



Cloud Volumes ONTAP documentation

Cloud Volumes ONTAP

NetApp
August 10, 2022

This PDF was generated from <https://docs.netapp.com/us-en/cloud-manager-cloud-volumes-ontap/gcp/index.html> on August 10, 2022. 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	13
Cloud Volumes ONTAP Release Notes	13
Get started	14
Learn about Cloud Volumes ONTAP	14
Get started in Google Cloud	15
Use Cloud Volumes ONTAP	54
License management	54
Volume and LUN administration	65
Aggregate administration	86
Storage VM administration	88
Security and data encryption	95
System administration	98
System health and events	115
Concepts	116
Cloud Volumes ONTAP licensing	116
Storage	121
High-availability pairs	132
Security	137
Performance	138
License management for node-based BYOL	139
AutoSupport and Active IQ Digital Advisor	142
Default configuration for Cloud Volumes ONTAP	142
Knowledge and support	146
Register for support	146
Get help	147
Legal notices	149
Copyright	149
Trademarks	149
Patents	149
Privacy policy	149
Open source	149

Cloud Volumes ONTAP documentation

Release notes

What's new

Learn what's new with Cloud Volumes ONTAP management in Cloud Manager.

The enhancements described on this page are specific to Cloud Manager 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](#)

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

Cloud Manager 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

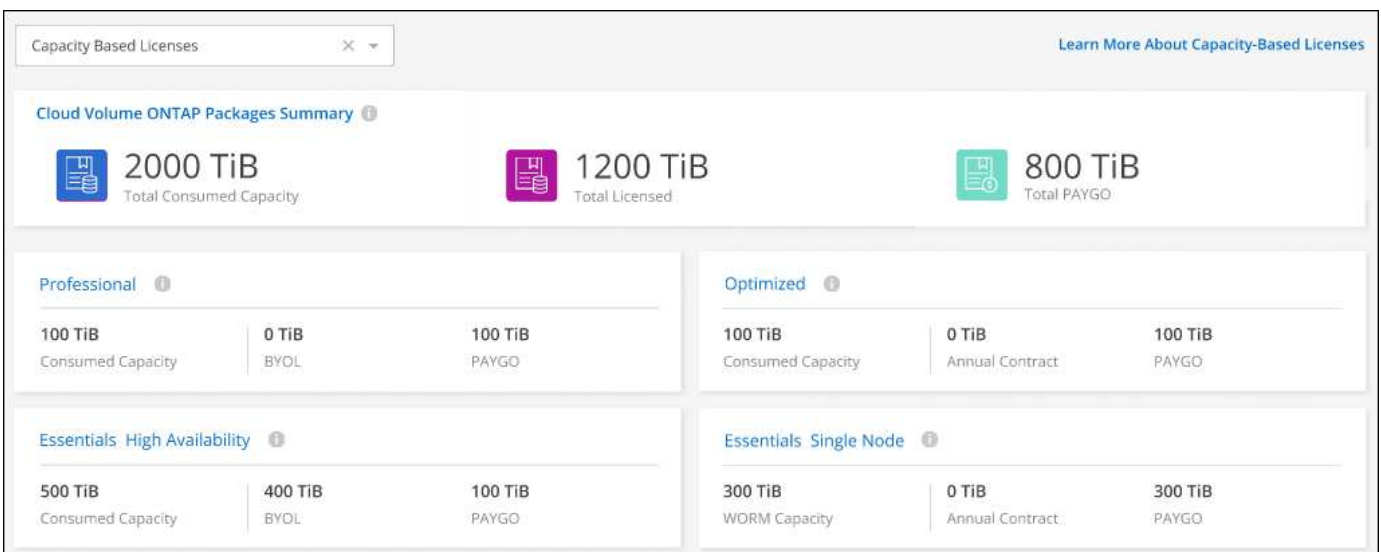
☒ Password
 ☐ Key Pair

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.



Unresolved directive in whats-new.adoc - include::_include/whats-new-july-gcp.adoc[]

7 June 2022

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

Cloud Volumes ONTAP 9.11.1

Cloud Manager 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 Cloud Manager so that you don't need to leave Cloud Manager 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 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, Cloud Manager 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

Cloud Manager 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 Cloud Manager 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 Cloud Manager](#)

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

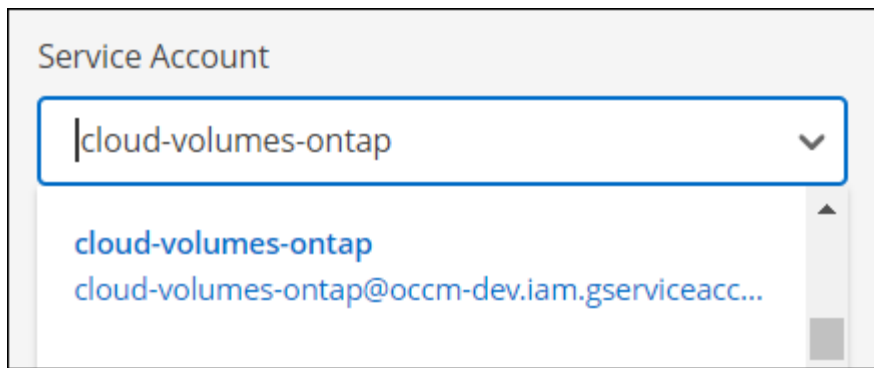
- When you create a Cloud Volumes ONTAP HA pair in Google Cloud, Cloud Manager will now display all existing firewall policies in a VPC.

Previously, Cloud Manager 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, Cloud Manager 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, Cloud Manager 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.

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

Cloud Manager 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.

The screenshot shows the 'Volumes Protocol' configuration page. At the top, there is a navigation bar with five steps: 1. Details, Protection & Tags (checked), 2. Protocol (active), 3. Disk Type, 4. Usage Profile & Tiering Policy, and 5. Review. The main content area is titled 'Volumes Protocol'. Below the title, there is a section 'Select the volume's protocol:' with three radio buttons: 'NFS Protocol' (selected), 'CIFS Protocol', and 'iSCSI Protocol'. Below this, there are two sections: 'Access Control' and 'Export Policy (1 rule defined)'. The 'Access Control' section has a dropdown menu currently showing 'Custom export policy'. The 'Export Policy' section has a link that says '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

Cloud Manager 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 Cloud Manager.

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

4 October 2021

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

Cloud Volumes ONTAP 9.10.0

Cloud Manager 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.

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.](#)

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.

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, Cloud Manager 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

Cloud Manager 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.

24 May 2021

Cloud Volumes ONTAP 9.9.1

Cloud Manager 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

Cloud Manager 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.

8 Mar 2021

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

Cloud Volumes ONTAP 9.9.0

Cloud Manager can now deploy and manage Cloud Volumes ONTAP 9.9.0.

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

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.

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

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 Cloud Manager. To view limitations with the Cloud Volumes ONTAP software itself, [go to the Cloud Volumes ONTAP Release Notes](#)

Cloud Manager doesn't support FlexGroup volumes

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

Cloud Manager 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, Cloud Manager 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.](#)

Cloud Manager doesn't support disaster recovery for storage VMs

Cloud Manager 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.

[Go to the Cloud Volumes ONTAP Release Notes](#)

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](#)

Get started in Google Cloud

Quick start for Cloud Volumes ONTAP in Google Cloud

Get started with Cloud Volumes ONTAP for GCP 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 GCP](#).

When you create your first Cloud Volumes ONTAP working environment, Cloud Manager prompts you to deploy a Connector if you don't have one yet.

2

Plan your configuration

Cloud Manager 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 so the Connector and Cloud Volumes ONTAP can contact several endpoints.

This step is important because the Connector can't manage Cloud Volumes ONTAP without outbound internet access. If you need to limit outbound connectivity, refer to the list of endpoints for [the Connector and Cloud Volumes ONTAP](#).

[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 Cloud Manager

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 Cloud Manager](#)
- [Installing the Connector software on a Linux host](#)
- [What Cloud Manager does with GCP 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 Cloud Manager 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, Cloud Manager 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

Cloud Manager 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 Cloud Manager, 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 GCP

Set up your Google Cloud Platform networking so Cloud Volumes ONTAP systems can operate properly. This includes networking for the Connector and Cloud Volumes ONTAP.

If you want to deploy an HA pair, you should [learn how HA pairs work in GCP](#).

Requirements for Cloud Volumes ONTAP

The following requirements must be met in GCP.

Internal load balancers

Cloud Manager 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.

One or multiple zones for HA pairs

You can ensure the high availability of your data by deploying an HA configuration across multiple or in a single zone. Cloud Manager 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.

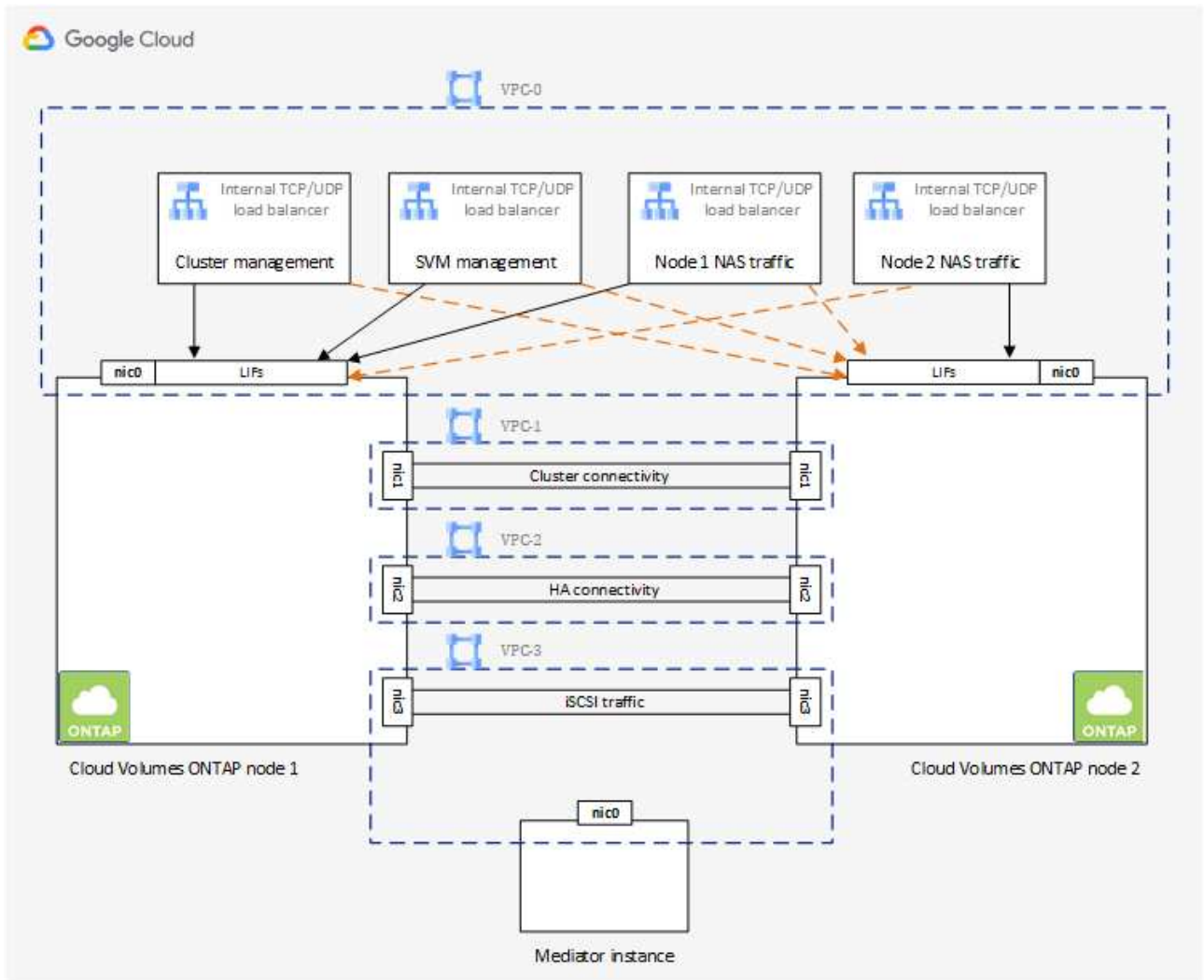
This deployment model does lower your costs because there are no data egress charges between zones.

Four Virtual Private Clouds for HA pairs

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

Cloud Manager 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 for HA pairs

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.

One Virtual Private Cloud for single node systems

One VPC is required for a single node system.

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 for Cloud Volumes ONTAP

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, Cloud Manager automatically configures your Cloud Volumes ONTAP systems to use the Connector as a proxy server. The only requirement is to ensure that the Connector's 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.

Private IP addresses

Cloud Manager allocates the following number of private IP addresses to Cloud Volumes ONTAP in GCP:

- **Single node:** 3 or 4 private IP addresses

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.

- **HA pair:** 14 or 15 private IP addresses
 - 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

Firewall rules

You don't need to create firewall rules because Cloud Manager does that for you. If you need to use your own, refer to the firewall rules listed below.

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

- One set of rules for HA components in VPC-0. These rules enable data access to Cloud Volumes ONTAP. [Learn more](#).
- Another set of rules for HA components in VPC-1, VPC-2, and VPC-3. These rules are open for inbound & outbound communication between the HA components. [Learn more](#).

Connection from Cloud Volumes ONTAP 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 Cloud Manager, 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 GCP 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](#).

Requirements for the Connector

Set up your networking so that the Connector can manage resources and processes within your public cloud environment. The most important step is ensuring outbound internet access to various endpoints.



If your network uses a proxy server for all communication to the internet, you can specify the proxy server from the Settings page. Refer to [Configuring the Connector to use a proxy server](#).

Connection to target networks

A Connector requires a network connection to the VPCs in which you want to deploy Cloud Volumes ONTAP. If you're deploying an HA pair, then the Connector needs a connection to VPC-0 only.

If you plan to deploy Cloud Volumes ONTAP in a VPC separate from the Connector, then you'll need to set up VPC Network Peering. [Learn more about VPC Network Peering](#)

Outbound internet access

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

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

Firewall rules for Cloud Volumes ONTAP

Cloud Manager creates GCP 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.

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	HTTPS access to the System Manager web console using the IP address of the cluster management LIF

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

Firewall rules for VPC-1, VPC-2, and VPC-3

In GCP, 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 Cloud Manager 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).

Firewall rules for the Connector

The firewall rules 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
TCP	3128	Provides Cloud Volumes ONTAP with internet access to send AutoSupport messages to NetApp Support. You must manually open this port after deploying the Connector.

Outbound rules

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

Basic outbound rules

The predefined firewall rules for the Connector includes the following outbound rules.

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

Advanced outbound rules

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



The source IP address is the Connector host.

Service	Protocol	Port	Destination	Purpose
API calls and AutoSupport	HTTPS	443	Outbound internet and ONTAP cluster management LIF	API calls to GCP and ONTAP, to Cloud Data Sense, to the Ransomware service, and sending AutoSupport messages to NetApp
DNS	UDP	53	DNS	Used for DNS resolve by Cloud Manager

Planning for VPC Service Controls in GCP

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

NetApp services such as Cloud Central and Cloud Manager communicate 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 Cloud Manager 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 Cloud Manager use images from a project within GCP that is managed by NetApp. This can affect the deployment of the Cloud Manager 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 Cloud Manager 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 Cloud Manager 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

Google Cloud Project

gcp-sub2

Marketplace Subscription

Edit Project

Details

Working Environment Name (Cluster Name)

cloudvolumesontap

Service Account

Service Account Name

account1

+ Add Labels

Optional Field | Up to four labels

Credentials

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 Cloud Manager 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 Cloud Manager 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.list`
- `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, Cloud Manager 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 [Cloud Manager 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. On the Canvas page, click **Add Working Environment** and follow the steps in Cloud Manager.
 - 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 Cloud Manager, 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 Cloud Manager](#)

Cloud Manager automatically queries NetApp's licensing service to obtain details about the licenses associated with your NetApp Support Site account. If there are no errors, Cloud Manager 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 Cloud Manager.
 - 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 Cloud Manager, 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, Cloud Manager 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. On the Canvas page, click **Add Working Environment** and follow the steps in Cloud Manager.
 - 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 Cloud Manager, 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.](#)



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 Cloud Manager.
 - 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 Cloud Manager, 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 Cloud Manager 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 Cloud Manager.
 - 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

By capacity

^

☐ 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 GCP

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

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 GCP 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 GCP

Create a working environment in Cloud Manager to launch Cloud Volumes ONTAP in GCP.

Steps

1. On the Canvas page, click **Add Working Environment** and follow the prompts.
2. **Choose a Location:** Select **Google Cloud** and **Cloud Volumes ONTAP**.
3. If you're prompted, [create a Connector](#).
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	Cloud Manager uses the working environment name to name both the Cloud Volumes ONTAP system and the GCP VM instance. It also uses the name as the prefix for the predefined security group, if you select that option.
Service Account Name	If you plan to use data tiering or Cloud Backup with Cloud Volumes ONTAP, then you need to enable Service Account and select a service account that has the predefined Storage Admin role. Learn how to create a service account .
Add Labels	<p>Labels are metadata for your GCP resources. Cloud Manager adds the labels to the Cloud Volumes ONTAP system and GCP 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 Google Cloud Documentation: Labeling Resources.</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 Cloud Manager resides.</p> <p>If you don't see any additional projects in the drop-down list, then you haven't yet associated the Cloud Manager 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 Cloud Manager 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 Cloud Manager, as described on this page.</p> </div> <p>Click Add Subscription 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 GCP project that's associated with a subscription to Cloud Volumes ONTAP from the GCP Marketplace.</p>

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

► 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.
6. **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 Google Cloud Documentation: Configuring Private Google Access .
Generated firewall policy	If you let Cloud Manager generate the firewall policy for you, you need to choose how you'll allow traffic: <ul style="list-style-type: none">• If you choose Selected VPC only, the source filter for inbound traffic is the subnet range of the selected VPC and the subnet range of the VPC where the Connector resides. This is the recommended option.• If you choose All VPCs, the source filter for inbound traffic is the 0.0.0.0/0 IP range.
Use existing firewall policy	If you use an existing firewall policy, ensure that it includes the required rules. Learn about firewall rules for Cloud Volumes ONTAP .

7. **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](#).
8. **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.

9. **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 Cloud Manager 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.

10. **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 Cloud Manager

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 GCP](#).

11. **Write Speed & WORM:** Choose **Normal** or **High** write speed, and activate write once, read many (WORM) storage, if desired.

Choosing a write speed is supported with single node systems only.

[Learn more about write speed.](#)

WORM can't be enabled if data tiering was enabled.

[Learn more about WORM storage.](#)

12. **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 GCP account (required for Cloud Volumes ONTAP 9.6).

Note the following:

- Cloud Manager 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 Cloud Manager.
- For help with adding a GCP account, see [Setting up and adding GCP 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 GCP console.

[Learn more about data tiering.](#)

13. **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, Cloud Manager enters a value that provides access to all instances in the subnet.

Field	Description
Permissions and Users / Groups (for CIFS only)	These fields enable you to control the level of access to a share for users and groups (also called access control lists or ACLs). You can specify local or domain Windows users or groups, or UNIX users or groups. If you specify a domain Windows user name, you must include the user's domain using the format domain\username.
Snapshot Policy	A Snapshot copy policy specifies the frequency and number of automatically created NetApp Snapshot copies. A NetApp Snapshot copy is a point-in-time file system image that has no performance impact and requires minimal storage. You can choose the default policy or none. You might choose none for transient data: for example, tempdb for Microsoft SQL Server.
Advanced options (for NFS only)	Select an NFS version for the volume: either NFSv3 or NFSv4.
Initiator group and IQN (for iSCSI only)	<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, Cloud Manager 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.</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

14. **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 OU=Computers,OU=Cloud in this field.</p> <p>Google Cloud Documentation: Organizational Units in Google Managed Microsoft AD</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 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 Cloud Manager automation docs 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>

15. **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](#).

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

Result

Cloud Manager 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 GCP

Create a working environment in Cloud Manager to launch Cloud Volumes ONTAP in GCP.

Steps

1. On the Canvas page, click **Add Working Environment** and follow the prompts.
2. **Choose a Location:** Select **Google Cloud** and **Cloud Volumes ONTAP HA**.
3. **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	Cloud Manager uses the working environment name to name both the Cloud Volumes ONTAP system and the GCP 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 Tiering or Cloud Backup services, you need to enable the Service Account switch and then select the Service Account that has the predefined Storage Admin role.
Add Labels	<p>Labels are metadata for your GCP resources. Cloud Manager adds the labels to the Cloud Volumes ONTAP system and GCP 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 Google Cloud Documentation: Labeling Resources.</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 Cloud Manager resides.</p> <p>If you don't see any additional projects in the drop-down list, then you haven't yet associated the Cloud Manager 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 Cloud Manager 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 Cloud Manager, as described on this page.</p> </div> <p>Click Add Subscription 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 GCP project that's associated with a subscription to Cloud Volumes ONTAP from the GCP Marketplace.</p>

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

► https://docs.netapp.com/us-en/cloud-manager-cloud-volumes-ontap//media/video_subscribing_gcp.mp4

(video)

4. **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.
5. **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.](#)

6. **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 Cloud Manager generate the firewall policy for you, you need to choose how you'll allow traffic:</p> <ul style="list-style-type: none">• If you choose Selected VPC only, the source filter for inbound traffic is the subnet range of the selected VPC and the subnet range of the VPC where the Connector resides. This is the recommended option.• If you choose All VPCs, the source filter for inbound traffic is the 0.0.0.0/0 IP range.
Use existing	<p>If you use an existing firewall policy, ensure that it includes the required rules.</p> <p>Learn about firewall rules for Cloud Volumes ONTAP.</p>

7. **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.](#)
8. **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.

9. **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 Cloud Manager 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.

10. **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 Cloud Manager 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 GCP](#).

11. **WORM:** Activate write once, read many (WORM) storage, if desired.

WORM can't be enabled if data tiering was enabled. [Learn more about WORM storage](#).

12. **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 select a service account that has the predefined Storage Admin role.

Note the following:

- Cloud Manager 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 Cloud Manager.
- 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 GCP console.

[Learn more about data tiering](#).

13. **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, Cloud Manager 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.

Field	Description
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, Cloud Manager 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.</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

Default Policy

Protocol

NFS
CIFS
iSCSI

Share name: Permissions:

Full Control

Users / Groups:

Valid users and groups separated by a semicolon

14. **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.

Field	Description
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 OU=Computers,OU=Cloud in this field.</p> <p>Google Cloud Documentation: Organizational Units in Google Managed Microsoft AD</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 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 Cloud Manager automation docs 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>

15. **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](#).

16. **Review & Approve:** Review and confirm your selections.
- Review details about the configuration.
 - Click **More information** to review details about support and the GCP resources that Cloud Manager will purchase.
 - Select the **I understand...** check boxes.
 - Click **Go**.

Result

Cloud Manager 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.

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

If Cloud Manager 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.](#)

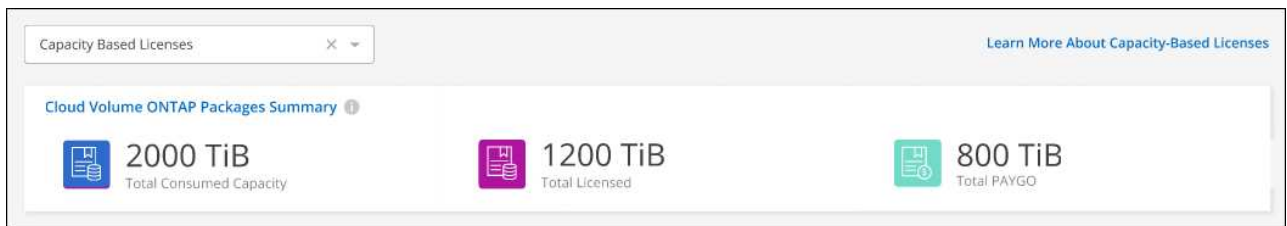
View the consumed capacity in your account

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 Cloud Manager so that the capacity is available for Cloud Volumes ONTAP.

What you'll need

- You need to provide Cloud Manager 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 Cloud Manager](#). 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, Cloud Manager automatically updates the license in the Digital Wallet. There's nothing that you need to do.

However, if you deployed Cloud Manager in a location that doesn't have internet access, then you'll need to manually update the license in Cloud Manager.

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

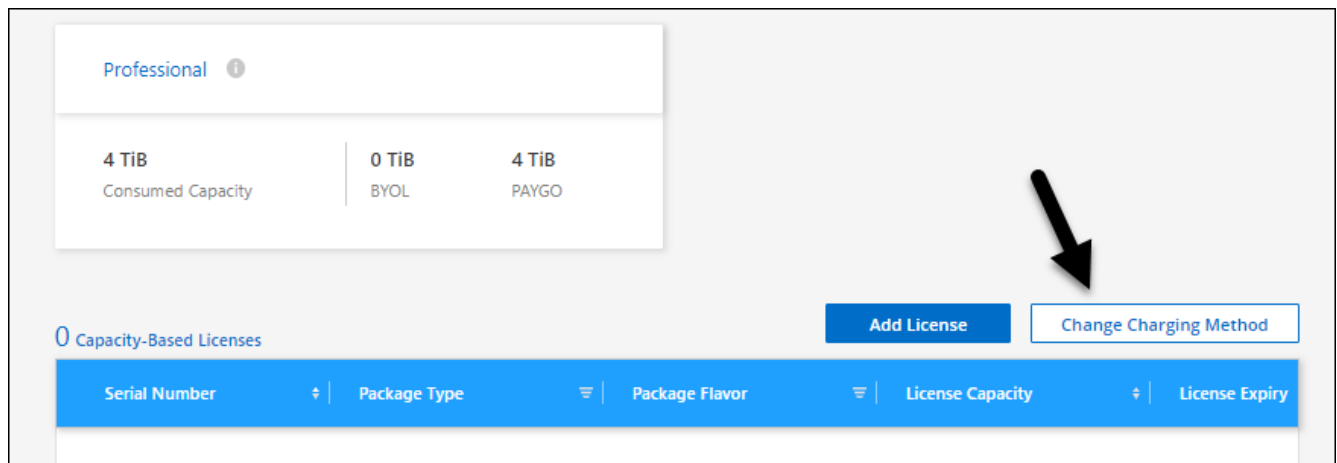
You can change the charging method for a Cloud Volumes ONTAP system that uses capacity-based licensing. For example, if you deployed a Cloud Volumes ONTAP system with the Essentials package, you can change it to the Professional package if your business needs changed.

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

Cloud Manager 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

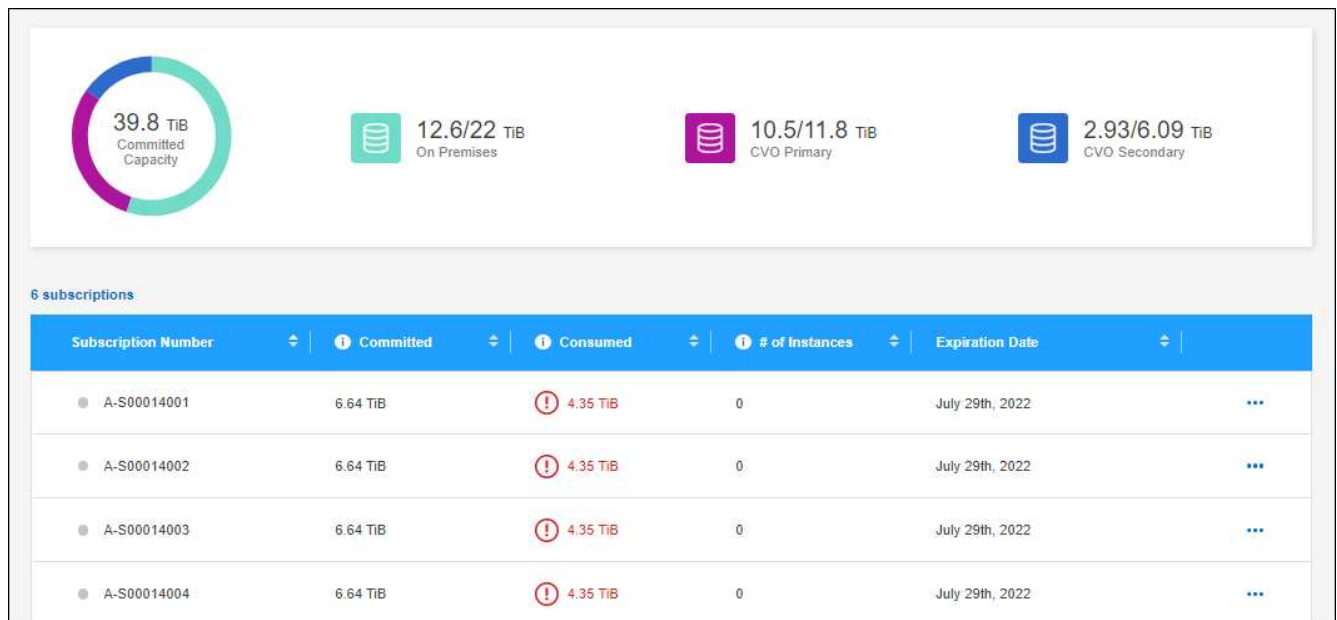
Before you can use and manage Keystone Flex Subscriptions in Cloud Manager, you need to contact NetApp to authorize your Cloud Manager user account with your Keystone Flex Subscriptions.

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 Cloud Manager 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 Cloud Manager 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 Cloud Manager 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.

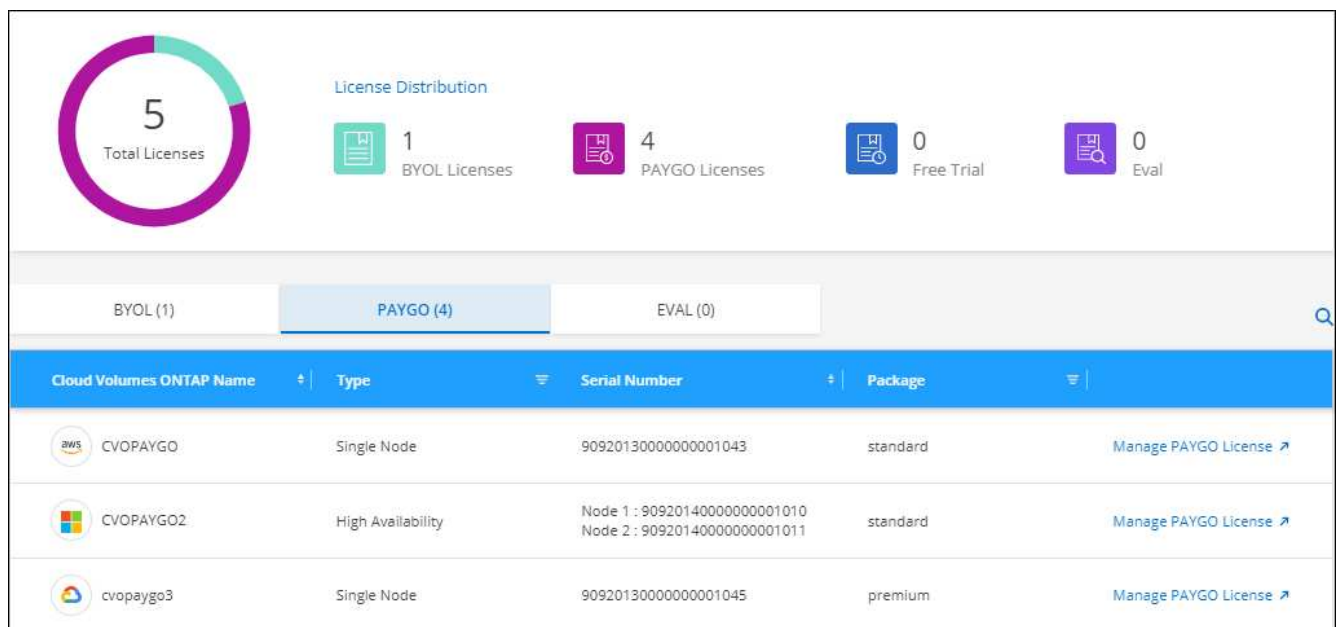
[Learn more about Cloud Volumes ONTAP licenses.](#)

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.



The screenshot displays the 'License Distribution' section of the Digital Wallet. It features a donut chart showing 5 total licenses, with a breakdown: 1 BYOL License (green), 4 PAYGO Licenses (purple), 0 Free Trial (blue), and 0 Eval (purple). Below the chart, there are tabs for 'BYOL (1)', 'PAYGO (4)', and 'EVAL (0)'. The 'PAYGO (4)' tab is selected, showing a table of four PAYGO licenses. The table has columns for 'Cloud Volumes ONTAP Name', 'Type', 'Serial Number', and 'Package'. Each row includes a 'Manage PAYGO License' link.

Cloud Volumes ONTAP Name	Type	Serial Number	Package	
CVOPAYGO	Single Node	90920130000000001043	standard	Manage PAYGO License
CVOPAYGO2	High Availability	Node 1 : 90920140000000001010 Node 2 : 90920140000000001011	standard	Manage PAYGO License
cvopaygo3	Single Node	90920130000000001045	premium	Manage PAYGO License

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

Cloud Manager 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)	<input type="text"/> <input type="button" value="Add Unassigned Licenses"/>		
Serial Number	Type	Cloud Provider	License Expiry	Status		
012345678901234567890	Single Node	All Providers	April 20, 2022	Unassigned	Exchange License ▾	...
012345678901234567891	Single Node	 Azure	April 20, 2022	Unassigned	Exchange License ▾	...
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

Cloud Manager 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, Cloud Manager 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.

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

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, Cloud Manager automatically obtains the new license from NetApp and installs it on the Cloud Volumes ONTAP system.

If Cloud Manager can't access the license file over the secure internet connection, you can obtain the file yourself and then manually upload the file to Cloud Manager.

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

Cloud Manager 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 Cloud Manager. 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 Cloud Manager.

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, Cloud Manager 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

Cloud Manager 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 Cloud Manager.

Cloud Manager provides several ways to create a new volume:

- Specify details for a new volume and let Cloud Manager 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, Cloud Manager 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.

Create a volume

The most common way to create a volume is to specify the type of volume that you need and then Cloud Manager 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. On the Canvas page, double-click the name of the Cloud Volumes ONTAP system on which you want to provision a FlexVol volume.
2. Create a new volume by letting Cloud Manager 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.**

3. 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.
Tags	Tags that you add to a volume are associated with the Application Templates service , 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, Cloud Manager 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, Cloud Manager 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 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 [Cloud Manager 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, Cloud Manager 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 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

Cloud Manager 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.

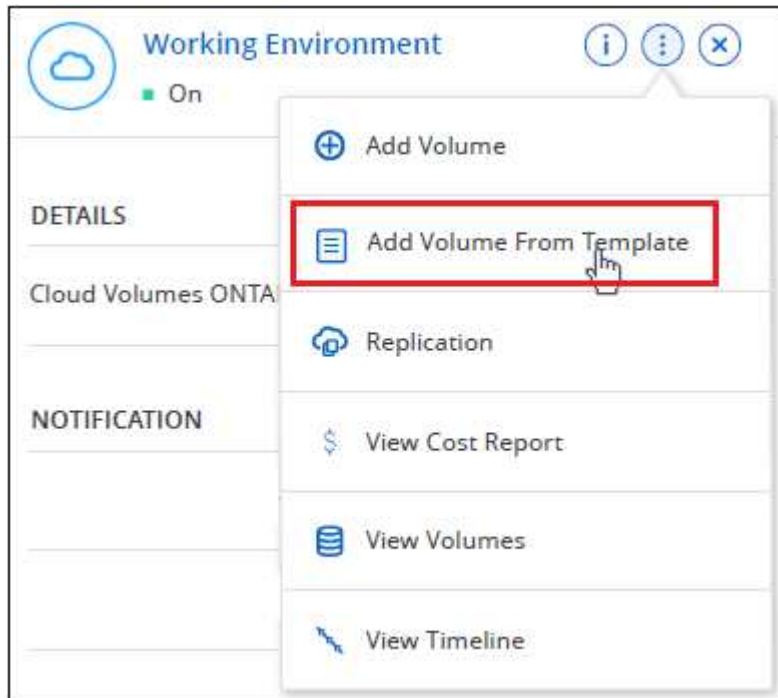
The template should make your job easier because certain volume parameters will already be defined in the template, such as disk type, size, protocol, snapshot policy, cloud provider, and more. When a parameter is already predefined, you can just skip to the next volume parameter.



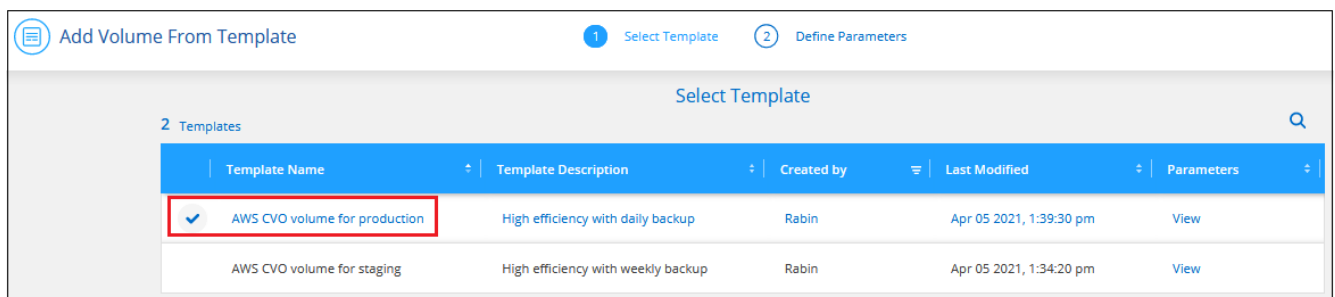
You can only create NFS or CIFS volumes when using templates.

Steps

1. On the Canvas page, click the name of the Cloud Volumes ONTAP system on which you want to provision a volume.
2. Click  > **Add Volume From Template**.



3. 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.

Define Parameters

Enter your values for the actions. Parameters that are locked by the template are not editable.

Actions

```

graph TD
    A[Create Volume in Cloud Volumes ONTAP (1)] --> B[Enable Cloud Backup (1)]
    B --> A
  
```

☐ Show read-only parameters

Details

Volume Name ?

Volume Name should start with "staging"

Volume Size (GB) ?

Minimum value is 160, Maximum value is 185

Protection

Snapshot Policy

Default X ▼

Usage Profile

☒ Storage Efficiency
 ☐ No Storage Efficiency

Disk Type

Disk Type

GP2 - General Purpose SSD X ▼



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.

4. 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.
5. 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.
6. 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.

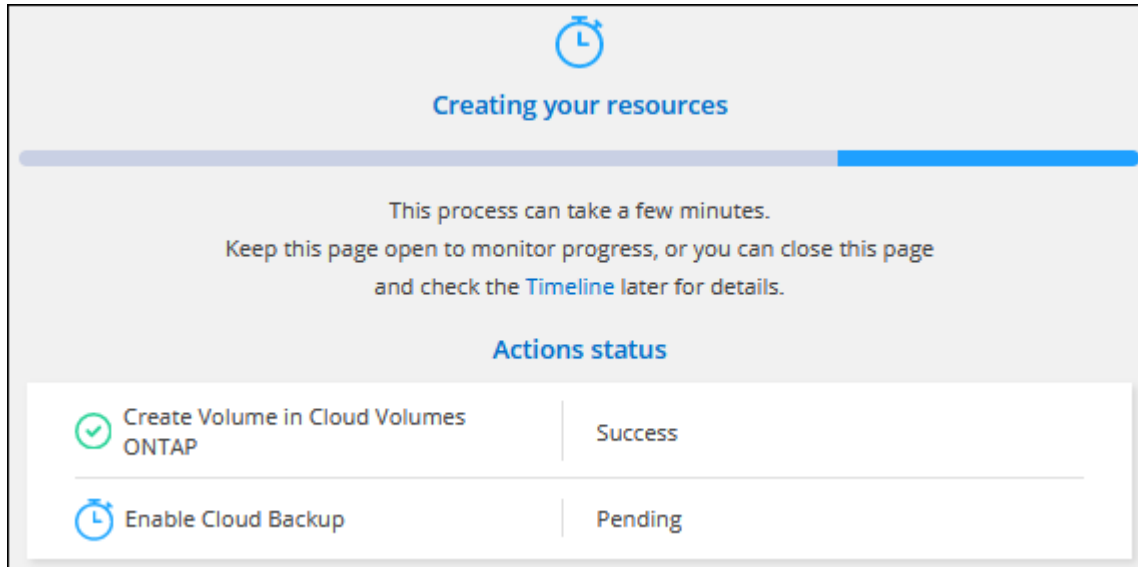


For example, if the Enable Cloud Backup action requires that you select a backup policy, you can do that now.

7. 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, Cloud Manager 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. On the Canvas page, double-click the name of the Cloud Volumes ONTAP working environment on which you want to manage aggregates.
2. Click the menu icon and then click **Advanced > Advanced allocation**.
3. Click **Add Aggregate** and then create the aggregate.
4. For Home Node, choose the second node in the HA pair.
5. After Cloud Manager creates the aggregate, select it and then click **Create volume**.
6. Enter details for the new volume, and then click **Create**.

Result

Cloud Manager creates the volume on the second node in the HA pair.

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


Cloud Manager 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. On the Canvas page, double-click the Cloud Volumes ONTAP working environment on which you want to manage volumes.
2. Manage your volumes:

Task	Action
View information about a volume	Select a volume, and then click Info .
Edit a volume (read-write volumes only)	<div><div><div>a. Select a volume, and then click Edit.</div><div>b. Modify the volume's Snapshot policy, NFS protocol version, NFS access control list (export policy), or share permissions, and then click Update.</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 Clone.</div><div>b. Modify the clone name as needed, and then click Clone.</div></div><div><p>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.</p><p>To learn more about FlexClone volumes, see the ONTAP 9 Logical Storage Management Guide.</p></div></div>
Restore data from a Snapshot copy to a new volume	<div><div><div>a. Select a volume, and then click Restore from Snapshot copy.</div><div>b. Select a Snapshot copy, enter a name for the new volume, and then click Restore.</div></div></div>
Create a Snapshot copy on demand	<div><div><div>a. Select a volume, and then click Create a Snapshot copy.</div><div>b. Change the name, if needed, and then click Create.</div></div></div>
Get the NFS mount command	<div><div><div>a. Select a volume, and then click Mount Command.</div><div>b. Click Copy.</div></div></div>

Task	Action
View the target iQN for an iSCSI volume	<ol style="list-style-type: none"> Select a volume, and then click Target iQN. Click Copy. Use the IQN to connect to the LUN from your hosts.
Change the underlying disk type	<ol style="list-style-type: none"> Select a volume, and then click Change Disk Type & Tiering Policy. Select the disk type, and then click Change. <div>  <p>Cloud Manager 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"> Select a volume, and then click Change Disk Type & Tiering Policy. Click Edit Policy. Select a different policy and click Change. <div>  <p>Cloud Manager 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"> Select a volume, and then click Delete. Click Delete again to confirm.

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

- From the working environment, click the menu icon and then click **Advanced > CIFS setup**.
- 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"> To configure Google Managed Microsoft AD as the AD server for Cloud Volumes ONTAP, enter OU=Computers,OU=Cloud in this field. <p>Google Cloud Documentation: Organizational Units in Google Managed Microsoft AD</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.

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 Cloud Manager displays an Action Required message

Cloud Manager 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.



Cloud Manager 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 the issue.](#)
2. Based on your analysis, move volumes to avoid capacity issues:
 - [Move volumes to another system.](#)
 - [Move volumes to another aggregate on the same system.](#)

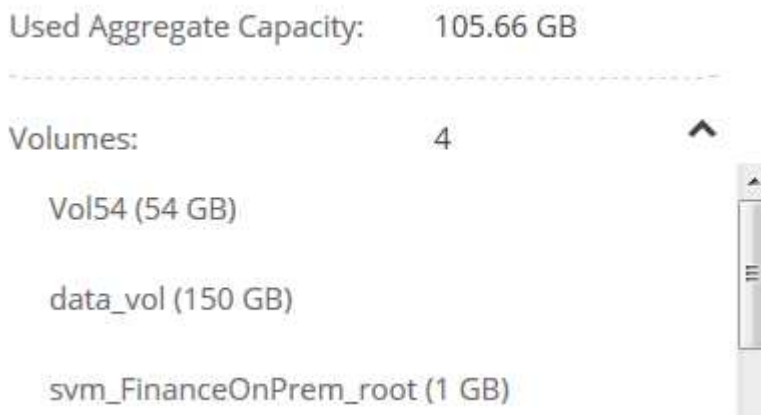
Identify how to correct capacity issues

If Cloud Manager 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, Cloud Manager 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, Cloud Manager 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 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

Cloud Manager 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. Cloud Manager does that for you.
- You don't need to enable data tiering at the system level.

Cloud Manager 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 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 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

Cloud Manager 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. On the Canvas page, double-click the name of the Cloud Volumes ONTAP instance.
3. Click the menu icon and select **Enable capacity tiering**.



You'll only see this option if data tiering couldn't be enabled when Cloud Manager 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.](#)

4. Click **Enable** so Cloud Manager 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**

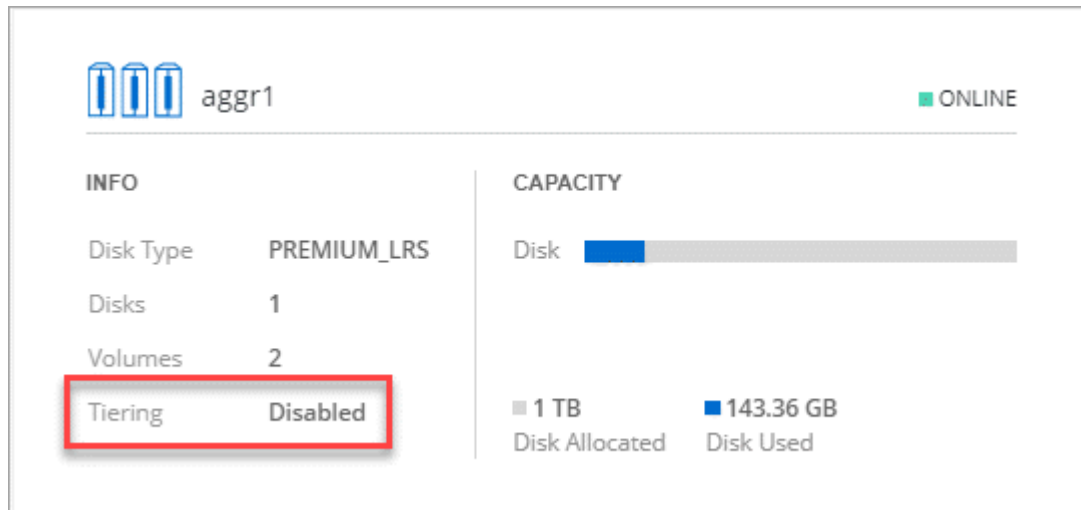
If you're enabling data tiering on a new volume, then you don't need to worry about enabling data tiering on an aggregate. Cloud Manager creates the volume on an existing aggregate that has tiering enabled, or it creates a new aggregate for the volume if a data tiering-enabled aggregate doesn't already 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 Cloud Manager.
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 Add New Volume .
Modify an existing volume	Select the volume and click Change Disk Type & Tiering Policy .

2. Select a tiering policy.

For a description of these policies, see [Data tiering overview](#).

Example


Tiering data to object storage


Volume Tiering Policy

☒ **All** - Immediately tiers all data (not including metadata) to object storage.

☐ **Auto** - Tiers cold Snapshot copies and cold user data from the active file system to object storage.

☐ **Snapshot Only** - Tiers cold Snapshot copies to object storage

☐ **None** - Data tiering is disabled.


Working Environment S3 Storage classes: Standard

Cloud Manager 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. 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.
2. Follow the prompts until you reach the tiering page and enable data tiering to object storage.

Example


S3 Tiering
What are storage tiers?

☒ **Enabled**
☐ **Disabled**

Note: If you enable S3 tiering, thin provisioning must be enabled on volumes created in this aggregate.

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. Cloud Manager 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 Cloud Manager 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, Cloud Manager 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:

- Cloud Manager's automatic capacity management doesn't apply to LUNs. When Cloud Manager creates a LUN, it disables the autogrow feature.
- You can create additional LUNs from System Manager or the CLI.

Steps

1. On the Canvas page, double-click the Cloud Volumes ONTAP working environment on which you want to manage volumes.
2. Select a volume, and then click **Target iQN**.
3. Click **Copy** to copy the iQN name.
4. 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](#)

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.

Cloud Manager 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, Cloud Manager 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 Cloud Manager 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 Cloud Manager. 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. On the Canvas page, double-click the name of the Cloud Volumes ONTAP instance on which you want to manage aggregates.
2. Click the menu icon, and then click **Advanced > Advanced allocation**.
3. Click **Add Aggregate** and then specify details for the aggregate.

Google Cloud

For help with disk type and disk size, refer to [Plan your Cloud Volumes ONTAP configuration in Google Cloud](#).

4. 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 Cloud Manager. 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. On the Canvas page, double-click the Cloud Volumes ONTAP working environment on which you want to manage aggregates.
2. Click the menu icon and then click **Advanced > Advanced allocation**.
3. Manage your aggregates:

Task	Action
View information about an aggregate	Select an aggregate and click Info .
Create a volume on a specific aggregate	Select an aggregate and click Create volume .
Add disks to an aggregate	<ol style="list-style-type: none">a. Select an aggregate and click Add disks.b. Select the number of disks that you want to add and click Add. <div> All disks in an aggregate must be the same size.</div>
Delete an aggregate	<ol style="list-style-type: none">a. Select an aggregate that does not contain any volumes and click Delete.b. Click Delete again to confirm.

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 Cloud Manager console, click the Settings icon, and select **Connector Settings**.
2. Under **Capacity**, modify any of the following settings:

Capacity Management Mode

Choose whether Cloud Manager notifies you of storage capacity decisions or whether Cloud Manager 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 Cloud Manager

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

Cloud Manager 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

Cloud Manager 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 Cloud Manager. 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.

 **Working Environment Information**

ONTAP

Serial Number:	
System ID:	system-id-capacitytest
Cluster Name:	capacitytest
ONTAP Version:	9.7RC1
Date Created:	Jul 6, 2020 07:42:02 am
Storage VM Name:	svm_capacitytest 

3. In the Modify SVM Name dialog box, change the name, and then click **Save**.

Manage storage VMs for disaster recovery

Cloud Manager 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 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 Cloud Manager 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 Cloud Manager 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 Cloud Manager 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 Cloud Manager 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

Starting with the 3.9.19 release, the Connector requires the following permissions to create and manage storage VMs for Cloud Volumes ONTAP HA pairs:

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

These 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 Cloud Manager 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:

- 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 Cloud Manager](#)
- [Registering pay-as-you-go systems](#)



Cloud Manager 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.
 - Google Cloud: [Google Cloud Key Management Service](#)

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
- 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 vservice_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
```

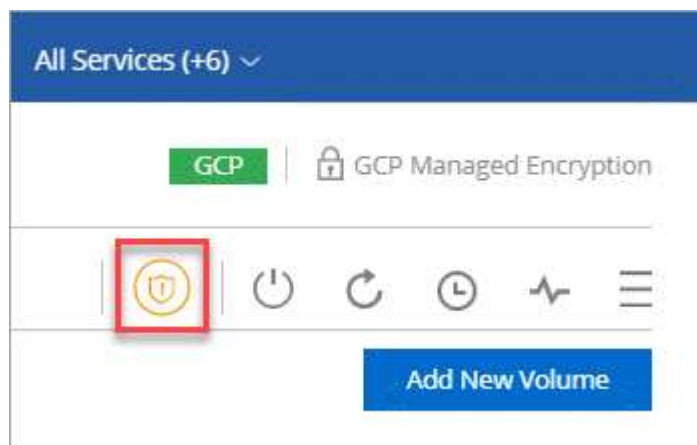
Improving protection against ransomware

Ransomware attacks can cost a business time, resources, and reputation. Cloud Manager enables you to implement the NetApp solution for ransomware, which provides effective tools for visibility, detection, and remediation.

Using this feature to improve protection against ransomware addresses a separate use case from [the ONTAP anti-ransomware feature](#) that you can enable through System Manager or the ONTAP CLI.

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



Cloud Manager 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 Cloud Manager 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 Cloud Manager only

Upgrades of Cloud Volumes ONTAP must be completed from Cloud Manager. You should not upgrade Cloud Volumes ONTAP by using System Manager or the CLI. Doing so can impact system stability.

How to upgrade

Cloud Manager 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 Cloud Manager 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
9.11.0	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, Cloud Manager 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 Cloud Manager 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

Cloud Manager 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 Cloud Manager must have a network connection to Cloud Volumes ONTAP. For example, you might need to log in to Cloud Manager 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**.

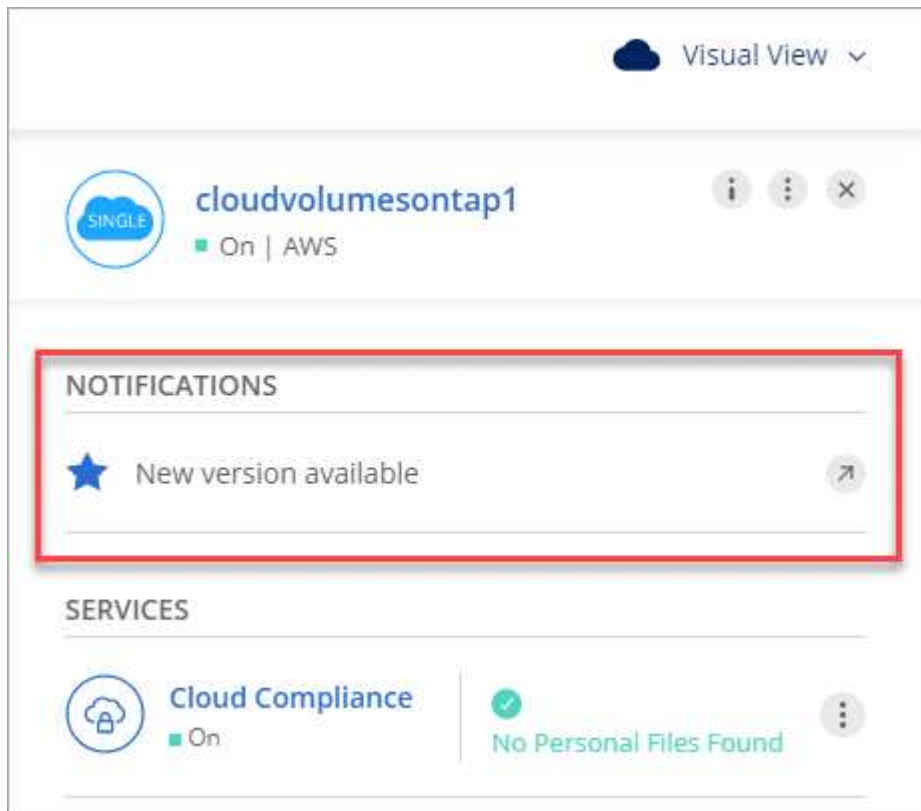
Upgrade Cloud Volumes ONTAP

Cloud Manager notifies you when a new version is available for upgrade. You can start the upgrade process from this notification. For details, see [Upgrade from Cloud Manager notifications](#).

Another way to perform software upgrades by using an image on an external URL. This option is helpful if Cloud Manager 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 Cloud Manager notifications

Cloud Manager 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.

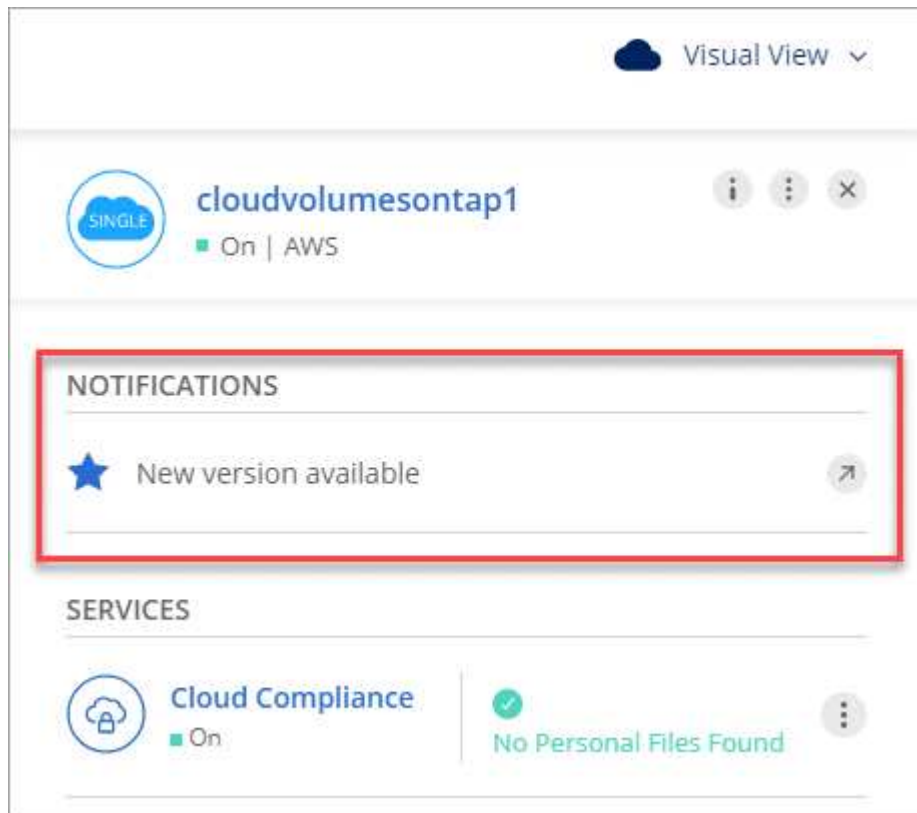
Before you begin

Cloud Manager 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 **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

Cloud Manager 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 Cloud Manager. You might use this option if Cloud Manager can't access the S3 bucket to upgrade the software.

Before you begin

Cloud Manager operations such as volume or aggregate creation must not be in progress on the Cloud Volumes ONTAP system.

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.

For example, you can copy the software image to the following path on the Connector:

```
/opt/application/netapp/cloudmanager/docker_occm/data/ontap/images/
```

5. From the working environment in Cloud Manager, 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

Cloud Manager 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 Cloud Manager 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](#).



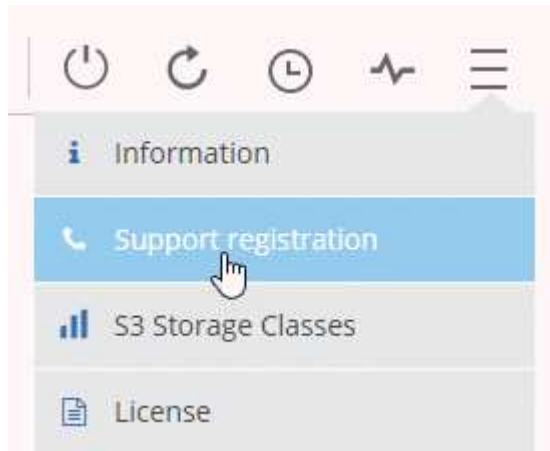
A system that isn't registered for support will still receive the software update notifications that appear in Cloud Manager when a new version is available. But you will need to register the system before you can upgrade the software.

Steps

1. If you have not yet added your NetApp Support Site account to Cloud Manager, go to **Account Settings** and add it now.

[Learn how to add NetApp Support Site accounts.](#)

2. On the Canvas page, double-click the name of the system that you want to register.
3. Click the menu icon and then click **Support registration**:



4. Select a NetApp Support Site account and click **Register**.

Result

Cloud Manager registers the system with NetApp.

Managing the state of Cloud Volumes ONTAP

You can stop and start Cloud Volumes ONTAP from Cloud Manager 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 Cloud Manager 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, Cloud Manager postpones the shutdown if an active data transfer is in progress.

Cloud Manager 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 Cloud Manager to shut down the system every Saturday at 12:00 a.m. for 48 hours. Cloud Manager restarts the system every Monday at 12:00 a.m.

<input type="checkbox"/>	Turn off every weekday Mon, Tue, Wed, Thu, Fri	turn off at	08	:	00	PM	for	12	Hours (1-24)
<input checked="" type="checkbox"/>	Turn off every weekend Sat	turn off at	12	:	00	AM	for	48	Hours (1-48)

3. Click **Save**.

Result

Cloud Manager 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, Cloud Manager 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, Cloud Manager 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 [Cloud Manager API](#) or from the user interface when you [create a CIFS server](#).

Modify system write speed

Cloud Manager 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 Cloud Manager, 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 Cloud Manager. As a result, Cloud Manager 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 Cloud Manager

You can discover and add existing Cloud Volumes ONTAP systems to Cloud Manager. You might do this if you deployed a new Cloud Manager system.

Before you begin

You must know the password for the Cloud Volumes ONTAP admin user account.

Steps

1. On the Canvas page, click **Add Working Environment**.
2. Select the cloud provider in which the system resides.
3. Choose the type of Cloud Volumes ONTAP system.
4. Click the link to discover an existing system.



5. On the Region page, choose the region where the instances are running, and then select the instances.
6. On the Credentials page, enter the password for the Cloud Volumes ONTAP admin user, and then click **Go**.

Result

Cloud Manager 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 Cloud Manager. It does not delete the Cloud Volumes ONTAP system. You can later rediscover the working environment.

Removing a working environment from Cloud Manager enables you to do the following:

- Rediscover it in another workspace
- Rediscover it from another Cloud Manager system
- Rediscover it if you had problems during the initial discovery

Steps

1. In the upper right of the Cloud Manager 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

Cloud Manager 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 Cloud Manager, 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 Cloud Manager to release the license.

When you delete a working environment, Cloud Manager 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 Cloud Manager 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 or Monitoring on this working environment and no other working environments use those services, then you'll need to delete the instances for those services.
 - [Learn more about the Cloud Data Sense instance](#).
 - [Learn more about the Monitoring Acquisition Unit](#).
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.

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.



Cloud Manager 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 working environment, click the menu icon, and then select **Change machine**.
2. If you are using a node-based PAYGO license, you can optionally choose a different license.
3. 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 Cloud Manager so that you don't need to leave Cloud Manager 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 Cloud Manager 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 Cloud Manager'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 Cloud Manager's Standard View.

- Firmware upgrades

Automatic firmware updates from the **Cluster > Settings** page is not supported with Cloud Volumes ONTAP.

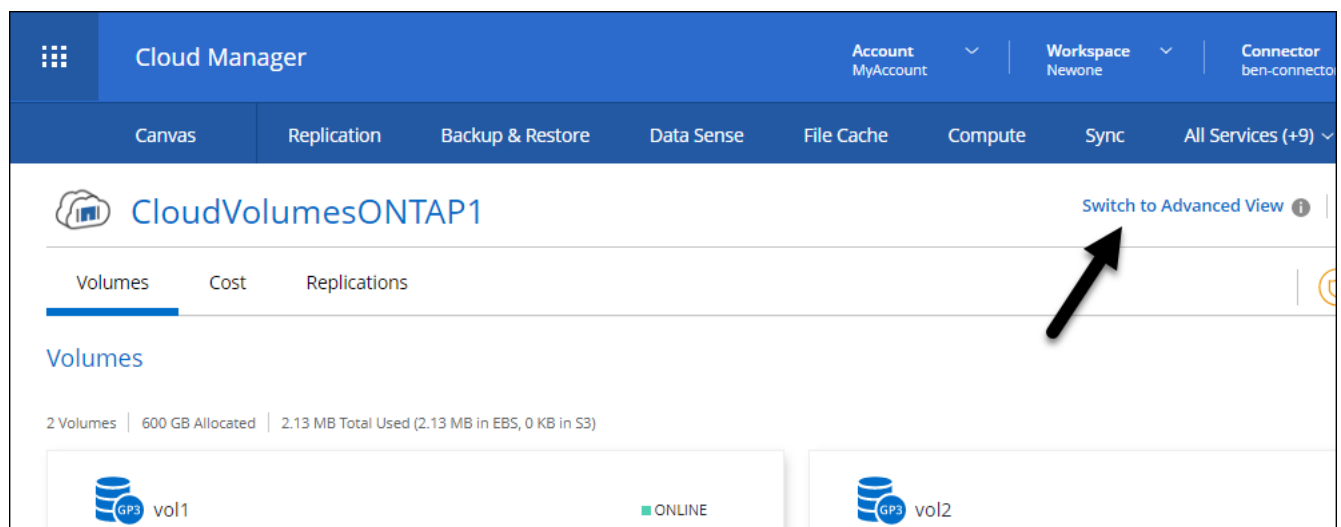
In addition, role-based access control from System Manager is not supported.

How to get started

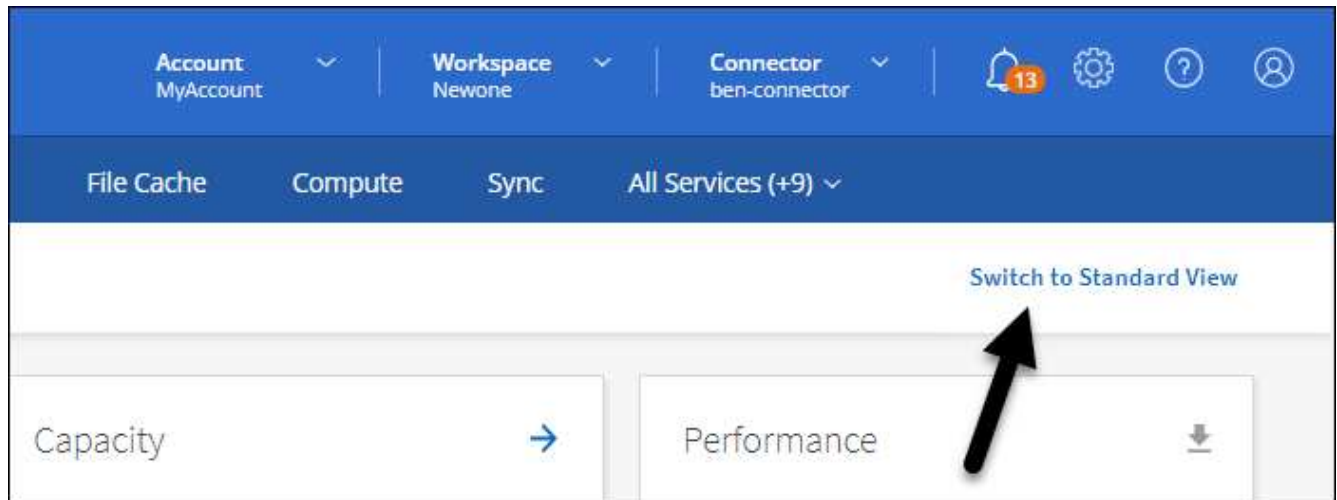
Open a Cloud Volumes ONTAP working environment and click the Advanced View option.

Steps

1. On the Canvas page, double-click the name of a Cloud Volumes ONTAP system.
2. In the top-right, click **Switch to Advanced View**.



3. If the confirmation message appears, read through it and click **Close**.
4. Use System Manager to manage Cloud Volumes ONTAP.
5. If needed, click **Switch to Standard View** to return to standard management through Cloud Manager.



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.

Steps

1. In Cloud Manager, identify the IP address of the cluster management interface:
 - a. On the Canvas page, select the Cloud Volumes ONTAP system.
 - b. 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.

- [Google Cloud networking requirements](#)

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](#).

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, Cloud Manager 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).

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 deployed with the Professional package
- Add on any of NetApp's cloud data services at extra cost

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.
- **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 Cloud Central](#).

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 Cloud Manager 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 Cloud Manager 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 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 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, 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.

Disks and aggregates

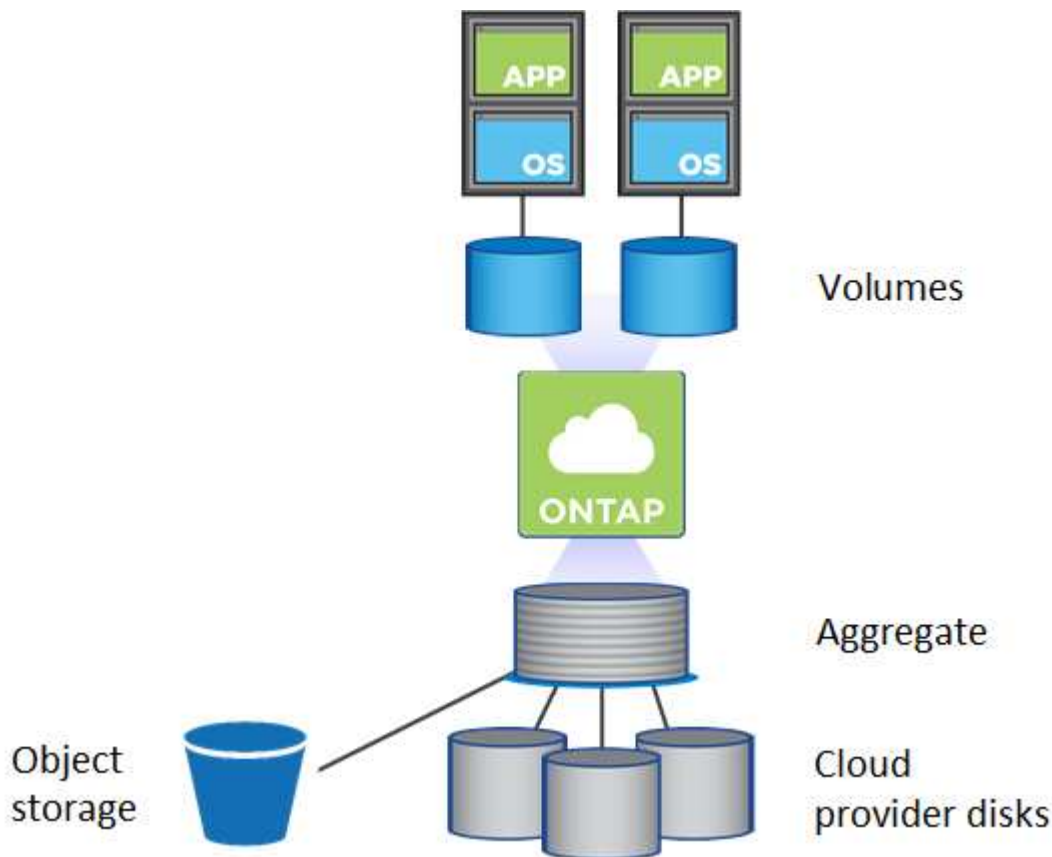
Understanding how Cloud Volumes ONTAP uses cloud storage can help you understand your storage costs.



All disks and aggregates must be created and deleted directly from Cloud Manager. 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 Cloud Manager creates a 500 GiB aggregate, the usable capacity is 442.94 GiB.

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.

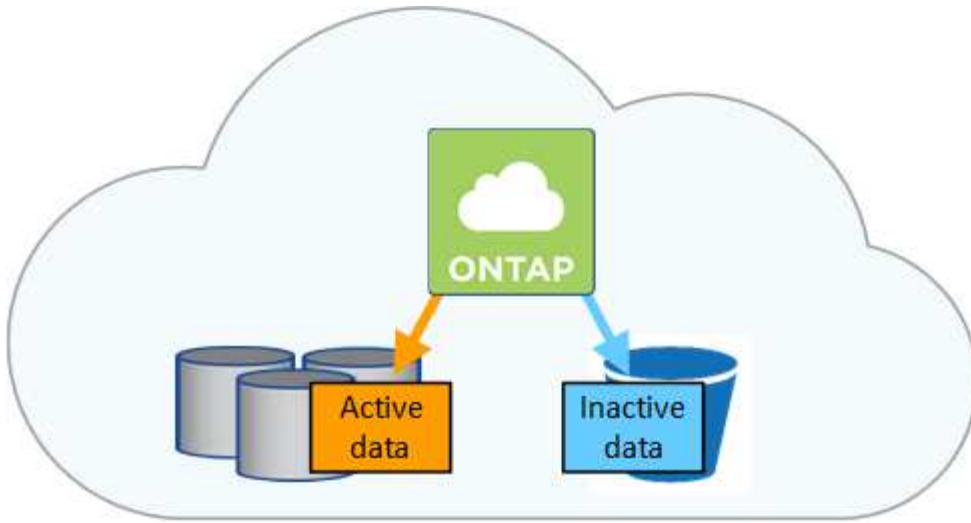
Hot spares

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.

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 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.

Cloud Manager 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 Cloud Manager 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 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 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](#).

Cloud Manager 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, Cloud Manager 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

Cloud Manager provides simplified and advanced management of Cloud Volumes ONTAP storage.



All disks and aggregates must be created and deleted directly from Cloud Manager. 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

Cloud Manager 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. Cloud Manager creates aggregates for you when you launch an instance, and when you provision additional volumes.

When you create a volume, Cloud Manager 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.

- It purchases disks for a new aggregate and places the volume on that aggregate.

Cloud Manager 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.

Advanced allocation

Rather than let Cloud Manager 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 Cloud Manager notifies you of storage capacity decisions or whether Cloud Manager 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, Cloud Manager 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, Cloud Manager automatically purchases new disks for that aggregate so volumes can continue to grow.

Cloud Manager checks the free space ratio every 15 minutes to determine if it needs to purchase additional disks.

- If an aggregate reaches the capacity threshold and it can't support any additional disks, Cloud Manager automatically moves a volume from that aggregate to an aggregate with available capacity or to a new aggregate.

If Cloud Manager 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, Cloud Manager deletes it.

Management of LUNs with automatic capacity management

Cloud Manager's automatic capacity management doesn't apply to LUNs. When Cloud Manager creates a LUN, it disables the autogrow feature.

Manual capacity management

If the Account Admin set the Capacity Management Mode to manual, Cloud Manager 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

Cloud Manager 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.

Configurations that support high write speed

Not all Cloud Volumes ONTAP configurations support high write speed. Those configurations use normal write speed by default.

Google Cloud

If you use a single node system, Cloud Volumes ONTAP supports high write speed with all machine types.

Cloud Volumes ONTAP doesn't support high write speed with HA pairs in Google Cloud.

[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 9.11.0 or later

```
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.

Choose no storage efficiency when creating a volume from Cloud Manager, 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.

Charging

Charging for WORM storage is hourly, according to the total provisioned capacity of WORM volumes.

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

Activating WORM storage

You can activate WORM storage on a Cloud Volumes ONTAP system when you create a new working environment. This includes setting the default retention period for files.



You can't activate WORM storage on individual volumes—WORM must be activated at the system level.

The following image shows how to activate WORM storage when creating a working environment:

The screenshot shows the 'Create a New Working Environment' wizard in the Cloud Manager interface. The current step is 'WORM (write once, read many)'. The interface includes a top navigation bar with 'Cloud Manager' and various service tabs like 'Canvas', 'Replication', 'Backup & Restore', etc. The main content area is divided into two columns. The left column, titled 'Write Speed', has two radio button options: 'Normal' (selected) and 'High'. The 'Normal' option description states: 'Data is written directly to disk, reducing the likelihood of data loss in the event of an unplanned system outage.' The 'High' option description states: '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 in the event of an unplanned system outage.' The right column, titled 'WORM', contains explanatory text about WORM storage, a 'Learn More' link, and two radio button options: 'Disable WORM' and 'Activate WORM' (selected). Below these is a 'Notice' stating: 'If you activate WORM storage, data tiering to object storage will be disabled on the system.' At the bottom of the right column is a 'Retention Period' field set to '15' with a unit dropdown menu currently showing 'years'. A blue 'Continue' button is located at the bottom center of the wizard. The footer of the interface shows 'Cloud Manager 3.9.9 Build: 0 Jun 30, 2021 02:52:27 pm UTC Environment: staging'.

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](#).

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.
- When WORM storage is activated, data tiering to object storage can't be enabled.

High-availability pairs

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, Cloud Manager 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, Cloud Manager 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, Cloud Manager 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 Cloud Manager:

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 Cloud Manager is *Degraded*.

The following actions are unavailable from Cloud Manager during 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)
- 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:

- 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](#).

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 Cloud Manager 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. Cloud Manager enables you to implement the NetApp solution for ransomware, which provides effective tools for visibility, detection, and remediation.

- Cloud Manager 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.

- Cloud Manager 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 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.

[Learn how to monitor Cloud Volumes ONTAP performance](#), or check out this [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. Cloud Manager 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, Cloud Manager prompts you for the serial number of your license and your NetApp Support Site account. Cloud Manager 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 Cloud Manager.](#)

If Cloud Manager can't access the license file over the secure internet connection, you can [obtain the file yourself and then manually upload the file to Cloud Manager](#).

License expiration

Cloud Manager 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.

Cloud Manager 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, Cloud Manager automatically obtains the new license from NetApp and installs it on the Cloud Volumes ONTAP system.

If Cloud Manager can't access the license file over the secure internet connection, you can [obtain the file yourself and then manually upload the file to Cloud Manager](#).

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

- Cloud Manager 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 Cloud Manager 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.

- Cloud Manager 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 9.11.1
 - NetApp Volume Encryption (only for BYOL or registered PAYGO systems)
 - NFS
 - 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 Google Cloud
 - 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.

- Cloud Manager 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 Cloud Manager sets differently from the defaults:

Attribute	Value set by Cloud Manager
Autosize mode	grow
Maximum autosize	1,000 percent <div>  The Account Admin can modify this value from the Settings page. </div>
Security style	NTFS for CIFS volumes UNIX for NFS volumes
Space guarantee style	none
UNIX permissions (NFS only)	777

See the *volume create* man page for information about these attributes.

Internal disks for system data

In addition to the storage for user data, Cloud Manager also purchases cloud storage for system data.

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
- Snapshots for boot and root data
- Boot and root disks are encrypted by default.

Where the disks reside

Cloud Manager 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 account to Cloud Manager and then register for support.

Add an NSS account

The Support Dashboard enables you to add and manage all of your NetApp Support Site accounts from a single location.

Steps

1. If you don't have a NetApp Support Site account yet, [register for one](#).
2. In the upper right of the Cloud Manager console, click the Help icon, and select **Support**.



3. Click **NSS Management > Add NSS Account**.
4. 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.
5. At the login page, provide your NetApp Support Site registered email address and password to perform the authentication process.

This action enables Cloud Manager to use your NSS account.

Note the account must be a customer-level account (not a guest or temp account).

Register your account for support

Support registration is available from Cloud Manager in the Support Dashboard.

Steps

1. In the upper right of the Cloud Manager console, click the Help icon, and select **Support**.



2. In the **Resources** tab, click **Register for Support**.
3. Select the NSS credentials that you want to register and then click **Register**.

Get help

NetApp provides support for Cloud Manager 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.

Self support

These options are available for free, 24 hours a day, 7 days a week:

- [Knowledge base](#)

Search through the Cloud Manager knowledge base to find helpful articles to troubleshoot issues.

- [Communities](#)

Join the Cloud Manager community to follow ongoing discussions or create new ones.

- [Documentation](#)

The Cloud Manager documentation that you're currently viewing.

- [Feedback email](#)

We value your input. Submit feedback to help us improve Cloud Manager.

NetApp support

In addition to the self-support options above, you can work with a NetApp Support Engineer to resolve any issues after you activate support.

Steps

1. In Cloud Manager, click **Help > Support**.
2. Choose one of the available options under Technical Support:
 - a. Click **Call Us** to find phone numbers for NetApp technical support.
 - b. Click **Open an Issue**, select one the options, and then click **Send**.

A NetApp representative will review your case and get back to you soon.

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 Cloud Manager 3.9](#)

Copyright Information

Copyright © 2022 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.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

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.