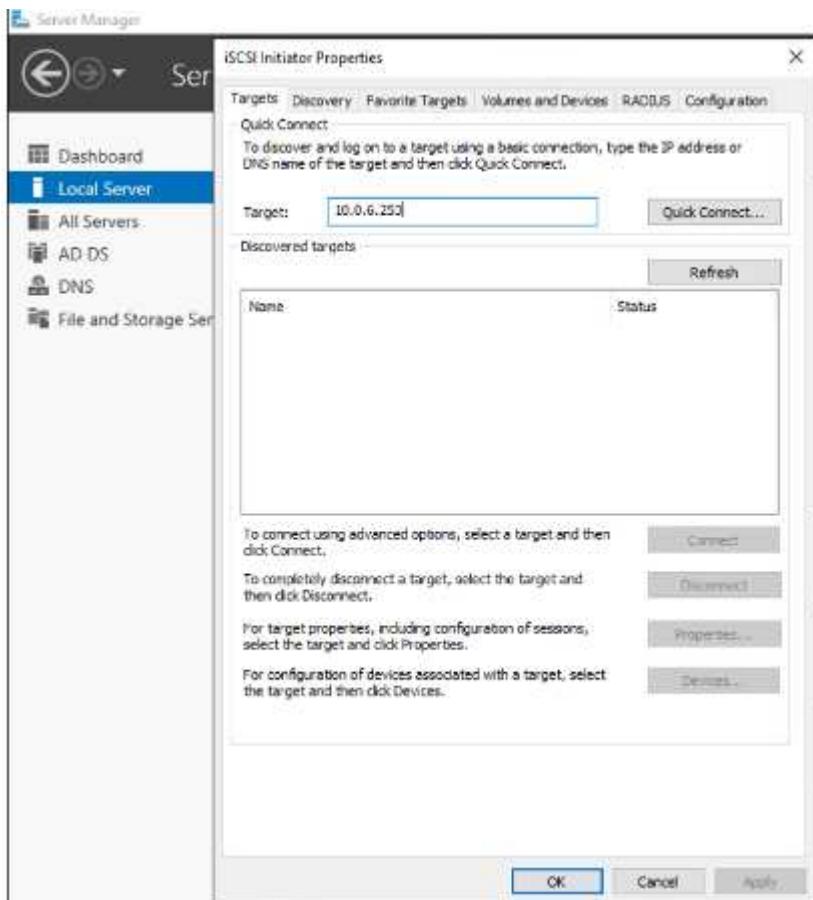
To accomplish the same for the host residing on Google Cloud VMware Engine:

- 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.

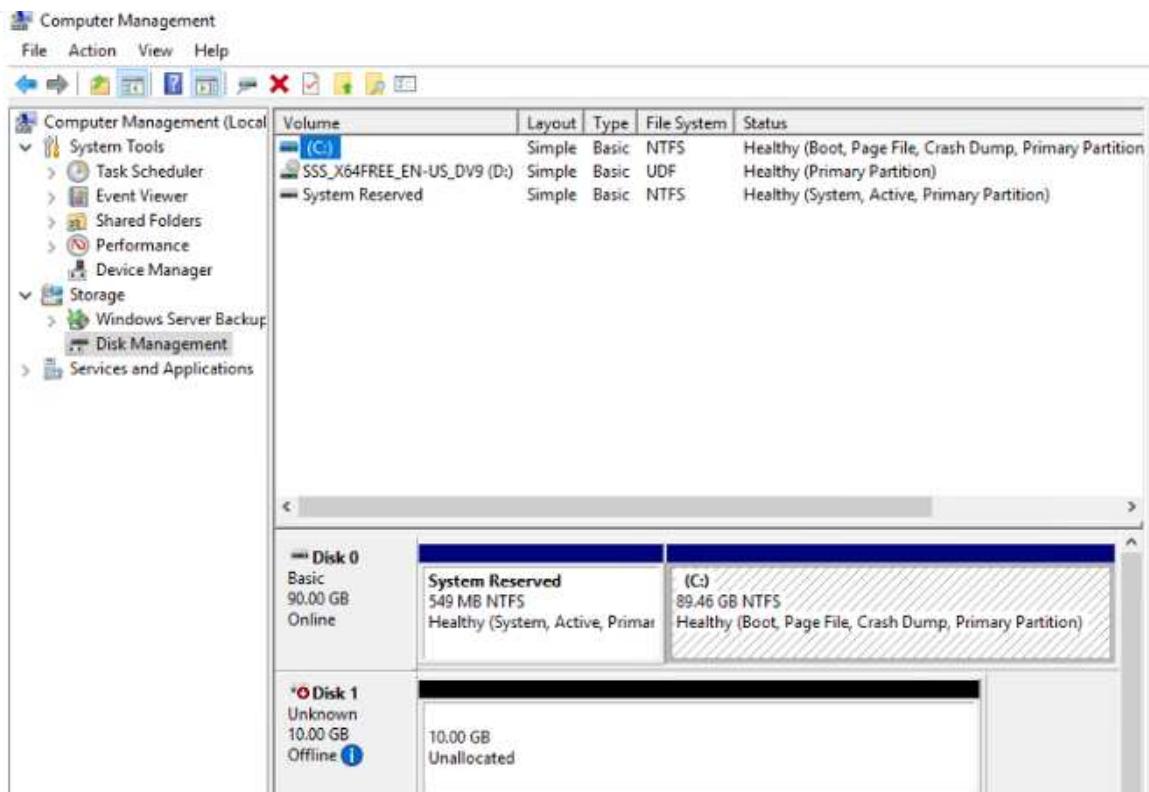


The Windows host must have an iSCSI connection to each node in the cluster.  
The native DSM selects the best paths to use.



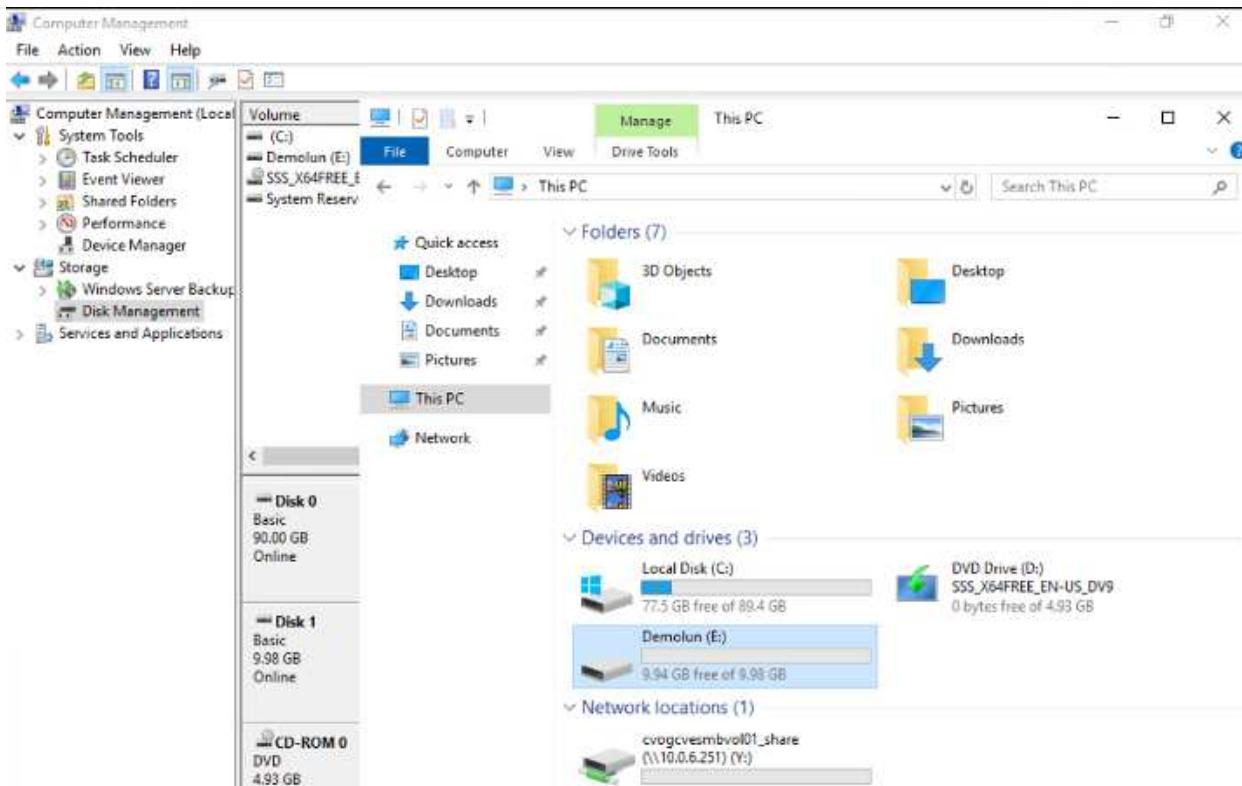
LUNs on storage virtual machine (SVM) appear as disks to the Windows host. Any new disks that are added are not automatically discovered by the host. Trigger a manual rescan to discover the disks by completing the following steps:

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 `lsblk` cmd from the shell.

```
niyaz@nimubu01:~$ lsblk
NAME   MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
loop0    7:0    0 55.4M  1 loop /snap/core18/2128
loop1    7:1    0 219M  1 loop /snap/gnome-3-34-1804/72
loop2    7:2    0 65.1M  1 loop /snap/gtk-common-themes/1515
loop3    7:3    0  51M  1 loop /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    0 15.5G 0 part /
sdb      8:16   0   1G  0 disk
```

```
niyaz@nimubu01:~$ df -h
Filesystem      Size  Used Avail Use% Mounted on
udev            1.9G   0    1.9G  0% /dev
tmpfs           394M  1.5M  392M  1% /run
/dev/sda5        16G  7.6G  6.9G  53% /
tmpfs           2.0G   0    2.0G  0% /dev/shm
tmpfs           5.0M   0    5.0M  0% /run/lock
tmpfs           2.0G   0    2.0G  0% /sys/fs/cgroup
/dev/loop1       219M  219M   0  100% /snap/gnome-3-34-1804/72
/dev/loop2       66M   66M   0  100% /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   0  100% /snap/snapd/12704
/dev/sda1       511M  4.0K  511M  1% /boot/efi
tmpfs           394M  64K  394M  1% /run/user/1000
/dev/loop5       33M   33M   0  100% /snap/snapd/13640
/dev/loop6       56M   56M   0  100% /snap/core18/2246
/dev/loop7      128K  128K   0  100% /snap/bare/5
/dev/loop8       66M   66M   0  100% /snap/gtk-common-themes/1519
/dev/sdb        976M  2.6M  907M  1% /mnt
```

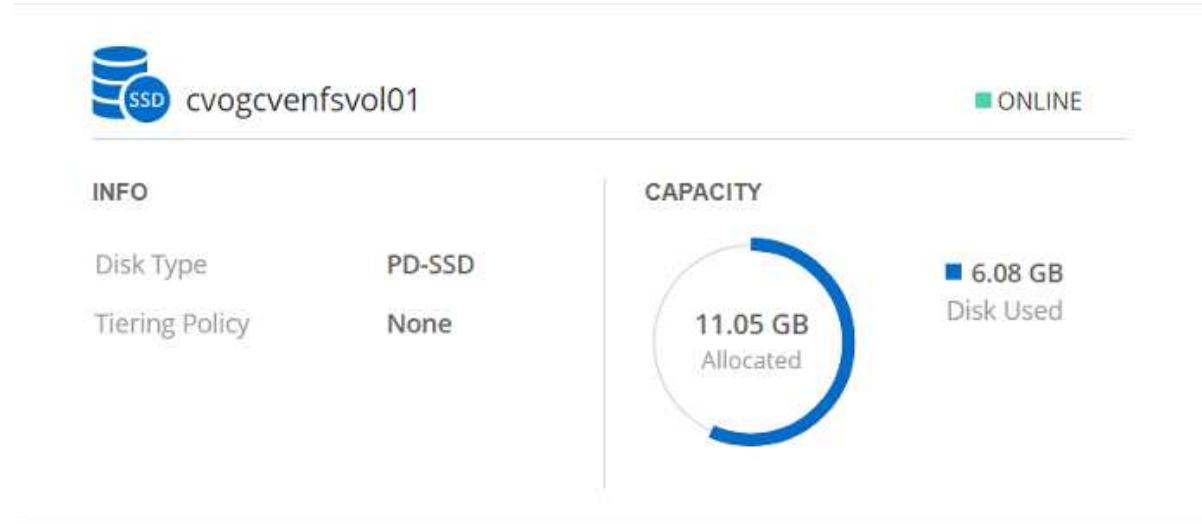


## Mount Cloud Volumes ONTAP NFS volume on Linux client

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:



3. In the Volumes tab, place your mouse cursor over the volume, select the menu icon (°), and then click Mount Command.

Volumes      Replications

 [Mount Volume cvogcvenfsvol01](#)

Go to your Linux machine and enter this mount command

```
mount 10.0.6.251:/cvogcvenfsvol01 <dest_dir>
```

 [Copy](#)

4. Click Copy.
5. Connect to the designated Linux instance.
6. Open a terminal on the instance using secure shell (SSH) and log in with the appropriate credentials.
7. Make a directory for the volume's mount point with the following command.

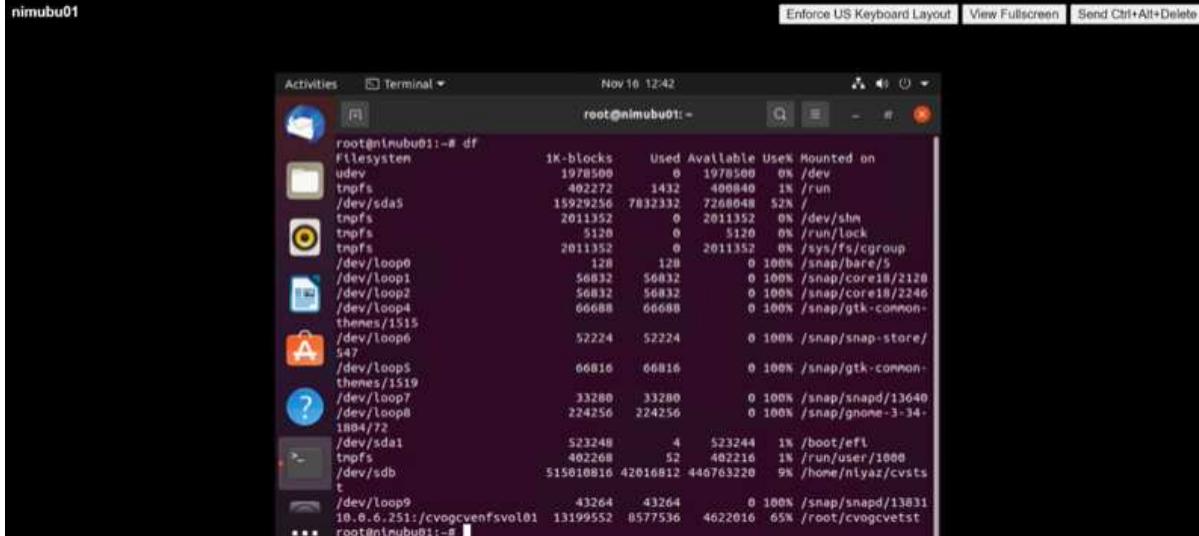
```
$ sudo mkdir /cvogcvetst
```

```
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
```



## 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.

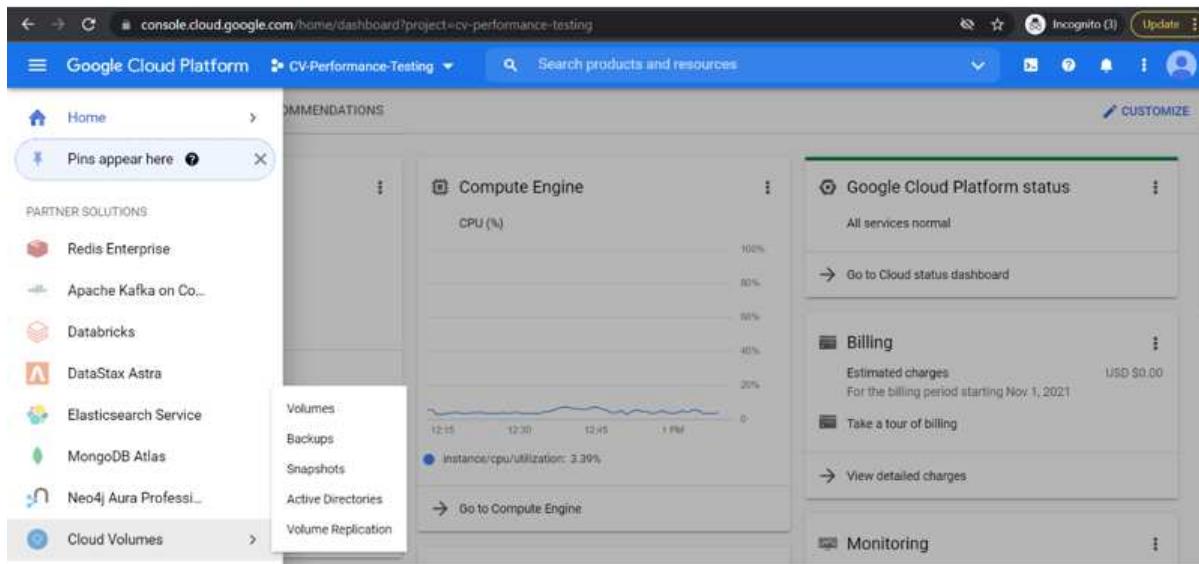
To purchase, enable and configure NetApp Cloud Volumes Service for Google Cloud from the Google Cloud Marketplace, follow this detailed [guide](#).



## Create a CVS NFS volume to GCVE private cloud

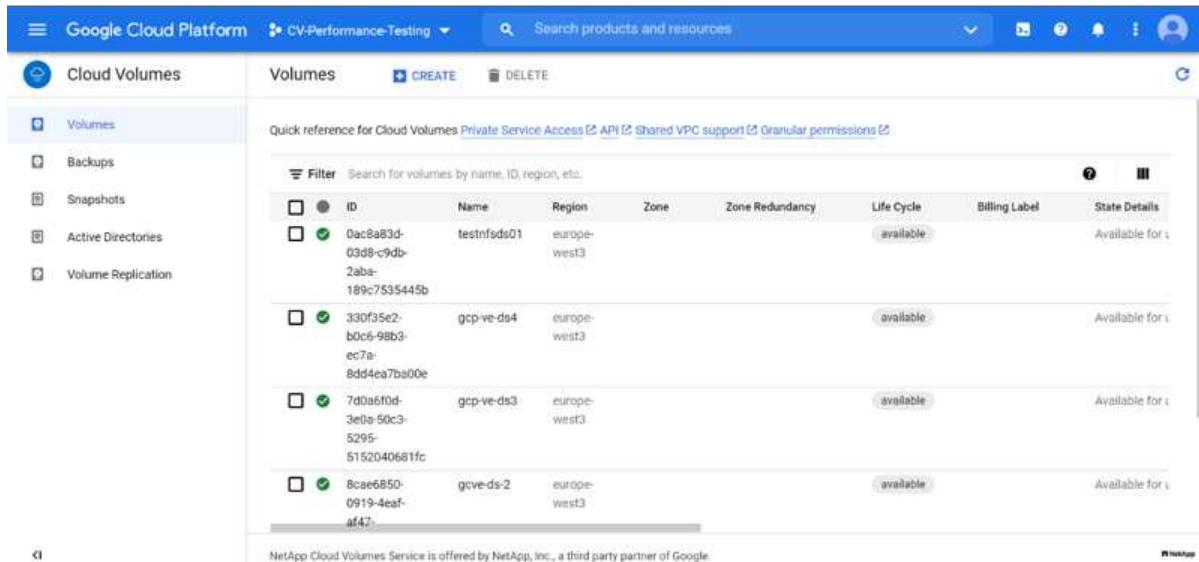
To create and mount NFS volumes, complete the following steps:

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



The screenshot shows the Google Cloud Platform dashboard for the project 'CV-Performance-Testing'. The 'Cloud Volumes' option is highlighted in the 'PARTNER SOLUTIONS' sidebar. A dropdown menu for 'Cloud Volumes' is open, showing sub-options: Volumes, Backups, Snapshots, Active Directories, and Volume Replication. The 'Volumes' option is selected. The main content area displays a 'Compute Engine' dashboard with a CPU utilization chart and a 'Google Cloud Platform status' section indicating 'All services normal'.

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



The screenshot shows the 'Volumes' page within the Cloud Volumes console. The page has a sidebar with options: Volumes, Backups, Snapshots, Active Directories, and Volume Replication. The 'Volumes' option is selected. At the top, there are 'CREATE' and 'DELETE' buttons. The main area shows a table of existing volumes, each with a checkbox, an ID, a name, a region, a zone, a zone redundancy, a life cycle status, a billing label, and a state details column. The table includes the following data:

ID	Name	Region	Zone	Zone Redundancy	Life Cycle	Billing Label	State Details
0ac8a83d-03d8-c9db-2a8a-189c7535445b	testnfsds01	europe-west3			available		Available for use
330f35e2-b0c6-98b3-ec7a-8dd4ea7ba00e	gcp-ve-ds4	europe-west3			available		Available for use
7d0a610d-3e0a-50c3-5295-5152040681fc	gcp-ve-ds3	europe-west3			available		Available for use
8cae6850-0919-4eaf-af47-	gcve-ds-2	europe-west3			available		Available for use

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

 <b>Cloud Volumes</b> <ul style="list-style-type: none"> <li> <a href="#">Volumes</a></li> <li> <a href="#">Backups</a></li> <li> <a href="#">Snapshots</a></li> <li> <a href="#">Active Directories</a></li> <li> <a href="#">Volume Replication</a></li> </ul>	<p><a href="#">← Create File System</a></p> <p> <b>Volumes</b></p> <p><b>Volume Name</b></p> <p>Name * <input type="text" value="nimCVNFSvol01"/></p> <p>A human readable name used for display purposes.</p> <p><b>Billing Labels</b></p> <p>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.</p> <p><a href="#">+ ADD LABEL</a></p>
--	--

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.

 <b>Cloud Volumes</b> <ul style="list-style-type: none"> <li> <a href="#">Volumes</a></li> <li> <a href="#">Backups</a></li> <li> <a href="#">Snapshots</a></li> <li> <a href="#">Active Directories</a></li> <li> <a href="#">Volume Replication</a></li> </ul>	<p><a href="#">← Create File System</a></p> <p><b>Service Type</b></p> <p>Cloud Volumes Service is offered as two service types: CVS and CVS-Performance. Select the service type that matches your workload needs. <a href="#">Region availability</a> varies by service type. <a href="#">Learn more</a></p> <p><input checked="" type="radio"/> <b>CVS</b> Offers volumes created with zonal high availability.</p> <p><input checked="" type="radio"/> <b>CVS-Performance</b> Offers 3 performance levels and improved latency to address higher performance application requirements.</p> <p><b>Volume Replication</b></p> <p><input type="checkbox"/> <b>Secondary</b> Select to create volume as a destination target for volume replication. Applicable only to CVS-performance volumes.</p>
--	--

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)

 <b>Cloud Volumes</b> <ul style="list-style-type: none"> <li> <a href="#">Volumes</a></li> <li> <a href="#">Backups</a></li> <li> <a href="#">Snapshots</a></li> <li> <a href="#">Active Directories</a></li> <li> <a href="#">Volume Replication</a></li> </ul>	<p><a href="#">← Create File System</a></p> <p><b>Region</b></p> <p>Region availability varies by service type.</p> <p>Region * <input type="text" value="europe-west3"/></p> <p>Volume will be provisioned in the region you select.</p> <p>Volume Path * <input type="text" value="nimCVSNFSvol01"/></p> <p>Must be unique to the project.</p>
--	--

6. Select the level of performance for the volume.

The screenshot shows the 'Create File System' wizard. On the left, a sidebar lists 'Cloud Volumes' options: Volumes (selected), Backups, Snapshots, Active Directories, and Volume Replication. The main panel is titled 'Service Level' with the sub-instruction 'Select the performance level required for your workload.' It shows three radio button options: 'Standard' (selected, 'Up to 16 MiB/s per TiB'), 'Premium' (Up to 64 MiB/s per TiB), and 'Extreme' (Up to 128 MiB/s per TiB). Below these is a dropdown menu labeled 'Snapshot' with the sub-instruction 'The snapshot to create the volume from.' A small downward arrow icon is to the right of the dropdown.

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

The screenshot shows the 'Create File System' wizard. The sidebar on the left is identical to the previous screenshot. The main panel is titled 'Volume Details' with the sub-instruction 'Allocated Capacity \*'. A text input field contains '1024' with a 'GiB' unit indicator. Below the input field is the sub-instruction 'Allocated size must be between 1 TiB (1024 GiB) and 100 TiB (102400 GiB)'. The next section is 'Protocol Type \*' with a dropdown menu showing 'NFSv3'. Below this are two optional checkboxes: 'Make snapshot directory (.snapshot) visible' (with a sub-instruction about visibility to clients) and 'Enable LDAP' (with a sub-instruction about user lookup from AD LDAP server).

8. In this step, select the VPC Network from which the volume will be accessible. Ensure VPC peering is in place.

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.

Cloud Volumes

Volumes

Backups

Snapshots

Active Directories

Volume Replication

← Create File System

Network Details

Shared VPC configuration  
Provide the host project name when deploying in a shared VPC service project.

VPC Network Name \*

Select the VPC Network from which the volume will be accessible. This cannot be changed later.

Use Custom Address Range  
Reserved Address range

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.

Cloud Volumes

Volumes

Backups

Snapshots

Active Directories

Volume Replication

← Create File System

Export Policy

Rules

Item 1

Allowed Clients 1 \*

Access

Read & Write  
 Read Only

Root Access

On  
 Off

Protocol Type (Select at least 1 of the below options)

Must select for Protocol type NFSv3. Optional for Protocol Type Both. Do not select for NFSv4.1

Allows Matching Clients for NFSv3

10. Click Save to create the volume.

	4b8ed9d9- bc6d-f3d5- 5a0f- 7da26aed3ed0	nimnfsdemods02	europe- west3	Available for use	CVS- Performance	Primary	Extreme	NFSv3 : 10.53.0.4/nimnfsdemods02
<input type="checkbox"/>								



## Mounting NFS exports to VMs running on VMware Engine

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:

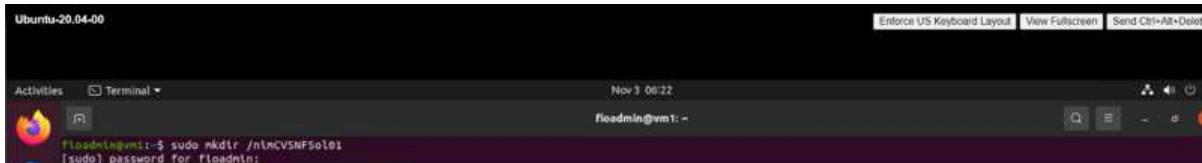
```
sudo yum install -y nfs-utils
```

- b. On an Ubuntu or Debian instance:

```
sudo apt-get install nfs-common
```

3. Create a new directory on the instance, such as "/nimCVSNFS01":

```
sudo mkdir /nimCVSNFS01
```



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:/nimCVSNFS01 /nimCVSNFS01
```

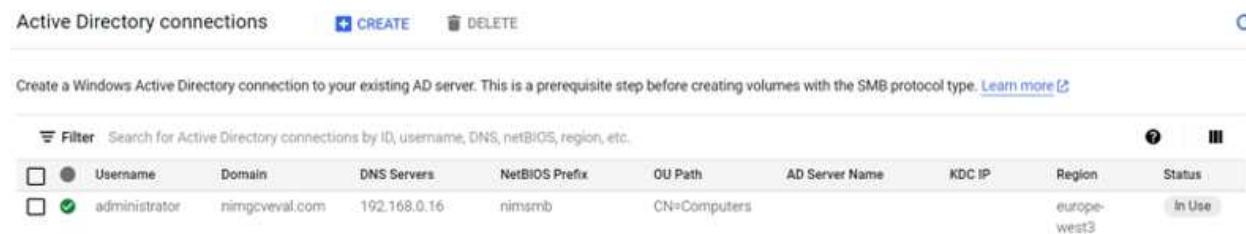
```
root@vm1:~# sudo mkdir /nimCVSNFS01  
root@vm1:~# sudo mount -t nfs -o rw,hard,rsize=65536,wsize=65536,vers=3,tcp 10.53.0.4:/nimCVSNFS01 /nimCVSNFS01
```

```
root@vm1:~# df
Filesystem      1K-blocks   Used   Available Use% Mounted on
udev            16409952     0    16409952  0% /dev
tmpfs           3288328    1580    3286748  1% /run
/dev/sdb5        61145932  19231356  38778832  34% /
tmpfs           16441628     0    16441628  0% /dev/shm
tmpfs            5120       0      5120  0% /run/lock
tmpfs           16441628     0    16441628  0% /sys/fs/cgroup
/dev/loop0        128       128      0 100% /snap/bare/5
/dev/loop1        56832     56832      0 100% /snap/core18/2128
/dev/loop2        66688     66688      0 100% /snap/gtk-common-themes/1515
/dev/loop4        66816     66816      0 100% /snap/gtk-common-themes/1519
/dev/loop3        52224     52224      0 100% /snap/snap-store/547
/dev/loop5        224256    224256      0 100% /snap/gnome-3-34-1804/72
/dev/sdb1        523248      4    523244  1% /boot/efi
tmpfs           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  363770996  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:/nimCVSNFSol01  107374182400      256 107374182144  1% /nimCVSNFSol01
root@vm1:~#
```



## Creating and Mounting SMB Share to VMs running on VMware Engine

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



<input type="checkbox"/>	<input checked="" type="checkbox"/>	Username	Domain	DNS Servers	NetBIOS Prefix	OU Path	AD Server Name	KDC IP	Region	Status
	<input checked="" type="checkbox"/>	administrator	nimgcveval.com	192.168.0.16	nimsmb	CN=Computers			europe-west3	In Use

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.

### [←](#) Create File System

#### Volume Name

Name \*

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.

[+ ADD LABEL](#)

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. [Region availability](#) varies by service type. [Learn more](#)

CVS

Offers volumes created with zonal high availability.

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.

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)

## [Create File System](#)

### Region

Region availability varies by service type.

Region \* —

europe-west3



Volume will be provisioned in the region you select.

Volume Path \* —

nimCVSMBvol01



Must be unique to the project.

5. Select the level of performance for the volume.

## [←](#) Create File System

### Service Level

Select the performance level required for your workload.

Standard

Up to 16 MiB/s per TiB

Premium

Up to 64 MiB/s per TiB

Extreme

Up to 128 MiB/s per TiB

Snapshot

The snapshot to create the volume from.

6. Specify the size of the volume and the protocol type. In this testing, SMB is used.

## [←](#) Create File System

### Volume Details

Allocated Capacity \*

1024

GiB

Allocated size must be between 1 TiB (1024 GiB) and 100 TiB (102400 GiB)

Protocol Type \*

SMB

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.

Enable CA share support for SQL Server, FSLogix

Enable this option only for SQL Server and FSLogix workloads that require continuous availability.

Hide SMB Share

Enable this option to make SMB shares non-browsable

7. In this step, select the VPC Network from which the volume will be accessible. Ensure VPC peering is in place.

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](#).

## Network Details

### Shared VPC configuration

Provide the host project name when deploying in a shared VPC service project.

### VPC Network Name \*

cloud-volumes-vpc

Select the VPC Network from which the volume will be accessible. This cannot be changed later.

### Use Custom Address Range

#### Reserved Address range

netapp-addresses

## SHOW SNAPSHOT POLICY

**SAVE**

**CANCEL**

8. Click Save to create the volume.

	6a4552ed-7378-7302-be2b-21a169374f28	nimCVSMBvol01	europe-west3	Available for use	CVS-Performance	Primary	Standard	SMB : \\nimsmb-3830.nimgcveval.com\\nimCVSMBvol01
<input type="checkbox"/>								

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



### What network folder would you like to map?

Specify the drive letter for the connection and the folder that you want to connect to:

Drive: Z:

Folder:

Example: \\server\share

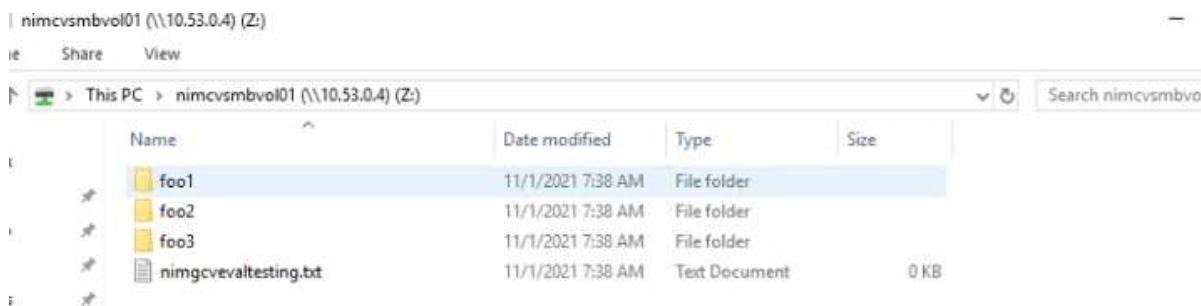
Reconnect at sign-in

Connect using different credentials

[Connect to a Web site that you can use to store your documents and pictures.](#)

To connect every time you log on to your computer, select the Reconnect at sign-in check box.

5. Click Finish.



### Region Availability for NFS datastores on AWS / VMC, Azure / AVS, and GCP / GCVE

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

#### AWS Region Availability

## 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)	No	Yes	No

Last updated on: June 2, 2022.

## Azure Region Availability

## Americas

Azure Region	AVS Availability	ANF Availability	NFS Datastore Availability
Central US	Yes	Yes	Yes
East US	Yes	Yes	Yes
East US 2	No	Yes	No
North Central US	Yes	Yes	Yes
South Central US	Yes	Yes	Yes
West Central US	No	No	No
West US	Yes	Yes	Yes
West US2	No	Yes	No
West US3	GA: H1-2023	Yes	Yes
Canada Central	Yes	Yes	Yes
Canada East	Yes	Yes	Yes
Brazil South	Yes	Yes	Yes
Brazil Southeast	No	GA: Q2-2022	No

Last updated on: June 7, 2022.

## EMEA

Azure Region	AVS Availability	ANF Availability	NFS Datastore Availability
North Europe	Yes	Yes	Yes
West Europe	No	Yes	No
France Central	Yes	Yes	Yes
France South	No	GA: H2-2022	No
Germany North	No	Yes	No
Germany West Central	Yes	Yes	Yes
Norway East	No	Yes	No
Norway West	No	Yes	No
Sweden Central	GA: Q2-2022	GA: Q2-2022	No
Sweden South	No	No	No
Switzerland North	No	Yes	No
Switzerland West	No	Yes	No
UAE Central	No	Yes	No
UAE North	No	Yes	No
UK South	Yes	Yes	Yes

UK West	Yes	Yes	Yes
---------	-----	-----	-----

Last updated on: June 7, 2022.

#### Asia Pacific

Azure Region	AVS Availability	ANF Availability	NFS Datastore Availability
Australia East	Yes	Yes	Yes
Australia Southeast	Yes	Yes	Yes
Australia Central	No	Yes	No
Japan East	Yes	Yes	No
Japan West	Yes	Yes	Yes
East Asia	No	Yes	No
Southeast Asia	Yes	Yes	Yes
Central India	No	Yes	No
South India	No	Yes	No
Korea Central	No	Yes	No

Last updated on: June 20, 2022.

#### 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 hybrid-cloud 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 native 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 Native Storage Options

While VMware in any cloud delivers unique hybrid capabilities to every 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—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 \(guest connected\)](#)

### Migrate

COMING SOON!!

### 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 \(native datastore\)](#)
- [Disaster Recovery with ANF and JetStream \(guest connected storage\)](#)

**Migrate**

COMING SOON!!

**Extend**

COMING SOON!!

## NetApp Solutions for Google Cloud Virtualization 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**

COMING SOON!!

**Migrate**

COMING SOON!!

**Extend**

COMING SOON!!

## NetApp Hybrid Multicloud Solutions for AWS / VMC

### Protecting Workloads

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

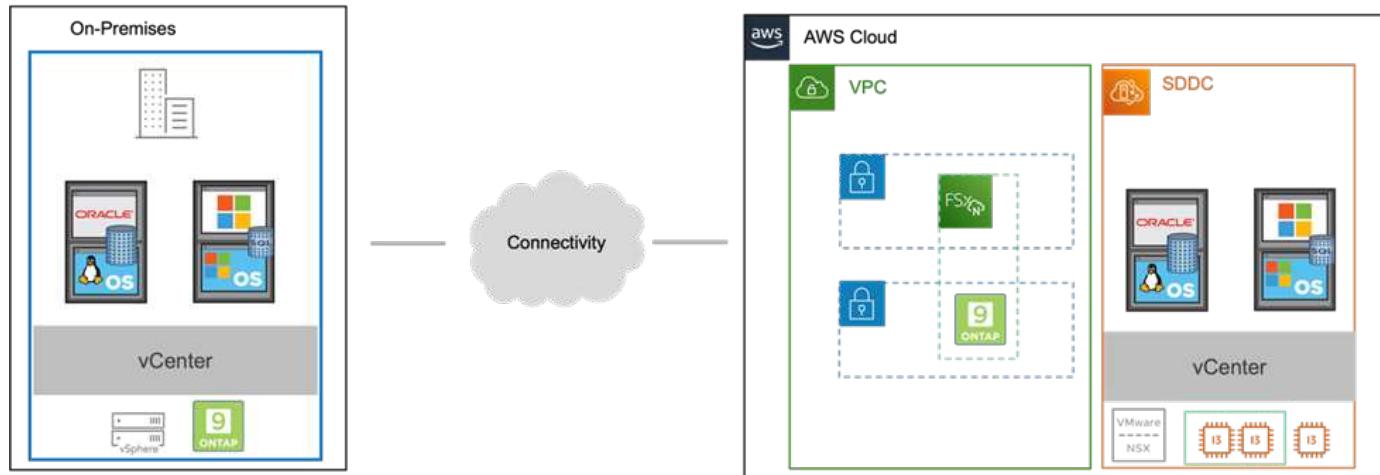
Chris Reno, Josh Powell, and Suresh Thoppay

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.

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.



[Next: Technology.](#)

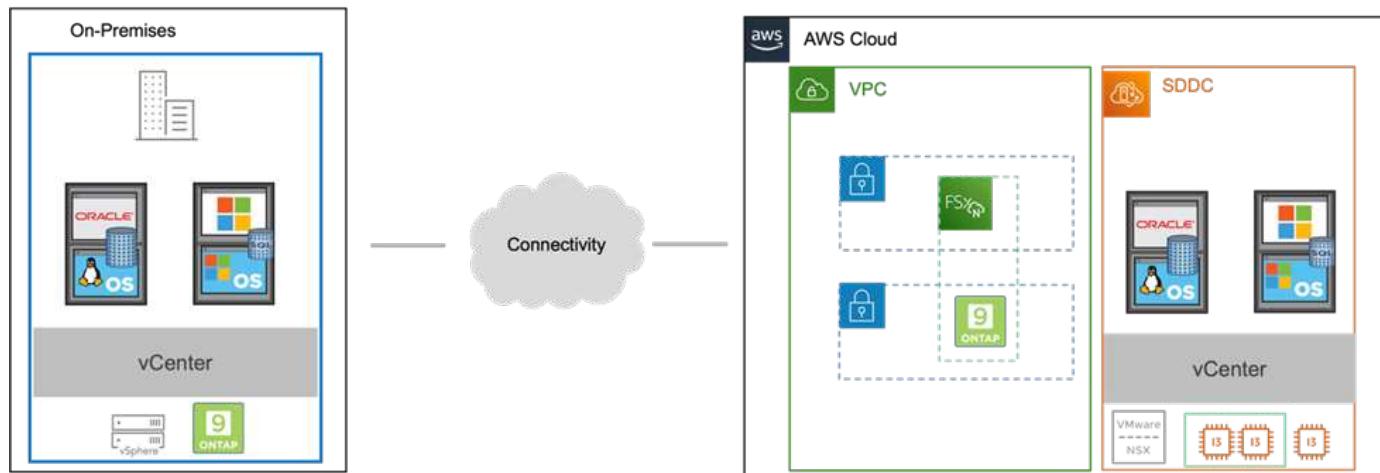
#### TR-4931: Disaster Recovery with VMware Cloud on Amazon Web Services and Guest Connect

Chris Reno, Josh Powell, and Suresh Thoppay

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.

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.



[Next: Technology.](#)

## Technology

[Previous: Solution overview.](#)

This solution includes innovative technologies from NetApp, VMware, Amazon Web Services (AWS), and Veeam.

## VMware

### VMware Cloud Foundation

The VMware Cloud Foundation platform integrates multiple products offerings that enable administrators to provision logical infrastructures across a heterogenous environment. These infrastructures (known as domains) provide consistent operations across private and public clouds. Accompanying the Cloud Foundation software is a bill of materials that identifies prevalidated and qualified components to reduce risk for customers and ease deployment.

The components of the Cloud Foundation BoM include the following:

- Cloud Builder
- SDDC Manager
- VMware vCenter Server Appliance
- VMware ESXi
- VMware NSX
- vRealize Automation
- vRealize Suite Lifecycle Manager
- vRealize Log Insight

For more information on the VMware Cloud Foundation, see the [VMware Cloud Foundation documentation](#).

### VMware vSphere

VMware vSphere is a virtualization platform that transforms physical resources into pools of compute, network, and storage that can be used to satisfy customers' workload and application requirements. The main components of VMware vSphere include the following:

- **ESXi.** This VMware hypervisor enables the abstraction of compute processors, memory, network, and other resources and makes them available to virtual machines and container workloads.
- **vCenter.** VMware vCenter creates a central management experience for interacting with compute resources, networking, and storage as part of your virtual infrastructure.

Customers realize the full potential of their vSphere environment by using NetApp ONTAP with deep product integration, robust support, and powerful features and storage efficiencies to create a robust hybrid multi-cloud.

For more information about VMware vSphere, follow [this link](#).

For more information about NetApp solutions with VMware, follow [this link](#).

## VMware NSX

Commonly referred to as a network hypervisor, VMware NSX employs a software-defined model to connect virtualized workloads. VMware NSX is ubiquitous on premises and in VMware Cloud on AWS where it powers network virtualization and security for customer applications and workloads.

For more information on VMware NSX, follow [this link](#).

## NetApp

### NetApp ONTAP

NetApp ONTAP software has been a leading storage solution for VMware vSphere environments for almost two decades and continues to add innovative capabilities to simplify management while reducing costs. Using ONTAP together with vSphere is a great combination that lets you reduce host hardware and VMware software expenses. You can also protect your data at lower cost with consistent high performance while taking advantage of native storage efficiencies.

For more information on NetApp ONTAP, follow [this link](#).

### NetApp ONTAP tools for VMware

ONTAP tools for VMware combine multiple plugins into a single virtual appliance that provides end-to-end lifecycle management for virtual machines in VMware environments that use NetApp storage systems. ONTAP tools for VMware includes the following:

- **Virtual Storage Console (VSC).** Performs comprehensive administrative tasks for VMs and datastores using NetApp storage.
- **VASA Provider for ONTAP.** Enables Storage Policy- Based Management (SPBM) with VMware virtual volumes (vVols) and NetApp storage.
- **Storage Replication Adapter (SRA).** Recovers vCenter datastores and virtual machines in the event of a failure when coupled with VMware Site Recovery Manager (SRM).

ONTAP tools for VMware allows users to manage not only external storage but also integrate with vVols as well as VMware Site Recovery Manager. This makes it much easier to deploy and operate NetApp storage from within your vCenter environment.

For more information on NetApp ONTAP tools for VMware, follow [this link](#).

## NetApp SnapCenter

NetApp SnapCenter software is an easy-to-use enterprise platform to securely coordinate and manage data protection across applications, databases, and file systems. SnapCenter simplifies backup, restore, and clone lifecycle management by offloading these tasks to application owners without sacrificing the ability to oversee and regulate activity on the storage systems. By leveraging storage-based data management, SnapCenter increases performance and availability as well as reducing testing and development times.

The SnapCenter Plug-in for VMware vSphere supports crash-consistent and VM-consistent backup and restore operations for virtual machines (VMs), datastores, and virtual machine disks (VMDKs). It also supports SnapCenter application-specific plug-ins to protect application-consistent backup and restore operations for virtualized databases and file systems.

For more information on NetApp SnapCenter, follow [this link](#).

## Third-party data protection

### Veeam Backup & Replication

Veeam Backup & Replication is a backup, recovery, and data management solution for cloud, virtual, and physical workloads. Veeam Backup & Replication has specialized integrations with NetApp Snapshot technology that further protect vSphere environments.

For more information on Veeam Backup & Replication, follow [this link](#).

### Public cloud

#### AWS identity and access management

AWS environments contain a wide variety of products including compute, storage, database, network, analytics, and much more to help solve business challenges. Enterprises must be able to define who is authorized to access these products, services, and resources. It is equally important to determine under which conditions users are allowed to manipulate, change, or add configurations.

AWS Identity and Access Management (IAM) provides a secure control plane for managing access to AWS services and products. Properly configured users, access keys, and permissions allow for the deployment of VMware Cloud on AWS and Amazon FSx.

For more information on AIM, follow [this link](#).

#### 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 the 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.

For more information on VMware Cloud on AWS, follow [this link](#).

#### Amazon FSx for NetApp ONTAP

Amazon FSx for NetApp ONTAP is a fully featured and fully managed ONTAP system available as a native AWS service. Built on NetApp ONTAP, it offers familiar features while offering the simplicity of a fully managed cloud service.

Amazon FSx for ONTAP offers multiprotocol support to a variety of compute types including VMware in the public cloud or on premises. Available for guest-connected use cases today and NFS datastores in tech preview, Amazon FSx for ONTAP allows enterprises to take advantage of familiar features from their on-premises environments and in the cloud.

For more information on Amazon FSx for NetApp ONTAP, follow [this link](#).

[Next: Overview - AWS guest-connected storage disaster recovery](#).

#### AWS guest-connected storage disaster recovery

## Overview - AWS guest-connected storage disaster recovery

### [Previous: Technology.](#)

This section provides instructions to help users verify, configure, and validate their on-premises and cloud environments for use with NetApp and VMware. Specifically, this solution is focused on the VMware guest-connected use case with ONTAP AFF on-premises and VMware Cloud and AWS FSx ONTAP for the cloud. This solution is demonstrated with two applications: Oracle and MS SQL in a disaster recovery scenario.

### [Next: Requirements.](#)

## Requirements

### [Previous: Overview - AWS guest-connected storage disaster recovery.](#)

This section details the requirements to access and configure on-premises resources, VMware Cloud, and Amazon FSx ONTAP.

## Skills and knowledge

The following skills and information are required to access Cloud Volumes Service for AWS:

- Access to and knowledge of your VMware and ONTAP on-premises environment.
- Access to and knowledge of VMware Cloud and AWS.
- Access to and knowledge of AWS and Amazon FSx ONTAP.
- Knowledge of your SDDC and AWS resources.
- Knowledge of the network connectivity between your on-premises and cloud resources.
- Working knowledge of disaster recovery scenarios.
- Working knowledge of applications deployed on VMware.

## Administrative

Whether interacting with resources on-premises or in the cloud, users and administrators must have the ability and entitlements to provision those resources where they need them when they need according to their entitlements. The interaction of your roles and permissions for your on-premises systems, including ONTAP and VMware, and your cloud resources, including VMware Cloud and AWS, is paramount for a successful hybrid cloud deployment.

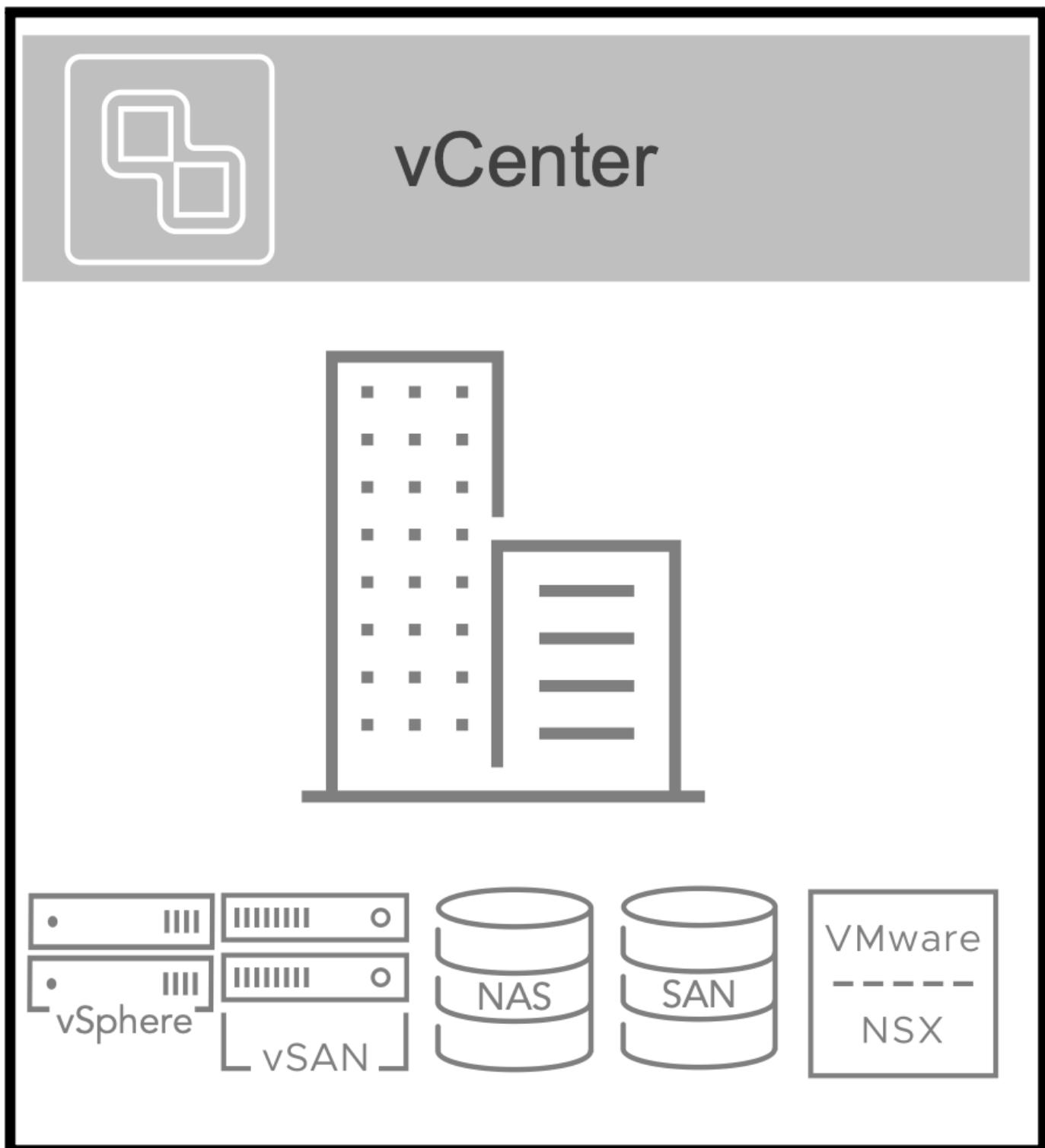
The following administrative tasks must be in place to construct a DR solution with VMware and ONTAP on-premises and VMware Cloud on AWS and FSx ONTAP.

- Roles and accounts enabling provisioning of the following:
  - ONTAP storage resources
  - VMware VMs, datastores, and so on
  - AWS VPC and security groups
- Provisioning of on-premises VMware environment and ONTAP
- VMware Cloud environment
- An Amazon for FSx for ONTAP file system
- Connectivity between your on-premises environment and AWS

- Connectivity for your AWS VPC

## On-premises

The VMware virtual environment includes licensing of ESXi hosts, VMware vCenter Server, NSX networking, and other components, as can be seen in the following figure. All are licensed differently, and it is important to understand how the underlying components consume the available licensed capacity.



## ESXi hosts

Compute hosts in a VMware environment are deployed with ESXi. When licensed with vSphere at various capacity tiers, virtual machines can take advantage of the physical CPUs on each host and applicable entitled features.

## VMware vCenter

Managing ESXi hosts and storage is one of the many capabilities made available to the VMware administrator with vCenter Server. As of VMware vCenter 7.0, there are three editions of VMware vCenter available, depending on the license:

- vCenter Server Essentials
- vCenter Server Foundation
- vCenter Server Standard

## VMware NSX

VMware NSX provides administrators with the flexibility required to enable advanced features. Features are enabled depending upon the version of NSX-T Edition that is licensed:

- Professional
- Advanced
- Enterprise Plus
- Remote Office/Branch Office

## NetApp ONTAP

Licensing with NetApp ONTAP refers to how administrators gain access to various capabilities and features within NetApp storage. A license is a record of one or more software entitlements. Installing license keys, also known as license codes, enables you to use certain features or services on your storage system. For instance, ONTAP supports all major industry-standard client protocols (NFS, SMB, FC, FCoE, iSCSI, and NVMe/FC) through licensing.

Data ONTAP feature licenses are issued as packages, each of which contains multiple features or a single feature. A package requires a license key, and installing the key enables you to access all features in the package.

License types are as follows:

- **Node-locked license.** Installing a node-locked license entitles a node to the licensed functionality. For the cluster to use the licensed functionality, at least one node must be licensed for the functionality.
- **Master/site license.** A master or site license is not tied to a specific system serial number. When you install a site license, all the nodes in the cluster are entitled to the licensed functionality.
- **Demo/temporary license.** A demo or temporary license expires after a certain time. This license enables you to try certain software functionality without purchasing an entitlement.
- **Capacity license (ONTAP Select and FabricPool only).** An ONTAP Select instance is licensed according to the amount of data that the user wants to manage. Starting with ONTAP 9.4, FabricPool requires a capacity license to be used with a third-party storage tier (for example, AWS).

## NetApp SnapCenter

SnapCenter requires several licenses to enable data protection operations. The type of SnapCenter licenses you install depends on your storage environment and the features that you want to use. The SnapCenter Standard license protects applications, databases, file systems, and virtual machines. Before you add a storage system to SnapCenter, you must install one or more SnapCenter licenses.

To enable the protection of applications, databases, file systems, and virtual machines, you must have either a Standard controller-based license installed on your FAS or AFF storage system or a Standard capacity-based license installed on your ONTAP Select and Cloud Volumes ONTAP platforms.

See the following SnapCenter Backup prerequisites for this solution:

- 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. 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.

## MS SQL

As part of this solution validation, we use MS SQL to demonstrate disaster recovery.

For more information regarding best practices with MS SQL and NetApp ONTAP, follow [this link](#).

## Oracle

As part of this solution validation, we use ORACLE to demonstrate disaster recovery. For more information regarding best practices with ORACLE and NetApp ONTAP, follow [this link](#).

## Veeam

As part of this solution validation, we use Veeam to demonstrate disaster recovery. For more information regarding best practices with Veeam and NetApp ONTAP, follow [this link](#).

## Cloud

### AWS

You must be able to perform the following tasks:

- Deploy and configure domain services.
- Deploy FSx ONTAP per application requirements in a given VPC.
- Configure VMware Cloud on the AWS Compute gateway to allow for traffic from FSx ONTAP.
- Configure an AWS security group to allow communication between the VMware Cloud on AWS subnets to the AWS VPC subnets where FSx ONTAP service is deployed.

### VMware Cloud

You must be able to perform the following tasks:

- Configure the VMware Cloud on AWS SDDC.

## Cloud Manager account verification

You must be able to deploy resources with NetApp Cloud Manager. To verify that you can, complete the following tasks:

- [Sign up for Cloud Central](#) if you haven't already.
- [Log into Cloud Manager](#).
- [Set up Workspaces and Users](#).
- [Create a connector](#).

## Amazon FSx for NetApp ONTAP

You must be able to perform the following task after you have an AWS account:

- Create an IAM administrative user capable of provisioning Amazon FSx for the NetApp ONTAP file system.

## Configuration prerequisites

Given the varying topologies that customers have, this section focuses on the ports necessary to enable communication from on-premises to cloud resources.

### Required ports and firewall considerations

The following tables describe the ports that must be enabled throughout your infrastructure.

For a more comprehensive list of required ports for Veeam Backup & Replication software, follow [this link](#).

For a more comprehensive list of port requirements for SnapCenter, follow [this link](#).

The following table lists the Veeam port requirements for Microsoft Windows Server.

From	To	Protocol	Port	Notes
Backup server	Microsoft Windows server	TCP	445	Port required for deploying Veeam Backup & Replication components.
Backup proxy		TCP	6160	Default port used by the Veeam Installer Service.
Backup repository		TCP	2500 to 3500	Default range of ports used as data transmission channels and for collecting log files.
Mount server		TCP	6162	Default port used by the Veeam Data Mover.



For every TCP connection that a job uses, one port from this range is assigned.

The following table lists the Veeam port requirements for Linux Server.

From	To	Protocol	Port	Notes
Backup server	Linux server	TCP	22	Port used as a control channel from the console to the target Linux host.
		TCP	6162	Default port used by the Veeam Data Mover.
		TCP	2500 to 3500	Default range of ports used as data transmission channels and for collecting log files.



For every TCP connection that a job uses, one port from this range is assigned.

The following table lists the Veeam Backup Server port requirements.

From	To	Protocol	Port	Notes
Backup server	vCenter Server	HTTPS, TCP	443	Default port used for connections to vCenter Server. Port used as a control channel from the console to the target Linux host.
	Microsoft SQL Server hosting the Veeam Backup & Replication configuration database	TCP	1443	Port used for communication with Microsoft SQL Server on which the Veeam Backup & Replication configuration database is deployed (if you use a Microsoft SQL Server default instance).
	DNS Server with name resolution of all backup servers	TCP	3389	Port used for communication with the DNS Server



If you use vCloud Director, make sure to open port 443 on underlying vCenter Servers.

The following table lists Veeam Backup Proxy port requirements.

From	To	Protocol	Port	Notes
Backup server	Backup proxy	TCP	6210	Default port used by the Veeam Backup VSS Integration Service for taking a VSS snapshot during the SMB file share backup.
Backup proxy	vCenter Server	TCP	1443	Default VMware web service port that can be customized in vCenter settings.

The following table lists SnapCenter port requirements.

Port Type	Protocol	Port	Notes
SnapCenter management port	HTTPS	8146	This port is used for communication between the SnapCenter client (the SnapCenter user) and the SnapCenter Server. Also used for communication from the plug-in hosts to the SnapCenter Server.
SnapCenter SMCore communication port	HTTPS	8043	This port is used for communication between the SnapCenter Server and the hosts where the SnapCenter plug-ins are installed.
Windows plug-in hosts, installation	TCP	135, 445	These ports are used for communication between the SnapCenter Server and the host where the plug-in is being installed. The ports can be closed after installation. In addition, Windows Instrumentation Services searches ports 49152 through 65535, which must be open.

Port Type	Protocol	Port	Notes
Linux plug-in hosts, installation	SSH	22	These ports are used for communication between the SnapCenter Server and the host where the plug-in is being installed. The ports are used by SnapCenter to copy plug-in package binaries to Linux plug-in hosts.
SnapCenter Plug-ins Package for Windows / Linux	HTTPS	8145	This port is used for communication between SMCore and hosts where the SnapCenter plug-ins are installed.
VMware vSphere vCenter Server port	HTTPS	443	This port is used for communication between the SnapCenter Plug-in for Vmware vSphere and vCenter server.
SnapCenter Plug-in for Vmware vSphere port	HTTPS	8144	This port is used for communication from the vCenter vSphere web client and from the SnapCenter Server.

[Next: Networking.](#)

## Networking

[Previous: Requirements.](#)

This solution requires successful communication from the on-premises ONTAP cluster to AWS FSx for NetApp ONTAP interconnect cluster network addresses to perform NetApp SyncMirror operations. Also, a Veeam backup server must have access to an AWS S3 bucket. Instead of using Internet transport, an existing VPN or Direct Connect link can be used as a private link to an S3 bucket.

### On premises

ONTAP supports all major storage protocols used for virtualization, including iSCSI, Fibre Channel (FC), Fibre Channel over Ethernet (FCoE), or Non-Volatile Memory Express over Fibre Channel (NVMe/FC) for SAN environments. ONTAP also supports NFS (v3 and v4.1) and SMB or S3 for guest connections. You are free to pick what works best for your environment, and you can combine protocols as needed on a single system. For example, you can augment general use of NFS datastores with a few iSCSI LUNs or guest shares.

This solution leverages NFS datastores for on-premises datastores for guest VMDKs and both iSCSI and NFS for guest application data.

### Client networks

VMkernel network ports and software-defined networking provide connectivity to ESXi hosts allowing them to communicate with elements outside the VMware environment. Connectivity depends on the type of VMkernel

interfaces used.

For this solution, the following VMkernel interfaces were configured:

- Management
- vMotion
- NFS
- iSCSI

### Storage networks provisioned

A LIF (logical interface) represents a network access point to a node in the cluster. This allows communication with the storage virtual machines that house the data accessed by clients. You can configure LIFs on ports over which the cluster sends and receives communications over the network.

For this solution, LIFs are configured for the following storage protocols:

- NFS
- iSCSI

### Cloud connectivity options

Customers have a lot of options when connecting their on-premises environment to cloud resources, including deploying VPN or Direct Connect topologies.

#### Virtual Private Network (VPN)

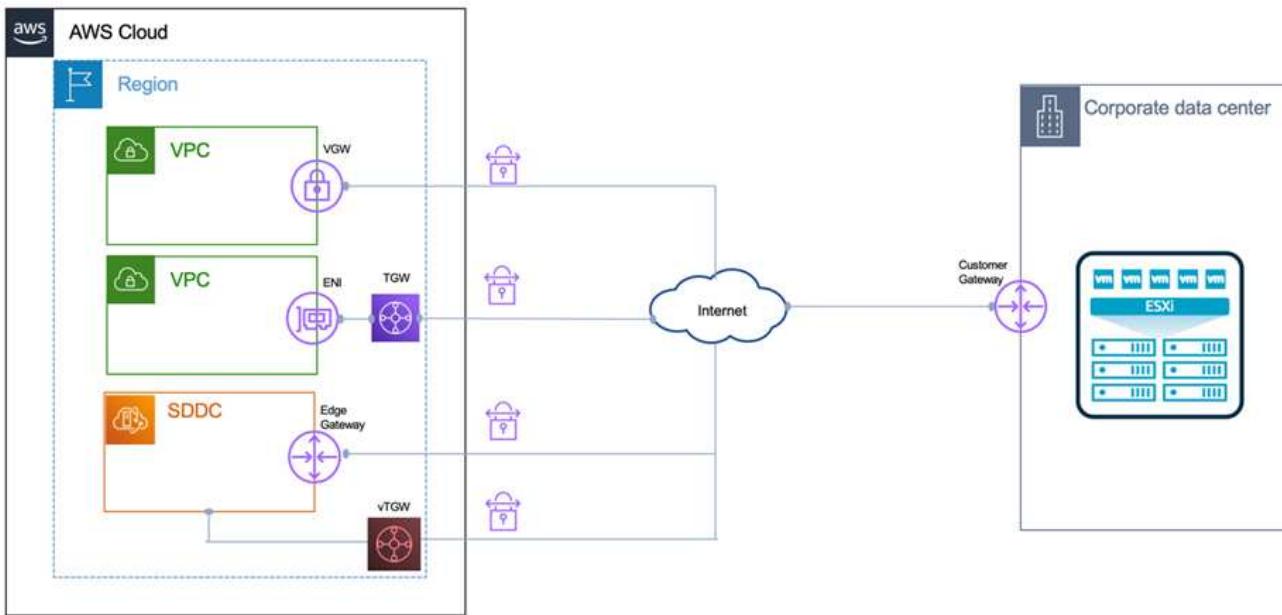
VPNs (Virtual Private Networks) are often used to create a secure IPSec tunnel with internet-based or private MPLS networks. A VPN is easy to set up, but it lacks reliability (if internet-based) and speed. The end point can be terminated at the AWS VPC or at the VMware Cloud SDDC. For this disaster recovery solution, we created connectivity to AWS FSx for NetApp ONTAP from the on-premises network. So, it can be terminated at the AWS VPC (Virtual Private Gateway or Transit Gateway) where FSx for NetApp ONTAP is connected.

VPN setup can be route-based or policy-based. With a route-based setup, the endpoints exchange the routes automatically and setup learns the route to the newly created subnets. With a policy-based setup, you must define the local and remote subnets, and, when new subnets are added and allowed to communicate in the IPSec tunnel, you must update the routes.



If the IPSec VPN tunnel is not created on the default gateway, remote network routes must be defined in route tables via the local VPN tunnel end point.

The following figure depicts typical VPN connection options.

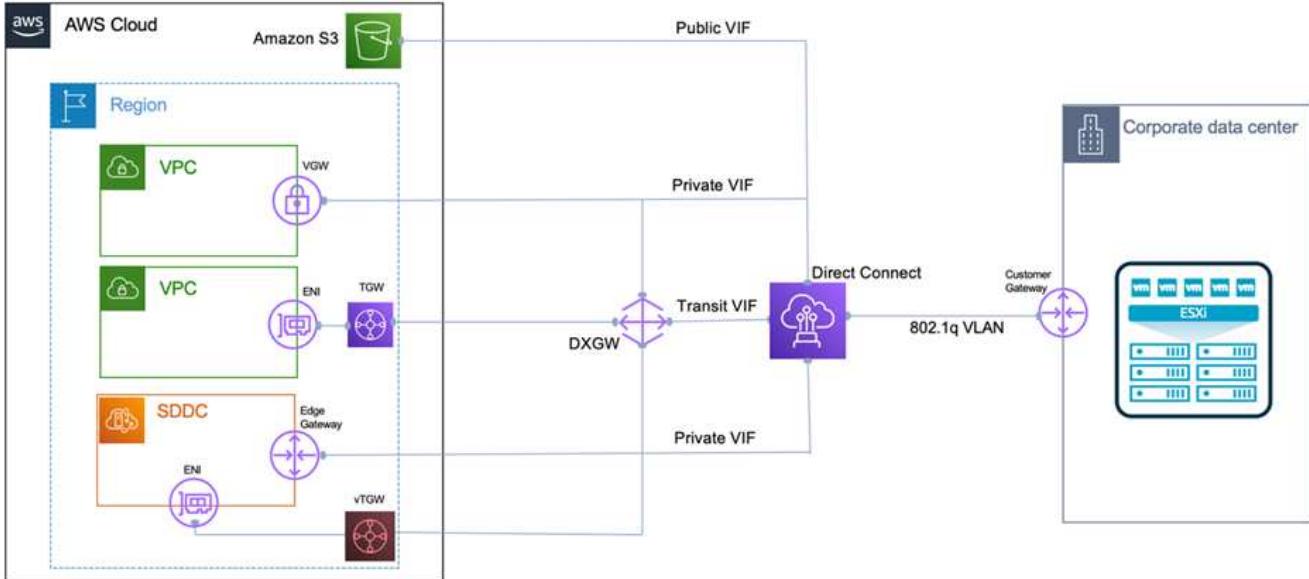


## Direct Connect

Direct Connect provides a dedicated link to the AWS network. Dedicated connections create links to AWS using a 1Gbps, 10Gbps, or 100Gbps Ethernet port. AWS Direct Connect partners provide hosted connections using pre-established network links between themselves and AWS and are available from 50Mbps up to 10Gbps. By default, the traffic is unencrypted. However, options are available to secure traffic with MACsec or IPsec. MACsec provides layer-2 encryption while IPsec provides layer-3 encryption. MACsec provides better security by concealing which devices are communicating.

Customers must have their router equipment in an AWS Direct Connect location. To set this up, you can work with AWS Partner Network (APN). A physical connection is made between that router and the AWS router. To enable access to FSx for NetApp ONTAP on VPC, you must have either a private virtual interface or a transit virtual interface from Direct Connect to a VPC. With a private virtual interface, the Direct Connect to VPC connection scalability is limited.

The following figure depicts the Direct Connect interface options.



## Transit gateway

The transit gateway is a region-level construct that allows increased scalability of a Direct Connect-to-VPC connection within a region. If a cross- region connection is required, the transit gateways must be peered. For more information, check the [AWS Direct Connect documentation](#).

## Cloud network considerations

In the cloud, the underlying network infrastructure is managed by the cloud service provider, whereas customers must manage the VPC networks, subnets, route tables, and so on in AWS. They must also manage NSX network segments at the compute edge. SDDC groups routes for the external VPC and Transit Connect.

When FSx for NetApp ONTAP with Multi-AZ availability is deployed on a VPC connected to VMware Cloud, iSCSI traffic receives necessary route table updates to enable communication. By default, there is no route available from VMware Cloud to the FSx ONTAP NFS/SMB subnet on the connected VPC for Multi-AZ deployment. To define that route, we used the VMware Cloud SDDC group, which is a VMware- managed transit gateway, to allow communication between the VMware Cloud SDDCs in the same region as well as to external VPCs and other transit gateways.



There are data transfer costs associated with using a transit gateway. For cost details specific to a region, see [this link](#).

VMware Cloud SDDC can be deployed in a single availability zone, which is like having a single datacenter. A stretch cluster option is also available, which is like a NetApp MetroCluster solution that can provide higher availability and reduced downtime in case of availability-zone failure.

To minimize data-transfer cost, keep the VMware Cloud SDDC and AWS Instances or services in the same availability zone. It is better to match with an availability zone ID rather than with a name because AWS provides the AZ order list specific to the account to spread the load across availability zones. For example, one account (US-East-1a) might point to AZ ID 1 whereas another account (US-East-1c) might point to AZ ID 1. The availability zone ID can be retrieved in several ways. In the following example, we retrieved the AZ ID from the VPC subnet.

## subnet-04f5fe7073ff514fb / priv-subnet-01

Details			
Subnet ID	Subnet ARN	State	IPv4 CIDR
<input type="text"/>	<input type="text"/>	<span>Available</span>	<input type="text"/> 172.30.15.0/25
Available IPv4 addresses	IPv6 CIDR	Availability Zone	Availability Zone ID
<input type="text"/> 97	<input type="text"/> -	<input type="text"/> us-east-1a	<input type="text"/> us-east-1a26
Network border group	VPC	Route table	Network ACL
<input type="text"/> us-east-1	<input type="text"/>	<input type="text"/> rtb-08c08b5db175cded2	<input type="text"/> acl-0b7f41adaade25077
Default subnet	Auto-assign public IPv4 address	Auto-assign IPv6 address	Auto-assign customer-owned IPv4 address
No	<input type="text"/> No	<input type="text"/> No	<input type="text"/> No
Customer-owned IPv4 pool	Outpost ID	IPv4 CIDR reservations	IPv6 CIDR reservations
<input type="text"/> -	<input type="text"/> -	<input type="text"/> -	<input type="text"/> -
IPv6-only	Hostname type	Resource name DNS A record	Resource name DNS AAAA record
No	<input type="text"/> IP name	<input type="text"/> Disabled	<input type="text"/> Disabled
DNS64	Owner		
Disabled			

In the VMware Cloud SDDC, networking is managed with NSX, and the edge gateway (Tier-0 router) that handles the north-south traffic uplink port is connected to the AWS VPC. The compute gateway and the management gateways (Tier-1 routers) handle east-west traffic. If the uplink ports of the edge becomes heavily used, you can create traffic groups to associate with specific host IPs or subnets. Creation of a traffic group creates additional edge nodes to separate the traffic. Check the [VMware documentation](#) on the minimum number of vSphere hosts required to use a multi-edge setup.

## Client networks

When you provision the VMware Cloud SDDC, VMKernel ports are already configured and are ready for consumption. VMware manages those ports and there is no need to make any updates.

The following figure depicts sample Host VMKernel info.

VMkernel adapters						
	Device	Network Label	Switch	IP Address	TCP/IP Stack	Enabled Services
⋮	vmk0	o-vmk0-1s	vmc-hostswitch	172.30.160.68	Default	Management
⋮	vmk1	VSAN	vmc-hostswitch	172.30.160.4	Default	vSAN
⋮	vmk2	VMOTION	vmc-hostswitch	172.30.160.36	vMotion	vMotion
⋮	vmk3	vmcd-backplane-1s	vmc-hostswitch	169.252.32.4	api	--
⋮	vmk4	vmk4-1s	vmc-hostswitch	172.30.160.196	api	--
⋮	vmk10	--	vmc-hostswitch	172.30.160.100	nsx-overlay	--
⋮	vmk50	--	vmc-hostswitch	169.254.1.1	nsx-hyperbus	--

## Storage networks provisioned (iSCSI, NFS)

For VM guest storage networks, we typically create port groups. With NSX, we create segments that are consumed on vCenter as port groups. Because storage networks are in a routable subnet, you can access the LUNs or mount the NFS exports using the default NIC even without creating separate network segments. To separate storage traffic, you can create additional segments, define rules, and control the MTU size on those segments. To provide fault tolerance, it is better to have at least two segments dedicated for the storage network. As we mentioned previously, if uplink bandwidth becomes an issue, you can create traffic groups and assign IP prefixes and gateways to perform source-based routing.

We recommend matching the segments in the DR SDDC with the source environment to prevent guessing of

mapping network segments during failover.

## Security groups

Many security options provide secure communication on the AWS VPC and the VMware Cloud SDDC network. Within the VMware Cloud SDDC network, you can use NSX trace flow to identify the path, including the rules used. Then, you can use a network analyzer on the VPC network to identify the path, including the route tables, security groups, and network access control lists, that is consumed during the flow.

[Next: Storage.](#)

## Storage

[Previous: Networking.](#)

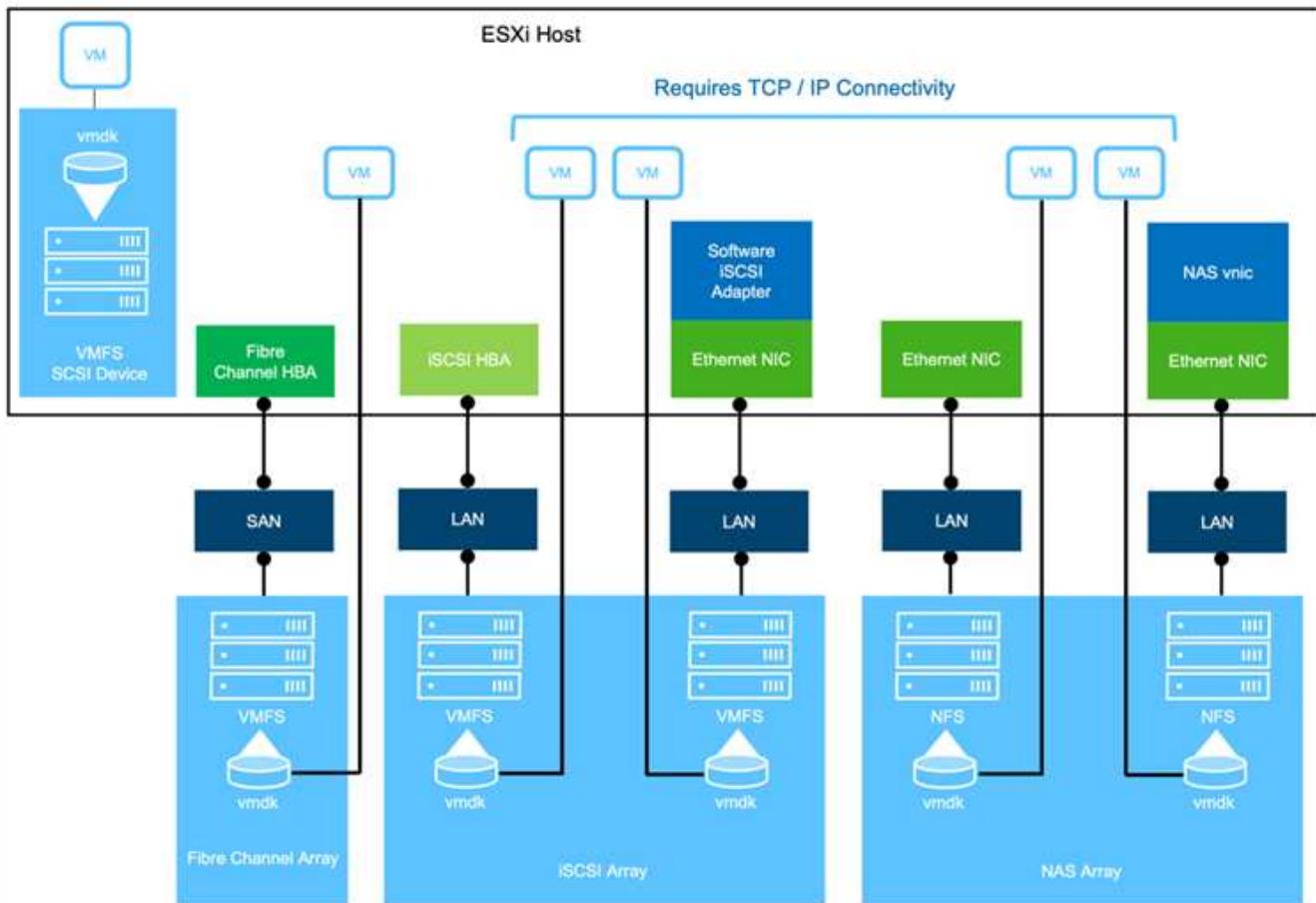
NetApp AFF A-Series systems deliver a high-performance storage infrastructure with flexible data management options that are cloud enabled to meet a wide variety of enterprise scenarios. In this solution, we used an ONTAP AFF A300 as our primary on-premises storage system.

NetApp ONTAP together with ONTAP Tools for VMware and SnapCenter were used in the solution to provide comprehensive management and application backup capabilities that are tightly integrated with VMware vSphere.

### On-premises

We used ONTAP storage for the VMware datastores that hosted the virtual machines and their VMDK files. VMware supports multiple storage protocols for connected datastores, and, in this solution, we used NFS volumes for datastores on the ESXi hosts. However, ONTAP storage systems support all protocols supported by VMware.

The following figure depicts VMware storage options.



ONTAP volumes were used for both iSCSI and NFS guest-connected storage for our application VMs. We used the following storage protocols for application data:

- NFS volumes for guest connected Oracle database files.
- iSCSI LUNs for guest connected Microsoft SQL Server databases and transaction logs.

Operating system	Database type	Storage protocol	Volume description
Windows Server 2019	SQL Server 2019	iSCSI	Database files
		iSCSI	Log files
Oracle Linux 8.5	Oracle 19c	NFS	Oracle binary
		NFS	Oracle data
		NFS	Oracle recovery files

We also used ONTAP storage for the primary Veeam backup repository as well as for a backup target for the SnapCenter database backups.

- SMB share for the Veeam backup repository.
- SMB share as a target for the SnapCenter database backups.

## Cloud storage

This solution includes VMware Cloud on AWS for hosting virtual machines that are restored as a part of the failover process. As of this writing, VMware supports vSAN storage for the datastores that host the VMs and VMDKs.

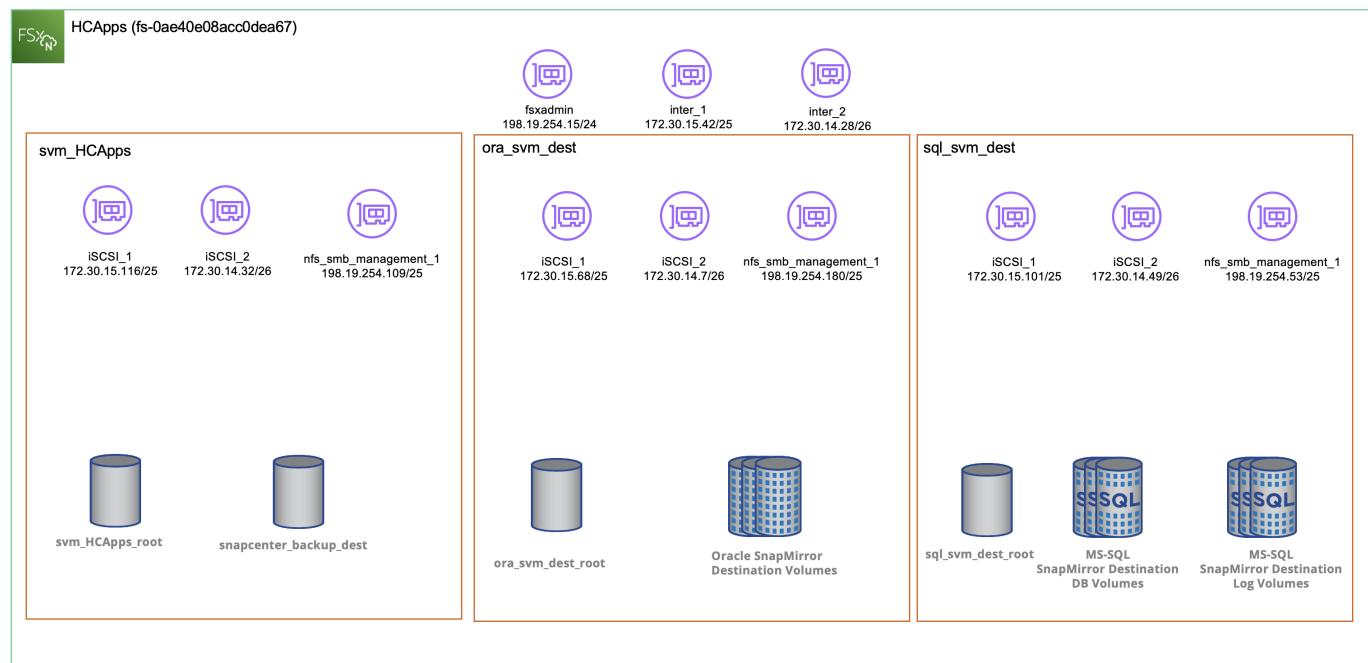
FSx for ONTAP is used as the secondary storage for application data that is mirrored using SnapCenter and SyncMirror. As a part of the failover process, the FSx for ONTAP cluster is converted to primary storage, and the database applications can resume normal function running on the FSx storage cluster.

## Amazon FSx for NetApp ONTAP setup

To deploy AWS FSx for NetApp ONTAP using Cloud Manager, follow the instructions at [this link](#).

After FSx ONTAP is deployed, drag and drop the on-premises ONTAP instances into FSx ONTAP to start replication setup of volumes.

The following figure depicts our FSx ONTAP environment.



## Network interfaces created

FSx for NetApp ONTAP has network interfaces preconfigured and ready to use for iSCSI, NFS, SMB, and inter-cluster networks.

## VM datastore storage

The VMware Cloud SDDC comes with two VSAN datastores named `vsandatastore` and `workloaddatastore`. We used `vsandatastore` to host management VMs with access restricted to `cloudadmin` credential. For workloads, we used `workloaddatastore`.

[Next: Compute.](#)

## Compute

[Previous: Storage.](#)

VMware vSphere provides virtualized infrastructure in the datacenter and across all the major cloud providers. This ecosystem is ideal for disaster recovery scenarios for which virtualized compute stays consistent regardless of location. This solution uses VMware virtualized compute resources at both the datacenter location and in the VMware Cloud on AWS.

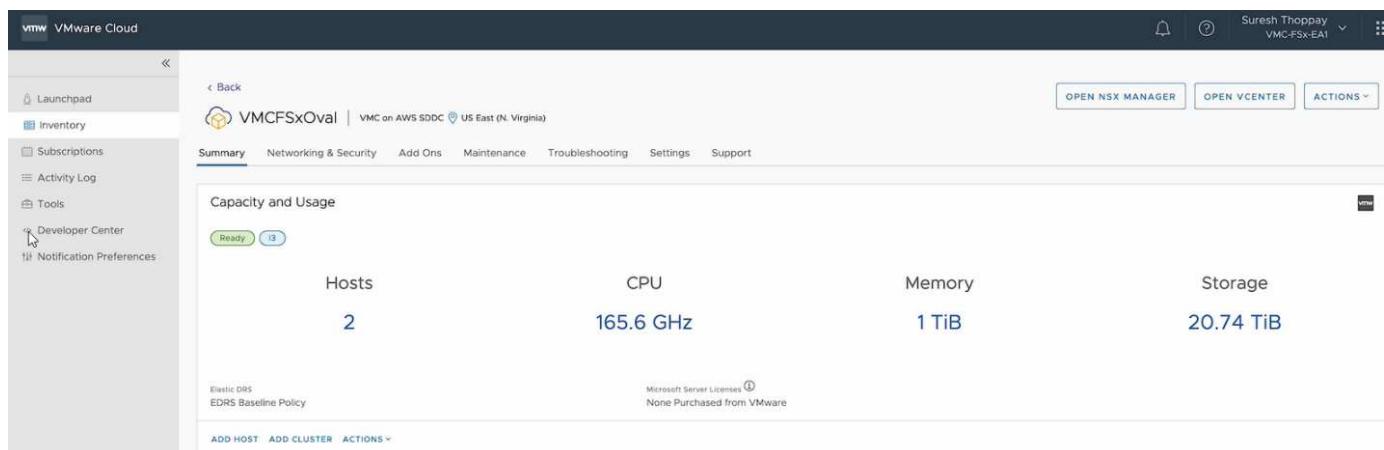
### On-premises

This solution uses HPE Proliant DL360 Gen 10 Servers running VMware vSphere v7.0U3. We deployed six compute instances to provide adequate resources for our SQL server and Oracle servers.

We deployed 10 Windows Server 2019 VMs running SQL Server 2019 with varying database sizes and 10 Oracle Linux 8.5 VMs running Oracle 19c, again, with varying database sizes.

### Cloud

We deployed an SDDC in VMware Cloud on AWS with two hosts to provide adequate resources to run the virtual machines restored from our primary site.



The screenshot shows the VMware Cloud interface. The left sidebar includes options like Launchpad, Inventory, Subscriptions, Activity Log, Tools, Developer Center, and Notification Preferences. The main content area is titled 'VMCFsxOval' and 'VMC on AWS SDDC US East (N. Virginia)'. The 'Summary' tab is selected, showing 'Capacity and Usage' details: 2 hosts, 165.6 GHz CPU, 1 TiB Memory, and 20.74 TiB Storage. It also lists 'Elastic DRS' and 'EDRS Baseline Policy'. Under 'Microsoft Server Licenses', it notes 'None Purchased from VMware'. Action buttons include 'OPEN NSX MANAGER', 'OPEN VCENTER', and 'ACTIONS'.

[Next: Cloud Backup Tools.](#)

## Cloud Backup Tools

[Previous: Compute.](#)

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

### Deployment of backup tools

SnapCenter server and Veeam Backup & Replication server can be installed in the VMware Cloud SDDC or they can be installed on EC2 instances residing in a VPC with network connectivity to the VMware Cloud environment.

## **SnapCenter Server**

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 found at [this link](#).

## **Veeam Backup & Replication server**

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

### **Backup tools and configuration**

After they are installed, SnapCenter and Veeam Backup & Replication must be configured to perform the necessary tasks to restore data to VMware Cloud on AWS.

### **SnapCenter configuration**

To restore application data that has been 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 primary storage.

For a list of steps to be completed on the SnapCenter Server residing in AWS, see the section [Deploy Secondary Windows SnapCenter Server](#).

### **Veeam Backup & Replication configuration**

To restore virtual machines that have been backed up to Amazon S3 storage, the Veeam Server must be installed on a Windows server and configured 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 once they are restored.

For a complete list of steps required to complete failover of the application VMs, see the section [Deploy Secondary Veeam Backup & Replication Server](#).

[Next: Overview - Disaster recovery.](#)

### **Disaster recovery**

#### **Overview - Disaster recovery**

[Previous: Cloud Backup Tools.](#)

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 and retention schedules (secondary storage).
- Deploy and configure Windows SnapCenter server on-premises.
- Deploy and configure Veeam Backup & Replication server on-premises.
- Deploy and configure cloud backup tools, SnapCenter, and Veeam.
- SnapCenter database backup for disaster recovery.
- SnapCenter database restore at a secondary site.
- Restore application virtual machines using Veeam Backup & Replication.
- Restore SQL Server application data.
- Restore Oracle application data.

[Next: Configure SnapMirror relationships and retention schedules.](#)

## Configure SnapMirror relationships and retention schedules

[Previous: Overview - Disaster recovery.](#)

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:

- Record the source and destination intercluster logical interfaces.
- Establish cluster peering between ONTAP and FSx.
- Establish an SVM peering relationship.
- Create a snapshot retention policy.
- Create the destination volume in FSx.
- Create the SnapMirror relationships between source and destination volumes.
- Initialize SnapMirror relationships.

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.

Name	Status	Storage VM	IPSpace	Address	Current Node	Current Port	Portset	Protocols	Type	Thru
veeam_repo	✓	Backup	Default	10.61.181.179	E13A300_1	a0a-181		SMB/CIFS , NFS, S3	Data	0
CM01	✓		Default	10.61.181.180	E13A300_1	a0a-181			Cluster/Node Mgmt	0
HC_N1	✓		Default	10.61.181.183	E13A300_1	a0a-181			Intercluster,Cluster/Node Mgmt	0
HC_N2	✓		Default	10.61.181.184	E13A300_2	a0a-181			Intercluster,Cluster/Node Mgmt	0
lif_ora_svm_614	✓	ora_svm	Default	10.61.181.185	E13A300_1	a0a-181		SMB/CIFS , NFS, FL...	Data	0

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
  Logical      Status      Network          Current      Current  Is
Vserver      Interface  Admin/Oper Address/Mask  Node        Port    Home
-----  -----
FsxId0ae40e08acc0dea67
  inter_1      up/up      172.30.15.42/25  FsxId0ae40e08acc0dea67-01
                                         e0e      true
  inter_2      up/up      172.30.14.28/26  FsxId0ae40e08acc0dea67-02
                                         e0e      true
2 entries were displayed.
```

## Establish cluster peering between ONTAP and FSx

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.

The screenshot shows the ONTAP System Manager interface. The left sidebar has sections for DASHBOARD, STORAGE, NETWORK, EVENTS & JOBS, PROTECTION, and HOSTS. The PROTECTION section is currently selected, with 'Overview' highlighted and a red box and number '1' indicating it. The main content area is titled 'Overview' and shows 'Intercluster Settings' with a back arrow. Below it is a 'Network Interfaces' section listing IP addresses: 10.61.181.184, 172.21.146.217, 10.61.181.183, and 172.21.146.216, each with a green checkmark. To the right of these is a red callout with number '2' pointing to a three-dot menu icon. A red box highlights the 'Peer Cluster' button in a dropdown menu. Below this are 'Generate Passphrase' and 'Manage Cluster Peers' buttons. The 'Cluster Peers' section shows 'PEERED CLUSTER NAME' with values 'FsxId0ae40e08acc0dea67' and 'OTS02', each with a green checkmark. To the right of this is a red callout with number '3' pointing to a three-dot menu icon. A red box highlights the 'Configure' button in a dropdown menu. The 'Mediator' section shows 'Not configured.' with a blue gear icon. The 'Storage VM Peers' section shows 'PEERED STORAGE VMS' with a value '3' and a green checkmark. To the right of this is a three-dot menu icon.

OVERVIEW

Intercluster Settings

Network Interfaces

IP ADDRESS

- ✓ 10.61.181.184
- ✓ 172.21.146.217
- ✓ 10.61.181.183
- ✓ 172.21.146.216

Cluster Peers

PEERED CLUSTER NAME

- ✓ FsxId0ae40e08acc0dea67
- ✓ OTS02

Mediator

Not configured.

Configure

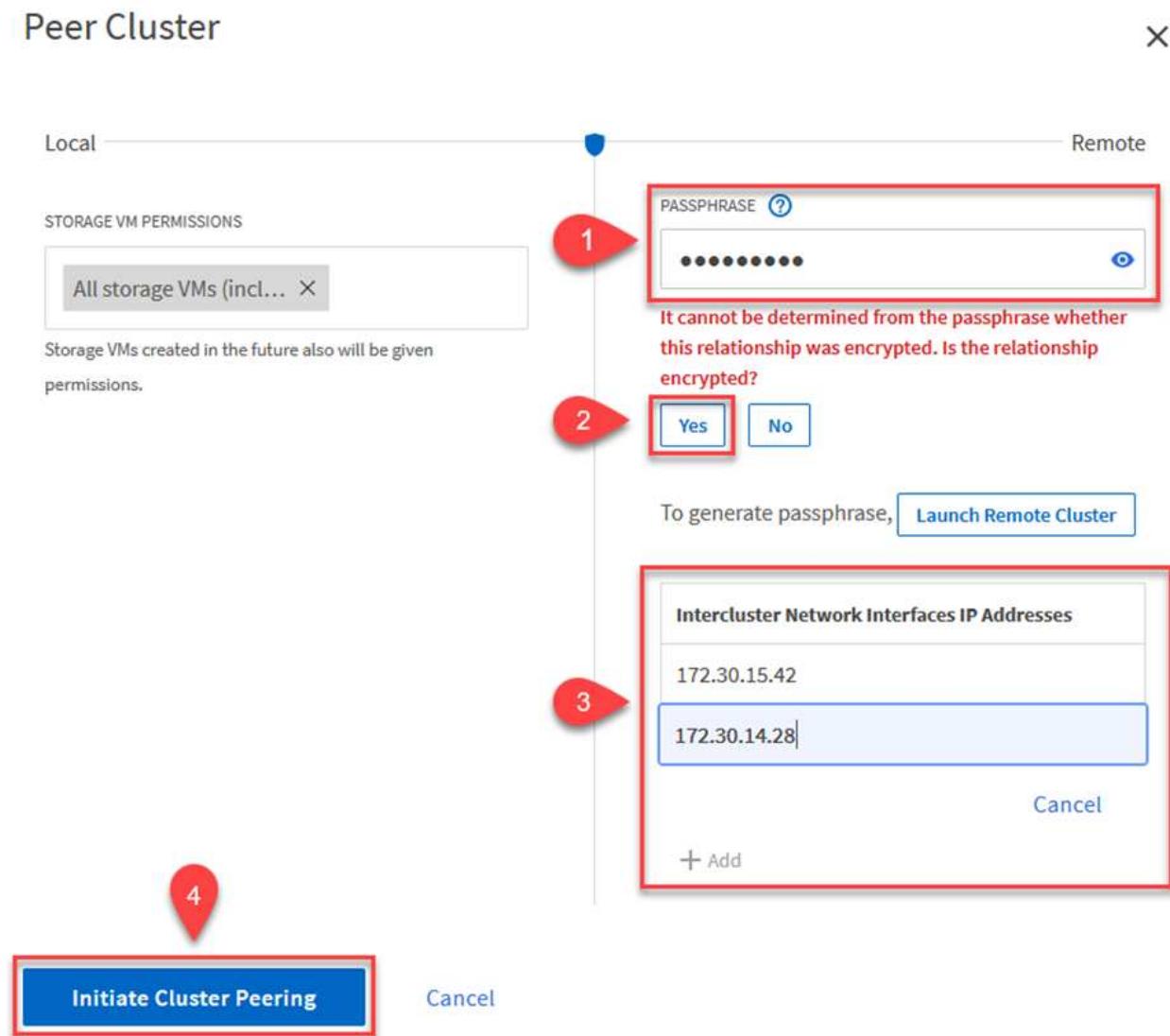
Storage VM Peers

PEERED STORAGE VMS

- ✓ 3

3. In the Peer Cluster dialog box, fill out the required information:
  - Enter the passphrase that was used to establish the peer cluster relationship on the destination FSx cluster.
  - Select Yes to establish an encrypted relationship.
  - Enter the intercluster LIF IP address(es) of the destination FSx cluster.

- d. Click Initiate Cluster Peering to finalize the process.



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

```
FSx-Dest::> cluster peer show
```

```
FSxId0ae40e08acc0dea67::> cluster peer show
Peer Cluster Name          Cluster Serial Number Availability  Authentication
----- 1-80-000011          Available          ok
```

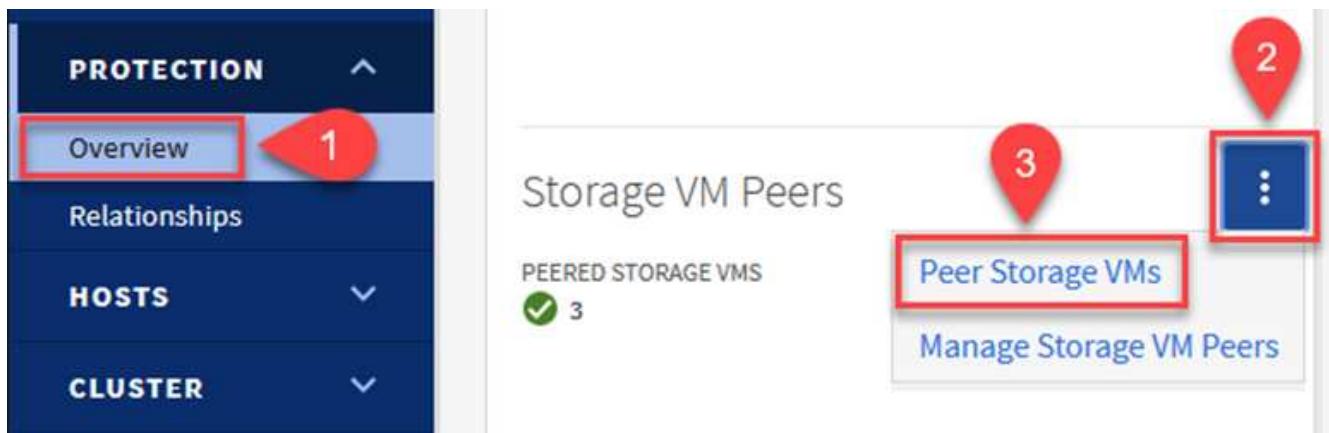
### Establish SVM peering relationship

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:

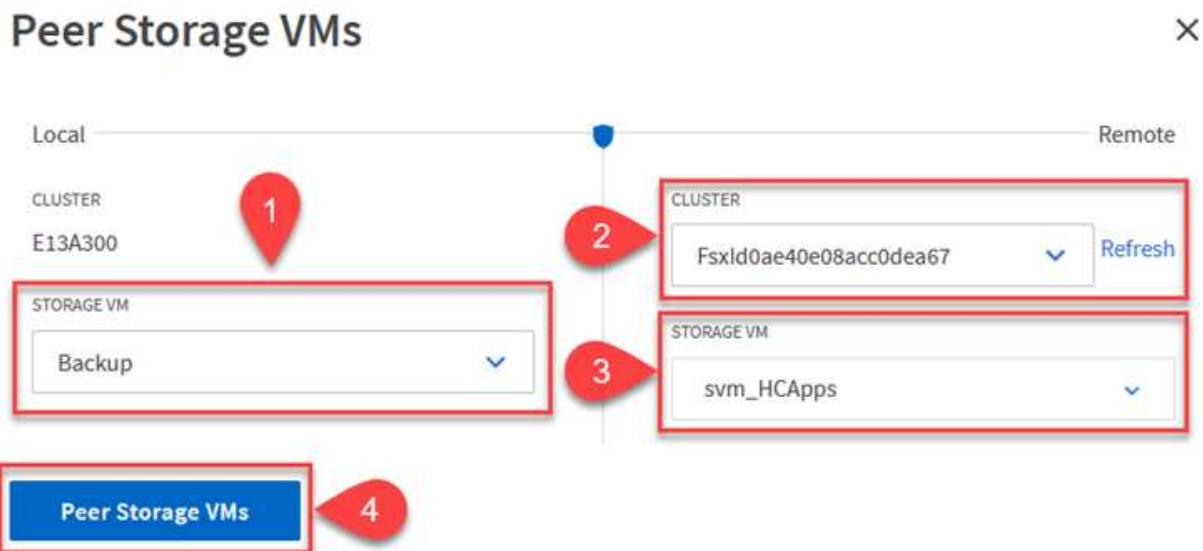
```
FSx-Dest::> vserver peer create -vserver DestSVM -peer-vserver Backup  
-peer-cluster OnPremSourceSVM -applications snapmirror
```

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.

## Create a snapshot retention policy

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 

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-on-demand -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.

To create a volume, run the following command on FSx ONTAP:

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

[Next: Deploy and configure Windows SnapCenter Server on premises.](#)

## Deploy and configure Windows SnapCenter Server on premises

[Previous: Configure SnapMirror relationships and retention schedules.](#)

## 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](https://Virtual_Cluster_IP_or_FQDN:8146).

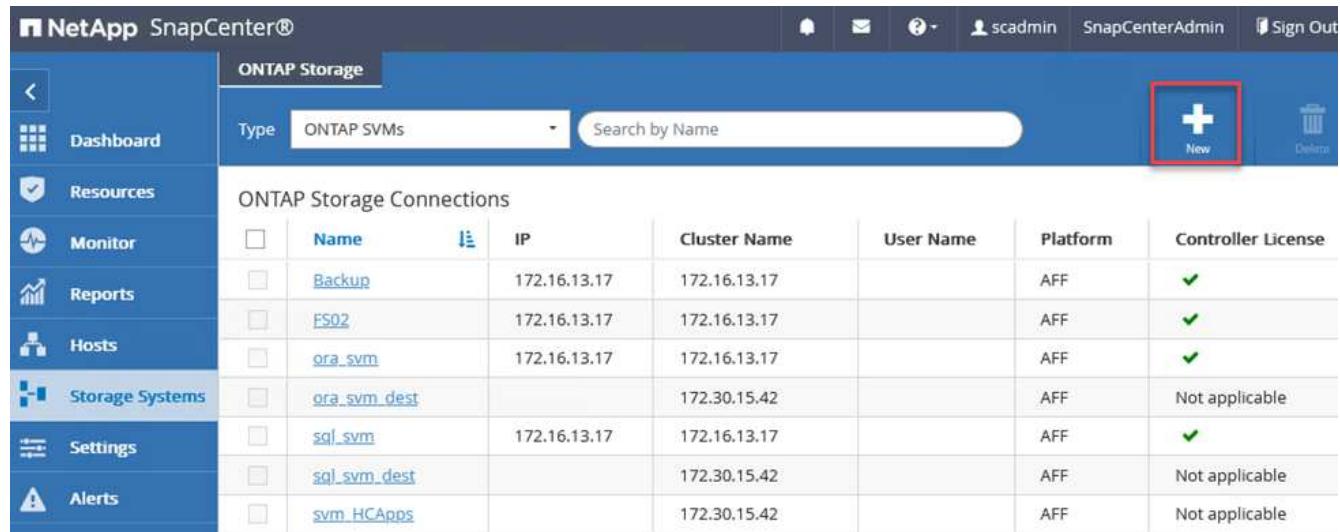
After you log into the console, you must configure SnapCenter for backup SQL Server and Oracle databases. To do so, complete the following high-level steps:

1. Add storage controllers that contain volumes hosting application data.
2. Add host systems to be backed up with SnapCenter.
3. Configure policies that specify backup parameters and schedules.
4. Configure resource groups that contain resources to be backed up and policies used for the backups.

## Add storage controllers to SnapCenter

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.



	Name	IP	Cluster Name	User Name	Platform	Controller License
<a href="#">Backup</a>	172.16.13.17	172.16.13.17			AFF	✓
<a href="#">ES02</a>	172.16.13.17	172.16.13.17			AFF	✓
<a href="#">ora_svm</a>	172.16.13.17	172.16.13.17			AFF	✓
<a href="#">ora_svm_dest</a>		172.30.15.42			AFF	Not applicable
<a href="#">sql_svm</a>	172.16.13.17	172.16.13.17			AFF	✓
<a href="#">sql_svm_dest</a>		172.30.15.42			AFF	Not applicable
<a href="#">svm_HCAppl</a>		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 i

Storage System

Username

Password

#### Event Management System (EMS) & AutoSupport Settings

Send AutoSupport notification to storage system

Log SnapCenter Server events to syslog

 **More Options :** Platform, Protocol, Preferred IP etc..

**Submit**

**Cancel**

**Reset**

3. Repeat this process to add the FSx ONTAP system to SnapCenter. In this case, select More Options at the bottom of the Add Storage System window and click the check box for Secondary to designate the FSx system as the secondary storage system updated with SnapMirror copies or our primary backup snapshots.

## More Options

Platform: FAS

Protocol: HTTPS

Port: 443

Timeout: 60 seconds

Secondary

Preferred IP

**Save** **Cancel**

For more information related to adding storage systems to SnapCenter, see the documentation at [this link](#).

### 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.

Managed Hosts

Search by Name

Name

oraclesrv\_01.sddc.netapp.com

oraclesrv\_02.sddc.netapp.com

oraclesrv\_03.sddc.netapp.com

oraclesrv\_04.sddc.netapp.com

oraclesrv\_05.sddc.netapp.com

oraclesrv\_06.sddc.netapp.com

oraclesrv\_07.sddc.netapp.com

oraclesrv\_08.sddc.netapp.com

oraclesrv\_09.sddc.netapp.com

oraclesrv\_10.sddc.netapp.com

Add Host

Host Type: Windows

Host Name: sqlsrv-01.sddc.netapp.com

Credentials: sddc-jpowell

Select Plug-ins to Install SnapCenter Plug-ins Package 4.6 for Windows

Microsoft Windows

Microsoft SQL Server

Microsoft Exchange Server

SAP HANA

[More Options](#) : Port, gMSA, Install Path, Custom Plug-Ins...

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.

### Add Host

Host Type: Linux

Host Name: oraclesrv\_11.sddc.netapp.com

Credentials: root

[More Options](#) [?](#)

### Select Plug-ins to Install SnapCenter Plug-ins Package 4.6 for Linux

- Oracle Database
- SAP HANA

[More Options](#) : Port, Install Path, Custom Plug-Ins...

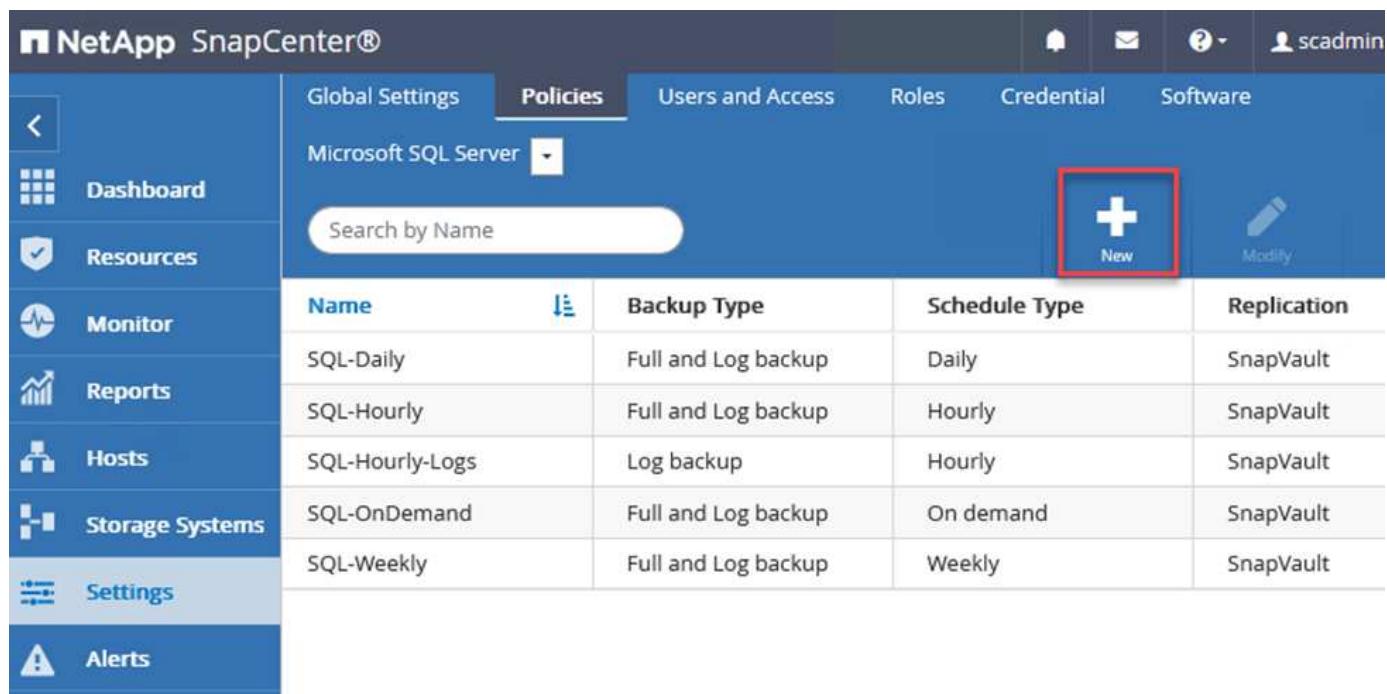
Submit

Cancel

### Create SnapCenter policies

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.



The screenshot shows the NetApp SnapCenter web interface. The top navigation bar includes 'Global Settings', 'Policies' (which is the active tab), 'Users and Access', 'Roles', 'Credential', and 'Software'. The user 'scadmin' is logged in. On the left, a sidebar lists 'Dashboard', 'Resources', 'Monitor', 'Reports', 'Hosts', 'Storage Systems', 'Settings' (which is the active section), and 'Alerts'. The main content area is titled 'Microsoft SQL Server'. It features a search bar labeled 'Search by Name' and a table with columns: 'Name', 'Backup Type', 'Schedule Type', and 'Replication'. The table contains five rows with the following data:

Name	Backup Type	Schedule Type	Replication
SQL-Daily	Full and Log backup	Daily	SnapVault
SQL-Hourly	Full and Log backup	Hourly	SnapVault
SQL-Hourly-Logs	Log backup	Hourly	SnapVault
SQL-OnDemand	Full and Log backup	On demand	SnapVault
SQL-Weekly	Full and Log backup	Weekly	SnapVault

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 Server Backup Policy

1 Name      2 Backup Type      3 Retention      4 Replication      5 Script

Select secondary replication options [i](#)

Update SnapMirror after creating a local Snapshot copy.

Update SnapVault after creating a local Snapshot copy.

Secondary policy label [Choose](#) [i](#)

Error retry count [3](#) [i](#)

### 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.

Name	Resource Count	Tags	Policies	Last Backup	Overall Status
SQLSRV-01	1		SQL-Daily SQL-Hourly SQL- OnDemand SQL-Weekly	05/11/2022 ...	Completed
SQLSRV-02	1		SQL-Daily SQL-Hourly SQL- OnDemand SQL-Weekly	03/28/2022 ...	Failed
SQLSRV-03	1		SQL-Daily SQL-Hourly	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](#).

Next: Deploy and configure Veeam Backup Server.

## Deploy and configure Veeam Backup Server

Previous: Deploy and configure Windows SnapCenter Server on premises.

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](#).

### Configure Veeam scale-out backup repository

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.

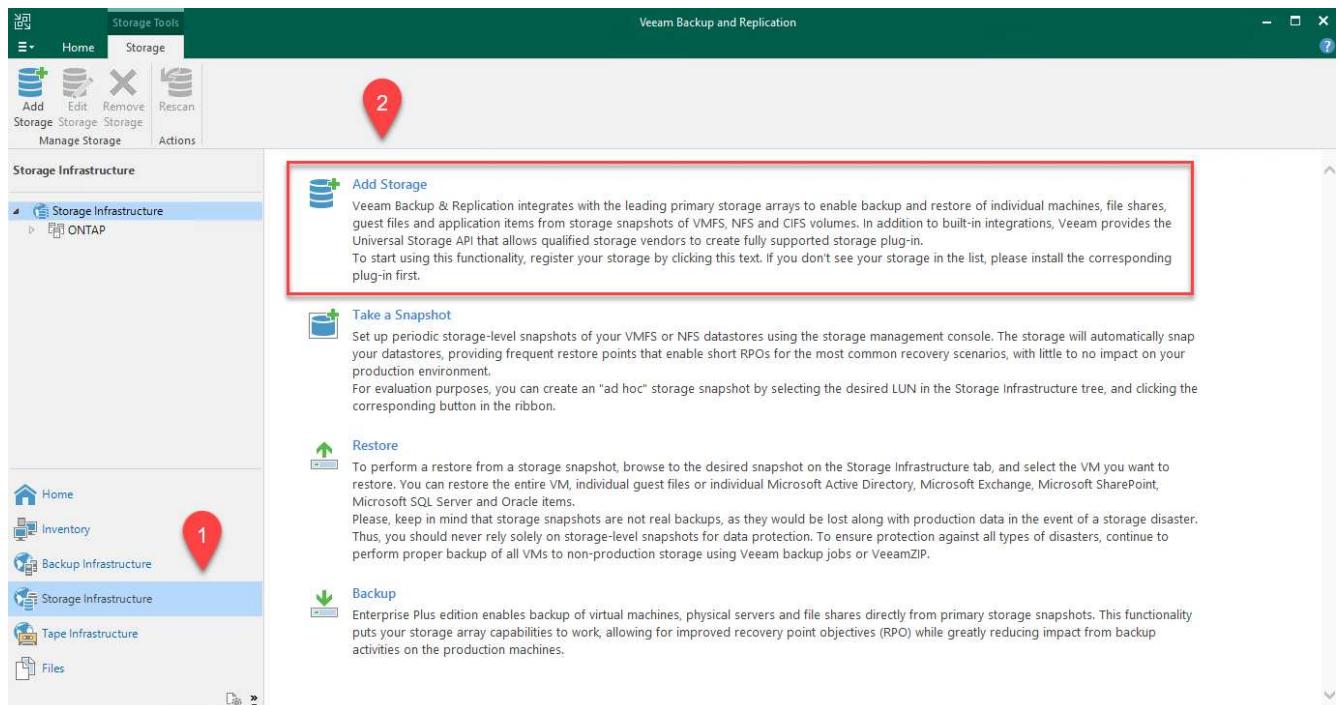
See the following prerequisites before getting started.

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.

### Add ONTAP Storage to Veeam

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**  
Register NetApp Data ONTAP storage by specifying DNS name or IP address.

Name	Management server DNS name or IP address: 10.61.181.180
Credentials	
NAS Filer	Description: Created by SDDC\jpowell at 5/17/2022 10:34 AM.
Apply	
Summary	<b>Role:</b> <input type="checkbox"/> Block or file storage for VMware vSphere <input type="checkbox"/> Block storage for Microsoft Windows servers <input checked="" type="checkbox"/> <b>NAS filer</b>

[< Previous](#) [Next >](#) [Finish](#) [Cancel](#)

4. Add your credentials to access the ONTAP cluster.

**Credentials**  
Specify account with storage administrator privileges.

Name	Credentials:
Credentials	<input type="button" value="HCIEUC\Admin (HCIEUC\Admin, last edited: 98 days ago)"/> <input type="button" value="Add..."/> <a href="#">Manage accounts</a>
NAS Filer	Protocol: <input type="button" value="HTTPS"/>
Apply	Port: <input type="button" value="443"/>
Summary	

5. On the NAS Filer page choose the desired protocols to scan and select Next.

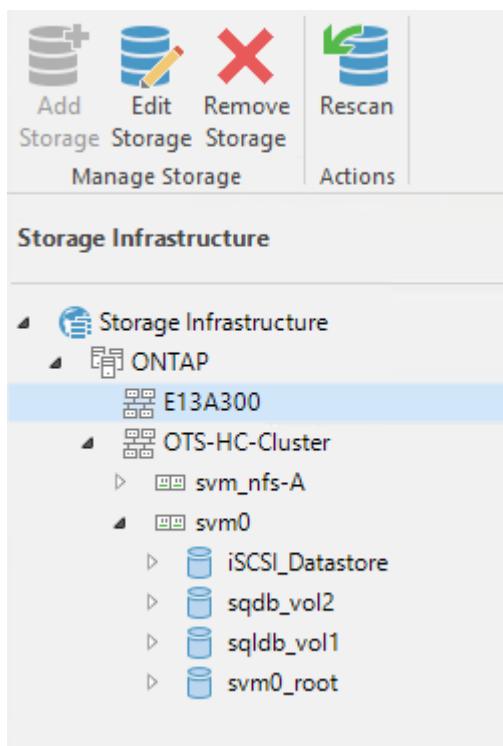


**NAS Filer**  
Specify how this storage can be accessed by file backup jobs.

Name	Protocol to use:
	<input checked="" type="checkbox"/> SMB
Credentials	<input type="checkbox"/> NFS
	<input checked="" type="checkbox"/> Create required export rules automatically
NAS Filer	Volumes to scan:
Apply	All volumes <input type="button" value="Choose..."/>
Summary	Backup proxies to use:
	Automatic selection <input type="button" value="Choose..."/>

< Previous  Finish

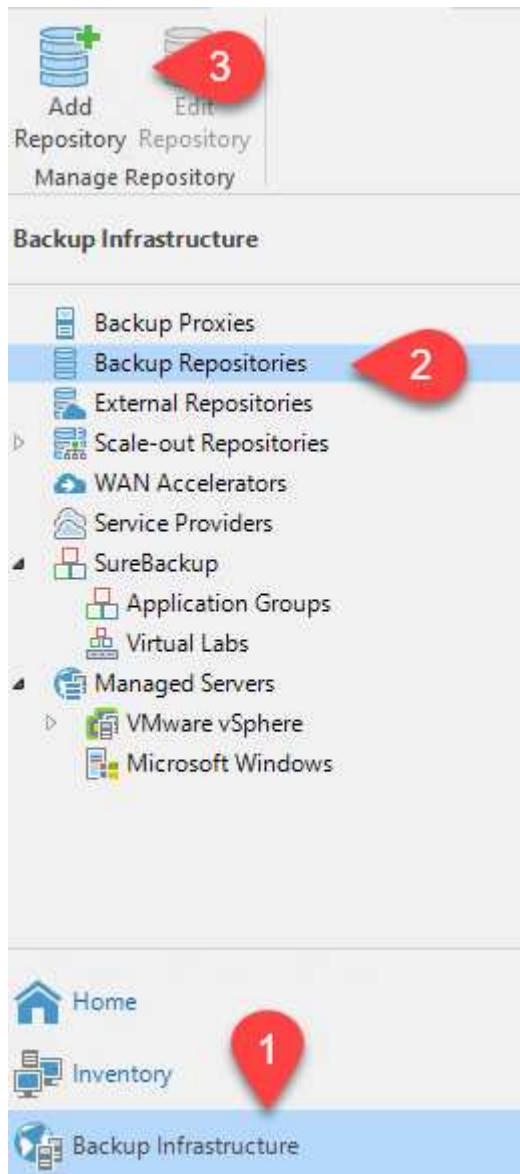
6. Complete the Apply and Summary pages of the wizard and click Finish to begin the storage discovery process. After the scan completes, the ONTAP cluster is added along with the NAS filers as available resources.



**Storage Infrastructure**

- Storage Infrastructure
  - ONTAP
    - E13A300
    - OTS-HC-Cluster
      - svm\_nfs-A
      - svm0
        - iSCSI\_Datastore
        - sqldb\_vol2
        - sqldb\_vol1
        - svm0\_root

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

X

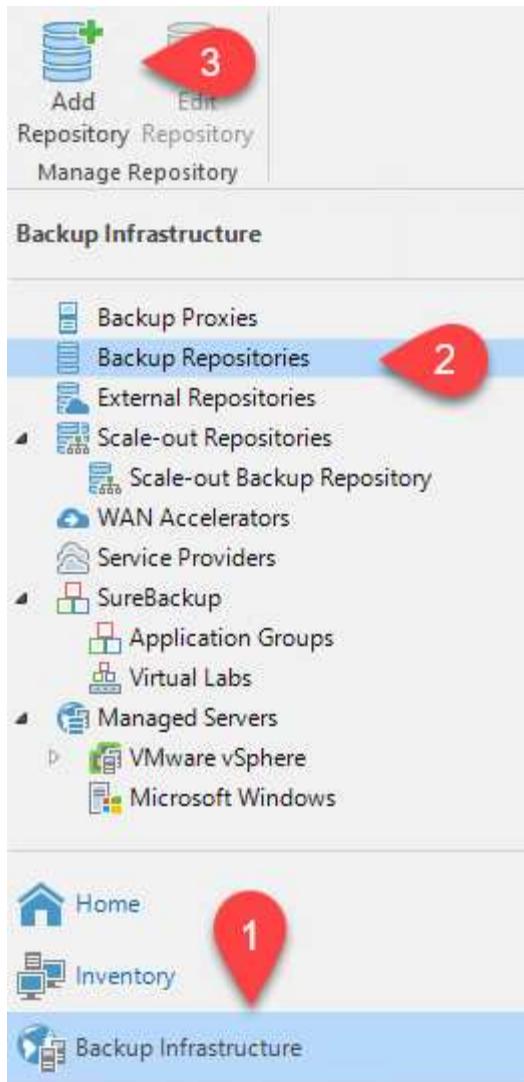
**Share**  
Type in UNC path to share (mapped drives are not supported), specify share access credentials and how backup jobs should write data to this share.

Name	Shared folder: \\172.21.162.181\VBRRepo	Browse...
Share	Use \\server\folder format	
Repository	<input checked="" type="checkbox"/> This share requires access credentials: sddc\administrator (sddc\administrator, last edited: 85 days ago) <input type="button" value="Manage accounts"/> Add...	
Mount Server	Gateway server: <input checked="" type="radio"/> Automatic selection <input type="radio"/> The following server: veeam.sddc.netapp.com (Backup server)	
Review	Use this option to improve performance and reliability of backup to a NAS located in a remote site.	
Apply		
Summary		

## Add the Amazon S3 bucket as a backup repository

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.



### 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 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.

### New Object Storage Repository

X



#### Account

Specify AWS account to use for connecting to Amazon S3 storage bucket.

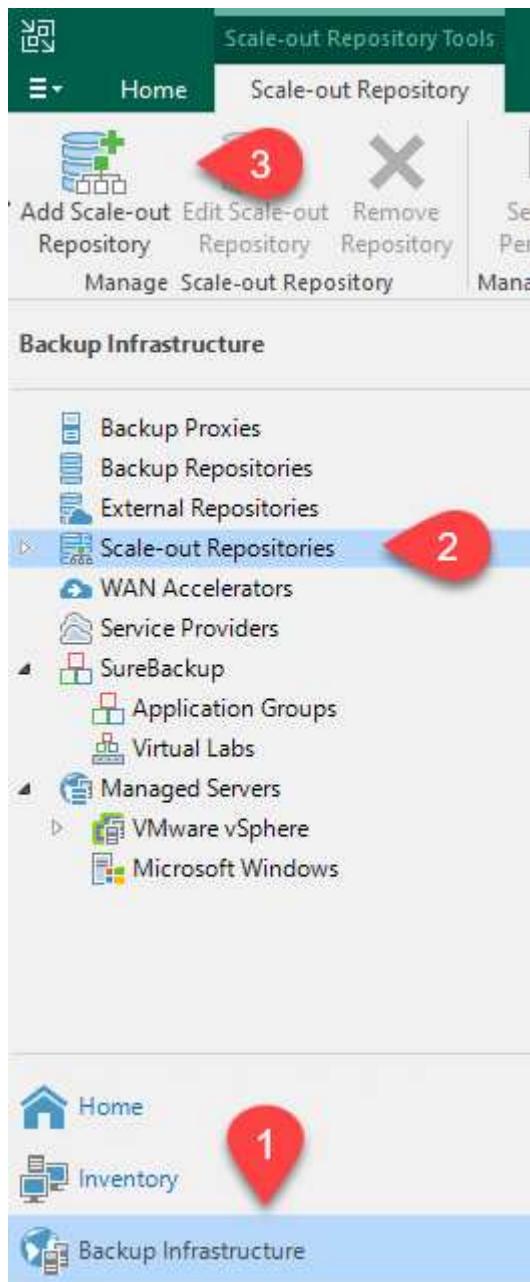
Name	Credentials:	
Account	<input type="text" value="AKIA4H43ZT557HXQT2W (last edited: 107 days ago)"/> <a href="#">Add...</a>	
Bucket	AWS region:	
Summary	<input type="text" value="Global"/>	
<input type="checkbox"/> Use the following gateway server:		
<input type="text" value="veeam.sddc.netapp.com (Backup server)"/>		
Select a gateway server to proxy access to Amazon S3. If no gateway server is specified, all scale-out backup repository extents must have direct Internet access.		
<a href="#">&lt; Previous</a> <a href="#">Next &gt;</a> <a href="#">Finish</a> <a href="#">Cancel</a>		

5. After the Amazon configuration loads, choose your datacenter, bucket, and folder and click Apply. Finally, click Finish to close out the wizard.

## Create scale-out backup repository

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.

## New Scale-out Backup Repository

X

**Performance Tier**  
Select backup repositories to use as the landing zone and for the short-term retention.



Name	Extents:		
Performance Tier	<table border="1"><thead><tr><th>Name</th></tr></thead><tbody><tr><td>VBRRepo2</td></tr></tbody></table>	Name	VBRRepo2
Name			
VBRRepo2			
Placement Policy			

**Add...** **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 Repository

X

**Capacity Tier**  
Specify object storage to copy backups to for redundancy and DR purposes. Older backups can be moved to object storage completely to reduce 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	<input checked="" type="checkbox"/> Amazon S3 Repo <b>Add...</b>
Placement Policy	Define time windows when uploading to capacity tier is allowed <b>Window...</b>
Capacity Tier	<input checked="" type="checkbox"/> Copy backups to object storage as soon as they are created 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.
Archive Tier	<input checked="" type="checkbox"/> 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.
Summary	Move backup files older than <b>14</b> days (your operational restore window) <b>Override...</b>
	<input type="checkbox"/> Encrypt data uploaded to object storage Password: <b>Add...</b> <b>Manage passwords</b>

**< Previous** **Next >** **Finish** **Cancel**

6. Finally, select Apply and 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](#).

Next: [Cloud backup tools and configuration](#).

## Cloud backup tools and configuration

Previous: [Deploy and configure Veeam Backup Server](#).

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.

For more information on completing these steps, see to section ["SnapCenter database Restore Process"](#).

### 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](#).

### Configure secondary Veeam Backup & Replication server

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"](#)".

[Next: SnapCenter database backup for disaster recovery.](#)

## **SnapCenter database backup for disaster recovery**

[Previous: Cloud backup tools and configuration.](#)

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.

## **SnapCenter backup and restore process summary**

- 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.

## Back up the SnapCenter database and configuration

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](#).

### Log into Swagger and obtain authorization token

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 API

[ Base URL: /api ]

<https://snapcenter.sddc.netapp.com:8146/Content/swagger/SnapCenter.yaml>

Manage your SnapCenter Server using the SnapCenter API.

To access the swagger documentation of "SnapCenter Plug-in for VMware vSphere" API's, please use  
[https://\(SCV\\_hostname\):\(SCV\\_host\\_port\)/api/swagger-ui.html](https://(SCV_hostname):(SCV_host_port)/api/swagger-ui.html)

2. Expand the Auth section and click Try it Out.

### Auth

POST /4.6/auth/login Service login

The login endpoint exposes the method required to log in to the SnapCenter service. The login method returns a token that is used to authenticate subsequent requests.

Parameters

Try it out

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

Name	Description
TokenNeverExpires boolean (query)	Token never expires  <input type="text" value="false"/>
UserOperationContext * required object (body)	User credentials  <a href="#">Edit Value</a> <a href="#">Model</a>  <pre>{   "UserOperationContext": {     "User": {       "Name": "localhost\\scadmin",       "Passphrase": "NetApp321",       "Rolename": "SnapCenterAdmin"     }   } }</pre>  <input type="button" value="Cancel"/>
Parameter content type  <input type="text" value="application/json"/>	
<input type="button" value="Execute"/>	

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

```

  "LogonMode": 0,
  "PluginName": null,
  "HostId": 0,
  "RoleId": null,
  "JobIds": null
},
"User": {
  "Token": "K1YxOg==tsV6Z0tdAmAYpe8q5SG6wcoGaSjwME6jrNy5CsY63HKQ5LkoZLIESRNAhpGJJ0UUQ/nEndgtVGDZnvx+I/ZJZIn5M1NZrj6
CLfGTApq1GmacagT08bgb5bMTx07EcdrAidzAXUDb3GyLOKtW0GdwKzSeUwKj3uVupnk1E3lskK6PRBv9RS8j0qHQvo4v4RL0hhThhwPhV
9/23nFeJVP/p1Ev4vrV/zeZVTUHFHUM069XRe5cuW9nwyj4b0I5Y5FN3XDkjQ==",
  "Name": "SCAdmin",
  "TokenHashed": null,
  "Type": "",
  "TokenTime": "2022-03-22T14:21:57.3665661-07:00",
  "Id": "1",
  "FullName": "SCAdmin",
  "Host": null,
  "Author": null,
  "UserName": "",
  "Domain": "",
  "Passphrase": ""
}

```

[Download](#)

## Perform a SnapCenter database backup

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/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 creates 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.



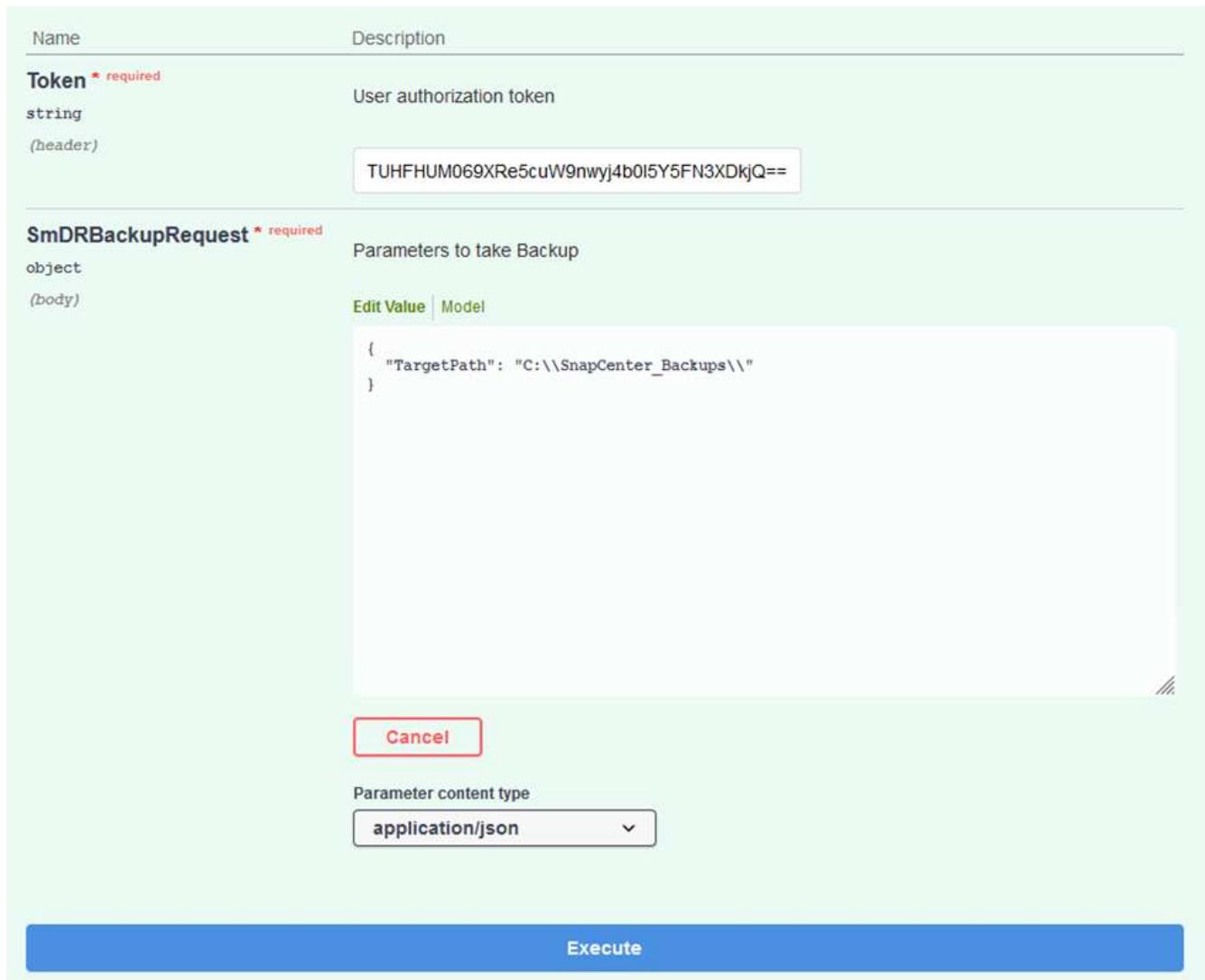
The backup process does not allow backing up directly to an NFS or CIFS file share.

Name	Description
<b>Token</b> * required string (header)	User authorization token  TUHFHUM069XRe5cuW9nwyj4b0l5Y5FN3XDkjQ==
<b>SmDRBackupRequest</b> * required object (body)	Parameters to take Backup  Edit Value   Model  { "TargetPath": "C:\\\\SnapCenter_Backups\\\\" }

**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.

Job Details X

SnapCenter Server disaster recovery backup

- ✓ ▾ 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'
  - ✓ ► 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'
  - ✓ ► 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'
  - ✓ ► Disaster recovery backup of 'oraclesrv\_09.sddc.netapp.com'
  - ✓ ► Disaster recovery backup of 'sqlsrv-06.sddc.netapp.com'
  - ✓ ► Disaster recovery backup of 'sqlsrv-07.sddc.netapp.com'

**Task Name:** SnapCenter Server disaster recovery backup **Start Time:** 03/23/2022 10:27:11 AM **End Time:** 03/23/2022 10:27:47 AM

View Logs Cancel Job Close

### Use XCOPY utility to copy the database backup file to the SMB share

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
```

[Next: Failover.](#)

## Failover

[Previous: SnapCenter database backup for disaster recovery.](#)

### 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 database restore process

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 SnapCenter Server Restore.

Parameters

**Try it out**

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

Name	Description
<b>Token</b> <small>* required</small> <small>string</small> <small>(header)</small>	User authorization token  KIYxOg==rMXzS7EPIGRzTXjftn6Q+JoNGpueQt
<b>SmDRRestoreRequest</b> <small>* required</small> <small>object</small> <small>(body)</small>	Parameters to take for Restore  Edit Value   Model  { "BackupName": "SnapCenter.sddc.netapp.com_03-23-2022_12.38.00.6713", "BackupPath": "C:\\\\SnapCenter\\\\" }

4. Select the Execute button to start the restore process.  
5. From SnapCenter, navigate to the Monitor section to view the progress of the restore job.

NetApp SnapCenter®

Jobs   Schedules   Events   Logs

search by name

Jobs - Filter

ID	Status	Name
20482	✓	SnapCenter Server Disaster Recovery
20481	✓	SnapCenter Server disaster recovery backup
20480	✗	SnapCenter Server disaster recovery backup
20475	✓	Backup of Resource Group 'SQLSRV-09' with policy 'SQL-Hourly'
20474	✓	Backup of Resource Group 'SQLSRV-05' with policy 'SQL-Hourly'
20473	⌚	Backup of Resource Group 'OracleSrv_06' with policy 'Oracle-Hourly'
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
<b>Token</b> <small>* required</small> string (header)	User authorization token KIYxOg==rMXzS7EPIGRzTXjfton6Q+JoNGpueQI
<b>SmSetDisasterRecoverySettingsRequest</b> <small>* required</small> object (body)	Parameters to enable or disable the DR mode Edit Value   Model { "EnableDisasterRecovery": true }



See comments regarding additional procedures.

[Next: Restore application VMs with Veeam full restore.](#)

### Restore application VMs with Veeam full restore

[Previous: Failover.](#)

### Create a backup repository and import backups from S3

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.

## Add Backup Repository

Select the 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 Capacity Tier of scale-out backup repositories, backing up directly to object storage is not currently supported.

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.

 **S3 Compatible**  
Adds an on-premises object storage system or a cloud object storage provider.

 **Amazon S3**  
Adds Amazon cloud object storage. Amazon S3, Amazon S3 Glacier (including Deep Archive) and Amazon Snowball Edge are supported.

 **Google Cloud Storage**  
Adds Google Cloud storage. Both Standard and Nearline storage classes are supported.

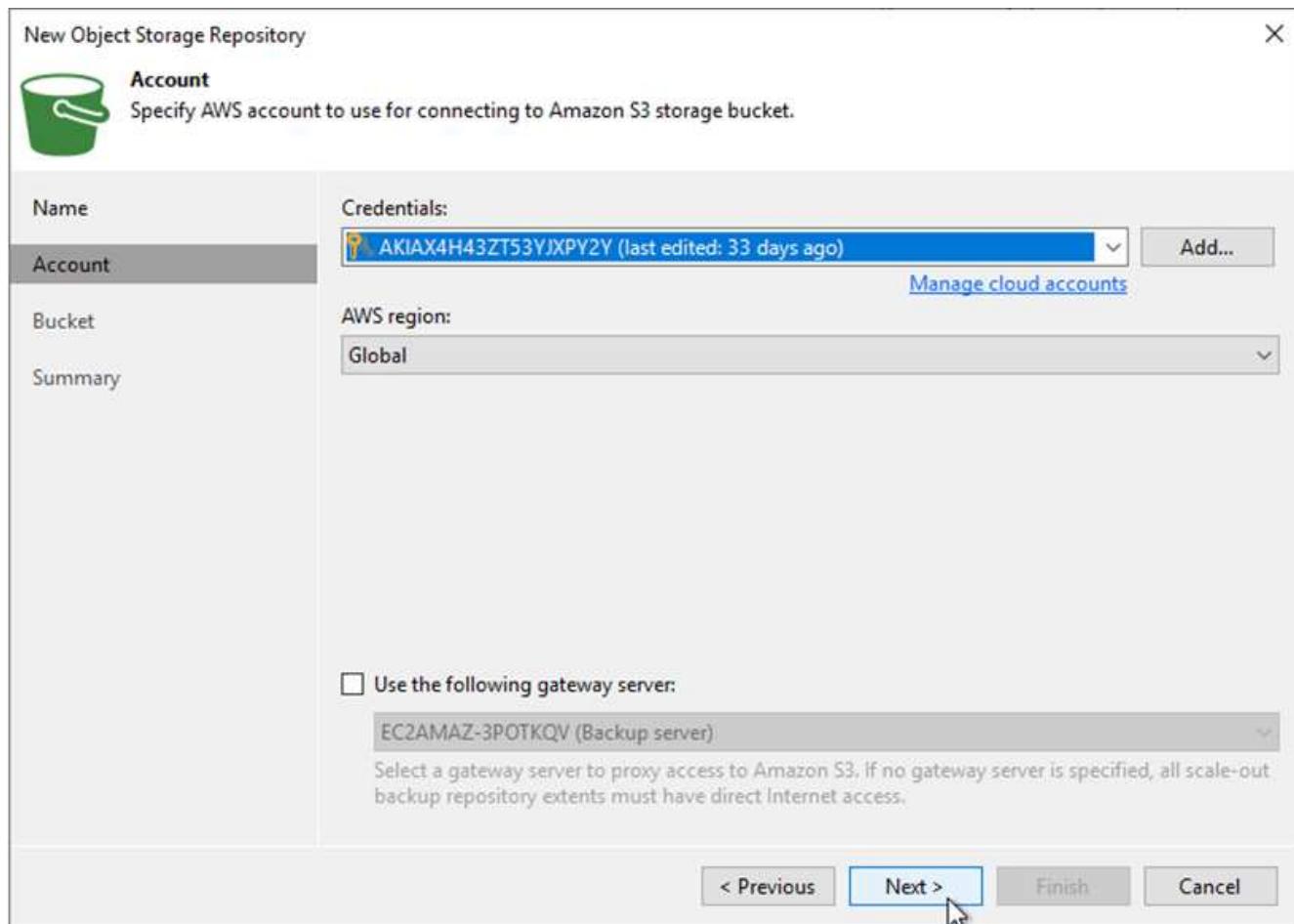
 **IBM Cloud Object Storage**  
Adds IBM Cloud object storage. S3 compatible versions of both on-premises and IBM Cloud storage offerings are supported.

 **Microsoft Azure Storage**  
Adds Microsoft Azure cloud object storage. Microsoft Azure Blob Storage, Microsoft Azure Archive Storage and Microsoft Azure Data Box are supported.

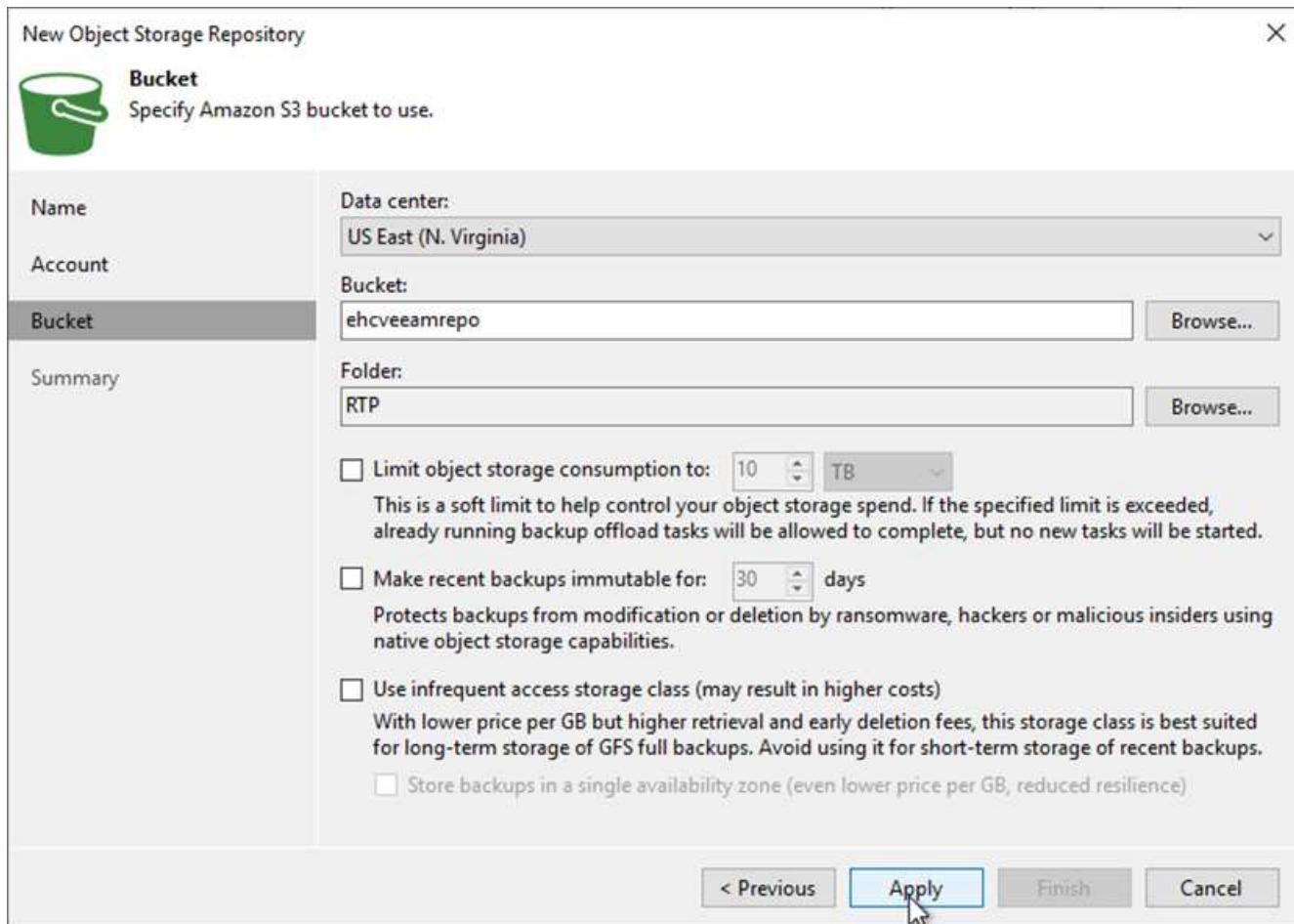
3. From the list of Amazon Cloud Storage Services, select Amazon S3.



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.



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

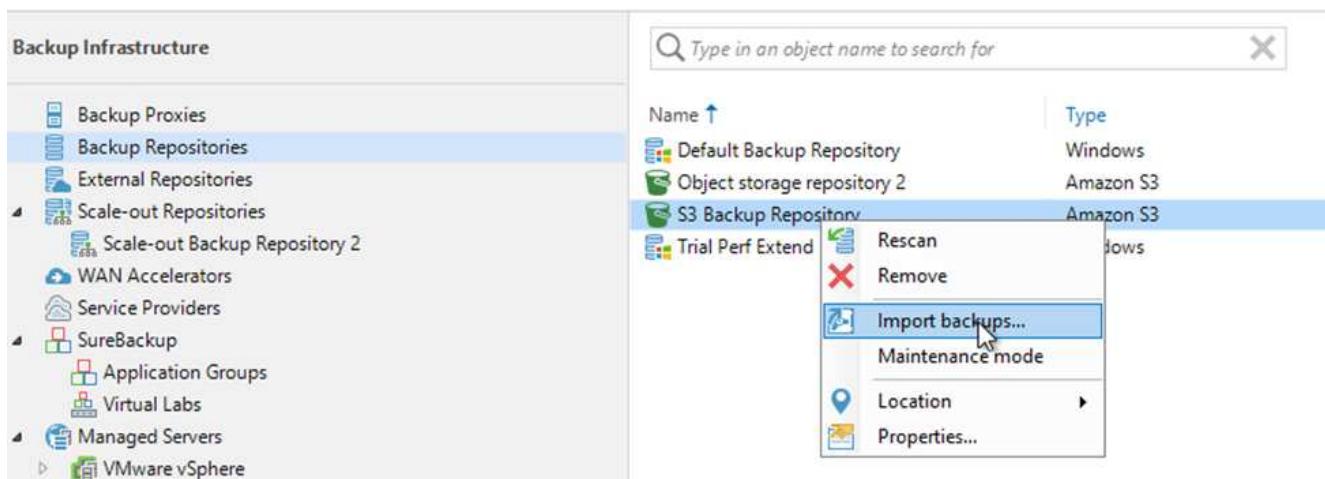


- Finally, select Finish to complete the process and add the repository.

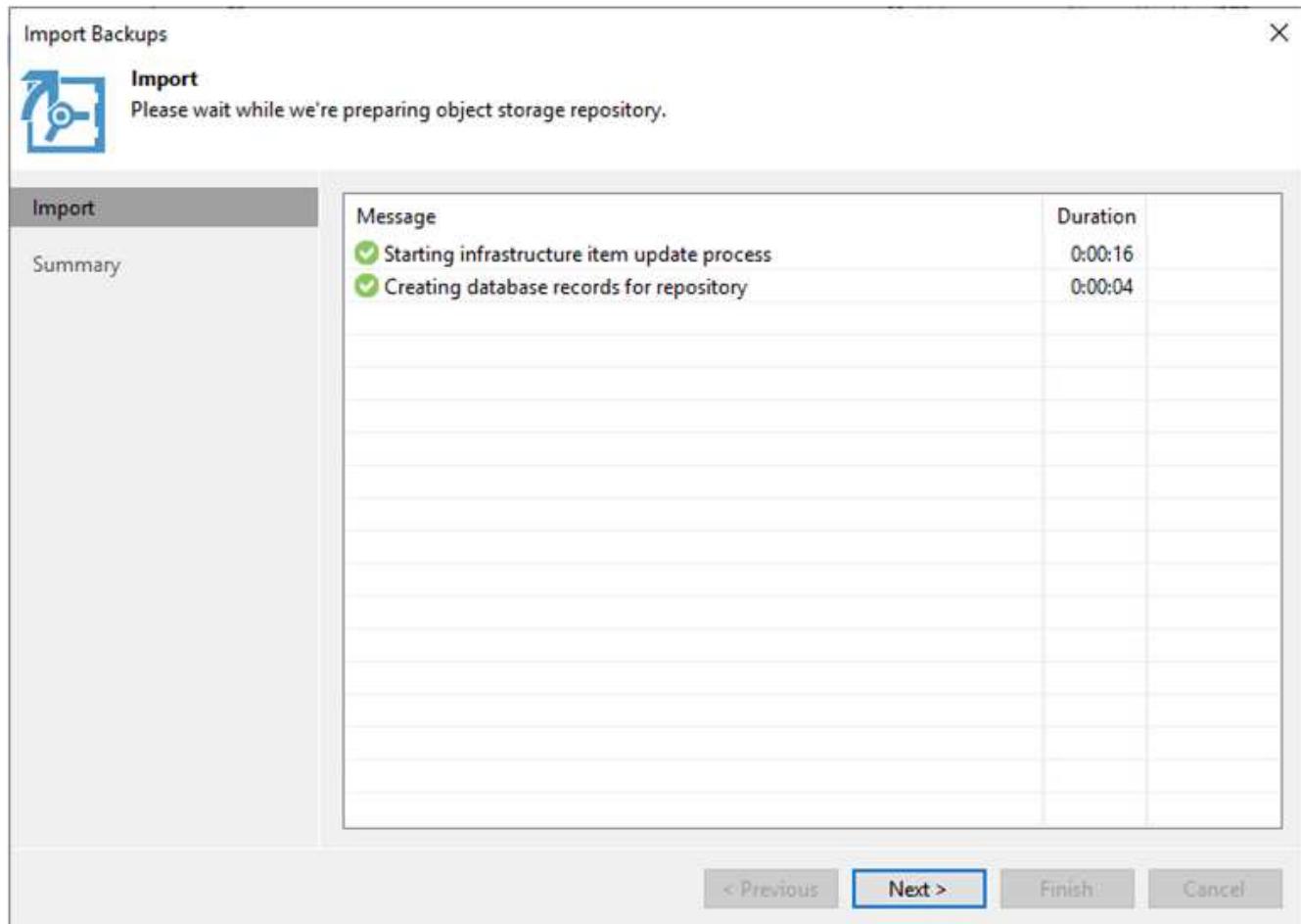
### Import backups from S3 object storage

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

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



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



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

System X

Name:	<b>Configuration Database Resynchroniz...</b>	Status:	<b>Success</b>
Action type:	Configuration Resynchronize	Start time:	4/6/2022 3:01:30 PM
Initiated by:	EC2AMAZ-3POTKQV\administrator	End time:	4/6/2022 3:04:57 PM

**Log**

Message	Duration
✓ Starting backup repositories synchronization	
✓ Enumerating repositories	
✓ Found 1 repository	
✓ Processing capacity tier extent of S3 Backup Repository 2	0:03:23
✓ S3 Backup Repository: added 2 unencrypted	0:03:20
✓ Importing backup 2 out of 2	0:03:15
✓ Backup repositories synchronization completed successfully	

**Close**

### Restore application VMs with Veeam full restore to VMware Cloud

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**.

The screenshot shows the Veeam Backup & Replication software interface. The left sidebar has 'Object Storage (Imported)' selected. The main pane shows a list of SQL servers with 'SQLSRV-04' selected. A context menu is open for 'SQLSRV-04', with 'Restore entire VM...' highlighted.

Job Name	Creation Time
Oracle Servers	3/27/2022 1:00 AM
SQL Servers	3/27/2022 1:00 AM
SQLSRV-01	
SQLSRV-02	
SQLSRV-03	
SQLSRV-04	
SQLSRV-05	
SQLSRV-06	
SQLSRV-07	
SQLSRV-08	
SQLSRV-09	
SQLSRV-10	

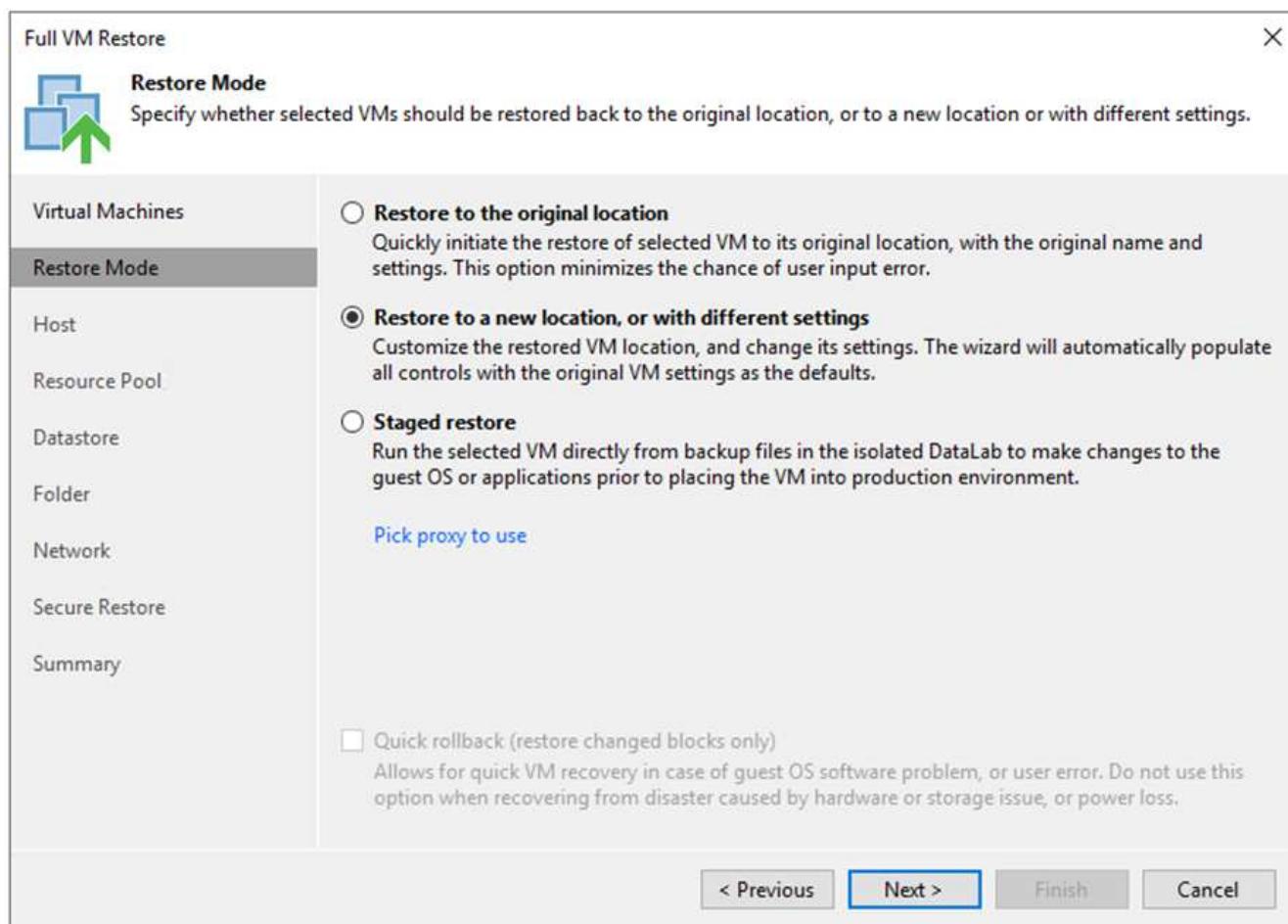
2. On the first page of the Full VM Restore wizard, modify the VMs to backup if desired and select Next.

The screenshot shows the 'Full VM Restore' wizard. The left sidebar has 'Virtual Machines' selected. The main pane shows a table of virtual machines with 'SQLSRV-04' selected. On the right, there are buttons for 'Add...', 'Point...', and 'Remove'.

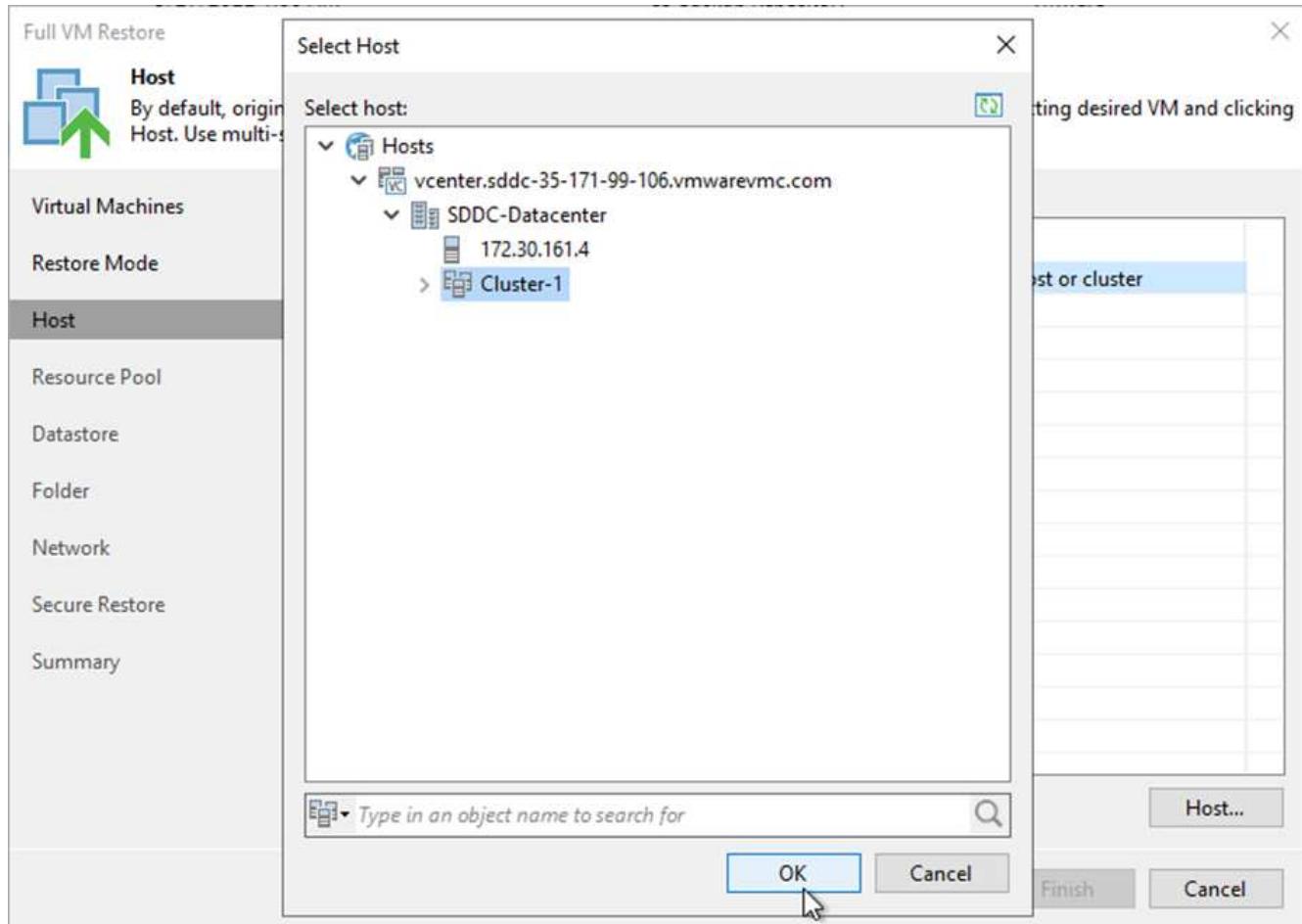
Name	Size	Restore point
SQLSRV-04	62.7 GB	less than a day ago (1:03 AM ...)

Buttons at the bottom: < Previous, **Next >**, Finish, Cancel

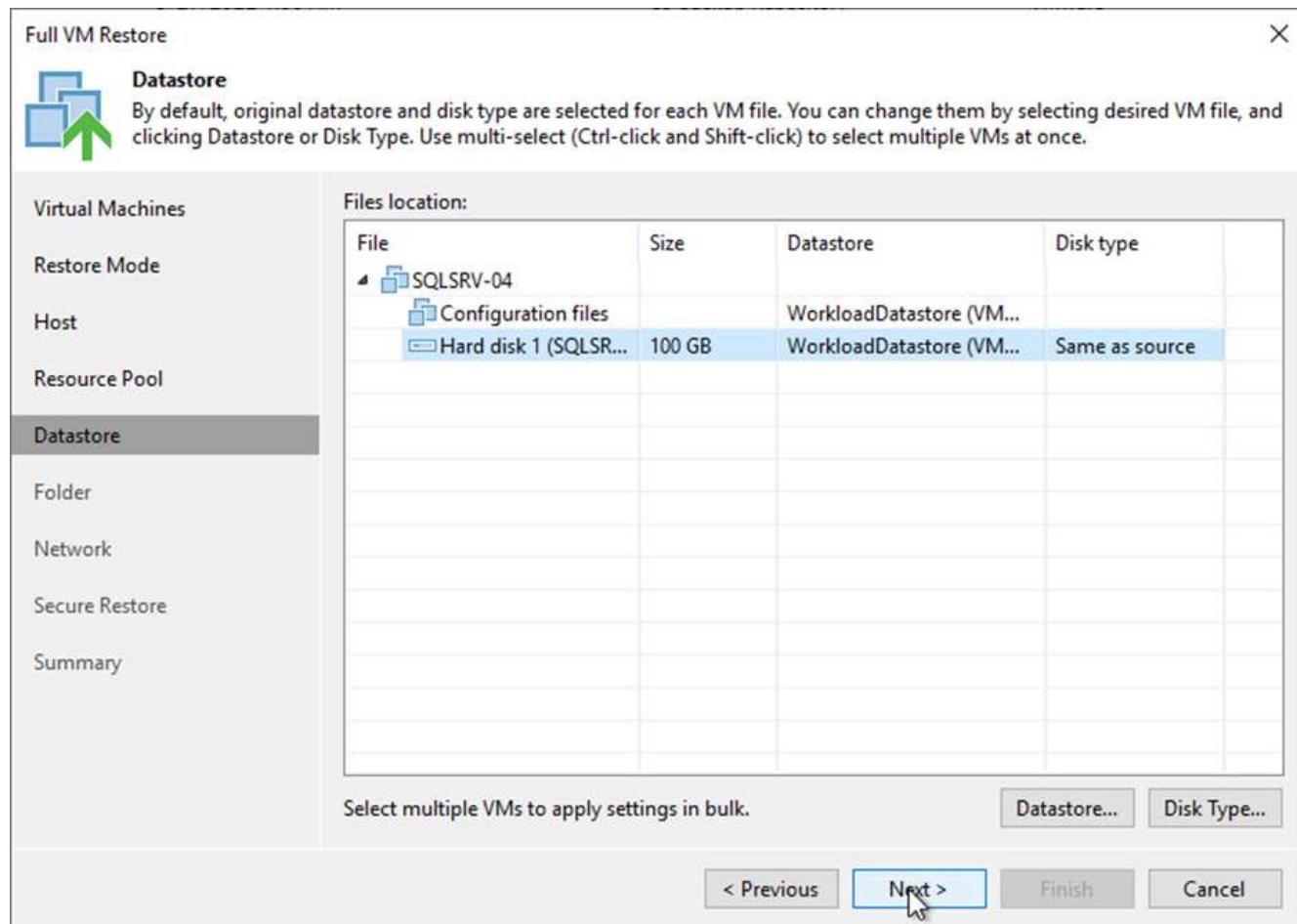
3. On the Restore Mode page, select Restore to a New Location, or with Different Settings.



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



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



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

**Network**

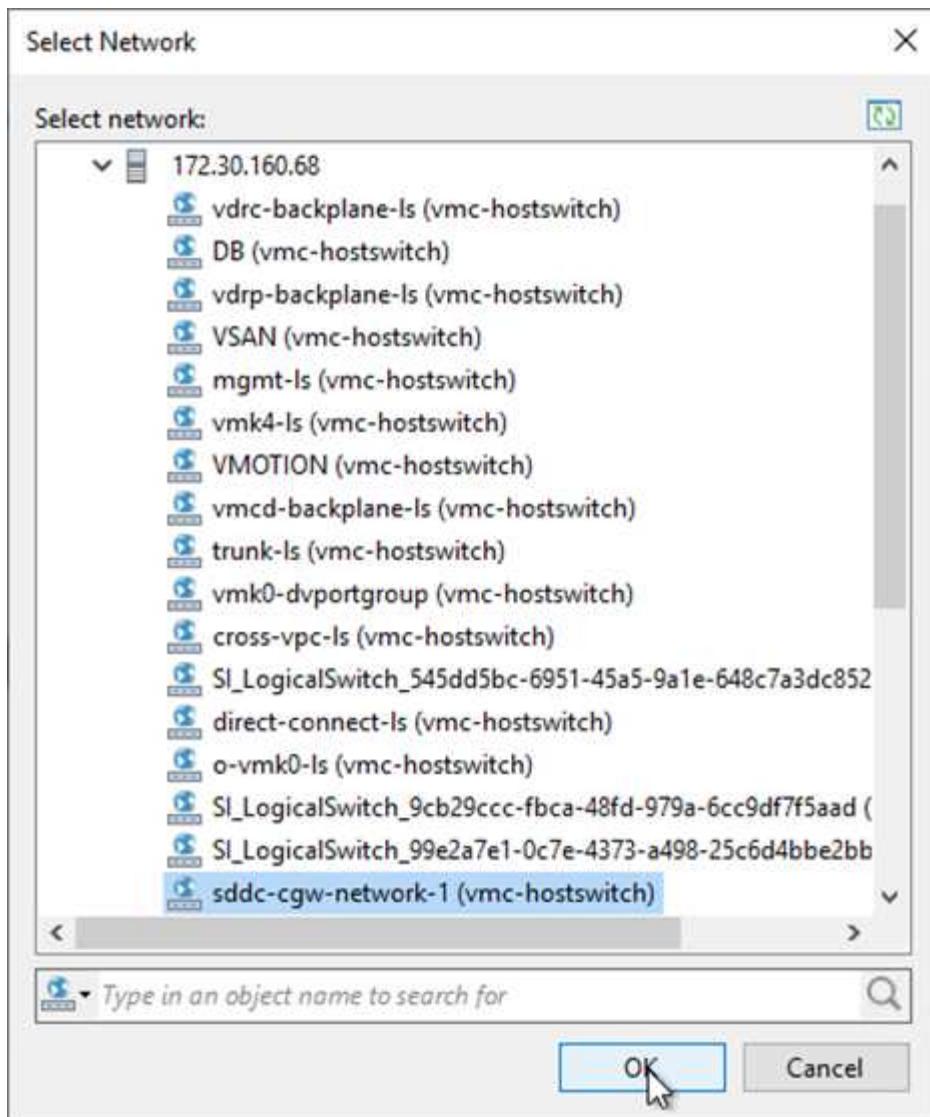
By default, we will connect the restored VM to the same virtual networks as the original VM. If you are restoring to a different location, specify how networks map between original and new locations.

**Virtual Machines****Restore Mode****Host****Resource Pool****Datastore****Folder****Network****Secure Restore****Summary****Network connections:**

Source	Target
SQLSRV-04	
Management 181 (DSwitch)	Not connected
Data - A - 3374 (DSwitch)	Not connected
Data - B - 3375 (DSwitch)	Not connected

Select multiple VMs to apply settings change in bulk.

[Network...](#)[Disconnect](#)[< Previous](#)[Next >](#)[Finish](#)[Cancel](#)



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

Next: [Restore SQL Server application data.](#)

### Restore SQL Server application data

[Previous: Restore application VMs with Veeam full restore.](#)

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.
2. 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."](#)

A summary of the SQL Server application data recovery process is as follows:

1. Configure the VM in preparation for the restore process.
2. Set up FSx for iSCSI access.
3. Set up the Windows VM for iSCSI access.
4. Attach the SQL Server database and bring it online.
5. Confirm communication between SnapCenter and the SnapCenter SQL Server Plug-in.

## VM: Post restore configuration for SQL Server VM

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::> igrup create -vserver DestSVM -igroup igrupNome -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 igrup igrupNome
```

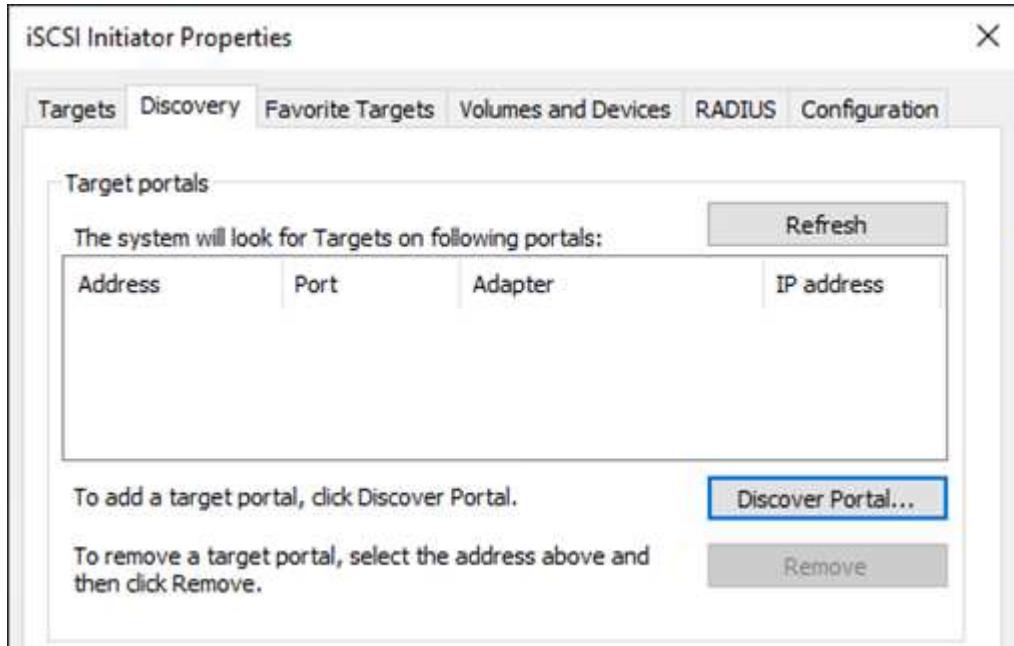
4. To find the path name, run the `lun show` command.

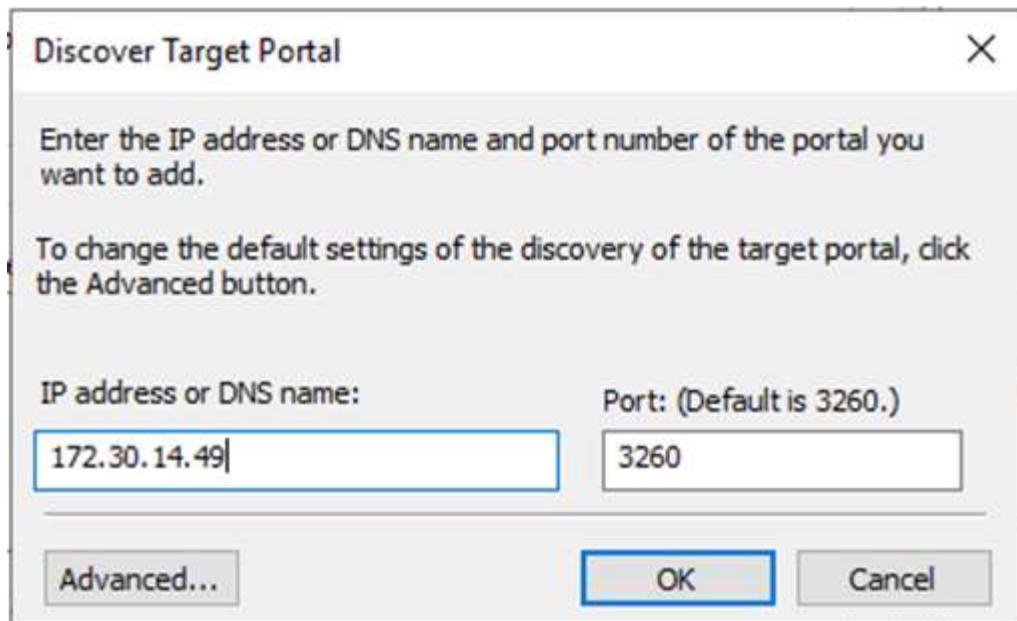
## Set up the Windows VM for iSCSI access and discover the file systems

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.

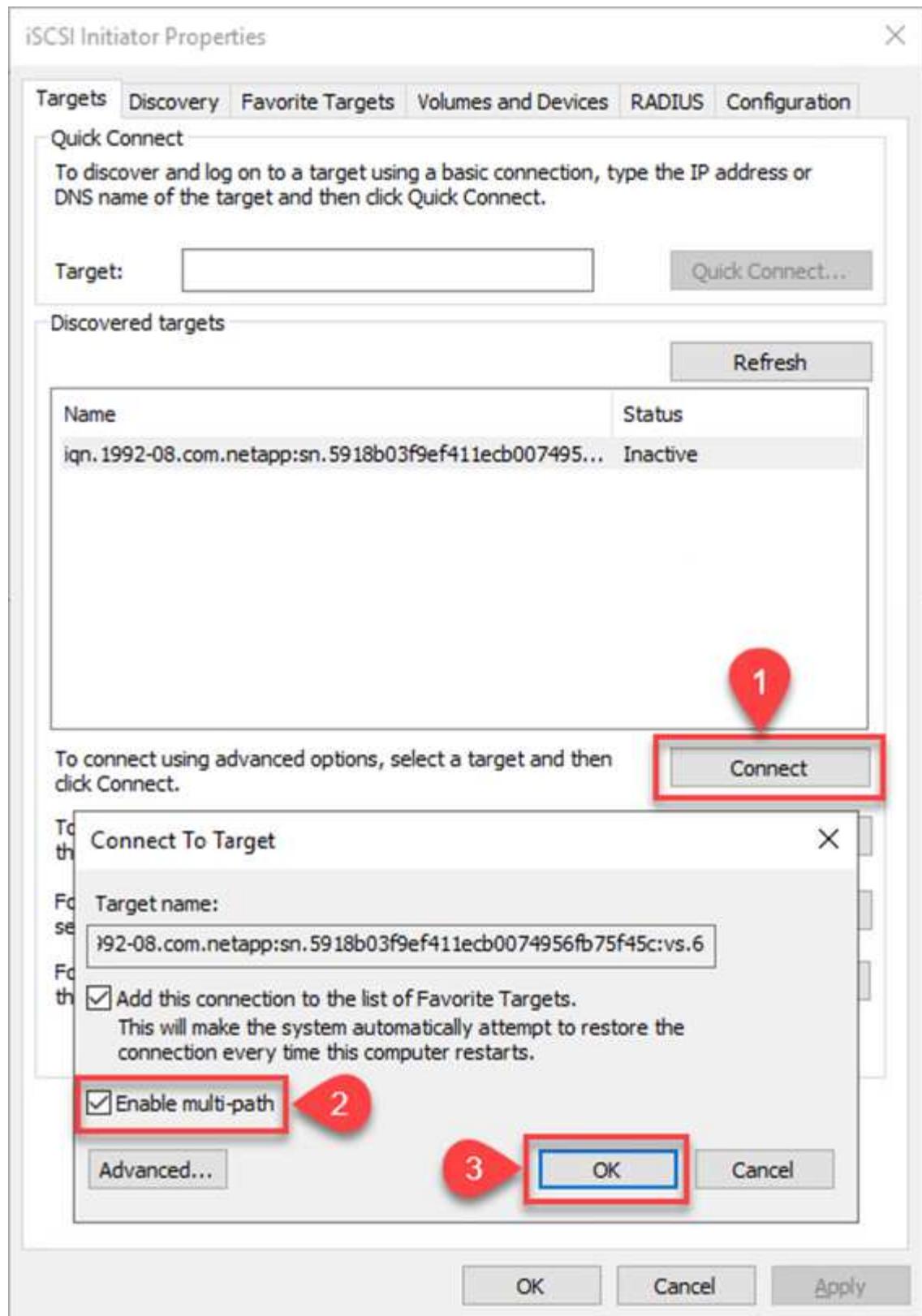
Endpoints	
Management DNS name	Management IP address
svm-045c077375d3d9799.fs-0ae40e08acc0dea67.fsx.us-east-1.amazonaws.com	198.19.254.53
NFS DNS name	NFS IP address
svm-045c077375d3d9799.fs-0ae40e08acc0dea67.fsx.us-east-1.amazonaws.com	198.19.254.53
iSCSI DNS name	iSCSI IP addresses
iscsi.svm-045c077375d3d9799.fs-0ae40e08acc0dea67.fsx.us-east-1.amazonaws.com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

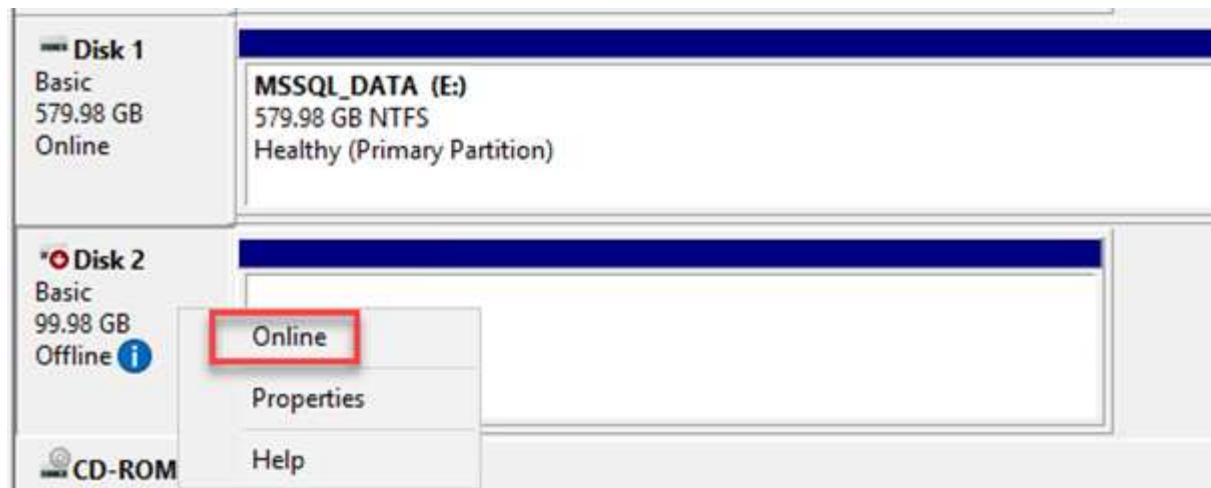




5. On the Target tab, click Connect, select Enable Multi-Path if appropriate for your configuration and then click OK to connect to the target.

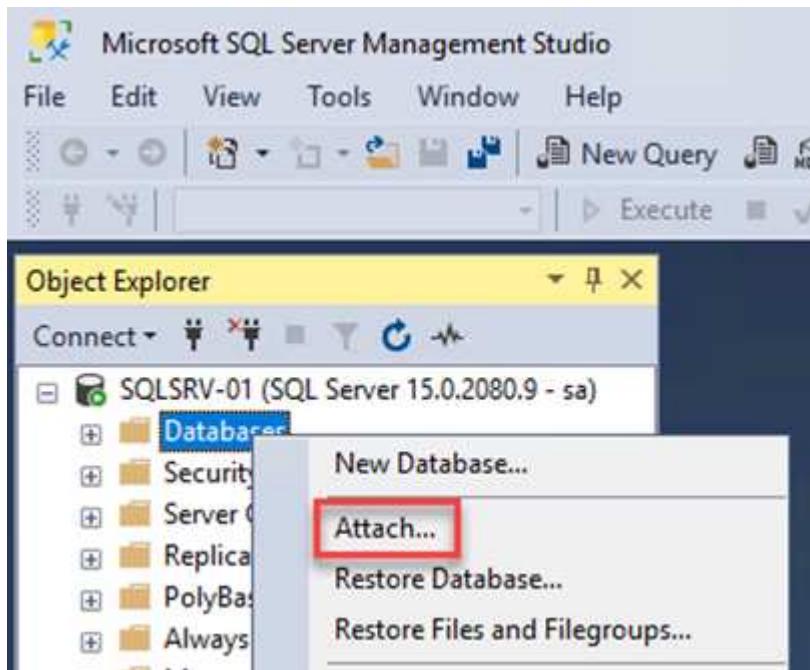


6. Open the Computer Management utility and bring the disks online. Verify that they retain the same drive letters that they previously held.

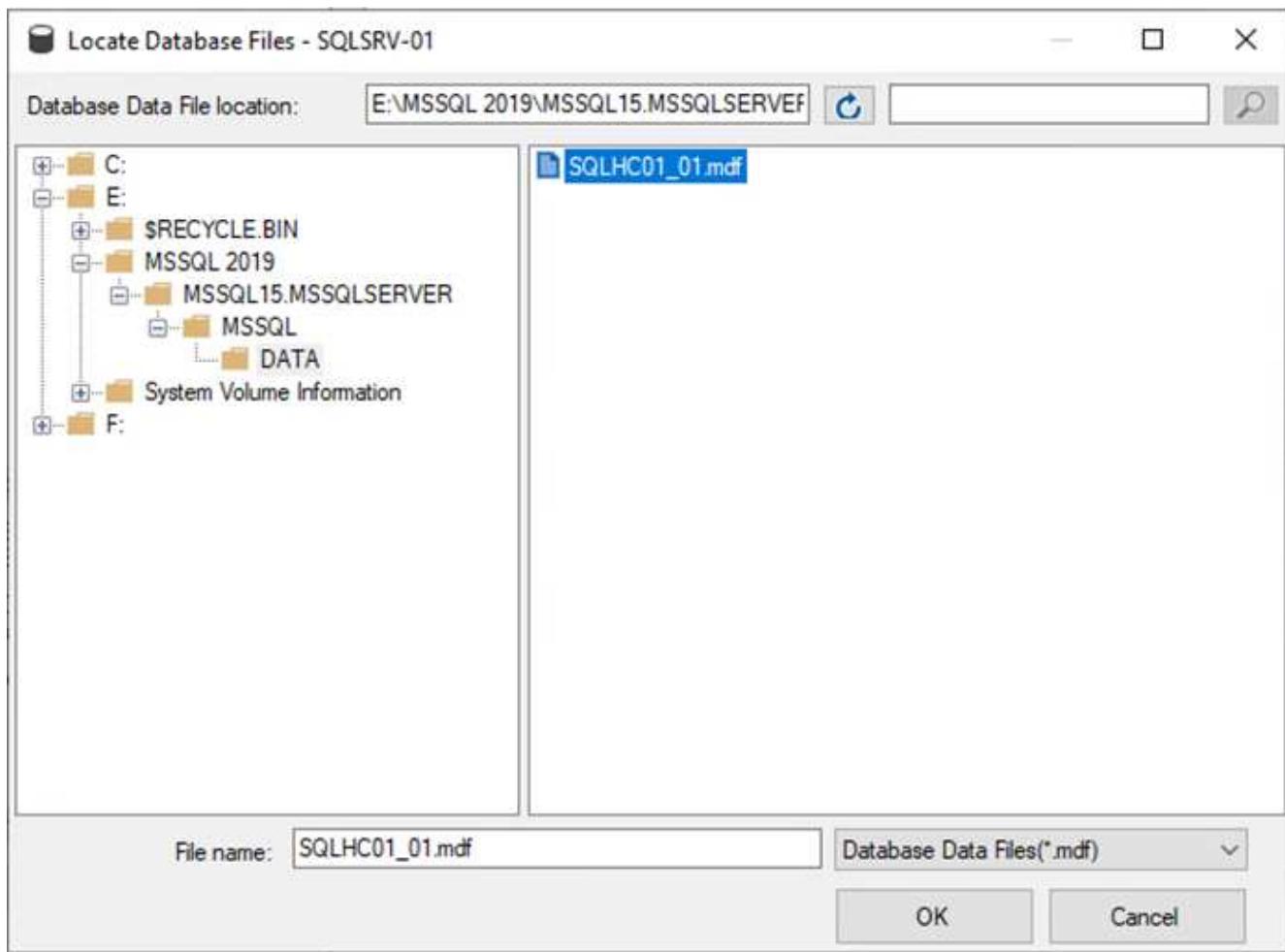


### Attach the SQL Server databases

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.



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.

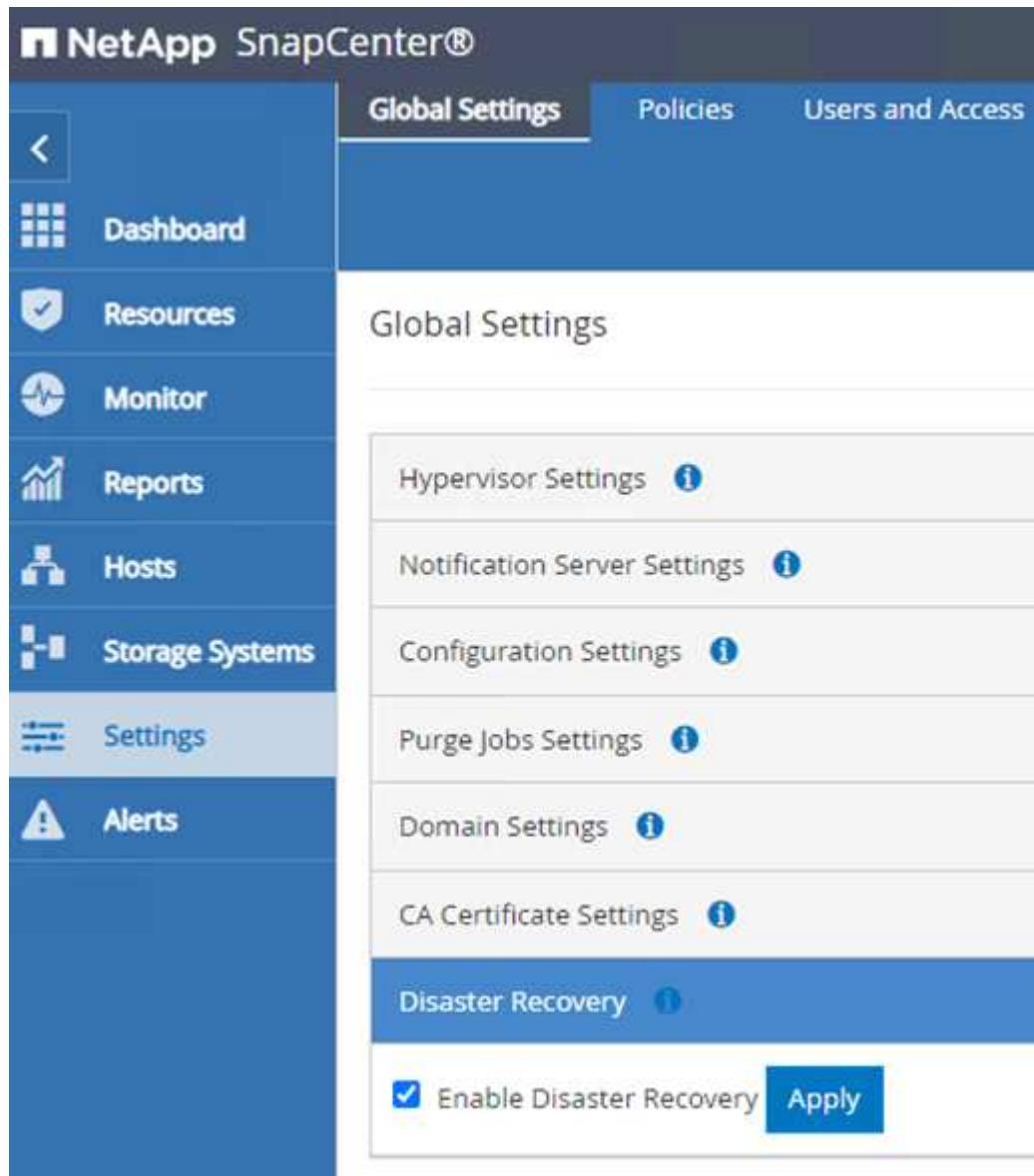
Database Properties - SQLHC01	
<b>Select a page</b>	Script ▾   Help
General	
Files	
Filegroups	
Options	
Change Tracking	
Permissions	
Extended Properties	
Mirroring	
Transaction Log Shipping	
Query Store	
<b>Backup</b>	
Last Database Backup	None
Last Database Log Backup	None
<b>Database</b>	
Name	SQLHC01
<b>Status</b>	Normal
Owner	sa
Date Created	4/13/2022 9:37:18 PM
Size	514944.00 MB
Space Available	501701.86 MB
Number of Users	4
Memory Allocated To Memory Optimized Obj	0.00 MB
Memory Used By Memory Optimized Objects	0.00 MB
<b>Maintenance</b>	
Collation	SQL_Latin1_General_CI_AS

### Confirm SnapCenter communication with SQL Server Plug-in

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.



The screenshot shows the NetApp SnapCenter web interface. The left sidebar contains navigation links: Dashboard, Resources, Monitor, Reports, Hosts, Storage Systems (which is selected and highlighted in blue), Settings, and Alerts. The main content area has a header with tabs: Global Settings (selected), Policies, and Users and Access. Below the header, the page title is "Global Settings". The main content area lists several settings sections: Hypervisor Settings, Notification Server Settings, Configuration Settings, Purge Jobs Settings, Domain Settings, and CA Certificate Settings. The "Disaster Recovery" section is highlighted with a blue background. Within this section, there is a checkbox labeled "Enable Disaster Recovery" which is checked, and a blue "Apply" button. The "Apply" button is highlighted with a blue border.

Next: [Restore Oracle application data](#).

### Restore Oracle application data

Previous: [Restore SQL Server 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."](#)

A summary of the Oracle application data recovery process is as follows:

1. Configure the VM in preparation for the restore process.
2. Set up FSx for iSCSI access.
3. Set up the Linux VM for NFS access.
4. Attach the SQL Server database and bring it online.
5. Confirm communication between SnapCenter and the SnapCenter SQL Server Plug-in.

A summary of the Oracle Server failover process is as follows:

1. Restore the Oracle VM to the VMware Cloud using Veeam.
2. Clean up the VM in preparation for the restore process:
  - a. Change the IP addresses as required.
  - b. Add the system to DNS with an FQDN identical to the original.
3. Set up FSx for NFS access.
4. Mount the NFS volumes on the Oracle Linux Server.

### **Configure FSx for Oracle restore – Break the SnapMirror relationship**

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
        agg1       online    DP      100GB   93.12GB   6%
ora_svm_dest
    oraclesrv_03_u02_dest
        agg1       online    DP      200GB   34.98GB   82%
ora_svm_dest
    oraclesrv_03_u03_dest
        agg1       online    DP      150GB   33.37GB   77%
3 entries were displayed.
```

```
FsxId0ae40e08acc0dea67::> 
```

- 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".
```

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

oraclesrv\_03\_u01\_dest (fsvol-01167370e9b7aefa0)

Summary		Actions ▾	
Volume ID fsvol-01167370e9b7aefa0	Creation time 2022-03-08T14:52:09-05:00	SVM ID svm-02b2ad25c6b2e5bc2	Attach Update volume (highlighted) Create backup Delete volume
Volume name oraclesrv_03_u01_dest	Lifecycle state Created	Junction path -	
UUID 3d7338ce-9f19-11ec-b007-4956fb75f45c	Volume type ONTAP	Tiering policy name SNAPSHOT_ONLY	
File system ID fs-0ae40e08acc0dea67	Size 100.00 GB	Tiering policy cooling period (days) 2	
Resource ARN arn:aws:fsx:us-east-1:541696183547:volume/fs-0ae40e08acc0dea67/fsvol-01167370e9b7aefa0		Storage efficiency enabled Disabled	

4. Add the junction path name and click Update. Specify this junction path when mounting the NFS volume from the Oracle server.

## Update volume

X

### 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.

Enabled (recommended)

Disabled

### Capacity pool tiering policy

You can optionally enable automatic tiering of your data to lower-cost capacity pool storage.

Snapshot Only

▼

Cancel

Update

## Mount NFS volumes on Oracle Server

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.

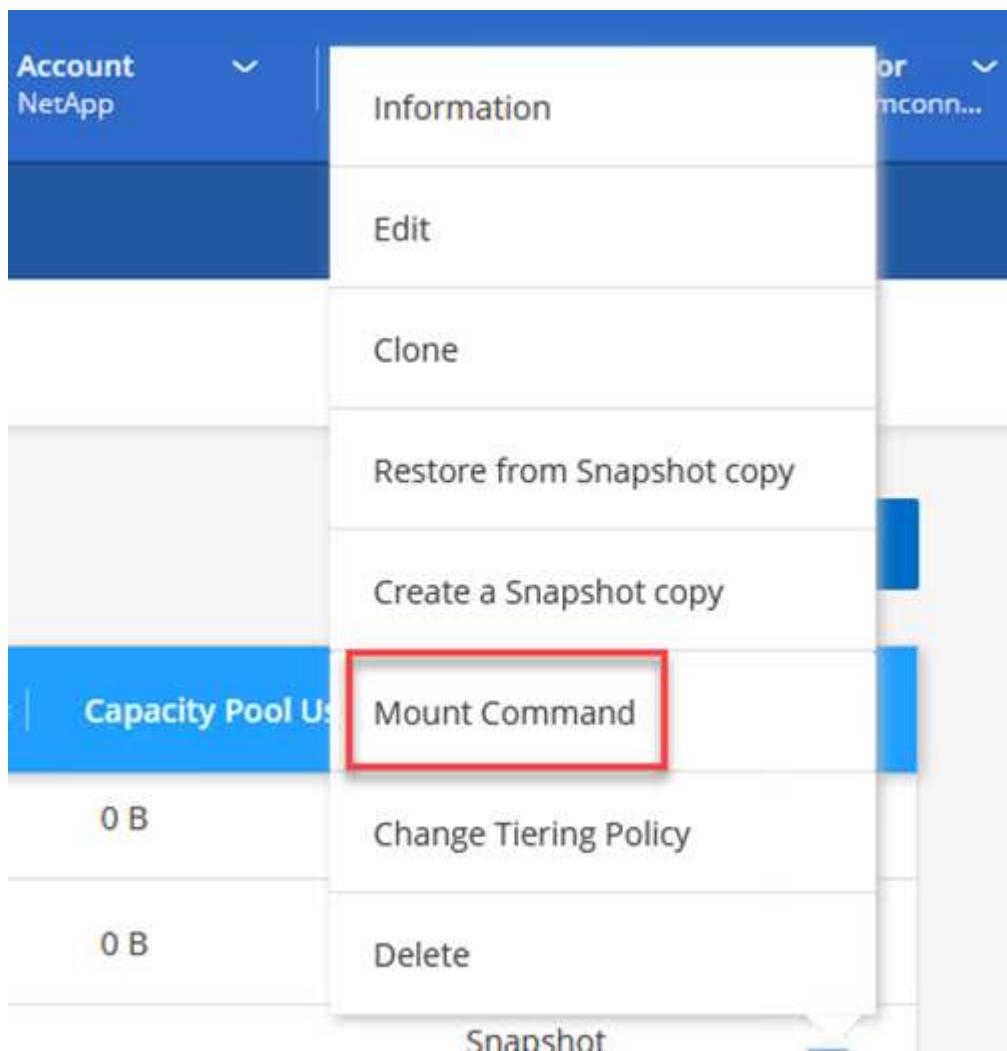
1. In Cloud Manager, access the list of volumes for your FSx cluster.



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.



## Mount Volume NFS

oraclesrv\_03\_u01\_dest

Go to your linux machine and enter this mount command

### Mount Command

```
mount 198.19.254.180:/oraclesrv_03_u01_dest <dest_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.

[Next: Fallback.](#)

### Fallback

[Previous: Restore Oracle application data.](#)

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.

Fallback is outside the scope of this documentation, but fallback differs little from the detailed process outlined here.

[Next: Conclusion.](#)

## Conclusion

[Previous: Failback.](#)

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](#)

## Region Availability – 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.

## 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)	No	Yes	No

Last updated on: June 2, 2022.

# NetApp Hybrid Multicloud Solutions for Azure / AVS

## Protecting Workloads

### Disaster Recovery with ANF and JetStream

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

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

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

## Solution deployment overview

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

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

CPT performs the following functions:

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



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

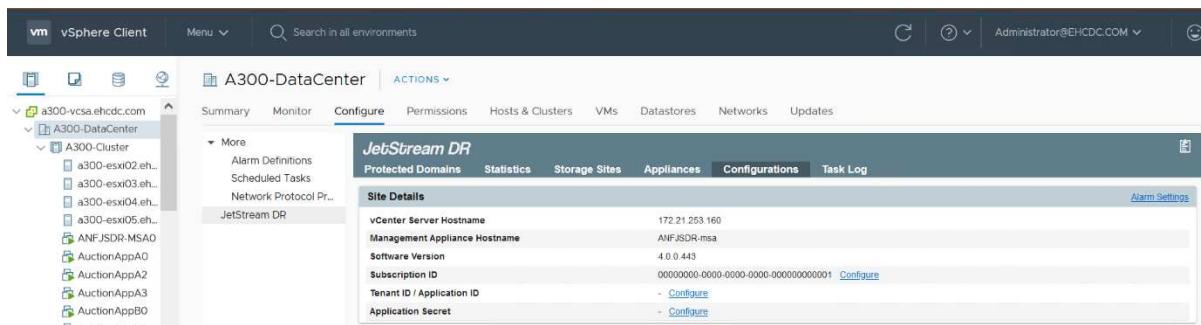
#### **Install JetStream DR in On-Premises Datacenter**

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

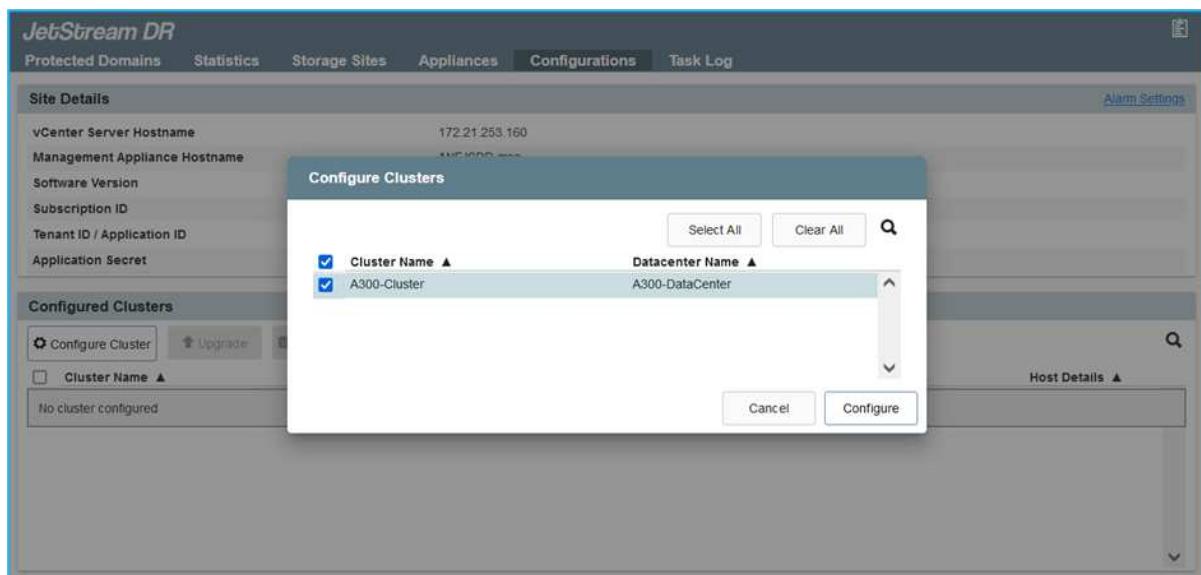


## Details

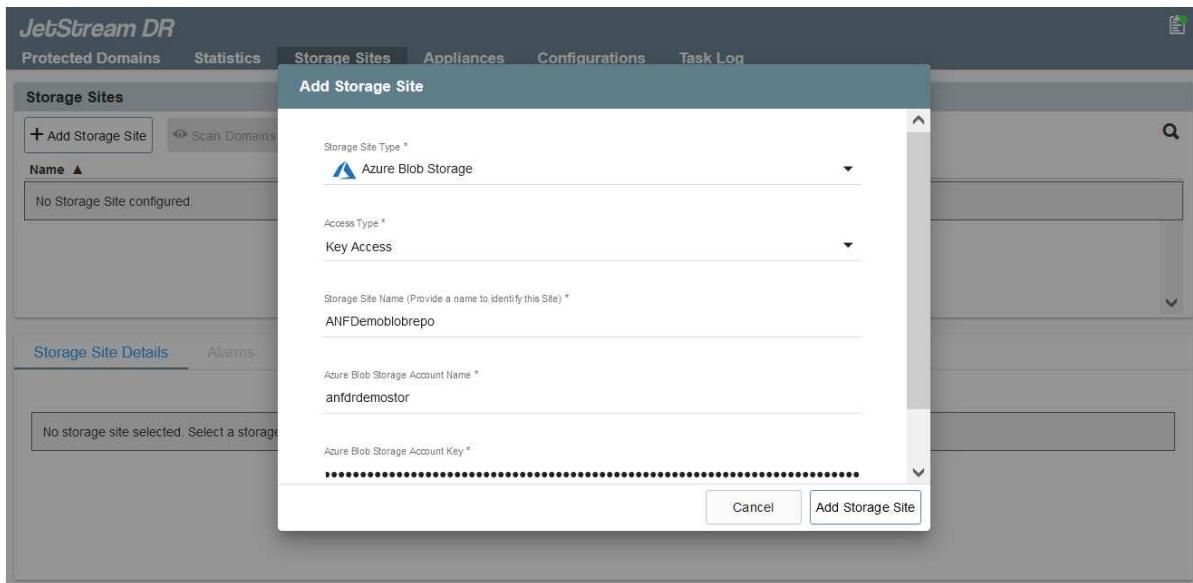
1. Check prerequisites.
2. Run the Capacity Planning Tool for resource and configuration recommendations (optional but recommended for proof-of-concept trials).
3. Deploy the JetStream DR MSA to a vSphere host in the designated cluster.
4. Launch the MSA using its DNS name in a browser.
5. Register the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



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



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

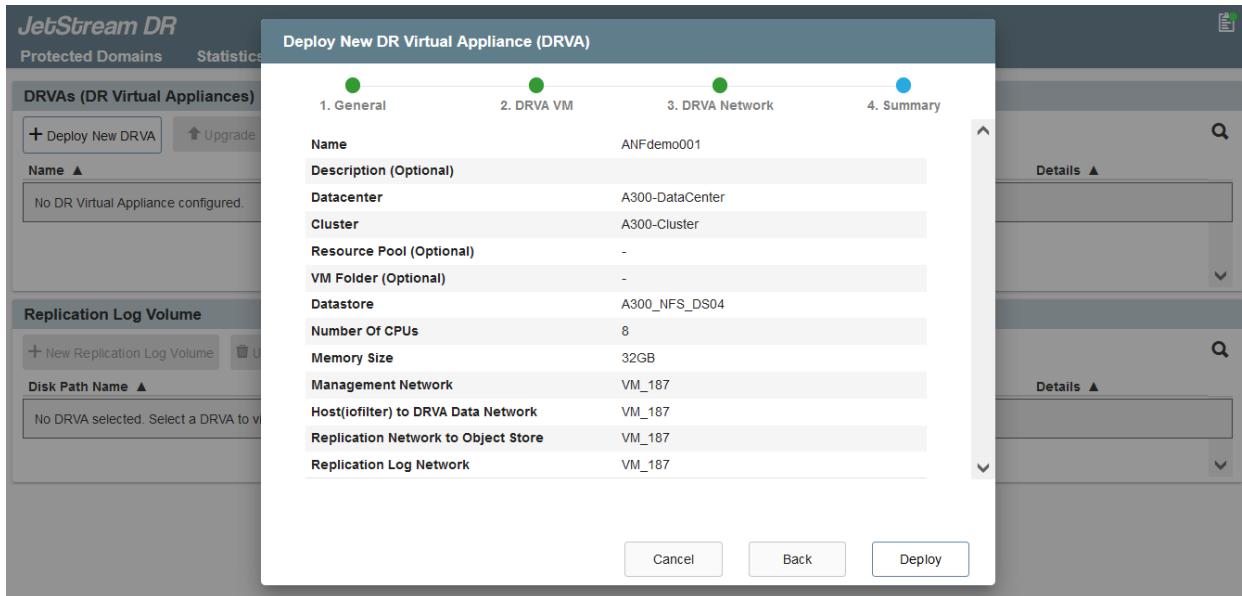


9. Add Azure Blob Storage located at the recovery site.
10. Deploy a DR Virtual Appliance (DRVA) from the Appliances tab.



DRVAs can be automatically created by CPT, but for POC trials we recommend configuring and running the DR cycle manually (start protection > failover > failback).

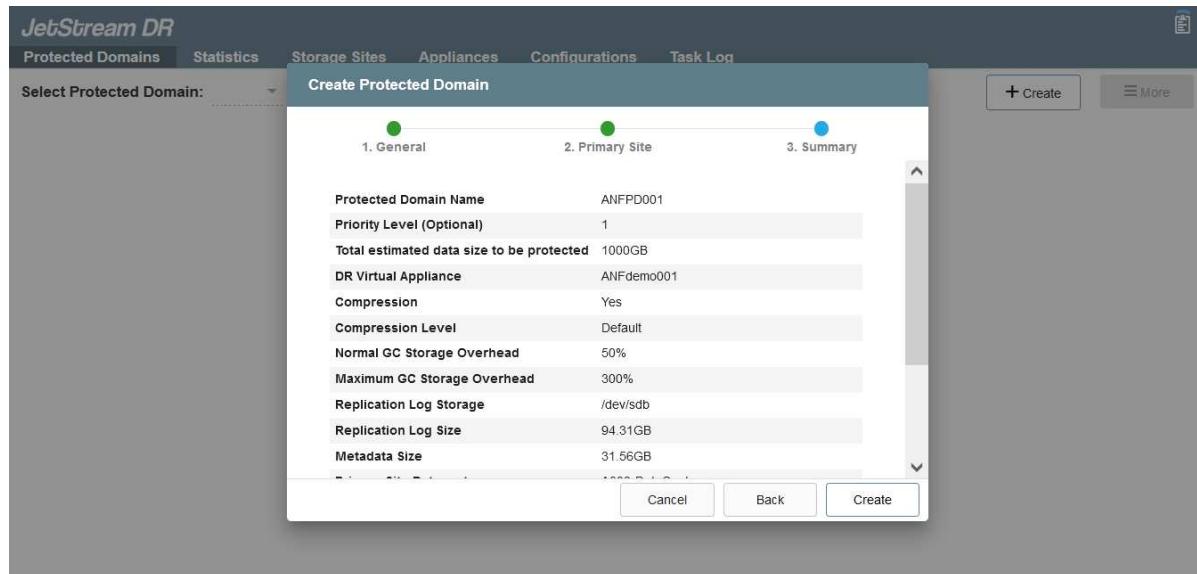
The JetStream DRVA is a virtual appliance that facilitates key functions in the data replication process. A protected cluster must contain at least one DRVA, and typically one DRVA is configured per host. Each DRVA can manage multiple protected domains.



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

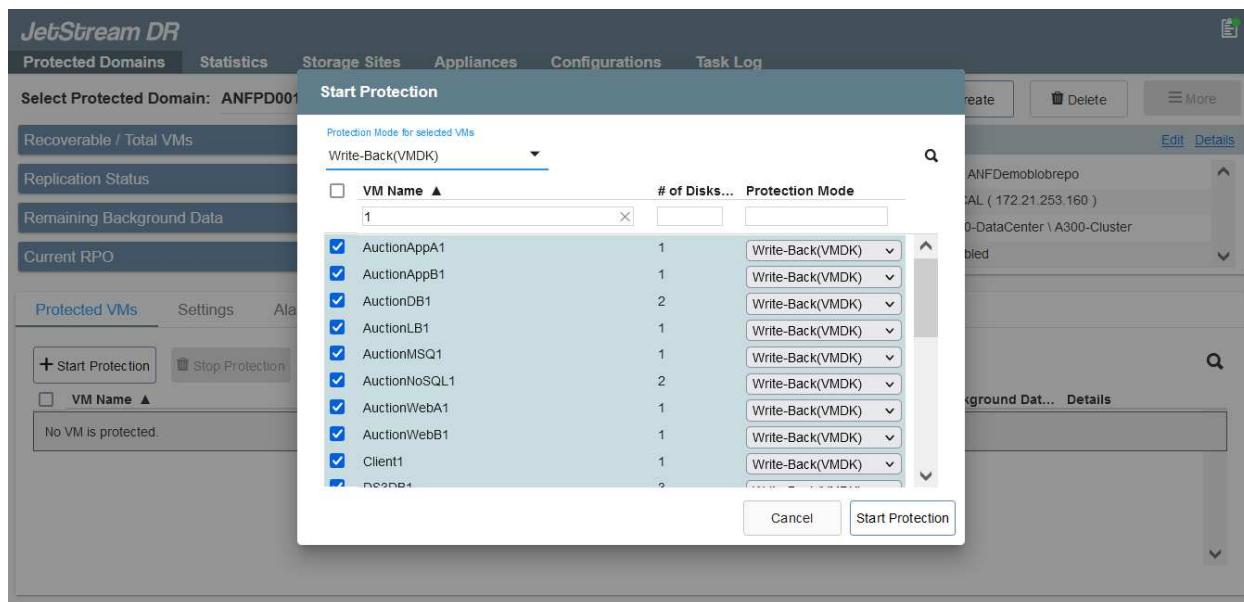
1. Create replication log volumes for each DRVA using VMDK from the datastores available or independent shared iSCSI storage pools.
2. From the Protected Domains tab, create the required number of protected domains using information about the Azure Blob Storage site, DRVA instance, and replication log. A protected domain defines a specific VM or set of VMs within the cluster that are protected together and

assigned a priority order for failover/failback operations.



3. Select VMs you want to protect and start VM protection of the protected domain. This begins data replication to the designated Blob Store.

- i Verify that the same protection mode is used for all VMs in a protected domain.
- i Write- Back(VMDK) mode can offer higher performance.



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

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

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

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

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



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

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



## Details

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 > JSR.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.

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

Command parameters

RegisterWithIp:  True

ProtectedCluster:  Cluster-1

Datastore:  vsanDatastore

VMName:  anfjval-msa

Cluster:  Cluster-1

Credential:

Username: root

Password: \*\*\*\*\*

HostName: DHCP

anfjval-msa

Network: DRSeg

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.

Cluster Name	Datacenter Name	Status	Software Version	Host Details
Cluster-1	SDDC-Datacenter	Ok	4.0.2.132	<a href="#">Details</a>

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	<a href="#">Import</a>
ANFPD001	-	20	20	<a href="#">Import</a>
ANFPD002	Protected Domain 02	20	20	<a href="#">Import</a>
ANFPD003	Protected Domain Tile 03	20	20	<a href="#">Import</a>

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.



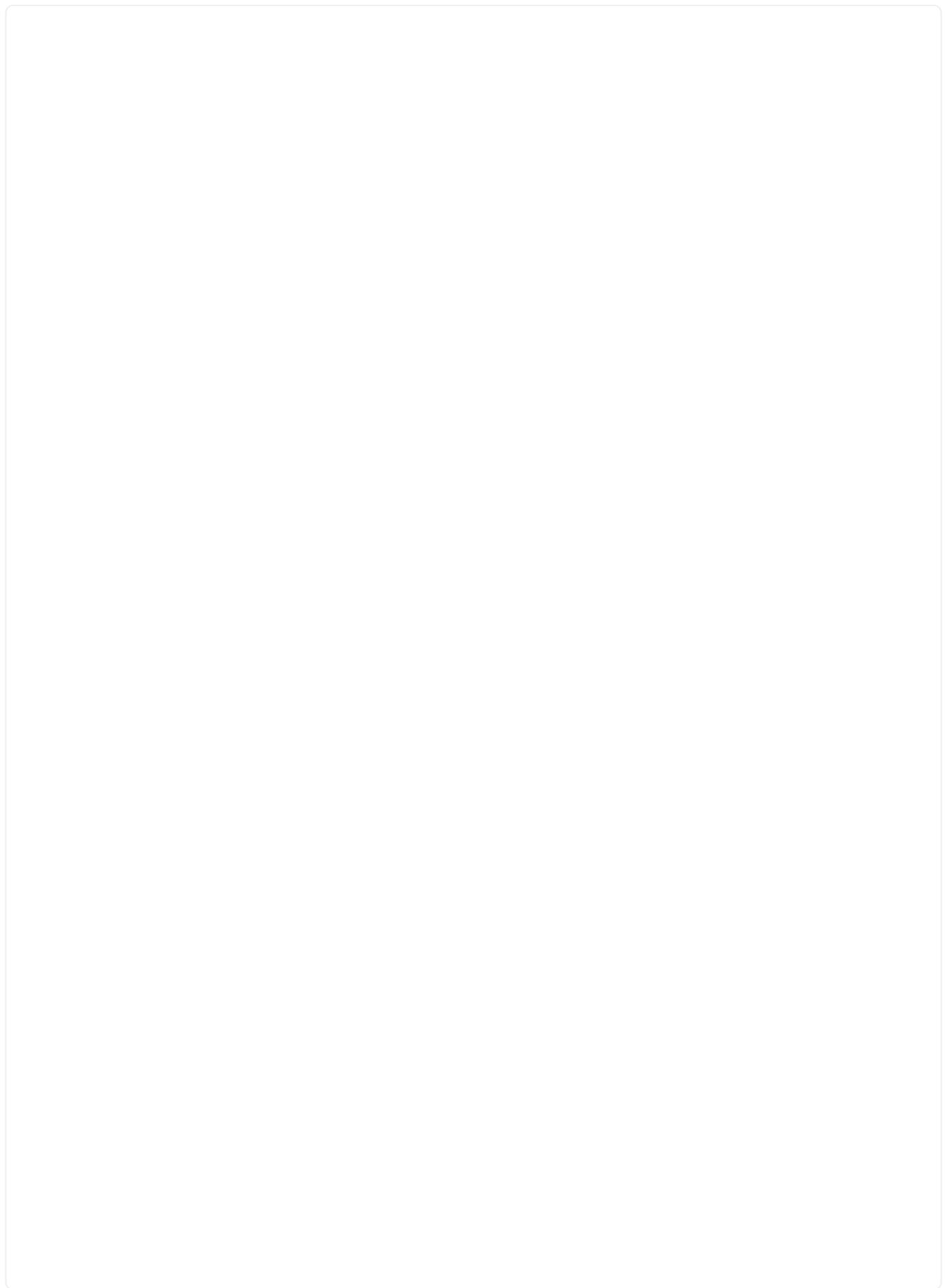
Make sure that DHCP is enabled on the selected segment and enough IPs are available. Dynamic IPs are temporarily used while domains are recovering. Each recovering VM (including continuous rehydration) requires an individual dynamic IP. After recovery is complete, the IP is released and can be reused.

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

The screenshot shows the JetStream DR web interface. The top navigation bar includes 'Protected Domains', 'Statistics', 'Storage Sites', 'Appliances', 'Configurations', and 'Task Log'. A sub-menu for 'Configurations' is open, showing 'Storage Site' and 'Owner Site' with a 'RE' icon. A context menu is displayed with options: 'Restore', 'Failover', 'Continuous Failover' (which is highlighted in grey), and 'Test Failover'. Below this, a table lists 'Protected VMs' with the following data:

VM Name	Protection Status	Protection Mode	Details
AuctionAppA0	Recoverable	Write-Back(VMDK)	<a href="#">Details</a>
AuctionAppB0	Recoverable	Write-Back(VMDK)	<a href="#">Details</a>

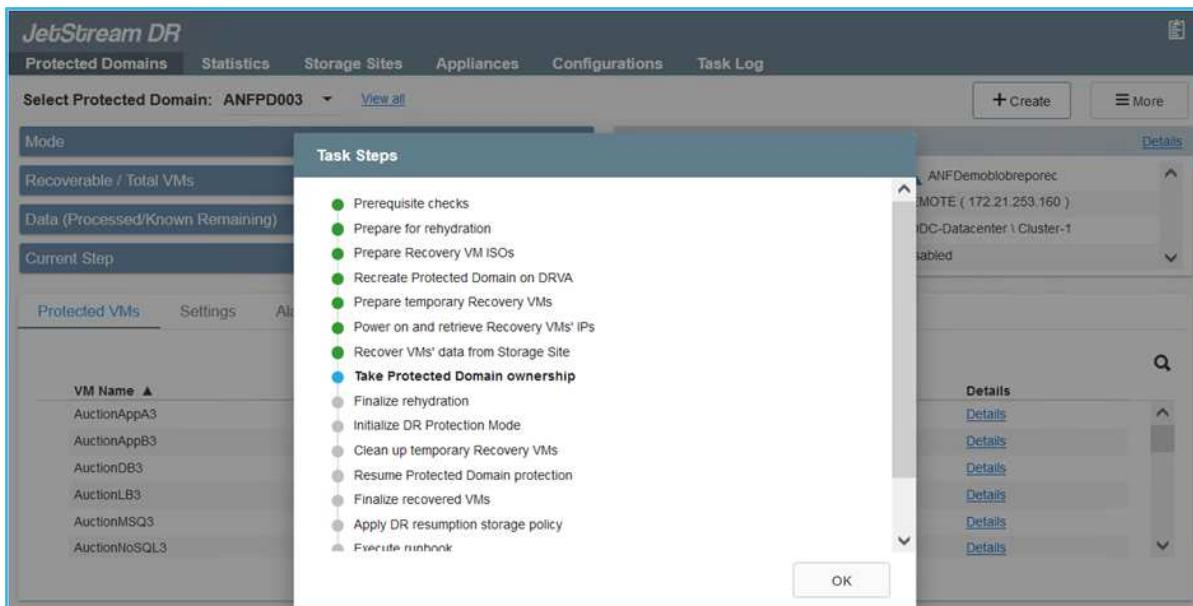
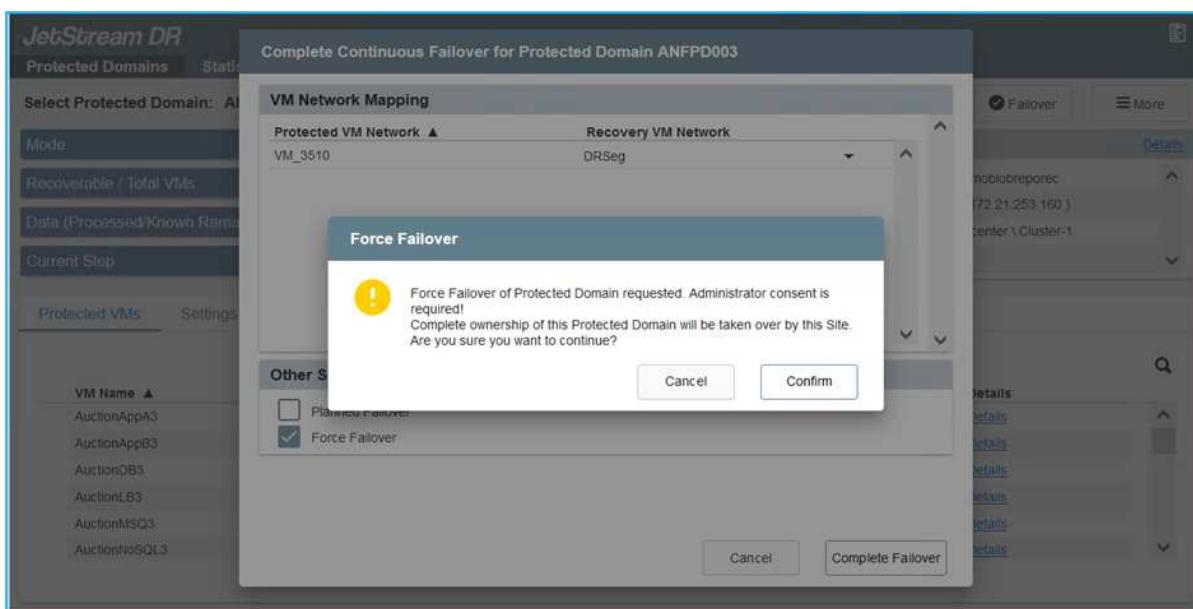
### Performing Failover / Failback



## Details

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

- i** CPT can be used to execute the failover plan to recover the VMs from Azure Blob Storage into the AVS cluster recovery site.
- i** After failover (for continuous or standard rehydration) when the protected VMs have been started in AVS, protection is automatically resumed and JetStream DR continues to replicate their data into the appropriate/original containers in Azure Blob Storage.



The task bar shows progress of failover activities.

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

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

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



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

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



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



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

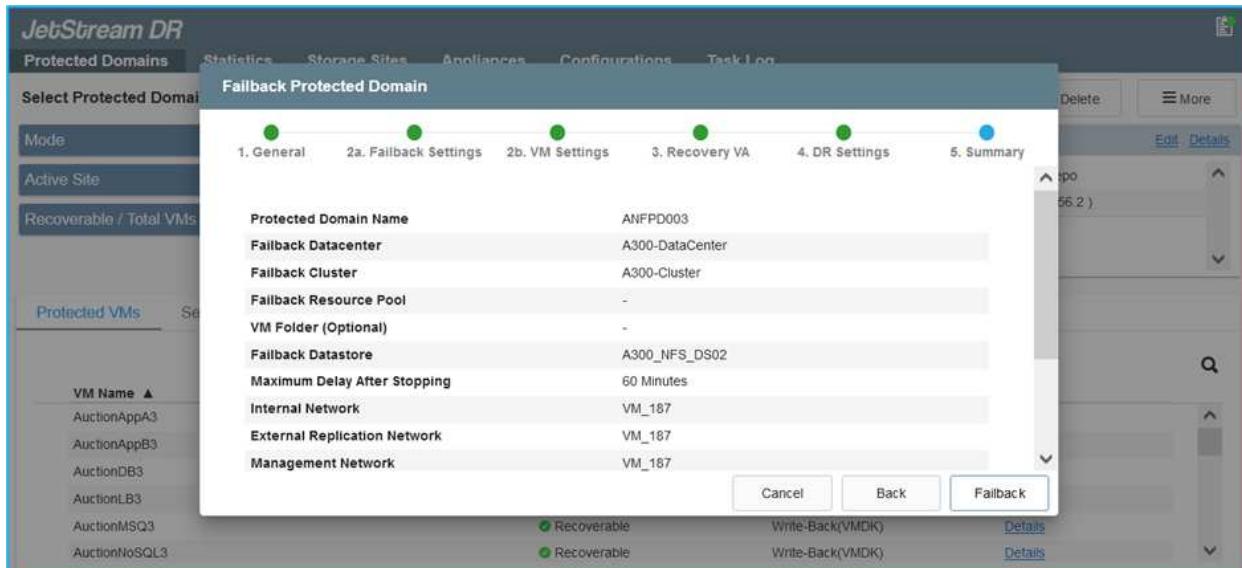
Complete the failback process, and then confirm the resumption of VM protection and data consistency.

## Ransomware Recovery

Recovering from ransomware can be a daunting task. Specifically, it can be hard for IT organizations to determine the safe point of return and, once determined, how to ensure that recovered workloads are safeguarded from the attacks reoccurring (from sleeping malware or through vulnerable applications).

### Details

JetStream DR for AVS together with Azure NetApp Files datastores can address these concerns by allowing organizations to recover from available points in time, so that workloads are recovered to a functional, isolated network if required. Recovery allows applications to function and communicate with each other while not exposing them to north- south traffic, thereby giving security teams a safe place to perform forensics and other necessary remediation.



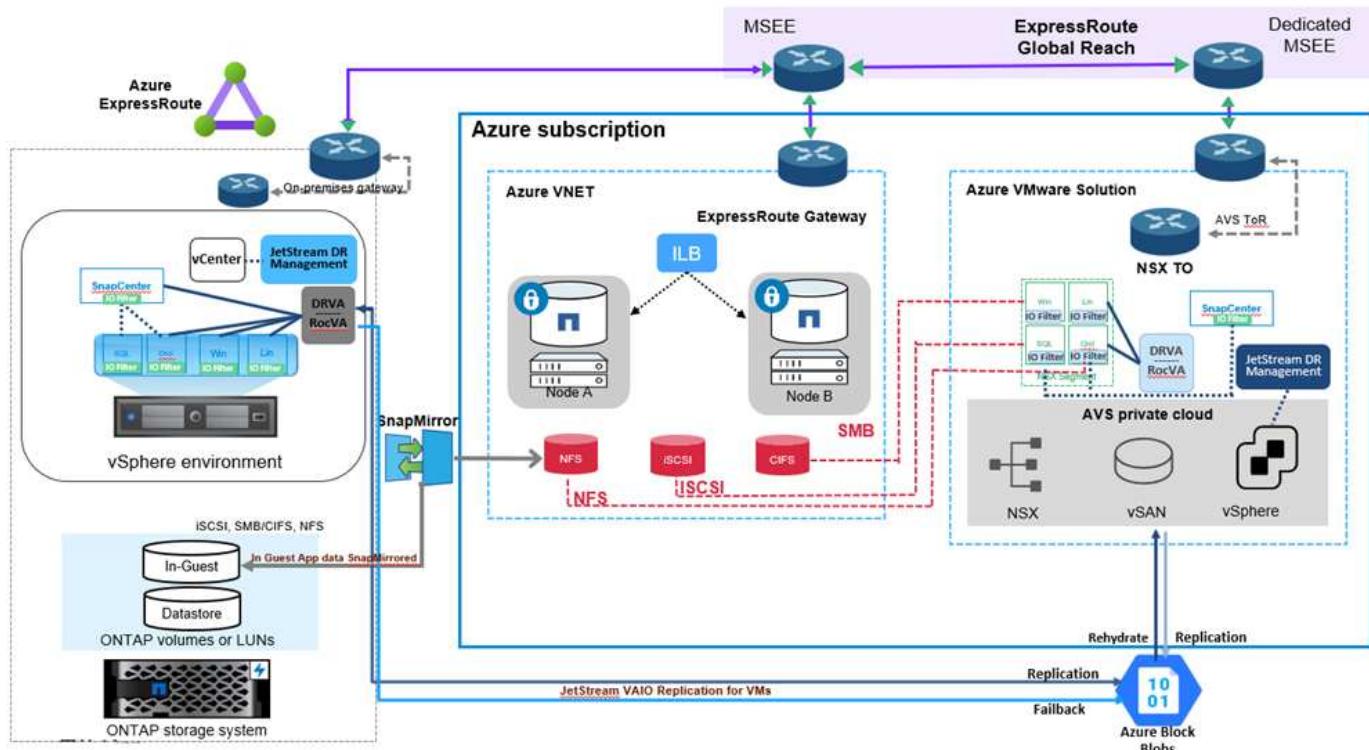
## Disaster Recovery with CVO and JetStream for AVS (guest-connected storage)

### Overview

Authors: Ravi BCB and Niyaz Mohamed, NetApp

Disaster recovery to cloud is a resilient and cost-effective way of protecting workloads against site outages and data corruption events such as ransomware. With NetApp SnapMirror, on-premises VMware workloads that use guest-connected storage can be replicated to NetApp Cloud Volumes ONTAP running in Azure. This covers application data; however, what about the actual VMs themselves. Disaster recovery should cover all dependent components, including virtual machines, VMDKs, application data, and more. To accomplish this, SnapMirror along with Jetstream can be used to seamlessly recover workloads replicated from on-premises to Cloud Volumes ONTAP while using vSAN storage for VM VMDKs.

This document provides a step-by-step approach for setting up and performing disaster recovery that uses NetApp SnapMirror, JetStream, and the Azure VMware Solution (AVS).



## Assumptions

This document focuses on in-guest storage for application data (also known as guest connected), and we assume that the on-premises environment is using SnapCenter for application-consistent backups.

**Info:** 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.

**Info:** There are multiple options for connecting on-premises datacenters to Azure, which prevents us from outlining a specific workflow in this document. Refer to the Azure documentation for the appropriate on-premises-to-Azure connectivity method.

## Deploying the DR Solution

### Solution Deployment Overview

1. Make sure that application data is backed up using SnapCenter with the necessary RPO requirements.
2. Provision Cloud Volumes ONTAP with the correct instance size using Cloud manager within the appropriate subscription and virtual network.
  - a. Configure SnapMirror for the relevant application volumes.
  - b. Update the backup policies in SnapCenter to trigger SnapMirror updates after the scheduled jobs.
3. Install the JetStream DR software in the on-premises data center and start protection for virtual machines.
4. Install JetStream DR software in the Azure VMware Solution private cloud.
5. During a disaster event, break the SnapMirror relationship using Cloud Manager and trigger failover of virtual machines to Azure NetApp Files or to vSAN datastores in the designated AVS DR site.
  - a. Reconnect the iSCSI LUNs and NFS mounts for the application VMs.
6. Invoke failback to the protected site by reverse resyncing SnapMirror after the primary site has been recovered.

### Deployment Details

#### Configure CVO on Azure and replicate volumes to CVO

The first step is to configure Cloud Volumes ONTAP on Azure ([Link](#)) and replicate the desired volumes to Cloud Volumes ONTAP with the desired frequencies and snapshot retentions.

Health Status	Source Volume	Target Volume	Total Transfer Time	Status	Mirror State	Last Successful Transfer	...
✓	gcsdrsqldb_sc46_ntaphci-a300e9u25	gcsdrsqldb_sc46_copy_ANFCVODRDemo	17 seconds	idle	snapmirrored	May 6, 2022, 11:43:18 AM 105.06 KiB	...
✓	gcsdrsqlhld_sc46_copy_ANFCVODRDemo	gcsdrsqlhld_sc46_ntaphci-a300e9u25	7 seconds	idle	snapmirrored	May 6, 2022, 11:42:20 AM 7.22 MiB	...
✓	gcsdrsqllog_sc46_ntaphci-a300e9u25	gcsdrsqllog_sc46_copy_ANFCVODRDemo	16 seconds	idle	snapmirrored	May 6, 2022, 11:43:52 AM 130.69 KiB	...

## Configure AVS hosts and CVO data access

Two important factors to consider when deploying the SDDC are the size of the SDDC cluster in the Azure VMware solution and how long to keep the SDDC in service. These two key considerations for a disaster recovery solution help reduce the overall operational costs. The SDDC can be as small as three hosts, all the way up to a multi-host cluster in a full-scale deployment.

The decision to deploy an AVS cluster is primarily based on the RPO/RTO requirements. With the Azure VMware solution, the SDDC can be provisioned just in time in preparation for either testing or an actual disaster event. An SDDC deployed just in time saves on ESXi host costs when you are not dealing with a disaster. However, this form of deployment affects the RTO by a few of hours while SDDC is being provisioned.

The most common deployed option is to have SDDC running in an always-on, pilot-light mode of operation. This option provides a small footprint of three hosts that are always available, and it also speeds up recovery operations by providing a running baseline for simulation activities and compliance checks, thus avoiding the risk of operational drift between the production and DR sites. The pilot-light cluster can be scaled up quickly to the desired level when needed to handle an actual DR event.

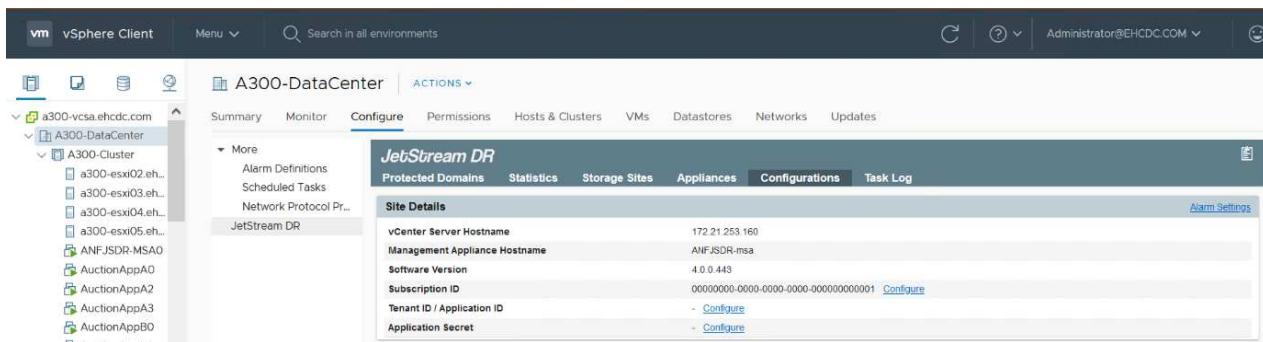
To configure AVS SDDC (be it on-demand or in pilot-light mode), see [Deploy and configure the Virtualization Environment on Azure](#). As a prerequisite, verify that the guest VMs residing on the AVS hosts are able to consume data from Cloud Volumes ONTAP after connectivity has been established.

After Cloud Volumes ONTAP and AVS have been configured properly, begin configuring Jetstream to automate the recovery of on-premises workloads to AVS (VMs with application VMDKs and VMs with in-guest storage) by using the VAIO mechanism and by leveraging SnapMirror for application volumes copies to Cloud Volumes ONTAP.

## Install JetStream DR in on-premises datacenter

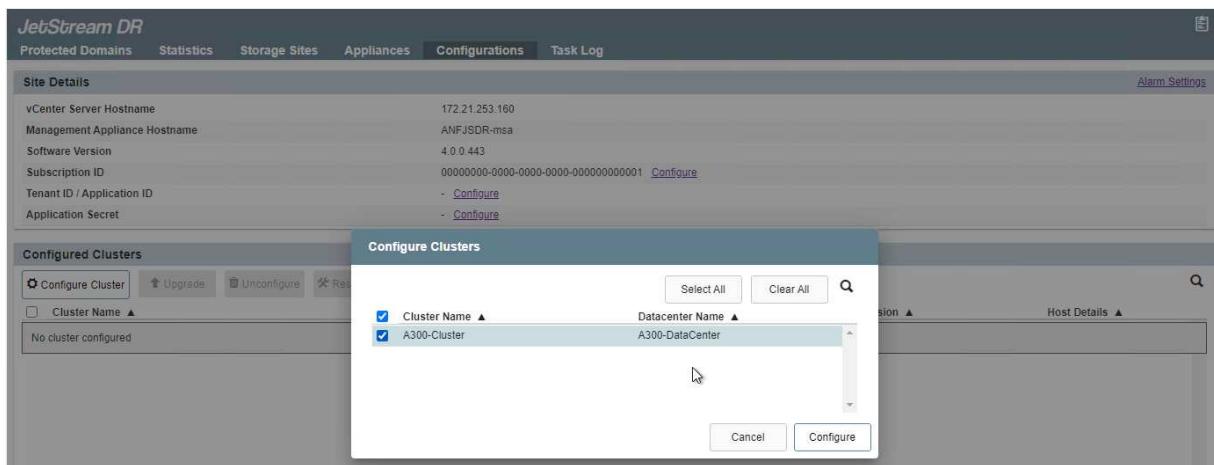
JetStream DR software consists of three major components: the JetStream DR Management Server Virtual Appliance (MSA), the DR Virtual Appliance (DRVA), and host components (I/O filter packages). The MSA is used to install and configure host components on the compute cluster and then to administer JetStream DR software. The installation process is as follows:

1. Check the prerequisites.
2. Run the Capacity Planning Tool for resource and configuration recommendations.
3. Deploy the JetStream DR MSA to each vSphere host in the designated cluster.
4. Launch the MSA using its DNS name in a browser.
5. Register the vCenter server with the MSA.
6. After JetStream DR MSA has been deployed and the vCenter Server has been registered, navigate to the JetStream DR plug-in with the vSphere Web Client. This can be done by navigating to Datacenter > Configure > JetStream DR.

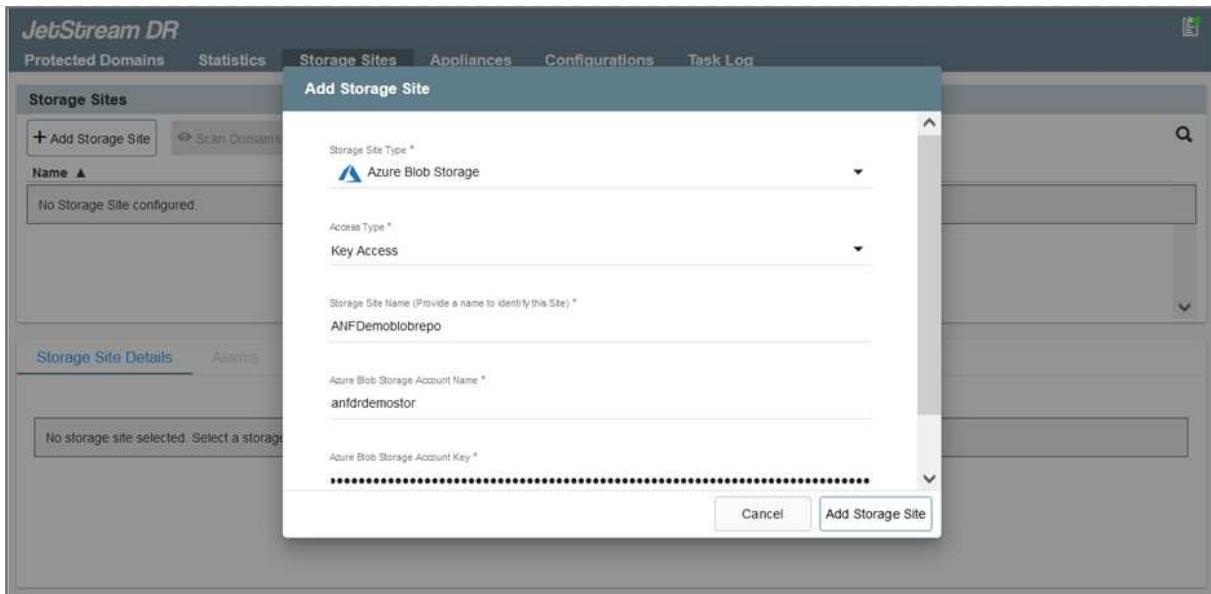


7. From the JetStream DR interface, complete the following tasks:

- a. Configure the cluster with the I/O filter package.



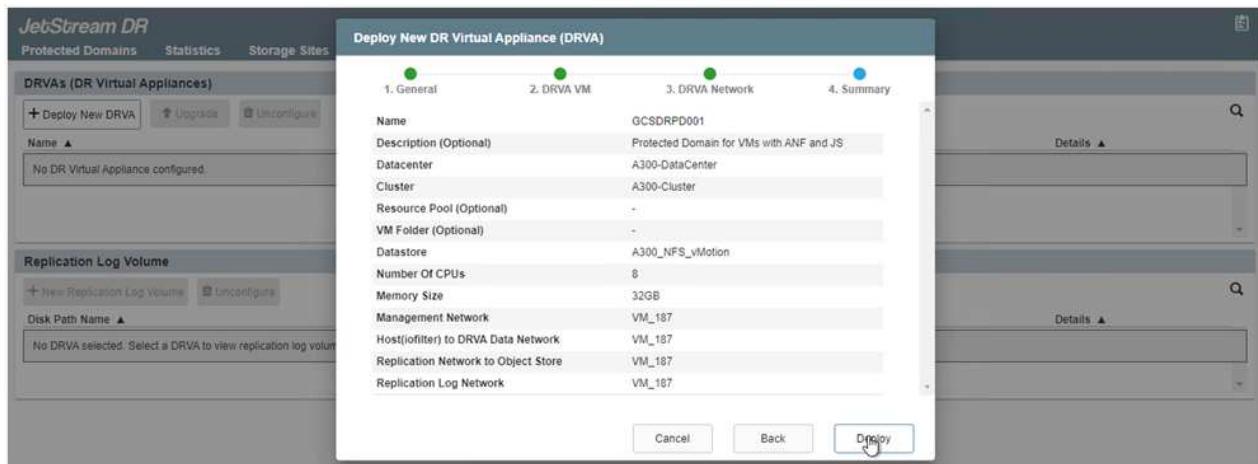
- b. Add the Azure Blob storage located at the recovery site.



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



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



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

The screenshot shows the JetStream DR interface with the following sections:

- DRVAs (DR Virtual Appliances):** A table with columns: Name, Status, Child Alarm, Software Version, and Details. One entry is shown: GCSDRPD001, Status: Running, Child Alarm: 0, Software Version: 4.0.0.134, Details: [link].
- Replication Log Volume:** A table with columns: Disk Path Name, Status, Child Alarm, Size (available/total), and Details. One entry is shown: /dev/sdb, Status: Ok, Child Alarm: 0, Size: 179.88 GB / 200 GB, Details: [link].
- Replication Log Volume Details:** A detailed view of the replication log volume, showing its configuration and status.

- 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.

The screenshot shows the 'Create Protected Domain' dialog box in Step 1: General. The fields are as follows:

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
Replication Log Size	400GB

The screenshot shows the 'Create Protected Domain' dialog box in Step 2: Primary Site. The fields are as follows:

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

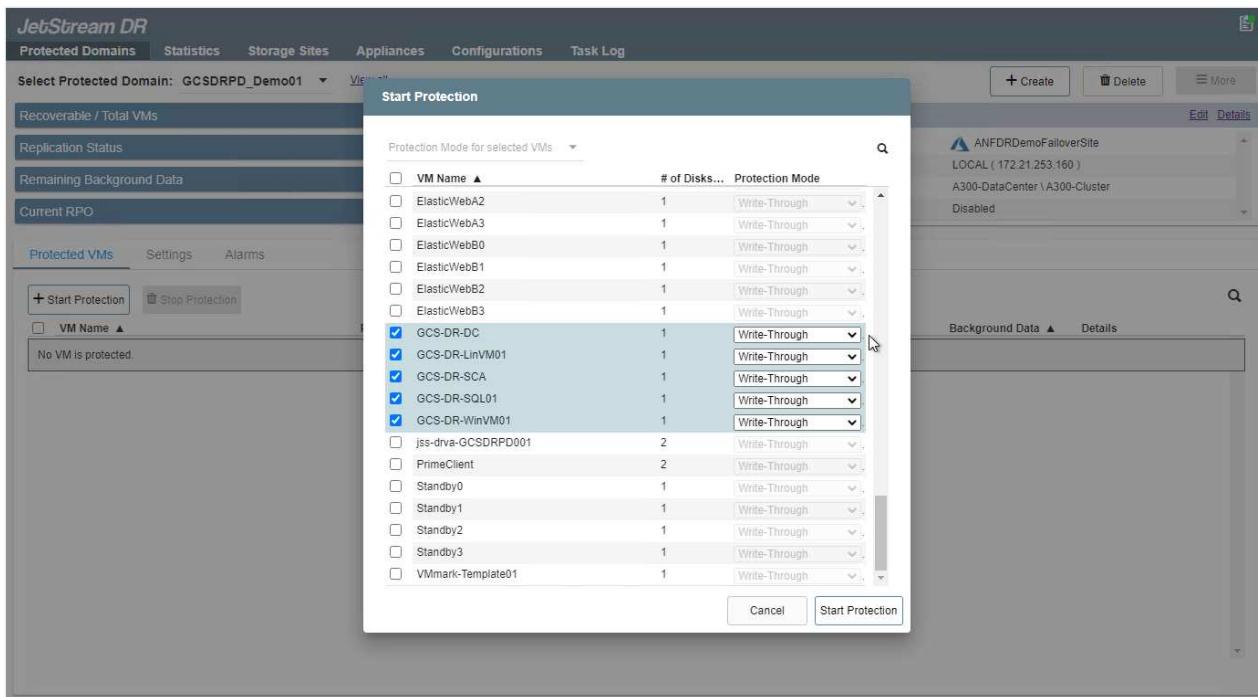
- Select the VMs to be protected and group the VMs into applications groups based on dependency. Application definitions allow you to group sets of VMs into logical groups that contain their boot orders, boot delays, and optional application validations that can be executed upon recovery.



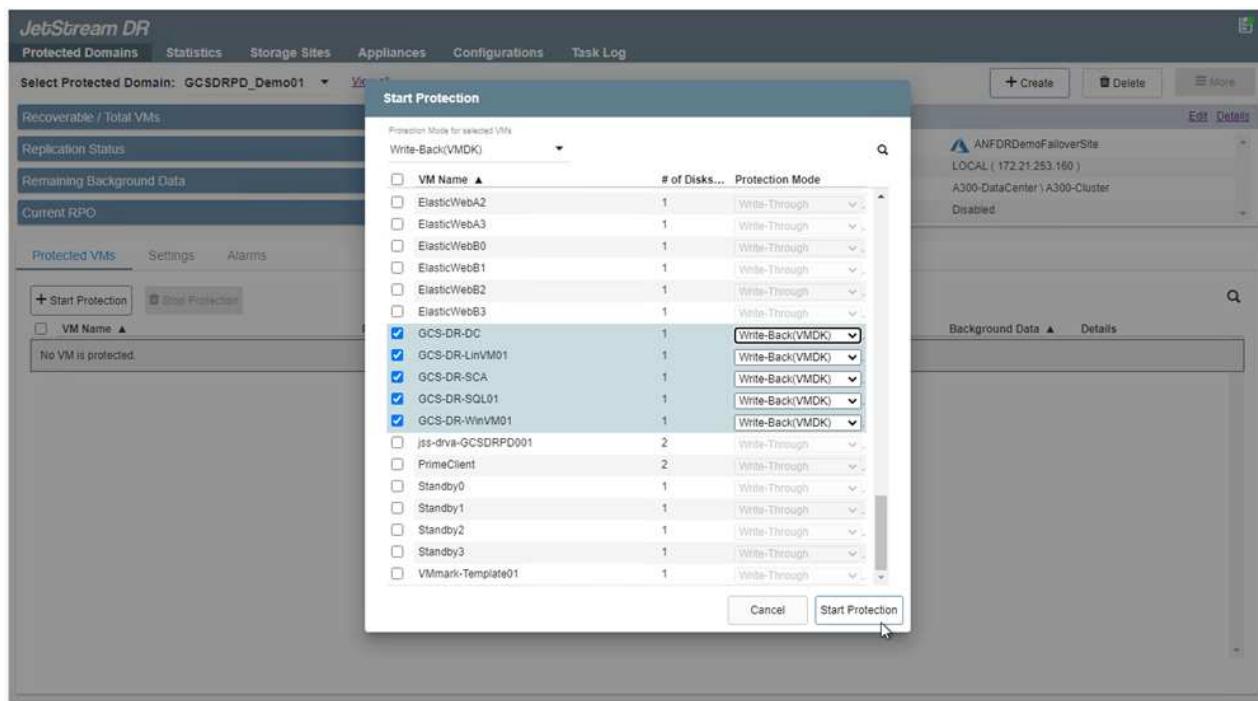
Make sure that the same protection mode is used for all VMs in a protected domain.



Write-Back(VMDK) mode offers higher performance.



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



13. After you are done, click Start Protection for the protected domain. This starts data replication for the selected VMs to the designated Blob store.

Protected Domains Statistics Storage Sites Appliances Configurations Task Log

Select Protected Domain: GCSDRPD\_Demo01 View all

Recoverable / Total VMs 0 / 5

Replication Status OK

Remaining Background Data 0 B

Current RPO

Protected VMs Settings Alarms

+ Start Protection Stop Protection

VM Name	Protection Status	Replication Status	Protection Mode	Background Data	Details
GCS-DR-DC	Initializing	-	Write-Back(VMDK)	-	<a href="#">Details</a>
GCS-DR-LinVM01	Initializing	-	Write-Back(VMDK)	-	<a href="#">Details</a>
GCS-DR-SCA	Initializing	-	Write-Back(VMDK)	-	<a href="#">Details</a>
GCS-DR-SQL01	Initializing	-	Write-Back(VMDK)	-	<a href="#">Details</a>
GCS-DR-WinVM01	Initializing	-	Write-Back(VMDK)	-	<a href="#">Details</a>

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

Protected Domains Statistics Storage Sites Appliances Configurations Task Log

Select Protected Domain: GCSDRPD\_Demo01 View all

Recoverable / Total VMs 5 / 5

Replication Status OK

Remaining Background Data 0 B

Current RPO 0s

Protected VMs Settings Alarms

+ Start Protection Stop Protection

VM Name	Protection Status	Replication Status	Protection Mode	Background Data	Details
GCS-DR-DC	Recoverable	OK	Write-Back(VMDK)	0 B	<a href="#">Details</a>
GCS-DR-LinVM01	Recoverable	OK	Write-Back(VMDK)	0 B	<a href="#">Details</a>
GCS-DR-SCA	Recoverable	OK	Write-Back(VMDK)	0 B	<a href="#">Details</a>
GCS-DR-SQL01	Recoverable	OK	Write-Back(VMDK)	0 B	<a href="#">Details</a>
GCS-DR-WinVM01	Recoverable	OK	Write-Back(VMDK)	0 B	<a href="#">Details</a>



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

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

Protected Domains Statistics Storage Sites Appliances Configurations Task Log

Select Protected Domain: GCSDRPD\_Demo01 View all

Recoverable / Total VMs 5 / 5

Replication Status OK

Remaining Background Data 0 B

Current RPO 0s

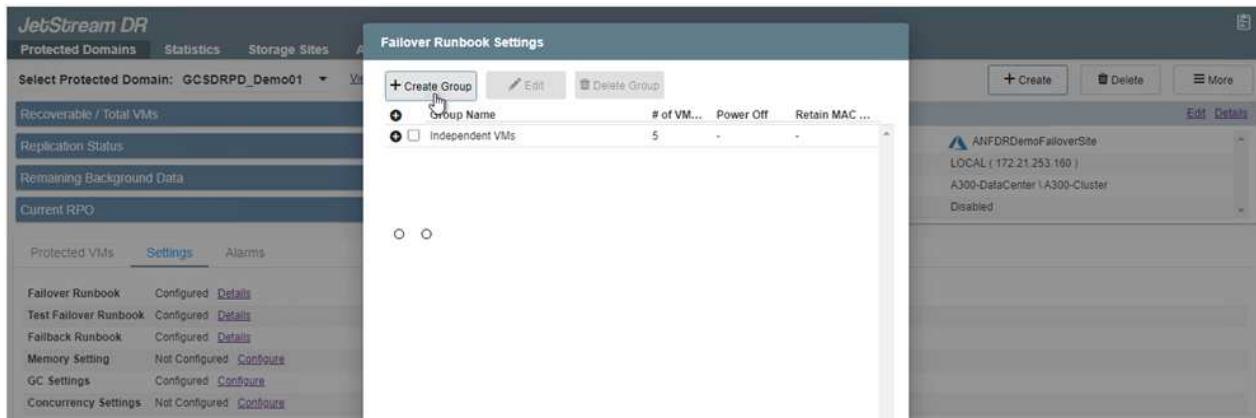
Protected VMs Settings Alarms

Failover Runbook	Not Configured	<a href="#">Configure</a>
Test Failover Runbook	Not Configured	<a href="#">Configure</a>
Fallback Runbook	Not Configured	<a href="#">Configure</a>
Memory Setting	Not Configured	<a href="#">Configure</a>
GC Settings	Configured	<a href="#">Configure</a>
Concurrency Settings	Not Configured	<a href="#">Configure</a>

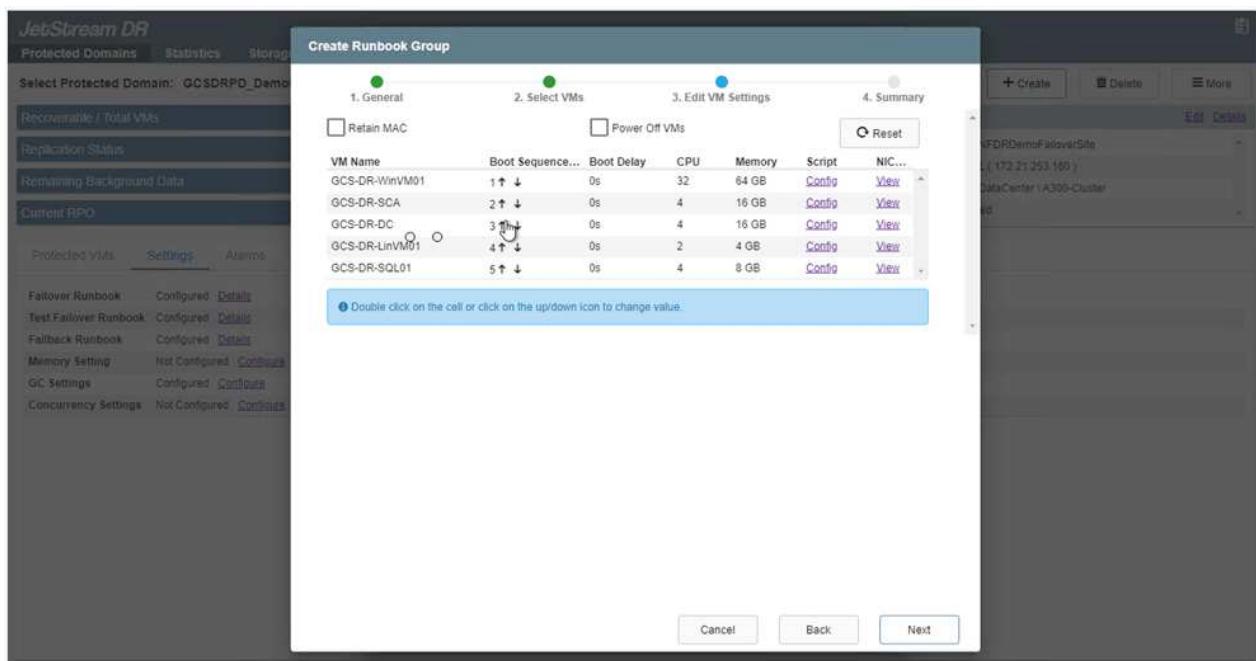
16. Click the Create Group button to begin creating a new runbook group.



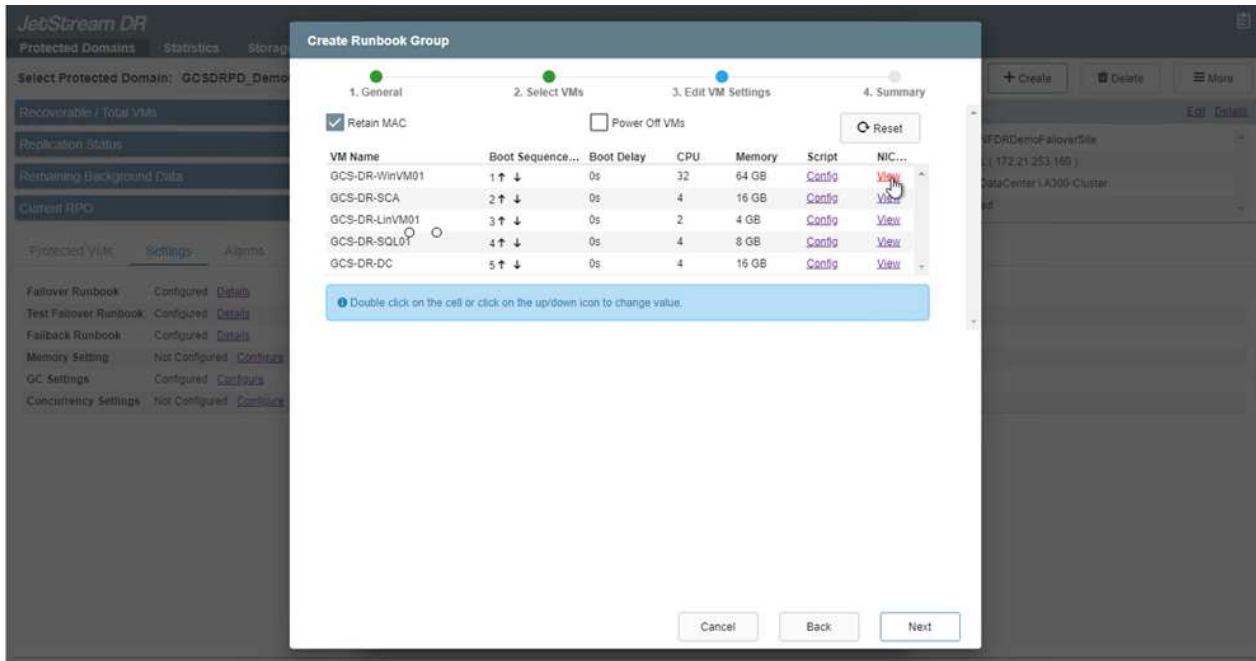
If needed, in the lower portion of the screen, apply custom pre-scripts and post-scripts to automatically run prior to and following operation of the runbook group. Make sure that the Runbook scripts are residing on the management server.



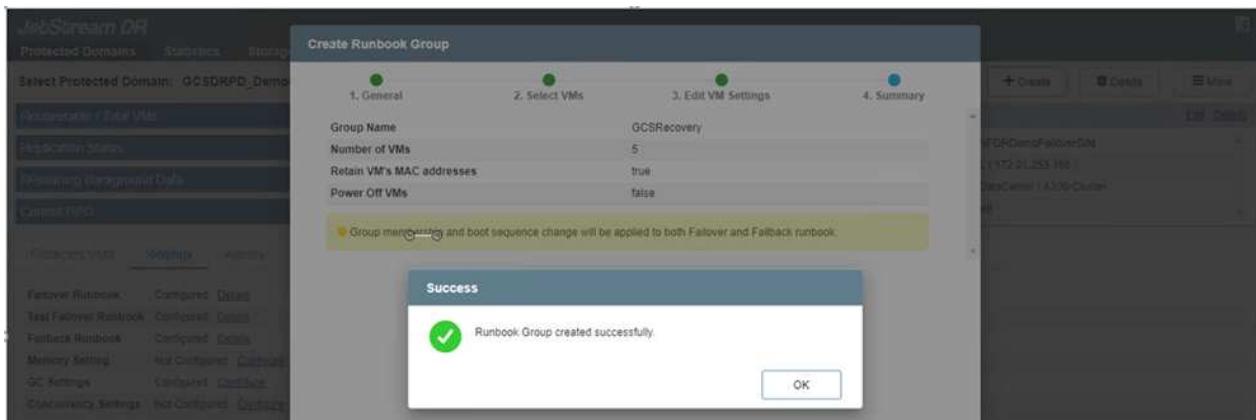
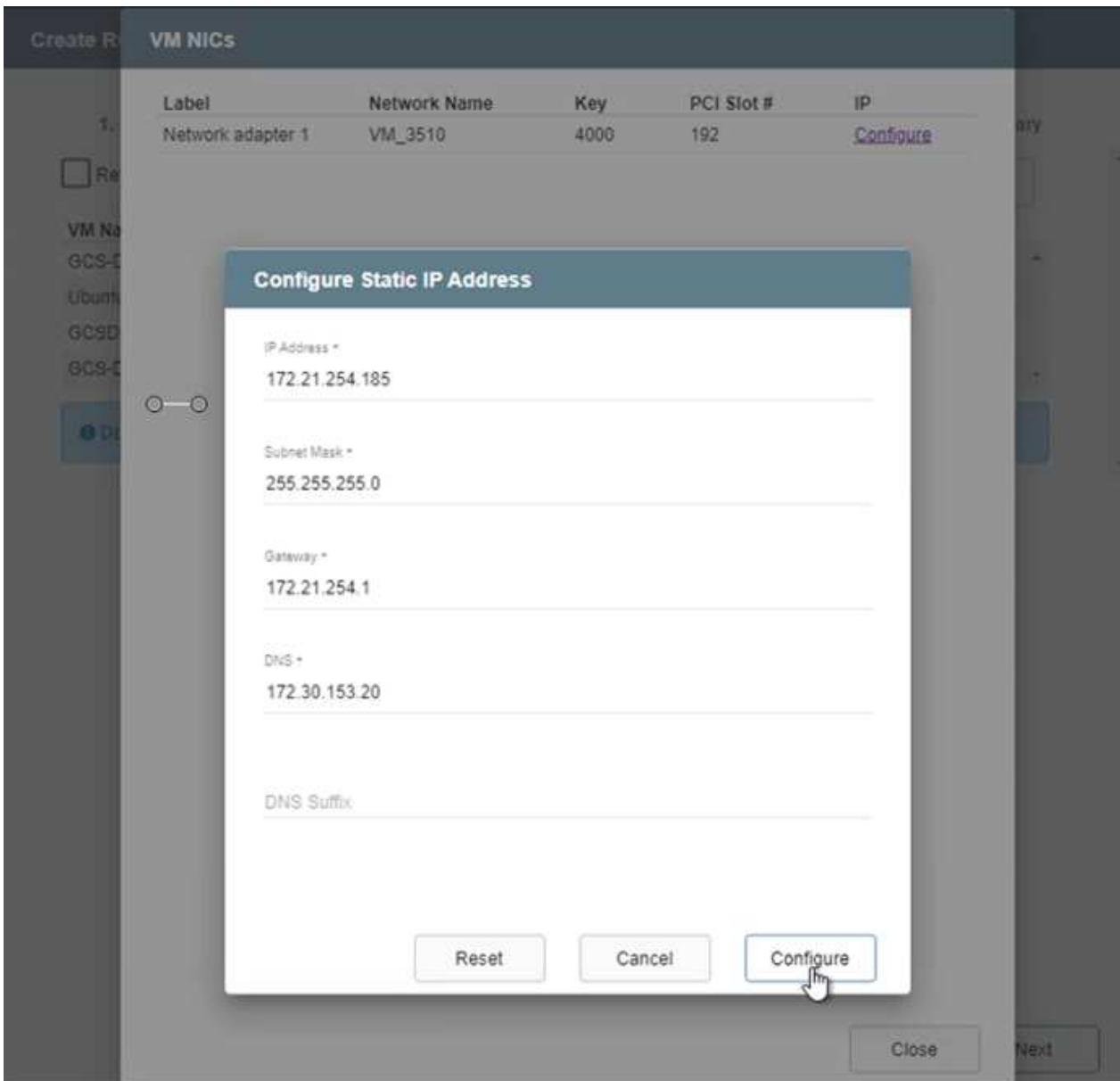
17. Edit the VM settings as required. Specify the parameters for recovering the VMs, including the boot sequence, the boot delay (specified in seconds), the number of CPUs, and the amount of memory to allocate. Change the boot sequence of the VMs by clicking the up or down arrows. Options are also provided to Retain MAC.



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



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



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

## Install JetStream DR for AVS in private cloud

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

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

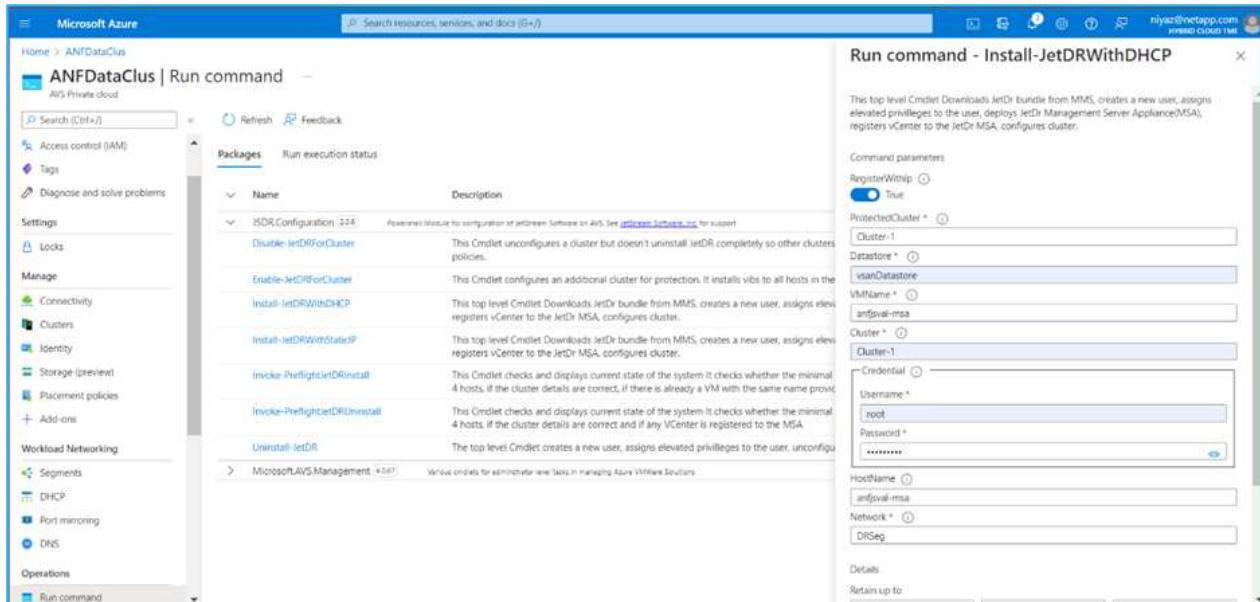
JetStream DR supports a near-zero RTO mode for mission-critical domains. For these domains, destination storage should be preinstalled. ANF is a recommended storage type in this case.

- i Network configuration including segment creation should be configured on the AVS cluster to match on-premises requirements.
- i Depending on the SLA and RTO requirements, you can use continuous failover or regular (standard) failover mode. For near-zero RTO, you should start continuous rehydration at the recovery site.

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

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

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



2. After JetStream DR for AVS installation is complete, refresh the browser. To access the JetStream DR UI, go to SDDC Datacenter > Configure > JetStream DR.

## JetStream DR

Protected Domains   Statistics   Storage Sites   Appliances   Configurations   Task Log

### Site Details

[Alarm Settings](#)

vCenter Server Hostname 172.30.156.2

Management Appliance Hostname anfjsval-msa

Software Version 4.0.2.450

Subscription ID - [Configure](#)

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

Application Secret - [Configure](#)

[Configure Cluster](#)

[Upgrade](#)

[Unconfigure](#)

[Resolve Configure Issue](#)



Cluster Name ▲

Datacenter Name ▲

Status ▲

Software Version ▲

Host Details ▲

Cluster-1

SDDC-Datacenter

Ok

4.0.2.132

[Details](#)

3. From the JetStream DR interface, complete the following tasks:

- 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.
- In the pop-up dialog window that appears, select the protected domain to import and then click its Import link.

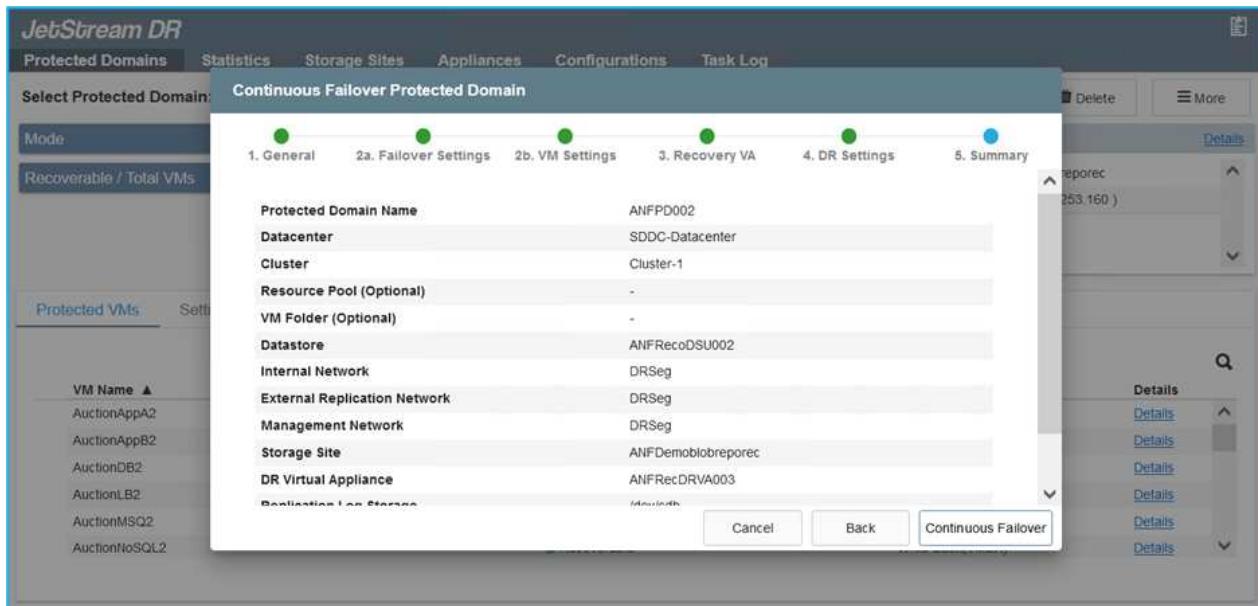
4. The domain is imported for recovery. Go to the Protected Domains tab and verify that the intended domain has been selected or choose the desired one from the Select Protected Domain menu. A list of the recoverable VMs in the protected domain is displayed.

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



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

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

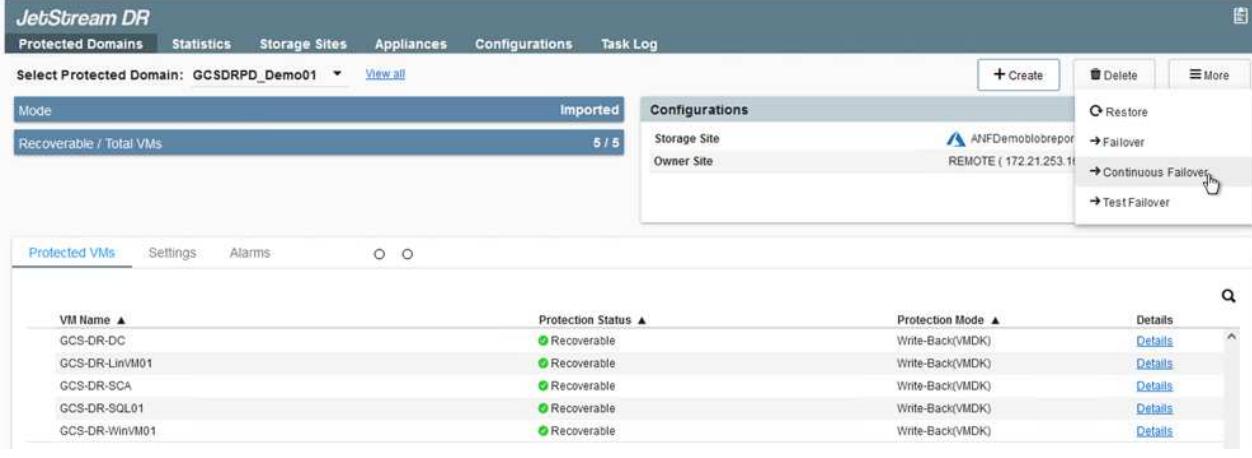


Make sure that DHCP is enabled on the selected segment and that enough IPs are available. Dynamic IPs are temporarily used while domains are recovering. Each recovering VM (including continuous rehydration) requires an individual dynamic IP. After recovery is complete, the IP is released and can be reused.

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).



The screenshot shows the JetStream DR software interface. At the top, there is a navigation bar with tabs: Protected Domains, Statistics, Storage Sites, Appliances, Configurations, and Task Log. The 'Protected Domains' tab is selected, showing a dropdown menu with 'GCSDRPD\_Demo01' and a 'View all' link. Below this, there is a table with a single row: 'Mode' (Imported), 'Recoverable / Total VMs' (5 / 5), and a 'Configurations' section with 'Storage Site' (ANFDemoblobrepo) and 'Owner Site' (REMOTE (172.21.253.1)). A context menu is open over the 'Configurations' section, with 'Continuous Failover' highlighted. The main content area shows a table of 'Protected VMs' with columns: VM Name, Protection Status, Protection Mode, and Details. The table lists five VMs: GCS-DR-DC, GCS-DR-LinVM01, GCS-DR-SCA, GCS-DR-SQL01, and GCS-DR-WinVM01, all in 'Recoverable' status and 'Write-Back(VMDD)' mode.

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.

Health Status	Source Volume	Target Volume	Total Transfer Time	Status	Mirror State	Last Successful Transfer
Green	gcsdrsqldb_sc46_ntaphci-a300e9u25	gcsdrsqldb_sc46_copy_ANFCVODRDemo	6 minutes 41 seconds	idle	snapmirrored	May 5, 2022, 12:08:34 PM 33.66 KB
Green	gcsdrsqlhld_sc46_ntaphci-a300e9u25	gcsdrsqlhld_sc46_copy_ANFCVODRDemo	4 minutes 56 seconds	idle	snapmirrored	Information
Green	gcsdrsqllog_sc46_ntaphci-a300e9u25	gcsdrsqllog_sc46_copy_ANFCVODRDemo	10 minutes 18 seconds	idle	snapmirrored	Break Reverse Resync Edit Schedule Edit Max Transfer Rate Update Delete

Health Status	Source Volume	Target Volume	Total Transfer Time	Status	Mirror State	Last Successful Transfer
Green	gcsdrsqldb_sc46_ntaphci-a300e9u25	gcsdrsqldb_sc46_copy_ANFCVODRDemo	6 minutes 41 seconds	idle	snapmirrored	May 5, 2022, 12:08:34 PM 33.66 KB
Green	gcsdrsqlhld_sc46_ntaphci-a300e9u25	gcsdrsqlhld_sc46_copy_ANFCVODRDemo	4 minutes 56 seconds	idle	snapmirrored	May 5, 2022, 12:09:15 PM 69.84 KB
Green	gcsdrsqllog_sc46_ntaphci-a300e9u25	gcsdrsqllog_sc46_copy_ANFCVODRDemo	10 minutes 18 seconds	idle	snapmirrored	May 5, 2022, 12:08:34 PM 104.34 KB



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

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

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

**JetStream DR**

Protected Domains Statistics Storage Sites Appliances Configurations Task Log

Select Protected Domain: GCSDRPD\_Demo01 [View all](#)

Mode: Continuous Rehydration in Progress 4 / 4

Recoverable / Total VMs: 4 / 4

Data (Processed/Known Remaining): 329.01 GB / 6.19 GB

Current Step: Recover VMs' data from Storage Site

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

**Configurations**

Storage Site	ANFDemobilobrerec
Owner Site	REMOTE ( 172.21.253.160 )
Datacenter / Cluster	SDDC-Datacenter / Cluster-1
Point-in-time Recovery	Disabled

**Protected VMs**

VM Name	Protection Status	Protection Mode	Details
GCS-DR-DC	Recoverable	Write-Back(VMDK)	<a href="#">Details</a>
GCS-DR-LinVM01	Recoverable	Write-Back(VMDK)	<a href="#">Details</a>
GCS-DR-SCA	Recoverable	Write-Back(VMDK)	<a href="#">Details</a>
GCS-DR-SQL01	Recoverable	Write-Back(VMDK)	<a href="#">Details</a>
GCS-DR-WinVM01	Recoverable	Write-Back(VMDK)	<a href="#">Details</a>

**Complete Continuous Failover for Protected Domain**

**VM Network Mapping**

Protected VM Network	Recovery VM Network
VM_3510	DRStretchSeg

**Other Settings**

Planned Failover

Force Failover

Some VMs' guest credential are required because of network configuration: [Configure](#)

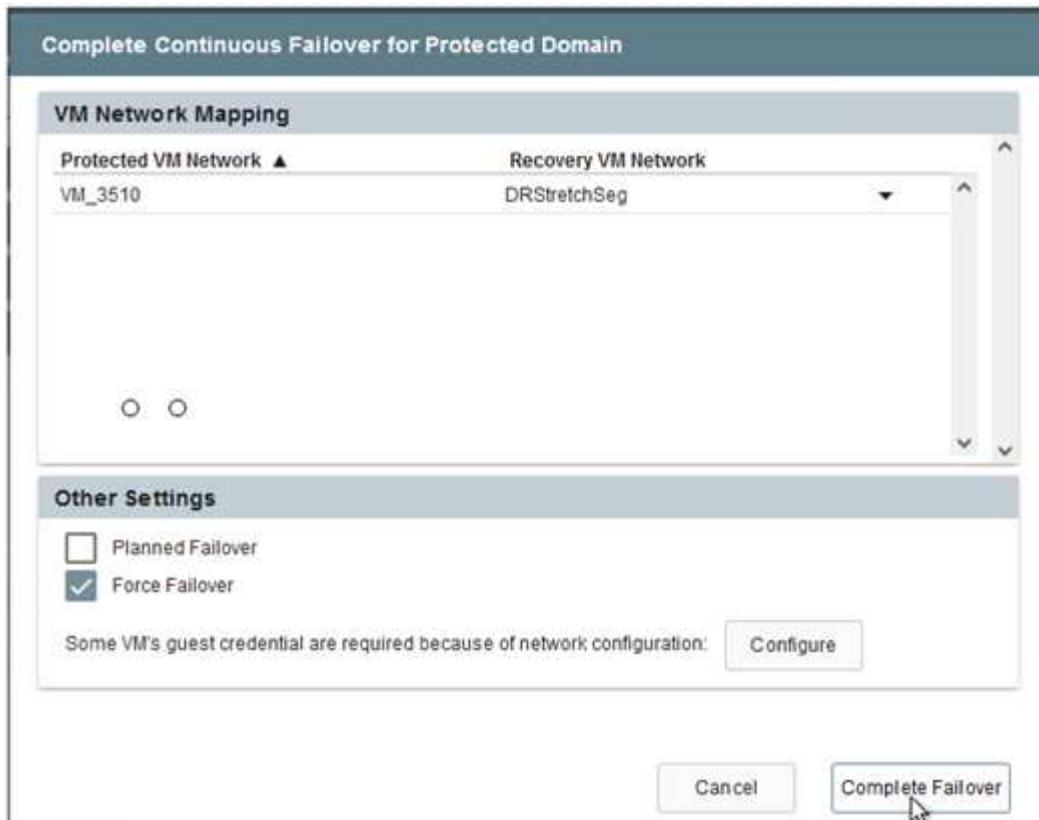
[Cancel](#) [Complete Failover](#)

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

**Force Failover**

**!** Force Failover of Protected Domain requested. Administrator consent is required!  
Complete ownership of this Protected Domain will be taken over by this Site.  
Are you sure you want to continue?

[Cancel](#) [Confirm](#)



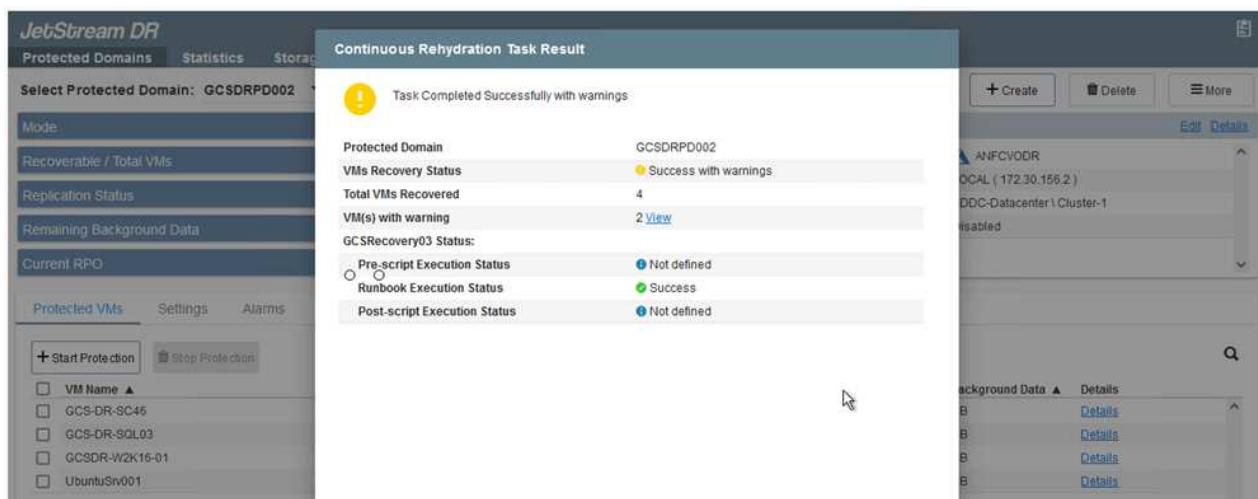
3. After continuous failover is complete, a message appears confirming completion of the task. When the task is complete, access the recovered VMs to configure iSCSI or NFS sessions.



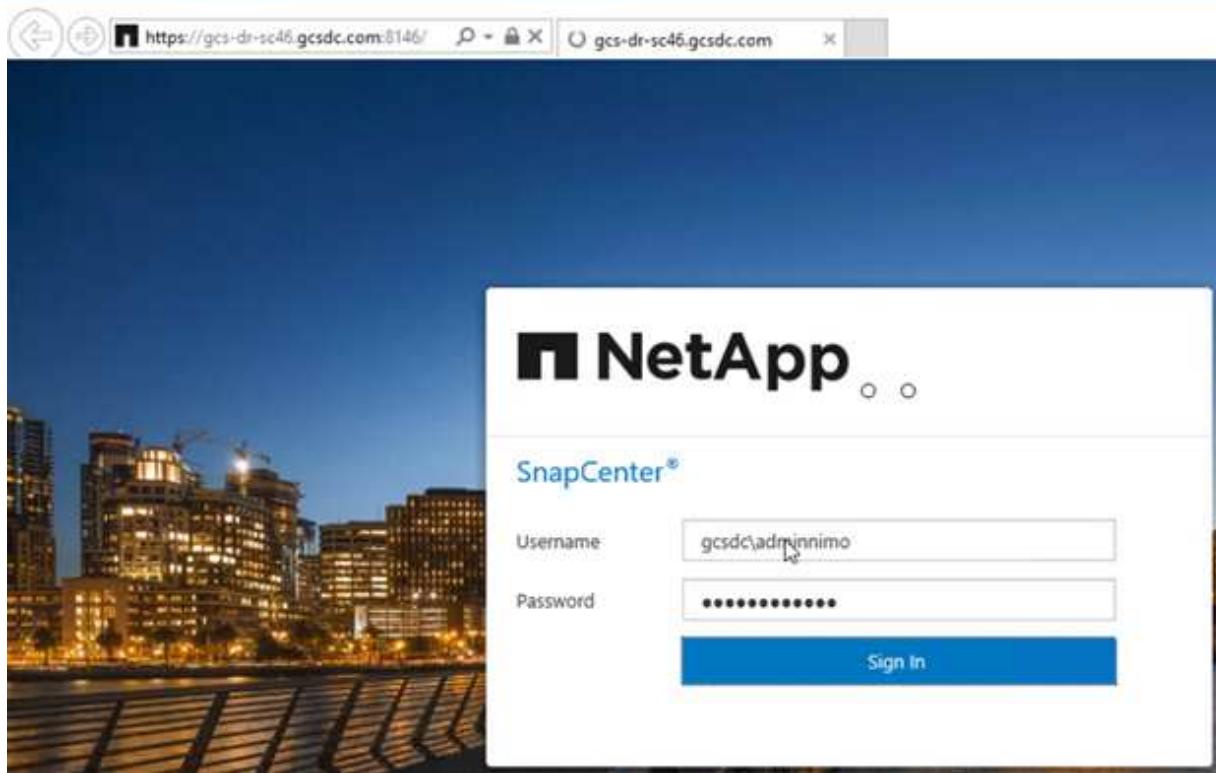
The failover mode changes to Running in Failover and the VM status is Recoverable. All the VMs of the protected domain are now running at the recovery site in the state specified by the failover runbook settings.



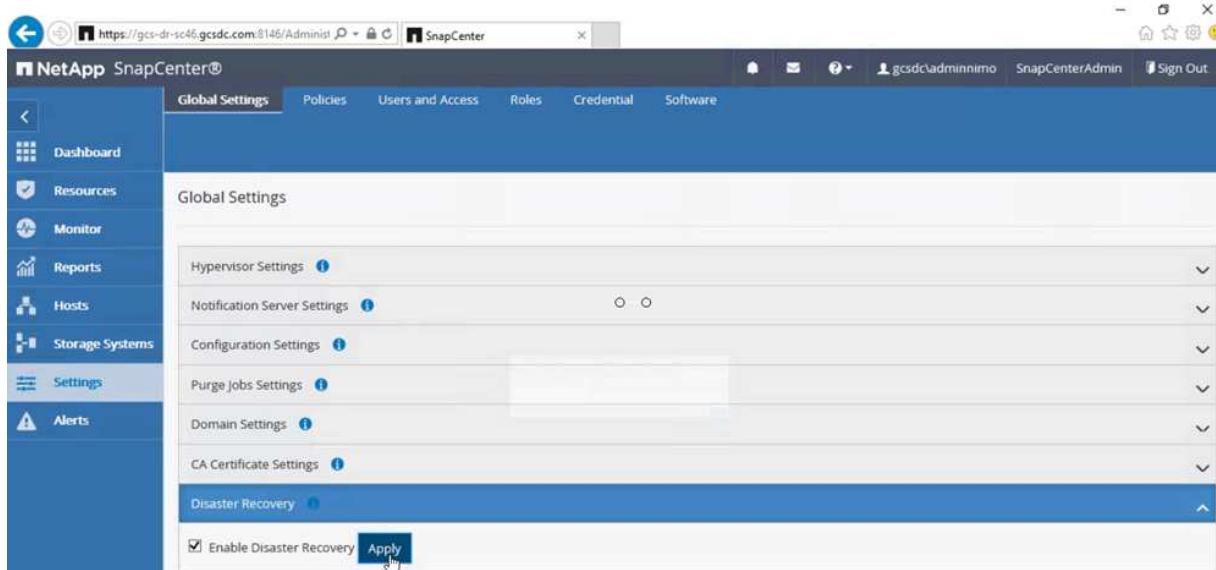
To verify the failover configuration and infrastructure, JetStream DR can be operated in test mode (Test Failover option) to observe the recovery of virtual machines and their data from the object store into a test recovery environment. When a failover procedure is executed in test mode, its operation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



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 browser.



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



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



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

6. Make sure that the SnapMirror relationship is broken.

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

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

## iSCSI Initiator Properties

X

Targets Discovery Favorite Targets Volumes and Devices RADIUS Configuration

### Quick Connect

To discover and log on to a target using a basic connection, type the IP address or DNS name of the target and then click Quick Connect.

Target:

Quick Connect...

### Discovered targets

Refresh

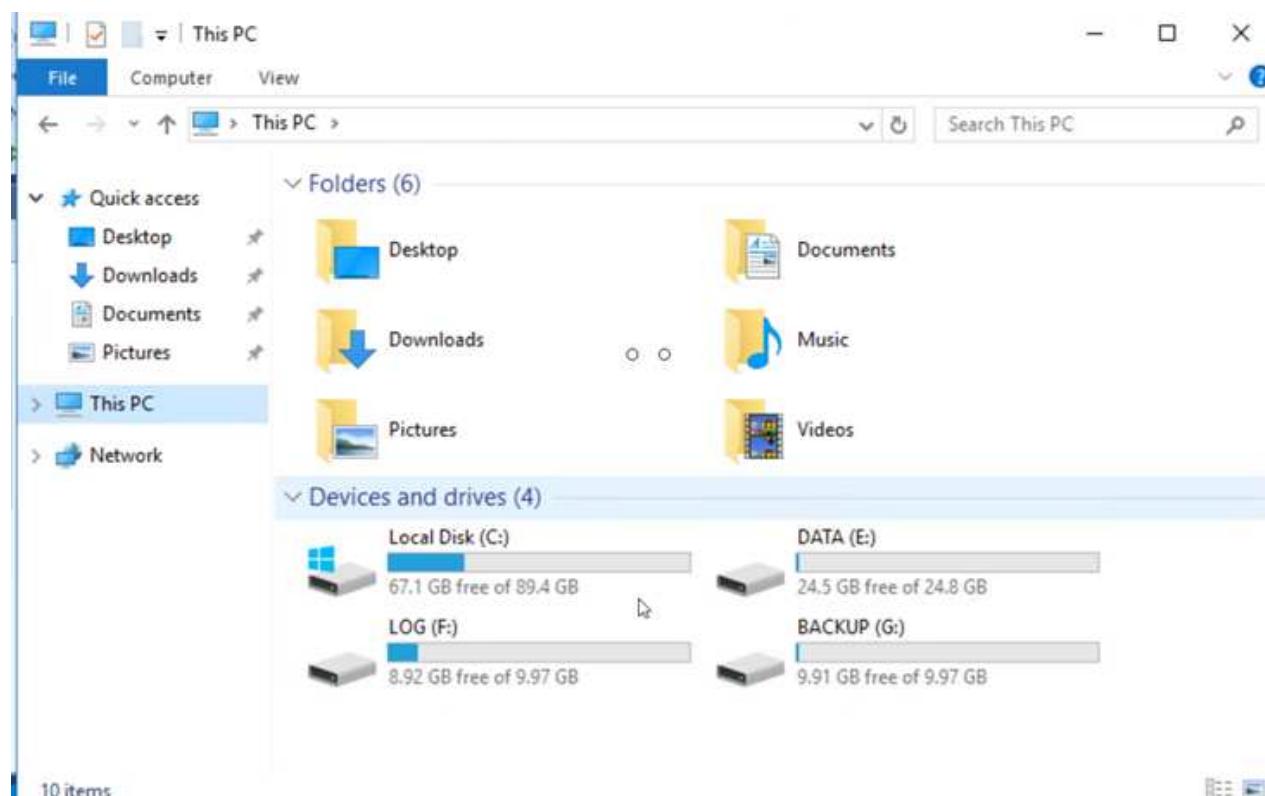
Name

Status

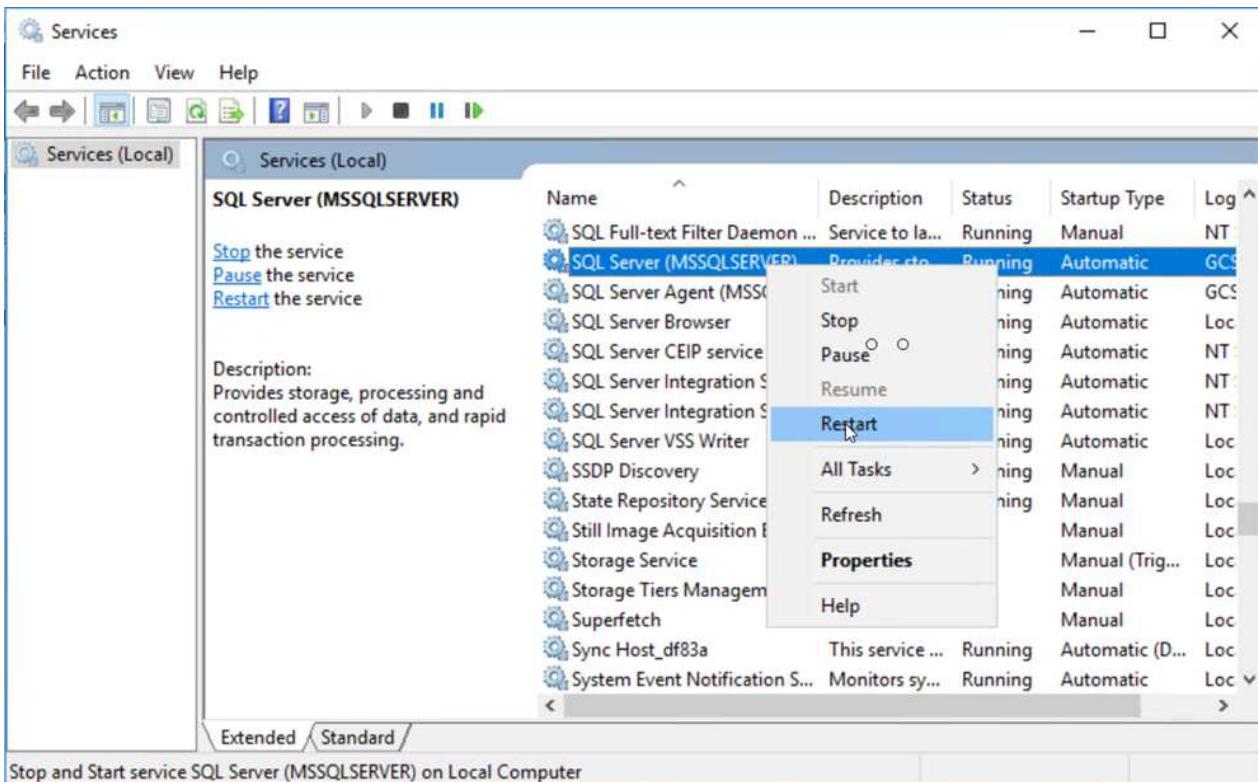
iqn.1992-08.com.netapp:sn.547772ccc47811ecbb62000... Connected

iqn.1992-08.com.netapp:sn.aeab78ab720011ec939800... Reconnecting...

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



10. Restart the MSSQL server service.



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

The screenshot shows the Microsoft SQL Server Management Studio (SSMS) interface. The title bar reads 'SQLQuery1.sql - GCS-DR-SQL03.CarDB (GCSDC\adminnimo (66)) - Microsoft SQL Server Management Studio (Administrator)'. The 'Object Explorer' on the left shows the database structure, including 'CarDB' and its tables. The 'SQLQuery1.sql' query window in the center contains the following SQL script:

```

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

```

The 'Results' tab shows the query results:

	Id	Name	Price
1	1	Car-1	1000
2	2	Car-2	2000
3	3	Car-3	3000
4	4	Car-4	4000
5	5	Car-5	5000

A message at the bottom of the results window says 'Query executed successfully.'



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

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



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

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

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



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

VM Name	Protection Status	Protection Mode	Details
GCS-DR-DC	Recoverable	Write-Back(VMDK)	<a href="#">Details</a>
GCS-DR-Lin\MO1	Recoverable	Write-Back(VMDK)	<a href="#">Details</a>
GCS-DR-SCA	Recoverable	Write-Back(VMDK)	<a href="#">Details</a>
GCS-DR-SQL01	Recoverable	Write-Back(VMDK)	<a href="#">Details</a>
GCS-DR-Win\MO1	Recoverable	Write-Back(VMDK)	<a href="#">Details</a>



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.

**Fallback Protected Domain**

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

Fallback Datacenter	A300-DataCenter
Fallback Cluster	A300-Cluster
Fallback Resource Pool	-
VM Folder (Optional)	-
Fallback Datastore	A300_NFS_vMotion
Maximum Delay After Stopping	10 Minutes
Internal Network	VM_187
External Replication Network	VM_187
Management Network	VM_187
Storage Site	ANFCVODR
DR Virtual Appliance	GCSDRVA002
Replication Log Storage	/dev/sdb

**Buttons:** Cancel, Back, Fallback

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

**JetStream DR**

Protected Domains   Statistics   Storage S...

Select Protected Domain: GCSDRPD002

Recoverable / Total VMs

Replication Status

Remaining Background Data

Current RPO

Protected VMs   Settings   Alarms

**Fallback Task Result**

Task Completed Successfully

Protected Domain	GCSDRPD002
VMs Recovery Status	Success
Total VMs Recovered	4
GCSR03 Status:	
Pre-script Execution Status	Not defined
Runbook Execution Status	Success
Post-script Execution Status	Not defined

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

Health Status	Source Volume	Target Volume	Total Transfer Time	Status	Mirror State	Last Successful Transfer	More
✓	gcsdrsqldb_sc46_ntaphci-a300e9u25	gcsdrsqldb_sc46_copy_ANFCVODRDemo	6 minutes 41 seconds	idle	broken-off	May 5, 2022, 12:08:34 PM 33.66 kB	...
✓	gcsdrsqlhld_sc46_ntaphci-a300e9u25	gcsdrsqlhld_sc46_copy_ANFCVODRDemo	4 minutes 56 seconds	idle	broken-off		Information
✓	gcsdrsqllog_sc46_ntaphci-a300e9u25	gcsdrsqllog_sc46_copy_ANFCVODRDemo	10 minutes 18 seconds	idle	broken-off		Resync Reverse Resync Edit Schedule Edit Max Transfer Rate Delete

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



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.

#### Region Availability – 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.

## Americas

Azure Region	AVS Availability	ANF Availability	NFS Datastore Availability
Central US	Yes	Yes	Yes
East US	Yes	Yes	Yes
East US 2	No	Yes	No
North Central US	Yes	Yes	Yes
South Central US	Yes	Yes	Yes
West Central US	No	No	No
West US	Yes	Yes	Yes
West US2	No	Yes	No
West US3	GA: H1-2023	Yes	Yes
Canada Central	Yes	Yes	Yes
Canada East	Yes	Yes	Yes
Brazil South	Yes	Yes	Yes
Brazil Southeast	No	GA: Q2-2022	No

Last updated on: June 7, 2022.

## EMEA

Azure Region	AVS Availability	ANF Availability	NFS Datastore Availability
North Europe	Yes	Yes	Yes
West Europe	No	Yes	No
France Central	Yes	Yes	Yes
France South	No	GA: H2-2022	No
Germany North	No	Yes	No
Germany West Central	Yes	Yes	Yes
Norway East	No	Yes	No
Norway West	No	Yes	No
Sweden Central	GA: Q2-2022	GA: Q2-2022	No
Sweden South	No	No	No
Switzerland North	No	Yes	No
Switzerland West	No	Yes	No
UAE Central	No	Yes	No
UAE North	No	Yes	No
UK South	Yes	Yes	Yes

UK West	Yes	Yes	Yes
---------	-----	-----	-----

Last updated on: June 7, 2022.

#### Asia Pacific

Azure Region	AVS Availability	ANF Availability	NFS Datastore Availability
Australia East	Yes	Yes	Yes
Australia Southeast	Yes	Yes	Yes
Australia Central	No	Yes	No
Japan East	Yes	Yes	No
Japan West	Yes	Yes	Yes
East Asia	No	Yes	No
Southeast Asia	Yes	Yes	Yes
Central India	No	Yes	No
South India	No	Yes	No
Korea Central	No	Yes	No

Last updated on: June 20, 2022.

## NetApp Hybrid Multicloud Solutions for GCP / GCVE

### 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

#### Document scope

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	

Next: [How Cloud Volumes Service in Google Cloud secures your data.](#)

## How Cloud Volumes Service in Google Cloud secures your data

Previous: [Overview.](#)

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.

[Next: Security considerations and attack surfaces](#).

## Security considerations and attack surfaces

[Previous: How Cloud Volumes Service in Google Cloud secures your data.](#)

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.

[Next: Architecture overview.](#)

## Architecture

### Overview

[Previous: Security considerations and attack surfaces.](#)

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.

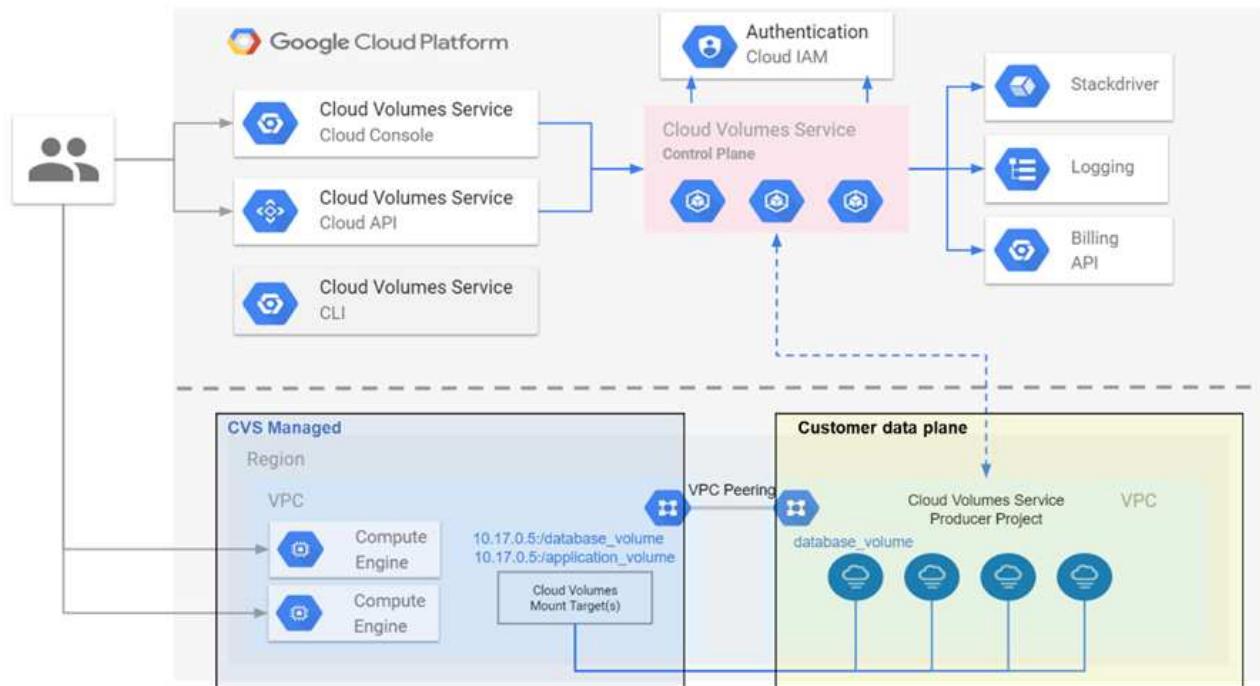
There are distinct differences in how each plane is secured and managed. The following sections cover these differences, starting with a Cloud Volumes Service architecture overview.

[Next: Cloud Volumes Service architecture.](#)

## 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 projects 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 well-defined 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. Both CVS-SW and CVS-Performance support LDAP signing.

IP addresses of the LDAP server and CVS instance				LDAP base DN and search type, search result		
No.	Time	Source	Destination	Protocol	Length	Info
2320...	366.244071	10.194.0.6	10.10.0.11	LDAP	225	searchRequest(2) "DC=cvsdemo,DC=local" wholeSubtree
2320...	366.244381	10.10.0.11	10.194.0.6	LDAP	330	searchResRef(2)   searchResRef(2)   searchResRef(2)   searchResDone(2) success [0 results]
<span>▼ <b>searchRequest</b></span> <pre>baseObject: DC=cvsdemo,DC=local scope: wholeSubtree (2) derefAliases: neverDerefAliases (0) sizeLimit: 0 timeLimit: 3 typesOnly: False   ▼ Filter: (&amp;(objectClass=User)(uidNumber=1025))     ▼ filter: and (0)       ▼ and: (&amp;(objectClass=User)(uidNumber=1025))         ▼ and: 2 items           ▼ Filter: (objectClass=User)             ▼ and: item: equalityMatch (3)               ▼ equalityMatch                 attributeDesc: objectClass                 assertionValue: User             ▼ Filter: (uidNumber=1025)               ▼ and: item: equalityMatch (3)                 ▼ equalityMatch                   attributeDesc: uidNumber                   assertionValue: 1025   ▼ attributes: 7 items     AttributeDescription: uid     AttributeDescription: uidNumber     AttributeDescription: gidNumber     AttributeDescription: unixUserPassword     AttributeDescription: name     AttributeDescription: unixHomeDirectory     AttributeDescription: loginShell</pre> <span>Attributes queried</span>						

i 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.

IP addresses of the NFS client and CVS instance				Genericized NFS call/reply		
No.	Time	Source	Destination	Protocol	Length	Info
380	9.218014	10.193.67.225	10.193.67.219	NFS	346	V4 Call (Reply In 381)
381	9.218480	10.193.67.219	10.193.67.225	NFS	426	V4 Reply (Call In 380)
382	9.218641	10.193.67.225	10.193.67.219	NFS	370	V4 Call (Reply In 397)
397	9.369035	10.193.67.219	10.193.67.225	NFS	458	V4 Reply (Call In 382)
<span>► Frame 381: 426 bytes on wire (3408 bits), 426 bytes captured (3408 bits)</span> <span>► Ethernet II, Src: IntelCor_7f:da:bc (90:e2:ba:7f:da:bc), Dst: VMware_a0:2c:2d (00:50:56:a0:2c:2d)</span> <span>► Internet Protocol Version 4, Src: 10.193.67.219, Dst: 10.193.67.225</span> <span>► Transmission Control Protocol, Src Port: 2049, Dst Port: 738, Seq: 6305, Ack: 6569, Len: 360</span> <span>► Remote Procedure Call, Type:Reply XID:0xef5e998d</span> <span data-cs="2" data-kind="parent" style="border: 1px solid #ccc; padding: 2px;">GSS-Wrap</span> <span data-kind="ghost"></span> <span>Length: 300</span> <span>GSS Data: 050407ff000000000000000025913451ee1d43d298cf3031...</span> <span>► krb5_blob: 050407ff000000000000000025913451ee1d43d298cf3031...</span> <span data-cs="2" data-kind="parent" style="border: 1px solid #ccc; padding: 2px;">Network File System</span> <span data-kind="ghost"></span> <span>[Program Version: 4]</span> <span>[V4 Procedure: COMPOUND (1)]</span>						

IP addresses of the NFS client and CVS instance				Detailed NFS call types and file handle information		
No.	Time	Source	Destination	Protocol	Length	Info
	33 0.958480	10.193.67.201	10.193.67.204	NFS	458	V4 Reply (Call In 32) OPEN StateID: 0x0481
	34 0.958784	10.193.67.204	10.193.67.201	NFS	308	V4 Call (Reply In 35) SETATTR FH: 0x6c07918a
	35 0.959284	10.193.67.201	10.193.67.204	NFS	356	V4 Reply (Call In 34) SETATTR

```

> Opcode: PUTFH (22)
> Opcode: SETATTR (34)
< Opcode: GETATTR (9)
  Status: NFS4_OK (0)
  < Attr mask[0]: 0x0010011a (Type, Change, Size, FSID, fileId)
    > reqd_attr: Type (1)
    > reqd_attr: Change (3)
    > reqd_attr: Size (4)
    > reqd_attr: FSID (8)
    < reco_attr: fileId (20)          File ID
      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
      > fatt4_owner: root@NTAP.LOCAL
    < reco_attr: Owner_Group (37)
      > fatt4_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)

```

## 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.

[Next: Control plane architecture.](#)

## Control plane architecture

[Previous: Cloud Volumes Service 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.

[Next: Data plane architecture.](#)

## Data plane architecture

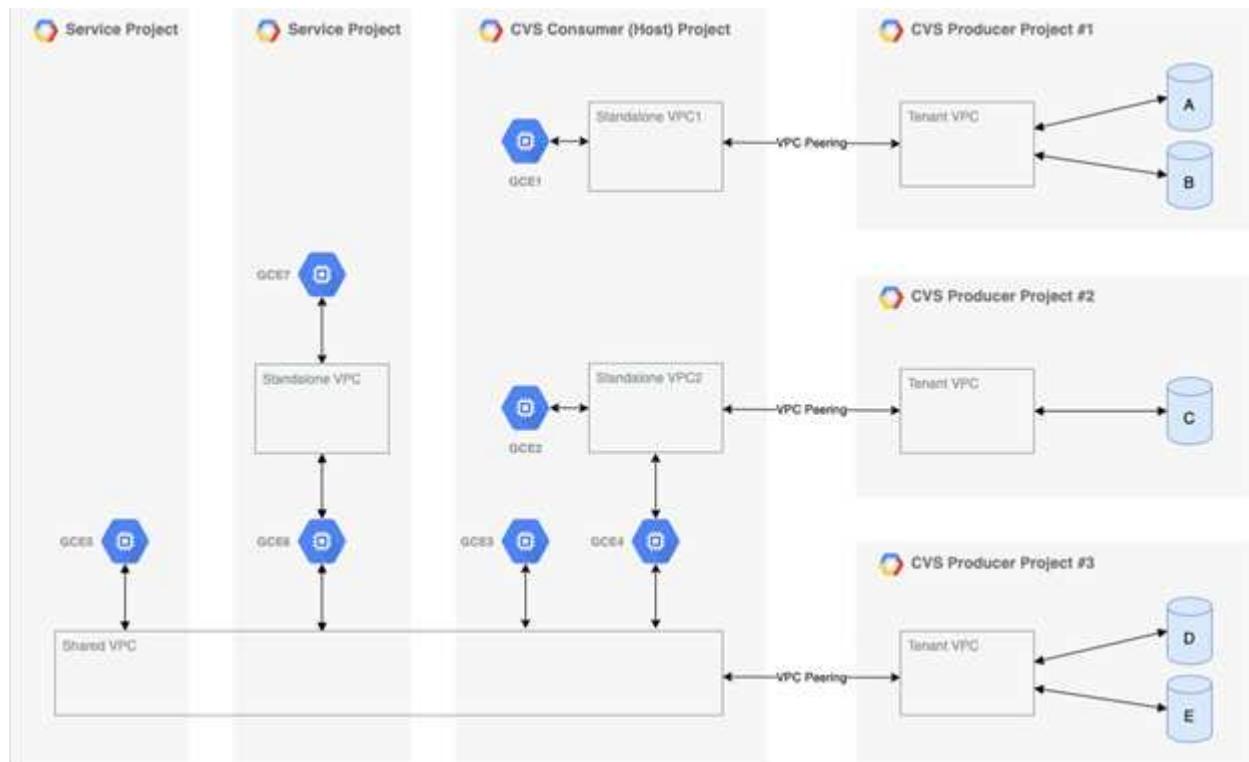
[Previous: Control plane architecture.](#)

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.

[Next: Data encryption in transit.](#)

**Data encryption in transit**

[Previous: Data plane architecture.](#)

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).

The following table shows differences in what each level does for security and performance.

Security level	Security	Performance
NFSv3—sys	<ul style="list-style-type: none"><li>Least secure; plain text with numeric user IDs/group IDs</li><li>Able to view UID, GID, client IP addresses, export paths, file names, permissions in packet captures</li></ul>	<ul style="list-style-type: none"><li>Best for most cases</li></ul>
NFSv4.x—sys	<ul style="list-style-type: none"><li>More secure than NFSv3 (client IDs, name string/domain string matching) but still plain text</li><li>Able to view UID, GID, client IP addresses, name strings, domain IDs, export paths, file names, permissions in packet captures</li></ul>	<ul style="list-style-type: none"><li>Good for sequential workloads (such as VMs, databases, large files)</li><li>Bad with high file count/high metadata (30-50% worse)</li></ul>
NFS—krb5	<ul style="list-style-type: none"><li>Kerberos encryption for credentials in every NFS packet—wraps UID/GID of users/groups in RPC calls in GSS wrapper</li><li>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</li><li>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)</li></ul>	<ul style="list-style-type: none"><li>Best in most cases for Kerberos; worse than AUTH_SYS</li></ul>

Security level	Security	Performance
NFS—krb5i	<ul style="list-style-type: none"> <li>• Kerberos encryption for credentials in every NFS packet—wraps UID/GID of users/groups in RPC calls in GSS wrapper</li> <li>• 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</li> <li>• 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)</li> <li>• Kerberos GSS checksum is added to every packet to ensure nothing intercepts the packets. If checksums match, conversation is allowed.</li> </ul>	<ul style="list-style-type: none"> <li>• 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.</li> </ul>

Security level	Security	Performance
NFS – krb5p	<ul style="list-style-type: none"> <li>• Kerberos encryption for credentials in every NFS packet—wraps UID/GID of users/groups in RPC calls in GSS wrapper</li> <li>• 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</li> <li>• All of the NFS packet payloads are encrypted with the GSS wrapper (cannot see file handles, permissions, file names, atime/mtime in packet captures).</li> <li>• Includes integrity check.</li> <li>• NFS operation type is visible (FSINFO, ACCESS, GETATTR, and so on).</li> <li>• Ancillary protocols (mount, portmap, nlm, and so on) are not encrypted - (can see export paths, IP addresses)</li> </ul>	<ul style="list-style-type: none"> <li>• Worst performance of the security levels; krb5p has to encrypt/decrypt more.</li> <li>• Better performance than krb5p with NFSv4.x for high file count workloads.</li> </ul>

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.”](#)

[Next: Data encryption at rest.](#)

[Data encryption at rest](#)

[Previous: Data encryption in transit.](#)

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](#).

Next: [Firewall](#).

## Firewall

Previous: [Data encryption at rest](#).

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](#).

Next: [NAS protocols overview](#).

## NAS protocols

### NAS protocols overview

Previous: [Firewall](#).

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.

Next: [Basics of NAS protocols](#).

### Basics of NAS protocols

Previous: [NAS protocols overview](#).

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.

[Next: NFS.](#)

## NFS

[Previous: Basics of NAS protocols \\_ overview.](#)

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
<ul style="list-style-type: none"><li>• root:0</li><li>• pcuser:65534</li><li>• nobody:65535</li></ul>	<ul style="list-style-type: none"><li>• root:0</li><li>• daemon:1</li><li>• pcuser:65534</li><li>• nobody:65535</li></ul>



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
<ul style="list-style-type: none"> <li>• Set user ID on execution</li> <li>• Set group ID on execution</li> <li>• Save swapped text (not defined in POSIX)</li> <li>• Read permission for owner</li> <li>• Write permission for owner</li> <li>• Execute permission for owner on a file; or look up (search) permission for owner in directory</li> <li>• Read permission for group</li> <li>• Write permission for group</li> <li>• Execute permission for group on a file; or look up (search) permission for group in directory</li> <li>• Read permission for others</li> <li>• Write permission for others</li> <li>• Execute permission for others on a file; or look up (search) permission for others in directory</li> </ul>	Access control entry (ACE) types (Allow/Deny/Audit) * Inheritance flags * directory-inherit * file-inherit * no-propagate-inherit * inherit-only  Permissions * read-data (files) / list-directory (directories) * write-data (files) / create-file (directories) * append-data (files) / create-subdirectory (directories) * execute (files) / change-directory (directories) * 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 additional 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:rwtTnNcCy
```

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](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   root   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 apache apache-group 0 Feb  3 12:07 ldap-user-file
-rw-r--r-- 1 root   root   0 Feb  3 12:06 root-user-file
```

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 `ls` 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 -l  
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 qtree1
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 -l
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
```

[Next: SMB.](#)

**SMB**

[Previous: NFS.](#)

**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 `\\\$ERVERNAME` 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:

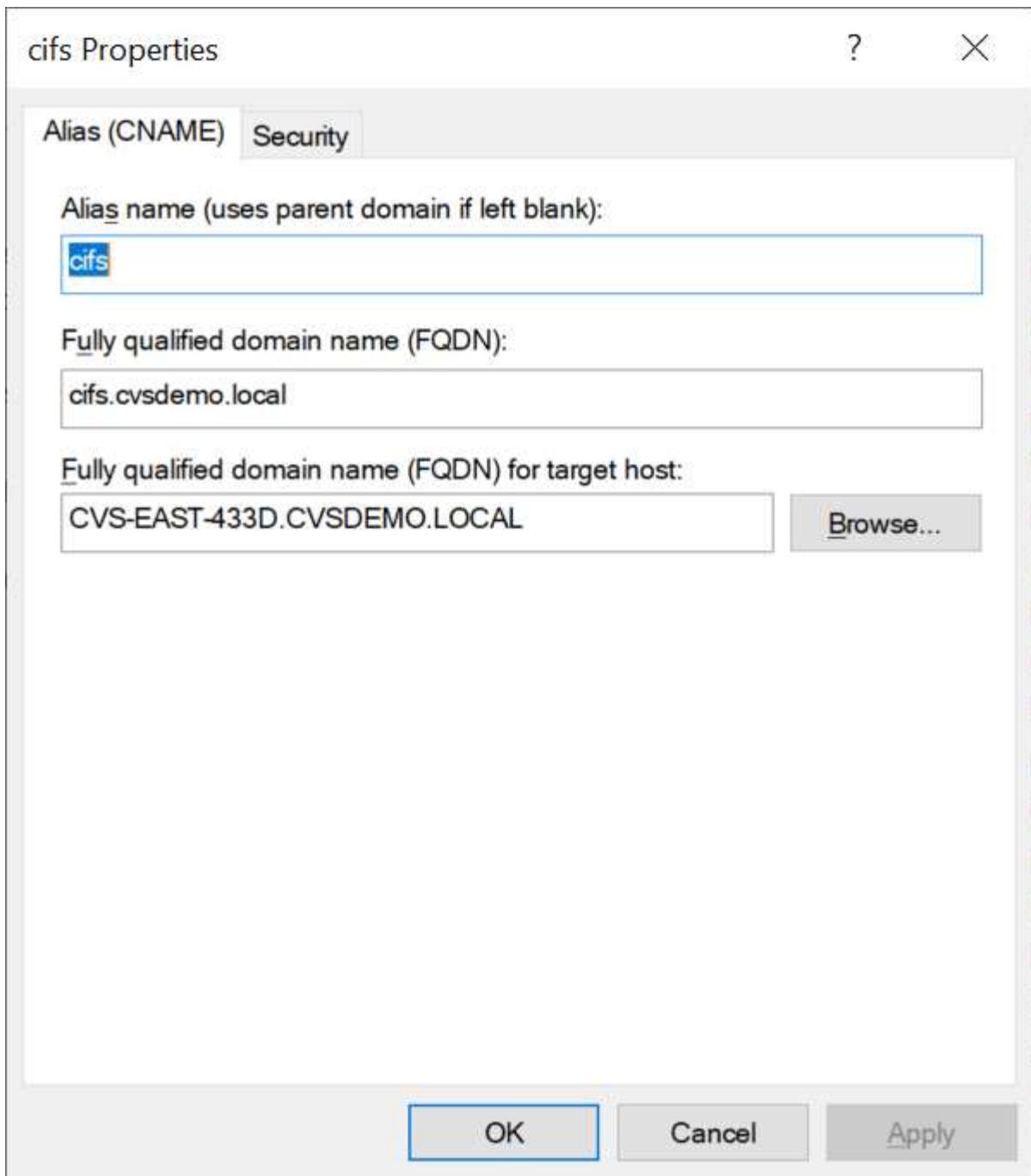
```
PS C:\> nslookup CVS-EAST-433D
Server:  activedirectory. region. lab. internal
Address: 10. xx.0. xx
Name:    CVS-EAST-433D.cvsdemo.local
Address: 10. xxx.0. x
PS C:\> nslookup 10. xxx.0. x
Server:  activedirectory.region.lab.internal
Address: 10.xx.0.xx
Name:    CVS-EAST-433D.CVSDEMO.LOCAL
Address: 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.



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.

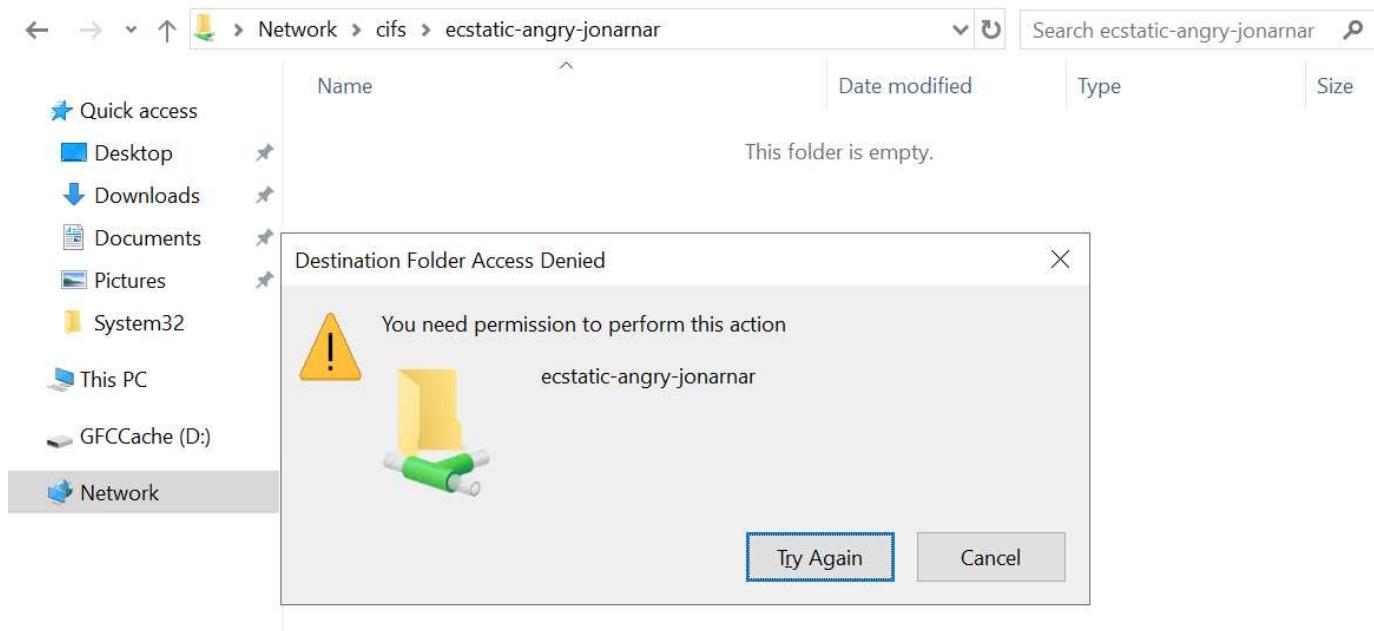
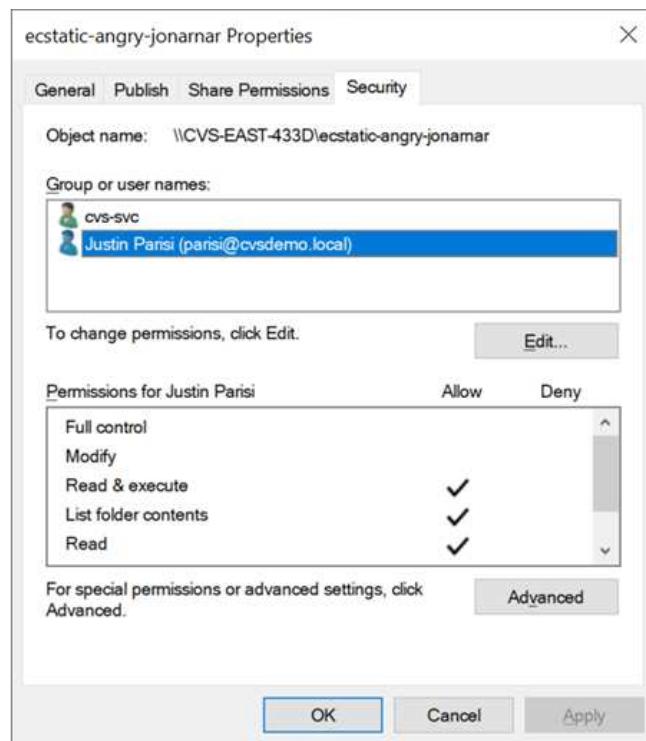
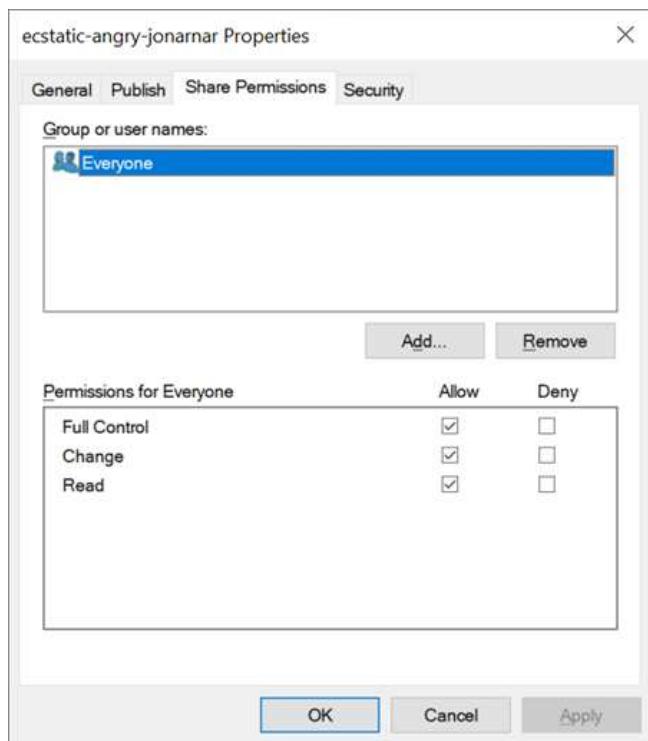
## Share permissions

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.



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

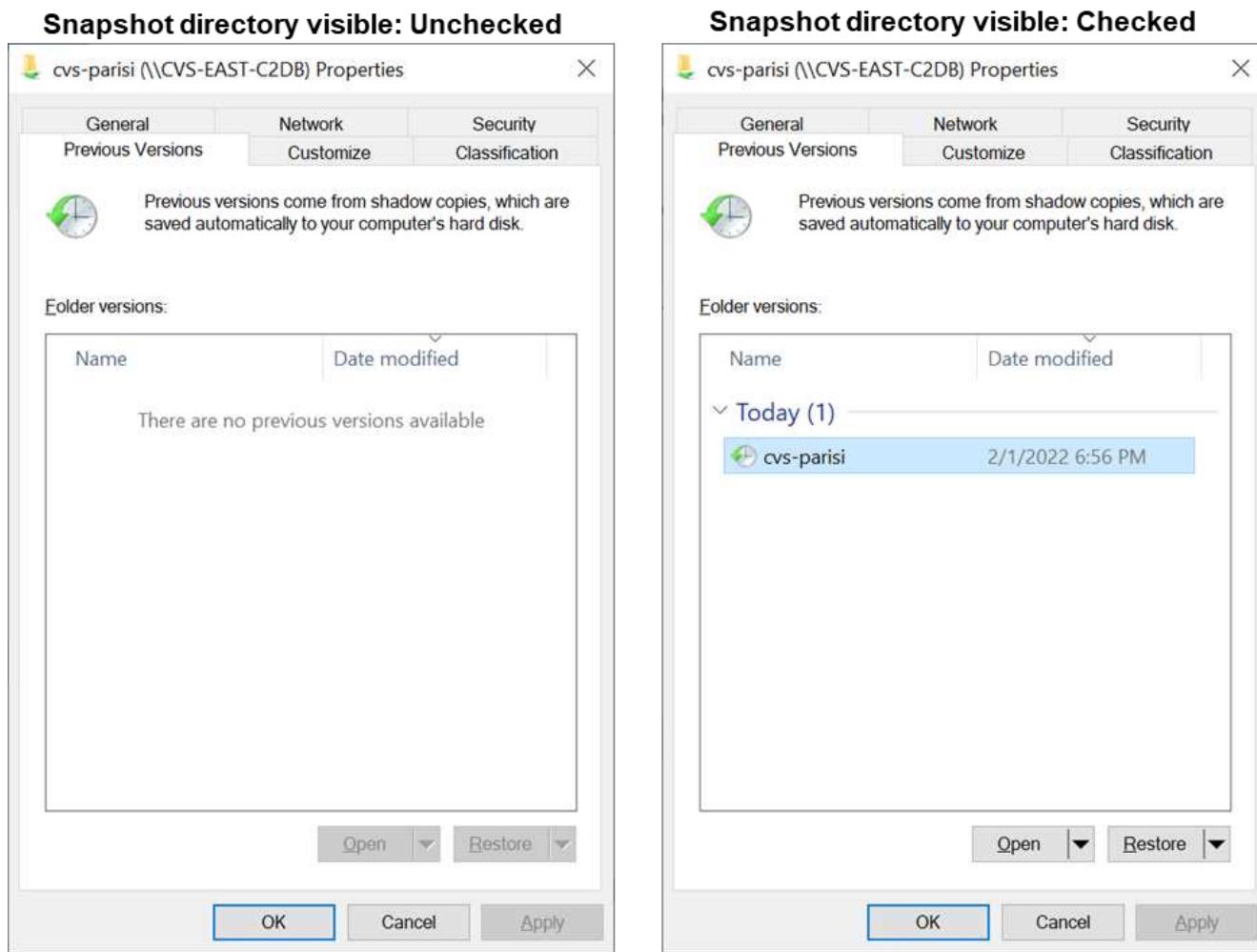
directory or volume has inherited permissions added to it, which can create unwanted behavior such as unintended access/denial and long churn of permission modification as each file is adjusted.

## SMB share security features

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.



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

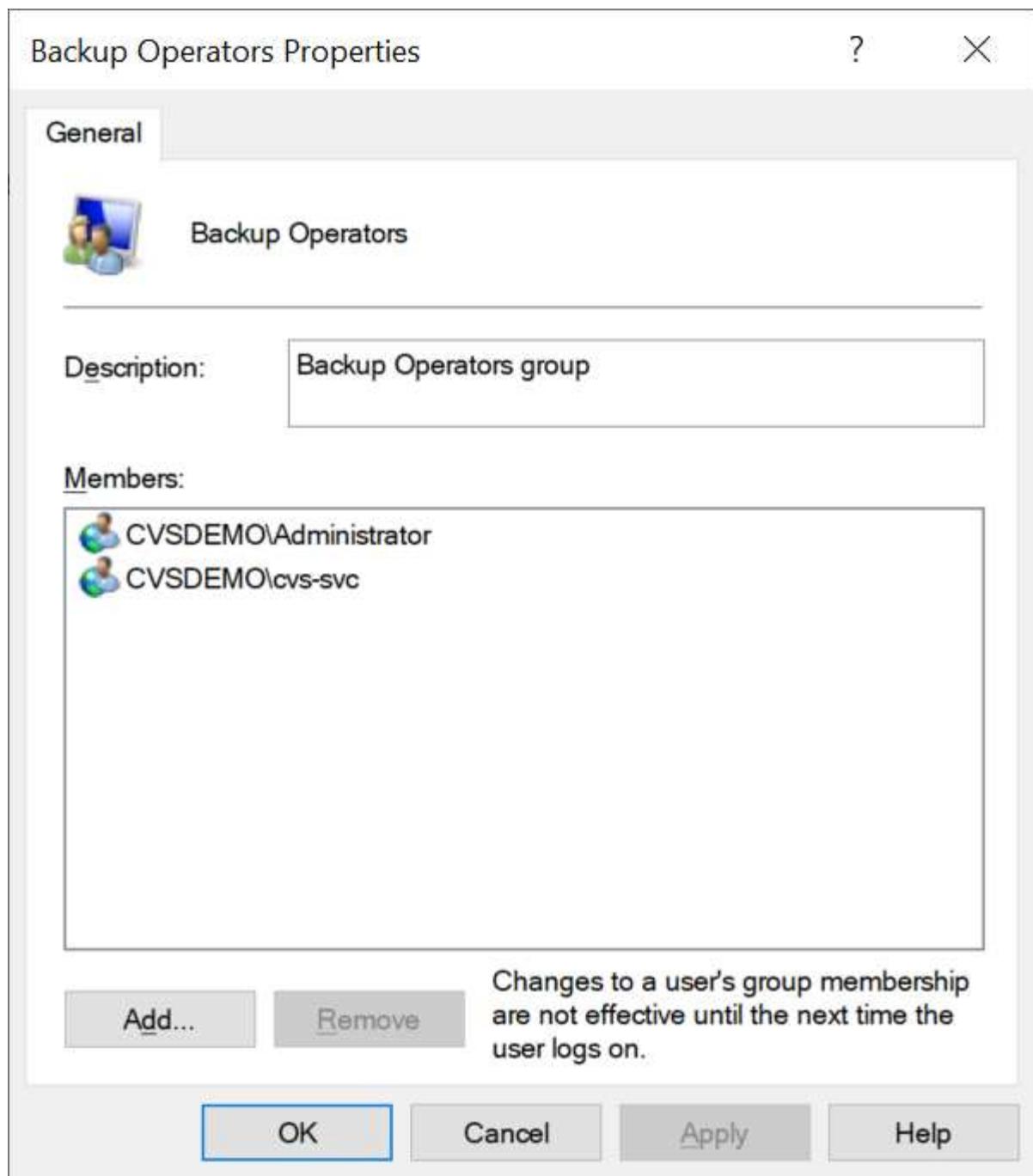
## Security Privilege Users

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.



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 memberships) 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-C2DB)	Name	Full Name	Description
System Tools Task Scheduler Event Viewer Shared Folders Shares Sessions Open Files Local Users and Groups Users Groups	Administrator		Built-in administrator account

Computer Management (CVS-EAST-C2DB)	Name	Description
System Tools Task Scheduler Event Viewer Shared Folders Shares Sessions Open Files Local Users and Groups Users Groups	Administrators	Built-in Administrators group
	Users	All users
	Guests	Built-in Guests Group
	Power Users	Restricted administrative privileges
	Backup Operators	Backup Operators group

Administrators Properties

General

Administrators

Description: Built-in Administrators group

Members:

Administrator  
CVSDEMO\Domain Admins

Add... Remove

Changes to a user's group membership are not effective until the next time the user logs on.

OK Cancel Apply Help

## MMC/Computer Management access

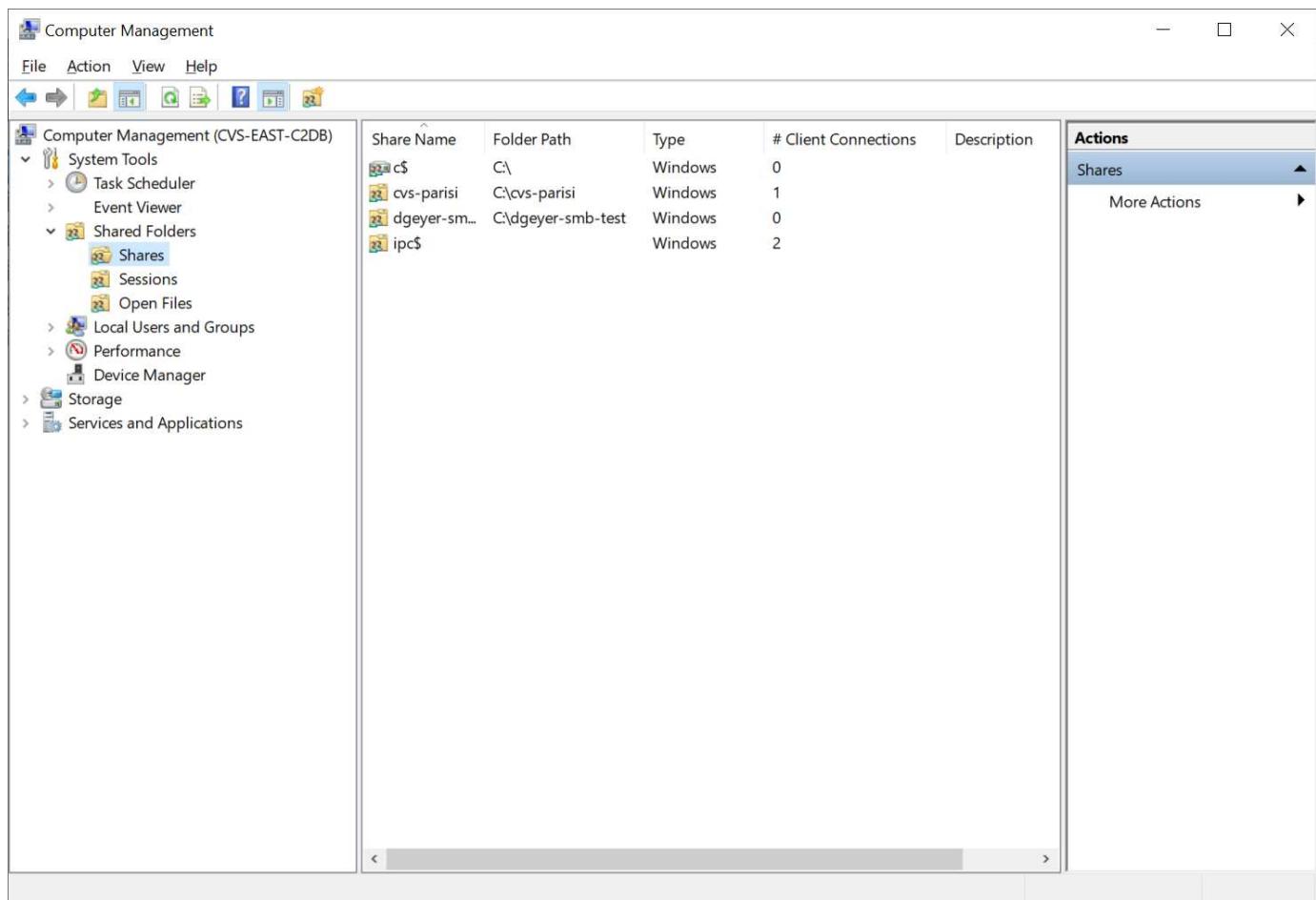
SMB access in Cloud Volumes Service provides connectivity to the Computer Management MMC, which allows you to view shares, manage share ACLs, and view/manage SMB sessions and open files.

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.

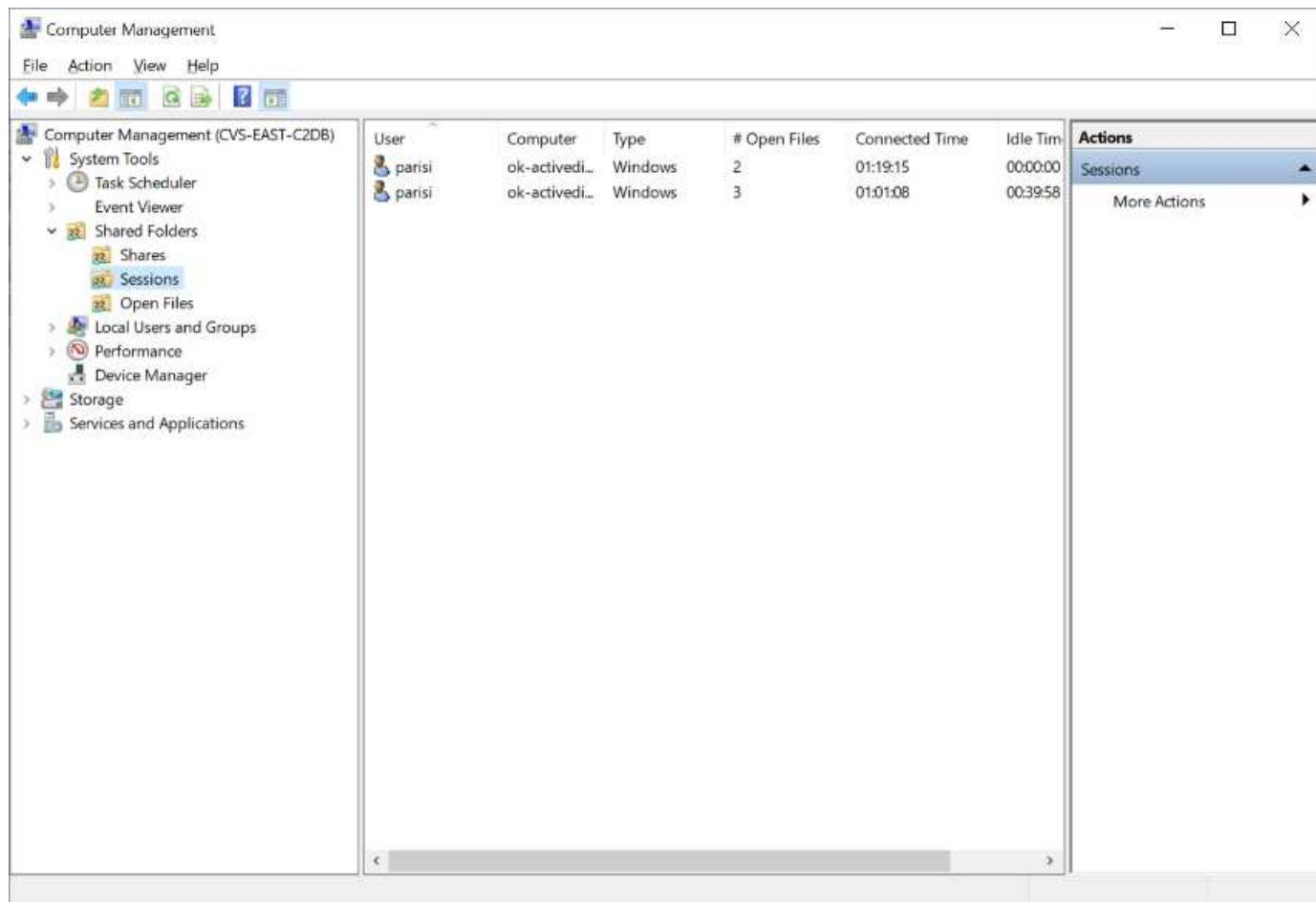
Remember, only one Active Directory connection is allowed per region.



The screenshot shows the Windows Computer Management console. The left navigation pane lists various management tools like Task Scheduler, Event Viewer, Shared Folders, Local Users and Groups, Performance, Device Manager, Storage, and Services and Applications. The 'Shared Folders' node is expanded, and its 'Shares' sub-node is selected, highlighted with a blue border. The main pane displays a table of SMB shares:

Share Name	Folder Path	Type	# Client Connections	Description
c\$	C:\	Windows	0	
cvs-parisi	C\cvs-parisi	Windows	1	
dgeyer-sm...	C\dgeyer-smb-test	Windows	0	
ipc\$		Windows	2	

The 'Actions' pane on the right shows a 'Shares' button and a 'More Actions' dropdown menu.



The following table shows a list of supported/unsupported functionality for the MMC.

Supported functions	Unsupported functions
<ul style="list-style-type: none"> <li>View shares</li> <li>View active SMB sessions</li> <li>View open files</li> <li>View local users and groups</li> <li>View local group memberships</li> <li>Enumerate the list of sessions, files, and tree connections in the system</li> <li>Close open files in the system</li> <li>Close open sessions</li> <li>Create/manage shares</li> </ul>	<ul style="list-style-type: none"> <li>Creating new local users/groups</li> <li>Managing/viewing existing local user/groups</li> <li>View events or performance logs</li> <li>Managing storage</li> <li>Managing services and applications</li> </ul>

## 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 “ <a href="#">SMB authentication dialects</a> ” 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 “ <a href="#">SMB share security features</a> ”).	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 “ <a href="#">LDAP channel binding</a> .”.	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

[Next: Dual-protocol/multiprotocol.](#)

[Dual-protocol/multiprotocol](#)

[Previous: SMB.](#)

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.

[Next: Considerations for creating Active Directory connections.](#)

## Considerations for creating Active Directory connections

[Previous: Dual-protocol/multiprotocol.](#)

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.

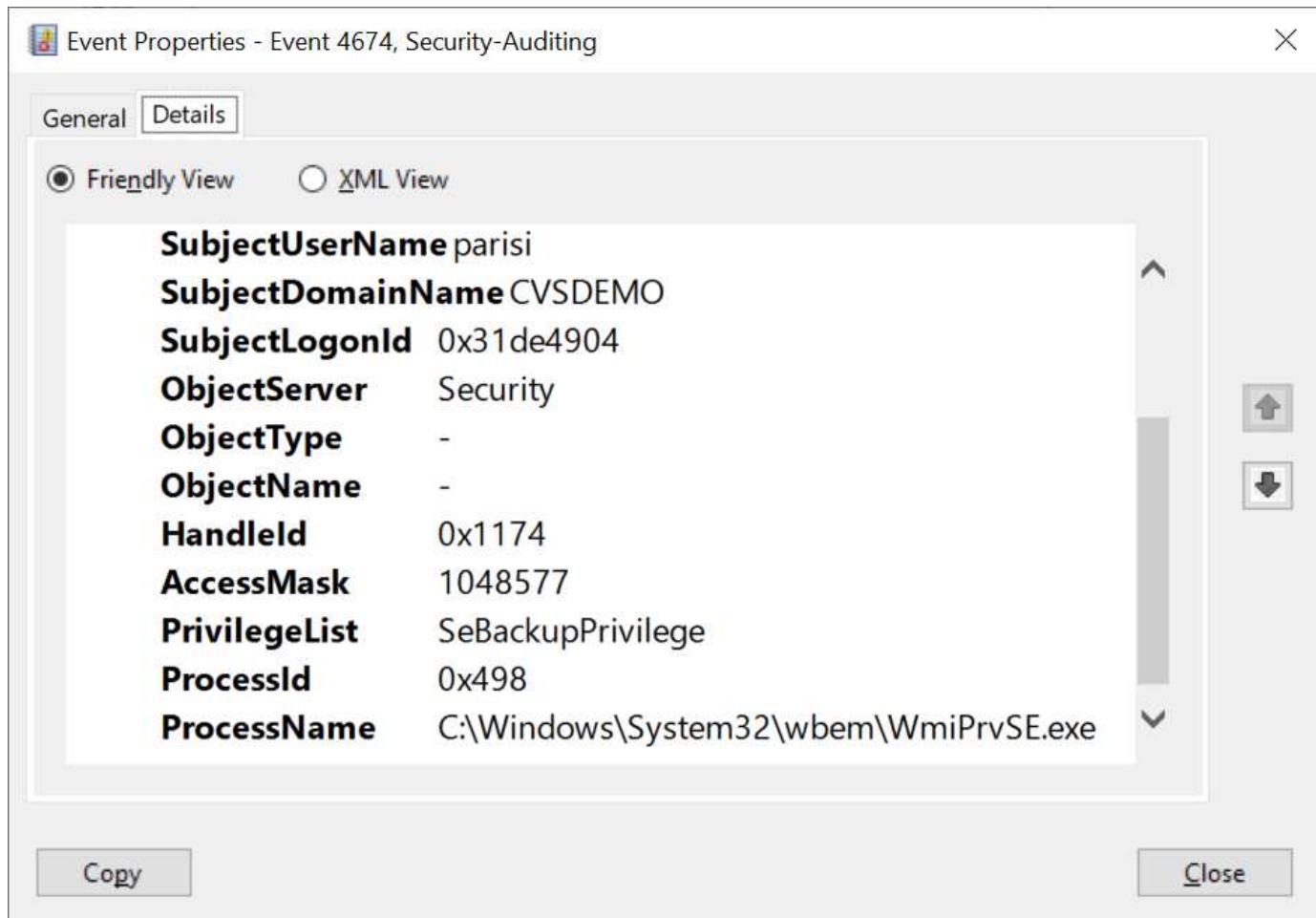
## Region

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.



## 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 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](#).

[Next: Other NAS Infrastructure service dependencies \(KDC, LDAP, DNS\).](#)

[Other NAS Infrastructure service dependencies \(KDC, LDAP, and DNS\)](#)

[Previous: Considerations for creating Active Directory connections.](#)

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	<ul style="list-style-type: none"> <li>Client ID mapping configuration (/etc/idmap.conf)</li> <li>Windows Active Directory: KDC DNS LDAP</li> </ul>
SMB only	Active Directory: * KDC * DNS
Multiprotocol NAS (NFS and SMB)	<ul style="list-style-type: none"> <li>Client ID mapping configuration (NFSv4.1 only; /etc/idmap.conf)</li> <li>Windows Active Directory: KDC DNS LDAP</li> </ul>

### 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](mailto: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 read-only 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 used 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, onlevel, 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, onlevel, 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, onlevel, 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, onlevel 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 Cloud Volumes Service, but sealing is not currently 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.

Published Certificates		Member Of		Password Replication		Dial-in		Object													
Security		Environment		Sessions		Remote control															
General	Address	Account	Profile	Telephones	Organization																
Remote Desktop Services Profile				COM+		Attribute Editor															
<b>Attributes:</b>																					
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 Time																				
replPropertyMetaData	AttID	Ver	Loc.USN	Org.DSA																	
sAMAccountName	asymmetric																				
sAMAccountType	805306368 = ( NORMAL_USER_ACCOUNT )																				
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.

[Next: Service operation.](#)

## Service operation

[Previous: Other NAS Infrastructure service dependencies \(KDC, LDAP, DNS\).](#)

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.

[Next: Additional information, version history, and contact information.](#)

## Additional information, version history, and contact information

Previous: [Service operation](#).

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](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>

## Version history

Version	Date	Document version history
Version 1.0	May 2022	Initial release.

## Contact us

Let us know how we can improve this technical report.

Contact us at [doccomments@netapp.com](mailto:doccomments@netapp.com). Include TECHNICAL REPORT 4918 in the subject line.

## Copyright Information

Copyright © 2022 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.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

## 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.