# Set up your networking

## Cloud Volumes ONTAP

NetApp
September 22, 2022

# Table of Contents

# Set up your networking

## Networking requirements for Cloud Volumes ONTAP in AWS

Cloud Manager handles the set up of networking components for Cloud Volumes ONTAP, such as IP addresses, netmasks, and routes. You need to make sure that outbound internet access is available, that enough private IP addresses are available, that the right connections are in place, and more.

### General requirements

The following requirements must be met in AWS.

#### Outbound internet access for Cloud Volumes ONTAP nodes

Cloud Volumes ONTAP nodes require outbound internet access for NetApp AutoSupport, which proactively monitors the health of your system and sends messages to NetApp technical support.

Routing and firewall policies must allow 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.

If an outbound internet connection isn't available to send AutoSupport messages, Cloud Manager automatically configures your Cloud Volumes ONTAP systems to use the Connector as a proxy server. The only requirement is to ensure that the Connector's security group allows *inbound* connections over port 3128. You'll need to open this port after you deploy the Connector.

If you defined strict outbound rules for Cloud Volumes ONTAP, then you'll also need to ensure that the Cloud Volumes ONTAP security group allows *outbound* connections over port 3128.

After you've verified that outbound internet access is available, you can test AutoSupport to ensure that it can send messages. For instructions, refer to ONTAP docs: Set up AutoSupport.

If Cloud Manager notifies you that AutoSupport messages can't be sent, troubleshoot your AutoSupport configuration.

#### 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).

## Private IP addresses

Cloud Manager automatically allocates the required number of private IP addresses to Cloud Volumes ONTAP. You need to ensure that your networking has enough private IP addresses available.

The number of LIFs that Cloud Manager allocates for Cloud Volumes ONTAP depends on whether you deploy a single node system or an HA pair. A LIF is an IP address associated with a physical port.

### IP addresses for a single node system

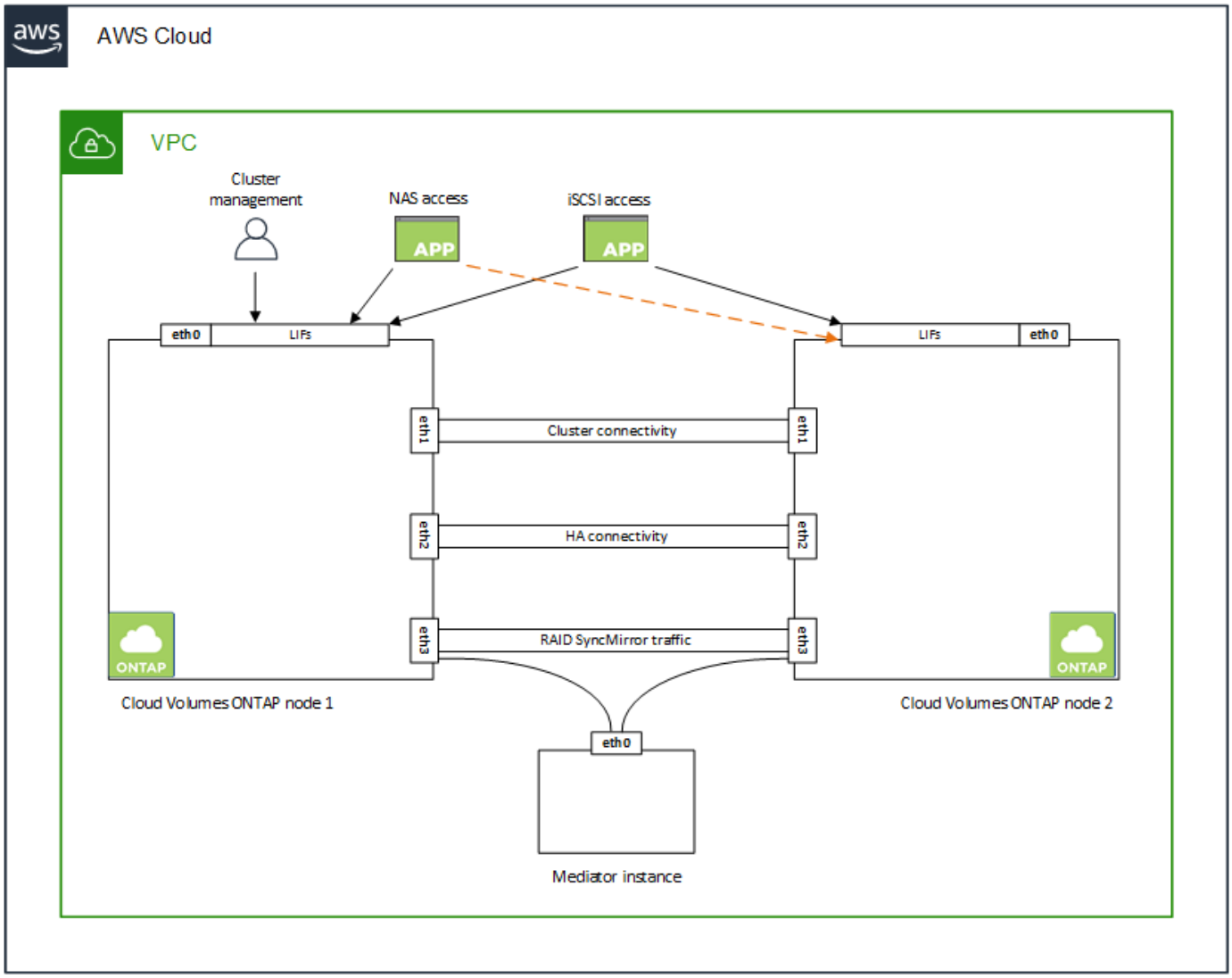
Cloud Manager allocates 6 IP addresses to a single node system:

- Cluster management LIF
- Node management LIF
- Intercluster LIF
- NAS data LIF
- iSCSI data LIF
- Storage VM management LIF

  A storage VM management LIF is used with management tools like SnapCenter.

### IP addresses for HA pairs

HA pairs require more IP addresses than a single node system does. These IP addresses are spread across different ethernet interfaces, as shown in the following image:




The number of private IP addresses required for an HA pair depends on which deployment model you choose. An HA pair deployed in a *single* AWS Availability Zone (AZ) requires 15 private IP addresses, while an HA pair deployed in *multiple* AZs requires 13 private IP addresses.

The following tables provide details about the LIFs that are associated with each private IP address.

### LIFs for HA pairs in a single AZ

| LIF | Interface | Node | Purpose |
|---|---|---|---|
| Cluster management | eth0 | node 1 | Administrative management of the entire cluster (HA pair). |
| Node management | eth0 | node 1 and node 2 | Administrative management of a node. |
| Intercluster | eth0 | node 1 and node 2 | Cross-cluster communication, backup, and replication. |
| NAS data | eth0 | node 1 | Client access over NAS protocols. |

| LIF | Interface | Node | Purpose |
|---|---|---|---|
| iSCSI data | eth0 | node 1 and node 2 | Client access over the iSCSI protocol and system use for important networking workflows. These LIFs are required and should not be deleted. |
| Cluster connectivity | eth1 | node 1 and node 2 | Enables the nodes to communicate with each other and to move data within the cluster. |
| HA connectivity | eth2 | node 1 and node 2 | Communication between the two nodes in case of failover. |
| RSM iSCSI traffic | eth3 | node 1 and node 2 | RAID SyncMirror iSCSI traffic, as well as communication between the two Cloud Volumes ONTAP nodes and the mediator. |
| Mediator | eth0 | Mediator | A communication channel between the nodes and the mediator to assist in storage takeover and giveback processes. |

**LIFs for HA pairs in multiple AZs**

| LIF | Interface | Node | Purpose |
|---|---|---|---|
| Node management | eth0 | node 1 and node 2 | Administrative management of a node. |
| Intercluster | eth0 | node 1 and node 2 | Cross-cluster communication, backup, and replication. |
| iSCSI data | eth0 | node 1 and node 2 | Client access over the iSCSI protocol. This LIF also manages the migration of floating IP addresses between nodes. |
| Cluster connectivity | eth1 | node 1 and node 2 | Enables the nodes to communicate with each other and to move data within the cluster. |
| HA connectivity | eth2 | node 1 and node 2 | Communication between the two nodes in case of failover. |
| RSM iSCSI traffic | eth3 | node 1 and node 2 | RAID SyncMirror iSCSI traffic, as well as communication between the two Cloud Volumes ONTAP nodes and the mediator. |
| Mediator | eth0 | Mediator | A communication channel between the nodes and the mediator to assist in storage takeover and giveback processes. |

When deployed in multiple Availability Zones, several LIFs are associated with floating IP addresses, which don't count against the AWS private IP limit.

### 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 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

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, 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.

### VPC sharing

Starting with the 9.11.1 release, Cloud Volumes ONTAP HA pairs are supported in AWS with VPC sharing. VPC sharing enables your organization to share subnets with other AWS accounts. To use this configuration, you must set up your AWS environment and then deploy the HA pair using the API.

Learn how to deploy an HA pair in a shared subnet.

## Requirements for HA pairs 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 when you create the working environment.

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.

A subnet should be available in each Availability Zone.

### 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.

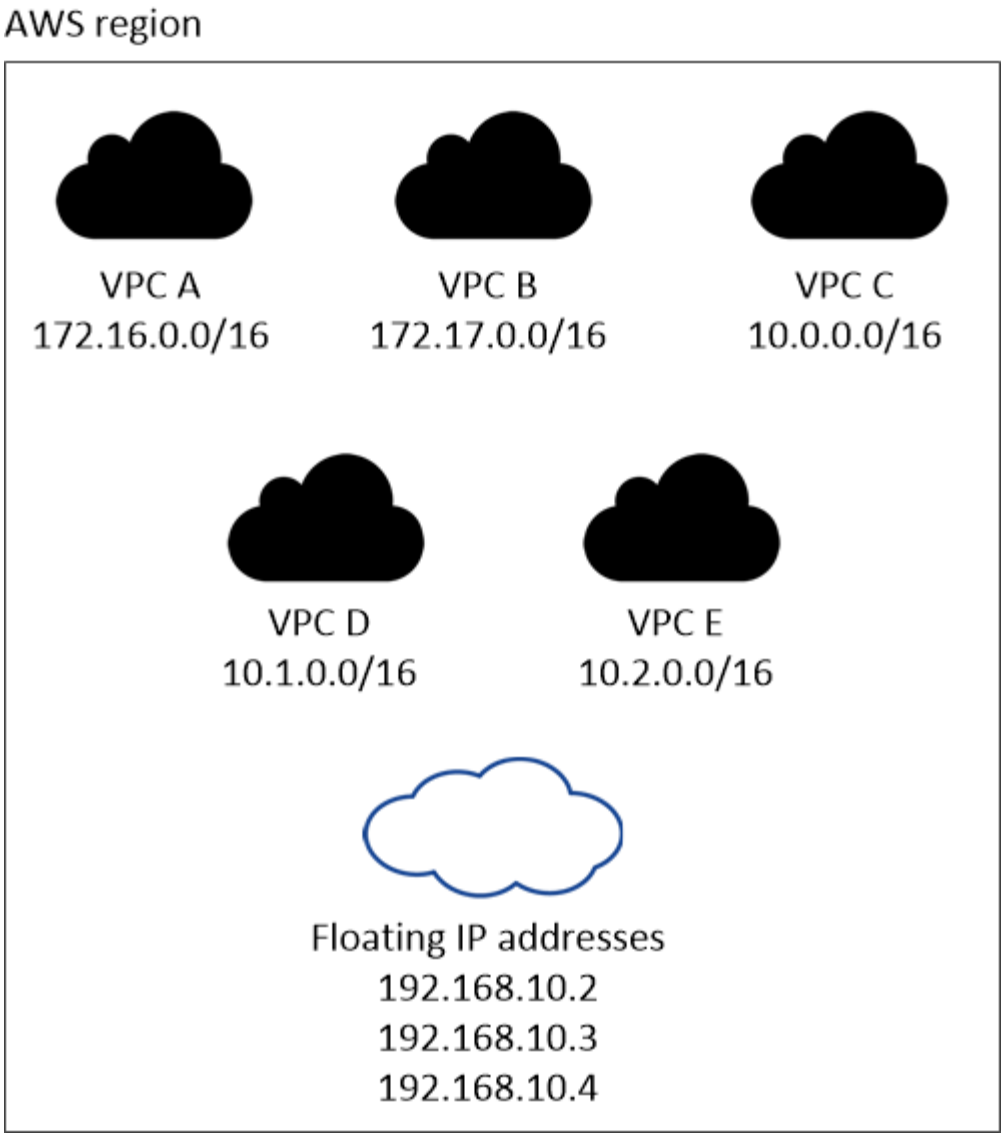
One floating IP address is for cluster management, one is for NFS/CIFS data on node 1, and one is for NFS/CIFS data on node 2. A fourth floating IP address for SVM management is optional.

A floating IP address is required for the SVM management LIF if you use SnapDrive for Windows or SnapCenter with the HA pair.

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**

If needed, 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 are then prompted 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.

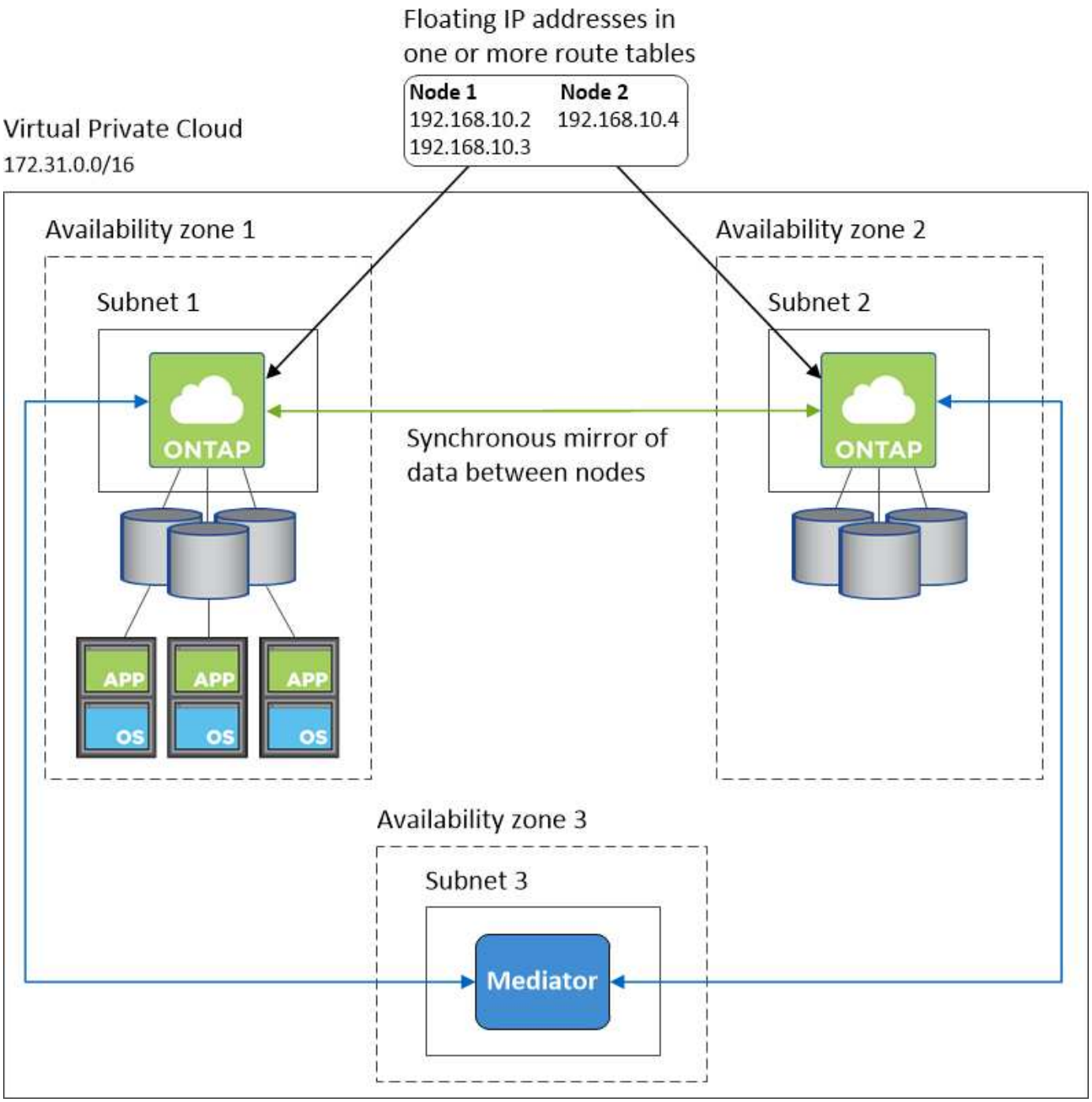
### Connection to NetApp management tools

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 HA configuration

The following image illustrates the networking components specific to an HA pair in multiple AZs: three Availability Zones, three subnets, floating IP addresses, and a route table.




## Requirements for the Connector

Set up your networking so that the Connector can manage resources and processes within your public cloud environment. 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, you can specify the proxy server from the Settings page. Refer to Configuring the Connector to use a proxy server.

### Connection to target networks

A Connector requires a network connection to the VPCs and VNets in which you want to deploy Cloud Volumes ONTAP.

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

**Outbound internet access**

The Connector requires outbound internet access to manage resources and processes within your public cloud environment.

| Endpoints | Purpose |
|---|---|
| https://support.netapp.com | To obtain licensing information and to send AutoSupport messages to NetApp support. |
| https://*.cloudmanager.cloud.netapp.com | To provide SaaS features and services within Cloud Manager. |
| https://cloudmanagerinfraprod.azurecr.io<br><br>https://*.blob.core.windows.net | To upgrade the Connector and its Docker components. |

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

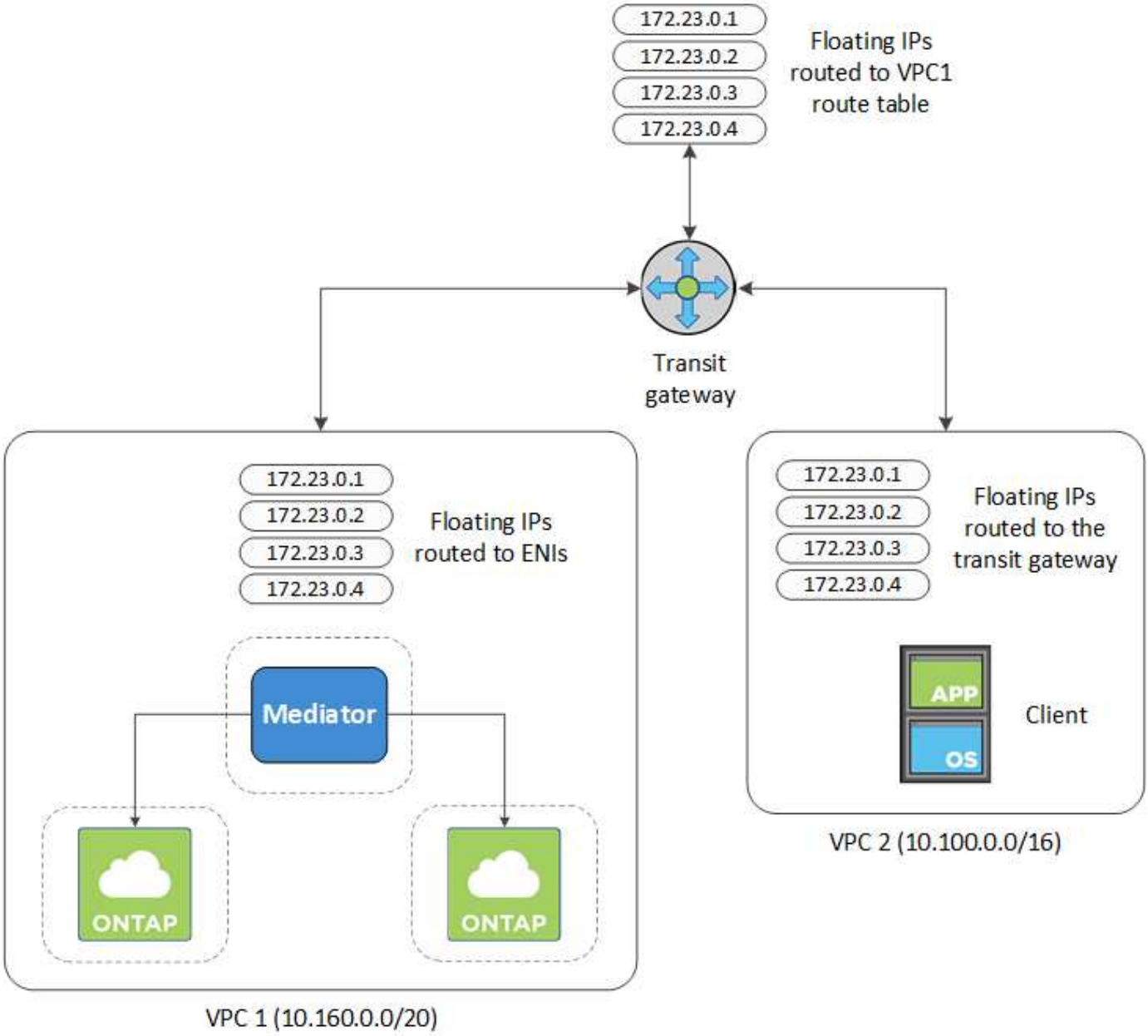
Set up an AWS transit gateway to enable access to an HA pair's floating IP addresses from outside the VPC where the HA pair resides.

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.

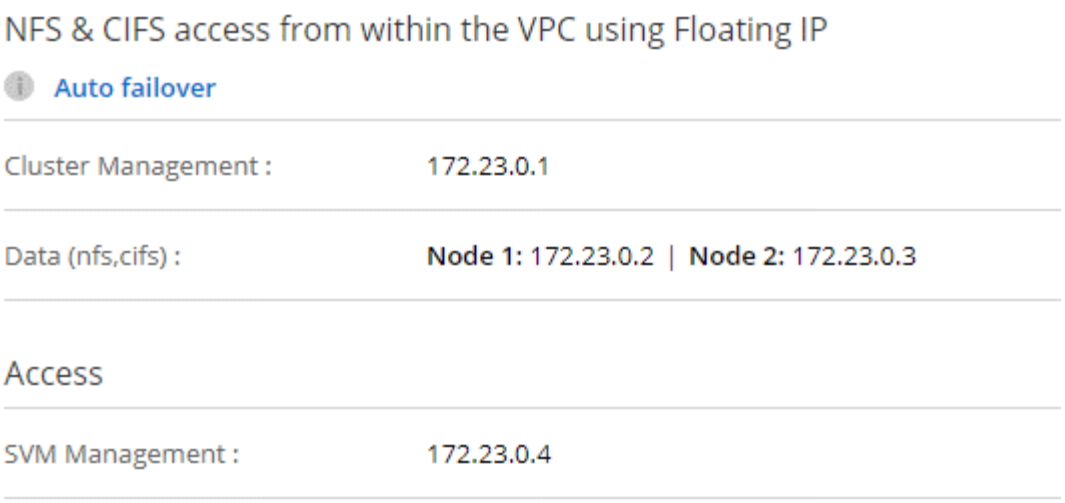



The following steps illustrate how to set up a similar configuration.

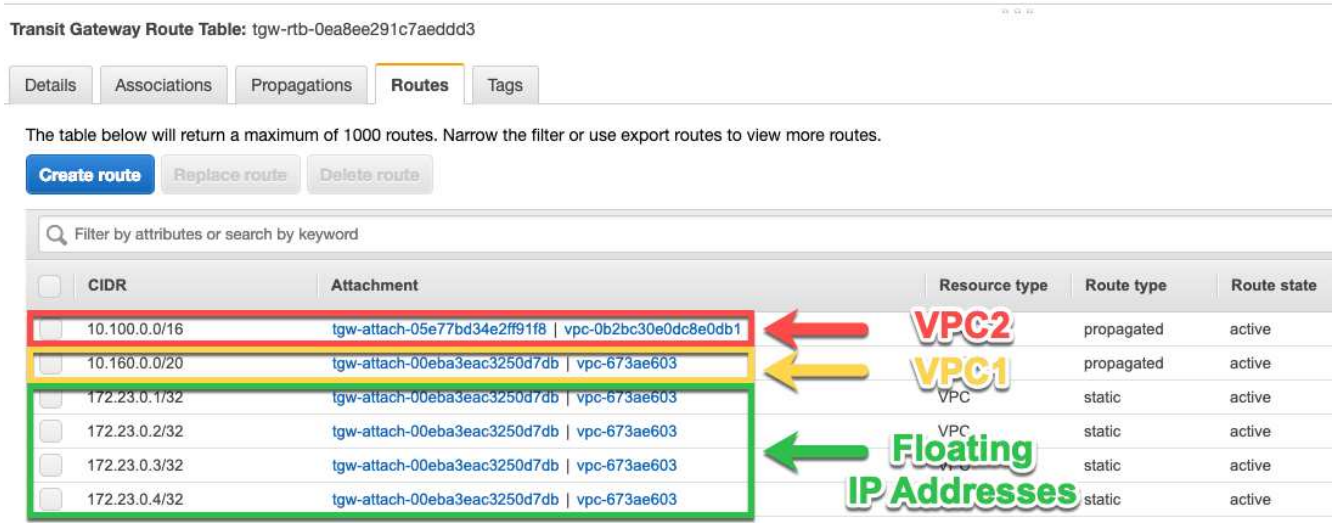
**Steps**

1. Create a transit gateway and attach the VPCs to the gateway.
2. Associate the VPCs with the transit gateway route table.
   a. In the **VPC** service, click **Transit Gateway Route Tables**.
   b. Select the route table.
   c. Click **Associations** and then select **Create association**.
   d. Choose the attachments (the VPCs) to associate and then click **Create association**.
3. 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:

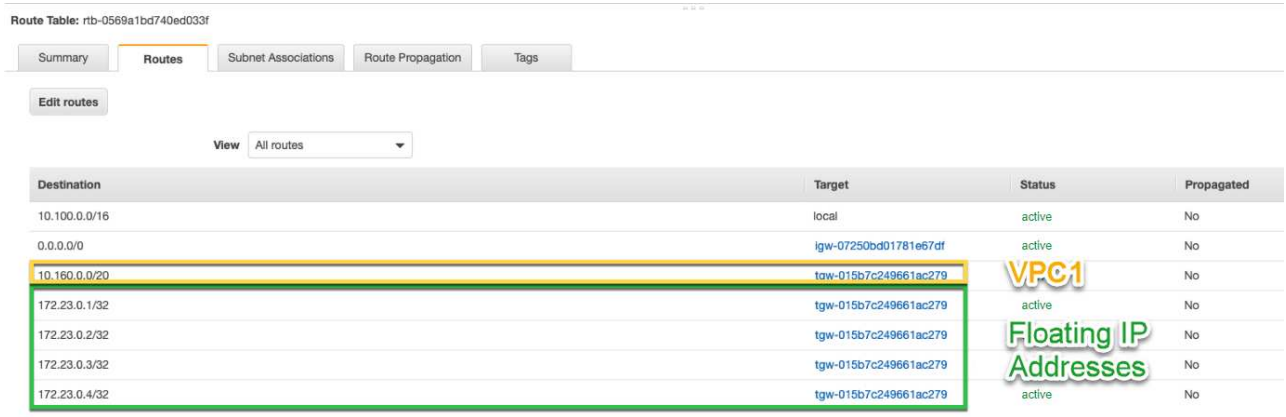



The following sample image shows the route table for the transit gateway. It includes routes to the CIDR blocks of the two VPCs and four floating IP addresses used by Cloud Volumes ONTAP.




4. 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.

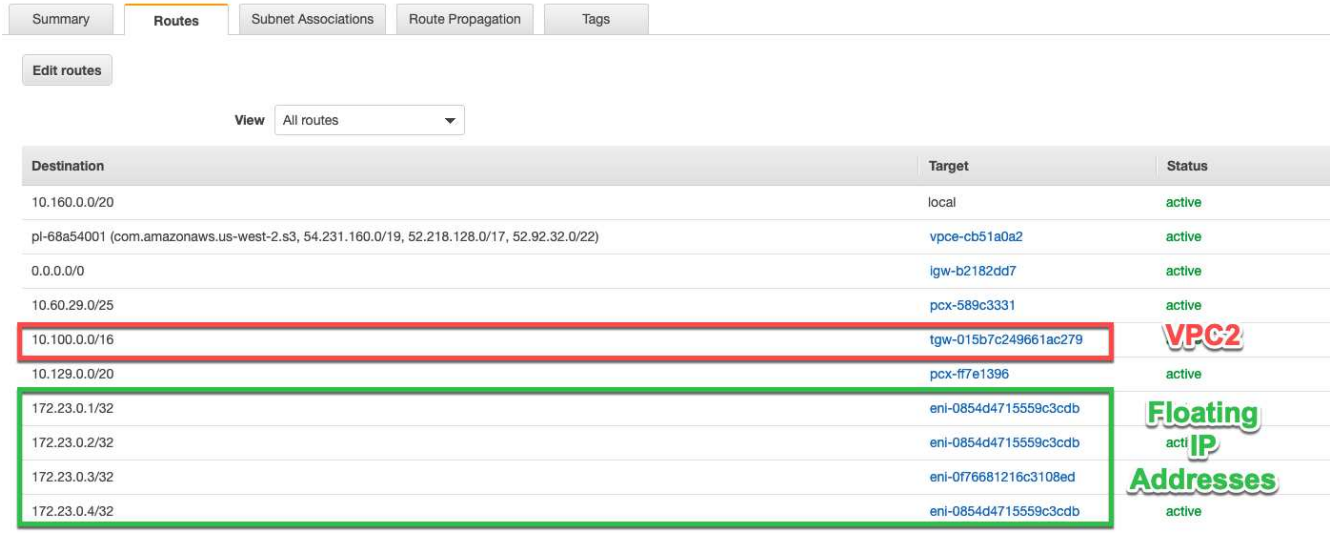
      The following sample image shows the route table for VPC 2, which includes routes to VPC 1 and the floating IP addresses.




5. 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.

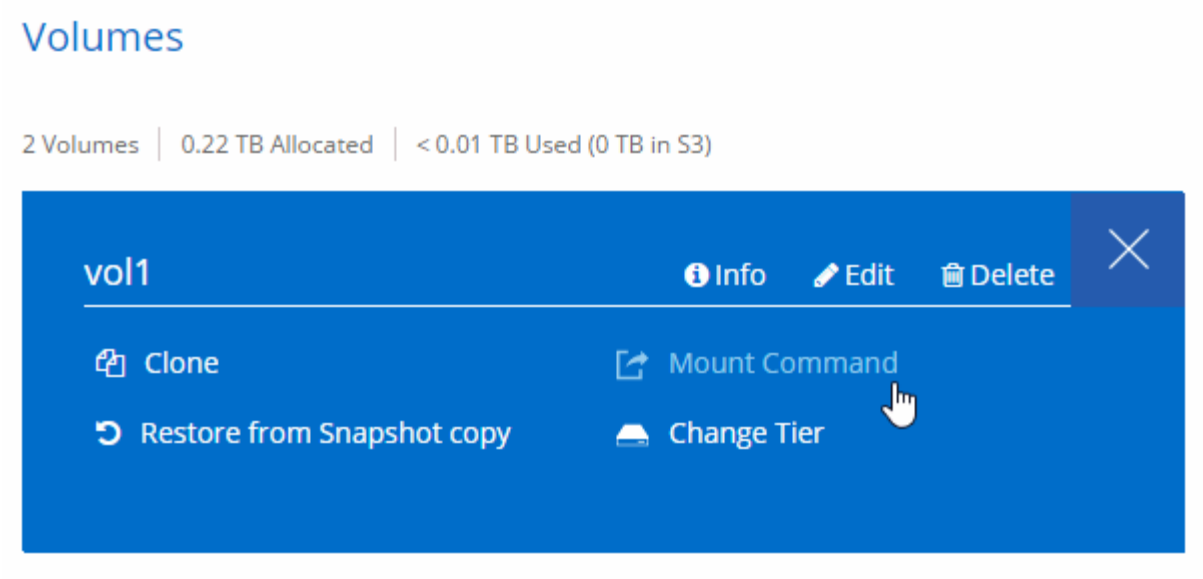
   This step is important because it completes the routing between the VPCs.

   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.




6. 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**.




7. If you're mounting an NFS volume, configure the export policy to match the subnet of the client VPC.

   Learn how to edit a volume.

**Related links**

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

# Deploy an HA pair in a shared subnet

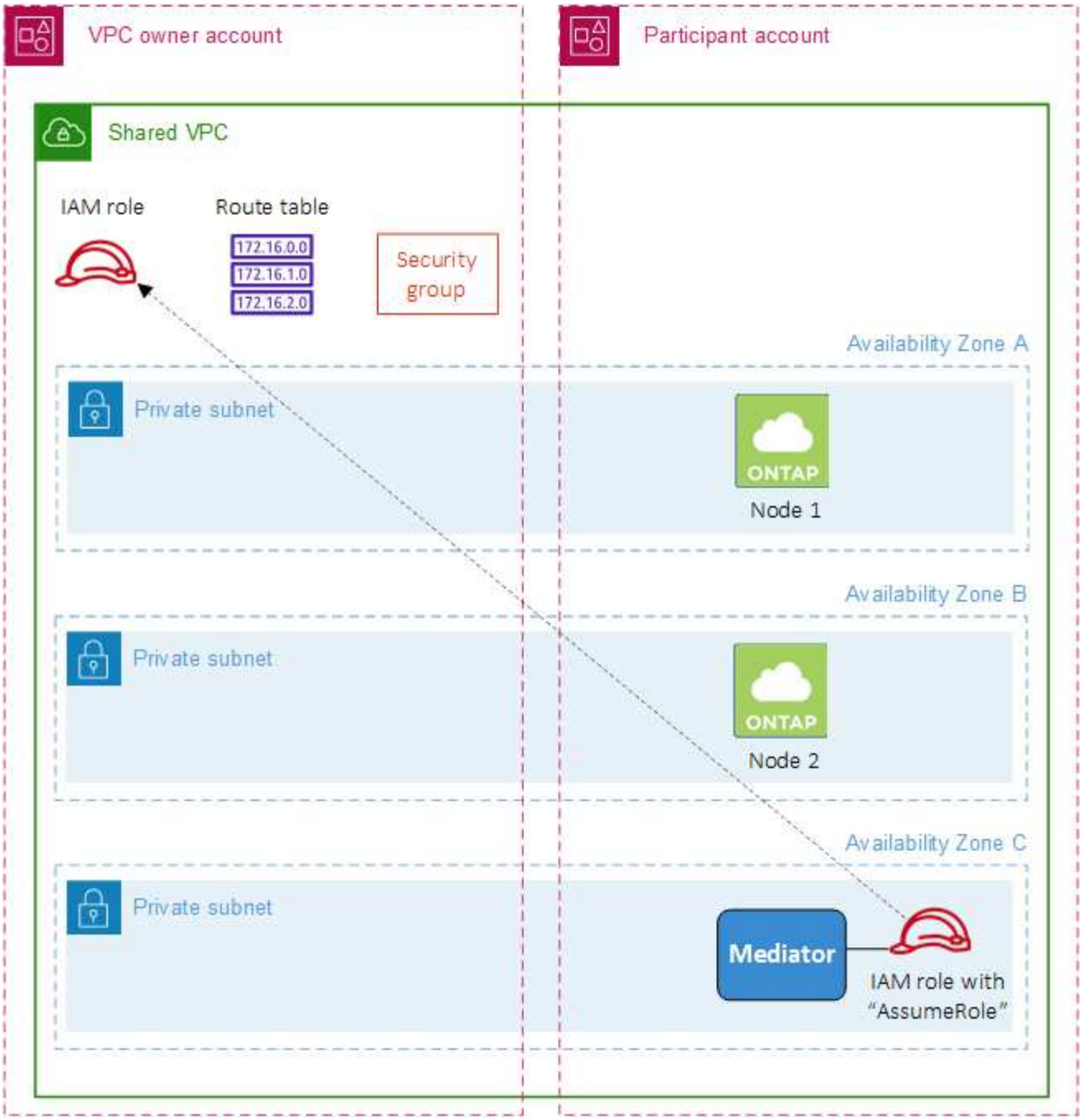
Starting with the 9.11.1 release, Cloud Volumes ONTAP HA pairs are supported in AWS with VPC sharing. VPC sharing enables your organization to share subnets with other AWS accounts. To use this configuration, you must set up your AWS environment and then deploy the HA pair using the API.

With VPC sharing, a Cloud Volumes ONTAP HA configuration is spread across two accounts:

- The VPC owner account, which owns the networking (the VPC, subnets, route tables, and Cloud Volumes ONTAP security group)
- The participant account, where the EC2 instances are deployed in shared subnets (this includes the two HA nodes and the mediator)

In the case of a Cloud Volumes ONTAP HA configuration that is deployed across multiple Availability Zones, the HA mediator needs specific permissions to write to the route tables in the VPC owner account. You need to provide those permissions by setting up an IAM role that the mediator can assume.

The following image shows the components involved this deployment:




As described in the steps below, you'll need to share the subnets with the participant account, and then create the IAM role and security group in the VPC owner account.

When you create the Cloud Volumes ONTAP working environment, Cloud Manager automatically creates and attaches an IAM role to the mediator. This role assumes the IAM role that you created in the VPC owner account in order to make changes to the route tables associated with the HA pair.

**Steps**

1. Share the subnets in the VPC owner account with the participant account.

   This step is required to deploy the HA pair in shared subnets.

   AWS documentation: Share a subnet

2. In the VPC owner account, create a security group for Cloud Volumes ONTAP.

   Refer to the security group rules for Cloud Volumes ONTAP. Note that you don't need to create a security group for the HA mediator. Cloud Manager does that for you.

3. In the VPC owner account, create an IAM role that includes the following permissions:

```
Action": [
                "ec2:AssignPrivateIpAddresses",
                "ec2:CreateRoute",
                "ec2:DeleteRoute",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRouteTables",
                "ec2:DescribeVpcs",
                "ec2:ReplaceRoute",
                "ec2:UnassignPrivateIpAddresses"
```

4. Use the Cloud Manager API to create a new Cloud Volumes ONTAP working environment.

   Note that you must specify the following fields:

   - "securityGroupId"

     The "securityGroupId" field should specify the security group that you created in the VPC owner account (see step 2 above).

   - "assumeRoleArn" in the "haParams" object

     The "assumeRoleArn" field should include the ARN of the IAM role that you created in the VPC owner account (see step 3 above).

     For example:

```
"haParams": {
     "assumeRoleArn":
"arn:aws:iam::642991768967:role/mediator_role_assume_fromdev"
}
```

     Learn about the Cloud Volumes ONTAP API

# Security group rules for AWS

Cloud Manager creates AWS security groups that include the inbound and outbound rules that the Connector and Cloud Volumes ONTAP need to operate successfully. You might want to refer to the ports for testing purposes or if you prefer your to use own security groups.

## Rules for Cloud Volumes ONTAP

The security group for Cloud Volumes ONTAP requires both inbound and outbound rules.

### Inbound rules

When you create a working environment and choose a predefined security group, you can choose to allow traffic within one of the following:

- **Selected VPC only**: the source for inbound traffic is the subnet range of the VPC for the Cloud Volumes ONTAP system and the subnet range of the VPC where the Connector resides. This is the recommended option.
- **All VPCs**: the source for inbound traffic is the 0.0.0.0/0 IP range.

| Protocol | Port | Purpose |
|---|---|---|
| All ICMP | All | Pinging the instance |
| HTTP | 80 | HTTP access to the System Manager web console using the IP address of the cluster management LIF |
| HTTPS | 443 | Connectivity with the Connector and HTTPS access to the System Manager web console using the IP address of the cluster management LIF |
| SSH | 22 | SSH access to the IP address of the cluster management LIF or a node management LIF |
| TCP | 111 | Remote procedure call for NFS |
| TCP | 139 | NetBIOS service session for CIFS |
| TCP | 161-162 | Simple network management protocol |
| TCP | 445 | Microsoft SMB/CIFS over TCP with NetBIOS framing |
| TCP | 635 | NFS mount |
| TCP | 749 | Kerberos |
| TCP | 2049 | NFS server daemon |
| TCP | 3260 | iSCSI access through the iSCSI data LIF |
| TCP | 4045 | NFS lock daemon |
| TCP | 4046 | Network status monitor for NFS |
| TCP | 10000 | Backup using NDMP |
| TCP | 11104 | Management of intercluster communication sessions for SnapMirror |
| TCP | 11105 | SnapMirror data transfer using intercluster LIFs |
| UDP | 111 | Remote procedure call for NFS |
| UDP | 161-162 | Simple network management protocol |
| UDP | 635 | NFS mount |
| UDP | 2049 | NFS server daemon |
| UDP | 4045 | NFS lock daemon |

| Protocol | Port | Purpose |
|---|---|---|
| UDP | 4046 | Network status monitor for NFS |
| UDP | 4049 | NFS rquotad protocol |

### Outbound rules

The predefined security group for Cloud Volumes ONTAP opens all outbound traffic. If that is acceptable, follow the basic outbound rules. If you need more rigid rules, use the advanced outbound rules.

#### Basic outbound rules

The predefined security group for Cloud Volumes ONTAP includes the following outbound rules.

| Protocol | Port | Purpose |
|---|---|---|
| All ICMP | All | All outbound traffic |
| All TCP | All | All outbound traffic |
| All UDP | All | All outbound traffic |

#### Advanced outbound rules

If you need rigid rules for outbound traffic, you can use the following information to open only those ports that are required for outbound communication by Cloud Volumes ONTAP.

The source is the interface (IP address) on the Cloud Volumes ONTAP system.

| Service | Protocol | Port | Source | Destination | Purpose |
|---|---|---|---|---|---|
| Active Directory | TCP | 88 | Node management LIF | Active Directory forest | Kerberos V authentication |
| | UDP | 137 | Node management LIF | Active Directory forest | NetBIOS name service |
| | UDP | 138 | Node management LIF | Active Directory forest | NetBIOS datagram service |
| | TCP | 139 | Node management LIF | Active Directory forest | NetBIOS service session |
| | TCP & UDP | 389 | Node management LIF | Active Directory forest | LDAP |
| | TCP | 445 | Node management LIF | Active Directory forest | Microsoft SMB/CIFS over TCP with NetBIOS framing |
| | TCP | 464 | Node management LIF | Active Directory forest | Kerberos V change & set password (SET_CHANGE) |
| | UDP | 464 | Node management LIF | Active Directory forest | Kerberos key administration |
| | TCP | 749 | Node management LIF | Active Directory forest | Kerberos V change & set Password (RPCSEC_GSS) |
| | TCP | 88 | Data LIF (NFS, CIFS, iSCSI) | Active Directory forest | Kerberos V authentication |
| | UDP | 137 | Data LIF (NFS, CIFS) | Active Directory forest | NetBIOS name service |
| | UDP | 138 | Data LIF (NFS, CIFS) | Active Directory forest | NetBIOS datagram service |
| | TCP | 139 | Data LIF (NFS, CIFS) | Active Directory forest | NetBIOS service session |
| | TCP & UDP | 389 | Data LIF (NFS, CIFS) | Active Directory forest | LDAP |
| | TCP | 445 | Data LIF (NFS, CIFS) | Active Directory forest | Microsoft SMB/CIFS over TCP with NetBIOS framing |
| | TCP | 464 | Data LIF (NFS, CIFS) | Active Directory forest | Kerberos V change & set password (SET_CHANGE) |
| | UDP | 464 | Data LIF (NFS, CIFS) | Active Directory forest | Kerberos key administration |
| | TCP | 749 | Data LIF (NFS, CIFS) | Active Directory forest | Kerberos V change & set password (RPCSEC_GSS) |

| Service | Protocol | Port | Source | Destination | Purpose |
|---|---|---|---|---|---|
| AutoSupport | HTTPS | 443 | Node management LIF | support.netapp.com | AutoSupport (HTTPS is the default) |
| | HTTP | 80 | Node management LIF | support.netapp.com | AutoSupport (only if the transport protocol is changed from HTTPS to HTTP) |
| | TCP | 3128 | Node management LIF | Connector | Sending AutoSupport messages through a proxy server on the Connector, if an outbound internet connection isn't available |
| Backup to S3 | TCP | 5010 | Intercluster LIF | Backup endpoint or restore endpoint | Back up and restore operations for the Backup to S3 feature |
| Cluster | All traffic | All traffic | All LIFs on one node | All LIFs on the other node | Intercluster communications (Cloud Volumes ONTAP HA only) |
| | TCP | 3000 | Node management LIF | HA mediator | ZAPI calls (Cloud Volumes ONTAP HA only) |
| | ICMP | 1 | Node management LIF | HA mediator | Keep alive (Cloud Volumes ONTAP HA only) |
| DHCP | UDP | 68 | Node management LIF | DHCP | DHCP client for first-time setup |
| DHCPS | UDP | 67 | Node management LIF | DHCP | DHCP server |
| DNS | UDP | 53 | Node management LIF and data LIF (NFS, CIFS) | DNS | DNS |
| NDMP | TCP | 18600–18699 | Node management LIF | Destination servers | NDMP copy |
| SMTP | TCP | 25 | Node management LIF | Mail server | SMTP alerts, can be used for AutoSupport |
| SNMP | TCP | 161 | Node management LIF | Monitor server | Monitoring by SNMP traps |
| | UDP | 161 | Node management LIF | Monitor server | Monitoring by SNMP traps |
| | TCP | 162 | Node management LIF | Monitor server | Monitoring by SNMP traps |
| | UDP | 162 | Node management LIF | Monitor server | Monitoring by SNMP traps |
| SnapMirror | TCP | 11104 | Intercluster LIF | ONTAP intercluster LIFs | Management of intercluster communication sessions for SnapMirror |
| | TCP | 11105 | Intercluster LIF | ONTAP intercluster LIFs | SnapMirror data transfer |

| Service | Protocol | Port | Source | Destination | Purpose |
|---|---|---|---|---|---|
| Syslog | UDP | 514 | Node management LIF | Syslog server | Syslog forward messages |

## Rules for the HA mediator external security group

The predefined external security group for the Cloud Volumes ONTAP HA mediator includes the following inbound and outbound rules.

### Inbound rules

The source for inbound rules is 0.0.0.0/0.

| Protocol | Port | Purpose |
|---|---|---|
| SSH | 22 | SSH connections to the HA mediator |
| TCP | 3000 | RESTful API access from the Connector |

### Outbound rules

The predefined security group for the HA mediator opens all outbound traffic. If that is acceptable, follow the basic outbound rules. If you need more rigid rules, use the advanced outbound rules.

#### Basic outbound rules

The predefined security group for the HA mediator includes the following outbound rules.

| Protocol | Port | Purpose |
|---|---|---|
| All TCP | All | All outbound traffic |
| All UDP | All | All outbound traffic |

#### Advanced outbound rules

If you need rigid rules for outbound traffic, you can use the following information to open only those ports that are required for outbound communication by the HA mediator.

| Protocol | Port | Destination | Purpose |
|---|---|---|---|
| HTTP | 80 | Connector IP address | Download upgrades for the mediator |
| HTTPS | 443 | AWS API services | Assist with storage failover |
| UDP | 53 | AWS API services | Assist with storage failover |

Rather than open ports 443 and 53, you can create an interface VPC endpoint from the target subnet to the AWS EC2 service.

## Rules for the HA configuration internal security group

The predefined internal security group for a Cloud Volumes ONTAP HA configuration includes the following rules. This security group enables communication between the HA nodes and between the mediator and the nodes.

Cloud Manager always creates this security group. You do not have the option to use your own.

### Inbound rules

The predefined security group includes the following inbound rules.

| Protocol | Port | Purpose |
|---|---|---|
| All traffic | All | Communication between the HA mediator and HA nodes |

### Outbound rules

The predefined security group includes the following outbound rules.

| Protocol | Port | Purpose |
|---|---|---|
| All traffic | All | Communication between the HA mediator and HA nodes |

## Rules for the Connector

The security group for the Connector requires both inbound and outbound rules.

### Inbound rules

| Protocol | Port | Purpose |
|---|---|---|
| SSH | 22 | Provides SSH access to the Connector host |
| HTTP | 80 | Provides HTTP access from client web browsers to the local user interface and connections from Cloud Data Sense |
| HTTPS | 443 | Provides HTTPS access from client web browsers to the local user interface |
| TCP | 3128 | Provides Cloud Volumes ONTAP with internet access to send AutoSupport messages to NetApp Support. You must manually open this port after deploying the Connector. |

### Outbound rules

The predefined security group for the Connector opens all outbound traffic. If that is acceptable, follow the basic outbound rules. If you need more rigid rules, use the advanced outbound rules.

#### Basic outbound rules

The predefined security group for the Connector includes the following outbound rules.

| Protocol | Port | Purpose |
|---|---|---|
| All TCP | All | All outbound traffic |
| All UDP | All | All outbound traffic |

#### Advanced outbound rules

If you need rigid rules for outbound traffic, you can use the following information to open only those ports that are required for outbound communication by the Connector.

The source IP address is the Connector host.

| Service | Protocol | Port | Destination | Purpose |
|---|---|---|---|---|
| API calls and AutoSupport | HTTPS | 443 | Outbound internet and ONTAP cluster management LIF | API calls to AWS and ONTAP, to Cloud Data Sense, to the Ransomware service, and sending AutoSupport messages to NetApp |
| API calls | TCP | 3000 | ONTAP HA mediator | Communication with the ONTAP HA mediator |
| | TCP | 8088 | Backup to S3 | API calls to Backup to S3 |
| DNS | UDP | 53 | DNS | Used for DNS resolve by Cloud Manager |
| Cloud Data Sense | HTTP | 80 | Cloud Data Sense instance | Cloud Data Sense for Cloud Volumes ONTAP |