



NetApp Cloud Volumes Service for AWS

AWS Account Setup

Cloud Volumes Team, NetApp, Inc.
December 13, 2019

Abstract

This document provides instructions to set up the initial AWS environment for using the NetApp® Cloud Volumes Service for Amazon Web Services (AWS).

TABLE OF CONTENTS

1	Overview	3
2	Important Information	3
3	Prerequisites	3
3.1	Administrative	3
3.2	Skills and Knowledge	3
3.3	Compute Resources	3
4	Workflow Overview.....	4
4.1	Virtual Private Gateways and Direct Connect Gateways	4
4.2	Cloud Volumes Service Setup Workflow.....	5
5	Set Up your AWS Account for the Cloud Volumes Service	5
5.1	Create a VPC to use with Cloud Volumes (optional).....	6
5.2	Create a Virtual Private Gateway and attach it to your VPC	8
5.3	Create a Subnet for the VPC	9
5.4	Set Up Routes.....	10
5.5	Create a Direct Connect Gateway and Associate it with the Virtual Private Gateway (optional).....	12
5.6	Gather Required AWS Configuration Information	14
6	Enable AWS Subscription and Cloud Volumes Service.....	16
6.1	Access AWS Marketplace Listing for Cloud Volumes Service	16
6.2	Register and Log into NetApp Cloud Central	18
6.3	Create Your First Cloud Volume	19
6.4	Accept the Direct Connect Virtual Interfaces.....	22
7	Manage Cloud Volumes	24
8	Sharing Cloud Volumes Service between AWS accounts (optional).....	25
	Support	26
	Where to Find Additional Information	26
	Version History	26

LIST OF FIGURES

Figure 1)	Workflow diagram: Cloud Volumes Service for AWS setup.	5
Figure 2)	Cloud Volumes Service Architecture for AWS.....	6

1 Overview

This document guides you through the required steps to (1) Set up your network connections from your AWS account to your Cloud Volumes Service account, (2) Subscribe to NetApp Cloud Volumes Service (CVS) on the AWS Marketplace, and (3) Set up a user account in Cloud Volumes Service.

2 Important Information

To activate your Cloud Volumes Service, you will need to follow these instructions carefully to ensure that your AWS account is set up to accept and connect to the CVS service through the Virtual interfaces that will be published to your account from NetApp, as part of this setup procedure.

Before proceeding with the subscription, you may need to first consult with your AWS administrator, and/or your network security and administration team to review these setup instructions and to provide guidance.

3 Prerequisites

3.1 Administrative

The following administrative tasks are required to access Cloud Volumes Service for AWS:

- Willingness to accept the NetApp End-User License Agreement (EULA)
This EULA is presented as part of the AWS Marketplace subscription process.
- An active AWS account (with permissions to subscribe to new Marketplace listings)
You should have your 12-digit AWS account ID available as you will need it during the setup process.
To find your account ID, refer to this [AWS content](#).

3.2 Skills and Knowledge

The following skills and information are required to access Cloud Volumes Service for AWS:

- Access to and knowledge of the AWS Marketplace.
- You must have an unused IPv4 CIDR block for your cloud volumes where the network must be a /28. The network must also fall within the ranges reserved for private networks (RFC 1918).

Warning: Do not choose a network that overlaps your VPC CIDR allocations.

- Knowledge of your AWS network and connectivity settings and controls.
If necessary, consult with your AWS and network team prior to completing these setup instructions.

3.3 Compute Resources

The following compute resources are required to access Cloud Volumes Service for AWS:

Important: All AWS compute and other resources used are the sole responsibility of the user.

- A Virtual Private Cloud (VPC), Virtual Private Gateway, and optionally a Direct Connect Gateway that are running prior to the setup of Cloud Volumes Service for AWS. These instructions describe how to do this if you do not have these components already set up.
- When planning to create a cloud volume using the SMB protocol, instead of NFS, you can perform authentication using your own Windows Active Directory server or a Microsoft Active Directory in the AWS Cloud (AWS Managed Microsoft AD).
See [AWS security group settings for Windows AD servers](#) for additional information.

4 Workflow Overview

The next two pages provide an overview of the setup steps you need to complete before you can create your first cloud volume. It is important that you understand the setup tasks. The actual steps begin in section 5.1 on page 6.

DO NOT click the **Subscribe** button from the AWS Marketplace until you have completed all the steps in section 5.

4.1 Virtual Private Gateways and Direct Connect Gateways

NetApp Cloud Volumes Service can be connected to either a Virtual Private Gateway or a Direct Connect Gateway. This provides options to best meet your needs. You need to decide which gateway you will use before completing the steps.

Virtual Private Gateways

Virtual Private Gateways allow only one VPC to be connected to the Cloud Volumes Service. This can be useful to further enhance security by isolating data access to a single VPC.

Connectivity to Cloud Volumes from on-premise clients

Virtual Private Gateways also enable you to connect to Cloud Volumes from your on-premise clients when using a Virtual Private Gateway that has AWS Direct Connections to your premise and is used to connect Cloud Volumes.

Important: The CIDR range selected for Cloud Volumes cannot overlap ranges used in the on-premise network.

Direct Connect Gateways

Direct Connect Gateways provide additional flexibility, such as the ability to connect EC2 instances from up to 10 VPCs to a cloud volume and for the VPCs to be in different regions. It enables cloud volumes from multiple regions to be connected via the same Direct Connect Gateway. Additionally, if you plan to use NetApp [Cloud Sync](#) to sync data to or from cloud volumes that may be in different regions, you must use a Direct Connect Gateway.

Important:

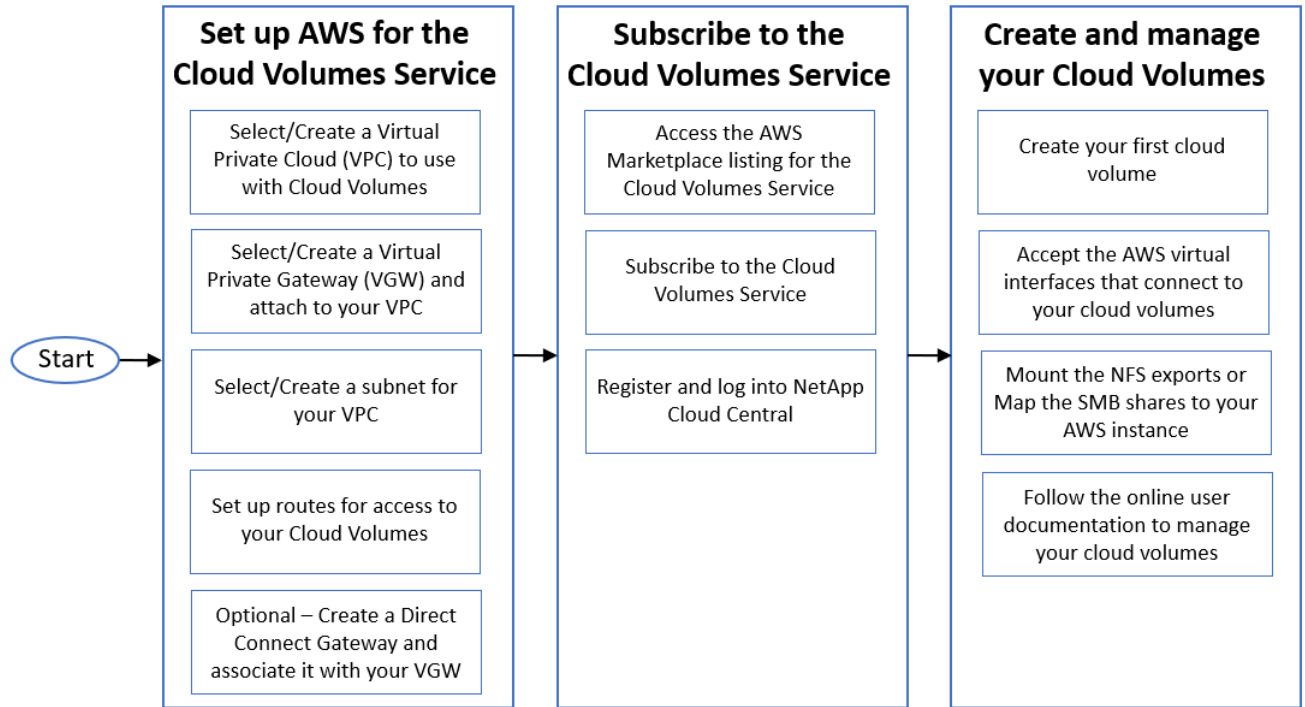
- Direct Connect Gateways allow multiple VPCs to be added, however the CIDR ranges of the VPCs cannot overlap as the gateway effectively creates a single network. If you require VPCs that have the same CIDR range, then connect Virtual Private Gateways directly to your cloud volume Virtual Interfaces.
- Direct Connect Gateways do not enable access from on-premise clients. Choose a Virtual Private Gateway if you require this functionality.

4.2 Cloud Volumes Service Setup Workflow

Figure 1 is a high-level workflow diagram illustrating how to set up your Cloud Volumes Service for AWS account, and how to subscribe to the Cloud Volumes Service for AWS.

For detailed steps for creating your Cloud Volumes Service for AWS account, see section 5 and section 6.

Figure 1) Workflow diagram: Cloud Volumes Service for AWS setup.



5 Set Up your AWS Account for the Cloud Volumes Service

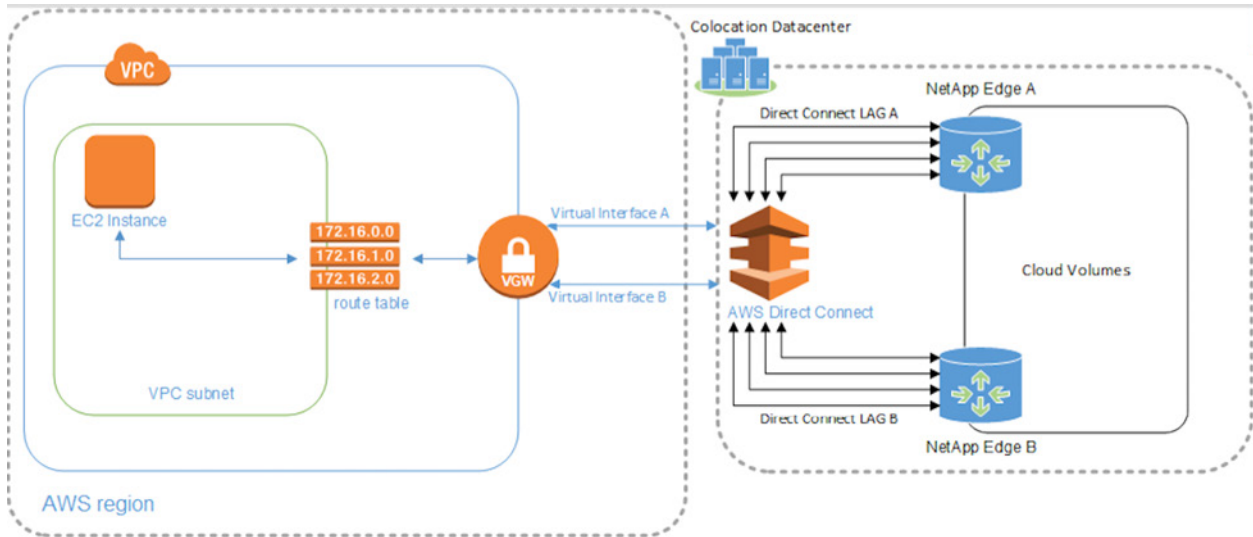
Before you subscribe to NetApp Cloud Volumes Service for AWS, you must create, or verify that your AWS account is correctly configured, with the following components:

- A Virtual Private Cloud (VPC) to use with Cloud Volumes (section 5.1)
- A Virtual Private Gateway (VGW) (section 5.2)
- A subnet for the VPC (section 5.3)
- Routes that include the Cloud Volumes network (section 5.4)
- Optionally, a Direct Connect Gateway associated with the VGW (section 5.5)

If you already have a VPC and Virtual Private Gateway or a Direct Connect Gateway configured, and you plan to use these components to connect to CVS, jump to section 5.4

Figure 2 illustrates the connectivity and setup for the Cloud Volumes Service for AWS.

Figure 2) Cloud Volumes Service Architecture for AWS.



Note: The sample text shown in the screenshots in the steps that follow are provided just as an example. Use your own information when configuring these AWS components. For example, use your own information for the Virtual Private Cloud name and Virtual Private Gateway name.

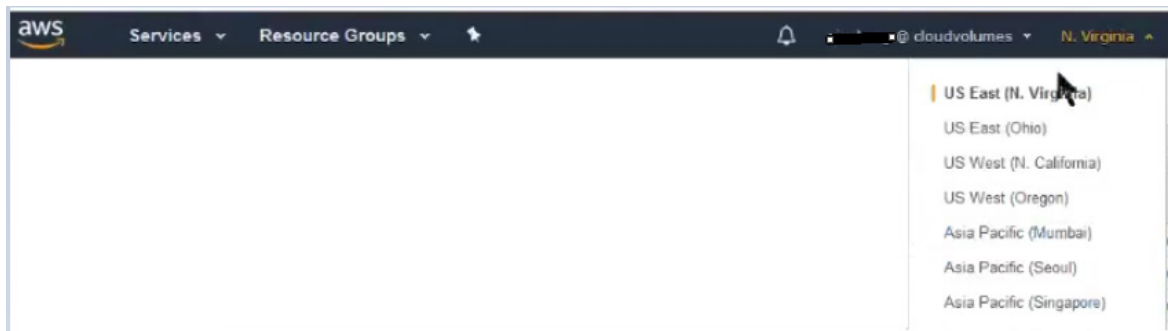
Note: You may want to open a text editor so you can capture the AWS network information that you will need to enter when creating your first cloud volume.

5.1 Create a VPC to use with Cloud Volumes (optional)

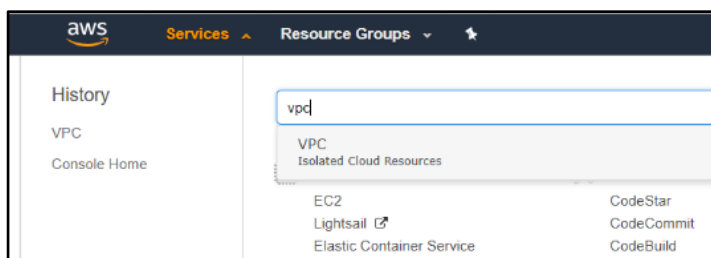
It is not mandatory that you create a new Amazon Virtual Private Cloud (VPC); however, you might need a new VPC to isolate instances associated with the Cloud Volumes project from work in other VPCs.

To create a VPC to use with Cloud Volumes you can use the VPC wizard, or you can follow the configuration steps shown below:

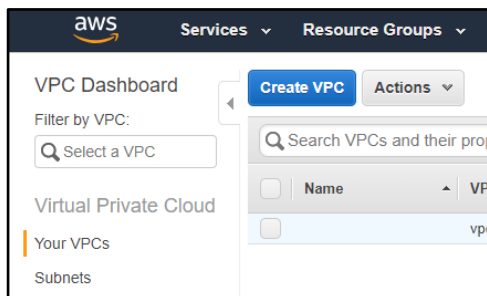
1. Log in to the AWS Management Console using your login credentials, and then select the AWS region in which you plan to deploy cloud volumes.



2. Click **Services** from the menu bar, type **vpc** in the search bar, and select **VPC (Isolated Cloud Resources)** to display the VPC dashboard.



3. Click **Your VPCs** on the navigation pane to the left. Then click **Create VPC** to display the Create VPC page.



4. On the Create VPC page, complete these tasks:
 - a. Enter a unique name to help you identify this VPC to use for Cloud Volumes.
 - b. Enter a private range Classless Inter-Domain Routing (CIDR) block that works for your environment. It doesn't matter what it is, you can select from any private class range. A /24 CIDR block is sufficient. In this example, the CIDR block name is 10.2.0.0/24. Check with your network administrator if you need assistance for selecting the CIDR range.

Note: The VPC CIDR range and the storage CIDR range, which you will enter when creating your first cloud volume, cannot overlap. Online CIDR/subnet calculators may be useful to show the IP range for your proposed CIDR and help determine if they overlap.

 - c. Do not change the default values in the IPv6 CIDR block or Tenancy fields.
 - d. Click **Yes, Create**. A new VPC is created.

Create VPC

A VPC is an isolated portion of the AWS cloud populated by AWS objects, such as Amazon EC2 instances. You must specify an IPv4 address range for your VPC. Specify the IPv4 address range as a Classless Inter-Domain Routing (CIDR) block; for example, 10.0.0.0/16. You cannot specify an IPv4 CIDR block larger than /16. You can optionally associate an Amazon-provided IPv6 CIDR block with the VPC.

Name tag

MyCloudVolumesVPC

IPv4 CIDR block*

10.2.0.0/24

IPv6 CIDR block*

☒ No IPv6 CIDR Block
 ☐ Amazon provided IPv6 CIDR block

Tenancy

Default

Cancel

Yes, Create

5. Click **Close** to close the window.

5.2 Create a Virtual Private Gateway and attach it to your VPC

The VGW is a network gateway that provides a route to NetApp Cloud Volumes.

To create a VGW and attach it to your VPC, complete the following steps:

1. On the VPC page of the AWS console, select **Virtual Private Gateways**.
2. At the top of the page, select **Create Virtual Private Gateway** and the Create Virtual Private Gateway page is displayed.

Virtual Private Gateways > Create Virtual Private Gateway

Create Virtual Private Gateway

A virtual private gateway is the router on the Amazon side of the VPN tunnel.

Name tag:

ASN: ☒ Amazon default ASN ☐ Custom ASN

[Cancel](#) [Create Virtual Private Gateway](#)

3. On the Create Virtual Private Gateway page, complete these tasks:
 - a. Provide an appropriate name tag for the VGW.
 - b. In the ASN field, NetApp recommends selecting **Amazon default ASN**, in which case your VGW will be assigned an ASN of **64512**. You can select the Custom ASN option and assign any valid private ASN.
 - c. Click **Create Virtual Private Gateway** and the VGW is created.

Virtual Private Gateways > Create Virtual Private Gateway

Create Virtual Private Gateway

✔ Create Virtual Private Gateway succeeded

Virtual Private Gateway ID: **vgw-e1e01688**

[Close](#)

4. Make a note of the VGW ID and click **Close**. The new VGW is displayed in the `detached` state.
5. Select the box next to the new Virtual Private Gateway and press **Actions** (above the table).

[Create Virtual Private Gateway](#) [Actions](#)

Filter by tags and attributes or search by keyword

	Name	Name	ID	State	Type
<input checked="" type="checkbox"/>	MyCloudVol...	MyCloudVol...	vgw-0d2c9f541415a885f	detached	ipsec.1

6. Click **Attach to VPC** and the Attach to VPC page is displayed.

7. Click in the VPC field and select the newly created VPC to attach to the VGW, and then click **Yes, Attach**.

You are returned to the Virtual Private Gateway page.

Note: You may have to wait several minutes for the VGW to transition from the **attaching** state to the **attached** state.

Use the **Refresh** button in the upper-right corner of the page to refresh the status.

5.3 Create a Subnet for the VPC

To create a subnet for the VPC, complete the following steps:

1. On the VPC dashboard, select **Subnets** from the navigation pane on the left. A list of existing subnets is displayed.
2. Click **Create Subnet** and the Create Subnet page is displayed.

3. On the Create Subnet page, complete these steps:
 - a. Enter an appropriate name tag for your environment.
 - b. Select the newly created VPC.
 - c. Unless you want to select a specific availability zone, leave the No Preference default value and the system will select the availability zone for you.
 - d. Unless you need to divide the VPC into multiple subnets, use the CIDR block for the entire VPC. In this example, the `10.2.0.0/24` CIDR block was used—it represents the entire VPC CIDR block.
 - e. Click **Yes, Create**. The new subnet will reside in the VPC you selected.

Note: This process can take a several minutes.

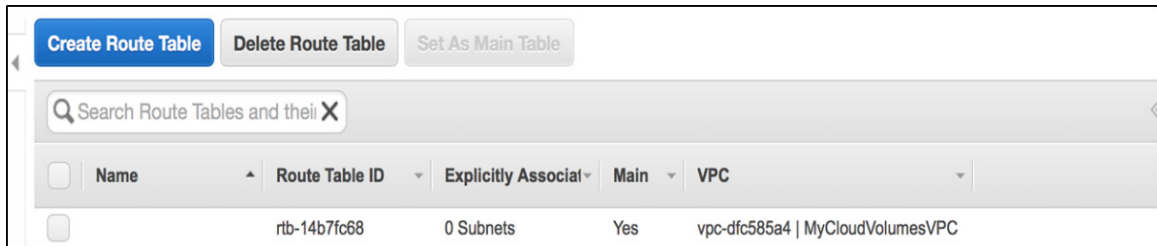
4. Click **Close** to close the window.

5.4 Set Up Routes

To set up routes, complete the following steps:

1. On the VPC dashboard, select **Route Tables** from the navigation pane on the left.

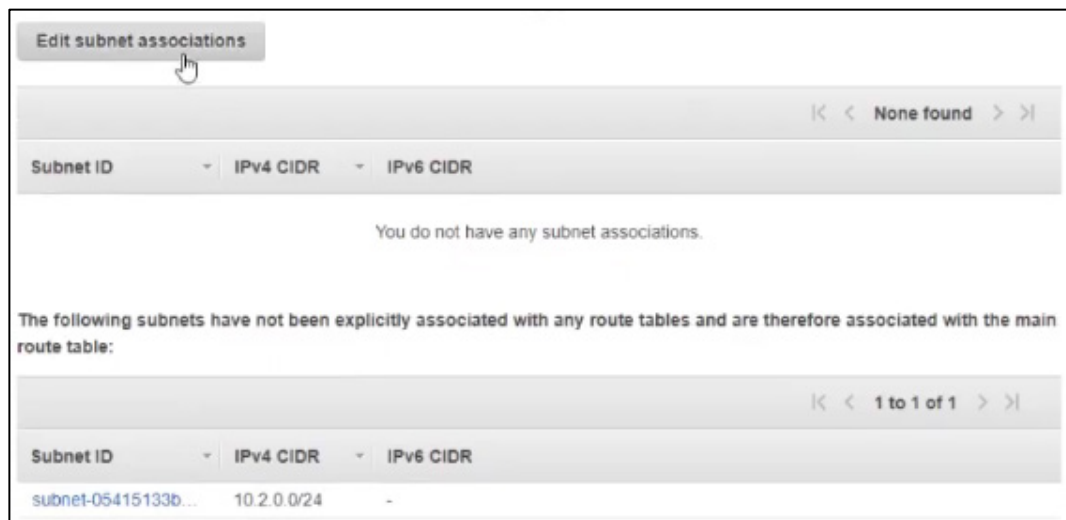
Note: A route table is automatically assigned as part of the VPC creation.



2. Select the route table that corresponds with the VPC you created, and the details are displayed at the bottom of the page.



3. Select the **Subnet Associations** tab.



4. Click the **Edit subnet associations** button to associate the newly created subnet with this route table and the Edit subnet associations page is displayed.

Edit subnet associations

Route table: rtb-0c8f8340e318fcab5

Associated subnets: No subnets selected

Subnet ID	IPv4 CIDR	IPv6 CIDR	Current Route Table
subnet-05415133b90024e79 Test_instr...	10.2.0.0/24	-	Main

* Required

Cancel Save

5. In the Edit subnet associations page, select the subnet and click **Save**.

Note: You can choose to configure a static route **or** to propagate the routes. **Do not** both propagate routes **and** create a static route. Check with your network administrator if you are not sure about the route configuration. See the AWS topic about [Route Tables](#) for details.

- Follow step 6 only to propagate routes.
- Follow step 7 only to configure a static route.

6. Select the **Route Propagation** tab to *propagate the routes*.

If you want to create a static route, go to step 7.

Route Table: rtb-0c8f8340e318fcab5

Summary Routes Subnet Associations **Route Propagation** Tags

Edit route propagation

Virtual Private Gateway	Propagate
vgw-0d483b62dcb97f1ef Test_instructions	No

- a. Click the **Edit route propagation** button to propagate the routes to the Virtual Private Gateway.

Edit route propagation

Route table: rtb-0c8f8340e318fcab5

Virtual Private Gateway	Propagate
vgw-0d483b62dcb97f1ef Test_instructions	<input type="checkbox"/>

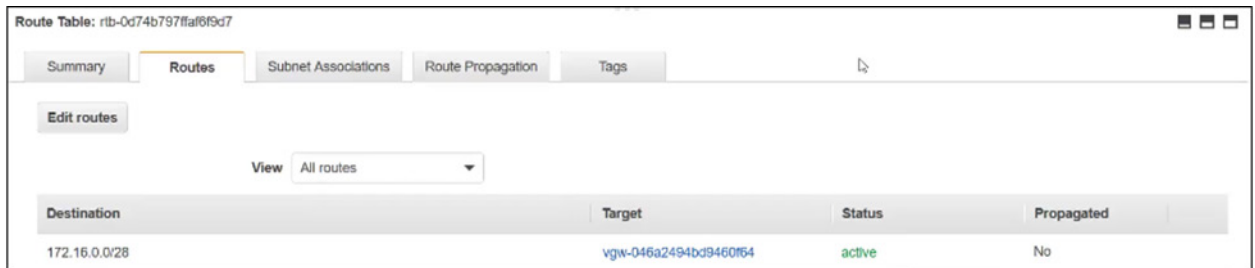
* Required

Cancel Save

- b. In the Edit route propagation page, check the Propagate box to the right of the VGW name, and then click **Save**.

7. Select the **Routes** tab to configure a *static route*.
If you want to propagate the routes, go back to step 6.
 - a. In the Routes tab, click **Edit routes**.
 - b. Enter the destination CIDR block for Destination and select a target for Target, then **Save** the configuration.
The CIDR block must be an IPv4 range for the region in the /28 range. This CIDR must only contain RFC 1918 (private) addresses.

Note: The VPC CIDR range and this storage CIDR range cannot overlap.

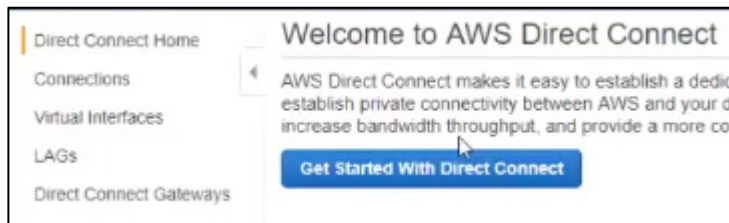


5.5 Create a Direct Connect Gateway and Associate it with the Virtual Private Gateway (optional)

If you have decided to use a Direct Connect Gateway (DCG) in your configuration, create the Direct Connect Gateway and associate it with the Virtual Private Gateway. See section 4.1 for an explanation why you may want to use a Direct Connect gateway.

If you do not plan to use a DCG, jump to section 5.6.

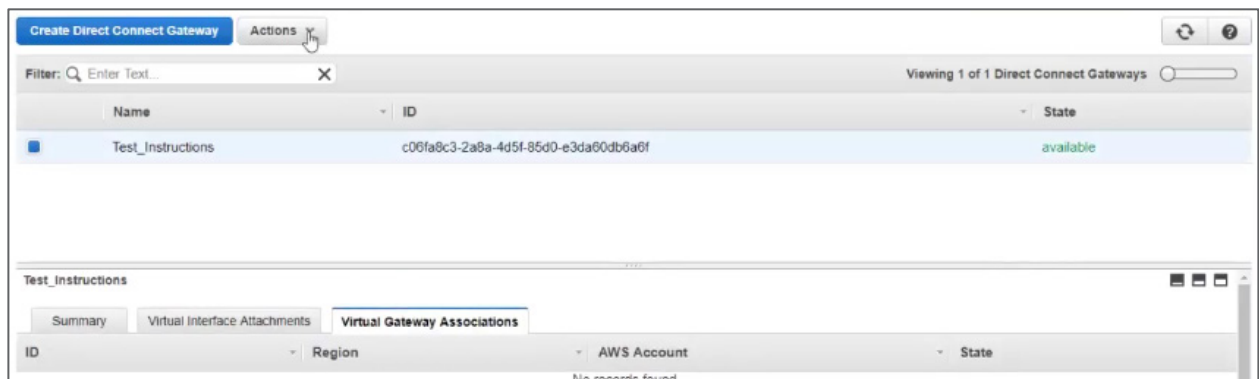
1. From the AWS console for your account, navigate to **Services** and type **direct connect** in the search bar. The Direct Connect Home page appears.



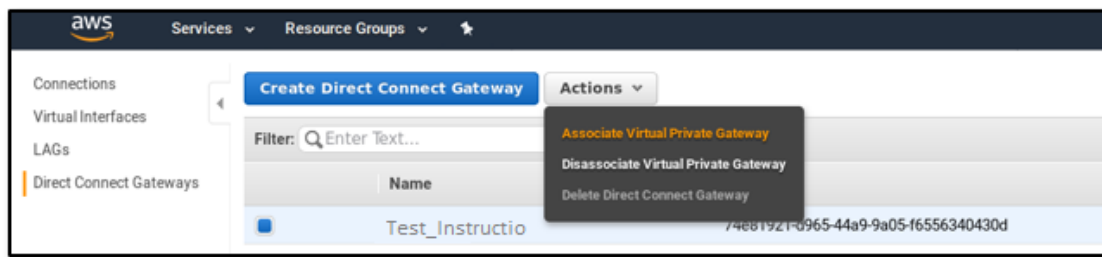
2. From the left navigation, click **Direct Connect Gateways**, then click the **Create Direct Connect Gateway** button from the next page, and the Create a Direct Connect Gateway page is displayed.

3. On the Create a Direct Connect Gateway page, complete these tasks:
 - a. Provide an appropriate name for the DCG.
 - b. In the ASN field, you can enter the same ASN as you used when creating your VGW or you can use a different ASN. Check with your networking team if you are not sure what number to use here.

- c. Click **Create** and the new DCG is displayed.



4. Select the Direct Connect Gateway and then click the **Actions** button.



5. Select **Associate Virtual Private Gateway** and the Associate Virtual Private Gateways page displays.
6. Select the Virtual Private Gateway and click **Associate**.



7. Click on the **Virtual Gateway Associations** tab in the lower pane to confirm the VGW is associated.



8. Wait until the gateway State transitions from the **associating** to **associated**. This can take several minutes.

5.6 Gather Required AWS Configuration Information

You are now ready to subscribe to NetApp Cloud Volumes in the AWS Marketplace. When subscribing, be prepared to provide the following information that you have collected during the previous steps:

Required Information	Your Value
12-digit Amazon account identifier with no dashes	
AWS region that you selected in section 5.1	
<p>Classless Inter-Domain Routing (CIDR) Block</p> <p>An unused IPv4 CIDR block for the cloud volumes. The network must be a /28, and it must fall within the ranges reserved for private networks (RFC 1918).</p> <p>The CIDR range must not overlap with existing CIDRs in your VPCs.</p> <p>Note: If connecting Cloud Volumes to on-premise clients the CIDR range also must not overlap existing on-premise CIDRs.</p> <p>If you configured a static route, use the CIDR block you entered there (section 5.4, step 7).</p>	

Test that the CIDR ranges do not overlap

A python3 script is available to check that the CIDR range you're planning to use does not overlap CIDRs in your AWS VPCs.

- [test-cidr.py](#)

Download the script to either a Linux EC2 instance or a Windows, Linux, or MAC client with python3 and the AWS boto3 python module installed. See the AWS instructions for boto3 [here](#).

The -h option provides help on how to use the command. The -k option enables you to pass your AWS credentials as arguments if your credentials are not configured on your client, or to check a different AWS account.

Command examples for checking the CIDR

To check that the CIDR 10.16.51.80/28 does not overlap existing CIDR ranges, run this command:

```
$ ./test-cidr.py -c 10.16.51.80/28  
For account: 695990169366  
Checking in each region if 10.16.51.80/28 overlaps existing CIDRs  
10.16.51.80/28 does not overlap existing CIDRs in your account
```

The output from this command shows that CIDR 10.16.51.80/28 can be used for the Cloud Volumes Service.

`$./test-cidr.py -c 172.32.0.0/28`
Please enter a private (RFC1918) CIDR

The IP spaces for private internets are, 10.0.0.0-10.255.255.255, 172.16.0.0-172.31.255.255 and 192.168.0.0-192.168.255.255

Please see <https://tools.ietf.org/html/rfc1918>

The output from this command shows that CIDR 172.32.0.0/28 is not a private CIDR and therefore it cannot be used for the Cloud Volumes Service.

`$./test-cidr.py -c 172.31.2.0/28 -k <AWS-access-key> <AWS-secret-key>`
For account: 695990169366
Checking in each region if 172.31.2.0/28 overlaps existing CIDRs
172.31.2.0/28 overlaps with 172.31.0.0/16 in region ap-northeast-1
172.31.2.0/28 overlaps with 172.31.0.0/16 in region us-east-1
172.31.2.0/28 overlaps in 2 existing VPCs

The output from this command shows that CIDR 172.31.2.0/28 overlaps with CIDRs in existing VPCs and therefore it cannot be used for the Cloud Volumes Service.

6 Enable AWS Subscription and Cloud Volumes Service

6.1 Access AWS Marketplace Listing for Cloud Volumes Service

Locate the **NetApp Cloud Volumes Service** listing on the AWS Marketplace.

Complete the following steps:

1. Go to the [AWS marketplace page](#) and sign in to your AWS account.
2. Type “NetApp Cloud Volumes Service” in the search bar to view these NetApp products.
3. Select the **NetApp Cloud Volumes for AWS** product.

Cloud Volumes for AWS

Sold by: **NetApp, Inc.**

NetApp Cloud Volumes for AWS - Monthly or annual, is a simple to consume file service that delivers advanced, enterprise-class management to your cloud applications

☆☆☆☆☆ (0)

Continue to Subscribe

Save to list

Overview Pricing Usage Support Reviews

Product Overview

BEFORE SUBSCRIBING PLEASE READ THIS DOCUMENT
https://docs.netapp.com/us-en/cloud_volumes/aws/media/cvs_aws_account_setup.pdf

NetApp Cloud Volumes for AWS available in a monthly or annual subscription is simple to consume file service that delivers advanced, enterprise-class management to your cloud applications, so your technology stack becomes rocket fuel for innovation. You can subscribe starting at 1TB, or any TB quantity you desire. And, you can add capacity at any time during your contract. You crave screaming fast, file-storage performance, and you deserve it as a service. The subscription is available in 3 performance levels, standard, premium and extreme. You can now migrate any workload to the public cloud and run it there without sacrifice. Cloud Volumes allows the majority of file-based applications to be moved to the cloud by giving you NFSv3 support. Plus, you can now schedule snapshots of your Cloud Volumes, restore them, create clones and then migrate or continuously keep your datasets in sync. You get persistent storage for your cloud-native environments or lift-and-shift your enterprise applications, without adding complexity. Use Cloud Volumes to keep you productive across your file services-based workloads, such as analytics, DevOps, and disaster recovery.

Highlights

- READ ME FIRST - SELF ONBOARD INSTRUCTIONS
https://docs.netapp.com/us-en/cloud_volumes/aws/media/cvs_aws_account_setup.pdf
- Self Onboarding Video instructions -
<http://tv.netapp.com/detail/video/5985394922001>
- This service is available in the following regions -
<https://cloud.netapp.com/cloud-volumes-global-regions>

4. Review the content on this page to fully understand the solutions the product provides, and the cost based on the capacity and the service level that you select.
5. Click on the READ ME FIRST document link and the Self Onboarding Video link to identify the prerequisites tasks you must perform before creating your first cloud volume.
6. Click **Continue to Subscribe**.
7. In the Configure your Software Contract page:
 - a. Select the contract duration: 1 month or 12 months.
 - b. Select whether you want the contract to automatically renew at the end of the duration period.
 - c. In the Contract Options area, specify the capacity (in TB) and the service level (Standard, Premium, or Extreme) that you plan to use for your cloud volumes.

See the [description of available service levels](#) for details.

Configure your Software Contract

Choose the contract that suits your needs. You're charged for your purchase on your AWS bill. After you purchase a contract, you're directed to the vendor's site to complete setup and begin using this software. For any software use beyond your contract limit, you're charged consumption pricing.

Contract Duration

☒ 1 month

☐ 12 months

Renewal Settings

Auto Renew when this contract ends on - Mon Feb 04 2019?

☒ Yes

☐ No

I understand that when I renew, the seller's pricing terms and end user license agreement (EULA) might have changed. On the renewal date, I will be billed based on the price and EULA applicable on that date, which I can find on the Your Marketplace Software page.

Create Contract

By subscribing to this software, you agree to the pricing terms and the seller's [end user license agreement \(EULA\)](#). Your use of AWS services is subject to the [AWS Customer Agreement](#).

Total Contract Price

\$0

Due Today
Auto Renew - Yes

Select contract Option(s)

Contract Options

1TB_Standard Tier

\$100/TB

1TB or 1TB increment, Standard Performance Tier

1TB_Premium Tier

\$200/TB

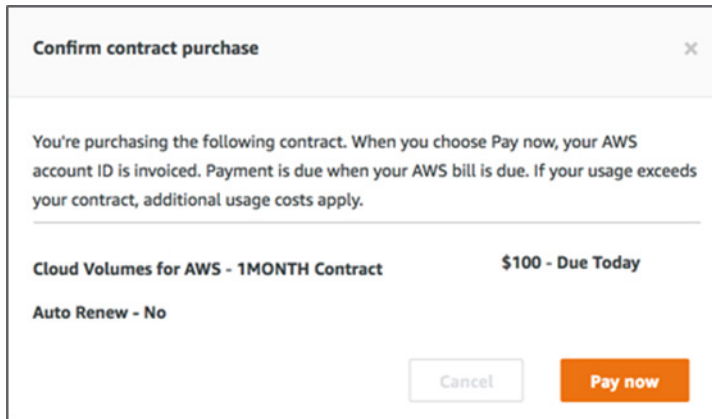
1TB or 1TB increment, Premium Performance Tier

1TB_Extreme Tier

\$300/TB

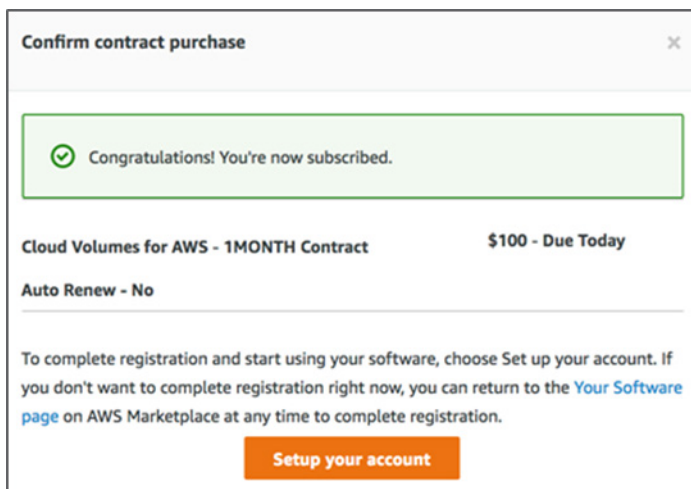
1TB or 1TB increment, Extreme Performance Tier

- After you have specified all the details for the cloud volumes you plan to create, click **Create Contract**.
- The Confirm contract purchase window displays. If all is OK, click **Pay now**.



10. When the congratulations message is displayed, click **Setup your account**.

Note: Ensure you turn off any ad blocker or pop-up blocker on your browser before you select **Setup your account**.



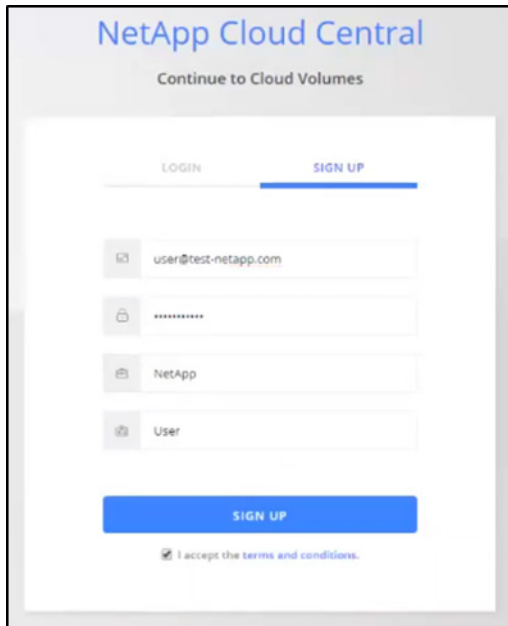
11. You will be redirected to the NetApp Cloud Central page. Complete the steps in the next section to register and log into NetApp Cloud Central.

6.2 Register and Log into NetApp Cloud Central

You may already have a NetApp Cloud Central account. If you do, and this is the account you want to use for CVS, select the "LOGIN" tab and enter your existing User ID and Password.

If this is your first time registering with NetApp Cloud Central, or if you wish to set up an additional account, you will need to register a new account. Select the "SIGN UP" tab.

1. Enter a valid email address.
2. Enter a Password.
3. Enter your company name.
4. Enter your full name.
5. Check the box to accept the terms and conditions and then click **Sign Up**.



NetApp Cloud Central

Continue to Cloud Volumes

LOGIN SIGN UP

user@test-netapp.com

NetApp

User

SIGN UP

☒ I accept the terms and conditions.

You have completed the initial process for accessing Cloud Volumes Service for AWS. The Cloud Volumes user interface is displayed.

6.3 Create Your First Cloud Volume

Create your first cloud volume using the Cloud Volumes user interface. You can create an NFS, SMB, or Dual-protocol volume.

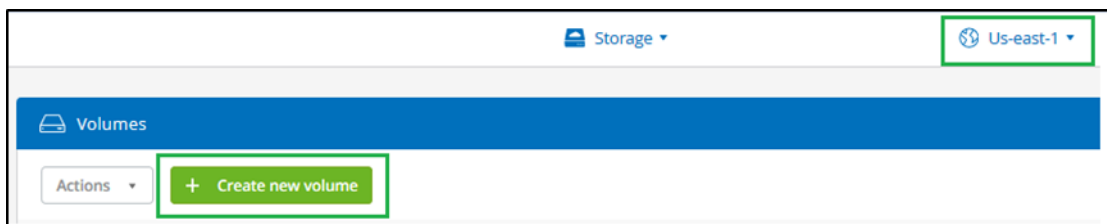
Note: When planning to create an SMB volume, you must have an existing Windows Active Directory server available to which you can connect. You must have the details of this server available so you can enter it when creating the volume.

It is recommended that you [activate your NetApp support entitlement](#) so that you can access technical support in case you run into any issues.

The steps below show how to populate the required fields to create a cloud volume. For information about the other optional sections and fields of the Create Volume page, go to the [Creating a cloud volume topic](#) in the NetApp Cloud Volumes Service for AWS documentation.

1. Select the same AWS region that you used on AWS from the top of the Cloud Volumes user interface. See [Regions and Availability Zones](#) for a mapping of the AWS region names to Cloud Volumes region names.

If you need to change the region you will be prompted to log into NetApp Cloud Central again. Again, make sure no pop-up blocker is enabled on your browser or the second login could fail.



Storage ▾ Us-east-1 ▾

Volumes

Actions ▾ + Create new volume

2. Click the **Create new volume** button.
3. In the top of the Create Volume page, select **NFS**, **SMB**, or **Dual-protocol**.

4. Complete the following fields to define the volume name, size, service level, and more:

Field	Description
Name	The volume name
Region	The AWS region where you want to create the volume
Volume path	Specify the unique path you want to use, or accept the automatically generated path
Service level	Select Standard, Premium, or Extreme. See the description of available service levels for details
Allocated capacity	Set the initial size of the volume. See the description of allocated capacity for details
NFS version	Select NFSv3 , NFSv4.1 , or Both depending on your requirements
Security style	If you selected Dual-protocol, you can select NTFS or UNIX
Show snapshot directory	Choose whether you want the .snapshot directory (previous Snapshot versions in Windows) to be hidden or shown

The screenshot shows the configuration interface for a NetApp Cloud Volume, specifically for the NFS protocol. At the top, there are three tabs: 'NFS' (selected), 'SMB', and 'Dual-protocol'. Below the tabs, the configuration is organized into several sections:

- Name:** A text input field.
- Region Required:** A dropdown menu showing 'us-east-1'.
- Timezone:** A dropdown menu showing 'Any'.
- Volume path Required:** A text input field containing 'hip-elated-lewin' with a refresh icon.
- Service level Required:** A dropdown menu showing 'Standard'.
- Allocated capacity:** A text input field showing '1000' and a unit dropdown set to 'GB'.
- NFS version:** A dropdown menu showing 'NFSv3'.
- Security style:** A dropdown menu showing 'UNIX'.
- Show snapshot directory (read-only):** A checkbox that is checked.

5. If you selected SMB or Dual-protocol, you can enable SMB session encryption by checking the box for the **Enable SMB3 Protocol Encryption** field.
6. In the Network section, complete the following fields using the data you collected in section 5.6 to connect your Cloud Volumes account to your AWS account:

Field	Description
CIDR (IPv4)	Enter the desired IPv4 range for the region. The network must be a /28, and it must fall within the ranges reserved for private networks (RFC 1918). The CIDR range must not overlap with existing VPCs.
AWS account ID	Enter your 12-digit Amazon account identifier with no dashes

Network

! 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 /28 prefix that does not overlap with your existing networks. Also, ensure that the ASN you enter matches the ASN of the Direct Connect Gateway or Virtual Private Gateway to which the Virtual Interfaces will be attached. See the [Cloud Volumes Service for AWS Account Setup document](#) for details.

CIDR (IPv4) Required

172.30.0.0/28



AWS account ID Required

123456789012

- In the Export policy section, complete the following fields if you want to restrict the clients that can access the volume:

Field	Description
Allowed clients	Specify the allowed clients by using an IP address or Classless Inter-Domain Routing (CIDR)
Access	Select Read & Write or Read only
Protocol	Select the protocol or protocols that you want to use

Export policy

+ Add export policy rule

Rule index	Allowed clients <small>Required</small>	Access	Protocol/s
Rule-1	0.0.0.0/0	<input checked="" type="button" value="Read & Write"/> <input type="button" value="Read only"/>	<input checked="" type="button" value="NFSv3"/> <input type="button" value="NFSv4.1"/>



i "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.

- If you selected SMB or Dual-protocol, you can integrate the volume with an existing Windows Active Directory server by completing the fields in the Active directory section:

Field	Description
DNS server	Enter the IP address of the DNS server that you want to use
Domain	Enter the domain for the SMB share.
NetBIOS	Enter a NetBIOS name for the SMB server that will be created.
Organizational unit	Enter "CN=Computers" for connections to your own Windows Active Directory server. Enter "OU=<NetBIOS_name>" when using an AWS Managed Microsoft AD.
Username	Enter a username for your Active Directory server.
Password	Enter the password for the AD username that you specified in Username.

☐ Enable data encryption

Active directory ▼

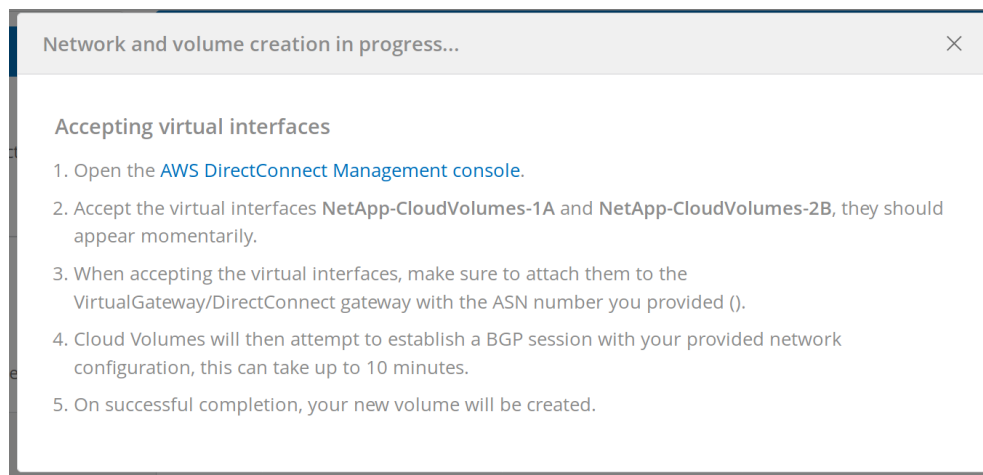
Available settings  \\cloudvol.NGS-AWS.io ▼	DNS server Required 10.252.135.15	Domain Required NGS-AWS.local
NetBIOS Required cloudvol	Username Required administrator	Password Required 

Note: 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.

9. In the Snapshot policy section, create a snapshot policy for this volume if required.

You can create a snapshot policy after you have created the volume, so this step is not required at this time.

10. Click the **Create Volume** button and a dialog prompts you 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.



Note: You must accept the interfaces within 10 minutes after clicking the Create 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.

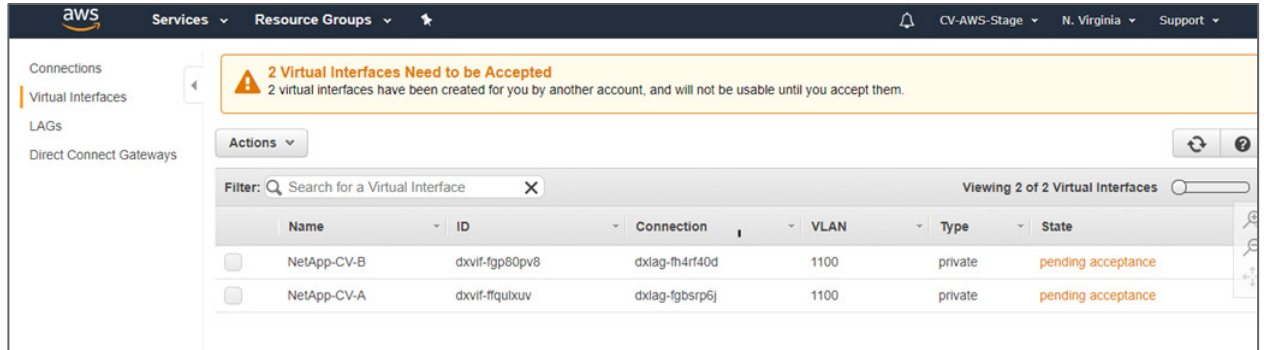
6.4 Accept the Direct Connect Virtual Interfaces

NetApp provides virtual interfaces for connectivity to the Cloud Volumes Service. These virtual interfaces must be accepted before they can be used.

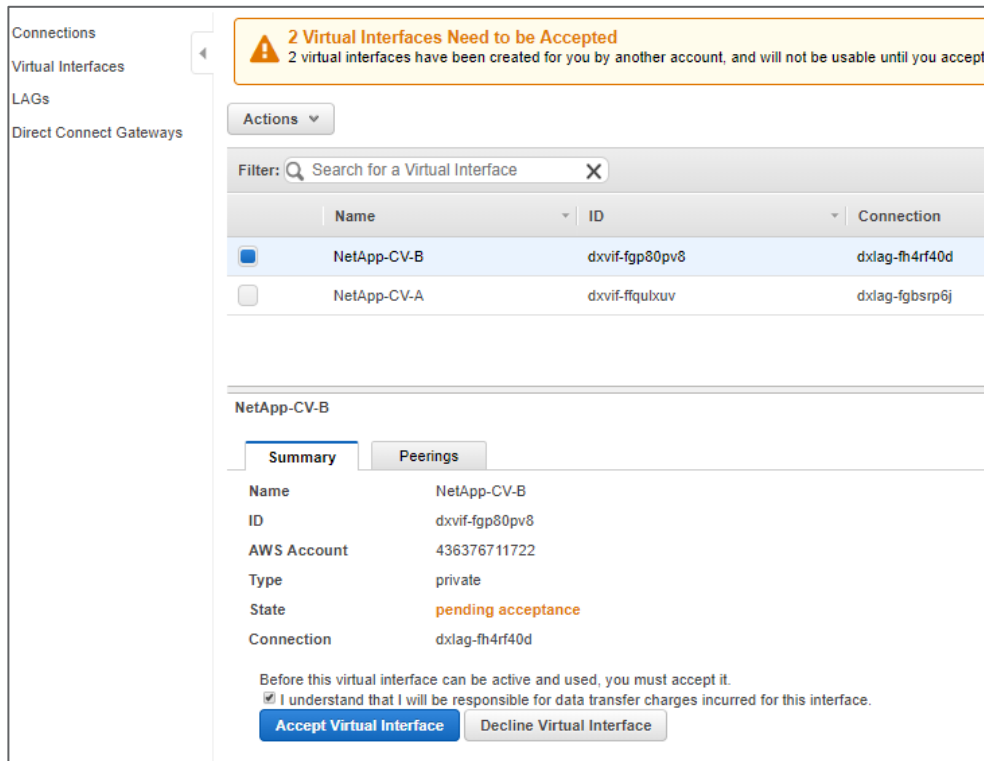
If the interfaces do not appear within 10 minutes there may be a configuration issue; in which case you should contact support.

To accept the virtual interfaces, complete the following steps:

1. From the AWS console for your account, navigate to the Direct Connect service and click **Virtual Interfaces**.



2. Select one of the virtual interfaces, and in the Summary tab, check the box that you understand how you will be charged for this service, and click **Accept Virtual Interface**.



3. From the Accept Virtual Interface dialog, select whether you will connect the interfaces to the **Virtual Private Gateway** or **Direct Connect Gateway**, choose the gateway from the drop-down menu, and click **Accept**.

Note: If you created a Direct Connect Gateway, select **Direct Connect Gateway**.



4. Repeat steps 1 through 3 for each interface.
5. After the **pending** state, the state of the virtual interface initially goes to **down**, changes to **up**, and finally to **available**.

Note: It can take up to 10 minutes before the virtual interfaces become available.

6. Verify that the virtual interfaces are **available**.

Connections	Actions	Filter: Search for a Virtual Interface					Viewing 2 of 2 Virtual Interfaces
Virtual Interfaces		Name	ID	Connection	VLAN	Type	State
LAGs		NetAppCVS-PM-B	dxvif-ffm4ubqv	dxlag-fguxo1ms	1022	private	available
Direct Connect Gateways		NetAppCVS-PM-A	dxvif-fgbqfox3	dxlag-fg51xgdt	1022	private	available

7. After the interfaces become **available**, return to the Cloud Volumes Service user interface and verify that the new volume appears in the Volumes page and that the volume is listed as **Available**.

Note: It can take an additional 5 to 10 minutes for routes to be distributed through the AWS network before the volume status changes from **Creating** to **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

8. Refer to the steps in the topic [Mounting a cloud volume](#) to mount the volume to your AWS instance that is in the same VPC.

7 Manage Cloud Volumes

To manage your volume, or to create additional cloud volumes, follow the instructions on [NetApp Cloud Volumes Service for AWS Documentation](#). For example, you can create a cloud volume, mount the volume, create a NetApp Snapshot™ copy of the volume, and more.

8 Sharing Cloud Volumes Service between AWS accounts (optional)

The Cloud Volumes Service can be shared between AWS accounts that are in the same organization using the AWS Resource Access Manager.

1. To enable sharing, log in to the AWS console for the account with Cloud Volumes Service and select the Organizations service.
2. If not already configured, add a master account and additional accounts to the organization that the Cloud Volumes Service will be shared between.
3. In the AWS console select the **Resource Access Manager** service.

Create resource share

Create a resource share to provide AWS accounts, organizational units, or organizations with access to resources

Description

Name
Provide a descriptive name for the resource share

Share Cloud Volumes Service

Resources - optional
Choose the resources to add to the resource share

Select resource type

Subnets

Filter by attributes or search by keyword

<input checked="" type="checkbox"/>	ID	Name	VPC ID	Availability zone	Availability zone ID	IPv4 CIDR
<input checked="" type="checkbox"/>	subnet-0b83d9e148458ce74	vpc2-sub-a	vpc-05abd00011fd61ef9	us-west-1a	usw1-az1	172.32.2.0/24
<input checked="" type="checkbox"/>	subnet-0654581380bc92f56	vpc-sub2-c	vpc-05abd00011fd61ef9	us-west-1c	usw1-az3	172.32.3.0/24

Selected resources

subnet-0b83d9e148458ce74 X subnet-0654581380bc92f56 X

4. Click on **Create resource share**, provide a name, and select “Subnets” as the resource type.
5. Select the subnets to be shared, meaning those with routes to Cloud Volumes Service.
6. Select the “Principals” (AWS accounts) to share the resources with and deselect the “Allow external accounts” option, as subnets cannot currently be shared outside of an organization.
7. Click **Create Resource Share**, and within a few minutes the subnets will be shared to the additional accounts, as will access to the Cloud Volumes Service.
8. Log in to an account that now shares the subnets and go to the VPC page.
9. Notice that a VPC has been added from the master account, as have the shared subnets, to the Cloud Volumes Service.

Subnet ID subnet-0654581380bc92f56
VPC vpc-05abd00011fd61ef9
Available IPv4 Addresses 251
Availability Zone us-west-1b (usw1-az3)
Network ACL acl-0ca2594738a5234e0
Auto-assign public IPv4 address Yes
Owner 695990169366 (shared)

To learn more about sharing the Cloud Volumes Service watch this [video](#).

Support

For any questions about this document, about the initial AWS setup, or about the setup of your initial cloud volume, it is recommended that you send email to cvs-support@netapp.com. Please provide a clear description of the question or problem you are experiencing. A NetApp engineer will assist and arrange a web conference as required.

Once you have successfully completed the steps in this document and provisioned your first volume, it is highly recommended that you perform the actions described in the topic [Activating support entitlement and accessing support](#) in order to further receive technical support for issues that may occur with future activities.

Where to Find Additional Information

To learn more about the information that is described in this document, review the following documents and/or websites:

- [NetApp Cloud Volumes product page](#)
- [NetApp Cloud Volumes Service for AWS documentation](#)
- [NetApp Cloud Documentation](#)

Version History

Version	Date	Document Version History
1.0	December 10, 2018	Initial release for self-subscription
1.0.1	December 19	Update routing and Support content
1.0.2	January 10, 2019	Update AWS Marketplace section and add note about ASN restriction
1.0.3	March 06	Add ability to use AWS Managed Microsoft AD
1.0.4	March 29	Add that Virtual Private Gateway enables connection to Cloud Volumes from on-premise clients
1.0.5	April 26	Add link to scripts to verify CIDR and ASN
1.0.6	July 05	Update Python scripts to check CIDR and ASN. Add section on sharing CVS between AWS accounts
1.0.7	July 18	Add note about Direct Connect Gateway usage
1.0.8	Aug 15	Remove steps to check ASN as this is now automatic. Also improve guidance for on-premise connectivity to Cloud Volumes
1.0.9	Dec 13	Add content about selecting NFSv4.1 protocol and show/hide Snapshot directory

Copyright Information

Copyright © 2019 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.

Data contained herein pertains to a commercial item (as defined in FAR 2.101) and is proprietary to NetApp, Inc. The U.S. Government has a non-exclusive, non-transferrable, non-sublicensable, 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).

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.