



# **Cloud Volumes ONTAP documentation**

## **Cloud Volumes ONTAP**

NetApp

March 10, 2023

This PDF was generated from <https://docs.netapp.com/us-en/cloud-manager-cloud-volumes-ontap/index.html> on March 10, 2023. Always check docs.netapp.com for the latest.

# Table of Contents

Cloud Volumes ONTAP documentation	1
Release notes	2
What's new	2
Known limitations	23
Cloud Volumes ONTAP Release Notes	23
Get started	25
Learn about Cloud Volumes ONTAP	25
Supported versions for new deployments	26
Get started in Amazon Web Services	28
Get started in Microsoft Azure	95
Get started in Google Cloud	131
Use Cloud Volumes ONTAP	180
License management	180
Volume and LUN administration	192
Aggregate administration	214
Storage VM administration	217
Security and data encryption	249
System administration	261
System health and events	287
Concepts	292
Cloud Volumes ONTAP licensing	292
Storage	298
High-availability pairs	319
Security	336
Performance	338
License management for node-based BYOL	338
AutoSupport and Active IQ Digital Advisor	341
Default configuration for Cloud Volumes ONTAP	342
Knowledge and support	346
Register for support	346
Get help	350
Legal notices	356
Copyright	356
Trademarks	356
Patents	356
Privacy policy	356
Open source	356

# Cloud Volumes ONTAP documentation

# Release notes

## What's new

Learn what's new with Cloud Volumes ONTAP management in BlueXP (formerly Cloud Manager).

The enhancements described on this page are specific to BlueXP features that enable management of Cloud Volumes ONTAP. To learn what's new with the Cloud Volumes ONTAP software itself, [go to the Cloud Volumes ONTAP Release Notes](#)

### 5 March 2023

The following changes were introduced with the 3.9.27 release of the Connector.

#### 16 TiB and 32 TiB support in Azure

Cloud Volumes ONTAP now supports 16 TiB and 32 TiB disk sizes for high availability deployments running on managed disks in Azure.

Learn more about [supported disk sizes in Azure](#).

#### MTEKM license

The Multi-tenant Encryption Key Management (MTEKM) license is now included with new and existing Cloud Volumes ONTAP systems running version 9.12.1 GA or later.

Multi-tenant external key management enables individual storage VMs (SVMs) to maintain their own keys through a KMIP server when using NetApp Volume Encryption.

[Learn how to encrypt volumes with NetApp encryption solutions.](#)

#### Support for environments without internet

Cloud Volumes ONTAP is now supported in any cloud environment that has complete isolation from the internet. Only node-based licensing (BYOL) is supported in these environments. Capacity-based licensing is not supported. To get started, manually install the Connector software, log in to the BlueXP console that's running on the Connector, add your BYOL license to the Digital Wallet, and then deploy Cloud Volumes ONTAP.

- [Install the Connector in a location without internet access](#)
- [Access the BlueXP console on the Connector](#)
- [Add an unassigned license](#)

### 5 February 2023

The following changes were introduced with the 3.9.26 release of the Connector.

#### Placement group creation in AWS

A new configuration setting is now available for placement group creation with AWS HA single availability zone

(AZ) deployments. Now you can choose to bypass failed placement group creations and allow AWS HA single AZ deployments to complete successfully.

For detailed information on how to configure the placement group creation setting, see [Configure placement group creation for AWS HA Single AZ](#).

### **Private DNS zone configuration update**

A new configuration setting is now available so that you can avoid creating a link between a private DNS zone and a virtual network when using Azure Private Links. Creation is enabled by default.

[Provide BlueXP with details about your Azure Private DNS](#)

### **WORM storage and data tiering**

You can now enable both data tiering and WORM storage together when you create a Cloud Volumes ONTAP 9.8 system or later. Enabling data tiering with WORM storage allows you to tier the data to an object store in the cloud.

[Learn about WORM storage.](#)

## **1 January 2023**

The following changes were introduced with the 3.9.25 release of the Connector.

### **Licensing packages available in Google Cloud**

Optimized and Edge Cache capacity-based licensing packages are available for Cloud Volumes ONTAP in the Google Cloud Marketplace as a pay-as-you-go offering or as an annual contract.

See [Cloud Volumes ONTAP licensing](#).

### **Default configuration for Cloud Volumes ONTAP**

The Multi-tenant Encryption Key Management (MTEKM) license is no longer included in new Cloud Volumes ONTAP deployments.

For more information on the ONTAP feature licenses automatically installed with Cloud Volumes ONTAP, see [Default Configuration for Cloud Volumes ONTAP](#).

## **15 December 2022**

### **Cloud Volumes ONTAP 9.12.0**

BlueXP can now deploy and manage Cloud Volumes ONTAP 9.12.0 in AWS and Google Cloud.

[Learn about the new features included in this release of Cloud Volumes ONTAP.](#)

## **8 December 2022**

### **Cloud Volumes ONTAP 9.12.1**

BlueXP can now deploy and manage Cloud Volumes ONTAP 9.12.1, which includes support for new features and additional cloud provider regions.

[Learn about the new features included in this release of Cloud Volumes ONTAP](#)

## 4 December 2022

The following changes were introduced with the 3.9.24 release of the Connector.

### **WORM + Cloud Backup now available during Cloud Volumes ONTAP creation**

The ability to activate both write once, read many (WORM) and Cloud Backup features is now available during the Cloud Volumes ONTAP creation process.

### **Israel region now supported in Google Cloud**

The Israel region is now supported in Google Cloud for Cloud Volumes ONTAP and the Connector for Cloud Volumes ONTAP 9.11.1 P3 and later.

## 15 November 2022

The following changes were introduced with the 3.9.23 release of the Connector.

### **ONTAP S3 license in GCP**

An ONTAP S3 license is now included on new and existing Cloud Volumes ONTAP systems running version 9.12.1 or later in Google Cloud Platform.

[Learn how to configure and manage S3 object storage services in ONTAP](#)

## 6 November 2022

The following changes were introduced with the 3.9.23 release of the Connector.

### **Moving resource groups in Azure**

You can now move a working environment from one resource group to a different resource group in Azure within the same Azure subscription.

For more information, see [Moving resource groups](#).

### **NDMP-copy certification**

NDMP-copy is now certified for use with Cloud Volume ONTAP.

For information on how to configure and use NDMP, see [NDMP configuration overview](#).

### **Managed disk encryption support for Azure**

A new Azure permission has been added that now allows you to encrypt all managed disks upon creation.

For more information on this new functionality, see [Set up Cloud Volumes ONTAP to use a customer-managed key in Azure](#).

## 18 September 2022

The following changes were introduced with the 3.9.22 release of the Connector.

### Digital Wallet enhancements

- The Digital Wallet now shows a summary of the Optimized I/O licensing package and the provisioned WORM capacity for Cloud Volumes ONTAP systems across your account.

These details can help you better understand how you're being charged and whether you need to purchase additional capacity.

[Learn how to view the consumed capacity in your account.](#)

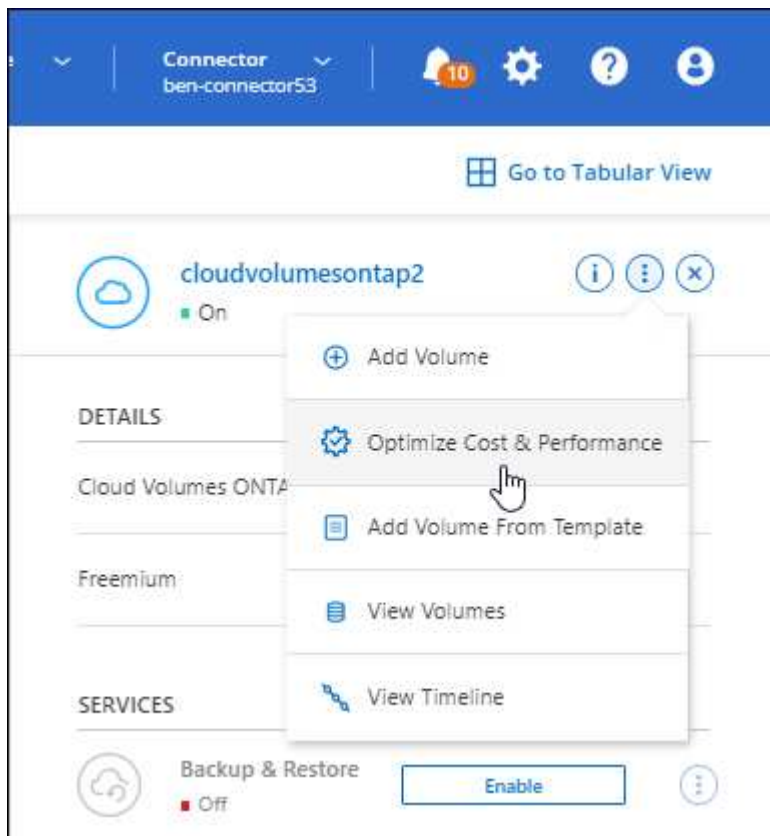
- You can now change from one charging method to the Optimized charging method.

[Learn how to change charging methods.](#)

### Optimize cost and performance

You can now optimize the cost and performance of a Cloud Volumes ONTAP system directly from the Canvas.

After you select a working environment, you can choose the **Optimize Cost & Performance** option to change the instance type for Cloud Volumes ONTAP. Choosing a smaller-sized instance can help you reduce costs, while changing to a larger-sized instance can help you optimize performance.



## AutoSupport notifications

BlueXP will now generate a notification if a Cloud Volumes ONTAP system is unable to send AutoSupport messages. The notification includes a link to instructions that you can use to troubleshoot networking issues.

## 31 July 2022

The following changes were introduced with the 3.9.21 release of the Connector.

### MTEKM license

The Multi-tenant Encryption Key Management (MTEKM) license is now included with new and existing Cloud Volumes ONTAP systems running version 9.11.1 or later.

Multi-tenant external key management enables individual storage VMs (SVMs) to maintain their own keys through a KMIP server when using NetApp Volume Encryption.

[Learn how to encrypt volumes with NetApp encryption solutions.](#)

### Proxy server

BlueXP now automatically configures your Cloud Volumes ONTAP systems to use the Connector as a proxy server, if an outbound internet connection isn't available to send AutoSupport messages.

AutoSupport proactively monitors the health of your system and sends messages to NetApp technical support.

The only requirement is to ensure that the Connector's security group allows *inbound* connections over port 3128. You'll need to open this port after you deploy the Connector.

### Change charging method

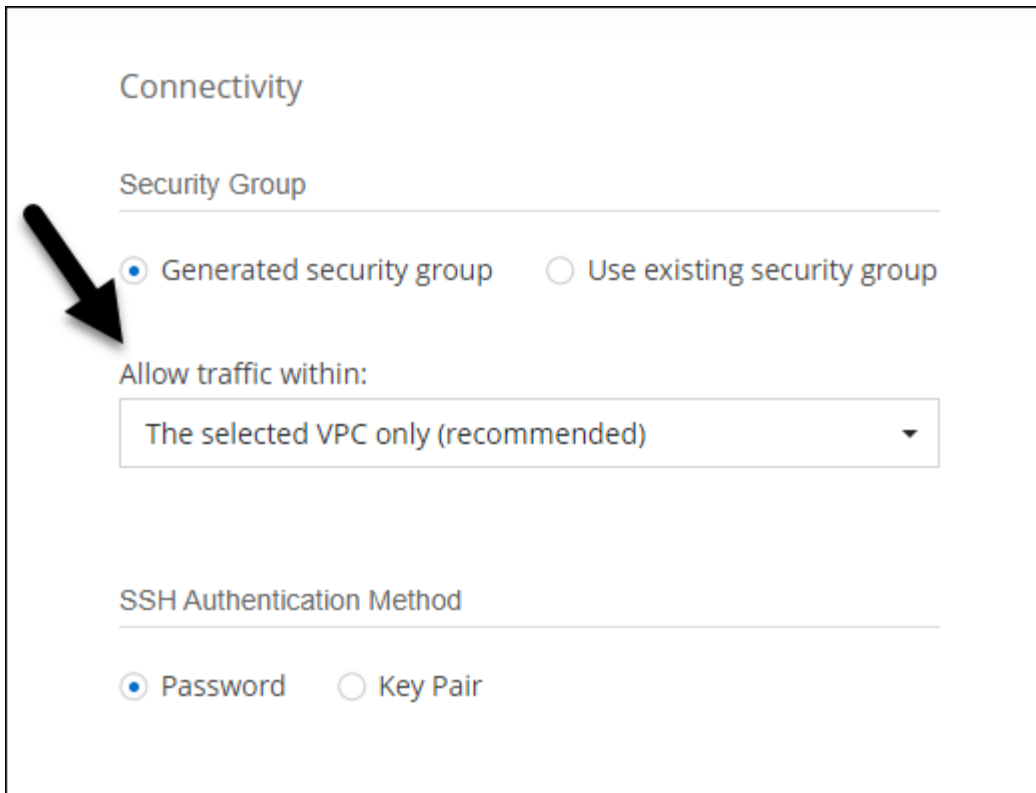
You can now change the charging method for a Cloud Volumes ONTAP system that uses capacity-based licensing. For example, if you deployed a Cloud Volumes ONTAP system with the Essentials package, you can change it to the Professional package if your business needs changed. This feature is available from the Digital Wallet.

[Learn how to change charging methods.](#)

### Security group enhancement

When you create a Cloud Volumes ONTAP working environment, the user interface now enables you to choose whether you want the predefined security group to allow traffic within the selected network only (recommended) or all networks.





Connectivity

Security Group

☒ Generated security group ☐ Use existing security group

Allow traffic within:

The selected VPC only (recommended) ▼

SSH Authentication Method

☒ Password ☐ Key Pair

## 18 July 2022

### New licensing packages in Azure

Two new capacity-based licensing packages are available for Cloud Volumes ONTAP in Azure when you pay through an Azure Marketplace subscription:

- **Optimized:** Pay for provisioned capacity and I/O operations separately
- **Edge Cache:** Licensing for [Cloud Volumes Edge Cache](#)

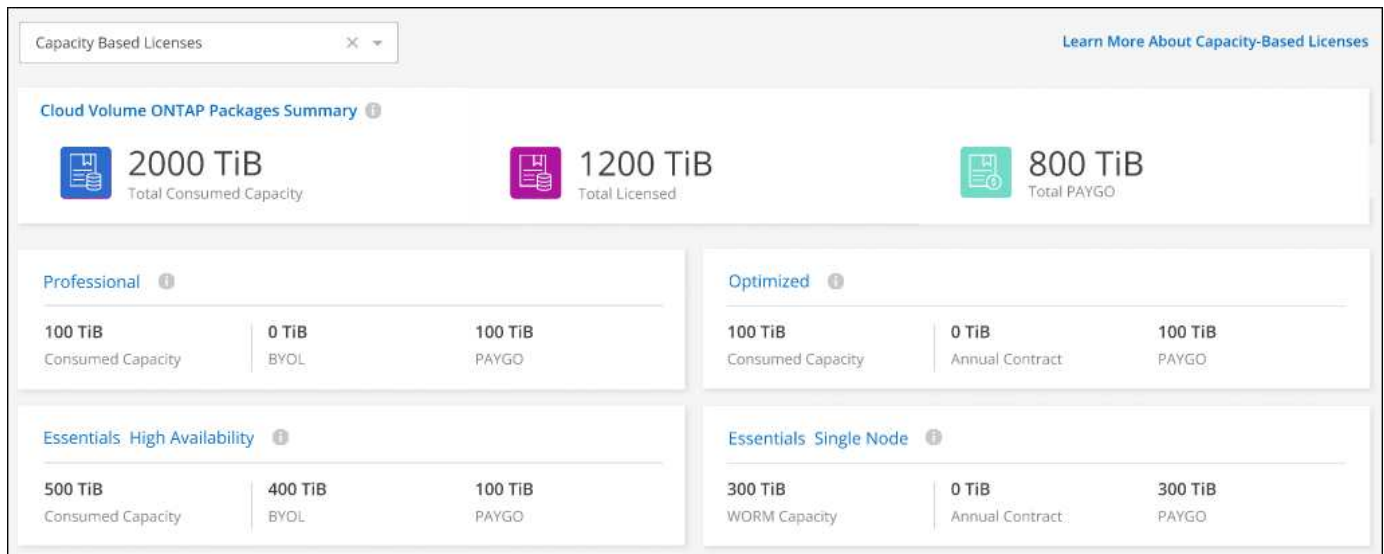
[Learn more about these licensing packages.](#)

## 3 July 2022

The following changes were introduced with the 3.9.20 release of the Connector.

### Digital Wallet

The Digital Wallet now shows you the total consumed capacity in your account and the consumed capacity by licensing package. This can help you understand how you're being charged and whether you need to purchase additional capacity.



## Elastic Volumes enhancement

BlueXP now supports the Amazon EBS Elastic Volumes feature when creating a Cloud Volumes ONTAP working environment from the user interface. The Elastic Volumes feature is enabled by default when using gp3 or io1 disks. 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.](#)

## ONTAP S3 license in AWS

An ONTAP S3 license is now included on new and existing Cloud Volumes ONTAP systems running version 9.11.0 or later in AWS.

[Learn how to configure and manage S3 object storage services in ONTAP](#)

## New Azure Cloud region support

Starting with the 9.10.1 release, Cloud Volumes ONTAP is now supported in the Azure West US 3 region.

[View the full list of supported regions for Cloud Volumes ONTAP](#)

## ONTAP S3 license in Azure

An ONTAP S3 license is now included on new and existing Cloud Volumes ONTAP systems running version 9.9.1 or later in Azure.

[Learn how to configure and manage S3 object storage services in ONTAP](#)

## 7 June 2022

The following changes were introduced with the 3.9.19 release of the Connector.

### Cloud Volumes ONTAP 9.11.1

BlueXP can now deploy and manage Cloud Volumes ONTAP 9.11.1, which includes support for new features and additional cloud provider regions.

[Learn about the new features included in this release of Cloud Volumes ONTAP](#)

## New Advanced View

If you need to perform advanced management of Cloud Volumes ONTAP, you can do so using ONTAP System Manager, which is a management interface that's provided with an ONTAP system. We have included the System Manager interface directly inside BlueXP so that you don't need to leave BlueXP for advanced management.

This Advanced View is available as a Preview with Cloud Volumes ONTAP 9.10.0 and later. We plan to refine this experience and add enhancements in upcoming releases. Please send us feedback by using the in-product chat.

[Learn more about the Advanced View.](#)

## Support for Amazon EBS Elastic Volumes

Support for the Amazon EBS Elastic Volumes feature with a Cloud Volumes ONTAP aggregate provides better performance and additional capacity, while enabling BlueXP to automatically increase the underlying disk capacity as needed.

Support for Elastic Volumes is available starting with *new* Cloud Volumes ONTAP 9.11.0 systems and with gp3 and io1 EBS disk types.

[Learn more about support for Elastic Volumes.](#)

Note that support for Elastic Volumes requires new AWS permissions for the Connector:

```
"ec2:DescribeVolumesModifications",  
"ec2:ModifyVolume",
```

Be sure to provide these permissions to each set of AWS credentials that you've added to BlueXP. [View the latest Connector policy for AWS.](#)

## Support for deploying HA pairs in shared AWS subnets

Cloud Volumes ONTAP 9.11.1 includes support for AWS VPC sharing. This release of the Connector enables you to deploy an HA pair in an AWS shared subnet when using the API.

[Learn how to deploy an HA pair in a shared subnet.](#)

## Limited network access when using service endpoints

BlueXP now limits network access when using a VNet service endpoint for connections between Cloud Volumes ONTAP and storage accounts. BlueXP uses a service endpoint if you disable Azure Private Link connections.

[Learn more about Azure Private Link connections with Cloud Volumes ONTAP.](#)

## Support for creating storage VMs in Google Cloud

Multiple storage VMs are now supported with Cloud Volumes ONTAP in Google Cloud, starting with the 9.11.1 release. Starting with this release of the Connector, BlueXP enables you to create storage VMs on Cloud

Volumes ONTAP HA pairs in Google Cloud by using the API.

Support for creating storage VMs requires new Google Cloud permissions for the Connector:

- `compute.instanceGroups.get`
- `compute.addresses.get`

Note that you must use the ONTAP CLI or System Manager to create a storage VM on a single node system.

- [Learn more about storage VM limits in Google Cloud](#)
- [Learn how to create data-serving storage VMs for Cloud Volumes ONTAP in Google Cloud](#)

## 2 May 2022

The following changes were introduced with the 3.9.18 release of the Connector.

### Cloud Volumes ONTAP 9.11.0

BlueXP can now deploy and manage Cloud Volumes ONTAP 9.11.0.

[Learn about the new features included in this release of Cloud Volumes ONTAP.](#)

### Enhancement to mediator upgrades

When BlueXP upgrades the mediator for an HA pair, it now validates that a new mediator image is available before it deletes the boot disk. This change ensures that the mediator can continue to operate successfully if the upgrade process is unsuccessful.

### K8s tab has been removed

The K8s tab was deprecated in a previous and has now been removed. If you want to use Kubernetes with Cloud Volumes ONTAP, you can add managed-Kubernetes clusters to the Canvas as a working environment for advanced data management.

[Learn about Kubernetes data management in BlueXP](#)

### Annual contract in Azure

The Essentials and Professional packages are now available in Azure through an annual contract. You can contact your NetApp sales representative to purchase an annual contract. The contract is available as a private offer in the Azure Marketplace.

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

[Learn more about licensing.](#)

### S3 Glacier Instant Retrieval

You can now store tiered data in the Amazon S3 Glacier Instant Retrieval storage class.

[Learn how to change the storage class for tiered data.](#)

## New AWS permissions required for the Connector

The following permissions are now required to create an AWS spread placement group when deploying an HA pair in a single Availability Zone (AZ):

```
"ec2:DescribePlacementGroups",  
"iam:GetRolePolicy",
```

These permissions are now required to optimize how BlueXP creates the placement group.

Be sure to provide these permissions to each set of AWS credentials that you've added to BlueXP. [View the latest Connector policy for AWS.](#)

## New Google Cloud region support

Cloud Volumes ONTAP is now supported in the following Google Cloud regions starting with the 9.10.1 release:

- Delhi (asia-south2)
- Melbourne (australia-southeast2)
- Milan (europe-west8) - single node only
- Santiago (southamerica-west1) - single node only

[View the full list of supported regions for Cloud Volumes ONTAP](#)

## Support for n2-standard-16 in Google Cloud

The n2-standard-16 machine type is now supported with Cloud Volumes ONTAP in Google Cloud, starting with the 9.10.1 release.

[View supported configurations for Cloud Volumes ONTAP in Google Cloud](#)

## Enhancements to Google Cloud firewall policies

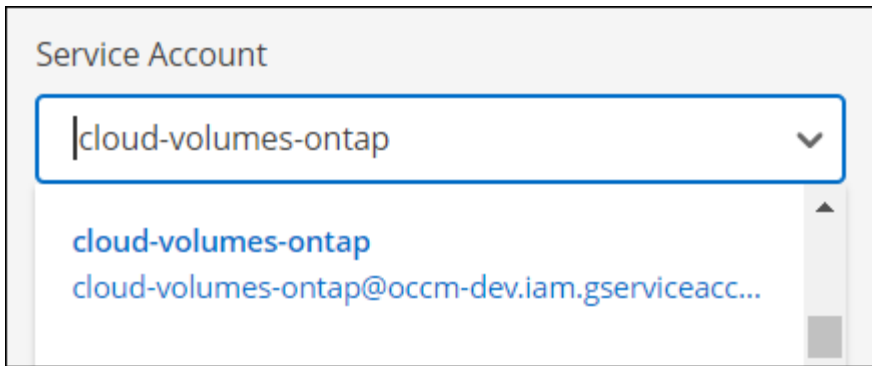
- When you create a Cloud Volumes ONTAP HA pair in Google Cloud, BlueXP will now display all existing firewall policies in a VPC.

Previously, BlueXP wouldn't display any policies in VPC-1, VPC-2, or VPC-3 that didn't have a target tag.

- When you create a Cloud Volumes ONTAP single node system in Google Cloud, you can now choose whether you want the predefined firewall policy to allow traffic within the selected VPC only (recommended) or all VPCs.

## Enhancement to Google Cloud service accounts

When you select the Google Cloud service account to use with Cloud Volumes ONTAP, BlueXP now displays the email address that's associated with each service account. Viewing the email address can make it easier to distinguish between service accounts that share the same name.



## 3 April 2022

### System Manager link has been removed

We have removed the System Manager link that was previously available from within a Cloud Volumes ONTAP working environment.

You can still connect to System Manager by entering the cluster management IP address in a web browser that has a connection to the Cloud Volumes ONTAP system. [Learn more about connecting to System Manager.](#)

### Charging for WORM storage

Now that the introductory special rate has expired, you will now be charged for using WORM storage. Charging is hourly, according to the total provisioned capacity of WORM volumes. This applies to new and existing Cloud Volumes ONTAP systems.

[Learn about pricing for WORM storage.](#)

## 27 February 2022

The following changes were introduced with the 3.9.16 release of the Connector.

### Redesigned volume wizard

The create new volume wizard that we recently introduced is now available when creating a volume on a specific aggregate from the **Advanced allocation** option.

[Learn how to create volumes on a specific aggregate.](#)

## 9 February 2022

### Marketplace updates

- The Essentials package and Professional package are now available in all cloud provider marketplaces.

These by-capacity charging methods enable you to pay by the hour or to purchase an annual contract directly from your cloud provider. You still have the option to purchase a by-capacity license directly from NetApp.

If you have an existing subscription in a cloud marketplace, you're automatically subscribed to these new offerings as well. You can choose by-capacity charging when you deploy a new Cloud Volumes ONTAP working environment.

If you're a new customer, BlueXP will prompt you to subscribe when you create a new working environment.

- By-node licensing from all cloud provider marketplaces is deprecated and no longer available for new subscribers. This includes annual contracts and hourly subscriptions (Explore, Standard, and Premium).

This charging method is still available for existing customers who have an active subscription.

[Learn more about the licensing options for Cloud Volumes ONTAP.](#)

## 6 February 2022

### Exchange unassigned licenses

If you have an unassigned node-based license for Cloud Volumes ONTAP that you haven't used, you can now exchange the license by converting it to a Cloud Backup license, Cloud Data Sense license, or Cloud Tiering license.

This action revokes the Cloud Volumes ONTAP license and creates a dollar-equivalent license for the service with the same expiry date.

[Learn how to exchange unassigned node-based licenses.](#)

## 30 January 2022

The following changes were introduced with the 3.9.15 release of the Connector.

### Redesigned licensing selection

We redesigned the licensing selection screen when creating a new Cloud Volumes ONTAP working environment. The changes highlight the by-capacity charging methods that were introduced in July 2021 and support upcoming offerings through the cloud provider marketplaces.

### Digital Wallet update

We updated the **Digital Wallet** by consolidating Cloud Volumes ONTAP licenses in a single tab.

## 2 January 2022

The following changes were introduced with the 3.9.14 release of the Connector.

### Support for additional Azure VM types

Cloud Volumes ONTAP is now supported with the following VM types in Microsoft Azure, starting with the 9.10.1 release:

- E4ds\_v4
- E8ds\_v4
- E32ds\_v4
- E48ds\_v4

Go to the [Cloud Volumes ONTAP Release Notes](#) for more details about supported configurations.

## FlexClone charging update

If you use a [capacity-based license](#) for Cloud Volumes ONTAP, you are no longer charged for the capacity used by FlexClone volumes.

## Charging method now displayed

BlueXP now shows the charging method for each Cloud Volumes ONTAP working environment in the right panel of the Canvas.



## Choose your user name

When you create a Cloud Volumes ONTAP working environment, you now have the option to enter your preferred user name, instead of the default admin user name.



Credentials

User Name

customusername

Password

.....

Confirm Password

.....

## Volume creation enhancements

We made a few enhancements to volume creation:

- We redesigned the create volume wizard for ease of use.
- Tags that you add to a volume are now associated with the Application Templates service, which can help you organize and simplify the management of your resources.
- You can now choose a custom export policy for NFS.

✓ Details, Protection & Tags

2 Protocol

3 Disk Type

4 Usage Profile & Tiering Policy

5 Review

Volumes Protocol

Select the volume's protocol: ☒ NFS Protocol ☐ CIFS Protocol ☐ iSCSI Protocol

Access Control

Custom export policy

Export Policy (1 rule defined)

Manage volume's export policy

## 28 November 2021

The following changes were introduced with the 3.9.13 release of the Connector.

### Cloud Volumes ONTAP 9.10.1

BlueXP can now deploy and manage Cloud Volumes ONTAP 9.10.1.

[Learn about the new features included in this release of Cloud Volumes ONTAP.](#)

## Keystone Flex Subscriptions

You can now use Keystone Flex Subscriptions to pay for Cloud Volumes ONTAP HA pairs.

A Keystone Flex Subscription is a pay-as-you-grow subscription-based service that delivers a seamless hybrid cloud experience for those preferring OpEx consumption models to upfront CapEx or leasing.

A Keystone Flex Subscription is supported with all new versions of Cloud Volumes ONTAP that you can deploy from BlueXP.

- [Learn more about Keystone Flex Subscriptions.](#)
- [Learn how to get started with Keystone Flex Subscriptions in BlueXP.](#)

## New AWS region support

Cloud Volumes ONTAP is now supported in the AWS Asia Pacific (Osaka) region (ap-northeast-3).

## Port reduction

Ports 8023 and 49000 are no longer open on Cloud Volumes ONTAP systems in Azure for both single node systems and HA pairs.

This change applies to *new* Cloud Volumes ONTAP systems starting with the 3.9.13 release of the Connector.

## 4 October 2021

The following changes were introduced with the 3.9.11 release of the Connector.

### Cloud Volumes ONTAP 9.10.0

BlueXP can now deploy and manage Cloud Volumes ONTAP 9.10.0.

[Learn about the new features included in this release of Cloud Volumes ONTAP.](#)

## Reduced deployment time

We reduced the amount of time that it takes to deploy a Cloud Volumes ONTAP working environment in Microsoft Azure or in Google Cloud when normal write speed is enabled. The deployment time is now 3-4 minutes shorter on average.

## 2 September 2021

The following changes were introduced with the 3.9.10 release of the Connector.

### Customer-managed encryption 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 now use your own customer-managed encryption key instead by completing the following steps:

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

[Learn more about these steps.](#)

## 7 July 2021

The following changes were introduced with the 3.9.8 release of the Connector.

### New charging methods

New charging methods are available for Cloud Volumes ONTAP.

- **Capacity-based BYOL:** A capacity-based license enables you to pay for Cloud Volumes ONTAP per TiB of capacity. The license is associated with your NetApp account and enables you to create as multiple Cloud Volumes ONTAP systems, as long as enough capacity is available through your license. Capacity-based licensing is available in the form of a package, either *Essentials* or *Professional*.
- **Freemium offering:** Freemium enables you to use all Cloud Volumes ONTAP features free of charge from NetApp (cloud provider charges still apply). You're limited to 500 GiB of provisioned capacity per system and there's no support contract. You can have up to 10 Freemium systems.


[Learn more about these licensing options.](#)

Here's an example of the charging methods that you can choose from:


### Cloud Volumes ONTAP Charging Methods

[Learn more about our charging methods](#)

---

☐ Pay-As-You-Go by the hour

---

☒ Bring your own license


Bring your own license type

Capacity-Based

Package

Professional

---

☐ Freemium (Up to 500GB)

---

### WORM storage available for general use

Write once, read many (WORM) storage is no longer in Preview and is now available for general use with Cloud Volumes ONTAP. [Learn more about WORM storage.](#)

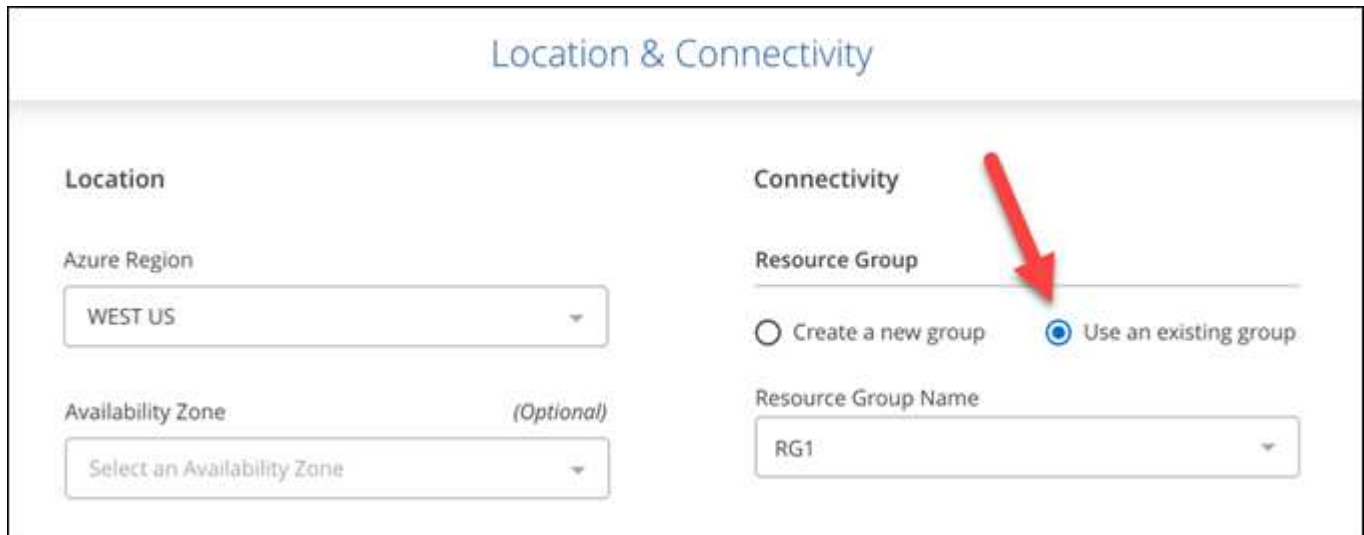
## Support for m5dn.24xlarge in AWS

Starting with the 9.9.1 release, Cloud Volumes ONTAP now supports the m5dn.24xlarge instance type with the following charging methods: PAYGO Premium, bring your own license (BYOL), and Freemium.

[View supported configurations for Cloud Volumes ONTAP in AWS.](#)

## Select existing Azure resource groups

When creating a Cloud Volumes ONTAP system in Azure, you now have the option to select an existing resource group for the VM and its associated resources.



The screenshot shows the 'Location & Connectivity' configuration page. Under 'Location', 'Azure Region' is 'WEST US' and 'Availability Zone' is 'Select an Availability Zone' (Optional). Under 'Connectivity', the 'Resource Group' section has two radio buttons: 'Create a new group' and 'Use an existing group'. A red arrow points to the 'Use an existing group' option, which is selected. Below this, the 'Resource Group Name' is 'RG1'.

The following permissions enable BlueXP to remove Cloud Volumes ONTAP resources from a resource group, in case of deployment failure or deletion:

```
"Microsoft.Network/privateEndpoints/delete",  
"Microsoft.Compute/availabilitySets/delete",
```

Be sure to provide these permissions to each set of Azure credentials that you've added to BlueXP. [View the latest Connector policy for Azure.](#)

## Blob public access now disabled in Azure

As a security enhancement, BlueXP now disables **Blob public access** when creating a storage account for Cloud Volumes ONTAP.

## Azure Private Link enhancement

By default, BlueXP now enables an Azure Private Link connection on the boot diagnostics storage account for new Cloud Volumes ONTAP systems.

This means *all* storage accounts for Cloud Volumes ONTAP will now use a private link.

[Learn more about using an Azure Private Link with Cloud Volumes ONTAP.](#)

## Balanced persistent disks in Google Cloud

Starting with the 9.9.1 release, Cloud Volumes ONTAP now supports Balanced persistent disks (pd-balanced).

These SSDs balance performance and cost by providing lower IOPS per GiB.

## custom-4-16384 no longer supported in Google Cloud

The custom-4-16384 machine type is no longer supported with new Cloud Volumes ONTAP systems.

If you have an existing system running on this machine type, you can keep using it, but we recommend switching to the n2-standard-4 machine type.

[View supported configurations for Cloud Volumes ONTAP in GCP.](#)

## 30 May 2021

The following changes were introduced with the 3.9.7 release of the Connector.

### New Professional Package in AWS

A new Professional Package enables you to bundle Cloud Volumes ONTAP and Cloud Backup Service by using an annual contract from the AWS Marketplace. Payment is per TiB. This subscription doesn't enable you to back up on-prem data.

If you choose this payment option, you can provision up to 2 PiB per Cloud Volumes ONTAP system through EBS disks and tiering to S3 object storage (single node or HA).

Go to the [AWS Marketplace page](#) to view pricing details and go to the [Cloud Volumes ONTAP Release Notes](#) to learn more about this licensing option.

### Tags on EBS volumes in AWS

BlueXP now adds tags to EBS volumes when it creates a new Cloud Volumes ONTAP working environment. The tags were previously created after Cloud Volumes ONTAP was deployed.

This change can help if your organization uses service control policies (SCPs) to manage permissions.

### Minimum cooling period for auto tiering policy

If you enabled data tiering on a volume using the *auto* tiering policy, you can now adjust the minimum cooling period using the API.

[Learn how to adjust the minimum cooling period.](#)

### Enhancement to custom export policies

When you create a new NFS volume, BlueXP now displays custom export policies in ascending order, making it easier for you to find the export policy that you need.

### Deletion of old cloud snapshots

BlueXP now deletes older cloud snapshots of root and boot disks that are created when a Cloud Volumes ONTAP system is deployed and every time its powered down. Only the two most recent snapshots are retained for both the root and boot volumes.

This enhancement helps reduce cloud provider costs by removing snapshots that are no longer needed.

Note that a Connector requires a new permission to delete Azure snapshots. [View the latest Connector policy for Azure.](#)

```
"Microsoft.Compute/snapshots/delete"
```

## 24 May 2021

### Cloud Volumes ONTAP 9.9.1

BlueXP can now deploy and manage Cloud Volumes ONTAP 9.9.1.

[Learn about the new features included in this release of Cloud Volumes ONTAP.](#)

## 11 Apr 2021

The following changes were introduced with the 3.9.5 release of the Connector.

### Logical space reporting

BlueXP now enables logical space reporting on the initial storage VM that it creates for Cloud Volumes ONTAP.

When space is reported logically, ONTAP reports the volume space such that all the physical space saved by the storage efficiency features are also reported as used.

### Support for gp3 disks in AWS

Cloud Volumes ONTAP now supports *General Purpose SSD (gp3)* disks, starting with the 9.7 release. gp3 disks are the lowest-cost SSDs that balance cost and performance for a broad range of workloads.

[Learn more about using gp3 disks with Cloud Volumes ONTAP.](#)

### Cold HDD disks no longer supported in AWS

Cloud Volumes ONTAP no longer supports Cold HDD (sc1) disks.

### TLS 1.2 for Azure storage accounts

When BlueXP creates storage accounts in Azure for Cloud Volumes ONTAP, the TLS version for the storage account is now version 1.2.

## 8 Mar 2021

The following changes were introduced with the 3.9.4 release of the Connector.

### Cloud Volumes ONTAP 9.9.0

BlueXP can now deploy and manage Cloud Volumes ONTAP 9.9.0.

[Learn about the new features included in this release of Cloud Volumes ONTAP.](#)

## Support for the AWS C2S environment

You can now deploy Cloud Volumes ONTAP 9.8 in the AWS Commercial Cloud Services (C2S) environment.

[Learn how to get started in C2S.](#)

## AWS encryption with customer-managed CMKs

BlueXP has always enabled you to encrypt Cloud Volumes ONTAP data using the AWS Key Management Service (KMS). Starting with Cloud Volumes ONTAP 9.9.0, data on EBS disks and data tiered to S3 are encrypted if you select a customer-managed CMK. Previously, only EBS data would be encrypted.

Note that you'll need to provide the Cloud Volumes ONTAP IAM role with access to use the CMK.

[Learn more about setting up the AWS KMS with Cloud Volumes ONTAP.](#)

## Support for Azure DoD

You can now deploy Cloud Volumes ONTAP 9.8 in the Azure Department of Defense (DoD) Impact Level 6 (IL6).

## IP address reduction in Google Cloud

We've reduced the number of IP addresses that are required for Cloud Volumes ONTAP 9.8 and later in Google Cloud. By default, one less IP address is required (we unified the intercluster LIF with the node management LIF). You also have the option to skip the creation of the SVM management LIF when using the API, which would reduce the need for an additional IP address.

[Learn more about IP address requirements in Google Cloud.](#)

## Shared VPC support in Google Cloud

When you deploy a Cloud Volumes ONTAP HA pair in Google Cloud, you can now choose shared VPCs for VPC-1, VPC-2, and VPC-3. Previously, only VPC-0 could be a shared VPC. This change is supported with Cloud Volumes ONTAP 9.8 and later.

[Learn more about Google Cloud networking requirements.](#)

## 4 Jan 2021

The following changes were introduced with the 3.9.2 release of the Connector.

### AWS Outposts

A few months ago, we announced that Cloud Volumes ONTAP had achieved the Amazon Web Services (AWS) Outposts Ready designation. Today, we're pleased to announce that we've validated BlueXP and Cloud Volumes ONTAP with AWS Outposts.

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

There are a few limitations to point out:

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

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

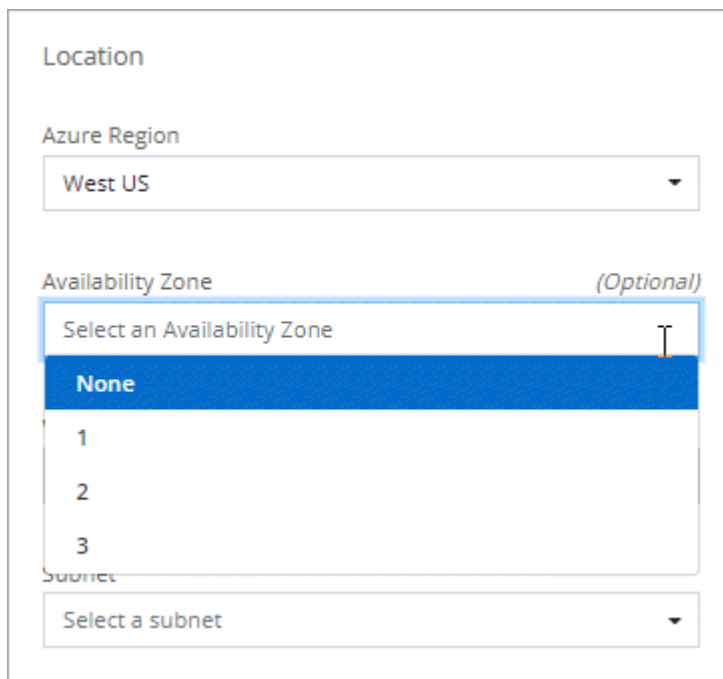
### Ultra SSD VNVRAM in supported Azure regions

Cloud Volumes ONTAP can now use an Ultra SSD as VNVRAM when you use the E32s\_v3 VM type with a single node system [in any supported Azure region](#).

VNVRAM provides better write performance.

### Choose an Availability Zone in Azure

You can now choose the Availability Zone in which you'd like to deploy a single node Cloud Volumes ONTAP system. If you don't select an AZ, BlueXP will select one for you.



The screenshot shows a configuration form for Azure. Under the 'Location' section, the 'Azure Region' is set to 'West US'. Below this, the 'Availability Zone' section is marked as '(Optional)'. A dropdown menu is open, showing the text 'Select an Availability Zone'. The menu options are 'None' (highlighted in blue), '1', '2', and '3'. Below the dropdown, there is a 'Subnet' dropdown menu with the text 'Select a subnet'.

### Larger disks in Google Cloud

Cloud Volumes ONTAP now supports 64 TB disks in GCP.



The maximum system capacity with disks alone remains at 256 TB due to GCP limits.

### New machine types in Google Cloud

Cloud Volumes ONTAP now supports the following machine types:

- n2-standard-4 with the Explore license and with BYOL
- n2-standard-8 with the Standard license and with BYOL
- n2-standard-32 with the Premium license and with BYOL



**3 Nov 2020**

The following changes were introduced with the 3.9.0 release of the Connector.

### **Azure Private Link for Cloud Volumes ONTAP**

By default, BlueXP now enables an Azure Private Link connection between Cloud Volumes ONTAP and its associated storage accounts. A Private Link secures connections between endpoints in Azure.

- [Learn more about Azure Private Links](#)
- [Learn more about using an Azure Private Link with Cloud Volumes ONTAP](#)

## **Known limitations**

Known limitations identify platforms, devices, or functions that are not supported by this release of the product, or that do not interoperate correctly with it. Review these limitations carefully.

These limitations are specific to Cloud Volumes ONTAP management in BlueXP (formerly Cloud Manager). To view limitations with the Cloud Volumes ONTAP software itself, [go to the Cloud Volumes ONTAP Release Notes](#)

### **BlueXP doesn't support FlexGroup volumes**

While Cloud Volumes ONTAP supports FlexGroup volumes, BlueXP does not. If you create a FlexGroup volume from System Manager or from the CLI, then you should set BlueXP's Capacity Management mode to Manual. Automatic mode might not work properly with FlexGroup volumes.

### **BlueXP doesn't support S3 with Cloud Volumes ONTAP**

While Cloud Volumes ONTAP supports S3 as an option for scale-out storage in some cloud providers, BlueXP doesn't provide any management capabilities for this feature. Using the CLI is the best practice to configure S3 client access from Cloud Volumes ONTAP. For details, refer to the [S3 Configuration Power Guide](#).

[Learn more about Cloud Volumes ONTAP support for S3 and other client protocols.](#)

### **BlueXP doesn't support disaster recovery for storage VMs**

BlueXP doesn't provide any setup or orchestration support for storage VM disaster recovery. You must use System Manager or the CLI.

- [SVM Disaster Recovery Preparation Express Guide](#)
- [SVM Disaster Recovery Express Guide](#)

## **Cloud Volumes ONTAP Release Notes**

The Release Notes for Cloud Volumes ONTAP provide release-specific information. What's new in the release, supported configurations, storage limits, and any known limitations or issues that can affect product functionality.



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

[Learn more about Cloud Backup](#)

- 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 Cloud Data Sense helps you understand data context and identify sensitive data.

[Learn more about Cloud Data Sense](#)



Licenses for ONTAP features are included with Cloud Volumes ONTAP.

[View supported Cloud Volumes ONTAP configurations](#)

## Supported versions for new deployments

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

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

### AWS

#### Single node

- 9.13.0
- 9.12.1 GA
- 9.12.1 RC1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9.8
- 9.7 P5
- 9.5 P6

#### HA pair

- 9.13.0
- 9.12.1 GA
- 9.12.1 RC1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9.8
- 9.7 P5
- 9.5 P6

### Azure

#### Single node

- 9.13.0
- 9.12.1 GA
- 9.12.1 RC1
- 9.11.1 P3

- 9.10.1 P3
- 9.9.1 P8
- 9.9.1 P7
- 9.8 P10
- 9.7 P6
- 9.5 P6

#### **HA pair**

- 9.13.0
- 9.12.1 GA
- 9.12.1 RC1
- 9.11.1 P3
- 9.10.1 P3
- 9.9.1 P8
- 9.9.1 P7
- 9.8 P10
- 9.7 P6

## **Google Cloud**

#### **Single node**

- 9.13.0
- 9.12.1 GA
- 9.12.1 RC1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9.8
- 9.7 P5

#### **HA pair**

- 9.13.0
- 9.12.1 GA
- 9.12.1 RC1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9.8

# Get started in Amazon Web Services

## Quick start for Cloud Volumes ONTAP in AWS

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

1

### Create a Connector

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

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

2

### Plan your configuration

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

3

### Set up your networking

- a. Ensure that your VPC and subnets will support connectivity between the Connector and Cloud Volumes ONTAP.
- b. Enable outbound internet access from the target VPC for NetApp AutoSupport.

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

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

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

[Learn more about networking requirements.](#)

4

### Set up the AWS KMS

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

5

### Launch Cloud Volumes ONTAP using BlueXP

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

## Related links

- [Creating a Connector from BlueXP](#)
- [Launching a Connector from the AWS Marketplace](#)
- [Installing the Connector software on a Linux host](#)
- [What BlueXP does with AWS permissions](#)

## Plan your Cloud Volumes ONTAP configuration in AWS

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

### Choose a Cloud Volumes ONTAP license

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

- [Learn about licensing options for Cloud Volumes ONTAP](#)
- [Learn how to set up licensing](#)

### Choose a supported region

Cloud Volumes ONTAP is supported in most AWS regions. [View the full list of supported regions.](#)

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

### Choose a supported instance

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

### [Supported configurations for Cloud Volumes ONTAP in AWS](#)

### Understand storage limits

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

### [Storage limits for Cloud Volumes ONTAP in AWS](#)

### Size your system in AWS

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

#### Instance type

- Match your workload requirements to the maximum throughput and IOPS for each EC2 instance type.
- If several users write to the system at the same time, choose an instance type that has enough CPUs to manage the requests.

- If you have an application that is mostly reads, then choose a system with enough RAM.
  - [AWS Documentation: Amazon EC2 Instance Types](#)
  - [AWS Documentation: Amazon EBS–Optimized Instances](#)

## EBS disk type

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

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

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

Note that Cloud Volumes ONTAP supports the Amazon EBS Elastic Volumes feature with gp3 disks. [Learn more about Elastic Volumes support](#).

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

Note that Cloud Volumes ONTAP supports the Amazon EBS Elastic Volumes feature with io1 disks. [Learn more about Elastic Volumes support](#).

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



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

## EBS disk size

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

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

For more details about EBS disk performance, refer to [AWS Documentation: EBS Volume Types](#).

As noted above, choosing a disk size is not supported with Cloud Volumes ONTAP configurations that



support the Amazon EBS Elastic Volumes feature. [Learn more about Elastic Volumes support.](#)

## View default system disks

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

[View the default disks for Cloud Volumes ONTAP system data in AWS.](#)



The Connector also requires a system disk. [View details about the Connector's default configuration.](#)

## Prepare to deploy Cloud Volumes ONTAP in an AWS Outpost

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

There are a few limitations to point out:

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

## Collect networking information

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

### Single node or HA pair in a single AZ

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

### HA pair in multiple AZs

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

AWS information	Your value
Node 1 availability zone	
Node 1 subnet	
Node 2 availability zone	
Node 2 subnet	
Mediator availability zone	
Mediator subnet	
Key pair for the mediator	
Floating IP address for cluster management port	
Floating IP address for data on node 1	
Floating IP address for data on node 2	
Route tables for floating IP addresses	

### Choose a write speed

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

### Choose a volume usage profile

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

NetApp storage efficiency features provide the following benefits:

#### Thin provisioning

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

#### Deduplication

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

#### Compression

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

## Set up your networking

### Networking requirements for Cloud Volumes ONTAP in AWS

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

#### General requirements

The following requirements must be met in AWS.

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

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

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

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

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

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

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

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

If BlueXP notifies you that AutoSupport messages can't be sent, [troubleshoot your AutoSupport configuration](#).

#### Outbound internet access for the HA mediator

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

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

#### Private IP addresses

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

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

### **IP addresses for a single node system**

BlueXP allocates 6 IP addresses to a single node system:

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

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

### **IP addresses for HA pairs**

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



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

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

### LIFs for HA pairs in a single AZ

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

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

### LIFs for HA pairs in multiple AZs

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



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

### Security groups

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



Looking for information about the Connector? [View security group rules for the Connector](#)

## Connection for data tiering

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

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

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

## Connections to ONTAP systems

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

## DNS and Active Directory for CIFS

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

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

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

## VPC sharing

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

[Learn how to deploy an HA pair in a shared subnet.](#)

## Requirements for HA pairs in multiple AZs

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

To understand how HA pairs work, see [High-availability pairs](#).

## Availability Zones

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

A subnet should be available in each Availability Zone.

### Floating IP addresses for NAS data and cluster/SVM management

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

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



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

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

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

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



## AWS region



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

### Transit gateway to enable floating IP access from outside the VPC

If needed, [set up an AWS transit gateway](#) to enable access to an HA pair's floating IP addresses from outside the VPC where the HA pair resides.

### Route tables

After you specify the floating IP addresses in BlueXP, you are then prompted to select the route tables that should include routes to the floating IP addresses. This enables client access to the HA pair.

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

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

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

For more information about route tables, refer to [AWS Documentation: Route Tables](#).

### Connection to NetApp management tools

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

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

### Example HA configuration

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



#### Requirements for the Connector

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

- [View networking requirements for the Connector](#)
- [Security group rules in AWS](#)

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

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

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

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

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

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



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

## Steps

1. [Create a transit gateway and attach the VPCs to the gateway.](#)
2. Associate the VPCs with the transit gateway route table.
  - a. In the **VPC** service, click **Transit Gateway Route Tables**.
  - b. Select the route table.
  - c. Click **Associations** and then select **Create association**.
  - d. Choose the attachments (the VPCs) to associate and then click **Create association**.
3. Create routes in the transit gateway's route table by specifying the HA pair's floating IP addresses.

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

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

#### 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-0ea8ee291c7aedd3

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

<input type="checkbox"/>	CIDR	Attachment	Resource type	Route type	Route state
<input type="checkbox"/>	10.100.0.0/16	tgw-attach-05e77bd34e2ff91f8   vpc-0b2bc30e0dc8e0db1	VPC2	propagated	active
<input type="checkbox"/>	10.160.0.0/20	tgw-attach-00eba3eac3250d7db   vpc-673ae603	VPC1	propagated	active
<input type="checkbox"/>	172.23.0.1/32	tgw-attach-00eba3eac3250d7db   vpc-673ae603	VPC	static	active
<input type="checkbox"/>	172.23.0.2/32	tgw-attach-00eba3eac3250d7db   vpc-673ae603	VPC	static	active
<input type="checkbox"/>	172.23.0.3/32	tgw-attach-00eba3eac3250d7db   vpc-673ae603	VPC	static	active
<input type="checkbox"/>	172.23.0.4/32	tgw-attach-00eba3eac3250d7db   vpc-673ae603	VPC	static	active

**Floating IP Addresses**

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.

Route Table: rtb-0569a1bd740ed033f

Summary Routes Subnet Associations Route Propagation Tags

Edit routes

View All routes

Destination	Target	Status	Propagated
10.100.0.0/16	local	active	No
0.0.0.0/0	lgw-07250bd01781e67df	active	No
10.160.0.0/20	tgw-015b7c249661ac279	active	No
172.23.0.1/32	tgw-015b7c249661ac279	active	No
172.23.0.2/32	tgw-015b7c249661ac279	active	No
172.23.0.3/32	tgw-015b7c249661ac279	active	No
172.23.0.4/32	tgw-015b7c249661ac279	active	No

VPC1  
Floating IP  
Addresses

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

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

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

Summary Routes Subnet Associations Route Propagation Tags

Edit routes

View All routes

Destination	Target	Status
10.160.0.0/20	local	active
pl-68a54001 (com.amazonaws.us-west-2.s3, 54.231.160.0/19, 52.218.128.0/17, 52.92.32.0/22)	vpce-cb51a0a2	active
0.0.0.0/0	lgw-b2182dd7	active
10.60.29.0/25	pcx-589c3331	active
10.100.0.0/16	tgw-015b7c249661ac279	active
10.129.0.0/20	pcx-f7e1396	active
172.23.0.1/32	eni-0854d4715559c3cdb	active
172.23.0.2/32	eni-0854d4715559c3cdb	active
172.23.0.3/32	eni-0f76681216c3108ed	active
172.23.0.4/32	eni-0854d4715559c3cdb	active

VPC2  
Floating  
IP  
Addresses

- Mount volumes to clients using the floating IP address.

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

## Volumes

2 Volumes | 0.22 TB Allocated | < 0.01 TB Used (0 TB in S3)



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

[Learn how to edit a volume.](#)

### Related links

- [High-availability pairs in AWS](#)
- [Networking requirements for Cloud Volumes ONTAP in AWS](#)

### Deploy an HA pair in a shared subnet

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

With [VPC sharing](#), a Cloud Volumes ONTAP HA configuration is spread across two accounts:

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

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

The following image shows the components involved this deployment:





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

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

### Steps

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

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

[AWS documentation: Share a subnet](#)



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

[Refer to the security group rules for Cloud Volumes ONTAP](#). Note that you don't need to create a security group for the HA mediator. BlueXP does that for you.

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

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

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

Note that you must specify the following fields:

- "securityGroupId"

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

- "assumeRoleArn" in the "haParams" object

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

For example:

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

[Learn about the Cloud Volumes ONTAP API](#)

## Security group rules for AWS

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

## Rules for Cloud Volumes ONTAP

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

### Inbound rules

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

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

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

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

## Outbound rules

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

### Basic outbound rules

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

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

### Advanced outbound rules

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



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

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

Service	Protocol	Port	Source	Destination	Purpose
AutoSupport	HTTPS	443	Node management LIF	support.netapp.com	AutoSupport (HTTPS is the default)
	HTTP	80	Node management LIF	support.netapp.com	AutoSupport (only if the transport protocol is changed from HTTPS to HTTP)
	TCP	3128	Node management LIF	Connector	Sending AutoSupport messages through a proxy server on the Connector, if an outbound internet connection isn't available
Backup to S3	TCP	5010	Intercluster LIF	Backup endpoint or restore endpoint	Back up and restore operations for the Backup to S3 feature
Cluster	All traffic	All traffic	All LIFs on one node	All LIFs on the other node	Intercluster communications (Cloud Volumes ONTAP HA only)
	TCP	3000	Node management LIF	HA mediator	ZAPI calls (Cloud Volumes ONTAP HA only)
	ICMP	1	Node management LIF	HA mediator	Keep alive (Cloud Volumes ONTAP HA only)
DHCP	UDP	68	Node management LIF	DHCP	DHCP client for first-time setup
DHCPs	UDP	67	Node management LIF	DHCP	DHCP server
DNS	UDP	53	Node management LIF and data LIF (NFS, CIFS)	DNS	DNS
NDMP	TCP	1860–18699	Node management LIF	Destination servers	NDMP copy
SMTP	TCP	25	Node management LIF	Mail server	SMTP alerts, can be used for AutoSupport
SNMP	TCP	161	Node management LIF	Monitor server	Monitoring by SNMP traps
	UDP	161	Node management LIF	Monitor server	Monitoring by SNMP traps
	TCP	162	Node management LIF	Monitor server	Monitoring by SNMP traps
	UDP	162	Node management LIF	Monitor server	Monitoring by SNMP traps
SnapMirror	TCP	11104	Intercluster LIF	ONTAP intercluster LIFs	Management of intercluster communication sessions for SnapMirror
	TCP	11105	Intercluster LIF	ONTAP intercluster LIFs	SnapMirror data transfer

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

### Rules for the HA mediator external security group

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

#### Inbound rules

The source for inbound rules is 0.0.0.0/0.

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

#### Outbound rules

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

#### Basic outbound rules

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

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

#### Advanced outbound rules

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

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



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

## Rules for the HA configuration internal security group

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

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

### Inbound rules

The predefined security group includes the following inbound rules.

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

### Outbound rules

The predefined security group includes the following outbound rules.

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

## Rules for the Connector

[View security group rules for the Connector](#)

## Setting up the AWS KMS

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

### Steps

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

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

[AWS Documentation: Customer Master Keys \(CMKs\)](#)

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

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

[AWS Documentation: Editing Keys](#)

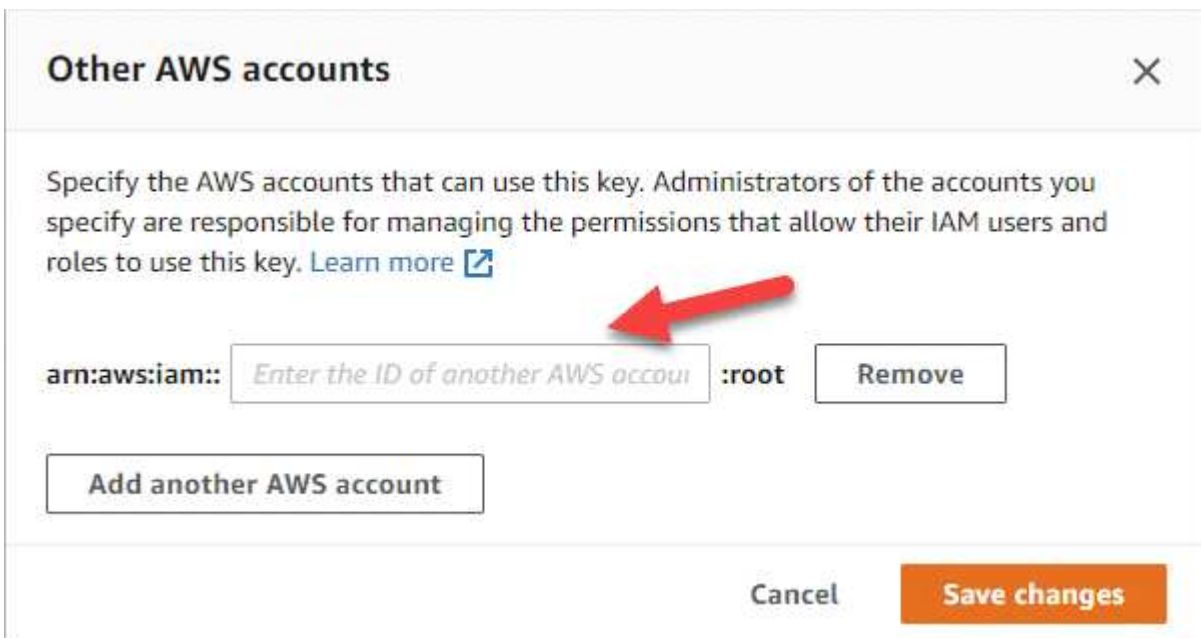
3. If the CMK is in a different AWS account, complete the following steps:
  - a. Go to the KMS console from the account where the CMK resides.
  - b. Select the key.

- c. In the **General configuration** pane, copy the ARN of the key.

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

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

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



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

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



```

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

```

For additional details about this process, see [AWS Documentation: Allowing users in other accounts to use a KMS key](#).

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

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

stored in the S3 bucket.

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

[AWS Documentation: Editing Keys](#)

## Set up IAM roles for Cloud Volumes ONTAP

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

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



Providing your own IAM role is required in the AWS Commercial Cloud Services Environment.  
[Learn how to deploy Cloud Volumes ONTAP in C2S.](#)

### Steps

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

## Standard regions

```
{
  "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"
  }]
}

```

## C2S environment

```

{
  "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"
  }]
}

```

- Backup policy for Cloud Volumes ONTAP nodes

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

## Standard regions

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

## GovCloud (US) regions

```

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

```

**C2S environment**

```

{
  "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"
    }
  ]
}

```

- 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": "*"
  }]
}
```

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

## Result

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

## More information

- [AWS documentation: Creating IAM policies](#)
- [AWS documentation: Creating IAM roles](#)

## Set up licensing for Cloud Volumes ONTAP in AWS

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

### Freemium

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

### Steps

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

You won't be charged through the marketplace subscription unless you exceed 500 GiB of provisioned

capacity, at which time the system is automatically converted to the [Essentials](#) package.

### 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 BlueXP, select **Freemium** 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.](#)

## Capacity-based license

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

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

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

[Learn more about capacity-based licensing.](#)

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

### BYOL

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

### Steps

1. [Contact NetApp Sales to obtain a license](#)
2. [Add your NetApp Support Site account to BlueXP](#)

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

Your license must be available from the Digital Wallet before you can use it with Cloud Volumes ONTAP. If needed, you can [manually add the license to the Digital Wallet](#).

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

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

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

### Select Charging Method

<input checked="" type="radio"/> Professional	By capacity	▼
<input type="radio"/> Essential	By capacity	▼
<input type="radio"/> Freemium (Up to 500 GiB)	By capacity	▼
<input type="radio"/> 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 working environment, BlueXP prompts you to subscribe to the agreement that's available in the AWS Marketplace. That subscription is then associated with the working environment for charging. You can use that same subscription for additional working environments.

### Steps

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

The screenshot shows a dialog box titled "Edit Credentials & Add Subscription". Below the title is a horizontal line. The main text reads: "Select a subscription option and click **Continue**. The AWS Marketplace enables you to view pricing details and then subscribe." Below this text are two selectable options, each in a light gray box. The first option is "Pay-Per-TiB - Annual Contract" with a radio button, and its description is "Pay for Cloud Volumes ONTAP with an annual, upfront payment." The second option is "Pay-as-you-go" with a selected radio button (indicated by a blue dot), and its description is "Pay for Cloud Volumes ONTAP at an hourly rate." Below these options is another horizontal line. Underneath is the heading "The next steps:" followed by a numbered list. Step 1 is "AWS Marketplace" with the instruction "Subscribe and then click **Set Up Your Account** to configure your account." Step 2 is "Cloud Manager" with the instruction "Save your subscription and associate the Marketplace subscription with your AWS credentials." At the bottom right of the dialog box are two buttons: a blue "Continue" button and a gray "Cancel" button.

- b. After you return to BlueXP, 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.](#)



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

### Annual contract

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

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

### Steps

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

## 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 BlueXP, 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 Flex Subscription

A Keystone Flex Subscription is a pay-as-you-grow subscription-based service. [Learn more about Keystone Flex Subscriptions.](#)

### Steps

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

The screenshot shows a 'Select Charging Method' dialog box. It contains five rows, each representing a different subscription option. The first row, 'Keystone', is selected with a blue checkmark. It includes a 'By capacity' button and an upward arrow. Below the name, it says 'Storage management' and 'Charged against your NetApp credit'. There is a dropdown menu for 'Keystone Subscription' with 'A-AMRITA1' selected. The other four rows are 'Professional', 'Essential', 'Freemium (Up to 500 GiB)', and 'Per Node'. Each of these has a radio button, a 'By capacity' button (except for 'Per Node' which has a 'By node' button), and a downward arrow.

Charging Method	Subscription Name	Charging Method Button	Arrow
<input checked="" type="radio"/>	Keystone	By capacity	^
<input type="radio"/>	Professional	By capacity	v
<input type="radio"/>	Essential	By capacity	v
<input type="radio"/>	Freemium (Up to 500 GiB)	By capacity	v
<input type="radio"/>	Per Node	By node	v

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

## Launching Cloud Volumes ONTAP in AWS

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

### Before you get started

You need the following to create a working environment.

- A Connector that's up and running.



- You should have a [Connector that is associated with your workspace](#).
- [You should be prepared to leave the Connector running at all times](#).
- An understanding of the configuration that you want to use.

You should have prepared by choosing a configuration and by obtaining AWS networking information from your administrator. For details, see [Planning your Cloud Volumes ONTAP configuration](#).

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

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

- DNS and Active Directory for CIFS configurations.

For details, see [Networking requirements for Cloud Volumes ONTAP in AWS](#).

## Launching a single-node Cloud Volumes ONTAP system in AWS

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

### About this task

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

### Steps

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

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

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

Field	Description
Add tags	<p>AWS tags are metadata for your AWS resources. BlueXP adds the tags to the Cloud Volumes ONTAP instance and each AWS resource associated with the instance.</p> <p>You can add up to four tags from the user interface when creating a working environment, and then you can add more after its created. Note that the API does not limit you to four tags when creating a working environment.</p> <p>For information about tags, refer to <a href="#">AWS Documentation: Tagging your Amazon EC2 Resources</a>.</p>
User name and password	<p>These are the credentials for the Cloud Volumes ONTAP cluster administrator account. You can use these credentials to connect to Cloud Volumes ONTAP through System Manager or its CLI. Keep the default <i>admin</i> user name or change it to a custom user name.</p>
Edit Credentials	<p>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.</p> <p>Click <b>Add Subscription</b> 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.</p> <p><a href="#">Learn how to add additional AWS credentials to BlueXP</a>.</p>

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

► [https://docs.netapp.com/us-en/cloud-manager-cloud-volumes-ontap//media/video\\_subscribing\\_aws.mp4](https://docs.netapp.com/us-en/cloud-manager-cloud-volumes-ontap//media/video_subscribing_aws.mp4)

(video)

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



### Cloud Manager (for Cloud Volumes ONTAP)

You are currently subscribed to this product and will be charged for your accumulated usage at the end of your next billing cycle, based on the costs listed in Pricing information on the right.

**Having issues signing up for your product?**

If you were unable to complete the set-up process for this software, please [click here](#) to be taken to the product's registration area.

Subscribe

You are already subscribed to this product

#### Pricing Details

Software Fees

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

- [Learn more about Cloud Data Sense](#)
- [Learn more about Cloud Backup](#)



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

7. **Location & Connectivity:** Enter the network information that you recorded in the [AWS worksheet](#).

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

Field	Description
VPC	If you have an AWS Outpost, you can deploy a single node Cloud Volumes ONTAP system in that Outpost by selecting the Outpost VPC. The experience is the same as any other VPC that resides in AWS.
Generated security group	If you let BlueXP generate the security group for you, you need to choose how you'll allow traffic: <ul style="list-style-type: none"><li>• If you choose <b>Selected VPC only</b>, the source for inbound traffic is the subnet range of the selected VPC and the subnet range of the VPC where the Connector resides. This is the recommended option.</li><li>• If you choose <b>All VPCs</b>, the source for inbound traffic is the 0.0.0.0/0 IP range.</li></ul>
Use existing security group	If you use an existing firewall policy, ensure that it includes the required rules. <a href="#">Learn about firewall rules for Cloud Volumes ONTAP</a> .

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

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



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

[Learn how to set up the AWS KMS for Cloud Volumes ONTAP.](#)

[Learn more about supported encryption technologies.](#)

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

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

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

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

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

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

If you prefer to use your own policy, it must meet [policy requirements for Cloud Volumes ONTAP nodes](#).

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



If a newer Release Candidate, General Availability, or patch release is available for the selected version, then BlueXP updates the system to that version when creating the working environment. For example, the update occurs if you select Cloud Volumes ONTAP 9.10.1 and 9.10.1 P4 is available. The update does not occur from one release to another—for example, from 9.6 to 9.7.

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

Note the following:

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

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

[Learn how data tiering works.](#)

#### 15. **Write Speed & WORM:**

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

[Learn more about write speed.](#)

- 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.](#)

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

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

[Learn about supported client protocols and versions.](#)

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

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

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

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

### Volume Details, Protection & Protocol

#### Details & Protection

Volume Name:

Size (GB):

Snapshot Policy:

Default Policy

#### Protocol

NFS **CIFS** iSCSI

Share name:

Permissions:

Users / Groups:

Valid users and groups separated by a semicolon

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

Field	Description
DNS Primary and Secondary IP Address	<p>The IP addresses of the DNS servers that provide name resolution for the CIFS server.</p> <p>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.</p>
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 <b>OU=Computers,OU=corp</b> 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 <b>Use Active Directory Domain</b> to configure an NTP server using the Active Directory DNS. If you need to configure an NTP server using a different address, then you should use the API. See the <a href="#">BlueXP automation docs</a> for details.  Note that you can configure an NTP server only when creating a CIFS server. It's not configurable after you create the CIFS server.

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

For more information, see [Understanding volume usage profiles](#) and [Data tiering overview](#).

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

- Review details about the configuration.
- Click **More information** to review details about support and the AWS resources that BlueXP will purchase.
- Select the **I understand...** check boxes.
- Click **Go**.

## Result

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

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

For additional help, go to [NetApp Cloud Volumes ONTAP Support](#).

## After you finish

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

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

## Launching a Cloud Volumes ONTAP HA pair in AWS

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

## Limitation

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

## About this task

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

## Steps

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

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

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

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

► [https://docs.netapp.com/us-en/cloud-manager-cloud-volumes-ontap//media/video\\_subscribing\\_aws.mp4](https://docs.netapp.com/us-en/cloud-manager-cloud-volumes-ontap//media/video_subscribing_aws.mp4)



(video)



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

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

- [Learn more about Cloud Data Sense](#)
- [Learn more about Cloud Backup](#)



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

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

For an overview of the deployment models, see [Cloud Volumes ONTAP HA for AWS](#).

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

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

Field	Description
Generated security group	If you let BlueXP generate the security group for you, you need to choose how you'll allow traffic: <ul style="list-style-type: none"><li>• If you choose <b>Selected VPC only</b>, the source for inbound traffic is the subnet range of the selected VPC and the subnet range of the VPC where the Connector resides. This is the recommended option.</li><li>• If you choose <b>All VPCs</b>, the source for inbound traffic is the 0.0.0.0/0 IP range.</li></ul>
Use existing security group	If you use an existing firewall policy, ensure that it includes the required rules. <a href="#">Learn about firewall rules for Cloud Volumes ONTAP</a> .

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

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

The IP addresses must be outside of the CIDR block for all VPCs in the region. For additional details, see [AWS networking requirements for Cloud Volumes ONTAP HA in multiple AZs](#).

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

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

route tables, refer to [AWS Documentation: Route Tables](#).

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

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



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

[Learn how to set up the AWS KMS for Cloud Volumes ONTAP.](#)

[Learn more about supported encryption technologies.](#)

12. **Charging Methods and NSS Account:** Specify which charging option would you like to use with this system, and then specify a NetApp Support Site account.

- [Learn about licensing options for Cloud Volumes ONTAP.](#)
- [Learn how to set up licensing.](#)

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

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

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

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

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

If you prefer to use your own policy, it must meet [policy requirements for Cloud Volumes ONTAP nodes and the HA mediator](#).

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



If a newer Release Candidate, General Availability, or patch release is available for the selected version, then BlueXP updates the system to that version when creating the working environment. For example, the update occurs if you select Cloud Volumes ONTAP 9.10.1 and 9.10.1 P4 is available. The update does not occur from one release to another—for example, from 9.6 to 9.7.

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

Note the following:

- The disk type is for the initial volume (and aggregate). You can choose a different disk type for subsequent volumes (and aggregates).
- If you choose a gp3 or io1 disk, BlueXP uses the Elastic Volumes feature in AWS to automatically increase the underlying storage disk capacity as needed. You can choose the initial capacity based on

your storage needs and revise it after Cloud Volumes ONTAP is deployed. [Learn more about support for Elastic Volumes in AWS.](#)

- If you choose a gp2 or st1 disk, you can select a disk size for all disks in the initial aggregate and for any additional aggregates that BlueXP creates when you use the simple provisioning option. You can create aggregates that use a different disk size by using the advanced allocation option.
- You can choose a specific volume tiering policy when you create or edit a volume.
- If you disable data tiering, you can enable it on subsequent aggregates.

[Learn how data tiering works.](#)

#### 18. Write Speed & WORM:

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

[Learn more about write speed.](#)

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

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

[Learn more about WORM storage.](#)

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

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

[Learn about supported client protocols and versions.](#)

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

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

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

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

### Volume Details, Protection & Protocol

#### Details & Protection

Volume Name:

Size (GB):

Snapshot Policy:

Default Policy

#### Protocol

NFS **CIFS** iSCSI

Share name:

Permissions:

Users / Groups:

Valid users and groups separated by a semicolon

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

Field	Description
DNS Primary and Secondary IP Address	<p>The IP addresses of the DNS servers that provide name resolution for the CIFS server.</p> <p>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.</p>
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 <b>OU=Computers,OU=corp</b> 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 <b>Use Active Directory Domain</b> to configure an NTP server using the Active Directory DNS. If you need to configure an NTP server using a different address, then you should use the API. See the <a href="#">BlueXP automation docs</a> for details.  Note that you can configure an NTP server only when creating a CIFS server. It's not configurable after you create the CIFS server.

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

For more information, see [Understanding volume usage profiles](#) and [Data tiering overview](#).

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

- Review details about the configuration.
- Click **More information** to review details about support and the AWS resources that BlueXP will purchase.
- Select the **I understand...** check boxes.
- Click **Go**.

## Result

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

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

For additional help, go to [NetApp Cloud Volumes ONTAP Support](#).

## After you finish

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

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

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

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

region users.

## Supported versions in C2S

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

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



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

## Supported features in C2S

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

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

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

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

## Limitations

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

## Deployment overview

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

### 1. [Preparing your AWS environment](#)

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

### 2. [Installing the Connector and setting up Cloud Manager](#)

Before you can start using Cloud Manager to deploy Cloud Volumes ONTAP, you'll need to create a *Connector*. The Connector enables Cloud Manager to manage resources and processes within your public

cloud environment (this includes Cloud Volumes ONTAP).

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

### 3. [Launching Cloud Volumes ONTAP from Cloud Manager](#)

Each of these steps are described below.

#### **Preparing your AWS environment**

Your AWS environment must meet a few requirements.

##### **Set up your networking**

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

##### **Steps**

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

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

#### **Subscribe to Cloud Volumes ONTAP**

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

##### **Steps**

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

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

##### **Set up permissions**

Set up IAM policies and roles that provide the Connector and Cloud Volumes ONTAP with the permissions that they need to perform actions in the AWS Commercial Cloud Services environment.

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

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

##### **Steps**

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

```
{
  "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.

```

{
  "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"
  }]
}

```

4. 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": "*"
  }]
}

```

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

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

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

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

### **Set up the AWS KMS**

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

#### **Steps**

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

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

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

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

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

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

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

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

#### **Steps**

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

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

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

Note the following as you configure the instance:

- We recommend t3.xlarge.
- You must choose the IAM role that you created when preparing your AWS environment.

- You should keep the default storage options.
  - The required connection methods for the Connector are as follows: SSH, HTTP, and HTTPS.
3. Set up Cloud Manager from a host that has a connection to the Connector instance:
    - a. Open a web browser and enter the following URL: <http://ipaddress>
    - b. Specify a proxy server for connectivity to AWS services.
    - c. Upload the certificate that you obtained in step 1.
    - d. Complete the steps in the Setup wizard to set up Cloud Manager.
      - **System Details:** Enter a name for this instance of Cloud Manager and provide your company name.
      - **Create User:** Create the Admin user that you'll use to administer Cloud Manager.
      - **Review:** Review the details and approve the end user license agreement.
    - e. To complete installation of the CA-signed certificate, restart the Connector instance from the EC2 console.
  4. After the Connector restarts, log in using the administrator user account that you created in the Setup wizard.

## Launching Cloud Volumes ONTAP from Cloud Manager

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

### What you'll need

- If you purchased a license, you must have the license file that you received from NetApp. The license file is a .NLF file in JSON format.
- A key pair is required to enable key-based SSH authentication to the HA mediator.

### Steps

1. On the Working Environments page, click **Add Working Environment**.
2. Under Create, select Cloud Volumes ONTAP or Cloud Volumes ONTAP HA.
3. Complete the steps in the wizard to launch the Cloud Volumes ONTAP system.

Note the following as you complete the wizard:

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

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

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

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

You can choose a different disk type for subsequent volumes.

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

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

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



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

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

## Result

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

## Security group rules

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

### Security group for the Connector

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

#### Inbound rules

Protocol	Port	Purpose
SSH	22	Provides SSH access to the Connector host
HTTP	80	Provides HTTP access from client web browsers to the local user interface
HTTPS	443	Provides HTTPS access from client web browsers to the local user interface

#### Outbound rules

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

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

### Security group for Cloud Volumes ONTAP

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

## Inbound rules

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

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

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

## 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

## External security group for the HA mediator

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

### Inbound rules

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

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

## Outbound rules

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

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

## Internal security group for the HA mediator

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

### Inbound rules

The predefined security group includes the following inbound rules.

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

# Get started in Microsoft Azure

## Quick start for Cloud Volumes ONTAP in Azure

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

1

### Create a Connector

If you don't have a [Connector](#) yet, an Account Admin needs to create one. [Learn how to create a Connector in Azure](#)

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

2

### Plan your configuration

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

3

### Set up your networking

- Ensure that your VNet and subnets will support connectivity between the Connector and Cloud Volumes ONTAP.
- Enable outbound internet access from the target VPC for NetApp AutoSupport.

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

[Learn more about networking requirements.](#)

4

### Launch Cloud Volumes ONTAP using BlueXP

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

#### Related links

- [Creating a Connector from BlueXP](#)
- [Creating a Connector from the Azure Marketplace](#)
- [Installing the Connector software on a Linux host](#)
- [What BlueXP does with permissions](#)

## Plan your Cloud Volumes ONTAP configuration in Azure

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

### Choose a Cloud Volumes ONTAP license

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

- [Learn about licensing options for Cloud Volumes ONTAP](#)
- [Learn how to set up licensing](#)

### Choose a supported region

Cloud Volumes ONTAP is supported in most Microsoft Azure regions. [View the full list of supported regions.](#)

### Choose a supported VM type

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

[Supported configurations for Cloud Volumes ONTAP in Azure](#)

### Understand storage limits

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

[Storage limits for Cloud Volumes ONTAP in Azure](#)

### Size your system in Azure

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

#### Virtual machine type

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

- [Azure documentation: General purpose virtual machine sizes](#)
- [Azure documentation: Memory optimized virtual machine sizes](#)

#### Azure disk type with single node systems

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

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

- *Premium SSD Managed Disks* provide high performance for I/O-intensive workloads at a higher cost.

- *Standard SSD Managed Disks* provide consistent performance for workloads that require low IOPS.
- *Standard HDD Managed Disks* are a good choice if you don't need high IOPS and want to reduce your costs.

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

### Azure disk type with HA pairs

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

### Azure disk size

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



All disks in an aggregate must be the same size.

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

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

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

Refer to Azure for IOPS and throughput by disk size:

- [Microsoft Azure: Managed Disks pricing](#)
- [Microsoft Azure: Page Blobs pricing](#)

### View default system disks

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

[View the default disks for Cloud Volumes ONTAP system data in Azure.](#)



The Connector also requires a system disk. [View details about the Connector's default configuration.](#)

### Collect networking information

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

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

### Choose a write speed

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

### Choose a volume usage profile

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

NetApp storage efficiency features provide the following benefits:

#### Thin provisioning

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

#### Deduplication

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

#### Compression

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

## Networking requirements for Cloud Volumes ONTAP in Azure

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

### Requirements for Cloud Volumes ONTAP

The following networking requirements must be met in Azure.

#### Outbound internet access

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

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

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

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

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

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

If BlueXP notifies you that AutoSupport messages can't be sent, [troubleshoot your AutoSupport configuration](#).

### IP addresses

BlueXP automatically allocates the required number of private IP addresses to Cloud Volumes ONTAP in Azure. You need to make sure that your networking has enough private IP addresses available.

The number of LIFs that BlueXP allocates for Cloud Volumes ONTAP depends on whether you deploy a single node system or an HA pair. A LIF is an IP address associated with a physical port. An SVM management LIF is required for management tools like SnapCenter.



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

### IP addresses for a single node system

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

- Cluster management IP
- Node management IP
- Intercluster IP for SnapMirror
- NFS/CIFS IP
- iSCSI IP



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

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

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

### NIC0

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

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

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

[Learn more about using Azure Private Links or service endpoints with Cloud Volumes ONTAP.](#)

## Connections to other ONTAP systems

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

For instructions, refer to [Microsoft Azure Documentation: Create a Site-to-Site connection in the Azure portal.](#)

## Port for the HA interconnect

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

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

## Only one HA pair in an Azure resource group

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

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

## Security group rules

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

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



Looking for information about the Connector? [View security group rules for the Connector](#)

## Inbound rules for single node systems

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

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

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 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

Priority and name	Port and protocol	Source and destination	Description
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 Connector and HTTPS access to the 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
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



Priority and name	Port and protocol	Source and destination	Description
65000 AllowVnetInBound	Any port Any protocol	VirtualNetwork to VirtualNetwork	Inbound traffic from within the VNet
65001 AllowAzureLoadBalancerInBound	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

### Inbound rules for HA systems

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

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



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

Priority and name	Port and protocol	Source and destination	Description
100 inbound_443	443 Any protocol	Any to Any	Connectivity with the Connector and HTTPS access to the 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

Priority and name	Port and protocol	Source and destination	Description
65001 AllowAzureLoadBalancerInBound	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	support.netapp.com	AutoSupport (HTTPS is the default)
	HTTP	80	Node management LIF	support.netapp.com	AutoSupport (only if the transport protocol is changed from HTTPS to HTTP)
	TCP	3128	Node management LIF	Connector	Sending AutoSupport messages through a proxy server on the Connector, if an outbound internet connection isn't available
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 Connector

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

- [View networking requirements for the Connector](#)
- [Security group rules in Azure](#)

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

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

### Data encryption overview

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

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

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

### Key rotation

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

### How data is encrypted

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

#### Azure HA multiple availability zone

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

#### Azure HA single availability zone

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

#### Single node

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

### Footnote

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

## Create a 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.

### Steps

1. [Create a key vault in your Azure subscription.](#)

Note the following requirements for the key vault:

- The key vault must reside in the same region as the Cloud Volumes ONTAP system.
- The following options should be enabled:
  - **Soft-delete** (this option is enabled by default, but must *not* be disabled)
  - **Purge protection**
  - **Azure Disk Encryption for volume encryption** (for single node systems or HA pairs in multiple zones)

2. [Generate a key in the key vault.](#)

Note the following requirements for the key:

- The key type must be **RSA**.
- The recommended RSA key size is **2048**, but other sizes are supported.

## Create a working environment that uses the encryption key

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

### Required permissions

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

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

[View the latest list of permissions](#)



The permissions aren't required for HA pairs in a single zone.

## Steps

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

For an HA pair: GET /azure/ha/metadata/vaults

For single node: GET /azure/vsa/metadata/vaults

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

[Learn more about this API call.](#)

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

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

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

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

[Learn more about this API call.](#)

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

- a. For an HA pair:

POST /azure/ha/working-environments

The request body must include the following fields:

```
"azureEncryptionParameters": {  
    "key": "keyName",  
    "vaultName": "vaultName",  
    "userAssignedIdentity": " userAssignedIdentityId",  
[Optional] ***  
}
```

[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",  
    "userAssignedIdentity": " userAssignedIdentityId",  
    [Optional] ***  
}
```

[Learn more about this API call.](#)

## Result

You have a new Cloud Volumes ONTAP system that is configured to use your customer-managed key for data encryption.

## Set up licensing for Cloud Volumes ONTAP in Azure

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

### Freemium

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

### Steps

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

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



### Edit Credentials & Add Subscription

Associate Subscription to Credentials ⓘ

Credentials

Managed Service Identity

Azure Subscription

OCCM Dev (Default)

Marketplace Subscription

ⓘ A marketplace subscription isn't associated with the selected Azure subscription.

+ Add Subscription

Apply Cancel

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

### Select Charging Method

<input type="radio"/>	Professional	By capacity	▼
<input type="radio"/>	Essential	By capacity	▼
<input checked="" type="radio"/>	Freemium (Up to 500 GiB)	By capacity	▼
<input type="radio"/>	Per Node	By node	▼

[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:

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

[Learn more about capacity-based licensing.](#)

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

## BYOL

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

### Steps

1. [Contact NetApp Sales to obtain a license](#)
2. [Add your NetApp Support Site account to BlueXP](#)

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

Your license must be available from the Digital Wallet before you can use it with Cloud Volumes ONTAP. If needed, you can [manually add the license to the Digital Wallet](#).

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

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

## Edit Credentials & Add Subscription

Associate Subscription to Credentials ⓘ

Credentials

Managed Service Identity

Azure Subscription

OCCM Dev (Default)

Marketplace Subscription

ⓘ A marketplace subscription isn't associated with the selected Azure subscription.

+ Add Subscription

Apply Cancel

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

## Select Charging Method

<input checked="" type="radio"/>	Professional	By capacity	▼
<input type="radio"/>	Essential	By capacity	▼
<input type="radio"/>	Freemium (Up to 500 GiB)	By capacity	▼
<input type="radio"/>	Per Node	By node	▼

[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 working environment, BlueXP prompts you to subscribe to the agreement that's available in the Azure Marketplace. That subscription is then associated with the working

environment for charging. You can use that same subscription for additional working environments.

### Steps

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

The screenshot shows a dialog box titled "Edit Credentials & Add Subscription". It has a section "Associate Subscription to Credentials" with a help icon. Below this are two dropdown menus: "Credentials" set to "Managed Service Identity" and "Azure Subscription" set to "OCCM Dev (Default)". A message box states: "A marketplace subscription isn't associated with the selected Azure subscription." Below the message is a "+ Add Subscription" link. At the bottom are "Apply" and "Cancel" buttons.

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

The screenshot shows a dialog box titled "Select Charging Method". It lists four options with radio buttons: "Professional", "Essential", "Freemium (Up to 500 GiB)", and "Per Node". To the right of each option is a button labeled "By capacity" (for the first three) or "By node" (for the last one), followed by a dropdown arrow. The "Professional" option is selected.

[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 working environment creation.

2. On the Canvas page, click **Add Working Environment** and follow the steps in BlueXP.
  - a. On the **Details and Credentials** page, click **Edit Credentials > Add Subscription > Continue**.
  - b. In the Azure portal, select the annual plan that was shared with your Azure account and then click **Subscribe**.
  - c. After you return to BlueXP, select a capacity-based package when you reach the charging methods page.

Select Charging Method	
<input checked="" type="radio"/> Professional	By capacity ▼
<input type="radio"/> Essential	By capacity ▼
<input type="radio"/> Freemium (Up to 500 GiB)	By capacity ▼
<input type="radio"/> Per Node	By node ▼

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

### Keystone Flex Subscription

A Keystone Flex Subscription is a pay-as-you-grow subscription-based service. [Learn more about Keystone Flex Subscriptions](#).

### Steps

1. If you don't have a subscription yet, [contact NetApp](#)
2. [Contact NetApp](#) to authorize your BlueXP user account with one or more Keystone Flex Subscriptions.

3. After NetApp authorizes your account, [link your subscriptions for use with Cloud Volumes ONTAP](#).
4. On the Canvas page, click **Add Working Environment** and follow the steps in BlueXP.
  - a. Select the Keystone Flex Subscription charging method when prompted to choose a charging method.

**Select Charging Method**

☒ **Keystone**

Storage management

Charged against your NetApp credit

Keystone Subscription

A-AMRITA1

☐ **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 Azure.](#)

## Enable high availability mode in Azure

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

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

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

Note the following:

- There are no problems with the high availability of your Cloud Volumes ONTAP HA pair. This Azure feature works in concert with ONTAP to reduce the client observed application outage time for NFS protocols that result from unplanned failover events.

- Enabling this feature is non-disruptive to Cloud Volumes ONTAP HA pairs.
- Enabling this feature on your Azure subscription won't cause issues to other VMs.

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

### Steps

1. [Access the Azure Cloud Shell from the Azure Portal](#)
2. Register the high availability mode feature:

```
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"
}
```

## Launching Cloud Volumes ONTAP in Azure

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

### What you'll need

You need the following to create a working environment.

- A Connector that's up and running.
  - You should have a [Connector that is associated with your workspace](#).
  - [You should be prepared to leave the Connector running at all times](#).

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

You should have chose a configuration and obtained Azure networking information from your administrator. For details, see [Planning your Cloud Volumes ONTAP configuration](#).

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

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

### About this task

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



#### Potential for Data Loss

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

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

### Launching a single-node Cloud Volumes ONTAP system in Azure

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

#### Steps

1. From the left navigation menu, select **Storage > Canvas**.
2. On the Canvas page, click **Add Working Environment** and follow the prompts.
3. **Choose a Location:** Select **Microsoft Azure** and **Cloud Volumes ONTAP Single Node**.
4. If you're prompted, [create a Connector](#).
5. **Details and Credentials:** Optionally change the Azure credentials and subscription, specify a cluster name, add tags if needed, and then specify credentials.

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

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



Field	Description
Resource Group Tags	<p>Tags are metadata for your Azure resources. When you enter tags in this field, BlueXP adds them to the resource group associated with the Cloud Volumes ONTAP system.</p> <p>You can add up to four tags from the user interface when creating a working environment, and then you can add more after its created. Note that the API does not limit you to four tags when creating a working environment.</p> <p>For information about tags, refer to <a href="#">Microsoft Azure Documentation: Using tags to organize your Azure resources</a>.</p>
User name and password	<p>These are the credentials for the Cloud Volumes ONTAP cluster administrator account. You can use these credentials to connect to Cloud Volumes ONTAP through System Manager or its CLI. Keep the default <i>admin</i> user name or change it to a custom user name.</p>
Edit Credentials	<p>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. <a href="#">Learn how to add credentials</a>.</p>

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

► <https://docs.netapp.com/us-en/cloud-manager-cloud-volumes->

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

- [Learn more about Cloud Data Sense](#)
- [Learn more about Cloud Backup](#)



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

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

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

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

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

Field	Description
Resource Group	<p>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.</p> <div><p>If the Azure account that you're using has the <a href="#">required permissions</a>, BlueXP removes Cloud Volumes ONTAP resources from a resource group, in case of deployment failure or deletion.</p></div>
Generated security group	<p>If you let BlueXP generate the security group for you, you need to choose how you'll allow traffic:</p> <ul style="list-style-type: none"><li>• If you choose <b>Selected VNet only</b>, the source for inbound traffic is the subnet range of the selected VNet and the subnet range of the VNet where the Connector resides. This is the recommended option.</li><li>• If you choose <b>All VNets</b>, the source for inbound traffic is the 0.0.0.0/0 IP range.</li></ul>
Use existing	<p>If you choose an existing security group, then it must meet Cloud Volumes ONTAP requirements. <a href="#">View the default security group</a>.</p>

9. **Charging Methods and NSS Account:** Specify which charging option would you like to use with this system, and then specify a NetApp Support Site account.

- [Learn about licensing options for Cloud Volumes ONTAP](#).
- [Learn how to set up licensing](#).

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

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

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



If a newer Release Candidate, General Availability, or patch release is available for the selected version, then BlueXP updates the system to that version when creating the working environment. For example, the update occurs if you select Cloud Volumes ONTAP 9.10.1 and 9.10.1 P4 is available. The update does not occur from one release to another—for example, from 9.6 to 9.7.

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

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

Note the following:

- The disk type is for the initial volume. You can choose a different disk type for subsequent volumes.
- The disk size is for all disks in the initial aggregate and for any additional aggregates that BlueXP creates when you use the simple provisioning option. You can create aggregates that use a different disk size by using the advanced allocation option.

For help choosing a disk type and size, see [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, see [Supported configurations by license for HA pairs](#).

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

[Learn more about WORM storage](#).

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

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

[Learn about supported client protocols and versions](#).

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

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

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

Volume Details, Protection & Protocol

---

### Details & Protection

Volume Name:  Size (GB):  ⓘ

Snapshot Policy:  ▼

ⓘ Default Policy

### Protocol

NFS
CIFS
iSCSI

Share name:  Permissions:  ▼

Users / Groups:

Valid users and groups separated by a semicolon

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 <b>OU=AADDC Computers</b> or <b>OU=AADDC Users</b> in this field. <a href="#">Azure Documentation: Create an Organizational Unit (OU) in an Azure AD Domain Services managed domain</a>
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 <b>Use Active Directory Domain</b> to configure an NTP server using the Active Directory DNS. If you need to configure an NTP server using a different address, then you should use the API. See the <a href="#">BlueXP automation docs</a> for details.  Note that you can configure an NTP server only when creating a CIFS server. It's not configurable after you create the CIFS server.

17. **Usage Profile, Disk Type, and Tiering Policy:** Choose whether you want to enable storage efficiency

features and change the volume tiering policy, if needed.

For more information, see [Understanding volume usage profiles](#) and [Data tiering overview](#).

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

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

## Result

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

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

For additional help, go to [NetApp Cloud Volumes ONTAP Support](#).

## After you finish

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

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

## Launching a Cloud Volumes ONTAP HA pair in Azure

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

## Steps

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

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

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

Field	Description
Resource Group Tags	<p>Tags are metadata for your Azure resources. When you enter tags in this field, BlueXP adds them to the resource group associated with the Cloud Volumes ONTAP system.</p> <p>You can add up to four tags from the user interface when creating a working environment, and then you can add more after its created. Note that the API does not limit you to four tags when creating a working environment.</p> <p>For information about tags, refer to <a href="#">Microsoft Azure Documentation: Using tags to organize your Azure resources</a>.</p>
User name and password	<p>These are the credentials for the Cloud Volumes ONTAP cluster administrator account. You can use these credentials to connect to Cloud Volumes ONTAP through System Manager or its CLI. Keep the default <i>admin</i> user name or change it to a custom user name.</p>
Edit Credentials	<p>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. <a href="#">Learn how to add credentials</a>.</p>

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

► <https://docs.netapp.com/us-en/cloud-manager-cloud-volumes->

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

- [Learn more about Cloud Data Sense](#)
- [Learn more about Cloud Backup](#)




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

## 6. HA Deployment Models:

- Select **Single Availability Zone** or **Multiple Availability Zone**.
  - Location and Connectivity** (single AZ) and **Region and Connectivity** (multiple AZs)
    - For single AZ, select a region, VNet, and subnet.
    - For multiple AZs, select a region, VNet, subnet, zone for node 1, and zone for node 2.
  - 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	<p>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.</p> <p>You must use a dedicated resource group for each Cloud Volumes ONTAP HA pair that you deploy in Azure. Only one HA pair is supported in a resource group. BlueXP experiences connection issues if you try to deploy a second Cloud Volumes ONTAP HA pair in an Azure resource group.</p> <div><p>If the Azure account that you're using has the <a href="#">required permissions</a>, BlueXP removes Cloud Volumes ONTAP resources from a resource group, in case of deployment failure or deletion.</p></div>
Generated security group	<p>If you let BlueXP generate the security group for you, you need to choose how you'll allow traffic:</p> <ul style="list-style-type: none"><li>• If you choose <b>Selected VNet only</b>, the source for inbound traffic is the subnet range of the selected VNet and the subnet range of the VNet where the Connector resides. This is the recommended option.</li><li>• If you choose <b>All VNets</b>, the source for inbound traffic is the 0.0.0.0/0 IP range.</li></ul>



Field	Description
Use existing	If you choose an existing security group, then it must meet Cloud Volumes ONTAP requirements. <a href="#">View the default security group.</a>

8. **Charging Methods and NSS Account:** Specify which charging option would you like to use with this system, and then specify a NetApp Support Site account.

- [Learn about licensing options for Cloud Volumes ONTAP.](#)
- [Learn how to set up licensing.](#)

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

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

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



If a newer Release Candidate, General Availability, or patch release is available for the selected version, then BlueXP updates the system to that version when creating the working environment. For example, the update occurs if you select Cloud Volumes ONTAP 9.10.1 and 9.10.1 P4 is available. The update does not occur from one release to another—for example, from 9.6 to 9.7.

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

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

Note the following:

- The disk size is for all disks in the initial aggregate and for any additional aggregates that BlueXP creates when you use the simple provisioning option. You can create aggregates that use a different disk size by using the advanced allocation option.

For help choosing a disk size, see [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.](#)

13. **Write Speed & WORM:**

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

[Learn more about write speed.](#)

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

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

WORM can't be enabled if data tiering was enabled for Cloud Volumes ONTAP versions 9.7 and below.

Reverting or downgrading to Cloud Volumes ONTAP 9.8 is blocked after enabling WORM and tiering.

[Learn more about WORM storage.](#)

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

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

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

[Learn more about WORM storage.](#)

WORM can't be enabled if data tiering was enabled.

[Learn more about WORM storage.](#)

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

[Learn about supported client protocols and versions.](#)

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

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

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

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

### Volume Details, Protection & Protocol

#### Details & Protection

Volume Name:  Size (GB):

Snapshot Policy:

Default Policy

#### Protocol

NFS
CIFS
iSCSI

Share name:  Permissions:

Users / Groups:

Valid users and groups separated by a semicolon

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

Field	Description
DNS Primary and Secondary IP Address	<p>The IP addresses of the DNS servers that provide name resolution for the CIFS server.</p> <p>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.</p>
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	<p>The organizational unit within the AD domain to associate with the CIFS server. The default is CN=Computers.</p> <p>To configure Azure AD Domain Services as the AD server for Cloud Volumes ONTAP, you should enter <b>OU=AADDC Computers</b> or <b>OU=AADDC Users</b> in this field.</p> <p><a href="#">Azure Documentation: Create an Organizational Unit (OU) in an Azure AD Domain Services managed domain</a></p>
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	<p>Select <b>Use Active Directory Domain</b> to configure an NTP server using the Active Directory DNS. If you need to configure an NTP server using a different address, then you should use the API. See the <a href="#">BlueXP automation docs</a> for details.</p> <p>Note that you can configure an NTP server only when creating a CIFS server. It's not configurable after you create the CIFS server.</p>

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

For more information, see [Understanding volume usage profiles](#) and [Data tiering overview](#).

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

## Result

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

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

For additional help, go to [NetApp Cloud Volumes ONTAP Support](#).

## After you finish

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

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

# Get started in Google Cloud

## Quick start for Cloud Volumes ONTAP in Google Cloud

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

1

### Create a Connector

If you don't have a [Connector](#) yet, an Account Admin needs to create one. [Learn how to create a Connector in Google Cloud](#)

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

2

### Plan your configuration

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

[Learn more about planning your configuration.](#)

3

### Set up your networking

- a. Ensure that your VPC and subnets will support connectivity between the Connector and Cloud Volumes ONTAP.
- b. If you plan to enable data tiering, [configure the Cloud Volumes ONTAP subnet for Private Google Access](#).
- c. If you're deploying an HA pair, ensure that you have four VPCs, each with their own subnet.
- d. If you're using a shared VPC, provide the *Compute Network User* role to the Connector service account.
- e. Enable outbound internet access from the target VPC for NetApp AutoSupport.

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

[Learn more about networking requirements.](#)

4

### Set up a service account

Cloud Volumes ONTAP requires a Google Cloud service account for two purposes. The first is when you enable [data tiering](#) to tier cold data to low-cost object storage in Google Cloud. The second is when you enable the [Cloud Backup Service](#) to back up volumes to low-cost object storage.

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

[Read step-by-step instructions.](#)

## 5

### Enable Google Cloud APIs

Enable the following [Google Cloud APIs in your project](#). These APIs are required to deploy the Connector and Cloud Volumes ONTAP.

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

## 6

### Launch Cloud Volumes ONTAP using BlueXP

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

#### Related links

- [Creating a Connector from BlueXP](#)
- [Installing the Connector software on a Linux host](#)
- [What BlueXP does with Google Cloud permissions](#)

## Plan your Cloud Volumes ONTAP configuration in Google Cloud

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

### Choose a Cloud Volumes ONTAP license

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

- [Learn about licensing options for Cloud Volumes ONTAP](#)
- [Learn how to set up licensing](#)

### Choose a supported region

Cloud Volumes ONTAP is supported in most Google Cloud regions. [View the full list of supported regions](#).

### Choose a supported machine type

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

[Supported configurations for Cloud Volumes ONTAP in GCP](#)

## Understand storage limits

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

### Storage limits for Cloud Volumes ONTAP in GCP

## Size your system in GCP

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

### Machine type

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

Refer to the following for more details:

- [Google Cloud documentation: N1 standard machine types](#)
- [Google Cloud documentation: Performance](#)

### GCP disk type

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

- *Zonal SSD persistent disks*: SSD persistent disks are best for workloads that require high rates of random IOPS.
- *Zonal Balanced persistent disks*: These SSDs balance performance and cost by providing lower IOPS per GB.
- *Zonal Standard persistent disks* : Standard persistent disks are economical and can handle sequential read/write operations.

For more details, see [Google Cloud documentation: Zonal Persistent disks \(Standard and SSD\)](#).

### GCP disk size

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

- All disks in an aggregate must be the same size.
- Determine the space that you need, while taking performance into consideration.
- The performance of persistent disks scales automatically with disk size and the number of vCPUs available to the system.

Refer to the following for more details:

- [Google Cloud documentation: Zonal Persistent disks \(Standard and SSD\)](#)
- [Google Cloud documentation: Optimizing Persistent Disk and Local SSD Performance](#)

## View default system disks

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

- [View the default disks for Cloud Volumes ONTAP system data in Google Cloud.](#)
- [Google Cloud docs: Resource quotas](#)

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



The Connector also requires a system disk. [View details about the Connector's default configuration.](#)

## Collect networking information

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

### Network information for a single-node system

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

### Network information for an HA pair in multiple zones

GCP 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

GCP information	Your value
Region	
Zone	
VPC-0 and subnet	
VPC-1 and subnet	
VPC-2 and subnet	
VPC-3 and subnet	
Firewall policy (if using your own)	

### Choose a write speed

BlueXP enables you to choose a write speed setting for Cloud Volumes ONTAP, except for high availability (HA) pairs in Google Cloud. Before you choose a write speed, you should understand the differences between the normal and high settings and risks and recommendations when using high write speed. [Learn more about write speed](#).

### Choose a volume usage profile

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

NetApp storage efficiency features provide the following benefits:

#### Thin provisioning

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

#### Deduplication

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

#### Compression

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

## Networking requirements for Cloud Volumes ONTAP in Google Cloud

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

If you want to deploy an HA pair, you should [learn how HA pairs work in Google Cloud](#).

## Requirements for Cloud Volumes ONTAP

The following requirements must be met in Google Cloud.

### Requirements specific to single node systems

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

#### One VPC

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

#### Private IP addresses

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

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

```
skipSvmManagementLif: true
```



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

### Requirements specific to HA pairs

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

#### One or multiple zones

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

- Multiple zones (recommended)

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

- Single zone

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

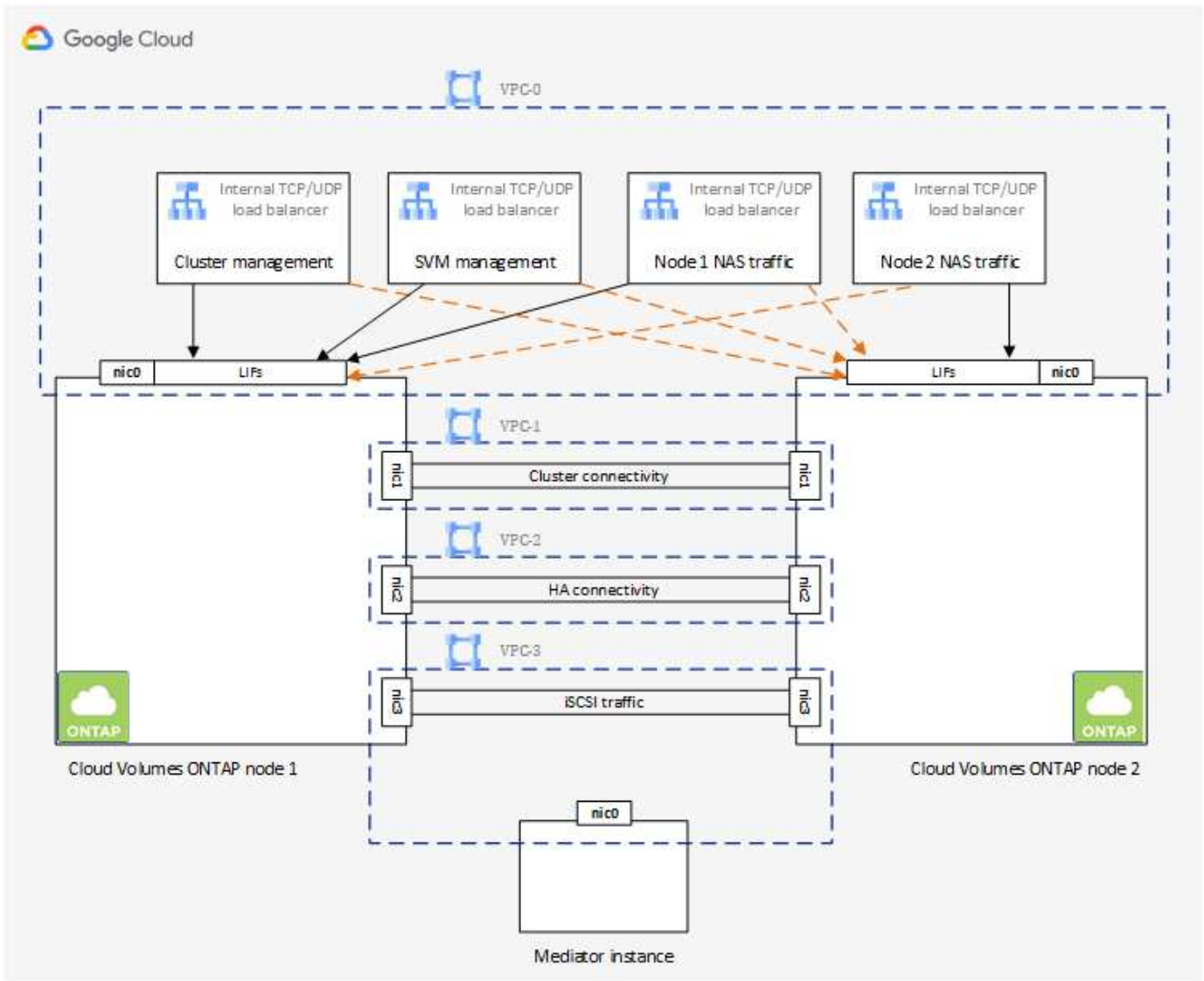
This deployment model does lower your costs because there are no data egress charges between zones.

## Four Virtual Private Clouds

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

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

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



## Subnets

A private subnet is required for each VPC.

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

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

## Private IP addresses

BlueXP allocates 14 or 15 private IP addresses to an HA pair in Google Cloud:

- 7 or 8 private IP addresses for VPC-0

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
```

- Two private IP addresses for VPC-1
- Two private IP addresses for VPC-2
- Three private IP addresses for VPC-3

## Internal load balancers

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

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

The setup for each load balancer is as follows:

- One shared private IP address
- One global health check

By default, the ports used by the health check are 63001, 63002, and 63003.

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

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

## Shared VPCs

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

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

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

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

[Review the required shared VPC permissions covered in Connector deployment](#)

## Packet mirroring in VPCs

[Packet mirroring](#) must be disabled in the Google Cloud VPC in which you deploy Cloud Volumes ONTAP. Cloud Volumes ONTAP can't operate properly if packet mirroring is enabled.

## Outbound internet access

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

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

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

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

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

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



If you're using an HA pair, the HA mediator doesn't require outbound internet access.

If BlueXP notifies you that AutoSupport messages can't be sent, [troubleshoot your AutoSupport configuration](#).

## Connection to Google Cloud Storage for data tiering

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

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

## Connections to ONTAP systems in other networks

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

For instructions, refer to [Google Cloud documentation: Cloud VPN overview](#).

## Firewall rules

BlueXP creates Google Cloud firewall rules that include the inbound and outbound rules that Cloud Volumes ONTAP needs to operate successfully. You might want to refer to the ports for testing purposes or if you prefer your to use own firewall rules.

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

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

- One set of rules for HA components in VPC-0. These rules enable data access to Cloud Volumes ONTAP.
- Another set of rules for HA components in VPC-1, VPC-2, and VPC-3. These rules are open for inbound & outbound communication between the HA components. [VPC-2, and VPC-3, Learn more.](#)



Looking for information about the Connector? [View firewall rules for the Connector](#)

## Inbound rules

When you create a working environment, you can choose the source filter for the predefined firewall policy during deployment:

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

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

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

Protocol	Port	Purpose
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 source is the interface (IP address) on the Cloud Volumes ONTAP system.

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



Service	Protocol	Port	Source	Destination	Purpose
AutoSupport	HTTPS	443	Node management LIF	support.netapp.com	AutoSupport (HTTPS is the default)
	HTTP	80	Node management LIF	support.netapp.com	AutoSupport (only if the transport protocol is changed from HTTPS to HTTP)
	TCP	3128	Node management LIF	Connector	Sending AutoSupport messages through a proxy server on the Connector, if an outbound internet connection isn't available
Cluster	All traffic	All traffic	All LIFs on one node	All LIFs on the other node	Intercluster communications (Cloud Volumes ONTAP HA only)
DHCP	UDP	68	Node management LIF	DHCP	DHCP client for first-time setup
DHCPs	UDP	67	Node management LIF	DHCP	DHCP server
DNS	UDP	53	Node management LIF and data LIF (NFS, CIFS)	DNS	DNS
NDMP	TCP	1860-18699	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 that BlueXP creates for instances in VPC-1, VPC-2, and VPC-3 enables ingress communication over *all* protocols and ports. These rules enable communication between HA nodes.

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

### Requirements for the Connector

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

- [View networking requirements for the Connector](#)
- [Firewall rules in Google Cloud](#)

## Planning for VPC Service Controls in GCP

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

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

### How NetApp services communicate with VPC Service Controls

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

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

### Images

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

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

### Deploying a Connector

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

### Deploying Cloud Volumes ONTAP

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

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

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

### VPC Service Controls perimeter policies

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

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

#### Ingress rules

##### Rule 1

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

OR

##### Rule 2

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

OR

### Rule 3

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

### Egress rules

#### Rule 1:

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



The project number outlined above is the project *netapp-cloudmanager* used by NetApp to store images for the Connector and for Cloud Volumes ONTAP.

## Create a service account for data tiering and backups

Cloud Volumes ONTAP requires a Google Cloud service account for two purposes. The first is when you enable [data tiering](#) to tier cold data to low-cost object storage in Google Cloud. The second is when you enable the [Cloud Backup Service](#) to back up volumes to low-cost object storage.

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

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

### Steps

1. In the Google Cloud console, [go to the Service accounts page](#).

2. Select your project.
3. Click **Create service account** and provide the required information.
  - a. **Service account details:** Enter a name and description.
  - b. **Grant this service account access to project:** Select the **Storage Admin** role.



- c. **Grant users access to this service account:** Add the Connector service account as a *Service Account User* to this new service account.

This step is required for data tiering only. It's not required for the Cloud Backup Service.

Create service account

✓ Service account details

|

✓ Grant this service account access to project (optional)

|

3 Grant users access to this service account (optional)

Grant access to users or groups that need to perform actions as this service account. [Learn more](#)

Service account users role

netapp-cloud-manager@iam.gserviceaccount.com ✕ ?

Grant users the permissions to deploy jobs and VMs with this service account

Service account admins role ?

Grant users the permission to administer this service account

DONE

CANCEL

### What's next?

You'll need to select the service account later when you create a Cloud Volumes ONTAP working environment.

## Details and Credentials

default-project

gcp-sub2

Google Cloud Project

Marketplace Subscription

Edit Project

Details

Credentials

Working Environment Name (Cluster Name)

cloudvolumesontap

Service Account ⓘ

Service Account Name

account1

+ Add Labels

Optional Field | Up to four labels

User Name

admin

Password

Confirm Password

## Using customer-managed encryption keys with Cloud Volumes ONTAP

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

### Steps

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

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

The permissions are as follows:

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

2. Ensure that the service account for the [Google Compute Engine Service Agent](#) has Cloud KMS Encrypter/Decrypter permissions on the key.

The name of the service account uses the following format: "service-[service\_project\_number]@compute-system.iam.gserviceaccount.com".

[Google Cloud Documentation: Using IAM with Cloud KMS - Granting roles on a resource](#)

3. Obtain the "id" of the key by invoking the get command for the `/gcp/vsa/metadata/gcp-encryption-keys` API call or by choosing "Copy Resource Name" on the key in the GCP console.
4. If using customer-managed encryption keys and tiering data to object storage, BlueXP attempts to utilize the same keys that are used to encrypt the persistent disks. But you'll first need to enable Google Cloud Storage buckets to use the keys:
  - a. Find the Google Cloud Storage service agent by following the [Google Cloud Documentation: Getting the Cloud Storage service agent](#).
  - b. Navigate to the encryption key and assign the Google Cloud Storage service agent with Cloud KMS Encrypter/Decrypter permissions.

For more information, refer to [Google Cloud Documentation: Using customer-managed encryption keys](#)

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

### Example

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

Refer to the [BlueXP automation docs](#) for more details about using the "GcpEncryption" parameter.

## Set up licensing for Cloud Volumes ONTAP in Google Cloud

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

### Freemium

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

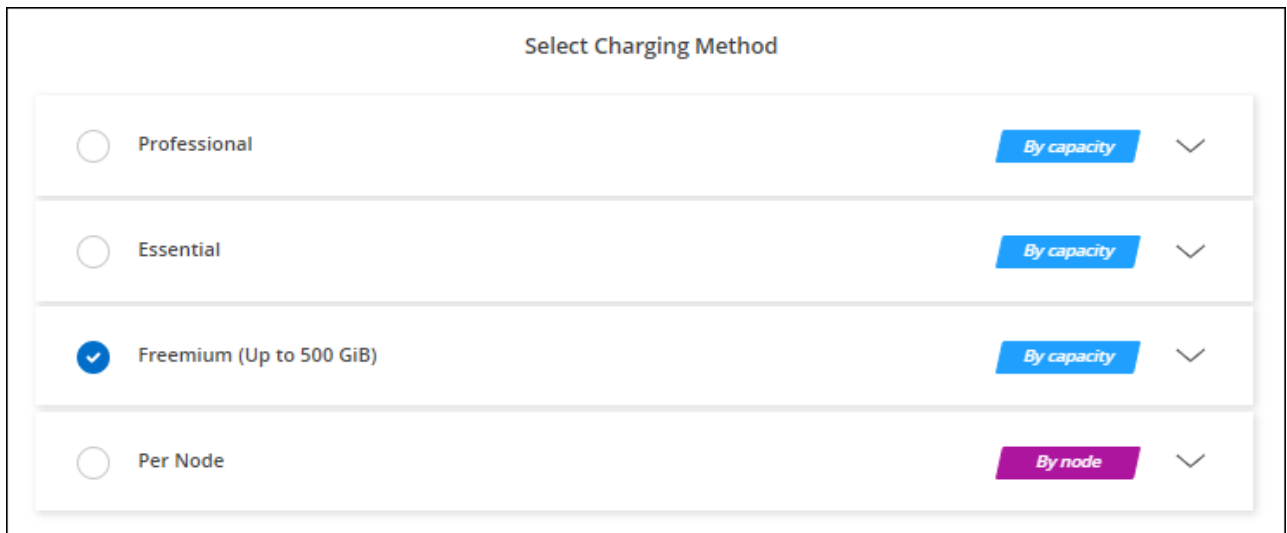
### Steps

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

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



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



Select Charging Method		
<input type="radio"/>	Professional	By capacity ▾
<input type="radio"/>	Essential	By capacity ▾
<input checked="" type="radio"/>	Freemium (Up to 500 GiB)	By capacity ▾
<input type="radio"/>	Per Node	By node ▾

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

### Capacity-based license

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

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

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

[Learn more about capacity-based licensing.](#)

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

#### BYOL

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

#### Steps

1. [Contact NetApp Sales to obtain a license](#)
2. [Add your NetApp Support Site account to BlueXP](#)

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

Your license must be available from the Digital Wallet before you can use it with Cloud Volumes ONTAP. If needed, you can [manually add the license to the Digital Wallet](#).

3. On the Canvas page, click **Add Working Environment** and follow the steps in BlueXP.

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

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

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

Select Charging Method

<input checked="" type="radio"/> Professional	By capacity
<input type="radio"/> Essential	By capacity
<input type="radio"/> Freemium (Up to 500 GiB)	By capacity
<input type="radio"/> Per Node	By node

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

### Steps

1. From the left navigation menu, select **Storage > Canvas**.
2. On the Canvas page, click **Add Working Environment** and follow the steps in BlueXP.
  - a. On the **Details and Credentials** page, click **Edit Credentials > Add Subscription** and then follow the prompts to subscribe to the pay-as-you-go offering in the Google Cloud Marketplace.
  - b. After you return to BlueXP, select a capacity-based package when you reach the charging methods page.

### Select Charging Method

<input checked="" type="radio"/> Professional	By capacity <span>▼</span>
<input type="radio"/> Essential	By capacity <span>▼</span>
<input type="radio"/> Freemium (Up to 500 GiB)	By capacity <span>▼</span>
<input type="radio"/> Per Node	By node <span>▼</span>

[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 working environment creation.

2. On the Canvas page, click **Add Working Environment** and follow the steps in BlueXP.
  - a. On the **Details and Credentials** page, click **Edit Credentials > Add Subscription** and then follow the prompts to subscribe to the annual plan in the Google Cloud Marketplace.
  - b. In Google Cloud, select the annual plan that was shared with your account and then click **Subscribe**.
  - c. After you return to BlueXP, select a capacity-based package when you reach the charging methods page.

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 Google Cloud.](#)

## Keystone Flex Subscription

A Keystone Flex Subscription is a pay-as-you-grow subscription-based service. [Learn more about Keystone Flex Subscriptions.](#)

### Steps

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

Select Charging Method

☒ **Keystone** By capacity ^

Storage management

Charged against your NetApp credit

Keystone Subscription

A-AMRITA1 v

☐ **Professional** By capacity v

☐ **Essential** By capacity v

☐ **Freemium (Up to 500 GiB)** By capacity v

☐ **Per Node** By node v

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

## Launching Cloud Volumes ONTAP in Google Cloud

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

### Before you get started

You need the following to create a working environment.

- A Connector that's up and running.
  - You should have a [Connector that is associated with your workspace](#).
  - [You should be prepared to leave the Connector running at all times](#).
  - The service account associated with the Connector [should have the required permissions](#)
- An understanding of the configuration that you want to use.

You should have prepared by choosing a configuration and by obtaining Google Cloud networking information from your administrator. For details, see [Planning your Cloud Volumes ONTAP configuration](#).

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

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

- Google Cloud APIs should be [enabled in your project](#):
  - Cloud Deployment Manager V2 API
  - Cloud Logging API
  - Cloud Resource Manager API
  - Compute Engine API
  - Identity and Access Management (IAM) API

## Launching a single-node system in Google Cloud

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

### Steps

1. From the left navigation menu, select **Storage > Canvas**.
2. On the Canvas page, click **Add Working Environment** and follow the prompts.
3. **Choose a Location**: Select **Google Cloud** and **Cloud Volumes ONTAP**.
4. If you're prompted, [create a Connector](#).
5. **Details & Credentials**: Select a project, specify a cluster name, optionally select a service account, optionally add labels, and then specify credentials.

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

Field	Description
Working Environment Name	BlueXP uses the working environment name to name both the Cloud Volumes ONTAP system and the Google Cloud VM instance. It also uses the name as the prefix for the predefined security group, if you select that option.
Service Account Name	If you plan to use <a href="#">data tiering</a> or <a href="#">Cloud Backup</a> with Cloud Volumes ONTAP, then you need to enable <b>Service Account</b> and select a service account that has the predefined Storage Admin role. <a href="#">Learn how to create a service account</a> .
Add Labels	<p>Labels are metadata for your Google Cloud resources. BlueXP adds the labels to the Cloud Volumes ONTAP system and Google Cloud resources associated with the system.</p> <p>You can add up to four labels from the user interface when creating a working environment, and then you can add more after its created. Note that the API does not limit you to four labels when creating a working environment.</p> <p>For information about labels, refer to <a href="#">Google Cloud Documentation: Labeling Resources</a>.</p>
User name and password	These are the credentials for the Cloud Volumes ONTAP cluster administrator account. You can use these credentials to connect to Cloud Volumes ONTAP through System Manager or its CLI. Keep the default <i>admin</i> user name or change it to a custom user name.

Field	Description
Edit Project	<p>Select the project where you want Cloud Volumes ONTAP to reside. The default project is the project where BlueXP resides.</p> <p>If you don't see any additional projects in the drop-down list, then you haven't yet associated the BlueXP service account with other projects. Go to the Google Cloud console, open the IAM service, and select the project. Add the service account with the BlueXP role to that project. You'll need to repeat this step for each project.</p> <div>  <p>This is the service account that you set up for BlueXP, <a href="#">as described on this page</a>.</p> </div> <p>Click <b>Add Subscription</b> to associate the selected credentials with a subscription.</p> <p>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.</p>

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

► [https://docs.netapp.com/us-en/cloud-manager-cloud-volumes-ontap//media/video\\_subscribing\\_gcp.mp4](https://docs.netapp.com/us-en/cloud-manager-cloud-volumes-ontap//media/video_subscribing_gcp.mp4)

(video)

6. **Services:** Select the services that you want to use on this system. In order to select Cloud Backup, or to use Tiering, you must have specified the Service Account in step 3.



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

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

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

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 <a href="#">Google Cloud Documentation: Configuring Private Google Access</a> .
Generated firewall policy	If you let BlueXP generate the firewall policy for you, you need to choose how you'll allow traffic: <ul style="list-style-type: none"><li>• If you choose <b>Selected VPC only</b>, the source filter for inbound traffic is the subnet range of the selected VPC and the subnet range of the VPC where the Connector resides. This is the recommended option.</li><li>• If you choose <b>All VPCs</b>, the source filter for inbound traffic is the 0.0.0.0/0 IP range.</li></ul>
Use existing firewall policy	If you use an existing firewall policy, ensure that it includes the required rules. <a href="#">Learn about firewall rules for Cloud Volumes ONTAP</a> .

8. **Charging Methods and NSS Account:** Specify which charging option would you like to use with this system, and then specify a NetApp Support Site account.
- [Learn about licensing options for Cloud Volumes ONTAP](#).
  - [Learn how to set up licensing](#).
9. **Preconfigured Packages:** Select one of the packages to quickly deploy a Cloud Volumes ONTAP system, or click **Create my own configuration**.

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

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



If a newer Release Candidate, General Availability, or patch release is available for the selected version, then BlueXP updates the system to that version when creating the working environment. For example, the update occurs if you select Cloud Volumes ONTAP 9.10.1 and 9.10.1 P4 is available. The update does not occur from one release to another—for example, from 9.6 to 9.7.

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



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

The disk size is for all disks in the initial aggregate and for any additional aggregates that BlueXP creates when you use the simple provisioning option. You can create aggregates that use a different disk size by using the advanced allocation option.

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

12. **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.

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

Note the following:

- BlueXP sets the service account on the Cloud Volumes ONTAP instance. This service account provides permissions for data tiering to a Google Cloud Storage bucket. Be sure to add the Connector service account as a user of the tiering service account, otherwise, you can't select it from BlueXP
- For help with adding a Google Cloud account, see [Setting up and adding Google Cloud accounts for data tiering with 9.6](#).
- You can choose a specific volume tiering policy when you create or edit a volume.
- If you disable data tiering, you can enable it on subsequent aggregates, but you'll need to turn off the system and add a service account from the Google Cloud console.

[Learn more about data tiering.](#)

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

[Learn about supported client protocols and versions.](#)

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

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.

Field	Description
Access control (for NFS only)	An export policy defines the clients in the subnet that can access the volume. By default, BlueXP enters a value that provides access to all instances in the subnet.
Permissions and Users / Groups (for CIFS only)	These fields enable you to control the level of access to a share for users and groups (also called access control lists or ACLs). You can specify local or domain Windows users or groups, or UNIX users or groups. If you specify a domain Windows user name, you must include the user's domain using the format domain\username.
Snapshot Policy	A Snapshot copy policy specifies the frequency and number of automatically created NetApp Snapshot copies. A NetApp Snapshot copy is a point-in-time file system image that has no performance impact and requires minimal storage. You can choose the default policy or none. You might choose none for transient data: for example, tempdb for Microsoft SQL Server.
Advanced options (for NFS only)	Select an NFS version for the volume: either NFSv3 or NFSv4.
Initiator group and IQN (for iSCSI only)	<p>iSCSI storage targets are called LUNs (logical units) and are presented to hosts as standard block devices.</p> <p>Initiator groups are tables of iSCSI host node names and control which initiators have access to which LUNs.</p> <p>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).</p> <p>When you create an iSCSI volume, BlueXP automatically creates a LUN for you. We've made it simple by creating just one LUN per volume, so there's no management involved. After you create the volume, <a href="#">use the IQN to connect to the LUN from your hosts</a>.</p>

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

### Volume Details, Protection & Protocol

#### Details & Protection

Volume Name:  Size (GB):

Snapshot Policy:

*Default Policy*

#### Protocol

NFS **CIFS** iSCSI

Share name:  Permissions:

Users / Groups:

Valid users and groups separated by a semicolon

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

Field	Description
DNS Primary and Secondary IP Address	<p>The IP addresses of the DNS servers that provide name resolution for the CIFS server.</p> <p>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.</p> <p>If you're configuring Google Managed Active Directory, AD can be accessed by default with the 169.254.169.254 IP address.</p>
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	<p>The organizational unit within the AD domain to associate with the CIFS server. The default is CN=Computers.</p> <p>To configure Google Managed Microsoft AD as the AD server for Cloud Volumes ONTAP, enter <b>OU=Computers,OU=Cloud</b> in this field.</p> <p><a href="#">Google Cloud Documentation: Organizational Units in Google Managed Microsoft AD</a></p>
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	<p>Select <b>Use Active Directory Domain</b> to configure an NTP server using the Active Directory DNS. If you need to configure an NTP server using a different address, then you should use the API. See the <a href="#">BlueXP automation docs</a> for details.</p> <p>Note that you can configure an NTP server only when creating a CIFS server. It's not configurable after you create the CIFS server.</p>

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

For more information, see [Understanding volume usage profiles](#) and [Data tiering overview](#).

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

- Review details about the configuration.
- Click **More information** to review details about support and the Google Cloud resources that BlueXP will purchase.
- Select the **I understand...** check boxes.
- Click **Go**.

## Result

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

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

For additional help, go to [NetApp Cloud Volumes ONTAP Support](#).

#### After you finish

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

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

## Launching an HA pair in Google Cloud

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

#### Steps

1. From the left navigation menu, select **Storage > Canvas**.
2. On the Canvas page, click **Add Working Environment** and follow the prompts.
3. **Choose a Location:** Select **Google Cloud** and **Cloud Volumes ONTAP HA**.
4. **Details & Credentials:** Select a project, specify a cluster name, optionally select a Service Account, optionally add labels, and then specify credentials.

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

Field	Description
Working Environment Name	BlueXP uses the working environment name to name both the Cloud Volumes ONTAP system and the Google Cloud VM instance. It also uses the name as the prefix for the predefined security group, if you select that option.
Service Account Name	If you plan to use the <a href="#">Tiering</a> or <a href="#">Cloud Backup</a> services, you need to enable the <b>Service Account</b> switch and then select the Service Account that has the predefined Storage Admin role.
Add Labels	<p>Labels are metadata for your Google Cloud resources. BlueXP adds the labels to the Cloud Volumes ONTAP system and Google Cloud resources associated with the system.</p> <p>You can add up to four labels from the user interface when creating a working environment, and then you can add more after its created. Note that the API does not limit you to four labels when creating a working environment.</p> <p>For information about labels, refer to <a href="#">Google Cloud Documentation: Labeling Resources</a>.</p>
User name and password	These are the credentials for the Cloud Volumes ONTAP cluster administrator account. You can use these credentials to connect to Cloud Volumes ONTAP through System Manager or its CLI. Keep the default <i>admin</i> user name or change it to a custom user name.

Field	Description
Edit Project	<p>Select the project where you want Cloud Volumes ONTAP to reside. The default project is the project where BlueXP resides.</p> <p>If you don't see any additional projects in the drop-down list, then you haven't yet associated the BlueXP service account with other projects. Go to the Google Cloud console, open the IAM service, and select the project. Add the service account with the BlueXP role to that project. You'll need to repeat this step for each project.</p> <div>  <p>This is the service account that you set up for BlueXP, <a href="#">as described on this page</a>.</p> </div> <p>Click <b>Add Subscription</b> to associate the selected credentials with a subscription.</p> <p>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.</p>

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

► [https://docs.netapp.com/us-en/cloud-manager-cloud-volumes-ontap//media/video\\_subscribing\\_gcp.mp4](https://docs.netapp.com/us-en/cloud-manager-cloud-volumes-ontap//media/video_subscribing_gcp.mp4)

(video)

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



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

6. **HA Deployment Models:** Choose multiple zones (recommended) or a single zone for the HA configuration. Then select a region and zones.

[Learn more about HA deployment models.](#)

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

[Learn more about networking requirements.](#)

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

Field	Description
Generated policy	<p>If you let BlueXP generate the firewall policy for you, you need to choose how you'll allow traffic:</p> <ul style="list-style-type: none"><li>• If you choose <b>Selected VPC only</b>, the source filter for inbound traffic is the subnet range of the selected VPC and the subnet range of the VPC where the Connector resides. This is the recommended option.</li><li>• If you choose <b>All VPCs</b>, the source filter for inbound traffic is the 0.0.0.0/0 IP range.</li></ul>
Use existing	<p>If you use an existing firewall policy, ensure that it includes the required rules.</p> <p><a href="#">Learn about firewall rules for Cloud Volumes ONTAP.</a></p>

8. **Charging Methods and NSS Account:** Specify which charging option would you like to use with this system, and then specify a NetApp Support Site account.
  - [Learn about licensing options for Cloud Volumes ONTAP.](#)
  - [Learn how to set up licensing.](#)
9. **Preconfigured Packages:** Select one of the packages to quickly deploy a Cloud Volumes ONTAP system, or click **Create my own configuration**.

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

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



If a newer Release Candidate, General Availability, or patch release is available for the selected version, then BlueXP updates the system to that version when creating the working environment. For example, the update occurs if you select Cloud Volumes ONTAP 9.10.1 and 9.10.1 P4 is available. The update does not occur from one release to another—for example, from 9.6 to 9.7.

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

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

The disk size is for all disks in the initial aggregate and for any additional aggregates that BlueXP creates when you use the simple provisioning option. You can create aggregates that use a different disk size by using the advanced allocation option.

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

12. **Write Speed & WORM:**

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

[Learn more about write speed.](#)



*Flash Cache*, high write speed, and a higher maximum transmission unit (MTU) of 8,896 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 VCP-1, VPC-2, or VCP-3 for the deployment. *Flash Cache*, high write speed, and an MTU of 8,896 are feature-dependent and cannot be disabled individually within a configured instance.

- 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:

- BlueXP sets the service account on the Cloud Volumes ONTAP instance. This service account provides permissions for data tiering to a Google Cloud Storage bucket. Be sure to add the Connector service account as a user of the tiering service account, otherwise, you can't select it from BlueXP.
- You can choose a specific volume tiering policy when you create or edit a volume.
- If you disable data tiering, you can enable it on subsequent aggregates, but you'll need to turn off the system and add a service account from the Google Cloud console.

[Learn more about data tiering.](#)

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

[Learn about supported client protocols and versions.](#)

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

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

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



Volume Details, Protection & Protocol

---

### Details & Protection

Volume Name:  Size (GB):  ⓘ

Snapshot Policy:  ▼

ⓘ Default Policy

### Protocol

NFS
CIFS
iSCSI

Share name:  Permissions:  ▼

Users / Groups:

Valid users and groups separated by a semicolon

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

Field	Description
DNS Primary and Secondary IP Address	<p>The IP addresses of the DNS servers that provide name resolution for the CIFS server.</p> <p>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.</p> <p>If you're configuring Google Managed Active Directory, AD can be accessed by default with the 169.254.169.254 IP address.</p>
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	<p>The organizational unit within the AD domain to associate with the CIFS server. The default is CN=Computers.</p> <p>To configure Google Managed Microsoft AD as the AD server for Cloud Volumes ONTAP, enter <b>OU=Computers,OU=Cloud</b> in this field.</p> <p><a href="#">Google Cloud Documentation: Organizational Units in Google Managed Microsoft AD</a></p>
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.

Field	Description
NTP Server	<p>Select <b>Use Active Directory Domain</b> to configure an NTP server using the Active Directory DNS. If you need to configure an NTP server using a different address, then you should use the API. See the <a href="#">BlueXP automation docs</a> for details.</p> <p>Note that you can configure an NTP server only when creating a CIFS server. It's not configurable after you create the CIFS server.</p>

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

For more information, see [Understanding volume usage profiles](#) and [Data tiering overview](#).

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

- Review details about the configuration.
- Click **More information** to review details about support and the Google Cloud resources that BlueXP will purchase.
- Select the **I understand...** check boxes.
- Click **Go**.

## Result

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

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

For additional help, go to [NetApp Cloud Volumes ONTAP Support](#).

## After you finish

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

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

## Google Cloud Platform Image Verification

### Google Cloud image verification overview

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



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

## Convert image to raw format on Google Cloud

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

### Why is this step needed?

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

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

- Access to Google storage bucket
- Write to Google Storage bucket
- Create cloud build jobs (used during export process)
- Access to the desired image
- Create export image tasks

To verify the image, it must be converted to a disk.raw format and then downloaded.

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

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

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

### Export Google Cloud image using gcloud

## Click to display the script

```
$ 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/xxxxxxxxxxxxx].  
Logs are available at [https://console.cloud.google.com/cloud-  
build/builds;region=us-central1/xxxxxxxxxxxxx?project=xxxxxxxxxxxxx].  
[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
```



See [Google Cloud doc on Exporting an image](#) for more information on how to export an image through Google Cloud.

## Image signature verification

### Verify Google Cloud signed images

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

### Signed image verification workflow summary

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

- From the [NSS](#), download the Google Cloud archive containing the following files:
  - Signed digest (.sig)
  - Certificate containing the public key (.pem)
  - Certificate chain (.pem)



## Cloud Volumes ONTAP 9.13.0

Date Posted:

### Restrictions on Encryption Technology

NetApp Volume Encryption (available with ONTAP 9.1 and later releases) provides for data-at-rest encryption that requires authorizations, permits, or licenses to import, export, re-export or use this software.

A state license for importing encryption equipment is required to import ONTAP 9.1 (or later) with NetApp Volume Encryption into Member States of the Eurasian Economic Union: Russia, Belarus, Kazakhstan, Armenia and Kyrgyzstan. Moreover, in certain cases, an end-user customer must have a valid state encryption license to this software.

Consult your legal advisor on this matter.

#### Cloud Volumes ONTAP

##### Non-Restricted Countries

If you are upgrading to ONTAP 9.13.0, and you are in "Non-restricted Countries", please download the image with NetApp Volume Encryption.

[DOWNLOAD 9130\\_V\\_IMAGE.TGZ \[2.58 GB\]](#)

[View and download checksums](#)

[DOWNLOAD 9130\\_V\\_IMAGE.TGZ.PEM \[451 B\]](#)

[View and download checksums](#)

[DOWNLOAD 9130\\_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 9130\\_V\\_NODAR\\_IMAGE.TGZ \[2.58 GB\]](#)

[View and download checksums](#)

[DOWNLOAD 9130\\_V\\_NODAR\\_IMAGE.TGZ.PEM \[451 B\]](#)

[View and download checksums](#)

[DOWNLOAD 9130\\_V\\_NODAR\\_IMAGE.TGZ.SIG \[256 B\]](#)

[View and download checksums](#)

#### Cloud Volumes ONTAP

##### Google Image Digest Files

[DOWNLOAD GCP-X-9-13-0\\_PKG.TAR.GZ \[7.52 KB\]](#)

[View and download checksums](#)

##### Azure Image Digest File

[DOWNLOAD AZURE-9.13.0\\_PKG.TAR.GZ \[7.55 KB\]](#)

[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



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

You can verify the Google Cloud downloaded disk.raw file against the digest file contents available through the [NSS](#) using OpenSSL.



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

### Steps

1. Verify the certificate using OpenSSL.

## Click to display the script

```
# 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 OSCP 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 OSCP 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: CE894F8251AA15A28462CA312361D261F8FE78

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 the script

```
# 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
```

# Use Cloud Volumes ONTAP

## License management

### Manage capacity-based licenses

Manage your capacity-based licenses from the Digital Wallet to ensure that your NetApp account has enough capacity for your Cloud Volumes ONTAP systems.

*Capacity-based licenses* enable you to pay for Cloud Volumes ONTAP per TiB of capacity.

The *Digital Wallet* enables you to manage licenses for Cloud Volumes ONTAP from a single location. You can add new licenses and update existing licenses.

[Learn more about Cloud Volumes ONTAP licenses.](#)

### How licenses are added to the Digital Wallet

After you purchase a license from your NetApp sales representative, NetApp will send you an email with the serial number and additional licensing details.

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

If BlueXP can't add the license, you'll need to manually add them to the Digital Wallet yourself. For example, if the Connector is installed in a location that doesn't have internet access, you'll need to add the licenses yourself. [Learn how to add purchased licenses to your account.](#)

### View the consumed capacity in your account

The Digital Wallet shows you the total consumed capacity in your account and the consumed capacity by licensing package. This can help you understand how you're being charged and whether you need to purchase additional capacity.

#### Steps

1. From the left navigation menu, select **Digital Wallet**.
2. With **Capacity Based Licenses** selected, view the packages summary, which shows you consumed capacity, total licensed capacity, and total PAYGO capacity.
  - *Total consumed capacity* is the total provisioned capacity of all Cloud Volumes ONTAP systems in your NetApp account. The charging is based on each volume's provisioned size, regardless of local, used, stored, or effective space within the volume.
  - *Total licensed* is the total licensed capacity (BYOL) that you purchased from NetApp.
  - *Total PAYGO* is the total provisioned capacity using cloud marketplace subscriptions. Charging via PAYGO is used only if the consumed capacity is higher than the licensed capacity or if there is no BYOL license available in the Digital Wallet.

Here's an example of an account that has 2000 TiB of consumed capacity:



3. Under the summary, view the consumed capacity for each of your licensing packages.

- *Consumed capacity* shows you the total capacity of the volumes for that package. For more details about a specific package, hover your mouse over the tooltip.

To better understand the capacities that display for the Essentials package, you should be familiar with how charging works. [Learn about charging for the Essentials package.](#)

- *BYOL* shows you the licensed capacity that you purchased from NetApp.
- *PAYGO* shows you the total consumed capacity by license consumption model.

Here's an example for an account that has several licensing packages:

## Add purchased licenses to your account

If you don't see your purchased licenses in the Digital Wallet, you'll need to add the licenses to BlueXP so that the capacity is available for Cloud Volumes ONTAP.

### What you'll need

- You need to provide BlueXP the serial number of the license or the license file.
- If you want to enter the serial number, you first need to [add your NetApp Support Site account to BlueXP](#). This is the NetApp Support Site account that's authorized to access the serial number.

### Steps

1. From the left navigation menu, select **Digital Wallet**.
2. On the **Cloud Volumes ONTAP** tab, keep **Capacity Based Licenses** selected and click **Add License**.
3. Enter the serial number for your capacity-based license or upload the license file.

If you entered a serial number, you also need to select the NetApp Support Site account that's authorized to access the serial number.

4. Click **Add License**.

## Update a capacity-based license

If you purchased additional capacity or extended the term of your license, BlueXP automatically updates the license in the Digital Wallet. There's nothing that you need to do.

However, if you deployed BlueXP in a location that doesn't have internet access, then you'll need to manually update the license in BlueXP.

### What you'll need

The license file (or *files* if you have an HA pair).

## Steps

1. From the left navigation menu, select **Digital Wallet**.
2. On the **Cloud Volumes ONTAP** tab, click the action menu next to the license and select **Update License**.
3. Upload the license file.
4. Click **Upload License**.

## Change charging methods

You can change the charging method for a Cloud Volumes ONTAP system that uses capacity-based licensing. For example, if you deployed a Cloud Volumes ONTAP system with the Essentials package, you can change it to the Professional package if your business needs changed.

### Limitation

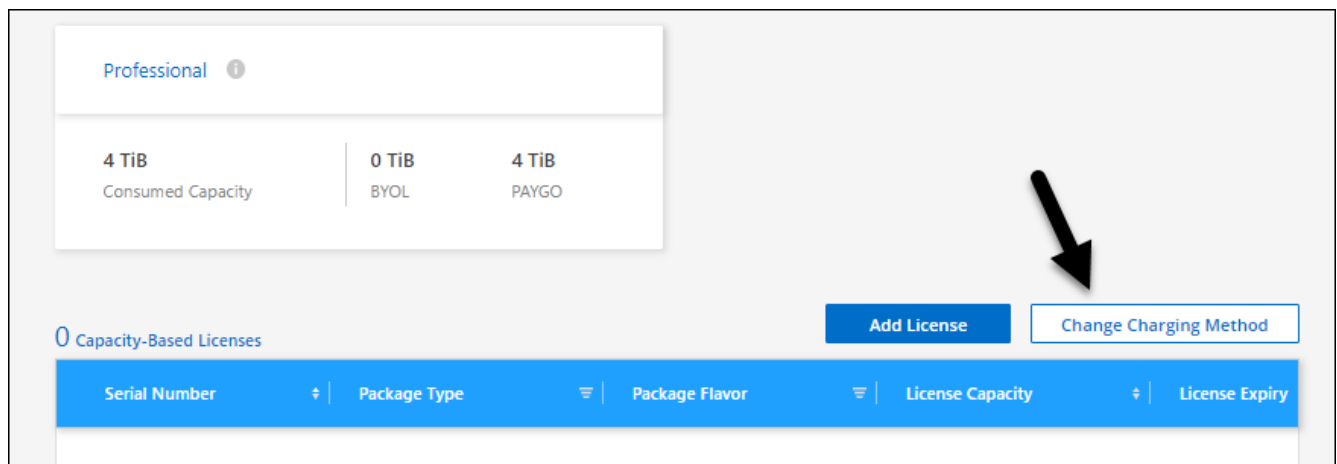
Changing to or from the Edge Cache license isn't supported.

### Important note

If you have a private offer or contract from your cloud provider's marketplace, changing to a charging method that's not included in your contract will result in charging against BYOL (if you purchased a license from NetApp) or PAYGO.

## Steps

1. From the left navigation menu, select **Digital Wallet**.
2. On the **Cloud Volumes ONTAP** tab, click **Change Charging Method**.



3. Select a working environment, choose the new charging method, and then confirm your understanding that changing the package type will affect service charges.



4. Click **Change Charging Method**.

### Result

BlueXP changes the charging method for the Cloud Volumes ONTAP system.

You might also notice that the Digital Wallet refreshes the consumed capacity for each package type to account for the change that you just made.

### Remove a capacity-based license

If a capacity-based license expired and is no longer in use, then you can remove it at any time.

### Steps

1. From the left navigation menu, select **Digital Wallet**.
2. On the **Cloud Volumes ONTAP** tab, click the action menu next to the license and select **Remove License**.
3. Click **Remove** to confirm.

## Manage Keystone Flex Subscriptions

Manage your Keystone Flex Subscriptions from the Digital Wallet by enabling subscriptions for use with Cloud Volumes ONTAP. You can also request changes to the committed capacity and you can unlink subscriptions.

*A Keystone Flex Subscription is a pay-as-you-grow storage service offered by NetApp.*

The *Digital Wallet* enables you to manage licenses for Cloud Volumes ONTAP from a single location. You can add new licenses and update existing licenses.

[Learn more about Cloud Volumes ONTAP licenses.](#)

## Authorize your account

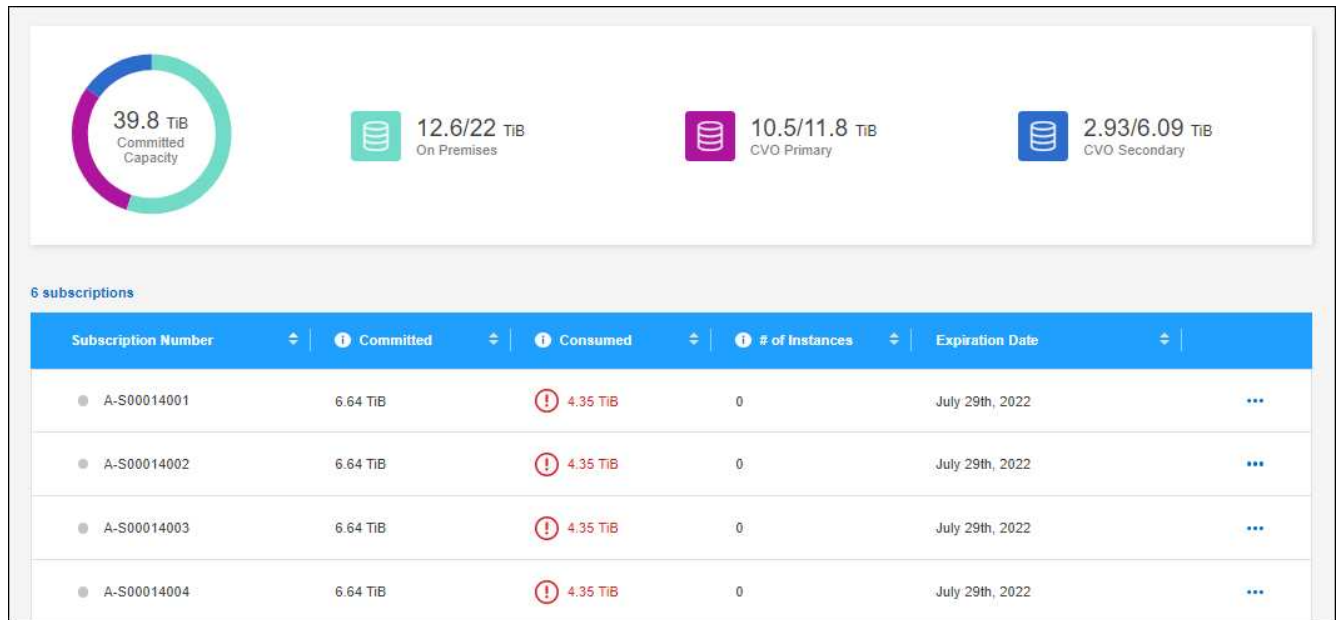
Before you can use and manage Keystone Flex Subscriptions in BlueXP, you need to contact NetApp to authorize your BlueXP user account with your Keystone Flex Subscriptions.

### Steps

1. From the left navigation menu, select **Digital Wallet**.
2. Click **Keystone Flex Subscription**.
3. If you see the **Welcome to NetApp Keystone** page, send an email to the address listed on the page.

A NetApp representative will process your request by authorizing your user account to access the subscriptions.

4. Come back to the **Keystone Flex Subscription** to view your subscriptions.



## What's next?

Link the subscriptions that you want to use with Cloud Volumes ONTAP.

## Link a subscription

After NetApp authorizes your account, you need to link Keystone Flex Subscriptions for use with Cloud Volumes ONTAP. This action enables users to select the subscription as the charging method for new Cloud Volumes ONTAP systems.

### Steps

1. From the left navigation menu, select **Digital Wallet**.
2. Click **Keystone Flex Subscription**.

3. For the subscription that you want to link, click **...** and select **Link**.

Subscription Number	Committed	Consumed	# of Instances	Expiration Date	
A-S00014001	6.64 TiB	4.35 TiB	0	July 29th, 2022	...
A-S00014002	6.64 TiB	4.35 TiB	0	July 29th, 2022	View detail and edit
A-S00014003	6.64 TiB	4.35 TiB	0	July 29th, 2022	Link

## Result

The subscription is now linked to your BlueXP account and available to select when creating a Cloud Volumes ONTAP working environment.

## Request more or less committed capacity

If you need to adjust the committed capacity for a subscription, you can send a request right from the BlueXP interface.

## Steps

1. From the left navigation menu, select **Digital Wallet**.
2. Click **Keystone Flex Subscription**.
3. For the subscription that you want adjust the capacity, click **...** and select **View detail and edit**.
4. Enter the requested committed capacity for one or more subscriptions.

### Subscription Modification for A-S00014001

Service Level	Current Committed Capacity	Current Consumed Capacity	Requested Committed Capacity
Extreme	0.977 TiB	0.293 TiB	<input type="text" value="Enter amount"/> TiB
Premium	0.977 TiB	0.488 TiB	<input type="text" value="Enter amount"/> TiB
Performance	0 TiB	0 TiB	<input type="text" value="Enter amount"/> TiB
Standard	0.732 TiB	0.439 TiB	<input type="text" value="Enter amount"/> TiB
Value	0.977 TiB	 0.879 TiB	<input type="text" value="Enter amount"/> TiB
Data Tiering	0 TiB	0 TiB	<input type="text" value="Enter amount"/> TiB
CVO Primary	1.96 TiB	 1.76 TiB	<input type="text" value="3"/> TiB
CVO Secondary	1.02 TiB	0.488 TiB	<input type="text" value="Enter amount"/> TiB

#### Additional Information

Is there anything else we should know about your request?  
Please be as descriptive as possible.

5. Scroll down, enter any additional details for the request, and then click **Submit**.

## Result

Your request creates a ticket in NetApp's system for processing.

## Unlink a subscription

If you no longer want to use a Keystone Flex Subscription with new Cloud Volumes ONTAP systems, you can unlink the subscription. Note that you can only unlink a subscription that isn't attached to an existing Cloud Volumes ONTAP subscription.

## Steps

1. From the left navigation menu, select **Digital Wallet**.
2. Click **Keystone Flex Subscription**.
3. For the subscription that you want to unlink, click  and select **Unlink**.

## Result

The subscription is unlinked from your BlueXP account and no longer available to select when creating a Cloud Volumes ONTAP working environment.

## Manage node-based licenses

Manage node-based licenses in the Digital Wallet to ensure that each Cloud Volumes ONTAP system has a valid license with the required capacity.

*Node-based licenses* are the previous generation licensing model (and not available for new customers):

- BYOL licenses purchased from NetApp
- Hourly pay-as-you-go (PAYGO) subscriptions from your cloud provider's marketplace

The *Digital Wallet* enables you to manage licenses for Cloud Volumes ONTAP from a single location. You can add new licenses and update existing licenses.

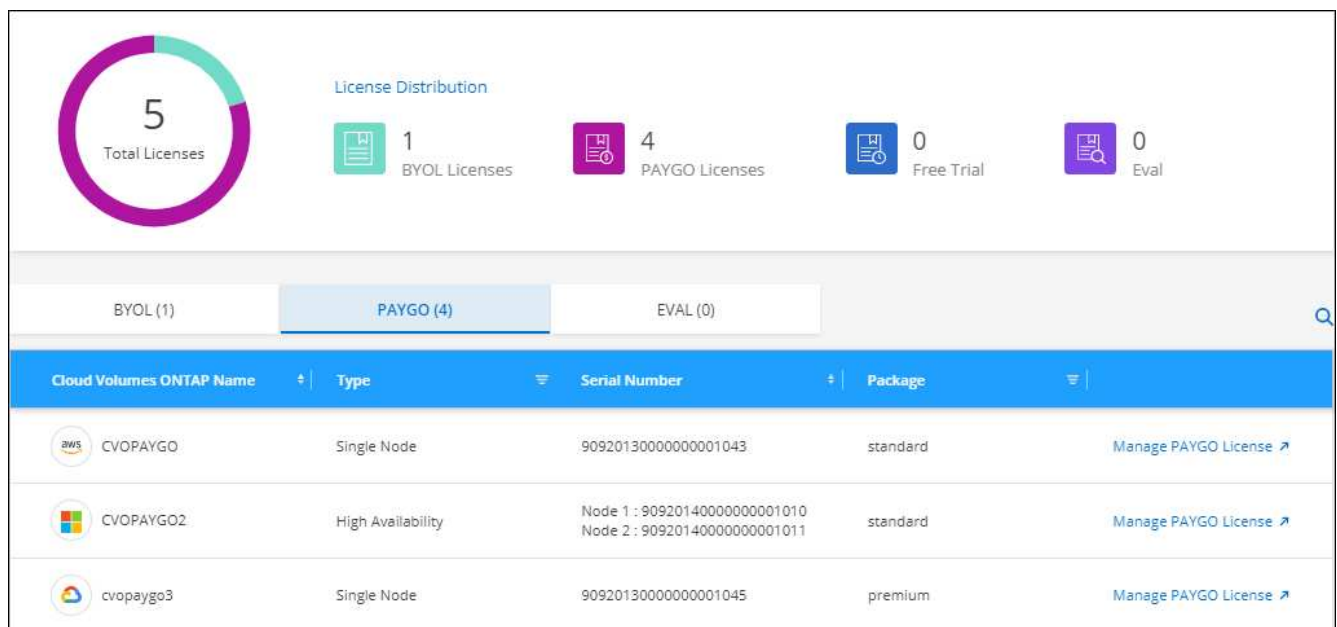
[Learn more about Cloud Volumes ONTAP licenses.](#)

## Manage PAYGO licenses

The Digital Wallet page enables you to view details about each of your PAYGO Cloud Volumes ONTAP systems, including the serial number and PAYGO license type.

### Steps

1. From the left navigation menu, select **Digital Wallet**.
2. On the **Cloud Volumes ONTAP** tab, select **Node Based Licenses** from the drop-down.
3. Click **PAYGO**.
4. View details in the table about each of your PAYGO licenses.



5. If needed, click **Manage PAYGO License** to change the PAYGO license or to change the instance type.

## Manage BYOL licenses

Manage licenses that you purchased directly from NetApp by adding and removing system licenses and extra capacity licenses.

## Add unassigned licenses

Add a node-based license to the Digital Wallet so that you can select the license when you create a new Cloud Volumes ONTAP system. The Digital Wallet identifies these licenses as *unassigned*.

### Steps

1. From the left navigation menu, select **Digital Wallet**.
2. On the **Cloud Volumes ONTAP** tab, select **Node Based Licenses** from the drop-down.
3. Click **Unassigned**.
4. Click **Add Unassigned Licenses**.
5. Enter the serial number of the license or upload the license file.

If you don't have the license file yet, refer to the section below.

6. Click **Add License**.

### Result

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

## Exchange unassigned node-based licenses

If you have an unassigned node-based license for Cloud Volumes ONTAP that you haven't used, you can exchange the license by converting it to a Cloud Backup license, a Cloud Data Sense license, or a Cloud Tiering license.

Exchanging the license revokes the Cloud Volumes ONTAP license and creates a dollar-equivalent license for the service:

- Licensing for a Cloud Volumes ONTAP HA pair is converted to a 51 TiB data service license
- Licensing for a Cloud Volumes ONTAP single node is converted to a 32 TiB data service license

The converted license has the same expiry date as the Cloud Volumes ONTAP license.

### Steps

1. From the left navigation menu, select **Digital Wallet**.
2. On the **Cloud Volumes ONTAP** tab, select **Node Based Licenses** from the drop-down.
3. Click **Unassigned**.
4. Click **Exchange License**.

BYOL (14)	Eval (2)	Unassigned (3)	PAYGO (6)	 <a href="#">Add Unassigned Licenses</a>		
Serial Number	Type	Cloud Provider	License Expiry	Status		
012345678901234567890	Single Node	All Providers	April 20, 2022	Unassigned	<a href="#">Exchange License</a>	...
012345678901234567891	Single Node	 Azure	April 20, 2022	Unassigned	<a href="#">Exchange License</a>	...
012345678901234567892	Single Node	 AWS	January 1, 2022	Exchanged to Cloud Tiering on August 1, 2021		...

5. Select the service that you'd like to exchange the license with.
6. If you're prompted, select an additional license for the HA pair.
7. Read the legal consent and click **Agree**.

## Result

BlueXP converts the unassigned license to the service that you selected. You can view the new license in the **Data Services Licenses** tab.

## Obtain a system license file

In most cases, BlueXP can automatically obtain your license file using your NetApp Support Site account. But if it can't, then you'll need to manually upload the license file. If you don't have the license file, you can obtain it from [netapp.com](https://netapp.com).

## Steps

1. Go to the [NetApp License File Generator](#) and log in using your NetApp Support Site credentials.
2. Enter your password, choose your product, enter the serial number, confirm that you have read and accepted the privacy policy, and then click **Submit**.

## Example

## License Generator

The following fields are pre-populated based on the NetApp SSO login provided.  
To download the corresponding NetApp license file, re-enter your SSO password along with the correct Product Line and Product Serial number.

First Name	<input type="text" value="Ben"/>
Last Name	<input type="text"/>
Company	<input type="text" value="Network Appliance, Inc"/>
Email Address	<input type="text"/>
Username	<input type="text"/>

Product Line\*

ONTAP Select - Standard  
ONTAP Select - Premium  
ONTAP Select - Premium XL  
Cloud Volumes ONTAP for AWS (single node)  
Cloud Volumes ONTAP for AWS (HA)  
Cloud Volumes ONTAP for GCP (single node or HA)  
Cloud Volumes ONTAP for Microsoft Azure (single node)  
Cloud Volumes ONTAP for Microsoft Azure (HA)  
Service Level Manager - SLO Advanced  
StorageGRID Webscale  
StorageGRID WhiteBox  
SnapCenter Standard (capacity-based)

Not only is protecting your data required by

☐ I have read NetApp's new **Global Data** may use my personal data.

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

### Update a system license

When you renew a BYOL subscription by contacting a NetApp representative, BlueXP automatically obtains the new license from NetApp and installs it on the Cloud Volumes ONTAP system.

If BlueXP can't access the license file over the secure internet connection, you can obtain the file yourself and then manually upload the file to BlueXP.

### Steps

1. From the left navigation menu, select **Digital Wallet**.
2. On the **Cloud Volumes ONTAP** tab, select **Node Based Licenses** from the drop-down.
3. In the **BYOL** tab, expand the details for a Cloud Volumes ONTAP system.
4. Click the action menu next to the system license and select **Update License**.
5. Upload the license file (or files if you have an HA pair).
6. Click **Update License**.

### Result

BlueXP updates the license on the Cloud Volumes ONTAP system.

### Manage extra capacity licenses

You can purchase extra capacity licenses for a Cloud Volumes ONTAP BYOL system to allocate more than the 368 TiB of capacity that's provided with a BYOL system license. For example, you might purchase one extra license capacity to allocate up to 736 TiB of capacity to Cloud Volumes ONTAP. Or you could purchase three



extra capacity licenses to get up to 1.4 PiB.

The number of licenses that you can purchase for a single node system or HA pair is unlimited.

### Add capacity licenses

Purchase an extra capacity license by contacting us through the chat icon in the lower-right of BlueXP. After you purchase the license, you can apply it to a Cloud Volumes ONTAP system.

#### Steps

1. From the left navigation menu, select **Digital Wallet**.
2. On the **Cloud Volumes ONTAP** tab, select **Node Based Licenses** from the drop-down.
3. In the **BYOL** tab, expand the details for a Cloud Volumes ONTAP system.
4. Click **Add Capacity License**.
5. Enter the serial number or upload the license file (or files if you have an HA pair).
6. Click **Add Capacity License**.

### Update capacity licenses

If you extended the term of an extra capacity license, you'll need to update the license in BlueXP.

#### Steps

1. From the left navigation menu, select **Digital Wallet**.
2. On the **Cloud Volumes ONTAP** tab, select **Node Based Licenses** from the drop-down.
3. In the **BYOL** tab, expand the details for a Cloud Volumes ONTAP system.
4. Click the action menu next to the capacity license and select **Update License**.
5. Upload the license file (or files if you have an HA pair).
6. Click **Update License**.

### Remove capacity licenses

If an extra capacity license expired and is no longer in use, then you can remove it at any time.

#### Steps

1. From the left navigation menu, select **Digital Wallet**.
2. On the **Cloud Volumes ONTAP** tab, select **Node Based Licenses** from the drop-down.
3. In the **BYOL** tab, expand the details for a Cloud Volumes ONTAP system.
4. Click the action menu next to the capacity license and select **Remove License**.
5. Click **Remove**.

### Convert an Eval license to a BYOL

An evaluation license is good for 30 days. You can apply a new BYOL license on top of the evaluation license for an in-place upgrade.

When you convert an Eval license to a BYOL, BlueXP restarts the Cloud Volumes ONTAP system.

- For a single-node system, the restart results in I/O interruption during the reboot process.
- For an HA pair, the restart initiates takeover and giveback to continue serving I/O to clients.

### Steps

1. From the left navigation menu, select **Digital Wallet**.
2. On the **Cloud Volumes ONTAP** tab, select **Node Based Licenses** from the drop-down.
3. Click **Eval**.
4. In the table, click **Convert to BYOL License** for a Cloud Volumes ONTAP system.
5. Enter the serial number or upload the license file.
6. Click **Convert License**.

### Result

BlueXP starts the conversion process. Cloud Volumes ONTAP automatically restarts as part of this process. When it's back up, the licensing information will reflect the new license.

### Change between PAYGO and BYOL

Converting a system from PAYGO by-node licensing to BYOL by-node licensing (and vice versa) isn't supported. If you want to switch between a pay-as-you-go subscription and a BYOL subscription, then you need to deploy a new system and replicate data from the existing system to the new system.

### Steps

1. Create a new Cloud Volumes ONTAP working environment.
2. Set up a one-time data replication between the systems for each volume that you need to replicate.

[Learn how to replicate data between systems](#)

3. Terminate the Cloud Volumes ONTAP system that you no longer need by deleting the original working environment.

[Learn how to delete a Cloud Volumes ONTAP working environment.](#)

## Volume and LUN administration

### Create FlexVol volumes

If you need more storage after you launch your initial Cloud Volumes ONTAP system, you can create new FlexVol volumes for NFS, CIFS, or iSCSI from BlueXP.

BlueXP provides several ways to create a new volume:

- Specify details for a new volume and let BlueXP handle the underlying data aggregates for you. [Learn more](#).
- Create a volume on a data aggregate of your choice. [Learn more](#).
- Create volume from a template to optimize the volume for the workload requirements for certain applications, such as databases or streaming services. [Learn more](#).
- Create a volume on the second node in an HA configuration. [Learn more](#).

## Before you get started

A few notes about volume provisioning:

- When you create an iSCSI volume, BlueXP automatically creates a LUN for you. We've made it simple by creating just one LUN per volume, so there's no management involved. After you create the volume, [use the IQN to connect to the LUN from your hosts](#).
- You can create additional LUNs from System Manager or the CLI.
- If you want to use CIFS in AWS, you must have set up DNS and Active Directory. For details, see [Networking requirements for Cloud Volumes ONTAP for AWS](#).
- If your Cloud Volumes ONTAP configuration supports the Amazon EBS Elastic Volumes feature, you might want to [learn more about what happens when you create a volume](#).

## Create a volume

The most common way to create a volume is to specify the type of volume that you need and then BlueXP handles the disk allocation for you. But you also have the option to choose the specific aggregate on which you want to create the volume.

### Steps

1. From the left navigation menu, select **Storage > Canvas**.
2. On the Canvas page, double-click the name of the Cloud Volumes ONTAP system on which you want to provision a FlexVol volume.
3. Create a new volume by letting BlueXP handle the disk allocation for you, or choose a specific aggregate for the volume.

Choosing a specific aggregate is recommended only if you have a good understanding of the data aggregates on your Cloud Volumes ONTAP system.

#### Any aggregate

In the Volumes tab, click **Add Volume > New volume**.

#### Specific aggregate

- a. Click the menu icon, and then click **Advanced > Advanced allocation**.
- b. Click the menu for an aggregate.
- c. Click **Create volume**.

4. Follow the steps in the wizard to create the volume.
  - a. **Details, Protection, and Tags:** Enter basic details about the volume and select a Snapshot policy.

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

Field	Description
Volume 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.

Field	Description
Tags	Tags that you add to a volume are associated with the <a href="#">Application Templates service</a> , which can help you organize and simplify the management of your resources.
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.

- b. **Protocol:** Choose a protocol for the volume (NFS, CIFS, or iSCSI) and then provide the required information.

If you select CIFS and a server isn't set up, BlueXP prompts you to set up CIFS connectivity after you click **Next**.

[Learn about supported client protocols and versions.](#)

The following sections describe fields for which you might need guidance. The descriptions are organized by protocol.

## NFS

### Access control

Choose a custom export policy to make the volume available to clients.

### Export policy

Defines the clients in the subnet that can access the volume. By default, BlueXP enters a value that provides access to all instances in the subnet.

## CIFS

### Permissions and users/groups

Enables you to control the level of access to an SMB 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.

### 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 AWS Managed Microsoft AD as the AD server for Cloud Volumes ONTAP, enter **OU=Computers,OU=corp** in this field.
- To configure Azure AD Domain Services as the AD server for Cloud Volumes ONTAP, 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](#)
- To configure Google Managed Microsoft AD as the AD server for Cloud Volumes ONTAP, enter **OU=Computers,OU=Cloud** in this field.  
[Google Cloud Documentation: Organizational Units in Google Managed Microsoft AD](#)

### DNS Domain

The DNS domain for the Cloud Volumes ONTAP storage virtual machine (SVM). In most cases, the domain is the same as the AD domain.

### NTP Server

Select **Use Active Directory Domain** to configure an NTP server using the Active Directory DNS. If you need to configure an NTP server using a different address, then you should use the API. See the [BlueXP automation docs](#) for details.

Note that you can configure an NTP server only when creating a CIFS server. It's not configurable after you create the CIFS server.

### iSCSI

#### LUN

iSCSI storage targets are called LUNs (logical units) and are presented to hosts as standard block devices. When you create an iSCSI volume, BlueXP automatically creates a LUN for you. We've made it simple by creating just one LUN per volume, so there's no management involved. After you create the volume, [use the IQN to connect to the LUN from your hosts](#).

#### Initiator group

Initiator groups (igroups) specify which hosts can access specified LUNs on the storage system

#### Host initiator (IQN)

iSCSI targets connect to the network through standard Ethernet network adapters (NICs), TCP offload engine (TOE) cards with software initiators, converged network adapters (CNAs) or dedicated host bus adapters (HBAs) and are identified by iSCSI qualified names (IQNs).

- c. **Disk Type:** Choose an underlying disk type for the volume based on your performance needs and cost requirements.
- [Sizing your system in AWS](#)
  - [Sizing your system in Azure](#)
  - [Sizing your system in Google Cloud](#)
- d. **Usage Profile & Tiering Policy:** Choose whether to enable or disable storage efficiency features on the volume and then select a [volume tiering policy](#).

ONTAP includes several storage efficiency features that can reduce the total amount of storage that you need. 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.

- e. **Review:** Review details about the volume and then click **Add**.

## Result

BlueXP creates the volume on the Cloud Volumes ONTAP system.

## Create a volume from a template


If your organization has created Cloud Volumes ONTAP volume templates so you can deploy volumes that are optimized for the workload requirements for certain applications, follow the steps in this section.

The template should make your job easier because certain volume parameters will already be defined in the template, such as disk type, size, protocol, snapshot policy, cloud provider, and more. When a parameter is already predefined, you can just skip to the next volume parameter.



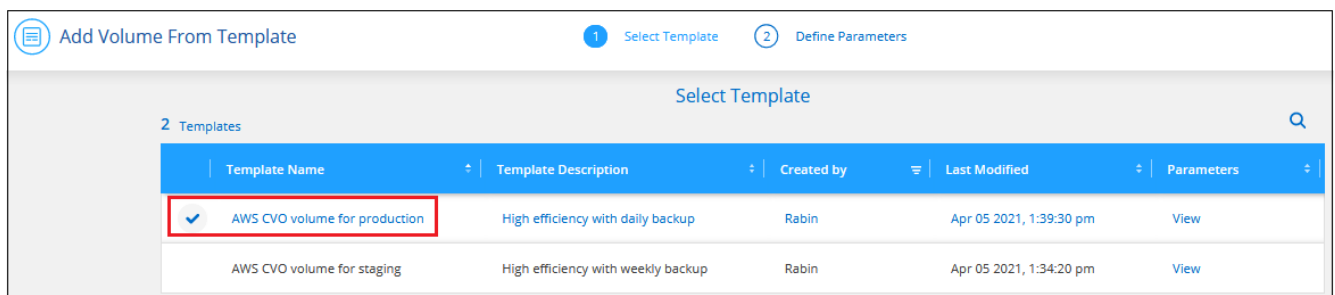
You can only create NFS or CIFS volumes when using templates.

## Steps

1. From the left navigation menu, select **Storage > Canvas**.
2. On the Canvas page, click the name of the Cloud Volumes ONTAP system on which you want to provision a volume.
3. Click  > **Add Volume From Template**.



4. In the *Select Template* page, select the template that you want to use to create the volume and click **Next**.



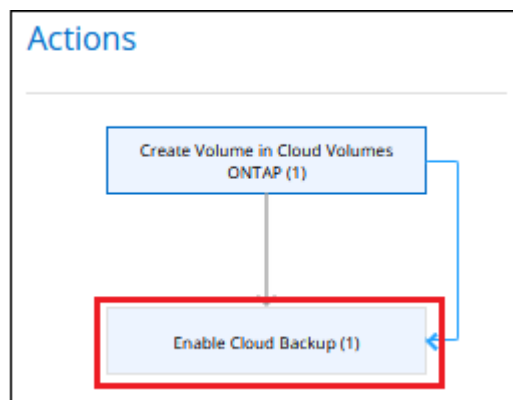
The *Define Parameters* page is displayed.



You can click the checkbox **Show read-only parameters** to show all the fields that have been locked by the template if you want to see the values for those parameters. By default these predefined fields are hidden and only the fields you need to complete are shown.

5. In the *Context* area, the Working Environment is filled in with the name of the working environment you started with. You need to select the **Storage VM** where the volume will be created.
6. Add values for all of the parameters that are not hard-coded from the template. See [Create a volume](#) for details about all the parameters you need to complete to deploy a Cloud Volumes ONTAP volume.
7. If there are no other Actions that you need to define (for example, configuring Cloud Backup), click **Run Template**.

If there are other actions, click the action in the left pane to display the parameters you need to complete.



For example, if the Enable Cloud Backup action requires that you select a backup policy, you can do that now.



8. Click **Run Template**.

## Result

Cloud Volumes ONTAP provisions the volume and displays a page so that you can see the progress.



Additionally, if any secondary action is implemented in the template, for example, enabling Cloud Backup on the volume, that action is also performed.

## Create a volume on the second node in an HA configuration

By default, BlueXP creates volumes on the first node in an HA configuration. If you need an active-active configuration, in which both nodes serve data to clients, you must create aggregates and volumes on the second node.

### Steps

1. From the left navigation menu, select **Storage > Canvas**.
2. On the Canvas page, double-click the name of the Cloud Volumes ONTAP working environment on which you want to manage aggregates.
3. Click the menu icon and then click **Advanced > Advanced allocation**.
4. Click **Add Aggregate** and then create the aggregate.
5. For Home Node, choose the second node in the HA pair.
6. After BlueXP creates the aggregate, select it and then click **Create volume**.
7. Enter details for the new volume, and then click **Create**.

## Result

BlueXP creates the volume on the second node in the HA pair.



For HA pairs deployed in multiple AWS Availability Zones, you must mount the volume to clients by using the floating IP address of the node on which the volume resides.

After you create a volume

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

Manage existing volumes


BlueXP enables you to manage volumes and CIFS servers. It also prompts you to move volumes to avoid capacity issues.



Manage volumes

You can manage volumes as your storage needs change. You can view, edit, clone, restore, and delete volumes.

Steps

- 1. From the left navigation menu, select **Storage > Canvas**.
- 2. On the Canvas page, double-click the Cloud Volumes ONTAP working environment on which you want to manage volumes.
- 3. Manage your volumes:

Task	Action
View information about a volume	Select a volume, and then click <b>Info</b> .
Edit a volume (read-write volumes only)	<div><div><div>a. Select a volume, and then click <b>Edit</b>.</div><div>b. Modify the volume’s Snapshot policy, NFS protocol version, NFS access control list (export policy), or share permissions, and then click <b>Update</b>.</div></div><div><div></div><div>If you need custom Snapshot policies, you can create them by using System Manager.</div></div></div>
Clone a volume	<div><div><div>a. Select a volume, and then click <b>Clone</b>.</div><div>b. Modify the clone name as needed, and then click <b>Clone</b>.</div></div><div><div>This process creates a FlexClone volume. A FlexClone volume is a writable, point-in-time copy that is space-efficient because it uses a small amount of space for metadata, and then only consumes additional space as data is changed or added.</div><div>To learn more about FlexClone volumes, see the <a href="#">ONTAP 9 Logical Storage Management Guide</a>.</div></div></div>

Task	Action
Restore data from a Snapshot copy to a new volume	<ol style="list-style-type: none"> <li>Select a volume, and then click <b>Restore from Snapshot copy</b>.</li> <li>Select a Snapshot copy, enter a name for the new volume, and then click <b>Restore</b>.</li> </ol>
Create a Snapshot copy on demand	<ol style="list-style-type: none"> <li>Select a volume, and then click <b>Create a Snapshot copy</b>.</li> <li>Change the name, if needed, and then click <b>Create</b>.</li> </ol>
Get the NFS mount command	<ol style="list-style-type: none"> <li>Select a volume, and then click <b>Mount Command</b>.</li> <li>Click <b>Copy</b>.</li> </ol>
View the target iQN for an iSCSI volume	<ol style="list-style-type: none"> <li>Select a volume, and then click <b>Target iQN</b>.</li> <li>Click <b>Copy</b>.</li> <li><a href="#">Use the IQN to connect to the LUN from your hosts</a>.</li> </ol>
Change the underlying disk type	<ol style="list-style-type: none"> <li>Select a volume, and then click <b>Change Disk Type &amp; Tiering Policy</b>.</li> <li>Select the disk type, and then click <b>Change</b>.</li> </ol> <div>  <p>BlueXP moves the volume to an existing aggregate that uses the selected disk type or it creates a new aggregate for the volume.</p> </div>
Change the tiering policy	<ol style="list-style-type: none"> <li>Select a volume, and then click <b>Change Disk Type &amp; Tiering Policy</b>.</li> <li>Click <b>Edit Policy</b>.</li> <li>Select a different policy and click <b>Change</b>.</li> </ol> <div>  <p>BlueXP moves the volume to an existing aggregate that uses the selected disk type with tiering, or it creates a new aggregate for the volume.</p> </div>
Delete a volume	<ol style="list-style-type: none"> <li>Select a volume, and then click <b>Delete</b>.</li> <li>Click <b>Delete</b> again to confirm.</li> </ol>

## Resize a volume

By default, a volume automatically grows to a maximum size when it's out of space. The default value is 1,000, which means the volume can grow to 11 times it's size. This value is configurable in a Connector's settings.

If you need to resize your volume, you can do it through [ONTAP System Manager](#). Be sure to take your system's capacity limits into consideration as you resize volumes. Go to the [Cloud Volumes ONTAP Release Notes](#) for more details.

## Modify the CIFS server

If you change your DNS servers or Active Directory domain, you need to modify the CIFS server in Cloud Volumes ONTAP so that it can continue to serve storage to clients.

### Steps

1. From the working environment, click the menu icon and then click **Advanced > CIFS setup**.
2. Specify settings for the CIFS server:

Task	Action
DNS Primary and Secondary IP Address	<p>The IP addresses of the DNS servers that provide name resolution for the CIFS server.</p> <p>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.</p> <p>If you're configuring Google Managed Active Directory, AD can be accessed by default with the 169.254.169.254 IP address.</p>
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	<p>The organizational unit within the AD domain to associate with the CIFS server. The default is CN=Computers.</p> <ul style="list-style-type: none"><li>• To configure AWS Managed Microsoft AD as the AD server for Cloud Volumes ONTAP, enter <b>OU=Computers,OU=corp</b> in this field.</li><li>• To configure Azure AD Domain Services as the AD server for Cloud Volumes ONTAP, enter <b>OU=AADDC Computers</b> or <b>OU=AADDC Users</b> in this field. <a href="#">Azure Documentation: Create an Organizational Unit (OU) in an Azure AD Domain Services managed domain</a></li><li>• To configure Google Managed Microsoft AD as the AD server for Cloud Volumes ONTAP, enter <b>OU=Computers,OU=Cloud</b> in this field. <a href="#">Google Cloud Documentation: Organizational Units in Google Managed Microsoft AD</a></li></ul>
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.

3. Click **Save**.

### Result

Cloud Volumes ONTAP updates the CIFS server with the changes.

## Move a volume

Move volumes for capacity utilization, improved performance, and to satisfy service-level agreements.

You can move a volume in System Manager by selecting a volume and the destination aggregate, starting the volume move operation, and optionally monitoring the volume move job. When using System Manager, a volume move operation finishes automatically.

### Steps

1. Use System Manager or the CLI to move the volumes to the aggregate.

In most situations, you can use System Manager to move volumes.

For instructions, see the [ONTAP 9 Volume Move Express Guide](#).

## Move a volume when BlueXP displays an Action Required message

BlueXP might display an Action Required message that says moving a volume is necessary to avoid capacity issues, but that you need to correct the issue yourself. If this happens, you need to identify how to correct the issue and then move one or more volumes.



BlueXP displays these Action Required messages when an aggregate has reached 90% used capacity. If data tiering is enabled, the messages display when an aggregate has reached 80% used capacity. By default, 10% free space is reserved for data tiering. [Learn more about the free space ratio for data tiering.](#)

### Steps

1. [Identify how to correct capacity issues.](#)
2. Based on your analysis, move volumes to avoid capacity issues:
  - [Move volumes to another system to avoid capacity issues.](#)
  - [Move volumes to another aggregate to avoid capacity issues.](#)

### Identify how to correct capacity issues

If BlueXP can't provide recommendations for moving a volume to avoid capacity issues, you must identify the volumes that you need to move and whether you should move them to another aggregate on the same system or to another system.

### Steps

1. View the advanced information in the Action Required message to identify the aggregate that has reached its capacity limit.

For example, the advanced information should say something similar to the following: Aggregate aggr1 has reached its capacity limit.

2. Identify one or more volumes to move out of the aggregate:
  - a. In the working environment, click the menu icon, and then click **Advanced > Advanced allocation**.
  - b. Select the aggregate, and then click **Info**.
  - c. Expand the list of volumes.



d. Review the size of each volume and choose one or more volumes to move out of the aggregate.

You should choose volumes that are large enough to free space in the aggregate so that you avoid additional capacity issues in the future.

3. If the system has not reached the disk limit, you should move the volumes to an existing aggregate or a new aggregate on the same system.

For details, see [Moving volumes to another aggregate to avoid capacity issues](#).

4. If the system has reached the disk limit, do any of the following:

- a. Delete any unused volumes.
- b. Rearrange volumes to free space on an aggregate.

For details, see [Moving volumes to another aggregate to avoid capacity issues](#).

c. Move two or more volumes to another system that has space.

For details, see [Moving volumes to another system to avoid capacity issues](#).

#### Move volumes to another system to avoid capacity issues

You can move one or more volumes to another Cloud Volumes ONTAP system to avoid capacity issues. You might need to do this if the system reached its disk limit.

#### About this task

You can follow the steps in this task to correct the following Action Required message:

Moving a volume is necessary to avoid capacity issues; however, BlueXP cannot perform this action for you because the system has reached the disk limit.

#### Steps

1. Identify a Cloud Volumes ONTAP system that has available capacity, or deploy a new system.
2. Drag and drop the source working environment on the target working environment to perform a one-time data replication of the volume.

For details, see [Replicating data between systems](#).

3. Go to the Replication Status page, and then break the SnapMirror relationship to convert the replicated volume from a data protection volume to a read/write volume.

For details, see [Managing data replication schedules and relationships](#).

4. Configure the volume for data access.

For information about configuring a destination volume for data access, see the [ONTAP 9 Volume Disaster Recovery Express Guide](#).

5. Delete the original volume.

For details, see [Manage volumes](#).

### Move volumes to another aggregate to avoid capacity issues

You can move one or more volumes to another aggregate to avoid capacity issues.

#### About this task

You can follow the steps in this task to correct the following Action Required message:

Moving two or more volumes is necessary to avoid capacity issues; however, BlueXP cannot perform this action for you.

#### Steps

1. Verify whether an existing aggregate has available capacity for the volumes that you need to move:
  - a. In the working environment, click the menu icon, and then click **Advanced > Advanced allocation**.
  - b. Select each aggregate, click **Info**, and then view the available capacity (aggregate capacity minus used aggregate capacity).

**aggr1**

Aggregate Capacity: 442.94 GB

Used Aggregate Capacity: 105.66 GB

2. If needed, add disks to an existing aggregate:
  - a. Select the aggregate, and then click **Add disks**.
  - b. Select the number of disks to add, and then click **Add**.
3. If no aggregates have available capacity, create a new aggregate.

For details, see [Creating aggregates](#).

4. Use System Manager or the CLI to move the volumes to the aggregate.
5. In most situations, you can use System Manager to move volumes.

For instructions, see the [ONTAP 9 Volume Move Express Guide](#).

## Reasons why a volume move might perform slowly

Moving a volume might take longer than you expect if any of the following conditions are true for Cloud Volumes ONTAP:

- The volume is a clone.
- The volume is a parent of a clone.
- The source or destination aggregate has a single Throughput Optimized HDD (st1) disk.
- One of the aggregates uses an older naming scheme for objects. Both aggregates have to use the same name format.

An older naming scheme is used if data tiering was enabled on an aggregate in the 9.4 release or earlier.

- The encryption settings don't match on the source and destination aggregates, or a rekey is in progress.
- The *-tiering-policy* option was specified on the volume move to change the tiering policy.
- The *-generate-destination-key* option was specified on the volume move.

## Tiering inactive data to low-cost object storage

You can reduce storage costs for Cloud Volumes ONTAP by combining an SSD or HDD performance tier for hot data with an object storage capacity tier for inactive data. Data tiering is powered by FabricPool technology. For a high-level overview, see [Data tiering overview](#).

To set up data tiering, you need to do the following:

1

### Choose a supported configuration

Most configurations are supported. If you have a Cloud Volumes ONTAP system running the most recent version, then you should be good to go. [Learn more](#).

2

### Ensure connectivity between Cloud Volumes ONTAP and object storage

- For AWS, you'll need a VPC Endpoint to S3. [Learn more](#).
- For Azure, you won't need to do anything as long as BlueXP has the required permissions. [Learn more](#).
- For Google Cloud, you need to configure the subnet for Private Google Access and set up a service account. [Learn more](#).

3

### Ensure that you have an aggregate with tiering enabled

Data tiering must be enabled on an aggregate in order to enable data tiering on a volume. You should be aware of the requirements for new volumes and for existing volumes. [Learn more](#).



## 4

### Choose a tiering policy when creating, modifying, or replicating a volume

BlueXP prompts you to choose a tiering policy when you create, modify, or replicate a volume.

- [Tiering data on read-write volumes](#)
- [Tiering data on data protection volumes](#)

#### What's not required for data tiering?

- You don't need to install a feature license to enable data tiering.
- You don't need to create an object store for the capacity tier. BlueXP does that for you.
- You don't need to enable data tiering at the system level.



BlueXP creates an object store for cold data when the system is created, [as long as there are no connectivity or permissions issues](#). After that, you just need to enable data tiering on volumes (and in some cases, [on aggregates](#)).

### Configurations that support data tiering

You can enable data tiering when using specific configurations and features.

#### Support in AWS

- Data tiering is supported in AWS starting with Cloud Volumes ONTAP 9.2.
- The performance tier can be General Purpose SSDs (gp3 or gp2) or Provisioned IOPS SSDs (io1).



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

#### Support in Azure

- Data tiering is supported in Azure as follows:
  - Version 9.4 in with single node systems
  - Version 9.6 in with HA pairs
- The performance tier can be Premium SSD managed disks, Standard SSD managed disks, or Standard HDD managed disks.

#### Support in Google Cloud

- Data tiering is supported in Google Cloud starting with Cloud Volumes ONTAP 9.6.
- The performance tier can be either SSD persistent disks, balanced persistent disks, or standard persistent disks.

#### Feature interoperability

- Data tiering is supported with encryption technologies.
- Thin provisioning must be enabled on volumes.

## Requirements

Depending on your cloud provider, certain connections and permissions must be set up so that Cloud Volumes ONTAP can tier cold data to object storage.

### Requirements to tier cold data to AWS S3

Ensure that Cloud Volumes ONTAP has a connection to S3. The best way to provide that connection is by creating a VPC Endpoint to the S3 service. For instructions, see [AWS Documentation: Creating a Gateway Endpoint](#).

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

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

### Requirements to tier cold data to Azure Blob storage

You don't need to set up a connection between the performance tier and the capacity tier as long as BlueXP has the required permissions. BlueXP enables a VNet service endpoint for you if the custom role for the Connector has these permissions:

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

The permissions are included in the custom role by default. [View Azure permission for the Connector](#)

### Requirements 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](#).
- A service account must be attached to Cloud Volumes ONTAP.

[Learn how to set up this service account.](#)

You're prompted to select this service account when you create a Cloud Volumes ONTAP working environment.

If you don't select a service account during deployment, you'll need to shut down Cloud Volumes ONTAP, go to the Google Cloud console, and then attach the service account to the Cloud Volumes ONTAP instances. You can then enable data tiering as described in the next section.

- To encrypt the bucket with customer-managed encryption keys, enable the Google Cloud storage bucket to use the key.

[Learn how to use customer-managed encryption keys with Cloud Volumes ONTAP.](#)

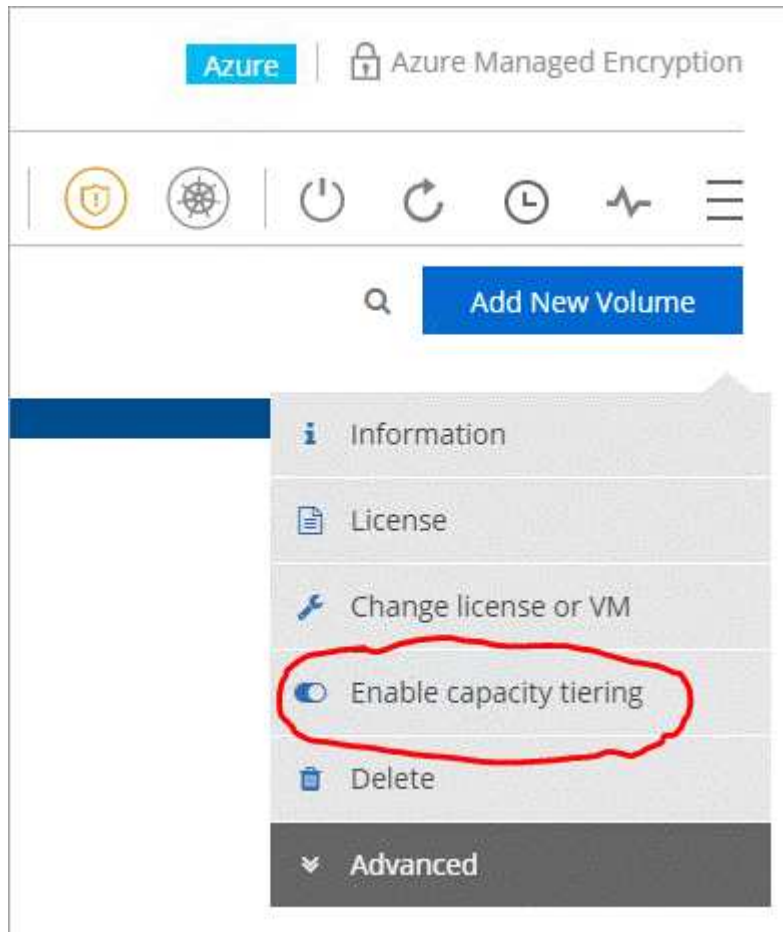
### Enabling data tiering after implementing the requirements

BlueXP creates an object store for cold data when the system is created, as long as there are no connectivity or permissions issues. If you didn't implement the requirements listed above until after you created the system,

then you'll need to manually enable tiering, which creates the object store.

### Steps

1. [Ensure that you've met all requirements.](#)
2. From the left navigation menu, select **Storage > Canvas**.
3. On the Canvas page, double-click the name of the Cloud Volumes ONTAP instance.
4. Click the menu icon and select **Enable capacity tiering**.



You'll only see this option if data tiering couldn't be enabled when BlueXP created the system.

In Google Cloud, a service account must be attached to Cloud Volumes ONTAP before this option will appear. [Ensure that you've met all requirements.](#)

5. Click **Enable** so BlueXP can create the object store that this Cloud Volumes ONTAP system will use for tiered data.

### Ensuring that tiering is enabled on aggregates

Data tiering must be enabled on an aggregate in order to enable data tiering on a volume. You should be aware of the requirements for new volumes and for existing volumes.

- **New volumes**

If you're enabling data tiering on a new volume, then you don't need to worry about enabling data tiering on an aggregate. BlueXP creates the volume on an existing aggregate that has tiering enabled, or it creates a

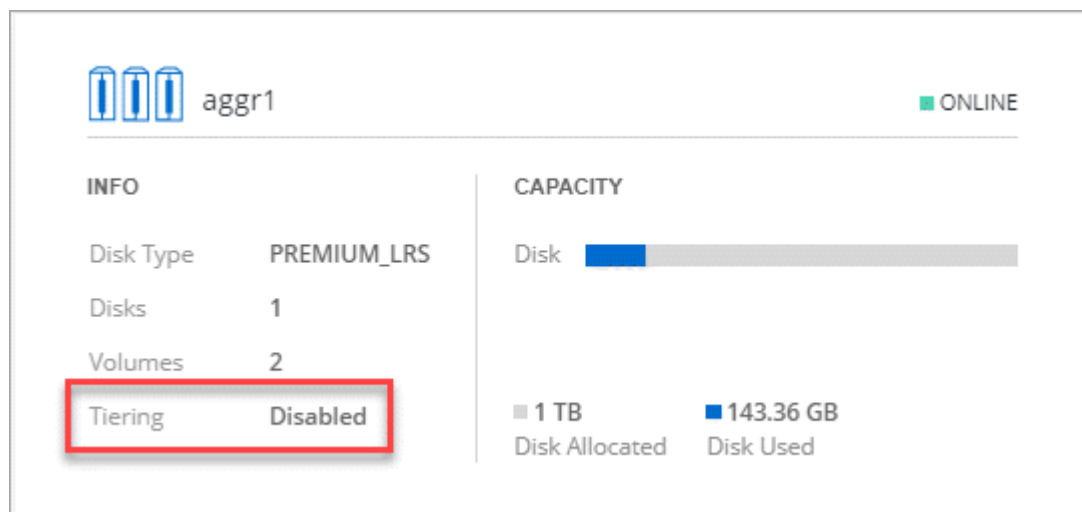
new aggregate for the volume if a data tiering-enabled aggregate doesn't already exist.

- **Existing volumes**

If you want to enable data tiering on an existing volume, then you'll need to ensure that data tiering is enabled on the underlying aggregate. If data tiering isn't enabled on the existing aggregate, then you'll need to use System Manager to attach an existing aggregate to the object store.

**Steps to confirm whether tiering is enabled on an aggregate**

1. Open the working environment in BlueXP.
2. Click the menu icon, click **Advanced**, and then click **Advanced allocation**.
3. Verify whether tiering is enabled or disabled on the aggregate.



**Steps to enable tiering on an aggregate**

1. In System Manager, click **Storage > Tiers**.
2. Click the action menu for the aggregate and select **Attach Cloud Tiers**.
3. Select the cloud tier to attach and click **Save**.

**What's next?**

You can now enable data tiering on new and existing volumes, as explained in the next section.

**Tiering data from read-write volumes**

Cloud Volumes ONTAP can tier inactive data on read-write volumes to cost-effective object storage, freeing up the performance tier for hot data.

**Steps**

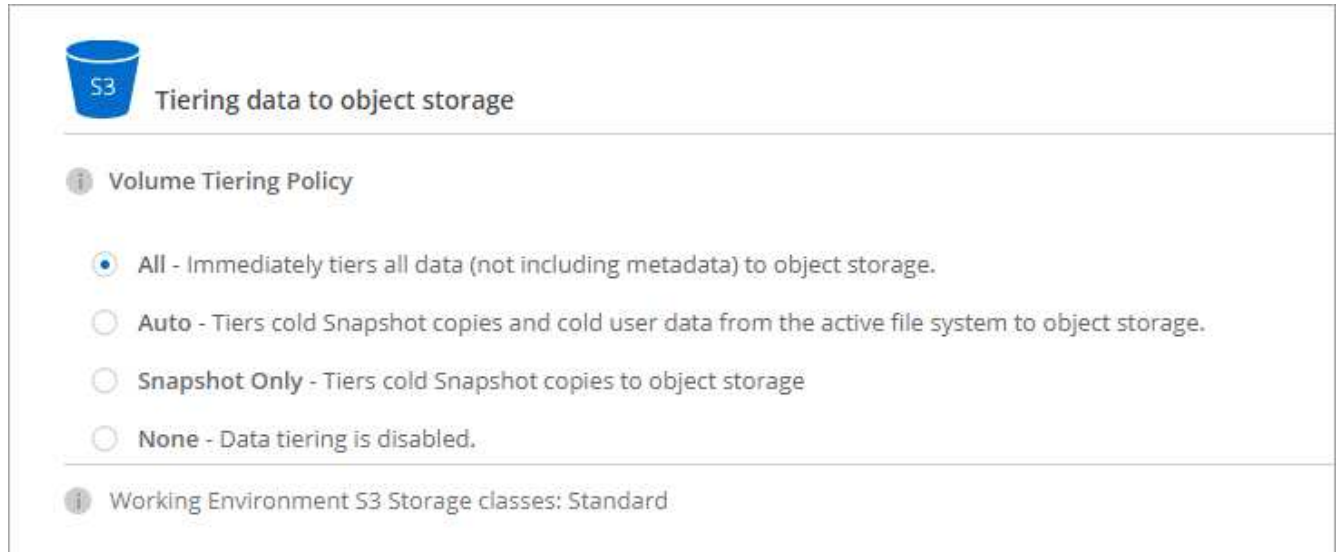
1. In the working environment, create a new volume or change the tier of an existing volume:

Task	Action
Create a new volume	Click <b>Add New Volume</b> .
Modify an existing volume	Select the volume and click <b>Change Disk Type &amp; Tiering Policy</b> .

2. Select a tiering policy.

For a description of these policies, see [Data tiering overview](#).

### Example



BlueXP creates a new aggregate for the volume if a data tiering-enabled aggregate does not already exist.

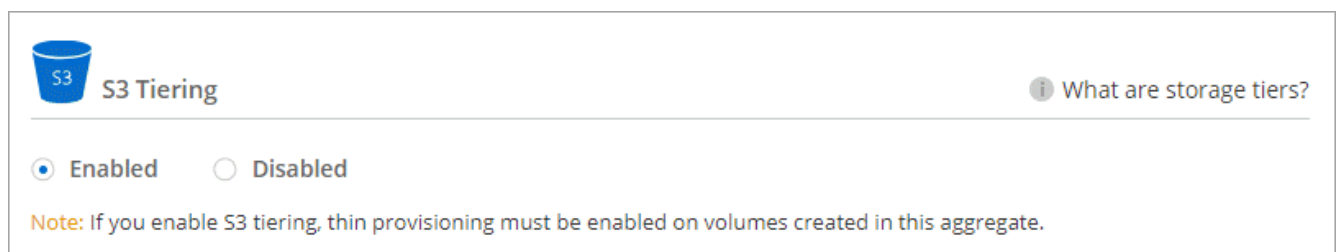
### Tiering data from data protection volumes

Cloud Volumes ONTAP can tier data from a data protection volume to a capacity tier. If you activate the destination volume, the data gradually moves to the performance tier as it is read.

#### Steps

1. From the left navigation menu, select **Storage > Canvas**.
2. On the Canvas page, select the working environment that contains the source volume, and then drag it to the working environment to which you want to replicate the volume.
3. Follow the prompts until you reach the tiering page and enable data tiering to object storage.

### Example



For help with replicating data, see [Replicating data to and from the cloud](#).

### Changing the storage class for tiered data

After you deploy Cloud Volumes ONTAP, you can reduce your storage costs by changing the storage class for inactive data that hasn't been accessed for 30 days. The access costs are higher if you do access the data, so

you must take that into consideration before you change the storage class.

The storage class for tiered data is system wide—it's not per volume.

For information about supported storage classes, see [Data tiering overview](#).

### Steps

1. From the working environment, click the menu icon and then click **Storage Classes** or **Blob Storage Tiering**.
2. Choose a storage class and then click **Save**.

### Changing the free space ratio for data tiering

The free space ratio for data tiering defines how much free space is required on Cloud Volumes ONTAP SSDs/HDDs when tiering data to object storage. The default setting is 10% free space, but you can tweak the setting based on your requirements.

For example, you might choose less than 10% free space to ensure that you are utilizing the purchased capacity. BlueXP can then purchase additional disks for you when additional capacity is required (up until you reach the disk limit for the aggregate).



If there isn't sufficient space, then Cloud Volumes ONTAP can't move the data and you might experience performance degradation. Any change should be done with caution. If you're unsure, reach out to NetApp support for guidance.

The ratio is important for disaster recovery scenarios because as data is read from the object store, Cloud Volumes ONTAP moves the data to SSDs/HDDs to provide better performance. If there isn't sufficient space, then Cloud Volumes ONTAP can't move the data. Take this into consideration when changing the ratio so that you can meet your business requirements.

### Steps

1. In the upper right of the BlueXP console, click the **Settings** icon, and select **Connector Settings**.



2. Under **Capacity**, click **Aggregate Capacity Thresholds - Free Space Ratio for Data Tiering**.
3. Change the free space ratio based on your requirements and click **Save**.

### Changing the cooling period for the auto tiering policy

If you enabled data tiering on a Cloud Volumes ONTAP volume using the *auto* tiering policy, you can adjust the default cooling period based on your business needs. This action is supported using the API only.

The cooling period is the number of days that user data in a volume must remain inactive before it is considered "cold" and moved to object storage.

The default cooling period for the auto tiering policy is 31 days. You can change the cooling period as follows:

- 9.8 or later: 2 days to 183 days

- 9.7 or earlier: 2 days to 63 days

### Step

1. Use the *minimumCoolingDays* parameter with your API request when creating a volume or modifying an existing volume.

## Connect a LUN to a host

When you create an iSCSI volume, BlueXP automatically creates a LUN for you. We've made it simple by creating just one LUN per volume, so there's no management involved. After you create the volume, use the IQN to connect to the LUN from your hosts.

Note the following:

- BlueXP's automatic capacity management doesn't apply to LUNs. When BlueXP creates a LUN, it disables the autogrow feature.
- You can create additional LUNs from System Manager or the CLI.

### Steps

1. From the left navigation menu, select **Storage > Canvas**.
2. On the Canvas page, double-click the Cloud Volumes ONTAP working environment on which you want to manage volumes.
3. Select a volume, and then click **Target iQN**.
4. Click **Copy** to copy the iQN name.
5. Set up an iSCSI connection from the host to the LUN.
  - [ONTAP 9 iSCSI express configuration for Red Hat Enterprise Linux: Starting the iSCSI sessions with the target](#)
  - [ONTAP 9 iSCSI express configuration for Windows: Starting iSCSI sessions with the target](#)
  - [ONTAP SAN host configuration](#)

## Accelerate data access with FlexCache volumes

A FlexCache volume is a storage volume that caches NFS read data from an origin (or source) volume. Subsequent reads to the cached data result in faster access to that data.

You can use FlexCache volumes to speed up access to data or to offload traffic from heavily accessed volumes. FlexCache volumes help improve performance, especially when clients need to access the same data repeatedly, because the data can be served directly without having to access the origin volume. FlexCache volumes work well for system workloads that are read-intensive.

BlueXP does not provide management of FlexCache volumes at this time, but you can use the ONTAP CLI or ONTAP System Manager to create and manage FlexCache volumes:

- [FlexCache Volumes for Faster Data Access Power Guide](#)
- [Creating FlexCache volumes in System Manager](#)

Starting with the 3.7.2 release, BlueXP generates a FlexCache license for all new Cloud Volumes ONTAP systems. The license includes a 500 GiB usage limit.





## Aggregate administration

### Create aggregates

You can create aggregates yourself or let BlueXP do it for you when it creates volumes. The benefit of creating aggregates yourself is that you can choose the underlying disk size, which enables you to size your aggregate for the capacity or the performance that you need.



All disks and aggregates must be created and deleted directly from BlueXP. You should not perform these actions from another management tool. Doing so can impact system stability, hamper the ability to add disks in the future, and potentially generate redundant cloud provider fees.

### Steps

1. From the left navigation menu, select **Storage > Canvas**.
2. On the Canvas page, double-click the name of the Cloud Volumes ONTAP instance on which you want to manage aggregates.
3. Click the menu icon, and then click **Advanced > Advanced allocation**.
4. Click **Add Aggregate** and then specify details for the aggregate.



## AWS

- If you're prompted to choose a disk type and disk size, refer to [Plan your Cloud Volumes ONTAP configuration in AWS](#).
- If you're prompted to enter the aggregate's capacity size, then you're creating an aggregate on a configuration that supports the Amazon EBS Elastic Volumes feature. The following screenshot shows an example of a new aggregate comprised of gp3 disks.



[Learn more about support for Elastic Volumes.](#)

## Azure

For help with disk type and disk size, refer to [Plan your Cloud Volumes ONTAP configuration in Azure](#).

## Google Cloud

For help with disk type and disk size, refer to [Plan your Cloud Volumes ONTAP configuration in Google Cloud](#).

5. Click **Go**, and then click **Approve and Purchase**.

## Manage aggregates

Manage aggregates yourself by adding disks, viewing information about the aggregates, and by deleting them.



All disks and aggregates must be created and deleted directly from BlueXP. You should not perform these actions from another management tool. Doing so can impact system stability, hamper the ability to add disks in the future, and potentially generate redundant cloud provider fees.

### Before you begin

If you want to delete an aggregate, you must have first deleted the volumes in the aggregate.


### About this task

If an aggregate is running out of space, you can move volumes to another aggregate by using System

Manager.

### Steps

1. From the left navigation menu, select **Storage > Canvas**.
2. On the Canvas page, double-click the Cloud Volumes ONTAP working environment on which you want to manage aggregates.
3. Click the menu icon and then click **Advanced > Advanced allocation**.
4. Manage your aggregates:

Task	Action
View information about an aggregate	Select an aggregate and click <b>Info</b> .
Create a volume on a specific aggregate	Select an aggregate and click <b>Create volume</b> .
Add disks to an aggregate	<ol style="list-style-type: none"><li>a. Select an aggregate and click <b>Add disks</b>.</li><li>b. Select the number of disks that you want to add and click <b>Add</b>.</li></ol> <div> All disks in an aggregate must be the same size.</div>
Increase the capacity of an aggregate that supports Amazon EBS Elastic Volumes	<ol style="list-style-type: none"><li>a. Select an aggregate and click <b>Increase capacity</b>.</li><li>b. Enter the additional capacity that you'd like to add and then click <b>Add</b>.</li></ol> <p>Note that you must increase the capacity of the aggregate by a minimum of 256 GiB or 10% of the aggregate's size.</p> <p>For example, if you have a 1.77 TiB aggregate, 10% is 181 GiB. That's lower than 256 GiB, so the size of the aggregate must be increased by the 256 GiB minimum.</p>
Delete an aggregate	<ol style="list-style-type: none"><li>a. Select an aggregate that does not contain any volumes and click <b>Delete</b>.</li><li>b. Click <b>Delete</b> again to confirm.</li></ol>

## Manage capacity settings on a Connector

Each Connector has settings that determines how it manages aggregate capacity for Cloud Volumes ONTAP.

These settings affect all Cloud Volumes ONTAP systems managed by a Connector. If you have another Connector, it can be configured differently.

### Required permissions

Account Admin privileges are required to modify Connector settings.

### Steps

1. In the upper right of the BlueXP console, click the Settings icon, and select **Connector Settings**.
2. Under **Capacity**, modify any of the following settings:

#### **Capacity Management Mode**

Choose whether BlueXP notifies you of storage capacity decisions or whether BlueXP automatically manages capacity requirements for you.

[Learn how Capacity Management Mode works.](#)

#### **Free Space Ratio**

Triggers a notification when the free space ratio on an aggregate drops below the specified threshold.

The free space ratio is calculated as follows:

$(\text{aggregate capacity} - \text{total used capacity on the aggregate}) / \text{aggregate capacity}$

#### **Free Space Ratio for Data Tiering**

Defines how much free space is required on the performance tier (disks) when tiering data to a capacity tier (object storage).

The ratio is important for disaster recovery scenarios. As data is read from the capacity tier, Cloud Volumes ONTAP moves data to the performance tier to provide better performance. If there isn't sufficient space, then Cloud Volumes ONTAP can't move the data.

3. Click **Save**.

## **Storage VM administration**

### **Manage storage VMs in BlueXP**

A storage VM is a virtual machine running within ONTAP that provides storage and data services to your clients. You might know this as an *SVM* or a *vserver*. Cloud Volumes ONTAP is configured with one storage VM by default, but some configurations support additional storage VMs.

#### **Supported number of storage VMs**

Multiple storage VMs are supported with certain configurations. Go to the [Cloud Volumes ONTAP Release Notes](#) to verify the supported number of storage VMs for your version of Cloud Volumes ONTAP.

#### **Work with multiple storage VMs**

BlueXP supports any additional storage VMs that you create from System Manager or the CLI.

For example, the following image shows how you can choose a storage VM when you create a volume.

### Details & Protection

Storage VM Name

svm\_name1

Volume Name

Size (GiB)

Volume size

Snapshot Policy

default

Default Policy

And the following image shows how you can choose a storage VM when replicating a volume to another system.

Destination Volume Name

volume\_copy

Destination Storage VM Name

svm\_name1

Destination Aggregate

Automatically select the best aggregate

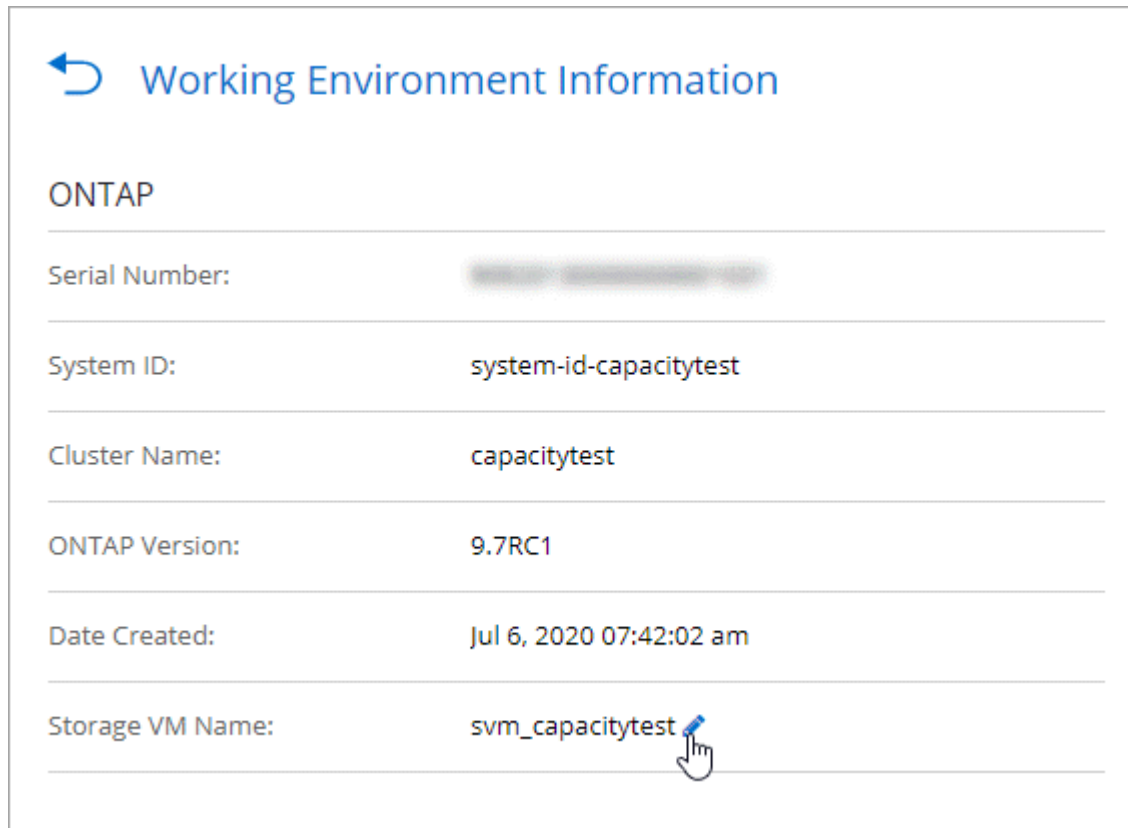
### Modify the name of the default storage VM

BlueXP automatically names the single storage VM that it creates for Cloud Volumes ONTAP. You can modify the name of the storage VM if you have strict naming standards. For example, you might want the name to match how you name the storage VMs for your ONTAP clusters.

If you created any additional storage VMs for Cloud Volumes ONTAP, then you can't rename the storage VMs from BlueXP. You'll need to do so directly from Cloud Volumes ONTAP by using System Manager or the CLI.

## Steps

1. From the working environment, click the menu icon, and then click **Information**.
2. Click the edit icon to the right of the storage VM name.

The image shows a 'Working Environment Information' dialog box. It has a title bar with a blue circular arrow icon and the text 'Working Environment Information'. Below the title bar, there is a section titled 'ONTAP'. This section contains several fields with labels on the left and values on the right, separated by horizontal lines. The fields are: 'Serial Number:' with a blurred value; 'System ID:' with the value 'system-id-capacitytest'; 'Cluster Name:' with the value 'capacitytest'; 'ONTAP Version:' with the value '9.7RC1'; 'Date Created:' with the value 'Jul 6, 2020 07:42:02 am'; and 'Storage VM Name:' with the value 'svm\_capacitytest'. A blue pencil icon is positioned to the right of the 'Storage VM Name' value, indicating it is editable.

3. In the Modify SVM Name dialog box, change the name, and then click **Save**.

## Manage storage VMs for disaster recovery

BlueXP doesn't provide any setup or orchestration support for storage VM disaster recovery. You must use System Manager or the CLI.

- [SVM Disaster Recovery Preparation Express Guide](#)
- [SVM Disaster Recovery Express Guide](#)

## Create data-serving storage VMs for Cloud Volumes ONTAP in AWS

A storage VM is a virtual machine running within ONTAP that provides storage and data services to your clients. You might know this as an *SVM* or a *vserver*. Cloud Volumes ONTAP is configured with one storage VM by default, but some configurations support additional storage VMs.

To create additional data-serving storage VMs, you need to allocate IP addresses in AWS and then run ONTAP commands based on your Cloud Volumes ONTAP configuration.

## Supported number of storage VMs

Multiple storage VMs are supported with specific Cloud Volumes ONTAP configurations starting with the 9.7

release. Go to the [Cloud Volumes ONTAP Release Notes](#) to verify the supported number of storage VMs for your version of Cloud Volumes ONTAP.

All other Cloud Volumes ONTAP configurations support one data-serving storage VM and one destination storage VM used for disaster recovery. You can activate the destination storage VM for data access if there's an outage on the source storage VM.

**Verify limits for your configuration**

Each EC2 instance supports a maximum number of private IPv4 addresses per network interface. You need to verify the limit before you allocate IP addresses in AWS for the new storage VM.

**Steps**

- 1. Go the [Storage limits section in the Cloud Volumes ONTAP Release Notes](#).
- 2. Identify the maximum number of IP addresses per interface for your instance type.
- 3. Make note of this number because you'll need it in the next section when you allocate IP addresses in AWS.

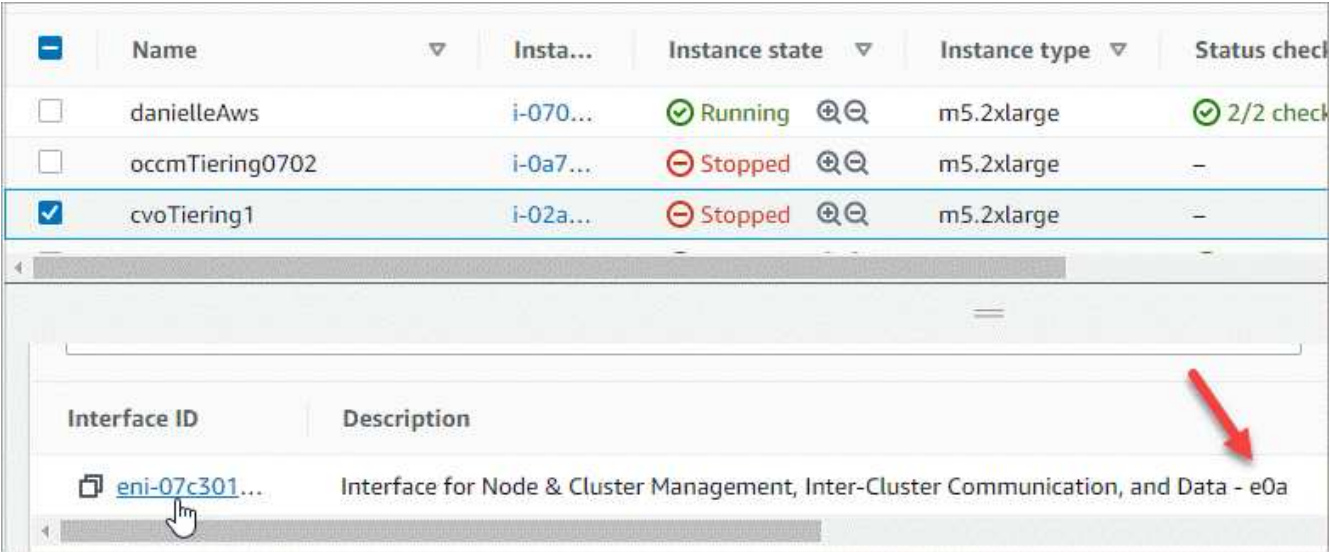
**Allocate IP addresses in AWS**

Private IPv4 addresses must be assigned to port e0a in AWS before you create LIFs for the new storage VM.

Note that an optional management LIF for a storage VM requires a private IP address on a single node system and on an HA pair in a single AZ. This management LIF provides a connection to management tools like SnapCenter.

**Steps**

- 1. Log in to AWS and open the EC2 service.
- 2. Select the Cloud Volumes ONTAP instance and click **Networking**.  
  
If you're creating a storage VM on an HA pair, select node 1.
- 3. Scroll down to **Network interfaces** and click the **Interface ID** for port e0a.



- 4. Select the network interface and click **Actions > Manage IP addresses**.

5. Expand the list of IP addresses for e0a.

6. Verify the IP addresses:

- a. Count the number of allocated IP addresses to confirm that the port has room for additional IPs.

You should have identified the maximum number of supported IP addresses per interface in the previous section of this page.

- b. Optional: Go to the CLI for Cloud Volumes ONTAP and run **network interface show** to confirm that each of these IP addresses are in use.

If an IP address isn't in use, then you can use it with the new storage VM.

7. Back in the AWS Console, click **Assign new IP address** to assign additional IP addresses based on the amount that you need for the new storage VM.

- Single node system: One unused secondary private IP is required.

An optional secondary private IP is required if you want to create a management LIF on the storage VM.

- HA pair in a single AZ: One unused secondary private IP is required on node 1.

An optional secondary private IP is required if you want to create a management LIF on the storage VM.

- HA pair in multiple AZs: One unused secondary private IP is required on each node.

8. If you're allocating the IP address on an HA pair in a single AZ, enable **Allow secondary private IPv4 addresses to be reassigned**.

9. Click **Save**.

10. If you have an HA pair in multiple AZs, then you'll need to repeat these steps for node 2.

### Create a storage VM on a single node system

These steps create a new storage VM on a single node system. One private IP address is required to create a NAS LIF and another optional private IP address is needed if you want to create a management LIF.

#### Steps

1. Create the storage VM and a route to the storage VM.

```
vserver create -rootvolume-security-style unix -rootvolume root_svm_2  
-snapshot-policy default -vserver svm_2 -aggregate aggr1
```

```
network route create -destination 0.0.0.0/0 -vserver svm_2 -gateway  
subnet_gateway
```

2. Create a NAS LIF.

```
network interface create -auto-revert true -vserver svm_2 -service
-policy default-data-files -home-port e0a -address private_ip_x -netmask
node1Mask -lif ip_nas_2 -home-node cvo-node
```

Where *private\_ip\_x* is an unused secondary private IP on e0a.

### 3. Optional: Create a storage VM management LIF.

```
network interface create -auto-revert true -vserver svm_2 -service
-policy default-management -home-port e0a -address private_ip_y -netmask
node1Mask -lif ip_svm_mgmt_2 -home-node cvo-node
```

Where *private\_ip\_y* is another unused secondary private IP on e0a.

### 4. Assign one or more aggregates to the storage VM.

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

This step is required because the new storage VM needs access to at least one aggregate before you can create volumes on the storage VM.

## Create a storage VM on an HA pair in a single AZ

These steps create a new storage VM on an HA pair in a single AZ. One private IP address is required to create a NAS LIF and another optional private IP address is needed if you want to create a management LIF.

Both of these LIFs get allocated on node 1. The private IP addresses can move between nodes if failures occur.

### Steps

#### 1. Create the storage VM and a route to the storage VM.

```
vserver create -rootvolume-security-style unix -rootvolume root_svm_2
-snapshot-policy default -vserver svm_2 -aggregate aggr1
```

```
network route create -destination 0.0.0.0/0 -vserver svm_2 -gateway
subnet_gateway
```

#### 2. Create a NAS LIF on node 1.



```
network interface create -auto-revert true -vserver svm_2 -service
-policy default-data-files -home-port e0a -address private_ip_x -netmask
node1Mask -lif ip_nas_2 -home-node cvo-node1
```

Where *private\_ip\_x* is an unused secondary private IP on e0a of cvo-node1. This IP address can be relocated to the e0a of cvo-node2 in case of takeover because the service policy default-data-files indicates that IPs can migrate to the partner node.

3. Optional: Create a storage VM management LIF on node 1.

```
network interface create -auto-revert true -vserver svm_2 -service
-policy default-management -home-port e0a -address private_ip_y -netmask
node1Mask -lif ip_svm_mgmt_2 -home-node cvo-node1
```

Where *private\_ip\_y* is another unused secondary private IP on e0a.

4. Assign one or more aggregates to the storage VM.

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

This step is required because the new storage VM needs access to at least one aggregate before you can create volumes on the storage VM.

5. If you're running Cloud Volumes ONTAP 9.11.1 or later, modify the network service policies for the storage VM.

Modifying the services is required because it ensures that Cloud Volumes ONTAP can use the iSCSI LIF for outbound management connections.

```

network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service data-fpolicy-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ad-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-dns-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ldap-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-nis-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-ad-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-dns-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-ldap-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-nis-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-ad-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-dns-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-ldap-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-nis-client

```

## Create a storage VM on an HA pair in multiple AZs

These steps create a new storage VM on an HA pair in multiple AZs.

A *floating* IP address is required for a NAS LIF and is optional for a management LIF. These floating IP addresses don't require you to allocate private IPs in AWS. Instead, the floating IPs are automatically configured in the AWS route table to point to a specific node's ENI in the same VPC.

In order for floating IPs to work with ONTAP, a private IP address must be configured on every storage VM on each node. This is reflected in the steps below where an iSCSI LIF is created on node 1 and on node 2.

### Steps

1. Create the storage VM and a route to the storage VM.

```
vserver create -rootvolume-security-style unix -rootvolume root_svm_2
-snapshot-policy default -vserver svm_2 -aggregate aggr1
```

```
network route create -destination 0.0.0.0/0 -vserver svm_2 -gateway
subnet_gateway
```

## 2. Create a NAS LIF on node 1.

```
network interface create -auto-revert true -vserver svm_2 -service
-policy default-data-files -home-port e0a -address floating_ip -netmask
node1Mask -lif ip_nas_floating_2 -home-node cvo-node1
```

- The floating IP address must be outside of the CIDR blocks for all VPCs in the AWS region in which you deploy the HA configuration. 192.168.209.27 is an example floating IP address. [Learn more about choosing a floating IP address.](#)
- `-service-policy default-data-files` indicates that IPs can migrate to the partner node.

## 3. Optional: Create a storage VM management LIF on node 1.

```
network interface create -auto-revert true -vserver svm_2 -service
-policy default-management -home-port e0a -address floating_ip -netmask
node1Mask -lif ip_svm_mgmt_2 -home-node cvo-node1
```

## 4. Create an iSCSI LIF on node 1.

```
network interface create -vserver svm_2 -service-policy default-data-
blocks -home-port e0a -address private_ip -netmask node1Mask -lif
ip_node1_iscsi_2 -home-node cvo-node1
```

- This iSCSI LIF is required to support LIF migration of the floating IPs in the storage VM. It doesn't have to be an iSCSI LIF, but it can't be configured to migrate between nodes.
- `-service-policy default-data-block` indicates that an IP address does not migrate between nodes.
- `private_ip` is an unused secondary private IP address on eth0 (e0a) of cvo\_node1.

## 5. Create an iSCSI LIF on node 2.

```
network interface create -vserver svm_2 -service-policy default-data-
blocks -home-port e0a -address private_ip -netmaskNode2Mask -lif
ip_node2_iscsi_2 -home-node cvo-node2
```

- This iSCSI LIF is required to support LIF migration of the floating IPs in the storage VM. It doesn't have to be an iSCSI LIF, but it can't be configured to migrate between nodes.
- `-service-policy default-data-block` indicates that an IP address does not migrate between nodes.
- `private_ip` is an unused secondary private IP address on eth0 (e0a) of `cvo_node2`.

6. Assign one or more aggregates to the storage VM.

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

This step is required because the new storage VM needs access to at least one aggregate before you can create volumes on the storage VM.

7. If you're running Cloud Volumes ONTAP 9.11.1 or later, modify the network service policies for the storage VM.

Modifying the services is required because it ensures that Cloud Volumes ONTAP can use the iSCSI LIF for outbound management connections.

```

network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service data-fpolicy-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ad-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-dns-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ldap-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-nis-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-ad-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-dns-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-ldap-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-nis-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-ad-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-dns-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-ldap-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-nis-client

```

## Create data-serving storage VMs for Cloud Volumes ONTAP in Azure

A storage VM is a virtual machine running within ONTAP that provides storage and data services to your clients. You might know this as an *SVM* or a *vserver*. Cloud Volumes ONTAP is configured with one storage VM by default, but additional storage VMs are supported when running Cloud Volumes ONTAP in Azure.

To create additional data-serving storage VMs, you need to allocate IP addresses in Azure and then run ONTAP commands to create the storage VM and data LIFs.

### Supported number of storage VMs

Multiple storage VMs are supported with specific Cloud Volumes ONTAP configurations starting with the 9.9.0 release. Go to the [Cloud Volumes ONTAP Release Notes](#) to verify the supported number of storage VMs for your version of Cloud Volumes ONTAP.

All other Cloud Volumes ONTAP configurations support one data-serving storage VM and one destination storage VM used for disaster recovery. You can activate the destination storage VM for data access if there's an outage on the source storage VM.

## Allocate IP addresses in Azure

You need to allocate IP addresses in Azure before you create a storage VM and allocate LIFs.

### Single node system

IP addresses must be assigned to nic0 in Azure before you create a storage VM and allocate LIFs.

You'll need to create an IP address for data LIF access and another optional IP address for a storage VM (SVM) management LIF. This management LIF provides a connection to management tools like SnapCenter.

### Steps

1. Log in to the Azure portal and open the **Virtual machine** service.
2. Click the name of the Cloud Volumes ONTAP VM.
3. Click **Networking**.
4. Click the name of the network interface for nic0.
5. Under **Settings**, click **IP configurations**.
6. Click **Add**.
7. Enter a name for the IP configuration, select **Dynamic**, and then click **OK**.
8. Click the name of the IP configuration that you just created, change the **Assignment** to **Static**, and click **Save**.

It's best to use a static IP address because a static IP ensures that the IP address won't change, which can help to prevent unnecessary outages to your application.

If you want to create an SVM management LIF, repeat these steps to create an additional IP address.

### After you finish

Copy the private IP addresses that you just created. You'll need to specify those IP addresses when you create LIFs for the new storage VM.

### HA pair

How you allocate IP addresses for an HA pair depends on the storage protocol that you're using.

## iSCSI

iSCSI IP addresses must be assigned to nic0 in Azure before you create a storage VM and allocate LIFs. IPs for iSCSI are assigned to nic0 and not the load balancer because iSCSI uses ALUA for failover.

You'll need to create the following IP addresses:

- One IP address for iSCSI data LIF access from node 1
- One IP address for iSCSI data LIF access from node 2
- An optional IP address for a storage VM (SVM) management LIF

This management LIF provides a connection to management tools like SnapCenter.

### Steps

1. Log in to the Azure portal and open the **Virtual machine** service.
2. Click the name of the Cloud Volumes ONTAP VM for node 1.
3. Click **Networking**.
4. Click the name of the network interface for nic0.
5. Under **Settings**, click **IP configurations**.
6. Click **Add**.
7. Enter a name for the IP configuration, select **Dynamic**, and then click **OK**.
8. Click the name of the IP configuration that you just created, change the **Assignment** to **Static**, and click **Save**.

It's best to use a static IP address because a static IP ensures that the IP address won't change, which can help to prevent unnecessary outages to your application.

9. Repeat these steps on node 2.
10. If you want to create an SVM management LIF, repeat these steps on node 1.

## NFS

IP addresses that you use for NFS are allocated in the load balancer so that the IP addresses can migrate to the other node in case failover events occur.

You'll need to create the following IP addresses:

- One IP address for NAS data LIF access from node 1
- One IP address for NAS data LIF access from node 2
- An optional IP address for a storage VM (SVM) management LIF

This management LIF provides a connection to management tools like SnapCenter.

### Steps

1. In the Azure portal, open the **Load balancers** service.
2. Click the name of the load balancer for the HA pair.
3. Create one frontend IP configuration for data LIF access from node 1, another for data LIF access from node 2, and another optional frontend IP for a storage VM (SVM) management LIF.

- a. Under **Settings**, click **Frontend IP configuration**.
- b. Click **Add**.
- c. Enter a name for the frontend IP, select the subnet for the Cloud Volumes ONTAP HA pair, leave **Dynamic** selected, and in regions with Availability Zones, leave **Zone-redundant** selected to ensure that the IP address remains available if a zone fails.



The screenshot shows the Microsoft Azure portal interface. At the top, there's a navigation bar with the Microsoft Azure logo and a search bar. Below the navigation bar, the breadcrumb trail reads: Home > Load balancing > azureha1011s3-rg-lb >. The main heading is 'Add frontend IP configuration' with a three-dot menu icon to its right. Below the heading, the resource name 'azureha1011s3-rg-lb' is displayed. The form contains the following fields:

- Name \***: A text input field containing 'ip-for-svm2' with a checkmark icon on the right.
- Virtual network**: A text input field containing 'Default-Networking-vnet'.
- Subnet \***: A dropdown menu showing 'default (172.19.2.0/24)' with a downward arrow.
- Assignment**: Two radio buttons, 'Dynamic' (which is selected) and 'Static'.
- Availability zone \***: A dropdown menu showing 'Zone-redundant' with a downward arrow.

- d. Click the name of the frontend IP configuration that you just created, change the **Assignment** to **Static**, and click **Save**.

It's best to use a static IP address because a static IP ensures that the IP address won't change, which can help to prevent unnecessary outages to your application.

4. Add a health probe for each frontend IP that you just created.

- a. Under the load balancer's **Settings**, click **Health probes**.
- b. Click **Add**.
- c. Enter a name for the health probe and enter a port number that's between 63005 and 65000. Keep the default values for the other fields.

It's important that the port number is between 63005 and 65000. For example, if you are creating three health probes, you could enter probes that use the port numbers 63005, 63006, and 63007.



Microsoft Azure

Search resources, services, and

[Home](#) > [Load balancers](#) > [azureha1011s3-rg-lb](#) >

## Add health probe

azureha1011s3-rg-lb

Name *	svm2-health-probe1	✓
Protocol *	TCP	▼
Port * ⓘ	63005	✓
Interval * ⓘ	5	seconds
Unhealthy threshold * ⓘ	2	consecutive failures
Used by ⓘ	Not used	

5. Create new load balancing rules for each frontend IP.
  - a. Under the load balancer's **Settings**, click **Load balancing rules**.
  - b. Click **Add** and enter the required information:
    - **Name**: Enter a name for the rule.
    - **IP Version**: Select **IPv4**.
    - **Frontend IP address**: Select one of the frontend IP addresses that you just created.
    - **HA Ports**: Enable this option.
    - **Backend pool**: Keep the default Backend pool that was already selected.
    - **Health probe**: Select the health probe that you created for the selected frontend IP.
    - **Session persistence**: Select **None**.
    - **Floating IP**: Select **Enabled**.

## Add load balancing rule

chandanaTcpRst3-rg-lb

**i** A load balancing rule distributes incoming traffic that is sent to a selected IP address and port combination across a group of backend pool instances. Only backend instances that the health probe considers healthy receive new traffic.

Name \*

jimmy\_new\_rule ✓

IP Version \*

☒ IPv4 ☐ IPv6

Frontend IP address \* ⓘ

10.1.0.156 (dataAFIP) ▼

☒ HA Ports ⓘ

Backend pool ⓘ

backendPool (2 virtual machines) ▼

Health probe ⓘ

dataProbe (TCP:63002) ▼

Session persistence ⓘ

None ▼

Floating IP ⓘ

☐ Disabled ☒ Enabled

6. Ensure that the network security group rules for Cloud Volumes ONTAP allows the load balancer to send TCP probes for the health probes that were created in step 4 above. Note that this is allowed by default.

### SMB

IP addresses that you use for SMB data are allocated in the load balancer so that the IP addresses can migrate to the other node in case failover events occur.

You'll need to create the following IP addresses:

- One IP address for NAS data LIF access from node 1
- One IP address for NAS data LIF access from node 2
- One IP address for an iSCSI LIF on node 1
- One IP address for an iSCSI LIF on node 2

The iSCSI LIFs are required for DNS and SMB communication. An iSCSI LIF is used for this purpose because it doesn't migrate on failover.

- An optional IP address for a storage VM (SVM) management LIF

This management LIF provides a connection to management tools like SnapCenter.

## Steps

1. In the Azure portal, open the **Load balancers** service.
2. Click the name of the load balancer for the HA pair.
3. Create the required number of frontend IP configurations:
  - a. Under **Settings**, click **Frontend IP configuration**.
  - b. Click **Add**.
  - c. Enter a name for the frontend IP, select the subnet for the Cloud Volumes ONTAP HA pair, leave **Dynamic** selected, and in regions with Availability Zones, leave **Zone-redundant** selected to ensure that the IP address remains available if a zone fails.

The screenshot shows the 'Add frontend IP configuration' page in the Microsoft Azure portal. The breadcrumb navigation is 'Home > Load balancing > azureha1011s3-rg-lb >'. The title is 'Add frontend IP configuration' with a three-dot menu icon. Below the title is the load balancer name 'azureha1011s3-rg-lb'. The form contains the following fields:

- Name \***: A text input field containing 'ip-for-svm2' with a checkmark icon on the right.
- Virtual network**: A text input field containing 'Default-Networking-vnet'.
- Subnet \***: A dropdown menu showing 'default (172.19.2.0/24)' with a downward arrow.
- Assignment**: Two radio buttons, 'Dynamic' (which is selected) and 'Static'.
- Availability zone \***: A dropdown menu showing 'Zone-redundant' with a downward arrow and an information icon.

- d. Click the name of the frontend IP configuration that you just created, change the **Assignment** to **Static**, and click **Save**.

It's best to use a static IP address because a static IP ensures that the IP address won't change, which can help to prevent unnecessary outages to your application.

4. Add a health probe for each frontend IP that you just created.
  - a. Under the load balancer's **Settings**, click **Health probes**.
  - b. Click **Add**.
  - c. Enter a name for the health probe and enter a port number that's between 63005 and 65000. Keep the default values for the other fields.

It's important that the port number is between 63005 and 65000. For example, if you are creating three health probes, you could enter probes that use the port numbers 63005, 63006, and 63007.

Microsoft Azure

Search resources, services, and

[Home](#) > [Load balancers](#) > [azureha1011s3-rg-lb](#) >

## Add health probe ...

azureha1011s3-rg-lb

Name *	svm2-health-probe1 ✓
Protocol *	TCP ▾
Port * ⓘ	63005 ✓
Interval * ⓘ	5 seconds
Unhealthy threshold * ⓘ	2 consecutive failures
Used by ⓘ	Not used

5. Create new load balancing rules for each frontend IP.
  - a. Under the load balancer's **Settings**, click **Load balancing rules**.
  - b. Click **Add** and enter the required information:
    - **Name**: Enter a name for the rule.
    - **IP Version**: Select **IPv4**.
    - **Frontend IP address**: Select one of the frontend IP addresses that you just created.
    - **HA Ports**: Enable this option.
    - **Backend pool**: Keep the default Backend pool that was already selected.
    - **Health probe**: Select the health probe that you created for the selected frontend IP.
    - **Session persistence**: Select **None**.
    - **Floating IP**: Select **Enabled**.

## Add load balancing rule

chandanaTcpRst3-rg-lb

**i** A load balancing rule distributes incoming traffic that is sent to a selected IP address and port combination across a group of backend pool instances. Only backend instances that the health probe considers healthy receive new traffic.

Name \*

jimmy\_new\_rule

IP Version \*



IPv4



IPv6

Frontend IP address \* ⓘ

10.1.0.156 (dataAFIP)



HA Ports ⓘ

Backend pool ⓘ

backendPool (2 virtual machines)

Health probe ⓘ

dataAProbe (TCP:63002)

Session persistence ⓘ

None

Floating IP ⓘ

Disabled

Enabled

6. Ensure that the network security group rules for Cloud Volumes ONTAP allows the load balancer to send TCP probes for the health probes that were created in step 4 above. Note that this is allowed by default.

### After you finish

Copy the private IP addresses that you just created. You'll need to specify those IP addresses when you create LIFs for the new storage VM.

### Create a storage VM and LIFs

After you allocate IP addresses in Azure, you can create a new storage VM on a single node system or on an HA pair.

#### Single node system

How you create a storage VM and LIFs on a single node system depends on the storage protocol that you're using.

## iSCSI

Follow these steps to create a new storage VM, along with the required LIFs.

### Steps

1. Create the storage VM and a route to the storage VM.

```
vserver create -vserver <svm-name> -subtype default -rootvolume  
<root-volume-name> -rootvolume-security-style unix
```

```
network route create -destination 0.0.0.0/0 -vserver <svm-name>  
-gateway <ip-of-gateway-server>
```

2. Create a data LIF:

```
network interface create -vserver <svm-name> -home-port e0a -address  
<iscsi-ip-address> -lif <lif-name> -home-node <name-of-node1> -data  
-protocol iscsi
```

3. Optional: Create a storage VM management LIF.

```
network interface create -vserver <svm-name> -lif <lif-name> -role  
data -data-protocol none -address <svm-mgmt-ip-address> -netmask  
-length <length> -home-node <name-of-node1> -status-admin up  
-failover-policy system-defined -firewall-policy mgmt -home-port e0a  
-auto-revert false -failover-group Default
```

4. Assign one or more aggregates to the storage VM.

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

This step is required because the new storage VM needs access to at least one aggregate before you can create volumes on the storage VM.

## NFS

Follow these steps to create a new storage VM, along with the required LIFs.

### Steps

1. Create the storage VM and a route to the storage VM.

```
vserver create -vserver <svm-name> -subtype default -rootvolume  
<root-volume-name> -rootvolume-security-style unix
```

```
network route create -destination 0.0.0.0/0 -vserver <svm-name>  
-gateway <ip-of-gateway-server>
```

## 2. Create a data LIF:

```
network interface create -vserver <svm-name> -lif <lif-name> -role  
data -data-protocol cifs,nfs -address <nfs-ip-address> -netmask  
-length <length> -home-node <name-of-node1> -status-admin up  
-failover-policy disabled -firewall-policy data -home-port e0a -auto  
-revert true -failover-group Default
```

## 3. Optional: Create a storage VM management LIF.

```
network interface create -vserver <svm-name> -lif <lif-name> -role  
data -data-protocol none -address <svm-mgmt-ip-address> -netmask  
-length <length> -home-node <name-of-node1> -status-admin up  
-failover-policy system-defined -firewall-policy mgmt -home-port e0a  
-auto-revert false -failover-group Default
```

## 4. Assign one or more aggregates to the storage VM.

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

This step is required because the new storage VM needs access to at least one aggregate before you can create volumes on the storage VM.

## SMB

Follow these steps to create a new storage VM, along with the required LIFs.

### Steps

#### 1. Create the storage VM and a route to the storage VM.

```
vserver create -vserver <svm-name> -subtype default -rootvolume  
<root-volume-name> -rootvolume-security-style unix
```

```
network route create -destination 0.0.0.0/0 -vserver <svm-name>
-gateway <ip-of-gateway-server>
```

## 2. Create a data LIF:

```
network interface create -vserver <svm-name> -lif <lif-name> -role
data -data-protocol cifs,nfs -address <nfs-ip-address> -netmask
-length <length> -home-node <name-of-node1> -status-admin up
-failover-policy disabled -firewall-policy data -home-port e0a -auto
-revert true -failover-group Default
```

## 3. Optional: Create a storage VM management LIF.

```
network interface create -vserver <svm-name> -lif <lif-name> -role
data -data-protocol none -address <svm-mgmt-ip-address> -netmask
-length <length> -home-node <name-of-node1> -status-admin up
-failover-policy system-defined -firewall-policy mgmt -home-port e0a
-auto-revert false -failover-group Default
```

## 4. Assign one or more aggregates to the storage VM.

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

This step is required because the new storage VM needs access to at least one aggregate before you can create volumes on the storage VM.

### HA pair

How you create a storage VM and LIFs on an HA pair depends on the storage protocol that you're using.



## iSCSI

Follow these steps to create a new storage VM, along with the required LIFs.

### Steps

1. Create the storage VM and a route to the storage VM.

```
vserver create -vserver <svm-name> -subtype default -rootvolume  
<root-volume-name> -rootvolume-security-style unix
```

```
network route create -destination 0.0.0.0/0 -vserver <svm-name>  
-gateway <ip-of-gateway-server>
```

2. Create data LIFs:

- a. Use the following command to create an iSCSI LIF on node 1.

```
network interface create -vserver <svm-name> -home-port e0a  
-address <iscsi-ip-address> -lif <lif-name> -home-node <name-of-  
node1> -data-protocol iscsi
```

- b. Use the following command to create an iSCSI LIF on node 2.

```
network interface create -vserver <svm-name> -home-port e0a  
-address <iscsi-ip-address> -lif <lif-name> -home-node <name-of-  
node2> -data-protocol iscsi
```

3. Optional: Create a storage VM management LIF on node 1.

```
network interface create -vserver <svm-name> -lif <lif-name> -role  
data -data-protocol none -address <svm-mgmt-ip-address> -netmask  
-length <length> -home-node <name-of-node1> -status-admin up  
-failover-policy system-defined -firewall-policy mgmt -home-port e0a  
-auto-revert false -failover-group Default
```

This management LIF provides a connection to management tools like SnapCenter.

4. Assign one or more aggregates to the storage VM.

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

This step is required because the new storage VM needs access to at least one aggregate before you

can create volumes on the storage VM.

5. If you're running Cloud Volumes ONTAP 9.11.1 or later, modify the network service policies for the storage VM.

Modifying the services is required because it ensures that Cloud Volumes ONTAP can use the iSCSI LIF for outbound management connections.

```
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service data-fpolicy-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ad-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-dns-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ldap-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-nis-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-ad-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-dns-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-ldap-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-nis-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-ad-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-dns-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-ldap-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-nis-client
```

## NFS

Follow these steps to create a new storage VM, along with the required LIFs.

### Steps

1. Create the storage VM and a route to the storage VM.

```
vserver create -vserver <svm-name> -subtype default -rootvolume  
<root-volume-name> -rootvolume-security-style unix
```

```
network route create -destination 0.0.0.0/0 -vserver <svm-name>  
-gateway <ip-of-gateway-server>
```

## 2. Create data LIFs:

- a. Use the following command to create a NAS LIF on node 1.

```
network interface create -vserver <svm-name> -lif <lif-name>  
-role data -data-protocol cifs,nfs -address <nfs-ip-address>  
-netmask-length <length> -home-node <name-of-node1> -status-admin  
up -failover-policy system-defined -firewall-policy data -home  
-port e0a -auto-revert true -failover-group Default -probe-port  
<port-number-for-azure-health-probe1>
```

- b. Use the following command to create a NAS LIF on node 2.

```
network interface create -vserver <svm-name> -lif <lif-name>  
-role data -data-protocol cifs,nfs -address <nfs-cifs-ip-address>  
-netmask-length <length> -home-node <name-of-node2> -status-admin  
up -failover-policy system-defined -firewall-policy data -home  
-port e0a -auto-revert true -failover-group Default -probe-port  
<port-number-for-azure-health-probe2>
```

## 3. Optional: Create a storage VM management LIF on node 1.

```
network interface create -vserver <svm-name> -lif <lif-name> -role  
data -data-protocol none -address <svm-mgmt-ip-address> -netmask  
-length <length> -home-node <name-of-node1> -status-admin up  
-failover-policy system-defined -firewall-policy mgmt -home-port e0a  
-auto-revert false -failover-group Default -probe-port <port-number-  
for-azure-health-probe3>
```

This management LIF provides a connection to management tools like SnapCenter.

## 4. Assign one or more aggregates to the storage VM.

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

This step is required because the new storage VM needs access to at least one aggregate before you can create volumes on the storage VM.

5. If you're running Cloud Volumes ONTAP 9.11.1 or later, modify the network service policies for the storage VM.

Modifying the services is required because it ensures that Cloud Volumes ONTAP can use the iSCSI LIF for outbound management connections.

```
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service data-fpolicy-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ad-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-dns-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ldap-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-nis-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-ad-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-dns-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-ldap-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-nis-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-ad-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-dns-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-ldap-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-nis-client
```

## SMB

Follow these steps to create a new storage VM, along with the required LIFs.

### Steps

1. Create the storage VM and a route to the storage VM.

```
vserver create -vserver <svm-name> -subtype default -rootvolume  
<root-volume-name> -rootvolume-security-style unix
```

```
network route create -destination 0.0.0.0/0 -vserver <svm-name>  
-gateway <ip-of-gateway-server>
```

## 2. Create NAS data LIFs:

- a. Use the following command to create a NAS LIF on node 1.

```
network interface create -vserver <svm-name> -lif <lif-name>  
-role data -data-protocol cifs,nfs -address <nfs-ip-address>  
-netmask-length <length> -home-node <name-of-node1> -status-admin  
up -failover-policy system-defined -firewall-policy data -home  
-port e0a -auto-revert true -failover-group Default -probe-port  
<port-number-for-azure-health-probe1>
```

- b. Use the following command to create a NAS LIF on node 2.

```
network interface create -vserver <svm-name> -lif <lif-name>  
-role data -data-protocol cifs,nfs -address <nfs-cifs-ip-address>  
-netmask-length <length> -home-node <name-of-node2> -status-admin  
up -failover-policy system-defined -firewall-policy data -home  
-port e0a -auto-revert true -failover-group Default -probe-port  
<port-number-for-azure-health-probe2>
```

## 3. Create iSCSI LIFs to provide DNS and SMB communication:

- a. Use the following command to create an iSCSI LIF on node 1.

```
network interface create -vserver <svm-name> -home-port e0a  
-address <iscsi-ip-address> -lif <lif-name> -home-node <name-of-  
node1> -data-protocol iscsi
```

- b. Use the following command to create an iSCSI LIF on node 2.

```
network interface create -vserver <svm-name> -home-port e0a  
-address <iscsi-ip-address> -lif <lif-name> -home-node <name-of-  
node2> -data-protocol iscsi
```

## 4. Optional: Create a storage VM management LIF on node 1.

```
network interface create -vserver <svm-name> -lif <lif-name> -role
data -data-protocol none -address <svm-mgmt-ip-address> -netmask
-length <length> -home-node <name-of-node1> -status-admin up
-failover-policy system-defined -firewall-policy mgmt -home-port e0a
-auto-revert false -failover-group Default -probe-port <port-number-
for-azure-health-probe3>
```

This management LIF provides a connection to management tools like SnapCenter.

5. Assign one or more aggregates to the storage VM.

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

This step is required because the new storage VM needs access to at least one aggregate before you can create volumes on the storage VM.

6. If you're running Cloud Volumes ONTAP 9.11.1 or later, modify the network service policies for the storage VM.

Modifying the services is required because it ensures that Cloud Volumes ONTAP can use the iSCSI LIF for outbound management connections.

```

network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service data-fpolicy-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ad-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-dns-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ldap-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-nis-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-ad-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-dns-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-ldap-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-nis-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-ad-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-dns-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-ldap-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-nis-client

```

### What's next?

After you create a storage VM on an HA pair, it's best to wait 12 hours before you provision storage on that SVM. Starting with the Cloud Volumes ONTAP 9.10.1 release, BlueXP scans the settings for an HA pair's load balancer at a 12-hour interval. If there are new SVMs, BlueXP will enable a setting that provides shorter unplanned failover.

## Create data-serving storage VMs for Cloud Volumes ONTAP in Google Cloud

A storage VM is a virtual machine running within ONTAP that provides storage and data services to your clients. You might know this as an *SVM* or a *vserver*. Cloud Volumes ONTAP is configured with one storage VM by default, but some configurations support additional storage VMs.

## Supported number of storage VMs

Multiple storage VMs are supported with specific Cloud Volumes ONTAP configurations in Google Cloud starting with the 9.11.1 release. Go to the [Cloud Volumes ONTAP Release Notes](#) to verify the supported number of storage VMs for your version of Cloud Volumes ONTAP.

All other Cloud Volumes ONTAP configurations support one data-serving storage VM and one destination storage VM used for disaster recovery. You can activate the destination storage VM for data access if there's an outage on the source storage VM.

## Create a storage VM

If supported by your license, you can create multiple storage VMs on a single node system or on an HA pair. Note that you must use the BlueXP API to create a storage VM on an HA pair, while you can use the CLI or System Manager to create a storage VM on a single node system.

### Single node system

These steps create a new storage VM on a single node system using the CLI. One private IP address is required to create a data LIF and another optional private IP address is needed if you want to create a management LIF.

### Steps

1. In Google Cloud, go to the Cloud Volumes ONTAP instance and add an IP address to nic0 for each LIF.



### Edit network interface

Network \*  
default

Subnetwork \*  
default IPv4 (10.138.0.0/20)

*i* To use IPv6, you need an IPv6 subnet range. [LEARN MORE](#)

**IP stack type**  
☒ IPv4 (single-stack)  
☐ IPv4 and IPv6 (dual-stack)

Primary internal IP  
gcpcvo-vm-ip-nic0-nodemgmt (10.138.0.46)

**Alias IP ranges**

Subnet range 1 Primary (10.138.0.0/20)	Alias IP range 1 * 10.138.0.25/32
Subnet range 2 Primary (10.138.0.0/20)	Alias IP range 2 * 10.138.0.23/32
Subnet range 3 Primary (10.138.0.0/20)	Alias IP range 3 * 10.138.0.21/32
Subnet range 4 Primary (10.138.0.0/20)	Alias IP range 4 * 10.138.0.31/32

+ ADD IP RANGE

External IPv4 address  
None

You need one IP address for a data LIF and another optional IP address if you want to create a management LIF on the storage VM.

[Google Cloud documentation: Adding alias IP ranges to an existing instance](#)

2. Create the storage VM and a route to the storage VM.

```
vserver create -vserver <svm-name> -subtype default -rootvolume <root-volume-name> -rootvolume-security-style unix
```

```
network route create -destination 0.0.0.0/0 -vserver <svm-name> -gateway <ip-of-gateway-server>
```

3. Create a data LIF by specifying the IP address that you added in Google Cloud.

#### iSCSI

```
network interface create -vserver <svm-name> -home-port e0a -address  
<iscsi-ip-address> -lif <lif-name> -home-node <name-of-node1> -data  
-protocol iscsi
```

#### NFS or SMB

```
network interface create -vserver <svm-name> -lif <lif-name> -role  
data -data-protocol cifs,nfs -address <nfs-ip-address> -netmask  
-length <length> -home-node <name-of-node1> -status-admin up  
-failover-policy disabled -firewall-policy data -home-port e0a -auto  
-revert true -failover-group Default
```

4. Optional: Create a storage VM management LIF by specifying the IP address that you added in Google Cloud.

```
network interface create -vserver <svm-name> -lif <lif-name> -role data  
-data-protocol none -address <svm-mgmt-ip-address> -netmask-length  
<length> -home-node <name-of-node1> -status-admin up -failover-policy  
system-defined -firewall-policy mgmt -home-port e0a -auto-revert false  
-failover-group Default
```

5. Assign one or more aggregates to the storage VM.

```
vserver add-aggregates -vserver <svm-name> -aggregates <aggr1,aggr2>
```

This step is required because the new storage VM needs access to at least one aggregate before you can create volumes on the storage VM.

#### HA pair

You must use the BlueXP API to create a storage VM on a Cloud Volumes ONTAP system in Google Cloud. Using the API (and not System Manager or the CLI) is required because BlueXP configures the storage VM with the required LIF services, as well as an iSCSI LIF that's required for outbound SMB/CIFS communication.

Note that BlueXP allocates the required IP addresses in Google Cloud and creates the storage VM with a data LIF for SMB/NFS access and an iSCSI LIF for outbound SMB communication.

#### Required Google Cloud permissions

The Connector requires specific permissions to create and manage storage VMs for Cloud Volumes ONTAP HA pairs. The required permissions are included in [the policies provided by NetApp](#).

## Steps

1. Use the following API call to create a storage VM:

```
POST /occm/api/gcp/ha/working-environments/{WE_ID}/svm/
```

The request body should include the following:

```
{ "svmName": "myNewSvm1" }
```

## Manage storage VMs on HA pairs

The BlueXP API also supports renaming and deleting storage VMs on HA pairs.

### Rename a storage VM

If needed, you can change the name of a storage VM at any time.

## Steps

1. Use the following API call to rename a storage VM:

```
PUT /occm/api/gcp/ha/working-environments/{WE_ID}/svm
```

The request body should include the following:

```
{
  "svmNewName": "newSvmName",
  "svmName": "oldSvmName"
}
```

### Delete a storage VM

If you no longer need a storage VM, you can delete it from Cloud Volumes ONTAP.

## Steps

1. Use the following API call to delete a storage VM:

```
DELETE /occm/api/gcp/ha/working-environments/{WE_ID}/svm/{SVM_NAME}
```

# Security and data encryption

## Encrypting volumes with NetApp encryption solutions

Cloud Volumes ONTAP supports NetApp Volume Encryption (NVE) and NetApp Aggregate Encryption (NAE). NVE and NAE are software-based solutions that enable FIPS 140-2–compliant data-at-rest encryption of volumes. [Learn more about these encryption solutions.](#)

Both NVE and NAE are supported with an external key manager.

If you use NVE, you have the option to use your cloud provider's key vault to protect ONTAP encryption keys:

- Azure Key Vault (AKV)
- Google Cloud Key Management Service

New aggregates will have NAE enabled by default after you set up an external key manager. New volumes that aren't part of an NAE aggregate will have NVE enabled by default (for example, if you have existing aggregates that were created before setting up an external key manager).

Cloud Volumes ONTAP doesn't support onboard key management.

### What you'll need

Your Cloud Volumes ONTAP system should be registered with NetApp support. A NetApp Volume Encryption license is automatically installed on each Cloud Volumes ONTAP system that is registered with NetApp Support.

- [Adding NetApp Support Site accounts to BlueXP](#)
- [Registering pay-as-you-go systems](#)



BlueXP doesn't install the NVE license on systems that reside in the China region.

### Steps

1. Review the list of supported key managers in the [NetApp Interoperability Matrix Tool](#).



Search for the **Key Managers** solution.

2. [Connect to the Cloud Volumes ONTAP CLI](#).
3. Configure external key management.
  - AWS: [Go to the ONTAP documentation for instructions](#)
  - Azure: [Azure Key Vault \(AKV\)](#)
  - Google Cloud: [Google Cloud Key Management Service](#)

## Manage keys with Azure Key Vault

You can use [Azure Key Vault \(AKV\)](#) to protect your ONTAP encryption keys in an Azure-deployed application.

AKV can be used to protect [NetApp Volume Encryption \(NVE\) keys](#) only for data SVMs.

Key management with AKV can be enabled with the CLI or the ONTAP REST API.

When using AKV, be aware that by default a data SVM LIF is used to communicate with the cloud key management endpoint. A node management network is used to communicate with the cloud provider's authentication services (login.microsoftonline.com). If the cluster network is not configured correctly, the cluster will not properly utilize the key management service.

### Prerequisites

- Cloud Volumes ONTAP must be running version 9.10.1 or later
- Volume Encryption (VE) license installed (NetApp Volume Encryption license is automatically installed on

each Cloud Volumes ONTAP system that is registered with NetApp Support)

- You must have a Multi-tenant Encryption Key Management (MT\_EK\_MGMT) license
- You must be a cluster or SVM administrator
- An Active Azure subscription

## Limitations

- AKV can only be configured on a data SVM

## Configuration process

The outlined steps capture how to register your Cloud Volumes ONTAP configuration with Azure and how to create an Azure Key Vault and keys. If you have already completed these steps, ensure you have the correct configuration settings, particularly in [Create an Azure Key Vault](#), and then proceed to [Cloud Volumes ONTAP configuration](#).

- [Azure Application Registration](#)
- [Create Azure client secret](#)
- [Create an Azure Key Vault](#)
- [Create encryption key](#)
- [Create an Azure Active Directory Endpoint \(HA only\)](#)
- [Cloud Volumes ONTAP configuration](#)

## Azure Application Registration

1. You must first register your application in the Azure subscription that you want the Cloud Volumes ONTAP to use for access the Azure Key Vault. Within the Azure portal, select **App registrations**.
2. Select **New registration**.
3. Provide a name for your application and select a supported application type. The default single tenant suffices for Azure Key Vault usage. Select **Register**.
4. In the Azure Overview window, select the application you have registered. Copy the **application (client) ID** and the **directory (tenant) ID** to a secure location. They will be required later in the registration process.

## Create Azure client secret

1. In the Azure portal for your Azure Key Vault app registration, select the **Certificates & secrets** pane.
2. Select **New client secret**. Enter a meaningful name for your client secret. NetApp recommends a 24-month expiration period; however, your specific cloud governance policies may require a different setting.
3. Click **Add** to create the client secret. Copy the secret string listed in the **Value** column and store it in a secure location for use later in [Cloud Volumes ONTAP configuration](#). The secret value will not be displayed again after you navigate away from the page.

## Create an Azure Key Vault

1. If you have an existing Azure Key Vault, you can connect it to your Cloud Volumes ONTAP configuration; however, you must adapt the access policies to the settings in this process.
2. In the Azure portal, navigate to the **Key Vaults** section.
3. Click **+Create** and enter the required information including resource group, region, and pricing tier. In addition, enter the number of days to retain deleted vaults and select **Enable purge protection** on the key vault.

4. Select **Next** to choose an access policy.
5. Select the following options:
  - a. Under **Access configuration**, select the **Vault access policy**.
  - b. Under **Resource access**, select **Azure Disk Encryption for volume encryption**.
6. Select **+Create** to add an access policy.
7. Under **Configure from a template**, click the drop-down menu and then select the **Key, Secret, and Certificate Management** template.
8. Choose each of the drop-down permissions menus (key, secret, certificate) and then **Select all** at the top of the menu list to select all the permissions available. You should have:
  - **Key permissions**: 20 selected
  - **Secret permissions**: 8 selected
  - **Certificate permissions**: 16 selected

# Create an access policy



- 1 Permissions 2 Principal 3 Application (optional) 4 Review + create

Configure from a template

Key, Secret, & Certificate Management

## Key permissions

### Key Management Operations

- ☒ Select all
- ☒ Get
- ☒ List
- ☒ Update
- ☒ Create
- ☒ Import
- ☒ Delete
- ☒ Recover
- ☒ Backup
- ☒ Restore

### Cryptographic Operations

- ☒ Select all
- ☒ Decrypt
- ☒ Encrypt
- ☒ Unwrap Key
- ☒ Wrap Key
- ☒ Verify
- ☒ Sign

### Privileged Key Operations

- ☒ Select all
- ☒ Purge
- ☒ Release

### Rotation Policy Operations

- ☒ Select all
- ☒ Rotate
- ☒ Get Rotation Policy
- ☒ Set Rotation Policy

## Secret permissions

### Secret Management Operations

- ☒ Select all
- ☒ Get
- ☒ List
- ☒ Set
- ☒ Delete
- ☒ Recover
- ☒ Backup
- ☒ Restore

### Privileged Secret Operations

- ☒ Select all
- ☒ Purge

## Certificate permissions

### Certificate Management Operations

- ☒ Select all
- ☒ Get
- ☒ List
- ☒ Update
- ☒ Create
- ☒ Import
- ☒ Delete
- ☒ Recover
- ☒ Backup
- ☒ Restore
- ☒ Manage Contacts
- ☒ Manage Certificate Authorities
- ☒ Get Certificate Authorities
- ☒ List Certificate Authorities
- ☒ Set Certificate Authorities
- ☒ Delete Certificate Authorities

### Privileged Certificate Operations

- ☒ Select all
- ☒ Purge

Previous

Next

9. Click **Next** to select the **Principal** Azure registered application you created in [Azure Application Registration](#). Select **Next**.



Only one principal can be assigned per policy.

### Create an access policy

Permissions **Principal** Application (optional) Review + create

Only 1 principal can be assigned per access policy.  
Use the new embedded experience to select a principal. The previous popup experience can be accessed here. [Select a principal](#)

**Selected item**  
No item selected

Previous **Next**

10. Click **Next** two times until you arrive at **Review and create**. Then, click **Create**.
11. Select **Next** to advance to **Networking** options.
12. Choose the appropriate network access method or select **All networks** and **Review + Create** to create the key vault. (Network access method may be prescribed by a governance policy or your corporate cloud security team.)
13. Record the Key Vault URI: In the key vault you created, navigate to the Overview menu and copy the **Vault URI** from the right-hand column. You need this for a later step.

#### Create encryption key

1. In the menu for the Key Vault you have created for Cloud Volumes ONTAP, navigate to the **Keys** option.
2. Select **Generate/import** to create a new key.
3. Leave the default option set to **Generate**.
4. Provide the following information:
  - Encryption key name



- Key type: RSA
- RSA key size: 2048
- Enabled: Yes

5. Select **Create** to create the encryption key.
6. Return to the **Keys** menu and select the key you just created.
7. Select the key ID under **Current version** to view the key properties.
8. Locate the **Key Identifier** field. Copy the URI up to but not including the hexadecimal string.

#### **Create an Azure Active Directory Endpoint (HA only)**

1. This process is only required if you are configuring Azure Key Vault for an HA Cloud Volumes ONTAP Working Environment.
2. In the Azure portal navigate to **Virtual Networks**.
3. Select the Virtual Network where you deployed the Cloud Volumes ONTAP working environment and select the **Subnets** menu on the left side of the page.
4. Select the subnet name for your Cloud Volumes ONTAP deployment from the list.
5. Navigate to the **Service Endpoints** heading. In the drop-down menu, select the following:
  - **Microsoft.AzureActiveDirectory**
  - **Microsoft.KeyVault**
  - **Microsoft.Storage** (optional)

### SERVICE ENDPOINTS

Create service endpoint policies to allow traffic to specific azure resources from your virtual network over service endpoints. [Learn more](#)

Services ⓘ

3 selected

Service	Status	
Microsoft.Storage	Succeeded	
Microsoft.AzureActiveDirectory	Succeeded	
Microsoft.KeyVault	Succeeded	

Service endpoint policies

0 selected

### SUBNET DELEGATION

Delegate subnet to a service ⓘ

None

### NETWORK POLICY FOR PRIVATE ENDPOINTS

The network policy affects all private endpoints in this subnet. To use network security groups, application security groups, or user defined routes to control traffic going to a private endpoint, set the private endpoint network policy to enabled. [Learn more](#)

Private endpoint network policy

Disabled

Save

Cancel

6. Select **Save** to capture your settings.

#### Cloud Volumes ONTAP configuration

1. Connect to the cluster management LIF with your preferred SSH client.
2. Enter the advanced privilege mode in ONTAP:

```
set advanced -con off
```

3. Identify the desired data SVM and verify its DNS configuration:

```
vserver services name-service dns show
```

- a. If a DNS entry for the desired data SVM exists and it contains an entry for the Azure DNS, then no action is required. If it does not, add a DNS server entry for the data SVM that points to the Azure DNS, private DNS, or on-premise server. This should match the entry for the cluster admin SVM:

```
vserver services name-service dns create -vserver SVM_name -domains domain  
-name-servers IP_address
```

- b. Verify the DNS service has been created for the data SVM:

```
vserver services name-service dns show
```

4. Enable Azure Key Vault using the client ID and tenant ID saved after the application registration:

```
security key-manager external azure enable -vserver SVM_name -client-id  
Azure_client_ID -tenant-id Azure_tenant_ID -name Azure_key_vault_name -key-id  
Azure_key_ID
```

5. Check the status of the key manager:

```
security key-manager external azure check
```

The output will look like:

```
::*> security key-manager external azure check
```

```
Vserver: data_svm_name
```

```
Node: akvlab01-01
```

```
Category: service_reachability
```

```
Status: OK
```

```
Category: ekvip_server
```

```
Status: OK
```

```
Category: kms_wrapped_key_status
```

```
Status: UNKNOWN
```

```
Details: No volumes created yet for the vserver. Wrapped KEK status  
will be available after creating encrypted volumes.
```

```
3 entries were displayed.
```

If the `service_reachability` status is not OK, the SVM cannot reach the Azure Key Vault service with all the required connectivity and permissions. Ensure that your Azure network policies and routing don't block your private vNet from reaching the Azure KeyVault Public endpoint. If they do, consider using an Azure Private endpoint to access the Key vault from within the vNet. You may also need to add a static hosts entry on your SVM to resolve the private IP address for your endpoint.

The `kms_wrapped_key_status` will report UNKNOWN at initial configuration. Its status will change to OK after the first volume is encrypted.

6. OPTIONAL: Create a test volume to verify the functionality of NVE.

```
vol create -vserver SVM_name -volume volume_name -aggregate aggr -size size
-state online -policy default
```

If configured correctly, Cloud Volumes ONTAP will automatically create the volume and enable volume encryption.

7. Confirm the volume was created and encrypted correctly. If it is, the `-is-encrypted` parameter will display as `true`.

```
vol show -vserver SVM_name -fields is-encrypted
```

## Manage keys with Google's Cloud Key Management Service

You can use [Google Cloud Platform's Key Management Service \(Cloud KMS\)](#) to protect your ONTAP encryption keys in a Google Cloud Platform-deployed application.

Key management with Cloud KMS can be enabled with the CLI or the ONTAP REST API.

When using Cloud KMS, be aware that by default a data SVMs LIF is used to communicate with the cloud key management endpoint. A node management network is used to communicate with the cloud provider's authentication services (oauth2.googleapis.com). If the cluster network is not configured correctly, the cluster will not properly utilize the key management service.

### Prerequisites

- Cloud Volumes ONTAP must be running version 9.10.1 or later
- Volume Encryption (VE) license installed
- Multi-tenant Encryption Key Management (MTEKM) license installed, starting with Cloud Volumes ONTAP 9.12.1 GA.
- You must be a cluster or SVM administrator
- An active Google Cloud Platform subscription

### Limitations

- Cloud KMS can only be configured on a data SVM

### Configuration

#### Google Cloud

1. In your Google Cloud environment, [create a symmetric GCP key ring and key](#).
2. Create a custom role for your Cloud Volumes ONTAP service account.

```

gcloud iam roles create kmsCustomRole
  --project=<project_id>
  --title=<kms_custom_role_name>
  --description=<custom_role_description>

  --permissions=cloudkms.cryptoKeyVersions.get,cloudkms.cryptoKeyVersions.
list,cloudkms.cryptoKeyVersions.useToDecrypt,cloudkms.cryptoKeyVersions.
useToEncrypt,cloudkms.cryptoKeys.get,cloudkms.keyRings.get,cloudkms.loca
tions.get,cloudkms.locations.list,resourceManager.projects.get
  --stage=GA

```

3. Assign the custom role to the Cloud KMS key and Cloud Volumes ONTAP service account:

```

gcloud kms keys add-iam-policy-binding key_name --keyring key_ring_name
--location key_location --member serviceAccount:_service_account_Name_ --role
projects/customer_project_id/roles/kmsCustomRole

```

4. Download service account JSON key:

```

gcloud iam service-accounts keys create key-file --iam-account=sa-name
@project-id.iam.gserviceaccount.com

```

## Cloud Volumes ONTAP

1. Connect to the cluster management LIF with your preferred SSH client.

2. Switch to the advanced privilege level:

```
set -privilege advanced
```

3. Create a DNS for the data SVM.

```
dns create -domains c.<project>.internal -name-servers server_address -vserver
SVM_name
```

4. Create CMEK entry:

```
security key-manager external gcp enable -vserver SVM_name -project-id project
-key-ring-name key_ring_name -key-ring-location key_ring_location -key-name
key_name
```

5. When prompted, enter the service account JSON key from your GCP account.

6. Confirm the enabled process succeeded:

```
security key-manager external gcp check -vserver svm_name
```

7. OPTIONAL: Create a volume to test encryption `vol create volume_name -aggregate aggregate -vserver vserver_name -size 10G`

## Troubleshoot

If you need to troubleshoot, you can tail the raw REST API logs in the final two steps above:

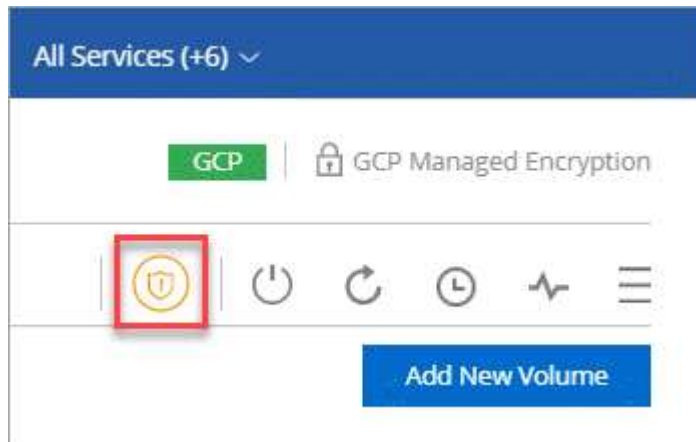
1. `set d`
2. `systemshell -node node -command tail -f /mroot/etc/log/mlog/kmip2_client.log`

## Improving protection against ransomware

Ransomware attacks can cost a business time, resources, and reputation. BlueXP enables you to implement the NetApp solution for ransomware, which provides effective tools for visibility, detection, and remediation.

### Steps

1. From the working environment, click the **Ransomware** icon.



2. Implement the NetApp solution for ransomware:

- a. Click **Activate Snapshot Policy**, if you have volumes that do not have a Snapshot policy enabled.

NetApp Snapshot technology provides the industry's best solution for ransomware remediation. The key to a successful recovery is restoring from uninfected backups. Snapshot copies are read-only, which prevents ransomware corruption. They can also provide the granularity to create images of a single file copy or a complete disaster recovery solution.

- b. Click **Activate FPolicy** to enable ONTAP's FPolicy solution, which can block file operations based on a file's extension.

This preventative solution improves protection from ransomware attacks by blocking common ransomware file types.

The default FPolicy scope blocks files that have the following extensions:

micro, encrypted, locked, crypto, crypt, crinf, r5a, XRNT, XTBL, R16M01D05, pzdc, good, LOL!, OMG!, RDM, RRK, encryptedRS, crjoker, EnCiPhErEd, LeChiffre



BlueXP creates this scope when you activate FPolicy on Cloud Volumes ONTAP. The list is based on common ransomware file types. You can customize the blocked file extensions by using the `vserver fpolicy policy scope` commands from the Cloud Volumes ONTAP CLI.

### Ransomware Protection

Ransomware attacks can cost a business time, resources, and reputation. The NetApp solution for ransomware provides effective tools for visibility, detection, and remediation. [Learn More](#)

#### 1 Enable Snapshot Copy Protection

50 % Protection

1 Volumes without a Snapshot Policy

To protect your data, activate the default Snapshot policy for these volumes

Activate Snapshot Policy

#### 2 Block Ransomware File Extensions



ONTAP's native FPolicy configuration monitors and blocks file operations based on a file's extension.

[View Denied File Names](#)

Activate FPolicy

## System administration

### Upgrade Cloud Volumes ONTAP software

Upgrade Cloud Volumes ONTAP from BlueXP to gain access to the latest new features and enhancements. You should prepare Cloud Volumes ONTAP systems before you upgrade the software.

#### Upgrade overview

You should be aware of the following before you start the Cloud Volumes ONTAP upgrade process.

#### Upgrade from BlueXP only

Upgrades of Cloud Volumes ONTAP must be completed from BlueXP. You should not upgrade Cloud Volumes ONTAP by using System Manager or the CLI. Doing so can impact system stability.

#### How to upgrade

BlueXP provides two ways to upgrade Cloud Volumes ONTAP:

- By following upgrade notifications that appear in the working environment
- By placing the upgrade image at an HTTPS location and then providing BlueXP with the URL

#### Supported upgrade paths

The version of Cloud Volumes ONTAP that you can upgrade to depends on the version of Cloud Volumes ONTAP that you're currently running.

Current version	Versions that you can directly upgrade to
9.12.1	9.13.0
9.12.0	9.12.1

Current version	Versions that you can directly upgrade to
9.11.1	9.12.1
	9.12.0
9.11.0	9.11.1
9.10.1	9.11.1
	9.11.0
9.10.0	9.10.1
9.9.1	9.10.1
	9.10.0
9.9.0	9.9.1
9.8	9.9.1
9.7	9.8
9.6	9.7
9.5	9.6
9.4	9.5
9.3	9.4
9.2	9.3
9.1	9.2
9.0	9.1
8.3	9.0

Note the following:

- The supported upgrade paths for Cloud Volumes ONTAP are different than they are for an on-premises ONTAP cluster.
- If you upgrade by following the upgrade notifications that appear in a working environment, BlueXP will prompt you to upgrade to a release that follows these supported upgrade paths.
- If you upgrade by placing an upgrade image at an HTTPS location, be sure to follow these supported upgrade paths.
- In some cases, you might need to upgrade a few times to reach your target release.

For example, if you're running version 9.8 and you want to upgrade to 9.10.1, you first need to upgrade to version 9.9.1 and then to 9.10.1.

### Reverting or downgrading

Reverting or downgrading Cloud Volumes ONTAP to a previous release is not supported.



## Support registration

Cloud Volumes ONTAP must be registered with NetApp support in order to upgrade the software using any of the methods described on this page. This applies to both PAYGO and BYOL. You'll need to [manually register PAYGO systems](#), while BYOL systems are registered by default.



A system that isn't registered for support will still receive the software update notifications that appear in BlueXP when a new version is available. But you will need to register the system before you can upgrade the software.

## Upgrades of the HA mediator

BlueXP also updates the mediator instance as needed during the Cloud Volumes ONTAP upgrade process.

## Prepare to upgrade

Before performing an upgrade, you must verify that your systems are ready and make any required configuration changes.

- [Plan for downtime](#)
- [Verify that automatic giveback is still enabled](#)
- [Suspend SnapMirror transfers](#)
- [Verify that aggregates are online](#)

### Plan for downtime

When you upgrade a single-node system, the upgrade process takes the system offline for up to 25 minutes, during which I/O is interrupted.

Upgrading an HA pair is nondisruptive and I/O is uninterrupted. During this nondisruptive upgrade process, each node is upgraded in tandem to continue serving I/O to clients.

### Verify that automatic giveback is still enabled

Automatic giveback must be enabled on a Cloud Volumes ONTAP HA pair (this is the default setting). If it isn't, then the operation will fail.

[ONTAP 9 Documentation: Commands for configuring automatic giveback](#)

### Suspend SnapMirror transfers

If a Cloud Volumes ONTAP system has active SnapMirror relationships, it is best to suspend transfers before you update the Cloud Volumes ONTAP software. Suspending the transfers prevents SnapMirror failures. You must suspend the transfers from the destination system.



Even though Cloud Backup uses an implementation of SnapMirror to create backup files (called SnapMirror Cloud), backups do not need to be suspended when a system is upgraded.

## About this task

These steps describe how to use System Manager for version 9.3 and later.

## Steps

1. Log in to System Manager from the destination system.

You can log in to System Manager by pointing your web browser to the IP address of the cluster management LIF. You can find the IP address in the Cloud Volumes ONTAP working environment.



The computer from which you are accessing BlueXP must have a network connection to Cloud Volumes ONTAP. For example, you might need to log in to BlueXP from a jump host that's in your cloud provider network.

2. Click **Protection > Relationships**.
3. Select the relationship and click **Operations > Quiesce**.

#### Verify that aggregates are online

Aggregates for Cloud Volumes ONTAP must be online before you update the software. Aggregates should be online in most configurations, but if they are not, then you should bring them online.

#### About this task

These steps describe how to use System Manager for version 9.3 and later.

#### Steps

1. In the working environment, click the menu icon, and then click **Advanced > Advanced allocation**.
2. Select an aggregate, click **Info**, and then verify that the state is online.

aggr1		
Aggregate Capacity:	88.57 GB	
-----		
Used Aggregate Capacity:	1.07 GB	
-----		
Volumes:	2	▼
-----		
AWS Disks:	1	▼
-----		
State:	online	
-----		

3. If the aggregate is offline, use System Manager to bring the aggregate online:
  - a. Click **Storage > Aggregates & Disks > Aggregates**.
  - b. Select the aggregate, and then click **More Actions > Status > Online**.

#### Upgrade Cloud Volumes ONTAP

BlueXP notifies you when a new version is available for upgrade. You can start the upgrade process from this

notification. For details, see [Upgrade from BlueXP notifications](#).

Another way to perform software upgrades by using an image on an external URL. This option is helpful if BlueXP can't access the S3 bucket to upgrade the software or if you were provided with a patch. For details, see [Upgrade from an image available at a URL](#).

### Upgrade from BlueXP notifications

BlueXP displays a notification in Cloud Volumes ONTAP working environments when a new version of Cloud Volumes ONTAP is available:



You can start the upgrade process from this notification, which automates the process by obtaining the software image from an S3 bucket, installing the image, and then restarting the system.

### Before you begin

BlueXP operations such as volume or aggregate creation must not be in progress on the Cloud Volumes ONTAP system.

### Steps

1. From the left navigation menu, select **Storage > Canvas**.
2. Select a working environment.

A notification appears in the right pane if a new version is available:



3. If a new version is available, click **Upgrade**.
4. In the Release Information page, click the link to read the Release Notes for the specified version, and then select the **I have read...** check box.
5. In the End User License Agreement (EULA) page, read the EULA, and then select **I read and approve the EULA**.
6. In the Review and Approve page, read the important notes, select **I understand...**, and then click **Go**.

### Result

BlueXP starts the software upgrade. You can perform actions on the working environment once the software update is complete.

### After you finish

If you suspended SnapMirror transfers, use System Manager to resume the transfers.

### Upgrade from an image available at a URL

You can place the Cloud Volumes ONTAP software image on the Connector or on an HTTP server and then initiate the software upgrade from BlueXP. You might use this option if BlueXP can't access the S3 bucket to upgrade the software.

### Before you begin

- BlueXP operations such as volume or aggregate creation must not be in progress on the Cloud Volumes ONTAP system.
- If you use HTTPS to host ONTAP images, the upgrade can fail due to SSL authentication issues, which are caused by missing certificates. The workaround is to generate and install a CA-signed certificate to be used for authentication between ONTAP and BlueXP.

Go to the NetApp Knowledge Base to view step-by-step instructions:

## Steps

1. Optional: Set up an HTTP server that can host the Cloud Volumes ONTAP software image.

If you have a VPN connection to the virtual network, you can place the Cloud Volumes ONTAP software image on an HTTP server in your own network. Otherwise, you must place the file on an HTTP server in the cloud.

2. If you use your own security group for Cloud Volumes ONTAP, ensure that the outbound rules allow HTTP connections so Cloud Volumes ONTAP can access the software image.



The predefined Cloud Volumes ONTAP security group allows outbound HTTP connections by default.

3. Obtain the software image from [the NetApp Support Site](#).
4. Copy the software image to a directory on the Connector or on an HTTP server from which the file will be served.

Two paths are available. The correct path depends on your Connector version.

- /opt/application/netapp/cloudmanager/docker\_occm/data/ontap/images/
- /opt/application/netapp/cloudmanager/ontap/images/

5. From the working environment in BlueXP, click the menu icon, and then click **Advanced > Update Cloud Volumes ONTAP**.
6. On the update software page, enter the URL, and then click **Change Image**.

If you copied the software image to the Connector in the path shown above, you would enter the following URL:

`http://<Connector-private-IP-address>/ontap/images/<image-file-name>`

7. Click **Proceed** to confirm.

## Result

BlueXP starts the software update. You can perform actions on the working environment once the software update is complete.

## After you finish

If you suspended SnapMirror transfers, use System Manager to resume the transfers.

## Fix download failures when using a Google Cloud NAT gateway

The Connector automatically downloads software updates for Cloud Volumes ONTAP. The download can fail if your configuration uses a Google Cloud NAT gateway. You can correct this issue by limiting the number of parts that the software image is divided into. This step must be completed by using the BlueXP API.

## Step

1. Submit a PUT request to /occm/config with the following JSON as body:

```
{
  "maxDownloadSessions": 32
}
```

The value for *maxDownloadSessions* can be 1 or any integer greater than 1. If the value is 1, then the downloaded image will not be divided.

Note that 32 is an example value. The value that you should use depends on your NAT configuration and the number of sessions that you can have simultaneously.

[Learn more about the /occm/config API call.](#)

## Registering pay-as-you-go systems

Support from NetApp is included with Cloud Volumes ONTAP PAYGO systems, but you must first activate support by registering the systems with NetApp.

Registering a PAYGO system with NetApp is required to upgrade ONTAP software using any of the methods [described on this page](#).



A system that isn't registered for support will still receive the software update notifications that appear in BlueXP when a new version is available. But you will need to register the system before you can upgrade the software.

### Steps

1. If you have not yet added your NetApp Support Site account to BlueXP, go to **Account Settings** and add it now.

[Learn how to add NetApp Support Site accounts.](#)

2. From the left navigation menu, select **Storage > Canvas**
3. On the Canvas page, double-click the name of the system that you want to register.
4. Click the menu icon and then click **Support registration**:



5. Select a NetApp Support Site account and click **Register**.

## Result

BlueXP registers the system with NetApp.

## Managing the state of Cloud Volumes ONTAP

You can stop and start Cloud Volumes ONTAP from BlueXP to manage your cloud compute costs.

### Scheduling automatic shutdowns of Cloud Volumes ONTAP

You might want to shut down Cloud Volumes ONTAP during specific time intervals to lower your compute costs. Rather than do this manually, you can configure BlueXP to automatically shut down and then restart systems at specific times.

#### About this task

- When you schedule an automatic shutdown of your Cloud Volumes ONTAP system, BlueXP postpones the shutdown if an active data transfer is in progress.

BlueXP shuts down the system after the transfer is complete.

- This task schedules automatic shutdowns of both nodes in an HA pair.
- Snapshots of boot and root disks are not created when turning off Cloud Volumes ONTAP through scheduled shutdowns.

Snapshots are automatically created only when performing a manual shutdown, as described in the next section.

#### Steps

1. From the working environment, click the clock icon:



2. Specify the shutdown schedule:
  - a. Choose whether you want to shut down the system every day, every weekday, every weekend, or any combination of the three options.
  - b. Specify when you want to turn off the system and for how long you want it turned off.

#### Example

The following image shows a schedule that instructs BlueXP to shut down the system every Saturday at 12:00 a.m. for 48 hours. BlueXP restarts the system every Monday at 12:00 a.m.

<input type="checkbox"/>	<b>Turn off every weekday</b> Mon, Tue, Wed, Thu, Fri	turn off at	08	:	00	PM	for	12	Hours (1-24)
<input checked="" type="checkbox"/>	<b>Turn off every weekend</b> Sat	turn off at	12	:	00	AM	for	48	Hours (1-48)

3. Click **Save**.

## Result

BlueXP saves the schedule. The clock icon changes to indicate that a schedule is set:



## Stopping Cloud Volumes ONTAP

Stopping Cloud Volumes ONTAP saves you from accruing compute costs and creates snapshots of the root and boot disks, which can be helpful for troubleshooting.



To reduce costs, BlueXP periodically deletes older snapshots of root and boot disks. Only the two most recent snapshots are retained for both the root and boot disks.

### About this task

When you stop an HA pair, BlueXP shuts down both nodes.

### Steps

1. From the working environment, click the **Turn off** icon.



2. Keep the option to create snapshots enabled because the snapshots can enable system recovery.
3. Click **Turn Off**.

It can take up to a few minutes to stop the system. You can restart systems at a later time from the working environment page.

## Synchronize the system time using NTP

Specifying an NTP server synchronizes the time between the systems in your network, which can help prevent issues due to time differences.

Specify an NTP server using the [BlueXP API](#) or from the user interface when you [create a CIFS server](#).

## Modify system write speed

BlueXP enables you to choose a normal or high write speed for Cloud Volumes ONTAP. The default write speed is normal. You can change to high write speed if fast write performance is required for your workload.

High write speed is supported with all types of single node systems and some HA pair configurations. View supported configurations in the [Cloud Volumes ONTAP Release Notes](#)

Before you change the write speed, you should [understand the differences between the normal and high settings](#).

### About this task



- Ensure that operations such as volume or aggregate creation are not in progress.
- Be aware that this change restarts the Cloud Volumes ONTAP system. This is disruptive process that requires downtime for the entire system.

### Steps

1. From the working environment, click the menu icon, and then click **Advanced > Writing Speed**.
2. Select **Normal** or **High**.

If you choose High, then you'll need to read the "I understand..." statement and confirm by checking the box.

3. Click **Save**, review the confirmation message, and then click **Proceed**.

## Change the password for Cloud Volumes ONTAP

Cloud Volumes ONTAP includes a cluster admin account. You can change the password for this account from BlueXP, if needed.



You should not change the password for the admin account through System Manager or the CLI. The password will not be reflected in BlueXP. As a result, BlueXP cannot monitor the instance properly.

### Steps

1. From the working environment, click the menu icon, and then click **Advanced > Set password**.
2. Enter the new password twice and then click **Save**.

The new password must be different than one of the last six passwords that you used.

## Add, remove, or delete systems

### Adding existing Cloud Volumes ONTAP systems to BlueXP

You can discover and add existing Cloud Volumes ONTAP systems to BlueXP. You might do this if you deployed a new BlueXP system.

### Before you begin

You must know the password for the Cloud Volumes ONTAP admin user account.

### Steps

1. From the left navigation menu, select **Storage > Canvas**.
2. On the Canvas page, click **Add Working Environment**.
3. Select the cloud provider in which the system resides.
4. Choose the type of Cloud Volumes ONTAP system.
5. Click the link to discover an existing system.



6. On the Region page, choose the region where the instances are running, and then select the instances.
7. On the Credentials page, enter the password for the Cloud Volumes ONTAP admin user, and then click **Go**.

### Result

BlueXP adds the Cloud Volumes ONTAP instances to the workspace.

### Removing Cloud Volumes ONTAP working environments

The Account Admin can remove a Cloud Volumes ONTAP working environment to move it to another system or to troubleshoot discovery issues.

#### About this task

Removing a Cloud Volumes ONTAP working environment removes it from BlueXP. It does not delete the Cloud Volumes ONTAP system. You can later rediscover the working environment.

Removing a working environment from BlueXP enables you to do the following:

- Rediscover it in another workspace
- Rediscover it from another BlueXP system
- Rediscover it if you had problems during the initial discovery

### Steps

1. In the upper right of the BlueXP console, click the Settings icon, and select **Tools**.



2. From the Tools page, click **Launch**.
3. Select the Cloud Volumes ONTAP working environment that you want to remove.
4. On the Review and Approve page, click **Go**.

## Result

BlueXP removes the working environment. Users can rediscover this working environment from the Canvas page at any time.

## Deleting a Cloud Volumes ONTAP system

You should always delete Cloud Volumes ONTAP systems from BlueXP, rather than from your cloud provider's console. For example, if you terminate a licensed Cloud Volumes ONTAP instance from your cloud provider, then you can't use the license key for another instance. You must delete the working environment from BlueXP to release the license.

When you delete a working environment, BlueXP terminates Cloud Volumes ONTAP instances and deletes disks and snapshots.

Resources managed by other services like backups for Cloud Backup and instances for Cloud Data Sense and Monitoring are not deleted when you delete a working environment. You'll need to manually delete them yourself. If you don't, then you'll continue to receive charges for these resources.



When BlueXP deploys Cloud Volumes ONTAP in your cloud provider, it enables termination protection on the instances. This option helps prevent accidental termination.

## Steps

1. If you enabled Cloud Backup on the working environment, determine whether the backed up data is still required and then [delete the backups, if necessary](#).

Cloud Backup is independent from Cloud Volumes ONTAP by design. Cloud Backup doesn't automatically delete backups when you delete a Cloud Volumes ONTAP system, and there is no current support in the UI to delete the backups after the system has been deleted.

2. If you enabled Cloud Data Sense on this working environment and no other working environments use this service, then you'll need to delete the instance for the service.

[Learn more about the Cloud Data Sense instance.](#)

3. Delete the Cloud Volumes ONTAP working environment.
  - a. On the Canvas page, double-click the name of the Cloud Volumes ONTAP working environment that you want to delete.
  - b. Click menu icon and then click **Delete**.



c. Type the name of the working environment and then click **Delete**.

It can take up to 5 minutes to delete the working environment.

## AWS administration

### Change the EC2 instance type for Cloud Volumes ONTAP

You can choose from several instance or types when you launch Cloud Volumes ONTAP in AWS. You can change the instance type at any time if you determine that it is undersized or oversized for your needs.

#### About this task

- Automatic giveback must be enabled on a Cloud Volumes ONTAP HA pair (this is the default setting). If it isn't, then the operation will fail.

[ONTAP 9 Documentation: Commands for configuring automatic giveback](#)

- Changing the instance type can affect AWS service charges.
- The operation restarts Cloud Volumes ONTAP.

For single node systems, I/O is interrupted.

For HA pairs, the change is nondisruptive. HA pairs continue to serve data.



BlueXP gracefully changes one node at a time by initiating takeover and waiting for give back. NetApp's QA team tested both writing and reading files during this process and didn't see any issues on the client side. As connections changed, we did see retries on the I/O level, but the application layer overcame these short "re-wire" of NFS/CIFS connections.

## Steps

1. From the left navigation menu, select **Storage > Canvas**.
2. From the Canvas, select the working environment.
3. In the right pane, click the menu icon and select **Optimize Cost & Performance**.



This option is also available by entering the working environment, opening the action menu, and selecting **Change instance**.

4. If you are using a node-based PAYGO license, you can optionally choose a different license.
5. Choose an instance type, select the check box to confirm that you understand the implications of the change, and then click **OK**.

## Result

Cloud Volumes ONTAP reboots with the new configuration.

## Change route tables for HA pairs in multiple AZs

You can modify the AWS route tables that include routes to the floating IP addresses for an HA pair that's deployed in multiple AWS Availability Zones (AZs). You might do this if new NFS or CIFS clients need to access an HA pair in AWS.

## Steps

1. From the working environment, click the menu icon and then click **Information**.
2. Click **Route Tables**.
3. Modify the list of selected route tables and then click **Save**.

## Result

BlueXP sends an AWS request to modify the route tables.

## Monitoring AWS resource costs

BlueXP enables you to view the resource costs associated with running Cloud Volumes ONTAP in AWS. You can also see how much money you saved by using NetApp features that can reduce storage costs.

### About this task

BlueXP updates the costs when you refresh the page. You should refer to AWS for final cost details.

### Step

1. Verify that BlueXP can obtain cost information from AWS:
  - a. Ensure that the IAM policy that provides BlueXP with permissions includes the required permissions.

[View the required permissions](#)

- b. [Activate the \*\*WorkingEnvironmentId\*\* tag.](#)

To track your AWS costs, BlueXP assigns a cost allocation tag to Cloud Volumes ONTAP instances. After you create your first working environment, activate the **WorkingEnvironmentId** tag. User-defined tags don't appear on AWS billing reports until you activate them in the Billing and Cost Management console.

2. From the left navigation menu, select **Storage > Canvas**.
3. On the Canvas page, select a Cloud Volumes ONTAP working environment and then click **Cost**.

The Cost page displays costs for the current and previous months and shows your annual NetApp savings, if you enabled NetApp's cost-saving features on volumes.

The following image shows a sample Cost page:

Cloud Manager obtains AWS resource costs by using the AWS Cost Explorer service



## Azure administration

### Change the Azure VM type for Cloud Volumes ONTAP

You can choose from several VM types when you launch Cloud Volumes ONTAP in Microsoft Azure. You can change the VM type at any time if you determine that it is undersized or oversized for your needs.

#### About this task

- Automatic giveback must be enabled on a Cloud Volumes ONTAP HA pair (this is the default setting). If it isn't, then the operation will fail.

[ONTAP 9 Documentation: Commands for configuring automatic giveback](#)

- Changing the VM type can affect Microsoft Azure service charges.
- The operation restarts Cloud Volumes ONTAP.

For single node systems, I/O is interrupted.

For HA pairs, the change is nondisruptive. HA pairs continue to serve data.



BlueXP gracefully changes one node at a time by initiating takeover and waiting for give back. NetApp's QA team tested both writing and reading files during this process and didn't see any issues on the client side. As connections changed, we did see retries on the I/O level, but the application layer overcame these short "re-wire" of NFS/CIFS connections.

#### Steps

- From the left navigation menu, select **Storage > Canvas**.

2. From the Canvas, select the working environment.
3. In the right pane, click the menu icon and select **Optimize Cost & Performance**.



This option is also available by entering the working environment, opening the action menu, and selecting **Change VM**.

4. If you are using a node-based PAYGO license, you can optionally choose a different license.
5. Select a VM type, select the check box to confirm that you understand the implications of the change, and then click **OK**.

## Result

Cloud Volumes ONTAP reboots with the new configuration.

## Overriding CIFS locks for Cloud Volumes ONTAP HA pairs in Azure

The Account Admin can enable a setting in BlueXP that prevents issues with Cloud Volumes ONTAP storage giveback during Azure maintenance events. When you enable this setting, Cloud Volumes ONTAP vetoes CIFS locks and resets active CIFS sessions.

### About this task

Microsoft Azure schedules periodic maintenance events on its virtual machines. When a maintenance event occurs on a Cloud Volumes ONTAP HA pair, the HA pair initiates storage takeover. If there are active CIFS sessions during this maintenance event, the locks on CIFS files can prevent storage giveback.

If you enable this setting, Cloud Volumes ONTAP will veto the locks and reset the active CIFS sessions. As a result, the HA pair can complete storage giveback during these maintenance events.





This process might be disruptive to CIFS clients. Data that is not committed from CIFS clients could be lost.

### What you'll need

You need to create a Connector before you can change BlueXP settings. [Learn how.](#)

### Steps

1. In the upper right of the BlueXP console, click the Settings icon, and select **Connector Settings**.



2. Under **Azure**, click **Azure CIFS locks for Azure HA working environments**.
3. Click the checkbox to enable the feature and then click **Save**.

### Use an Azure Private Link or service endpoints

Cloud Volumes ONTAP uses an Azure Private Link for connections to its associated storage accounts. If needed, you can disable Azure Private Links and use service endpoints instead.

#### Overview

By default, BlueXP enables an Azure Private Link for connections between Cloud Volumes ONTAP and its associated storage accounts. An Azure Private Link secures connections between endpoints in Azure and provides performance benefits.

If required, you can configure Cloud Volumes ONTAP to use service endpoints instead of an Azure Private Link.

With either configuration, BlueXP always limits network access for connections between Cloud Volumes ONTAP and storage accounts. Network access is limited to the VNet where Cloud Volumes ONTAP is deployed and the VNet where the Connector is deployed.

#### Disable Azure Private Links and use service endpoints instead

If required by your business, you can change a setting in BlueXP so that it configures Cloud Volumes ONTAP to use service endpoints instead of an Azure Private Link. Changing this setting applies to new Cloud Volumes ONTAP systems that you create. Service endpoints are only supported in [Azure region pairs](#) between the Connector and Cloud Volumes ONTAP VNets.

The Connector should be deployed in the same Azure region as the Cloud Volumes ONTAP systems that it manages, or in the [Azure region pair](#) for the Cloud Volumes ONTAP systems.

### Steps

1. In the upper right of the BlueXP console, click the Settings icon, and select **Connector Settings**.
2. Under **Azure**, click **Use Azure Private Link**.
3. Deselect **Private Link connection between Cloud Volumes ONTAP and storage accounts**.
4. Click **Save**.

## After you finish

If you disabled Azure Private Links and the Connector uses a proxy server, you must enable direct API traffic.

[Learn how to enable direct API traffic on the Connector](#)

## Work with Azure Private Links

In most cases, there's nothing that you need to do to set up Azure Private links with Cloud Volumes ONTAP. BlueXP manages Azure Private Links for you. But if you use an existing Azure Private DNS zone, then you'll need to edit a configuration file.

## Requirement for custom DNS

Optionally, if you work with custom DNS, you need to create a conditional forwarder to the Azure private DNS zone from your custom DNS servers. To learn more, refer to [Azure's documentation on using a DNS forwarder](#).

## How Private Link connections work

When BlueXP deploys Cloud Volumes ONTAP in Azure, it creates a private endpoint in the resource group. The private endpoint is associated with storage accounts for Cloud Volumes ONTAP. As a result, access to Cloud Volumes ONTAP storage travels through the Microsoft backbone network.

Client access goes through the private link when clients are within the same VNet as Cloud Volumes ONTAP, within peered VNets, or in your on-premises network when using a private VPN or ExpressRoute connection to the VNet.

Here's an example that shows client access over a private link from within the same VNet and from an on-prem network that has either a private VPN or ExpressRoute connection.



If the Connector and Cloud Volumes ONTAP systems are deployed in different VNets, then you must set up VNet peering between the VNet where the Connector is deployed and the VNet where the Cloud Volumes ONTAP systems are deployed.

## Provide BlueXP with details about your Azure Private DNS

If you use [Azure Private DNS](#), then you need to modify a configuration file on each Connector. Otherwise, BlueXP can't enable the Azure Private Link connection between Cloud Volumes ONTAP and its associated storage accounts.

Note that the DNS name must match Azure DNS naming requirements [as shown in Azure documentation](#).

### Steps

1. SSH to the Connector host and log in.
2. Navigate to the following directory: `/opt/application/netapp/cloudmanager/docker_occm/data`
3. Edit `app.conf` by adding the "user-private-dns-zone-settings" parameter with the following keyword-value pairs:

```
"user-private-dns-zone-settings" : {
  "resource-group" : "<resource group name of the DNS zone>",
  "subscription" : "<subscription ID>",
  "use-existing" : true
  "create-private-dns-zone-link" : true
}
```

The parameter should be entered at the same level as "system-id" like shown below:

```
"system-id" : "<system ID>",
"user-private-dns-zone-settings" : {
```

Note that the subscription keyword is required only if the Private DNS Zone exists in a different subscription than the Connector.

#### 4. Save the file and log off the Connector.

A reboot isn't required.

### Enable rollback on failures

If BlueXP fails to create an Azure Private Link as part of specific actions, it completes the action without the Azure Private Link connection. This can happen when creating a new working environment (single node or HA pair), or when the following actions occur on an HA pair: creating a new aggregate, adding disks to an existing aggregate, or creating a new storage account when going above 32 TiB.

You can change this default behavior by enabling rollback if BlueXP fails to create the Azure Private Link. This can help to ensure that you're fully compliant with your company's security regulations.

If you enable rollback, BlueXP stops the action and rolls back all resources that were created as part of the action.

You can enable rollback through the API or by updating the app.conf file.

### Enable rollback through the API

#### Step

1. Use the `PUT /occm/config` API call with the following request body:

```
{ "rollbackOnAzurePrivateLinkFailure": true }
```

### Enable rollback by updating app.conf

#### Step

1. Use the `PUT /occm/config` API call with the following request body:

```
{ "rollbackOnAzurePrivateLinkFailure": false }
```

## Moving resource groups

Cloud Volumes ONTAP supports Azure resource groups moves but the workflow happens in the Azure console only.

You can move a working environment from one resource group to a different resource group in Azure within the same Azure subscription. Moving resource groups between different Azure subscriptions is not supported.

### Steps

1. Remove the working environment from **Canvas**.

To learn how to remove a working environment, see [Removing Cloud Volumes ONTAP working environments](#).

2. Execute the resource group move in the Azure console.

To complete the move, refer to [Move resources to a new resource group or subscription in Microsoft Azure's documentation](#).

3. In **Canvas**, discover the working environment.
4. Look for the new resource group in the information for the working environment.

### Result

The working environment and its resources (VMs, disks, storage accounts, network interfaces, snapshots) are in the new resource group.

## Google Cloud administration

### Change the Google Cloud machine type for Cloud Volumes ONTAP

You can choose from several machine types when you launch Cloud Volumes ONTAP in Google Cloud. You can change the instance or machine type at any time if you determine that it is undersized or oversized for your needs.

#### About this task

- Automatic giveback must be enabled on a Cloud Volumes ONTAP HA pair (this is the default setting). If it isn't, then the operation will fail.

[ONTAP 9 Documentation: Commands for configuring automatic giveback](#)

- Changing the machine type can affect Google Cloud service charges.
- The operation restarts Cloud Volumes ONTAP.

For single node systems, I/O is interrupted.

For HA pairs, the change is nondisruptive. HA pairs continue to serve data.



BlueXP gracefully changes one node at a time by initiating takeover and waiting for give back. NetApp's QA team tested both writing and reading files during this process and didn't see any issues on the client side. As connections changed, we did see retries on the I/O level, but the application layer overcame these short "re-wire" of NFS/CIFS connections.

## Steps

1. From the Canvas, select the working environment.
2. In the right pane, click the menu icon and select **Optimize Cost & Performance**.



This option is also available by entering the working environment, opening the action menu, and selecting **Change machine**.

3. If you are using a node-based PAYGO license, you can optionally choose a different license.
4. Select a machine type, select the check box to confirm that you understand the implications of the change, and then click **OK**.

## Result

Cloud Volumes ONTAP reboots with the new configuration.

## Administer Cloud Volumes ONTAP using the Advanced View

If you need to perform advanced management of Cloud Volumes ONTAP, you can do so using ONTAP System Manager, which is a management interface that's provided with an ONTAP system. We have included the System Manager interface directly inside BlueXP so that you don't need to leave BlueXP for advanced management.

This Advanced View is available as a Preview. We plan to refine this experience and add enhancements in upcoming releases. Please send us feedback by using the in-product chat.

## Features

The Advanced View in BlueXP gives you access to additional management features:

- Advanced storage management

Manage consistency groups, shares, qtrees, quotas, and Storage VMs.

- Networking management

Manage IPspaces, network interfaces, portsets, and ethernet ports.

- Events and jobs

View event logs, system alerts, jobs, and audit logs.

- Advanced data protection

Protect storage VMs, LUNs, and consistency groups.

- Host management

Set up SAN initiator groups and NFS clients.

## Supported configurations

Advanced management through System Manager is supported with Cloud Volumes ONTAP 9.10.0 and later in standard cloud regions.

System Manager integration is not supported in GovCloud regions or in regions that have no outbound internet access.

## Limitations

A few features that appear in the System Manager interface are not supported with Cloud Volumes ONTAP:

- Cloud Tiering

The Cloud Tiering service is not supported with Cloud Volumes ONTAP. Tiering data to object storage must be set up directly from BlueXP's Standard View when creating volumes.

- Tiers

Aggregate management (including local tiers and cloud tiers) is not supported from System Manager. You must manage aggregates directly from BlueXP's Standard View.

- Firmware upgrades

Automatic firmware updates from the **Cluster > Settings** page is not supported with Cloud Volumes ONTAP.

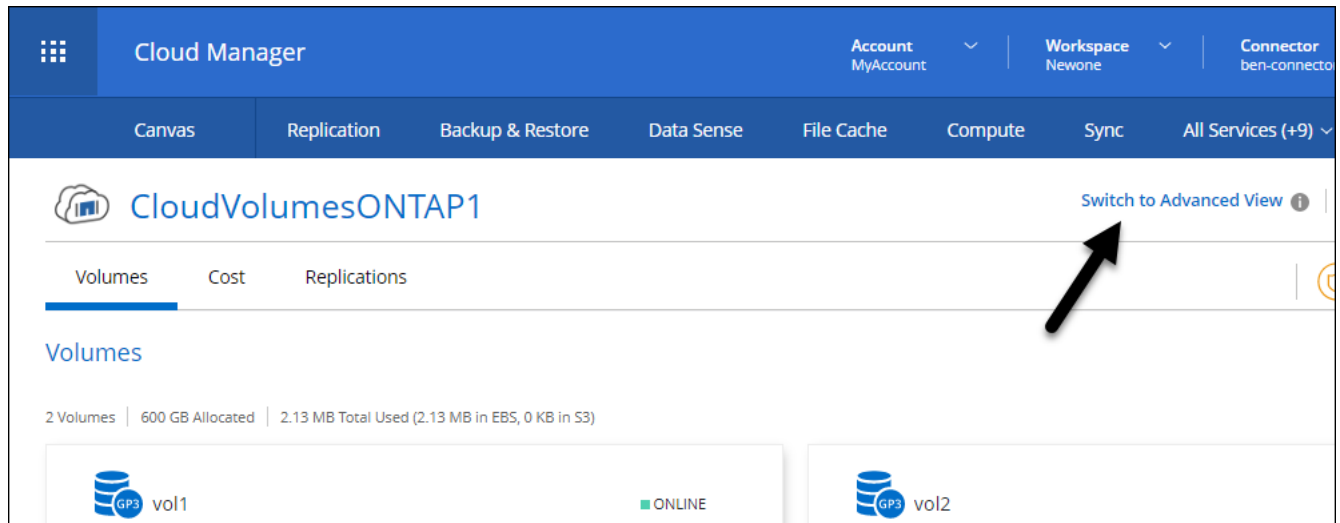
In addition, role-based access control from System Manager is not supported.

## How to get started

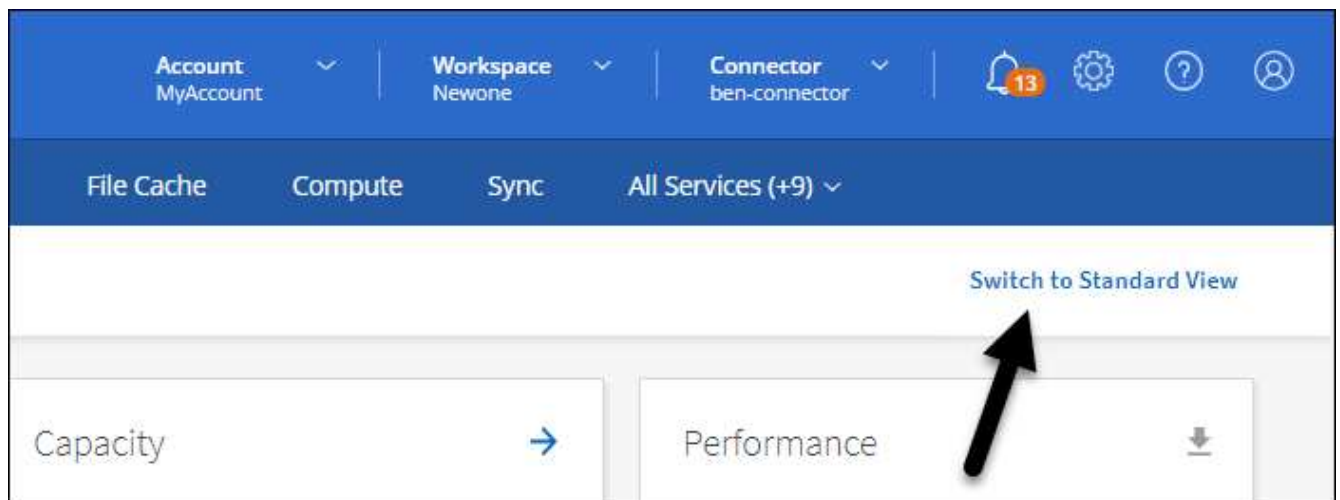
Open a Cloud Volumes ONTAP working environment and click the Advanced View option.

### Steps

1. From the left navigation menu, select **Storage > Canvas**.
2. On the Canvas page, double-click the name of a Cloud Volumes ONTAP system.
3. In the top-right, click **Switch to Advanced View**.



4. If the confirmation message appears, read through it and click **Close**.
5. Use System Manager to manage Cloud Volumes ONTAP.
6. If needed, click **Switch to Standard View** to return to standard management through BlueXP.



## Help with using System Manager

If you need help using System Manager with Cloud Volumes ONTAP, you can refer to [ONTAP documentation](#) for step-by-step instructions. Here are a few links that might help:

- [Volume and LUN management](#)
- [Network management](#)



- [Data protection](#)

## Administer Cloud Volumes ONTAP from the CLI

The Cloud Volumes ONTAP CLI enables you to run all administrative commands and is a good choice for advanced tasks or if you are more comfortable using the CLI. You can connect to the CLI using Secure Shell (SSH).

### Before you begin

The host from which you use SSH to connect to Cloud Volumes ONTAP must have a network connection to Cloud Volumes ONTAP. For example, you might need to SSH from a jump host that's in your cloud provider network.



When deployed in multiple AZs, Cloud Volumes ONTAP HA configurations use a floating IP address for the cluster management interface, which means external routing is not available. You must connect from a host that is part of the same routing domain.

### Steps

1. In BlueXP, identify the IP address of the cluster management interface:
  - a. From the left navigation menu, select **Storage > Canvas**.
  - b. On the Canvas page, select the Cloud Volumes ONTAP system.
  - c. Copy the cluster management IP address that appears in the right pane.
2. Use SSH to connect to the cluster management interface IP address using the admin account.

### Example

The following image shows an example using PuTTY:



3. At the login prompt, enter the password for the admin account.

### Example

```
Password: *****  
COT2::>
```

## System health and events

## Verify AutoSupport setup

AutoSupport proactively monitors the health of your system and sends messages to NetApp technical support. By default, AutoSupport is enabled on each node to send messages to technical support using the HTTPS transport protocol. It's best to verify that AutoSupport can send these messages.

The only required configuration step is to ensure that Cloud Volumes ONTAP has outbound internet connectivity. For details, refer to the networking requirements for your cloud provider.

### AutoSupport requirements

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

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

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

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

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

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

### Troubleshoot your AutoSupport configuration

If an outbound connection isn't available and BlueXP can't configure your Cloud Volumes ONTAP system to use the Connector as a proxy server, you'll receive a notification from BlueXP titled "<working environment name> is unable to send AutoSupport messages."

You're most likely receiving this message because of networking issues.

Follow these steps to address this problem.

#### Steps

1. SSH to the Cloud Volumes ONTAP system so that you can administer the system from the CLI.

[Learn how to SSH to Cloud Volumes ONTAP](#).

2. Display the detailed status of the AutoSupport subsystem:

```
autosupport check show-details
```

The response should be similar to the following:

```

Category: smtp
  Component: mail-server
    Status: failed
    Detail: SMTP connectivity check failed for destination:
           mailhost. Error: Could not resolve host -
'mailhost'
    Corrective Action: Check the hostname of the SMTP server

Category: http-https
  Component: http-put-destination
    Status: ok
    Detail: Successfully connected to:
           <https://support.netapp.com/put/AsupPut/>.

  Component: http-post-destination
    Status: ok
    Detail: Successfully connected to:

https://support.netapp.com/asupprod/post/1.0/postAsup.

Category: on-demand
  Component: ondemand-server
    Status: ok
    Detail: Successfully connected to:
           https://support.netapp.com/aods/asupmessage.

Category: configuration
  Component: configuration
    Status: ok
    Detail: No configuration issues found.
5 entries were displayed.

```

If the status of the http-https category is "ok" then it means AutoSupport is configured properly and messages can be sent.

3. If the status is not ok, verify the proxy URL for each Cloud Volumes ONTAP node:

```
autosupport show -fields proxy-url
```

4. If the proxy URL parameter is empty, configure Cloud Volumes ONTAP to use the Connector as a proxy:

```
autosupport modify -proxy-url http://<connector private ip>:3128
```

5. Verify AutoSupport status again:

```
autosupport check show-details
```

6. If the status is still failed, validate that there is connectivity between Cloud Volumes ONTAP and the Connector over port 3128.
7. If the status ID is still failed after verifying that there is connectivity, SSH to the Connector.

[Learn more about Connecting to the Linux VM for the Connector](#)

8. Go to `/opt/application/netapp/cloudmanager/docker_occm/data/`
9. Open the proxy configuration file `squid.conf`

The basic structure of the file is as follows:

```
http_port 3128
acl localnet src 172.31.0.0/16
acl azure_aws_metadata dst 169.254.169.254

http_access allow localnet
http_access deny azure_aws_metadata
http_access allow localhost
http_access deny all
```

The `localnet` `src` value is the CIDR of the Cloud Volumes ONTAP system.

10. If the CIDR block of the Cloud Volumes ONTAP system isn't in the range that's specified in the file, either update the value or add a new entry as follows:

```
acl cvonet src <cidr>
```

If you add this new entry, don't forget to also add an allow entry:

```
http_access allow cvonet
```

Here's an example:

```
http_port 3128
acl localnet src 172.31.0.0/16
acl cvonet src 172.33.0.0/16
acl azure_aws_metadata dst 169.254.169.254

http_access allow localnet
http_access allow cvonet
http_access deny azure_aws_metadata
http_access allow localhost
http_access deny all
```

11. After editing the config file, restart the proxy container as `sudo`:

```
docker restart squid
```

12. Go back to the Cloud Volumes ONTAP CLI and verify that Cloud Volumes ONTAP can send AutoSupport messages:

```
autosupport check show-details
```

## Configure EMS

The Event Management System (EMS) collects and displays information about events that occur on ONTAP systems. To receive event notifications, you can set event destinations (email addresses, SNMP trap hosts, or syslog servers) and event routes for a particular event severity.

You can configure EMS using the CLI. For instructions, refer to [ONTAP docs: EMS configuration overview](#).

# Concepts

## Cloud Volumes ONTAP licensing

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

### Licensing overview

The following licensing options are available for new customers.

#### Capacity-based licensing

Pay for multiple Cloud Volumes ONTAP systems in your NetApp account by provisioned capacity. Includes the ability to purchase add-on cloud data services.

#### Keystone Flex Subscription

A pay-as-you-grow subscription-based service that delivers a seamless hybrid cloud experience for HA pairs.

The previous by-node licensing model remains available for existing customers who have already purchased a license or who have an active marketplace subscription.

The following sections provide more details about each of these options.

### Capacity-based licensing

Capacity-based licensing packages enable you to pay for Cloud Volumes ONTAP per TiB of capacity. The license is associated with your NetApp account and enables you to charge multiple systems against the license, as long as enough capacity is available through the license.

For example, you could purchase a single 20 TiB license, deploy four Cloud Volumes ONTAP systems, and then allocate a 5 TiB volume to each system, for a total of 20 TiB. The capacity is available to the volumes on each Cloud Volumes ONTAP system deployed in that account.

Capacity-based licensing is available in the form of a *package*. When you deploy a Cloud Volumes ONTAP system, you can choose from several licensing packages based on your business needs.

### Packages

The following capacity-based packages are available for Cloud Volumes ONTAP.

#### Freemium

Provides all Cloud Volumes ONTAP features free of charge from NetApp (cloud provider charges still apply).

- No license or contract is needed.
- Support from NetApp is not included.
- You're limited to 500 GiB of provisioned capacity per Cloud Volumes ONTAP system.
- You can use up to 10 Cloud Volumes ONTAP systems with the Freemium offering per NetApp account, in any cloud provider.

- If the provisioned capacity for a Cloud Volumes ONTAP system exceeds 500 GiB, BlueXP converts the system to the Essentials package.

As soon as a system is converted to the Essentials package, the [minimum charge](#) applies.

Any other systems that have less than 500 GiB of provisioned capacity stay on Freemium (as long as they were deployed using the Freemium offering).

### Optimized

Pay for provisioned capacity and I/O operations separately.

- Cloud Volumes ONTAP single node or HA
- Charging is based on two cost components: storage and usage (I/O)

You will not be charged for I/O related to data replication (SnapMirror) or NDMP.

- Available in the Azure Marketplace as a pay-as-you-go offering or as an annual contract
- Available in the Google Cloud Marketplace as a pay-as-you-go offering or as an annual contract
- Supported with selected VM types:
  - For Azure: E4s\_v3, E4ds\_v4, DS4\_v2, DS13\_v2, E8s\_v3, and E8ds\_v4
  - For Google Cloud: n2-standard-4, n2-standard-8
- Add on any of NetApp's cloud data services at extra cost

### Essentials

Pay by capacity for Cloud Volumes ONTAP in a number of different configurations.

- Choose your Cloud Volumes ONTAP configuration:
  - A single node or HA system
  - File and block storage or secondary data for disaster recovery (DR)
- Add on any of NetApp's cloud data services at extra cost

### Professional

Pay by capacity for any type of Cloud Volumes ONTAP configuration with unlimited backups.

- Provides licensing for any Cloud Volumes ONTAP configuration

Single node or HA with capacity charging for primary and secondary volumes at the same rate

- Includes unlimited volume backups using Cloud Backup, but only for Cloud Volumes ONTAP systems that use the Professional package
- Add on any of NetApp's cloud data services at extra cost

### Edge Cache

Provides licensing for Cloud Volumes Edge Cache.

- The same capabilities as the Professional package with business continuity and data protection for a

distributed enterprise

- Intelligent edge caching through a small-footprint Windows VM at each location
- One edge node with every 3 TiBs of capacity purchased
- Available in the Azure Marketplace as a pay-as-you-go offering or as an annual contract
- Available in the Google Cloud Marketplace as a pay-as-you-go offering or as an annual contract

[Learn more about how Cloud Volumes Edge Cache can help your business](#)

## Consumption models

Capacity-based licensing packages are available with the following consumption models:

- **BYOL**: A license purchased from NetApp that can be used to deploy Cloud Volumes ONTAP in any cloud provider.

Note that the Optimized and Edge Cache packages are not available with BYOL.

- **PAYGO**: An hourly subscription from your cloud provider's marketplace.
- **Annual**: An annual contract from your cloud provider's marketplace.

Note the following:

- If you purchase a license from NetApp (BYOL), you also need to subscribe to the PAYGO offering from your cloud provider's marketplace.

Your license is always charged first, but you'll be charged from the hourly rate in the marketplace in these cases:

- If you exceed your licensed capacity
- If the term of your license expires
- If you have an annual contract from a marketplace, *all* Cloud Volumes ONTAP systems that you deploy are charged against that contract. You can't mix and match an annual marketplace contract with BYOL.

## Changing packages

After deployment, you can change the package for a Cloud Volumes ONTAP system that uses capacity-based licensing. For example, if you deployed a Cloud Volumes ONTAP system with the Essentials package, you can change it to the Professional package if your business needs changed.

[Learn how to change charging methods.](#)

## Pricing

For details about pricing, go to [NetApp BlueXP website](#).

## Free trials

A 30-day free trial is available from the pay-as-you-go subscription in your cloud provider's marketplace. The free trial includes Cloud Volumes ONTAP and Cloud Backup. The trial starts when you subscribe to the offering in the marketplace.

There are no instance or capacity limitations. You can deploy as many Cloud Volumes ONTAP systems as



you'd like and allocate as much capacity as needed, free of charge for 30 days. The free trial automatically converts to a paid hourly subscription after 30 days.

There are no hourly software license charges for Cloud Volumes ONTAP, but infrastructure charges from your cloud provider still apply.

You will receive a notification in BlueXP when the free trial starts, when there are 7 days left, and when there is 1 day remaining. For example:



**Your Cloud Manager free trial is almost over (7 days left)**

23 minutes ago | Digital Wallet

## Supported configurations

Capacity-based licensing packages are available with Cloud Volumes ONTAP 9.7 and later.

### Capacity limit

With this licensing model, each individual Cloud Volumes ONTAP system supports up to 2 PiB of capacity through disks and tiering to object storage.

There is no maximum capacity limitation when it comes to the license itself.

### Max number of systems

With capacity-based licensing, the maximum number of Cloud Volumes ONTAP systems is limited to 20 per NetApp account. A *system* is a Cloud Volumes ONTAP HA pair, a Cloud Volumes ONTAP single node system, or any additional storage VMs that you create. The default storage VM does not count against the limit. This limit applies to all licensing models.

For example, let's say you have three working environments:

- A single node Cloud Volumes ONTAP system with one storage VM (this is the default storage VM that's created when you deploy Cloud Volumes ONTAP)

This working environment counts as one system.

- A single node Cloud Volumes ONTAP system with two storage VMs (the default storage VM, plus one additional storage VM that you created)

This working environment counts as two systems: one for the single node system and one for the additional storage VM.

- A Cloud Volumes ONTAP HA pair with three storage VMs (the default storage VM, plus two additional storage VMs that you created)

This working environment counts as three systems: one for the HA pair and two for the additional storage VMs.

That's six systems in total. You would then have room for an additional 14 systems in your account.

If you have a large deployment that requires more than 20 systems, contact your account rep or sales team.

[Learn more about NetApp accounts.](#)

## Notes about charging

The following details can help you understand how charging works with capacity-based licensing.

### Minimum charge

There is a 4 TiB minimum charge for each data-serving storage VM that has at least one primary (read-write) volume. If the sum of the primary volumes is less than 4 TiB, then BlueXP applies the 4 TiB minimum charge to that storage VM.

If you haven't provisioned any volumes yet, then the minimum charge doesn't apply.

The 4 TiB minimum capacity charge doesn't apply to storage VMs that contain secondary (data protection) volumes only. For example, if you have a storage VM with 1 TiB of secondary data, then you're charged just for that 1 TiB of data.

### Overages

If you exceed your BYOL capacity or if your license expires, you'll be charged for overages at the hourly rate based on your marketplace subscription.

### Essentials package

With the Essentials package, you're billed by the deployment type (HA or single node) and the volume type (primary or secondary). For example, *Essentials HA* has different pricing than *Essentials Secondary HA*.

If you purchased an Essentials license from NetApp (BYOL) and you exceed the licensed capacity for that deployment and volume type, the Digital Wallet charges overages against a higher priced Essentials license (if you have one). This happens because we first use the available capacity that you've already purchased as prepaid capacity before charging against the marketplace. Charging to the marketplace would add costs to your monthly bill.

Here's an example. Let's say you have the following licenses for the Essentials package:

- A 500 TiB *Essentials Secondary HA* license that has 500 TiB of committed capacity
- A 500 TiB *Essentials Single Node* license that only has 100 TiB of committed capacity

Another 50 TiB is provisioned on an HA pair with secondary volumes. Instead of charging that 50 TiB to PAYGO, the Digital Wallet charges the 50 TiB overage against the *Essentials Single Node* license. That license is priced higher than *Essentials Secondary HA*, but it's cheaper than the PAYGO rate.

In the Digital Wallet, that 50 TiB will be shown as charged against the *Essentials Single Node* license.

### Storage VMs

- There are no extra licensing costs for additional data-serving storage VMs (SVMs), but there is a 4 TiB minimum capacity charge per data-serving SVM.
- Disaster recovery SVMs are charged according to the provisioned capacity.

## HA pairs

For HA pairs, you're only charged for the provisioned capacity on a node. You aren't charged for data that is synchronously mirrored to the partner node.

## FlexClone and FlexCache volumes

- You won't be charged for the capacity used by FlexClone volumes.
- Source and destination FlexCache volumes are considered primary data and charged according to the provisioned space.

## How to get started

Learn how to get started with capacity-based licensing:

- [Set up licensing for Cloud Volumes ONTAP in AWS](#)
- [Set up licensing for Cloud Volumes ONTAP in Azure](#)
- [Set up licensing for Cloud Volumes ONTAP in Google Cloud](#)

## Keystone Flex Subscription

A pay-as-you-grow subscription-based service that delivers a seamless hybrid cloud experience for those preferring OpEx consumption models to upfront CapEx or leasing.

Charging is based on the size of your committed capacity for one or more Cloud Volumes ONTAP HA pairs in your Keystone Flex Subscription.

The provisioned capacity for each volume is aggregated and compared to the committed capacity on your Keystone Flex Subscription periodically, and any overages are charged as burst on your Keystone Flex Subscription.

[Learn more about Keystone Flex Subscriptions.](#)

## Supported configurations

Keystone Flex Subscriptions are supported with HA pairs. This licensing option isn't supported with single node systems at this time.

## Capacity limit

Each individual Cloud Volumes ONTAP system supports up to 2 PiB of capacity through disks and tiering to object storage.

## How to get started

Learn how to get started with a Keystone Flex Subscription:

- [Set up licensing for Cloud Volumes ONTAP in AWS](#)
- [Set up licensing for Cloud Volumes ONTAP in Azure](#)
- [Set up licensing for Cloud Volumes ONTAP in Google Cloud](#)

## Node-based licensing

Node-based licensing is the previous generation licensing model that enabled you to license Cloud Volumes ONTAP by node. This licensing model is not available for new customers and no free trials are available. By-node charging has been replaced with the by-capacity charging methods described above.

Node-based licensing is still available for existing customers:

- If you have an active license, BYOL is available for license renewals only.
- If you have an active marketplace subscription, charging is still available through that subscription.

## License conversions

Converting an existing Cloud Volumes ONTAP system to another licensing method isn't supported. The three current licensing methods are capacity-based licensing, Keystone Flex Subscriptions, and node-based licensing. For example, you can't convert a system from node-based licensing to capacity-based licensing (and vice versa).

If you want to transition to another licensing method, you can purchase a license, deploy a new Cloud Volumes ONTAP system using that license, and then replicate the data to that new system.

Note that converting a system from PAYGO by-node licensing to BYOL by-node licensing (and vice versa) isn't supported. You need to deploy a new system and then replicate data to that system. [Learn how to change between PAYGO and BYOL.](#)

## Storage

### Client protocols

Cloud Volumes ONTAP supports the iSCSI, NFS, SMB, NVMe-TCP, and S3 client protocols.

#### iSCSI

iSCSI is a block protocol that can run on standard Ethernet networks. Most client operating systems offer a software initiator that runs over a standard Ethernet port.

#### NFS

NFS is the traditional file access protocol for UNIX and LINUX systems. Clients can access files in ONTAP volumes using the NFSv3, NFSv4, and NFSv4.1 protocols. You can control file access using UNIX-style permissions, NTFS-style permissions, or a mix of both.

Clients can access the same files using both NFS and SMB protocols.

#### SMB

SMB is the traditional file access protocol for Windows systems. Clients can access files in ONTAP volumes using the SMB 2.0, SMB 2.1, SMB 3.0, and SMB 3.1.1 protocols. Just like with NFS, a mix of permission styles are supported.

## S3

Cloud Volumes ONTAP supports S3 as an option for scale-out storage. S3 protocol support enables you to configure S3 client access to objects contained in a bucket in a storage VM (SVM).

[Learn how S3 multiprotocol works.](#)

[Learn how to configure and manage S3 object storage services in ONTAP.](#)

## NVMe-TCP

NVMe-TCP is supported for cloud providers if you are using Cloud Volumes ONTAP version 9.12.1 or newer. BlueXP does not provide any management capabilities for NVMe-TCP.

For more information on configuring NVMe through ONTAP, see [Configure a storage VM for NVMe](#).

## Disks and aggregates

Understanding how Cloud Volumes ONTAP uses cloud storage can help you understand your storage costs.



All disks and aggregates must be created and deleted directly from BlueXP. You should not perform these actions from another management tool. Doing so can impact system stability, hamper the ability to add disks in the future, and potentially generate redundant cloud provider fees.

## Overview

Cloud Volumes ONTAP uses cloud provider storage as disks and groups them into one or more aggregates. Aggregates provide storage to one or more volumes.



Several types of cloud disks are supported. You choose the disk type when you create a volume and the default disk size when you deploy Cloud Volumes ONTAP.



The total amount of storage purchased from a cloud provider is the *raw capacity*. The *usable capacity* is less because approximately 12 to 14 percent is overhead that is reserved for Cloud Volumes ONTAP use. For example, if BlueXP creates a 500 GiB aggregate, the usable capacity is 442.94 GiB.

## AWS storage

In AWS, Cloud Volumes ONTAP uses EBS storage for user data and local NVMe storage as Flash Cache on some EC2 instance types.

## EBS storage

In AWS, an aggregate can contain up to 6 disks that are all the same size. But if you have a configuration that supports the Amazon EBS Elastic Volumes feature, then an aggregate can contain up to 8 disks. [Learn more about support for Elastic Volumes.](#)

The maximum disk size is 16 TiB.

The underlying EBS disk type can be either General Purpose SSDs (gp3 or gp2), Provisioned IOPS SSD (io1), or Throughput Optimized HDD (st1). You can pair an EBS disk with Amazon S3 to [tier inactive data to low-cost object storage](#).



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

## Local NVMe storage

Some EC2 instance types include local NVMe storage, which Cloud Volumes ONTAP uses as [Flash Cache](#).

## Related links

- [AWS documentation: EBS Volume Types](#)
- [Learn how to choose disk types and disk sizes for your systems in AWS](#)
- [Review storage limits for Cloud Volumes ONTAP in AWS](#)
- [Review supported configurations for Cloud Volumes ONTAP in AWS](#)

## Azure storage

In Azure, an aggregate can contain up to 12 disks that are all the same size. The disk type and maximum disk size depends on whether you use a single node system or an HA pair:

### Single node systems

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

- *Premium SSD Managed Disks* provide high performance for I/O-intensive workloads at a higher cost.
- *Standard SSD Managed Disks* provide consistent performance for workloads that require low IOPS.
- *Standard HDD Managed Disks* are a good choice if you don't need high IOPS and want to reduce your costs.

Each managed disk type has a maximum disk size of 32 TiB.

You can pair a managed disk with Azure Blob storage to [tier inactive data to low-cost object storage](#).

### HA pairs

HA pairs use two types of disks which provide high performance for I/O-intensive workloads at a higher cost:

- *Premium page blobs* with a maximum disk size of 8 TiB
- *Managed disks* with a maximum disk size of 32 TiB

## Related links

- [Microsoft Azure documentation: Azure managed disk types](#)
- [Microsoft Azure documentation: Overview of Azure page blobs](#)
- [Learn how to choose disk types and disk sizes for your systems in Azure](#)
- [Review storage limits for Cloud Volumes ONTAP in Azure](#)

## Google Cloud storage

In Google Cloud, an aggregate can contain up to 6 disks that are all the same size. The maximum disk size is 64 TiB.

The disk type can be either *Zonal SSD persistent disks*, *Zonal Balanced persistent disks*, or *Zonal standard persistent disks*. You can pair persistent disks with a Google Storage bucket to [tier inactive data to low-cost object storage](#).

## Related links

- [Google Cloud documentation: Storage Options](#)
- [Review storage limits for Cloud Volumes ONTAP in Google Cloud](#)

## RAID type

The RAID type for each Cloud Volumes ONTAP aggregate is RAID0 (striping). Cloud Volumes ONTAP relies on the cloud provider for disk availability and durability. No other RAID types are supported.

## Hot spares

RAID0 doesn't support the use of hot spares for redundancy.

Creating unused disks (hot spares) attached to a Cloud Volumes ONTAP instance is an unnecessary expense and may prevent provisioning additional space as needed. Therefore, it's not recommended.

## Elastic Volumes in AWS

Support for the Amazon EBS Elastic Volumes feature with a Cloud Volumes ONTAP aggregate provides better performance and additional capacity, while enabling BlueXP to automatically increase the underlying disk capacity as needed.

## Benefits

- Dynamic disk growth

BlueXP can dynamically increase the size of disks while Cloud Volumes ONTAP is running and while disks are still attached.

- Better performance

Aggregates that are enabled with Elastic Volumes can have up to eight disks that are equally utilized across two RAID groups. This configuration provides more throughput and consistent performance.

- Larger aggregates

Support for eight disks provides a maximum aggregate capacity of 128 TiB. These limits are higher than the six disk limit and 96 TiB limit for aggregates that aren't enabled with the Elastic Volumes feature.

Note that total system capacity limits remain the same.

[Learn more about Elastic Volumes from AWS](#)

## Supported configurations

The Amazon EBS Elastic Volumes feature is supported with specific Cloud Volumes ONTAP versions and specific EBS disk types.

### Cloud Volumes ONTAP version

The Elastic Volumes feature is supported with *new* Cloud Volumes ONTAP systems created from version 9.11.0 or later. The feature is *not* supported with existing Cloud Volumes ONTAP systems that were deployed



prior to 9.11.0.

For example, the Elastic Volumes feature is not supported if you created a Cloud Volumes ONTAP 9.9.0 system and then later upgraded that system to version 9.11.0. It must be a new system deployed using version 9.11.0 or later.

### EBS disk types

The Elastic Volumes feature is automatically enabled at the aggregate level when using General Purpose SSDs (gp3) or Provisioned IOPS SSDs (io1). The Elastic Volumes feature is not supported with aggregates that use any other disk type.

### Required AWS permissions

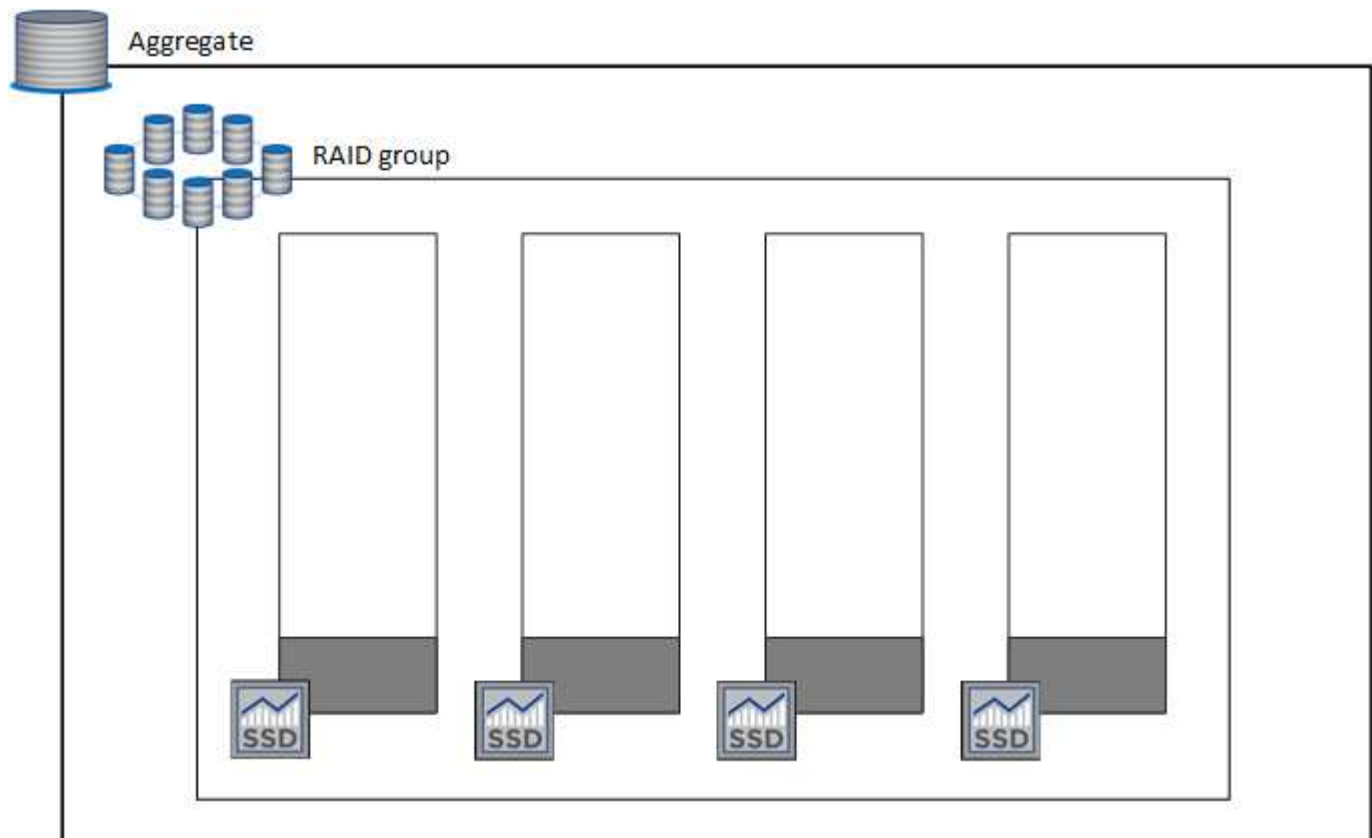
Starting with the 3.9.19 release, the Connector requires the following permissions to enable and manage the Elastic Volumes feature on a Cloud Volumes ONTAP aggregate:

- ec2:DescribeVolumesModifications
- ec2:ModifyVolume

These permissions are included in [the policies provided by NetApp](#)

### How support for Elastic Volumes works

An aggregate that has the Elastic Volumes feature enabled is comprised of one or two RAID groups. Each RAID group has four identical disks that have the same capacity. Here's an example of a 10 TiB aggregate that has four disks that are 2.5 TiB each:



When BlueXP creates an aggregate, it starts with one RAID group. If additional capacity is needed, BlueXP

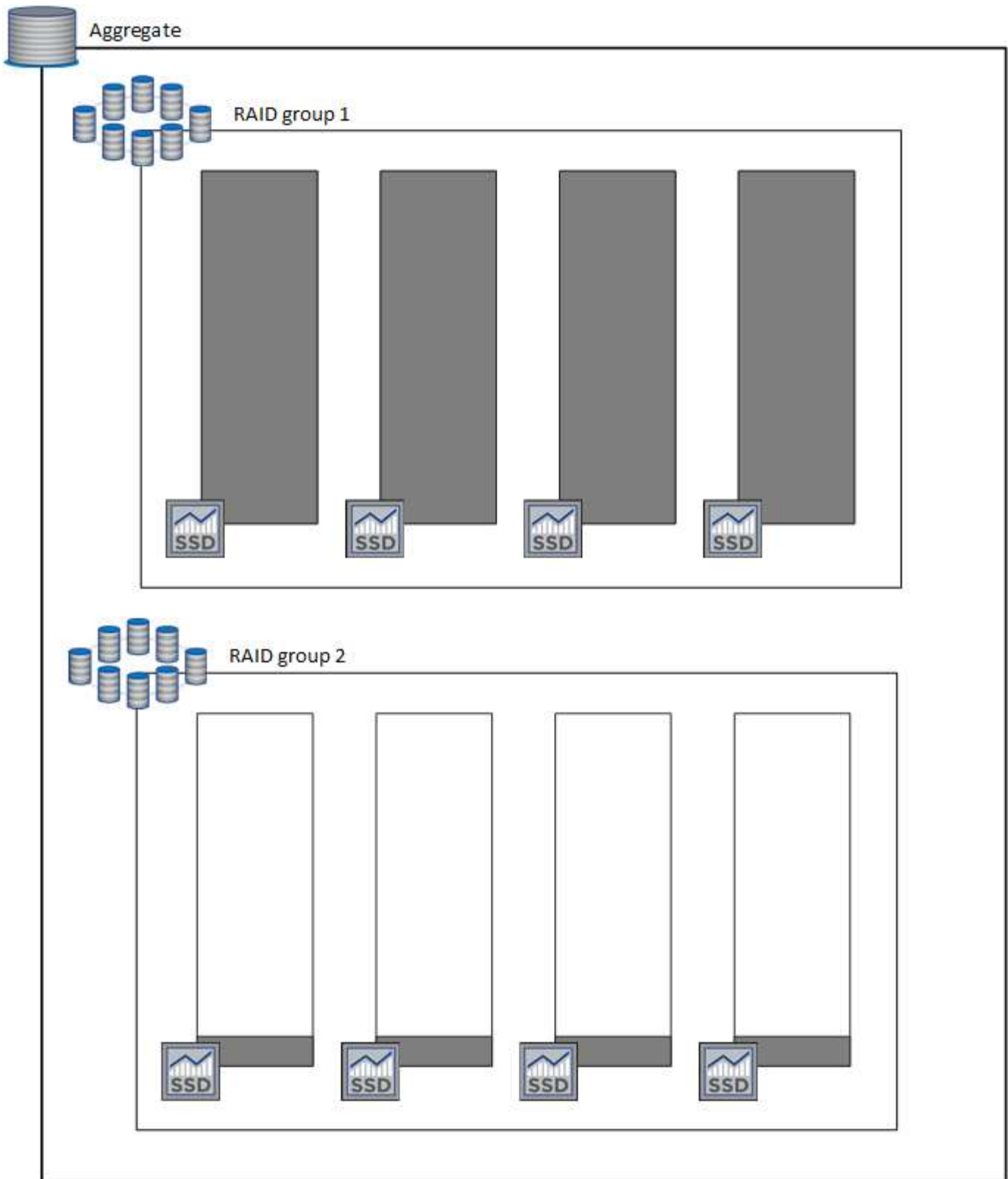
grows the aggregate by increasing the capacity of all disks in the RAID group by the same amount. The capacity increase is either a minimum of 256 GiB or 10% of the aggregate's size.

For example, if you have a 1 TiB aggregate, each disk is 250 GiB. 10% of the aggregate's capacity is 100 GiB. That's lower than 256 GiB, so the size of the aggregate is increased by the 256 GiB minimum (or 64 GiB for each disk).

BlueXP increases the size of the disks while the Cloud Volumes ONTAP system is running and while the disks are still attached. The change is non-disruptive.

If an aggregate reaches 64 TiB (or 16 TiB on each disk), BlueXP creates a second RAID group for additional capacity. This second RAID group works just like the first one: it has four disks that have the exact same capacity and it can grow up to 64 TiB. That means an aggregate can have a maximum capacity of 128 TiB.

Here's an example of an aggregate with two RAID groups. The capacity limit has been reached on the first RAID group, while the disks in the second RAID group have plenty of free space.



### What happens when you create a volume

If you create a volume that uses gp3 or io1 disks, BlueXP creates the volume on an aggregate as follows:

- If there is an existing gp3 or io1 aggregate that has Elastic Volumes enabled, BlueXP creates the volume on that aggregate.

- If there are multiple gp3 or io1 aggregates that have Elastic Volumes enabled, BlueXP creates the volume on the aggregate that requires the least amount of resources.
- If the system only has gp3 or io1 aggregates that aren't enabled for Elastic Volumes, then the volume is created on that aggregate.



While this scenario is unlikely, it's possible in two cases:

- You explicitly disabled the Elastic Volumes feature when creating an aggregate from the API.
- You created a new Cloud Volumes ONTAP system from the user interface, in which case the Elastic Volumes feature is disabled on the initial aggregate. Review [Limitations](#) below to learn more.

- If no existing aggregates have enough capacity, BlueXP creates the aggregate with Elastic Volumes enabled and then creates the volume on that new aggregate.

The size of the aggregate is based on the requested volume size plus an additional 10% capacity.

### Capacity Management Mode

The Capacity Management Mode for a Connector works with Elastic Volumes similar to how it works with other types of aggregates:

- When Automatic mode is enabled (this is the default setting), BlueXP automatically increases the size of aggregates if additional capacity is needed.
- If you change the capacity management mode to Manual, BlueXP asks for your approval to purchase additional capacity.

[Learn more about the Capacity Management Mode.](#)

### Limitations

Increasing the size of an aggregate can take up to 6 hours. During that time, BlueXP can't request any additional capacity for that aggregate.

### How to work with Elastic Volumes

You can work with Elastic Volumes in BlueXP as follows:

- Create a new system that has Elastic Volumes enabled on the initial aggregate when using gp3 or io1 disks

[Learn how to create Cloud Volumes ONTAP system](#)

- Create a new volume on an aggregate that has Elastic Volumes enabled

If you create a volume that uses gp3 or io1 disks, BlueXP automatically creates the volume on an aggregate that has Elastic Volumes enabled. For more details, refer to [What happens when you create a volume.](#)

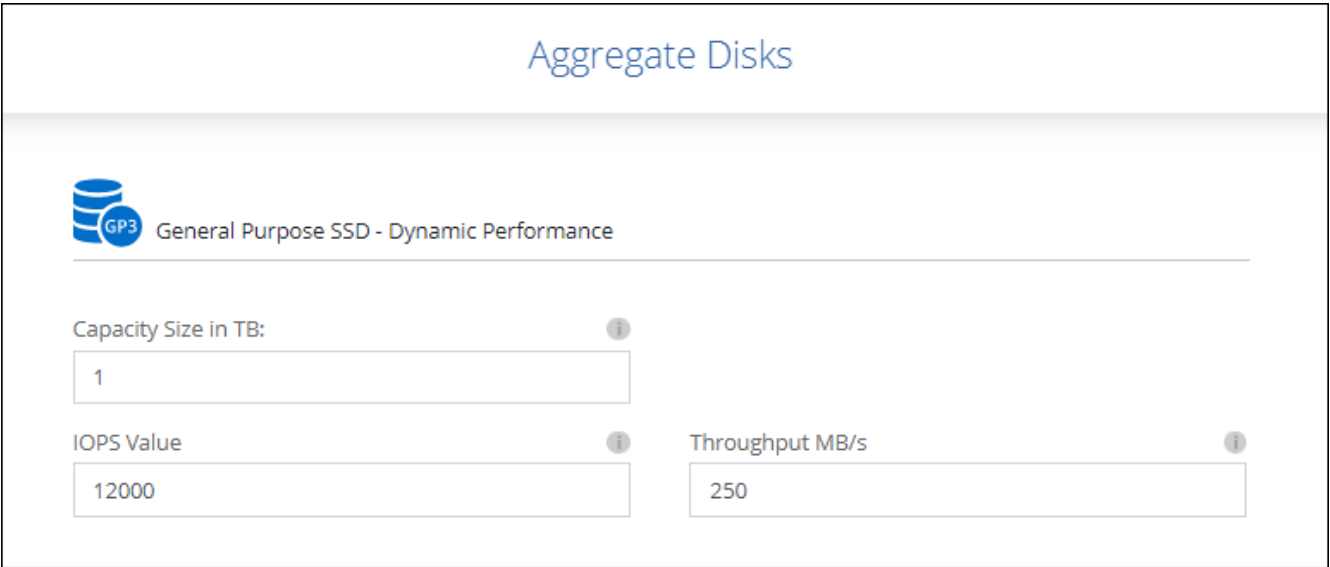
[Learn how to create volumes.](#)

- Create a new aggregate that has Elastic Volumes enabled

Elastic Volumes is automatically enabled on new aggregates that use gp3 or io1 disks, as long as the Cloud Volumes ONTAP system was created from version 9.11.0 or later.

When you create the aggregate, BlueXP will prompt you for the aggregate’s capacity size. This is different than other configurations where you choose a disk size and number of disks.

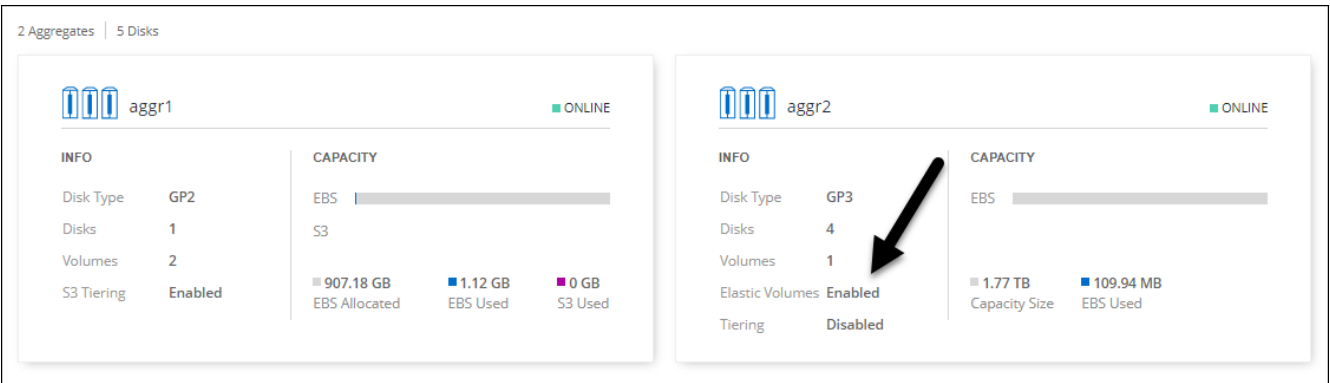
The following screenshot shows an example of a new aggregate comprised of gp3 disks.



[Learn how to create aggregates.](#)

- Identify aggregates that have Elastic Volumes enabled

When you go to the Advanced Allocation page, you can identify whether the Elastic Volumes feature is enabled on an aggregate. In the following example, aggr2 has Elastic Volumes enabled whereas aggr1 does not.



- Add capacity to an aggregate

While BlueXP automatically adds capacity to aggregates as needed, you can manually increase the capacity yourself.

[Learn how to increase aggregate capacity.](#)

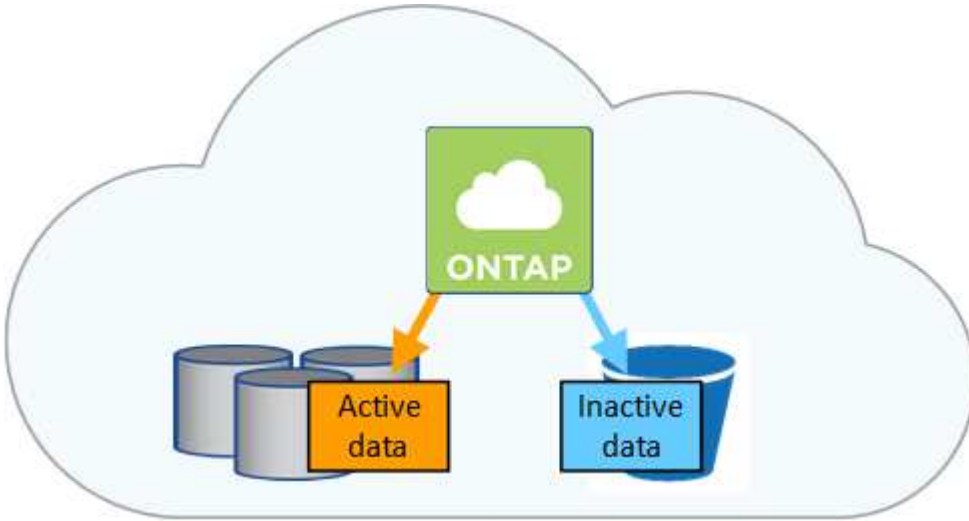
- Replicate data to an aggregate that has Elastic Volumes enabled

If the destination Cloud Volumes ONTAP system supports Elastic Volumes, a destination volume will be placed on an aggregate that has Elastic Volumes enabled (as long as you choose a gp3 or io1 disk).

[Learn how to set up data replication](#)

## Data tiering overview

Reduce your storage costs by enabling automated tiering of inactive data to low-cost object storage. Active data remains in high-performance SSDs or HDDs, while inactive data is tiered to low-cost object storage. This enables you to reclaim space on your primary storage and shrink secondary storage.



Data tiering is powered by FabricPool technology.



You don't need to install a feature license to enable data tiering (FabricPool).

## Data tiering in AWS

When you enable data tiering in AWS, Cloud Volumes ONTAP uses EBS as a performance tier for hot data and AWS S3 as a capacity tier for inactive data.

### Performance tier

The performance tier can be General Purpose SSDs (gp3 or gp2) or Provisioned IOPS SSDs (io1).

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

### Capacity tier

A Cloud Volumes ONTAP system tiers inactive data to a single S3 bucket.

BlueXP creates a single S3 bucket for each working environment and names it *fabric-pool-cluster unique identifier*. A different S3 bucket is not created for each volume.

When BlueXP creates the S3 bucket, it uses the following default settings:

- Storage class: Standard
- Default encryption: Disabled

- Block public access: Block all public access
- Object ownership: ACLs enabled
- Bucket versioning: Disabled
- Object lock: Disabled

## Storage classes

The default storage class for tiered data in AWS is *Standard*. Standard is ideal for frequently accessed data stored across multiple Availability Zones.

If you don't plan to access the inactive data, you can reduce your storage costs by changing the storage class to one of the following: *Intelligent Tiering*, *One-Zone Infrequent Access*, *Standard-Infrequent Access*, or *S3 Glacier Instant Retrieval*. When you change the storage class, inactive data starts in the Standard storage class and transitions to the storage class that you selected, if the data is not accessed after 30 days.

The access costs are higher if you do access the data, so take that into consideration before you change the storage class. [Learn more about Amazon S3 storage classes](#).

You can select a storage class when you create the working environment and you can change it any time after. For details about changing the storage class, see [Tiering inactive data to low-cost object storage](#).

The storage class for data tiering is system wide—it's not per volume.

## Data tiering in Azure

When you enable data tiering in Azure, Cloud Volumes ONTAP uses Azure managed disks as a performance tier for hot data and Azure Blob storage as a capacity tier for inactive data.

### Performance tier

The performance tier can be either SSDs or HDDs.

### Capacity tier

A Cloud Volumes ONTAP system tiers inactive data to a single Blob container.

BlueXP creates a new storage account with a container for each Cloud Volumes ONTAP working environment. The name of the storage account is random. A different container is not created for each volume.

BlueXP creates the storage account with the following settings:

- Access tier: Hot
- Performance: Standard
- Redundancy: Locally-redundant storage (LRS)
- Account: StorageV2 (general purpose v2)
- Require secure transfer for REST API operations: Enabled
- Storage account key access: Enabled
- Minimum TLS version: Version 1.2
- Infrastructure encryption: Disabled

## Storage access tiers

The default storage access tier for tiered data in Azure is the *hot* tier. The hot tier is ideal for frequently accessed data in the capacity tier.

If you don't plan to access the inactive data in the capacity tier, you can reduce your storage costs by changing to the *cool* storage tier. When you change the storage tier to cool, inactive capacity tier data moves directly to the cool storage tier.

The access costs are higher if you do access the data, so take that into consideration before you change the storage tier. [Learn more about Azure Blob storage access tiers](#).

You can select a storage tier when you create the working environment and you can change it any time after. For details about changing the storage tier, see [Tiering inactive data to low-cost object storage](#).

The storage access tier for data tiering is system wide—it's not per volume.

## Data tiering in Google Cloud

When you enable data tiering in Google Cloud, Cloud Volumes ONTAP uses persistent disks as a performance tier for hot data and a Google Cloud Storage bucket as a capacity tier for inactive data.

### Performance tier

The performance tier can be either SSD persistent disks, balanced persistent disks, or standard persistent disks.

### Capacity tier

A Cloud Volumes ONTAP system tiers inactive data to a single Google Cloud Storage bucket.

BlueXP creates a bucket for each working environment and names it *fabric-pool-cluster unique identifier*. A different bucket is not created for each volume.

When BlueXP creates the bucket, it uses the following default settings:

- Location type: Region
- Storage class: Standard
- Public access: Subject to object ACLs
- Access control: Fine-grained
- Protection: None
- Data encryption: Google-managed key

## Storage classes

The default storage class for tiered data is the *Standard Storage* class. If the data is infrequently accessed, you can reduce your storage costs by changing to *Nearline Storage* or *Coldline Storage*. When you change the storage class, inactive data moves directly to the class that you selected.

The access costs are higher if you do access the data, so take that into consideration before you change the storage class. [Learn more about storage classes for Google Cloud Storage](#).

You can select a storage tier when you create the working environment and you can change it any time after. For details about changing the storage class, see [Tiering inactive data to low-cost object storage](#).

The storage class for data tiering is system wide—it's not per volume.



## Data tiering and capacity limits

If you enable data tiering, a system's capacity limit stays the same. The limit is spread across the performance tier and the capacity tier.

### Volume tiering policies

To enable data tiering, you must select a volume tiering policy when you create, modify, or replicate a volume. You can select a different policy for each volume.

Some tiering policies have an associated minimum cooling period, which sets the time that user data in a volume must remain inactive for the data to be considered "cold" and moved to the capacity tier. The cooling period starts when data is written to the aggregate.



You can change the minimum cooling period and default aggregate threshold of 50% (more on that below). [Learn how to change the cooling period](#) and [learn how to change the threshold](#).

BlueXP enables you to choose from the following volume tiering policies when you create or modify a volume:

#### Snapshot Only

After an aggregate has reached 50% capacity, Cloud Volumes ONTAP tiers cold user data of Snapshot copies that are not associated with the active file system to the capacity tier. The cooling period is approximately 2 days.

If read, cold data blocks on the capacity tier become hot and are moved to the performance tier.

#### All

All data (not including metadata) is immediately marked as cold and tiered to object storage as soon as possible. There is no need to wait 48 hours for new blocks in a volume to become cold. Note that blocks located in the volume prior to the All policy being set require 48 hours to become cold.

If read, cold data blocks on the cloud tier stay cold and are not written back to the performance tier. This policy is available starting with ONTAP 9.6.

#### Auto

After an aggregate has reached 50% capacity, Cloud Volumes ONTAP tiers cold data blocks in a volume to a capacity tier. The cold data includes not just Snapshot copies but also cold user data from the active file system. The cooling period is approximately 31 days.

This policy is supported starting with Cloud Volumes ONTAP 9.4.

If read by random reads, the cold data blocks in the capacity tier become hot and move to the performance tier. If read by sequential reads, such as those associated with index and antivirus scans, the cold data blocks stay cold and do not move to the performance tier.

#### None

Keeps data of a volume in the performance tier, preventing it from being moved to the capacity tier.

When you replicate a volume, you can choose whether to tier the data to object storage. If you do, BlueXP applies the **Backup** policy to the data protection volume. Starting with Cloud Volumes ONTAP 9.6, the **All** tiering policy replaces the backup policy.

## Turning off Cloud Volumes ONTAP impacts the cooling period

Data blocks are cooled by cooling scans. During this process, blocks that haven't been used have their block temperature moved (cooled) to the next lower value. The default cooling time depends on the volume tiering policy:

- Auto: 31 days
- Snapshot Only: 2 days

Cloud Volumes ONTAP must be running for the cooling scan to work. If Cloud Volumes ONTAP is turned off, cooling will stop, as well. As a result, you can experience longer cooling times.



When Cloud Volumes ONTAP is turned off, the temperature of each block is preserved until you restart the system. For example, if the temperature of a block is 5 when you turn the system off, the temp is still 5 when you turn the system back on.

## Setting up data tiering

For instructions and a list of supported configurations, see [Tiering inactive data to low-cost object storage](#).

## Storage management

BlueXP (formerly Cloud Manager) provides simplified and advanced management of Cloud Volumes ONTAP storage.



All disks and aggregates must be created and deleted directly from BlueXP. You should not perform these actions from another management tool. Doing so can impact system stability, hamper the ability to add disks in the future, and potentially generate redundant cloud provider fees.

## Storage provisioning

BlueXP makes storage provisioning for Cloud Volumes ONTAP easy by purchasing disks and managing aggregates for you. You simply need to create volumes. You can use an advanced allocation option to provision aggregates yourself, if desired.

### Simplified provisioning

Aggregates provide cloud storage to volumes. BlueXP creates aggregates for you when you launch an instance, and when you provision additional volumes.

When you create a volume, BlueXP does one of three things:

- It places the volume on an existing aggregate that has sufficient free space.
- It places the volume on an existing aggregate by purchasing more disks for that aggregate.

In the case of an aggregate in AWS that supports Elastic Volumes, BlueXP also increases the size of the disks in a RAID group. [Learn more about support for Elastic Volumes](#).

- It purchases disks for a new aggregate and places the volume on that aggregate.

BlueXP determines where to place a new volume by looking at several factors: an aggregate's maximum size, whether thin provisioning is enabled, and free space thresholds for aggregates.



The Account Admin can modify free space thresholds from the **Settings** page.

## Disk size selection for aggregates in AWS

When BlueXP creates new aggregates for Cloud Volumes ONTAP in AWS, it gradually increases the disk size in an aggregate, as the number of aggregates in the system increases. BlueXP does this to ensure that you can utilize the system's maximum capacity before it reaches the maximum number of data disks allowed by AWS.

For example, BlueXP might choose the following disk sizes:

Aggregate number	Disk size	Max aggregate capacity
1	500 GiB	3 TiB
4	1 TiB	6 TiB
6	2 TiB	12 TiB



This behavior does not apply to aggregates that support the Amazon EBS Elastic Volumes feature. Aggregates that have Elastic Volumes enabled are comprised of one or two RAID groups. Each RAID group has four identical disks that have the same capacity. [Learn more about support for Elastic Volumes.](#)

You can choose the disk size yourself by using the advanced allocation option.

### Advanced allocation

Rather than let BlueXP manage aggregates for you, you can do it yourself. [From the Advanced allocation page](#), you can create new aggregates that include a specific number of disks, add disks to an existing aggregate, and create volumes in specific aggregates.

## Capacity management

The Account Admin can choose whether BlueXP notifies you of storage capacity decisions or whether BlueXP automatically manages capacity requirements for you.

This behavior is determined by the *Capacity Management Mode* on a Connector. The Capacity Management Mode affects all Cloud Volumes ONTAP systems managed by that Connector. If you have another Connector, it can be configured differently.

### Automatic capacity management

The Capacity Management Mode is set to automatic by default. In this mode, BlueXP automatically purchases new disks for Cloud Volumes ONTAP instances when more capacity is needed, deletes unused collections of disks (aggregates), moves volumes between aggregates when needed, and attempts to unfail disks.

The following examples illustrate how this mode works:

- If an aggregate reaches the capacity threshold and it has room for more disks, BlueXP automatically purchases new disks for that aggregate so volumes can continue to grow.

BlueXP checks the free space ratio every 15 minutes to determine if it needs to purchase additional disks.

In the case of an aggregate in AWS that supports Elastic Volumes, BlueXP also increases the size of the disks in a RAID group. [Learn more about support for Elastic Volumes.](#)

- If an aggregate reaches the capacity threshold and it can't support any additional disks, BlueXP automatically moves a volume from that aggregate to an aggregate with available capacity or to a new aggregate.

If BlueXP creates a new aggregate for the volume, it chooses a disk size that accommodates the size of that volume.

Note that free space is now available on the original aggregate. Existing volumes or new volumes can use that space. The space can't be returned to the cloud provider in this scenario.

- If an aggregate contains no volumes for more than 12 hours, BlueXP deletes it.

## Management of LUNs with automatic capacity management

BlueXP's automatic capacity management doesn't apply to LUNs. When BlueXP creates a LUN, it disables the autogrow feature.

### Manual capacity management

If the Account Admin set the Capacity Management Mode to manual, BlueXP displays Action Required messages when capacity decisions must be made. The same examples described in the automatic mode apply to the manual mode, but it is up to you to accept the actions.

### Learn more

[Learn how to modify the capacity management mode.](#)

## Write speed

BlueXP enables you to choose normal or high write speed for most Cloud Volumes ONTAP configurations. 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.

### Normal write speed

When you choose normal write speed, data is written directly to disk. When data is written directly to disk, reduces the likelihood of data loss in the event of an unplanned system outage, or a cascading failure involving an unplanned system outage (HA pairs only).

Normal write speed is the default option.

### High write speed

When you choose high write speed, data is buffered in memory before it is written to disk, which provides faster write performance. Due to this caching, there is the potential for data loss if an unplanned system outage occurs.

The amount of data that can be lost in the event of an unplanned system outage is the span of the last two consistency points. A consistency point is the act of writing buffered data to disk. A consistency point occurs when the write log is full or after 10 seconds (whichever comes first). However, the performance of the storage

provided by your cloud provider can affect consistency point processing time.

### **When to use high write speed**

High write speed is a good choice if fast write performance is required for your workload and you can withstand the risk of data loss in the event of an unplanned system outage, or a cascading failure involving an unplanned system outage (HA pairs only).

### **Recommendations when using high write speed**

If you enable high write speed, you should ensure write protection at the application layer, or that the applications can tolerate data loss, if it occurs.

### **High write speed with an HA pair in AWS**

If you plan to enable high write speed on an HA pair in AWS, you should understand the difference in protection levels between a multiple Availability Zone (AZ) deployment and a single AZ deployment. Deploying an HA pair across multiple AZs provides more resiliency and can help to mitigate the chance of data loss.

[Learn more about HA pairs in AWS.](#)

### **Configurations that support high write speed**

Not all Cloud Volumes ONTAP configurations support high write speed. Those configurations use normal write speed by default.

## **AWS**

If you use a single node system, Cloud Volumes ONTAP supports high write speed with all instance types.

Starting with the 9.8 release, Cloud Volumes ONTAP supports high write speed with HA pairs when using almost all supported EC2 instance types, except for m5.xlarge and r5.xlarge.

[Learn more about the Amazon EC2 instances that Cloud Volumes ONTAP supports.](#)

## **Azure**

If you use a single node system, Cloud Volumes ONTAP supports high write speed with all VM types.

If you use an HA pair, Cloud Volumes ONTAP supports high write speed with several VM types, starting with the 9.8 release. Go to the [Cloud Volumes ONTAP Release Notes](#) to view the VM types that support high write speed.

## **Google Cloud**

If you use a single node system, Cloud Volumes ONTAP supports high write speed with all machine types.

If you use an HA pair, Cloud Volumes ONTAP supports high write speed with several VM types, starting with the 9.13.0 release. Go to the [Cloud Volumes ONTAP Release Notes](#) to view the VM types that support high write speed.

[Learn more about the Google Cloud machine types that Cloud Volumes ONTAP supports.](#)

## How to select a write speed

You can choose a write speed when you create a new working environment and you can [change the write speed for an existing system](#).

## What to expect if data loss occurs

If data loss occurs due to high write speed, the Event Management System (EMS) reports the following two events:

- Cloud Volumes ONTAP 9.12.1 or later

```
NOTICE nv.data.loss.possible: An unexpected shutdown occurred while in high write speed mode, which possibly caused a loss of data.
```

- Cloud Volumes ONTAP 9.11.0 to 9.11.1

```
DEBUG nv.check.failed: NVRAM check failed with error "NVRAM disabled due to dirty shutdown with High Write Speed mode"
```

```
ERROR wafl.root.content.changed: Contents of the root volume '' might have changed. Verify that all recent configuration changes are still in effect..
```

- Cloud Volumes ONTAP 9.8 to 9.10.1

```
DEBUG nv.check.failed: NVRAM check failed with error "NVRAM disabled due to dirty shutdown"
```

```
ERROR wafl.root.content.changed: Contents of the root volume '' might have changed. Verify that all recent configuration changes are still in effect.
```

When this happens, Cloud Volumes ONTAP should be able to boot up and continue to serve data without user intervention.

## How to stop data access if data loss occurs

If you are concerned about data loss, want the applications to stop running upon data loss, and the data access to be resumed after the data loss issue is properly addressed, you can use the NVFAIL option from the CLI to achieve that goal.

### To enable the NVFAIL option

```
vol modify -volume <vol-name> -nvfail on
```

### To check NVFAIL settings

```
vol show -volume <vol-name> -fields nvfail
```

### To disable the NVFAIL option

```
vol modify -volume <vol-name> -nvfail off
```

When data loss occurs, an NFS or iSCSI volume with NVFAIL enabled should stop serving data (there's no impact to CIFS which is a stateless protocol). For more details, refer to [How NVFAIL impacts access to NFS volumes or LUNs](#).

### To check the NVFAIL state

```
vol show -fields in-nvfailed-state
```

After the data loss issue is properly addressed, you can clear the NVFAIL state and the volume will be available for data access.

### To clear the NVFAIL state

```
vol modify -volume <vol-name> -in-nvfailed-state false
```

## Flash Cache

Some Cloud Volumes ONTAP configurations include local NVMe storage, which Cloud Volumes ONTAP uses as *Flash Cache* for better performance.

### What's Flash Cache?

Flash Cache speeds access to data through real-time intelligent caching of recently read user data and NetApp metadata. It's effective for random read-intensive workloads, including databases, email, and file services.

### Supported configurations

Flash Cache is supported with specific Cloud Volumes ONTAP configurations. View supported configurations in the [Cloud Volumes ONTAP Release Notes](#)

### Limitations

- Compression must be disabled on all volumes to take advantage of the Flash Cache performance improvements up to Cloud Volumes ONTAP 9.12.0. When you deploy or upgrade to Cloud Volumes ONTAP 9.12.1, you don't need to disable compression.

Choose no storage efficiency when creating a volume from BlueXP, or create a volume and then [disable data compression by using the CLI](#).

- Cache rewarming after a reboot is not supported with Cloud Volumes ONTAP.

## WORM storage

You can activate write once, read many (WORM) storage on a Cloud Volumes ONTAP system to retain files in unmodified form for a specified retention period. Cloud WORM

storage is powered by SnapLock technology, which means WORM files are protected at the file level.

### How WORM storage works

Once a file has been committed to WORM storage, it can't be modified, even after the retention period has expired. A tamper-proof clock determines when the retention period for a WORM file has elapsed.

After the retention period has elapsed, you are responsible for deleting any files that you no longer need.

### Activating WORM storage

How you activate WORM storage depends on the Cloud Volumes ONTAP version that you're using.

#### Version 9.10.1 and later

Starting with Cloud Volumes ONTAP 9.10.1, you have the option to enable or disable WORM at the volume level.

When you create a new Cloud Volumes ONTAP working environment, you're prompted to enable or disable WORM storage:

- If you enable WORM storage when creating a working environment, every volume that you create from BlueXP has WORM enabled. But you can use System Manager or the CLI to create volumes that have WORM disabled.
- If you disable WORM storage when creating a working environment, every volume that you create from BlueXP, System Manager, or the CLI has WORM disabled. If you want to enable WORM on a Cloud Volumes ONTAP working environment that was not enabled during creation, you must create a support ticket with NetApp support for assistance.

With either option, you should [understand how charging works](#).

#### Version 9.10.0 and earlier

You can activate WORM storage on a Cloud Volumes ONTAP system when you create a new working environment. Every volume that you create from BlueXP has WORM enabled. You can't disable WORM storage on individual volumes.

### Charging

Charging for WORM storage is hourly, according to the total provisioned capacity of WORM volumes.

You should understand the following charging behavior with Cloud Volumes ONTAP 9.10.1 and later:

- Beginning with ONTAP 9.10.1, WORM volumes and non-WORM volumes can exist on the same aggregate.
- If you enable WORM when you create a Cloud Volumes ONTAP working environment, every volume that you create from BlueXP has WORM enabled. However, you can use the ONTAP CLI or System Manager to create volumes that have WORM disabled. Those volumes are not charged at the WORM rate.
- If you don't enable WORM when you create a working environment, every volume that you create from BlueXP has WORM disabled. You are not charged at the WORM rate for those volumes.

[Learn about pricing for WORM storage](#)



## Committing files to WORM

You can use an application to commit files to WORM over NFS or CIFS, or use the ONTAP CLI to autocommit files to WORM automatically. You can also use a WORM appendable file to retain data that is written incrementally, like log information.

After you activate WORM storage on a Cloud Volumes ONTAP system, you must use the ONTAP CLI for all management of WORM storage. For instructions, refer to [ONTAP documentation](#).

## WORM and data tiering

When you create a new Cloud Volumes ONTAP 9.8 system or later, you can enable both data tiering and WORM storage together. Enabling data tiering with WORM storage allows you to tier the data to an object store in the cloud.

You should understand the following about enabling both data tiering and WORM storage:

- Data that is tiered to object storage doesn't include the ONTAP WORM functionality. To ensure end-to-end WORM capability, you'll need to set up the bucket permissions correctly.
- The data that is tiered to object storage doesn't carry the WORM functionality, which means technically anyone with full access to buckets and containers can go and delete the objects tiered by ONTAP.
- Reverting or downgrading to Cloud Volumes ONTAP 9.8 is blocked after enabling WORM and tiering.

## Limitations

- WORM storage in Cloud Volumes ONTAP operates under a "trusted storage administrator" model. While WORM files are protected from alteration or modification, volumes can be deleted by a cluster administrator even if those volumes contain unexpired WORM data.
- In addition to the trusted storage administrator model, WORM storage in Cloud Volumes ONTAP also implicitly operates under a "trusted cloud administrator" model. A cloud administrator could delete WORM data before its expiry date by removing or editing cloud storage directly from the cloud provider.

# High-availability pairs

## High-availability pairs in AWS

A Cloud Volumes ONTAP high availability (HA) configuration provides nondisruptive operations and fault tolerance. In AWS, data is synchronously mirrored between the two nodes.

## HA components

In AWS, Cloud Volumes ONTAP HA configurations include the following components:

- Two Cloud Volumes ONTAP nodes whose data is synchronously mirrored between each other.
- A mediator instance that provides a communication channel between the nodes to assist in storage takeover and giveback processes.

## Mediator

Here are some key details about the mediator instance in AWS:

## Instance type

t2-micro

## Disks

One EBS magnetic disk that is approximately 8 GiB.

## Operating system

Debian 11



For Cloud Volumes ONTAP 9.10.0 and earlier, Debian 10 was installed on the mediator.

## Upgrades

When you upgrade Cloud Volumes ONTAP, BlueXP also updates the mediator instance as needed.

## Access to the instance

When you create a Cloud Volumes ONTAP HA pair from BlueXP, you're prompted to provide a key pair for the mediator instance. You can use that key pair for SSH access using the `admin` user.

## Third-party agents

Third-party agents or VM extensions are not supported on the mediator instance.

## Storage takeover and giveback

If a node goes down, the other node can serve data for its partner to provide continued data service. Clients can access the same data from the partner node because the data was synchronously mirrored to the partner.

After the node reboots, the partner must resync data before it can return the storage. The time that it takes to resync data depends on how much data was changed while the node was down.

Storage takeover, resync, and giveback are all automatic by default. No user action is required.

## RPO and RTO

An HA configuration maintains high availability of your data as follows:

- The recovery point objective (RPO) is 0 seconds.  
Your data is transactionally consistent with no data loss.
- The recovery time objective (RTO) is 60 seconds.  
In the event of an outage, data should be available in 60 seconds or less.

## HA deployment models

You can ensure the high availability of your data by deploying an HA configuration across multiple Availability Zones (AZs) or in a single AZ. You should review more details about each configuration to choose which best fits your needs.

### Multiple Availability Zones

Deploying an HA configuration in multiple Availability Zones (AZs) ensures high availability of your data if a failure occurs with an AZ or an instance that runs a Cloud Volumes ONTAP node. You should understand how NAS IP addresses impact data access and storage failover.

## NFS and CIFS data access

When an HA configuration is spread across multiple Availability Zones, *floating IP addresses* enable NAS client access. The floating IP addresses, which must be outside of the CIDR blocks for all VPCs in the region, can migrate between nodes when failures occur. They aren't natively accessible to clients that are outside of the VPC, unless you [set up an AWS transit gateway](#).

If you can't set up a transit gateway, private IP addresses are available for NAS clients that are outside the VPC. However, these IP addresses are static—they can't failover between nodes.

You should review requirements for floating IP addresses and route tables before you deploy an HA configuration across multiple Availability Zones. You must specify the floating IP addresses when you deploy the configuration. The private IP addresses are automatically created by BlueXP.

For details, see [AWS networking requirements for Cloud Volumes ONTAP HA in multiple AZs](#).

## iSCSI data access

Cross-VPC data communication is not an issue since iSCSI does not use floating IP addresses.

## Takeover and giveback for iSCSI

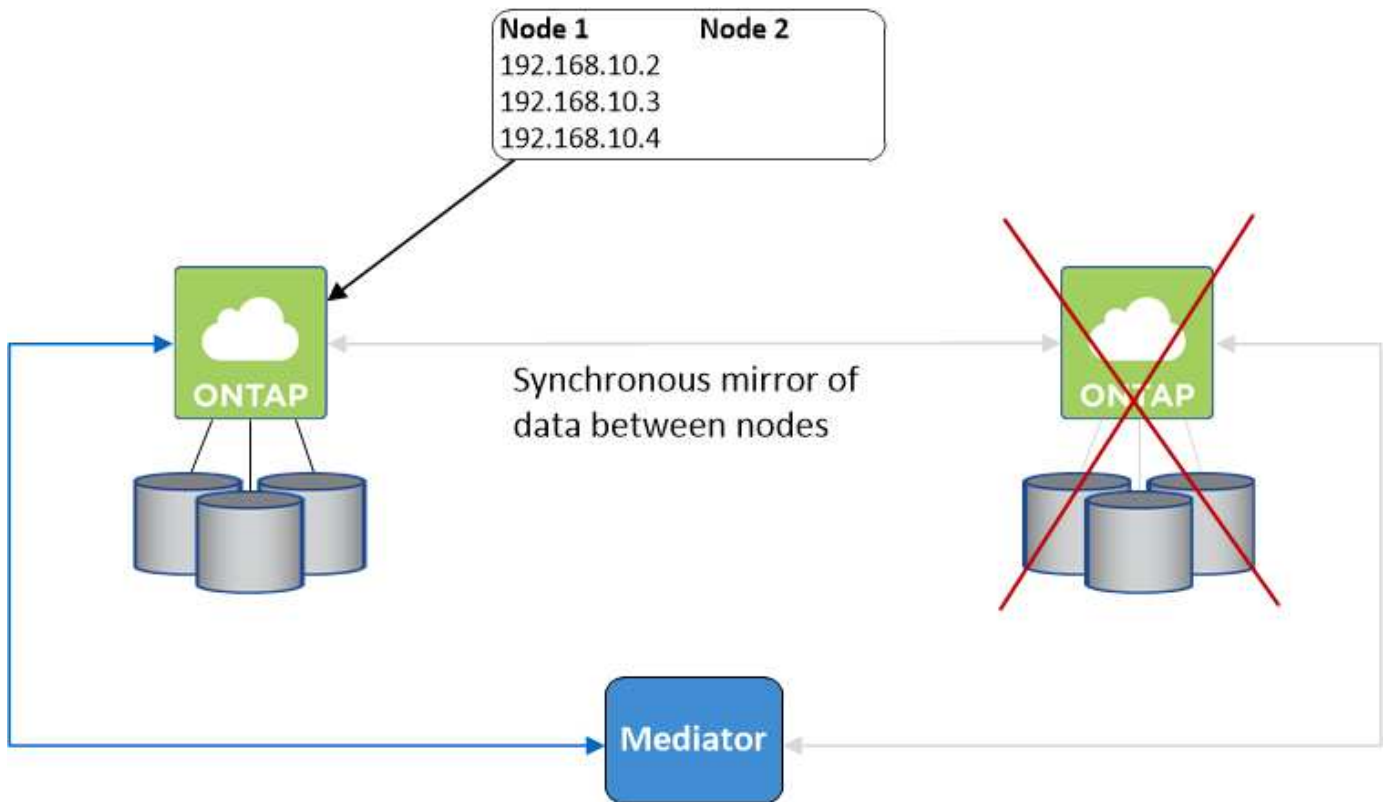
For iSCSI, Cloud Volumes ONTAP uses multipath I/O (MPIO) and Asymmetric Logical Unit Access (ALUA) to manage path failover between the active-optimized and non-optimized paths.



For information about which specific host configurations support ALUA, see the [NetApp Interoperability Matrix Tool](#) and the Host Utilities Installation and Setup Guide for your host operating system.

## Takeover and giveback for NAS

When takeover occurs in a NAS configuration using floating IPs, the node's floating IP address that clients use to access data moves to the other node. The following image depicts storage takeover in a NAS configuration using floating IPs. If node 2 goes down, the floating IP address for node 2 moves to node 1.



NAS data IPs used for external VPC access cannot migrate between nodes if failures occur. If a node goes offline, you must manually remount volumes to clients outside the VPC by using the IP address on the other node.

After the failed node comes back online, remount clients to volumes using the original IP address. This step is needed to avoid transferring unnecessary data between two HA nodes, which can cause significant performance and stability impact.

You can easily identify the correct IP address from BlueXP by selecting the volume and clicking **Mount Command**.

### Single Availability Zone

Deploying an HA configuration in a single Availability Zone (AZ) can ensure high availability of your data if an instance that runs a Cloud Volumes ONTAP node fails. All data is natively accessible from outside of the VPC.



BlueXP creates an [AWS spread placement group](#) and launches the two HA nodes in that placement group. The placement group reduces the risk of simultaneous failures by spreading the instances across distinct underlying hardware. This feature improves redundancy from a compute perspective and not from disk failure perspective.

### Data access

Because this configuration is in a single AZ, it does not require floating IP addresses. You can use the same IP address for data access from within the VPC and from outside the VPC.

The following image shows an HA configuration in a single AZ. Data is accessible from within the VPC and from outside the VPC.



### Takeover and giveback

For iSCSI, Cloud Volumes ONTAP uses multipath I/O (MPIO) and Asymmetric Logical Unit Access (ALUA) to manage path failover between the active-optimized and non-optimized paths.



For information about which specific host configurations support ALUA, see the [NetApp Interoperability Matrix Tool](#) and the Host Utilities Installation and Setup Guide for your host operating system.

For NAS configurations, the data IP addresses can migrate between HA nodes if failures occur. This ensures client access to storage.

### How storage works in an HA pair

Unlike an ONTAP cluster, storage in a Cloud Volumes ONTAP HA pair is not shared between nodes. Instead, data is synchronously mirrored between the nodes so that the data is available in the event of failure.

## Storage allocation

When you create a new volume and additional disks are required, BlueXP allocates the same number of disks to both nodes, creates a mirrored aggregate, and then creates the new volume. For example, if two disks are required for the volume, BlueXP allocates two disks per node for a total of four disks.

## Storage configurations

You can use an HA pair as an active-active configuration, in which both nodes serve data to clients, or as an active-passive configuration, in which the passive node responds to data requests only if it has taken over storage for the active node.



You can set up an active-active configuration only when using BlueXP in the Storage System View.

## Performance expectations

A Cloud Volumes ONTAP HA configuration synchronously replicates data between nodes, which consumes network bandwidth. As a result, you can expect the following performance in comparison to a single-node Cloud Volumes ONTAP configuration:

- For HA configurations that serve data from only one node, read performance is comparable to the read performance of a single-node configuration, whereas write performance is lower.
- For HA configurations that serve data from both nodes, read performance is higher than the read performance of a single-node configuration, and write performance is the same or higher.

For more details about Cloud Volumes ONTAP performance, see [Performance](#).

## Client access to storage

Clients should access NFS and CIFS volumes by using the data IP address of the node on which the volume resides. If NAS clients access a volume by using the IP address of the partner node, traffic goes between both nodes, which reduces performance.



If you move a volume between nodes in an HA pair, you should remount the volume by using the IP address of the other node. Otherwise, you can experience reduced performance. If clients support NFSv4 referrals or folder redirection for CIFS, you can enable those features on the Cloud Volumes ONTAP systems to avoid remounting the volume. For details, see ONTAP documentation.

You can easily identify the correct IP address from BlueXP:

## Volumes

2 Volumes | 0.22 TB Allocated | < 0.01 TB Used (0 TB in S3)



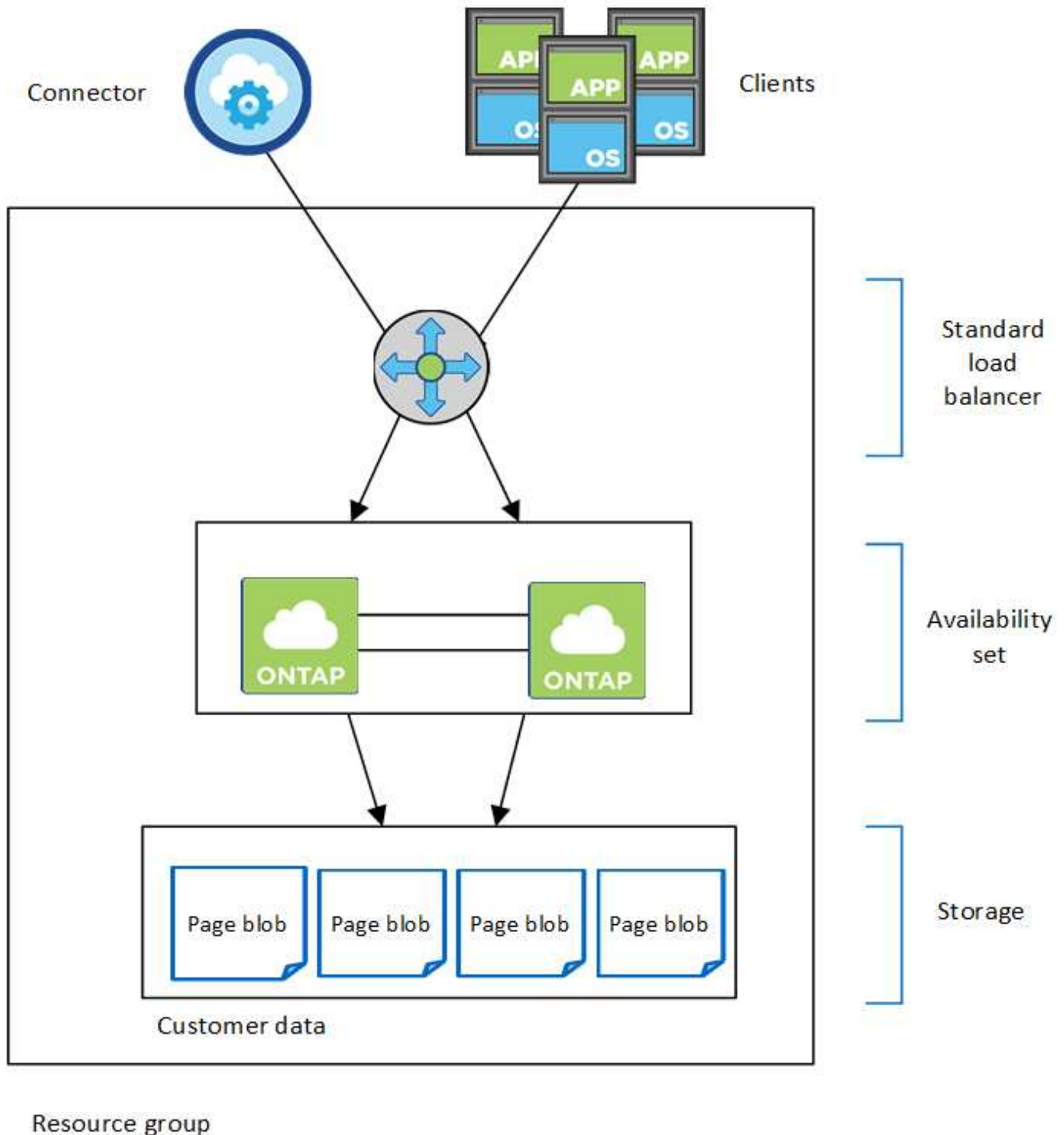
### High-availability pairs in Azure

A Cloud Volumes ONTAP high availability (HA) pair provides enterprise reliability and continuous operations in case of failures in your cloud environment. In Azure, storage is shared between the two nodes.

#### HA components

##### HA single availability zone configuration with page blobs

A Cloud Volumes ONTAP HA page blob configuration in Azure includes the following components:



Note the following about the Azure components that BlueXP deploys for you:

#### Azure Standard Load Balancer

The load balancer manages incoming traffic to the Cloud Volumes ONTAP HA pair.

#### Availability Set

The Azure Availability Set is a logical grouping of the Cloud Volumes ONTAP nodes. The Availability Set ensures that the nodes are in different fault and update domains to provide redundancy and availability.

[Learn more about Availability Sets in the Azure docs.](#)



## Disks

Customer data resides on Premium Storage page blobs. Each node has access to the other node's storage. Additional storage is also required for [boot, root, and core data](#).

## Storage accounts

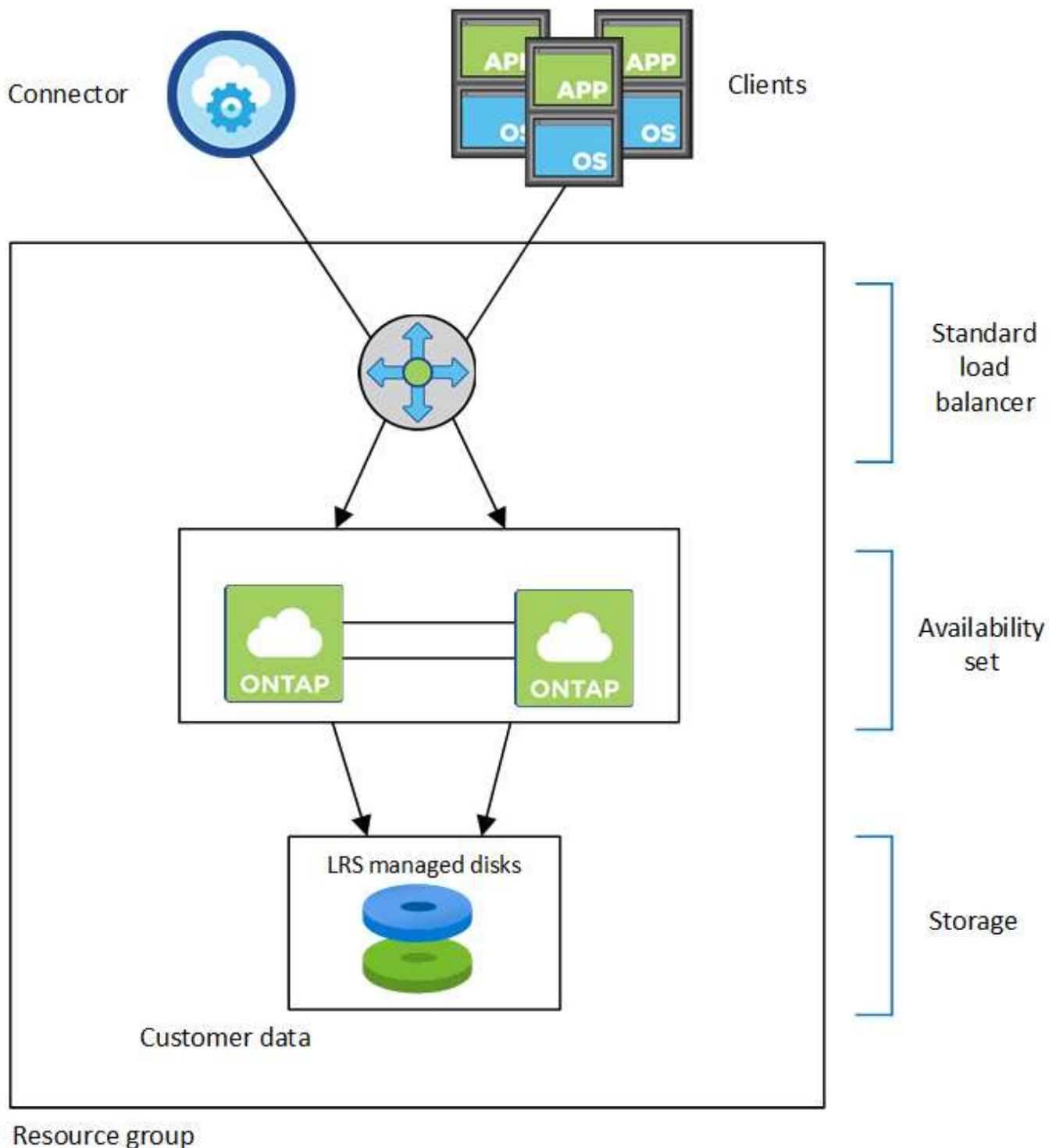
- One storage account is required for managed disks.
- One or more storage accounts are required for the Premium Storage page blobs, as the disk capacity limit per storage account is reached.

[Azure documentation: Azure Storage scalability and performance targets for storage accounts](#).

- One storage account is required for data tiering to Azure Blob storage.
- Starting with Cloud Volumes ONTAP 9.7, the storage accounts that BlueXP creates for HA pairs are general-purpose v2 storage accounts.
- You can enable an HTTPS connection from a Cloud Volumes ONTAP 9.7 HA pair to Azure storage accounts when creating a working environment. Note that enabling this option can impact write performance. You can't change the setting after you create the working environment.

## HA single availability zone configuration with shared managed disks

A Cloud Volumes ONTAP HA single availability zone configuration running on top of shared managed disk includes the following components:



Note the following about the Azure components that BlueXP deploys for you:

#### Azure Standard Load Balancer

The load balancer manages incoming traffic to the Cloud Volumes ONTAP HA pair.

#### Availability Set

The Azure Availability Set is a logical grouping of the Cloud Volumes ONTAP nodes. The Availability Set ensures that the nodes are in different fault and update domains to provide redundancy and availability.

[Learn more about Availability Sets in the Azure docs.](#)

## **Disks**

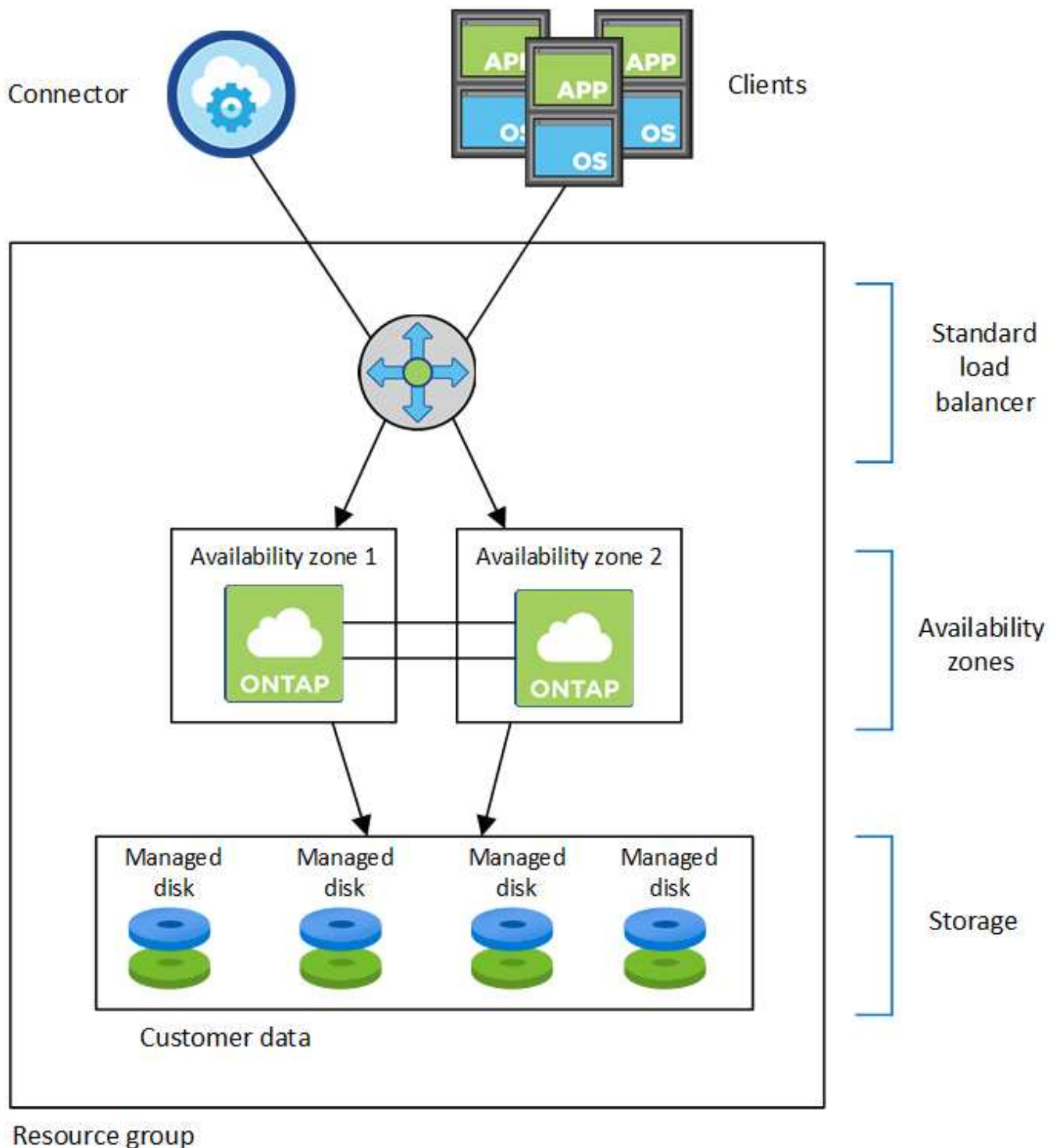
Customer data resides on locally redundant storage (LRS) managed disks. Each node has access to the other node's storage. Additional storage is also required for [boot](#), [root](#), [partner root](#), [core](#), and [NVRAM data](#).

## **Storage accounts**

Storage accounts are used for managed disk based deployments to handle diagnostic logs and tiering to blob storage.

## **HA multiple availability zone configuration**

A Cloud Volumes ONTAP HA multiple availability zone configuration in Azure includes the following components:



Note the following about the Azure components that BlueXP deploys for you:

#### Azure Standard Load Balancer

The load balancer manages incoming traffic to the Cloud Volumes ONTAP HA pair.

#### Availability Zones

Two Cloud Volumes ONTAP nodes are deployed in to different availability zones. Availability zones ensure that the nodes are in different fault domains. [Learn more about Azure zone-redundant storage for managed disks in the Azure docs.](#)

## Disks

Customer data resides on zone-redundant storage (ZRS) managed disks. Each node has access to the other node's storage. Additional storage is also required for [boot, root, partner root, and core data](#).

## Storage accounts

Storage accounts are used for managed disk based deployments to handle diagnostic logs and tiering to blob storage.

## RPO and RTO

An HA configuration maintains high availability of your data as follows:

- The recovery point objective (RPO) is 0 seconds.  
Your data is transactionally consistent with no data loss.
- The recovery time objective (RTO) is 60 seconds.  
In the event of an outage, data should be available in 60 seconds or less.

## Storage takeover and giveback

Similar to a physical ONTAP cluster, storage in an Azure HA pair is shared between nodes. Connections to the partner's storage allows each node to access the other's storage in the event of a *takeover*. Network path failover mechanisms ensure that clients and hosts continue to communicate with the surviving node. The partner *gives back* storage when the node is brought back on line.

For NAS configurations, data IP addresses automatically migrate between HA nodes if failures occur.

For iSCSI, Cloud Volumes ONTAP uses multipath I/O (MPIO) and Asymmetric Logical Unit Access (ALUA) to manage path failover between the active-optimized and non-optimized paths.



For information about which specific host configurations support ALUA, see the [NetApp Interoperability Matrix Tool](#) and the Host Utilities Installation and Setup Guide for your host operating system.

Storage takeover, resync, and giveback are all automatic by default. No user action is required.

## Storage configurations

You can use an HA pair as an active-active configuration, in which both nodes serve data to clients, or as an active-passive configuration, in which the passive node responds to data requests only if it has taken over storage for the active node.

## High-availability pairs in Google Cloud

A Cloud Volumes ONTAP high availability (HA) configuration provides nondisruptive operations and fault tolerance. In Google Cloud, data is synchronously mirrored between the two nodes.

## HA components

Cloud Volumes ONTAP HA configurations in Google Cloud include the following components:

- Two Cloud Volumes ONTAP nodes whose data is synchronously mirrored between each other.

- A mediator instance that provides a communication channel between the nodes to assist in storage takeover and giveback processes.
- One zone or three zones (recommended).

If you choose three zones, the two nodes and mediator are in separate Google Cloud zones.

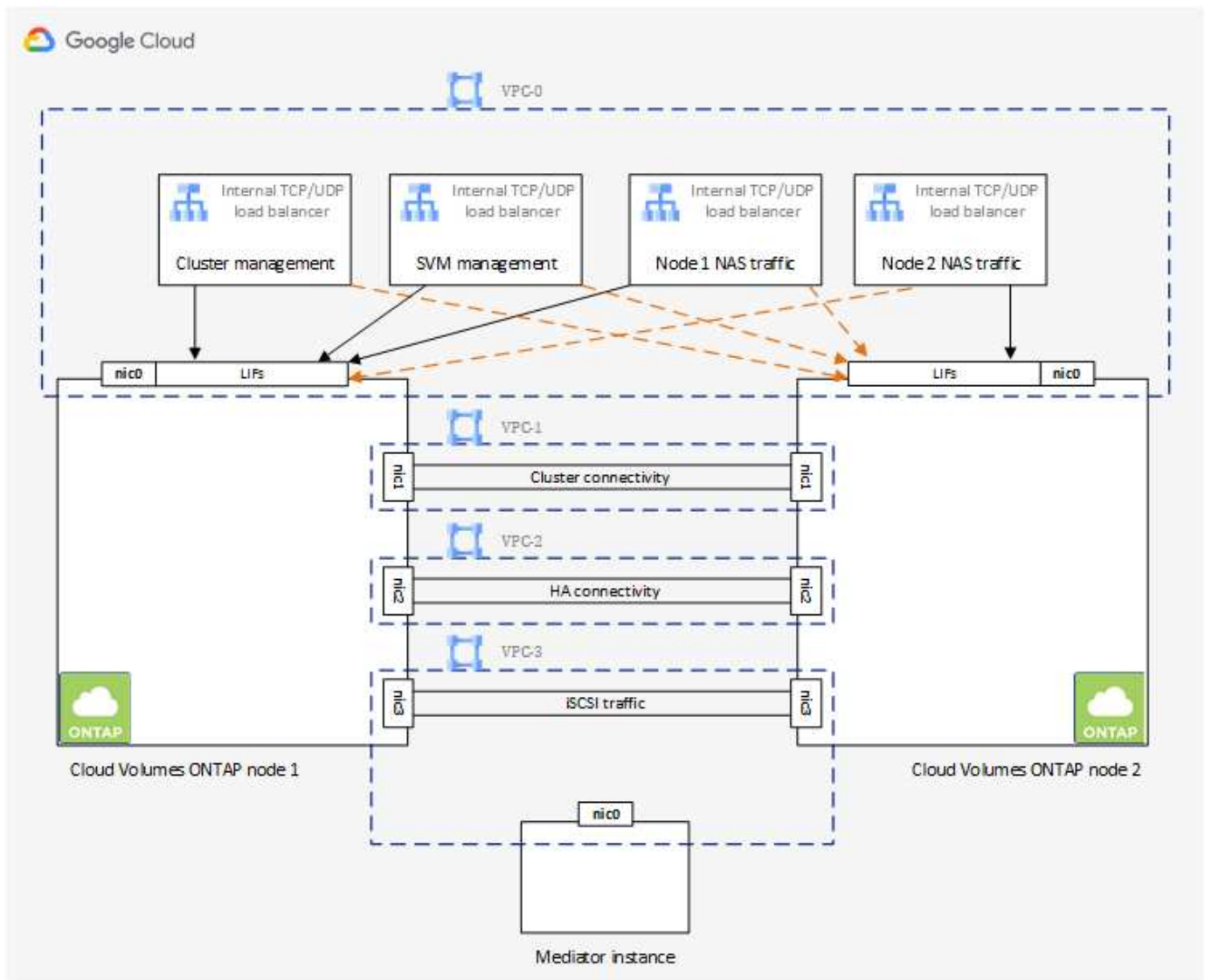
- Four Virtual Private Clouds (VPCs).

The configuration uses four VPCs because GCP requires that each network interface resides in a separate VPC network.

- Four Google Cloud internal load balancers (TCP/UDP) that manage incoming traffic to the Cloud Volumes ONTAP HA pair.

[Learn about networking requirements](#), including more details about load balancers, VPCs, internal IP addresses, subnets, and more.

The following conceptual image shows a Cloud Volumes ONTAP HA pair and its components:



## Mediator

Here are some key details about the mediator instance in Google Cloud:

### Instance type

e2-micro (an f1-micro instance was previously used)

### Disks

Two standard persistent disks that are 10 GiB each

### Operating system

Debian 11



For Cloud Volumes ONTAP 9.10.0 and earlier, Debian 10 was installed on the mediator.

### Upgrades

When you upgrade Cloud Volumes ONTAP, BlueXP also updates the mediator instance as needed.

### Access to the instance

For Debian, the default cloud user is `admin`. Google Cloud creates and adds a certificate for the `admin` user when SSH access is requested through the Google Cloud console or `gcloud` command line. You can specify `sudo` to gain root privileges.

### Third-party agents

Third-party agents or VM extensions are not supported on the mediator instance.

### Storage takeover and giveback

If a node goes down, the other node can serve data for its partner to provide continued data service. Clients can access the same data from the partner node because the data was synchronously mirrored to the partner.

After the node reboots, the partner must resync data before it can return the storage. The time that it takes to resync data depends on how much data was changed while the node was down.

Storage takeover, resync, and giveback are all automatic by default. No user action is required.

### RPO and RTO

An HA configuration maintains high availability of your data as follows:

- The recovery point objective (RPO) is 0 seconds.

Your data is transactionally consistent with no data loss.

- The recovery time objective (RTO) is 60 seconds.

In the event of an outage, data should be available in 60 seconds or less.

### HA deployment models

You can ensure the high availability of your data by deploying an HA configuration in multiple zones or in a single zone.

## 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.

## How storage works in an HA pair

Unlike an ONTAP cluster, storage in a Cloud Volumes ONTAP HA pair in GCP is not shared between nodes. Instead, data is synchronously mirrored between the nodes so that the data is available in the event of failure.

### Storage allocation

When you create a new volume and additional disks are required, BlueXP allocates the same number of disks to both nodes, creates a mirrored aggregate, and then creates the new volume. For example, if two disks are required for the volume, BlueXP allocates two disks per node for a total of four disks.

### Storage configurations

You can use an HA pair as an active-active configuration, in which both nodes serve data to clients, or as an active-passive configuration, in which the passive node responds to data requests only if it has taken over storage for the active node.

### Performance expectations for an HA configuration

A Cloud Volumes ONTAP HA configuration synchronously replicates data between nodes, which consumes network bandwidth. As a result, you can expect the following performance in comparison to a single-node Cloud Volumes ONTAP configuration:

- For HA configurations that serve data from only one node, read performance is comparable to the read performance of a single-node configuration, whereas write performance is lower.
- For HA configurations that serve data from both nodes, read performance is higher than the read performance of a single-node configuration, and write performance is the same or higher.

For more details about Cloud Volumes ONTAP performance, see [Performance](#).

### Client access to storage

Clients should access NFS and CIFS volumes by using the data IP address of the node on which the volume resides. If NAS clients access a volume by using the IP address of the partner node, traffic goes between both nodes, which reduces performance.



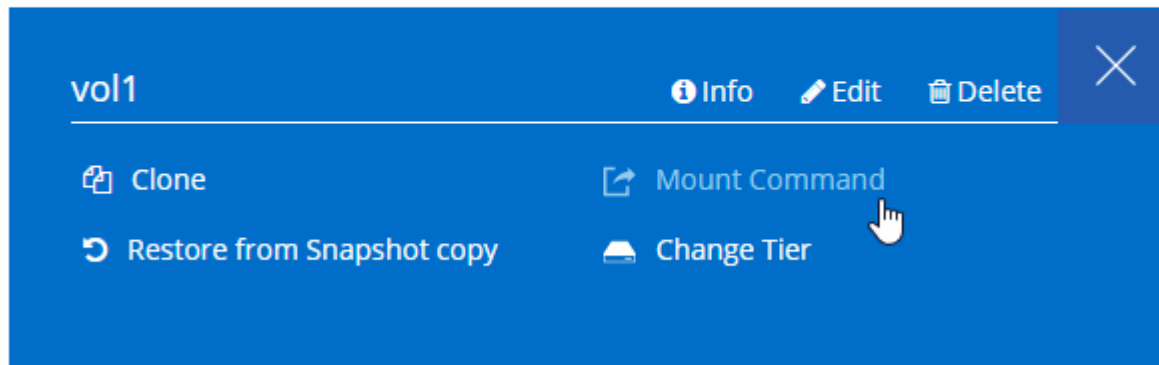
If you move a volume between nodes in an HA pair, you should remount the volume by using the IP address of the other node. Otherwise, you can experience reduced performance. If clients support NFSv4 referrals or folder redirection for CIFS, you can enable those features on the Cloud Volumes ONTAP systems to avoid remounting the volume. For details, see ONTAP documentation.



You can easily identify the correct IP address from BlueXP:

## Volumes

2 Volumes | 0.22 TB Allocated | < 0.01 TB Used (0 TB in S3)



### Related links

- [Learn about networking requirements](#)
- [Learn how to get started in GCP](#)

## Actions unavailable during takeover

When a node in an HA pair isn't available, the other node serves data for its partner to provide continued data service. This is called *storage takeover*. Several actions are unavailable until in storage giveback is complete.



When a node in an HA pair is unavailable, the state of the working environment in BlueXP is *Degraded*.

The following actions are unavailable from BlueXP storage takeover:

- Support registration
- License changes
- Instance or VM type changes
- Write speed changes
- CIFS setup
- Changing the location of configuration backups
- Setting the cluster password
- Managing disks and aggregates (advanced allocation)

These actions are available again after storage giveback completes and the state of the working environment changes back to normal.

# Security

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

## Encryption of data at rest

Cloud Volumes ONTAP supports the following encryption technologies:

- NetApp encryption solutions (NVE and NAE)
- AWS Key Management Service
- Azure Storage Service Encryption
- Google Cloud Platform default encryption

You can use NetApp encryption solutions with native encryption from your cloud provider, which encrypts data at the hypervisor level. Doing so would provide double encryption, which might be desired for very sensitive data. When the encrypted data is accessed, it's unencrypted twice—once at the hypervisor-level (using keys from the cloud provider) and then again using NetApp encryption solutions (using keys from an external key manager).

### NetApp encryption solutions (NVE and NAE)

Cloud Volumes ONTAP supports [NetApp Volume Encryption \(NVE\)](#) and [NetApp Aggregate Encryption \(NAE\)](#). NVE and NAE are software-based solutions that enable (FIPS) 140-2-compliant data-at-rest encryption of volumes. Both NVE and NAE use AES 256-bit encryption.

- NVE encrypts data at rest one volume at a time. Each data volume has its own unique encryption key.
- NAE is an extension of NVE—it encrypts data for each volume, and the volumes share a key across the aggregate. NAE also allows common blocks across all volumes in the aggregate to be deduplicated.

Both NVE and NAE are supported with an external key manager.

If you use NVE, you have the option to use your cloud provider's key vault to protect ONTAP encryption keys:

- Azure Key Vault (AKV)
- Google Cloud Key Management Service

New aggregates have NetApp Aggregate Encryption (NAE) enabled by default after you set up an external key manager. New volumes that aren't part of an NAE aggregate will have NetApp Volume Encryption (NVE) enabled by default (for example, if you have existing aggregates that were created before setting up an external key manager).

Setting up a supported key manager is the only required step. For set up instructions, refer to [Encrypting volumes with NetApp encryption solutions](#).

### AWS Key Management Service

When you launch a Cloud Volumes ONTAP system in AWS, you can enable data encryption using the [AWS Key Management Service \(KMS\)](#). BlueXP requests data keys using a customer master key (CMK).



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

If you want to use this encryption option, then you must ensure that the AWS KMS is set up appropriately. For details, see [Setting up the AWS KMS](#).

## Azure Storage Service Encryption

Data is automatically encrypted on Cloud Volumes ONTAP in Azure using [Azure Storage Service Encryption](#) with a Microsoft-managed key.

You can use your own encryption keys if you prefer. [Learn how to set up Cloud Volumes ONTAP to use a customer-managed key in Azure](#).

## Google Cloud Platform default encryption

[Google Cloud Platform data-at-rest encryption](#) is enabled by default for Cloud Volumes ONTAP. No setup is required.

While Google Cloud Storage always encrypts your data before it's written to disk, you can use BlueXP 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. [Learn more](#).

## ONTAP virus scanning

You can use integrated antivirus functionality on ONTAP systems to protect data from being compromised by viruses or other malicious code.

ONTAP virus scanning, called *Vscan*, combines best-in-class third-party antivirus software with ONTAP features that give you the flexibility you need to control which files get scanned and when.

For information about the vendors, software, and versions supported by Vscan, see the [NetApp Interoperability Matrix](#).

For information about how to configure and manage the antivirus functionality on ONTAP systems, see the [ONTAP 9 Antivirus Configuration Guide](#).

## Ransomware protection

Ransomware attacks can cost a business time, resources, and reputation. BlueXP enables you to implement the NetApp solution for ransomware, which provides effective tools for visibility, detection, and remediation.

- BlueXP identifies volumes that are not protected by a Snapshot policy and enables you to activate the default Snapshot policy on those volumes.

Snapshot copies are read-only, which prevents ransomware corruption. They can also provide the granularity to create images of a single file copy or a complete disaster recovery solution.

- BlueXP also enables you to block common ransomware file extensions by enabling ONTAP's FPolicy solution.

### Ransomware Protection

Ransomware attacks can cost a business time, resources, and reputation. The NetApp solution for ransomware provides effective tools for visibility, detection, and remediation. [Learn More](#)

#### 1 Enable Snapshot Copy Protection ⓘ



50 %  
Protection

1 Volumes without a Snapshot Policy

To protect your data, activate the default Snapshot policy for these volumes ⓘ

Activate Snapshot Policy

#### 2 Block Ransomware File Extensions ⓘ



ONTAP's native FPolicy configuration monitors and blocks file operations based on a file's extension.

View Denied File Names ⓘ

Activate FPolicy

[Learn how to implement the NetApp solution for ransomware.](#)

## Performance

You can review performance results to help you decide which workloads are appropriate for Cloud Volumes ONTAP.

### Performance technical reports

- Cloud Volumes ONTAP for AWS

[NetApp Technical Report 4383: Performance Characterization of Cloud Volumes ONTAP in Amazon Web Services with Application Workloads](#)

- Cloud Volumes ONTAP for Microsoft Azure

[NetApp Technical Report 4671: Performance Characterization of Cloud Volumes ONTAP in Azure with Application Workloads](#)

- Cloud Volumes ONTAP for Google Cloud

[NetApp Technical Report 4816: Performance Characterization of Cloud Volumes ONTAP for Google Cloud](#)

### CPU performance

Cloud Volumes ONTAP nodes show as highly utilized (over 90%) from your cloud provider's monitoring tools. This is because ONTAP reserves all vCPUs presented to the virtual machine so that they are available when needed.

For help, see the [NetApp knowledgebase article about how to monitor ONTAP CPU utilization using the CLI](#)

## License management for node-based BYOL

Each Cloud Volumes ONTAP system that has a node-based BYOL must have a system license installed with an active subscription. BlueXP simplifies the process by managing

licenses for you and by displaying a warning before they expire.



A node-based license is the previous generation BYOL for Cloud Volumes ONTAP. A node-based license is available for license renewals only.

[Learn more about Cloud Volumes ONTAP licensing options.](#)

## BYOL system licenses

A node-based license provides up to 368 TiB of capacity for a single node or HA pair.

You can purchase multiple licenses for a Cloud Volumes ONTAP BYOL system to allocate more than 368 TiB of capacity. For example, you might purchase two licenses to allocate up to 736 TiB of capacity to Cloud Volumes ONTAP. Or you could purchase four licenses to get up to 1.4 PiB.

The number of licenses that you can purchase for a single node system or HA pair is unlimited.



Some on-premises ONTAP storage systems that you purchased may have included a free Cloud Volumes ONTAP license. You can use the license to create a new Cloud Volumes ONTAP system, or you can apply the license to an existing Cloud Volumes ONTAP system to expand the capacity. [See if you have any available licenses to use.](#)

Be aware that disk limits can prevent you from reaching the capacity limit by using disks alone. You can go beyond the disk limit by [tiering inactive data to object storage](#). For information about disk limits, refer to [storage limits in the Cloud Volumes ONTAP Release Notes](#).

## License management for a new system

When you create a node-based BYOL system, BlueXP prompts you for the serial number of your license and your NetApp Support Site account. BlueXP uses the account to download the license file from NetApp and to install it on the Cloud Volumes ONTAP system.

[Learn how to add NetApp Support Site accounts to BlueXP.](#)

If BlueXP can't access the license file over the secure internet connection, you can [obtain the file yourself and then manually upload the file to BlueXP](#).

## License expiration

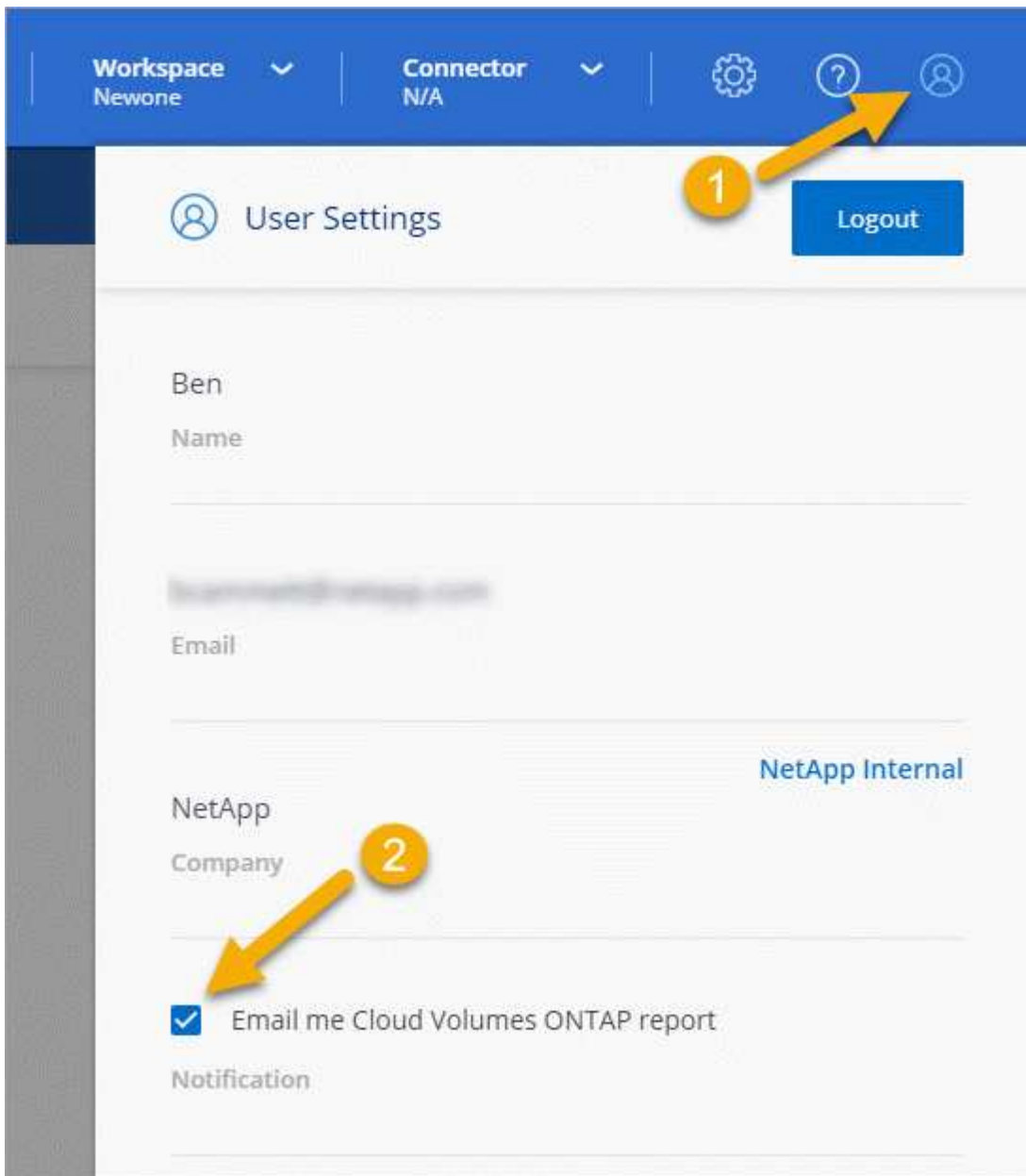
BlueXP displays a warning 30 days before a node-based license is due to expire and again when the license expires. The following image shows a 30-day expiration warning that appears in the user interface:



You can select the working environment to review the message.

BlueXP includes a license expiration warning in the Cloud Volumes ONTAP report that's emailed to you, if you

are an Account Admin and you enabled the option:



The emailed report includes the license expiration warning every 2 weeks.

If you don't renew the license in time, the Cloud Volumes ONTAP system shuts itself down. If you restart it, it shuts itself down again.

## License renewal

When you renew a node-based BYOL subscription by contacting a NetApp representative, BlueXP automatically obtains the new license from NetApp and installs it on the Cloud Volumes ONTAP system.

If BlueXP can't access the license file over the secure internet connection, you can [obtain the file yourself and then manually upload the file to BlueXP](#).

## License transfer to a new system

A node-based BYOL license is transferable between Cloud Volumes ONTAP systems when you delete an existing system and then create a new one using the same license.

For example, you might want to delete an existing licensed system and then use the license with a new BYOL system in a different VPC/VNet or cloud provider. Note that only *cloud-agnostic* serial numbers work in any cloud provider. Cloud-agnostic serial numbers start with the *908xxxx* prefix.

It's important to note that your BYOL license is tied to your company and a specific set of NetApp Support Site credentials.

## AutoSupport and Active IQ Digital Advisor

The AutoSupport component of ONTAP collects telemetry and sends it for analysis. Active IQ Digital Advisor analyzes the data from AutoSupport and provides proactive care and optimization. Using artificial intelligence, Active IQ can identify potential problems and help you resolve them before they impact your business.

Active IQ enables you to optimize your data infrastructure across your global hybrid cloud by delivering actionable predictive analytics and proactive support through a cloud-based portal and mobile app. Data-driven insights and recommendations from Active IQ are available to all NetApp customers with an active SupportEdge contract (features vary by product and support tier).

Here are some things you can do with Active IQ:

- Plan upgrades.

Active IQ identifies issues in your environment that can be resolved by upgrading to a newer version of ONTAP and the Upgrade Advisor component helps you plan for a successful upgrade.

- View system wellness.

Your Active IQ dashboard reports any issues with wellness and helps you correct those issues. Monitor system capacity to make sure you never run out of storage space. View support cases for your system.

- Manage performance.

Active IQ shows system performance over a longer period than you can see in ONTAP System Manager. Identify configuration and system issues that are impacting your performance. Maximize efficiency. View storage efficiency metrics and identify ways to store more data in less space.

- View inventory and configuration.

Active IQ displays complete inventory and software and hardware configuration information. See when service contracts are expiring and renew them to ensure you remain supported.

### Related information

- [NetApp Documentation: Active IQ Digital Advisor](#)
- [Launch Active IQ](#)
- [SupportEdge Services](#)

# Default configuration for Cloud Volumes ONTAP

Understanding how Cloud Volumes ONTAP is configured by default can help you set up and administer your systems, especially if you are familiar with ONTAP because the default setup for Cloud Volumes ONTAP is different than ONTAP.

## Default setup

- BlueXP creates one data-serving storage VM when it deploys Cloud Volumes ONTAP. Some configurations support additional storage VMs. [Learn more about managing storage VMs.](#)

Starting with the BlueXP 3.9.5 release, logical space reporting is enabled on the initial storage VM. When space is reported logically, ONTAP reports the volume space such that all the physical space saved by the storage efficiency features are also reported as used.

- BlueXP automatically installs the following ONTAP feature licenses on Cloud Volumes ONTAP:
  - CIFS
  - FlexCache
  - FlexClone
  - iSCSI
  - Multi-tenant Encryption Key Management (MTEKM), starting with Cloud Volumes ONTAP 9.12.1 GA
  - NetApp Volume Encryption (only for BYOL or registered PAYGO systems)
  - NFS
  - ONTAP S3

Starting with Cloud Volumes ONTAP 9.11.0 in AWS

Starting with Cloud Volumes ONTAP 9.9.1 in Azure

- SnapMirror
- SnapRestore
- SnapVault
- Several network interfaces are created by default:
  - A cluster management LIF
  - An intercluster LIF
  - An SVM management LIF on HA systems in Azure
  - An SVM management LIF on HA systems in Google Cloud
  - An SVM management LIF on single node systems in AWS
  - A node management LIF

In Google Cloud, this LIF is combined with the intercluster LIF.

- An iSCSI data LIF
- A CIFS and NFS data LIF






LIF failover is disabled by default for Cloud Volumes ONTAP due to cloud provider requirements. Migrating a LIF to a different port breaks the external mapping between IP addresses and network interfaces on the instance, making the LIF inaccessible.

- Cloud Volumes ONTAP sends configuration backups to the Connector using HTTPS.

The backups are accessible from <https://ipaddress/occm/offboxconfig/> where *ipaddress* is the IP address of the Connector host.

- BlueXP sets a few volume attributes differently than other management tools (System Manager or the CLI, for example).

The following table lists the volume attributes that BlueXP sets differently from the defaults:

Attribute	Value set by BlueXP
Autosize mode	grow
Maximum autosize	1,000 percent  The Account Admin can modify this value from the Settings page.
Security style	NTFS for CIFS volumes UNIX for NFS volumes
Space guarantee style	none
UNIX permissions (NFS only)	777

See the [ONTAP \*volume create\* man page](#) for information about these attributes.

## Internal disks for system data

In addition to the storage for user data, BlueXP also purchases cloud storage for system data.

### AWS

- Three disks per node for boot, root, and core data:
  - 45 GiB io1 disk for boot data
  - 140 GiB gp3 disk for root data
  - 540 GiB gp2 disk for core data
- One EBS snapshot for each boot disk and root disk
- For HA pairs, one EBS volume for the Mediator instance, which is approximately 8 GiB
- When you enable data encryption in AWS using the Key Management Service (KMS), the boot and root disks for Cloud Volumes ONTAP are encrypted, as well. This includes the boot disk for the mediator instance in an HA pair. The disks are encrypted using the CMK that you select when you create the working environment.



In AWS, NVRAM is on the boot disk.

### **Azure (single node)**

- Three Premium SSD disks:
  - One 10 GiB disk for boot data
  - One 140 GiB disk for root data
  - One 512 GiB disk for NVRAM

If the virtual machine that you chose for Cloud Volumes ONTAP supports Ultra SSDs, then the system uses a 32 GiB Ultra SSD for NVRAM, rather than a Premium SSD.

- One 1024 GiB Standard HDD disk for saving cores
- One Azure snapshot for each boot disk and root disk
- Every disk by default in Azure is encrypted at rest.

### **Azure (HA pair)**

#### **HA pairs with page blob**

- Two 10 GiB Premium SSD disks for the boot volume (one per node)
- Two 140 GiB Premium Storage page blobs for the root volume (one per node)
- Two 1024 GiB Standard HDD disks for saving cores (one per node)
- Two 512 GiB Premium SSD disks for NVRAM (one per node)
- One Azure snapshot for each boot disk and root disk
- Every disk by default in Azure is encrypted at rest.

#### **HA pairs in multiple availability zones**

- Two 10 GiB Premium SSD disks for the boot volume (one per node)
- Two 512 GiB Premium Storage page blobs for the root volume (one per node)
- Two 1024 GiB Standard HDD disks for saving cores (one per node)
- Two 512 GiB Premium SSD disks for NVRAM (one per node)
- One Azure snapshot for each boot disk and root disk
- Every disk by default in Azure is encrypted at rest.

### **Google Cloud (single node)**

- One 10 GiB SSD persistent disk for boot data
- One 64 GiB SSD persistent disk for root data
- One 500 GiB SSD persistent disk for NVRAM
- One 315 GiB Standard persistent disk for saving cores
- Snapshots for boot and root data
- Boot and root disks are encrypted by default.

## Google Cloud (HA pair)

- Two 10 GiB SSD persistent disks for boot data
- Four 64 GiB SSD persistent disk for root data
- Two 500 GiB SSD persistent disk for NVRAM
- Two 315 GiB Standard persistent disk for saving cores
- One 10 GiB Standard persistent disk for mediator data
- One 10 GiB Standard persistent disk for mediator boot data
- Snapshots for boot and root data
- Boot and root disks are encrypted by default.

## Where the disks reside

BlueXP lays out the storage as follows:

- Boot data resides on a disk attached to the instance or virtual machine.

This disk, which contains the boot image, is not available to Cloud Volumes ONTAP.

- Root data, which contains the system configuration and logs, resides in aggr0.
- The storage virtual machine (SVM) root volume resides in aggr1.
- Data volumes also reside in aggr1.

# Knowledge and support

## Register for support

Before you can open a support case with NetApp technical support, you need to add a NetApp Support Site (NSS) account to BlueXP and then register for support.

### Support for cloud provider solutions

For technical support on the following cloud provider solutions you've integrated into BlueXP, refer to "Getting help" in the BlueXP documentation for that product.

- [Amazon FSx for ONTAP](#)
- [Azure NetApp Files](#)
- [Cloud Volumes Service for Google Cloud](#)

### Support registration overview

There are two forms of registration to activate support entitlement:

- Registering your BlueXP account ID support subscription (your 20 digit 960xxxxxxx serial number located on the Support Resources page in BlueXP).

This serves as your single support subscription ID for any service within BlueXP. Each BlueXP account-level support subscription must be registered.

- Registering the Cloud Volumes ONTAP serial numbers associated with a subscription in your cloud provider's marketplace (these are 20 digit 909201xxxxxxx serial numbers).

These serial numbers are commonly referred to as *PAYGO serial numbers* and get generated by BlueXP at the time of Cloud Volumes ONTAP deployment.

Registering both types of serial numbers enables capabilities like opening support tickets and automatic case generation.

How you register depends on whether you're a new or existing customer or partner.

- Existing customer or partner

As an existing NetApp customer or partner, you can use your NetApp Support Site (NSS) SSO account to perform these registrations above. In the Support Dashboard, BlueXP provides an **NSS Management** page where you can add your NSS account. Once you add your NSS account, BlueXP automatically registers these serial numbers for you.

[Learn how to add your NSS account.](#)

- New to NetApp

If you're brand new to NetApp, you must complete a one-time registration of your BlueXP account ID serial number on NetApp's support registration site. Once you complete this registration and create a new NSS account, you can use this account in BlueXP to auto register going forward.

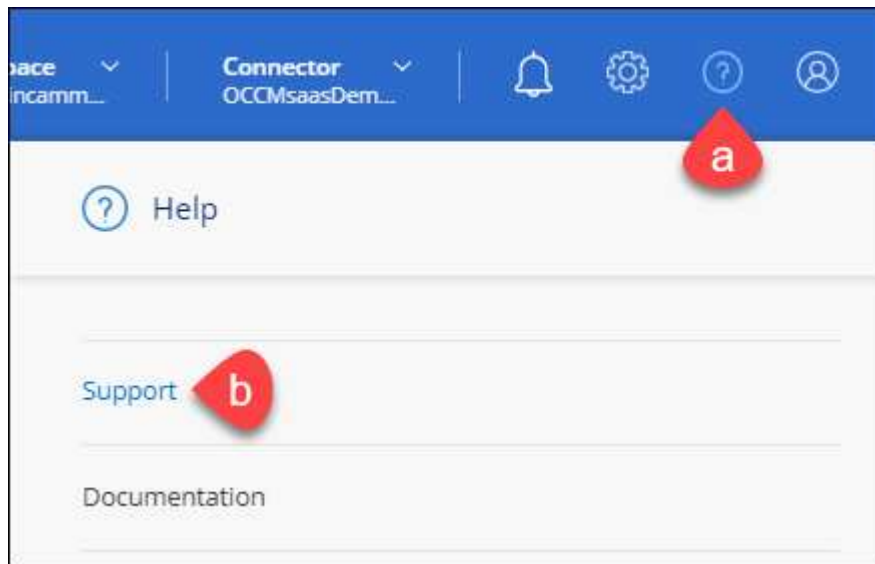
## Add an NSS account to BlueXP

The Support Dashboard enables you to add and manage your NetApp Support Site accounts for use with BlueXP.

- If you have a customer-level account, you can add one or more NSS accounts.
- If you have a partner or reseller account, you can add one or more NSS accounts, but they can't be added alongside customer-level accounts.

### Steps

1. In the upper right of the BlueXP console, click the Help icon, and select **Support**.



2. Click **NSS Management > Add NSS Account**.
3. When you're prompted, click **Continue** to be redirected to a Microsoft login page.

NetApp uses Microsoft Azure Active Directory as the identity provider for authentication services specific to support and licensing.

4. At the login page, provide your NetApp Support Site registered email address and password to perform the authentication process.

These actions enable BlueXP to use your NSS account for things like license downloads, software upgrade verification, and future support registrations.

Note the following:

- The NSS account must be a customer-level account (not a guest or temp account). You can have multiple customer-level NSS accounts.
- There can be only one NSS account if that account is a partner-level account. If you try to add customer-level NSS accounts and a partner-level account exists, you'll get the following error message:

"The NSS customer type is not allowed for this account as there are already NSS Users of different type."

The same is true if you have pre-existing customer-level NSS accounts and try to add a partner-level account.

- Upon successful login, NetApp will store the NSS user name.

This is a system-generated ID that maps to your email. On the **NSS Management** page, you can display your email from the **...** menu.

- If you ever need to refresh your login credential tokens, there is also an **Update Credentials** option in the **...** menu.

Using this option prompts you to log in again. Note that the token for these accounts expire after 90 days. A notification will be posted to alert you of this.

## Register with NetApp

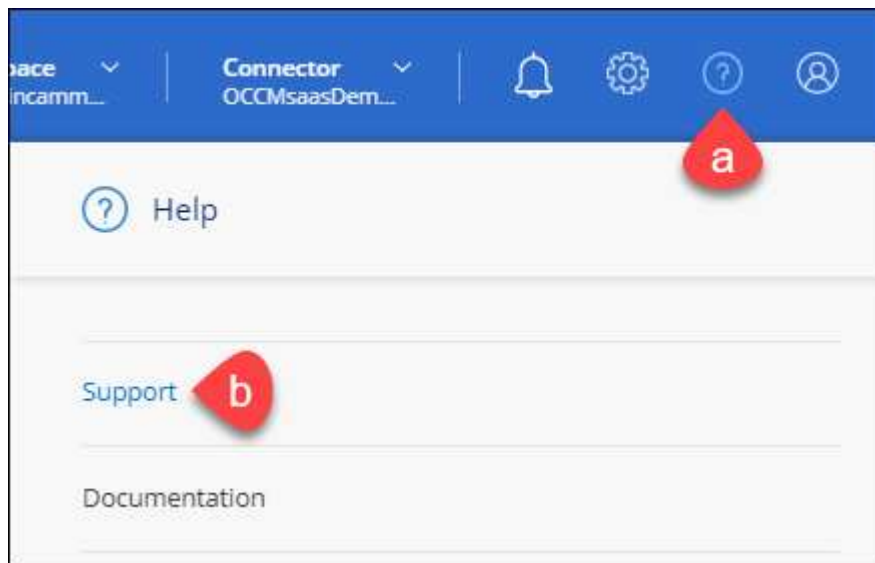
How you register for NetApp support depends on whether you already have a NetApp Support Site (NSS) account.

### Existing customer with an NSS account

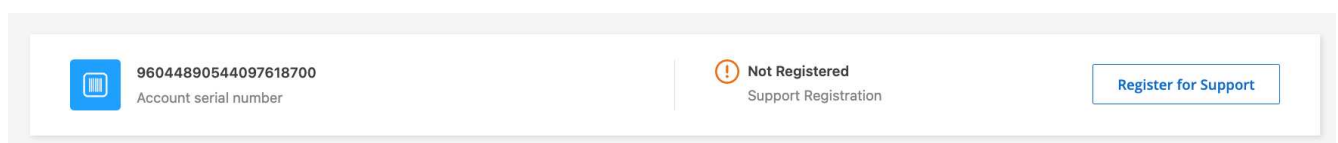
If you're a NetApp customer with an NSS account, you simply need to register for support through BlueXP.

#### Steps

1. In the upper right of the BlueXP console, click the Help icon, and select **Support**.



2. If you haven't already done so, add your NSS account to BlueXP.
3. On the **Resources** page, click **Register for Support**.



## Existing customer but no NSS account

If you're an existing NetApp customer with existing licenses and serial numbers but *no* NSS account, you just need to create an NSS account.

### Steps

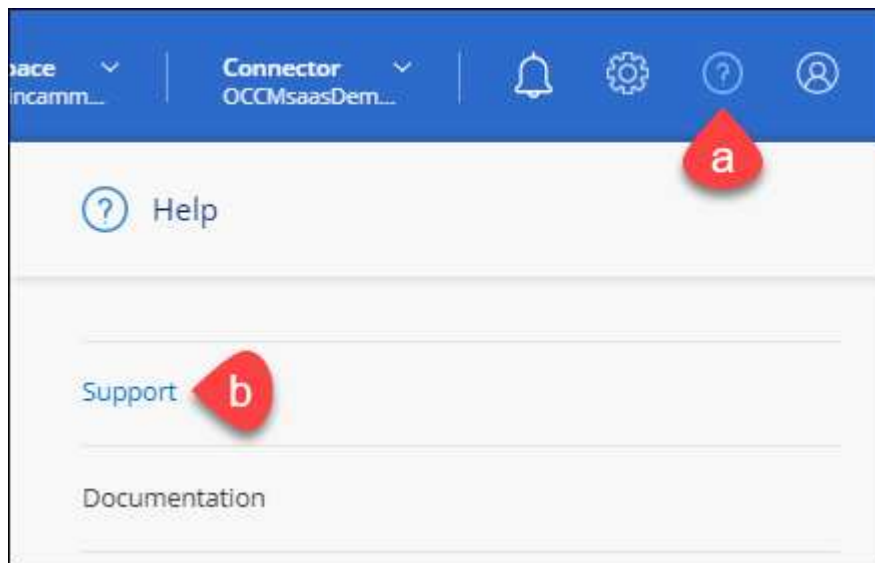
1. Create a NetApp Support Site account by completing the [NetApp Support Site User Registration form](#)
  - a. Be sure to select the appropriate User Level, which is typically **NetApp Customer/End User**.
  - b. Be sure to copy the BlueXP account serial number (960xxxx) used above for the serial number field. This will speed up the account processing.

## Brand new to NetApp

If you are brand new to NetApp and you don't have an NSS account, follow each step below.

### Steps

1. In the upper right of the BlueXP console, click the Help icon, and select **Support**.



2. Locate your account ID serial number from the Support Registration page.



3. Navigate to [NetApp's support registration site](#) and select **I am not a registered NetApp Customer**.
4. Fill out the mandatory fields (those with red asterisks).
5. In the **Product Line** field, select **Cloud Manager** and then select your applicable billing provider.
6. Copy your account serial number from step 2 above, complete the security check, and then confirm that you read NetApp's Global Data Privacy Policy.

An email is immediately sent to the mailbox provided to finalize this secure transaction. Be sure to check your spam folders if the validation email doesn't arrive in few minutes.

7. Confirm the action from within the email.

Confirming submits your request to NetApp and recommends that you create a NetApp Support Site account.

8. Create a NetApp Support Site account by completing the [NetApp Support Site User Registration form](#)
  - a. Be sure to select the appropriate User Level, which is typically **NetApp Customer/End User**.
  - b. Be sure to copy the account serial number (960xxxx) used above for the serial number field. This will speed up the account processing.

#### After you finish

NetApp should reach out to you during this process. This is a one-time onboarding exercise for new users.

Once you have your NetApp Support Site account, you can navigate to BlueXP to add this NSS account for future registrations.

## Get help

NetApp provides support for BlueXP and its cloud services in a variety of ways. Extensive free self-support options are available 24x7, such as knowledgebase (KB) articles and a community forum. Your support registration includes remote technical support via web ticketing.

### Use self-support options

These options are available for free, 24 hours a day, 7 days a week:

- [Knowledge base](#)

Search through the BlueXP knowledge base to find helpful articles to troubleshoot issues.

- [Communities](#)

Join the BlueXP community to follow ongoing discussions or create new ones.

- Documentation

The BlueXP documentation that you're currently viewing.

- [Feedback email](#)

We value your input. Submit feedback to help us improve BlueXP.

### Create a case with NetApp support

In addition to the self-support options above, you can work with a NetApp Support specialist to resolve any issues after you activate support.

#### Before you get started

To use the **Create a Case** capability, you must first perform a one-time registration of your BlueXP Account ID serial number (ie. 960xxxx) with NetApp. [Learn how to register for support.](#)

#### Steps

1. In BlueXP, click **Help > Support**.



2. On the **Resources** page, choose one of the available options under Technical Support:

- a. Click **Call Us** if you'd like to speak with someone on the phone. You'll be directed to a page on netapp.com that lists the phone numbers that you can call.
- b. Click **Create a Case** to open a ticket with a NetApp Support specialist:

- **NetApp Support Site Account:** Select the applicable NSS account associated with the person opening the support case. This person will be the primary contact for NetApp to reach out to, in addition to the additional emails provided below.

If you don't see your NSS account, you can navigate to the **NSS Management** tab within Support section of BlueXP to add it there.

- **Service:** Select the service that the issue is associated with. For example, BlueXP when specific to a technical support issue with workflows or functionality within the service.
- **Working Environment:** If applicable to storage, select **Cloud Volumes ONTAP** or **On-Prem** and then the associated working environment.


The list of working environments are within scope of the BlueXP account, workspace, and Connector you have selected in the top banner of the service.

- **Case Priority:** Choose the priority for the case, which can be Low, Medium, High, or Critical.

To learn more details about these priorities, hover your mouse over the information icon next to the field name.


- **Issue Description:** Provide a detailed description of your problem, including any applicable error messages or troubleshooting steps that you performed.
- **Additional Email Addresses:** Enter additional email addresses if you'd like to make someone else aware of this issue.

Create a Case


TESTCLOUD2NTAP 


NetApp Support Site Account


Service

Cloud Manager 

Working Environment


Select... 

Case Priority 

Low- General Guidance 


Issue Description

Provide a detailed description of your problem, including any applicable error messages or troubleshooting steps that you performed.

Additional Email Addresses (Optional) 

Attachment (Optional) Coming Soon

No files selected



### After you finish

A pop-up will appear with your support case number. A NetApp Support specialist will review your case and get back to you soon.

For a history of your support cases, you can click **Settings > Timeline** and look for actions named "create support case." A button to the far right lets you expand the action to see details.

It's possible that you might encounter the following error message when trying to create a case:

"You are not authorized to Create a Case against the selected service"

This error could mean that the NSS account and the company of record it's associated with is not the same company of record for the BlueXP account serial number (ie. 960xxxx) or the working environment serial number. You can check your list of NSS accounts at the top of the **Create a Case** form to find the right match, or you can seek assistance using one of the following options:

- Use the in-product chat
- Submit a non-technical case at <https://mysupport.netapp.com/site/help>

## Manage your support cases (Preview)

You can view and manage active and resolved support cases directly from BlueXP. You can manage the cases associated with your NSS account and with your company.

Case management is available as a Preview. We plan to refine this experience and add enhancements in upcoming releases. Please send us feedback by using the in-product chat.

Note the following:

- The case management dashboard at the top of the page offers two views:
  - The view on the left shows the total cases opened in the past 3 months by the user NSS account you provided.
  - The view on the right shows the total cases opened in the past 3 months at your company level based on your user NSS account.

The results in the table reflect the cases related to the view that you selected.

- You can add or remove columns of interest and you can filter the contents of columns like Priority and Status. Other columns provide just sorting capabilities.

View the steps below for more details.

- At a per-case level, we offer the ability to update case notes or close a case that is not already in Closed or Pending Closed status.

### Steps

1. In BlueXP, click **Help > Support**.
2. Click **Case Management** and if you're prompted, add your NSS account to BlueXP.

The **Case management** page shows open cases related to the NSS account that is associated with your BlueXP user account. This is the same NSS account that appears at the top of the **NSS management** page.

3. Optionally modify the information that displays in the table:
  - Under **Organization's cases**, click **View** to view all cases associated with your company.
  - Modify the date range by choosing an exact date range or by choosing a different time frame.

Search icon | Cases opened on the last 3 months | Create a case

Date created	Last updated		Status (5)	
December 22, 2022	December 29, 2022	Last 7 days	Assigned	...
December 21, 2022	December 28, 2022	Last 30 days	Active	...
December 15, 2022	December 27, 2022	Last 3 months	Pending customer	...
December 14, 2022	December 26, 2022	Medium (P3)	Solution proposed	...
		Low (P4)		


Apply | Reset

- Filter the contents of the columns.

Search icon | Cases opened on the last 3 months | Create a case

Last updated	Priority	Status (5)	
December 29, 2022	Critical (P1)	Active	...
December 28, 2022	High (P2)	Pending customer	...
December 27, 2022	Medium (P3)	Solution proposed	...
December 26, 2022	Low (P4)	Pending closed	...
		Closed	...

Apply | Reset

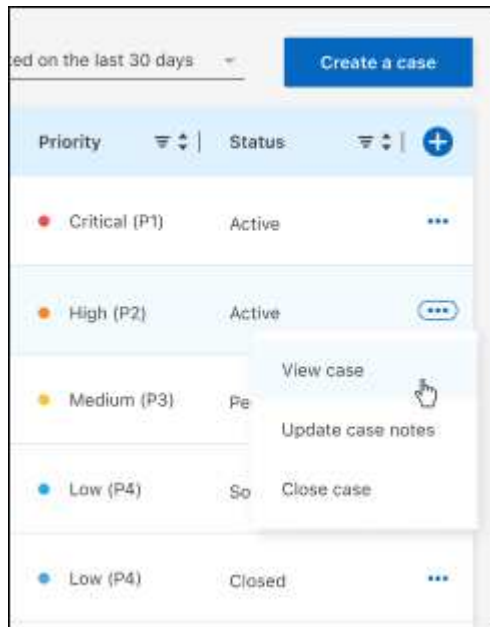
- Change the columns that appear in the table by clicking  and then choosing the columns that you'd like to display.

Search icon | Cases opened on the last 3 months | Create a case

Last updated	Priority	Status (5)	
December 29, 2022	Critical (P1)	Last updated	...
December 28, 2022	High (P2)	Priority	...
December 27, 2022	Medium (P3)	Cluster name	...
December 26, 2022	Low (P4)	Case owner	...
		Opened by	...

Apply | Reset

4. Manage an existing case by clicking ... and selecting one of the available options:
- **View case:** View full details about a specific case.
  - **Update case notes:** Provide additional details about your problem.
  - **Close case:** Provide details about why you're closing the case and click **Close case**.



# Legal notices

Legal notices provide access to copyright statements, trademarks, patents, and more.

## Copyright

<http://www.netapp.com/us/legal/copyright.aspx>

## Trademarks

NETAPP, the NETAPP logo, and the marks listed on the NetApp Trademarks page are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.

<http://www.netapp.com/us/legal/netapptmlist.aspx>

## Patents

A current list of NetApp owned patents can be found at:

<https://www.netapp.com/us/media/patents-page.pdf>

## Privacy policy

<https://www.netapp.com/us/legal/privacypolicy/index.aspx>

## Open source

Notice files provide information about third-party copyright and licenses used in NetApp software.

- [Notice for BlueXP](#)
- [Notices for the Cloud Volumes ONTAP mediator](#)
- [Notice for ONTAP](#)

## Copyright information

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

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

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

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

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

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

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

## Trademark information

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