

NetApp Storage in Hyperscaler Clouds

NetApp Solutions

NetApp August 03, 2023

This PDF was generated from https://docs.netapp.com/us-en/netapp-solutions/ehc/aws/aws-native-overview.html on August 03, 2023. Always check docs.netapp.com for the latest.

Table of Contents

V	etApp Storage options for Public Cloud Providers	1
	TR-4938: Mount Amazon FSx for ONTAP as a NFS datastore with VMware Cloud on AWS	1
	NetApp Guest Connected Storage Options for AWS	3
	Overview of ANF Datastore Solutions	. 32
	NetApp Guest Connected Storage Options for Azure	. 34
	Google Cloud VMware Engine Supplemental NFS Datastore with NetApp Cloud Volume Service	. 51
	NetApp Storage Options for GCP	. 54
	Region Availability for Supplemental NFS datastores on AWS, Azure, and GCP	. 80

NetApp Storage options for Public Cloud Providers

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

AWS / VMC

AWS supports NetApp storage in the following configurations:

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

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

Azure / AVS

Azure supports NetApp storage in the following configurations:

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

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

GCP / GCVE

Google Cloud supports NetApp storage in the following configurations:

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

View the detailed guest connect storage options for GCVE.

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

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

Niyaz Mohamed, NetApp

Introduction

Every successful organization is on a path of transformation and modernization. As part of this process, companies typically use their existing VMware investments to leverage cloud benefits and exploring how to

migrate, burst, extend, and provide disaster recovery for processes as seamlessly as possible. Customers migrating to the cloud must evaluate the use cases for elasticity and burst, data-center exit, data-center consolidation, end-of-life scenarios, mergers, acquisitions, and so on.

Although VMware Cloud on AWS is the preferred option for the majority of the customers because it delivers unique hybrid capabilities to a customer, limited native storage options have restricted its usefulness for organizations with storage-heavy workloads. Because storage is directly tied to hosts, the only way to scale storage is to add more hosts, which can increase costs by 35-40% or more for storage intensive workloads. These workloads need additional storage and segregated performance, not additional horsepower, but that means paying for additional hosts. This is where the recent integration of FSx for ONTAP comes in handy for storage and performance intensive workloads with VMware Cloud on AWS.

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

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



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

Connectivity options



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

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



The high-level deployment steps are as follows:

- 1. Create Amazon FSx for ONTAP in a new designated VPC.
- 2. Create an SDDC group.
- 3. Create VMware Transit Connect and a TGW attachment.
- 4. Configure routing (AWS VPC and SDDC) and security groups.
- 5. Attach an NFS volume as a datastore to the SDDC cluster.

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



FSx for ONTAP is not currently supported with stretched clusters.

Conclusion

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

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

Amazon FSX for Ontap VMware Cloud

NetApp Guest Connected Storage Options for AWS

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

FSx ONTAP

Amazon FSx for NetApp ONTAP is a fully managed service that provides highly reliable, scalable, 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.

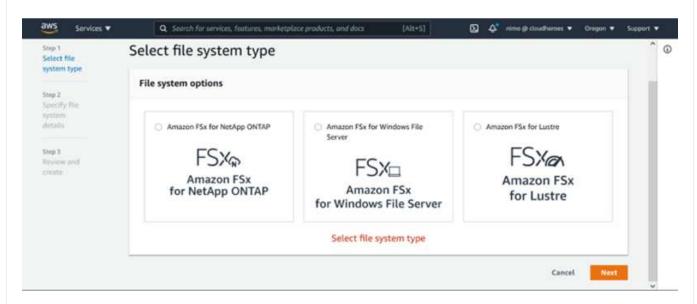


Amazon FSx for NetApp ONTAP and VMware Cloud on AWS must be in the same availability zone to achieve better performance and avoid data transfer charges between availability zones.

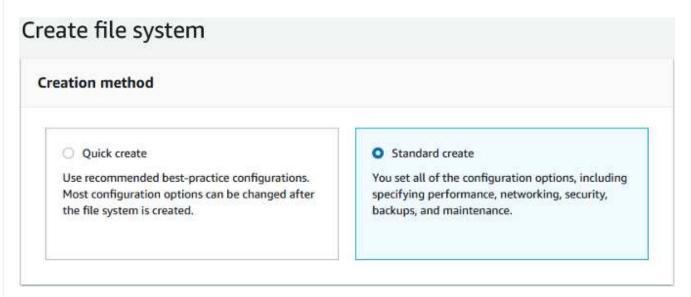
Create and mount Amazon FSx for ONTAP volumes

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

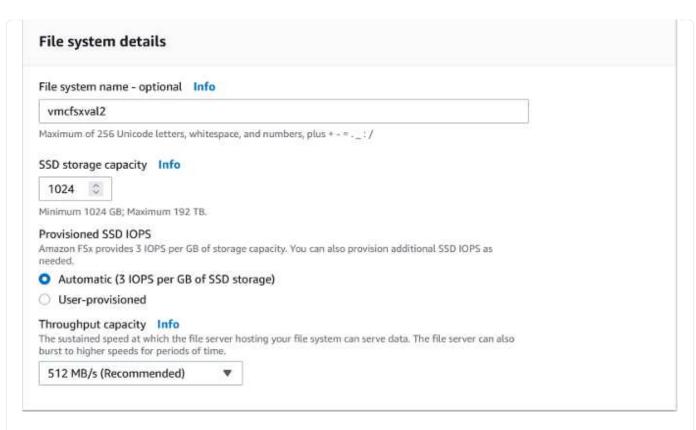
- 1. Open the Amazon FSx console and choose Create file system to start the file system creation wizard.
- 2. On the Select File System Type page, choose Amazon FSx for NetApp ONTAP, and then choose Next. The Create File System page appears.



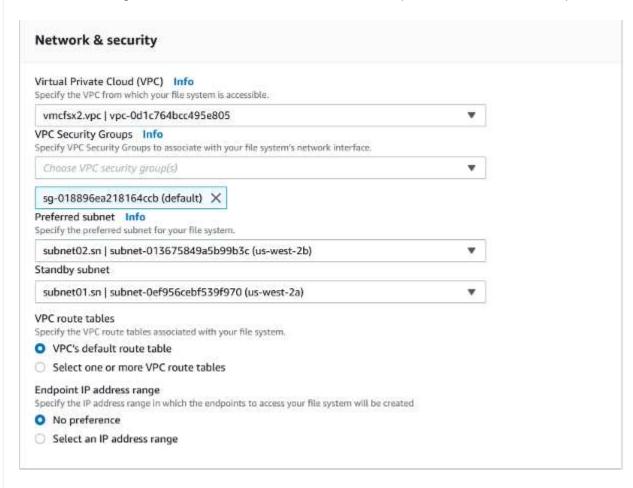
1. In the Networking section, for Virtual Private Cloud (VPC), choose the appropriate VPC and preferred subnets along with the route table. In this case, vmcfsx2.vpc is selected from the dropdown.



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



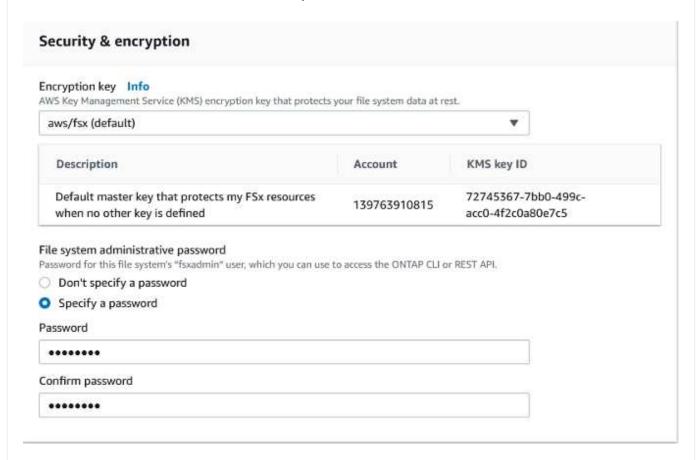
1. In the Networking section, for Virtual Private Cloud (VPC), choose the appropriate VPC and preferred subnets along with the route table. In this case, vmcfsx2.vpc is selected from the dropdown.



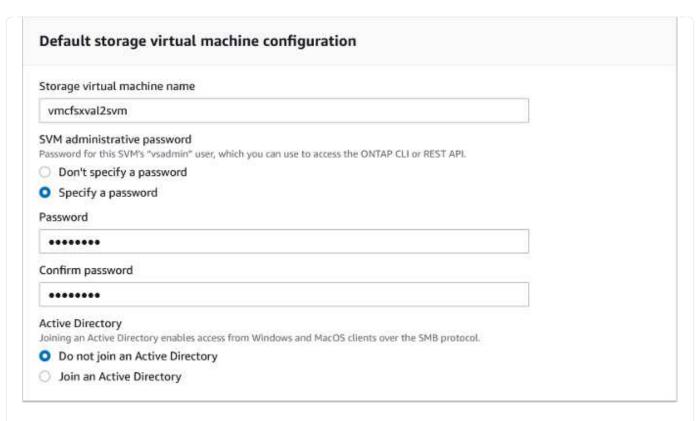


In the Networking section, for Virtual Private Cloud (VPC), choose the appropriate VPC and preferred subnets along with the route table. In this case, vmcfsx2.vpc is selected from the dropdown.

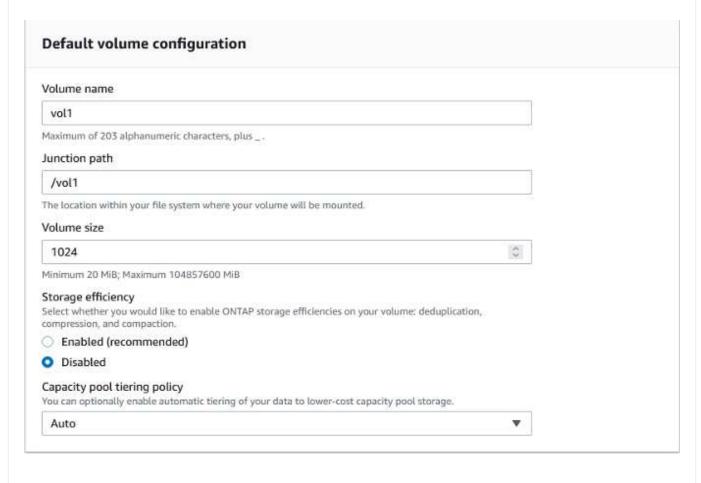
1. In the Security & Encryption section, for the Encryption Key, choose the AWS Key Management Service (AWS KMS) encryption key that protects the file system's data at rest. For the File System Administrative Password, enter a secure password for the fsxadmin user.



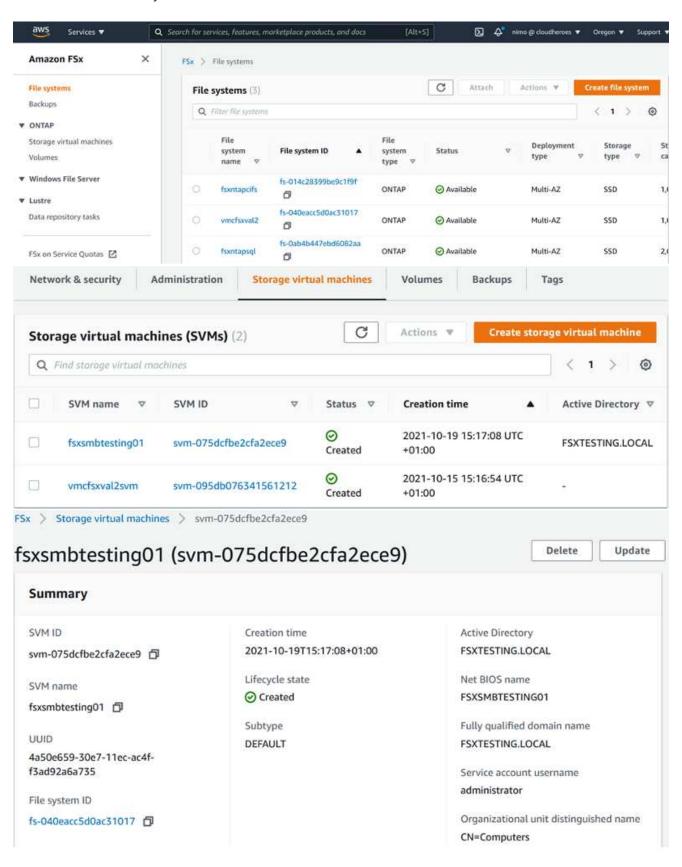
1. In virtual machine and specify the password to use with vsadmin for administering ONTAP using REST APIs or the CLI. If no password is specified, a fsxadmin user can be used for administering the SVM. In the Active Directory section, make sure to join Active Directory to the SVM for provisioning SMB 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.



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



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



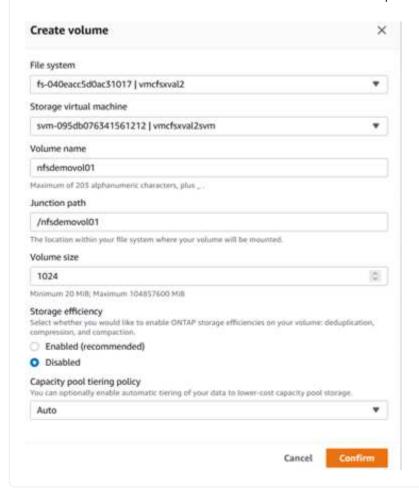
For more detailed information, see Getting started with Amazon FSx for NetApp ONTAP.

9

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:

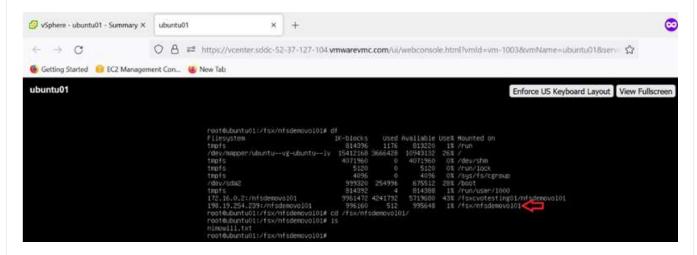
```
$ sudo mkdir /fsx/nfsdemovol01
```

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

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



Mount FSx ONTAP volume on Linux client

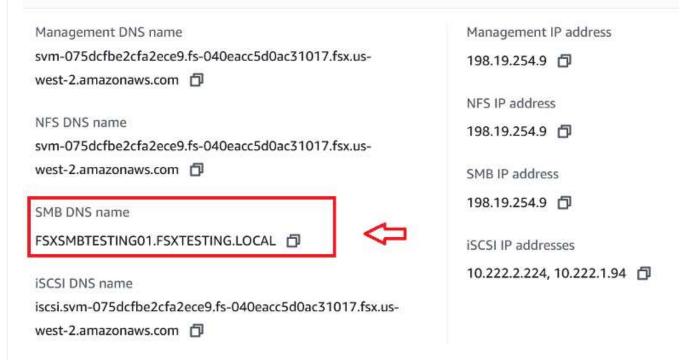
To manage and map file shares on an Amazon FSx file system, the Shared Folders GUI must be used.

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

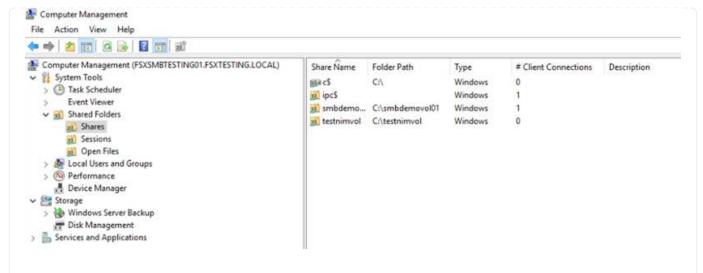


Tp find the SVM's DNS name on the Amazon FSx console, choose Storage Virtual Machines, choose SVM, and then scroll down to Endpoints to find the SMB DNS name. Click OK. The Amazon FSx file system appears in the list for the Shared Folders.

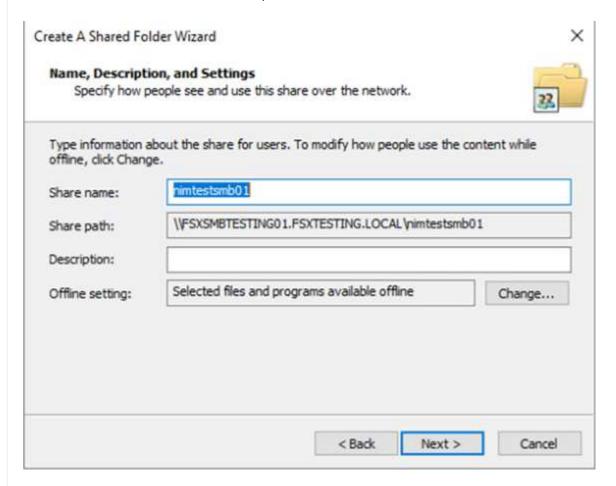
Endpoints

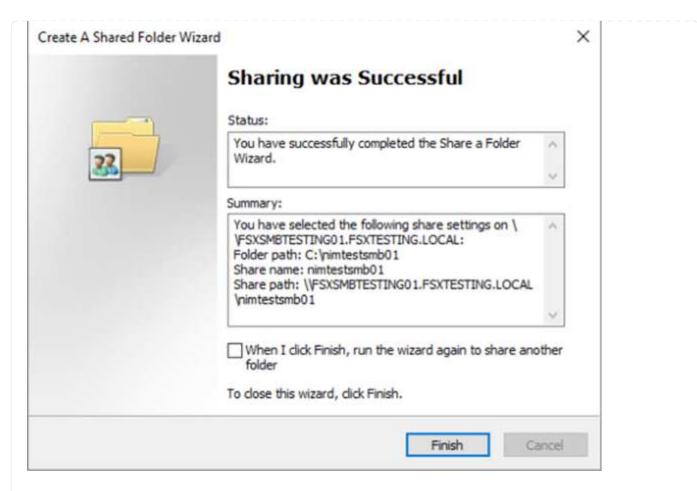


1. In the Shared Folders tool, choose Shares in the left pane to see the active shares for the Amazon FSx file system.



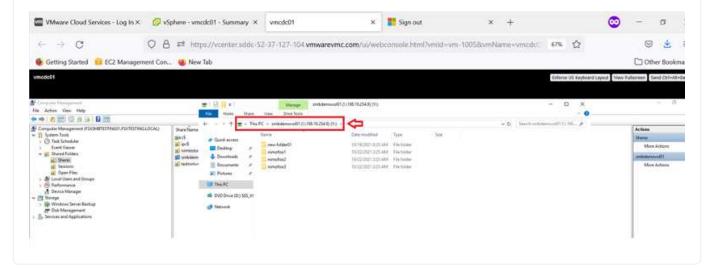
1. Now choose a new share and complete the Create a Shared Folder wizard.





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

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



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

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

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

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

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

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).

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

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

Two entries were displayed.

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

FsxId040eacc5d0ac31017::> lun map -vserver vmcfsxval2svm -path /vol/nimfsxscsivol/nimofsxlun01 -igroup winIG FsxId040eacc5d0ac31017::> lun show Vserver Path State Mapped Type Size vmcfsxval2svm /vol/blocktest01/lun01 online mapped linux 5GB vmcfsxval2svm /vol/nimfsxscsivol/nimofsxlun01 online mapped windows 5GB

Two entries were displayed.

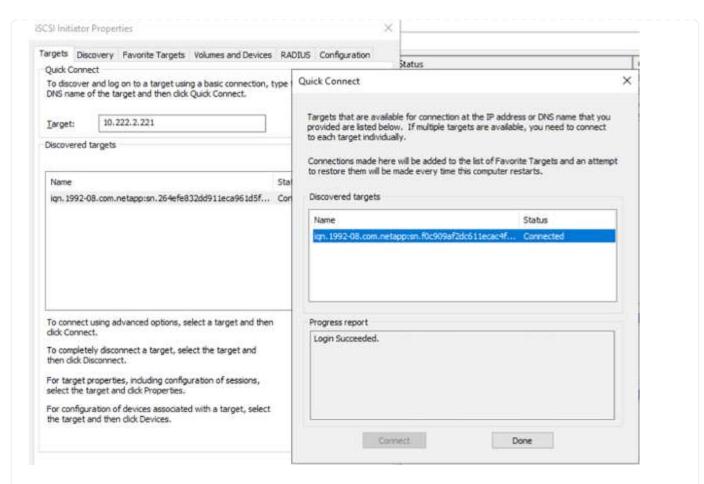
1. Connect the newly provisioned LUN to a Windows VM:

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

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

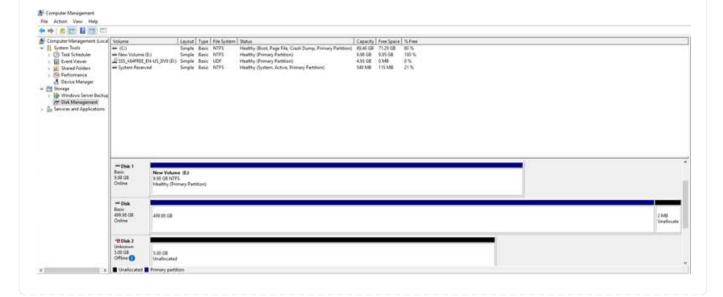


The Windows host must have an iSCSI connection to each node in the cluster. The native DSM selects the best paths to use.



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.



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)

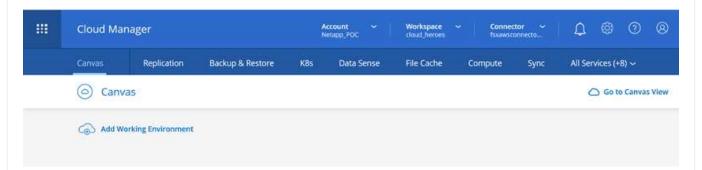
Cloud Volumes ONTAP shares and LUNs can be mounted from VMs that are created in the VMware Cloud on AWS SDDC environment. The volumes can also be mounted on native AWS VM Linux Windows clients, and LUNS can be accessed on Linux or Windows clients as block devices when mounted over iSCSI because Cloud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

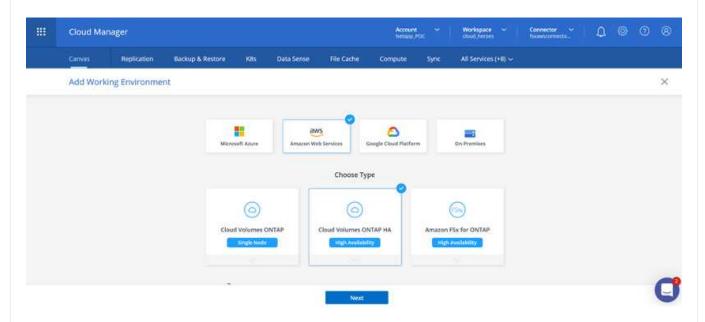


Use the Cloud Volumes ONTAP sizer to accurately size the Cloud Volumes ONTAP instances. Also, monitor on-premises performance to use as inputs in the Cloud Volumes ONTAP sizer.

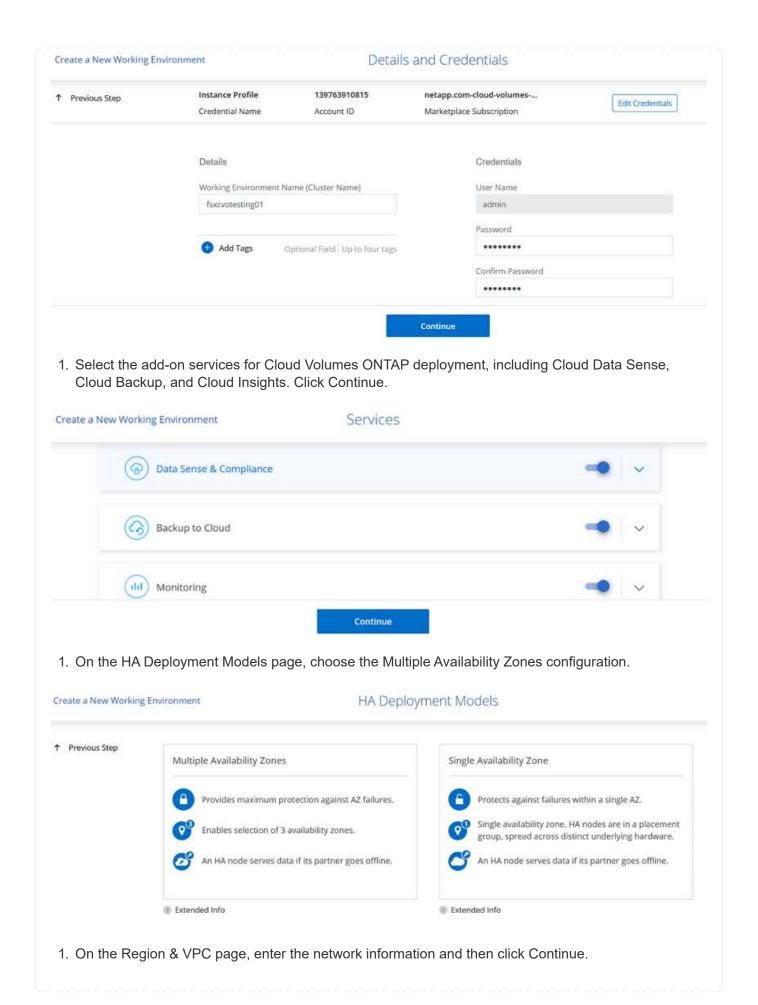
1. Log into NetApp Cloud Central; the Fabric View screen is displayed. Locate the Cloud Volumes ONTAP tab and select Go to Cloud Manager. After you are logged in, the Canvas screen is displayed.

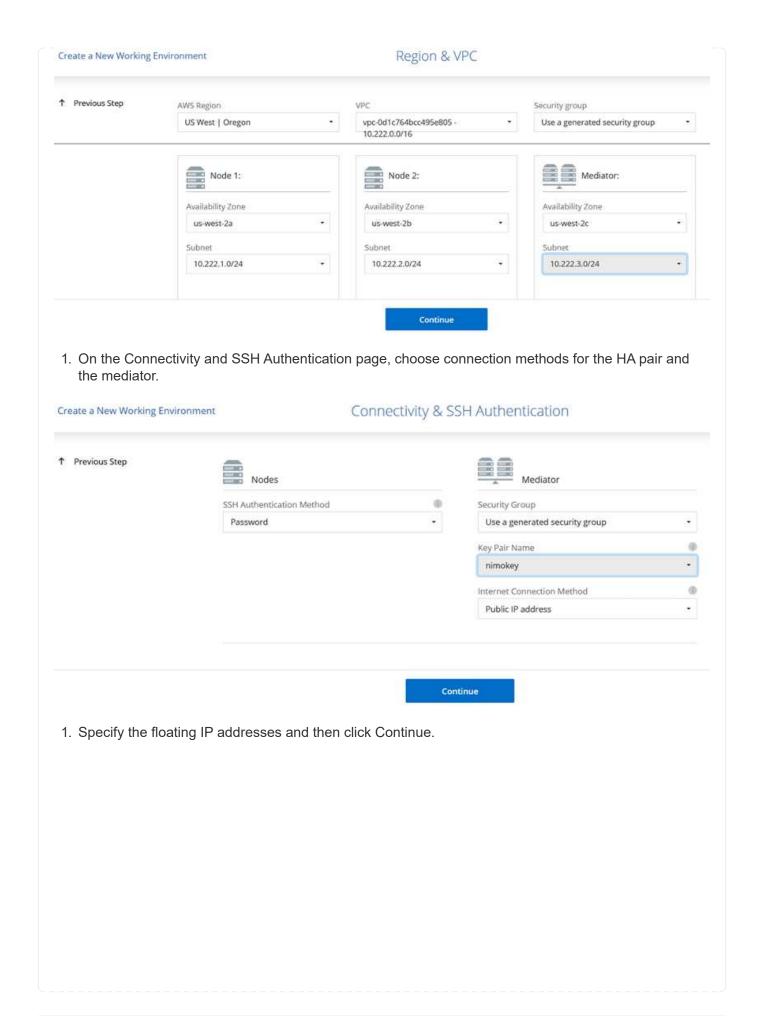


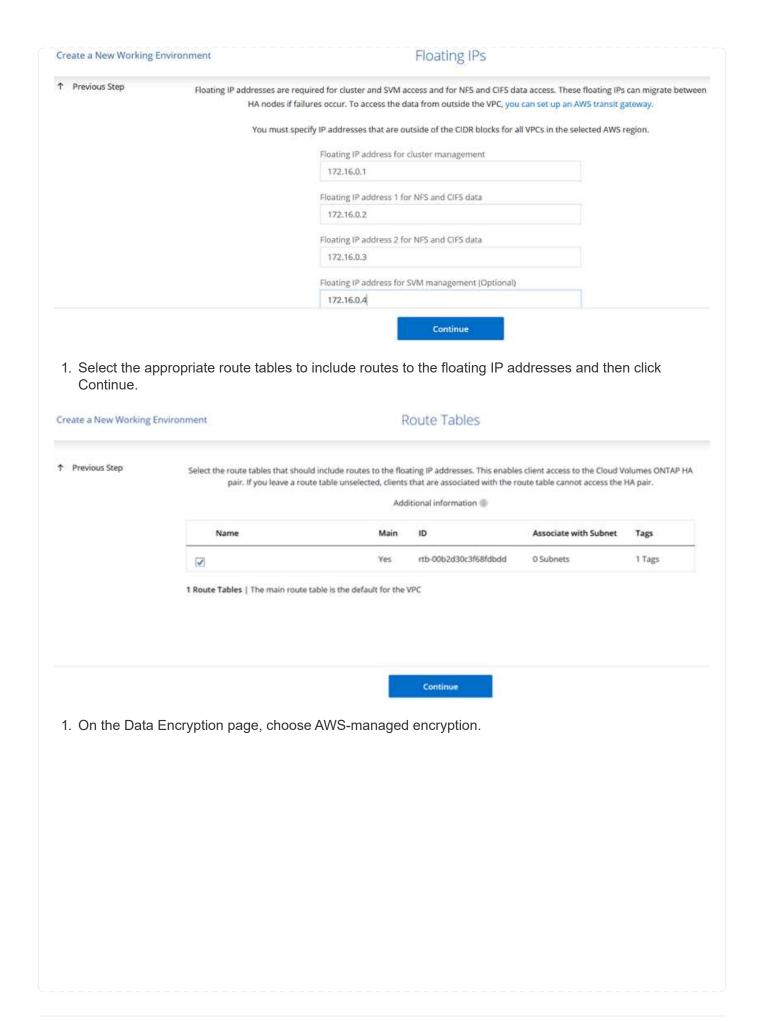
1. On the Cloud Manager home page, click Add a Working Environment and then select AWS as the cloud and the type of the system configuration.

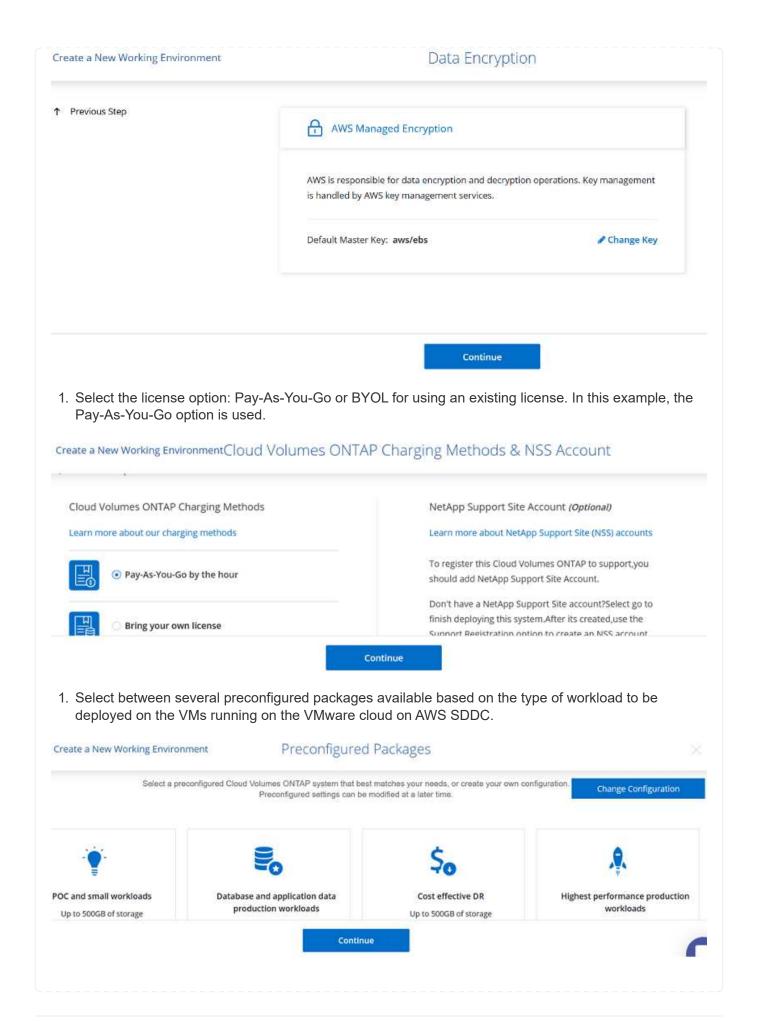


1. Provide the details of the environment to be created including the environment name and admin credentials. Click Continue.

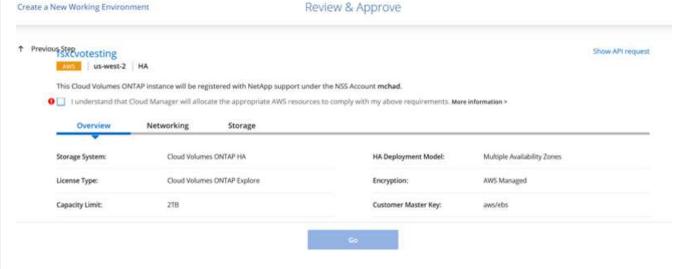








1. On the Review & Approve page, review and confirm the selections. To create the Cloud Volumes ONTAP instance, click Go.

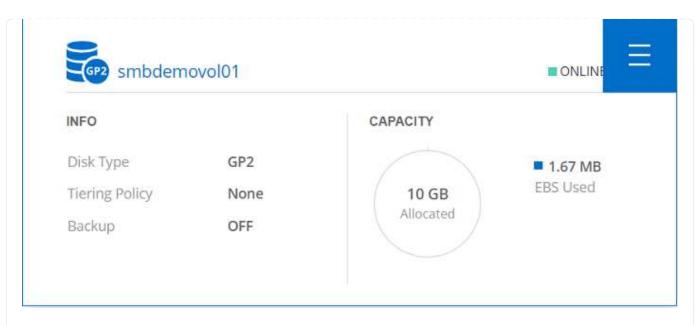


1. After Cloud Volumes ONTAP is provisioned, it is listed in the working environments on the Canvas page.

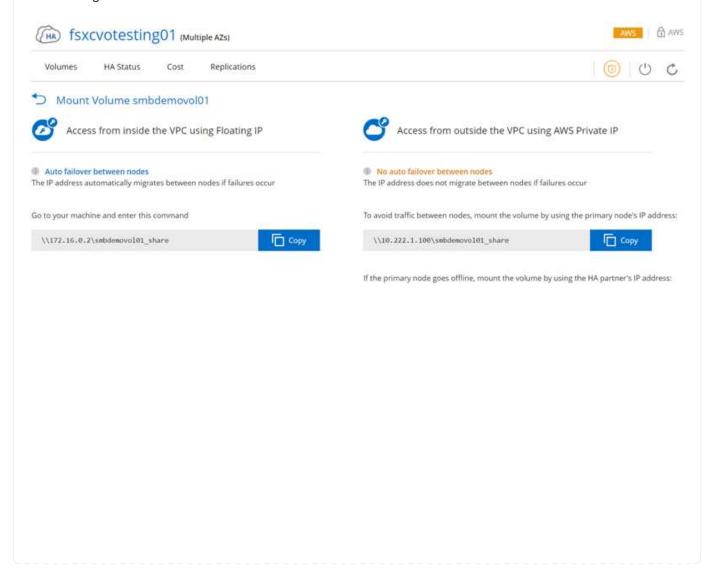


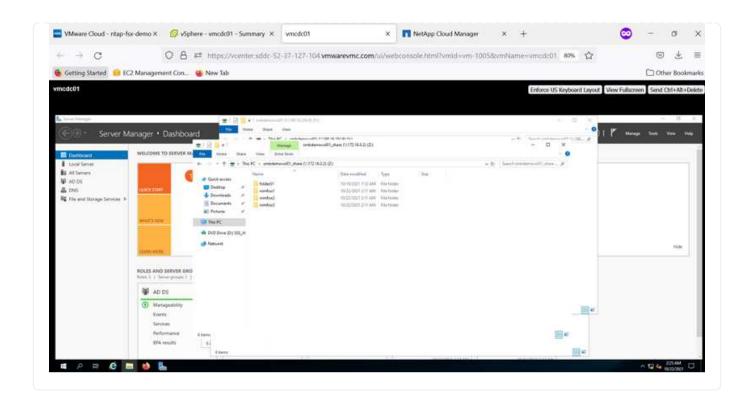
Additional configurations for SMB volumes

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. AWS Managed Encryption (HA) fsxcvotesting01 (Multiple AZs) Volumes HA Status Cost Replications (a) (b) (c) (c) 4 ≡ Create a CIFS server + Advanced DNS Primary IP Address Active Directory Domain to Join 192.168.1.3 fixtesting.local DNS Secondary IP Address (Optional) Credentials authorized to join the domain Example: 127.0.0.1 Username Password Cancel 1. Select the CVO instance to create the volume and click the Create Volume option. Choose the appropriate size and cloud manager chooses the containing aggregate or use advanced allocation mechanism to place on a specific aggregate. For this demo, SMB is selected as the protocol. Volume Details, Protection & Protocol Create new volume in fsxcvotesting01 Details & Protection Protocol Volume Name: Size (GB): NFS CIFS iscsi smbdemovol01 100 Share name: Permissions: Snapshot Policy: smbdemovol01_share Full Control default Default Policy Users / Groups: Everyone; Valid users and groups separated by a semicolon Continue 1. After the volume is provisioned, it is availabe under the Volumes pane. Because a CIFS share is provisioned, you should give your users or groups permission to the files and folders and verify that those users can access the share and create a file.



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

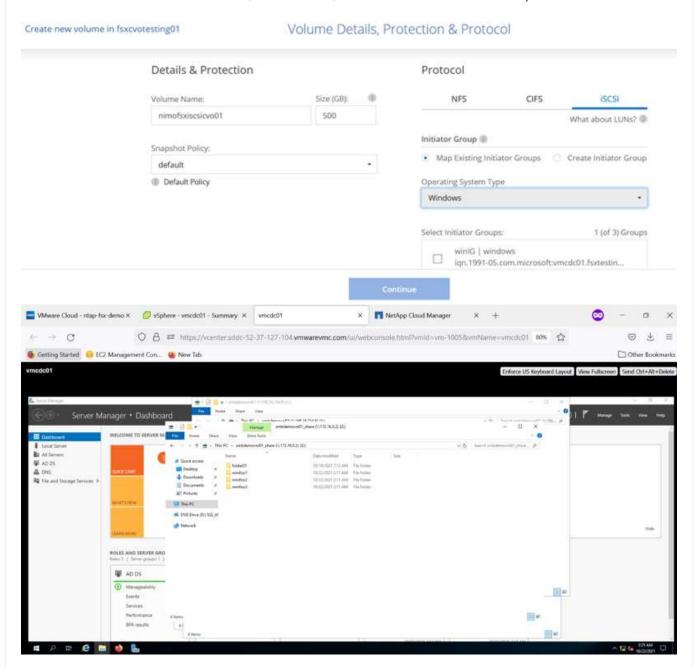




Connect the LUN to a host

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.



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

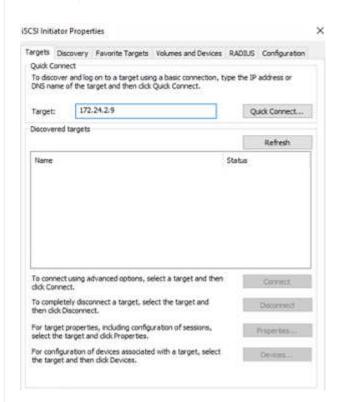
To accomplish the same for the host residing on the VMware Cloud on AWS SDDC, complete the following steps:

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

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

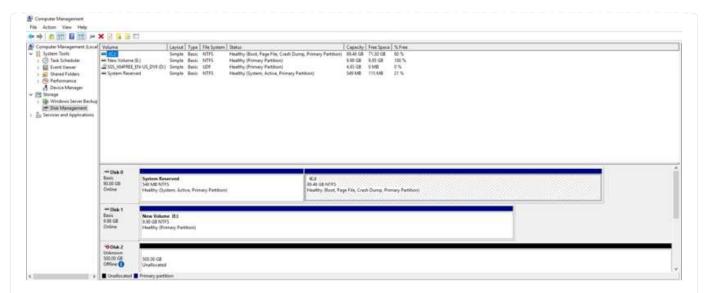


The Windows host must have an iSCSI connection to each node in the cluster. The native DSM selects the best paths to use.



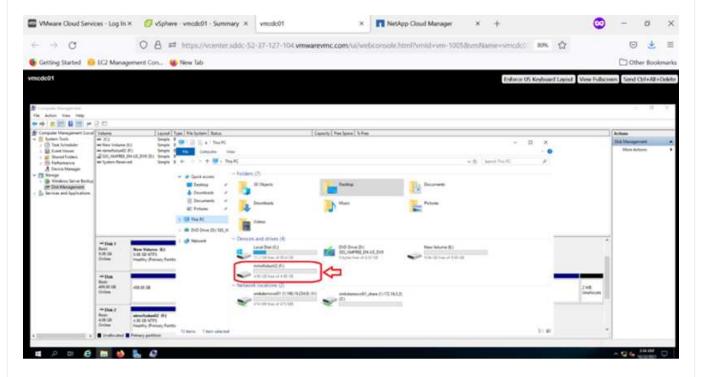
LUNs from the SVM appear as disks to the Windows host. Any new disks that are added are not automatically discovered by the host. Trigger a manual rescan to discover the disks by completing the following steps:

- 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 Isblk cmd from the shell.

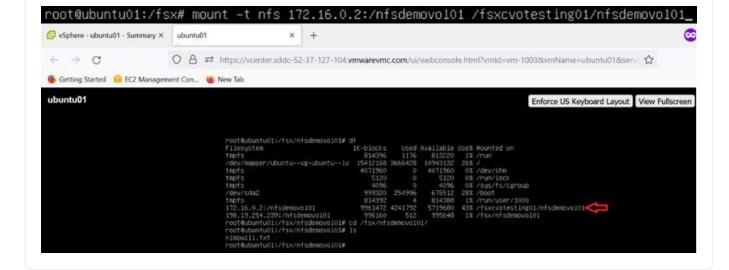
To mount the Cloud Volumes ONTAP (DIY) file system from VMs within VMC on AWS SDDC, complete the following steps:

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

```
$ sudo mkdir /fsxcvotesting01/nfsdemovol01
```

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

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



Overview of ANF Datastore Solutions

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

Use Cases

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

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

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

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

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



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

VMware Cloud options in Azure

Azure VMware Solution

The Azure VMware Solution (AVS) is a hybrid cloud service that provides fully functioning VMware SDDCs within a Microsoft Azure public cloud. AVS is a first-party solution fully managed and supported by Microsoft and verified by VMware that uses Azure infrastructure. Therefore, customers get VMware ESXi for compute virtualization, vSAN for hyper-converged storage, and NSX for networking and security, all while taking advantage of Microsoft Azure's global presence, class-leading data center facilities, and proximity to the rich ecosystem of native Azure services and solutions. A combination of Azure VMware Solution SDDC and Azure NetApp Files provides the best performance with minimal network latency.

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

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

Conclusion

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

Takeaways

The key points of this document include:

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

Where to find additional information

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

Azure VMware Solution documentation

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

Azure NetApp Files documentation

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

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

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

NetApp Guest Connected Storage Options for Azure

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

Azure NetApp Files (ANF)

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

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

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

Because the service is delivered through the Microsoft Azure Portal, users experience a fully managed service as part of their Microsoft enterprise Agreement. World-class support, managed by Microsoft, gives you complete peace of mind. This single solution enables you to quickly and easily add multiprotocol workloads. you can build and deploy both Windows and Linux file-based applications, even for legacy environments.

Azure NetApp Files (ANF) as guest connected storage

Configure Azure NetApp Files with Azure VMware Solution (AVS)

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

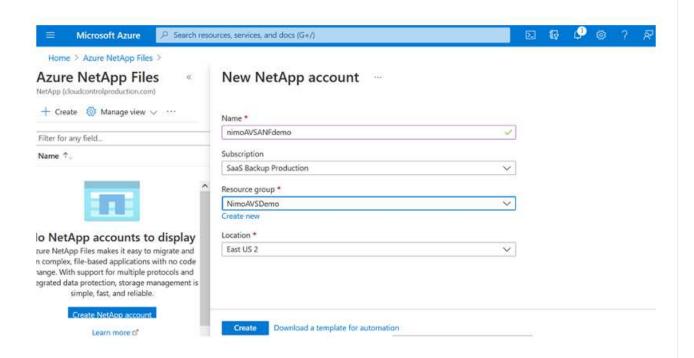
Azure NetApp Files and Azure VMware Solution must be in the same Azure region.

Create and mount Azure NetApp Files volumes

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

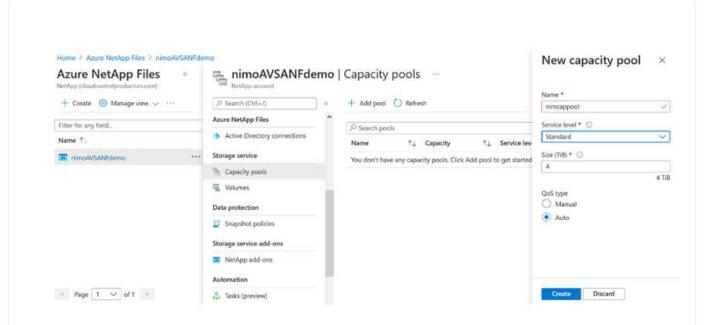
 Log in to the Azure Portal and access Azure NetApp Files. Verify access to the Azure NetApp Files service and register the Azure NetApp Files Resource Provider by using the az provider register --namespace Microsoft.NetApp –wait command. After registration is complete, create a NetApp account.

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

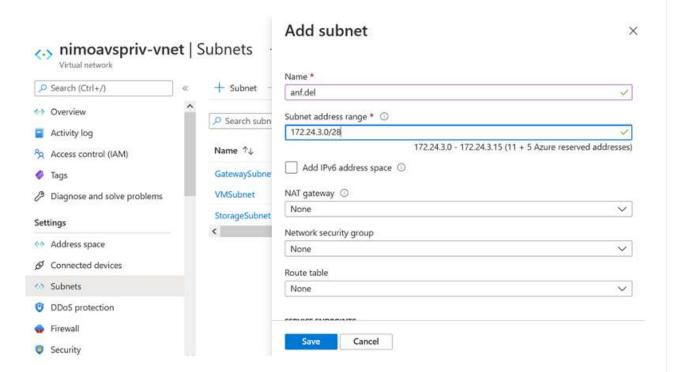


2. After the NetApp account is created, set up the capacity pools with the required service level and size.

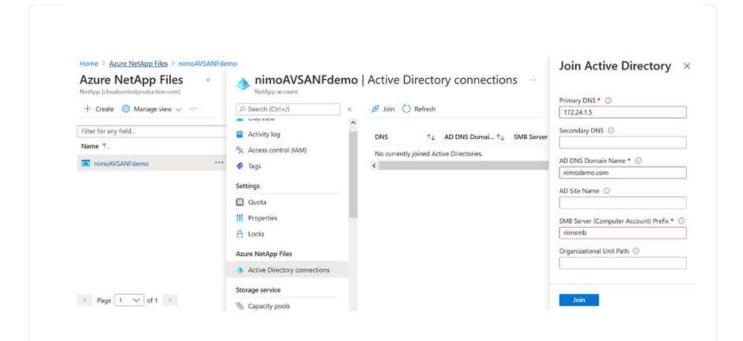
For more information, see Set up a capacity pool.



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.

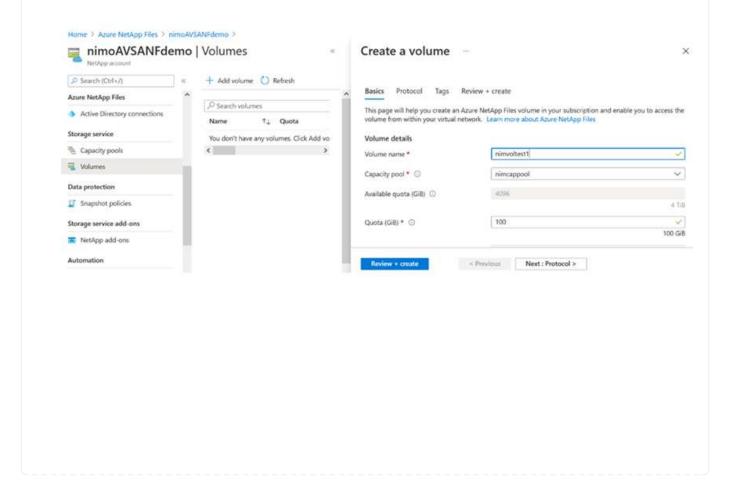


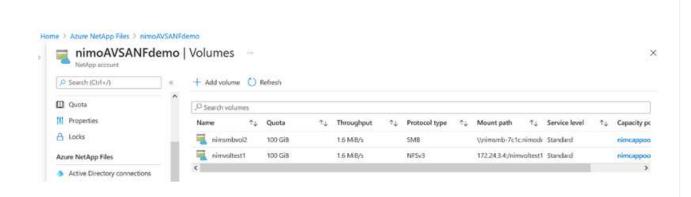
4. Add an SMB volume by using the Volumes blade under the Capacity Pools blade. Make sure the Active Directory connector is configured prior to creating the SMB volume.



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

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

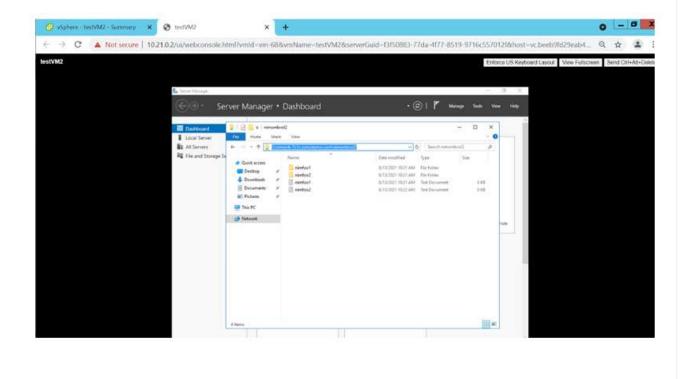


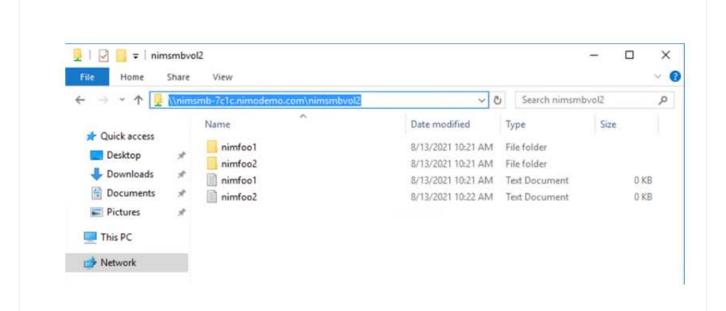


To learn more about Azure NetApp Files volume performance by size or quota, see Performance considerations for Azure NetApp Files.

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.





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

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

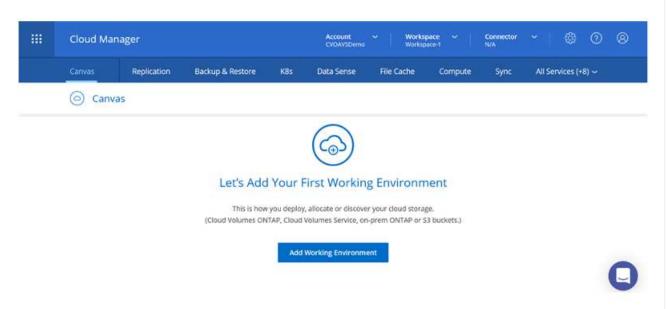
Cloud Volumes ONTAP shares and LUNs can be mounted from VMs that are created in the Azure VMware Solution SDDC environment. The volumes can also be mounted on the Linux client and on Windows client because Cloud Volumes ONTAP supports iSCSI, SMB, and NFS protocols. Cloud Volumes ONTAP volumes can be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

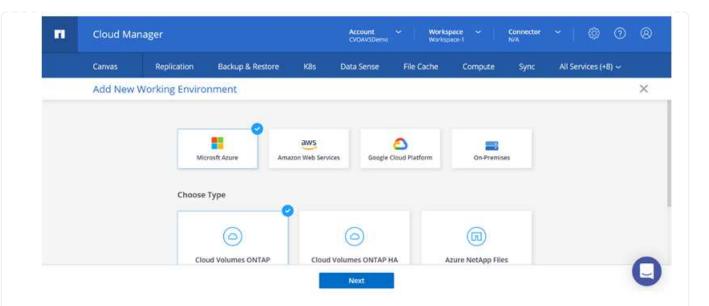


Use Cloud Volumes ONTAP sizer to accurately size the Cloud Volumes ONTAP instances. Also monitor on-premises performance to use as inputs in the Cloud Volumes ONTAP sizer.

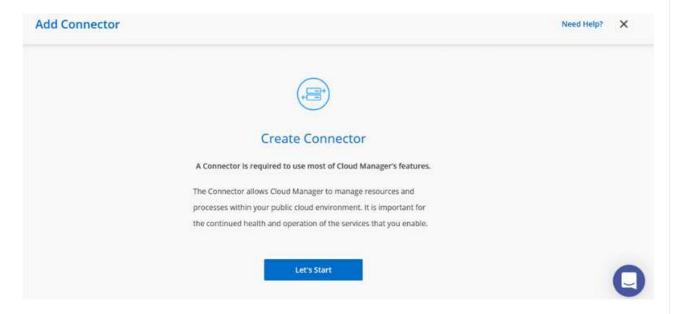
1. Log in to NetApp Cloud Central—the Fabric View screen is displayed. Locate the Cloud Volumes ONTAP tab and select Go to Cloud Manager. After you are logged in, the Canvas screen is displayed.



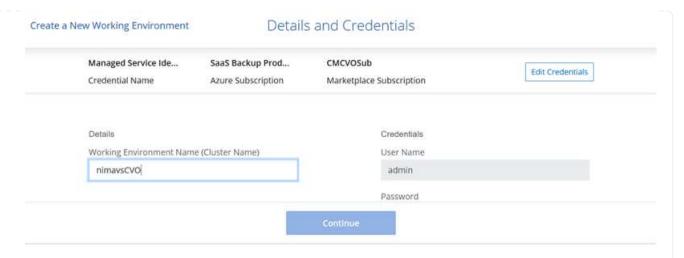
2. On the Cloud Manager home page, click Add a Working Environment and then select Microsoft Azure as the cloud and the type of the system configuration.



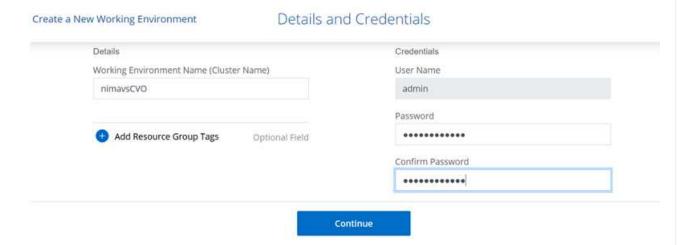
3. When creating the first Cloud Volumes ONTAP working environment, Cloud Manager prompts you to deploy a Connector.



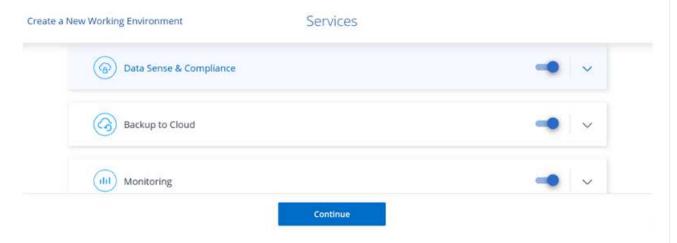
4. After the connector is created, update the Details and Credentials fields.



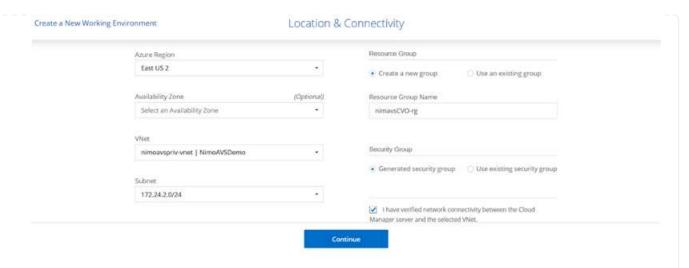
5. Provide the details of the environment to be created including the environment name and admin credentials. Add resource group tags for the Azure environment as an optional parameter. After you are done, click Continue.



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.

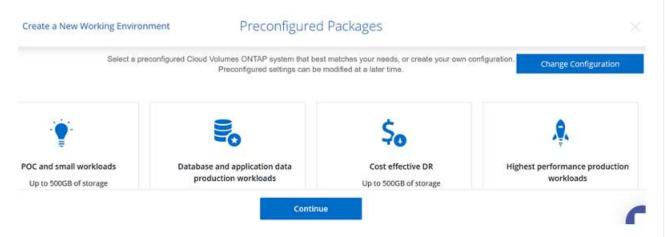


8. Select the license option: Pay-As-You-Go or BYOL for using existing license. In this example, Pay-As-You-Go option is used.

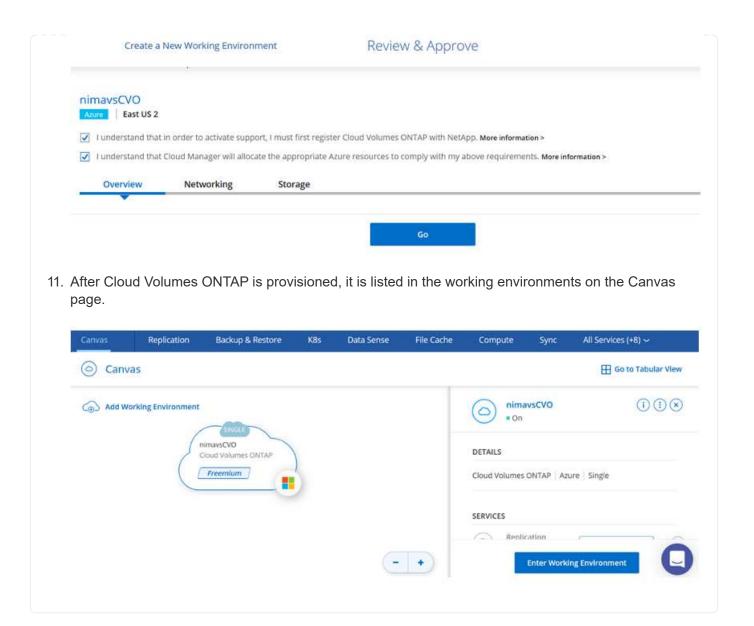
Create a New Working EnvironmentCloud Volumes ONTAP Charging Methods & NSS Account



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.

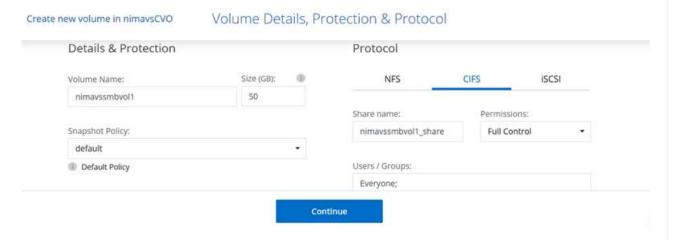


Additional configurations for SMB volumes

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.



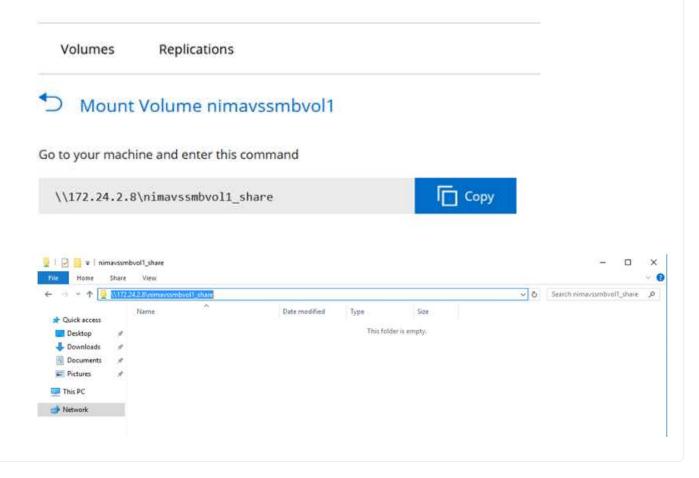
2. Creating the SMB volume is an easy process. Select the CVO instance to create the volume and click the Create Volume option. Choose the appropriate size and cloud manager chooses the containing aggregate or use advanced allocation mechanism to place on a specific aggregate. For this demo, SMB is selected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



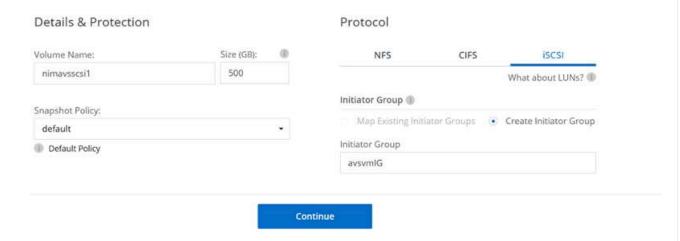
- 4. After the volume is created, use the mount command to connect to the share from the VM running on the Azure VMware Solution SDDC hosts.
- 5. Copy the following path and use the Map Network Drive option to mount the volume on the VM running on Azure VMware Solution SDDC.



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:

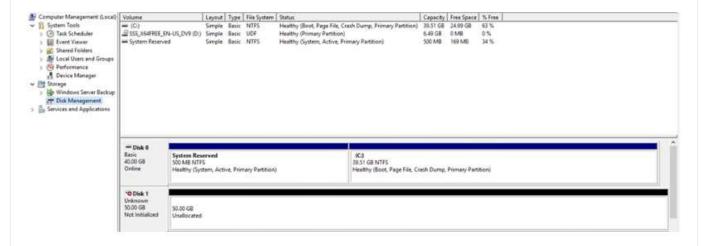
- a. RDP to the VM hosted on Azure VMware Solution SDDC.
- b. Open the iSCSI Initiator Properties dialog box: Server Manager > Dashboard > Tools > iSCSI Initiator.
- c. From the Discovery tab, click Discover Portal or Add Portal and then enter the IP address of the iSCSI target port.
- d. From the Targets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

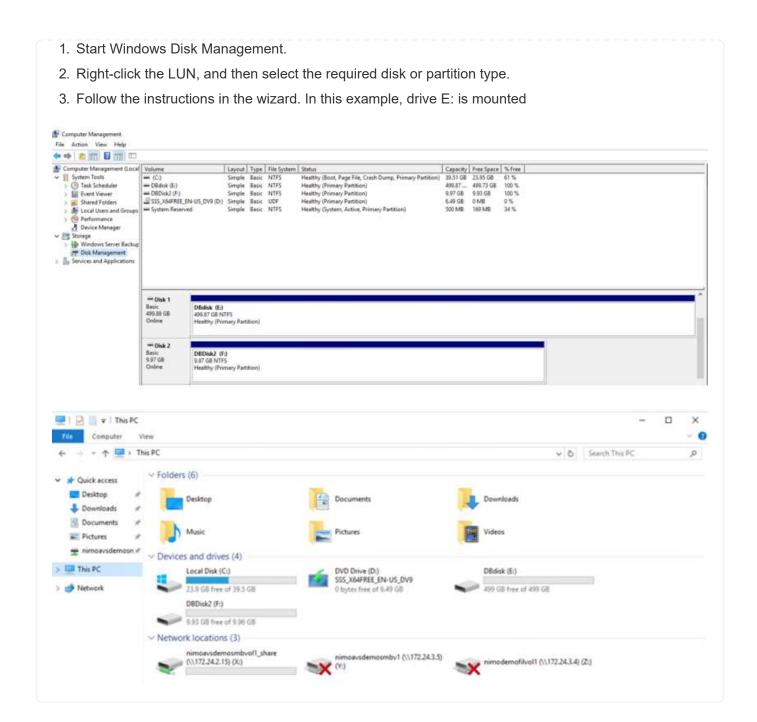


LUNs on storage virtual machine (SVM) appear as disks to the Windows host. Any new disks that are added are not automatically discovered by the host. Trigger a manual rescan to discover the disks by completing the following steps:

- 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:



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

Overview

Authors: Suresh Thoppay, NetApp

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

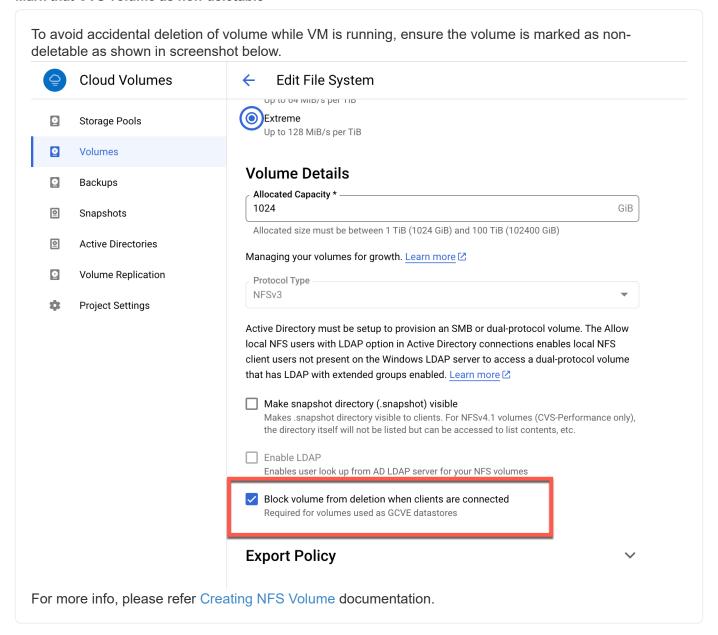


Deployment steps to mount NFS datastore from NetApp CVS on GCVE

Provision CVS-Performance Volume

The NetApp Cloud Volume Service volume can be either provisioned by Using Google Cloud Console Using NetApp BlueXP portal or API

Mark that CVS volume as non-deletable



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

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

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

Mount NFS datastore

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



As vSphere hosts are managed by Google, you don't have access to install NFS vSphere API for Array Integration (VAAI) vSphere Installation Bundle (VIB). If you need support for Virtual Volumes (vVoI), please let us know. If you like to use Jumbo Frames, please refer Maximum supported MTU sizes on GCP

Savings with NetApp Cloud Volume Service

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

Reference Links

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

NetApp Storage Options for GCP

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

Cloud Volumes ONTAP (CVO)

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

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

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

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

Cloud Volumes ONTAP (CVO) as guest connected storage

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

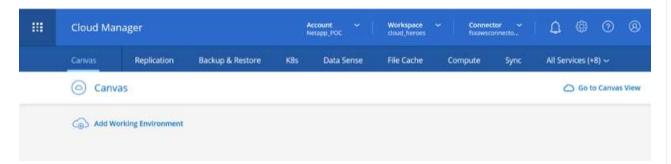
Cloud Volumes ONTAP shares and LUNs can be mounted from VMs that are created in the GCVE private cloud environment. The volumes can also be mounted on the Linux client and on Windows client and LUNS can be accessed on Linux or Windows clients as block devices when mounted over iSCSI because Cloud Volumes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

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

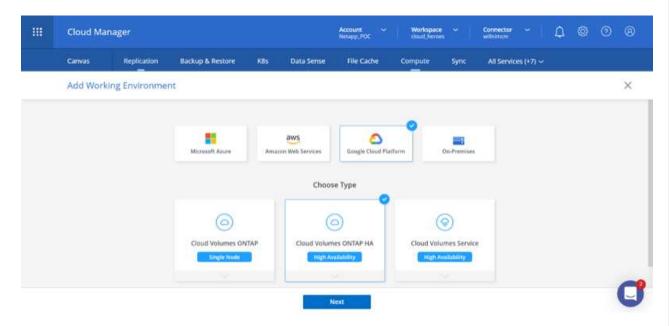


Use Cloud Volumes ONTAP sizer to accurately size the Cloud Volumes ONTAP instances. Also monitor on-premises performance to use as inputs in the Cloud Volumes ONTAP sizer.

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



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

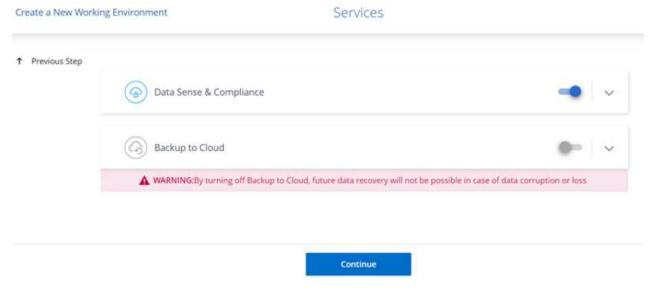


3. Provide the details of the environment to be created including the environment name and admin

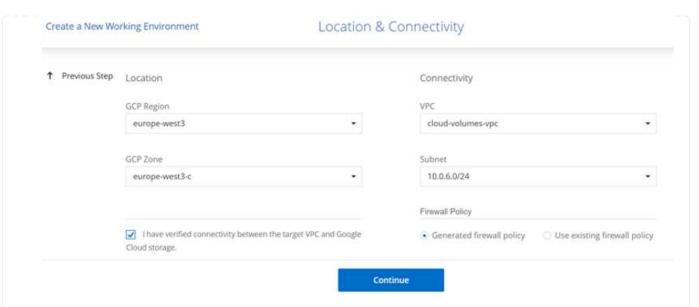
credentials. After you are done, click Continue. Details and Credentials Create a New Working Environment CV-Performance-Testing HCLMainBillingAccountSubs... ↑ Previous Step Edit Project Google Cloud Project Marketplace Subscription Details Credentials Working Environment Name (Cluster Name) User Name cvogcveva admin Password Service Account ****** Notice: A Google Cloud service account is required Confirm Password to use two features: backing up data using Backup 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.



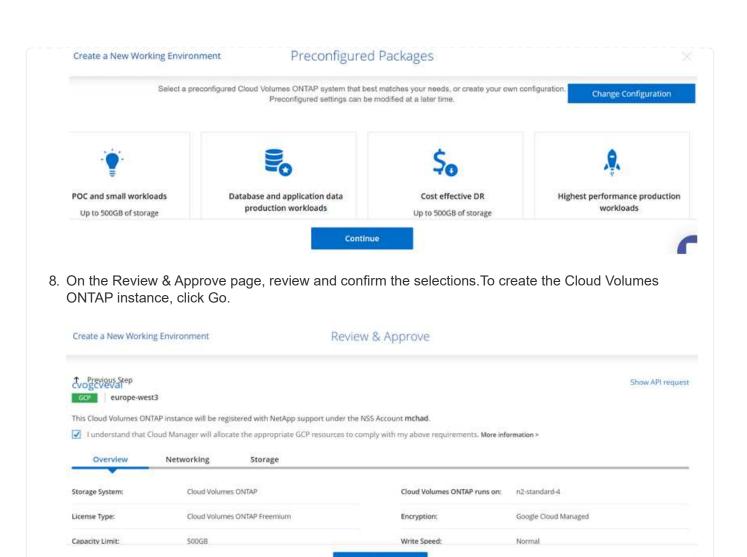
6. Select the license option: Pay-As-You-Go or BYOL for using existing license. In this example, Freemium option is used. Then, click on Continue.

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

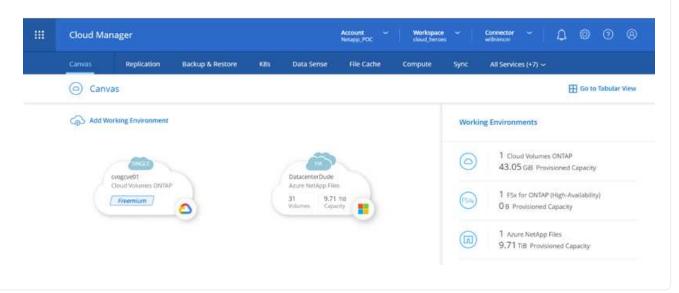


7. Select between several preconfigured packages available based on the type of workload that will be deployed on the VMs running on VMware cloud on AWS SDDC.

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



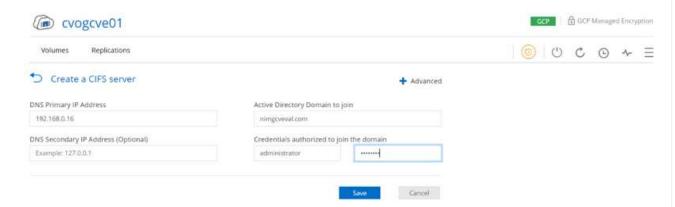
9. After Cloud Volumes ONTAP is provisioned, it is listed in the working environments on the Canvas page.



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.

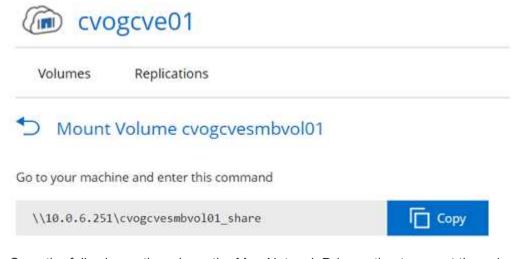


3. After the volume is provisioned, it will be availabe under the Volumes pane. Because a CIFS share is provisioned, give your users or groups permission to the files and folders and verify that those users can access the share and create a file. This step is not required if the volume is replicated 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.



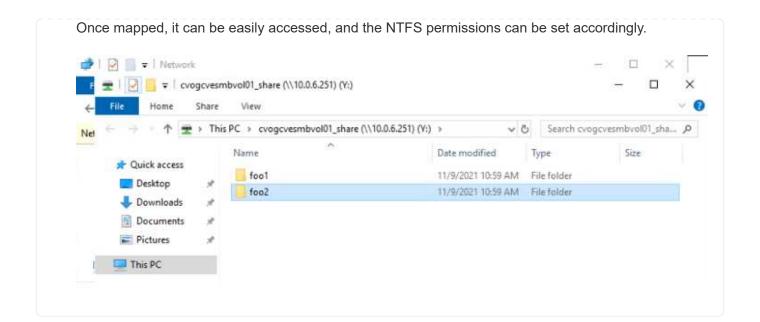
4. After the volume is created, use the mount command to display the volume connection instructions, then connect to the share from the VMs on Google Cloud VMware Engine.



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.

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

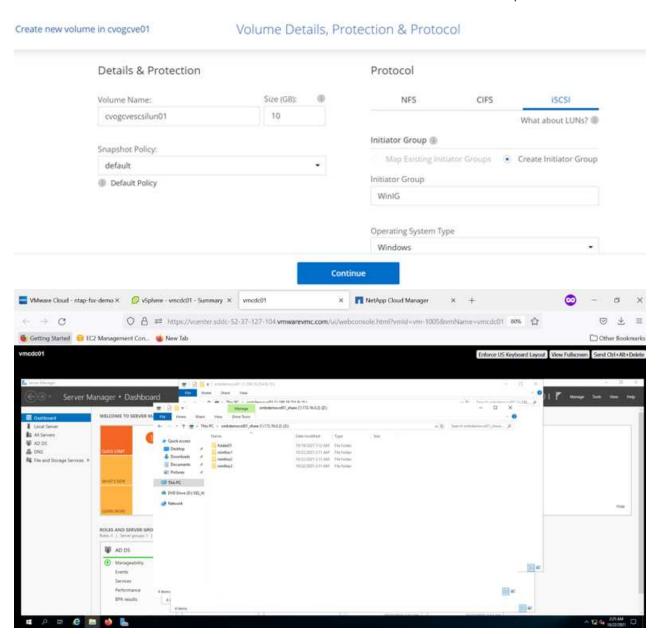




Connect the LUN on Cloud Volumes ONTAP to a host

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.

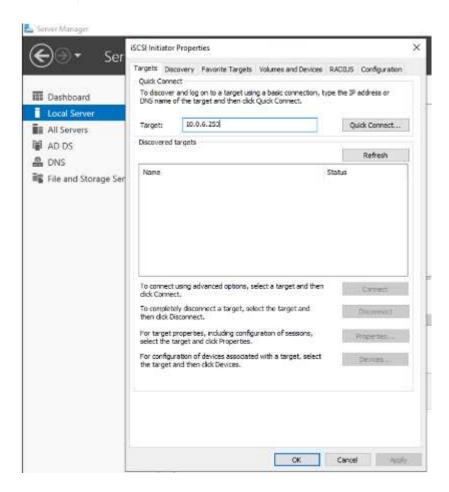
To accomplish the same for the host residing on Google Cloud VMware Engine:

- 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.



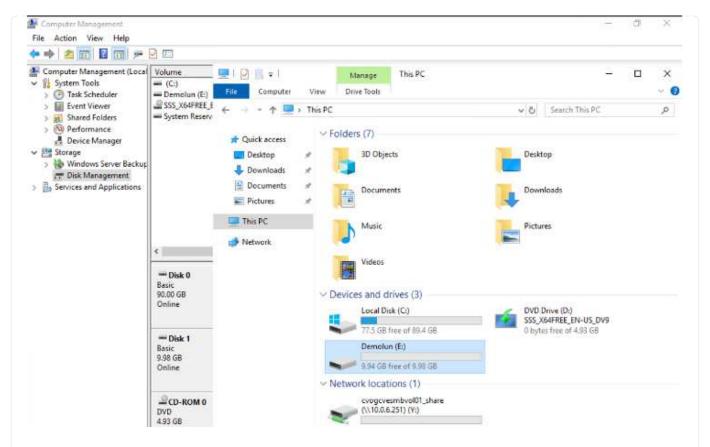
LUNs on storage virtual machine (SVM) appear as disks to the Windows host. Any new disks that are added are not automatically discovered by the host. Trigger a manual rescan to discover the disks by completing the following steps:

- 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
                           1 loop /snap/gnome-3-34-1804/72
         7:1
                 0
                    219M
                           1 loop /snap/gtk-common-themes/1515
loop2
         7:2
                 0
                   65.1M
loop3
         7:3
                 0
                      51M
                           1 loop /snap/snap-store/547
loop4
         7:4
                           1 loop /snap/snapd/12704
                 0
                   32.3M
loop5
         7:5
                 0
                   32.5M
                             loop /snap/snapd/13640
loop6
         7:6
                 0
                   55.5M
                           1 loop /snap/core18/2246
loop7
         7:7
                 0
                       4K
                           1 loop /snap/bare/5
loop8
         7:8
                 0
                   65.2M
                           1 loop /snap/gtk-common-themes/1519
sda
         8:0
                 0
                      16G
                           0 disk
 -sda1
         8:1
                 0
                    512M
                           0 part /boot/efi
  sda2
         8:2
                 0
                       1K
                             part
  -sda5
         8:5
                 0 15.5G
                           0 part /
sdb
         8:16
                       1G
                           0 disk
```

```
niyaz@nimubu01: $ df -h
                      Used Avail Use% Mounted on
Filesystem
                Size
udev
                1.9G
                         0 1.9G
                                   0% /dev
tmpfs
                394M
                      1.5M
                            392M
                                    1% /run
/dev/sda5
                                  53% /
                 16G
                      7.6G
                            6.9G
                                   0% /dev/shm
                2.0G
                         0 2.0G
tmpfs
                           5.0M
                                   0% /run/lock
tmpfs
                5.0M
                         0
tmpfs
                2.0G
                         0 2.0G
                                   0% /sys/fs/cgroup
                               0 100% /snap/gnome-3-34-1804/72
/dev/loop1
                219M
                      219M
/dev/loop2
                               0 100% /snap/gtk-common-themes/1515
                 66M
                       ббМ
/dev/loop3
                               0 100% /snap/snap-store/547
                 51M
                       51M
/dev/loop0
                 56M
                       56M
                               0 100% /snap/core18/2128
/dev/loop4
                               0 100% /snap/snapd/12704
                 33M
                       33M
                      4.0K
/dev/sda1
                511M
                            511M
                                    1% /boot/efi
tmpfs
                394M
                       64K
                            394M
                                   1% /run/user/1000
/dev/loop5
                               0 100% /snap/snapd/13640
                 33M
                       33M
/dev/loop6
                 56M
                               0 100% /snap/core18/2246
                       56M
/dev/loop7
                               0 100% /snap/bare/5
                128K
                      128K
                               0 100% /snap/gtk-common-themes/1519
/dev/loop8
                 66M
                       66M
/dev/sdb
                      2.6M
                976M
                           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.



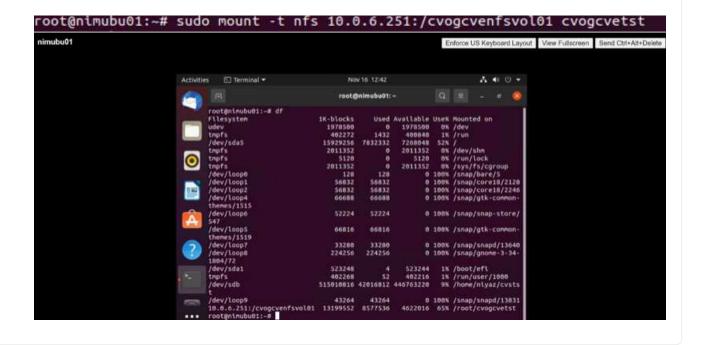
- 4. Click Copy.
- 5. Connect to the designated Linux instance.
- 6. Open a terminal on the instance using secure shell (SSH) and log in with the appropriate credentials.
- 7. Make a directory for the volume's mount point with the following command.

\$ 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.

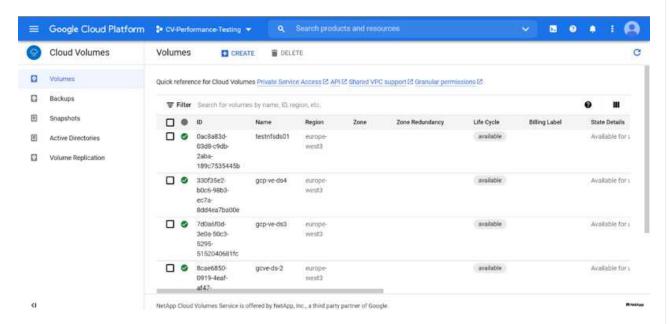
Create a CVS NFS volume to GCVE private cloud

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

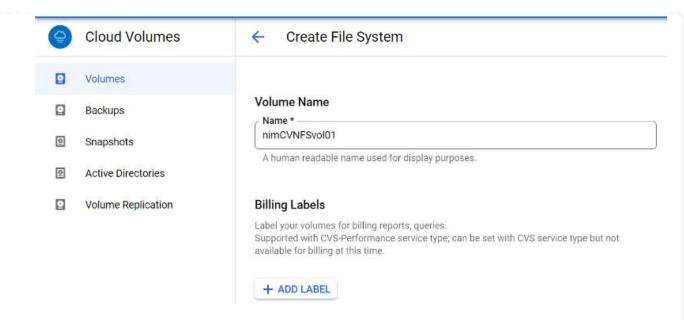
1. Access Cloud Volumes from Partner Solutions within the Google cloud console.



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



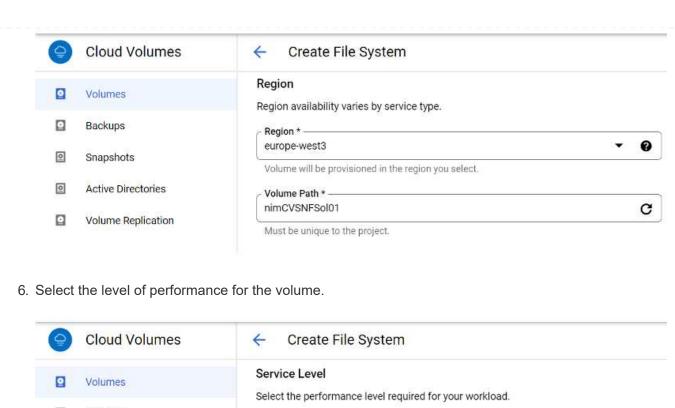
3. On the Create File System page, specify the volume name and billing labels as required for chargeback mechanisms.

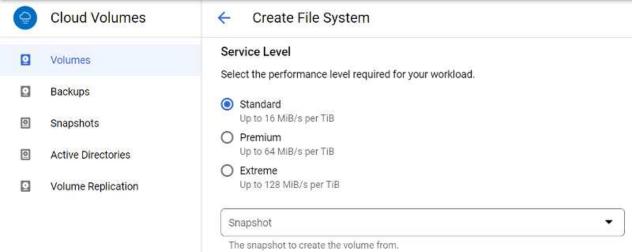


4. Select the appropriate service. For GCVE, choose CVS-Performance and desired service level for improved latency and higher performance based on the application workload requirements.

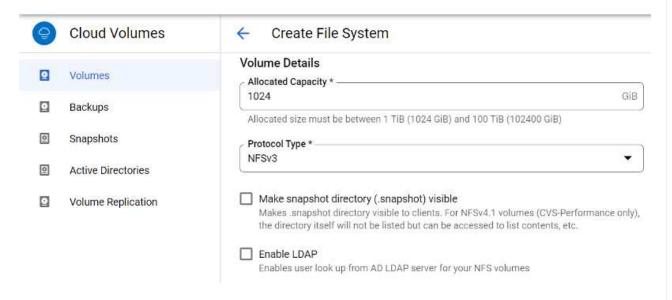


5. Specify the Google Cloud region for the volume and volume path (The volume path must be unique across all of cloud volumes in the project)





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



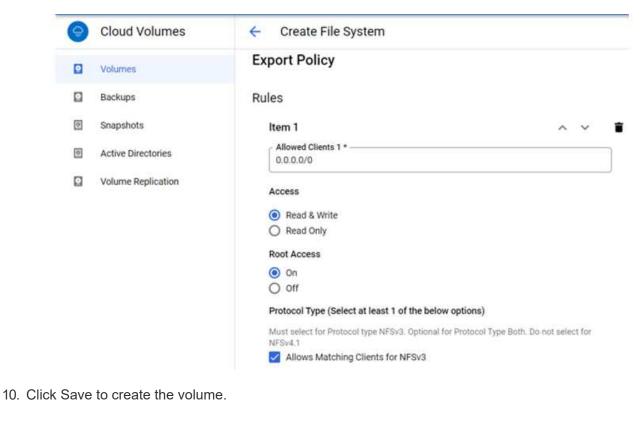
8. In this step, select the VPC Network from which the volume will be accessible. Ensure VPC peering is in place.

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.



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

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



 Ø 458ed9d9- nitrinfsdemods02
 europe- Available for use
 CVS- Primary
 Extreme
 NF9v3:10:53:0.4/mimfsdemods02

 bc6d-f3d5- west3
 Performance

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



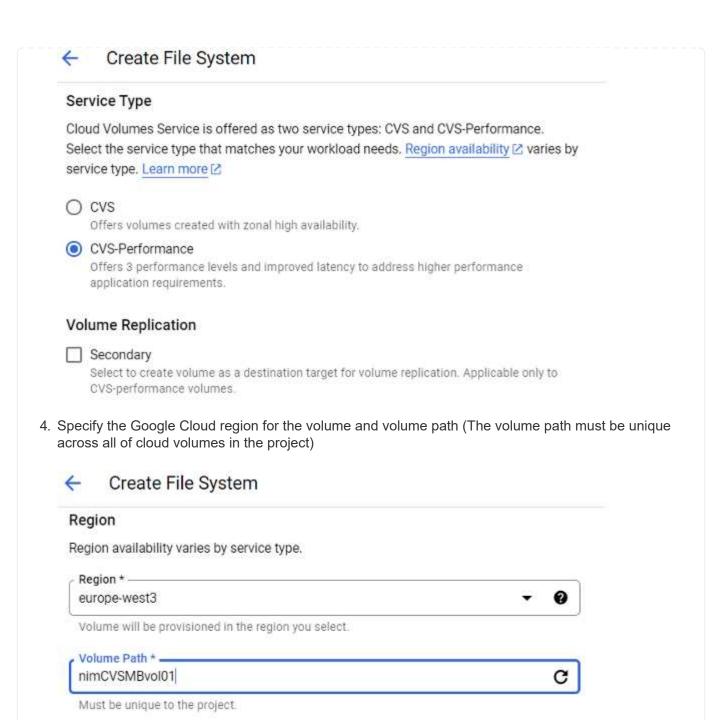
4. Mount the volume using the appropriate command. Example command from the lab is below:

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

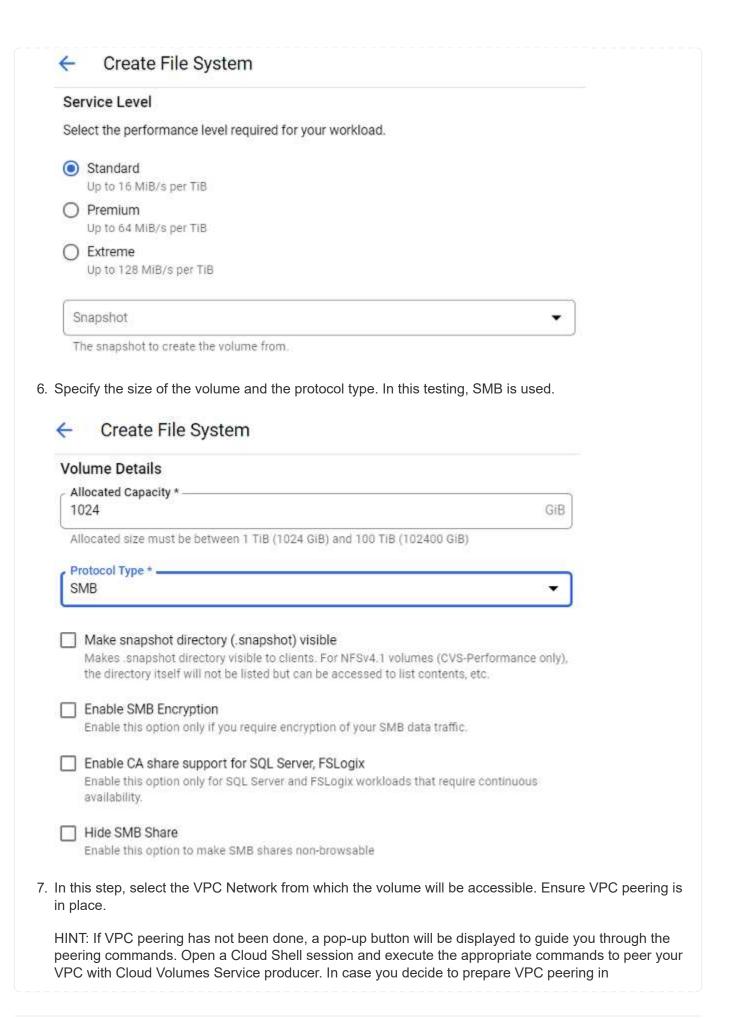
```
root@vm1:-# sudo mkdir nimcVsNFSol01
root@vm1:-# sudo mount -t nfs -o rw,hard,rsize=65536,wsize=65536,vers=3,tcp 10.53.0.4:/nimCVSNFSol01 /nimCVSNFSol01
```

root@vm1:~# df					
Filesystem	1K-blocks	Used			Mounted on
udev	16409952	0	16409952	0%	/dev
tmpfs	3288328	1580	3286748	1%	/run
/dev/sdb5	61145932	19231356	38778832	34%	
tmpfs	16441628	0	16441628	0%	/dev/shm
tmpfs	5120	0	5120	0%	/run/lock
tmpfs	16441628	0	16441628	0%	/sys/fs/cgroup
/dev/loop0	128	128	0	100%	/snap/bare/5
/dev/loop1	56832	56832	0	100%	/snap/core18/2128
/dev/loop2	66688	66688	0	100%	/snap/gtk-common-themes/1515
/dev/loop4	66816	66816	0	100%	/snap/gtk-common-themes/1519
/dev/loop3	52224	52224	0	100%	/snap/snap-store/547
/dev/loop5	224256	224256	0	100%	/snap/gnome-3-34-1804/72
/dev/sdb1	523248	4	523244	1%	/boot/efi
tmpfs	3288324	28	3288296	1%	/run/user/1000
10.53.0.4:/gcve-ds-1	107374182400	1136086016	106238096384	2%	/base
/dev/mapper/nfsprdvg1-prod01	419155968	55384972	363770996	14%	/datastore1
/dev/loop8	33280	33280	0		/snap/snapd/13270
/dev/loop6	33280	33280			/snap/snapd/13640
/dev/loop7	56832	56832			/snap/core18/2246
10.53.0.4:/nimCVSNFSol01	107374182400	256	107374182144	1%	/nimCVSNFSol01
root@vm1:~#					

Creating and Mounting SMB Share to VMs running on VMware Engine For SMB volumes, make sure the Active Directory connections is configured prior to creating the SMB volume. Active Directory connections C CREATE @ DELETE Create a Windows Active Directory connection to your existing AD server. This is a prerequisite step before creating volumes with the SMB protocol type. Learn more [2] ₹ Filter Search for Active Directory connections by ID, username, DNS, netBIOS, region, etc. DNS Servers NetBIOS Prefix OU Path Region administrator nimgoveval.com 192.168.0.16 nimsmb CN=Computers in Use Once the AD connection is in place, create the volume with the desired service level. The steps are like creating NFS volume except selecting the appropriate protocol. 1. In the Cloud Volumes Console, go to the Volumes page and click Create. 2. On the Create File System page, specify the volume name and billing labels as required for chargeback mechanisms. Create File System Volume Name Name * nimCVSMBvol01 A human readable name used for display purposes. Billing Label Label your volumes for billing reports, queries. Supported with CVS-Performance service type; can be set with CVS service type but not available for billing at this time. + ADD LABEL 3. Select the appropriate service. For GCVE, choose CVS-Performance and desired service level for improved latency and higher performance based on the workload requirements.



5. Select the level of performance for the volume.





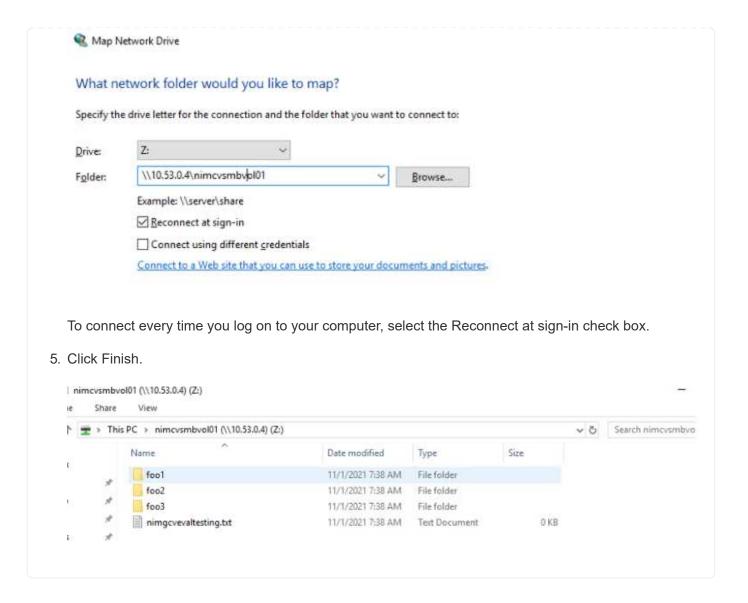
To mount the SMB volume, do the following:

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

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

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

\\nimsmb-3830.nimgcveval.com\nimCVSMBvol01



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

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

AWS Region Availability

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

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

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

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

Last updated on: June 2, 2022.

EMEA

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

Last updated on: June 2, 2022.

Asia Pacific

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

Last updated on: September 28, 2022.

Azure Region Availability

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

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

GCP Region Availability

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

Copyright information

Copyright © 2023 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

Trademark information

NETAPP, the NETAPP logo, and the marks listed at http://www.netapp.com/TM are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.