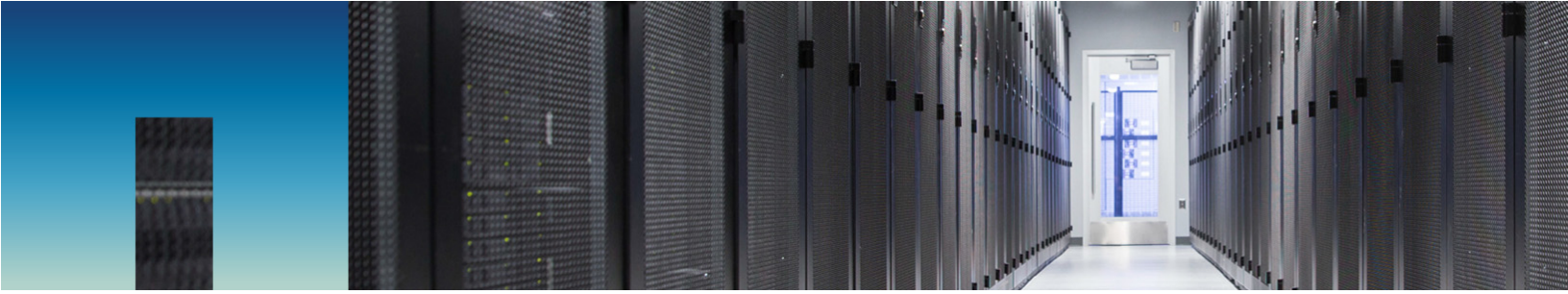


NetApp Cloud Volumes Service for AWS

AWS Account Setup

Cloud Volumes Team, NetApp, Inc.
July 18, 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).

NetApp®

TABLE OF CONTENTS

LIST OF FIGURES

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.

3.4 Current Restrictions

The Cloud Volumes Service currently supports only a private Autonomous System Number (ASN) from 64512 to 65535. You can select the Amazon default ASN (recommended) during these setup steps, in which case your Virtual Private Gateway and/or Direct Connect Gateway will be assigned an ASN of 64512.

If you need to use an ASN outside of this range, or if you already have a VGW or DCG that uses a number outside this range, you will need to open a support ticket via the email cvs-support@netapp.com before you set up your AWS networking requirements.

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.

Virtual Private Gateways also enable customers to connect to Cloud Volumes from on-premise clients when using the same Virtual Private Gateway for AWS Direct Connections to their premise and to connect Cloud Volumes.

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:

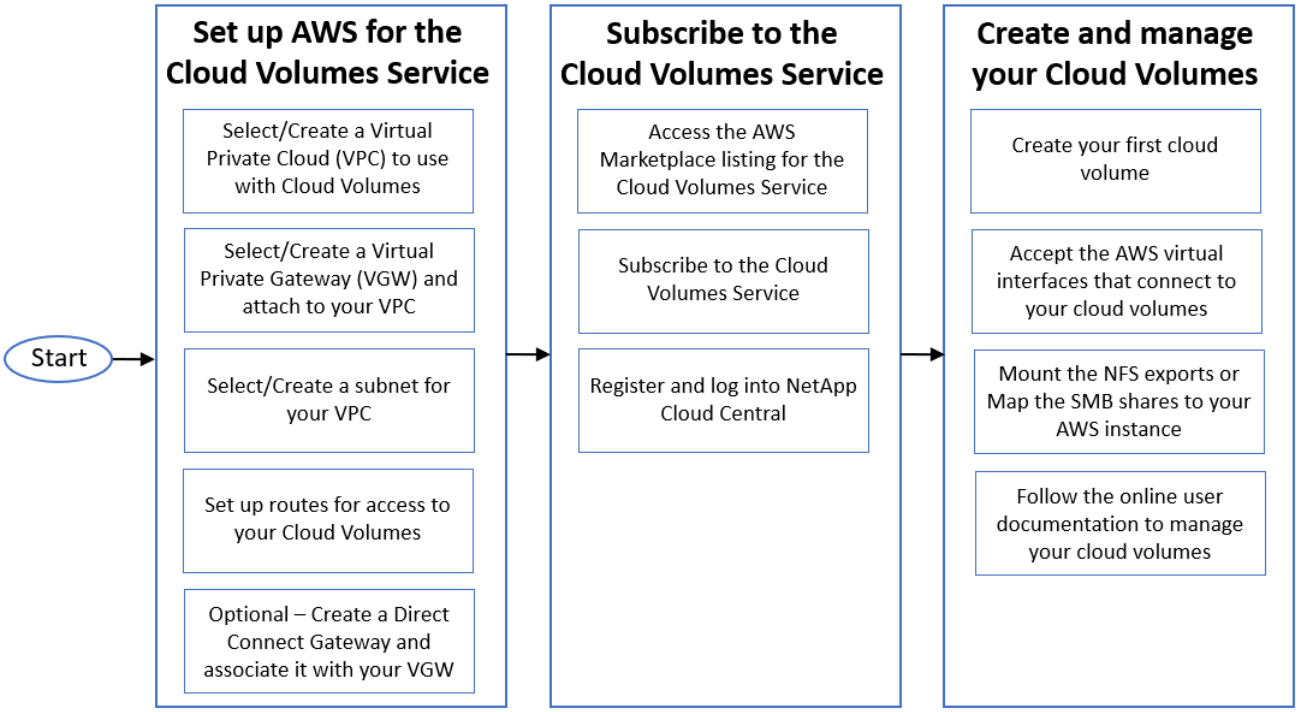
- Direct Connect Gateways allow multiple VPCs to be added, however the CIDR ranges of the VPCs cannot overlap as the gateway effectively creates a single network. If you require VPCs that have the same CIDR range, then connect Virtual Private Gateways directly to your cloud volume Virtual Interfaces.
- 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

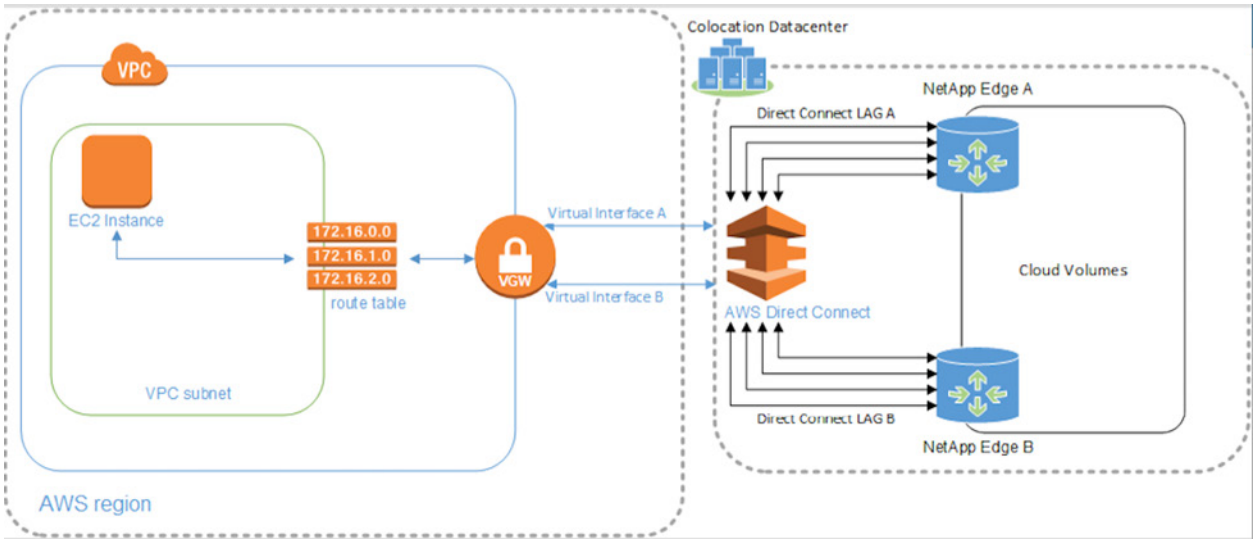
Before you subscribe to NetApp Cloud Volumes Service for AWS, you must create, or verify that your AWS account is correctly configured, with the following components:

- 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.

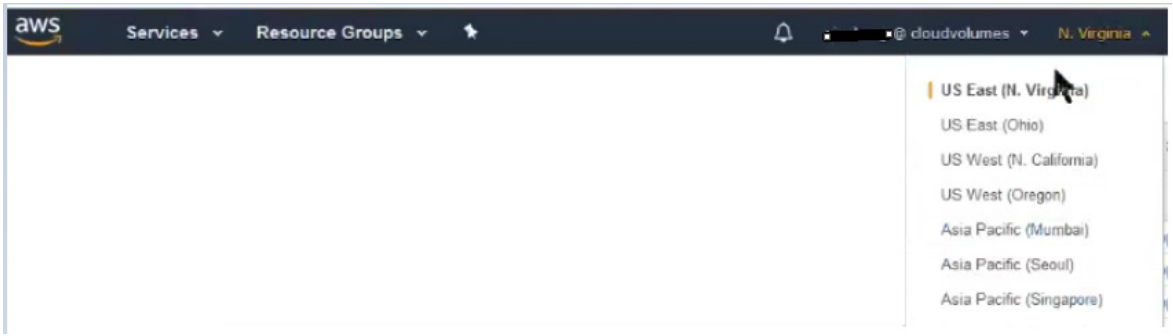
Note: You may want to open a text editor so you can capture the AWS network information that you will need to enter when creating your first cloud volume.

5.1 Create a VPC to use with Cloud Volumes

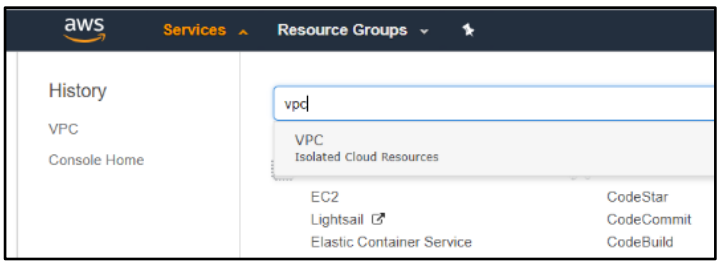
It is not mandatory that you create a new Amazon Virtual Private Cloud (VPC); however, you might need a new VPC to isolate instances associated with the Cloud Volumes project from work in other VPCs.

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

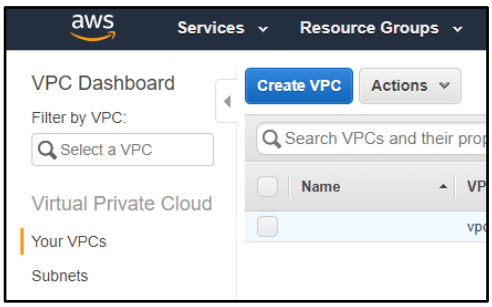
1. Log in to the AWS Management Console using your login credentials, and then select the AWS region in which you plan to deploy cloud volumes.



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



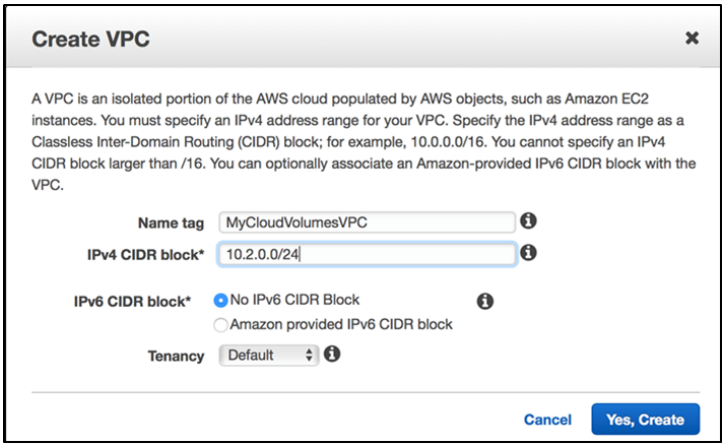
3. Click **Your VPCs** on the navigation pane to the left. Then click **Create VPC** to display the Create VPC page.



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.



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.

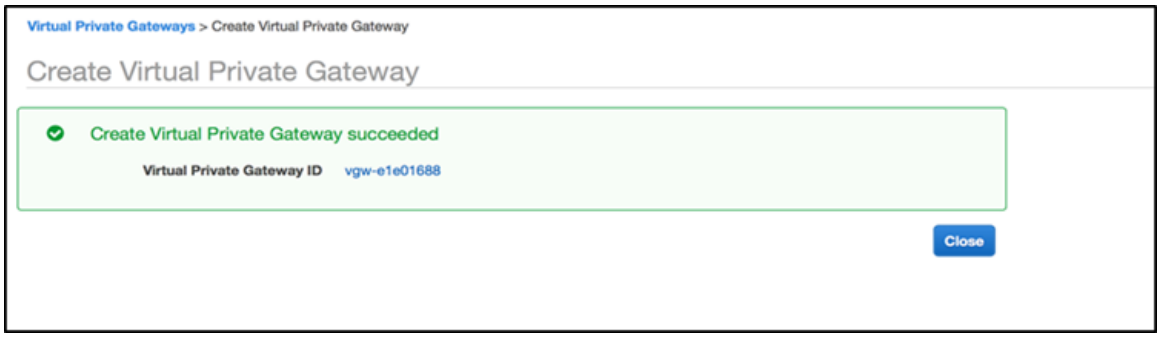
To create a VGW and attach it to your VPC, complete the following steps:

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.

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. See section 3.4 for current restrictions.

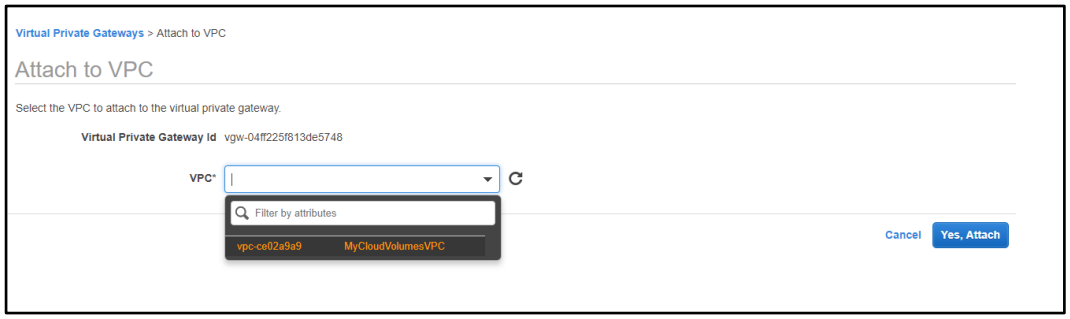
      Note: Make a note of the ASN as you will need to enter this information when setting up your first cloud volume in an AWS region.

   c. Click **Create Virtual Private Gateway** and the VGW is created.



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).

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.

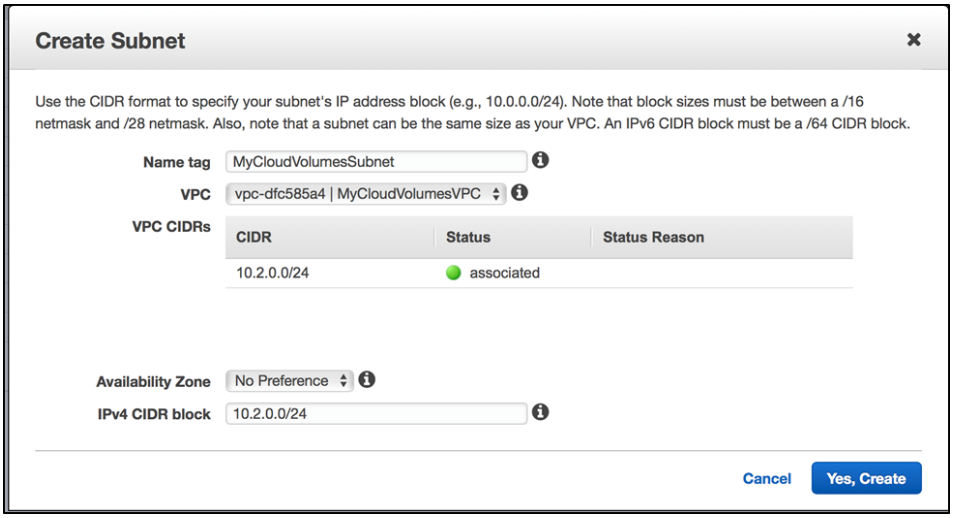
   Note: You may have to wait several minutes for the VGW to transition from the `attaching` state to the `attached` state.

   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.

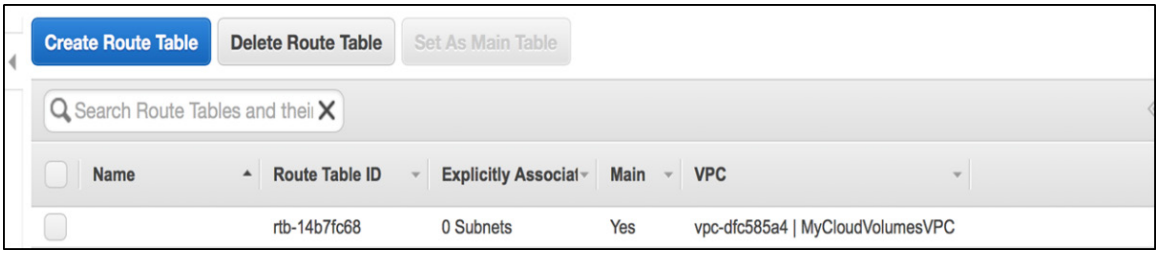
4. Click **Close** to close the window.

5.4 Set Up Routes

To set up routes, complete the following steps:

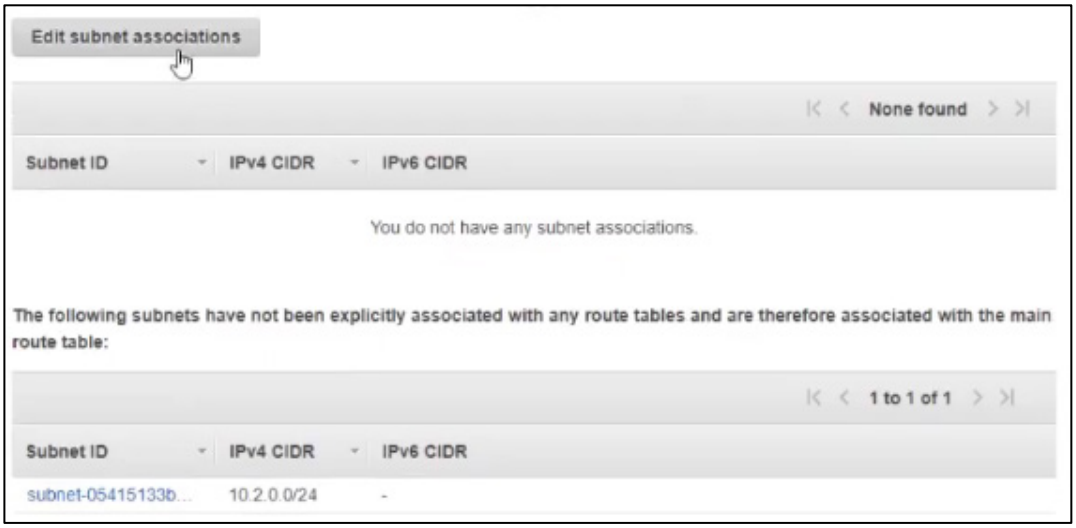
1. On the VPC dashboard, select **Route Tables** from the navigation pane on the left.

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

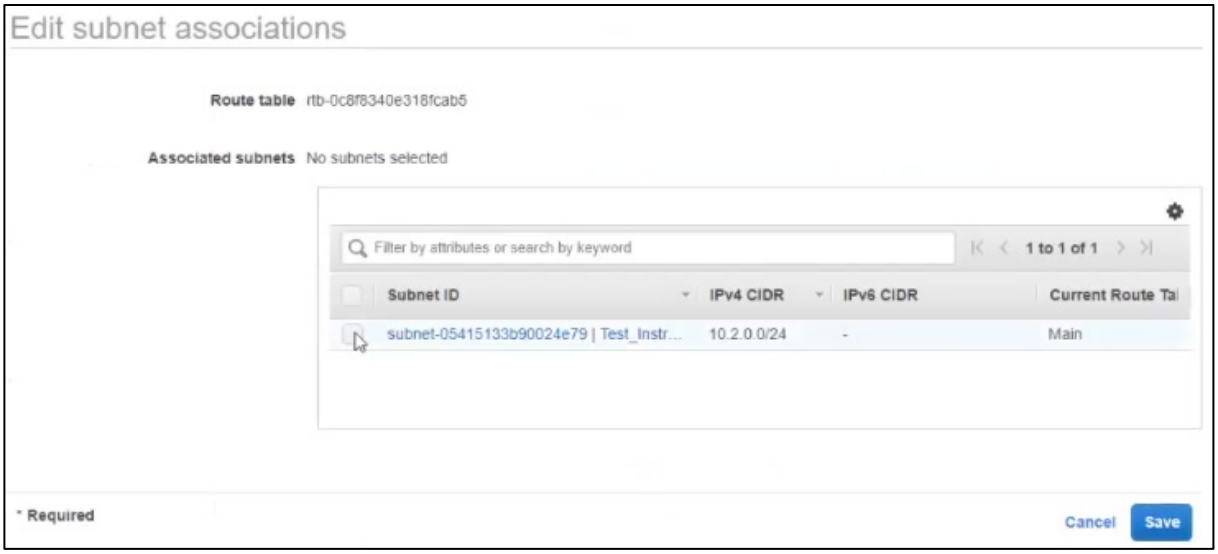


2. Select the route table that corresponds with the VPC you created, and the details are displayed at the bottom of the page.

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.



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** 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.

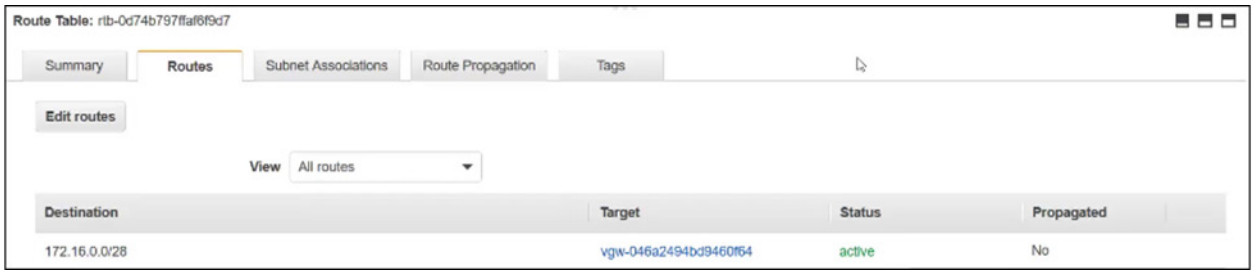
   a. Click the **Edit route propagation** button to propagate the routes to the Virtual Private Gateway.

   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, and **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.

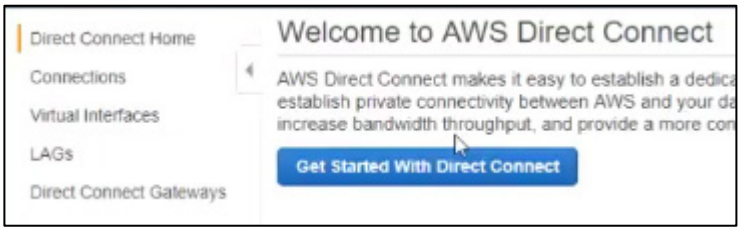


5.5 Create a Direct Connect Gateway and Associate it with the Virtual Private Gateway (Optional)

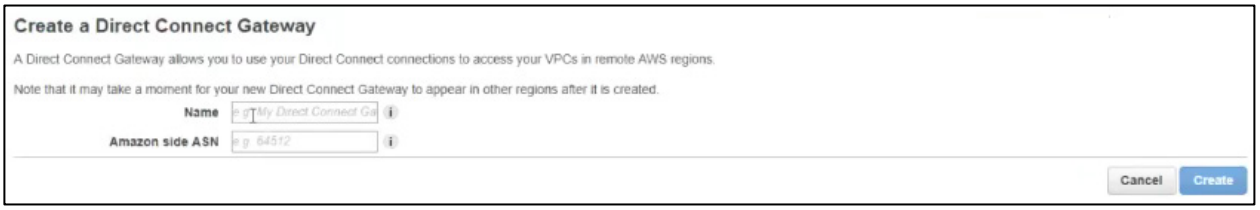
If you have decided to use a Direct Connect Gateway (DCG) in your configuration, create the Direct Connect Gateway and associate it with the Virtual Private Gateway. See section 4.1 for an explanation why you may want to use a Direct Connect gateway.

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.



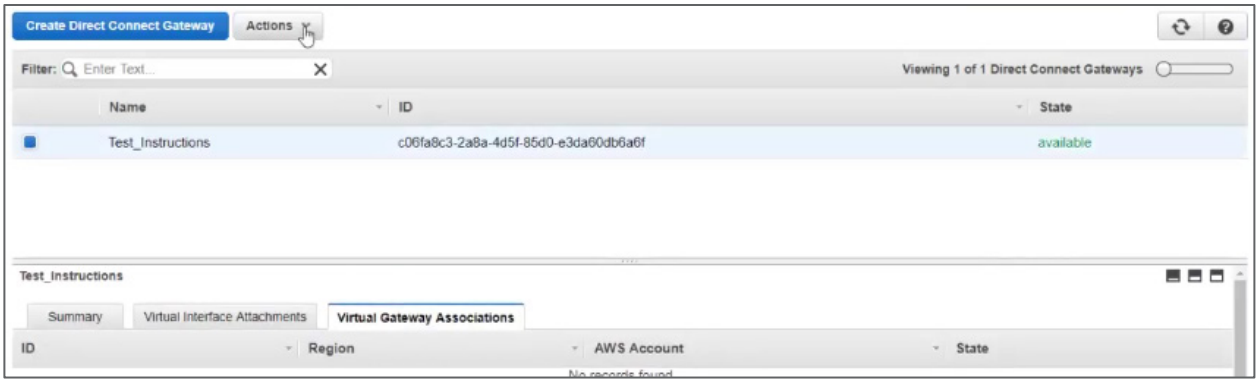
2. From the left navigation, click **Direct Connect Gateways**, then click the **Create Direct Connect Gateway** button from the next page, and the Create a Direct Connect Gateway page is displayed.



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. See section 3.4 for current restrictions.

Note: Make a note of the ASN as you will need to enter this information when setting up your first cloud volume in an AWS region.

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	
Classless Inter-Domain Routing (CIDR) Block An unused IPv4 CIDR block for the cloud volume. 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 CIDRs. If you configured a static route, use the CIDR block you entered there (section 5.4, step 7).	
Autonomous System Number (ASN) When using a Virtual Private Gateway only, use that ASN. When using a Direct Connect Gateway, use that ASN.	

Python3 scripts are available to help check that the CIDR range you're planning to use does not overlap CIDRs in your VPCs, and that the ASN matches at least one gateway in your AWS account.

- test-cidr.py
- test-asn.py

Download the scripts 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 commands. 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.

Command examples for checking the ASN

*$ **./test-asn.py -a 64512 -k <AWS-access-key> <AWS-secret-key>***
For account: 695990169366
Checking for gateways that match ASN 64512
Virtual private gateway(s) with ASN of 64512 in region(s) ['eu-west-2', 'eu-west-1', 'ap-northeast-1', 'ap-southeast-2', 'eu-central-1', 'us-east-1', 'us-west-1', 'us-west-2']
Direct connect gateway found with ASN of 64512

The output from this command shows that ASN 64512 matches a Virtual Private Gateway and a Direct Connect Gateway, so the Cloud Volumes Service can be connected to either gateway using this ASN.

*$ **./test-asn.py -a 64511***
For account: 695990169366
Checking for gateways that match ASN 64511
No virtual private gateways found with ASN of 64511
No direct connect gateways found with ASN of 64511

The output from this command shows that ASN 64511 does not match a gateway, so the Cloud Volumes Service cannot be connected using this ASN.

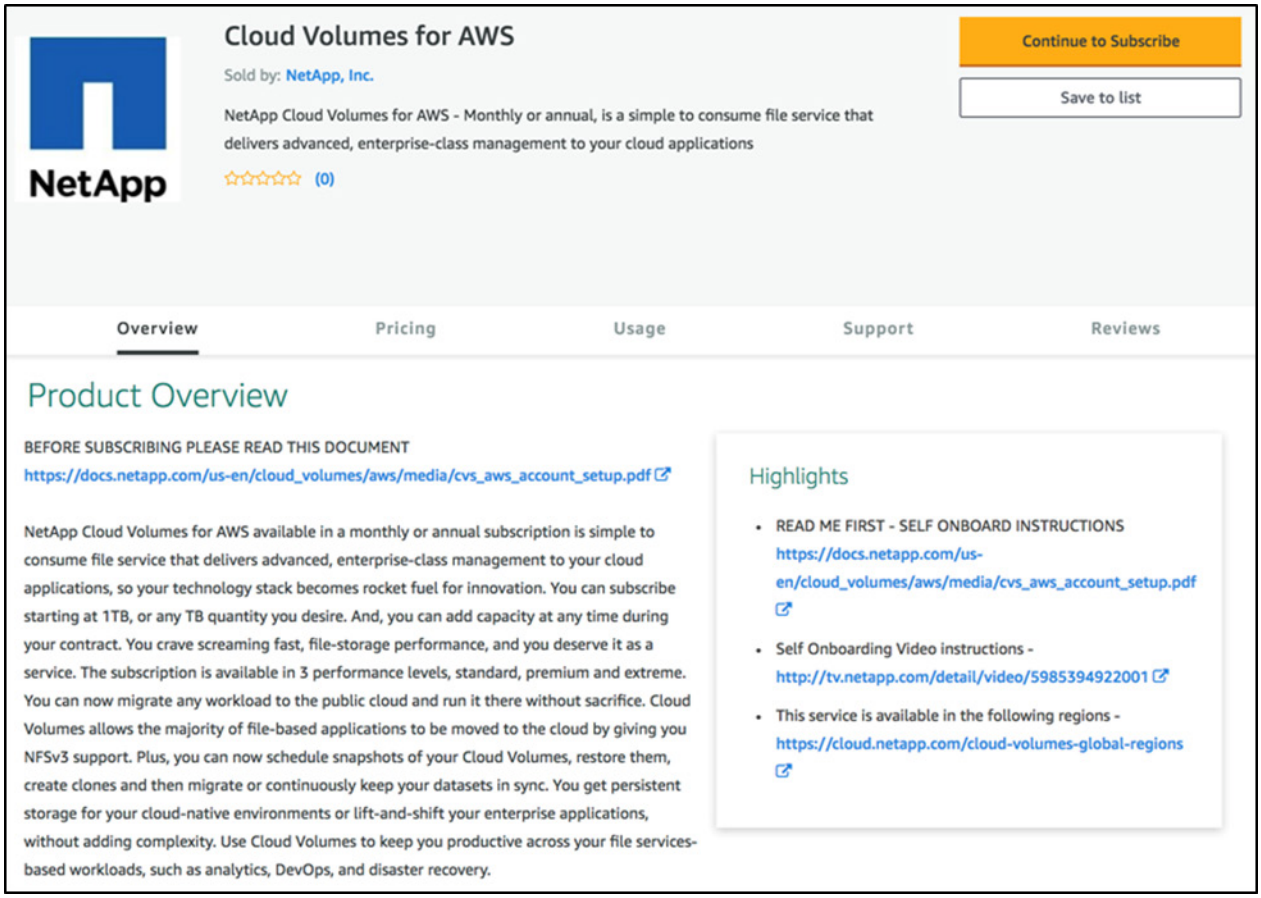
6 Enable AWS Subscription and Cloud Volumes Service

6.1 Access AWS Marketplace Listing for Cloud Volumes Service

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

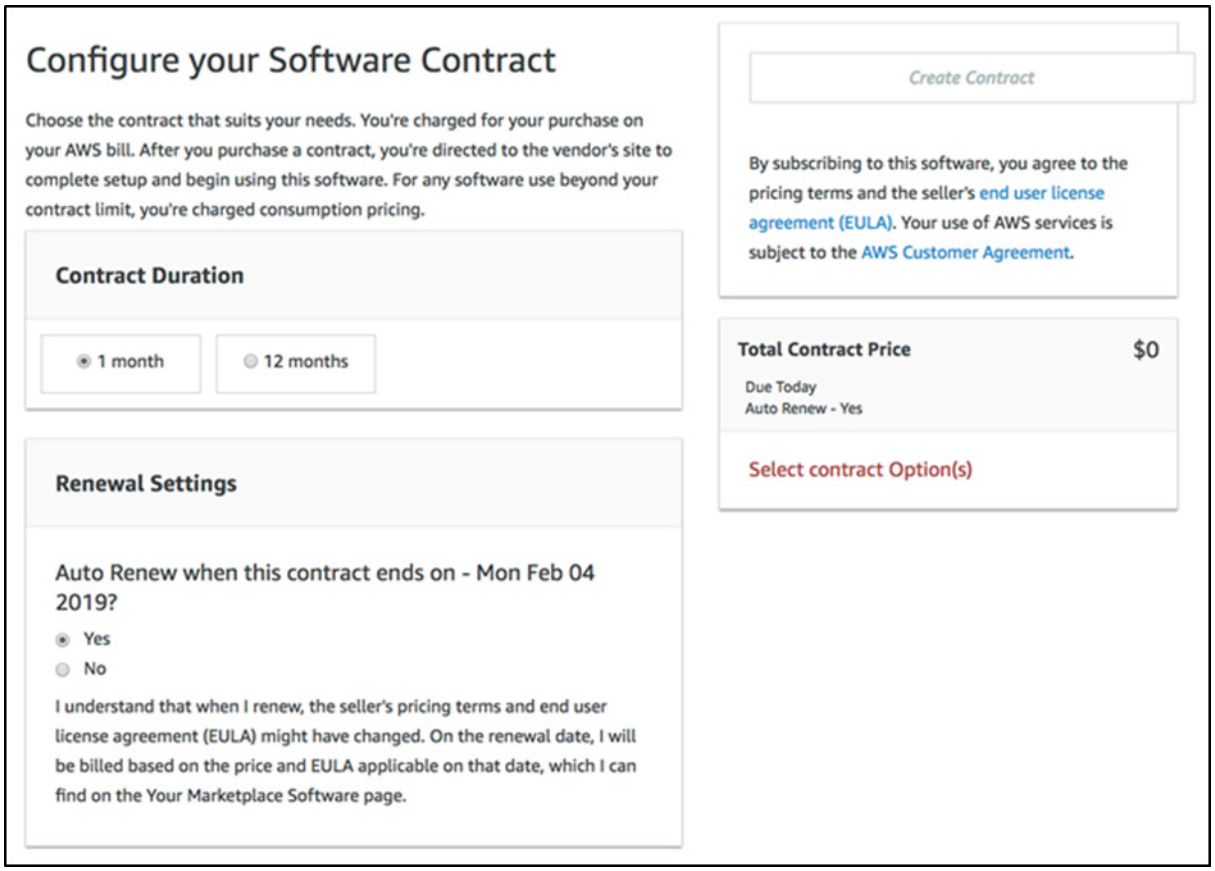
Complete the following steps:

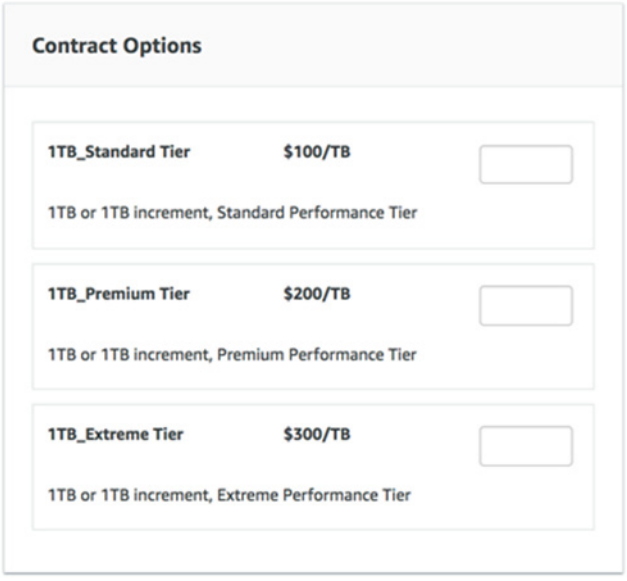
1. Go to the AWS marketplace page and sign in to your AWS account.
2. Type “NetApp Cloud Volumes Service” in the search bar to view these NetApp products.
3. Select the **NetApp Cloud Volumes for AWS** product.



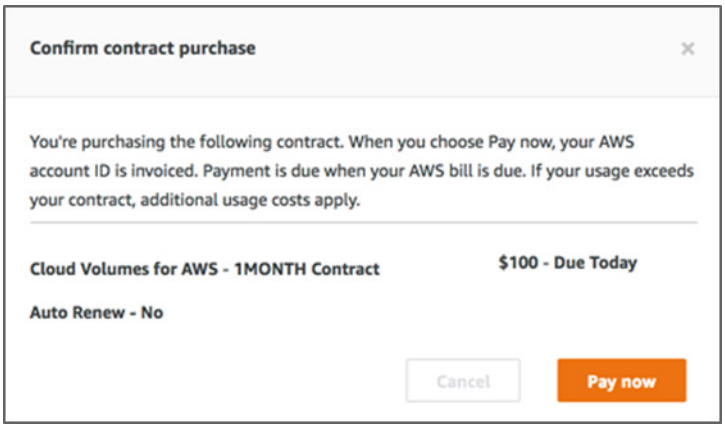
4. Review the content on this page to fully understand the solutions the product provides, and the cost based on the capacity and the service level that you select.
5. Click on the READ ME FIRST document link and the Self Onboarding Video link to identify the prerequisites tasks you must perform before 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.



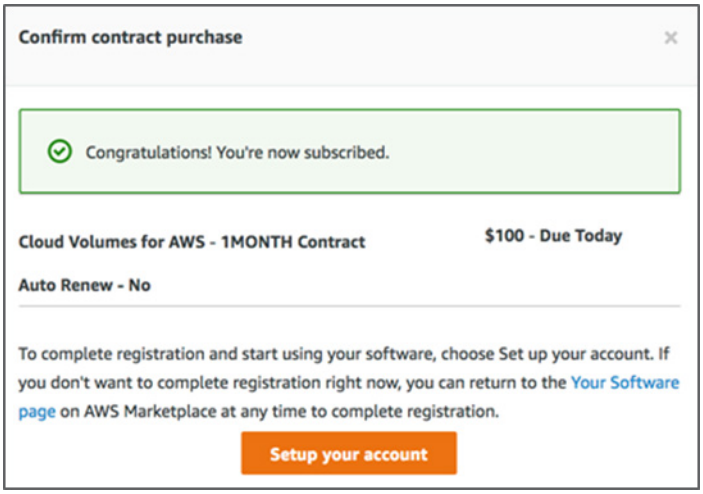


8. After you have specified all the details for the cloud volumes you plan to create, click **Create Contract**.
9. The Confirm contract purchase window displays. If all is OK, click **Pay now**.



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**.



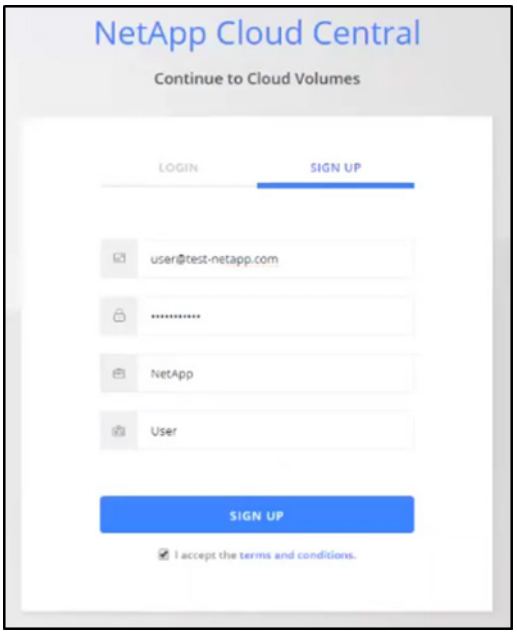
11. You will be redirected to the NetApp Cloud Central page. Complete the steps in the next section to register and log into NetApp Cloud Central.

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**.



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.

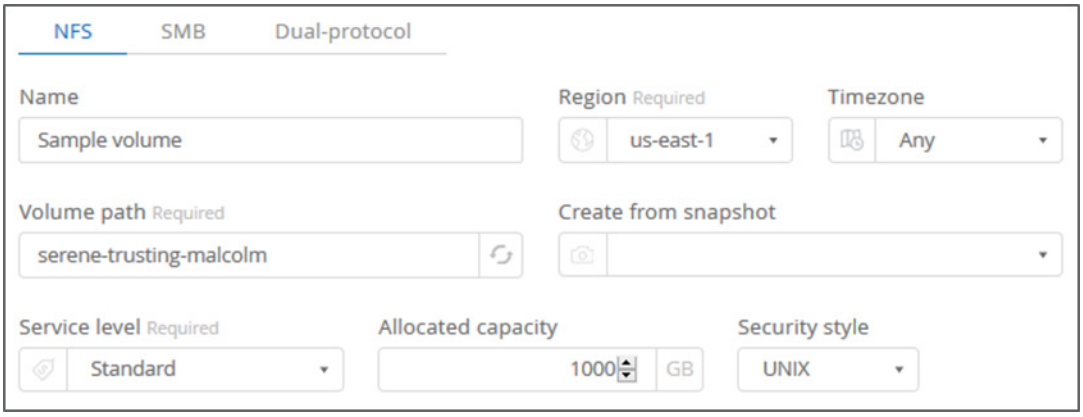
The steps below show how to populate the required fields to create a cloud volume. For information about the other optional sections and fields of the Create Volume page, go to the Creating a cloud volume topic in the NetApp Cloud Volumes Service for AWS documentation.

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.

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:

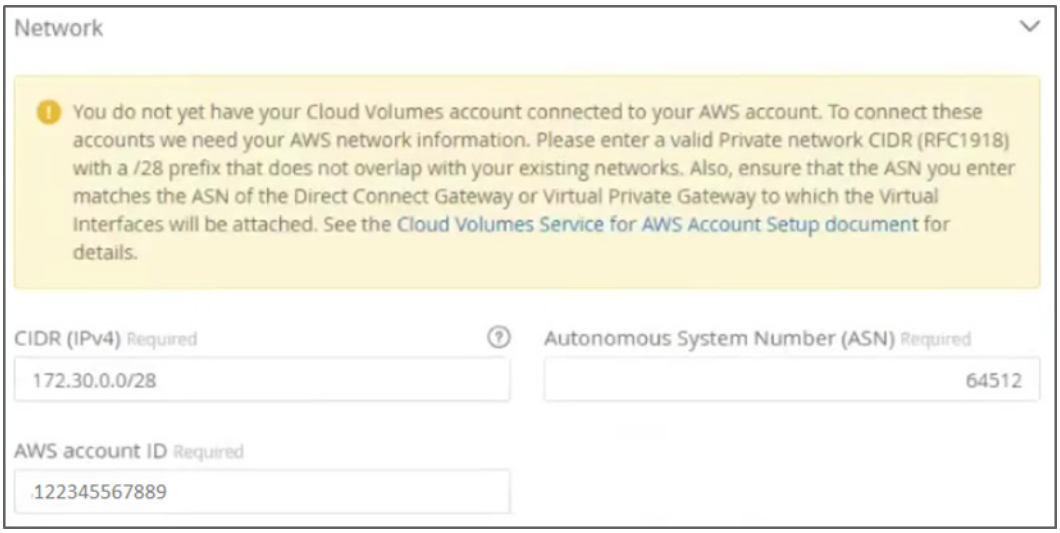
Field	Description
Name	The volume name
Region	The AWS region where you want to create the volume
Volume path	Specify the unique path you want to use, or accept the automatically generated path
Service level	Select Standard, Premium, or Extreme. See the description of available service levels for details
Allocated capacity	Set the initial size of the volume. See the description of allocated capacity for details
Security style	If you selected Dual-protocol, you can select NTFS or UNIX



5. If you selected SMB or Dual-protocol, you can enable SMB session encryption by checking the box for the **Enable data encryption** field.

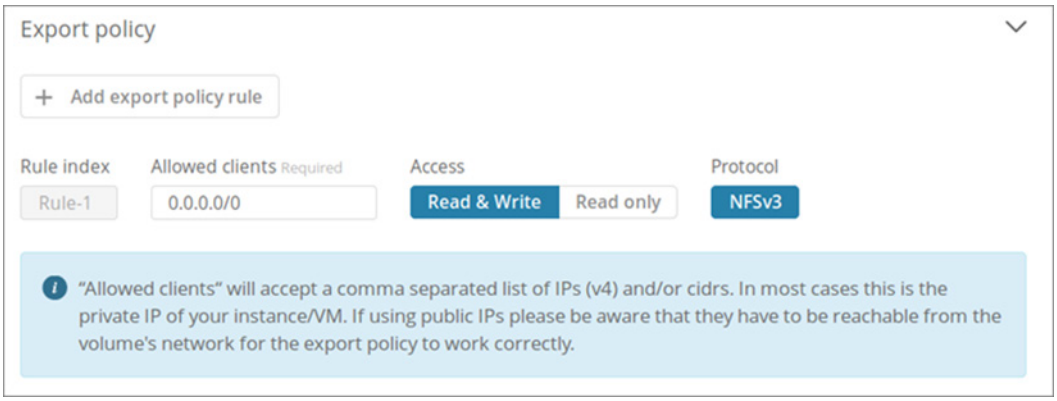
6. In the Network section, complete the following fields using the data you collected in section 5.6 to connect your Cloud Volumes account to your AWS account:

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.
Autonomous System Number (ASN)	When using a VGW in your AWS configuration, use that ASN. When using a Direct Connect Gateway, use that ASN
AWS account ID	Enter your 12-digit Amazon account identifier with no dashes



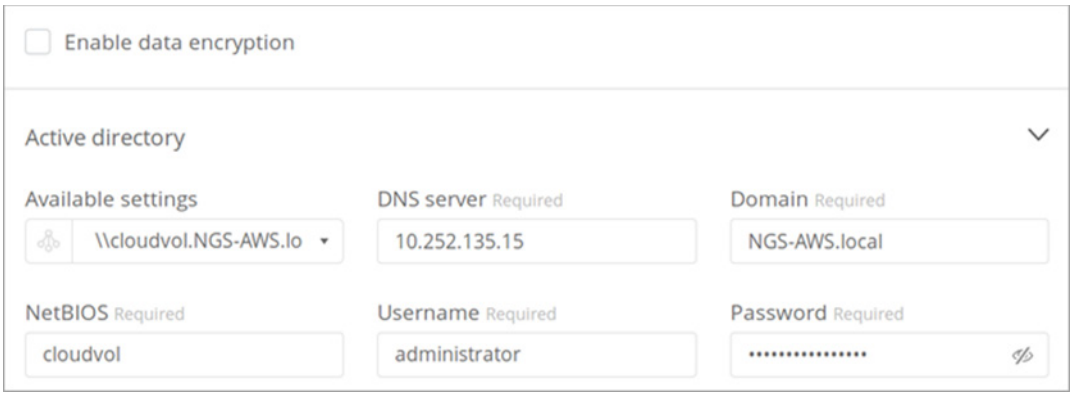
7. In the Export policy section, complete the following fields if you want to restrict the clients that can access the volume:

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	If available, select the protocol



8. 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.
Username	Enter a username for your Active Directory server.
Password	Enter the password for the AD username that you specified in Username.

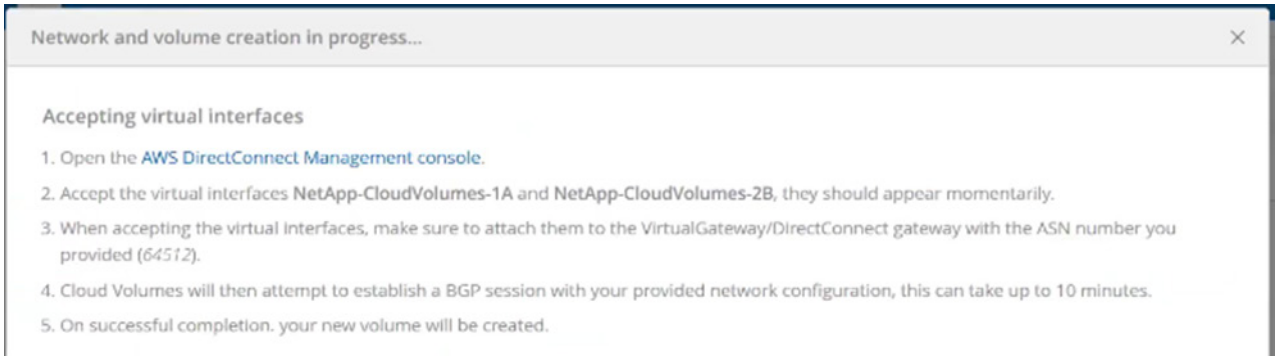


Note: You should follow the guidance on AWS security group settings to enable cloud volumes to integrate with Windows Active Directory servers correctly. See AWS security group settings for Windows AD servers for more information.

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.

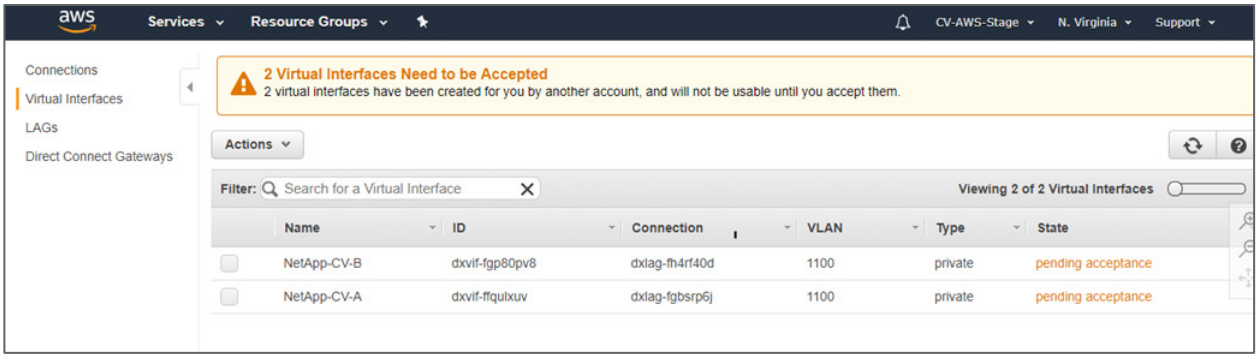
6.4 Accept the Direct Connect Virtual Interfaces

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

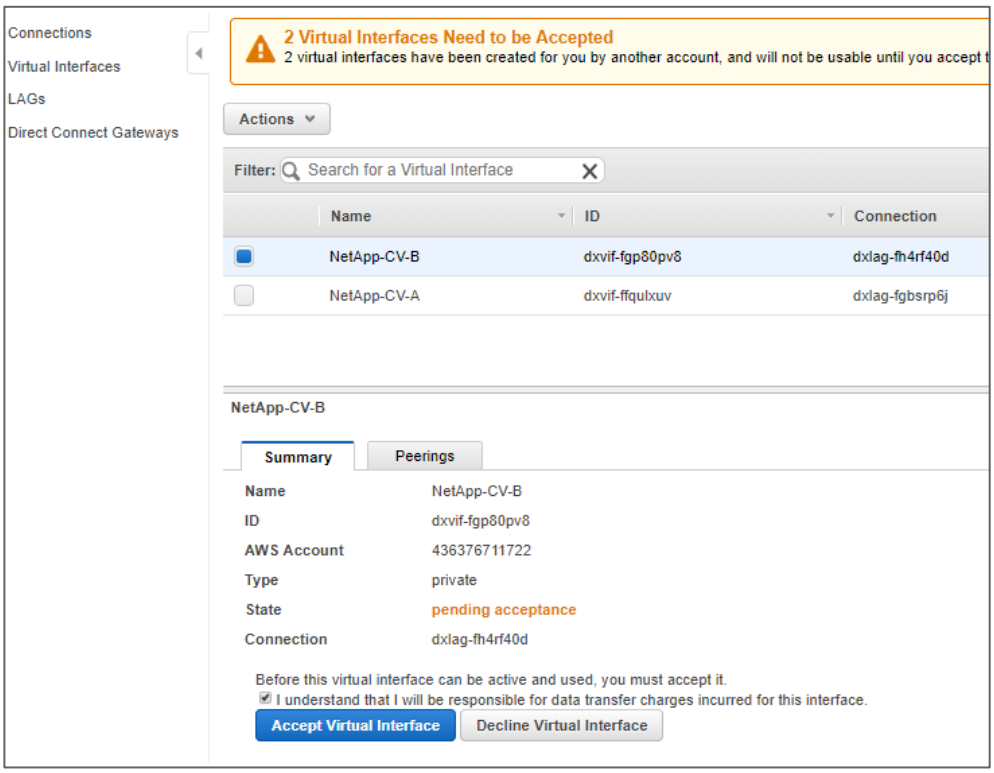
If the interfaces do not appear within 10 minutes there may be a configuration issue; in which case you should contact support.

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`**.

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`**.

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.

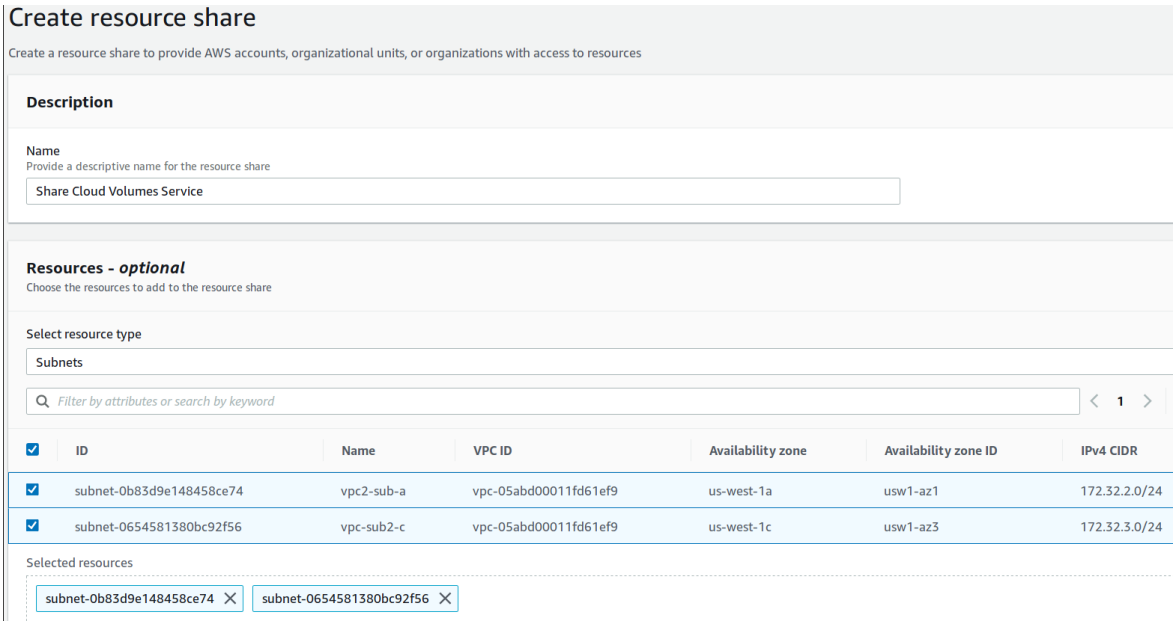
7 Manage Cloud Volumes

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.

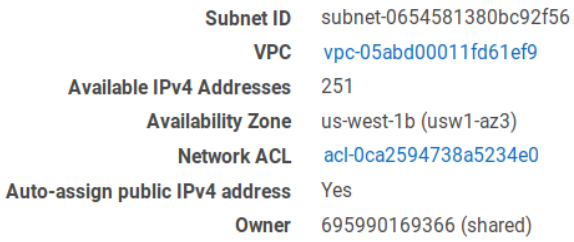
8 Sharing the Cloud Volumes between AWS accounts (optional)

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.



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.



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	Updated Python scripts to check CIDR and ASN. Added section on sharing CVS between AWS accounts
1.0.7	July 18	Added note about Direct Connect Gateway usage

NetApp