Get started in Amazon Web Services

Cloud Volumes ONTAP

NetApp
September 13, 2024

Table of Contents

Get started in Amazon Web Services

Quick start for Cloud Volumes ONTAP in AWS

Get started with Cloud Volumes ONTAP in AWS in a few steps.

1 Create a Connector

If you don't have a Connector yet, an Account Admin needs to create one. Learn how to create a Connector in AWS

Note that if you want to deploy Cloud Volumes ONTAP in a subnet where no internet access is available, then you need to manually install the Connector and access the BlueXP user interface that's running on that Connector. Learn how to manually install the Connector in a location without internet access

2 Plan your configuration

BlueXP offers preconfigured packages that match your workload requirements, or you can create your own configuration. If you choose your own configuration, you should understand the options available to you. Learn more.

3 Set up your networking

a. Ensure that your VPC and subnets will support connectivity between the Connector and Cloud Volumes ONTAP.

b. Enable outbound internet access from the target VPC for NetApp AutoSupport.

   This step isn't required if you're deploying Cloud Volumes ONTAP in a location where no internet access is available.

c. Set up a VPC endpoint to the S3 service.

   A VPC endpoint is required if you want to tier cold data from Cloud Volumes ONTAP to low-cost object storage.

Learn more about networking requirements.

4 Set up the AWS KMS

If you want to use Amazon encryption with Cloud Volumes ONTAP, then you need to ensure that an active Customer Master Key (CMK) exists. You also need to modify the key policy for each CMK by adding the IAM role that provides permissions to the Connector as a *key user*. Learn more.

5 Launch Cloud Volumes ONTAP using BlueXP

Click **Add Working Environment**, select the type of system that you would like to deploy, and complete the steps in the wizard. Read step-by-step instructions.

Related links

- Create a Connector in AWS from BlueXP
- Create a Connector from the AWS Marketplace
- Install and set up a Connector on premises
- AWS permissions for the Connector

Plan your Cloud Volumes ONTAP configuration in AWS

When you deploy Cloud Volumes ONTAP in AWS, you can choose a preconfigured system that matches your workload requirements, or you can create your own configuration. If you choose your own configuration, you should understand the options available to you.

Choose a Cloud Volumes ONTAP license

Several licensing options are available for Cloud Volumes ONTAP. Each option enables you to choose a consumption model that meets your needs.

- Learn about licensing options for Cloud Volumes ONTAP
- Learn how to set up licensing

Choose a supported region

Cloud Volumes ONTAP is supported in most AWS regions. View the full list of supported regions.

Newer AWS regions must be enabled before you can create and manage resources in those regions. Learn how to enable a region.

Choose a supported Local Zone

Cloud Volumes ONTAP is supported in some AWS Local Zones including Singapore. Selecting a Local Zone is optional.

View the full list of Local Zones.
Local Zones must be enabled before you can create and manage resources in those zones.

Learn how to enable a Local Zone.

Phoenix is not a supported Local Zone.

Choose a supported instance

Cloud Volumes ONTAP supports several instance types, depending on the license type that you choose.

Supported configurations for Cloud Volumes ONTAP in AWS

Understand storage limits

The raw capacity limit for a Cloud Volumes ONTAP system is tied to the license. Additional limits impact the size of aggregates and volumes. You should be aware of these limits as you plan your configuration.

Storage limits for Cloud Volumes ONTAP in AWS

Size your system in AWS

Sizing your Cloud Volumes ONTAP system can help you meet requirements for performance and capacity. You should be aware of a few key points when choosing an instance type, disk type, and disk size:

Instance type

- Match your workload requirements to the maximum throughput and IOPS for each EC2 instance type.
- If several users write to the system at the same time, choose an instance type that has enough CPUs to manage the requests.
- If you have an application that is mostly reads, then choose a system with enough RAM.
  - AWS Documentation: Amazon EC2 Instance Types
  - AWS Documentation: Amazon EBS–Optimized Instances

EBS disk type

At a high level, the differences between EBS disk types are as follows. To learn more about the use cases for EBS disks, refer to AWS Documentation: EBS Volume Types.

- *General Purpose SSD (gp3)* disks are the lowest-cost SSDs that balance cost and performance for a broad range of workloads. Performance is defined in terms of IOPS and throughput. gp3 disks are supported with Cloud Volumes ONTAP 9.7 and later.

  When you select a gp3 disk, BlueXP fills in default IOPS and throughput values that provide performance that is equivalent to a gp2 disk based on the selected disk size. You can increase the values to get better performance at a higher cost, but we do not support lower values because it can result in inferior performance. In short, stick with the default values or increase them. Don't lower them. Learn more about gp3 disks and their performance.

  Note that Cloud Volumes ONTAP supports the Amazon EBS Elastic Volumes feature with gp3 disks. Learn more about Elastic Volumes support.

- *General Purpose SSD (gp2)* disks balance cost and performance for a broad range of workloads. Performance is defined in terms of IOPS.
- *Provisioned IOPS SSD (io1)* disks are for critical applications that require the highest performance at a higher cost.

  Note that Cloud Volumes ONTAP supports the Amazon EBS Elastic Volumes feature with io1 disks. Learn more about Elastic Volumes support.

- *Throughput Optimized HDD (st1)* disks are for frequently accessed workloads that require fast and consistent throughput at a lower price.

  Tiering data to object storage is not recommended when using Throughput Optimized HDDs (st1).

EBS disk size

If you choose a configuration that doesn't support the Amazon EBS Elastic Volumes feature, then you need to choose an initial disk size when you launch a Cloud Volumes ONTAP system. After that, you can let BlueXP manage a system's capacity for you, but if you want to create aggregates yourself, be aware of the following:

- All disks in an aggregate must be the same size.
- The performance of EBS disks is tied to disk size. The size determines the baseline IOPS and maximum burst duration for SSD disks and the baseline and burst throughput for HDD disks.
- Ultimately, you should choose the disk size that gives you the *sustained performance* that you need.
- Even if you do choose larger disks (for example, six 4 TiB disks), you might not get all of the IOPS because the EC2 instance can reach its bandwidth limit.

  For more details about EBS disk performance, refer to AWS Documentation: EBS Volume Types.

  As noted above, choosing a disk size is not supported with Cloud Volumes ONTAP configurations that support the Amazon EBS Elastic Volumes feature. Learn more about Elastic Volumes support.

View default system disks

In addition to the storage for user data, BlueXP also purchases cloud storage for Cloud Volumes ONTAP system data (boot data, root data, core data, and NVRAM). For planning purposes, it might help for you to review these details before you deploy Cloud Volumes ONTAP.

View the default disks for Cloud Volumes ONTAP system data in AWS.

The Connector also requires a system disk. View details about the Connector's default configuration.

Prepare to deploy Cloud Volumes ONTAP in an AWS Outpost

If you have an AWS Outpost, you can deploy Cloud Volumes ONTAP in that Outpost by selecting the Outpost VPC in the Working Environment wizard. The experience is the same as any other VPC that resides in AWS. Note that you will need to first deploy a Connector in your AWS Outpost.

There are a few limitations to point out:

- Only single node Cloud Volumes ONTAP systems are supported at this time
- The EC2 instances that you can use with Cloud Volumes ONTAP are limited to what's available in your Outpost
- Only General Purpose SSDs (gp2) are supported at this time

Collect networking information

When you launch Cloud Volumes ONTAP in AWS, you need to specify details about your VPC network. You can use a worksheet to collect the information from your administrator.

Single node or HA pair in a single AZ

AWS information	Your value
Region	
VPC	
Subnet	

AWS information	Your value
Security group (if using your own)	

HA pair in multiple AZs

AWS information	Your value
Region	
VPC	
Security group (if using your own)	
Node 1 availability zone	
Node 1 subnet	
Node 2 availability zone	
Node 2 subnet	
Mediator availability zone	
Mediator subnet	
Key pair for the mediator	
Floating IP address for cluster management port	
Floating IP address for data on node 1	
Floating IP address for data on node 2	
Route tables for floating IP addresses	

Choose a write speed

BlueXP enables you to choose a write speed setting for Cloud Volumes ONTAP. Before you choose a write speed, you should understand the differences between the normal and high settings and risks and recommendations when using high write speed. Learn more about write speed.

Choose a volume usage profile

ONTAP includes several storage efficiency features that can reduce the total amount of storage that you need. When you create a volume in BlueXP, you can choose a profile that enables these features or a profile that disables them. You should learn more about these features to help you decide which profile to use.

NetApp storage efficiency features provide the following benefits:

Thin provisioning

Presents more logical storage to hosts or users than you actually have in your physical storage pool. Instead of preallocating storage space, storage space is allocated dynamically to each volume as data is

written.

Deduplication

Improves efficiency by locating identical blocks of data and replacing them with references to a single shared block. This technique reduces storage capacity requirements by eliminating redundant blocks of data that reside in the same volume.

Compression

Reduces the physical capacity required to store data by compressing data within a volume on primary, secondary, and archive storage.

Set up your networking

Networking requirements for Cloud Volumes ONTAP in AWS

BlueXP 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 to contact the following endpoints for day-to-day operations.

Cloud Volumes ONTAP endpoints

Cloud Volumes ONTAP requires outbound internet access to contact various endpoints for day-to-day operations.

The following endpoints are specific to Cloud Volumes ONTAP. The Connector also contacts several endpoints for day-to-day operations, as well as the BlueXP web-based console. Refer to View endpoints contacted from the Connector and Prepare networking for using the BlueXP console.

Endpoints	Applicable for	Purpose	BlueXP deployment modes	Impact if endpoint is not available
https://netapp-cloud-account.auth0.com	Authentication	Used for BlueXP authentication.	Standard and restricted modes.	User authentication fails and the following services remain unavailable: • Cloud Volumes ONTAP services • ONTAP services • Protocols and proxy services
https://keyvault-production-aks.vault.azure.net	Key Vault	Used to retrieve client secret key from the Azure Key Vault to communicate with S3 buckets for metadata handling. Cloud Volumes ONTAP service uses this component internally.	Standard, restricted, and private modes.	Cloud Volumes ONTAP services are unavailable.
https://cloudmanager.cloud.netapp.com/tenancy	Tenancy	Used to retrieve the Cloud Volumes ONTAP resources from BlueXP tenancy to authorize resources and users.	Standard and restricted modes.	Cloud Volumes ONTAP resources and the users are not authorized.
https://support.netapp.com/aods/asupmessage https://support.netapp.com/asupprod/post/1.0/postAsup	AutoSupport	Used to send AutoSupport telemetry data to NetApp support.	Standard and restricted modes.	AutoSupport information remains undelivered.
The exact commercial endpoint for AWS service (suffixed with `amazonaws.com`) depends on the AWS region that you are using. Refer to AWS documentation for details.	• CloudFormation • Elastic Compute Cloud (EC2) • Identity and Access Management (IAM) • Key Management Service (KMS) • Security Token Service (STS) • Simple Storage Service (S3)	Communication with AWS services.	Standard and private modes.	Cloud Volumes ONTAP cannot communicate with AWS service to perform specific BlueXP operations on AWS.

Endpoints	Applicable for	Purpose	BlueXP deployment modes	Impact if endpoint is not available
The exact government endpoint for AWS service depends on the AWS region that you are using. The endpoints are suffixed with `amazonaws.com` and `c2s.ic.gov`. Refer to AWS SDK and Amazon documentation for more information.	• CloudFormation • Elastic Compute Cloud (EC2) • Identity and Access Management (IAM) • Key Management Service (KMS) • Security Token Service (STS) • Simple Storage Service (S3)	Communication with AWS services.	Restricted mode.	Cloud Volumes ONTAP cannot communicate with AWS service to perform specific BlueXP operations on AWS.

Outbound internet access for NetApp AutoSupport

Cloud Volumes ONTAP nodes require outbound internet access for accessing external endpoints for various functions. Cloud Volumes ONTAP can't operate properly if these endpoints are blocked in environments with strict security requirements.

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, BlueXP 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 BlueXP 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 the AWS Documentation: Interface VPC Endpoints (AWS PrivateLink).

Private IP addresses

BlueXP 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 BlueXP 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

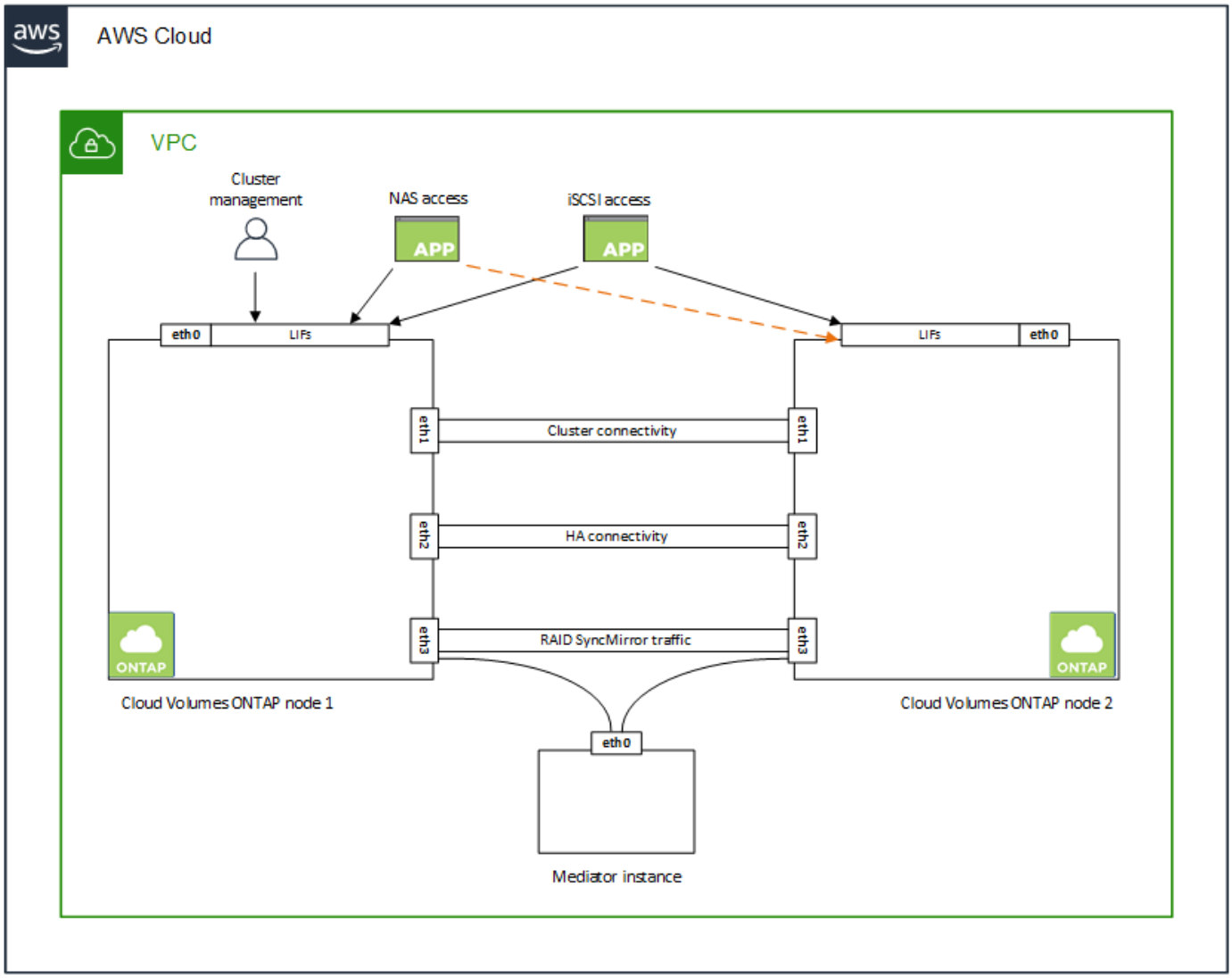
BlueXP allocates 6 IP addresses to a single node system.

The following table provides details about the LIFs that are associated with each private IP address.

LIF	Purpose
Cluster management	Administrative management of the entire cluster (HA pair).
Node management	Administrative management of a node.
Intercluster	Cross-cluster communication, backup, and replication.
NAS data	Client access over NAS protocols.
iSCSI data	Client access over the iSCSI protocol. Also used by the system for other important networking workflows. This LIF is required and should not be deleted.
Storage VM management	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. Also used by the system for other 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. These LIFs also manage the migration of floating IP addresses between nodes. 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.

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 don't need to create security groups because BlueXP does that for you. If you need to use your own, refer to Security group rules.

Looking for information about the Connector? View security group rules for the Connector

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, refer to the 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, refer to the 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, refer to the 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 the 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 BlueXP when you create the working environment.

To understand how HA pairs work, refer to 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.

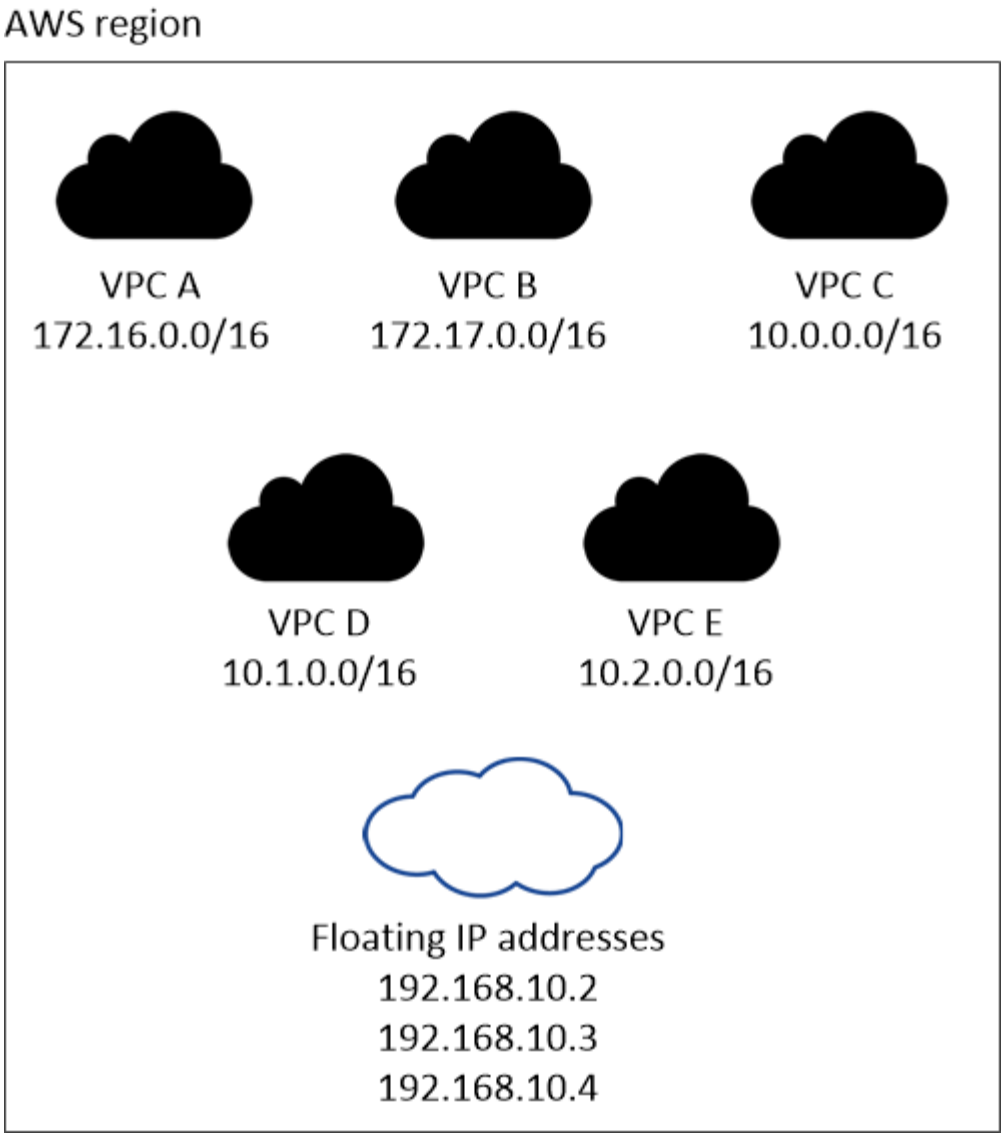
One floating IP address is for cluster management, one is for NFS/CIFS data on node 1, and one is for NFS/CIFS data on node 2. A fourth floating IP address for SVM management is optional.

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 BlueXP when you create a Cloud Volumes ONTAP HA working environment. BlueXP 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.



BlueXP 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 BlueXP, 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 BlueXP 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 the AWS Documentation: Route Tables.

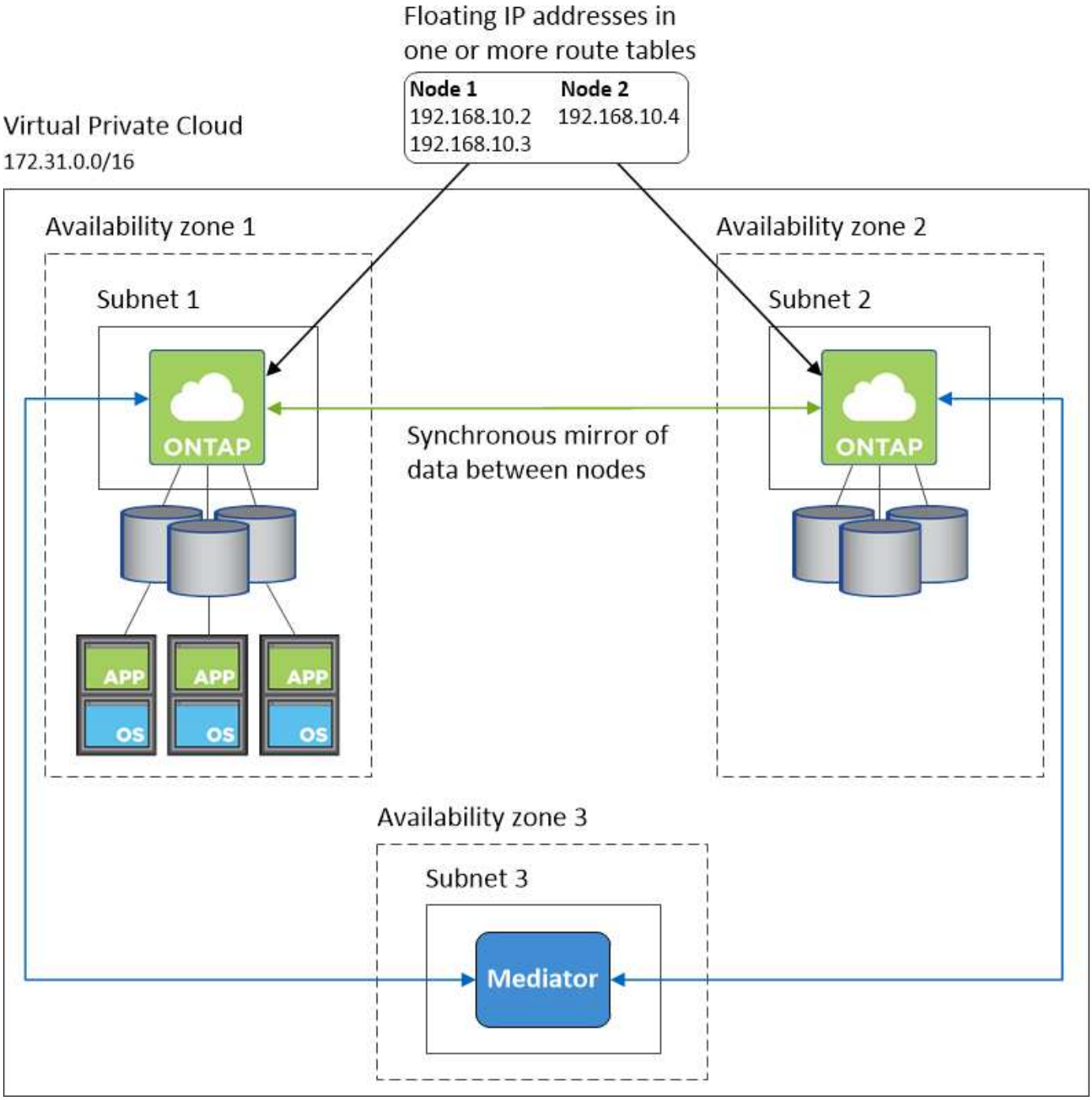
Connection to NetApp management tools

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

If you haven't created a Connector yet, you should review networking requirements for the Connector as well.

- View networking requirements for the Connector
- Security group rules in AWS

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

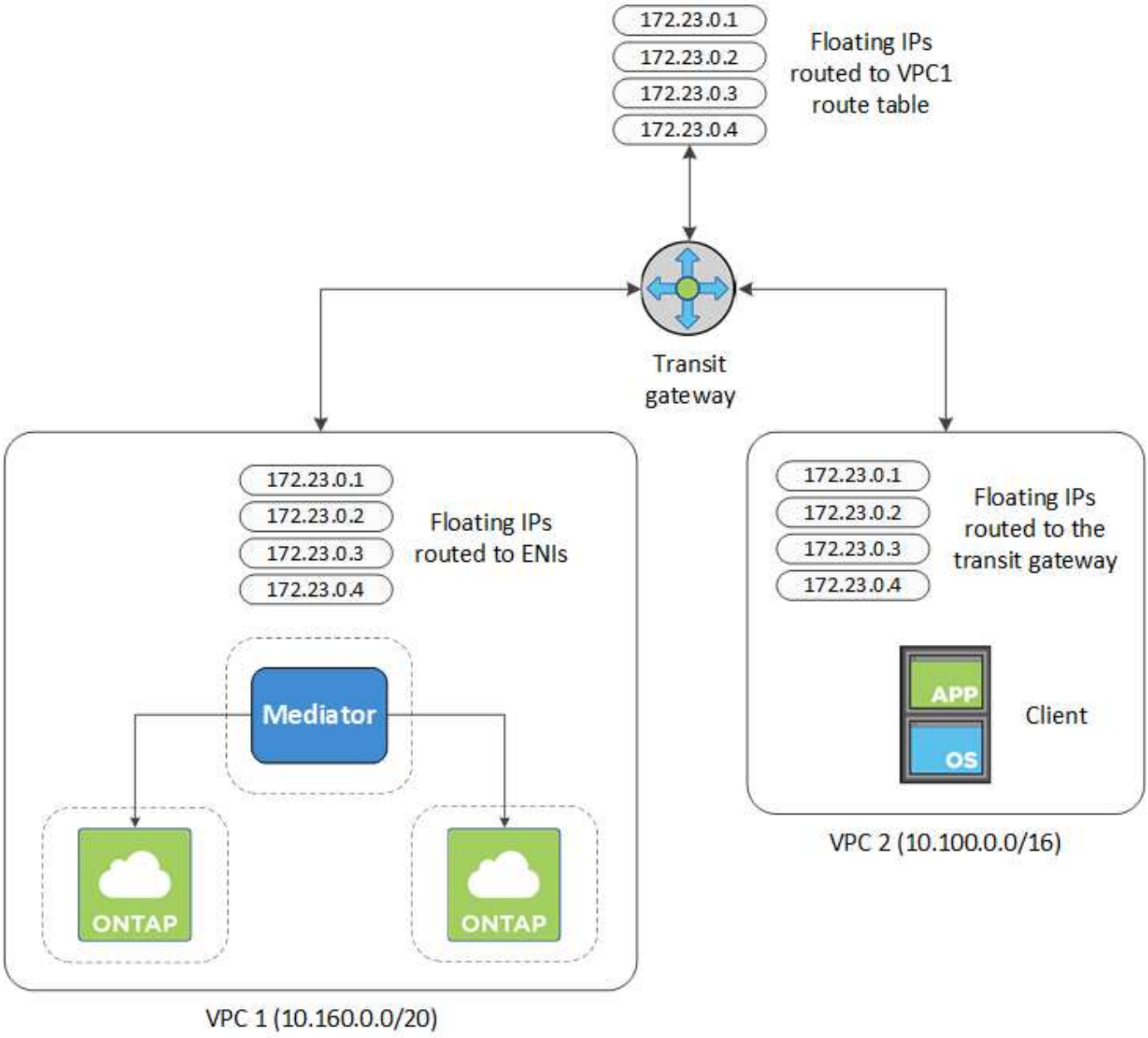
Set up an AWS transit gateway to enable access to an HA pair's floating IP addresses from outside the VPC where the HA pair resides.

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.

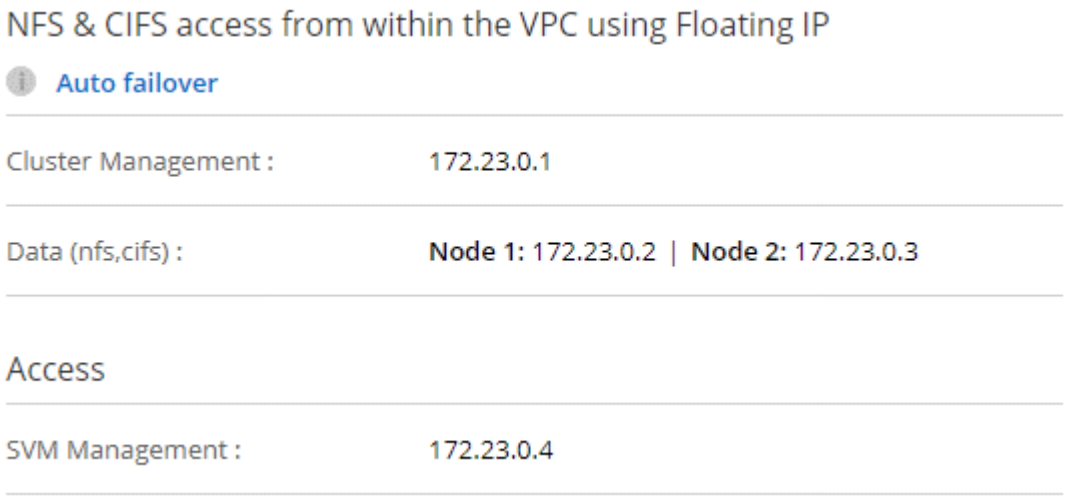


The following steps illustrate how to set up a similar configuration.

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.

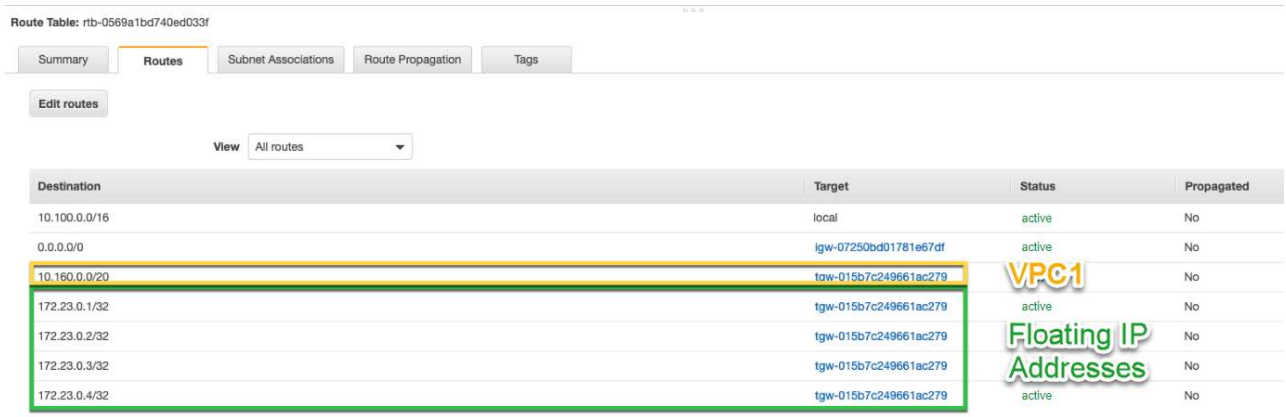
   You can find the floating IP addresses on the Working Environment Information page in BlueXP. Here's an example:



   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.

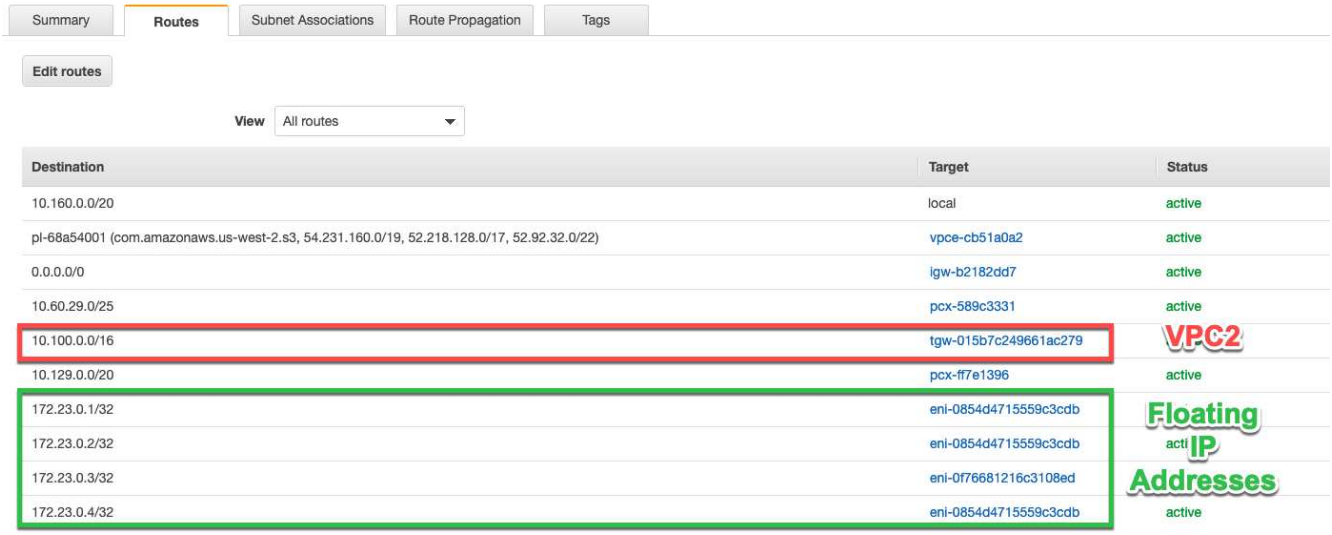
The following sample image shows the route table for VPC 2, which includes routes to VPC 1 and the floating IP addresses.



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.

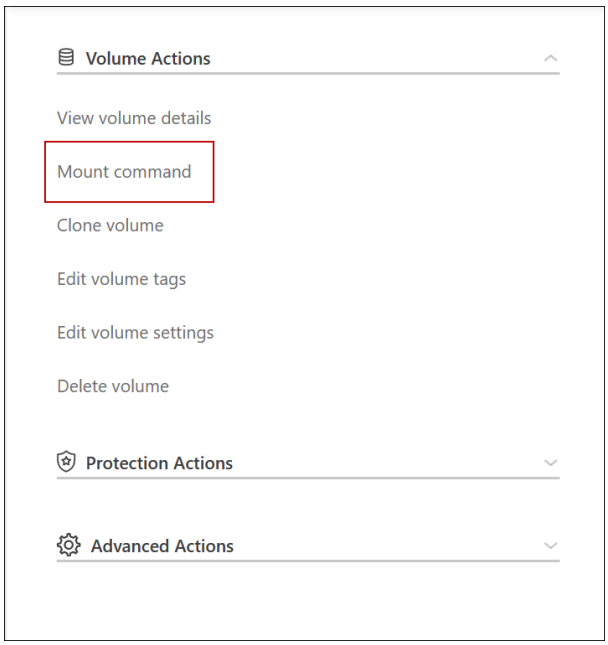
   The following sample image shows the route table for VPC 1. It includes a route to the floating IP addresses and to VPC 2, which is where a client resides. BlueXP automatically added the floating IPs to the route table when it deployed the HA pair.



6. Update the security groups settings to All traffic for the VPC.
   a. Under Virtual Private Cloud, click **Subnets**.
   b. Click the **Route table** tab, select the desired environment for one of the floating IP addresses for an HA pair.
   c. Click **Security groups**.
   d. Select **Edit Inbound Rules**.
   e. Click **Add rule**.
   f. Under Type, select **All traffic**, and then select the VPC IP address.
   g. Click **Save Rules** to apply the changes.

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

   You can find the correct IP address in BlueXP through the **Mount Command** option under the Manage Volumes panel in BlueXP.



8. 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

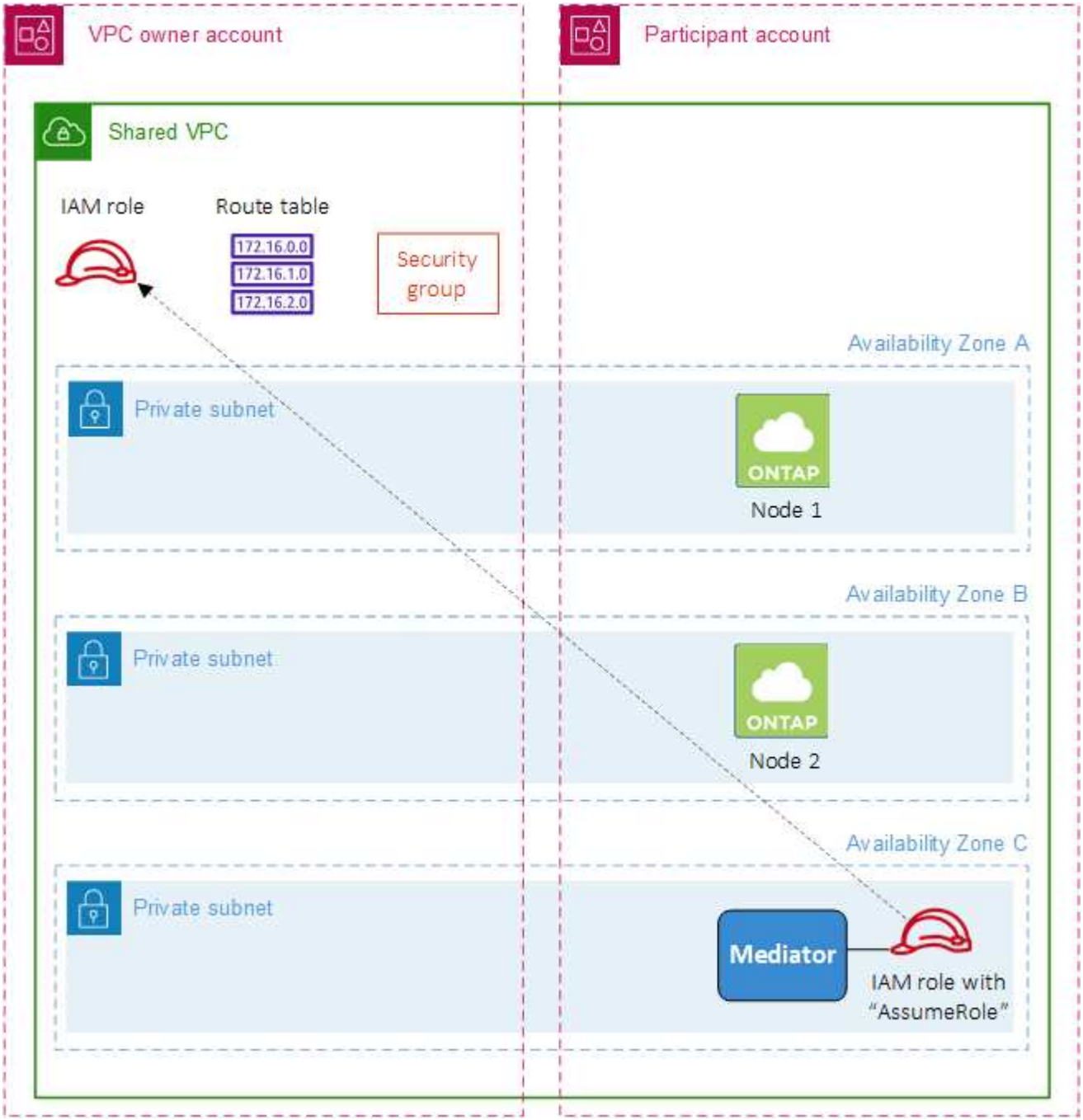
Starting with the 9.11.1 release, Cloud Volumes ONTAP HA pairs are supported in AWS with VPC sharing. VPC sharing enables your organization to share subnets with other AWS accounts. To use this configuration, you must set up your AWS environment and then deploy the HA pair using the API.

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, BlueXP 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. BlueXP 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 BlueXP 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

BlueXP creates AWS security groups that include the inbound and outbound rules that Cloud Volumes ONTAP needs to operate successfully. You might want to refer to the ports for testing purposes or if you prefer to use your 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 ONTAP System Manager web console using the IP address of the cluster management LIF
HTTPS	443	Connectivity with the Connector and HTTPS access to the ONTAP 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)
Configuration backups	HTTP	80	Node management LIF	http://<connector-IP-address>/occm/offboxconfig	Send configuration backups to the Connector. Learn about configuration backup files.
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

Service	Protocol	Port	Source	Destination	Purpose
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
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 predefined security group for the HA mediator includes the following inbound rule.

Protocol	Port	Source	Purpose
TCP	3000	CIDR of the Connector	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	IP address of the Connector on AWS EC2 instance	Download upgrades for the mediator
HTTPS	443	ec2.amazonaws.com	Assist with storage failover
UDP	53	ec2.amazonaws.com	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.

BlueXP 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

View security group rules for the Connector

Setting up the AWS KMS

If you want to use Amazon encryption with Cloud Volumes ONTAP, then you need to set up the AWS Key Management Service (KMS).

Steps

1. Ensure that an active Customer Master Key (CMK) exists.

   The CMK can be an AWS-managed CMK or a customer-managed CMK. It can be in the same AWS account as BlueXP and Cloud Volumes ONTAP or in a different AWS account.

   AWS Documentation: Customer Master Keys (CMKs)

2. Modify the key policy for each CMK by adding the IAM role that provides permissions to BlueXP as a *key user*.

   Adding the IAM role as a key user gives BlueXP permissions to use the CMK with Cloud Volumes ONTAP.

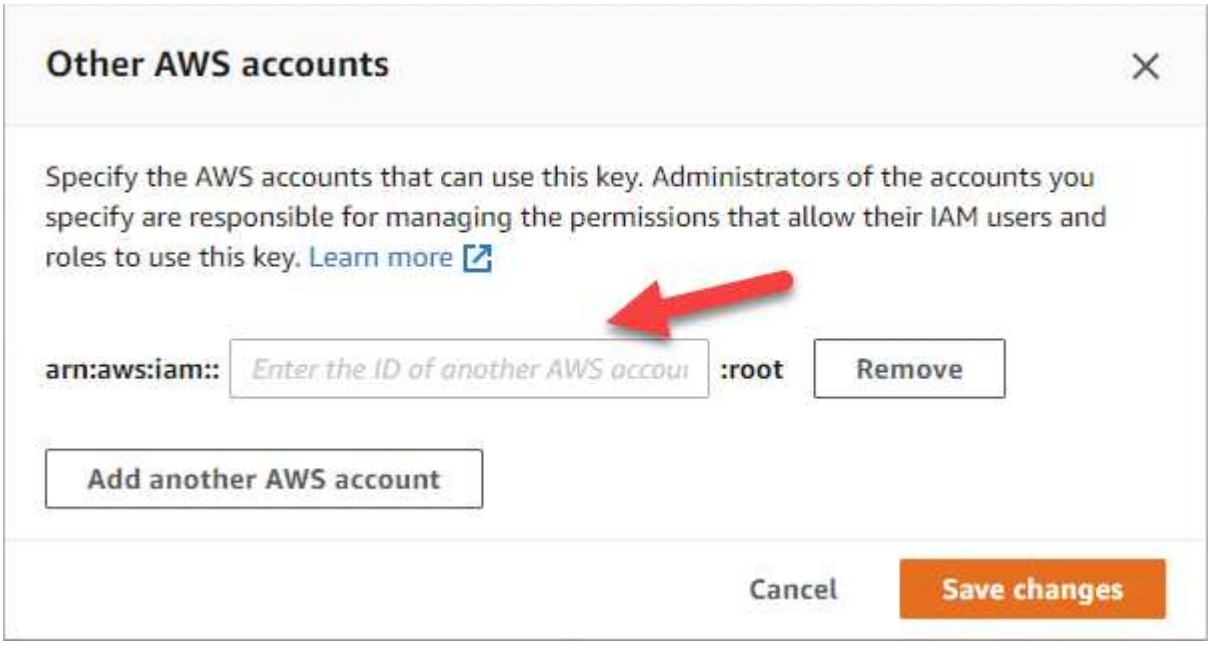
   AWS Documentation: Editing Keys

3. If the CMK is in a different AWS account, complete the following steps:
   a. Go to the KMS console from the account where the CMK resides.
   b. Select the key.
   c. In the **General configuration** pane, copy the ARN of the key.

      You'll need to provide the ARN to BlueXP when you create the Cloud Volumes ONTAP system.

   d. In the **Other AWS accounts** pane, add the AWS account that provides BlueXP with permissions.

      In most cases, this is the account where BlueXP resides. If BlueXP wasn't installed in AWS, it would be the account for which you provided AWS access keys to BlueXP.



   e. Now switch to the AWS account that provides BlueXP with permissions and open the IAM console.
   f. Create an IAM policy that includes the permissions listed below.
   g. Attach the policy to the IAM role or IAM user that provides permissions to BlueXP.

      The following policy provides the permissions that BlueXP needs to use the CMK from the external AWS account. Be sure to modify the region and account ID in the "Resource" sections.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowUseOfTheKey",
            "Effect": "Allow",
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:ReEncrypt*",
                "kms:GenerateDataKey*",
                "kms:DescribeKey"
            ],
            "Resource": [
                "arn:aws:kms:us-east-
1:externalaccountid:key/externalkeyid"
            ]
        },
        {
            "Sid": "AllowAttachmentOfPersistentResources",
            "Effect": "Allow",
            "Action": [
                "kms:CreateGrant",
                "kms:ListGrants",
                "kms:RevokeGrant"
            ],
            "Resource": [
                "arn:aws:kms:us-east-
1:externalaccountid:key/externalaccountid"
            ],
            "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": true
                }
            }
        }
    ]
}
```

For additional details about this process, refer to the AWS Documentation: Allowing users in other accounts to use a KMS key.

4. If you are using a customer-managed CMK, modify the key policy for the CMK by adding the Cloud Volumes ONTAP IAM role as a *key user*.

   This step is required if you enabled data tiering on Cloud Volumes ONTAP and want to encrypt the data

stored in the S3 bucket.

You'll need to perform this step *after* you deploy Cloud Volumes ONTAP because the IAM role is created when you create a working environment. (Of course, you do have the option to use an existing Cloud Volumes ONTAP IAM role, so it's possible to perform this step before.)

AWS Documentation: Editing Keys

Set up IAM roles for Cloud Volumes ONTAP

IAM roles with the required permissions must be attached to each Cloud Volumes ONTAP node. The same is true for the HA mediator. It's easiest to let BlueXP create the IAM roles for you, but you can use your own roles.

This task is optional. When you create a Cloud Volumes ONTAP working environment, the default option is to let BlueXP create the IAM roles for you. If your business's security policies require you to create the IAM roles yourself, then follow the steps below.

Providing your own IAM role is required in AWS Secret Cloud. Learn how to deploy Cloud Volumes ONTAP in C2S.

Steps

1. Go to the AWS IAM console.
2. Create IAM policies that include the following permissions:
    - Base policy for Cloud Volumes ONTAP nodes

Standard regions

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Action": "s3:ListAllMyBuckets",
            "Resource": "arn:aws:s3:::*",
            "Effect": "Allow"
        }, {
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws:s3:::fabric-pool-*",
            "Effect": "Allow"
        }, {
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject"
            ],
            "Resource": "arn:aws:s3:::fabric-pool-*",
            "Effect": "Allow"
        }
    ]
}
```

GovCloud (US) regions

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Action": "s3:ListAllMyBuckets",
        "Resource": "arn:aws-us-gov:s3:::*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:ListBucket",
            "s3:GetBucketLocation"
        ],
        "Resource": "arn:aws-us-gov:s3:::fabric-pool-*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:GetObject",
            "s3:PutObject",
            "s3:DeleteObject"
        ],
        "Resource": "arn:aws-us-gov:s3:::fabric-pool-*",
        "Effect": "Allow"
    }]
}
```

Top Secret regions

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Action": "s3:ListAllMyBuckets",
        "Resource": "arn:aws-iso:s3:::*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:ListBucket",
            "s3:GetBucketLocation"
        ],
        "Resource": "arn:aws-iso:s3:::fabric-pool-*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:GetObject",
            "s3:PutObject",
            "s3:DeleteObject"
        ],
        "Resource": "arn:aws-iso:s3:::fabric-pool-*",
        "Effect": "Allow"
    }]
}
```

Secret regions

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Action": "s3:ListAllMyBuckets",
        "Resource": "arn:aws-iso-b:s3:::*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:ListBucket",
            "s3:GetBucketLocation"
        ],
        "Resource": "arn:aws-iso-b:s3:::fabric-pool-*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:GetObject",
            "s3:PutObject",
            "s3:DeleteObject"
        ],
        "Resource": "arn:aws-iso-b:s3:::fabric-pool-*",
        "Effect": "Allow"
    }]
}
```

- Backup policy for Cloud Volumes ONTAP nodes

  If you plan to use BlueXP backup and recovery with your Cloud Volumes ONTAP systems, the IAM role for the nodes must include the second policy shown below.

Standard regions

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws:s3:::netapp-backup*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject",
                "s3:ListAllMyBuckets",
                "s3:PutObjectTagging",
                "s3:GetObjectTagging",
                "s3:RestoreObject",
                "s3:GetBucketObjectLockConfiguration",
                "s3:GetObjectRetention",
                "s3:PutBucketObjectLockConfiguration",
                "s3:PutObjectRetention"
            ],
            "Resource": "arn:aws:s3:::netapp-backup*/*",
            "Effect": "Allow"
        }
    ]
}
```

GovCloud (US) regions

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws-us-gov:s3:::netapp-backup*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject",
                "s3:ListAllMyBuckets",
                "s3:PutObjectTagging",
                "s3:GetObjectTagging",
                "s3:RestoreObject",
                "s3:GetBucketObjectLockConfiguration",
                "s3:GetObjectRetention",
                "s3:PutBucketObjectLockConfiguration",
                "s3:PutObjectRetention"
            ],
            "Resource": "arn:aws-us-gov:s3:::netapp-backup*/*",
            "Effect": "Allow"
        }
    ]
}
```

Top Secret regions

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws-iso:s3:::netapp-backup*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject",
                "s3:ListAllMyBuckets",
                "s3:PutObjectTagging",
                "s3:GetObjectTagging",
                "s3:RestoreObject",
                "s3:GetBucketObjectLockConfiguration",
                "s3:GetObjectRetention",
                "s3:PutBucketObjectLockConfiguration",
                "s3:PutObjectRetention"
            ],
            "Resource": "arn:aws-iso:s3:::netapp-backup*/*",
            "Effect": "Allow"
        }
    ]
}
```

Secret regions

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws-iso-b:s3:::netapp-backup*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject",
                "s3:ListAllMyBuckets",
                "s3:PutObjectTagging",
                "s3:GetObjectTagging",
                "s3:RestoreObject",
                "s3:GetBucketObjectLockConfiguration",
                "s3:GetObjectRetention",
                "s3:PutBucketObjectLockConfiguration",
                "s3:PutObjectRetention"
            ],
            "Resource": "arn:aws-iso-b:s3:::netapp-backup*/*",
            "Effect": "Allow"
        }
    ]
}
```

- HA mediator

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "ec2:AssignPrivateIpAddresses",
                "ec2:CreateRoute",
                "ec2:DeleteRoute",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRouteTables",
                "ec2:DescribeVpcs",
                "ec2:ReplaceRoute",
                "ec2:UnassignPrivateIpAddresses",
                "sts:AssumeRole",
                "ec2:DescribeSubnets"
            ],
            "Resource": "*"
        }
    ]
}
```

3. Create an IAM role and attach the policies that you created to the role.

Result

You now have IAM roles that you can select when you create a new Cloud Volumes ONTAP working environment.

More information

- AWS documentation: Creating IAM policies
- AWS documentation: Creating IAM roles

Set up licensing for Cloud Volumes ONTAP in AWS

After you decide which licensing option you want to use with Cloud Volumes ONTAP, a few steps are required before you can choose that licensing option when creating a new working environment.

Freemium

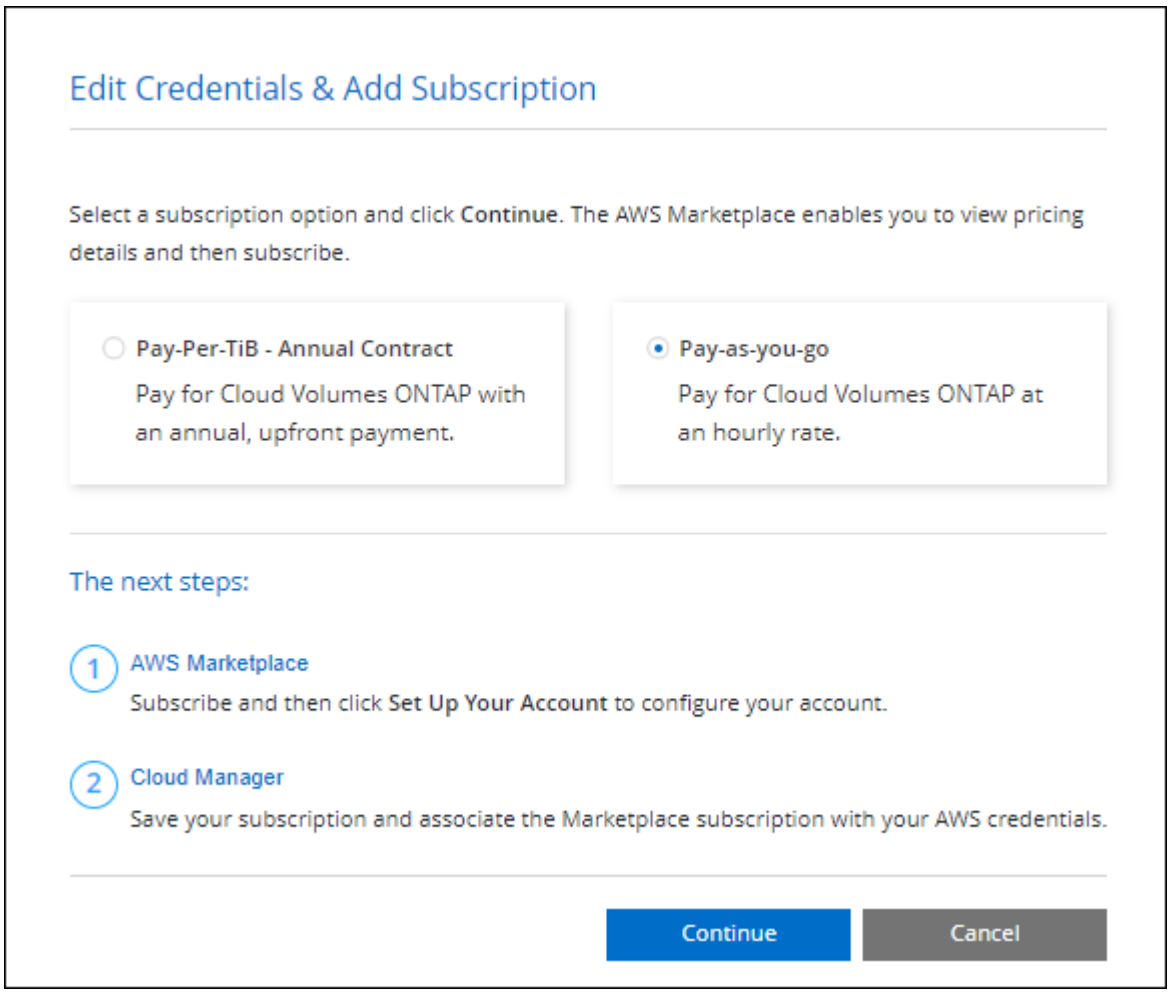
Select the Freemium offering to use Cloud Volumes ONTAP free of charge with up to 500 GiB of provisioned capacity. Learn more about the Freemium offering.

Steps

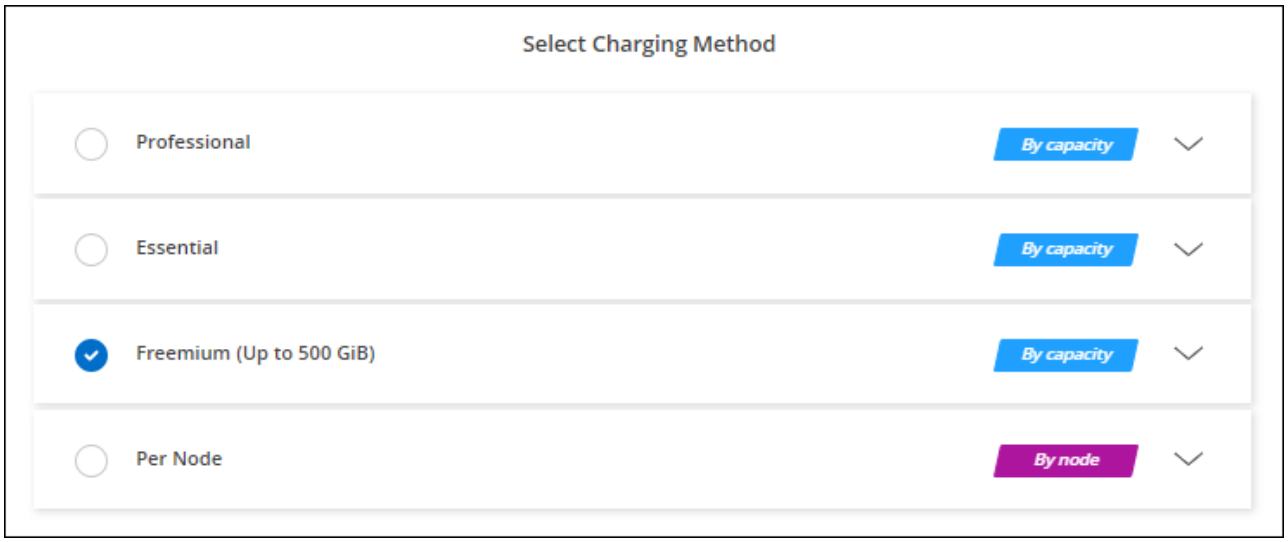
1. From the left navigation menu, select **Storage > Canvas**.
2. On the Canvas page, click **Add Working Environment** and follow the steps in BlueXP.

a. On the **Details and Credentials** page, click **Edit Credentials > Add Subscription** and then follow the prompts to subscribe to the pay-as-you-go offering in the AWS Marketplace.

   You won't be charged through the marketplace subscription unless you exceed 500 GiB of provisioned capacity, at which time the system is automatically converted to the Essentials package.



b. After you return to BlueXP, select **Freemium** when you reach the charging methods page.



View step-by-step instructions to launch Cloud Volumes ONTAP in AWS.

Capacity-based license

Capacity-based licensing enables you to pay for Cloud Volumes ONTAP per TiB of capacity. Capacity-based licensing is available in the form of a *package*: the Essentials package or the Professional package.

The Essentials and Professional packages are available with the following consumption models:

- A license (BYOL) purchased from NetApp
- An hourly, pay-as-you-go (PAYGO) subscription from the AWS Marketplace
- An annual contract from the AWS Marketplace

Learn more about capacity-based licensing.

The following sections describe how to get started with each of these consumption models.

BYOL

Pay upfront by purchasing a license (BYOL) from NetApp to deploy Cloud Volumes ONTAP systems in any cloud provider.

Steps

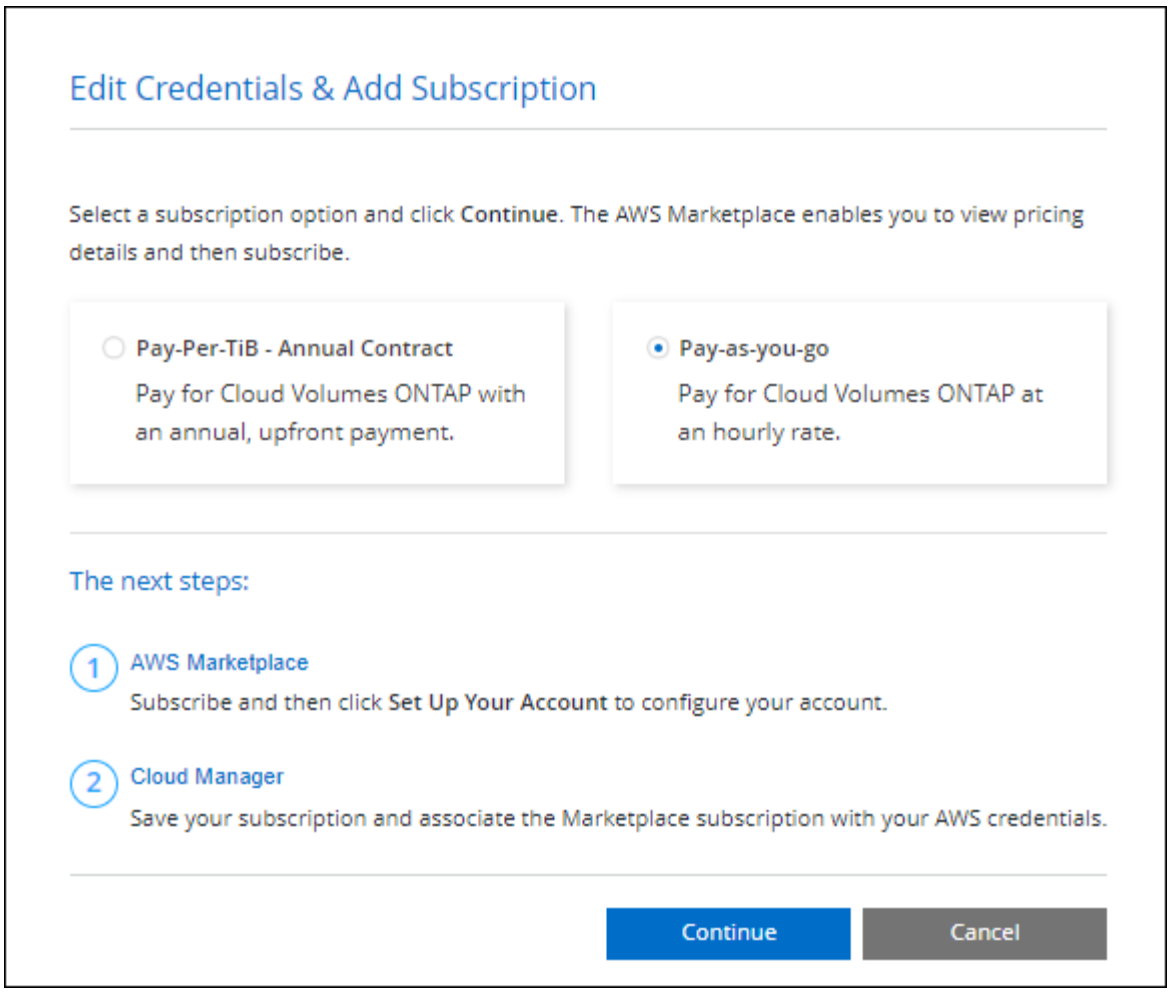
1. Contact NetApp Sales to obtain a license
2. Add your NetApp Support Site account to BlueXP

   BlueXP automatically queries NetApp's licensing service to obtain details about the licenses associated with your NetApp Support Site account. If there are no errors, BlueXP automatically adds the licenses to the digital wallet.

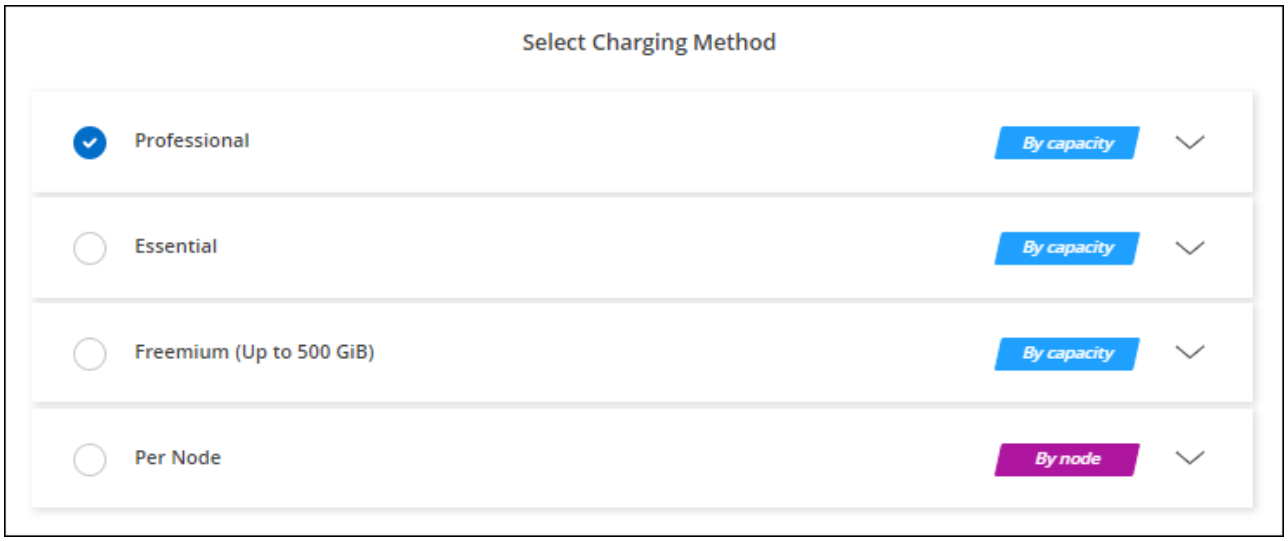
   Your license must be available from the BlueXP digital wallet before you can use it with Cloud Volumes ONTAP. If needed, you can manually add the license to the BlueXP digital wallet.

3. On the Canvas page, click **Add Working Environment** and follow the steps in BlueXP.
   a. On the **Details and Credentials** page, click **Edit Credentials > Add Subscription** and then follow the prompts to subscribe to the pay-as-you-go offering in the AWS Marketplace.

      The license that you purchased from NetApp is always charged first, but you'll be charged from the hourly rate in the marketplace if you exceed your licensed capacity or if the term of your license expires.



b. After you return to BlueXP, select a capacity-based package when you reach the charging methods page.



View step-by-step instructions to launch Cloud Volumes ONTAP in AWS.

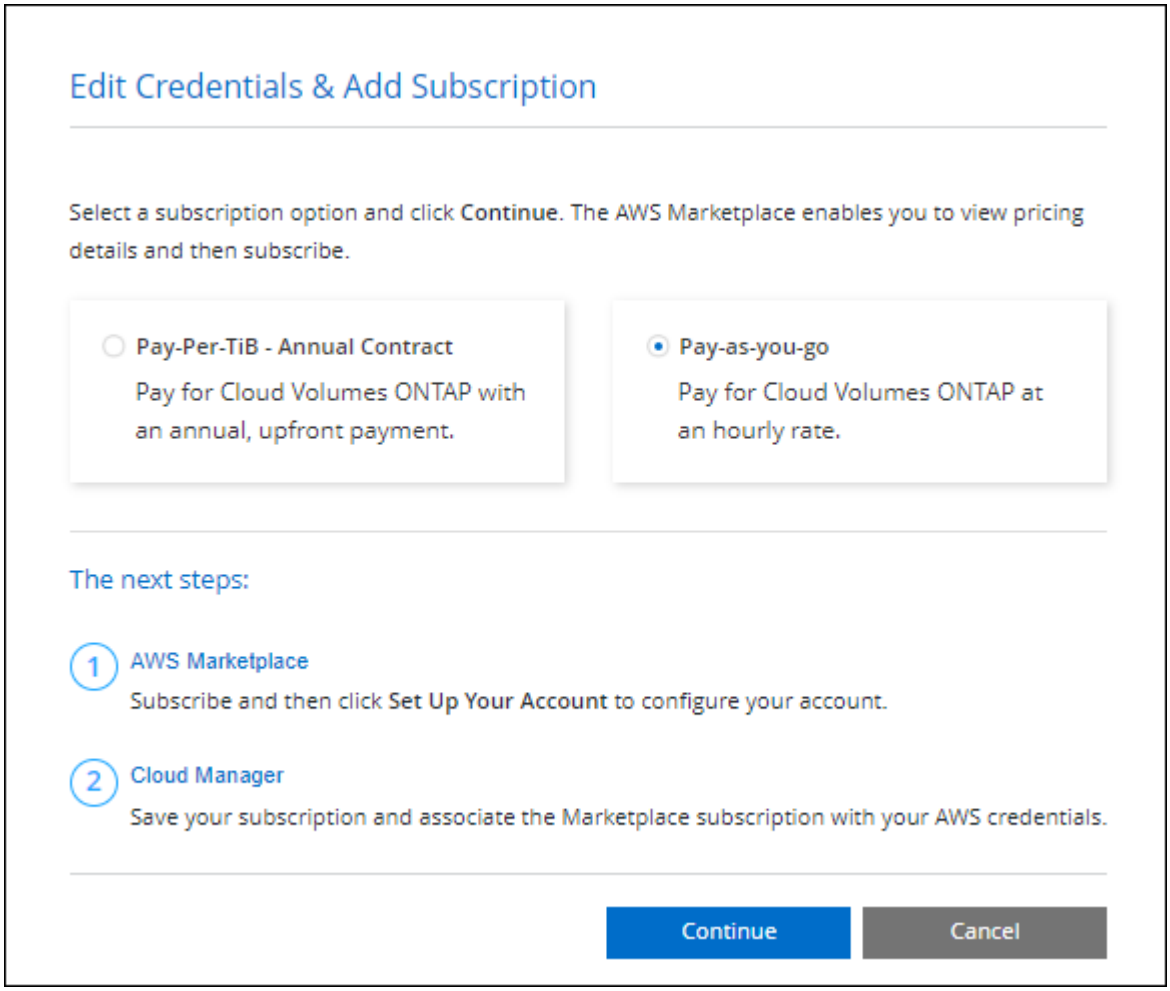
PAYGO subscription

Pay hourly by subscribing to the offer from your cloud provider's marketplace.

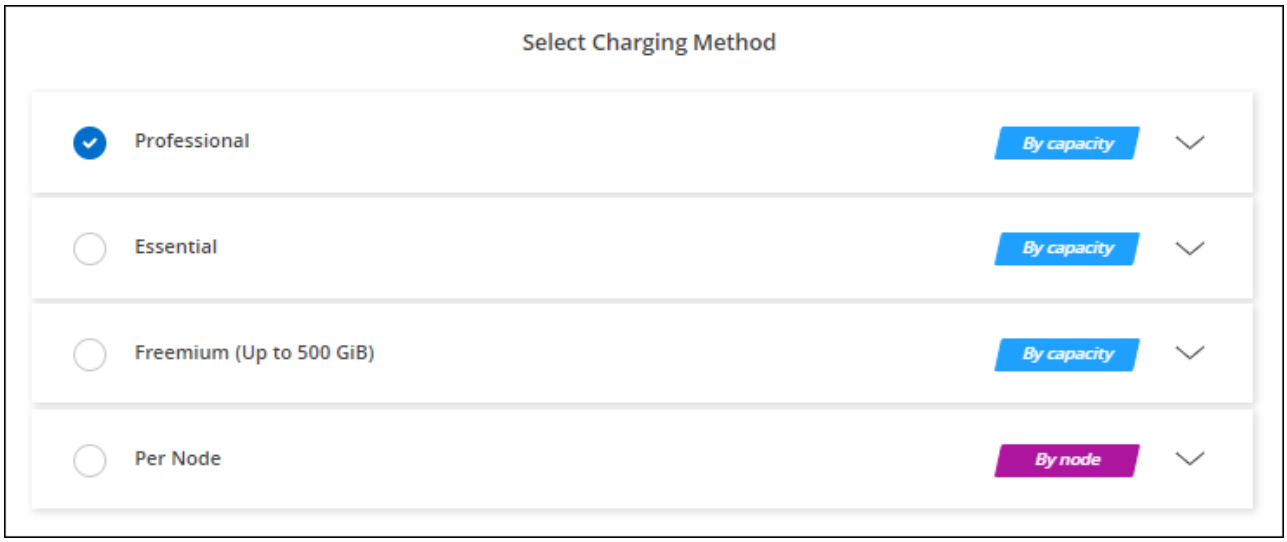
When you create a Cloud Volumes ONTAP working environment, BlueXP prompts you to subscribe to the agreement that's available in the AWS Marketplace. That subscription is then associated with the working environment for charging. You can use that same subscription for additional working environments.

Steps

1. From the left navigation menu, select **Storage > Canvas**.
2. On the Canvas page, click **Add Working Environment** and follow the steps in BlueXP.
   a. On the **Details and Credentials** page, click **Edit Credentials > Add Subscription** and then follow the prompts to subscribe to the pay-as-you-go offering in the AWS Marketplace.



   b. After you return to BlueXP, select a capacity-based package when you reach the charging methods page.



View step-by-step instructions to launch Cloud Volumes ONTAP in AWS.

You can manage the AWS Marketplace subscriptions associated with your AWS accounts from the Settings > Credentials page. Learn how to manage your AWS accounts and subscriptions

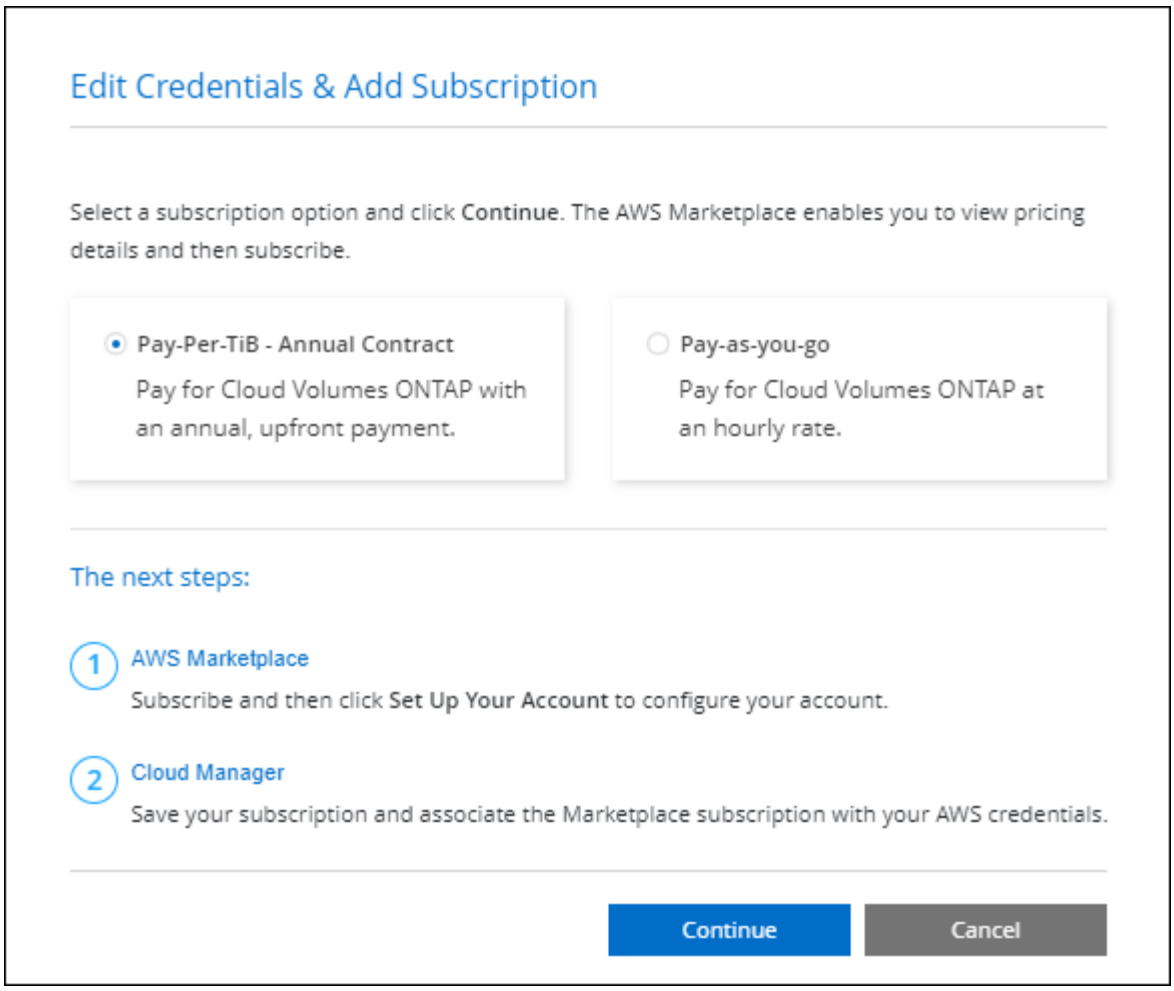
Annual contract

Pay annually by purchasing an annual contract from your cloud provider's marketplace.

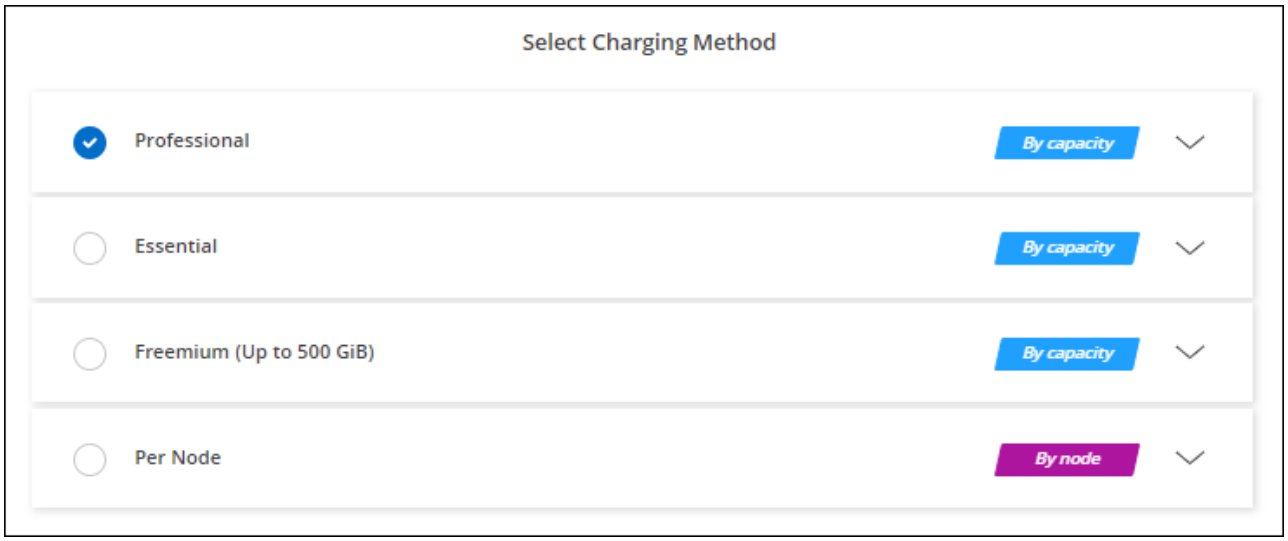
Similar to an hourly subscription, BlueXP prompts you to subscribe to the annual contract that's available in the AWS Marketplace.

Steps

1. On the Canvas page, click **Add Working Environment** and follow the steps in BlueXP.
    a. On the **Details and Credentials** page, click **Edit Credentials > Add Subscription** and then follow the prompts to subscribe to the annual contract in the AWS Marketplace.



b. After you return to BlueXP, select a capacity-based package when you reach the charging methods page.



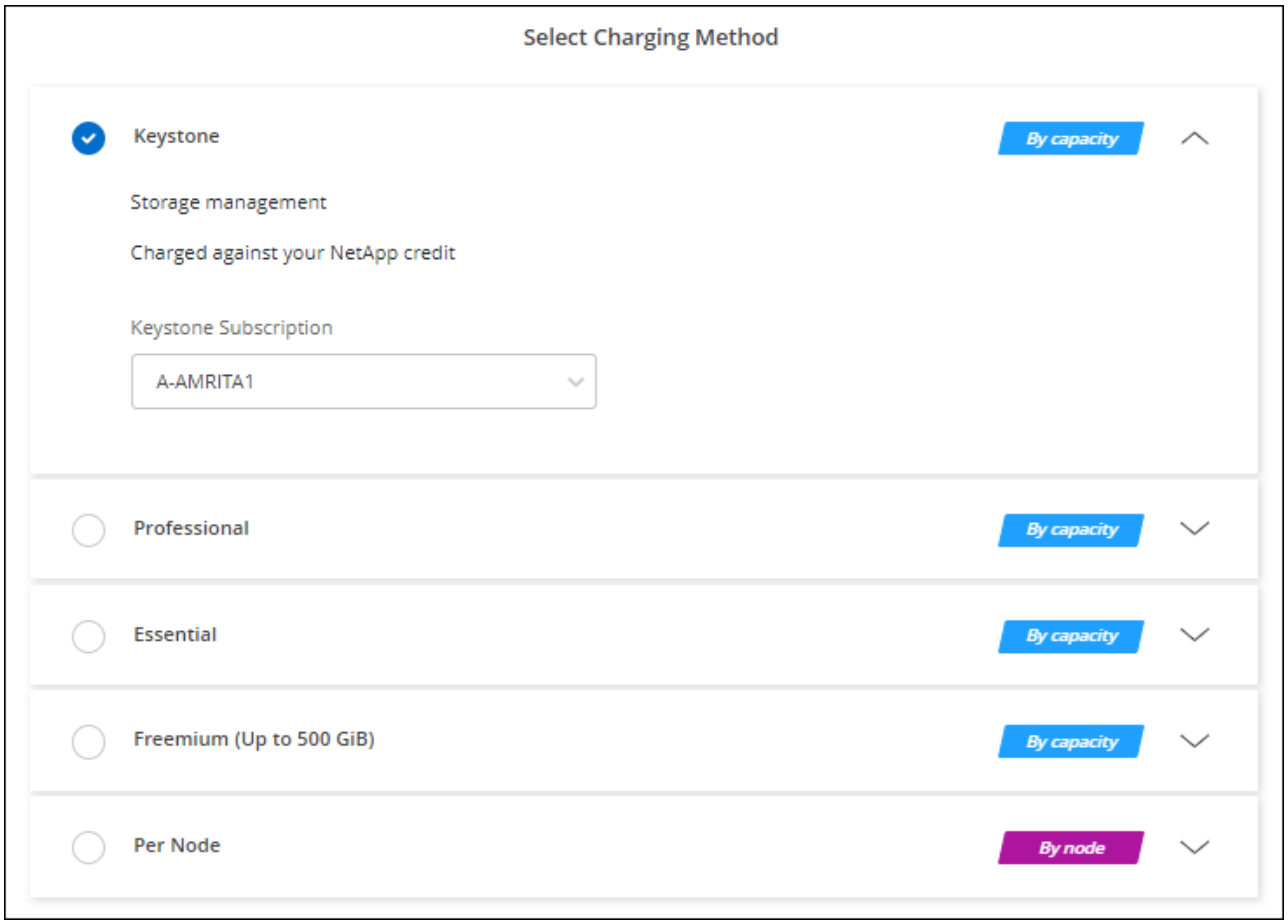
View step-by-step instructions to launch Cloud Volumes ONTAP in AWS.

Keystone Subscription

A Keystone Subscription is a pay-as-you-grow subscription-based service. Learn more about NetApp Keystone Subscriptions.

Steps

1. If you don't have a subscription yet, contact NetApp
2. Contact NetApp to authorize your BlueXP user account with one or more Keystone Subscriptions.
3. After NetApp authorizes your account, link your subscriptions for use with Cloud Volumes ONTAP.
4. On the Canvas page, click **Add Working Environment** and follow the steps in BlueXP.
   a. Select the Keystone Subscription charging method when prompted to choose a charging method.



View step-by-step instructions to launch Cloud Volumes ONTAP in AWS.

Launching Cloud Volumes ONTAP in AWS

You can launch Cloud Volumes ONTAP in a single-system configuration or as an HA pair in AWS.

Before you get started

You need the following to create a working environment.

- A Connector that's up and running.
  - You should have a Connector that is associated with your workspace.
  - You should be prepared to leave the Connector running at all times.
- An understanding of the configuration that you want to use.

  You should have prepared by choosing a configuration and by obtaining AWS networking information from your administrator. For details, refer to Planning your Cloud Volumes ONTAP configuration.
- An understanding of what's required to set up licensing for Cloud Volumes ONTAP.

  Learn how to set up licensing.
- DNS and Active Directory for CIFS configurations.

  For details, refer to Networking requirements for Cloud Volumes ONTAP in AWS.

Launching a single-node Cloud Volumes ONTAP system in AWS

If you want to launch Cloud Volumes ONTAP in AWS, you need to create a new working environment in BlueXP

About this task

Immediately after you create the working environment, BlueXP launches a test instance in the specified VPC to verify connectivity. If successful, BlueXP immediately terminates the instance and then starts deploying the Cloud Volumes ONTAP system. If BlueXP cannot verify connectivity, creation of the working environment fails. The test instance is either a t2.nano (for default VPC tenancy) or m3.medium (for dedicated VPC tenancy).

Steps

1. From the left navigation menu, select **Storage > Canvas**.
2. On the Canvas page, click **Add Working Environment** and follow the prompts.
3. **Choose a Location**: Select **Amazon Web Services** and **Cloud Volumes ONTAP Single Node**.
4. If you're prompted, create a Connector.
5. **Details and Credentials**: Optionally change the AWS credentials and subscription, enter a working environment name, add tags if needed, and then enter a password.

   Some of the fields in this page are self-explanatory. The following table describes fields for which you might need guidance:

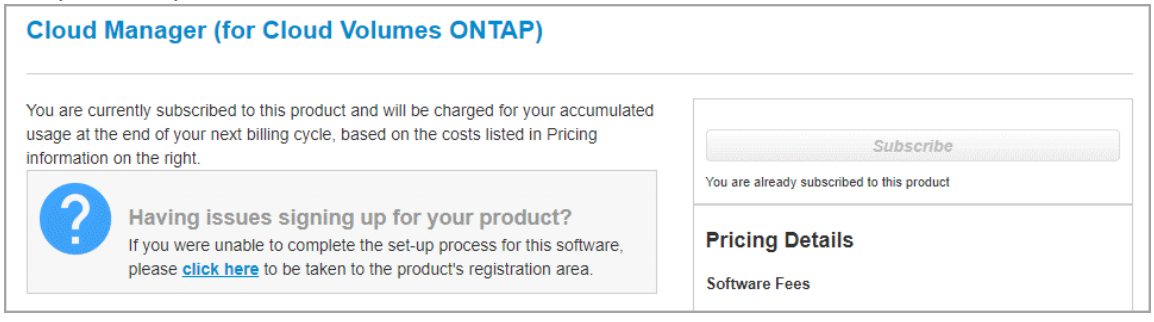
Field	Description
Working Environment Name	BlueXP uses the working environment name to name both the Cloud Volumes ONTAP system and the Amazon EC2 instance. It also uses the name as the prefix for the predefined security group, if you select that option.

Field	Description
Add tags	AWS tags are metadata for your AWS resources. BlueXP adds the tags to the Cloud Volumes ONTAP instance and each AWS resource associated with the instance. You can add up to four tags from the user interface when creating a working environment, and then you can add more after its created. Note that the API does not limit you to four tags when creating a working environment. For information about tags, refer to AWS Documentation: Tagging your Amazon EC2 Resources.
User name and password	These are the credentials for the Cloud Volumes ONTAP cluster administrator account. You can use these credentials to connect to Cloud Volumes ONTAP through ONTAP System Manager or the ONTAP CLI. Keep the default *admin* user name or change it to a custom user name.
Edit Credentials	Choose the AWS credentials associated with the account where you want to deploy this system. You can also associate the AWS Marketplace subscription to use with this Cloud Volumes ONTAP system. Click **Add Subscription** to associate the selected credentials with a new AWS Marketplace subscription. The subscription can be for an annual contract or to pay for Cloud Volumes ONTAP at an hourly rate. Learn how to add additional AWS credentials to BlueXP.

The following video shows how to associate a pay-as-you-go Marketplace subscription to your AWS credentials:

Subscribe to BlueXP from the AWS Marketplace

If multiple IAM users work in the same AWS account, then each user needs to subscribe. After the first user subscribes, the AWS Marketplace informs subsequent users that they're already subscribed, as shown in the image below. While a subscription is in place for the AWS *account*, each IAM user needs to associate themselves with that subscription. If you see the message shown below, click the **click here** link to go to the BlueXP website and complete the process.



6. **Services**: Keep the services enabled or disable the individual services that you don't want to use with Cloud Volumes ONTAP.
   - Learn more about BlueXP classification
   - Learn more about BlueXP backup and recovery

If you would like to utilize WORM and data tiering, you must disable BlueXP backup and recovery and deploy a Cloud Volumes ONTAP working environment with version 9.8 or above.

7. **Location & Connectivity**: Enter the network information that you recorded in the AWS worksheet.

   The following table describes fields for which you might need guidance:

Field	Description
VPC	If you have an AWS Outpost, you can deploy a single node Cloud Volumes ONTAP system in that Outpost by selecting the Outpost VPC. The experience is the same as any other VPC that resides in AWS.
Generated security group	If you let BlueXP generate the security group for you, you need to choose how you'll allow traffic: • If you choose **Selected VPC only**, the source for inbound traffic is the subnet range of the selected VPC and the subnet range of the VPC where the Connector resides. This is the recommended option. • If you choose **All VPCs**, the source for inbound traffic is the 0.0.0.0/0 IP range.
Use existing security group	If you use an existing firewall policy, ensure that it includes the required rules. Learn about firewall rules for Cloud Volumes ONTAP.

8. **Data Encryption**: Choose no data encryption or AWS-managed encryption.

   For AWS-managed encryption, you can choose a different Customer Master Key (CMK) from your account or another AWS account.

   You can't change the AWS data encryption method after you create a Cloud Volumes ONTAP system.

   Learn how to set up the AWS KMS for Cloud Volumes ONTAP.

   Learn more about supported encryption technologies.

9. **Charging Methods and NSS Account**: Specify which charging option would you like to use with this system, and then specify a NetApp Support Site account.
   - Learn about licensing options for Cloud Volumes ONTAP.
   - Learn how to set up licensing.
10. **Cloud Volumes ONTAP Configuration** (annual AWS Marketplace contract only): Review the default configuration and click **Continue** or click **Change Configuration** to select your own configuration.

    If you keep the default configuration, then you only need to specify a volume and then review and approve the configuration.

11. **Preconfigured Packages**: Select one of the packages to quickly launch Cloud Volumes ONTAP, or click **Change Configuration** to select your own configuration.

    If you choose one of the packages, then you only need to specify a volume and then review and approve

the configuration.

12. **IAM Role**: It's best to keep the default option to let BlueXP create the role for you.

    If you prefer to use your own policy, it must meet policy requirements for Cloud Volumes ONTAP nodes.

13. **Licensing**: Change the Cloud Volumes ONTAP version as needed and select an instance type and the instance tenancy.

    > If a newer Release Candidate, General Availability, or patch release is available for the selected version, then BlueXP updates the system to that version when creating the working environment. For example, the update occurs if you select Cloud Volumes ONTAP 9.13.1 and 9.13.1 P4 is available. The update does not occur from one release to another—for example, from 9.13 to 9.14.

14. **Underlying Storage Resources**: Choose a disk type, configure the underlying storage, and choose whether to keep data tiering enabled.

    Note the following:

    - The disk type is for the initial volume (and aggregate). You can choose a different disk type for subsequent volumes (and aggregates).
    - If you choose a gp3 or io1 disk, BlueXP uses the Elastic Volumes feature in AWS to automatically increase the underlying storage disk capacity as needed. You can choose the initial capacity based on your storage needs and revise it after Cloud Volumes ONTAP is deployed. Learn more about support for Elastic Volumes in AWS.
    - If you choose a gp2 or st1 disk, you can select a disk size for all disks in the initial aggregate and for any additional aggregates that BlueXP creates when you use the simple provisioning option. You can create aggregates that use a different disk size by using the advanced allocation option.
    - You can choose a specific volume tiering policy when you create or edit a volume.
    - If you disable data tiering, you can enable it on subsequent aggregates.

    Learn how data tiering works.

15. **Write Speed & WORM**:
    a. Choose **Normal** or **High** write speed, if desired.

       Learn more about write speed.

    b. Activate write once, read many (WORM) storage, if desired.

       WORM can't be enabled if data tiering was enabled for Cloud Volumes ONTAP versions 9.7 and below. Reverting or downgrading to Cloud Volumes ONTAP 9.8 is blocked after enabling WORM and tiering.

       Learn more about WORM storage.

    c. If you activate WORM storage, select the retention period.
16. **Create Volume**: Enter details for the new volume or click **Skip**.

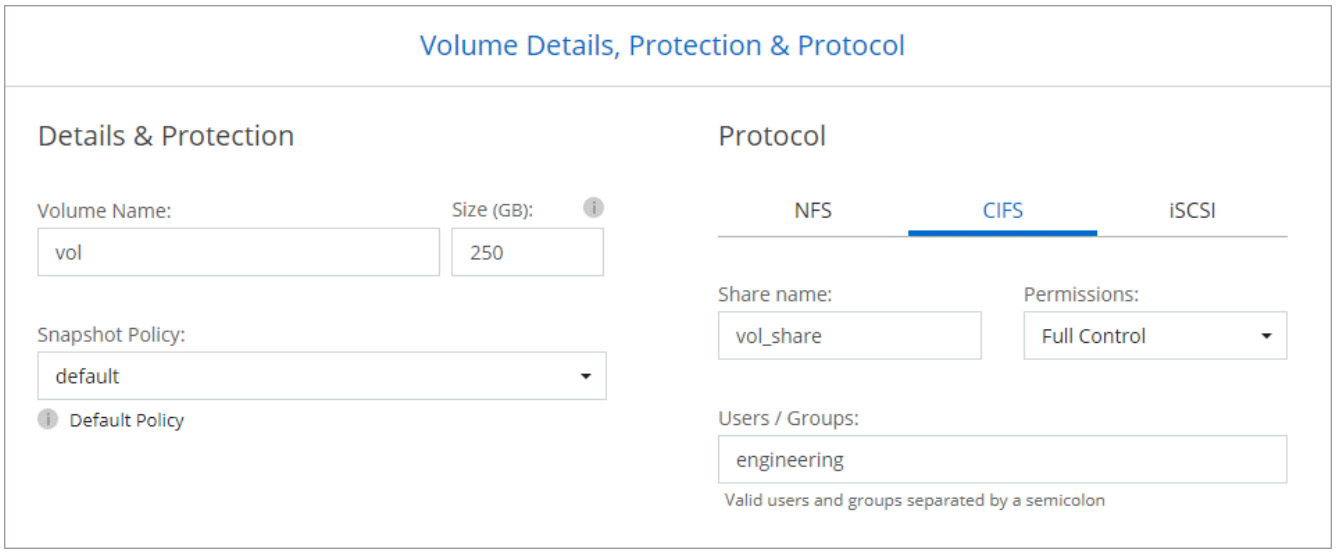
    Learn about supported client protocols and versions.

    Some of the fields in this page are self-explanatory. The following table describes fields for which you might

need guidance:

Field	Description
Size	The maximum size that you can enter largely depends on whether you enable thin provisioning, which enables you to create a volume that is bigger than the physical storage currently available to it.
Access control (for NFS only)	An export policy defines the clients in the subnet that can access the volume. By default, BlueXP enters a value that provides access to all instances in the subnet.
Permissions and Users / Groups (for CIFS only)	These fields enable you to control the level of access to a share for users and groups (also called access control lists or ACLs). You can specify local or domain Windows users or groups, or UNIX users or groups. If you specify a domain Windows user name, you must include the user's domain using the format domain\username.
Snapshot Policy	A Snapshot copy policy specifies the frequency and number of automatically created NetApp Snapshot copies. A NetApp Snapshot copy is a point-in-time file system image that has no performance impact and requires minimal storage. You can choose the default policy or none. You might choose none for transient data: for example, tempdb for Microsoft SQL Server.
Advanced options (for NFS only)	Select an NFS version for the volume: either NFSv3 or NFSv4.
Initiator group and IQN (for iSCSI only)	iSCSI storage targets are called LUNs (logical units) and are presented to hosts as standard block devices. Initiator groups are tables of iSCSI host node names and control which initiators have access to which LUNs. iSCSI targets connect to the network through standard Ethernet network adapters (NICs), TCP offload engine (TOE) cards with software initiators, converged network adapters (CNAs) or dedicated host bust adapters (HBAs) and are identified by iSCSI qualified names (IQNs). When you create an iSCSI volume, BlueXP automatically creates a LUN for you. We've made it simple by creating just one LUN per volume, so there's no management involved. After you create the volume, use the IQN to connect to the LUN from your hosts.

The following image shows the Volume page filled out for the CIFS protocol:



17. **CIFS Setup**: If you chose the CIFS protocol, set up a CIFS server.

Field	Description
DNS Primary and Secondary IP Address	The IP addresses of the DNS servers that provide name resolution for the CIFS server. The listed DNS servers must contain the service location records (SRV) needed to locate the Active Directory LDAP servers and domain controllers for the domain that the CIFS server will join.
Active Directory Domain to join	The FQDN of the Active Directory (AD) domain that you want the CIFS server to join.
Credentials authorized to join the domain	The name and password of a Windows account with sufficient privileges to add computers to the specified Organizational Unit (OU) within the AD domain.
CIFS server NetBIOS name	A CIFS server name that is unique in the AD domain.
Organizational Unit	The organizational unit within the AD domain to associate with the CIFS server. The default is CN=Computers. If you configure AWS Managed Microsoft AD as the AD server for Cloud Volumes ONTAP, you should enter **OU=Computers,OU=corp** in this field.
DNS Domain	The DNS domain for the Cloud Volumes ONTAP storage virtual machine (SVM). In most cases, the domain is the same as the AD domain.
NTP Server	Select **Use Active Directory Domain** to configure an NTP server using the Active Directory DNS. If you need to configure an NTP server using a different address, then you should use the API. Refer to the BlueXP automation docs for details. Note that you can configure an NTP server only when creating a CIFS server. It's not configurable after you create the CIFS server.

18. **Usage Profile, Disk Type, and Tiering Policy**: Choose whether you want to enable storage efficiency features and edit the volume tiering policy, if needed.

    For more information, refer to Understanding volume usage profiles and Data tiering overview.

19. **Review & Approve**: Review and confirm your selections.
    a. Review details about the configuration.
    b. Click **More information** to review details about support and the AWS resources that BlueXP will purchase.
    c. Select the **I understand…** check boxes.
    d. Click **Go**.

Result

BlueXP launches the Cloud Volumes ONTAP instance. You can track the progress in the timeline.

If you experience any issues launching the Cloud Volumes ONTAP instance, review the failure message. You can also select the working environment and click Re-create environment.

For additional help, go to NetApp Cloud Volumes ONTAP Support.

After you finish

- If you provisioned a CIFS share, give users or groups permissions to the files and folders and verify that those users can access the share and create a file.
- If you want to apply quotas to volumes, use ONTAP System Manager or the ONTAP CLI.

  Quotas enable you to restrict or track the disk space and number of files used by a user, group, or qtree.

Launching a Cloud Volumes ONTAP HA pair in AWS

If you want to launch a Cloud Volumes ONTAP HA pair in AWS, you need to create an HA working environment in BlueXP.

Limitation

At this time, HA pairs are not supported with AWS Outposts.

About this task

Immediately after you create the working environment, BlueXP launches a test instance in the specified VPC to verify connectivity. If successful, BlueXP immediately terminates the instance and then starts deploying the Cloud Volumes ONTAP system. If BlueXP cannot verify connectivity, creation of the working environment fails. The test instance is either a t2.nano (for default VPC tenancy) or m3.medium (for dedicated VPC tenancy).

Steps

1. From the left navigation menu, select **Storage > Canvas**.
2. On the Canvas page, click **Add Working Environment** and follow the prompts.
3. **Choose a Location**: Select **Amazon Web Services** and **Cloud Volumes ONTAP HA**.

   Some AWS Local Zones are available.

   Before you can use AWS Local Zones, you must enable Local Zones and create a subnet in the Local Zone in your AWS account. Follow the **Opt in to an AWS Local Zone** and **Extend your Amazon VPC to the Local Zone** steps in the AWS tutorial "Get Started Deploying Low Latency Applications with AWS Local Zones.

   If you are running a Connector version 3.9.36 or below, you need to add the following permission to the AWS Connector role in the AWS EC2 console: DescribeAvailabilityZones.

4. **Details and Credentials**: Optionally change the AWS credentials and subscription, enter a working environment name, add tags if needed, and then enter a password.

   Some of the fields in this page are self-explanatory. The following table describes fields for which you might need guidance:

Field	Description
Working Environment Name	BlueXP uses the working environment name to name both the Cloud Volumes ONTAP system and the Amazon EC2 instance. It also uses the name as the prefix for the predefined security group, if you select that option.
Add tags	AWS tags are metadata for your AWS resources. BlueXP adds the tags to the Cloud Volumes ONTAP instance and each AWS resource associated with the instance. You can add up to four tags from the user interface when creating a working environment, and then you can add more after its created. Note that the API does not limit you to four tags when creating a working environment. For information about tags, refer to AWS Documentation: Tagging your Amazon EC2 Resources.
User name and password	These are the credentials for the Cloud Volumes ONTAP cluster administrator account. You can use these credentials to connect to Cloud Volumes ONTAP through ONTAP System Manager or the ONTAP CLI. Keep the default *admin* user name or change it to a custom user name.
Edit Credentials	Choose the AWS credentials and marketplace subscription to use with this Cloud Volumes ONTAP system. Click **Add Subscription** to associate the selected credentials with a new AWS Marketplace subscription. The subscription can be for an annual contract or to pay for Cloud Volumes ONTAP at an hourly rate. If purchased a license directly from NetApp (BYOL), then an AWS subscription isn't required. Learn how to add additional AWS credentials to BlueXP.

   The following video shows how to associate a pay-as-you-go Marketplace subscription to your AWS credentials:

   Subscribe to BlueXP from the AWS Marketplace

   If multiple IAM users work in the same AWS account, then each user needs to subscribe. After the first user subscribes, the AWS Marketplace informs subsequent users that they're already subscribed, as shown in the image below. While a subscription is in place for the AWS *account*, each IAM user needs to associate themselves with that subscription. If you see the message shown below, click the **click here** link to go to BlueXP website and complete the process.

5. **Services**: Keep the services enabled or disable the individual services that you don't want to use with this Cloud Volumes ONTAP system.

- Learn more about BlueXP classification
- Learn more about BlueXP backup and recovery

If you would like to utilize WORM and data tiering, you must disable BlueXP backup and recovery and deploy a Cloud Volumes ONTAP working environment with version 9.8 or above.

6. **HA Deployment Models**: Choose an HA configuration.

   For an overview of the deployment models, refer to Cloud Volumes ONTAP HA for AWS.

7. **Location and Connectivity** (single AZ) or **Region & VPC** (multiple AZs): Enter the network information that you recorded in the AWS worksheet.

   The following table describes fields for which you might need guidance:

Field	Description
Generated security group	If you let BlueXP generate the security group for you, you need to choose how you'll allow traffic: • If you choose **Selected VPC only**, the source for inbound traffic is the subnet range of the selected VPC and the subnet range of the VPC where the Connector resides. This is the recommended option. • If you choose **All VPCs**, the source for inbound traffic is the 0.0.0.0/0 IP range.
Use existing security group	If you use an existing firewall policy, ensure that it includes the required rules. Learn about firewall rules for Cloud Volumes ONTAP.

8. **Connectivity and SSH Authentication**: Choose connection methods for the HA pair and the mediator.
9. **Floating IPs**: If you chose multiple AZs, specify the floating IP addresses.

   The IP addresses must be outside of the CIDR block for all VPCs in the region. For additional details, refer to AWS networking requirements for Cloud Volumes ONTAP HA in multiple AZs.

10. **Route Tables**: If you chose multiple AZs, select the route tables that should include routes to the floating IP addresses.

    If you have more than one route table, it is very important to select the correct route tables. Otherwise, some clients might not have access to the Cloud Volumes ONTAP HA pair. For more information about route tables, refer to the AWS Documentation: Route Tables.

11. **Data Encryption**: Choose no data encryption or AWS-managed encryption.

    For AWS-managed encryption, you can choose a different Customer Master Key (CMK) from your account or another AWS account.

    You can't change the AWS data encryption method after you create a Cloud Volumes ONTAP system.

    Learn how to set up the AWS KMS for Cloud Volumes ONTAP.

Learn more about supported encryption technologies.

12. **Charging Methods and NSS Account**: Specify which charging option would you like to use with this system, and then specify a NetApp Support Site account.
    - Learn about licensing options for Cloud Volumes ONTAP.
    - Learn how to set up licensing.
13. **Cloud Volumes ONTAP Configuration** (annual AWS Marketplace contract only): Review the default configuration and click **Continue** or click **Change Configuration** to select your own configuration.

    If you keep the default configuration, then you only need to specify a volume and then review and approve the configuration.
14. **Preconfigured Packages** (hourly or BYOL only): Select one of the packages to quickly launch Cloud Volumes ONTAP, or click **Change Configuration** to select your own configuration.

    If you choose one of the packages, then you only need to specify a volume and then review and approve the configuration.
15. **IAM Role**: It's best to keep the default option to let BlueXP create the role for you.

    If you prefer to use your own policy, it must meet policy requirements for Cloud Volumes ONTAP nodes and the HA mediator.
16. **Licensing**: Change the Cloud Volumes ONTAP version as needed and select an instance type and the instance tenancy.

    If a newer Release Candidate, General Availability, or patch release is available for the selected version, then BlueXP updates the system to that version when creating the working environment. For example, the update occurs if you select Cloud Volumes ONTAP 9.13.1 and 9.13.1 P4 is available. The update does not occur from one release to another—for example, from 9.13 to 9.14.
17. **Underlying Storage Resources**: Choose a disk type, configure the underlying storage, and choose whether to keep data tiering enabled.

    Note the following:
    - The disk type is for the initial volume (and aggregate). You can choose a different disk type for subsequent volumes (and aggregates).
    - If you choose a gp3 or io1 disk, BlueXP uses the Elastic Volumes feature in AWS to automatically increase the underlying storage disk capacity as needed. You can choose the initial capacity based on your storage needs and revise it after Cloud Volumes ONTAP is deployed. Learn more about support for Elastic Volumes in AWS.
    - If you choose a gp2 or st1 disk, you can select a disk size for all disks in the initial aggregate and for any additional aggregates that BlueXP creates when you use the simple provisioning option. You can create aggregates that use a different disk size by using the advanced allocation option.
    - You can choose a specific volume tiering policy when you create or edit a volume.
    - If you disable data tiering, you can enable it on subsequent aggregates.

    Learn how data tiering works.

18. **Write Speed & WORM**:
    a. Choose **Normal** or **High** write speed, if desired.

       Learn more about write speed.

    b. Activate write once, read many (WORM) storage, if desired.

       WORM can't be enabled if data tiering was enabled for Cloud Volumes ONTAP versions 9.7 and below. Reverting or downgrading to Cloud Volumes ONTAP 9.8 is blocked after enabling WORM and tiering.

       Learn more about WORM storage.

    c. If you activate WORM storage, select the retention period.
19. **Create Volume**: Enter details for the new volume or click **Skip**.

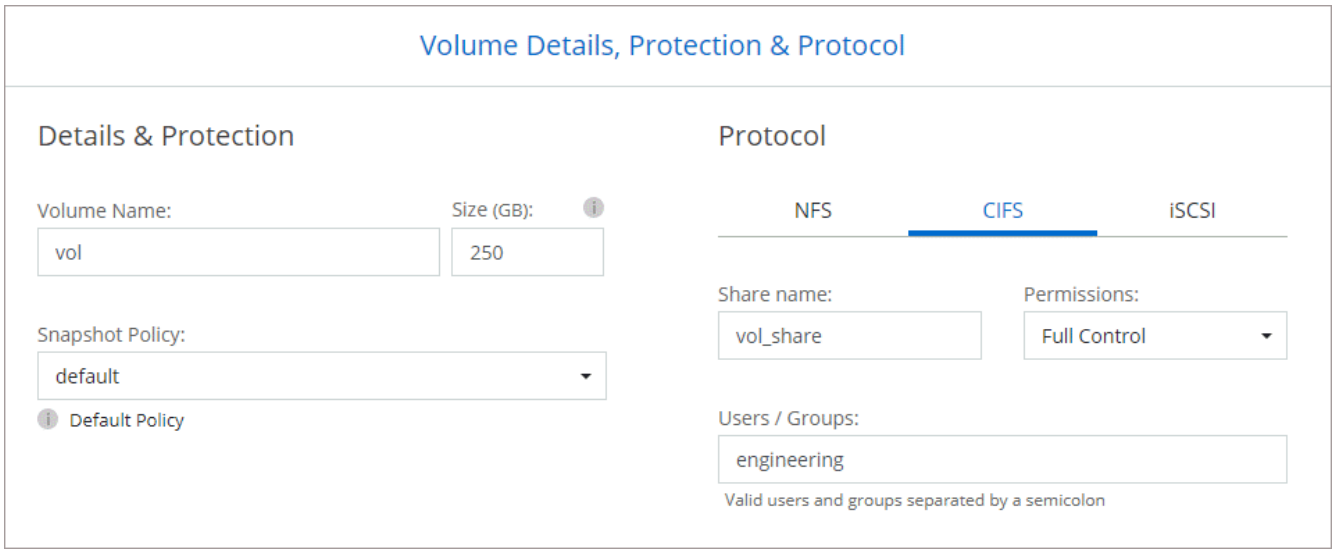
    Learn about supported client protocols and versions.

    Some of the fields in this page are self-explanatory. The following table describes fields for which you might need guidance:

Field	Description
Size	The maximum size that you can enter largely depends on whether you enable thin provisioning, which enables you to create a volume that is bigger than the physical storage currently available to it.
Access control (for NFS only)	An export policy defines the clients in the subnet that can access the volume. By default, BlueXP enters a value that provides access to all instances in the subnet.
Permissions and Users / Groups (for CIFS only)	These fields enable you to control the level of access to a share for users and groups (also called access control lists or ACLs). You can specify local or domain Windows users or groups, or UNIX users or groups. If you specify a domain Windows user name, you must include the user's domain using the format domain\username.
Snapshot Policy	A Snapshot copy policy specifies the frequency and number of automatically created NetApp Snapshot copies. A NetApp Snapshot copy is a point-in-time file system image that has no performance impact and requires minimal storage. You can choose the default policy or none. You might choose none for transient data: for example, tempdb for Microsoft SQL Server.
Advanced options (for NFS only)	Select an NFS version for the volume: either NFSv3 or NFSv4.

Field	Description
Initiator group and IQN (for iSCSI only)	iSCSI storage targets are called LUNs (logical units) and are presented to hosts as standard block devices. Initiator groups are tables of iSCSI host node names and control which initiators have access to which LUNs. iSCSI targets connect to the network through standard Ethernet network adapters (NICs), TCP offload engine (TOE) cards with software initiators, converged network adapters (CNAs) or dedicated host bust adapters (HBAs) and are identified by iSCSI qualified names (IQNs). When you create an iSCSI volume, BlueXP automatically creates a LUN for you. We've made it simple by creating just one LUN per volume, so there's no management involved. After you create the volume, use the IQN to connect to the LUN from your hosts.

The following image shows the Volume page filled out for the CIFS protocol:



20. **CIFS Setup**: If you selected the CIFS protocol, set up a CIFS server.

Field	Description
DNS Primary and Secondary IP Address	The IP addresses of the DNS servers that provide name resolution for the CIFS server. The listed DNS servers must contain the service location records (SRV) needed to locate the Active Directory LDAP servers and domain controllers for the domain that the CIFS server will join.
Active Directory Domain to join	The FQDN of the Active Directory (AD) domain that you want the CIFS server to join.
Credentials authorized to join the domain	The name and password of a Windows account with sufficient privileges to add computers to the specified Organizational Unit (OU) within the AD domain.
CIFS server NetBIOS name	A CIFS server name that is unique in the AD domain.

Field	Description
Organizational Unit	The organizational unit within the AD domain to associate with the CIFS server. The default is CN=Computers. If you configure AWS Managed Microsoft AD as the AD server for Cloud Volumes ONTAP, you should enter **OU=Computers,OU=corp** in this field.
DNS Domain	The DNS domain for the Cloud Volumes ONTAP storage virtual machine (SVM). In most cases, the domain is the same as the AD domain.
NTP Server	Select **Use Active Directory Domain** to configure an NTP server using the Active Directory DNS. If you need to configure an NTP server using a different address, then you should use the API. Refer to the BlueXP automation docs for details. Note that you can configure an NTP server only when creating a CIFS server. It's not configurable after you create the CIFS server.

21. **Usage Profile, Disk Type, and Tiering Policy**: Choose whether you want to enable storage efficiency features and edit the volume tiering policy, if needed.

    For more information, refer to Choose a volume usage profile and Data tiering overview.

22. **Review & Approve**: Review and confirm your selections.
    a. Review details about the configuration.
    b. Click **More information** to review details about support and the AWS resources that BlueXP will purchase.
    c. Select the **I understand…** check boxes.
    d. Click **Go**.

Result

BlueXP launches the Cloud Volumes ONTAP HA pair. You can track the progress in the timeline.

If you experience any issues launching the HA pair, review the failure message. You can also select the working environment and click Re-create environment.

For additional help, go to NetApp Cloud Volumes ONTAP Support.

After you finish

- If you provisioned a CIFS share, give users or groups permissions to the files and folders and verify that those users can access the share and create a file.
- If you want to apply quotas to volumes, use ONTAP System Manager or the ONTAP CLI.

  Quotas enable you to restrict or track the disk space and number of files used by a user, group, or qtree.

Deploy Cloud Volumes ONTAP in AWS Secret Cloud and Top Secret Cloud regions

Similar to a standard AWS region, you can use BlueXP in AWS Secret Cloud and in AWS Top Secret Cloud to deploy Cloud Volumes ONTAP, which provides enterprise-class

features for your cloud storage. AWS Secret Cloud and Top Secret Cloud are closed regions specific to the U.S. Intelligence Community; the instructions on this page only apply to AWS Secret Cloud and Top Secret Cloud region users.

Before you begin

Before you get started, review the supported versions in AWS Secret Cloud and Top Secret Cloud, and learn about private mode in BlueXP.

- Review the following supported versions in AWS Secret Cloud and Top Secret Cloud:
  - Cloud Volumes ONTAP 9.12.1 P2
  - Version 3.9.32 of the Connector

    The Connector is software that's required to deploy and manage Cloud Volumes ONTAP in AWS. You'll log in to BlueXP from the software that gets installed on the Connector instance. The SaaS website for BlueXP isn't supported in AWS Secret Cloud and Top Secret Cloud.
- Learn about private mode

  In AWS Secret Cloud and Top Secret Cloud, BlueXP operates in *private mode*. In private mode, there is no connectivity to the BlueXP SaaS layer. Users access BlueXP locally from the web-based console that's available from the Connector, not from the SaaS layer.

  To learn more about how private mode works, refer to BlueXP private deployment mode.

Step 1: Set up your networking

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

Steps

1. Choose the VPC and subnets in which you want to launch the Connector instance and Cloud Volumes ONTAP instances.
2. Ensure that your VPC and subnets will support connectivity between the Connector and Cloud Volumes ONTAP.
3. Set up a VPC endpoint to the S3 service.

   A VPC endpoint is required if you want to tier cold data from Cloud Volumes ONTAP to low-cost object storage.

Step 2: Set up permissions

Set up IAM policies and roles that provide the Connector and Cloud Volumes ONTAP with the permissions that they need to perform actions in the AWS Secret Cloud or Top Secret Cloud.

You need an IAM policy and IAM role for each of the following:

- The Connector instance
- Cloud Volumes ONTAP instances
- For HA pairs, the Cloud Volumes ONTAP HA mediator instance (if you want to deploy HA pairs)

Steps

1. Go to the AWS IAM console and click **Policies**.
2. Create a policy for the Connector instance.

You create these policies to support the S3 buckets in your AWS environment. While creating the buckets later, ensure that the bucket names are prefixed with `fabric-pool-`. This requirement applies to both the AWS Secret Cloud and Top Secret Cloud regions.

Secret regions

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:RunInstances",
                "ec2:ModifyInstanceAttribute",
                "ec2:DescribeRouteTables",
                "ec2:DescribeImages",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DescribeVolumes",
                "ec2:ModifyVolumeAttribute",
                "ec2:DeleteVolume",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup",
                "ec2:DescribeSecurityGroups",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateNetworkInterface",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DeleteNetworkInterface",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DescribeDhcpOptions",
                "ec2:CreateSnapshot",
                "ec2:DeleteSnapshot",
                "ec2:DescribeSnapshots",
                "ec2:GetConsoleOutput",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeRegions",
                "ec2:DeleteTags",
                "ec2:DescribeTags",
                "cloudformation:CreateStack",
                "cloudformation:DeleteStack",
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackEvents",
                "cloudformation:ValidateTemplate",
                "iam:PassRole",
```

```
                "iam:CreateRole",
                "iam:DeleteRole",
                "iam:PutRolePolicy",
                "iam:ListInstanceProfiles",
                "iam:CreateInstanceProfile",
                "iam:DeleteRolePolicy",
                "iam:AddRoleToInstanceProfile",
                "iam:RemoveRoleFromInstanceProfile",
                "iam:DeleteInstanceProfile",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:GetBucketTagging",
                "s3:GetBucketLocation",
                "s3:ListAllMyBuckets",
                "kms:List*",
                "kms:Describe*",
                "ec2:AssociateIamInstanceProfile",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:DescribeInstanceAttribute",
                "ec2:CreatePlacementGroup",
                "ec2:DeletePlacementGroup"
            ],
            "Resource": "*"
        },
        {
            "Sid": "fabricPoolPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions"
            ],
            "Resource": [
                "arn:aws-iso-b:s3:::fabric-pool*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances",
                "ec2:AttachVolume",
```

```
                "ec2:DetachVolume"
            ],
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/WorkingEnvironment": "*"
                }
            },
            "Resource": [
                "arn:aws-iso-b:ec2:*:*:instance/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Resource": [
                "arn:aws-iso-b:ec2:*:*:volume/*"
            ]
        }
    ]
}
```

Top Secret regions

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:RunInstances",
                "ec2:ModifyInstanceAttribute",
                "ec2:DescribeRouteTables",
                "ec2:DescribeImages",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DescribeVolumes",
                "ec2:ModifyVolumeAttribute",
                "ec2:DeleteVolume",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup",
                "ec2:DescribeSecurityGroups",
                "ec2:RevokeSecurityGroupEgress",
```

```
                "ec2:RevokeSecurityGroupIngress",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateNetworkInterface",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DeleteNetworkInterface",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DescribeDhcpOptions",
                "ec2:CreateSnapshot",
                "ec2:DeleteSnapshot",
                "ec2:DescribeSnapshots",
                "ec2:GetConsoleOutput",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeRegions",
                "ec2:DeleteTags",
                "ec2:DescribeTags",
                "cloudformation:CreateStack",
                "cloudformation:DeleteStack",
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackEvents",
                "cloudformation:ValidateTemplate",
                "iam:PassRole",
                "iam:CreateRole",
                "iam:DeleteRole",
                "iam:PutRolePolicy",
                "iam:ListInstanceProfiles",
                "iam:CreateInstanceProfile",
                "iam:DeleteRolePolicy",
                "iam:AddRoleToInstanceProfile",
                "iam:RemoveRoleFromInstanceProfile",
                "iam:DeleteInstanceProfile",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:GetBucketTagging",
                "s3:GetBucketLocation",
                "s3:ListAllMyBuckets",
                "kms:List*",
                "kms:Describe*",
                "ec2:AssociateIamInstanceProfile",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:DescribeInstanceAttribute",
                "ec2:CreatePlacementGroup",
                "ec2:DeletePlacementGroup"
```

```
            ],
            "Resource": "*"
        },
        {
            "Sid": "fabricPoolPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions"
            ],
            "Resource": [
                "arn:aws-iso:s3:::fabric-pool*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances",
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/WorkingEnvironment": "*"
                }
            },
            "Resource": [
                "arn:aws-iso:ec2:*:*:instance/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Resource": [
                "arn:aws-iso:ec2:*:*:volume/*"
            ]
        }
    ]
```

```
}
```

3. Create a policy for Cloud Volumes ONTAP.

Secret regions

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Action": "s3:ListAllMyBuckets",
        "Resource": "arn:aws-iso-b:s3:::*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:ListBucket",
            "s3:GetBucketLocation"
        ],
        "Resource": "arn:aws-iso-b:s3:::fabric-pool-*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:GetObject",
            "s3:PutObject",
            "s3:DeleteObject"
        ],
        "Resource": "arn:aws-iso-b:s3:::fabric-pool-*",
        "Effect": "Allow"
    }]
}
```

Top Secret regions

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Action": "s3:ListAllMyBuckets",
        "Resource": "arn:aws-iso:s3:::*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:ListBucket",
            "s3:GetBucketLocation"
        ],
        "Resource": "arn:aws-iso:s3:::fabric-pool-*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:GetObject",
            "s3:PutObject",
            "s3:DeleteObject"
        ],
        "Resource": "arn:aws-iso:s3:::fabric-pool-*",
        "Effect": "Allow"
    }]
}
```

For HA pairs, if you plan to deploy a Cloud Volumes ONTAP HA pair, create a policy for the HA mediator.

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "ec2:AssignPrivateIpAddresses",
                "ec2:CreateRoute",
                "ec2:DeleteRoute",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRouteTables",
                "ec2:DescribeVpcs",
                "ec2:ReplaceRoute",
                "ec2:UnassignPrivateIpAddresses"
            ],
            "Resource": "*"
        }
    ]
}
```

4. Create IAM roles with the role type Amazon EC2 and attach the policies that you created in the previous steps.

   Create the role:

   Similar to the policies, you should have one IAM role for the Connector and one for the Cloud Volumes ONTAP nodes.
   For HA pairs: Similar to the policies, you should have one IAM role for the Connector, one for the Cloud Volumes ONTAP nodes, and one for the HA mediator (if you want to deploy HA pairs).

   Select the role:

   You must select the Connector IAM role when you launch the Connector instance. You can select the IAM roles for Cloud Volumes ONTAP when you create a Cloud Volumes ONTAP working environment from BlueXP.
   For HA pairs, you can select the IAM roles for Cloud Volumes ONTAP and the HA mediator when you create a Cloud Volumes ONTAP working environment from BlueXP.

Step 3: Set up the AWS KMS

If you want to use Amazon encryption with Cloud Volumes ONTAP, ensure that requirements are met for the AWS Key Management Service (KMS).

Steps

1. Ensure that an active Customer Master Key (CMK) exists in your account or in another AWS account.

   The CMK can be an AWS-managed CMK or a customer-managed CMK.

2. If the CMK is in an AWS account separate from the account where you plan to deploy Cloud Volumes ONTAP, then you need to obtain the ARN of that key.

You'll need to provide the ARN to BlueXP when you create the Cloud Volumes ONTAP system.

3. Add the IAM role for the Connector instance to the list of key users for a CMK.

   This gives BlueXP permissions to use the CMK with Cloud Volumes ONTAP.

Step 4: Install the Connector and set up BlueXP

Before you can start using BlueXP to deploy Cloud Volumes ONTAP in AWS, you must install and set up the BlueXP Connector. The Connector enables BlueXP to manage resources and processes within your public cloud environment (this includes Cloud Volumes ONTAP).

Steps

1. Obtain a root certificate signed by a certificate authority (CA) in the Privacy Enhanced Mail (PEM) Base-64 encoded X.509 format. Consult your organization's policies and procedures for obtaining the certificate.

   For AWS Secret Cloud regions, you should upload the `NSS Root CA 2` certificate, and for Top Secret Cloud, the `Amazon Root CA 4` certificate. Ensure that you upload only these certificates and not the entire chain. The file for the certificate chain is large, and the upload can fail. If you have additional certificates, you can upload them later, as described in the next step.

   You'll need to upload the certificate during the setup process. BlueXP uses the trusted certificate when sending requests to AWS over HTTPS.

2. Launch the Connector instance:
   a. Go to the AWS Intelligence Community Marketplace page for BlueXP.
   b. On the Custom Launch tab, choose the option to launch the instance from the EC2 console.
   c. Follow the prompts to configure the instance.

      Note the following as you configure the instance:

      - We recommend t3.xlarge.
      - You must choose the IAM role that you created when you set up permissions.
      - You should keep the default storage options.
      - The required connection methods for the Connector are as follows: SSH, HTTP, and HTTPS.
3. Set up BlueXP from a host that has a connection to the Connector instance:
   a. Open a web browser and enter https://*ipaddress* where *ipaddress* is the IP address of the Linux host where you installed the Connector.
   b. Specify a proxy server for connectivity to AWS services.
   c. Upload the certificate that you obtained in step 1.
   d. Select **Set Up New BlueXP** and follow the prompts to set up the system.
      - **System Details**: Enter a name for the Connector and your company name.
      - **Create Admin User**: Create the admin user for the system.

        This user account runs locally on the system. There's no connection to the auth0 service available through BlueXP.

- **Review**: Review the details, accept the license agreement, and then select **Set Up**.

e. To complete installation of the CA-signed certificate, restart the Connector instance from the EC2 console.

4. After the Connector restarts, log in using the administrator user account that you created in the Setup wizard.

Step 5: (optional) Install a private mode certificate

This step is optional for AWS Secret Cloud and Top Secret Cloud regions, and is required only if you have additional certificates apart from the root certificates that you installed in the previous step.

Steps

1. List existing installed certificates.

   a. To collect the occm container docker id (identified name “ds-occm-1”), run the following command:

   ```
   docker ps
   ```

   b. To get inside occm container, run the following command:

   ```
   docker exec -it <docker-id> /bin/sh
   ```

   c. To collect the password from “TRUST_STORE_PASSWORD” environment variable, run the following command:

   ```
   env
   ```

   d. To list all installed certificates in truststore, run the following command and use the password collected in the previous step:

   ```
   keytool -list -v -keystore occm.truststore
   ```

2. Add a certificate.

   a. To collect occm container docker id (identified name “ds-occm-1”), run the following command:

   ```
   docker ps
   ```

   b. To get inside occm container, run the following command:

   ```
   docker exec -it <docker-id> /bin/sh
   ```

   Save the new certificate file inside.

c. To collect the password from “TRUST_STORE_PASSWORD” environment variable, run the following command:

```
env
```

d. To add the certificate to the truststore, run the following command and use the password from the previous step:

```
keytool -import -alias <alias-name> -file <certificate-file-name>
-keystore occm.truststore
```

e. To check that the certificate installed, run the following command:

```
keytool -list -v -keystore occm.truststore -alias <alias-name>
```

f. To exit occm container, run the following command:

```
exit
```

g. To reset occm container, run the following command:

```
docker restart <docker-id>
```

Step 6: Add a license to the BlueXP digital wallet

If you purchased a license from NetApp, you need to add it to the BlueXP digital wallet so that you can select the license when you create a new Cloud Volumes ONTAP system. The digital wallet identifies these licenses as unassigned.

Steps

1. From the BlueXP navigation menu, select **Governance > Digital wallet**.
2. On the **Cloud Volumes ONTAP** tab, select **Node Based Licenses** from the drop-down.
3. Click **Unassigned**.
4. Click **Add Unassigned Licenses**.
5. Enter the serial number of the license or upload the license file.
6. If you don’t have the license file yet, you’ll need to manually upload the license file from netapp.com.
   a. Go to the NetApp License File Generator and log in using your NetApp Support Site credentials.
   b. Enter your password, choose your product, enter the serial number, confirm that you have read and accepted the privacy policy, and then click **Submit**.
   c. Choose whether you want to receive the serialnumber.NLF JSON file through email or direct download.

7. Click **Add License**.

Result

BlueXP adds the license to the digital wallet. The license will be identified as unassigned until you associate it with a new Cloud Volumes ONTAP system. After that happens, the license moves to the BYOL tab in the digital wallet.

Step 7: Launch Cloud Volumes ONTAP from BlueXP

You can launch Cloud Volumes ONTAP instances in AWS Secret Cloud and Top Secret Cloud by creating new working environments in BlueXP.

Before you begin

For HA pairs, a key pair is required to enable key-based SSH authentication to the HA mediator.

Steps

1. On the Working Environments page, click **Add Working Environment**.
2. Under **Create**, select Cloud Volumes ONTAP.

   For HA: Under **Create**, select Cloud Volumes ONTAP or Cloud Volumes ONTAP HA.

3. Complete the steps in the wizard to launch the Cloud Volumes ONTAP system.

While making selections through the wizard, do not select **Data Sense & Compliance** and **Backup to Cloud** under **Services**. Under **Preconfigured Packages**, select **Change Configuration** only, and ensure that you haven't selected any other option. Preconfigured packages aren't supported in AWS Secret Cloud and Top Secret Cloud regions, and if selected, your deployment will fail.

Notes for deploying Cloud Volumes ONTAP HA in multiple Availability Zones

Note the following as you complete the wizard for HA pairs.

- You should configure a transit gateway when you deploy Cloud Volumes ONTAP HA in multiple Availability Zones (AZs). For instructions, refer to Set up an AWS transit gateway.
- Deploy the configuration as the following because only two AZs were available in the AWS Top Secret Cloud at the time of publication:
  - Node 1: Availability Zone A
  - Node 2: Availability Zone B
  - Mediator: Availability Zone A or B

Notes for deploying Cloud Volumes ONTAP in both single and HA nodes

Note the following as you complete the wizard:

- You should leave the default option to use a generated security group.

  The predefined security group includes the rules that Cloud Volumes ONTAP needs to operate successfully. If you have a requirement to use your own, you can refer to the security group section below.

- You must choose the IAM role that you created when preparing your AWS environment.
- The underlying AWS disk type is for the initial Cloud Volumes ONTAP volume.

You can choose a different disk type for subsequent volumes.

- The performance of AWS disks is tied to disk size.

  You should choose the disk size that gives you the sustained performance that you need. Refer to AWS documentation for more details about EBS performance.

- The disk size is the default size for all disks on the system.

> If you need a different size later, you can use the Advanced allocation option to create an aggregate that uses disks of a specific size.

Result

BlueXP launches the Cloud Volumes ONTAP instance. You can track the progress in the timeline.

Step 8: Install security certificates for data tiering

You need to manually install security certificates for enabling data tiering in AWS Secret Cloud and Top Secret Cloud regions.

Before you begin

1. Create S3 buckets.

> Ensure that the bucket names are prefixed with `fabric-pool-`. For example `fabric-pool-testbucket`.

2. Keep the root certificates that you installed in `step 4` handy.

Steps

1. Copy the text from the root certificates that you installed in `step 4`.
2. Securely connect to the Cloud Volumes ONTAP system by using the CLI.
3. Install the root certificates. You might need to press the `ENTER` key multiple times:

```
security certificate install -type server-ca -cert-name <certificate-
name>
```

4. When prompted, enter the entire copied text, including and from `----- BEGIN CERTIFICATE -----` to `----- END CERTIFICATE -----`.
5. Keep a copy of the CA-signed digital certificate for future reference.
6. Retain the CA name and certificate serial number.
7. Configure the object store for AWS Secret Cloud and Top Secret Cloud regions: `set -privilege advanced -confirmations off`
8. Run this command to configure the object store.

All Amazon Resource Names (ARNs) should be suffixed with `-iso-b`, such as `arn:aws-iso-b`. For example, if a resource requires an ARN with a region, for Top Secret Cloud, use the naming convention as `us-iso-b` for the `-server` flag. For AWS Secret Cloud, use `us-iso-b-1`.

```
storage aggregate object-store config create -object-store-name
<S3Bucket> -provider-type AWS_S3 -auth-type EC2-IAM -server <s3.us-iso-
b-1.server_name> -container-name <fabric-pool-testbucket> -is-ssl
-enabled true -port 443
```

9. Verify that the object store was created successfully: `storage aggregate object-store show -instance`
10. Attach the object store to the aggregate. This should be repeated for every new aggregate: `storage aggregate object-store attach -aggregate <aggr1> -object-store-name <S3Bucket>`

Copyright information

Trademark information