Cloud Volumes Service for AWS docs

Cloud Volumes Service

NetApp
October 26, 2021

This PDF was generated from https://docs.netapp.com/us-en/cloud_volumes/index.html on October 26, 2021. Always check docs.netapp.com for the latest.

Table of Contents

NetApp Cloud Volumes Service for AWS documentation

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

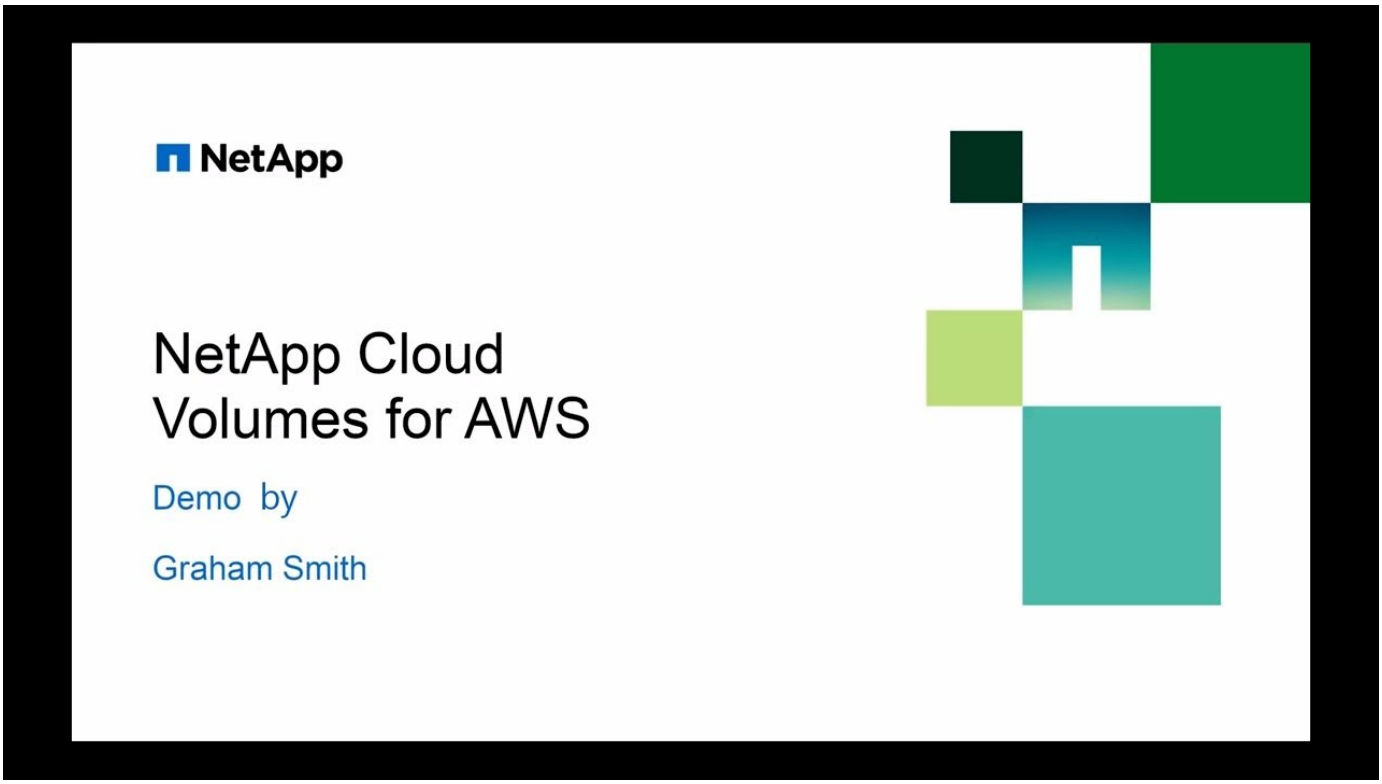
Cloud Volumes Service for AWS provides the following benefits:

- Consistent high performance
- Data protection without performance impacts
- Instant cloning to support operations, development, and test workflows
- Support for NFSv3 and NFSv4.1, SMB 2.1, 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
- Fully managed service, therefore no need to configure or manage storage devices
- Choice of bundled and pay-as-you-go pricing

Perform top tasks

- Selecting the region
- Creating a cloud volume
- Mounting a cloud volume
- Creating an on-demand snapshot for a cloud volume

Learn about Cloud Volumes Service for AWS



Find more information

- NetApp Cloud Central
- Get a first look at the new NetApp Cloud Volumes Service for AWS

Release notes

What's new in Cloud Volumes Service for AWS

NetApp periodically updates Cloud Volumes Service for AWS to bring you new features and enhancements.

February 2021

- A new Cloud Volumes API (`PerformanceMetrics`) is now available to retrieve performance statistics including IOPS, Bandwidth, and Latency. To learn more, see Cloud Volumes APIs.

July 2020

- The Cloud Volumes Service now supports wider RFC 1918 private network ranges between /16 and /28. Previously only /28 ranges where supported.
- The 'Sync' feature now integrates directly with the Cloud Sync UI to provide increased functionality.
- Volumes can be converted to and from NSFv3, NFSv4.1, and both NFSv3 and NFSv4.1 via API calls.
- The API examples and sample Python scripts have been updated to the v2 API. See Cloud Volumes APIs.
- ACLs are now enabled for NFSv4.1 volumes.
- The Cloud Volumes Service is now certified with SOC 2 type 1.
- The Cloud Volumes Service is now available in Singapore (ap-southeast-1).

March 2020

- Cloud Volumes Service now supports a maximum I/O size of 1 MiB for NFSv3 and NFSv4.1 mounts. Previously the maximum I/O size was 64 KiB. Increasing the I/O size may improve performance for some workloads.
  To increase the I/O size, use the mount options "rsize" and/or "wsize", for example:
  `mount -o nfsvers=4.1,rsize=1048576,wsize=1048576 172.25.0.4:/vol1 /mnt/cv`

February 2020

- Cloud Volumes Service is now available as a Metered (pay as you go) subscription in the AWS Marketplace. See the Marketplace listing for more details at: https://aws.amazon.com/marketplace/pp/B0848MXK74
  Note that the original monthly and annual subscription plans are still available.

January 2020

- Cloud Volumes Service now supports SMB multichannel which uses multiple network connections simultaneously to provide increased performance. Multichannel is enabled by default on Windows clients, but requires that the EC2 instance uses a network adapter that support RSS (Receive Side Scaling).
- Reverting a volume from a snapshot is now available from the Cloud Volumes Service user interface. This enables you to revert volumes to a point in time snapshot without requiring clients to remount. See Reverting a volume from a snapshot for details.

Known Issues and limitations

The following known issues and limitations exist in Cloud Volumes Service for AWS.

- **Issue**: If an existing volume only supports NFSv3, and a volume is created or converted with NFSv4.1 or both NFSv3 and NFSv4.1 support, then the existing volume may not be mountable without specifying the NFS version (vers=3).

  Workaround: Either add the option to specify the NFS version to the mount command, for example, `mount -o vers=3 …` or ensure all volumes are converted to support NFSv4.1. Note that Linux clients will default to NFSv4.1 unless the version is specified.

- **Issue**: Creating a new volume from a snapshot may fail with the message 'Unable to set volume attribute "files" for volume *<volume>* … Reason: New count must be larger than current allocated count of *<number>*'.

  Workaround: This issue occurs when trying to create a volume from a snapshot that currently has more files allocated to it than the new volume would be assigned for its allocated capacity. You must increase the allocated capacity for the new volume to assign enough files (inodes). See Selecting the allocated capacity for details.

- **Issue**: The network virtual interfaces will be deleted automatically in CVS regions that have no volumes after 72 hours. When creating a new volume, you will need to re-provide the AWS account # and CIDR.

  Workaround: To avoid the network virtual interfaces from being deleted during periods of inactivity, leave at least one volume and lower the allocation and service level to minimize cost.

- **Issue**: Users with expired subscriptions cannot log in to the Cloud Volumes Service user interface or interact with the API.

  Workaround: Go to the AWS Marketplace page for the Cloud Volumes Service and renew your subscription.

Getting started

Cloud Volumes Service for AWS prerequisites

Cloud volumes are simple to use and fast to deploy. Some prerequisites apply for using Cloud Volumes Service for AWS.

You must have subscribed to Cloud Volumes Service for AWS before you can perform the Cloud Volumes tasks that are described in this documentation. The subscription process includes the initial setup and configuration that are required for using the service.

See the Get a first look at the new NetApp Cloud Volumes Service for AWS page for more information.

Quick start instructions

You can get started with the Cloud Volumes Service for AWS by completing a few quick steps.

Note: You must have configured the required AWS networking components prior to creating a cloud volume. See the *NetApp Cloud Volumes Service for AWS Account Setup Guide* [EN]|[JA] if you have not yet completed these steps.

Select the region

Specify the AWS region where you plan to create cloud volumes.

Create the cloud volume

Create the cloud volume in the AWS cloud by specifying the size and service level, and define other options.

Mount the cloud volume

Mount the cloud volume to your AWS instance using NFS for Linux and UNIX clients, or SMB for Windows clients.

Activating support entitlement and accessing support

Once you have access to Cloud Volumes Service shortly after subscribing in AWS marketplace, it is strongly recommended that you activate support entitlement. Activating support entitlement enables you to access technical support over online chat, web ticketing system, and phone.

The default support level is self-service until serial number activation and registration is completed.

Activating support entitlement

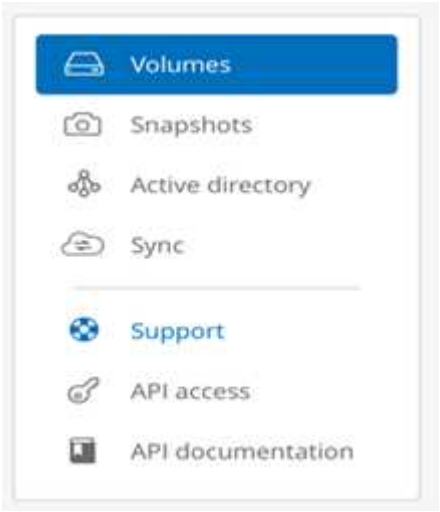
During the initial subscription process with Cloud Volumes Service for AWS, your cloud volumes instance generates a 20-digit NetApp serial number that starts with "930". The NetApp serial number represents the Cloud Volumes Service subscription associated to your AWS account. You must register the NetApp serial number to activate support entitlement. We offer 2 options for support registration:

1. Current NetApp customer with existing NetApp Support Site (NSS) SSO account
2. New NetApp customer with no existing NetApp Support Site (NSS) SSO account

Option 1: Current NetApp customer with existing NetApp Support Site (NSS) SSO account

Steps

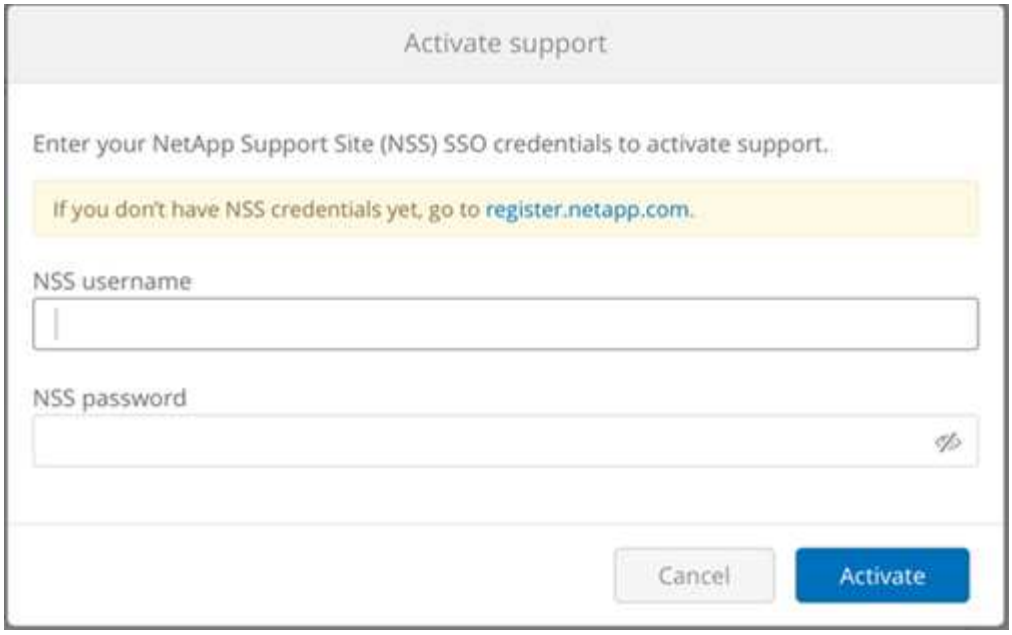
1. Navigate to the Cloud Volumes Service URL, or access this service through the NetApp Cloud Central portal. Then login with your NetApp Cloud Central credentials.
2. Display your NetApp serial number by selecting **Support** in the Cloud Volumes Service user interface (UI).



3. In the **Support** page, verify that your Support status shows `Not registered`.

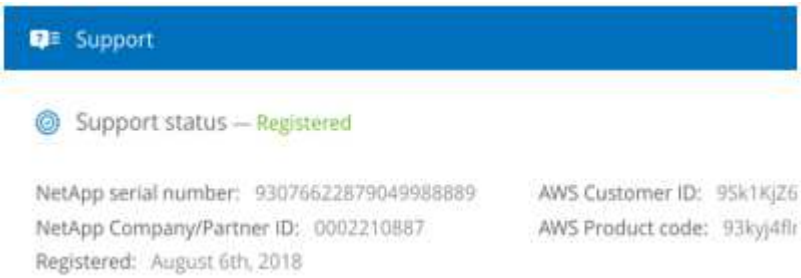
   If you do not see the Support status and your NetApp serial number, refresh the browser page.

4. Click **Activate support** to register your NetApp serial number:
   - If you have an NSS account, enter your NSS credentials (username and password) in the **Activate support** page and click **Activate** to activate support entitlement for your NetApp serial number.



- If you are an existing NetApp customer, but you do not have NSS SSO credentials, go to the NetApp Support Registration site to create your account first. Then return here to register with your NSS credentials.
- If you are a new NetApp customer, see the instructions for Option 2 below.

After your NetApp serial number is activated, the **Support** page shows the status `Registered`, indicating that you have activated support entitlement.

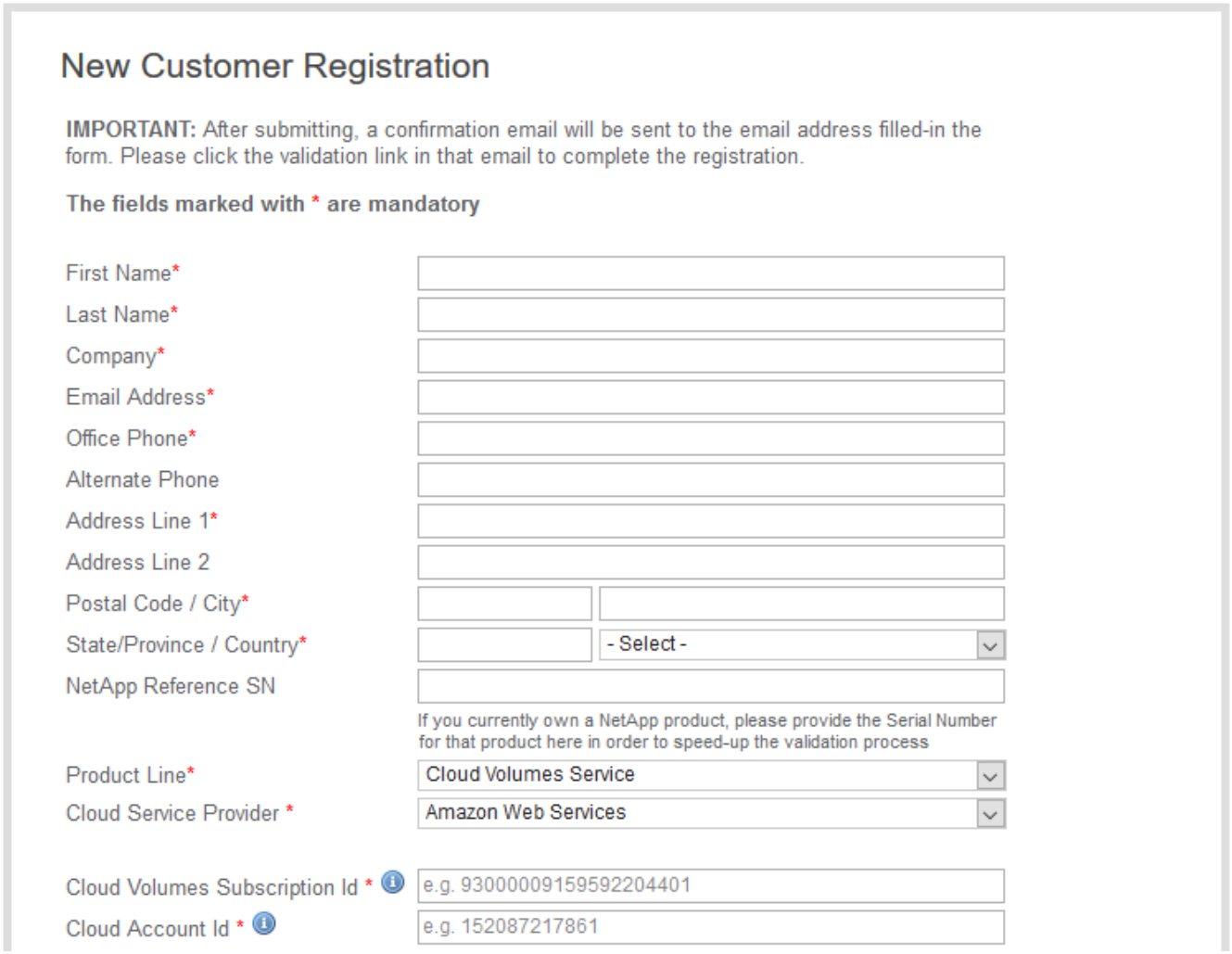


This is a one-time support registration for the applicable Cloud Volumes Service serial number. Any new Cloud Volumes Service subscription and subsequent new serial number requires support activation as well. If you have any questions or problems with support registration, contact us at cvs-support@netapp.com.

Option 2: New NetApp customer with no existing NetApp Support Site (NSS) SSO account

Steps

1. Navigate to the Cloud Data Services Support Registration page to create an NSS account.
2. Select **I am not a registered NetApp Customer** and the New Customer Registration form is displayed.



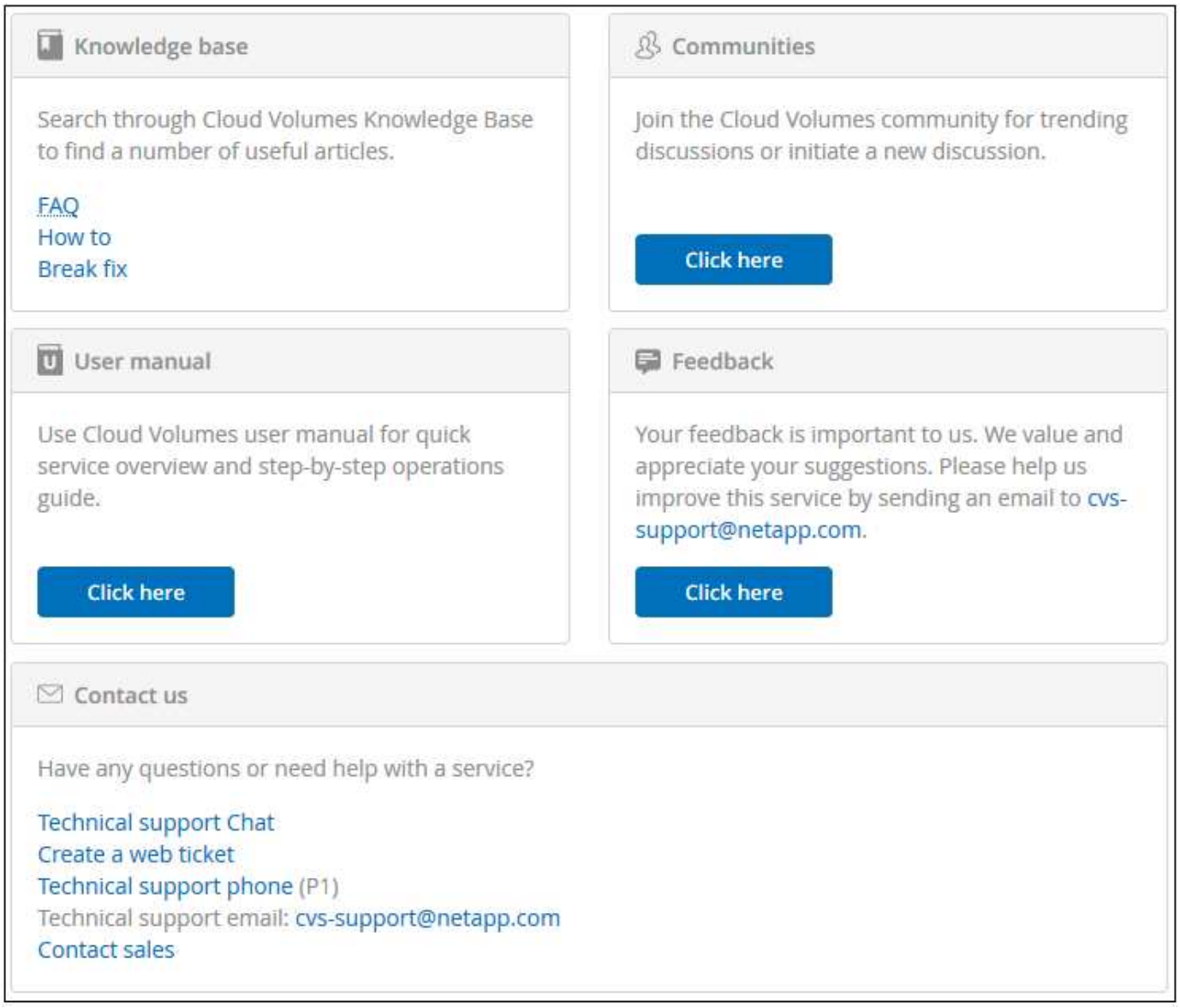
3. Complete the required information on the form:
   a. Enter your name and company information.
   b. Select **Cloud Volumes Service** as the Product Line and **Amazon Web Services** as the Cloud Service Provider.
   c. Enter your **NetApp serial number** and **AWS Customer ID** from the Cloud Volumes Service **Support** page into the next two fields.
   d. Click **Submit Registration**.
4. You will receive a confirmation email from your submitted registration. If no errors occur, you will be re-directed to a “Registration Submitted Successfully” page. You will also receive an email within an hour stating that “your product is now eligible for support”.
5. As a new NetApp customer, you also need to create a NetApp Support Site (NSS) user account for future support activations and for access to the support portal for technical support chat and web ticketing. Go to the NetApp Support Registration site to perform this task. You can provide your newly registered Cloud Volumes Service serial number to expedite the process.

This is a one-time support registration for the applicable Cloud Volumes Service serial number. Any new Cloud Volumes Service subscription and subsequent new serial number requires support activation as well. If you have any questions or problems with support registration, contact us at cvs-support@netapp.com.

Obtaining support information

NetApp provides support for Cloud Volumes Service in a variety of ways. Extensive free self-support options are available 24x7, such as knowledgebase (KB) articles or the NetApp community. The Cloud Volumes Service subscription purchased from the AWS SaaS marketplace includes remote technical support via chat, email, web ticketing, or phone. You must first activate support for each NetApp serial number in order to use these non self-service support options. A NetApp Support Site (NSS) SSO account is required for chat and web ticketing along with case management.

You can access support options from the Cloud Volumes Service UI by selecting the **Support** tab from the main menu. The support options available to you depend on whether you are in Trial mode or Subscription mode.



Self support

These options are available in Trial mode and are available for free 24x7:

- Knowledge base
  Selecting the links in this section takes you to the NetApp Knowledgebase, where you can search for articles, How-to's, FAQ's, or Break Fix information related to Cloud Volumes Service.

- User manual
  Selecting the **Click here** link takes you to the Cloud Volumes Service for AWS documentation center.
- Communities
  Selecting the **Click here** link takes you to the Cloud Volumes Service community, where you can connect with peers and experts.
- Email
  Selecting the **Click here** link in the Feedback section initiates an email to support through cvs-support@netapp.com. This a great place to ask general questions about service, provide feedback and suggestions, or seek assistance for onboarding related problems.

Subscription Support

In addition to the self-support options above, if you have a Cloud Volumes Service paid subscription, you can work with a NetApp Support Engineer to resolve any issues.

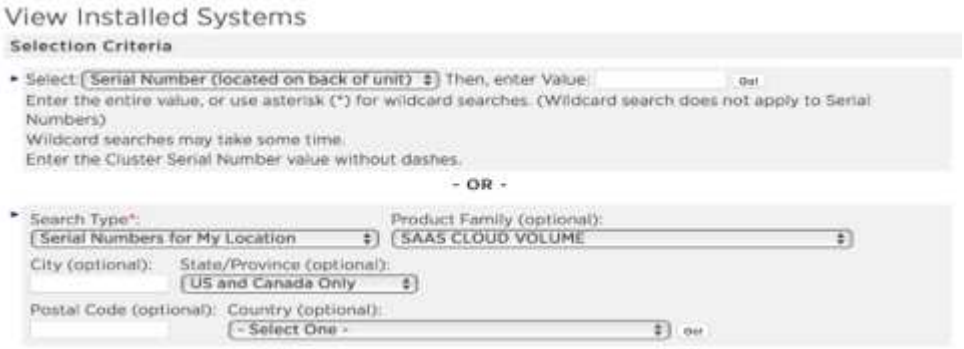
Once your Cloud Volumes Service serial number is activated, you can access NetApp technical support resources by any of the following methods. You must have an active Cloud Volumes subscription to use these support options.

- Chat
  This will open a support ticket as well.
- Support Ticket
  Select Cloud Data Services > Cloud Volumes Service AWS
- Phone
  For reporting new issues or calling about existing tickets. This method is best for P1 or immediate assistance.

You can also request sales support by clicking on the Contact sales link.

Your Cloud Volumes Service serial number is visible within the service from the Support menu option. If you are experiencing issues accessing the service and have registered a serial number with NetApp previously, you can contact cvs-support@netapp.com for assistance. You can also view your list of Cloud Volumes Service serial numbers from the NetApp Support Site as follows:

1. Login to mysupport.netapp.com.
2. From the Products > My Products menu tab, select the Product Family **SaaS Cloud Volume** to locate all your registered serial numbers:



Selecting the region

Cloud Volumes Service is available in many AWS regions. You must specify the region where you want to use the service before you create a cloud volume.

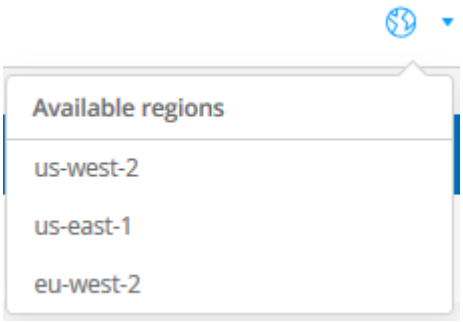
Steps

1. Navigate to the NetApp Cloud Orchestrator site, and then log in with the email address that you provided during your subscription.

   You should bookmark this URL. You will need to return to it later.

2. From the **Available regions** drop-down menu in the top panel, select the region that you want to work in.

   This selection process is similar to how you change regions in the AWS console.



3. Repeat the above step for each additional region when you want to create a cloud volume.

Note: The regions displayed in the Cloud Volumes user interface may use a different format than the region you selected in the AWS user interface. For example *us-east-1* in the Cloud Volumes UI corresponds to the *N.Virginia* region selected in the AWS console. See Regions and Availability Zones for a mapping of the region names to make sure you select the same region in both interfaces.

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.

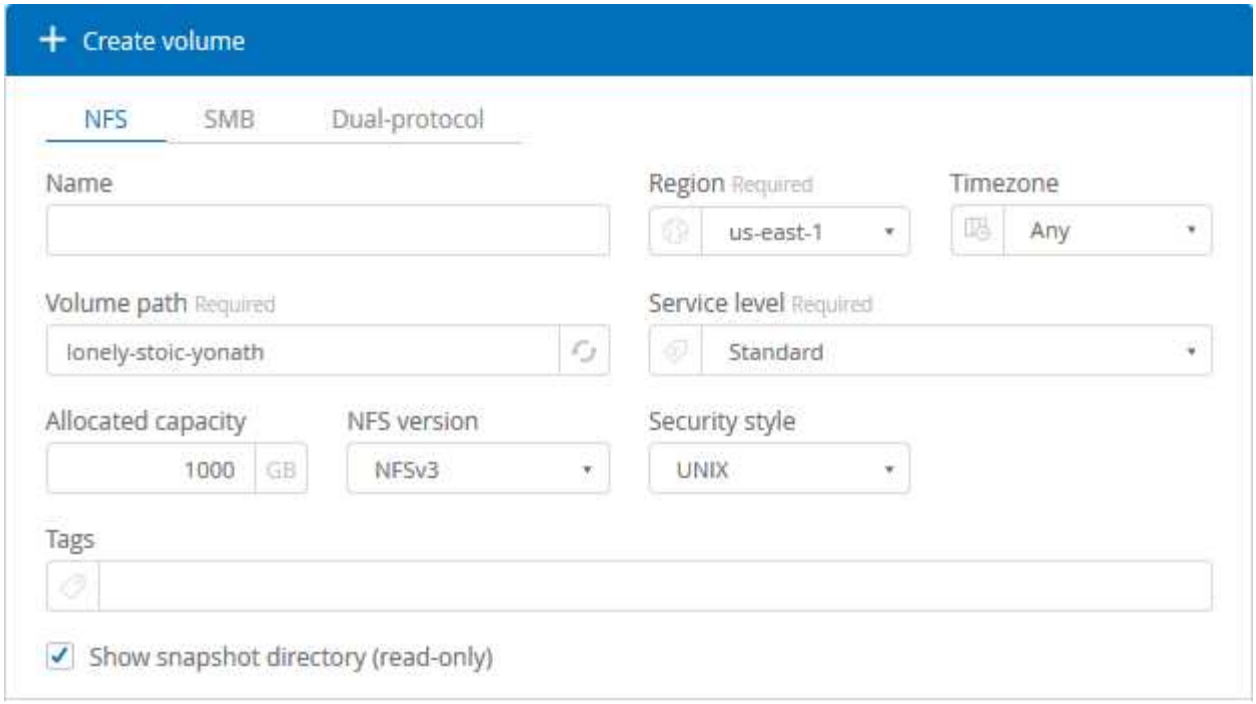
If you have not configured the required AWS networking components, see the NetApp Cloud Volumes Service for AWS Account Setup guide for details.

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.



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.

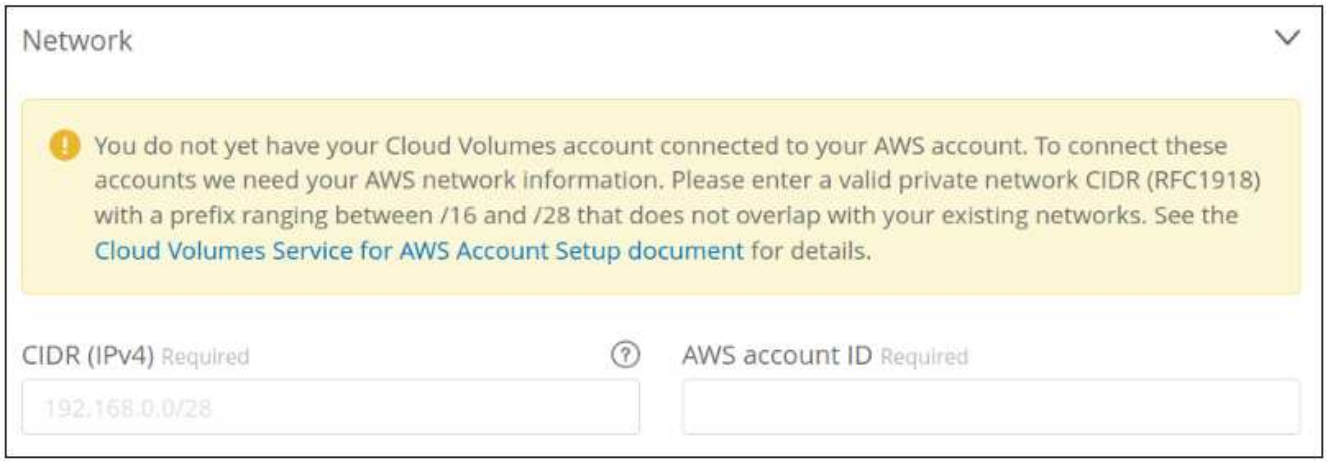
    Security styles affect the file permission type used and how permissions can be modified.

    - 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.



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.

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=THIRDLEVEL,OU=SECONDLEVEL,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.

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.

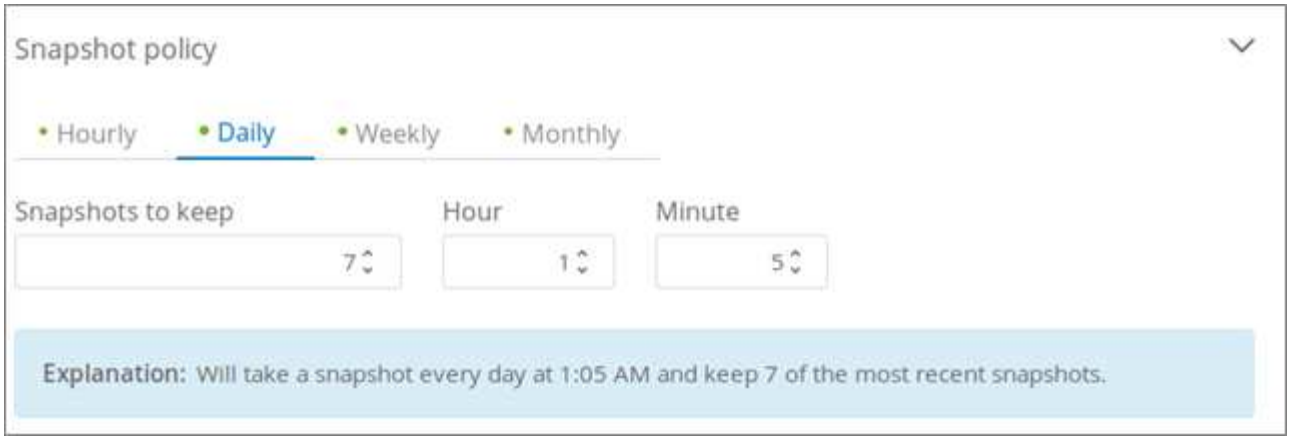
You should follow the guidance on AWS security group settings to enable cloud volumes to integrate with Windows Active Directory servers correctly. See AWS security group settings for Windows AD servers for more information.

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.



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.

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.

After you finish

Continue with Mounting a cloud volume.

Mounting a cloud volume

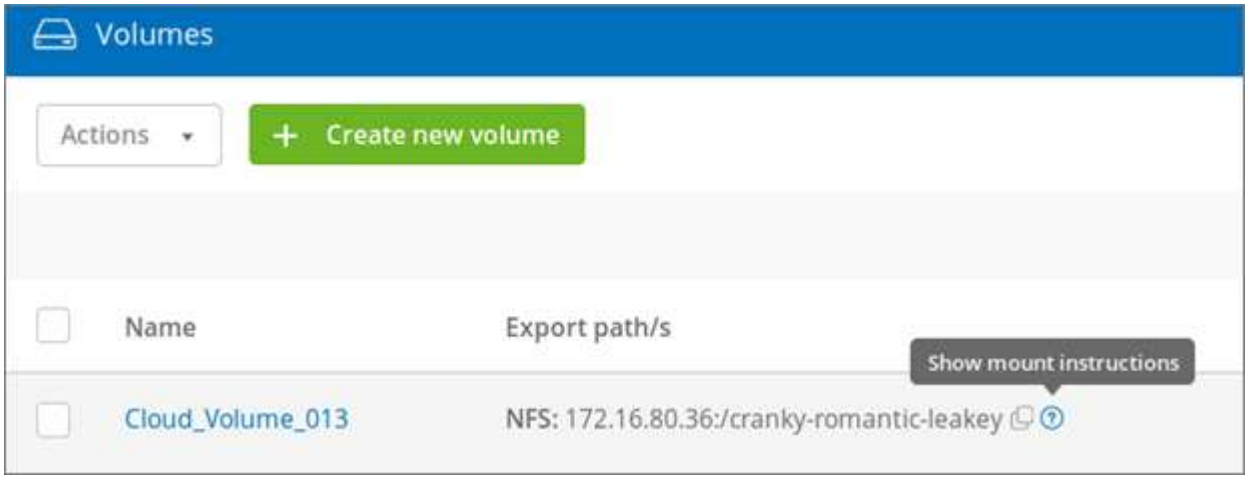
You can mount a cloud volume to your AWS instance. Cloud volumes currently support NFSv3 and NFSv4.1 for Linux and UNIX clients, and SMB 2.1, 3.0, and 3.1.1 for Windows clients.

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

Steps

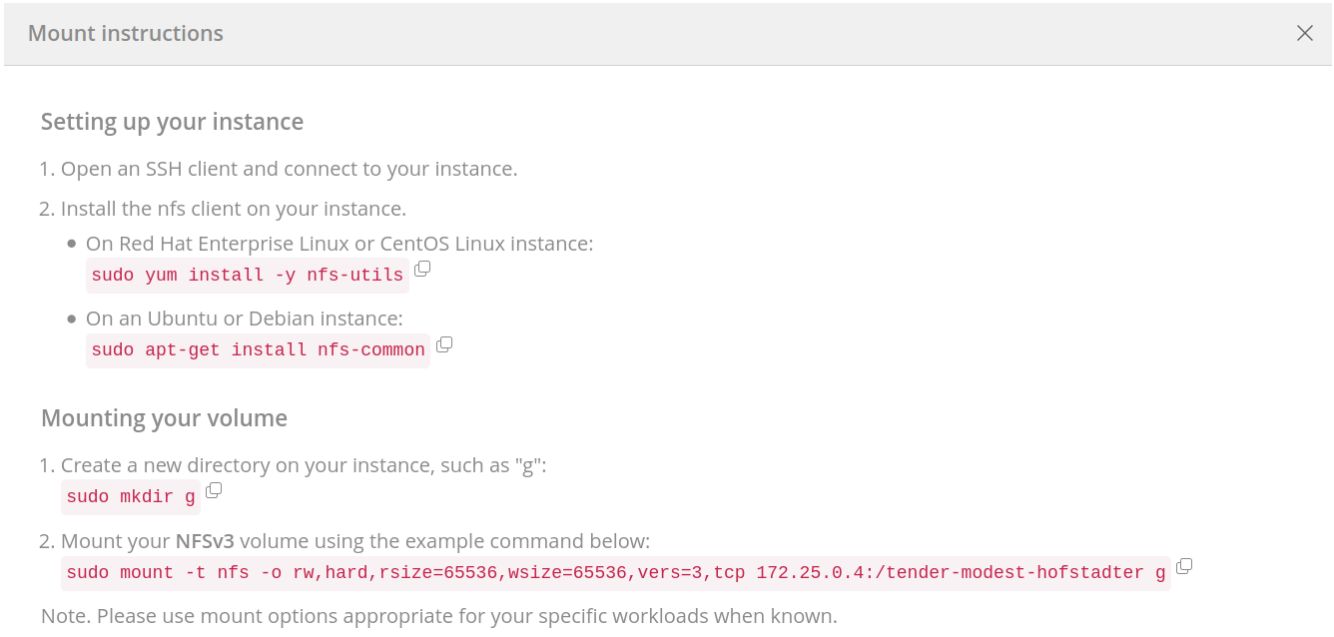
1. Obtain mount instructions for the volume you created by clicking the blue question mark (?) at the end of the Export Paths field next to the volume name.

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



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

   NFS example:



   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.

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**.

Managing cloud volume snapshots

Creating an on-demand snapshot for a cloud volume

You can create an on-demand snapshot of a cloud volume from either the Volumes or Snapshots page.

Creating snapshots from the Volumes page

Steps

1. Click the volume name, select **Snapshots**, and then click **+ Create new snapshot**.
2. Enter a name for the snapshot, or use the automatically generated name.
3. Select the volume name, and then, from the drop-down list, select the volume for which you want to create a snapshot.
4. Click **Create snapshot**.

The created snapshot appears.

Creating snapshots from the Snapshots page

Steps

1. Click **+ Create new snapshot**.
2. Enter a name for the snapshot, or use the automatically generated name.
3. From the drop-down list, select the volume for which you want to create a snapshot.
4. Click **Create snapshot**.

The created snapshot is now listed.

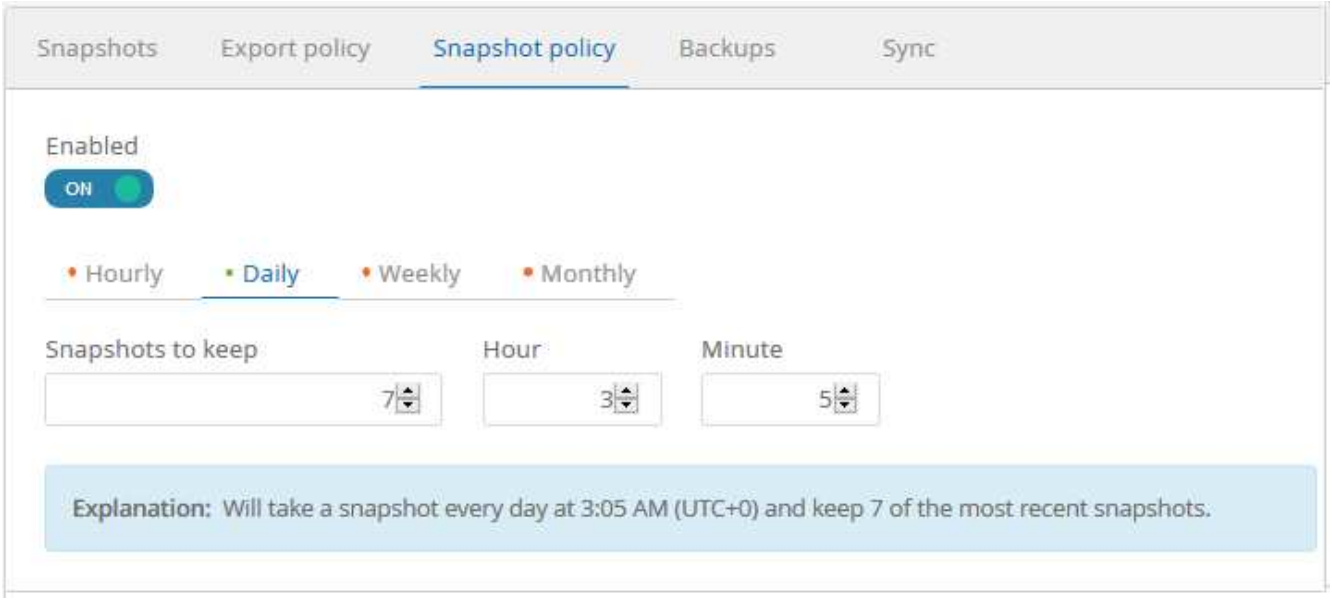
Creating or modifying a snapshot policy

You can create or modify a snapshot policy as necessary for a cloud volume.

Steps

1. From the Volumes page, click the volume name, and then select **Snapshot policy**.
2. Select **Hourly**, **Daily**, **Weekly**, or **Monthly** to specify the frequency for creating snapshots.

   Configured policies are marked with a green dot. Undefined policies are marked with a red dot.
3. Select the number of snapshots you want to keep.
4. Select the day, hour, and minute when the snapshot should be taken.
5. If you want to create additional snapshots with different frequencies, for example, both monthly and daily snapshots, repeat steps 2 through 4.



6. If the **Enabled** button is not already set to **ON**, click the button to enable or re-enable the policy.
7. Click **Save changes**.

Disabling 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. From the Volumes page, click the volume name, and then select **Snapshot policy**.
2. Click the **Enabled** button to **OFF** to disable snapshots from being created.

3. Click **Save changes**.

When you want to re-enable the snapshot policy, click the **Enabled** button to **ON** and click **Save changes**.

Reverting 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. On the Snapshots page or in the Snapshots tab in Volume details, select the snapshot that you want to revert to, click **Available**, and then select **Revert volume to snapshot**.

2. In the Revert snapshot dialog box, reenter the name of the volume that you want to revert and click **Revert**.

Deleting a snapshot

You can delete a snapshot from the Volumes or Snapshots page.

Deleting a snapshot from the Volumes page

Steps

1. Click the volume name, and then select **Snapshots** to see a list of snapshots for the volume.
2. Specify the snapshots that you want to delete by selecting the corresponding checkboxes, click **Actions**, and then select **Delete snapshot/s** from the drop-down list.

   Alternatively, you can click **Available** under Actions, then select **Delete snapshot** from the drop-down list.

3. In the confirmation dialog box, type `delete` to confirm, and then click **Delete**.

Deleting a snapshot from the Snapshots page

Steps

1. (Optional) Use the search box to filter the listed snapshots.
2. Specify the snapshots that you want to delete by selecting the corresponding checkboxes, click **Actions**, and then select **Delete snapshot/s** from the drop-down list.
3. In the confirmation dialog box, type `delete` to confirm, and then click **Delete**.

Restoring a snapshot to a new volume

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

Steps

1. On the Snapshots page or in the Snapshots section in Volume details, select the snapshot from which to restore, click **Available**, and then select **Restore to Volume**.
2. In the Create Volume dialog box, enter a name for the new volume, and edit other settings if necessary.

   Creating a cloud volume

3. Review the settings and then click **Create volume** to finish restoring the snapshot to the new volume.

Managing export policy rules

Modifying an export policy rule

You can modify the export policy rule for a volume as needed.

Steps

1. Click the volume name, and then select **Export policy**.
2. To change an existing export policy rule, modify the following fields as necessary:
   - **Allowed client**
   - **Access type**
3. Click **Save changes**.

Creating additional export policy rules

You can create additional export policy rules to enable flexible client access. For example, you can specify that a given IP range should have only read-only access to a volume.

Steps

1. Click the volume name, and then select **Export policy**.
2. Click **+ Add export policy rule**.
3. Set values for the following fields:
   - **Allowed client**
   - **Access type**
4. Click **Save changes**.

Deleting export policy rules

You can delete export policy rules that are no longer needed.

Steps

1. Click the volume name, and then select **Export policy**.
2. Click **X** for the policy rule that you want to delete.

3. Click **Save changes**.

Managing Cloud Sync for cloud volumes

Creating a Cloud Sync data broker

NetApp Cloud Sync is integrated with NetApp Cloud Volumes Service for AWS to enable fast data syncing over NFS to or from a cloud volume. A Cloud Sync data broker enables you to create a Cloud Sync relationship for syncing data.

About this task

If you already have a Cloud Sync data broker in the same AWS Virtual Private Cloud (VPC) that you use for your Cloud Volumes account, you can skip this task.

NetApp Cloud Sync Documentation

Steps

1. Go to the Sync page or the Sync tab for a volume on the Volumes page.
2. Create a data broker by clicking **Create data broker**.
3. Provide information for the following fields:
    - **Name**

      Provide a name for the data broker.

    - **Type**

      Select AWS.

    - **Region**

      Select an available region.

    - **API key**

      Provide the access key for your AWS account.

    - **Secret key**

      Provide the secret key for your AWS account.

    - **Keypair**

      Select an available keypair.

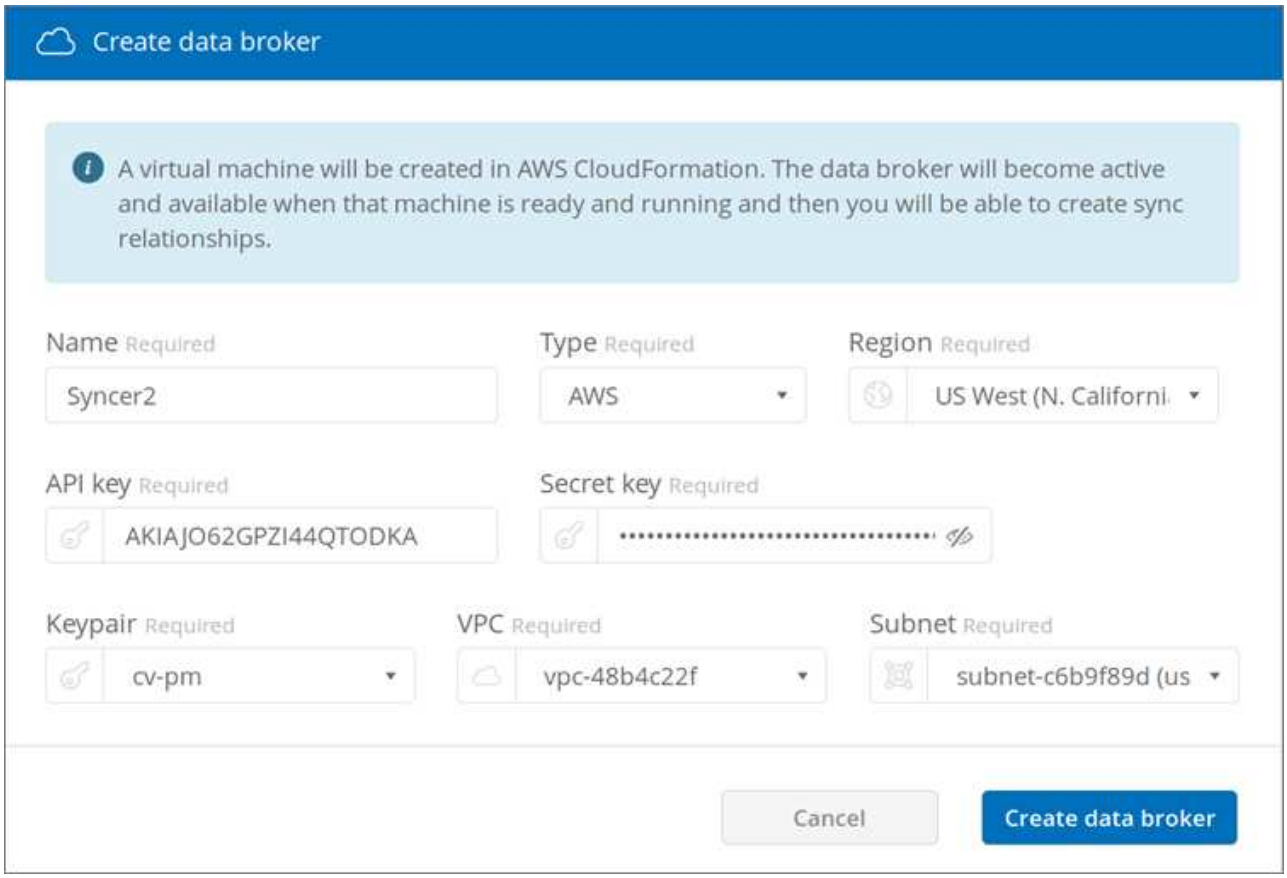
      The keypair will be updated after you enter valid keys.

    - **VPC**

      Select the VPC that is connected to your Cloud Volumes account.

    - **Subnet**

      Select an available subnet to use for the data broker.



4. Click **Create data broker** to start the data broker creation process.

   It takes a few minutes to create a data broker.
   After the data broker is created, it is marked with a green dot to indicate that it is ready.

After you finish

Continue with Creating a Cloud Sync Relationship.

Creating a Cloud Sync relationship

A Cloud Sync relationship enables you to sync data to or from the cloud volume.

Before you begin

- You must already have a Cloud Sync data broker.

  Creating a Cloud Sync data broker

- The data broker IP address must have been added to the export policy for both the source and the target volumes.

  The export policy on the target volume must allow write access to the data broker.

  Creating additional export policy rules

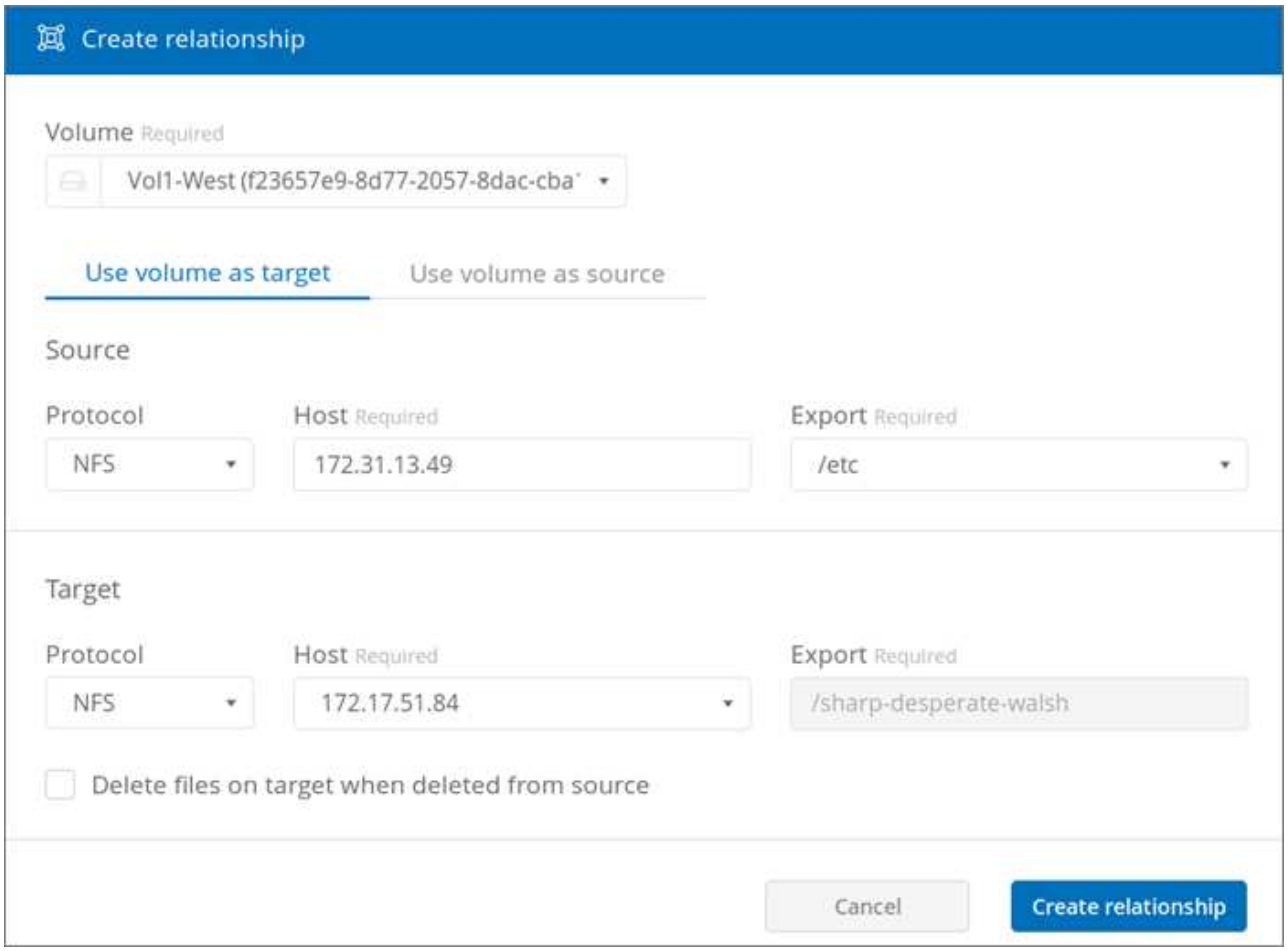
About this task

The Cloud Sync functionality that is integrated with Cloud Volumes Service currently supports only NFSv3. If

you want to sync between SMB volumes, you use the Cloud Sync Service directly (cloudsync.netapp.com).

Steps

1. Go to the Sync page or the Sync tab for a volume on the Volumes page.
2. Create a Cloud Sync relationship by clicking **Create new relationship**.
3. Take one of the following actions:
   - To sync data to the volume, select **Use volume as target**.
   - To sync data from the volume, select **Use volume as source**.



4. In the **Host** field (unpopulated), enter the IP address of the NFS server that you want to sync to or sync from.

   After a few moments, a list of the available exports is automatically discovered.

5. In the **Export** field, select one of the available exports.
6. (Optional) Check the **Delete files on target when deleted from source** box if you want to delete the files on target when they are deleted from source.
7. Click **Create relationship**.

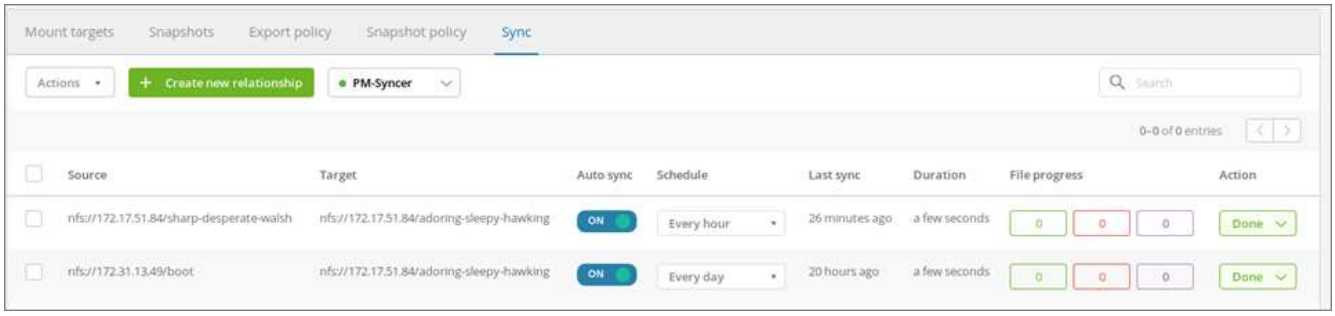
   The relationship status is displayed and the file progress fields show the number of files that are copied.

Modifying the Cloud Sync schedule

When a Cloud Sync relationship is initially created, auto sync is enabled by default and scheduled to run once a day. You can modify the Cloud Sync schedule as appropriate.

Steps

1. Go to the Sync page or the Sync tab for a volume on the Volumes page to see the Cloud Sync relationships.



2. To turn off auto sync for a Cloud Sync relationship, click the blue **ON** slider for the relationship.

3. To change the sync schedule, click the drop-down list under **Schedule**, select **Day/s** or **Hour/s**, select an interval number, and then click the checkmark.

4. To start Cloud Sync immediately, click **Done** under Action, select **Sync Now**, and click **Sync Now** again to confirm.

Deleting a Cloud Sync relationship

You can delete a Cloud Sync relationship that is no longer needed.

Steps

1. Go to the Sync page or the Sync tab for a volume on the Volumes page.
2. Click the box for the relationship you want to delete, click **Actions**, and then select **Delete relationship/s**.
3. In the confirmation dialog box, type `delete` to confirm, and then click **Delete**.

Deleting a Cloud Sync data broker

You can delete a Cloud Sync data broker that is no longer needed.

About this task

This task removes the data broker from cloud volumes, but it does not delete the data broker instance in AWS.

To delete the data broker instance in AWS, you must go to the AWS console for your account, locate the EC2 instance for the broker by name, and then terminate it as needed.

Before you begin

All Cloud Sync relationships that use the data broker must have already been deleted before you can delete the data broker.

Deleting a Cloud Sync Relationship

Steps

1. Go to the Sync page or the Sync tab for a volume on the Volumes page.
2. Delete a data broker by clicking the data broker's name and click the trash can icon.
3. In the confirmation dialog box, type `delete` to confirm, and then click **Delete**.

Cloud Volumes APIs

The Cloud Volumes capabilities that are available through the web UI are also available through RESTful APIs. The APIs enable you to create and manage cloud volumes and develop provisioning scripts and tools.

Finding the API URL, API key, and Secret key

You need to obtain the Cloud Volumes API URL, API key, and Secret key for running an API call.

Steps

1. Click **API access** on the storage page or in the drop-down menu under your username.
2. Record the Cloud Volumes API URL, API key, and Secret key.

Sample file showing the API URL, API key, and Secret key for an account

Listing the available APIs

The storage page displays the available APIs that you can use.

Steps

1. Click **API documentation** on the storage page.

   The page lists the available APIs.

2. Scroll through the page to see the available APIs.

   The APIs are listed by function, for example:

   - `volumes`
   - `mounttargets`
   - `storage`
   - `snapshots`

3. To obtain details and examples of how to use an API call, select the function and click one of the following actions:

   - `GET`: reads
   - `POST`: creates
   - `PUT`: updates or modifies
   - `DELETE`: destroys

Using the Cloud Volumes APIs

This section shows you how to use the Cloud Volumes APIs. The examples use curl from a Linux bash shell. You need to replace `<api_url>`, `<api_key>`, and `<secret_key>` with the values you recorded from Finding the API URL, API key, and Secret key.

Syntax

```
curl -s -H accept:application/json -H "Content-type: application/json" -H api-key:<api_key> -H secret-key:<secret_key> -X [GET,POST,PUT,DELETE] <api_url>/v2/<command>
```

Examples

Listing volumes

The following example displays information about all volumes:

Piping the command through `jq` improves the formatting of the `json` output. You might need to install `jq` on your system.

```
curl -s -H accept:application/json -H "Content-type: application/json" -H api-key:<api_key> -H secret-key:<secret_key> -X GET <api_url>/v2/Volumes | jq
```

Script to list cloud volumes in an account

Listing the details for a specific volume

Each volume has an ID called `volumeId`, for example, `07c9ab6c-b655-a9fe-f904-b9b97ef9baaa`. Including the ID in the API call provides details for the specific volume:

```
curl -s -H accept:application/json -H "Content-type: application/json" -H api-key:<api_key> -H secret-key:<secret_key> -X GET <api_url>/v2/Volumes/<volumeId> | jq
```

Creating a volume

The following example uses a `POST` call to create a volume called `Test`, in region `us-west-1`, with an `allocated capacity` of 100 GB and exported using `nfsv3`:

```
curl -s -H accept:application/json -H "Content-type: application/json" -H
api-key:<api_key> -H secret-key:<secret_key> -X POST <api_url>/v2/Volumes
-d '
{
    "name": "Test",
    "creationToken": "grahams-test-volume3",
    "region": "us-west-1",
    "serviceLevel": "standard",
    "quotaInBytes": 100000000000,
    "exportPolicy": {"rules": [{"ruleIndex": 1,"allowedClients":
"0.0.0.0/0","unixReadOnly": false,"unixReadWrite": true,"cifs": false
,"nfsv3": true,"nfsv4": false}]},
    "protocolTypes": ["NFSv3"],
    "labels": ["test"]
}'
```

Script to create a cloud volume

Updating a volume

The following example uses a `PUT` call to update a volume called `Test`, change the service level to `extreme`, and change the allocated capacity to 600 GB:

```
curl -s -H accept:application/json -H "Content-type: application/json" -H
api-key:<api_key> -H secret-key:<secret_key> -X PUT <api_url>/v
2/Volumes/<volumeId> -d '
{
    "serviceLevel": "extreme",
    "quotaInBytes": 600000000000
}'
```

Script to update a cloud volume

Deleting a volume

The following example uses a `DELETE` call to delete a volume specified by `volumeId`:

```
curl -s -H accept:application/json -H "Content-type: application/json" -H
api-key:<api_key> -H secret-key:<secret_key> -X DELETE <api_url>/v
2/Volumes/<volumeId>
```

Script to delete a cloud volume by mountpoint

Use with caution. This API call deletes the volume and all its data.

Creating a snapshot

The following example uses a `POST` call to create a snapshot called `snappy` for a specific volume:

```
curl -s -H accept:application/json -H "Content-type: application/json" -H
api-key:<api_key> -H secret-key:<secret_key> -X POST <api_url>/v
2/Volumes/<volumeId>/Snapshots -d '
{
    "name": "<snapshot-name>"
}'
```

Script to create snapshots of a cloud volume by mountpoint

Creating a snapshot policy

The following example uses a `PUT` call to create snapshot policies for a specific volume:

```
curl -s -H accept:application/json -H "Content-type: application/json" -H
api-key:<api_key> -H secret-key:<secret_key> -X PUT <api_url>/v
2/Volumes/<volumeId> -d '
{
    "snapshotPolicy": {
        "dailySchedule": {},
        "enabled": true,
        "hourlySchedule": {
            "minute": 33,
            "snapshotsToKeep": 24
        },
        "monthlySchedule": {},
        "weeklySchedule": {}
    }
}'
```

Script to create snapshot policies for a cloud volume by mountpoint

Listing snapshots for a specific volume

The following example uses a `GET` call to list the snapshots for a specific volume:

```
curl -s -H accept:application/json -H "Content-type: application/json" -H
api-key:<api_key> -H secret-key:<secret_key> -X GET <api_url>/v
2/Volumes/<volumeId>/Snapshots
```

Script to list snapshots of a cloud volume by mountpoint

Reverting a snapshot

The following example uses a `POST` call to revert a volume from a snapshot specified by `snapshotId` and `volumeId`:

```
curl -s -H accept:application/json -H "Content-type: application/json" -H
api-key:<api_key> -H secret-key:<secret_key> -X POST <api_url>/v
2/Volumes/<volumeId>/Revert -d '
{
    "snapshotId": "<snapshotId>"
}'
```

Script to revert to a snapshot of a cloud volume by mountpoint and snapshotId

Use with caution. This API call causes any data written after the date of that snapshot to be lost.

Creating a new volume from a snapshot

The following example uses a `POST` call to create a new volume based on a snapshot of an existing volume, specified by `snapshotId`:

```
curl -s -H accept:application/json -H "Content-type: application/json" -H
api-key:<api_key> -H secret-key:<secret_key> -X POST <api_url>/v2/Volumes
-d '
{
    "snapshotId": "<snapshotId>",
    "name": "Copy",
    "creationToken": "perfectly-copied-volume",
    "region": "us-west-1",
    "serviceLevel": "extreme",
    "protocolTypes": ["NFSv3"]
}'
```

Script to copy a cloud volume

Deleting a snapshot

The following example uses a `DELETE` call to delete a snapshot specified by `snapshotId`:

```
curl -s -H accept:application/json -H "Content-type: application/json" -H
api-key:<api_key> -H secret-key:<secret_key> -X DELETE <api_url>/v
2/Volumes/<volumeId>/Snapshots/<snapshotId>
```

Script to delete a snapshot of a cloud volume by mountpoint and snapshotId

Use with caution. This API call deletes the snapshot and all its data.

Joining a directory service

The following example uses a `POST` call to join a directory service and provides the DNS IP address, domain, the NetBIOS name for the SMB server, the username and password for a directory service admin, and the organizational unit (optional and defaults to CN=Computers).

```
curl -s -H accept:application/json -H "Content-type: application/json" -H
api-key:<api_key> -H secret-key:<secret_key> -X POST <api_url>/v
2/Storage/ActiveDirectory -d '
{
    "DNS": "<ip-address>",
    "domain": "<domain>",
    "netBIOS": "<netbios-name>",
    "organizationalUnit": "OU=Cloud Servers,DC=nas-cloud,DC=local",
    "password": "secret",
    "region": "us-west-1",
    "username": "Administrator"
}'
```

Script to join a directory service

Viewing directory service integration

The following example uses a `GET` call to display the configuration for directory service integration.

```
curl -s -H accept:application/json -H "Content-type: application/json" -H
api-key:<api_key> -H secret-key:<secret_key> -X GET <api_url>/v
2/Storage/ActiveDirectory
```

Script to view directory service integration

Unjoining a directory service

The following example uses a `DELETE` call to unjoin a directory service integration. This requires the UUID for the current join, which can be found using the `GET` call listed above.

You cannot unjoin a directory service that is in use; status "in use".

```
curl -s -H accept:application/json -H "Content-type: application/json" -H
api-key:<api_key> -H secret-key:<secret_key> -X DELETE <api_url>/v
2/Storage/ActiveDirectory/<UUID>
```

Script to unjoin a directory service

Get performance statistics

The following example uses a `GET` call to list the read and write IOPS, throughput, and latency statistics over a specific time period for a volume specified by `volumeId`.

```
curl -s -H accept:application/json -H "Content-type: application/json" -H
api-key:<api_key> -H secret-key:<secret_key> -X GET '<api_url>/v
2/Volumes/<volumeId>/PerformanceMetrics?startDate=2021-02-05T09:
00&endDate=2021-02-05T09:
05&type=READ_IOPS,WRITE_IOPS,TOTAL_THROUGHPUT,AVERAGE_OTHER_LATENCY'
```

Script to get performance statistics of a cloud volume by mountpoint

Reference

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
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" }
        }
    }
}
```

Selecting the appropriate service level 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.

All pricing information in this article is based on the list prices as of September 12, 2018. The information is provided for example purposes only and is subject to change.

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.

Creating cloud volumes
Modifying cloud volumes

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.

  - List Price: $0.10 per GB per month (as of September 12, 2018)
  - 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.

  - List Price: $0.20 per GB per month (as of September 12, 2018)
  - 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.

  - List Price: $0.30 per GB per month (as of September 12, 2018)
  - 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.

Creating cloud volumes
Modifying cloud volumes

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.

Cost comparison for service levels and allocated capacity

The table below compares cost for different service levels and allocated capacity sizes. In the table, the leftmost column indicates the capacity, and the other columns define the MB/s available at each capacity point and its cost.

All pricing information is based on the list prices as of September 12, 2018. The information is provided for example purposes only and is subject to change.

Capacity	Standard		Premium		Extreme	
TB	**MB/s**	**Cost**	**MB/s**	**Cost**	**MB/s**	**Cost**
0.1 (100 GB)	1.6	$10	6.4	$20	12.8	$30
1	16	$100	64	$200	128	$300
2	32	$200	128	$400	256	$600
3	48	$300	192	$600	384	$900
4	64	$400	256	$800	512	$1,200
5	80	$500	320	$1,000	640	$1,500
6	96	$600	384	$1,200	768	$1,800
7	112	$700	448	$1,400	896	$2,100
8	128	$800	512	$1,600	1,024	$2,400
9	144	$900	576	$1,800	1,152	$2,700
10	160	$1,000	640	$2,000	1,280	$3,000
11	176	$1,100	704	$2,200	1,408	$3,300
12	192	$1,200	768	$2,400	1,536	$3,600
13	208	$1,300	832	$2,600	1,664	$3,900
14	224	$1,400	896	$2,800	1,792	$4,200
15	240	$1,500	960	$3,000	1,920	$4,500

Capacity	Standard		Premium		Extreme	
16	256	$1,600	1,024	$3,200	2,048	$4,800
17	272	$1,700	1,088	$3,400	2,176	$5,100
18	288	$1,800	1,152	$3,600	2,304	$5,400
19	304	$1,900	1,216	$3,800	2,432	$5,700
20	320	$2,000	1,280	$4,000	2,560	$6,000
21	336	$2,100	1,344	$4,200	2,688	$6,300
22	352	$2,200	1,408	$4,400	2,816	$6,600
23	368	$2,300	1,472	$4,600	2,944	$6,900
24	384	$2,400	1,536	$4,800	3,072	$7,200
25	400	$2,500	1,600	$5,000	3,200	$7,500
26	416	$2,600	1,664	$5,200	3,328	$7,800
27	432	$2,700	1,728	$5,400	3,456	$8,100
28	448	$2,800	1,792	$5,600	3,584	$8,400
29	464	$2,900	1,856	$5,800	3,712	$8,700
30	480	$3,000	1,920	$6,000	3,840	$9,000
31	496	$3,100	1,984	$6,200	3,968	$9,300
32	512	$3,200	2,048	$6,400	4,096	$9,600
33	528	$3,300	2,112	$6,600	4,224	$9,900
34	544	$3,400	2,176	$6,800	4,352	$10,200
35	560	$3,500	2,240	$7,000	4,480	$10,500
36	576	$3,600	2,304	$7,200	4,500	$10,800
37	592	$3,700	2,368	$7,400	4,500	$11,100
38	608	$3,800	2,432	$7,600	4,500	$11,400
39	624	$3,900	2,496	$7,800	4,500	$11,700
40	640	$4,000	2,560	$8,000	4,500	$12,000
41	656	$4,100	2,624	$8,200	4,500	$12,300
42	672	$4,200	2,688	$8,400	4,500	$12,600
43	688	$4,300	2,752	$8,600	4,500	$12,900
44	704	$4,400	2,816	$8,800	4,500	$13,200
45	720	$4,500	2,880	$9,000	4,500	$14,500
46	736	$4,600	2,944	$9,200	4,500	$13,800
47	752	$4,700	3,008	$9,400	4,500	$14,100

Capacity	Standard		Premium		Extreme	
48	768	$4,800	3,072	$9,600	4,500	$14,400
49	784	$4,900	3,136	$9,800	4,500	$14,700
50	800	$5,000	3,200	$10,000	4,500	$15,000
51	816	$5,100	3,264	$10,200	4,500	$15,300
52	832	$5,200	3,328	$10,400	4,500	$15,600
53	848	$5,300	3,392	$10,600	4,500	$15,900
54	864	$5,400	3,456	$10,800	4,500	$16,200
55	880	$5,500	3,520	$11,000	4,500	$16,500
56	896	$5,600	3,584	$11,200	4,500	$16,800
57	912	$5,700	3,648	$11,400	4,500	$17,100
58	928	$5,800	3,712	$11,600	4,500	$17,400
59	944	$5,900	3,776	$11,800	4,500	$17,700
60	960	$6,000	3,840	$12,000	4,500	$18,000
61	976	$6,100	3,904	$12,200	4,500	$18,300
62	992	$6,200	3,968	$12,400	4,500	$18,600
63	1,008	$6,300	4,032	$12,600	4,500	$18,900
64	1,024	$6,400	4,096	$12,800	4,500	$19,200
65	1,040	$6,500	4,160	$13,000	4,500	$19,500
66	1,056	$6,600	4,224	$13,200	4,500	$19,800
67	1,072	$6,700	4,288	$13,400	4,500	$20,100
68	1,088	$6,800	4,352	$13,600	4,500	$20,400
69	1,104	$6,900	4,416	$13,800	4,500	$20,700
70	1,120	$7,000	4,480	$14,000	4,500	$21,000
71	1,136	$7,100	4,500	$14,200	4,500	$21,300
72	1,152	$7,200	4,500	$14,400	4,500	$21,600
73	1,168	$7,300	4,500	$14,600	4,500	$21,900
74	1,184	$7,400	4,500	$14,800	4,500	$22,200
75	1,200	$7,500	4,500	$15,000	4,500	$22,500
76	1,216	$7,600	4,500	$15,200	4,500	$22,800
77	1,232	$7,700	4,500	$15,400	4,500	$23,100
78	1,248	$7,800	4,500	$15,600	4,500	$23,400
79	1,264	$7,900	4,500	$15,800	4,500	$23,700

Capacity	Standard		Premium		Extreme	
80	1,280	$8,000	4,500	$16,000	4,500	$24,000
81	1,296	$8,100	4,500	$16,200	4,500	$24,300
82	1,312	$8,200	4,500	$16,400	4,500	$24,600
83	1,328	$8,300	4,500	$16,600	4,500	$24,900
84	1,344	$8,400	4,500	$16,800	4,500	$25,200
85	1,360	$8,500	4,500	$17,000	4,500	$25,500
86	1,376	$8,600	4,500	$17,200	4,500	$25,800
87	1,392	$8,700	4,500	$17,400	4,500	$26,100
88	1,408	$8,800	4,500	$17,600	4,500	$26,400
89	1,424	$8,900	4,500	$17,800	4,500	$26,700
90	1,440	$9,000	4,500	$18,000	4,500	$27,000
91	1,456	$9,100	4,500	$18,200	4,500	$27,300
92	1,472	$9,200	4,500	$18,400	4,500	$27,600
93	1,488	$9,300	4,500	$18,600	4,500	$27,900
94	1,504	$9,400	4,500	$18,800	4,500	$28,200
95	1,520	$9,500	4,500	$19,000	4,500	$28,500
96	1,536	$9,600	4,500	$19,200	4,500	$28,800
97	1,552	$9,700	4,500	$19,400	4,500	$29,100
98	1,568	$9,800	4,500	$19,600	4,500	$29,400
99	1,584	$9,900	4,500	$19,800	4,500	$29,700
100	1,600	$10,000	4,500	$20,000	4,500	$30,000

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, 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 to select 13 TB at the Premium service level.

Legal notices

Legal notices provide access to copyright statements, trademarks, patents, and more.

Copyright

http://www.netapp.com/us/legal/copyright.aspx

Trademarks

NETAPP, the NETAPP logo, and the marks listed on the NetApp Trademarks page are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.

http://www.netapp.com/us/legal/netapptmlist.aspx

Patents

A current list of NetApp owned patents can be found at:

https://www.netapp.com/us/media/patents-page.pdf

Privacy policy

https://www.netapp.com/us/legal/privacypolicy/index.aspx

Open source

Notice files provide information about third-party copyright and licenses used in NetApp software.

- Notice for NetApp Cloud Volumes Service
- Notice for ONTAP

Copyright Information

Copyright © 2021 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.