



# **Guest Connected storage for VMC**

## **NetApp Solutions**

NetApp  
October 20, 2023

This PDF was generated from <https://docs.netapp.com/us-en/netapp-solutions/ehc/aws/aws-guest.html> on October 20, 2023. Always check docs.netapp.com for the latest.

# Table of Contents

- NetApp Guest Connected Storage Options for AWS ..... 1
  - FSx ONTAP ..... 1
  - Cloud Volumes ONTAP (CVO)..... 16

# 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 file shares and LUNs can be mounted from VMs that are created within the VMware SDDC environment at VMware Cloud on 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.

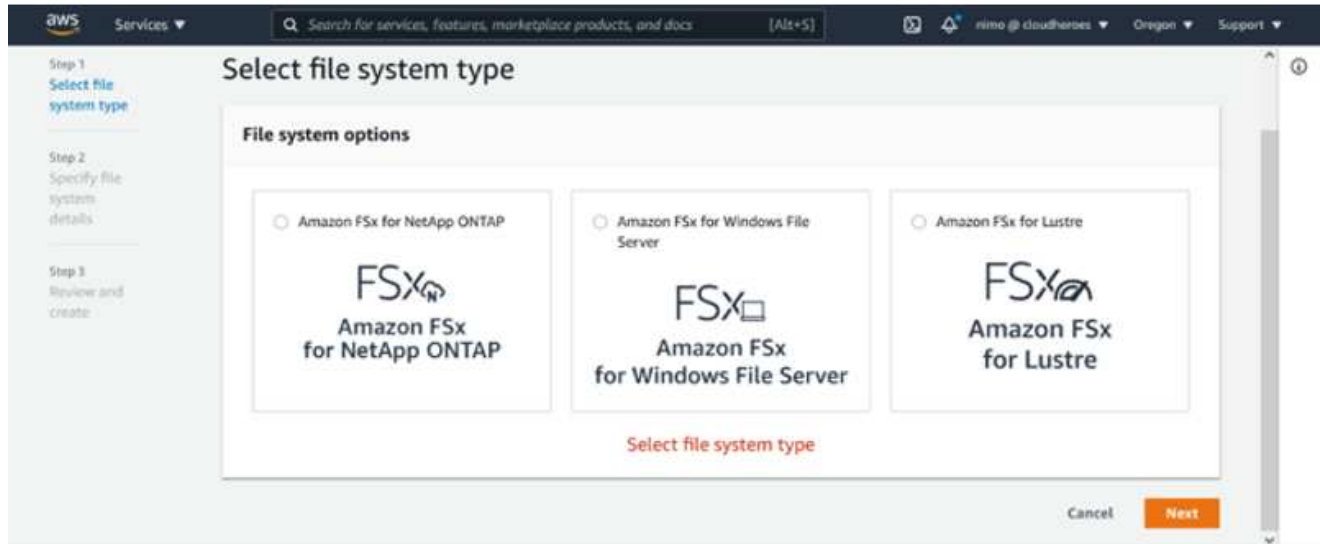


Amazon FSx for NetApp ONTAP and VMware Cloud on AWS must be in the same availability zone to achieve better performance and avoid data transfer charges between availability zones.

## Create and mount Amazon FSx for ONTAP volumes

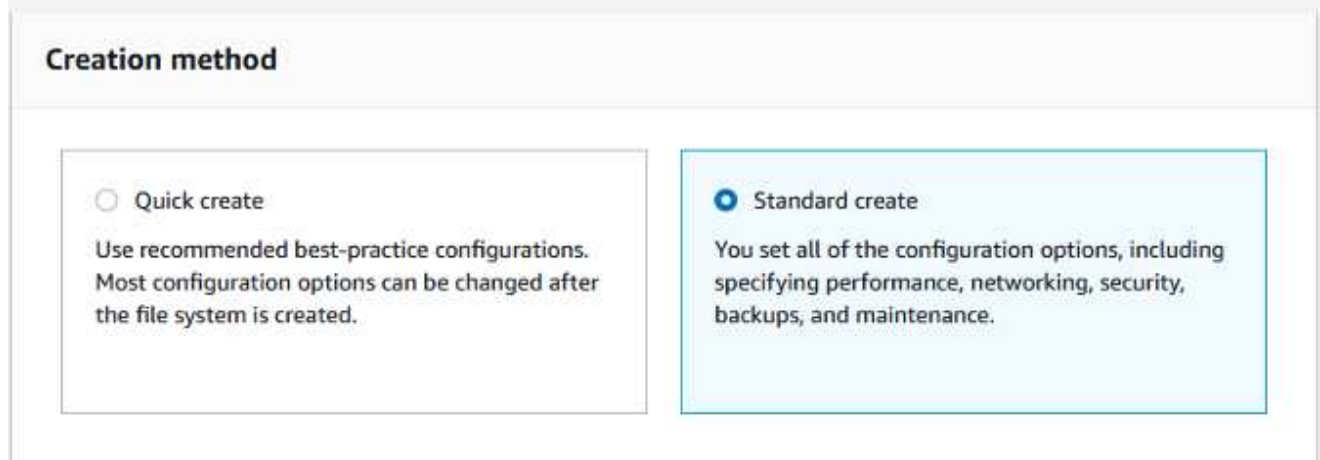
To create and mount Amazon FSx for NetApp ONTAP file system, complete the following steps:

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.

## Create file system



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

## File system details

File system name - optional [Info](#)

vmcfsxval2

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

SSD storage capacity [Info](#)

1024

Minimum 1024 GB; Maximum 192 TB.

Provisioned SSD IOPS

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

☒ Automatic (3 IOPS per GB of SSD storage)

☐ User-provisioned

Throughput capacity [Info](#)

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

512 MB/s (Recommended)

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.

## Network & security

Virtual Private Cloud (VPC) [Info](#)

Specify the VPC from which your file system is accessible.

vmcfsx2.vpc | vpc-0d1c764bcc495e805

VPC Security Groups [Info](#)

Specify VPC Security Groups to associate with your file system's network interface.

Choose VPC security group(s)

sg-018896ea218164ccb (default) X

Preferred subnet [Info](#)

Specify the preferred subnet for your file system.

subnet02.sn | subnet-013675849a5b99b3c (us-west-2b)

Standby subnet

subnet01.sn | subnet-0ef956cebf539f970 (us-west-2a)

VPC route tables

Specify the VPC route tables associated with your file system.

☒ VPC's default route table

☐ Select one or more VPC route tables

Endpoint IP address range

Specify the IP address range in which the endpoints to access your file system will be created

☒ No preference

☐ Select an IP address range



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

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

## Security & encryption

### Encryption key [Info](#)

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

aws/fsx (default) ▼

Description	Account	KMS key ID
Default master key that protects my FSx resources when no other key is defined	139763910815	72745367-7bb0-499c-acc0-4f2c0a80e7c5

### File system administrative password

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

☐ Don't specify a password

☒ Specify a password

Password

••••••••

Confirm password

••••••••

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.

## Default storage virtual machine configuration

Storage virtual machine name

vmcfsxval2svm

SVM administrative password

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

- ☐ Don't specify a password  
☒ Specify a password

Password

••••••••

Confirm password

••••••••

Active Directory

Joining an Active Directory enables access from Windows and MacOS clients over the SMB protocol.

- ☒ Do not join an Active Directory  
☐ Join an Active Directory

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.

## Default volume configuration

Volume name

vol1

Maximum of 203 alphanumeric characters, plus \_ -

Junction path

/vol1

The location within your file system where your volume will be mounted.

Volume size

1024

Minimum 20 MiB; Maximum 104857600 MiB

Storage efficiency

Select whether you would like to enable ONTAP storage efficiencies on your volume: deduplication, compression, and compaction.

- ☐ Enabled (recommended)  
☒ Disabled

Capacity pool tiering policy

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

Auto

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

The screenshot displays the Amazon FSx console interface. The top navigation bar includes the AWS logo, 'Services', a search bar, and user information. The left sidebar shows the 'Amazon FSx' menu with options like 'File systems', 'Backups', 'ONTAP', 'Storage virtual machines', 'Volumes', 'Windows File Server', 'Lustre', and 'FSx on Service Quotas'.

The main content area is divided into two sections. The top section, 'File systems (3)', shows a table of existing file systems:

File system name	File system ID	File system type	Status	Deployment type	Storage type	Size
fsxntapcifs	fs-014c28399be9c1f9f	ONTAP	Available	Multi-AZ	SSD	1,024 GiB
vmcfsxval2	fs-040eacc5d0ac31017	ONTAP	Available	Multi-AZ	SSD	1,024 GiB
fsxntapsql	fs-0ab4b447ebd6082aa	ONTAP	Available	Multi-AZ	SSD	2,048 GiB

The bottom section, 'Storage virtual machines (SVMs) (2)', shows a table of existing SVMs:

SVM name	SVM ID	Status	Creation time	Active Directory
fsxmbtesting01	svm-075dcfbe2cfa2ece9	Created	2021-10-19 15:17:08 UTC +01:00	FSXTESTING.LOCAL
vmcfsxval2svm	svm-095db076341561212	Created	2021-10-15 15:16:54 UTC +01:00	-

Below the SVMs table, the console shows the details for 'fsxmbtesting01 (svm-075dcfbe2cfa2ece9)'. The details are organized into a 'Summary' section with the following information:

Property	Value
SVM ID	svm-075dcfbe2cfa2ece9
SVM name	fsxmbtesting01
UUID	4a50e659-30e7-11ec-ac4f-f3ad92a6a735
File system ID	fs-040eacc5d0ac31017
Creation time	2021-10-19T15:17:08+01:00
Lifecycle state	Created
Subtype	DEFAULT
Active Directory	FSXTESTING.LOCAL
Net BIOS name	FSXSMBTESTING01
Fully qualified domain name	FSXTESTING.LOCAL
Service account username	administrator
Organizational unit distinguished name	CN=Computers

For more detailed information, see [Getting started with Amazon FSx for NetApp ONTAP](#).



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

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

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

**Create volume** [X]

**File system**  
fs-040eacc5d0ac31017 | vmcfsxval2 ▼

**Storage virtual machine**  
svm-095db076341561212 | vmcfsxval2svm ▼

**Volume name**  
nfsdemovol01  
Maximum of 205 alphanumeric characters, plus \_.

**Junction path**  
/nfsdemovol01  
The location within your file system where your volume will be mounted.

**Volume size**  
1024 [v]  
Minimum 20 MiB; Maximum 104857600 MiB

**Storage efficiency**  
Select whether you would like to enable ONTAP storage efficiencies on your volume: deduplication, compression, and compaction.  
☐ Enabled (recommended)  
☒ Disabled

**Capacity pool tiering policy**  
You can optionally enable automatic tiering of your data to lower-cost capacity pool storage.  
Auto ▼

Cancel Confirm

## 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:

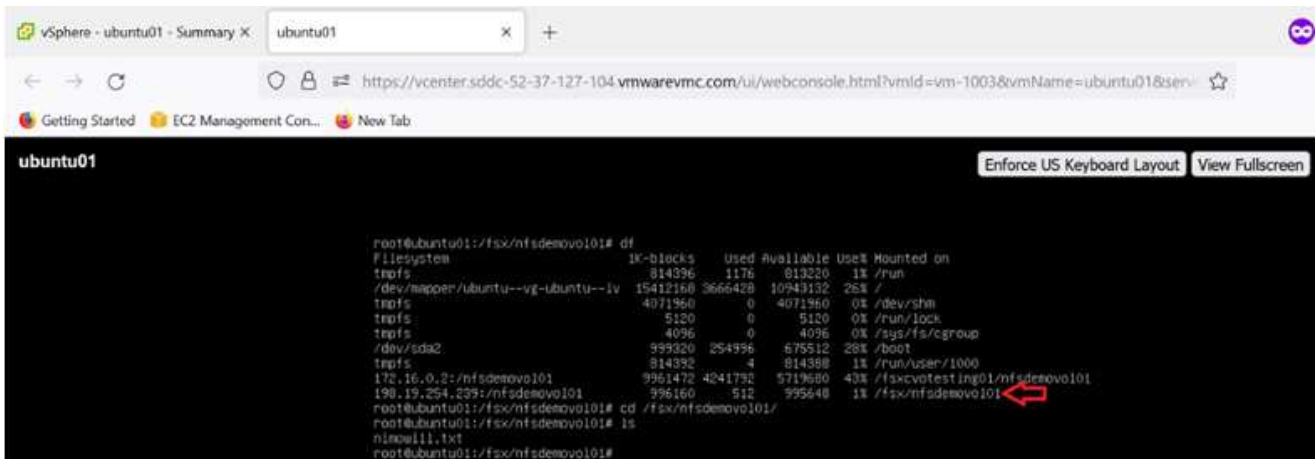
```
$ sudo mkdir /fsx/nfsdemovol01
```

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.



```
root@ubuntu01:/fsx/nfsdemovol01# df
Filesystem            1K-blocks    Used Available Use% Mounted on
tmpfs                  814396      1176    813220   1% /run
/dev/mapper/ubuntu--vg-ubuntu--lv 15412160 3666428 10845732 26% /
tmpfs                  4071960      0 4071960   0% /dev/shm
tmpfs                   5120        0    5120   0% /run/lock
tmpfs                   4096        0    4096   0% /sys/fs/cgroup
/dev/sda2              999320 254996 675512 28% /boot
tmpfs                   814392      4    814388   1% /run/user/1000
172.16.0.2:/nfsdemovol01 9961472 4241792 5719680 43% /fsx/votesting01/nfsdemovol01
198.19.254.239:/nfsdemovol01 996160    512    995648   1% /fsx/nfsdemovol01
```

## Mount FSx ONTAP volume on Linux client

## Attach FSx ONTAP volumes to Microsoft Windows clients

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

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



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

### Endpoints

Management DNS name

svm-075dcfbe2cfa2ece9.fs-040eacc5d0ac31017.fsx.us-west-2.amazonaws.com

NFS DNS name

svm-075dcfbe2cfa2ece9.fs-040eacc5d0ac31017.fsx.us-west-2.amazonaws.com

SMB DNS name

FSXSMBTESTING01.FSXTESTING.LOCAL



iSCSI DNS name

iscsi.svm-075dcfbe2cfa2ece9.fs-040eacc5d0ac31017.fsx.us-west-2.amazonaws.com

Management IP address

198.19.254.9

NFS IP address

198.19.254.9

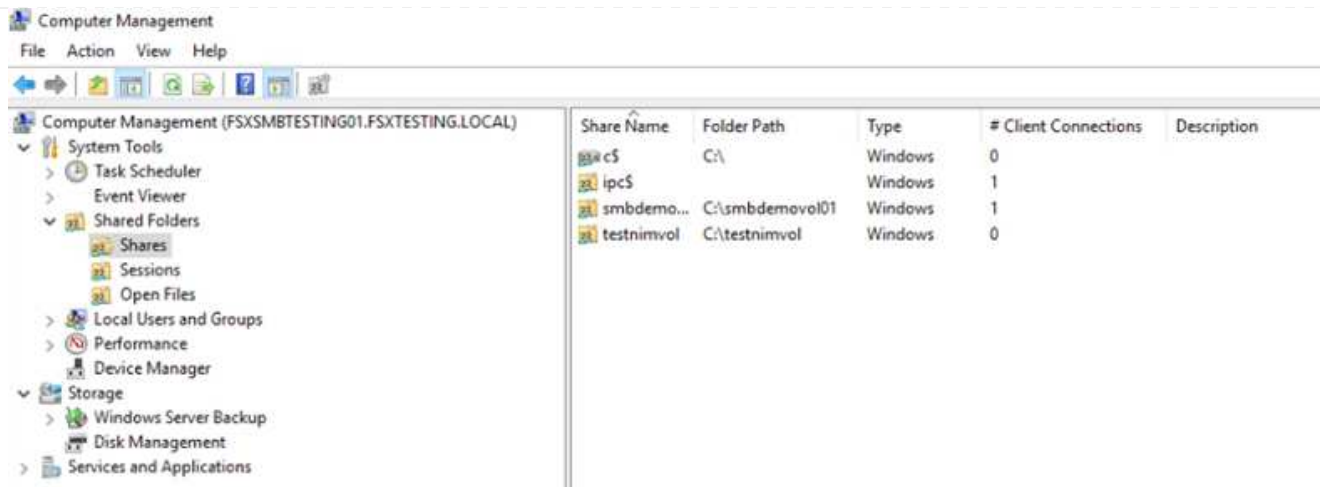
SMB IP address

198.19.254.9

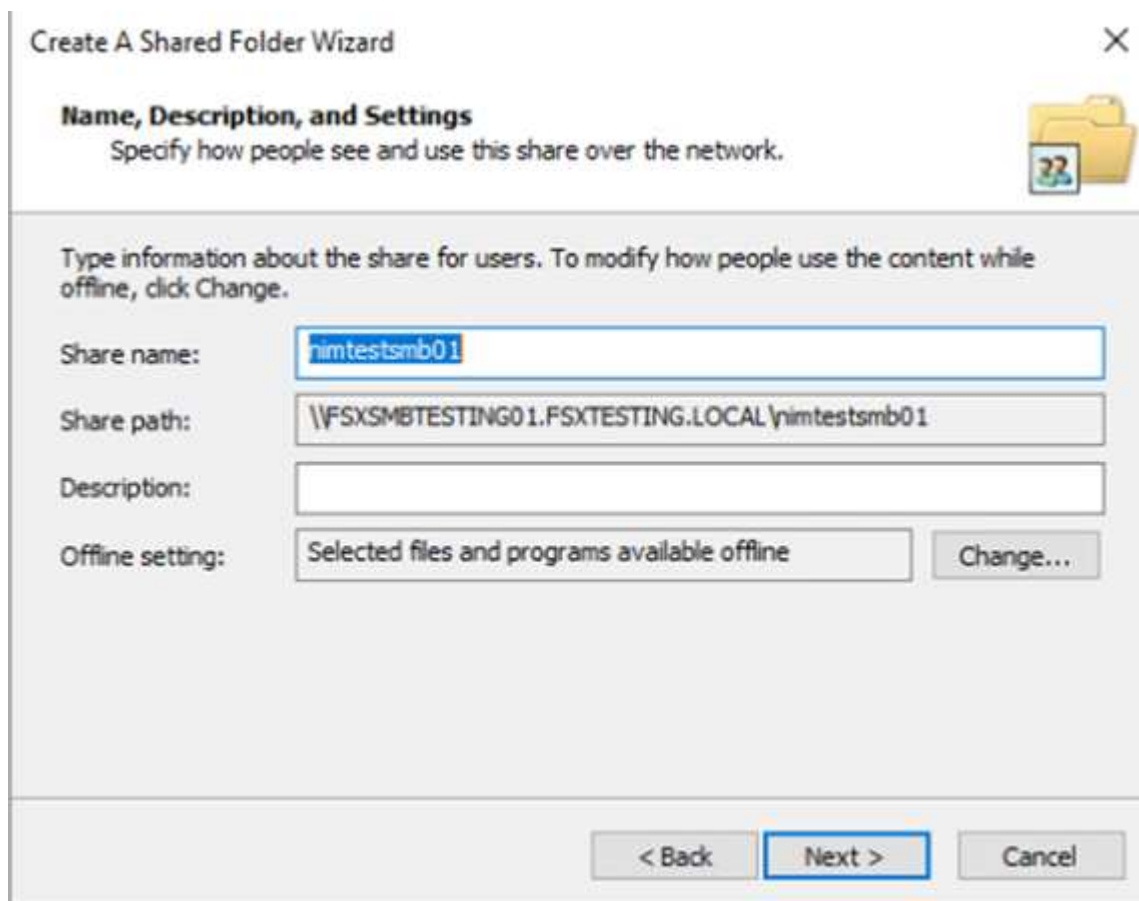
iSCSI IP addresses

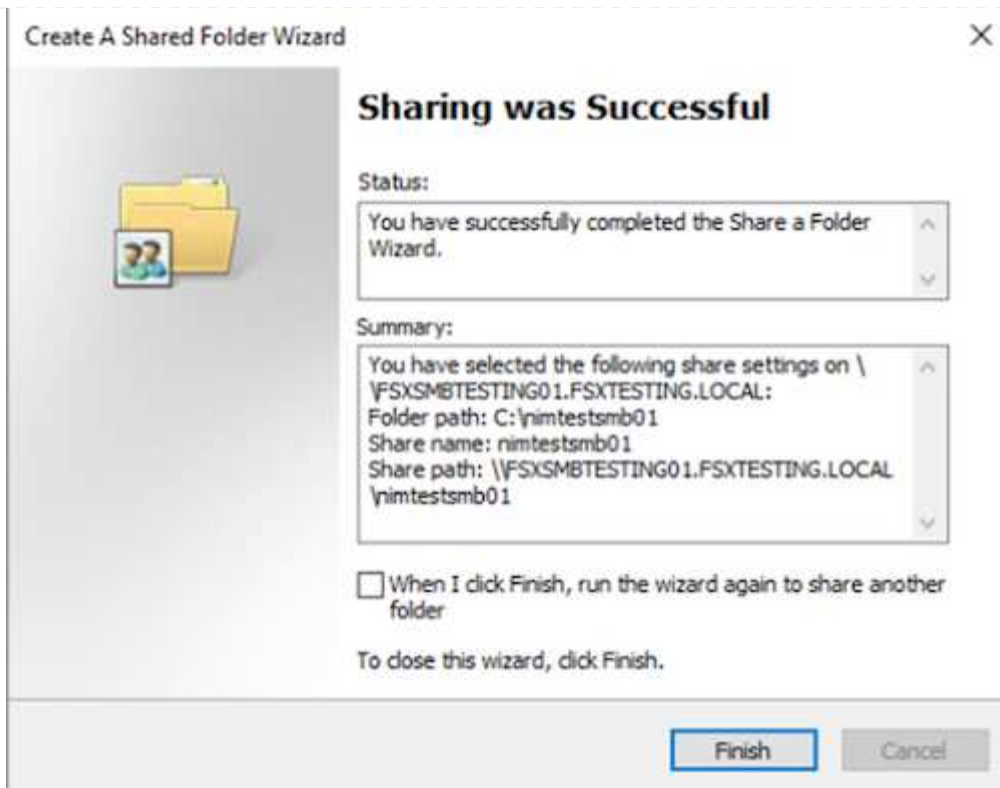
10.222.2.224, 10.222.1.94

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



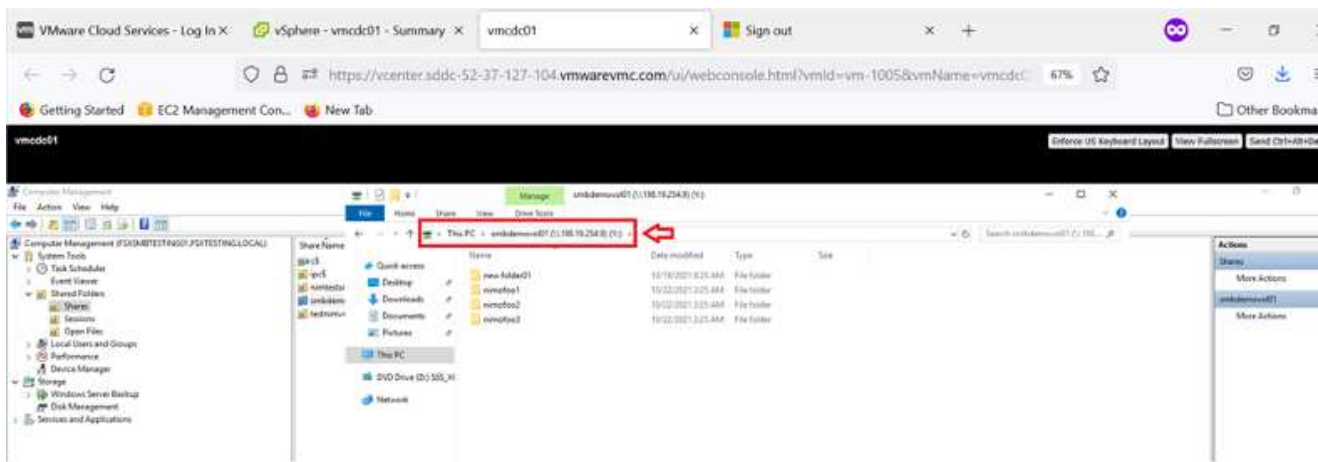
1. Now choose a new share and complete the Create a Shared Folder wizard.





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 vmcfsexval2svm -volume  
nimfsxscsivol -lun nimofsxslun01 -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 vmcfsexval2svm -igroup  
winIG -protocol iscsi -ostype windows -initiator iqn.1991-  
05.com.microsoft:vmcdc01.fsxtesting.local
```

```
FsxId040eacc5d0ac31017::> igroup show
```

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

-----	-----	-----	-----	
-----	-----	-----	-----	

vmcfsexval2svm

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

vmcfsexval2svm

	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 vmcfjsxval2svm -path  
/vol/nimfsxscsivol/nimofsx1un01 -igroup winIG
```

```
FsxId040eacc5d0ac31017::> lun show
```

Vserver	Path	State	Mapped	Type
Size				
-----				
-----				
vmcfjsxval2svm				
	/vol/blocktest01/lun01	online	mapped	linux
5GB				
vmcfjsxval2svm				
	/vol/nimfsxscsivol/nimofsx1un01	online	mapped	windows
5GB				

Two entries were displayed.

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

To connect the new LUN for 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.



## Quick Connect

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

Target: 10.222.2.221

## Discovered targets

Name	Status
iqn.1992-08.com.netapp:sn.264efe832dd911eca961d5f...	Connected

To connect using advanced options, select a target and then click Connect.

To completely disconnect a target, select the target and then click Disconnect.

For target properties, including configuration of sessions, select the target and click Properties.

For configuration of devices associated with a target, select the target and then click Devices.

## Quick Connect

Targets that are available for connection at the IP address or DNS name that you provided are listed below. If multiple targets are available, you need to connect to each target individually.

Connections made here will be added to the list of Favorite Targets and an attempt to restore them will be made every time this computer restarts.

## Discovered targets

Name	Status
iqn.1992-08.com.netapp:sn.f0c909af2dc611ecac4f...	Connected

## Progress report

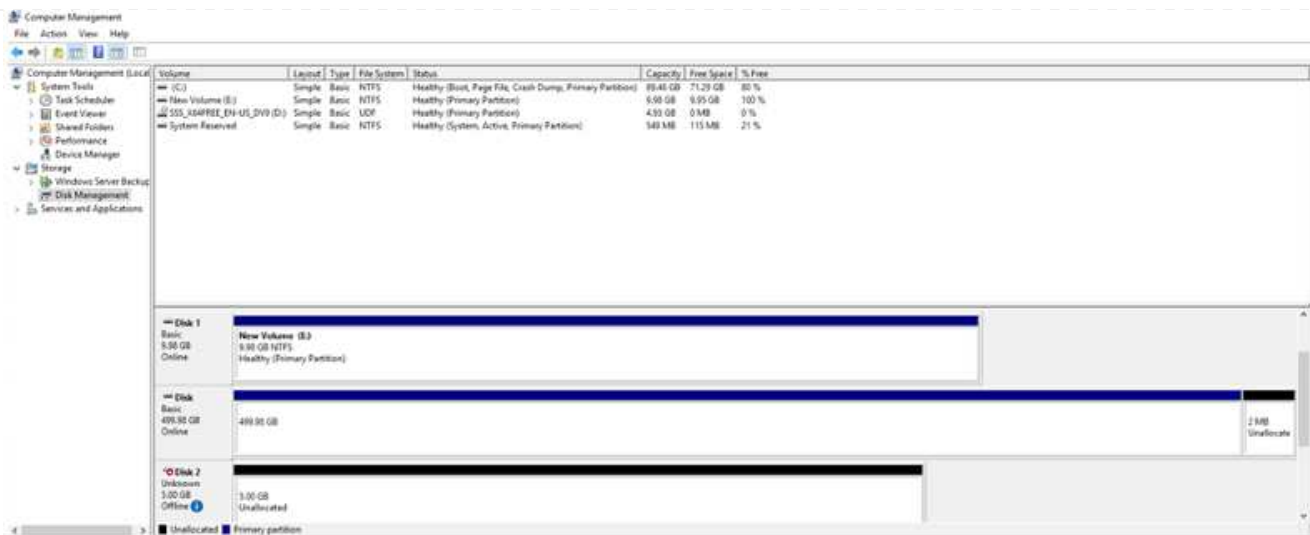
Login Succeeded.

Connect

Done

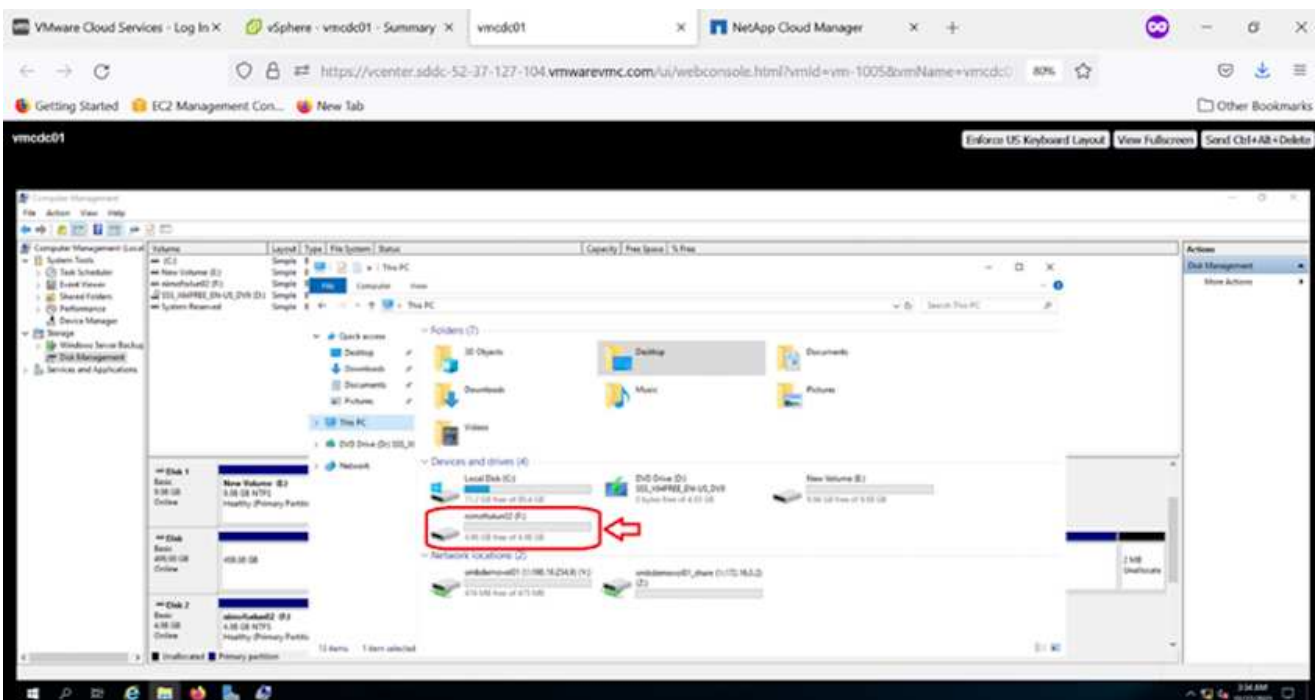
LUNs on the storage virtual machine (SVM) appear as disks to the Windows host. Any new disks that are added are not automatically discovered by the host. Trigger a manual rescan to discover the disks by completing the following steps:

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



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

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



## Cloud Volumes ONTAP (CVO)

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

It is a software-defined version of ONTAP that consumes cloud-native storage, allowing you to have the same

storage software in the cloud and on-premises, reducing the need to retrain your IT staff in all-new methods to manage your data.

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

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

## **Cloud Volumes ONTAP (CVO) as guest connected storage**

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

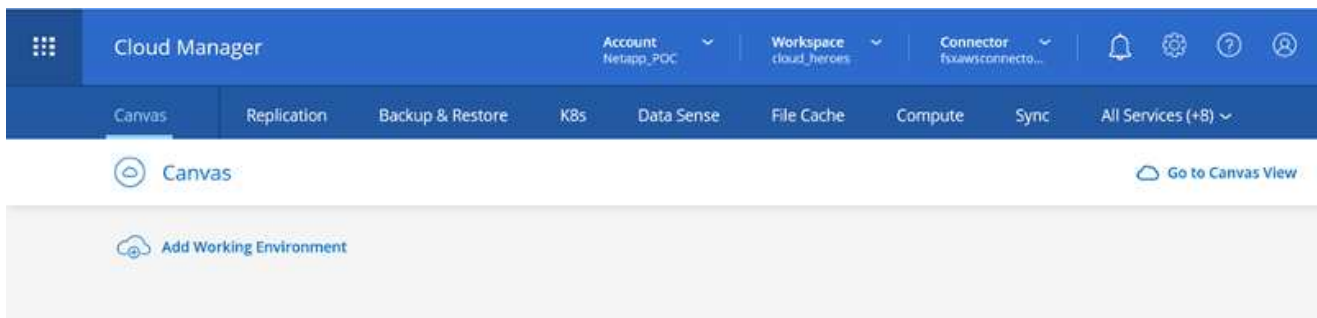
Cloud Volumes ONTAP shares and LUNs can be mounted from VMs that are created in the VMware Cloud on AWS SDDC environment. The volumes can also be mounted on native AWS VM Linux Windows clients, and LUNS can be accessed on Linux or Windows clients as block devices when mounted over iSCSI because Cloud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

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

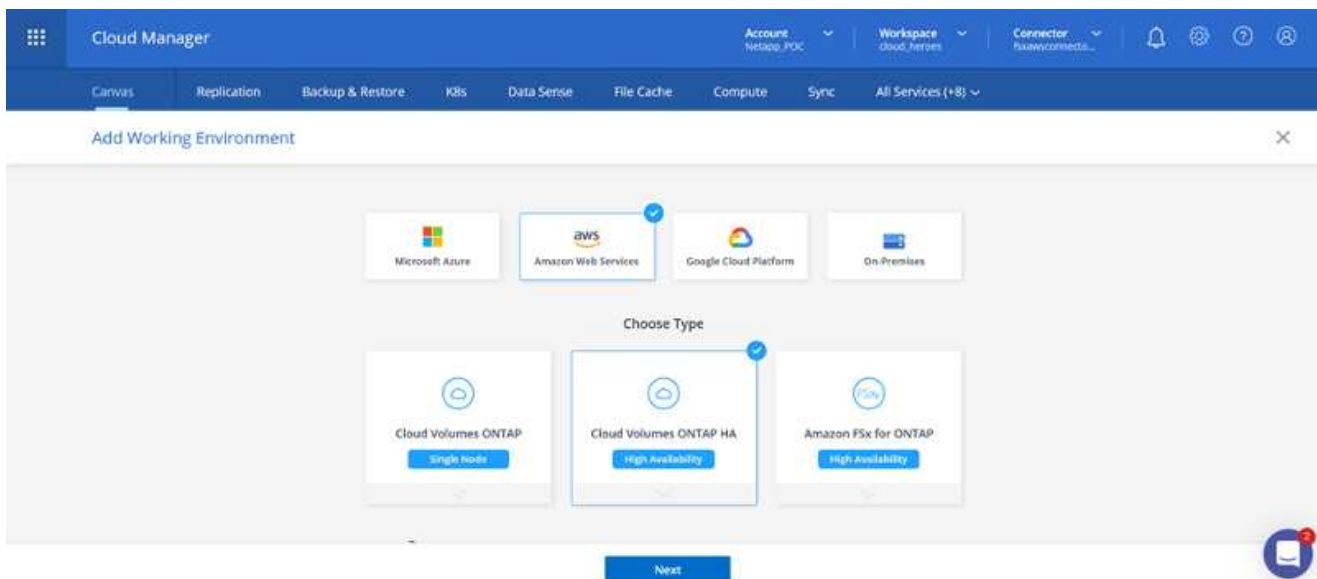


Use the [Cloud Volumes ONTAP sizer](#) to accurately size the Cloud Volumes ONTAP instances. Also, monitor on-premises performance to use as inputs in the Cloud Volumes ONTAP sizer.

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



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.

[↑ Previous Step](#)

Instance Profile

139763910815

netapp.com-cloud-volumes-...

[Edit Credentials](#)

Credential Name

Account ID

Marketplace Subscription

## Details

Working Environment Name (Cluster Name)

fsxcvotesting01

[+ Add Tags](#)

Optional Field | Up to four tags

## Credentials

User Name

admin

Password

••••••••

Confirm Password

••••••••

[Continue](#)

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



Data Sense &amp; Compliance



Backup to Cloud



Monitoring

[Continue](#)

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

[↑ Previous Step](#)

## Multiple Availability Zones



Provides maximum protection against AZ failures.



Enables selection of 3 availability zones.



An HA node serves data if its partner goes offline.

[Extended Info](#)

## Single Availability Zone



Protects against failures within a single AZ.



Single availability zone. HA nodes are in a placement group, spread across distinct underlying hardware.



An HA node serves data if its partner goes offline.

[Extended Info](#)

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

[↑ Previous Step](#)

AWS Region

US West | Oregon

VPC

vpc-0d1c764bcc495e805 -  
10.222.0.0/16

Security group

Use a generated security group



Node 1:

Availability Zone

us-west-2a

Subnet

10.222.1.0/24



Node 2:

Availability Zone

us-west-2b

Subnet

10.222.2.0/24



Mediator:

Availability Zone

us-west-2c

Subnet

10.222.3.0/24

Continue

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

[↑ Previous Step](#)

Nodes

SSH Authentication Method

Password



Mediator

Security Group

Use a generated security group

Key Pair Name

nimokey

Internet Connection Method

Public IP address

Continue

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

[↑ Previous Step](#)

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

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

Floating IP address for cluster management

Floating IP address 1 for NFS and CIFS data

Floating IP address 2 for NFS and CIFS data

Floating IP address for SVM management (Optional)

[Continue](#)

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

[↑ Previous Step](#)

Select the route tables that should include routes to the floating IP addresses. This enables client access to the Cloud Volumes ONTAP HA pair. If you leave a route table unselected, clients that are associated with the route table cannot access the HA pair.

Additional information ⓘ

Name	Main	ID	Associate with Subnet	Tags
<input checked="" type="checkbox"/>	Yes	rtb-00b2d30c3f68fdbdd	0 Subnets	1 Tags

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

[Continue](#)

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

[↑ Previous Step](#)

## AWS Managed Encryption

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

Default Master Key: `aws/ebs`

[Change Key](#)[Continue](#)

1. 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.

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

## Cloud Volumes ONTAP Charging Methods

[Learn more about our charging methods](#)☒ Pay-As-You-Go by the hour☐ Bring your own license

## NetApp Support Site Account (Optional)

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

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

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

[Continue](#)

1. 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.



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

[Change Configuration](#)**POC and small workloads**

Up to 500GB of storage

**Database and application data  
production workloads****Cost effective DR**  
Up to 500GB of storage**Highest performance production  
workloads**[Continue](#)



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

Create a New Working Environment Review & Approve

↑ Previous Step **fsxcvotesting** Show API request

**AWS** | **us-west-2** | **HA**

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

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

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

**Go**

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

Canvas | Replication | Backup & Restore | KBs | Data Sense | File Cache | Compute | Sync | All Services (+8) v

Canvas Go to Tabular View

**Add Working Environment**

**vmchval2**  
FSa for ONTAP  
9 Volumes 26.49 GiB Capacity **AWS**

**fsxcvotesting01**  
Cloud Volumes ONTAP  
4G GiB Capacity **AWS**

**Amazon S3**  
4 Buckets 2 Regions **AWS**

**fsxcvotesting01**  
On

**DETAILS**  
Cloud Volumes ONTAP | AWS | HA

**SERVICES**

Replication **Off** **Enable**

Backup & Restore **Loading...**

## Additional configurations for SMB volumes

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

The screenshot shows the AWS Management Console interface for configuring a CIFS server. At the top, the instance name 'fsxcvotesting01' is displayed with a 'Multiple AZs' tag. Below this are tabs for 'Volumes', 'HA Status', 'Cost', and 'Replications'. A navigation bar includes icons for monitoring, power, refresh, and other actions. The main section is titled 'Create a CIFS server' with a '+ Advanced' link. The configuration fields are as follows:

Field	Value
DNS Primary IP Address	192.168.1.3
DNS Secondary IP Address (Optional)	Example: 127.0.0.1
Active Directory Domain to join	fsxtesting.local
Credentials authorized to join the domain	Username: , Password:

At the bottom, there are 'Save' and 'Cancel' buttons.

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.

The screenshot shows the 'Volume Details, Protection & Protocol' configuration page. It is divided into two main sections: 'Details & Protection' and 'Protocol'.

**Details & Protection:**

Field	Value
Volume Name:	smbdemo01
Size (GB):	100
Snapshot Policy:	default

**Protocol:**

The 'Protocol' section has tabs for 'NFS', 'CIFS' (selected), and 'iSCSI'.

Field	Value
Share name:	smbdemo01_share
Permissions:	Full Control
Users / Groups:	Everyone;

Below the 'Users / Groups' field, a note states: 'Valid users and groups separated by a semicolon'.

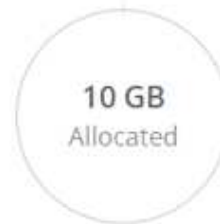
At the bottom, there is a 'Continue' button.

1. 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.

## INFO

Disk Type	GP2
Tiering Policy	None
Backup	OFF

## CAPACITY



1.67 MB  
EBS Used

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.

## Mount Volume smbdemovol01



Access from inside the VPC using Floating IP

### Auto failover between nodes

The IP address automatically migrates between nodes if failures occur

Go to your machine and enter this command

```
\\172.16.0.2\smbdemovo101_share
```

Copy



Access from outside the VPC using AWS Private IP

### No auto failover between nodes

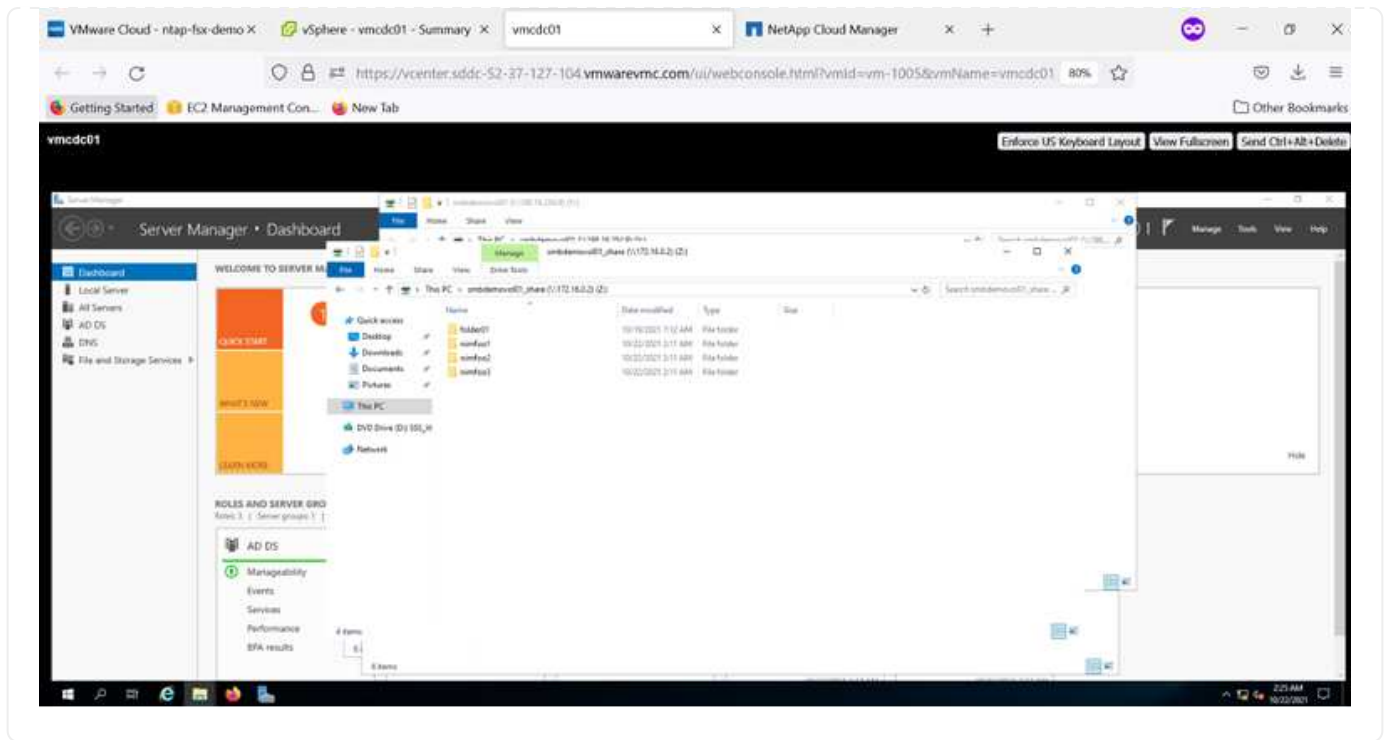
The IP address does not migrate between nodes if failures occur

To avoid traffic between nodes, mount the volume by using the primary node's IP address:

```
\\10.222.1.100\smbdemovo101_share
```

Copy

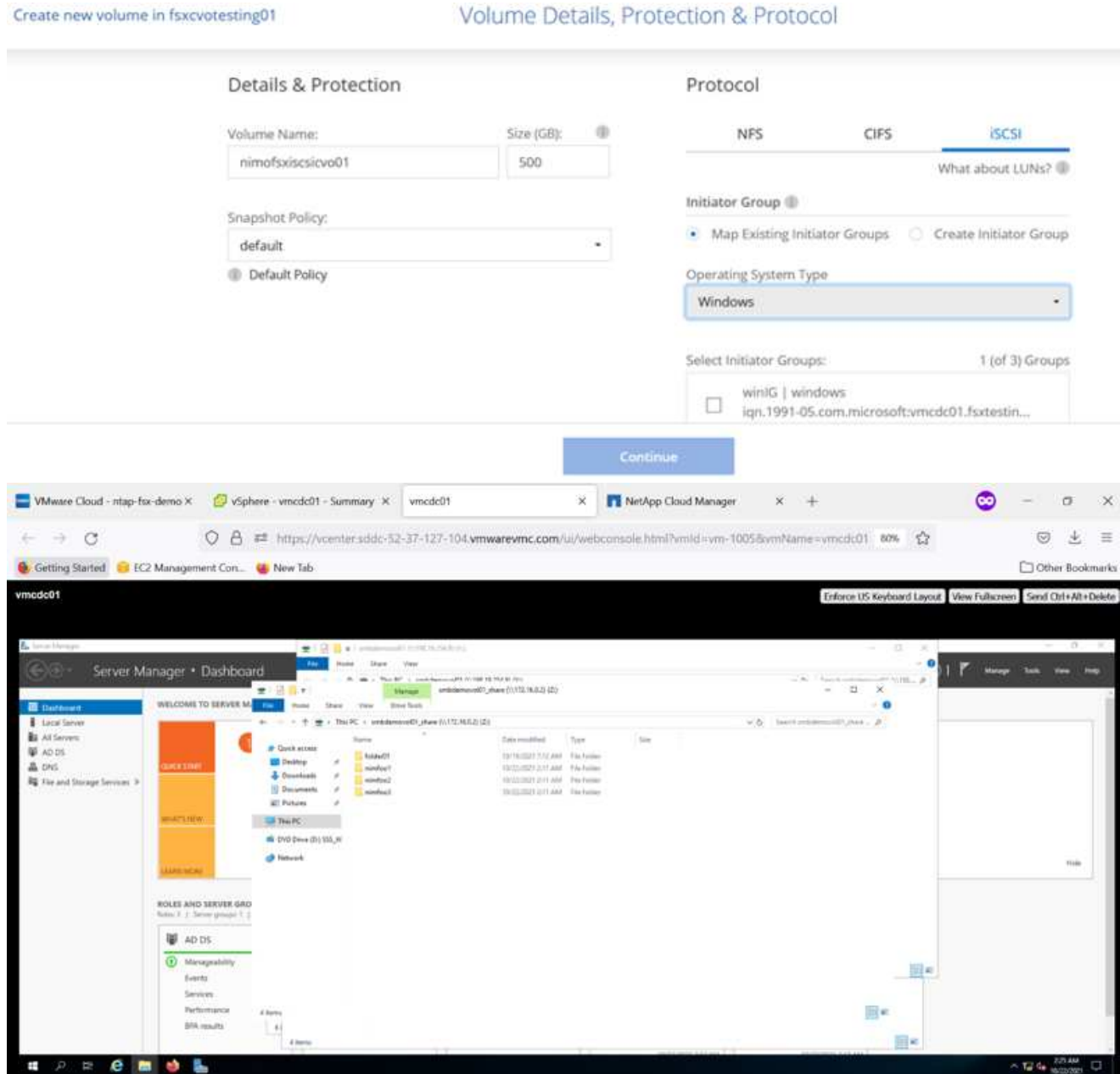
If the primary node goes offline, mount the volume by using the HA partner's IP address:



## Connect the LUN to a host

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

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



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.

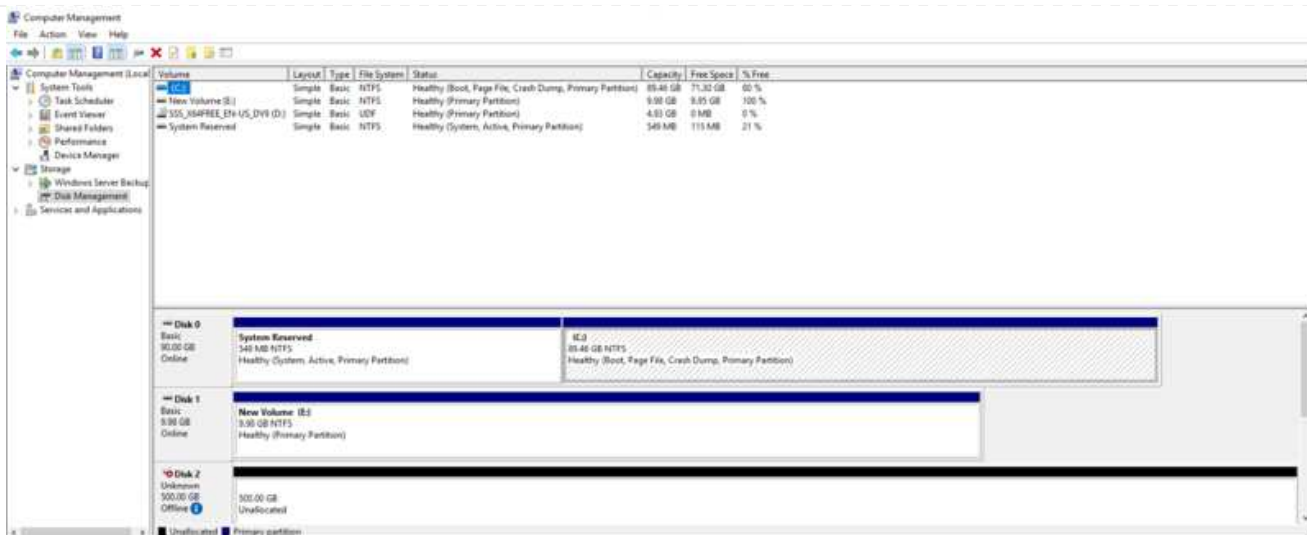


The Windows host must have an iSCSI connection to each node in the cluster. The native DSM selects the best paths to use.



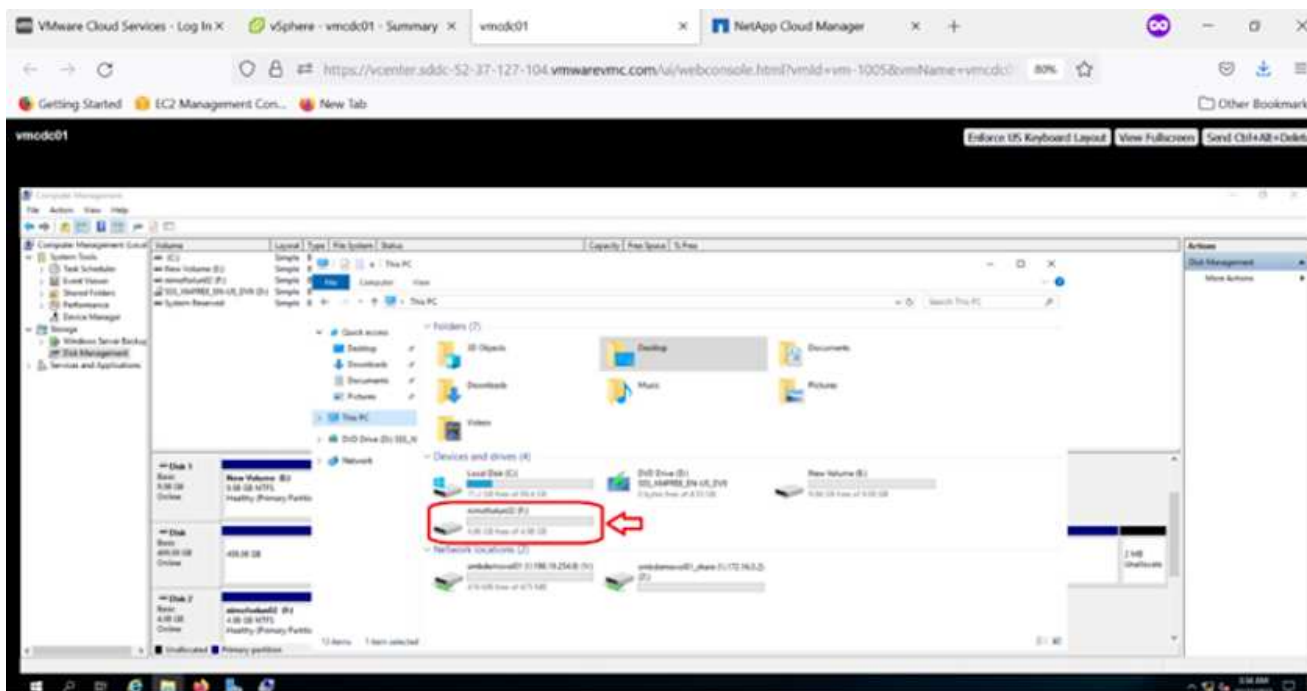
LUNs from the SVM appear as disks to the Windows host. Any new disks that are added are not automatically discovered by the host. Trigger a manual rescan to discover the disks by completing the following steps:

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



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

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



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

## Mount Cloud Volumes ONTAP NFS volume on Linux client

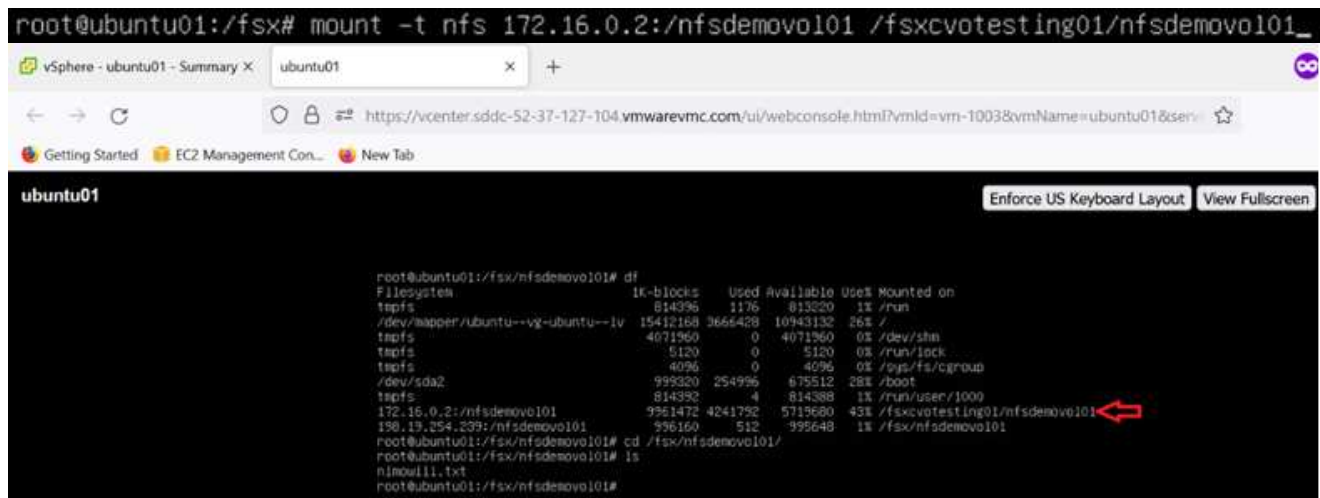
To mount the Cloud Volumes ONTAP (DIY) file system from VMs within VMC on AWS SDDC, complete the following steps:

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

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

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

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



The screenshot shows a terminal window titled 'ubuntu01' with the command `mount -t nfs 172.16.0.2:/nfsdemovol01 /fsxcvotesting01/nfsdemovol01_` entered. Below the command, the output of the `df` command is displayed, showing the newly mounted NFS volume. A red arrow points to the line `172.16.0.2:/nfsdemovol01` in the output.

Filesystem	1k-blocks	Used	Available	Use%	Mounted on
tmpfs	814396	1176	813220	1%	/run
/dev/mapper/ubuntu--vg-ubuntu--lv	15412168	3666428	10943132	26%	/
tmpfs	4071960	0	4071960	0%	/dev/shm
tmpfs	5120	0	5120	0%	/run/lock
tmpfs	4096	0	4096	0%	/sys/fs/cgroup
/dev/sda2	999320	254996	675512	28%	/boot
tmpfs	814392	4	814388	1%	/run/user/1000
172.16.0.2:/nfsdemovol01	9961472	4241792	5719680	43%	/fsxcvotesting01/nfsdemovol01
198.19.254.239:/nfsdemovol01	996160	512	995648	1%	/fsx/nfsdemovol01



## 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.