

VMware for Public Cloud

NetApp Solutions

NetApp July 15, 2022

This PDF was generated from https://docs.netapp.com/us-en/netapp-solutions/ehc/ehc-overview.html on July 15, 2022. Always check docs.netapp.com for the latest.

Table of Contents

| VMware for Public Cloud | 1 |
|--|-----|
| Overview of NetApp Hybrid Multi-Cloud with VMware | 1 |
| NetApp Solutions for VMware in Hyperscalers | 5 |
| Supported Configurations for NetApp Hybrid Multi-Cloud with VMware | 9 |
| Configuring the virtualization environment in the cloud provider | 9 |
| NetApp Storage options for Public Cloud Providers | 38 |
| Summary and Conclusion: Why NetApp Hybrid Multi-Cloud with VMware | 132 |

VMware for Public Cloud

Overview of NetApp Hybrid Multi-Cloud 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 (laaS) 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!



(i)

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

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

• VMware in the Hyperscalers Configuration

- NetApp Storage Options
- NetApp / VMware Cloud Solutions

VMware in the Hyperscalers Configuration

As with on-premises, planning a cloud based virtualization environment is critical for a successful 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 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 guess connected or as a native datastore - within each of the 3 major hyperscalers.

Please visit Supported NetApp Storage Options for more information.

AWS supports NetApp storage in the following configurations:

- FSx ONTAP as guest connected storage
- Cloud Volumes ONTAP (CVO) as guest connected storage
- FSx ONTAP as a native datastore¹

View the detailed guest connect storage options for VMC.

Read more about FSx ONTAP as a native datastore public preview from the AWS Press Release (COMING SOON!).

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 datastore¹

View the detailed guest connect storage options for AVS.

Read more about Azure NetApp Files (ANF) as a native datastore - Public Preview.

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 datastore¹

View the detailed guest connect storage options for GCVE.

Read more about Cloud Volumes Service (CVS) as a native datastore¹.



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

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 Multi-Cloud with VMware

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

| | Guest Connected | Native Datastore |
|-------|-----------------------------|---|
| AWS | CVO FSx ONTAP Details | FSx ONTAP Press Release coming soon! |
| Azure | CVO ANF Details | ANF Details¹ |
| GCP | CVO CVS Details | CVS Details ² |

NOTE:

- 1 Currently in Public Preview
- 2 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.

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.

 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.





- Single-host configuration is used in this validation.
- 4. Select the desired AWS VPC to connect the VMC environment with.



 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.



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

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



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

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





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.





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.





5. Create the Transit Gateway Attachment.



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:



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 onpremises networks. The CIDR represents the private cloud management network and is used for the cluster management services, such as vCenter Server and NSX-T Manager. NetApp recommends using a /22 address space. In this example, 10.21.0.0/22 is used.



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.



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.



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



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



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.



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.



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.



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.



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



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

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



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 datastore¹

View the detailed guest connect storage options for VMC.

Read more about FSx ONTAP as a native datastore public preview from the AWS Press Release (COMING SOON!).

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 datastore¹

View the detailed guest connect storage options for AVS.

Read more about Azure NetApp Files (ANF) as a native datastore - Public Preview.

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 datastore¹

View the detailed guest connect storage options for GCVE.

Read more about Cloud Volumes Service (CVS) as a native datastore¹.



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.



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



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.





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.



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.



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.



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



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.



▶ 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.



Endpoints

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

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

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



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





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 (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.

Two entries were displayed.

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



Two entries were displayed.

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

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

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



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



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 you IT staff in all-new methods to manage your data.

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

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

Cloud Volumes ONTAP (CVO) as guest connected storage



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.

 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.



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



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



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



9. Select the appropriate route tables to include routes to the floating IP addresses and then click 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 @ ID Associate with Subnet Name Tags rtb-00b2d30c3f68fdbdd 0 Subnets 1 Tags 1 1 Route Tables | The main route table is the default for the VPC 10. On the Data Encryption page, choose AWS-managed encryption. Data Encryption Create a New Working Environment ↑ 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 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.



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.



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



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





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. 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 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.





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.



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:

- 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 Ø vSphere - ubuntu01 - Summary × ubuntu01 O A ## https://vcenter.sddc-52-37-127-104.vmwarevmc.com/ui/webconsole.html?vmld=vm-1003&vmName=ubuntu01&sen ☆ ubuntu01 Enforce US Keyboard Layout View Fullscre

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:

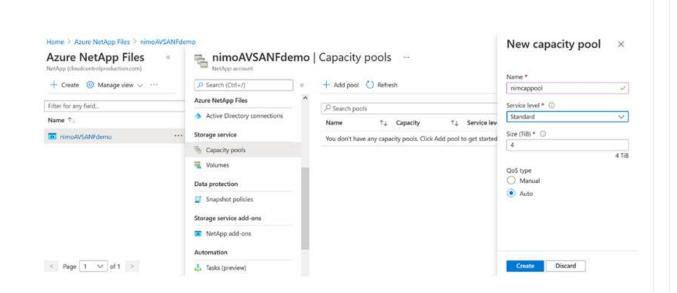
 Log in to the Azure Portal and access Azure NetApp Files. Verify access to the Azure NetApp Files service and register the Azure NetApp Files Resource Provider by using the az provider register --namespace Microsoft.NetApp -wait command. After registration is complete, create a NetApp account.

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



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

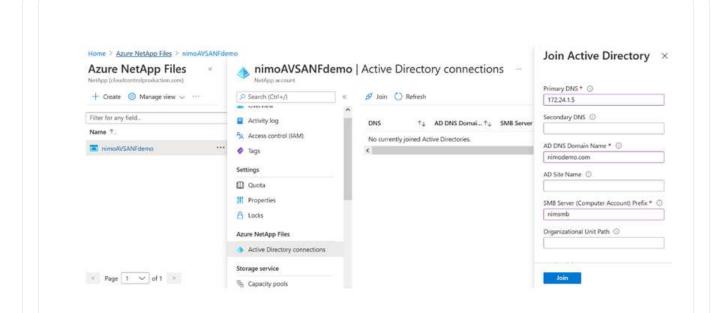
For more information, see Set up a capacity pool.



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.

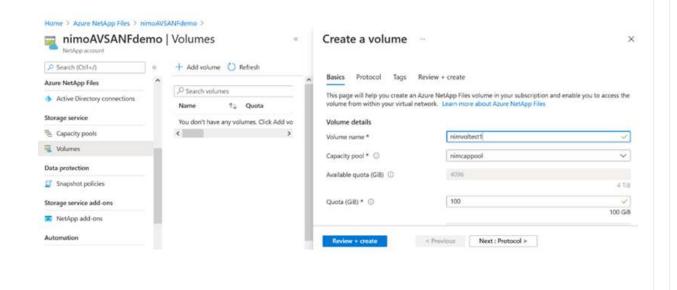


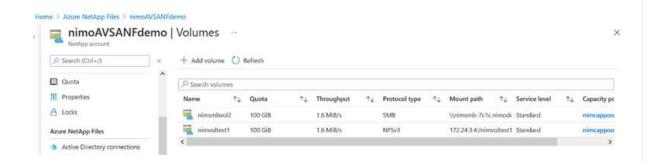
4. Add an SMB volume by using the Volumes blade under the Capacity Pools blade. Make sure the Active Directory connector is configured prior to creating the SMB volume.



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

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

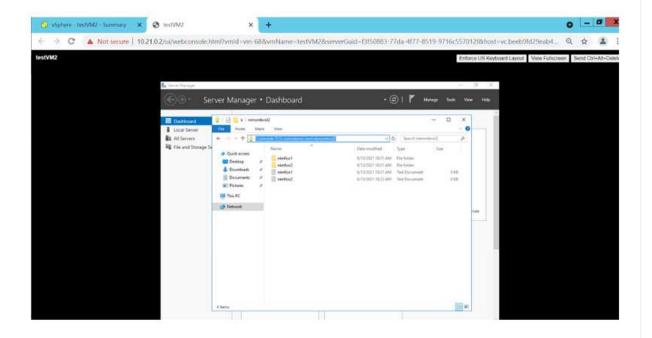




To learn more about Azure NetApp Files volume performance by size or quota, see Performance considerations for Azure NetApp Files.

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.





 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.

```
imoadmin@nimoadmin-virtual-machine:~$ sudo mount -t nfs -o rw,hard,tcp 172.24.
3.4:/nimodemonfsv1 /home/nimoadmin/nimodemo11
nimoadmin@nimoadmin-virtual-machine:-$ df
ilesystem
                          1K-blocks
                                        Used Available Use% Mounted on
udev
                            8168112
                                           0
                                               8168112
                                                         0% /dev
tmpfs
                            1639548
                                        1488
                                               1638060
                                                         1% /run
                           50824704 7902752
                                              40310496
                                                        17% /
/dev/sda5
tmpfs
                             8197728
                                           0
                                               8197728
                                                         0% /dev/shm
tmpfs
                                5120
                                           0
                                                  5120
                                                         0% /run/lock
                                           0
tmpfs
                            8197728
                                               8197728
                                                         0% /sys/fs/cgroup
/dev/loop0
                               56832
                                       56832
                                                     0 100% /snap/core18/2128
/dev/loop2
                              66688
                                       66688
                                                     0 100% /snap/gtk-common-the
nes/1515
/dev/loop1
                                                     0 100% /snap/gnome-3-34-180
                             224256 224256
4/72
/dev/loop3
                              52224
                                       52224
                                                     0 100% /snap/snap-store/547
/dev/loop4
                                                     0 100% /snap/snapd/12704
                               33152
                                       33152
/dev/sda1
                              523248
                                          4
                                                523244
                                                         1% /boot/efi
                             1639544
tmpfs
                                          52
                                                          1% /run/user/1000
                                               1639492
/dev/sr0
                              54738
                                       54738
                                                     0 100% /media/nimoadmin/VMw
are Tools
172.24.3.4:/nimodemonfsv1 104857600
                                           0 104857600
                                                          0% /home/nimoadmin/nimo
demo11
imoadmin@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 you IT staff in all-new methods to manage your data.

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

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

Cloud Volumes ONTAP (CVO) as guest connected storage



Deploy new Cloud Volumes ONTAP in Azure

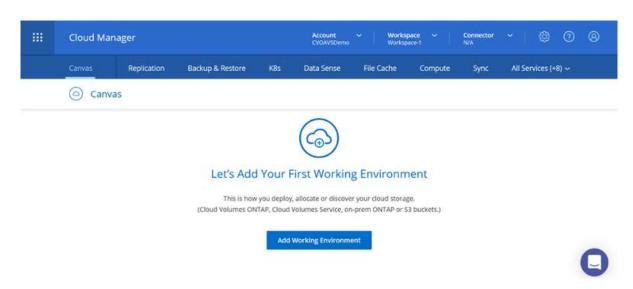
Cloud Volumes ONTAP shares and LUNs can be mounted from VMs that are created in the Azure VMware Solution SDDC environment. The volumes can also be mounted on the Linux client and on Windows client because Cloud Volumes ONTAP supports iSCSI, SMB, and NFS protocols. Cloud Volumes ONTAP volumes can be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

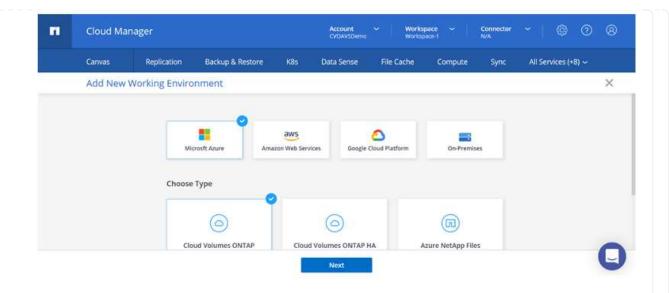


Use Cloud Volumes ONTAP sizer to accurately size the Cloud Volumes ONTAP instances. Also monitor on-premises performance to use as inputs in the Cloud Volumes ONTAP sizer.

 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.

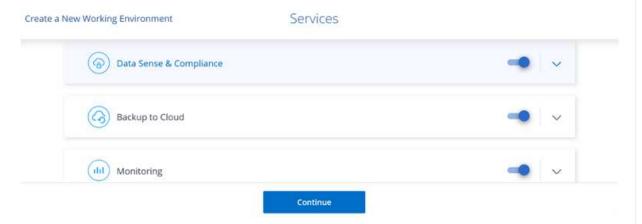


5. Provide the details of the environment to be created including the environment name and admin

credentials. Add resource group tags for the Azure environment as an optional parameter. After you are done, click Continue.



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.



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



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.



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

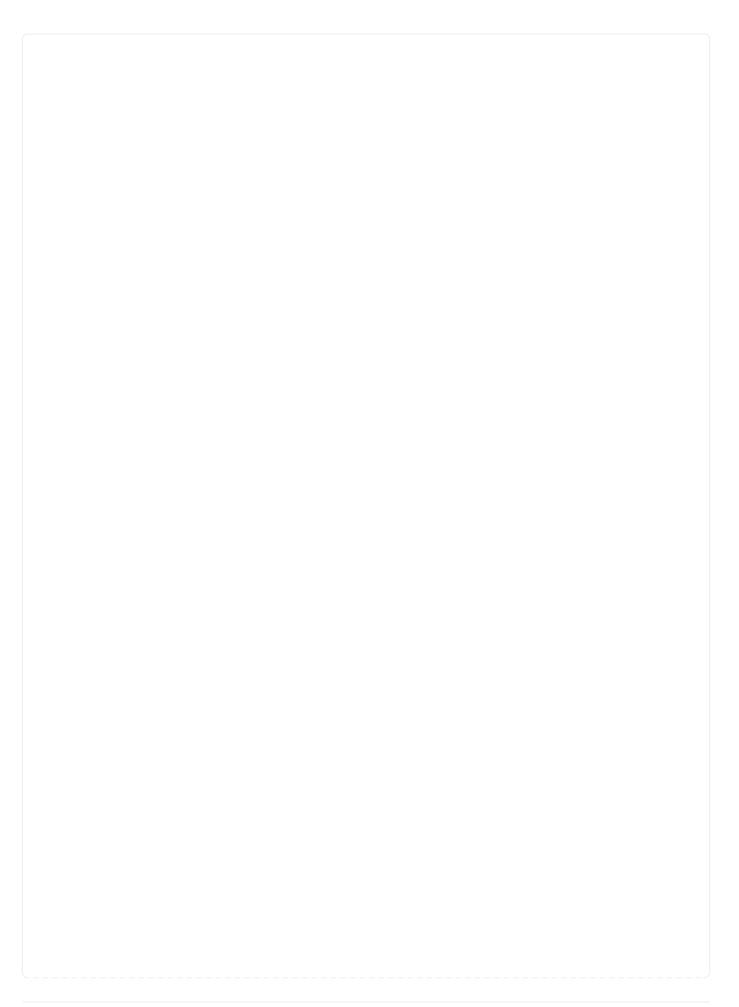


10. Accept the two agreements regarding activating support and allocation of Azure resources. To create the Cloud Volumes ONTAP instance, click Go.



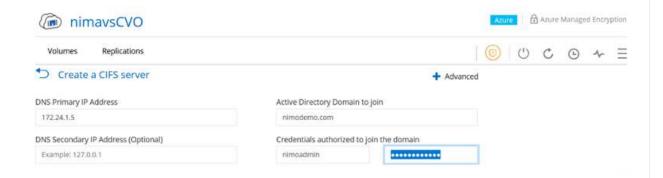
11. After Cloud Volumes ONTAP is provisioned, it is listed in the working environments on the Canvas page.



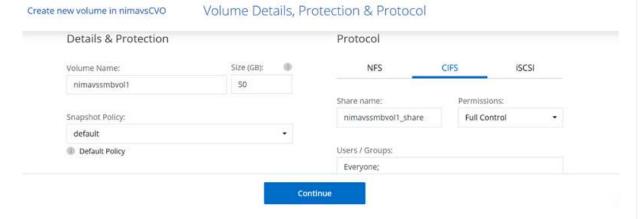


Additional configurations for SMB volumes

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.

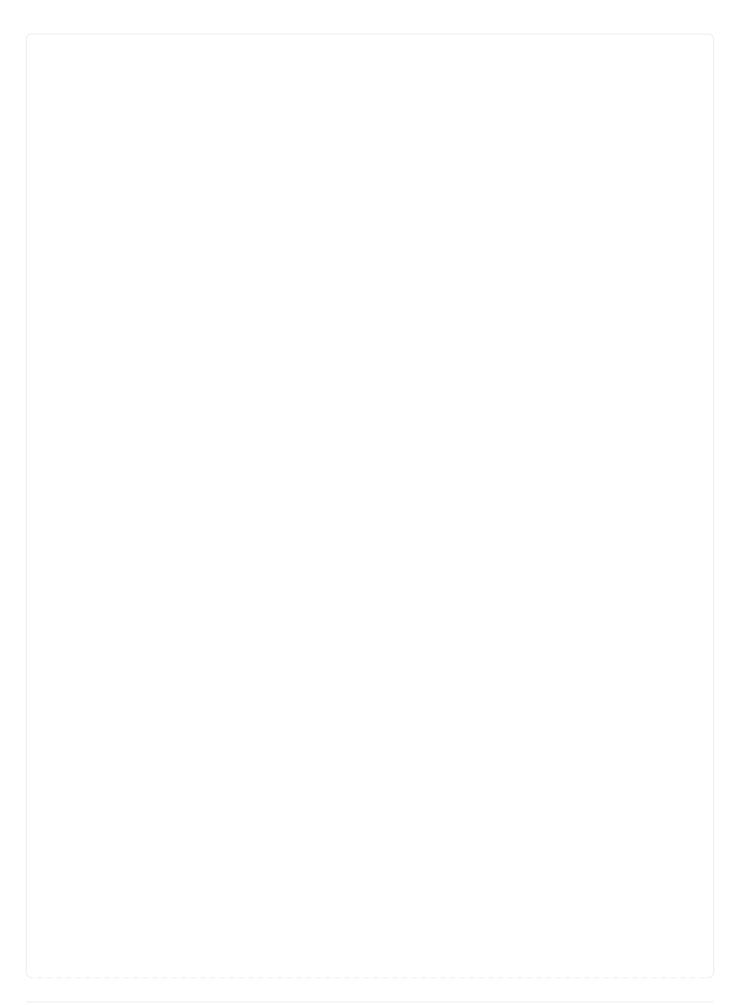


3. After the volume is provisioned, it will be availabe under the Volumes pane. Because a CIFS share is provisioned, give your users or groups permission to the files and folders and verify that those users can access the share and create a file. This step is not required if the volume is replicated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



- 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.

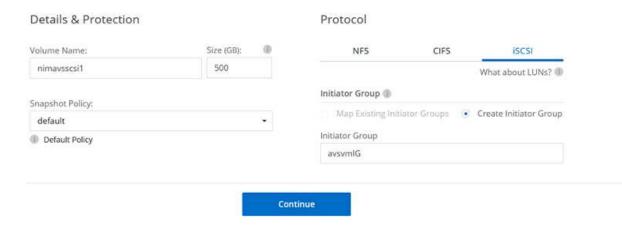




Connect the LUN to a host

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.



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:

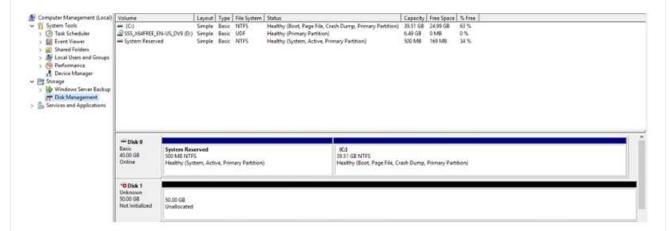
- a. RDP to the VM hosted on Azure VMware Solution SDDC.
- b. Open the iSCSI Initiator Properties dialog box: Server Manager > Dashboard > Tools > iSCSI Initiator.
- c. From the Discovery tab, click Discover Portal or Add Portal and then enter the IP address of the iSCSI target port.
- d. From the Targets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



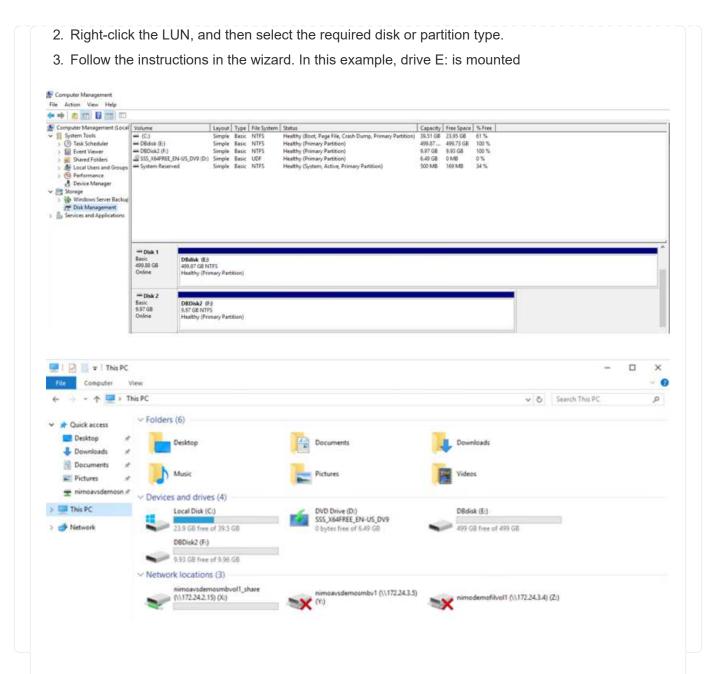
LUNs on storage virtual machine (SVM) appear as disks to the Windows host. Any new disks that are added are not automatically discovered by the host. Trigger a manual rescan to discover the disks by completing the following steps:

- 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.



NetApp Storage Options for GCP

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

Cloud Volumes ONTAP (CVO)

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

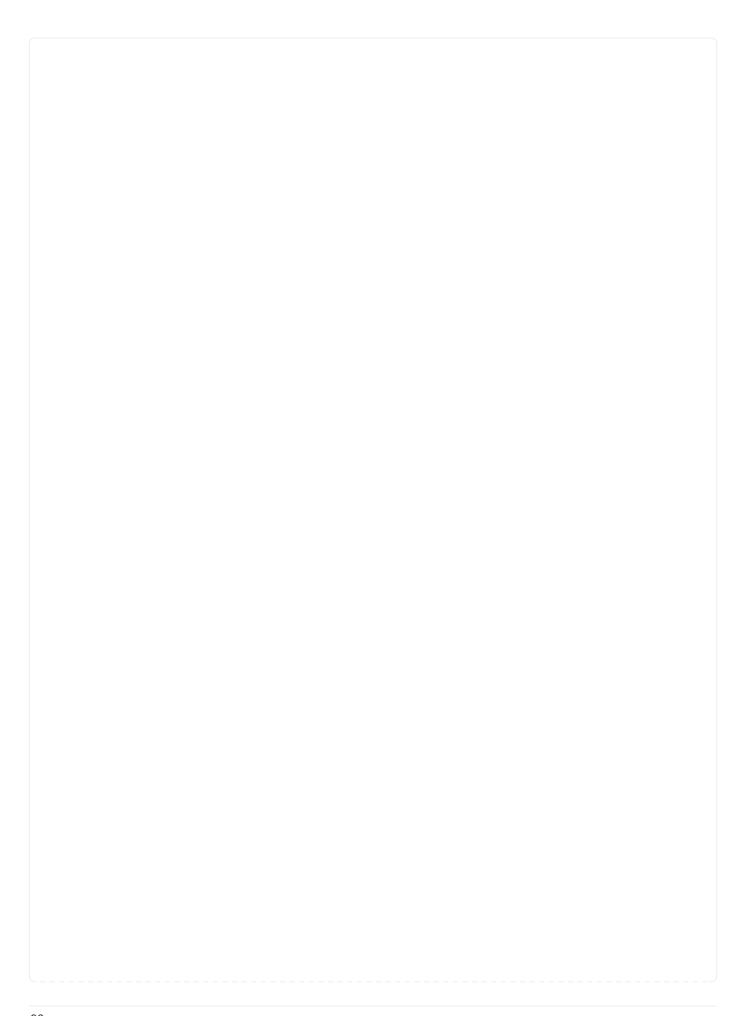
It is a software-defined version of ONTAP that consumes cloud-native storage, allowing you to have the same storage software in the cloud and on-premises, reducing the need to retrain you IT staff in all-new methods to manage your data.

CVO gives customers the ability to seamlessly move data from the edge, to the data center, to the cloud and

back, bringing your hybrid cloud together — all managed with a single-pane management console, NetApp Cloud Manager.

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

Cloud Volumes ONTAP (CVO) as guest connected storage



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

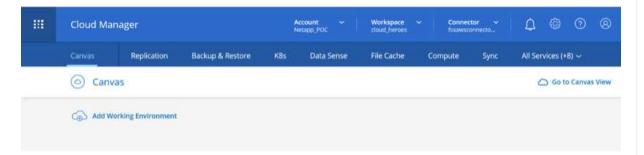
Cloud Volumes ONTAP shares and LUNs can be mounted from VMs that are created in the GCVE private cloud environment. The volumes can also be mounted on the Linux client and on Windows client and LUNS can be accessed on Linux or Windows clients as block devices when mounted over iSCSI because Cloud Volumes 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.

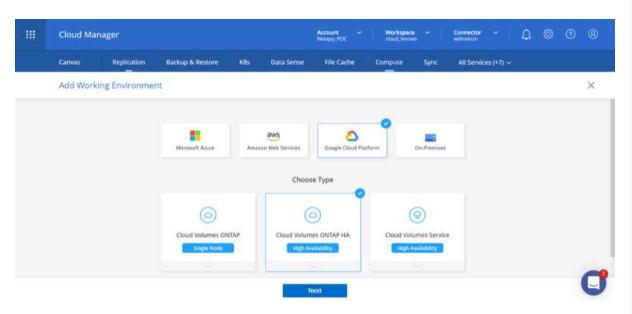


Use Cloud Volumes ONTAP sizer to accurately size the Cloud Volumes ONTAP instances. Also monitor on-premises performance to use as inputs in the Cloud Volumes ONTAP sizer.

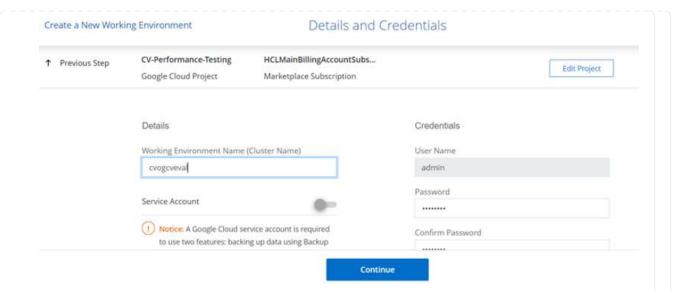
 Log in to NetApp Cloud Central—the Fabric View screen is displayed. Locate the Cloud Volumes ONTAP tab and select Go to Cloud Manager. After you are logged in, the Canvas screen is displayed.



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.

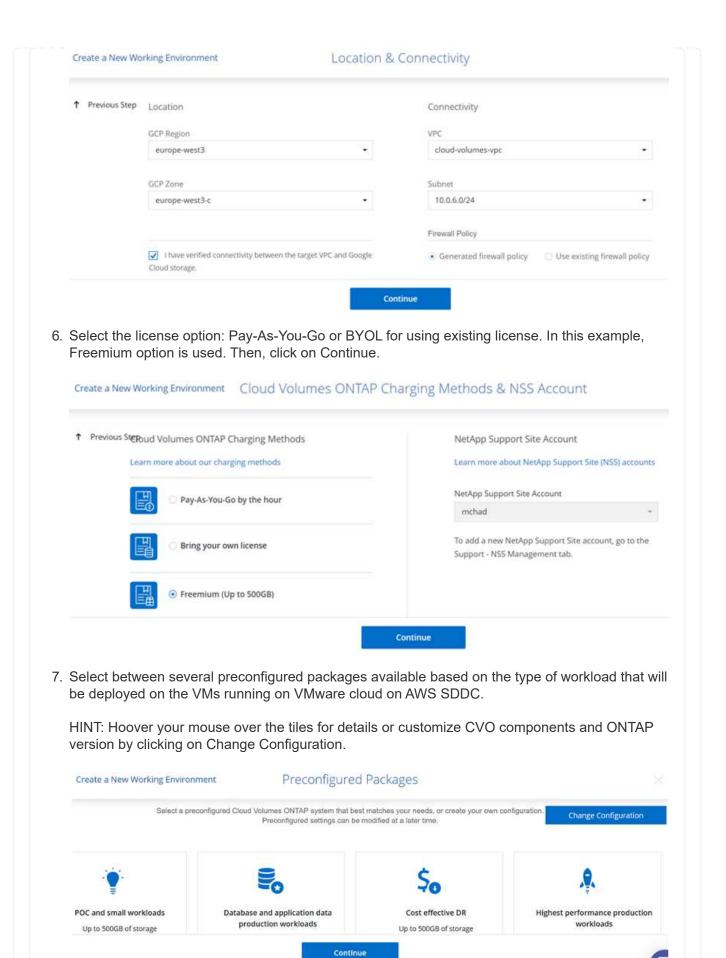


4. Select or deselect the add-on services for Cloud Volumes ONTAP deployment, including Data Sense & Compliance or Backup to Cloud. Then, click Continue.

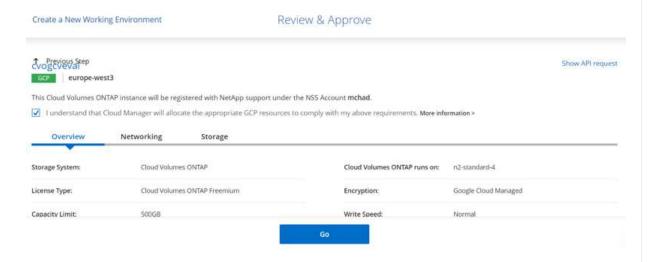
HINT: A verification pop-up message will be displayed when deactivating add-on services. Add-on services can be added/removed after CVO deployment, consider to deselect them if not needed from the beginning to avoid costs.



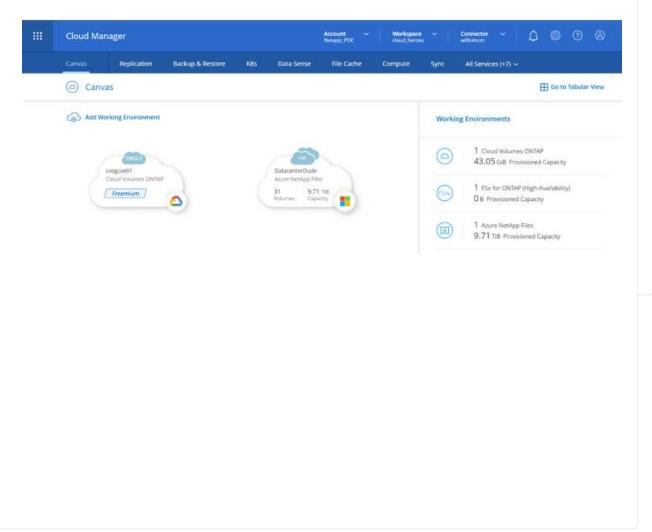
5. Select a location, choose a firewall policy, and select the checkbox to confirm network connectivity to Google Cloud storage.



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



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





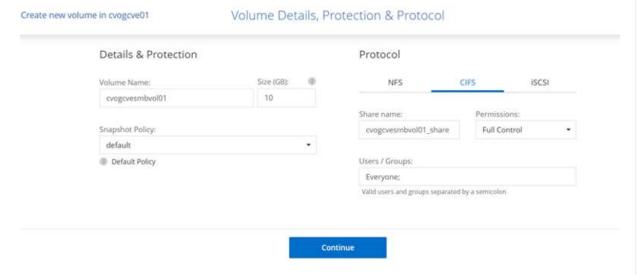
Additional configurations for SMB volumes

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.



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

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



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.



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.

Drive: Y:

Folder: \\10.0.6.251\cvogcvesmbvol01_share

Example: \\server\share

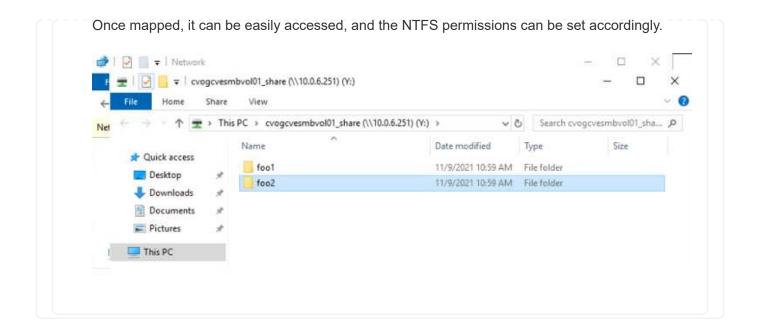
☐ Reconnect at sign-in

☐ Connect using different credentials

Connect to a Web site that you can use to store your documents and pictures.

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







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.



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
                     51M
                             loop
                 0
                           1
                                  /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
         8:1
                 0
                    512M
                           0 part /boot/efi
 -sda1
  -sda2
         8:2
                 0
                           0
                      1K
                            part
 -sda5
         8:5
                   15.5G
                 0
                           0
                            part /
                      1G
                            disk
sdb
         8:16
                 0
                           0
```

```
niyaz@nimubu01: $ df -h
Filesystem
               Size Used Avail Use% Mounted on
udev
               1.9G
                      0 1.9G
                                  0% /dev
                                  1% /run
tmpfs
               394M 1.5M 392M
                16G 7.6G 6.9G 53% /
/dev/sda5
                                  0% /dev/shm
                       0 2.0G
               2.0G
tmpfs
                        0 5.0M
                                  0% /run/lock
tmpfs
               5.0M
               2.0G
tmpfs
                        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
                              0 100% /snap/snap-store/547
                51M
                      51M
/dev/loop0
                56M
                      56M
                              0 100% /snap/core18/2128
/dev/loop4
                33M
                     33M
                              0 100% /snap/snapd/12704
/dev/sda1
                                  1% /boot/efi
               511M 4.0K 511M
                                  1% /run/user/1000
               394M
                      64K
                           394M
tmpfs
/dev/loop5
                33M
                      33M
                              0 100% /snap/snapd/13640
/dev/loop6
                56M
                      56M
                              0 100% /snap/core18/2246
               128K 128K
/dev/loop7
                              0 100% /snap/bare/5
/dev/loop8
                              0 100% /snap/gtk-common-themes/1519
                66M
                      66M
/dev/sdb
               976M
                     2.6M 907M
                                  1% /mnt
```

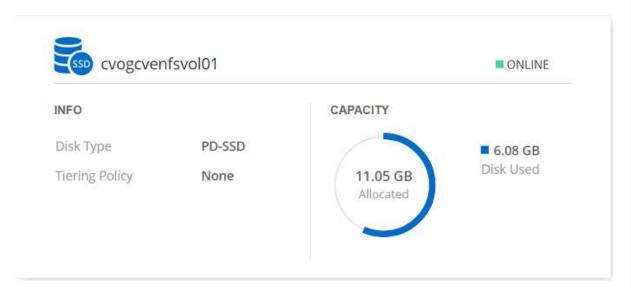


Mount Cloud Volumes ONTAP NFS volume on Linux client

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.



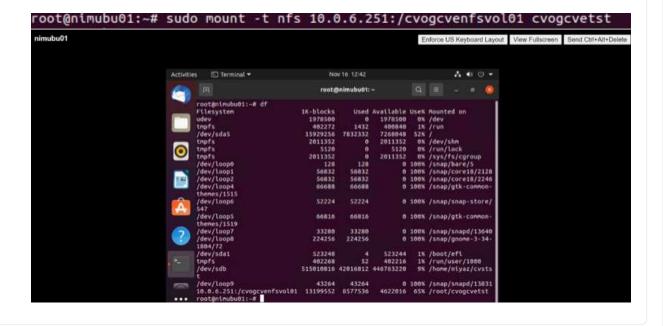
- 4. Click Copy.
- 5. Connect to the designated Linux instance.
- 6. Open a terminal on the instance using secure shell (SSH) and log in with the appropriate credentials.
- 7. Make a directory for the volume's mount point with the following command.

\$ 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



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.



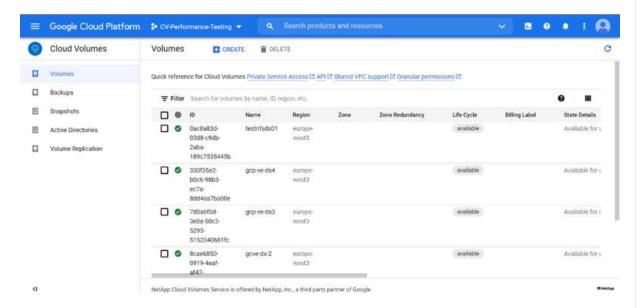
Create a CVS NFS volume to GCVE private cloud

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

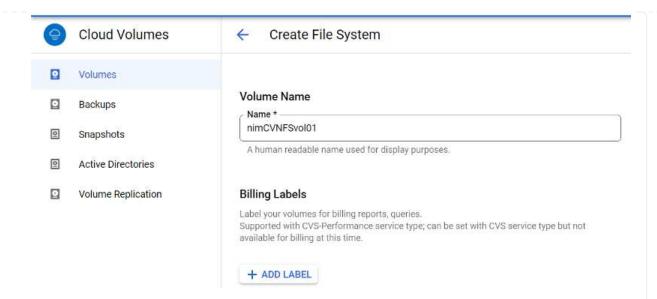
1. Access Cloud Volumes from Partner Solutions within the Google cloud console.



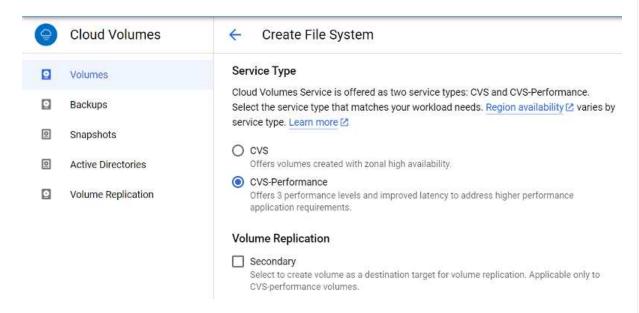
2. In the Cloud Volumes Console, go to the Volumes page and click Create.



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



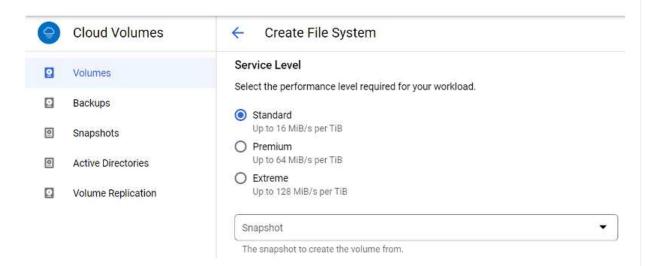
4. Select the appropriate service. For GCVE, choose CVS-Performance and desired service level for improved latency and higher performance based on the application workload requirements.



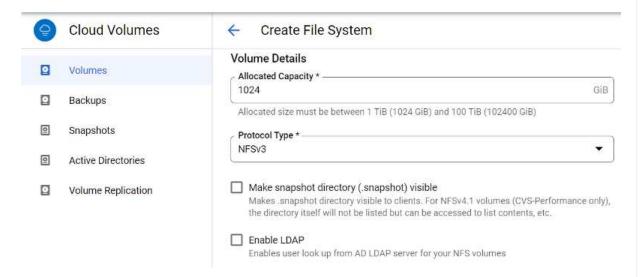
5. Specify the Google Cloud region for the volume and volume path (The volume path must be unique across all of cloud volumes in the project)



6. Select the level of performance for the volume.

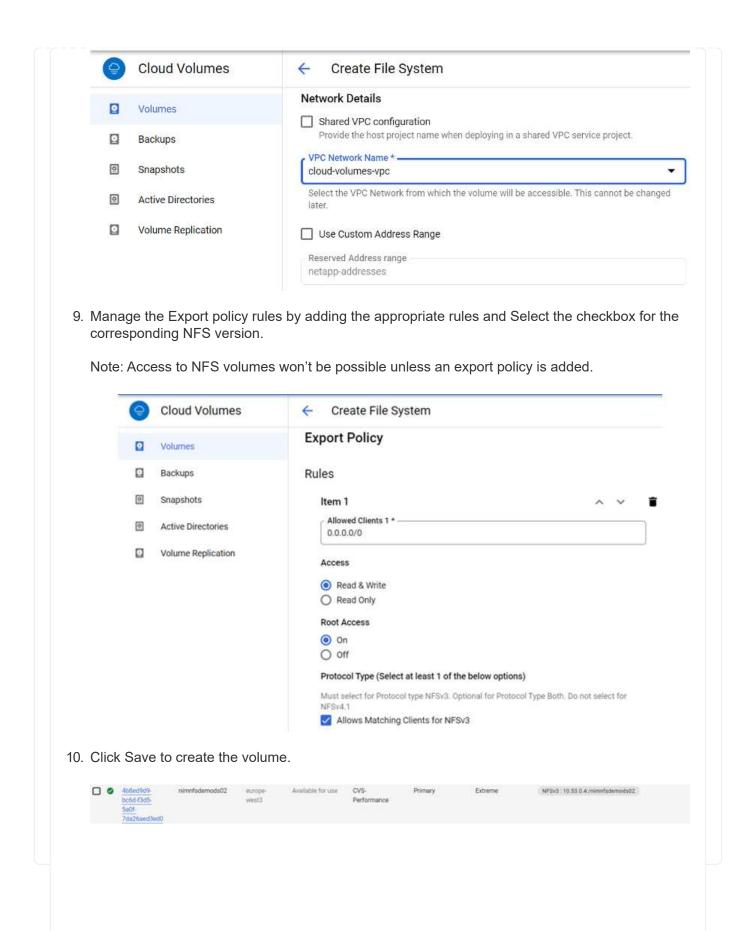


7. Specify the size of the volume and the protocol type. In this testing, NFSv3 is used.



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.





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 "/nimCVSNFSol01":

sudo mkdir /nimCVSNFSol01

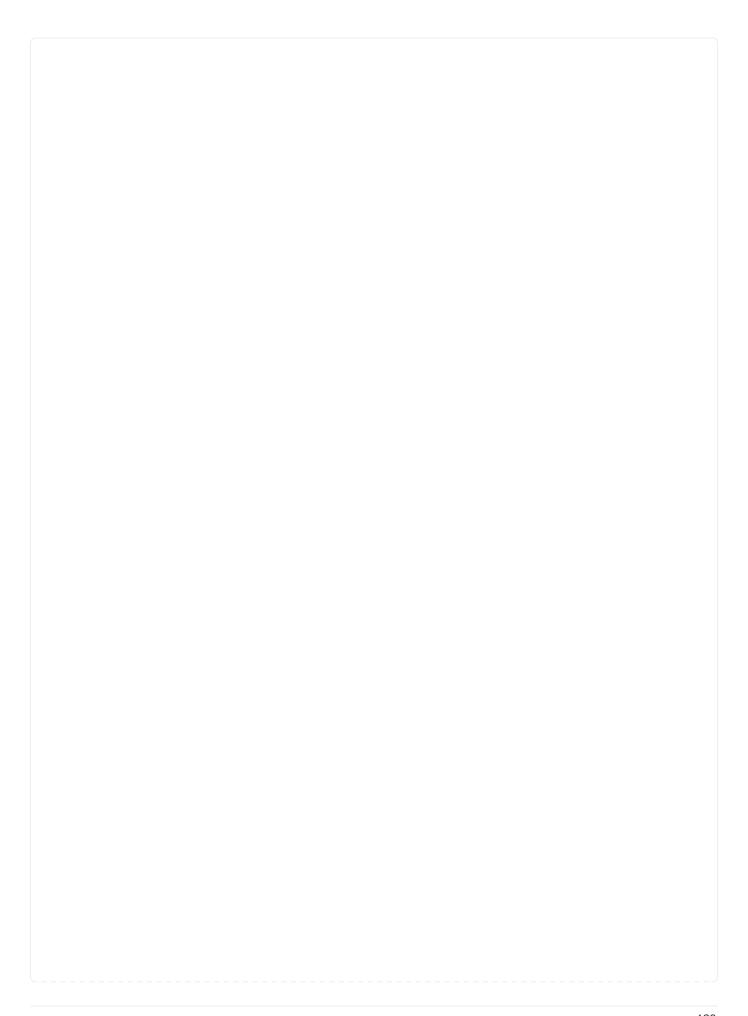


4. Mount the volume using the appropriate command. Example command from the lab is below:

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

root@vm1:-# sudo mkdir nimCVSNFSol01 root@vm1:-# sudo mount -t nfs -o rw,hard,rsize=65536,wsize=65536,vers=3,tcp 10.53.0.4:/nimCVSNFSol01 /nimCVSNFSol01

| root@vm1:~# df | The second second second | | | | |
|-----------------------------|--------------------------|------------|--------------|------|------------------------------|
| ilesystem | 1K-blocks | Used | Available | | Mounted on |
| idev | 16409952 | 0 | 16409952 | 0% | /dev |
| mpfs | 3288328 | 1580 | 3286748 | 1% | /run |
| dev/sdb5 | 61145932 | 19231356 | 38778832 | 34% | |
| mpfs | 16441628 | 0 | 16441628 | 0% | /dev/shm |
| mpfs | 5120 | 0 | 5120 | 0% | /run/lock |
| mpfs | 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 |
| mpfs | 3288324 | 28 | 3288296 | 1% | /run/user/1000 |
| 0.53.0.4:/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 |
| 0.53.0.4:/nimCVSNFSol01 | 107374182400 | 256 | 107374182144 | | /nimCVSNFSol01 |
| oot@vm1:~# | | | | | |



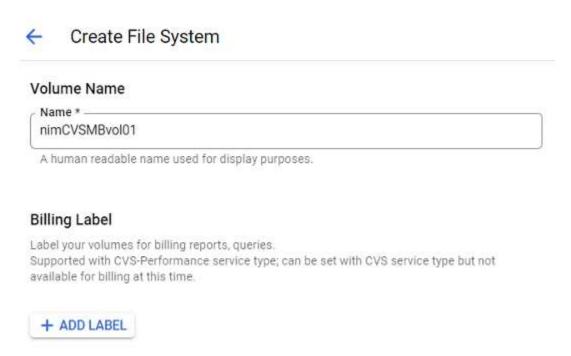
Creating and Mounting SMB Share to VMs running on VMware Engine

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

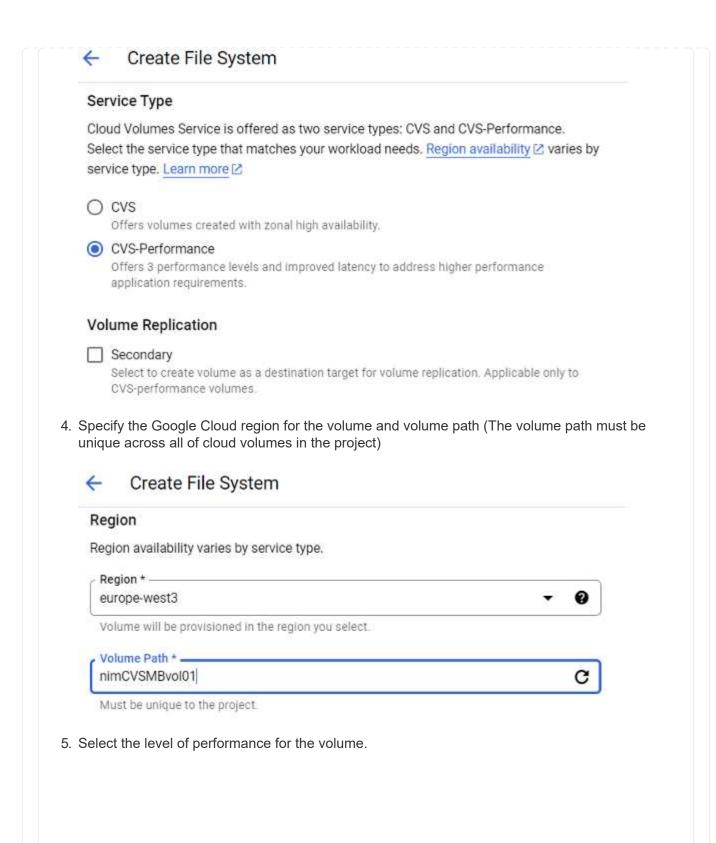


Once the AD connection is in place, create the volume with the desired service level. The steps are like creating NFS volume except selecting the appropriate protocol.

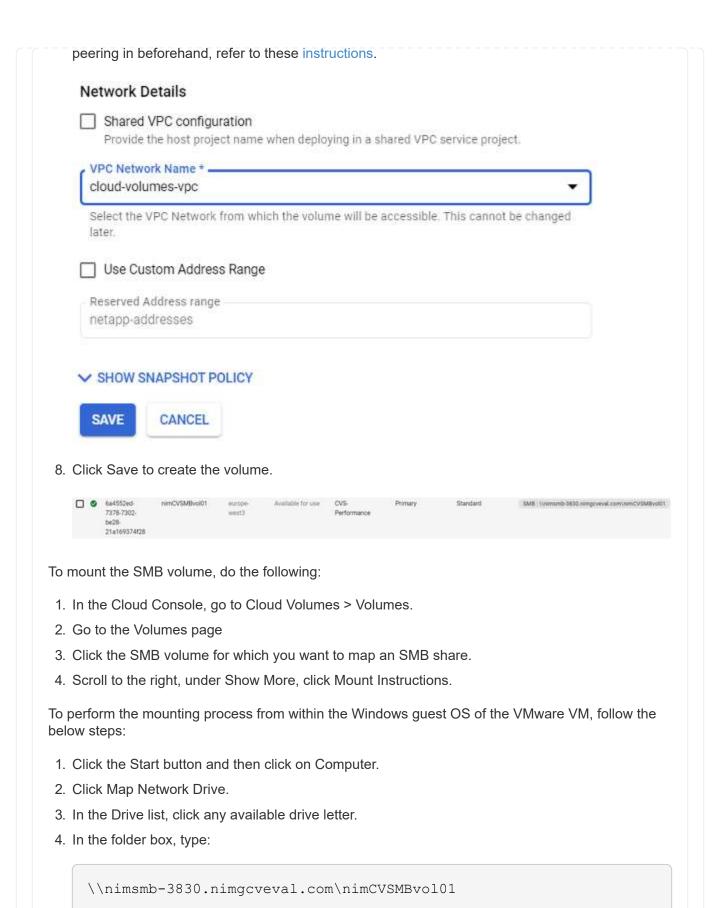
- 1. In the Cloud Volumes Console, go to the Volumes page and click Create.
- 2. On the Create File System page, specify the volume name and billing labels as required for chargeback mechanisms.

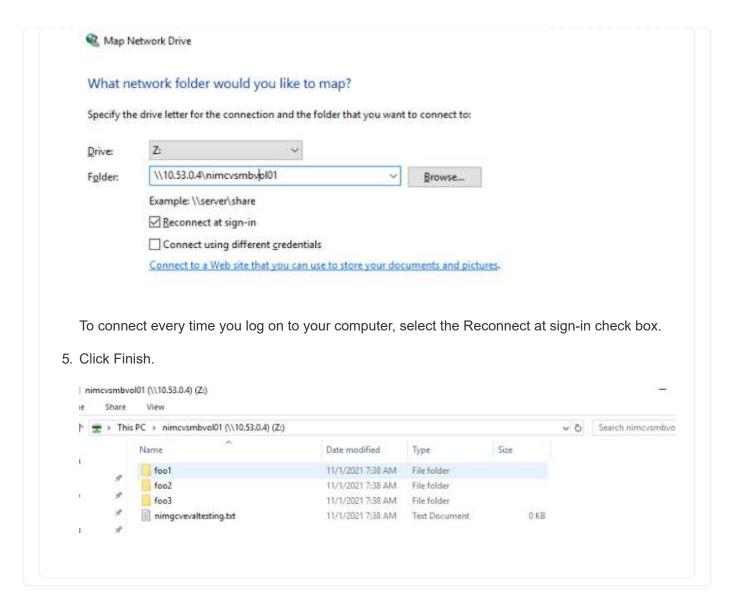


3. Select the appropriate service. For GCVE, choose CVS-Performance and desired service level for improved latency and higher performance based on the workload requirements.









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

Learn more about 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.

Summary and Conclusion: Why NetApp Hybrid Multi-Cloud 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 multi-cloud 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 laaS 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.

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.