Cloud Volumes Service for GCP

Cloud Manager

NetApp
March 09, 2022

Table of Contents

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.

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.

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.

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.

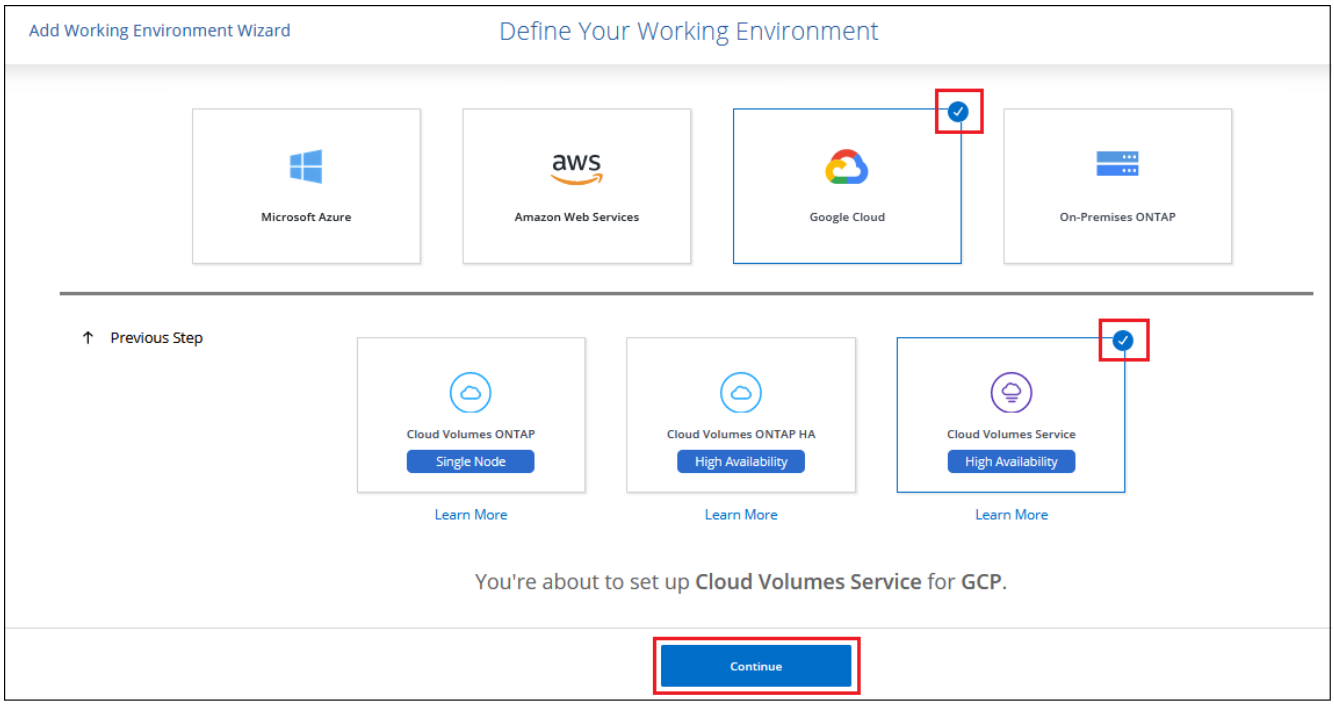
Before you begin

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

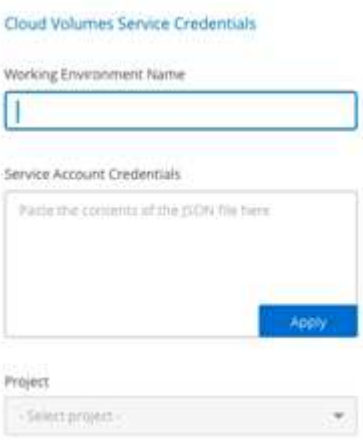
- Service account credentials (JSON private key you downloaded)
- Project name

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.

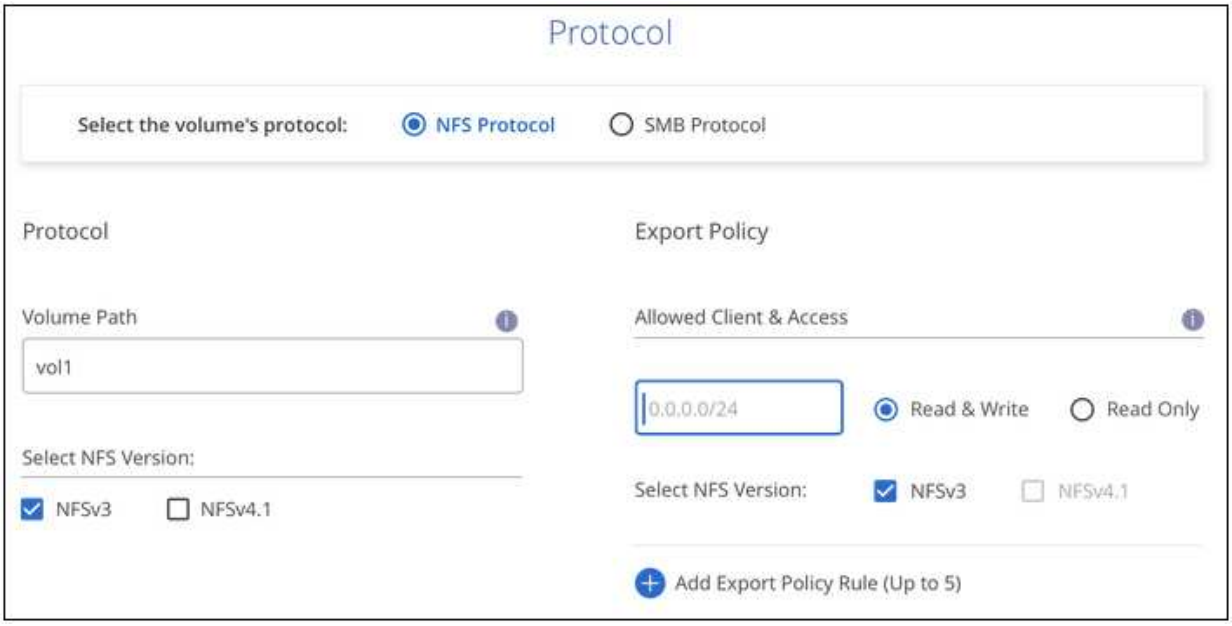
   d. Select the Google Cloud region.
   e. Select the VPC Network from which the volume will be accessible. Note that the VPC cannot be

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.

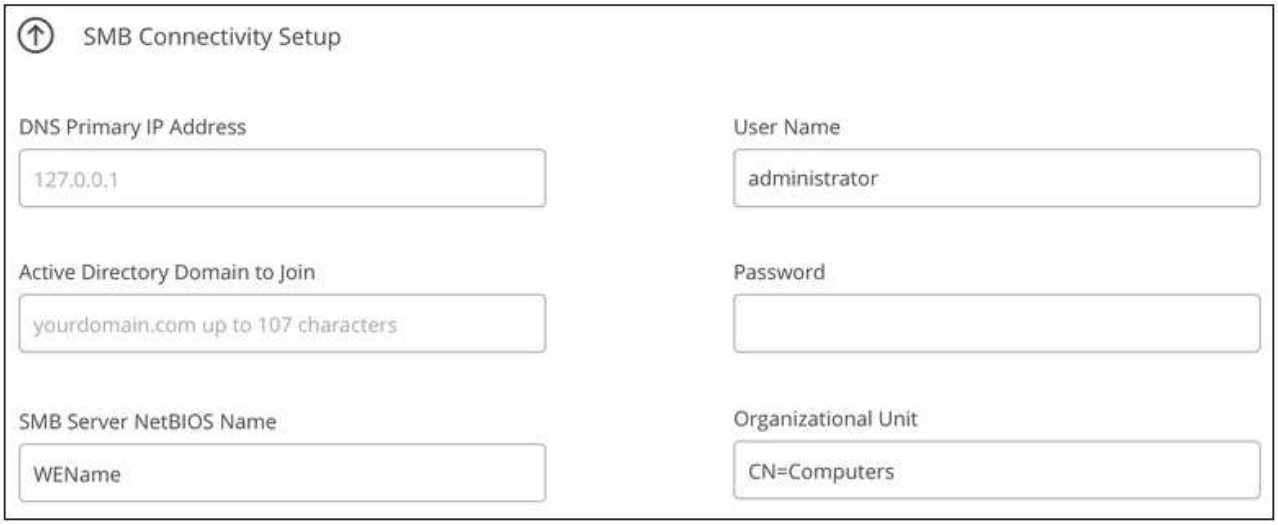
        The following image shows the Volume page filled out for the NFS protocol:



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.
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.

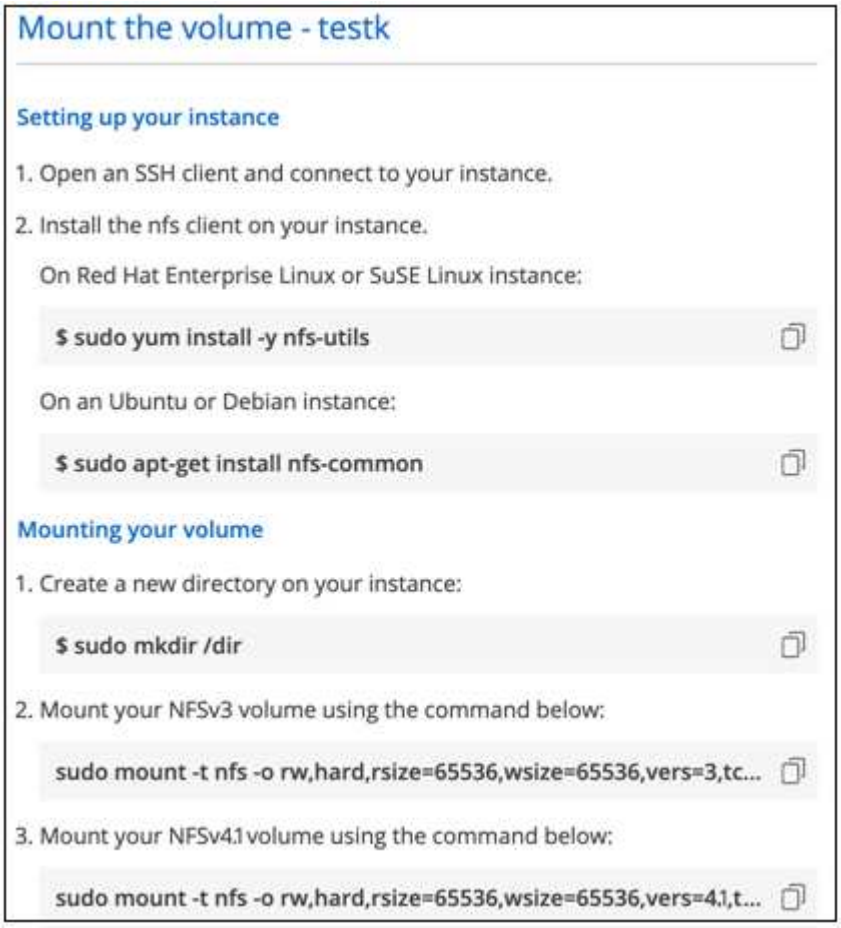
Steps

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.

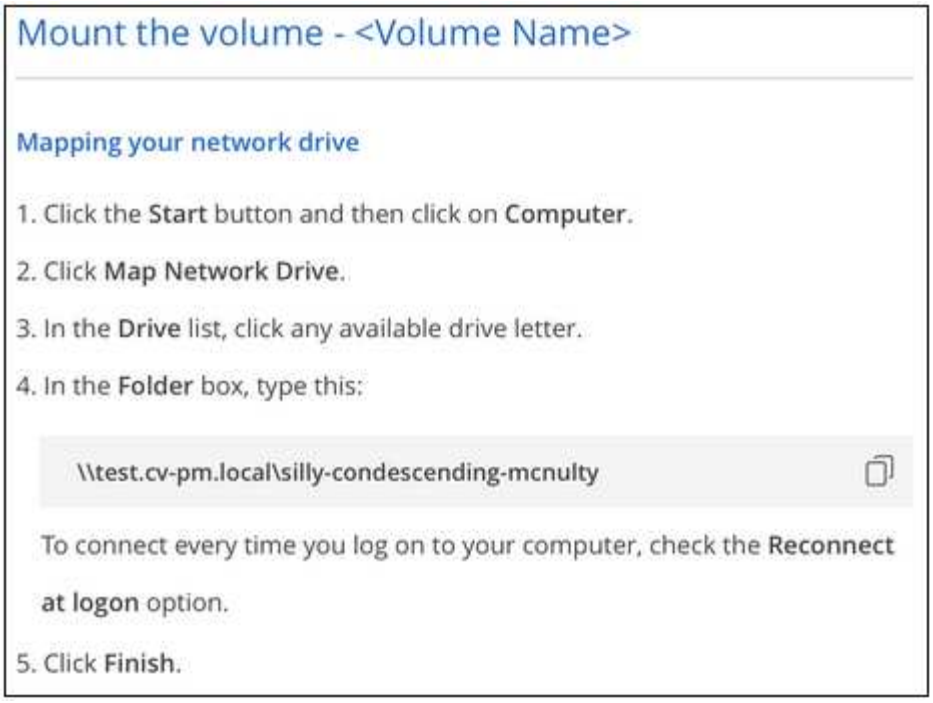
   NFS example:



   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:



4. Map your network drive by following the mount instructions for your instance.

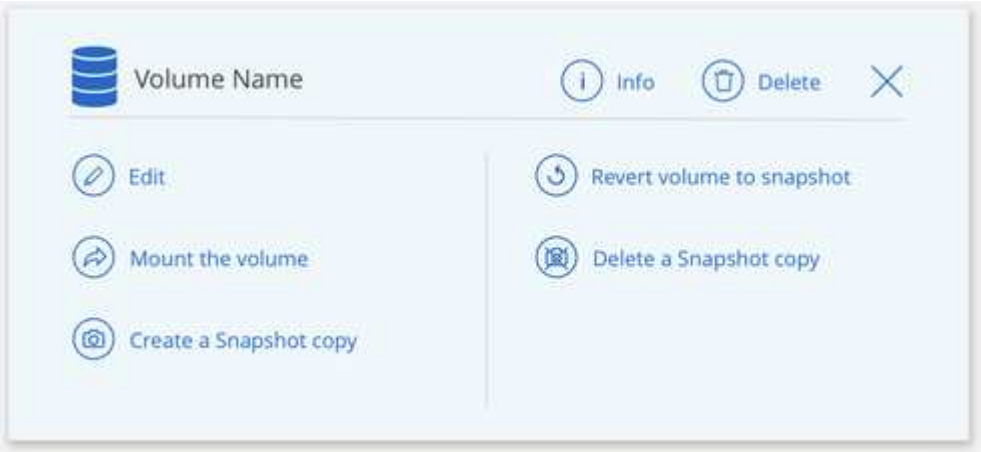
   After completing the steps in the mount instructions, you have successfully mounted the cloud volume to your GCP instance.

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

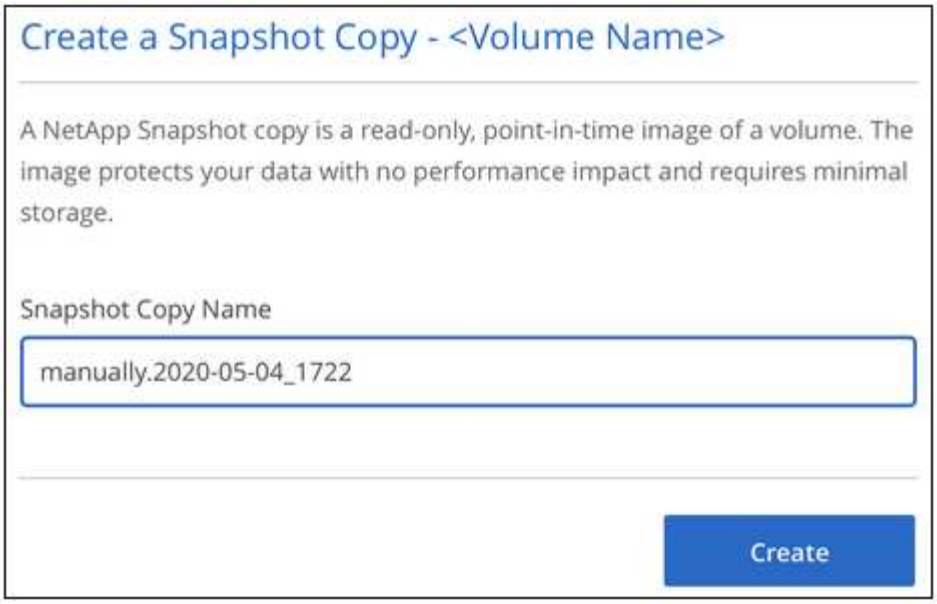
You can create a snapshot policy for each volume so that you can recover or restore the entire contents of a volume from an earlier time. You can also create an on-demand snapshot of a cloud volume when needed.

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**.



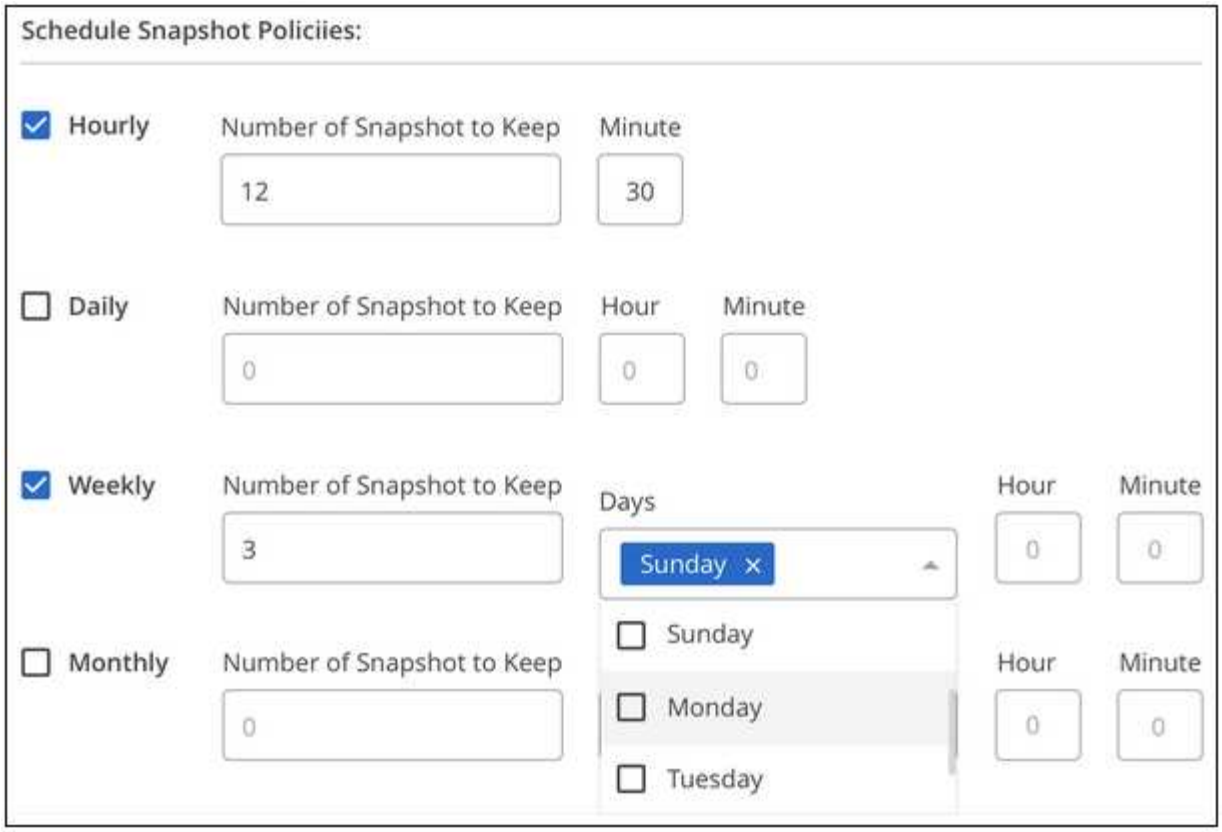
The snapshot is created.

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.



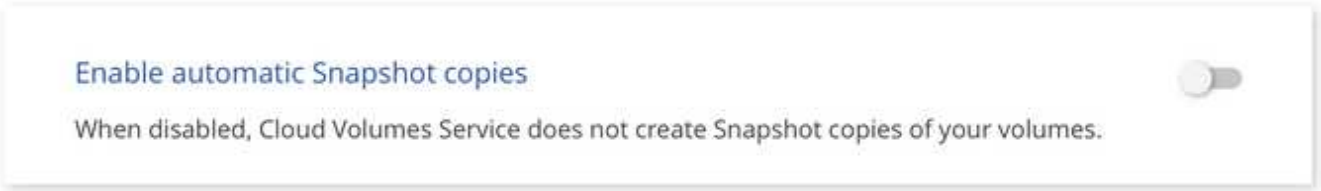
5. Click **Add volume** or **Update volume** to save your policy settings.

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**.

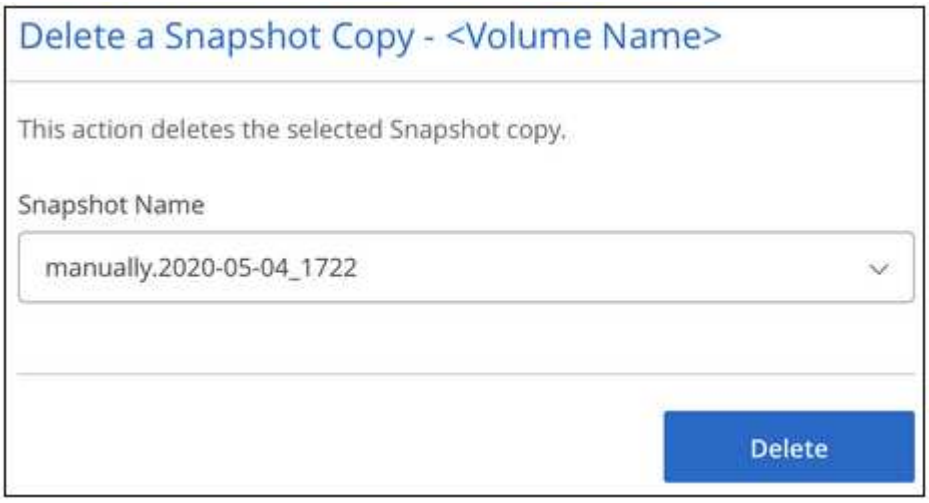
When you want to re-enable the snapshot policy, move the enable snapshots slider to the right and click **Update volume**.

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**.



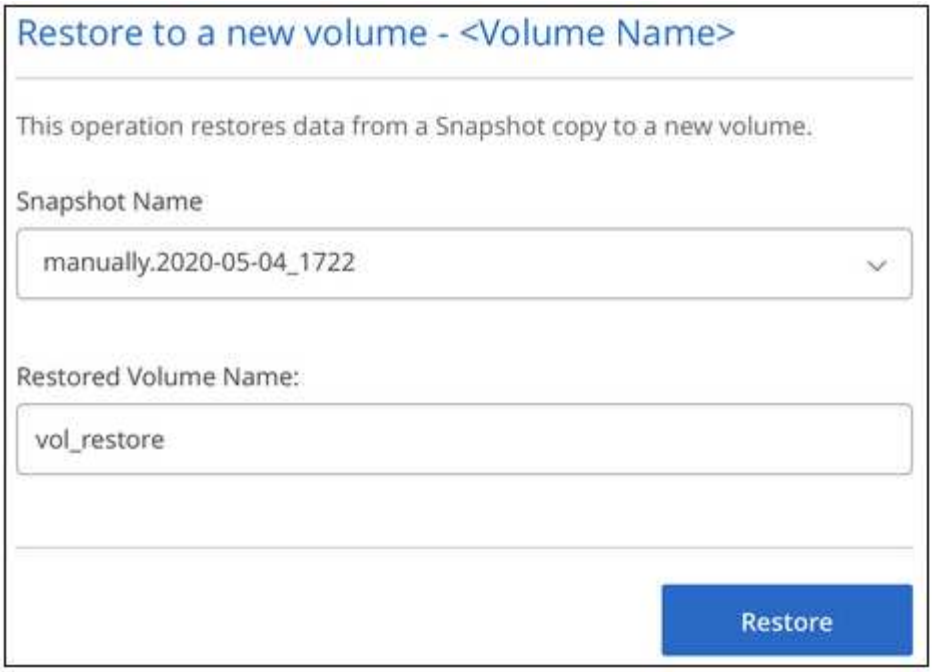
4. In the confirmation dialog box, click **Delete**.

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**.



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.