Networking requirements

Cloud Manager 3.6

NetApp
October 27, 2021

Table of Contents

Networking requirements

Networking requirements for Cloud Manager

You must set up your networking so that Cloud Manager can deploy Cloud Volumes ONTAP systems in AWS or in Microsoft Azure. The most important step is ensuring outbound internet access to various endpoints.

If your network uses a proxy server for all communication to the internet, Cloud Manager prompts you to specify the proxy during setup. You can also specify the proxy server from the Settings page. Refer to Configuring Cloud Manager to use a proxy server.

Connection to target networks

Cloud Manager requires a network connection to the AWS VPCs and Azure VNets in which you want to deploy Cloud Volumes ONTAP.

For example, if you install Cloud Manager in your corporate network, then you must set up a VPN connection to the AWS VPC or Azure VNet in which you launch Cloud Volumes ONTAP.

Outbound internet access

Cloud Manager requires outbound internet access to deploy and manage Cloud Volumes ONTAP. Outbound internet access is also required when accessing Cloud Manager from your web browser and when running the Cloud Manager installer on a Linux host.

The following sections identify the specific endpoints.

Outbound internet access to manage Cloud Volumes ONTAP in AWS

Cloud Manager requires outbound internet access to contact the following endpoints when deploying and managing Cloud Volumes ONTAP in AWS:

Endpoints	Purpose
AWS services (amazonaws.com): • CloudFormation • Elastic Compute Cloud (EC2) • Key Management Service (KMS) • Security Token Service (STS) • Simple Storage Service (S3) The exact endpoint depends on the region in which you deploy Cloud Volumes ONTAP. Refer to AWS documentation for details.	Enables Cloud Manager to deploy and manage Cloud Volumes ONTAP in AWS.
https://api.services.cloud.netapp.com:443	API requests to NetApp Cloud Central.

Endpoints	Purpose
https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com	Provides access to software images, manifests, and templates.
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com	Enables Cloud Manager to access and download manifests, templates, and Cloud Volumes ONTAP upgrade images.
https://kinesis.us-east-1.amazonaws.com	Enables NetApp to stream data from audit records.
https://cloudmanager.cloud.netapp.com	Communication with the Cloud Manager service, which includes Cloud Central accounts.
https://netapp-cloud-account.auth0.com	Communication with NetApp Cloud Central for centralized user authentication.
https://support.netapp.com/aods/asupmessage https://support.netapp.com/asupprod/post/1.0/postAsup	Communication with NetApp AutoSupport.
https://support.netapp.com/svcgw https://support.netapp.com/ServiceGW/entitlement	Communication with NetApp for licensing and support registration.
https://packages.cloud.google.com/yum https://github.com/NetApp/trident/releases/download/	Required to connect Cloud Volumes ONTAP systems with a Kubernetes cluster. The endpoints enable installation of NetApp Trident.
Various third-party locations, for example: • https://repo1.maven.org/maven2 • https://oss.sonatype.org/content/repositories • https://repo.typesafe.org Third-party locations are subject to change.	During upgrades, Cloud Manager downloads the latest packages for third-party dependencies.

Outbound internet access to manage Cloud Volumes ONTAP in Azure

Cloud Manager requires outbound internet access to contact the following endpoints when deploying and managing Cloud Volumes ONTAP in Microsoft Azure:

Endpoints	Purpose
https://management.azure.com https://login.microsoftonline.com	Enables Cloud Manager to deploy and manage Cloud Volumes ONTAP in most Azure regions.
https://management.microsoftazure.de https://login.microsoftonline.de	Enables Cloud Manager to deploy and manage Cloud Volumes ONTAP in the Azure Germany regions.
https://management.usgovcloudapi.net https://login.microsoftonline.com	Enables Cloud Manager to deploy and manage Cloud Volumes ONTAP in the Azure US Gov regions.

Endpoints	Purpose
https://api.services.cloud.netapp.com:443	API requests to NetApp Cloud Central.
https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com	Provides access to software images, manifests, and templates.
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com https://sts.amazonaws.com	Enables Cloud Manager to access and download manifests, templates, and Cloud Volumes ONTAP upgrade images.
https://kinesis.us-east-1.amazonaws.com	Enables NetApp to stream data from audit records.
https://netapp-cloud-account.auth0.com	Communication with NetApp Cloud Central for centralized user authentication.
https://mysupport.netapp.com	Communication with NetApp AutoSupport.
https://support.netapp.com/svcgw https://support.netapp.com/ServiceGW/entitlement	Communication with NetApp for licensing and support registration.
https://packages.cloud.google.com/yum https://github.com/NetApp/trident/releases/download/	Required to connect Cloud Volumes ONTAP systems with a Kubernetes cluster. The endpoints enable installation of NetApp Trident.
Various third-party locations, for example: • https://repo1.maven.org/maven2 • https://oss.sonatype.org/content/repositories • https://repo.typesafe.org Third-party locations are subject to change.	During upgrades, Cloud Manager downloads the latest packages for third-party dependencies.

Outbound internet access from your web browser

Users must access Cloud Manager from a web browser. The machine running the web browser must have connections to the following endpoints:

Endpoints	Purpose
The Cloud Manager host	You must enter the host's IP address from a web browser to load the Cloud Manager console. Depending on your connectivity to your cloud provider, you can use the private IP or a public IP assigned to the host: • A private IP works if you have a VPN and direct connect access to your virtual network • A public IP works in any networking scenario In any case, you should secure network access by ensuring that security group rules allow access from only authorized IPs or subnets.
https://auth0.com https://cdn.auth0.com https://netapp-cloud-account.auth0.com https://services.cloud.netapp.com	Your web browser connects to these endpoints for centralized user authentication through NetApp Cloud Central.
https://widget.intercom.io	For in-product chat that enables you to talk to NetApp cloud experts.

Outbound internet access to install Cloud Manager on a Linux host

The Cloud Manager installer must access the following URLs during the installation process:

- http://dev.mysql.com/get/mysql-community-release-el7-5.noarch.rpm
- https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm
- https://s3.amazonaws.com/aws-cli/awscli-bundle.zip

Ports and security groups

- If you deploy Cloud Manager from Cloud Central or from the marketplace images, refer to the following:
  - Security group rules for Cloud Manager in AWS
  - Security group rules for Cloud Manager in Azure
- If you install Cloud Manager on an existing Linux host, see Cloud Manager host requirements.

Networking requirements for Cloud Volumes ONTAP in AWS

Set up your AWS networking so Cloud Volumes ONTAP systems can operate properly.

> Looking for the list of endpoints to which Cloud Manager requires access? They're now maintained in a single location. Click here for details.

General AWS networking requirements for Cloud Volumes ONTAP

The following requirements must be met in AWS.

Outbound internet access for Cloud Volumes ONTAP nodes

Cloud Volumes ONTAP nodes require outbound internet access to send messages to NetApp AutoSupport, which proactively monitors the health of your storage.

Routing and firewall policies must allow AWS HTTP/HTTPS traffic to the following endpoints so Cloud Volumes ONTAP can send AutoSupport messages:

- https://support.netapp.com/aods/asupmessage
- https://support.netapp.com/asupprod/post/1.0/postAsup

  If you have a NAT instance, you must define an inbound security group rule that allows HTTPS traffic from the private subnet to the internet.

Outbound internet access for the HA mediator

The HA mediator instance must have an outbound connection to the AWS EC2 service so it can assist with storage failover. To provide the connection, you can add a public IP address, specify a proxy server, or use a manual option.

The manual option can be a NAT gateway or an interface VPC endpoint from the target subnet to the AWS EC2 service. For details about VPC endpoints, refer to AWS Documentation: Interface VPC Endpoints (AWS PrivateLink).

Security groups

You do not need to create security groups because Cloud Manager does that for you. If you need to use your own, refer to Security group rules.

Connection from Cloud Volumes ONTAP to AWS S3 for data tiering

If you want to use EBS as a performance tier and AWS S3 as a capacity tier, you must ensure that Cloud Volumes ONTAP has a connection to S3. The best way to provide that connection is by creating a VPC Endpoint to the S3 service. For instructions, see AWS Documentation: Creating a Gateway Endpoint.

When you create the VPC Endpoint, be sure to select the region, VPC, and route table that corresponds to the Cloud Volumes ONTAP instance. You must also modify the security group to add an outbound HTTPS rule that enables traffic to the S3 endpoint. Otherwise, Cloud Volumes ONTAP cannot connect to the S3 service.

If you experience any issues, see AWS Support Knowledge Center: Why can't I connect to an S3 bucket using a gateway VPC endpoint?

Connections to ONTAP systems in other networks

To replicate data between a Cloud Volumes ONTAP system in AWS and ONTAP systems in other networks, you must have a VPN connection between the AWS VPC and the other network—for example, an Azure VNet or your corporate network. For instructions, see AWS Documentation: Setting Up an AWS VPN Connection.

DNS and Active Directory for CIFS

If you want to provision CIFS storage, you must set up DNS and Active Directory in AWS or extend your on-premises setup to AWS.

The DNS server must provide name resolution services for the Active Directory environment. You can configure DHCP option sets to use the default EC2 DNS server, which must not be the DNS server used by the Active Directory environment.

For instructions, refer to AWS Documentation: Active Directory Domain Services on the AWS Cloud Quick Start Reference Deployment.

AWS networking requirements for Cloud Volumes ONTAP HA in multiple AZs

Additional AWS networking requirements apply to Cloud Volumes ONTAP HA configurations that use multiple Availability Zones (AZs). You should review these requirements before you launch an HA pair because you must enter the networking details in Cloud Manager.

To understand how HA pairs work, see High-availability pairs.

Availability Zones

This HA deployment model uses multiple AZs to ensure high availability of your data. You should use a dedicated AZ for each Cloud Volumes ONTAP instance and the mediator instance, which provides a communication channel between the HA pair.

Floating IP addresses for NAS data and cluster/SVM management

HA configurations in multiple AZs use floating IP addresses that migrate between nodes if failures occur. They are not natively accessible from outside the VPC, unless you set up an AWS transit gateway.

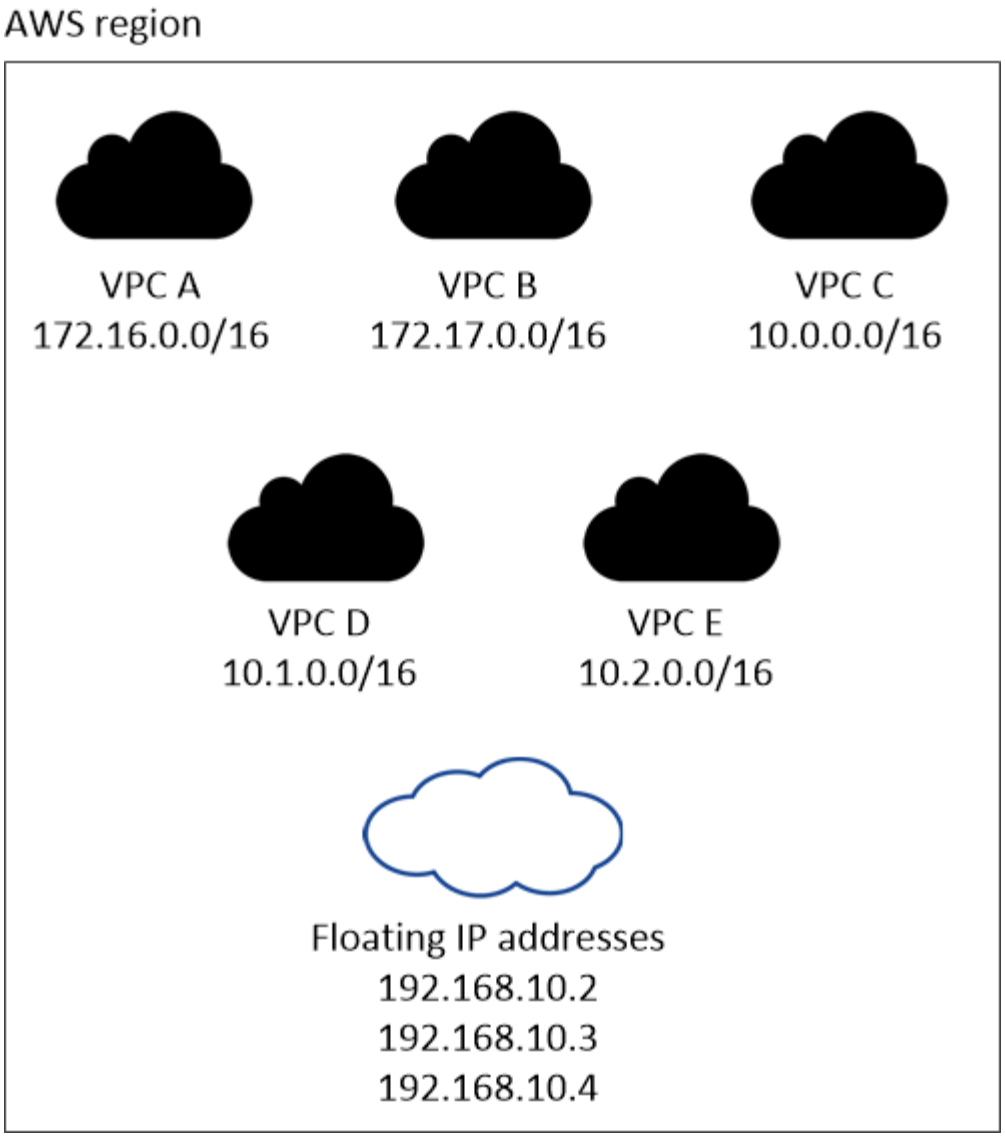
One floating IP address is for cluster management, one is for NFS/CIFS data on node 1, and one is for NFS/CIFS data on node 2. A fourth floating IP address for SVM management is optional.

> ⓘ A floating IP address is required for the SVM management LIF if you use SnapDrive for Windows or SnapCenter with the HA pair. If you don't specify the IP address when you deploy the system, you can create the LIF later. For details, see Setting up Cloud Volumes ONTAP.

You need to enter the floating IP addresses in Cloud Manager when you create a Cloud Volumes ONTAP HA working environment. Cloud Manager allocates the IP addresses to the HA pair when it launches the system.

The floating IP addresses must be outside of the CIDR blocks for all VPCs in the AWS region in which you deploy the HA configuration. Think of the floating IP addresses as a logical subnet that's outside of the VPCs in your region.

The following example shows the relationship between floating IP addresses and the VPCs in an AWS region. While the floating IP addresses are outside the CIDR blocks for all VPCs, they're routable to subnets through route tables.



Cloud Manager automatically creates static IP addresses for iSCSI access and for NAS access from clients outside the VPC. You don't need to meet any requirements for these types of IP addresses.

Transit gateway to enable floating IP access from outside the VPC

Set up an AWS transit gateway to enable access to an HA pair's floating IP addresses from outside the VPC where the HA pair resides.

Route tables

After you specify the floating IP addresses in Cloud Manager, you need to select the route tables that should include routes to the floating IP addresses. This enables client access to the HA pair.

If you have just one route table for the subnets in your VPC (the main route table), then Cloud Manager automatically adds the floating IP addresses to that route table. If you have more than one route table, it's very important to select the correct route tables when launching the HA pair. Otherwise, some clients might not have access to Cloud Volumes ONTAP.

For example, you might have two subnets that are associated with different route tables. If you select route table A, but not route table B, then clients in the subnet associated with route table A can access the HA

pair, but clients in the subnet associated with route table B can't.

For more information about route tables, refer to AWS Documentation: Route Tables.

Connection to NetApp management tools

To use NetApp management tools with HA configurations that are in multiple AZs, you have two connection options:

1. Deploy the NetApp management tools in a different VPC and set up an AWS transit gateway. The gateway enables access to the floating IP address for the cluster management interface from outside the VPC.
2. Deploy the NetApp management tools in the same VPC with a similar routing configuration as NAS clients.

Example configuration

The following image shows an optimal HA configuration in AWS operating as an active-passive configuration:

Sample VPC configurations

To better understand how you can deploy Cloud Manager and Cloud Volumes ONTAP in AWS, you should review the most common VPC configurations.

- A VPC with public and private subnets and a NAT device
- A VPC with a private subnet and a VPN connection to your network

A VPC with public and private subnets and a NAT device

This VPC configuration includes public and private subnets, an internet gateway that connects the VPC to the internet, and a NAT gateway or NAT instance in the public subnet that enables outbound internet traffic from the private subnet. In this configuration, you can run Cloud Manager in a public subnet or private subnet, but the public subnet is recommended because it allows access from hosts outside the VPC. You can then launch Cloud Volumes ONTAP instances in the private subnet.

Instead of a NAT device, you can use an HTTP proxy to provide internet connectivity.

For more details about this scenario, refer to AWS Documentation: Scenario 2: VPC with Public and Private Subnets (NAT).

The following graphic shows Cloud Manager running in a public subnet and single node systems running in a private subnet:

A VPC with a private subnet and a VPN connection to your network

This VPC configuration is a hybrid cloud configuration in which Cloud Volumes ONTAP becomes an extension of your private environment. The configuration includes a private subnet and a virtual private gateway with a VPN connection to your network. Routing across the VPN tunnel allows EC2 instances to access the internet through your network and firewalls. You can run Cloud Manager in the private subnet or in your data center. You would then launch Cloud Volumes ONTAP in the private subnet.

You can also use a proxy server in this configuration to allow internet access. The proxy server can be in your data center or in AWS.

If you want to replicate data between FAS systems in your data center and Cloud Volumes ONTAP systems in AWS, you should use a VPN connection so that the link is secure.

For more details about this scenario, refer to AWS Documentation: Scenario 4: VPC with a Private Subnet Only and AWS Managed VPN Access.

The following graphic shows Cloud Manager running in your data center and single node systems running in a private subnet:

Setting up an AWS transit gateway for HA pairs in multiple AZs

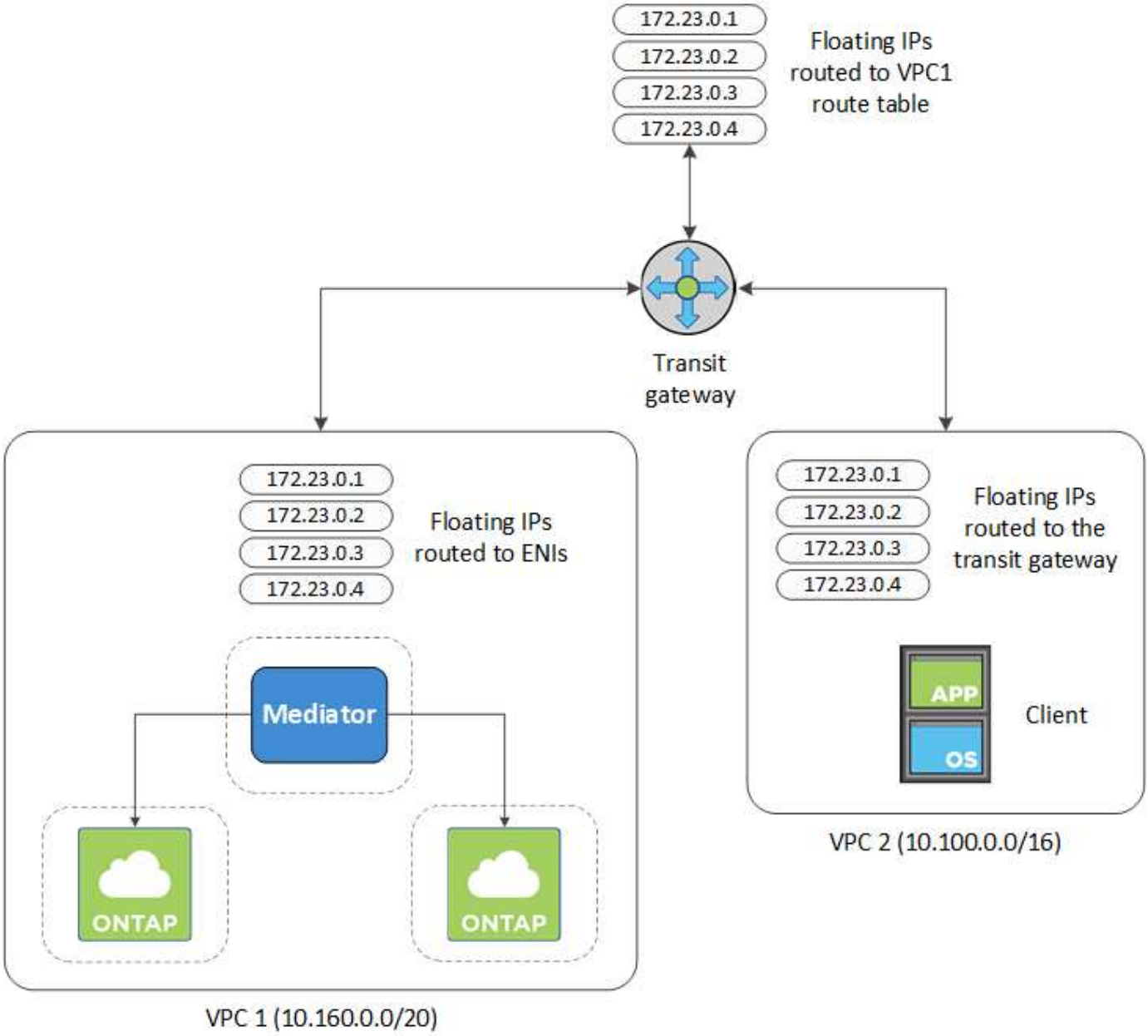
Set up an AWS transit gateway to enable access to an HA pair's floating IP addresses from outside the VPC where the HA pair resides.

When a Cloud Volumes ONTAP HA configuration is spread across multiple AWS Availability Zones, floating IP addresses are required for NAS data access from within the VPC. These floating IP addresses can migrate between nodes when failures occur, but they are not natively accessible from outside the VPC. Separate private IP addresses provide data access from outside the VPC, but they don't provide automatic failover.

Floating IP addresses are also required for the cluster management interface and the optional SVM management LIF.

If you set up an AWS transit gateway, you enable access to the floating IP addresses from outside the VPC where the HA pair resides. That means NAS clients and NetApp management tools outside the VPC can access the floating IPs.

Here's an example that shows two VPCs connected by a transit gateway. An HA system resides in one VPC, while a client resides in the other. You could then mount a NAS volume on the client using the floating IP address.

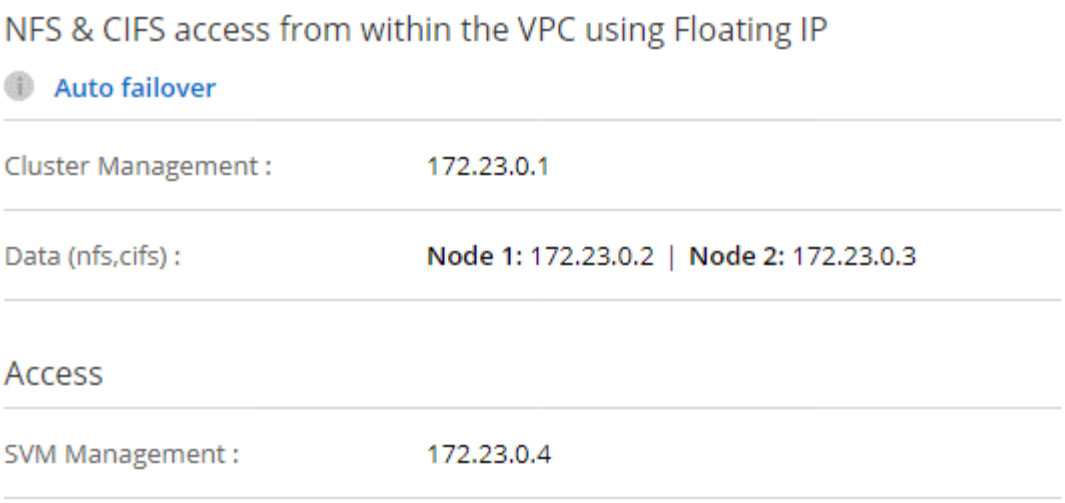


The following steps illustrate how to set up a similar configuration.

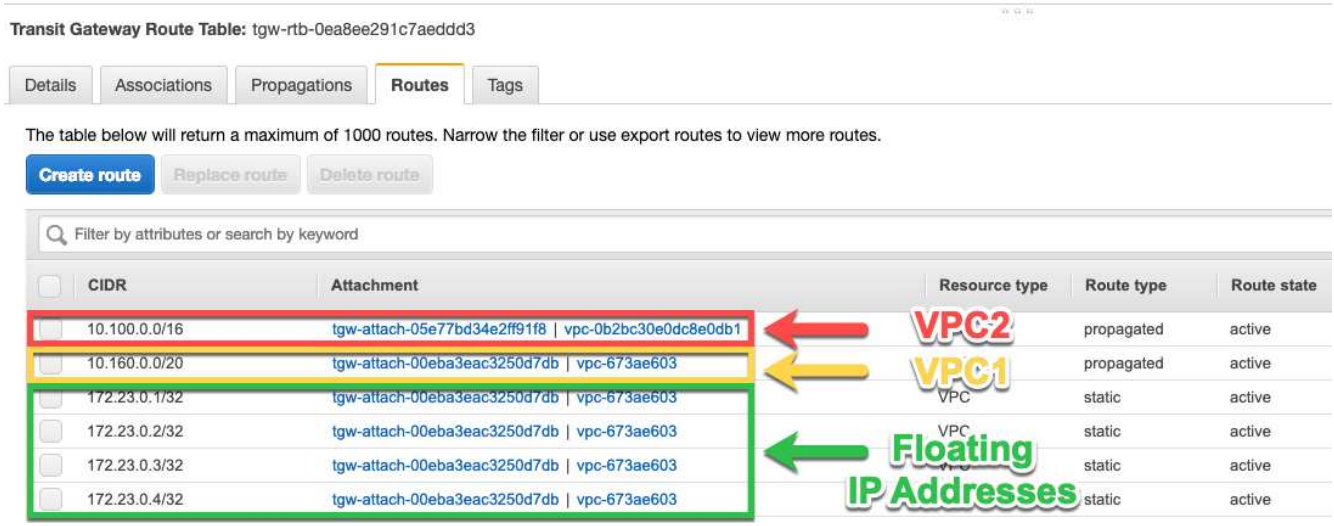
Steps

1. Create a transit gateway and attach the VPCs to the gateway.
2. Create routes in the transit gateway's route table by specifying the HA pair's floating IP addresses.

   You can find the floating IP addresses on the Working Environment Information page in Cloud Manager. Here's an example:

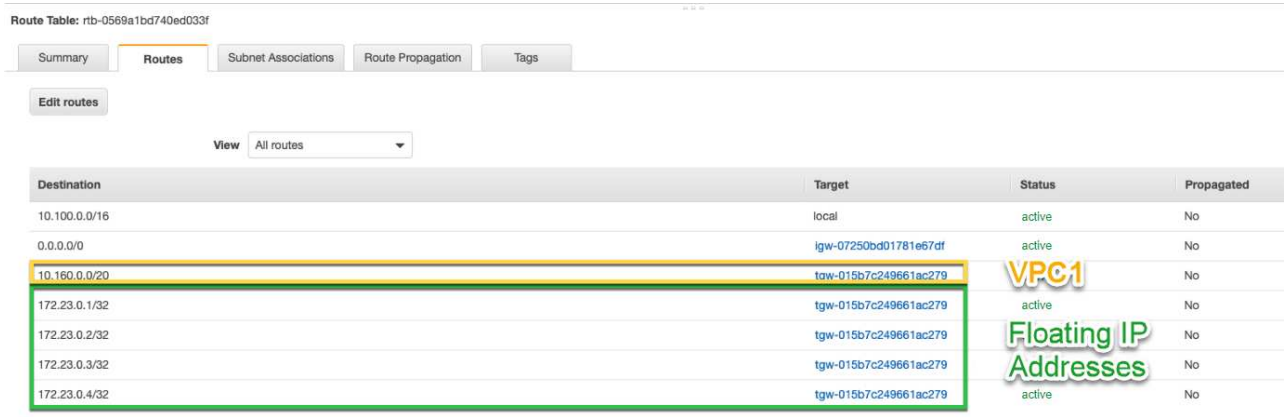


The following sample image shows the route table for the transit gateway. It includes routes to the CIDR blocks of the two VPCs and four floating IP addresses used by Cloud Volumes ONTAP.



3. Modify the route table of VPCs that need to access the floating IP addresses.
   a. Add route entries to the floating IP addresses.
   b. Add a route entry to the CIDR block of the VPC where the HA pair resides.

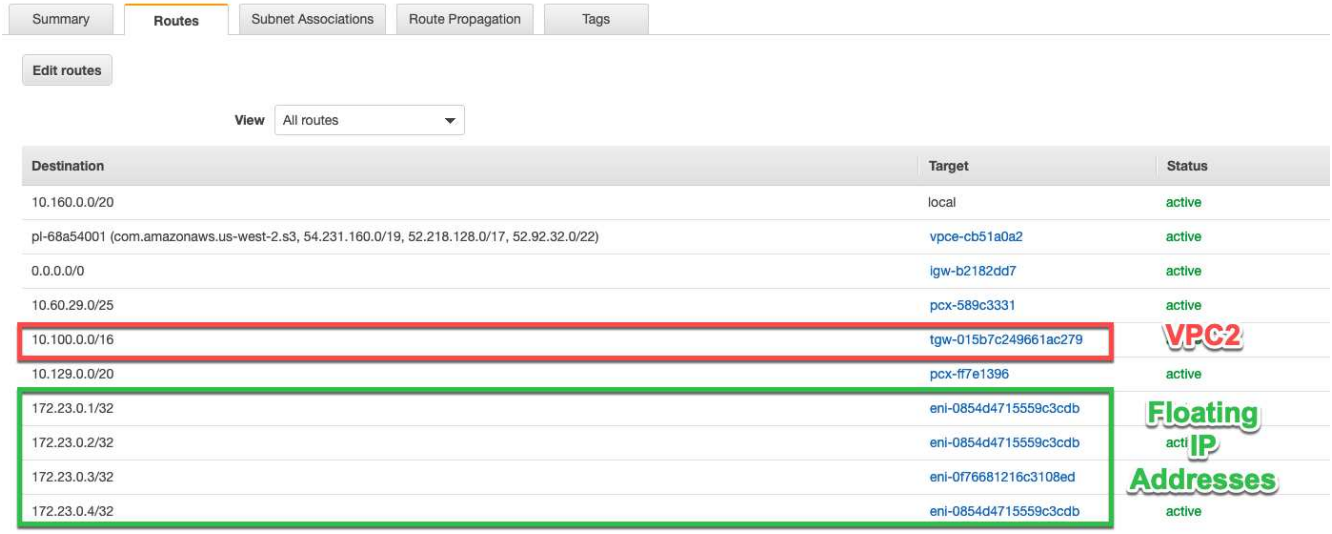
      The following sample image shows the route table for VPC 2, which includes routes to VPC 1 and the floating IP addresses.



4. Modify the route table for the HA pair's VPC by adding a route to the VPC that needs access to the floating IP addresses.

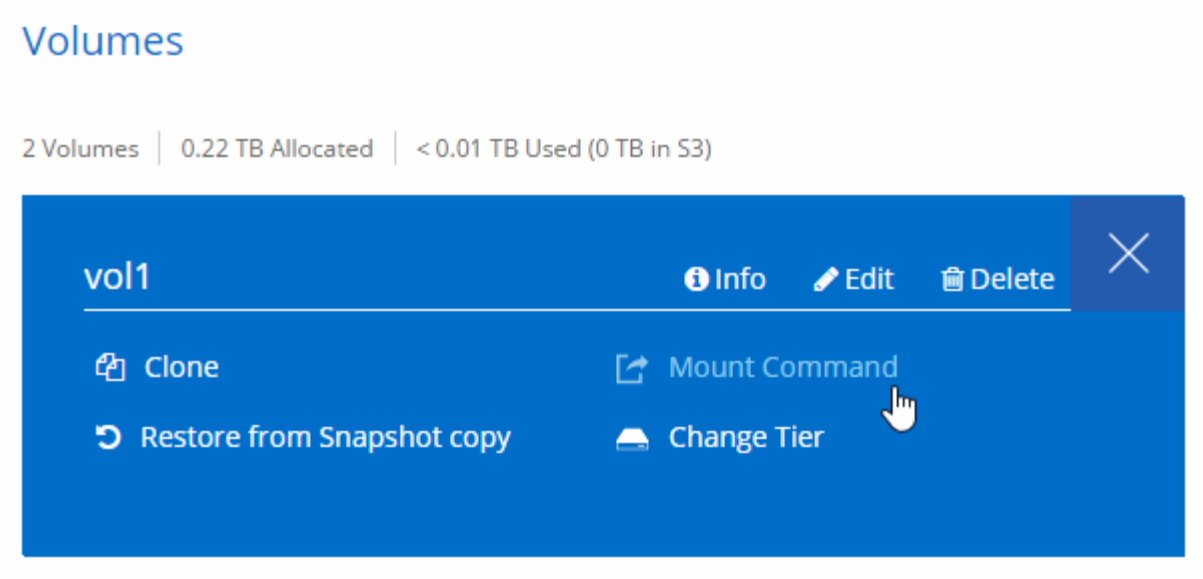
   This step is important because it completes the routing between the VPCs.

   The following sample image shows the route table for VPC 1. It includes a route to the floating IP addresses and to VPC 2, which is where a client resides. Cloud Manager automatically added the floating IPs to the route table when it deployed the HA pair.



5. Mount volumes to clients using the floating IP address.

   You can find the correct IP address in Cloud Manager by selecting a volume and clicking **Mount Command**.



Related links

- High-availability pairs in AWS
- Networking requirements for Cloud Volumes ONTAP in AWS

Networking requirements for Cloud Volumes ONTAP in Azure

You must set up your Azure networking so Cloud Volumes ONTAP systems can operate properly.

> Looking for the list of endpoints to which Cloud Manager requires access? They're now maintained in a single location. Click here for details.

Outbound internet access for Cloud Volumes ONTAP

Cloud Volumes ONTAP requires outbound internet access to send messages to NetApp AutoSupport, which proactively monitors the health of your storage.

Routing and firewall policies must allow AWS HTTP/HTTPS traffic to the following endpoints so Cloud Volumes ONTAP can send AutoSupport messages:

- https://support.netapp.com/aods/asupmessage
- https://support.netapp.com/asupprod/post/1.0/postAsup

Security groups

You do not need to create security groups because Cloud Manager does that for you. If you need to use your own, refer to Security group rules.

Connection from Cloud Volumes ONTAP to Azure Blob storage for data tiering

If you want to tier cold data to Azure Blob storage, you do not need to set up a VNet service endpoint as long as Cloud Manager has the required permissions:

```
"Microsoft.Network/virtualNetworks/subnets/write",
"Microsoft.Network/routeTables/join/action",
```

These permissions are included in the latest Cloud Manager policy.

For details about setting up data tiering, see Tiering cold data to low-cost object storage.

Connections to ONTAP systems in other networks

To replicate data between a Cloud Volumes ONTAP system in Azure and ONTAP systems in other networks, you must have a VPN connection between the Azure VNet and the other network—for example, an AWS VPC or your corporate network.

For instructions, refer to Microsoft Azure Documentation: Create a Site-to-Site connection in the Azure portal.