NetApp

Get started

Cloud Volumes ONTAP

NetApp
February 27, 2026

Table of Contents

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 NetApp Backup and Recovery to deliver backup and restore capabilities for protection, and long-term archive of your cloud data.

  Learn more about 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 NetApp Data Classification helps you understand data context and identify sensitive data.

  Learn more about Data Classification

ⓘ   Licenses for ONTAP features are included with Cloud Volumes ONTAP.

View supported Cloud Volumes ONTAP configurations

Supported ONTAP versions for Cloud Volumes ONTAP deployments

The NetApp Console enables you to choose from several different ONTAP versions when you add a Cloud Volumes ONTAP system.

Cloud Volumes ONTAP versions other than those listed here are not available for new deployments. The patch or the generic (General Availability) version in a release here represents the base version available for deployment. For details about the available patches, refer to the versioned release notes for each release.

For information on upgrade, refer to Supported upgrade paths.

AWS

Single node

- 9.18.1
- 9.17.1 P1
- 9.16.1
- 9.15.1
- 9.15.0 P1
- 9.14.1
- 9.14.1
- 9.14.0
- 9.13.1
- 9.12.1
- 9.12.1
- 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

- 9.18.1
- 9.17.1 P1
- 9.16.1
- 9.15.1
- 9.15.0 P1

- 9.14.1
- 9.14.1
- 9.14.0
- 9.13.1
- 9.12.1
- 9.12.1
- 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
- 9.18.1
- 9.17.1 P1
- 9.16.1 P3
- 9.15.1 P10
- 9.14.1 P13
- 9.13.1 P16
- 9.12.1 P18

HA pair
- 9.18.1
- 9.17.1 P1
- 9.16.1 P3
- 9.15.1 P10
- 9.14.1 P13
- 9.13.1 P16
- 9.12.1 P18

Google Cloud

Single node
- 9.18.1
- 9.17.1 P1
- 9.16.1

- 9.15.1
- 9.15.0 P1
- 9.14.1
- 9.14.1
- 9.14.0
- 9.13.1
- 9.12.1
- 9.12.1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9.8
- 9.7 P5

HA pair

- 9.18.1
- 9.17.1 P1
- 9.16.1
- 9.15.1
- 9.15.0 P1
- 9.14.1
- 9.14.1
- 9.14.0
- 9.13.1
- 9.12.1
- 9.12.1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9.8

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 Console agent**

If you don't have a Console agent yet, you need to create one. Learn how to create a Console agent 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 Console agent and access the NetApp Console user interface that's running on that Console agent. Learn how to manually install the Console agent in a location without internet access.

2 **Plan your configuration**

The Console 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 Console agent 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 Amazon Simple Storage Service (Amazon 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 Console agent as a *key user*. Learn more.

5 **Launch Cloud Volumes ONTAP using the Console**

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

Related links

- Create a Console agent for AWS
- Create a Console agent from the AWS Marketplace
- Install and set up a Console agent on premises
- AWS permissions for the Console agent

Plan your Cloud Volumes ONTAP configuration in AWS

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

Choose a Cloud Volumes ONTAP license

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

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

Choose a supported region

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

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

Choose a supported Local Zone

Selecting a Local Zone is optional. Cloud Volumes ONTAP is supported in some AWS Local Zones including Singapore. Cloud Volumes ONTAP in AWS supports only high availability (HA) mode in a single availability zone. Single node deployments are not supported.

> ℹ️ Cloud Volumes ONTAP does not have support for data tiering and cloud tiering in AWS Local Zones. Additionally, Local Zones with instances that have not been qualified for Cloud Volumes ONTAP are not supported. An example of this is Miami, that is not available as a Local Zone, because it has only Gen6 instances that are unsupported and unqualified.

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

AWS Documentation: Getting started with AWS Local Zones.

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, the NetApp Console 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. AWS Documentation: 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.

  ⓘ Data tiering to Amazon Simple Storage Service (Amazon S3) is not supported if your Cloud Volumes ONTAP system is in an AWS Local Zone, because accessing the Amazon S3 buckets outside of the Local Zone involves higher latency and impacts Cloud Volumes ONTAP activities.

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 the Console 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, the Console 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 Console agent also requires a system disk. View details about the Console agent'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 during the deployment process. The experience is the same as any other VPC that resides in AWS. Note that you will need to first deploy a Console agent in your AWS Outpost.

There are a few limitations to point out:

- Only single node Cloud Volumes ONTAP systems are supported at this time

- The EC2 instances that you can use with Cloud Volumes ONTAP are limited to what's available in your Outpost

- Only General Purpose SSDs (gp2) are supported at this time

Collect networking information

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

Single node or HA pair in a single AZ

AWS information	Your value
Region	
VPC	
Subnet	

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

HA pair in multiple AZs

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

Choose a write speed

The Console 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 the Console, 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

Set up AWS networking for Cloud Volumes ONTAP

The NetApp Console 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

Ensure that you have fulfilled the following requirements in AWS.

Outbound internet access for Cloud Volumes ONTAP nodes

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

The Console agent contacts several endpoints for day-to-day operations. For information about the endpoints used, refer to View endpoints contacted from the Console agent and Prepare networking for using the Console.

Cloud Volumes ONTAP endpoints

Cloud Volumes ONTAP uses these endpoints to communicate with various services.

Endpoints	Applicable for	Purpose	Deployment modes	Impact if endpoint is not available
https://netapp-cloud-account.auth0.com	Authentication	Used for authentication in the Console.	Standard and restricted modes.	User authentication fails and the following services remain unavailable: • Cloud Volumes ONTAP services • ONTAP services • Protocols and proxy services

Endpoints	Applicable for	Purpose	Deployment modes	Impact if endpoint is not available
https://api.bluexp.netapp.com/tenancy	Tenancy	Used to retrieve Cloud Volumes ONTAP resource from the Console to authorize resources and users.	Standard and restricted modes.	Cloud Volumes ONTAP resources and the users are not authorized.
https://mysupport.netapp.com/aods/asupmessage https://mysupport.netapp.com/asupprod/post/1.0/postAsup	AutoSupport	Used to send AutoSupport telemetry data to NetApp support.	Standard and restricted modes	AutoSupport information remains undelivered.
The exact commercial endpoint for AWS service (suffixed with `amazonaws.com`) depends on the AWS region that you are using. Refer to the AWS documentation for details.	- CloudFormation - Elastic Compute Cloud (EC2) - Identity and Access Management (IAM) - Key Management Service (KMS) - Security Token Service (STS) - Amazon Simple Storage Service (S3)	Communication with AWS services.	Standard and private modes.	Cloud Volumes ONTAP cannot communicate with AWS service to perform specific operations in AWS.
The exact government endpoint for AWS service depends on the AWS region that you are using. The endpoints are suffixed with `amazonaws.com` and `c2s.ic.gov`. Refer to AWS SDK and AWS Documentation for more information.	- CloudFormation - Elastic Compute Cloud (EC2) - Identity and Access Management (IAM) - Key Management Service (KMS) - Security Token Service (STS) - Simple Storage Service (S3)	Communication with AWS services.	Restricted mode.	Cloud Volumes ONTAP cannot communicate with AWS service to perform specific operations in AWS.

Outbound internet access for the HA mediator

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

The manual option can be a NAT gateway or an interface VPC endpoint from the target subnet to the AWS

EC2 service. For details about VPC endpoints, refer to the AWS Documentation: Interface VPC Endpoints (AWS PrivateLink).

Network proxy configuration of NetApp Console agent

You can use the proxy servers configuration of the NetApp Console agent to enable outbound internet access from Cloud Volumes ONTAP. The Console supports two types of proxies:

- **Explicit proxy**: The outbound traffic from Cloud Volumes ONTAP uses the HTTP address of the proxy server specified during the proxy configuration of the Console agent. The administrator might also have configured user credentials and root CA certificates for additional authentication. If a root CA certificate is available for the explicit proxy, make sure to obtain and upload the same certificate to your Cloud Volumes ONTAP system using the ONTAP CLI: security certificate install command.

- **Transparent proxy**: The network is configured to automatically route outbound traffic from Cloud Volumes ONTAP through the proxy for the Console agent. When setting up a transparent proxy, the administrator needs to provide only a root CA certificate for connectivity from Cloud Volumes ONTAP, not the HTTP address of the proxy server. Make sure that you obtain and upload the same root CA certificate to your Cloud Volumes ONTAP system using the ONTAP CLI: security certificate install command.

For information about configuring proxy servers, refer to the Configure the Console agent to use a proxy server.

Private IP addresses

The Console 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 the Console 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

The Console allocates 6 IP addresses to a single-node system.

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

LIF	Purpose
Cluster management	Administrative management of the entire cluster (HA pair).
Node management	Administrative management of a node.
Intercluster	Cross-cluster communication, backup, and replication.
NAS data	Client access over NAS protocols.
iSCSI data	Client access over the iSCSI protocol. Also used by the system for other important networking workflows. This LIF is required and should not be deleted.
Storage VM management	A storage VM management LIF is used with management tools like SnapCenter.

IP addresses for HA pairs

HA pairs require more IP addresses than a single-node system does. These IP addresses are spread across

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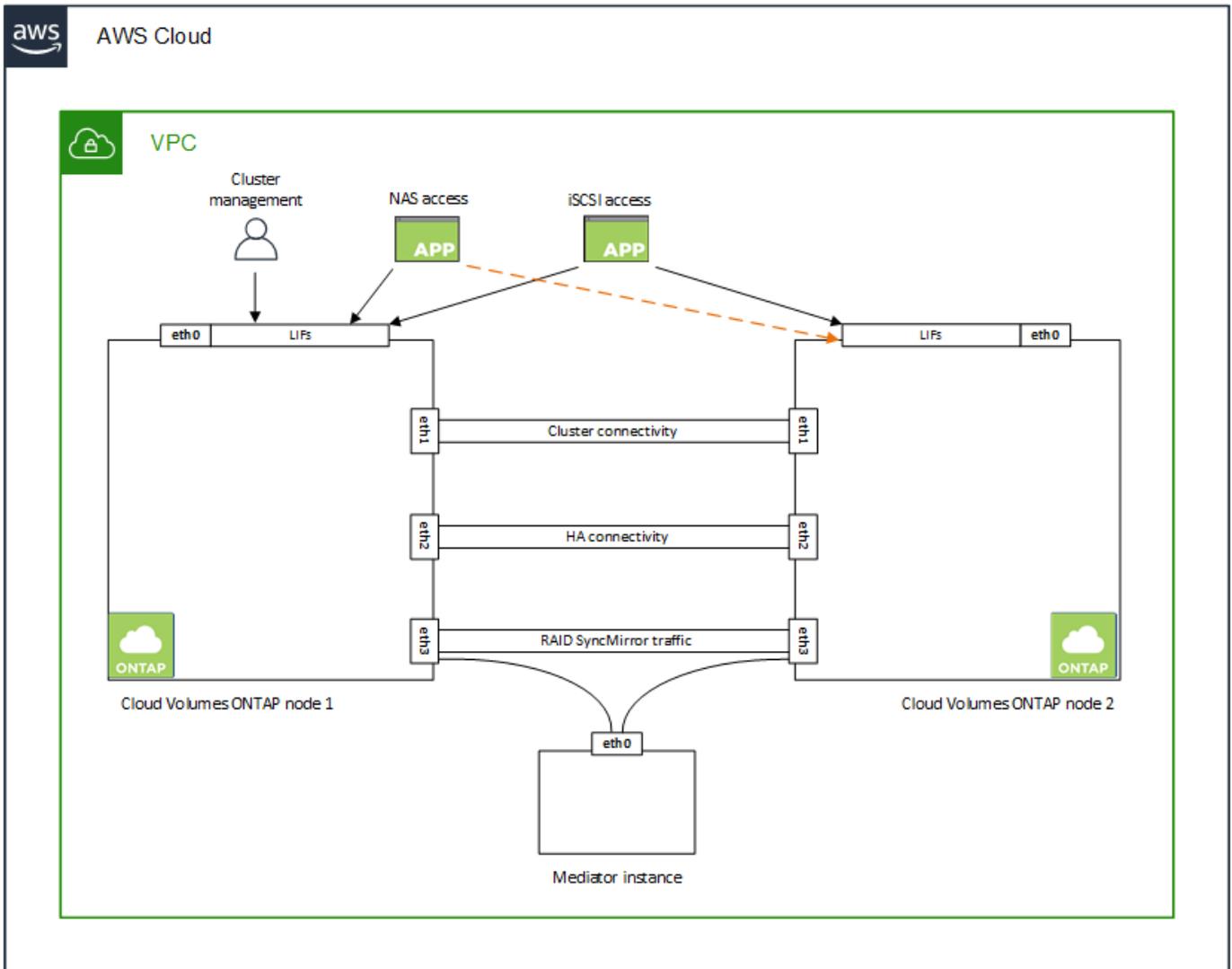
The number of private IP addresses required for an HA pair depends on which deployment model you choose. An HA pair deployed in a *single* AWS Availability Zone (AZ) requires 15 private IP addresses, while an HA pair deployed in *multiple* AZs requires 13 private IP addresses.

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

Table 1. LIFs for HA pairs in a single AZ

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

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

Table 2. LIFs for HA pairs in multiple AZs

LIF	Interface	Node	Purpose
Node management	eth0	node 1 and node 2	Administrative management of a node.
Intercluster	eth0	node 1 and node 2	Cross-cluster communication, backup, and replication.
iSCSI data	eth0	node 1 and node 2	Client access over the iSCSI protocol. These LIFs also manage the migration of floating IP addresses between nodes. These LIFs are required and should not be deleted.
Cluster connectivity	eth1	node 1 and node 2	Enables the nodes to communicate with each other and to move data within the cluster.
HA connectivity	eth2	node 1 and node 2	Communication between the two nodes in case of failover.
RSM iSCSI traffic	eth3	node 1 and node 2	RAID SyncMirror iSCSI traffic, as well as communication between the two Cloud Volumes ONTAP nodes and the mediator.
Mediator	eth0	Mediator	A communication channel between the nodes and the mediator to assist in storage takeover and giveback processes.

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

Security groups

You don't need to create security groups because the Console does that for you. If you need to use your own,

refer to Security group rules.

> 💡 Looking for information about the Console agent? View security group rules for the Console agent

Connection for data tiering

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

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

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

Connections to ONTAP systems

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

DNS and Active Directory for CIFS

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

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

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

VPC sharing

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

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

Requirements for HA pairs in multiple AZs

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

To understand how HA pairs work, refer to High-availability pairs.

Availability Zones

This HA deployment model uses multiple AZs to ensure high availability of your data. You should use a

dedicated AZ for each Cloud Volumes ONTAP instance and the mediator instance, which provides a communication channel between the HA pair.

A subnet should be available in each Availability Zone.

Floating IP addresses for NAS data and cluster/SVM management

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

One floating IP address is for cluster management, one is for NFS/CIFS data on node 1, and one is for NFS/CIFS data on node 2. A fourth floating IP address for SVM management is optional.
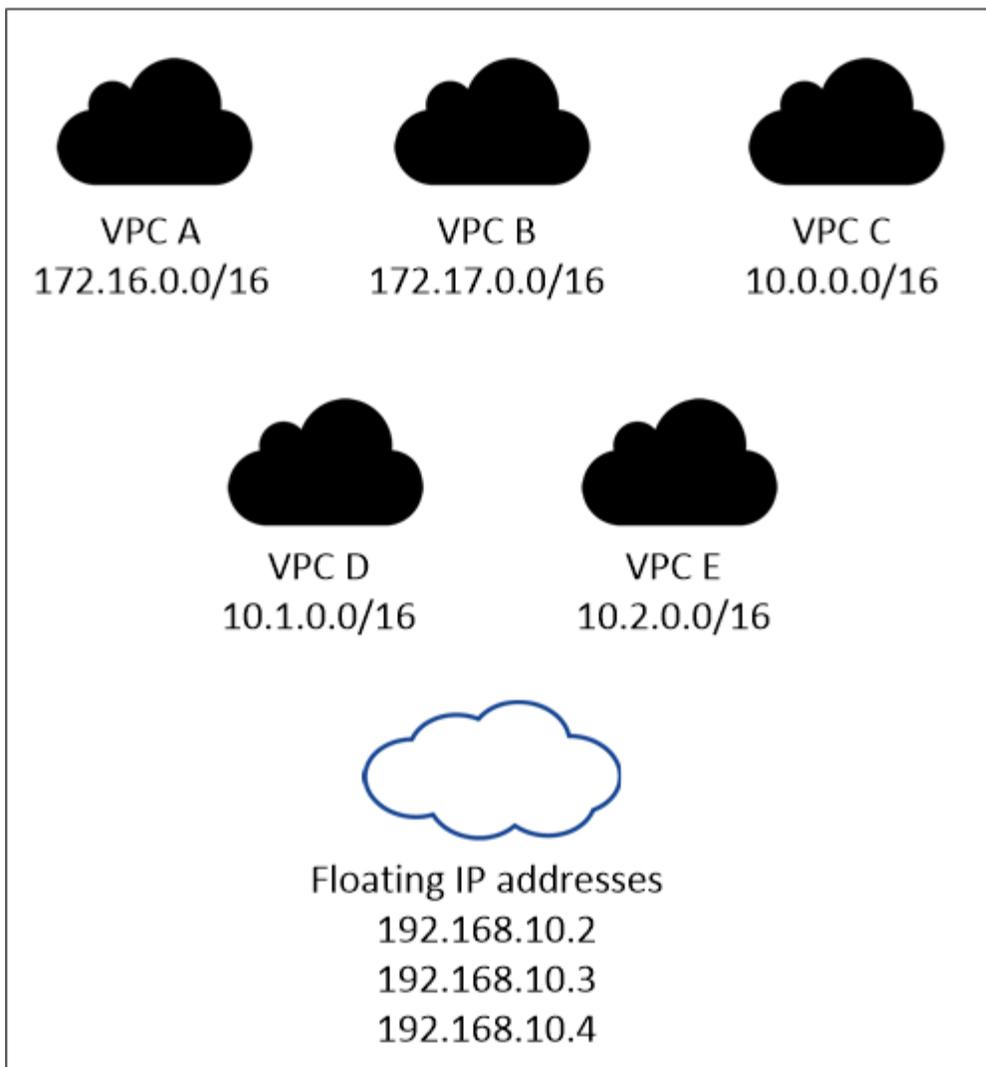
> (i) A floating IP address is required for the SVM management LIF if you use SnapDrive for Windows or SnapCenter with the HA pair.

You need to enter the floating IP addresses when you add a Cloud Volumes ONTAP HA system. The Console 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.

AWS region

VPC A
172.16.0.0/16

VPC B
172.17.0.0/16

VPC C
10.0.0.0/16

VPC D
10.1.0.0/16

VPC E
10.2.0.0/16

Floating IP addresses
192.168.10.2
192.168.10.3
192.168.10.4

(i) The Console 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, 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 the Console automatically adds the floating IP addresses to that route table. If you have more than one route table, it's very important to select the correct route tables when launching the HA pair. Otherwise, some clients might not have access to Cloud Volumes ONTAP.

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

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

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

Connection to NetApp management tools

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

1. Deploy the NetApp management tools in a different VPC and set up an AWS transit gateway. The gateway enables access to the floating IP address for the cluster management interface from outside the VPC.

2. Deploy the NetApp management tools in the same VPC with a similar routing configuration as NAS clients.

Example HA configuration

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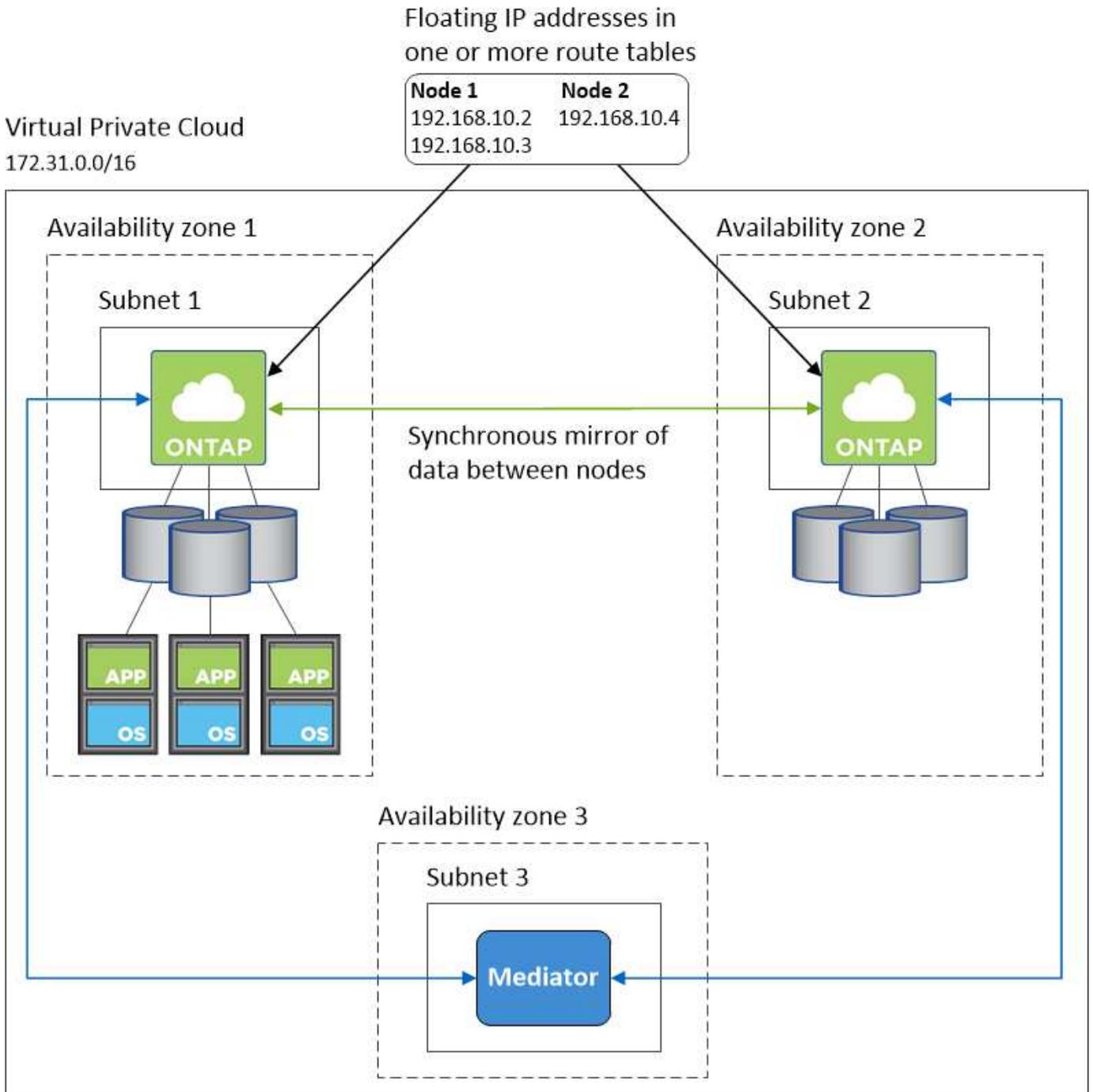
Requirements for the Console agent

If you haven't created a Console agent yet, you should review networking requirements.

- View networking requirements for the Console agent
- Security group rules in AWS

Related topics

- Verify AutoSupport setup for Cloud Volumes ONTAP
- Learn about ONTAP internal ports.

**Set up an AWS transit gateway for Cloud Volumes ONTAP HA pairs**

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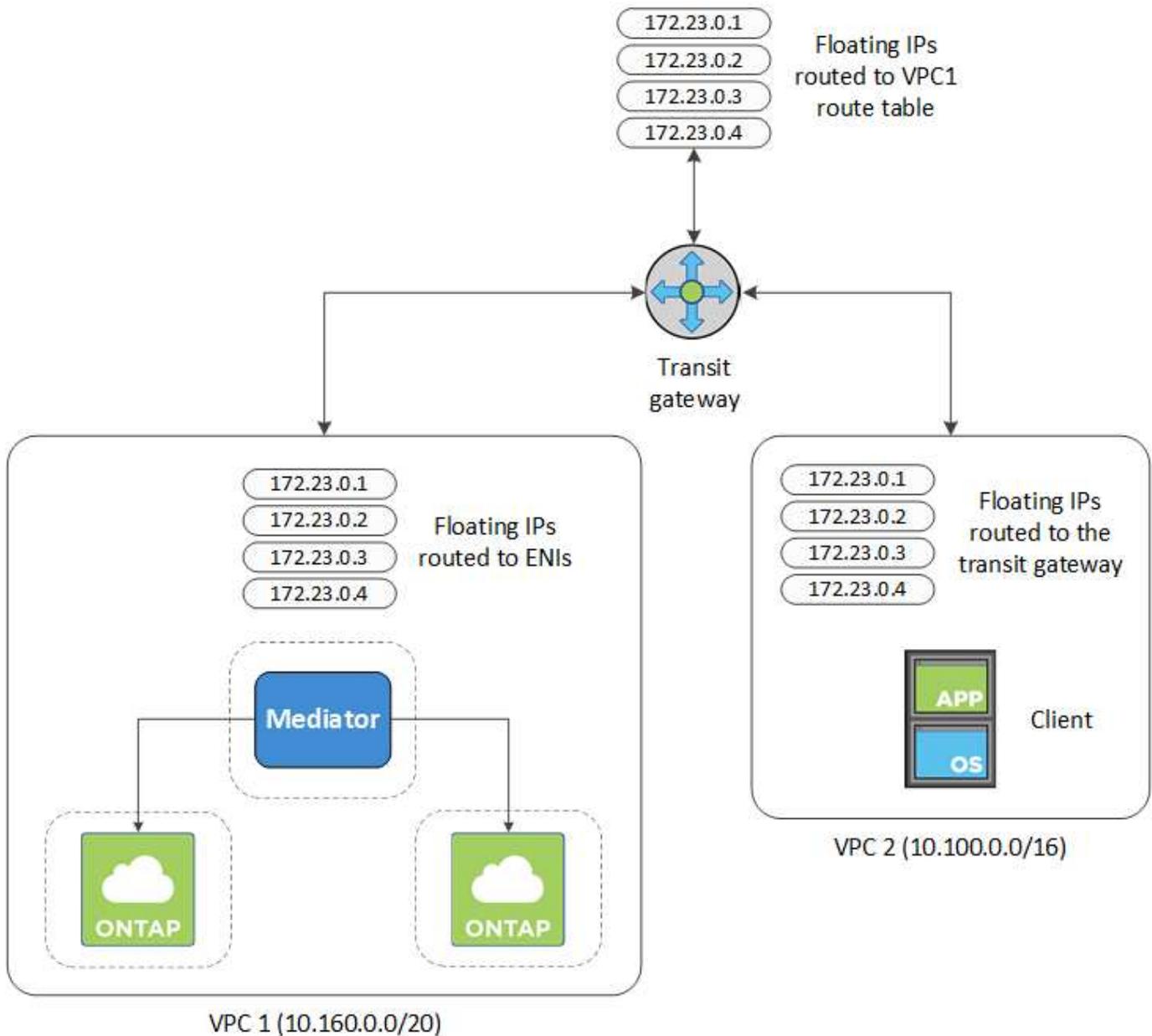
The following steps illustrate how to set up a similar configuration.

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 system information page in the NetApp Console. Here's an example:

NFS & CIFS access from within the VPC using Floating IP

ⓘ **Auto failover**

Cluster Management :	172.23.0.1
Data (nfs,cifs) :	Node 1: 172.23.0.2 | Node 2: 172.23.0.3

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.

Transit Gateway Route Table: tgw-rtb-0ea8ee291c7aeddd3

| Details | Associations | Propagations | **Routes** | Tags |

The table below will return a maximum of 1000 routes. Narrow the filter or use export routes to view more routes.

Create route | Replace route | Delete route

🔍 Filter by attributes or search by keyword

	CIDR	Attachment	Resource type	Route type	Route state
☐	10.100.0.0/16	tgw-attach-05e77bd34e2ff91f8 | vpc-0b2bc30e0dc8e0db1	⬅ **VPC2**	propagated	active
☐	10.160.0.0/20	tgw-attach-00eba3eac3250d7db | vpc-673ae603	⬅ **VPC1** VPC	propagated	active
☐	172.23.0.1/32	tgw-attach-00eba3eac3250d7db | vpc-673ae603	VPC	static	active
☐	172.23.0.2/32	tgw-attach-00eba3eac3250d7db | vpc-673ae603	VPC	static	active
☐	172.23.0.3/32	tgw-attach-00eba3eac3250d7db | vpc-673ae603	⬅ **Floating**	static	active
☐	172.23.0.4/32	tgw-attach-00eba3eac3250d7db | vpc-673ae603	**IP Addresses** static		active

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. The Console 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 the Console through the **Mount Command** option under the Manage

Volumes panel in the Console.
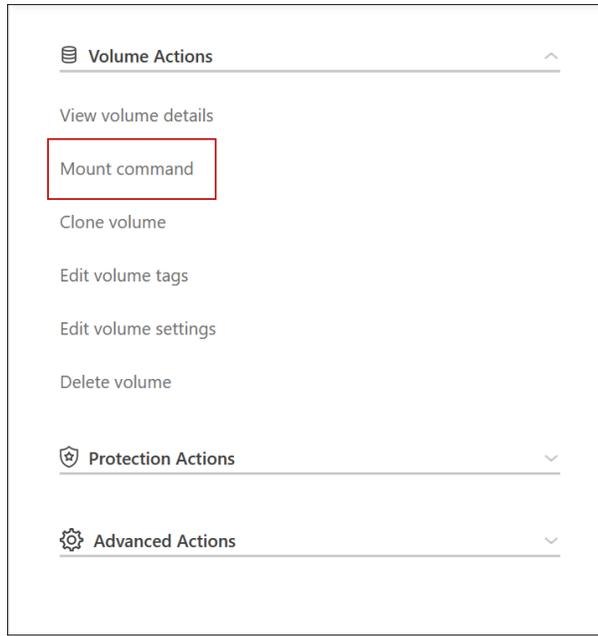
8. If you're mounting an NFS volume, configure the export policy to match the subnet of the client VPC.

   Learn how to edit a volume.

Related links

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

Deploy Cloud Volumes ONTAP HA pairs in an AWS 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:
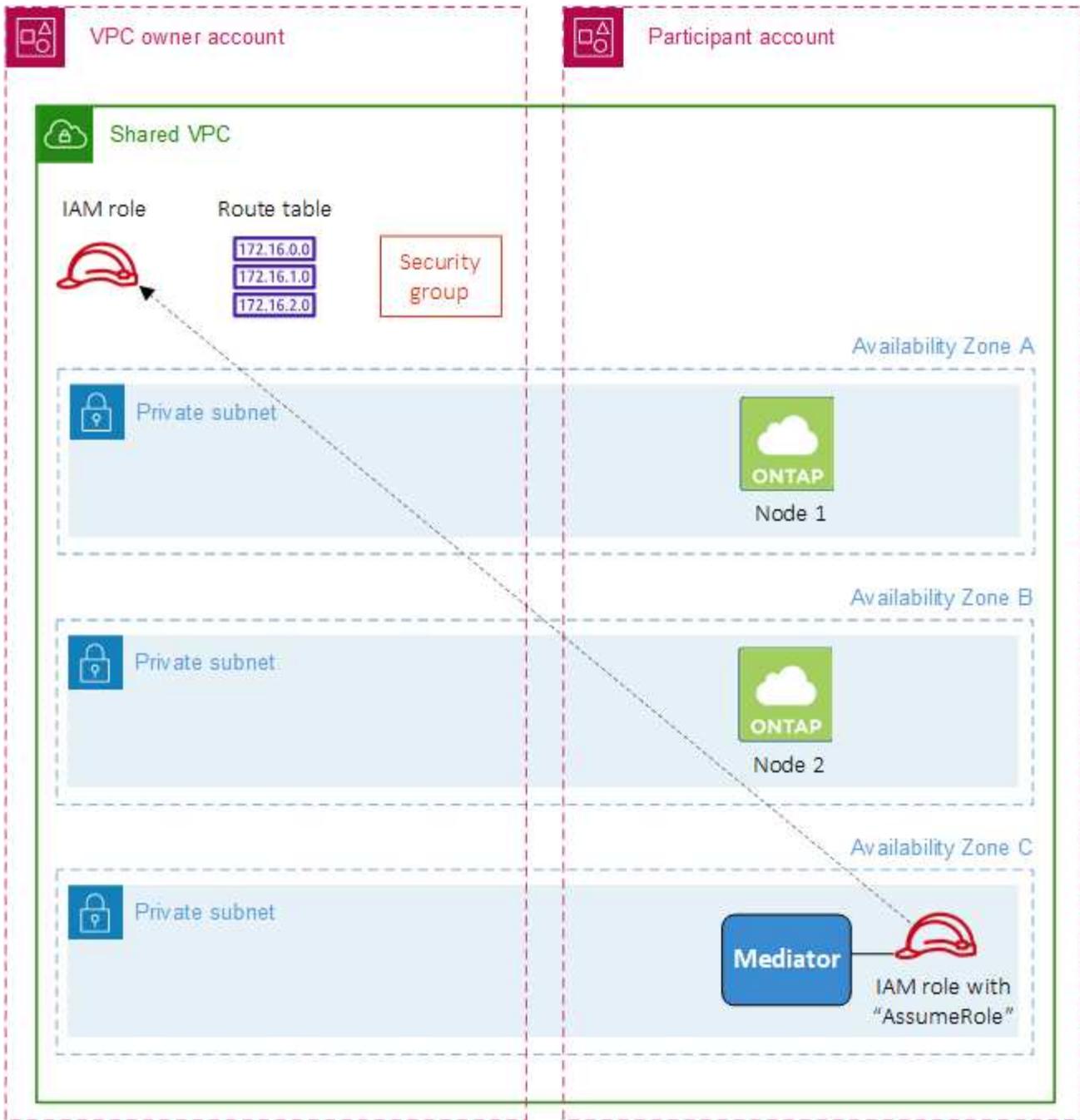
As described in the steps below, you'll need to share the subnets with the participant account, and then create the IAM role and security group in the VPC owner account.

When you create the Cloud Volumes ONTAP system, the NetApp Console 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. The Console does that for you.

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

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

4. Use the API to create a new Cloud Volumes ONTAP system.

   Note that you must specify the following fields:

   - "securityGroupId"

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

   - "assumeRoleArn" in the "haParams" object

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

     For example:

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

   Learn about the Cloud Volumes ONTAP API

Configure placement group creation for Cloud Volumes ONTAP HA pairs in AWS single AZs

Cloud Volumes ONTAP high-availability (HA) deployments in AWS single availability Zone (AZ) can fail and roll back if the creation of the placement group fails. Creation of the placement group also fails and the deployment rolls back if the Cloud Volumes ONTAP node and mediator instance are not available. To avoid this, you can modify the configuration to allow the deployment to finish even if the placement group creation fails.

On bypassing the rollback process, the Cloud Volumes ONTAP deployment process completes successfully, and notifies you that the placement group creation is incomplete.

Steps

1. Use SSH to connect to the NetApp Console agent host and log in.

2. Navigate to `/opt/application/netapp/cloudmanager/docker_occm/data`.

3. Edit `app.conf` by changing the value of the `rollback-on-placement-group-failure` parameter to `false`. The default value of this parameter is `true`.

```
{
    "occm" : {
        "aws" : {
            "rollback-on-placement-group-failure" : false
        }
    }
}
```

4. Save the file and log off the Console agent. You don't need to restart the Console agent.

AWS security group inbound and outbound rules for Cloud Volumes ONTAP

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

Rules for Cloud Volumes ONTAP

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

Inbound rules

When you add a Cloud Volumes ONTAP system 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 Console agent resides. This is the recommended option.

• **All VPCs**: the source for inbound traffic is the 0.0.0.0/0 IP range.

Protocol	Port	Purpose
All ICMP	All	Pinging the instance
HTTP	80	HTTP access to the ONTAP System Manager web console using the IP address of the cluster management LIF
HTTPS	443	Connectivity with the Console agent and HTTPS access to the ONTAP System Manager web console using the IP address of the cluster management LIF

Protocol	Port	Purpose
SSH	22	SSH access to the IP address of the cluster management LIF or a node management LIF
TCP	111	Remote procedure call for NFS
TCP	139	NetBIOS service session for CIFS
TCP	161-162	Simple network management protocol
TCP	445	Microsoft SMB/CIFS over TCP with NetBIOS framing
TCP	635	NFS mount
TCP	749	Kerberos
TCP	2049	NFS server daemon
TCP	3260	iSCSI access through the iSCSI data LIF
TCP	4045	NFS lock daemon
TCP	4046	Network status monitor for NFS
TCP	10000	Backup using NDMP
TCP	11104	Management of intercluster communication sessions for SnapMirror
TCP	11105	SnapMirror data transfer using intercluster LIFs
UDP	111	Remote procedure call for NFS
UDP	161-162	Simple network management protocol
UDP	635	NFS mount
UDP	2049	NFS server daemon
UDP	4045	NFS lock daemon
UDP	4046	Network status monitor for NFS
UDP	4049	NFS rquotad protocol

Outbound rules

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

Basic outbound rules

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

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

Advanced outbound rules

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

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

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

Service	Protocol	Port	Source	Destination	Purpose
AutoSupport	HTTPS	443	Node management LIF	mysupport.netapp.com	AutoSupport (HTTPS is the default)
	HTTP	80	Node management LIF	mysupport.netapp.com	AutoSupport (only if the transport protocol is changed from HTTPS to HTTP)
	TCP	3128	Node management LIF	Console agent	Sending AutoSupport messages through a proxy server on the Console agent, if an outbound internet connection isn't available
Backup to S3	TCP	5010	Intercluster LIF	Backup endpoint or restore endpoint	Back up and restore operations for the Backup to S3 feature
Cluster	All traffic	All traffic	All LIFs on one node	All LIFs on the other node	Intercluster communications (Cloud Volumes ONTAP HA only)
	TCP	3000	Node management LIF	HA mediator	ZAPI calls (Cloud Volumes ONTAP HA only)
	ICMP	1	Node management LIF	HA mediator	Keep alive (Cloud Volumes ONTAP HA only)
Configuration backups	HTTP	80	Node management LIF	http://<console-agent-IP-address>/occm/offboxconfig	Send configuration backups to the Console agent. ONTAP documentation
DHCP	UDP	68	Node management LIF	DHCP	DHCP client for first-time setup
DHCPS	UDP	67	Node management LIF	DHCP	DHCP server
DNS	UDP	53	Node management LIF and data LIF (NFS, CIFS)	DNS	DNS
NDMP	TCP	18600–18699	Node management LIF	Destination servers	NDMP copy
SMTP	TCP	25	Node management LIF	Mail server	SMTP alerts, can be used for AutoSupport
SNMP	TCP	161	Node management LIF	Monitor server	Monitoring by SNMP traps
	UDP	161	Node management LIF	Monitor server	Monitoring by SNMP traps
	TCP	162	Node management LIF	Monitor server	Monitoring by SNMP traps
	UDP	162	Node management LIF	Monitor server	Monitoring by SNMP traps

Service	Protocol	Port	Source	Destination	Purpose
SnapMirror	TCP	11104	Intercluster LIF	ONTAP intercluster LIFs	Management of intercluster communication sessions for SnapMirror
	TCP	11105	Intercluster LIF	ONTAP intercluster LIFs	SnapMirror data transfer
Syslog	UDP	514	Node management LIF	Syslog server	Syslog forward messages

Rules for the HA mediator external security group

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

Inbound rules

The predefined security group for the HA mediator includes the following inbound rule.

Protocol	Port	Source	Purpose
TCP	3000	CIDR of the Console agent	RESTful API access from the Console agent

Outbound rules

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

Basic outbound rules

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

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

Advanced outbound rules

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

Protocol	Port	Destination	Purpose
HTTP	80	IP address of the Console agent on AWS EC2 instance	Download upgrades for the mediator
HTTPS	443	ec2.amazonaws.com	Assist with storage failover

Protocol	Port	Destination	Purpose
UDP	53	ec2.amazonaws.com	Assist with storage failover

> ℹ️ 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.

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

Inbound rules

The predefined security group includes the following inbound rules.

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

Outbound rules

The predefined security group includes the following outbound rules.

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

Rules for the Console agent

View security group rules for the Console agent

Set up Cloud Volumes ONTAP to use a customer-managed key in AWS

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 the NetApp Console 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 the Console as a *key user*.

Adding the Identity and Access Management (IAM) role as a key user gives the Console 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 the Console when you create the Cloud Volumes ONTAP system.

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

       Typically, this is the account where the Console is deployed. If the Console is not installed in AWS, use the account for which you provided AWS access keys to the Console.
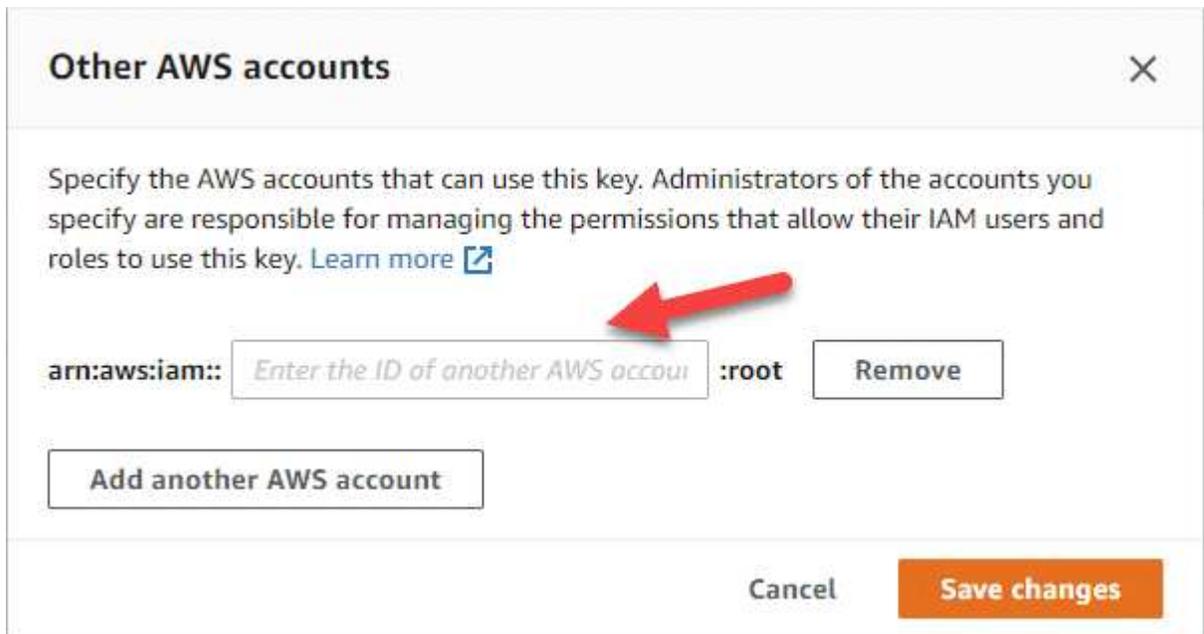
    e. Now switch to the AWS account that provides the Console with permissions and open the IAM console.

    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 the Console.

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

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

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

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

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

stored in the Amazon Simple Storage Service (Amazon 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 Cloud Volumes ONTAP system. (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 AWS IAM roles for Cloud Volumes ONTAP nodes

AWS Identity and Access management (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 the NetApp Console create the IAM roles for you, but you can use your own roles.

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

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

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

Standard regions

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

GovCloud (US) regions

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

Top Secret regions

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

Secret regions

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

◦ Backup policy for Cloud Volumes ONTAP nodes

If you plan to use NetApp 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

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

Top Secret regions

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

Secret regions

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

- HA mediator

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

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

Result

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

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 system.

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 of the NetApp Console, select **Storage > Management**.

2. On the **Systems** page, click **Add System** and follow the steps.

   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 the Console, select **Freemium** when you reach the charging methods page.

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

Capacity-based license

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

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

- A license (bring your own 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.

NetApp has restricted the purchase, extension, and renewal of BYOL licensing. For more information, refer to Restricted availability of BYOL licensing for Cloud Volumes ONTAP.
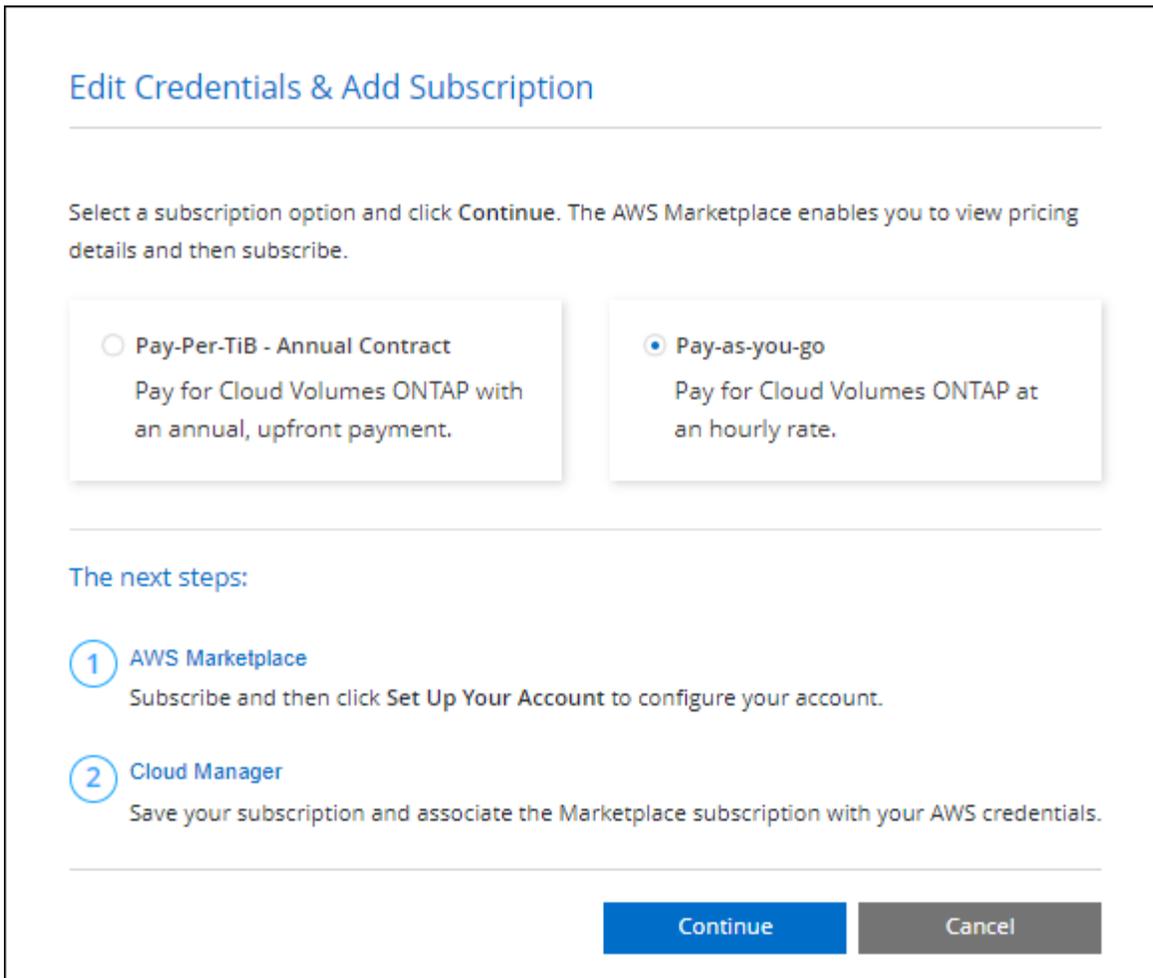
Steps

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

   The Console automatically queries NetApp's licensing service to obtain details about the licenses associated with your NetApp Support Site account. If there are no errors, the Console automatically adds the licenses to the Console.
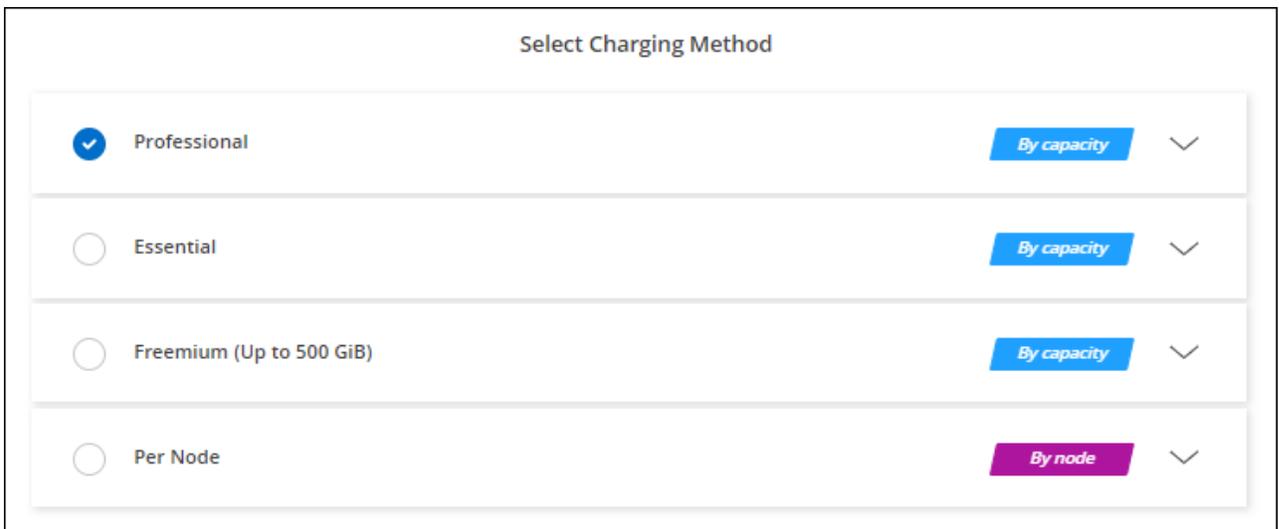
   Your license must be available from the Console before you can use it with Cloud Volumes ONTAP. If needed, you can manually add the license to the Console.

3. On the **Systems** page of the Console, click **Add System** and follow the steps.

   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.

Edit Credentials & Add Subscription

Select a subscription option and click **Continue**. The AWS Marketplace enables you to view pricing details and then subscribe.

○ **Pay-Per-TiB - Annual Contract**
Pay for Cloud Volumes ONTAP with an annual, upfront payment.

● **Pay-as-you-go**
Pay for Cloud Volumes ONTAP at an hourly rate.

The next steps:

① **AWS Marketplace**
Subscribe and then click **Set Up Your Account** to configure your account.

② **Cloud Manager**
Save your subscription and associate the Marketplace subscription with your AWS credentials.

Continue   Cancel

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

Select Charging Method

✔ Professional	By capacity	⌄
○ Essential	By capacity	⌄
○ Freemium (Up to 500 GiB)	By capacity	⌄
○ Per Node	By node	⌄

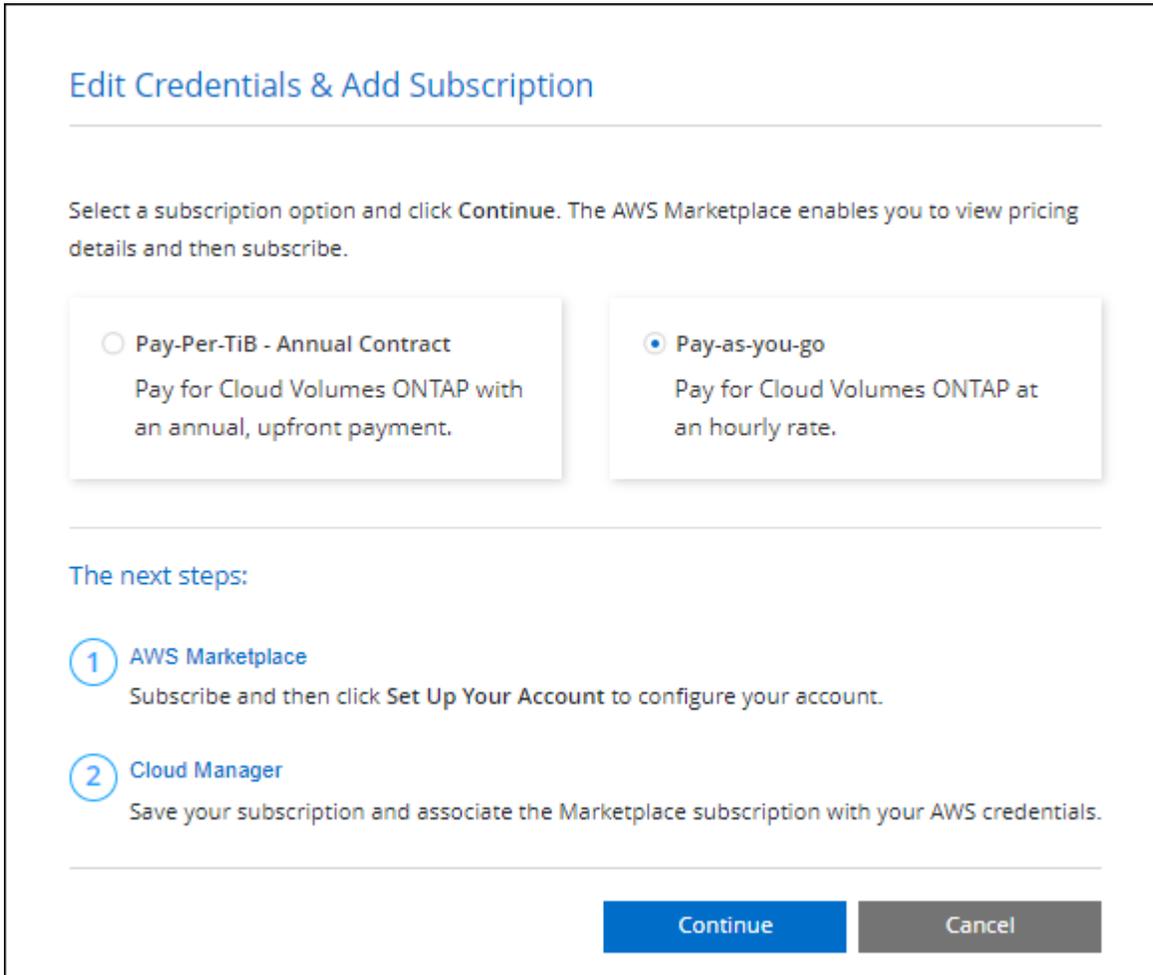View step-by-step instructions to launch Cloud Volumes ONTAP in AWS.

PAYGO subscription

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

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

Steps

1. From the left navigation menu, select **Storage > Management**.

2. On the **Systems** page, click **Add System** and follow the steps.

   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

   ---

   ## Edit Credentials & Add Subscription

   Select a subscription option and click **Continue**. The AWS Marketplace enables you to view pricing details and then subscribe.

   ○ **Pay-Per-TiB - Annual Contract**
   Pay for Cloud Volumes ONTAP with an annual, upfront payment.

   ● **Pay-as-you-go**
   Pay for Cloud Volumes ONTAP at an hourly rate.

   The next steps:

   ① **AWS Marketplace**
   Subscribe and then click **Set Up Your Account** to configure your account.

   ② **Cloud Manager**
   Save your subscription and associate the Marketplace subscription with your AWS credentials.

   [Continue]   [Cancel]

   ---

   b. After you return to the Console, 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, the Console prompts you to subscribe to the annual contract that's available in the AWS Marketplace.

Steps

1. On the **Systems** page, click **Add System** and follow the steps.

    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.

Edit Credentials & Add Subscription

Select a subscription option and click **Continue**. The AWS Marketplace enables you to view pricing details and then subscribe.

- Pay-Per-TiB - Annual Contract
  Pay for Cloud Volumes ONTAP with an annual, upfront payment.

- Pay-as-you-go
  Pay for Cloud Volumes ONTAP at an hourly rate.

The next steps:

1. AWS Marketplace
   Subscribe and then click **Set Up Your Account** to configure your account.

2. Cloud Manager
   Save your subscription and associate the Marketplace subscription with your AWS credentials.

Continue   Cancel

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

Select Charging Method

- Professional   By capacity
- Essential   By capacity
- Freemium (Up to 500 GiB)   By capacity
- Per Node   By node

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 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 **Systems** page, click **Add System** and follow the steps.

   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.

Node-based license

A node-based license is the previous generation license for Cloud Volumes ONTAP. A node-based license could be procured from NetApp (BYOL) and is available for license renewals, only in specific cases. For information, refer to:

- End of availability for node-based licenses
- End of availability of node-based licenses
- Convert a node-based license to a capacity-based license

Deploy Cloud Volumes ONTAP in AWS using quick deployment

You can deploy Cloud Volumes ONTAP in AWS using a quick deployment method for both single node and high availability (HA) configurations. This simplified process reduces deployment steps compared to the advanced method. It also offers more clarity in the workflow by automatically setting default values on a single page and minimizing navigation.

Before you begin

You need the following to add a Cloud Volumes ONTAP system in AWS from the NetApp Console.

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

  You should have prepared by choosing a configuration and by obtaining AWS networking information from your administrator. For details, refer to Planning your Cloud Volumes ONTAP configuration.

- An understanding of what's required to set up licensing for Cloud Volumes ONTAP.

  Learn how to set up licensing.

- DNS and Active Directory for CIFS configurations.

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

About this task

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

Steps

1. From the left navigation menu, select **Storage > Management**.
2. On the Canvas page, click **Add System** and follow the prompts.
3. Select **Amazon Web Services** > **Cloud Volumes ONTAP** > **Add new**. The **Quick create** option is selected by default.

system details

1. **Cloud provider account**: The account details are automatically populated based on your selected Console agent. If you have multiple accounts, select the one you want to use. If a Console agent is unavailable, you'll be prompted to create a Console agent.

2. **Name**: The system name. The Console uses the system (cluster) name to name 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.

3. **ONTAP credentials** These are the credentials for the Cloud Volumes ONTAP cluster administrator account. You can use these credentials to connect to Cloud Volumes ONTAP through ONTAP System Manager or the ONTAP CLI. You can keep the default *admin* user name or change it to a custom user name.

4. **Tags** AWS tags are metadata for your AWS resources. The Console adds the tags to the Cloud Volumes ONTAP instance and each AWS resource associated with the instance. You can add up to 15 tags from the

user interface when creating a Cloud Volumes ONTAP system, and then you can add more after its created. Note that the API does not limit you to four tags when creating a system.
For information about tags, refer to AWS Documentation: Tagging your Amazon EC2 Resources.

Deployment and configuration

1. **Deployment type**: Select the deployment type that you want to use, single node, high availability (HA) in a single availability zone (AZ), or HA in a multiple AZ.

2. **Network configuration**: Enter the network information that you recorded in the AWS worksheet.

   a. **AWS region**: By default, the region of the associated cloud account that has VPC with subnet resources is selected.

   b. **VPC**: Enter a VPC for the AWS region with a subnet. If there are no subnets, then the default value for the VPC is selected.

   c. **Subnet**: You can select a subnet for the VPC only for a single node deployment or HA deployment in a single AZ.

High Availability

If you have selected HA configuration, enter the following information:

HA in single AZ

1. **Mediator Access**: Specify the mediator access information. The mediator is a separate instance that monitors the health of the HA pair and provides quorum in case of a failure. Provide the key pair name to enable the mediator instance to connect to the AWS EC2 service, and select the connection method.

HA in multiple AZ

1. **Availability zones and mediator**: Select the availability zones (AZs) for each node and the mediator and the corresponding subnets where you want to deploy the Cloud Volumes ONTAP HA pair.

2. **Floating IPs**: If you chose multiple AZs, specify the floating IP addresses for the NFS and CIFS services and cluster and SVM management. The IP addresses must be outside of the CIDR block for all VPCs in the region. For additional details, refer to AWS networking requirements for Cloud Volumes ONTAP HA in multiple AZs.

3. **Mediator Access**: Specify the mediator access information. The mediator is a separate instance that monitors the health of the HA pair and provides quorum in case of a failure. Provide the key pair name to enable the mediator instance to connect to the AWS EC2 service, and select the connection method.

4. **Route Tables**: If you chose multiple AZs, select the route tables that include routes to the floating IP addresses. If you have more than one route table, it is important to select the correct route tables. Otherwise, some clients might not have access to the Cloud Volumes ONTAP HA pair. For more information about route tables, refer to the AWS Documentation: Route Tables.

Charging and Services

1. **Marketplace Subscription**: Select the AWS marketplace subscription you want to use with this Cloud Volumes ONTAP system.

2. **License**: Select the license type you want to use with this Cloud Volumes ONTAP system. You can choose from Professional, Essential, and Premium licenses. For information about different licenses, refer to Learn about Cloud Volumes ONTAP licenses.

3. **Data services and features**: Keep the services enabled or disable the services you don't want to use with Cloud Volumes ONTAP.

- Learn more about NetApp Classification
- Learn more about NetApp Backup and Recovery
- Learn about WORM storage on Cloud Volumes ONTAP

> 💡 If you want to utilize WORM and data tiering, you must disable Backup and Recovery and deploy a Cloud Volumes ONTAP system with version 9.8 or above.

- **NetApp Support Site account**: If you have multiple accounts, select the one you want to use.

Summary

Check or edit the details you entered, and then click **Create**.

> ⚠️ After the deployment process completes, do not modify the system-generated Cloud Volumes ONTAP configurations in the AWS cloud portal, especially the system tags. Any changes made to these configurations may lead to unexpected behavior or data loss.

Related links

- Planning your Cloud Volumes ONTAP configuration
- Deploy Cloud Volumes ONTAP in AWS using advanced deployment

Launch Cloud Volumes ONTAP in AWS

You can launch Cloud Volumes ONTAP in a single-system configuration or as an HA pair in AWS. This method provides an advanced deployment experience that offers more configuration options and flexibility than the quick deployment method.

Before you begin

You need the following before you begin.

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

  You should have prepared by choosing a configuration and by obtaining AWS networking information from your administrator. For details, refer to Planning your Cloud Volumes ONTAP configuration.

- An understanding of what's required to set up licensing for Cloud Volumes ONTAP.

  Learn how to set up licensing.

- DNS and Active Directory for CIFS configurations.

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

Launch 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 system in the NetApp

Console.

About this task

Immediately after you create the system, the Console launches a test instance in the specified VPC to verify connectivity. If successful, the Console immediately terminates the instance and then starts deploying the Cloud Volumes ONTAP system. If the connectivity can't be verified, system creation 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 > Management**.

2. On the **Systems** page, click **Add System** and follow the prompts.

3. Select **Amazon Web Services** and **Cloud Volumes ONTAP Single Node**.

4. Select **Advanced create**. Because the **Quick create** mode is selected by default, you might see a message for default values. Click **Continue**.

5. If you're prompted, create a Console agent.

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

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

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

> 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 Console website and complete the process.

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

   ◦ Learn more about NetApp Data Classification

   ◦ Learn more about NetApp Backup and Recovery

   > If you would like to utilize WORM and data tiering, you must disable Backup and Recovery and deploy a Cloud Volumes ONTAP system with version 9.8 or above.

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

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

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

9. **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.

10. **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.

11. **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.

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

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

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

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

14. **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 the Console updates the system to that version when creating the system. For example, the update occurs if you select Cloud Volumes ONTAP 9.13.1 and 9.13.1 P4 is available. The update does not occur from one release to another—for example, from 9.13 to 9.14.

15. **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, the Console 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 the Console 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.

16. **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.

17. **Create Volume**: Enter details for the new volume or click **Skip**.

Learn about supported client protocols and versions.

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

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

Field	Description
Initiator group and IQN (for iSCSI only)	iSCSI storage targets are called LUNs (logical units) and are presented to hosts as standard block devices. Initiator groups are tables of iSCSI host node names and control which initiators have access to which LUNs. iSCSI targets connect to the network through standard Ethernet network adapters (NICs), TCP offload engine (TOE) cards with software initiators, converged network adapters (CNAs) or dedicated host bust adapters (HBAs) and are identified by iSCSI qualified names (IQNs). When you create an iSCSI volume, the Console 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 first page of the volume creation wizard:

Volume Details & Protection

Volume Name: ABDcv5689

Storage VM (SVM): svm_c____i'CVO1

Volume Size: 100

Unit: GiB

Snapshot Policy: default

default policy

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

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

Field	Description
Organizational Unit	The organizational unit within the AD domain to associate with the CIFS server. The default is CN=Computers. If you configure AWS Managed Microsoft AD as the AD server for Cloud Volumes ONTAP, you should enter **OU=Computers,OU=corp** in this field.
DNS Domain	The DNS domain for the Cloud Volumes ONTAP storage virtual machine (SVM). In most cases, the domain is the same as the AD domain.
NTP Server	Select **Use Active Directory Domain** to configure an NTP server using the Active Directory DNS. If you need to configure an NTP server using a different address, then you should use the API. Refer to the NetApp Console 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.

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

    For more information, refer to Understanding volume usage profiles, Data tiering overview, and KB: What Inline Storage Efficiency features are supported with CVO?

20. **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 the Console will purchase.

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

    d. Click **Go**.

Result

The Console launches the Cloud Volumes ONTAP instance. You can track the progress on the **Audit** page.

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

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

> ⚠️ After the deployment process completes, do not modify the system-generated Cloud Volumes ONTAP configurations in the AWS cloud portal, especially the system tags. Any changes made to these configurations may lead to unexpected behavior or data loss.

After you finish

- If you provisioned a CIFS share, give users or groups permissions to the files and folders and verify that those users can access the share and create a file.

- If you want to apply quotas to volumes, use ONTAP System Manager or the ONTAP CLI.

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

Launch 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 system in the Console.

Limitation

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

About this task

Immediately after you create the Cloud Volumes ONTAP system, the Console launches a test instance in the specified VPC to verify connectivity. If successful, the Console immediately terminates the instance and then starts deploying the Cloud Volumes ONTAP system. If the connectivity can't be verified, system creation 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 > Management**.

2. On the **Systems** page, click **Add System** and follow the prompts.

3. Select **Amazon Web Services** and **Cloud Volumes ONTAP HA**.

   Some AWS Local Zones are available.

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

   If you are running the Console agent 3.9.36 or below, you need to add the `DescribeAvailabilityZones` permission to the AWS role in the AWS EC2 console.

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

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

Field	Description
System Name	The Console uses the system name to name both the Cloud Volumes ONTAP system and the Amazon EC2 instance. It also uses the name as the prefix for the predefined security group, if you select that option.
Add tags	AWS tags are metadata for your AWS resources. The Console 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 system, and then you can add more after it's created. Note that the API does not limit you to four tags when creating a system. For information about tags, refer to AWS Documentation: Tagging your Amazon EC2 Resources.

Field	Description
User name and password	These are the credentials for the Cloud Volumes ONTAP cluster administrator account. You can use these credentials to connect to Cloud Volumes ONTAP through ONTAP System Manager or the ONTAP CLI. Keep the default *admin* user name or change it to a custom user name.
Edit Credentials	Choose the AWS credentials and marketplace subscription to use with this Cloud Volumes ONTAP system. Click **Add Subscription** to associate the selected credentials with a new AWS marketplace subscription. The subscription can be for an annual contract or to pay for Cloud Volumes ONTAP at an hourly rate. If you purchased a license directly from NetApp (bring your own license (BYOL)), then an AWS subscription isn't required. NetApp has restricted the purchase, extension, and renewal of BYOL licensing. For more information, refer to Restricted availability of BYOL licensing for Cloud Volumes ONTAP. Learn how to add additional AWS credentials to the Console.

> 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 Console website and complete the process.

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

   - Learn more about NetApp Data Classification
   - Learn more about Backup and Recovery

   > If you would like to utilize WORM and data tiering, you must disable Backup and Recovery and deploy a Cloud Volumes ONTAP system with version 9.8 or above.

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

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

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

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

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

8. **Connectivity and SSH Authentication**: Choose connection methods for the HA pair and the mediator.

9. **Floating IPs**: If you chose multiple AZs, specify the floating IP addresses.

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

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

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

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

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

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

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

    Learn more about supported encryption technologies.

12. **Charging Methods and NSS Account**: Specify which charging option would you like to use with this system, and then specify a NetApp Support Site account.
    - Learn about licensing options for Cloud Volumes ONTAP.
    - Learn how to set up licensing.

13. **Cloud Volumes ONTAP Configuration** (annual AWS Marketplace contract only): Review the default configuration and click **Continue** or click **Change Configuration** to select your own configuration.

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

14. **Preconfigured Packages** (hourly or BYOL only): Select one of the packages to quickly launch Cloud Volumes ONTAP, or click **Change Configuration** to select your own configuration.

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

15. **IAM Role**: It's best to keep the default option to let the Console 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 the Console updates the system to that version when creating the system. For example, the update occurs if you select Cloud Volumes ONTAP 9.13.1 and 9.13.1 P4 is available. The update does not occur from one release to another—for example, from 9.13 to 9.14.

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

    Note the following:

    ◦ The disk type is for the initial volume (and aggregate). You can choose a different disk type for subsequent volumes (and aggregates).

    ◦ If you choose a gp3 or io1 disk, the Console 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 the Console creates when you use the simple provisioning option. You can create aggregates that use a different disk size by using the advanced allocation option.

    ◦ You can choose a specific volume tiering policy when you create or edit a volume.

    ◦ If you disable data tiering, you can enable it on subsequent aggregates.

    Learn how data tiering works.

18. **Write Speed & WORM**:

    a. Choose **Normal** or **High** write speed, if desired.

       Learn more about write speed.

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

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

       Learn more about WORM storage.

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

19. **Create Volume**: Enter details for the new volume or click **Skip**.

    Learn about supported client protocols and versions.

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

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

Volume Details & Protection

Volume Name

ABDcv5689

Storage VM (SVM)

svm_c⬛⬛CVO1 ▼

Volume Size ⓘ

100

Unit

GiB ▼

Snapshot Policy

default ▼

default policy ⓘ

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

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

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

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

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

a. Review details about the configuration.

b. Click **More information** to review details about support and the AWS resources that the Console will purchase.

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

d. Click **Go**.

Result

The Console launches the Cloud Volumes ONTAP HA pair. You can track the progress on the **Audit** page.

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

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

After you finish

- If you provisioned a CIFS share, give users or groups permissions to the files and folders and verify that those users can access the share and create a file.

- If you want to apply quotas to volumes, use ONTAP System Manager or the ONTAP CLI.

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

> ⚠️ After the deployment process completes, do not modify the system-generated Cloud Volumes ONTAP configurations in the AWS cloud portal, especially the system tags. Any changes made to these configurations may lead to unexpected behavior or data loss.

Related links

- Planning your Cloud Volumes ONTAP configuration
- Deploy Cloud Volumes ONTAP in AWS using quick deployment

Deploy Cloud Volumes ONTAP in AWS Secret Cloud or AWS Top Secret Cloud

Similar to a standard AWS region, you can use the NetApp Console in AWS Secret Cloud and in AWS Top Secret Cloud to deploy Cloud Volumes ONTAP, which provides enterprise-class features for your cloud storage. AWS Secret Cloud and Top Secret Cloud are closed regions specific to the U.S. Intelligence Community; the instructions on this page only apply to AWS Secret Cloud and Top Secret Cloud region users.

Before you begin

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

- Review the following supported versions in AWS Secret Cloud and Top Secret Cloud:

  ◦ Cloud Volumes ONTAP 9.12.1 P2

  ◦ Version 3.9.32 of the Console agent

  The Console agent is required to deploy and manage Cloud Volumes ONTAP in AWS. You'll log in to the Console from the software that gets installed on the instance of the Console agent. The SaaS website for the Console isn't supported in AWS Secret Cloud and Top Secret Cloud.

- Learn about private mode

  In AWS Secret Cloud and Top Secret Cloud, the Console operates in *private mode*. In private mode, there is no connectivity to the SaaS layer from the Console. You can access the Console through a local a web-based application that can access the Console agent.

  To learn more about how private mode works, refer to the private deployment mode in the Console.

Step 1: Set up your networking

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

Steps

1. Choose the VPC and subnets in which you want to launch the instance of the Console agent and Cloud Volumes ONTAP instances.

2. Ensure that your VPC and subnets will support connectivity between the Console agent and Cloud Volumes ONTAP.

3. Set up a VPC endpoint to the Amazon Simple Storage Service (Amazon S3) service.

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

Step 2: Set up permissions

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

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

- The instance of the Console agent

- Cloud Volumes ONTAP instances

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

Steps

1. Go to the AWS IAM console and click **Policies**.

2. Create a policy for the instance of the Console agent.

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

Secret regions

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

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

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

Top Secret regions

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

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

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

```
    }
```

3. Create a policy for Cloud Volumes ONTAP.

Secret regions

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

Top Secret regions

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

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

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

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

Create the role:

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

Select the role:

You must select the Console agent IAM role when you launch the instance of the Console agent. You can select the IAM roles for Cloud Volumes ONTAP when you create a Cloud Volumes ONTAP system from the Console.
For HA pairs, you can select the IAM roles for Cloud Volumes ONTAP and the HA mediator when you create a Cloud Volumes ONTAP system.

Step 3: Set up the AWS KMS

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

Steps

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

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

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

   You need to provide the ARN to the Console when you create the Cloud Volumes ONTAP system.

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

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

Step 4: Install the Console agent and set up the Console

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

Steps

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

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

   You need to upload the certificate during the setup process. The Console uses the trusted certificate when sending requests to AWS over HTTPS.

2. Launch the instance of the Console agent:

   a. Go to the AWS Intelligence Community Marketplace page for the Console.

   b. On the Custom Launch tab, choose the option to launch the instance from the EC2 console.

   c. Follow the prompts to configure the instance.

      Note the following as you configure the instance:

      - We recommend t3.xlarge.
      - You must choose the IAM role that you created when you set up permissions.
      - You should keep the default storage options.
      - The required connection methods for the Console agent are as follows: SSH, HTTP, and HTTPS.

3. Set up the Console from a host that has a connection to the instance:

   a. Open a web browser and enter https://*ipaddress* where *ipaddress* is the IP address of the Linux host where you installed the Console agent.

   b. Specify a proxy server for connectivity to AWS services.

   c. Upload the certificate that you obtained in step 1.

   d. Follow the prompts to set up a new system.

      - **System Details**: Enter a name for the Console agent and your company name.
      - **Create Admin User**: Create the admin user for the system.

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

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

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

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

Step 5: (optional) Install a private mode certificate

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

Steps

1. List existing installed certificates.

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

    ```
    docker ps
    ```

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

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

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

    ```
    env
    ```

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

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

2. Add a certificate.

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

    ```
    docker ps
    ```

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

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

    Save the new certificate file inside.

    c. To collect the password from "TRUST_STORE_PASSWORD" environment variable, run the following

command:

```
env
```

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

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

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

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

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

```
exit
```

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

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

Step 6: Add a license to the Console

If you purchased a license from NetApp, you need to add it to the Console, so that you can select the license when you create a new Cloud Volumes ONTAP system. These licenses remain unassigned until you associate them with a new Cloud Volumes ONTAP system.

Steps

1. From the left navigation menu, select **Licenses and subscriptions**.
2. On the **Cloud Volumes ONTAP** panel, select **View**.
3. On the **Cloud Volumes ONTAP** tab, select **Licenses > Node Based Licenses**.
4. Click **Unassigned**.
5. Click **Add Unassigned Licenses**.
6. Enter the serial number of the license or upload the license file.
7. If you don't have the license file yet, you'll need to manually upload the license file from netapp.com.

   a. Go to the NetApp License File Generator and log in using your NetApp Support Site credentials.

   b. Enter your password, choose your product, enter the serial number, confirm that you have read and accepted the privacy policy, and then click **Submit**.

   c. Choose whether you want to receive the serialnumber.NLF JSON file through email or direct download.

8. Click **Add License**.

Result

The Console adds the license as unassigned until you associate it with a new Cloud Volumes ONTAP system. You can see the license on the left navigation menu under **Licenses and subscriptions > Cloud Volumes ONTAP > View > Licenses**.

Step 7: Launch Cloud Volumes ONTAP from the Console

You can launch Cloud Volumes ONTAP instances in AWS Secret Cloud and Top Secret Cloud by creating new systems in the Console.

Before you begin

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

Steps

1. On the **Systems** page, click **Add System**.

2. Under **Create**, select Cloud Volumes ONTAP.

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

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

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

Notes for deploying Cloud Volumes ONTAP HA in multiple Availability Zones

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

- You should configure a transit gateway when you deploy Cloud Volumes ONTAP HA in multiple Availability Zones (AZs). For instructions, refer to Set up an AWS transit gateway.

- Deploy the configuration as the following because only two AZs were available in the AWS Top Secret Cloud at the time of publication:

  - Node 1: Availability Zone A

  - Node 2: Availability Zone B

  - Mediator: Availability Zone A or B

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

Note the following as you complete the wizard:

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

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

- You must choose the IAM role that you created when preparing your AWS environment.

- The underlying AWS disk type is for the initial Cloud Volumes ONTAP volume.

You can choose a different disk type for subsequent volumes.

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

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

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

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

Result

The Cloud Volumes ONTAP instance is launched. You can track the progress in the **Audit** page.

Step 8: Install security certificates for data tiering

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

Before you begin

1. Create S3 buckets.

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

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

Steps

1. Copy the text from the root certificates that you installed in `step 4`.

2. Securely connect to the Cloud Volumes ONTAP system by using the CLI.

3. Install the root certificates. You might need to press the `ENTER` key multiple times:

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

4. When prompted, enter the entire copied text, including and from `----- BEGIN CERTIFICATE -----` to `----- END CERTIFICATE -----`.

5. Keep a copy of the CA-signed digital certificate for future reference.

6. Retain the CA name and certificate serial number.

7. Configure the object store for AWS Secret Cloud and Top Secret Cloud regions: `set -privilege advanced -confirmations off`

8. Run this command to configure the object store.

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

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

9. Verify that the object store was created successfully: `storage aggregate object-store show -instance`

10. Attach the object store to the aggregate. This should be repeated for every new aggregate: `storage aggregate object-store attach -aggregate <aggr1> -object-store-name <S3Bucket>`

Get started in Microsoft Azure

Learn about Cloud Volumes ONTAP deployment options in Azure

NetApp provides two options for deploying Cloud Volumes ONTAP on Azure. Cloud Volumes ONTAP traditionally relies on the NetApp Console for deployment and orchestration. Beginning with Cloud Volumes ONTAP 9.16.1, you can take advantage of Azure marketplace direct deployment, a streamlined process that provides access to a limited, but still powerful set of Cloud Volumes ONTAP features and options.

When you deploy Cloud Volumes ONTAP directly from the Azure marketplace, you're not required to set up the Console agent or meet other security and onboarding criteria required for deploying Cloud Volumes ONTAP through the Console. From the Azure marketplace, you can quickly deploy Cloud Volumes ONTAP in a few clicks and explore its core features and capabilities in your environment.

On completing the deployment in the Azure marketplace, you can discover these systems in the Console. After discovery, you can manage them as Cloud Volumes ONTAP systems and take advantage of all the Console capabilities. Refer to Discover the deployed systems in the Console.

Here is the feature comparison between the two options. Note that the features of a standalone instance deployed through the Azure marketplace change when it is discovered in the Console.

	Azure marketplace	NetApp Console
Onboarding	Shorter and easier, minimal preparation required for direct deployment	Longer onboarding process, including the installation of the Console agent
Supported virtual machine (VM) types	Eds_v5 and Ls_v3 instance types	Full range of VM types. Supported configurations in Azure
License	Free license	Any capacity-based license. Cloud Volumes ONTAP licensing

	Azure marketplace	NetApp Console
NetApp support	Not included	Available, based on the license type
Capacity	Up to 500 GiB	Expandable by configuration
Deployment model	High-availability (HA) mode deployment in single availability zone (AZ)	All supported configurations, including single node and HA modes, single and multiple AZ deployments
Supported disk type	Premium SSD v2 Managed Disks	Wider support. Default configuration for Cloud Volumes ONTAP
Write speed (fast write mode)	Not supported	Supported, based on your configuration. Learn about write speeds in Cloud Volumes ONTAP.
Orchestration capabilities	Not available	Available through NetApp Console, based on the license type
Number of supported storage VMs	One per deployment	Multiple storage VMs, based on your configuration. Supported number of storage VMs
Changing the instance type	Not supported	Supported
FabricPool tiering	Not supported	Supported

Related links

- Azure marketplace direct deployment: Deploy Cloud Volumes ONTAP from the Azure marketplace
- Deployment through the Console: Quick start for Cloud Volumes ONTAP in Azure
- NetApp Console documentation

Get started in NetApp Console

Quick start for Cloud Volumes ONTAP in Azure

Get started with Cloud Volumes ONTAP for Azure in a few steps.

1   **Create a Console agent**

If you don't have a Console agent yet, you need to create one. Learn how to create a Console agent 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 Console agent and access the NetApp Console that's running on that Console agent. Learn how to manually install the Console agent in a location without internet access

2   **Plan your configuration**

The Console 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.

For information, refer to Plan your Cloud Volumes ONTAP configuration in Azure.

③ Set up your networking

a. Ensure that your VNet and subnets will support connectivity between the Console agent 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

Click **Add System**, 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 Console agent from the Console
- Creating a Console agent from the Azure Marketplace
- Installing the Console agent software on a Linux host
- What the Console 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 these types of Azure Managed Disks:

- *Premium SSD Managed Disks* provide high performance for I/O-intensive workloads at a higher cost.
- *Premium SSD v2 Managed Disks* provide higher performance with lower latency at a lower cost, compared to Premium SSD Managed Disks.
- *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, refer to [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. The NetApp Console 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, the Console 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 Console agent also requires a system disk. View details about the Console agent'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.

Azure information	Your value
Region	
Virtual network (VNet)	
Subnet	
Network security group (if using your own)	

Choose a write speed

The Console 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 the Console, 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 Azure networking for Cloud Volumes ONTAP

The NetApp Console 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.

Requirements for Cloud Volumes ONTAP

The following networking requirements must be met in Azure.

Outbound internet access

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

The Console agent also contacts several endpoints for day-to-day operations. For information about endpoints, refer to View endpoints contacted from the Console agent and Prepare networking for using the Console.

Cloud Volumes ONTAP endpoints

Cloud Volumes ONTAP uses these endpoints to communicate with various services.

Endpoints	Applicable for	Purpose	Deployment modes	Impact if unavailable
https://netapp-cloud-account.auth0.com	Authentication	Used for authentication in the Console.	Standard and restricted modes.	User authentication fails and the following services remain unavailable: • Cloud Volumes ONTAP services • ONTAP services • Protocols and proxy services

Endpoints	Applicable for	Purpose	Deployment modes	Impact if unavailable
https://vault.azure.net	Key Vault	Used to retrieve client secret keys from the Azure Key Vault when using customer-managed keys (CMK).	Standard, restricted, and private modes.	Cloud Volumes ONTAP services are unavailable.
https://api.bluexp.netapp.com/tenancy	Tenancy	Used to retrieve the Cloud Volumes ONTAP resources from the Console to authorize resources and users.	Standard and restricted modes.	Cloud Volumes ONTAP resources and the users are not authorized.
https://mysupport.netapp.com/aods/asupmessage https://mysupport.netapp.com/asupprod/post/1.0/postAsup	AutoSupport	Used to send AutoSupport telemetry data to NetApp support.	Standard and restricted modes.	AutoSupport information remains undelivered.
https://management.azure.com https://login.microsoftonline.com https://bluexpinfraprod.eastus2.data.azurecr.io https://core.windows.net	Public regions	Communication with Azure services.	Standard, restricted, and private modes.	Cloud Volumes ONTAP cannot communicate with Azure service to perform specific operations for the Console in Azure.
https://management.chinacloudapi.cn https://login.chinacloudapi.cn https://blob.core.chinacloudapi.cn https://core.chinacloudapi.cn	China Region	Communication with Azure services.	Standard, restricted, and private modes.	Cloud Volumes ONTAP cannot communicate with Azure service to perform specific operations for the Console in Azure.
https://management.microsoftazure.de https://login.microsoftonline.de https://blob.core.cloudapi.de https://core.cloudapi.de	Germany Region	Communication with Azure services.	Standard, restricted, and private modes.	Cloud Volumes ONTAP cannot communicate with Azure service to perform specific operations for the Console in Azure.
https://management.usgovcloudapi.net https://login.microsoftonline.us https://blob.core.usgovcloudapi.net https://core.usgovcloudapi.net	Government regions	Communication with Azure services.	Standard, restricted, and private modes.	Cloud Volumes ONTAP cannot communicate with Azure service to perform specific operations for the Console in Azure.

Endpoints	Applicable for	Purpose	Deployment modes	Impact if unavailable
https://management.azure.microsoft.scloud https://login.microsoftonline.microsoft.scloud https://blob.core.microsoft.scloud https://core.microsoft.scloud	Government DoD regions	Communication with Azure services.	Standard, restricted, and private modes.	Cloud Volumes ONTAP cannot communicate with Azure service to perform specific operations for the Console in Azure.

Network proxy configuration of NetApp Console agent

You can use the proxy servers configuration of the NetApp Console agent to enable outbound internet access from Cloud Volumes ONTAP. The Console supports two types of proxies:

- **Explicit proxy**: The outbound traffic from Cloud Volumes ONTAP uses the HTTP address of the proxy server specified during the proxy configuration of the Console agent. The administrator might also have configured user credentials and root CA certificates for additional authentication. If a root CA certificate is available for the explicit proxy, make sure to obtain and upload the same certificate to your Cloud Volumes ONTAP system using the ONTAP CLI: security certificate install command.

- **Transparent proxy**: The network is configured to automatically route outbound traffic from Cloud Volumes ONTAP through the proxy for the Console agent. When setting up a transparent proxy, the administrator needs to provide only a root CA certificate for connectivity from Cloud Volumes ONTAP, not the HTTP address of the proxy server. Make sure that you obtain and upload the same root CA certificate to your Cloud Volumes ONTAP system using the ONTAP CLI: security certificate install command.

For information about configuring proxy servers, refer to the Configure the Console agent to use a proxy server.

IP addresses

The Console 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 allocated 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

The Console 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

  > ⓘ 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.

- SVM management (optional - not configured by default)

IP addresses for HA pairs

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

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

NIC0

- Node management IP
- Intercluster IP
- iSCSI IP

  > ⓘ 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, the Console 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—the Console 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 location of the Console agent in Azure.

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

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

Networking for Azure VNet encryption

Cloud Volumes ONTAP supports Azure Virtual Network (VNet) encryption for encrypting VM-to-VM traffic inside a VNet or across peered VNets. This feature is configured at the Azure VNet layer and is independent of Cloud Volumes ONTAP topology (single node or HA).

You only need to ensure that Accelerated Networking is enabled on the VM's NICs and review Azure VNet encryption requirements and limitations before enabling the feature. You should not modify NetApp managed load balancer objects.

Azure documentation: VNet encryption and Accelerated Networking.

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 the 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.

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

Security group rules

The Console creates Azure security groups that include the inbound and outbound rules for Cloud Volumes ONTAP to operate successfully. View security group rules for the Console agent.

The Azure security groups for Cloud Volumes ONTAP require the appropriate ports to be open for internal communication between the nodes. Learn about ONTAP internal ports.

We do not recommend modifying the predefined security groups or using custom security groups. However, if you must, note that the deployment process requires the Cloud Volumes ONTAP system to have full access within its own subnet. After the deployment is complete, if you decide to modify the network security group, ensure to keep the cluster ports and HA network ports open. This ensures seamless communication within the Cloud Volumes ONTAP cluster (any-to-any communication between the nodes).

Inbound rules for single-node systems

When you add a Cloud Volumes ONTAP system 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 Console agent resides. This is the recommended option.
- **All VNets**: The source for inbound traffic is the 0.0.0.0/0 IP range.
- **Disabled**: This option restricts the public network access to your storage account, and disables data tiering for Cloud Volumes ONTAP systems. This is a recommended option if your private IP addresses should not be exposed even within the same VNet due to security regulations and policies.

Priority and name	Port and protocol	Source and destination	Description
1000 inbound_ssh	22 TCP	Any to Any	SSH access to the IP address of the cluster management LIF or a node management LIF
1001 inbound_http	80 TCP	Any to Any	HTTP access to the ONTAP System Manager web console using the IP address of the cluster management LIF
1002 inbound_111_tcp	111 TCP	Any to Any	Remote procedure call for NFS
1003 inbound_111_udp	111 UDP	Any to Any	Remote procedure call for NFS
1004 inbound_139	139 TCP	Any to Any	NetBIOS service session for CIFS
1005 inbound_161-162 _tcp	161-162 TCP	Any to Any	Simple network management protocol
1006 inbound_161-162 _udp	161-162 UDP	Any to Any	Simple network management protocol
1007 inbound_443	443 TCP	Any to Any	Connectivity with the Console agent and HTTPS access to the ONTAP System Manager web console using the IP address of the cluster management LIF
1008 inbound_445	445 TCP	Any to Any	Microsoft SMB/CIFS over TCP with NetBIOS framing
1009 inbound_635_tcp	635 TCP	Any to Any	NFS mount

Priority and name	Port and protocol	Source and destination	Description
1010 inbound_635_udp	635 UDP	Any to Any	NFS mount
1011 inbound_749	749 TCP	Any to Any	Kerberos
1012 inbound_2049_tcp	2049 TCP	Any to Any	NFS server daemon
1013 inbound_2049_udp	2049 UDP	Any to Any	NFS server daemon
1014 inbound_3260	3260 TCP	Any to Any	iSCSI access through the iSCSI data LIF
1015 inbound_4045-4046_tcp	4045-4046 TCP	Any to Any	NFS lock daemon and network status monitor
1016 inbound_4045-4046_udp	4045-4046 UDP	Any to Any	NFS lock daemon and network status monitor
1017 inbound_10000	10000 TCP	Any to Any	Backup using NDMP
1018 inbound_11104-11105	11104-11105 TCP	Any to Any	SnapMirror data transfer
3000 inbound_deny _all_tcp	Any port TCP	Any to Any	Block all other TCP inbound traffic
3001 inbound_deny _all_udp	Any port UDP	Any to Any	Block all other UDP inbound traffic
65000 AllowVnetInBound	Any port Any protocol	VirtualNetwork to VirtualNetwork	Inbound traffic from within the VNet
65001 AllowAzureLoad BalancerInBound	Any port Any protocol	AzureLoadBalan cer to Any	Data traffic from the Azure Standard Load Balancer
65500 DenyAllInBound	Any port Any protocol	Any to Any	Block all other inbound traffic

Inbound rules for HA systems

When you add a Cloud Volumes ONTAP system 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 Console agent 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.

- **Disabled**: This option restricts the public network access to your storage account, and disables data tiering for Cloud Volumes ONTAP systems. This is a recommended option if your private IP addresses should not be exposed even within the same VNet due to security regulations and policies.

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

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.

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

Advanced outbound rules

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

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

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

Service	Port	Protocol	Source	Destination	Purpose
AutoSupport	HTTPS	443	Node management LIF	mysupport.netapp.com	AutoSupport (HTTPS is the default)
	HTTP	80	Node management LIF	mysupport.netapp.com	AutoSupport (only if the transport protocol is changed from HTTPS to HTTP)
	TCP	3128	Node management LIF	Console agent	Sending AutoSupport messages through a proxy server on the Console agent, if an outbound internet connection isn't available
Configuration backups	HTTP	80	Node management LIF	http://<console-agent-IP-address>/occm/offboxconfig	Send configuration backups to the Console agent. ONTAP documentation.
DHCP	68	UDP	Node management LIF	DHCP	DHCP client for first-time setup
DHCPS	67	UDP	Node management LIF	DHCP	DHCP server
DNS	53	UDP	Node management LIF and data LIF (NFS, CIFS)	DNS	DNS
NDMP	18600–18699	TCP	Node management LIF	Destination servers	NDMP copy
SMTP	25	TCP	Node management LIF	Mail server	SMTP alerts, can be used for AutoSupport
SNMP	161	TCP	Node management LIF	Monitor server	Monitoring by SNMP traps
	161	UDP	Node management LIF	Monitor server	Monitoring by SNMP traps
	162	TCP	Node management LIF	Monitor server	Monitoring by SNMP traps
	162	UDP	Node management LIF	Monitor server	Monitoring by SNMP traps
SnapMirror	11104	TCP	Intercluster LIF	ONTAP intercluster LIFs	Management of intercluster communication sessions for SnapMirror
	11105	TCP	Intercluster LIF	ONTAP intercluster LIFs	SnapMirror data transfer
Syslog	514	UDP	Node management LIF	Syslog server	Syslog forward messages

Requirements for the Console agent

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

- View networking requirements for the Console agent
- Security group rules in Azure

Related topics

- Verify AutoSupport setup for Cloud Volumes ONTAP
- Learn about ONTAP internal ports.

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 the NetApp Console, use the API to create a Cloud Volumes ONTAP system that uses the key.

How data is encrypted

The Console uses a disk encryption set, which enables management of encryption keys with managed disks not page blobs. Any new data disks also use the same disk encryption set. Lower versions will use Microsoft-managed key, instead of the customer-managed key.

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

Cloud Volumes ONTAP configuration	System disks used for key encryption	Data disks used for key encryption
Single node	• Boot • Core • NVRAM	• Root • Data
Azure HA single availability zone with page blobs	• Boot • Core • NVRAM	None

Cloud Volumes ONTAP configuration	System disks used for key encryption	Data disks used for key encryption
Azure HA single availability zone with shared managed disks	• Boot • Core • NVRAM	• Root • Data
Azure HA multiple availability zones with shared managed disks	• Boot • Core • NVRAM	• Root • Data

All Azure storage accounts for Cloud Volumes ONTAP are encrypted using a customer-managed key. If you want to encrypt your storage accounts during their creation, you must create and provide the ID of the resource in the Cloud Volumes ONTAP creation request. This applies for all type of deployments. If you do not provide it, the storage accounts still will be encrypted, but the Console first creates the storage accounts with Microsoft-managed key encryption and then updates the storage accounts to use the customer-managed key.

Key rotation in Cloud Volumes ONTAP

When you configure your encryption keys, you must use the Azure portal to set up and enable automatic key rotation. Creating and enabling a new version of encryption keys ensures that Cloud Volumes ONTAP can automatically detect and use the latest key version for encryption, ensuring your data remains secure without the need for manual intervention.

For information about configuring your keys and setting up key rotation, refer to the following Microsoft Azure documentation topics:

- Configure cryptographic key auto-rotation in Azure Key Vault
- Azure PowerShell - Enable customer-managed keys

> ⓘ After configuring the keys, ensure that you have selected *Enable auto rotation*, so that Cloud Volumes ONTAP can use the new keys when the previous keys expire. If you don't enable this option on the Azure portal, Cloud Volumes ONTAP can't automatically detect the new keys, which might cause issues with storage provisioning.

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 system. 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 subscription of the Console agent.

- **Resource group**: Use an existing resource group or create a new one.
- **Region**: Optionally, select the same region as the Console agent.
- **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, HA pairs in multiple zones, and HA single AZ deployments)

       > ⓘ Usage of Azure customer-managed encryption keys is contingent upon having Azure Disk encryption enabled for the key vault.

   - 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 system 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 API.

Required permissions

If you want to use a customer-managed key with a single node Cloud Volumes ONTAP system, ensure that the Console agent 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 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 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 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 system.

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 of the NetApp Console, select **Storage > Management**.

2. On the **Systems** page, click **Add System** and follow the steps.

    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 the Console, select **Freemium** when you reach the charging methods page.

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

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 or purchase options:

- A license (bring your own 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.

> (i) NetApp has restricted the purchase, extension, and renewal of BYOL licensing. For more information, refer to Restricted availability of BYOL licensing for Cloud Volumes ONTAP.

Steps

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

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

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

3. On the **Systems** page, click **Add System** and follow the steps.

   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 the Console, select a capacity-based package when you reach the charging methods page.

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

PAYGO subscription

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

When you create a Cloud Volumes ONTAP system, the Console prompts you to subscribe to the agreement that's available in the Azure Marketplace. That subscription is then associated with the system for charging.

You can use that same subscription for additional systems.

Steps

1. From the left navigation menu, select **Storage > Management**.

2. On the **Systems** page, click **Add System** and follow the steps.

    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 the Console, select a capacity-based package when you reach the charging methods page.

[View step-by-step instructions to launch Cloud Volumes ONTAP in Azure](#).

> 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 system creation.

2. On the **Systems** page, click **Add System** and follow the steps.

   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 the Console, select a capacity-based package when you reach the charging methods page.

[View step-by-step instructions to launch Cloud Volumes ONTAP in Azure](#).

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 user account in the Console with one or more Keystone Subscriptions.

3. After NetApp authorizes your account, link your subscriptions for use with Cloud Volumes ONTAP.

4. On the **Systems** page, click **Add System** and follow the steps.

   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 Azure.

Node-based license

A node-based license is the previous generation license for Cloud Volumes ONTAP. A node-based license could be procured from NetApp (BYOL) and is available for license renewals, only in specific cases. For information, refer to:

- End of availability for node-based licenses
- End of availability of node-based licenses
- Convert a node-based license to a capacity-based license

Enable high-availability mode for Cloud Volumes ONTAP in Azure

You should enable Microsoft Azure's high-availability (HA) mode to reduce unplanned failover times and to enable NFSv4 support for Cloud Volumes ONTAP. If you enable this mode, your Cloud Volumes ONTAP HA nodes can achieve a low (60 seconds) recovery time objective (RTO) during unplanned failovers on CIFS and NFSv4 clients.

Beginning with Cloud Volumes ONTAP 9.10.1, 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.

About this task

NetApp Console prompts you with these details 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 doesn't cause issues to other VMs.
- Cloud Volumes ONTAP uses an internal Azure Load Balancer during failovers of cluster and SVM management LIFs on CIFS and NFS clients.
- When the HA mode is enabled, the Console scans the system every 12 hours to update the internal Azure Load Balancer rules.

Steps

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

1. Access the Azure Cloud Shell from the Azure Portal

2. Register the high-availability mode feature:

```
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:

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

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

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

Related links

1. Microsoft Azure documentation: High availability ports overview
2. Microsoft Azure documentation: Get started with Azure CLI

Enable VMOrchestratorZonalMultiFD for Cloud Volumes ONTAP in Azure

For deploying VM instances in locally-redundant storage (LRS) single availability zones (AZ), you should activate the Microsoft `Microsoft.Compute/VMOrchestratorZonalMultiFD` feature for your subscriptions. In a high-availability (HA) mode, this feature facilitates deploying nodes in separate fault domains in the same availability zone.

Unless you activate this feature, zonal deployment doesn't occur, and the previous LRS non-zonal deployment becomes effective.

For information about VM deployment in single availability zone, refer to High-availability pairs in Azure.

Perform these steps as a user with "Owner" privileges:

Steps

1. Access Azure Cloud Shell from the Azure portal. For information, refer to the Microsoft Azure documentation: Get started with Azure Cloud Shell.

2. Register for the `Microsoft.Compute/VMOrchestratorZonalMultiFD` feature by running this command:

   ```
   az account set -s <Azure_subscription_name_or_ID>
   az feature register --name VMOrchestratorZonalMultiFD --namespace Microsoft.Compute
   ```

3. Verify the registration status and output sample:

```
az feature show -n VMOrchestratorZonalMultiFD --namespace Microsoft.Compute
{
"id": "/subscriptions/
<ID>/providers/Microsoft.Features/providers/Microsoft.Compute/features/VMOrchestratorZonalMultiF
D",
"name": "Microsoft.Compute/VMOrchestratorZonalMultiFD",
"properties": {
"state": "Registered"
},
"type": "Microsoft.Features/providers/features"
}
```

Launch Cloud Volumes ONTAP in Azure

You can launch a single-node system or an HA pair in Azure by creating a Cloud Volumes ONTAP system in NetApp Console.

Before you begin

You need the following before you begin.

- A Console agent that's up and running.

  - You should have a [Console agent that is associated with your system](#).

  - [You should be prepared to leave the Console agent running at all times](#).

- An understanding of the configuration that you want to use.

  You should have a configuration planned, and the necessary Azure networking details from your administrator. For more information, refer to [Planning your Cloud Volumes ONTAP configuration](#).

- An understanding of what's required to set up licensing for Cloud Volumes ONTAP.

  [Learn how to set up licensing](#).

About this task

When the Console 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 the Console 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.

Launch 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 system in the Console.

Steps

1. From the left navigation menu, select **Storage > Management**.

2. On the **Systems** page, click **Add System** and follow the prompts.

3. **Choose a Location**: Select **Microsoft Azure** and **Cloud Volumes ONTAP Single Node**.

4. If you're prompted, create a Console agent.

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:

Field	Description
System Name	The Console uses the system 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.
Resource Group Tags	Tags are metadata for your Azure resources. When you enter tags in this field, the Console 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 system, and then you can add more after it's created. Note that the API does not limit you to four tags when creating a system. For information about tags, refer to the Microsoft Azure Documentation: Using tags to organize your Azure resources.
User name and password	These are the credentials for the Cloud Volumes ONTAP cluster administrator account. You can use these credentials to connect to Cloud Volumes ONTAP through ONTAP System Manager or the ONTAP CLI. Keep the default *admin* user name or change it to a custom user name.
Edit Credentials	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.

6. **Services**: Enable or disable the individual services that you want to or don't want to use with Cloud Volumes ONTAP.

   - Learn more about NetApp Data Classification

   - Learn more about NetApp Backup and Recovery

   > 💡 If you would like to utilize WORM and data tiering, you must disable Backup and Recovery and deploy a Cloud Volumes ONTAP system 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 Console agent and the target location.

For China regions, single node deployments are supported only in Cloud Volumes ONTAP 9.12.1 GA and 9.13.0 GA. You can upgrade these versions to later patches and releases of Cloud Volumes ONTAP as supported in Azure. If you want to deploy later Cloud Volumes ONTAP versions in China regions, contact NetApp Support. Only licenses purchased directly from NetApp are supported in China regions, marketplace subscriptions are not available.

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:

Field	Description
Resource Group	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, the Console removes Cloud Volumes ONTAP resources from a resource group, in case of deployment failure or deletion.
Generated security group	If you let the Console 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 Console agent 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 if required, and select a virtual machine type.

(i) 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 9.16.1 P3 and 9.16.1 P4 is available. The update does not occur from one release to another—for example, from 9.15 to 9.16.

12. **Subscribe from the Azure Marketplace**: You see this page if the Console could not enable programmatic deployments of Cloud Volumes ONTAP. Follow the steps listed on the screen. refer to Programmatic deployment of Marketplace products for more information.

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:

    ◦ If the public access to your storage account is disabled within the VNet, you cannot enable data tiering in your Cloud Volumes ONTAP system. For information, refer to Security group rules.

    ◦ 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 the Console 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, refer to Sizing 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.

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, refer to 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:

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

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

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

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

   d. Click **Go**.

Result

The Console deploys the Cloud Volumes ONTAP system. You can track the progress on the Audit page.

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

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

> ⚠️ After the deployment process completes, do not modify the system-generated Cloud Volumes ONTAP configurations in the Azure portal, especially the system tags. Any changes made to these configurations may lead to unexpected behavior or data loss.

After you finish

- If you provisioned a CIFS share, give users or groups permissions to the files and folders and verify that those users can access the share and create a file.

- If you want to apply quotas to volumes, use ONTAP System Manager or the ONTAP CLI.

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

Launch 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 system in the Console.

Steps

1. From the left navigation menu, select **Storage > Management**.

2. On the **Systems** page, click **Add System** and follow the prompts.

3. If you're prompted, create a Console agent.

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:

Field	Description
System Name	The Console uses the system 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.

Field	Description
Resource Group Tags	Tags are metadata for your Azure resources. When you enter tags in this field, the Console 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 system, and then you can add more after it's created. Note that the API does not limit you to four tags when creating a system. For information about tags, refer to the Microsoft Azure Documentation: Using tags to organize your Azure resources.
User name and password	These are the credentials for the Cloud Volumes ONTAP cluster administrator account. You can use these credentials to connect to Cloud Volumes ONTAP through ONTAP System Manager or the ONTAP CLI. Keep the default *admin* user name or change it to a custom user name.
Edit Credentials	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.

5. **Services**: Enable or disable the individual services based on whether you want to use them with Cloud Volumes ONTAP.

   ◦ Learn more about NetApp Data Classification

   ◦ Learn more about NetApp Backup and Recovery

   > 💡 If you would like to utilize WORM and data tiering, you must disable Backup and Recovery and deploy a Cloud Volumes ONTAP system with version 9.8 or above.

6. **HA Deployment Models**:

   a. Select **Single Availability Zone** or **Multiple Availability Zone**.

      ▪ For single availability zones, select an Azure region, availability zone, VNet, and subnet.

        Beginning with Cloud Volumes ONTAP 9.15.1, you can deploy virtual machine (VM) instances in HA mode in single availability zones (AZs) in Azure. You need to select a zone and a region that support this deployment. If the zone or the region does not support zonal deployment, then the previous non-zonal deployment mode for LRS is followed. For understanding the supported configurations for shared managed disks, refer to HA single availability zone configuration with shared managed disks.

      ▪ For multiple availability zones, select a region, VNet, subnet, zone for node 1, and zone for node 2.

   b. 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:

Field	Description
Resource Group	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. The Console experiences connection issues if you try to deploy a second Cloud Volumes ONTAP HA pair in an Azure resource group. 💡 If the Azure account that you're using has the required permissions, the Console removes Cloud Volumes ONTAP resources from a resource group, in case of deployment failure or deletion.
Generated security group	If you let the Console 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 Console agent 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.

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 the Console updates the system to that version when creating it. For example, the update occurs if you select Cloud Volumes ONTAP 9.13.1 and 9.13.1 P4 is available. The update does not occur from one release to another— for example, from 9.13 to 9.14.

11. **Subscribe from the Azure Marketplace**: Follow the steps if the Console 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 the Console 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, refer to Size your system in Azure.

- If the public access to your storage account is disabled within the VNet, you cannot enable data tiering in your Cloud Volumes ONTAP system. For information, refer to Security group rules.

- 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.

- Starting with Cloud Volumes ONTAP 9.15.0P1, Azure page blobs are no longer supported for new high-availability pair deployments. If you currently use Azure page blobs in existing high-availability pair deployments, you can migrate to newer VM instance types in the Edsv4-series VMs and Edsv5-series VMs.

  Learn more about supported configurations in Azure.

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, refer to 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 system.

   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:

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

Volume Details & Protection

| Volume Name | | | Storage VM (SVM) |
| ABDcv5689 | | | svm_c████CVO1 ▾ |

Volume Size	Unit		Snapshot Policy
100	GiB ▾		default ▾
			default policy ⓘ

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

Field	Description
DNS Primary and Secondary IP Address	The IP addresses of the DNS servers that provide name resolution for the CIFS server. The listed DNS servers must contain the service location records (SRV) needed to locate the Active Directory LDAP servers and domain controllers for the domain that the CIFS server will join.
Active Directory Domain to join	The FQDN of the Active Directory (AD) domain that you want the CIFS server to join.
Credentials authorized to join the domain	The name and password of a Windows account with sufficient privileges to add computers to the specified Organizational Unit (OU) within the AD domain.
CIFS server NetBIOS name	A CIFS server name that is unique in the AD domain.
Organizational Unit	The organizational unit within the AD domain to associate with the CIFS server. The default is CN=Computers. 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. Refer to the NetApp Console 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, refer to Choose a volume usage profile, Data tiering overview, and KB: What Inline Storage Efficiency features are supported with CVO?

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 the Console will purchase.

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

   d. Click **Go**.

Result

The Console deploys the Cloud Volumes ONTAP system. You can track the progress on the Audit page.

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

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

After you finish

- If you provisioned a CIFS share, give users or groups permissions to the files and folders and verify that those users can access the share and create a file.

- If you want to apply quotas to volumes, use ONTAP System Manager or the ONTAP CLI.

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

> ⚠️ After the deployment process completes, do not modify the system-generated Cloud Volumes ONTAP configurations in the Azure portal, especially the system tags. Any changes made to these configurations may lead to unexpected behavior or data loss.

Related links

*Planning your Cloud Volumes ONTAP configuration in Azure
*Deploy Cloud Volumes ONTAP in Azure from the Azure Marketplace

Verify Azure platform image

Azure marketplace image verification for Cloud Volumes ONTAP

Azure image verification complies with enhanced NetApp security requirements. Verifying an image file is a straightforward process. However, the Azure image signature verification requires specific considerations for the Azure VHD image file because it is altered in the Azure marketplace.

> ℹ️ Azure image verification is supported on Cloud Volumes ONTAP 9.15.0 and later.

Azure's alteration of published VHD files

The 1 MB (1048576 bytes) at the beginning and 512 bytes at the end of the VHD file is modified by Azure. NetApp signs the remaining VHD file.

In the example, the VHD file is of 10GB. The portion that NetApp signed is marked in green (10 GB - 1 MB - 512 bytes).

Related links

- [Page Fault Blog: How to sign and verify using OpenSSL](#)
- [Use Azure Marketplace image to create VM image for your Azure Stack Edge Pro GPU | Microsoft Learn](#)
- [Export/Copy a managed disk to a storage account using the Azure CLI | Microsoft Learn](#)
- [Azure Cloud Shell Quickstart - Bash | Microsoft Learn](#)
- [How to install the Azure CLI | Microsoft Learn](#)
- [az storage blob copy | Microsoft Learn](#)
- [Sign in with Azure CLI — Login and Authentication | Microsoft Learn](#)

Download the Azure image file for Cloud Volumes ONTAP

You can download the Azure image file from the [NetApp Support Site](#).

The *tar.gz* file contains the files required for image signature verification. Along with the *tar.gz* file, you should also download the *checksum* file for the image. The checksum file contains the `md5` and `sha256` checksums of the *tar.gz* file.

Steps

1. Go to the [Cloud Volumes ONTAP product page on the NetApp Support Site](#) and download the required software version from the **Downloads** section.

2. On the Cloud Volumes ONTAP download page, click the downloadable file for the Azure image and download the *tar.gz* file.

3. On Linux, run `md5sum AZURE-<version>_PKG.TAR.GZ`.

   On macOS, run `sha256sum AZURE-<version>_PKG.TAR.GZ`.

4. Verify that the `md5sum` and `sha256sum` values match those in the downloaded Azure image.

5. On Linux and macOS, extract the *tar.gz* file using the `tar -xzf` command.

   The extracted *tar.gz* file contains the digest (*.sig*) file, public key certificate (*.pem*) file, and chain certificate (*.pem*) file.

   Example output after extracting the tar.gz file:

```
$ ls cert/ -l
-rw-r----- 1 netapp netapp  384 May  13 13:00 9.15.0P1_azure_digest.sig
-rw-r----- 1 netapp netapp 2365 May  13 13:00 Certificate-
9.15.0P1_azure.pem
-rw-r----- 1 netapp netapp 8537 May  13 13:00 Certificate-Chain-
9.15.0P1_azure.pem
-rw-r----- 1 netapp netapp 8537 May  13 13:00 version_readme
```

Export VHD images for Cloud Volumes ONTAP from the Azure marketplace

Once the VHD image is published to Azure cloud, it is no longer managed by NetApp. Instead, the published image is placed on the Azure marketplace. When the image is staged and published on the Azure marketplace, Azure modifies 1 MB at the beginning and 512 bytes at the end of the VHD. To verify the signature of the VHD file, you need to export the VHD image modified by Azure from the Azure marketplace.

Before you begin

Ensure that the Azure CLI is installed on your system, or the Azure Cloud Shell is available through the Azure portal. For more information about how to install the Azure CLI, refer to the Microsoft documentation: How to install the Azure CLI.

Steps

1. Map the Cloud Volumes ONTAP version on your system to the Azure marketplace image version using the contents of the *version_readme* file. The Cloud Volumes ONTAP version is represented by `buildname` and the Azure marketplace image version is represented by `version` in the version mappings.

   In the following example, the Cloud Volumes ONTAP version `9.15.0P1` is mapped to the Azure marketplace image version `9150.01000024.05090105`. This Azure marketplace image version is later used to set the image URN.

```
[
  "buildname": "9.15.0P1",
    "publisher": "netapp",
      "version": "9150.01000024.05090105"


]
```

2. Identify the region where you want to create the VMs. The region name is used as the value for the `locName` variable when setting the URN of the marketplace image. To list the available regions, run this command:

```
az account list-locations -o table
```

In this table, the region name appears in the `Name` field.

```
$ az account list-locations -o table
DisplayName                      Name                    RegionalDisplayName
-----------------------  -------------------
------------------------------------
East US                          eastus                  (US) East US
East US 2                        eastus2                 (US) East US 2
South Central US                 southcentralus          (US) South Central US
...
```

3. Review the SKU names for the corresponding Cloud Volumes ONTAP versions and VM deployment types in the table below. The SKU name is used as the value for the `skuName` variable when setting the URN of the marketplace image.

   For example, all single node deployments with Cloud Volumes ONTAP 9.15.0 should use `ontap_cloud_byol` as the SKU name.

Cloud Volumes ONTAP version	VM deployment through	SKU name
9.17.1 and later	The Azure marketplace	ontap_cloud_direct_gen2
9.17.1 and later	The NetApp Console	ontap_cloud_gen2
9.16.1	The Azure marketplace	ontap_cloud_direct
9.16.1	The Console	ontap_cloud
9.15.1	The Console	ontap_cloud
9.15.0	The Console, single node deployments	ontap_cloud_byol
9.15.0	The Console, high availability (HA) deployments	ontap_cloud_byol_ha

4. After mapping the ONTAP version and Azure marketplace image, export the VHD file from the Azure marketplace using the Azure Cloud Shell or Azure CLI.

Export VHD file using the Azure Cloud Shell on Linux

From the Azure Cloud Shell, export the marketplace image to the VHD file (for example, *9150.01000024.05090105.vhd*), and download it to your local Linux system. Perform these steps to get the VHD image from the Azure marketplace.

Steps

1. Set the URN and other parameters of the marketplace image. The URN format is `<publisher>:<offer>:<sku>:<version>`. Optionally, you can list NetApp marketplace images to confirm the correct image version.

```
PS /home/user1> $urn="netapp:netapp-ontap-
cloud:ontap_cloud_byol:9150.01000024.05090105"
PS /home/user1> $locName="eastus2"
PS /home/user1> $pubName="netapp"
PS /home/user1> $offerName="netapp-ontap-cloud"
PS /home/user1> $skuName="ontap_cloud_byol"
PS /home/user1> Get-AzVMImage -Location $locName -PublisherName $pubName
-Offer $offerName -Sku $skuName |select version
...
141.20231128
9.141.20240131
9.150.20240213
9150.01000024.05090105
...
```

2. Create a new managed disk from the marketplace image with the matching image version:

```
PS /home/user1> $diskName = "9150.01000024.05090105-managed-disk"
PS /home/user1> $diskRG = "fnf1"
PS /home/user1> az disk create -g $diskRG -n $diskName --image-reference
$urn
PS /home/user1> $sas = az disk grant-access --duration-in-seconds 3600
--access-level Read --name $diskName --resource-group $diskRG
PS /home/user1> $diskAccessSAS = ($sas | ConvertFrom-Json)[0].accessSas
```

3. Export the VHD file from the managed disk to Azure Storage. Create a container with the appropriate access level. In this example, we've used a container named `vm-images` with `Container` access level. Get the storage account access key from the Azure portal: **Storage Accounts > *examplesaname* > Access Key > *key1 > key* > Show > *<copy>***

```
PS /home/user1> $storageAccountName = "examplesaname"
PS /home/user1> $containerName = "vm-images"
PS /home/user1> $storageAccountKey = "<replace with the above access
key>"
PS /home/user1> $destBlobName = "9150.01000024.05090105.vhd"
PS /home/user1> $destContext = New-AzureStorageContext
-StorageAccountName $storageAccountName -StorageAccountKey
$storageAccountKey
PS /home/user1> Start-AzureStorageBlobCopy -AbsoluteUri $diskAccessSAS
-DestContainer $containerName -DestContext $destContext -DestBlob
$destBlobName
PS /home/user1> Get-AzureStorageBlobCopyState -Container $containerName
-Context $destContext -Blob $destBlobName
```

4. Download the generated image to your Linux system. Use the `wget` command to download the VHD file:

```
wget <URL of filename/Containers/vm-images/9150.01000024.05090105.vhd>
```

The URL follows a standard format. For automation, you can derive the URL string as shown below.
Alternatively, you can use the Azure CLI `az` command to get the URL.
Example URL:
https://examplesaname.bluexpinfraprod.eastus2.data.azurecr.io/vm-images/9150.01000024.05090105.vhd

5. Clean up the managed disk

```
PS /home/user1> Revoke-AzDiskAccess -ResourceGroupName $diskRG -DiskName
$diskName
PS /home/user1> Remove-AzDisk -ResourceGroupName $diskRG -DiskName
$diskName
```

Export VHD file using the Azure CLI on Linux

Export the marketplace image to a VHD file using the Azure CLI from a local Linux system.

Steps

1. Log in to the Azure CLI and list marketplace images:

```
% az login --use-device-code
```

2. To sign in, use a web browser to open the page https://microsoft.com/devicelogin and enter the authentication code.

```
% az vm image list --all --publisher netapp --offer netapp-ontap-cloud
--sku ontap_cloud_byol
...
{
"architecture": "x64",
"offer": "netapp-ontap-cloud",
"publisher": "netapp",
"sku": "ontap_cloud_byol",
"urn": "netapp:netapp-ontap-
cloud:ontap_cloud_byol:9150.01000024.05090105",
"version": "9150.01000024.05090105"
},
...
```

3. Create a new managed disk from the marketplace image with the matching image version.

```
% export urn="netapp:netapp-ontap-
cloud:ontap_cloud_byol:9150.01000024.05090105"
% export diskName="9150.01000024.05090105-managed-disk"
% export diskRG="new_rg_your_rg"
% az disk create -g $diskRG -n $diskName --image-reference $urn
% az disk grant-access --duration-in-seconds 3600 --access-level Read
--name $diskName --resource-group $diskRG
{
  "accessSas": "https://md-
xxxxxx.bluexpinfraprod.eastus2.data.azurecr.io/xxxxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxx&sigxxxxxxxxxxxxxxxxxxxxxxxxx"
}
% export diskAccessSAS="https://md-
xxxxxx.bluexpinfraprod.eastus2.data.azurecr.io/xxxxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxxx-xxxx-xx-xx-xx&sigxxxxxxxxxxxxxxxxxxxxxxxxx"
```

To automate the process, the SAS needs to be extracted from the standard output. Refer to the appropriate documents for guidance.

4. Export the VHD file from the managed disk.

   a. Create a container with the appropriate access level. In this example, a container named `vm-images` with `Container` access level is used.

   b. Get the storage account access key from the Azure portal: **Storage Accounts > *examplesaname* > Access Key > *key1* > *key* > Show > *<copy>***

   You can also use the `az` command for this step.

```
% export storageAccountName="examplesaname"
% export containerName="vm-images"
% export storageAccountKey="xxxxxxxxxx"
% export destBlobName="9150.01000024.05090105.vhd"

% az storage blob copy start --source-uri $diskAccessSAS
--destination-container $containerName --account-name
$storageAccountName --account-key $storageAccountKey --destination
-blob $destBlobName

{
  "client_request_id": "xxxx-xxxx-xxxx-xxxx-xxxx",
  "copy_id": "xxxx-xxxx-xxxx-xxxx-xxxx",
  "copy_status": "pending",
  "date": "2022-11-02T22:02:38+00:00",
  "etag": "\"0xXXXXXXXXXXXXXXXX\"",
  "last_modified": "2022-11-02T22:02:39+00:00",
  "request_id": "xxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxx",
  "version": "2020-06-12",
  "version_id": null
}
```

5. Check the status of the blob copy.

```
% az storage blob show --name $destBlobName --container-name
$containerName --account-name $storageAccountName

....
    "copy": {
      "completionTime": null,
      "destinationSnapshot": null,
      "id": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxx",
      "incrementalCopy": null,
      "progress": "10737418752/10737418752",
      "source": "https://md-
xxxxxx.bluexpinfraprod.eastus2.data.azurecr.io/xxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
      "status": "success",
      "statusDescription": null
    },
....
```

6. Download the generated image to your Linux server.

```
wget <URL of file examplesaname/Containers/vm-
images/9150.01000024.05090105.vhd>
```

The URL follows a standard format. For automation, you can derive the URL string as shown below.
Alternatively, you can use the Azure CLI `az` command to get the URL.
Example URL:
https://examplesaname.bluexpinfraprod.eastus2.data.azurecr.io/vm-images/9150.01000024.05090105.vhd

7. Clean up the managed disk

```
az disk revoke-access --name $diskName --resource-group $diskRG
az disk delete --name $diskName --resource-group $diskRG --yes
```

Verify file signature

Azure marketplace image signature verfication for Cloud Volumes ONTAP

The Azure image verification process generates a digest file from the VHD file by
stripping 1 MB at the beginning and 512 bytes at the end, then applying a hash function.
To match the signing procedure, *sha256* is used for hashing.

File signature verification workflow summary

The following is an overview of the file signature verification workflow process.
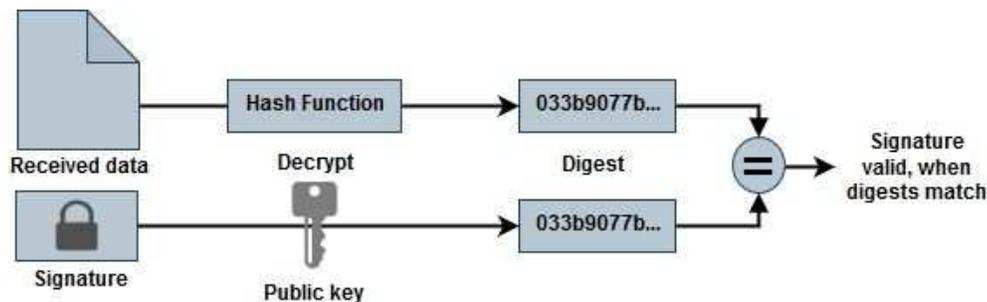
- Downloading the Azure image from the NetApp Support Site and extracting the digest (.sig) file, public key
  certificate (.pem) file, and chain certificate (.pem) file. Refer to Download the Azure image digest file for
  more information.

- Verification of the chain of trust.

- Extracting the public key (.pub) from the public key certificate (.pem).

- Decrypting the digest file by using the extracted public key.

- Comparing the result against a newly generated digest of a temporary file created from the image file after
  removing 1 MB at the beginning and 512 bytes at the end. This step is performed by using the OpenSSL
  command line tool. The OpenSSL CLI tool displays appropriate messaging on success or failure in
  matching the files.

```
openssl dgst -verify <public_key> -keyform <form> <hash_function>
-signature <digest_file> -binary <temporary_file>
```

Verify Azure marketplace image signature for Cloud Volumes ONTAP on Linux

Verification of an exported VHD file signature on Linux includes validating the chain of trust, editing the file, and verifying the signature.

Steps

1. Download the Azure image file from the NetApp Support Site and extract the digest (.sig) file, public key certificate (.pem) file, and chain certificate (.pem) file.

   Refer to Download the Azure image digest file for more information.

2. Verify the chain of trust.

   ```
   % openssl verify -CAfile Certificate-Chain-9.15.0P1_azure.pem
   Certificate-9.15.0P1_azure.pem
   Certificate-9.15.0P1_azure.pem: OK
   ```

3. Remove 1 MB (1,048,576 bytes) at the beginning and 512 bytes at the end of the VHD file. When using `tail`, the `-c +K` option generates bytes from the Kth byte of the file. Therefore, it passes 1048577 to `tail -c`.

   ```
   % tail -c +1048577 ./9150.01000024.05090105.vhd > ./sign.tmp.tail
   % head -c -512 ./sign.tmp.tail > sign.tmp
   % rm ./sign.tmp.tail
   ```

4. Use OpenSSL to extract the public key from the certificate and verify the stripped file (sign.tmp) with the signature file and the public key.

   The command prompt displays messages indicating success or failure based on the verification.

   ```
   % openssl x509 -pubkey -noout -in ./Certificate-9.15.0P1_azure.pem >
   ./Code-Sign-Cert-Public-key.pub

   % openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
   -sha256 -signature digest.sig -binary ./sign.tmp
   Verification OK

   % openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
   -sha256 -signature digest.sig -binary ./another_file_from_nowhere.tmp
   Verification Failure
   ```

5. Clean up the workspace.

```
% rm ./9150.01000024.05090105.vhd ./sign.tmp
% rm *.sig *.pub *.pem
```

Verify Azure marketplace image signature for Cloud Volumes ONTAP on macOS

Verification of an exported VHD file signature on Linux includes validating the chain of trust, editing the file, and verifying the signature.

Steps

1. Download the Azure image file from the NetApp Support Site and extract the digest (.sig) file, public key certificate (.pem) file, and chain certificate (.pem) file.

   Refer to Download the Azure image digest file for more information.

2. Verify the chain of trust.

```
% openssl verify -CAfile Certificate-Chain-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem: OK
```

3. Remove 1MB (1,048,576 bytes) at the beginning and 512 bytes at the end of the VHD file. When using `tail`, the `-c +K` option generates bytes from the Kth byte of the file. Therefore, it passes 1048577 to `tail -c`. Note that on macOS, the tail command might take about ten minutes to complete.

```
% tail -c +1048577 ./9150.01000024.05090105.vhd > ./sign.tmp.tail
% head -c -512 ./sign.tmp.tail > sign.tmp
% rm ./sign.tmp.tail
```

4. Use OpenSSL to extract the public key from the certificate and verify the stripped file (sign.tmp) with the signature file and public key. The command prompt displays messages indicating success or failure based on the verification.

```
% openssl x509 -pubkey -noout -in ./Certificate-9.15.0P1_azure.pem >
./Code-Sign-Cert-Public-key.pub

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./sign.tmp
Verified OK

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./another_file_from_nowhere.tmp
Verification Failure
```

5. Clean up the workspace.

```
% rm ./9150.01000024.05090105.vhd ./sign.tmp
% rm *.sig *.pub *.pem
```

Deploy Cloud Volumes ONTAP from the Azure marketplace

You can use Azure marketplace direct deployment to quickly and easily deploy Cloud Volumes ONTAP. From the Azure marketplace, you can quickly deploy Cloud Volumes ONTAP in a few clicks and explore its core features and capabilities in your environment.

For more information about this offering, refer to Learn about Cloud Volumes ONTAP offerings in the NetApp Console and the marketplace.

About this task

The Cloud Volumes ONTAP system deployed by using Azure marketplace direct deployment has these properties. Note that the features of a standalone instance deployed through the Azure marketplace change when it is discovered in the NetApp Console.

- The latest Cloud Volumes ONTAP version (9.16.1 or later).

- A free license for Cloud Volumes ONTAP that is limited to 500 GiB of provisioned capacity. This license includes no NetApp support and has no expiry date.

- Two nodes configured in a high availability (HA) mode in a single availability zone (AZ), provisioned with default serial numbers. The storage virtual machines (storage VMs) are deployed in a flexible orchestration mode.

- An aggregate for the instance created by default.

- A Premium SSD v2 Managed Disk of 500 GiB provisioned capacity, and a root and a data disk.

- One data storage VM deployed, with NFS, CIFS, iSCSI, and NVMe/TCP data-services. You cannot add any additional data storage VMs.

- Licenses installed for NFS, CIFS (SMB), iSCSI, Autonomous Ransomware Protection (ARP), SnapLock, and SnapMirror.

- ONTAP temperature-sensitive storage efficiency (TSSE), volume encryption, and external key-management enabled by default.

- These features are not supported:
  - FabricPool tiering
  - Changing the storage VM type
  - Fast write mode

Before you begin
- Ensure that you have a valid Azure marketplace subscription.

- Ensure you meet the networking requirements for an HA deployment in a single AZ in Azure. Refer to Set up Azure networking for Cloud Volumes ONTAP.

- You need to be assigned one of these Azure roles to deploy Cloud Volumes ONTAP:
  - The `contributor` role with the default permissions. For more information, refer to the Microsoft Azure

documentation: Azure built-in roles.

- A custom RBAC role with the following permissions. For more information, refer to the Azure documentation: Azure custom roles.

```
"permissions": [
{
"actions": [
"Microsoft.AAD/register/action",
"Microsoft.Resources/subscriptions/resourceGroups/write",
"Microsoft.Network/loadBalancers/write",
"Microsoft.ClassicCompute/virtualMachines/write",
"Microsoft.Compute/capacityReservationGroups/deploy/action",
"Microsoft.ClassicCompute/virtualMachines/networkInterfaces/associatedNetworkSecurityGroups/
write",
"Microsoft.Network/networkInterfaces/write",
"Microsoft.Compute/virtualMachines/write",
"Microsoft.Compute/virtualMachines/extensions/write",
"Microsoft.Resources/deployments/validate/action",
"Microsoft.Resources/subscriptions/resourceGroups/read",
"Microsoft.Network/virtualNetworks/write",
"Microsoft.Network/virtualNetworks/read",
"Microsoft.Network/networkSecurityGroups/write",
"Microsoft.Network/networkSecurityGroups/read",
"Microsoft.Compute/disks/write",
"Microsoft.Compute/virtualMachineScaleSets/write",
"Microsoft.Resources/deployments/write",
"Microsoft.Network/virtualNetworks/subnets/read",
"Microsoft.Network/virtualNetworks/subnets/write"
],
"notActions": [],
"dataActions": [],
"notDataActions": []
}
]
```

> ⓘ If you have registered the resource provider "Microsoft.storage" to your subscription, then you don't need the `Microsoft.AAD/register/action` permission. For more information, refer to the Azure documentation: Azure permissions for Storage.

Steps

1. From the Azure marketplace site, search for NetApp products.

2. Select **NetApp Cloud Volumes ONTAP direct**.

3. Click **Create** to launch the deployment wizard.

4. Select a plan. The **Plan** list typically displays the latest releases of Cloud Volumes ONTAP.

5. In the **Basics** tab, provide these details:

   - **Subscription**: Select a subscription. The deployment will be linked to the subscription number.

   - **Resource group**: Use an existing resource group or create a new one. Resource groups help in allocating all resources, such as disks and storage VMs, within a single group for a Cloud Volumes

ONTAP system.

- ◦ **Region**: Select a region that supports Azure HA deployment in a single AZ. You see only the available regions on the list.

- ◦ **Size**: Select an storage VM size for the supported Premium SSD v2 Managed Disk.

- ◦ **Zone**: Select a zone for the region you selected.

- ◦ **Admin Password**: Set a password. You use this admin password to log in to the system after the deployment.

- ◦ **Confirm Password**: Re-enter the same password for confirmation.

  - ▪ In the **Network** tab, add a virtual network and a subnet, or select them from the lists.

    > (i) To comply with Microsoft Azure restrictions, you should create a new subnet when setting up a new virtual network. Likewise, if you choose an existing network, you should select an existing subnet.

  - ▪ To select a predefined network security group, select **Yes**. Select **No** to assign a predefined Azure network security group with the necessary traffic rules. For more information, refer to Security group rules for Azure.

  - ▪ In the **Advanced** tab confirm whether the two Azure features necessary for this deployment have been set. Refer to Enable an Azure feature for Cloud Volumes ONTAP single AZ deployments and Enable high-availability mode for Cloud Volumes ONTAP in Azure.

  - ▪ You can define name and value pairs for the resources or resource groups in the **Tags** tab.

  - ▪ In the **Review + create** tab, review the details and start the deployment.

After you finish

Select the notification icon to view the progress of your deployment. After Cloud Volumes ONTAP is deployed, you can view the storage VM listed for operations.

Once accessible, use ONTAP System Manager or the ONTAP CLI to log in to the storage VM with the admin credentials that you set. Thereafter, you can create volumes, LUNs, or shares and start utilizing the storage capabilities of Cloud Volumes ONTAP.

Troubleshoot deployment issues

Cloud Volumes ONTAP systems deployed directly through the Azure marketplace do not include support from NetApp. If any issues arise during deployment, you can independently troubleshoot and resolve them.

Steps

1. On the Azure marketplace site, go to **Boot diagnostics > Serial log**.

2. Download and investigate the serial logs.

3. Consult the product documentation and knowledge base (KB) articles for troubleshooting.

   - ◦ Azure marketplace documentation
   - ◦ NetApp documentation
   - ◦ NetApp KB articles

Discover the deployed systems in Console

You can discover the Cloud Volumes ONTAP systems that you deployed using Azure marketplace direct

deployment and manage them on the **Systems** page in the Console. The Console agent discovers the systems, adds them and applies the necessary licenses, and unlocks the full capabilities of the Console for these systems. The original HA configuration in a single AZ with PSSD v2 Managed Disks is retained, and the system is registered to the same Azure subscription and resource group as the original deployment.

About this task

On discovering the Cloud Volumes ONTAP systems deployed using Azure marketplace direct deployment, the Console agent performs these tasks:

- Replaces the free licenses of the discovered systems as regular capacity-based Freemium licenses.
- Retains the existing capabilities of the deployed systems, and adds the additional capabilities of the Console, such as data protection, data management, and security features.
- Replaces the installed licenses on the nodes with new ONTAP licenses for NFS, CIFS (SMB), iSCSI, ARP, SnapLock, and SnapMirror.
- Converts the generic node serial numbers to unique serial numbers.
- Assigns new system tags on the resources as required.
- Converts the dynamic IP addresses of the instance to static IP addresses.
- Enables the functionalities of FabricPool tiering, AutoSupport, and write-once-read-many (WORM) storage on the deployed systems. You can activate these features from the Console when you need them.
- Registers the instances to the NSS accounts used to discover them.
- Enables capacity management features in automatic and manual modes for the discovered systems.

Before you begin

Ensure that the deployment is complete on the Azure marketplace. The Console agent can discover the systems only when the deployment is complete and are available for discovery.

Steps

In the Console, you follow the standard procedure for discovering existing systems. Refer to Add an existing Cloud Volumes ONTAP system to the Console.

> ⚠ During discovery, you might see failure messages, but you can ignore them until the discovery process is complete. Do not modify the system-generated Cloud Volumes ONTAP configurations in the Azure marketplace portal during discovery, especially the system tags. Any changes made to these configurations may lead to unexpected system behavior.

After you finish

After the discovery is complete, you can view the systems listed on the **Systems** page in the Console. You can perform various management tasks, such as expanding the aggregate, adding volumes, provisioning additional storage VMs, and changing the instance types.

Related links

Refer to the ONTAP documentation for more information about creating storage:

- Create volumes for NFS
- Create LUNs for iSCSI
- Create shares for CIFS

Get started in Google Cloud

Quick start for Cloud Volumes ONTAP in Google Cloud

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

(1) Create a Console agent

If you don't have a Console agent yet, you need to create one. Learn how to create a Console agent 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 Console agent and access the NetApp Console that's running on that Console agent. Learn how to manually install the Console agent in a location without internet access

(2) Plan your configuration

The Console 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 Console agent 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 Console agent 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 NetApp 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 Google Cloud APIs in your project. These APIs, which you might have already enabled as part of creating the Console agent, are required to deploy Cloud Volumes ONTAP in Google Cloud.

6   **Launch Cloud Volumes ONTAP using the Console**

Click **Add System**, 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 Console agent
- Installing the Console agent software on a Linux host
- Google Cloud permissions for the Console agent

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 Google Cloud

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 Google Cloud

Size your system in Google Cloud

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

Disk types

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, refer to the Google Cloud documentation: Zonal Persistent disks (Standard and SSD).

Disk size

You need to choose an initial disk size when you deploy a Cloud Volumes ONTAP system. After that you can let the NetApp Console 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)
  - Google Cloud documentation: Optimizing Persistent Disk and Local SSD Performance

View default system disks

In addition to the storage for user data, the Console 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: Cloud Quotas overview

  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 Console agent also requires a system disk. View details about the Console agent's default configuration.

Collect networking information

When you deploy Cloud Volumes ONTAP in Google Cloud, 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

Google Cloud information	Your value
Region	
Zone	
VPC network	
Subnet	
Firewall policy (if using your own)	

Network information for an HA pair in multiple zones

Google Cloud information	Your value
Region	
Zone for Node 1	
Zone for Node 2	
Zone for the mediator	
VPC-0 and subnet	
VPC-1 and subnet	
VPC-2 and subnet	
VPC-3 and subnet	
Firewall policy (if using your own)	

Network information for an HA pair in a single zone

Google Cloud information	Your value
Region	
Zone	
VPC-0 and subnet	
VPC-1 and subnet	
VPC-2 and subnet	
VPC-3 and subnet	

Google Cloud information	Your value
Firewall policy (if using your own)	

Choose a write speed

The Console 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 the Console, 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 Google Cloud networking for Cloud Volumes ONTAP

The NetApp Console 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.

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

For a single-node system in Google Cloud, the Console allocates private IP addresses to the following:

- Node
- Cluster
- Storage VM
- Data NAS LIF
- Data iSCSI 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:

```
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. The Console prompts 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.

The Console prompts 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
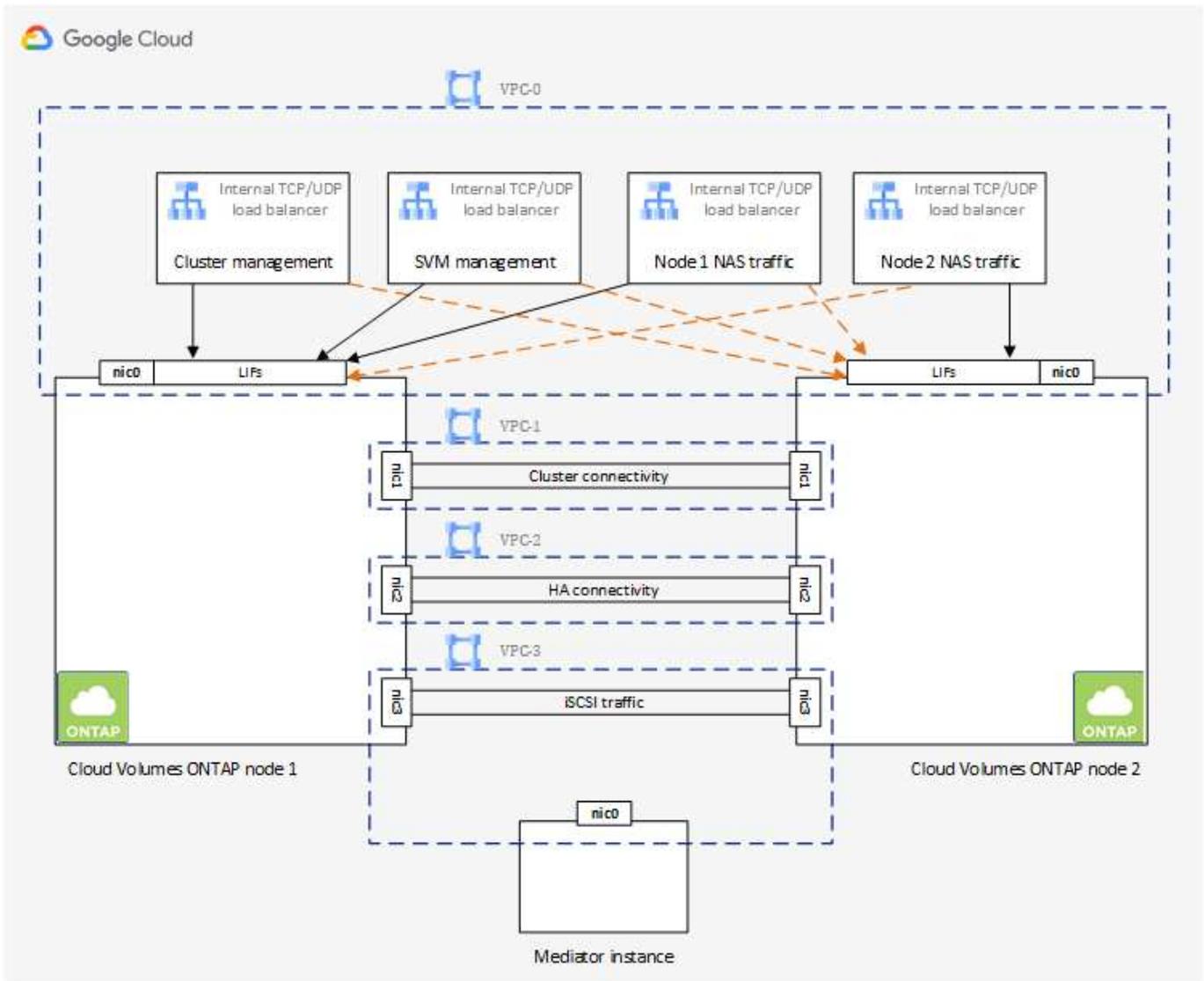
Subnets

A private subnet is required for each VPC.

If you place the Console agent 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

The Console 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 allocated 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**
  The Console 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:

    ```
    skipSvmManagementLif: true
    ```

- **HA pair**
  The Console 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:

    ```
    skipSvmManagementLif: true
    ```

Internal load balancers

The Console 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 Console agent 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 Console agent and Cloud Volumes ONTAP virtual machine instances in a *service project*.

Google Cloud documentation: Shared VPC overview.

Review the required shared VPC permissions covered in Console agent deployment

Packet mirroring in VPCs

Packet mirroring must be disabled in the Google Cloud subnet in which you deploy Cloud Volumes ONTAP.

Outbound internet access

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

The Console agent also contacts several endpoints for day-to-day operations. For information about the endpoints, refer to View endpoints contacted from the Console agent and Prepare networking for using the Console.

Cloud Volumes ONTAP endpoints

Cloud Volumes ONTAP uses these endpoints to communicate with various services.

Endpoints	Applicable for	Purpose	Deployment mode	Impact if endpoint is not available
https://netapp-cloud-account.auth0.com	Authentication	Used for authentication in the Console.	Standard and restricted modes.	User authentication fails and the following services remain unavailable: • Cloud Volumes ONTAP services • ONTAP services • Protocols and proxy services
https://api.bluexp.netapp.com/tenancy	Tenancy	Used to retrieve Cloud Volumes ONTAP resource from the Console to authorize resources and users.	Standard and restricted modes.	Cloud Volumes ONTAP resources and the users are not authorized.
https://mysupport.netapp.com/aods/asupmessage https://mysupport.netapp.com/asupprod/post/1.0/postAsup	AutoSupport	Used to send AutoSupport telemetry data to NetApp support.	Standard and restricted modes.	AutoSupport information remains undelivered.
https://cloudbuild.googleapis.com/v1 (for only private mode deployments) https://cloudkms.googleapis.com/v1 https://cloudresourcemanager.googleapis.com/v1/projects https://compute.googleapis.com/compute/v1 https://www.googleapis.com/compute/beta https://www.googleapis.com/compute/v1/projects/ https://www.googleapis.com/deploymentmanager/v2/projects https://www.googleapis.com/storage/v1 https://www.googleapis.com/upload/storage/v1 https://config.googleapis.com/v1 https://iam.googleapis.com/v1 https://storage.googleapis.com/storage/v1	Google Cloud (Commercial use).	Communication with Google Cloud services.	Standard, restricted, and private modes.	Cloud Volumes ONTAP cannot communicate with Google Cloud service to perform specific operations for the Console in Google Cloud.

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.

Google Cloud documentation: Cloud VPN overview.

Firewall rules

The Console 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 to use your 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 Console agent? View firewall rules for the Console agent

Inbound rules

When you add a Cloud Volumes ONTAP system, 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 Console agent 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 the Google Cloud documentation: Load Balancer Firewall Rules.

Protocol	Port	Purpose
All ICMP	All	Pinging the instance
HTTP	80	HTTP access to the ONTAP System Manager web console using the IP address of the cluster management LIF
HTTPS	443	Connectivity with the Console agent and HTTPS access to the ONTAP System Manager web console using the IP address of the cluster management LIF
SSH	22	SSH access to the IP address of the cluster management LIF or a node management LIF
TCP	111	Remote procedure call for NFS
TCP	139	NetBIOS service session for CIFS

Protocol	Port	Purpose
TCP	161-162	Simple network management protocol
TCP	445	Microsoft SMB/CIFS over TCP with NetBIOS framing
TCP	635	NFS mount
TCP	749	Kerberos
TCP	2049	NFS server daemon
TCP	3260	iSCSI access through the iSCSI data LIF
TCP	4045	NFS lock daemon
TCP	4046	Network status monitor for NFS
TCP	10000	Backup using NDMP
TCP	11104	Management of intercluster communication sessions for SnapMirror
TCP	11105	SnapMirror data transfer using intercluster LIFs
TCP	63001-63050	Load balance probe ports to determine which node is healthy (required for HA pairs only)
UDP	111	Remote procedure call for NFS
UDP	161-162	Simple network management protocol
UDP	635	NFS mount
UDP	2049	NFS server daemon
UDP	4045	NFS lock daemon
UDP	4046	Network status monitor for NFS
UDP	4049	NFS rquotad protocol

Outbound rules

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

Basic outbound rules

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

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

Advanced outbound rules

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

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

Service	Protocol	Port	Source	Destination	Purpose
AutoSupport	HTTPS	443	Node management LIF	mysupport.netapp.com	AutoSupport (HTTPS is the default)
	HTTP	80	Node management LIF	mysupport.netapp.com	AutoSupport (only if the transport protocol is changed from HTTPS to HTTP)
	TCP	3128	Node management LIF	Console agent	Sending AutoSupport messages through a proxy server on the Console agent, if an outbound internet connection isn't available
Configuration backups	HTTP	80	Node management LIF	http://<console-agent-IP-address>/occm/offboxconfig	Send configuration backups to the Console agent. ONTAP documentation
DHCP	UDP	68	Node management LIF	DHCP	DHCP client for first-time setup
DHCPS	UDP	67	Node management LIF	DHCP	DHCP server
DNS	UDP	53	Node management LIF and data LIF (NFS, CIFS)	DNS	DNS
NDMP	TCP	18600–18699	Node management LIF	Destination servers	NDMP copy
SMTP	TCP	25	Node management LIF	Mail server	SMTP alerts, can be used for AutoSupport
SNMP	TCP	161	Node management LIF	Monitor server	Monitoring by SNMP traps
	UDP	161	Node management LIF	Monitor server	Monitoring by SNMP traps
	TCP	162	Node management LIF	Monitor server	Monitoring by SNMP traps
	UDP	162	Node management LIF	Monitor server	Monitoring by SNMP traps
SnapMirror	TCP	11104	Intercluster LIF	ONTAP intercluster LIFs	Management of intercluster communication sessions for SnapMirror
	TCP	11105	Intercluster LIF	ONTAP intercluster LIFs	SnapMirror data transfer
Syslog	UDP	514	Node management LIF	Syslog server	Syslog forward messages

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 created for the instances in VPC-1, VPC-2, and VPC-3 enable 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.

Infrastructure Manager configuration for private mode deployments

If you want to deploy Cloud Volumes ONTAP 9.16.1 or later in private mode, you need to make a few configuration changes so that Cloud Volumes ONTAP can use Google Cloud Infrastructure Manager as the deployment service instead of Deployment Manager, which Google will eventually deprecate.

Before you begin

- Ensure that your Cloud Volumes ONTAP system is 9.16.1 or later. If it isn't, upgrade your system. Refer to Upgrade Cloud Volumes ONTAP for instructions.

- Ensure that the Google Cloud APIs are enabled. Refer to Enable Google Cloud APIs.

- Ensure that the Cloud Build API is enabled. Refer to Enable the Cloud Build API here.

- Verify that the Console agent's service account has all standard permissions. Additionally, ensure that the service account has the `cloudbuild.workerpools.get` and `cloudbuild.workerpools.list` permissions. Refer to Google Cloud permissions for the Console agent.

Steps

1. Create a private worker pool with this configuration in the same region as the Cloud Volumes ONTAP deployments. For information about creating a private worker pool, refer to Google Cloud documentation: Create and manage private pools and Google Cloud Build pricing.

   The worker pool must have the following configuration:

   - Machine type: e2-medium

   - Disk size: 100 GB

   - Assign external IP: False

   - Network: Default or a private.

   - The subnet configured to access Google APIs. Perform these steps to ensure that the subnet can access Google APIs:

     a. Ensure "Private Google Access" is turned on for the subnet.

     b. Go to **VPC Network level > Private Service Access Tab > Allocated IP ranges for services**.

     c. Select **Allocate IP range** and allocate the internal IP range for the private connection to the Google Compute Service.

     d. On **Private connection to services**, select **Create Connection**.

e. Select **Connected service producer = Google Cloud Platform**.

f. Assign the allocation for the private connection IP range you created in the previous step.

2. Deploy this worker pool and keep it running for Cloud Volumes ONTAP management. Google Cloud uses this worker pool to run all Terraform operations in an isolated environment.

3. When deploying Cloud Volumes ONTAP in private mode, select the name of this worker pool in the **GCP Worker Pool** field. Refer to Launch Cloud Volumes ONTAP in Google Cloud for instructions.

Requirements for the Console agent

If you haven't created a Console agent yet, you should review networking requirements.

- View networking requirements for the Console agent
- Firewall rules in Google Cloud

Network configurations to support Console agent proxy

You can use the proxy servers configured for the Console agent to enable outbound internet access from Cloud Volumes ONTAP. The Console supports two types of proxies:

- **Explicit proxy**: The outbound traffic from Cloud Volumes ONTAP uses the HTTP address of the proxy server specified during the Console agent proxy configuration. The Console agent administrator might also have configured user credentials and root CA certificates for additional authentication. If a root CA certificate is available for the explicit proxy, make sure to obtain and upload the same certificate to your Cloud Volumes ONTAP system using the ONTAP CLI: security certificate install command.

- **Transparent proxy**: The network is configured to automatically route outbound traffic from Cloud Volumes ONTAP through the Console agent proxy. When setting up a transparent proxy, the Console agent administrator needs to provide only a root CA certificate for connectivity from Cloud Volumes ONTAP, not the HTTP address of the proxy server. Make sure that you obtain and upload the same root CA certificate to your Cloud Volumes ONTAP system using the ONTAP CLI: security certificate install command.

For information about configuring proxy servers for the Console agent, refer to the Configure a Console agent to use a proxy server.

Configure network tags for Cloud Volumes ONTAP in Google Cloud

During the transparent proxy configuration of the Console agent, the administrator adds a network tag for Google Cloud. You need to obtain and manually add the same network tag for your Cloud Volumes ONTAP configuration. This tag is necessary for the proxy server to function correctly.

1. In the Google Cloud Console, locate your Cloud Volumes ONTAP system.

2. Go to **Details > Networking > Network tags**.

3. Add the tag used for the Console agent and save the configuration.

Related topics
- Verify AutoSupport setup for Cloud Volumes ONTAP
- Learn about ONTAP internal ports.

Set up VPC Service Controls to deploy Cloud Volumes ONTAP in Google Cloud

When choosing to lock down your Google Cloud environment with VPC Service Controls, you should understand how NetApp Console and Cloud Volumes ONTAP interact with the

Google Cloud APIs, as well as how to configure your service perimeter to deploy the Console 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

The Console 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 Console agent.

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

Images

Both Cloud Volumes ONTAP and the Console use images from a project within Google Cloud that is managed by NetApp. This can affect the deployment of the Console agent 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 Console agent 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 Console agent and Cloud Volumes ONTAP.

Deploying a Console agent

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

Deploying Cloud Volumes ONTAP

- The Console 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 Google Cloud VPC Service Controls Policy Documentation.

To set the policies that the Console 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 Console agent and for Cloud Volumes ONTAP.

Create a Google Cloud service account for Cloud Volumes ONTAP

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 NetApp 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.

Create service account

Service account details ✓

2 **Grant this service account access to project**
(optional)

Grant this service account access to OCCM-Dev so that it has permission to complete specific actions on the resources in your project. Learn more

Select a role — Condition 🗑

≡ storage admin ✕

Cloud ML Service Agent
Cloud ML service agent can act as log writer, Cloud Storage admin, Artifact Registry Reader, BigQuery writer, and service account access token creator.

Storage Admin
Full control of GCS resources.

Storage HMAC Key Admin
Full control of GCS HMAC Keys.

Storage Object Admin
Full control of GCS objects

MANAGE ROLES

c. **Grant users access to this service account**: Add the Console agent 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 Backup and Recovery.

What's next?

You'll need to select the service account later when you create a Cloud Volumes ONTAP system.

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 APIs 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 Console agent service account has the correct permissions at the project level, in the project where the key is stored.

   The permissions are provided in the the 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, the NetApp Console 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 system.

   Example

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

Refer to the [NetApp Console 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 system.

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 > Management**.

2. On the **Systems** page, click **Add System** and follow the steps in the NetApp Console.

   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 the Console, select **Freemium** when you reach the charging methods page.

[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 or Professional package.

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

- A license (bring your own 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.

> (i) NetApp has restricted the purchase, extension, and renewal of BYOL licensing. For more information, refer to [Restricted availability of BYOL licensing for Cloud Volumes ONTAP](#).

Steps
1. [Contact NetApp Sales to obtain a license](#)
2. [Add your NetApp Support Site account to the NetApp Console](#)

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

   Your license must be available from the Console before you can use it with Cloud Volumes ONTAP. If

needed, you can manually add the license to the Console.

3. On the **Systems** page, click **Add System** and follow the steps.

   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 the Console, select a capacity-based package when you reach the charging methods page.

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

PAYGO subscription

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

When you create a Cloud Volumes ONTAP system, the Console prompts you to subscribe to the agreement that's available in the Google Cloud Marketplace. That subscription is then associated with the system for charging. You can use that same subscription for additional systems.

Steps

1. From the left navigation menu, select **Storage > Management**.

2. On the **Systems** page, click **Add System** and follow the steps.

   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 the Console, select a capacity-based package when you reach the charging methods page.

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

> 💡 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 system creation.

2. On the **Systems** page, click **Add System** and follow the steps.

   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 the Console, select a capacity-based package when you reach the charging methods page.

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

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 the Console 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 **Systems** page, click **Add System** and follow the steps.
   a. Select the Keystone Subscription charging method when prompted to choose a charging method.

Node-based license

A node-based license is the previous generation license for Cloud Volumes ONTAP. A node-based license could be procured from NetApp (BYOL) and is available for license renewals, only in specific cases. For information, refer to:

- End of availability for node-based licenses
- End of availability of node-based licenses
- Convert a node-based license to a capacity-based license

Launch 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 begin

You need the following before you begin.

- A NetApp Console agent that's up and running.
  - You should have a Console agent that is associated with your system.
  - You should be prepared to leave the Console agent running at all times.

◦ The service account associated with the Console agent 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, refer to Planning your Cloud Volumes ONTAP configuration.

• An understanding of what's required to set up licensing for Cloud Volumes ONTAP.

  Learn how to set up licensing.

• 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

Launch a single-node system in Google Cloud

Create a system in the NetApp Console to launch Cloud Volumes ONTAP in Google Cloud.

Steps

1. From the left navigation menu, select **Storage > Management**.
2. On the **Systems** page, click **Add System** and follow the prompts.
3. **Choose a Location**: Select **Google Cloud** and **Cloud Volumes ONTAP**.
4. If you're prompted, create a Console agent.
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:

Field	Description
System Name	The Console uses the system 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.
Service Account Name	If you plan to use data tiering or NetApp 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.

Field	Description
Add Labels	Labels are metadata for your Google Cloud resources. The Console 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 system, and then you can add more after it's created. Note that the API does not limit you to four labels when creating a system. For information about labels, refer to the 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 ONTAP System Manager or the ONTAP CLI. Keep the default *admin* user name or change it to a custom user name.
Edit Project	Select the project where you want Cloud Volumes ONTAP to reside. The default project is the project where of the Console. If you don't see any additional projects in the drop-down list, then you haven't yet associated the 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 role that you use for the Console to that project. You'll need to repeat this step for each project. ⓘ This is the service account that you set up for the Console, 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. Refer to Associating a marketplace subscription with Google Cloud credentials.

6. **Services**: Select the services that you want to use on this system. In order to select Backup and Recovery, or to use NetApp Cloud Tiering, you must have specified the Service Account in step 3.

   💡 If you would like to utilize WORM and data tiering, you must disable Backup and Recovery and deploy a Cloud Volumes ONTAP system with version 9.8 or above.

7. **Location & Connectivity**: Select the Google Cloud region and zone for your system, 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:

Field	Description
Connectivity verification	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 Google Cloud Documentation: Configuring Private Google Access.
Generated firewall policy	If you let the Console 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 Console agent 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 firewall policy	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**. The preconfigured packages vary with the selected Cloud Volumes ONTAP version. For example, for Cloud Volumes ONTAP 9.18.1 and later, the Console shows packages with C3 VMs, including Hyperdisk Balanced disks. You can modify the configurations, such as IOPS and throughput parameters, based on your workload needs.

   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 a selected version, then the Console updates the system to that version when creating it. For example, the update occurs if you select Cloud Volumes ONTAP 9.13.1 and 9.13.1 P4 is available. The update does not occur from one release to another— for example, from 9.13 to 9.14.

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 the Console 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, refer to Size your system in Google Cloud.

12. **Flash Cache, Write Speed & WORM**:

a. Enable **Flash Cache** or choose **Normal** or **High** write speed if you need.

Learn more about Flash Cache and 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, refer to Rules for VPC-1, VPC-2, and VPC-3.

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.

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:

- The Console 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 Console agent service account as a user of the tiering service account, otherwise, you can't select it from the Console.

- For help with adding a Google Cloud account, refer to 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:

Field	Description
Size	The maximum size that you can enter largely depends on whether you enable thin provisioning, which enables you to create a volume that is bigger than the physical storage currently available to it.
Access control (for NFS only)	An export policy defines the clients in the subnet that can access the volume. By default, the Console enters a value that provides access to all instances in the subnet.

Field	Description
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, the Console 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 first page of the volume creation wizard:

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. For information, refer to the NetApp Console 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, refer to Choose a volume usage profile, Data tiering overview, and KB: What Inline Storage Efficiency features are supported with CVO?

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 the Console will purchase.

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

    d. Click **Go**.

Result

The Console deploys the Cloud Volumes ONTAP system. You can track the progress on the **Audit** page.

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

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

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

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

> ⚠️ After the deployment process completes, do not modify the system-generated Cloud Volumes ONTAP configurations in the Google Cloud portal, such as the system tags, and the labels set in the Google Cloud resources. Any changes made to these configurations may lead to unexpected behavior or data loss.

Launch an HA pair in Google Cloud

Create a system in the Console to launch Cloud Volumes ONTAP in Google Cloud.

Steps
1. From the left navigation menu, select **Storage > Management**.
2. On the **Systems** page, click **Storage > System** 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:

Field	Description
System Name	The Console uses the system 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.
Service Account Name	If you plan to use the NetApp Cloud Tiering or Backup and Recovery services, you need to enable the **Service Account** switch and then select the Service Account that has the predefined Storage Admin role.
Add Labels	Labels are metadata for your Google Cloud resources. The Console 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 system, and then you can add more after it's created. Note that the API does not limit you to four labels when creating a system. For information about labels, refer to Google Cloud Documentation: Labeling Resources.

Field	Description
User name and password	These are the credentials for the Cloud Volumes ONTAP cluster administrator account. You can use these credentials to connect to Cloud Volumes ONTAP through ONTAP System Manager or the ONTAP CLI. Keep the default *admin* user name or change it to a custom user name.
Edit Project	Select the project where you want Cloud Volumes ONTAP to reside. If you don't see any additional projects in the drop-down list, then you haven't yet associated the 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 role that you use for the Console to that project. You'll need to repeat this step for each project. ⓘ This is the service account that you set up for the Console, 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. Refer to Associating a marketplace subscription with Google Cloud credentials.

5. **Services**: Select the services that you want to use on this system. To select Backup and Recovery, or to use NetApp Cloud Tiering, you must have specified the Service Account in step 3.

> 💡 If you would like to utilize WORM and data tiering, you must disable Backup and Recovery and deploy a Cloud Volumes ONTAP system 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 zone.

   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 the Console 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 Console agent 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 the Console updates the system to that version when creating it. For example, the update occurs if you select Cloud Volumes ONTAP 9.13.1 and 9.13.1 P4 is available. The update does not occur from one release to another—for example, from 9.13 to 9.14.

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 the Console 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, refer to Size your system in Google Cloud.

12. **Flash Cache, Write Speed & WORM**:

    a. Enable **Flash Cache** or choose **Normal** or **High** write speed if you need.

       Learn more about Flash Cache and 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, refer to Rules for VPC-1, VPC-2, and VPC-3.

    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.

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:

- The Console 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 Console agent service account as a user of the tiering service account, otherwise, you can't select it from the Console.

- 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:

Field	Description
Size	The maximum size that you can enter largely depends on whether you enable thin provisioning, which enables you to create a volume that is bigger than the physical storage currently available to it.
Access control (for NFS only)	An export policy defines the clients in the subnet that can access the volume. By default, the Console enters a value that provides access to all instances in the subnet.
Permissions and Users / Groups (for CIFS only)	These fields enable you to control the level of access to a share for users and groups (also called access control lists or ACLs). You can specify local or domain Windows users or groups, or UNIX users or groups. If you specify a domain Windows user name, you must include the user's domain using the format domain\username.

Field	Description
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, the Console 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 first page of the volume creation wizard:

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. Refer to the NetApp Console 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, refer to Choose a volume usage profile, Data tiering overview, and KB: What Inline Storage Efficiency features are supported with CVO?

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 the Console will purchase.

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

    d. Click **Go**.

Result

The Console deploys the Cloud Volumes ONTAP system. You can track the progress on the **Audit** page.

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

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

After you finish

- If you provisioned a CIFS share, give users or groups permissions to the files and folders and verify that those users can access the share and create a file.

- If you want to apply quotas to volumes, use ONTAP System Manager or the ONTAP CLI.

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

> ⚠️ After the deployment process completes, do not modify the system-generated Cloud Volumes ONTAP configurations in the Google Cloud portal, such as the system tags, and the labels set in the Google Cloud resources. Any changes made to these configurations may lead to unexpected behavior or data loss.

Related links

- Planning your Cloud Volumes ONTAP configuration in Google Cloud

Google Cloud Platform Image Verification

Learn how Google Cloud image is verfied in Cloud Volumes ONTAP

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 Google Cloud image by using the signed digest and public certificate for Google Cloud which can be downloaded via NSS for a specific release.

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

Convert Google Cloud image to raw format for Cloud Volumes ONTAP

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 in 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

```
$ 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 "setup-disks"
[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 "wait-for-inst-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
```

```
[image-export]: 2023-01-25T18:13:51Z Workflow GCSPath: gs://example-
demo-project-example-bkt-us/
[image-export]: 2023-01-25T18:13:51Z Example scratch path:
https://console.cloud.google.com/storage/browser/example-demo-project-
example-bkt-us/example-image-export-20230125-18:13:49-r88px
[image-export]: 2023-01-25T18:13:51Z Uploading sources
[image-export]: 2023-01-25T18:13:51Z Running workflow
[image-export]: 2023-01-25T18:13:51Z Running step "setup-disks"
(CreateDisks)
[image-export.setup-disks]: 2023-01-25T18:13:51Z CreateDisks: Creating
disk "disk-image-export-image-export-r88px".
[image-export]: 2023-01-25T18:14:02Z Step "setup-disks" (CreateDisks)
successfully finished.
[image-export]: 2023-01-25T18:14:02Z Running step "image-export-export-
disk" (IncludeWorkflow)
[image-export.image-export-export-disk]: 2023-01-25T18:14:02Z Running
step "setup-disks" (CreateDisks)
[image-export.image-export-export-disk.setup-disks]: 2023-01-
25T18:14:02Z CreateDisks: Creating disk "disk-image-export-export-disk-
image-export-image-export--r88px".
[image-export.image-export-export-disk]: 2023-01-25T18:14:02Z Step
"setup-disks" (CreateDisks) successfully finished.
[image-export.image-export-export-disk]: 2023-01-25T18:14:02Z Running
step "run-image-export-export-disk" (CreateInstances)
[image-export.image-export-export-disk.run-image-export-export-disk]:
2023-01-25T18:14:02Z CreateInstances: Creating instance "inst-image-
export-export-disk-image-export-image-export--r88px".
[image-export.image-export-export-disk]: 2023-01-25T18:14:08Z Step
"run-image-export-export-disk" (CreateInstances) successfully finished.
[image-export.image-export-export-disk.run-image-export-export-disk]:
2023-01-25T18:14:08Z CreateInstances: Streaming instance "inst-image-
export-export-disk-image-export-image-export--r88px" serial port 1
output to https://storage.cloud.google.com/example-demo-project-
example-bkt-us/example-image-export-20230125-18:13:49-r88px/logs/inst-
image-export-export-disk-image-export-image-export--r88px-serial-
port1.log
[image-export.image-export-export-disk]: 2023-01-25T18:14:08Z Running
step "wait-for-inst-image-export-export-disk" (WaitForInstancesSignal)
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:08Z 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:".
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
```

StatusMatch found: "GCEExport: <serial-output key:'source-size-gb' value:'10'>"
[image-export.image-export-export-disk.wait-for-inst-image-export-export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance "inst-image-export-export-disk-image-export-image-export--r88px": StatusMatch found: "GCEExport: Running export tool."
[image-export.image-export-export-disk.wait-for-inst-image-export-export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance "inst-image-export-export-disk-image-export-image-export--r88px": StatusMatch found: "GCEExport: Disk /dev/sdb is 10 GiB, compressed size will most likely be much smaller."
[image-export.image-export-export-disk.wait-for-inst-image-export-export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance "inst-image-export-export-disk-image-export-image-export--r88px": StatusMatch found: "GCEExport: Beginning export process..."
[image-export.image-export-export-disk.wait-for-inst-image-export-export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance "inst-image-export-export-disk-image-export-image-export--r88px": StatusMatch found: "GCEExport: Copying \"/dev/sdb\" to gs://example-demo-project-example-bkt-us/example-image-export-20230125-18:13:49-r88px/outs/image-export-export-disk.tar.gz."
[image-export.image-export-export-disk.wait-for-inst-image-export-export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance "inst-image-export-export-disk-image-export-image-export--r88px": StatusMatch found: "GCEExport: Using \"/root/upload\" as the buffer prefix, 1.0 GiB as the buffer size, and 4 as the number of workers."
[image-export.image-export-export-disk.wait-for-inst-image-export-export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance "inst-image-export-export-disk-image-export-image-export--r88px": StatusMatch found: "GCEExport: Creating gzipped image of \"/dev/sdb\"."
[image-export.image-export-export-disk.wait-for-inst-image-export-export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance "inst-image-export-export-disk-image-export-image-export--r88px": StatusMatch found: "GCEExport: Read 1.0 GiB of 10 GiB (212 MiB/sec), total written size: 992 MiB (198 MiB/sec)"
[image-export.image-export-export-disk.wait-for-inst-image-export-export-disk]: 2023-01-25T18:14:59Z WaitForInstancesSignal: Instance "inst-image-export-export-disk-image-export-image-export--r88px": StatusMatch found: "GCEExport: Read 8.0 GiB of 10 GiB (237 MiB/sec), total written size: 1.5 GiB (17 MiB/sec)"
[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": 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":
StatusMatch found: "GCEExport: Finished export in  48.957347731s"
[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":
StatusMatch found: "GCEExport: <serial-output key:'target-size-gb'
value:'2'>"
[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"
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Step
"wait-for-inst-image-export-export-disk" (WaitForInstancesSignal)
successfully finished.
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Running
step "copy-image-object" (CopyGCSObjects)
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Running
step "delete-inst" (DeleteResources)
[image-export.image-export-export-disk.delete-inst]: 2023-01-
25T18:15:19Z DeleteResources: Deleting instance "inst-image-export-
export-disk".
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Step
"copy-image-object" (CopyGCSObjects) successfully finished.
[image-export.image-export-export-disk]: 2023-01-25T18:15:34Z Step
"delete-inst" (DeleteResources) successfully finished.
[image-export]: 2023-01-25T18:15:34Z Step "image-export-export-disk"
(IncludeWorkflow) successfully finished.
[image-export]: 2023-01-25T18:15:34Z Serial-output value -> source-
size-gb:10
[image-export]: 2023-01-25T18:15:34Z Serial-output value -> target-
size-gb:2
[image-export]: 2023-01-25T18:15:34Z Workflow "image-export" cleaning
up (this may take up to 2 minutes).
[image-export]: 2023-01-25T18:15:35Z 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
```

> ℹ️ For more information on how to export an image through Google Cloud, refer to the Google Cloud doc on Exporting an image.

Image signature verification

Google Cloud image signature verification for Cloud Volumes ONTAP

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)

Cloud Volumes ONTAP 9.15.0P1

Date Posted : 17-May-2024

Cloud Volumes ONTAP
Non-Restricted Countries

If you are upgrading to ONTAP 9.15.0P1, and you are in "Non-restricted Countries", please download the image with NetApp Volume Encryption.

DOWNLOAD 9150P1_V_IMAGE.TGZ [2.58 GB]

View and download checksums

DOWNLOAD 9150P1_V_IMAGE.TGZ.PEM [451 B]

View and download checksums

DOWNLOAD 9150P1_V_IMAGE.TGZ.SIG [256 B]

View and download checksums

Cloud Volumes ONTAP
Restricted Countries

If you are unsure whether your company complied with all applicable legal requirements on encryption technology, download the image without NetApp Volume Encryption.

DOWNLOAD 9150P1_V_NODAR_IMAGE.TGZ [2.58 GB]

View and download checksums

DOWNLOAD 9150P1_V_NODAR_IMAGE.TGZ.PEM [451 B]

View and download checksums

DOWNLOAD 9150P1_V_NODAR_IMAGE.TGZ.SIG [256 B]

View and download checksums

Cloud Volumes ONTAP

DOWNLOAD GCP-9-15-0P1_PKG.TAR.GZ [7.49 KB]

View and download checksums

DOWNLOAD AZURE-9-15-0P1_PKG.TAR.GZ [7.64 KB]

View and download checksums

- 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
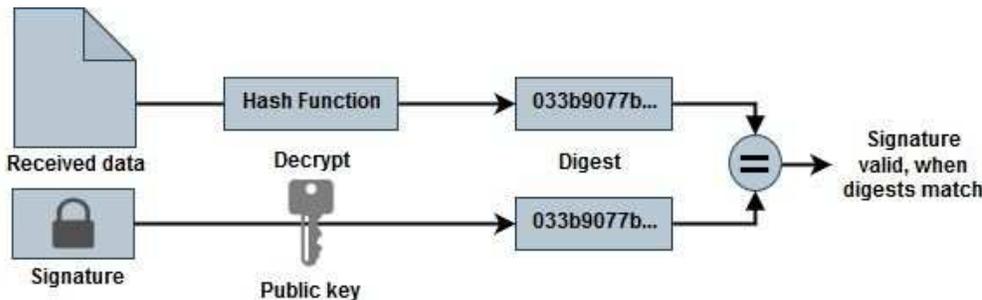
Verify the Google Cloud image disk.raw file for Cloud Volumes ONTAP using OpenSSL

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, macOS, and Windows machines.

Steps

1. Verify the certificate using OpenSSL.

Click to display

```
# 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>
$ openssl ocsp -issuer Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem
-CAfile Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem -cert
Certificate-GCP-CVO-20230119-0XXXXX.pem -reqout req.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 ${ocsp_url} -resp_text
-respout <response.der>
```

```
$ openssl ocsp -issuer Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem
-CAfile Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem -cert
Certificate-GCP-CVO-20230119-0XXXXX.pem  -url ${ocsp_url} -resp_text
-respout resp.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
         0b:b6:61:e4:03:5f:98:6f:10:1c:9a:f7:5f:6f:c7:e3:f4:72:
         f2:30:f4:86:88:9a:b9:ba:1e:d6:f6:47:af:dc:ea:e4:cd:31:
         af:e3:7a:20:35:9e:60:db:28:9c:7f:2e:17:7b:a5:11:40:4f:
         1e:72:f7:f8:ef:e3:23:43:1b:bb:28:1a:6f:c6:9c:c5:0c:14:
         d3:5d:bd:9b:6b:28:fb:94:5e:8a:ef:40:20:72:a4:41:df:55:
         cf:f3:db:1b:39:e0:30:63:c9:c7:1f:38:7e:7f:ec:f4:25:7b:
         1e:95:4c:70:6c:83:17:c3:db:b2:47:e1:38:53:ee:0a:55:c0:
         15:6a:82:20:b2:ea:59:eb:9c:ea:7e:97:aa:50:d7:bc:28:60:
         8c:d4:21:92:1c:13:19:b4:e0:66:cb:59:ed:2e:f8:dc:7b:49:
         e3:40:f2:b6:dc:d7:2d:2e:dd:21:82:07:bb:3a:55:99:f7:59:
         5d:4a:4d:ca:e7:8f:1c:d3:9a:3f:17:7b:7a:c4:57:b2:57:a8:
         b4:c0:a5:02:bd:59:9c:50:32:ff:16:b1:65:3a:9c:8c:70:3b:
         9e:be:bc:4f:f9:86:97:b1:62:3c:b2:a9:46:08:be:6b:1b:3c:
         24:14:59:28:c6:ae:e8:d5:64:b2:f8:cc:28:24:5c:b2:c8:d8:
         5a:af:9d:55:48:96:f6:3e:c6:bf:a6:0c:a4:c0:ab:d6:57:03:
         2b:72:43:b0:6a:9f:52:ef:43:bb:14:6a:ce:66:cc:6c:4e:66:
         17:20:a3:64:e0:c6:d1:82:0a:d7:41:8a:cc:17:fd:21:b5:c6:
         d2:3a:af:55:2e:2a:b8:c7:21:41:69:e1:44:ab:a1:dd:df:6d:
         15:99:90:cc:a0:74:1e:e5:2e:07:3f:50:e6:72:a6:b9:ae:fc:
         44:15:eb:81:3d:1a:f8:17:b6:0b:ff:05:76:9d:30:06:40:72:
         cf:d5:c4:6f:8b:c9:14:76:09:6b:3d:6a:70:2c:5a:c4:51:92:
         e5:cd:84:b6:f9:d9:d5:bc:8d:72:b7:7c:13:9c:41:89:a8:97:
         6f:4a:11:5f:8f:b6:c9:b5:df:00:7e:97:20:e7:29:2e:2b:12:
         77:dc:e2:63:48:87:42:49:1d:fc:d0:94:a8:8d:18:f9:07:85:
```

```
            e4:d0:3e:9a:4a:d7:d5:d0:02:51:c3:51:1c:73:12:96:2d:75:
            22:83:a6:70:5a:4a:2b:f2:98:d9:ae:1b:57:53:3d:3b:58:82:
            38:fc:fa:cb:57:43:3f:3e:7e:e0:6d:5b:d6:fc:67:7e:07:7e:
            fb:a3:76:43:26:8f:d1:42:d6:a6:33:4e:9e:e0:a0:51:b4:c4:
            bc:e3:10:0d:bf:23:6c:4b
WARNING: no nonce in response
Response Verify OK
Certificate-GCP-CVO-20230119-0XXXXX.pem: good
     This Update: Jan 19 15:00:00 2023 GMT
     Next Update: Jan 26 14:59:59 2023 GMT

# Step 1.5 - Optional: Check the response file "response.der" has
been generated. Verify its contents.
$ ls -l
total 64
-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
-rw-r--r--  1 example-user  engr   806 Jan 19 16:51 resp.der

# Step 1.6 - Verify the chain of trust and expiration dates against
the local host
$ openssl version -d
OPENSSLDIR: "/private/etc/ssl"
$ OPENSSLDIR=$(openssl version -d | cut -d '"' -f2)
$ echo $OPENSSLDIR
/private/etc/ssl

$ openssl verify -untrusted <Certificate-Chain.pem> -CApath <OpenSSL
dir> <Certificate.pem>
$ openssl verify -untrusted Certificate-Chain-GCP-CVO-20230119-
0XXXXX.pem -CApath ${OPENSSLDIR} Certificate-GCP-CVO-20230119-
0XXXXX.pem
Certificate-GCP-CVO-20230119-0XXXXX.pem: OK
```

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.

Click to display

```
# 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
```