NetApp

Provision volumes using a file service

Cloud Manager

NetApp
March 22, 2022

Table of Contents

Provision volumes using a file service

Azure NetApp Files

Learn about Azure NetApp Files

Azure NetApp Files enables enterprises to migrate and run their performance-intensive and latency-sensitive core, business-critical applications in Azure with no need to refactor for the cloud.

Features

- Support for multiple protocols enables "lift & shift" of both Linux & Windows applications to run seamlessly in Azure.
- Multiple performance tiers allow for close alignment with workload performance requirements.
- Leading certifications including SAP HANA, GDPR, and HIPAA enables migration of the most demanding workloads to Azure.

Additional features in Cloud Manager

- Migrate NFS or SMB data to Azure NetApp Files directly from Cloud Manager. Data migrations are powered by NetApp's Cloud Sync service. Learn more.
- Using Artificial Intelligence (AI) driven technology, Cloud Data Sense can help you understand data context and identify sensitive data that resides in your Azure NetApp Files accounts. Learn more.

Cost

View Azure NetApp Files pricing.

Note that your subscription and charging are maintained by the Azure NetApp Files service and not by Cloud Manager.

Supported regions

View supported Azure regions.

Getting help

For technical support issues associated with Azure NetApp Files, use the Azure portal to log a support request to Microsoft. Select your associated Microsoft subscription and select the **Azure NetApp Files** service name under **Storage**. Provide the remaining information required to create your Microsoft support request.

For issues related to Cloud Sync and Azure NetApp Files, you can start with NetApp using your Cloud Sync serial number directly from the Cloud Sync service. You will need to access the Cloud Sync service through the link in Cloud Manager. View the process to enable Cloud Sync support.

Related links

- NetApp Cloud Central: Azure NetApp Files
- Azure NetApp Files documentation

- Cloud Sync documentation

Setting up and discovering Azure NetApp Files

Create an Azure NetApp Files working environment in Cloud Manager to create and manage NetApp accounts, capacity pools, volumes, and snapshots.

If you haven't set up Azure NetApp Files yet, you'll need to complete all of the steps on this page.

If you already set up Azure NetApp Files from outside of Cloud Manager, then you simply need to set up an Azure AD application and then create the Azure NetApp Files working environment.

Quick start

Get started quickly by following these steps or scroll down to the remaining sections for full details.

1   **Set up an Azure AD application**

From Azure, grant permissions to an Azure AD application and copy the application (client) ID, the directory (tenant) ID, and the value of a client secret.

2   **Create an Azure NetApp Files working environment**

In Cloud Manager, click **Add Working Environment** > **Microsoft Azure** > **Azure NetApp Files** and then provide details about the AD application.

Setting up an Azure AD application

Cloud Manager needs permissions to set up and manage Azure NetApp Files. You can grant the required permissions to an Azure account by creating and setting up an Azure AD application and by obtaining the Azure credentials that Cloud Manager needs.

Creating the AD application

Create an Azure Active Directory (AD) application and service principal that Cloud Manager can use for role-based access control.

Before you begin

You must have the right permissions in Azure to create an Active Directory application and to assign the application to a role. For details, refer to Microsoft Azure Documentation: Required permissions.

Steps

1. From the Azure portal, open the **Azure Active Directory** service.

2. In the menu, click **App registrations**.

3. Create the application:

   a. Click **New registration**.

   b. Specify details about the application:

      ▪ **Name**: Enter a name for the application.

      ▪ **Account type**: Select an account type (any will work with Cloud Manager).

      ▪ **Redirect URI**: You can leave this blank.

   c. Click **Register**.

4. Copy the **Application (client) ID** and the **Directory (tenant) ID**.

When you create the Azure NetApp Files working environment in Cloud Manager, you need to provide the application (client) ID and the directory (tenant) ID for the application. Cloud Manager uses the IDs to programmatically sign in.

5. Create a client secret for the application so Cloud Manager can use it to authenticate with Azure AD:

   a. Click **Certificates & secrets > New client secret**.

   b. Provide a description of the secret and a duration.

   c. Click **Add**.

   d. Copy the value of the client secret.
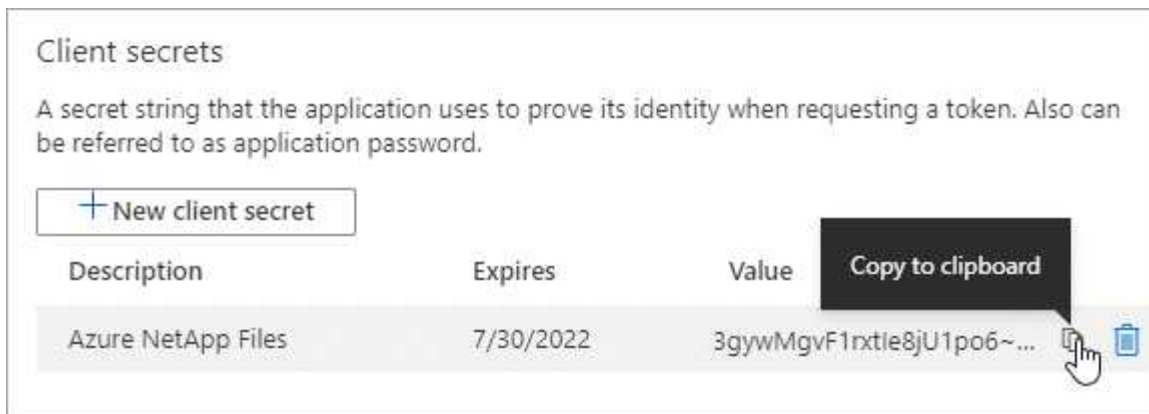
Result

Your AD application is now setup and you should have copied the application (client) ID, the directory (tenant) ID, and the value of the client secret. You need to enter this information in Cloud Manager when you add an Azure NetApp Files working environment.

Assigning the app to a role

You must bind the service principal to your Azure subscription and assign it a custom role that has the required permissions.

Steps

1. Create a custom role in Azure.

   The following steps describe how to create the role from the Azure portal.

   a. Open the subscription and click **Access control (IAM)**.

   b. Click **Add > Add custom role**.

c. In the **Basics** tab, enter a name and description for the role.

d. Click **JSON** and click **Edit** which appears at the top right of the JSON format.

e. Add the following permission under *actions*:

```
"actions": [
    "Microsoft.NetApp/*",
    ],
```

f. Click **Save**, click **Next**, and then click **Create**.

2. Now assign the application to the role that you just created:

a. From the Azure portal, open the **Subscriptions** service.

b. Select the subscription.

c. Click **Access control (IAM) > Add > Add role assignment**.

d. In the **Role** tab, select the custom role that you created and click **Next**.

e. In the **Members** tab, complete the following steps:

  ▪ Keep **User, group, or service principal** selected.

  ▪ Click **Select members**.

  ▪ Search for the name of the application.

  Here's an example:

> - Select the application and click **Select**.
> - Click **Next**.

f. Click **Review + assign**.

The service principal for Cloud Manager now has the required Azure permissions for that subscription.

Creating an Azure NetApp Files working environment

Set up an Azure NetApp Files working environment in Cloud Manager so you can start creating volumes.

1. From the Canvas page, click **Add Working Environment**.
2. Select **Microsoft Azure** and then **Azure NetApp Files**.
3. Provide details about the AD application that you previously set up.

Azure NetApp Files Credentials

Working Environment Name

ANF

Application (client) ID

e461f4ca-9d9a-4aec-8f39-fc842b684c97

Client Secret

••••••••••••••••••••••••••••••

Directory (tenant) ID

8e21f23a-10b9-46fb-9d50-720ef604be98

4. Click **Add**.

Result

You should now have an Azure NetApp Files working environment.

What's next?

Start creating and managing volumes.

Creating and managing volumes for Azure NetApp Files

After you set up your working environment, you can create and manage Azure NetApp Files accounts, capacity pools, volumes, and snapshots.

Creating volumes

You can create NFS or SMB volumes in a new or existing Azure NetApp Files account.

A Cloud Manager feature called "templates" enables you to create volumes that are optimized for the workload requirements for certain applications; such as databases or streaming services. If your organization has created volume templates that you should use, follow these steps.

Before you begin

- If you want to use SMB, you must have set up DNS and Active Directory.
- When planning to create an SMB volume, you must have a Windows Active Directory server available to which you can connect. You will enter this information when creating the volume.

Steps

1. Open the Azure NetApp Files working environment.
2. Click **Add New Volume**.
3. Provide the required information on each page:
   - **Azure NetApp Files Account**: Choose an existing Azure NetApp Files account or create a new account. When creating a new account you can also choose the Resource Group that you want to use.

   - **Capacity Pool**: Select an existing capacity pool or create a new capacity pool.

     If you create a new capacity pool, you need to specify a size and select a service level.

     The minimum size for the capacity pool is 4 TB. You can specify a size in multiples of 4 TB.

   - **Details & Tags**: Enter a volume name and size, the VNet and subnet where the volume should reside, and optionally specify tags for the volume.
   - **Protocol**: Choose the NFS or SMB protocol and enter the required information.

     Here's an example of details for NFS.

Here's an example of details for SMB. You'll need to provide Active Directory information on the next page when you set up your first SMB volume.

4. If you want this volume to be created based on a snapshot of an existing volume, select the snapshot from the Snapshot Name drop-down list.

5. Click **Add Volume**.

Result

The new volume is added to the working environment.

Continue with mounting the cloud volume.

Creating volumes from templates

If your organization has created ANF volume templates so you can deploy volumes that are optimized for the workload requirements for certain applications, follow the steps in this section.

The template should make your job easier because certain volume parameters will already be defined in the template, such as capacity pool, size, protocol, VNet and subnet where the volume should reside, and more. When a parameter is already predefined, you can just skip to the next volume parameter.

Steps

1. On the Canvas page, click the Azure NetApp Files working environment on which you want to provision a volume.

2. Click ⋮ > **Add Volume From Template**.

3. In the *Select Template* page, select the template that you want to use to create the volume and click **Next**.
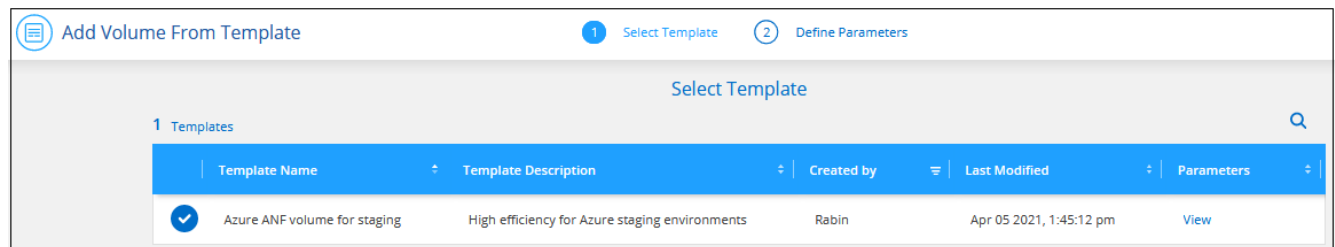
The *Define Parameters* page is displayed.

Note: You can click the checkbox **Show read-only parameters** to show all the fields that have been locked by the template if you want to see the values for those parameters. By default these predefined fields are hidden and only the fields you need to complete are shown.

4. Add values for all of the parameters that are not hard-coded from the template. See creating volumes for details about all the parameters you need to complete to deploy an ANF volume.

5. Click **Run Template** after you have defined all the parameters needed for this volume.

Result

Cloud Manager provisions the volume and displays a page so that you can see the progress.

Then the new volume is added to the working environment.

Continue with mounting the cloud volume.

Mounting volumes

Access mounting instructions from within Cloud Manager so you can mount the volume to a host.

Steps
1. Open the working environment.
2. Hover over the volume and select **Mount the volume**.

3. Follow the instructions to mount the volume.

Editing a volume's size and tags

After you create a volume, you can modify its size and tags at any time.

Steps
1. Open the working environment.
2. Hover over the volume and select **Edit**.
3. Modify the size and tags as needed.
4. Click **Apply**.

Changing the volume's service level

After you create a volume, you can change the service level at any time as long as the destination capacity pool already exists.

Steps

1. Open the working environment.

2. Hover over the volume and select **Change service level**.

3. Select the capacity pool that provides the service level that you want.

4. Click **Change**.

Result

The volume is moved to the other capacity pool with no impact to the volume.

Managing Snapshot copies

Snapshot copies provide a point-in-time copy of your volume. Create Snapshot copies, restore the data to a new volume, and delete Snapshot copies.

Steps

1. Open the working environment.

2. Hover over the volume and choose one of the available options to manage Snapshot copies:

   ◦ **Create a Snapshot copy**

   ◦ **Revert volume to Snapshot**

   ◦ **Delete a Snapshot copy**

3. Follow the prompts to complete the selected action.

Deleting volumes

Delete the volumes that you no longer need.

Steps

1. Open the working environment.

2. Hover over the volume and click **Delete**.

3. Confirm that you want to delete the volume.

Removing Azure NetApp Files

This action removes Azure NetApp Files from Cloud Manager. It doesn't delete your Azure NetApp Files account or volumes. You can add Azure NetApp Files back to Cloud Manager at any time.

Steps

1. Open the Azure NetApp Files working environment.

2. At the top right of the page, select the actions menu and click **Remove Azure NetApp Files**.
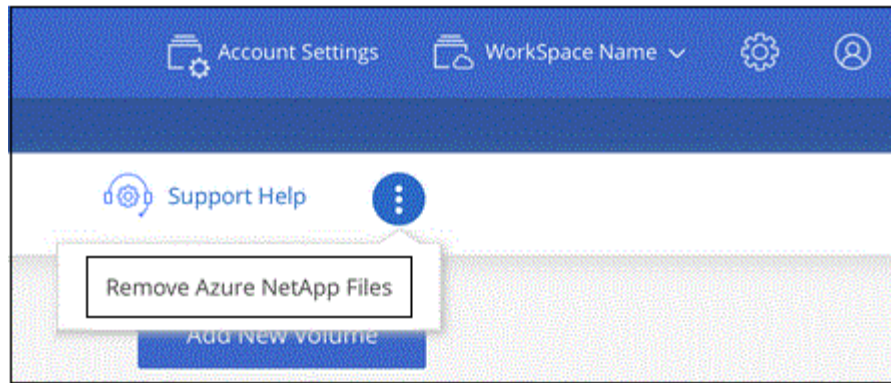
3. Click **Remove** to confirm.

Amazon FSx for ONTAP

Learn about Amazon FSx for ONTAP

Amazon FSx for ONTAP is a fully managed service allowing customers to launch and run file systems powered by NetApp's ONTAP storage operating system. FSx for ONTAP provides the same features, performance, and administrative capabilities NetApp customers use on premises, with the simplicity, agility, security, and scalability of a native AWS service.

Features

- No need to configure or manage storage devices, software, or backups.
- Support for CIFS, NFSv3, NFSv4.x, and SMB v2.0 - v3.1.1 protocols.
- Low cost, virtually unlimited data storage capacity using available Infrequently Accessed (IA) storage tier.
- Certified to run on latency-sensitive applications including Oracle RAC.
- Choice of bundled and pay-as-you-go pricing.

Additional features in Cloud Manager

- Using a Connector in AWS and Cloud Manager, you can create and manage volumes, replicate data, and integrate FSx for ONTAP with NetApp cloud services, such as Data Sense and Cloud Sync.
- Using Artificial Intelligence (AI) driven technology, Cloud Data Sense can help you understand data context and identify sensitive data that resides in your FSx for ONTAP accounts. Learn more.
- Using NetApp Cloud Sync, you can automate data migration to any target in the cloud or on premises. Learn more

Cost

Your FSx for ONTAP account is maintained by AWS and not by Cloud Manager. Amazon FSx for ONTAP getting started guide

There is an additional cost associated with using the Connector in AWS and the optional data services such as Cloud Sync and Data Sense.

Supported regions

View supported Amazon regions.

Getting help

Amazon FSx for ONTAP is an AWS first-party solution. For questions or technical support issues associated with your AWS FSx file system, infrastructure or any AWS solution using this service, use the Support Center in your AWS console to open a support case to AWS. Select the "FSx for ONTAP" service and appropriate category. Provide the remaining information required to create your AWS support case.

For general questions specific to Cloud Manager or Cloud Manager micro-services, you can start with the in-line Cloud Manager chat.

For technical support issues specific to Cloud Manager or micro-services within, you can open a NetApp support ticket using your Cloud Manager account level serial number. You will need to register your Cloud Manager serial number to activate support.

Limitations

- Cloud Manager can replicate data only from on-premises or Cloud Volumes ONTAP to FSx for ONTAP.
- At this time iSCSI volumes can be created using the ONTAP CLI, ONTAP API, or Cloud Manager API.

Get started with Amazon FSx for ONTAP

Get started with Amazon FSx for ONTAP in a few steps.

You can get started with FSx for ONTAP in just a few steps.

1   **Create an FSx for ONTAP working environment**

You must create an Amazon FSx for ONTAP working environment before adding volumes. You will need to set up an IAM role that enables the Cloud Manager SaaS to assume the role.

2   **Create a Connector**

You must have a Connector for AWS to open the FSx for ONTAP working environment, create volumes, or perform other actions. When a Connector is required, Cloud Manager will prompt you if one is not already added.

3   **Add volumes**

You can create FSx for ONTAP volumes using Cloud Manager.

4   **Manage your volumes**

Use Cloud Manager to manage your volumes and configure additional services such as replication, Cloud Sync, and Data Sense.

Related links

- [Creating a Connector from Cloud Manager](#)
- [Launching a Connector from the AWS Marketplace](#)
- [Installing the Connector software on a Linux host](#)

Set up permissions for FSx for ONTAP

To create or manage an Amazon FSx for ONTAP working environment, you need to add AWS credentials to Cloud Manager by providing the ARN of an IAM role that gives Cloud Manager the permissions needed to create an FSx for ONTAP working environment.

Set up the IAM role

Set up an IAM role that enables the Cloud Manager SaaS to assume the role.

Steps

1. Go to the IAM console in the target account.

2. Under Access Management, click **Roles > Create Role** and follow the steps to create the role.

   Be sure to do the following:

   - Under **Trusted entity type**, select **AWS account**.

   - Select **Another AWS account** and enter the ID of the Cloud Manager SaaS: 952013314444

   - Create a policy that includes the following permissions:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "fsx:*",
                "ec2:Describe*",
                "ec2:CreateTags",
                "kms:Describe*",
                "kms:List*",
                "iam:CreateServiceLinkedRole"
            ],
            "Resource": "*"
        }
    ]
}
```

3. Copy the Role ARN of the IAM role so that you can paste it in Cloud Manager in the next step.

Result

The IAM role now has the required permissions.

Add the credentials

After you provide the IAM role with the required permissions, add the role ARN to Cloud Manager.

Before you get started

If you just created the IAM role, it might take a few minutes until they are available for use. Wait a few minutes before you add the credentials to Cloud Manager.

Steps

1. In the upper right of the Cloud Manager console, click the Settings icon, and select **Credentials**.

2. Click **Add Credentials** and follow the steps in the wizard.

   a. **Credentials Location**: Select **Amazon Web Services > Cloud Manager**.

   b. **Define Credentials**: Provide the ARN (Amazon Resource Name) of the IAM role.

   c. **Review**: Confirm the details about the new credentials and click **Add**.

Result

You can now use the credentials when creating an FSx for ONTAP working environment.

Related links

- AWS credentials and permissions
- Managing AWS credentials for Cloud Manager

Security group rules for FSx for ONTAP

Cloud Manager creates AWS security groups that include the inbound and outbound rules that Cloud Manager and FSx for ONTAP need to operate successfully. You might want to refer to the ports for testing purposes or if you need to use your own.

Rules for FSx for ONTAP

The security group for FSx for ONTAP requires both inbound and outbound rules.

Inbound rules

The source for inbound rules in the predefined security group is 0.0.0.0/0.

Protocol	Port	Purpose
All ICMP	All	Pinging the instance
HTTP	80	HTTP access to the System Manager web console using the IP address of the cluster management LIF

Protocol	Port	Purpose
HTTPS	443	HTTPS access to the System Manager web console using the IP address of the cluster management LIF
SSH	22	SSH access to the IP address of the cluster management LIF or a node management LIF
TCP	111	Remote procedure call for NFS
TCP	139	NetBIOS service session for CIFS
TCP	161-162	Simple network management protocol
TCP	445	Microsoft SMB/CIFS over TCP with NetBIOS framing
TCP	635	NFS mount
TCP	749	Kerberos
TCP	2049	NFS server daemon
TCP	3260	iSCSI access through the iSCSI data LIF
TCP	4045	NFS lock daemon
TCP	4046	Network status monitor for NFS
TCP	10000	Backup using NDMP
TCP	11104	Management of intercluster communication sessions for SnapMirror
TCP	11105	SnapMirror data transfer using intercluster LIFs
UDP	111	Remote procedure call for NFS
UDP	161-162	Simple network management protocol
UDP	635	NFS mount
UDP	2049	NFS server daemon
UDP	4045	NFS lock daemon
UDP	4046	Network status monitor for NFS
UDP	4049	NFS rquotad protocol

Outbound rules

The predefined security group for FSx for ONTAP opens all outbound traffic. If that is acceptable, follow the basic outbound rules. If you need more rigid rules, use the advanced outbound rules.

Basic outbound rules

The predefined security group for FSx for ONTAP includes the following outbound rules.

Protocol	Port	Purpose
All ICMP	All	All outbound traffic
All TCP	All	All outbound traffic
All UDP	All	All outbound traffic

Advanced outbound rules

If you need rigid rules for outbound traffic, you can use the following information to open only those ports that are required for outbound communication by FSx for ONTAP.

> ℹ️ The source is the interface (IP address) on the FSx for ONTAP system.

Service	Protocol	Port	Source	Destination	Purpose
Active Directory	TCP	88	Node management LIF	Active Directory forest	Kerberos V authentication
	UDP	137	Node management LIF	Active Directory forest	NetBIOS name service
	UDP	138	Node management LIF	Active Directory forest	NetBIOS datagram service
	TCP	139	Node management LIF	Active Directory forest	NetBIOS service session
	TCP & UDP	389	Node management LIF	Active Directory forest	LDAP
	TCP	445	Node management LIF	Active Directory forest	Microsoft SMB/CIFS over TCP with NetBIOS framing
	TCP	464	Node management LIF	Active Directory forest	Kerberos V change & set password (SET_CHANGE)
	UDP	464	Node management LIF	Active Directory forest	Kerberos key administration
	TCP	749	Node management LIF	Active Directory forest	Kerberos V change & set Password (RPCSEC_GSS)
	TCP	88	Data LIF (NFS, CIFS, iSCSI)	Active Directory forest	Kerberos V authentication
	UDP	137	Data LIF (NFS, CIFS)	Active Directory forest	NetBIOS name service
	UDP	138	Data LIF (NFS, CIFS)	Active Directory forest	NetBIOS datagram service
	TCP	139	Data LIF (NFS, CIFS)	Active Directory forest	NetBIOS service session
	TCP & UDP	389	Data LIF (NFS, CIFS)	Active Directory forest	LDAP
	TCP	445	Data LIF (NFS, CIFS)	Active Directory forest	Microsoft SMB/CIFS over TCP with NetBIOS framing
	TCP	464	Data LIF (NFS, CIFS)	Active Directory forest	Kerberos V change & set password (SET_CHANGE)
	UDP	464	Data LIF (NFS, CIFS)	Active Directory forest	Kerberos key administration
	TCP	749	Data LIF (NFS, CIFS)	Active Directory forest	Kerberos V change & set password (RPCSEC_GSS)
Backup to S3	TCP	5010	Intercluster LIF	Backup endpoint or restore endpoint	Back up and restore operations for the Backup to S3 feature

Service	Protocol	Port	Source	Destination	Purpose
Cluster	All traffic	All traffic	All LIFs on one node	All LIFs on the other node	Intercluster communications (Cloud Volumes ONTAP HA only)
	TCP	3000	Node management LIF	HA mediator	ZAPI calls (Cloud Volumes ONTAP HA only)
	ICMP	1	Node management LIF	HA mediator	Keep alive (Cloud Volumes ONTAP HA only)
DHCP	UDP	68	Node management LIF	DHCP	DHCP client for first-time setup
DHCPS	UDP	67	Node management LIF	DHCP	DHCP server
DNS	UDP	53	Node management LIF and data LIF (NFS, CIFS)	DNS	DNS
NDMP	TCP	18600–18699	Node management LIF	Destination servers	NDMP copy
SMTP	TCP	25	Node management LIF	Mail server	SMTP alerts, can be used for AutoSupport
SNMP	TCP	161	Node management LIF	Monitor server	Monitoring by SNMP traps
	UDP	161	Node management LIF	Monitor server	Monitoring by SNMP traps
	TCP	162	Node management LIF	Monitor server	Monitoring by SNMP traps
	UDP	162	Node management LIF	Monitor server	Monitoring by SNMP traps
SnapMirror	TCP	11104	Intercluster LIF	ONTAP intercluster LIFs	Management of intercluster communication sessions for SnapMirror
	TCP	11105	Intercluster LIF	ONTAP intercluster LIFs	SnapMirror data transfer
Syslog	UDP	514	Node management LIF	Syslog server	Syslog forward messages

Rules for the Connector

The security group for the Connector requires both inbound and outbound rules.

Inbound rules

Protocol	Port	Purpose
SSH	22	Provides SSH access to the Connector host

Protocol	Port	Purpose
HTTP	80	Provides HTTP access from client web browsers to the local user interface and connections from Cloud Data Sense
HTTPS	443	Provides HTTPS access from client web browsers to the local user interface
TCP	3128	Provides the Cloud Data Sense instance with internet access, if your AWS network doesn't use a NAT or proxy

Outbound rules

The predefined security group for the Connector opens all outbound traffic. If that is acceptable, follow the basic outbound rules. If you need more rigid rules, use the advanced outbound rules.

Basic outbound rules

The predefined security group for the Connector includes the following outbound rules.

Protocol	Port	Purpose
All TCP	All	All outbound traffic
All UDP	All	All outbound traffic

Advanced outbound rules

If you need rigid rules for outbound traffic, you can use the following information to open only those ports that are required for outbound communication by the Connector.

> (i) The source IP address is the Connector host.

Service	Protocol	Port	Destination	Purpose
Active Directory	TCP	88	Active Directory forest	Kerberos V authentication
	TCP	139	Active Directory forest	NetBIOS service session
	TCP	389	Active Directory forest	LDAP
	TCP	445	Active Directory forest	Microsoft SMB/CIFS over TCP with NetBIOS framing
	TCP	464	Active Directory forest	Kerberos V change & set password (SET_CHANGE)
	TCP	749	Active Directory forest	Active Directory Kerberos V change & set password (RPCSEC_GSS)
	UDP	137	Active Directory forest	NetBIOS name service
	UDP	138	Active Directory forest	NetBIOS datagram service
	UDP	464	Active Directory forest	Kerberos key administration
API calls and AutoSupport	HTTPS	443	Outbound internet and ONTAP cluster management LIF	API calls to AWS and ONTAP, and sending AutoSupport messages to NetApp

Service	Protocol	Port	Destination	Purpose
API calls	TCP	3000	ONTAP HA mediator	Communication with the ONTAP HA mediator
	TCP	8088	Backup to S3	API calls to Backup to S3
DNS	UDP	53	DNS	Used for DNS resolve by Cloud Manager
Cloud Data Sense	HTTP	80	Cloud Data Sense instance	Cloud Data Sense for Cloud Volumes ONTAP

Create and manage an Amazon FSx for ONTAP working environment

Using Cloud Manager you can create and manage FSx for ONTAP working environments to add and manage volumes and additional data services.

Create an Amazon FSx for ONTAP working environment

The first step is to create an FSx for ONTAP working environment. If you already created an FSx for ONTAP file system in the AWS Management Console, you can discover it using Cloud Manager.

Before you begin

Before creating your FSx for ONTAP working environment in Cloud Manager, you will need:

- The ARN of an IAM role that gives Cloud Manager the permissions needed to create an FSx for ONTAP working environment. See adding AWS credentials to Cloud Manager for details.
- The region and VPN information for where you will create the FSx for ONTAP instance.

Steps

1. In Cloud Manager, add a new Working Environment, select the location **Amazon Web Services**, and click **Next**.
2. Select **Amazon FSx for ONTAP** and click **Next**.

3. Authenticate FSx for ONTAP in Cloud Manager.

   a. If there is an existing IAM role in your account with the correct AWS permissions for FSx for ONTAP, select it from the dropdown.

   b. If there is no IAM role in your account, click **Credentials Page** and follow the steps in the wizard to add an ARN for an AWS IAM role with FSx for ONTAP credentials. See adding AWS credentials to Cloud Manager for details.
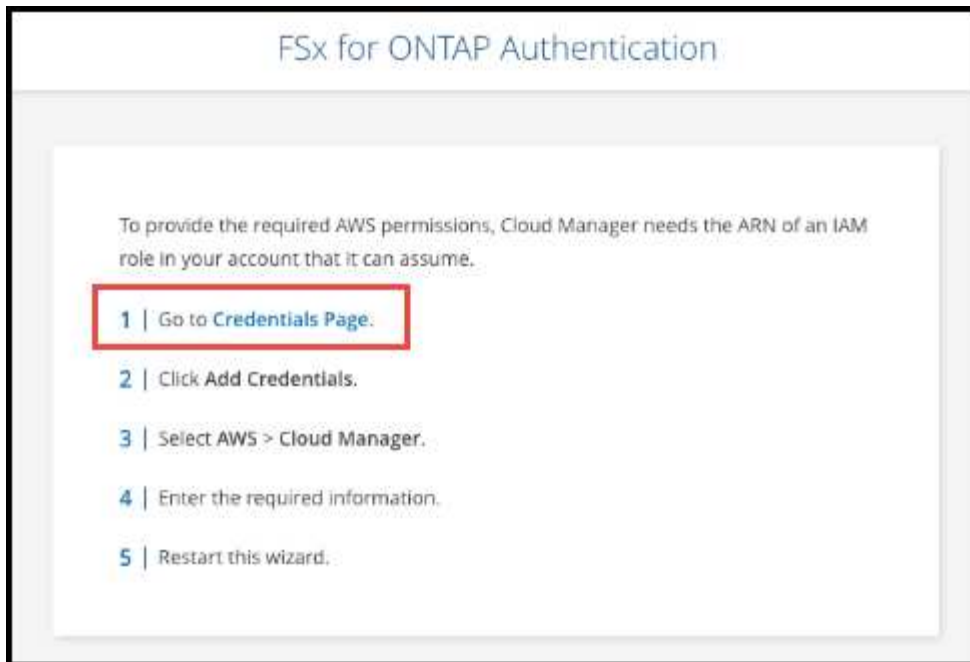
4. Provide information about your FSx for ONTAP instance:

   a. Enter the working environment name you want to use.

   b. Optionally, you can create tags by clicking the plus sign and entering a tag name and value.

   c. Enter and confirm the ONTAP Cluster password you want to use.

   d. Select the option to use the same password for your SVM user or set a different password.

   e. Click **Next**.

5. Provide region and VPC information:

   a. Select a region and VPC with subnets in at least two Availability Zones so each node is in a dedicated Availability Zone.

   b. Accept the default security group or select a different one. AWS security groups control inbound and outbound traffic. These are configured by your AWS admin and are associated with your AWS elastic

network interface (ENI).

    c. Select an Availability Zone and subnet for each node.

    d. Click **Next**.

6. Leave *CIDR Range* empty and click **Next** to automatically set an available range. Optionally, you can use AWS Transit Gateway to manually configure a range.

7. Select route tables that include routes to the floating IP addresses. If you have just one route table for the subnets in your VPC (the main route table), Cloud Manager automatically adds the floating IP addresses to that route table. Click **Next** to continue.

8. Accept the default AWS master key or click **Change Key** to select a different AWS Customer Master Key (CMK). For more information on CMK, see Setting up the AWS KMS. Click **Next** to continue.

9. Configure your storage:

   a. Select the throughput, capacity, and unit.

   b. You can optionally specify an IOPS value. If you don't specify an IOPS value, Cloud Manager will set a default value based on 3 IOPS per GiB of the total capacity entered. For example, if you enter 2000 GiB for the total capacity and no value for the IOPS, the effective IOPS value will be set to 6000.

> If you specify an IOPS value that does not meet the minimum requirements, you'll
> receive an error when adding the working environment.
>
> ⊗ Failed to create FSx for ONTAP systems Show Less ^ ✕
>
> Invalid SSD IOPS provided: 400 IOPS. Amazon FSx does not support provisioning fewer than 3 IOPS per GB of SSD storage capacity on a ONTAP file system.
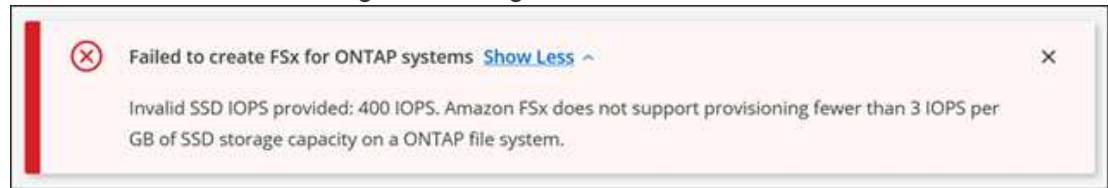
c. Click **Next**.

Add FSx for ONTAP	Storage Configuration

SSD Disk Properties

Throughput
512 MBps

Capacity
3

Unit
TiB

IOPS Value   *Optional* ⓘ
400

Notice: The current version of FSx does not allow changing the capacity after creation. Also, note that the capacity drives the cost of the service.

Previous   Next

10. Review your configuration:

    a. Click the tabs to review your ONTAP properties, provider properties, and networking configuration.

    b. Click **Previous** to make changes to any settings.

    c. Click **Add** to accept the settings and create your Working Environment.

Result

Cloud Manager displays your FSx for ONTAP configuration on the Canvas page.


You can now add volumes to your FSx for ONTAP working environment using Cloud Manager.

Discover an existing FSx for ONTAP file system

If you created an FSx for ONTAP file system using the AWS Management Console or if you want to restore a working environment you previously removed, you can discover it using Cloud Manager.

Steps

1. In Cloud Manager, click **Add Working Environment**, select **Amazon Web Services**.
2. Select **Amazon FSx for ONTAP** and click **Click Here**.
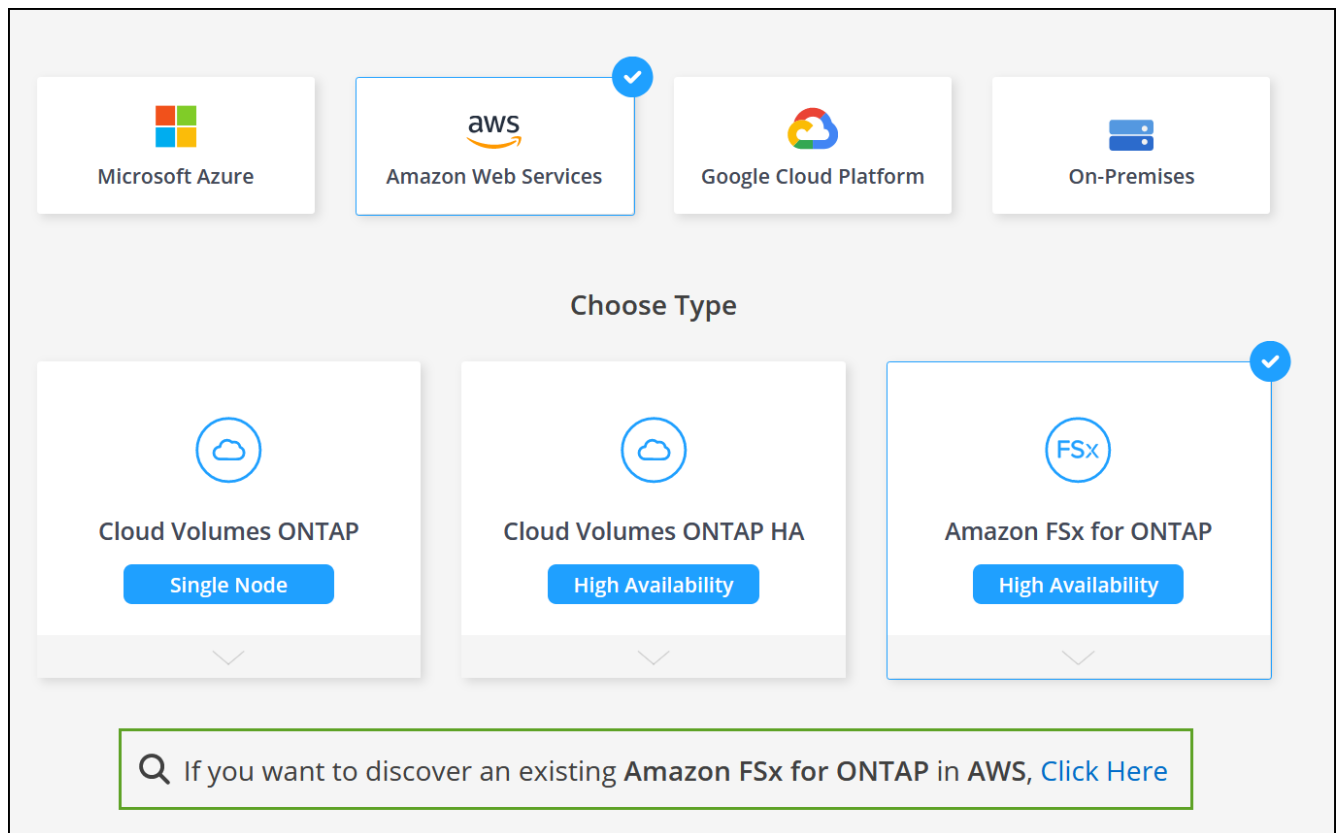
3. Select existing credentials or create new credentials. Click **Next**.
4. Select the AWS region and the working environment you want to add.

5. Click **Add**.

Result

Cloud Manager displays your discovered FSx for ONTAP file system.

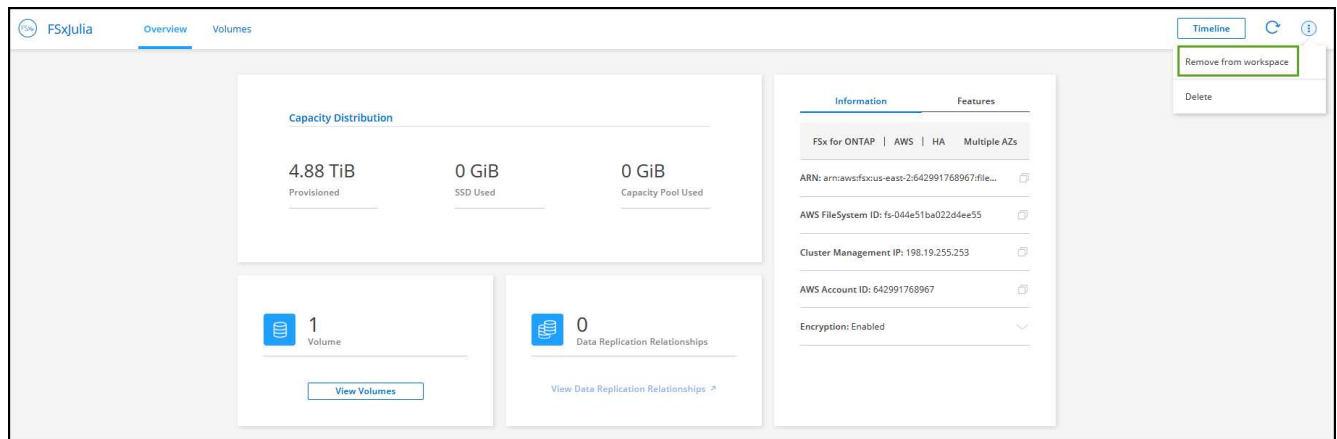**Remove FSx for ONTAP from the workspace**

You can remove FSx for ONTAP from Cloud Manager without deleting your FSx for ONTAP account or volumes. You can add the FSx for ONTAP working environment back to Cloud Manager at any time.

Steps

1. Open the working environment. If you don't have a Connector in AWS, you will see the prompt screen. You can ignore this and proceed with removing the working environment.

2. At the top right of the page, select the actions menu and click **Remove from workspace**.

3. Click **Remove** to remove FSx for ONTAP from Cloud Manager.

Delete the FSx for ONTAP working environment

You can delete the FSx for ONTAP from Cloud Manager.

Before you begin

- You must delete all volumes associated with the file system.

> ⓘ You will need an active Connector in AWS to remove or delete volumes.

- You cannot delete a working environment that contains failed volumes. Failed volumes must be deleted using the AWS Management Console or CLI prior to deleting FSx for ONTAP files system.

> ⚠ This action will delete all resources associated with the working environment. This action cannot be undone.

Steps

1. Open the working environment. If you don't have a Connector in AWS, you will see the prompt screen. You can ignore this and proceed to deleting the working environment.
2. At the top right of the page, select the actions menu and click **Delete**.
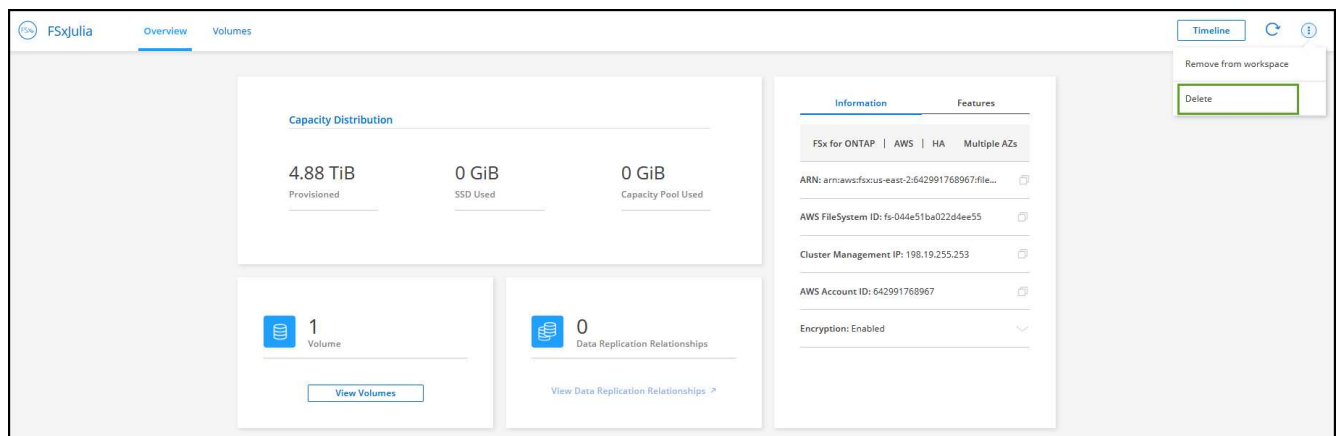
3. Enter the name of the working environment and click **Delete**.

Create and manage volumes for Amazon FSx for ONTAP

After you set up your working environment, you can create and manage FSx for ONTAP volumes, clones, and snapshots, and change tiering policies for FSx for ONTAP.

Create volumes

You can create and manage NFS and CIFS volumes from your FSx for ONTAP working environment in Cloud Manager. NFS and CIFS volumes created using ONTAP CLI will also be visible in your FSx for ONTAP working environment.

You can create iSCSI volumes using ONTAP CLI, ONTAP API, or Cloud Manager API and manage them using Cloud Manager in your FSx for ONTAP working environment.
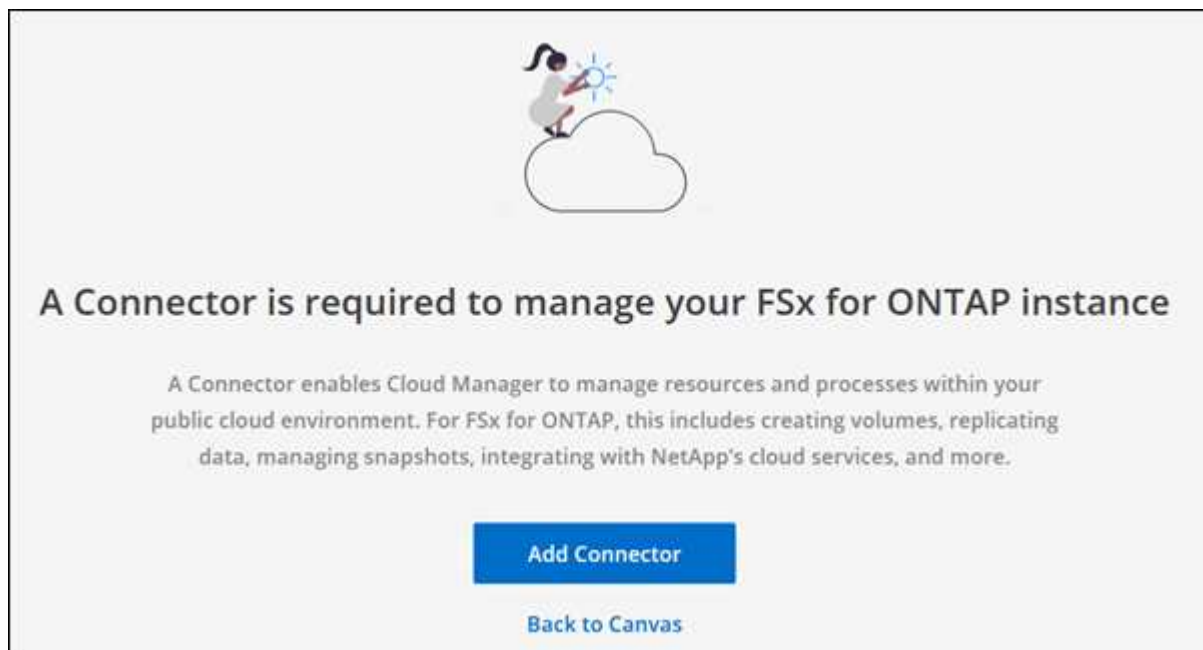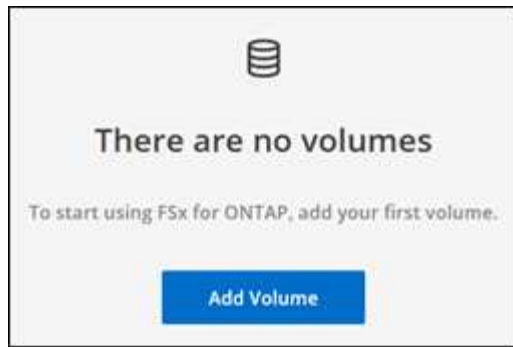
Before you begin

You need:

- An active Connector in AWS.
- If you want to use SMB, you must have set up DNS and Active Directory. For more information on DNS and Active Directory network configuration, see AWS: Prerequisites for using a self-managed Microsoft AD.

Steps

1. Open the FSx for ONTAP working environment.
2. If you don't have a Connector enabled, you'll be prompted to add one.

A Connector is required to manage your FSx for ONTAP instance

A Connector enables Cloud Manager to manage resources and processes within your public cloud environment. For FSx for ONTAP, this includes creating volumes, replicating data, managing snapshots, integrating with NetApp's cloud services, and more.

Add Connector

Back to Canvas

3. Click the **Volumes** tab
4. Click **Add Volume**.

5. **Volume Details and Protection**:

   a. Enter a name for your new volume.

   b. The Storage VM (SVM) fields auto-populates the SVM based on the name of your working environment.

   c. Enter the volume size and select a unit (GiB or TiB). Note that the volume size will grow with usage.

   d. Select a snapshot policy. By default, a snapshot is taken every hour (keeping the last six copies), every day (keeping the last two copies), and every week (keeping the last two copies).

   e. Click **Next**.

6. **Protocol**: Select the an NFS or CIFS volume protocol.

   a. For NFS:

      ▪ Select an Access Control policy.

      ▪ Select the NFS versions.

      ▪ Select a Custom Export Policy. Click the information icon for valid value criteria.

b. For CIFS:

- Enter a Share Name.

- Enter users or groups separated by a semicolon.

- Select the permission level for the volume.

If this is the first CIFS volume for this working environment, you will be prompted to configure CIFS connectivity using an *Active Directory* or *Workgroup* setup.

- If you select an Active Directory setup, you'll need to provide the following configuration information.

Field	Description
DNS Primary IP Address	The IP addresses of the DNS servers that provides name resolution for the CIFS server. The listed DNS server must contain the service location records (SRV) needed to locate the Active Directory LDAP servers and domain controllers for the domain the CIFS server will join.
Active Directory Domain to join	The FQDN of the Active Directory (AD) domain you want the CIFS server to join.
Credentials authorized to join the domain	The name and password of a Windows account with sufficient privileges to add computers to the specified Organizational Unit (OU) within the AD domain.
CIFS server NetBIOS name	A CIFS server name that is unique in the AD domain.
Organizational Unit	The organizational unit within the AD domain to associate with the CIFS server. The default is CN=Computers.
DNS Domain	The DNS domain for the storage virtual machine (SVM). In most cases, the domain is the same as the AD domain.
NTP Server	Select **Enable NTP Server Configuration** to configure an NTP server using the Active Directory DNS. If you need to configure an NTP server using a different address, then you should use the API. See the Cloud Manager automation docs for details.

- If you select a Workgroup setup, enter the server and workgroup name for a workgroup configured for CIFS.

   c. Click **Next**.

7. **Usage Profile and Tiering**:

   a. By default, **Storage Efficiency** is disabled. You can change this setting to enable deduplication and compression.

   b. By default, **Tiering Policy** is set to **Snapshot Only**. You can select a different tiering policy based on your needs.

   c. Click **Next**.

8. **Review**: Review your volume configuration. Click **Previous** to change settings or click **Add** to create the volume.

Result

The new volume is added to the working environment.

Mount volumes

Access mounting instructions from within Cloud Manager so you can mount the volume to a host.

Steps

1. Open the working environment.

2. Open the volume menu and select **Mount the volume**.

3. Follow the instructions to mount the volume.

Edit volumes

After you create a volume, you can modify it at any time.

Steps

1. Open the working environment.
2. Open the volume menu and select **Edit**.
   a. For NFS, you can modify the size and tags.
   b. For CIFS, you can modify the share name, users, permissions, and Snapshot policy as needed.
3. Click **Apply**.

Clone volumes

After you create a volume, you can create a new read-write volume from a new Snapshot.

Steps

1. Open the working environment.
2. Open the volume menu and select **Clone**.
3. Enter a name for the cloned volume.
4. Click **Clone**.

Manage Snapshot copies

Snapshot copies provide a point-in-time copy of your volume. Create Snapshot copies and restore the data to a new volume.

Steps

1. Open the working environment.
2. Open the volume menu and choose one of the available options to manage Snapshot copies:
   - **Create a Snapshot copy**
   - **Restore from a Snapshot copy**
3. Follow the prompts to complete the selected action.

Change the tiering policy

Change the tiering policy for the volume.

Steps

1. Open the working environment.
2. Open the volume menu and select **Change Tiering policy**.
3. Select a new volume tiering policy and click **Change**.

Replicate and sync data

You can replicate data between storage environments using Cloud Manager. To configure FSx for ONTAP replication, see replicating data between systems.

You can create sync relationships using Cloud Sync in Cloud Manager. To configure sync relationships, see

Delete volumes

Delete the volumes that you no longer need.

Before you begin

You cannot delete a volume that was previously part of a SnapMirror relationship using Cloud Manager. SnapMirror volumes must be deleted using the AWS Management Console or CLI.

Steps

1. Open the working environment.

2. Open the volume menu and select **Delete**.

3. Enter the working environment name and confirm that you want to delete the volume. It can take up to an hour before the volume is completely removed from Cloud Manager.

> (i) If you try to delete a cloned volume, you will receive an error.

Cloud Volumes Service for AWS

Learn about Cloud Volumes Service for AWS

NetApp Cloud Volumes Service for AWS is a cloud native file service that provides NAS volumes over NFS and SMB with all-flash performance. This service enables any workload, including legacy applications, to run in the AWS cloud.

> (i) With the launch of Amazon FSx for ONTAP, you can no longer create new CVS for AWS working environments in Cloud Manager. However, if you had previously added CVS for AWS working environments to Cloud Manager, you can continue to create and manage volumes.

Benefits of using Cloud Volumes Service for AWS

Cloud Volumes Service for AWS provides the following benefits:

- Fully managed service, therefore no need to configure or manage storage devices
- Support for NFSv3 and NFSv4.1, and SMB 3.0 and 3.1.1 NAS protocols
- Secure access to Linux and Windows Elastic Container Service (ECS) instances, with support including the following:
  - Amazon Linux 2, Red Hat Enterprise Linux 7.5, SLES 12 SP3, and Ubuntu 16.04 LTS
  - Windows Server 2008 R2, Windows Server 2012 R2, and Windows Server 2016
- Choice of bundled and pay-as-you-go pricing

Cost

Volumes created by the Cloud Volumes Service for AWS are charged based on your subscription to the service, not through Cloud Manager.

There are no charges to discover a Cloud Volumes Service for AWS region or volume from Cloud Manager.

Quick start

Get started quickly by following these steps, or go to the next sections for full details.

1   **Verify support for your configuration**

You must have set up AWS for Cloud Volumes Service and subscribed to one of the NetApp Cloud Volumes Service offerings on the AWS Marketplace and have an existing CVS for AWS working environment configured in Cloud Manager to create and manage volumes.

2   **Create, mount, and manage cloud volumes**

Using an existing CVS for AWS working environment, you can create, mount, and manage cloud volumes for existing CVS for AWS subscriptions using Cloud Manager.

Getting help

Use the Cloud Manager chat for general service questions.

For technical support issues associated with your cloud volumes, use your 20 digit "930" serial number located in the "Support" tab of the Cloud Volumes Service user interface. Use this support ID when opening a web ticket or calling for support. Be sure to activate your Cloud Volumes Service serial number for support from the Cloud Volumes Service user interface. Those steps are explained here.

Limitations

- Cloud Manager doesn't support data replication between working environments when using Cloud Volumes Service volumes.

- Removing your Cloud Volumes Service for AWS subscription from Cloud Manager isn't supported. You can do this only through the Cloud Volumes Service for AWS interface.

Related links

- NetApp Cloud Central: Cloud Volumes Service for AWS

- NetApp Cloud Volumes Service for AWS documentation

Managing Cloud Volumes Service for AWS

Cloud Manager enables you to create cloud volumes based on your Cloud Volumes Service for AWS subscription. You can also discover cloud volumes that you have already created from the Cloud Volumes Service interface and add them to a working environment.

ⓘ   With the launch of Amazon FSx for ONTAP, you can no longer create new CVS for AWS working environments in Cloud Manager. However, if you had previously added CVS for AWS working environments to Cloud Manager, you can continue to create and manage volumes.

Create cloud volumes

For configurations where volumes already exist in the Cloud Volumes Service working environment you can

use these steps to add new volumes.

For configurations where no volumes exist, you can create your first volume directly from Cloud Manager after you have set up your Cloud Volumes Service for AWS subscription. In the past, the first volume had to be created directly in the Cloud Volumes Service user interface.

Before you begin

- If you want to use SMB in AWS, you must have set up DNS and Active Directory.

- When planning to create an SMB volume, you must have a Windows Active Directory server available to which you can connect. You will enter this information when creating the volume. Also, make sure that the Admin user is able to create a machine account in the Organizational unit (OU) path specified.

- You will need this information when creating the first volume in a new region/working environment:

  ◦ AWS account ID: A 12-digit Amazon account identifier with no dashes. To find your account ID, refer to this AWS topic.

  ◦ Classless Inter-Domain Routing (CIDR) Block: An unused IPv4 CIDR block. The network prefix must range between /16 and /28, and it must also fall within the ranges reserved for private networks (RFC 1918). Do not choose a network that overlaps your VPC CIDR allocations.

Steps

1. Select a CVS for AWS working environment and click **Add New Volume**.

2. If you are adding the first volume to the working environment in the region, you have to add AWS networking information.

   a. Enter the IPv4 range (CIDR) for the region.

   b. Enter the 12-digit AWS account ID (with no dashes) to connect your Cloud Volumes account to your AWS account.

   c. Click **Continue**.

3. The Accepting Virtual Interfaces page describes some steps you will need to perform after you add the volume so that you are prepared to complete that step. Just click **Continue** again.

4. In the Details & Tags page, enter details about the volume:

   a. Enter a name for the volume.

   b. Specify a size within the range of 100 GiB to 90,000 GiB (equivalent to 88 TiBs).

   Learn more about allocated capacity.

   c. Specify a service level: Standard, Premium, or Extreme.

   Learn more about service levels.

   d. Enter one or more tag names to categorize the volume if you want.

   e. Click **Continue**.

5. In the Protocol page, select NFS, SMB, or Dual Protocol and then define the details. Required entries for NFS and SMB are shown in separate sections below.

6. In the Volume Path field, specify the name of the volume export you will see when you mount the volume.

7. If you select Dual-protocol you can select the security style by selecting NTFS or UNIX. Security styles affect the file permission type used and how permissions can be modified.

   ○ UNIX uses NFSv3 mode bits, and only NFS clients can modify permissions.

   ○ NTFS uses NTFS ACLs, and only SMB clients can modify permissions.

8. For NFS:

   a. In the NFS Version field, select NFSv3, NFSv4.1, or both depending on your requirements.

   b. Optionally, you can create an export policy to identify the clients that can access the volume. Specify the:

      ▪ Allowed clients by using an IP address or Classless Inter-Domain Routing (CIDR).

      ▪ Access rights as Read & Write or Read Only.

      ▪ Access protocol (or protocols if the volume allows both NFSv3 and NFSv4.1 access) used for users.

      ▪ Click **+ Add Export Policy Rule** if you want to define additional export policy rules.
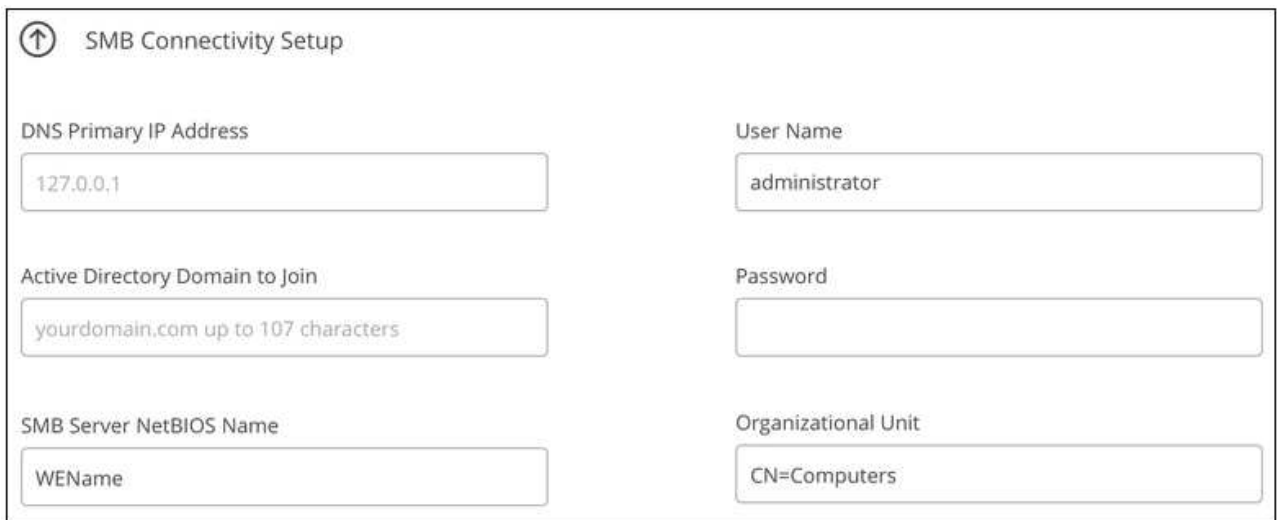
      The following image shows the Volume page filled out for the NFS protocol:

9. For SMB:

   a. You can enable SMB session encryption by checking the box for SMB Protocol Encryption.

   b. You can integrate the volume with an existing Windows Active Directory server by completing the fields in the Active directory section:

Field	Description
DNS Primary IP Address	The IP addresses of the DNS servers that provide name resolution for the SMB server. Use a comma to separate the IP addresses when referencing multiple servers, for example, 172.31.25.223, 172.31.2.74..
Active Directory Domain to join	The FQDN of the Active Directory (AD) domain that you want the SMB server to join. When using AWS Managed Microsoft AD, use the value from the "Directory DNS name" field.
SMB Server NetBIOS name	A NetBIOS name for the SMB server that will be created.
Credentials authorized to join the domain	The name and password of a Windows account with sufficient privileges to add computers to the specified Organizational Unit (OU) within the AD domain.
Organizational Unit	The organizational unit within the AD domain to associate with the SMB server. The default is CN=Computers for connections to your own Windows Active Directory server. If you configure AWS Managed Microsoft AD as the AD server for the Cloud Volumes Service, you should enter **OU=Computers,OU=corp** in this field.

The following image shows the Volume page filled out for the SMB protocol:

SMB Connectivity Setup

DNS Primary IP Address

127.0.0.1

User Name

administrator

Active Directory Domain to Join

yourdomain.com up to 107 characters

Password

SMB Server NetBIOS Name

WEName

Organizational Unit

CN=Computers

> You should follow the guidance on AWS security group settings to enable cloud volumes to integrate with Windows Active Directory servers correctly. See AWS security group settings for Windows AD servers for more information.

10. In the Volume from Snapshot page, if you want this volume to be created based on a snapshot of an existing volume, select the snapshot from the Snapshot Name drop-down list.

11. In the Snapshot Policy page, you can enable Cloud Volumes Service to create snapshot copies of your volumes based on a schedule. You can do this now or edit the volume later to define the snapshot policy.

   See Creating a snapshot policy for more information about snapshot functionality.

12. Click **Add Volume**.

The new volume is added to the working environment.

After you finish

If this is the first volume created in this AWS subscription, you need to launch the AWS Management Console to accept the two virtual interface that will be used in this AWS region to connect all your cloud volumes. See the NetApp Cloud Volumes Service for AWS Account Setup Guide for details.

You must accept the interfaces within 10 minutes after clicking the **Add Volume** button or the system may time out. If this happens, email cvs-support@netapp.com with your AWS Customer ID and NetApp Serial Number. Support will fix the issue and you can restart the onboarding process.

Then continue with Mounting the cloud volume.

Mount the cloud volume

You can mount a cloud volume to your AWS instance. Cloud volumes currently support NFSv3 and NFSv4.1 for Linux and UNIX clients, and SMB 3.0 and 3.1.1 for Windows clients.

Note: Please use the highlighted protocol/dialect supported by your client.

Steps

1. Open the working environment.

2. Hover over the volume and click **Mount the volume**.

NFS and SMB volumes display mount instructions for that protocol. Dual-protocol volumes provide both sets of instructions.

3. Hover over the commands and copy them to your clipboard to make this process easier. Just add the destination directory/mount point at the end of the command.

NFS example:

The maximum I/O size defined by the `rsize` and `wsize` options is 1048576, however 65536 is the recommended default for most use cases.

Note that Linux clients will default to NFSv4.1 unless the version is specified with the `vers=<nfs_version>` option.

SMB example:

Mount the volume - <Volume Name>

Mapping your network drive

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 this:

   \\test.cv-pm.local\silly-condescending-mcnulty

   To connect every time you log on to your computer, check the **Reconnect**

   at logon option.

5. Click **Finish**.

4. Connect to your Amazon Elastic Compute Cloud (EC2) instance by using an SSH or RDP client, and then follow the mount instructions for your instance.
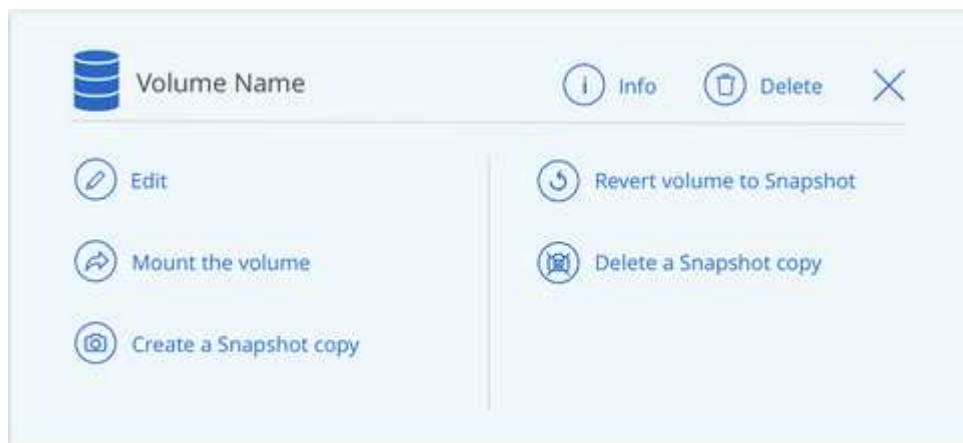
   After completing the steps in the mount instructions, you have successfully mounted the cloud volume to your AWS instance.

Managing existing volumes

You can manage existing volumes as your storage needs change. You can view, edit, restore, and delete volumes.

Steps

1. Open the working environment.

2. Hover over the volume.
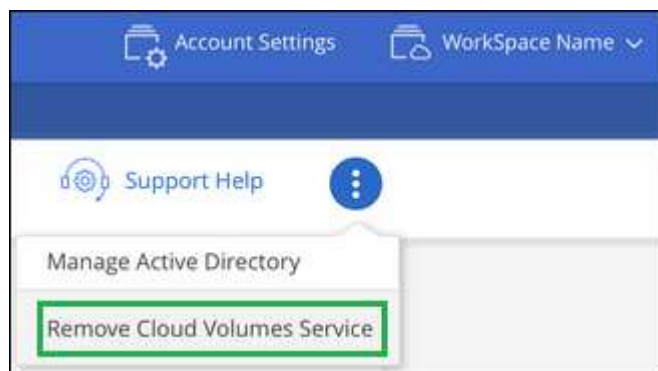

3. Manage your volumes:

Task	Action
View information about a volume	Select a volume, and then click **Info**.
Edit a volume (including snapshot policy)	a. Select a volume, and then click **Edit**. b. Modify the volume's properties and then click **Update**.
Get the NFS or SMB mount command	a. Select a volume, and then click **Mount the volume**. b. Click **Copy** to copy the command(s).
Create a Snapshot copy on demand	a. Select a volume, and then click **Create a Snapshot copy**. b. Change the snapshot name, if needed, and then click **Create**.
Replace the volume with the contents of a Snapshot copy	a. Select a volume, and then click **Revert volume to Snapshot**. b. Select a Snapshot copy and click **Revert**.
Delete a Snapshot copy	a. Select a volume, and then click **Delete a Snapshot copy**. b. Select the Snapshot copy you want to delete and click **Delete**. c. Click **Delete** again to confirm.
Delete a volume	a. Unmount the volume from all clients: ◦ On Linux clients, use the `umount` command. ◦ On Windows clients, click **Disconnect network drive**. b. Select a volume, and then click **Delete**. c. Click **Delete** again to confirm.

Remove Cloud Volumes Service from Cloud Manager

You can remove a Cloud Volumes Service for AWS subscription and all existing volumes from Cloud Manager. The volumes are not deleted, they are just removed from the Cloud Manager interface.

Steps

1. Open the working environment.

2. Click the ⋮ button at the top of the page and click **Remove Cloud Volumes Service**.

3. In the confirmation dialog box, click **Remove**.

Manage Active Directory configuration

If you change your DNS servers or Active Directory domain, you need to modify the SMB server in Cloud Volumes Services so that it can continue to serve storage to clients.

You can also delete the link to an Active Directory if you no longer need it.

Steps

1. Open the working environment.

2. Click the ⋮ button at the top of the page and click **Manage Active Directory**.

3. If no Active Directory is configured, you can add one now. If one is configured, you can modify the settings or delete it using the ⋮ button.

4. Specify the settings for the Active Directory that you want to join:

Field	Description
DNS Primary IP Address	The IP addresses of the DNS servers that provide name resolution for the SMB server. Use a comma to separate the IP addresses when referencing multiple servers, for example, 172.31.25.223, 172.31.2.74.
Active Directory Domain to join	The FQDN of the Active Directory (AD) domain that you want the SMB server to join. When using AWS Managed Microsoft AD, use the value from the "Directory DNS name" field.
SMB Server NetBIOS name	A NetBIOS name for the SMB server that will be created.
Credentials authorized to join the domain	The name and password of a Windows account with sufficient privileges to add computers to the specified Organizational Unit (OU) within the AD domain.
Organizational Unit	The organizational unit within the AD domain to associate with the SMB server. The default is CN=Computers for connections to your own Windows Active Directory server. If you configure AWS Managed Microsoft AD as the AD server for the Cloud Volumes Service, you should enter **OU=Computers,OU=corp** in this field.

5. Click **Save** to save your settings.

Manage cloud volumes snapshots

You can create a snapshot policy for each volume so that you can recover or restore the entire contents of a volume from an earlier time. You can also create an on-demand snapshot of a cloud volume when needed.
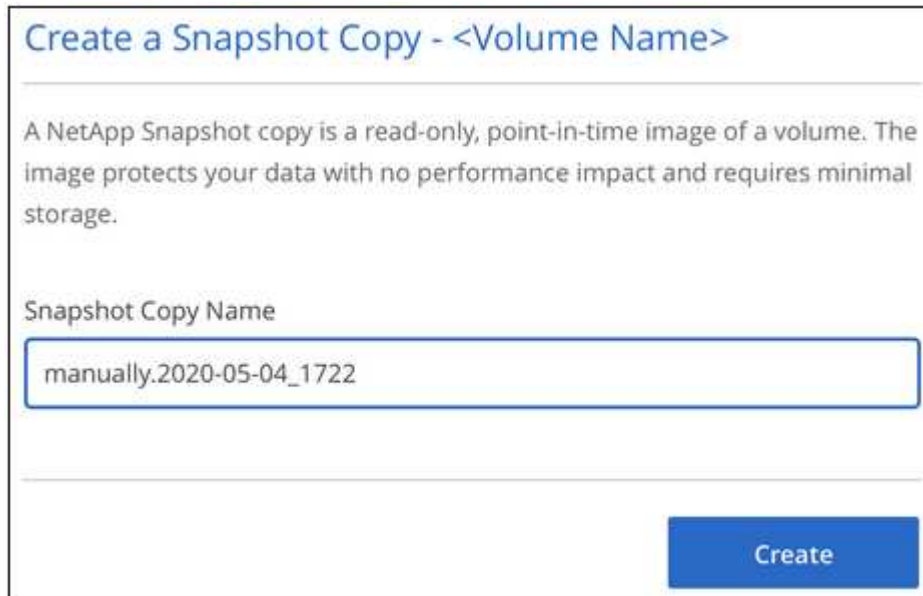
Create an on-demand snapshot

You can create an on-demand snapshot of a cloud volume if you want to create a snapshot with the current

volume state.

Steps

1. Open the working environment.

2. Hover over the volume and click **Create a snapshot copy**.

3. Enter a name for the snapshot, or use the automatically generated name, and click **Create**.

Create a Snapshot Copy - <Volume Name>

A NetApp Snapshot copy is a read-only, point-in-time image of a volume. The image protects your data with no performance impact and requires minimal storage.

Snapshot Copy Name

manually.2020-05-04_1722

Create

Create or modify a snapshot policy

You can create or modify a snapshot policy as necessary for a cloud volume. You define the snapshot policy from the *Snapshot Policy* tab either when creating a volume or when editing a volume.

Steps

1. Open the working environment.

2. Hover over the volume and click **Edit**.

3. From the *Snapshot Policy* tab, move the enable snapshots slider to the right.

4. Define the schedule for snapshots:

    a. Select the frequency: **Hourly**, **Daily**, **Weekly**, or **Monthly**

    b. Select the number of snapshots you want to keep.

    c. Select the day, hour, and minute when the snapshot should be taken.

5. Click **Add volume** or **Update volume** to save your policy settings.

Disable a snapshot policy

You can disable a snapshot policy to stop snapshots from being created for a short period of time while retaining your snapshot policy settings.

Steps

1. Open the working environment.
2. Hover over the volume and click **Edit**.
3. From the *Snapshot Policy* tab, move the enable snapshots slider to the left.

4. Click **Update volume**.

When you want to re-enable the snapshot policy, move the enable snapshots slider to the right and click **Update volume**.

Delete a snapshot

You can delete a snapshot from the Volumes page.

Steps

1. Open the working environment.

2. Hover over the volume and click **Delete a Snapshot copy**.

3. Select the snapshot from the drop-down list and click **Delete**.

Delete a Snapshot Copy - <Volume Name>

This action deletes the selected Snapshot copy.

Snapshot Name

manually.2020-05-04_1722

Delete

4. In the confirmation dialog box, click **Delete**.

Revert a volume from a snapshot

You can revert a volume to an earlier point in time from an existing snapshot.

When you revert a volume, the content of the snapshot overwrites the existing volume configuration. Any changes that were made to the data in the volume after the snapshot was created are lost.

Note that clients do not need to remount the volume after the revert operation.

Steps

1. Open the working environment.

2. Hover over the volume and click **Revert volume to Snapshot**.

3. Select the snapshot that you want to use to restore the existing volume from the drop-down list and click **Revert**.

Reference

Service levels and allocated capacity

The cost for Cloud Volumes Service for AWS is based on the *service level* and the *allocated capacity* that you select. Selecting the appropriate service level and capacity helps you meet your storage needs at the lowest cost.

Considerations

Storage needs include two fundamental aspects:

- The storage *capacity* for holding data
- The storage *bandwidth* for interacting with data

If you consume more storage space than the capacity you selected for the volume, the following considerations apply:

- You will be billed for the additional storage capacity that you consume at the price defined by your service level.
- The amount of storage bandwidth available to the volume does not increase until you increase the allocated capacity size or change the service level.

Service levels

Cloud Volumes Service for AWS supports three service levels. You specify your service level when you create or modify the volume.

The service levels are catered to different storage capacity and storage bandwidth needs:

- **Standard** (capacity)

  If you want capacity at the lowest cost, and your bandwidth needs are limited, then the Standard service level might be most appropriate for you. An example is using the volume as a backup target.

◦ Bandwidth: 16 KB of bandwidth per GB provisioned capacity

- **Premium** (a balance of capacity and performance)

  If your application has a balanced need for storage capacity and bandwidth, then the Premium service level might be most appropriate for you. This level is less expensive per MB/s than the Standard service level, and it is also less expensive per GB of storage capacity than the Extreme service level.

  ◦ Bandwidth: 64 KB of bandwidth per GB provisioned capacity

- **Extreme** (performance)

  The Extreme service level is least expensive in terms of storage bandwidth. If your application demands storage bandwidth without the associated demand for lots of storage capacity, then the Extreme service level might be most appropriate for you.

  ◦ Bandwidth: 128 KB of bandwidth per GB provisioned capacity

Allocated capacity

You specify your allocated capacity for the volume when you create or modify the volume.

While you would select your service level based on your general, high-level business needs, you should select your allocated capacity size based on the specific needs of applications, for example:

- How much storage space the applications need
- How much storage bandwidth per second the applications or the users require

Allocated capacity is specified in GBs. A volume's allocated capacity can be set within the range of 100 GB to 100,000 GB (equivalent to 100 TBs).

Number of inodes

Volumes less than or equal to 1 TB can use up to 20 million inodes. The number of inodes increase by 20 million for each TB you allocate, up to a maximum of 100 million inodes.

- <= 1TB = 20 million inodes
- >1 TB to 2 TB = 40 million inodes
- >2 TB to 3 TB = 60 million inodes
- >3 TB to 4 TB = 80 million inodes
- >4 TB to 100 TB = 100 million inodes

Bandwidth

The combination of both the service level and the allocated capacity you select determines the maximum bandwidth for the volume.

If your applications or users need more bandwidth than your selections, you can change the service level or increase the allocated capacity. The changes do not disrupt data access.

Selecting the service level and the allocated capacity

To select the most appropriate service level and allocated capacity for your needs, you need to know how much capacity and bandwidth you require at the peak or the edge.

List of service levels and allocated capacity

The leftmost column indicates the capacity, and the other columns define the MB/s available at each capacity point based on service level.

See Contract subscription pricing and Metered subscription pricing for complete details on pricing.

Capacity (TB)	Standard (MB/s)	Premium (MB/s)	Extreme (MB/s)
0.1 (100 GB)	1.6	6.4	12.8
1	16	64	128
2	32	128	256
3	48	192	384
4	64	256	512
5	80	320	640
6	96	384	768
7	112	448	896
8	128	512	1,024
9	144	576	1,152
10	160	640	1,280
11	176	704	1,408
12	192	768	1,536
13	208	832	1,664
14	224	896	1,792
15	240	960	1,920
16	256	1,024	2,048
17	272	1,088	2,176
18	288	1,152	2,304
19	304	1,216	2,432
20	320	1,280	2,560
21	336	1,344	2,688
22	352	1,408	2,816
23	368	1,472	2,944
24	384	1,536	3,072
25	400	1,600	3,200
26	416	1,664	3,328
27	432	1,728	3,456
28	448	1,792	3,584

Capacity (TB)	Standard (MB/s)	Premium (MB/s)	Extreme (MB/s)
29	464	1,856	3,712
30	480	1,920	3,840
31	496	1,984	3,968
32	512	2,048	4,096
33	528	2,112	4,224
34	544	2,176	4,352
35	560	2,240	4,480
36	576	2,304	4,500
37	592	2,368	4,500
38	608	2,432	4,500
39	624	2,496	4,500
40	640	2,560	4,500
41	656	2,624	4,500
42	672	2,688	4,500
43	688	2,752	4,500
44	704	2,816	4,500
45	720	2,880	4,500
46	736	2,944	4,500
47	752	3,008	4,500
48	768	3,072	4,500
49	784	3,136	4,500
50	800	3,200	4,500
51	816	3,264	4,500
52	832	3,328	4,500
53	848	3,392	4,500
54	864	3,456	4,500
55	880	3,520	4,500
56	896	3,584	4,500
57	912	3,648	4,500
58	928	3,712	4,500
59	944	3,776	4,500
60	960	3,840	4,500
61	976	3,904	4,500

Capacity (TB)	Standard (MB/s)	Premium (MB/s)	Extreme (MB/s)
62	992	3,968	4,500
63	1,008	4,032	4,500
64	1,024	4,096	4,500
65	1,040	4,160	4,500
66	1,056	4,224	4,500
67	1,072	4,288	4,500
68	1,088	4,352	4,500
69	1,104	4,416	4,500
70	1,120	4,480	4,500
71	1,136	4,500	4,500
72	1,152	4,500	4,500
73	1,168	4,500	4,500
74	1,184	4,500	4,500
75	1,200	4,500	4,500
76	1,216	4,500	4,500
77	1,232	4,500	4,500
78	1,248	4,500	4,500
79	1,264	4,500	4,500
80	1,280	4,500	4,500
81	1,296	4,500	4,500
82	1,312	4,500	4,500
83	1,328	4,500	4,500
84	1,344	4,500	4,500
85	1,360	4,500	4,500
86	1,376	4,500	4,500
87	1,392	4,500	4,500
88	1,408	4,500	4,500
89	1,424	4,500	4,500
90	1,440	4,500	4,500
91	1,456	4,500	4,500
92	1,472	4,500	4,500
93	1,488	4,500	4,500
94	1,504	4,500	4,500

Capacity (TB)	Standard (MB/s)	Premium (MB/s)	Extreme (MB/s)
95	1,520	4,500	4,500
96	1,536	4,500	4,500
97	1,552	4,500	4,500
98	1,568	4,500	4,500
99	1,584	4,500	4,500
100	1,600	4,500	4,500

Example 1

For example, your application requires 25 TB of capacity and 100 MB/s of bandwidth. At 25 TB of capacity, the Standard service level would provide 400 MB/s of bandwidth at a cost of $2,500 (estimate: see current pricing), making Standard the most suitable service level in this case.

Example 2

For example, your application requires 12 TB of capacity and 800 MB/s of peak bandwidth. Although the Extreme service level can meet the demands of the application at the 12 TB mark, it is more cost-effective (estimate: see current pricing) to select 13 TB at the Premium service level.

AWS security group settings for Windows AD servers

If you use Windows Active Directory (AD) servers with cloud volumes, you should familiarize yourself with the guidance on AWS security group settings. The settings enable cloud volumes to integrate with AD correctly.

By default, the AWS security group applied to an EC2 Windows instance does not contain inbound rules for any protocol except RDP. You must add rules to the security groups that are attached to each Windows AD instance to enable inbound communication from Cloud Volumes Service. The required ports are as follows:

Service	Port	Protocol
AD Web Services	9389	TCP
DNS	53	TCP
DNS	53	UDP
ICMPv4	N/A	Echo Reply
Kerberos	464	TCP
Kerberos	464	UDP
Kerberos	88	TCP
Kerberos	88	UDP
LDAP	389	TCP

Service	Port	Protocol
LDAP	389	UDP
LDAP	3268	TCP
NetBIOS name	138	UDP
SAM/LSA	445	TCP
SAM/LSA	445	UDP
Secure LDAP	636	TCP
Secure LDAP	3269	TCP
w32time	123	UDP

If you are deploying and managing your AD installation domain controllers and member servers on an AWS EC2 instance, you will require several security group rules to allow traffic for the Cloud Volumes Service. Below is an example of how to implement these rules for AD applications as part of the AWS CloudFormation template.

```json
{
    "AWSTemplateFormatVersion" : "2010-09-09",
    "Description" : "Security Group for AD",
    "Parameters" :
    {
        "VPC" :
        {
            "Type" : "AWS::EC2::VPC::Id",
            "Description" : "VPC where the Security Group will belong:"
        },
        "Name" :
        {
            "Type" : "String",
            "Description" : "Name Tag of the Security Group:"
        },
        "Description" :
        {
            "Type" : "String",
            "Description" : "Description Tag of the Security Group:",
            "Default" : "Security Group for Active Directory for CVS "
        },
        "CIDRrangeforTCPandUDP" :
        {
            "Type" : "String",
            "Description" : "CIDR Range for the UDP ports
445,138,464,389,53,123 and for the TCP ports
464,339,3389,3268,88,636,9389,445 and 0-65535: *CIDR range format:
10.0.0.0/24"
```

```
                }
        },
        "Resources" :
        {
            "ADSGWest" :
            {
                "Type" : "AWS::EC2::SecurityGroup",
                "Properties" :
                {
                    "GroupDescription" : {"Ref" : "Description"},
                    "VpcId" : { "Ref" : "VPC" },
                    "SecurityGroupIngress" : [
                        {
                            "IpProtocol" : "udp",
                            "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                            "FromPort" : "445",
                            "ToPort" : "445"
                        },
                        {
                            "IpProtocol" : "udp",
                            "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                            "FromPort" : "138",
                            "ToPort" : "138"
                        },
                        {
                            "IpProtocol" : "udp",
                            "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                            "FromPort" : "464",
                            "ToPort" : "464"
                        },
                        {
                            "IpProtocol" : "tcp",
                            "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                            "FromPort" : "464",
                            "ToPort" : "464"
                        },
                        {
                            "IpProtocol" : "udp",
                            "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                            "FromPort" : "389",
                            "ToPort" : "389"
                        },
                        {
                            "IpProtocol" : "udp",
                            "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                            "FromPort" : "53",
```

```
                    "ToPort" : "53"
                },
                {

                    "IpProtocol" : "tcp",
                    "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                    "FromPort" : "339",
                    "ToPort" : "339"
                },
                {

                    "IpProtocol" : "udp",
                    "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                    "FromPort" : "123",
                    "ToPort" : "123"
                },
                {

                    "IpProtocol" : "tcp",
                    "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                    "FromPort" : "3389",
                    "ToPort" : "3389"
                },
                {

                    "IpProtocol" : "tcp",
                    "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                    "FromPort" : "3268",
                    "ToPort" : "3268"
                },
                {

                    "IpProtocol" : "tcp",
                    "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                    "FromPort" : "88",
                    "ToPort" : "88"
                },
                {

                    "IpProtocol" : "tcp",
                    "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                    "FromPort" : "636",
                    "ToPort" : "636"
                },
                {

                    "IpProtocol" : "tcp",
                    "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                    "FromPort" : "3269",
                    "ToPort" : "3269"
                },
                {

                    "IpProtocol" : "tcp",
```

```
                    "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                    "FromPort" : "53",
                    "ToPort" : "53"
            },
            {

                    "IpProtocol" : "tcp",
                    "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                    "FromPort" : "0",
                    "ToPort" : "65535"
            },
            {

                    "IpProtocol" : "tcp",
                    "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                    "FromPort" : "9389",
                    "ToPort" : "9389"
            },
            {

                    "IpProtocol" : "tcp",
                    "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                    "FromPort" : "445",
                    "ToPort" : "445"
            }
        ]
    }
  },
  "Outputs" :
  {
     "SecurityGroupID" :
     {
        "Description" : "Security Group ID",
        "Value" : { "Ref" : "ADSGWest" }
     }
  }
}
```

Cloud Volumes Service for GCP

Learn about Cloud Volumes Service for Google Cloud

NetApp Cloud Volumes Service for Google Cloud enables you to quickly add multi-protocol workloads as well as build and deploy both Windows-based and UNIX-based apps.

Key features:

- Migrate data between on-premises and Google Cloud.

- Provision volumes from 1 to 100 TiB in seconds.

- Multiprotocol support (you can create an NFS or SMB volume).

- Protect data with automated, efficient snapshots.

- Accelerate app development with rapid cloning.

Cost

Volumes created by the Cloud Volumes Service for Google Cloud are charged to your subscription to the service, not through Cloud Manager.

View pricing

There are no charges to discover a Cloud Volumes Service for Google Cloud region or volume from Cloud Manager.

Supported regions

View supported Google Cloud regions.

Before you get started

Cloud Manager can discover existing Cloud Volumes Service for GCP subscriptions and volumes. See the NetApp Cloud Volumes Service for Google Cloud documentation if you haven't set up your subscription yet.

Getting help

Use the Cloud Manager chat for general questions about Cloud Volumes Service operation in Cloud Manager.

For general questions about Cloud Volumes Service for Google Cloud, email NetApp's Google Cloud Team at gcinfo@netapp.com.

For technical issues associated with your cloud volumes, you can create a technical support case from the Google Cloud Console. See obtaining support for details.

Limitations

- Cloud Manager doesn't support data replication between working environments when using Cloud Volumes Service volumes.

- Deleting your Cloud Volumes Service for Google Cloud subscription from Cloud Manager isn't supported. You can do this only through the Google Cloud Console.

Related links

- NetApp Cloud Central: Cloud Volumes Service for Google Cloud

- NetApp Cloud Volumes Service for Google Cloud documentation

Set up Cloud Volumes Service for Google Cloud

Create a Cloud Volumes Service for Google Cloud working environment in Cloud Manager to create and manage volumes and snapshots.

Quick start

Get started quickly by following these steps, or go to the next section for full details.

1   **Enable the Cloud Volumes Service API**

From Google, enable the Cloud Volumes Service for GCP API so that Cloud Manager can manage the subscription and cloud volumes.

2   **Create a GCP service account and download credentials**

From Google, create a GCP service account and role so that Cloud Manager can access your Cloud Volumes Service for GCP account.

3   **Create a Cloud Volumes Service for GCP working environment**

In Cloud Manager, click **Add Working Environment** > **Google Cloud** > **Cloud Volumes Service** and then provide details about the service account and Google Cloud project.

Enable the Cloud Volumes Service API

In Google Cloud Shell, run the following command to enable the Cloud Volumes Service API:

```
gcloud --project=<my-cvs-project> services enable cloudvolumesgcp-api.netapp.com
```

Give Cloud Manager access to the Cloud Volumes Service for GCP account

You must complete the following tasks so that Cloud Manager can access your Google Cloud project:

- Create a new service account
- Add the new service account member to your project and assign it specific roles (permissions)
- Create and download a key pair for the service account that is used to authenticate to Google

Steps

1. In the Google Cloud console, go to the Service accounts page.
2. Click **Select a project**, choose your project, and click **Open**.
3. Click **Create service account**.
4. Enter the service account name (friendly display name) and description.

   The Cloud Console generates a service account ID based on this name. Edit the ID if necessary - you cannot change the ID later.

5. To set access controls now, click **Create** and then **DONE** from the bottom of the page, and continue to the next step.

6. From the *IAM page* click **Add** and fill out the fields in the *Add Members* page:

    a. In the New Members field, enter the full service account ID, for example, user1-service-account-cvs@project1.iam.gserviceaccount.com.

    b. Add these roles:

        ▪ *NetApp Cloud Volumes Admin*

        ▪ *Compute Network Viewer*

    c. Click **Save**.

7. Click the Service Account name, and then from the *Service account details* page, click **Add key > Create new key**.

8. Select **JSON** as the key type and click **Create**.

    By clicking **Create** your new public/private key pair is generated and downloaded to your system. It serves as the only copy of the private key. Store this file securely because it can be used to authenticate as your service account.

For detailed steps, see the Google Cloud topics Creating and managing service accounts, Granting, changing, and revoking access to resources, and Creating and managing service account keys.

Create a Cloud Volumes Service for GCP working environment

Set up a Cloud Volumes Service for GCP working environment in Cloud Manager so you can start creating volumes.

Regardless of whether you have already created volumes from the Google Cloud Console, or if you just signed up for Cloud Volumes Service for GCP and have no volumes yet, the first step is to create a working environment for the volumes based on your GCP subscription.

If cloud volumes already exist for this subscription, then the volumes will appear in the new working environment. If you haven't added any cloud volumes yet for the GCP subscription, then you do that after you create the new working environment.

> If you have subscriptions and volumes in multiple GCP projects, you need to perform this task for each project.

Before you begin

You must have the following information available when adding a subscription for each project:

- Service account credentials (JSON private key you downloaded)
- Project name

Steps

1. In Cloud Manager, add a new Working Environment, select the location **Google Cloud**, and click **Continue**.

2. Select **Cloud Volumes Service** and click **Continue**.
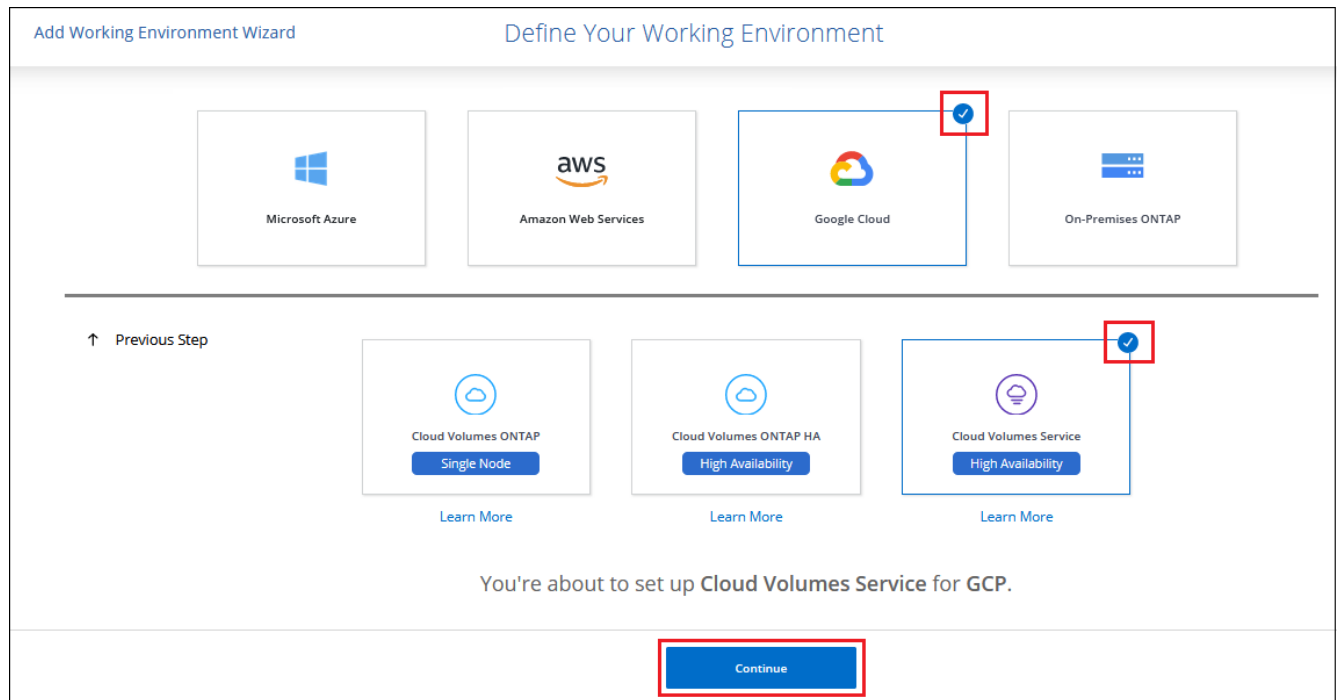
3. Provide information about your Cloud Volumes Service subscription:

   a. Enter the Working Environment Name you want to use.

   b. Copy/paste the JSON private key you downloaded in the previous steps.

   c. Select the name of your Google Cloud project.

   d. Click **Continue**.

Result

Cloud Manager displays your Cloud Volumes Service for Google Cloud working environment.

If cloud volumes already exist for this subscription, then the volumes appear in the new working environment. You can add additional cloud volumes from Cloud Manager.

If no cloud volumes exist for this subscription, create them now.

What's next?

Start creating and managing volumes.

Create and manage volumes for Cloud Volumes Service for Google Cloud

Cloud Manager enables you to create cloud volumes based on your Cloud Volumes Service for Google Cloud subscription. You can also edit certain attributes of a volume, get the relevant mount commands, create snapshot copies, and delete cloud volumes.

Create cloud volumes

You can create NFS or SMB volumes in a new or existing Cloud Volumes Service for Google Cloud account. Cloud volumes currently support NFSv3 and NFSv4.1 for Linux and UNIX clients, and SMB 3.x for Windows clients.

Before you begin

- If you want to use SMB in GCP, you must have set up DNS and Active Directory.

- When planning to create an SMB volume, you must have a Windows Active Directory server available to which you can connect. You will enter this information when creating the volume. Also, make sure that the Admin user is able to create a machine account in the Organizational unit (OU) path specified.

Steps

1. Select the working environment and click **Add New Volume**.

2. In the Details & Location page, enter details about the volume:

   a. Enter a name for the volume.

   b. Specify a size within the range of 1 TiB (1024 GiB) to 100 TiB.

   Learn more about allocated capacity.

   c. Specify a service level: Standard, Premium, or Extreme.

   Learn more about service levels.

   d. Select the Google Cloud region.

   e. Select the VPC Network from which the volume will be accessible. Note that the VPC cannot be changed or edited after the volume is created.

   f. Click **Continue**.

3. In the Protocol page, select NFS or SMB and then define the details. Required entries for NFS and SMB are shown in separate sections below.

4. For NFS:

   a. In the Volume Path field, specify the name of the volume export you will see when you mount the volume.

b. Select NFSv3, NFSv4.1, or both depending on your requirements.

c. Optionally, you can create an export policy to identify the clients that can access the volume. Specify the:

-   Allowed clients by using an IP address or Classless Inter-Domain Routing (CIDR).

-   Access rights as Read & Write or Read Only.

-   Access protocol (or protocols if the volume allows both NFSv3 and NFSv4.1 access) used for users.

-   Click **+ Add Export Policy Rule** if you want to define additional export policy rules.

The following image shows the Volume page filled out for the NFS protocol:

5. For SMB:

a. In the Volume Path field, specify the name of the volume export you will see when you mount the volume and click **Continue**.

b. If Active Directory has been set up, you see the configuration. If it is the first volume being set up and no Active Directory has been set up, you can enable SMB session encryption in the SMB Connectivity Setup page:

Field	Description
DNS Primary IP Address	The IP addresses of the DNS servers that provide name resolution for the SMB server. Use a comma to separate the IP addresses when referencing multiple servers, for example, 172.31.25.223, 172.31.2.74..
Active Directory Domain to join	The FQDN of the Active Directory (AD) domain that you want the SMB server to join.
SMB Server NetBIOS name	A NetBIOS name for the SMB server that will be created.
Credentials authorized to join the domain	The name and password of a Windows account with sufficient privileges to add computers to the specified Organizational Unit (OU) within the AD domain.

Field	Description
Organizational Unit	The organizational unit within the AD domain to associate with the SMB server. The default is CN=Computers for connections to your own Windows Active Directory server.

The following image shows the Volume page filled out for the SMB protocol:

6. Click **Continue**.

7. If you want to create the volume based on a snapshot of an existing volume, select the snapshot from the Snapshot Name drop-down list. Otherwise just click **Continue**.

8. In the Snapshot Policy page, you can enable Cloud Volumes Service to create snapshot copies of your volumes based on a schedule. You can do this now by moving the selector to the right, or you can edit the volume later to define the snapshot policy.

   See Creating a snapshot policy for more information about snapshot functionality.

9. Click **Add Volume**.

The new volume is added to the working environment.

Continue with Mounting the cloud volume.

Mount cloud volumes

Access mounting instructions from within Cloud Manager so you can mount the volume to a host.

Note: Please use the highlighted protocol/dialect supported by your client.

Steps

1. Open the working environment.

2. Hover over the volume and click **Mount the volume**.

   NFS and SMB volumes display mount instructions for that protocol.

3. Hover over the commands and copy them to your clipboard to make this process easier. Just add the destination directory/mount point at the end of the command.

NFS example:

Mount the volume - testk

Setting up your instance

1. Open an SSH client and connect to your instance.

2. Install the nfs client on your instance.

On Red Hat Enterprise Linux or SuSE Linux instance:

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

On an Ubuntu or Debian instance:

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

Mounting your volume

1. Create a new directory on your instance:

```
$ sudo mkdir /dir
```

2. Mount your NFSv3 volume using the command below:

```
sudo mount -t nfs -o rw,hard,rsize=65536,wsize=65536,vers=3,tc...
```

3. Mount your NFSv4.1 volume using the command below:

```
sudo mount -t nfs -o rw,hard,rsize=65536,wsize=65536,vers=4.1,t...
```

The maximum I/O size defined by the `rsize` and `wsize` options is 1048576, however 65536 is the recommended default for most use cases.

Note that Linux clients will default to NFSv4.1 unless the version is specified with the `vers=<nfs_version>` option.

SMB example:

Mount the volume - <Volume Name>

Mapping your network drive

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 this:

   \\test.cv-pm.local\silly-condescending-mcnulty

   To connect every time you log on to your computer, check the **Reconnect at logon** option.

5. Click **Finish**.
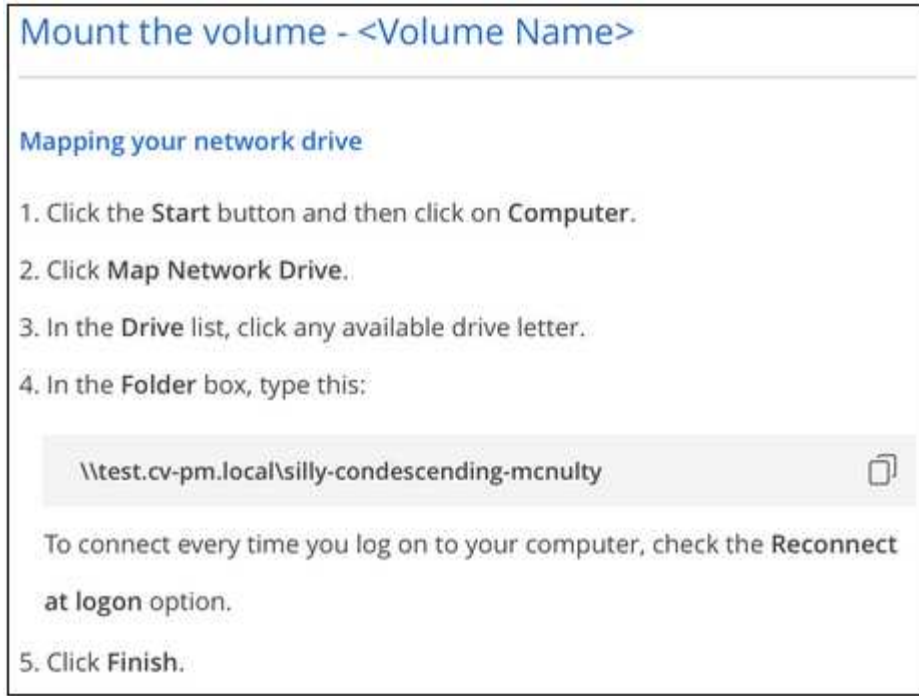
4. Map your network drive by following the mount instructions for your instance.

   After completing the steps in the mount instructions, you have successfully mounted the cloud volume to your GCP instance.

Manage existing volumes

You can manage existing volumes as your storage needs change. You can view, edit, restore, and delete volumes.

Steps

1. Open the working environment.

2. Hover over the volume.

3. Manage your volumes:

Task	Action
View information about a volume	Click **Info**.
Edit a volume (including snapshot policy)	a. Click **Edit**. b. Modify the volume's properties and then click **Update**.
Get the NFS or SMB mount command	a. Click **Mount the volume**. b. Click **Copy** to copy the command(s).
Create a Snapshot copy on demand	a. Click **Create a Snapshot copy**. b. Change the name, if needed, and then click **Create**.
Replace the volume with the contents of a Snapshot copy	a. Click **Revert volume to snapshot**. b. Select a Snapshot copy and click **Restore**.
Delete a Snapshot copy	a. Click **Delete a Snapshot copy**. b. Select the snapshot and click **Delete**. c. Click **Delete** again when prompted to confirm.
Delete a volume	a. Unmount the volume from all clients: ◦ On Linux clients, use the `umount` command. ◦ On Windows clients, click **Disconnect network drive**. b. Select a volume, and then click **Delete**. c. Click **Delete** again to confirm.

Remove Cloud Volumes Service from Cloud Manager

You can remove a Cloud Volumes Service for Google Cloud subscription and all existing volumes from Cloud Manager. The volumes are not deleted, they are just removed from the Cloud Manager interface.

Steps

1. Open the working environment.

2. Click the ⋮ button at the top of the page and click **Remove Cloud Volumes Service**.

3. In the confirmation dialog box, click **Remove**.

Manage Active Directory configuration

If you change your DNS servers or Active Directory domain, you need to modify the SMB server in Cloud Volumes Services so that it can continue to serve storage to clients.

Steps

1. Open the working environment.

2. Click the ⋮ button at the top of the page and click **Manage Active Directory**.
   If no Active Directory is configured, you can add one now. If one is configured, you can modify or delete the settings using the ⋮ button.

3. Specify the settings for the SMB server:

Field	Description
DNS Primary IP Address	The IP addresses of the DNS servers that provide name resolution for the SMB server. Use a comma to separate the IP addresses when referencing multiple servers, for example, 172.31.25.223, 172.31.2.74.
Active Directory Domain to join	The FQDN of the Active Directory (AD) domain that you want the SMB server to join.
SMB Server NetBIOS name	A NetBIOS name for the SMB server that will be created.
Credentials authorized to join the domain	The name and password of a Windows account with sufficient privileges to add computers to the specified Organizational Unit (OU) within the AD domain.
Organizational Unit	The organizational unit within the AD domain to associate with the SMB server. The default is CN=Computers for connections to your own Windows Active Directory server.

4. Click **Save** to save your settings.

Manage cloud volumes snapshots

You can create a snapshot policy for each volume so that you can recover or restore the entire contents of a volume from an earlier time. You can also create an on-demand snapshot of a cloud volume when needed.

Create an on-demand snapshot

You can create an on-demand snapshot of a cloud volume if you want to create a snapshot with the current volume state.

Steps
1. Open the working environment.
2. Hover over the volume and click **Create a snapshot copy**.
3. Enter a name for the snapshot, or use the automatically generated name, and click **Create**.

Create a Snapshot Copy - <Volume Name>

A NetApp Snapshot copy is a read-only, point-in-time image of a volume. The image protects your data with no performance impact and requires minimal storage.

Snapshot Copy Name

manually.2020-05-04_1722

Create

The snapshot is created.

Create or modify a snapshot policy

You can create or modify a snapshot policy as necessary for a cloud volume. You define the snapshot policy from the *Snapshot Policy* tab either when creating a volume or when editing a volume.

Steps

1. Open the working environment.

2. Hover over the volume and click **Edit**.

3. From the *Snapshot Policy* tab, move the enable snapshots slider to the right.

4. Define the schedule for snapshots:

    a. Select the frequency: **Hourly**, **Daily**, **Weekly**, or **Monthly**

    b. Select the number of snapshots you want to keep.

    c. Select the day, hour, and minute when the snapshot should be taken.

5. Click **Add volume** or **Update volume** to save your policy settings.

Disable a snapshot policy

You can disable a snapshot policy to stop snapshots from being created for a short period of time while retaining your snapshot policy settings.

Steps

1. Open the working environment.

2. Hover over the volume and click **Edit**.

3. From the *Snapshot Policy* tab, move the enable snapshots slider to the left.

4. Click **Update volume**.

When you want to re-enable the snapshot policy, move the enable snapshots slider to the right and click **Update volume**.

Delete a snapshot

You can delete a snapshot if it is no longer needed.

Steps

1. Open the working environment.
2. Hover over the volume and click **Delete a Snapshot copy**.
3. Select the snapshot from the drop-down list and click **Delete**.

Delete a Snapshot Copy - <Volume Name>

This action deletes the selected Snapshot copy.

Snapshot Name

manually.2020-05-04_1722

Delete

4. In the confirmation dialog box, click **Delete**.

Restore a snapshot to a new volume

You can restore a snapshot to a new volume as necessary.

Steps

1. Open the working environment.
2. Hover over the volume and click **Restore to a new volume**.
3. Select the snapshot that you want to use to create the new volume from the drop-down list.
4. Enter a name for the new volume and click **Restore**.

Restore to a new volume - <Volume Name>

This operation restores data from a Snapshot copy to a new volume.

Snapshot Name

manually.2020-05-04_1722

Restored Volume Name:

vol_restore

Restore

The volume is created in the working environment.

5. If you need to change any of the volume attributes, such as volume path or service level:

a. Hover over the volume and click **Edit**.

b. Make your changes and click **Update volume**.

After you finish

Continue with Mounting the cloud volume.