Get started
Cloud Volumes ONTAP
NetApp
November 08, 2023
# Table of Contents

Get started .................................................................................................................. 1
  Learn about Cloud Volumes ONTAP ........................................................................ 1
  Supported versions for new deployments ............................................................... 2
  Get started in Amazon Web Services ...................................................................... 4
  Get started in Microsoft Azure ............................................................................... 71
  Get started in Google Cloud ................................................................................... 106
Get started

Learn about Cloud Volumes ONTAP

Cloud Volumes ONTAP enables you to optimize your cloud storage costs and performance while enhancing data protection, security, and compliance.

Cloud Volumes ONTAP is a software-only storage appliance that runs ONTAP data management software in the cloud. It provides enterprise-grade storage with the following key features:

• Storage efficiencies
  Leverage built-in data deduplication, data compression, thin provisioning, and cloning to minimize storage costs.

• High availability
  Ensure enterprise reliability and continuous operations in case of failures in your cloud environment.

• Data protection
  Cloud Volumes ONTAP leverages SnapMirror, NetApp’s industry-leading replication technology, to replicate on-premises data to the cloud so it’s easy to have secondary copies available for multiple use cases.

Cloud Volumes ONTAP also integrates with BlueXP backup and recovery to deliver backup and restore capabilities for protection, and long-term archive of your cloud data.

Learn more about BlueXP backup and recovery

• Data tiering
  Switch between high and low-performance storage pools on-demand without taking applications offline.

• Application consistency
  Ensure consistency of NetApp Snapshot copies using NetApp SnapCenter.

Learn more about SnapCenter

• Data security
  Cloud Volumes ONTAP supports data encryption and provides protection against viruses and ransomware.

• Privacy compliance controls
  Integration with BlueXP classification helps you understand data context and identify sensitive data.

Learn more about BlueXP classification

Licenses for ONTAP features are included with Cloud Volumes ONTAP.

View supported Cloud Volumes ONTAP configurations
Learn more about Cloud Volumes ONTAP

**Supported versions for new deployments**

BlueXP enables you to choose from several different ONTAP versions when you create a new Cloud Volumes ONTAP working environment.

All other Cloud Volumes ONTAP versions are not supported with new deployments.

**AWS**

**Single node**
- 9.14.0 GA
- 9.13.1 GA
- 9.12.1 GA
- 9.12.1 RC1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9.8
- 9.7 P5
- 9.5 P6

**HA pair**
- 9.14.0 GA
- 9.13.1 GA
- 9.12.1 GA
- 9.12.1 RC1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9.8
- 9.7 P5
- 9.5 P6

**Azure**

**Single node**
- 9.14.0 GA
- 9.13.1 GA
• 9.12.1 GA
• 9.12.1 RC1
• 9.11.1 P3
• 9.10.1 P3
• 9.9.1 P8
• 9.9.1 P7
• 9.8 P10
• 9.7 P6
• 9.5 P6

HA pair
• 9.14.0 GA
• 9.13.1 GA
• 9.12.1 GA
• 9.12.1 RC1
• 9.11.1 P3
• 9.10.1 P3
• 9.9.1 P8
• 9.9.1 P7
• 9.8 P10
• 9.7 P6

Google Cloud

Single node
• 9.14.0 GA
• 9.13.1 GA
• 9.12.1 GA
• 9.12.1 RC1
• 9.12.0 P1
• 9.11.1 P3
• 9.10.1
• 9.9.1 P6
• 9.8
• 9.7 P5

HA pair
• 9.14.0 GA
• 9.13.1 GA
• 9.12.1 GA
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 \textit{key user}. Learn more.

5 Launch Cloud Volumes ONTAP using BlueXP

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

Related links

- Creating a Connector from BlueXP
- Launching a Connector from the AWS Marketplace
- Installing the Connector software on a Linux host
- What BlueXP does with AWS permissions

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. \textit{View the full list of supported regions.}

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

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

<table>
<thead>
<tr>
<th>AWS information</th>
<th>Your value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Region</td>
<td></td>
</tr>
<tr>
<td>VPC</td>
<td></td>
</tr>
<tr>
<td>Subnet</td>
<td></td>
</tr>
<tr>
<td>Security group (if using your own)</td>
<td></td>
</tr>
</tbody>
</table>
### HA pair in multiple AZs

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

### 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 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 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.

<table>
<thead>
<tr>
<th>LIF</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster management</td>
<td>Administrative management of the entire cluster (HA pair).</td>
</tr>
<tr>
<td>Node management</td>
<td>Administrative management of a node.</td>
</tr>
<tr>
<td>Intercluster</td>
<td>Cross-cluster communication, backup, and replication.</td>
</tr>
<tr>
<td>NAS data</td>
<td>Client access over NAS protocols.</td>
</tr>
<tr>
<td>iSCSI data</td>
<td>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.</td>
</tr>
<tr>
<td>Storage VM management</td>
<td>A storage VM management LIF is used with management tools like SnapCenter.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>LIF</th>
<th>Interface</th>
<th>Node</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster management</td>
<td>eth0</td>
<td>node 1</td>
<td>Administrative management of the entire cluster (HA pair).</td>
</tr>
<tr>
<td>Node management</td>
<td>eth0</td>
<td>node 1 and node 2</td>
<td>Administrative management of a node.</td>
</tr>
<tr>
<td>Intercluster</td>
<td>eth0</td>
<td>node 1 and node 2</td>
<td>Cross-cluster communication, backup, and replication.</td>
</tr>
<tr>
<td>NAS data</td>
<td>eth0</td>
<td>node 1</td>
<td>Client access over NAS protocols.</td>
</tr>
<tr>
<td>LIF</td>
<td>Interface</td>
<td>Node</td>
<td>Purpose</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------</td>
<td>----------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>iSCSI data</td>
<td>eth0</td>
<td>node 1 and node 2</td>
<td>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.</td>
</tr>
<tr>
<td>Cluster connectivity</td>
<td>eth1</td>
<td>node 1 and node 2</td>
<td>Enables the nodes to communicate with each other and to move data within the cluster.</td>
</tr>
<tr>
<td>HA connectivity</td>
<td>eth2</td>
<td>node 1 and node 2</td>
<td>Communication between the two nodes in case of failover.</td>
</tr>
<tr>
<td>RSM iSCSI traffic</td>
<td>eth3</td>
<td>node 1 and node 2</td>
<td>RAID SyncMirror iSCSI traffic, as well as communication between the two Cloud Volumes ONTAP nodes and the mediator.</td>
</tr>
<tr>
<td>Mediator</td>
<td>eth0</td>
<td>Mediator</td>
<td>A communication channel between the nodes and the mediator to assist in storage takeover and giveback processes.</td>
</tr>
</tbody>
</table>

**LIFs for HA pairs in multiple AZs**

<table>
<thead>
<tr>
<th>LIF</th>
<th>Interface</th>
<th>Node</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node management</td>
<td>eth0</td>
<td>node 1 and node 2</td>
<td>Administrative management of a node.</td>
</tr>
<tr>
<td>Intercluster</td>
<td>eth0</td>
<td>node 1 and node 2</td>
<td>Cross-cluster communication, backup, and replication.</td>
</tr>
<tr>
<td>iSCSI data</td>
<td>eth0</td>
<td>node 1 and node 2</td>
<td>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.</td>
</tr>
<tr>
<td>Cluster connectivity</td>
<td>eth1</td>
<td>node 1 and node 2</td>
<td>Enables the nodes to communicate with each other and to move data within the cluster.</td>
</tr>
<tr>
<td>HA connectivity</td>
<td>eth2</td>
<td>node 1 and node 2</td>
<td>Communication between the two nodes in case of failover.</td>
</tr>
<tr>
<td>RSM iSCSI traffic</td>
<td>eth3</td>
<td>node 1 and node 2</td>
<td>RAID SyncMirror iSCSI traffic, as well as communication between the two Cloud Volumes ONTAP nodes and the mediator.</td>
</tr>
<tr>
<td>Mediator</td>
<td>eth0</td>
<td>Mediator</td>
<td>A communication channel between the nodes and the mediator to assist in storage takeover and giveback processes.</td>
</tr>
</tbody>
</table>

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.

Connection for data tiering

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

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

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

Connections to ONTAP systems

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

DNS and Active Directory for CIFS

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

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


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, see High-availability pairs.
Availability Zones

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

A subnet should be available in each Availability Zone.

Floating IP addresses for NAS data and cluster/SVM management

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

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

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

You need to enter the floating IP addresses in 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 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:

   **NFS & CIFS access from within the VPC using Floating IP**

<table>
<thead>
<tr>
<th>Auto failover</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster Management: 172.23.0.1</td>
</tr>
<tr>
<td>Data (nfs,cifs): Node 1: 172.23.0.2</td>
</tr>
</tbody>
</table>

   **Access**

   | SVM Management: 172.23.0.4 |

   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.

   ![Route Table Image]

   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:

   ```json
   "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:

     ```json
     "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 your to use own security groups.
Rules for Cloud Volumes ONTAP

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

**Inbound rules**

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

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

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

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Port</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>All ICMP</td>
<td>All</td>
<td>All outbound traffic</td>
</tr>
<tr>
<td>All TCP</td>
<td>All</td>
<td>All outbound traffic</td>
</tr>
<tr>
<td>All UDP</td>
<td>All</td>
<td>All outbound traffic</td>
</tr>
</tbody>
</table>

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.
<table>
<thead>
<tr>
<th>Service</th>
<th>Protocol</th>
<th>Port</th>
<th>Source</th>
<th>Destination</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Directory</td>
<td>TCP</td>
<td>88</td>
<td>Node management LIF</td>
<td>Active Directory forest</td>
<td>Kerberos V authentication</td>
</tr>
<tr>
<td></td>
<td>UDP</td>
<td>137</td>
<td>Node management LIF</td>
<td>Active Directory forest</td>
<td>NetBIOS name service</td>
</tr>
<tr>
<td></td>
<td>UDP</td>
<td>138</td>
<td>Node management LIF</td>
<td>Active Directory forest</td>
<td>NetBIOS datagram service</td>
</tr>
<tr>
<td></td>
<td>TCP</td>
<td>139</td>
<td>Node management LIF</td>
<td>Active Directory forest</td>
<td>NetBIOS service session</td>
</tr>
<tr>
<td></td>
<td>TCP &amp; UDP</td>
<td>389</td>
<td>Node management LIF</td>
<td>Active Directory forest</td>
<td>LDAP</td>
</tr>
<tr>
<td></td>
<td>TCP</td>
<td>445</td>
<td>Node management LIF</td>
<td>Active Directory forest</td>
<td>Microsoft SMB/CIFS over TCP with NetBIOS framing</td>
</tr>
<tr>
<td></td>
<td>TCP</td>
<td>464</td>
<td>Node management LIF</td>
<td>Active Directory forest</td>
<td>Kerberos V change &amp; set password (SET_CHANGE)</td>
</tr>
<tr>
<td></td>
<td>UDP</td>
<td>464</td>
<td>Node management LIF</td>
<td>Active Directory forest</td>
<td>Kerberos key administration</td>
</tr>
<tr>
<td></td>
<td>TCP</td>
<td>749</td>
<td>Node management LIF</td>
<td>Active Directory forest</td>
<td>Kerberos V change &amp; set Password (RPCSEC_GSS)</td>
</tr>
<tr>
<td></td>
<td>TCP</td>
<td>88</td>
<td>Data LIF (NFS, CIFS)</td>
<td>Active Directory forest</td>
<td>Kerberos V authentication</td>
</tr>
<tr>
<td></td>
<td>UDP</td>
<td>137</td>
<td>Data LIF (NFS, CIFS)</td>
<td>Active Directory forest</td>
<td>NetBIOS name service</td>
</tr>
<tr>
<td></td>
<td>UDP</td>
<td>138</td>
<td>Data LIF (NFS, CIFS)</td>
<td>Active Directory forest</td>
<td>NetBIOS datagram service</td>
</tr>
<tr>
<td></td>
<td>TCP</td>
<td>139</td>
<td>Data LIF (NFS, CIFS)</td>
<td>Active Directory forest</td>
<td>NetBIOS service session</td>
</tr>
<tr>
<td></td>
<td>TCP &amp; UDP</td>
<td>389</td>
<td>Data LIF (NFS, CIFS)</td>
<td>Active Directory forest</td>
<td>LDAP</td>
</tr>
<tr>
<td></td>
<td>TCP</td>
<td>445</td>
<td>Data LIF (NFS, CIFS)</td>
<td>Active Directory forest</td>
<td>Microsoft SMB/CIFS over TCP with NetBIOS framing</td>
</tr>
<tr>
<td></td>
<td>TCP</td>
<td>464</td>
<td>Data LIF (NFS, CIFS)</td>
<td>Active Directory forest</td>
<td>Kerberos V change &amp; set password (SET_CHANGE)</td>
</tr>
<tr>
<td></td>
<td>UDP</td>
<td>464</td>
<td>Data LIF (NFS, CIFS)</td>
<td>Active Directory forest</td>
<td>Kerberos key administration</td>
</tr>
<tr>
<td></td>
<td>TCP</td>
<td>749</td>
<td>Data LIF (NFS, CIFS)</td>
<td>Active Directory forest</td>
<td>Kerberos V change &amp; set password (RPCSEC_GSS)</td>
</tr>
<tr>
<td>Service</td>
<td>Protocol</td>
<td>Port</td>
<td>Source</td>
<td>Destination</td>
<td>Purpose</td>
</tr>
<tr>
<td>------------------</td>
<td>----------</td>
<td>------</td>
<td>-------------------</td>
<td>---------------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>AutoSupport</td>
<td>HTTPS</td>
<td>443</td>
<td>Node management LIF</td>
<td>support.netapp.com</td>
<td>AutoSupport (HTTPS is the default)</td>
</tr>
<tr>
<td></td>
<td>HTTP</td>
<td>80</td>
<td>Node management LIF</td>
<td>support.netapp.com</td>
<td>AutoSupport (only if the transport protocol is changed from HTTPS to HTTP)</td>
</tr>
<tr>
<td></td>
<td>TCP</td>
<td>3128</td>
<td>Node management LIF</td>
<td>Connector</td>
<td>Sending AutoSupport messages through a proxy server on the Connector, if an outbound internet connection isn't available</td>
</tr>
<tr>
<td>Backup to S3</td>
<td>TCP</td>
<td>5010</td>
<td>Intercluster LIF</td>
<td>Backup endpoint or restore endpoint</td>
<td>Back up and restore operations for the Backup to S3 feature</td>
</tr>
<tr>
<td>Cluster</td>
<td>All traffic</td>
<td>All traffic</td>
<td>All LIFs on one node</td>
<td>All LIFs on the other node</td>
<td>Intercluster communications (Cloud Volumes ONTAP HA only)</td>
</tr>
<tr>
<td></td>
<td>TCP</td>
<td>3000</td>
<td>Node management LIF</td>
<td>HA mediator</td>
<td>ZAPI calls (Cloud Volumes ONTAP HA only)</td>
</tr>
<tr>
<td></td>
<td>ICMP</td>
<td>1</td>
<td>Node management LIF</td>
<td>HA mediator</td>
<td>Keep alive (Cloud Volumes ONTAP HA only)</td>
</tr>
<tr>
<td>Configuration backups</td>
<td>HTTP</td>
<td>80</td>
<td>Node management LIF</td>
<td>http://&lt;connector-IP-address&gt;/occm/offboxconfig</td>
<td>Send configuration backups to the Connector. Learn about configuration backup files.</td>
</tr>
<tr>
<td></td>
<td>DHCP</td>
<td>68</td>
<td>Node management LIF</td>
<td>DHCP</td>
<td>DHCP client for first-time setup</td>
</tr>
<tr>
<td></td>
<td>DHCPS</td>
<td>67</td>
<td>Node management LIF</td>
<td>DHCP</td>
<td>DHCP server</td>
</tr>
<tr>
<td></td>
<td>DNS</td>
<td>53</td>
<td>Node management LIF and data LIF (NFS, CIFS)</td>
<td>DNS</td>
<td>DNS</td>
</tr>
<tr>
<td></td>
<td>NDMP</td>
<td>TCP</td>
<td>Node management LIF</td>
<td>Destination servers</td>
<td>NDMP copy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1860</td>
<td>Node management LIF</td>
<td>Destination servers</td>
<td>NDMP copy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0–1869</td>
<td>Node management LIF</td>
<td>Destination servers</td>
<td>NDMP copy</td>
</tr>
<tr>
<td></td>
<td>SMTP</td>
<td>TCP</td>
<td>Node management LIF</td>
<td>Mail server</td>
<td>SMTP alerts, can be used for AutoSupport</td>
</tr>
<tr>
<td></td>
<td>SNMP</td>
<td>TCP</td>
<td>Node management LIF</td>
<td>Monitor server</td>
<td>Monitoring by SNMP traps</td>
</tr>
<tr>
<td></td>
<td></td>
<td>161</td>
<td>Node management LIF</td>
<td>Monitor server</td>
<td>Monitoring by SNMP traps</td>
</tr>
<tr>
<td></td>
<td></td>
<td>UDP</td>
<td>Node management LIF</td>
<td>Monitor server</td>
<td>Monitoring by SNMP traps</td>
</tr>
<tr>
<td></td>
<td></td>
<td>162</td>
<td>Node management LIF</td>
<td>Monitor server</td>
<td>Monitoring by SNMP traps</td>
</tr>
<tr>
<td></td>
<td></td>
<td>UDP</td>
<td>Node management LIF</td>
<td>Monitor server</td>
<td>Monitoring by SNMP traps</td>
</tr>
<tr>
<td>Service</td>
<td>Protocol</td>
<td>Port</td>
<td>Source</td>
<td>Destination</td>
<td>Purpose</td>
</tr>
<tr>
<td>---------------</td>
<td>----------</td>
<td>------</td>
<td>----------------------</td>
<td>----------------------</td>
<td>---------------------------------------------------</td>
</tr>
<tr>
<td>SnapMirror</td>
<td>TCP</td>
<td>1110</td>
<td>Intercluster LIF</td>
<td>ONTAP intercluster LIFs</td>
<td>Management of intercluster communication sessions for SnapMirror</td>
</tr>
<tr>
<td></td>
<td>TCP</td>
<td>514</td>
<td>Node management LIF</td>
<td>Syslog server</td>
<td>Syslog forward messages</td>
</tr>
</tbody>
</table>

### 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.

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Port</th>
<th>Source</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
<td>3000</td>
<td>CIDR of the Connector</td>
<td>RESTful API access from the Connector</td>
</tr>
</tbody>
</table>

#### 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.

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Port</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>All TCP</td>
<td>All</td>
<td>All outbound traffic</td>
</tr>
<tr>
<td>All UDP</td>
<td>All</td>
<td>All outbound traffic</td>
</tr>
</tbody>
</table>

#### 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.

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Port</th>
<th>Destination</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP</td>
<td>80</td>
<td>IP address of the Connector on AWS EC2 instance</td>
<td>Download upgrades for the mediator</td>
</tr>
<tr>
<td>HTTPS</td>
<td>443</td>
<td>ec2.amazonaws.com</td>
<td>Assist with storage failover</td>
</tr>
<tr>
<td>UDP</td>
<td>53</td>
<td>ec2.amazonaws.com</td>
<td>Assist with storage failover</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Port</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>All traffic</td>
<td>All</td>
<td>Communication between the HA mediator and HA nodes</td>
</tr>
</tbody>
</table>

**Outbound rules**

The predefined security group includes the following outbound rules.

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Port</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>All traffic</td>
<td>All</td>
<td>Communication between the HA mediator and HA nodes</td>
</tr>
</tbody>
</table>

**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.
For additional details about this process, see 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 the AWS Commercial Cloud Services Environment.

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

```json
{
    "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"
    }]
}
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

```json
{
   "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
```json
{
   "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"
      }
   ]
}
```
{  
    "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"
        }
    ]
}
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.
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.
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, see 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, see 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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Working Environment Name</td>
<td>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.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Add tags</td>
<td>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.</td>
</tr>
<tr>
<td>User name and password</td>
<td>These are the credentials for the Cloud Volumes ONTAP cluster administrator account. You can use these credentials to connect to Cloud Volumes ONTAP through System Manager or its CLI. Keep the default admin user name or change it to a custom user name.</td>
</tr>
<tr>
<td>Edit Credentials</td>
<td>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.</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPC</td>
<td>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.</td>
</tr>
<tr>
<td>Generated security group</td>
<td>If you let BlueXP generate the security group for you, you need to choose how you'll allow traffic:</td>
</tr>
<tr>
<td></td>
<td>• If you choose <strong>Selected VPC only</strong>, 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.</td>
</tr>
<tr>
<td></td>
<td>• If you choose <strong>All VPCs</strong>, the source for inbound traffic is the 0.0.0.0/0 IP range.</td>
</tr>
<tr>
<td>Use existing security group</td>
<td>If you use an existing firewall policy, ensure that it includes the required rules. Learn about firewall rules for Cloud Volumes ONTAP.</td>
</tr>
</tbody>
</table>

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
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 9.10.1 and 9.10.1 P4 is available. The update does not occur from one release to another—for example, from 9.6 to 9.7.

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
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Size</td>
<td>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.</td>
</tr>
<tr>
<td>Access control (for NFS only)</td>
<td>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.</td>
</tr>
<tr>
<td>Permissions and Users / Groups (for CIFS only)</td>
<td>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.</td>
</tr>
<tr>
<td>Snapshot Policy</td>
<td>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.</td>
</tr>
<tr>
<td>Advanced options (for NFS only)</td>
<td>Select an NFS version for the volume: either NFSv3 or NFSv4.</td>
</tr>
<tr>
<td>Initiator group and IQN (for iSCSI only)</td>
<td>iSCSI storage targets are called LUNs (logical units) and are presented to hosts as standard block devices.</td>
</tr>
<tr>
<td></td>
<td>Initiator groups are tables of iSCSI host node names and control which initiators have access to which LUNs.</td>
</tr>
<tr>
<td></td>
<td>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 bus adapters (HBAs) and are identified by iSCSI qualified names (IQNs).</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS Primary and Secondary IP Address</td>
<td>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.</td>
</tr>
<tr>
<td>Active Directory Domain to join</td>
<td>The FQDN of the Active Directory (AD) domain that you want the CIFS server to join.</td>
</tr>
<tr>
<td>Credentials authorized to join the domain</td>
<td>The name and password of a Windows account with sufficient privileges to add computers to the specified Organizational Unit (OU) within the AD domain.</td>
</tr>
<tr>
<td>CIFS server NetBIOS name</td>
<td>A CIFS server name that is unique in the AD domain.</td>
</tr>
<tr>
<td>Organizational Unit</td>
<td>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 <strong>OU=Computers,OU=corp</strong> in this field.</td>
</tr>
<tr>
<td>DNS Domain</td>
<td>The DNS domain for the Cloud Volumes ONTAP storage virtual machine (SVM). In most cases, the domain is the same as the AD domain.</td>
</tr>
<tr>
<td>NTP Server</td>
<td>Select <strong>Use Active Directory Domain</strong> 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. See the <a href="#">BlueXP automation docs</a> 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.</td>
</tr>
</tbody>
</table>

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, see [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 System Manager or the 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**.
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:
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Working Environment Name</td>
<td>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.</td>
</tr>
<tr>
<td>Add tags</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>For information about tags, refer to <a href="#">AWS Documentation: Tagging your Amazon EC2 Resources</a>.</td>
</tr>
<tr>
<td>User name and password</td>
<td>These are the credentials for the Cloud Volumes ONTAP cluster administrator account. You can use these credentials to connect to Cloud Volumes ONTAP through System Manager or its CLI. Keep the default admin user name or change it to a custom user name.</td>
</tr>
<tr>
<td>Edit Credentials</td>
<td>Choose the AWS credentials and marketplace subscription to use with this Cloud Volumes ONTAP system.</td>
</tr>
<tr>
<td></td>
<td>Click <strong>Add Subscription</strong> 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.</td>
</tr>
<tr>
<td></td>
<td>If purchased a license directly from NetApp (BYOL), then an AWS subscription isn’t required.</td>
</tr>
<tr>
<td></td>
<td>Learn how to add additional AWS credentials to BlueXP.</td>
</tr>
</tbody>
</table>

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.

![Subscribe to BlueXP from the AWS Marketplace](#)

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, see [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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generated security group</td>
<td>If you let BlueXP generate the security group for you, you need to choose how you'll allow traffic:</td>
</tr>
<tr>
<td></td>
<td>• If you choose <strong>Selected VPC only</strong>, 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.</td>
</tr>
<tr>
<td></td>
<td>• If you choose <strong>All VPCs</strong>, the source for inbound traffic is the 0.0.0.0/0 IP range.</td>
</tr>
<tr>
<td>Use existing security group</td>
<td>If you use an existing firewall policy, ensure that it includes the required rules. Learn about firewall rules for Cloud Volumes ONTAP.</td>
</tr>
</tbody>
</table>

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, see [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 [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 9.10.1 and 9.10.1 P4 is available. The update does not occur from one release to another—for example, from 9.6 to 9.7.

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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Size</td>
<td>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.</td>
</tr>
<tr>
<td>Access control (for NFS only)</td>
<td>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.</td>
</tr>
<tr>
<td>Permissions and Users / Groups (for CIFS only)</td>
<td>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.</td>
</tr>
<tr>
<td>Snapshot Policy</td>
<td>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.</td>
</tr>
<tr>
<td>Advanced options (for NFS only)</td>
<td>Select an NFS version for the volume: either NFSv3 or NFSv4.</td>
</tr>
</tbody>
</table>
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:

---

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS Primary and Secondary IP Address</td>
<td>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.</td>
</tr>
<tr>
<td>Active Directory Domain to join</td>
<td>The FQDN of the Active Directory (AD) domain that you want the CIFS server to join.</td>
</tr>
<tr>
<td>Credentials authorized to join the domain</td>
<td>The name and password of a Windows account with sufficient privileges to add computers to the specified Organizational Unit (OU) within the AD domain.</td>
</tr>
<tr>
<td>CIFS server NetBIOS name</td>
<td>A CIFS server name that is unique in the AD domain.</td>
</tr>
</tbody>
</table>

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

---
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organizational Unit</td>
<td>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 <strong>OU=Computers,OU=corp</strong> in this field.</td>
</tr>
<tr>
<td>DNS Domain</td>
<td>The DNS domain for the Cloud Volumes ONTAP storage virtual machine (SVM). In most cases, the domain is the same as the AD domain.</td>
</tr>
<tr>
<td>NTP Server</td>
<td>Select <strong>Use Active Directory Domain</strong> 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. See the <strong>BlueXP automation docs</strong> 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.</td>
</tr>
</tbody>
</table>

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, see **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 System Manager or the CLI.

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

**Get started with Cloud Volumes ONTAP in the AWS C2S environment**

Similar to a standard AWS region, you can use Cloud Manager in the **AWS Commercial Cloud Services (C2S)** environment to deploy Cloud Volumes ONTAP, which provides enterprise-class features for your cloud storage. AWS C2S is a closed region specific to the U.S. Intelligence Community; the instructions on this page only apply to AWS C2S.
Support versions in C2S

- Cloud Volumes ONTAP 9.8 is supported
- Version 3.9.4 of the Connector is supported

The Connector is software that’s required to deploy and manage Cloud Volumes ONTAP in AWS. You’ll log in to Cloud Manager from the software that gets installed on the Connector instance. The SaaS website for Cloud Manager isn’t supported in the C2S environment.

Cloud Manager was recently renamed to BlueXP, but we’re continuing to refer to it as Cloud Manager in C2S because the user interface that’s included with version 3.9.4 of the Connector is still called Cloud Manager.

Supported features in C2S

The following features are available from Cloud Manager in the C2S environment:

- Cloud Volumes ONTAP
- Data replication
- A timeline for auditing

For Cloud Volumes ONTAP, you can create a single node system or an HA pair. Both licensing options are available: pay-as-you-go and bring your own license (BYOL).

Data tiering to S3 is also supported with Cloud Volumes ONTAP in C2S.

Limitations

- None of NetApp’s cloud services are available from Cloud Manager.
- Because there’s no internet access in the C2S environment, the following features aren’t available either:
  - Automated software upgrades from Cloud Manager
  - NetApp AutoSupport
  - AWS cost information for Cloud Volumes ONTAP resources
- Freemium licenses are not supported in the C2S environment.

Deployment overview

Getting started with Cloud Volumes ONTAP in C2S includes a few steps.

1. Preparing your AWS environment

   This includes setting up networking, subscribing to Cloud Volumes ONTAP, setting up permissions, and optionally setting up the AWS KMS.

2. Installing the Connector and setting up Cloud Manager

   Before you can start using Cloud Manager to deploy Cloud Volumes ONTAP, you’ll need to create a Connector. The Connector enables Cloud Manager to manage resources and processes within your public
cloud environment (this includes Cloud Volumes ONTAP).

You’ll log in to Cloud Manager from the software that gets installed on the Connector instance.

3. Launching Cloud Volumes ONTAP from Cloud Manager

Each of these steps are described below.

Preparing your AWS environment

Your AWS environment must meet a few requirements.

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.

Subscribe to Cloud Volumes ONTAP

A Marketplace subscription is required to deploy Cloud Volumes ONTAP from Cloud Manager.

Steps

1. Go to the AWS Intelligence Community Marketplace and search for Cloud Volumes ONTAP.
2. Select the offering that you plan to deploy.
3. Review the terms and click Accept.
4. Repeat these steps for the other offerings, if you plan to deploy them.

   You must use Cloud Manager to launch Cloud Volumes ONTAP instances. You must not launch Cloud Volumes ONTAP instances from the EC2 console.

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 Commercial Cloud Services environment.

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

• The Connector instance
• Cloud Volumes ONTAP instances
• 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.

```json
{
   "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:GetBucketTagging",
  "s3:ListBucketVersions"
],
"Resource": [
  "arn:aws-iso:s3:::fabric-pool*"
]}
},
{
"Effect": "Allow",
"Action": [
  "ec2:StartInstances",
  "ec2:StopInstances",
  "ec2:TerminateInstances",
  "ec2:CreatePlacementGroup",
  "ec2:DeletePlacementGroup"
],
"Resource": "*
"
3. Create a policy for Cloud Volumes ONTAP.
4. If you plan to deploy a Cloud Volumes ONTAP HA pair, create a policy for the HA mediator.

```json
{
    "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": "*"
    }]
}
```
5. Create IAM roles with the role type Amazon EC2 and attach the policies that you created in the previous steps.

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).

You must select the Connector IAM role when you launch the Connector instance.

You can select the IAM roles for Cloud Volumes ONTAP and the HA mediator when you create a Cloud Volumes ONTAP working environment from Cloud Manager.

**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.

**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 Cloud Manager 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 Cloud Manager permissions to use the CMK with Cloud Volumes ONTAP.

**Installing the Connector and setting up Cloud Manager**

Before you can launch Cloud Volumes ONTAP systems in AWS, you must first launch the Connector instance from the AWS Marketplace and then log in and set up Cloud Manager.

**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.

   You’ll need to upload the certificate during the setup process. Cloud Manager 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 Cloud Manager.
   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 preparing your AWS environment.
You should keep the default storage options.

The required connection methods for the Connector are as follows: SSH, HTTP, and HTTPS.

3. Set up Cloud Manager 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. Complete the steps in the Setup wizard to set up Cloud Manager.
      - **System Details**: Enter a name for this instance of Cloud Manager and provide your company name.
      - **Create User**: Create the Admin user that you’ll use to administer Cloud Manager.
      - **Review**: Review the details and approve the end user license agreement.
   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.

**Launching Cloud Volumes ONTAP from Cloud Manager**

You can launch Cloud Volumes ONTAP instances in the AWS Commercial Cloud Services environment by creating new working environments in Cloud Manager.

**What you’ll need**

- If you purchased a license, you must have the license file that you received from NetApp. The license file is a .NLF file in JSON format.
- 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 or Cloud Volumes ONTAP HA.
3. Complete the steps in the wizard to launch the Cloud Volumes ONTAP system.

Note the following as you complete the wizard:

- If you want to deploy Cloud Volumes ONTAP HA in multiple Availability Zones, deploy the configuration as follows because only two AZs were available in the AWS Commercial Cloud Services environment at the time of publication:
  - Node 1: Availability Zone A
  - Node 2: Availability Zone B
  - Mediator: Availability Zone A or B
- 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.

Storage efficiency features can improve storage utilization and reduce the total amount of storage that you need.

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

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

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

Inbound rules

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Port</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSH</td>
<td>22</td>
<td>Provides SSH access to the Connector host</td>
</tr>
<tr>
<td>HTTP</td>
<td>80</td>
<td>Provides HTTP access from client web browsers to the local user interface</td>
</tr>
<tr>
<td>HTTPS</td>
<td>443</td>
<td>Provides HTTPS access from client web browsers to the local user interface</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Port</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>All TCP</td>
<td>All</td>
<td>All outbound traffic</td>
</tr>
<tr>
<td>All UDP</td>
<td>All</td>
<td>All outbound traffic</td>
</tr>
</tbody>
</table>

Security group for Cloud Volumes ONTAP
The security group for Cloud Volumes ONTAP nodes 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.

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Port</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>All ICMP</td>
<td>All</td>
<td>Pinging the instance</td>
</tr>
<tr>
<td>HTTP</td>
<td>80</td>
<td>HTTP access to the System Manager web console using the IP address of the cluster management LIF</td>
</tr>
<tr>
<td>HTTPS</td>
<td>443</td>
<td>HTTPS access to the System Manager web console using the IP address of the cluster management LIF</td>
</tr>
<tr>
<td>SSH</td>
<td>22</td>
<td>SSH access to the IP address of the cluster management LIF or a node management LIF</td>
</tr>
<tr>
<td>TCP</td>
<td>111</td>
<td>Remote procedure call for NFS</td>
</tr>
<tr>
<td>TCP</td>
<td>139</td>
<td>NetBIOS service session for CIFS</td>
</tr>
<tr>
<td>TCP</td>
<td>161-162</td>
<td>Simple network management protocol</td>
</tr>
<tr>
<td>TCP</td>
<td>445</td>
<td>Microsoft SMB/CIFS over TCP with NetBIOS framing</td>
</tr>
<tr>
<td>TCP</td>
<td>635</td>
<td>NFS mount</td>
</tr>
<tr>
<td>TCP</td>
<td>749</td>
<td>Kerberos</td>
</tr>
<tr>
<td>TCP</td>
<td>2049</td>
<td>NFS server daemon</td>
</tr>
<tr>
<td>TCP</td>
<td>3260</td>
<td>iSCSI access through the iSCSI data LIF</td>
</tr>
<tr>
<td>TCP</td>
<td>4045</td>
<td>NFS lock daemon</td>
</tr>
<tr>
<td>TCP</td>
<td>4046</td>
<td>Network status monitor for NFS</td>
</tr>
<tr>
<td>TCP</td>
<td>10000</td>
<td>Backup using NDMP</td>
</tr>
<tr>
<td>TCP</td>
<td>11104</td>
<td>Management of intercluster communication sessions for SnapMirror</td>
</tr>
<tr>
<td>TCP</td>
<td>11105</td>
<td>SnapMirror data transfer using intercluster LIFs</td>
</tr>
<tr>
<td>UDP</td>
<td>111</td>
<td>Remote procedure call for NFS</td>
</tr>
<tr>
<td>UDP</td>
<td>161-162</td>
<td>Simple network management protocol</td>
</tr>
<tr>
<td>UDP</td>
<td>635</td>
<td>NFS mount</td>
</tr>
<tr>
<td>UDP</td>
<td>2049</td>
<td>NFS server daemon</td>
</tr>
<tr>
<td>UDP</td>
<td>4045</td>
<td>NFS lock daemon</td>
</tr>
<tr>
<td>UDP</td>
<td>4046</td>
<td>Network status monitor for NFS</td>
</tr>
<tr>
<td>UDP</td>
<td>4049</td>
<td>NFS rquotad protocol</td>
</tr>
</tbody>
</table>
Outbound rules

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

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Port</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>All ICMP</td>
<td>All</td>
<td>All outbound traffic</td>
</tr>
<tr>
<td>All TCP</td>
<td>All</td>
<td>All outbound traffic</td>
</tr>
<tr>
<td>All UDP</td>
<td>All</td>
<td>All outbound traffic</td>
</tr>
</tbody>
</table>

External security group for the HA mediator

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

Inbound rules

The source for inbound rules is traffic from the VPC where the Connector resides.

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Port</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSH</td>
<td>22</td>
<td>SSH connections to the HA mediator</td>
</tr>
<tr>
<td>TCP</td>
<td>3000</td>
<td>RESTful API access from the Connector</td>
</tr>
</tbody>
</table>

Outbound rules

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

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Port</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>All TCP</td>
<td>All</td>
<td>All outbound traffic</td>
</tr>
<tr>
<td>All UDP</td>
<td>All</td>
<td>All outbound traffic</td>
</tr>
</tbody>
</table>

Internal security group for the HA mediator

The predefined internal security group for the Cloud Volumes ONTAP HA mediator includes the following rules. Cloud Manager always creates this security group. You don’t have the option to use your own.

Inbound rules

The predefined security group includes the following inbound rules.

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Port</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>All traffic</td>
<td>All</td>
<td>Communication between the HA mediator and HA nodes</td>
</tr>
</tbody>
</table>

Outbound rules

The predefined security group includes the following outbound rules.
<table>
<thead>
<tr>
<th>Protocol</th>
<th>Port</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>All traffic</td>
<td>All</td>
<td>Communication between the HA mediator and HA nodes</td>
</tr>
</tbody>
</table>

Get started in Microsoft Azure

Quick start for Cloud Volumes ONTAP in Azure

Get started with Cloud Volumes ONTAP for Azure 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 Azure.

   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 VNet 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.

   Learn more about networking requirements.

4. **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

- Creating a Connector from BlueXP
- Creating a Connector from the Azure Marketplace
- Installing the Connector software on a Linux host
- What BlueXP does with permissions
Plan your Cloud Volumes ONTAP configuration in Azure

When you deploy Cloud Volumes ONTAP in Azure, 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 Microsoft Azure regions. View the full list of supported regions.

Choose a supported VM type

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

Supported configurations for Cloud Volumes ONTAP in Azure

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 Azure

Size your system in Azure

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 a VM type, disk type, and disk size:

Virtual machine type

Look at the supported virtual machine types in the Cloud Volumes ONTAP Release Notes and then review details about each supported VM type. Be aware that each VM type supports a specific number of data disks.

- Azure documentation: General purpose virtual machine sizes
- Azure documentation: Memory optimized virtual machine sizes

Azure disk type with single node systems

When you create volumes for Cloud Volumes ONTAP, you need to choose the underlying cloud storage that Cloud Volumes ONTAP uses as a disk.

Single node systems can use three types of Azure Managed Disks:

- Premium SSD Managed Disks provide high performance for I/O-intensive workloads at a higher cost.
• **Standard SSD Managed Disks** provide consistent performance for workloads that require low IOPS.

• **Standard HDD Managed Disks** are a good choice if you don’t need high IOPS and want to reduce your costs.

For additional details about the use cases for these disks, see Microsoft Azure Documentation: What disk types are available in Azure?.

**Azure disk type with HA pairs**

HA systems use Premium SSD Shared Managed Disks which both provide high performance for I/O-intensive workloads at a higher cost. HA deployments created before the 9.12.1 release use Premium page blobs.

**Azure disk size**

When you launch Cloud Volumes ONTAP instances, you must choose the default disk size for aggregates. BlueXP uses this disk size for the initial aggregate, and for any additional aggregates that it creates when you use the simple provisioning option. You can create aggregates that use a disk size different from the default by using the advanced allocation option.

All disks in an aggregate must be the same size.

When choosing a disk size, you should take several factors into consideration. The disk size impacts how much you pay for storage, the size of volumes that you can create in an aggregate, the total capacity available to Cloud Volumes ONTAP, and storage performance.

The performance of Azure Premium Storage is tied to the disk size. Larger disks provide higher IOPS and throughput. For example, choosing 1 TiB disks can provide better performance than 500 GiB disks, at a higher cost.

There are no performance differences between disk sizes for Standard Storage. You should choose disk size based on the capacity that you need.

Refer to Azure for IOPS and throughput by disk size:

• Microsoft Azure: Managed Disks pricing

• Microsoft Azure: Page Blobs pricing

**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 Azure.

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

**Collect networking information**

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

Networking requirements for Cloud Volumes ONTAP in Azure

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

Requirements for Cloud Volumes ONTAP

The following networking requirements must be met in Azure.

Outbound internet access

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:
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.

IP addresses

BlueXP automatically allocates the required number of private IP addresses to Cloud Volumes ONTAP in Azure. You need to make sure 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. An SVM management LIF is required for management tools like SnapCenter.

- An iSCSI LIF provides client access over the iSCSI protocol and is used by the system for other important networking workflows. These LIFs are required and should not be deleted.

**IP addresses for a single node system**

BlueXP allocates 5 or 6 IP addresses to a single node system:

- Cluster management IP
- Node management IP
- Intercluster IP for SnapMirror
- NFS/CIFS IP
- iSCSI IP
- SVM management (optional - not configured by default)

**IP addresses for HA pairs**

BlueXP allocates IP addresses to 4 NICs (per node) during deployment.

Note that BlueXP creates an SVM management LIF on HA pairs, but not on single node systems in Azure.

**NIC0**
The iSCSI IP provides client access over the iSCSI protocol. It is also used by the system for other important networking workflows. This LIF is required and should not be deleted.

NIC1

• Cluster network IP

NIC2

• Cluster Interconnect IP (HA IC)

NIC3

• Pageblob NIC IP (disk access)

NIC3 is only applicable to HA deployments that use page blob storage.

The above IP addresses do not migrate on failover events.

Additionally, 4 frontend IPs (FIPs) are configured to migrate on failover events. These frontend IPs live in the load balancer.

• Cluster management IP
• NodeA data IP (NFS/CIFS)
• NodeB data IP (NFS/CIFS)
• SVM management IP

Secure connections to Azure services

By default, BlueXP enables an Azure Private Link for connections between Cloud Volumes ONTAP and Azure page blob storage accounts.

In most cases, there’s nothing that you need to do—BlueXP manages the Azure Private Link for you. But if you use Azure Private DNS, then you’ll need to edit a configuration file. You should also be aware of a requirement for the Connector location in Azure.

You can also disable the Private Link connection, if required by your business needs. If you disable the link, BlueXP configures Cloud Volumes ONTAP to use a service endpoint instead.

Learn more about using Azure Private Links or service endpoints with Cloud Volumes ONTAP.

Connections to other ONTAP systems

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

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

A Cloud Volumes ONTAP HA pair includes an HA interconnect, which allows each node to continually check whether its partner is functioning and to mirror log data for the other’s nonvolatile memory. The HA interconnect uses TCP port 10006 for communication.

By default, communication between the HA interconnect LIFs is open and there are no security group rules for this port. But if you create a firewall between the HA interconnect LIFs, then you need to ensure that TCP traffic is open for port 10006 so that the HA pair can operate properly.

Only one HA pair in an Azure resource group

You must use a dedicated resource group for each Cloud Volumes ONTAP HA pair that you deploy in Azure. Only one HA pair is supported in a resource group.

BlueXP experiences connection issues if you try to deploy a second Cloud Volumes ONTAP HA pair in an Azure resource group.

Security group rules

BlueXP creates Azure 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 your to use own security groups.

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

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

Inbound rules for single node systems

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

- **Selected VNet only**: the source for inbound traffic is the subnet range of the VNet for the Cloud Volumes ONTAP system and the subnet range of the VNet where the Connector resides. This is the recommended option.

- **All VNets**: the source for inbound traffic is the 0.0.0.0/0 IP range.

<table>
<thead>
<tr>
<th>Priority and name</th>
<th>Port and protocol</th>
<th>Source and destination</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1000 inbound_ssh</td>
<td>22 TCP</td>
<td>Any to Any</td>
<td>SSH access to the IP address of the cluster management LIF or a node management LIF</td>
</tr>
<tr>
<td>1001 inbound_http</td>
<td>80 TCP</td>
<td>Any to Any</td>
<td>HTTP access to the System Manager web console using the IP address of the cluster management LIF</td>
</tr>
<tr>
<td>1002 inbound_111_tcp</td>
<td>111 TCP</td>
<td>Any to Any</td>
<td>Remote procedure call for NFS</td>
</tr>
<tr>
<td>1003 inbound_111_udp</td>
<td>111 UDP</td>
<td>Any to Any</td>
<td>Remote procedure call for NFS</td>
</tr>
<tr>
<td>1004 inbound_139</td>
<td>139 TCP</td>
<td>Any to Any</td>
<td>NetBIOS service session for CIFS</td>
</tr>
<tr>
<td>Priority and name</td>
<td>Port and protocol</td>
<td>Source and destination</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>------------------</td>
<td>-----------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>1005 inbound_161-162 _tcp</td>
<td>161-162 TCP</td>
<td>Any to Any</td>
<td>Simple network management protocol</td>
</tr>
<tr>
<td>1006 inbound_161-162 _udp</td>
<td>161-162 UDP</td>
<td>Any to Any</td>
<td>Simple network management protocol</td>
</tr>
<tr>
<td>1007 inbound_443</td>
<td>443 TCP</td>
<td>Any to Any</td>
<td>Connectivity with the Connector and HTTPS access to the System Manager web console using the IP address of the cluster management LIF</td>
</tr>
<tr>
<td>1008 inbound_445</td>
<td>445 TCP</td>
<td>Any to Any</td>
<td>Microsoft SMB/CIFS over TCP with NetBIOS framing</td>
</tr>
<tr>
<td>1009 inbound_635_tcp</td>
<td>635 TCP</td>
<td>Any to Any</td>
<td>NFS mount</td>
</tr>
<tr>
<td>1010 inbound_635_udp</td>
<td>635 UDP</td>
<td>Any to Any</td>
<td>NFS mount</td>
</tr>
<tr>
<td>1011 inbound_749</td>
<td>749 TCP</td>
<td>Any to Any</td>
<td>Kerberos</td>
</tr>
<tr>
<td>1012 inbound_2049_tcp</td>
<td>2049 TCP</td>
<td>Any to Any</td>
<td>NFS server daemon</td>
</tr>
<tr>
<td>1013 inbound_2049_udp</td>
<td>2049 UDP</td>
<td>Any to Any</td>
<td>NFS server daemon</td>
</tr>
<tr>
<td>1014 inbound_3260</td>
<td>3260 TCP</td>
<td>Any to Any</td>
<td>iSCSI access through the iSCSI data LIF</td>
</tr>
<tr>
<td>1015 inbound_4045-4046_tcp</td>
<td>4045-4046 TCP</td>
<td>Any to Any</td>
<td>NFS lock daemon and network status monitor</td>
</tr>
<tr>
<td>1016 inbound_4045-4046_udp</td>
<td>4045-4046 UDP</td>
<td>Any to Any</td>
<td>NFS lock daemon and network status monitor</td>
</tr>
<tr>
<td>1017 inbound_10000</td>
<td>10000 TCP</td>
<td>Any to Any</td>
<td>Backup using NDMP</td>
</tr>
<tr>
<td>1018 inbound_11104-11105</td>
<td>11104-11105 TCP</td>
<td>Any to Any</td>
<td>SnapMirror data transfer</td>
</tr>
<tr>
<td>3000 inbound_deny _all_tcp</td>
<td>Any port TCP</td>
<td>Any to Any</td>
<td>Block all other TCP inbound traffic</td>
</tr>
<tr>
<td>3001 inbound_deny _all_udp</td>
<td>Any port UDP</td>
<td>Any to Any</td>
<td>Block all other UDP inbound traffic</td>
</tr>
<tr>
<td>Priority and name</td>
<td>Port and protocol</td>
<td>Source and destination</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-------------------</td>
<td>---------------------------</td>
<td>-------------------------------------------------------</td>
</tr>
<tr>
<td>65000</td>
<td>Any port</td>
<td>VirtualNetwork to VirtualNetwork</td>
<td>Inbound traffic from within the VNet</td>
</tr>
<tr>
<td>AllowVnetInBound</td>
<td>Any protocol</td>
<td></td>
<td></td>
</tr>
<tr>
<td>65001</td>
<td>Any port</td>
<td>AzureLoadBalancer to Any</td>
<td>Data traffic from the Azure Standard Load Balancer</td>
</tr>
<tr>
<td>AllowAzureLoadBalancerInBound</td>
<td>Any protocol</td>
<td></td>
<td></td>
</tr>
<tr>
<td>65500</td>
<td>Any port</td>
<td>Any to Any</td>
<td>Block all other inbound traffic</td>
</tr>
<tr>
<td>DenyAllInBound</td>
<td>Any protocol</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Inbound rules for HA systems**

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

- **Selected VNet only**: the source for inbound traffic is the subnet range of the VNet for the Cloud Volumes ONTAP system and the subnet range of the VNet where the Connector resides. This is the recommended option.

- **All VNets**: the source for inbound traffic is the 0.0.0.0/0 IP range.

HA systems have less inbound rules than single node systems because inbound data traffic goes through the Azure Standard Load Balancer. Because of this, traffic from the Load Balancer should be open, as shown in the "AllowAzureLoadBalancerInBound" rule.

<table>
<thead>
<tr>
<th>Priority and name</th>
<th>Port and protocol</th>
<th>Source and destination</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>100 inbound_443</td>
<td>443 Any protocol</td>
<td>Any to Any</td>
<td>Connectivity with the Connector and HTTPS access to the System Manager web console using the IP address of the cluster management LIF</td>
</tr>
<tr>
<td>101 inbound_111_tcp</td>
<td>111 Any protocol</td>
<td>Any to Any</td>
<td>Remote procedure call for NFS</td>
</tr>
<tr>
<td>102 inbound_2049_tcp</td>
<td>2049 Any protocol</td>
<td>Any to Any</td>
<td>NFS server daemon</td>
</tr>
<tr>
<td>111 inbound_ssh</td>
<td>22 Any protocol</td>
<td>Any to Any</td>
<td>SSH access to the IP address of the cluster management LIF or a node management LIF</td>
</tr>
<tr>
<td>121 inbound_53</td>
<td>53 Any protocol</td>
<td>Any to Any</td>
<td>DNS and CIFS</td>
</tr>
<tr>
<td>65000 AllowVnetInBound</td>
<td>Any port Any protocol</td>
<td>VirtualNetwork to VirtualNetwork</td>
<td>Inbound traffic from within the VNet</td>
</tr>
<tr>
<td>Priority and name</td>
<td>Port and protocol</td>
<td>Source and destination</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------------</td>
<td>------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>65001 AllowAzureLoadBalancerInBound</td>
<td>Any port Any protocol</td>
<td>AzureLoadBalancer to Any</td>
<td>Data traffic from the Azure Standard Load Balancer</td>
</tr>
<tr>
<td>65500 DenyAllInBound</td>
<td>Any port Any protocol</td>
<td>Any to Any</td>
<td>Block all other inbound traffic</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>All</td>
<td>All TCP</td>
<td>All outbound traffic</td>
</tr>
<tr>
<td>All</td>
<td>All UDP</td>
<td>All outbound traffic</td>
</tr>
</tbody>
</table>

**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.

ℹ️ The source is the interface (IP address) on the Cloud Volumes ONTAP system.
<table>
<thead>
<tr>
<th>Service</th>
<th>Port</th>
<th>Protocol</th>
<th>Source</th>
<th>Destination</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Directory</td>
<td>88</td>
<td>TCP</td>
<td>Node management LIF</td>
<td>Active Directory forest</td>
<td>Kerberos V authentication</td>
</tr>
<tr>
<td></td>
<td>137</td>
<td>UDP</td>
<td>Node management LIF</td>
<td>Active Directory forest</td>
<td>NetBIOS name service</td>
</tr>
<tr>
<td></td>
<td>138</td>
<td>UDP</td>
<td>Node management LIF</td>
<td>Active Directory forest</td>
<td>NetBIOS datagram service</td>
</tr>
<tr>
<td></td>
<td>139</td>
<td>TCP</td>
<td>Node management LIF</td>
<td>Active Directory forest</td>
<td>NetBIOS service session</td>
</tr>
<tr>
<td></td>
<td>389</td>
<td>TCP &amp; UDP</td>
<td>Node management LIF</td>
<td>Active Directory forest</td>
<td>LDAP</td>
</tr>
<tr>
<td></td>
<td>445</td>
<td>TCP</td>
<td>Node management LIF</td>
<td>Active Directory forest</td>
<td>Microsoft SMB/CIFS over TCP with NetBIOS framing</td>
</tr>
<tr>
<td></td>
<td>464</td>
<td>TCP</td>
<td>Node management LIF</td>
<td>Active Directory forest</td>
<td>Kerberos V change &amp; set password (SET_CHANGE)</td>
</tr>
<tr>
<td></td>
<td>464</td>
<td>UDP</td>
<td>Node management LIF</td>
<td>Active Directory forest</td>
<td>Kerberos key administration</td>
</tr>
<tr>
<td></td>
<td>749</td>
<td>TCP</td>
<td>Node management LIF</td>
<td>Active Directory forest</td>
<td>Kerberos V change &amp; set Password (RPCSEC_GSS)</td>
</tr>
<tr>
<td></td>
<td>88</td>
<td>TCP</td>
<td>Data LIF (NFS, CIFS, iSCSI)</td>
<td>Active Directory forest</td>
<td>Kerberos V authentication</td>
</tr>
<tr>
<td></td>
<td>137</td>
<td>UDP</td>
<td>Data LIF (NFS, CIFS)</td>
<td>Active Directory forest</td>
<td>NetBIOS name service</td>
</tr>
<tr>
<td></td>
<td>138</td>
<td>UDP</td>
<td>Data LIF (NFS, CIFS)</td>
<td>Active Directory forest</td>
<td>NetBIOS datagram service</td>
</tr>
<tr>
<td></td>
<td>139</td>
<td>TCP</td>
<td>Data LIF (NFS, CIFS)</td>
<td>Active Directory forest</td>
<td>NetBIOS service session</td>
</tr>
<tr>
<td></td>
<td>389</td>
<td>TCP &amp; UDP</td>
<td>Data LIF (NFS, CIFS)</td>
<td>Active Directory forest</td>
<td>LDAP</td>
</tr>
<tr>
<td></td>
<td>445</td>
<td>TCP</td>
<td>Data LIF (NFS, CIFS)</td>
<td>Active Directory forest</td>
<td>Microsoft SMB/CIFS over TCP with NetBIOS framing</td>
</tr>
<tr>
<td></td>
<td>464</td>
<td>TCP</td>
<td>Data LIF (NFS, CIFS)</td>
<td>Active Directory forest</td>
<td>Kerberos V change &amp; set password (SET_CHANGE)</td>
</tr>
<tr>
<td></td>
<td>464</td>
<td>UDP</td>
<td>Data LIF (NFS, CIFS)</td>
<td>Active Directory forest</td>
<td>Kerberos key administration</td>
</tr>
<tr>
<td></td>
<td>749</td>
<td>TCP</td>
<td>Data LIF (NFS, CIFS)</td>
<td>Active Directory forest</td>
<td>Kerberos V change &amp; set password (RPCSEC_GSS)</td>
</tr>
<tr>
<td>Service</td>
<td>Port</td>
<td>Protocol</td>
<td>Source</td>
<td>Destination</td>
<td>Purpose</td>
</tr>
<tr>
<td>------------------</td>
<td>------</td>
<td>----------</td>
<td>-----------------------------</td>
<td>----------------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>AutoSupport</td>
<td>HTTPS</td>
<td>443</td>
<td>Node management LIF</td>
<td>support.netapp.com</td>
<td>AutoSupport (HTTPS is the default)</td>
</tr>
<tr>
<td></td>
<td>HTTP</td>
<td>80</td>
<td>Node management LIF</td>
<td>support.netapp.com</td>
<td>AutoSupport (only if the transport protocol is changed from HTTPS to HTTP)</td>
</tr>
<tr>
<td></td>
<td>TCP</td>
<td>3128</td>
<td>Node management LIF</td>
<td>Connector</td>
<td>Sending AutoSupport messages through a proxy server on the Connector, if an outbound internet connection isn’t available</td>
</tr>
<tr>
<td>Configuration backups</td>
<td>HTTP</td>
<td>80</td>
<td>Node management LIF</td>
<td>http://&lt;connector-IP-address&gt;/occm/offboxconfig</td>
<td>Send configuration backups to the Connector. Learn about configuration backup files.</td>
</tr>
<tr>
<td>DHCP</td>
<td>68</td>
<td>UDP</td>
<td>Node management LIF</td>
<td>DHCP</td>
<td>DHCP client for first-time setup</td>
</tr>
<tr>
<td>DHCPS</td>
<td>67</td>
<td>UDP</td>
<td>Node management LIF</td>
<td>DHCP</td>
<td>DHCP server</td>
</tr>
<tr>
<td>DNS</td>
<td>53</td>
<td>UDP</td>
<td>Node management LIF and data LIF (NFS, CIFS)</td>
<td>DNS</td>
<td>DNS</td>
</tr>
<tr>
<td>NDMP</td>
<td>18600–18699</td>
<td>TCP</td>
<td>Node management LIF</td>
<td>Destination servers</td>
<td>NDMP copy</td>
</tr>
<tr>
<td>SMTP</td>
<td>25</td>
<td>TCP</td>
<td>Node management LIF</td>
<td>Mail server</td>
<td>SMTP alerts, can be used for AutoSupport</td>
</tr>
<tr>
<td>SNMP</td>
<td>161</td>
<td>TCP</td>
<td>Node management LIF</td>
<td>Monitor server</td>
<td>Monitoring by SNMP traps</td>
</tr>
<tr>
<td></td>
<td>161</td>
<td>UDP</td>
<td>Node management LIF</td>
<td>Monitor server</td>
<td>Monitoring by SNMP traps</td>
</tr>
<tr>
<td></td>
<td>162</td>
<td>TCP</td>
<td>Node management LIF</td>
<td>Monitor server</td>
<td>Monitoring by SNMP traps</td>
</tr>
<tr>
<td></td>
<td>162</td>
<td>UDP</td>
<td>Node management LIF</td>
<td>Monitor server</td>
<td>Monitoring by SNMP traps</td>
</tr>
<tr>
<td>SnapMirror</td>
<td>11104</td>
<td>TCP</td>
<td>Intercluster LIF</td>
<td>ONTAP intercluster LIFs</td>
<td>Management of intercluster communication sessions for SnapMirror</td>
</tr>
<tr>
<td></td>
<td>11105</td>
<td>TCP</td>
<td>Intercluster LIF</td>
<td>ONTAP intercluster LIFs</td>
<td>SnapMirror data transfer</td>
</tr>
<tr>
<td>Syslog</td>
<td>514</td>
<td>UDP</td>
<td>Node management LIF</td>
<td>Syslog server</td>
<td>Syslog forward messages</td>
</tr>
</tbody>
</table>

**Requirements for the Connector**

If you haven’t created a Connector yet, you should review networking requirements for the Connector as well.
Set up Cloud Volumes ONTAP to use a customer-managed key in Azure

Data is automatically encrypted on Cloud Volumes ONTAP in Azure using Azure Storage Service Encryption with a Microsoft-managed key. But you can use your own encryption key instead by following the steps on this page.

Data encryption overview

Cloud Volumes ONTAP data is automatically encrypted in Azure using Azure Storage Service Encryption. The default implementation uses a Microsoft-managed key. No setup is required.

If you want to use a customer-managed key with Cloud Volumes ONTAP, then you need to complete the following steps:

1. From Azure, create a key vault and then generate a key in that vault
2. From BlueXP, use the API to create a Cloud Volumes ONTAP working environment that uses the key

Key rotation

If you create a new version of your key, Cloud Volumes ONTAP automatically uses the latest key version.

How data is encrypted

After you create a Cloud Volumes ONTAP working environment that is configured to use a customer-managed key, Cloud Volumes ONTAP data is encrypted as follows.

Azure HA multiple availability zone

- All Azure storage accounts for Cloud Volumes ONTAP are encrypted using a customer-managed key.¹
- For root, boot, NVRAM, core and data disks, BlueXP uses a disk encryption set, which enables management of encryption keys with managed disks.
- Any new data disks also use the same disk encryption set.

Azure HA single availability zone

- All Azure storage accounts for Cloud Volumes ONTAP are encrypted using a customer-managed key.¹
- Any new storage accounts (for example, when you add disks or aggregates) also use the same key.¹
- From ONTAP 9.10.1P3, For NVRAM and the core disk, BlueXP uses a disk encryption set, which enables management of encryption keys with managed disks. Lower versions will use Microsoft-managed key, instead of the customer-managed key.

Single node

- All Azure storage accounts for Cloud Volumes ONTAP are encrypted using a customer-managed key.¹
- For root, boot, and data disks, BlueXP uses a disk encryption set, which enables management of encryption keys with managed disks.
- Any new data disks also use the same disk encryption set.
- From ONTAP 9.9.1P7, for NVRAM and the core disk, BlueXP uses a disk encryption set, which enables management of encryption keys with managed disks. Lower versions will use Microsoft-managed key,
instead of the customer-managed key.

Footnote
1. If you want to encrypt your storage accounts during their creation, you must create and provide the ID of the resource in the CVO creation request. This applies for all type of deployments. If you do not provide it, the storage accounts still will be encrypted, but BlueXP will first create the storage accounts with Microsoft-managed key encryption and then will update the storage accounts to use the customer-managed key.

Create a user-assigned managed identity

You have the option to create a resource called a user-assigned managed identity. Doing so allows you to encrypt your storage accounts when you create a Cloud Volumes ONTAP working environment. We recommend creating this resource prior to creating a key vault and generating a key.

The resource has the following ID: userassignedidentity.

Steps
1. In Azure, go to Azure services and select Managed Identities.
2. Click Create.
3. Provide the following details:
   - Subscription: Choose a subscription. We recommend choosing the same subscription as the Connector subscription.
   - Resource group: Use an existing resource group or create a new one.
   - Region: Optionally, select the same region as the Connector.
   - Name: Enter a name for the resource.
4. Optionally, add tags.
5. Click Create.

Create a key vault and generate a key

The key vault must reside in the same Azure subscription and region in which you plan to create the Cloud Volumes ONTAP system.

If you created a user-assigned managed identity, while creating the key vault, you should also create an access policy for the key vault.

Steps
1. Create a key vault in your Azure subscription.

Note the following requirements for the key vault:
   - The key vault must reside in the same region as the Cloud Volumes ONTAP system.
   - The following options should be enabled:
     - Soft-delete (this option is enabled by default, but must not be disabled)
     - Purge protection
     - Azure Disk Encryption for volume encryption (for single node systems or HA pairs in multiple zones)
   - The following option should be enabled if you created a user-assigned managed identity:
- Vault access policy

2. If you selected Vault access policy, click Create to create an access policy for the key vault. If not, skip to step 3.

   a. Select the following permissions:
      - get
      - list
      - decrypt
      - encrypt
      - unwrap key
      - wrap key
      - verify
      - sign

   b. Select the user-assigned managed identity (resource) as the principal.

   c. Review and create the access policy.

3. Generate a key in the key vault.

   Note the following requirements for the key:
   - The key type must be RSA.
   - The recommended RSA key size is 2048, but other sizes are supported.

Create a working environment that uses the encryption key

After you create the key vault and generate an encryption key, you can create a new Cloud Volumes ONTAP system that is configured to use the key. These steps are supported by using the BlueXP API.

Required permissions

If you want to use a customer-managed key with a single node Cloud Volumes ONTAP system, ensure that the BlueXP Connector has the following permissions:

```
"Microsoft.Compute/diskEncryptionSets/read",
"Microsoft.Compute/diskEncryptionSets/write",
"Microsoft.Compute/diskEncryptionSets/delete",
"Microsoft.KeyVault/vaults/deploy/action",
"Microsoft.KeyVault/vaults/read",
"Microsoft.KeyVault/vaults/accessPolicies/write",
"Microsoft.ManagedIdentity/userAssignedIdentities/assign/action"
```

View the latest list of permissions

Steps

1. Obtain the list of key vaults in your Azure subscription by using the following BlueXP API call.

   For an HA pair: GET /azure/ha/metadata/vaults
For single node: GET /azure/vsa/metadata/vaults

Make note of the name and resourceGroup. You'll need to specify those values in the next step.

Learn more about this API call.

2. Obtain the list of keys within the vault by using the following BlueXP API call.

For an HA pair: GET /azure/ha/metadata/keys-vault

For single node: GET /azure/vsa/metadata/keys-vault

Make note of the keyName. You'll need to specify that value (along with the vault name) in the next step.

Learn more about this API call.

3. Create a Cloud Volumes ONTAP system by using the following BlueXP API call.

   a. For an HA pair:

      POST /azure/ha/working-environments

      The request body must include the following fields:

      "azureEncryptionParameters": {
          "key": "keyName",
          "vaultName": "vaultName"
      }

      Include the "userAssignedIdentity": "userAssignedIdentityId" field if you created this resource to be used for storage account encryption.

      Learn more about this API call.

   b. For a single node system:

      POST /azure/vsa/working-environments

      The request body must include the following fields:

      "azureEncryptionParameters": {
          "key": "keyName",
          "vaultName": "vaultName"
      }

      Include the "userAssignedIdentity": "userAssignedIdentityId" field if you created this resource to be used for storage account encryption.

      Learn more about this API call.
Result
You have a new Cloud Volumes ONTAP system that is configured to use your customer-managed key for data encryption.

Set up licensing for Cloud Volumes ONTAP in Azure

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 Azure 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.

**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 Azure Marketplace
- An annual contract

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 Azure 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.

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

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

Annual contract

Pay for Cloud Volumes ONTAP annually by purchasing an annual contract.

Steps

1. Contact your NetApp sales representative to purchase an annual contract.

   The contract is available as a private offer in the Azure Marketplace.

   After NetApp shares the private offer with you, you can select the annual plan when you subscribe from the Azure Marketplace during working environment creation.

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 > Continue.
   
   b. In the Azure portal, select the annual plan that was shared with your Azure account and then click Subscribe.
   
   c. After you return to BlueXP, select a capacity-based package when you reach the charging methods page.

**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.

Enable high availability mode in Azure

Microsoft Azure’s high availability mode should be enabled to reduce unplanned failover times and to enable NFSv4 support for Cloud Volumes ONTAP.

Starting with the Cloud Volumes ONTAP 9.10.1 release, we reduced the unplanned failover time for Cloud Volumes ONTAP HA pairs running in Microsoft Azure and added support for NFSv4. To make these enhancements available to Cloud Volumes ONTAP, you need to enable the high availability feature on your Azure subscription.

BlueXP will prompt you with these details in an Action Required message when the feature needs to be enabled on an Azure subscription.

Note the following:

- There are no problems with the high availability of your Cloud Volumes ONTAP HA pair. This Azure feature works in concert with ONTAP to reduce the client observed application outage time for NFS protocols that result from unplanned failover events.
- Enabling this feature is non-disruptive to Cloud Volumes ONTAP HA pairs.
- Enabling this feature on your Azure subscription won’t cause issues to other VMs.

An Azure user who has "Owner" privileges can enable the feature from the Azure CLI.
Steps

1. Access the Azure Cloud Shell from the Azure Portal

2. Register the high availability mode feature:

   ```bash
   az account set -s AZURE_SUBSCRIPTION_NAME_OR_ID
   az feature register --name EnableHighAvailabilityMode --namespace Microsoft.Network
   az provider register -n Microsoft.Network
   ```

3. Optionally verify that the feature is now registered:

   ```bash
   az feature show --name EnableHighAvailabilityMode --namespace Microsoft.Network
   ```

   The Azure CLI should return a result similar to the following:

   ```json
   {
     "id": "/subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx/providers/Microsoft.Features/providers/Microsoft.Network/features/EnableHighAvailabilityMode",
     "name": "Microsoft.Network/EnableHighAvailabilityMode",
     "properties": {
       "state": "Registered"
     },
     "type": "Microsoft.Features/providers/features"
   }
   ```

Launching Cloud Volumes ONTAP in Azure

You can launch a single node system or an HA pair in Azure by creating a Cloud Volumes ONTAP working environment in BlueXP.

What you’ll need

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 chose a configuration and obtained Azure networking information from your administrator. For details, see 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.

About this task
When BlueXP creates a Cloud Volumes ONTAP system in Azure, it creates several Azure objects, such as a resource group, network interfaces, and storage accounts. You can review a summary of the resources at the end of the wizard.

Potential for Data Loss
The best practice is to use a new, dedicated resource group for each Cloud Volumes ONTAP system.

Deploying Cloud Volumes ONTAP in an existing, shared resource group is not recommended due to the risk of data loss. While BlueXP can remove Cloud Volumes ONTAP resources from a shared resource group in case of deployment failure or deletion, an Azure user might accidentally delete Cloud Volumes ONTAP resources from a shared resource group.

Launching a single-node Cloud Volumes ONTAP system in Azure
If you want to launch a single-node Cloud Volumes ONTAP system in Azure, you need to create an single node working environment in BlueXP.

Steps
1. From the left navigation menu, select Storage > Canvas.
2. On the Canvas page, click Add Working Environment and follow the prompts.
4. If you’re prompted, create a Connector.
5. Details and Credentials: Optionally change the Azure credentials and subscription, specify a cluster name, add tags if needed, and then specify credentials.

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Working Environment Name</td>
<td>BlueXP uses the working environment name to name both the Cloud Volumes ONTAP system and the Azure virtual machine. It also uses the name as the prefix for the predefined security group, if you select that option.</td>
</tr>
<tr>
<td>Resource Group Tags</td>
<td>Tags are metadata for your Azure resources. When you enter tags in this field, BlueXP adds them to the resource group associated with the Cloud Volumes ONTAP system. 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.</td>
</tr>
</tbody>
</table>

For information about tags, refer to Microsoft Azure Documentation: Using tags to organize your Azure resources.
The following video shows how to associate a Marketplace subscription to an Azure subscription:

Subscribe to BlueXP from the Azure Marketplace

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: Select a region, availability zone, VNet, and subnet, and then select the checkbox to confirm network connectivity between the Connector and the target location.

   For single node systems, you can choose the Availability Zone in which you’d like to deploy Cloud Volumes ONTAP. If you don’t select an AZ, BlueXP will select one for you.

8. Connectivity: Choose a new or existing resource group and then choose whether to use the predefined security group or to use your own.

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resource Group</td>
<td>Create a new resource group for Cloud Volumes ONTAP or use an existing resource group. The best practice is to use a new, dedicated resource group for Cloud Volumes ONTAP. While it is possible to deploy Cloud Volumes ONTAP in an existing, shared resource group, it's not recommended due to the risk of data loss. See the warning above for more details. If the Azure account that you’re using has the required permissions, BlueXP removes Cloud Volumes ONTAP resources from a resource group, in case of deployment failure or deletion.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| 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 VNet only**, the source for inbound traffic is the subnet range of the selected VNet and the subnet range of the VNet where the Connector resides. This is the recommended option.  
  - If you choose **All VNets**, the source for inbound traffic is the 0.0.0.0/0 IP range. |
| Use existing          | If you choose an existing security group, then it must meet Cloud Volumes ONTAP requirements. [View the default security group](#). |

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. **Preconfigured Packages**: Select one of the packages to quickly deploy a Cloud Volumes ONTAP system, or click [Create my own configuration](#).

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

11. **Licensing**: Change the Cloud Volumes ONTAP version as needed and select a virtual machine type.

    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 9.10.1 and 9.10.1 P4 is available. The update does not occur from one release to another—for example, from 9.6 to 9.7.

12. **Subscribe from the Azure Marketplace**: Follow the steps if BlueXP could not enable programmatic deployments of Cloud Volumes ONTAP.

13. **Underlying Storage Resources**: Choose settings for the initial aggregate: a disk type, a size for each disk, and whether data tiering to Blob storage should be enabled.

    Note the following:

    - The disk type is for the initial volume. You can choose a different disk type for subsequent volumes.
    - The disk size is 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 more about data tiering.
14. **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.

   This option is only available for certain VM types. To find out which VM types are supported, see Supported configurations by license for HA pairs.

   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.

15. **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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Size</td>
<td>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.</td>
</tr>
<tr>
<td>Access control (for NFS only)</td>
<td>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.</td>
</tr>
<tr>
<td>Permissions and Users / Groups (for CIFS only)</td>
<td>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.</td>
</tr>
<tr>
<td>Snapshot Policy</td>
<td>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.</td>
</tr>
<tr>
<td>Advanced options (for NFS only)</td>
<td>Select an NFS version for the volume: either NFSv3 or NFSv4.</td>
</tr>
</tbody>
</table>
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:

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS Primary and Secondary IP Address</td>
<td>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.</td>
</tr>
<tr>
<td>Active Directory Domain to join</td>
<td>The FQDN of the Active Directory (AD) domain that you want the CIFS server to join.</td>
</tr>
<tr>
<td>Credentials authorized to join the domain</td>
<td>The name and password of a Windows account with sufficient privileges to add computers to the specified Organizational Unit (OU) within the AD domain.</td>
</tr>
<tr>
<td>CIFS server NetBIOS name</td>
<td>A CIFS server name that is unique in the AD domain.</td>
</tr>
</tbody>
</table>
### Field

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Organizational Unit | The organizational unit within the AD domain to associate with the CIFS server. The default is CN=Computers. To configure Azure AD Domain Services as the AD server for Cloud Volumes ONTAP, you should enter **OU=AADDC Computers** or **OU=AADDC Users** in this field. 

**Azure Documentation: Create an Organizational Unit (OU) in an Azure AD Domain Services managed domain** |
| 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. See 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.** |

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

For more information, see **Understanding volume usage profiles** and **Data tiering overview**.

18. **Review & Approve**: Review and confirm your selections.

   a. Review details about the configuration.
   
   b. Click **More information** to review details about support and the Azure resources that BlueXP will purchase.
   
   c. Select the **I understand…** check boxes.
   
   d. Click **Go**.

**Result**

BlueXP deploys the Cloud Volumes ONTAP system. You can track the progress in the timeline.

If you experience any issues deploying the Cloud Volumes ONTAP system, 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 System Manager or the 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 Azure

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

**Steps**

1. From the left navigation menu, select **Storage > Canvas**.
2. On the Canvas page, click **Add Working Environment** and follow the prompts.
3. If you're prompted, create a Connector.
4. **Details and Credentials**: Optionally change the Azure credentials and subscription, specify a cluster name, add tags if needed, and then specify credentials.

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Working Environment Name</td>
<td>BlueXP uses the working environment name to name both the Cloud VolumesONTAP system and the Azure virtual machine. It also uses the name as the prefix for the predefined security group, if you select that option.</td>
</tr>
<tr>
<td>Resource Group Tags</td>
<td>Tags are metadata for your Azure resources. When you enter tags in this field, BlueXP adds them to the resource group associated with the Cloud VolumesONTAP system.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>For information about tags, refer to Microsoft Azure Documentation: Using tags to organize your Azure resources.</td>
</tr>
<tr>
<td>User name and password</td>
<td>These are the credentials for the Cloud Volumes ONTAP cluster administrator account. You can use these credentials to connect to Cloud Volumes ONTAP through System Manager or its CLI. Keep the default admin user name or change it to a custom user name.</td>
</tr>
<tr>
<td>Edit Credentials</td>
<td>You can choose different Azure credentials and a different Azure subscription to use with this Cloud Volumes ONTAP system. You need to associate an Azure Marketplace subscription with the selected Azure subscription in order to deploy a pay-as-you-go Cloud Volumes ONTAP system. Learn how to add credentials.</td>
</tr>
</tbody>
</table>

The following video shows how to associate a Marketplace subscription to an Azure subscription:

**Subscribe to BlueXP from the Azure Marketplace**

5. **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.

6. **HA Deployment Models**:
a. Select **Single Availability Zone** or **Multiple Availability Zone**.

b. **Location and Connectivity** (single AZ) and **Region and Connectivity** (multiple AZs)
   - For single AZ, select a region, VNet, and subnet.
   - For multiple AZs, select a region, VNet, subnet, zone for node 1, and zone for node 2.

c. Select the **I have verified network connectivity…** check box.

7. **Connectivity**: Choose a new or existing resource group and then choose whether to use the predefined security group or to use your own.

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resource Group</td>
<td>Create a new resource group for Cloud Volumes ONTAP or use an existing resource group. The best practice is to use a new, dedicated resource group for Cloud Volumes ONTAP. While it is possible to deploy Cloud Volumes ONTAP in an existing, shared resource group, it’s not recommended due to the risk of data loss. See the warning above for more details. You must use a dedicated resource group for each Cloud Volumes ONTAP HA pair that you deploy in Azure. Only one HA pair is supported in a resource group. BlueXP experiences connection issues if you try to deploy a second Cloud Volumes ONTAP HA pair in an Azure resource group.</td>
</tr>
</tbody>
</table>
| 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 VNet only**, the source for inbound traffic is the subnet range of the selected VNet and the subnet range of the VNet where the Connector resides. This is the recommended option.  
  - If you choose **All VNets**, the source for inbound traffic is the 0.0.0.0/0 IP range. |
| Use existing           | If you choose an existing security group, then it must meet Cloud Volumes ONTAP requirements. [View the default security group](https://example.com). |

8. **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.

9. **Preconfigured Packages**: Select one of the packages to quickly deploy a Cloud Volumes ONTAP system, or click **Change configuration**.

If you choose one of the packages, you only need to specify a volume and then review and approve the configuration.
10. **Licensing**: Change the Cloud Volumes ONTAP version as needed and select a virtual machine type.

    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 9.10.1 and 9.10.1 P4 is available. The update does not occur from one release to another—for example, from 9.6 to 9.7.

11. **Subscribe from the Azure Marketplace**: Follow the steps if BlueXP could not enable programmatic deployments of Cloud Volumes ONTAP.

12. **Underlying Storage Resources**: Choose settings for the initial aggregate: a disk type, a size for each disk, and whether data tiering to Blob storage should be enabled.

    Note the following:
    
    ◦ The disk size is 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.

    For help choosing a disk size, see [Size your system in Azure](#).

    ◦ 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 more about data tiering](#).

13. **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.

    This option is only available for certain VM types. To find out which VM types are supported, see [Supported configurations by license for HA pairs](#).

    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.

14. **Secure Communication to Storage & WORM**: Choose whether to enable an HTTPS connection to Azure storage accounts, and activate write once, read many (WORM) storage, if desired.

    The HTTPS connection is from a Cloud Volumes ONTAP 9.7 HA pair to Azure page blob storage accounts. Note that enabling this option can impact write performance. You can’t change the setting after you create the working environment.

    [Learn more about WORM storage](#).

    WORM can’t be enabled if data tiering was enabled.
Learn more about WORM storage.

15. **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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Size</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Access control (for NFS only)</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Permissions and Users / Groups (for CIFS only)</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Snapshot Policy</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Advanced options (for NFS only)</strong></td>
<td>Select an NFS version for the volume: either NFSv3 or NFSv4.</td>
</tr>
<tr>
<td><strong>Initiator group and IQN (for iSCSI only)</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>

The following image shows the Volume page filled out for the CIFS protocol:
16. **CIFS Setup**: If you chose the CIFS protocol, set up a CIFS server.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS Primary and Secondary IP Address</td>
<td>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.</td>
</tr>
<tr>
<td>Active Directory Domain to join</td>
<td>The FQDN of the Active Directory (AD) domain that you want the CIFS server to join.</td>
</tr>
<tr>
<td>Credentials authorized to join the domain</td>
<td>The name and password of a Windows account with sufficient privileges to add computers to the specified Organizational Unit (OU) within the AD domain.</td>
</tr>
<tr>
<td>CIFS server NetBIOS name</td>
<td>A CIFS server name that is unique in the AD domain.</td>
</tr>
<tr>
<td>Organizational Unit</td>
<td>The organizational unit within the AD domain to associate with the CIFS server. The default is CN=Computers.</td>
</tr>
<tr>
<td>To configure Azure AD Domain Services as the AD server for Cloud Volumes ONTAP, you should enter OU=AADDC Computers or OU=AADDC Users in this field.</td>
<td>Azure Documentation: Create an Organizational Unit (OU) in an Azure AD Domain Services managed domain</td>
</tr>
<tr>
<td>DNS Domain</td>
<td>The DNS domain for the Cloud Volumes ONTAP storage virtual machine (SVM). In most cases, the domain is the same as the AD domain.</td>
</tr>
<tr>
<td>NTP Server</td>
<td>Select <strong>Use Active Directory Domain</strong> 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. See the BlueXP automation docs for details.</td>
</tr>
<tr>
<td>Note that you can configure an NTP server only when creating a CIFS server. It’s not configurable after you create the CIFS server.</td>
<td></td>
</tr>
</tbody>
</table>

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

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

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

**Result**

BlueXP deploys the Cloud Volumes ONTAP system. You can track the progress in the timeline.

If you experience any issues deploying the Cloud Volumes ONTAP system, 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 System Manager or the CLI.

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

**Get started in Google Cloud**

**Quick start for Cloud Volumes ONTAP in Google Cloud**

Get started with Cloud Volumes ONTAP for Google Cloud 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 Google Cloud

   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 about planning your configuration.
3  **Set up your networking**

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

b. If you plan to enable data tiering, configure the Cloud Volumes ONTAP subnet for Private Google Access.

c. If you’re deploying an HA pair, ensure that you have four VPCs, each with their own subnet.

d. If you’re using a shared VPC, provide the *Compute Network User* role to the Connector service account.

e. 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.

Learn more about networking requirements.

4  **Set up a service account**

Cloud Volumes ONTAP requires a Google Cloud service account for two purposes. The first is when you enable *data tiering* to tier cold data to low-cost object storage in Google Cloud. The second is when you enable the *BlueXP backup and recovery* to back up volumes to low-cost object storage.

You can set up one service account and use it for both purposes. The service account must have the *Storage Admin* role.

Read step-by-step instructions.

5  **Enable Google Cloud APIs**

Enable the following Google Cloud APIs in your project. These APIs are required to deploy the Connector and Cloud Volumes ONTAP.

- Cloud Deployment Manager V2 API
- Cloud Logging API
- Cloud Resource Manager API
- Compute Engine API
- Identity and Access Management (IAM) API

6  **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

- Creating a Connector from BlueXP
- Installing the Connector software on a Linux host
- What BlueXP does with Google Cloud permissions
Plan your Cloud Volumes ONTAP configuration in Google Cloud

When you deploy Cloud Volumes ONTAP in Google Cloud, 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 Google Cloud regions. View the full list of supported regions.

Choose a supported machine type

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

Supported configurations for Cloud Volumes ONTAP in GCP

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 GCP

Size your system in GCP

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 a machine type, disk type, and disk size:

Machine type

Look at the supported machine types in the Cloud Volumes ONTAP Release Notes and then review details from Google about each supported machine type. Match your workload requirements to the number of vCPUs and memory for the machine type. Note that each CPU core increases networking performance.

Refer to the following for more details:

- Google Cloud documentation: N1 standard machine types
- Google Cloud documentation: Performance

GCP disk type

When you create volumes for Cloud Volumes ONTAP, you need to choose the underlying cloud storage that Cloud Volumes ONTAP uses for a disk. The disk type can be any of the following:

- Zonal SSD persistent disks: SSD persistent disks are best for workloads that require high rates of random IOPS.
• **Zonal Balanced persistent disks**: These SSDs balance performance and cost by providing lower IOPS per GB.

• **Zonal Standard persistent disks**: Standard persistent disks are economical and can handle sequential read/write operations.

For more details, see [Google Cloud documentation: Zonal Persistent disks (Standard and SSD)](https://cloud.google.com/compute/docs/disks/standard-persistent-disk).

### GCP disk size

You need to choose an initial disk size when you deploy a Cloud Volumes ONTAP system. After that you can let BlueXP manage a system’s capacity for you, but if you want to build aggregates yourself, be aware of the following:

• All disks in an aggregate must be the same size.

• Determine the space that you need, while taking performance into consideration.

• The performance of persistent disks scales automatically with disk size and the number of vCPUs available to the system.

Refer to the following for more details:

- [Google Cloud documentation: Zonal Persistent disks (Standard and SSD)](https://cloud.google.com/compute/docs/disks/standard-persistent-disk)
- [Google Cloud documentation: Optimizing Persistent Disk and Local SSD Performance](https://cloud.google.com/compute/docs/disks/optimizing-persistent-disk-performance)

### 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 Google Cloud.

• [Google Cloud docs: Resource quotas](https://cloud.google.com/compute/docs/quotas)

Google Cloud Compute Engine enforces quotas on resource usage so you should ensure that you haven’t reached your limit before you deploy Cloud Volumes ONTAP.

The Connector also requires a system disk. [View details about the Connector’s default configuration](https://cloud.google.com/compute/docs/quotas).

### Collect networking information

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

**Network information for a single-node system**

<table>
<thead>
<tr>
<th>GCP information</th>
<th>Your value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Region</td>
<td></td>
</tr>
<tr>
<td>Zone</td>
<td></td>
</tr>
<tr>
<td>VPC network</td>
<td></td>
</tr>
</tbody>
</table>
Choose a write speed

BlueXP enables you to choose a write speed setting for Cloud Volumes ONTAP, except for high availability (HA) pairs in Google Cloud. 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.

### Networking requirements for Cloud Volumes ONTAP in Google Cloud

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

If you want to deploy an HA pair, you should learn how HA pairs work in Google Cloud.

### Requirements for Cloud Volumes ONTAP

The following requirements must be met in Google Cloud.

**Requirements specific to single node systems**

If you want to deploy a single node system, ensure that your networking meets the following requirements.

**One VPC**

One Virtual Private Cloud (VPC) is required for a single node system.

**Private IP addresses**

BlueXP allocates 3 or 4 private IP addresses to a single node system in Google Cloud.

You can skip creation of the storage VM (SVM) management LIF if you deploy Cloud Volumes ONTAP using the API and specify the following flag:

```
skipSvmManagementLif: true
```

A LIF is an IP address associated with a physical port. A storage VM (SVM) management LIF is required for management tools like SnapCenter.

**Requirements specific to HA pairs**

If you want to deploy an HA pair, ensure that your networking meets the following requirements.
One or multiple zones

You can ensure the high availability of your data by deploying an HA configuration across multiple or in a single zone. BlueXP will prompt you to choose multiple zones or a single zone when you create the HA pair.

- **Multiple zones (recommended)**

  Deploying an HA configuration across three zones ensures continuous data availability if a failure occurs within a zone. Note that write performance is slightly lower compared to using a single zone, but it’s minimal.

- **Single zone**

  When deployed in a single zone, a Cloud Volumes ONTAP HA configuration uses a spread placement policy. This policy ensures that an HA configuration is protected from a single point of failure within the zone, without having to use separate zones to achieve fault isolation.

  This deployment model does lower your costs because there are no data egress charges between zones.

Four Virtual Private Clouds

Four Virtual Private Clouds (VPCs) are required for an HA configuration. Four VPCs are required because Google Cloud requires that each network interface resides in a separate VPC network.

BlueXP will prompt you to choose four VPCs when you create the HA pair:

- VPC-0 for inbound connections to the data and nodes
- VPC-1, VPC-2, and VPC-3 for internal communication between the nodes and the HA mediator
Subnets

A private subnet is required for each VPC.

If you place the Connector in VPC-0, then you will need to enable Private Google Access on the subnet to access the APIs and to enable data tiering.

The subnets in these VPCs must have distinct CIDR ranges. They can’t have overlapping CIDR ranges.

Private IP addresses

BlueXP automatically allocates the required number of private IP addresses to Cloud Volumes ONTAP in Google Cloud. You need to make sure that your networking has enough private 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. An SVM management LIF is required for management tools like SnapCenter.

- Single node
  BlueXP allocates 4 IP addresses to a single node system:
- Node management LIF
- Cluster management LIF
- iSCSI data LIF

An iSCSI LIF provides client access over the iSCSI protocol and is used by the system for other important networking workflows. These LIFs are required and should not be deleted.

- NAS LIF

You can skip creation of the storage VM (SVM) management LIF if you deploy Cloud Volumes ONTAP using the API and specify the following flag:

```latex
skipSvmManagementLif: true
```

- **HA pair**

BlueXP allocates 12-13 IP addresses to an HA pair:

- 2 Node management LIFs (e0a)
- 1 Cluster management LIF (e0a)
- 2 iSCSI LIFs (e0a)

An iSCSI LIF provides client access over the iSCSI protocol and is used by the system for other important networking workflows. These LIFs are required and should not be deleted.

- 1 or 2 NAS LIFs (e0a)
- 2 Cluster LIFs (e0b)
- 2 HA Interconnect IP addresses (e0c)
- 2 RSM iSCSI IP addresses (e0d)

You can skip creation of the storage VM (SVM) management LIF if you deploy Cloud Volumes ONTAP using the API and specify the following flag:

```latex
skipSvmManagementLif: true
```

**Internal load balancers**

BlueXP automatically creates four Google Cloud internal load balancers (TCP/UDP) that manage incoming traffic to the Cloud Volumes ONTAP HA pair. No setup is required from your end. We’ve listed this as a requirement simply to inform you of the network traffic and to mitigate any security concerns.

One load balancer is for cluster management, one is for storage VM (SVM) management, one is for NAS traffic to node 1, and the last is for NAS traffic to node 2.

The setup for each load balancer is as follows:

- One shared private IP address
- One global health check
By default, the ports used by the health check are 63001, 63002, and 63003.

- One regional TCP backend service
- One regional UDP backend service
- One TCP forwarding rule
- One UDP forwarding rule
- Global access is disabled

Even though global access is disabled by default, enabling it post deployment is supported. We disabled it because cross region traffic will have significantly higher latencies. We wanted to ensure that you didn’t have a negative experience due to accidental cross region mounts. Enabling this option is specific to your business needs.

**Shared VPCs**

Cloud Volumes ONTAP and the Connector are supported in a Google Cloud shared VPC and also in standalone VPCs.

For a single node system, the VPC can be either a shared VPC or a standalone VPC.

For an HA pair, four VPCs are required. Each of those VPCs can be either shared or standalone. For example, VPC-0 could be a shared VPC, while VPC-1, VPC-2, and VPC-3 could be standalone VPCs.

A shared VPC enables you to configure and centrally manage virtual networks across multiple projects. You can set up shared VPC networks in the *host project* and deploy the Connector and Cloud Volumes ONTAP virtual machine instances in a *service project*. [Google Cloud documentation: Shared VPC overview](#).

**Packet mirroring in VPCs**

Packet mirroring must be disabled in the Google Cloud VPC in which you deploy Cloud Volumes ONTAP. Cloud Volumes ONTAP can’t operate properly if packet mirroring is enabled.

**Outbound internet access**

Cloud Volumes ONTAP requires 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 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 firewall 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 firewall 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 you’re using an HA pair, the HA mediator doesn’t require outbound internet access.

If BlueXP notifies you that AutoSupport messages can’t be sent, troubleshoot your AutoSupport configuration.

Firewall rules
You don’t need to create firewall rules because BlueXP does that for you. If you need to use your own, refer to the firewall rules listed below.

Note that two sets of firewall rules are required for an HA configuration:

• One set of rules for HA components in VPC-0. These rules enable data access to Cloud Volumes ONTAP. Learn more.

• Another set of rules for HA components in VPC-1, VPC-2, and VPC-3. These rules are open for inbound & outbound communication between the HA components. Learn more.

If you want to tier cold data to a Google Cloud Storage bucket, the subnet in which Cloud Volumes ONTAP resides must be configured for Private Google Access (if you’re using an HA pair, this is the subnet in VPC-0). For instructions, refer to Google Cloud documentation: Configuring Private Google Access.

For additional steps required to set up data tiering in BlueXP, see Tiering cold data to low-cost object storage.

Connections to ONTAP systems in other networks
To replicate data between a Cloud Volumes ONTAP system in Google Cloud and ONTAP systems in other networks, you must have a VPN connection between the VPC and the other network—for example, your corporate network.

For instructions, refer to Google Cloud documentation: Cloud VPN overview.

Firewall rules
BlueXP creates Google Cloud firewall rules 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 your to use own firewall rules.

The firewall rules for Cloud Volumes ONTAP requires both inbound and outbound rules. If you’re deploying an HA configuration, these are the firewall rules for Cloud Volumes ONTAP in VPC-0.

Note that two sets of firewall rules are required for an HA configuration:

• One set of rules for HA components in VPC-0. These rules enable data access to Cloud Volumes ONTAP.

• Another set of rules for HA components in VPC-1, VPC-2, and VPC-3. These rules are open for inbound & outbound communication between the HA components. Learn more.

Looking for information about the Connector? View firewall rules for the Connector

Inbound rules
When you create a working environment, you can choose the source filter for the predefined firewall policy during deployment:
• **Selected VPC only**: the source filter 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 filter for inbound traffic is the 0.0.0.0/0 IP range.

If you use your own firewall policy, ensure that you add all networks that need to communicate with Cloud Volumes ONTAP, but also ensure to add both address ranges to allow the internal Google Load Balancer to function correctly. These addresses are 130.211.0.0/22 and 35.191.0.0/16. For more information, refer to Google Cloud documentation: Load Balancer Firewall Rules.

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Port</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>All ICMP</td>
<td>All</td>
<td>Pinging the instance</td>
</tr>
<tr>
<td>HTTP</td>
<td>80</td>
<td>HTTP access to the System Manager web console using the IP address of the cluster management LIF</td>
</tr>
<tr>
<td>HTTPS</td>
<td>443</td>
<td>Connectivity with the Connector and HTTPS access to the System Manager web console using the IP address of the cluster management LIF</td>
</tr>
<tr>
<td>SSH</td>
<td>22</td>
<td>SSH access to the IP address of the cluster management LIF or a node management LIF</td>
</tr>
<tr>
<td>TCP</td>
<td>111</td>
<td>Remote procedure call for NFS</td>
</tr>
<tr>
<td>TCP</td>
<td>139</td>
<td>NetBIOS service session for CIFS</td>
</tr>
<tr>
<td>TCP</td>
<td>161-162</td>
<td>Simple network management protocol</td>
</tr>
<tr>
<td>TCP</td>
<td>445</td>
<td>Microsoft SMB/CIFS over TCP with NetBIOS framing</td>
</tr>
<tr>
<td>TCP</td>
<td>635</td>
<td>NFS mount</td>
</tr>
<tr>
<td>TCP</td>
<td>749</td>
<td>Kerberos</td>
</tr>
<tr>
<td>TCP</td>
<td>2049</td>
<td>NFS server daemon</td>
</tr>
<tr>
<td>TCP</td>
<td>3260</td>
<td>iSCSI access through the iSCSI data LIF</td>
</tr>
<tr>
<td>TCP</td>
<td>4045</td>
<td>NFS lock daemon</td>
</tr>
<tr>
<td>TCP</td>
<td>4046</td>
<td>Network status monitor for NFS</td>
</tr>
<tr>
<td>TCP</td>
<td>10000</td>
<td>Backup using NDMP</td>
</tr>
<tr>
<td>TCP</td>
<td>11104</td>
<td>Management of intercluster communication sessions for SnapMirror</td>
</tr>
<tr>
<td>TCP</td>
<td>11105</td>
<td>SnapMirror data transfer using intercluster LIFs</td>
</tr>
<tr>
<td>TCP</td>
<td>63001-63050</td>
<td>Load balance probe ports to determine which node is healthy (required for HA pairs only)</td>
</tr>
<tr>
<td>UDP</td>
<td>111</td>
<td>Remote procedure call for NFS</td>
</tr>
<tr>
<td>UDP</td>
<td>161-162</td>
<td>Simple network management protocol</td>
</tr>
<tr>
<td>UDP</td>
<td>635</td>
<td>NFS mount</td>
</tr>
<tr>
<td>UDP</td>
<td>2049</td>
<td>NFS server daemon</td>
</tr>
<tr>
<td>UDP</td>
<td>4045</td>
<td>NFS lock daemon</td>
</tr>
<tr>
<td>UDP</td>
<td>4046</td>
<td>Network status monitor for NFS</td>
</tr>
<tr>
<td>Protocol</td>
<td>Port</td>
<td>Purpose</td>
</tr>
<tr>
<td>----------</td>
<td>------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>UDP</td>
<td>4049</td>
<td>NFS rquotad protocol</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Port</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>All ICMP</td>
<td>All</td>
<td>All outbound traffic</td>
</tr>
<tr>
<td>All TCP</td>
<td>All</td>
<td>All outbound traffic</td>
</tr>
<tr>
<td>All UDP</td>
<td>All</td>
<td>All outbound traffic</td>
</tr>
</tbody>
</table>

**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.

ℹ️ The source is the interface (IP address) on the Cloud Volumes ONTAP system.
<table>
<thead>
<tr>
<th>Service</th>
<th>Protocol</th>
<th>Port</th>
<th>Source</th>
<th>Destination</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Directory</td>
<td>TCP</td>
<td>88</td>
<td>Node management LIF</td>
<td>Active Directory forest</td>
<td>Kerberos V authentication</td>
</tr>
<tr>
<td>UDP</td>
<td>137</td>
<td>Node management LIF</td>
<td>Active Directory forest</td>
<td>NetBIOS name service</td>
<td></td>
</tr>
<tr>
<td>UDP</td>
<td>138</td>
<td>Node management LIF</td>
<td>Active Directory forest</td>
<td>NetBIOS datagram service</td>
<td></td>
</tr>
<tr>
<td>TCP</td>
<td>139</td>
<td>Node management LIF</td>
<td>Active Directory forest</td>
<td>NetBIOS service session</td>
<td></td>
</tr>
<tr>
<td>TCP &amp; UDP</td>
<td>389</td>
<td>Node management LIF</td>
<td>Active Directory forest</td>
<td>LDAP</td>
<td></td>
</tr>
<tr>
<td>TCP</td>
<td>445</td>
<td>Node management LIF</td>
<td>Active Directory forest</td>
<td>Microsoft SMB/CIFS over TCP with NetBIOS framing</td>
<td></td>
</tr>
<tr>
<td>TCP</td>
<td>464</td>
<td>Node management LIF</td>
<td>Active Directory forest</td>
<td>Kerberos V change &amp; set password (SET_CHANGE)</td>
<td></td>
</tr>
<tr>
<td>UDP</td>
<td>464</td>
<td>Node management LIF</td>
<td>Active Directory forest</td>
<td>Kerberos key administration</td>
<td></td>
</tr>
<tr>
<td>TCP</td>
<td>749</td>
<td>Node management LIF</td>
<td>Active Directory forest</td>
<td>Kerberos V change &amp; set Password (RPCSEC_GSS)</td>
<td></td>
</tr>
<tr>
<td>TCP</td>
<td>88</td>
<td>Data LIF (NFS, CIFS, iSCSI)</td>
<td>Active Directory forest</td>
<td>Kerberos V authentication</td>
<td></td>
</tr>
<tr>
<td>UDP</td>
<td>137</td>
<td>Data LIF (NFS, CIFS)</td>
<td>Active Directory forest</td>
<td>NetBIOS name service</td>
<td></td>
</tr>
<tr>
<td>UDP</td>
<td>138</td>
<td>Data LIF (NFS, CIFS)</td>
<td>Active Directory forest</td>
<td>NetBIOS datagram service</td>
<td></td>
</tr>
<tr>
<td>TCP</td>
<td>139</td>
<td>Data LIF (NFS, CIFS)</td>
<td>Active Directory forest</td>
<td>NetBIOS service session</td>
<td></td>
</tr>
<tr>
<td>TCP &amp; UDP</td>
<td>389</td>
<td>Data LIF (NFS, CIFS)</td>
<td>Active Directory forest</td>
<td>LDAP</td>
<td></td>
</tr>
<tr>
<td>TCP</td>
<td>445</td>
<td>Data LIF (NFS, CIFS)</td>
<td>Active Directory forest</td>
<td>Microsoft SMB/CIFS over TCP with NetBIOS framing</td>
<td></td>
</tr>
<tr>
<td>TCP</td>
<td>464</td>
<td>Data LIF (NFS, CIFS)</td>
<td>Active Directory forest</td>
<td>Kerberos V change &amp; set password (SET_CHANGE)</td>
<td></td>
</tr>
<tr>
<td>UDP</td>
<td>464</td>
<td>Data LIF (NFS, CIFS)</td>
<td>Active Directory forest</td>
<td>Kerberos key administration</td>
<td></td>
</tr>
<tr>
<td>TCP</td>
<td>749</td>
<td>Data LIF (NFS, CIFS)</td>
<td>Active Directory forest</td>
<td>Kerberos V change &amp; set password (RPCSEC_GSS)</td>
<td></td>
</tr>
<tr>
<td>Service</td>
<td>Protocol</td>
<td>Port</td>
<td>Source</td>
<td>Destination</td>
<td>Purpose</td>
</tr>
<tr>
<td>--------------------</td>
<td>----------</td>
<td>--------</td>
<td>-----------------------------</td>
<td>------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>AutoSupport</td>
<td>HTTPS</td>
<td>443</td>
<td>Node management LIF</td>
<td>support.netapp.com</td>
<td>AutoSupport (HTTPS is the default)</td>
</tr>
<tr>
<td></td>
<td>HTTP</td>
<td>80</td>
<td>Node management LIF</td>
<td>support.netapp.com</td>
<td>AutoSupport (only if the transport protocol is changed from HTTPS to HTTP)</td>
</tr>
<tr>
<td></td>
<td>TCP</td>
<td>3128</td>
<td>Node management LIF</td>
<td>Connector</td>
<td>Sending AutoSupport messages through a proxy server on the Connector, if an outbound internet connection isn't available</td>
</tr>
<tr>
<td>Cluster</td>
<td>All traffic</td>
<td>All traffic</td>
<td>All LIFs on one node</td>
<td>All LIFs on the other node</td>
<td>Intercluster communications (Cloud Volumes ONTAP HA only)</td>
</tr>
<tr>
<td>Configuration backups</td>
<td>HTTP</td>
<td>80</td>
<td>Node management LIF</td>
<td>http://&lt;connector-IP-address&gt;/occm/offboxconfig</td>
<td>Send configuration backups to the Connector. Learn about configuration backup files.</td>
</tr>
<tr>
<td>DHCP</td>
<td>UDP</td>
<td>68</td>
<td>Node management LIF</td>
<td>DHCP</td>
<td>DHCP client for first-time setup</td>
</tr>
<tr>
<td>DHCPS</td>
<td>UDP</td>
<td>67</td>
<td>Node management LIF</td>
<td>DHCP</td>
<td>DHCP server</td>
</tr>
<tr>
<td>DNS</td>
<td>UDP</td>
<td>53</td>
<td>Node management LIF</td>
<td>DNS</td>
<td>DNS</td>
</tr>
<tr>
<td>NDMP</td>
<td>TCP</td>
<td>1860–699</td>
<td>Node management LIF</td>
<td>Destination servers</td>
<td>NDMP copy</td>
</tr>
<tr>
<td>SMTP</td>
<td>TCP</td>
<td>25</td>
<td>Node management LIF</td>
<td>Mail server</td>
<td>SMTP alerts, can be used for AutoSupport</td>
</tr>
<tr>
<td>SNMP</td>
<td>TCP</td>
<td>161</td>
<td>Node management LIF</td>
<td>Monitor server</td>
<td>Monitoring by SNMP traps</td>
</tr>
<tr>
<td></td>
<td>UDP</td>
<td>161</td>
<td>Node management LIF</td>
<td>Monitor server</td>
<td>Monitoring by SNMP traps</td>
</tr>
<tr>
<td></td>
<td>TCP</td>
<td>162</td>
<td>Node management LIF</td>
<td>Monitor server</td>
<td>Monitoring by SNMP traps</td>
</tr>
<tr>
<td></td>
<td>UDP</td>
<td>162</td>
<td>Node management LIF</td>
<td>Monitor server</td>
<td>Monitoring by SNMP traps</td>
</tr>
<tr>
<td>SnapMirror</td>
<td>TCP</td>
<td>1110</td>
<td>Intercluster LIF</td>
<td>ONTAP intercluster LIFs</td>
<td>Management of intercluster communication sessions for SnapMirror</td>
</tr>
<tr>
<td></td>
<td>TCP</td>
<td>1110</td>
<td>Intercluster LIF</td>
<td>ONTAP intercluster LIFs</td>
<td>SnapMirror data transfer</td>
</tr>
<tr>
<td>Syslog</td>
<td>UDP</td>
<td>514</td>
<td>Node management LIF</td>
<td>Syslog server</td>
<td>Syslog forward messages</td>
</tr>
</tbody>
</table>
Rules for VPC-1, VPC-2, and VPC-3

In Google Cloud, an HA configuration is deployed across four VPCs. The firewall rules needed for the HA configuration in VPC-0 are listed above for Cloud Volumes ONTAP.

Meanwhile, the predefined firewall rules that BlueXP creates for instances in VPC-1, VPC-2, and VPC-3 enables ingress communication over all protocols and ports. These rules enable communication between HA nodes.

Communication from the HA nodes to the HA mediator takes place over port 3260 (iSCSI).

To enable high write speed for new Google Cloud HA pair deployments, a maximum transmission unit (MTU) of at least 8,896 bytes is required for VPC-1, VPC-2, and VPC-3. If you choose to upgrade existing VPC-1, VPC-2, and VPC-3 to an MTU of 8,896 bytes, you must shutdown all existing HA systems using these VPCs during the configuration process.

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
- Firewall rules in Google Cloud

Planning for VPC Service Controls in GCP

When choosing to lock down your Google Cloud environment with VPC Service Controls, you should understand how BlueXP and Cloud Volumes ONTAP interact with the Google Cloud APIs, as well as how to configure your service perimeter to deploy BlueXP and Cloud Volumes ONTAP.

VPC Service Controls enable you to control access to Google-managed services outside of a trusted perimeter, to block data access from untrusted locations, and to mitigate unauthorized data transfer risks. Learn more about Google Cloud VPC Service Controls.

How NetApp services communicate with VPC Service Controls

BlueXP communicates directly with the Google Cloud APIs. This is either triggered from an external IP address outside of Google Cloud (for example, from api.services.cloud.netapp.com), or within Google Cloud from an internal address assigned to the BlueXP Connector.

Depending on the deployment style of the Connector, certain exceptions may have to be made for your service perimeter.

Images

Both Cloud Volumes ONTAP and BlueXP use images from a project within GCP that is managed by NetApp. This can affect the deployment of the BlueXP Connector and Cloud Volumes ONTAP, if your organization has a policy that blocks the use of images that are not hosted within the organization.

You can deploy a Connector manually using the manual installation method, but Cloud Volumes ONTAP will also need to pull images from the NetApp project. You must provide an allowed list in order to deploy a Connector and Cloud Volumes ONTAP.
Deploying a Connector

The user who deploys a Connector needs to be able to reference an image hosted in the projectId netapp-cloudmanager and the project number 14190056516.

Deploying Cloud Volumes ONTAP

• The BlueXP service account needs to reference an image hosted in the projectId netapp-cloudmanager and the project number 14190056516 from the service project.

• The service account for the default Google APIs Service Agent needs to reference an image hosted in the projectId netapp-cloudmanager and the project number 14190056516 from the service project.

Examples of the rules needed for pulling these images with VPC Service Controls are defined below.

VPC Service Controls perimeter policies

Policies allow exceptions to the VPC Service Controls rule sets. For more information about policies, please visit the GCP VPC Service Controls Policy Documentation.

To set the policies that BlueXP requires, navigate to your VPC Service Controls Perimeter within your organization and add the following policies. The fields should match the options given in the VPC Service Controls policy page. Also note that all rules are required and the OR parameters should be used in the rule set.

Ingress rules

Rule 1

From:
   Identities:
       [User Email Address]
   Source > All sources allowed

To:
   Projects =
       [Service Project]
   Services =
       Service name: iam.googleapis.com
       Service methods: All actions
       Service name: compute.googleapis.com
       Service methods:All actions

OR
Rule 2

From:
   Identities:
       [User Email Address]
   Source > All sources allowed
To:
   Projects =
       [Host Project]
   Services =
       Service name: compute.googleapis.com
       Service methods: All actions

OR

Rule 3

From:
   Identities:
       [Service Project Number]@cloudservices.gserviceaccount.com
   Source > All sources allowed
To:
   Projects =
       [Service Project]
       [Host Project]
   Services =
       Service name: compute.googleapis.com
       Service methods: All actions

Egress rules

Rule 1:

From:
   Identities:
       [Service Project Number]@cloudservices.gserviceaccount.com
To:
   Projects =
       14190056516
   Service =
       Service name: compute.googleapis.com
       Service methods: All actions

The project number outlined above is the project netapp-cloudmanager used by NetApp to store images for the Connector and for Cloud Volumes ONTAP.
Create a service account for data tiering and backups

Cloud Volumes ONTAP requires a Google Cloud service account for two purposes. The first is when you enable data tiering to tier cold data to low-cost object storage in Google Cloud. The second is when you enable the BlueXP backup and recovery to back up volumes to low-cost object storage.

Cloud Volumes ONTAP uses the service account to access and manage one bucket for tiered data and another bucket for backups.

You can set up one service account and use it for both purposes. The service account must have the Storage Admin role.

Steps
1. In the Google Cloud console, go to the Service accounts page.
2. Select your project.
3. Click Create service account and provide the required information.
   a. Service account details: Enter a name and description.
   b. Grant this service account access to project: Select the Storage Admin role.
c. **Grant users access to this service account**: Add the Connector service account as a Service Account User to this new service account.

   This step is required for data tiering only. It’s not required for BlueXP backup and recovery.
What's next?

You’ll need to select the service account later when you create a Cloud Volumes ONTAP working environment.
Using customer-managed encryption keys with Cloud Volumes ONTAP

While Google Cloud Storage always encrypts your data before it’s written to disk, you can use the BlueXP API to create a Cloud Volumes ONTAP system that uses customer-managed encryption keys. These are keys that you generate and manage in GCP using the Cloud Key Management Service.

Steps

1. Ensure that the BlueXP Connector service account has the correct permissions at the project level, in the project where the key is stored.

   The permissions are provided in the Connector service account permissions by default, but may not be applied if you use an alternate project for the Cloud Key Management Service.

   The permissions are as follows:

   - `cloudkms.cryptoKeyVersions.useToEncrypt`
   - `cloudkms.cryptoKeys.get`
   - `cloudkms.cryptoKeys.list`
   - `cloudkms.keyRings.list`

2. Ensure that the service account for the Google Compute Engine Service Agent has Cloud KMS Encrypter/Decrypter permissions on the key.
The name of the service account uses the following format: "service-[service_project_number]@compute-system.iam.gserviceaccount.com".

Google Cloud Documentation: Using IAM with Cloud KMS - Granting roles on a resource

3. Obtain the "id" of the key by invoking the get command for the /gcp/vsa/metadata/gcp-encryption-keys API call or by choosing "Copy Resource Name" on the key in the GCP console.

4. If using customer-managed encryption keys and tiering data to object storage, BlueXP attempts to utilize the same keys that are used to encrypt the persistent disks. But you'll first need to enable Google Cloud Storage buckets to use the keys:
   a. Find the Google Cloud Storage service agent by following the Google Cloud Documentation: Getting the Cloud Storage service agent.
   b. Navigate to the encryption key and assign the Google Cloud Storage service agent with Cloud KMS Encrypter/Decrypter permissions.

For more information, refer to Google Cloud Documentation: Using customer-managed encryption keys.

5. Use the "GcpEncryption" parameter with your API request when creating a working environment.

Example

```
"gcpEncryptionParameters": {
"key": "projects/project-1/locations/us-east4/keyRings/keyring-1/cryptoKeys/generatedkey1"
}
```

Refer to the BlueXP automation docs for more details about using the "GcpEncryption" parameter.

Set up licensing for Cloud Volumes ONTAP in Google Cloud

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 Google Cloud 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.

![Select Charging Method]

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

**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 Google Cloud Marketplace
- An annual contract

**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 Google Cloud 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.


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

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

**Annual contract**

Pay for Cloud Volumes ONTAP annually by purchasing an annual contract.

**Steps**

1. Contact your NetApp sales representative to purchase an annual contract.
   
   The contract is available as a *private* offer in the Google Cloud Marketplace.

   After NetApp shares the private offer with you, you can select the annual plan when you subscribe from the Google Cloud Marketplace during working environment creation.

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 annual plan in the Google Cloud Marketplace.
   b. In Google Cloud, select the annual plan that was shared with your account and then click **Subscribe**.
   c. After you return to BlueXP, select a capacity-based package when you reach the charging methods page.

**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.

**Launching Cloud Volumes ONTAP in Google Cloud**

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

**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.
  - The service account associated with the Connector should have the required permissions
- An understanding of the configuration that you want to use.

You should have prepared by choosing a configuration and by obtaining Google Cloud networking information from your administrator. For details, see 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.
• Google Cloud APIs should be enabled in your project:
  ◦ Cloud Deployment Manager V2 API
  ◦ Cloud Logging API
  ◦ Cloud Resource Manager API
  ◦ Compute Engine API
  ◦ Identity and Access Management (IAM) API

**Launching a single-node system in Google Cloud**

Create a working environment in BlueXP to launch Cloud Volumes ONTAP in Google Cloud.

**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 *Google Cloud* and *Cloud Volumes ONTAP*.
4. If you’re prompted, create a **Connector**.
5. **Details & Credentials**: Select a project, specify a cluster name, optionally select a service account, optionally add labels, and then specify credentials.

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Working Environment Name</td>
<td>BlueXP uses the working environment name to name both the Cloud Volumes ONTAP system and the Google Cloud VM instance. It also uses the name as the prefix for the predefined security group, if you select that option.</td>
</tr>
<tr>
<td>Service Account Name</td>
<td>If you plan to use data tiering or BlueXP backup and recovery with Cloud Volumes ONTAP, then you need to enable Service Account and select a service account that has the predefined Storage Admin role. Learn how to create a service account.</td>
</tr>
</tbody>
</table>
| Add Labels        | Labels are metadata for your Google Cloud resources. BlueXP adds the labels to the Cloud Volumes ONTAP system and Google Cloud resources associated with the system.  
                      
                      You can add up to four labels 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 labels when creating a working environment.  
                      
                      For information about labels, refer to Google Cloud Documentation: Labeling 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 System Manager or its CLI. Keep the default *admin* user name or change it to a custom user name. |
Field | Description
--- | ---
Edit Project | Select the project where you want Cloud Volumes ONTAP to reside. The default project is the project where BlueXP resides.

If you don’t see any additional projects in the drop-down list, then you haven’t yet associated the BlueXP service account with other projects. Go to the Google Cloud console, open the IAM service, and select the project. Add the service account with the BlueXP role to that project. You’ll need to repeat this step for each project.

This is the service account that you set up for BlueXP, as described on this page.

Click **Add Subscription** to associate the selected credentials with a subscription.

To create a pay-as-you-go Cloud Volumes ONTAP system, you need to select a Google Cloud project that’s associated with a subscription to Cloud Volumes ONTAP from the Google Cloud Marketplace.

The following video shows how to associate a pay-as-you-go Marketplace subscription to your Google Cloud project. Alternatively, follow the steps to subscribe located in the [Associating a Marketplace subscription with Google Cloud credentials](#) section.

**Subscribe to BlueXP from the Google Cloud Marketplace**

6. **Services**: Select the services that you want to use on this system. In order to select BlueXP backup and recovery, or to use BlueXP tiering, you must have specified the Service Account in step 3.

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**: Select a location, choose a firewall policy, and confirm network connectivity to Google Cloud storage for data tiering.

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connectivity verification</td>
<td>To tier cold data to a Google Cloud Storage bucket, the subnet in which Cloud Volumes ONTAP resides must be configured for Private Google Access. For instructions, refer to <a href="#">Google Cloud Documentation: Configuring Private Google Access</a>.</td>
</tr>
</tbody>
</table>
8. **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.

9. **Preconfigured Packages**: Select one of the packages to quickly deploy a Cloud Volumes ONTAP system, or click **Create my own configuration**.

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

10. **Licensing**: Change the Cloud Volumes ONTAP version as needed and select a machine type.

    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 9.10.1 and 9.10.1 P4 is available. The update does not occur from one release to another—for example, from 9.6 to 9.7.

11. **Underlying Storage Resources**: Choose settings for the initial aggregate: a disk type and the size for each disk.

    The disk type is for the initial volume. You can choose a different disk type for subsequent volumes.

    The disk size is 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.

    For help choosing a disk type and size, see **Size your system in Google Cloud**.

12. **Flash Cache, Write Speed & WORM**:  
    a. Enable **Flash Cache**, if desired.

    Starting with Cloud Volumes ONTAP 9.13.1, **Flash Cache** is supported on the n2-standard-16, n2-standard-32, n2-standard-48, and n2-standard-64 instance types. You cannot disable Flash Cache after deployment.

    b. Choose **Normal** or **High** write speed, if desired.
Learn more about write speed.

High write speed and a higher maximum transmission unit (MTU) of 8,896 bytes are available through the **High** write speed option. In addition, the higher MTU of 8,896 requires the selection of VPC-1, VPC-2 and VPC-3 for the deployment. For more information on VPC-1, VPC-2, and VPC-3, see Rules for VPC-1, VPC-2, and VPC-3.

c. 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.

d. If you activate WORM storage, select the retention period.

13. **Data Tiering in Google Cloud Platform**: Choose whether to enable data tiering on the initial aggregate, choose a storage class for the tiered data, and then either select a service account that has the predefined Storage Admin role (required for Cloud Volumes ONTAP 9.7 or later), or select a Google Cloud account (required for Cloud Volumes ONTAP 9.6).

Note the following:

- BlueXP sets the service account on the Cloud Volumes ONTAP instance. This service account provides permissions for data tiering to a Google Cloud Storage bucket. Be sure to add the Connector service account as a user of the tiering service account, otherwise, you can’t select it from BlueXP.
- For help with adding a Google Cloud account, see Setting up and adding Google Cloud accounts for data tiering with 9.6.
- 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, but you’ll need to turn off the system and add a service account from the Google Cloud console.

Learn more about data tiering.

14. **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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Size</td>
<td>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.</td>
</tr>
<tr>
<td>Access control (for NFS only)</td>
<td>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.</td>
</tr>
</tbody>
</table>
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:

![Volume page filled out for the CIFS protocol](image)

15. CIFS Setup: If you chose the CIFS protocol, set up a CIFS server.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS Primary and Secondary IP Address</td>
<td>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. If you’re configuring Google Managed Active Directory, AD can be accessed by default with the 169.254.169.254 IP address.</td>
</tr>
<tr>
<td>Active Directory Domain to join</td>
<td>The FQDN of the Active Directory (AD) domain that you want the CIFS server to join.</td>
</tr>
<tr>
<td>Credentials authorized to join the domain</td>
<td>The name and password of a Windows account with sufficient privileges to add computers to the specified Organizational Unit (OU) within the AD domain.</td>
</tr>
<tr>
<td>CIFS server NetBIOS name</td>
<td>A CIFS server name that is unique in the AD domain.</td>
</tr>
<tr>
<td>Organizational Unit</td>
<td>The organizational unit within the AD domain to associate with the CIFS server. The default is CN=Computers.</td>
</tr>
<tr>
<td>To configure Google Managed Microsoft AD as the AD server for Cloud Volumes ONTAP, enter OU=Computers,OU=Cloud in this field. Google Cloud Documentation: Organizational Units in Google Managed Microsoft AD</td>
<td></td>
</tr>
<tr>
<td>DNS Domain</td>
<td>The DNS domain for the Cloud Volumes ONTAP storage virtual machine (SVM). In most cases, the domain is the same as the AD domain.</td>
</tr>
<tr>
<td>NTP Server</td>
<td>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. See 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.</td>
</tr>
</tbody>
</table>

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

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

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

**Result**
BlueXP deploys the Cloud Volumes ONTAP system. You can track the progress in the timeline.
If you experience any issues deploying the Cloud Volumes ONTAP system, 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 System Manager or the CLI.

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

**Launching an HA pair in Google Cloud**

Create a working environment in BlueXP to launch Cloud Volumes ONTAP in Google Cloud.

**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 **Google Cloud** and **Cloud Volumes ONTAP HA**.
4. **Details & Credentials**: Select a project, specify a cluster name, optionally select a Service Account, optionally add labels, and then specify credentials.

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Working Environment Name</td>
<td>BlueXP uses the working environment name to name both the Cloud Volumes ONTAP system and the Google Cloud VM instance. It also uses the name as the prefix for the predefined security group, if you select that option.</td>
</tr>
<tr>
<td>Service Account Name</td>
<td>If you plan to use the BlueXP tiering or BlueXP backup and recovery services, you need to enable the <strong>Service Account</strong> switch and then select the Service Account that has the predefined Storage Admin role.</td>
</tr>
<tr>
<td>Add Labels</td>
<td>Labels are metadata for your Google Cloud resources. BlueXP adds the labels to the Cloud Volumes ONTAP system and Google Cloud resources associated with the system. You can add up to four labels from the user interface when creating a working environment, and then you can add more after it's created. Note that the API does not limit you to four labels when creating a working environment. For information about labels, refer to Google Cloud Documentation: Labeling Resources.</td>
</tr>
<tr>
<td>User name and password</td>
<td>These are the credentials for the Cloud Volumes ONTAP cluster administrator account. You can use these credentials to connect to Cloud Volumes ONTAP through System Manager or its CLI. Keep the default admin user name or change it to a custom user name.</td>
</tr>
</tbody>
</table>
**Field** | **Description**
--- | ---
Edit Project | Select the project where you want Cloud Volumes ONTAP to reside. The default project is the project where BlueXP resides.

If you don’t see any additional projects in the drop-down list, then you haven’t yet associated the BlueXP service account with other projects. Go to the Google Cloud console, open the IAM service, and select the project. Add the service account with the BlueXP role to that project. You’ll need to repeat this step for each project.

This is the service account that you set up for BlueXP, as described on this page.

Click **Add Subscription** to associate the selected credentials with a subscription.

To create a pay-as-you-go Cloud Volumes ONTAP system, you need to select a Google Cloud project that's associated with a subscription to Cloud Volumes ONTAP from the Google Cloud Marketplace.

The following video shows how to associate a pay-as-you-go Marketplace subscription to your Google Cloud project. Alternatively, follow the steps to subscribe located in the **Associating a Marketplace subscription with Google Cloud credentials** section.

**Subscribe to BlueXP from the Google Cloud Marketplace**

5. **Services**: Select the services that you want to use on this system. In order to select BlueXP backup and recovery, or to use BlueXP Tiering, you must have specified the Service Account in step 3.

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 multiple zones (recommended) or a single zone for the HA configuration. Then select a region and zones.

   Learn more about HA deployment models.

7. **Connectivity**: Select four different VPCs for the HA configuration, a subnet in each VPC, and then choose a firewall policy.

   Learn more about networking requirements.

The following table describes fields for which you might need guidance:
### Field | Description
--- | ---
Generated policy | If you let BlueXP generate the firewall policy for you, you need to choose how you’ll allow traffic:
  - If you choose **Selected VPC only**, the source filter 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 filter for inbound traffic is the 0.0.0.0/0 IP range.
Use existing | If you use an existing firewall policy, ensure that it includes the required rules. Learn about firewall rules for Cloud Volumes ONTAP.

8. **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.

9. **Preconfigured Packages**: Select one of the packages to quickly deploy a Cloud Volumes ONTAP system, or click **Create my own configuration**.

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

10. **Licensing**: Change the Cloud Volumes ONTAP version as needed and select a machine type.

    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 9.10.1 and 9.10.1 P4 is available. The update does not occur from one release to another—for example, from 9.6 to 9.7.

11. **Underlying Storage Resources**: Choose settings for the initial aggregate: a disk type and the size for each disk.

    The disk type is for the initial volume. You can choose a different disk type for subsequent volumes.

    The disk size is 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.

    For help choosing a disk type and size, see [Size your system in Google Cloud](#).

12. **Flash Cache, Write Speed & WORM**:
   a. Enable **Flash Cache**, if desired.

      Starting with Cloud Volumes ONTAP 9.13.1, **Flash Cache** is supported on the n2-standard-16, n2-standard-32, n2-standard-48, and n2-standard-64 instance types. You cannot disable Flash Cache after deployment.

   b. Choose **Normal** or **High** write speed, if desired.
Learn more about write speed.

High write speed and a higher maximum transmission unit (MTU) of 8,896 bytes are available through the High write speed option with the n2-standard-16, n2-standard-32, n2-standard-48, and n2-standard-64 instance types. In addition, the higher MTU of 8,896 requires the selection of VPC-1, VPC-2 and VPC-3 for the deployment. High write speed and an MTU of 8,896 are feature-dependent and cannot be disabled individually within a configured instance. For more information on VPC-1, VPC-2, and VPC-3, see Rules for VPC-1, VPC-2, and VPC-3.

c. 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.

d. If you activate WORM storage, select the retention period.

13. Data Tiering in Google Cloud: Choose whether to enable data tiering on the initial aggregate, choose a storage class for the tiered data, and then select a service account that has the predefined Storage Admin role.

Note the following:

◦ BlueXP sets the service account on the Cloud Volumes ONTAP instance. This service account provides permissions for data tiering to a Google Cloud Storage bucket. Be sure to add the Connector service account as a user of the tiering service account, otherwise, you can’t select it from BlueXP.

◦ 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, but you’ll need to turn off the system and add a service account from the Google Cloud console.

Learn more about data tiering.

14. 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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Size</td>
<td>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.</td>
</tr>
<tr>
<td>Access control (for NFS only)</td>
<td>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.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Permissions and Users / Groups (for CIFS only)</td>
<td>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.</td>
</tr>
<tr>
<td>Snapshot Policy</td>
<td>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.</td>
</tr>
<tr>
<td>Advanced options (for NFS only)</td>
<td>Select an NFS version for the volume: either NFSv3 or NFSv4.</td>
</tr>
<tr>
<td>Initiator group and IQN (for iSCSI only)</td>
<td>iSCSI storage targets are called LUNs (logical units) and are presented to hosts as standard block devices.</td>
</tr>
<tr>
<td></td>
<td>Initiator groups are tables of iSCSI host node names and control which initiators have access to which LUNs.</td>
</tr>
<tr>
<td></td>
<td>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).</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>

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

![Volume page](image)

15. **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.

If you’re configuring Google Managed Active Directory, AD can be accessed by default with the 169.254.169.254 IP address.

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.

To configure Google Managed Microsoft AD as the AD server for Cloud Volumes ONTAP, enter **OU=Computers,OU=Cloud** in this field.

[Google Cloud Documentation: Organizational Units in Google Managed Microsoft AD](#)

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. See 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.

### 16. Usage Profile, Disk Type, and Tiering Policy
Choose whether you want to enable storage efficiency features and change the volume tiering policy, if needed.

For more information, see [Choose a volume usage profile](#) and [Data tiering overview](#).

### 17. Review & Approve
Review and confirm your selections.

a. Review details about the configuration.

b. Click **More information** to review details about support and the Google Cloud resources that BlueXP will purchase.

c. Select the **I understand...** check boxes.

d. Click **Go**.

### Result
BlueXP deploys the Cloud Volumes ONTAP system. You can track the progress in the timeline.
If you experience any issues deploying the Cloud Volumes ONTAP system, 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 System Manager or the CLI.

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

### Google Cloud Platform Image Verification

#### Google Cloud image verification overview

Google Cloud image verification complies with enhanced NetApp security requirements. Changes have been made to the script generating the images to sign the image along the way using private keys specifically generated for this task. You can verify the integrity of the GCP image by using the signed digest and public certificate for Google Cloud which can be downloaded via NSS for a specific release.

[Google Cloud NSS](#)

Google Cloud image verification is supported on Cloud Volumes ONTAP software version 9.13.0 or greater.

#### Convert image to raw format on Google Cloud

The image being used to deploy new instances, upgrades, or being used in existing images will be shared with the clients through the NetApp Support Site (NSS). The signed digest, and the certificates will be available to download through the NSS portal. Make sure you are downloading the digest and certificates for the right release corresponding to the image shared by NetApp Support. For instance, 9.13.0 images will have a 9.13.0 signed digest and certificates available on NSS.

#### Why is this step needed?

The images from Google Cloud cannot be downloaded directly. In order to verify the image against the signed digest and the certificates, you need to have a mechanism to compare the two files and download the image. To do so, you must export/convert the image into a disk.raw format and save the results in a storage bucket on Google Cloud. The disk.raw file is tarred and gzipped in the process.

The user/service-account will need privileges to perform the following:

- Access to Google storage bucket
- Write to Google Storage bucket
- Create cloud build jobs (used during export process)
- Access to the desired image
- Create export image tasks
To verify the image, it must be converted to a disk.raw format and then downloaded.

**Use Google Cloud command line to export Google Cloud image**

The preferred way to export an image to Cloud Storage is to use the `gcloud compute images export` command. This command takes the provided image and converts it to a disk.raw file which gets tarred and gzipped. The generated file is saved at the destination URL and can then be downloaded for verification.

The user/account must have privileges to access and write to the desired bucket, export the image, and cloud builds (used by Google to export the image) to execute this operation.

**Export Google Cloud image using gcloud**
Click to display the script

```bash
$ gcloud compute images export
   --destination-uri DESTINATION_URI \
   --image IMAGE_NAME

# For our example:
$ gcloud compute images export
   --destination-uri gs://vsa-dev-bucket1/example-user-exportimage-gcp-demo \
   --image example-user-20230120115139

## DEMO ##
# Step 1 - Optional: Checking access and listing objects in the destination bucket
$ gsutil ls gs://example-user-export-image-bucket/

# Step 2 - Exporting the desired image to the bucket
$ gcloud compute images export --image example-user-export-image-demo --destination-uri gs://example-user-export-image-bucket/export-demo.tar.gz
Created [https://cloudbuild.googleapis.com/v1/projects/example-demo-project/locations/us-central1/builds/xxxxxxxxxxxx].
Logs are available at [https://console.cloud.google.com/cloud-build/builds;region=us-central1/xxxxxxxxxxxx?project=xxxxxxxxxxxx].
[image-export]: 2023-01-25T18:13:48Z Fetching image "example-user-export-image-demo" from project "example-demo-project".
[image-export]: 2023-01-25T18:13:49Z Validating workflow
[image-export]: 2023-01-25T18:13:49Z Validating step "setup-disks"
[image-export]: 2023-01-25T18:13:49Z Validating step "image-export-export-disk"
[image-export.image-export-export-disk]: 2023-01-25T18:13:49Z Validating step "run-image-export-export-disk"
[image-export.image-export-export-disk]: 2023-01-25T18:13:50Z Validating step "copy-image-object"
[image-export.image-export-export-disk]: 2023-01-25T18:13:50Z Validating step "delete-inst"
[image-export]: 2023-01-25T18:13:51Z Validation Complete
[image-export]: 2023-01-25T18:13:51Z Workflow Project: example-demo-project
[image-export]: 2023-01-25T18:13:51Z Workflow Zone: us-central1-c
```
Workflow GCPath: gs://example-demo-project-example-bkt-us/

Example scratch path: https://console.cloud.google.com/storage/browser/example-demo-project-example-bkt-us/example-image-export-20230125-18:13:49-r88px

Uploading sources

Running workflow

Running step "setup-disks" (CreateDisks)

CreateDisks: Creating disk "disk-image-export-image-export-r88px".

Step "setup-disks" (CreateDisks) successfully finished.

Running step "image-export-export-disk" (IncludeWorkflow)

Running step "setup-disks" (CreateDisks)

CreateDisks: Creating disk "disk-image-export-export-disk-image-export-image-export--r88px".

Step "setup-disks" (CreateDisks) successfully finished.

Running step "run-image-export-export-disk" (CreateInstances)

CreateInstances: Creating instance "inst-image-export-export-disk-image-export-image-export--r88px".

Step "run-image-export-export-disk" (CreateInstances) successfully finished.


Running step "wait-for-inst-image-export-export-disk" (WaitForInstancesSignal)

WaitForInstancesSignal: Instance "inst-image-export-export-disk-image-export-image-export--r88px": watching serial port 1, SuccessMatch: "ExportSuccess", FailureMatch: ["ExportFailed:""] (this is not an error), StatusMatch: "GCEExport:"

WaitForInstancesSignal: Instance "inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: <serial-output key:'source-size-gb' value:'10'>"
StatusMatch found: "GCEExport: Running export tool."
StatusMatch found: "GCEExport: Disk /dev/sdb is 10 GiB, compressed size will most likely be much smaller."
StatusMatch found: "GCEExport: Beginning export process...
StatusMatch found: "GCEExport: Using "/root/upload" as the buffer prefix, 1.0 GiB as the buffer size, and 4 as the number of workers."
StatusMatch found: "GCEExport: Creating gzipped image of "/dev/sdb"."
StatusMatch found: "GCEExport: Read 1.0 GiB of 10 GiB (212 MiB/sec), total written size: 992 MiB (198 MiB/sec)"
StatusMatch found: "GCEExport: Read 8.0 GiB of 10 GiB (237 MiB/sec), total written size: 1.5 GiB (17 MiB/sec)"
StatusMatch found: "GCEExport: Finished creating gzipped image of "/dev/sdb" in 48.956433327s [213 MiB/s] with a compression ratio of 6."
[image-export.image-export-export-disk.wait-for-inst-image-export-export-disk]: 2023-01-25T18:15:19Z WaitForInstancesSignal: Instance "inst-image-export-export-disk-image-export-image-export--r88px": SuccessMatch found "ExportSuccess"

Step "wait-for-inst-image-export-export-disk" (WaitForInstancesSignal) successfully finished.

Step "copy-image-object" (CopyGCSObjects) successfully finished.

Step "delete-inst" (DeleteResources) successfully finished.

Step "copy-image-object" (CopyGCSObjects) successfully finished.

Step "delete-inst" (DeleteResources) successfully finished.

Step "image-export-export-disk" (IncludeWorkflow) successfully finished.

Serial-output value -> source-size-gb:10
Serial-output value -> target-size-gb:2

Workflow "image-export" cleaning up (this may take up to 2 minutes).

Workflow "image-export" finished cleanup.

# Step 3 - Validating the image was successfully exported
$ gsutil ls gs://example-user-export-image-bucket/
gs://example-user-export-image-bucket/export-demo.tar.gz

# Step 4 - Download the exported image
$ gcloud storage cp gs://BUCKET_NAME/OBJECT_NAME SAVE_TO_LOCATION
$ gcloud storage cp gs://example-user-export-image-bucket/export-demo.tar.gz CVO_GCP_Signed_Digest.tar.gz
Copying gs://example-user-export-image-bucket/export-demo.tar.gz to file://CVO_GCP_Signed_Digest.tar.gz
  Completed files 1/1 | 1.5GiB/1.5GiB | 185.0MiB/s

Average throughput: 213.3MiB/s
$ ls -l
  total 1565036
  -rw-r--r-- 1 example-user example-user 1602589949 Jan 25 18:44 CVO_GCP_Signed_Digest.tar.gz

Extract zipped files

# Extracting files from the digest
$ tar -xf CVO_GCP_Signed_Digest.tar.gz

See Google Cloud doc on Exporting an image for more information on how to export an image through Google Cloud.

Image signature verification

Verify Google Cloud signed images

To verify the exported Google Cloud signed image, you must download the image digest file from the NSS to validate the disk.raw file and digest file contents.

Signed image verification workflow summary

The following is an overview of the Google Cloud signed image verification workflow process.

- From the NSS, download the Google Cloud archive containing the following files:
  - Signed digest (.sig)
  - Certificate containing the public key (.pem)
  - Certificate chain (.pem)
• Download the converted disk.raw file
• Validate the certificate using the certificate chain
• Validate the signed digest using the certificate contain the public key
  ◦ Decrypt the signed digest using the public key to extract the digest of the image file
  ◦ Create a digest of the downloaded disk.raw file
  ◦ Compare the two digest file for validation

Verification of disk.raw file and digest file contents using OpenSSL

You can verify the Google Cloud downloaded disk.raw file against the digest file contents available through the NSS using OpenSSL.

The OpenSSL commands to validate the image are compatible with Linux, Mac OS, and Windows machines.

Steps
1. Verify the certificate using OpenSSL.
# Step 1 - Optional, but recommended: Verify the certificate using OpenSSL

# Step 1.1 - Copy the Certificate and certificate chain to a directory
$ openssl version
LibreSSL 3.3.6
$ ls -l
total 48
-rw-r--r--@ 1 example-user  engr  8537 Jan 19 15:42 Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  engr  2365 Jan 19 15:42 Certificate-GCP-CVO-20230119-0XXXXX.pem

# Step 1.2 - Get the OSCP URL
$ oscp_url=$(openssl x509 -noout -ocsp_uri -in Certificate-Chain.pem)
$ oscp_url=$(openssl x509 -noout -ocsp_uri -in Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem)
$ echo $oscp_url
http://ocsp.entrust.net

# Step 1.3 - Generate an OCSP request for the certificate
$ openssl ocsp -issuer <Certificate-Chain.pem> -CAfile <Certificate-Chain.pem> -cert <Certificate.pem> -reqout <request.der>

# Step 1.4 - Optional: Check the new file "req.der" has been generated
$ ls -l
total 56
-rw-r--r--@ 1 example-user  engr  8537 Jan 19 15:42 Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  engr  2365 Jan 19 15:42 Certificate-GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--  1 example-user  engr   120 Jan 19 16:50 req.der

# Step 1.5 - Connect to the OCSP Manager using openssl to send the OCSP request
$ openssl ocsp -issuer <Certificate-Chain.pem> -CAfile <Certificate-Chain.pem> -cert <Certificate.pem> -url ${oscp_url} -resp_text -respout <response.der>
OCSP Response Data:

  OCSP Response Status: successful (0x0)
  Response Type: Basic OCSP Response
  Version: 1 (0x0)
  Responder Id: C = US, O = "Entrust, Inc.", CN = Entrust Extended Validation Code Signing CA - EVCS2

  Produced At: Jan 19 15:14:00 2023 GMT

Responses:

  Certificate ID:
    Hash Algorithm: sha1
    Issuer Name Hash: 69FA640329AB84E27220FE0927647B8194B91F2A
    Issuer Key Hash: CE894F8251AA15A28462CA312361D261FBF8FE78
    Serial Number: 5994B3D01D26D594BD1D0FA7098C6FF5
  Cert Status: good
  This Update: Jan 19 15:00:00 2023 GMT
  Next Update: Jan 26 14:59:59 2023 GMT

Signature Algorithm: sha512WithRSAEncryption

2. Place the downloaded disk.raw file, the signature, and certificates in a directory.

3. Extract the public key from the certificate using OpenSSL.

4. Decrypt the signature using the extracted public key and verify the contents of the downloaded disk.raw file.
# Step 1 - Place the downloaded disk.raw, the signature and the certificates in a directory
$ ls -l
-rw-r-r--@ 1 example-user staff Jan 19 15:42 Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem
-rw-r-r--@ 1 example-user staff Jan 19 15:42 Certificate-GCP-CVO-20230119-0XXXXX.pem
-rw-r-r--@ 1 example-user staff Jan 19 15:42 GCP_CVO_20230119-XXXXXX_digest.sig
-rw-r-r--@ 1 example-user staff Jan 19 16:39 disk.raw

# Step 2 - Extract the public key from the certificate
$ openssl x509 -pubkey -noout -in (certificate.pem) > (public_key.pem)
$ openssl x509 -pubkey -noout -in Certificate-GCP-CVO-20230119-0XXXXX.pem > CVO-GCP-pubkey.pem

$ ls -l
-rw-r-r--@ 1 example-user staff Jan 19 15:42 Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem
-rw-r-r--@ 1 example-user staff Jan 19 15:42 Certificate-GCP-CVO-20230119-0XXXXX.pem
-rw-r-r--@ 1 example-user staff Jan 19 17:02 CVO-GCP-pubkey.pem
-rw-r-r--@ 1 example-user staff Jan 19 15:42 GCP_CVO_20230119-XXXXXX_digest.sig
-rw-r-r--@ 1 example-user staff Jan 19 16:39 disk.raw

# Step 3 - Decrypt the signature using the extracted public key and verify the contents of the downloaded disk.raw
$ openssl dgst -verify (public_key) -keyform PEM -sha256 -signature (signed digest) -binary (downloaded or obtained disk.raw)
$ openssl dgst -verify CVO-GCP-pubkey.pem -keyform PEM -sha256 -signature GCP_CVO_20230119-XXXXXX_digest.sig -binary disk.raw
Verified OK

# A failed response would look like this
$ openssl dgst -verify CVO-GCP-pubkey.pem -keyform PEM -sha256 -signature GCP_CVO_20230119-XXXXXX_digest.sig -binary../sample_file.txt
Verification Failure
Copyright information

Copyright © 2023 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

Trademark information

NETAPP, the NETAPP logo, and the marks listed at http://www.netapp.com/TM are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.