



Cloud Volumes Service for AWS

Cloud Manager

NetApp

November 10, 2020

This PDF was generated from https://docs.netapp.com/us-en/occm/concept_cvs_aws.html on November 10, 2020.
Always check docs.netapp.com for the latest.

Table of Contents

- Cloud Volumes Service for AWS 1
 - Learn about Cloud Volumes Service for AWS 1
 - Managing Cloud Volumes Service for AWS 3
 - Manage cloud volumes snapshots 15
 - Reference 18

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.

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.

Before you get started

- Cloud Manager can discover existing Cloud Volumes Service for AWS subscriptions and volumes. See the [NetApp Cloud Volumes Service for AWS Account Setup Guide](#) if you haven't set up your subscription yet. You must follow this setup process for each region before you can add the AWS subscriptions and volumes in Cloud Manager.
- You need to obtain the Cloud Volumes API key and secret key so you can provide them to Cloud Manager. [For instructions, refer to Cloud Volumes Service for AWS documentation.](#)

Quick start

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



Verify support for your configuration

You have set up AWS for Cloud Volumes Service and you must have subscribed to one of the [NetApp Cloud Volumes Service offerings on the AWS Marketplace](#).



Add your Cloud Volumes Service for AWS subscription

You must create a working environment for the volumes based on your Cloud Volumes Service for AWS subscription.



Create a cloud volumes

Cloud volumes that already exist for this subscription appear in the new working environment. Otherwise you create new volumes from Cloud Manager.



Mount a cloud volume

Mount new cloud volumes to your AWS instance so that users can begin to use the storage.

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.

Add your Cloud Volumes Service for AWS subscription

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

If cloud volumes already exist for this subscription, then the volumes are automatically added to the new working environment. If you haven't added any cloud volumes yet for the AWS subscription, then you do that after you create the new working environment.



If you have subscriptions and volumes in multiple AWS regions, you need to perform this task for each region.

Before you begin

You must have the following information available when adding a subscription in each region:


- Cloud Volumes API key and Secret key: [See the Cloud Volumes Service for AWS documentation to get this information.](#)
- The AWS region where the subscription was created.

Steps


1. In Cloud Manager, add a new Working Environment, select the location **Amazon Web Services**, and click **Continue**.
2. Select **Cloud Volumes Service** and click **Continue**.

Add Working Environment Wizard


Define Your Working Environment




Microsoft Azure



Amazon Web Services




Google Cloud




On-Premises ONTAP

↑ Previous Step




Cloud Volumes ONTAP
Single Node

[Learn More](#)



Cloud Volumes ONTAP HA
High Availability

[Learn More](#)



Cloud Volumes Service

[Learn More](#)

[Continue](#)

3. Provide information about your Cloud Volumes Service subscription:

- Enter the Working Environment Name you want to use.
- Enter the Cloud Volumes Service API key and secret key.
- Select the AWS region where your cloud volumes reside, or where they will be deployed.
- Click **Add**.

Cloud Volumes Service Credentials

Working Environment Name

AWS Cloud Volume Services volumes

Cloud Volumes Service API Key

ddgdgdexample4vtbntbtbrtb

Cloud Volumes Service Secret Key

.....

AWS Region

us-east-1 | US East (N. Virginia) ▼

Result

Cloud Manager displays your Cloud Volumes Service for AWS configuration on the Working Environments page.



If cloud volumes already exist for this subscription, then the volumes are automatically added to the new working environment, as shown in the screenshot. You can add additional cloud volumes from Cloud Manager.

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

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.

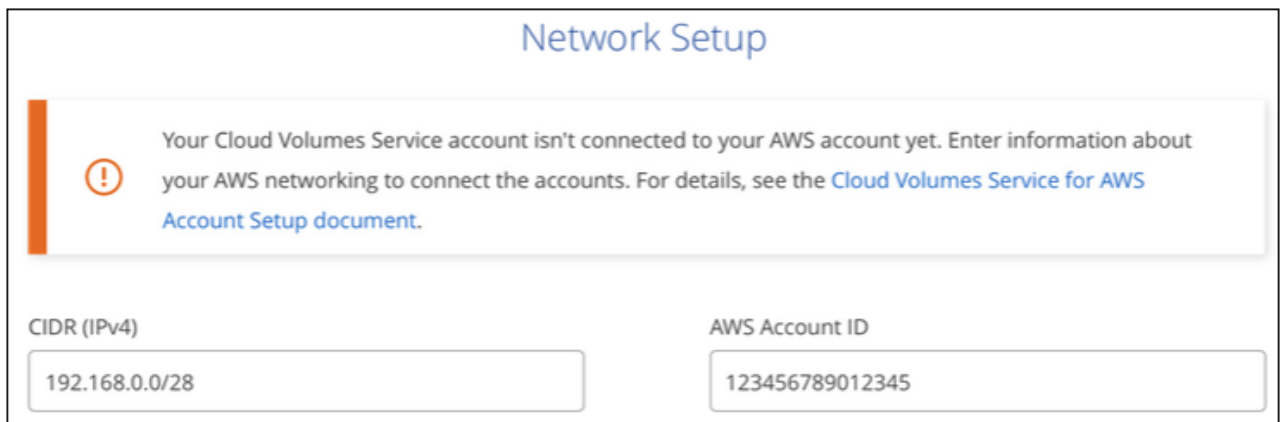
For configurations where no volumes exist, you can create your first volume directly from Cloud Manager after you have set up your Cloud Volumes Service for AWS subscription. In the past, the first volume had to be created directly in the Cloud Volumes Service user interface.

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 the new 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**.



The screenshot shows a 'Network Setup' form. At the top, the title 'Network Setup' is displayed in blue. Below the title is a message box with an orange exclamation mark icon. The message reads: 'Your Cloud Volumes Service account isn't connected to your AWS account yet. Enter information about your AWS networking to connect the accounts. For details, see the [Cloud Volumes Service for AWS Account Setup document](#).' Below the message box are two input fields. The first field is labeled 'CIDR (IPv4)' and contains the text '192.168.0.0/28'. The second field is labeled 'AWS Account ID' and contains the text '123456789012345'.

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:

Protocol

Select the volume's protocol:
 ☒ NFS Protocol
 ☐ SMB Protocol
 ☐ Dual Protocol

Volume Path i

vol1

Select NFS Version:

☒ NFSv3
 ☒ NFSv4.1

Export Policy i

192.168.1.2/24

☒ Read & Write
 ☐ Read Only

Select NFS Version: ☒ NFSv3 ☐ NFSv4.1

192.168.1.22/24

☒ Read & Write
 ☐ Read Only

Select NFS Version: ☐ NFSv3 ☒ NFSv4.1

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.

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. 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:



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:

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,wsiz=65536,vers=3,t...
```

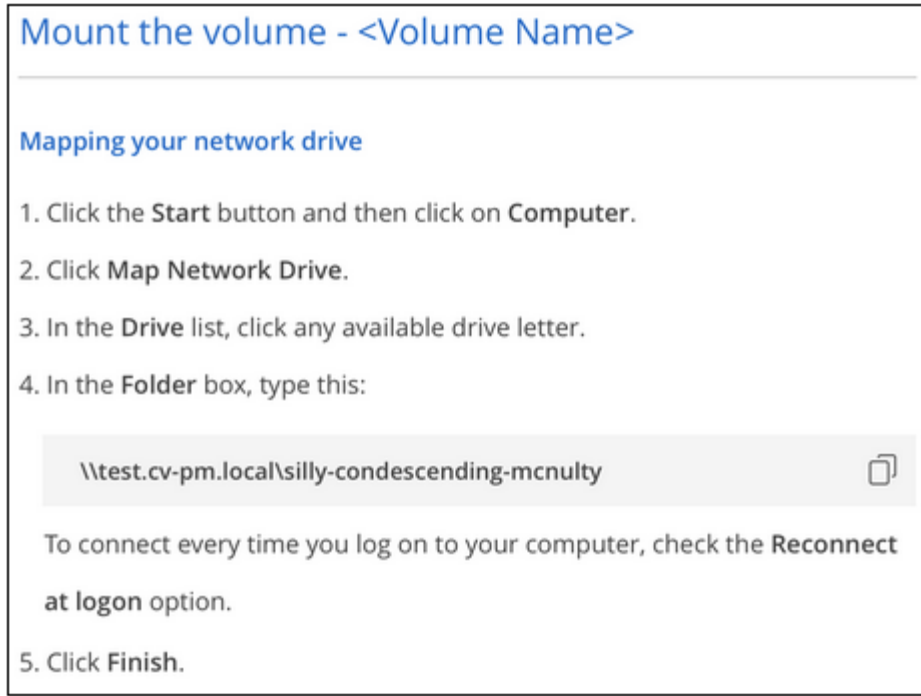
3. Mount your NFSv4.1 volume using the command below:

```
sudo mount -t nfs -o rw,hard,rsize=65536,wsiz=65536,vers=4,1,t...
```

The maximum I/O size defined by the `rsize` and `wsiz` 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. 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.

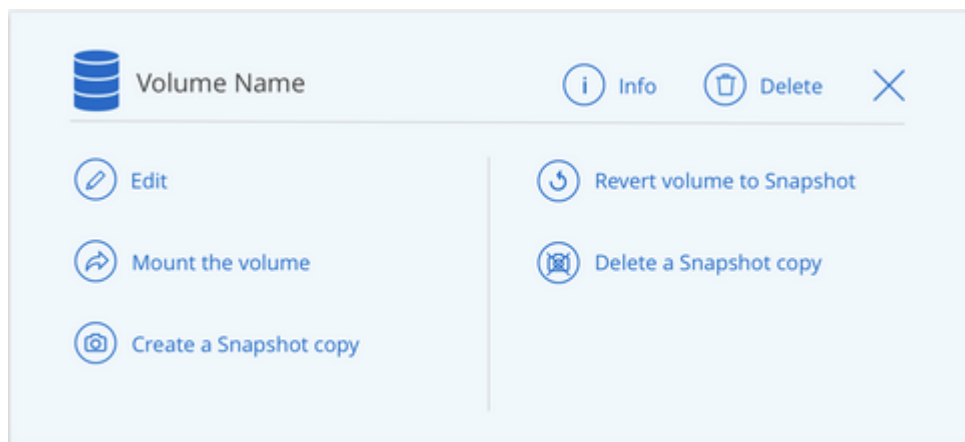
After completing the steps in the mount instructions, you have successfully mounted the cloud volume to your AWS instance.

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:

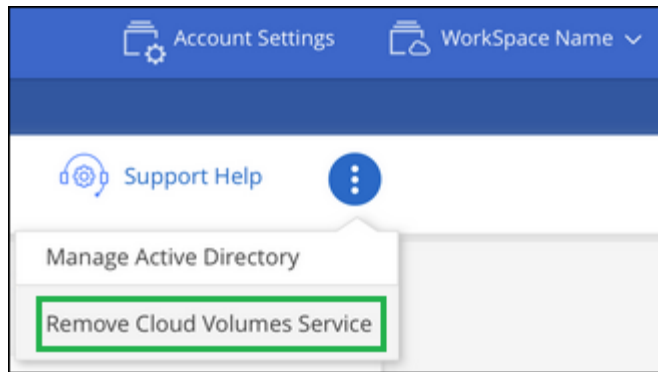
Task	Action
View information about a volume	Select a volume, and then click Info .
Edit a volume (including snapshot policy)	a. Select a volume, and then click Edit . b. Modify the volume's properties and then click Update .
Get the NFS or SMB mount command	a. Select a volume, and then click Mount the 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: <ul style="list-style-type: none">◦ 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.

Field	Description
Organizational Unit	<p>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.</p> <p>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.</p>

- 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

- Open the working environment.
- Hover over the volume and click **Create a snapshot copy**.
- 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

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.

Schedule Snapshot Policies:

<input checked="" type="checkbox"/> Hourly	Number of Snapshot to Keep	Minute	
	<input type="text" value="12"/>	<input type="text" value="30"/>	
<input type="checkbox"/> Daily	Number of Snapshot to Keep	Hour	Minute
	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
<input checked="" type="checkbox"/> Weekly	Number of Snapshot to Keep	Days	Hour
	<input type="text" value="3"/>	<div>Sunday x</div>	<input type="text" value="0"/>
		<input type="checkbox"/> Sunday	<input type="text" value="0"/>
		<input type="checkbox"/> Monday	<input type="text" value="0"/>
		<input type="checkbox"/> Tuesday	<input type="text" value="0"/>
<input type="checkbox"/> Monthly	Number of Snapshot to Keep	Hour	Minute
	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>

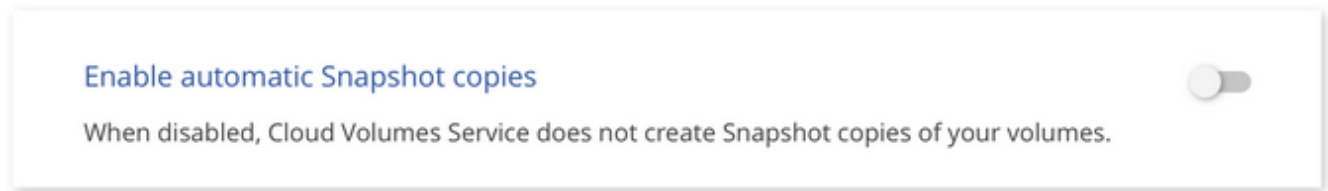
5. Click **Add volume** or **Update volume** to save your policy settings.

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**.

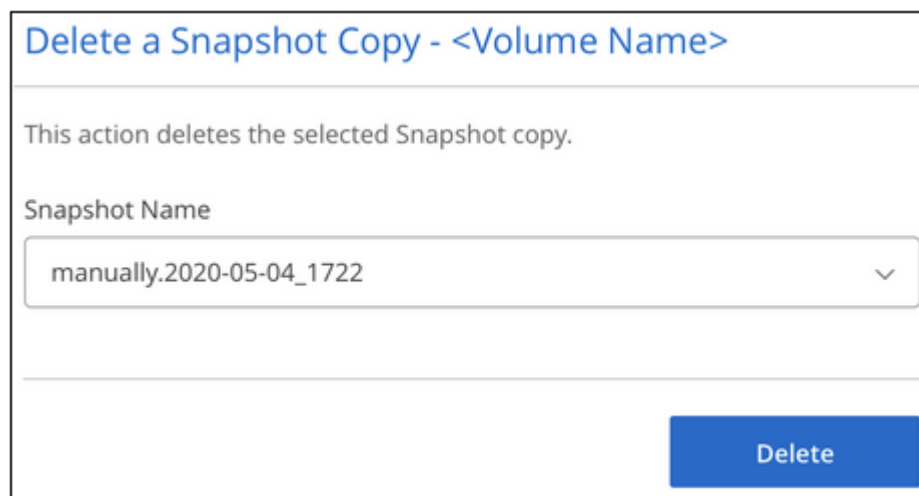
When you want to re-enable the snapshot policy, move the enable snapshots slider to the right and click **Update volume**.

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**.



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

Revert a volume from a snapshot

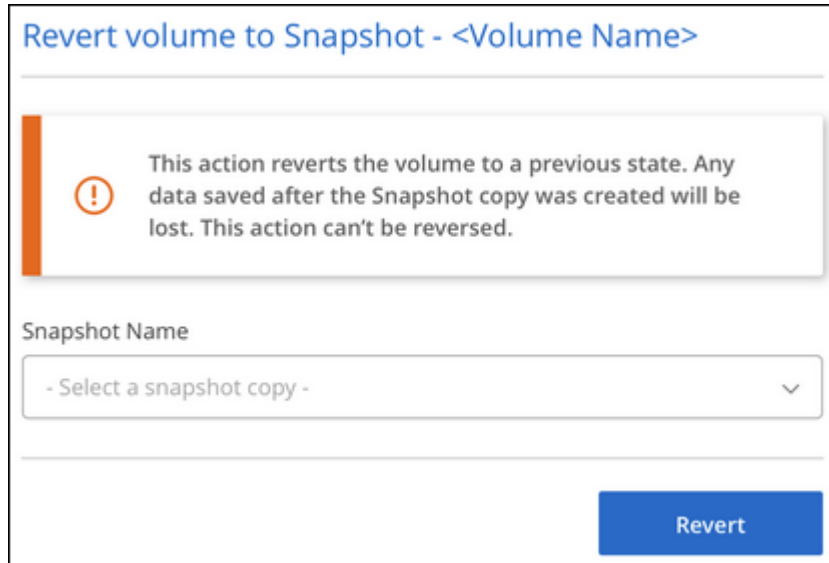
You can revert a volume to an earlier point in time from an existing snapshot.

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**.



Revert volume to Snapshot - <Volume Name>

⚠ This action reverts the volume to a previous state. Any data saved after the Snapshot copy was created will be lost. This action can't be reversed.

Snapshot Name

- Select a snapshot copy -

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

Capacity (TB)	Standard (MB/s)	Premium (MB/s)	Extreme (MB/s)
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
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

Capacity (TB)	Standard (MB/s)	Premium (MB/s)	Extreme (MB/s)
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
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

Capacity (TB)	Standard (MB/s)	Premium (MB/s)	Extreme (MB/s)
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
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
LDAP	389	UDP
LDAP	3268	TCP
NetBIOS name	138	UDP

Service	Port	Protocol
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.

```
{
  "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" }
  }
}
}

```

Copyright Information

Copyright © 2020 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means-graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system-without prior written permission of the copyright owner.

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

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

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

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

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark Information

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