



Managing cloud volumes

Cloud Volumes Service

NetApp

February 12, 2024

This PDF was generated from https://docs.netapp.com/us-en/cloud_volumes/aws/task_creating_cloud_volumes_for_aws.html on February 12, 2024. Always check docs.netapp.com for the latest.

Table of Contents

- Managing cloud volumes 1
 - Creating a cloud volume 1
 - Mounting a cloud volume 7
 - Modifying a cloud volume 8
 - Deleting a cloud volume 8

Managing cloud volumes

Creating a cloud volume

You create cloud volumes from the NetApp Cloud Orchestrator site.

Prerequisites

Your AWS environment must meet certain requirements before you can create your first cloud volume. For each AWS region where you plan to deploy cloud volumes, you must have a:

- Virtual Private Cloud (VPC)
- Virtual Private Gateway (VGW) that is connected to your VPC
- Subnet for the VPC
- Routes defined that include the network on which cloud volumes will run
- Optionally, a Direct Connect Gateway

You must have the following information available when creating your first cloud volume in a region:

- **AWS account ID:** A 12-digit Amazon account identifier with no dashes.
- **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.
- You must have selected the correct region where you want to use the service. See [Selecting the region](#).

If you have not configured the required AWS networking components, see the [NetApp Cloud Volumes Service for AWS Account Setup](#) guide for details.

Note: 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.

Enter volume details

Complete the fields at the top of the Create Volume page to define the volume name, size, service level, and more.

1. After you have logged in to the [NetApp Cloud Orchestrator](#) site with the email address that you provided during your subscription, and you have [selected the region](#), click the **Create new volume** button.

+ Create volume

NFS | SMB | Dual-protocol

Name

Region Required
 us-east-1

Timezone
 Any

Volume path Required

Service level Required
 Standard

Allocated capacity

NFS version
 NFSv3

Security style
 UNIX

Tags

☒ Show snapshot directory (read-only)

2. From the Create Volume page, select **NFS**, **SMB**, or **Dual-protocol** as the protocol for the volume you want to create.
3. In the **Name** field, specify the name you want to use for the volume.
4. In the **Region** field, select the AWS region where you want to create the volume. This region must match the region you configured on AWS.
5. In the **Timezone** field, select your time zone.
6. In the **Volume path** field, specify the path you want to use or accept the automatically generated path.
7. In the **Service level** field, select the level of performance for the volume: **Standard**, **Premium**, or **Extreme**.

See [Selecting the service level](#) for details.

8. In the **Allocated capacity** field, select the capacity required. Note that the number of available inodes is dependent on allocated capacity.

See [Selecting the allocated capacity](#) for details.

9. In the **NFS version** field, select **NFSv3**, **NFSv4.1**, or **Both** depending on your requirements.
10. If you selected Dual-protocol, you can select the security style in the **Security style** field by selecting **NTFS** or **UNIX** from the drop-down menu.

Security styles affect the file permission type used and how permissions can be modified.

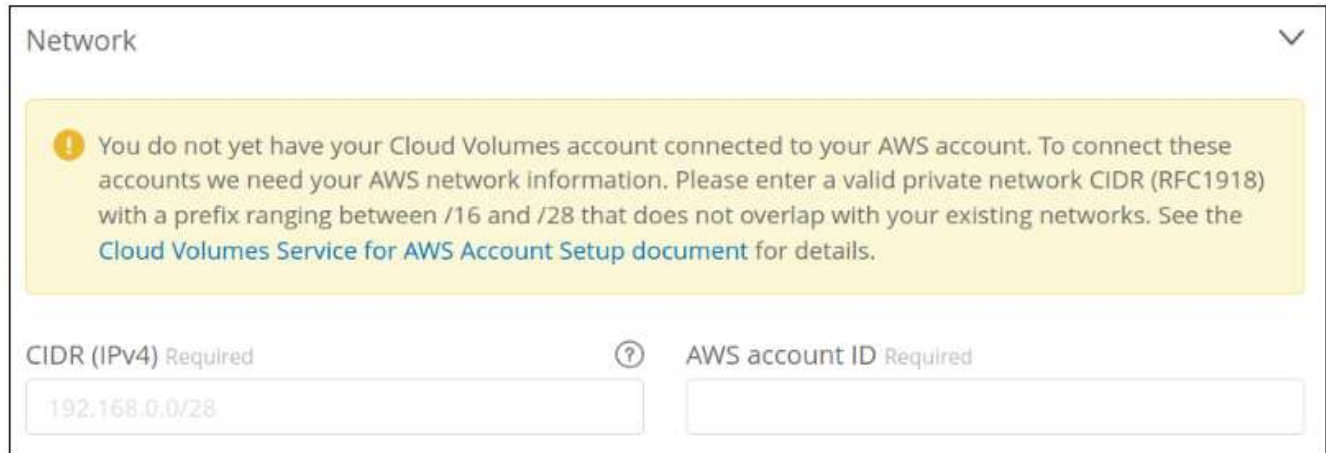
- UNIX uses NFSv3 mode bits, and only NFS clients can modify permissions.
- NTFS uses NTFS ACLs, and only SMB clients can modify permissions.

11. In the **Show snapshot directory** field, keep the default where you can view the Snapshot directory for this volume, or uncheck the box to hide the list of Snapshot copies.

Enter network details (one-time setting per AWS region)

If this is the first time you have created a cloud volume in this AWS region, the **Network** section is displayed so you can connect your Cloud Volumes account to your AWS account:

1. In the **CIDR (IPv4)** field, enter the desired IPv4 range for the region. The network prefix must range between /16 and /28. The network must also fall within the ranges reserved for private networks (RFC 1918). Do not choose a network that overlaps your VPC CIDR allocations.
2. In the **AWS account ID** field, enter your 12-digit Amazon account identifier with no dashes.



The screenshot shows the 'Network' section of the AWS console. It features a yellow warning box at the top stating: 'You do not yet have your Cloud Volumes account connected to your AWS account. To connect these accounts we need your AWS network information. Please enter a valid private network CIDR (RFC1918) with a prefix ranging between /16 and /28 that does not overlap with your existing networks. See the [Cloud Volumes Service for AWS Account Setup document](#) for details.' Below the warning box are two input fields. The first is labeled 'CIDR (IPv4) Required' and contains the text '192.168.0.0/28'. The second is labeled 'AWS account ID Required' and is empty. Both labels have a question mark icon to their right.

Enter export policy rules (optional)

If you selected NFS or Dual-protocol, you can create an export policy in the **Export policy** section to identify the clients that can access the volume:

1. In the **Allowed clients** field, specify the allowed clients by using an IP address or Classless Inter-Domain Routing (CIDR).
2. In the **Access** field, select **Read & Write** or **Read only**.
3. In the **Protocols** field, select the protocol (or protocols if the volume allows both NFSv3 and NFSv4.1 access) used for user access.



The screenshot shows the 'Export policy' section of the AWS console. At the top is a button labeled '+ Add export policy rule'. Below this is a table with four columns: 'Rule index', 'Allowed clients Required', 'Access', and 'Protocol/s'. The first row shows 'Rule-1' in the first column, '0.0.0.0/0' in the second, 'Read & Write' (selected) and 'Read only' in the third, and 'NFSv3' (selected) and 'NFSv4.1' in the fourth. Below the table is a blue information box with a question mark icon and the text: '“Allowed clients” will accept a comma separated list of IPs (v4) and/or cidrs. In most cases this is the private IP of your instance/VM. If using public IPs please be aware that they have to be reachable from the volume’s network for the export policy to work correctly.'

Click **+ Add export policy rule** if you want to define additional export policy rules.

Enable data encryption (optional)

1. If you selected SMB or Dual-protocol, you can enable SMB session encryption by checking the box for the **Enable SMB3 Protocol Encryption** field.

Note: Do not enable encryption if SMB 2.1 clients need to mount the volume.

Integrate the volume with an Active Directory server (SMB and Dual Protocol)

If you selected SMB or Dual-protocol, you can choose to integrate the volume with a Windows Active Directory server or an AWS Managed Microsoft AD in the **Active Directory** section.

In the **Available settings** field, select an existing Active Directory server or add a new AD server.

To configure a connection to a new AD server:

1. In the **DNS server** field, enter the IP address(es) of the DNS server(s). Use a comma to separate the IP addresses when referencing multiple servers, for example, 172.31.25.223, 172.31.2.74.
2. In the **Domain** field, enter the domain for the SMB share.

When using AWS Managed Microsoft AD, use the value from the "Directory DNS name" field.

3. In the **SMB Server NetBIOS** field, enter a NetBIOS name for the SMB server that will be created.
4. In the **Organizational unit** field, enter "CN=Computers" for connections to your own Windows Active Directory server.

When using AWS Managed Microsoft AD, the Organizational unit must be entered in the format "OU=<NetBIOS_name>". For example, **OU=AWSmanagedAD**.

To use a nested OU you must call out the lowest level OU first up to the highest level OU. For example: **OU=THIRDDLEVEL,OU=SECONDDLEVEL,OU=FIRSTLEVEL**.

5. In the **Username** field, enter a username for your Active Directory server.


You can use any username that is authorized to create machine accounts in the Active Directory domain to which you are joining the SMB server.

6. In the **Password** field, enter the password for the AD username that you specified.

☐ Enable SMB3 Protocol Encryption ?

Active directory

Available settings

 \\cloudvol.NGS-AWS.local

DNS server Required

Domain Required

NetBIOS Required ?

Organizational unit ?

Username Required

Password Required

See [Designing a site topology for Active Directory Domain Services](#) for guidelines about designing an optimal Microsoft AD implementation.

See the [AWS Directory service setup with NetApp Cloud Volumes Service for AWS](#) guide for detailed instructions for using AWS Managed Microsoft AD.



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.

Note: UNIX users mounting the volume using NFS will be authenticated as Windows user "root" for UNIX root and "pcuser" for all other users. Make sure that these user accounts exist in your Active Directory prior to mounting a dual protocol volume when using NFS.

Create a Snapshot policy (optional)

If you want to create a snapshot policy for this volume, enter the details in the **Snapshot policy** section:

1. Select the snapshot frequency: **Hourly**, **Daily**, **Weekly**, or **Monthly**.
2. Select the number of snapshots to keep.
3. Select the time when the snapshot should be taken.

Snapshot policy

☐ Hourly
 ☒ Daily
 ☐ Weekly
 ☐ Monthly

Snapshots to keep:
 Hour:
 Minute:

Explanation: Will take a snapshot every day at 1:05 AM and keep 7 of the most recent snapshots.

You can create additional snapshot policies by repeating the steps above, or by selecting the Snapshots tab from the left navigation area.

Create the volume

1. Scroll down to the bottom of the page and click **Create Volume**.

If you have previously created a cloud volume in this region, the new volume appears in the Volumes page.

If this is the first cloud volume you have created in this AWS region and you have entered the networking information in the Network section of this page, a Progress dialog is displayed that identifies the next steps you must follow to connect the volume with AWS interfaces.

Network and volume creation in progress...

Accepting virtual interfaces

1. Open the [AWS DirectConnect Management console](#).
2. Accept the virtual interfaces **NetApp-CloudVolumes-1A** and **NetApp-CloudVolumes-2B**; they should appear momentarily.
3. When accepting the virtual interfaces, make sure to attach them to the VirtualGateway/DirectConnect gateway with the ASN number you provided (64512).
4. Cloud Volumes will then attempt to establish a BGP session with your provided network configuration; this can take up to 10 minutes.
5. On successful completion, your new volume will be created.

2. Accept the virtual interfaces as described in section 6.4 of the [NetApp Cloud Volumes Service for AWS Account Setup](#) guide. You must perform this task within 10 minutes or the system may time out.

If the interfaces do not appear within 10 minutes there may be a configuration issue; in which case you should contact support.

After the interfaces and other networking components are created, the volume you created appears in the Volumes page and the Actions field is listed as Available.

<input type="checkbox"/>	Name ↓	Export path/s	Region	Allocated capacity	Created	Actions
<input type="checkbox"/>	Cloud_Volume_013	NFS: 172.16.80.36/jolly-nostalgic-walsh ⓘ ⓘ	us-east	1 TB	2018-07-20 20:01:16	Available ▾

After you finish

Continue with [Mounting a cloud volume](#).

Mounting a 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 2.1, 3.0, and 3.1.1 for Windows clients.

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

Steps

1. Obtain mount instructions for the volume you created by clicking the blue question mark (?) at the end of the Export Paths field next to the volume name.

When you hover over the question mark, it displays **Show mount instructions**.



2. Click the question mark to display the mount instructions.

NFS example:

Mount instructions ×

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 CentOS 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, such as "g":

```
sudo mkdir g
```
2. Mount your NFSv3 volume using the example command below:

```
sudo mount -t nfs -o rw,hard,rsz=65536,wsz=65536,vers=3,tcp 172.25.0.4:/tender-modest-hofstadter g
```

Note. Please use mount options appropriate for your specific workloads when known.

The maximum I/O size defined by the `rsz` and `wsz` 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.

SMB example:



3. 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.

Modifying a cloud volume

You can modify existing volumes, including changing the volume name, allocated capacity, or service level.

Steps

1. Log in to [NetApp Cloud Orchestrator](#).
2. Click the name of the volume that you want to manage.
3. Modify the following volume fields as applicable:
 - Name
 - Tags
 - Allocated capacity
 - Service level

Changing the service level is not disruptive and does not affect client data access.

Note that the number of available inodes is dependent on allocated capacity.

See [Selecting the appropriate service level and allocated capacity](#) for details.

Deleting a cloud volume

You can delete a cloud volume that is no longer needed.

Steps

1. Unmount the volume from all clients:
 - On Linux clients, use the `umount` command.
 - On Windows clients, click **Disconnect network drive**.
2. From the Volumes page, specify the volumes that you want to delete by selecting the corresponding checkboxes, click **Actions**, and then select **Delete volume/s** from the drop-down list.
3. In the confirmation dialog box, type `delete` to confirm that you want to delete the volume, and then click **Delete**.

Copyright information

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

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

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

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

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

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

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

Trademark information

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