



# **Cloud Manager and Cloud Volumes ONTAP documentation**

## **Cloud Manager**

NetApp

February 28, 2021

# Table of Contents

Cloud Manager and Cloud Volumes ONTAP documentation .....	1
Discover what's new .....	1
Get started .....	1
Automate with APIs .....	1
Connect with peers, get help, and find more information .....	1
Release notes .....	2
Cloud Manager .....	2
Important changes in Cloud Manager .....	20
Cloud Volumes ONTAP AMI change .....	20
SaaS changes .....	20
Machine type changes .....	20
Account settings .....	20
New permissions .....	21
New endpoints .....	23
Get started with Cloud Manager .....	24
Learn about Cloud Manager .....	24
Networking overview .....	25
Signing up to NetApp Cloud Central .....	26
Logging in to Cloud Manager .....	27
Set up a Cloud Central account .....	27
Set up a Connector .....	37
Where to go next .....	56
Manage Cloud Volumes ONTAP .....	57
Learn .....	57
Get started in AWS .....	89
Get started in Azure .....	127
Get started in GCP .....	146
Provision and manage storage .....	175
Replicating data between systems .....	206
Monitor performance .....	213
Improving protection against ransomware .....	221
Administer .....	222
Provision volumes using a file service .....	246
Azure NetApp Files .....	246
Cloud Volumes Service for AWS .....	256
Cloud Volumes Service for GCP .....	280
Manage ONTAP clusters .....	296
Discovering ONTAP clusters .....	296
Monitoring ONTAP clusters .....	297
Managing storage for ONTAP clusters .....	298
Back up to the cloud .....	301
Learn about Cloud Backup .....	301
Get started .....	307

Managing backups for Cloud Volumes ONTAP and on-premises ONTAP systems . . . . .	328
Restoring data from backup files . . . . .	332
Copy and synchronize data . . . . .	341
Cloud Sync overview . . . . .	341
Get started . . . . .	344
Tutorials . . . . .	376
Managing sync relationships . . . . .	387
Manage data brokers . . . . .	392
Uninstalling the data broker . . . . .	397
Cloud Sync APIs . . . . .	397
Cloud Sync technical FAQ . . . . .	400
Gain insight into data privacy . . . . .	407
Learn about Cloud Compliance . . . . .	407
Get started . . . . .	411
Viewing details about the private data stored in your organization . . . . .	443
Managing your private data . . . . .	454
Adding personal data identifiers using Data Fusion . . . . .	464
Viewing compliance reports . . . . .	466
Responding to a Data Subject Access Request . . . . .	471
Categories of private data . . . . .	473
Removing data sources from Cloud Compliance . . . . .	478
Frequently asked questions about Cloud Compliance . . . . .	480
Enable real-time global file sharing . . . . .	485
Learn about Global File Cache . . . . .	485
Before you begin to deploy Global File Cache . . . . .	489
Getting started . . . . .	492
Before you begin to deploy Global File Cache Edge instances . . . . .	504
Deploy Global File Cache Edge instances . . . . .	510
End-user training . . . . .	513
Additional information . . . . .	513
Optimize cloud compute costs . . . . .	515
Learn about the Compute service . . . . .	515
Start optimizing your cloud compute costs . . . . .	516
Tier data to the cloud . . . . .	519
Learn about Cloud Tiering . . . . .	519
Get started . . . . .	523
Set up licensing for Cloud Tiering . . . . .	544
Measure network latency and throughput performance . . . . .	546
Managing data tiering from your clusters . . . . .	547
Get an overview of data tiering from your clusters . . . . .	550
Cloud Tiering technical FAQ . . . . .	551
Reference . . . . .	554
Viewing your Amazon S3 buckets . . . . .	558
Administer Cloud Manager . . . . .	560
Finding your Cloud Manager system ID . . . . .	560

Manage Connectors . . . . .	560
Manage credentials . . . . .	575
Managing users, workspaces, Connectors, and subscriptions . . . . .	599
Managing an HTTPS certificate for secure access . . . . .	605
Removing Cloud Volumes ONTAP working environments . . . . .	607
Configuring a Connector to use a proxy server . . . . .	608
Reference . . . . .	609
Automate with the API and IaC tools . . . . .	620
Automation resources for infrastructure as code . . . . .	620
Where to get help and find more information . . . . .	621
Earlier versions of Cloud Manager documentation . . . . .	623
Legal notices . . . . .	624
Copyright . . . . .	624
Trademarks . . . . .	624
Patents . . . . .	624
Privacy policy . . . . .	624
Open source . . . . .	624

# Cloud Manager and Cloud Volumes ONTAP documentation

Cloud Manager enables IT experts and cloud architects to centrally manage their hybrid multi-cloud infrastructure using NetApp's cloud solutions.

## Discover what's new

- [Important changes in Cloud Manager](#)
- [What's new in Cloud Manager](#)
- [What's new in Cloud Volumes ONTAP](#)

## Get started

- [Cloud Manager](#)
- [Account settings](#)
- [Cloud Volumes ONTAP for AWS](#)
- [Cloud Volumes ONTAP for Azure](#)
- [Cloud Volumes ONTAP for Google Cloud](#)
- [Azure NetApp Files](#)
- [Cloud Volumes Service for AWS](#)
- [Cloud Volumes Service for Google Cloud](#)
- [Cloud Compliance](#)
- [Global File Cache](#)
- [Cloud Backup](#)
- [Cloud Analyzer](#)
- [Cloud Tiering](#)
- [Cloud Insights](#)
- [Active IQ](#)

## Automate with APIs

- [API Developer Guide](#)
- [Automation resources for infrastructure as code](#)

## Connect with peers, get help, and find more information

- [NetApp Community: Cloud Data Services](#)
- [NetApp Cloud Volumes ONTAP Support](#)
- [Where to get help and find more information](#)

# Release notes

## Cloud Manager

### What's new in Cloud Manager 3.9

Cloud Manager typically introduces a new release every month to bring you new features, enhancements, and bug fixes.



Looking for a previous release?

[What's new in 3.8](#)

[What's new in 3.7](#)

### Cloud Manager 3.9.3 update (16 Feb 2021)

#### Cloud Backup Service enhancements

- Now you can restore volumes to on-premises ONTAP systems from backup files that reside in Amazon S3, Azure Blob, and Google Cloud Storage.
- A new Restore Dashboard has been added that provides details about all the volumes and files you have restored.

The Dashboard is also the starting place to perform all volume and file restore operations. See [the Restore Dashboard](#) for details. In previous releases the restore volumes option was included in the Backup Dashboard.

- Cloud Backup is now supported on Cloud Volumes ONTAP HA systems in Google Cloud.

### Cloud Manager 3.9.3 update (14 Feb 2021)

#### Cloud Compliance enhancements

- View and manage Azure Information Protection (AIP) labels in files you are scanning.
  - After you integrate the AIP label functionality into Cloud Compliance, you can view the labels that are assigned to files, add labels to files, and change labels. See [how to integrate AIP labels](#) in your workspace.
  - Assign labels individually to files, or use the Highlights functionality to [add labels to all files that match the Highlight criteria](#). With Highlights, labels are updated continuously as Cloud Compliance finds matches in your files.
  - Filter data in the Investigation page by AIP label to view all files that match the label.
- Send email alerts to Cloud Manager users (daily, weekly, or monthly) when any of your Highlights return results so you can get notifications to protect your data.

Select this option when [creating or editing any highlight](#).

- View File Owner and Permission information when [viewing individual file details](#).

You can also use this criteria to further filter your data in the Investigation page.

- Delete files directly from Cloud Compliance.

You can [permanently remove files](#) that seem insecure or risky to leave in your storage system.

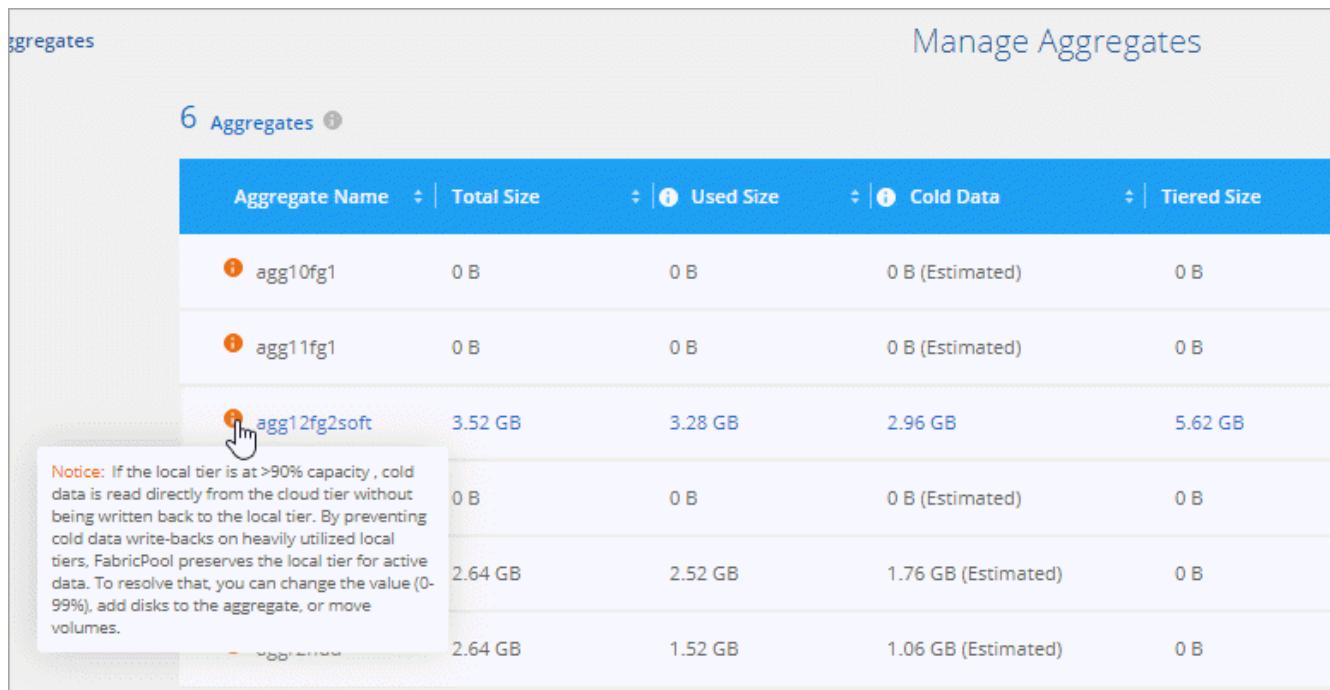
## Cloud Manager 3.9.3 update (10 Feb 2021)

- [Cloud Tiering enhancements](#)
- [Cloud Sync enhancements](#)

### Cloud Tiering enhancements

- Cloud Tiering now activates write-back prevention on a cluster when an aggregate is at >90% capacity (70% for ONTAP 9.6 and earlier). By preventing cold data write-backs on heavily utilized local tiers, Cloud Tiering preserves the local tier for active data.

When this happens, an indication appears in the Manage Aggregates table.



The screenshot shows a table titled "Manage Aggregates" with 6 entries. The columns are: Aggregate Name, Total Size, Used Size, Cold Data, and Tiered Size. The "Cold Data" column includes a tooltip: "Notice: If the local tier is at >90% capacity , cold data is read directly from the cloud tier without being written back to the local tier. By preventing cold data write-backs on heavily utilized local tiers, FabricPool preserves the local tier for active data. To resolve that, you can change the value (0-99%), add disks to the aggregate, or move volumes." The "Cold Data" value for agg12fg2soft is 2.96 GB.

Aggregate Name	Total Size	Used Size	Cold Data	Tiered Size
agg10fg1	0 B	0 B	0 B (Estimated)	0 B
agg11fg1	0 B	0 B	0 B (Estimated)	0 B
agg12fg2soft	3.52 GB	3.28 GB	2.96 GB	5.62 GB
	0 B	0 B	0 B (Estimated)	0 B
	2.64 GB	2.52 GB	1.76 GB (Estimated)	0 B
	2.64 GB	1.52 GB	1.06 GB (Estimated)	0 B

- You can now add on-prem ONTAP clusters more easily from the Cloud Tiering service.

When you click **Add cluster** from the Cloud Tiering page, you're now sent directly to the **Add Working Environment** wizard.

- You can now filter the Timeline to show actions specific to the Cloud Tiering service.

The screenshot shows the Timeline interface with a filter overlay. The filter bar at the top includes tabs for Time (1), Service (1), Action, Agent (1), Resource, User, Status, and a dropdown for 'Rese'. A dropdown menu is open under 'Service' with two options: 'Cloud Manager' (unchecked) and 'Cloud Tiering' (checked). Below the dropdown are 'Clear' and 'Apply' buttons. To the right of the filter bar, there are buttons for 'Service' and 'Agent' with dropdown arrows. At the bottom right of the interface is a small icon representing a file or document.

### Cloud Sync enhancements

- We've simplified the process for syncing data to or from Cloud Volumes ONTAP. You can now select a Cloud Volumes ONTAP working environment and choose an option to sync data to or from this working environment.

The screenshot shows the Canvas interface. On the left, there's a 'CloudVolumesONTAP' cloud icon labeled 'SINGLE' containing 'Cloud Volumes ONTAP' and '51 GiB Capacity'. An 'aws' logo is at the bottom right of the cloud. On the right, there's a list of configurations for 'CloudVolumesONTAP':

- Compliance: Off (button to 'Enable')
- Monitoring: On (button to 'Sync data from this location')
- File Cache: Off (button to 'Sync data to this location')
- Sync: On (button to 'View Dashboard')
  - 559.16TiB Data Synced

- In the last release, we introduced a new Reports feature that provides information that you can use with the help of NetApp personnel to tune a data broker's configuration and improve performance. These reports are now supported with object storage.

## Cloud Manager 3.9.3 (9 Feb 2021)

- Monitoring enhancements
- Support improvements

### Monitoring enhancements

- The Monitoring service is now supported with Cloud Volumes ONTAP for Azure.
- The Monitoring service is also supported in Government regions in AWS and Azure.

The Monitoring service gives you complete visibility into your Cloud Volumes ONTAP infrastructure. Enable the service to monitor, troubleshoot, and optimize your Cloud Volumes ONTAP resources.

[Learn more about the Monitoring service.](#)

### Support improvements

We've updated the Support Dashboard by enabling you to add your NetApp Support Site credentials, which registers you for support. You can also initiate a NetApp Support case directly from the dashboard. Just click the Help icon and then **Support**.

The screenshot shows the 'Support Dashboard' interface. At the top, there are tabs for 'Account' (which is selected) and 'Connector'. Below the tabs, there's a section for 'Support Registration' showing a green checkmark and the text 'Registered for Support'. It includes links to 'View Active NSS Credentials', 'Learn More', and a prominent blue button labeled 'Add NSS Credentials'. The main area is divided into several sections: 'Documentation' (with a link to 'Cloud Manager Documentation'), 'Knowledge Base' (with a link to 'Knowledge Base'), 'Communities' (with a link to 'Communities'), 'Feedback' (with a link to 'Feedback'), 'API' (with a link to 'API Documentation'), and 'Support' (with a link to 'Open an Issue'). Each section has a small circular icon next to its title.

## Cloud Manager 3.9.2 update (11 Jan 2021)

- Cloud Compliance enhancements

- [Cloud Backup enhancements](#)

## Cloud Compliance enhancements

- Added support for scanning Microsoft OneDrive accounts.

Now you can add your corporate OneDrive accounts to Cloud Compliance in order to scan folders and files from all your OneDrive users. See [scanning OneDrive accounts](#) for details.

- The "Highlights" feature now allows you can create your own custom Highlights that provide results for searches specific to your organization.

In the last release, Cloud Compliance provided a set predefined highlight filters that all users could use. Now you can create your own Highlights to return specific scan results in the Investigation page. See how to [create your own custom highlights](#).

- Ability to scan backup files from on-premises ONTAP systems for free.

If you don't want Cloud Compliance to scan volumes directly on your on-prem ONTAP systems, a new Beta feature released this month allows you to run compliance scans on backup files created from your on-prem ONTAP volumes. So if you're already creating backups of your on-prem ONTAP volumes using [Cloud Backup](#), you can use this new feature to run compliance scans on those backup files - for **FREE**.

See how to [back up on-prem ONTAP volumes to object storage](#) and how you can [scan those backup files](#).

- Cloud Compliance can now find the personal data type "IP Address" in files. See the list of all [personal data types](#) that Cloud Compliance finds in scans.

## Cloud Backup enhancements

You can restore individual files to additional destination working environments:

- Backup files in Azure Blob can be used to restore individual files to Cloud Volumes ONTAP systems installed on Azure, and to on-premises ONTAP systems.
- Backup files in Amazon S3 can be used to restore individual files to on-premises ONTAP systems (restoring files to Cloud Volumes ONTAP systems installed on AWS was already supported).

View the [backup and restore matrix](#) to see which working environments are supported for creating backups, restoring volumes, and restoring files.

## Cloud Manager 3.9.2 (4 Jan 2021)

- [Cloud Volumes ONTAP enhancements](#)
- [Cloud Tiering enhancements](#)
- [General enhancements](#)

## Cloud Volumes ONTAP enhancements

This release of Cloud Manager introduces the following enhancements for Cloud Volumes ONTAP.

## Support for AWS Outposts

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

## Cloud Volumes ONTAP with AWS Outposts.

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

There are a few limitations to point out:

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

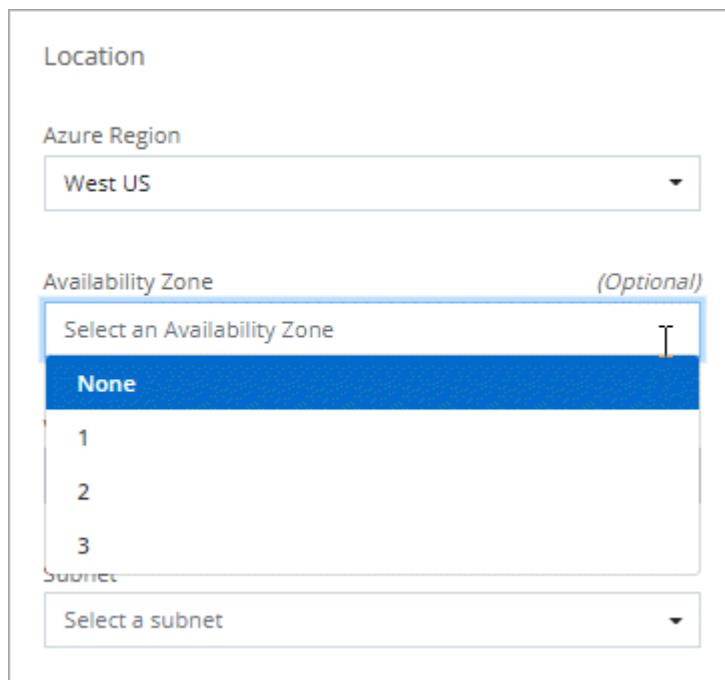
## Support for Ultra SSD VNVRAM in all supported Azure regions

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

VNVRAM provides better write performance.

## Ability to choose an Availability Zone in Azure

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



## Support for bigger disks and new instances in GCP

- 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.

- 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

### Cloud Tiering enhancements

- A new Cloud Performance Test gives you the ability to measure network latency and throughput performance from an ONTAP cluster to an object store before and after setting up data tiering.

**Your cluster performance results**

Node: Node A      Last Check: 11/14/2020 08:54 am      [↻ Recheck Performance](#)

Operation	Size	Avg. Latency (ms)	Throughput
Write	4 KB	17687	337.5 MB
Read	8 KB	5348	14.33 MB
Read	8 KB	5568	27.98 MB
Read	32 KB	5668	108.5 MB
Read	256 KB	5809	706.8 MB

**Notice:** We recommend that you run this check when the cluster is under 50% CPU utilization.

- The Tiering Setup wizards were redesigned for ease of use.

### Additional enhancements

- New Support Dashboard

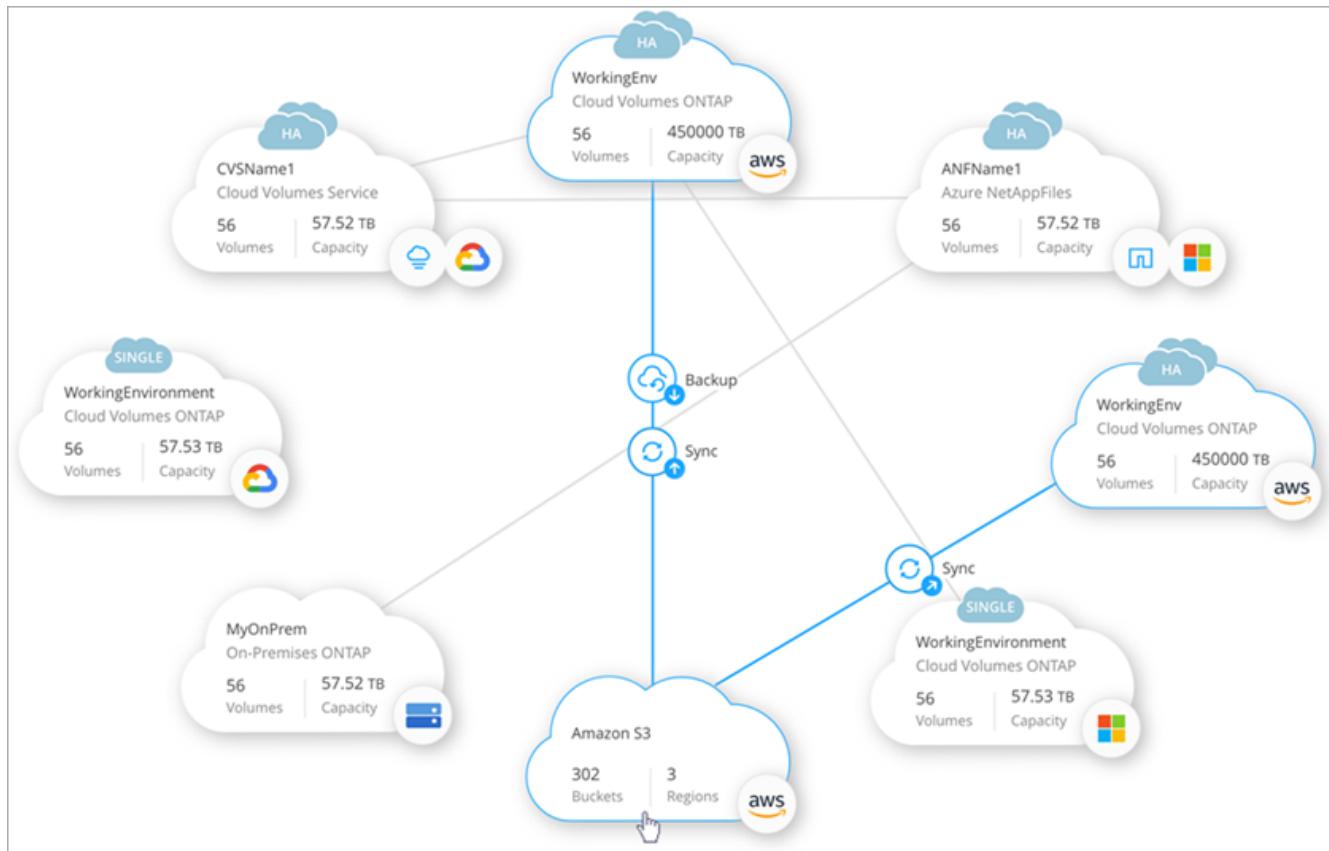
In the Help menu, a new Support Dashboard includes links to resources that can enable you to get help, submit feedback, and contact NetApp Support. You can also send and download AutoSupport messages from the **Connector AutoSupport** tab.

The screenshot shows the Support Dashboard interface. At the top, there are tabs for 'Support Dashboard', 'Account' (which is selected), and 'Connector'. Below the tabs, there's a section for 'Account serial number' with the value '960002998664...'. A green checkmark icon indicates 'Registered for Support' under 'Support Registration'. There are buttons for 'View Active NSS Credentials', 'Learn More', and 'Add NSS Credentials'. The main content area is divided into several sections: 'Documentation' (with a link to 'Cloud Manager Documentation'), 'Knowledge Base' (with a link to 'Knowledge Base'), 'Communities' (with a link to 'Communities'), 'Feedback' (with a link to 'Feedback'), 'API' (with a link to 'API Documentation'), and 'Support' (with a link to 'Open an Issue').

- Visual representation between working environments

Cloud Manager makes it easier to view the relationships between the services enabled on your working environments.

For example, the following image shows an example of two working environments where data is backed up from Cloud Volumes ONTAP to Amazon S3, and where data is synced between Amazon S3 and two Cloud Volumes ONTAP systems.



## Cloud Manager 3.9.1 (7 Dec 2020)

- General enhancements
- Cloud Volumes ONTAP AMI change
- Cloud Backup enhancements
- Cloud Compliance enhancements
- Cloud Tiering enhancements
- Cloud Sync enhancements

### General enhancements

- We've renamed the **Working Environments** tab to **Canvas**.

This tab starts as a blank canvas and enables you to add your working environments by deploying, allocating, and discovering storage across your hybrid cloud.

The screenshot shows the Cloud Manager 3.9.0 interface. At the top, there's a navigation bar with tabs: Canvas (selected), Replication, Backup, Sync, K8s, Compliance, File Cache, Compute, and All Services (+6). Below the navigation bar is a "Canvas" section with a "Add Working Environment" button. It displays four cloud environments: "CVOAzure" (Azure, West US, 0.29 TB Allocated Capacity), "AzureNetAppFiles" (Azure NetApp Files, 1 Volumes, 500.00 GB Capacity), "CVVAHA1" (AWS, US-EAST-1B, HA, 0.59 TB Allocated Capacity), and "Amazon S3" (AWS, 89 Buckets, 1 Regions). To the right is a "Working Environments" section listing five items: 1 On-Premises (1 TB Allocated Capacity), 1 Cloud Volume ONTAP (High-Availability) (0.59 TB Allocated Capacity), 1 Cloud Volumes ONTAP (0.29 TB Allocated Capacity), 1 Azure NetApp Files (0.00 Byte Allocated Capacity), and 1 Amazon S3 (89 Buckets). A "Visual View" button is in the top right corner.

- It's now easier to navigate between Cloud Manager and Spot.

A new **Storage Operations** section in Spot enables you to navigate directly to Cloud Manager. After you're done, you can get back to Spot from the **Compute** tab in Cloud Manager.

#### Cloud Volumes ONTAP AMI change

Starting with the 9.8 release, the Cloud Volumes ONTAP PAYGO AMI is no longer available in the AWS Marketplace. If you use the Cloud Manager API to deploy Cloud Volumes ONTAP PAYGO, you'll need to [subscribe to the Cloud Manager subscription in the AWS Marketplace](#) before deploying a 9.8 system.

#### Cloud Backup enhancements

- You now have the ability to restore individual files from a backup file.
  - If you need to restore a few files from a certain point in time, now you can just restore those files instead of having to restore the whole volume.
  - You can restore the files to a volume in the same working environment, or to a volume in a different working environment that's using the same cloud account.
  - This single file restore option relies on a new Cloud Restore instance that is deployed in your environment. [Go here for details about this new functionality.](#)
- You can configure Cloud Backup in a Google Cloud environment now while deploying a new Cloud Volumes ONTAP system. In the past you could only configure Cloud Backup on existing Cloud Volumes ONTAP systems.
- Now you can restore volumes that you had backed up from on-prem ONTAP systems to Cloud Volumes ONTAP systems deployed in AWS or Azure.

## Cloud Compliance enhancements

- Ability to scan data directly from your on-premises ONTAP clusters

If you have discovered your on-prem clusters in Cloud Manager, now you can run Compliance scans directly on those volumes. No longer do you have to copy those volumes to a Cloud Volumes ONTAP system before you can run a Compliance scan.

- Ability to install Cloud Compliance in your on-premises location

If you plan to scan on-premises ONTAP cluster data, now you can install Cloud Compliance on-premises as well. It is still integrated in the Cloud Manager UI and it can still be used to scan other working environments, including cloud based volumes, buckets, and databases.

[See the prerequisites and installation steps here.](#)

- Ability to easily scan CIFS data protection volumes

In the past you have been able to scan NFS DP volumes. This release allows you to easily scan CIFS DP volumes directly within Cloud Compliance. [Learn how.](#)

- A new "Highlights" feature provides a predefined selection of combination filters that return results in the Investigation page

Ten highlights are available with this release. For example, the "HIPAA – Stale data over 30 days" highlight identifies files that contain Health information that is over 30 days old. [See the full list of predefined highlights.](#)

You can select Highlights from a tab in the Compliance Dashboard and as a filter in the Investigation page.

- Cloud Compliance can now find the sensitive personal data type "Political Opinions Reference" in files. See the list of all [sensitive personal data types](#) that Cloud Compliance finds in scans.
- A new filter for "file size" is available from the Investigation page to refine your search results for files of a certain size

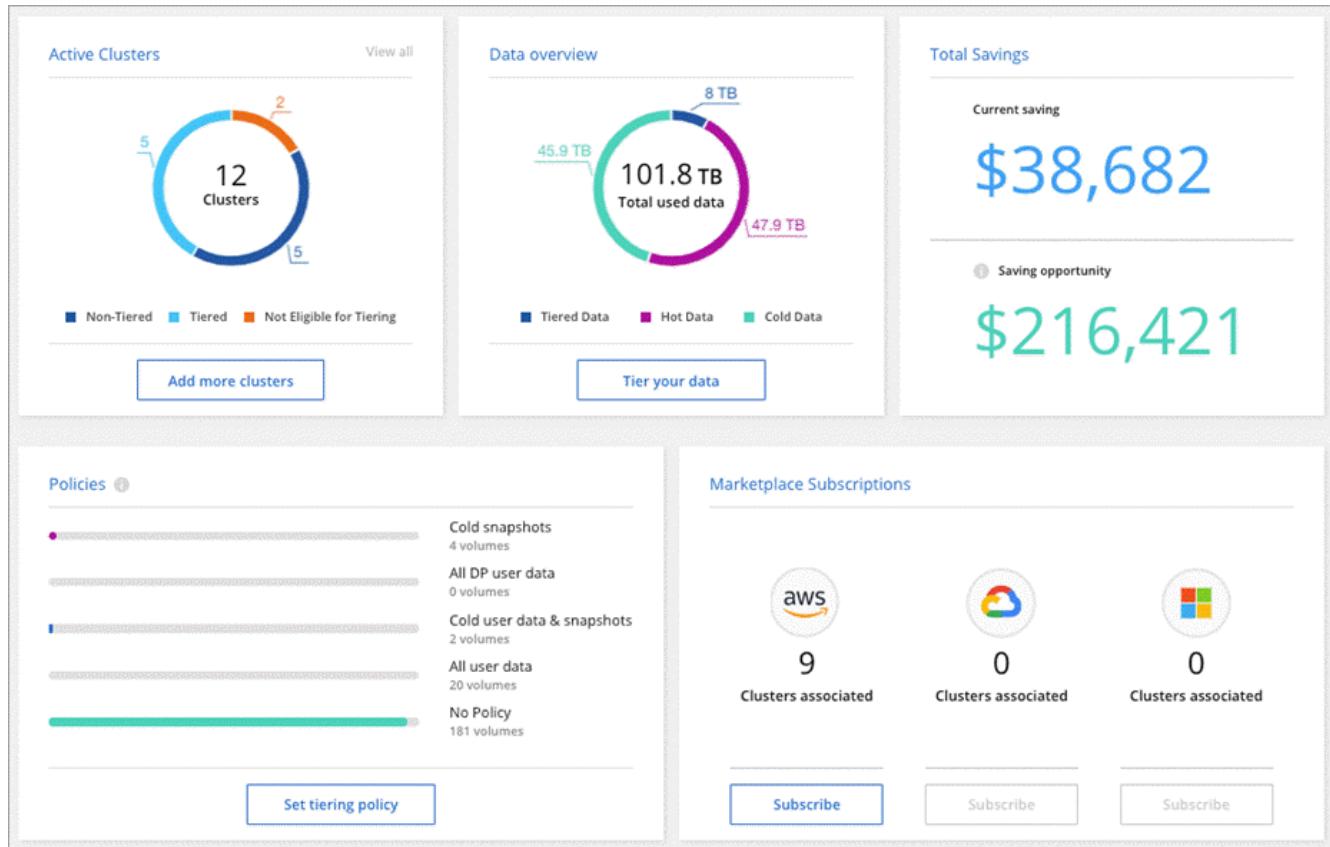
Note that the list of required endpoints for Cloud Compliance deployments has been revised based on cloud provider. [Review this list for AWS, Azure, and on-prem requirements.](#)

## Cloud Tiering enhancements

- You can now change the tiering policy and minimum cooling days for multiple volumes at the same time.

Volume Name	SVM Name	Volume Size	Used Size	Snapshot Used Size	Cold Data	Tier Status	Tiering Policy
vol1	svm_AFF1	50 GB	3.54 MB	444 KB	2.47 MB	70 %	Tiered Volume
vol2	svm_AFF1	200 GB	1 MB	0 B	716.8 KB	70 %	Tiered Volume
vol3	svm_AFF1	200 GB	1 MB	0 B	716.8 KB	70 %	Tiered Volume

- Cloud Tiering now provides an aggregated view of data tiering from each of your on-premises clusters. This overview provides a clear picture of your environment and enables you to take proper actions. [Learn more about this page.](#)



## Cloud Sync enhancements

- You can now manage data broker groups.

Grouping data brokers together can help improve the performance of sync relationships. Manage groups by adding a new data broker to a group, viewing information about data brokers, and more.

[Learn how to manage data brokers.](#)

- Cloud Sync now supports an ONTAP S3 Storage to ONTAP S3 Storage sync relationship.

[View the entire list of supported sources and targets.](#)

## Cloud Manager 3.9 Update (18 Nov 2020)

Cloud Backup is now supported on Cloud Volumes ONTAP in Google Cloud. Click [here](#) for details.

**Note:** Only single-node systems are currently supported.

## Cloud Volumes ONTAP 9.8 (16 Nov 2020)

Cloud Volumes ONTAP 9.8 is available in AWS, Azure, and Google Cloud Platform. This release includes support for [HA pairs in GCP](#).



The GCP service account associated with the Connector [needs the latest permissions](#) to deploy an HA pair in GCP.

[Learn what else is new in Cloud Volumes ONTAP 9.8.](#)

## Cloud Manager 3.9 update (8 Nov 2020)

We released an enhancement to Cloud Manager 3.9.

### Cloud Compliance enhancements

- Now you can create custom personal data identifiers from your databases. This gives you the full picture about where potentially sensitive data resides in **all** your files.

A feature we call "Data Fusion" allows you to scan your files to identify whether unique identifiers from your databases are found in those files—basically making your own list of "personal data" that is identified in Cloud Compliance scans.

[Learn how to create custom personal identifiers from your databases.](#)

- Added support for scanning MySQL database schemas.

Go to [scanning database schemas](#) for the list of all supported databases and for instructions.

## Cloud Manager 3.9 (3 Nov 2020)

- [Azure Private Link for Cloud Volumes ONTAP](#)
- [Active IQ cluster insights](#)
- [Cloud Tiering enhancements](#)

### Azure Private Link for Cloud Volumes ONTAP

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

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

### Active IQ cluster insights

Active IQ cluster insights are now available within Cloud Manager. This initial release provides the following functionality:

- Shows a list of your on-prem clusters based on your NetApp Support Site (NSS) credentials.
- Identifies which of those clusters have been discovered within Cloud Manager, and those that have not been discovered.
- Enables you to view unused Cloud Volumes ONTAP licenses.
- Identifies if any of your discovered ONTAP clusters need to have their shelf or disk firmware updated.

Go to [Monitoring ONTAP clusters](#) for details. This information is provided to Cloud Manager from the [Active IQ Digital Advisor](#).

### Cloud Tiering enhancements

- When you set up data tiering from your volumes, Cloud Tiering now identifies the Snapshot used size for each volume. This information can help you decide which type of data to tier to the cloud.

Tier Volumes		Tier volumes				Learn how much you can save with each Tiering Policy	
50 Volumes						Search	
Volume Name	SVM Name	Volume Size	Used Size	Snapshot used size	Cold Data (Estimated)	Tier Status	TieringPolicy
Volume 1	SVMNameB...	462 TB	100 TB	50 TB	70 TB   70%	Available for Tiering	Cold User Data

- Cloud Tiering now enables inactive data reporting on HDD aggregates, if the cluster is running ONTAP 9.6 or later.

This enhancement makes it easier for Cloud Tiering to show you the potential savings from tiering cold data.

- Cloud Tiering now prompts you to change thick-provisioned volumes to thin-provisioned volumes, if that's required to enable data tiering on the volumes in an aggregate.

## Cloud Manager transition to SaaS

We've introduced a software-as-a-service experience for Cloud Manager. This new experience makes it easier for you to use Cloud Manager and enables us to provide additional features to manage your hybrid cloud infrastructure.

### The previous Cloud Manager experience

Cloud Manager software was previously comprised of a user interface and a management layer that sent requests to cloud providers. To get started, you would deploy Cloud Manager in your cloud network or on-premises network and then access the user interface that runs on that instance.

That experience has changed.

### The new SaaS experience

The Cloud Manager interface is now accessible through a SaaS-based user interface that you log in to from NetApp Cloud Central. You no longer need to access a user interface from software that runs in your network.

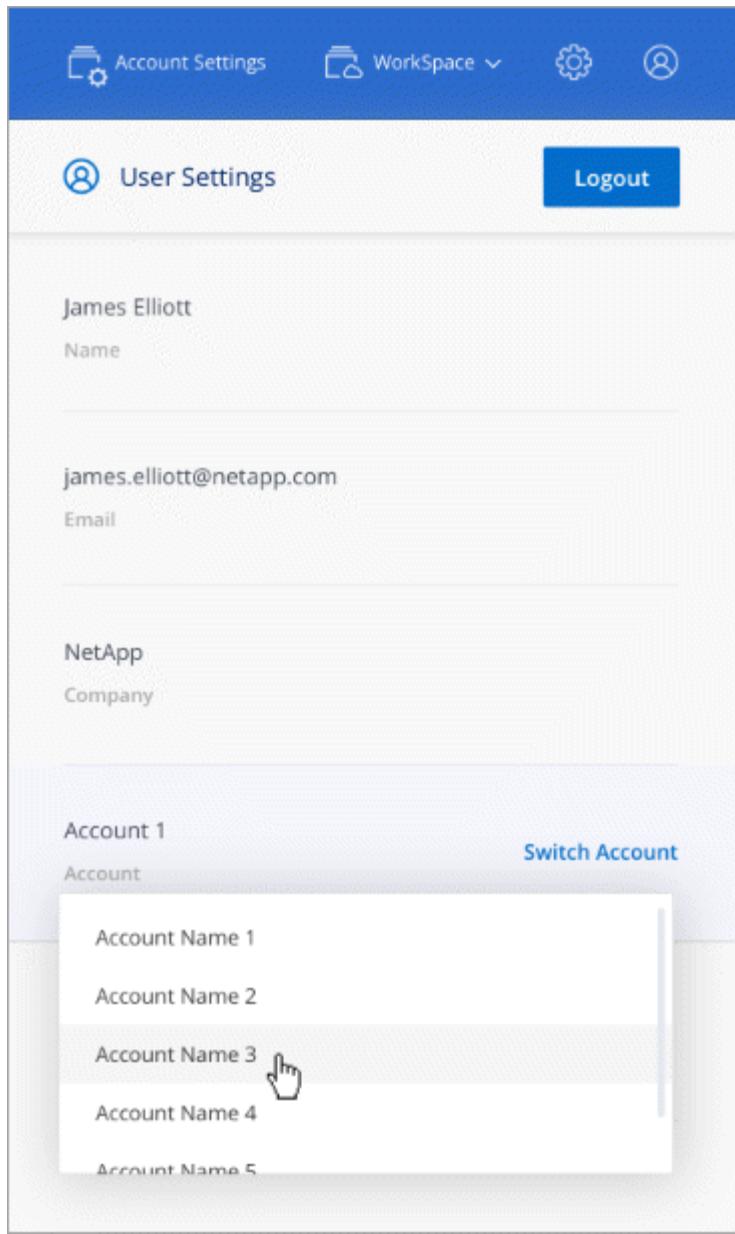
In most cases, you need to deploy a *Connector* in your cloud or on-premises network. The Connector is software that's needed to manage Cloud Volumes ONTAP and other cloud data services. (The Connector is actually the same as the existing Cloud Manager software that you have installed.)

### Benefits

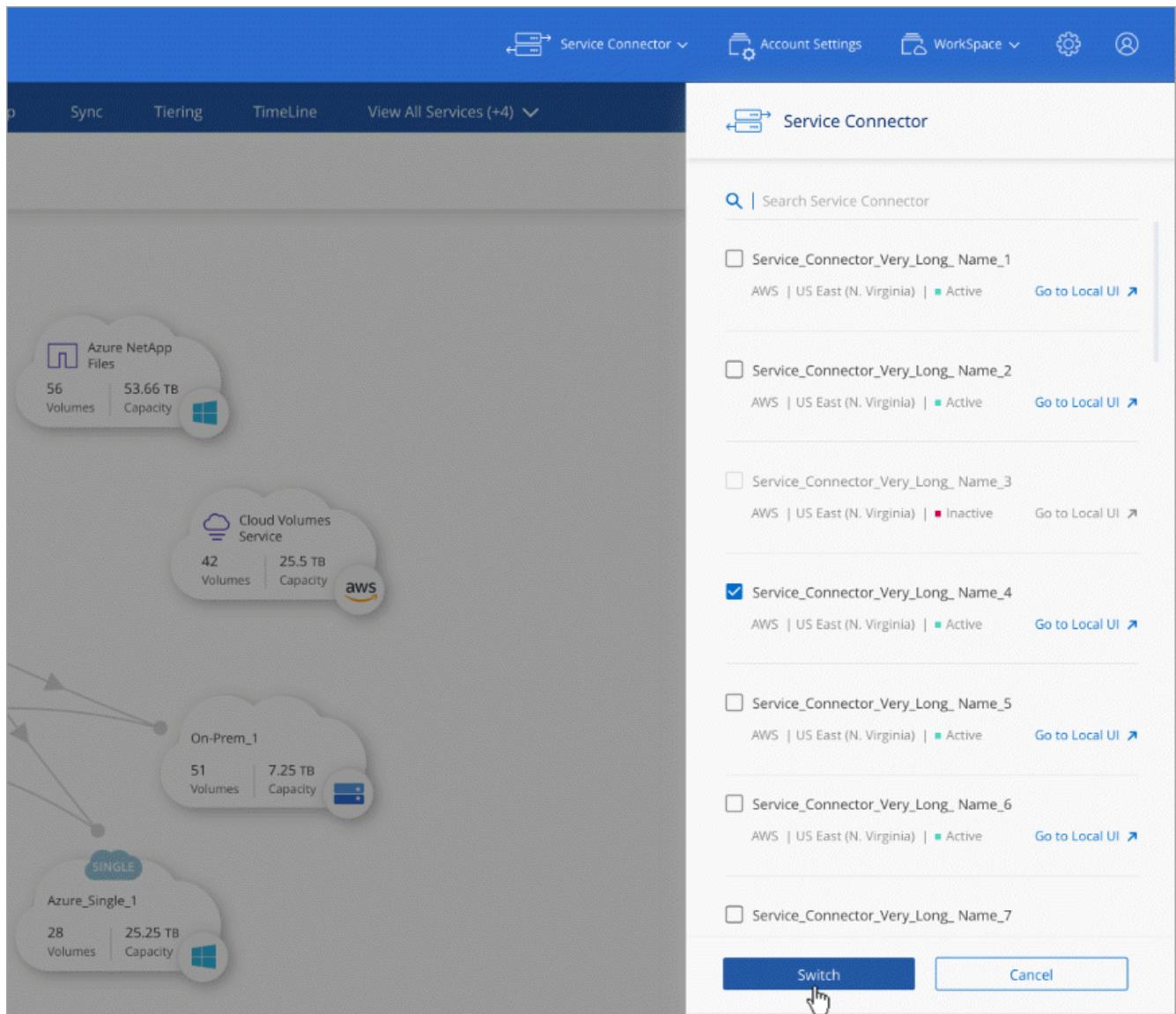
This SaaS-based approach provides several benefits:

- It enables us to offer additional management capabilities for Azure NetApp Files and Cloud Volumes Service without needing to deploy software in your environment.
- You can easily switch between your Cloud Central accounts.

If a user is associated with multiple Cloud Central accounts, they can change to a different account at any time from the User Settings menu. They can then see the Connectors and working environments that are associated with that account.



- You can easily switch between Connectors (what you know today as the Cloud Manager software) that are installed in different networks or different cloud providers.

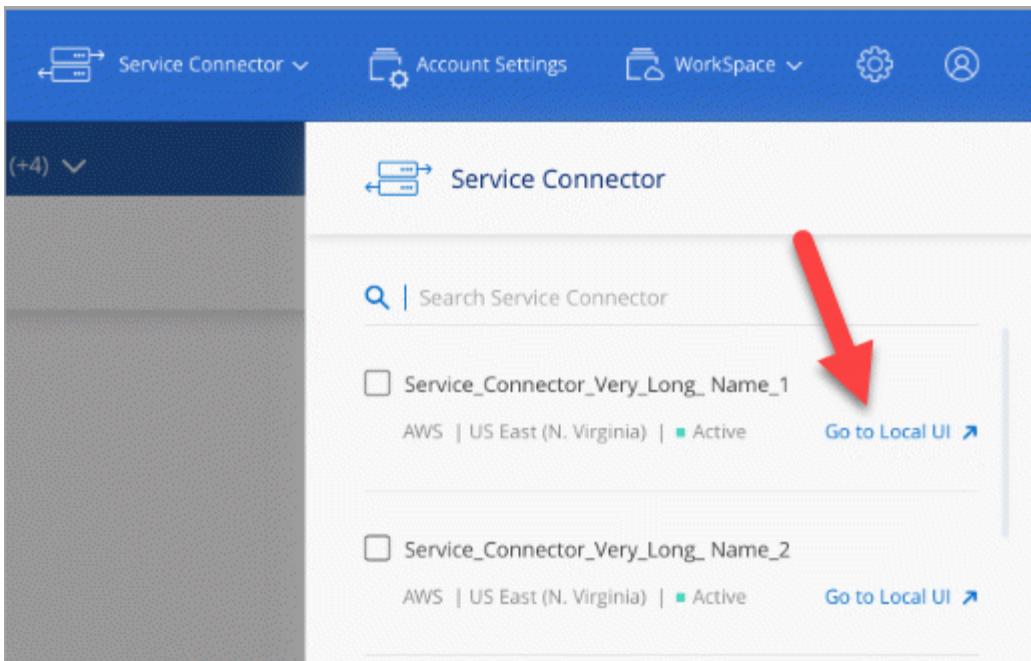


## The local user interface

While you should perform almost all tasks from the SaaS user interface, a local user interface is still available on the Connector. This interface is needed for a few tasks that need to be performed from the Connector itself:

- Setting a proxy server
- Installing a patch
- Downloading AutoSupport messages

You can access the local user interface directly from the SaaS user interface:



## Instance, VM, and machine type changes

To ensure that adequate resources are available for new and upcoming features in Cloud Manager, we've changed the minimum required instance, VM, and machine type as follows:

- AWS: t3.xlarge
- Azure: DS3 v2
- GCP: n1-standard-4

When you upgrade the machine type, you'll get access to features like a new Kubernetes experience, Global File Cache, Monitoring, and more.

These default sizes are the minimum supported [based on CPU and RAM requirements](#).

Cloud Manager will prompt you with instructions to change the machine type of the Connector.

## Known issues

Known issues identify problems that might prevent you from using this release of the product successfully.

There are no known issues in this release of Cloud Manager.

You can find known issues for Cloud Volumes ONTAP in the [Cloud Volumes ONTAP Release Notes](#) and for ONTAP software in general in the [ONTAP Release Notes](#).

## 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.

## **Connectors should remain running**

A Connector should remain running at all times. It's important for the continued health and operation of the services that you enable.

For example, a Connector is a key component in the health and operation of Cloud Volumes ONTAP PAYGO systems. If a Connector is powered down, Cloud Volumes ONTAP PAYGO systems will shut down after losing communication with a Connector for longer than 14 days.

## **SaaS platform is disabled for Government regions**

If you deploy a Connector in an AWS GovCloud region, an Azure Gov region, or an Azure DoD region, access to Cloud Manager is available only through a Connector's host IP address. Access to the SaaS platform is disabled for the entire account.

This means that only privileged users who can access the end-user internal VPC/VNet can use Cloud Manager's UI or API.

It also means that the following services aren't available from Cloud Manager:

- Cloud Compliance
- Kubernetes
- Cloud Tiering
- Global File Cache

The SaaS platform is required to use these services.



The Monitoring service is supported and available in Government regions.

## **Cloud Manager doesn't support downgrades of Cloud Volumes ONTAP**

Cloud Manager doesn't support downgrading Cloud Volumes ONTAP to a previous version. Contact NetApp technical support for help with downgrades.

## **Shared Linux hosts are not supported**

The Connector isn't supported on a host that is shared with other applications. The host must be a dedicated host.

## **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.

# Important changes in Cloud Manager

This page highlights important changes in Cloud Manager that can help you use the service as we introduce new enhancements. You should continue to read the [What's new](#) page to learn about all new features and enhancements.

## Cloud Volumes ONTAP AMI change

Starting with the 9.8 release, the Cloud Volumes ONTAP PAYGO AMI is no longer available in the AWS Marketplace. If you use the Cloud Manager API to deploy Cloud Volumes ONTAP PAYGO, you'll need to [subscribe to the Cloud Manager subscription in the AWS Marketplace](#) before deploying a 9.8 system.

## SaaS changes

We have introduced a software-as-a-service experience for Cloud Manager. This new experience makes it easier for you to use Cloud Manager and enables us to provide additional features to manage your hybrid cloud infrastructure.

- [Cloud Manager transition to SaaS](#)
- [Learn how Cloud Manager works](#)

## Machine type changes

To ensure that adequate resources are available for new and upcoming features in Cloud Manager, we've changed the minimum required instance, VM, and machine type as follows:

- AWS: t3.xlarge
- Azure: DS3 v2
- GCP: n1-standard-4

When you upgrade the machine type, you'll get access to features like a new Kubernetes experience, Global File Cache, Monitoring, and more.

These default sizes are the minimum supported [based on CPU and RAM requirements](#).

Cloud Manager will prompt you with instructions to change the machine type of the Connector.

## Account settings

We introduced Cloud Central accounts to provide multi-tenancy, to help you organize users and resources in isolated workspaces, and to manage access to Connectors and subscriptions.

- [Learn about Cloud Central accounts: users, workspaces, Connectors, and subscriptions](#)
- [Learn how to get started with your account](#)
- [Learn how to manage your account after you set it up](#)

# New permissions

Cloud Manager occasionally requires additional cloud provider permissions as we introduce new features and enhancements. This section identifies new permissions that are now required.

You can find the latest list of permissions on the [Cloud Manager policies page](#).

## AWS

Starting with the 3.8.1 release, the following permissions are required to use Cloud Backup with Cloud Volumes ONTAP. [Learn more](#).

```
{  
    "Sid": "backupPolicy",  
    "Effect": "Allow",  
    "Action": [  
        "s3:DeleteBucket",  
        "s3:GetLifecycleConfiguration",  
        "s3:PutLifecycleConfiguration",  
        "s3:PutBucketTagging",  
        "s3>ListBucketVersions",  
        "s3:GetObject",  
        "s3>ListBucket",  
        "s3>ListAllMyBuckets",  
        "s3:GetBucketTagging",  
        "s3:GetBucketLocation",  
        "s3:GetBucketPolicyStatus",  
        "s3:GetBucketPublicAccessBlock",  
        "s3:GetBucketAcl",  
        "s3:GetBucketPolicy",  
        "s3:PutBucketPublicAccessBlock"  
    ],  
    "Resource": [  
        "arn:aws:s3:::netapp-backup-*"  
    ]  
}
```

## Azure

- To avoid Azure deployment failures, make sure that your Cloud Manager policy in Azure includes the following permission:

```
"Microsoft.Resources/deployments/operationStatuses/read"
```

- Starting with the 3.8.7 release, the following permission is required to encrypt Azure managed disks on single node Cloud Volumes ONTAP systems using external keys from another account. [Learn more](#).

```
"Microsoft.Compute/diskEncryptionSets/read"
```

- The following permissions are required to enable Global File Cache on Cloud Volumes ONTAP. [Learn more](#).

```
"Microsoft.Resources/deployments/operationStatuses/read",
"Microsoft.Insights/Metrics/Read",
"Microsoft.Compute/virtualMachines/extensions/write",
"Microsoft.Compute/virtualMachines/extensions/read",
"Microsoft.Compute/virtualMachines/extensions/delete",
"Microsoft.Compute/virtualMachines/delete",
"Microsoft.Network/networkInterfaces/delete",
"Microsoft.Network/networkSecurityGroups/delete",
"Microsoft.Resources/deployments/delete",
```

## GCP

### New permissions for HA pairs

Starting with the 3.9 release, the service account for a Connector requires additional permissions to deploy a Cloud Volumes ONTAP HA pair in GCP:

- compute.addresses.list
- compute.backendServices.create
- compute.networks.updatePolicy
- compute.regionBackendServices.create
- compute.regionBackendServices.get
- compute.regionBackendServices.list

### New permissions for data tiering

Starting with the 3.9 release, additional permissions are required to set a service account on the Cloud Volumes ONTAP instance. This service account provides permissions for data tiering to a Google Cloud Storage bucket.

- iam.serviceAccounts.actAs
- storage.objects.get
- storage.objects.list

### New permissions for Kubernetes management

Starting with the 3.8.8 release, the service account for a Connector requires additional permissions to discover and manage Kubernetes clusters running in Google Kubernetes Engine (GKE):

- `container.*`

## New permissions for data tiering

Starting with the 3.8 release, the following permissions are now required to use a service account for data tiering. [Learn more about this change.](#)

- `storage.buckets.update`
- `compute.instances.setServiceAccount`
- `iam.serviceAccounts.getIamPolicy`
- `iam.serviceAccounts.list`

## New endpoints

The Connector requires outbound internet access to manage resources and processes within your public cloud environment. This section identifies new endpoints that are now required.

You can find the [full list of endpoints accessed from your web browser here](#) and the [full list of endpoints accessed by the Connector here](#).

- Users need to access Cloud Manager from a web browser by contacting the following endpoint:

<https://cloudmanager.netapp.com>

- Connectors require access to the following endpoint to obtain software images of container components for a Docker infrastructure:

<https://cloudmanagerinfraprod.azurecr.io>

Ensure that your firewall enables access to this endpoint from the Connector.

# Get started with Cloud Manager

## Learn about Cloud Manager

Cloud Manager enables IT experts and cloud architects to centrally manage their hybrid multi-cloud infrastructure using NetApp's cloud solutions.

### Features

Cloud Manager is an enterprise-class, SaaS-based management platform that keeps you in control of your data no matter where it is.

- Set up and use [Cloud Volumes ONTAP](#) for efficient, multi-protocol data management across clouds.
- Set up and use file-storage services: [Azure NetApp Files](#), [Cloud Volumes Service for AWS](#), and [Cloud Volumes Service for Google Cloud](#).
- Discover and manage your on-prem ONTAP clusters by creating volumes, backing up to the cloud, replicating data across your hybrid cloud, and tiering cold data to the cloud.
- Enable integrated cloud services and software like [Cloud Compliance](#), [Cloud Insights](#), [Cloud Backup Service](#), [Trident](#), and more.

[Learn more about Cloud Manager](#).

### Supported object storage providers

Cloud Manager enables you to manage cloud storage and use cloud services in Amazon Web Services, Microsoft Azure, and Google Cloud.

### Cost

Cloud Manager software is free of charge from NetApp.

For most tasks, Cloud Manager prompts you to deploy a Connector in your cloud network, which results in charges from your cloud provider for the compute instance and associated storage. You do have the option to run the Connector software on your premises.

### How Cloud Manager works

Cloud Manager includes a SaaS-based interface that is integrated with NetApp Cloud Central, and Connectors that manage Cloud Volumes ONTAP and other cloud services.

### Software-as-a-service

Cloud Manager is accessible through a [SaaS-based user interface](#) and APIs. This SaaS experience enables you to automatically access the latest features as they're released and to easily switch between your Cloud Central accounts and Connectors.

### NetApp Cloud Central

[NetApp Cloud Central](#) provides a centralized location to access and manage [NetApp cloud services](#). With centralized user authentication, you can use the same set of credentials to access Cloud Manager and other cloud services like Cloud Insights.

When you log in to Cloud Manager for the first time, you're prompted to create a *Cloud Central account*. This account provides multi-tenancy and enables you to organize users and resources in isolated *workspaces*.

## Connectors

In most cases, an Account Admin will need to deploy a *Connector* in your cloud or on-premises network. The Connector enables Cloud Manager to manage resources and processes within your public cloud environment.

A Connector should remain running at all times. It's important for the continued health and operation of the services that you enable.

For example, a Connector is a key component in the health and operation of Cloud Volumes ONTAP PAYGO systems. If a Connector is powered down, Cloud Volumes ONTAP PAYGO systems will shut down after losing communication with a Connector for longer than 14 days.

[Learn more about when Connectors are required and how they work.](#)

## Networking overview

Before users log in to Cloud Manager, you'll need to ensure that their web browsers can access specific endpoints. After that, you need to verify networking requirements for the specific type of working environment and services that will be used.

### Endpoints accessed from your web browser

Users must access Cloud Manager from a web browser. The machine running the web browser must have connections to the following endpoints:

Endpoints	Purpose
<a href="https://cloudmanager.cloud.netapp.com">https://cloudmanager.cloud.netapp.com</a>	To connect you to the Cloud Manager SaaS interface.
<a href="https://api.services.cloud.netapp.com">https://api.services.cloud.netapp.com</a>	To contact Cloud Central APIs.
<a href="https://auth0.com">https://auth0.com</a> <a href="https://cdn.auth0.com">https://cdn.auth0.com</a> <a href="https://netapp-cloud-account.auth0.com">https://netapp-cloud-account.auth0.com</a> <a href="https://services.cloud.netapp.com">https://services.cloud.netapp.com</a>	Your web browser connects to these endpoints for centralized user authentication through NetApp Cloud Central.
<a href="https://widget.intercom.io">https://widget.intercom.io</a>	For in-product chat that enables you to talk to NetApp cloud experts.

### Index of networking requirements

- [Connectors](#)
- [Cloud Volumes ONTAP for AWS](#)
- [Cloud Volumes ONTAP for Azure](#)
- [Cloud Volumes ONTAP for GCP](#)
- [Data replication between ONTAP systems](#)
- [Cloud Compliance for Cloud Volumes ONTAP or Azure NetApp Files](#)
- [Cloud Compliance for Amazon S3](#)

- On-prem ONTAP clusters
  - Data tiering from ONTAP clusters to Amazon S3
  - Data tiering from ONTAP clusters to Azure Blob storage
  - Data tiering from ONTAP clusters to Google Cloud Storage
  - Data tiering from ONTAP clusters to StorageGRID

## Signing up to NetApp Cloud Central

Sign up to NetApp Cloud Central so you can access NetApp's cloud services.

### Steps

1. Open a web browser and go to [NetApp Cloud Central](#).
2. Click **Sign Up**.
3. Fill out the form and click **Sign Up**.

The screenshot shows the 'Log In to NetApp Cloud Central' page. At the top, there is a link 'Already signed up? [Login](#)'. Below it are five input fields: 1. Email: 'user@example.com'. 2. Password: '.....'. 3. Organization: 'NetApp'. 4. First Name: 'New user'. 5. Phone: 'Phone \*optional'. At the bottom, there is a blue 'SIGN UP' button and a checkbox with the text 'I accept the [terms and conditions](#).'. The entire form is contained within a light gray box.

Log In to NetApp Cloud Central

Already signed up? [Login](#)

user@example.com

.....

NetApp

New user

Phone \*optional

**SIGN UP**

I accept the [terms and conditions](#).

4. Wait for an email from NetApp Cloud Central.
5. Click the link in the email to verify your email address.

## Result

You now have an active Cloud Central user login.

## Logging in to Cloud Manager

The Cloud Manager interface is accessible through a SaaS-based user interface by going to <https://cloudmanager.netapp.com>.

### Steps

1. Open a web browser and go to <https://cloudmanager.netapp.com>.
2. Log in using your NetApp Cloud Central credentials.

The screenshot shows the NetApp Cloud Central login interface. At the top left is the NetApp logo. Below it is a large button labeled "Continue to Cloud Manager". The main title "Log In to NetApp Cloud Central" is centered above two input fields: one for "Email" and one for "Password". A large blue "LOGIN" button is positioned below the password field. At the bottom left, there is a link "Forgot your password?".

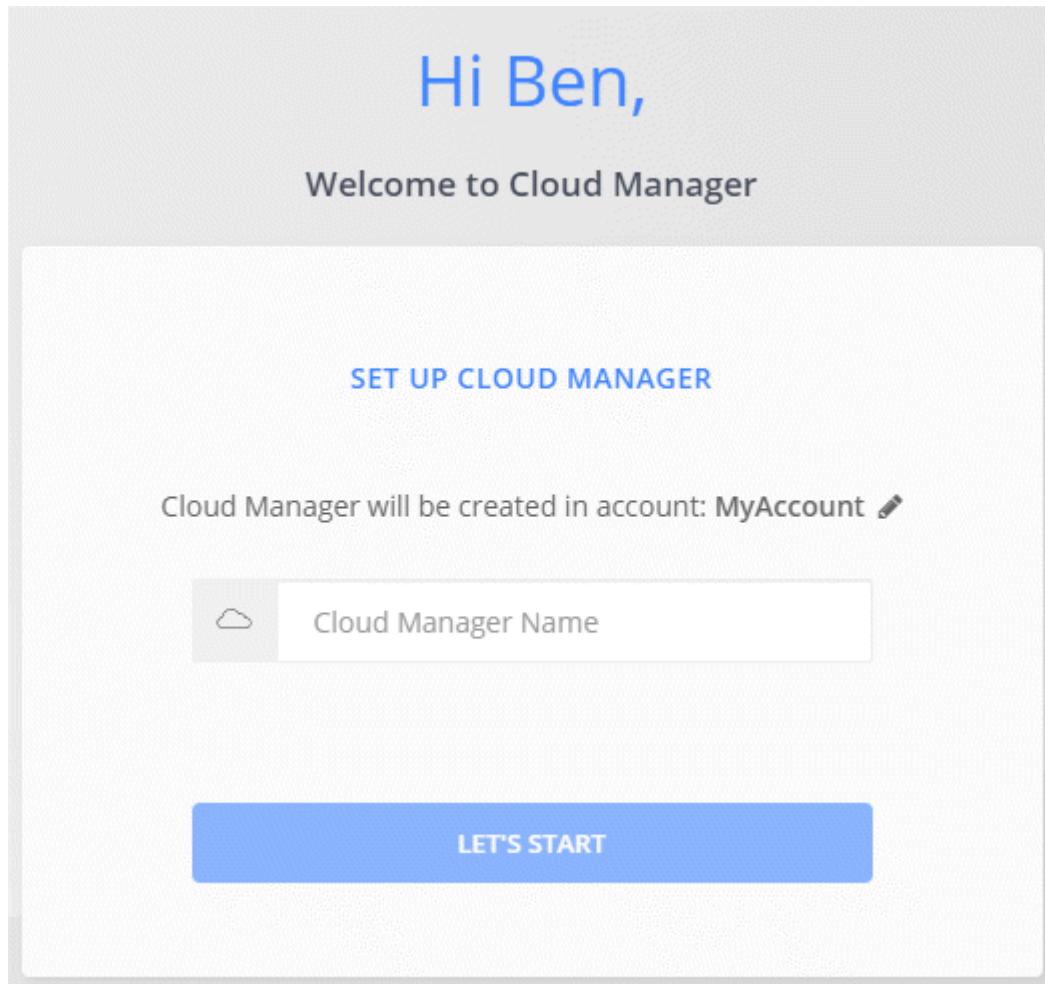
## Set up a Cloud Central account

## Account settings: users, workspaces, Connectors, and subscriptions

A *Cloud Central account* provides multi-tenancy and enables you to organize users and resources in isolated workspaces from within Cloud Manager.

For example, multiple users can deploy and manage Cloud Volumes ONTAP systems in isolated environments called *workspaces*. These workspaces are invisible to other users, unless they are shared.

When you first access Cloud Manager, you're prompted to select or create a Cloud Central account:



Account Admins can then modify the settings for this account by managing users, workspaces, Connectors, and subscriptions:

The screenshot shows the 'Account Settings' page in Cloud Manager. The top navigation bar includes 'Account Settings', 'Users', 'Workspaces' (which is underlined in blue), 'Service Connector', and 'Subscriptions'. Below the navigation is a section titled 'MyAccount' with a cloud icon. A sub-section titled 'Manage the Account's Workspaces' contains a button '+ Add New Workspace'. A table lists two workspaces: 'Workspace-2' and 'Workspace-1', each with a trash can icon and a pencil icon for editing.

For step-by-step instructions, see [Setting up the Cloud Central account](#).

## Account Settings

The Account Settings widget in Cloud Manager enables Account Admins to manage a Cloud Central account. If you just created your account, then you'll start from scratch. But if you've already set up an account, then you'll see *all* the users, workspaces, Connectors, and subscriptions that are associated with the account.

## Users

The users that display in the Account Settings are NetApp Cloud Central users that you associate with your Cloud Central account. Associating a user with an account and one or more workspaces in that account enables those users to create and manage working environments in Cloud Manager.

When you associate a user, you assign them a role:

- *Account Admin*: Can perform any action in Cloud Manager.
- *Workspace Admin*: Can create and manage resources in the assigned workspace.
- *Cloud Compliance Viewer*: Can only view compliance information and generate reports for systems that they have permission to access.

## Workspaces

In Cloud Manager, a workspace isolates any number of *working environments* from other working environments. Workspace Admins can't access the working environments in a workspace unless the Account Admin associates the admin with that workspace.

A working environment represents a storage system:

- A single-node Cloud Volumes ONTAP system or an HA pair
- An on-premises ONTAP cluster in your network
- An ONTAP cluster in a NetApp Private Storage configuration

## Connectors

A Connector enables Cloud Manager to manage resources and processes within your public cloud environment. The Connector runs on a virtual machine instance that you deploy in your cloud provider, or on an on-prem host that you configured.

You can use a Connector with more than one NetApp cloud data service. For example, if you already have a Connector for Cloud Manager, you can select it when you set up the Cloud Tiering service.

## Subscriptions

The Account Settings widget shows the NetApp subscriptions associated with the selected account.

When you subscribe to Cloud Manager from a cloud provider's marketplace, you're redirected to Cloud Central where you need to save your subscription and associate it with specific accounts.

After you've subscribed, each subscription is available from the Account Settings widget. You'll only see the subscriptions that are associated with the account that you're currently viewing.

You have the option to rename a subscription and to disassociate the subscription from one or more accounts.

For example, let's say that you have two accounts and each is billed through separate subscriptions. You might disassociate a subscription from one of the accounts so the users in that account don't accidentally choose the wrong subscription when creating a Cloud Volume ONTAP working environment.

## Examples

The following examples depict how you might set up your accounts.

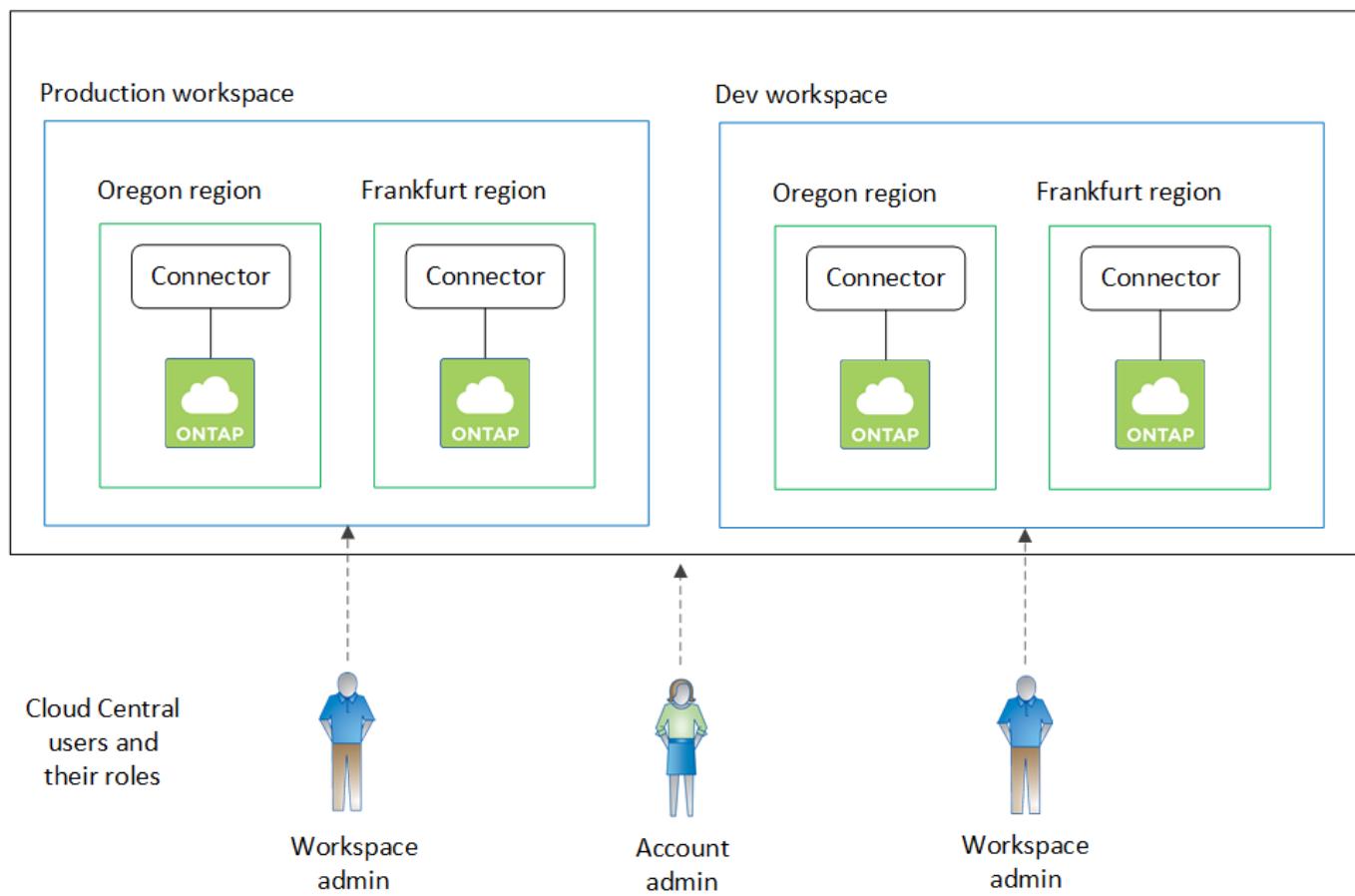


In both example images that follow, the Connector and the Cloud Volumes ONTAP systems don't actually reside *in* the NetApp Cloud Central account—they're running in a cloud provider. This is a conceptual representation of the relationship between each component.

### Example 1

The following example shows an account that uses two workspaces to create isolated environments. The first workspace is for a production environment and the second is for a dev environment.

## Account

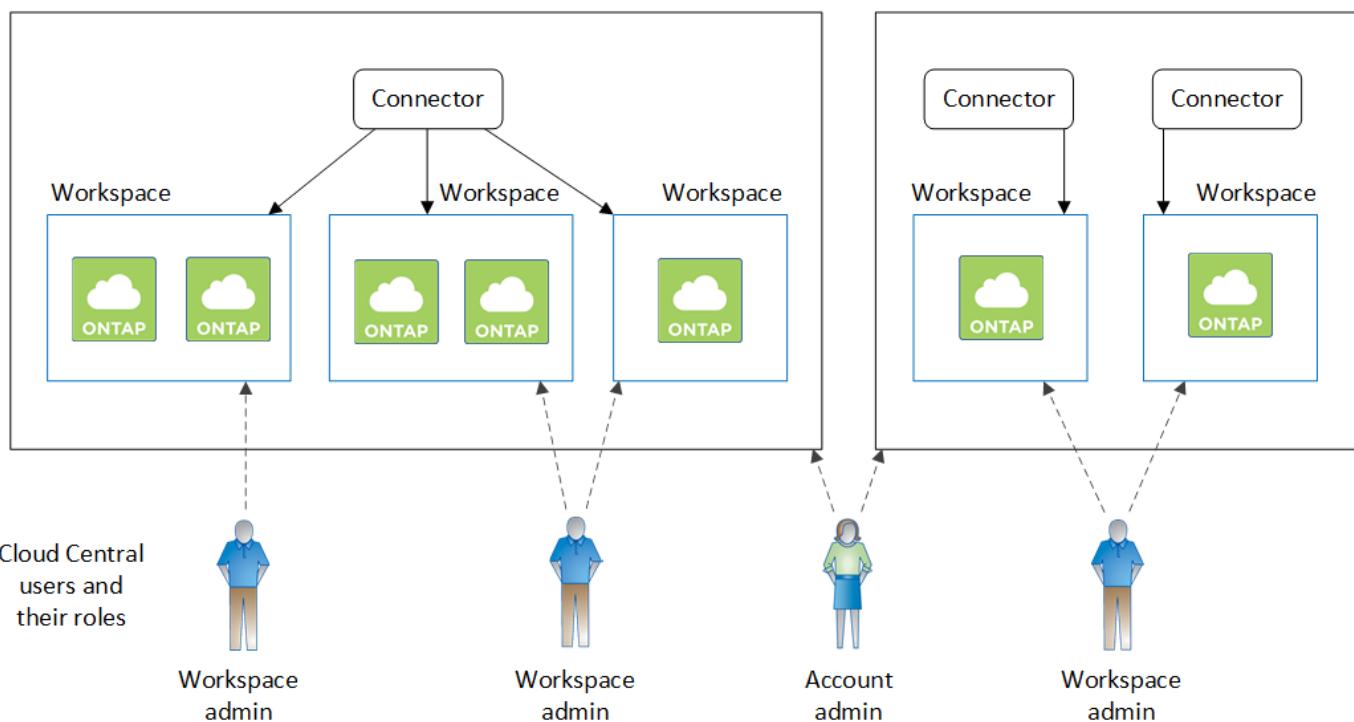


### Example 2

Here's another example that shows the highest level of multi-tenancy by using two separate Cloud Central accounts. For example, a service provider might use Cloud Manager in one account to provide services for their customers, while using another account to provide disaster recovery for one of their business units.

Note that account 2 includes two separate Connectors. This might happen if you have systems in separate regions or in separate cloud providers.

Account #1



## Setting up workspaces and users in the Cloud Central account

When you log in to Cloud Manager for the first time, you're prompted to create a *NetApp Cloud Central account*. This account provides multi-tenancy and enables you to organize users and resources in isolated *workspaces*.

[Learn more about how Cloud Central accounts work.](#)

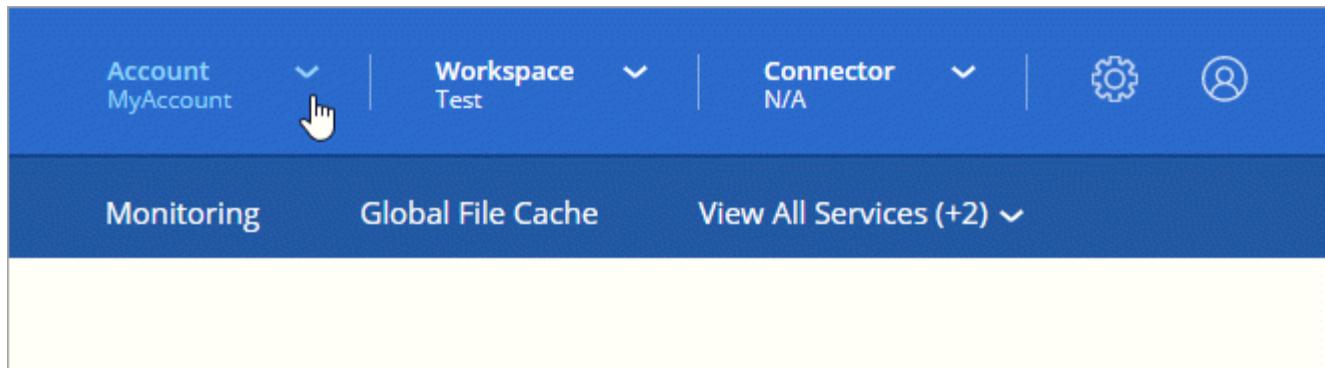
Set up your Cloud Central account so users can access Cloud Manager and access the working environments in a workspace. Just add a single user or add multiple users and workspaces.

### Adding workspaces

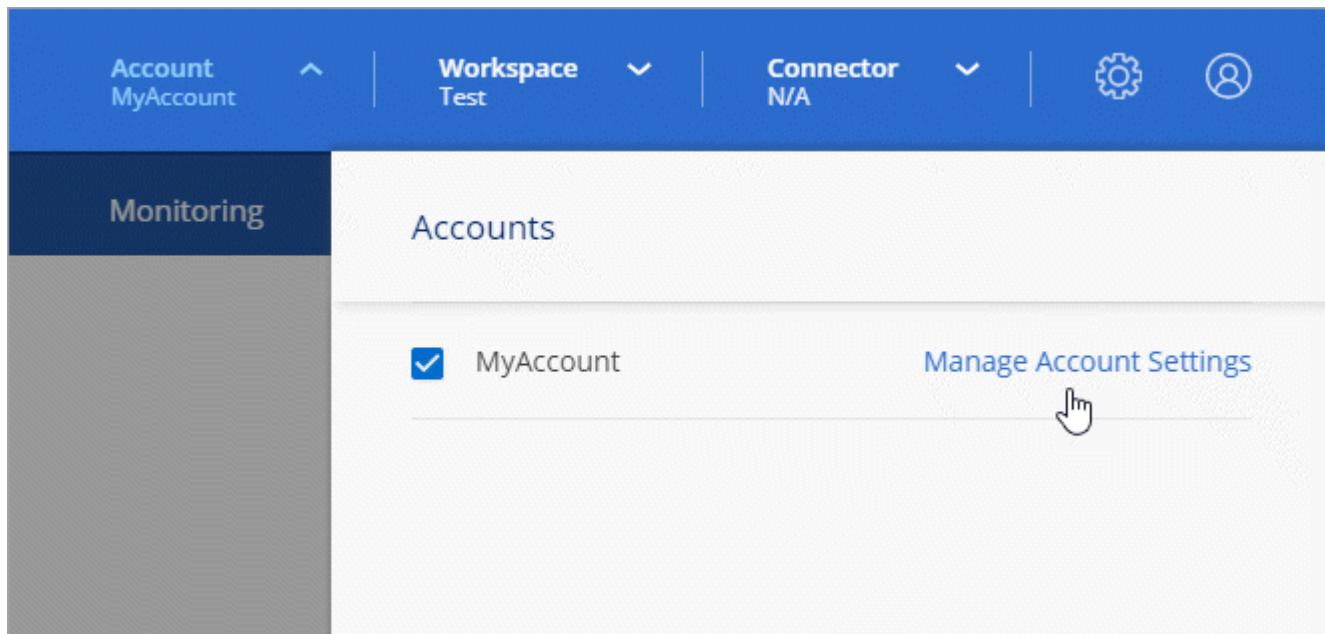
In Cloud Manager, workspaces enable you to isolate a set of working environments from other working environments and from other users. For example, you can create two workspaces and associate separate users with each workspace.

#### Steps

- From the top of Cloud Manager, click the **Account** drop-down.



2. Click **Manage Account** next to the currently selected account.



3. Click **Workspaces**.
4. Click **Add New Workspace**.
5. Enter a name for the workspace and click **Add**.

#### After you finish

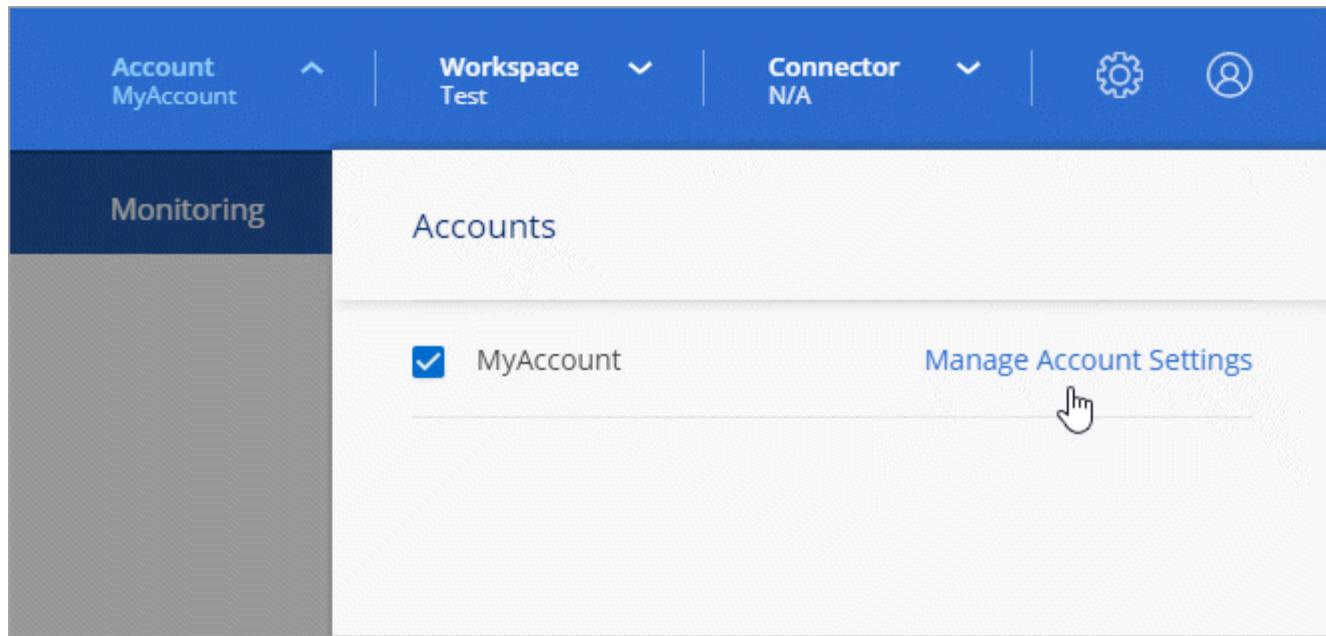
If a Workspace Admin needs access to this workspace, then you'll need to associate the user. You'll also need to associate Connectors with the workspace so Workspace Admins can use those Connectors.

#### Adding users

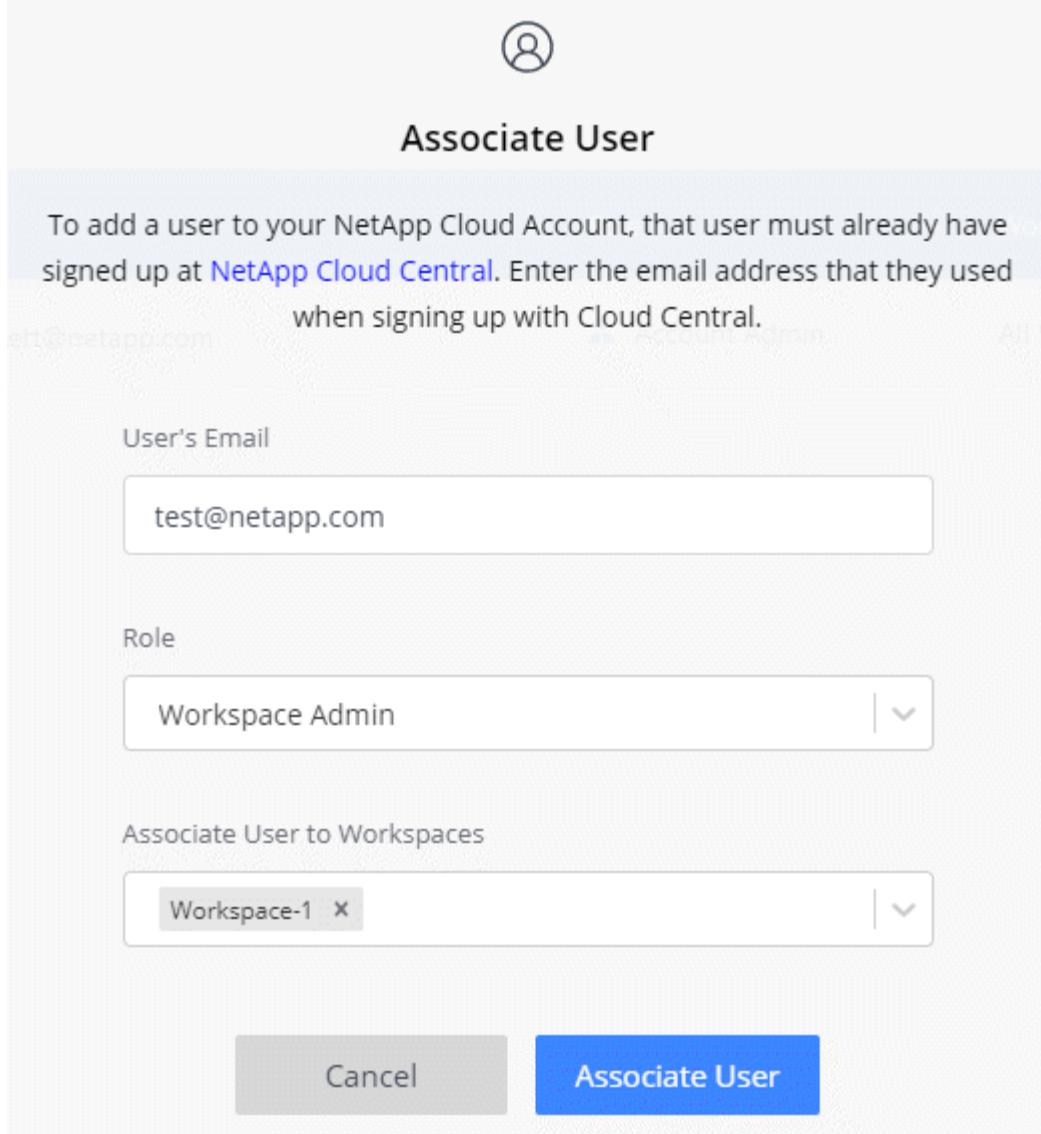
Associate Cloud Central users with the Cloud Central account so those users can create and manage working environments in Cloud Manager.

#### Steps

1. If the user hasn't already done so, ask the user to go to [NetApp Cloud Central](#) and sign up.
2. From the top of Cloud Manager, click the **Account** drop-down and click **Manage Account**.



3. From the Users tab, click **Associate User**.
4. Enter the user's email address and select a role for the user:
  - **Account Admin:** Can perform any action in Cloud Manager.
  - **Workspace Admin:** Can create and manage resources in assigned workspaces.
  - **Compliance Viewer:** Can only view compliance information and generate reports for workspaces that they have permission to access.
5. If you selected Workspace Admin or Compliance Viewer, select one or more workspaces to associate with that user.



The screenshot shows a 'Associate User' dialog box. At the top is a user icon. Below it is the title 'Associate User'. A descriptive text explains that the user must already be signed up at NetApp Cloud Central and provides a placeholder for their email address. The 'User's Email' field contains 'test@netapp.com'. The 'Role' dropdown is set to 'Workspace Admin'. Under 'Associate User to Workspaces', 'Workspace-1' is listed. At the bottom are 'Cancel' and 'Associate User' buttons.

To add a user to your NetApp Cloud Account, that user must already have signed up at [NetApp Cloud Central](#). Enter the email address that they used when signing up with Cloud Central.

User's Email

test@netapp.com

Role

Workspace Admin

Associate User to Workspaces

Workspace-1 X

Cancel Associate User

6. Click **Associate User**.

## Result

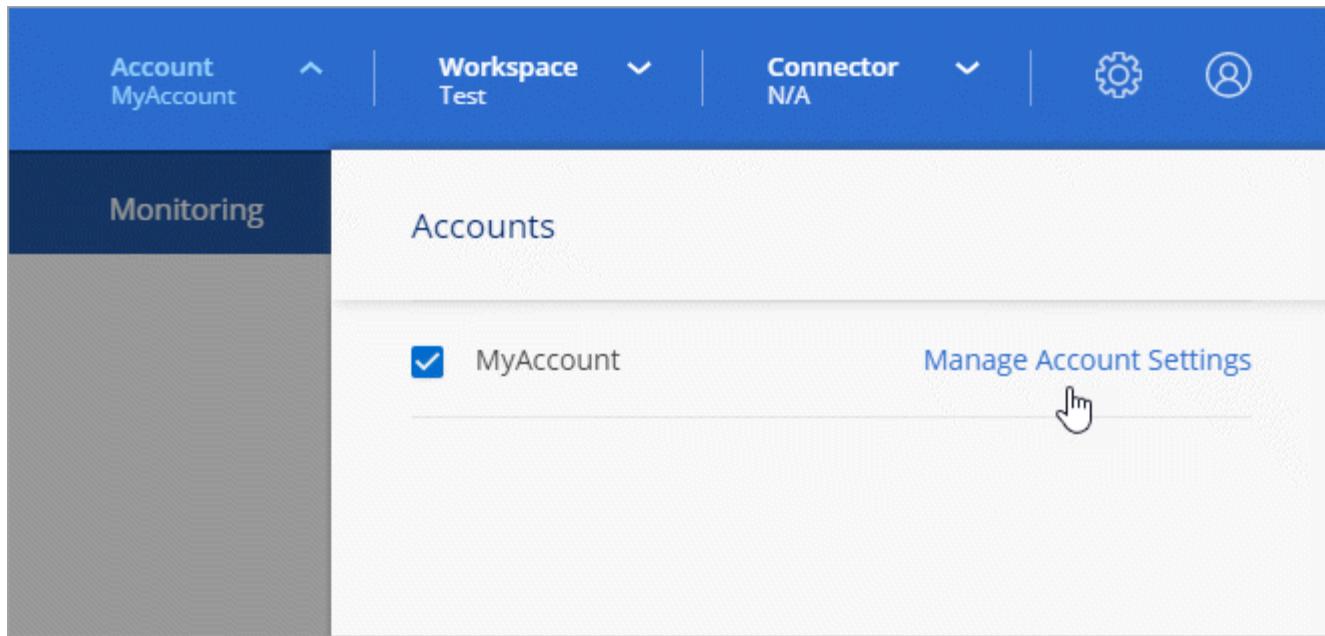
The user should receive an email from NetApp Cloud Central titled "Account Association." The email includes the information needed to access Cloud Manager.

## Associating Workspace Admins with workspaces

You can associate Workspace Admins with additional workspaces at any time. Associating the user enables them to create and view the working environments in that workspace.

## Steps

1. From the top of Cloud Manager, click the **Account** drop-down and click **Manage Account**.



2. From the Users tab, click the action menu in the row that corresponds to the user.

A screenshot of the 'Users' tab in Cloud Manager. The table header includes columns for Name, Email, Role, and Workspaces. There are two rows of data:

- Ben: Account Admin, All Workspaces
- test: Workspace Admin, None

The action menu icon for the 'test' user's row is highlighted with a red box and a hand cursor icon pointing at it.

3. Click **Manage Workspaces**.

4. Select one or more workspaces and click **Apply**.

## Result

The user can now access those workspaces from Cloud Manager, as long as the Connector was also associated with the workspaces.

## Associating Connectors with workspaces

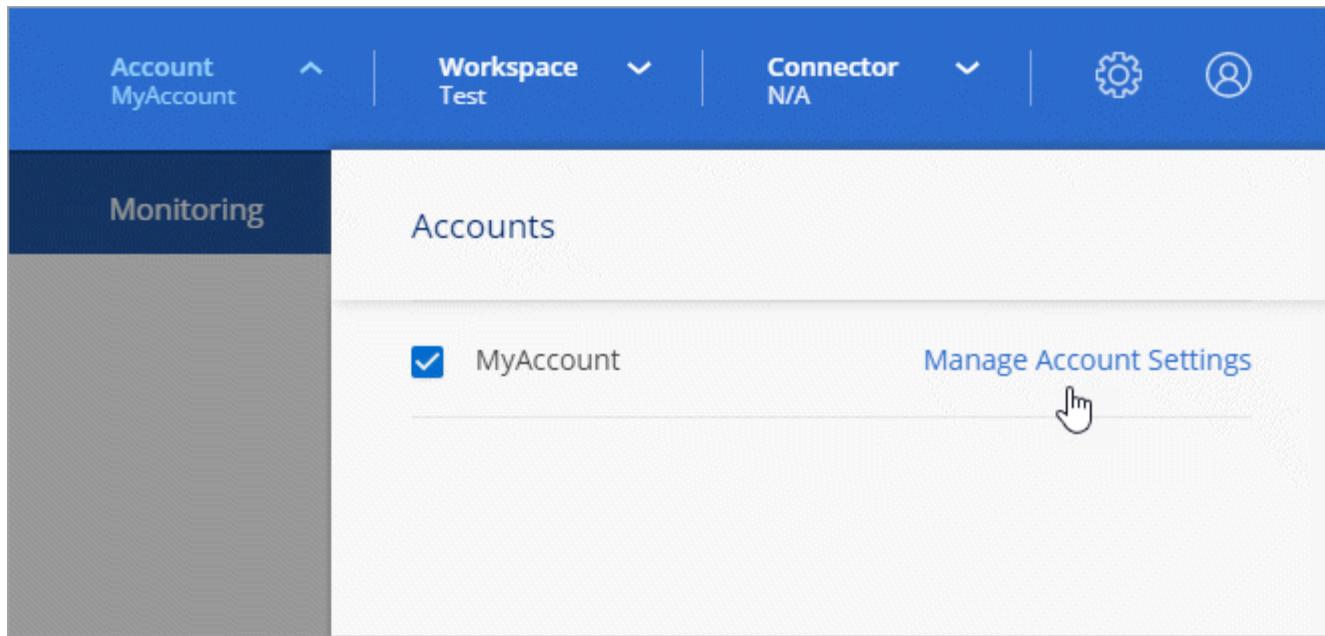
You need to associate a Connector with workspaces so Workspace Admins can use those Connectors to create Cloud Volumes ONTAP systems.

If you only have Account Admins, then associating the Connector with workspaces isn't required. Account Admins have the ability to access all workspaces in Cloud Manager by default.

[Learn more about users, workspaces, and Connectors.](#)

## Steps

1. From the top of Cloud Manager, click the **Account** drop-down and click **Manage Account**.



2. Click **Connector**.
3. Click **Manage Workspaces** for the Connector that you want to associate.
4. Select one or more workspaces and click **Apply**.

## Result

Workspace Admins can now use those Connectors to create Cloud Volumes ONTAP systems.

## What's next?

Now that you've set up your account, you can manage it any time by removing users, managing workspaces, Connectors, and subscriptions. [Learn more](#).

# Set up a Connector

## Learn about Connectors

In most cases, an Account Admin will need to deploy a **Connector** in your cloud or on-premises network. The Connector enables Cloud Manager to manage resources and processes within your public cloud environment.

## When a Connector is required

A Connector is required to use any of the following features within Cloud Manager:

- Cloud Volumes ONTAP
- On-premises ONTAP clusters
- Cloud Compliance
- Kubernetes
- Cloud Backup
- Monitoring

- On-prem tiering
- Global File Cache
- Amazon S3 bucket discovery

A Connector is **not** required for Azure NetApp Files, Cloud Volumes Service, or Cloud Sync.



While a Connector isn't required to set up and manage Azure NetApp Files, a Connector is required if you want to use Cloud Compliance to scan Azure NetApp Files data.

## Supported locations

A Connector is supported in the following locations:

- Amazon Web Services
- Microsoft Azure
- Google Cloud
- On your premises



If you want to create a Cloud Volumes ONTAP system in Google Cloud, then you must have a Connector running in Google Cloud, as well. You can't use a Connector that's running in another location.

## Connectors should remain running

A Connector should remain running at all times. It's important for the continued health and operation of the services that you enable.

For example, a Connector is a key component in the health and operation of Cloud Volumes ONTAP PAYGO systems. If a Connector is powered down, Cloud Volumes ONTAP PAYGO systems will shut down after losing communication with a Connector for longer than 14 days.

## How to create a Connector

An Account Admin needs to create a Connector before a Workspace Admin can create a Cloud Volumes ONTAP working environment and use any of the other features listed above.

An Account Admin can create a Connector in a number of ways:

- Directly from Cloud Manager (recommended)
  - [Create in AWS](#)
  - [Create in Azure](#)
  - [Create in GCP](#)
- [From the AWS Marketplace](#)
- [From the Azure Marketplace](#)
- [By downloading and installing the software on an existing Linux host](#)

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

## Permissions

Specific permissions are needed to create the Connector and another set of permissions are needed for the Connector instance itself.

### Permissions to create a Connector

The user who creates a Connector from Cloud Manager needs specific permissions to deploy the instance in your cloud provider of choice. Cloud Manager will remind you of the permissions requirements when you create a Connector.

[View policies for each cloud provider.](#)

### Permissions for the Connector instance

The Connector needs specific cloud provider permissions to perform operations on your behalf. For example, to deploy and manage Cloud Volumes ONTAP.

When you create a Connector directly from Cloud Manager, Cloud Manager creates the Connector with the permissions that it needs. There's nothing that you need to do.

If you create the Connector yourself from the AWS Marketplace, the Azure Marketplace, or by manually installing the software, then you'll need to make sure that the right permissions are in place.

[View policies for each cloud provider.](#)

## When to use multiple Connectors

In some cases, you might only need one Connector, but you might find yourself needing two or more Connectors.

Here are a few examples:

- You're using a multi-cloud environment (AWS and Azure), so you have one Connector in AWS and another in Azure. Each manages the Cloud Volumes ONTAP systems running in those environments.
- A service provider might use one Cloud Central account to provide services for their customers, while using another account to provide disaster recovery for one of their business units. Each account would have separate Connectors.

## When to switch between Connectors

When you create your first Connector, Cloud Manager automatically uses that Connector for each additional working environment that you create. Once you create an additional Connector, you'll need to switch between them to see the working environments that are specific to each Connector.

[Learn how to switch between Connectors.](#)

## The local user interface

While you should perform almost all tasks from the [SaaS user interface](#), a local user interface is still available on the Connector. This interface is needed for a few tasks that need to be performed from the Connector itself:

- [Setting a proxy server](#)
- Installing a patch (you'll typically work with NetApp personnel to install a patch)

- Downloading AutoSupport messages (usually directed by NetApp personnel when you have issues)

[Learn how to access the local UI.](#)

## Connector upgrades

The Connector automatically updates its software to the latest version, as long as it has [outbound internet access](#) to obtain the software update.

## Networking requirements for the Connector

Set up your networking so 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 type of working environment that you're creating and the services that you're planning to enable.

For example, if you install a Connector in your corporate network, then you must set up a VPN connection to the VPC or VNet in which you launch Cloud Volumes ONTAP.

### Outbound internet access

The Connector requires outbound internet access to manage resources and processes within your public cloud environment. Outbound internet access is also required if you want to manually install the Connector on a Linux host or access the local UI running on the Connector.

The following sections identify the specific endpoints.

#### Endpoints to manage resources in AWS

A Connector contacts the following endpoints when managing resources in AWS:

Endpoints	Purpose
<p>AWS services (amazonaws.com):</p> <ul style="list-style-type: none"> <li>• CloudFormation</li> <li>• Elastic Compute Cloud (EC2)</li> <li>• Key Management Service (KMS)</li> <li>• Security Token Service (STS)</li> <li>• Simple Storage Service (S3)</li> </ul> <p>The exact endpoint depends on the region in which you deploy Cloud Volumes ONTAP. <a href="#">Refer to AWS documentation for details.</a></p>	Enables the Connector to deploy and manage Cloud Volumes ONTAP in AWS.
<a href="https://api.services.cloud.netapp.com:443">https://api.services.cloud.netapp.com:443</a>	API requests to NetApp Cloud Central.
<a href="https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com">https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com</a>	Provides access to software images, manifests, and templates.
<a href="https://cognito-idp.us-east-1.amazonaws.com">https://cognito-idp.us-east-1.amazonaws.com</a> <a href="https://cognito-identity.us-east-1.amazonaws.com">https://cognito-identity.us-east-1.amazonaws.com</a> <a href="https://sts.amazonaws.com">https://sts.amazonaws.com</a> <a href="https://cloud-support-netapp-com-accelerated.s3.amazonaws.com">https://cloud-support-netapp-com-accelerated.s3.amazonaws.com</a>	Enables the Connector to access and download manifests, templates, and Cloud Volumes ONTAP upgrade images.
<a href="https://cloudmanagerinfraprod.azurecr.io">https://cloudmanagerinfraprod.azurecr.io</a>	Access to software images of container components for an infrastructure that's running Docker and provides a solution for service integrations with Cloud Manager.
<a href="https://kinesis.us-east-1.amazonaws.com">https://kinesis.us-east-1.amazonaws.com</a>	Enables NetApp to stream data from audit records.
<a href="https://cloudmanager.cloud.netapp.com">https://cloudmanager.cloud.netapp.com</a>	Communication with the Cloud Manager service, which includes Cloud Central accounts.
<a href="https://netapp-cloud-account.auth0.com">https://netapp-cloud-account.auth0.com</a>	Communication with NetApp Cloud Central for centralized user authentication.
<a href="https://support.netapp.com:443">support.netapp.com:443</a>	Communication with NetApp AutoSupport.
<a href="https://support.netapp.com/svcgw">https://support.netapp.com/svcgw</a> <a href="https://support.netapp.com/ServiceGW/entitlement">https://support.netapp.com/ServiceGW/entitlement</a> <a href="https://eval.lic.netapp.com.s3.us-west-1.amazonaws.com">https://eval.lic.netapp.com.s3.us-west-1.amazonaws.com</a> <a href="https://cloud-support-netapp-com.s3.us-west-1.amazonaws.com">https://cloud-support-netapp-com.s3.us-west-1.amazonaws.com</a>	Communication with NetApp for system licensing and support registration.
<a href="https://client.infra.support.netapp.com.s3.us-west-1.amazonaws.com">https://client.infra.support.netapp.com.s3.us-west-1.amazonaws.com</a> <a href="https://cloud-support-netapp-com-accelerated.s3.us-west-1.amazonaws.com">https://cloud-support-netapp-com-accelerated.s3.us-west-1.amazonaws.com</a> <a href="https://trigger.asup.netapp.com.s3.us-west-1.amazonaws.com">https://trigger.asup.netapp.com.s3.us-west-1.amazonaws.com</a>	Enables NetApp to collect information needed to troubleshoot support issues.

Endpoints	Purpose
<a href="https://ipa-signer.cloudmanager.netapp.com">https://ipa-signer.cloudmanager.netapp.com</a>	Enables Cloud Manager to generate licenses (for example, a FlexCache license for Cloud Volumes ONTAP)
Various third-party locations, for example: <ul style="list-style-type: none"> <li data-bbox="156 318 584 350"><a href="https://repo1.maven.org/maven2">https://repo1.maven.org/maven2</a></li> <li data-bbox="156 371 172 392">•</li> <li data-bbox="181 392 703 456"><a href="https://oss.sonatype.org/content/repositories">https://oss.sonatype.org/content/repositories</a></li> <li data-bbox="156 477 496 498">• <a href="https://repo.typesafe.com">https://repo.typesafe.com</a></li> </ul>	During upgrades, Cloud Manager downloads the latest packages for third-party dependencies.
Third-party locations are subject to change.	

#### Endpoints to manage resources in Azure

A Connector contacts the following endpoints when managing resources in Azure:

Endpoints	Purpose
<a href="https://management.azure.com">https://management.azure.com</a> <a href="https://login.microsoftonline.com">https://login.microsoftonline.com</a>	Enables Cloud Manager to deploy and manage Cloud Volumes ONTAP in most Azure regions.
<a href="https://management.microsoftazure.de">https://management.microsoftazure.de</a> <a href="https://login.microsoftonline.de">https://login.microsoftonline.de</a>	Enables Cloud Manager to deploy and manage Cloud Volumes ONTAP in the Azure Germany regions.
<a href="https://management.usgovcloudapi.net">https://management.usgovcloudapi.net</a> <a href="https://login.microsoftonline.com">https://login.microsoftonline.com</a>	Enables Cloud Manager to deploy and manage Cloud Volumes ONTAP in the Azure US Gov regions.
<a href="https://api.services.cloud.netapp.com:443">https://api.services.cloud.netapp.com:443</a>	API requests to NetApp Cloud Central.
<a href="https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com">https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com</a>	Provides access to software images, manifests, and templates.
<a href="https://cognito-idp.us-east-1.amazonaws.com">https://cognito-idp.us-east-1.amazonaws.com</a> <a href="https://cognito-identity.us-east-1.amazonaws.com">https://cognito-identity.us-east-1.amazonaws.com</a> <a href="https://sts.amazonaws.com">https://sts.amazonaws.com</a> <a href="https://cloud-support-netapp-com-accelerated.s3.amazonaws.com">https://cloud-support-netapp-com-accelerated.s3.amazonaws.com</a>	Enables the Connector to access and download manifests, templates, and Cloud Volumes ONTAP upgrade images.
<a href="https://cloudmanagerinfraprod.azurecr.io">https://cloudmanagerinfraprod.azurecr.io</a>	Access to software images of container components for an infrastructure that's running Docker and provides a solution for service integrations with Cloud Manager.
<a href="https://kinesis.us-east-1.amazonaws.com">https://kinesis.us-east-1.amazonaws.com</a>	Enables NetApp to stream data from audit records.
<a href="https://cloudmanager.cloud.netapp.com">https://cloudmanager.cloud.netapp.com</a>	Communication with the Cloud Manager service, which includes Cloud Central accounts.
<a href="https://netapp-cloud-account.auth0.com">https://netapp-cloud-account.auth0.com</a>	Communication with NetApp Cloud Central for centralized user authentication.
<a href="support.netapp.com:443">support.netapp.com:443</a>	Communication with NetApp AutoSupport.

Endpoints	Purpose
<a href="https://support.netapp.com/svcgw">https://support.netapp.com/svcgw</a> <a href="https://support.netapp.com/ServiceGW/entitlement">https://support.netapp.com/ServiceGW/entitlement</a> <a href="https://eval.lic.netapp.com.s3.us-west-1.amazonaws.com">https://eval.lic.netapp.com.s3.us-west-1.amazonaws.com</a> <a href="https://cloud-support-netapp-com.s3.us-west-1.amazonaws.com">https://cloud-support-netapp-com.s3.us-west-1.amazonaws.com</a>	Communication with NetApp for system licensing and support registration.
<a href="https://client.infra.support.netapp.com.s3.us-west-1.amazonaws.com">https://client.infra.support.netapp.com.s3.us-west-1.amazonaws.com</a> <a href="https://cloud-support-netapp-com-accelerated.s3.us-west-1.amazonaws.com">https://cloud-support-netapp-com-accelerated.s3.us-west-1.amazonaws.com</a> <a href="https://trigger.asup.netapp.com.s3.us-west-1.amazonaws.com">https://trigger.asup.netapp.com.s3.us-west-1.amazonaws.com</a>	Enables NetApp to collect information needed to troubleshoot support issues.
<a href="https://ipa-signer.cloudmanager.netapp.com">https://ipa-signer.cloudmanager.netapp.com</a>	Enables Cloud Manager to generate licenses (for example, a FlexCache license for Cloud Volumes ONTAP)
*.blob.core.windows.net	Required for HA pairs when using a proxy.
Various third-party locations, for example: <ul style="list-style-type: none"> <li>• <a href="https://repo1.maven.org/maven2">https://repo1.maven.org/maven2</a></li> <li>• <a href="https://oss.sonatype.org/content/repositories">https://oss.sonatype.org/content/repositories</a></li> <li>• <a href="https://repo.typesafe.com">https://repo.typesafe.com</a></li> </ul>	During upgrades, Cloud Manager downloads the latest packages for third-party dependencies.
Third-party locations are subject to change.	

#### Endpoints to manage resources in GCP

A Connector contacts the following endpoints when managing resources in GCP:

Endpoints	Purpose
<a href="https://www.googleapis.com">https://www.googleapis.com</a>	Enables the Connector to contact Google APIs for deploying and managing Cloud Volumes ONTAP in GCP.
<a href="https://api.services.cloud.netapp.com:443">https://api.services.cloud.netapp.com:443</a>	API requests to NetApp Cloud Central.
<a href="https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com">https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com</a>	Provides access to software images, manifests, and templates.
<a href="https://cognito-idp.us-east-1.amazonaws.com">https://cognito-idp.us-east-1.amazonaws.com</a> <a href="https://cognito-identity.us-east-1.amazonaws.com">https://cognito-identity.us-east-1.amazonaws.com</a> <a href="https://sts.amazonaws.com">https://sts.amazonaws.com</a> <a href="https://cloud-support-netapp-com-accelerated.s3.amazonaws.com">https://cloud-support-netapp-com-accelerated.s3.amazonaws.com</a>	Enables the Connector to access and download manifests, templates, and Cloud Volumes ONTAP upgrade images.
<a href="https://cloudmanagerinfraprod.azurecr.io">https://cloudmanagerinfraprod.azurecr.io</a>	Access to software images of container components for an infrastructure that's running Docker and provides a solution for service integrations with Cloud Manager.

Endpoints	Purpose
<a href="https://kinesis.us-east-1.amazonaws.com">https://kinesis.us-east-1.amazonaws.com</a>	Enables NetApp to stream data from audit records.
<a href="https://cloudmanager.cloud.netapp.com">https://cloudmanager.cloud.netapp.com</a>	Communication with the Cloud Manager service, which includes Cloud Central accounts.
<a href="https://netapp-cloud-account.auth0.com">https://netapp-cloud-account.auth0.com</a>	Communication with NetApp Cloud Central for centralized user authentication.
<a href="support.netapp.com:443">support.netapp.com:443</a>	Communication with NetApp AutoSupport.
<a href="https://support.netapp.com/svcgw">https://support.netapp.com/svcgw</a> <a href="https://support.netapp.com/ServiceGW/entitlement">https://support.netapp.com/ServiceGW/entitlement</a> <a href="https://eval.lic.netapp.com.s3.us-west-1.amazonaws.com">https://eval.lic.netapp.com.s3.us-west-1.amazonaws.com</a> <a href="https://cloud-support-netapp-com.s3.us-west-1.amazonaws.com">https://cloud-support-netapp-com.s3.us-west-1.amazonaws.com</a>	Communication with NetApp for system licensing and support registration.
<a href="https://client.infra.support.netapp.com.s3.us-west-1.amazonaws.com">https://client.infra.support.netapp.com.s3.us-west-1.amazonaws.com</a> <a href="https://cloud-support-netapp-com-accelerated.s3.us-west-1.amazonaws.com">https://cloud-support-netapp-com-accelerated.s3.us-west-1.amazonaws.com</a> <a href="https://trigger.asup.netapp.com.s3.us-west-1.amazonaws.com">https://trigger.asup.netapp.com.s3.us-west-1.amazonaws.com</a>	Enables NetApp to collect information needed to troubleshoot support issues.
<a href="https://ipa-signer.cloudmanager.netapp.com">https://ipa-signer.cloudmanager.netapp.com</a>	Enables Cloud Manager to generate licenses (for example, a FlexCache license for Cloud Volumes ONTAP)
Various third-party locations, for example: <ul style="list-style-type: none"> <li>• <a href="https://repo1.maven.org/maven2">https://repo1.maven.org/maven2</a></li> <li>• <a href="https://oss.sonatype.org/content/repositories">https://oss.sonatype.org/content/repositories</a></li> <li>• <a href="https://repo.typesafe.com">https://repo.typesafe.com</a></li> </ul>	During upgrades, Cloud Manager downloads the latest packages for third-party dependencies.
Third-party locations are subject to change.	

#### Endpoints to install the Connector on a Linux host

You have the option to manually install the Connector software on your own Linux host. If you do, the installer for the Connector must access the following URLs during the installation process:

- <http://dev.mysql.com/get/mysql-community-release-el7-5.noarch.rpm>
- <https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm>
- <https://s3.amazonaws.com/aws-cli/awscli-bundle.zip>

The host might try to update operating system packages during installation. The host can contact different mirroring sites for these OS packages.

## Endpoints accessed from your web browser when using the local UI

While you should perform almost all tasks from the SaaS user interface, a local user interface is still available on the Connector. The machine running the web browser must have connections to the following endpoints:

Endpoints	Purpose
The Connector host	<p>You must enter the host's IP address from a web browser to load the Cloud Manager console.</p> <p>Depending on your connectivity to your cloud provider, you can use the private IP or a public IP assigned to the host:</p> <ul style="list-style-type: none"><li>• A private IP works if you have a VPN and direct connect access to your virtual network</li><li>• A public IP works in any networking scenario</li></ul> <p>In any case, you should secure network access by ensuring that security group rules allow access from only authorized IPs or subnets.</p>
<a href="https://auth0.com">https://auth0.com</a> <a href="https://cdn.auth0.com">https://cdn.auth0.com</a> <a href="https://netapp-cloud-account.auth0.com">https://netapp-cloud-account.auth0.com</a> <a href="https://services.cloud.netapp.com">https://services.cloud.netapp.com</a>	Your web browser connects to these endpoints for centralized user authentication through NetApp Cloud Central.
<a href="https://widget.intercom.io">https://widget.intercom.io</a>	For in-product chat that enables you to talk to NetApp cloud experts.

## Ports and security groups

There's no incoming traffic to the Connector, unless you initiate it. HTTP and HTTPS provide access to the [local UI](#), which you'll use in rare circumstances. SSH is only needed if you need to connect to the host for troubleshooting.

### Rules for the Connector in AWS

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

#### Inbound rules

Protocol	Port	Purpose
SSH	22	Provides SSH access to the Connector host
HTTP	80	Provides HTTP access from client web browsers to the local user interface and connections from Cloud Compliance
HTTPS	443	Provides HTTPS access from client web browsers to the local user interface
TCP	3128	Provides the Cloud Compliance instance with internet access, if your AWS network doesn't use a NAT or proxy

## Outbound rules

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

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

### 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
Active Directory	TCP	88	Active Directory forest	Kerberos V authentication
	TCP	139	Active Directory forest	NetBIOS service session
	TCP	389	Active Directory forest	LDAP
	TCP	445	Active Directory forest	Microsoft SMB/CIFS over TCP with NetBIOS framing
	TCP	464	Active Directory forest	Kerberos V change & set password (SET_CHANGE)
	TCP	749	Active Directory forest	Active Directory Kerberos V change & set password (RPCSEC_GSS)
	UDP	137	Active Directory forest	NetBIOS name service
	UDP	138	Active Directory forest	NetBIOS datagram service
	UDP	464	Active Directory forest	Kerberos key administration
API calls and AutoSupport	HTTP	443	Outbound internet and ONTAP cluster management LIF	API calls to AWS and ONTAP, and sending AutoSupport messages to NetApp
API calls	TCP	3000	ONTAP cluster management LIF	API calls to ONTAP
	TCP	8088	Backup to S3	API calls to Backup to S3
DNS	UDP	53	DNS	Used for DNS resolve by Cloud Manager
Cloud Compliance	HTTP	80	Cloud Compliance instance	Cloud Compliance for Cloud Volumes ONTAP

## Rules for the Connector in Azure

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

### Inbound rules

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

### Outbound rules

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

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

### Advanced outbound rules

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



The source IP address is the Connector host.

Service	Port	Protocol	Destination	Purpose
Active Directory	88	TCP	Active Directory forest	Kerberos V authentication
	139	TCP	Active Directory forest	NetBIOS service session
	389	TCP	Active Directory forest	LDAP
	445	TCP	Active Directory forest	Microsoft SMB/CIFS over TCP with NetBIOS framing
	464	TCP	Active Directory forest	Kerberos V change & set password (SET_CHANGE)
	749	TCP	Active Directory forest	Active Directory Kerberos V change & set password (RPCSEC_GSS)
	137	UDP	Active Directory forest	NetBIOS name service
	138	UDP	Active Directory forest	NetBIOS datagram service
	464	UDP	Active Directory forest	Kerberos key administration
API calls and AutoSupport	443	HTTP	Outbound internet and ONTAP cluster management LIF	API calls to AWS and ONTAP, and sending AutoSupport messages to NetApp
API calls	3000	TCP	ONTAP cluster management LIF	API calls to ONTAP
DNS	53	UDP	DNS	Used for DNS resolve by Cloud Manager

#### Rules for the Connector in GCP

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

#### 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
Active Directory	TCP	88	Active Directory forest	Kerberos V authentication
	TCP	139	Active Directory forest	NetBIOS service session
	TCP	389	Active Directory forest	LDAP
	TCP	445	Active Directory forest	Microsoft SMB/CIFS over TCP with NetBIOS framing
	TCP	464	Active Directory forest	Kerberos V change & set password (SET_CHANGE)
	TCP	749	Active Directory forest	Active Directory Kerberos V change & set password (RPCSEC_GSS)
	UDP	137	Active Directory forest	NetBIOS name service
	UDP	138	Active Directory forest	NetBIOS datagram service
	UDP	464	Active Directory forest	Kerberos key administration
API calls and AutoSupport	HTTP	443	Outbound internet and ONTAP cluster management LIF	API calls to GCP and ONTAP, and sending AutoSupport messages to NetApp
API calls	TCP	3000	ONTAP cluster management LIF	API calls to ONTAP
DNS	UDP	53	DNS	Used for DNS resolve by Cloud Manager

## Creating a Connector in AWS from Cloud Manager

An Account Admin needs to deploy a *Connector* before you can use most Cloud Manager features. [Learn when a Connector is required](#). The Connector enables Cloud Manager to manage resources and processes within your public cloud environment.

This page describes how to create a Connector in AWS directly from Cloud Manager. You also have the option to [create the Connector from the AWS Marketplace](#), or to [download the software and install it on your own host](#).

These steps must be completed by a user who has the Account Admin role. A Workspace Admin can't create a Connector.



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

## Setting up AWS permissions to create a Connector

Before you can deploy a Connector from Cloud Manager, you need to ensure that your AWS account has the correct permissions.

### Steps

1. Download the Connector IAM policy from the following location:

[NetApp Cloud Manager: AWS, Azure, and GCP Policies](#)

2. From the AWS IAM console, create your own policy by copying and pasting the text from the Connector IAM policy.
3. Attach the policy that you created in the previous step to the IAM user who will create the Connector from Cloud Manager.

### Result

The AWS user now has the permissions required to create the Connector from Cloud Manager. You'll need to specify AWS access keys for this user when you're prompted by Cloud Manager.

## Creating a Connector in AWS

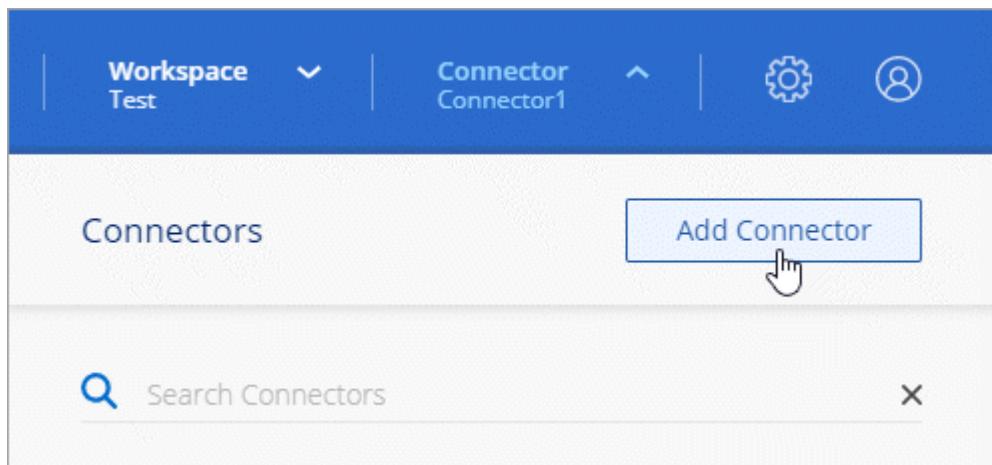
Cloud Manager enables you to create a Connector in AWS directly from its user interface.

### What you'll need

- An AWS access key and secret key for an IAM user who has the [required permissions](#).
- A VPC, subnet, and keypair in your AWS region of choice.

### Steps

1. If you're creating your first Working Environment, click **Add Working Environment** and follow the prompts. Otherwise, click the **Connector** drop-down and select **Add Connector**.



2. Click **Let's Start**.
3. Choose **Amazon Web Services** as your cloud provider.

Remember that the Connector must have a network connection to the type of working environment that you're creating and the services that you're planning to enable.

[Learn more about networking requirements for the Connector](#).

4. Review what you'll need and click **Continue**.
5. Provide the required information:
  - **AWS Credentials:** Enter a name for the instance and specify the AWS access key and secret key that meet permissions requirements.
  - **Location:** Specify an AWS region, VPC, and subnet for the instance.
  - **Network:** Select the key pair to use with the instance, whether to enable a public IP address, and optionally specify a proxy configuration.
  - **Security Group:** Choose whether to create a new security group or whether to select an existing security group that allows inbound HTTP, HTTPS, and SSH access.



There's no incoming traffic to the Connector, unless you initiate it. HTTP and HTTPS provide access to the [local UI](#), which you'll use in rare circumstances. SSH is only needed if you need to connect to the host for troubleshooting.

6. Click **Create**.

The instance should be ready in about 7 minutes. You should stay on the page until the process is complete.

#### After you finish

You need to associate a Connector with workspaces so Workspace Admins can use those Connectors to create Cloud Volumes ONTAP systems. If you only have Account Admins, then associating the Connector with workspaces isn't required. Account Admins have the ability to access all workspaces in Cloud Manager by default. [Learn more](#).

## Creating a Connector in Azure from Cloud Manager

An Account Admin needs to deploy a *Connector* before you can use most Cloud Manager features. [Learn when a Connector is required](#). The Connector enables Cloud Manager to manage resources and processes within your public cloud environment.

This page describes how to create a Connector in Azure directly from Cloud Manager. You also have the option to [create the Connector from the Azure Marketplace](#), or to [download the software and install it on your own host](#).

These steps must be completed by a user who has the Account Admin role. A Workspace Admin can't create a Connector.



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

#### Setting up Azure permissions to create a Connector

Before you can deploy a Connector from Cloud Manager, you need to ensure that your Azure account has the correct permissions.

#### Steps

1. Create a custom role using the Azure policy for the Connector:
  - a. Download the [Azure policy for the Connector](#).



Right-click the link and click **Save link as...** to download the file.

- b. Modify the JSON file by adding your Azure subscription ID to the assignable scope.

### Example

```
"AssignableScopes": [  
    "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzz"  
],
```

- c. Use the JSON file to create a custom role in Azure.

The following example shows how to create a custom role using the Azure CLI 2.0:

```
az role definition create --role-definition  
C:\Policy_for_Setup_As_Service_Azure.json
```

You should now have a custom role called *Azure SetupAsService*.

2. Assign the role to the user who will deploy the Connector from Cloud Manager:

- a. Open the **Subscriptions** service and select the user's subscription.
- b. Click **Access control (IAM)**.
- c. Click **Add > Add role assignment** and then add the permissions:
  - Select the **Azure SetupAsService** role.



Azure SetupAsService is the default name provided in the [Connector deployment policy for Azure](#). If you chose a different name for the role, then select that name instead.

- Assign access to an **Azure AD user, group, or application**.
- Select the user account.
- Click **Save**.

### Result

The Azure user now has the permissions required to deploy the Connector from Cloud Manager.

## Creating a Connector in Azure

Cloud Manager enables you to create a Connector in Azure directly from its user interface.

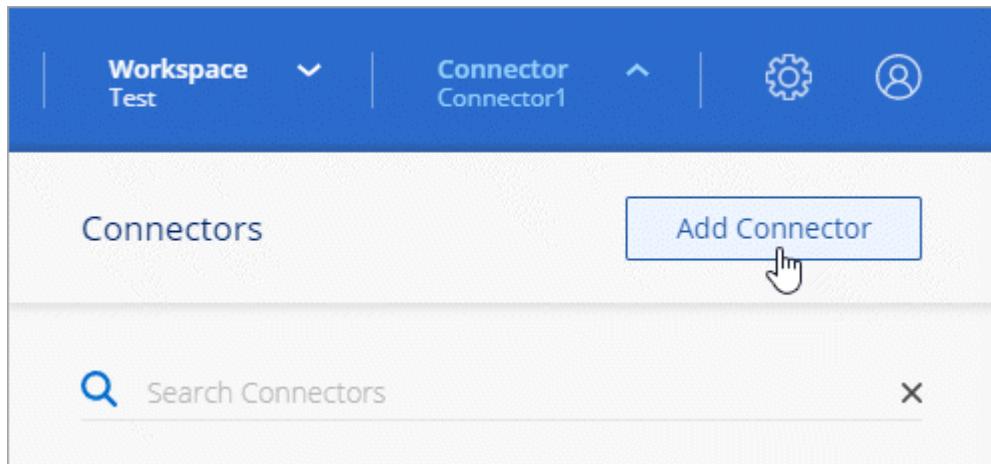
### What you'll need

- The [required permissions](#) for your Azure account.
- An Azure subscription.
- A VNet and subnet in your Azure region of choice.

### Steps

1. If you're creating your first Working Environment, click **Add Working Environment** and follow the prompts.

Otherwise, click the **Connector** drop-down and select **Add Connector**.



2. Click **Let's Start**.

3. Choose **Microsoft Azure** as your cloud provider.

Remember that the Connector must have a network connection to the type of working environment that you're creating and the services that you're planning to enable.

[Learn more about networking requirements for the Connector.](#)

4. Review what you'll need and click **Continue**.

5. If you're prompted, log in to your Microsoft account, which should have the required permissions to create the virtual machine.

The form is owned and hosted by Microsoft. Your credentials are not provided to NetApp.



If you're already logged in to an Azure account, then Cloud Manager will automatically use that account. If you have multiple accounts, then you might need to log out first to ensure that you're using the right account.

6. Provide the required information:

- **VM Authentication:** Enter a name for the virtual machine and a user name and password or public key.
- **Basic Settings:** Choose an Azure subscription, an Azure region, and whether to create a new resource group or to use an existing resource group.
- **Network:** Choose a VNet and subnet, whether to enable a public IP address, and optionally specify a proxy configuration.
- **Security Group:** Choose whether to create a new security group or whether to select an existing security group that allows inbound HTTP, HTTPS, and SSH access.



There's no incoming traffic to the Connector, unless you initiate it. HTTP and HTTPS provide access to the [local UI](#), which you'll use in rare circumstances. SSH is only needed if you need to connect to the host for troubleshooting.

7. Click **Create**.

The virtual machine should be ready in about 7 minutes. You should stay on the page until the process is

complete.

## After you finish

You need to associate a Connector with workspaces so Workspace Admins can use those Connectors to create Cloud Volumes ONTAP systems. If you only have Account Admins, then associating the Connector with workspaces isn't required. Account Admins have the ability to access all workspaces in Cloud Manager by default. [Learn more](#).

## Creating a Connector in GCP from Cloud Manager

An Account Admin needs to deploy a *Connector* before you can use most Cloud Manager features. [Learn when a Connector is required](#). The Connector enables Cloud Manager to manage resources and processes within your public cloud environment.

This page describes how to create a Connector in GCP directly from Cloud Manager. You also have the option to [download the software and install it on your own host](#).

These steps must be completed by a user who has the Account Admin role. A Workspace Admin can't create a Connector.



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

### Setting up GCP permissions to create a Connector

Before you can deploy a Connector from Cloud Manager, you need to ensure that your GCP account has the correct permissions and that a service account is set up for the Connector VM.

#### Steps

1. Ensure that the GCP user who deploys Cloud Manager from NetApp Cloud Central has the permissions in the [Connector deployment policy for GCP](#).

[You can create a custom role using the YAML file](#) and then attach it to the user. You'll need to use the gcloud command line to create the role.

2. Set up a service account that has the permissions that Cloud Manager needs to create and manage Cloud Volumes ONTAP systems in projects.

You'll associate this service account with the Connector VM when you create it from Cloud Manager.

- a. [Create a role in GCP](#) that includes the permissions defined in the [Cloud Manager policy for GCP](#). Again, you'll need to use the gcloud command line.

The permissions contained in this YAML file are different than the permissions in step 1.

- b. [Create a GCP service account and apply the custom role that you just created](#).
- c. If you want to deploy Cloud Volumes ONTAP in other projects, [grant access by adding the service account with the Cloud Manager role to that project](#). You'll need to repeat this step for each project.

#### Result

The GCP user now has the permissions required to create the Connector from Cloud Manager and the service account for the Connector VM is set up.

## Enabling Google Cloud APIs

Several APIs are required to deploy the Connector and Cloud Volumes ONTAP.

### Step

1. [Enable the following Google Cloud APIs in your project.](#)

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

## Creating a Connector in GCP

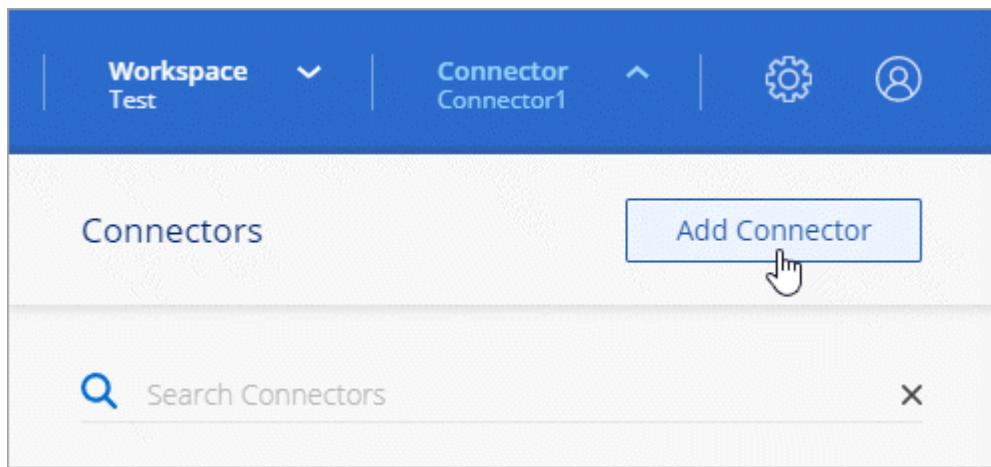
Cloud Manager enables you to create a Connector in GCP directly from its user interface.

### What you'll need

- The [required permissions](#) for your Google Cloud account.
- A Google Cloud project.
- A service account that has the required permissions to create and manage Cloud Volumes ONTAP.
- A VPC and subnet in your Google Cloud region of choice.

### Steps

1. If you're creating your first Working Environment, click **Add Working Environment** and follow the prompts. Otherwise, click the **Connector** drop-down and select **Add Connector**.



2. Click **Let's Start**.
3. Choose **Google Cloud Platform** as your cloud provider.

Remember that the Connector must have a network connection to the type of working environment that you're creating and the services that you're planning to enable.

[Learn more about networking requirements for the Connector.](#)

4. Review what you'll need and click **Continue**.

5. If you're prompted, log in to your Google account, which should have the required permissions to create the virtual machine instance.

The form is owned and hosted by Google. Your credentials are not provided to NetApp.

6. Provide the required information:

- **Basic Settings:** Enter a name for the virtual machine instance and specify a project and service account that has the required permissions.
- **Location:** Specify a region, zone, VPC, and subnet for the instance.
- **Network:** Choose whether to enable a public IP address and optionally specify a proxy configuration.
- **Firewall Policy:** Choose whether to create a new firewall policy or whether to select an existing firewall policy that allows inbound HTTP, HTTPS, and SSH access.



There's no incoming traffic to the Connector, unless you initiate it. HTTP and HTTPS provide access to the [local UI](#), which you'll use in rare circumstances. SSH is only needed if you need to connect to the host for troubleshooting.

7. Click **Create**.

The instance should be ready in about 7 minutes. You should stay on the page until the process is complete.

#### After you finish

You need to associate a Connector with workspaces so Workspace Admins can use those Connectors to create Cloud Volumes ONTAP systems. If you only have Account Admins, then associating the Connector with workspaces isn't required. Account Admins have the ability to access all workspaces in Cloud Manager by default. [Learn more](#).

## Where to go next

Now that you've logged in and set up Cloud Manager, users can start creating and discovering working environments.

- [Get started with Cloud Volumes ONTAP for AWS](#)
- [Get started with Cloud Volumes ONTAP for Azure](#)
- [Get started with Cloud Volumes ONTAP for Google Cloud](#)
- [Set up Azure NetApp Files](#)
- [Set up Cloud Volumes Service for AWS](#)
- [Discover an on-premises ONTAP cluster](#)
- [Discover your Amazon S3 buckets](#)

If you're an administrator, you can manage Cloud Manager settings after you create your first Connector.

- [Learn about Connectors](#)
- [Manage an HTTPS certificate for secure access](#)
- [Configure proxy settings](#)

# Manage Cloud Volumes ONTAP

## Learn

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

- 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.

- Data security

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

- Privacy compliance controls

Integration with Cloud Compliance helps you understand data context and identify sensitive data.



Licenses for ONTAP features are included with Cloud Volumes ONTAP.

[View supported Cloud Volumes ONTAP configurations](#)

[Learn more about Cloud Volumes ONTAP](#)

# Storage

## Disks and aggregates

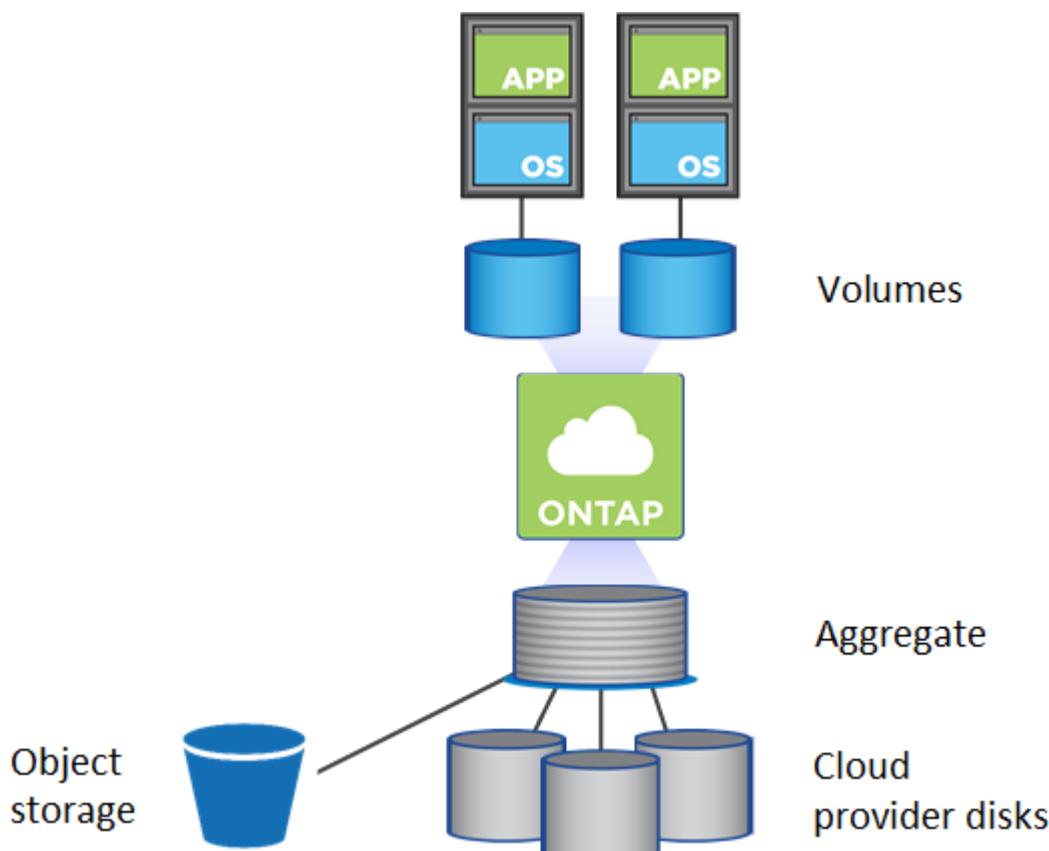
Understanding how Cloud Volumes ONTAP uses cloud storage can help you understand your storage costs.



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 GB aggregate, the usable capacity is 442.94 GB.

## AWS storage

In AWS, Cloud Volumes ONTAP uses EBS storage for user data and local NVMe storage as Flash Cache on some EC2 instance types.

### EBS storage

In AWS, an aggregate can contain up to 6 disks that are all the same size. The maximum disk size is 16 TB.

The underlying EBS disk type can be either General Purpose SSD, Provisioned IOPS SSD, Throughput Optimized HDD, or Cold HDD. You can pair an EBS disk with Amazon S3 to [tier inactive data to low-cost object storage](#).

At a high level, the differences between EBS disk types are as follows:

- *General Purpose SSD* disks balance cost and performance for a broad range of workloads. Performance is defined in terms of IOPS.
- *Provisioned IOPS SSD* disks are for critical applications that require the highest performance at a higher cost.
- *Throughput Optimized HDD* disks are for frequently accessed workloads that require fast and consistent throughput at a lower price.
- *Cold HDD* disks are meant for backups, or infrequently accessed data, because the performance is very low. Like Throughput Optimized HDD disks, performance is defined in terms of throughput.



Cold HDD disks are not supported with HA configurations and with data tiering.

## Local NVMe storage

Some EC2 instance types include local NVMe storage, which Cloud Volumes ONTAP uses as [Flash Cache](#).

### Related links

- [AWS documentation: EBS Volume Types](#)
- [Learn how to choose disk types and disk sizes for your systems in AWS](#)
- [Review storage limits for Cloud Volumes ONTAP in AWS](#)
- [Review supported configurations for Cloud Volumes ONTAP in AWS](#)

## Azure storage

In Azure, an aggregate can contain up to 12 disks that are all the same size. The disk type and maximum disk size depends on whether you use a single node system or an HA pair:

### Single node systems

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

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

Each managed disk type has a maximum disk size of 32 TB.

You can pair a managed disk with Azure Blob storage to [tier inactive data to low-cost object storage](#).

## HA pairs

HA pairs use Premium page blobs, which have a maximum disk size of 8 TB.

## Related links

- [Microsoft Azure documentation: Introduction to Microsoft Azure Storage](#)
- [Learn how to choose disk types and disk sizes for your systems in Azure](#)
- [Review storage limits for Cloud Volumes ONTAP in Azure](#)

## GCP storage

In GCP, an aggregate can contain up to 6 disks that are all the same size. The maximum disk size is 16 TB.

The disk type can be either *Zonal SSD 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

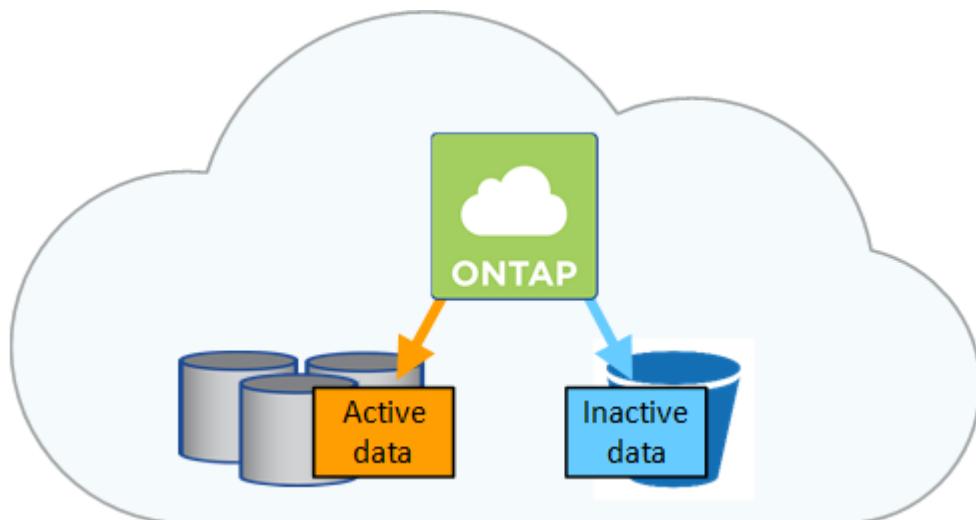
- [Google Cloud Platform documentation: Storage Options](#)
- [Review storage limits for Cloud Volumes ONTAP in GCP](#)

## RAID type

The RAID type for each Cloud Volumes ONTAP aggregate is RAID0 (striping). No other RAID types are supported. Cloud Volumes ONTAP relies on the cloud provider for disk availability and durability.

## 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.



Cloud Volumes ONTAP supports data tiering in AWS, Azure, and Google Cloud Platform. Data tiering is

powered by FabricPool technology.



You don't need to install a feature license to enable data tiering (FabricPool).

## Data tiering in AWS

When you enable data tiering in AWS, Cloud Volumes ONTAP uses EBS as a performance tier for hot data and AWS S3 as a capacity tier for inactive data.

### Performance tier

The performance tier can be General Purpose SSDs, Provisioned IOPS SSDs, or Throughput Optimized HDDs.

### Capacity tier

A Cloud Volumes ONTAP system tiers inactive data to a single S3 bucket using the *Standard* storage class. Standard is ideal for frequently accessed data stored across multiple Availability Zones.



Cloud Manager creates a single S3 bucket for each working environment and names it `fabric-pool-cluster unique identifier`. A different S3 bucket is not created for each volume.

## Storage classes

The default storage class for tiered data in AWS is *Standard*. If you don't plan to access the inactive data, you can reduce your storage costs by changing the storage class to one of the following: *Intelligent Tiering*, *One-Zone Infrequent Access*, or *Standard-Infrequent Access*. When you change the storage class, inactive data starts in the Standard storage class and transitions to the storage class that you selected, if the data is not accessed after 30 days.

The access costs are higher if you do access the data, so take that into consideration before you change the storage class. [Learn more about Amazon S3 storage classes](#).

You can select a storage class when you create the working environment and you can change it any time after. For details about changing the storage class, see [Tiering inactive data to low-cost object storage](#).

The storage class for data tiering is system wide—it's not per volume.

## Data tiering in Azure

When you enable data tiering in Azure, Cloud Volumes ONTAP uses Azure managed disks as a performance tier for hot data and Azure Blob storage as a capacity tier for inactive data.

### Performance tier

The performance tier can be either SSDs or HDDs.

### Capacity tier

A Cloud Volumes ONTAP system tiers inactive data to a single Blob container using the Azure *hot* storage tier. The hot tier is ideal for frequently accessed data.



Cloud Manager creates a new storage account with a single container for each Cloud Volumes ONTAP working environment. The name of the storage account is random. A different container is not created for each volume.

## Storage access tiers

The default storage access tier for tiered data in Azure is the *hot* tier. If you don't plan to access the inactive data, you can reduce your storage costs by changing to the *cool* storage tier. When you change the storage tier, inactive data starts in the hot storage tier and transitions to the cool storage tier, 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 tier. [Learn more about Azure Blob storage access tiers](#).

You can select a storage tier when you create the working environment and you can change it any time after. For details about changing the storage tier, see [Tiering inactive data to low-cost object storage](#).

The storage access tier for data tiering is system wide—it's not per volume.

## Data tiering in GCP

When you enable data tiering in GCP, 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 SSDs or HDDs (standard disks).

### Capacity tier

A Cloud Volumes ONTAP system tiers inactive data to a single Google Cloud Storage bucket using the *Regional* storage class.



Cloud Manager creates a single bucket for each working environment and names it *fabric-pool-cluster unique identifier*. A different bucket is not created for each volume.

## 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.

### Disk size selection for aggregates in AWS

When Cloud Manager creates new aggregates for Cloud Volumes ONTAP in AWS, it gradually increases the disk size in an aggregate, as the number of aggregates in the system increases. Cloud Manager does this to ensure that you can utilize the system's maximum capacity before it reaches the maximum number of data disks allowed by AWS.

For example, Cloud Manager might choose the following disk sizes for aggregates in a Cloud Volumes ONTAP Premium or BYOL system:

Aggregate number	Disk size	Max aggregate capacity
1	500 MB	3 TB
4	1 TB	6 TB
6	2 TB	12 TB

You can choose the disk size yourself by using the advanced allocation option.

## 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. It might help for you to understand how these modes work.

### 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 with 5 or fewer EBS disks reaches the capacity threshold, Cloud Manager automatically purchases new disks for that aggregate so volumes can continue to grow.
- If an aggregate with 12 Azure disks reaches the capacity threshold, 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 AWS, Azure, or GCP 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.

### Management of inodes with automatic capacity management

Cloud Manager monitors inode usage on a volume. When 85% of the inodes are used, Cloud Manager increases the size of the volume to increase the number of available inodes. The number of files a volume can contain is determined by how many inodes it has.

## **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.

### **Write speed**

Cloud Manager enables you to choose normal or high write speed for Cloud Volumes ONTAP. Before you choose a write speed, you should understand the differences between the normal and high settings and risks and recommendations when using high write speed.

High write speed is supported with all types of single node systems. It's also supported with HA pairs in AWS and Azure when using a specific instance or VM type (refer to the sections below for the list of supported instances and VM types). High write speed is not supported with HA pairs in GCP.

#### **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.

## AWS

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

If you use an HA pair, Cloud Volumes ONTAP supports high write speed with the following instance types, starting with the 9.8 release:

- c5.9xlarge
- c5.18xlarge
- c5d.4xlarge
- c5d.9xlarge
- c5d.18xlarge
- c5n.9xlarge
- c5n.18xlarge
- m5.2xlarge
- m5.4xlarge
- m5.16xlarge
- m5d.8xlarge
- m5d.12xlarge
- m5n.2xlarge
- r5.2xlarge
- r5.8xlarge
- r5.12xlarge
- r5d.2xlarge

## Azure

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

If you use an HA pair, Cloud Volumes ONTAP supports high write speed with the following VM types, starting with the 9.8 release:

- DS5\_v2
- DS14\_v2
- DS15\_v2
- E48s\_v3

## 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.

### 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 you choose high write speed and data loss occurs, the system should be able to boot up and continue to serve data without user intervention. Two EMS messages will be reported when a node runs into data loss. One is wafl.root.content.changed with the ERROR severity level event, the other is nv.check.failed with the DEBUG severity level event. Both messages must be present as an indication of data loss.

#### 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 in AWS and Azure 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 instances in AWS

Select one of the following EC2 instance types with a new or existing Cloud Volumes ONTAP Premium or BYOL system:

- c5d.4xlarge

- c5d.9xlarge
- c5d.18xlarge
- m5d.8xlarge
- m5d.12xlarge
- r5d.2xlarge

#### Supported VM type in Azure

Select the Standard\_L8s\_v2 VM type with a single node Cloud Volumes ONTAP BYOL system in Azure.

#### 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. WORM storage is powered by SnapLock technology in Enterprise mode, which means WORM files are protected at the file level.

Once a file has been committed to WORM storage, it cannot be modified, even after the retention period has expired. A tamper-proof clock determines when the retention period for a WORM file has elapsed.

After the retention period has elapsed, you are responsible for deleting any files that you no longer need.

#### Activating WORM storage

You can activate WORM storage on a Cloud Volumes ONTAP system when you create a new working environment. This includes specifying an activation code and setting the default retention period for files. You can obtain an activation code by using the chat icon in the lower right of the Cloud Manager interface.



You cannot 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:

## WORM | [Preview](#)

You can use write once, read many (WORM) storage to retain critical files in unmodified form for regulatory and governance purposes and to protect from malware attacks. WORM files are protected at the file level.

[Learn More](#)

Disable WORM       Activate WORM

**Notice:** If you enable WORM storage, you cannot enable data tiering to object storage.

WORM Activation Code



Worm-111112222aaaaaa

Retention Period

15

years



### 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](#).



Cloud Volumes ONTAP support for WORM storage is equivalent to SnapLock Enterprise mode.

### Limitations

- If you delete or move a disk directly from AWS or Azure, then a volume can be deleted before its expiry date.
- When WORM storage is activated, data tiering to object storage can't be enabled.
- Cloud Backup must be disabled in order to enable WORM storage.

## High-availability pairs

### High-availability pairs in AWS

A Cloud Volumes ONTAP high availability (HA) configuration provides nondisruptive operations and fault tolerance. In AWS, data is synchronously mirrored between the two nodes.

## Overview

In AWS, Cloud Volumes ONTAP HA configurations include the following components:

- Two Cloud Volumes ONTAP nodes whose data is synchronously mirrored between each other.
- A mediator instance that provides a communication channel between the nodes to assist in storage takeover and giveback processes.



The mediator instance runs the Linux operating system on a t2.micro instance and uses one EBS magnetic disk that is approximately 8 GB.

## Storage takeover and giveback

If a node goes down, the other node can serve data for its partner to provide continued data service. Clients can access the same data from the partner node because the data was synchronously mirrored to the partner.

After the node reboots, the partner must resync data before it can return the storage. The time that it takes to resync data depends on how much data was changed while the node was down.

Storage takeover, resync, and giveback are all automatic by default. No user action is required.

## RPO and RTO

An HA configuration maintains high availability of your data as follows:

- The recovery point objective (RPO) is 0 seconds.  
Your data is transactionally consistent with no data loss.
- The recovery time objective (RTO) is 60 seconds.  
In the event of an outage, data should be available in 60 seconds or less.

## HA deployment models

You can ensure the high availability of your data by deploying an HA configuration across multiple Availability Zones (AZs) or in a single AZ. You should review more details about each configuration to choose which best fits your needs.

### Multiple Availability Zones

Deploying an HA configuration in multiple Availability Zones (AZs) ensures high availability of your data if a failure occurs with an AZ or an instance that runs a Cloud Volumes ONTAP node. You should understand how NAS IP addresses impact data access and storage failover.

### NFS and CIFS data access

When an HA configuration is spread across multiple Availability Zones, *floating IP addresses* enable NAS client access. The floating IP addresses, which must be outside of the CIDR blocks for all VPCs in the region, can migrate between nodes when failures occur. They aren't natively accessible to clients that are outside of the VPC, unless you [set up an AWS transit gateway](#).

If you can't set up a transit gateway, private IP addresses are available for NAS clients that are outside the VPC. However, these IP addresses are static—they can't failover between nodes.

You should review requirements for floating IP addresses and route tables before you deploy an HA configuration across multiple Availability Zones. You must specify the floating IP addresses when you deploy

the configuration. The private IP addresses are automatically created by Cloud Manager.

For details, see [AWS networking requirements for Cloud Volumes ONTAP HA in multiple AZs](#).

## iSCSI data access

Cross-VPC data communication is not an issue since iSCSI does not use floating IP addresses.

## Takeover and giveback for iSCSI

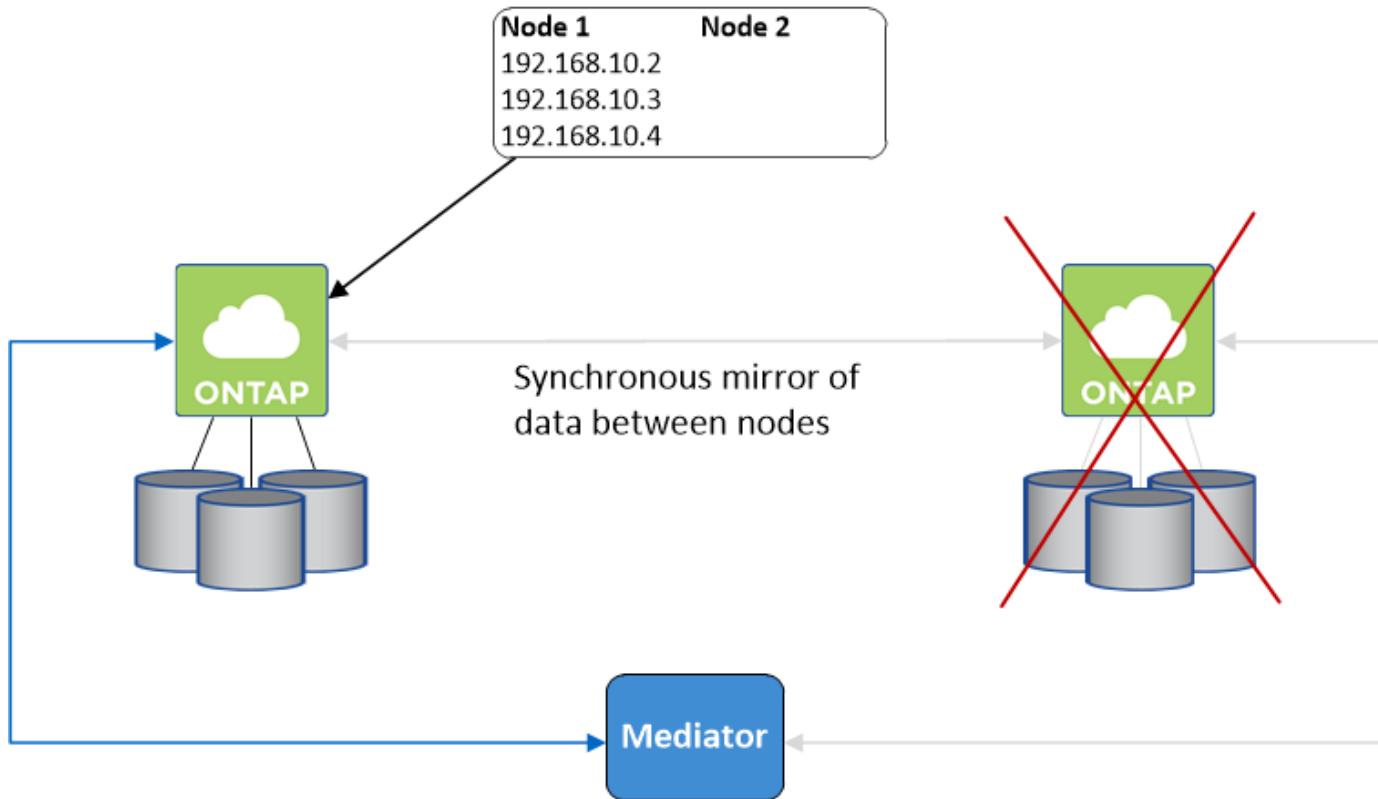
For iSCSI, Cloud Volumes ONTAP uses multipath I/O (MPIO) and Asymmetric Logical Unit Access (ALUA) to manage path failover between the active-optimized and non-optimized paths.



For information about which specific host configurations support ALUA, see the [NetApp Interoperability Matrix Tool](#) and the Host Utilities Installation and Setup Guide for your host operating system.

## Takeover and giveback for NAS

When takeover occurs in a NAS configuration using floating IPs, the node's floating IP address that clients use to access data moves to the other node. The following image depicts storage takeover in a NAS configuration using floating IPs. If node 2 goes down, the floating IP address for node 2 moves to node 1.



NAS data IPs used for external VPC access cannot migrate between nodes if failures occur. If a node goes offline, you must manually remount volumes to clients outside the VPC by using the IP address on the other node.

After the failed node comes back online, remount clients to volumes using the original IP address. This step is needed to avoid transferring unnecessary data between two HA nodes, which can cause significant performance and stability impact.

You can easily identify the correct IP address from Cloud Manager by selecting the volume and clicking **Mount Command**.

#### Cloud Volumes ONTAP HA in a single Availability Zone

Deploying an HA configuration in a single Availability Zone (AZ) can ensure high availability of your data if an instance that runs a Cloud Volumes ONTAP node fails. All data is natively accessible from outside of the VPC.



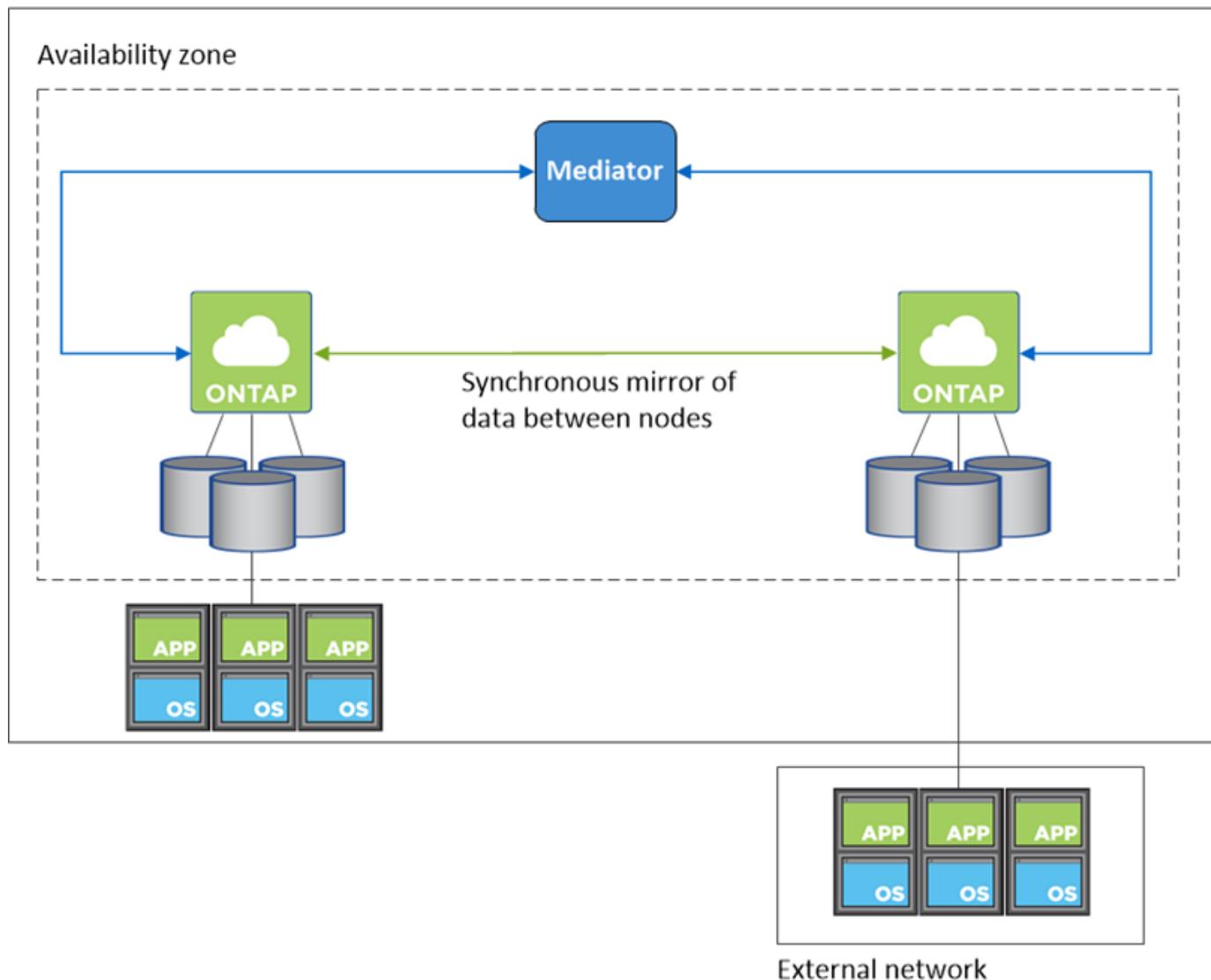
Cloud Manager creates an [AWS spread placement group](#) and launches the two HA nodes in that placement group. The placement group reduces the risk of simultaneous failures by spreading the instances across distinct underlying hardware. This feature improves redundancy from a compute perspective and not from disk failure perspective.

#### Data access

Because this configuration is in a single AZ, it does not require floating IP addresses. You can use the same IP address for data access from within the VPC and from outside the VPC.

The following image shows an HA configuration in a single AZ. Data is accessible from within the VPC and from outside the VPC.

## VPC in AWS



### Takeover and giveback

For iSCSI, Cloud Volumes ONTAP uses multipath I/O (MPIO) and Asymmetric Logical Unit Access (ALUA) to manage path failover between the active-optimized and non-optimized paths.



For information about which specific host configurations support ALUA, see the [NetApp Interoperability Matrix Tool](#) and the Host Utilities Installation and Setup Guide for your host operating system.

For NAS configurations, the data IP addresses can migrate between HA nodes if failures occur. This ensures client access to storage.

### How storage works in an HA pair

Unlike an ONTAP cluster, storage in a Cloud Volumes ONTAP HA pair is not shared between nodes. Instead, data is synchronously mirrored between the nodes so that the data is available in the event of failure.

## Storage allocation

When you create a new volume and additional disks are required, 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.



You can set up an active-active configuration only when using Cloud Manager in the Storage System View.

## Performance expectations

A Cloud Volumes ONTAP HA configuration synchronously replicates data between nodes, which consumes network bandwidth. As a result, you can expect the following performance in comparison to a single-node Cloud Volumes ONTAP configuration:

- For HA configurations that serve data from only one node, read performance is comparable to the read performance of a single-node configuration, whereas write performance is lower.
- For HA configurations that serve data from both nodes, read performance is higher than the read performance of a single-node configuration, and write performance is the same or higher.

For more details about Cloud Volumes ONTAP performance, see [Performance](#).

## Client access to storage

Clients should access NFS and CIFS volumes by using the data IP address of the node on which the volume resides. If NAS clients access a volume by using the IP address of the partner node, traffic goes between both nodes, which reduces performance.

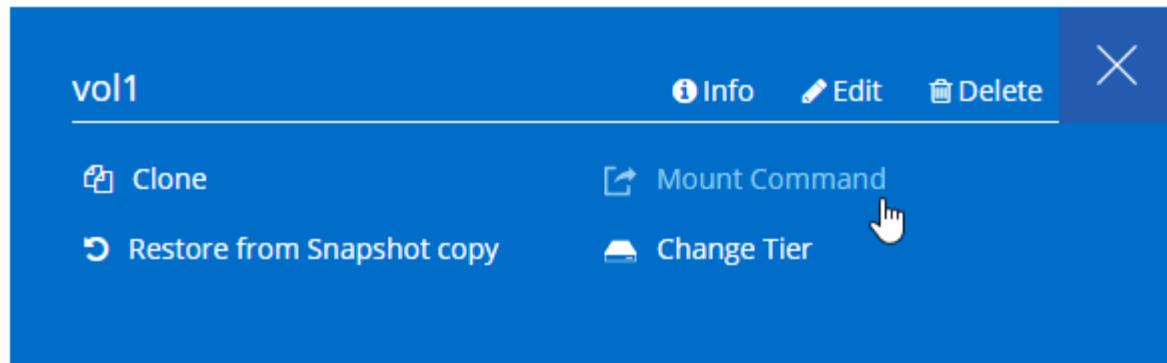


If you move a volume between nodes in an HA pair, you should remount the volume by using the IP address of the other node. Otherwise, you can experience reduced performance. If clients support NFSv4 referrals or folder redirection for CIFS, you can enable those features on the Cloud Volumes ONTAP systems to avoid remounting the volume. For details, see ONTAP documentation.

You can easily identify the correct IP address from Cloud Manager:

## Volumes

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

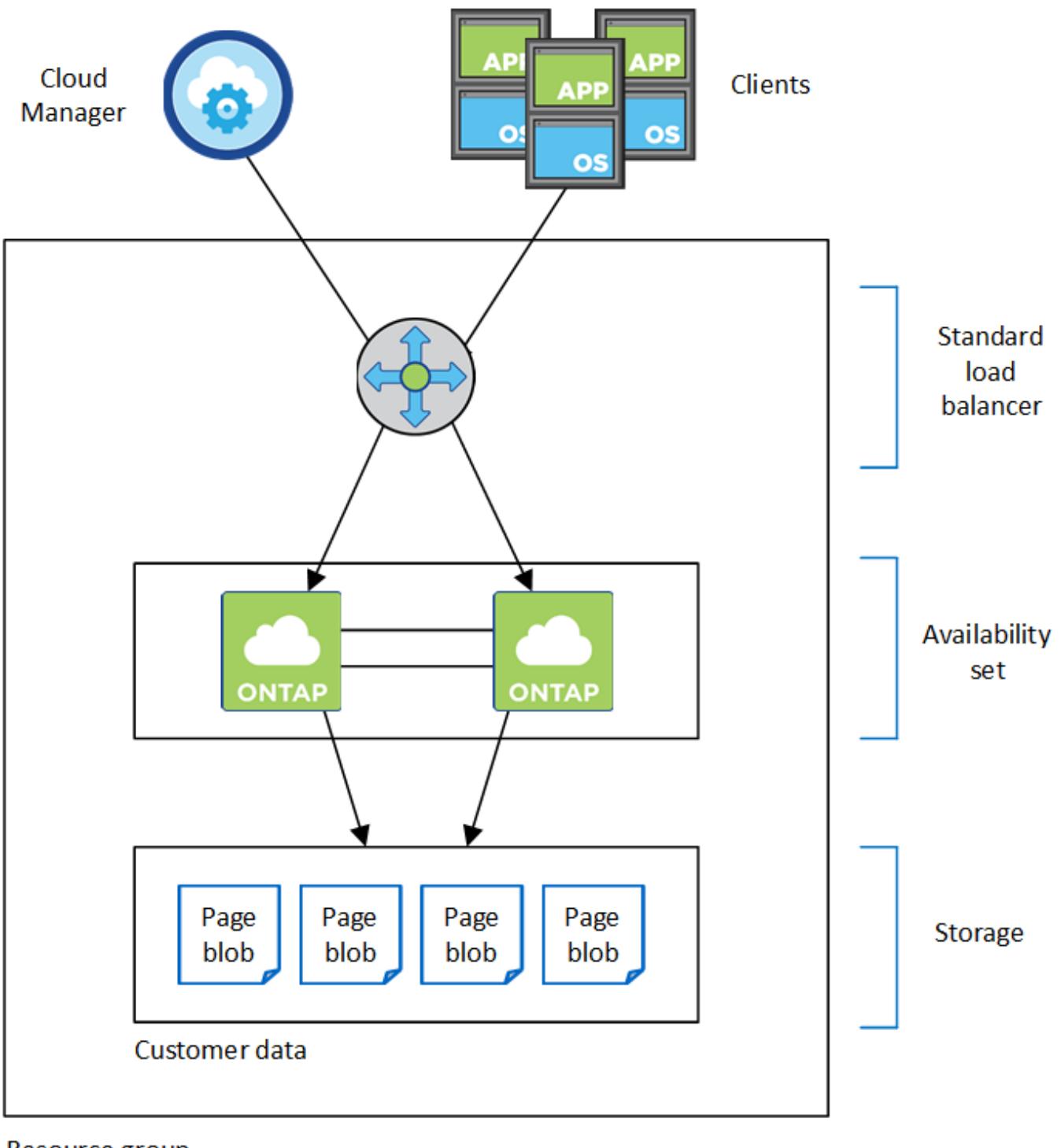


### High-availability pairs in Azure

A Cloud Volumes ONTAP high availability (HA) pair provides enterprise reliability and continuous operations in case of failures in your cloud environment. In Azure, storage is shared between the two nodes.

#### HA components

A Cloud Volumes ONTAP HA configuration in Azure includes the following components:



## Resource group

Note the following about the Azure components that Cloud Manager deploys for you:

### Azure Standard Load Balancer

The load balancer manages incoming traffic to the Cloud Volumes ONTAP HA pair.

### Availability Set

The Availability Set ensures that the nodes are in different fault and update domains.

## Disks

Customer data resides on Premium Storage page blobs. Each node has access to the other node's storage. Additional storage is also required for [boot, root, and core data](#).

## Storage accounts

- One storage account is required for managed disks.
- One or more storage accounts are required for the Premium Storage page blobs, as the disk capacity limit per storage account is reached.

[Azure documentation: Azure Storage scalability and performance targets for storage accounts](#).

- One storage account is required for data tiering to Azure Blob storage.
- Starting with Cloud Volumes ONTAP 9.7, the storage accounts that Cloud Manager creates for HA pairs are general-purpose v2 storage accounts.
- You can enable an HTTPS connection from a Cloud Volumes ONTAP 9.7 HA pair to Azure storage accounts when creating a working environment. Note that enabling this option can impact write performance. You can't change the setting after you create the working environment.

## RPO and RTO

An HA configuration maintains high availability of your data as follows:

- The recovery point objective (RPO) is 0 seconds.  
Your data is transactionally consistent with no data loss.
- The recovery time objective (RTO) is 60 seconds.  
In the event of an outage, data should be available in 60 seconds or less.

## Storage takeover and giveback

Similar to a physical ONTAP cluster, storage in an Azure HA pair is shared between nodes. Connections to the partner's storage allows each node to access the other's storage in the event of a *takeover*. Network path failover mechanisms ensure that clients and hosts continue to communicate with the surviving node. The partner *gives back* storage when the node is brought back on line.

For NAS configurations, data IP addresses automatically migrate between HA nodes if failures occur.

For iSCSI, Cloud Volumes ONTAP uses multipath I/O (MPIO) and Asymmetric Logical Unit Access (ALUA) to manage path failover between the active-optimized and non-optimized paths.



For information about which specific host configurations support ALUA, see the [NetApp Interoperability Matrix Tool](#) and the Host Utilities Installation and Setup Guide for your host operating system.

Storage takeover, resync, and giveback are all automatic by default. No user action is required.

## Storage configurations

You can use an HA pair as an active-active configuration, in which both nodes serve data to clients, or as an active-passive configuration, in which the passive node responds to data requests only if it has taken over storage for the active node.

## HA limitations

The following limitations affect Cloud Volumes ONTAP HA pairs in Azure:

- HA pairs are supported with Cloud Volumes ONTAP Standard, Premium, and BYOL. Explore is not supported.
- NFSv4 is not supported. NFSv3 is supported.
- HA pairs are not supported in some regions.

[See the list of supported Azure regions.](#)

[Learn how to deploy an HA system in Azure.](#)

## High-availability pairs in Google Cloud Platform

A Cloud Volumes ONTAP high availability (HA) configuration provides nondisruptive operations and fault tolerance. In Google Cloud Platform, data is synchronously mirrored between the two nodes.

### HA components

Cloud Volumes ONTAP HA configurations in GCP 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.

The mediator runs the Linux operating system on a f1-micro instance and uses two standard persistent disks that are 10 GB each.

- Four Virtual Private Clouds (VPCs) are required for the HA configuration.

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.](#)

### 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)

The screenshot shows a Cloud Manager interface for a volume named 'vol1'. At the top, there's a blue header bar with the volume name 'vol1' on the left and three action buttons: 'Info', 'Edit', and 'Delete' on the right. Below the header, there's a list of actions: 'Clone', 'Mount Command' (which has a cursor icon pointing to it), 'Restore from Snapshot copy', and 'Change Tier'. The background of the main area is blue.

## Related links

- [Learn about networking requirements](#)
- [Learn how to get started in GCP](#)

## Evaluating

You can evaluate Cloud Volumes ONTAP before you pay for the software. The most common way is to launch the PAYGO version of your first Cloud Volumes ONTAP system to get a 30-day free trial. An evaluation BYOL license is also an option.

If you need assistance with your proof of concept, contact [the Sales team](#) or reach out through the chat option available from [NetApp Cloud Central](#) and from within Cloud Manager.

### 30-day free trials for PAYGO

A 30-day free trial is available if you plan to pay for Cloud Volumes ONTAP as you go. You can start a 30-day free trial of Cloud Volumes ONTAP from Cloud Manager by creating your first Cloud Volumes ONTAP system in a payer's account.

There are no hourly software license charges for the instance, but infrastructure charges from your cloud

provider still apply.

A free trial automatically converts to a paid hourly subscription when it expires. If you terminate the instance within the time limit, the next instance that you deploy is not part of the free trial (even if it's deployed within those 30 days).

Pay-as-you-go trials are awarded through a cloud provider and are not extendable by any means.

## Evaluation licenses for BYOL

An evaluation BYOL license is an option for customers who expect to pay for Cloud Volumes ONTAP by purchasing a termed license from NetApp. You can obtain an evaluation license from your account team, your Sales Engineer, or your partner.

The evaluation key is good for 30 days, and can be used multiple times, each for 30 days (regardless of the creation day).

At the end of 30 days, daily shutdowns will occur, so it's best to plan ahead. You can apply a new BYOL license on top of the evaluation license for an in-place upgrade (this requires a restart of single node systems). Your hosted data is **not** deleted at the end of the trial period.



You can't upgrade Cloud Volumes ONTAP software when using an evaluation license.

## Licensing

Each Cloud Volumes ONTAP BYOL system must have a system license installed with an active subscription. Cloud Manager simplifies the process by managing licenses for you and by notifying you before they expire. BYOL licenses are also available for Cloud Backup.

### BYOL system licenses

You can purchase multiple licenses for a Cloud Volumes ONTAP BYOL system to allocate more than 368 TB of capacity. For example, you might purchase two licenses to allocate up to 736 TB of capacity to Cloud Volumes ONTAP. Or you could purchase four licenses to get up to 1.4 PB.

The number of licenses that you can purchase for a single node system or HA pair is unlimited.

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

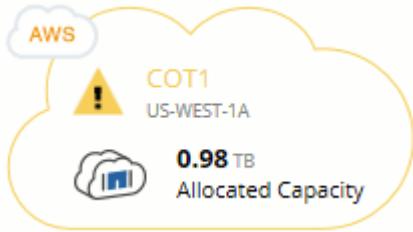
When you create a BYOL system, Cloud Manager prompts you for the serial number of your license and your NetApp Support Site account. Cloud Manager uses the account to download the license file from NetApp and to install it on the Cloud Volumes ONTAP system.

[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. For instructions, see [Managing BYOL licenses for Cloud Volumes ONTAP](#).

## License expiration warning

Cloud Manager warns you 30 days before a license is due to expire and again when the license expires. The following image shows a 30-day expiration warning:



You can select the working environment to review the message.

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.



Cloud Volumes ONTAP can also notify you through email, an SNMP traphost, or syslog server using EMS (Event Management System) event notifications. For instructions, see the [ONTAP 9 EMS Configuration Express Guide](#).

## License renewal

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. For instructions, see [Managing BYOL licenses for Cloud Volumes ONTAP](#).

## BYOL backup licenses

A BYOL backup license allows you to purchase a license from NetApp to use Cloud Backup for a certain period of time and for a maximum amount backup space. When either limit is reached you will need to renew the license.

[Learn more about the Cloud Backup BYOL license.](#)

## Security

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

### Encryption of data at rest

Cloud Volumes ONTAP supports the following encryption technologies:

- NetApp encryption solutions (NVE and NAE)
- AWS Key Management Service
- Azure Storage Service Encryption
- Google Cloud Platform default encryption

You can use NetApp encryption solutions with native encryption from AWS, Azure, or GCP, which encrypt 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 both NetApp Volume Encryption (NVE) and NetApp Aggregate Encryption (NAE) with an external key manager. NVE and NAE are software-based solutions that enable (FIPS) 140-2-compliant data-at-rest encryption of volumes.

- 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 use AES 256-bit encryption.

[Learn more about NetApp Volume Encryption and NetApp Aggregate Encryption.](#)

Starting with Cloud Volumes ONTAP 9.7, new aggregates will 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, see [Encrypting volumes with NetApp encryption solutions](#).

### AWS Key Management Service

When you launch a Cloud Volumes ONTAP system in AWS, you can enable data encryption using the [AWS Key Management Service \(KMS\)](#). Cloud Manager requests data keys using a customer master key (CMK).



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

If you want to use this encryption option, then you must ensure that the AWS KMS is set up appropriately. For details, see [Setting up the AWS KMS](#).

### Azure Storage Service Encryption

[Azure Storage Service Encryption](#) for data at rest is enabled by default for Cloud Volumes ONTAP data in Azure. No setup is required.

You can encrypt Azure managed disks on single node Cloud Volumes ONTAP systems using external keys from another account. This feature is supported using Cloud Manager APIs.

You just need to add the following to the API request when creating the single node system:

```
"azureEncryptionParameters": {  
    "key": <azure id of encryptionset>  
}
```



Customer-managed keys are not supported with Cloud Volumes ONTAP HA pairs.

## 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.

- Cloud Volumes ONTAP for AWS

[NetApp Technical Report 4383: Performance Characterization of Cloud Volumes ONTAP in Amazon Web Services with Application Workloads.](#)

- Cloud Volumes ONTAP for Microsoft Azure

[NetApp Technical Report 4671: Performance Characterization of Cloud Volumes ONTAP in Azure with Application Workloads.](#)

- Cloud Volumes ONTAP for Google Cloud

[NetApp Technical Report 4816: Performance Characterization of Cloud Volumes ONTAP for Google Cloud.](#)

## 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.

### Defaults

- Cloud Volumes ONTAP is available as a single-node system and as an HA pair in AWS, Azure, and GCP.
- 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.](#)
- Cloud Manager automatically installs the following ONTAP feature licenses on Cloud Volumes ONTAP:
  - CIFS

- FlexCache
- FlexClone
- iSCSI
- 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 Azure and in GCP, on single node systems in AWS, and optionally on HA systems in multiple AWS Availability Zones
  - A node management LIF
  - An iSCSI data LIF
  - A CIFS and NFS data LIF



LIF failover is disabled by default for Cloud Volumes ONTAP due to EC2 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 data-bbox="432 1615 489 1679" data-label="Image"> </div> The Account Admin can modify this value from the Settings page.
Security style	NTFS for CIFS volumes UNIX for NFS volumes
Space guarantee style	none

Attribute	Value set by Cloud Manager
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.

### AWS

- Two disks per node for boot and root data:
  - 9.7: 160 GB io1 disk for boot data and a 220 GB gp2 disk for root data
  - 9.6: 93 GB io1 disk for boot data and a 140 GB gp2 disk for root data
  - 9.5: 45 GB io1 disk for boot data and a 140 GB gp2 disk for root data
- Starting with version 9.8, a 540 GB General Purpose SSD for a core disk when using a C5, M5, or R5 instance type
- One EBS snapshot for each boot disk and root disk
- For HA pairs, one EBS volume for the Mediator instance, which is approximately 8 GB

### Azure (single node)

- Three Premium SSD disks:
  - One 10 GB disk for boot data
  - One 140 GB disk for root data
  - One 128 GB disk for NVRAM

If the virtual machine that you chose for Cloud Volumes ONTAP supports Ultra SSDs, then the system uses an Ultra SSD for NVRAM, rather than a Premium SSD.

- One 1024 GB Standard HDD disk for saving cores
- One Azure snapshot for each boot disk and root disk

### Azure (HA pairs)

- Two 10 GB Premium SSD disks for the boot volume (one per node)
- Two 140 GB Premium Storage page blobs for the root volume (one per node)
- Two 1024 GB Standard HDD disks for saving cores (one per node)
- Two 128 GB Premium SSD disks for NVRAM (one per node)
- One Azure snapshot for each boot disk and root disk

### GCP

- One 10 GB Standard persistent disk for boot data

- One 64 GB Standard persistent disk for root data
- One 500 GB Standard persistent disk for NVRAM
- One 315 GB Standard persistent disk for saving cores
- One GCP snapshot each for the boot disk and root disk

For an HA pair, there are two disks per node for root data.

#### **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.

#### **Encryption**

Boot and root disks are always encrypted in Azure and Google Cloud Platform because encryption is enabled by default in those cloud providers.

When you enable data encryption in AWS using the Key Management Service (KMS), the boot and root disks for Cloud Volumes ONTAP are encrypted, as well. This includes the boot disk for the mediator instance in an HA pair. The disks are encrypted using the CMK that you select when you create the working environment.

## **Get started in AWS**

### **Getting started with Cloud Volumes ONTAP for AWS**

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



#### **Create a Connector**

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

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.



#### **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.](#)

## 3

### Set up your networking

- a. Ensure that your VPC and subnets will support connectivity between the Connector and Cloud Volumes ONTAP.
- b. Enable outbound internet access from the target VPC 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](#).

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

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

[Learn more about networking requirements](#).

## 4

### Set up the AWS KMS

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

## 5

### Launch Cloud Volumes ONTAP using 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

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

## Planning your Cloud Volumes ONTAP configuration in AWS

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

## **Viewing supported regions**

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

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

## **Choosing a license type**

Cloud Volumes ONTAP is available in two pricing options: pay-as-you-go and Bring Your Own License (BYOL). For pay-as-you-go, you can choose from three licenses: Explore, Standard, or Premium. Each license provides different capacity and compute options.

[Supported configurations for Cloud Volumes ONTAP 9.8 in AWS](#)

## **Choosing a supported instance**

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

[Supported configurations for Cloud Volumes ONTAP 9.8 in AWS](#)

## **Choosing a configuration that supports Flash Cache**

Some Cloud Volumes ONTAP configurations in AWS include local NVMe storage, which Cloud Volumes ONTAP uses as *Flash Cache* for better performance. [Learn more about Flash Cache.](#)

## **Understanding 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 9.8 in AWS](#)

## **Sizing your system in AWS**

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

### **Instance type**

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

### **EBS disk type**

General Purpose SSDs are the most common disk type for Cloud Volumes ONTAP. To view the use cases for EBS disks, refer to [AWS Documentation: EBS Volume Types](#).

### **EBS disk size**

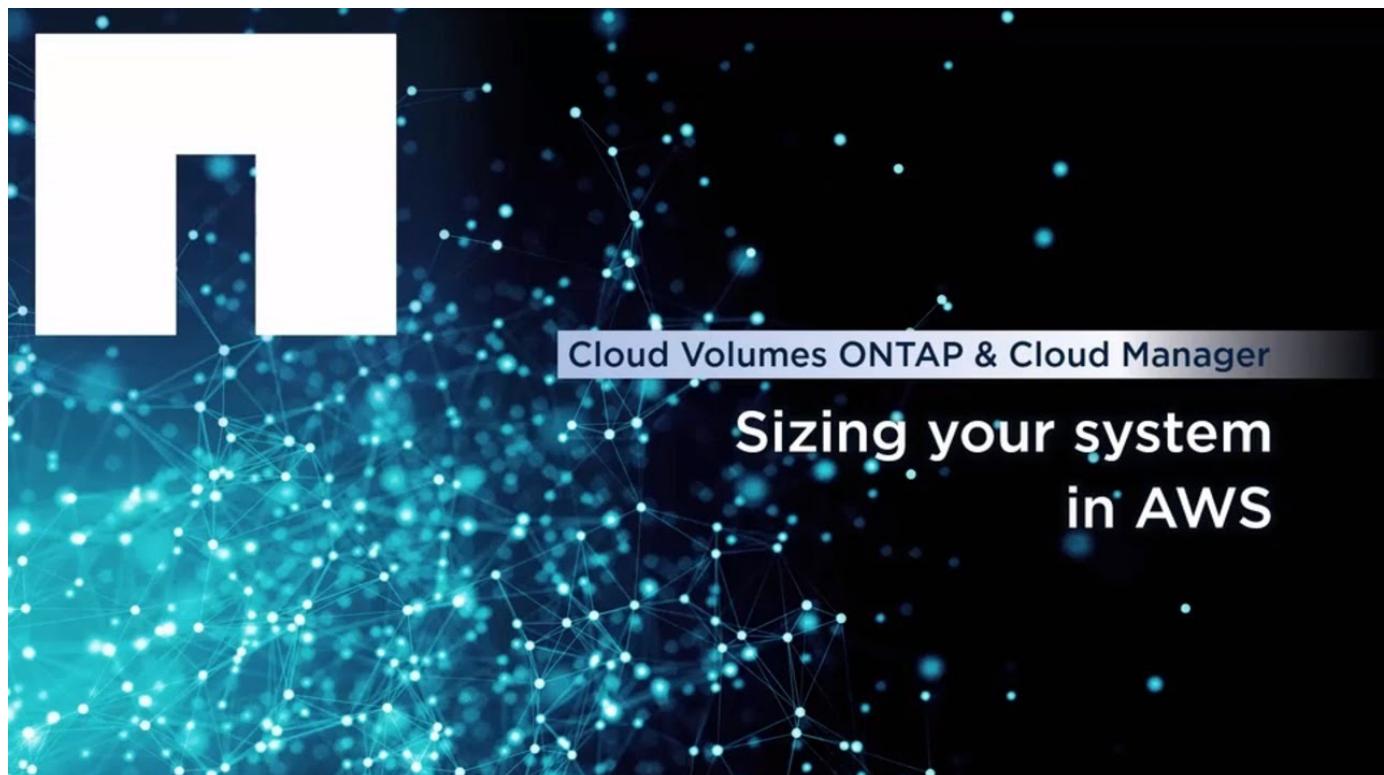
You need to choose an initial disk size when you launch a Cloud Volumes ONTAP system. After that, you

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

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

Watch the following video for more details about sizing your Cloud Volumes ONTAP system in AWS:



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

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

There are a few limitations to point out:

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

## AWS network information worksheet

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

### Network information for Cloud Volumes ONTAP

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

### Network information for an HA pair in multiple AZs

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

### Choosing a write speed

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

## Choosing 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.

## Set up your networking

### Networking requirements for Cloud Volumes ONTAP in AWS

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

#### General requirements for Cloud Volumes ONTAP

The following requirements must be met in AWS.

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

Cloud Volumes ONTAP nodes require outbound internet access to send messages to NetApp AutoSupport, which proactively monitors the health of your storage.

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

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

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

[Learn how to configure AutoSupport.](#)

#### Outbound internet access for the HA mediator

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

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

EC2 service. For details about VPC endpoints, refer to [AWS Documentation: Interface VPC Endpoints \(AWS PrivateLink\)](#).

## Number of IP addresses

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

- Single node: 6 IP addresses
- HA pairs in single AZs: 15 addresses
- HA pairs in multiple AZs: 15 or 16 IP addresses

Note that Cloud Manager creates an SVM management LIF on single node systems, but not on HA pairs in a single AZ. You can choose whether to create an SVM management LIF on HA pairs in multiple AZs.



A LIF is an IP address associated with a physical port. An SVM management LIF is required for management tools like SnapCenter.

## Security groups

You do not need to create security groups because Cloud Manager does that for you. If you need to use your own, refer to [Security group rules](#).

## Connection from Cloud Volumes ONTAP to AWS S3 for data tiering

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

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

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

## Connections to ONTAP systems in other networks

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

## DNS and Active Directory for CIFS

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

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

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

## Requirements for HA pairs in multiple AZs

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

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

## Availability Zones

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

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

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

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



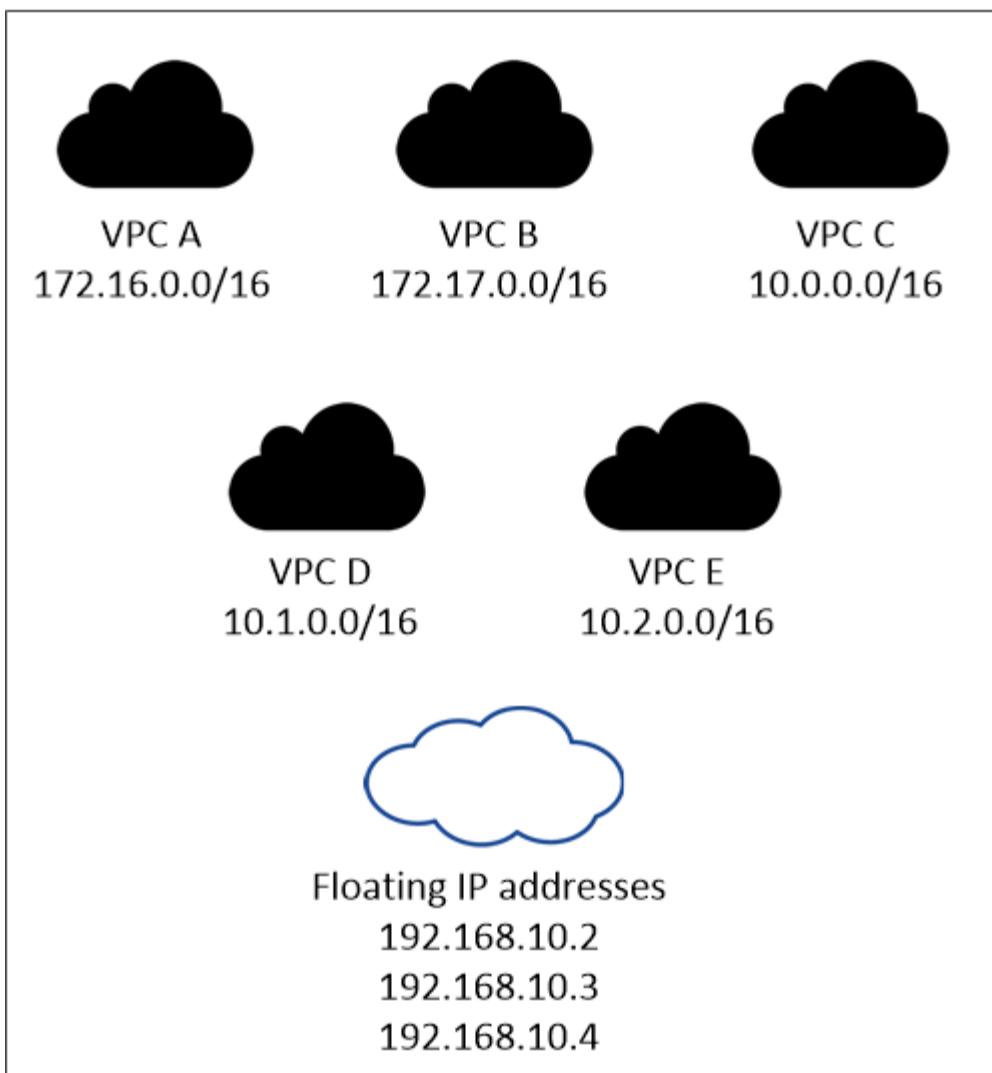
A floating IP address is required for the SVM management LIF if you use SnapDrive for Windows or SnapCenter with the HA pair. If you don't specify the IP address when you deploy the system, you can create the LIF later. For details, see [Setting up Cloud Volumes ONTAP](#).

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

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

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

## AWS region



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

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

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

### Route tables

After you specify the floating IP addresses in Cloud Manager, you need to select the route tables that should include routes to the floating IP addresses. This enables client access to the HA pair.

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

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

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

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

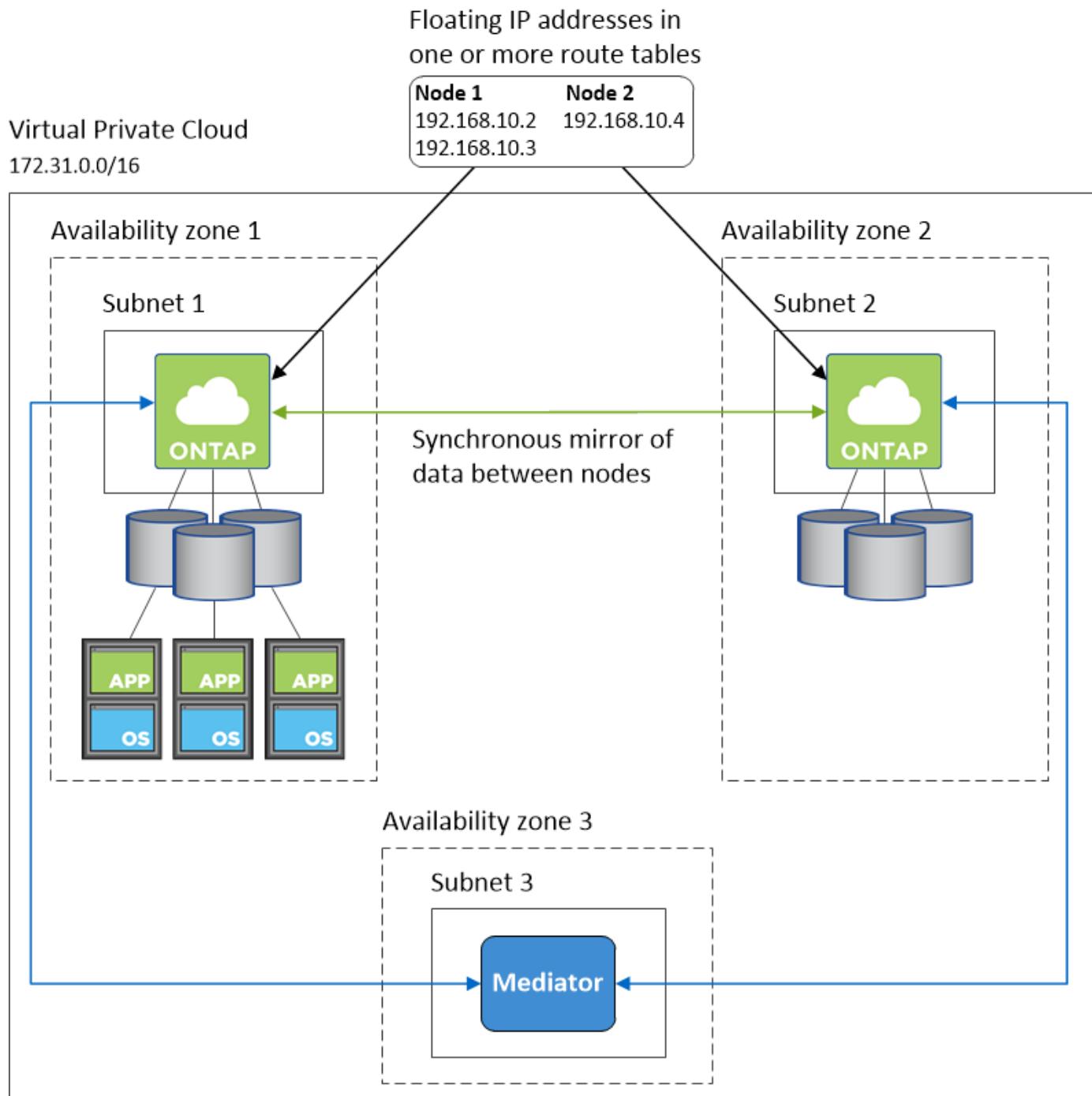
## Connection to NetApp management tools

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

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

## Example HA configuration

The following image shows an optimal HA configuration in AWS operating as an active-passive configuration:



#### 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 and VNets in which you want to deploy Cloud

## Volumes ONTAP

For example, if you install a Connector in your corporate network, then you must set up a VPN connection to the VPC or VNet in which you launch Cloud Volumes ONTAP.

### Outbound internet access

The Connector requires outbound internet access to manage resources and processes within your public cloud environment. A Connector contacts the following endpoints when managing resources in AWS:

Endpoints	Purpose
AWS services (amazonaws.com): <ul style="list-style-type: none"><li>• CloudFormation</li><li>• Elastic Compute Cloud (EC2)</li><li>• Key Management Service (KMS)</li><li>• Security Token Service (STS)</li><li>• Simple Storage Service (S3)</li></ul> <p>The exact endpoint depends on the region in which you deploy Cloud Volumes ONTAP. <a href="#">Refer to AWS documentation for details.</a></p>	Enables the Connector to deploy and manage Cloud Volumes ONTAP in AWS.
<a href="https://api.services.cloud.netapp.com:443">https://api.services.cloud.netapp.com:443</a>	API requests to NetApp Cloud Central.
<a href="https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com">https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com</a>	Provides access to software images, manifests, and templates.
<a href="https://cognito-idp.us-east-1.amazonaws.com">https://cognito-idp.us-east-1.amazonaws.com</a> <a href="https://cognito-identity.us-east-1.amazonaws.com">https://cognito-identity.us-east-1.amazonaws.com</a> <a href="https://sts.amazonaws.com">https://sts.amazonaws.com</a> <a href="https://cloud-support-netapp-com-accelerated.s3.amazonaws.com">https://cloud-support-netapp-com-accelerated.s3.amazonaws.com</a>	Enables the Connector to access and download manifests, templates, and Cloud Volumes ONTAP upgrade images.
<a href="https://cloudmanagerinfraprod.azurecr.io">https://cloudmanagerinfraprod.azurecr.io</a>	Access to software images of container components for an infrastructure that's running Docker and provides a solution for service integrations with Cloud Manager.
<a href="https://kinesis.us-east-1.amazonaws.com">https://kinesis.us-east-1.amazonaws.com</a>	Enables NetApp to stream data from audit records.
<a href="https://cloudmanager.cloud.netapp.com">https://cloudmanager.cloud.netapp.com</a>	Communication with the Cloud Manager service, which includes Cloud Central accounts.
<a href="https://netapp-cloud-account.auth0.com">https://netapp-cloud-account.auth0.com</a>	Communication with NetApp Cloud Central for centralized user authentication.
<a href="https://support.netapp.com:443">support.netapp.com:443</a>	Communication with NetApp AutoSupport.

Endpoints	Purpose
<a href="https://support.netapp.com/svcgw">https://support.netapp.com/svcgw</a> <a href="https://support.netapp.com/ServiceGW/entitlement">https://support.netapp.com/ServiceGW/entitlement</a> <a href="https://eval.lic.netapp.com.s3.us-west-1.amazonaws.com">https://eval.lic.netapp.com.s3.us-west-1.amazonaws.com</a> <a href="https://cloud-support-netapp-com.s3.us-west-1.amazonaws.com">https://cloud-support-netapp-com.s3.us-west-1.amazonaws.com</a>	Communication with NetApp for system licensing and support registration.
<a href="https://client.infra.support.netapp.com.s3.us-west-1.amazonaws.com">https://client.infra.support.netapp.com.s3.us-west-1.amazonaws.com</a> <a href="https://cloud-support-netapp-com-accelerated.s3.us-west-1.amazonaws.com">https://cloud-support-netapp-com-accelerated.s3.us-west-1.amazonaws.com</a> <a href="https://trigger.asup.netapp.com.s3.us-west-1.amazonaws.com">https://trigger.asup.netapp.com.s3.us-west-1.amazonaws.com</a>	Enables NetApp to collect information needed to troubleshoot support issues.
<a href="https://ipa-signer.cloudmanager.netapp.com">https://ipa-signer.cloudmanager.netapp.com</a>	Enables Cloud Manager to generate licenses (for example, a FlexCache license for Cloud Volumes ONTAP)
Various third-party locations, for example: <ul style="list-style-type: none"> <li>• <a href="https://repo1.maven.org/maven2">https://repo1.maven.org/maven2</a></li> <li>• <a href="https://oss.sonatype.org/content/repositories">https://oss.sonatype.org/content/repositories</a></li> <li>• <a href="https://repo.typesafe.com">https://repo.typesafe.com</a></li> </ul> <p>Third-party locations are subject to change.</p>	During upgrades, Cloud Manager downloads the latest packages for third-party dependencies.

While you should perform almost all tasks from the SaaS user interface, a local user interface is still available on the Connector. The machine running the web browser must have connections to the following endpoints:

Endpoints	Purpose
The Connector host	<p>You must enter the host's IP address from a web browser to load the Cloud Manager console.</p> <p>Depending on your connectivity to your cloud provider, you can use the private IP or a public IP assigned to the host:</p> <ul style="list-style-type: none"> <li>• A private IP works if you have a VPN and direct connect access to your virtual network</li> <li>• A public IP works in any networking scenario</li> </ul> <p>In any case, you should secure network access by ensuring that security group rules allow access from only authorized IPs or subnets.</p>
<a href="https://auth0.com">https://auth0.com</a> <a href="https://cdn.auth0.com">https://cdn.auth0.com</a> <a href="https://netapp-cloud-account.auth0.com">https://netapp-cloud-account.auth0.com</a> <a href="https://services.cloud.netapp.com">https://services.cloud.netapp.com</a>	Your web browser connects to these endpoints for centralized user authentication through NetApp Cloud Central.

Endpoints	Purpose
<a href="https://widget.intercom.io">https://widget.intercom.io</a>	For in-product chat that enables you to talk to NetApp cloud experts.

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

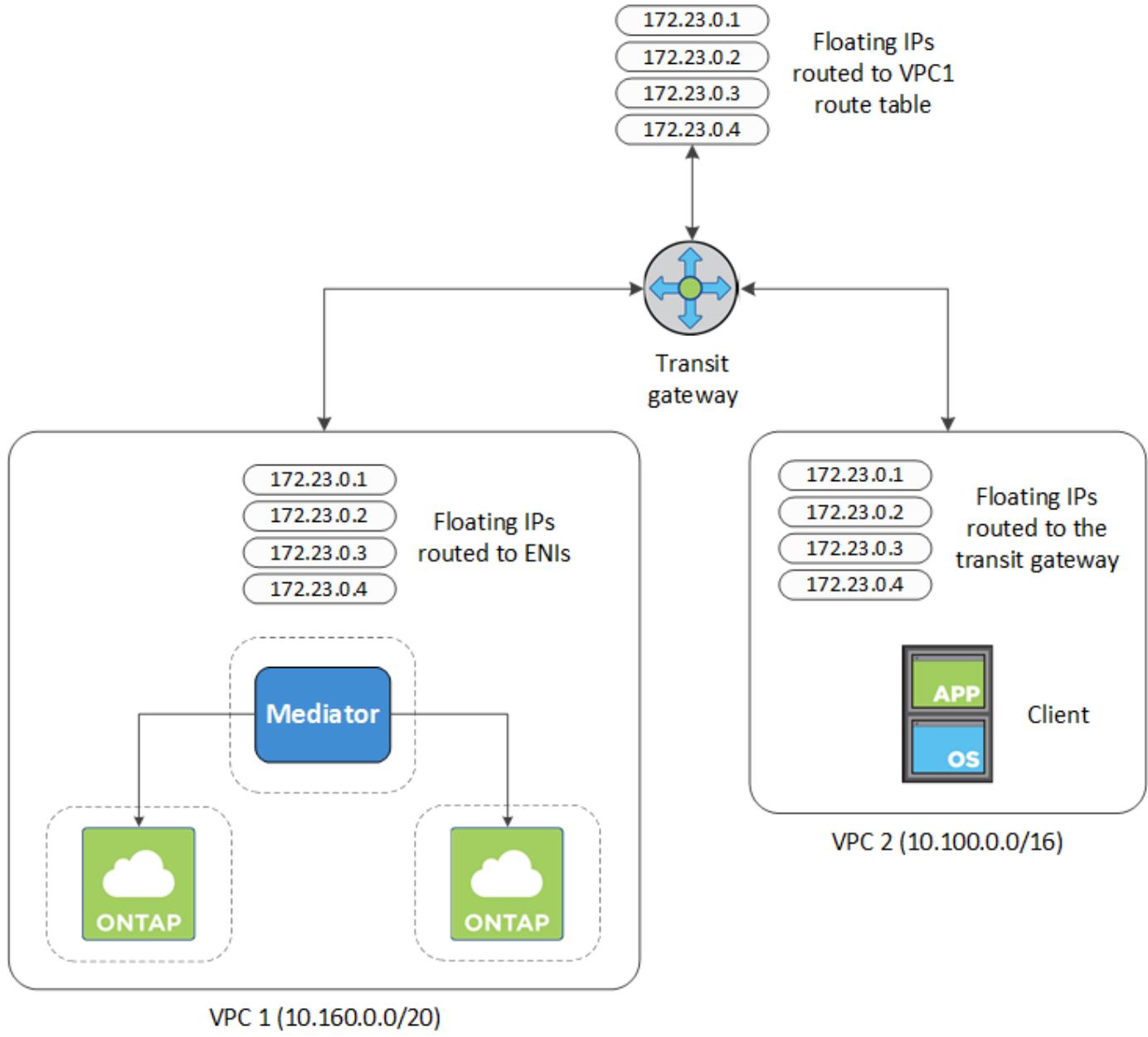
Set up an AWS transit gateway to enable access to an HA pair's [floating IP addresses](#) from outside the VPC where the HA pair resides.

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

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

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

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



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

## Steps

1. Create a transit gateway and attach the VPCs to the gateway.
2. Create routes in the transit gateway's route table by specifying the HA pair's floating IP addresses.

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

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

### Auto failover

Cluster Management : 172.23.0.1

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

### Access

SVM Management : 172.23.0.4

The following sample image shows the route table for the transit gateway. It includes routes to the CIDR blocks of the two VPCs and four floating IP addresses used by Cloud Volumes ONTAP.

Transit Gateway Route Table: tgw-rtb-0ea8ee291c7aedd3					
Details	Associations	Propagations	Routes	Tags	
The table below will return a maximum of 1000 routes. Narrow the filter or use export routes to view more routes.					
<a href="#">Create route</a>	<a href="#">Replace route</a>	<a href="#">Delete route</a>			
<input type="text"/> Filter by attributes or search by keyword					
CIDR	Attachment		Resource type	Route type	Route state
10.100.0.0/16	tgw-attach-05e77bd34e2ff91f8   vpc-0b2bc30e0dc8e0db1		VPC2	propagated	active
10.160.0.0/20	tgw-attach-00eba3eac3250d7db   vpc-673ae603		VPC1	propagated	active
172.23.0.1/32	tgw-attach-00eba3eac3250d7db   vpc-673ae603	VPC	static	active	
172.23.0.2/32	tgw-attach-00eba3eac3250d7db   vpc-673ae603	VPC	static	active	
172.23.0.3/32	tgw-attach-00eba3eac3250d7db   vpc-673ae603	VPC	static	active	
172.23.0.4/32	tgw-attach-00eba3eac3250d7db   vpc-673ae603	VPC	static	active	

3. Modify the route table of VPCs that need to access the floating IP addresses.

- Add route entries to the floating IP addresses.
- Add a route entry to the CIDR block of the VPC where the HA pair resides.

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

Route Table: rtb-0569a1bd740ed033f				
Summary	Routes	Subnet Associations	Route Propagation	Tags
<a href="#">Edit routes</a>				
View <a href="#">All routes</a> ▾				
Destination	Target	Status	Propagated	
10.100.0.0/16	local	active	No	
0.0.0.0/0	igw-07250bd01781e67df	active	No	
10.160.0.0/20	taw-015b7c249661ac279	active	No	VPC1
172.23.0.1/32	tgw-015b7c249661ac279	active	No	
172.23.0.2/32	tgw-015b7c249661ac279	active	No	
172.23.0.3/32	tgw-015b7c249661ac279	active	No	
172.23.0.4/32	tgw-015b7c249661ac279	active	No	Floating IP Addresses

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

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

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

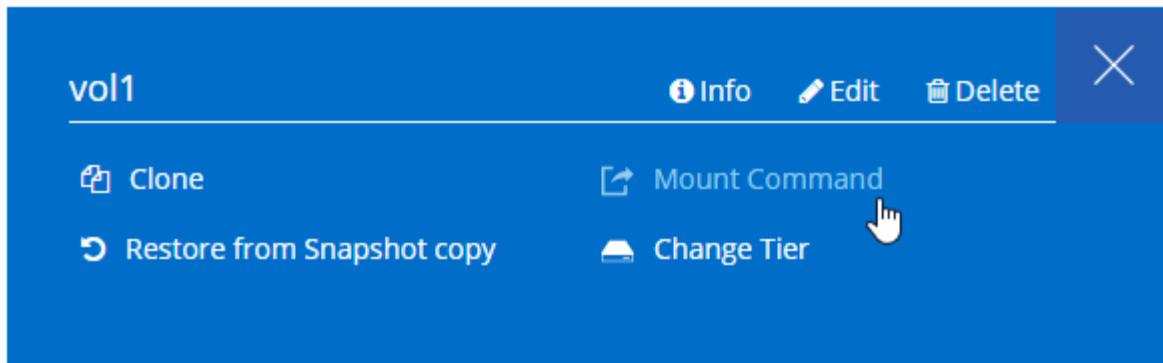
Route Table: rtb-0569a1bd740ed033f				
Summary	Routes	Subnet Associations	Route Propagation	Tags
<a href="#">Edit routes</a>				
View <a href="#">All routes</a> ▾				
Destination	Target	Status		
10.160.0.0/20	local	active		
pl-68a54001 (com.amazonaws.us-west-2.s3, 54.231.160.0/19, 52.218.128.0/17, 52.92.32.0/22)	vpce-cb51a0a2	active		
0.0.0.0/0	igw-b2182dd7	active		
10.60.29.0/25	pcx-589c3331	active		
10.100.0.0/16	tgw-015b7c249661ac279	active		VPC2
10.129.0.0/20	pcx-ff7e1396	active		
172.23.0.1/32	eni-0854d4715559c3cdb	active		
172.23.0.2/32	eni-0854d4715559c3cdb	active		
172.23.0.3/32	eni-0f76681216c3108ed	active		
172.23.0.4/32	eni-0854d4715559c3cdb	active		Floating IP Addresses

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

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

## Volumes

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



### Related links

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

### Security group rules for AWS

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

#### Rules for Cloud Volumes ONTAP

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

#### Inbound rules

The source for inbound rules in the predefined security group is 0.0.0.0/0.

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

Protocol	Port	Purpose
TCP	161-162	Simple network management protocol
TCP	445	Microsoft SMB/CIFS over TCP with NetBIOS framing
TCP	635	NFS mount
TCP	749	Kerberos
TCP	2049	NFS server daemon
TCP	3260	iSCSI access through the iSCSI data LIF
TCP	4045	NFS lock daemon
TCP	4046	Network status monitor for NFS
TCP	10000	Backup using NDMP
TCP	11104	Management of intercluster communication sessions for SnapMirror
TCP	11105	SnapMirror data transfer using intercluster LIFs
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)
Backup to S3	TCP	5010	Intercluster LIF	Backup endpoint or restore endpoint	Back up and restore operations for the Backup to S3 feature

Service	Protocol	Port	Source	Destination	Purpose
Cluster	All traffic	All traffic	All LIFs on one node	All LIFs on the other node	Intercluster communications (Cloud Volumes ONTAP HA only)
	TCP	3000	Node management LIF	HA mediator	ZAPI calls (Cloud Volumes ONTAP HA only)
	ICMP	1	Node management LIF	HA mediator	Keep alive (Cloud Volumes ONTAP HA only)
DHCP	UDP	68	Node management LIF	DHCP	DHCP client for first-time setup
DHCPS	UDP	67	Node management LIF	DHCP	DHCP server
DNS	UDP	53	Node management LIF and data LIF (NFS, CIFS)	DNS	DNS
NDMP	TCP	1860 0–18 699	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
SnapMirr or	TCP	1110 4	Intercluster LIF	ONTAP intercluster LIFs	Management of intercluster communication sessions for SnapMirror
	TCP	1110 5	Intercluster LIF	ONTAP intercluster LIFs	SnapMirror data transfer
Syslog	UDP	514	Node management LIF	Syslog server	Syslog forward messages

#### Rules for the HA mediator external security group

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

#### Inbound rules

The source for inbound rules is 0.0.0.0/0.

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

## Outbound rules

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

### Basic outbound rules

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

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

### Advanced outbound rules

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

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



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

### Rules for the HA mediator internal security group

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

## Inbound rules

The predefined security group includes the following inbound rules.

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

## Outbound rules

The predefined security group includes the following outbound rules.

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

## Rules for the Connector

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

## Inbound rules

Protocol	Port	Purpose
SSH	22	Provides SSH access to the Connector host
HTTP	80	Provides HTTP access from client web browsers to the local user interface and connections from Cloud Compliance
HTTPS	443	Provides HTTPS access from client web browsers to the local user interface
TCP	3128	Provides the Cloud Compliance instance with internet access, if your AWS network doesn't use a NAT or proxy

## Outbound rules

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

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

## 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
Active Directory	TCP	88	Active Directory forest	Kerberos V authentication
	TCP	139	Active Directory forest	NetBIOS service session
	TCP	389	Active Directory forest	LDAP
	TCP	445	Active Directory forest	Microsoft SMB/CIFS over TCP with NetBIOS framing
	TCP	464	Active Directory forest	Kerberos V change & set password (SET_CHANGE)
	TCP	749	Active Directory forest	Active Directory Kerberos V change & set password (RPCSEC_GSS)
	UDP	137	Active Directory forest	NetBIOS name service
	UDP	138	Active Directory forest	NetBIOS datagram service
	UDP	464	Active Directory forest	Kerberos key administration
API calls and AutoSupport	HTTP	443	Outbound internet and ONTAP cluster management LIF	API calls to AWS and ONTAP, and sending AutoSupport messages to NetApp
API calls	TCP	3000	ONTAP cluster management LIF	API calls to ONTAP
	TCP	8088	Backup to S3	API calls to Backup to S3
DNS	UDP	53	DNS	Used for DNS resolve by Cloud Manager
Cloud Compliance	HTTP	80	Cloud Compliance instance	Cloud Compliance for Cloud Volumes ONTAP

## Setting up the AWS KMS

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

### Steps

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

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

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

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

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

[AWS Documentation: Editing Keys](#)

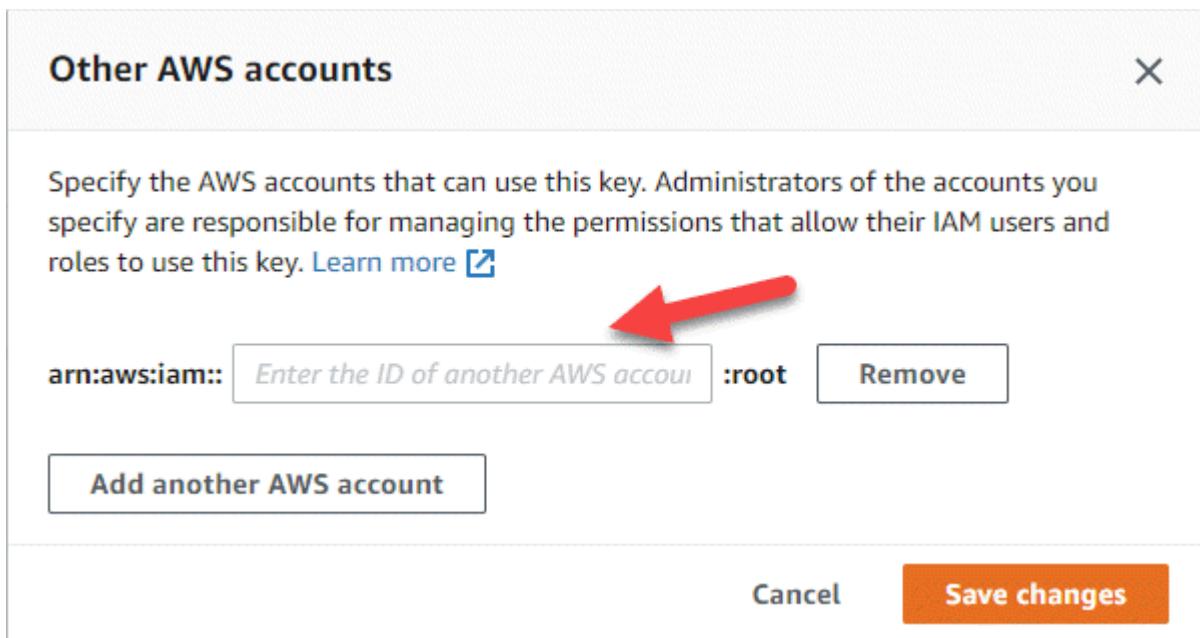
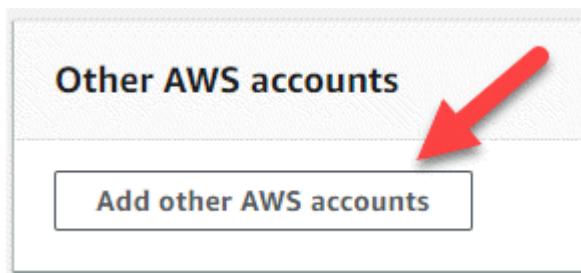
3. If the CMK is in a different AWS account, complete the following steps:

- Go to the KMS console from the account where the CMK resides.
- Select the key.
- In the **General configuration** pane, copy the ARN of the key.

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

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

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



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

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

```

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

```

For additional details about this process, see [AWS Documentation: Allowing External AWS Accounts to Access a CMK](#).

## Launching Cloud Volumes ONTAP in AWS

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

in AWS.

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

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

### Before you begin

- You should have a [Connector that is associated with your workspace](#).



You must be an Account Admin to create a Connector. When you create your first Cloud Volumes ONTAP working environment, Cloud Manager prompts you to create a Connector if you don't have one yet.

- [You should be prepared to leave the Connector running at all times](#).
- You should have prepared by choosing a configuration and by obtaining AWS networking information from your administrator. For details, see [Planning your Cloud Volumes ONTAP configuration](#).
- If you want to launch a BYOL system, you must have the 20-digit serial number (license key).
- If you want to use CIFS, you must have set up DNS and Active Directory. For details, see [Networking requirements for Cloud Volumes ONTAP in AWS](#).

### About this task

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

### Steps

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

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

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

Field	Description
Add tags	<p>AWS tags are metadata for your AWS resources. Cloud Manager adds the tags to the Cloud Volumes ONTAP instance and each AWS resource associated with the instance.</p> <p>You can add up to four tags from the user interface when creating a working environment, and then you can add more after its created. Note that the API does not limit you to four tags when creating a working environment.</p> <p>For information about tags, refer to <a href="#">AWS Documentation: Tagging your Amazon EC2 Resources</a>.</p>
User name and password	<p>These are the credentials for the Cloud Volumes ONTAP cluster admin account. You can use these credentials to connect to Cloud Volumes ONTAP through OnCommand System Manager or its CLI.</p>
Edit Credentials	<p>Choose the AWS credentials and marketplace subscription to use with this Cloud Volumes ONTAP system.</p> <p>Click <b>Add Subscription</b> to associate the selected credentials with a subscription.</p> <p>To create a pay-as-you-go Cloud Volumes ONTAP system, you need to select AWS credentials that are associated with a subscription to Cloud Volumes ONTAP from the AWS Marketplace. You'll be charged from this subscription for every Cloud Volumes ONTAP 9.6 and later PAYGO system that you create and each add-on feature that you enable.</p> <p><a href="#">Learn how to add additional AWS credentials to Cloud Manager.</a></p>

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

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

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



#### Cloud Manager (for Cloud Volumes ONTAP)

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



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

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

[Subscribe](#)

You are already subscribed to this product

#### Pricing Details

Software Fees

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

- Learn more about Cloud Compliance.
  - Learn more about Cloud Backup.
  - Learn more about Monitoring.
5. **Location & Connectivity:** Enter the network information that you recorded in the AWS worksheet.

If you have an AWS Outpost, you can deploy a single node Cloud Volumes ONTAP system in that Outpost by selecting the Outpost VPC. The experience is the same as any other VPC that resides in AWS.

The following image shows the page filled out:

Location	Connectivity
AWS Region US West   Oregon	Security Group <input checked="" type="radio"/> Generated security group <input type="radio"/> Use existing security group
VPC vpc-3a01e05f - 172.31.0.0/16	SSH Authentication Method <input checked="" type="radio"/> Password <input type="radio"/> Key Pair
Subnet 172.31.5.0/24 (OCCM subnet)	

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

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



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

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

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

7. **License and Support Site Account:** Specify whether you want to use pay-as-you-go or BYOL, and then specify a NetApp Support Site account.

To understand how licenses work, see [Licensing](#).

A NetApp Support Site Account is optional for pay-as-you-go, but required for BYOL systems. [Learn how to add NetApp Support Site accounts.](#)

8. **Preconfigured Packages:** Select one of the packages to quickly launch Cloud Volumes ONTAP, 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. **IAM Role:** You should keep the default option to let Cloud Manager create the role for you.

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

10. **Licensing:** Change the Cloud Volumes ONTAP version as needed, select a license, an instance type, and the instance tenancy.

If your needs change after you launch the instance, you can modify the license or instance type later.



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 9.6 RC1 and 9.6 GA is available. The update does not occur from one release to another—for example, from 9.6 to 9.7.

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

Note the following:

- The disk type is for the initial volume. You can choose a different disk type for subsequent volumes.
- The disk size is for all disks in the initial aggregate and for any additional aggregates that 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 AWS](#).

- You can choose a specific volume tiering policy when you create or edit a volume.
- If you disable data tiering, you can enable it on subsequent aggregates.

[Learn how data tiering works.](#)

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

[Learn more about write speed.](#)

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

[Learn more about WORM storage.](#)

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

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, <a href="#">use the IQN to connect to the LUN from your hosts</a>.</p>

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

### Volume Details, Protection & Protocol

<h4>Details &amp; Protection</h4> <div style="margin-top: 10px;"> <div style="display: flex; justify-content: space-between;"> <span>Volume Name:</span> <span>Size (GB):</span> </div> <div style="display: flex; align-items: center;"> <input style="width: 150px; height: 30px; margin-right: 10px; border: 1px solid #ccc; border-radius: 5px; padding: 2px;" type="text" value="vol"/> <span style="border: 1px solid #ccc; padding: 2px 10px; border-radius: 5px;">250</span> </div> </div> <div style="margin-top: 10px;"> <span>Snapshot Policy:</span> <div style="display: flex; align-items: center;"> <input style="width: 150px; height: 30px; margin-right: 10px; border: 1px solid #ccc; border-radius: 5px; padding: 2px;" type="text" value="default"/> <span style="border: 1px solid #ccc; padding: 2px 10px; border-radius: 5px;">▼</span> </div> </div> <div style="margin-top: 10px;"> <span>Default Policy</span> </div>	<h4>Protocol</h4> <div style="display: flex; justify-content: space-around; border-bottom: 1px solid #ccc; margin-bottom: 10px;"> <span>NFS</span> <span style="background-color: #0070C0; color: white; padding: 2px 10px; border-radius: 5px;">CIFS</span> <span>iSCSI</span> </div> <div style="display: flex; justify-content: space-between;"> <span>Share name:</span> <span style="border: 1px solid #ccc; padding: 2px 10px; border-radius: 5px;">vol_share</span> </div> <div style="display: flex; justify-content: space-between;"> <span>Permissions:</span> <span style="border: 1px solid #ccc; padding: 2px 10px; border-radius: 5px;">Full Control</span> </div> <div style="margin-top: 10px;"> <span>Users / Groups:</span> <div style="border: 1px solid #ccc; padding: 2px 10px; width: 150px; margin-top: 5px;">engineering</div> </div> <div style="font-size: small; margin-top: 5px;">     Valid users and groups separated by a semicolon   </div>
--	---

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

Field	Description
DNS Primary and Secondary IP Address	The IP addresses of the DNS servers that provide name resolution for the CIFS server. The listed DNS servers must contain the service location records (SRV) needed to locate the Active Directory LDAP servers and domain controllers for the domain that the CIFS server will join.
Active Directory Domain to join	The FQDN of the Active Directory (AD) domain that you want the CIFS server to join.
Credentials authorized to join the domain	The name and password of a Windows account with sufficient privileges to add computers to the specified Organizational Unit (OU) within the AD domain.
CIFS server NetBIOS name	A CIFS server name that is unique in the AD domain.
Organizational Unit	The organizational unit within the AD domain to associate with the CIFS server. The default is CN=Computers. If you configure AWS Managed Microsoft AD as the AD server for Cloud Volumes ONTAP, you should enter <b>OU=Computers,OU=corp</b> in this field.
DNS Domain	The DNS domain for the Cloud Volumes ONTAP storage virtual machine (SVM). In most cases, the domain is the same as the AD domain.
NTP Server	Select <b>Use Active Directory Domain</b> to configure an NTP server using the Active Directory DNS. If you need to configure an NTP server using a different address, then you should use the API. See the <a href="#">Cloud Manager API Developer Guide</a> for details.

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

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

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

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

## Result

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

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

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

## After you finish

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

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

## Launching a Cloud Volumes ONTAP HA pair in AWS

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

### Before you begin

- You should have a [Connector that is associated with your workspace](#).



You must be an Account Admin to create a Connector. When you create your first Cloud Volumes ONTAP working environment, Cloud Manager prompts you to create a Connector if you don't have one yet.

- [You should be prepared to leave the Connector running at all times](#).
- You should have prepared by choosing a configuration and by obtaining AWS networking information from your administrator. For details, see [Planning your Cloud Volumes ONTAP configuration](#).
- If you purchased BYOL licenses, you must have a 20-digit serial number (license key) for each node.
- If you want to use CIFS, you must have set up DNS and Active Directory. For details, see [Networking requirements for Cloud Volumes ONTAP in AWS](#).

### Limitation

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

### About this task

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

### Steps

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

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

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

Field	Description
Add tags	<p>AWS tags are metadata for your AWS resources. Cloud Manager adds the tags to the Cloud Volumes ONTAP instance and each AWS resource associated with the instance.</p> <p>You can add up to four tags from the user interface when creating a working environment, and then you can add more after its created. Note that the API does not limit you to four tags when creating a working environment.</p> <p>For information about tags, refer to <a href="#">AWS Documentation: Tagging your Amazon EC2 Resources</a>.</p>
User name and password	<p>These are the credentials for the Cloud Volumes ONTAP cluster admin account. You can use these credentials to connect to Cloud Volumes ONTAP through OnCommand System Manager or its CLI.</p>
Edit Credentials	<p>Choose the AWS credentials and marketplace subscription to use with this Cloud Volumes ONTAP system.</p> <p>Click <b>Add Subscription</b> to associate the selected credentials with a subscription.</p> <p>To create a pay-as-you-go Cloud Volumes ONTAP system, you need to select AWS credentials that are associated with a subscription to Cloud Volumes ONTAP from the AWS Marketplace. You'll be charged from this subscription for every Cloud Volumes ONTAP 9.6 and later PAYGO system that you create and each add-on feature that you enable.</p> <p><a href="#">Learn how to add additional AWS credentials to Cloud Manager</a>.</p>

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

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



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

4. **Services:** Keep the services enabled or disable the individual services that you don't want to use with this Cloud Volumes ONTAP system.
  - [Learn more about Cloud Compliance](#).
  - [Learn more about Cloud Backup](#).
  - [Learn more about Monitoring](#).
5. **HA Deployment Models:** Choose an HA configuration.

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

**6. Region & VPC:** Enter the network information that you recorded in the AWS worksheet.

The following image shows the page filled out for a multiple AZ configuration:

The screenshot shows the 'Region & VPC' configuration page. At the top, there are three dropdown menus: 'AWS Region' (set to 'US East | N. Virginia'), 'VPC' (set to 'vpc-a76d91c2 - 172.31.0.0/16'), and 'Security group' (set to 'Use a generated security group'). Below these, there are three separate sections for 'Node 1', 'Node 2', and 'Mediator'. Each section has a server icon and a title. Under each title, there are two dropdown menus: 'Availability Zone' and 'Subnet'. For Node 1, the Availability Zone is 'us-east-1a' and the Subnet is '172.31.8.0/24'. For Node 2, the Availability Zone is 'us-east-1b' and the Subnet is '172.31.9.0/24'. For the Mediator, the Availability Zone is 'us-east-1c' and the Subnet is '172.31.2.0/24'.

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

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

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

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

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

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

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



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

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

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

**11. License and Support Site Account:** Specify whether you want to use pay-as-you-go or BYOL, and then specify a NetApp Support Site account.

To understand how licenses work, see [Licensing](#).

A NetApp Support Site Account is optional for pay-as-you-go, but required for BYOL systems. Learn how to add [NetApp Support Site accounts](#).

12. **Preconfigured Packages:** Select one of the packages to quickly launch 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.

13. **IAM Role:** You should keep the default option to let Cloud Manager create the roles for you.

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

14. **Licensing:** Change the Cloud Volumes ONTAP version as needed, select a license, an instance type, and the instance tenancy.

If your needs change after you launch the instances, you can modify the license or instance type later.



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 9.6 RC1 and 9.6 GA is available. The update does not occur from one release to another—for example, from 9.6 to 9.7.

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

Note the following:

- The disk type is for the initial volume. You can choose a different disk type for subsequent volumes.
- The disk size is for all disks in the initial aggregate and for any additional aggregates that 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 AWS](#).

- You can choose a specific volume tiering policy when you create or edit a volume.
- If you disable data tiering, you can enable it on subsequent aggregates.

[Learn how data tiering works](#).

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

[Learn more about write speed](#).

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

[Learn more about WORM storage](#).

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

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.
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, <a href="#">use the IQN to connect to the LUN from your hosts</a>.</p>

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

**Volume Details, Protection & Protocol**

<b>Details &amp; Protection</b> <div style="margin-top: 10px;">         Volume Name: <input type="text" value="vol"/> Size (GB): <input type="text" value="250"/> </div> <div style="margin-top: 10px;">         Snapshot Policy: <input type="text" value="default"/> </div> <div style="margin-top: 10px;"> <small><a href="#">Default Policy</a></small> </div>	<b>Protocol</b> <div style="margin-top: 10px;"> <span style="margin-right: 10px;">NFS</span> <span style="background-color: #0070C0; color: white; padding: 2px 10px; border-radius: 5px;">CIFS</span> <span>iSCSI</span> </div> <div style="margin-top: 10px;">         Share name: <input type="text" value="vol_share"/> Permissions: <input type="text" value="Full Control"/> </div> <div style="margin-top: 10px;">         Users / Groups: <input type="text" value="engineering"/> </div> <div style="margin-top: 5px; font-size: small;">         Valid users and groups separated by a semicolon       </div>
--	---

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

Field	Description
DNS Primary and Secondary IP Address	The IP addresses of the DNS servers that provide name resolution for the CIFS server. The listed DNS servers must contain the service location records (SRV) needed to locate the Active Directory LDAP servers and domain controllers for the domain that the CIFS server will join.
Active Directory Domain to join	The FQDN of the Active Directory (AD) domain that you want the CIFS server to join.
Credentials authorized to join the domain	The name and password of a Windows account with sufficient privileges to add computers to the specified Organizational Unit (OU) within the AD domain.
CIFS server NetBIOS name	A CIFS server name that is unique in the AD domain.
Organizational Unit	The organizational unit within the AD domain to associate with the CIFS server. The default is CN=Computers. If you configure AWS Managed Microsoft AD as the AD server for Cloud Volumes ONTAP, you should enter <b>OU=Computers,OU=corp</b> in this field.
DNS Domain	The DNS domain for the Cloud Volumes ONTAP storage virtual machine (SVM). In most cases, the domain is the same as the AD domain.
NTP Server	Select <b>Use Active Directory Domain</b> to configure an NTP server using the Active Directory DNS. If you need to configure an NTP server using a different address, then you should use the API. See the <a href="#">Cloud Manager API Developer Guide</a> for details.

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

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

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

- Review details about the configuration.

- b. Click **More information** to review details about support and the AWS resources that Cloud Manager will purchase.
- c. Select the **I understand...** check boxes.
- d. Click **Go**.

## Result

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

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

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

## After you finish

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

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

# Get started in Azure

## Getting started with Cloud Volumes ONTAP for Azure

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



### Create a Connector

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

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.



### 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](#).



### Set up your networking

- a. Ensure that your VNet and subnets will support connectivity between the Connector and Cloud Volumes ONTAP.
- b. Enable outbound internet access from the target VNet 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.](#)



## 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

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

## Planning your Cloud Volumes ONTAP configuration in Azure

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

### Choosing a license type

Cloud Volumes ONTAP is available in two pricing options: pay-as-you-go and Bring Your Own License (BYOL). For pay-as-you-go, you can choose from three licenses: Explore, Standard, or Premium. Each license provides different capacity and compute options.

[Supported configurations for Cloud Volumes ONTAP 9.8 in Azure](#)

### Supported VM types

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

[Supported configurations for Cloud Volumes ONTAP 9.8 in Azure](#)

### Understanding 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 9.8 in Azure](#)

### Sizing your system in Azure

Sizing your Cloud Volumes ONTAP system can help you meet requirements for performance and capacity. You

should be aware of a few key points when choosing a VM type, disk type, and disk size:

## Virtual machine type

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

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

## Azure disk type

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

HA systems use Premium page blobs. Meanwhile, single node systems can use two types of Azure Managed Disks:

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

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

## Azure disk size

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



All disks in an aggregate must be the same size.

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

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

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

Refer to Azure for IOPS and throughput by disk size:

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

## Choosing a configuration that supports Flash Cache

A Cloud Volumes ONTAP configuration in Azure includes local NVMe storage, which Cloud Volumes ONTAP uses as *Flash Cache* for better performance. [Learn more about Flash Cache](#).

## Azure network information worksheet

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

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

## Choosing a write speed

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

## Choosing 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 Azure

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

## Requirements for Cloud Volumes ONTAP

The following networking requirements must be met in Azure.

### Outbound internet access for Cloud Volumes ONTAP

Cloud Volumes ONTAP requires outbound internet access to send messages to NetApp AutoSupport, which proactively monitors the health of your storage.

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>

[Learn how to configure AutoSupport.](#)

### Security groups

You do not need to create security groups because Cloud Manager does that for you. If you need to use your own, refer to the security group rules listed below.

### Number of IP addresses

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

- Single node: 5 IP addresses
- HA pair: 16 IP addresses

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



A LIF is an IP address associated with a physical port. An SVM management LIF is required for management tools like SnapCenter.

### Connection from Cloud Volumes ONTAP to Azure Blob storage for data tiering

If you want to tier cold data to Azure Blob storage, you don't need to set up a connection between the performance tier and the capacity tier as long as Cloud Manager has the required permissions. Cloud Manager enables a VNet service endpoint for you if the Cloud Manager policy has these permissions:

```
"Microsoft.Network/virtualNetworks/subnets/write",  
"Microsoft.Network/routeTables/join/action",
```

These permissions are included in the latest [Cloud Manager policy](#).

For details about setting up data tiering, 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 Azure and ONTAP systems in other networks, you must have a VPN connection between the Azure VNet and the other network—for example, an AWS VPC or your corporate network.

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

portal.

## 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](#).

### Connections to target networks

A Connector requires a network connection to the VPCs and VNets in which you want to deploy Cloud Volumes ONTAP.

For example, if you install a Connector in your corporate network, then you must set up a VPN connection to the VPC or VNet in which you launch Cloud Volumes ONTAP.

### Outbound internet access

The Connector requires outbound internet access to manage resources and processes within your public cloud environment. A Connector contacts the following endpoints when managing resources in Azure:

Endpoints	Purpose
<a href="https://management.azure.com">https://management.azure.com</a> <a href="https://login.microsoftonline.com">https://login.microsoftonline.com</a>	Enables Cloud Manager to deploy and manage Cloud Volumes ONTAP in most Azure regions.
<a href="https://management.microsoftazure.de">https://management.microsoftazure.de</a> <a href="https://login.microsoftonline.de">https://login.microsoftonline.de</a>	Enables Cloud Manager to deploy and manage Cloud Volumes ONTAP in the Azure Germany regions.
<a href="https://management.usgovcloudapi.net">https://management.usgovcloudapi.net</a> <a href="https://login.microsoftonline.com">https://login.microsoftonline.com</a>	Enables Cloud Manager to deploy and manage Cloud Volumes ONTAP in the Azure US Gov regions.
<a href="https://api.services.cloud.netapp.com:443">https://api.services.cloud.netapp.com:443</a>	API requests to NetApp Cloud Central.
<a href="https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com">https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com</a>	Provides access to software images, manifests, and templates.
<a href="https://cognito-idp.us-east-1.amazonaws.com">https://cognito-idp.us-east-1.amazonaws.com</a> <a href="https://cognito-identity.us-east-1.amazonaws.com">https://cognito-identity.us-east-1.amazonaws.com</a> <a href="https://sts.amazonaws.com">https://sts.amazonaws.com</a> <a href="https://cloud-support-netapp-com-accelerated.s3.amazonaws.com">https://cloud-support-netapp-com-accelerated.s3.amazonaws.com</a>	Enables the Connector to access and download manifests, templates, and Cloud Volumes ONTAP upgrade images.
<a href="https://cloudmanagerinfraprod.azurecr.io">https://cloudmanagerinfraprod.azurecr.io</a>	Access to software images of container components for an infrastructure that's running Docker and provides a solution for service integrations with Cloud Manager.
<a href="https://kinesis.us-east-1.amazonaws.com">https://kinesis.us-east-1.amazonaws.com</a>	Enables NetApp to stream data from audit records.
<a href="https://cloudmanager.cloud.netapp.com">https://cloudmanager.cloud.netapp.com</a>	Communication with the Cloud Manager service, which includes Cloud Central accounts.

Endpoints	Purpose
<a href="https://netapp-cloud-account.auth0.com">https://netapp-cloud-account.auth0.com</a>	Communication with NetApp Cloud Central for centralized user authentication.
<a href="https://support.netapp.com:443">support.netapp.com:443</a>	Communication with NetApp AutoSupport.
<a href="https://support.netapp.com/svcgw">https://support.netapp.com/svcgw</a> <a href="https://support.netapp.com/ServiceGW/entitlement">https://support.netapp.com/ServiceGW/entitlement</a> <a href="https://eval.lic.netapp.com.s3.us-west-1.amazonaws.com">https://eval.lic.netapp.com.s3.us-west-1.amazonaws.com</a> <a href="https://cloud-support-netapp-com.s3.us-west-1.amazonaws.com">https://cloud-support-netapp-com.s3.us-west-1.amazonaws.com</a>	Communication with NetApp for system licensing and support registration.
<a href="https://client.infra.support.netapp.com.s3.us-west-1.amazonaws.com">https://client.infra.support.netapp.com.s3.us-west-1.amazonaws.com</a> <a href="https://cloud-support-netapp-com-accelerated.s3.us-west-1.amazonaws.com">https://cloud-support-netapp-com-accelerated.s3.us-west-1.amazonaws.com</a> <a href="https://trigger.asup.netapp.com.s3.us-west-1.amazonaws.com">https://trigger.asup.netapp.com.s3.us-west-1.amazonaws.com</a>	Enables NetApp to collect information needed to troubleshoot support issues.
<a href="https://ipa-signer.cloudmanager.netapp.com">https://ipa-signer.cloudmanager.netapp.com</a>	Enables Cloud Manager to generate licenses (for example, a FlexCache license for Cloud Volumes ONTAP)
<a href="*.blob.core.windows.net">*.blob.core.windows.net</a>	Required for HA pairs when using a proxy.
Various third-party locations, for example: <ul style="list-style-type: none"> <li>• <a href="https://repo1.maven.org/maven2">https://repo1.maven.org/maven2</a></li> <li>• <a href="https://oss.sonatype.org/content/repositories">https://oss.sonatype.org/content/repositories</a></li> <li>• <a href="https://repo.typesafe.com">https://repo.typesafe.com</a></li> </ul>	During upgrades, Cloud Manager downloads the latest packages for third-party dependencies.
Third-party locations are subject to change.	

While you should perform almost all tasks from the SaaS user interface, a local user interface is still available on the Connector. The machine running the web browser must have connections to the following endpoints:

Endpoints	Purpose
The Connector host	<p>You must enter the host's IP address from a web browser to load the Cloud Manager console.</p> <p>Depending on your connectivity to your cloud provider, you can use the private IP or a public IP assigned to the host:</p> <ul style="list-style-type: none"> <li>• A private IP works if you have a VPN and direct connect access to your virtual network</li> <li>• A public IP works in any networking scenario</li> </ul> <p>In any case, you should secure network access by ensuring that security group rules allow access from only authorized IPs or subnets.</p>
<a href="https://auth0.com">https://auth0.com</a> <a href="https://cdn.auth0.com">https://cdn.auth0.com</a> <a href="https://netapp-cloud-account.auth0.com">https://netapp-cloud-account.auth0.com</a> <a href="https://services.cloud.netapp.com">https://services.cloud.netapp.com</a>	Your web browser connects to these endpoints for centralized user authentication through NetApp Cloud Central.
<a href="https://widget.intercom.io">https://widget.intercom.io</a>	For in-product chat that enables you to talk to NetApp cloud experts.

## Security group rules for Cloud Volumes ONTAP

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

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

### Inbound rules for single node systems

The rules listed below allow traffic, unless the description notes that it blocks specific inbound traffic.

Priority and name	Port and protocol	Source and destination	Description
1000 inbound_ssh	22 TCP	Any to Any	SSH access to the IP address of the cluster management LIF or a node management LIF
1001 inbound_http	80 TCP	Any to Any	HTTP access to the System Manager web console using the IP address of the cluster management LIF
1002 inbound_111_tcp	111 TCP	Any to Any	Remote procedure call for NFS
1003 inbound_111_udp	111 UDP	Any to Any	Remote procedure call for NFS
1004 inbound_139	139 TCP	Any to Any	NetBIOS service session for CIFS

<b>Priority and name</b>	<b>Port and protocol</b>	<b>Source and destination</b>	<b>Description</b>
1005 inbound_161-162_tcp	161-162 TCP	Any to Any	Simple network management protocol
1006 inbound_161-162_udp	161-162 UDP	Any to Any	Simple network management protocol
1007 inbound_443	443 TCP	Any to Any	HTTPS access to the System Manager web console using the IP address of the cluster management LIF
1008 inbound_445	445 TCP	Any to Any	Microsoft SMB/CIFS over TCP with NetBIOS framing
1009 inbound_635_tcp	635 TCP	Any to Any	NFS mount
1010 inbound_635_udp	635 UDP	Any to Any	NFS mount
1011 inbound_749	749 TCP	Any to Any	Kerberos
1012 inbound_2049_tcp	2049 TCP	Any to Any	NFS server daemon
1013 inbound_2049_udp	2049 UDP	Any to Any	NFS server daemon
1014 inbound_3260	3260 TCP	Any to Any	iSCSI access through the iSCSI data LIF
1015 inbound_4045-4046_tcp	4045-4046 TCP	Any to Any	NFS lock daemon and network status monitor
1016 inbound_4045-4046_udp	4045-4046 UDP	Any to Any	NFS lock daemon and network status monitor
1017 inbound_10000	10000 TCP	Any to Any	Backup using NDMP
1018 inbound_11104-11105	11104-11105 TCP	Any to Any	SnapMirror data transfer
3000 inbound_deny_all_tcp	Any port TCP	Any to Any	Block all other TCP inbound traffic
3001 inbound_deny_all_udp	Any port UDP	Any to Any	Block all other UDP inbound traffic

<b>Priority and name</b>	<b>Port and protocol</b>	<b>Source and destination</b>	<b>Description</b>
65000 AllowVnetInBound	Any port Any protocol	VirtualNetwork to VirtualNetwork	Inbound traffic from within the VNet
65001 AllowAzureLoadBalancerInBound	Any port Any protocol	AzureLoadBalancer to Any	Data traffic from the Azure Standard Load Balancer
65500 DenyAllInBound	Any port Any protocol	Any to Any	Block all other inbound traffic

#### Inbound rules for HA systems

The rules listed below allow traffic, unless the description notes that it blocks specific inbound traffic.



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

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

Priority and name	Port and protocol	Source and destination	Description
65500 DenyAllInBound	Any port Any protocol	Any to Any	Block all other inbound traffic

## Outbound rules

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

### Basic outbound rules

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

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

### Advanced outbound rules

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



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

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

Service	Port	Protocol	Source	Destination	Purpose
DHCPS	67	UDP	Node management LIF	DHCP	DHCP server
DNS	53	UDP	Node management LIF and data LIF (NFS, CIFS)	DNS	DNS
NDMP	18600–18699	TCP	Node management LIF	Destination servers	NDMP copy
SMTP	25	TCP	Node management LIF	Mail server	SMTP alerts, can be used for AutoSupport
SNMP	161	TCP	Node management LIF	Monitor server	Monitoring by SNMP traps
	161	UDP	Node management LIF	Monitor server	Monitoring by SNMP traps
	162	TCP	Node management LIF	Monitor server	Monitoring by SNMP traps
	162	UDP	Node management LIF	Monitor server	Monitoring by SNMP traps
SnapMirror	11104	TCP	Intercluster LIF	ONTAP intercluster LIFs	Management of intercluster communication sessions for SnapMirror
	11105	TCP	Intercluster LIF	ONTAP intercluster LIFs	SnapMirror data transfer
Syslog	514	UDP	Node management LIF	Syslog server	Syslog forward messages

## Security group rules for the Connector

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

### Inbound rules

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

### Outbound rules

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

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

## Advanced outbound rules

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



The source IP address is the Connector host.

Service	Port	Protocol	Destination	Purpose
Active Directory	88	TCP	Active Directory forest	Kerberos V authentication
	139	TCP	Active Directory forest	NetBIOS service session
	389	TCP	Active Directory forest	LDAP
	445	TCP	Active Directory forest	Microsoft SMB/CIFS over TCP with NetBIOS framing
	464	TCP	Active Directory forest	Kerberos V change & set password (SET_CHANGE)
	749	TCP	Active Directory forest	Active Directory Kerberos V change & set password (RPCSEC_GSS)
	137	UDP	Active Directory forest	NetBIOS name service
	138	UDP	Active Directory forest	NetBIOS datagram service
	464	UDP	Active Directory forest	Kerberos key administration
API calls and AutoSupport	443	HTTP	Outbound internet and ONTAP cluster management LIF	API calls to AWS and ONTAP, and sending AutoSupport messages to NetApp
API calls	3000	TCP	ONTAP cluster management LIF	API calls to ONTAP
DNS	53	UDP	DNS	Used for DNS resolve by Cloud Manager

## Launching Cloud Volumes ONTAP in Azure

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

### Before you begin

- You should have a [Connector that is associated with your workspace](#).



You must be an Account Admin to create a Connector. When you create your first Cloud Volumes ONTAP working environment, Cloud Manager prompts you to create a Connector if you don't have one yet.

- You should be prepared to leave the Connector running at all times.
- You should have chosen a configuration and obtained Azure networking information from your administrator. For details, see [Planning your Cloud Volumes ONTAP configuration](#).
- To deploy a BYOL system, you need the 20-digit serial number (license key) for each node.

## About this task

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

### Potential for Data Loss

Deploying Cloud Volumes ONTAP in an existing, shared resource group is not recommended due to the risk of data loss. While rollback is currently disabled by default when using the API to deploy into an existing resource group, deleting Cloud Volumes ONTAP will potentially delete other resources from that shared group.



The best practice is to use a new, dedicated resource group for Cloud Volumes ONTAP. This is the default and only recommended option when deploying Cloud Volumes ONTAP in Azure from Cloud Manager.

## Steps

1. On the Canvas page, click **Add Working Environment** and follow the prompts.
2. **Choose a Location:** Select **Microsoft Azure** and **Cloud Volumes ONTAP Single Node** or **Cloud Volumes ONTAP High Availability**.
3. **Details and Credentials:** Optionally change the Azure credentials and subscription, specify a cluster name and resource group name, add tags if needed, and then specify credentials.

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

Field	Description
Working Environment Name	Cloud Manager uses the working environment name to name both the Cloud Volumes ONTAP system and the Azure virtual machine. It also uses the name as the prefix for the predefined security group, if you select that option.
Resource Group Name	Keep the default name for the new resource group or uncheck <b>Use Default</b> and enter your own name for the new resource group.  The best practice is to use a new, dedicated resource group for Cloud Volumes ONTAP. While it is possible to deploy Cloud Volumes ONTAP in an existing, shared resource group by using the API, it's not recommended due to the risk of data loss. See the warning above for more details.

Field	Description
Tags	<p>Tags are metadata for your Azure resources. When you enter tags in this field, Cloud Manager adds them to the resource group associated with the Cloud Volumes ONTAP system.</p> <p>You can add up to four tags from the user interface when creating a working environment, and then you can add more after its created. Note that the API does not limit you to four tags when creating a working environment.</p> <p>For information about tags, refer to <a href="#">Microsoft Azure Documentation: Using tags to organize your Azure resources</a>.</p>
User name and password	<p>These are the credentials for the Cloud Volumes ONTAP cluster admin account. You can use these credentials to connect to Cloud Volumes ONTAP through OnCommand System Manager or its CLI.</p>
Edit Credentials	<p>You can choose different Azure credentials and a different Azure subscription to use with this Cloud Volumes ONTAP system. You need to associate an Azure Marketplace subscription with the selected Azure subscription in order to deploy a pay-as-you-go Cloud Volumes ONTAP system. <a href="#">Learn how to add credentials</a>.</p>

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

▶ [https://docs.netapp.com/us-en/occm/media/video\\_subscribing\\_azure.mp4 \(video\)](https://docs.netapp.com/us-en/occm/media/video_subscribing_azure.mp4)

4. **Services:** Keep the services enabled or disable the individual services that you don't want to use with Cloud Volumes ONTAP.
  - [Learn more about Cloud Compliance](#).
  - [Learn more about Cloud Backup](#).
  - [Learn more about the Monitoring service](#).

5. **Location & Connectivity:** Select a location and security group, and select the checkbox to confirm network connectivity between the Connector and the target location.

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

6. **License and Support Site Account:** Specify whether you want to use pay-as-you-go or BYOL, and then specify a NetApp Support Site account.

To understand how licenses work, see [Licensing](#).

A NetApp Support Site Account is optional for pay-as-you-go, but required for BYOL systems. [Learn how to add NetApp Support Site accounts](#).

7. **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.

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

If your needs change after you launch the system, you can modify the license or virtual machine type later.



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 9.6 RC1 and 9.6 GA is available. The update does not occur from one release to another—for example, from 9.6 to 9.7.

9. **Subscribe from the Azure Marketplace:** Follow the steps if Cloud Manager could not enable programmatic deployments of Cloud Volumes ONTAP.
10. **Underlying Storage Resources:** Choose settings for the initial aggregate: a disk type, a size for each disk, and whether data tiering to Blob storage should be enabled.

Note the following:

- The disk type is for the initial volume. You can choose a different disk type for subsequent volumes.
- The disk size is for all disks in the initial aggregate and for any additional aggregates that 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 Azure](#).

- You can choose a specific volume tiering policy when you create or edit a volume.
- If you disable data tiering, you can enable it on subsequent aggregates.

[Learn more about data tiering](#).

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

[Learn more about write speed](#).

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

[Learn more about WORM storage](#).

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

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

[Learn more about WORM storage](#).

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

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.
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, <a href="#">use the IQN to connect to the LUN from your hosts</a>.</p>

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

**Volume Details, Protection & Protocol**

<b>Details &amp; Protection</b> <div style="margin-top: 10px;">         Volume Name: <input type="text" value="vol"/> Size (GB): <input type="text" value="250"/> </div> <div style="margin-top: 10px;">         Snapshot Policy: <input type="text" value="default"/> <div style="float: right;"><small><a href="#">Default Policy</a></small></div> </div>	<b>Protocol</b> <div style="margin-top: 10px;"> <span style="margin-right: 10px;">NFS</span> <span style="background-color: #0072bc; color: white; padding: 2px 10px; border-radius: 10px;">CIFS</span> <span>iSCSI</span> </div> <div style="margin-top: 10px;">         Share name: <input type="text" value="vol_share"/> Permissions: <input type="text" value="Full Control"/> </div> <div style="margin-top: 10px;">         Users / Groups: <input type="text" value="engineering"/> <div style="font-size: small; margin-top: -10px;">Valid users and groups separated by a semicolon</div> </div>
--	--

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

Field	Description
DNS Primary and Secondary IP Address	The IP addresses of the DNS servers that provide name resolution for the CIFS server. The listed DNS servers must contain the service location records (SRV) needed to locate the Active Directory LDAP servers and domain controllers for the domain that the CIFS server will join.
Active Directory Domain to join	The FQDN of the Active Directory (AD) domain that you want the CIFS server to join.
Credentials authorized to join the domain	The name and password of a Windows account with sufficient privileges to add computers to the specified Organizational Unit (OU) within the AD domain.
CIFS server NetBIOS name	A CIFS server name that is unique in the AD domain.
Organizational Unit	The organizational unit within the AD domain to associate with the CIFS server. The default is CN=Computers.  To configure Azure AD Domain Services as the AD server for Cloud Volumes ONTAP, you should enter <b>OU=AADDC Computers</b> or <b>OU=AADDC Users</b> in this field. <a href="#">Azure Documentation: Create an Organizational Unit (OU) in an Azure AD Domain Services managed domain</a>
DNS Domain	The DNS domain for the Cloud Volumes ONTAP storage virtual machine (SVM). In most cases, the domain is the same as the AD domain.
NTP Server	Select <b>Use Active Directory Domain</b> to configure an NTP server using the Active Directory DNS. If you need to configure an NTP server using a different address, then you should use the API. See the <a href="#">Cloud Manager API Developer Guide</a> for details.

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 Azure 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.

# Get started in GCP

## Getting started with Cloud Volumes ONTAP for 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

- [Evaluating](#)
- [Creating a Connector from Cloud Manager](#)

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

## Planning 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.

### Choosing a license type

Cloud Volumes ONTAP is available in two pricing options: pay-as-you-go and Bring Your Own License (BYOL). For pay-as-you-go, you can choose from three licenses: Explore, Standard, or Premium. Each license provides different capacity and compute options.

[Supported configurations for Cloud Volumes ONTAP 9.8 in GCP](#)

### Supported machine types

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

[Supported configurations for Cloud Volumes ONTAP 9.8 in GCP](#)

### Understanding 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 9.8 in GCP](#)

### Sizing 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 either *Zonal SSD persistent disks* or *Zonal standard persistent disks*.

SSD persistent disks are best for workloads that require high rates of random IOPS, while 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](#)

## GCP network information worksheet

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	

GCP information	Your value
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)	

## Choosing 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](#).

## Choosing 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.

### Virtual Private Cloud for single node systems

One VPC is required for a single node system.

Cloud Volumes ONTAP and the Connector are supported in a Google Cloud shared VPC and also in 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](#).

The only requirement when using a shared VPC is to provide the [Compute Network User role](#) to the Connector service account. Cloud Manager needs these permissions to query the firewalls, VPC, and subnets in the host project.

### Virtual Private Clouds for HA pairs

Four Virtual Private Clouds (VPCs) are required for the 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

Similar to a single node system, an HA pair is supported in a shared VPC and also in standalone VPCs. However, only VPC-0 can be a shared VPC. All other VPCs must be a standalone VPC.

The only requirement when using a shared VPC is to provide the [Compute Network User role](#) to the Connector service account. Cloud Manager needs these permissions to query the firewalls, VPC, and subnets in the host project.

## Outbound internet access for Cloud Volumes ONTAP

Cloud Volumes ONTAP requires outbound internet access to send messages to NetApp AutoSupport, which proactively monitors the health of your storage.

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>

[Learn how to configure AutoSupport](#).



If you're using an HA pair, the HA mediator doesn't require outbound internet access.

## Number of IP addresses

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

- **Single node:** 5 IP addresses

Cloud Manager doesn't create an SVM management LIF for single node systems in GCP.

A LIF is an IP address associated with a physical port. An SVM management LIF is required for management tools like SnapCenter.

- **HA pair:** 17 IP addresses

- 10 IP addresses for VPC-0
- Two IP addresses for VPC-1
- Two IP addresses for VPC-2
- Three 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 all four VPCs.

## Outbound internet access

The Connector requires outbound internet access to manage resources and processes within your public cloud environment. A Connector contacts the following endpoints when managing resources in GCP:

Endpoints	Purpose
<a href="https://www.googleapis.com">https://www.googleapis.com</a>	Enables the Connector to contact Google APIs for deploying and managing Cloud Volumes ONTAP in GCP.
<a href="https://api.services.cloud.netapp.com:443">https://api.services.cloud.netapp.com:443</a>	API requests to NetApp Cloud Central.
<a href="https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com">https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com</a>	Provides access to software images, manifests, and templates.
<a href="https://cognito-idp.us-east-1.amazonaws.com">https://cognito-idp.us-east-1.amazonaws.com</a> <a href="https://cognito-identity.us-east-1.amazonaws.com">https://cognito-identity.us-east-1.amazonaws.com</a> <a href="https://sts.amazonaws.com">https://sts.amazonaws.com</a> <a href="https://cloud-support-netapp-com-accelerated.s3.amazonaws.com">https://cloud-support-netapp-com-accelerated.s3.amazonaws.com</a>	Enables the Connector to access and download manifests, templates, and Cloud Volumes ONTAP upgrade images.
<a href="https://cloudmanagerinfraprod.azurecr.io">https://cloudmanagerinfraprod.azurecr.io</a>	Access to software images of container components for an infrastructure that's running Docker and provides a solution for service integrations with Cloud Manager.
<a href="https://kinesis.us-east-1.amazonaws.com">https://kinesis.us-east-1.amazonaws.com</a>	Enables NetApp to stream data from audit records.
<a href="https://cloudmanager.cloud.netapp.com">https://cloudmanager.cloud.netapp.com</a>	Communication with the Cloud Manager service, which includes Cloud Central accounts.
<a href="https://netapp-cloud-account.auth0.com">https://netapp-cloud-account.auth0.com</a>	Communication with NetApp Cloud Central for centralized user authentication.
<a href="https://support.netapp.com:443">support.netapp.com:443</a>	Communication with NetApp AutoSupport.
<a href="https://support.netapp.com/svcgw">https://support.netapp.com/svcgw</a> <a href="https://support.netapp.com/ServiceGW/entitlement">https://support.netapp.com/ServiceGW/entitlement</a> <a href="https://eval.lic.netapp.com.s3.us-west-1.amazonaws.com">https://eval.lic.netapp.com.s3.us-west-1.amazonaws.com</a> <a href="https://cloud-support-netapp-com.s3.us-west-1.amazonaws.com">https://cloud-support-netapp-com.s3.us-west-1.amazonaws.com</a>	Communication with NetApp for system licensing and support registration.
<a href="https://client.infra.support.netapp.com.s3.us-west-1.amazonaws.com">https://client.infra.support.netapp.com.s3.us-west-1.amazonaws.com</a> <a href="https://cloud-support-netapp-com-accelerated.s3.us-west-1.amazonaws.com">https://cloud-support-netapp-com-accelerated.s3.us-west-1.amazonaws.com</a> <a href="https://trigger.asup.netapp.com.s3.us-west-1.amazonaws.com">https://trigger.asup.netapp.com.s3.us-west-1.amazonaws.com</a>	Enables NetApp to collect information needed to troubleshoot support issues.
<a href="https://ipa-signer.cloudmanager.netapp.com">https://ipa-signer.cloudmanager.netapp.com</a>	Enables Cloud Manager to generate licenses (for example, a FlexCache license for Cloud Volumes ONTAP)

Endpoints	Purpose
<p>Various third-party locations, for example:</p> <ul style="list-style-type: none"> <li>• <a href="https://repo1.maven.org/maven2">https://repo1.maven.org/maven2</a></li> <li>• <a href="https://oss.sonatype.org/content/repositories">https://oss.sonatype.org/content/repositories</a></li> <li>• <a href="https://repo.typesafe.com">https://repo.typesafe.com</a></li> </ul> <p>Third-party locations are subject to change.</p>	<p>During upgrades, Cloud Manager downloads the latest packages for third-party dependencies.</p>

While you should perform almost all tasks from the SaaS user interface, a local user interface is still available on the Connector. The machine running the web browser must have connections to the following endpoints:

Endpoints	Purpose
The Connector host	<p>You must enter the host's IP address from a web browser to load the Cloud Manager console.</p> <p>Depending on your connectivity to your cloud provider, you can use the private IP or a public IP assigned to the host:</p> <ul style="list-style-type: none"> <li>• A private IP works if you have a VPN and direct connect access to your virtual network</li> <li>• A public IP works in any networking scenario</li> </ul> <p>In any case, you should secure network access by ensuring that security group rules allow access from only authorized IPs or subnets.</p>
<a href="https://auth0.com">https://auth0.com</a> <a href="https://cdn.auth0.com">https://cdn.auth0.com</a> <a href="https://netapp-cloud-account.auth0.com">https://netapp-cloud-account.auth0.com</a> <a href="https://services.cloud.netapp.com">https://services.cloud.netapp.com</a>	<p>Your web browser connects to these endpoints for centralized user authentication through NetApp Cloud Central.</p>
<a href="https://widget.intercom.io">https://widget.intercom.io</a>	<p>For in-product chat that enables you to talk to NetApp cloud experts.</p>

## 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

The source for inbound rules in the predefined security group is 0.0.0.0/0.

Protocol	Port	Purpose
All ICMP	All	Pinging the instance
HTTP	80	HTTP access to the System Manager web console using the IP address of the cluster management LIF
HTTPS	443	HTTPS access to the System Manager web console using the IP address of the cluster management LIF
SSH	22	SSH access to the IP address of the cluster management LIF or a node management LIF
TCP	111	Remote procedure call for NFS
TCP	139	NetBIOS service session for CIFS
TCP	161-162	Simple network management protocol
TCP	445	Microsoft SMB/CIFS over TCP with NetBIOS framing
TCP	635	NFS mount
TCP	749	Kerberos
TCP	2049	NFS server daemon
TCP	3260	iSCSI access through the iSCSI data LIF
TCP	4045	NFS lock daemon
TCP	4046	Network status monitor for NFS
TCP	10000	Backup using NDMP
TCP	11104	Management of intercluster communication sessions for SnapMirror
TCP	11105	SnapMirror data transfer using intercluster LIFs
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
Cluster	All traffic	All traffic	All LIFs on one node	All LIFs on the other node	Intercluster communications (Cloud Volumes ONTAP HA only)
	TCP	3000	Node management LIF	HA mediator	ZAPI calls (Cloud Volumes ONTAP HA only)
	ICMP	1	Node management LIF	HA mediator	Keep alive (Cloud Volumes ONTAP HA only)
DHCP	UDP	68	Node management LIF	DHCP	DHCP client for first-time setup
DHCPS	UDP	67	Node management LIF	DHCP	DHCP server
DNS	UDP	53	Node management LIF and data LIF (NFS, CIFS)	DNS	DNS
NDMP	TCP	1860 0–18 699	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
SnapMirr or	TCP	1110 4	Intercluster LIF	ONTAP intercluster LIFs	Management of intercluster communication sessions for SnapMirror
	TCP	1110 5	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 policy 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 the HA nodes and the HA mediator.

## 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

### 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
Active Directory	TCP	88	Active Directory forest	Kerberos V authentication
	TCP	139	Active Directory forest	NetBIOS service session
	TCP	389	Active Directory forest	LDAP
	TCP	445	Active Directory forest	Microsoft SMB/CIFS over TCP with NetBIOS framing
	TCP	464	Active Directory forest	Kerberos V change & set password (SET_CHANGE)
	TCP	749	Active Directory forest	Active Directory Kerberos V change & set password (RPCSEC_GSS)
	UDP	137	Active Directory forest	NetBIOS name service
	UDP	138	Active Directory forest	NetBIOS datagram service
	UDP	464	Active Directory forest	Kerberos key administration
API calls and AutoSupport	HTTP	443	Outbound internet and ONTAP cluster management LIF	API calls to GCP and ONTAP, and sending AutoSupport messages to NetApp
API calls	TCP	3000	ONTAP cluster management LIF	API calls to ONTAP
DNS	UDP	53	DNS	Used for DNS resolve by Cloud Manager

## 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.

## Create service account

### Service account details

### **2** Grant this service account access to project (optional)

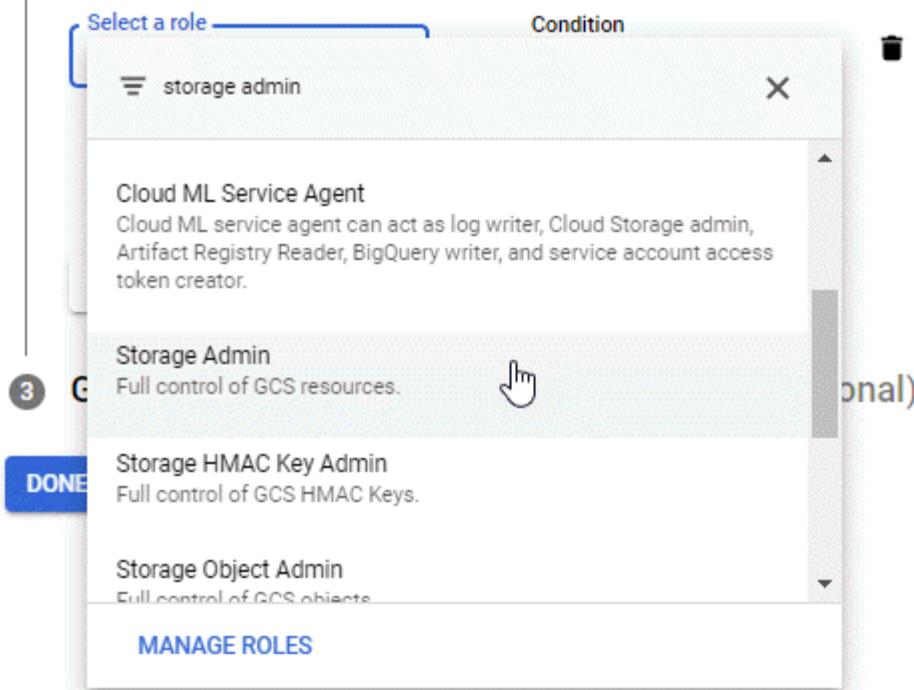
Grant this service account access to OCCM-Dev so that it has permission to complete specific actions on the resources in your project. [Learn more](#)

Select a role  Condition

Role	Description	Condition
storage admin	Cloud ML Service Agent Cloud ML service agent can act as log writer, Cloud Storage admin, Artifact Registry Reader, BigQuery writer, and service account access token creator.	
Storage Admin	Storage Admin Full control of GCS resources.	
Storage HMAC Key Admin	Storage HMAC Key Admin Full control of GCS HMAC Keys.	
Storage Object Admin	Storage Object Admin Full control of GCS objects.	

**DONE**

[MANAGE ROLES](#)



- c. **Grant users access to this service account:** Add the Connector service account as a *Service Account User* to this new service account.

This step is required for data tiering only. It's not required for the Cloud Backup Service.

## Create service account

### Service account details

### Grant this service account access to project (optional)

### **3** Grant users access to this service account (optional)

Grant access to users or groups that need to perform actions as this service account. [Learn more](#)

Service account users role

netapp-cloud-manager@iam.gserviceaccount.com 



Grant users the permissions to deploy jobs and VMs with this service account

Service account admins role



Grant users the permission to administer this service account

**DONE**

CANCEL

## What's next?

You'll need to select the service account later when you create a Cloud Volumes ONTAP working environment.

## Details and Credentials

default-project	gcp-sub2	<a href="#">Edit Project</a>
Google Cloud Project	Marketplace Subscription	
<b>Details</b>	<b>Credentials</b>	
Working Environment Name (Cluster Name)	User Name	
<input type="text" value="cloudvolumesontap"/>	<input type="text" value="admin"/>	
<b>Service Account</b> ⓘ	<b>Password</b>	
<input checked="" type="checkbox"/>	<input type="text"/>	
Service Account Name	Confirm Password	
<input type="text" value="account1"/>	<input type="text"/>	
 <a href="#">+ Add Labels</a> <small>Optional Field   Up to four labels</small>		

## 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 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.

### Steps

1. Give the Connector service account permission to use the encryption key.

The screenshot shows the Google Cloud Platform IAM & Admin interface. At the top, there are navigation icons and a user profile. Below that is a header with 'HIDE INFO PANEL' and a back arrow. The main title is 'key1'. Under the 'PERMISSIONS' tab, there is a note: 'Edit or delete permissions below or "Add Member" to grant new'. A button '+ ADD MEMBER' with a person icon is present. There is also a toggle switch for 'Show inherited permissions'. Below this, there are filters for 'Filter tree' and a help icon. The main list is titled 'Role / Member' with an up arrow. It contains two items: 'Cloud KMS Admin (1)' and 'Cloud KMS CryptoKey Encrypter/Decrypter (2)'. The first item has a dropdown arrow and a list of members. One member, 'cloudmanager-service-account-1@occm-dev.iam.gserviceaccount.com', is highlighted with a yellow box. To the right of the member list are a trash bin icon and a pencil icon.

2. Obtain the "id" of the key by invoking the get command for the /gcp/vsa/metadata/gcp-encryption-keys API.
3. Use the "GcpEncryption" parameter with your API request when creating a working environment.

#### Example

```
"gcpEncryptionParameters": {  
    "key": "projects/tlv-support/locations/us-  
east4/keyRings/Nikiskeys/cryptoKeys/generatedkey1"  
}
```

Refer to the [API Developer Guide](#) for more details about using the "GcpEncryption" parameter.

## 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.

## Launching a single-node system in GCP

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

### What you'll need

- You should have a [Connector that is associated with your workspace](#).



You must be an Account Admin to create a Connector. When you create your first Cloud Volumes ONTAP working environment, Cloud Manager prompts you to create a Connector if you don't have one yet.

- [You should be prepared to leave the Connector running at all times.](#)
- You should have chosen a configuration and obtained GCP networking information from your administrator. For details, see [Planning your Cloud Volumes ONTAP configuration](#).
- To deploy a BYOL system, you need the 20-digit serial number (license key).
- The following 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

### 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. **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 <a href="#">data tiering</a> or <a href="#">Cloud Backup</a> with Cloud Volumes ONTAP, then you need to enable <b>Service Account</b> and select a service account that has the predefined Storage Admin role. <a href="#">Learn how to create a service account</a> .
Add Labels	<p>Labels are metadata for your 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 <a href="#">Google Cloud Documentation: Labeling Resources</a>.</p>

Field	Description
User name and password	These are the credentials for the Cloud Volumes ONTAP cluster admin account. You can use these credentials to connect to Cloud Volumes ONTAP through System Manager or its CLI.
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> <p> This is the service account that you set up for Cloud Manager, <a href="#">as described in step 4b on this page</a>.</p> <p>Click <b>Add Subscription</b> to associate the selected credentials with a subscription.</p> <p>To create a pay-as-you-go Cloud Volumes ONTAP system, you need to select a 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:

► [https://docs.netapp.com/us-en/occm/media/video\\_subscribing\\_gcp.mp4](https://docs.netapp.com/us-en/occm/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. **Location & Connectivity:** Select a location, choose a firewall policy, and select the checkbox to confirm network connectivity 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. For instructions, refer to [Google Cloud Documentation: Configuring Private Google Access](#).

6. **License & Support Site Account:** Specify whether you want to use pay-as-you-go or BYOL, and then specify a NetApp Support Site account.

To understand how licenses work, see [Licensing](#).

A NetApp Support Site Account is optional for pay-as-you-go, but required for BYOL systems. [Learn how to add NetApp Support Site accounts](#).

7. **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.

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

If your needs change after you launch the system, you can modify the license or virtual machine type later.



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 9.6 RC1 and 9.6 GA is available. The update does not occur from one release to another—for example, from 9.6 to 9.7.

9. **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](#).

10. **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](#).

11. **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](#).

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

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.
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, <a href="#">use the IQN to connect to the LUN from your hosts</a>.</p>

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

**Volume Details, Protection & Protocol**

<b>Details &amp; Protection</b> <div style="margin-top: 10px;">         Volume Name: <input type="text" value="vol"/> Size (GB): <input type="text" value="250"/> </div> <div style="margin-top: 10px;">         Snapshot Policy: <input type="text" value="default"/> <div style="float: right;"><small><a href="#">Default Policy</a></small></div> </div>	<b>Protocol</b> <div style="margin-top: 10px;"> <span style="margin-right: 10px;">NFS</span> <span style="background-color: #0070C0; color: white; padding: 2px 10px; border-radius: 5px;">CIFS</span> <span>iSCSI</span> </div> <div style="margin-top: 10px;">         Share name: <input type="text" value="vol_share"/> Permissions: <input type="text" value="Full Control"/> </div> <div style="margin-top: 10px;">         Users / Groups: <input type="text" value="engineering"/> <div style="font-size: small; margin-top: -10px;">Valid users and groups separated by a semicolon</div> </div>
--	---

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

Field	Description
DNS Primary and Secondary IP Address	The IP addresses of the DNS servers that provide name resolution for the CIFS server. The listed DNS servers must contain the service location records (SRV) needed to locate the Active Directory LDAP servers and domain controllers for the domain that the CIFS server will join.
Active Directory Domain to join	The FQDN of the Active Directory (AD) domain that you want the CIFS server to join.
Credentials authorized to join the domain	The name and password of a Windows account with sufficient privileges to add computers to the specified Organizational Unit (OU) within the AD domain.
CIFS server NetBIOS name	A CIFS server name that is unique in the AD domain.
Organizational Unit	The organizational unit within the AD domain to associate with the CIFS server. The default is CN=Computers.
DNS Domain	The DNS domain for the Cloud Volumes ONTAP storage virtual machine (SVM). In most cases, the domain is the same as the AD domain.
NTP Server	Select <b>Use Active Directory Domain</b> to configure an NTP server using the Active Directory DNS. If you need to configure an NTP server using a different address, then you should use the API. See the <a href="#">Cloud Manager API Developer Guide</a> for details.

14. **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](#).

15. **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.

### What you'll need

- You should have a [Connector that is associated with your workspace](#).



You must be an Account Admin to create a Connector. When you create your first Cloud Volumes ONTAP working environment, Cloud Manager prompts you to create a Connector if you don't have one yet.

- The service account associated with the Connector [should have the latest permissions](#).
- [You should be prepared to leave the Connector running at all times](#).
- You should have chosen a configuration and obtained GCP networking information from your administrator. For details, see [Planning your Cloud Volumes ONTAP configuration](#).
- To deploy a BYOL system, you need the 20-digit serial number (license key) for each node.
- The following 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

## 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 <a href="#">Tiering</a> or <a href="#">Cloud Backup</a> services, you need to enable the <b>Service Account</b> switch and then select the Service Account that has the predefined Storage Admin role.
Add Labels	<p>Labels are metadata for your 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 <a href="#">Google Cloud Documentation: Labeling Resources</a>.</p>
User name and password	These are the credentials for the Cloud Volumes ONTAP cluster admin account. You can use these credentials to connect to Cloud Volumes ONTAP through System Manager or its CLI.
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> <p> This is the service account that you set up for Cloud Manager, <a href="#">as described in step 4b on this page</a>.</p> <p>Click <b>Add Subscription</b> to associate the selected credentials with a subscription.</p> <p>To create a pay-as-you-go Cloud Volumes ONTAP system, you need to select a 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:

► [https://docs.netapp.com/us-en/occm/media/video\\_subscribing\\_gcp.mp4](https://docs.netapp.com/us-en/occm/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.](#)

7. **License & Support Site Account:** Specify whether you want to use pay-as-you-go or BYOL, and then specify a NetApp Support Site account.

To understand how licenses work, see [Licensing](#).

A NetApp Support Site Account is optional for pay-as-you-go, but required for BYOL systems. [Learn how to add NetApp Support Site accounts](#).

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, select a license, and select a virtual machine type.

If your needs change after you launch the system, you can modify the license or virtual machine type later.



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 9.8 RC1 and 9.8 GA is available. The update does not occur from one release to another—for example, from 9.7 to 9.8.

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**.

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.
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, <a href="#">use the IQN to connect to the LUN from your hosts</a>.</p>

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

The screenshot shows the 'Volume Details, Protection & Protocol' page. In the 'Protocol' section, 'CIFS' is selected. Under 'Details & Protection', the 'Volume Name' is 'vol' and the 'Size (GB)' is '250'. The 'Snapshot Policy' is set to 'default'. A note indicates 'Default Policy'. In the 'Protocol' section, the 'Share name' is 'vol\_share' and the 'Permissions' are 'Full Control'. The 'Users / Groups' field contains 'engineering'. A note states '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	The IP addresses of the DNS servers that provide name resolution for the CIFS server. The listed DNS servers must contain the service location records (SRV) needed to locate the Active Directory LDAP servers and domain controllers for the domain that the CIFS server will join.
Active Directory Domain to join	The FQDN of the Active Directory (AD) domain that you want the CIFS server to join.
Credentials authorized to join the domain	The name and password of a Windows account with sufficient privileges to add computers to the specified Organizational Unit (OU) within the AD domain.
CIFS server NetBIOS name	A CIFS server name that is unique in the AD domain.
Organizational Unit	The organizational unit within the AD domain to associate with the CIFS server. The default is CN=Computers.
DNS Domain	The DNS domain for the Cloud Volumes ONTAP storage virtual machine (SVM). In most cases, the domain is the same as the AD domain.
NTP Server	Select <b>Use Active Directory Domain</b> to configure an NTP server using the Active Directory DNS. If you need to configure an NTP server using a different address, then you should use the API. See the <a href="#">Cloud Manager API Developer Guide</a> for details.

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.

# Provision and manage storage

## Provisioning storage

You can provision additional storage for your Cloud Volumes ONTAP systems from Cloud Manager by managing volumes and aggregates.



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.

### Creating FlexVol volumes

If you need more storage after you launch a Cloud Volumes ONTAP system, you can create new FlexVol volumes for NFS, CIFS, or iSCSI from Cloud Manager.

#### About this task

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.

#### Before you begin

If you want to use CIFS in AWS, you must have set up DNS and Active Directory. For details, see [Networking requirements for Cloud Volumes ONTAP for AWS](#).

#### Steps

1. On the Canvas page, double-click the name of the Cloud Volumes ONTAP system on which you want to provision FlexVol volumes.
2. Create a new volume on any aggregate or on a specific aggregate:

Action	Steps
Create a new volume and let Cloud Manager choose the containing aggregate	Click <b>Add New Volume</b> .
Create a new volume on a specific aggregate	<ol style="list-style-type: none"> <li>a. Click the menu icon, and then click <b>Advanced &gt; Advanced allocation</b>.</li> <li>b. Click the menu for an aggregate.</li> <li>c. Click <b>Create volume</b>.</li> </ol>

3. Enter details for the new volume, and then click **Continue**.

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.
Advanced options (for NFS only)	Select an NFS version for the volume: either NFSv3 or NFSv4.

Field	Description
Initiator group and IQN (for iSCSI only)	<p>iSCSI storage targets are called LUNs (logical units) and are presented to hosts as standard block devices.</p> <p>Initiator groups are tables of iSCSI host node names and control which initiators have access to which LUNs.</p> <p>iSCSI targets connect to the network through standard Ethernet network adapters (NICs), TCP offload engine (TOE) cards with software initiators, converged network adapters (CNAs) or dedicated host bus adapters (HBAs) and are identified by iSCSI qualified names (IQNs).</p> <p>When you create an iSCSI volume, 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, <a href="#">use the IQN to connect to the LUN from your hosts</a>.</p>

4. If you chose the CIFS protocol and the CIFS server has not been set up, specify details for the server in the Create a CIFS Server dialog box, and then click **Save and continue**:

Field	Description
DNS Primary and Secondary IP Address	<p>The IP addresses of the DNS servers that provide name resolution for the CIFS server.</p> <p>The listed DNS servers must contain the service location records (SRV) needed to locate the Active Directory LDAP servers and domain controllers for the domain that the CIFS server will join.</p>
Active Directory Domain to join	The FQDN of the Active Directory (AD) domain that you want the CIFS server to join.
Credentials authorized to join the domain	The name and password of a Windows account with sufficient privileges to add computers to the specified Organizational Unit (OU) within the AD domain.
CIFS server NetBIOS name	A CIFS server name that is unique in the AD domain.
Organizational Unit	<p>The organizational unit within the AD domain to associate with the CIFS server. The default is CN=Computers.</p> <ul style="list-style-type: none"> <li>• To configure AWS Managed Microsoft AD as the AD server for Cloud Volumes ONTAP, you should enter <b>OU=Computers,OU=corp</b> in this field.</li> <li>• To configure Azure AD Domain Services as the AD server for Cloud Volumes ONTAP, you should enter <b>OU=AADDC Computers</b> or <b>OU=AADDC Users</b> in this field.</li> </ul> <p><a href="#">Azure Documentation: Create an Organizational Unit (OU) in an Azure AD Domain Services managed domain</a></p>
DNS Domain	The DNS domain for the Cloud Volumes ONTAP storage virtual machine (SVM). In most cases, the domain is the same as the AD domain.

Field	Description
NTP Server	Select <b>Use Active Directory Domain</b> to configure an NTP server using the Active Directory DNS. If you need to configure an NTP server using a different address, then you should use the API. See the <a href="#">Cloud Manager API Developer Guide</a> for details.

5. On the Usage Profile, Disk Type, and Tiering Policy page, choose whether you want to enable storage efficiency features, choose a disk type, and edit the tiering policy, if needed.

For help, refer to the following:

- [Understanding volume usage profiles](#)
- [Sizing your system in AWS](#)
- [Sizing your system in Azure](#)
- [Data tiering overview](#)

6. Click **Go**.

## Result

Cloud Volumes ONTAP provisions the volume.

## 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, 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.

## Creating FlexVol volumes 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**.

## After you finish

You can create additional volumes on this aggregate if required.



For HA pairs deployed in multiple AWS Availability Zones, you must mount the volume to clients by using the floating IP address of the node on which the volume resides.

## **Creating 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.

### **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.

For help with disk type and disk size, see [Planning your configuration](#).

4. Click **Go**, and then click **Approve and Purchase**.

## **Connecting 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:

1. Cloud Manager's automatic capacity management doesn't apply to LUNs. When Cloud Manager creates a LUN, it disables the autogrow feature.
2. 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](#)

## **Using FlexCache volumes to accelerate data access**

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 GB usage limit.



To generate the license, Cloud Manager needs to access <https://ipa-signer.cloudmanager.netapp.com>. Make sure that this URL is accessible from your firewall.



## Managing existing storage

Cloud Manager enables you to manage volumes, aggregates, and CIFS servers. It also prompts you to move volumes to avoid capacity issues.

### Managing existing volumes

You can manage existing 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 <b>Info</b> .

Task	Action
Edit a volume (read-write volumes only)	<p>a. Select a volume, and then click <b>Edit</b>.</p> <p>b. Modify the volume's Snapshot policy, NFS protocol version, NFS access control list, or share permissions, and then click <b>Update</b>.</p> <p> If you need custom Snapshot policies, you can create them by using System Manager.</p>
Clone a volume	<p>a. Select a volume, and then click <b>Clone</b>.</p> <p>b. Modify the clone name as needed, and then click <b>Clone</b>.</p> <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 <a href="#">ONTAP 9 Logical Storage Management Guide</a>.</p>
Restore data from a Snapshot copy to a new volume	<p>a. Select a volume, and then click <b>Restore from Snapshot copy</b>.</p> <p>b. Select a Snapshot copy, enter a name for the new volume, and then click <b>Restore</b>.</p>
Create a Snapshot copy on demand	<p>a. Select a volume, and then click <b>Create a Snapshot copy</b>.</p> <p>b. Change the name, if needed, and then click <b>Create</b>.</p>
Get the NFS mount command	<p>a. Select a volume, and then click <b>Mount Command</b>.</p> <p>b. Click <b>Copy</b>.</p>
View the target iQN for an iSCSI volume	<p>a. Select a volume, and then click <b>Target iQN</b>.</p> <p>b. Click <b>Copy</b>.</p> <p>c. <a href="#">Use the IQN to connect to the LUN from your hosts</a>.</p>
Change the underlying disk type	<p>a. Select a volume, and then click <b>Change Disk Type &amp; Tiering Policy</b>.</p> <p>b. Select the disk type, and then click <b>Change</b>.</p> <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>

Task	Action
Change the tiering policy	<ol style="list-style-type: none"> <li>a. Select a volume, and then click <b>Change Disk Type &amp; Tiering Policy</b>.</li> <li>b. Click <b>Edit Policy</b>.</li> <li>c. Select a different policy and click <b>Change</b>.</li> </ol> <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>
Delete a volume	<ol style="list-style-type: none"> <li>a. Select a volume, and then click <b>Delete</b>.</li> <li>b. Click <b>Delete</b> again to confirm.</li> </ol>

## Managing existing aggregates

Manage aggregates yourself by adding disks, viewing information about the aggregates, and by deleting them.

### 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 OnCommand 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 <b>Info</b> .
Create a volume on a specific aggregate	Select an aggregate and click <b>Create volume</b> .
Add disks to an aggregate	<ol style="list-style-type: none"> <li>a. Select an aggregate and click <b>Add AWS disks</b> or <b>Add Azure disks</b>.</li> <li>b. Select the number of disks that you want to add and click <b>Add</b>.</li> </ol> <p> All disks in an aggregate must be the same size.</p>
Delete an aggregate	<ol style="list-style-type: none"> <li>a. Select an aggregate that does not contain any volumes and click <b>Delete</b>.</li> <li>b. Click <b>Delete</b> again to confirm.</li> </ol>

## Modifying the CIFS server

If you change your DNS servers or Active Directory domain, you need to modify the CIFS server in Cloud Volumes ONTAP so that it can continue to serve storage to clients.

### Steps

1. From the working environment, click the menu icon and then click **Advanced > CIFS setup**.
2. Specify settings for the CIFS server:

Task	Action
DNS Primary and Secondary IP Address	The IP addresses of the DNS servers that provide name resolution for the CIFS server.  The listed DNS servers must contain the service location records (SRV) needed to locate the Active Directory LDAP servers and domain controllers for the domain that the CIFS server will join.
Active Directory Domain to join	The FQDN of the Active Directory (AD) domain that you want the CIFS server to join.
Credentials authorized to join the domain	The name and password of a Windows account with sufficient privileges to add computers to the specified Organizational Unit (OU) within the AD domain.
CIFS server NetBIOS name	A CIFS server name that is unique in the AD domain.
Organizational Unit	The organizational unit within the AD domain to associate with the CIFS server. The default is CN=Computers.  If you configure AWS Managed Microsoft AD as the AD server for Cloud Volumes ONTAP, you should enter <b>OU=Computers,OU=corp</b> in this field.
DNS Domain	The DNS domain for the Cloud Volumes ONTAP storage virtual machine (SVM). In most cases, the domain is the same as the AD domain.
NTP Server	Select <b>Use Active Directory Domain</b> to configure an NTP server using the Active Directory DNS. If you need to configure an NTP server using a different address, then you should use the API. See the <a href="#">Cloud Manager API Developer Guide</a> for details.

3. Click **Save**.

### Result

Cloud Volumes ONTAP updates the CIFS server with the changes.

## Moving 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](#).

## Moving 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 it cannot provide recommendations to correct the issue. If this happens, you need to identify how to correct the issue and then move one or more volumes.

### 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](#).

### Identifying how to correct capacity issues

If Cloud Manager cannot 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.

Used Aggregate Capacity: 105.66 GB

Volumes:

4

Vol54 (54 GB)

data\_vol (150 GB)

svm\_FinanceOnPrem\_root (1 GB)



- 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](#).

#### **Moving 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 [Managing existing volumes](#).

## Moving 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.
- The Cloud Volumes ONTAP system is in AWS and one aggregate 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:



### Choose a supported configuration

Most configurations are supported. If you have a Cloud Volumes ONTAP Standard, Premium, or BYOL system running the most recent version, then you should be good to go. [Learn more](#).



### Ensure connectivity between Cloud Volumes ONTAP and object storage

- For AWS, you'll need a VPC Endpoint to S3. [Learn more](#).
- For Azure, you won't need to do anything as long as Cloud Manager has the required permissions. [Learn more](#).
- For GCP, you need to configure the subnet for Private Google Access and set up a service account. [Learn more](#).



### 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](#).



### 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 the capacity tier (an S3 bucket, Azure Blob container, or GCP bucket). 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:

- Data tiering is supported with Cloud Volumes ONTAP Standard, Premium, and BYOL, starting with the following versions:
  - Version 9.2 in AWS
  - Version 9.4 in Azure with single node systems
  - Version 9.6 in Azure with HA pairs
  - Version 9.6 in GCP



Data tiering is not supported in Azure with the DS3\_v2 virtual machine type.

- In AWS, the performance tier can be General Purpose SSDs, Provisioned IOPS SSDs, or Throughput Optimized HDDs.
- In Azure, the performance tier can be Premium SSD managed disks, Standard SSD managed disks, or Standard HDD managed disks.
- In GCP, the performance tier can be either SSDs or HDDs (standard disks).
- Data tiering is supported with encryption technologies.
- Thin provisioning must be enabled on volumes.

## Requirements

Depending on your cloud provider, certain connections and permissions must be set up so that Cloud Volumes ONTAP can tier cold data to object storage.

### Requirements to tier cold data to AWS S3

Ensure that Cloud Volumes ONTAP has a connection to S3. The best way to provide that connection is by creating a VPC Endpoint to the S3 service. For instructions, see [AWS Documentation: Creating a Gateway Endpoint](#).

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

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

## Requirements to tier cold data to Azure Blob storage

You don't need to set up a connection between the performance tier and the capacity tier as long as Cloud Manager has the required permissions. Cloud Manager enables a VNet service endpoint for you if the Cloud Manager policy has these permissions:

```
"Microsoft.Network/virtualNetworks/subnets/write",  
"Microsoft.Network/routeTables/join/action",
```

The permissions are included in the latest [Cloud Manager policy](#).

## 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](#).
- You need a service account that meets the following requirements:
  - It must have the predefined Storage Admin role.
  - The Connector service account must be a *Service Account User* of this tiering service account.

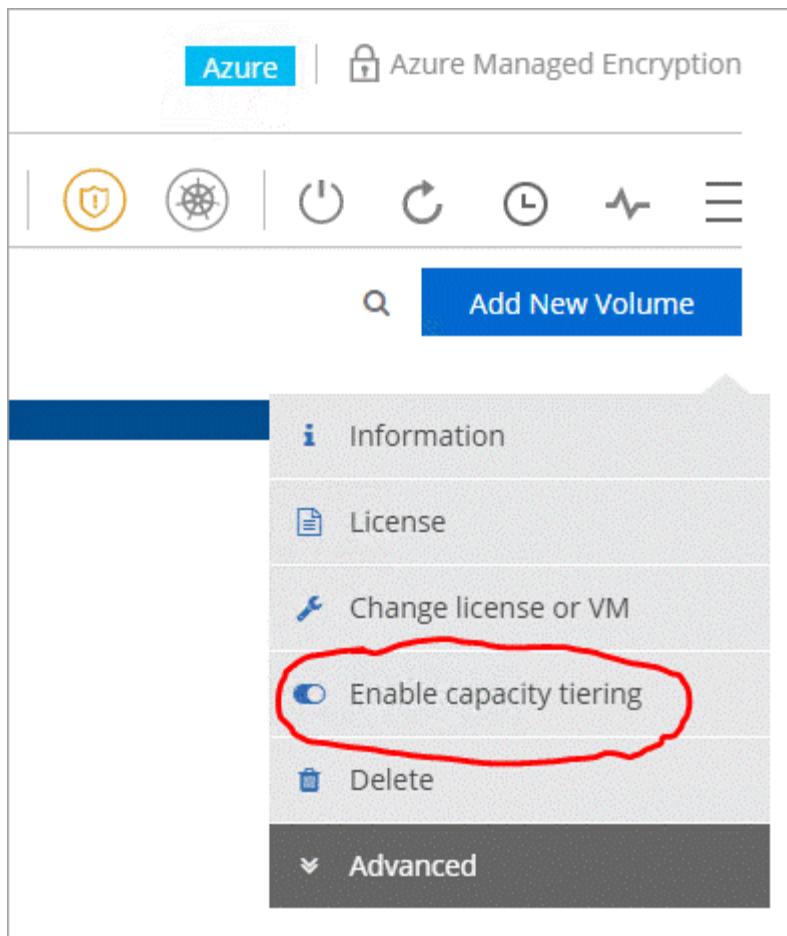
[Read step-by-step instructions](#).

## 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.

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.

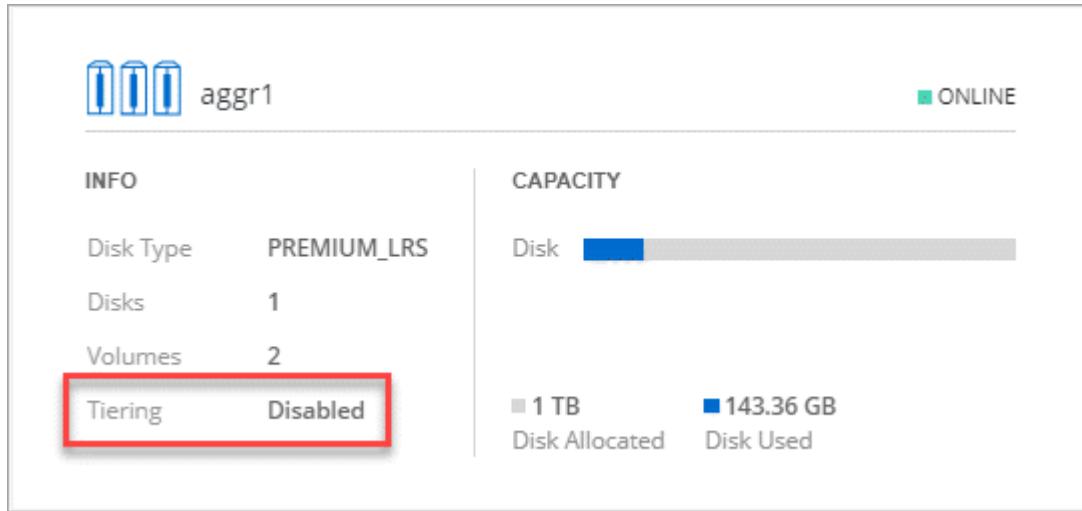
- **Existing volumes**

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 <b>Add New Volume</b> .
Modify an existing volume	Select the volume and click <b>Change Disk Type &amp; Tiering Policy</b> .

2. Select a tiering policy.

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

#### Example



## Tiering data to object storage

### i 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.

### i 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

i 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**.

## Manage storage VMs

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

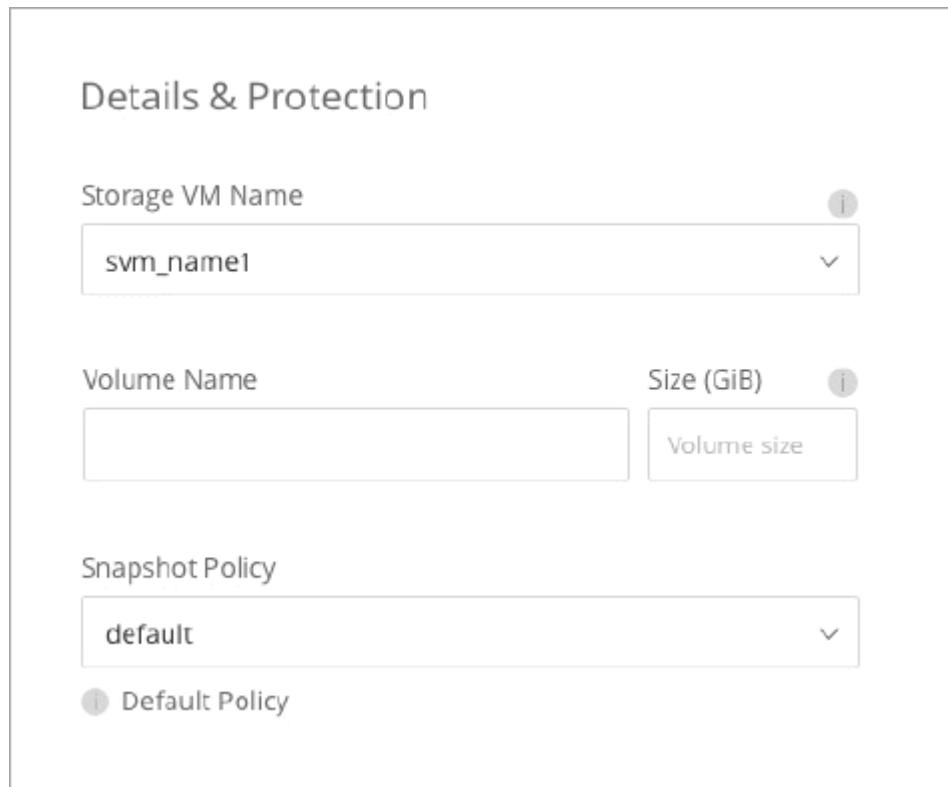
Cloud Volumes ONTAP 9.7 and 9.8 support multiple storage VMs in AWS with certain configurations and an add-on license. [View the number of supported storage VMs in AWS](#). Contact your account team to obtain an SVM add-on license.

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.

### Work with storage VMs in Cloud Manager

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.



And the following image shows how you can choose a storage VM when replicating a volume to another system.

The screenshot shows a configuration interface with three main input fields:

- Destination Volume Name:** A text input field containing "volume\_copy".
- Destination Storage VM Name:** A dropdown menu currently set to "svm\_name1".
- Destination Aggregate:** A dropdown menu currently set to "Automatically select the best aggregate".

## Create data-serving storage VMs for Cloud Volumes ONTAP in AWS

As noted above, multiple storage VMs are supported with Cloud Volumes ONTAP in AWS. To create additional storage VMs, you need to allocate IP addresses in AWS and then run ONTAP commands based on your Cloud Volumes ONTAP configuration.

### Verify limits for your configuration

Each EC2 instance supports a maximum number of private IPv4 addresses per network interface. You need to verify the limit before you allocate IP addresses in AWS for the new storage VM.

#### Steps

1. Go the [Storage limits section in the Cloud Volumes ONTAP Release Notes](#).
2. Identify the maximum number of IP addresses per interface for your instance type.
3. Make note of this number because you'll need it in the next section when you allocate IP addresses in AWS.

#### Allocate IP addresses in AWS

Private IPv4 addresses must be assigned to port e0a in AWS before you create LIFs for the new storage VM.

Note that an optional management LIF for a storage VM requires a private IP address on a single node system and on an HA pair in a single AZ. This management LIF provides a connection to management tools like SnapCenter.

#### Steps

1. Log in to AWS and open the EC2 service.
2. Select the Cloud Volumes ONTAP instance and click **Networking**.

If you're creating a storage VM on an HA pair, select node 1.

3. Scroll down to **Network interfaces** and click the **Interface ID** for port e0a.

Name	Insta...	Instance state	Instance type	Status check
danielleAws	i-070...	Running	m5.2xlarge	2/2 check
occmTiering0702	i-0a7...	Stopped	m5.2xlarge	-
cvoTiering1	i-02a...	Stopped	m5.2xlarge	-

Interface ID	Description
<a href="#">eni-07c301...</a>	Interface for Node & Cluster Management, Inter-Cluster Communication, and Data - e0a

4. Select the network interface and click **Actions > Manage IP addresses**.
5. Expand the list of IP addresses for e0a.
6. Verify the IP addresses:
  - a. Count the number of allocated IP addresses to confirm that the port has room for additional IPs.  
You should have identified the maximum number of supported IP addresses per interface in the previous section of this page.
  - b. Optional: Go to the CLI for Cloud Volumes ONTAP and run **network interface show** to confirm that each of these IP addresses are in use.  
If an IP address isn't in use, then you can use it with the new storage VM.
7. Back in the AWS Console, click **Assign new IP address** to assign additional IP addresses based on the amount that you need for the new storage VM.
  - Single node system: One unused secondary private IP is required.  
An optional secondary private IP is required if you want to create a management LIF on the storage VM.
  - HA pair in a single AZ: One unused secondary private IP is required on node 1.  
An optional secondary private IP is required if you want to create a management LIF on the storage VM.
  - HA pair in multiple AZs: One unused secondary private IP is required on each node.
8. If you're allocating the IP address on an HA pair in a single AZ, enable **Allow secondary private IPv4 addresses to be reassigned**.
9. Click **Save**.
10. If you have an HA pair in multiple AZs, then you'll need to repeat these steps for node 2.

#### Create a storage VM on a single node system

These steps create a new storage VM on a single node system. One private IP address is required to create a NAS LIF and another optional private IP address is needed if you want to create a management LIF.

## Steps

1. Create the storage VM and a route to the storage VM.

```
vserver create -rootvolume-security-style mixed -rootvolume root_svm_2  
-snapshot-policy default -vserver svm_2 -aggregate aggr1
```

```
network route create -destination 0.0.0.0/0 -vserver svm_2 -gateway  
subnet_gateway
```

2. Create a NAS LIF.

```
network interface create -auto-revert true -vserver svm_2 -service  
-policy default-data-files -home-port e0a -address private_ip_x -netmask  
node1Mask -lif ip_nas_2 -home-node cvo-node
```

Where *private\_ip\_x* is an unused secondary private IP on e0a.

3. Optional: Create a storage VM management LIF.

```
network interface create -auto-revert true -vserver svm_2 -service  
-policy default-management -home-port e0a -address private_ip_y -netmask  
node1Mask -lif ip_svm_mgmt_2 -home-node cvo-node
```

Where *private\_ip\_y* is another unused secondary private IP on e0a.

## Create a storage VM on an HA pair in a single AZ

These steps create a new storage VM on an HA pair in a single AZ. One private IP address is required to create a NAS LIF and another optional private IP address is needed if you want to create a management LIF.

Both of these LIFs get allocated on node 1. The private IP addresses can move between nodes if failures occur.

## Steps

1. Create the storage VM and a route to the storage VM.

```
vserver create -rootvolume-security-style mixed -rootvolume root_svm_2  
-snapshot-policy default -vserver svm_2 -aggregate aggr1
```

```
network route create -destination 0.0.0.0/0 -vserver svm_2 -gateway  
subnet_gateway
```

## 2. Create a NAS LIF on node 1.

```
network interface create -auto-revert true -vserver svm_2 -service  
-policy default-data-files -home-port e0a -address private_ip_x -netmask  
node1Mask -lif ip_nas_2 -home-node cvo-node1
```

Where *private\_ip\_x* is an unused secondary private IP on e0a of cvo-node1. This IP address can be relocated to the e0a of cvo-node2 in case of takeover because the service policy default-data-files indicates that IPs can migrate to the partner node.

## 3. Optional: Create a storage VM management LIF on node 1.

```
network interface create -auto-revert true -vserver svm_2 -service  
-policy default-management -home-port e0a -address private_ip_y -netmask  
node1Mask -lif ip_svm_mgmt_2 -home-node cvo-node1
```

Where *private\_ip\_y* is another unused secondary private IP on e0a.

### Create a storage VM on an HA pair in multiple AZs

These steps create a new storage VM on an HA pair in multiple AZs.

A *floating* IP address is required for a NAS LIF and is optional for a management LIF. These floating IP addresses don't require you to allocate private IPs in AWS. Instead, the floating IPs are automatically configured in the AWS route table to point to a specific node's ENI in the same VPC.

In order for floating IPs to work with ONTAP, a private IP address must be configured on every storage VM on each node. This is reflected in the steps below where an iSCSI LIF is created on node 1 and on node 2.

### Steps

#### 1. Create the storage VM and a route to the storage VM.

```
vserver create -rootvolume-security-style mixed -rootvolume root_svm_2  
-snapshot-policy default -vserver svm_2 -aggregate aggr1
```

```
network route create -destination 0.0.0.0/0 -vserver svm_2 -gateway  
subnet_gateway
```

#### 2. Create a NAS LIF on node 1.

```
network interface create -auto-revert true -vserver svm_2 -service  
-policy default-data-files -home-port e0a -address floating_ip -netmask  
node1Mask -lif ip_nas_floating_2 -home-node cvo-node1
```

- The floating IP address must be outside of the CIDR blocks for all VPCs in the AWS region in which you deploy the HA configuration. 192.168.209.27 is an example floating IP address. [Learn more about choosing a floating IP address](#).
- `-service-policy default-data-files` indicates that IPs can migrate to the partner node.

3. Optional: Create a storage VM management LIF on node 1.

```
network interface create -auto-revert true -vserver svm_2 -service
-policy default-management -home-port e0a -address floating_ip -netmask
node1Mask -lif ip_svm_mgmt_2 -home-node cvo-node1
```

4. Create an iSCSI LIF on node 1.

```
network interface create -vserver svm_2 -service-policy default-data-
blocks -home-port e0a -address private_ip -netmask node1Mask -lif
ip_node1_iscsi_2 -home-node cvo-node1
```

- This iSCSI LIF is required to support LIF migration of the floating IPs in the storage VM. It doesn't have to be an iSCSI LIF, but it can't be configured to migrate between nodes.
- `-service-policy default-data-block` indicates that an IP address does not migrate between nodes.
- `private_ip` is an unused secondary private IP address on eth0 (e0a) of cvo\_node1.

5. Create an iSCSI LIF on node 2.

```
network interface create -vserver svm_2 -service-policy default-data-
blocks -home-port e0a -address private_ip -netmaskNode2Mask -lif
ip_node2_iscsi_2 -home-node cvo-node2
```

- This iSCSI LIF is required to support LIF migration of the floating IPs in the storage VM. It doesn't have to be an iSCSI LIF, but it can't be configured to migrate between nodes.
- `-service-policy default-data-block` indicates that an IP address does not migrate between nodes.
- `private_ip` is an unused secondary private IP address on eth0 (e0a) of cvo\_node2.

## 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](#)

# Using Cloud Volumes ONTAP as persistent storage for Kubernetes

Cloud Manager can automate the deployment of NetApp Trident on Kubernetes clusters so you can use Cloud Volumes ONTAP as persistent storage for containers.

Trident is a fully-supported open source project maintained by NetApp. Trident integrates natively with Kubernetes and its Persistent Volume framework to seamlessly provision and manage volumes from systems running any combination of NetApp's storage platforms. [Learn more about Trident](#).



The Kubernetes feature isn't supported with on-prem ONTAP clusters. It's supported with Cloud Volumes ONTAP only.

## Quick start

Get started quickly by following these steps or scroll down to the remaining sections for full details.



### Review prerequisites

Ensure that your environment can meet the prerequisites, which includes connectivity between Kubernetes clusters and Cloud Volumes ONTAP, connectivity between Kubernetes clusters and a Connector, a minimum Kubernetes version of 1.14, at least one worker node in a cluster, and more. [See the complete list](#).



### Add your Kubernetes clusters to Cloud Manager

In Cloud Manager, click **K8s** and discover clusters directly from your cloud provider's managed service or import a cluster by providing a kubeconfig file.



### Connect your clusters to Cloud Volumes ONTAP

After you add a Kubernetes cluster, click **Connect to Working Environment** to connect the cluster to one or more Cloud Volumes ONTAP systems.



### Start provisioning Persistent Volumes

Request and manage Persistent Volumes using native Kubernetes interfaces and constructs. Cloud Manager creates NFS and iSCSI storage classes that you can use when provisioning Persistent Volumes.

[Learn more about provisioning your first volume with Trident for Kubernetes](#).

## Reviewing prerequisites

Before you get started, ensure that your Kubernetes clusters and Connector meet specific requirements.

### Kubernetes cluster requirements

- Network connectivity is required between a Kubernetes cluster and the Connector and between a Kubernetes cluster and Cloud Volumes ONTAP.

Both the Connector and Cloud Volumes ONTAP need a connection to the Kubernetes API endpoint:

- For managed clusters, set up a route between a cluster’s VPC and the VPC where the Connector and Cloud Volumes ONTAP reside.
- For other clusters, the IP address of the master node or load balancer (as listed in the kubeconfig file) must be reachable by the Connector and Cloud Volumes ONTAP, and it must present a valid TLS certificate.
- A Kubernetes cluster can be in any location that has the network connectivity listed above.
- A Kubernetes cluster must be running version 1.14 at a minimum.

The maximum supported version is defined by Trident. [Click here to see the maximum supported Kubernetes version.](#)

- A Kubernetes cluster must have at least one worker node.
- For clusters running in Amazon Elastic Kubernetes Service (Amazon EKS), each cluster needs an IAM role added in order to resolve a permissions error. After you add the cluster, Cloud Manager will prompt you with the exact `eksctl` command that resolves the error.

[Learn about IAM permissions boundaries.](#)

- For clusters running in Azure Kubernetes Service (AKS), those clusters must be assigned the *Azure Kubernetes Service RBAC Cluster Admin* role. This is required so Cloud Manager can install Trident and configure storage classes on the cluster.
- For clusters running in Google Kubernetes Engine (GKE), those clusters must not use the default Container Optimized OS. You should switch them to use Ubuntu.

GKE defaults to using the Google [container-optimized image](#), which doesn’t have the utilities that Trident needs to mount volumes.

## Connector requirements

Ensure that the following permissions are in place for the Connector.

### Required permissions to discover and manage EKS clusters

The Connector needs Admin permissions to discover and manage Kubernetes clusters running in Amazon Elastic Kubernetes Service (EKS):

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": "eks:*",
      "Resource": "*"
    }
  ]
}
```

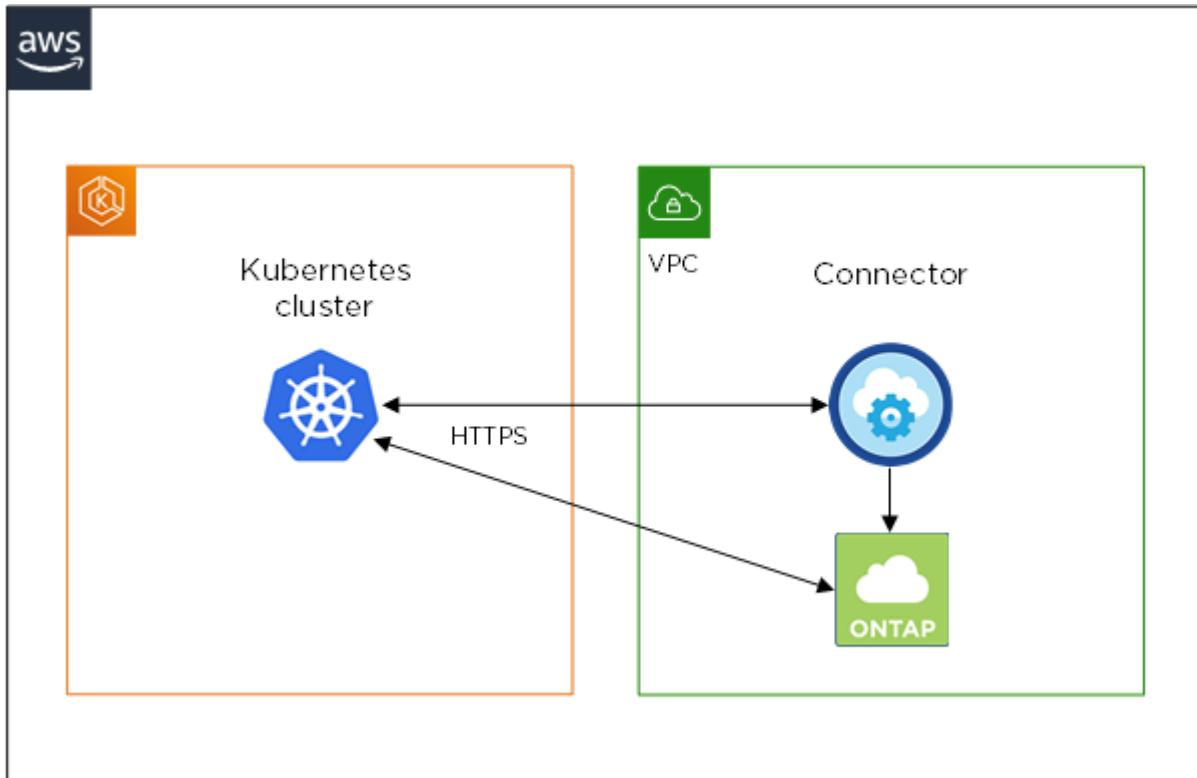
## Required permissions to discover and manage GKE clusters

The Connector needs the following permissions to discover and manage Kubernetes clusters running in Google Kubernetes Engine (GKE):

```
container.*
```

## Example setup

The following image shows an example of a Kubernetes cluster running in Amazon Elastic Kubernetes Service (Amazon EKS) and its connections to the Connector and Cloud Volumes ONTAP.



## Adding Kubernetes clusters

Add Kubernetes clusters to Cloud Manager by discovering the clusters running in your cloud provider's managed Kubernetes service or by importing a cluster's kubeconfig file.

### Steps

1. At the top of Cloud Manager, click **K8s**.
2. Click **Add Cluster**.
3. Choose one of the available options:
  - Click **Discover Clusters** to discover the managed clusters that Cloud Manager has access to based on permissions that you provided to the Connector.

For example, if your Connector is running in Google Cloud, Cloud Manager uses the permissions from the Connector's service account to discover clusters running in Google Kubernetes Engine (GKE).

- Click **Import Cluster** to import a cluster using a kubeconfig file.

After you upload the file, Cloud Manager verifies connectivity to the cluster and saves an encrypted copy of the kubeconfig file.

### Result

Cloud Manager adds the Kubernetes cluster. You can now connect the cluster to Cloud Volumes ONTAP.

## Connecting a cluster to Cloud Volumes ONTAP

Connect a Kubernetes cluster to Cloud Volumes ONTAP so you can use Cloud Volumes ONTAP as persistent storage for containers.

### Steps

1. At the top of Cloud Manager, click **K8s**.
2. Click **Connect to Working Environment** for the cluster that you just added.

Status	Cluster Name	Added By	Version	Working Environments	Date Added
✓	kubernetes	Import	v1.18.0	<a href="#">Connect to Working Environment</a>	August 30, 2020

3. Select a working environment and click **Continue**.
4. Choose the NetApp storage class to use as the default storage class for the Kubernetes cluster and click **Continue**.

When a user creates a persistent volume, the Kubernetes cluster can use this storage class as the backend storage by default.

5. Choose whether to use default auto export policies or whether to add a custom CIDR block.

Select Storage Class Type

**Working Environment Information**

Name	ishai0ntap4k8
Connected Clusters	None
Region	asia-east1
Zones	asia-east1-a
High Availability	Not Supported
Storage Classes	NFS Single Node <b>Default</b> iSCSI Single Node

**Export Policy Information**

If you plan to use NFS volumes you will need to set an export policy to allow connectivity between your clusters and your volumes.

Use the default auto-export policies. (Suitable for most cases.)

OR

General Network CIDR ⓘ  
0.0.0.0/0

## 6. Click **Add Working Environment**.

### Result

Cloud Manager connects the working environment to the cluster, which can take up to 15 minutes.

## Managing your clusters

Cloud Manager enables you to manage your Kubernetes clusters by changing the default storage class, upgrading Trident, and more.

### Changing the default storage class

Make sure that you've set a Cloud Volumes ONTAP storage class as the default storage class so clusters use Cloud Volumes ONTAP as the backend storage.

### Steps

1. At the top of Cloud Manager, click **K8s**.
2. Click the name of the Kubernetes cluster.
3. In the **Storage Classes** table, click the actions menu on the far right for the storage class that you'd like to set as the default.

6 Storage Classes

Storage Class ID	Provisioner	Volumes	Labels	
Gp2	aws	0		...
NFS Single Node	NetApp	0		...
NFS High Availability <b>Default</b>	NetApp	0		...
iSCSI High Availability	NetApp	0		
iSCSI Single Node	NetApp	0		

**Set as Default**

## 4. Click **Set as Default**.

## Upgrading Trident

You can upgrade Trident from Cloud Manager when a new version is available.

### Steps

1. At the top of Cloud Manager, click **K8s**.
2. Click the name of the Kubernetes cluster.
3. If a new version is available, click **Upgrade** next to the Trident version.

The screenshot shows the 'Cluster Details' page for a cluster named 'kubernetes-baldwin'. The page includes a header with 'Cluster List > Cluster Details >' and a top navigation bar with 'Connect to Working Environment' and 'Remove Cluster' buttons. Below the header, the cluster name 'kubernetes-baldwin' is displayed. The main content area contains the following information:

Status	Cluster Version	Added by	Volumes	VPC	Date Added	Trident Version	Provider
Running	1.15	Discovery	2	vpc-0485a0b201c3a1f2d	September 3, 2020	v20.04	AWS

On the far right, there is a 'Working Environment' section with a 'Trident Version' field set to 'v20.04' and a green 'Upgrade' button. A red arrow points to the 'Upgrade' button.

### Updating the kubeconfig file

If you added your cluster to Cloud Manager by importing the kubeconfig file, you can upload the latest kubeconfig file to Cloud Manager at any time. You might do this if you've updated the credentials, if you've changed users or roles, or if something changed that affects the cluster, user, namespaces, or authentication.

### Steps

1. At the top of Cloud Manager, click **K8s**.
2. Click the name of the Kubernetes cluster.
3. Click **Update Kubeconfig**.
4. When prompted through your web browser, select the updated kubeconfig file and click **Open**.

### Result

Cloud Manager updates information about the Kubernetes cluster based on the latest kubeconfig file.

### Disconnecting a cluster

When you disconnect a cluster from Cloud Volumes ONTAP, you can no longer use that Cloud Volumes ONTAP system as persistent storage for containers. Existing Persistent Volumes are not deleted.

### Steps

1. At the top of Cloud Manager, click **K8s**.
2. Click the name of the Kubernetes cluster.
3. In the **Working Environments** table, click the actions menu on the far right for the working environment that you want to disconnect.

#### 4. Click **Disconnect**.

### Result

Cloud Manager disconnects the cluster from the Cloud Volumes ONTAP system.

### Removing a cluster

Remove decommissioned clusters from Cloud Manager after you disconnect all working environments from the cluster.

### Steps

1. At the top of Cloud Manager, click **K8s**.
2. Click the name of the Kubernetes cluster.
3. Click **Remove Cluster**.

## Encrypting volumes with NetApp encryption solutions

Cloud Volumes ONTAP supports both NetApp Volume Encryption (NVE) and NetApp Aggregate Encryption (NAE) with an external key manager. 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](#).

Starting with Cloud Volumes ONTAP 9.7, 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. Starting with Cloud Manager 3.7.1, 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. Install SSL certificates and connect to the external key management servers.

[ONTAP 9 NetApp Encryption Power Guide: Configuring external key management](#)

## Replicating data between systems

You can replicate data between working environments by choosing a one-time data replication for data transfer, or a recurring schedule for disaster recovery or long-term retention. For example, you can set up data replication from an on-prem ONTAP system to Cloud Volumes ONTAP for disaster recovery.

Cloud Manager simplifies data replication between volumes on separate systems using SnapMirror and SnapVault technologies. You simply need to identify the source volume and the destination volume, and then choose a replication policy and schedule. Cloud Manager purchases the required disks, configures relationships, applies the replication policy, and then initiates the baseline transfer between volumes.



The baseline transfer includes a full copy of the source data. Subsequent transfers contain differential copies of the source data.

Cloud Manager enables data replication between the following types of working environments:

- From a Cloud Volumes ONTAP system to another Cloud Volumes ONTAP system
- Between a Cloud Volumes ONTAP system and an on-prem ONTAP cluster
- From an on-prem ONTAP cluster to another on-prem ONTAP cluster

## Data replication requirements

Before you can replicate data, you should confirm that specific requirements are met for both Cloud Volumes ONTAP systems and ONTAP clusters.

### Version requirements

You should verify that the source and destination volumes are running compatible ONTAP versions before replicating data. For details, see the [Data Protection Power Guide](#).

### Requirements specific to Cloud Volumes ONTAP

- The instance's security group must include the required inbound and outbound rules: specifically, rules for ICMP and ports 11104 and 11105.

These rules are included in the predefined security group.

- To replicate data between two Cloud Volumes ONTAP systems in different subnets, the subnets must be routed together (this is the default setting).
- To replicate data between a Cloud Volumes ONTAP system in AWS and a system in Azure, you must have a VPN connection between the AWS VPC and the Azure VNet.

### Requirements specific to ONTAP clusters

- An active SnapMirror license must be installed.
- If the cluster is on your premises, you should have a connection from your corporate network to AWS or Azure, which is typically a VPN connection.
- ONTAP clusters must meet additional subnet, port, firewall, and cluster requirements.

For details, see the Cluster and SVM Peering Express Guide for your version of ONTAP.

## Setting up data replication between systems

You can replicate data between Cloud Volumes ONTAP systems and ONTAP clusters by choosing a one-time data replication, which can help you move data to and from the cloud, or a recurring schedule, which can help with disaster recovery or long-term retention.

### About this task

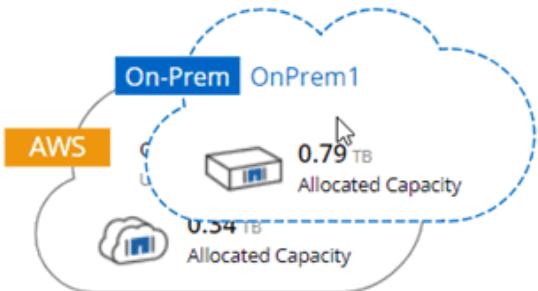
Cloud Manager supports simple, fanout, and cascade data protection configurations:

- In a simple configuration, replication occurs from volume A to volume B.
- In a fanout configuration, replication occurs from volume A to multiple destinations.
- In a cascade configuration, replication occurs from volume A to volume B and from volume B to volume C.

You can configure fanout and cascade configurations in Cloud Manager by setting up multiple data replications between systems. For example, by replicating a volume from system A to system B and then by replicating the same volume from system B to system C.

### Steps

- 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. If the Source and Destination Peering Setup pages appear, select all of the intercluster LIFs for the cluster peer relationship.

The intercluster network should be configured so that cluster peers have *pair-wise full-mesh connectivity*, which means that each pair of clusters in a cluster peer relationship has connectivity among all of their intercluster LIFs.

These pages appear if an ONTAP cluster that has multiple LIFs is the source or destination.

3. On the Source Volume Selection page, select the volume that you want to replicate.
4. On the Destination Volume Name and Tiering page, specify the destination volume name, choose an underlying disk type, change any of the advanced options, and then click **Continue**.

If the destination is an ONTAP cluster, you must also specify the destination SVM and aggregate.

5. On the Max Transfer Rate page, specify the maximum rate (in megabytes per second) at which data can be transferred.
6. On the Replication Policy page, choose one of the default policies or click **Additional Policies**, and then select one of the advanced policies.

For help, see [Choosing a replication policy](#).

If you choose a custom backup (SnapVault) policy, the labels associated with the policy must match the labels of the Snapshot copies on the source volume. For more information, see [How backup policies work](#).

7. On the Schedule page, choose a one-time copy or a recurring schedule.

Several default schedules are available. If you want a different schedule, you must create a new schedule on the *destination* cluster using System Manager.

8. On the Review page, review your selections, and then click **Go**.

## Result

Cloud Manager starts the data replication process. You can view details about the replication in the Replication Status page.

## Managing data replication schedules and relationships

After you set up data replication between two systems, you can manage the data replication schedule and relationship from Cloud Manager.

## Steps

1. On the Canvas page, view the replication status for all working environments in the workspace or for a

specific working environment:

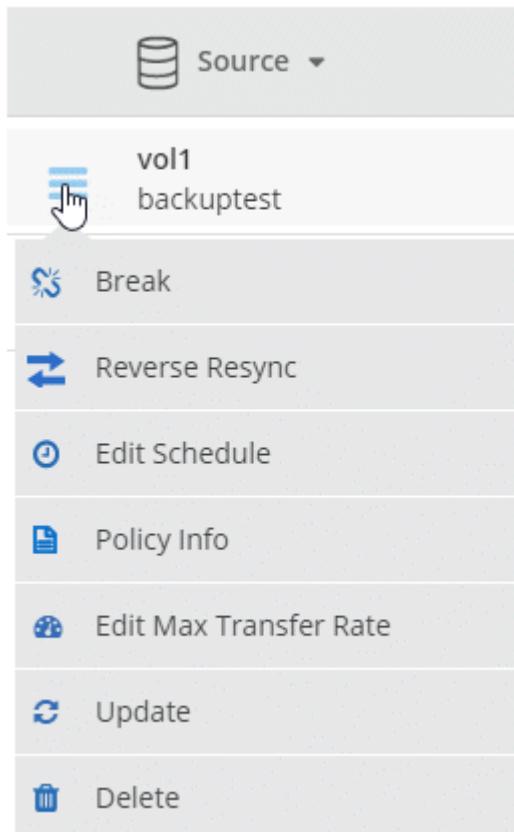
Option	Action
All working environments in the workspace	At the top of Cloud Manager, click <b>Replication</b> .
A specific working environment	Open the working environment and click <b>Replications</b> .

2. Review the status of the data replication relationships to verify that they are healthy.



If the Status of a relationship is idle and the Mirror State is uninitialized, you must initialize the relationship from the destination system for the data replication to occur according to the defined schedule. You can initialize the relationship by using System Manager or the command-line interface (CLI). These states can appear when the destination system fails and then comes back online.

3. Select the menu icon next to the source volume, and then choose one of the available actions.



The following table describes the available actions:

Action	Description
Break	<p>Breaks the relationship between the source and destination volumes, and activates the destination volume for data access.</p> <p>This option is typically used when the source volume cannot serve data due to events such as data corruption, accidental deletion, or an offline state.</p> <p>For information about configuring a destination volume for data access and reactivating a source volume, see the <a href="#">ONTAP 9 Volume Disaster Recovery Express Guide</a>.</p>
Resync	<p>Reestablishes a broken relationship between volumes and resumes data replication according to the defined schedule.</p> <p> When you resynchronize the volumes, the contents on the destination volume are overwritten by the contents on the source volume.</p> <p>To perform a reverse resync, which resynchronizes the data from the destination volume to the source volume, see the <a href="#">ONTAP 9 Volume Disaster Recovery Express Guide</a>.</p>
Reverse Resync	<p>Reverses the roles of the source and destination volumes. Contents from the original source volume are overwritten by contents of the destination volume. This is helpful when you want to reactivate a source volume that went offline.</p> <p>Any data written to the original source volume between the last data replication and the time that the source volume was disabled is not preserved.</p>
Edit Schedule	Enables you to choose a different schedule for data replication.
Policy Info	Shows you the protection policy assigned to the data replication relationship.
Edit Max Transfer Rate	Enables you to edit the maximum rate (in kilobytes per second) at which data can be transferred.
Update	Starts an incremental transfer to update the destination volume.
Delete	Deletes the data protection relationship between the source and destination volumes, which means that data replication no longer occurs between the volumes. This action does not activate the destination volume for data access. This action also deletes the cluster peer relationship and the storage virtual machine (SVM) peer relationship, if there are no other data protection relationships between the systems.

## Result

After you select an action, Cloud Manager updates the relationship or schedule.

## Choosing a replication policy

You might need help choosing a replication policy when you set up data replication in Cloud Manager. A replication policy defines how the storage system replicates data from a source volume to a destination volume.

### What replication policies do

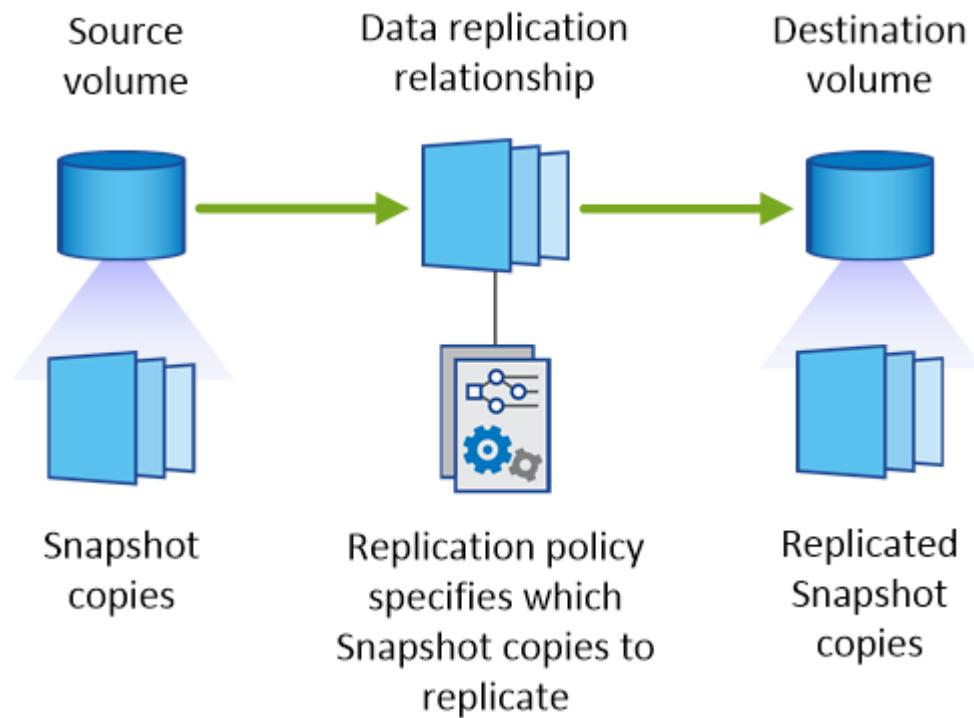
The ONTAP operating system automatically creates backups called Snapshot copies. A Snapshot copy is a read-only image of a volume that captures the state of the file system at a point in time.

When you replicate data between systems, you replicate Snapshot copies from a source volume to a destination volume. A replication policy specifies which Snapshot copies to replicate from the source volume to the destination volume.



Replication policies are also referred to as *protection* policies because they are powered by SnapMirror and SnapVault technologies, which provide disaster recovery protection and disk-to-disk backup and recovery.

The following image shows the relationship between Snapshot copies and replication policies:



## Types of replication policies

There are three types of replication policies:

- A *Mirror* policy replicates newly created Snapshot copies to a destination volume.

You can use these Snapshot copies to protect the source volume in preparation for disaster recovery or for one-time data replication. You can activate the destination volume for data access at any time.

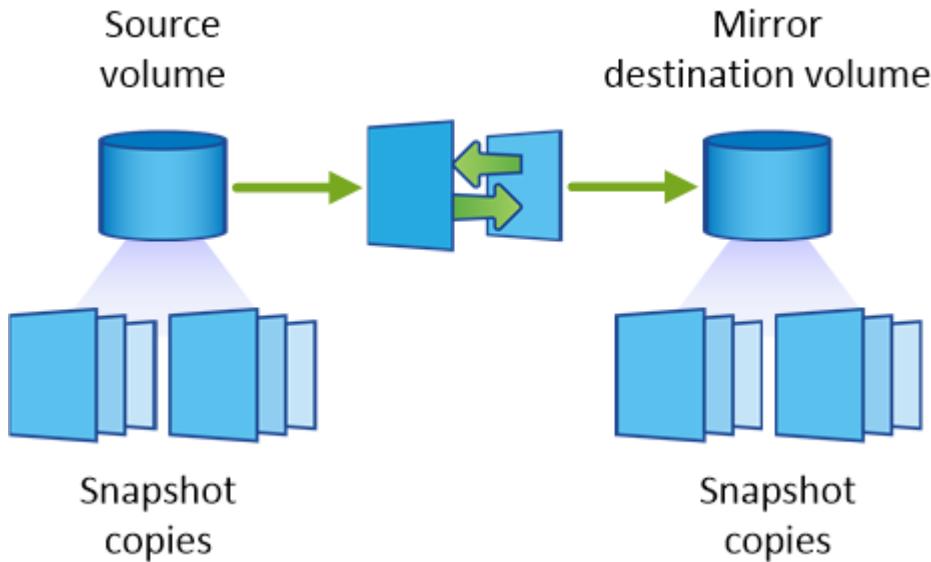
- A *Backup* policy replicates specific Snapshot copies to a destination volume and typically retains them for a longer period of time than you would on the source volume.

You can restore data from these Snapshot copies when data is corrupted or lost, and retain them for standards compliance and other governance-related purposes.

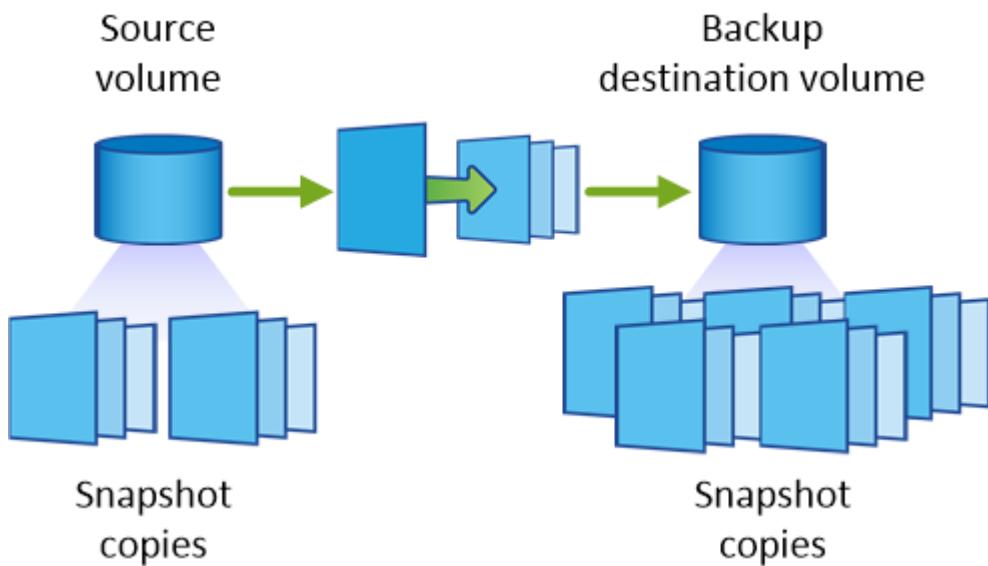
- A *Mirror and Backup* policy provides both disaster recovery and long-term retention.

Each system includes a default Mirror and Backup policy, which works well for many situations. If you find that you need custom policies, you can create your own using System Manager.

The following images show the difference between the Mirror and Backup policies. A Mirror policy mirrors the Snapshot copies available on the source volume.



A Backup policy typically retains Snapshot copies longer than they are retained on the source volume:



## How Backup policies work

Unlike Mirror policies, Backup (SnapVault) policies replicate specific Snapshot copies to a destination volume. It is important to understand how Backup policies work if you want to use your own policies instead of the default policies.

### Understanding the relationship between Snapshot copy labels and Backup policies

A Snapshot policy defines how the system creates Snapshot copies of volumes. The policy specifies when to create the Snapshot copies, how many copies to retain, and how to label them. For example, a system might create one Snapshot copy every day at 12:10 a.m., retain the two most recent copies, and label them "daily".

A Backup policy includes rules that specify which labeled Snapshot copies to replicate to a destination volume and how many copies to retain. The labels defined in a Backup policy must match one or more labels defined in a Snapshot policy. Otherwise, the system cannot replicate any Snapshot copies.

For example, a Backup policy that includes the labels "daily" and "weekly" results in replication of Snapshot

copies that include only those labels. No other Snapshot copies are replicated, as shown in the following image:

#### **Default policies and custom policies**

The default Snapshot policy creates hourly, daily, and weekly Snapshot copies, retaining six hourly, two daily, and two weekly Snapshot copies.

You can easily use a default Backup policy with the default Snapshot policy. The default Backup policies replicate daily and weekly Snapshot copies, retaining seven daily and 52 weekly Snapshot copies.

If you create custom policies, the labels defined by those policies must match. You can create custom policies using System Manager.

## **Data replication from NetApp HCI to Cloud Volumes ONTAP**

If you're trying to replicate data from NetApp HCI to Cloud Volumes ONTAP, you can do so on a NetApp HCI system running NetApp Element software using SnapMirror. Alternatively, you can replicate data on volumes created on an ONTAP Select system running as a virtual guest in a NetApp HCI solution to Cloud Volumes ONTAP.

Refer to the following technical reports for details:

- [Technical Report 4641: NetApp HCI Data Protection](#)
- [Technical Report 4651: NetApp SolidFire SnapMirror Architecture and Configuration](#)

## **Monitor performance**

### **Learn about the Monitoring service**

The Monitoring service gives you insights into the health and performance of your Cloud Volumes ONTAP instances and helps you troubleshoot and optimize the performance of your cloud storage environment.

#### **Features**

- Automatically monitor all volumes
- View volume performance data in terms of IOPS, throughput, and latency
- Identify performance issues to minimize impact on your users and apps

#### **Supported cloud providers**

The Monitoring service is supported with Cloud Volumes ONTAP for AWS and Cloud Volumes ONTAP for Azure.

#### **Cost**

NetApp doesn't charge you for using the Monitoring service, but Cloud Manager launches a virtual machine in your VPC to facilitate monitoring. This VM results in charges from your cloud provider.

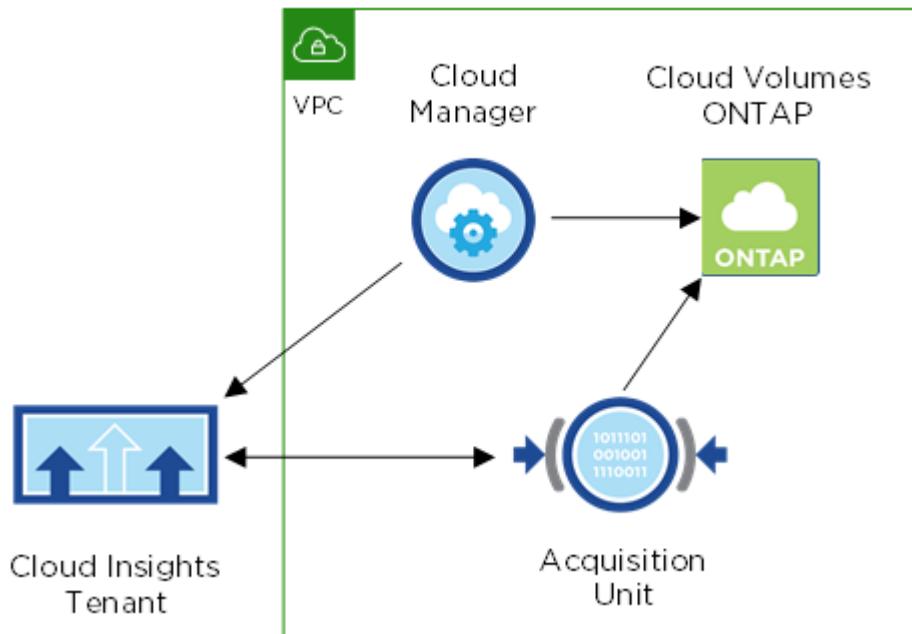
## How the Monitoring service works

Cloud Manager leverages [NetApp's Cloud Insights service](#) to provide monitoring.

At a high-level, Cloud Insights integration with Cloud Manager works like this:

1. You enable the Monitoring service on Cloud Volumes ONTAP.
2. Cloud Manager configures your environment. It does the following:
  - a. Creates a Cloud Insights tenant (also called *environment*) and associates all users in your Cloud Central account to the tenant.
  - b. Enables a 30-day free trial of Cloud Insights.
  - c. Deploys a virtual machine in your VPC/VNet called an Acquisition Unit. The Acquisition Unit facilitates monitoring of volumes (this is the VM mentioned in the Cost section above).
  - d. Connects the Acquisition Unit to Cloud Volumes ONTAP and to the Cloud Insights tenant.
3. In Cloud Manager, you click Monitoring and use the performance data to troubleshoot and optimize performance.

The following image shows the relationship between these components in an AWS VPC:



### The Acquisition Unit

When you enable Monitoring, Cloud Manager deploys an Acquisition Unit in the same subnet as the Connector.

An *Acquisition Unit* collects performance data from Cloud Volumes ONTAP and sends it to the Cloud Insights tenant. Cloud Manager then queries that data and presents it to you.

Note the following about the Acquisition Unit instance:

- In AWS, the Acquisition Unit runs on a t3.xlarge instance with a 100 GB GP2 volume.
- In Azure, the Acquisition Unit runs on a D4\_v3 virtual machine with a 30 GB Standard SSD.
- The instance is named *AcquisitionUnit* with a generated hash (UUID) concatenated to it. For example:

## *AcquisitionUnit-FAN7FqeH*

- Only one Acquisition Unit is deployed per Connector.
- The instance must be running to access performance information in the Monitoring tab.

### **Cloud Insights tenant**

Cloud Manager sets up a *tenant* for you when you enable Monitoring. A Cloud Insights tenant enables you to access the performance data that the Acquisition Unit collects. The tenant is a secure data partition within the NetApp Cloud Insights service.

### **Cloud Insights web interface**

The Monitoring tab in Cloud Manager provides basic performance data for your volumes. You can go to the Cloud Insights web interface from your browser to perform more in-depth monitoring and to configure alerts for your Cloud Volumes ONTAP systems.

### **Free trial and subscription**

Cloud Manager enables a 30-day free trial of Cloud Insights to provide performance data within Cloud Manager and for you to explore the features that Cloud Insights Standard Edition has to offer.

You need to subscribe by the end of the free trial or your Cloud Insights tenant will eventually be deleted. You can subscribe to either the Basic, Standard, or Premium edition to continue using the Monitoring feature within Cloud Manager.

[Learn how to subscribe to Cloud Insights.](#)

## **Monitoring Cloud Volumes ONTAP**

Complete a few steps to start monitoring Cloud Volumes ONTAP performance.

### **Quick start**

Get started quickly by following these steps or scroll down to the remaining sections for full details.



### **Verify support for your configuration**

- You must be a new Cloud Insights customer.
- You need a Cloud Volumes ONTAP system running in AWS or Azure.
- For AWS, you need a Connector running version 3.8.4 or later.
- For Azure, you need a Connector running version 3.9.3 or later.



### **Enable Monitoring on your new or existing system**

- New working environments: Be sure to keep Monitoring enabled when you create the working environment (it's enabled by default).
- Existing working environments: Select a working environment and click **Start Monitoring**.



### 3 View performance data

Click **Monitoring** and view performance data for your volumes.



### 4 Subscribe to Cloud Insights

Subscribe before your 30-day free trial ends to continue seeing performance data within Cloud Manager and Cloud Insights. [Learn how to subscribe](#).

## Requirements

Read the following requirements to make sure that you have a supported configuration.

### Supported Cloud Volumes ONTAP versions

Any version of Cloud Volumes ONTAP in AWS or in Azure.

### Supported Connector

- For AWS, you need a Connector running version 3.8.4 or later.
- For Azure, you need a Connector running version 3.9.3 or later.



You can view a Connector's version by clicking the icon and then **Support > Connector**.

### Cloud Insights requirement

You must be a new Cloud Insights customer. Monitoring isn't supported if you already have a Cloud Insights tenant.

### Email address for Cloud Central

The email address for your Cloud Central user account should be your business email address. Free email domains like gmail and hotmail aren't supported when creating a Cloud Insights tenant.

### Networking for the Acquisition Unit

The Acquisition Unit uses 2-way/mutual authentication to connect to the Cloud Insights server. The client certificate must be passed to the Cloud Insights server to be authenticated. To accomplish this, the proxy must be set up to forward the http request to the Cloud Insights server without decrypting the data.

The Acquisition Unit uses the following two endpoints to communicate with Cloud Insights. If you have a firewall between the Acquisition Unit server and Cloud Insights, you need these endpoints when configuring firewall rules:

```
https://aulogin.<Cloud Insights Domain>
https://<your-tenant-ID>.<Cloud Insights Domain>
```

For example:

```
https://aulogin.c01.cloudinsights.netapp.com  
https://cg0c586a-ee05-45rb-a5ac-  
333b5ae7718d7.c01.cloudinsights.netapp.com
```

Contact us through the in-product chat if you need help identifying your Cloud Insights domain and tenant ID.

### **Networking for the Connector**

Similar to the Acquisition Unit, the Connector must have outbound connectivity to the Cloud Insights tenant. But the endpoint that the Connector contacts is slightly different. It contacts the tenant host URL using the shortened tenant ID:

```
https://<your-short-tenant-ID>.<Cloud Insights Domain>
```

For example:

```
https://abcd12345.c01.cloudinsights.netapp.com
```

Again, you can contact us through the in-product chat if you need help identifying the tenant host URL.

### **Enabling monitoring on a new system**

The Monitoring service is enabled by default in the working environment wizard. Be sure to keep the option enabled.

#### **Steps**

1. Click **Create Cloud Volumes ONTAP**.
2. Select Amazon Web Services or Microsoft Azure as the cloud provider and then choose a single node or HA system.
3. Fill out the Details & Credentials page.
4. On the Services page, leave the Monitoring service enabled and click **Continue**.



## Monitoring



NetApp Monitoring is an infrastructure monitoring tool that gives you visibility into your complete infrastructure. With Monitoring, you can monitor, troubleshoot and optimize all your resources including your public clouds and your private data centers.

### ADVANTAGES

- Automatically monitor all volumes - no configuration is required
- Prevent performance issues from impacting your users and apps

### CLARIFICATIONS

- Activation is free, but requires deploying a small-size cloud instance which will incur charges by your cloud provider
- Monitoring can be disabled at any time

## Enabling monitoring on an existing system

Enable monitoring at any time from the working environment.

### Steps

1. At the top of Cloud Manager, click **Canvas**.
2. Select a working environment.
3. In the pane on the right, click **Start Monitoring**.

The screenshot shows the Cloud Manager interface with the following details:

- CVO2**: Status is **On | AWS**. Action buttons: **i**, **⋮**, **X**.
- SERVICES** section:
  - Cloud Compliance**: Status is **Off**. Action button: **Enable Compliance**.
  - Backup to Cloud**: Status is **On**. Information: **1 Volume Backed Up**. Action button: **⋮**.
  - Kubernetes**: Status is **Off**. Action button: **Activate Kubernetes**.
  - Monitoring**: Status is **Off**. Action button: **Start Monitoring** (with a hand cursor icon).

## Monitoring your volumes

Monitor performance by viewing IOPS, throughput, and latency for each of your volumes.

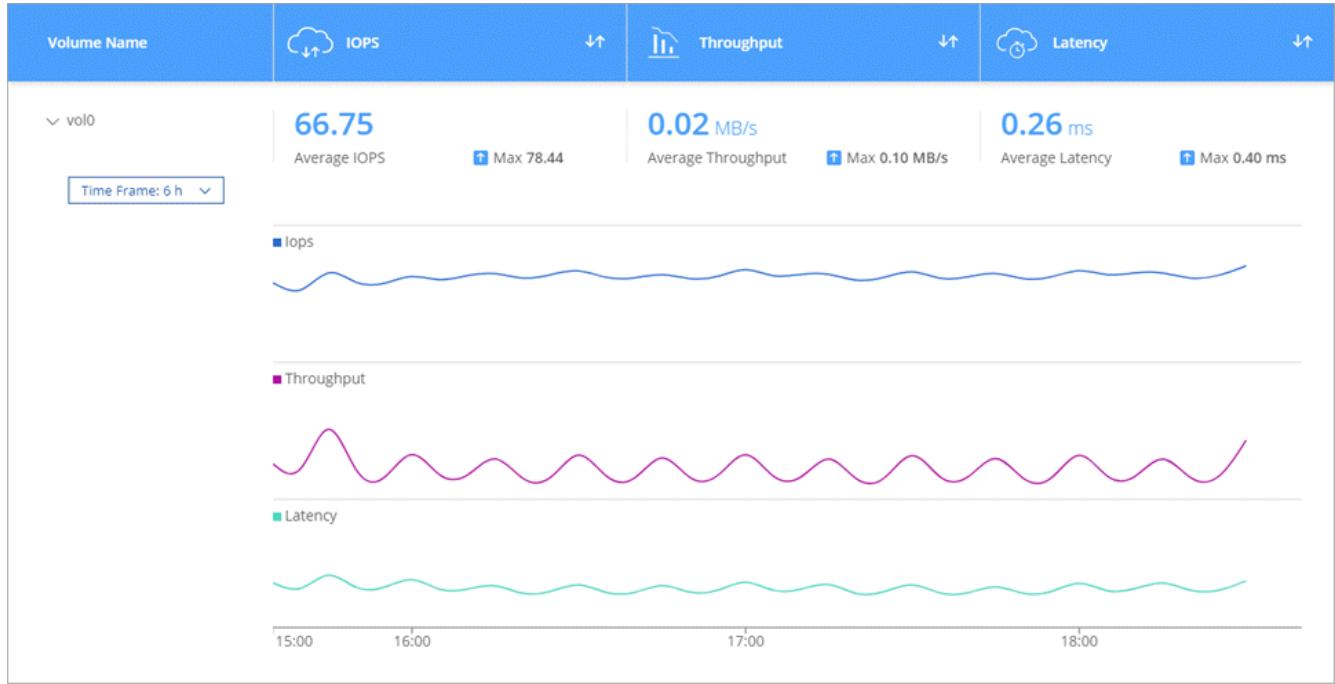
### Steps

1. At the top of Cloud Manager, click **Monitoring**.
2. Filter the contents of the dashboard to get the information that you need.
  - Select a specific working environment.
  - Select a different timeframe.
  - Select a specific SVM.
  - Search for a specific volume.

The following image highlights each of these options:

The screenshot shows the Cloud Manager interface with the 'Monitoring' tab selected. At the top, there are two status cards: '0.02 MB/s Average Network Throughput' and '5.55 % Average CPU Utilization'. Below these are two volume entries: 'vol0' with IOPS of 66.75, throughput of 0.02 MB/s, and latency of 0.26 ms; and 'volaws2' with IOPS of 50.02, throughput of 12.60 MB/s, and latency of 0.19 ms. A search bar and a 'Time Frame: 6 h' dropdown are also visible.

- Click a volume in the table to expand the row and view a timeline for IOPS, throughput, and latency.



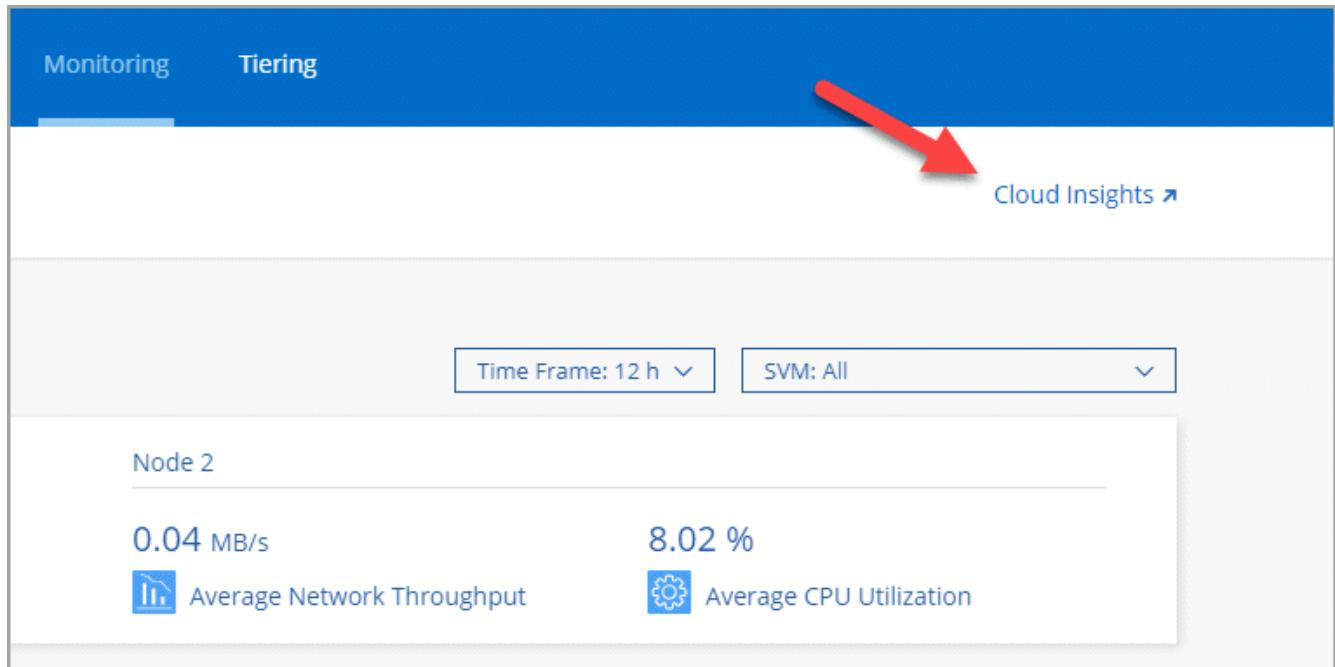
- Use the data to identify performance issues to minimize impact on your users and apps.

## Getting more information from Cloud Insights

The Monitoring tab in Cloud Manager provides basic performance data for your volumes. You can go to the Cloud Insights web interface from your browser to perform more in-depth monitoring and to configure alerts for your Cloud Volumes ONTAP systems.

### Steps

- At the top of Cloud Manager, click **Monitoring**.
- Click the **Cloud Insights** link.



## Result

Cloud Insights open in a new browser tab. If you need help, refer to the [Cloud Insights documentation](#).

## Disabling monitoring

If you no longer want to monitor Cloud Volumes ONTAP, you can disable the service at any time.



If you disable monitoring from each of your working environments, you'll need to delete the virtual machine instance yourself. The instance is named *AcquisitionUnit* with a generated hash (UUID) concatenated to it. For example: *AcquisitionUnit-FAN7FqeH*

## Steps

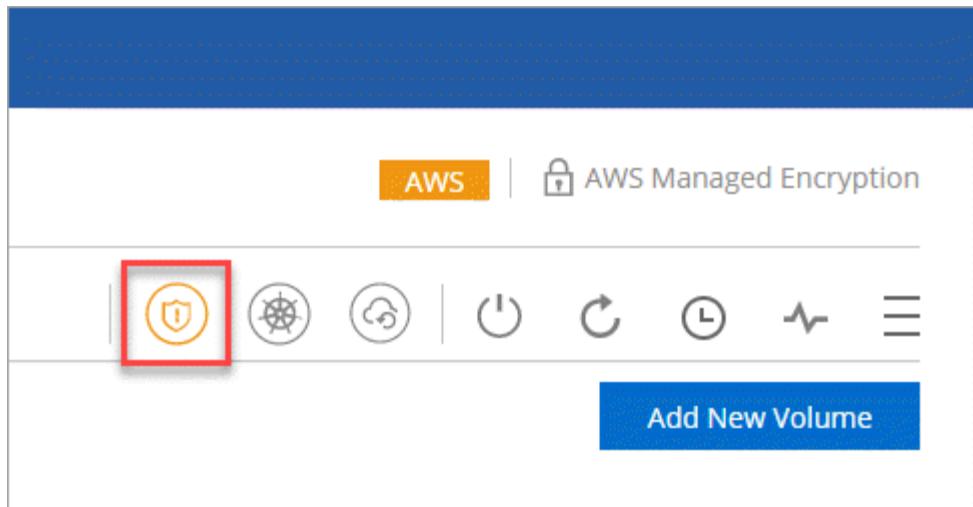
1. At the top of Cloud Manager, click **Canvas**.
2. Select a working environment.
3. In the pane on the right, click the icon and select **Deactivate Scan**.

## 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.

## Steps

1. From the working environment, click the **Ransomware** icon.



## 2. Implement the NetApp solution for ransomware:

- 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.

- 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 screenshot shows the 'Ransomware Protection' page. It has two main sections:

- 1 Enable Snapshot Copy Protection**: Shows a progress circle at 50% Protection. Below it, a message says "1 Volumes without a Snapshot Policy". A button to "Activate Snapshot Policy" is present.
- 2 Block Ransomware File Extensions**: Shows a shield icon with a file. Below it, a message says "ONTAP's native FPolicy configuration monitors and blocks file operations based on a file's extension". Buttons for "View Denied File Names" and "Activate FPolicy" are shown.

## Administer

### Registering pay-as-you-go systems

Support from NetApp is included with Cloud Volumes ONTAP Explore, Standard, and Premium 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.



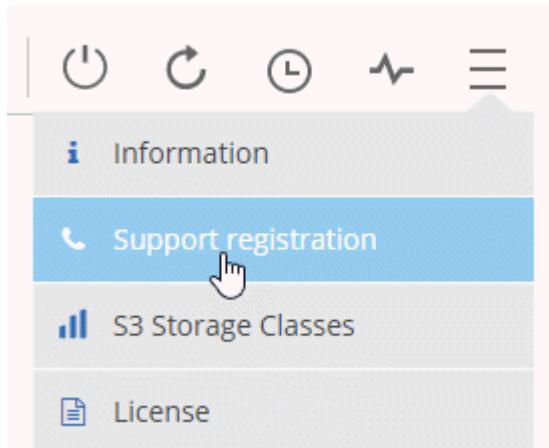
A system that isn't registered for support will still receive the software update notifications that appear in Cloud Manager when a new version is available. But you will need to register the system before you can upgrade the software.

### 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**:



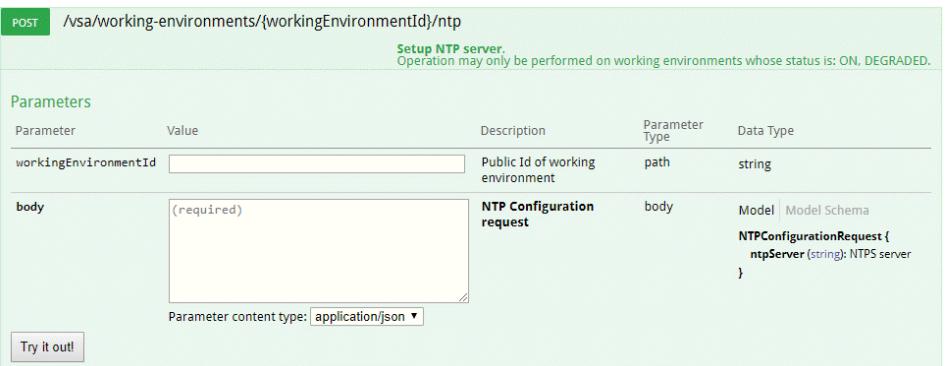
4. Select a NetApp Support Site account and click **Register**.

### Result

Cloud Manager registers the system with NetApp.

## Setting up Cloud Volumes ONTAP

After you deploy Cloud Volumes ONTAP, you can set it up by synchronizing the system time using NTP and by performing a few optional tasks from either System Manager or the CLI.

Task	Description
<p>Synchronize the system time using NTP</p>	<p>Specifying an NTP server synchronizes the time between the systems in your network, which can help prevent issues due to time differences.</p> <p>Specify an NTP server using the Cloud Manager API or from the user interface when you set up a CIFS server.</p> <ul style="list-style-type: none"> <li>• <a href="#">Modifying the CIFS server</a></li> <li>• <a href="#">Cloud Manager API Developer Guide</a></li> </ul> <p>For example, here's the API for a single-node system in AWS:</p>  <pre> POST /vsa/working-environments/{workingEnvironmentId}/ntp  Setup NTP server. Operation may only be performed on working environments whose status is: ON, DEGRADED.  Parameters Parameter Value Description Parameter Type Data Type workingEnvironmentId [ ] Public Id of working environment path string body (required) NTP Configuration request body Model&lt;NTPConfigurationRequest&gt; NTPConfigurationRequest {   ntpServer(string): NTPs server }  Parameter content type: application/json ▾ Try it out! </pre>
<p>Optional: Configure AutoSupport</p>	<p>AutoSupport proactively monitors the health of your system and automatically sends messages to NetApp technical support by default.</p> <p>If the Account Admin added a proxy server to Cloud Manager before you launched your instance, Cloud Volumes ONTAP is configured to use that proxy server for AutoSupport messages.</p> <p>You should test AutoSupport to ensure that it can send messages. For instructions, see the System Manager Help or the <a href="#">ONTAP 9 System Administration Reference</a>.</p>
<p>Optional: Configure the Cloud Manager Connector as the AutoSupport proxy</p>	<p>If your environment requires a proxy server to send AutoSupport messages, you can configure the Connector to act as the proxy. No configuration for the Connector is required, other than internet access. You simply need to go to the CLI for Cloud Volumes ONTAP and run the following command:</p> <pre>system node autosupport modify -proxy-url &lt;connector-ip-address&gt;</pre>
<p>Optional: Configure EMS</p>	<p>The Event Management System (EMS) collects and displays information about events that occur on Cloud Volumes 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.</p> <p>You can configure EMS using the CLI. For instructions, see the <a href="#">ONTAP 9 EMS Configuration Express Guide</a>.</p>

Task	Description
Optional: Change the backup location of configuration files	<p>Cloud Volumes ONTAP automatically creates configuration backup files that contain information about the configurable options that it needs to operate properly.</p> <p>By default, Cloud Volumes ONTAP backs up the files to the Connector host every eight hours. If you want to send the backups to an alternate location, you can change the location to an FTP or HTTP server in your data center or in AWS. For example, you might already have a backup location for your FAS storage systems.</p> <p>You can change the backup location using the CLI. See the <a href="#">ONTAP 9 System Administration Reference</a>.</p>

## Managing BYOL licenses for Cloud Volumes ONTAP

Add a Cloud Volumes ONTAP BYOL system license to add additional capacity, update an existing system license, and manage BYOL licenses for Cloud Backup.

### Managing system licenses

You can purchase multiple licenses for a Cloud Volumes ONTAP BYOL system to allocate more than 368 TB of capacity. For example, you might purchase two licenses to allocate up to 736 TB of capacity to Cloud Volumes ONTAP. Or you could purchase four licenses to get up to 1.4 PB.

The number of licenses that you can purchase for a single node system or HA pair is unlimited.

### Obtaining 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](http://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.

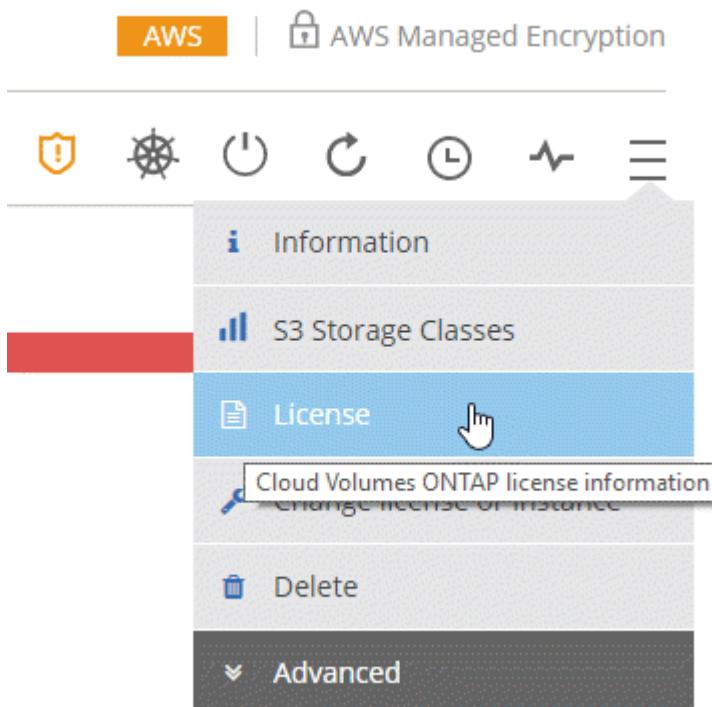
### Adding a new system license

Add a new BYOL system license at any time to allocate an additional 368 TB of capacity to your Cloud Volumes ONTAP BYOL system.

### Steps

1. In Cloud Manager, open the Cloud Volumes ONTAP BYOL working environment.

2. Click the menu icon and then click **License**.



3. Click **Add CVO System License**.

A screenshot of the "BYOL Licenses" page. At the top, it shows "1 Cloud Volumes ONTAP System License | 0 Backup License". There are two buttons: "Add CVO System License" and "Add Backup License". Below this is a card for a "Cloud Volumes ONTAP System License". It includes a circular icon with a document, the text "Cloud Volumes ONTAP System License", "License Type", "Platform Serial Number: 90820", and "Update CVO System License". A note at the bottom says "① License Expired: August 01, 2020".

4. Choose to enter the serial number or to upload the license file.

5. Click **Add License**.

## Result

Cloud Manager installs the new license file on the Cloud Volumes ONTAP system.

### Updating 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. In Cloud Manager, open the Cloud Volumes ONTAP BYOL working environment.
2. Click the menu icon and then click **License**.

### 3. Click **Update CVO System License**.

The screenshot shows the 'BYOL Licenses' section of the Cloud Manager interface. At the top, it displays '1 Cloud Volumes ONTAP System License | 0 Backup License'. Below this, there's a card for the 'Cloud Volumes ONTAP System License' with a 'License Type' icon (a document with a lock). The card also shows 'Platform Serial Number: 90820' and a note that the license is 'Expired: August 01, 2020'. At the top right of the card is a blue button labeled 'Update CVO System License'. Above the card, there are two other buttons: 'Add CVO System License' and 'Add Backup License'.

4. Click **Upload File** and select the license file.

5. Click **Update License**.

### Result

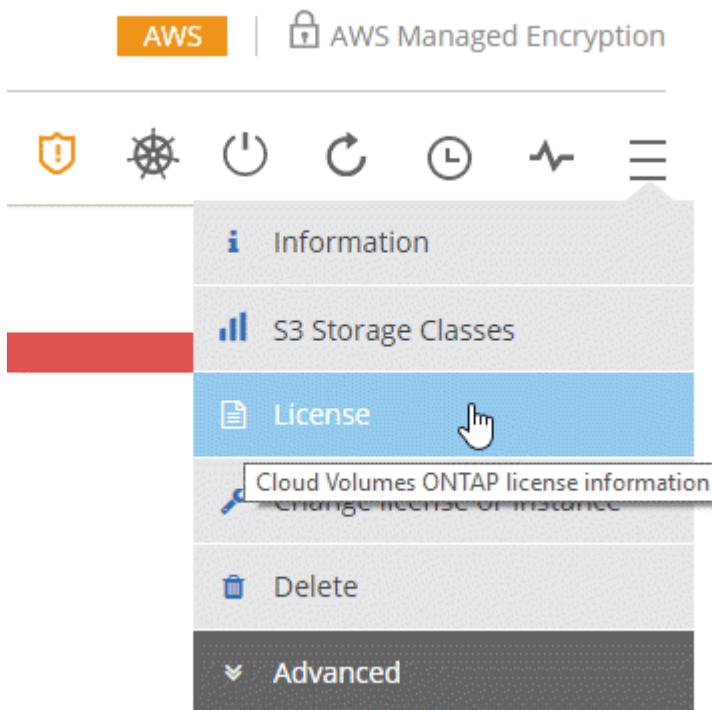
Cloud Manager updates the license on the Cloud Volumes ONTAP system.

### Adding and updating your Backup BYOL license

You use the BYOL Licenses page to add or update your Backup BYOL license.

### Steps

1. In Cloud Manager, open the Cloud Volumes ONTAP BYOL working environment.
2. Click the menu icon and then click **License**.



3. Click **Add Backup License** or **Update Backup License** depending on whether you are adding a new license or updating an existing license.

## Total License Information

Instance Type:	m5.2xlarge	Total Attached EBS Capacity :	200 TB	Total Used Tiering Capacity:	60 TB
Total License Limit :	368 TB 	Total Used EBS Capacity :	180 TB	Total Allocated ONTAP Capacity :	100 TB
Total Backup Capacity Limit :	368 TB	Total Used Backup Capacity :	200 TB		

## BYOL Licenses

1 Cloud Volumes ONTAP System License | 1 Backup License

Add CVO System License

Add Backup License 



Cloud Volumes ONTAP System License

License Type

Update CVO System License

Platform Serial Number Node 1: 9012013000000000000020

License Expiry: April 10, 2021

Platform Serial Number Node 2: 9012013000000000000021

License Expiry: April 10, 2021



Backup License

License Type

Update Backup License 

Platform Serial Number: 90120130000000000022

License Expiry: April 10, 2021

License Capacity Limit: 368 TB (Used Capacity 200 TB)

#### 4. Enter the license information and click **Add License**:

- If you have the serial number, select the **Enter Backup BYOL Serial Number** option and enter the serial number.
- If you have the backup license file, select the **Upload Backup BYOL License** option and follow the prompts to attach the file.

### Add Backup License

A Backup license enables Backup to Cloud for a certain period of time and for a maximum amount backup space.

Enter Backup BYOL Serial Number    Upload Backup BYOL License

Enter Backup BYOL Serial Number

**Add License**   **Cancel**

## Result

Cloud Manager adds or updates the license so that your Cloud Backup service is active.

## Upgrading Cloud Volumes ONTAP software

Cloud Manager includes several options that you can use to upgrade to the current Cloud

Volumes ONTAP release. You should prepare Cloud Volumes ONTAP systems before you upgrade the software.

## Requirements

You should be aware of the following requirements before you start the Cloud Volumes ONTAP upgrade process.

### Software upgrades must be completed by Cloud Manager

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.

### Cloud Volumes ONTAP must be registered with NetApp Support

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.

### A note about downgrades

Cloud Manager doesn't support downgrading Cloud Volumes ONTAP to a previous version. Contact NetApp technical support for help with downgrades.

## Ways to upgrade Cloud Volumes ONTAP

Cloud Manager displays a notification in Cloud Volumes ONTAP working environments when a new version of Cloud Volumes ONTAP is available:

The screenshot shows the Cloud Manager dashboard. At the top, there's a cloud icon and the text "Visual View". Below it, a system card for "cloudvolumesontap1" is displayed, indicating it is "On | AWS". The card has three icons: a blue circle with a white "i", a grey circle with three dots, and a grey circle with an "X". Underneath the card, a red box highlights the "NOTIFICATIONS" section. Inside this section, a blue star icon is followed by the text "New version available" and a small grey arrow icon. The "SERVICES" section follows, featuring a "Cloud Compliance" card with a blue cloud icon containing a lock, the text "Cloud Compliance", "On", and a green checkmark icon with the text "No Personal Files Found".

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. For details, see [Upgrading Cloud Volumes ONTAP from Cloud Manager notifications](#).



For HA systems in AWS, Cloud Manager might upgrade the HA mediator as part of the upgrade process.

Cloud Manager also provides the following advanced options for upgrading Cloud Volumes ONTAP software with both PAYGO and BYOL:

- Software upgrades 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 [Upgrading Cloud Volumes ONTAP by using an HTTP or FTP server](#).

- Software upgrades using the alternate image on the system

You can use this option to upgrade by making the alternate software image the default image. This option is not available for HA pairs.

For details, see [Upgrading Cloud Volumes ONTAP by using a local image](#).

## Preparing to upgrade Cloud Volumes ONTAP software

Before performing an upgrade, you must verify that your systems are ready and make any required configuration changes.

- Understanding supported upgrade paths
- Planning for downtime
- Verifying that automatic giveback is still enabled
- Suspending SnapMirror transfers
- Verifying that aggregates are online

#### **Understanding supported upgrade paths**

You need to upgrade Cloud Volumes ONTAP by one release at a time. You can't upgrade by skipping a release.

For example, if you're currently running Cloud Volumes ONTAP 9.6 and you want to upgrade to 9.8, then you first need to upgrade to 9.7. From there, you can upgrade to 9.8.

Refer to the "Upgrade notes" in the [Cloud Volumes ONTAP Release Notes](#) for more details.

#### **Planning 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.

#### **Verifying 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](#)

#### **Suspending 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.

#### **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.
2. Click **Protection > Relationships**.
3. Select the relationship and click **Operations > Quiesce**.

#### **Verifying 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.

The screenshot shows a detailed view of an aggregate named 'aggr1'. The aggregate has a capacity of 88.57 GB and is currently using 1.07 GB. It contains 2 volumes and 1 AWS disk. The 'State' field is explicitly labeled as 'online' and is highlighted with a red rectangular border.

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. [Log in to System Manager](#).
  - b. Click **Storage > Aggregates & Disks > Aggregates**.
  - c. Select the aggregate, and then click **More Actions > Status > Online**.

## Upgrading Cloud Volumes ONTAP from Cloud Manager notifications

Cloud Manager notifies you when a new version of Cloud Volumes ONTAP is available. Click the notification to start the upgrade process.

### Before you begin

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

## Steps

1. Click **Canvas**.
2. Select a working environment.

A notification appears in the right pane if a new version is available:

The screenshot shows the Cloud Manager interface. At the top, there's a cloud icon and the text "Visual View". Below that, a card for "cloudvolumesontap1" is shown, indicating it's "On | AWS". The main area has two sections: "NOTIFICATIONS" and "SERVICES". The "NOTIFICATIONS" section has a red border around it and contains a message: "★ New version available". The "SERVICES" section contains a card for "Cloud Compliance" which is "On" and shows "No Personal Files Found".

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.

## Upgrading Cloud Volumes ONTAP by using an HTTP or FTP server

You can place the Cloud Volumes ONTAP software image on an HTTP or FTP 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.

## Steps

1. Set up an HTTP server or FTP server that can host the Cloud Volumes ONTAP software image.
2. If you have a VPN connection to the virtual network, you can place the Cloud Volumes ONTAP software image on an HTTP server or FTP server in your own network. Otherwise, you must place the file on an HTTP server or FTP server in the cloud.
3. If you use your own security group for Cloud Volumes ONTAP, ensure that the outbound rules allow HTTP or FTP connections so Cloud Volumes ONTAP can access the software image.



The predefined Cloud Volumes ONTAP security group allows outbound HTTP and FTP connections by default.

4. Obtain the software image from [the NetApp Support Site](#).
5. Copy the software image to the directory on the HTTP or FTP server from which the file will be served.
6. From the working environment in Cloud Manager, click the menu icon, and then click **Advanced > Update Cloud Volumes ONTAP**.
7. On the update software page, choose **Select an image available from a URL**, enter the URL, and then click **Change Image**.
8. 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.

## Upgrading Cloud Volumes ONTAP by using a local image

Each Cloud Volumes ONTAP system can hold two software images: the current image that is running, and an alternate image that you can boot. Cloud Manager can change the alternate image to be the default image.

### Steps

1. From the working environment, click the menu icon, and then click **Advanced > Update Cloud Volumes ONTAP**.
2. On the update software page, select the alternate image, and then click **Change Image**.
3. 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.

## Modifying Cloud Volumes ONTAP systems

You might need to change the configuration of Cloud Volumes ONTAP systems as your storage needs change. For example, you can change between pay-as-you-go configurations, change the instance or VM type, and more.

### Changing the instance or machine type for Cloud Volumes ONTAP

You can choose from several instance or machine types when you launch Cloud Volumes ONTAP in AWS, Azure, or GCP. 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 instance or machine type affects cloud provider 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

- From the working environment, click the menu icon, and then click **Change license or instance** for AWS, **Change license or VM** for Azure, or **Change license or machine** for GCP.
- If you are using a pay-as-you-go configuration, you can optionally choose a different license.
- Select an instance or 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.

### Changing between pay-as-you-go configurations

After you launch pay-as-you-go Cloud Volumes ONTAP systems, you can change between the Explore, Standard, and Premium configurations at any time by modifying the license. Changing the license increases or decreases the raw capacity limit and enables you to choose from different AWS instance types or Azure virtual machine types.



In GCP, a single machine type is available for each pay-as-you-go configuration. You can't choose between different machine types.

### About this task

Note the following about changing between pay-as-you-go licenses:

- 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.

- Changing the instance or machine type affects cloud provider service charges.

### Steps

- From the working environment, click the menu icon, and then click **Change license or instance** for AWS,

**Change license or VM** for Azure, or **Change license or machine** for GCP.

2. Select a license type and an instance type or 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 license, instance type or machine type, or both.

## Moving to an alternate Cloud Volumes ONTAP configuration

If you want to switch between a pay-as-you-go subscription and a BYOL subscription or between a single Cloud Volumes ONTAP system and an HA pair, then you need to deploy a new system and then replicate data from the existing system to the new system.

## Steps

1. Create a new Cloud Volumes ONTAP working environment.

[Launching Cloud Volumes ONTAP in AWS](#)

[Launching Cloud Volumes ONTAP in Azure](#)

[Launching Cloud Volumes ONTAP in GCP](#)

2. [Set up one-time data replication](#) between the systems for each volume that you must replicate.
3. Terminate the Cloud Volumes ONTAP system that you no longer need by [deleting the original working environment](#).

## Changing write speed to normal or high

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. It's also supported with HA pairs in AWS and Azure when using a specific instance or VM type ([click here to see the list of supported instances and VM types](#)). High write speed is not supported with HA pairs in GCP.

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 Cloud Volumes ONTAP.

## 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**.

## Modifying the storage VM name

Cloud Manager automatically names the single storage VM (SVM) that it creates for Cloud Volumes ONTAP. You can modify the name of the SVM if you have strict naming standards. For example, you might want the name to match how you name the SVMs for your ONTAP clusters.

But if you created any additional SVMs for Cloud Volumes ONTAP, then you can't rename the SVMs 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.

The screenshot shows the 'Working Environment Information' page for an ONTAP system. The page lists the following details:

ONTAP	
Serial Number:	[REDACTED]
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**.

## Changing 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.

## Changing the network MTU for c4.4xlarge and c4.8xlarge instances

By default, Cloud Volumes ONTAP is configured to use 9,000 MTU (also called jumbo frames) when you choose the c4.4xlarge instance or the c4.8xlarge instance in AWS. You can change the network MTU to 1,500 bytes if that is more appropriate for your network configuration.

### About this task

A network maximum transmission unit (MTU) of 9,000 bytes can provide the highest maximum network throughput possible for specific configurations.

9,000 MTU is a good choice if clients in the same VPC communicate with the Cloud Volumes ONTAP system and some or all of those clients also support 9,000 MTU. If traffic leaves the VPC, packet fragmentation can occur, which degrades performance.

A network MTU of 1,500 bytes is a good choice if clients or systems outside of the VPC communicate with the Cloud Volumes ONTAP system.

### Steps

1. From the working environment, click the menu icon and then click **Advanced > Network Utilization**.
2. Select **Standard or Jumbo Frames**.
3. Click **Change**.

## Changing route tables associated with HA pairs in multiple AWS AZs

You can modify the AWS route tables that include routes to the floating IP addresses for an HA pair. You might do this if new NFS or CIFS clients need to access an HA pair in AWS.

### Steps

1. From the working environment, click the menu icon and then click **Information**.
2. Click **Route Tables**.
3. Modify the list of selected route tables and then click **Save**.

### Result

Cloud Manager sends an AWS request to modify the route tables.

## 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.

## 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)
<hr/>								
<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.

### 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.

## Monitoring AWS resource costs

Cloud Manager enables you to view the resource costs associated with running Cloud Volumes ONTAP in AWS. You can also see how much money you saved by using NetApp features that can reduce storage costs.

### About this task

Cloud Manager updates the costs when you refresh the page. You should refer to AWS for final cost details.

### Step

1. Verify that Cloud Manager can obtain cost information from AWS:

- a. Ensure that the IAM policy that provides Cloud Manager with permissions includes the following actions:

```
"ce:GetReservationUtilization",
"ce:GetDimensionValues",
"ce:GetCostAndUsage",
"ce:GetTags"
```

These actions are included in the latest [Cloud Manager policy](#). New systems deployed from NetApp Cloud Central automatically include these permissions.

- b. [Activate the \*\*WorkingEnvironmentId\*\* tag](#).

To track your AWS costs, Cloud Manager assigns a cost allocation tag to Cloud Volumes ONTAP instances. After you create your first working environment, activate the **WorkingEnvironmentId** tag. User-defined tags don't appear on AWS billing reports until you activate them in the Billing and Cost Management console.

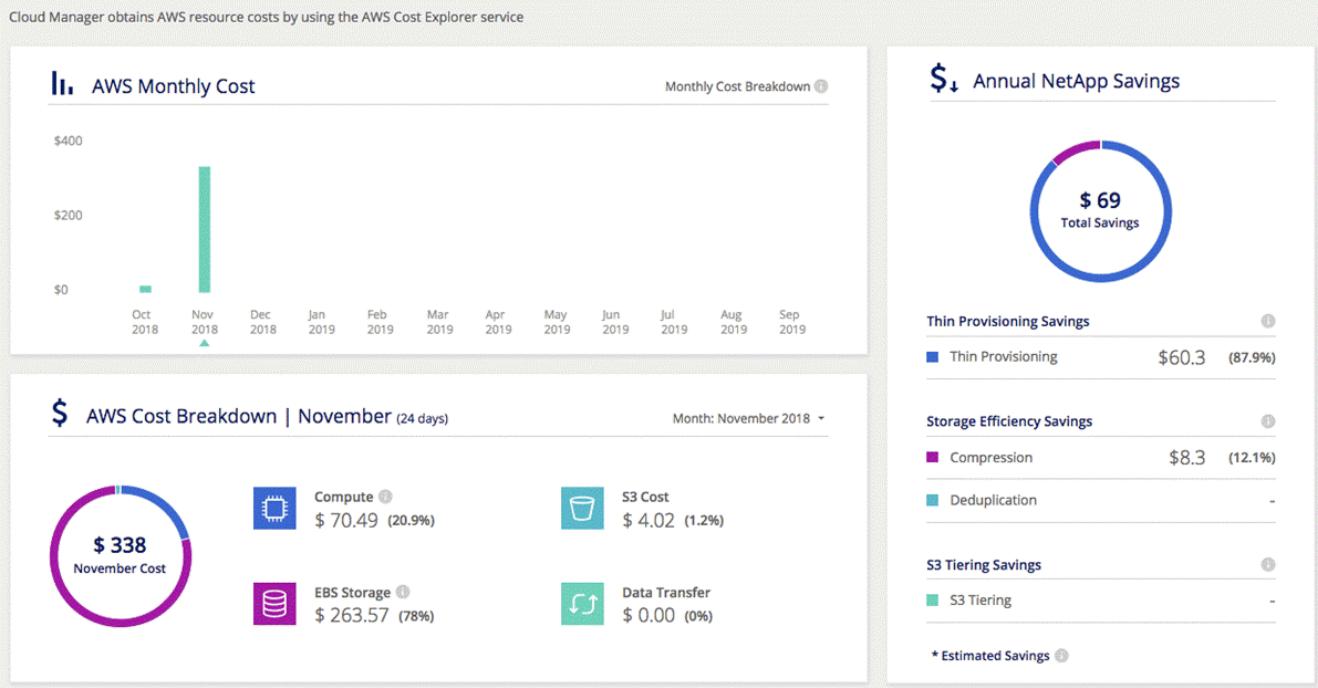
2. On the Canvas page, select a Cloud Volumes ONTAP working environment and then click **Cost**.

The Cost page displays costs for the current and previous months and shows your annual NetApp savings, if you enabled NetApp's cost-saving features on volumes.

The following image shows a sample Cost page:

## AWS Resource Costs

[Learn how we calculate the costs and savings](#)



## Connecting to Cloud Volumes ONTAP

If you need to perform advanced management of Cloud Volumes ONTAP, you can do so using OnCommand System Manager or the command line interface.

### Connecting to System Manager

You might need to perform some Cloud Volumes ONTAP tasks from System Manager, which is a browser-based management tool that runs on the Cloud Volumes ONTAP system. For example, you need to use System Manager if you want to create LUNs.

#### Before you begin

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 in AWS or Azure.



When deployed in multiple AWS Availability Zones, Cloud Volumes ONTAP HA configurations use a floating IP address for the cluster management interface, which means external routing is not available. You must connect from a host that is part of the same routing domain.

### Steps

- From the Canvas page, double-click the Cloud Volumes ONTAP system that you want to manage with System Manager.
  - Click the menu icon, and then click **Advanced > System Manager**.
  - Click **Launch**.
- System Manager loads in a new browser tab.
- At the login screen, enter **admin** in the User Name field, enter the password that you specified when you created the working environment, and then click **Sign In**.

## Result

The System Manager console loads. You can now use it to manage Cloud Volumes ONTAP.

## Connecting to the Cloud Volumes ONTAP CLI

The Cloud Volumes ONTAP CLI enables you to execute 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 use SSH from a jump host in AWS or Azure.



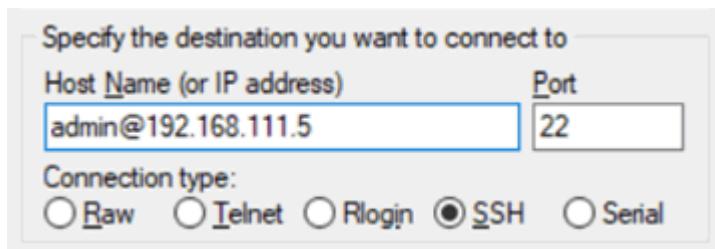
When deployed in multiple AZs, Cloud Volumes ONTAP HA configurations use a floating IP address for the cluster management interface, which means external routing is not available. You must connect from a host that is part of the same routing domain.

### Steps

1. In 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.

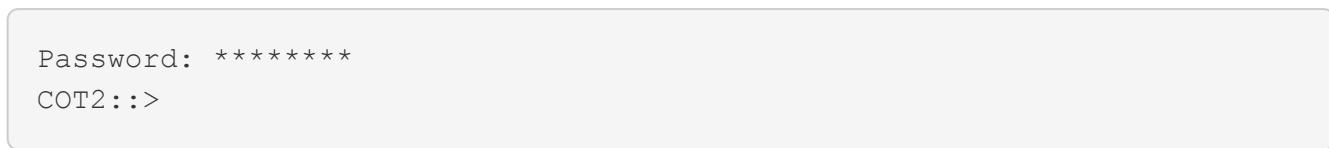
### Example

The following image shows an example using PuTTY:



3. At the login prompt, enter the password for the admin account.

### Example



## 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.

The screenshot shows the 'Define Your Working Environment' page. It features three main options:

- Cloud Volumes ONTAP** (Single Node): Selected, indicated by a blue border and a checkmark icon. [Learn More](#)
- Cloud Volumes ONTAP HA** (High Availability): [Learn More](#)
- Cloud Volumes Service** (High Availability): [Learn More](#)

A message below states: "You're about to create a new Cloud Volumes ONTAP system in AWS." A red box highlights a link: "If you want to discover an existing Cloud Volumes ONTAP in AWS, [click here](#)".

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.

## Overriding CIFS locks for Cloud Volumes ONTAP HA in Azure

The Account Admin can enable a setting in Cloud Manager that prevents issues with Cloud Volumes ONTAP storage failover during Azure maintenance events. When you enable this setting, Cloud Volumes ONTAP vetoes CIFS locks and resets active CIFS sessions.

### About this task

Microsoft Azure schedules periodic maintenance events on its virtual machines. When a maintenance event occurs on a node in a Cloud Volumes ONTAP HA pair, the HA pair initiates storage takeover. If there are active CIFS sessions during this maintenance event, the locks on CIFS files can prevent storage failover.

If you enable this setting, Cloud Volumes ONTAP will veto the locks and reset the active CIFS sessions. As a result, the HA pair can complete storage failover during these maintenance events.



This process might be disruptive to CIFS clients. Data that is not committed from CIFS clients could be lost.

## What you'll need

You need to create a Connector before you can change Cloud Manager settings. [Learn how](#).

### Steps

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



2. Under **HA CIFS Locks**, select the checkbox and click **Save**.

## Using an Azure Private Link with Cloud Volumes ONTAP

By default, Cloud Manager enables an Azure Private Link connection between Cloud Volumes ONTAP and its associated storage accounts. A Private Link secures connections between endpoints in Azure and provides performance benefits. [Learn more](#).

In most cases, there's nothing that you need to do—Cloud Manager manages the Azure Private Link for you. But if you use Azure Private DNS, then you'll need to edit a configuration file. You can also disable the Private Link connection, if desired.

### Providing Cloud Manager with details about your Azure Private DNS

If you use [Azure Private DNS](#), then you need to modify a configuration file on each Connector. Otherwise, Cloud Manager can't enable the Azure Private Link connection between Cloud Volumes ONTAP and its associated storage accounts.

Note that the DNS name must match Azure DNS naming requirements [as shown in Azure documentation](#).

### Steps

1. SSH to the Connector host and log in.
2. Navigate to the following directory: /opt/application/netapp/cloudmanager
3. Edit app.conf by modifying the following parameter as shown:

```
"user-private-dns-zone-settings": {  
    "use-existing": true,  
    "resource-group": "<resource group name of the DNS zone>"  
}
```

4. Save the file and log off the Connector.

A reboot isn't required.

## Disabling Azure Private Link connections

If required for your Azure configuration, you can disable the Azure Private Link connection between Cloud Volumes ONTAP and storage accounts.

### Steps

1. In the upper right of the Cloud Manager console, click the Settings icon, and select **Cloud Manager Settings**.
2. Under Azure Cloud Volumes ONTAP Configuration, deselect **Private Link connection between Cloud Volumes ONTAP and storage accounts**.
3. Click **Save**.

## Deleting a Cloud Volumes ONTAP working environment

It is best to 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 AWS, then you can't use the license key for another instance. You must delete the working environment from Cloud Manager to release the license.

### About this task

When you delete a working environment, Cloud Manager terminates instances, deletes disks, and snapshots.



Cloud Volumes ONTAP instances have termination protection enabled to help prevent accidental termination from AWS. However, if you do terminate a Cloud Volumes ONTAP instance from AWS, you must go to the AWS CloudFormation console and delete the instance's stack. The stack name is the name of the working environment.

### Steps

1. From the working environment, click menu icon and then click **Delete**.
2. Type the name of the working environment and then click **Delete**.

It can take up to 5 minutes to delete the working environment.

# Provision volumes using a file service

## Azure NetApp Files

### Learn about Azure NetApp Files

Azure NetApp Files enables enterprises to migrate and run their performance-intensive and latency-sensitive core, business-critical applications in Azure with no need to refactor for the cloud.

### Features

- Support for multiple protocols enables "lift & shift" of both Linux & Windows applications to run seamlessly in Azure.
- Multiple performance tiers allow for close alignment with workload performance requirements.
- Leading certifications including SAP HANA, GDPR, and HIPPA enables migration of the most demanding workloads to Azure.

### Additional features in Cloud Manager

- Migrate NFS or SMB data to Azure NetApp Files directly from Cloud Manager. Data migrations are powered by NetApp's Cloud Sync service. [Learn more](#).
- Using Artificial Intelligence (AI) driven technology, Cloud Compliance can help you understand data context and identify sensitive data that resides in your Azure NetApp Files accounts. [Learn more](#).

### Cost

[View Azure NetApp Files pricing](#).

Note that your subscription and charging are maintained by the Azure NetApp Files service and not by Cloud Manager.

### Supported regions

[View supported Azure regions](#).

### Requesting access

You need to be granted access to Azure NetApp Files by [submitting an online request](#). You'll need to wait for approval from the Azure NetApp Files team before you can proceed.

### Getting help

For technical support issues associated with Azure NetApp Files, use the Azure portal to log a support request to Microsoft. Select your associated Microsoft subscription and select the **Azure NetApp Files** service name under **Storage**. Provide the remaining information required to create your Microsoft support request.

For issues related to Cloud Sync and Azure NetApp Files, you can start with NetApp using your Cloud Sync serial number directly from the Cloud Sync service. You will need to access the Cloud Sync service through the link in Cloud Manager. [View the process to enable Cloud Sync support](#).

## Related links

- [NetApp Cloud Central: Azure NetApp Files](#)
- [Azure NetApp Files documentation](#)
- [Cloud Sync documentation](#)

## Setting up Azure NetApp Files

Create an Azure NetApp Files working environment in Cloud Manager to create and manage NetApp accounts, capacity pools, volumes, and snapshots.

### Quick start

Get started quickly by following these steps or scroll down to the remaining sections for full details.



### Request access

Submit an [online request](#) to be granted access to Azure NetApp Files.



### Set up an Azure AD application

From Azure, grant permissions to an Azure AD application and copy the application (client) ID, the directory (tenant) ID, and the value of a client secret.



### Create an Azure NetApp Files working environment

In Cloud Manager, click **Add Working Environment > Microsoft Azure > Azure NetApp Files** and then provide details about the AD application.

### Requesting access

You need to be granted access to Azure NetApp Files by [submitting an online request](#). You'll need to wait for approval from the Azure NetApp Files team before you can proceed.

### Setting up an Azure AD application

Cloud Manager needs permissions to set up and manage Azure NetApp Files. You can grant the required permissions to an Azure account by creating and setting up an Azure AD application and by obtaining the Azure credentials that Cloud Manager needs.

#### Creating the AD application

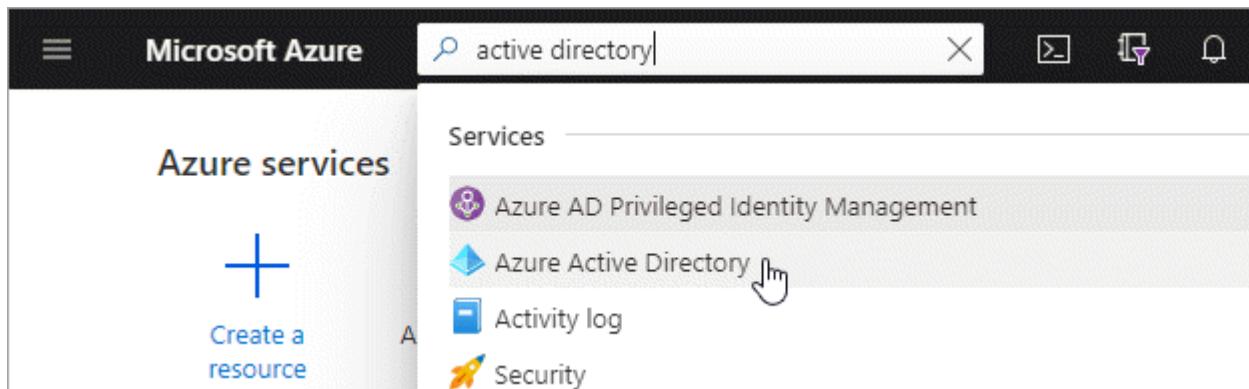
Create an Azure Active Directory (AD) application and service principal that Cloud Manager can use for role-based access control.

#### Before you begin

You must have the right permissions in Azure to create an Active Directory application and to assign the application to a role. For details, refer to [Microsoft Azure Documentation: Required permissions](#).

## Steps

1. From the Azure portal, open the **Azure Active Directory** service.



The screenshot shows the Microsoft Azure portal interface. In the top left, there's a sidebar titled "Azure services" with a "Create a resource" button. The main area has a search bar with "active directory" typed in. Below the search bar, under the heading "Services", there are four items: "Azure AD Privileged Identity Management", "Azure Active Directory" (which is highlighted with a hand cursor icon), "Activity log", and "Security".

2. In the menu, click **App registrations**.

3. Create the application:

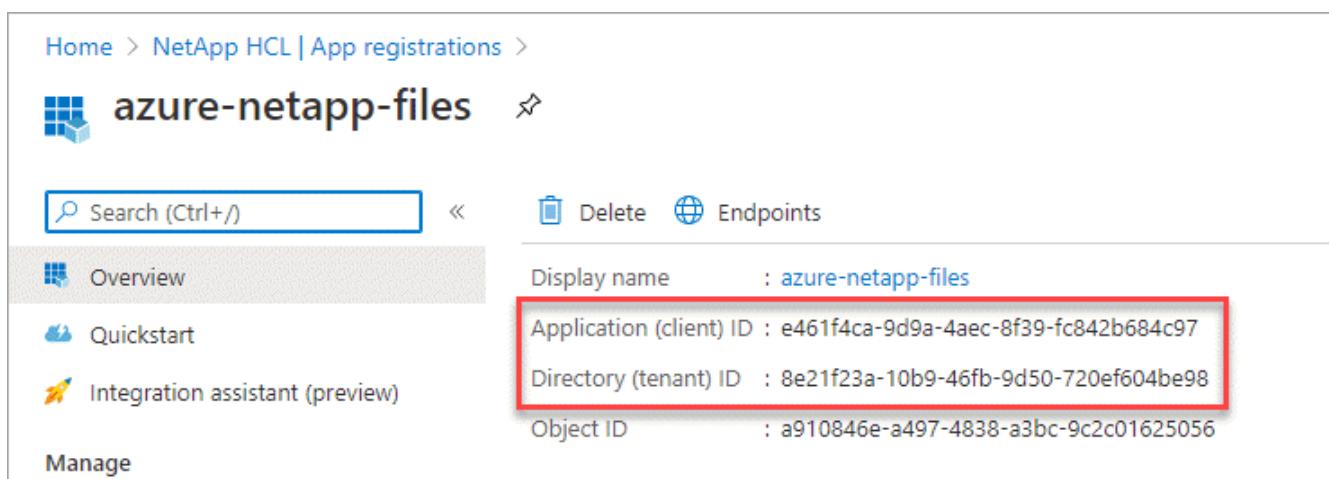
- a. Click **New registration**.

- b. Specify details about the application:

- **Name:** Enter a name for the application.
- **Account type:** Select an account type (any will work with Cloud Manager).
- **Redirect URI:** You can leave this blank.

- c. Click **Register**.

4. Copy the **Application (client) ID** and the **Directory (tenant) ID**.



The screenshot shows the "App registrations" section of the Azure portal. On the left, there's a navigation pane with "Overview", "Quickstart", and "Integration assistant (preview)". The main area shows a list of registered apps, with "azure-netapp-files" selected. The app details are shown on the right:

- Display name : [azure-netapp-files](#)
- Application (client) ID : e461f4ca-9d9a-4aec-8f39-fc842b684c97
- Directory (tenant) ID : 8e21f23a-10b9-46fb-9d50-720ef604be98
- Object ID : a910846e-a497-4838-a3bc-9c2c01625056

The "Application (client) ID" and "Directory (tenant) ID" fields are highlighted with a red box.

When you create the Azure NetApp Files working environment in Cloud Manager, you need to provide the application (client) ID and the directory (tenant) ID for the application. Cloud Manager uses the IDs to programmatically sign in.

5. Create a client secret for the application so Cloud Manager can use it to authenticate with Azure AD:

- a. Click **Certificates & secrets > New client secret**.

- b. Provide a description of the secret and a duration.

- c. Click **Add**.

- d. Copy the value of the client secret.

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

Description	Expires	Value
Azure NetApp Files	7/30/2022	3gywMgvF1rxtle8jU1po6~... 

## Result

Your AD application is now setup and you should have copied the application (client) ID, the directory (tenant) ID, and the value of the client secret. You need to enter this information in Cloud Manager when you add an Azure NetApp Files working environment.

## Assigning the app to a role

You must bind the service principal to your Azure subscription and assign it a custom role that has the required permissions.

## Steps

1. [Create a custom role in Azure](#).

The following steps describe how to create the role form the Azure portal.

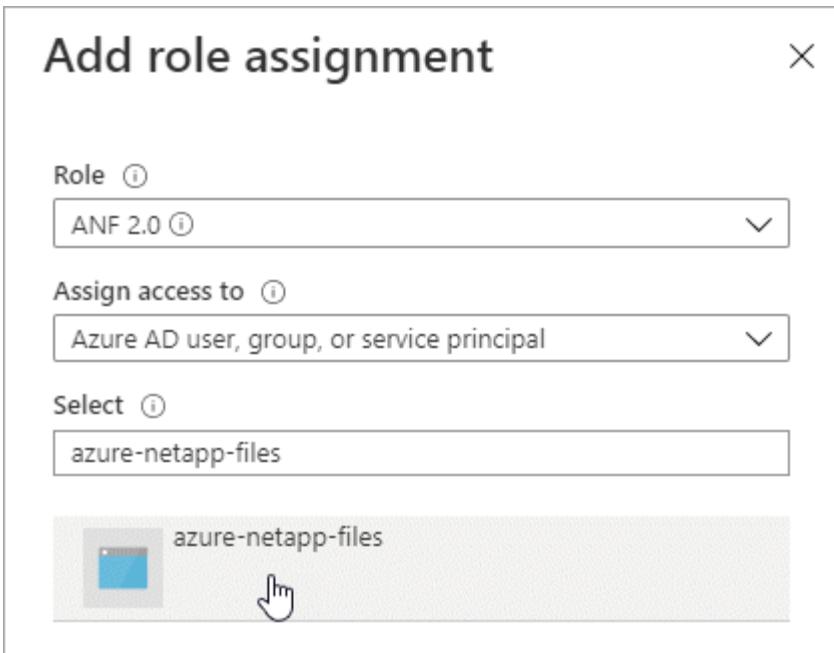
- a. Open the subscription and click **Access control (IAM)**.
- b. Click **Add > Add custom role**.

The screenshot shows the Microsoft Azure portal interface. At the top, there's a navigation bar with 'Microsoft Azure' and a search bar. Below that, the breadcrumb navigation shows 'Home > OCCM Dev'. The main title is 'OCCM Dev | Access control (IAM)'. On the left, there's a sidebar with links: 'Overview', 'Activity log', 'Access control (IAM)' (which is highlighted with a blue circle 'a'), 'Tags', 'Diagnose and solve problems', and 'Security'. To the right of the sidebar is a content area with a search bar, a 'Download role assignments' button, and a context menu. The context menu has options: 'Add role assignment', 'Add co-administrator (disabled)', 'Add custom role' (which has a mouse cursor icon over it and is circled with 'a'), 'View my level of access to this resource.' (with a blue circle 'b' pointing to it), 'View my access' (in a blue button), and 'Check access'.

- c. In the **Basics** tab, enter a name and description for the role.
- d. Click **JSON** and click **Edit** which appears at the top right of the JSON format.
- e. Add the following permissions under *actions*:

```
"actions": [  
    "Microsoft.NetApp/*",  
    "Microsoft.Resources/resources/read",  
    "Microsoft.Resources/subscriptions/resourceGroups/read",  
  
    "Microsoft.Resources/subscriptions/resourcegroups/resources/read",  
    "Microsoft.Resources/subscriptions/resourceGroups/write",  
    "Microsoft.Network/virtualNetworks/read",  
    "Microsoft.Insights/Metrics/Read"  
],
```

- f. Click **Save**, click **Next**, and then click **Create**.
2. Now assign the application to the role that you just created:
  - a. From the Azure portal, open the subscription and click **Access control (IAM)** > **Add** > **Add role assignment**.
  - b. Select the custom role that you created.
  - c. Keep **Azure AD user, group, or service principal** selected.
  - d. Search for the name of the application (you can't find it in the list by scrolling).



- e. Select the application and click **Save**.

The service principal for Cloud Manager now has the required Azure permissions for that subscription.

### Creating an Azure NetApp Files working environment

Set up an Azure NetApp Files working environment in Cloud Manager so you can start creating volumes.

1. From the Canvas page, click **Add Working Environment**.
2. Select **Microsoft Azure** and then **Azure NetApp Files**.
3. Provide details about the AD application that you previously set up.

## Azure NetApp Files Credentials

Working Environment Name

ANF

Application (client) ID

e461f4ca-9d9a-4aec-8f39-fc842b684c97

Client Secret

.....

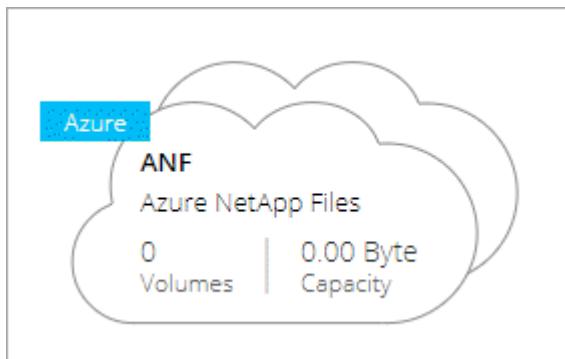
Directory (tenant) ID

8e21f23a-10b9-46fb-9d50-720ef604be98

4. Click **Add**.

### Result

You should now have an Azure NetApp Files working environment.



### What's next?

[Start creating and managing volumes.](#)

## Creating and managing volumes for Azure NetApp Files

After you set up your working environment, you can create and manage Azure NetApp Files accounts, capacity pools, volumes, and snapshots.

## Creating volumes

You can create NFS or SMB volumes in a new or existing Azure NetApp Files account.

### Steps

1. Open the Azure NetApp Files working environment.
2. Click **Add New Volume**.
3. Provide the required information on each page:
  - **Azure NetApp Files Account:** Choose an existing Azure NetApp Files account or create a new account.

The screenshot shows the 'Azure NetApp Files Account' creation interface. At the top, it says 'Choose an Azure NetApp Files account:' with two options: 'Select existing account' (radio button) and 'Create new account' (radio button, which is selected). Below this, there are four main input fields: 'Account Name' containing 'anf1', 'Location' set to 'West US', 'Azure Subscription' set to 'OCCM Dev', and 'Resource Group'. Under 'Resource Group', there are two options: 'Create new' (radio button, selected) and 'Use existing'. Below 'Create new', there is a field for 'Resource Group Name' containing 'anf'.

- **Capacity Pool:** Select an existing capacity pool or create a new capacity pool.

If you create a new capacity pool, you need to specify a size and select a [service level](#).

The minimum size for the capacity pool is 4 TB. You can specify a size in multiples of 4 TB.

- **Details & Tags:** Enter a volume name and size, the VNet and subnet where the volume should reside, and optionally specify tags for the volume.
- **Protocol:** Choose the NFS or SMB protocol and enter the required information.

Here's an example of details for NFS.

### Protocol

Select the volume's protocol:  **NFS Protocol**  SMB Protocol

Volume Path: vol1

Allowed Client & Access:

192.168.1.22/24	<input checked="" type="radio"/> Read & Write	<input type="radio"/> Read Only
-----------------	---	---------------------------------

Select NFS Version:

NFSv3  NFSv4.1

192.168.1.22/24	<input checked="" type="radio"/> Read & Write	<input type="radio"/> Read Only
-----------------	---	---------------------------------

Here's an example of details for SMB. You'll need to provide Active Directory information when you set up your first SMB volume.

### Protocol

Select the volume's protocol:  NFS Protocol  **SMB Protocol**

Protocol

Share Name: vol1

Active Directory

Choose an Active Directory connection joined to your Azure NetApp Files account

Active Directory

ActiveDirectory1

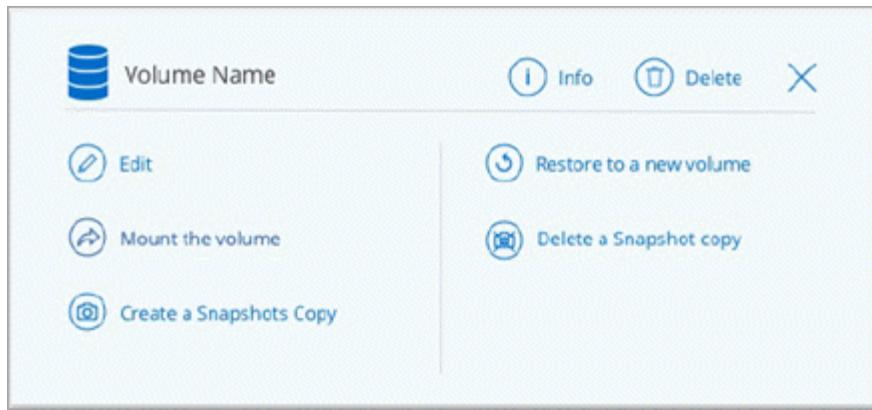
#### 4. Click **Add Volume**.

### Mounting volumes

Access mounting instructions from within Cloud Manager so you can mount the volume to a host.

### Steps

1. Open the working environment.
2. Hover over the volume and select **Mount the volume**.



3. Follow the instructions to mount the volume.

### Editing a volume's size and tags

After you create a volume, you can modify its size and tags at any time.

#### Steps

1. Open the working environment.
2. Hover over the volume and select **Edit**.
3. Modify the size and tags as needed.
4. Click **Apply**.

### Managing Snapshot copies

Snapshot copies provide a point-in-time copy of your volume. Create Snapshot copies, restore the data to a new volume, and delete Snapshot copies.

#### Steps

1. Open the working environment.
2. Hover over the volume and choose one of the available options to manage Snapshot copies:
  - **Create a Snapshot copy**
  - **Restore to a new volume**
  - **Delete a Snapshot copy**
3. Follow the prompts to complete the selected action.

### Deleting volumes

Delete the volumes that you no longer need.

#### Steps

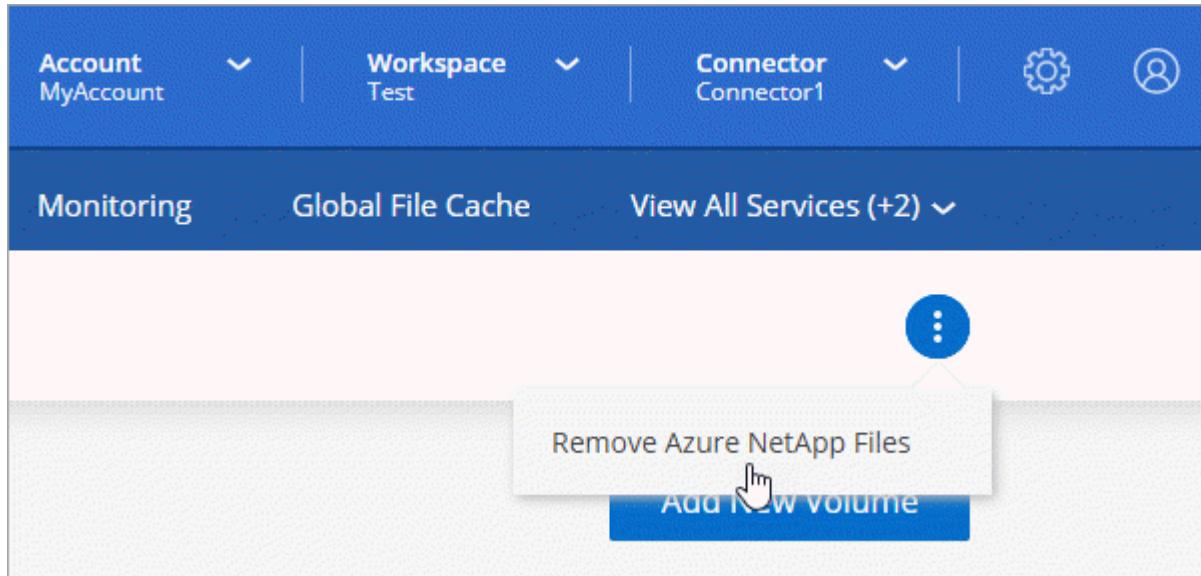
1. Open the working environment.
2. Hover over the volume and click **Delete**.
3. Confirm that you want to delete the volume.

## Removing Azure NetApp Files

This action removes Azure NetApp Files from Cloud Manager. It doesn't delete your Azure NetApp Files account or volumes. You can add Azure NetApp Files back to Cloud Manager at any time.

### Steps

1. Open the Azure NetApp Files working environment.
2. At the top right of the page, select the actions menu and click **Remove Azure NetApp Files**.



3. Click **Remove** to confirm.

## Cloud Volumes Service for AWS

### Learn about Cloud Volumes Service for AWS

NetApp Cloud Volumes Service for AWS is a cloud native file service that provides NAS volumes over NFS and SMB with all-flash performance. This service enables any workload, including legacy applications, to run in the AWS cloud.

### Benefits of using Cloud Volumes Service for AWS

Cloud Volumes Service for AWS provides the following benefits:

- Fully managed service, therefore no need to configure or manage storage devices
- Support for NFSv3 and NFSv4.1, and SMB 3.0 and 3.1.1 NAS protocols
- Secure access to Linux and Windows Elastic Container Service (ECS) instances, with support including the following:
  - Amazon Linux 2, Red Hat Enterprise Linux 7.5, SLES 12 SP3, and Ubuntu 16.04 LTS
  - Windows Server 2008 R2, Windows Server 2012 R2, and Windows Server 2016
- Choice of bundled and pay-as-you-go pricing

## Cost

Volumes created by the Cloud Volumes Service for AWS are charged based on your subscription to the service, not through Cloud Manager.

There are no charges to discover a Cloud Volumes Service for AWS region or volume from Cloud Manager.

## Before you get started

- Cloud Manager can discover existing Cloud Volumes Service for AWS subscriptions and volumes. See the [NetApp Cloud Volumes Service for AWS Account Setup Guide](#) if you haven't set up your subscription yet. You must follow this setup process for each region before you can add the AWS subscriptions and volumes in Cloud Manager.
- You need to obtain the Cloud Volumes API key and secret key so you can provide them to Cloud Manager. [For instructions, refer to Cloud Volumes Service for AWS documentation.](#)

## Quick start

Get started quickly by following these steps, or go to the next section for full details.



### Verify support for your configuration

You have set up AWS for Cloud Volumes Service and you must have subscribed to one of the [NetApp Cloud Volumes Service offerings on the AWS Marketplace](#).



### Add your Cloud Volumes Service for AWS subscription

You must create a working environment for the volumes based on your Cloud Volumes Service for AWS subscription.



### Create a cloud volumes

Cloud volumes that already exist for this subscription appear in the new working environment. Otherwise you create new volumes from Cloud Manager.



### Mount a cloud volume

Mount new cloud volumes to your AWS instance so that users can begin to use the storage.

## Getting help

Use the Cloud Manager chat for general service questions.

For technical support issues associated with your cloud volumes, use your 20 digit "930" serial number located in the "Support" tab of the Cloud Volumes Service user interface. Use this support ID when opening a web ticket or calling for support. Be sure to activate your Cloud Volumes Service serial number for support from the Cloud Volumes Service user interface. [Those steps are explained here.](#)

## Limitations

- Cloud Manager doesn't support data replication between working environments when using Cloud Volumes Service volumes.
- Removing your Cloud Volumes Service for AWS subscription from Cloud Manager isn't supported. You can do this only through the Cloud Volumes Service for AWS interface.

## Related links

- [NetApp Cloud Central: Cloud Volumes Service for AWS](#)
- [NetApp Cloud Volumes Service for AWS documentation](#)

## Managing Cloud Volumes Service for AWS

Cloud Manager enables you to create cloud volumes based on your [Cloud Volumes Service for AWS](#) subscription. You can also discover cloud volumes that you have already created from the Cloud Volumes Service interface and add them to a working environment.

### Add your Cloud Volumes Service for AWS subscription

Regardless of whether you have already created volumes from the Cloud Volumes Service user interface, or if you just signed up for Cloud Volumes Service for AWS and have no volumes yet, the first step is to create a working environment for the volumes based on your AWS subscription.

If cloud volumes already exist for this subscription, then the volumes are automatically added to the new working environment. If you haven't added any cloud volumes yet for the AWS subscription, then you do that after you create the new working environment.



If you have subscriptions and volumes in multiple AWS regions, you need to perform this task for each region.

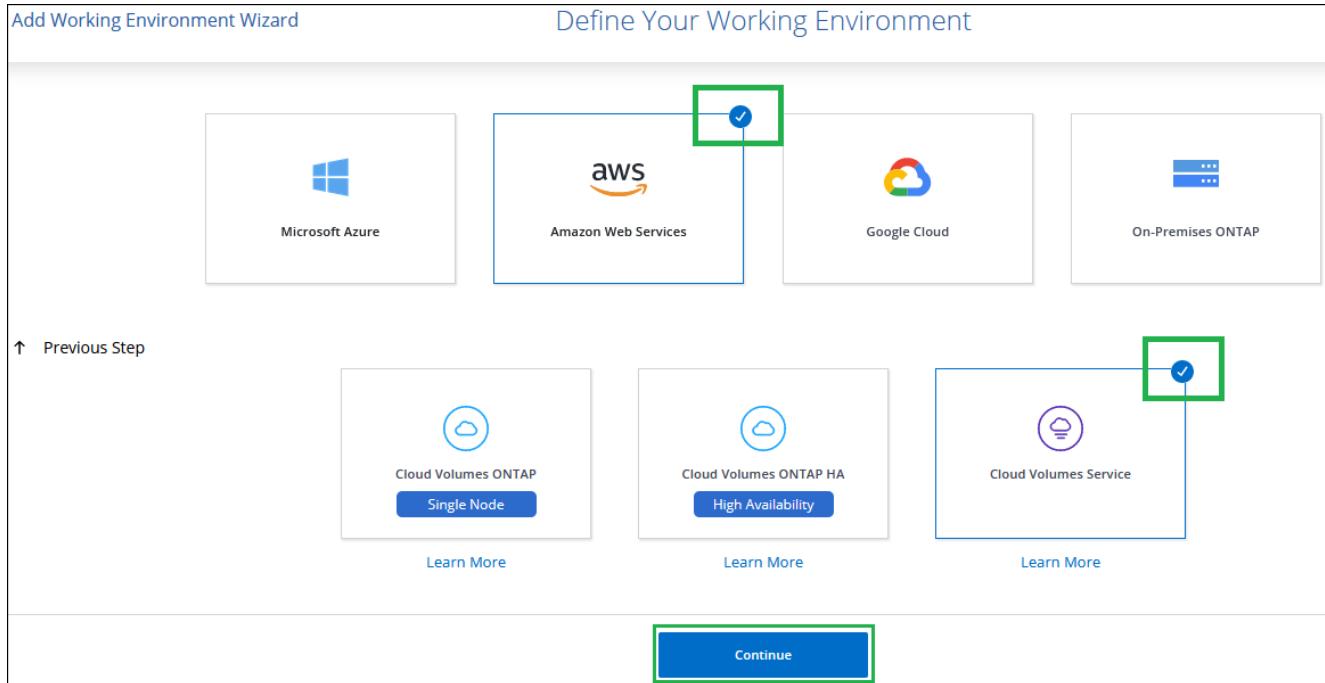
### Before you begin

You must have the following information available when adding a subscription in each region:

- Cloud Volumes API key and Secret key: [See the Cloud Volumes Service for AWS documentation to get this information.](#)
- The AWS region where the subscription was created.

### Steps

1. In Cloud Manager, add a new Working Environment, select the location **Amazon Web Services**, and click **Continue**.
2. Select **Cloud Volumes Service** and click **Continue**.



3. Provide information about your Cloud Volumes Service subscription:
  - a. Enter the Working Environment Name you want to use.
  - b. Enter the Cloud Volumes Service API key and secret key.
  - c. Select the AWS region where your cloud volumes reside, or where they will be deployed.
  - d. Click **Add**.

### Cloud Volumes Service Credentials

Working Environment Name

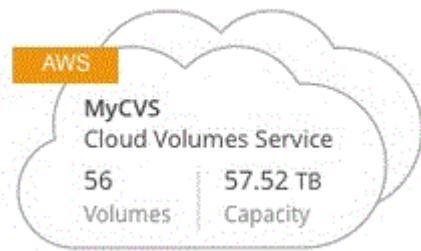
Cloud Volumes Service API Key

Cloud Volumes Service Secret Key

AWS Region

## Result

Cloud Manager displays your Cloud Volumes Service for AWS configuration on the Canvas page.



If cloud volumes already exist for this subscription, then the volumes are automatically added to the new working environment, as shown in the screenshot. You can add additional cloud volumes from Cloud Manager.

If no cloud volumes exist for this subscription, then you can create them now.

### Create cloud volumes

For configurations where volumes already exist in the Cloud Volumes Service working environment you can use these steps to add new volumes.

For configurations where no volumes exist, you can create your first volume directly from Cloud Manager after you have set up your Cloud Volumes Service for AWS subscription. In the past, the first volume had to be created directly in the Cloud Volumes Service user interface.

#### Before you begin

- If you want to use SMB in AWS, you must have set up DNS and Active Directory.
- When planning to create an SMB volume, you must have a Windows Active Directory server available to which you can connect. You will enter this information when creating the volume. Also, make sure that the Admin user is able to create a machine account in the Organizational unit (OU) path specified.
- You will need this information when creating the first volume in a new region/working environment:
  - AWS account ID: A 12-digit Amazon account identifier with no dashes. To find your account ID, refer to this [AWS topic](#).
  - Classless Inter-Domain Routing (CIDR) Block: An unused IPv4 CIDR block. The network prefix must range between /16 and /28, and it must also fall within the ranges reserved for private networks (RFC 1918). Do not choose a network that overlaps your VPC CIDR allocations.

#### Steps

1. Select the new working environment and click **Add New Volume**.
2. If you are adding the first volume to the working environment in the region, you have to add AWS networking information.
  - a. Enter the IPv4 range (CIDR) for the region.
  - b. Enter the 12-digit AWS account ID (with no dashes) to connect your Cloud Volumes account to your AWS account.
  - c. Click **Continue**.

## Network Setup



Your Cloud Volumes Service account isn't connected to your AWS account yet. Enter information about your AWS networking to connect the accounts. For details, see the [Cloud Volumes Service for AWS Account Setup document](#).

CIDR (IPv4)

192.168.0.0/28

AWS Account ID

123456789012345

3. The Accepting Virtual Interfaces page describes some steps you will need to perform after you add the volume so that you are prepared to complete that step. Just click **Continue** again.
4. In the Details & Tags page, enter details about the volume:
  - a. Enter a name for the volume.
  - b. Specify a size within the range of 100 GiB to 90,000 GiB (equivalent to 88 TiBs).  
[Learn more about allocated capacity](#).
  - c. Specify a service level: Standard, Premium, or Extreme.  
[Learn more about service levels](#).
  - d. Enter one or more tag names to categorize the volume if you want.
  - e. Click **Continue**.
5. In the Protocol page, select NFS, SMB, or Dual Protocol and then define the details. Required entries for NFS and SMB are shown in separate sections below.
6. In the Volume Path field, specify the name of the volume export you will see when you mount the volume.
7. If you select Dual-protocol you can select the security style by selecting NTFS or UNIX. Security styles affect the file permission type used and how permissions can be modified.
  - UNIX uses NFSv3 mode bits, and only NFS clients can modify permissions.
  - NTFS uses NTFS ACLs, and only SMB clients can modify permissions.
8. For NFS:
  - a. In the NFS Version field, select NFSv3, NFSv4.1, or both depending on your requirements.
  - b. Optionally, you can create an export policy to identify the clients that can access the volume. Specify the:
    - Allowed clients by using an IP address or Classless Inter-Domain Routing (CIDR).
    - Access rights as Read & Write or Read Only.
    - Access protocol (or protocols if the volume allows both NFSv3 and NFSv4.1 access) used for users.
    - Click **+ Add Export Policy Rule** if you want to define additional export policy rules.

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

**Protocol**

Select the volume's protocol:  NFS Protocol  SMB Protocol  Dual Protocol

**Volume Path**

**Export Policy**

**Allowed Client & Access**

192.168.1.2/24  Read & Write  Read Only

**Select NFS Version:**

NFSv3  NFSv4.1

**Select NFS Version:**

NFSv3  NFSv4.1

192.168.1.22/24  Read & Write  Read Only

**Select NFS Version:**

NFSv3  NFSv4.1

9. For SMB:

- You can enable SMB session encryption by checking the box for SMB Protocol Encryption.
- You can integrate the volume with an existing Windows Active Directory server by completing the fields in the Active directory section:

Field	Description
DNS Primary IP Address	The IP addresses of the DNS servers that provide name resolution for the SMB server. Use a comma to separate the IP addresses when referencing multiple servers, for example, 172.31.25.223, 172.31.2.74..
Active Directory Domain to join	The FQDN of the Active Directory (AD) domain that you want the SMB server to join. When using AWS Managed Microsoft AD, use the value from the "Directory DNS name" field.
SMB Server NetBIOS name	A NetBIOS name for the SMB server that will be created.
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.
Organizational Unit	The organizational unit within the AD domain to associate with the SMB server. The default is CN=Computers for connections to your own Windows Active Directory server. If you configure AWS Managed Microsoft AD as the AD server for the Cloud Volumes Service, you should enter <b>OU=Computers,OU=corp</b> in this field.

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

SMB Connectivity Setup	
DNS Primary IP Address	User Name
<input type="text" value="127.0.0.1"/>	<input type="text" value="administrator"/>
Active Directory Domain to Join	Password
<input type="text" value="yourdomain.com up to 107 characters"/>	<input type="password"/>
SMB Server NetBIOS Name	Organizational Unit
<input type="text" value="WENName"/>	<input type="text" value="CN=Computers"/>



You should follow the guidance on AWS security group settings to enable cloud volumes to integrate with Windows Active Directory servers correctly. See [AWS security group settings for Windows AD servers](#) for more information.

10. In the Volume from Snapshot page, if you want this volume to be created based on a snapshot of an existing volume, select the snapshot from the Snapshot Name drop-down list.
11. In the Snapshot Policy page, you can enable Cloud Volumes Service to create snapshot copies of your volumes based on a schedule. You can do this now or edit the volume later to define the snapshot policy.

See [Creating a snapshot policy](#) for more information about snapshot functionality.

## 12. Click **Add Volume**.

The new volume is added to the working environment.

### After you finish

If this is the first volume created in this AWS subscription, you need to launch the AWS Management Console to accept the two virtual interface that will be used in this AWS region to connect all your cloud volumes. See the [NetApp Cloud Volumes Service for AWS Account Setup Guide](#) for details.

You must accept the interfaces within 10 minutes after clicking the **Add Volume** button or the system may time out. If this happens, email [cvs-support@netapp.com](mailto:cvs-support@netapp.com) with your AWS Customer ID and NetApp Serial Number. Support will fix the issue and you can restart the onboarding process.

Then continue with [Mounting the cloud volume](#).

### Mount the cloud volume

You can mount a cloud volume to your AWS instance. Cloud volumes currently support NFSv3 and NFSv4.1 for Linux and UNIX clients, and SMB 3.0 and 3.1.1 for Windows clients.

**Note:** Please use the highlighted protocol/dialect supported by your client.

### Steps

1. Open the working environment.
2. Hover over the volume and click **Mount the volume**.

NFS and SMB volumes display mount instructions for that protocol. Dual-protocol volumes provide both sets of instructions.

3. Hover over the commands and copy them to your clipboard to make this process easier. Just add the destination directory/mount point at the end of the command.

#### NFS example:

**Mount the volume - testk**

---

**Setting up your instance**

1. Open an SSH client and connect to your instance.
2. Install the nfs client on your instance.  
On Red Hat Enterprise Linux or SuSE Linux instance:  

```
$ sudo yum install -y nfs-utils
```

  
On an Ubuntu or Debian instance:  

```
$ sudo apt-get install nfs-common
```

**Mounting your volume**

1. Create a new directory on your instance:  

```
$ sudo mkdir /dir
```
2. Mount your NFSv3 volume using the command below:  

```
sudo mount -t nfs -o rw,hard,rsize=65536,wsize=65536,vers=3,tc...
```
3. Mount your NFSv4.1 volume using the command below:  

```
sudo mount -t nfs -o rw,hard,rsize=65536,wsize=65536,vers=4,1,t...
```

The maximum I/O size defined by the `rsize` and `wsize` options is 1048576, however 65536 is the recommended default for most use cases.

Note that Linux clients will default to NFSv4.1 unless the version is specified with the `vers=<nfs_version>` option.

#### SMB example:

## Mount the volume - <Volume Name>

### Mapping your network drive

1. Click the Start button and then click on Computer.
2. Click Map Network Drive.
3. In the Drive list, click any available drive letter.
4. In the Folder box, type this:

```
\test.cv-pm.local\silly-condescending-mcnulty
```



To connect every time you log on to your computer, check the **Reconnect at logon** option.

5. Click Finish.

4. Connect to your Amazon Elastic Compute Cloud (EC2) instance by using an SSH or RDP client, and then follow the mount instructions for your instance.

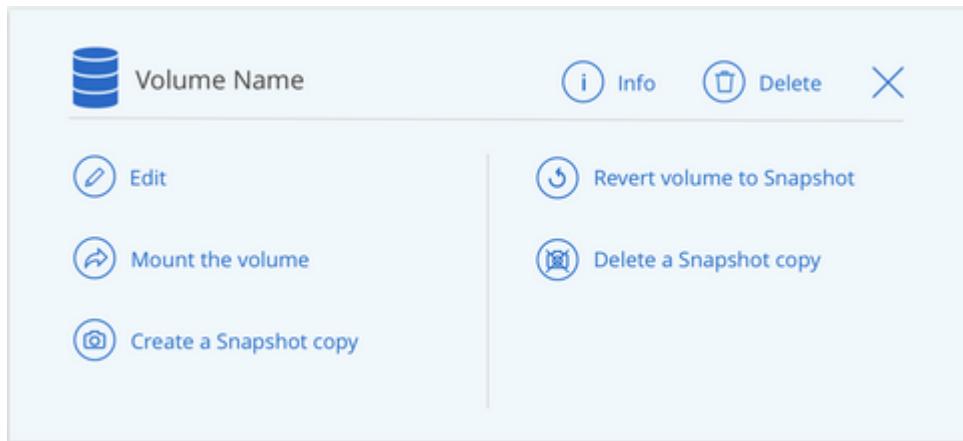
After completing the steps in the mount instructions, you have successfully mounted the cloud volume to your AWS instance.

## Managing existing volumes

You can manage existing volumes as your storage needs change. You can view, edit, restore, and delete volumes.

### Steps

1. Open the working environment.
2. Hover over the volume.



3. Manage your volumes:

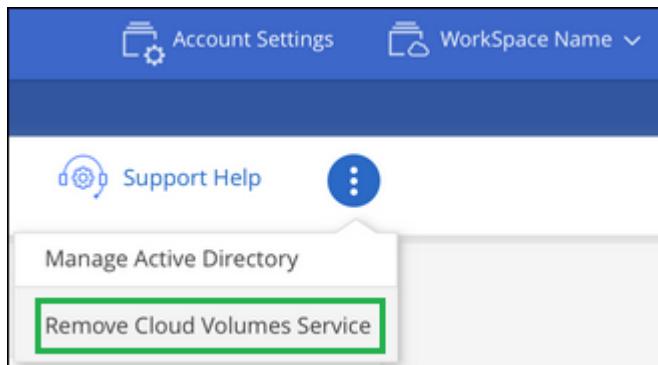
Task	Action
View information about a volume	Select a volume, and then click <b>Info</b> .
Edit a volume (including snapshot policy)	a. Select a volume, and then click <b>Edit</b> . b. Modify the volume's properties and then click <b>Update</b> .
Get the NFS or SMB mount command	a. Select a volume, and then click <b>Mount the volume</b> . b. Click <b>Copy</b> to copy the command(s).
Create a Snapshot copy on demand	a. Select a volume, and then click <b>Create a Snapshot copy</b> . b. Change the snapshot name, if needed, and then click <b>Create</b> .
Replace the volume with the contents of a Snapshot copy	a. Select a volume, and then click <b>Revert volume to Snapshot</b> . b. Select a Snapshot copy and click <b>Revert</b> .
Delete a Snapshot copy	a. Select a volume, and then click <b>Delete a Snapshot copy</b> . b. Select the Snapshot copy you want to delete and click <b>Delete</b> . c. Click <b>Delete</b> again to confirm.
Delete a volume	a. Unmount the volume from all clients: ◦ On Linux clients, use the <code>umount</code> command. ◦ On Windows clients, click <b>Disconnect network drive</b> . b. Select a volume, and then click <b>Delete</b> . c. Click <b>Delete</b> again to confirm.

## Remove Cloud Volumes Service from Cloud Manager

You can remove a Cloud Volumes Service for AWS subscription and all existing volumes from Cloud Manager. The volumes are not deleted, they are just removed from the Cloud Manager interface.

### Steps

1. Open the working environment.



2. Click the  button at the top of the page and click **Remove Cloud Volumes Service**.
3. In the confirmation dialog box, click **Remove**.

## Manage Active Directory configuration

If you change your DNS servers or Active Directory domain, you need to modify the SMB server in Cloud Volumes Services so that it can continue to serve storage to clients.

You can also delete the link to an Active Directory if you no longer need it.

### Steps

1. Open the working environment.
2. Click the  button at the top of the page and click **Manage Active Directory**.
3. If no Active Directory is configured, you can add one now. If one is configured, you can modify the settings or delete it using the  button.
4. Specify the settings for the Active Directory that you want to join:

Field	Description
DNS Primary IP Address	The IP addresses of the DNS servers that provide name resolution for the SMB server. Use a comma to separate the IP addresses when referencing multiple servers, for example, 172.31.25.223, 172.31.2.74.
Active Directory Domain to join	The FQDN of the Active Directory (AD) domain that you want the SMB server to join. When using AWS Managed Microsoft AD, use the value from the "Directory DNS name" field.
SMB Server NetBIOS name	A NetBIOS name for the SMB server that will be created.
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.
Organizational Unit	The organizational unit within the AD domain to associate with the SMB server. The default is CN=Computers for connections to your own Windows Active Directory server. If you configure AWS Managed Microsoft AD as the AD server for the Cloud Volumes Service, you should enter <b>OU=Computers,OU=corp</b> in this field.

5. Click **Save** to save your settings.

## Manage cloud volumes snapshots

You can create a snapshot policy for each volume so that you can recover or restore the entire contents of a volume from an earlier time. You can also create an on-demand snapshot of a cloud volume when needed.

### Create an on-demand snapshot

You can create an on-demand snapshot of a cloud volume if you want to create a snapshot with the current

volume state.

## Steps

1. Open the working environment.
2. Hover over the volume and click **Create a snapshot copy**.
3. Enter a name for the snapshot, or use the automatically generated name, and click **Create**.

**Create a Snapshot Copy - <Volume Name>**

---

A NetApp Snapshot copy is a read-only, point-in-time image of a volume. The image protects your data with no performance impact and requires minimal storage.

Snapshot Copy Name

---

**Create**

## Create or modify a snapshot policy

You can create or modify a snapshot policy as necessary for a cloud volume. You define the snapshot policy from the *Snapshot Policy* tab either when creating a volume or when editing a volume.

## Steps

1. Open the working environment.
2. Hover over the volume and click **Edit**.
3. From the *Snapshot Policy* tab, move the enable snapshots slider to the right.
4. Define the schedule for snapshots:
  - a. Select the frequency: **Hourly**, **Daily**, **Weekly**, or **Monthly**
  - b. Select the number of snapshots you want to keep.
  - c. Select the day, hour, and minute when the snapshot should be taken.

Schedule Snapshot Policies:

<input checked="" type="checkbox"/> Hourly	Number of Snapshot to Keep	Minute	
	<input type="text" value="12"/>	<input type="text" value="30"/>	
<input type="checkbox"/> Daily	Number of Snapshot to Keep	Hour      Minute	
	<input type="text" value="0"/>	<input type="text" value="0"/> <input type="text" value="0"/>	
<input checked="" type="checkbox"/> Weekly	Number of Snapshot to Keep	Days	Hour      Minute
	<input type="text" value="3"/>	<input type="button" value="Sunday X"/>	<input type="text" value="0"/> <input type="text" value="0"/>
<input type="checkbox"/> Monthly	Number of Snapshot to Keep	Days	Hour      Minute
	<input type="text" value="0"/>	<input type="checkbox"/> Sunday <input type="checkbox"/> Monday <input type="checkbox"/> Tuesday	<input type="text" value="0"/> <input type="text" value="0"/>

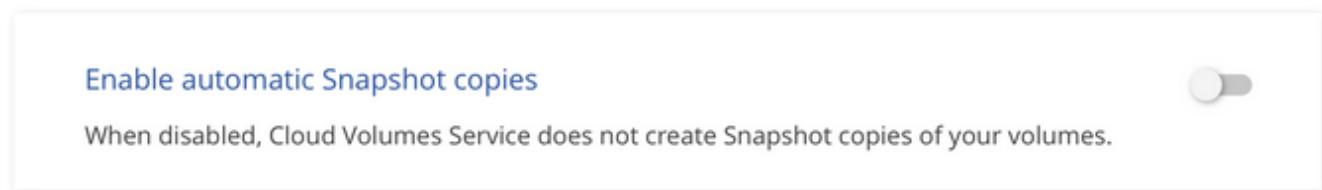
5. Click **Add volume** or **Update volume** to save your policy settings.

### Disable a snapshot policy

You can disable a snapshot policy to stop snapshots from being created for a short period of time while retaining your snapshot policy settings.

#### Steps

1. Open the working environment.
2. Hover over the volume and click **Edit**.
3. From the *Snapshot Policy* tab, move the enable snapshots slider to the left.



4. Click **Update volume**.

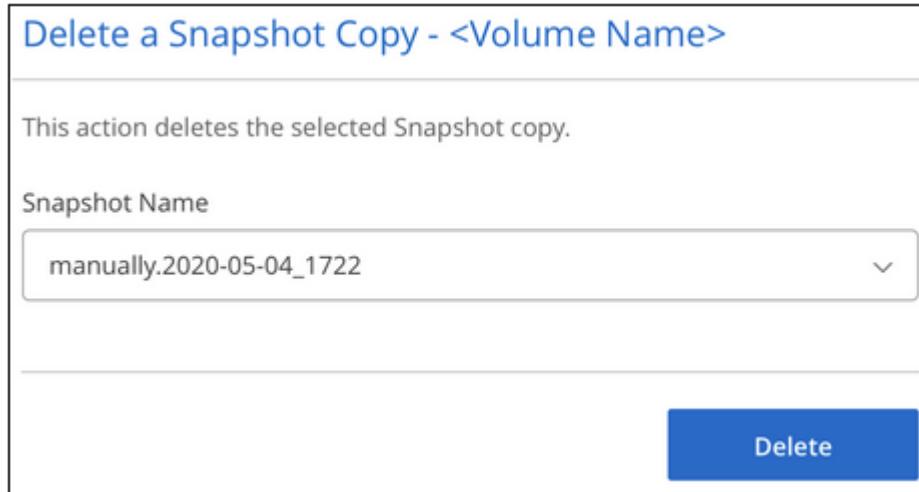
When you want to re-enable the snapshot policy, move the enable snapshots slider to the right and click **Update volume**.

### Delete a snapshot

You can delete a snapshot from the Volumes page.

## Steps

1. Open the working environment.
2. Hover over the volume and click **Delete a Snapshot copy**.
3. Select the snapshot from the drop-down list and click **Delete**.



4. In the confirmation dialog box, click **Delete**.

## Revert a volume from a snapshot

You can revert a volume to an earlier point in time from an existing snapshot.

When you revert a volume, the content of the snapshot overwrites the existing volume configuration. Any changes that were made to the data in the volume after the snapshot was created are lost.

Note that clients do not need to remount the volume after the revert operation.

## Steps

1. Open the working environment.
2. Hover over the volume and click **Revert volume to Snapshot**.
3. Select the snapshot that you want to use to restore the existing volume from the drop-down list and click **Revert**.

Revert volume to Snapshot - <Volume Name>

This action reverts the volume to a previous state. Any data saved after the Snapshot copy was created will be lost. This action can't be reversed.

Snapshot Name

- Select a snapshot copy -

Revert

## Reference

### Service levels and allocated capacity

The cost for Cloud Volumes Service for AWS is based on the *service level* and the *allocated capacity* that you select. Selecting the appropriate service level and capacity helps you meet your storage needs at the lowest cost.

### Considerations

Storage needs include two fundamental aspects:

- The storage *capacity* for holding data
- The storage *bandwidth* for interacting with data

If you consume more storage space than the capacity you selected for the volume, the following considerations apply:

- You will be billed for the additional storage capacity that you consume at the price defined by your service level.
- The amount of storage bandwidth available to the volume does not increase until you increase the allocated capacity size or change the service level.

### Service levels

Cloud Volumes Service for AWS supports three service levels. You specify your service level when you create or modify the volume.

The service levels are catered to different storage capacity and storage bandwidth needs:

- **Standard** (capacity)

If you want capacity at the lowest cost, and your bandwidth needs are limited, then the Standard service level might be most appropriate for you. An example is using the volume as a backup target.

- Bandwidth: 16 KB of bandwidth per GB provisioned capacity

- **Premium** (a balance of capacity and performance)

If your application has a balanced need for storage capacity and bandwidth, then the Premium service level might be most appropriate for you. This level is less expensive per MB/s than the Standard service level, and it is also less expensive per GB of storage capacity than the Extreme service level.

- Bandwidth: 64 KB of bandwidth per GB provisioned capacity

- **Extreme** (performance)

The Extreme service level is least expensive in terms of storage bandwidth. If your application demands storage bandwidth without the associated demand for lots of storage capacity, then the Extreme service level might be most appropriate for you.

- Bandwidth: 128 KB of bandwidth per GB provisioned capacity

### **Allocated capacity**

You specify your allocated capacity for the volume when you create or modify the volume.

While you would select your service level based on your general, high-level business needs, you should select your allocated capacity size based on the specific needs of applications, for example:

- How much storage space the applications need
- How much storage bandwidth per second the applications or the users require

Allocated capacity is specified in GBs. A volume's allocated capacity can be set within the range of 100 GB to 100,000 GB (equivalent to 100 TBs).

### **Number of inodes**

Volumes less than or equal to 1 TB can use up to 20 million inodes. The number of inodes increase by 20 million for each TB you allocate, up to a maximum of 100 million inodes.

- <= 1TB = 20 million inodes
- >1 TB to 2 TB = 40 million inodes
- >2 TB to 3 TB = 60 million inodes
- >3 TB to 4 TB = 80 million inodes
- >4 TB to 100 TB = 100 million inodes

### **Bandwidth**

The combination of both the service level and the allocated capacity you select determines the maximum bandwidth for the volume.

If your applications or users need more bandwidth than your selections, you can change the service level or increase the allocated capacity. The changes do not disrupt data access.

### **Selecting the service level and the allocated capacity**

To select the most appropriate service level and allocated capacity for your needs, you need to know how much capacity and bandwidth you require at the peak or the edge.

## List of service levels and allocated capacity

The leftmost column indicates the capacity, and the other columns define the MB/s available at each capacity point based on service level.

See [Contract subscription pricing](#) and [Metered subscription pricing](#) for complete details on pricing.

Capacity (TB)	Standard (MB/s)	Premium (MB/s)	Extreme (MB/s)
0.1 (100 GB)	1.6	6.4	12.8
1	16	64	128
2	32	128	256
3	48	192	384
4	64	256	512
5	80	320	640
6	96	384	768
7	112	448	896
8	128	512	1,024
9	144	576	1,152
10	160	640	1,280
11	176	704	1,408
12	192	768	1,536
13	208	832	1,664
14	224	896	1,792
15	240	960	1,920
16	256	1,024	2,048
17	272	1,088	2,176
18	288	1,152	2,304
19	304	1,216	2,432
20	320	1,280	2,560
21	336	1,344	2,688
22	352	1,408	2,816
23	368	1,472	2,944
24	384	1,536	3,072
25	400	1,600	3,200
26	416	1,664	3,328
27	432	1,728	3,456
28	448	1,792	3,584

Capacity (TB)	Standard (MB/s)	Premium (MB/s)	Extreme (MB/s)
29	464	1,856	3,712
30	480	1,920	3,840
31	496	1,984	3,968
32	512	2,048	4,096
33	528	2,112	4,224
34	544	2,176	4,352
35	560	2,240	4,480
36	576	2,304	4,500
37	592	2,368	4,500
38	608	2,432	4,500
39	624	2,496	4,500
40	640	2,560	4,500
41	656	2,624	4,500
42	672	2,688	4,500
43	688	2,752	4,500
44	704	2,816	4,500
45	720	2,880	4,500
46	736	2,944	4,500
47	752	3,008	4,500
48	768	3,072	4,500
49	784	3,136	4,500
50	800	3,200	4,500
51	816	3,264	4,500
52	832	3,328	4,500
53	848	3,392	4,500
54	864	3,456	4,500
55	880	3,520	4,500
56	896	3,584	4,500
57	912	3,648	4,500
58	928	3,712	4,500
59	944	3,776	4,500
60	960	3,840	4,500
61	976	3,904	4,500

Capacity (TB)	Standard (MB/s)	Premium (MB/s)	Extreme (MB/s)
62	992	3,968	4,500
63	1,008	4,032	4,500
64	1,024	4,096	4,500
65	1,040	4,160	4,500
66	1,056	4,224	4,500
67	1,072	4,288	4,500
68	1,088	4,352	4,500
69	1,104	4,416	4,500
70	1,120	4,480	4,500
71	1,136	4,500	4,500
72	1,152	4,500	4,500
73	1,168	4,500	4,500
74	1,184	4,500	4,500
75	1,200	4,500	4,500
76	1,216	4,500	4,500
77	1,232	4,500	4,500
78	1,248	4,500	4,500
79	1,264	4,500	4,500
80	1,280	4,500	4,500
81	1,296	4,500	4,500
82	1,312	4,500	4,500
83	1,328	4,500	4,500
84	1,344	4,500	4,500
85	1,360	4,500	4,500
86	1,376	4,500	4,500
87	1,392	4,500	4,500
88	1,408	4,500	4,500
89	1,424	4,500	4,500
90	1,440	4,500	4,500
91	1,456	4,500	4,500
92	1,472	4,500	4,500
93	1,488	4,500	4,500
94	1,504	4,500	4,500

Capacity (TB)	Standard (MB/s)	Premium (MB/s)	Extreme (MB/s)
95	1,520	4,500	4,500
96	1,536	4,500	4,500
97	1,552	4,500	4,500
98	1,568	4,500	4,500
99	1,584	4,500	4,500
100	1,600	4,500	4,500

### Example 1

For example, your application requires 25 TB of capacity and 100 MB/s of bandwidth. At 25 TB of capacity, the Standard service level would provide 400 MB/s of bandwidth at a cost of \$2,500 (estimate: see current pricing), making Standard the most suitable service level in this case.

### Example 2

For example, your application requires 12 TB of capacity and 800 MB/s of peak bandwidth. Although the Extreme service level can meet the demands of the application at the 12 TB mark, it is more cost-effective (estimate: see current pricing) to select 13 TB at the Premium service level.

### AWS security group settings for Windows AD servers

If you use Windows Active Directory (AD) servers with cloud volumes, you should familiarize yourself with the guidance on AWS security group settings. The settings enable cloud volumes to integrate with AD correctly.

By default, the AWS security group applied to an EC2 Windows instance does not contain inbound rules for any protocol except RDP. You must add rules to the security groups that are attached to each Windows AD instance to enable inbound communication from Cloud Volumes Service. The required ports are as follows:

Service	Port	Protocol
AD Web Services	9389	TCP
DNS	53	TCP
DNS	53	UDP
ICMPv4	N/A	Echo Reply
Kerberos	464	TCP
Kerberos	464	UDP
Kerberos	88	TCP
Kerberos	88	UDP
LDAP	389	TCP

Service	Port	Protocol
LDAP	389	UDP
LDAP	3268	TCP
NetBIOS name	138	UDP
SAM/LSA	445	TCP
SAM/LSA	445	UDP
Secure LDAP	636	TCP
Secure LDAP	3269	TCP
w32time	123	UDP

If you are deploying and managing your AD installation domain controllers and member servers on an AWS EC2 instance, you will require several security group rules to allow traffic for the Cloud Volumes Service. Below is an example of how to implement these rules for AD applications as part of the AWS CloudFormation template.

```
{
    "AWSTemplateFormatVersion" : "2010-09-09",
    "Description" : "Security Group for AD",
    "Parameters" :
    {
        "VPC" :
        {
            "Type" : "AWS::EC2::VPC::Id",
            "Description" : "VPC where the Security Group will belong:"
        },
        "Name" :
        {
            "Type" : "String",
            "Description" : "Name Tag of the Security Group:"
        },
        "Description" :
        {
            "Type" : "String",
            "Description" : "Description Tag of the Security Group:",
            "Default" : "Security Group for Active Directory for CVS"
        },
        "CIDRrangeforTCPandUDP" :
        {
            "Type" : "String",
            "Description" : "CIDR Range for the UDP ports
445,138,464,389,53,123 and for the TCP ports
464,339,3389,3268,88,636,9389,445 and 0-65535: *CIDR range format:
10.0.0.0/24"
        }
    }
}
```

```

        }
    },
    "Resources" :
    {
        "ADSGWest" :
        {
            "Type" : "AWS::EC2::SecurityGroup",
            "Properties" :
            {
                "GroupDescription" : { "Ref" : "Description" },
                "VpcId" : { "Ref" : "VPC" },
                "SecurityGroupIngress" : [
                    {
                        "IpProtocol" : "udp",
                        "CidrIp" : { "Ref" : "CIDRrangeforTCPandUDP" },
                        "FromPort" : "445",
                        "ToPort" : "445"
                    },
                    {
                        "IpProtocol" : "udp",
                        "CidrIp" : { "Ref" : "CIDRrangeforTCPandUDP" },
                        "FromPort" : "138",
                        "ToPort" : "138"
                    },
                    {
                        "IpProtocol" : "udp",
                        "CidrIp" : { "Ref" : "CIDRrangeforTCPandUDP" },
                        "FromPort" : "464",
                        "ToPort" : "464"
                    },
                    {
                        "IpProtocol" : "tcp",
                        "CidrIp" : { "Ref" : "CIDRrangeforTCPandUDP" },
                        "FromPort" : "464",
                        "ToPort" : "464"
                    },
                    {
                        "IpProtocol" : "udp",
                        "CidrIp" : { "Ref" : "CIDRrangeforTCPandUDP" },
                        "FromPort" : "389",
                        "ToPort" : "389"
                    },
                    {
                        "IpProtocol" : "udp",
                        "CidrIp" : { "Ref" : "CIDRrangeforTCPandUDP" },
                        "FromPort" : "53",
                        "ToPort" : "53"
                    }
                ]
            }
        }
    }
}

```

```
        "ToPort" : "53"
    },
{
    "IpProtocol" : "tcp",
    "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
    "FromPort" : "339",
    "ToPort" : "339"
},
{
    "IpProtocol" : "udp",
    "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
    "FromPort" : "123",
    "ToPort" : "123"
},
{
    "IpProtocol" : "tcp",
    "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
    "FromPort" : "3389",
    "ToPort" : "3389"
},
{
    "IpProtocol" : "tcp",
    "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
    "FromPort" : "3268",
    "ToPort" : "3268"
},
{
    "IpProtocol" : "tcp",
    "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
    "FromPort" : "88",
    "ToPort" : "88"
},
{
    "IpProtocol" : "tcp",
    "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
    "FromPort" : "636",
    "ToPort" : "636"
},
{
    "IpProtocol" : "tcp",
    "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
    "FromPort" : "3269",
    "ToPort" : "3269"
},
{
    "IpProtocol" : "tcp",
```

```

        "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},  

        "FromPort" : "53",  

        "ToPort" : "53"  

    },  

    {  

        "IpProtocol" : "tcp",  

        "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},  

        "FromPort" : "0",  

        "ToPort" : "65535"  

    },  

    {  

        "IpProtocol" : "tcp",  

        "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},  

        "FromPort" : "9389",  

        "ToPort" : "9389"  

    },  

    {  

        "IpProtocol" : "tcp",  

        "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},  

        "FromPort" : "445",  

        "ToPort" : "445"  

    }  

}  

]  

}  

},  

"Outputs" :  

{  

    "SecurityGroupID" :  

    {  

        "Description" : "Security Group ID",  

        "Value" : { "Ref" : "ADSGWest" }  

    }  

}
}

```

## Cloud Volumes Service for GCP

### Learn about Cloud Volumes Service for Google Cloud

NetApp Cloud Volumes Service for Google Cloud enables you to quickly add multi-protocol workloads as well as build and deploy both Windows-based and UNIX-based apps.

## **Key features:**

- Migrate data between on-premises and Google Cloud.
- Provision volumes from 1 to 100 TiB in seconds.
- Multiprotocol support (you can create an NFS or SMB volume).
- Protect data with automated, efficient snapshots.
- Accelerate app development with rapid cloning.

## **Cost**

Volumes created by the Cloud Volumes Service for Google Cloud are charged to your subscription to the service, not through Cloud Manager.

[View pricing](#)

There are no charges to discover a Cloud Volumes Service for Google Cloud region or volume from Cloud Manager.

## **Supported regions**

[View supported Google Cloud regions.](#)

## **Before you get started**

Cloud Manager can discover existing Cloud Volumes Service for GCP subscriptions and volumes. See the [NetApp Cloud Volumes Service for Google Cloud documentation](#) if you haven't set up your subscription yet.

## **Getting help**

Use the Cloud Manager chat for general questions about Cloud Volumes Service operation in Cloud Manager.

For general questions about Cloud Volumes Service for Google Cloud, email NetApp's Google Cloud Team at [gcinfo@netapp.com](mailto:gcinfo@netapp.com).

For technical issues associated with your cloud volumes, you can create a technical support case from the Google Cloud Console. See [obtaining support](#) for details.

## **Limitations**

- Cloud Manager doesn't support data replication between working environments when using Cloud Volumes Service volumes.
- Deleting your Cloud Volumes Service for Google Cloud subscription from Cloud Manager isn't supported. You can do this only through the Google Cloud Console.

## **Related links**

- [NetApp Cloud Central: Cloud Volumes Service for Google Cloud](#)
- [NetApp Cloud Volumes Service for Google Cloud documentation](#)

## Set up Cloud Volumes Service for Google Cloud

Create a Cloud Volumes Service for Google Cloud working environment in Cloud Manager to create and manage volumes and snapshots.

### Quick start

Get started quickly by following these steps, or go to the next section for full details.



#### 1 Enable the Cloud Volumes Service API

From Google, enable the Cloud Volumes Service for GCP API so that Cloud Manager can manage the subscription and cloud volumes.



#### 2 Create a GCP service account and download credentials

From Google, create a GCP service account and role so that Cloud Manager can access your Cloud Volumes Service for GCP account.



#### 3 Create a Cloud Volumes Service for GCP working environment

In Cloud Manager, click **Add Working Environment > Google Cloud > Cloud Volumes Service** and then provide details about the service account and Google Cloud project.

### Enable the Cloud Volumes Service API

In Google Cloud Shell, run the following command to enable the Cloud Volumes Service API:

```
gcloud --project=<my-cvs-project> services enable cloudvolumesgcp-api.netapp.com
```

### Give Cloud Manager access to the Cloud Volumes Service for GCP account

You must complete the following tasks so that Cloud Manager can access your Google Cloud project:

- Create a new service account
- Add the new service account member to your project and assign it specific roles (permissions)
- Create and download a key pair for the service account that is used to authenticate to Google

### Steps

1. In the Google Cloud Console, go to the **Service Accounts** page.
2. Click **Select a project**, choose your project, and click **Open**.
3. Click **Create Service Account**, enter the service account name (friendly display name) and description, and click **Create**.
4. From the *IAM* page click **Add** and fill out the fields in the *Add Members* page:
  - a. In the *New Members* field, enter the full service account ID, for example, [user1-service-account-cvs@project1.iam.gserviceaccount.com](mailto:user1-service-account-cvs@project1.iam.gserviceaccount.com).

- b. Add these roles:
    - *NetApp Cloud Volumes Admin*
    - *Compute Network Viewer*
    - *Folder Viewer*
  - c. Click **Save**.
5. From the *Service account details* page click **Add key > Create new key**.
6. Select **JSON** as the key type and click **Create**.

By clicking **Create** your new public/private key pair is generated and downloaded to your system. It serves as the only copy of the private key. Store this file securely because it can be used to authenticate as your service account.

For detailed steps, see the Google Cloud topics [Creating and managing service accounts](#), [Granting, changing, and revoking access to resources](#), and [Creating and managing service account keys](#).

### Create a Cloud Volumes Service for GCP working environment

Set up a Cloud Volumes Service for GCP working environment in Cloud Manager so you can start creating volumes.

Regardless of whether you have already created volumes from the Google Cloud Console, or if you just signed up for Cloud Volumes Service for GCP and have no volumes yet, the first step is to create a working environment for the volumes based on your GCP subscription.

If cloud volumes already exist for this subscription, then the volumes will appear in the new working environment. If you haven't added any cloud volumes yet for the GCP subscription, then you do that after you create the new working environment.



If you have subscriptions and volumes in multiple GCP projects, you need to perform this task for each project.

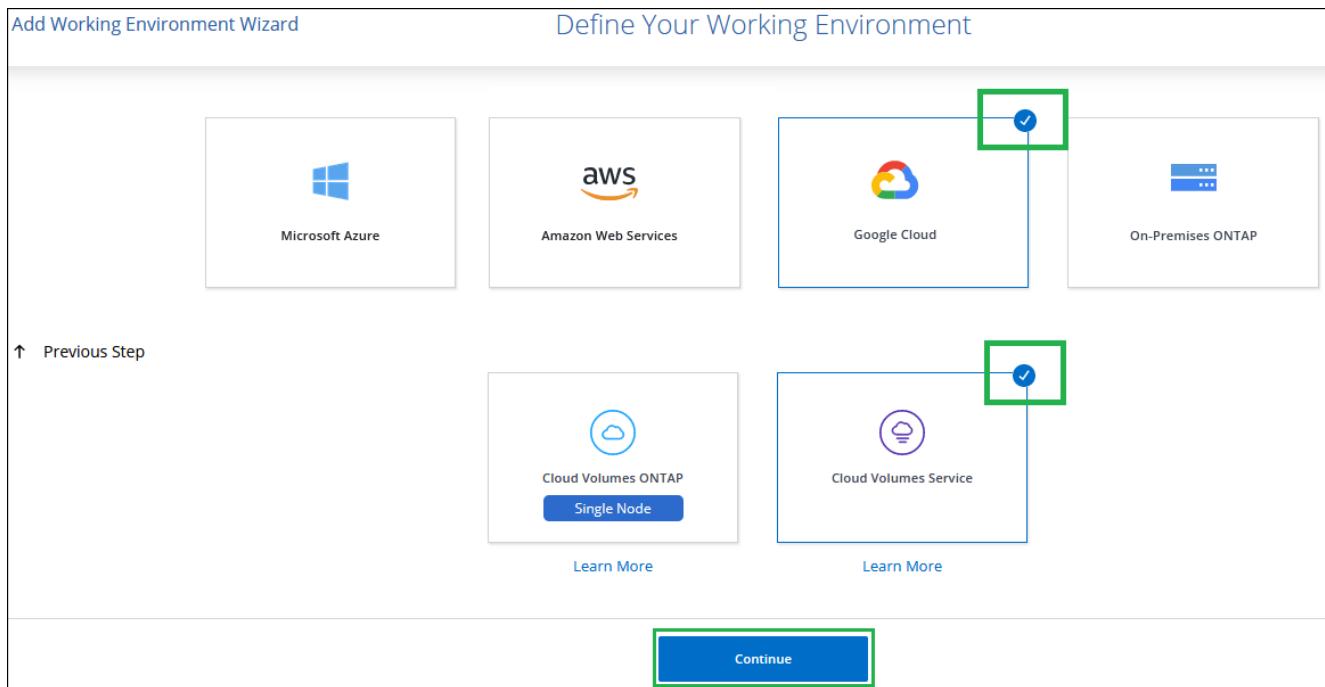
#### Before you begin

You must have the following information available when adding a subscription for each project:

- Service account credentials (JSON private key you downloaded)
- Project name

#### Steps

1. In Cloud Manager, add a new Working Environment, select the location **Google Cloud**, and click **Continue**.
2. Select **Cloud Volumes Service** and click **Continue**.



3. Provide information about your Cloud Volumes Service subscription:

- Enter the Working Environment Name you want to use.
- Copy/paste the JSON private key you downloaded in the previous steps.
- Select the name of your Google Cloud project.
- Click **Add**.

**Cloud Volumes Service Credentials**

Working Environment Name

Service Account Credentials  
 Paste the contents of the JSON file here

Project  
 - Select project -

## Result

Cloud Manager displays your Cloud Volumes Service for Google Cloud working environment.



If cloud volumes already exist for this subscription, then the volumes appear in the new working environment, as shown in the screenshot. You can add additional cloud volumes from Cloud Manager.

If no cloud volumes exist for this subscription, create them now.

#### What's next?

[Start creating and managing volumes](#).

## Create and manage volumes for Cloud Volumes Service for Google Cloud

Cloud Manager enables you to create cloud volumes based on your [Cloud Volumes Service for Google Cloud](#) subscription. You can also edit certain attributes of a volume, get the relevant mount commands, create snapshot copies, and delete cloud volumes.

### Create cloud volumes

You can create NFS or SMB volumes in a new or existing Cloud Volumes Service for Google Cloud account. Cloud volumes currently support NFSv3 and NFSv4.1 for Linux and UNIX clients, and SMB 3.x for Windows clients.

#### Before you begin

- If you want to use SMB in GCP, you must have set up DNS and Active Directory.
- When planning to create an SMB volume, you must have a Windows Active Directory server available to which you can connect. You will enter this information when creating the volume. Also, make sure that the Admin user is able to create a machine account in the Organizational unit (OU) path specified.

#### Steps

1. Select the working environment and click **Add New Volume**.
2. In the Details & Location page, enter details about the volume:
  - a. Enter a name for the volume.
  - b. Specify a size within the range of 1 TiB (1024 GiB) to 100 TiB.  
[Learn more about allocated capacity](#).
  - c. Specify a service level: Standard, Premium, or Extreme.  
[Learn more about service levels](#).
  - d. Select the Google Cloud region.
  - e. Select the VPC Network from which the volume will be accessible. Note that the VPC cannot be changed or edited after the volume is created.
  - f. Click **Continue**.
3. In the Protocol page, select NFS or SMB and then define the details. Required entries for NFS and SMB are shown in separate sections below.
4. For NFS:
  - a. In the Volume Path field, specify the name of the volume export you will see when you mount the volume.

- b. Select NFSv3, NFSv4.1, or both depending on your requirements.
- c. Optionally, you can create an export policy to identify the clients that can access the volume. Specify the:
  - Allowed clients by using an IP address or Classless Inter-Domain Routing (CIDR).
  - Access rights as Read & Write or Read Only.
  - Access protocol (or protocols if the volume allows both NFSv3 and NFSv4.1 access) used for users.
  - Click **+ Add Export Policy Rule** if you want to define additional export policy rules.

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

**Protocol**

Select the volume's protocol:  **NFS Protocol**  SMB Protocol

<b>Protocol</b>	<b>Export Policy</b>
Volume Path <input type="text" value="vol1"/>	Allowed Client & Access <input type="text" value="0.0.0.0/24"/> <input checked="" type="radio"/> Read & Write <input type="radio"/> Read Only
Select NFS Version: <input checked="" type="checkbox"/> NFSv3 <input type="checkbox"/> NFSv4.1	Select NFS Version: <input checked="" type="checkbox"/> NFSv3 <input type="checkbox"/> NFSv4.1

**+ Add Export Policy Rule (Up to 5)**

##### 5. For SMB:

- a. In the Volume Path field, specify the name of the volume export you will see when you mount the volume and click **Continue**.
- b. If Active Directory has been set up, you see the configuration. If it is the first volume being set up and no Active Directory has been set up, you can enable SMB session encryption in the SMB Connectivity Setup page:

Field	Description
DNS Primary IP Address	The IP addresses of the DNS servers that provide name resolution for the SMB server. Use a comma to separate the IP addresses when referencing multiple servers, for example, 172.31.25.223, 172.31.2.74..
Active Directory Domain to join	The FQDN of the Active Directory (AD) domain that you want the SMB server to join.
SMB Server NetBIOS name	A NetBIOS name for the SMB server that will be created.
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.

Field	Description
Organizational Unit	The organizational unit within the AD domain to associate with the SMB server. The default is CN=Computers for connections to your own Windows Active Directory server.

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

The screenshot shows the 'SMB Connectivity Setup' page with the following field values:

- DNS Primary IP Address: 127.0.0.1
- Active Directory Domain to Join: yourdomain.com up to 107 characters
- SMB Server NetBIOS Name: WEName
- User Name: administrator
- Password: (empty)
- Organizational Unit: CN=Computers

6. Click **Continue**.
7. If you want to create the volume based on a snapshot of an existing volume, select the snapshot from the Snapshot Name drop-down list. Otherwise just click **Continue**.
8. In the Snapshot Policy page, you can enable Cloud Volumes Service to create snapshot copies of your volumes based on a schedule. You can do this now by moving the selector to the right, or you can edit the volume later to define the snapshot policy.

See [Creating a snapshot policy](#) for more information about snapshot functionality.

9. Click **Add Volume**.

The new volume is added to the working environment.

Continue with [Mounting the cloud volume](#).

## Mount cloud volumes

Access mounting instructions from within Cloud Manager so you can mount the volume to a host.

**Note:** Please use the highlighted protocol/dialect supported by your client.

### Steps

1. Open the working environment.
2. Hover over the volume and click **Mount the volume**.

NFS and SMB volumes display mount instructions for that protocol.

3. Hover over the commands and copy them to your clipboard to make this process easier. Just add the destination directory/mount point at the end of the command.

## NFS example:

### Mount the volume - testk

#### Setting up your instance

1. Open an SSH client and connect to your instance.
2. Install the nfs client on your instance.

On Red Hat Enterprise Linux or SuSE Linux instance:

```
$ sudo yum install -y nfs-utils
```

On an Ubuntu or Debian instance:

```
$ sudo apt-get install nfs-common
```

#### Mounting your volume

1. Create a new directory on your instance:

```
$ sudo mkdir /dir
```
2. Mount your NFSv3 volume using the command below:

```
sudo mount -t nfs -o rw,hard,rsize=65536,wsize=65536,vers=3,tc...
```
3. Mount your NFSv4.1 volume using the command below:

```
sudo mount -t nfs -o rw,hard,rsize=65536,wsize=65536,vers=4,1,t...
```

The maximum I/O size defined by the `rsize` and `wszie` options is 1048576, however 65536 is the recommended default for most use cases.

Note that Linux clients will default to NFSv4.1 unless the version is specified with the `vers=<nfs_version>` option.

## SMB example:

## Mount the volume - <Volume Name>

### Mapping your network drive

1. Click the Start button and then click on Computer.
2. Click Map Network Drive.
3. In the Drive list, click any available drive letter.
4. In the Folder box, type this:

```
\test.cv-pm.local\silly-condescending-mcnulty
```



To connect every time you log on to your computer, check the **Reconnect at logon** option.

5. Click Finish.

4. Map your network drive by following the mount instructions for your instance.

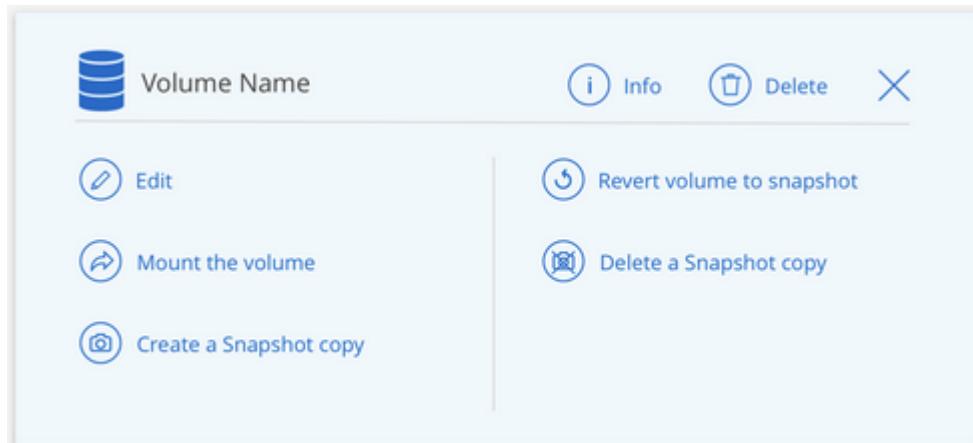
After completing the steps in the mount instructions, you have successfully mounted the cloud volume to your GCP instance.

## Manage existing volumes

You can manage existing volumes as your storage needs change. You can view, edit, restore, and delete volumes.

### Steps

1. Open the working environment.
2. Hover over the volume.



3. Manage your volumes:

Task	Action
View information about a volume	Click <b>Info</b> .
Edit a volume (including snapshot policy)	<ol style="list-style-type: none"> <li>Click <b>Edit</b>.</li> <li>Modify the volume's properties and then click <b>Update</b>.</li> </ol>
Get the NFS or SMB mount command	<ol style="list-style-type: none"> <li>Click <b>Mount the volume</b>.</li> <li>Click <b>Copy</b> to copy the command(s).</li> </ol>
Create a Snapshot copy on demand	<ol style="list-style-type: none"> <li>Click <b>Create a Snapshot copy</b>.</li> <li>Change the name, if needed, and then click <b>Create</b>.</li> </ol>
Replace the volume with the contents of a Snapshot copy	<ol style="list-style-type: none"> <li>Click <b>Revert volume to snapshot</b>.</li> <li>Select a Snapshot copy and click <b>Restore</b>.</li> </ol>
Delete a Snapshot copy	<ol style="list-style-type: none"> <li>Click <b>Delete a Snapshot copy</b>.</li> <li>Select the snapshot and click <b>Delete</b>.</li> <li>Click <b>Delete</b> again when prompted to confirm.</li> </ol>
Delete a volume	<ol style="list-style-type: none"> <li>Unmount the volume from all clients:             <ul style="list-style-type: none"> <li>◦ On Linux clients, use the <code>umount</code> command.</li> <li>◦ On Windows clients, click <b>Disconnect network drive</b>.</li> </ul> </li> <li>Select a volume, and then click <b>Delete</b>.</li> <li>Click <b>Delete</b> again to confirm.</li> </ol>

## Remove Cloud Volumes Service from Cloud Manager

You can remove a Cloud Volumes Service for Google Cloud subscription and all existing volumes from Cloud Manager. The volumes are not deleted, they are just removed from the Cloud Manager interface.

### Steps

1. Open the working environment.
2. Click the  button at the top of the page and click **Remove Cloud Volumes Service**.
3. In the confirmation dialog box, click **Remove**.

## Manage Active Directory configuration

If you change your DNS servers or Active Directory domain, you need to modify the SMB server in Cloud Volumes Services so that it can continue to serve storage to clients.

### Steps

1. Open the working environment.

2. Click the  button at the top of the page and click **Manage Active Directory**. If no Active Directory is configured, you can add one now. If one is configured, you can modify or delete the settings using the  button.
3. Specify the settings for the SMB server:

Field	Description
DNS Primary IP Address	The IP addresses of the DNS servers that provide name resolution for the SMB server. Use a comma to separate the IP addresses when referencing multiple servers, for example, 172.31.25.223, 172.31.2.74.
Active Directory Domain to join	The FQDN of the Active Directory (AD) domain that you want the SMB server to join.
SMB Server NetBIOS name	A NetBIOS name for the SMB server that will be created.
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.
Organizational Unit	The organizational unit within the AD domain to associate with the SMB server. The default is CN=Computers for connections to your own Windows Active Directory server.

4. Click **Save** to save your settings.

## Manage cloud volumes snapshots

You can create a snapshot policy for each volume so that you can recover or restore the entire contents of a volume from an earlier time. You can also create an on-demand snapshot of a cloud volume when needed.

### Create an on-demand snapshot

You can create an on-demand snapshot of a cloud volume if you want to create a snapshot with the current volume state.

#### Steps

1. Open the working environment.
2. Hover over the volume and click **Create a snapshot copy**.
3. Enter a name for the snapshot, or use the automatically generated name, and click **Create**.

## Create a Snapshot Copy - <Volume Name>

A NetApp Snapshot copy is a read-only, point-in-time image of a volume. The image protects your data with no performance impact and requires minimal storage.

Snapshot Copy Name

manually.2020-05-04\_1722

Create

The snapshot is created.

## Create or modify a snapshot policy

You can create or modify a snapshot policy as necessary for a cloud volume. You define the snapshot policy from the *Snapshot Policy* tab either when creating a volume or when editing a volume.

### Steps

1. Open the working environment.
2. Hover over the volume and click **Edit**.
3. From the *Snapshot Policy* tab, move the enable snapshots slider to the right.
4. Define the schedule for snapshots:
  - a. Select the frequency: **Hourly**, **Daily**, **Weekly**, or **Monthly**
  - b. Select the number of snapshots you want to keep.
  - c. Select the day, hour, and minute when the snapshot should be taken.

Schedule Snapshot Policies:

<input checked="" type="checkbox"/> Hourly	Number of Snapshot to Keep	Minute	
	<input type="text" value="12"/>	<input type="text" value="30"/>	
<input type="checkbox"/> Daily	Number of Snapshot to Keep	Hour      Minute	
	<input type="text" value="0"/>	<input type="text" value="0"/> <input type="text" value="0"/>	
<input checked="" type="checkbox"/> Weekly	Number of Snapshot to Keep	Days	Hour      Minute
	<input type="text" value="3"/>	<input type="button" value="Sunday X"/>	<input type="text" value="0"/> <input type="text" value="0"/>
<input type="checkbox"/> Monthly	Number of Snapshot to Keep	Days	Hour      Minute
	<input type="text" value="0"/>	<input type="checkbox"/> Sunday <input type="checkbox"/> Monday <input type="checkbox"/> Tuesday	<input type="text" value="0"/> <input type="text" value="0"/>

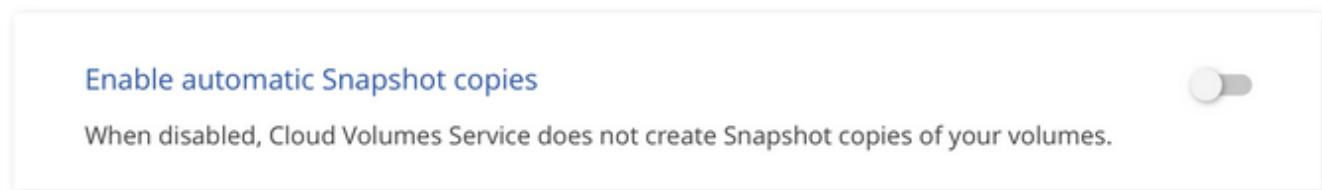
5. Click **Add volume** or **Update volume** to save your policy settings.

### Disable a snapshot policy

You can disable a snapshot policy to stop snapshots from being created for a short period of time while retaining your snapshot policy settings.

#### Steps

1. Open the working environment.
2. Hover over the volume and click **Edit**.
3. From the *Snapshot Policy* tab, move the enable snapshots slider to the left.



4. Click **Update volume**.

When you want to re-enable the snapshot policy, move the enable snapshots slider to the right and click **Update volume**.

### Delete a snapshot

You can delete a snapshot if it is no longer needed.

## Steps

1. Open the working environment.
2. Hover over the volume and click **Delete a Snapshot copy**.
3. Select the snapshot from the drop-down list and click **Delete**.

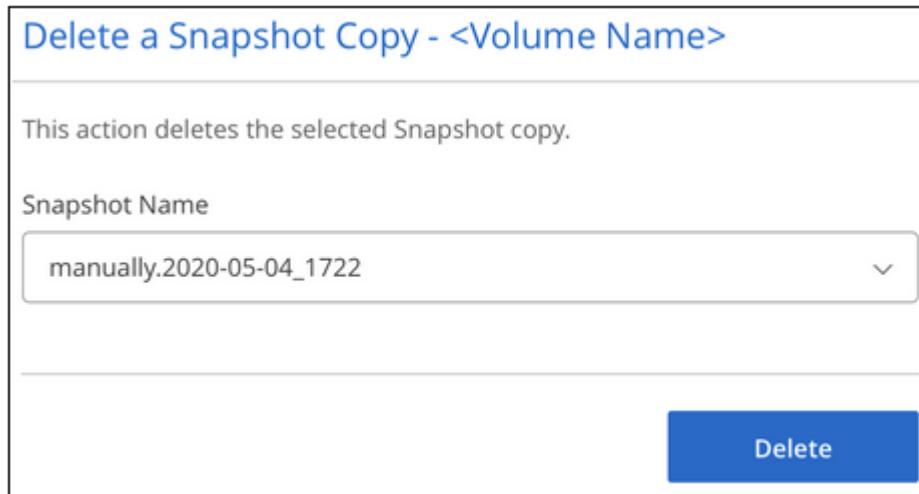
**Delete a Snapshot Copy - <Volume Name>**

This action deletes the selected Snapshot copy.

Snapshot Name

manually.2020-05-04\_1722

**Delete**



4. In the confirmation dialog box, click **Delete**.

## Restore a snapshot to a new volume

You can restore a snapshot to a new volume as necessary.

## Steps

1. Open the working environment.
2. Hover over the volume and click **Restore to a new volume**.
3. Select the snapshot that you want to use to create the new volume from the drop-down list.
4. Enter a name for the new volume and click **Restore**.

## Restore to a new volume - <Volume Name>

This operation restores data from a Snapshot copy to a new volume.

Snapshot Name

manually.2020-05-04\_1722



Restored Volume Name:

vol\_restore

**Restore**

The volume is created in the working environment.

5. If you need to change any of the volume attributes, such as volume path or service level:
  - a. Hover over the volume and click **Edit**.
  - b. Make your changes and click **Update volume**.

### After you finish

Continue with [Mounting the cloud volume](#).

# Manage ONTAP clusters

## Discovering ONTAP clusters

Cloud Manager can discover the ONTAP clusters in your on-premises environment, in a NetApp Private Storage configuration, and in the IBM Cloud. Discovering an ONTAP cluster enables you to provision storage, view whether shelf and disk firmware is recommended, replicate data, back up data, and tier cold data from an on-prem cluster to the cloud.

### What you'll need

- A Connector installed in a cloud provider or on your premises.

If you want to tier cold data to the cloud, then you should review requirements for the Connector based on where you plan to tier cold data.

- [Learn about Connectors](#)
- [Switching between Connectors](#)
- [Learn about Cloud Tiering](#)

- The cluster management IP address and the password for the admin user account to add the cluster to Cloud Manager.

Cloud Manager discovers ONTAP clusters using HTTPS. If you use custom firewall policies, they must meet the following requirements:

- The Connector host must allow outbound HTTPS access through port 443.

If the Connector is in the cloud, all outbound communication is allowed by the predefined security group.

- The ONTAP cluster must allow inbound HTTPS access through port 443.

The default "mgmt" firewall policy allows inbound HTTPS access from all IP addresses. If you modified this default policy, or if you created your own firewall policy, you must associate the HTTPS protocol with that policy and enable access from the Connector host.

- A valid set of NetApp Support Site credentials for accessing the Active IQ page.

## Viewing clusters from the Active IQ page

You can use the Active IQ service in Cloud Manager to discover, view, and manage all your on-prem clusters in a single location.

**Note:** The Active IQ page shows systems with a valid support contract. If contracts expire, a grace period of 90 days is given in which systems continue to be visible. Thereafter, systems are not searchable or visible on the Active IQ page. See how to [renew your support contract from Active IQ Digital Advisor](#). However, if you have already discovered on-prem clusters, you can continue to manage in their working environment using the Cloud Manager UI.

### Steps

1. Click the **Active IQ** tab, enter your NetApp Support Site user name and password, and click **Save**.

The clusters that have a valid support contract are displayed along with a status of whether they have been

discovered in Cloud Manager. Discovered clusters will also appear in their working environment.

Clusters	Licenses	Firmware Updates
Cluster Name	Cluster Status	OS Version
drgcsnsng	● Undiscovered	9.4
drgcsnsng	● Undiscovered	9.4
ccgsnprdsng	● Undiscovered	9.4
<a href="#">sti6-vsim-ucs</a>	● Discovered	9.4
<a href="#">sti6-vsim-ucs</a>	● Discovered	9.4

## Discovering clusters from the Canvas page

You can discover your ONTAP clusters and add them to a working environment from the Canvas page.

### Steps

1. On the Canvas page, click **Add Working Environment** and select **On-Premises ONTAP**.
2. If you're prompted, create a Connector.

Refer to the links above for more details.

3. On the *ONTAP Cluster Details* page, enter the cluster management IP address, the password for the admin user account, and the location of the cluster.
4. On the Details page, enter a name and description for the working environment, and then click **Go**.

### Result

Cloud Manager discovers the cluster and adds it to the working environment. You can now create volumes, replicate data to and from the cluster, set up data tiering to the cloud, back up volumes to the cloud, and launch System Manager to perform advanced tasks.

## Monitoring ONTAP clusters

The Active IQ page in Cloud Manager can show you any undiscovered ONTAP clusters in your on-premises environment, whether any clusters require new firmware to be installed, and if they are using all the licenses that you have paid for. This information is provided to Cloud Manager from the [Active IQ Digital Advisor](#).

## Checking for on-premises clusters that have not been added to Cloud Manager

The Active IQ page shows a list of all the on-prem clusters you are able to manage based on your NetApp Support Site (NSS) credentials. It also lists those clusters that have been discovered within Cloud Manager, and those that have not been discovered.

### Steps

1. Click the **Active IQ** tab, enter your NetApp Support Site user name and password, and click **Save**.

The clusters that have a valid support contract are displayed along with a status of whether they have been discovered in Cloud Manager.

See [Discovering clusters](#).

## Checking for new disk and shelf firmware

You can see whether any of your discovered ONTAP clusters need to have their shelf or disk firmware updated.

### Steps

1. From the Active IQ page, click the **Firmware Updates** tab.
2. See the following instructions to [update your storage system firmware](#).

## Viewing unused Cloud Volumes ONTAP licenses

You can see whether any of your Cloud Volumes ONTAP clusters have licenses that you are not using.

### Steps

1. From the Active IQ page, click the **Licenses** tab.

## Managing storage for ONTAP clusters

After you discover your ONTAP cluster from Cloud Manager, you can open the working environment to provision and manage storage.

## Creating volumes for ONTAP clusters

Cloud Manager enables you to provision NFS, CIFS, and iSCSI volumes on ONTAP clusters.

### Before you begin

The data protocols must be set up on the cluster using System Manager or the CLI.

### About this task

You can create volumes on existing aggregates. You can't create new aggregates from Cloud Manager.

### Steps

1. On the Canvas page, double-click the name of the ONTAP cluster on which you want to provision volumes.
2. Click **Add New Volume**.
3. On the Create New Volume page, enter details for the volume, and then click **Create**.

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.
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.
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.
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, select it, click Target IQN, and then use the IQN to connect to the LUN from your hosts.</p>
Usage Profile	Usage profiles define the NetApp storage efficiency features that are enabled for a volume.

## Replicating data

You can replicate data between Cloud Volumes ONTAP systems and ONTAP clusters by choosing a one-time data replication, which can help you move data to and from the cloud, or a recurring schedule, which can help with disaster recovery or long-term retention.

[Click here for more details.](#)

## Backing up data

You can back up data from your on-premises ONTAP system to low-cost object storage in the cloud by using the Cloud Manager Cloud Backup service. This service provides backup and restore capabilities for protection and long-term archive of your cloud data.

[Click here for more details.](#)

## Tiering data to the cloud

Extend your data center to the cloud by automatically tiering inactive data from ONTAP clusters to object storage.

[Click here for more details.](#)

# Back up to the cloud

## Learn about Cloud Backup

Cloud Backup is an add-on service for Cloud Volumes ONTAP and on-premises ONTAP clusters that delivers backup and restore capabilities for protection, and long-term archive of your cloud data. Backups are automatically generated and stored in an object store in your cloud account, independent of volume Snapshot copies used for near-term recovery or cloning.

A snapshot is an instant record of your system metadata at a given moment in similar storage as the original file, while a data backup is a standalone replica of your data, stored away in a separate system.

There are two services that provide the full suite of backup and restore functionality:

- The **Cloud Backup service** enables you to create backup files from volumes on your Cloud Volumes ONTAP and on-prem ONTAP clusters.
- The **Restore service** enables you to restore an entire *volume*, or one or more *files*, from a backup file to the same or different Cloud Volumes ONTAP or on-prem ONTAP cluster.

[Learn more about the Cloud Backup Service.](#)



You must use Cloud Manager for all backup and restore operations. Any actions taken directly from ONTAP or from your cloud provider results in an unsupported configuration.

## Features

- Back up independent copies of your data volumes to low-cost object storage in the cloud.
- Backup data is secured with AES-256 bit encryption at-rest and TLS 1.2 HTTPS connections in-flight.
- Back up from cloud to cloud, and from on-premises ONTAP systems to cloud.
- Support for up to 1,019 backups of a single volume.
- Restore data from a specific point in time.
- Restore a volume or individual files to the source system or to a different system.
- Browsable file catalog for single file restore.

## Supported working environments and object storage providers

Cloud Backup enables you to back up volumes from the following working environments to object storage in the following cloud providers:

Source Working Environment	Backup File Destination
Cloud Volumes ONTAP in AWS	Amazon S3
Cloud Volumes ONTAP in Azure	Azure Blob
Cloud Volumes ONTAP in Google	Google Cloud Storage

Source Working Environment	Backup File Destination
On-premises ONTAP system	Amazon S3 Azure Blob

You can restore a volume, or individual files, from a backup file to the following working environments:

Backup File Location	Destination Working Environment	
	Volume Restore	File Restore
Amazon S3	Cloud Volumes ONTAP in AWS On-premises ONTAP system	Cloud Volumes ONTAP in AWS On-premises ONTAP system
Azure Blob	Cloud Volumes ONTAP in Azure On-premises ONTAP system	Cloud Volumes ONTAP in Azure On-premises ONTAP system
Google Cloud Storage	Cloud Volumes ONTAP in Google On-premises ONTAP system	

## Cost

There are two types of costs associated with using Cloud Backup: resource charges and service charges.

### Resource charges

Resource charges are paid to the cloud provider for storage and for running a virtual machine-instance in the cloud.

- For backup, you pay your cloud provider for object storage costs.

Since Cloud Backup preserves the storage efficiencies of the source volume, you pay the cloud provider object storage costs for the data *after* ONTAP efficiencies (for the smaller amount of data after deduplication and compression have been applied).

- For file restore, you pay your cloud provider for compute costs only when the Restore instance is running.

The instance runs only when browsing the backup file to locate the individual files you want to restore. The instance is turned off when not in use to save costs. And it is not deployed at all if you never attempt to restore individual files.

See the [type of virtual machine-instance that is deployed](#) for each supported cloud provider.

- For volume restore there is no cost because no separate instance is required.

### Service charges

Backup service charges are paid to NetApp and cover both the cost to *create* backups and to *restore* volumes, or files, from those backups. You pay only for the data that you protect, calculated by the target backup capacity *before* ONTAP efficiencies.

There are two ways to pay for the Backup service. The first option is to subscribe from the service provider, which enables you to pay per month based on the amount of backed up data. The second option is to purchase licenses directly from NetApp. Read the [Licensing](#) section for details.

## Licensing

Cloud Backup is available in two licensing options: Bring Your Own License (BYOL) and Pay As You Go (PAYGO). A 30-day free trial is available if you don't have a license.

### Free trial

When using the 30-day free trial, you are notified about the number of free trial days that remain. At the end of your free trial, backups stop being created. You must subscribe to the service or purchase a license to continue using the service.

Backup are not deleted when the service is disabled. You'll continue to be charged by your cloud provider for object storage costs for the capacity that your backups use unless you delete the backups.

### Pay-as-you-go subscription

For PAYGO you'll need to pay your cloud provider for object storage costs (as described earlier) and NetApp for backup licensing costs. The licensing costs are based on target backup capacity (before ONTAP storage efficiencies):

- AWS: [Go to the Cloud Manager Marketplace offering for pricing details](#).
- Azure: [Go to the Cloud Manager Marketplace offering for pricing details](#).
- GCP: [Go to the Cloud Manager Marketplace offering for pricing details](#)

### Bring your own license

BYOL is term-based (1YR/2YR/3YR) and capacity-based in 1 TB increments, based on the logical (before ONTAP storage efficiencies) backed up capacity. You pay NetApp to use the service for a period of time, say 1 year, and for a maximum amount backup capacity, say 10 TB, and you'll need to pay your cloud provider for object storage costs (as described earlier).

You'll receive a serial number that you enter in the Cloud Manager Licensing page to enable the service. When either limit is reached you'll need to renew the license. See [Adding and updating your Backup BYOL license](#). The Backup BYOL license applies to all Cloud Volumes ONTAP and on-premises systems associated with your [Cloud Central account](#).

### BYOL license considerations

When using a Cloud Backup BYOL license, Cloud Manager notifies you when backups are nearing the capacity limit or nearing the license expiration date. You receive these notifications:

- When backups have reached 80% of licensed capacity, and again when you have reached the limit
- 30 days before a license is due to expire, and again when the license expires

Use the chat icon in the lower right of the Cloud Manager interface to renew your license when you receive these notifications.

Two things can happen when your license expires:

- If the account you are using for your ONTAP systems has a marketplace account, the backup service continues to run, but you are shifted over to a PAYGO licensing model. You are charged by your cloud provider for object storage costs, and by NetApp for backup licensing costs, for the capacity that your backups are using.

- If the account you are using for your ONTAP systems does not have a marketplace account, the backup service continues to run, but you will continue to receive the expiration message.

Once you renew your BYOL subscription, Cloud Manager automatically obtains the new license from NetApp and installs it. If Cloud Manager can't access the license file over the secure internet connection, you can obtain the file yourself and manually upload it to Cloud Manager. For instructions, see [Adding and updating your Backup BYOL license](#).

Systems that were shifted over to a PAYGO license are returned to the BYOL license automatically. And systems that were running without a license will stop receiving the warning message and will be charged for backups that occurred while the license was expired.

## How Cloud Backup works

When you enable Cloud Backup on a Cloud Volumes ONTAP or on-premises ONTAP system, the service performs a full backup of your data. Volume snapshots are not included in the backup image. After the initial backup, all additional backups are incremental, which means that only changed blocks and new blocks are backed up.

### Where backups reside

Backup copies are stored in an S3 bucket, Azure Blob container, or Google Cloud Storage bucket that Cloud Manager creates in your cloud account. For Cloud Volumes ONTAP systems the object store is created in the same region where the Cloud Volumes ONTAP system is located. For on-premises ONTAP systems you identify the region when you enable the service.

There's one object store per Cloud Volumes ONTAP or on-premises ONTAP system. Cloud Manager names the object store as follows: `netapp-backup-clusteruuid`

Be sure not to delete this object store.

Notes:

- In AWS, Cloud Manager enables the [Amazon S3 Block Public Access feature](#) on the S3 bucket.
- In Azure, Cloud Manager uses a new or existing resource group with a storage account for the Blob container.
- In GCP, Cloud Manager uses a new or existing project with a storage account for the Google Cloud Storage bucket.

### Supported storage classes or access tiers

- In Amazon S3, backups start in the *Standard* storage class and transition to the *Standard-Infrequent Access* storage class after 30 days.
- In Azure, backups are associated with the *cool* access tier.
- In GCP, backups are associated with the *Standard* storage class by default.

You can also use the lower cost *Nearline* storage class, or the *Coldline* or *Archive* storage classes. See the Google topic [Storage classes](#) for information about changing the storage class.

### Backup settings are system wide

When you enable Cloud Backup, all the volumes you identify on the system are backed up to the cloud.

The schedule and number of backups to retain are defined at the system level. The backup settings affect all volumes on the system.

### **The schedule is daily, weekly, monthly, or a combination**

You can choose daily, or weekly, or monthly backups of all volumes. You can also select one of the system-defined policies that provide backups and retention for 3 months, 1 year, and 7 years. These policies are:

<b>Backup Policy Name</b>	<b>Backups per interval...</b>			<b>Max. Backups</b>
	<b>Daily</b>	<b>Weekly</b>	<b>Monthly</b>	
Netapp3MonthsRetention	30	13	3	46
Netapp1YearRetention	30	13	12	55
Netapp7YearsRetention	30	53	84	167

Backup protection policies that you have created on the system using ONTAP System Manager or the ONTAP CLI are also available as selections.

Once you have reached the maximum number of backups for a category, or interval, older backups are removed so you always have the most current backups.

Note that the retention period for backups of data protection volumes is the same as defined in the source SnapMirror relationship. You can change this if you want by using the API.

### **Backups are taken at midnight**

- Daily backups start just after midnight each day.
- Weekly backups start just after midnight on Sunday mornings.
- Monthly backups start just after midnight on the first of each month.

The start time is based on the time zone set on each source ONTAP system. At this time, you can't schedule backup operations at a user specified time.

### **Backup copies are associated with your Cloud Central account**

Backup copies are associated with the [Cloud Central account](#) in which Cloud Manager resides.

If you have multiple Cloud Manager systems in the same Cloud Central account, each Cloud Manager system will display the same list of backups. That includes the backups associated with Cloud Volumes ONTAP and on-premises ONTAP instances from other Cloud Manager systems.

### **Supported volumes**

Cloud Backup supports FlexVol read-write volumes and data protection (DP) volumes.

FlexGroup volumes and SnapLock volumes aren't currently supported.

## FabricPool tiering policy considerations

There are certain things you need to be aware of when the volume you are backing up resides on a FabricPool aggregate and it has an assigned policy other than `none`:

- The first backup of a FabricPool-tiered volume requires retrieval of all local and all tiered data (from the object store). This operation could cause a one-time increase in cost to read the data from your cloud provider.
  - Subsequent backups are incremental and do not have this effect.
  - If the tiering policy is assigned to the volume when it is initially created you will not see this issue.
- Consider the impact of backups before assigning the `all` tiering policy to volumes. Because data is tiered immediately, Cloud Backup will read data from the cloud tier rather than from the local tier. Because concurrent backup operations share the network link to the cloud object store, performance degradation might occur if network resources become saturated. In this case, you may want to proactively configure multiple network interfaces (LIFs) to decrease this type of network saturation.
- A backup operation does not "reheat" the cold data tiered in object storage.

## Limitations

- When making backups from on-premises ONTAP systems, Cloud Manager must be deployed in the cloud. There is no support for on-premises Cloud Manager deployments.
- When backing up data protection (DP) volumes, the rule that is defined for the SnapMirror policy on the source volume must use a label that matches the allowed Cloud Backup policy names of **daily**, **weekly**, or **monthly**. Otherwise the backup will fail for that DP volume.
- In Azure, if you enable Cloud Backup when Cloud Volumes ONTAP is deployed, Cloud Manager creates the resource group for you and you cannot change it. If you want to pick your own resource group when enabling Cloud Backup, **disable** Cloud Backup when deploying Cloud Volumes ONTAP and then enable Cloud Backup and choose the resource group from the Cloud Backup Settings page.
- When backing up volumes from Cloud Volumes ONTAP systems, volumes that you create outside of Cloud Manager aren't automatically backed up. For example, if you create a volume from the ONTAP CLI, ONTAP API, or System Manager, then the volume won't be automatically backed up. If you want to back up these volumes, you would need to disable Cloud Backup and then enable it again.
- ILM (tiering) from the object storage, or direct write to AWS Glacier or similar lower tier object storage, is not supported.
- SVM-DR and SM-BC configurations are not supported.
- MetroCluster (MCC) backup is supported from ONTAP secondary only: MCC → SnapMirror → ONTAP → Cloud Backup Service → object storage.
- WORM/Compliance mode on an object store is not supported.

## Single File Restore limitations

- Single file restore can restore individual files. There is currently no support for restoring folders/directories.
- The ONTAP version must be 9.6 or greater in your Cloud Volumes ONTAP or on-premises systems.
- Cross account restore requires manual action in the cloud provider console. See the AWS topic [granting cross-account bucket permissions](#) for details.
- Non supported configurations:
  - Gov Cloud is currently not supported.

- Same account with different Cloud Managers in different subnets.
- Restore can browse a single directory with flat files up to a maximum of 30,000 files. Larger directories are currently not supported.

## Get started

### Backing up data to Amazon S3

Complete a few steps to get started backing up data from Cloud Volumes ONTAP to Amazon S3.

#### Quick start

Get started quickly by following these steps or scroll down to the remaining sections for full details.



#### Verify support for your configuration

- You're running Cloud Volumes ONTAP 9.6 or later in AWS.
- You have subscribed to the [Cloud Manager Marketplace Backup offering](#), or you have purchased [and activated](#) a Cloud Backup BYOL license from NetApp.
- The IAM role that provides Cloud Manager with permissions includes S3 permissions from the latest [Cloud Manager policy](#).



#### Enable Cloud Backup on your new or existing system

- New systems: Cloud Backup is enabled by default in the working environment wizard. Be sure to keep the option enabled.
- Existing systems: Select the working environment and click **Activate** next to the Cloud Backup service in the right-panel, and then follow the setup wizard.



#### Define the backup policy

The default policy backs up volumes every day and retains the most recent 30 backup copies of each volume. Change to weekly or monthly backups, or select one of the system-defined policies that provide more options. You can also change the number of backup copies to retain.

## Define Policy

<a href="#" style="color: blue; text-decoration: none;">Policy - Retention &amp; Schedule</a>	<input checked="" type="radio"/> Create a New Policy	<input type="radio"/> Select an Existing Policy
<div style="display: flex; justify-content: space-between;"> <span style="width: 45%;">Backup Every</span> <span style="width: 45%;">Number of backups to retain</span> </div> <div style="display: flex; justify-content: space-around; margin-top: 5px;"> <span style="border: 1px solid #ccc; padding: 2px 10px;">Day</span> <span style="border: 1px solid #ccc; padding: 2px 10px;">30</span> </div>		
<b>DP Volumes</b> Data protection volume backups use the same retention period as defined in the source SnapMirror relationship by default. Use the API if you want to change this value		
<b>Information</b> Backup_Bucket_Name Bucket Name		



## Select the volumes that you want to back up

Identify which volumes you want to back up in the Select Volumes page.



## Restore your data, as needed

Choose to restore an entire backup to a new volume, or to restore individual files from the backup to an existing volume. You can restore data to a Cloud Volumes ONTAP system in AWS, or to an on-premises ONTAP system.

See [Restoring volume data from backup files](#) for details.

## Requirements

Read the following requirements to make sure that you have a supported configuration before you start backing up volumes to S3.

### Supported ONTAP versions

Cloud Volumes ONTAP 9.6 and later.

### Supported AWS regions

Cloud Backup is supported in all AWS regions [where Cloud Volumes ONTAP is supported](#).

### License requirements

For Cloud Backup PAYGO licensing, a Cloud Manager subscription is available in the AWS Marketplace that enables deployments of Cloud Volumes ONTAP 9.6 and later (PAYGO) and Cloud Backup. You need to [subscribe to this Cloud Manager subscription](#) before you enable Cloud Backup. Billing for Cloud Backup is done through this subscription.

For Cloud Backup BYOL licensing, you do not need an AWS Cloud Backup subscription. You need the serial number from NetApp that enables you to use the service for the duration and capacity of the license. See [Adding and updating your Backup BYOL license](#).

And you need to have a AWS subscription for the storage space where your backups will be located.

## AWS permissions required

The IAM role that provides Cloud Manager with permissions must include S3 permissions from the latest [Cloud Manager policy](#).

Here are the specific permissions from the policy:

```
{  
    "Sid": "backupPolicy",  
    "Effect": "Allow",  
    "Action": [  
        "s3:DeleteBucket",  
        "s3:GetLifecycleConfiguration",  
        "s3:PutLifecycleConfiguration",  
        "s3:PutBucketTagging",  
        "s3>ListBucketVersions",  
        "s3:GetObject",  
        "s3>ListBucket",  
        "s3>ListAllMyBuckets",  
        "s3:GetBucketTagging",  
        "s3:GetBucketLocation",  
        "s3:GetBucketPolicyStatus",  
        "s3:GetBucketPublicAccessBlock",  
        "s3:GetBucketAcl",  
        "s3:GetBucketPolicy",  
        "s3:PutBucketPublicAccessBlock"  
    ],  
    "Resource": [  
        "arn:aws:s3:::netapp-backup-*"  
    ]  
},
```

## Enabling Cloud Backup on a new system

Cloud Backup is enabled by default in the working environment wizard. Be sure to keep the option enabled.

### Steps

1. Click **Create Cloud Volumes ONTAP**.
2. Select Amazon Web Services as the cloud provider and then choose a single node or HA system.
3. Fill out the Details & Credentials page.
4. On the Services page, leave the service enabled and click **Continue**.



## Backup to Cloud



Integrated backup for Cloud Volumes ONTAP based on SnapMirror and Snapshot technologies. Backup copies are maintained in S3 buckets. Backups stored in S3 are charged separately from Cloud Volumes ONTAP.

### ADVANTAGES

- ✓ Automatically back up all volumes.
- ✓ Creates new backup copy every day.
- ✓ Retains backups for 30 days.

### CLARIFICATIONS

- Backup settings are editable after working environment creation.

## 5. Complete the pages in the wizard to deploy the system.

### Result

Cloud Backup is enabled on the system and backs up volumes every day and retains the most recent 30 backup copies.

### What's next?

You can [start and stop backups for volumes](#) or [change the backup schedule](#) and you can [restore entire volumes](#) or individual files from a backup file.

## Enabling Cloud Backup on an existing system

Enable Cloud Backup at any time directly from the working environment.

### Steps

1. Select the working environment and click **Activate** next to the Cloud Backup service in the right-panel.



2. Define the backup schedule and retention value and click **Continue**.

## Define Policy

**Policy - Retention & Schedule**

Create a New Policy     Select an Existing Policy

Backup Every      Number of backups to retain

Day      30

**DP Volumes**

Data protection volume backups use the same retention period as defined in the source SnapMirror relationship by default. Use the API if you want to change this value

**Information**

Backup\_Bucket\_Name  
Bucket Name

[See the list of existing policies.](#)

3. Select the volumes that you want to back up and click **Activate**.

Select Volumes							
57 Volumes							
<input checked="" type="checkbox"/>	Volume Name	Volume Type	Disk Type	SVM Name	Used Capacity	Allocated Capacity	Volume Status
<input checked="" type="checkbox"/>	Volume_Name_1	RW	GP2	SVM_Name_1	2.25 TB	10 TB	Active
<input checked="" type="checkbox"/>	Volume_Name_2	RW	GP2	SVM_Name_2	2.25 TB	10 TB	Active
<input checked="" type="checkbox"/>	Volume_Name_3	RW	GP2	SVM_Name_3	2.25 TB	10 TB	Active
<input checked="" type="checkbox"/>	Volume_Name_4	DP <small>(i)</small>	GP2	SVM_Name_4	2.25 TB	10 TB	Active
<input checked="" type="checkbox"/>	Volume_Name_5	RW	GP2	SVM_Name_5	2.25 TB	10 TB	Active

- To back up all volumes, check the box in the title row ( **Volume Name**).
- To back up individual volumes, check the box for each volume ( Volume\_1).

### Result

Cloud Backup starts taking the initial backups of each selected volume.

### What's next?

You can [start and stop backups for volumes or change the backup schedule](#) and you can [restore entire volumes or individual files from a backup file](#).

## Backing up data to Azure Blob storage

Complete a few steps to get started backing up data from Cloud Volumes ONTAP to Azure Blob storage.

## Quick start

Get started quickly by following these steps or scroll down to the remaining sections for full details.

1

### Verify support for your configuration

- You're running Cloud Volumes ONTAP 9.7 or later in Azure.
- You have a valid cloud provider subscription for the storage space where your backups will be located.
- You have subscribed to the [Cloud Manager Marketplace Backup offering](#), or you have purchased [and activated](#) a Cloud Backup BYOL license from NetApp.

2

### Enable Cloud Backup on your new or existing system

- New systems: Cloud Backup is enabled by default in the working environment wizard. Be sure to keep the option enabled.
- Existing systems: Select the working environment and click **Activate** next to the Cloud Backup service in the right-panel, and then follow the setup wizard.



3

### Enter the provider details

Select the provider subscription and choose whether you want to create a new resource group or use an already existing resource group.

A screenshot of a 'Provider Settings' dialog box. At the top, the title 'Provider Settings' is visible. Below it, under 'Azure Subscription', there is a dropdown menu showing 'Azure\_Subscription\_1'. Under 'Resource Group', there are two options: 'Create a new' (an empty radio button) and 'Use an existing' (a radio button with a blue dot). Below these, a section titled 'Select an Existing Resource Group' contains a dropdown menu showing 'Resource\_Group\_1'. The entire dialog box has a light gray background and is enclosed in a thin black border.

**4**

## Define the backup policy

The default policy backs up volumes every day and retains the most recent 30 backup copies of each volume. Change to weekly or monthly backups, or select one of the system-defined policies that provide more options.

### Define Policy

**Policy - Retention & Schedule**

Create a New Policy     Select an Existing Policy

Backup Every    Number of backups to retain

Day    30

---

**DP Volumes**    Data protection volume backups use the same retention period as defined in the source SnapMirror relationship by default. Use the API if you want to change this value

---

**Storage Account**    Cloud Manager will create the storage account after you complete the wizard

**5**

## Select the volumes that you want to back up

Identify which volumes you want to back up in the Select Volumes page.

**6**

## Restore your data, as needed

Choose to restore an entire backup to a new volume, or to restore individual files from the backup to an existing volume. You can restore data to a Cloud Volumes ONTAP system in Azure, or to an on-premises ONTAP system.

See [Restoring volume data from backup files](#) for details.

### Requirements

Read the following requirements to make sure that you have a supported configuration before you start backing up volumes to Azure Blob storage.

#### Supported ONTAP versions

Cloud Volumes ONTAP 9.7 and later.

#### Supported Azure regions

Cloud Backup is supported in all Azure regions [where Cloud Volumes ONTAP is supported](#).

#### License requirements

For Cloud Backup PAYGO licensing, a subscription through the Azure Marketplace is required before you enable Cloud Backup. Billing for Cloud Backup is done through this subscription. [You can subscribe from the Details & Credentials page of the working environment wizard](#).

For Cloud Backup BYOL licensing, you need the serial number from NetApp that enables you to use the service for the duration and capacity of the license. See [Adding and updating your Backup BYOL license](#).

And you need to have a Microsoft Azure subscription for the storage space where your backups will be located.

## Enabling Cloud Backup on a new system

Cloud Backup is enabled by default in the working environment wizard. Be sure to keep the option enabled.



If you want to pick the name of the resource group, **disable** Cloud Backup when deploying Cloud Volumes ONTAP. Follow the steps for [enabling Cloud Backup on an existing system](#) to enable Cloud Backup and choose the resource group.

### Steps

1. Click **Create Cloud Volumes ONTAP**.
2. Select Microsoft Azure as the cloud provider and then choose a single node or HA system.
3. Fill out the Details & Credentials page and be sure that an Azure Marketplace subscription is in place.
4. On the Services page, leave the service enabled and click **Continue**.

The screenshot shows the 'Backup to Cloud' configuration page. At the top, there's a cloud icon and the text 'Backup to Cloud'. To the right is a toggle switch set to 'On' and a collapse/expand button. Below this, a descriptive text states: 'Integrated backup for Cloud Volumes ONTAP based on SnapMirror and Snapshot technologies. Backup copies are maintained in Storage Accounts. Backups stored in Storage Accounts are charged separately from Cloud Volumes ONTAP.' Underneath, there are two sections: 'ADVANTAGES' and 'CLARIFICATIONS'. The 'ADVANTAGES' section lists three items with checkmarks: 'Automatically back up all volumes.', 'Creates new backup copy every day.', and 'Retains backups for 30 days.'. The 'CLARIFICATIONS' section contains one item: 'Backup settings are editable after working environment creation.'

5. Complete the pages in the wizard to deploy the system.

### Result

Cloud Backup is enabled on the system and backs up volumes every day and retains the most recent 30 backup copies.

### What's next?

You can [start and stop backups for volumes or change the backup schedule](#) and you can [restore entire volumes or individual files from a backup file](#).

## Enabling Cloud Backup on an existing system

Enable Cloud Backup at any time directly from the working environment.

### Steps

1. Select the working environment and click **Activate** next to the Cloud Backup service in the right-panel.



2. Select the provider details:

- The Azure subscription used to store the backups.
- The resource group - you can create a new resource group or select an existing resource group.
- And then click **Continue**.

**Provider Settings**

Azure Subscription

Azure\_Subscription\_1

Resource Group

Create a new     Use an existing

Select an Existing Resource Group

Resource\_Group\_1

Note that you cannot change the subscription or the resource group after the services has started.

3. In the *Define Policy* page, select the backup schedule and retention value and click **Continue**.

**Define Policy**

**Policy - Retention & Schedule**

Create a New Policy     Select an Existing Policy

Backup Every

Day

Number of backups to retain

30

**DP Volumes**

Data protection volume backups use the same retention period as defined in the source SnapMirror relationship by default. Use the API if you want to change this value

**Storage Account**

Cloud Manager will create the storage account after you complete the wizard

[See the list of existing policies.](#)

4. Select the volumes that you want to back up and click **Activate**.

Select Volumes							
57 Volumes							
<input checked="" type="checkbox"/>	Volume Name	Volume Type	Disk Type	SVM Name	Used Capacity	Allocated Capacity	Volume Status
<input checked="" type="checkbox"/>	Volume_Name_1	RW	GP2	SVM_Name_1	2.25 TB	10 TB	Active
<input checked="" type="checkbox"/>	Volume_Name_2	RW	GP2	SVM_Name_2	2.25 TB	10 TB	Active
<input checked="" type="checkbox"/>	Volume_Name_3	RW	GP2	SVM_Name_3	2.25 TB	10 TB	Active
<input checked="" type="checkbox"/>	Volume_Name_4	DP ⓘ	GP2	SVM_Name_4	2.25 TB	10 TB	Active
<input checked="" type="checkbox"/>	Volume_Name_5	RW	GP2	SVM_Name_5	2.25 TB	10 TB	Active

- To back up all volumes, check the box in the title row ( Volume Name).
- To back up individual volumes, check the box for each volume ( Volume\_1).

## Result

Cloud Backup starts taking the initial backups of each selected volume.

## What's next?

You can [start and stop backups for volumes or change the backup schedule](#) and you can [restore entire volumes or individual files from a backup file](#).

## Backing up data to Google Cloud Storage

Complete a few steps to get started backing up data from Cloud Volumes ONTAP to Google Cloud Storage.

### Quick start

Get started quickly by following these steps or scroll down to the remaining sections for full details.

1

### Verify support for your configuration

- You're running Cloud Volumes ONTAP 9.7P5 or later in GCP.
- You have a valid GCP subscription for the storage space where your backups will be located.
- You have a service account in your Google Cloud Project that has the predefined Storage Admin role.
- You have subscribed to the [Cloud Manager Marketplace Backup offering](#), or you have purchased and activated a Cloud Backup BYOL license from NetApp.

2

### Enable Cloud Backup on your new or existing system

- New systems: Cloud Backup can be enabled when you complete the new working environment wizard.
- Existing systems: Select the working environment and click **Activate** next to the Cloud Backup service in the right-panel, and then follow the setup wizard.

**3**

### Enter the provider details

Select the Google Cloud Project where you want the Google Cloud Storage bucket to be created for backups.

Provider Settings

Google Cloud Project

Default Project

**4**

### Define the backup policy

The default policy backs up volumes every day and retains the most recent 30 backup copies of each volume. Change to weekly or monthly backups, or select one of the system-defined policies that provide more options.

Define Policy

**Policy - Retention & Schedule**

Create a New Policy     Select an Existing Policy

Backup Every    Number of backups to retain

Day    30

**DP Volumes**    Data protection volume backups use the same retention period as defined in the source SnapMirror relationship by default. Use the API if you want to change this value

**Storage Account**    Cloud Manager will create the Google Cloud Storage Bucket after you complete the wizard

**5**

### Select the volumes that you want to back up

Identify which volumes you want to back up in the Select Volumes page.

**6**

### Restore your data, as needed

Restore a backup to a new volume. You can restore data to a Cloud Volumes ONTAP system in Google. A

Service Account is required on the Cloud Volumes ONTAP system where you are performing the restore.

See [Restoring volume data from backup files](#) for details.

## Requirements

Read the following requirements to make sure that you have a supported configuration before you start backing up volumes to Google Cloud storage.

### Supported ONTAP versions

Cloud Volumes ONTAP 9.7P5 and later.

### Supported GCP regions

Cloud Backup is supported in all GCP regions [where Cloud Volumes ONTAP is supported](#).

### License requirements

For Cloud Backup PAYGO licensing, a subscription through the [GCP Marketplace](#) is required before you enable Cloud Backup. Billing for Cloud Backup is done through this subscription. [You can subscribe from the Details & Credentials page of the working environment wizard](#).

For Cloud Backup BYOL licensing, you need the serial number from NetApp that enables you to use the service for the duration and capacity of the license. See [Adding and updating your Backup BYOL license](#).

And you need to have a Google subscription for the storage space where your backups will be located.

### GCP Service Account

You need to have a service account in your Google Cloud Project that has the predefined Storage Admin role. [Learn how to create a service account](#).

### Enabling Cloud Backup on a new system

Cloud Backup can be enabled when you complete the working environment wizard to create a new Cloud Volumes ONTAP system.

You must have a Service Account already configured. If you don't select a service account when you create the Cloud Volumes ONTAP system, then you'll need to turn off the system and add the service account to Cloud Volumes ONTAP from the GCP console.

See [Launching Cloud Volumes ONTAP in GCP](#) for requirements and details for creating your Cloud Volumes ONTAP system.

### Steps

1. On the Working Environments page, click **Add Working Environment** and follow the prompts.
2. **Choose a Location:** Select **Google Cloud Platform**.
3. **Choose Type:** Select **Cloud Volumes ONTAP** (either single-node or high-availability).
4. **Details & Credentials:** Enter the following information:
  - a. Click **Edit Project** and select a new project if the one you want to use is different than the default Project (where Cloud Manager resides).
  - b. Specify the cluster name.
  - c. Enable the **Service Account** switch and select the Service Account that has the predefined Storage Admin role. This is required to enable backups and tiering.

d. Specify the credentials.

Make sure that a GCP Marketplace subscription is in place.

Details & Credentials

Project1	MPAWSSubscription1222	<a href="#">Edit Project</a>
Google Cloud Project	Marketplace Subscription	
<b>Details</b>		<b>Credentials</b>
Working Environment Name (Cluster Name)		User Name
TamiVSA		admin
Service Account <a href="#">?</a>		Password
<input checked="" type="checkbox"/>		*****
Service Account Name		Confirm Password
ServiceAccount1		*****
<a href="#">+ Add Labels</a> Optional Field   Up to four labels		

5. **Services:** Leave the Cloud Backup service enabled and click **Continue**.

Services

 Backup to Cloud	<input checked="" type="checkbox"/>	<a href="#">▼</a>
---	-------------------------------------	-------------------

6. Complete the pages in the wizard to deploy the system as described in [Launching Cloud Volumes ONTAP in GCP](#).

## Result

Cloud Backup is enabled on the system and backs up the volume you created every day and retains the most recent 30 backup copies.

You can [start and stop backups for additional volumes](#) or [change the backup schedule](#) and you can [restore entire volumes from a backup file](#).

## Enabling Cloud Backup on an existing system

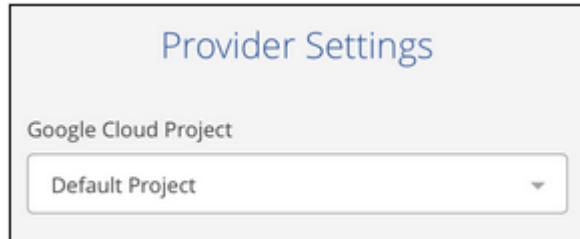
You can enable Cloud Backup at any time directly from the working environment.

## Steps

1. Select the working environment and click **Activate** next to the Cloud Backup service in the right-panel.

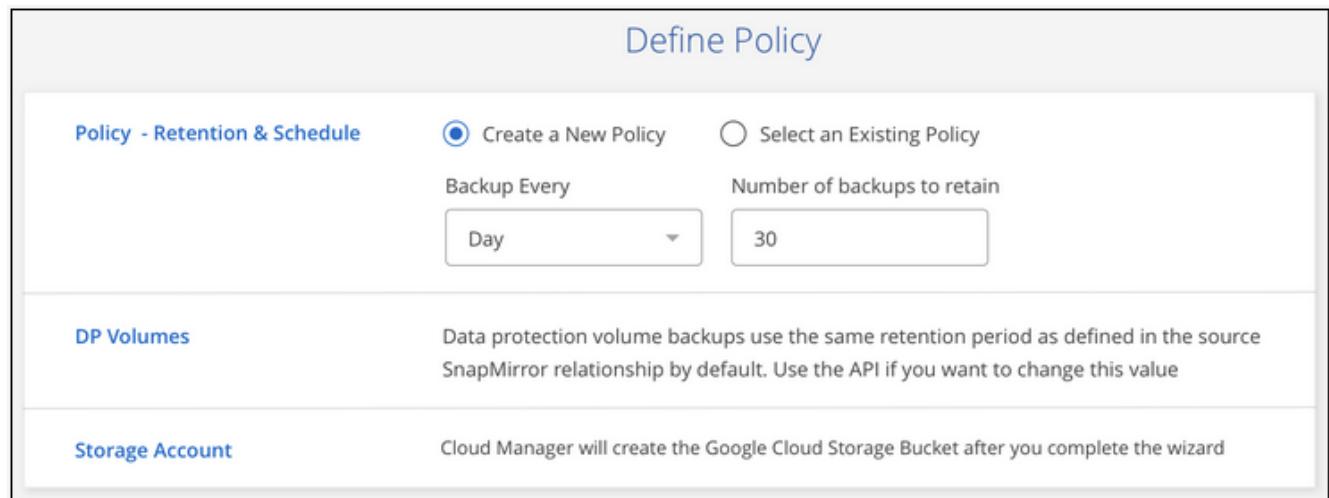


2. Select the Google Cloud Project where you want the Google Cloud Storage bucket to be created for backups, and click **Continue**. This can be a different Project than where the Cloud Volumes ONTAP system resides.



Note that the Project must have a Service Account that has the predefined Storage Admin role, and that you cannot change the Project after the service has started.

3. In the *Define Policy* page, select the backup schedule and retention value and click **Continue**.



See the [list of existing policies](#).

4. Select the volumes that you want to back up and click **Activate**.

Select Volumes							
57 Volumes							
	Volume Name	Volume Type	Disk Type	SVM Name	Used Capacity	Allocated Capacity	Volume Status
<input checked="" type="checkbox"/>	Volume_Name_1	RW	GP2	SVM_Name_1	2.25 TB	10 TB	Active
<input checked="" type="checkbox"/>	Volume_Name_2	RW	GP2	SVM_Name_2	2.25 TB	10 TB	Active
<input checked="" type="checkbox"/>	Volume_Name_3	RW	GP2	SVM_Name_3	2.25 TB	10 TB	Active
<input checked="" type="checkbox"/>	Volume_Name_4	DP ⓘ	GP2	SVM_Name_4	2.25 TB	10 TB	Active
<input checked="" type="checkbox"/>	Volume_Name_5	RW	GP2	SVM_Name_5	2.25 TB	10 TB	Active

- To back up all volumes, check the box in the title row ( **Volume Name**).
- To back up individual volumes, check the box for each volume ( **Volume\_1**).

## Result

Cloud Backup starts taking the initial backups of each selected volume.

## What's next?

You can [start and stop backups for volumes or change the backup schedule](#) and you can [restore entire volumes from a backup file](#).

## Backing up data from an on-premises ONTAP system to the cloud

Complete a few steps to get started backing up data from your on-premises ONTAP system to low-cost object storage in the cloud.

A Beta feature released in January 2021 allows you to run Compliance scans on the backed up volumes from your on-prem systems. Typically, compliance scans are free up to 1 TB of data, and then a cost for the service is applied for data over 1 TB. When combining Backup and Compliance for your on-prem volumes, the cost for scans on those on-prem volumes is free. Learn more about how [Cloud Compliance](#) can get your business applications and cloud environments privacy ready.

## Quick start

Get started quickly by following these steps or scroll down to the remaining sections for full details.



### Verify support for your configuration

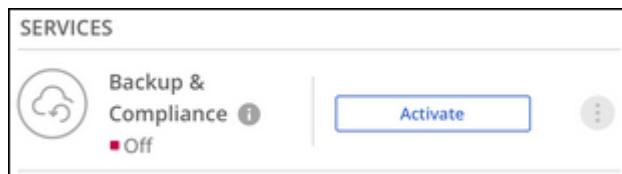
- You have discovered the on-premises cluster and added it to a working environment in Cloud Manager. See [Discovering ONTAP clusters](#) for details.
  - The cluster is running ONTAP 9.7P5 or later.
  - The cluster has a SnapMirror license—which is included as part of the PREM or Data Protection bundle.
- You have subscribed to the [Azure](#) or the [AWS](#) Cloud Manager Marketplace Backup offering, or you have purchased [and activated](#) a Cloud Backup BYOL license from NetApp.

- You have a valid cloud provider subscription for the object storage space where your backups will be located.
- For AWS, you need to have an account that has an access key and the required permissions so the ONTAP cluster can back up data to S3.

**2**

## Enable Cloud Backup on the system

Select the working environment and click **Activate** next to the Backup & Compliance service in the right-panel, and then follow the setup wizard.



**3**

## Select the cloud provider and enter provider details

Select the provider and then enter the provider details. You also need to specify the IPspace in the ONTAP cluster where the volumes reside.

**Note:** Backup to Google Cloud Storage from on-prem ONTAP systems is not currently supported from the UI.

**4**

## Define the backup policy

The default policy backs up volumes every day and retains the most recent 30 backup copies of each volume. Change to weekly or monthly backups, or select one of the system-defined policies that provide more options.

**Define Policy**

<b>Policy - Retention &amp; Schedule</b>	<input checked="" type="radio"/> Create a New Policy <input type="radio"/> Select an Existing Policy Backup Every      Number of backups to retain <div style="display: flex; justify-content: space-around;"> <div style="width: 150px;"> <input type="button" value="Day"/> </div> <div style="width: 150px;"> <input type="text" value="30"/> </div> </div>
<b>DP Volumes</b> Data protection volume backups use the same retention period as defined in the source SnapMirror relationship by default. Use the API if you want to change this value	
<b>Storage Account</b> Cloud Manager will create the storage account after you complete the wizard	

**5**

## Select the volumes that you want to back up

Identify which volumes you want to back up from the cluster.



## 6 Activate Compliance scans on the backed up volumes (optional)

Choose whether you want to have Cloud Compliance scan the volumes that are backed up in the cloud.



## 7 Restore your data, as needed

Choose to restore an entire backup to a new volume, or to restore individual files from the backup to an existing volume. You can restore data to a Cloud Volumes ONTAP system that is using the same cloud provider, or to an on-premises ONTAP system.

See [Restoring volume data from backup files](#) for details.

## Requirements

Read the following requirements to make sure you have a supported configuration before you start backing up on-prem volumes to object storage.

### ONTAP requirements

ONTAP 9.7P5 and later.

A SnapMirror license (included as part of the PREM or Data Protection bundle).

### Cluster networking requirements

An intercluster LIF is required on each ONTAP node that hosts the volumes you want to back up. The LIF must be associated with the *IPspace* that ONTAP should use to connect to object storage. [Learn more about IPspaces](#).

When you set up Cloud Backup, you are prompted for the *IPspace* to use. You should choose the *IPspace* that each LIF is associated with. That might be the "Default" *IPspace* or a custom *IPspace* that you created.

### Supported regions

Backups from on-prem systems are supported in all regions [where Cloud Volumes ONTAP is supported](#).

- For Azure, you specify the region where the backups will be stored when you set up the service.
- For AWS, backups are stored in the region where Cloud Manager is installed.

**Note:** Backup to Google Cloud Storage from on-prem ONTAP systems is not currently supported from the UI.

### License requirements

For Cloud Backup PAYGO licensing, you'll need a subscription to the [Azure](#) or the [AWS](#) Cloud Manager Marketplace Backup offering before you enable Cloud Backup. Billing for Cloud Backup is done through this subscription.

For Cloud Backup BYOL licensing, you need the serial number from NetApp that enables you to use the service for the duration and capacity of the license. See [Adding and updating your Backup BYOL license](#).

And you need to have a subscription from your cloud provider for the object storage space where your backups will be located.

## Preparing Amazon S3

When you are using Amazon S3, you must configure permissions for Cloud Manager to access the S3 bucket, and you must configure permissions so the on-prem ONTAP cluster can access the S3 bucket.

### Steps

1. Provide the following S3 permissions (from the latest [Cloud Manager policy](#)) to the IAM role that provides Cloud Manager with permissions:

```
{  
    "Sid": "backupPolicy",  
    "Effect": "Allow",  
    "Action": [  
        "s3:DeleteBucket",  
        "s3:GetLifecycleConfiguration",  
        "s3:PutLifecycleConfiguration",  
        "s3:PutBucketTagging",  
        "s3>ListBucketVersions",  
        "s3:GetObject",  
        "s3>ListBucket",  
        "s3>ListAllMyBuckets",  
        "s3:GetBucketTagging",  
        "s3:GetBucketLocation",  
        "s3:GetBucketPolicyStatus",  
        "s3:GetBucketPublicAccessBlock",  
        "s3:GetBucketAcl",  
        "s3:GetBucketPolicy",  
        "s3:PutBucketPublicAccessBlock"  
    ],  
    "Resource": [  
        "arn:aws:s3:::netapp-backup-*"  
    ]  
},
```

2. Provide the following permissions to the IAM user so that the ONTAP cluster can back up data to S3.

```
"s3>ListAllMyBuckets",  
"s3>ListBucket",  
"s3:GetBucketLocation",  
"s3:GetObject",  
"s3:PutObject",  
"s3>DeleteObject"
```

See the [AWS Documentation: Creating a Role to Delegate Permissions to an IAM User](#) for details.

3. Create or locate an access key.

Cloud Backup passes the access key on to the ONTAP cluster. The credentials are not stored in the Cloud Backup service.

See the [AWS Documentation: Managing Access Keys for IAM Users](#) for details.

## Enabling Cloud Backup

Enable Cloud Backup at any time directly from the on-premises working environment.

### Steps

- From the Canvas, select the working environment and click **Activate** next to the Backup & Compliance service in the right-panel.



- Select the provider, and then enter the provider details:

- For Azure, enter:
  - The Azure subscription used for backups and the Azure region where the backups will be stored.
  - The resource group - you can create a new resource group or select an existing resource group.
  - The IPspace in the ONTAP cluster where the volumes you want to back up reside.

Provider Settings	
<b>Provider Information</b>	
Azure Subscription	Azure_Subscription_1
Region	Default_CM_Region
IPspace	IP_Space_1
<b>Resource Group</b>	
<input type="radio"/> Create a new <input checked="" type="radio"/> Use an existing	
Select an Existing Resource Group	
Resource_Group_1	

- For AWS, enter:
  - The AWS Access Key and Secret Key used to store the backups.
  - The IPspace in the ONTAP cluster where the volumes you want to back up reside.

## Provider Settings

<b>AWS Credentials</b> <p>AWS Access Key  <input type="text" value="Enter AWS Access Key"/></p> <p>AWS Secret Key  <input type="text" value="Enter AWS Secret Key"/></p>	<b>Connectivity</b> <p>IPspace  <input type="text" value="IP_Space_1"/></p>
--	---

Note that you cannot change this information after the service has started.

3. Then click **Continue**.
4. In the *Define Policy* page, select the backup schedule and retention value and click **Continue**.

## Define Policy

<b>Policy - Retention &amp; Schedule</b> <p><input checked="" type="radio"/> Create a New Policy    <input type="radio"/> Select an Existing Policy</p> <p>Backup Every  <input type="text" value="Day"/>    Number of backups to retain  <input type="text" value="30"/></p>	<b>DP Volumes</b> <p>Data protection volume backups use the same retention period as defined in the source SnapMirror relationship by default. Use the API if you want to change this value</p> <b>Storage Account</b> <p>Cloud Manager will create the storage account after you complete the wizard</p>
---	--

[See the list of existing policies.](#)

5. Select the volumes that you want to back up.
  - To back up all volumes, check the box in the title row ( **Volume Name**).
  - To back up individual volumes, check the box for each volume ( **Volume\_1**).

**Select Volumes**

**57 Volumes**

<input checked="" type="checkbox"/> Volume Name	Volume Type	SVM Name	Used Capacity	Allocated Capacity	Volume Status
<input checked="" type="checkbox"/> Volume_Name_1	RW	SVM_Name_1	2.25 TB	10 TB	<span style="color: green;">Active</span>
<input checked="" type="checkbox"/> Volume_Name_2	RW	SVM_Name_2	2.25 TB	10 TB	<span style="color: green;">Active</span>
<input checked="" type="checkbox"/> Volume_Name_3	RW	SVM_Name_3	2.25 TB	10 TB	<span style="color: green;">Active</span>

6. Click **Activate** and Cloud Backup starts taking the initial backups of your volumes.

You are prompted whether you want to run compliance scans on the backed up volumes. Cloud Compliance scans are free when you run them on the backed up volumes (except for the [cost of the deployed Cloud Compliance instance](#)).

The screenshot shows a dialog box titled "Activate Compliance on your Backed Up Volumes". It contains the message: "You have successfully activated Backup to Cloud on 12 Volumes in your working environment 'Name 1'." Below this is a section titled "Cloud Compliance" with two bullet points: "Cloud Compliance offer automated controls for data privacy regulations such as the GDPR, CCPA and more." and "Driven by powerful artificial intelligence algorithms, Cloud Compliance gets your business application data and cloud environments privacy ready." At the bottom are two buttons: "Go to Compliance" (which is highlighted with a red box) and "Close".

7. Click **Go to Compliance** to activate compliance scans on the volumes. (If you choose **Close** and not to scan these backed up volumes, you can always [enable this functionality](#) later from Cloud Compliance.)

- If an instance of Cloud Compliance is already deployed in your environment, you are directed to the Configuration page to select the volumes you want to scan in each on-premises working environment that has backups. See [how to choose the volumes](#).

The screenshot shows the Cloud Compliance Configuration page. The top navigation bar includes "Cloud Compliance", "Dashboard", "Reports", "Investigation", "Highlights", and "Configuration" (which is underlined). Below this is a header "Working Environments" with a filter section containing "Filter by: CVO", "ANF", "S3", "DB", "ONEDR", "BACKUP" (which is highlighted with a red box), and "Clear filters". A "Working Environment 1 (back up)" card is shown, indicating "Cloud Backup of ONTAP" and "BETA". At the bottom of the card is a blue button with a red arrow pointing to it labeled "Activate Compliance for all Backed Up Volumes" and another red arrow pointing to the text "or select Volumes".

- If Cloud Compliance has not been deployed, you are directed to the Compliance page where you can choose to deploy Compliance in the cloud or in your premises. We strongly recommend deploying it in the cloud. Go [here](#) for installation requirements and instructions.

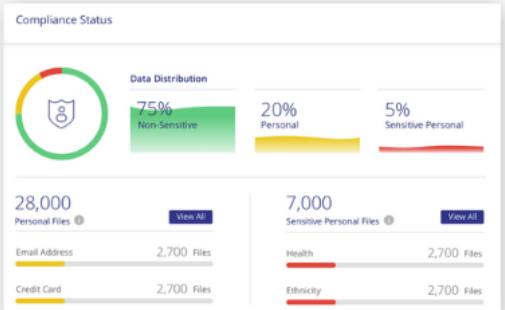
 Cloud Compliance

[How does it work? !\[\]\(412f6440973a65926ebe366941ddd4c3\_img.jpg\)](#)

## Always-on Privacy & Compliance Controls

Automated controls for data privacy regulations such as the GDPR, CCPA and more. Driven by powerful artificial intelligence algorithms, Cloud Compliance gets your business application data and cloud environments privacy ready.

[Deploy Compliance in the Cloud](#) [Deploy Compliance On-Premises](#)



 Learn about the differences between cloud deployment and on-premises deployment

After you have deployed Compliance you can choose the volumes you want to scan as described above.

## Result

Cloud Backup backs up your volumes from the on-prem ONTAP system, and optionally, Cloud Compliance runs compliance scans on the backed up volumes.

## What's next?

You can [start and stop backups for volumes or change the backup schedule](#) and you can [restore entire volumes or individual files](#) from a backup file.

You can also [view the results of the compliance scans](#) and review other features of Cloud Compliance that can help you understand data context and identify sensitive data in your organization.



The scan results are not available immediately because Cloud Backup has to finish creating the backups before Cloud Compliance can start compliance scans.

## Managing backups for Cloud Volumes ONTAP and on-premises ONTAP systems

You can manage backups for Cloud Volumes ONTAP and on-premises ONTAP systems by changing the backup schedule, enabling/disabling volume backups, deleting backups, and more.

### Changing the schedule and backup retention

The default policy backs up volumes every day and retains the most recent 30 backup copies of each volume. You can change to weekly or monthly backups and you can change the number of backup copies to retain. You can also select one of the system-defined policies that provide scheduled backups for 3 months, 1 year, and 7 years.

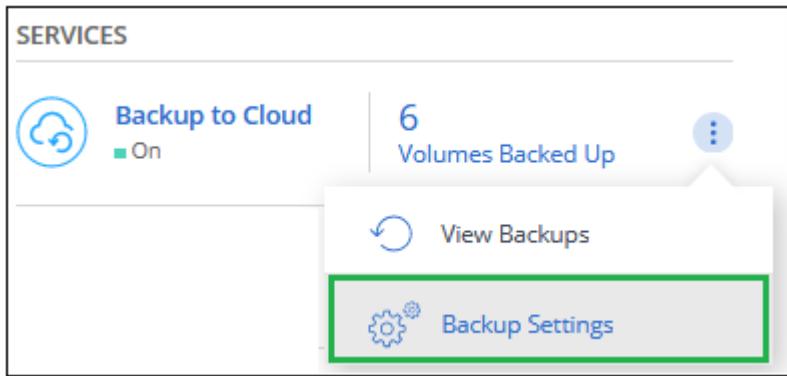


Changing the backup policy affects only new volumes created after you change the schedule. It doesn't affect the schedule for any existing volumes.

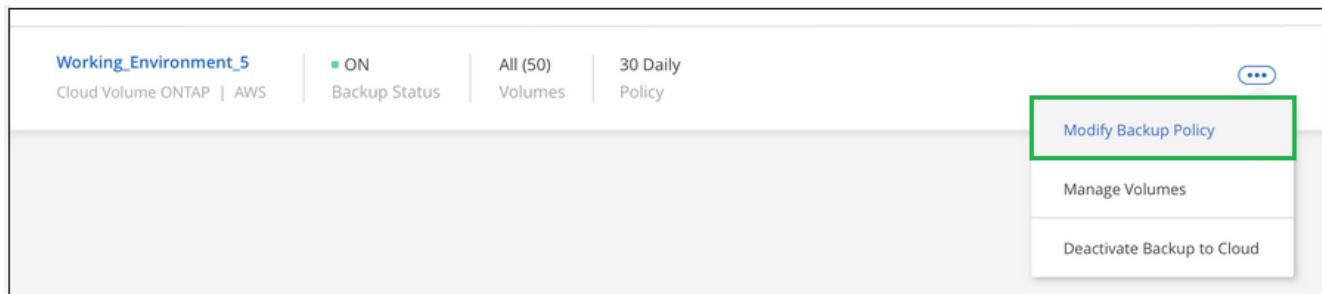
## Steps

1. Select the working environment.

2. Click  and select **Backup Settings**.



3. From the *Backup Settings* page, click  for the working environment and select **Modify Backup Policy**.



4. From the *Modify Backup Policy* page, change the schedule and backup retention and then click **Save**.

**Modify Backup Policy**

**Policy - Retention & Schedule**       Create a New Policy       Select an Existing Policy

Backup Every      Number of backups to retain  
Day      30

**Note:** The new backup policy is only applied to volumes created after the change.  
The backup policy for existing volumes cannot be changed.

**DP Volumes**      Data protection volume backups use the same retention period as defined in the source SnapMirror relationship by default. Use the API if you want to change this value

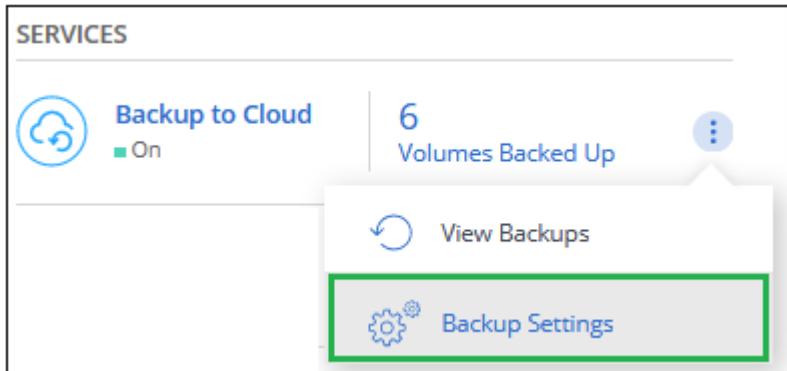
**Information**      Backup\_Bucket\_Name  
Bucket Name

## Starting and stopping backups of volumes

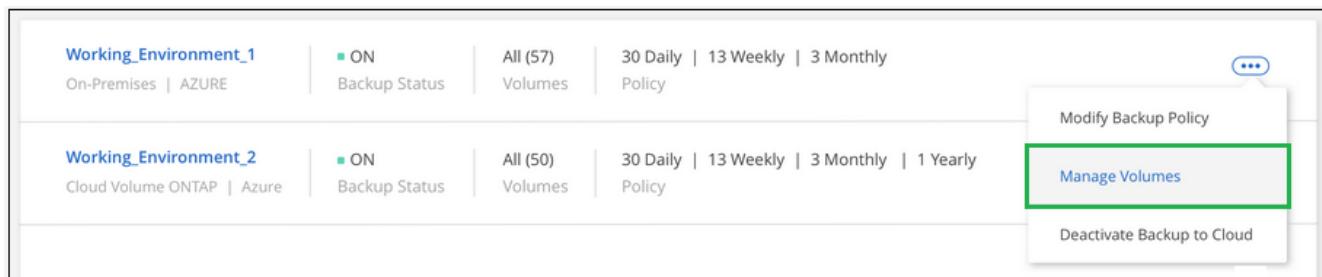
You can stop backing up a volume if you do not need backup copies of that volume and you do not want to pay for the cost to store the backups. You can also add a new volume to the backup list if it is not currently being backed up.

## Steps

1. Select the working environment.
2. Click  and select **Backup Settings**.



3. From the *Backup Settings* page, click  for the working environment and select **Manage Volumes**.



4. Select the checkbox for volumes that you want to start backing up, and deselect the checkbox for volumes that you want to stop backing up.

Manage Volumes						
57 Volumes   25 Selected Volumes						
<input type="checkbox"/>	Volume Name	Volume Type	SVM Name	Used Capacity	Allocated Capacity	Volume Status
<input type="checkbox"/>	Volume_Name_1	RW	SVM_Name_1	2.25 TB	10 TB	Active
<input type="checkbox"/>	Volume_Name_2	RW	SVM_Name_2	2.25 TB	10 TB	Active
<input checked="" type="checkbox"/>	Volume_Name_3	RW	SVM_Name_3	2.25 TB	10 TB	Active
<input type="checkbox"/>	Volume_Name_4	DP 	SVM_Name_4	2.25 TB	10 TB	Active

**Note:** When stopping a volume from being backed up you'll continue to be charged by your cloud provider for object storage costs for the capacity that the backups use unless you [delete the backups](#).

## Deleting backups

Cloud Backup enables you to delete *all* backups of a specific volume. You can't delete *individual* backups. You might do this if you no longer need the backups or if you deleted the source volume and want to remove all backups.

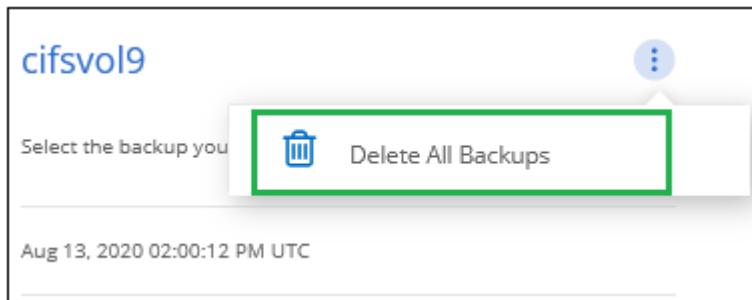
Note that deleting all backups also disables any further backups of this volume. If you later want to start creating backups of that volume, you can re-enable backups [as described here](#).



If you plan to delete a Cloud Volumes ONTAP or on-premises ONTAP system that has backups, you must delete the backups **before** deleting the system. Cloud Backup doesn't automatically delete backups when you delete a system, and there is no current support in the UI to delete the backups after the system has been deleted.

## Steps

1. At the top of Cloud Manager, click **Backup**.
2. From the volume list, find the volume and click **View Backup List**.
3. Click **...** and select **Delete All Backups**.



4. In the confirmation dialog box, click **Delete**.

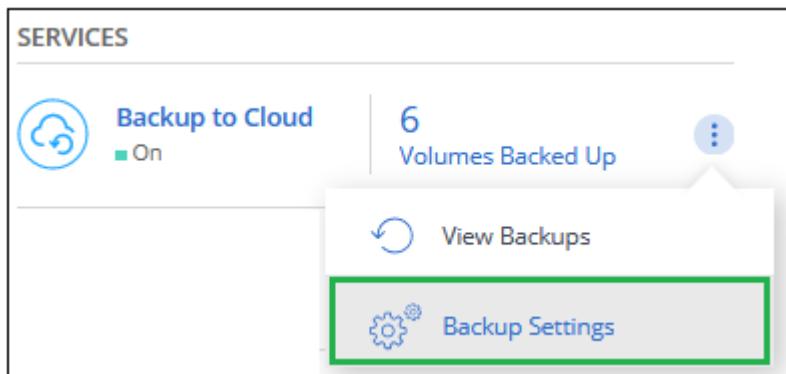
## Disabling Cloud Backup

Disabling Cloud Backup for a working environment disables backups of each volume on the system, and it also disables the ability to restore a volume. Any existing backups will not be deleted.

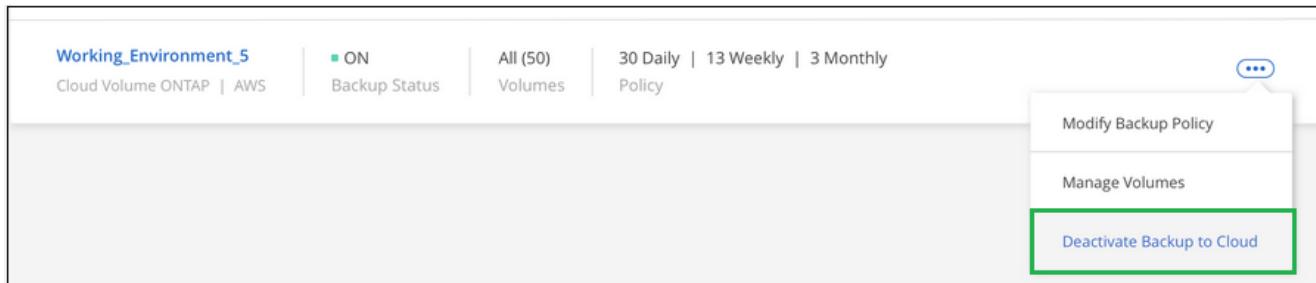
Note that you'll continue to be charged by your cloud provider for object storage costs for the capacity that your backups use unless you delete the backups.

## Steps

1. Select the working environment.
2. Click **...** and select **Backup Settings**.



3. From the *Backup Settings* page, click **...** for the working environment and select **Deactivate Cloud Backup**.



4. In the confirmation dialog box, click **Deactivate**.

## Restoring data from backup files

Backups are stored in an object store in your cloud account so that you can restore data from a specific point in time. You can restore an entire volume from a saved backup file, or if you only need to restore a few files, you can restore up to 8 individual files (at one time) from a saved backup file.

You can restore an entire volume to the same working environment, to a different working environment that's using the same cloud account, or to an on-premises ONTAP system. See [Restoring a volume from a backup](#).

You can restore files to a volume in the same working environment, to a volume in a different working environment that's using the same cloud account, or to a volume on an on-premises ONTAP system. See [Restoring files from a backup](#).

## Supported working environments and object storage providers

You can restore a volume, or individual files, from a backup file to the following working environments:

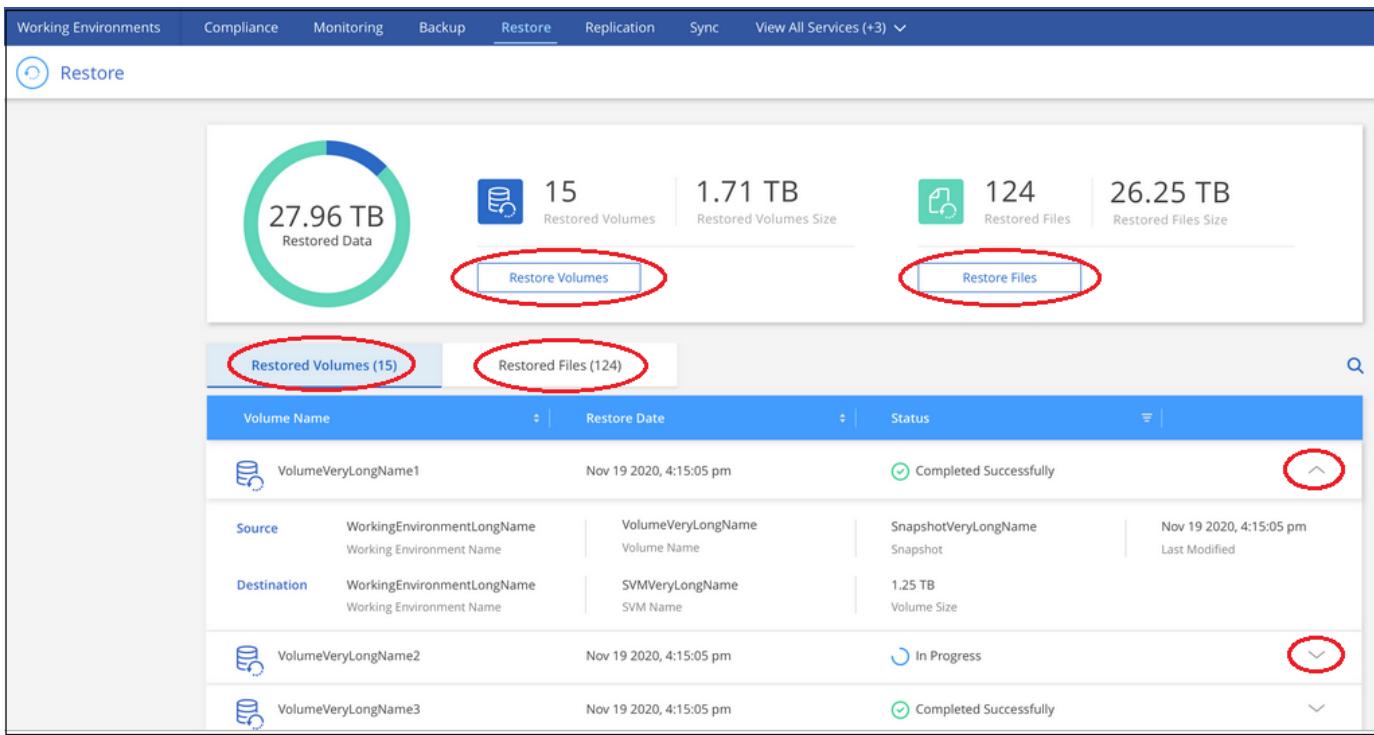
Backup File Location	Destination Working Environment	
	Volume Restore	File Restore
Amazon S3	Cloud Volumes ONTAP in AWS On-premises ONTAP system	Cloud Volumes ONTAP in AWS On-premises ONTAP system
Azure Blob	Cloud Volumes ONTAP in Azure On-premises ONTAP system	Cloud Volumes ONTAP in Azure On-premises ONTAP system
Google Cloud Storage	Cloud Volumes ONTAP in Google On-premises ONTAP system	

## The Restore Dashboard

You access the Restore Dashboard by clicking the **Restore** tab from the top of Cloud Manager, or you can click the **Activate** or **Enable** button for the Restore service from the Services panel.



The Cloud Backup service must already be activated for at least one working environment.



The Restore Dashboard provides buttons for you to restore volumes and files. Clicking the *Restore Volumes* or *Restore Files* buttons starts a wizard that walks you through the steps to restore that data.

The dashboard also provides a list of all the volumes and all the files you have restored in case you need a history of previous restore actions. You can expand the row for each restored volume or file to view the details about the source and destination locations for the volume or file.

## Restoring a volume from a backup file

When you restore a volume from a backup file, Cloud Manager creates a *new* volume using the data from the backup. You can restore the data to a volume in the same working environment or to a different working environment that's located in the same cloud account as the source working environment. You can also restore files to an on-premises ONTAP system.

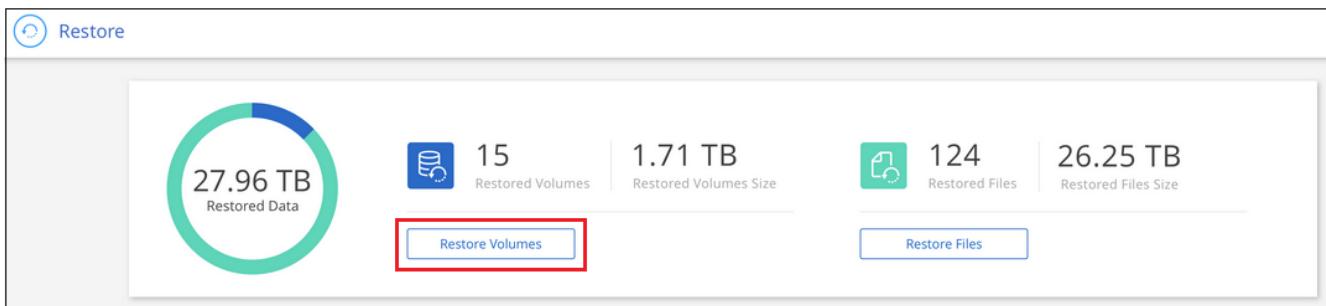
You should know the name of the volume you want to restore and the date of the backup file you want to use to create the newly restored volume.

### Steps

1. Select the **Restore** tab.

The Restore Dashboard appears.

2. Click **Restore Volumes**.



- In the **Select Source** page, navigate to the backup file (snapshot) for the volume you want to restore. Select the **Working Environment**, the **Volume**, and the **Snapshot** that has the date/time stamp that you want to restore.

The 'Select Source' page shows the following steps: 1. Select Source (highlighted with a blue circle) and 2. Select Destination. The left sidebar shows 'Selected Working Environment' (Working Environment Name 3), 'Selected Volume' (Volume Very Long Name), and 'Selected Snapshot > Snapshot Very Long Name'. The main area displays 556 Snapshots with columns for Snapshot Name, Date, and Snapshot Policy. One snapshot is selected: Snapshot Very Long Name (Nov 19 2020, 4:15:05 pm, Weekly).

- Click **Continue**.
- In the **Select Destination** page, select the **Working Environment** where you want to restore the volume.

The 'Select Destination' page shows the following steps: 1. Select Source (highlighted with a blue circle) and 2. Select Destination. The left sidebar shows 'Select Working Environment >' and 'Destination Volume'. The main area displays 5 Working Environments with columns for Working Environment Name, Type, and Provider. One destination is selected: Working Environment Name 2 (Status: On, Cloud Volumes ONTAP, AWS).

- If you select an on-premises ONTAP system and you haven't already configured the cluster connection to the object storage, you are prompted for additional information:
  - When restoring from Amazon S3, enter the IPspace in the ONTAP cluster where the destination volumes reside, and the AWS Access Key and Secret Key needed to access the object storage.

- When restoring from Azure Blob, enter the IPspace in the ONTAP cluster where the destination volumes reside.
  - When restoring from Google Cloud Storage, enter the IPspace in the ONTAP cluster where the destination volumes reside, and the Access Key and Secret Key needed to access the object storage.
7. Select the Storage VM where the volume will reside and enter the name you want to use for the restored volume. By default, <source\_volume\_name>\_Restore is used as the volume name.

You can select the Aggregate that the volume will use for its' capacity when restoring a volume to an on-prem ONTAP system.

8. Click **Restore** and you are returned to the Restore Dashboard so you can review the progress of the restore operation.

## Result

Cloud Manager creates a new volume based on the backup you selected. You can [manage this new volume](#) as required.

## Restoring files from a backup

If you only need to restore a few files from a volume, you can choose to restore individual files instead of restoring the entire volume. You can restore files to a volume in the same working environment, or to a different working environment that's using the same cloud account. You can also restore files to an on-premises ONTAP system.

You can restore up to 8 files at a time from a volume in a backup file. All the files are restored to the same destination volume that you choose. If you need to restore more than 8 files you can run the restore process a second time.



Restoring individual files from a backup file uses a separate Restore instance/virtual machine.

## File Restore process

The process goes like this:

1. When you want to restore one or more files from a volume, click the Restore tab, click **Restore Files**, and select the backup file in which the file (or files) reside.

2. The Restore instance starts up and displays the folders and files that exist within the backup file.

**Note:** The Restore instance is deployed in your cloud providers' environment the first time you restore a file.

3. Choose the file (or files) that you want to restore from that backup.

4. Select the location where you want the file(s) to be restored (the working environment, volume, and folder), and click **Restore**.

5. The file(s) are restored, and then the Restore instance is shut down to save costs after a period of inactivity.

## Details

### Costs

See [this topic](#) for the cost of the Cloud Backup service and the Restore instance.

### Instance type

- In AWS, the Restore instance runs on an [m5n.xlarge instance](#) with 4 CPUs, 16 GiB Memory, and EBS Only instance storage. In regions where m5n.xlarge instance isn't available, Restore runs on an m5.xlarge instance instead.
- In Azure, the Restore virtual machine runs on a [Standard\\_D4s\\_v3 VM](#) with 4 CPUs, 16 GiB Memory, and a 32 GB disk.

The instance is named *Cloud-Restore-Instance* with your Account ID concatenated to it. For example: *Cloud-Restore-Instance-MyAccount*.

## Reviewing prerequisites

Review the following prerequisites to make sure that you have a supported configuration before Cloud Restore is deployed.

### AWS permissions required

When using file Restore with AWS, the IAM role that provides Cloud Manager with permissions must include S3 permissions from the latest [Cloud Manager policy](#) as described in [AWS requirements](#).

Additionally, the following permissions are needed in the policy for file restore:

```
"Action": [
    "ec2:DescribeInstanceTypeOfferings",
    "ec2:startInstances",
    "ec2:stopInstances",
    "ec2:terminateInstances"
],
```

### Enable outbound internet access

Cloud Restore requires outbound internet access. If your virtual or physical network uses a proxy server for internet access, ensure that the instance has outbound internet access to contact the following endpoints. When you deploy Cloud Restore in the cloud, it is located in the same subnet as the Connector.

Review the appropriate table depending on whether you are deploying Cloud Restore in AWS or Azure.

#### Required endpoints for AWS deployments:

Endpoints	Purpose
http://amazonlinux.us-east-1.amazonaws.com/2/extras/docker/stable/x86_64/4bf88ee77c395ffe1e0c3ca68530dfb3a683ec65a4a1ce9c0ff394be50e922b2/	CentOS package for the Cloud Restore Instance AMI.
http://cloudmanagerinfraprod.azurecr.io https://cloudmanagerinfraprod.azurecr.io	Cloud Restore Instance image repository.

#### Required endpoints for Azure deployments:

Endpoints	Purpose
http://olcentgbl.trafficmanager.net https://olcentgbl.trafficmanager.net	Provides CentOS packages for the Cloud Restore virtual machine.
http://cloudmanagerinfraprod.azurecr.io https://cloudmanagerinfraprod.azurecr.io	Cloud Restore Instance image repository.

#### Restoring a single file from a backup file

Follow these steps to restore up to 8 files from a volume backup to a volume. You should know the name of the volume and the date of the backup file that you want to use to restore the file, or files. This functionality uses Live Browsing so that you can view the list of directories and files within the backup file.

Note that the wording in the UI calls each backup file a "snapshot" because backup files are created using NetApp Snapshot technology.

The following video shows a quick walkthrough of restoring a single file:

 | <https://img.youtube.com/vi/ROAY6gPL9N0/maxresdefault.jpg>



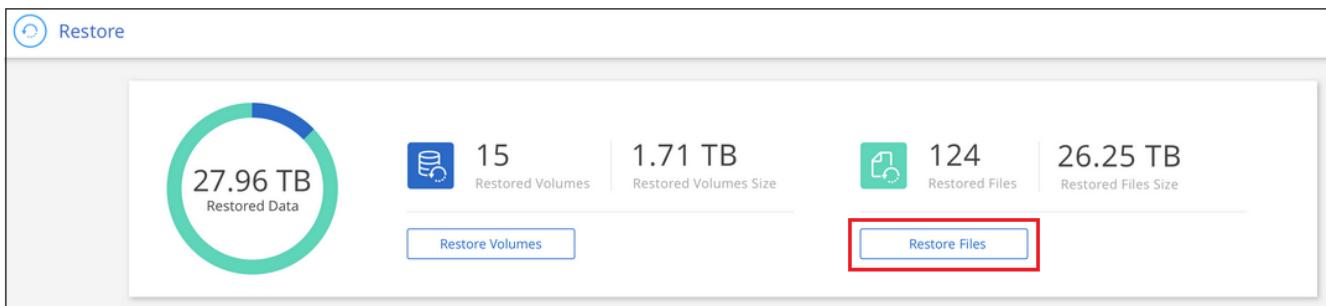
The ONTAP version must be 9.6 or greater in your source and destination ONTAP systems.

#### Steps

1. Click the **Restore** tab.

The Restore Dashboard appears.

2. Click the **Restore Files** button.



- In the **Select Source** page, navigate to the backup file (snapshot) for the volume that contains the files you want to restore. Select the **Working Environment**, the **Volume**, and the **Snapshot** that has the date/time stamp from which you want to restore files.

The screenshot shows the 'Select Source' step of the restore process. On the left, a sidebar lists 'Selected Working Environment' (Working Environment Name 3), 'Selected Volume' (Volume Very Long Name), and a 'Select Snapshot >' option (Snapshot Very Long Name). The 'Selected Volume' and 'Select Snapshot >' sections are highlighted with red boxes. On the right, a table titled '656 Snapshots' lists four entries. The third entry, 'Snapshot Very Long Name' (September 30 2020 00:00:00, NY, USA (GMT-4)), is selected and highlighted with a red box.

- Click **Continue** and the Restore instance is started. After a few minutes the Restore instance displays the list of folders and files from the volume snapshot.

**Note:** The Restore instance is deployed in your cloud providers' environment the first time you restore a file, so this step could take a few minutes longer the first time.

The screenshot shows the 'Select Files' page. On the left, a sidebar shows a selected file 'File D Very Long Name' (Last Modified: September 30 2020 00:00:00, Size: 1.25 MB). On the right, a main panel shows a tree view of 'All Folders & Files' under 'Folder A Very Long Name'. Below it is a table listing files: 'File D Very Long Name' (September 30 2020 00:00:00, 1.25 MB) and 'File E Very Long Name' (September 30 2020 00:00:00, 1.25 MB). A search icon is located at the top right of the main panel.

- In the **Select Files** page, select the file or files that you want to restore and click **Continue**.
  - You can click the search icon and enter the name of the file to navigate directly to the file.
  - You can click the file name if you see it.
  - You can navigate down levels in folders using the button at the end of the row to find the file.

As you select files they are added to the left side of the page so you can see the files that you have already chosen. You can remove a file from this list if needed by clicking the next to the file name.

6. In the **Select Destination** page, select the **Working Environment** where you want to restore the files.

The screenshot shows the 'Select Destination' page with a sidebar on the left containing 'Select Working Environment >', 'Select Volume', and 'Select Folder'. The main area displays a table titled '5 Working Environments' with columns for 'Working Environment Name', 'Type', and 'Provider'. The table lists three environments: 'Working Environment Name 3' (Cloud Volumes ONTAP, Azure), 'Working Environment Name 1' (Cloud Volumes ONTAP, AWS), and 'Working Environment Name 2' (On-Premises). A cursor is hovering over 'Working Environment Name 2'.

Working Environment Name	Type	Provider
Working Environment Name 3	Cloud Volumes ONTAP	Azure
Working Environment Name 1	Cloud Volumes ONTAP	AWS
Working Environment Name 2	On-Premises	---

If you select an on-premises cluster and you haven't already configured the cluster connection to the object storage, you are prompted for additional information:

- When restoring from Amazon S3, enter the IPspace in the ONTAP cluster where the destination volumes reside, and the AWS Access Key and Secret Key needed to access the object storage.
- When restoring from Azure Blob, enter the IPspace in the ONTAP cluster where the destination volumes reside.

7. Then select the **Volume** and the **Folder** where you want to restore the files.

The screenshot shows the 'Select Destination' page with a sidebar on the left containing 'Selected Working Environment Working Environment Name 3', 'Select Volume' (with 'Volume Very Long Name' highlighted by a red box), and 'Select Folder >'. The main area displays a table titled 'Folders' with columns for 'Name', 'Last Modified', and 'Size'. The table lists four folders: 'Folder A Very Long Name' (September 30 2020 00:00:00, ---), 'Folder B Very Long Name' (September 30 2020 00:00:00, ---), 'Folder C Very Long Name' (September 30 2020 00:00:00, ---, highlighted by a red box and a cursor), and 'Folder D Very Long Name' (September 30 2020 00:00:00, ---).

Name	Last Modified	Size
Folder A Very Long Name	September 30 2020 00:00:00	---
Folder B Very Long Name	September 30 2020 00:00:00	---
Folder C Very Long Name	September 30 2020 00:00:00	---
Folder D Very Long Name	September 30 2020 00:00:00	---

You have a few options for the location when restoring files.

- When you have chosen **Select Target Folder**, as shown above:
  - You can select any folder.
  - You can hover over a folder and click at the end of the row to drill down into subfolders, and then select a folder.
- If you have selected the same destination Working Environment and Volume as where the source file was located (as identified by the icon), you can select **Maintain Source Folder Path** to restore the file, or all files, to the same folder where they existed in the source structure. All the same folders and sub-folders must already exist; folders are not created.

8. Click **Restore** and you are returned to the Restore Dashboard so you can review the progress of the restore operation.

The Restore instance is shut down after a certain period of inactivity to save you money so that you incur costs only when it is active.

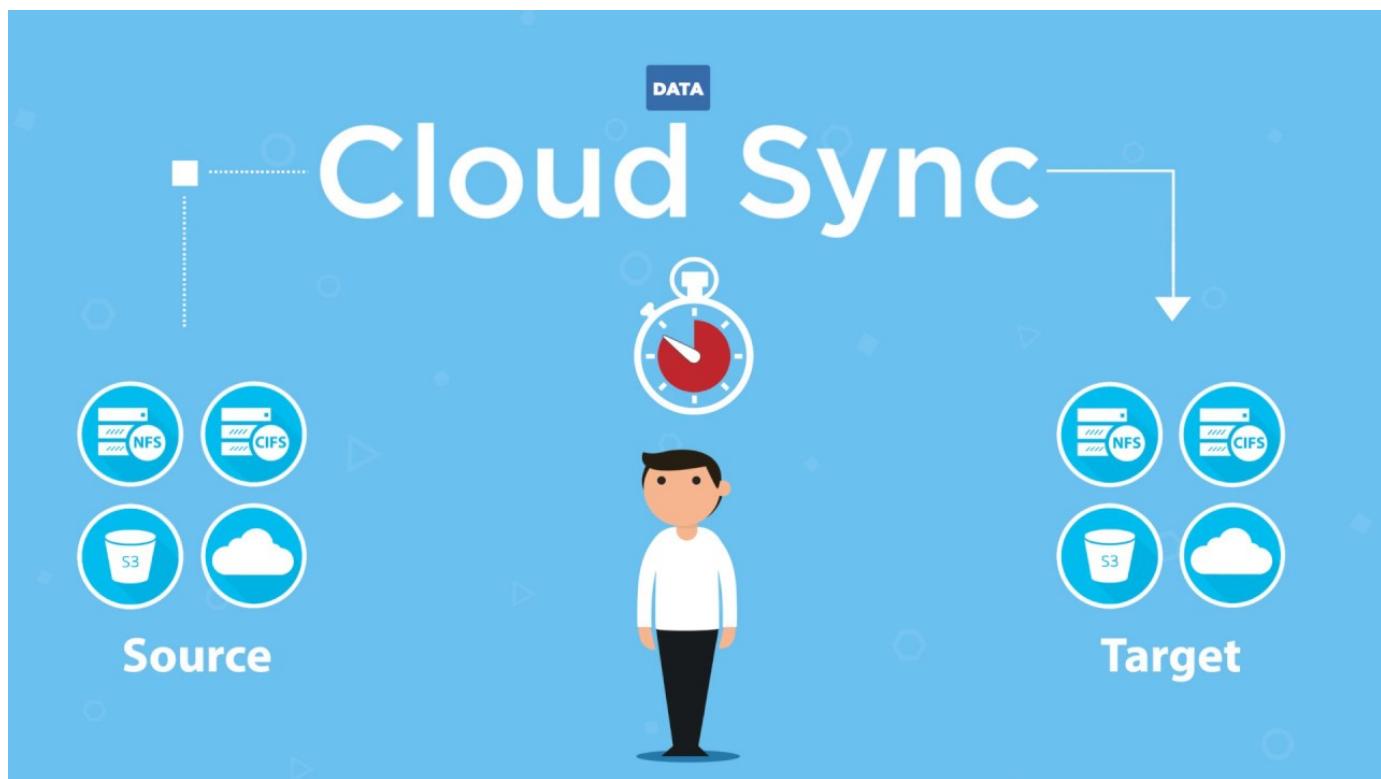
# Copy and synchronize data

## Cloud Sync overview

The NetApp Cloud Sync service offers a simple, secure, and automated way to migrate your data to any target, in the cloud or on your premises. Whether it's a file-based NAS dataset (NFS or SMB), Amazon Simple Storage Service (S3) object format, a NetApp StorageGRID® appliance, or any other cloud provider object store, Cloud Sync can convert and move it for you.

### Features

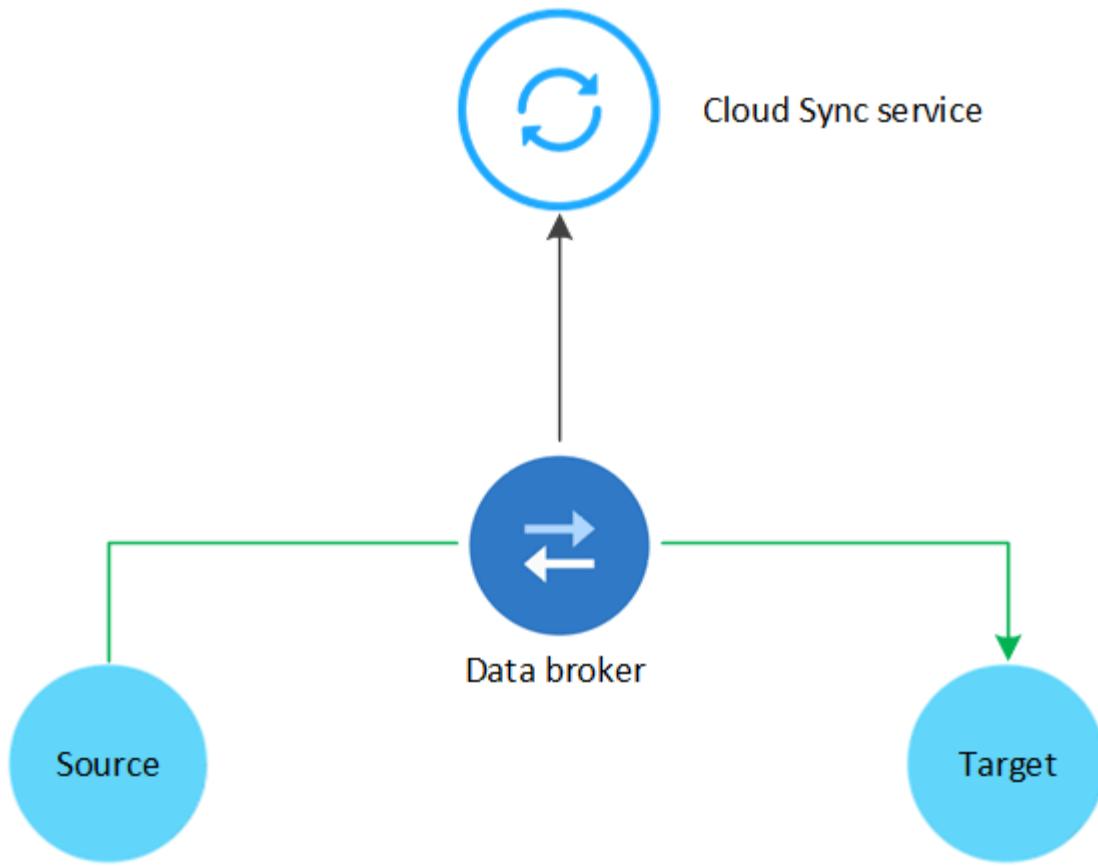
Watch the following video for an overview of Cloud Sync:



### How Cloud Sync works

Cloud Sync is a software-as-a-service (SaaS) platform that consists of a data broker, a cloud-based interface available through Cloud Manager, and a source and target.

The following image shows the relationship between Cloud Sync components:



The NetApp data broker software syncs data from a source to a target (this is called a *sync relationship*). You can run the data broker in AWS, Azure, Google Cloud Platform, or on your premises. The data broker needs an outbound internet connection over port 443 so it can communicate with the Cloud Sync service and contact a few other services and repositories. [View the list of endpoints](#).

After the initial copy, the service syncs any changed data based on the schedule that you set.

## Supported storage types

Cloud Sync supports the following storage types:

- Any NFS server
- Any SMB server
- AWS EFS
- AWS S3
- Azure Blob
- Azure NetApp Files
- Cloud Volumes Service
- Cloud Volumes ONTAP
- Google Cloud Storage
- IBM Cloud Object Storage
- On-premises ONTAP cluster
- ONTAP S3 Storage

- StorageGRID

[Review the supported sync relationships.](#)

## Cost

There are two types of costs associated with using Cloud Sync: resource charges and service charges.

### Resource charges

Resource charges are related to the compute and storage costs for running the data broker in the cloud.

### Service charges

There are two ways to pay for sync relationships after your 14-day free trial ends. The first option is to subscribe from AWS or Azure, which enables you to pay hourly or annually. The second option is to purchase licenses directly from NetApp. Read the following sections for more details.

#### Marketplace subscription

Subscribing to the Cloud Sync service from AWS or Azure enables you to pay at an hourly rate, or to pay annually. [You can subscribe through either AWS or Azure](#), depending on where you want to be billed.

#### Hourly subscriptions

With an hourly pay-as-you-go subscription, the Cloud Sync service charges hourly based on the number of sync relationships that you create.

- [View pricing in Azure](#)
- [View pay-as-you-go pricing in AWS](#)

#### Annual subscriptions

An annual subscription provides a license for 20 sync relationships that you pay for up front. If you go above 20 sync relationships and you've subscribed through Azure, you pay for the additional relationships by the hour.

[View annual pricing in AWS](#)

#### Licenses from NetApp

Another way to pay for sync relationships up front is by purchasing licenses directly from NetApp. Each license enables you to create up to 20 sync relationships.

You can use these licenses with an AWS or Azure subscription. For example, if you have 25 sync relationships, you can pay for the first 20 sync relationships using a license and then pay-as-you-go from AWS or Azure with the remaining 5 sync relationships.

[Learn how to purchase licenses and add them to Cloud Sync.](#)

#### License terms

Customers who purchase a Bring Your Own License (BYOL) to the Cloud Sync service should be aware of limitations associated with the license entitlement.

- Customers are entitled to leverage the BYOL license for a term not to exceed one year from the date of delivery.

- Customers are entitled to leverage the BYOL license to establish and not to exceed a total of 20 individual connections between a source and a target (each a “sync relationship”).
- A customer’s entitlement expires at the conclusion of the one-year license term, irrespective as to whether Customer has reached the 20 sync relationship limitation.
- In the event the Customer chooses to renew its license, unused sync relationships associated from the previous license grant DO NOT roll over to the license renewal.

## Data privacy

NetApp doesn’t have access to any credentials that you provide while using the Cloud Sync service. The credentials are stored directly on the data broker machine, which resides in your network.

Depending on the configuration that you choose, Cloud Sync might prompt you for credentials when you create a new relationship. For example, when setting up a relationship that includes an SMB server, or when deploying the data broker in AWS.

These credentials are always saved directly to the data broker itself. The data broker resides on a machine in your network, whether it’s on premises or in your cloud account. The credentials are never made available to NetApp.

The credentials are locally encrypted on the data broker machine using HashiCorp Vault.

## Limitations

- Cloud Sync is not supported in China.
- In addition to China, the Cloud Sync data broker is not supported in the following regions:
  - AWS GovCloud (US)
  - Azure US Gov
  - Azure US DoD

## Get started

### Quick start for Cloud Sync

Getting started with the Cloud Sync service includes a few steps.



#### Prepare your source and target

Verify that your source and target are supported and set up. The most important requirement is to verify connectivity between the data broker and the source and target locations. [Learn more](#).



#### Prepare a location for the NetApp data broker

The NetApp data broker software syncs data from a source to a target (this is called a *sync relationship*). You can run the data broker in AWS, Azure, Google Cloud Platform, or on your premises. The data broker needs an outbound internet connection over port 443 so it can communicate with the Cloud Sync service and contact a few other services and repositories. [View the list of endpoints](#).

Cloud Sync guides you through the installation process when you create a sync relationship, at which point you can deploy the data broker in the cloud or download an install script for your own Linux host.

- [Review AWS installation](#)
- [Review Azure installation](#)
- [Review GCP installation](#)
- [Review Linux host installation](#)



### Create your first sync relationship

Log in to [Cloud Manager](#), click **Sync**, and then drag and drop your selections for the source and target. Follow the prompts to complete the setup. [Learn more](#).



### Pay for your sync relationships after your free trial ends

Subscribe from AWS or Azure to pay-as-you-go or to pay annually. Or purchase licenses directly from NetApp. Just go to the License Settings page in Cloud Sync to set it up. [Learn more](#).

## Preparing the source and target

Prepare to sync data by verifying that your source and target are supported and setup.

### Supported sync relationships

Cloud Sync enables you to sync data from a source to a target (this is called a *sync relationship*). You should understand the supported relationships before you get started.

Source location	Supported target locations
AWS EFS	<ul style="list-style-type: none"><li>• AWS EFS</li><li>• AWS S3</li><li>• Azure Blob</li><li>• Azure NetApp Files (NFS)</li><li>• Cloud Volumes ONTAP (NFS)</li><li>• Cloud Volumes Service (NFS)</li><li>• IBM Cloud Object Storage</li><li>• Google Cloud Storage</li><li>• NFS server</li><li>• On-premises ONTAP cluster</li><li>• StorageGRID</li></ul>

Source location	Supported target locations
AWS S3	<ul style="list-style-type: none"> <li>• AWS EFS</li> <li>• AWS S3</li> <li>• Azure Blob</li> <li>• Azure NetApp Files</li> <li>• Cloud Volumes ONTAP</li> <li>• Cloud Volumes Service</li> <li>• IBM Cloud Object Storage</li> <li>• Google Cloud Storage</li> <li>• NFS server</li> <li>• On-premises ONTAP cluster</li> <li>• SMB Server</li> <li>• StorageGRID</li> </ul>
Azure Blob	<ul style="list-style-type: none"> <li>• AWS EFS</li> <li>• AWS S3</li> <li>• Azure Blob</li> <li>• Azure NetApp Files</li> <li>• Cloud Volumes ONTAP</li> <li>• Cloud Volumes Service</li> <li>• Google Cloud Storage</li> <li>• IBM Cloud Object Storage</li> <li>• NFS server</li> <li>• On-premises ONTAP cluster</li> <li>• SMB Server</li> <li>• StorageGRID</li> </ul>

Source location	Supported target locations
Azure NetApp Files (NFS)	<ul style="list-style-type: none"> <li>• AWS EFS</li> <li>• AWS S3</li> <li>• Azure Blob</li> <li>• Azure NetApp Files (NFS)</li> <li>• Cloud Volumes ONTAP (NFS)</li> <li>• Cloud Volumes Service (NFS)</li> <li>• IBM Cloud Object Storage</li> <li>• Google Cloud Storage</li> <li>• NFS server</li> <li>• On-premises ONTAP cluster</li> <li>• StorageGRID</li> </ul>
Azure NetApp Files (SMB)	<ul style="list-style-type: none"> <li>• AWS S3</li> <li>• Azure Blob</li> <li>• Azure NetApp Files (SMB)</li> <li>• Cloud Volumes ONTAP (SMB)</li> <li>• Cloud Volumes Service (SMB)</li> <li>• Google Cloud Storage</li> <li>• IBM Cloud Object Storage</li> <li>• On-premises ONTAP cluster</li> <li>• SMB Server</li> <li>• StorageGRID</li> </ul>
Cloud Volumes ONTAP (NFS)	<ul style="list-style-type: none"> <li>• AWS EFS</li> <li>• AWS S3</li> <li>• Azure Blob</li> <li>• Azure NetApp Files (NFS)</li> <li>• Cloud Volumes ONTAP (NFS)</li> <li>• Cloud Volumes Service (NFS)</li> <li>• IBM Cloud Object Storage</li> <li>• Google Cloud Storage</li> <li>• NFS server</li> <li>• On-premises ONTAP cluster</li> <li>• StorageGRID</li> </ul>

Source location	Supported target locations
Cloud Volumes ONTAP (SMB)	<ul style="list-style-type: none"> <li>• AWS S3</li> <li>• Azure Blob</li> <li>• Azure NetApp Files (SMB)</li> <li>• Cloud Volumes ONTAP (SMB)</li> <li>• Cloud Volumes Service (SMB)</li> <li>• Google Cloud Storage</li> <li>• IBM Cloud Object Storage</li> <li>• On-premises ONTAP cluster</li> <li>• SMB Server</li> <li>• StorageGRID</li> </ul>
Cloud Volumes Service (NFS)	<ul style="list-style-type: none"> <li>• AWS EFS</li> <li>• AWS S3</li> <li>• Azure Blob</li> <li>• Azure NetApp Files (NFS)</li> <li>• Cloud Volumes ONTAP (NFS)</li> <li>• Cloud Volumes Service (NFS)</li> <li>• IBM Cloud Object Storage</li> <li>• Google Cloud Storage</li> <li>• NFS server</li> <li>• On-premises ONTAP cluster</li> <li>• StorageGRID</li> </ul>
Cloud Volumes Service (SMB)	<ul style="list-style-type: none"> <li>• AWS S3</li> <li>• Azure Blob</li> <li>• Azure NetApp Files (SMB)</li> <li>• Cloud Volumes ONTAP (SMB)</li> <li>• Cloud Volumes Service (SMB)</li> <li>• Google Cloud Storage</li> <li>• IBM Cloud Object Storage</li> <li>• On-premises ONTAP cluster</li> <li>• SMB Server</li> <li>• StorageGRID</li> </ul>

Source location	Supported target locations
Google Cloud Storage	<ul style="list-style-type: none"> <li>• AWS EFS</li> <li>• AWS S3</li> <li>• Azure Blob</li> <li>• Azure NetApp Files</li> <li>• Cloud Volumes ONTAP</li> <li>• Cloud Volumes Service</li> <li>• Google Cloud Storage</li> <li>• IBM Cloud Object Storage</li> <li>• NFS server</li> <li>• On-premises ONTAP cluster</li> <li>• SMB Server</li> <li>• StorageGRID</li> </ul>
IBM Cloud Object Storage	<ul style="list-style-type: none"> <li>• AWS EFS</li> <li>• AWS S3</li> <li>• Azure Blob</li> <li>• Azure NetApp Files</li> <li>• Cloud Volumes ONTAP</li> <li>• Cloud Volumes Service</li> <li>• Google Cloud Storage</li> <li>• IBM Cloud Object Storage</li> <li>• NFS server</li> <li>• On-premises ONTAP cluster</li> <li>• SMB Server</li> <li>• StorageGRID</li> </ul>

Source location	Supported target locations
NFS server	<ul style="list-style-type: none"> <li>• AWS EFS</li> <li>• AWS S3</li> <li>• Azure Blob</li> <li>• Azure NetApp Files (NFS)</li> <li>• Cloud Volumes ONTAP (NFS)</li> <li>• Cloud Volumes Service (NFS)</li> <li>• IBM Cloud Object Storage</li> <li>• Google Cloud Storage</li> <li>• NFS server</li> <li>• On-premises ONTAP cluster</li> <li>• StorageGRID</li> </ul>
On-prem ONTAP cluster (NFS)	<ul style="list-style-type: none"> <li>• AWS EFS</li> <li>• AWS S3</li> <li>• Azure Blob</li> <li>• Azure NetApp Files (NFS)</li> <li>• Cloud Volumes ONTAP (NFS)</li> <li>• Cloud Volumes Service (NFS)</li> <li>• IBM Cloud Object Storage</li> <li>• Google Cloud Storage</li> <li>• NFS server</li> <li>• On-premises ONTAP cluster</li> <li>• StorageGRID</li> </ul>
On-prem ONTAP cluster (SMB)	<ul style="list-style-type: none"> <li>• AWS S3</li> <li>• Azure Blob</li> <li>• Azure NetApp Files (SMB)</li> <li>• Cloud Volumes ONTAP (SMB)</li> <li>• Cloud Volumes Service (SMB)</li> <li>• Google Cloud Storage</li> <li>• IBM Cloud Object Storage</li> <li>• On-premises ONTAP cluster</li> <li>• SMB Server</li> <li>• StorageGRID</li> </ul>

Source location	Supported target locations
ONTAP S3 Storage	<ul style="list-style-type: none"> <li>• StorageGRID</li> <li>• ONTAP S3 Storage</li> </ul>
SFTP <sup>1</sup>	S3
SMB server	<ul style="list-style-type: none"> <li>• AWS S3</li> <li>• Azure Blob</li> <li>• Azure NetApp Files (SMB)</li> <li>• Cloud Volumes ONTAP (NFS)</li> <li>• Cloud Volumes Service (NFS)</li> <li>• IBM Cloud Object Storage</li> <li>• Google Cloud Storage</li> <li>• On-premises ONTAP cluster</li> <li>• SMB Server</li> <li>• StorageGRID</li> </ul>
StorageGRID	<ul style="list-style-type: none"> <li>• AWS EFS</li> <li>• AWS S3</li> <li>• Azure Blob</li> <li>• Azure NetApp Files</li> <li>• Cloud Volumes ONTAP</li> <li>• Cloud Volumes Service</li> <li>• IBM Cloud Object Storage</li> <li>• Google Cloud Storage</li> <li>• NFS server</li> <li>• On-premises ONTAP cluster</li> <li>• ONTAP S3 Storage</li> <li>• SMB Server</li> <li>• StorageGRID</li> </ul>

Notes:

1. Cloud Sync supports sync relationships from SFTP to S3 by using the API only.
2. You can choose a specific Azure Blob storage tier when a Blob container is the target:
  - Hot storage
  - Cool storage
3. You can choose a specific S3 storage class when AWS S3 is the target:
  - Standard (this is the default class)

- Intelligent-Tiering
- Standard-Infrequent Access
- One Zone-Infrequent Access
- Glacier
- Glacier Deep Archive

## Networking for the source and target

- The source and target must have a network connection to the data broker.

For example, if an NFS server is in your data center and the data broker is in AWS, then you need a network connection (VPN or Direct Connect) from your network to the VPC.

- NetApp recommends configuring the source, target, and data broker to use a Network Time Protocol (NTP) service. The time difference between the three components should not exceed 5 minutes.

## Source and target requirements

Verify that your source and targets meet the following requirements.

### AWS S3 bucket requirements

Make sure that your AWS S3 bucket meets the following requirements.

### Supported data broker locations for AWS S3

Sync relationships that include S3 storage require a data broker deployed in AWS or on your premises. In either case, Cloud Sync prompts you to associate the data broker with an AWS account during installation.

- [Learn how to deploy the AWS data broker](#)
- [Learn how to install the data broker on a Linux host](#)

### Supported AWS regions

All regions are supported except for the China and GovCloud (US) regions.

### Permissions required for S3 buckets in other AWS accounts

When setting up a sync relationship, you can specify an S3 bucket that resides in an AWS account that isn't associated with the data broker.

[The permissions included in this JSON file](#) must be applied to that S3 bucket so the data broker can access it. These permissions enable the data broker to copy data to and from the bucket and to list the objects in the bucket.

Note the following about the permissions included in the JSON file:

1. <BucketName> is the name of the bucket that resides in the AWS account that isn't associated with the data broker.
2. <RoleARN> should be replaced with one of the following:
  - If the data broker was manually installed on a Linux host, *RoleARN* should be the ARN of the AWS user for which you provided AWS credentials when deploying the data broker.

- If the data broker was deployed in AWS using the CloudFormation template, *RoleARN* should be the ARN of the IAM role created by the template.

You can find the Role ARN by going to the EC2 console, selecting the data broker instance, and clicking the IAM role from the Description tab. You should then see the Summary page in the IAM console that contains the Role ARN.

The screenshot shows the 'Summary' page for an IAM role. At the top right is a 'Delete role' button. Below it, the 'Role ARN' field is highlighted with a red box and contains the value 'arn:aws:iam::[REDACTED]:role/tanyaBroker0304-DataBrokerIamRole-1VMHWXMW3AQ05'. Below the ARN are two buttons: 'Role description' and 'Edit'.

### Azure Blob storage requirements

Make sure that your Azure Blob storage meets the following requirements.

### Supported data broker locations for Azure Blob

The data broker can reside in any location when a sync relationship includes Azure Blob storage.

### Supported Azure regions

All regions are supported except for the China, US Gov, and US DoD regions.

### Connection string required for relationships that include Azure Blob and NFS/SMB

When creating a sync relationship between an Azure Blob container and an NFS or SMB server, you need to provide Cloud Sync with the storage account connection string:

The screenshot shows the 'Access keys' page for an Azure storage account named 'a63cde60b553020'. The left sidebar has a 'Settings' section with 'Access keys' selected, indicated by a red box. Other options in the sidebar include 'Overview', 'Activity log', 'Access control (IAM)', 'Tags', 'Diagnose and solve problems', and 'Storage Explorer (preview)'. The main content area shows the 'key1' access key details. The 'Key' field contains 'vScjFdVZqIPyO/'. Below it, the 'Connection string' field contains 'DefaultEndpoints'. Both fields have a red box around them. A note on the right says: 'Use access keys to authenticate your applications when making requests to this Azure storage account. Store your access keys securely - for example, using Azure Key Vault - and don't share them. We recommend regenerating your access keys regularly. You are provided two access keys so that you can maintain connections using one key while regenerating the other.' It also mentions that regenerating keys will update resources and applications.

If you want to sync data between two Azure Blob containers, then the connection string must include a [shared access signature \(SAS\)](#). You also have the option to use a SAS when syncing between a Blob container and

an NFS or SMB server.

The SAS must allow access to the Blob service and all resource types (Service, Container, and Object). The SAS must also include the following permissions:

- For the source Blob container: Read and List
- For the target Blob container: Read, Write, List, Add, and Create

The screenshot shows the Azure Storage account settings for a storage account named 'a63cde60b553020'. The 'Shared access signature' section is highlighted with a red box. Inside this box, the 'Allowed services', 'Allowed resource types', and 'Allowed permissions' sections are also highlighted with a red border. Below this, the 'Start and expiry date/time' and 'Allowed IP addresses' sections are shown. At the bottom of the page, the 'Generate SAS and connection string' button is highlighted with a red box.

**Shared access signature**

**Allowed services**

Blob  File  Queue  Table

**Allowed resource types**

Service  Container  Object

**Allowed permissions**

Read  Write  Delete  List  Add  Create  Update  Process

**Start and expiry date/time**

Start: 2018-10-23 10:07:32 AM

End: 2019-10-23 6:07:32 PM  
(UTC-04:00) --- Current Time Zone ---

**Allowed IP addresses**

for example, 168.1.5.65 or 168.1.5.65-168.1.5.70

**Allowed protocols**

HTTPS only  HTTPS and HTTP

**Signing key**

key1

**Generate SAS and connection string**

#### Azure NetApp Files requirement

Use the Premium or Ultra service level when you sync data to or from Azure NetApp Files. You might experience failures and performance issues if the disk service level is Standard.



Consult a solutions architect if you need help determining the right service level. The volume size and volume tier determines the throughput that you can get.

[Learn more about Azure NetApp Files service levels and throughput.](#)

#### Google Cloud Storage bucket requirements

Make sure that your Google Cloud Storage bucket meets the following requirements.

## Supported data broker locations for Google Cloud Storage

Sync relationships that include Google Cloud Storage require a data broker deployed in GCP or on your premises. Cloud Sync guides you through the data broker installation process when you create a sync relationship.

- [Learn how to deploy the GCP data broker](#)
- [Learn how to install the data broker on a Linux host](#)

## Supported GCP regions

All regions are supported.

### ONTAP requirements

If the sync relationship includes Cloud Volumes ONTAP or an on-prem ONTAP cluster and you selected NFSv4 or later, then you'll need to enable NFSv4 ACLs on the ONTAP system. This is required to copy the ACLs.

### NFS server requirements

- The NFS server can be a NetApp system or a non-NetApp system.
- The file server must allow the data broker host to access the exports.
- NFS versions 3, 4.0, 4.1, and 4.2 are supported.

The desired version must be enabled on the server.

- If you want to sync NFS data from an ONTAP system, ensure that access to the NFS export list for an SVM is enabled (`vserver nfs modify -vserver svm_name -showmount enabled`).



The default setting for showmount is `enabled` starting with ONTAP 9.2.

### ONTAP S3 Storage requirements

When you set up a sync relationship that includes [ONTAP S3 Storage](#), you'll need to provide the following:

- The IP address of the LIF that's connected to ONTAP S3
- The access key and secret key that ONTAP is configured to use

### SMB server requirements

- The SMB server can be a NetApp system or a non-NetApp system.
- The file server must allow the data broker host to access the exports.
- SMB versions 1.0, 2.0, 2.1, 3.0 and 3.11 are supported.
- Grant the "Administrators" group with "Full Control" permissions to the source and target folders.

If you don't grant this permission, then the data broker might not have sufficient permissions to get the ACLs on a file or directory. If this occurs, you'll receive the following error: "getxattr error 95"

## SMB limitation for hidden directories and files

An SMB limitation affects hidden directories and files when syncing data between SMB servers. If any of the directories or files on the source SMB server were hidden through Windows, the hidden attribute isn't copied to the target SMB server.

## SMB sync behavior due to case-insensitivity limitation

The SMB protocol is case-insensitive, which means uppercase and lowercase letters are treated as being the same. This behavior can result in overwritten files and directory copy errors, if a sync relationship includes an SMB server and data already exists on the target.

For example, let's say that there's a file named "a" on the source and a file named "A" on the target. When Cloud Sync copies the file named "a" to the target, file "A" is overwritten by file "a" from the source.

In the case of directories, let's say that there's a directory named "b" on the source and a directory named "B" on the target. When Cloud Sync tries to copy the directory named "b" to the target, Cloud Sync receives an error that says the directory already exists. As a result, Cloud Sync always fails to copy the directory named "b."

The best way to avoid this limitation is to ensure that you sync data to an empty directory.

## Permissions for a SnapMirror destination

If the source for a sync relationship is a SnapMirror destination (which is read-only), "read/list" permissions are sufficient to sync data from the source to a target.

## Networking overview for Cloud Sync

Networking for Cloud Sync includes connectivity between the data broker and the source and target locations, and an outbound internet connection from the data broker over port 443.

### Data broker location

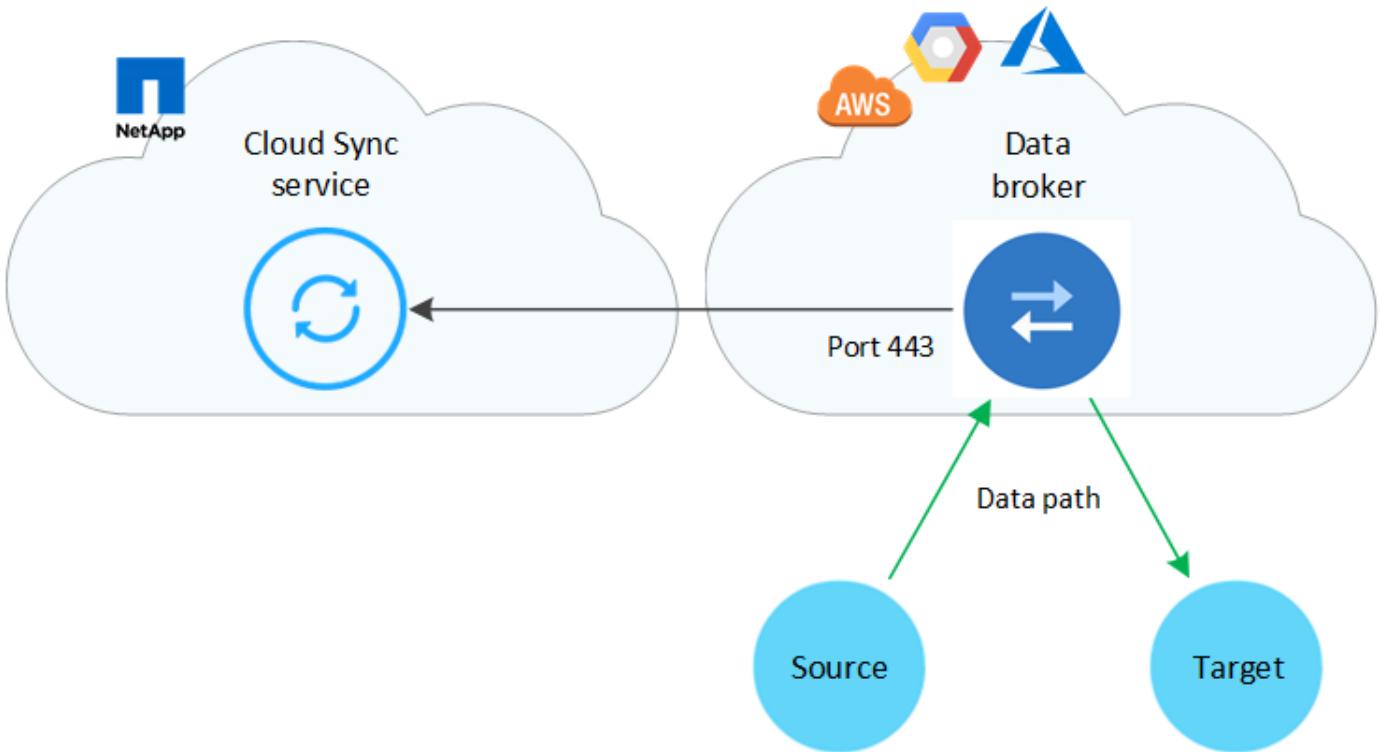
You can install the data broker in the cloud or on your premises.

#### Data broker in the cloud

The following image shows the data broker running in the cloud, in either AWS, GCP, or Azure. The source and target can be in any location, as long as there's a connection to the data broker. For example, you might have a VPN connection from your data center to your cloud provider.

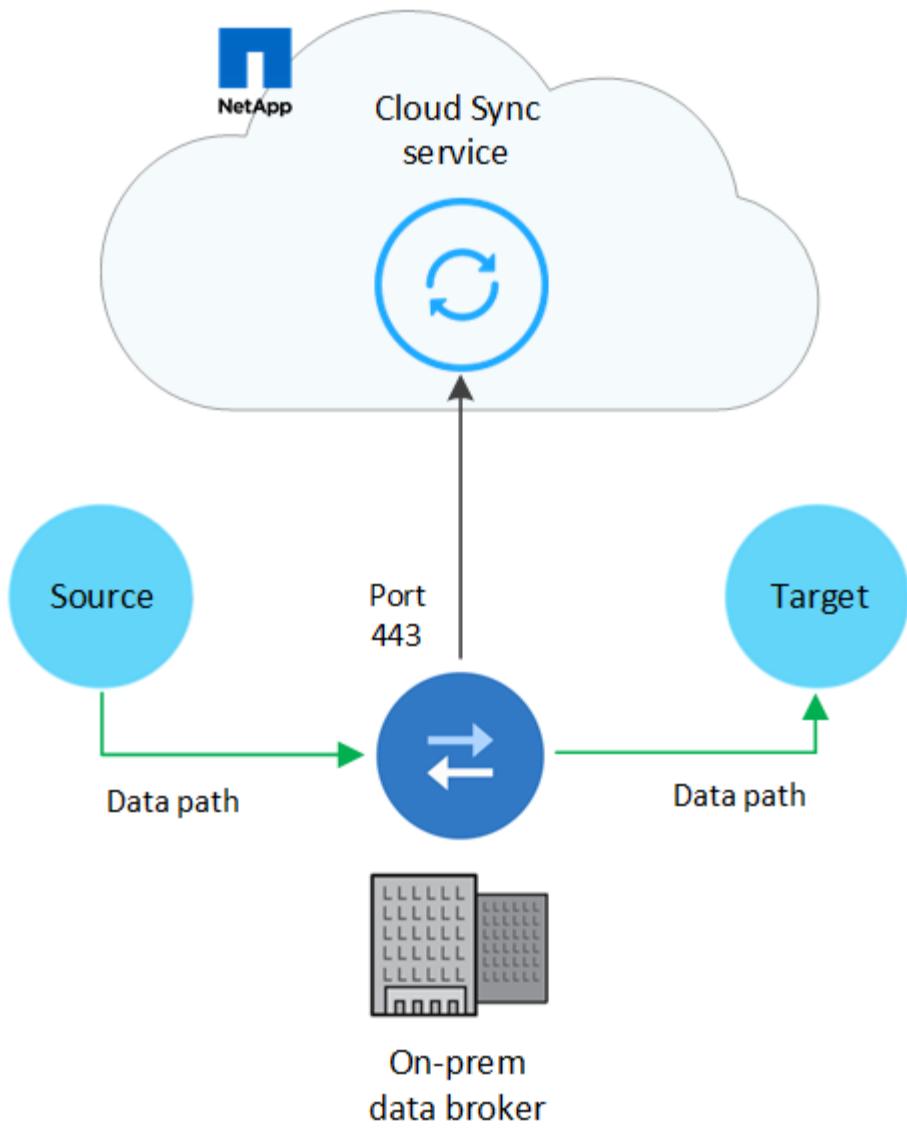


When Cloud Sync deploys the data broker in AWS, Azure, or GCP, it creates a security group that enables the required outbound communication.



#### Data broker on your premises

The following image shows the data broker running on-prem, in a data center. Again, the source and target can be in any location, as long as there's a connection to the data broker.



## Networking requirements

- The source and target must have a network connection to the data broker.

For example, if an NFS server is in your data center and the data broker is in AWS, then you need a network connection (VPN or Direct Connect) from your network to the VPC.

- The data broker needs an outbound internet connection so it can poll the Cloud Sync service for tasks over port 443.
- NetApp recommends configuring the source, target, and data broker to use a Network Time Protocol (NTP) service. The time difference between the three components should not exceed 5 minutes.

## Networking endpoints

The NetApp data broker requires outbound internet access over port 443 to communicate with the Cloud Sync service and to contact a few other services and repositories. Your local web browser also requires access to endpoints for certain actions. If you need to limit outbound connectivity, refer to the following list of endpoints when configuring your firewall for outbound traffic.

## Data broker endpoints

The data broker contacts the following endpoints:

Endpoints	Purpose
olcentgbl.trafficmanager.net:443	To contact a repository for updating CentOS packages for the data broker host. This endpoint is contacted only if you manually install the data broker on a CentOS host.
rpm.nodesource.com:443 registry.npmjs.org:443 nodejs.org:443	To contact repositories for updating Node.js, npm, and other 3rd party packages used in development.
tgz.pm2.io:443	To access a repository for updating PM2, which is a 3rd party package used to monitor Cloud Sync.
sqs.us-east-1.amazonaws.com:443 kinesis.us-east-1.amazonaws.com:443	To contact the AWS services that Cloud Sync uses for operations (queuing files, registering actions, and delivering updates to the data broker).
s3.region.amazonaws.com:443  For example: s3.us-east-2.amazonaws.com:443 <a href="#">See AWS documentation for a list of S3 endpoints</a>	To contact Amazon S3 when a sync relationship includes an S3 bucket.
cf.cloudsync.netapp.com:443 repo.cloudsync.netapp.com:443	To contact the Cloud Sync service.
support.netapp.com:443	To contact NetApp support when using a BYOL license for sync relationships.
fedoraproject.org:443	To install 7z on the data broker virtual machine during installation and updates. 7z is needed to send AutoSupport messages to NetApp technical support.
sts.amazonaws.com:443	To verify AWS credentials when the data broker is deployed in AWS or when it's deployed on your premises and AWS credentials are provided. The data broker contacts this endpoint during deployment, when it's updated, and when it's restarted.

## Web browser endpoints

Your web browser needs access to the following endpoint to download logs for troubleshooting purposes:

logs.cloudsync.netapp.com:443

## How to install a data broker

### Installing the data broker in AWS

When you create a new data broker, choose the AWS Data Broker option to deploy the data broker software on a new EC2 instance in a VPC. Cloud Sync guides you through the installation process, but the requirements and steps are repeated on this page to help you prepare for installation.

You also have the option to install the data broker on an existing Linux host in the cloud or on your premises. [Learn more](#).

## Supported AWS regions

All regions are supported except for the China and GovCloud (US) regions.

## Networking requirements

- The data broker needs an outbound internet connection so it can poll the Cloud Sync service for tasks over port 443.

When Cloud Sync deploys the data broker in AWS, it creates a security group that enables the required outbound communication. Note that you can configure the data broker to use a proxy server during the installation process.

If you need to limit outbound connectivity, see [the list of endpoints that the data broker contacts](#).

- NetApp recommends configuring the source, target, and data broker to use a Network Time Protocol (NTP) service. The time difference between the three components should not exceed 5 minutes.

## Permissions required to deploy the data broker in AWS

The AWS user account that you use to deploy the data broker must have the permissions included in [this NetApp-provided policy](#).

### Requirements to use your own IAM role with the AWS data broker

When Cloud Sync deploys the data broker, it creates an IAM role for the data broker instance. You can deploy the data broker using your own IAM role, if you prefer. You might use this option if your organization has strict security policies.

The IAM role must meet the following requirements:

- The EC2 service must be allowed to assume the IAM role as a trusted entity.
- [The permissions defined in this JSON file](#) must be attached to the IAM role so the data broker can function properly.

Follow the steps below to specify the IAM role when deploying the data broker.

## Installing the data broker

You can install a data broker in AWS when you create a sync relationship.

### Steps

- Click **Create New Sync**.
- On the **Define Sync Relationship** page, choose a source and target and click **Continue**.

Complete the steps until you reach the **Data Broker** page.

- On the **Data Broker** page, click **Create Data Broker** and then select **Amazon Web Services**.

If you already have a data broker, you'll need to click the  icon first.

4. Enter a name for the data broker and click **Continue**.
5. Enter an AWS access key so Cloud Sync can create the data broker in AWS on your behalf.

The keys aren't saved or used for any other purposes.

If you'd rather not provide access keys, click the link at the bottom of the page to use a CloudFormation template instead. When you use this option, you don't need to provide credentials because you are logging in directly to AWS.

The following video shows how to launch the data broker instance using a CloudFormation template:

▶ [https://docs.netapp.com/us-en/occm/media/video\\_cloud\\_sync.mp4](https://docs.netapp.com/us-en/occm/media/video_cloud_sync.mp4) (video)

6. If you entered an AWS access key, select a location for the instance, select a key pair, choose whether to enable a public IP address, and then select an existing IAM role, or leave the field blank so Cloud Sync creates the role for you.

If you choose your own IAM role, [you'll need to provide the required permissions](#).

### Basic Settings

<b>Location</b>	<b>Connectivity</b>
Region <div style="border: 1px solid #ccc; padding: 2px; width: 100%;">US West   Oregon ▾</div>	Key Pair <div style="border: 1px solid #ccc; padding: 2px; width: 100%;">newKey ▾</div>
VPC <div style="border: 1px solid #ccc; padding: 2px; width: 100%;">vpc-3c46c059 - 10.60.21.0/25 ▾</div>	Enable Public IP? <input checked="" type="radio"/> Enable <input type="radio"/> Disable
Subnet <div style="border: 1px solid #ccc; padding: 2px; width: 100%;">10.60.21.0/25 ▾</div>	IAM Role (optional) <div style="border: 1px solid #ccc; padding: 2px; width: 100%; text-align: right;">?</div>

7. Specify a proxy configuration, if a proxy is required for internet access in the VPC.
8. After the data broker is available, click **Continue** in Cloud Sync.

The following image shows a successfully deployed instance in AWS:

The screenshot shows a search results page titled 'Select a NetApp Data Broker'. At the top left, there is a blue circular icon with a white checkmark and the number '1'. To its right, it says 'NetApp Data Brokers'. On the far right is a magnifying glass icon. Below this, a table displays one data broker entry:

aws	name		Active
US West (Oregon) Region	10.60.21.0/25   vpc-3c46c059 VPC	10.60.21.5 Private IP	5f5002eefc378e000a560988 Broker ID
us-west-2c Availability Zone	10.60.21.0/25   subnet-e7f526be Subnet	i-0fc5c97e2f5f22c20 Instance ID	

9. Complete the pages in the wizard to create the new sync relationship.

## Result

You have deployed a data broker in AWS and created a new sync relationship. You can use this data broker with additional sync relationships.

## Installing the data broker in Azure

When you create a new data broker, choose the Azure Data Broker option to deploy the data broker software on a new virtual machine in a VNet. Cloud Sync guides you through the installation process, but the requirements and steps are repeated on this page to help you prepare for installation.

You also have the option to install the data broker on an existing Linux host in the cloud or on your premises. [Learn more](#).

## Supported Azure regions

All regions are supported except for the China, US Gov, and US DoD regions.

## Networking requirements

- The data broker needs an outbound internet connection so it can poll the Cloud Sync service for tasks over port 443.

When Cloud Sync deploys the data broker in Azure, it creates a security group that enables the required outbound communication.

If you need to limit outbound connectivity, see [the list of endpoints that the data broker contacts](#).

- NetApp recommends configuring the source, target, and data broker to use a Network Time Protocol (NTP) service. The time difference between the three components should not exceed 5 minutes.

## Authentication method

When you deploy the data broker, you'll need to choose an authentication method: a password or an SSH public-private key pair.

For help with creating a key pair, refer to [Azure Documentation: Create and use an SSH public-private key pair for Linux VMs in Azure](#).

## Installing the data broker

You can install a data broker in Azure when you create a sync relationship.

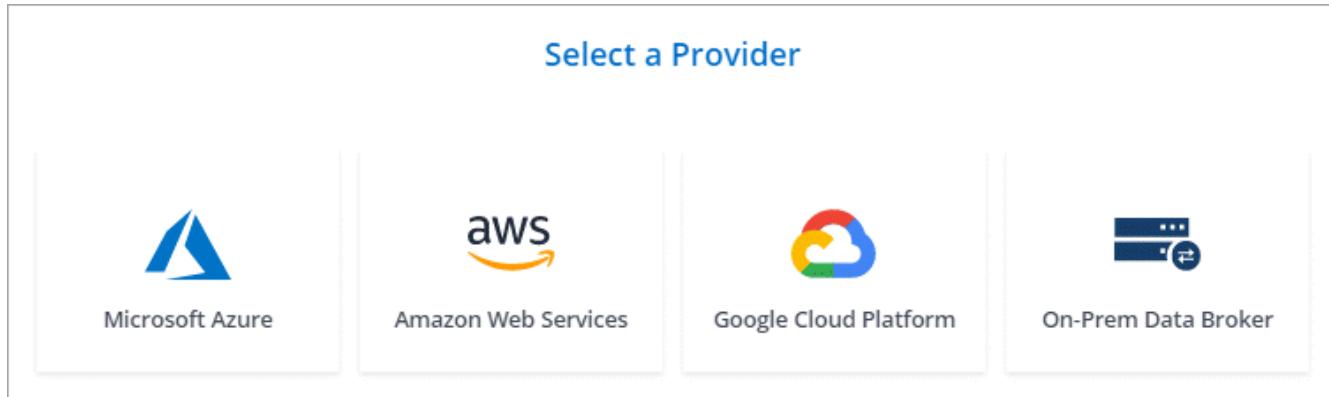
### Steps

1. Click **Create New Sync**.
2. On the **Define Sync Relationship** page, choose a source and target and click **Continue**.

Complete the pages until you reach the **Data Broker** page.

3. On the **Data Broker** page, click **Create Data Broker** and then select **Microsoft Azure**.

If you already have a data broker, you'll need to click the  icon first.



4. Enter a name for the data broker and click **Continue**.
5. If you're prompted, log in to your Microsoft account. If you're not prompted, click **Log in to Azure**.

The form is owned and hosted by Microsoft. Your credentials are not provided to NetApp.

6. Choose a location for the data broker and enter basic details about the virtual machine.

Location	Virtual Machine
Subscription OCCM Dev	VM Name netappdatabroker
Azure Region West US 2	User Name databroker
VNet Vnet1	Authentication Method: <input checked="" type="radio"/> Password <input type="radio"/> Public Key
Subnet Subnet1	Enter Password *****
	Resource Group: <input checked="" type="radio"/> Generate a new group <input type="radio"/> Use an existing group

7. Specify a proxy configuration, if a proxy is required for internet access in the VNet.
8. Click **Continue** and keep the page open until the deployment is complete.

The process can take up to 7 minutes.

9. In Cloud Sync, click **Continue** once the data broker is available.
10. Complete the pages in the wizard to create the new sync relationship.

## Result

You have deployed a data broker in Azure and created a new sync relationship. You can use this data broker with additional sync relationships.

## Getting a message about needing admin consent?

If Microsoft notifies you that admin approval is required because Cloud Sync needs permission to access resources in your organization on your behalf, then you have two options:

1. Ask your AD admin to provide you with the following permission:

In Azure, go to **Admin Centers > Azure AD > Users and Groups > User Settings** and enable **Users can consent to apps accessing company data on their behalf**.

2. Ask your AD admin to consent on your behalf to **CloudSync-AzureDataBrokerCreator** using the following URL (this is the admin consent endpoint):

`https://login.microsoftonline.com/{FILL HERE YOUR TENANT ID}/v2.0/adminconsent?client_id=8ee4ca3a-bafa-4831-97cc-5a38923cab85&redirect_uri=https://cloudsync.netapp.com&scope=https://management.azure.com/user_impersonationhttps://graph.microsoft.com/User.Read`

As shown in the URL, our app URL is `https://cloudsync.netapp.com` and the application client ID is `8ee4ca3a-bafa-4831-97cc-5a38923cab85`.

## Installing the data broker in Google Cloud Platform

When you create a new data broker, choose the GCP Data Broker option to deploy the data broker software on a new virtual machine instance in a VPC. Cloud Sync guides you through the installation process, but the requirements and steps are repeated on this page to help you prepare for installation.

You also have the option to install the data broker on an existing Linux host in the cloud or on your premises. [Learn more](#).

### Supported GCP regions

All regions are supported.

### Networking requirements

- The data broker needs an outbound internet connection so it can poll the Cloud Sync service for tasks over port 443.

When Cloud Sync deploys the data broker in GCP, it creates a security group that enables the required outbound communication.

If you need to limit outbound connectivity, see [the list of endpoints that the data broker contacts](#).

- NetApp recommends configuring the source, target, and data broker to use a Network Time Protocol (NTP) service. The time difference between the three components should not exceed 5 minutes.

### Permissions required to deploy the data broker in GCP

Ensure that the GCP user who deploys the data broker has the following permissions:

- compute.networks.list
- compute.regions.list
- deploymentmanager.deployments.create
- deploymentmanager.deployments.delete
- deploymentmanager.operations.get
- iam.serviceAccounts.list

#### Permissions required for the service account

When you deploy the data broker, you need to select a service account that has the following permissions:

- logging.logEntries.create
- resourcemanager.projects.get
- storage.buckets.get
- storage.buckets.list
- storage.objects.\*

#### Installing the data broker

You can install a data broker in GCP when you create a sync relationship.

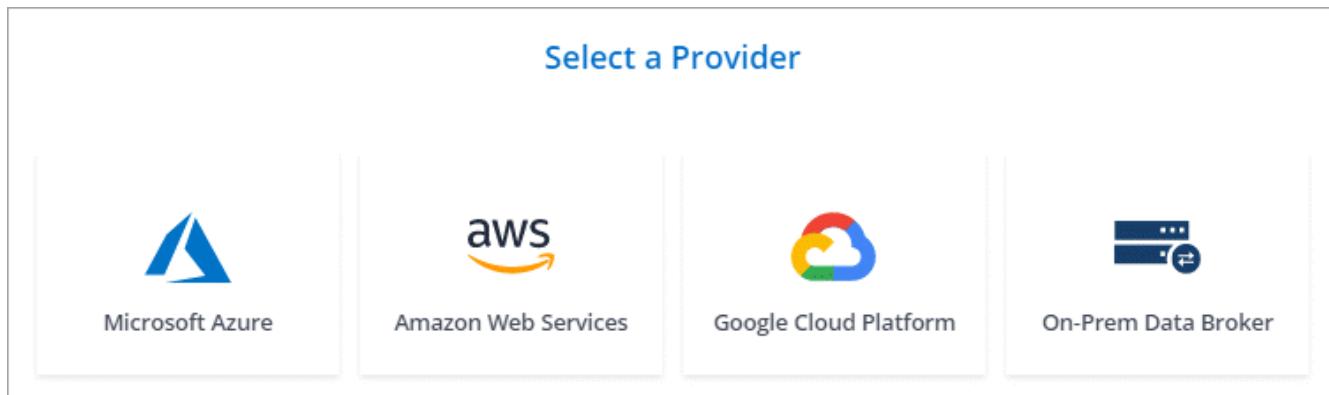
#### Steps

1. Click **Create New Sync**.
2. On the **Define Sync Relationship** page, choose a source and target and click **Continue**.

Complete the steps until you reach the **Data Broker** page.

3. On the **Data Broker** page, click **Create Data Broker** and then select **Google Cloud Platform**.

If you already have a data broker, you'll need to click the  icon first.



4. Enter a name for the data broker and click **Continue**.
5. If you're prompted, log in with your Google account.

The form is owned and hosted by Google. Your credentials are not provided to NetApp.

6. Select a project and service account and then choose a location for the data broker.

### Basic Settings

<p><b>Project</b></p> <p>Project</p> <div style="border: 1px solid #ccc; padding: 5px; width: 100%;">OCCM-Dev</div>	<p><b>Location</b></p> <p>Region</p> <div style="border: 1px solid #ccc; padding: 5px; width: 100%;">us-west1</div>
<p>Service Account</p> <div style="border: 1px solid #ccc; padding: 5px; width: 100%;">test</div>	<p>Zone</p> <div style="border: 1px solid #ccc; padding: 5px; width: 100%;">us-west1-a</div>
<p>Select a Service Account that includes <a href="#">these permissions</a></p>	
<p>VPC</p> <div style="border: 1px solid #ccc; padding: 5px; width: 100%;">default</div>	
<p>Subnet</p> <div style="border: 1px solid #ccc; padding: 5px; width: 100%;">default</div>	

7. Specify a proxy configuration, if a proxy is required for internet access in the VPC.

If a proxy is required for internet access, then the proxy must be in Google Cloud and use the same service account as the data broker.

8. Once the data broker is available, click **Continue** in Cloud Sync.

The instance takes approximately 5 to 10 minutes to deploy. You can monitor the progress from the Cloud Sync service, which automatically refreshes when the instance is available.

9. Complete the pages in the wizard to create the new sync relationship.

## Result

You've deployed a data broker in GCP and created a new sync relationship. You can use this data broker with additional sync relationships.

### Installing the data broker on a Linux host

When you create a new data broker, choose the On-Prem Data Broker option to install the data broker software on an on-premises Linux host, or on an existing Linux host in the cloud. Cloud Sync guides you through the installation process, but the requirements and steps are repeated on this page to help you prepare for installation.

#### Linux host requirements

- **Operating system:**

- CentOS 7.0, 7.7, and 8.0
- Red Hat Enterprise Linux 7.7 and 8.0

- Ubuntu Server 20.04 LTS
- SUSE Linux Enterprise Server 15 SP1

The command `yum update all` must be run on the host before you install the data broker.

A Red Hat Enterprise Linux system must be registered with Red Hat Subscription Management. If it is not registered, the system cannot access repositories to update required 3rd party software during installation.

- **RAM:** 16 GB
- **CPU:** 4 cores
- **Free disk space:** 10 GB
- **SELinux:** We recommend that you disable [SELinux](#) on the host.

SELinux enforces a policy that blocks data broker software updates and can block the data broker from contacting endpoints required for normal operation.

- **OpenSSL:** OpenSSL must be installed on the Linux host.

### **Networking requirements**

- The Linux host must have a connection to the source and target.
- The file server must allow the Linux host to access the exports.
- Port 443 must be open on the Linux host for outbound traffic to AWS (the data broker constantly communicates with the Amazon SQS service).
- NetApp recommends configuring the source, target, and data broker to use a Network Time Protocol (NTP) service. The time difference between the three components should not exceed 5 minutes.

### **Enabling access to AWS**

If you plan to use the data broker with a sync relationship that includes an S3 bucket, then you should prepare the Linux host for AWS access. When you install the data broker, you'll need to provide AWS keys for an AWS user that has programmatic access and specific permissions.

#### **Steps**

1. Create an IAM policy using [this NetApp-provided policy](#). [View AWS instructions](#).
2. Create an IAM user that has programmatic access. [View AWS instructions](#).

Be sure to copy the AWS keys because you need to specify them when you install the data broker software.

### **Enabling access to Google Cloud**

If you plan to use the data broker with a sync relationship that includes a Google Cloud Storage bucket, then you should prepare the Linux host for GCP access. When you install the data broker, you'll need to provide a key for a service account that has specific permissions.

#### **Steps**

1. Create a GCP service account that has Storage Admin permissions, if you don't already have one.
2. Create a service account key saved in JSON format. [View GCP instructions](#).

The file should contain at least the following properties: "project\_id", "private\_key", and "client\_email"



When you create a key, the file gets generated and downloaded to your machine.

3. Save the JSON file to the Linux host.

#### Enabling access to Microsoft Azure

Access to Azure is defined per relationship by providing a storage account and a connection string in the Sync Relationship wizard.

#### Installing the data broker

You can install a data broker on a Linux host when you create a sync relationship.

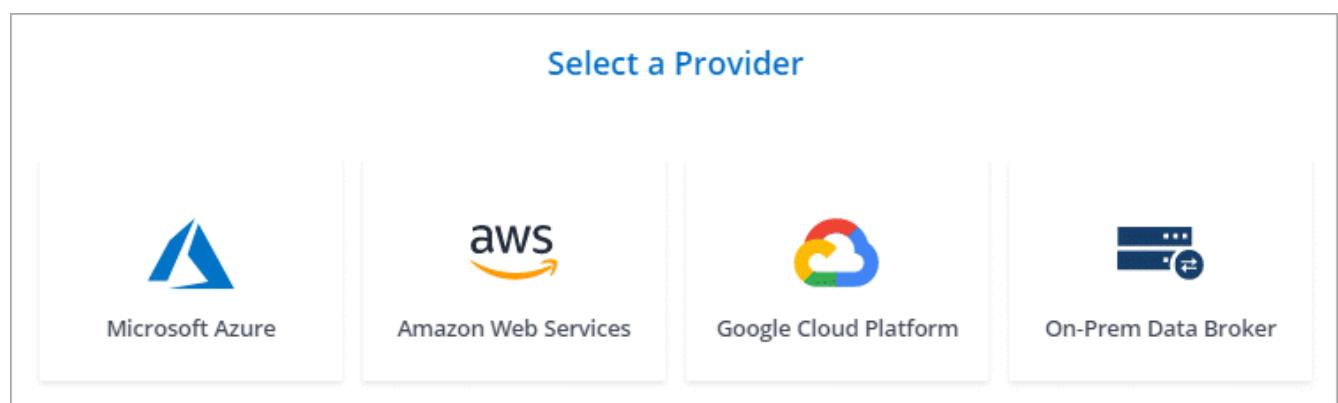
#### Steps

1. Click **Create New Sync**.
2. On the **Define Sync Relationship** page, choose a source and target and click **Continue**.

Complete the steps until you reach the **Data Broker** page.

3. On the **Data Broker** page, click **Create Data Broker** and then select **On-Prem Data Broker**.

If you already have a data broker, you'll need to click the icon first.



Even though the option is labeled **On-Prem Data Broker**, it applies to a Linux host on your premises or in the cloud.

4. Enter a name for the data broker and click **Continue**.

The instructions page loads shortly. You'll need to follow these instructions—they include a unique link to download the installer.

5. On the instructions page:
  - a. Select whether to enable access to **AWS**, **Google Cloud**, or both.
  - b. Select an installation option: **No proxy**, **Use proxy server**, or **Use proxy server with authentication**.
  - c. Use the commands to download and install the data broker.

The following steps provide details about each possible installation option. Follow the instructions page to get the exact command based on your installation option.

d. Download the installer:

- No proxy:

```
curl <URI> -o data_broker_installer.sh
```

- Use proxy server:

```
curl <URI> -o data_broker_installer.sh -x <proxy_host>:<proxy_port>
```

- Use proxy server with authentication:

```
curl <URI> -o data_broker_installer.sh -x  
<proxy_username>:<proxy_password>@<proxy_host>:<proxy_port>
```

### URI

Cloud Sync displays the URI of the installation file on the instructions page, which loads when you follow the prompts to deploy the On-Prem Data Broker. That URL isn't repeated here because the link is generated dynamically and can be used only once. [Follow these steps to obtain the URI from Cloud Sync](#).

e. Switch to superuser, make the installer executable and install the software:



Each command listed below includes parameters for AWS access and GCP access. Follow the instructions page to get the exact command based on your installation option.

- No proxy configuration:

```
sudo -s  
chmod +x data_broker_installer.sh  
./data_broker_installer.sh -a <aws_access_key> -s <aws_secret_key> -g  
<absolute_path_to_the_json_file>
```

- Proxy configuration:

```
sudo -s  
chmod +x data_broker_installer.sh  
./data_broker_installer.sh -a <aws_access_key> -s <aws_secret_key> -g  
<absolute_path_to_the_json_file> -h <proxy_host> -p <proxy_port>
```

- Proxy configuration with authentication:

```
sudo -s  
chmod +x data_broker_installer.sh  
./data_broker_installer.sh -a <aws_access_key> -s <aws_secret_key> -g  
<absolute_path_to_the_json_file> -h <proxy_host> -p <proxy_port> -u  
<proxy_username> -w <proxy_password>
```

## AWS keys

These are the keys for the user that you should have prepared [following these steps](#). The AWS keys are stored on the data broker, which runs in your on-premises or cloud network. NetApp doesn't use the keys outside of the data broker.

## JSON file

This is the JSON file that contains a service account key that you should have prepared [following these steps](#).

6. Once the data broker is available, click **Continue** in Cloud Sync.
7. Complete the pages in the wizard to create the new sync relationship.

## Creating a sync relationship

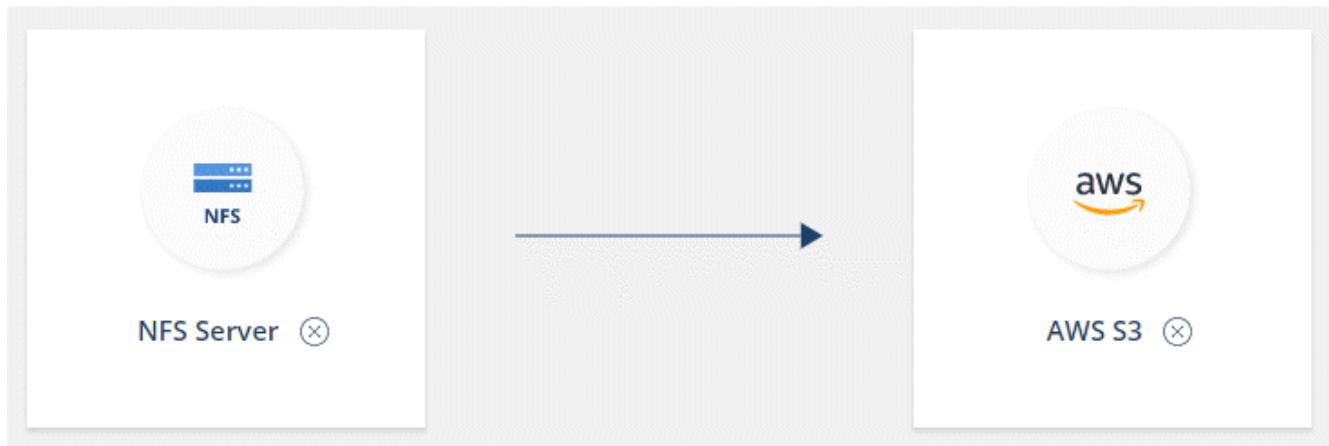
When you create a sync relationship, the Cloud Sync service copies files from the source to the target. After the initial copy, the service syncs any changed data every 24 hours.

### Creating a sync relationship

Use these steps to sync data to or from any supported storage type. The steps below provide an example that shows how to set up a sync relationship from an NFS server to an S3 bucket.

1. In Cloud Manager, click **Sync**.
2. On the **Define Sync Relationship** page, choose a source and target.

The following steps provide an example of how to create a sync relationship from an NFS server to an S3 bucket.



3. On the **NFS Server** page, enter the IP address or fully qualified domain name of the NFS server that you want to sync to AWS.
4. On the **Data Broker** page, follow the prompts to create a data broker virtual machine in AWS, Azure, or Google Cloud Platform, or to install the data broker software on an existing Linux host.

For more details, refer to the following pages:

- [Installing the data broker in AWS](#)
- [Installing the data broker in Azure](#)

- [Installing the data broker in GCP](#)
  - [Installing the data broker on a Linux host](#)
5. After you install the data broker, click **Continue**.

The following image shows a successfully deployed data broker in AWS:

The screenshot shows a table titled "Select a NetApp Data Broker" with one entry. The entry is for an "aws" broker named "name". The details are as follows:

Region	VPC	Private IP	Broker ID
US West (Oregon)	10.60.21.0/25   vpc-3c46c059	10.60.21.5	5f5002eefc378e000a560988
us-west-2c	Subnet	i-0fc5c97e2f5f22c20	Instance ID

A green checkmark icon next to the broker name indicates it is "Active".

6. On the **Directories** page, select a top-level directory or subdirectory.

If Cloud Sync is unable to retrieve the exports, click **Add Export Manually** and enter the name of an NFS export.



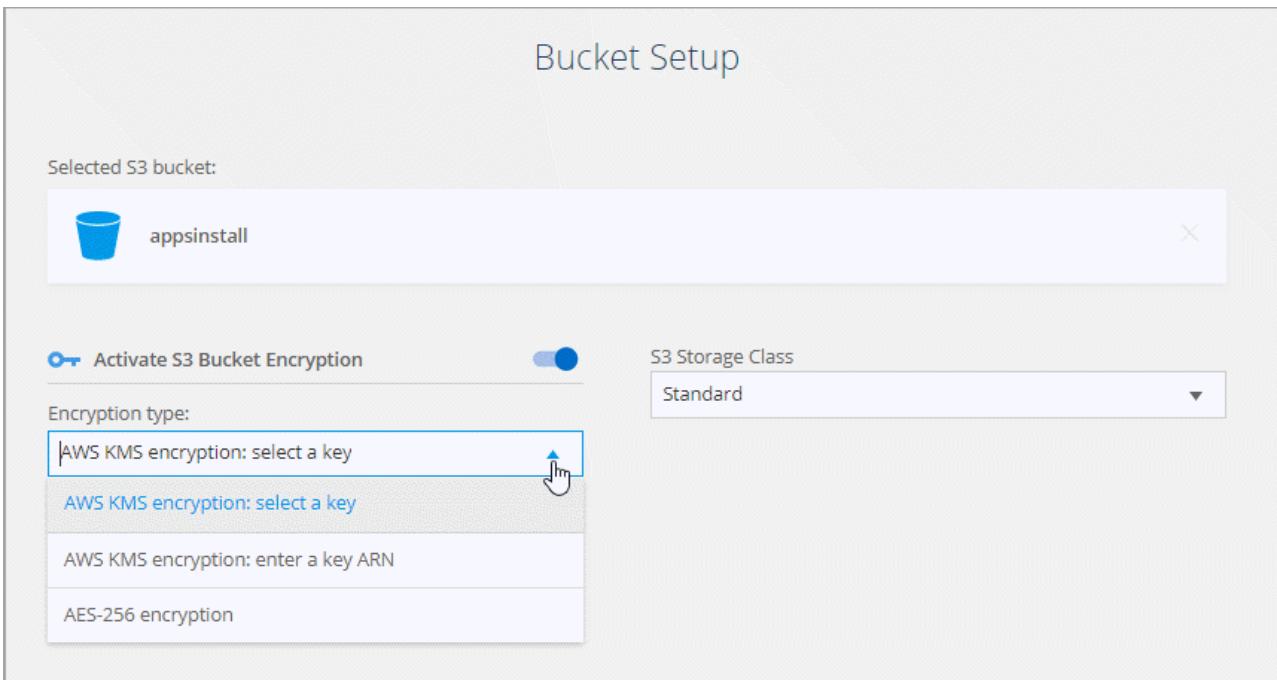
If you want to sync more than one directory on the NFS server, then you must create additional sync relationships after you are done.

7. On the **AWS S3 Bucket** page, select a bucket:

- Drill down to select an existing folder within the bucket or to select a new folder that you create inside the bucket.
- Click **Add to the list** to select an S3 bucket that is not associated with your AWS account. [Specific permissions must be applied to the S3 bucket](#).

8. On the **Bucket Setup** page, set up the bucket:

- Choose whether to enable S3 bucket encryption and then select an AWS KMS key, enter the ARN of a KMS key, or select AES-256 encryption.
- Select an S3 storage class. [View the supported storage classes](#).



9. On the **Settings** page, define how source files and folders are synced and maintained in the target location:

### Schedule

Choose a recurring schedule for future syncs or turn off the sync schedule. You can schedule a relationship to sync data as often as every 1 minute.

### Retries

Define the number of times that Cloud Sync should retry to sync a file before skipping it.

### Recently Modified Files

Choose to exclude files that were recently modified prior to the scheduled sync.

### Delete Files on Source

Choose to delete files from the source location after Cloud Sync copies the files to the target location. This option includes the risk of data loss because the source files are deleted after they're copied.

If you enable this option, you also need to change a parameter in the local.json file on the data broker. Open the file and change the parameter named `workers.transferrer.delete-on-source` to `true`.

### Delete Files on Target

Choose to delete files from the target location, if they were deleted from the source. The default is to never delete files from the target location.

### Object tagging

When AWS S3 is the target in a sync relationship, Cloud Sync tags S3 objects with metadata that's relevant to the sync operation. You can disable tagging of S3 objects, if it's not desired in your environment. There's no impact to Cloud Sync if you disable tagging—Cloud Sync just stores the sync metadata in a different way.

### File Types

Define the file types to include in each sync: files, directories, and symbolic links.

## **Exclude File Extensions**

Specify file extensions to exclude from the sync by typing the file extension and pressing **Enter**. For example, type *log* or *.log* to exclude \*.log files. A separator isn't required for multiple extensions. The following video provides a short demo:

► [https://docs.netapp.com/us-en/occm/media/video\\_file\\_extensions.mp4](https://docs.netapp.com/us-en/occm/media/video_file_extensions.mp4) (*video*)

## **File Size**

Choose to sync all files regardless of their size or just files that are in a specific size range.

## **Date Modified**

Choose all files regardless of their last modified date, files modified after a specific date, before a specific date, or between a time range.

10. On the **Relationship Tags** page, enter up to 9 relationship tags and then click **Continue**.

The Cloud Sync service assigns the tags to each object that it syncs to the S3 bucket.

11. Review the details of the sync relationship and then click **Create Relationship**.

## **Result**

Cloud Sync starts syncing data between the source and target.

## **Creating a sync relationship for an existing working environment**

Use these steps to sync data to or from any of the following:

- Amazon S3
- Azure NetApp Files
- Cloud Volumes ONTAP
- On-prem ONTAP cluster

## **Steps**

1. In Cloud Manager, click **Canvas**.
2. Select a working environment that matches any of the types listed above.
3. Select the action menu next to Sync.

The screenshot shows the NetApp Canvas interface. On the left, there's a 'Cloud' icon labeled 'SINGLE' containing 'CloudVolumesONTAP' and 'Cloud Volumes ONTAP' with a '51 GiB Capacity'. An 'aws' icon is connected to it. On the right, a detailed view of the 'CloudVolumesONTAP' location is shown. It has a status bar with 'CloudVolumesONTAP', 'On', and three icons (info, more, close). Below this are four sections: 'Compliance' (Off, Enable button), 'Monitoring' (On, Sync data from this location button), 'File Cache' (Off, Sync data to this location button), and 'Sync' (On, View Dashboard button). A summary at the bottom says '559.16TiB Data Synced' with a 'More' button.

4. Select **Sync data from this location** or **Sync data to this location** and follow the prompts to set up the sync relationship.

## Paying for sync relationships after your free trial ends

There are two ways to pay for sync relationships after your 14-day free trial ends. The first option is to subscribe from AWS or Azure to pay-as-you-go or to pay annually. The second option is to purchase licenses directly from NetApp.

You can use licenses from NetApp with an AWS or Azure subscription. For example, if you have 25 sync relationships, you can pay for the first 20 sync relationships using a license and then pay-as-you-go from AWS or Azure with the remaining 5 sync relationships.

[Learn more about how licenses work.](#)

### What if I don't immediately pay after my free trial ends?

You won't be able to create any additional relationships. Existing relationships are not deleted, but you cannot make any changes to them until you subscribe or enter a license.

## Subscribing from AWS

AWS enables you to pay-as-you-go or to pay annually.

### Steps to pay-as-you-go

1. Click **Sync > Licensing**.
2. Select **AWS**

3. Click **Subscribe** and then click **Continue**.
4. Subscribe from the AWS Marketplace, and then log back in to the Cloud Sync service to complete the registration.

The following video shows the process:

► [https://docs.netapp.com/us-en/occm/media/video\\_cloud\\_sync\\_registering.mp4](https://docs.netapp.com/us-en/occm/media/video_cloud_sync_registering.mp4) (video)

#### Steps to pay annually

1. [Go to the AWS Marketplace page](#).
2. Click **Continue to Subscribe**.
3. Select your contract options and click **Create contract**.

#### Subscribing from Azure

Azure enables you to pay-as-you-go or to pay annually.

#### What you'll need

An Azure user account that has Contributor or Owner permissions in the relevant subscription.

#### Steps

1. Click **Sync > Licensing**.
2. Select **Azure**.
3. Click **Subscribe** and then click **Continue**.
4. In the Azure portal, click **Create**, select your options, and click **Subscribe**.

Select **Monthly** to pay by the hour, or **Yearly** to pay for a year up front.

5. When deployment is complete, click the name of the SaaS resource in the notification pop-up.
6. Click **Configure Account** to return to Cloud Sync.

The following video shows the process:

► [https://docs.netapp.com/us-en/occm/media/video\\_cloud\\_sync\\_registering\\_azure.mp4](https://docs.netapp.com/us-en/occm/media/video_cloud_sync_registering_azure.mp4) (video)

#### Purchasing licenses from NetApp and adding them to Cloud Sync

To pay for your sync relationships up front, you must purchase one or more licenses and add them to the Cloud Sync service.

#### Steps

1. Purchase a license by [contacting NetApp](#).
2. In Cloud Manager, click **Sync > Licensing**.
3. Click **Add License** and add the license.

## Tutorials

## Copying ACLs between SMB shares

Cloud Sync can copy access control lists (ACLs) between a source SMB share and a target SMB share. If needed, you can manually preserve the ACLs yourself by using robocopy.

### Choices

- [Set up Cloud Sync to automatically copy ACLs](#)
- [Manually copy the ACLs yourself](#)

### Setting up Cloud Sync to copy ACLs between SMB servers

Copy ACLs between SMB servers by enabling a setting when you create a relationship or after you create a relationship.

Note that this feature is available for new sync relationships created after the 23 Feb 2020 release. If you'd like to use this feature with existing relationships created prior to that date, then you'll need to recreate the relationship.

### What you'll need

- A new sync relationship or an existing sync relationship created after the 23 Feb 2020 release.
- Any type of data broker.

This feature works with *any* type of data broker: the AWS, Azure, Google Cloud Platform, or on-prem data broker. The on-prem data broker can run [any supported operating system](#).

### Steps for a new relationship

1. From Cloud Sync, click **Create New Sync**.
2. Drag and drop **SMB Server** to the source and target and click **Continue**.
3. On the **SMB Server** page:
  - a. Enter a new SMB server or select an existing server and click **Continue**.
  - b. Enter credentials for the SMB server.
  - c. Select **Copy Access Control Lists to the target** and click **Continue**.

Select an SMB Source

SMB Version : 2.1 ▾

Selected SMB Server:  
10.20.30.152 X

Define SMB Credentials:

User Name user1	Password *****	Domain (Optional)
--------------------	-------------------	-------------------

ACL - Access Control List

Copy Access Control Lists to the target

**Notice:** Copying ACLs can affect sync performance.  
You can change this setting after you create the relationship.

4. Follow the remaining prompts to create the sync relationship.

### Steps for an existing relationship

1. Hover over the sync relationship and click the action menu.
2. Click **Settings**.
3. Select **Copy Access Control Lists to the target**.
4. Click **Save Settings**.

### Result

When syncing data, Cloud Sync preserves the ACLs between the source and target SMB shares.

### Manually copying ACLs

You can manually preserve ACLs between SMB shares by using the Windows robocopy command.

### Steps

1. Identify a Windows host that has full access to both SMB shares.
2. If either of the endpoints require authentication, use the **net use** command to connect to the endpoints from the Windows host.

You must perform this step before you use robocopy.
3. From Cloud Sync, create a new relationship between the source and target SMB shares or sync an existing relationship.
4. After the data sync is complete, run the following command from the Windows host to sync the ACLs and ownership:

```
robocopy /E /COPY:SOU /secfix [source] [target] /w:0 /r:0 /XD ~snapshots  
/UNILOG:"[filepath]"
```

Both *source* and *target* should be specified using the UNC format. For example: \\<server>\<share>\<path>

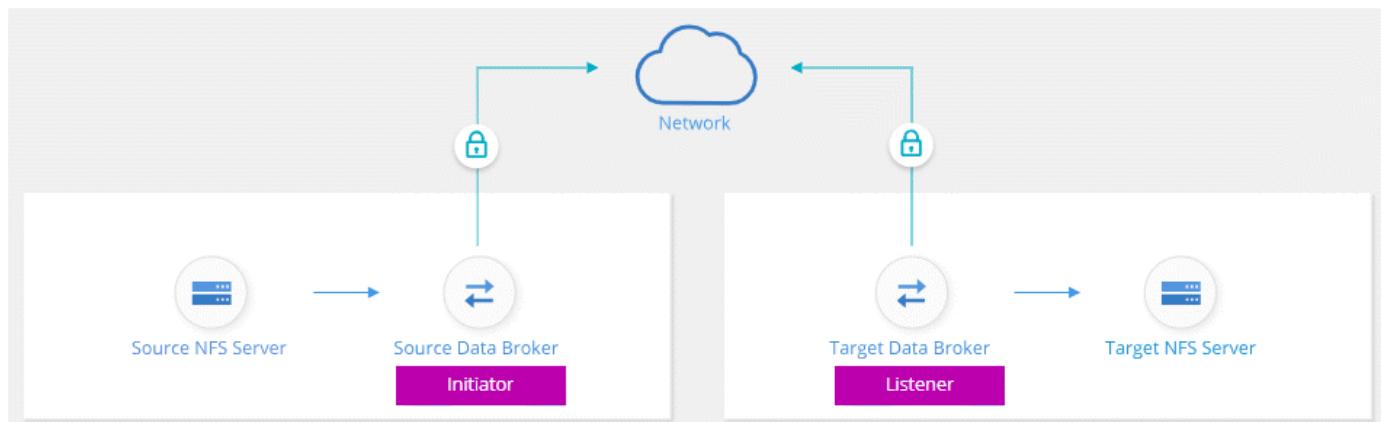
## Syncing NFS data using data-in-flight encryption

If your business has strict security policies, you can sync NFS data using data-in-flight encryption. This feature is supported from an NFS server to another NFS server and from Azure NetApp Files to Azure NetApp Files.

For example, you might want to sync data between two NFS servers that are in different networks. Or you might need to securely transfer data on Azure NetApp Files across subnets or regions.

### How data-in-flight encryption works

Data-in-flight encryption encrypts NFS data when it's sent over the network between two data brokers. The following image shows a relationship between two NFS servers and two data brokers:



One data broker functions as the *initiator*. When it's time to sync data, it sends a connection request to the other data broker, which is the *listener*. That data broker listens for requests on port 443. You can use a different port, if needed, but be sure to check that the port is not in use by another service.

For example, if you sync data from an on-premises NFS server to a cloud-based NFS server, you can choose which data broker listens for the connection requests and which sends them.

Here's how in-flight encryption works:

1. After you create the sync relationship, the initiator starts an encrypted connection with the other data broker.
2. The source data broker encrypts data from the source using TLS 1.3.
3. It then sends the data over the network to the target data broker.
4. The target data broker decrypts the data before sending it to the target.
5. After the initial copy, the service syncs any changed data every 24 hours. If there is data to sync, the process starts with the initiator opening an encrypted connection with the other data broker.

If you prefer to sync data more frequently, [you can change the schedule after you create the relationship](#).

## Supported NFS versions

- For NFS servers, data-in-flight encryption is supported with NFS versions 3, 4.0, 4.1, and 4.2.
- For Azure NetApp Files, data-in-flight encryption is supported with NFS versions 3 and 4.1.

## Proxy server limitation

If you create an encrypted sync relationship, the encrypted data is sent over HTTPS and isn't routable through a proxy server.

## What you'll need to get started

Be sure to have the following:

- Two NFS servers that meet [source and target requirements](#) or Azure NetApp Files in two subnets or regions.
- The IP addresses or fully qualified domain names of the servers.
- Network locations for two data brokers.

You can select an existing data broker but it must function as the initiator. The listener data broker must be a *new* data broker.

If you have not yet deployed a data broker, review the data broker requirements. Because you have strict security policies, be sure to review the networking requirements, which includes outbound traffic from port 443 and the [internet endpoints](#) that the data broker contacts.

- [Review AWS installation](#)
- [Review Azure installation](#)
- [Review GCP installation](#)
- [Review Linux host installation](#)

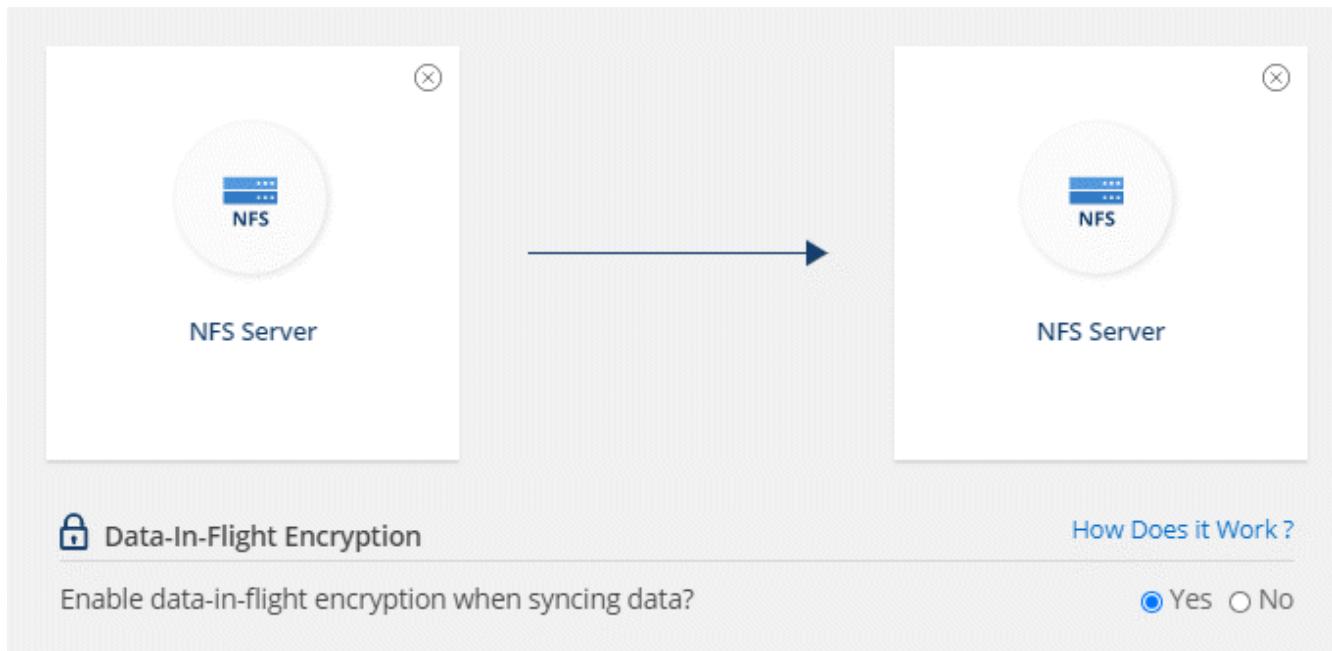
## Syncing NFS data using data-in-flight encryption

Create a new sync relationship between two NFS servers or between Azure NetApp Files, enable the in-flight encryption option, and follow the prompts.

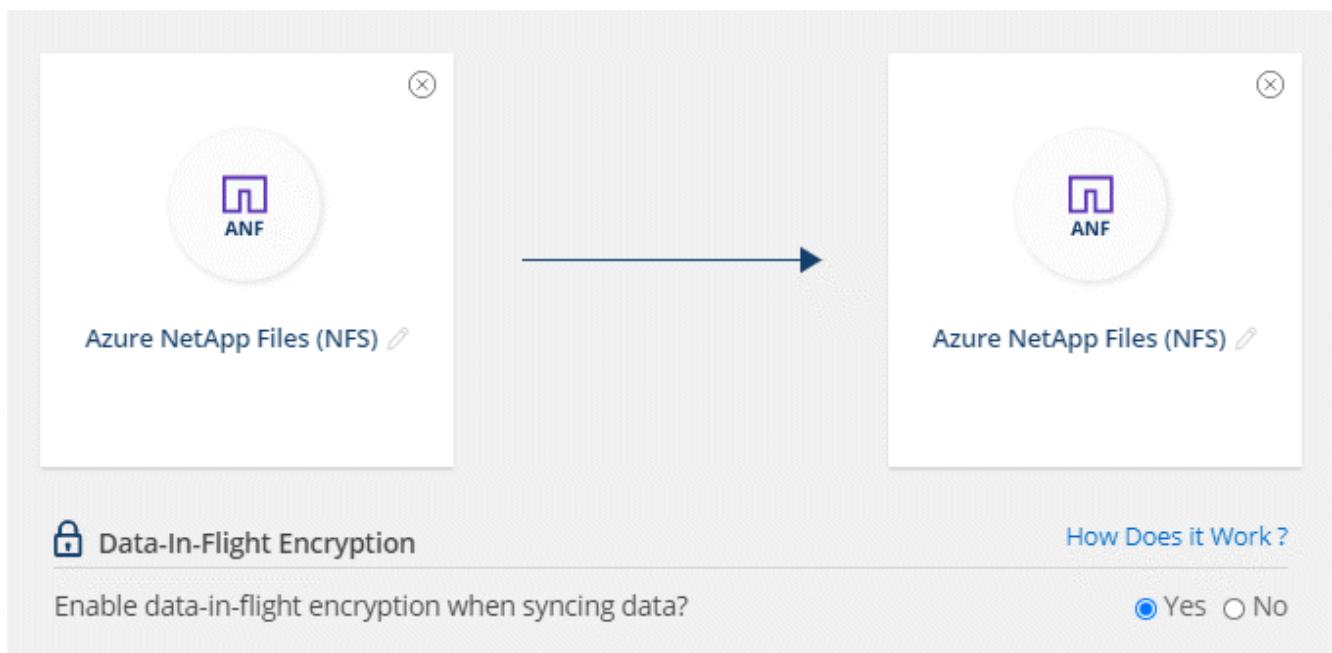
### Steps

1. Click **Create New Sync**.
2. Drag and drop **NFS Server** to the source and target locations or **Azure NetApp Files** to the source and target locations and select **Yes** to enable data-in-flight encryption.

The following image shows what you'd select to sync data between two NFS servers:



The following image shows what you'd select to sync data between Azure NetApp Files:

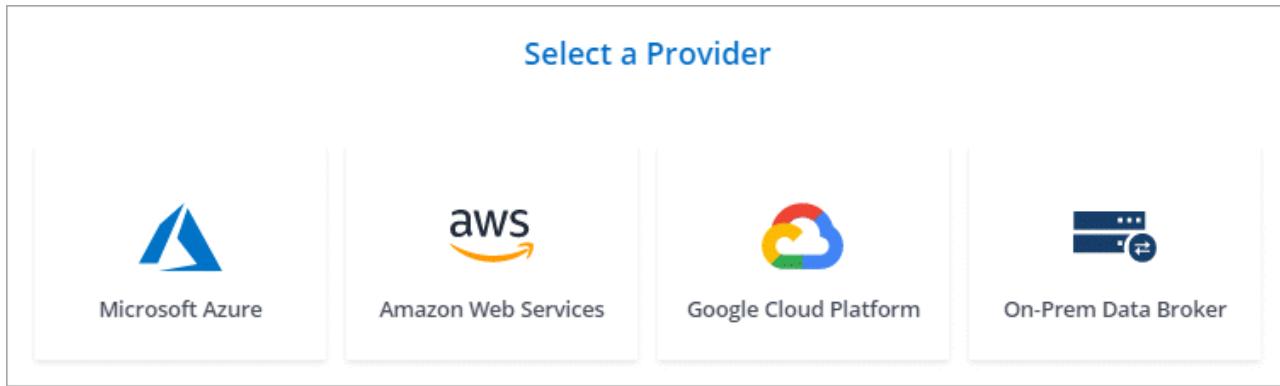


3. Follow the prompts to create the relationship:

- NFS Server/Azure NetApp Files:** Choose the NFS version and then specify a new NFS source or select an existing server.
- Define Data Broker Functionality:** Define which data broker *listens* for connection requests on a port and which one *initiates* the connection. Make your choice based on your networking requirements.
- Data Broker:** Follow the prompts to add a new source data broker or select an existing data broker.

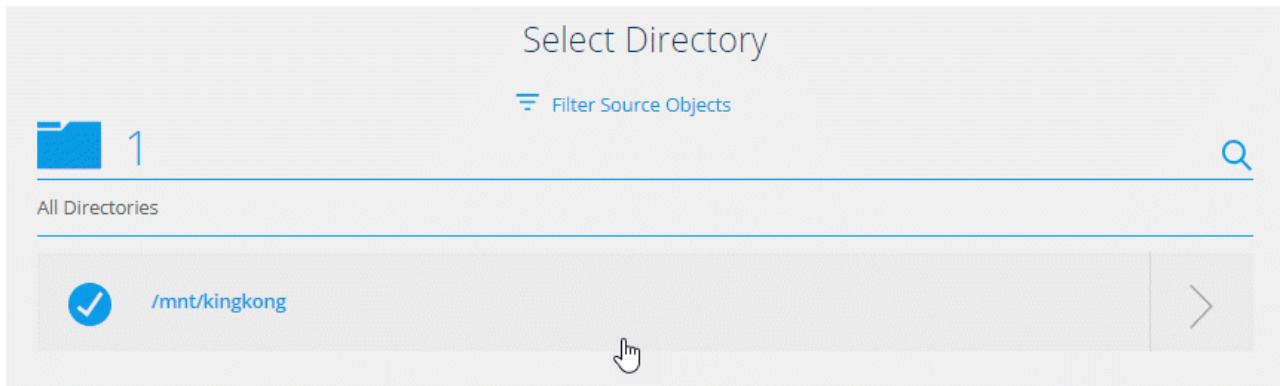
If the source data broker acts as the listener, then it must be a new data broker.

If you need a new data broker, Cloud Sync prompts you with the installation instructions. You can deploy the data broker in the cloud or download an installation script for your own Linux host.



- d. **Directories:** Choose the directories that you want to sync by selecting all directories, or by drilling down and selecting a subdirectory.

Click **Filter Source Objects** to modify settings that define how source files and folders are synced and maintained in the target location.



- e. **Target NFS Server/Target Azure NetApp Files:** Choose the NFS version and then enter a new NFS target or select an existing server.

- f. **Target Data Broker:** Follow the prompts to add a new source data broker or select an existing data broker.

If the target data broker acts as the listener, then it must be a new data broker.

Here's an example of the prompt when the target data broker functions as the listener. Notice the option to specify the port.

Select a Provider

Microsoft Azure

Amazon Web Services

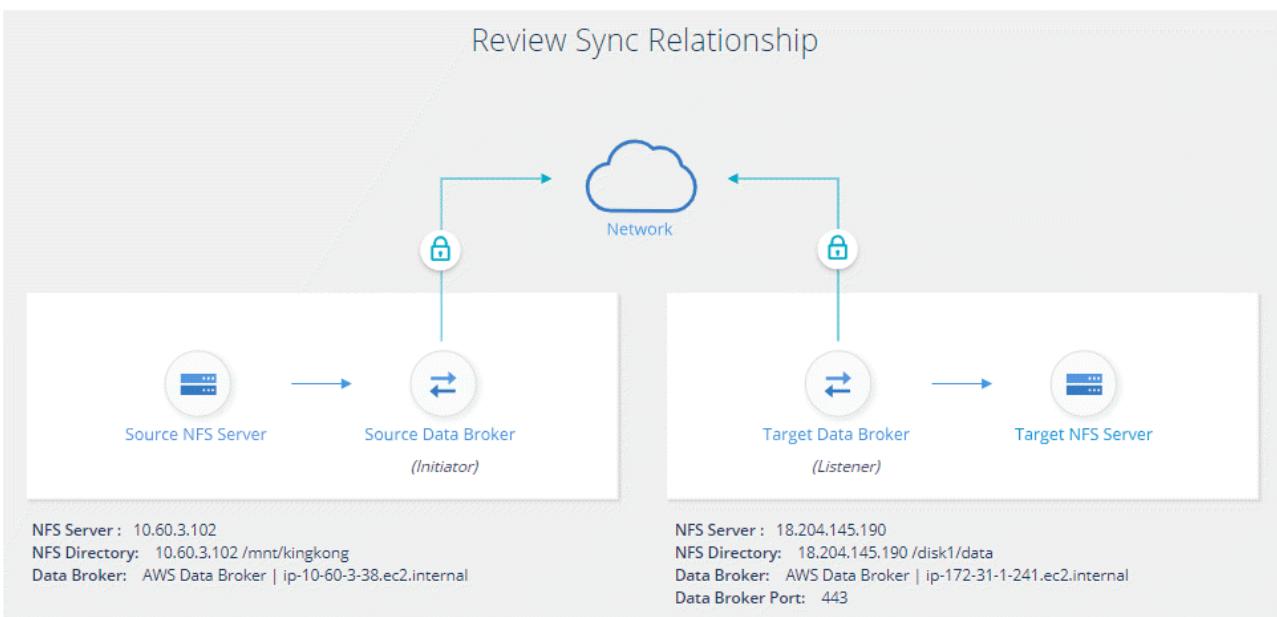
Google Cloud Platform

On-Prem Data Broker

Data Broker Name: listener-data-broker

Port: 443

- g. **Target Directories:** Select a top-level directory, or drill down to select an existing subdirectory or to create a new folder inside an export.
- h. **Settings:** Define how source files and folders are synced and maintained in the target location.
- i. **Review:** Review the details of the sync relationship and then click **Create Relationship**.



## Result

Cloud Sync starts creating the new sync relationship. When it's done, click **View in Dashboard** to view details about the new relationship.

## Setting up the data broker to use an external HashiCorp Vault

When you create a sync relationship that requires Amazon S3, Azure, or Google Cloud credentials, you need to specify those credentials through the Cloud Sync user interface or API. An alternative is to set up the data broker to access the credentials (or *secrets*) directly from an external HashiCorp Vault.

This feature is supported through the Cloud Sync API with sync relationships that require Amazon S3, Azure,

or Google Cloud credentials.



## 1 Prepare the vault

Prepare the vault to supply credentials to the data broker by setting up the URLs. The URLs to the secrets in the vault must end with *Creds*.



## 2 Prepare the data broker

Prepare the data broker to fetch credentials from the external vault by modifying the local config file for the data broker.



## 3 Create a sync relationship using the API

Now that everything is set up, you can send an API call to create a sync relationship that uses your vault to get the secrets.

### Preparing the vault

You'll need to provide Cloud Sync with the URL to the secrets in your vault. Prepare the vault by setting up those URLs. You need to set up URLs to the credentials for each source and target in the sync relationships that you plan to create.

The URL must be set up as follows:

/<path>/<requestid>/<endpoint-protocol>Creds

#### Path

The prefix path to the secret. This can be any value that's unique to you.

#### Request ID

A request ID that you need to generate. You'll need to provide the ID in one of the headers in the API POST request when you create the sync relationship.

#### Endpoint protocol

One of the following protocols, as defined [in the post relationship v2 documentation](#): S3, AZURE, or GCP (each must be in uppercase).

#### Creds

The URL must end with *Creds*.

### Examples

The following examples show URLs to secrets.

#### Example for the full URL and path for source credentials

`http://example.vault.com:8200/my-path/all-secrets/hb312vdasr2/S3Creds`

As you can see in the example, the prefix path is `/my-path/all-secrets/`, the request ID is `hb312vdasr2` and

the source endpoint is S3.

## Example for the full URL and path for target credentials

<http://example.vault.com:8200/my-path/all-secrets/n32hcbnejk2/AZURECreds>

The prefix path is `/my-path/all-secrets/`, the request ID is `n32hcbnejk2`, and the target endpoint is Azure.

## Preparing the data broker

Prepare the data broker to fetch credentials from the external vault by modifying the local config file for the data broker.

### Steps

1. SSH to the data broker.
2. Edit the `local.json` file that resides in `/opt/netapp/databroker/config`.
3. Set `enable` to `true` and set the config parameter fields under `external-integrations.hashicorp` as follows:

#### **enabled**

- Valid values: true/false
- Type: Boolean
- Default value: false
- True: The data broker gets secrets from your own external HashiCorp Vault
- False: The data broker stores credentials in its local vault

#### **url**

- Type: string
- Value: The URL to your external vault

#### **path**

- Type: string
- Value: Prefix path to the secret with your credentials

#### **Reject-unauthorized**

- Determines if you want the data broker to reject unauthorized external vault
- Type: Boolean
- Default: false

#### **auth-method**

- Your authentication method to the external vault
- Type: string
- Valid values: “aws-iam” / “role-app”

#### **role-name**

- Type: string
- Your role name (in case you use aws-iam)

### **Secretid & rootid**

- Type: string (in case you use app-role)

### **Namespace**

- Type: string
- Your namespace (X-Vault-Namespace header if needed)

### **Example**

```
{  
    "external-integrations": {  
        "hashicorp": {  
            "enabled": true,  
            "url": "https://example.vault.com:8200",  
            "path": "my-path/all-secrets",  
            "reject-unauthorized": false,  
            "auth-method": "aws-role",  
            "aws-role": {  
                "role-name": "my-role"  
            }  
        }  
    }  
}
```

### **Creating a new sync relationship using secrets from the vault**

Now that everything is set up, you can send an API call to create a sync relationship that uses your vault to get the secrets.

Post the relationship using the Cloud Sync REST API.

```
Headers:  
Authorization: Bearer <user-token>  
Content-Type: application/json  
x-account-id: <accountid>  
x-netapp-external-request-id-src: request ID as part of path for source  
credentials  
x-netapp-external-request-id-trg: request ID as part of path for target  
credentials  
Body: post relationship v2 body
```

- To obtain a user token and your Cloud Central account ID, refer to [this page in the documentation](#).
- To build a body for your post relationship, [refer to the relationships-v2 API call](#).

## Example

Example for the POST request:

```
url: https://api.cloudsync.netapp.com/api/relationships-v2
headers:
"x-account-id": "CS-SasdW"
"x-netapp-external-request-id-src": "hb312vdasr2"
"Content-Type": "application/json"
"Authorization": "Bearer eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6Ik..."
Body:
{
  "dataBrokerId": "5e6e111d578dtyuu1555sa60",
  "source": {
    "protocol": "s3",
    "s3": {
      "provider": "sgws",
      "host": "1.1.1.1",
      "port": "443",
      "bucket": "my-source"
    },
    "target": {
      "protocol": "s3",
      "s3": {
        "bucket": "my-target-bucket"
      }
    }
  }
}
```

## Managing sync relationships

You can manage sync relationships at any time by immediately syncing data, changing schedules, and more.

### Performing an immediate data sync

Rather than wait for the next scheduled sync, you can press a button to immediately sync data between the source and target.

#### Steps

1. From the **Sync Dashboard**, hover over the sync relationship and click the action menu.

Sync Relationships

6 syncs

Source	Target	NetApp Data Broker	Schedule	Sync Status
nfs://172.31.91.49/disk1/data/d...	nfs://172.31.91.49/disk2/target/...	vadimBroker1	ON	<span>Synced Successfully</span>
nfs://172.31.91.49/disk1/data/e...	nfs://172.31.91.49/disk2/target/...	vadimBroker1	ON	<span>Synced Successfully</span>

2. Click **Sync Now** and then click **Sync** to confirm.

11 Syncs

Source	Target	NetApp Data Broker	Sched...	Sync Status
nfs://172.31.91.49/disk1/data/...	s3://vadim-service-2test-e...	3 da	<span>Sync Now</span>	<span>Accelerate</span>
nfs://172.31.91.49/disk1/data/...	nfs://172.31.91.49/disk2/t...	3 data brokers	OFF	<span>Sync Completed</span>

## Result

Cloud Sync starts the data sync process for the relationship.

## Accelerating sync performance

Accelerate the performance of a sync relationship by adding an additional data broker to the relationship. The additional data broker must be a *new* data broker.

### How this works

If the existing data brokers in the relationship are used in other sync relationships, then Cloud Sync automatically adds the new data broker to those relationships, as well.

For example, let's say you have three relationships:

- Relationship 1 uses data broker A
- Relationship 2 uses data broker B
- Relationship 3 uses data broker A

You want to accelerate the performance of relationship 1 so you add a new data broker to that relationship (data broker C). Because data broker A is also used in relationship 3, the new data broker is automatically added to relationship 3, as well.

### Steps

1. Ensure that at least one of the existing data brokers in the relationship are online.
2. Hover over the sync relationship and click the action menu.
3. Click **Accelerate**.

Syncs					
Source	Target	NetApp Data Broker	Sched...	Sync Status	
nfs://172.31.91.49/disk1/data/...	s3://vadim-service-2test-e...	3 da	Sync Now	Accelerate	Settings  Delete
nfs://172.31.91.49/disk1/data/...	nfs://172.31.91.49/disk2/t...	3 data brokers	OFF	Sync Completed	

- Follow the prompts to create a new data broker.

## Result

Cloud Sync adds the new data broker to the sync relationships. The performance of the next data sync should be accelerated.

## Changing the settings for a sync relationship

Modify settings that define how source files and folders are synced and maintained in the target location.

- Hover over the sync relationship and click the action menu.
- Click **Settings**.
- Modify any of the settings.

General		
Schedule	ON   Every 1 Day	▼
Retries	Retry 3 times before skipping file	▼
Files and Directories		
Recently Modified Files	Exclude files that are modified up to 30 Seconds before a scheduled sync	▼
Delete Files On Source	Never delete files from the source location	▼
Delete Files On Target	Never delete files from the target location	▼
Object Tagging	Allow Cloud Sync to tag S3 objects	▼
File Types	Include All: Files, Directories, Symbolic Links	▼
Exclude File Extensions	None	▼
File Size	All	▼
Date Modified	All	▼
<a href="#">Reset to defaults</a>		

Here's a brief description of each setting:

### Schedule

Choose a recurring schedule for future syncs or turn off the sync schedule. You can schedule a relationship to sync data as often as every 1 minute.

### Retries

Define the number of times that Cloud Sync should retry to sync a file before skipping it.

### Recently Modified Files

Choose to exclude files that were recently modified prior to the scheduled sync.

### Delete Files on Source

Choose to delete files from the source location after Cloud Sync copies the files to the target location. This option includes the risk of data loss because the source files are deleted after they're copied.

If you enable this option, you also need to change a parameter in the local.json file on the data broker. Open the file and change the parameter named `workers.transferrer.delete-on-source` to `true`.

## Delete Files on Target

Choose to delete files from the target location, if they were deleted from the source. The default is to never deletes files from the target location.

## Object tagging

When AWS S3 is the target in a sync relationship, Cloud Sync tags S3 objects with metadata that's relevant to the sync operation. You can disable tagging of S3 objects, if it's not desired in your environment. There's no impact to Cloud Sync if you disable tagging—Cloud Sync just stores the sync metadata in a different way.

## File Types

Define the file types to include in each sync: files, directories, and symbolic links.

## Exclude File Extensions

Specify file extensions to exclude from the sync by typing the file extension and pressing **Enter**. For example, type *log* or *.log* to exclude \*.log files. A separator isn't required for multiple extensions. The following video provides a short demo:

▶ [https://docs.netapp.com/us-en/occm/media/video\\_file\\_extensions.mp4](https://docs.netapp.com/us-en/occm/media/video_file_extensions.mp4) (video)

## File Size

Choose to sync all files regardless of their size or just files that are in a specific size range.

## Date Modified

Choose all files regardless of their last modified date, files modified after a specific date, before a specific date, or between a time range.

## Copy Access Control Lists to the target

Choose to copy access control lists (ACLs) between source SMB shares and target SMB shares. Note that this option is only available for sync relationships created after the 23 Feb 2020 release.

## 4. Click **Save Settings**.

## Result

Cloud Sync modifies the sync relationship with the new settings.

## Creating and viewing reports about paths

Create and view reports to get information that you can use with the help of NetApp personnel to tune a data broker's configuration and improve performance.

Each report provides in-depth details about a path in a sync relationship. For example, the report for a file system shows how many directories and files there are, the distribution of file size, how deep and wide the directories are, and more.

## Steps

### 1. Click **Reports**.

The paths (source or target) in each of your sync relationships display in a table.

### 2. In the **Reports** column, click **Create New** for a path.

### 3. When the report is ready, click **View**.

Here's a sample report for a file system path.

And here's a sample report for object storage.

## Deleting relationships

You can delete a sync relationship, if you no longer need to sync data between the source and target. This action does not delete the data broker instance and it does not delete data from the target.

### Steps

1. Hover over the sync relationship and click the action menu.
2. Click **Delete** and then click **Delete** again to confirm.

### Result

Cloud Sync deletes the sync relationship.

## Manage data brokers

A data broker syncs data from a source location to a target location. A data broker is required for each sync relationship that you create. Manage data brokers by adding a new data broker to a group, by viewing information about data brokers, and more.

### Data broker groups

Grouping data brokers together can help improve the performance of sync relationships.

#### Determining the number of data brokers

In many cases, a single data broker can meet the performance requirements for a sync relationship. If it doesn't, you can accelerate sync performance by adding additional data brokers to the group. But you should first check other factors that can impact sync performance. [Learn more about how to determine when multiple data brokers are required.](#)

#### Groups can manage several relationships

A data broker group can manage one or more sync relationships at a time.

For example, let's say you have three relationships:

- Relationship 1 uses data broker A
- Relationship 2 uses data broker B
- Relationship 3 uses data broker A

You want to accelerate the performance of relationship 1 so you add a new data broker (data broker C) to the group. Because data broker A is also used to manage relationship 3, having two data brokers in the group also accelerates the performance of this relationship.

## New data brokers only

You can only add new data brokers to a group. You can't add existing data brokers to a group.

## Add a new data broker

There are several ways to create a new data broker:

- When creating a new sync relationship

[Learn how to create a new data broker when creating a sync relationship.](#)

- From the **Manage Data Brokers** page by clicking **Add New Data Broker** which creates the data broker in a new group
- From the **Manage Data Brokers** page by creating a new data broker in an existing group

### Things you should know

- You can't add data brokers to a group that manages an encrypted sync relationship.
- If you want to create a data broker in an existing group, the data broker must be an on-prem data broker or the same type of data broker.

For example, if a group includes an AWS data broker, then you can create an AWS data broker or on-prem data broker in that group. You can't create an Azure data broker or GCP data broker because they aren't the same data broker type.

### Steps to create a data broker in a new group

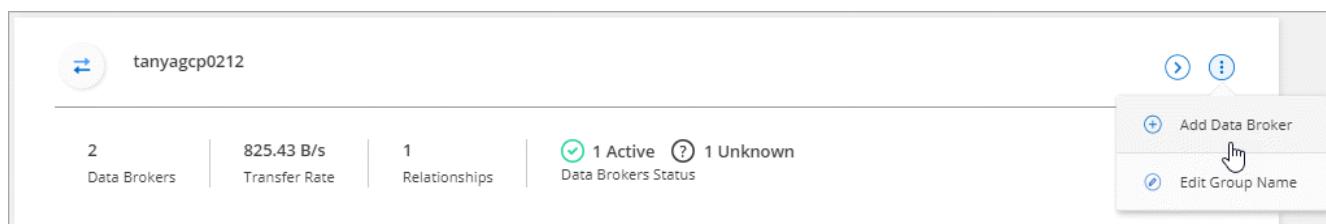
1. Click **Sync > Manage Data Brokers**.
2. Click **Add New Data Broker**.
3. Follow the prompts to create the data broker.

For help, refer to the following pages:

- [Installing the data broker in AWS](#)
- [Installing the data broker in Azure](#)
- [Installing the data broker in GCP](#)
- [Installing the data broker on a Linux host](#)

### Steps to create a data broker in an existing group

1. Click **Sync > Manage Data Brokers**.
2. Click the action menu and select **Add Data Broker**.



3. Follow the prompts to create the data broker.

For help, refer to the following pages:

- [Installing the data broker in AWS](#)
- [Installing the data broker in Azure](#)
- [Installing the data broker in GCP](#)
- [Installing the data broker on a Linux host](#)

## View a data broker's configuration

You might want to view details about a data broker to identify things like its host name, IP address, available CPU and RAM, and more.

Cloud Sync provides the following details about a data broker:

- Basic information: Instance ID, host name, etc.
- Network: Region, network, subnet, private IP, etc.
- Software: Linux distribution, data broker version, etc.
- Hardware: CPU and RAM
- Configuration: Details about the data broker's two kinds of main processes—scanner and transferrer



The scanner scans the source and target and decides what should be copied. The transferrer does the actual copying. NetApp personnel might use these configuration details to suggest actions that can optimize performance.

### Steps

1. Click **Sync > Manage Data Brokers**.
2. Click to expand the list of data brokers in a group.
3. Click to view details about a data broker.

tanyagcp0212

2 Data Brokers | 968.5 B/s Transfer Rate | 1 Relationships | 1 Active 1 Unknown Data Brokers Status

Information	5fc766b3d3e3664b9e116... Broker ID	288871247573080556 Instance ID	tanyagcp0212-mnx-data-... Host Name	cloudsync-dev-214020 Project Id
Network	us-east1-b Region	default Network	255.255.240.0 Subnet	10.142.0.37 Private IP
Software	linux Linux Distribution & Version	1.5.4 Vault Version	14.15.1 Node Version	1.3.0.18650-73f960d-integ Data Broker Version
Hardware	4 Available CPUs	62.22 MB Available RAM		
Configuration	50 Scanner Concurrency	4 Scanner CPUs	50 Transferrer Concurrency	4 Transferrer CPUs

## Remove a data broker from a group

You might remove a data broker from a group if it's no longer needed or if the initial deployment failed. This action only deletes the data broker from Cloud Sync's records. You'll need to manually delete the data broker and any additional cloud resources yourself.

### Things you should know

- Cloud Sync deletes a group when you remove the last data broker from the group.
- You can't remove the last data broker from a group if there is a relationship using that group.

### Steps

- Click **Sync > Manage Data Brokers**.
- Click to expand the list of data brokers in a group.
- Click the action menu for a data broker and select **Remove Data Broker**.

tanyagcp0212

2 Data Brokers | 968.5 B/s Transfer Rate | 1 Relationships | 1 Active 1 Unknown Data Brokers Status

tanyagcp0212	GCP	Transfer Rate: 968.5 B/s	Active
tanya1	ONPREM	Transfer Rate: N/A	Unknown

⋮ Remove Data Broker

#### 4. Click **Remove Data Broker**.

#### Result

Cloud Sync removes the data broker from the group.

### Edit a group's name

Change the name of a data broker group at any time.

#### Steps

1. Click **Sync > Manage Data Brokers**.
2. Click the action menu and select **Edit Group Name**.

The screenshot shows the 'Manage Data Brokers' page for a group named 'tanyagcp0212'. At the top right, there is an action menu with two options: 'Add Data Broker' and 'Edit Group Name'. The 'Edit Group Name' option is highlighted with a mouse cursor icon pointing to it.

3. Enter a new name and click **Save**.

#### Result

Cloud Sync updates the name of the data broker group.

### Address issues with a data broker

Cloud Sync displays a status for each data broker that can help you troubleshoot issues.

#### Steps

1. Identify any data brokers that have a status of "Unknown" or "Failed."

The screenshot shows the 'Manage Data Brokers' page for the 'tanyagcp0212' group. It lists two data brokers: 'tanyagcp0212' and 'tanya1'. The 'tanyagcp0212' broker is listed as 'Active' with a transfer rate of '968.5 B/s'. The 'tanya1' broker is listed as 'Unknown' with a transfer rate of 'N/A'. Each broker entry includes a status icon, a name, a type (GCP or ONPREM), a transfer rate, and a status indicator (green checkmark for Active, question mark for Unknown).

2. Hover over the icon to see the failure reason.

3. Correct the issue.

For example, you might need to simply restart the data broker if it's offline, or you might need to remove data broker if the initial deployment failed.

# Uninstalling the data broker

If needed, run an uninstall script to remove the data broker and the packages and directories that were created when the data broker was installed.

## Steps

1. Log in to the data broker host.
2. Change to the data broker directory: `/opt/netapp/databroker`
3. Run the following commands:

```
chmod +x uninstaller-DataBroker.sh  
./uninstaller-DataBroker.sh
```

4. Press 'y' to confirm the uninstallation.

# Cloud Sync APIs

The Cloud Sync capabilities that are available through the web UI are also available through the RESTful API.

## Getting started

To get started with the Cloud Sync API, you need to obtain a user token and your Cloud Central account ID. You'll need to add the token and account ID to the Authorization header when making API calls.

## Steps

1. Obtain a user token from NetApp Cloud Central.

```
POST https://netapp-cloud-account.auth0.com/oauth/token  
Header: Content-Type: application/json  
Body:  
{  
    "username": "<user_email>",  
    "scope": "profile",  
    "audience": "https://api.cloud.netapp.com",  
    "client_id": "UaVhOIXMWQs5i1WdDxauXe5Mqkb34NJQ",  
    "grant_type": "password",  
    "password": "<user_password>"  
}
```

2. Obtain your Cloud Central account ID.

```
GET https://api.cloudsync.netapp.com/api/accounts  
Headers: Authorization: Bearer <user_token>  
Content-Type: application/json
```

This API will return a response like the following:

```
[  
  {  
    "accountId": "account-JeL97Ry3",  
    "name": "Test"  
  }  
]
```

3. Add the user token and account ID in the Authorization header of each API call.

### Example

The following example shows an API call to create a data broker in Microsoft Azure. You would simply replace <user\_token> and <accountId> with the token and ID that you obtained in the previous steps.

```
POST https://api.cloudsync.netapp.com/api/data-brokers  
Headers: Authorization: Bearer <user_token>  
Content-Type: application/json  
x-account-id: <accountId>  
Body: { "name": "databroker1", "type": "AZURE" }
```

## What should I do when the token expires?

The user token from NetApp Cloud Central has an expiration date. To refresh the token, you need to call the API from step 1 again.

The API response includes an "expires\_in" field that states when the token expires.

## API reference

Documentation for each Cloud Sync API is available from <https://api.cloudsync.netapp.com/docs>.

## Using list APIs

List APIs are asynchronous APIs, so the result does not return immediately (for example: `GET /data-brokers/{id}/list-nfs-export-folders` and `GET /data-brokers/{id}/list-s3-buckets`). The only response from the server is HTTP status 202. To get the actual result, you must use the `GET /messages/client` API.

### Steps

1. Call the list API that you want to use.
2. Use the `GET /messages/client` API to view the result of the operation.
3. Use the same API by appending it with the ID that you just received: `GET http://api.cloudsync.netapp.com/api/messages/client?last=<id_from_step_2>`

Note that the ID changes each time that you call the `GET /messages/client` API.

## Example

When you call the `list-s3-buckets` API, a result is not immediately returned:

```
GET http://api.cloudsync.netapp.com/api/data-brokers/<data-broker-id>/list-s3-buckets
Headers: Authorization: Bearer <user_token>
Content-Type: application/json
x-account-id: <accountId>
```

The result is HTTP status code 202, which means the message was accepted, but was not processed yet.

To get the result of the operation, you need to use the following API:

```
GET http://api.cloudsync.netapp.com/api/messages/client
Headers: Authorization: Bearer <user_token>
Content-Type: application/json
x-account-id: <accountId>
```

The result is an array with one object that includes an ID field. The ID field represents the last message that the server sent. For example:

```
[
  {
    "header": {
      "requestId": "init",
      "clientId": "init",
      "agentId": "init"
    },
    "payload": {
      "init": {}
    },
    "id": "5801"
  }
]
```

You would now make the following API call using the ID that you just received:

```
GET  
http://api.cloudsync.netapp.com/api/messages/client?last=<id_from_step_2>  
Headers: Authorization: Bearer <user_token>  
Content-Type: application/json  
x-account-id: <accountId>
```

The result is an array of messages. Inside each message is a payload object, which consists of the name of the operation (as key) and its result (as value). For example:

```
[  
  {  
    "payload": {  
      "list-s3-buckets": [  
        {  
          "tags": [  
            {  
              "Value": "100$"  
              "Key": "price"  
            }  
          ],  
          "region": {  
            "displayName": "US West (Oregon)",  
            "name": "us-west-2"  
          },  
          "name": "small"  
        }  
      ]  
    },  
    "header": {  
      "requestId": "f687ac55-2f0c-40e3-9fa6-57fb8c4094a3",  
      "clientId": "5beb032f548e6e35f4ed1ba9",  
      "agentId": "5bed61f4489fb04e34a9aac6"  
    },  
    "id": "5802"  
  }  
]
```

## Cloud Sync technical FAQ

This FAQ can help if you're just looking for a quick answer to a question.

### Getting started

The following questions relate to getting started with Cloud Sync.

## **How does Cloud Sync work?**

Cloud Sync uses the NetApp data broker software to sync data from a source to a target (this is called a *sync relationship*).

The data broker controls the sync relationships between your sources and targets. After you set up a sync relationship, Cloud Sync analyzes your source system and breaks it up into multiple replication streams to push to your selected target data.

After the initial copy, the service syncs any changed data based on the schedule that you set.

## **How does the 14-day free trial work?**

The 14-day free trial starts when you sign up for the Cloud Sync service. You're not subject to NetApp charges for Cloud Sync relationships you create for 14 days. However, all resource charges for any data broker that you deploy still applies.

## **How much does Cloud Sync cost?**

There are two types of costs associated with using Cloud Sync: service charges and resource charges.

### **Service charges**

For pay-as-you-go pricing, Cloud Sync service charges are hourly, based on the number of sync relationships that you create.

- [View pay-as-you-go pricing in AWS](#)
- [View annual pricing in AWS](#)
- [View pricing in Azure](#)

Cloud Sync licenses are also available through your NetApp representative. Each license enables 20 sync relationships for 12 months.

[Learn more about licenses.](#)

### **Resource charges**

The resource charges are related to the compute and storage costs for running the data broker in the cloud.

## **How is Cloud Sync billed?**

There are two ways to pay for sync relationships after your 14-day free trial ends. The first option is to subscribe from AWS or Azure, which enables you to pay-as-you-go or to pay annually. The second option is to purchase licenses directly from NetApp.

## **Can I use Cloud Sync outside the cloud?**

Yes, you can use Cloud Sync in a non-cloud architecture. The source and target can reside on-premises and so can the data broker.

Note the following key points about using Cloud Sync outside of the cloud:

- For on-premises synchronization, a private Amazon S3 bucket is available through NetApp StorageGRID.
- The data broker does need an internet connection to communicate with the Cloud Sync service.

- If you don't purchase a license directly from NetApp, you will need an AWS or Azure account for the PAYGO Cloud Sync service billing.

## How do I access Cloud Sync?

Cloud Sync is available from Cloud Manager in the **Sync** tab.

## Supported sources and targets

The following questions related to the source and targets that are supported in a sync relationship.

### Which sources and targets does Cloud Sync support?

Cloud Sync supports many different types of sync relationships. [View the entire list.](#)

### What versions of NFS and SMB does Cloud Sync support?

Cloud Sync supports NFS version 3 and later, and SMB version 1 and later.

[Learn more about sync requirements.](#)

### When Amazon S3 is the target, can the data be tiered to a specific S3 storage class?

Yes, you can choose a specific S3 storage class when AWS S3 is the target:

- Standard (this is the default class)
- Intelligent-Tiering
- Standard-Infrequent Access
- One Zone-Infrequent Access
- Glacier
- Glacier Deep Archive

### What about storage tiers for Azure Blob storage?

You can choose a specific Azure Blob storage tier when a Blob container is the target:

- Hot storage
- Cool storage

## Networking

The following questions relate to networking requirements for Cloud Sync.

### What are the networking requirements for Cloud Sync?

The Cloud Sync environment requires that the data broker is connected with the source and the target through the selected protocol (NFS, SMB, EFS) or object storage API (Amazon S3, Azure Blob, IBM Cloud Object Storage).

In addition, the data broker needs an outbound internet connection over port 443 so it can communicate with the Cloud Sync service and contact a few other services and repositories.

For more details, [review networking requirements](#).

## Can I use a proxy server with the data broker?

Yes.

Cloud Sync supports proxy servers with or without basic authentication. If you specify a proxy server when you deploy a data broker, all HTTP and HTTPS traffic from the data broker is routed through the proxy. Note that non-HTTP traffic such as NFS or SMB can't be routed through a proxy server.

The only proxy server limitation is when using data-in-flight encryption with an NFS or Azure NetApp Files sync relationship. The encrypted data is sent over HTTPS and isn't routable through a proxy server.

## Data synchronization

The following questions relate to how data synchronization works.

### How often does synchronization occur?

The default schedule is set for daily synchronization. After the initial synchronization, you can:

- Modify the sync schedule to your desired number of days, hours, or minutes
- Disable the sync schedule
- Delete the sync schedule (no data will be lost; only the sync relationship will be removed)

### What is the minimum sync schedule?

You can schedule a relationship to sync data as often as every 1 minute.

### Does the data broker retry when a file fails to sync? Or does it timeout?

The data broker doesn't timeout when a single file fails to transfer. Instead, the data broker retries 3 times before skipping the file. The retry value is configurable in the settings for a sync relationship.

[Learn how to change the settings for a sync relationship.](#)

### What if I have a very large dataset?

If a single directory contains 600,000 files or more, [contact us](#) so we can help you configure the data broker to handle the payload. We might need to add additional memory to the data broker machine.

## Security

The following questions related to security.

### Is Cloud Sync secure?

Yes. All Cloud Sync service networking connectivity is done using [Amazon Simple Queue Service \(SQS\)](#).

All communication between the data broker and Amazon S3, Azure Blob, Google Cloud Storage, and IBM Cloud Object Storage is done through the HTTPS protocol.

If you're using Cloud Sync with on-premises (source or destination) systems, here's a few recommended

connectivity options:

- An AWS Direct Connect, Azure ExpressRoute, or Google Cloud Interconnect connection, which is non-internet routed (and can only communicate with the cloud networks that you specify)
- A VPN connection between your on-premises gateway device and your cloud networks
- For extra secure data transfer with S3 buckets, Azure Blob storage, or Google Cloud Storage, an Amazon Private S3 Endpoint, Azure Virtual Network service endpoints, or Private Google Access may be established.

Any of these methods establishes a secure connection between your on-premises NAS servers and a Cloud Sync data broker.

### **Is data encrypted by Cloud Sync?**

- Cloud Sync supports data-in-flight encryption between source and target NFS servers. [Learn more](#).
- Encryption is not supported with SMB.
- When an Amazon S3 bucket is the target in a sync relationship, you can choose whether to enable data encryption using AWS KMS encryption or AES-256 encryption.

## **Permissions**

The following questions relate to data permissions.

### **Are SMB data permissions synced to the target location?**

You can set up Cloud Sync to preserve access control lists (ACLs) between a source SMB share and a target SMB share. Or you can manually copy the ACLs yourself. [Learn how to copy ACLs between SMB shares](#).

### **Are NFS data permissions synced to the target location?**

Cloud Sync automatically copies NFS permissions between NFS servers as follows:

- NFS version 3: Cloud Sync copies the permissions and the user group owner.
- NFS version 4: Cloud Sync copies the ACLs.

## **Performance**

The following questions relate to Cloud Sync performance.

### **What does the progress indicator for a sync relationship represent?**

The sync relationship shows the throughput of the data broker's network adapter. If you accelerated sync performance by using multiple data brokers, then the throughput is the sum of all traffic. This throughput refreshes every 20 seconds.

### **I'm experiencing performance issues. Can we limit the number of concurrent transfers?**

The data broker can sync 4 files at a time. If you have very large files (multiple TBs each), it can take a long time to complete the transfer process and performance might be impacted.

Limiting the number of concurrent transfers can help. [Contact us for help](#).

## **Why am I experiencing low performance with Azure NetApp Files?**

When you sync data to or from Azure NetApp Files, you might experience failures and performance issues if the disk service level is Standard.

Change the service level to Premium or Ultra to enhance the sync performance.

[Learn more about Azure NetApp Files service levels and throughput.](#)

## **Why am I experiencing low performance with Cloud Volumes Service for AWS?**

When you sync data to or from a cloud volume, you might experience failures and performance issues if the level of performance for the cloud volume is Standard.

Change the Service level to Premium or Extreme to enhance the sync performance.

## **How many data brokers are required?**

When you create a new relationship, you start with a single data broker (unless you selected an existing data broker that belongs to an accelerated sync relationship). In many cases, a single data broker can meet the performance requirements for a sync relationship. If it doesn't, you can accelerate sync performance by adding additional data brokers. But you should first check other factors that can impact sync performance.

Multiple factors can impact data transfer performance. The overall sync performance might be impacted due to network bandwidth, latency, and network topology, as well as the data broker VM specs and storage system performance. For example, a single data broker in a sync relationship can reach 100 MB/s, while disk throughput on the target might only allow 64 MB/s. As a result, the data broker keeps trying to copy the data, but the target can't meet the performance of the data broker.

So be sure to check the performance of your networking and the disk throughput on the target.

Then you can consider accelerating sync performance by adding an additional data broker to share the load of that relationship. [Learn how to accelerate sync performance.](#)

## **Deleting things**

The following questions relate to deleting sync relationships and data from sources and targets.

### **What happens if I delete my Cloud Sync relationship?**

Deleting a relationship stops all future data syncs and terminates payment. Any data that was synced to the target remains as-is.

### **What happens if I delete something from my source server? Is it removed from the target too?**

By default, if you have an active sync relationship, the item deleted on the source server is not deleted from the target during the next synchronization. But there is an option in the sync settings for each relationship, where you can define that Cloud Sync will delete files in the target location if they were deleted from the source.

[Learn how to change the settings for a sync relationship.](#)

### **What happens if I delete something from my target? Is it removed from my source too?**

If an item is deleted from the target, it will not be removed from the source. The relationship is one-way—from source to target. On the next sync cycle, Cloud Sync compares the source to the target, identifies that the item

is missing, and Cloud Sync copies it again from the source to the target.

## Troubleshooting

[NetApp Knowledgebase: Cloud Sync FAQ: Support and Troubleshooting](#)

### Data broker deep dive

The following question relates to the data broker.

#### Can you explain the architecture of the data broker?

Sure. Here are the most important points:

- The data broker is a node.js application running on a Linux host.
- Cloud Sync deploys the data broker as follows:
  - AWS: From an AWS CloudFormation template
  - Azure: From Azure Resource Manager
  - Google: From Google Cloud Deployment Manager
  - If you use your own Linux host, you need to manually install the software
- The data broker software automatically upgrades itself to the latest version.
- The data broker uses AWS SQS as a reliable and secure communication channel and for control and monitoring. SQS also provides a persistency layer.
- You can add additional data brokers to a relationship to increase transfer speed and add high availability. There is service resiliency if one data broker fails.

# Gain insight into data privacy

## Learn about Cloud Compliance

Cloud Compliance is a data privacy and compliance service for Cloud Manager that scans your volumes, Amazon S3 buckets, databases, and OneDrive accounts to identify the personal and sensitive data that resides in those files. Using Artificial Intelligence (AI) driven technology, Cloud Compliance helps organizations understand data context and identify sensitive data.

[Learn about the use cases for Cloud Compliance.](#)

### Features

Cloud Compliance provides several tools that can help you with your compliance efforts. You can use Cloud Compliance to:

- Identify Personal Identifiable Information (PII)
- Identify a wide scope of sensitive information as required by GDPR, CCPA, PCI, and HIPAA privacy regulations
- Respond to Data Subject Access Requests (DSAR)
- Notify Cloud Manager users through email when files contain certain PII (you define this criteria using [highlights](#))
- View and modify [Azure Information Protection \(AIP\) labels](#) in your files
- Delete individual files

### Supported working environments and data sources

Cloud Compliance can scan data from the following types of data sources:

- Cloud Volumes ONTAP in AWS
- Cloud Volumes ONTAP in Azure
- On-premises ONTAP clusters
- Azure NetApp Files
- Amazon S3
- Databases that reside anywhere (there is no requirement that the database resides in a working environment)
- OneDrive accounts



A Beta feature released in January 2021 allows you to run Compliance scans for free on the backup files created from your on-prem ONTAP volumes (created using [Cloud Backup](#)). This gives you a choice whether you want to have Cloud Compliance scan your on-prem ONTAP volumes directly, or scan the backup files made from those volumes.

## Cost

- The cost to use Cloud Compliance depends on the amount of data that you're scanning. The first 1 TB of data that Cloud Compliance scans in a Cloud Manager workspace is free. This includes all data from all working environments and data sources. A subscription to the AWS or Azure Marketplace is required to continue scanning data after that point. See [pricing](#) for details.

[Learn how to subscribe.](#)

**Note:** This subscription is not needed to scan backup files created from your on-prem ONTAP systems.

- Installing Cloud Compliance in the cloud requires deploying a cloud instance, which results in charges from the cloud provider where it is deployed. See the [the type of instance that is deployed for each cloud provider](#). There is no cost if you install Cloud Compliance on an on-premises system.
- Cloud Compliance requires that you have deployed a Connector. In many cases you already have a Connector because of other storage and services you are using in Cloud Manager. The Connector instance results in charges from the cloud provider where it is deployed. See the [type of instance that is deployed for each cloud provider](#).

## Data transfer costs

Data transfer costs depend on your setup. If the Cloud Compliance instance and data source are in the same Availability Zone and region, then there are no data transfer costs. But if the data source, such as a Cloud Volumes ONTAP cluster or S3 Bucket, is in a *different* Availability Zone or region, then you'll be charged by your cloud provider for data transfer costs. See these links for more details:

- [AWS: Amazon EC2 Pricing](#)
- [Microsoft Azure: Bandwidth Pricing Details](#)

## How Cloud Compliance works

At a high-level, Cloud Compliance works like this:

- You deploy an instance of Cloud Compliance in Cloud Manager.
- You enable it on one or more working environments, databases, or OneDrive accounts.
- Cloud Compliance scans the data using an AI learning process.
- You click **Compliance** and use the provided dashboard and reporting tools to help in your compliance efforts.

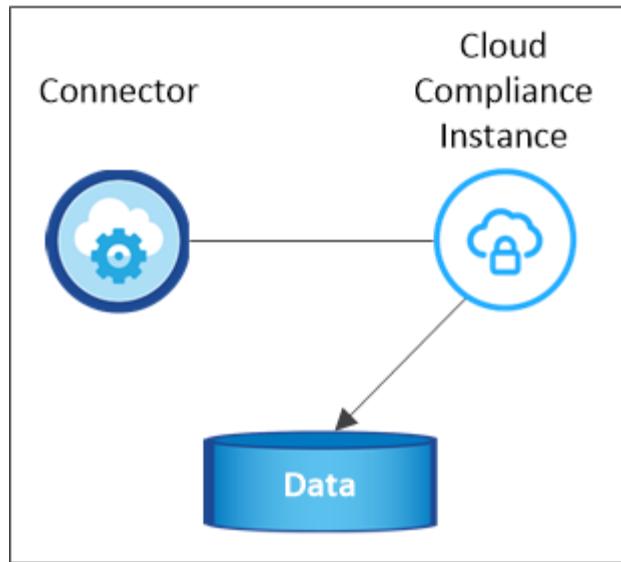
## The Cloud Compliance instance

When you deploy Cloud Compliance in the cloud, Cloud Manager deploys the instance in the same subnet as the Connector. [Learn more about Connectors.](#)



If the Connector is installed on-prem, it deploys the Cloud Compliance instance in same VPC or VNet as the first Cloud Volumes ONTAP system in the request.

## VPC or VNet



Note the following about the instance:

- In Azure, Cloud Compliance runs on a [Standard\\_D16s\\_v3 VM](#) with a 512 GB disk.
- In AWS, Cloud Compliance runs on an [m5.4xlarge instance](#) with a 500 GB GP2 disk.

In regions where m5.4xlarge isn't available, Cloud Compliance runs on an m4.4xlarge instance instead.



Changing or resizing the instance/VM type isn't supported. You need to use the size that's provided.

- The instance is named *CloudCompliance* with a generated hash (UUID) concatenated to it. For example: *CloudCompliance-16bb6564-38ad-4080-9a92-36f5fd2f71c7*
- Only one Cloud Compliance instance is deployed per Connector.
- Upgrades of Cloud Compliance software is automated—you don't need to worry about it.



The instance should remain running at all times because Cloud Compliance continuously scans the data.

## How scans work

After you enable Cloud Compliance and select the volumes, buckets, database schemas, or OneDrive users you want to scan, it immediately starts scanning the data to identify personal and sensitive data. It maps your organizational data, categorizes each file, and identifies and extracts entities and predefined patterns in the data. The result of the scan is an index of personal information, sensitive personal information, data categories, and file types.

Cloud Compliance connects to the data like any other client by mounting NFS and CIFS volumes. NFS volumes are automatically accessed as read-only, while you need to provide Active Directory credentials to scan CIFS volumes.

After the initial scan, Cloud Compliance continuously scans your data to detect incremental changes (this is

why it's important to keep the instance running).

You can enable and disable scans at the [volume level](#), at the [bucket level](#), the [database schema level](#), and at the [OneDrive user level](#).

## Information that Cloud Compliance indexes

Cloud Compliance collects, indexes, and assigns categories to your data (files). The data that Cloud Compliance indexes includes the following:

### Standard metadata

Cloud Compliance collects standard metadata about files: the file type, its size, creation and modification dates, and so on.

### Personal data

Personally identifiable information such as email addresses, identification numbers, or credit card numbers. [Learn more about personal data](#).

### Sensitive personal data

Special types of sensitive information, such as health data, ethnic origin, or political opinions, as defined by GDPR and other privacy regulations. [Learn more about sensitive personal data](#).

### Categories

Cloud Compliance takes the data that it scanned and divides it into different types of categories. Categories are topics based on AI analysis of the content and metadata of each file. [Learn more about categories](#).

### Types

Cloud Compliance takes the data that it scanned and breaks it down by file type. [Learn more about types](#).

### Name entity recognition

Cloud Compliance uses AI to extract natural persons' names from documents. [Learn about responding to Data Subject Access Requests](#).

## Networking overview

Cloud Manager deploys the Cloud Compliance instance with a security group that enables inbound HTTP connections from the Connector instance.

When using Cloud Manager in SaaS mode, the connection to Cloud Manager is served over HTTPS, and the private data sent between your browser and the Cloud Compliance instance are secured with end-to-end encryption, which means NetApp and third parties can't read it.

If you need to use the local user interface instead of the SaaS user interface for any reason, you can still [access the local UI](#).

Outbound rules are completely open. Internet access is needed to install and upgrade the Cloud Compliance software and to send usage metrics.

If you have strict networking requirements, [learn about the endpoints that Cloud Compliance contacts](#).

## User access to compliance information

The role each user has been assigned provides different capabilities within Cloud Manager and within Cloud

Compliance:

- **Account Admins** can manage compliance settings and view compliance information for all working environments.
- **Workspace Admins** can manage compliance settings and view compliance information only for systems that they have permissions to access. If a Workspace Admin can't access a working environment in Cloud Manager, then they can't see any compliance information for the working environment in the Compliance tab.
- Users with the **Cloud Compliance Viewer** role can only view compliance information and generate reports for systems that they have permission to access. These users cannot enable/disable scanning of volumes, buckets, or database schemas.

[Learn more about Cloud Manager roles](#) and how to [add users with specific roles](#).

## Get started

### Deploy Cloud Compliance

Complete a few steps to deploy the Cloud Compliance instance in your Cloud Manager workspace. You can deploy Cloud Compliance in the cloud or on an on-premises system.

The on-prem installation may be a good option if you prefer to scan on-premises ONTAP working environments using a Compliance instance that is also located on premises. But this is not a requirement. The Compliance software functions exactly the same way regardless of which installation method you choose.

#### Quick start

Get started quickly by following these steps or scroll down to the remaining sections for full details.



#### Create a Connector

If you don't already have a Connector, create a Connector in Azure or AWS. See [creating a Connector in AWS](#) or [creating a Connector in Azure](#).

You can also [deploy the Connector on-premises](#) on an existing Linux host in your network or in the cloud.



#### Review prerequisites

Ensure that your environment can meet the prerequisites. This includes outbound internet access for the instance, connectivity between the Connector and Cloud Compliance over port 80, and more. [See the complete list](#).

- When installed in the cloud, you need 16 vCPUs for the Cloud Compliance instance. See [more details about the instance type](#).
- When installed on premises, you need a Linux system that meets the [following requirements](#).

### 3

## Deploy Cloud Compliance

Launch the installation wizard to deploy the Cloud Compliance instance.

You can deploy Cloud Compliance in the cloud or in an on-premises location. The only difference you'll notice in the UI is the words "On-Premises Deployment".



### 4

## Subscribe to the Cloud Compliance service

The first 1 TB of data that Cloud Compliance scans in Cloud Manager is free. A subscription to the AWS or Azure Marketplace is required to continue scanning data after that point.

### Creating a Connector

If you don't already have a Connector, create a Connector in Azure or AWS. See [creating a Connector in AWS](#) or [creating a Connector in Azure](#). In most cases you will probably have a Connector set up before you attempt to activate Cloud Compliance because most [Cloud Manager features require a Connector](#), but there are cases when you need to set one up now.

There are some scenarios where you have to use a Connector in AWS or Azure for Cloud Compliance.

- When scanning data in Cloud Volumes ONTAP in AWS or in AWS S3 buckets, you use a connector in AWS.
- When scanning data in Cloud Volumes ONTAP in Azure or in Azure NetApp Files, you use a connector in Azure.
- Databases, OneDrive folders, and on-prem ONTAP systems can be scanned using either Connector.

Note that you can also [deploy the Connector on-premises](#) on an existing Linux host in your network or in the cloud. Some users planning to install Cloud Compliance on-prem may also choose to install the Connector on-prem.

As you can see, there may be some situations where you need to use [multiple Connectors](#).



If you are planning on scanning Azure NetApp Files, you need to make sure you're deploying in the same region as the volumes you wish to scan.

### Reviewing prerequisites

Review the following prerequisites to make sure that you have a supported configuration before you deploy Cloud Compliance.

### Enable outbound internet access from Cloud Compliance

Cloud Compliance requires outbound internet access. If your virtual or physical network uses a proxy server

for internet access, ensure that the Cloud Compliance instance has outbound internet access to contact the following endpoints. When you deploy Cloud Compliance in the cloud, it is located in the same subnet as the Connector.

Review the appropriate table below depending on whether you are deploying Cloud Compliance in AWS, Azure, or on-premises.

#### **Required endpoints for AWS deployments:**

Endpoints	Purpose
<a href="https://cloudmanager.cloud.netapp.com">https://cloudmanager.cloud.netapp.com</a>	Communication with the Cloud Manager service, which includes Cloud Central accounts.
<a href="https://netapp-cloud-account.auth0.com">https://netapp-cloud-account.auth0.com</a> <a href="https://auth0.com">https://auth0.com</a>	Communication with NetApp Cloud Central for centralized user authentication.
<a href="https://cloud-compliance-support-netapp.s3.us-west-2.amazonaws.com">https://cloud-compliance-support-netapp.s3.us-west-2.amazonaws.com</a> <a href="https://hub.docker.com">https://hub.docker.com</a> <a href="https://auth.docker.io">https://auth.docker.io</a> <a href="https://registry-1.docker.io">https://registry-1.docker.io</a> <a href="https://index.docker.io/">https://index.docker.io/</a> <a href="https://dseasb33srnrrn.cloudfront.net/">https://dseasb33srnrrn.cloudfront.net/</a> <a href="https://production.cloudflare.docker.com/">https://production.cloudflare.docker.com/</a>	Provides access to software images, manifests, and templates.
<a href="https://kinesis.us-east-1.amazonaws.com">https://kinesis.us-east-1.amazonaws.com</a>	Enables NetApp to stream data from audit records.
<a href="https://cognito-idp.us-east-1.amazonaws.com">https://cognito-idp.us-east-1.amazonaws.com</a> <a href="https://cognito-identity.us-east-1.amazonaws.com">https://cognito-identity.us-east-1.amazonaws.com</a> <a href="https://user-feedback-store-prod.s3.us-west-2.amazonaws.com">https://user-feedback-store-prod.s3.us-west-2.amazonaws.com</a> <a href="https://customer-data-production.s3.us-west-2.amazonaws.com">https://customer-data-production.s3.us-west-2.amazonaws.com</a>	Enables Cloud Compliance to access and download manifests and templates, and to send logs and metrics.

#### **Required endpoints for Azure and On-Prem deployments:**

Endpoints	Purpose
<a href="https://cloudmanager.cloud.netapp.com">https://cloudmanager.cloud.netapp.com</a>	Communication with the Cloud Manager service, which includes Cloud Central accounts.
<a href="https://netapp-cloud-account.auth0.com">https://netapp-cloud-account.auth0.com</a> <a href="https://auth0.com">https://auth0.com</a>	Communication with NetApp Cloud Central for centralized user authentication.
<a href="https://support.compliance.cloudmanager.cloud.netapp.com/">https://support.compliance.cloudmanager.cloud.netapp.com/</a> <a href="https://hub.docker.com">https://hub.docker.com</a> <a href="https://auth.docker.io">https://auth.docker.io</a> <a href="https://registry-1.docker.io">https://registry-1.docker.io</a> <a href="https://index.docker.io/">https://index.docker.io/</a> <a href="https://dseasb33srnrrn.cloudfront.net/">https://dseasb33srnrrn.cloudfront.net/</a> <a href="https://production.cloudflare.docker.com/">https://production.cloudflare.docker.com/</a>	Provides access to software images, manifests, and templates.

Endpoints	Purpose
<a href="https://support.compliance.cloudmanager.cloud.netapp.com/">https://support.compliance.cloudmanager.cloud.netapp.com/</a>	Enables NetApp to stream data from audit records.
<a href="https://support.compliance.cloudmanager.cloud.netapp.com/">https://support.compliance.cloudmanager.cloud.netapp.com/</a>	Enables Cloud Compliance to access and download manifests and templates, and to send logs and metrics.
<b>On-premises installs only:</b> <a href="https://github.com/docker">https://github.com/docker</a> <a href="https://download.docker.com">https://download.docker.com</a> <a href="https://rhui3.us-west-2.aws.ce.redhat.com">https://rhui3.us-west-2.aws.ce.redhat.com</a> <a href="https://github-production-release-asset-2e65be.s3.amazonaws.com">https://github-production-release-asset-2e65be.s3.amazonaws.com</a> <a href="https://pypi.org">https://pypi.org</a> <a href="https://pypi.python.org">https://pypi.python.org</a> <a href="https://files.pythonhosted.org">https://files.pythonhosted.org</a> <a href="http://mirror.centos.org">http://mirror.centos.org</a> <a href="http://mirrorlist.centos.org">http://mirrorlist.centos.org</a> <a href="http://mirror.centos.org/centos/7/extras/x86_64/Packages/container-selinux-2.107-3.el7.noarch.rpm">http://mirror.centos.org/centos/7/extras/x86_64/Packages/container-selinux-2.107-3.el7.noarch.rpm</a>	Provides prerequisite packages for installation.

### Ensure that Cloud Manager has the required permissions

Ensure that Cloud Manager has permissions to deploy resources and create security groups for the Cloud Compliance instance. You can find the latest Cloud Manager permissions in [the policies provided by NetApp](#).

### Check your vCPU limits

When installed in the cloud, ensure that your cloud provider's vCPU limit allows for the deployment of an instance with 16 cores. You'll need to verify the vCPU limit for the relevant instance family in the region where Cloud Manager is running.

In AWS, the instance family is *On-Demand Standard instances*. In Azure, the instance family is *Standard Dsv3 Family*.

For more details on vCPU limits, see the following:

- [AWS documentation: Amazon EC2 Service Limits](#)
- [Azure documentation: Virtual machine vCPU quotas](#)

### Ensure that Cloud Manager can access Cloud Compliance

Ensure connectivity between the Connector and the Cloud Compliance instance. The security group for the Connector must allow inbound and outbound traffic over port 80 to and from the Cloud Compliance instance.

This connection enables deployment of the Cloud Compliance instance and enables you to view information in the Compliance tab.

### Ensure that you can keep Cloud Compliance running

The Cloud Compliance instance needs to stay on to continuously scan your data.

## Ensure web browser connectivity to Cloud Compliance

After Cloud Compliance is enabled, ensure that users access the Cloud Manager interface from a host that has a connection to the Cloud Compliance instance.

The Cloud Compliance instance uses a private IP address to ensure that the indexed data isn't accessible to the internet. As a result, the web browser that you use to access Cloud Manager must have a connection to that private IP address. That connection can come from a direct connection to AWS or Azure (for example, a VPN), or from a host that's inside the same network as the Cloud Compliance instance.

## Deploying the Cloud Compliance instance in the cloud

Deploying an instance of Cloud Compliance in the cloud is the most common deployment model. But you have the option to [deploy the Compliance software on a Linux host](#) in your network or in the cloud.

The Compliance software functions exactly the same way regardless of which installation method you choose.

### Steps

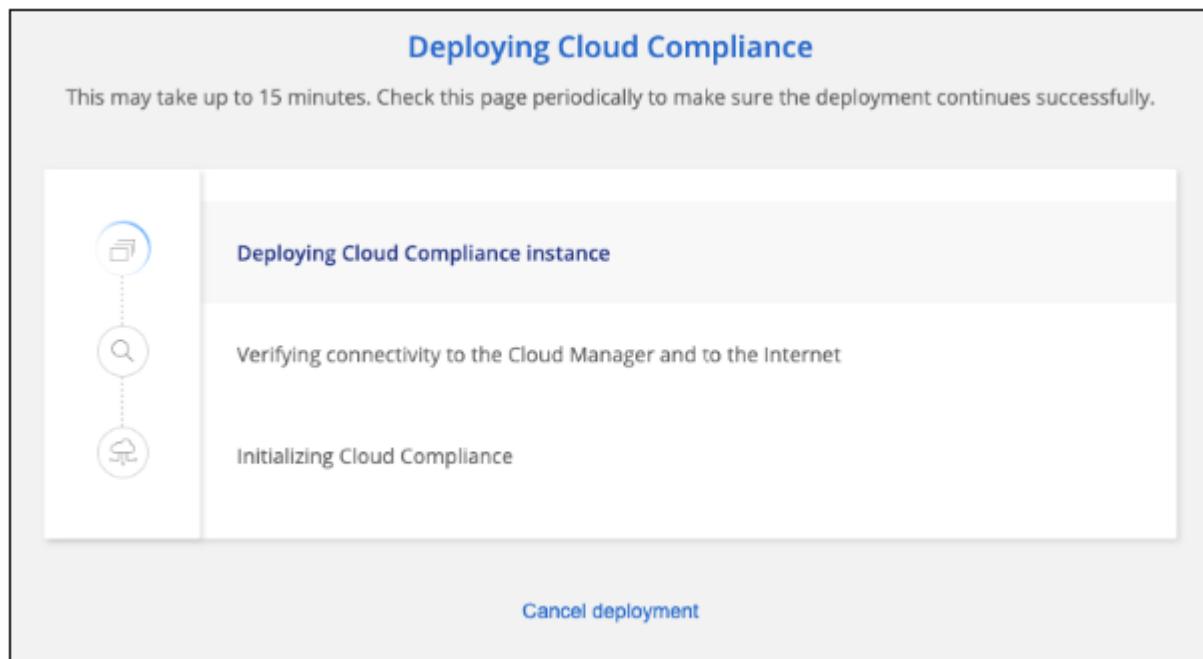
1. In Cloud Manager, click **Compliance**.
2. Click **Activate Cloud Compliance**.

The screenshot shows the Cloud Compliance dashboard. On the left, there's a sidebar with a 'Cloud Compliance' icon and a 'How does it work?' link. The main area features a heading 'Always-on Privacy & Compliance Controls' with a subtext about automated controls for GDPR, CCPA, etc., driven by AI. Below this is a large blue button labeled 'Activate Cloud Compliance' with a red border. To the right is a 'Compliance Status' section with a circular progress bar, a 'Data Distribution' chart, and two tables showing file counts for Personal and Sensitive Personal files across categories like Email Address and Credit Card.

3. Click **Activate Compliance** to start the deployment wizard.

This screenshot shows a modal dialog titled 'Select where to deploy the Compliance connector'. It offers two options: 'Deploy Compliance connector in the Cloud' (marked as 'Recommended') and 'Deploy Compliance connector On-Premises'. Each option has a detailed description below it. To the right of each description is a blue 'Activate Compliance' button with a red border. A small upward arrow icon is positioned next to the second button.

4. The wizard displays progress as it goes through the deployment steps. It will stop and ask for input if it runs into any issues.



5. When the instance is deployed, click **Continue to configuration** to go to the *Scan Configuration* page.

## Result

Cloud Manager deploys the Cloud Compliance instance in your cloud provider.

## What's Next

From the Scan Configuration page you can select the data sources that you want to scan.

You can also [subscribe to the Cloud Compliance service](#) at this time. You will not be charged until the amount of data exceeds 1 TB.

## Deploying the Cloud Compliance instance on premises

The most common way to deploy Cloud Compliance is to [deploy it in the cloud](#). But you have the option to download and install the Compliance software on a Linux host in your network.

The Compliance software functions exactly the same regardless of which installation method you choose.



Cloud Compliance is currently unable to scan S3 buckets and Azure NetApp Files when the Compliance instance is installed on premises. In these cases you'll need to deploy a separate Connector and instance of Compliance in the cloud and [switch between Connectors](#) for your different data sources.

## Host requirements

- Operating system: Red Hat Enterprise Linux or CentOS version 8.0 or 8.1
  - Version 7.8 can be used, but the Linux kernel version must be 4.14 or greater
  - The OS must be capable of installing the docker engine (for example, disable the *firewalld* service if needed)

- RAM: 64 GB (swap memory must be disabled on the host)
- CPU: 16 cores
- Disk: 500 GB SSD
- A Red Hat Enterprise Linux system must be registered with Red Hat Subscription Management. If it is not registered, the system cannot access repositories to update required 3rd party software during installation.
- Make sure port 8080 is open so you can see the installation progress in Cloud Manager.
- Root privileges are required to install Cloud Compliance.

See [Reviewing prerequisites](#) for the full list of requirements and endpoints that Cloud Compliance must be able to reach over the internet.

## Steps

1. Download the Cloud Compliance software from the [NetApp Support Site](#).
2. Copy the installer file to the Linux host you plan to use (using `scp` or some other method).
3. In Cloud Manager, click **Compliance**.
4. Click **Activate Cloud Compliance**.

The screenshot shows the Cloud Compliance dashboard. At the top left is a logo and the text "Cloud Compliance". Below it is a link "How does it work?". The main heading is "Always-on Privacy & Compliance Controls". A sub-section below it says "Automated controls for data privacy regulations such as the GDPR, CCPA and more. Driven by powerful artificial intelligence algorithms, Cloud Compliance gets your business application data and cloud environments privacy ready." To the right is a "Compliance Status" section with a circular progress bar, a "Data Distribution" chart, and several data summary cards:

Compliance Status	
	75% Non-Sensitive
20%	Personal
5%	Sensitive Personal
28,000 Personal Files	<a href="#">View All</a>
7,000 Sensitive Personal Files	<a href="#">View All</a>
Email Address	2,700 Files
Credit Card	2,700 Files
Health	2,700 Files
Ethnicity	2,700 Files

5. Click **Activate Compliance**.

The screenshot shows a dialog titled "Select where to deploy the Compliance connector". It contains two main options:

- Deploy Compliance connector in the Cloud** (with a "Recommended" label) - This option has its own "Activate Compliance" button.
- Deploy Compliance connector On-Premises** - This option also has its own "Activate Compliance" button, which is highlighted with a red box.

Below the "On-Premises" option is a note: "For special situations, for example, if you wish to scan on-premises Working Environments and you prefer the Compliance Connector accesses the data from an on-premises location."

6. In the *Deploy Cloud Compliance On Premises* dialog, copy the provided command and paste it in a text file

so you can use it later. For example:

```
sudo ./install.sh -a 12345 -c 27AG75 -t 2198qq
```

7. Unzip the installer file on the host machine:

```
tar -xzf cc_onprem_installer.tar.gz
```

8. When prompted by the installer, you can enter the required values in a series of prompts, or you can enter the complete command in the first prompt:

Enter parameters as prompted:	Enter the full command:
<ol style="list-style-type: none"><li>Paste the information you copied from step 6: <code>sudo ./install.sh -a &lt;account_id&gt; -c &lt;agent_id&gt; -t &lt;token&gt;</code></li><li>Enter the IP address or host name of the Compliance host machine so it can be accessed by the Connector instance.</li><li>Enter the IP address or host name of the Cloud Manager Connector host machine so it can be accessed by the Cloud Compliance instance.</li><li>Enter proxy details as prompted. If your Cloud Manager already uses a proxy, there is no need to enter this information again here since Cloud Compliance will automatically use the proxy used by Cloud Manager.</li></ol>	Alternatively, you can create the whole command in advance and enter it in the first prompt: <code>sudo ./install.sh -a &lt;account_id&gt; -c &lt;agent_id&gt; -t &lt;token&gt; --host &lt;cc_host&gt; --cm-host &lt;cm_host&gt; --proxy-host &lt;proxy_host&gt; --proxy-port &lt;proxy_port&gt; --proxy-scheme &lt;proxy_scheme&gt; --proxy-user &lt;proxy_user&gt; --proxy-password &lt;proxy_password&gt;</code>

Variable values:

- *account\_id* = NetApp Account ID
- *agent\_id* = Connector ID
- *token* = jwt user token
- *cc\_host* = IP address or host name of the Cloud Compliance Linux system.
- *cm\_host* = IP address or host name of the Cloud Manager Connector system.
- *proxy\_host* = IP or host name of the proxy server if the host is behind a proxy server.
- *proxy\_port* = Port to connect to the proxy server (default 80).
- *proxy\_scheme* = The connection schema: https or http (default http).
- *proxy\_user* = Authenticated user to connect to the proxy server, if basic authentication is required.
- *proxy\_password* = Password for the user name that you specified.

## Result

The Cloud Compliance installer installs packages, installs docker, registers the installation, and installs Cloud Compliance. Installation can take 10 to 20 minutes.

If there is connectivity over port 8080 between the host machine and the Connector instance, you will see the installation progress in the Compliance tab in Cloud Manager.

## What's Next

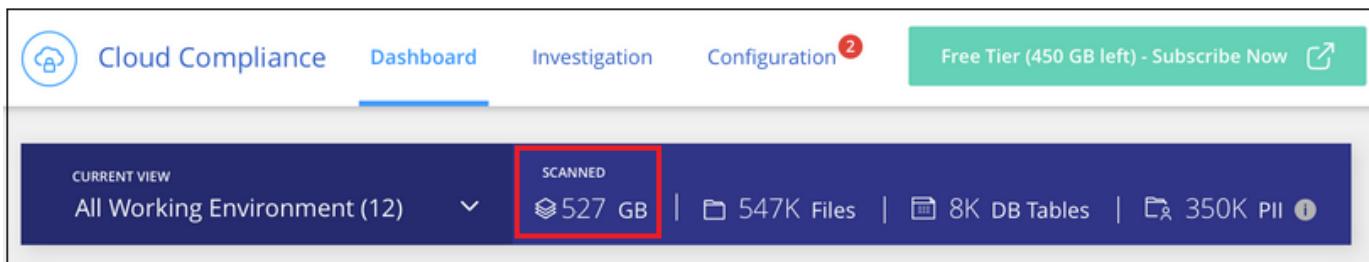
From the Scan Configuration page you can select the data sources that you want to scan.

You can also [subscribe to the Cloud Compliance service](#) at this time. You will not be charged until the amount of data exceeds 1 TB. A subscription to either the AWS or Azure Marketplace can be used when you have deployed Cloud Compliance on an on-premises system.

## Subscribing to the Cloud Compliance service

The first 1 TB of data that Cloud Compliance scans in a Cloud Manager workspace is free. A subscription to the AWS or Azure Marketplace is required to continue scanning data after that point.

You can subscribe at any time and you will not be charged until the amount of data exceeds 1 TB. You can always see the total amount of data that is being scanned from the Cloud Compliance Dashboard. And the *Subscribe Now* button makes it easy to subscribe when you are ready.



**Note:** If you are prompted by Cloud Compliance to subscribe, but you already have an Azure subscription, you're probably using the old **Cloud Manager** subscription and you need to change to the new **NetApp Cloud Manager** subscription. See [Changing to the new NetApp Cloud Manager plan in Azure](#) for details.

## Steps

These steps must be completed by a user who has the *Account Admin* role.

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



2. Find the credentials for the AWS Instance Profile or Azure Managed Service Identity.

The subscription must be added to the Instance Profile or Managed Service Identity. Charging won't work otherwise.

If you already have a subscription, then you're all set—there's nothing else that you need to do.

The screenshot shows the AWS Instance Profile page. At the top, it says "aws Instance Profile" and "Credential Type: AWS Keys". Below that, there's a section for "AWS Account ID" which is blurred. To the right of this, a red arrow points down to the "Subscription" section. The "Subscription" section contains the text "metering service subscription QA !!!!". On the right side of the page, there are two columns: "OCCM" (with "IAM Role" below it) and "0 Working Environments".

3. If you don't have a subscription yet, hover over the credentials and click the action menu.
4. Click **Add Subscription**.

The screenshot shows the same AWS Instance Profile page as before, but now the "Add Subscription" button in the blue header bar is highlighted with a white background and a black border. The rest of the page content remains the same, including the blurred AWS Account ID and the "No Subscription" entry in the list.

5. Click **Add Subscription**, click **Continue**, and follow the steps.

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

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

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

► [https://docs.netapp.com/us-en/occm/media/video\\_subscribing\\_azure.mp4](https://docs.netapp.com/us-en/occm/media/video_subscribing_azure.mp4) (video)

### Changing to the new Cloud Manager plan in Azure

Cloud Compliance was added to the Azure Marketplace subscription named **NetApp Cloud Manager** as of October 7, 2020. If you already have the original Azure **Cloud Manager** subscription it will not allow you to use Cloud Compliance.

You need to follow these steps to change to the new **NetApp Cloud Manager** subscription before you can start using Cloud Compliance.



If your existing Subscription was issued with a special private offer, you need to contact NetApp so that we can issue a new special private offer with Compliance included.

## Steps

1. In the upper right of the Cloud Manager console, click the Settings icon, and select **Credentials**.
2. Find the credentials for the Azure Managed Service Identity that you want to change the subscription for and hover over the credentials and click **Associate Subscription**.  
The details for your current Marketplace Subscription are displayed.
3. Log in to the [Azure portal](#) and select **Software as a Service (SaaS)**.
4. Select the subscription for which you want to change the plan and click **Change Plan**.

The screenshot shows the Azure portal interface for managing SaaS subscriptions. On the left, a list of subscriptions is shown, with 'shiranSub3008' selected. On the right, the 'Offer and plan details' page for this subscription is displayed. The 'Cloud Manager - Cloud Manager - Monthly NetApp' plan is selected. A red box highlights the 'Change plan' button, which is located under the 'Cloud Manager - Monthly' section. The 'Billing term & price' section shows 'Monthly \$0.00 per month'. Below the main plan information, there is a 'Plus:' section listing various cloud storage and backup services with their respective prices.

Cloud Manager - Monthly	Billing term & price
Subscribed	Monthly \$0.00 per month
OLD PLAN - DOES NOT INCLUDE COMPLIANCE	
<a href="#">Change plan</a>	
<a href="#">View this offer in Marketplace</a>	
<a href="#">Terms of use</a>   <a href="#">Privacy policy</a>	

**Plus:**

- CVO Explore HA upto 2TB in HA pair \$0.49/node/hour: \$0.49 per node
- Backup CVO to Blob \$50/TB per month (calc hourly): \$0.07 per tb/hour
- CVO Standard HA 10TB in HA pair \$1.77/node/hour: \$1.77 per node
- Restore CVO to Blob \$50/TB per month (calc hourly): \$0.07 per tb/hour
- CVO Standard plan, up to 10TB (\$1.98/node/hour): \$1.98 per node
- CVO Premium HA 368TB in HA pair \$2.56/node/hour: \$2.56 per node
- CVO Premium plan, up to 368TB (\$3.19/node/hour): \$3.19 per node
- Cloud Tiering for On Prem ONTAP (\$0.07/TB/hour): \$0.07 per tb/hour
- CVO Explore plan, up to 2TB (\$0.75/node/hour): \$0.75 per node

5. In the Change Plan page, select the **NetApp Cloud Manager** plan and click the **Change Plan** button.

## Change plan

Subscription plans

**i** You can only change plans within the billing term of the current plan. If you would like to make further changes please view this offer in the Marketplace, you might need to unsubscribe and resubscribe to a new subscription plan to accomodate more changes.

Billing term  Monthly  Yearly

Software plan	Description	Price
<input checked="" type="radio"/> NetApp Cloud Manager	PLAN - INCLUDES COMPLIANCE	\$0.00 per month  Plus: CVO Explore HA upto 2TB in HA pair \$0.49/node/hour: \$0.49 per node CVO Premium plan, up to 368TB (\$3.19/node/hour): \$3.19 per node CVO Standard plan, up to 10TB (\$1.98/node/hour): \$1.98 per node Cloud Compliance \$50/TB/Month: \$0.068 per tb/hour CVO Premium HA 368TB in HA pair \$2.56/node/hour: \$2.56 per node CVO Standar HA 10TB in HA pair \$1.77/node/hour: \$1.77 per node Cloud Tiering for On Prem ONTAP (\$0.07/TB/hour): \$0.07 per tb/hour Backup CVO to Blob \$50/TB per month (calc hourly): \$0.07 per tb/hour CVO Explore plan, up to 2TB (\$0.75/node/hour): \$0.75 per node
<input type="radio"/> Cloud Manager	OLD PLAN - DOES NOT INCLUDE COMPLIANCE	\$0.00 per month  <b>i</b> Current plan  Plus: CVO Explore HA upto 2TB in HA pair \$0.49/node/hour: \$0.49 per node Backup CVO to Blob \$50/TB per month (calc hourly): \$0.07 per tb/hour CVO Standar HA 10TB in HA pair \$1.77/node/hour: \$1.77 per node Restore CVO to Blob \$50/TB per month (calc hourly): \$0.07 per tb/hour CVO Standard plan, up to 10TB (\$1.98/node/hour): \$1.98 per node CVO Premium HA 368TB in HA pair \$2.56/node/hour: \$2.56 per node CVO Premium plan, up to 368TB (\$3.19/node/hour): \$3.19 per node Cloud Tiering for On Prem ONTAP (\$0.07/TB/hour): \$0.07 per tb/hour CVO Explore plan, up to 2TB (\$0.75/node/hour): \$0.75 per node

**Change plan**

**Cancel**

6. Return to Cloud Manager, select the subscription, and hover over the “i” above subscription in the Credentials card to verify your subscription has changed.

## Activate scanning on your data sources

### Getting started with Cloud Compliance for Cloud Volumes ONTAP, on-premises ONTAP, or Azure NetApp Files

Complete a few steps to get started with Cloud Compliance for Cloud Volumes ONTAP, on-premises ONTAP systems, or Azure NetApp Files.

#### Quick start

Get started quickly by following these steps or scroll down to the remaining sections for full details.

1

#### Discover the data sources that contain the data you want to scan

Before you can scan volumes, you must add the systems to working environments in Cloud Manager:

- For Cloud Volumes ONTAP systems, these working environments should already be available in Cloud Manager
- For on-premises ONTAP systems, [Cloud Manager must discover the ONTAP clusters](#)
- For Azure NetApp Files, [Cloud Manager must be set up to discover the configuration](#).

**2**

## Deploy the Cloud Compliance instance

Deploy [Cloud Compliance in Cloud Manager](#) if there isn't already an instance deployed.

**3**

## Enable Cloud Compliance in your working environments and select the volumes to scan

Click **Compliance**, select the **Configuration** tab, and activate compliance scans for volumes in specific working environments.

**4**

## Ensure access to volumes

Now that Cloud Compliance is enabled, ensure that it can access volumes.

- The Cloud Compliance instance needs a network connection to each Cloud Volumes ONTAP subnet, Azure NetApp Files subnet, or on-prem ONTAP system.
- Security groups for Cloud Volumes ONTAP must allow inbound connections from the Cloud Compliance instance.
- NFS volume export policies must allow access from the Cloud Compliance instance.
- Cloud Compliance needs Active Directory credentials to scan CIFS volumes.

Click **Compliance > Scan Configuration > Edit CIFS Credentials** and provide the credentials.

**5**

## Manage the volumes you want to scan

Select or deselect the volumes that you want to scan and Cloud Compliance will start or stop scanning them.

### Discovering the data sources that you want to scan

If the data sources you want to scan are not already in your Cloud Manager environment, you can add them to the canvas at this time.

Your Cloud Volumes ONTAP systems should already be available in the Canvas in Cloud Manager. For on-premises ONTAP systems you need to have [Cloud Manager discover these clusters](#). And for Azure NetApp Files, [Cloud Manager must be set up to discover the configuration](#).

### Deploying the Cloud Compliance instance

[Deploy Cloud Compliance](#) if there isn't already an instance deployed.

Cloud Compliance can be deployed in the cloud or in an on-premises location when scanning Cloud Volumes ONTAP or on-premises ONTAP systems.

Cloud Compliance must be deployed in the cloud when scanning Azure NetApp Files volumes, and it must be deployed in the same region as the volumes you wish to scan.

## Enabling Cloud Compliance in your working environments

You can enable Cloud Compliance on Cloud Volumes ONTAP systems (in AWS and Azure), on-premises ONTAP clusters, and Azure NetApp Files.



Following these steps for on-prem ONTAP systems scans the volumes directly on the on-prem ONTAP system. If you are already creating backup files from those on-prem systems using [Cloud Backup](#), you can run compliance scans on the backup files in the cloud instead. Go to [Scanning backup files from on-premises ONTAP systems](#) to scan the volumes by scanning the backup files.

1. At the top of Cloud Manager, click **Compliance** and then select the **Configuration** tab.

The screenshot shows the 'Scan Configuration' page in Cloud Manager. It lists three working environments:

- Working Environment 1**: On-Premises ONTAP. It features a blue icon with two horizontal bars. A blue button labeled 'Activate Compliance for All Volumes' is present, along with a link 'or select Volumes'.
- Azure Netapp Files**: Azure NetApp Files. It features a blue icon with a stylized 'N'. A blue button labeled 'Activate Compliance for All Volumes' is present, along with a link 'or select Volumes'.
- Working Environment Name 1**: Cloud Volumes ONTAP. It features a purple icon with a white cloud. A blue button labeled 'Activate Compliance for All Volumes' is present, along with a link 'or select Volumes'.

2. To scan all volumes in a working environment, click **Activate Compliance for All Volumes**.

To scan only certain volumes in a working environment, click **or select Volumes** and then choose the volumes you want to scan.

See [Enabling and disabling compliance scans on volumes](#) for details.

## Result

Cloud Compliance starts scanning the volumes you selected in the working environment. Results will be available in the Compliance dashboard as soon as Cloud Compliance finishes the initial scans. The time that it takes depends on the amount of data—it could be a few minutes or hours.

#### Verifying that Cloud Compliance has access to volumes

Make sure that Cloud Compliance can access volumes by checking your networking, security groups, and export policies. You'll need to provide Cloud Compliance with CIFS credentials so it can access CIFS volumes.

#### Steps

1. Make sure that there's a network connection between the Cloud Compliance instance and each network that includes volumes for Cloud Volumes ONTAP, Azure NetApp Files, or on-prem ONTAP clusters.

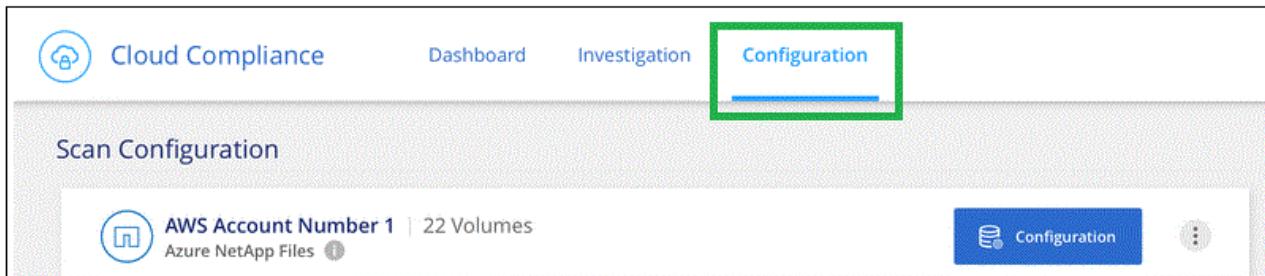


For Azure NetApp Files, Cloud Compliance can only scan volumes that are in the same region as Cloud Manager.

2. Ensure that the security group for Cloud Volumes ONTAP allows inbound traffic from the Cloud Compliance instance.

You can either open the security group for traffic from the IP address of the Cloud Compliance instance, or you can open the security group for all traffic from inside the virtual network.

3. Ensure that NFS volume export policies include the IP address of the Cloud Compliance instance so it can access the data on each volume.
4. If you use CIFS, provide Cloud Compliance with Active Directory credentials so it can scan CIFS volumes.
  - a. At the top of Cloud Manager, click **Compliance**.
  - b. Click the **Configuration** tab.



- c. For each working environment, click **Edit CIFS Credentials** and enter the user name and password that Cloud Compliance needs to access CIFS volumes on the system.

The credentials can be read-only, but providing admin credentials ensures that Cloud Compliance can read any data that requires elevated permissions. The credentials are stored on the Cloud Compliance instance.

After you enter the credentials, you should see a message that all CIFS volumes were authenticated successfully.

Name: Newdatastore

Volumes:

- 12 Continuously Scanning
- 8 Not Scanning

CIFS Credentials Status: Valid CIFS credentials for all accessible volumes

- On the **Scan Configuration** page, click **View Details** to review the status for each CIFS and NFS volume and correct any errors.

For example, the following image shows three volumes; one of which Cloud Compliance can't scan due to network connectivity issues between the Cloud Compliance instance and the volume.

Activate Compliance for all Volumes | 28/28 Volumes selected for compliance scan

Compliance	Name	Protocol	Status	Required Action
<input checked="" type="checkbox"/>	10.160.7.6:/yuval22	NFS	Continuously Scanning	
<input checked="" type="checkbox"/>	10.160.7.6:/yuvalnewtarget	NFS	Continuously Scanning	
<input checked="" type="checkbox"/>	\\\10.160.7.6\Danny_share	CIFS	No Access	The CIFS credentials that you provided have expired. Edit the CIFS credential...

### Enabling and disabling compliance scans on volumes

You can stop or start scanning volumes in a working environment at any time from the Scan Configuration page. We recommend that you scan all volumes.

Activate Compliance for all Volumes | 27/28 Volumes selected for compliance scan

Compliance	Volume Name	Status	Required Action
<input checked="" type="checkbox"/>	VolumeName1	Not Scanning	Add CIFS Credentials
<input checked="" type="checkbox"/>	VolumeName2	Continuously Scanning	
<input checked="" type="checkbox"/>	VolumeName3	Not Scanning	
<input checked="" type="checkbox"/>	VolumeName4	Continuously Scanning	
<input checked="" type="checkbox"/>	VolumeName5	Continuously Scanning	

To:	Do this:
Disable scanning for a volume	Move the volume slider to the left

To:	Do this:
Disable scanning for all volumes	Move the <b>Activate Compliance for all Volumes</b> slider to the left
Enable scanning for a volume	Move the volume slider to the right
Enable scanning for all volumes	Move the <b>Activate Compliance for all Volumes</b> slider to the right



New volumes added to the working environment are automatically scanned only when the **Activate Compliance for all Volumes** setting is enabled. When this setting is disabled, you'll need to activate scanning on each new volume you create in the working environment.

### Scanning backup files from on-premises ONTAP systems

If you don't want Cloud Compliance to scan volumes directly on your on-prem ONTAP systems, a new Beta feature released in January 2021 allows you to run compliance scans on backup files created from your on-prem ONTAP volumes. So if you are already creating backup files using [Cloud Backup](#), you can use this new feature to run compliance scans on those backup files.

The Compliance scans you run on backup files are **free** - no Cloud Compliance subscription or license is needed.

**Note:** When Compliance scans backup files it uses permissions granted through the Restore instance to access the backup files. Typically the Restore instance powers down when not actively restoring files, but it remains on when scanning backup files. See [more information about the Restore instance](#).

### Steps

If you want to scan the backup files from on-prem ONTAP systems:

1. At the top of Cloud Manager, click **Compliance** and then select the **Configuration** tab.
2. From the list of working environments, click the **BACKUP** button from the list of filters.

All the on-premises ONTAP working environments that have backup files are listed. If you don't have any backup files in an on-prem system, then the working environment is not shown.

The screenshot shows the Cloud Compliance Configuration page. At the top, there's a navigation bar with tabs: Cloud Compliance, Dashboard, Reports, Investigation, Highlights, and Configuration (which is underlined). Below the navigation bar, there's a section titled '(2/20) Working Environments'. Underneath this, there are several filter buttons: CVO, ANF, S3, DB, ONEDR, and BACKUP (which is highlighted with a red box). To the right of these filters is a 'Clear filters' link. Below the filters, there's a list of working environments. The first item in the list is 'Working Environment 1 (back up)', described as 'Cloud Backup of ONTAP' and marked as 'BETA'. At the bottom of the page, there's a large blue button with the text 'Activate Compliance for all Backed Up Volumes'. A red arrow points to this button. Below the button, there's another text field with the placeholder 'or select Volumes' and a red arrow pointing to it.

3. To scan all backed up volumes in a working environment, click **Activate Compliance for all backed up Volumes**.

To scan only certain backed up volumes in a working environment, click **or select Volumes** and then choose the backup files (volumes) that you want to scan.

See [Enabling and disabling compliance scans on volumes](#) for details.

### Scanning on-prem volumes versus backups of those volumes

When you view the entire list of working environments you will see two listings for each on-prem cluster if they have backed up files.

The screenshot shows the 'Scan Configuration' interface. It displays two items for a single 'Working Environment 1' (On-Premises ONTAP). Item 1 is labeled 'Activate Compliance for All Volumes' and has a red '1' icon. Item 2 is labeled 'Activate Compliance for all backed up Volumes' and has a red '2' icon. Both items include a 'or select Volumes' link below them. The 'Working Environment 1' section also includes a 'Cloud Backup of ONTAP' section with a 'BETA' label.

The first item is the on-prem cluster and the actual volumes.

The second item is the backup files from that same on-prem cluster.

Choose the first option to scan the volumes on the on-prem system. Choose the second option to scan the backup files from those volumes. Do not scan both on-prem volumes and backup files of the same cluster.

### Scanning data protection volumes

By default, data protection (DP) volumes are not scanned because they are not exposed externally and Cloud Compliance cannot access them. These are the destination volumes for SnapMirror operations from an on-premises ONTAP system or from a Cloud Volumes ONTAP system.

Initially, the volume list identifies these volumes as **Type DP** with the **Status Not Scanning** and the **Required Action Enable Access to DP volumes**.

**'Working Environment Name' Scan Configuration**

Activate Compliance for all Volumes | 22/28 Volumes selected for compliance scan | Enable Access to DP Volumes | Edit CIFS Credentials

Compliance	Volume Name	Type	Status	Required Action
<input checked="" type="checkbox"/>	VolumeName1	DP	<span style="color: red;">● Not Scanning</span>	Enable access to DP Volumes <span style="color: red;">(1)</span>
<input checked="" type="checkbox"/>	VolumeName2	NFS	<span style="color: green;">● Continuously Scanning</span>	
<input checked="" type="checkbox"/>	VolumeName3	CIFS	<span style="color: gray;">● Not Scanning</span>	

## Steps

If you want to scan these data protection volumes:

1. Click the **Enable Access to DP volumes** button at the top of the page.
2. Review the confirmation message and click **Enable Access to DP volumes** again.
  - Volumes that were initially created as NFS volumes in the source ONTAP system are enabled.
  - Volumes that were initially created as CIFS volumes in the source ONTAP system require that you enter CIFS credentials to scan those DP volumes. If you already entered Active Directory credentials so that Cloud Compliance can scan CIFS volumes you can use those credentials, or you can specify a different set of Admin credentials.

**Provide Active Directory Credentials**

Use existing CIFS Scanning Credentials (user1@domain2)  Use Custom Credentials

Active Directory Domain (1) DNS IP Address (1)

DP Volumes, created from a SnapMirror relationship, do not allow external access by default. Continuing will create NFS shares from DP Volumes which have been activated for Compliance. The shares' export policies will allow access only from the Cloud Compliance instance. [Learn More](#)

**Enable Access to DP Volumes** **Cancel**

**Provide Active Directory Credentials**

Use existing CIFS Scanning Credentials (user1@domain2)  Use Custom Credentials

Username (1) Password (1)

Active Directory Domain (1) DNS IP Address (1)

DP Volumes, created from a SnapMirror relationship, do not allow external access by default. Continuing will create NFS shares from DP Volumes which have been activated for Compliance. The shares' export policies will allow access only from the Cloud Compliance instance. [Learn More](#)

**Enable Access to DP Volumes** **Cancel**

3. Activate each DP volume that you want to scan [the same way you enabled other volumes](#), or use the **Activate Compliance for all Volumes** control to enable all volumes, including all DP volumes.

## Result

Once enabled, Cloud Compliance creates an NFS share from each DP volume that was activated for Compliance so that it can be scanned. The share export policies only allow access from the Cloud Compliance instance.

**Note:** If you had no CIFS data protection volumes when you initially enabled access to DP volumes, and later add some, the button **Enable Access to CIFS DP** appears at the top of the Scan Configuration page. Click this button and add CIFS credentials to enable access to these CIFS DP volumes.

## Getting started with Cloud Compliance for Amazon S3

Cloud Compliance can scan your Amazon S3 buckets to identify the personal and sensitive data that resides in S3 object storage. Cloud Compliance can scan any bucket in the account, regardless if it was created for a NetApp solution.

### Quick start

Get started quickly by following these steps, or scroll down to the remaining sections for full details.



#### 1 Set up the S3 requirements in your cloud environment

Ensure that your cloud environment can meet the requirements for Cloud Compliance, including preparing an IAM role and setting up connectivity from Cloud Compliance to S3. [See the complete list.](#)



#### 2 Deploy the Cloud Compliance instance

Deploy Cloud Compliance if there isn't already an instance deployed.



#### 3 Activate Compliance on your S3 working environment

Select the Amazon S3 working environment, click **Enable Compliance**, and select an IAM role that includes the required permissions.



#### 4 Select the buckets to scan

Select the buckets that you'd like to scan and Cloud Compliance will start scanning them.

### Reviewing S3 prerequisites

The following requirements are specific to scanning S3 buckets.

### Set up an IAM role for the Cloud Compliance instance

Cloud Compliance needs permissions to connect to the S3 buckets in your account and to scan them. Set up an IAM role that includes the permissions listed below. Cloud Manager prompts you to select an IAM role when you enable Cloud Compliance on the Amazon S3 working environment.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:Get*",
        "s3>List*",
        "s3:PutObject",
        "s3:HeadBucket"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:GetPolicyVersion",
        "iam:GetPolicy",
        "iam>ListAttachedRolePolicies"
      ],
      "Resource": [
        "arn:aws:iam::*:policy/*",
        "arn:aws:iam::*:role/*"
      ]
    }
  ]
}

```

## Provide connectivity from Cloud Compliance to Amazon S3

Cloud Compliance needs a connection to Amazon S3. The best way to provide that connection is through a VPC Endpoint to the S3 service. For instructions, see [AWS Documentation: Creating a Gateway Endpoint](#).

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

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

An alternative is to provide the connection by using a NAT Gateway.



You can't use a proxy to get to S3 over the internet.

## Deploying the Cloud Compliance instance

[Deploy Cloud Compliance in Cloud Manager](#) if there isn't already an instance deployed.

You need to deploy the instance in an AWS Connector so that Cloud Manager automatically discovers the S3

buckets in this AWS account and displays them in an Amazon S3 working environment.

**Note:** Deploying Cloud Compliance in an on-premises location is not currently supported when scanning S3 buckets.

#### Activating Compliance on your S3 working environment

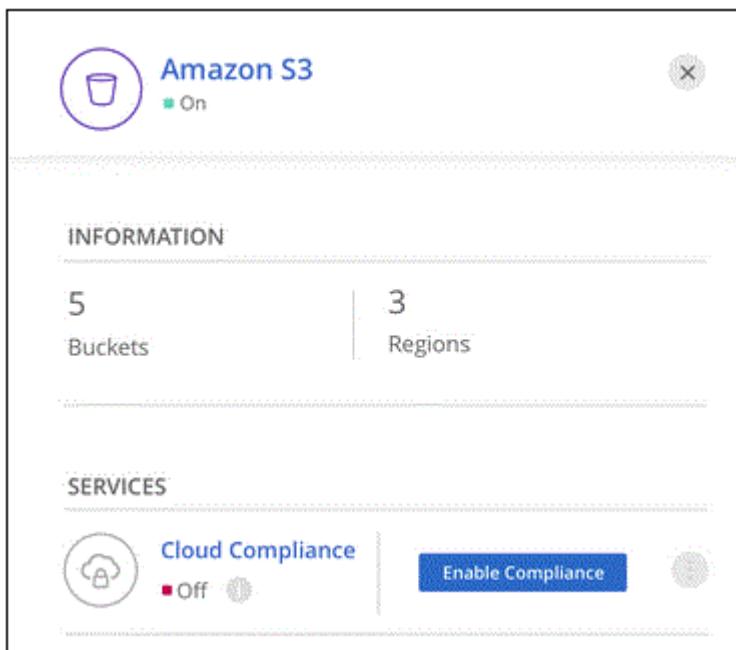
Enable Cloud Compliance on Amazon S3 after you verify the prerequisites.

#### Steps

1. At the top of Cloud Manager, click **Canvas**.
2. Select the Amazon S3 working environment.



3. In the pane on the right, click **Enable Compliance**.



4. When prompted, assign an IAM role to the Cloud Compliance instance that has [the required permissions](#).

## Assign an AWS IAM Role for Cloud Compliance

To enable Cloud Compliance on Amazon S3 buckets, select an existing IAM role. Make sure that your AWS IAM role has the permission defined in the [Policy Requirements](#).

### Select IAM Role

NetAppCloudCompliance

#### VPC Endpoint for Amazon S3 Required

A VPC endpoint to the Amazon S3 service is required so Cloud Compliance can securely scan the data.

Alternatively, ensure that the Cloud Compliance instance has direct access to the internet via a NAT Gateway or Internet Gateway.

#### Free for the 1st TB

Over 1 TB you pay only for what you use. [Learn more about pricing](#).

**Enable Compliance**

**Cancel**

### 5. Click **Enable Compliance**.



You can also enable compliance scans for a working environment from the Scan Configuration page by clicking the button and selecting **Activate Compliance**.

### Result

Cloud Manager assigns the IAM role to the instance.

### Enabling and disabling compliance scans on S3 buckets

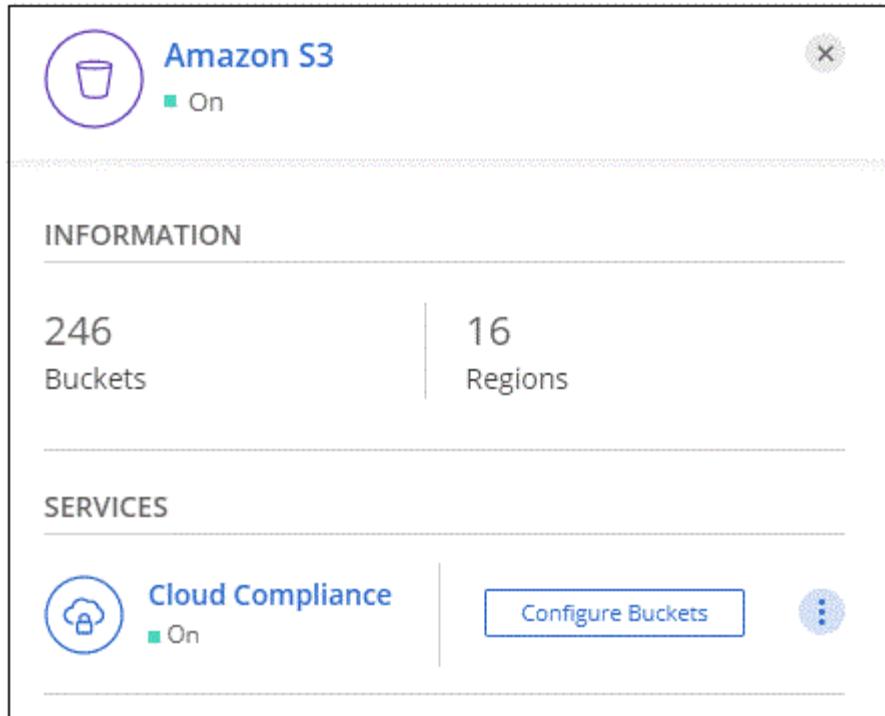
After Cloud Manager enables Cloud Compliance on Amazon S3, the next step is to configure the buckets that you want to scan.

When Cloud Manager is running in the AWS account that has the S3 buckets you want to scan, it discovers those buckets and displays them in an Amazon S3 working environment.

Cloud Compliance can also [scan S3 buckets that are in different AWS accounts](#).

### Steps

1. Select the Amazon S3 working environment.
2. In the pane on the right, click **Configure Buckets**.



3. Enable compliance on the buckets that you want to scan.

The image shows the "Amazon S3 Scan Configuration" page. At the top left is a circular icon with a cloud and lock symbol. To its right, the text "Cloud Compliance" is displayed above a green square with the word "On". On the far right is a magnifying glass icon. Below this, the heading "Amazon S3 Scan Configuration" is shown, followed by the text "15/28 Buckets in Scan Scope. Toggle ON/OFF to enable Compliance per Bucket". A table follows, with columns: "Compliance", "Bucket Name", "Status", and "Required Action". The table rows are:

Compliance	Bucket Name	Status	Required Action
<input checked="" type="checkbox"/>	BucketName1	● Not Scanning	Add Credentials
<input checked="" type="checkbox"/>	BucketName2	● Continuously Scanning	
<input type="checkbox"/>	BucketName3	● Not Scanning	

## Result

Cloud Compliance starts scanning the S3 buckets that you enabled. If there are any errors, they'll appear in the Status column, alongside the required action to fix the error.

### Scanning buckets from additional AWS accounts

You can scan S3 buckets that are under a different AWS account by assigning a role from that account to access the existing Cloud Compliance instance.

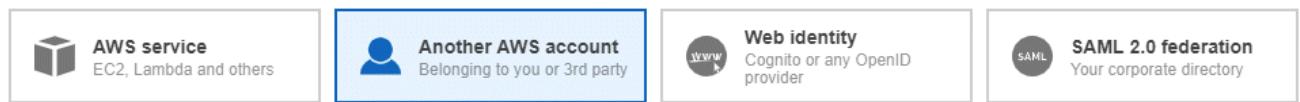
### Steps

1. Go to the target AWS account where you want to scan S3 buckets and create an IAM role by selecting **Another AWS account**.

## Create role

1 2 3 4

### Select type of trusted entity



Allows entities in other accounts to perform actions in this account. [Learn more](#)

### Specify accounts that can use this role

Account ID\*  ⓘ

Options  Require external ID (Best practice when a third party will assume this role)  
 Require MFA ⓘ

### Be sure to do the following:

- Enter the ID of the account where the Cloud Compliance instance resides.
- Change the **Maximum CLI/API session duration** from 1 hour to 12 hours and save that change.
- Attach the Cloud Compliance IAM policy. Make sure it has the required permissions.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "s3:Get*",  
                "s3>List*",  
                "s3:PutObject",  
                "s3:HeadBucket"  
            ],  
            "Resource": "*"  
        },  
    ]  
}
```

2. Go to the source AWS account where the Cloud Compliance instance resides and select the IAM role that is attached to the instance.
  - a. Change the **Maximum CLI/API session duration** from 1 hour to 12 hours and save that change.
  - b. Click **Attach policies** and then click **Create policy**.
  - c. Create a policy that includes the "sts:AssumeRole" action and the ARN of the role that you created in the target account.

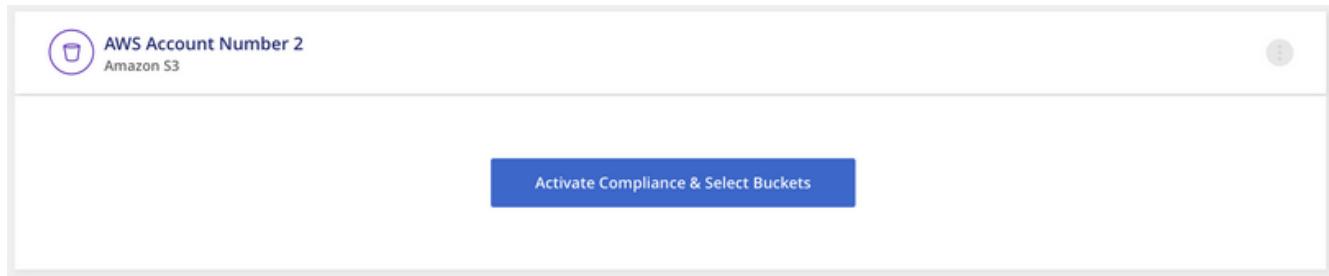
```

{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "sts:AssumeRole",
            "Resource": "arn:aws:iam::<ADDITIONAL-ACCOUNT-ID>:role/<ADDITIONAL_ROLE_NAME>"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam>ListAttachedRolePolicies"
            ],
            "Resource": [
                "arn:aws:iam::*:policy/*",
                "arn:aws:iam::*:role/*"
            ]
        }
    ]
}

```

The Cloud Compliance instance profile account now has access to the additional AWS account.

3. Go to the **Amazon S3 Scan Configuration** page and the new AWS account is displayed. Note that it can take a few minutes for Cloud Compliance to sync the new account's working environment and show this information.



4. Click **Activate Compliance & Select Buckets** and select the buckets you want to scan.

## Result

Cloud Compliance starts scanning the new S3 buckets that you enabled.

### Scanning database schemas

Complete a few steps to start scanning your database schemas with Cloud Compliance.

## Quick start

Get started quickly by following these steps or scroll down to the remaining sections for full details.



### Review database prerequisites

Ensure that your database is supported and that you have the information necessary to connect to the database.



### Deploy the Cloud Compliance instance

[Deploy Cloud Compliance](#) if there isn't already an instance deployed.



### Add the database server

Add the database server that you want to access.



### Select the schemas

Select the schemas that you want to scan.

#### Reviewing prerequisites

Review the following prerequisites to make sure that you have a supported configuration before you enable Cloud Compliance.

#### Supported databases

Cloud Compliance can scan schemas from the following databases:

- MongoDB
- MySQL
- Oracle
- PostgreSQL
- SAP HANA
- SQL Server (MSSQL)



The statistics gathering feature **must be enabled** in the database.

#### Database requirements

Any database with connectivity to the Cloud Compliance instance can be scanned, regardless of where it is hosted. You just need the following information to connect to the database:

- IP Address or host name

- Port
- Service name (only for accessing Oracle databases)
- Credentials that allow read access to the schemas

When choosing a user name and password, it's important to choose one that has full read permissions to all the schemas and tables you want to scan. We recommend that you create a dedicated user for the Cloud Compliance system with all the required permissions.

**Note:** For MongoDB, a read-only Admin role is required.

#### Adding the database server

You must have [deployed an instance of Cloud Compliance in Cloud Manager already](#).

Add the database server where the schemas reside.

1. From the Working Environments Configuration page, click **Add Data Source > Add Database Server**.

2. Enter the required information to identify the database server.
  - Select the database type.
  - Enter the port and the host name or IP address to connect to the database.
  - For Oracle databases, enter the Service name.
  - Enter the credentials so that Cloud Compliance can access the server.
  - Click **Add DB Server**.

## Add DB Server

To activate Compliance on Databases, first add a Database Server. After this step, you'll be able to select which Database Schemas you would like to activate Compliance for.

### Database

Database Type

Host Name or IP Address

Port

Service Name

### Credentials

Username

Password

Add DB Server

Cancel

The database is added to the list of working environments.

### Enabling and disabling compliance scans on database schemas

You can stop or start scanning schemas at any time.

1. From the *Scan Configuration* page, click the **Configuration** button for the database you want to configure.

Scan Configuration

Oracle DB 1 | 41 Schemas Oracle

No Schemas selected for Compliance

7 Not Scanning View Details

Configuration

2. Select the schemas that you want to scan by moving the slider to the right.

'Working Environment Name' Scan Configuration			
28/28 Schemas selected for compliance scan			Edit Credentials
Compliance	Schema Name	Status	Required Action
<input checked="" type="checkbox"/>	DB1 - SchemaName1	<span style="color: red;">●</span> Not Scanning	Add Credentials
<input checked="" type="checkbox"/>	DB1 - SchemaName2	<span style="color: green;">●</span> Continuously Scanning	
<input checked="" type="checkbox"/>	DB1 - SchemaName3	<span style="color: green;">●</span> Continuously Scanning	
<input checked="" type="checkbox"/>	DB1 - SchemaName4	<span style="color: green;">●</span> Continuously Scanning	

## Result

Cloud Compliance starts scanning the database schemas that you enabled. If there are any errors, they'll appear in the Status column, alongside the required action to fix the error.

## Scanning OneDrive accounts

Complete a few steps to start scanning files in your user's OneDrive folders with Cloud Compliance.

### Quick start

Get started quickly by following these steps or scroll down to the remaining sections for full details.

1

### Review OneDrive prerequisites

Ensure that you have the Admin credentials to log into the OneDrive account.

2

### Deploy the Cloud Compliance instance

Deploy Cloud Compliance if there isn't already an instance deployed.

3

### Add the OneDrive account

Using Admin user credentials, log into the OneDrive account that you want to access so that it is added as a new working environment.

4

### Add the users

Add the list of users from the OneDrive account that you want to scan. You can add up to 100 users at time.

## Reviewing prerequisites

Review the following prerequisites to make sure that you have a supported configuration before you enable Cloud Compliance.

## OneDrive requirements

You must have the Admin login credentials for the OneDrive for Business account that provides read access to all user files.

You will need a line-separated list of the email addresses for all the users whose OneDrive folders you want to scan.

### Adding the OneDrive account

You must have [deployed an instance of Cloud Compliance in Cloud Manager already](#).

Add the OneDrive account where the user files reside.

1. From the Working Environments Configuration page, click **Add Data Source > Add OneDrive Account**.

The screenshot shows the 'Working Environments' page with a filter bar at the top. The 'CVO' filter is selected. Below the filter bar, there is a list of working environments. The first item is 'Working Environment Name 1 | 127 Volumes' (Cloud Volumes ONTAP). To the right of this list is a 'Clear filters' button. A dropdown menu titled 'Add Data Source' is open, showing three options: 'Add Database Server' (with a database icon), 'Add OneDrive Account' (with a OneDrive icon, which is highlighted with a red box), and 'Add AWS S3 accounts' (with an S3 icon).

2. In the Add a OneDrive account dialog, click **Sign in to OneDrive**.
3. In the Microsoft page that appears, select the OneDrive account and enter the required Admin user and password, then click **Accept** to allow Cloud Compliance to read data from this account.

The OneDrive account is added to the list of working environments.

### Adding OneDrive users to compliance scans

You can add individual OneDrive users, or all of your OneDrive users, so that their files will be scanned by Cloud Compliance.

1. From the *Scan Configuration* page, click the **Configuration** button for the OneDrive account.

The screenshot shows the 'Scan Configuration' page. At the top left is the title 'Scan Configuration'. At the top right is a 'Add Data Source' button. Below the title, there is a list of accounts. The first item is 'OneDrive Account 1 | 41 Users' (OneDrive icon). To the right of this list is a 'Configuration' button, which is highlighted with a green box. There is also a more options button represented by three vertical dots.

2. If this is the first time adding users for this OneDrive account, click **Add your first OneDrive users**.

## 'Working Environment Name' Scan Configuration



No OneDrive users are being scanned

+ Add your first OneDrive users

If you are adding additional users, click **Add OneDrive users**.

## 'Working Environment Name' Scan Configuration

24 users are being scanned for compliance

+ Add OneDrive users

Username	Status	Required Action
user2@example.com	● Continuously Scanning	...
user3@example.com	● Continuously Scanning	...

3. Add the email addresses for the users whose files you want to scan - one email address per line (up to 100 maximum per session) - and click **Add Users**.

### Add OneDrive users

Provide a list of OneDrive users for Cloud Compliance to scan their data, line-separated. You can add up to 100 users at a time.

Type or paste below the OneDrive user accounts to add

User Accounts

user@example.com  
user@example.com  
user@example.com  
user@example.com  
user@example.com  
user@example.com  
user@example.com

Add Users

Cancel

A confirmation dialog displays the number of users who were added.

If the dialog lists any users who could not be added, capture this information so that you can resolve the

issue. In some cases you can re-add the user with a corrected email address.

## Result

Cloud Compliance starts scanning the files for the users you added, and the results are displayed in the Dashboard and in other locations.

### Removing OneDrive users from compliance scans

If users leave the company or if their email address changes, you can remove individual OneDrive users from having their files scanned at any time. Just click **Remove OneDrive User** from the Configuration page.

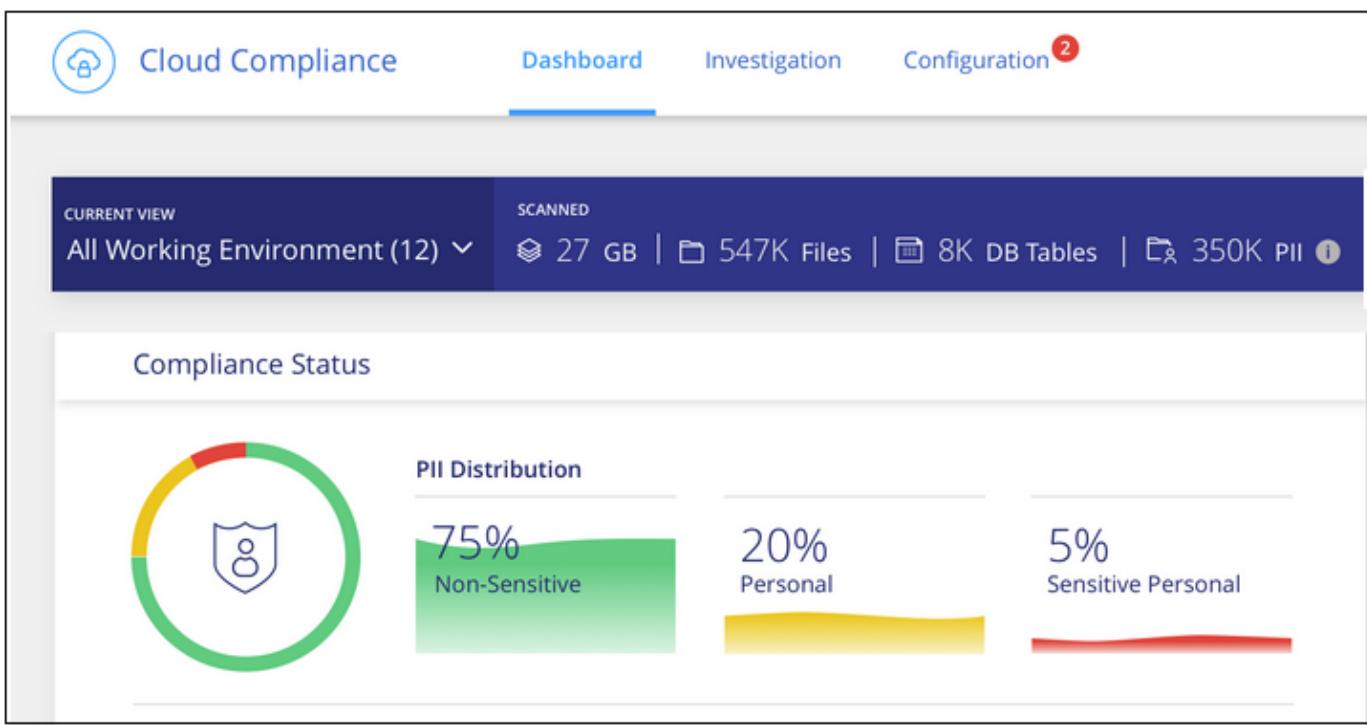
The screenshot shows a table titled 'Working Environment Name' Scan Configuration. At the top right is a blue button labeled '+ Add OneDrive users'. Below it, a message says '24 users are being scanned for compliance'. The table has three columns: 'Username', 'Status', and 'Required Action'. The first row shows 'user1@example.com' with a green status dot and the text 'Continuously Scanning'. To the right of this row is a green-bordered button with a red circle and a white minus sign, labeled 'Remove OneDrive User'.

Username	Status	Required Action
user1@example.com	Continuously Scanning	<span style="border: 2px solid green; padding: 2px;">✖ Remove OneDrive User</span>

## Viewing details about the private data stored in your organization

Gain control of your private data by viewing details about the personal data and sensitive personal data in your organization. You can also gain visibility by reviewing the categories and file types that Cloud Compliance found in your data.

By default, the Cloud Compliance dashboard displays compliance data for all working environments and databases.



If you want to see data for only some of the working environments, [select those working environments](#).

You can also filter the results from the Data Investigation page and download a report of the results as a CSV file. See [Filtering data in the Data Investigation page](#) for details.

## Personal data

Cloud Compliance automatically identifies specific words, strings, and patterns (Regex) inside the data. For example, Personal Identification Information (PII), credit card numbers, social security numbers, bank account numbers, and more. [See the full list](#).

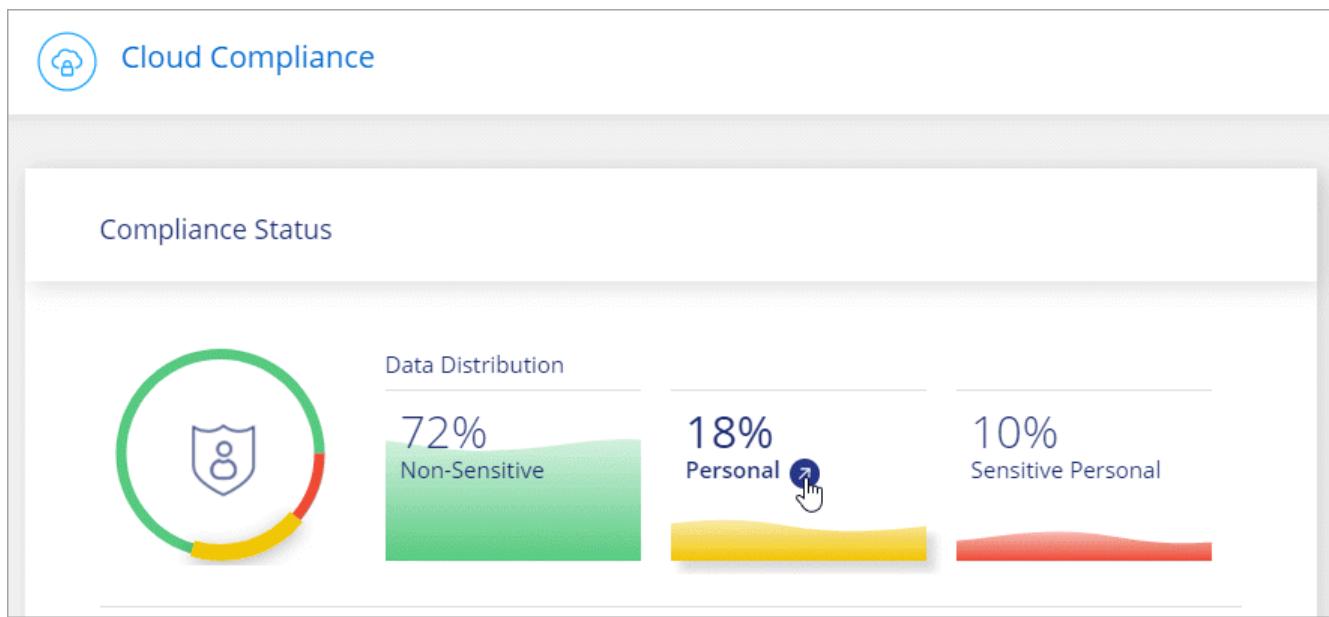
Additionally, if you have added a database server to be scanned, the *Data Fusion* feature allows you to scan your files to identify whether unique identifiers from your databases are found in those files or other databases. See [Adding personal data identifiers using Data Fusion](#) for details.

For some types of personal data, Cloud Compliance uses *proximity validation* to validate its findings. The validation occurs by looking for one or more predefined keywords in proximity to the personal data that was found. For example, Cloud Compliance identifies a U.S. social security number (SSN) as a SSN if it sees a proximity word next to it—for example, SSN or *social security*. [The table of personal data](#) shows when Cloud Compliance uses proximity validation.

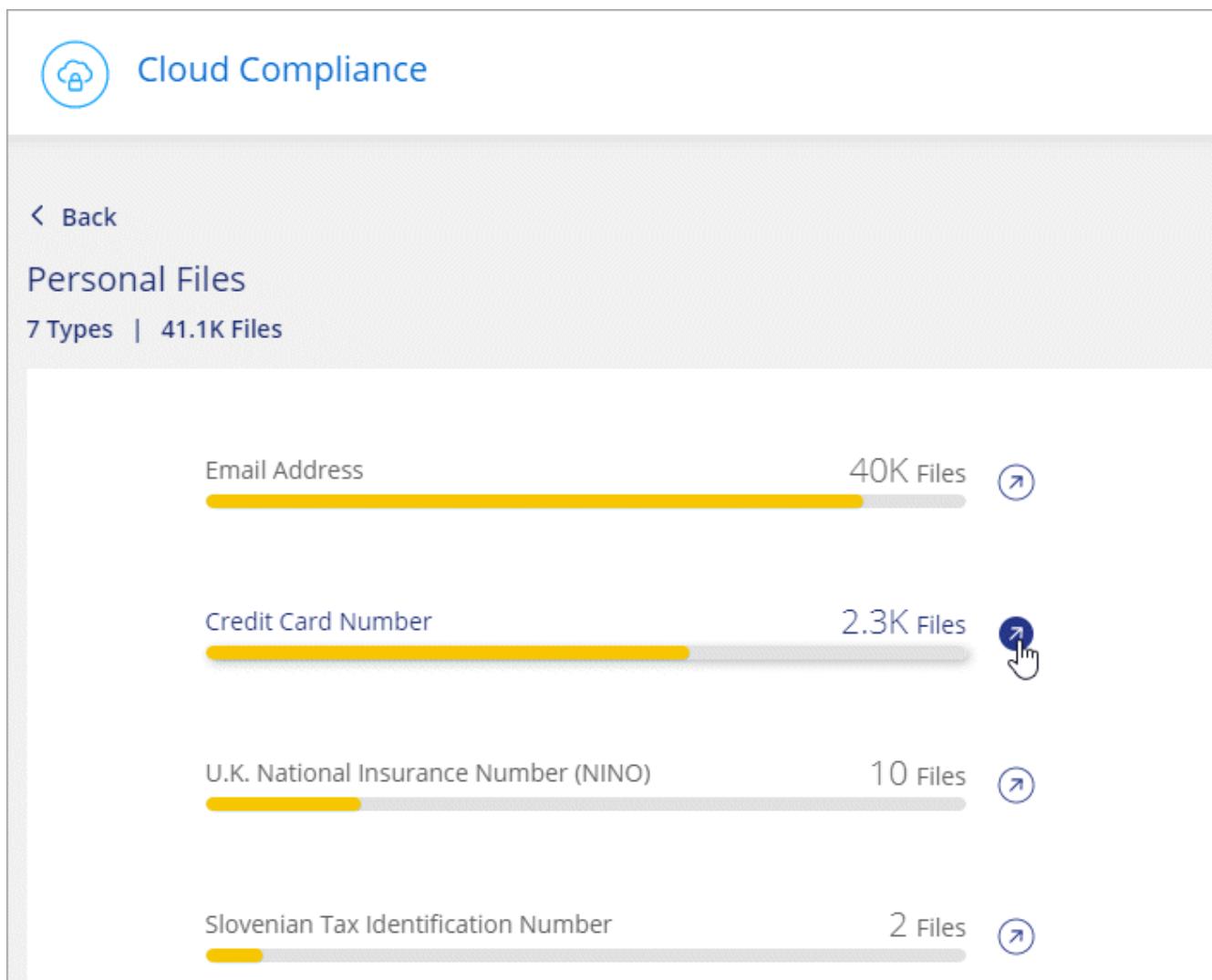
### Viewing files that contain personal data

#### Steps

1. At the top of Cloud Manager, click **Compliance** and click the **Dashboard** tab.
2. To investigate the details for all personal data, click the icon next to the personal data percentage.



3. To investigate the details for a specific type of personal data, click **View All** and then click the **Investigate Results** icon for a specific type of personal data.



4. Investigate the data by searching, sorting, expanding details for a specific file, clicking **Investigate Results** to see masked information, or by downloading the file list.

The screenshot shows a dashboard titled "Dashboard investigation for 'Credit Card Number'". It displays a table of file details for "customer-data.xls". The table includes columns for File Name, Personal, Sensitive Personal, Data Subjects, and File Type. The "Data Subjects" column shows a value of 63 with a tooltip labeled "Investigate Results". Other details shown include Working Environment (Amazon S3), Storage Repository (compliancedemofiles), File Path (/Patterns/NEW SSN), Category (Miscellaneous), File Size (142.35 KB), and Last Modified (2019-12-16 12:18).

## Sensitive personal data

Cloud Compliance automatically identifies special types of sensitive personal information, as defined by privacy regulations such as [articles 9 and 10 of the GDPR](#). For example, information regarding a person's health, ethnic origin, or sexual orientation. [See the full list](#).

Cloud Compliance uses artificial intelligence (AI), natural language processing (NLP), machine learning (ML), and cognitive computing (CC) to understand the meaning of the content that it scans in order to extract entities and categorize it accordingly.

For example, one sensitive GDPR data category is ethnic origin. Because of its NLP abilities, Cloud Compliance can distinguish the difference between a sentence that reads "George is Mexican" (indicating sensitive data as specified in article 9 of the GDPR), versus "George is eating Mexican food."

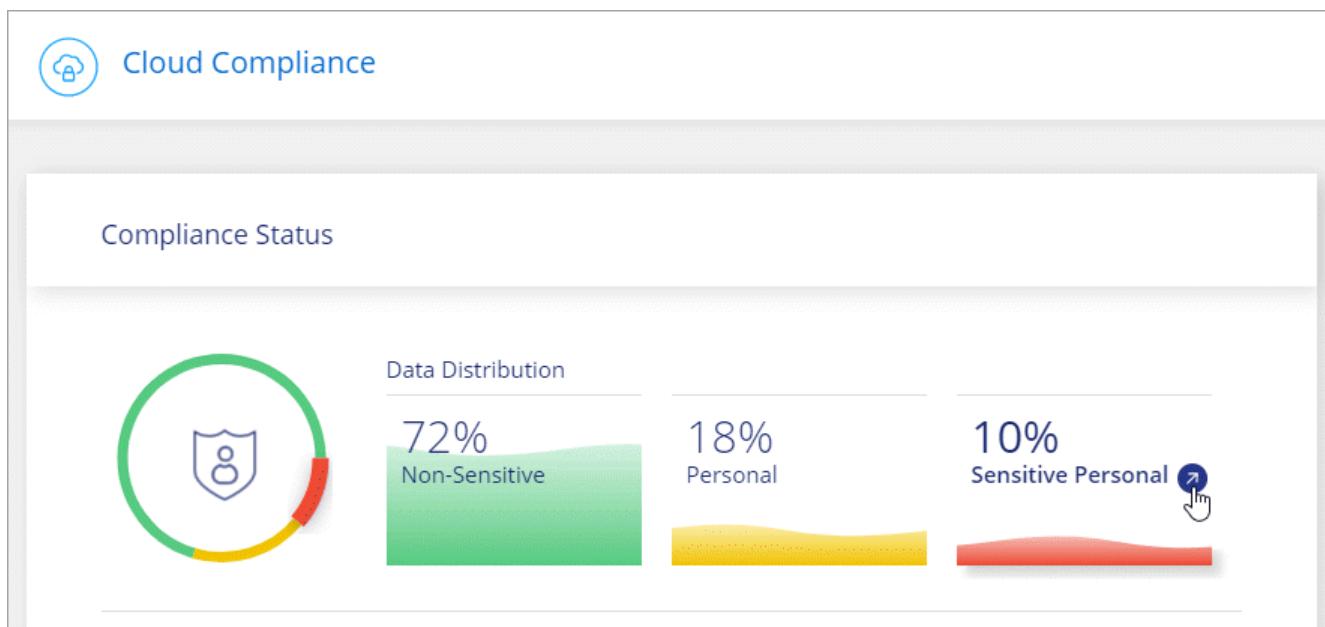


Only English is supported when scanning for sensitive personal data. Support for more languages will be added later.

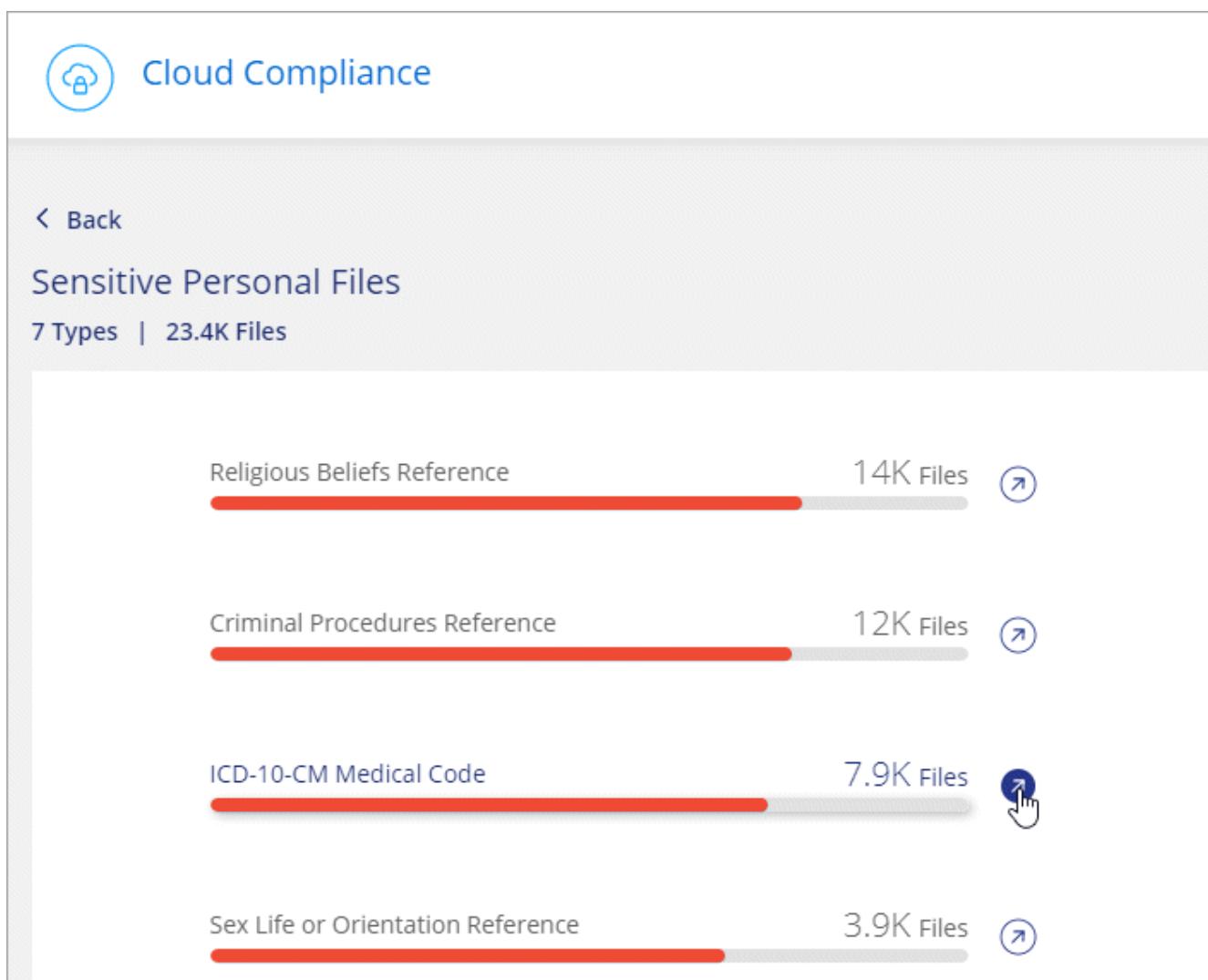
## Viewing files that contain sensitive personal data

### Steps

1. At the top of Cloud Manager, click **Compliance**.
2. To investigate the details for all sensitive personal data, click the icon next to the sensitive personal data percentage.



3. To investigate the details for a specific type of sensitive personal data, click **View All** and then click the **Investigate Results** icon for a specific type of sensitive personal data.



4. Investigate the data by searching, sorting, expanding details for a specific file, clicking **Investigate Results** to see masked information, or by downloading the file list.

## Categories

Cloud Compliance takes the data that it scanned and divides it into different types of categories. Categories are topics based on AI analysis of the content and metadata of each file. [See the list of categories](#).

Categories can help you understand what's happening with your data by showing you the types of information that you have. For example, a category like resumes or employee contracts can include sensitive data. When you investigate the results, you might find that employee contracts are stored in an insecure location. You can then correct that issue.



Only English is supported for categories. Support for more languages will be added later.

### Viewing files by categories

#### Steps

1. At the top of Cloud Manager, click **Compliance**.
2. Click the **Investigate Results** icon for one of the top 4 categories directly from the main screen, or click **View All** and then click the icon for any of the categories.

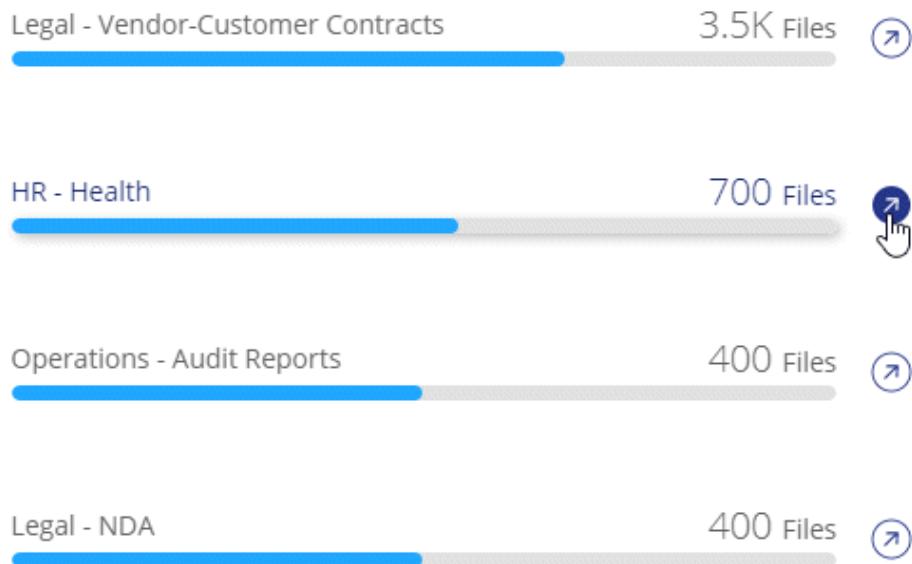


## Cloud Compliance

< Back

### Categories

27 Categories | 219.9K Files



3. Investigate the data by searching, sorting, expanding details for a specific file, clicking **Investigate Results** to see masked information, or by downloading the file list.

### File types

Cloud Compliance takes the data that it scanned and breaks it down by file type. Reviewing your file types can help you control your sensitive data because you might find that certain file types are not stored correctly. [See the list of file types.](#)

For example, you might be storing CAD files that include very sensitive information about your organization. If they are unsecured, you can take control of the sensitive data by restricting permissions or moving the files to another location.

### Viewing file types

#### Steps

1. At the top of Cloud Manager, click **Compliance**.
2. Click the **Investigate Results** icon for one of the top 4 file types directly from the main screen, or click **View All** and then click the icon for any of the file types.



## Cloud Compliance

< Back

### File Types

36 File Types | 219.9K Files

PDF

97K Files



DOCX

36K Files



XLS

1.7K Files



3. Investigate the data by searching, sorting, expanding details for a specific file, clicking **Investigate Results** to see masked information, or by downloading the file list.

### Viewing file metadata and permissions

In the Data Investigation results pane you can click for any single file to view the file metadata.

The screenshot shows a dashboard interface for managing files. At the top, there are two tabs: "Unstructured (32K Files)" and "Structured (323 DB Tables)". Below the tabs, a search bar and a download icon are visible. The main area has a header with columns: "File Name", "Personal", "Sensitive Personal", "Data Subjects", and "File Type". A file named "Expense Report EXP-TPO-10603888765435" is listed, categorized under "cvo", with counts of 6, 3, 16, and PDF type respectively. To the right of the file name, there are buttons for "View", "Edit", and "Delete". A detailed metadata panel for this file is expanded, showing the following information:

- Working Environment: WorkingEnvironment1
- Repository: Volume Name
- File Path: /Prod/labs-base/Expense Report EXP-TPO-1060388.pdf
- Category: Legal
- File Size: 22 MB
- Last Modified: 2019-08-06 07:51
- Open Permissions: NO OPEN PERMISSIONS
- File Owner: Assaf Vol

On the right side of the metadata panel, there are two buttons: "Assign a Label to this file" and "Delete this file". At the bottom right of the panel, there is a link "Give feedback on this result".

In addition to showing you the working environment and volume where the file resides, the metadata shows much more information, including the file permissions, file owner, and assigned AIP label (if you have [integrated AIP in Cloud Compliance](#)). This information is useful if you're planning to create highlights because you can see all the information that you can use to filter your data.

Note that not all information is available for all data sources - just what is appropriate for that data source. For example, permissions and AIP labels are not relevant for database files.

There are also two items in this metadata that allow you to make changes to files:

- If you have integrated AIP labels with Cloud Compliance, you can assign a label to this file, or change to a different label if one already exists. See [Assigning AIP labels manually](#) for details.
- You can delete the file. See [Deleting source files](#) for details.

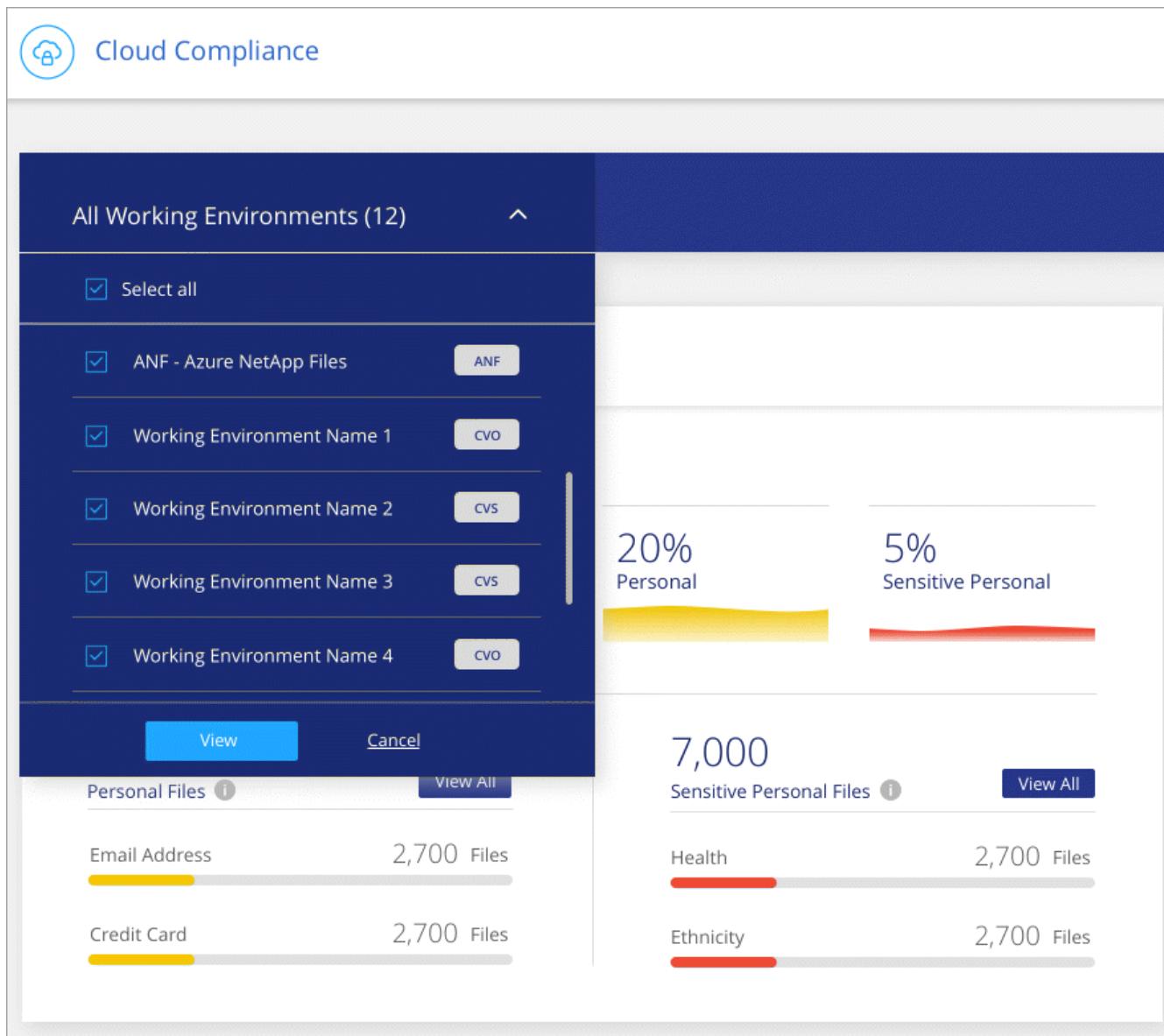
## Viewing Dashboard data for specific working environments

You can filter the contents of the Cloud Compliance dashboard to see compliance data for all working environments and databases, or for just specific working environments.

When you filter the dashboard, Cloud Compliance scopes the compliance data and reports to just those working environments that you selected.

### Steps

1. Click the filter drop-down, select the working environments that you'd like to view data for, and click **View**.



## Filtering data in the Data Investigation page

You can filter the contents of the investigation page to display only the results you want to see. If you want to save a CSV version of the content as a report after you have refined it, click the  button.

Data Investigation		Unstructured (32K Files)	Structured (323 DB Tables)			
FILTERS		File Name				
		Personal	Sensitive Personal	Data Subjects	File Type	
	> Expense Report EXP-TPO-10603888765435	cvo	6	3	16	PDF
	> Expense Report EXP-TPO-10603888765435	cvo	6	3	16	PDF
	> Expense Report EXP-TPO-10603888765435	cvo	6	3	16	PDF
	> Expense Report EXP-TPO-10603888765435	cvo	6	3	16	PDF
	> Expense Report EXP-TPO-10603888765435	cvo	6	3	16	PDF
	> Expense Report EXP-TPO-10603888765435	cvo	6	3	16	PDF
	> Expense Report EXP-TPO-10603888765435	cvo	6	3	16	PDF
	> Expense Report EXP-TPO-10603888765435	cvo	6	3	16	PDF

- The top-level tabs allow you to view data from files (unstructured data) or from databases (structured data).
- The controls at the top of each column allow you to sort the results in numerical or alphabetical order.
- The left-pane filters enable you to refine the results by working environment, storage repository, category, private data, file type, file size, last modified date, whether the S3 object's permissions are open to public access, etc...
- The *Highlights* filter at the top of the Filters pane lists the custom filters that provide commonly requested combinations of filters; like a saved database query or Favorites list. Go [here](#) to view the list of predefined highlights and to see how you can create your own custom highlights.

## What's included in each file list report (CSV file)

From each Investigation page you can click the button to download file lists (in CSV format) that include details about the identified files. If there are more than 10,000 results, only the top 10,000 appear in the list.

Each file list includes the following information:

- File name
- Location type
- Working environment
- Storage repository
- Protocol
- File path
- File type
- File size
- File owner
- Category
- Personal information
- Sensitive personal information
- Deletion detection date

A deletion detection date identifies the date that the file was deleted or moved. This enables you to identify when sensitive files have been moved. Deleted files aren't part of the file number count that appears in the dashboard or on the Investigation page. The files only appear in the CSV reports.

## Managing your private data

Cloud Compliance provides many ways for you to manage your private data. Some functionality just makes it easier to see the data that is most important to you, and other functionality allows you to make changes to the data.

- Using the "highlight" functionality you can create your own custom search queries so that you can easily see the results by clicking one button.
- You can send email alerts to Cloud Manager users when certain critical highlights return results.
- If you are subscribed to [Azure Information Protection \(AIP\)](#) to classify and protect your files, you can use Cloud Compliance to manage those AIP labels.
- You can delete files that seem insecure or too risky to leave in your storage system.

See below for more functionality that is provided with both the highlights and AIP features.

### Controlling your data using Highlights

Highlights are like a favorites list of custom filters that provide search results in the Investigation page for commonly requested compliance queries. Cloud Compliance provides a set of predefined Highlights based on common customer questions. You can also create custom Highlights that provide results for searches specific to your organization.

Highlights provide the following functionality:

- [Predefined highlights](#) from NetApp based on user requests
- Ability to create your own custom highlights
- Launch the Investigation page with the results from your highlights in one click
- Send email alerts to Cloud Manager users when certain critical highlights return results so you can get notifications to protect your data
- Assign AIP (Azure Information Protection) labels automatically to all files that match the criteria defined in a highlight

The **Highlights** tab in the Compliance Dashboard lists all the Highlights available on this instance of Cloud Compliance.

Cloud Compliance    Dashboard    Reports    Investigation    **Highlights**    Configuration (2)

### Highlights List

**GDPR - Old Sensitive Data**  
Predefined Highlight ⓘ

Email notifications: ON    **Edit**    ⋮

Data with European IDs for GDPR received from XDR database, sharing with Legal area in charged of Jon Doe. Also, this lines can take up to 2 lines, we need to limit character input so the description does not take more than 2 lines here in the component.

**HIPAA - Patients Personal Data**  
Last modified: 17-10-20

Email notifications: OFF    **Edit**    ⋮

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge.

In addition, Highlights appear in the list of Filters in the Investigation page.

### Viewing highlights results in the Investigation page

To display the results for a highlight in the Investigation page, click the ⋮ button for a specific highlight, and then select **Investigate Results**.

Cloud Compliance    Dashboard    Reports    Investigation    **Highlights**    Configuration (2)

### Highlights List

**GDPR - Old Sensitive Data**  
Last modified: 30-09-20

Email notifications: ON    **Edit**    ⋮

Data with European IDs for GDPR received from XDR database, sharing with Legal area in charged of Jon Doe. Also, this lines can take up to 2 lines, we need to limit character input so the description does not take more than 2 lines here in the component.

⋮    **Investigate Results**    Delete Highlight

### Creating custom highlights

You can create your own custom highlights that provide results for searches specific to your organization.

#### Steps

1. From the Data Investigation page, define your search by selecting all the filters you want to use. See [Filtering data in the Data Investigation page](#) for details.
2. Once you have all the filter characteristics just the way you want them, click **Save this search as a Highlight**.

**Data Investigation**

**FILTERS** Clear All

Search filters  X

Highlights +

Working Environment 4 +

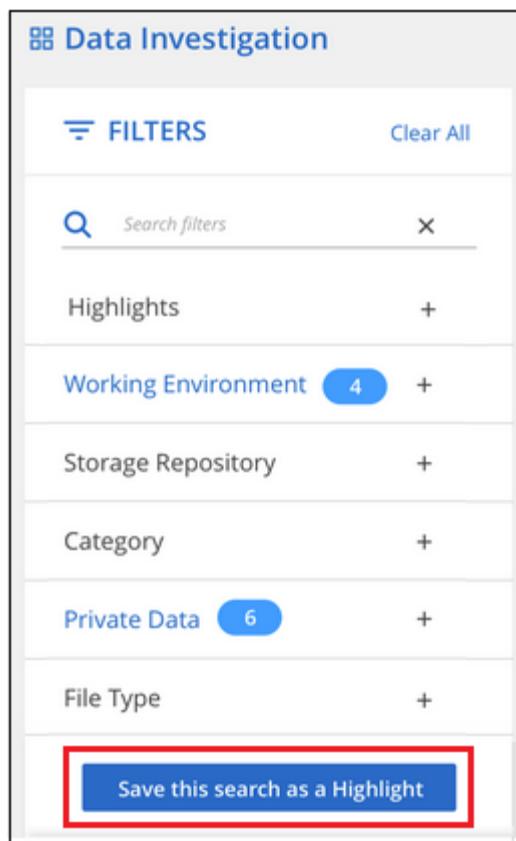
Storage Repository +

Category +

Private Data 6 +

File Type +

**Save this search as a Highlight**



3. Name the highlight and select other actions that can be performed by the highlight:
  - a. Enter a unique name and description.
  - b. Optionally, check the box if you want notification emails sent to Cloud Manager users, and choose the interval at which the email is sent.
  - c. Optionally, check the box to automatically assign AIP labels to files that match the highlight parameters, and select the label. (Learn more about [AIP labels](#).)
  - d. Click **Create Highlight**.

**Create Highlight**

Saving this filtered view will create a new Highlight, you can view/edit it in the "Highlights" tab

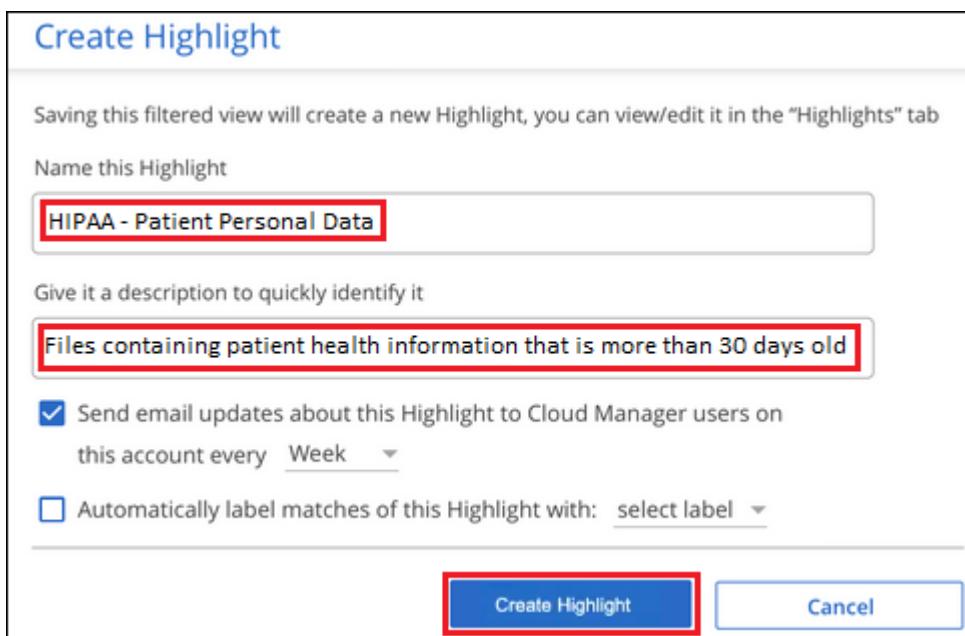
Name this Highlight

Give it a description to quickly identify it

Send email updates about this Highlight to Cloud Manager users on this account every Week ▾

Automatically label matches of this Highlight with: select label ▾

**Create Highlight** **Cancel**



## Result

The new highlight appears in the Highlights tab.

## Editing highlights

You can modify certain parts of a highlight depending on the type of highlight:

- Custom highlights - You can modify the *Name*, the *Description*, whether email notifications are sent, and whether AIP labels are added.
- Predefined highlights - You can modify only whether email notifications are sent and whether AIP labels are added.



If you need to change the filter parameters for a custom highlight, you'll need to create a new highlight with the parameters you want, and then delete the old highlight.

To modify a highlight, click the **Edit** button, enter your changes on the *Edit Highlight* page, and click **Save Highlight**.

## Deleting highlights

You can delete any custom highlight that you created if you no longer need it. You can't delete any of the predefined highlights.

To delete a highlight, click the button for a specific highlight, click **Delete Highlight**, and then click **Delete Highlight** again in the confirmation dialog.

## Categorizing your data using AIP labels

You can manage AIP labels in the files that Cloud Compliance is scanning if you have subscribed to [Azure Information Protection \(AIP\)](#). AIP enables you to classify and protect documents and files by applying labels to content. Cloud Compliance enables you to view the labels that are already assigned to files, add labels to files, and change labels when a label already exists.

Cloud Compliance support AIP labels within the following file types: .PDF, .DOCX, .DOC, .PPTX, .XLS, .XLSX.

Note that you can't currently change labels in files larger than 30 MB. For OneDrive accounts the maximum file size is 4 MB.



If a file has a label which doesn't exist anymore in AIP, Cloud Compliance considers it as a file without a label.

## Integrating AIP labels in your workspace

Before you can manage AIP labels, you need to integrate the AIP label functionality into Cloud Compliance by signing into your existing Azure account. Once enabled, you can manage AIP labels within files for all [working environments and data sources](#) in your current Cloud Manager workspace.

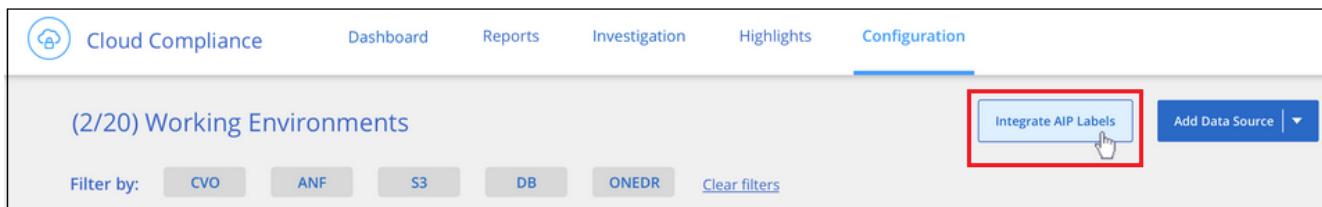
## Requirements

- You must have an account and an Azure Information Protection license.
- You must have the login credentials for the Azure account.
- If you plan to change labels in files that reside in Amazon S3 buckets, ensure that the permission

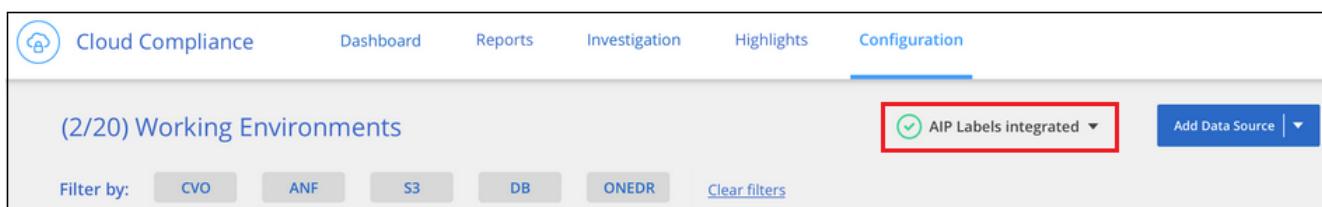
`s3:PutObject` is included in the IAM role. See [setting up the IAM role](#).

## Steps

1. From the Cloud Compliance Configuration page, click **Integrate AIP Labels**.



2. In the Integrate AIP Labels dialog, click **Sign in to Azure**.
3. In the Microsoft page that appears, select the account and enter the required credentials.
4. Return to the Cloud Compliance tab and you'll see the message "*AIP Labels were integrated successfully with the account <account\_name>*".
5. Click **Close** and you'll see the text *AIP Labels integrated* at the top of the page.



## Result

You can view and assign AIP labels from the results pane of the Investigation page. You can also assign AIP labels to files using highlights.

## Assigning AIP labels manually

You can add, change, and remove AIP labels from your files using Cloud Compliance.

Follow these steps to assign an AIP label to a single file.

## Steps

1. In the Data Investigation results pane, click **>** for the file to expand the file metadata details.

The screenshot shows a file management interface with two tabs at the top: "Unstructured (32K Files)" and "Structured (323 DB Tables)". Below the tabs is a header row with columns for "File Name", "Personal", "Sensitive Personal", "Data Subjects", and "File Type". A search bar and download icon are in the top right.

A specific file, "Expense Report EXP-TPO-10603888765435", is selected. Its details are shown in the main area:

- File Name:** Expense Report EXP-TPO-10603888765435
- Personal:** 6
- Sensitive Personal:** 3
- Data Subjects:** 16
- File Type:** PDF

Below these details, a "Working Environment" section lists various file properties:

- Working Environment: WorkingEnvironment1
- Repository: Volume Name
- File Path: /Prod/labs-base/Expense Report EXP-TPO-1060388.pdf
- Category: Legal
- File Size: 22 MB
- Last Modified: 2019-08-06 07:51
- Open Permissions: NO OPEN PERMISSIONS | View all Permissions
- File Owner: Assaf Vol

To the right, a modal window titled "Assign a Label to this file" is open, showing three categories: General, Finance (selected and highlighted with a red border), and Confidential.

- Click **Assign a Label to this file** and then select the label.

The label appears in the file metadata.

### Assigning AIP labels automatically with highlights

You can assign an AIP label to all the files that meet the criteria of the highlight. You can specify the AIP label when creating the highlight, or you can add the label when editing any highlight.

Labels are added or updated in files continuously as Cloud Compliance scans your files.

Depending on whether a label is already applied to a file, and the classification level of the label, the following actions are taken when changing a label:

If the file...	Then...
Has no label	The label is added
Has an existing label of a lower level of classification	The higher level label is added
Has an existing label of a higher level of classification	The higher level label is retained
Is assigned a label both manually and by a highlight	The higher level label is added
Is assigned two different labels by two highlights	The higher level label is added

Follow these steps to add an AIP label to an existing highlight.

#### Steps

- From the Highlights List page, click **Edit** for the highlight where you want to add (or change) the AIP label.

Cloud Compliance      Dashboard      Reports      Investigation      **Highlights**      Configuration <sup>2</sup>

### Highlights List

<b>GDPR - Old Sensitive Data</b> Predefined Highlight	Label: <b>General</b>	E-mail notifications: <b>Monthly</b>	<b>Edit</b>	⋮
Data with European IDs for GDPR received from XDR database, sharing with Legal area in charge of Jon Doe. Also, this lines can take up to 2 lines, we need to limit character input so the description does not take more than 2 lines here in the component.				
<b>HIPAA - Patients Personal Data</b> Last modified: 17-10-20	Label: <b>OFF</b>	E-mail notifications: <b>OFF</b>		
The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge.				

2. In the Edit Highlight page, check the box to enable automatic labels for files that match the highlight parameters, and select the label (for example, **General**).

### Edit Highlight

Saving this filtered view will create a new Highlight, you can view/edit it in the "Highlights" tab

Name this Highlight

Give it a description to quickly identify it

Send email updates about this Highlight to Cloud Manager users on this account every **Week** ▾

Automatically label matches of this Highlight with: **select label**

General

Finance

Confidential

3. Click **Save Highlight** and the label appears in the highlight description.



If a highlight was configured with a label, but the label has since been removed from AIP, the label name is turned to OFF and the label is not assigned anymore.

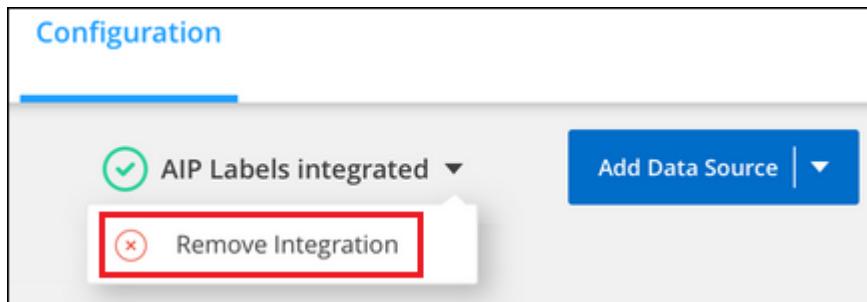
## Removing the AIP integration

If you no longer want the ability to manage AIP labels in files, you can remove the AIP account from the Cloud Compliance interface.

Note that no changes are made to the labels you have added using Cloud Compliance. The labels that exist in files will stay as they currently exist.

## Steps

1. From the Scan Configuration page, click **AIP Labels integrated > Remove Integration**.



2. Click **Remove Integration** from the confirmation dialog.

## Sending email alerts when non-compliant data is found

Cloud Compliance can send email alerts to Cloud Manager users when certain critical highlights return results so you can get notifications to protect your data. You can choose to send the email notifications on a daily, weekly, or monthly basis.

You can configure this setting when creating the highlight or when editing any highlight.

Follow these steps to add email updates to an existing highlight.

## Steps

1. From the Highlights List page, click **Edit** for the highlight where you want to add (or change) the email setting.

A screenshot of the Cloud Compliance Highlights List page. The top navigation bar includes 'Cloud Compliance', 'Dashboard', 'Reports', 'Investigation', 'Highlights' (which is underlined), and 'Configuration'. Below the navigation is a section titled 'Highlights List' containing two items:

- GDPR - Old Sensitive Data**: Predefined Highlight. It shows 'Label: General' and 'E-mail notifications: Monthly'. There is a blue 'Edit' button and a blue 'More options' button.
- HIPAA - Patients Personal Data**: Last modified: 17-10-20. It shows 'Label: OFF' and 'E-mail notifications: OFF'. The 'OFF' label is circled in green. There is a red 'Edit' button and a blue 'More options' button.

2. In the Edit Highlight page, check the box if you want notification emails sent to Cloud Manager users, and choose the interval at which the email is sent (for example, **Week**).

## Edit Highlight

Saving this filtered view will create a new Highlight, you can view/edit it in the "Highlights" tab

Name this Highlight

HIPAA - Patient Personal Data

Give it a description to quickly identify it

Files containing patient health information that is more than 30 days old

Send email updates about this Highlight to Cloud Manager users on this account every Week



Save Highlight

Cancel

- Click **Save Highlight** and the interval at which the email is sent appears in the highlight description.

### Result

The first email is sent now if there are any results from the highlight - but only if any files meet the highlight criteria. No personal information is sent in the notification emails. The email indicates that there are files that match the highlight criteria, and it provides a link to the highlight results.

## Deleting source files

You can permanently remove source files that seem insecure or too risky to leave in your storage system. This action is permanent and there is no undo.



You can't delete files that reside in databases or files that reside in volume backup files.

### Steps

- In the Data Investigation results pane, click  for the file to expand the file metadata details.

File Name	Personal	Sensitive Personal	Data Subjects	File Type
Expense Report EXP-TPO-10603888765435	cvo	6	3	16 PDF
Expense Report EXP-TPO-10603888765435	cvo	6 	3 	16  PDF 

 Working Environment: WorkingEnvironment1

 Repository: Volume Name

 File Path: /Prod/labs-base/Expense Report EXP-TPO-1060388.pdf

 Delete this file

- Click **Delete this file**.

3. Because the delete operation is permanent, you must type "**permanently delete**" in the subsequent *Delete File* dialog and click **Delete File**.

## List of predefined highlights

Cloud Compliance provides the following system-defined highlights:

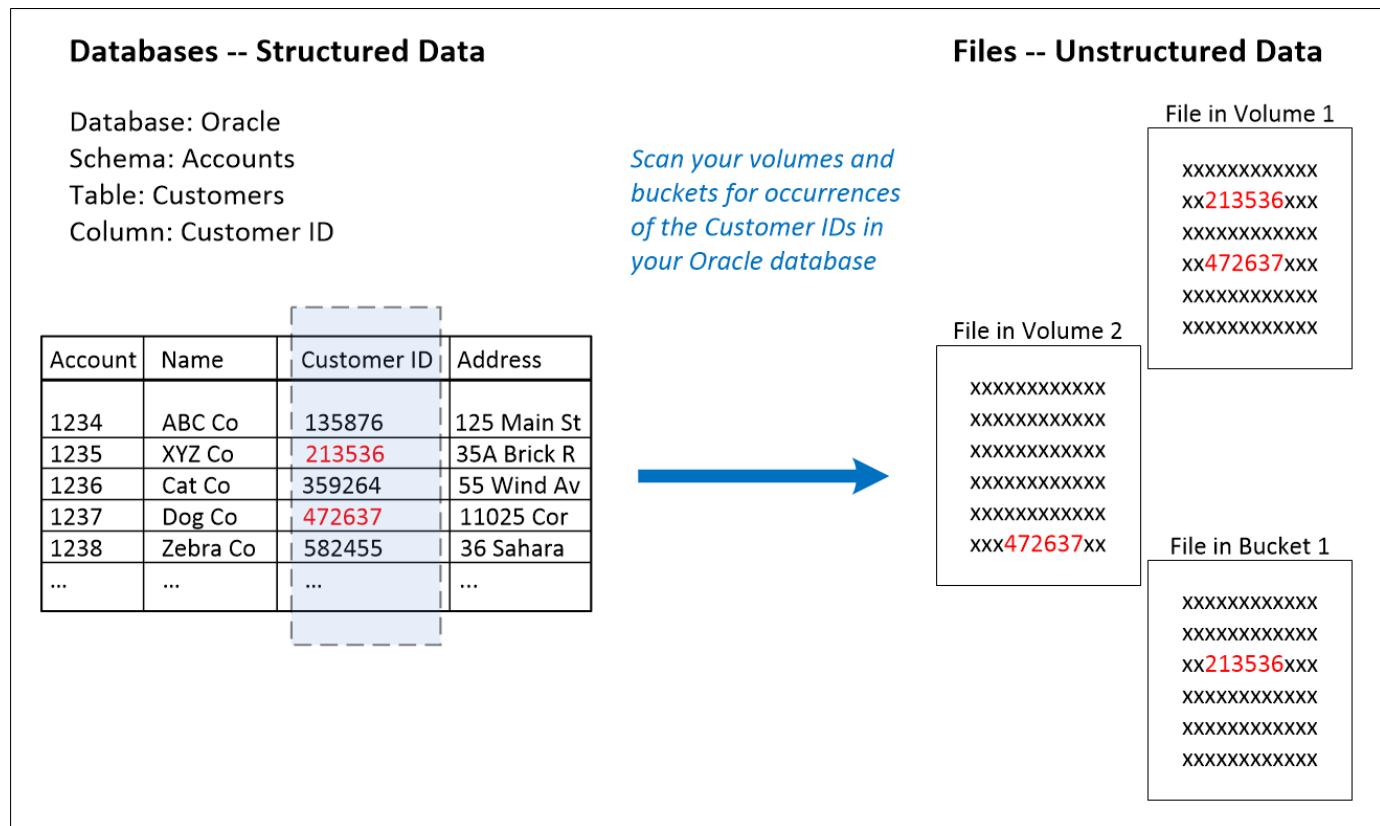
Name	Description	Logic
S3 publicly-exposed private data	S3 Objects containing personal or sensitive personal information, with open Public read access.	(S3 Public) AND contains personal OR sensitive personal info)
PCI DSS – Stale data over 30 days	Files containing Credit Card information, last modified over 30 days ago.	Contains credit card AND last modified over 30 days
HIPAA – Stale data over 30 days	Files containing Health information, last modified over 30 days ago.	Contains health data (defined same way as in HIPAA report) AND last modified over 30 days
Private data – Stale over 7 years	Files containing personal or sensitive personal information, last modified over 7 years ago.	Files containing personal or sensitive personal information, last modified over 7 years ago
GDPR – European citizens	Files containing more than 5 identifiers of an EU country's citizens or DB Tables containing identifiers of an EU country's citizens.	Files containing over 5 identifiers of an (one) EU citizens or DB Tables containing rows with over 15% of columns with one country's EU identifiers. (any one of the national identifiers of the European countries. Does not include Brazil, California, USA SSN, Israel, South Africa)
CCPA – California residents	Files containing over 10 California Driver's License identifiers or DB Tables with this identifier.	Files containing over 10 California Driver's License identifiers OR DB Tables containing California Driver's license
Data Subject names – High risk	Files with over 50 Data Subject names.	Files with over 50 Data Subject names
Email Addresses – High risk	Files with over 50 Email Addresses, or DB Columns with over 50% of their rows containing Email Addresses	Files with over 50 Email Addresses, or DB Columns with over 50% of their rows containing Email Addresses
Personal data – High risk	Files with over 20 Personal data identifiers, or DB Columns with over 50% of their rows containing Personal data identifiers.	Files with over 20 personal, or DB Columns with over 50% of their rows containing personal
Sensitive Personal data – High risk	Files with over 20 Sensitive Personal data identifiers, or DB Columns with over 50% of their rows containing Sensitive Personal data.	Files with over 20 sensitive personal, or DB Columns with over 50% of their rows containing sensitive personal

# Adding personal data identifiers using Data Fusion

A feature we call *Data Fusion* allows you to scan your organizations' data to identify whether unique identifiers from your databases are found in files or other databases - basically making your own list of "personal data" that is identified in Cloud Compliance scans. This gives you the full picture about where potentially sensitive data resides in *all* your files.

## Creating custom personal data identifiers from your databases

You can choose the additional identifiers that Cloud Compliance will look for in its' scans by selecting a specific column, or columns, in a database table. For example, the diagram below shows how data fusion is used to scan your volumes, buckets, and databases for occurrences of all your Customer IDs from your Oracle database.

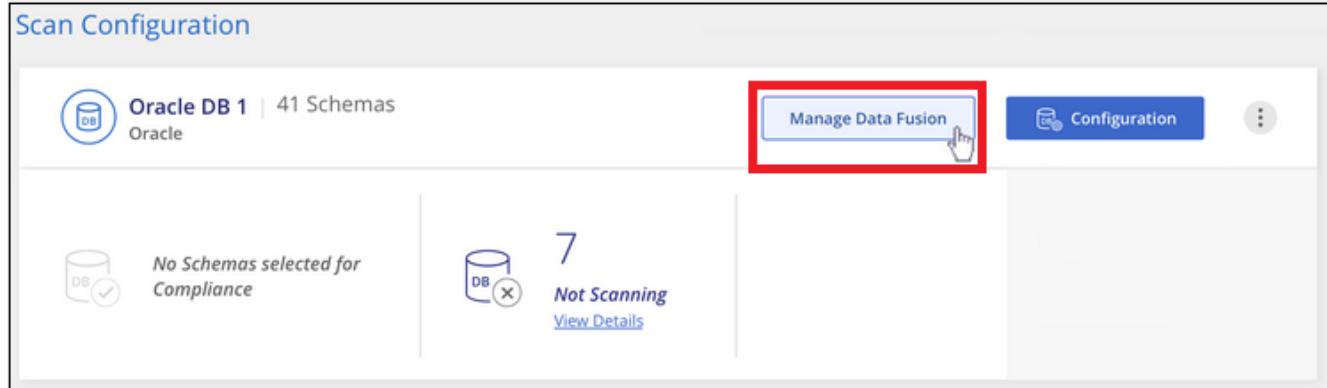


As you can see, two unique Customer IDs have been found in two volumes and in one S3 bucket. Any matches in database tables will also be identified.

## Steps

You must have [added at least one database server](#) to Cloud Compliance before you can add data fusion sources.

1. In the Scan Configuration page, click **Manage Data Fusion** in the database where the source data resides.



2. Click **Add Data Fusion source** on the next page.
3. In the *Add Data Fusion Source* page:
  - a. Select the Database Schema from the drop-down menu.
  - b. Enter the Table name in that schema.
  - c. Enter the Column, or Columns, that contain the unique identifiers you want to use.

When adding multiple columns, enter each column name, or table view name, on a separate line.

4. Click **Add Data Fusion Source**.

The Data Fusion inventory page displays the database source columns that you have configured for Cloud Compliance to scan.

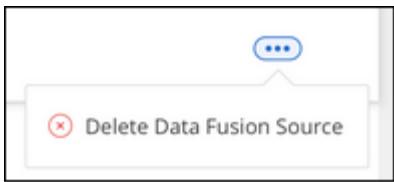
'DB Name 1' Data Fusion			+ Add Data Fusion source
With Data Fusion, Cloud Compliance can identify occurrences of your organization's unique identifiers found in your unstructured data stores, using structured data indexes containing those unique identifiers as a source reference. <a href="#">Learn More</a>			
Database Schema	Table	Data Fusion Source Columns	...
SchemaName1	Table 1	Column 12, Column 14, Column 18	...
SchemaName2	Table 2	Column 12, Column 14, Column 18	...

## Results

After the next scan, the results will include this new information in the Dashboard under the "Personal" results section, and in the Investigation page in the "Personal Data" filter. Each source column you added appears in the filter list as "Table.Column", for example `Customers.Customer ID`.

## Deleting a Data Fusion source

If at some point you decide not to scan your files using a certain Data Fusion source, you can select the source row from the Data Fusion inventory page and click **Delete Data Fusion Source**.



## Viewing compliance reports

Cloud Compliance provides reports that you can use to better understand the status of your organization's data privacy program.

By default, the Cloud Compliance dashboard displays compliance data for all working environments and databases. If you want to view reports that contain data for only some of the working environments, [select those working environments](#).



NetApp can't guarantee 100% accuracy of the personal data and sensitive personal data that Cloud Compliance identifies. You should always validate the information by reviewing the data.

### Privacy Risk Assessment Report

The Privacy Risk Assessment Report provides an overview of your organization's privacy risk status, as required by privacy regulations such as GDPR and CCPA. The report includes the following information:

#### Compliance status

A [severity score](#) and the distribution of data, whether it's non-sensitive, personal, or sensitive personal.

#### Assessment overview

A breakdown of the types of personal data found, as well as the categories of data.

#### Data subjects in this assessment

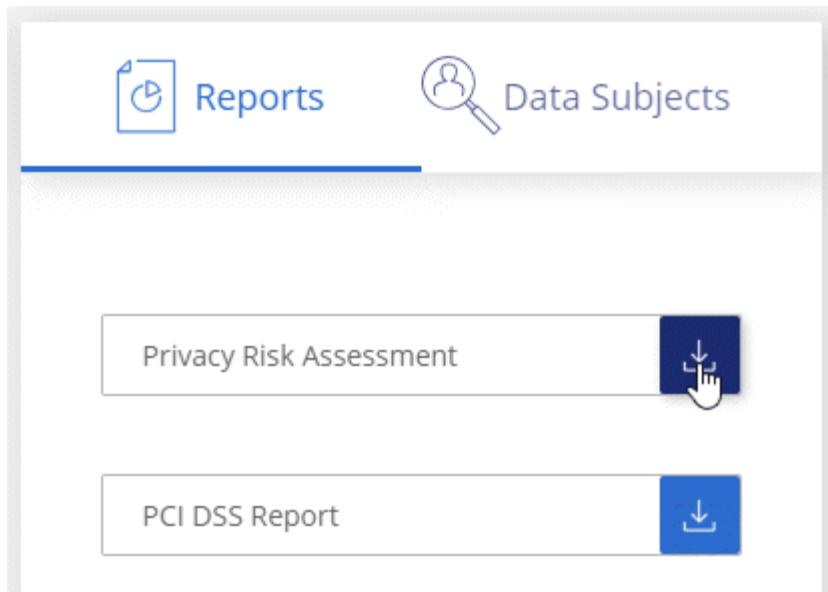
The number of people, by location, for which national identifiers were found.

### Generating the Privacy Risk Assessment Report

Go to the Compliance tab to generate the report.

#### Steps

1. At the top of Cloud Manager, click **Compliance**.
2. Under **Reports**, click the download icon next to **Privacy Risk Assessment**.



## Result

Cloud Compliance generates a PDF report that you can review and send to other groups as needed.

## Severity score

Cloud Compliance calculates the severity score for the Privacy Risk Assessment Report on the basis of three variables:

- The percentage of personal data out of all data.
- The percentage of sensitive personal data out of all data.
- The percentage of files that include data subjects, determined by national identifiers such as national IDs, Social Security numbers, and tax ID numbers.

The logic used to determine the score is as follows:

Severity score	Logic
0	All three variables are exactly 0%
1	One of the variables are larger than 0%
2	One of the variables are larger than 3%
3	Two of the variables are larger than 3%
4	Three of the variables are larger than 3%
5	One of the variables are larger than 6%
6	Two of the variables are larger than 6%
7	Three of the variables are larger than 6%
8	One of the variables are larger than 15%
9	Two of the variables are larger than 15%
10	Three of the variables are larger than 15%

## PCI DSS Report

The Payment Card Industry Data Security Standard (PCI DSS) Report can help you identify the distribution of credit card information across your files. The report includes the following information:

### Overview

How many files contain credit card information and in which working environments.

### Encryption

The percentage of files containing credit card information that are on encrypted or unencrypted working environments. This information is specific to Cloud Volumes ONTAP.

### Ransomware Protection

The percentage of files containing credit card information that are on working environments that do or don't have ransomware protection enabled. This information is specific to Cloud Volumes ONTAP.

### Retention

The timeframe in which the files were last modified. This is helpful because you shouldn't keep credit card information for longer than you need to process it.

### Distribution of Credit Card Information

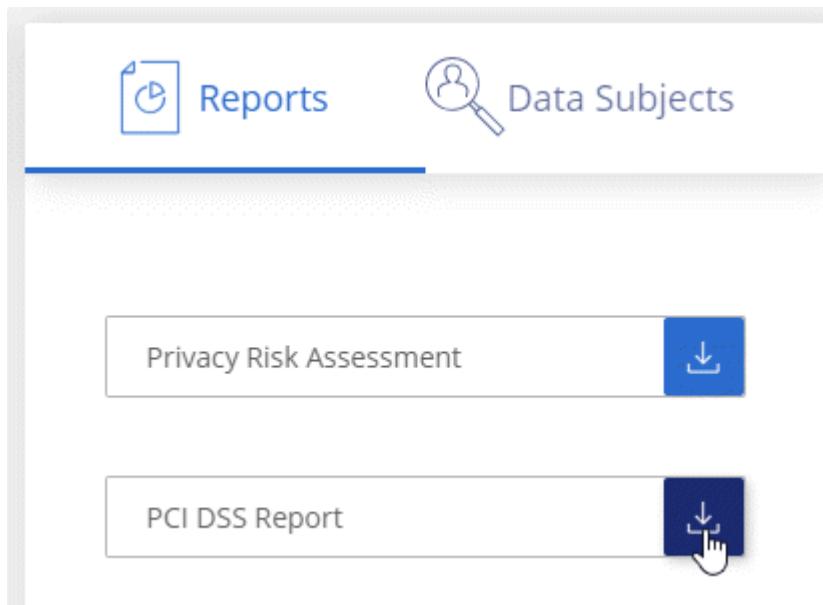
The working environments where the credit card information was found and whether encryption and ransomware protection are enabled.

### Generating the PCI DSS Report

Go to the Compliance tab to generate the report.

### Steps

1. At the top of Cloud Manager, click **Compliance**.
2. Under **Reports**, click the download icon next to **PCI DSS Report**.



### Result

Cloud Compliance generates a PDF report that you can review and send to other groups as needed.

## HIPAA Report

The Health Insurance Portability and Accountability Act (HIPAA) Report can help you identify files containing health information. It is designed to aid in your organization's requirement to comply with HIPAA data privacy laws. The information Cloud Compliance looks for includes:

- Health reference pattern
- ICD-10-CM Medical code
- ICD-9-CM Medical code
- HR – Health category
- Health Application Data category

The report includes the following information:

### Overview

How many files contain health information and in which working environments.

### Encryption

The percentage of files containing health information that are on encrypted or unencrypted working environments. This information is specific to Cloud Volumes ONTAP.

### Ransomware Protection

The percentage of files containing health information that are on working environments that do or don't have ransomware protection enabled. This information is specific to Cloud Volumes ONTAP.

### Retention

The timeframe in which the files were last modified. This is helpful because you shouldn't keep health information for longer than you need to process it.

### Distribution of Health Information

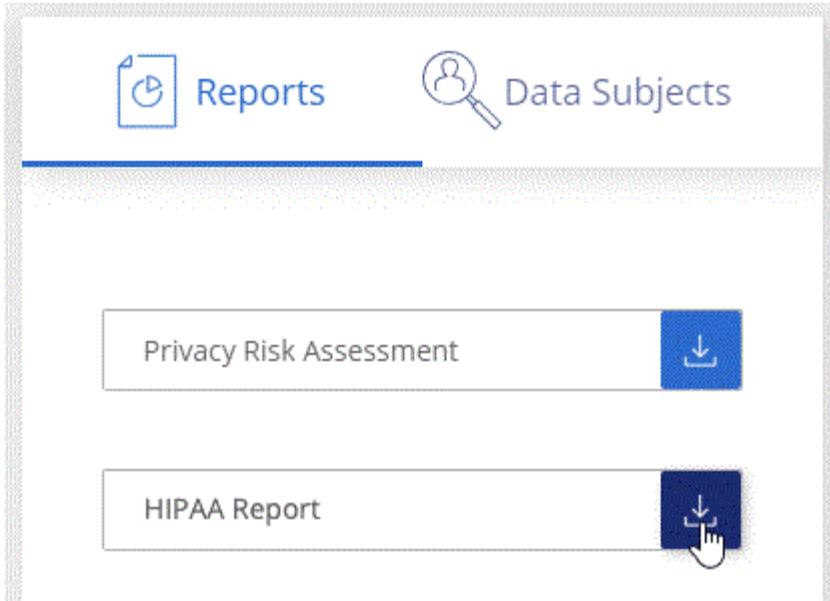
The working environments where the health information was found and whether encryption and ransomware protection are enabled.

### Generating the HIPAA Report

Go to the Compliance tab to generate the report.

### Steps

1. At the top of Cloud Manager, click **Compliance**.
2. Under **Reports**, click the download icon next to **HIPAA Report**.



## Result

Cloud Compliance generates a PDF report that you can review and send to other groups as needed.

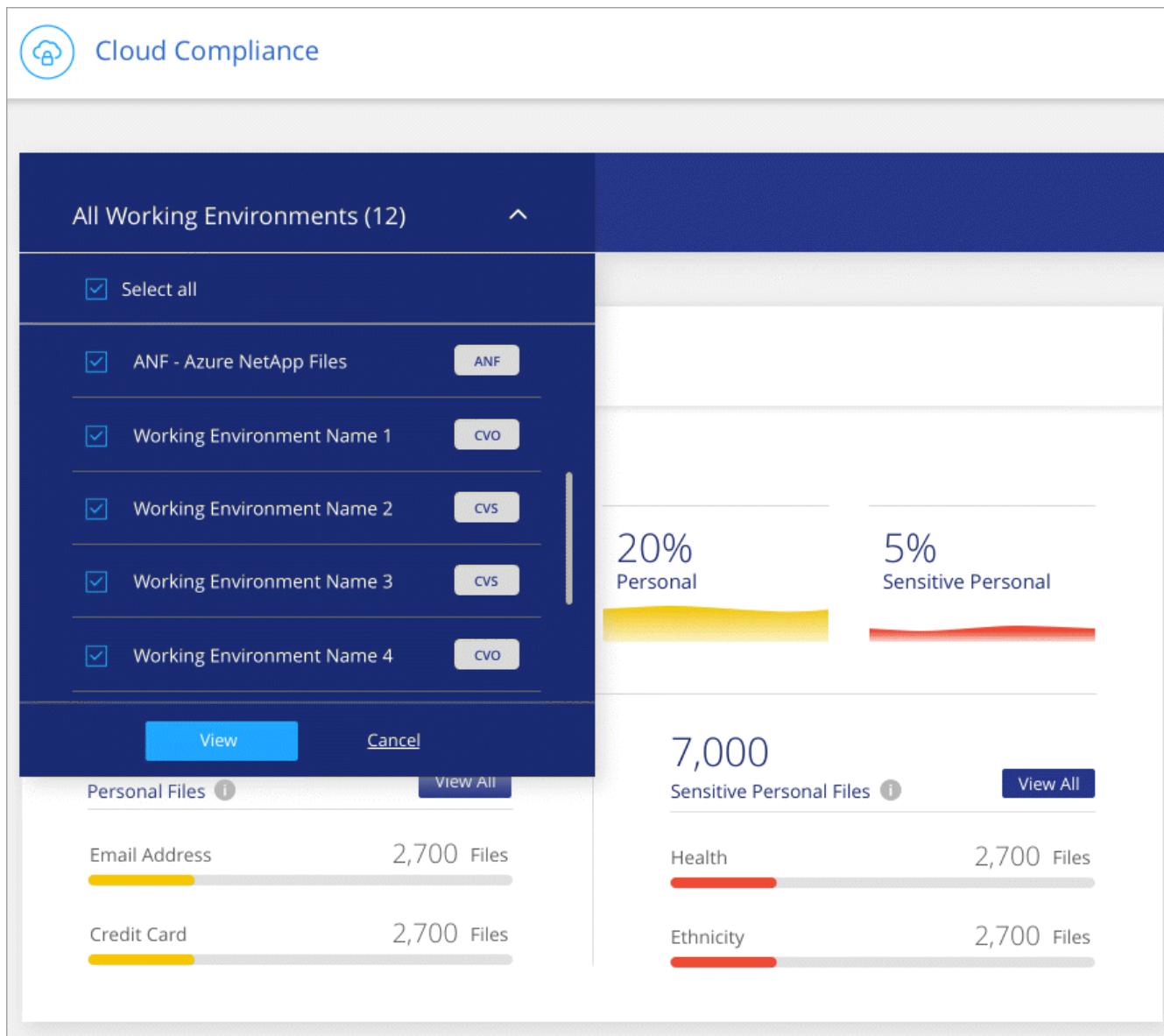
## Selecting the working environments for reports

You can filter the contents of the Cloud Compliance dashboard to see compliance data for all working environments and databases, or for just specific working environments.

When you filter the dashboard, Cloud Compliance scopes the compliance data and reports to just those working environments that you selected.

## Steps

1. Click the filter drop-down, select the working environments that you'd like to view data for, and click **View**.



## Responding to a Data Subject Access Request

Respond to a Data Subject Access Request (DSAR) by searching for a subject's full name or known identifier (such as an email address) and then downloading a report. The report is designed to aid in your organization's requirement to comply with GDPR or similar data privacy laws.



NetApp can't guarantee 100% accuracy of the personal data and sensitive personal data that Cloud Compliance identifies. You should always validate the information by reviewing the data.

### What is a Data Subject Access Request?

Privacy regulations such as the European GDPR grant data subjects (such as customers or employees) the right to access their personal data. When a data subject requests this information, this is known as a DSAR (data subject access request). Organizations are required to respond to these requests "without undue delay,"

and at the latest within one month of receipt.

## How can Cloud Compliance help you respond to a DSAR?

When you perform a data subject search, Cloud Compliance finds all of the files, buckets, and databases that have that person's name or identifier in it. Cloud Compliance checks the latest pre-indexed data for the name or identifier. It doesn't initiate a new scan.

After the search is complete, you can then download the list of files for a Data Subject Access Request report. The report aggregates insights from the data and puts it into legal terms that you can send back to the person.

### Searching for data subjects and downloading reports

Search for the data subject's full name or known identifier and then download a file list report or DSAR report. You can search by [any personal information type](#).

Only English is supported when searching for the names of data subjects. Support for more languages will be added later.



Data subject search is not supported within databases at this time.

#### Steps

1. At the top of Cloud Manager, click **Compliance**.
2. Click **Data Subjects**.
3. Search for the data subject's full name or known identifier.

Here's an example that shows a search for the name *john doe*:

The screenshot shows the 'Data Subjects' section of the Cloud Compliance interface. At the top, there are two navigation items: 'Reports' with a pie chart icon and 'Data Subjects' with a magnifying glass over a person icon. Below this is a back button labeled '< Back'. A search bar contains the text 'john doe Results' with a clear 'X' button. Underneath, a blue box displays '203 Files Found' next to a person icon. Two main buttons are visible: 'Download DSAR Report' with a download icon and 'Investigate Results' with a circular arrow icon.

4. Choose one of the available options:

- **Download DSAR Report:** A formal response to the access request that you can send to the data subject. This report contains automatically-generated information based on data that Cloud Compliance found on the data subject and is designed to be used as a template. You should complete the form and review it internally before sending it to the data subject.
- **Investigate Results:** A page that enables you to investigate the data by searching, sorting, expanding details for a specific file, and by downloading the file list.



If there are more than 10,000 results, only the top 10,000 appear in the file list.

## Categories of private data

There are many types of private data that Cloud Compliance can identify in your volumes, Amazon S3 buckets, databases, and OneDrive folders. See the categories below.



If you need Cloud Compliance to identify other private data types, such as additional national ID numbers or healthcare identifiers, email [ng-contact-cloud-compliance@netapp.com](mailto:ng-contact-cloud-compliance@netapp.com) with your request.

### Types of personal data

The personal data found in files can be general personal data or national identifiers. The third column identifies whether Cloud Compliance uses **proximity validation** to validate its findings for the identifier.

Note that you can add to the list of personal data that is found in your files if you are scanning a database server. The *Data Fusion* feature allows you to choose the additional identifiers that Cloud Compliance will look for in its' scans by selecting columns in a database table. See [Adding personal data identifiers using Data Fusion](#) for details.

Type	Identifier	Proximity validation?
General	Email address	No
	Credit card number	No
	IBAN number (International Bank Account Number)	No
	IP address	No

Type	Identifier	Proximity validation?
National Identifiers	Belgian ID (Numero National)	Yes
	Brazilian ID (CPF)	Yes
	Bulgarian ID (UCN)	Yes
	California Driver's License	Yes
	Croatian ID (OIB)	Yes
	Cyprus Tax Identification Number (TIC)	Yes
	Czech/Slovak ID	Yes
	Danish ID (CPR)	Yes
	Dutch ID (BSN)	Yes
	Estonian ID	Yes
	Finnish ID (HETU)	Yes
	French Tax Identification Number (SPI)	Yes
	German Tax Identification Number (Steuerliche Identifikationsnummer)	Yes
	Greek ID	Yes
	Hungarian Tax Identification Number	Yes
	Irish ID (PPS)	Yes
	Israeli ID	Yes
	Italian Tax Identification Number	Yes
	Latvian ID	Yes
	Lithuanian ID	Yes
	Luxembourg ID	Yes
	Maltese ID	Yes
	Polish ID (PESEL)	Yes
	Portuguese Tax Identification Number (NIF)	Yes
	Romanian ID (CNP)	Yes
	Slovenian ID (EMSO)	Yes
	South African ID	Yes
	Spanish Tax Identification Number	Yes
	Swedish ID	Yes
	U.K. ID (NINO)	Yes
	USA Social Security Number (SSN)	Yes

## **Types of sensitive personal data**

The sensitive personal data that Cloud Compliance can find in files includes the following:

### **Criminal Procedures Reference**

Data concerning a natural person's criminal convictions and offenses.

### **Ethnicity Reference**

Data concerning a natural person's racial or ethnic origin.

### **Health Reference**

Data concerning a natural person's health.

### **ICD-9-CM Medical Codes**

Codes used in the medical and health industry.

### **ICD-10-CM Medical Codes**

Codes used in the medical and health industry.

### **Philosophical Beliefs Reference**

Data concerning a natural person's philosophical beliefs.

### **Political Opinions Reference**

Data concerning a natural person's political opinions.

### **Religious Beliefs Reference**

Data concerning a natural person's religious beliefs.

### **Sex Life or Orientation Reference**

Data concerning a natural person's sex life or sexual orientation.

## **Types of categories**

Cloud Compliance categorizes your data as follows:

### **Finance**

- Balance Sheets
- Purchase Orders
- Invoices
- Quarterly Reports

### **HR**

- Background Checks
- Compensation Plans
- Employee Contracts
- Employee Reviews
- Health
- Resumes

## **Legal**

- NDAs
- Vendor-Customer contracts

## **Marketing**

- Campaigns
- Conferences

## **Operations**

- Audit Reports

## **Sales**

- Sales Orders

## **Services**

- RFI
- RFP
- SOW
- Training

## **Support**

- Complaints and Tickets

## **Metadata categories**

- Application Data
- Archive Files
- Audio
- Business Application Data
- CAD Files
- Code
- Database and index files
- Design Files
- Email Application Data
- Executables
- Financial Application Data
- Health Application Data
- Images
- Logs
- Miscellaneous Documents
- Miscellaneous Presentations
- Miscellaneous Spreadsheets
- Videos

## Types of files

Cloud Compliance scans all files for category and metadata insights and displays all file types in the file types section of the dashboard.

But when Cloud Compliance detects Personal Identifiable Information (PII), or when it performs a DSAR search, only the following file formats are supported:

.PDF, .DOCX, .DOC, .PPTX, .XLS, .XLSX, .CSV, .TXT, .RTF, and .JSON.

## Accuracy of information found

NetApp can't guarantee 100% accuracy of the personal data and sensitive personal data that Cloud Compliance identifies. You should always validate the information by reviewing the data.

Based on our testing, the table below shows the accuracy of the information that Cloud Compliance finds. We break it down by *precision* and *recall*:

### Precision

The probability that what Cloud Compliance finds has been identified correctly. For example, a precision rate of 90% for personal data means that 9 out of 10 files identified as containing personal information, actually contain personal information. 1 out of 10 files would be a false positive.

### Recall

The probability for Cloud Compliance to find what it should. For example, a recall rate of 70% for personal data means that Cloud Compliance can identify 7 out of 10 files that actually contain personal information in your organization. Cloud Compliance would miss 30% of the data and it won't appear in the dashboard.

Cloud Compliance is in a Controlled Availability release and we are constantly improving the accuracy of our results. Those improvements will be automatically available in future Cloud Compliance releases.

Type	Precision	Recall
Personal data - General	90%-95%	60%-80%
Personal data - Country identifiers	30%-60%	40%-60%
Sensitive personal data	80%-95%	20%-30%
Categories	90%-97%	60%-80%

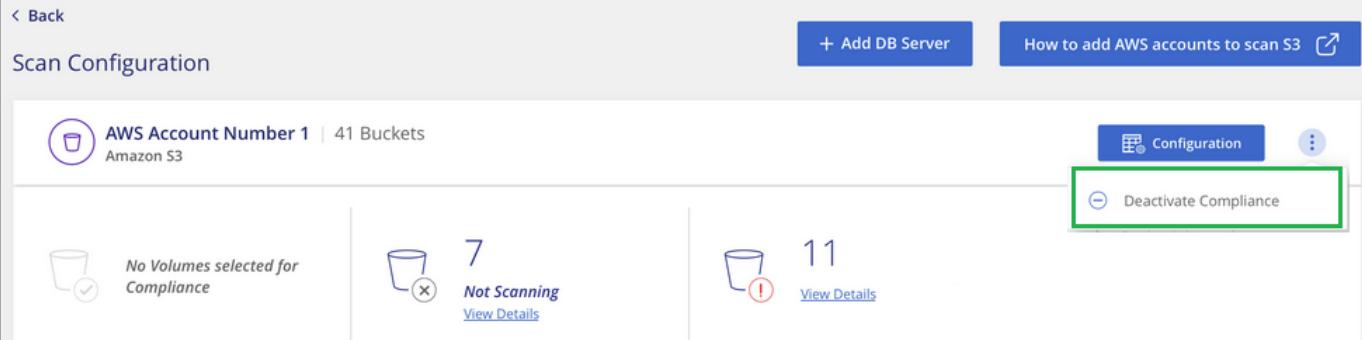
## Removing data sources from Cloud Compliance

If you need to, you can stop Cloud Compliance from scanning one or more working environments, databases, or OneDrive accounts. You can also delete the Cloud Compliance instance if you no longer want to use Cloud Compliance with your working environments.

### Deactivating compliance scans for a working environment

When you deactivate scans, Cloud Compliance no longer scans the data on the working environment and it removes the indexed compliance insights from the Cloud Compliance instance (the data from the working environment itself isn't deleted).

- From the *Scan Configuration* page, click the  button in the row for the working environment, and then click **Deactivate Compliance**.



The screenshot shows the 'Scan Configuration' page for an AWS account. At the top, it displays 'AWS Account Number 1 | 41 Buckets' and 'Amazon S3'. Below this, there are three main sections: 'No Volumes selected for Compliance' (7 items), 'Not Scanning' (11 items), and a 'View Details' link. In the top right corner, there are buttons for '+ Add DB Server', 'How to add AWS accounts to scan S3', and 'Configuration'. A green box highlights the 'Deactivate Compliance' button in the 'Configuration' dropdown menu.

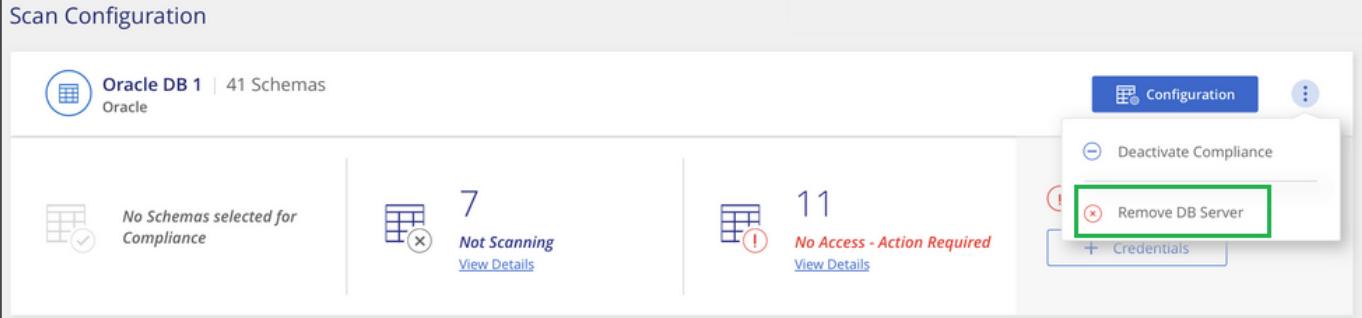


You can also disable compliance scans for a working environment from the Services panel when you select the working environment.

## Removing a database from Cloud Compliance

If you no longer want to scan a certain database, you can delete it from the Cloud Compliance interface and stop all scans.

- From the *Scan Configuration* page, click the  button in the row for the database, and then click **Remove DB Server**.



The screenshot shows the 'Scan Configuration' page for an Oracle database. At the top, it displays 'Oracle DB 1 | 41 Schemas' and 'Oracle'. Below this, there are three main sections: 'No Schemas selected for Compliance' (7 items), 'Not Scanning' (11 items), and a 'View Details' link. In the top right corner, there are buttons for '+ Add DB Server', 'How to add AWS accounts to scan S3', and 'Configuration'. A green box highlights the 'Remove DB Server' button in the 'Configuration' dropdown menu.

## Removing a OneDrive account from Cloud Compliance

If you no longer want to scan user files from a certain OneDrive account, you can delete the account from the Cloud Compliance interface and stop all scans.

### Steps

- From the *Scan Configuration* page, click the  button in the row for the OneDrive account, and then click **Remove OneDrive Account**.

The screenshot shows a user interface for managing cloud storage accounts. At the top, there's a header with the title 'Scan Configuration' and a 'Add Data Source' button. Below the header, a list displays a single account: 'OneDrive Account 1 | 41 Users'. To the right of this account entry are three buttons: 'Configuration' (with a gear icon), a vertical ellipsis menu, and a green-bordered 'Remove' button containing a red 'X' icon. A green rectangular box highlights the 'Remove' button.

2. Click **Delete Account** from the confirmation dialog.

## Deleting the Cloud Compliance instance

You can delete the Cloud Compliance instance if you no longer want to use Cloud Compliance. Deleting the instance also deletes the associated disks where the indexed data resides.

1. Go to your cloud provider's console and delete the Cloud Compliance instance.

The instance is named *CloudCompliance* with a generated hash (UUID) concatenated to it. For example:  
*CloudCompliance-16bb6564-38ad-4080-9a92-36f5fd2f71c7*

## Frequently asked questions about Cloud Compliance

This FAQ can help if you're just looking for a quick answer to a question.

### What is Cloud Compliance?

Cloud Compliance is a cloud offering that uses Artificial Intelligence (AI) driven technology to help organizations understand data context and identify sensitive data across your storage systems. The systems can be Azure NetApp Files configurations, Cloud Volumes ONTAP systems hosted in AWS or Azure, Amazon S3 buckets, on-prem ONTAP systems, databases, and OneDrive accounts.

Cloud Compliance provides pre-defined parameters (such as sensitive information types and categories) to address new data compliance regulations for data privacy and sensitivity, such as GDPR, CCPA, HIPAA, and more.

### Why should I use Cloud Compliance?

Cloud Compliance can empower you with data to help you:

- Comply with data compliance and privacy regulations.
- Comply with data retention policies.
- Easily locate and report on specific data in response to data subjects, as required by GDPR, CCPA, HIPAA, and other data privacy regulations.

### What are the common use cases for Cloud Compliance?

- Identify Personal Identifiable Information (PII).
- Identify a wide scope of sensitive information as required by GDPR and CCPA privacy regulations.
- Comply with new and upcoming data privacy regulations.

[Learn more about the use cases for Cloud Compliance.](#)

## **What types of data can be scanned with Cloud Compliance?**

Cloud Compliance supports scanning of unstructured data over NFS and CIFS protocols that are managed by Cloud Volumes ONTAP and Azure NetApp Files. Cloud Compliance can also scan data stored on Amazon S3 buckets and on-prem ONTAP systems.

Additionally, Cloud Compliance can scan databases that are located anywhere, and user files from OneDrive accounts.

[Learn how scans work.](#)

## **Which cloud providers are supported?**

Cloud Compliance operates as part of Cloud Manager and currently supports AWS and Azure. This provides your organization with unified privacy visibility across different cloud providers. Support for Google Cloud Platform (GCP) will be added soon.

## **How do I access Cloud Compliance?**

Cloud Compliance is operated and managed through Cloud Manager. You can access Cloud Compliance features from the **Compliance** tab in Cloud Manager.

## **How does Cloud Compliance work?**

Cloud Compliance deploys another layer of Artificial Intelligence alongside your Cloud Manager system and storage systems. It then scans the data on volumes, buckets, databases, and OneDrive and indexes the data insights that are found.

[Learn more about how Cloud Compliance works.](#)

## **How much does Cloud Compliance cost?**

The cost to use Cloud Compliance depends on the amount of data that you're scanning. The first 1 TB of data that Cloud Compliance scans in a Cloud Manager workspace is free. A subscription to the AWS or Azure Marketplace is required to continue scanning data after that point. See [pricing](#) for details.

## **How often does Cloud Compliance scan my data?**

Data changes frequently, so Cloud Compliance scans your data continuously with no impact to your data. While the initial scan of your data might take longer, subsequent scans only scan the incremental changes, which reduces system scan times.

[Learn how scans work.](#)

## **Does Cloud Compliance offer reports?**

Yes. The information offered by Cloud Compliance can be relevant to other stakeholders in your organizations, so we enable you to generate reports to share the insights.

The following reports are available for Cloud Compliance:

## **Privacy Risk Assessment report**

Provides privacy insights from your data and a privacy risk score. [Learn more.](#)

## **Data Subject Access Request report**

Enables you to extract a report of all files that contain information regarding a data subject's specific name or personal identifier. [Learn more.](#)

## **PCI DSS report**

Helps you identify the distribution of credit card information across your files. [Learn more.](#)

## **HIPAA report**

Helps you identify the distribution of health information across your files. [Learn more.](#)

## **Reports on a specific information type**

Reports are available that include details about the identified files that contain personal data and sensitive personal data. You can also see files broken down by category and file type. [Learn more.](#)

## **What type of instance or VM is required for Cloud Compliance?**

- In Azure, Cloud Compliance runs on a Standard\_D16s\_v3 VM with a 512 GB disk.
- In AWS, Cloud Compliance runs on an m5.4xlarge instance with a 500 GB GP2 disk.

In regions where m5.4xlarge isn't available, Cloud Compliance runs on an m4.4xlarge instance instead.

You can also download and install Compliance software on a Linux host in your network or in the cloud. Everything works the same and you continue to manage your scan configuration and results through Cloud Manager. See [Deploying Cloud Compliance on premises](#) for system requirements and installation details.



Cloud Compliance is currently unable to scan S3 buckets and ANF files when it is installed on premises.

[Learn more about how Cloud Compliance works.](#)

## **Does scan performance vary?**

Scan performance can vary based on the network bandwidth and the average file size in your cloud environment.

## **Which file types are supported?**

Cloud Compliance scans all files for category and metadata insights and displays all file types in the file types section of the dashboard.

When Cloud Compliance detects Personal Identifiable Information (PII), or when it performs a DSAR search, only the following file formats are supported:

.PDF, .DOCX, .DOC, .PPTX, .XLS, .XLSX, .CSV, .TXT, .RTF, and .JSON.

## **How do I enable Cloud Compliance?**

First you need to deploy an instance of Cloud Compliance in Cloud Manager. Once the instance is running, you can enable it on existing working environments and databases from the **Compliance** tab or by selecting a

specific working environment.

[Learn how to get started.](#)



Activating Cloud Compliance results in an immediate initial scan. Compliance results display shortly after.

## How do I disable Cloud Compliance?

You can disable Cloud Compliance from the Canvas page after you select an individual working environment.

[Learn more.](#)



To completely remove the Cloud Compliance instance, you can manually remove the Cloud Compliance instance from your cloud provider's portal.

## What happens if data tiering is enabled on Cloud Volumes ONTAP?

You might want to enable Cloud Compliance on a Cloud Volumes ONTAP system that tiers cold data to object storage. If data tiering is enabled, Cloud Compliance scans all of the data—data that's on disks and cold data tiered to object storage.

The compliance scan doesn't heat up the cold data—it stays cold and tiered to object storage.

## Can I use Cloud Compliance to scan on-premises ONTAP storage?

Yes. As long as you have discovered the on-prem ONTAP cluster as a working environment in Cloud Manager, you can scan any of the volume data.

Alternatively, you can run compliance scans on backup files created from your on-prem ONTAP volumes. So if you're already creating backup files from your on-prem systems using [Cloud Backup](#), you can run compliance scans on those backup files.

[Learn more.](#)

## Can Cloud Compliance send notifications to my organization?

Yes. In conjunction with the Highlights feature, you can send email alerts to Cloud Manager users (daily, weekly, or monthly) when a highlight return results so you can get notifications to protect your data. Learn more about [highlights](#).

You can also download status reports in .CSV format that you can share internally in your organization.

## Can I customize the service to my organization's needs?

Cloud Compliance provides out-of-the-box insights to your data. These insights can be extracted and used for your organization's needs.

Additionally, you can use the **Data Fusion** capability to have Cloud Compliance scan all your data based on criteria found in specific columns in databases you are scanning — essentially allowing you to make your own custom personal data types.

[Learn more.](#)

## **Can Cloud Compliance work with the AIP labels I have embedded in my files?**

Yes. You can manage AIP labels in the files that Cloud Compliance is scanning if you have subscribed to [Azure Information Protection \(AIP\)](#). You can view the labels that are already assigned to files, add labels to files, and change labels when a label already exists.

[Learn more.](#)

## **Can I limit Cloud Compliance information to specific users?**

Yes, Cloud Compliance is fully integrated with Cloud Manager. Cloud Manager users can only see information for the working environments they are eligible to view according to their workspace privileges.

Additionally, if you want to allow certain users to just view Cloud Compliance scan results without having the ability to manage Cloud Compliance settings, you can assign those users the *Cloud Compliance Viewer* role.

[Learn more.](#)

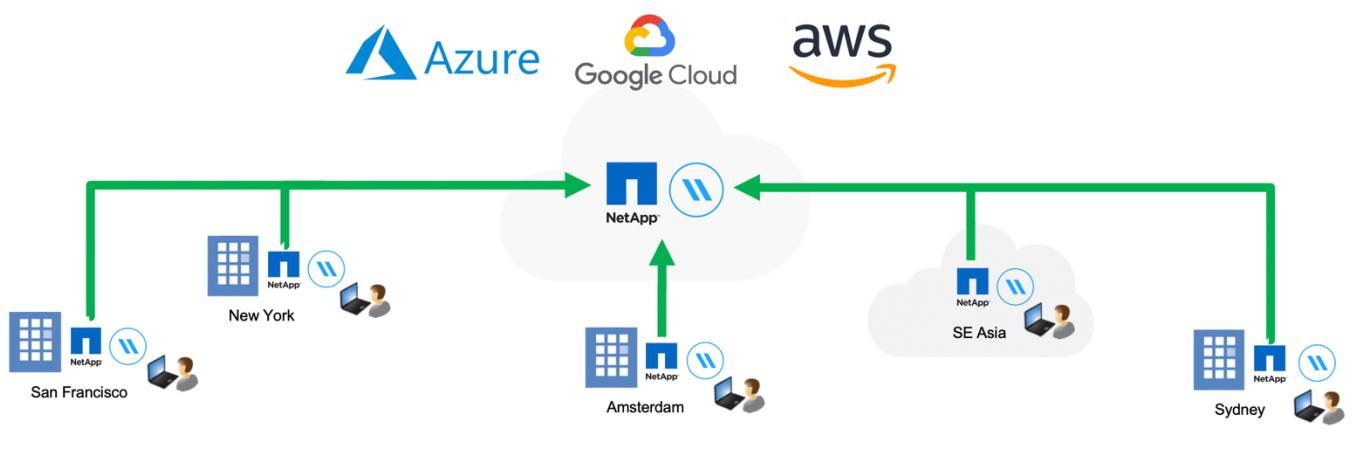
# Enable real-time global file sharing

## Learn about Global File Cache

NetApp Global File Cache enables you to consolidate silos of distributed file servers into one cohesive global storage footprint in the public cloud. This creates a globally accessible file system in the cloud that all remote locations can use as if they were local.

### Overview

Implementing Global File Cache results in a single, centralized storage footprint, versus a distributed storage architecture that requires local data management, backup, security management, storage, and infrastructure footprint in each location.



### Features

Global File Cache enables the following features:

- Consolidate and centralize your data into the public cloud and leverage the scalability and performance from enterprise-grade storage solutions
- Create a single set of data for users globally and leverage intelligent file caching to improve global data access, collaboration, and performance
- Rely on a self-sustaining, self-managing cache, and eliminate full data copies and backups. Utilize local file caching for active data and cut storage costs
- Transparent access from branch locations through a global namespace with real time central file locking

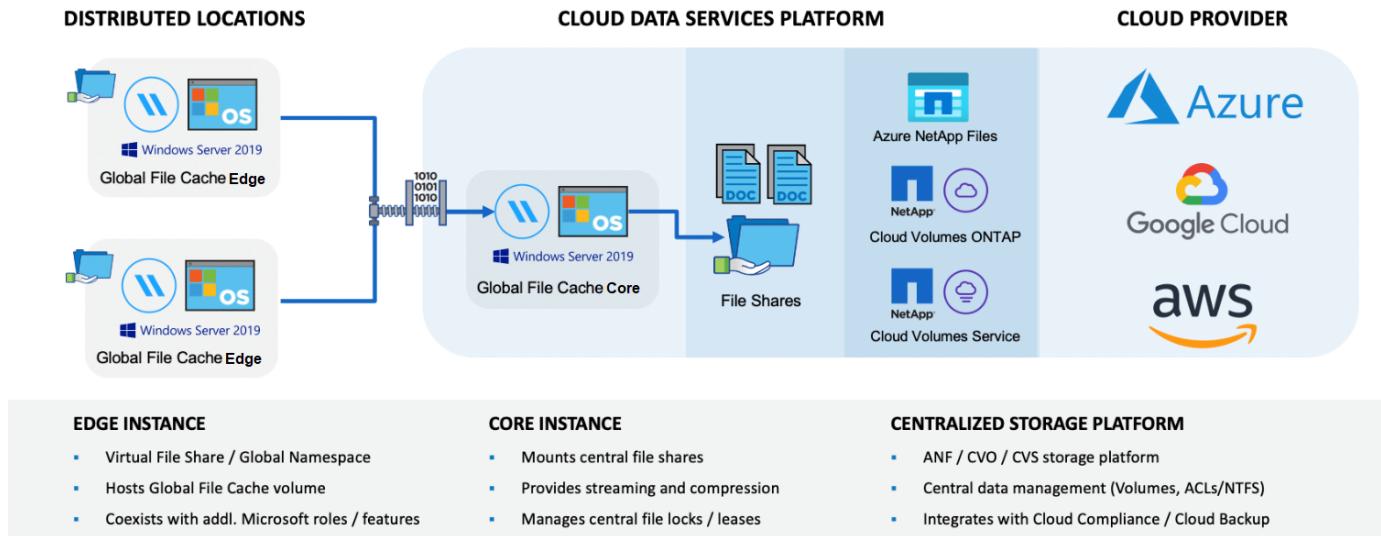
See more about Global File Cache features and use cases [here](#).

### Global File Cache components

Global File Cache consists of the following components:

- Global File Cache Management Server
- Global File Cache Core
- Global File Cache Edge (deployed in your remote locations)

The Global File Cache Core instance mounts to your corporate file shares hosted on your backend storage platform of choice (such as Cloud Volumes ONTAP, Cloud Volumes Service, and Azure NetApp Files) and creates the Global File Cache Fabric that provides the ability to centralize and consolidate unstructured data into a single set of data, whether it resides on one or multiple storage platforms in the public cloud.



## Supported storage platforms

The supported storage platforms for Global File Cache differ depending on the deployment option you select.

### Automated deployment options

Global File Cache is supported with the following types of working environments when deployed using Cloud Manager:

- Cloud Volumes ONTAP in Azure
- Cloud Volumes ONTAP in AWS

This configuration lets you deploy and manage the entire Global File Cache server-side deployment, including Global File Cache Management Server and Global File Cache Core, from within Cloud Manager.

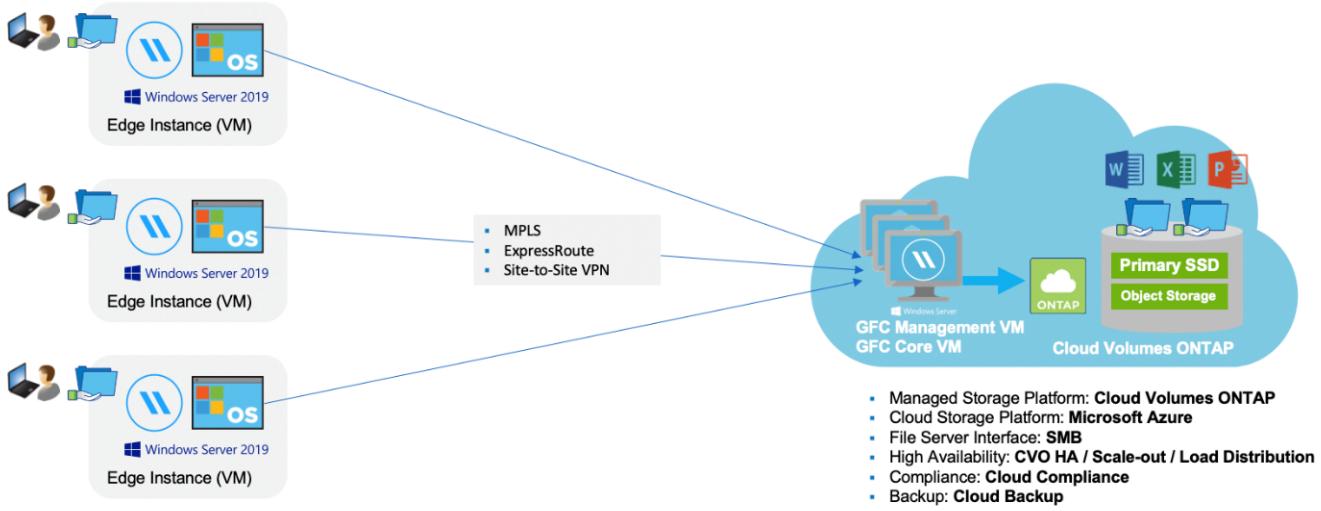
### Manual deployment options

Global File Cache configurations are also supported with Cloud Volumes ONTAP, Cloud Volumes Service, or Azure NetApp Files installed on Microsoft Azure, Google Cloud Platform, or Amazon Web Services public cloud storage infrastructure. On-premises solutions are also available on NetApp AFF and FAS platforms. In these installations the Global File Cache server-side components must be configured and deployed manually, not using Cloud Manager.

See the [NetApp Global File Cache User Guide](#) for details.

## How Global File Cache works

Global File Cache creates a software fabric that caches active data sets in remote offices globally. As a result, business users are guaranteed transparent data access and optimal performance on a global scale.



The topology referenced in this example is a hub and spoke model, whereby the network of remote offices/locations is accessing one common set of data in the cloud. The key points of this example are:

- Centralized data store:
  - Enterprise public cloud storage platform, such as Cloud Volumes ONTAP
- Global File Cache Fabric:
  - Extension of the central data store to the remote locations
  - Global File Cache Core instance, mounting to corporate file shares (SMB).
  - Global File Cache Edge instances running in each remote location.
  - Presents a virtual file share in each remote location that provides access to central data.
  - Hosts the Intelligent File Cache on a custom-sized NTFS volume ([D:\](#)).
- Network configuration:
  - Multiprotocol Label Switching (MPLS), ExpressRoute, or VPN connectivity
- Integration with customer's Active Directory domain services.
- DFS namespace for the use of a global namespace (recommended).

## Cost

The cost to use Global File Cache depends on the type of installation you have chosen.

- All installations require that you deploy one or more volumes in the cloud (Cloud Volumes ONTAP, Cloud Volumes Service, or Azure NetApp Files). This results in charges from the selected cloud provider.
- All installations also require that you deploy two or more virtual machines (VMs) in the cloud. This results in charges from the selected cloud provider.
  - Global File Cache Management Server:

In Azure, this runs on a D2s\_V3 or equivalent (2 vCPU/8GB RAM) VM with 127GB premium SSD

In AWS, this runs on a m4.large or equivalent (2 vCPU/8GB RAM) instance with 127GB general purpose SSD

- Global File Cache Core:

In Azure, this runs on a D4s\_V3 or equivalent (4 vCPU/16GB RAM) VM with 127GB premium SSD

In AWS, this runs on a m4.xlarge or equivalent (4 vCPU/16GB RAM) instance with 127GB general purpose SSD

- When installed with Cloud Volumes ONTAP in Azure or AWS (the supported configurations deployed completely through Cloud Manager), there is a charge of \$3,000 per site (for each Global File Cache Edge instance), per year.
- When installed using the manual deployment options the pricing is different. To see a high-level estimate of costs, see [Calculate Your Savings Potential](#) or consult your Global File Cache Solutions Engineer to discuss the best options for your enterprise deployment.

## Licensing

Global File Cache includes a software-based License Management Server (LMS), which allows you to consolidate your license management and deploy licenses to all Core and Edge instances using an automated mechanism.

When you deploy your first Core instance in the datacenter or cloud, you can choose to designate that instance as the LMS for your organization. This LMS instance is configured once, connects to the subscription service (over HTTPS) and validates your subscription using the customer ID provided by our support/operations department upon enablement of the subscription. After you have made this designation, you associate your Edge instances with the LMS by providing your customer ID and the IP address of the LMS instance.

When you purchase additional Edge licenses or renew your subscription, our support/operations department updates the license details, for example, the number of sites or subscription end date. After the LMS queries the subscription service, the license details are automatically updated on the LMS instance and will apply to your GFC Core and Edge instances.

See the [NetApp Global File Cache User Guide](#) for additional details about licensing.

## Limitations

- The version of Global File Cache supported within Cloud Manager requires that the backend storage platform used as your central storage must be a working environment where you have deployed a Cloud Volumes ONTAP single node or HA pair in Azure or AWS.

Other storage platforms and other cloud providers are not supported at this time using Cloud Manager, but can be deployed using legacy deployment procedures.

These other configurations, for example, Global File Cache using Cloud Volumes ONTAP or Cloud Volumes Service on Microsoft Azure, Google Cloud, or AWS continue to be supported using the legacy procedures. See [Global File Cache overview and onboarding](#) for details.

## Release Notes

### What's new in version 1.0.2

Released: 6 Jan 2021

- Global File Cache now supports subscription ID based licensing. The Subscription Number is emailed to

you after you register your system. See [Licensing Global File Cache](#) for details.

- The requirement for the GFC Core joining the domain has been relaxed. Now a username (part of Backup Operators group on the Cloud Volumes ONTAP system) is used to configure GFC services.
- The License Manager Server (LMS) now has an additional HTTPS endpoint to de-register any registration.

## Fixed issues in version 1.0.2

- Duplicate GFC icons are no longer displayed on the desktop during upgrade.
- The License Manager Client Service (LMC) now retains the correct licensing information when the service is restarted.

# Before you begin to deploy Global File Cache

There are many requirements you need to be aware of before you begin to deploy Global File Cache in the cloud and in your remote offices.

## Global File Cache Core design considerations

Depending on your requirements, you may need to deploy one or multiple Global File Cache Core instances to create the Global File Cache Fabric. The Core instance is designed to act as a traffic cop between your distributed Global File Cache Edge instances and the data center file server resources, for example, file shares, folders, and files.

When you are designing your Global File Cache deployment you need to determine what's right for your environment in terms of scale, availability of resources, and in terms of redundancy. Global File Cache Core can be deployed in the following ways:

- GFC Core stand-alone instance
- GFC Core Load Distributed design (Cold Standby)

See [Sizing guidelines](#) to understand the maximum number of Edge instances and total users that each configuration can support:

Consult your Global File Cache Solutions Engineer to discuss the best options for your enterprise deployment.

## Sizing guidelines

There are a few sizing guideline ratios that you need to keep in mind when configuring the initial system. You should revisit these ratios after some usage history has accumulated to make sure you are using the system optimally. These include:

- Global File Cache Edges/Core ratio
- Distributed users/Global File Cache Edge ratio
- Distributed users/Global File Cache Core ratio

## Number of Edge Instances per Core Instance

Our guidelines recommend up to 10 Edge instances per Global File Cache Core instance, with a maximum of 20 Edges per Global File Cache Core instance. This is dependent to a significant degree upon the type and mean file size of the most common workload. In some cases, with more common workloads you can add more

Edge instances per Core, but in these cases you should contact NetApp Support to correctly size the number of Edge and Core instances depending on the types and sizes of the file sets.



You can leverage multiple Global File Cache Edge and Core instances simultaneously to scale out your infrastructure depending on the requirements.

### **Number of concurrent users per Edge instance**

Global File Cache Edge handles the heavy lifting in terms of caching algorithms and file-level differencing. A single Global File Cache Edge instance can serve up to 400 users per dedicated physical Edge instance, and up to 200 users for dedicated virtual deployments. This is dependent to a significant degree upon the type and mean file size of the most common workload. For larger collaborative file types, guide towards 50% of the maximum users per Global File Cache Edge lower boundary (depending on physical or virtual deployment). For more common Office items with a mean file size <1MB, guide towards the 100% users per Global File Cache Edge upper boundary (depending on physical or virtual deployment).



Global File Cache Edge detects whether it is running on a virtual or physical instance and it will limit the number of SMB connections to the local virtual file share to the maximum of 200 or 400 concurrent connections.

### **Number of concurrent users per Core instance**

The Global File Cache Core instance is extremely scalable, with a recommended concurrent user count of 3,000 users per Core. This is dependent to a significant degree upon the type and mean file size of the most common workload.

Consult your Global File Cache Solutions Engineer to discuss the best options for your enterprise deployment.

## **Prerequisites**

The prerequisites described in this section are for the components installed in the cloud: the Global File Cache Management Server and the Global File Cache Core.

Global File Cache Edge prerequisites are described [here](#).

### **Cloud Manager instance**

When using Cloud Volumes ONTAP for Azure as your storage platform, ensure that Cloud Manager has permissions as shown in the latest [Cloud Manager policy for Azure](#).

Newly created instances will have all the required permissions by default. If you deployed your instance prior to version 3.8.7 (August 3, 2020), then you will need to add these items.

```
"Microsoft.Resources/deployments/operationStatuses/read",
"Microsoft.Insights/Metrics/Read",
"Microsoft.Compute/virtualMachines/extensions/write",
"Microsoft.Compute/virtualMachines/extensions/read",
"Microsoft.Compute/virtualMachines/extensions/delete",
"Microsoft.Compute/virtualMachines/delete",
"Microsoft.Network/networkInterfaces/delete",
"Microsoft.Network/networkSecurityGroups/delete",
"Microsoft.Resources/deployments/delete",
```

## Storage platform (volumes)

The back-end storage platform – in this case, your deployed Cloud Volumes ONTAP instance - should present SMB file shares. Any shares that will be exposed through Global File Cache must allow the Everyone group Full Control at the share level, while restricting permissions through NTFS permissions.

If you have not set up at least one SMB file share on the Cloud Volumes ONTAP instance, then you need to have the following information ready so you can configure this information during installation:

- Active Directory domain name, name server IP address, Active Directory admin credentials.
- The name and size of the volume you want to create, the name of the aggregate on which the volume will be created, and the share name.

We recommend that the volume is large enough to accommodate the total data set for the application along with the ability to scale accordingly as the data set grows. If you have multiple aggregates in the working environment, see [Managing existing aggregates](#) to determine which aggregate has the most available space for the new volume.

## Global File Cache Management Server

This Global File Cache Management Server requires external access over HTTPS (TCP port 443) to connect to the cloud provider subscription service and to access these URLs:

- <https://talonazuremicroservices.azurewebsites.net>
- <https://talonlicensing.table.core.windows.net>

This port must be excluded from any WAN optimization devices or firewall restriction policies for the Global File Cache software to operate properly.

The Global File Cache Management Server also requires a unique (geographical) NetBIOS name for the instance (such as GFC-MS1).



One Management Server can support multiple Global File Cache Core instances deployed in different working environments. When deployed from Cloud Manager, each working environment has its own separate backend storage and would not contain the same data.

## Global File Cache Core

This Global File Cache Core listens on TCP port range 6618-6630. Depending on your firewall or Network Security Group (NSG) configuration you may need to explicitly allow access to these ports through Inbound

Port Rules. Also, these ports must be excluded from any WAN optimization devices or firewall restriction policies for the Global File Cache software to operate properly.

The Global File Cache Core requirements are:

- A unique (geographical) NetBIOS name for the instance (such as GFC-CORE1)
- Active Directory domain name
  - Global File Cache instances should be joined to your Active Directory domain.
  - Global File Cache instances should be managed in a Global File Cache specific Organizational Unit (OU) and excluded from inherited company GPOs.
- Service account. The services on this Global File Cache Core run as a specific domain user account. This account, also known as the Service Account, must have the following privileges on each of the SMB servers that will be associated with the Global File Cache Core instance:
  - The provisioned Service Account must be a domain user.

Depending on the level of restrictions and GPOs in the network environment, this account might require domain admin privileges.

- It must have "Run as a Service" privileges.
- The password should be set to "Never Expire".
- The account option "User Must Change Password at Next Logon" should be DISABLED (unchecked).
- It must be a member of the back-end file server Built-in Backup Operators group (this is automatically enabled when deployed through Cloud Manager).

## **License Management Server**

- The Global File Cache License Management Server (LMS) should be configured on a Microsoft Windows Server 2016 Standard or Datacenter edition or Windows Server 2019 Standard or Datacenter edition, preferably on the Global File Cache Core instance in the datacenter or cloud.
- If you require a separate Global File Cache LMS instance, you need to install the latest Global File Cache software installation package on a pristine Microsoft Windows Server instance.
- The LMS instance needs to be able to connect to the subscription service (Azure Services / public internet) using HTTPS (TCP port 443).
- The Core and Edge instances need to connect to the LMS instance using HTTPS (TCP port 443).

## **Networking**

- Firewall: TCP ports should be allowed between Global File Cache Edge and Core instances.
- Global File Cache TCP Ports: 443 (HTTPS), 6618–6630.
- Network optimization devices (such as Riverbed Steelhead) must be configured to pass-thru Global File Cache specific ports (TCP 6618-6630).

# **Getting started**

You use Cloud Manager to deploy the Global File Cache Management Server and Global File Cache Core software in the working environment.

## Enable Global File Cache using Cloud Manager

In this configuration you will deploy the Global File Cache Management Server and Global File Cache Core in the same working environment where you created your Cloud Volumes ONTAP system using Cloud Manager.

Watch [this video](#) to see the steps from start to finish.

### Quick start

Get started quickly by following these steps or scroll down to the remaining sections for full details:



#### Deploy Cloud Volumes ONTAP

Deploy Cloud Volumes ONTAP in Azure or AWS and configure SMB file shares. For more information, see [Launching Cloud Volumes ONTAP in Azure](#) or [Launching Cloud Volumes ONTAP in AWS](#).



#### Deploy the Global File Cache Management Server

Deploy an instance of the Global File Cache Management Server in the same working environment as the instance of Cloud Volumes ONTAP.



#### Deploy the Global File Cache Core

Deploy an instance, or multiple instances, of the Global File Cache Core in the same working environment as the instance of Cloud Volumes ONTAP and join it to your Active Directory domain.



#### License Global File Cache

Configure the Global File Cache License Management Server (LMS) service on a Global File Cache Core instance. You will need your NSS Credentials or a Customer ID and Subscription Number provided by NetApp to activate your subscription.



#### Deploy the Global File Cache Edge instances

See [Deploying Global File Cache Edge instances](#) to deploy the Global File Cache Edge instances in each remote location. This step is not done using Cloud Manager.

### Deploy Cloud Volumes ONTAP as your storage platform

In the current release, Global File Cache supports Cloud Volumes ONTAP deployed in Azure or AWS. For detailed prerequisites, requirements, and deployment instructions, see [Launching Cloud Volumes ONTAP in Azure](#) or [Launching Cloud Volumes ONTAP in AWS](#).

Note the following additional Global File Cache requirement:

- You should configure SMB file shares on the instance of Cloud Volumes ONTAP.

If no SMB file shares are set up on the instance, then you are prompted to configure the SMB shares during the installation of the Global File Cache components.

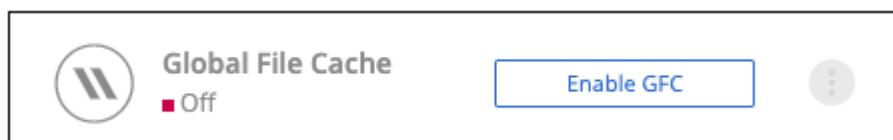
## Enable Global File Cache in your working environment

The Global File Cache wizard walks you through the steps to deploy the Global File Cache Management Server instance and the Global File Cache Core instance, as highlighted below.

The screenshot shows the Cloud Manager dashboard with the 'File Cache' tab selected. Below it, the 'Enable GFC' section is active, indicated by a blue icon. A progress bar at the top shows five steps: Overview (1), Enable GFC Service (2), GFC Service (Setup) (3), Deploy GFC Core (4), and GFC Core (Setup) (5). Step 1 is completed, while steps 2 through 5 are in progress. The main content area displays a diagram titled 'Thank you for enabling NetApp Global File Cache'. It illustrates a network topology where three 'Edge Instance (VM)' boxes on the left connect via 'ExpressRoute' or 'Site-to-Site VPN' to a central 'GFC Management Server' cloud icon. This server contains 'Microsoft OS' and 'GFC Core' components, which are connected to 'ONTAP' and 'Cloud Volumes ONTAP' storage. A note below the diagram states: 'From a high-level perspective, we will guide you through the process of deploying the GFC Core Instance in the public cloud and provide you with the instructions to start off your branch office deployment, the Edge instance.' A 'Continue' button is located at the bottom of the page.

### Steps

1. Select the working environment where you deployed Cloud Volumes ONTAP.
2. In the Services panel, click **Enable GFC**.



3. Read the Overview page and click **Continue**.
4. If no SMB shares are available on the Cloud Volumes ONTAP instance, you are prompted to enter the SMB Server and SMB Share details to create the share now. For details about the SMB configuration, see [Storage platform](#).

When finished, click **Continue** to create the SMB share.

### SMB Setup

<b>SMB Server</b>	<b>SMB Share</b>
Active Directory Domain <input type="text" value="gfc.netapp.com"/>	Volume Name <input type="text" value="Enter Volume Name"/> Volume Size(GB) <input type="text"/>
Name Server IP Address <input type="text" value="10.0.2.4"/>	Select Aggregate <input type="text" value="Select Aggregate"/>
Active Directory Admin User <input type="text" value="cvoadmin"/>	Share Name <input type="text" value="Enter Share Name"/>
Active Directory Admin Password <input type="password" value="*****"/>	Thin provisioning Enabled
	Deduplication Enabled

5. On the Global File Cache Service page, enter the number of Global File Cache Edge instances you plan to deploy, and then make sure your system meets the requirements for Network Configuration and Firewall Rules, Active Directory settings, and Antivirus exclusions. See [Prerequisites](#) for more details.

## Enable Global File Cache Service

### Licensing Global File Cache:

Once you've completed this deployment process, you will need your NSS Credentials to activate your subscription. If you haven't purchased or received your NetApp Global File Cache licenses, which are available as an Edge-based license, they can be purchased through your NetApp Partner or NetApp Sales Representative.

How many edge instances are you planning to deploy?

10



### Before you begin:

Here are the most important requirements for your environment before you can deploy the NetApp Global File Cache solution:

Configure the required Network Configuration and Firewall Rules for Global File Cache



Create a "Service Account" in your Active Directory domain: GFC.NETAPP.COM



Update Antivirus Exclusions for your Windows Server infrastructure by committing the required exclusions to your Antivirus services



For more information on all the solution requirements [Click Here](#)

**Continue**

6. After you have verified that the requirements have been met, or that you have the information to meet these requirements, click **Continue**.
7. Enter the admin credentials you will use to access to the Global File Cache Management Server VM and click **Enable GFC Service**. For Azure you enter the credentials as a user name and password; for AWS you select the appropriate key pair. You can change the VM/instance name if you want.

## Global File Cache Service (Setup)

### Information

Subscription Name OCCM Dev

Azure Region eastus

VNet Vnet1

Subnet Subnet2

Resource Group occm\_group\_eastus

### Credentials & Virtual Machine

Local Admin Name

GFCAdmin

Local Admin Password

\*\*\*\*\*

VM Name

GFC-MS1|

**Enable GFC Service**

8. After the Global File Cache Management Service is successfully deployed, click **Continue**.
9. For the Global File Cache Core, enter the admin user credentials to join the Active Directory domain, and the service account user credentials. Then click **Continue**.
  - The Global File Cache Core instance must be deployed in the same Active Directory domain as the Cloud Volumes ONTAP instance.
  - The service account is a domain user and it is part of the BUILTIN\Backup Operators group on the Cloud Volumes ONTAP instance.

## Deploy Global File Cache Core

### Active Directory and Admin Credentials

Provide administrative credentials to join the GFC Core instance to the Active Directory domain

Join Active Directory Domain i

Admin User i

Admin Password i

### Account User Credentials

Provide Service Account credentials

Service Account User i

Service Account Password i

**Continue**

10. Enter the admin credentials you will use to access to the Global File Cache Core VM and click **Deploy GFC Core**. For Azure you enter the credentials as a user name and password; for AWS you select the appropriate key pair. You can change the VM/instance name if you want.

## Global File Cache Core (Setup)

### Information

Subscription Name	Subscription_1234567891234...
Region	East US   Virginia
VNet	VNet_1234567
Subnet	10.0.0.0/24
Resource Group	Resource Group 1

### Credentials & Virtual Machine

Local Admin Name

Admin@netapp.com

Local Admin Password

\*\*\*\*\*

VM Name

GFC-CORE-1234

Local Admin Name & Password are inherited from the Global File Cache Management Service. The Virtual Machine Name is associated to your Cloud Manager Account

**Deploy GFC Core**

- After the Global File Cache Core is successfully deployed, click **Go to Dashboard**.

The screenshot shows the Global File Cache Management Instance dashboard. It displays a single instance with the following details:

Hostname: www.working-environment-1.com	Status: ON				
IP Address: 141.226.210.219	Region: East US	VNet: VNet1	Subnet: 10.10.10.10/24	RGName: Resource Group	CPU Utilization: 26%

**1 Working Environment**

Name: Working Environment_1	Type: High Availability	Status: ON	Core Instances: 2	Add Core Instance
-----------------------------	-------------------------	------------	-------------------	-------------------

**Instance Core 1 | ON**

Hostname: www.working-environment-1.com	IP Address: 141.226.210.219	CPU Utilization: 26%	Network Inbound: 2.5 TB	Network Outbound: 2.5 TB	Deploy GFC Edge
---	-----------------------------	----------------------	-------------------------	--------------------------	-----------------

The Dashboard shows that the Management Server instance and the Core instance are both **On** and working.

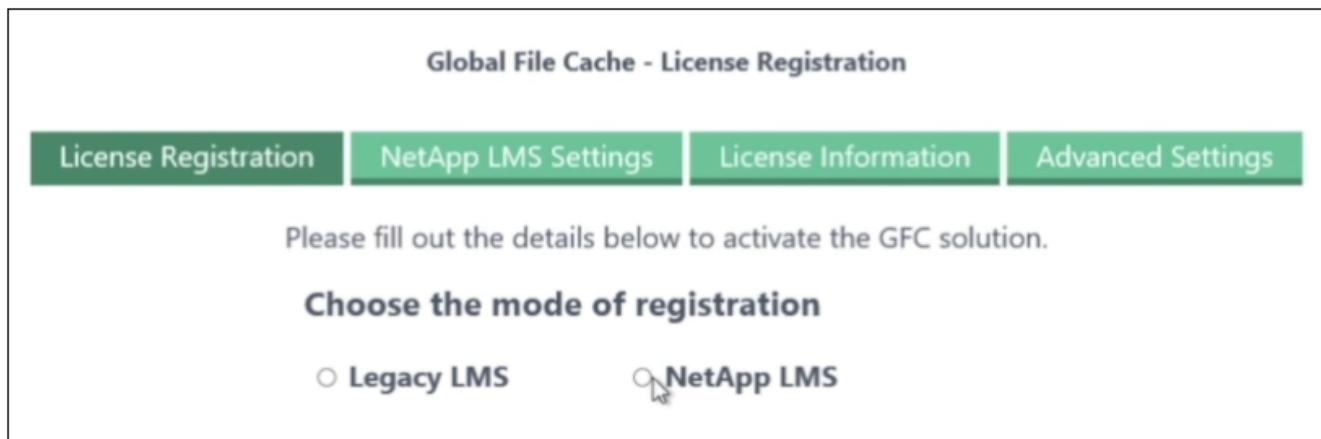
## License your Global File Cache installation

Before you can use Global File Cache, you need to configure the Global File Cache License Management Server (LMS) service on a Global File Cache Core instance. You will need your NSS Credentials or a Customer ID and Subscription Number provided NetApp to activate your subscription.

In this example, we will configure the LMS service on a Core instance that you just deployed in the public cloud. This is a one-time process that sets up your LMS service.

### Steps

1. Open the Global File Cache License Registration page on the Global File Cache Core (the Core you are designating as your LMS service) using the following URL. Replace <ip\_address> with the IP address of the Global File Cache Core:  
[https://<ip\\_address>/lms/api/v1/config/lmsconfig.html](https://<ip_address>/lms/api/v1/config/lmsconfig.html)
2. Click “**Continue to this website (not recommended)**” to continue. A page that allows you to configure the LMS, or check existing license information, is displayed.



Global File Cache - License Registration

License Registration    NetApp LMS Settings    License Information    Advanced Settings

Please fill out the details below to activate the GFC solution.

**Choose the mode of registration**

Legacy LMS     NetApp LMS

3. Choose the mode of registration:
  - “NetApp LMS” is used for customers who have purchased NetApp Global File Cache Edge licenses from NetApp or its certified partners. (Preferred)
  - “Legacy LMS” is used for existing or trial customers who have received a Customer ID through NetApp Support. (This option has been deprecated.)
4. For this example, click **NetApp LMS**, enter your Customer ID (preferably your email address), and click **Register LMS**.

## Global File Cache - License Registration

[License Registration](#)

[NetApp LMS Settings](#)

[License Information](#)

[Advanced Settings](#)

Please fill out the details below to activate the GFC solution.

### Choose the mode of registration

Legacy LMS

NetApp LMS

Customer Id:

john.doe@company.com

X

\* Choose a unique identifier for your GFC deployment, preferably your email address

[REGISTER LMS](#)

5. Check for a confirmation email from NetApp that includes your GFC Software Subscription Number and Serial Number.

The email snippet shows the NetApp logo and a circular image of a globe. To the right, the text reads "NetApp Support Site Available for GFC Customers". Below this, a blue link says "The NetApp Support Site is available for Global File Cache (GFC) customers. Please register for an account at this time." The body of the email continues with instructions for registering support, mentioning a software subscription number (A-S00008405) and a serial number (965000000000000000008405). It also encourages using the serial number as a unique identifier for support. A blue link at the bottom says "Activating Support Entitlement for your NetApp GFC serial number".

6. Click the **NetApp LMS Settings** tab.
7. Select **GFC License Subscription**, enter your GFC Software Subscription Number, and click **Submit**.

**Global File Cache - License Registration**

License Registration	NetApp LMS Settings	License Information	Advanced Settings
----------------------	---------------------	---------------------	-------------------

NSS Credentials  GFC License Subscription

GFC License Subscription:  X

**SUBMIT**

You will see a message that your GFC License Subscription was registered successfully and activated for the LMS instance. Any subsequent purchases will automatically be added to the GFC License Subscription.

8. Optionally, you can click the **License Information** tab to view all your GFC license information.

#### What's Next?

If you have determined that you need to deploy multiple Global File Cache Cores to support your configuration, click **Add Core Instance** from the Dashboard and follow the deployment wizard.

After you have completed your Core deployment, you need to [deploy the Global File Cache Edge instances](#) in each of your remote offices.

### Deploy additional Core instances

If your configuration requires more than one Global File Cache Core to be installed because of a large number of Edge instances, you can add another Core to the working environment.

When deploying Edge instances, you will configure some to connect to the first Core and others to the second Core. Both Core instances access the same backend storage (your Cloud Volumes ONTAP instance) in the working environment.

1. From the Global File Cache Dashboard, click **Add Core Instance**.

1 Working Environment				
 Working Environment_1	Name  <b>High Availability Type</b> ON	Status  <b>ON</b>	2  Core Instances	<a href="#" style="border: 2px solid green; padding: 2px 10px;">Add Core Instance</a> <span style="font-size: 20px; color: #ccc;">^</span>

Instance Core 1   ON					
www.working-environment-1.com  Hostname	141.226.210.219  IP Address	26%  CPU Utilization	2.5 TB  Network Inbound	2.5 TB  Network Outbound	<a href="#" style="border: 1px solid blue; padding: 2px 10px;">Deploy GFC Edge</a>

2. Enter the admin user credentials to join the Active Directory domain, and the service account user credentials. Then click **Continue**.
  - The Global File Cache Core instance must be in the same Active Directory domain as the Cloud Volumes ONTAP instance.
  - The service account is a domain user and it is part of the BUILTIN\Backup Operators group on the Cloud Volumes ONTAP instance.

## Deploy Global File Cache Core

### Active Directory and Admin Credentials

Provide administrative credentials to join the GFC Core instance to the Active Directory domain

Join Active Directory Domain (i)

Admin User (i)

Admin Password (i)

### Account User Credentials

Provide Service Account credentials

Service Account User (i)

Service Account Password (i)

**Continue**

3. Enter the admin credentials you will use to access to the Global File Cache Core VM and click **Deploy GFC Core**. For Azure you enter the credentials as a user name and password; for AWS you select the appropriate key pair. You can change the VM name if you want.

## Global File Cache Core (Setup)

### Information

Subscription Name	Subscription_1234567891234...
Region	East US   Virginia
VNet	VNet_1234567
Subnet	10.0.0.0/24
Resource Group	Resource Group 1

### Credentials & Virtual Machine

Local Admin Name

Admin@netapp.com

Local Admin Password

\*\*\*\*\*

VM Name

GFC-CORE-1234

Local Admin Name & Password are inherited from the Global File Cache Management Service. The Virtual Machine Name is associated to your Cloud Manager Account

[Deploy GFC Core](#)

- After the Global File Cache Core is successfully deployed, click **Go to Dashboard**.

1 Working Environment				
Name	Type	Status	Core Instances	
Working Environment_1	High Availability	ON	2	<a href="#">Add Core Instance</a>
<b>Instance Core 1   ON</b>				
www.working-environment-1.com	Hostname	141.226.210.219	2.5 TB	<a href="#">Deploy GFC Edge</a>
		IP Address	Network Inbound	Network Outbound
<b>Instance Core 1   ON</b>				
www.working-environment-1.com	Hostname	141.226.210.219	2.5 TB	<a href="#">Deploy GFC Edge</a>
		IP Address	Network Inbound	Network Outbound

The Dashboard reflects the second Core instance for the working environment.

## Before you begin to deploy Global File Cache Edge instances

There are many requirements you need to be aware of before you begin to install Global File Cache Edge software in your remote offices.

## Download required resources

Download the Global File Cache Virtual Templates you are planning to use in your branch offices, the software installation package, and additional reference documentation:

- Windows Server 2016 Virtual Template:

[Windows Server 2016 .OVA including NetApp GFC \(VMware VSphere 6.5+\)](#)

[Windows Server 2016 .VHDX including NetApp GFC \(Microsoft Hyper-v\)](#)

- Windows Server 2019 Virtual Template:

[Windows Server 2019 .OVA including NetApp GFC \(VMware VSphere 6.5+\)](#)

[Windows Server 2019 .VHDX including NetApp GFC \(Microsoft Hyper-v\)](#)

- Global File Cache Edge Software:

[NetApp GFC Software Installation Package \(.EXE\)](#)

- Global File Cache Documentation:

[NetApp Global File Cache User Guide \(.PDF\)](#)

## Designing and deploying Global File Cache Edge

Depending on your requirements, you might need to deploy one or multiple Global File Cache Edge instances based on the concurrent user sessions in a branch office. The Edge instance presents the virtual file share to the end users within the branch office, which has been transparently extended from the associated Global File Cache Core instance. The Global File Cache Edge should contain a `D:\` NTFS volume, which contains the cached files within the branch office.



For the Global File Cache Edge, it is important to understand the [sizing guidelines](#). This will assist you in making the correct design for your Global File Cache deployment. You would also need to determine what's right for your environment in terms of scale, availability of resources, and in terms of redundancy.

### Global File Cache Edge instance

When deploying a Global File Cache Edge instance, you need to provision a single VM, either by deploying Windows Server 2016 Standard or Datacenter Edition, or Windows Server 2019 Standard or Datacenter Edition, or using the Global File Cache `.OVA` or `.VHD` template, which includes the Windows Server operating system of choice and Global File Cache software.

#### Quick steps

1. Deploy the Global File Cache Virtual Template, or Windows Server 2016 VM, or Windows Server 2019 Standard or Datacenter edition.
2. Ensure the VM is connected to the network, joined to the domain, and accessible through RDP.
3. Install the latest Global File Cache Edge software.
4. Identify the Global File Cache Management Server and Core instance.
5. Configure the Global File Cache Edge instance.

## Global File Cache Edge requirements

Global File Cache Edge is designed to function across all platforms supporting Windows Server 2016 and 2019, bringing simplified IT to corporate remote offices and beyond. Critically, Global File Cache can be deployed on your existing hardware infrastructure, virtualization, or hybrid/public cloud environments in almost every case if they meet a few base-level requirements.

Global File Cache Edge requires the following hardware and software resources to function optimally. For more information about overall sizing guidelines, see [Sizing guidelines](#).

### Hardened server appliance

The Global File Cache installation package creates a hardened software appliance on any Microsoft Windows Server instance. *Do Not Uninstall* the Global File Cache Package. Uninstalling Global File Cache will impact the functionality of the server instance and might require a full rebuild of the server instance.

### Physical hardware requirements

- Minimum 4 CPU cores
- Minimum 16 GB RAM
- Dedicated single or redundant 1 Gbps NIC
- 10k RPM SAS HDD or SSD (preferred)
- RAID controller with write-back caching functionality enabled

### Virtual deployment requirements

Hypervisor platforms are known to be subject to performance degradation from a storage subsystem perspective (for example, latency). For optimal performance using Global File Cache, a physical server instance with SSD is recommended.

For best performance in virtual environments, in addition to the physical host requirements, the following requirements and resource reservations must be met:

Microsoft Hyper-V 2012 R2 and later:

- Processor (CPU): CPUs must be set as **Static**: Minimum: 4 vCPU cores.
- Memory (RAM): Minimum: 16 GB set as **Static**.
- Hard-disk provisioning: Hard Disks must be configured as **Fixed Disk**.

VMware vSphere 6.x and later:

- Processor (CPU): Reservation of CPU Cycles must be set. Minimum: 4 vCPU cores @ 10000 MHz.
- Memory (RAM): Minimum: Reservation of 16 GB.
- Hard-disk provisioning:
  - Disk Provisioning must be set as **Thick Provisioned Eager Zeroed**.
  - Hard Disk Shares must be set to **High**.
- Devices.hotplug must be set to **False** using the vSphere Client to prevent Microsoft Windows from presenting Global File Cache drives as removable.
- Networking: Network Interface must be set to **VMXNET3** (requires VM Tools).

Global File Cache runs on Windows Server 2016 and 2019, hence the virtualization platform needs to support the operating system, as well as integration with utilities enhancing the performance of the VM's guest operating system and management of the VM, such as VM Tools.

## Partition sizing requirements

- C:\ - minimum 250GB (system/boot volume)
- D:\ - minimum 1TB (separate data volume for Global File Cache Intelligent File Cache\*)

\*Minimum size is 2x the active data set. The cache volume (D:\) can be extended and is only restricted by the limitations of the Microsoft Windows NTFS file system.

## Global File Cache Intelligent File Cache disk requirements

Disk Latency on the Global File Cache Intelligent File Cache disk (D:\) should deliver < 0.5ms average I/O disk latency and 1MiBps throughput per concurrent user.

For more information, see the [NetApp Global File Cache User Guide](#).

## Networking

- Firewall: TCP ports should be allowed between the Global File Cache Edge and Management Server and Core instances.

Global File Cache TCP Ports: 443 (HTTPS - LMS), 6618 – 6630.

- Network optimization devices (such as Riverbed Steelhead) must be configured to pass-thru Global File Cache specific ports (TCP 6618-6630).

## Client workstation and application best practices

Global File Cache transparently integrates into customer's environments, allowing users to access centralized data using their client workstations, running enterprise applications. Using Global File Cache, data is accessed through a direct drive mapping or through a DFS namespace. For more information about the Global File Cache Fabric, Intelligent File Caching, and key aspects of the software, consult the [Before you begin to Deploy Global File Cache](#) section.

To ensure an optimal experience and performance, it is important to comply with the Microsoft Windows Client requirements and best practices as outlined in the Global File Cache User Guide. This applies to all versions of Microsoft Windows.

For more information, see the [NetApp Global File Cache User Guide](#).

## Firewall and Antivirus best practices

While Global File Cache makes a reasonable effort to validate that the most common antivirus application suites are compatible with Global File Cache, NetApp cannot guarantee and is not responsible for any incompatibilities or performance issues caused by these programs, or their associated updates, service packs, or modifications.

Global File Cache does not recommend the installation nor application of monitoring or antivirus solutions on any Global File Cache enabled instance (Core or Edge). Should a solution be installed, by choice or by policy, the following best practices and recommendations must be applied. For common antivirus suites, see Appendix A in the [NetApp Global File Cache User Guide](#).

## Firewall settings

- Microsoft firewall:
  - Retain firewall settings as default.
  - Recommendation: Leave Microsoft firewall settings and services at the default setting of OFF, and not started for standard Global File Cache Edge instances.
  - Recommendation: Leave Microsoft firewall settings and services at the default setting of ON, and started for Edge instances that also run the Domain Controller role.
- Corporate firewall:
  - Global File Cache Core instance listens on TCP ports 6618-6630, ensure that Global File Cache Edge instances can connect to these TCP ports.
  - Global File Cache instances require communications to the Global File Cache Management Server on TCP port 443 (HTTPS).
- Network optimization solutions/devices must be configured to pass-thru Global File Cache specific ports.

## Antivirus best practices

This section helps you to understand the requirements when running antivirus software on a Windows Server instance running Global File Cache. Global File Cache has tested most commonly used antivirus products including Cylance, McAfee, Symantec, Sophos, Trend Micro, Kaspersky and Windows Defender for use in conjunction with Global File Cache.



Adding antivirus to an Edge appliance can introduce a 10–20% impact on user performance.

For more information, see the [NetApp Global File Cache User Guide](#).

### Configure exclusions

Antivirus software or other third-party indexing or scanning utilities should never scan drive D:\ on the Edge instance. These scans of Edge server drive D:\ will result in numerous file open requests for the entire cache namespace. This will result in file fetches over the WAN to all file servers being optimized at the data center. WAN connection flooding and unnecessary load on the Edge instance will occur resulting in performance degradation.

In addition to the D:\ drive, the following Global File Cache directory and processes should generally be excluded from all antivirus applications:

- C:\Program Files\TalonFAST\
- C:\Program Files\TalonFAST\Bin\LMClientService.exe
- C:\Program Files\TalonFAST\Bin\LMServerService.exe
- C:\Program Files\TalonFAST\Bin\Optimus.exe
- C:\Program Files\TalonFAST\Bin\tafsexport.exe
- C:\Program Files\TalonFAST\Bin\tafsutils.exe
- C:\Program Files\TalonFAST\Bin\tapp.exe
- C:\Program Files\TalonFAST\Bin\trfs.exe
- C:\Program Files\TalonFAST\Bin\TService.exe

- C:\Program Files\TalonFAST\Bin\tum.exe
- C:\Program Files\TalonFAST\FastDebugLogs\
- C:\Windows\System32\drivers\tfast.sys
- \\?\TafsMtPt:\ or \\?\TafsMtPt\*
- \Device\TalonCacheFS\
- \\?\GLOBALROOT\Device\TalonCacheFS\
- \\?\GLOBALROOT\Device\TalonCacheFS\\*

## **NetApp Support policy**

Global File Cache instances are designed specifically for Global File Cache as the primary application running on a Windows Server 2016 and 2019 platform. Global File Cache requires priority access to platform resources, for example, disk, memory, network interfaces, and can place high demands on these resources. Virtual deployments require memory/CPU reservations and high-performance disks.

- For branch office deployments of Global File Cache, supported services and applications on the server running Global File Cache are limited to:
  - DNS/DHCP
  - Active Directory domain controller (Global File Cache must be on a separate volume)
  - Print services
  - Microsoft System Center Configuration Manager (SCCM)
  - Global File Cache approved client-side system agents and anti-virus applications
- NetApp Support and maintenance applies only to Global File Cache.
- Line of business productivity software, which are typically resource intensive, for example, database servers, mail servers, and so on, are not supported.
- The customer is responsible for any non-Global File Cache software which might be installed on the server running Global File Cache:
  - If any third-party software package causes software or resource conflicts with Global File Cache or performance is compromised, Global File Cache's support organization might require the customer to disable or remove the software from the server running Global File Cache.
  - It is the customer's responsibility for all installation, integration, support, and upgrade of any software added to the server running the Global File Cache application.
- Systems management utilities/agents such as antivirus tools and licensing agents might be able to coexist. However, except for the supported services and applications listed above, these applications are not supported by Global File Cache and the same guidelines as above must still be followed:
  - It is the customer's responsibility for all installation, integration, support, and upgrade of any software added.
  - If a customer does install any third-party software package that causes, or is suspected to be causing, software or resource conflicts with Global File Cache or performance is compromised, there might be a requirement by Global File Cache's support organization to disable/remove the software.

# Deploy Global File Cache Edge instances

After you have verified that your environment meets all the requirements, you install Global File Cache Edge software in each remote office.

## Before you begin

To complete Global File Cache Edge configuration tasks, you need the following information:

- Static IP addresses for each Global File Cache instance
- Subnet mask
- Gateway IP address
- The FQDN you wish to assign to each Global File Cache server
- The DNS suffix (optional)
- The user name and password of an administrative user in the domain
- The FQDN and/or IP address of the associated Core servers
- A volume to be used as the Intelligent File Cache. It is recommended this be at least 2x the size of the active dataset. This should be formatted as NTFS and assigned as D:\.

## Commonly used TCP ports

There are several TCP ports used by Global File Cache services. It is mandatory that the devices can communicate on these ports and they be excluded from any WAN optimization devices or firewall restriction policies:

- Global File Cache Licensing TCP Port: 443
- Global File Cache TCP Ports: 6618-6630

## Deploy the Global File Cache Virtual Template

The virtual template (.OVA and .VHD) images contain the latest release of the Global File Cache software. If you are deploying Global File Cache using the .OVA or .VHD virtual machine (VM) template, follow the steps as outlined in this section. It is assumed that you understand how to deploy the .OVA or .VHD template on the designated hypervisor platform.

Ensure that VM preferences, including resource reservations, are in line with the requirements as outlined in [Virtual deployment requirements](#).

### Steps

1. Extract the package from the template you downloaded.
2. Deploy the virtual template. Refer to the following videos before you start the deployment:
  - [Deploy the Virtual Template on VMware](#)
  - [Deploy the Virtual Template on Hyper-V](#)
3. After the Virtual Template has been deployed, and you have configured the VM settings, start the VM.
4. During initial boot, when the Windows Server 2016 or 2019 operating system is preparing for first use, complete the out-of-the-box experience by installing the correct drivers and installing the necessary components for the respective hardware.

5. When the base install of the Global File Cache Edge instance has been completed, the Windows Server 2016 or 2019 operating system will guide you through an initial configuration wizard to configure operating system specifics such as localization and product key.
6. After the initial configuration wizard has completed, log in locally to the Windows Server 2016 or 2019 operating system with the following credentials:
  - User name: **FASTAdmin**
  - Password: **Tal0nFAST!**
7. Configure your Windows Server VM, join to the organization's Active Directory domain, and proceed to the Global File Cache Edge configuration section.

## Configure the Global File Cache Edge instance

The Global File Cache Edge instance connects to a Global File Cache Core to provide users at the branch office access to data center file server resources.



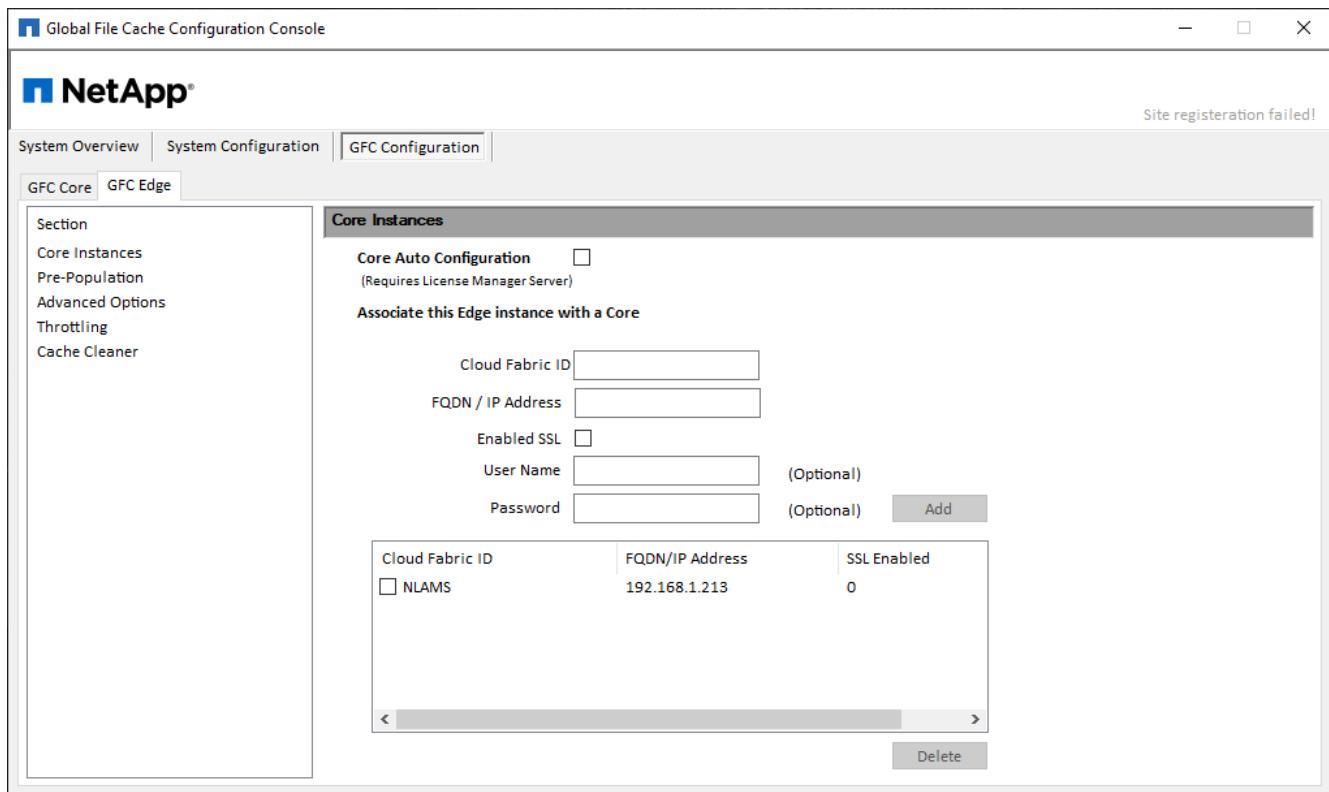
The Edge instance must be licensed as part of your Cloud Volumes ONTAP deployment prior to beginning the configuration. See [Licensing](#) for more information about licensing.

If your configuration requires more than one Global File Cache Core to be installed because of a large number of Edge instances, you will configure some Edge instances to connect to the first Core and others to connect to the second Core. Make sure you have the FQDN or IP address, and other required information, for the correct Core instance.

To configure the Edge instance, complete the following steps:

### Steps

1. Click **Perform** next to the unchecked Core Configuration step listed in the "Edge Configuration Steps" section of the Initial Configuration assistant. This opens a new tab, GFC Edge, and shows the section *Core Instances*.
2. Provide the **Cloud Fabric ID** of the Global File Cache Core server. The Cloud Fabric ID is typically the NetBIOS name or the geographical location of the backend file server.
3. Provide the **FQDN/IP Address** of the Global File Cache Core server:
  - a. (Optional) Check the **SSL** box to enable SSL support for enhanced encryption from the Edge to the Core.
  - b. Enter the User Name and Password, which are the credentials of the Service Account used on the Core.
4. Click **Add** to confirm the addition of the Global File Cache Core appliance. A confirmation box will appear. Click **OK** to dismiss it.



## Update Global File Cache Edge software

Global File Cache frequently releases updates to the software, either patches, enhancements, or new features/functionality. Although the virtual template (.OVA and .VHD) images contain the latest release of the Global File Cache software, it is possible that a newer version is available on the NetApp Support Download portal.

Ensure that your Global File Cache instances are up to date with the latest version.



This software package can also be used for pristine installations on Microsoft Windows Server 2016 Standard or Datacenter edition, or Windows Server 2019 Standard or Datacenter edition, or used as part of your upgrade strategy.

Below you can find the steps required to update the Global File Cache installation package:

### Steps

1. After saving the latest installation package to the desired Windows Server instance, double-click it to run the installation executable.
2. Click **Next** to continue the process.
3. Click **Next** to continue.
4. Accept the Licensing Agreement and click **Next**.
5. Select the desired Installation Destination Location.

NetApp recommends that the default installation location be used.

6. Click **Next** to continue.
7. Select the Start Menu Folder.

8. Click **Next** to continue.
9. Verify the desired installation parameters and click **Install** to begin the installation.

The installation process will execute.
10. After the installation has completed, reboot the server when prompted.

#### What's Next?

For details about Global File Cache Edge advanced configuration, see the [NetApp Global File Cache User Guide](#).

## End-user training

You will want to train your users on the best practices for accessing the shared files through Global File Cache.

This is the final phase of the Global File Cache deployment, the end-user implementation phase.

In order to prepare and streamline the end user on-boarding process, use the email template below that will help you to educate end users on what it means to work in a "central data" environment. This will help your users leverage all of the benefits of the Global File Cache solution. We have also published a video that can be shared to "train" users where needed.

Customize and forward the following resources to end users to prepare them for roll-out:

- User Training video  
[End user training video](#)
- Email Template  
[Mac Email Template \(.emltpl\)](#)  
  
[Windows Email Template \(.msg\)](#)
- Onboarding Communications  
[Word Document \(.docx\)](#)

See Chapter 12 in the [NetApp Global File Cache User Guide](#) for additional material.

## Additional information

Use the following links to learn more about Global File Cache and other NetApp products:

- Global File Cache FAQ
  - See a list of frequently asked questions and answers [here](#)
- [NetApp Global File Cache User Guide](#)
- NetApp Product Documentation
  - See additional documentation for NetApp cloud products [here](#)
  - See additional documentation for all NetApp products [here](#)
- Customer support for Global File Cache users with Cloud Volumes ONTAP is available through these channels:

- Guided Problem Solving, Case Management, Knowledgebase, Downloads, Tools, and more go [here](#)
- Login to the NetApp Support at <https://mysupport.netapp.com> with your NSS credentials
- For immediate assistance for a P1 issue call: +1 856.481.3990 (Option 2)
- Customer support for Global File Cache users utilizing Cloud Volumes Services and Azure NetApp Files is available through standard support from your provider. Please contact Google Customer Support or Microsoft Customer Support respectively.

# Optimize cloud compute costs

## Learn about the Compute service

By leveraging [Spot's Cloud Analyzer service](#), Cloud Manager can provide a high-level cost analysis of your cloud compute spending and identify potential savings.

Cloud Analyzer is a cloud infrastructure management solution that uses advanced analytics to provide visibility and insights into your cloud costs. It shows you where you can optimize those costs and lets you implement that optimization using Spot's portfolio of continuous optimization products in just a few clicks.

## Features

- A cost analysis that shows current cost for the month, projected monthly costs, and missed savings
- A view of spend efficiency by account, including the estimated additional savings
- A link to Spot's Cloud Analyzer for more in-depth details about the spending for all accounts

## Supported cloud providers

This service is supported with AWS.

## Cost

There's no cost to use this service through Cloud Manager.

## How Cloud Analyzer works with Cloud Manager

At a high-level, Cloud Analyzer integration with Cloud Manager works like this:

1. You click **Compute** and connect your AWS master payer account.
2. NetApp configures your environment as follows:
  - a. Creates an organization in the Spot platform.
  - b. Sends an email welcoming you to Spot.

You can log in to the Spot service using the same single-sign on credentials that you use with Cloud Central and Cloud Manager.

- c. Cloud Analyzer starts processing your AWS account data.
3. In Cloud Manager, the Compute page refreshes and you use the information to gain insights on past, current, and future cloud costs.
  4. You click **Get Full Analysis** at any time to go to Spot's Cloud Analyzer, which provides a full analysis of your cloud spend and savings opportunities.

## Data security

Cloud Analyzer data is encrypted at rest and no credentials are stored for any account.

# Start optimizing your cloud compute costs

Connect your AWS account and then view the analysis to start optimizing your cloud compute costs.

## Connect Cloud Analyzer to your AWS account

Click **Compute** and connect your AWS payer account.

### Steps

1. Click **Compute**.
2. Click **Add AWS Credentials to Start**.
3. Follow the steps on the page to connect your AWS account:
  - a. Log in to your AWS master payer account.
  - b. Set up cost and usage reports on the AWS account.
  - c. Run the CloudFormation template.
  - d. Paste the Spot RoleARN.

[View more details about these steps.](#)

### Connect your AWS Account to Optimize Costs

Connecting your billing data will allow Cloud Analyzer to access your Cost and Usage data.

**Step 1**

Log in to your AWS Master Payer account. [Log in](#)

**Step 2**

Set up your Cost and Usage Reports on your AWS account.  
[\(Learn How\)](#) or skip this if the report is already enabled.)

Enter the bucket name where the report is located: Bucket name  
123456789

**Step 3**

Open CloudFormation with Spot template. [Run Template](#)

Under capabilities, mark "I acknowledge that AWS CloudFormation might create IAM resources" and click 'Create'.

**Step 4**

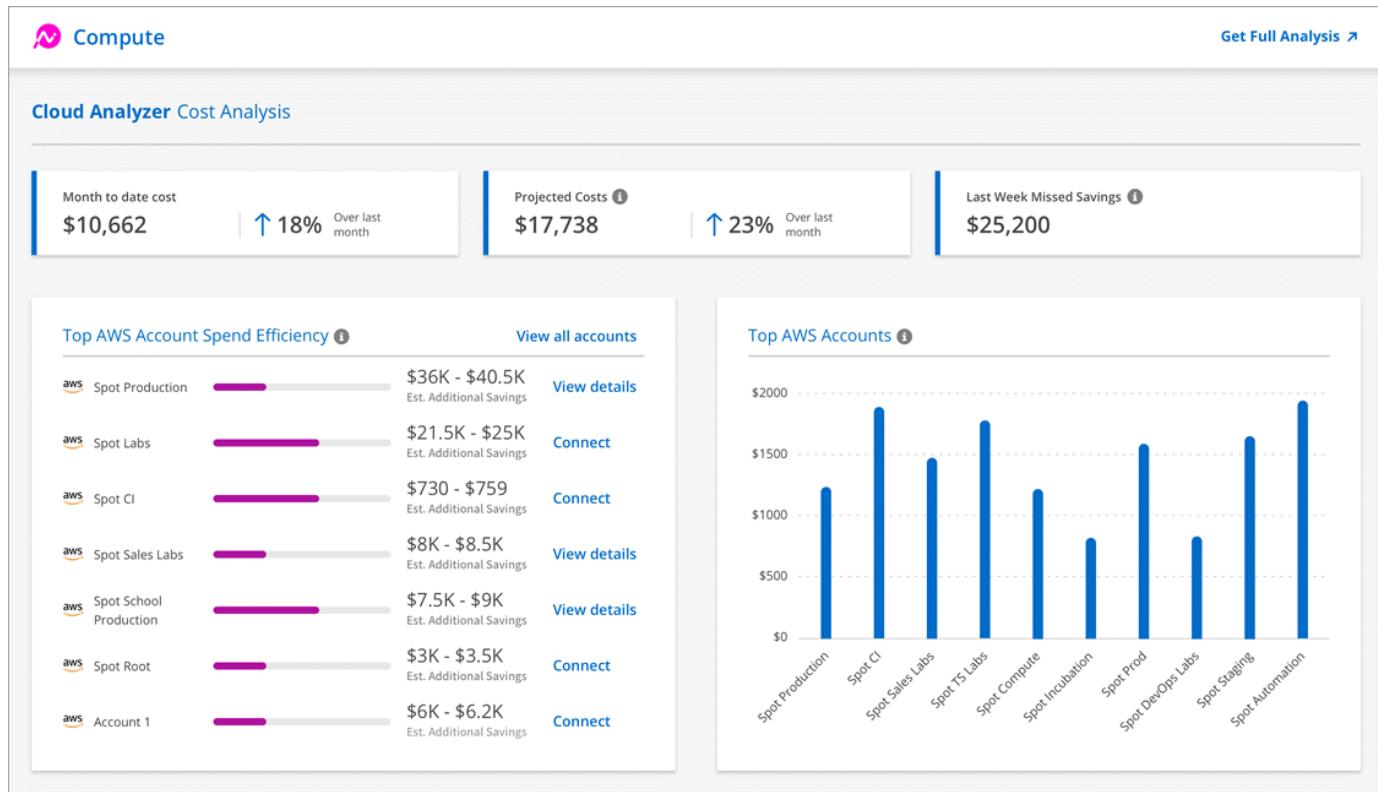
Copy the Spot RoleARN from the Output tab and paste below. Spot RoleARN  
arn:aws:iam:123412341234:role/test123

## Result

Cloud Analyzer starts processing your AWS account data. If you have multiple accounts, Cloud Analyzer starts with read-only capabilities for all linked accounts under the master payer account. If you want to get more details about the potential savings for those accounts, then you'll need to connect them, as well. You can find more details about that process in the section below.

## Analyze your compute costs

After Cloud Analyzer processes your account data, the Compute tab shows you insights on past, current, and future cloud costs.



### Month to date cost

The total cost of your workloads from the beginning of the current month to present.

### Projected Costs

The forecasted cost at the end of the month based on analysis of your usage pattern.

### Last Week Missed Savings

Savings that could have been achieved in the previous seven days using optimization of spot instances and reservations.

### Top AWS Account Spend Efficiency

The top 10 accounts according to the greatest amount of estimated additional savings.

Each account is assigned an efficiency score based on current and additional potential savings. The estimated additional savings indicates how much can be further saved by leveraging the use of spot and reserved instances.

You can take the following actions to further optimize your accounts:

- **View details:** View your cost optimization opportunities by going to Spot's Cloud Analyzer.
- **Connect:** Connect an account that is not yet managed. You will be directed to the wizard that connects the account.

## Top AWS Accounts

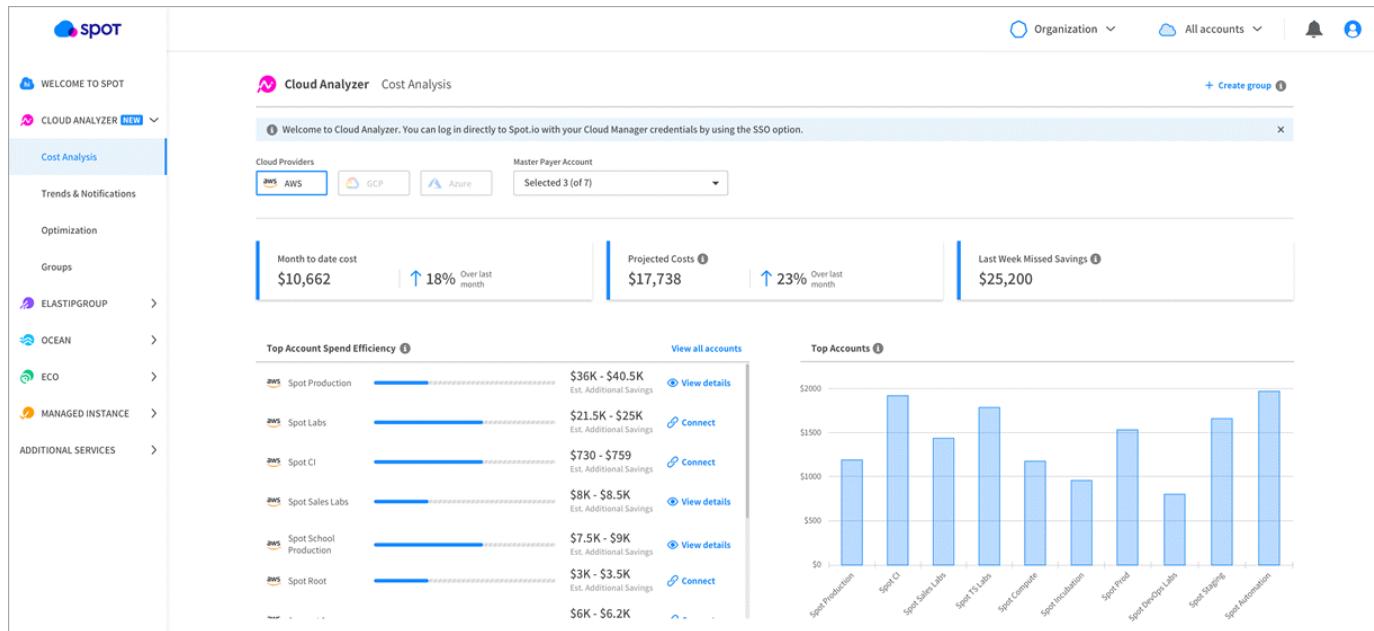
This is a bar graph showing your top ten accounts by cost. The graph is based on the last 30 days of spend activity.

[Learn more about the Cost Analysis page that's available in Spot's Cloud Analyzer.](#)

## Go to Cloud Analyzer for more analysis and recommendations

Click **Get Full Analysis** at any time to access more charts and analysis, in-depth recommendations, a use case optimization breakdown (containers, ElasticApps, and reservations), and more.

Here's an example of what you'll see in Cloud Analyzer:



- [View the product page for Cloud Analyzer to learn more about its capabilities.](#)
- [View the documentation for Spot to get help using Cloud Analyzer.](#)

# Tier data to the cloud

## Learn about Cloud Tiering

NetApp's Cloud Tiering service extends your data center to the cloud by automatically tiering inactive data from on-premises ONTAP clusters to object storage. This frees valuable space on the cluster for more workloads, without making changes to the application layer. Cloud Tiering can reduce costs in your data center and enables a switch from a CAPEX model to an OPEX model.

The Cloud Tiering service leverages the capabilities of *FabricPool*. FabricPool is a NetApp Data Fabric technology that enables automated tiering of data to low-cost object storage. Active data remains on high-performance SSDs, while inactive data is tiered to low-cost object storage while preserving ONTAP data efficiencies.

## Features

Cloud Tiering offers automation, monitoring, reports, and a common management interface:

- Automation makes it easier to set up and manage data tiering from on-prem ONTAP clusters to the cloud
- A single pane of glass removes the need to independently manage FabricPool across several clusters
- Reports show the amount of active and inactive data on each cluster
- A tiering health status helps you identify and correct issues as they occur
- If you have Cloud Volumes ONTAP systems, you'll find them in the Cluster Dashboard so you get a full view of data tiering in your hybrid cloud infrastructure



Cloud Volumes ONTAP systems are read-only from Cloud Tiering. You set up tiering for Cloud Volumes ONTAP from the working environment in Cloud Manager.

For more details about the value that Cloud Tiering provides, [check out the Cloud Tiering page on NetApp Cloud Central](#).



While Cloud Tiering can significantly reduce storage footprints, it is not a backup solution.

## Supported object storage providers

You can tier inactive data from an ONTAP cluster to Amazon S3, Microsoft Azure Blob storage, Google Cloud Storage, or StorageGRID (private cloud).

## Pricing and licenses

Pay for Cloud Tiering through a pay-as-you-go subscription, an ONTAP tiering license called *FabricPool*, or a combination of both. A 30-day free trial is available for your first cluster if you don't have a license.

There are no charges when tiering data to StorageGRID. Neither a BYOL license or PAYGO registration is required.

[View pricing details.](#)

## **30-day free trial**

If you don't have a FabricPool license, a 30-day free trial of Cloud Tiering starts when you set up tiering to your first cluster. After that 30-day free trial ends, you'll need to pay for Cloud Tiering through a pay-as-you-go subscription, a FabricPool license, or a combination of both.

If your free trial ends and you haven't subscribed or added a license, then ONTAP no longer tiers cold data to object storage, but existing data is still available for access.

## **Pay-as-you-go subscription**

Cloud Tiering offers consumption-based licensing in a pay-as-you-go model. After subscribing through your cloud provider's marketplace, you pay per GB for data that's tiered—there's no up-front payment. You are billed by your cloud provider through your monthly bill.

You should subscribe even if you have a free trial or if you bring your own license (BYOL):

- Subscribing ensures that there's no disruption of service after your free trial ends.

When the trial ends, you'll be charged hourly according to the amount of data that you tier.

- If you tier more data than allowed by your FabricPool license, then data tiering continues through your pay-as-you-go subscription.

For example, if you have a 10 TB license, all capacity beyond the 10 TB is charged through the pay-as-you-go subscription.

You won't be charged from your pay-as-you-go subscription during your free trial or if you haven't exceeded your FabricPool license.

[Learn how to set up a pay-as-you-go subscription.](#)

## **Bring your own license**

Bring your own license by purchasing an ONTAP FabricPool license from NetApp. You can purchase term-based or perpetual licenses.

After you purchase a FabricPool license, you'll need to add it to the cluster, [which you can do directly from Cloud Tiering](#).

After you activate the license through Cloud Tiering, if you purchase additional add-on capacity at a later time, the license on the cluster is automatically updated with the new capacity. There's no need to apply a new NetApp License File (NLF) to the cluster.

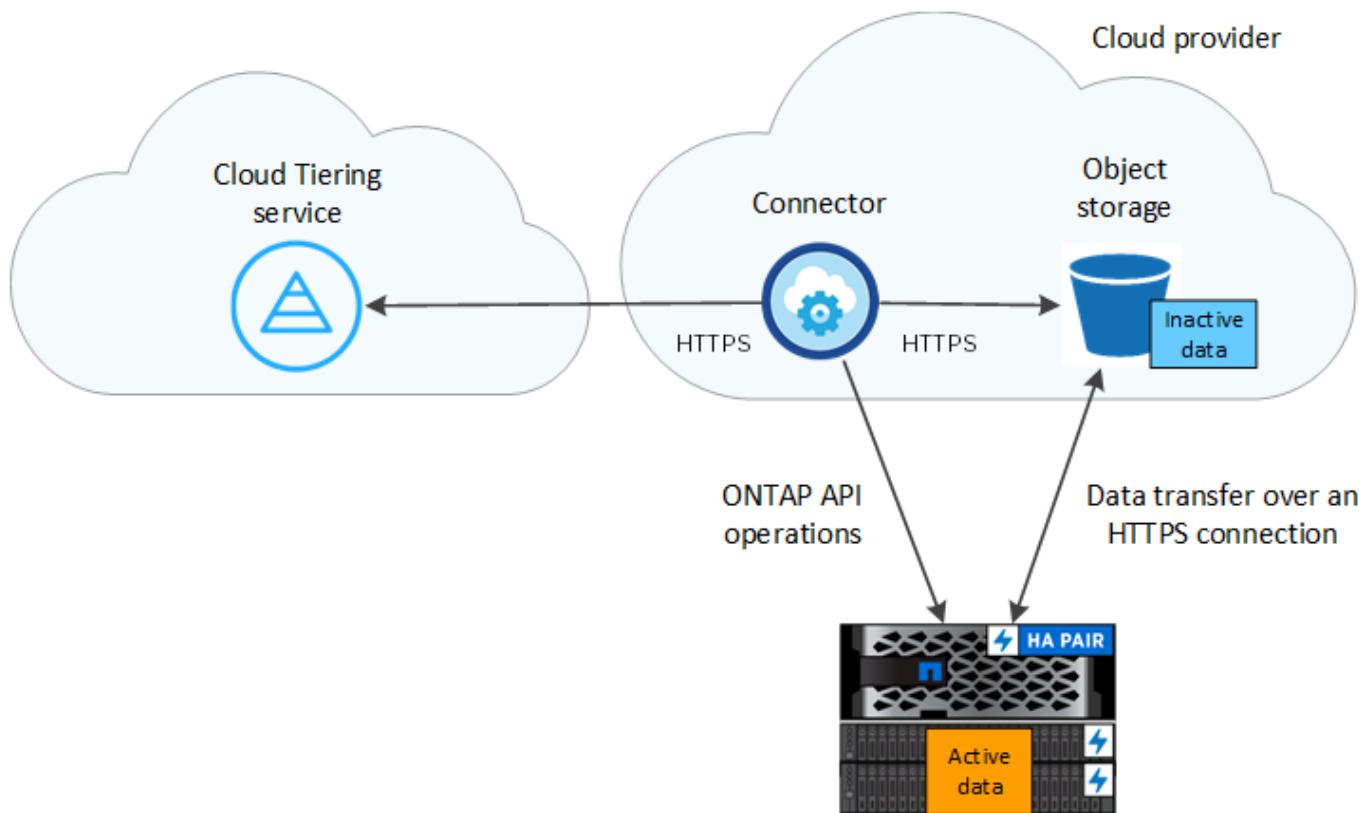
As noted above, we recommend that you set up a pay-as-you-go subscription, even if your cluster has a BYOL license.

[Contact us to purchase a license.](#)

## **How Cloud Tiering works**

Cloud Tiering is a NetApp-managed service that uses FabricPool technology to automatically tier inactive (cold) data from your on-premises ONTAP clusters to object storage in your public cloud or private cloud. Connections to ONTAP take place from a Connector.

The following image shows the relationship between each component:



At a high level, Cloud Tiering works like this:

1. You discover your on-prem cluster from Cloud Manager.
2. You set up tiering by providing details about your object storage, including the bucket/container and a storage class or access tier.
3. Cloud Manager configures ONTAP to use the object storage provider and discovers the amount of active and inactive data on the cluster.
4. You choose the volumes to tier and the tiering policy to apply to those volumes.
5. ONTAP starts tiering inactive data to the object store, as soon as the data has reached the thresholds to be considered inactive (see [Volume tiering policies](#)).

## Object storage

Each ONTAP cluster tiers inactive data to a single object store. When you set up data tiering, you have the choice to add a new bucket/container or to select an existing bucket/container, along with a storage class or access tier.

- [Learn about supported S3 storage classes](#)
- [Learn about supported Azure Blob access tiers](#)
- [Learn about supported Google Cloud storage classes](#)

## Volume tiering policies

When you select the volumes that you want to tier, you choose a *volume tiering policy* to apply to each volume. A tiering policy determines when or whether the user data blocks of a volume are moved to the cloud.

## No tiering policy

Keeps the data on a volume in the performance tier, preventing it from being moved to the cloud.

## Cold snapshots (Snapshot only)

ONTAP tiers cold Snapshot blocks in the volume that are not shared with the active file system to object storage. If read, cold data blocks on the cloud tier become hot and are moved to the performance tier.

Data is tiered only after an aggregate has reached 50% capacity and when the data has reached the cooling period. The default number of cooling days is 2, but you can adjust the number of days.



Writes from the cloud tier to the performance tier are disabled if performance tier capacity is greater than 70%. If this occurs, blocks are accessed directly from the cloud tier.

## Cold user data (Auto)

ONTAP tiers all cold blocks in the volume (not including metadata) to object storage. The cold data includes not just Snapshot copies but also cold user data from the active file system.

If read by random reads, cold data blocks on the cloud tier become hot and are moved to the performance tier. If read by sequential reads, such as those associated with index and antivirus scans, cold data blocks on the cloud tier stay cold and are not written to the performance tier.

Data is tiered only after an aggregate has reached 50% capacity and when the data has reached the cooling period. The cooling period is the time that user data in a volume must remain inactive for the data to be considered "cold" and moved to the object store. The default number of cooling days is 31, but you can adjust the number of days.



Writes from the cloud tier to the performance tier are disabled if performance tier capacity is greater than 70%. If this occurs, blocks are accessed directly from the cloud tier.

## All user data (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.

Take the following into consideration before you choose this tiering policy:

- Tiering data immediately reduces storage efficiencies (inline only).
- You should use this policy only if you are confident that cold data on the volume will not change.
- Object storage is not transactional and will result in significant fragmentation if subjected to change.
- Consider the impact of SnapMirror transfers before assigning the All tiering policy to source volumes in data protection relationships.

Because data is tiered immediately, SnapMirror will read data from the cloud tier rather than the performance tier. This will result in slower SnapMirror operations—possibly slowing other SnapMirror operations later in queue—even if they are using different tiering policies.

## All DP user data (Backup)

All data on a data protection volume (not including metadata) is immediately moved to the cloud tier. If read, cold data blocks on the cloud tier stay cold and are not written back to the performance tier (starting with ONTAP 9.4).



This policy is available for ONTAP 9.5 or earlier. It was replaced with the **All** tiering policy starting with ONTAP 9.6.

# Get started

## Tiering data from on-premises ONTAP clusters to Amazon S3

Free space on your on-prem ONTAP clusters by tiering data to Amazon S3. Data tiering is powered by NetApp's Cloud Tiering service.

### Quick start

Get started quickly by following these steps or scroll down to the remaining sections for full details.

1

### Prepare to tier data to Amazon S3

You need the following:

- An AFF or FAS system with all-SSD aggregates that's running ONTAP 9.2 or later and has an HTTPS connection to Amazon S3. [Learn how to discover a cluster](#).
- An AWS account that has an access key and [the required permissions](#) so the ONTAP cluster can tier inactive data in and out of S3.
- A Connector installed in an AWS VPC or on your premises.
- Networking for the Connector that enables an outbound HTTPS connection to the ONTAP cluster, to S3 storage, and to the Cloud Tiering service.

2

### Set up tiering

In Cloud Manager, select an on-prem working environment, click **Setup Tiering** and follow the prompts to tier data to Amazon S3.

3

### Set up licensing

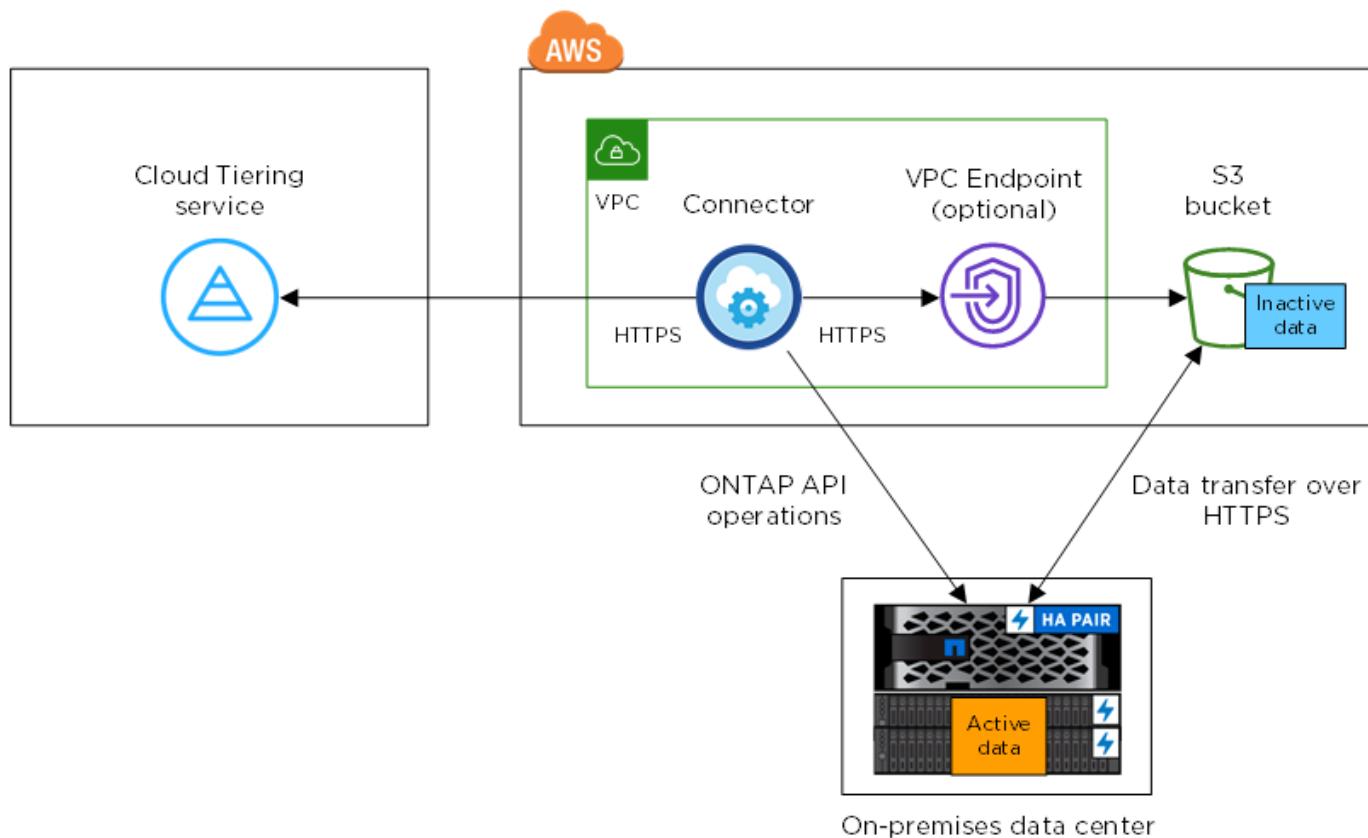
After your free trial ends, pay for Cloud Tiering through a pay-as-you-go subscription, an ONTAP tiering license, or a combination of both:

- To subscribe from the AWS Marketplace, click **Tiering > Licensing**, click **Subscribe**, and then follow the prompts.
- To pay using a tiering license, [contact us if you need to purchase one](#), and then [add it to your cluster from Cloud Tiering](#).

## Requirements

Verify support for your ONTAP cluster, set up your networking, and prepare your object storage.

The following image shows each component and the connections that you need to prepare between them:



Communication between a Connector and S3 is for object storage setup only. The Connector can reside on your premises, instead of in the cloud.

### Preparing your ONTAP clusters

Your ONTAP clusters must meet the following requirements when tiering data to Amazon S3.

#### Supported ONTAP platforms

Cloud Tiering supports AFF systems and all-SSD aggregates on FAS systems.

#### Supported ONTAP version

ONTAP 9.2 or later

#### Cluster networking requirements

- The ONTAP cluster initiates an HTTPS connection over port 443 to Amazon S3.

ONTAP reads and writes data to and from object storage. The object storage never initiates, it just responds.

Although AWS Direct Connect provides better performance and lower data transfer charges, it's not required between the ONTAP cluster and S3. Because performance is significantly better when using AWS Direct Connect, doing so is the recommended best practice.

- An inbound connection is required from the Connector, which can reside in an AWS VPC or on your premises.

A connection between the cluster and the Cloud Tiering service is not required.

- An intercluster LIF is required on each ONTAP node that hosts tiered volumes. The LIF must be associated with the *IPspace* that ONTAP should use to connect to object storage.

IPspaces enable network traffic segregation, allowing for separation of client traffic for privacy and security. [Learn more about IPspaces](#).

When you set up data tiering, Cloud Tiering prompts you for the IPspace to use. You should choose the IPspace that each LIF is associated with. That might be the "Default" IPspace or a custom IPspace that you created.

## Supported volumes and aggregates

The total number of volumes that Cloud Tiering can tier might be less than the number of volumes on your ONTAP system. That's because volumes can't be tiered from some aggregates. For example, you can't tier data from SnapLock volumes or from MetroCluster configurations. Refer to ONTAP documentation for [functionality or features not supported by FabricPool](#).



Cloud Tiering supports FlexGroup volumes, starting with ONTAP 9.5. Setup works the same as any other volume.

## Discovering an ONTAP cluster

You need to create an on-prem ONTAP working environment in Cloud Manager before you can start tiering cold data.

[Learn how to discover a cluster.](#)

## Creating or switching Connectors

A Connector is required to tier data to the cloud. When tiering data to AWS S3, you can use a Connector that's in an AWS VPC or on your premises. You'll either need to create a new Connector or make sure that the currently selected Connector resides in AWS or on-prem.

- [Learn about Connectors](#)
- [Creating a Connector in AWS](#)
- [Connector host requirements](#)
- [Installing the Connector on an existing Linux host](#)
- [Switching between Connectors](#)

## Preparing networking for the Connector

Ensure that the Connector has the required networking connections. A Connector can be installed on-prem or in AWS.

## Steps

1. Ensure that the network where the Connector is installed enables the following connections:
  - An outbound internet connection to the Cloud Tiering service over port 443 (HTTPS)

- An HTTPS connection over port 443 to S3
  - An HTTPS connection over port 443 to your ONTAP clusters
2. If needed, enable a VPC Endpoint to S3.

A VPC Endpoint to S3 is recommended if you have a Direct Connect or VPN connection from your ONTAP cluster to the VPC and you want communication between the Connector and S3 to stay in your AWS internal network.

### Preparing Amazon S3

When you set up data tiering to a new cluster, you're prompted to create an S3 bucket or to select an existing S3 bucket in the AWS account where the Connector is set up.

The AWS account must have permissions and an access key that you can enter in Cloud Tiering. The ONTAP cluster uses the access key to tier data in and out of S3.

### Steps

1. Provide the following permissions to the IAM user:

```
"s3>ListAllMyBuckets",
"s3>ListBucket",
"s3:GetBucketLocation",
"s3GetObject",
"s3PutObject",
"s3DeleteObject"
```

[AWS Documentation: Creating a Role to Delegate Permissions to an IAM User](#)

2. Create or locate an access key.

Cloud Tiering passes the access key on to the ONTAP cluster. The credentials are not stored in the Cloud Tiering service.

[AWS Documentation: Managing Access Keys for IAM Users](#)

### Tiering inactive data from your first cluster to Amazon S3

After you prepare your AWS environment, start tiering inactive data from your first cluster.

#### What you'll need

- [An on-premises working environment.](#)
- An AWS access key for an IAM user who has the required S3 permissions.

### Steps

1. Select an on-prem cluster.
2. Click **Enable**.

The screenshot shows the 'OnPrem1' configuration page. At the top, 'OnPrem1' is listed with a status of 'On'. Below this, there is a section titled 'SERVICES' containing five items:

- Replication**: Status 'Off', with an 'Enable' button.
- Backup & Compliance**: Status 'Unavailable' with an information icon.
- Restore**: Status 'Off', with an 'Enable' button.
- Compliance**: Status 'Off', with an 'Enable' button.
- Tiering**: Status 'Off', with an 'Enable' button.

A red arrow points to the 'Enable' button for the 'Tiering' service.

3. Complete the steps on the **Tiering Setup** page:

- a. **S3 Bucket**: Add a new S3 bucket or select an existing S3 bucket that starts with the prefix *fabric-pool* and click **Continue**.

The *fabric-pool* prefix is required because the IAM policy for the Connector enables the instance to perform S3 actions on buckets named with that exact prefix.

For example, you could name the S3 bucket fabric-pool-AFF1, where AFF1 is the name of the cluster.

- b. **Storage Class**: Select the S3 storage class that you want to transition the data to after 30 days.

If you choose Standard, then the data remains in that storage class.

- c. **Credentials**: Enter the access key ID and secret key for an IAM user who has the required S3 permissions.

The IAM user must be in the same AWS account as the bucket that you selected or created on the **S3 Bucket** page.

- d. **Cluster Network**: Select the IPspace that ONTAP should use to connect to object storage.

Selecting the correct IPspace ensures that Cloud Tiering can set up a connection from ONTAP to your

cloud provider's object storage.

4. Click **Continue** to select the volumes that you want to tier.
5. On the **Tier Volumes** page, set up tiering for each volume.

[Learn more about volume tiering policies.](#)

- To select a tiering policy for just one volume, click the  icon, select a tiering policy, and optionally adjust the cooling days.

3 Volumes 									
Volume Name	SVM Name	Volume Size	Used Size	Snapshot Used Size	Cold Data	Tier Status	Tiering Policy	Actions	
<input type="checkbox"/> vol1	svm_AFF1	50 GB	5.21 MB	864 KB	3.65 MB	70 %	 Tiered Volume	All user data	
<input type="checkbox"/> vol2	svm_AFF1	200 GB	4.11 MB	424 KB	2.88 MB	70 %	 Tiered Volume	Cold snapshots	
<input type="checkbox"/> vol3	svm_AFF1	200 GB	3.96 MB	424 KB	2.77 MB	70 %	 Tiered Volume	Cold snapshots	

- To select a tiering policy for several volumes, select multiple volumes, click **Modify selected volumes**, select a tiering policy, and optionally adjust the cooling days.

3 Volumes    2 selected  Modify selected volumes 									
Volume Name	SVM Name	Volume Size	Used Size	Snapshot Used Size	Cold Data	Tier Status	Tiering Policy	Actions	
<input type="checkbox"/> vol1	svm_AFF1	50 GB	3.54 MB	444 KB	2.47 MB	70 %	 Tiered Volume	All user data	
<input checked="" type="checkbox"/> vol2	svm_AFF1	200 GB	1 MB	0 B	716.8 KB	70 %	 Tiered Volume	Cold snapshots	
<input checked="" type="checkbox"/> vol3	svm_AFF1	200 GB	1 MB	0 B	716.8 KB	70 %	 Tiered Volume	Cold snapshots	

## Result

You've successfully set up data tiering from volumes on the cluster to S3 object storage.

## What's next?

[Be sure to subscribe from the Cloud Tiering service.](#)

You can also add additional clusters or review information about the active and inactive data on the cluster. For details, see [Managing data tiering from your clusters](#).

## Tiering data from on-premises ONTAP clusters to Azure Blob storage

Free space on your on-prem ONTAP clusters by tiering data to Azure Blob storage. Data tiering is powered by NetApp's Cloud Tiering service.

## Quick start

Get started quickly by following these steps or scroll down to the remaining sections for full details.

# 1

## Prepare to tier data to Azure Blob storage

You need the following:

- An AFF or FAS system with all-SSD aggregates that's running ONTAP 9.4 or later and has an HTTPS connection to Azure Blob storage. [Learn how to discover a cluster](#).
- A Connector installed in an Azure VNet.
- Networking for a Connector that enables an outbound HTTPS connection to the ONTAP cluster in your data center, to Azure Blob storage, and to the Cloud Tiering service.

# 2

## Set up tiering

In Cloud Manager, select an on-prem working environment, click **Setup Tiering** and follow the prompts to tier data to Azure Blob storage.

# 3

## Set up licensing

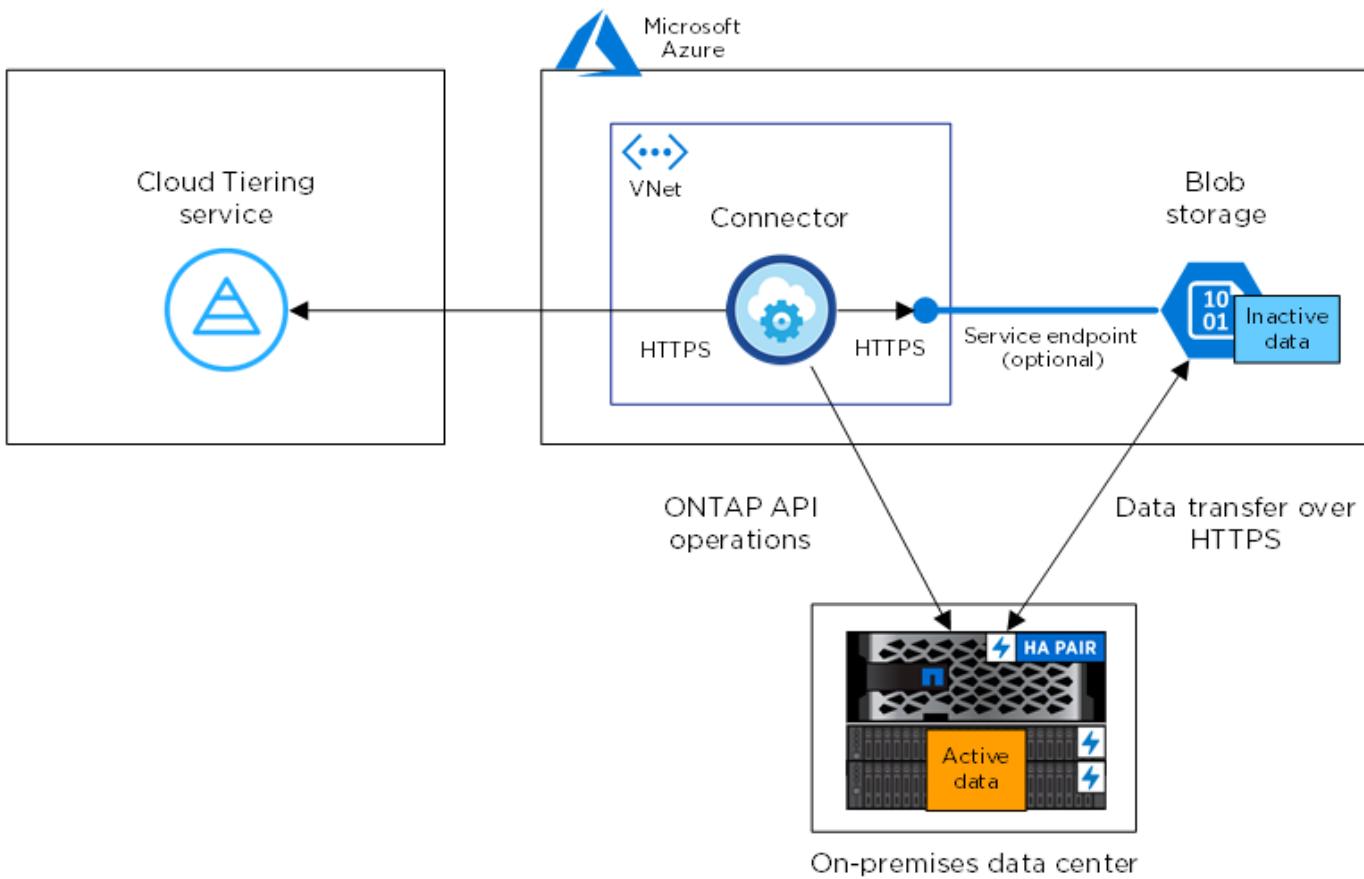
After your free trial ends, pay for Cloud Tiering through a pay-as-you-go subscription, an ONTAP tiering license, or a combination of both:

- To subscribe from the Azure Marketplace, click **Tiering > Licensing**, click **Subscribe**, and then follow the prompts.
- To add a tiering license, [contact us if you need to purchase one](#), and then [add it to your cluster from Cloud Tiering](#).

## Requirements

Verify support for your ONTAP cluster, set up your networking, and prepare your object storage.

The following image shows each component and the connections that you need to prepare between them:



Communication between the Connector and Blob storage is for object storage setup only.

#### Preparing your ONTAP clusters

Your ONTAP clusters must meet the following requirements when tiering data to Azure Blob storage.

#### Supported ONTAP platforms

Cloud Tiering supports AFF systems and all-SSD aggregates on FAS systems.

#### Supported ONTAP version

ONTAP 9.4 or later

#### Cluster networking requirements

- The ONTAP cluster initiates an HTTPS connection over port 443 to Azure Blob storage.

ONTAP reads and writes data to and from object storage. The object storage never initiates, it just responds.

Although ExpressRoute provides better performance and lower data transfer charges, it's not required between the ONTAP cluster and Azure Blob storage. Because performance is significantly better when using ExpressRoute, doing so is the recommended best practice.

- An inbound connection is required from the NetApp Service Connector, which resides in an Azure VNet.

A connection between the cluster and the Cloud Tiering service is not required.

- An intercluster LIF is required on each ONTAP node that hosts tiered volumes. The LIF must be

associated with the *IPspace* that ONTAP should use to connect to object storage.

IPspaces enable network traffic segregation, allowing for separation of client traffic for privacy and security. [Learn more about IPspaces](#).

When you set up data tiering, Cloud Tiering prompts you for the IPspace to use. You should choose the IPspace that each LIF is associated with. That might be the "Default" IPspace or a custom IPspace that you created.

## Supported volumes and aggregates

The total number of volumes that Cloud Tiering can tier might be less than the number of volumes on your ONTAP system. That's because volumes can't be tiered from some aggregates. For example, you can't tier data from SnapLock volumes or from MetroCluster configurations. Refer to ONTAP documentation for [functionality or features not supported by FabricPool](#).



Cloud Tiering supports FlexGroup volumes, starting with ONTAP 9.5. Setup works the same as any other volume.

## Discovering an ONTAP cluster

You need to create an on-prem ONTAP working environment in Cloud Manager before you can start tiering cold data.

[Learn how to discover a cluster](#).

## Creating or switching Connectors

A Connector is required to tier data to the cloud. When tiering data to Azure Blob storage, a Connector must be available in an Azure VNet. You'll either need to create a new Connector or make sure that the currently selected Connector resides in Azure.

- [Learn about Connectors](#)
- [Creating a Connector in Azure](#)
- [Switching between Connectors](#)

## Preparing networking for the Connector

Ensure that the Connector has the required networking connections.

## Steps

1. Ensure that the VNet where the Connector is installed enables the following connections:
  - An outbound internet connection to the Cloud Tiering service over port 443 (HTTPS)
  - An HTTPS connection over port 443 to Azure Blob storage
  - An HTTPS connection over port 443 to your ONTAP clusters
2. If needed, enable a VNet service endpoint to Azure storage.

A VNet service endpoint to Azure storage is recommended if you have an ExpressRoute or VPN connection from your ONTAP cluster to the VNet and you want communication between the Connector and Blob storage to stay in your virtual private network.

## Tiering inactive data from your first cluster to Azure Blob storage

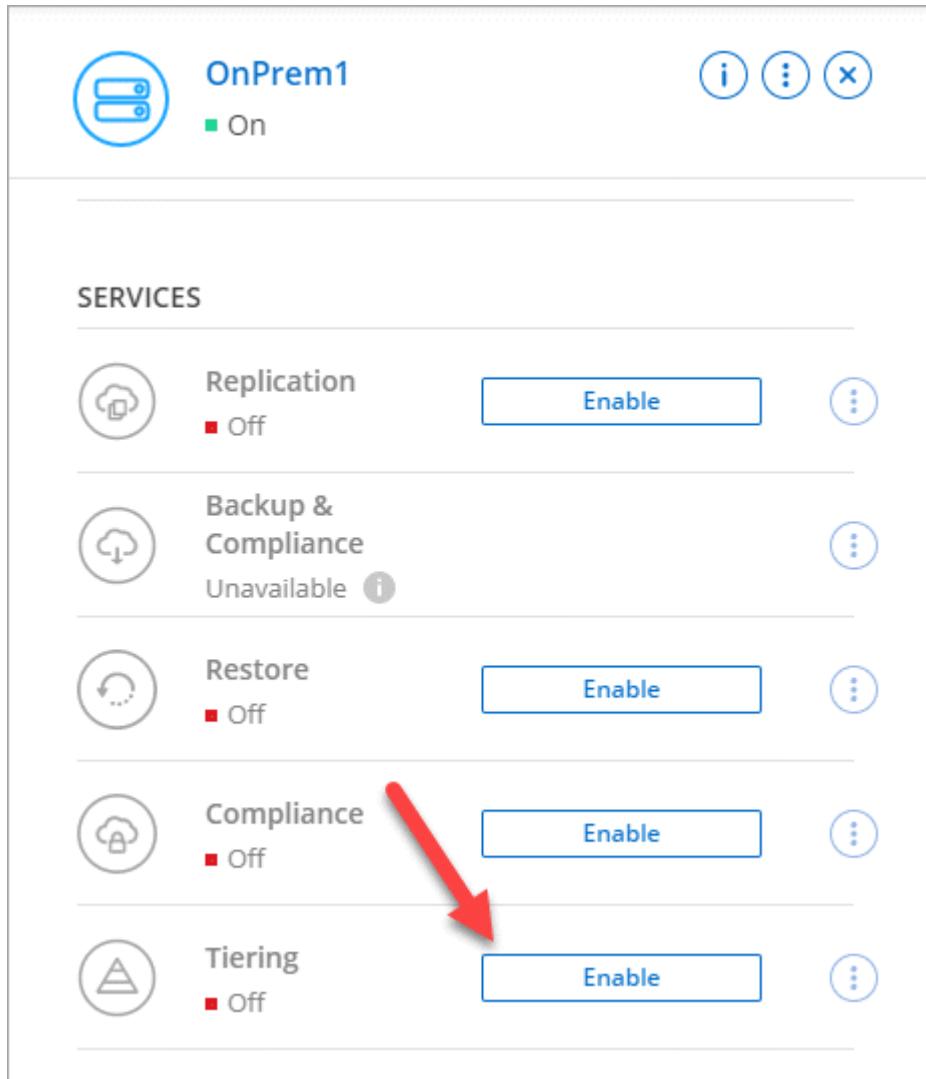
After you prepare your Azure environment, start tiering inactive data from your first cluster.

### What you'll need

An on-premises working environment.

### Steps

1. Select an on-prem cluster.
2. Click **Enable**.



3. Complete the steps on the **Tiering Setup** page:

- a. **Resource Group:** Select a resource group where an existing container is managed, or where you would like to create a new container for tiered data.
- b. **Azure Container:** Add a new Blob container to a storage account or select an existing container.

The storage account and containers that appear in this step belong to the resource group that you selected in the previous step.

- c. **Access Tier:** Select the access tier that you want to use for the tiered data.

d. **Cluster Network:** Select the IPspace that ONTAP should use to connect to object storage.

Selecting the correct IPspace ensures that Cloud Tiering can set up a connection from ONTAP to your cloud provider's object storage.

4. Click **Continue** to select the volumes that you want to tier.
5. On the **Tier Volumes** page, set up tiering for each volume.

[Learn more about volume tiering policies.](#)

- To select a tiering policy for just one volume, click the  icon, select a tiering policy, and optionally adjust the cooling days.

3 Volumes 								
Volume Name	SVM Name	Volume Size	Used Size	Snapshot Used Size	Cold Data	Tier Status	Tiering Policy	Action
<input type="checkbox"/> vol1	svm_AFF1	50 GB	5.21 MB	864 KB	3.65 MB	70 %	 Tiered Volume	All user data
<input type="checkbox"/> vol2	svm_AFF1	200 GB	4.11 MB	424 KB	2.88 MB	70 %	 Tiered Volume	Cold snapshots 
<input type="checkbox"/> vol3	svm_AFF1	200 GB	3.96 MB	424 KB	2.77 MB	70 %	 Tiered Volume	Cold snapshots 

- To select a tiering policy for several volumes, select multiple volumes, click **Modify selected volumes**, select a tiering policy, and optionally adjust the cooling days.

3 Volumes    2 selected <span>Modify selected volumes</span> 								
Volume Name	SVM Name	Volume Size	Used Size	Snapshot Used Size	Cold Data	Tier Status	Tiering Policy	Action
<input type="checkbox"/> vol1	svm_AFF1	50 GB	3.54 MB	444 KB	2.47 MB	70 %	 Tiered Volume	All user data
<input checked="" type="checkbox"/> vol2	svm_AFF1	200 GB	1 MB	0 B	716.8 KB	70 %	 Tiered Volume	Cold snapshots
<input checked="" type="checkbox"/> vol3	svm_AFF1	200 GB	1 MB	0 B	716.8 KB	70 %	 Tiered Volume	Cold snapshots

## Result

You've successfully set up data tiering from volumes on the cluster to Azure Blob object storage.

## What's next?

[Be sure to subscribe from the Cloud Tiering service.](#)

You can also add additional clusters or review information about the active and inactive data on the cluster. For details, see [Managing data tiering from your clusters](#).

## Tiering data from on-premises ONTAP clusters to Google Cloud Storage

Free space on your on-prem ONTAP clusters by tiering data to Google Cloud Storage. Data tiering is powered by NetApp's Cloud Tiering service.

## Quick start

Get started quickly by following these steps or scroll down to the remaining sections for full details.



### Prepare to tier data to Google Cloud Storage

You need the following:

- An AFF or FAS system with all-SSD aggregates that's running ONTAP 9.6 or later and has an HTTPS connection to Google Cloud Storage. [Learn how to discover a cluster](#).
- A service account that has the predefined Storage Admin role and storage access keys.
- A Connector installed in a Google Cloud Platform VPC.
- Networking for the Connector that enables an outbound HTTPS connection to the ONTAP cluster in your data center, to Google Cloud Storage, and to the Cloud Tiering service.



### Set up tiering

In Cloud Manager, select an on-prem working environment, click **Setup Tiering** and follow the prompts to tier data to Google Cloud Storage.



### Set up licensing

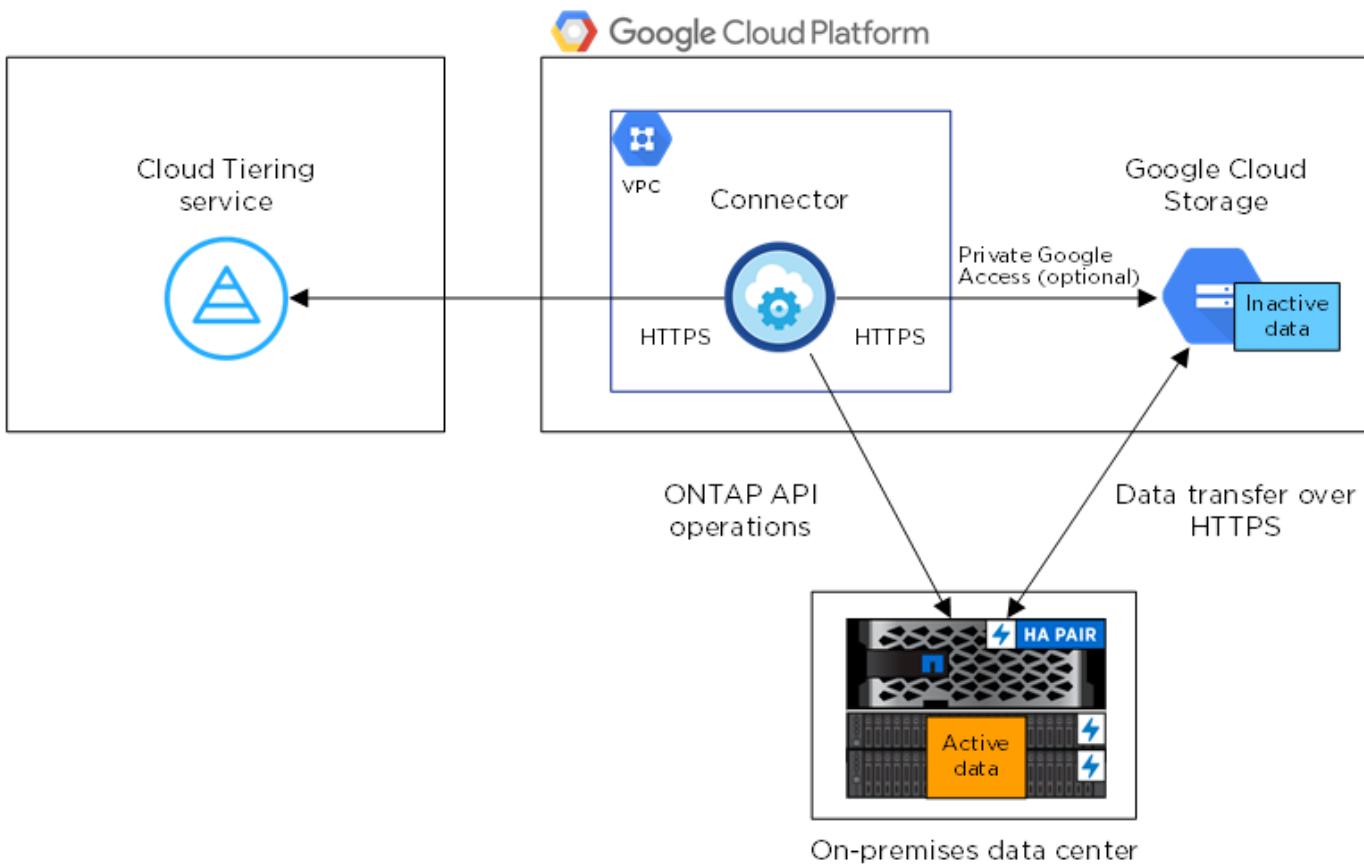
After your free trial ends, pay for Cloud Tiering through a pay-as-you-go subscription, an ONTAP tiering license, or a combination of both:

- To subscribe from the GCP Marketplace, click **Tiering > Licensing**, click **Subscribe**, and then follow the prompts.
- To add a tiering license, [contact us if you need to purchase one](#), and then [add it to your cluster from Cloud Tiering](#).

## Requirements

Verify support for your ONTAP cluster, set up your networking, and prepare your object storage.

The following image shows each component and the connections that you need to prepare between them:



Communication between the Connector and Google Cloud Storage is for object storage setup only.

#### Preparing your ONTAP clusters

Your ONTAP clusters must meet the following requirements when tiering data to Google Cloud Storage.

#### Supported ONTAP platforms

Cloud Tiering supports AFF systems and all-SSD aggregates on FAS systems.

#### Supported ONTAP versions

ONTAP 9.6 or later

#### Cluster networking requirements

- The ONTAP cluster initiates an HTTPS connection over port 443 to Google Cloud Storage.

ONTAP reads and writes data to and from object storage. The object storage never initiates, it just responds.

Although a Google Cloud Interconnect provides better performance and lower data transfer charges, it's not required between the ONTAP cluster and Google Cloud Storage. Because performance is significantly better when using Google Cloud Interconnect, doing so is the recommended best practice.

- An inbound connection is required from the NetApp Service Connector, which resides in an Google Cloud Platform VPC.

A connection between the cluster and the Cloud Tiering service is not required.

- An intercluster LIF is required on each ONTAP node that hosts tiered volumes. The LIF must be associated with the *IPspace* that ONTAP should use to connect to object storage.

IPspaces enable network traffic segregation, allowing for separation of client traffic for privacy and security. [Learn more about IPspaces](#).

When you set up data tiering, Cloud Tiering prompts you for the IPspace to use. You should choose the IPspace that each LIF is associated with. That might be the "Default" IPspace or a custom IPspace that you created.

## Supported volumes and aggregates

The total number of volumes that Cloud Tiering can tier might be less than the number of volumes on your ONTAP system. That's because volumes can't be tiered from some aggregates. For example, you can't tier data from SnapLock volumes or from MetroCluster configurations. Refer to ONTAP documentation for [functionality or features not supported by FabricPool](#).



Cloud Tiering supports FlexGroup volumes. Setup works the same as any other volume.

## Discovering an ONTAP cluster

You need to create an on-prem ONTAP working environment in Cloud Manager before you can start tiering cold data.

[Learn how to discover a cluster](#).

## Creating or switching Connectors

A Connector is required to tier data to the cloud. When tiering data to Google Cloud Storage, a Connector must be available in a Google Cloud Platform VPC. You'll either need to create a new Connector or make sure that the currently selected Connector resides in GCP.

- [Learn about Connectors](#)
- [Creating a Connector in GCP](#)
- [Switching between Connectors](#)

## Preparing networking for the Connector

Ensure that the Connector has the required networking connections.

## Steps

1. Ensure that the VPC where the Connector is installed enables the following connections:
  - An outbound internet connection to the Cloud Tiering service over port 443 (HTTPS)
  - An HTTPS connection over port 443 to Google Cloud Storage
  - An HTTPS connection over port 443 to your ONTAP clusters
2. Optional: Enable Private Google Access on the subnet where you plan to deploy the Service Connector.

[Private Google Access](#) is recommended if you have a direct connection from your ONTAP cluster to the VPC and you want communication between the Connector and Google Cloud Storage to stay in your virtual private network. Note that Private Google Access works with VM instances that have only internal (private) IP addresses (no external IP addresses).

## Preparing Google Cloud Storage for data tiering

When you set up tiering, you need to provide storage access keys for a service account that has Storage Admin permissions. A service account enables Cloud Tiering to authenticate and access Cloud Storage buckets used for data tiering. The keys are required so that Google Cloud Storage knows who is making the request.

### Steps

1. [Create a service account that has the predefined Storage Admin role](#).
2. Go to [GCP Storage Settings](#) and create access keys for the service account:
  - a. Select a project, and click **Interoperability**. If you haven't already done so, click **Enable interoperability access**.
  - b. Under **Access keys for service accounts**, click **Create a key for a service account**, select the service account that you just created, and click **Create Key**.

You'll need to [enter the keys in Cloud Tiering](#) later when you set up tiering.

## Tiering inactive data from your first cluster to Google Cloud Storage

After you prepare your Google Cloud environment, start tiering inactive data from your first cluster.

### What you'll need

- [An on-premises working environment](#).
- Storage access keys for a service account that has the Storage Admin role.

### Steps

1. Select an on-prem cluster.
2. Click **Enable**.

The screenshot shows the 'SERVICES' section of the ONTAP Cloud Tiering setup page. It lists five services with their current status and an 'Enable' button:

- Replication: Off, Enable
- Backup & Compliance: Unavailable, ⓘ, Enable
- Restore: Off, Enable
- Compliance: Off, Enable
- Tiering: Off, Enable

A large red arrow points to the 'Enable' button for the Tiering service.

3. Complete the steps on the **Tiering Setup** page:
  - a. **Bucket**: Add a new Google Cloud Storage bucket or select an existing bucket.
  - b. **Storage Class**: Select the storage class that you want to use for the tiered data.
  - c. **Credentials**: Enter the storage access key and secret key for a service account that has the Storage Admin role.
  - d. **Cluster Network**: Select the IPspace that ONTAP should use to connect to object storage.

Selecting the correct IPspace ensures that Cloud Tiering can set up a connection from ONTAP to your cloud provider's object storage.

4. Click **Continue** to select the volumes that you want to tier.

5. On the **Tier Volumes** page, set up tiering for each volume.

[Learn more about volume tiering policies.](#)

- To select a tiering policy for just one volume, click the icon, select a tiering policy, and optionally adjust the cooling days.

Volume Name	SVM Name	Volume Size	Used Size	Snapshot Used Size	Cold Data	Tier Status	Tiering Policy
vol1	svm_AFF1	50 GB	5.21 MB	864 KB	3.65 MB	70 %	<input checked="" type="checkbox"/> Tiered Volume All user data
vol2	svm_AFF1	200 GB	4.11 MB	424 KB	2.88 MB	70 %	<input checked="" type="checkbox"/> Tiered Volume Cold snapshots
vol3	svm_AFF1	200 GB	3.96 MB	424 KB	2.77 MB	70 %	<input checked="" type="checkbox"/> Tiered Volume Cold snapshots

- To select a tiering policy for several volumes, select multiple volumes, click **Modify selected volumes**, select a tiering policy, and optionally adjust the cooling days.

Volume Name	SVM Name	Volume Size	Used Size	Snapshot Used Size	Cold Data	Tier Status	Tiering Policy
vol1	svm_AFF1	50 GB	3.54 MB	444 KB	2.47 MB	70 %	<input checked="" type="checkbox"/> Tiered Volume All user data
vol2	svm_AFF1	200 GB	1 MB	0 B	716.8 KB	70 %	<input checked="" type="checkbox"/> Tiered Volume Cold snapshots
vol3	svm_AFF1	200 GB	1 MB	0 B	716.8 KB	70 %	<input checked="" type="checkbox"/> Tiered Volume Cold snapshots

## Result

You've successfully set up data tiering from volumes on the cluster to Google Cloud object storage.

## What's next?

Be sure to subscribe from the [Cloud Tiering service](#).

You can also add additional clusters or review information about the active and inactive data on the cluster. For details, see [Managing data tiering from your clusters](#).

## Tiering data from on-premises ONTAP clusters to StorageGRID

Free space on your on-prem ONTAP clusters by tiering data to StorageGRID. Data tiering is powered by NetApp's Cloud Tiering service.

### Quick start

Get started quickly by following these steps or scroll down to the remaining sections for full details.



### Prepare to tier data to StorageGRID

You need the following:

- An AFF or FAS system with all-SSD aggregates that's running ONTAP 9.4 or later, and a connection over a user-specified port to StorageGRID. [Learn how to discover a cluster](#).
- StorageGRID 10.3 or later with AWS access keys that have S3 permissions.
- A Connector installed on your premises.
- Networking for the Connector that enables an outbound HTTPS connection to the ONTAP cluster, to StorageGRID, and to the Cloud Tiering service.

## 2

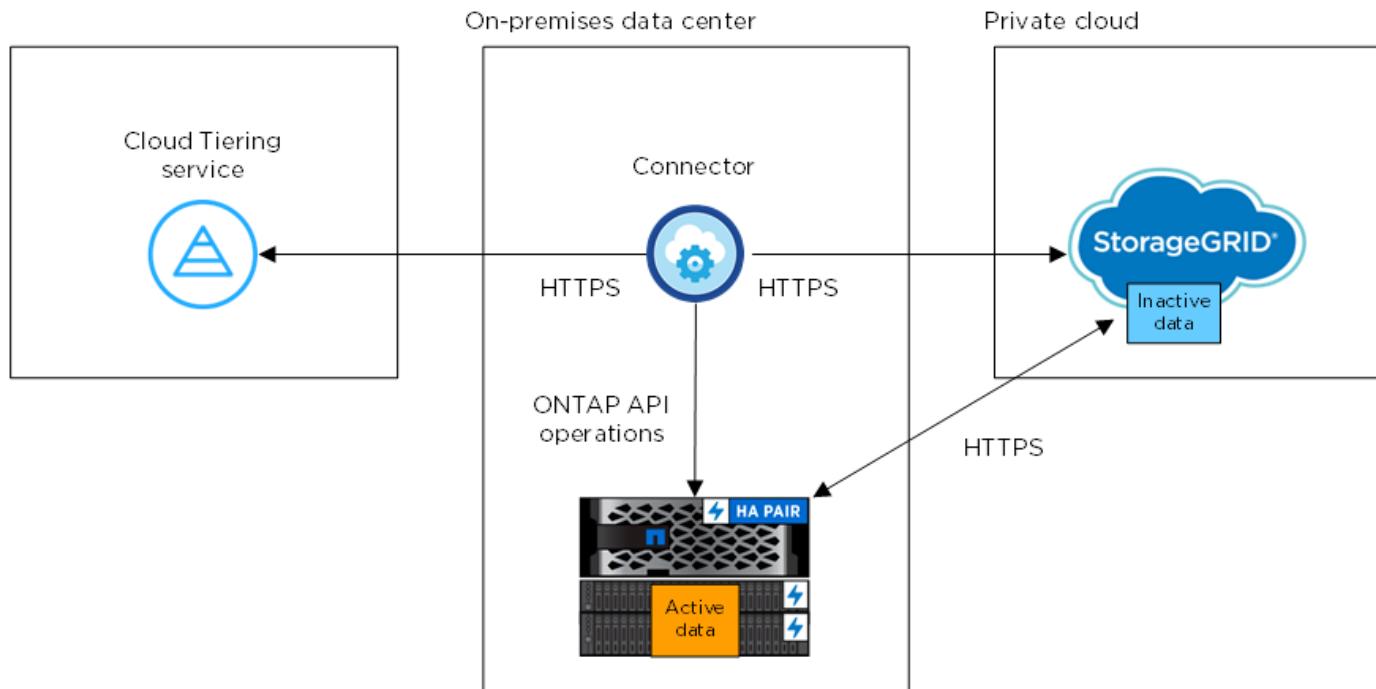
## Set up tiering

Select an on-prem working environment, click **Setup Tiering** and follow the prompts to tier data to StorageGRID.

### Requirements

Verify support for your ONTAP cluster, set up your networking, and prepare your object storage.

The following image shows each component and the connections that you need to prepare between them:



Communication between the Connector and StorageGRID is for object storage setup only.

### Preparing your ONTAP clusters

Your ONTAP clusters must meet the following requirements when tiering data to StorageGRID.

#### Supported ONTAP platforms

Cloud Tiering supports AFF systems and all-SSD aggregates on FAS systems.

#### Supported ONTAP version

ONTAP 9.4 or later

#### Licensing

A FabricPool license isn't required on the ONTAP cluster when tiering data to StorageGRID.

#### Cluster networking requirements

- The ONTAP cluster initiates an HTTPS connection over a user-specified port to StorageGRID (the port is configurable during tiering setup).

ONTAP reads and writes data to and from object storage. The object storage never initiates, it just

responds.

- An inbound connection is required from the Connector, which must reside on your premises.

A connection between the cluster and the Cloud Tiering service is not required.

- An intercluster LIF is required on each ONTAP node that hosts tiered volumes. The LIF must be associated with the *IPspace* that ONTAP should use to connect to object storage.

IPspaces enable network traffic segregation, allowing for separation of client traffic for privacy and security. [Learn more about IPspaces](#).

When you set up data tiering, Cloud Tiering prompts you for the IPspace to use. You should choose the IPspace that each LIF is associated with. That might be the "Default" IPspace or a custom IPspace that you created.

## Supported volumes and aggregates

The total number of volumes that Cloud Tiering can tier might be less than the number of volumes on your ONTAP system. That's because volumes can't be tiered from some aggregates. For example, you can't tier data from SnapLock volumes or from MetroCluster configurations. Refer to ONTAP documentation for [functionality or features not supported by FabricPool](#).



Cloud Tiering supports FlexGroup volumes, starting with ONTAP 9.5. Setup works the same as any other volume.

## Discovering an ONTAP cluster

You need to create an on-prem ONTAP working environment in Cloud Manager before you can start tiering cold data.

[Learn how to discover a cluster.](#)

## Preparing StorageGRID

StorageGRID must meet the following requirements.

## Supported StorageGRID versions

StorageGRID 10.3 and later are supported.

## S3 credentials

When you set up tiering to StorageGRID, you need to provide Cloud Tiering with an S3 access key and secret key. Cloud Tiering uses the keys to access your buckets.

These access keys must be associated with a user who has the following permissions:

```
"s3>ListAllMyBuckets",
"s3>ListBucket",
"s3GetObject",
"s3PutObject",
"s3DeleteObject",
"s3CreateBucket"
```

## Object versioning

You must not enable StorageGRID object versioning on the object store bucket.

## Creating or switching Connectors

A Connector is required to tier data to the cloud. When tiering data to StorageGRID, a Connector must be available on your premises. You'll either need to install a new Connector or make sure that the currently selected Connector resides on-prem.

- [Learn about Connectors](#)
- [Connector host requirements](#)
- [Installing the Connector on an existing Linux host](#)
- [Switching between Connectors](#)

## Preparing networking for the Connector

Ensure that the Connector has the required networking connections.

### Steps

1. Ensure that the network where the Connector is installed enables the following connections:
  - An outbound internet connection to the Cloud Tiering service over port 443 (HTTPS)
  - An HTTPS connection over port 443 to StorageGRID
  - An HTTPS connection over port 443 to your ONTAP clusters

## Tiering inactive data from your first cluster to StorageGRID

After you prepare your environment, start tiering inactive data from your first cluster.

### What you'll need

- [An on-premises working environment.](#)
- An AWS access key that has the required S3 permissions.

### Steps

1. Select an on-prem cluster.
2. Click **Enable**.

The screenshot shows the configuration page for the OnPrem1 cluster. At the top, there's a status summary with a blue icon, the name 'OnPrem1', and a green 'On' status indicator. Below this is a section titled 'SERVICES' containing five items:

- Replication**: Status: Off, with an 'Enable' button.
- Backup & Compliance**: Status: Unavailable, with a help icon (i).
- Restore**: Status: Off, with an 'Enable' button.
- Compliance**: Status: Off, with an 'Enable' button.
- Tiering**: Status: Off, with an 'Enable' button.

A large red arrow points to the 'Enable' button for the 'Tiering' service.

3. Complete the steps on the **Tiering Setup** page:
  - a. **Choose your provider:** Select StorageGRID.
  - b. **Server:** Enter the FQDN of the StorageGRID server, enter the port that ONTAP should use for HTTPS communication with StorageGRID, and enter the access key and secret key for an AWS account that has the required S3 permissions.
  - c. **Bucket:** Add a new bucket or select an existing bucket for the tiered data.
  - d. **Cluster Network:** Select the IPspace that ONTAP should use to connect to object storage.

Selecting the correct IPspace ensures that Cloud Tiering can set up a connection from ONTAP to your cloud provider's object storage.

4. Click **Continue** to select the volumes that you want to tier.

5. On the **Tier Volumes** page, set up tiering for each volume. Click the icon, select a tiering policy, optionally adjust the cooling days, and click **Apply**.

[Learn more about volume tiering policies.](#)

Tier Volumes	Tier volumes	Learn how much you can save with each Tiering Policy						
50 Volumes		Q						
Volume Name	SVM Name	Volume Size	Used Size	Snapshot used size	Cold Data (Estimated)	Tier Status	TieringPolicy	
Volume 1	SVMNameB...	462 TB	100 TB	50 TB	70 TB   70%	Available for Tiering	Cold User Data	

## Result

You've successfully set up data tiering from volumes on the cluster to StorageGRID.

## What's next?

You can add additional clusters or review information about the active and inactive data on the cluster. For details, see [Managing data tiering from your clusters](#).

## Set up licensing for Cloud Tiering

Pay for Cloud Tiering through a pay-as-you-go subscription, an ONTAP tiering license called *FabricPool*, or a combination of both. If you want to pay as you go, then you need to subscribe from the marketplace for the cloud provider to which you want to tier cold data. There's no need to subscribe from every marketplace.

A few notes before you read any further:

- If a FabricPool license is already installed on your cluster, then you're all set—there's nothing else that you need to do.
- If you've already subscribed to the Cloud Manager subscription in your cloud provider's marketplace, then you're automatically subscribed to Cloud Tiering, as well. You'll see an active subscription in the Cloud Tiering **Licensing** tab. You won't need to subscribe again.
- There are no charges when tiering data to StorageGRID. Neither a BYOL license or PAYGO registration is required.

[Learn more about how licensing works for Cloud Tiering.](#)

## Subscribing from the AWS Marketplace

Subscribe to Cloud Tiering from the AWS Marketplace to set up a pay-as-you-go subscription for data tiering from ONTAP clusters to AWS S3.

### Steps

1. In Cloud Manager, click **Tiering > Licensing**.
2. Click **Subscribe** under AWS Marketplace and then click **Continue**.
3. Subscribe from the AWS Marketplace, and then log back in to Cloud Central to complete the registration.

The following video shows the process:

► [https://docs.netapp.com/us-en/occm/media/video\\_subscribing\\_aws\\_tiering.mp4](https://docs.netapp.com/us-en/occm/media/video_subscribing_aws_tiering.mp4) (video)

## Subscribing from the Azure Marketplace

Subscribe to Cloud Tiering from the Azure Marketplace to set up a pay-as-you-go subscription for data tiering from ONTAP clusters to Azure Blob storage.

### Steps

1. In Cloud Manager, click **Tiering > Licensing**.
2. Click **Subscribe** under Azure Marketplace and then click **Continue**.
3. Subscribe from the Azure Marketplace, and then log back in to Cloud Central to complete the registration.

The following video shows the process:

► [https://docs.netapp.com/us-en/occm/media/video\\_subscribing\\_azure\\_tiering.mp4](https://docs.netapp.com/us-en/occm/media/video_subscribing_azure_tiering.mp4) (video)

## Subscribing from the GCP Marketplace

Subscribe to Cloud Tiering from the GCP Marketplace to set up a pay-as-you-go subscription for data tiering from ONTAP clusters to Google Cloud storage.

### Steps

1. In Cloud Manager, click **Tiering > Licensing**.
2. Click **Subscribe** under GCP Marketplace and then click **Continue**.
3. Subscribe from the GCP Marketplace, and then log back in to Cloud Central to complete the registration.

The following video shows the process:

► [https://docs.netapp.com/us-en/occm/media/video\\_subscribing\\_gcp\\_tiering.mp4](https://docs.netapp.com/us-en/occm/media/video_subscribing_gcp_tiering.mp4) (video)

## Adding a tiering license to ONTAP

Bring your own license by purchasing an ONTAP FabricPool license from NetApp.

### Steps

1. If you don't have a FabricPool license, [contact us to purchase one](#).
2. In Cloud Manager, click **Tiering > Licensing**.
3. In the Clusters List table, click **Activate license (BYOL)** for an on-prem ONTAP cluster.

Clusters List					
2 Clusters					
Cluster Name	Cluster Type	Tiered Capacity	License	Provider	
AFF1	On-prem	0 B	PAYGO		<a href="#">Activate license (BYOL)</a>
CloudVolumesONTAP1	Cloud Volumes ONTAP	0 B	---		

4. Enter the serial number of the license and then enter the NetApp Support Site account that's associated with the serial number.

5. Click **Activate license**.

## Result

Cloud Tiering registers the license and installs it on the cluster.

## After you finish

If you purchase additional add-on capacity at a later time, the license on the cluster is automatically updated with the new capacity. There's no need to apply a new NetApp License File (NLF) to the cluster.

# Measure network latency and throughput performance

Run a Cloud Performance Test to measure network latency and throughput performance from an ONTAP cluster to an object store before and after setting up data tiering. The test also identifies any failures that occurred.

Here are sample performance results:

Your cluster performance results			
Node: aff-01	Last check: 01/13/2021 04:25 pm		Recheck performance
Operation	Size	Avg.Latency (ms)	Throughput
PUT	4 MB	502	408.06 MB
GET	4 KB	79	15.05 MB
GET	8 KB	197	28.35 MB
GET	32 KB	291	109.71 MB
GET	256 KB	361	714.39 MB

## Before you get started

It's best to run this check when the cluster is under 50% CPU utilization.

### Steps for a cluster that hasn't been set up for tiering

1. At the top of Cloud Manager, click **Tiering**.
2. From the **Cluster Dashboard**, click the menu icon for a cluster and select **Cloud Performance Test**.
3. Review the details and click **Continue**.
4. Follow the prompts to provide the required information.

The information that you need to provide is the same as if you were setting up tiering on the cluster.

5. Optionally continue to the Tier Volumes wizard to complete the setup.

#### Steps for a cluster that has been set up for tiering

1. At the top of Cloud Manager, click **Tiering**.
2. From the **Cluster Dashboard**, click the menu icon for a cluster and select **Cloud Performance Test**.
3. Select a node from the drop-down list.
4. View the results or recheck the performance.

## Managing data tiering from your clusters

Now that you've set up data tiering from your ONTAP clusters, you can tier data from additional volumes, change a volume's tiering policy, and more.

### Tiering data from additional volumes

Set up data tiering for additional volumes at any time—for example, after creating a new volume.

#### Steps

1. At the top of Cloud Manager, click **Tiering**.
2. From the **Cluster Dashboard**, click **Tier Volumes** for the cluster.
3. On the **Tier Volumes** page, set up tiering for each volume.

[Learn more about volume tiering policies.](#)



You don't need to configure the object storage because it was already configured when you initially set up tiering for the cluster. ONTAP will tier inactive data from these volumes to the same object store.

- To select a tiering policy for just one volume, click the icon, select a tiering policy, and optionally adjust the cooling days.

3 Volumes								
Volume Name	SVM Name	Volume Size	Used Size	Snapshot Used Size	Cold Data	Tier Status	Tiering Policy	
<input type="checkbox"/> vol1	svm_AFF1	50 GB	5.21 MB	864 KB	3.65 MB	70 %	Tiered Volume	All user data
<input type="checkbox"/> vol2	svm_AFF1	200 GB	4.11 MB	424 KB	2.88 MB	70 %	Tiered Volume	Cold snapshots
<input type="checkbox"/> vol3	svm_AFF1	200 GB	3.96 MB	424 KB	2.77 MB	70 %	Tiered Volume	Cold snapshots

- To select a tiering policy for several volumes, select multiple volumes, click **Modify selected volumes**, select a tiering policy, and optionally adjust the cooling days.

Volume Name	SVM Name	Volume Size	Used Size	Snapshot Used Size	Cold Data	Tier Status	Tiering Policy
vol1	svm_AFF1	50 GB	3.54 MB	444 KB	2.47 MB   70 %	<input checked="" type="checkbox"/> Tiered Volume	All user data
vol2	svm_AFF1	200 GB	1 MB	0 B	716.8 KB   70 %	<input checked="" type="checkbox"/> Tiered Volume	Cold snapshots
vol3	svm_AFF1	200 GB	1 MB	0 B	716.8 KB   70 %	<input checked="" type="checkbox"/> Tiered Volume	Cold snapshots

## Changing a volume's tiering policy

Changing the tiering policy for a volume changes how ONTAP tiers cold data to object storage. The change starts from the moment that you change the policy—it changes only the subsequent tiering behavior for the volume.

### Steps

- At the top of Cloud Manager, click **Tiering**.
- From the **Cluster Dashboard**, click **Tier Volumes** for the cluster.
- Click the icon, select a tiering policy, optionally adjust the cooling days, and click **Apply**.

[Learn more about volume tiering policies.](#)

## Managing tiering settings on aggregates

Each aggregate has two settings that you can adjust: the tiering fullness threshold and whether inactive data reporting is enabled.

### Tiering fullness threshold

Setting the threshold to a lower number reduces the amount of data required to be stored on the performance tier before tiering takes place. This might be useful for large aggregates that contain little active data.

Setting the threshold to a higher number increases the amount of data required to be stored on the performance tier before tiering takes place. This might be useful for solutions designed to tier only when aggregates are near maximum capacity.

### Inactive data reporting

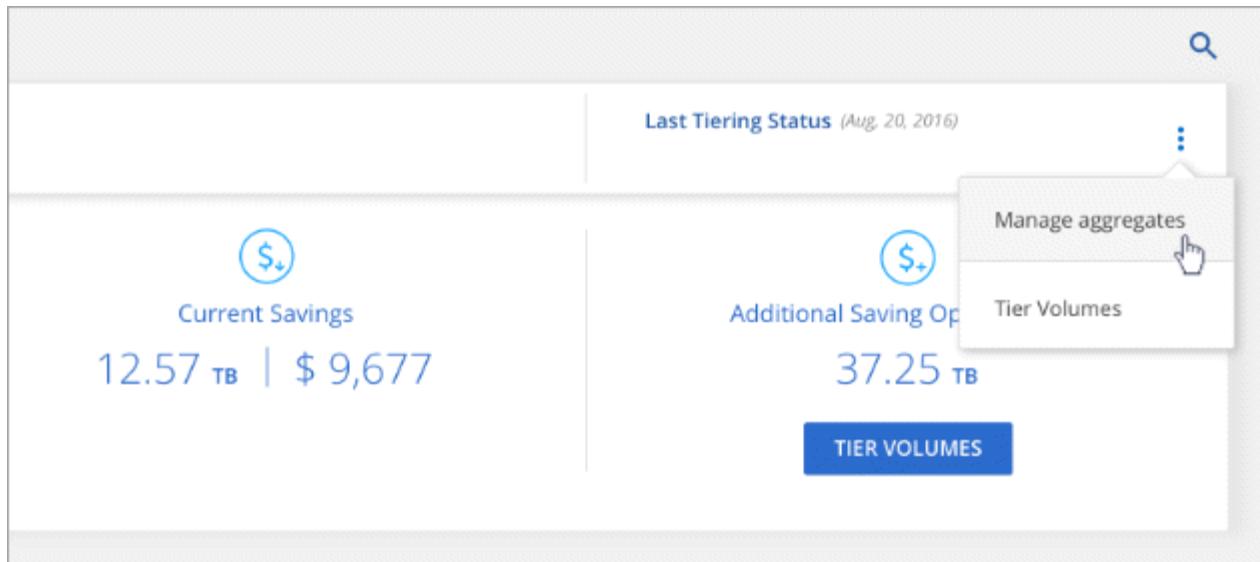
Inactive data reporting (IDR) uses a 31-day cooling period to determine which data is considered inactive. The amount of cold data that is tiered is dependent on the tiering policies set on volumes. This amount might be different than the amount of cold data detected by IDR using a 31-day cooling period.



It's best to keep IDR enabled because it helps to identify your inactive data and savings opportunities. IDR must remain enabled if data tiering was enabled on an aggregate.

### Steps

- At the top of Cloud Manager, click **Tiering**.
- From the **Cloud Tiering** page, click the menu icon for a cluster and select **Manage Aggregates**.



3. On the **Manage Aggregates** page, click the icon for an aggregate in the table.
4. Modify the fullness threshold and choose whether to enable or disable inactive data reporting.

The screenshot shows the "aggr1" configuration page with the following settings:

- Tier data when the aggregate is this full :** A slider set at 50 %.
- Activate inactive data reporting**: A toggle switch is turned on (blue).

5. Click **Apply**.

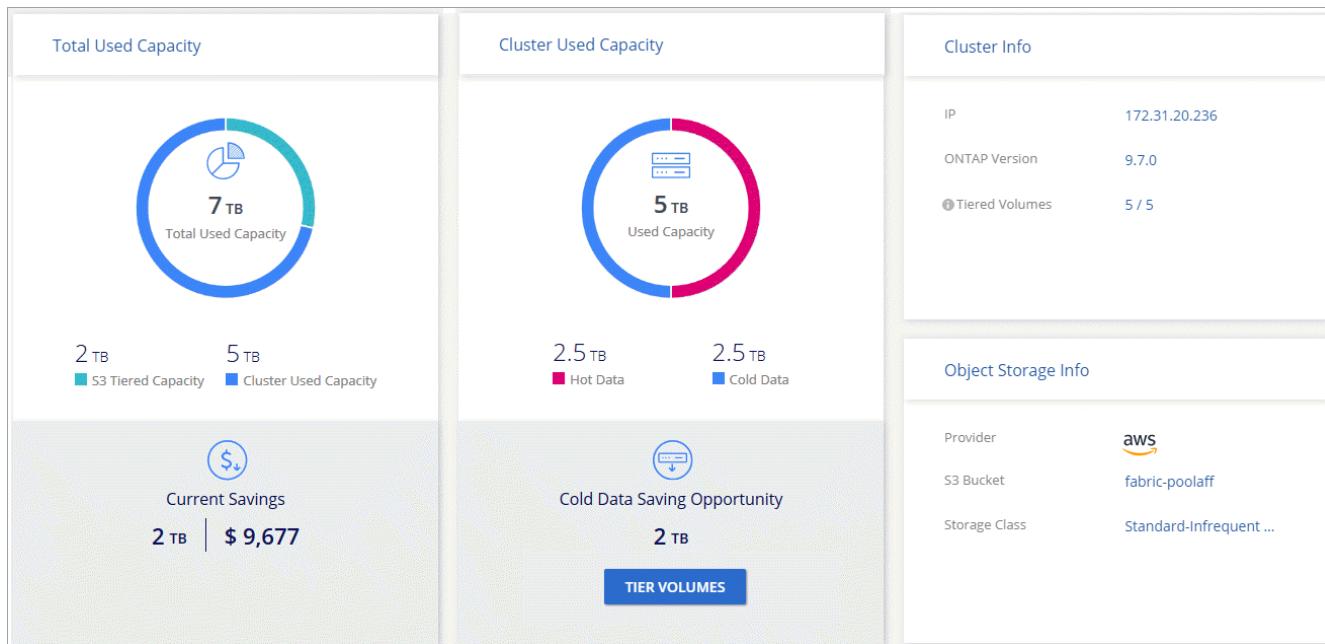
## Reviewing tiering info for a cluster

You might want to see how much data is in the cloud tier and how much data is on disks. Or, you might want to see the amount of hot and cold data on the cluster's disks. Cloud Tiering provides this information for each cluster.

### Steps

1. At the top of Cloud Manager, click **Tiering**.
2. From the **Cluster Dashboard**, click the menu icon for a cluster and select **Cluster info**.
3. Review details about the cluster.

Here's an example:

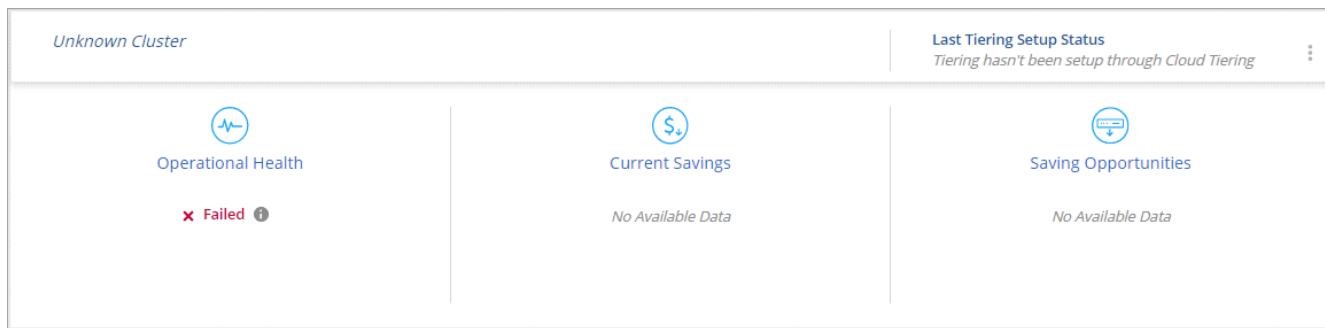


## Fixing operational health

Failures can happen. When they do, Cloud Tiering displays a "Failed" operational health status on the Cluster Dashboard. The health reflects the status of the ONTAP system and Cloud Manager.

### Steps

1. Identify any clusters that have an operational health of "Failed."



2. Hover over the ⓘ icon to see the failure reason.

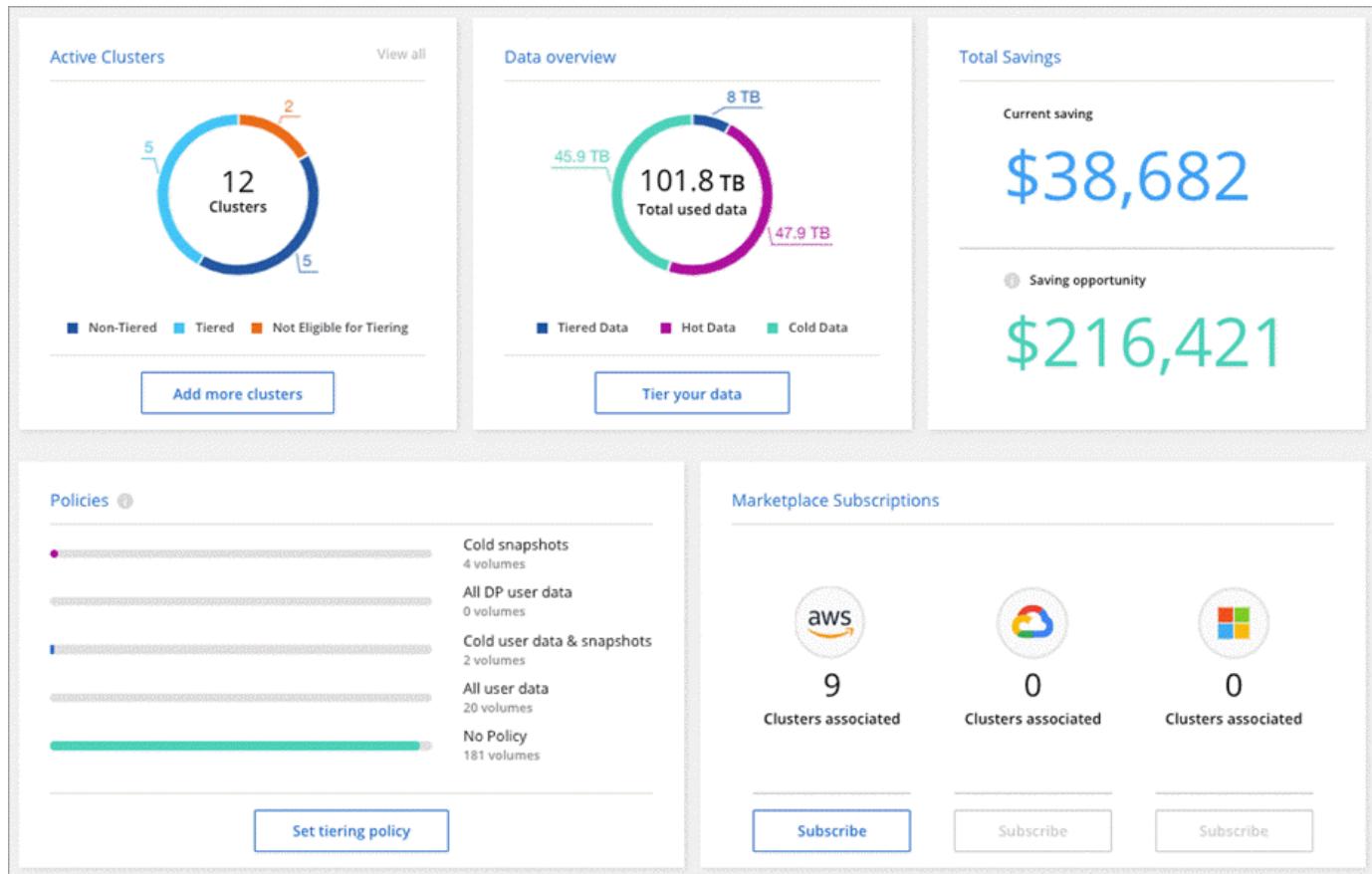
3. Correct the issue:

- a. Verify that the ONTAP cluster is operational and that it has an inbound and outbound connection to your object storage provider.
- b. Verify that Cloud Manager has outbound connections to the Cloud Tiering service, to the object store, and to the ONTAP clusters that it discovers.

## Get an overview of data tiering from your clusters

Cloud Tiering provides an aggregated view of data tiering from each of your on-premises clusters. This overview provides a clear picture of your environment and enables you to take proper actions.

Cloud Tiering provides the following details about your environment:



## Active Clusters

The number of clusters that are currently tiering data to the cloud, the clusters that aren't tiering data to the cloud, and the number of clusters that don't support data tiering.

## Data Overview

The amount of data that was tiered to the cloud, and the amount of hot and cold data on the cluster.

## Total Savings

The amount of money that you've saved by tiering data to the cloud, as well as the amount of money that you could save by tiering more data to the cloud.

## Policies

The number of times that each tiering policy has been applied to a volume.

## Marketplace Subscriptions

The number of clusters associated with each type of Marketplace Subscription and an indication about your subscription status.

## Steps

1. Click **Tiering > On-Prem Overview**.

# Cloud Tiering technical FAQ

This FAQ can help if you're just looking for a quick answer to a question.

## ONTAP

The following questions relate to ONTAP.

### What are the requirements for my ONTAP cluster?

It depends on where you tier the cold data. Refer to the following:

- [Tiering data from on-premises ONTAP clusters to Amazon S3](#)
- [Tiering data from on-premises ONTAP clusters to Azure Blob storage](#)
- [Tiering data from on-premises ONTAP clusters to Google Cloud Storage](#)
- [Tiering data from on-premises ONTAP clusters to StorageGRID](#)

### Does Cloud Tiering enable inactive data reporting?

Yes, Cloud Tiering enables inactive data reporting on each aggregate. This setting enables us to identify the amount of inactive data that can be tiered to low-cost object storage.



Cloud Tiering enables inactive data reporting on HDD aggregates if the cluster is running ONTAP 9.6 or later.

### Can I tier data from NAS volumes and SAN volumes?

You can use Cloud Tiering to tier data from NAS volumes to the public cloud and from SAN volumes to a private cloud using StorageGRID.

### What about Cloud Volumes ONTAP?

If you have Cloud Volumes ONTAP systems, you'll find them in the Cluster Dashboard so you get a full view of data tiering in your hybrid cloud infrastructure.

From the Cluster Dashboard, you can view tiering information similar to an on-prem ONTAP cluster: operational health, current savings, savings opportunities, details about volumes and aggregates, and more.

Cloud Volumes ONTAP systems are read-only from Cloud Tiering. You can't set up data tiering on Cloud Volumes ONTAP from Cloud Tiering. You'll still set up tiering the same way: from the working environment in Cloud Manager.

## Object storage

The following questions relate to object storage.

### Which object storage providers are supported?

Amazon S3, Azure Blob storage, Google Cloud Storage, and StorageGRID using the S3 protocol are supported.

### Can I use my own bucket/container?

Yes, you can. When you set up data tiering, you have the choice to add a new bucket/container or to select an existing bucket/container.

## **Which regions are supported?**

- [Supported AWS regions](#)
- [Supported Azure regions](#)
- [Supported Google Cloud regions](#)

## **Which S3 storage classes are supported?**

Cloud Tiering supports data tiering to the *Standard*, *Standard-Infrequent Access*, *One Zone-IA*, or *Intelligent* storage class. See [Supported S3 storage classes](#) for more details.

## **Which Azure Blob access tiers are supported?**

Cloud Tiering automatically uses the *Hot* access tier for your inactive data.

## **Which storage classes are supported for Google Cloud Storage?**

Cloud Tiering uses the *Standard* storage class for inactive data.

## **Does Cloud Tiering use one object store for the entire cluster or one per aggregate?**

One object store for the entire cluster.

## **Can I apply policies to my object store to move data around independent of tiering?**

No, Cloud Tiering does not support object lifecycle management rules that move or delete data from object stores.

## **Connectors**

The following questions relate to Connectors.

## **Where does the Connector need to be installed?**

- When tiering data to S3, a Connector can reside in an AWS VPC or on your premises.
- When tiering data to Blob storage, a Connector must reside in an Azure VNet.
- When tiering data to Google Cloud Storage, a Connector must reside in a Google Cloud Platform VPC.
- When tiering data to StorageGRID, a Connector must reside on an on premises Linux host.

## **Networking**

The following questions relate to networking.

## **What are the networking requirements?**

- The ONTAP cluster initiates an HTTPS connection over port 443 to your object storage provider.  
ONTAP reads and writes data to and from object storage. The object storage never initiates, it just responds.
- For StorageGRID, the ONTAP cluster initiates an HTTPS connection over a user-specified port to StorageGRID (the port is configurable during tiering setup).

- A Connector needs an outbound HTTPS connection over port 443 to your ONTAP clusters, to the object store, and to the Cloud Tiering service.

For more details, see:

- [Tiering data from on-premises ONTAP clusters to Amazon S3](#)
- [Tiering data from on-premises ONTAP clusters to Azure Blob storage](#)
- [Tiering data from on-premises ONTAP clusters to Google Cloud Storage](#)
- [Tiering data from on-premises ONTAP clusters to StorageGRID](#)

## Permissions

The following questions relate to permissions.

### What permissions are required in AWS?

Permissions are required to [manage the S3 bucket](#).

### What permissions are required in Azure?

No extra permissions are needed outside of the permissions that you need to provide to Cloud Manager.

### What permissions are required in Google Cloud Platform?

Storage Admin permissions are needed for a service account that has storage access keys.

### What permissions are required for StorageGRID?

[S3 permissions are needed](#).

## Reference

### Supported S3 storage classes and regions

Cloud Tiering supports several S3 storage classes and most regions.

### Supported S3 storage classes

Cloud Tiering can apply a lifecycle rule so the data transitions from the *Standard* storage class to another storage class after 30 days. You can choose from the following storage classes:

- Standard-Infrequent Access
- One Zone-IA
- Intelligent

If you choose Standard, then the data remains in that storage class.

[Learn about S3 storage classes](#).

## **Supported AWS regions**

Cloud Tiering supports the following AWS regions.

### **Asia Pacific**

- Mumbai
- Seoul
- Singapore
- Sydney
- Tokyo

### **Europe**

- Frankfurt
- Ireland
- London
- Paris
- Stockholm

### **North America**

- Canada Central
- GovCloud (US-West) – starting with ONTAP 9.3
- US East (N. Virginia)
- US East (Ohio)
- US West (N. California)
- US West (Oregon)

### **South America**

- São Paulo

## **Supported Azure Blob access tiers and regions**

Cloud Tiering supports the *Hot* access tier and most regions.

### **Supported Azure Blob access tiers**

When you set up data tiering to Azure, Cloud Tiering automatically uses the *Hot* access tier for your inactive data.

### **Supported Azure regions**

Cloud Tiering supports the following Azure regions.

## **Africa**

- South Africa North

## **Asia Pacific**

- Australia East
- Australia Southeast
- East Asia
- Japan East
- Japan West
- Korea Central
- Korea South
- Southeast Asia

## **Europe**

- France Central
- Germany Central
- Germany Northeast
- North Europe
- UK South
- UK West
- West Europe

## **North America**

- Canada Central
- Canada East
- Central US
- East US
- East US 2
- North Central US
- South Central US
- West US
- West US 2
- West Central US

## **South America**

- Brazil South

## **Supported Google Cloud storage classes and regions**

Cloud Tiering supports the Standard storage class and most Google Cloud regions.

### **Supported access tiers**

Cloud Tiering uses the *Standard* access tier for your inactive data.

### **Supported Google Cloud regions**

Cloud Tiering supports the following regions.

#### **Americas**

- Iowa
- Los Angeles
- Montreal
- N. Virginia
- Oregon
- Sao-Paulo
- South Carolina

#### **Asia Pacific**

- Hong Kong
- Mumbai
- Osaka
- Singapore
- Sydney
- Taiwan
- Tokyo

#### **Europe**

- Belgium
- Finland
- Frankfurt
- London
- Netherlands
- Zurich

# Viewing your Amazon S3 buckets

After you install a Connector in AWS, Cloud Manager can automatically discover information about the Amazon S3 buckets that reside in the AWS account where it's installed.

You can see details about your S3 buckets, including the region, access level, storage class, and whether the bucket is used with Cloud Volumes ONTAP for backups or data tiering. And you can scan the S3 buckets with Cloud Compliance.

## Steps

1. [Install a Connector](#) in the AWS account where you want to view your Amazon S3 buckets.

You should automatically see an Amazon S3 working environment shortly after.



2. Click the working environment and select an action from the right pane.

 **Amazon S3**  
■ On X

---

**INFORMATION**

241	15
Buckets	Regions

---

**SERVICES**

 <b>Cloud Compliance</b> ■ Off	<span style="border: 1px solid #ccc; padding: 2px 10px; color: #0072bc; text-decoration: none; font-weight: bold;">Enable Compliance</span> <span style="border: 1px solid #ccc; border-radius: 50%; padding: 2px 5px; margin-left: 10px;">...</span>
--	---

---

View Buckets 

3. Click **Enable Compliance** to scan the S3 buckets for personal and sensitive data.

For more details, see [Getting started with Cloud Compliance for Amazon S3](#).

4. Click **View Buckets** to view details about the S3 buckets in your AWS account.

# Administer Cloud Manager

## Finding your Cloud Manager system ID

To help you get started, your NetApp representative might ask you for your Cloud Manager system ID. The ID is typically used for licensing and troubleshooting purposes.

### What you'll need

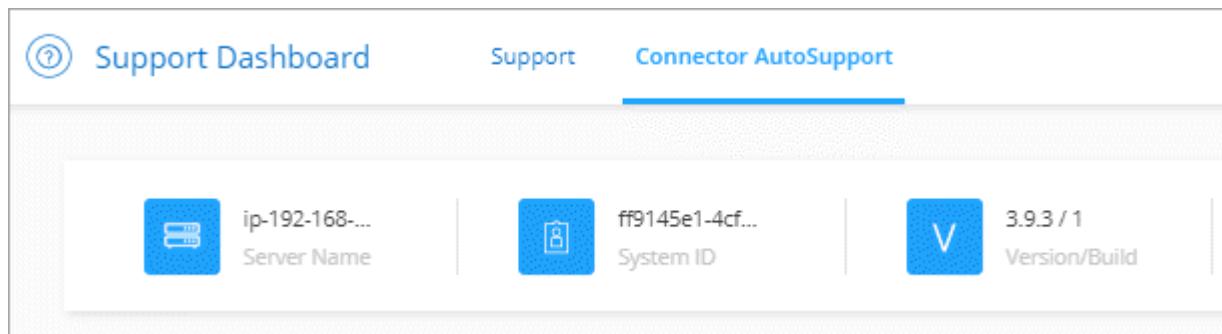
You need to create a Connector before you can change Cloud Manager settings. [Learn how](#).

### Steps

1. In the upper right of the Cloud Manager console, click the Help icon.
2. Click **Support > Connector AutoSupport**.

Your system ID appears at the top.

### Example



# Manage Connectors

## Managing existing Connectors

After you create one or more Connectors, you can manage them by switching between Connectors, connecting to the local user interface running on a Connector, and more.

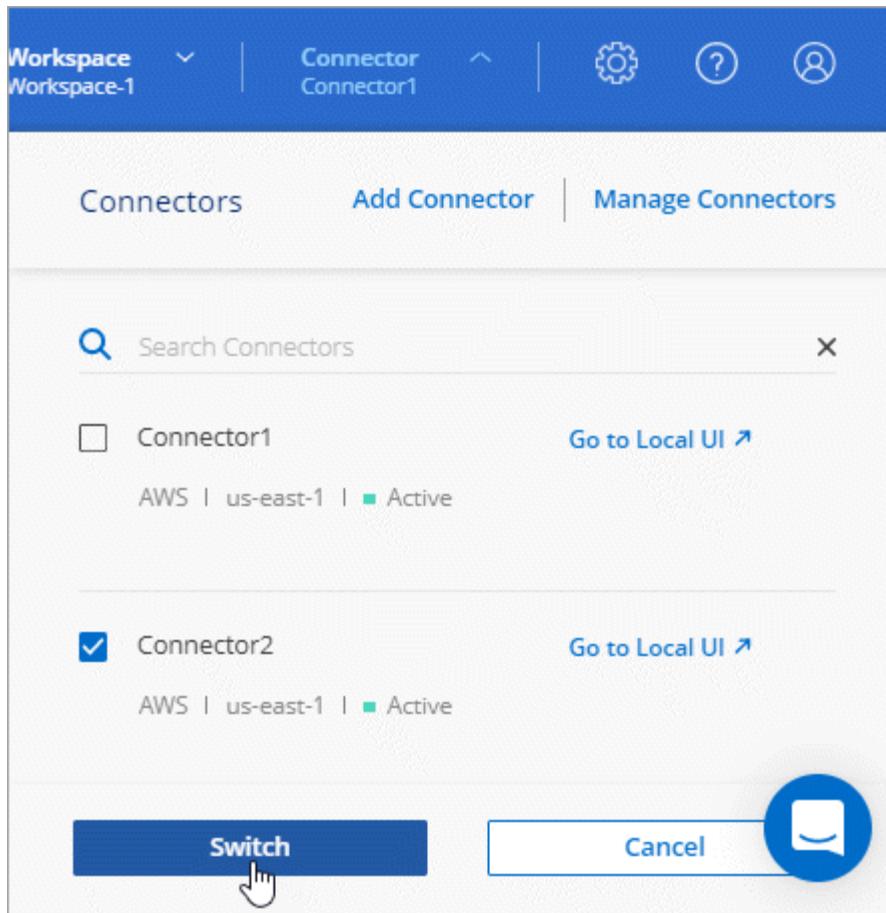
### Switching between Connectors

If you have multiple Connectors, you can switch between them to see the Working Environments that are associated with a specific Connector.

For example, let's say that you're working in a multi-cloud environment. You might have one Connector in AWS and another in Google Cloud. You'd need to switch between those Connectors to manage the Cloud Volumes ONTAP systems running in those clouds.

### Step

1. Click the **Connector** drop-down, select another Connector, and then click **Switch**.



Cloud Manager refreshes and shows the Working Environments associated with the selected Connector.

## Accessing the local UI

While you should perform almost all tasks from the SaaS user interface, a local user interface is still available on the Connector. This interface is needed for a few tasks that need to be performed from the Connector itself:

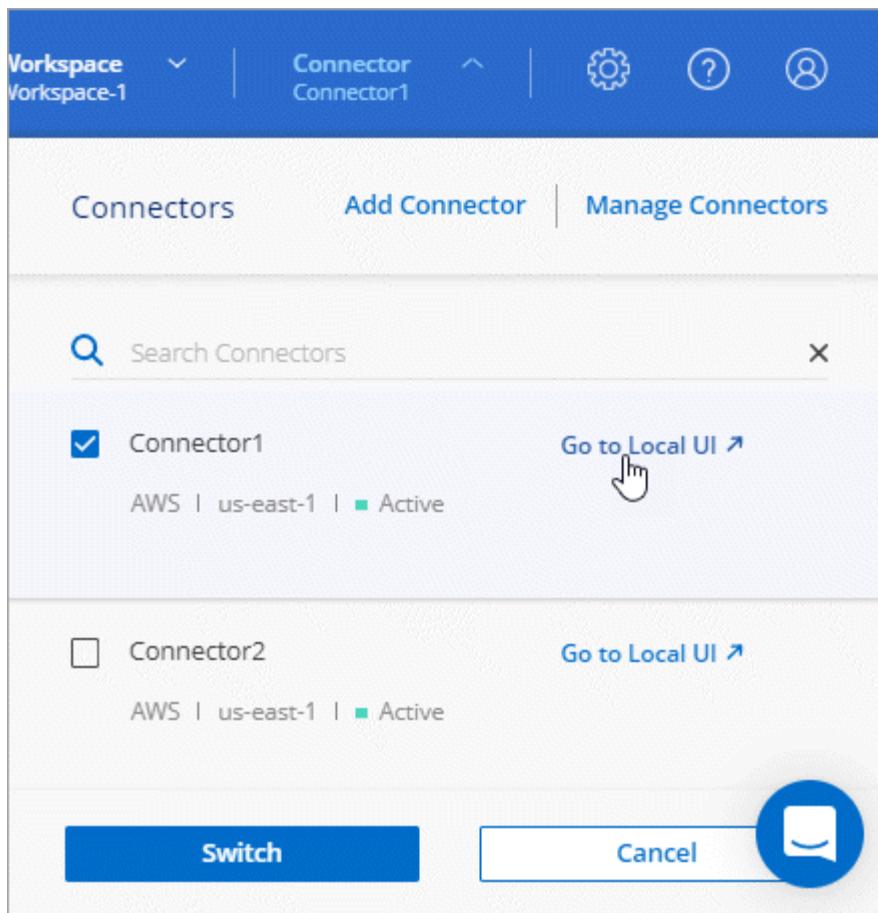
- [Setting a proxy server](#)
- Installing a patch (you'll typically work with NetApp personnel to install a patch)
- Downloading AutoSupport messages (usually directed by NetApp personnel when you have issues)

## Steps

1. [Log in to the Cloud Manager SaaS interface](#) from a machine that has a network connection to the Connector instance.

If the Connector doesn't have a public IP address, you'll need a VPN connection or you'll need to connect from a jump host that's in the same network as the Connector.

2. Click the **Connector** drop-down and then click **Go to Local UI**.



The Cloud Manager interface running on the Connector loads in a new browser tab.

## Editing a Connector's URIs

Add and remove the URIs for a Connector.

### Steps

1. Click the **Connector** drop-down from the Cloud Manager header.
2. Click **Manage Connectors**.
3. Click the action menu for a Connector and click **Edit URIs**.
4. Add and remove URIs and then click **Apply**.

## Removing Connectors from Cloud Manager

If a Connector is inactive, you can remove it from the list of Connectors in Cloud Manager. You might do this if you deleted the Connector virtual machine or if you uninstalled the Connector software.

Note the following about removing a Connector:

- This action doesn't delete the virtual machine.
- This action can't be reverted—once you remove a Connector from Cloud Manager, you can't add it back to Cloud Manager.

### Steps

1. Click the **Connector** drop-down from the Cloud Manager header.
2. Click **Manage Connectors**.
3. Click the action menu for an inactive Connector and click **Remove Connector**.

Connector Name	Status	Cloud Provider	Region	Actions
Connector1	● Active	aws	US East (N. Virginia)	...
Connector2	● Inactive	aws	US East (N. Virginia)	...

Context menu for Connector2:

- Go to Local UI ↗
- Connector Id: iEMkyjIEyG4U5fXpmpmsnZS... 📁
- Edit URIs
- Remove Connector** (highlighted)

4. Enter the name of the Connector to confirm and then click Remove.

## Result

Cloud Manager removes the Connector from its records.

## Uninstalling the Connector software

The Connector includes an uninstallation script that you can use to uninstall the software to troubleshoot issues or to permanently remove the software from the host.

### Step

1. From the Linux host, run the uninstallation script:

```
/opt/application/netapp/cloudmanager/bin/uninstall.sh [silent]
```

*silent* runs the script without prompting you for confirmation.

### What about software upgrades?

The Connector automatically updates its software to the latest version, as long as it has [outbound internet access](#) to obtain the software update.

## More ways to create Connectors

### Connector host requirements

The Connector software must run on a host that meets specific operating system requirements, RAM requirements, port requirements, and so on.

## A dedicated host is required

The Connector is not supported on a host that is shared with other applications. The host must be a dedicated host.

## CPU

4 cores or 4 vCPUs

## RAM

14 GB

## AWS EC2 instance type

An instance type that meets the CPU and RAM requirements above. We recommend t3.xlarge and use that instance type when you deploy the Connector directly from Cloud Manager.

## Azure VM size

An instance type that meets the CPU and RAM requirements above. We recommend DS3 v2 and use that VM size when you deploy the Connector directly from Cloud Manager.

## GCP machine type

An instance type that meets the CPU and RAM requirements above. We recommend n1-standard-4 and use that machine type when you deploy the Connector directly from Cloud Manager.

## Supported operating systems

- CentOS 7.6
- CentOS 7.7
- Red Hat Enterprise Linux 7.6
- Red Hat Enterprise Linux 7.7

The Red Hat Enterprise Linux system must be registered with Red Hat Subscription Management. If it is not registered, the system cannot access repositories to update required 3rd party software during Connector installation.

The Connector is supported on English-language versions of these operating systems.

## Hypervisor

A bare metal or hosted hypervisor that is certified to run CentOS or Red Hat Enterprise Linux

[Red Hat Solution: Which hypervisors are certified to run Red Hat Enterprise Linux?](#)

## Disk space in /opt

100 GB of space must be available

## Outbound internet access

Outbound internet access is required to install the Connector and for the Connector to manage resources and processes within your public cloud environment. For a list of endpoints, see [Networking requirements for the Connector](#).

## Creating a Connector from the AWS Marketplace

It's best to create a Connector directly from Cloud Manager, but you can launch a Connector from the AWS Marketplace, if you'd rather not specify AWS access keys. After

you create and set up the Connector, Cloud Manager will automatically use it when you create new working environments.

## Steps

1. Create an IAM policy and role for the EC2 instance:
  - a. Download the Cloud Manager IAM policy from the following location:

[NetApp Cloud Manager: AWS, Azure, and GCP Policies](#)
  - b. From the IAM console, create your own policy by copying and pasting the text from the Cloud Manager IAM policy.
  - c. Create an IAM role with the role type Amazon EC2 and attach the policy that you created in the previous step to the role.
2. Now go to the [Cloud Manager page on the AWS Marketplace](#) to deploy Cloud Manager from an AMI.

The IAM user must have AWS Marketplace permissions to subscribe and unsubscribe.
3. On the Marketplace page, click **Continue to Subscribe** and then click **Continue to Configuration**.

**a**

Cloud Manager - Manual Installation without access keys

By: [NetApp, Inc.](#) Latest Version: 3.8.4

Read below for instructions on how to deploy Cloud Volumes ONTAP.

Linux/Unix ★★★★★ 6 AWS reviews

Overview Pricing Usage Support Reviews

**Product Overview**

Do NOT subscribe on this page unless instructed by NetApp or redirected here from the NetApp website.

This listing lets you manually launch a Cloud Manager instance without providing your AWS credentials. After launching the Cloud Manager software in AWS, you can access it by entering the instance's IP address in a web browser. If you subscribe here, you still need to subscribe on the listing below for PAYGO charges.

**Highlights**

- See Product Overview for instructions on how to deploy NetApp Cloud Manager.

**b**

Cloud Manager - Manual Installation without access keys

< Product Detail [Subscribe](#)

## Subscribe to this software

You're subscribed to this software. Please see the terms and pricing details below or click the button above to configure your software.

### Terms and Conditions

**NetApp, Inc. Offer**

You have subscribed to this software and agreed that your use of this software is subject to the pricing terms and the seller's [End User License Agreement \(EULA\)](#). You agreed that AWS may share information about this transaction (including your payment terms) with the respective seller, reseller or underlying provider, as applicable, in accordance with the [AWS Privacy Notice](#). Your use of AWS services remains subject to the [AWS Customer Agreement](#) or other agreement with AWS governing your use of such services.

4. Change any of the default options and click **Continue to Launch**.

5. Under **Choose Action**, select **Launch through EC2** and then click **Launch**.

These steps describe how to launch the instance from the EC2 Console because the console enables you to attach an IAM role to the Cloud Manager instance. This isn't possible using the **Launch from Website** action.

6. Follow the prompts to configure and deploy the instance:

- **Choose Instance Type:** Depending on region availability, choose one of the supported instance types (t3.xlarge is recommended).

[Review the instance requirements](#).

- **Configure Instance:** Select a VPC and subnet, choose the IAM role that you created in step 1, enable termination protection (recommended), and choose any other configuration options that meet your requirements.

Number of instances	<input type="text" value="1"/>	Launch into Auto Scaling Group
Purchasing option	<input type="checkbox"/> Request Spot instances	
Network	vpc-a76d91c2   VPC4QA (default)	<input type="button" value="Create new VPC"/>
Subnet	subnet-39536c13   QASubnet1   us-east-1b 155 IP Addresses available	<input type="button" value="Create new subnet"/>
Auto-assign Public IP	Enable	
Placement group	<input type="checkbox"/> Add instance to placement group	
Capacity Reservation	Open	
IAM role	Cloud_Manager	<input type="button" value="Create new IAM role"/>
CPU options	<input type="checkbox"/> Specify CPU options	
Shutdown behavior	Stop	
Enable termination protection	<input checked="" type="checkbox"/> Protect against accidental termination	
Monitoring	<input type="checkbox"/> Enable CloudWatch detailed monitoring <small>Additional charges apply.</small>	

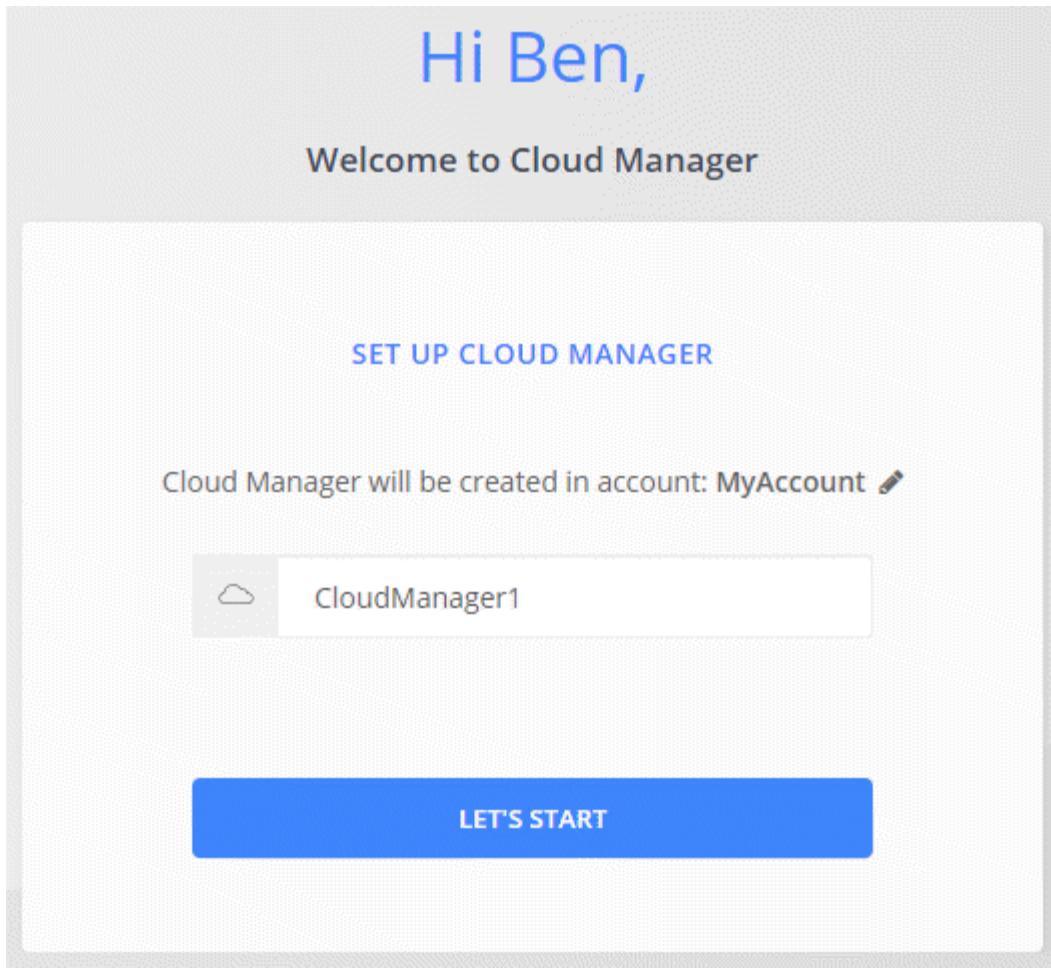
- **Add Storage:** Keep the default storage options.
- **Add Tags:** Enter tags for the instance, if desired.
- **Configure Security Group:** Specify the required connection methods for the Connector instance: SSH, HTTP, and HTTPS.
- **Review:** Review your selections and click **Launch**.

AWS launches the software with the specified settings. The Connector instance and software should be running in approximately five minutes.

7. Open a web browser from a host that has a connection to the Connector instance and enter the following URL:

<http://ipaddress:80>

8. After you log in, set up the Connector:
  - Specify the Cloud Central account to associate with the Connector.  
[Learn about Cloud Central accounts.](#)
  - Enter a name for the system.



## Result

The Connector is now installed and set up with your Cloud Central account. Cloud Manager will automatically use this Connector when you create new working environments. But if you have more than one Connector, you'll need to [switch between them](#).

## Creating a Connector from the Azure Marketplace

It's best to create a Connector directly from Cloud Manager, but you can launch a Connector from the Azure Marketplace, if you prefer. After you create and set up the Connector, Cloud Manager will automatically use it when you create new working environments.

### Creating a Connector in Azure

Deploy the Connector in Azure using the image in the Azure Marketplace and then log in to the Connector to specify your Cloud Central account.

### Steps

1. [Go to the Azure Marketplace page for Cloud Manager](#).
2. Click **Get it now** and then click **Continue**.
3. From the Azure portal, click **Create** and follow the steps to configure the virtual machine.

Note the following as you configure the VM:

- Cloud Manager can perform optimally with either HDD or SSD disks.
- Choose a VM size that meets CPU and RAM requirements. We recommend DS3 v2.

[Review the VM requirements.](#)

- For the network security group, the Connector requires inbound connections using SSH, HTTP, and HTTPS.

[Learn more about security group rules for the Connector.](#)

- Under **Management**, enable **System assigned managed identity** for the Connector by selecting **On**.

This setting is important because a managed identity allows the Connector virtual machine to identify itself to Azure Active Directory without providing any credentials. [Learn more about managed identities for Azure resources.](#)

4. On the **Review + create** page, review your selections and click **Create** to start the deployment.

Azure deploys the virtual machine with the specified settings. The virtual machine and Connector software should be running in approximately five minutes.

5. Open a web browser from a host that has a connection to the Connector virtual machine and enter the following URL:

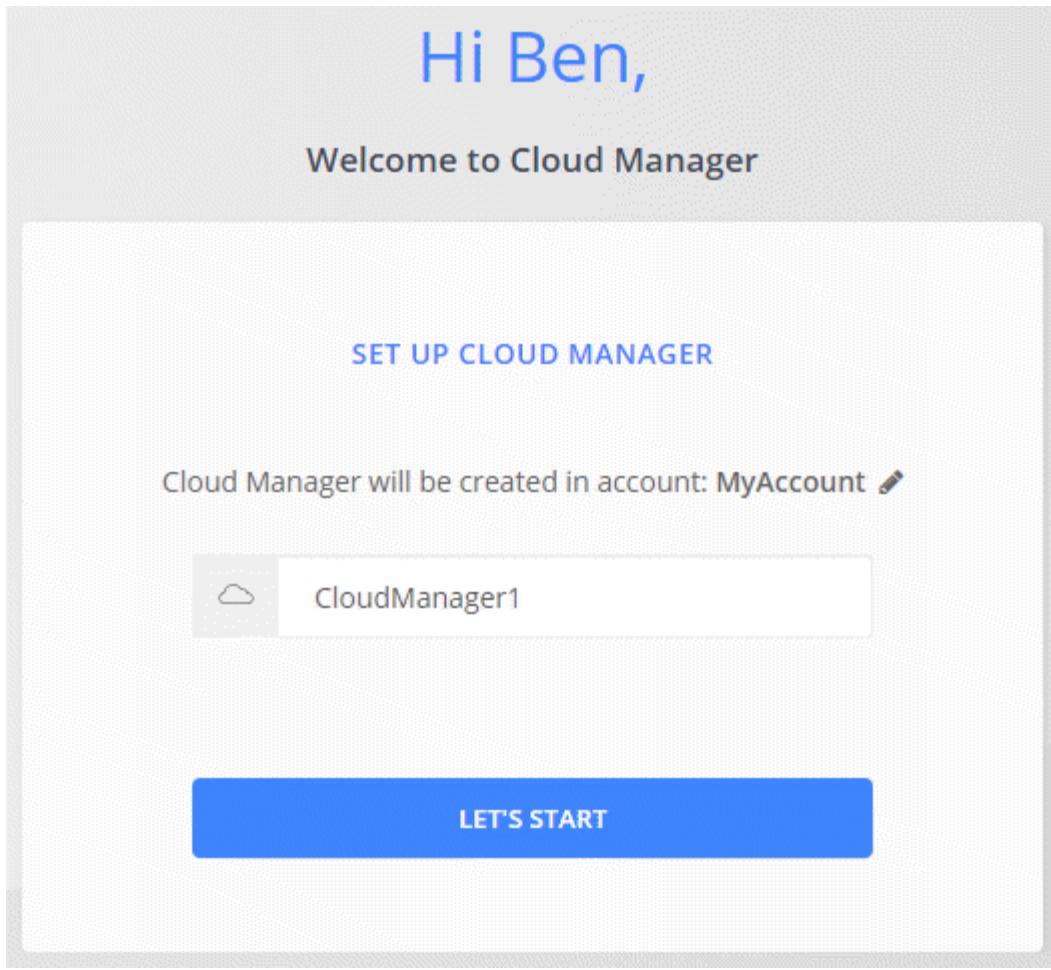
`http://ipaddress:80`

6. After you log in, set up the Connector:

- a. Specify the Cloud Central account to associate with the Connector.

[Learn about Cloud Central accounts.](#)

- b. Enter a name for the system.



## Result

The Connector is now installed and set up. You must grant Azure permissions before users can deploy Cloud Volumes ONTAP in Azure.

### Granting Azure permissions

When you deployed the Connector in Azure, you should have enabled a [system-assigned managed identity](#). You must now grant the required Azure permissions by creating a custom role and then by assigning the role to the Connector virtual machine for one or more subscriptions.

### Steps

1. Create a custom role using the Cloud Manager policy:
  - a. Download the [Cloud Manager Azure policy](#).
  - b. Modify the JSON file by adding Azure subscription IDs to the assignable scope.

You should add the ID for each Azure subscription from which users will create Cloud Volumes ONTAP systems.

### Example

```
"AssignableScopes": [  
    "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzz",  
    "/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzz",  
    "/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzz"
```

- c. Use the JSON file to create a custom role in Azure.

The following example shows how to create a custom role using the Azure CLI 2.0:

```
az role definition create --role-definition  
C:\Policy_for_cloud_Manager_Azure_3.8.7.json
```

You should now have a custom role called Cloud Manager Operator that you can assign to the Connector virtual machine.

2. Assign the role to the Connector virtual machine for one or more subscriptions:

- a. Open the **Subscriptions** service and then select the subscription in which you want to deploy Cloud Volumes ONTAP systems.
- b. Click **Access control (IAM)**.
- c. Click **Add > Add role assignment** and then add the permissions:
  - Select the **Cloud Manager Operator** role.



Cloud Manager Operator is the default name provided in the [Cloud Manager policy](#). If you chose a different name for the role, then select that name instead.

- d. Assign access to a **Virtual Machine**.
  - Select the subscription in which the Connector virtual machine was created.
  - Select the Connector virtual machine.
  - Click **Save**.
- d. If you want to deploy Cloud Volumes ONTAP from additional subscriptions, switch to that subscription and then repeat these steps.

## Result

The Connector now has the permissions that it needs to manage resources and processes within your public cloud environment. Cloud Manager will automatically use this Connector when you create new working environments. But if you have more than one Connector, you'll need to [switch between them](#).

## Installing the Connector software on an existing Linux host

The most common way to create a Connector is directly from Cloud Manager or from a cloud provider's marketplace. But you have the option to download and install the Connector software on an existing Linux host in your network or in the cloud.



If you want to create a Cloud Volumes ONTAP system in Google Cloud, then you must have a Connector running in Google Cloud, as well. You can't use a Connector that's running in another location.

## Requirements

- The host must meet [requirements for the Connector](#).
- A Red Hat Enterprise Linux system must be registered with Red Hat Subscription Management. If it is not registered, the system cannot access repositories to update required 3rd party software during installation.
- The Connector installer accesses several URLs during the installation process. You must ensure that outbound internet access is allowed to these endpoints:

- <http://dev.mysql.com/get/mysql-community-release-el7-5.noarch.rpm>
- <https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm>
- <https://s3.amazonaws.com/aws-cli/awscli-bundle.zip>

The host might try to update operating system packages during installation. The host can contact different mirroring sites for these OS packages.

## About this task

- Root privileges are not required to install the Connector.
- The installation installs the AWS command line tools (awscli) to enable recovery procedures from NetApp support.

If you receive a message that installing the awscli failed, you can safely ignore the message. The Connector can operate successfully without the tools.

- The installer that is available on the NetApp Support Site might be an earlier version. After installation, the Connector automatically updates itself if a new version is available.

## Steps

1. Download the Cloud Manager software from the [NetApp Support Site](#), and then copy it to the Linux host.

For help with connecting and copying the file to an EC2 instance in AWS, see [AWS Documentation: Connecting to Your Linux Instance Using SSH](#).

2. Assign permissions to execute the script.

### Example

```
chmod +x OnCommandCloudManager-V3.8.9.sh
```

3. Run the installation script:

```
./OnCommandCloudManager-V3.8.9.sh [silent] [proxy=ipaddress]
[proxyport=port] [proxyuser=user_name] [proxypwd=password]
```

*silent* runs the installation without prompting you for information.

*proxy* is required if the host is behind a proxy server.

*proxyport* is the port for the proxy server.

*proxyuser* is the user name for the proxy server, if basic authentication is required.

*proxypwd* is the password for the user name that you specified.

4. Unless you specified the silent parameter, type **Y** to continue the script, and then enter the HTTP and HTTPS ports when prompted.

Cloud Manager is now installed. At the end of the installation, the Cloud Manager service (occm) restarts

twice if you specified a proxy server.

5. Open a web browser and enter the following URL:

<https://ipaddress:port>

*ipaddress* can be localhost, a private IP address, or a public IP address, depending on the configuration of the host. For example, if the Connector is in the public cloud without a public IP address, you must enter a private IP address from a host that has a connection to the Connector host.

*port* is required if you changed the default HTTP (80) or HTTPS (443) ports. For example, if the HTTPS port was changed to 8443, you would enter <https://ipaddress:8443>

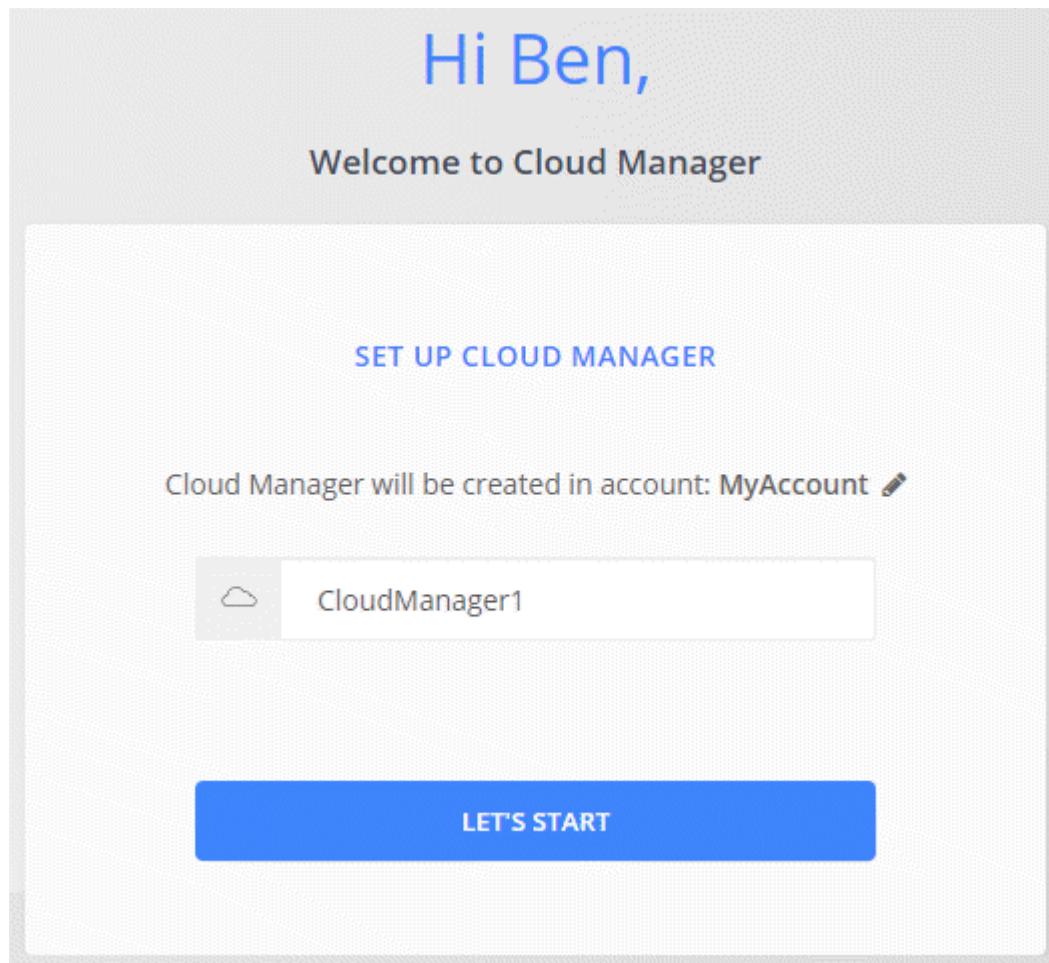
6. Sign up at NetApp Cloud Central or log in.

7. After you log in, set up Cloud Manager:

- Specify the Cloud Central account to associate with the Connector.

[Learn about Cloud Central accounts.](#)

- Enter a name for the system.



## Result

The Connector is now installed and set up with your Cloud Central account. Cloud Manager will automatically use this Connector when you create new working environments.

## After you finish

Set up permissions so Cloud Manager can manage resources and processes within your public cloud environment:

- AWS: [Set up an AWS account and then add it to Cloud Manager](#).
- Azure: [Set up an Azure account and then add it to Cloud Manager](#).
- GCP: Set up a service account that has the permissions that Cloud Manager needs to create and manage Cloud Volumes ONTAP systems in projects.
  1. [Create a role in GCP](#) that includes the permissions defined in the [Cloud Manager policy for GCP](#).
  2. [Create a GCP service account and apply the custom role that you just created](#).
  3. [Associate this service account with the Connector VM](#).
  4. If you want to deploy Cloud Volumes ONTAP in other projects, [grant access by adding the service account with the Cloud Manager role to that project](#). You'll need to repeat this step for each project.

## Default configuration for the Connector

If you need to troubleshoot the Connector, it might help to understand how it's configured.

- If you deployed the Connector from Cloud Manager (or directly from a cloud provider's marketplace), note the following:
  - In AWS, the user name for the EC2 Linux instance is ec2-user.
  - The operating system for the image is as follows:
    - AWS: Red Hat Enterprise Linux 7.5 (HVM)
    - Azure: Red Hat Enterprise Linux 7.6 (HVM)
    - GCP: CentOS 7.6

The operating system does not include a GUI. You must use a terminal to access the system.

- The Connector installation folder resides in the following location:

/opt/application/netapp/cloudmanager

- Log files are contained in the following folder:

/opt/application/netapp/cloudmanager/log

- The Cloud Manager service is named occm.
- The occm service is dependent on the MySQL service.

If the MySQL service is down, then the occm service is down too.

- Cloud Manager installs the following packages on the Linux host, if they are not already installed:
  - 7Zip
  - AWSCLI
  - Docker
  - Java

- Kubectl
- MySQL
- Tridentctl
- Pull
- Wget
- The Connector uses the following ports on the Linux host:
  - 80 for HTTP access
  - 443 for HTTPS access
  - 3306 for the Cloud Manager database
  - 8080 for the Cloud Manager API proxy
  - 8666 for the Service Manager API
  - 8777 for the Health-Checker Container Service API

## Manage credentials

### AWS

#### AWS credentials and permissions

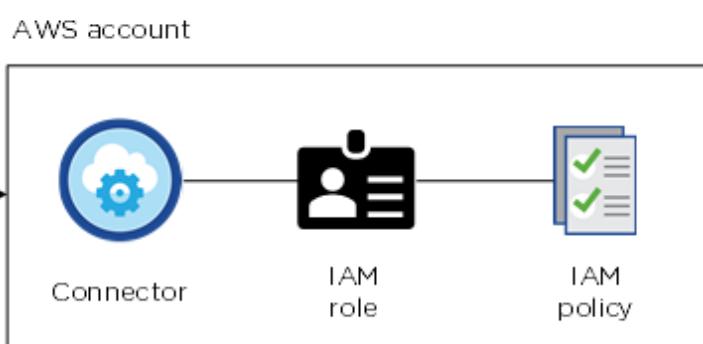
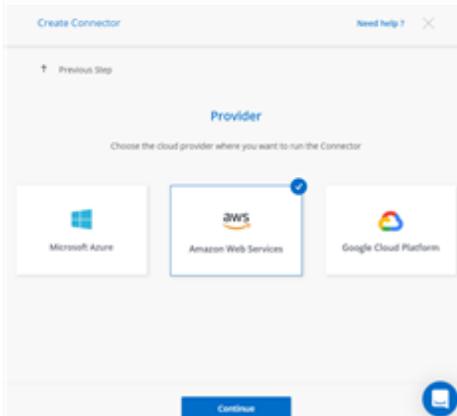
Cloud Manager enables you to choose the AWS credentials to use when deploying Cloud Volumes ONTAP. You can deploy all of your Cloud Volumes ONTAP systems using the initial AWS credentials, or you can add additional credentials.

##### Initial AWS credentials

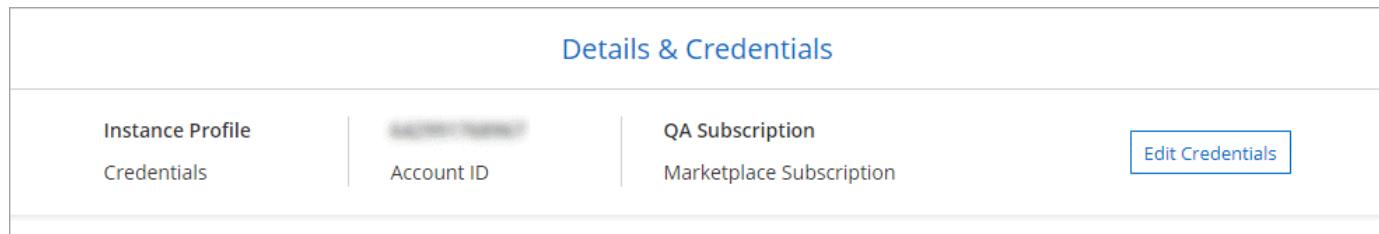
When you deploy a Connector from Cloud Manager, you need to use an AWS account that has permissions to launch the Connector instance. The required permissions are listed in the [Connector deployment policy for AWS](#).

When Cloud Manager launches the Connector instance in AWS, it creates an IAM role and an instance profile for the instance. It also attaches a policy that provides Cloud Manager with permissions to manage resources and processes within that AWS account. [Review how Cloud Manager uses the permissions](#).

#### Cloud Manager

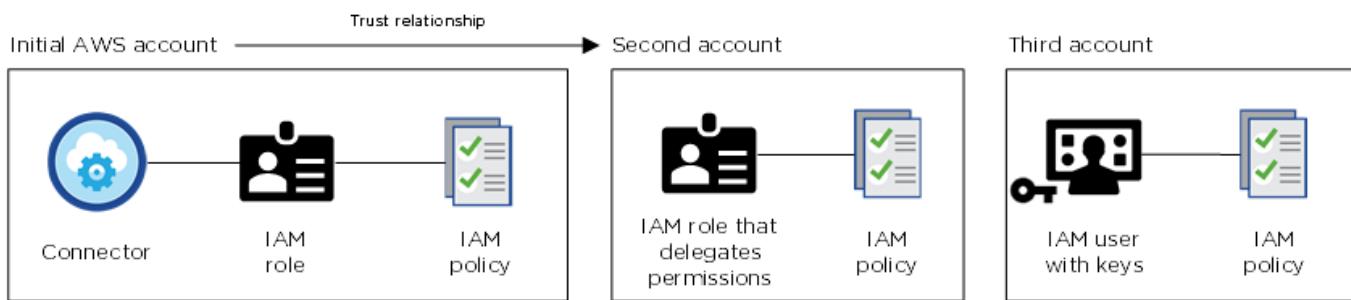


Cloud Manager selects these AWS credentials by default when you create a new working environment for Cloud Volumes ONTAP:



#### Additional AWS credentials

If you want to launch Cloud Volumes ONTAP in different AWS accounts, then you can either [provide AWS keys for an IAM user or the ARN of a role in a trusted account](#). The following image shows two additional accounts, one providing permissions through an IAM role in a trusted account and another through the AWS keys of an IAM user:

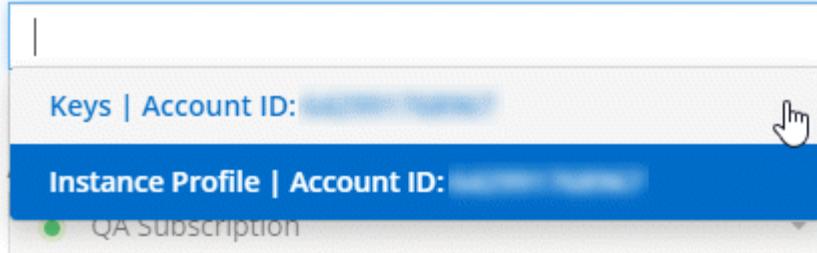


You would then [add the account credentials to Cloud Manager](#) by specifying the Amazon Resource Name (ARN) of the IAM role, or the AWS keys for the IAM user.

After you add another set of credentials, you can switch to them when creating a new working environment:

## Edit Account & Add Subscription

### Credentials



### Associate Subscription to Credentials

To create a pay-as-you-go Cloud Volumes ONTAP system, you need to select AWS credentials that are associated with a subscription to Cloud Volumes ONTAP from the AWS Marketplace.

 [Add Subscription](#)

[Apply](#)

[Cancel](#)

### What about Marketplace deployments and on-prem deployments?

The sections above describe the recommended deployment method for the Connector, which is from Cloud Manager. You can also deploy a Connector in AWS from the [AWS Marketplace](#) and you can [install the Connector on-premises](#).

If you use the Marketplace, permissions are provided in the same way. You just need to manually create and set up the IAM role, and then provide permissions for any additional accounts.

For on-premises deployments, you can't set up an IAM role for the Cloud Manager system, but you can provide permissions just like you would for additional AWS accounts.

### How can I securely rotate my AWS credentials?

As described above, Cloud Manager enables you to provide AWS credentials in a few ways: an IAM role associated with the Connector instance, by assuming an IAM role in a trusted account, or by providing AWS

access keys.

With the first two options, Cloud Manager uses the AWS Security Token Service to obtain temporary credentials that rotate constantly. This process is the best practice—it's automatic and it's secure.

If you provide Cloud Manager with AWS access keys, you should rotate the keys by updating them in Cloud Manager at a regular interval. This is a completely manual process.

## Managing AWS credentials and subscriptions for Cloud Manager

When you create a Cloud Volumes ONTAP system, you need to select the AWS credentials and subscription to use with that system. If you manage multiple AWS subscriptions, you can assign each one of them to different AWS credentials from the Credentials page.

Before you add AWS credentials to Cloud Manager, you need to provide the required permissions to that account. The permissions enable Cloud Manager to manage resources and processes within that AWS account. How you provide the permissions depends on whether you want to provide Cloud Manager with AWS keys or the ARN of a role in a trusted account.



When you deployed a Connector from Cloud Manager, Cloud Manager automatically added AWS credentials for the account in which you deployed the Connector. This initial account is not added if you manually installed the Connector software on an existing system. [Learn about AWS credentials and permissions](#).

### Choices

- [Granting permissions by providing AWS keys](#)
- [Granting permissions by assuming IAM roles in other accounts](#)

### How can I securely rotate my AWS credentials?

Cloud Manager enables you to provide AWS credentials in a few ways: an IAM role associated with the Connector instance, by assuming an IAM role in a trusted account, or by providing AWS access keys. [Learn more about AWS credentials and permissions](#).

With the first two options, Cloud Manager uses the AWS Security Token Service to obtain temporary credentials that rotate constantly. This process is the best practice, it's automatic and it's secure.

If you provide Cloud Manager with AWS access keys, you should rotate the keys by updating them in Cloud Manager at a regular interval. This is a completely manual process.

### Granting permissions by providing AWS keys

If you want to provide Cloud Manager with AWS keys for an IAM user, then you need to grant the required permissions to that user. The Cloud Manager IAM policy defines the AWS actions and resources that Cloud Manager is allowed to use.

### Steps

1. Download the Cloud Manager IAM policy from the [Cloud Manager Policies page](#).
2. From the IAM console, create your own policy by copying and pasting the text from the Cloud Manager

IAM policy.

[AWS Documentation: Creating IAM Policies](#)

### 3. Attach the policy to an IAM role or an IAM user.

- [AWS Documentation: Creating IAM Roles](#)
- [AWS Documentation: Adding and Removing IAM Policies](#)

## Result

The account now has the required permissions. [You can now add it to Cloud Manager.](#)

### Granting permissions by assuming IAM roles in other accounts

You can set up a trust relationship between the source AWS account in which you deployed the Connector instance and other AWS accounts by using IAM roles. You would then provide Cloud Manager with the ARN of the IAM roles from the trusted accounts.

## Steps

### 1. Go to the target account where you want to deploy Cloud Volumes ONTAP and create an IAM role by selecting **Another AWS account**.

Be sure to do the following:

- Enter the ID of the account where the Connector instance resides.
- Attach the Cloud Manager IAM policy, which is available from the [Cloud Manager Policies page](#).

### 2. Go to the source account where the Connector instance resides and select the IAM role that is attached to the instance.

#### a. Click **Attach policies** and then click **Create policy**.

#### b. Create a policy that includes the "sts:AssumeRole" action and the ARN of the role that you created in the target account.

## Example

```
{  
    "Version": "2012-10-17",  
    "Statement": {  
        "Effect": "Allow",  
        "Action": "sts:AssumeRole",  
        "Resource": "arn:aws:iam::ACCOUNT-B-ID:role/ACCOUNT-B-ROLENAME"  
    }  
}
```

## Result

The account now has the required permissions. [You can now add it to Cloud Manager.](#)

## Adding AWS credentials to Cloud Manager

After you provide an AWS account with the required permissions, you can add the credentials for that account to Cloud Manager. This enables you to launch Cloud Volumes ONTAP systems in that account.

### Steps

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



2. Click **Add Credentials** and select **AWS**.
3. Provide AWS keys or the ARN of a trusted IAM role.
4. Confirm that the policy requirements have been met and click **Continue**.
5. Choose the pay-as-you-go subscription that you want to associate with the credentials, or click **Add Subscription** if you don't have one yet.

To create a pay-as-you-go Cloud Volumes ONTAP system, AWS credentials must be associated with a subscription to Cloud Volumes ONTAP from the AWS Marketplace.

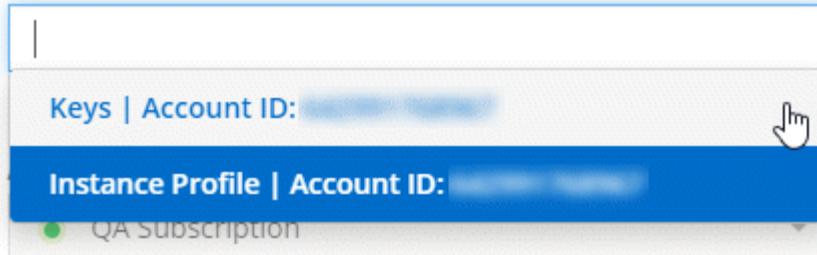
6. Click **Add**.

### Result

You can now switch to a different set of credentials from the Details and Credentials page when creating a new working environment:

## Edit Account & Add Subscription

### Credentials



### Associate Subscription to Credentials

To create a pay-as-you-go Cloud Volumes ONTAP system, you need to select AWS credentials that are associated with a subscription to Cloud Volumes ONTAP from the AWS Marketplace.

 [Add Subscription](#)

[Apply](#)

[Cancel](#)

### Associating an AWS subscription to credentials

After you add your AWS credentials to Cloud Manager, you can associate an AWS Marketplace subscription with those credentials. The subscription enables you to create a pay-as-you-go Cloud Volumes ONTAP system, and to use other NetApp cloud services.

There are two scenarios in which you might associate an AWS Marketplace subscription after you've already added the credentials to Cloud Manager:

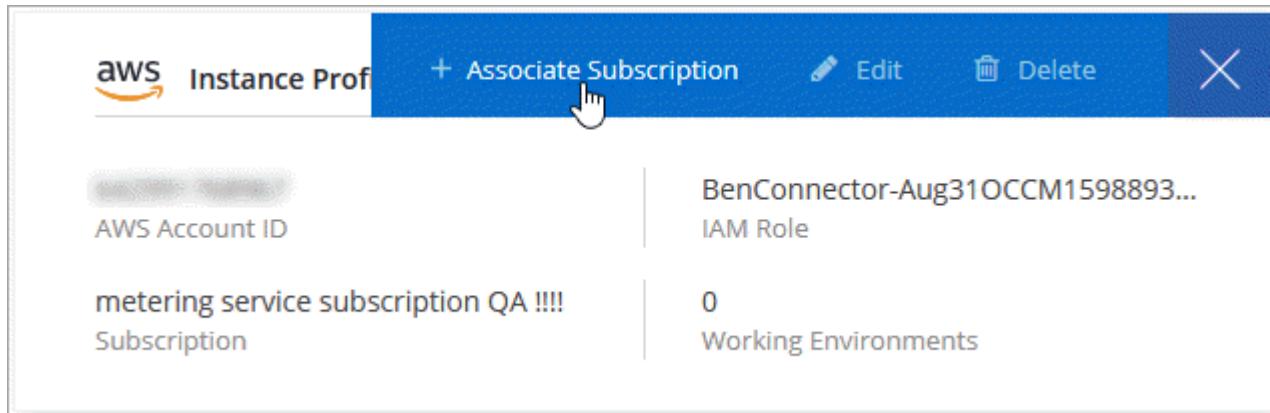
- You didn't associate a subscription when you initially added the credentials to Cloud Manager.
- You want to replace an existing AWS Marketplace subscription with a new subscription.

### What you'll need

You need to create a Connector before you can change Cloud Manager settings. [Learn how.](#)

### Steps

1. In the upper right of the Cloud Manager console, click the Settings icon, and select **Credentials**.
2. Hover over a set of credentials and click the action menu.
3. From the menu, click **Associate Subscription**.



4. Select a subscription from the down-down list or click **Add Subscription** and follow the steps to create a new subscription.

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

## Azure

### Azure credentials and permissions

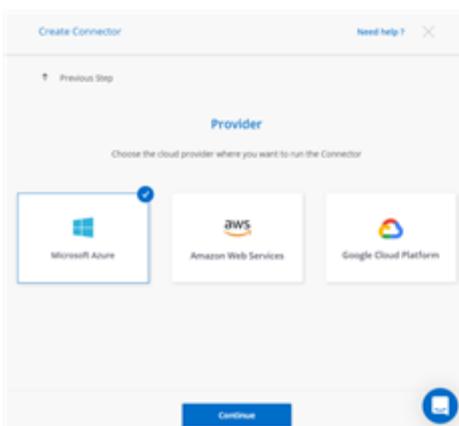
Cloud Manager enables you to choose the Azure credentials to use when deploying Cloud Volumes ONTAP. You can deploy all of your Cloud Volumes ONTAP systems using the initial Azure credentials, or you can add additional credentials.

#### Initial Azure credentials

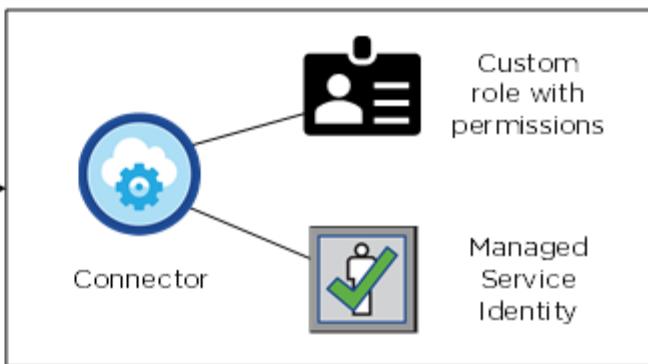
When you deploy a Connector from Cloud Manager, you need to use an Azure account that has permissions to deploy the Connector virtual machine. The required permissions are listed in the [Connector deployment policy for Azure](#).

When Cloud Manager deploys the Connector virtual machine in Azure, it enables a [system-assigned managed identity](#) on virtual machine, creates a custom role, and assigns it to the virtual machine. The role provides Cloud Manager with permissions to manage resources and processes within that Azure subscription. [Review how Cloud Manager uses the permissions](#).

## Cloud Manager



## Azure account



Cloud Manager selects these Azure credentials by default when you create a new working environment for Cloud Volumes ONTAP:

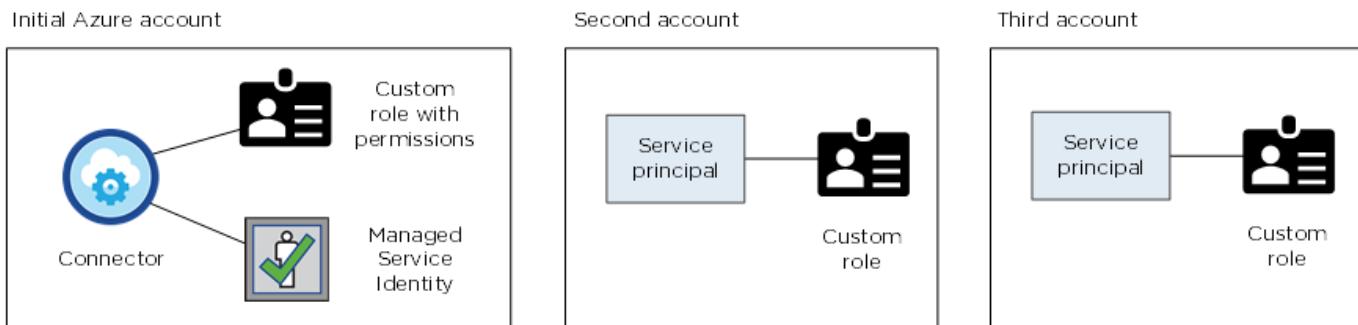
This screenshot shows the 'Details & Credentials' section. It displays the following information: Managed Service Ide... (Credential Name: OCCM QA1), Azure Subscription (Subscription Type: Marketplace Subscription), and a note indicating 'No subscription is associated'. A blue 'Edit Credentials' button is located on the right.

### Additional Azure subscriptions for a managed identity

The managed identity is associated with the subscription in which you launched the Connector. If you want to select a different Azure subscription, then you need to [associate the managed identity with those subscriptions](#).

### Additional Azure credentials

If you want to deploy Cloud Volumes ONTAP using different Azure credentials, then you must grant the required permissions by [creating and setting up a service principal in Azure Active Directory](#) for each Azure account. The following image shows two additional accounts, each set up with a service principal and custom role that provides permissions:



You would then [add the account credentials to Cloud Manager](#) by providing details about the AD service principal.

After you add another set of credentials, you can switch to them when creating a new working environment:

## Edit Account & Add Subscription

### Credentials

The screenshot shows a dropdown menu with the following options:

- cloud-manager-app | Application ID: 57c42424-88a0-480a.
- Managed Service Identity** (highlighted in blue)
- OCCM QA1 (Default)

### What about Marketplace deployments and on-prem deployments?

The sections above describe the recommended deployment method for the Connector, which is from NetApp Cloud Central. You can also deploy a Connector in Azure from the [Azure Marketplace](#), and you can [install the Connector on-premises](#).

If you use the Marketplace, permissions are provided in the same way. You just need to manually create and set up the managed identity for the Connector, and then provide permissions for any additional accounts.

For on-premises deployments, you can't set up a managed identity for the Connector, but you can provide permissions just like you would for additional accounts by using a service principal.

### Managing Azure credentials and subscriptions for Cloud Manager

When you create a Cloud Volumes ONTAP system, you need to select the Azure credentials and Marketplace subscription to use with that system. If you manage multiple Azure Marketplace subscriptions, you can assign each one of them to different Azure credentials from the Credentials page.

There are two ways to manage Azure credentials in Cloud Manager. First, if you want to deploy Cloud Volumes ONTAP in different Azure accounts, then you need to provide the required permissions and add the credentials to Cloud Manager. The second way is to associate additional subscriptions with the Azure managed identity.



When you deploy a Connector from Cloud Manager, Cloud Manager automatically adds the Azure account in which you deployed the Connector. An initial account is not added if you manually installed the Connector software on an existing system. [Learn about Azure accounts and permissions](#).

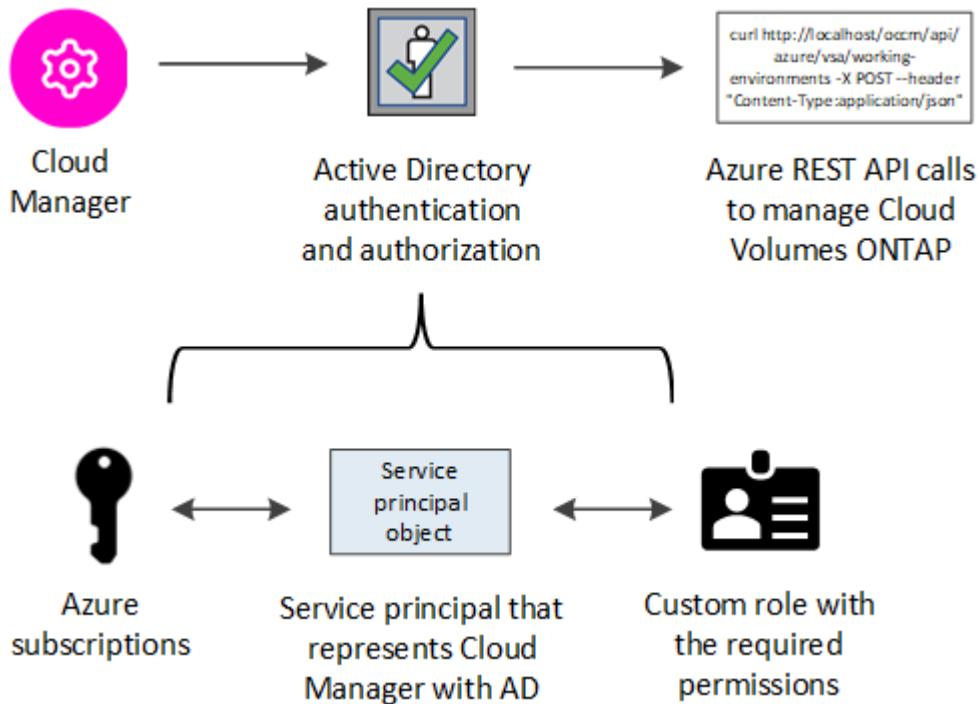
### Granting Azure permissions using a service principal

Cloud Manager needs permissions to perform actions in Azure. You can grant the required permissions to an Azure account by creating and setting up a service principal in Azure Active Directory and by obtaining the

Azure credentials that Cloud Manager needs.

### About this task

The following image depicts how Cloud Manager obtains permissions to perform operations in Azure. A service principal object, which is tied to one or more Azure subscriptions, represents Cloud Manager in Azure Active Directory and is assigned to a custom role that allows the required permissions.



### Steps

1. [Create an Azure Active Directory application](#).
2. [Assign the application to a role](#).
3. [Add Windows Azure Service Management API permissions](#).
4. [Get the application ID and directory ID](#).
5. [Create a client secret](#).

### Creating an Azure Active Directory application

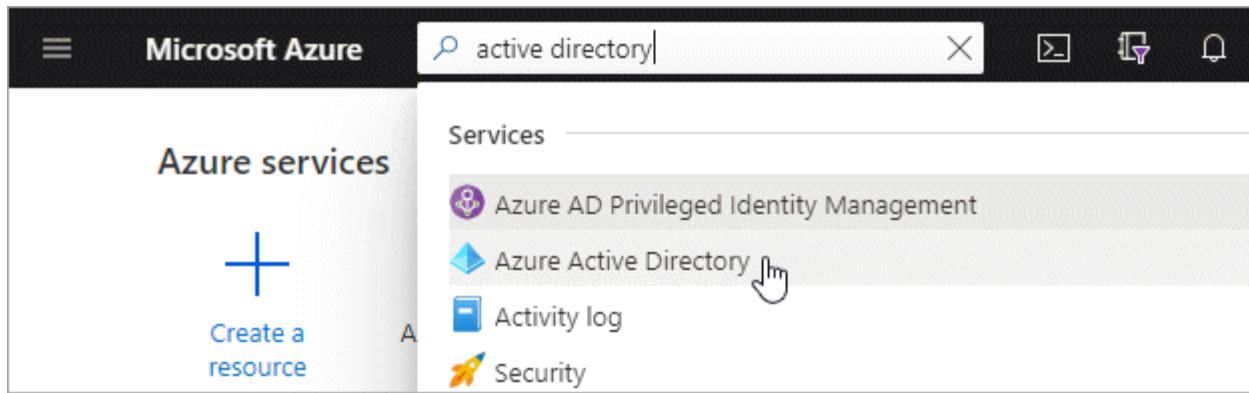
Create an Azure Active Directory (AD) application and service principal that Cloud Manager can use for role-based access control.

#### Before you begin

You must have the right permissions in Azure to create an Active Directory application and to assign the application to a role. For details, refer to [Microsoft Azure Documentation: Required permissions](#).

### Steps

1. From the Azure portal, open the **Azure Active Directory** service.



2. In the menu, click **App registrations**.
3. Click **New registration**.
4. Specify details about the application:
  - **Name:** Enter a name for the application.
  - **Account type:** Select an account type (any will work with Cloud Manager).
  - **Redirect URI:** You can leave this field blank.
5. Click **Register**.

## Result

You've created the AD application and service principal.

## Assigning the application to a role

You must bind the service principal to one or more Azure subscriptions and assign it the custom "OnCommand Cloud Manager Operator" role so Cloud Manager has permissions in Azure.

## Steps

1. Create a custom role:
  - a. Download the [Cloud Manager Azure policy](#).
  - b. Modify the JSON file by adding Azure subscription IDs to the assignable scope.

You should add the ID for each Azure subscription from which users will create Cloud Volumes ONTAP systems.

## Example

```
"AssignableScopes": [  
    "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzz",  
    "/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzz",  
    "/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzz"
```

- c. Use the JSON file to create a custom role in Azure.

The following example shows how to create a custom role using the Azure CLI 2.0:

```
az role definition create --role-definition
```

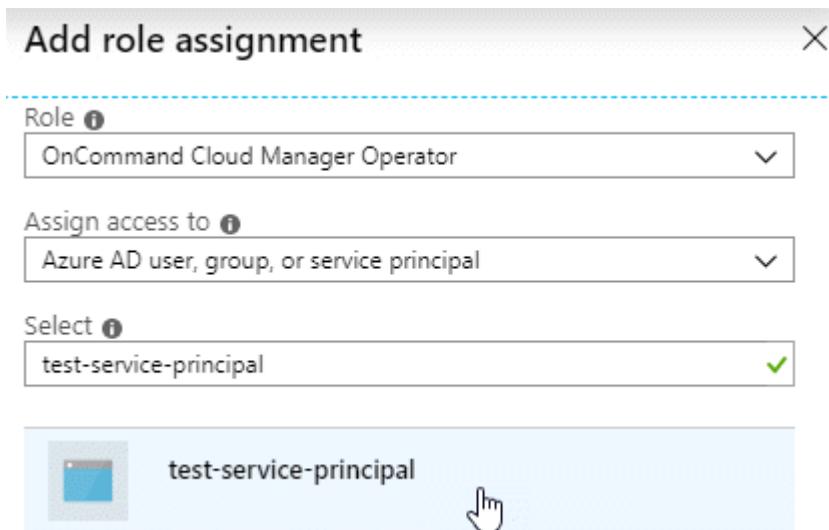
C:\Policy\_for\_cloud\_Manager\_Azure\_3.8.7.json

You should now have a custom role called *Cloud Manager Operator*.

2. Assign the application to the role:

- a. From the Azure portal, open the **Subscriptions** service.
- b. Select the subscription.
- c. Click **Access control (IAM) > Add > Add role assignment**.
- d. Select the **Cloud Manager Operator** role.
- e. Keep **Azure AD user, group, or service principal** selected.
- f. Search for the name of the application (you can't find it in the list by scrolling).

Here's an example:



- g. Select the application and click **Save**.

The service principal for Cloud Manager now has the required Azure permissions for that subscription.

If you want to deploy Cloud Volumes ONTAP from multiple Azure subscriptions, then you must bind the service principal to each of those subscriptions. Cloud Manager enables you to select the subscription that you want to use when deploying Cloud Volumes ONTAP.

## Adding Windows Azure Service Management API permissions

The service principal must have "Windows Azure Service Management API" permissions.

### Steps

1. In the **Azure Active Directory** service, click **App registrations** and select the application.
2. Click **API permissions > Add a permission**.
3. Under **Microsoft APIs**, select **Azure Service Management**.

## Request API permissions

### Select an API

[Microsoft APIs](#) [APIs my organization uses](#) [My APIs](#)

#### Commonly used Microsoft APIs

##### Microsoft Graph

Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.



##### Azure Batch

Schedule large-scale parallel and HPC applications in the cloud

##### Azure Data Lake

Access to storage and compute for big data analytic scenarios

##### Azure Key Vault

Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults

##### Azure Storage

Secure, massively scalable object and data lake storage for unstructured and semi-structured data

##### Azure Data Catalog

Programmatic access to Data Catalog resources to register, annotate and search data assets

##### Azure DevOps

Integrate with Azure DevOps and Azure DevOps server

##### Azure Rights Management Services

Allow validated users to read and write protected content

##### Customer Insights

Create profile and interaction models for your products

##### Azure Data Explorer

Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions

##### Azure Import/Export

Programmatic control of import/export jobs

##### Azure Service Management

Programmatic access to much of the functionality available through the Azure portal

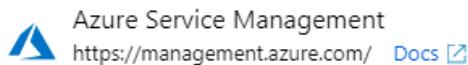
##### Data Export Service for Microsoft Dynamics 365

Export data from Microsoft Dynamics CRM organization to an external destination

4. Click **Access Azure Service Management as organization users** and then click **Add permissions**.

## Request API permissions

&gt;

[All APIs](#)

What type of permissions does your application require?

### Delegated permissions

Your application needs to access the API as the signed-in user.

### Application permissions

Your application runs as a background service or daemon without a signed-in user.

Select permissions

[expand all](#)

Type to search	
PERMISSION	ADMIN CONSENT REQUIRED
<input checked="" type="checkbox"/> <a href="#">user_impersonation</a> Access Azure Service Management as organization users (preview) <small> ⓘ</small>	-

## Getting the application ID and directory ID

When you add the Azure account to Cloud Manager, you need to provide the application (client) ID and the directory (tenant) ID for the application. Cloud Manager uses the IDs to programmatically sign in.

### Steps

1. In the **Azure Active Directory** service, click **App registrations** and select the application.
2. Copy the **Application (client) ID** and the **Directory (tenant) ID**.

The screenshot shows the Azure App Registrations page. At the top, there are 'Delete' and 'Endpoints' buttons. Below that is a message: 'Welcome to the new and improved App registrations. Looking to learn'. The application details are listed:  
Display name : test-service-principal  
Application (client) ID : 73de25f9-99be-4ae0-8b24-538ca787a6b3 (highlighted)  
Directory (tenant) ID : 4b0911a0-929b-4715-944b-c03745165b3a (highlighted)  
Object ID : b37489a9-379f-49c2-b27c-e630514106a5

## Creating a client secret

You need to create a client secret and then provide Cloud Manager with the value of the secret so Cloud Manager can use it to authenticate with Azure AD.



When you add the account to Cloud Manager, Cloud Manager refers to the client secret as the Application Key.

### Steps

1. Open the **Azure Active Directory** service.
2. Click **App registrations** and select your application.
3. Click **Certificates & secrets > New client secret**.
4. Provide a description of the secret and a duration.
5. Click **Add**.
6. Copy the value of the client secret.

### Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.



DESCRIPTION	EXPIRES	VALUE	Copy to clipboard
test secret	8/16/2020	*sZ1jSe2By:D*-ZRov4NLfdAcY7:+0vA	

### Result

Your service principal is now setup and you should have copied the application (client) ID, the directory (tenant) ID, and the value of the client secret. You need to enter this information in Cloud Manager when you add an Azure account.

### Adding Azure credentials to Cloud Manager

After you provide an Azure account with the required permissions, you can add the credentials for that account to Cloud Manager. This enables you to launch Cloud Volumes ONTAP systems in that account.

### What you'll need

You need to create a Connector before you can change Cloud Manager settings. [Learn how](#).

### Steps

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



2. Click **Add Credentials** and select **Microsoft Azure**.
3. Enter information about the Azure Active Directory service principal that grants the required permissions:
  - Application (client) ID: See [Getting the application ID and directory ID](#).
  - Directory (tenant) ID: See [Getting the application ID and directory ID](#).
  - Client Secret: See [Creating a client secret](#).
4. Confirm that the policy requirements have been met and then click **Continue**.
5. Choose the pay-as-you-go subscription that you want to associate with the credentials, or click **Add Subscription** if you don't have one yet.

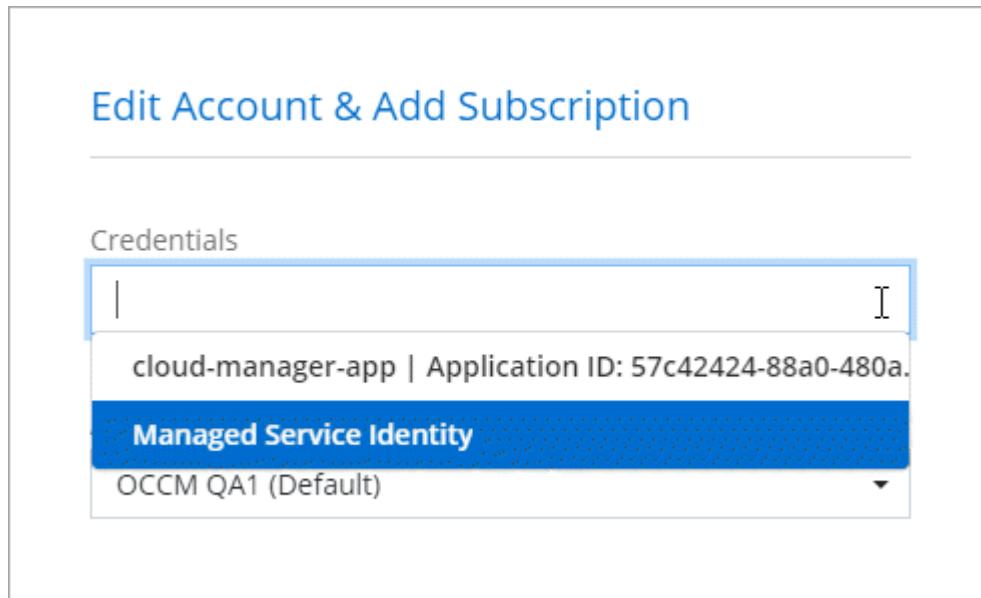
To create a pay-as-you-go Cloud Volumes ONTAP system, Azure credentials must be associated with a

subscription to Cloud Volumes ONTAP from the Azure Marketplace.

## 6. Click **Add**.

### Result

You can now switch to different set of credentials from the Details and Credentials page [when creating a new working environment](#):



### Associating an Azure Marketplace subscription to credentials

After you add your Azure credentials to Cloud Manager, you can associate an Azure Marketplace subscription to those credentials. The subscription enables you to create a pay-as-you-go Cloud Volumes ONTAP system, and to use other NetApp cloud services.

There are two scenarios in which you might associate an Azure Marketplace subscription after you've already added the credentials to Cloud Manager:

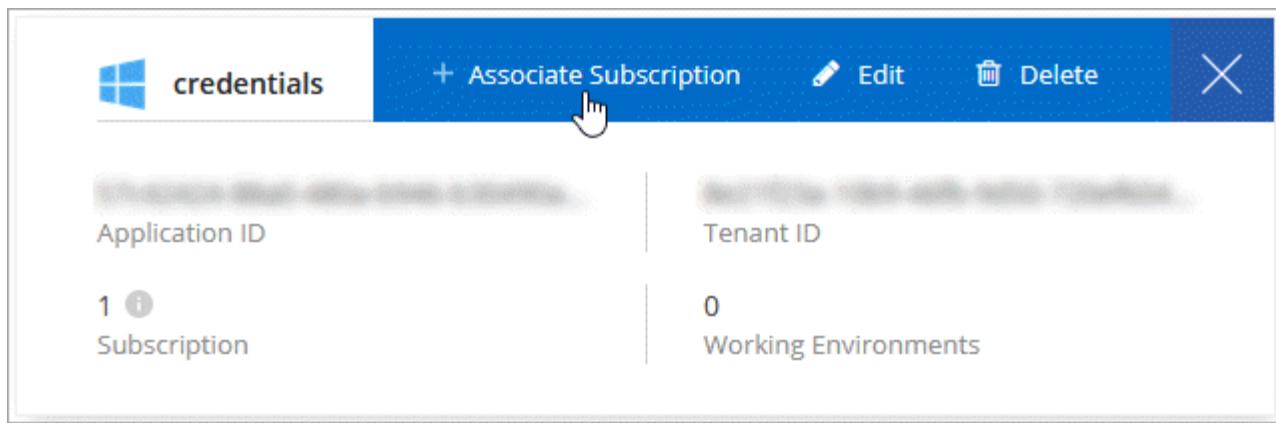
- You didn't associate a subscription when you initially added the credentials to Cloud Manager.
- You want to replace an existing Azure Marketplace subscription with a new subscription.

### What you'll need

You need to create a Connector before you can change Cloud Manager settings. [Learn how](#).

### Steps

1. In the upper right of the Cloud Manager console, click the Settings icon, and select **Credentials**.
2. Hover over a set of credentials and click the action menu.
3. From the menu, click **Associate Subscription**.



4. Select a subscription from the down-down list or click **Add Subscription** and follow the steps to create a new subscription.

The following video starts from the context of the working environment wizard, but shows you the same workflow after you click **Add Subscription**:

► [https://docs.netapp.com/us-en/occm/media/video\\_subscribing\\_azure.mp4](https://docs.netapp.com/us-en/occm/media/video_subscribing_azure.mp4) (video)

#### Associating additional Azure subscriptions with a managed identity

Cloud Manager enables you to choose the Azure credentials and Azure subscription in which you want to deploy Cloud Volumes ONTAP. You can't select a different Azure subscription for the managed identity profile unless you associate the [managed identity](#) with those subscriptions.

#### About this task

A managed identity is [the initial Azure account](#) when you deploy a Connector from Cloud Manager. When you deployed the Connector, Cloud Manager created the Cloud Manager Operator role and assigned it to the Connector virtual machine.

#### Steps

1. Log in to the Azure portal.
2. Open the **Subscriptions** service and then select the subscription in which you want to deploy Cloud Volumes ONTAP.
3. Click **Access control (IAM)**.
  - a. Click **Add > Add role assignment** and then add the permissions:
    - Select the **Cloud Manager Operator** role.



Cloud Manager Operator is the default name provided in the [Cloud Manager policy](#). If you chose a different name for the role, then select that name instead.

- Assign access to a **Virtual Machine**.
- Select the subscription in which the Connector virtual machine was created.
- Select the Connector virtual machine.
- Click **Save**.

4. Repeat these steps for additional subscriptions.

#### Result

When you create a new working environment, you should now have the ability to select from multiple Azure subscriptions for the managed identity profile.

The screenshot shows a user interface titled "Edit Account & Add Subscription". Under the "Credentials" section, a dropdown menu is open, showing "Managed Service Identity" as the selected option. Below this, under "Azure Subscription", there is a list of subscriptions. The list includes "OCCM Dev" and "OCCM QA1 (Default)". A blue bar highlights "OCCM QA1 (Default)", and a cursor icon is positioned over it, indicating it is being selected. A yellow informational message at the bottom of the list states: "No subscription is associated with this account".

## GCP

### Google Cloud projects, permissions, and accounts

A service account provides Cloud Manager with permissions to deploy and manage Cloud Volumes ONTAP systems in the same project as Cloud Manager, or in different projects.

#### Project and permissions for Cloud Manager

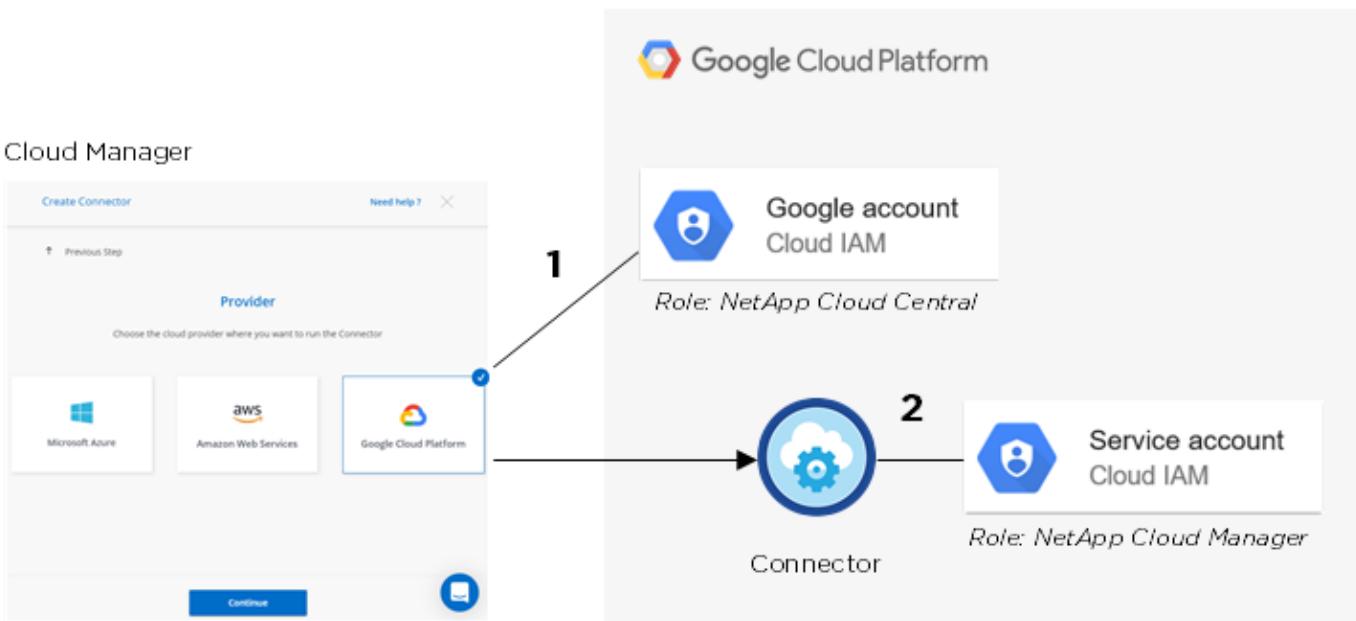
Before you can deploy Cloud Volumes ONTAP in Google Cloud, you must first deploy a Connector in a Google Cloud project. The Connector can't be running on your premises, or in a different cloud provider.

Two sets of permissions must be in place before you deploy a Connector directly from Cloud Manager:

1. You need to deploy a Connector using a Google account that has permissions to launch the Connector VM instance from Cloud Manager.
2. When deploying the Connector, you are prompted to select a [service account](#) for the VM instance. Cloud Manager gets permissions from the service account to create and manage Cloud Volumes ONTAP systems on your behalf. Permissions are provided by attaching a custom role to the service account.

We have set up two YAML files that include the required permissions for the user and the service account. [Learn how to use the YAML files to set up permissions.](#)

The following image depicts the permission requirements described in numbers 1 and 2 above:



### Project for Cloud Volumes ONTAP

Cloud Volumes ONTAP can reside in the same project as the Connector, or in a different project. To deploy Cloud Volumes ONTAP in a different project, you need to first add the Connector service account and role to that project.

- [Learn how to set up service account \(see step 2\).](#)
- [Learn how to deploy Cloud Volumes ONTAP in GCP and select a project.](#)

### Account for data tiering



Cloud Manager requires a GCP account for Cloud Volumes ONTAP 9.6, but not for 9.7 and later. If you want to use data tiering with Cloud Volumes ONTAP 9.7 or later, then follow step 4 in [Getting started with Cloud Volumes ONTAP in Google Cloud Platform](#).

Adding a Google Cloud account to Cloud Manager is required to enable data tiering on a Cloud Volumes ONTAP 9.6 system. Data tiering automatically tiers cold data to low-cost object storage, enabling you to reclaim space on your primary storage and shrink secondary storage.

When you add the account, you need to provide Cloud Manager with a storage access key for a service account that has Storage Admin permissions. Cloud Manager uses the access keys to set up and manage a Cloud Storage bucket for data tiering.

After you add a Google Cloud account, you can then enable data tiering on individual volumes when you create, modify, or replicate them.

- [Learn how to set up and add GCP accounts to Cloud Manager.](#)
- [Learn how to tier inactive data to low-cost object storage.](#)

### Managing GCP credentials and subscriptions for Cloud Manager

You can manage two types of Google Cloud Platform credentials from Cloud Manager: the credentials that are associated with the Connector VM instance and storage access keys used with a Cloud Volumes ONTAP 9.6 system for [data tiering](#).

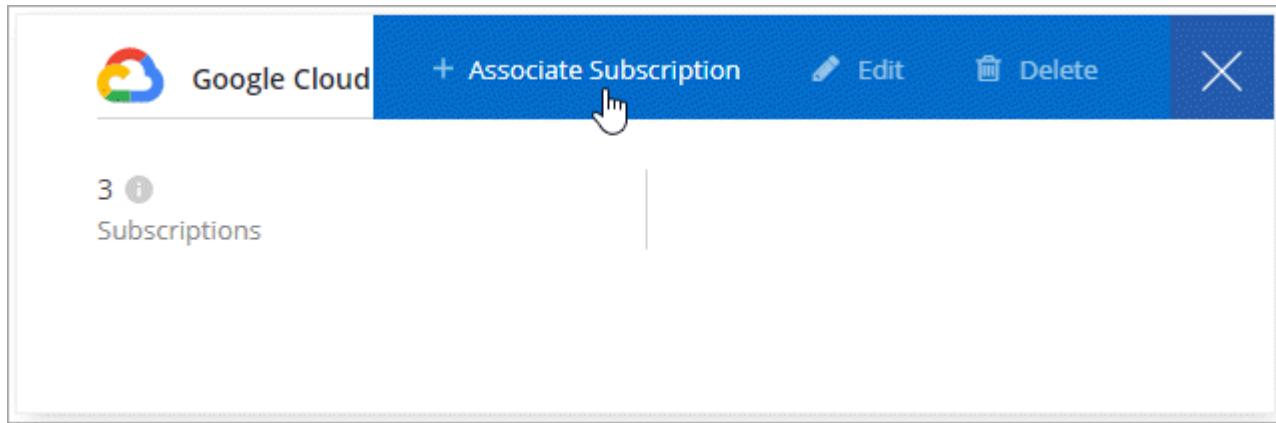
## Associating a Marketplace subscription with GCP credentials

When you deploy a Connector in GCP, Cloud Manager creates a default set of credentials that are associated with the Connector VM instance. These are the credentials that Cloud Manager uses to deploy Cloud Volumes ONTAP.

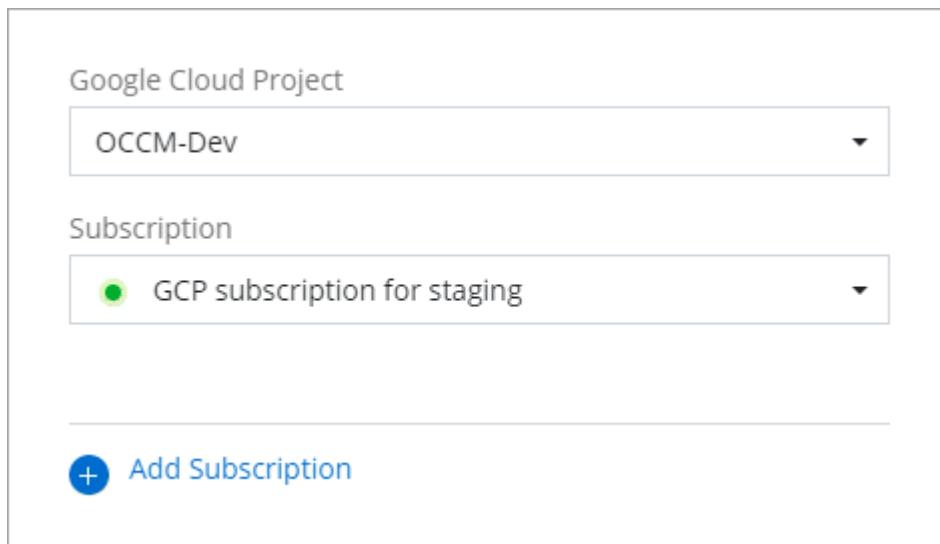
At any time, you can change the Marketplace subscription that's associated with these credentials. The subscription enables you to create a pay-as-you-go Cloud Volumes ONTAP system, and to use other NetApp cloud services.

### Steps

1. In the upper right of the Cloud Manager console, click the Settings icon, and select **Credentials**.
2. Hover over a set of credentials and click the action menu.
3. From the menu, click **Associate Subscription**.



4. Select a Google Cloud project and subscription from the down-down list or click **Add Subscription** and follow the steps to create a new subscription.



5. Click **Associate**.

## Setting up and adding GCP accounts for data tiering with Cloud Volumes ONTAP 9.6

If you want to enable a Cloud Volumes ONTAP 9.6 system for [data tiering](#), you need to provide Cloud Manager with a storage access key for a service account that has Storage Admin permissions. Cloud Manager uses the

access keys to set up and manage a Cloud Storage bucket for data tiering.



If you want to use data tiering with Cloud Volumes ONTAP 9.7 or later, then follow step 4 in [Getting started with Cloud Volumes ONTAP in Google Cloud Platform](#).

## Setting up a service account and access keys for Google Cloud Storage

A service account enables Cloud Manager to authenticate and access Cloud Storage buckets used for data tiering. The keys are required so that Google Cloud Storage knows who is making the request.

### Steps

1. Open the GCP IAM console and [create a service account](#) that has the Storage Admin role.

Create service account

**Service account details**

**Grant this service account access to project (optional)**

Grant this service account access to OCCM-Dev so that it has permission to complete specific actions on the resources in your project. [Learn more](#)

Select a role

Condition

storage admin

Cloud ML Service Agent

Cloud ML service agent can act as log writer, Cloud Storage admin, Artifact Registry Reader, BigQuery writer, and service account access token creator.

Storage Admin

Full control of GCS resources.

Storage HMAC Key Admin

Full control of GCS HMAC Keys.

Storage Object Admin

Full control of GCS objects.

DONE

MANAGE ROLES

2. Go to [GCP Storage Settings](#).
3. If you're prompted, select a project.
4. Click the **Interoperability** tab.
5. If you haven't already done so, click **Enable interoperability access**.

6. Under **Access keys for service accounts**, click **Create a key for a service account**.
7. Select the service account that you created in step 1.

## Select a service account

Search by prefix...

Email	Name	Keys
<input checked="" type="radio"/> data-tiering-for-netapp@top-monitor-250116.iam.gserviceaccount.com	data tiering for netapp	-

CANCEL    CREATE KEY | CREATE NEW ACCOUNT

8. Click **Create Key**.
9. Copy the access key and secret.

You'll need to enter this information in Cloud Manager when you add the GCP account for data tiering.

## Adding a GCP account to Cloud Manager

Now that you have an access key for a service account, you can add it to Cloud Manager.

### What you'll need

You need to create a Connector before you can change Cloud Manager settings. [Learn how](#).

### Steps

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



2. Click **Add Credentials** and select **Google Cloud**.
3. Enter the access key and secret for the service account.

The keys enable Cloud Manager to set up a Cloud Storage bucket for data tiering.

4. Confirm that the policy requirements have been met and then click **Create Account**.

### What's next?

You can now enable data tiering on individual volumes on a Cloud Volumes ONTAP 9.6 system when you create, modify, or replicate them. For details, see [Tiering inactive data to low-cost object storage](#).

But before you do, be sure that the subnet in which Cloud Volumes ONTAP resides is configured for Private Google Access. For instructions, refer to [Google Cloud Documentation: Configuring Private Google Access](#).

## Adding NetApp Support Site accounts to Cloud Manager

Adding your NetApp Support Site account to Cloud Manager is required to deploy a BYOL system. It's also required to register pay-as-you-go systems and to upgrade ONTAP software.

Watch the following video to learn how to add NetApp Support Site accounts to Cloud Manager. Or scroll down to read the steps.



### What you'll need

You need to create a Connector before you can change Cloud Manager settings. [Learn how.](#)

### 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 Settings icon, and select **Credentials**.



3. Click **Add Credentials** and select **NetApp Support Site**.
4. Specify a name for the account and then enter the user name and password.
  - The account must be a customer-level account (not a guest or temp account).
  - If you plan to deploy BYOL systems:
    - The account must be authorized to access the serial numbers of the BYOL systems.
    - If you purchased a secure BYOL subscription, then a secure NSS account is required.

5. Click **Create Account**.

#### What's next?

Users can now select the account when creating new Cloud Volumes ONTAP systems and when registering existing systems.

- [Launching Cloud Volumes ONTAP in AWS](#)
- [Launching Cloud Volumes ONTAP in Azure](#)
- [Registering pay-as-you-go systems](#)
- [Learn how Cloud Manager manages license files](#)

## Managing users, workspaces, Connectors, and subscriptions

After you perform initial setup, you might need to administer your account settings later by managing users, workspaces, Connectors, and subscriptions.

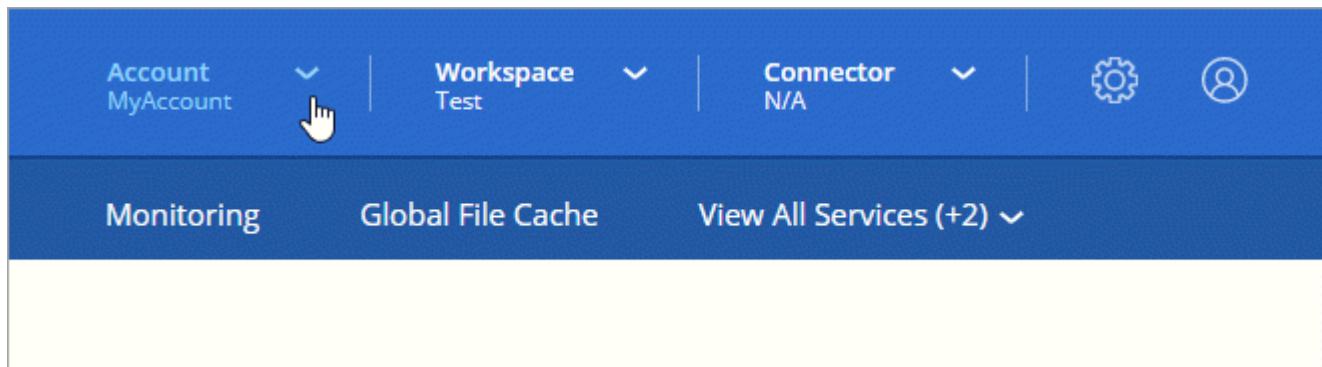
[Learn more about how Cloud Central accounts work.](#)

### Adding users

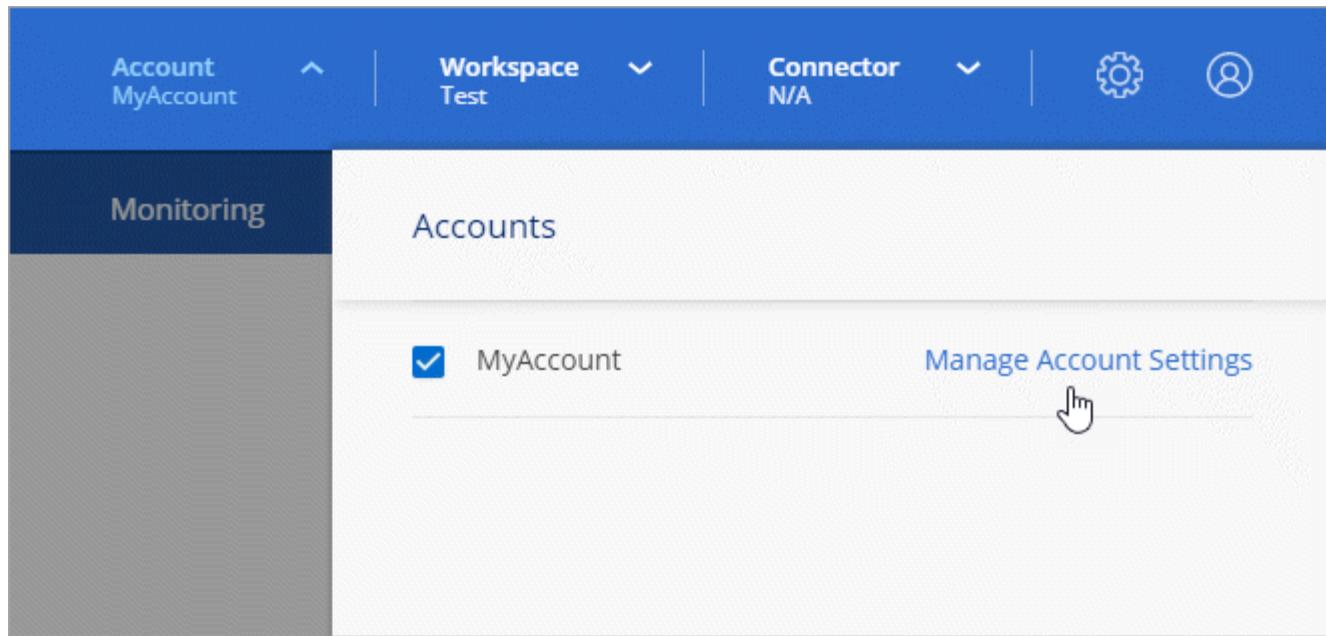
Associate Cloud Central users with the Cloud Central account so those users can create and manage working environments in Cloud Manager.

#### Steps

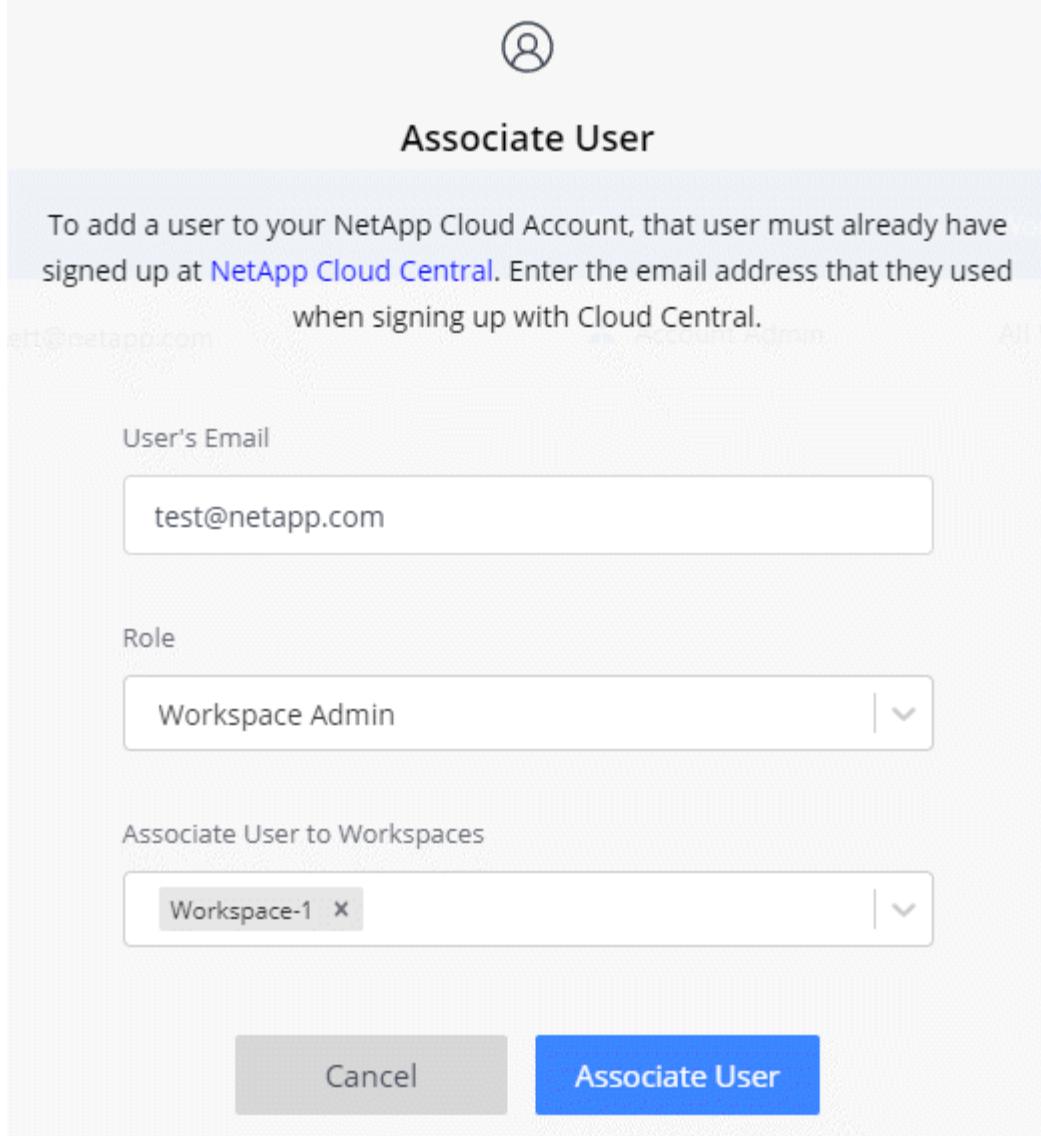
1. If the user hasn't already done so, ask the user to go to [NetApp Cloud Central](#) and sign up.
2. From the top of Cloud Manager, click the **Account** drop-down.



3. Click **Manage Account** next to the currently selected account.



4. From the Users tab, click **Associate User**.
5. Enter the user's email address and select a role for the user:
  - **Account Admin:** Can perform any action in Cloud Manager.
  - **Workspace Admin:** Can create and manage resources in assigned workspaces.
  - **Compliance Viewer:** Can only view compliance information and generate reports for workspaces that they have permission to access.
6. If you selected Workspace Admin or Compliance Viewer, select one or more workspaces to associate with that user.



The screenshot shows a "Associate User" dialog box. At the top is a user icon and the title "Associate User". Below the title is a descriptive text: "To add a user to your NetApp Cloud Account, that user must already have signed up at [NetApp Cloud Central](#). Enter the email address that they used when signing up with Cloud Central." A placeholder "User's Email" is followed by a text input field containing "test@netapp.com". A "Role" section shows "Workspace Admin" selected from a dropdown menu. An "Associate User to Workspaces" section shows "Workspace-1" selected from another dropdown menu. At the bottom are "Cancel" and "Associate User" buttons.

User's Email

test@netapp.com

Role

Workspace Admin

Associate User to Workspaces

Workspace-1

Cancel Associate User

7. Click **Associate User**.

## Result

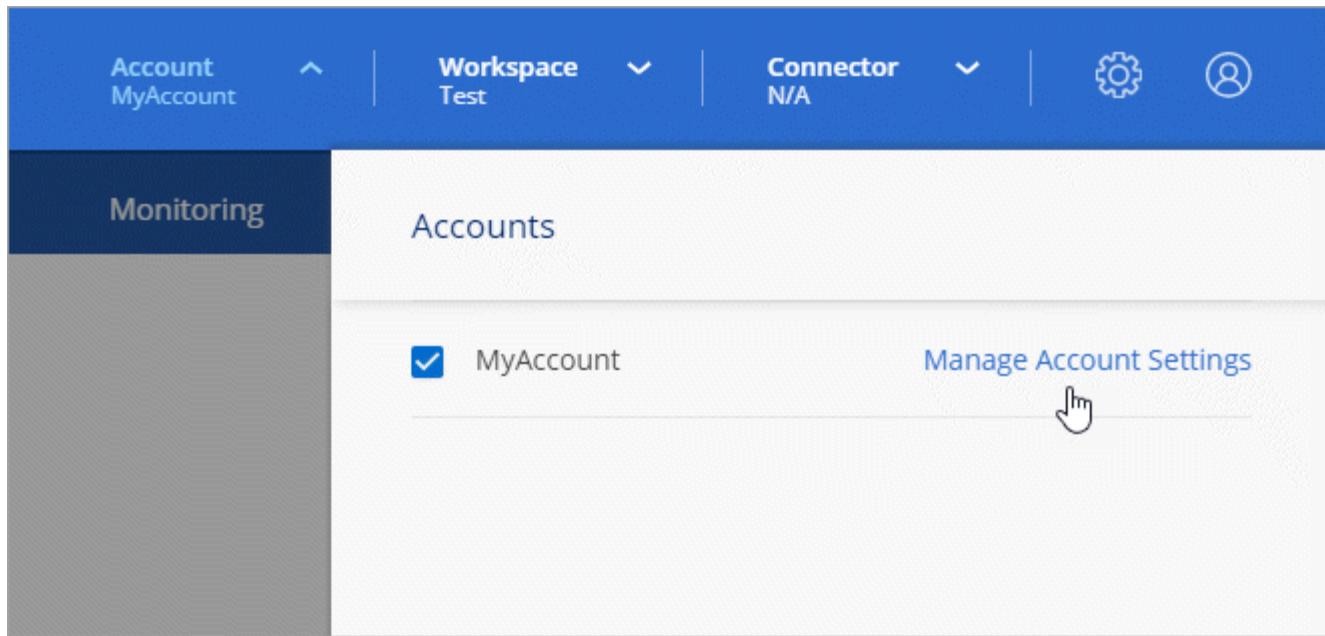
The user should receive an email from NetApp Cloud Central titled "Account Association." The email includes the information needed to access Cloud Manager.

## Removing users

Disassociating a user makes it so they can no longer access the resources in a Cloud Central account.

### Steps

1. From the top of Cloud Manager, click the **Account** drop-down and click **Manage Account**.



2. From the Users tab, click the action menu in the row that corresponds to the user.

2 Users			
Name	Email	Role	Workspaces
Ben	[REDACTED]	Account Admin	All Workspaces
test	test@netapp.com	Workspace Admin	None

3. Click **Disassociate User** and click **Disassociate** to confirm.

## Result

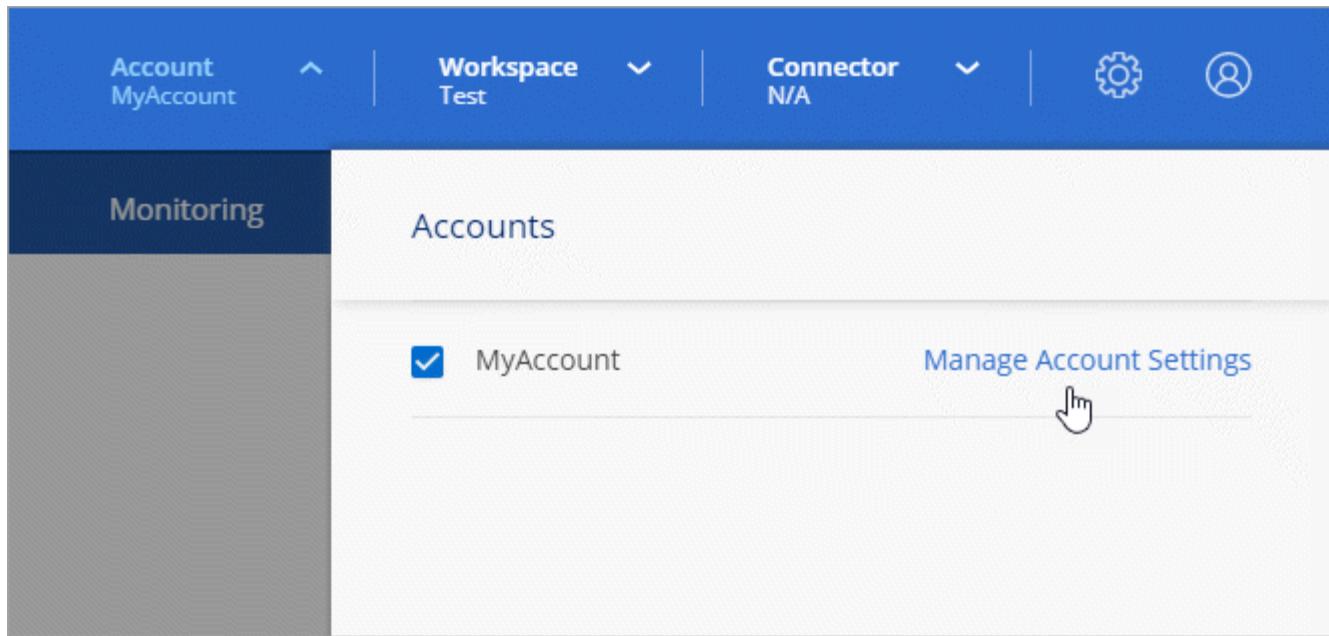
The user can no longer access the resources in this Cloud Central account.

## Managing a Workspace Admin's workspaces

You can associate and disassociate Workspace Admins with workspaces at any time. Associating the user enables them to create and view the working environments in that workspace.

## Steps

1. From the top of Cloud Manager, click the **Account** drop-down and click **Manage Account**.



2. From the Users tab, click the action menu in the row that corresponds to the user.

2 Users			
Name	Email	Role	Workspaces
Ben	[REDACTED]	Account Admin	All Workspaces
test	test@netapp.com	Workspace Admin	None

3. Click **Manage Workspaces**.

4. Select the workspaces to associate with the user and click **Apply**.

## Result

The user can now access those workspaces from Cloud Manager, as long as the Connector was also associated with the workspaces.

## Managing workspaces

Manage your workspaces by creating, renaming, and deleting them. Note that you can't delete a workspace if it contains any resources. It must be empty.

### Steps

1. From the top of Cloud Manager, click the **Account** drop-down and click **Manage Account**.
2. Click **Workspaces**.
3. Choose one of the following options:
  - Click **Add New Workspace** to create a new workspace.
  - Click **Rename** to rename the workspace.
  - Click **Delete** to delete the workspace.

## Managing a Connector's workspaces

You need to associate the Connector with workspaces so Workspace Admins can access those workspaces from Cloud Manager.

If you only have Account Admins, then associating the Connector with workspaces isn't required. Account Admins have the ability to access all workspaces in Cloud Manager by default.

[Learn more about users, workspaces, and Connectors.](#)

### Steps

1. From the top of Cloud Manager, click the **Account** drop-down and click **Manage Account**.
2. Click **Connector**.
3. Click **Manage Workspaces** for the Connector that you want to associate.
4. Select the workspaces to associate with the Connector and click **Apply**.

## Managing subscriptions

After you subscribe from a cloud provider's marketplace, each subscription is available from the Account Settings widget. You have the option to rename a subscription and to disassociate the subscription from one or more accounts.

For example, let's say that you have two accounts and each is billed through separate subscriptions. You might disassociate a subscription from one of the accounts so the users in that account don't accidentally choose the wrong subscription when creating a Cloud Volume ONTAP working environment.

[Learn more about subscriptions.](#)

### Steps

1. From the top of Cloud Manager, click the **Account** drop-down and click **Manage Account**.
2. Click **Subscriptions**.

You'll only see the subscriptions that are associated with the account that you're currently viewing.

3. Click the action menu in the row that corresponds to the subscription that you want to manage.

Name	Service	Cloud Provider	Status
QA Subscription	test-service	aws	Unsubscribed
metering service subscription QA !!!!	cloud-volumes-ontap	aws	Subscribed

Rename Subscription  
Manage Accounts

4. Choose to rename the subscription or to manage the accounts that are associated with the subscription.

## Changing the account name

Change your account name at any time to change it to something meaningful for you.

### Steps

1. From the top of Cloud Manager, click the **Account** drop-down and click **Manage Account**.
2. In the **Overview** tab, click the edit icon next to the account name.
3. Type a new account name and click **Save**.

## Disabling the SaaS platform

We don't recommend disabling the SaaS platform unless you need to in order to comply with your company's security policies. Disabling the SaaS platform limits your ability to use NetApp's integrated cloud services.

The following services aren't available from Cloud Manager if you disable the SaaS platform:

- Cloud Compliance
- Kubernetes
- Cloud Tiering
- Global File Cache

If you do disable the SaaS platform, you'll need to perform all tasks from [the local user interface that is available on a Connector](#).



This is an irreversible action that will prevent you from using the Cloud Manager SaaS platform. You'll need to perform actions from the local Connector. You won't have the ability to use many of NetApp's integrated cloud services, and re-enabling the SaaS platform will require the help of NetApp support.

### Steps

1. From the top of Cloud Manager, click the **Account** drop-down and click **Manage Account**.
2. In the Overview tab, toggle the option to disable use of the SaaS platform.

## Managing an HTTPS certificate for secure access

By default, Cloud Manager uses a self-signed certificate for HTTPS access to the web console. You can install a certificate signed by a certificate authority (CA), which provides better security protection than a self-signed certificate.

### Before you get started

You need to create a Connector before you can change Cloud Manager settings. [Learn how](#).

### Installing an HTTPS certificate

Install a certificate signed by a CA for secure access.

### Steps

1. In the upper right of the Cloud Manager console, click the Settings icon, and select **HTTPS Setup**.



2. In the HTTPS Setup page, install a certificate by generating a certificate signing request (CSR) or by installing your own CA-signed certificate:

Option	Description
Generate a CSR	<ol style="list-style-type: none"><li>a. Enter the host name or DNS of the Connector host (its Common Name), and then click <b>Generate CSR</b>. Cloud Manager displays a certificate signing request.</li><li>b. Use the CSR to submit an SSL certificate request to a CA. The certificate must use the Privacy Enhanced Mail (PEM) Base-64 encoded X.509 format.</li><li>c. Copy the contents of the signed certificate, paste it in the Certificate field, and then click <b>Install</b>.</li></ol>
Install your own CA-signed certificate	<ol style="list-style-type: none"><li>a. Select <b>Install CA-signed certificate</b>.</li><li>b. Load both the certificate file and the private key and then click <b>Install</b>. The certificate must use the Privacy Enhanced Mail (PEM) Base-64 encoded X.509 format.</li></ol>

## Result

Cloud Manager now uses the CA-signed certificate to provide secure HTTPS access. The following image shows a Cloud Manager system that is configured for secure access:

## Cloud Manager HTTPS certificate

Expiration:

 Oct 27, 2016 05:13:28 am

Issuer:

CN=localhost, O=NetApp, OU=Tel-Aviv,  
EMAILADDRESS=admin@example.com

Subject:

EMAILADDRESS=admin@example.com,  
OU=Tel-Aviv, O=NetApp, CN=localhost

 [View Certificate](#)

 [Renew HTTPS Certificate](#)

## Renewing the Cloud Manager HTTPS certificate

You should renew the Cloud Manager HTTPS certificate before it expires to ensure secure access to the Cloud Manager web console. If you do not renew the certificate before it expires, a warning appears when users access the web console using HTTPS.

### Steps

1. In the upper right of the Cloud Manager console, click the Settings icon, and select **HTTPS Setup**.

Details about the Cloud Manager certificate displays, including the expiration date.

2. Click **Renew HTTPS Certificate** and follow the steps to generate a CSR or install your own CA-signed certificate.

### Result

Cloud Manager uses the new CA-signed certificate to provide secure HTTPS access.

## 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.

## Configuring a Connector to use a proxy server

If your corporate policies dictate that you use a proxy server for all HTTP communication to the internet, then you must configure your Connectors to use that proxy server. The proxy server can be in the cloud or in your network.

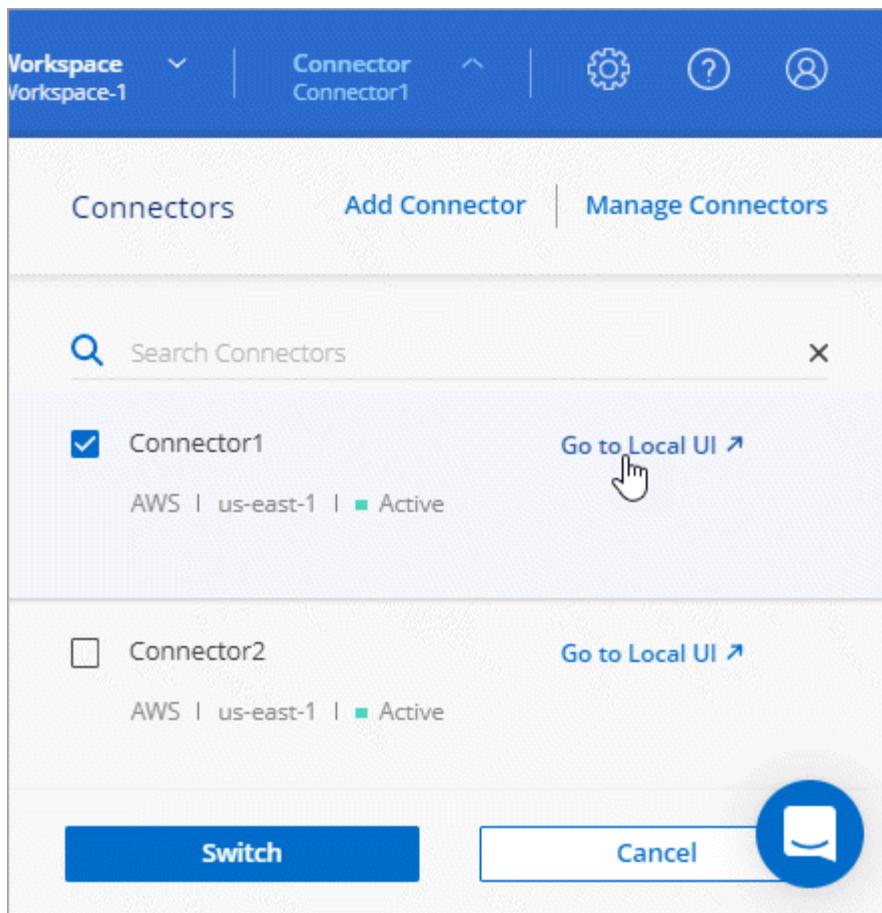
When you configure a Connector to use a proxy server, that Connector and the Cloud Volumes ONTAP systems that it manages (including any HA mediators), all use the proxy server.

#### Steps

1. [Log in to the Cloud Manager SaaS interface](#) from a machine that has a network connection to the Connector instance.

If the Connector doesn't have a public IP address, you'll need a VPN connection or you'll need to connect from a jump host that's in the same network as the Connector.

2. Click the **Connector** drop-down and then click **Go to local UI** for a specific Connector.



The Cloud Manager interface running on the Connector loads in a new browser tab.

3. In the upper right of the Cloud Manager console, click the Settings icon, and select **Cloud Manager Settings**.



4. Under HTTP Proxy, enter the server using the syntax `http://address:port`, specify a user name and password if basic authentication is required for the server, and then click **Save**.



Cloud Manager doesn't support passwords that include the @ character.

## Result

After you specify the proxy server, new Cloud Volumes ONTAP systems are automatically configured to use the proxy server when sending AutoSupport messages. If you didn't specify the proxy server before users create Cloud Volumes ONTAP systems, then they must use System Manager to manually set the proxy server in the AutoSupport options for each system.

## Reference

## Roles

The Account Admin, Workspace Admin, and Cloud Compliance Viewer roles provide specific permissions to users.

Task	Account Admin	Workspace Admin	Cloud Compliance Viewer
Manage working environments	Yes	Yes	No
Enable services on working environments	Yes	Yes	No
View data replication status	Yes	Yes	No
View the timeline	Yes	Yes	No
Switch between workspaces	Yes	Yes	Yes
View Compliance scan results	Yes	Yes	Yes
Delete working environments	Yes	No	No
Connect Kubernetes clusters to working environments	Yes	No	No
Receive the Cloud Volumes ONTAP report	Yes	No	No
Create Connectors	Yes	No	No
Manage Cloud Central accounts	Yes	No	No
Manage credentials	Yes	No	No
Modify Cloud Manager settings	Yes	No	No
View and manage the Support Dashboard	Yes	No	No
Remove working environments from Cloud Manager	Yes	No	No
Install an HTTPS certificate	Yes	No	No

### Related links

- [Setting up workspaces and users in the Cloud Central account](#)
- [Managing workspaces and users in the Cloud Central account](#)

### How Cloud Manager uses cloud provider permissions

Cloud Manager requires permissions to perform actions in your cloud provider. These permissions are included in [the policies provided by NetApp](#). You might want to understand what Cloud Manager does with these permissions.

### What Cloud Manager does with AWS permissions

Cloud Manager uses an AWS account to make API calls to several AWS services, including EC2, S3,

CloudFormation, IAM, the Security Token Service (STS), and the Key Management Service (KMS).

Actions	Purpose
<ul style="list-style-type: none"> <li>"ec2:StartInstances",</li> <li>"ec2:StopInstances",</li> <li>"ec2:DescribeInstances",</li> <li>"ec2:DescribeInstanceStatus",</li> <li>"ec2:RunInstances",</li> <li>"ec2:TerminateInstances",</li> <li>"ec2:ModifyInstanceState",</li> </ul>	Launches a Cloud Volumes ONTAP instance and stops, starts, and monitors the instance.
<ul style="list-style-type: none"> <li>"ec2:DescribeInstanceAttribute",</li> </ul>	Verifies that enhanced networking is enabled for supported instance types.
<ul style="list-style-type: none"> <li>"ec2:DescribeRouteTables",</li> <li>"ec2:DescribeImages",</li> </ul>	Launches a Cloud Volumes ONTAP HA configuration.
<ul style="list-style-type: none"> <li>"ec2&gt;CreateTags",</li> </ul>	Tags every resource that Cloud Manager creates with the "WorkingEnvironment" and "WorkingEnvironmentId" tags. Cloud Manager uses these tags for maintenance and cost allocation.
<ul style="list-style-type: none"> <li>"ec2&gt;CreateVolume",</li> <li>"ec2:DescribeVolumes",</li> <li>"ec2:ModifyVolumeAttribute",</li> <li>"ec2:AttachVolume",</li> <li>"ec2&gt;DeleteVolume",</li> <li>"ec2:DetachVolume",</li> </ul>	Manages the EBS volumes that Cloud Volumes ONTAP uses as back-end storage.
<ul style="list-style-type: none"> <li>"ec2&gt;CreateSecurityGroup",</li> <li>"ec2&gt;DeleteSecurityGroup",</li> <li>"ec2:DescribeSecurityGroups",</li> <li>"ec2:RevokeSecurityGroupEgress",</li> <li>"ec2:AuthorizeSecurityGroupEgress",</li> <li>"ec2:AuthorizeSecurityGroupIngress",</li> <li>"ec2:RevokeSecurityGroupIngress",</li> </ul>	Creates predefined security groups for Cloud Volumes ONTAP.
<ul style="list-style-type: none"> <li>"ec2&gt;CreateNetworkInterface",</li> <li>"ec2:DescribeNetworkInterfaces",</li> <li>"ec2:DeleteNetworkInterface",</li> <li>"ec2:ModifyNetworkInterfaceAttribute",</li> </ul>	Creates and manages network interfaces for Cloud Volumes ONTAP in the target subnet.
<ul style="list-style-type: none"> <li>"ec2:DescribeSubnets",</li> <li>"ec2:DescribeVpcs",</li> </ul>	Gets the list of destination subnets and security groups, which is needed when creating a new working environment for Cloud Volumes ONTAP.
<ul style="list-style-type: none"> <li>"ec2:DescribeDhcpOptions",</li> </ul>	Determines DNS servers and the default domain name when launching Cloud Volumes ONTAP instances.
<ul style="list-style-type: none"> <li>"ec2&gt;CreateSnapshot",</li> <li>"ec2&gt;DeleteSnapshot",</li> <li>"ec2:DescribeSnapshots",</li> </ul>	Takes snapshots of EBS volumes during initial setup and whenever a Cloud Volumes ONTAP instance is stopped.
<ul style="list-style-type: none"> <li>"ec2:GetConsoleOutput",</li> </ul>	Captures the Cloud Volumes ONTAP console, which is attached to AutoSupport messages.

Actions	Purpose
"ec2:DescribeKeyPairs",	Obtains the list of available key pairs when launching instances.
"ec2:DescribeRegions",	Gets a list of available AWS regions.
"ec2:DeleteTags", "ec2:DescribeTags",	Manages tags for resources associated with Cloud Volumes ONTAP instances.
"cloudformation>CreateStack", "cloudformation>DeleteStack", "cloudformation>DescribeStacks", "cloudformation>DescribeStackEvents", "cloudformation>ValidateTemplate",	Launches Cloud Volumes ONTAP instances.
"iam:PassRole", "iam>CreateRole", "iam>DeleteRole", "iam:PutRolePolicy", "iam>CreateInstanceProfile", "iam>DeleteRolePolicy", "iam>AddRoleToInstanceProfile", "iam:RemoveRoleFromInstanceProfile", "iam>DeleteInstanceProfile",	Launches a Cloud Volumes ONTAP HA configuration.
"iam>ListInstanceProfiles", "sts>DecodeAuthorizationMessage", "ec2:AssociateIamInstanceProfile", "ec2:DescribeIamInstanceProfileAssociations", "ec2:DisassociateIamInstanceProfile",	Manages instance profiles for Cloud Volumes ONTAP instances.
"s3:GetBucketTagging", "s3:GetBucketLocation", "s3>ListAllMyBuckets", "s3>ListBucket"	Obtains information about AWS S3 buckets so Cloud Manager can integrate with the NetApp Data Fabric Cloud Sync service.
"s3>CreateBucket", "s3>DeleteBucket", "s3>GetLifecycleConfiguration", "s3>PutLifecycleConfiguration", "s3>PutBucketTagging", "s3>ListBucketVersions", "s3>GetBucketPolicyStatus", "s3>GetBucketPublicAccessBlock", "s3>GetBucketAcl", "s3>GetBucketPolicy", "s3>PutBucketPublicAccessBlock"	Manages the S3 bucket that a Cloud Volumes ONTAP system uses as a capacity tier for data tiering.
"kms>List*", "kms>ReEncrypt*", "kms>Describe*", "kms>CreateGrant",	Enables data encryption of Cloud Volumes ONTAP using the AWS Key Management Service (KMS).

Actions	Purpose
"ce:GetReservationUtilization", "ce:GetDimensionValues", "ce:GetCostAndUsage", "ce:GetTags"	Obtains AWS cost data for Cloud Volumes ONTAP.
"ec2>CreatePlacementGroup", "ec2>DeletePlacementGroup"	When you deploy an HA configuration in a single AWS Availability Zone, Cloud Manager launches the two HA nodes and the mediator in an AWS spread placement group.
"ec2:DescribeReservedInstancesOfferings"	Cloud Manager uses the permission as part of Cloud Compliance deployment to choose which instance type to use.
"s3>DeleteBucket", "s3:GetLifecycleConfiguration", "s3:PutLifecycleConfiguration", "s3:PutBucketTagging", "s3>ListBucketVersions", "s3:GetObject", "s3>ListBucket", "s3>ListAllMyBuckets", "s3:GetBucketTagging", "s3:GetBucketLocation", "s3:GetBucketPolicyStatus", "s3:GetBucketPublicAccessBlock", "s3:GetBucketAcl", "s3:GetBucketPolicy", "s3:PutBucketPublicAccessBlock"	Cloud Manager uses these permissions when you enable the Backup to S3 service.

## What Cloud Manager does with Azure permissions

The Cloud Manager Azure policy includes the permissions that Cloud Manager needs to deploy and manage Cloud Volumes ONTAP in Azure.

Actions	Purpose
"Microsoft.Compute/locations/operations/read", "Microsoft.Compute/locations/vmSizes/read", "Microsoft.Compute/operations/read", "Microsoft.Compute/virtualMachines/instanceView/read", "Microsoft.Compute/virtualMachines/powerOff/action", "Microsoft.Compute/virtualMachines/read", "Microsoft.Compute/virtualMachines/restart/action", "Microsoft.Compute/virtualMachines/start/action", "Microsoft.Compute/virtualMachines/deallocate/action", ", "Microsoft.Compute/virtualMachines/vmSizes/read", "Microsoft.Compute/virtualMachines/write",	Creates Cloud Volumes ONTAP and stops, starts, deletes, and obtains the status of the system.
"Microsoft.Compute/images/write", "Microsoft.Compute/images/read",	Enables Cloud Volumes ONTAP deployment from a VHD.

Actions	Purpose
"Microsoft.Compute/disks/delete",           "Microsoft.Compute/disks/read",           "Microsoft.Compute/disks/write",           "Microsoft.Storage/checknameavailability/read",           "Microsoft.Storage/operations/read",           "Microsoft.Storage/storageAccounts/listkeys/action",           "Microsoft.Storage/storageAccounts/read",           "Microsoft.Storage/storageAccounts/regeneratekey/action",           "Microsoft.Storage/storageAccounts/write"           "Microsoft.Storage/storageAccounts/delete",           "Microsoft.Storage/usages/read",	Manages Azure storage accounts and disks, and attaches the disks to Cloud Volumes ONTAP.
"Microsoft.Network/networkInterfaces/read",           "Microsoft.Network/networkInterfaces/write",           "Microsoft.Network/networkInterfaces/join/action",	Creates and manages network interfaces for Cloud Volumes ONTAP in the target subnet.
"Microsoft.Network/networkSecurityGroups/read",           "Microsoft.Network/networkSecurityGroups/write",           "Microsoft.Network/networkSecurityGroups/join/action",	Creates predefined network security groups for Cloud Volumes ONTAP.
"Microsoft.Resources/subscriptions/locations/read",           "Microsoft.Network/locations/operationResults/read",           "Microsoft.Network/locations/operations/read",           "Microsoft.Network/virtualNetworks/read",           "Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read",           "Microsoft.Network/virtualNetworks/subnets/read",           "Microsoft.Network/virtualNetworks/subnets/virtualMachines/read",           "Microsoft.Network/virtualNetworks/virtualMachines/read",           "Microsoft.Network/virtualNetworks/subnets/join/action",	Gets network information about regions, the target VNet and subnet, and adds Cloud Volumes ONTAP to VNets.
"Microsoft.Network/virtualNetworks/subnets/write",           "Microsoft.Network/routeTables/join/action",	Enables VNet service endpoints for data tiering.
"Microsoft.Resources/deployments/operations/read",           "Microsoft.Resources/deployments/read",           "Microsoft.Resources/deployments/write",	Deploys Cloud Volumes ONTAP from a template.

Actions	Purpose
"Microsoft.Resources/deployments/operations/read", "Microsoft.Resources/deployments/read", "Microsoft.Resources/deployments/write", "Microsoft.Resources/resources/read", "Microsoft.Resources/subscriptions/operationresults/read", "Microsoft.Resources/subscriptions/resourceGroups/delete", "Microsoft.Resources/subscriptions/resourceGroups/read", "Microsoft.Resources/subscriptions/resourcegroups/resources/read", "Microsoft.Resources/subscriptions/resourceGroups/write",	Creates and manages resource groups for Cloud Volumes ONTAP.
"Microsoft.Compute/snapshots/write", "Microsoft.Compute/snapshots/read", "Microsoft.Compute/disks/beginGetAccess/action"	Creates and manages Azure managed snapshots.
"Microsoft.Compute/availabilitySets/write", "Microsoft.Compute/availabilitySets/read",	Creates and manages availability sets for Cloud Volumes ONTAP.
"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/read", "Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/write"	Enables programmatic deployments from the Azure Marketplace.
"Microsoft.Network/loadBalancers/read", "Microsoft.Network/loadBalancers/write", "Microsoft.Network/loadBalancers/delete", "Microsoft.Network/loadBalancers/backendAddressPools/read", "Microsoft.Network/loadBalancers/backendAddressPools/join/action", "Microsoft.Network/loadBalancers/frontendIPConfigurations/read", "Microsoft.Network/loadBalancers/loadBalancingRules/read", "Microsoft.Network/loadBalancers/probes/read", "Microsoft.Network/loadBalancers/probes/join/action",	Manages an Azure load balancer for HA pairs.
"Microsoft.Authorization/locks/*"	Enables management of locks on Azure disks.
"Microsoft.Authorization/roleDefinitions/write", "Microsoft.Authorization/roleAssignments/write", "Microsoft.Web/sites/*"	Manages failover for HA pairs.

Actions	Purpose
"Microsoft.Network/privateEndpoints/write",           "Microsoft.Storage/storageAccounts/PrivateEndpointConnectionsApproval/action",           "Microsoft.Storage/storageAccounts/privateEndpointConnections/read",           "Microsoft.Network/privateEndpoints/read",           "Microsoft.Network/privateDnsZones/write",           "Microsoft.Network/privateDnsZones/virtualNetworkLinks/write",           "Microsoft.Network/virtualNetworks/join/action",           "Microsoft.Network/privateDnsZones/A/write",           "Microsoft.Network/privateDnsZones/read",           "Microsoft.Network/privateDnsZones/virtualNetworkLinks/read",	Enables the management of private endpoints. Private endpoints are used when connectivity isn't provided to outside the subnet. Cloud Manager creates the storage account for HA with only internal connectivity within the subnet.
"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/delete",	Enables Cloud Manager to delete volumes for Azure NetApp Files.
"Microsoft.Resources/deployments/operationStatuses/read"	Azure requires this permission for some virtual machine deployments (it depends on the underlying physical hardware that's used during deployment).
"Microsoft.Resources/deployments/operationStatuses/read",           "Microsoft.Insights/Metrics/Read",           "Microsoft.Compute/virtualMachines/extensions/write",           "Microsoft.Compute/virtualMachines/extensions/read",           "Microsoft.Compute/virtualMachines/extensions/delete",           "Microsoft.Compute/virtualMachines/delete",           "Microsoft.Network/networkInterfaces/delete",           "Microsoft.Network/networkSecurityGroups/delete",           "Microsoft.Resources/deployments/delete",	Enables you to use Global File Cache.
"Microsoft.Compute/diskEncryptionSets/read"	Enables Cloud Manager to encrypt Azure managed disks on single node Cloud Volumes ONTAP systems using external keys from another account. This feature is supported using APIs.

## What Cloud Manager does with GCP permissions

The Cloud Manager policy for GCP includes the permissions that Cloud Manager needs to deploy and manage Cloud Volumes ONTAP.

Actions	Purpose
- compute.disks.create           - compute.disks.createSnapshot           - compute.disks.delete           - compute.disks.get           - compute.disks.list           - compute.disks.setLabels           - compute.disks.use	To create and manage disks for Cloud Volumes ONTAP.

Actions	Purpose
<ul style="list-style-type: none"> <li>- compute.firewalls.create</li> <li>- compute.firewalls.delete</li> <li>- compute.firewalls.get</li> <li>- compute.firewalls.list</li> </ul>	To create firewall rules for Cloud Volumes ONTAP.
<ul style="list-style-type: none"> <li>- compute.globalOperations.get</li> </ul>	To get the status of operations.
<ul style="list-style-type: none"> <li>- compute.images.get</li> <li>- compute.images.getFromFamily</li> <li>- compute.images.list</li> <li>- compute.images.useReadOnly</li> </ul>	To get images for VM instances.
<ul style="list-style-type: none"> <li>- compute.instances.attachDisk</li> <li>- compute.instances.detachDisk</li> </ul>	To attach and detach disks to Cloud Volumes ONTAP.
<ul style="list-style-type: none"> <li>- compute.instances.create</li> <li>- compute.instances.delete</li> </ul>	To create and delete Cloud Volumes ONTAP VM instances.
<ul style="list-style-type: none"> <li>- compute.instances.get</li> </ul>	To list VM instances.
<ul style="list-style-type: none"> <li>- compute.instances.getSerialPortOutput</li> </ul>	To get console logs.
<ul style="list-style-type: none"> <li>- compute.instances.list</li> </ul>	To retrieve the list of instances in a zone.
<ul style="list-style-type: none"> <li>- compute.instances.setDeletionProtection</li> </ul>	To set deletion protection on the instance.
<ul style="list-style-type: none"> <li>- compute.instances.setLabels</li> </ul>	To add labels.
<ul style="list-style-type: none"> <li>- compute.instances.setMachineType</li> </ul>	To change the machine type for Cloud Volumes ONTAP.
<ul style="list-style-type: none"> <li>- compute.instances.setMetadata</li> </ul>	To add metadata.
<ul style="list-style-type: none"> <li>- compute.instances.setTags</li> </ul>	To add tags for firewall rules.
<ul style="list-style-type: none"> <li>- compute.instances.start</li> <li>- compute.instances.stop</li> <li>- compute.instances.updateDisplayDevice</li> </ul>	To start and stop Cloud Volumes ONTAP.
<ul style="list-style-type: none"> <li>- compute.machineTypes.get</li> </ul>	To get the numbers of cores to check qoutas.
<ul style="list-style-type: none"> <li>- compute.projects.get</li> </ul>	To support multi-projects.
<ul style="list-style-type: none"> <li>- compute.snapshots.create</li> <li>- compute.snapshots.delete</li> <li>- compute.snapshots.get</li> <li>- compute.snapshots.list</li> <li>- compute.snapshots.setLabels</li> </ul>	To create and manage persistent disk snapshots.
<ul style="list-style-type: none"> <li>- compute.networks.get</li> <li>- compute.networks.list</li> <li>- compute.regions.get</li> <li>- compute.regions.list</li> <li>- compute.subnetworks.get</li> <li>- compute.subnetworks.list</li> <li>- compute.zoneOperations.get</li> <li>- compute.zones.get</li> <li>- compute.zones.list</li> </ul>	To get the networking information needed to create a new Cloud Volumes ONTAP virtual machine instance.

Actions	Purpose
<ul style="list-style-type: none"> <li>- deploymentmanager.compositeTypes.get</li> <li>- deploymentmanager.compositeTypes.list</li> <li>- deploymentmanager.deployments.create</li> <li>- deploymentmanager.deployments.delete</li> <li>- deploymentmanager.deployments.get</li> <li>- deploymentmanager.deployments.list</li> <li>- deploymentmanager.manifests.get</li> <li>- deploymentmanager.manifests.list</li> <li>- deploymentmanager.operations.get</li> <li>- deploymentmanager.operations.list</li> <li>- deploymentmanager.resources.get</li> <li>- deploymentmanager.resources.list</li> <li>- deploymentmanager.typeProviders.get</li> <li>- deploymentmanager.typeProviders.list</li> <li>- deploymentmanager.types.get</li> <li>- deploymentmanager.types.list</li> </ul>	To deploy the Cloud Volumes ONTAP virtual machine instance using Google Cloud Deployment Manager.
<ul style="list-style-type: none"> <li>- logging.logEntries.list</li> <li>- logging.privateLogEntries.list</li> </ul>	To get stack log drives.
<ul style="list-style-type: none"> <li>- resourcemanager.projects.get</li> </ul>	To support multi-projects.
<ul style="list-style-type: none"> <li>- storage.buckets.create</li> <li>- storage.buckets.delete</li> <li>- storage.buckets.get</li> <li>- storage.buckets.list</li> <li>- storage.buckets.update</li> </ul>	To create and manage a Google Cloud Storage bucket for data tiering.
<ul style="list-style-type: none"> <li>- cloudkms.cryptoKeyVersions.useToEncrypt</li> <li>- cloudkms.cryptoKeys.get</li> <li>- cloudkms.cryptoKeys.list</li> <li>- cloudkms.keyRings.list</li> </ul>	To use customer-managed encryption keys from the Cloud Key Management Service with Cloud Volumes ONTAP.
<ul style="list-style-type: none"> <li>- compute.instances.setServiceAccount</li> <li>- iam.serviceAccounts.actAs</li> <li>- iam.serviceAccounts.getIamPolicy</li> <li>- iam.serviceAccounts.list</li> <li>- storage.objects.get</li> <li>- storage.objects.list</li> </ul>	To set a service account on the Cloud Volumes ONTAP instance. This service account provides permissions for data tiering to a Google Cloud Storage bucket.
<ul style="list-style-type: none"> <li>- compute.addresses.list</li> <li>- compute.backendServices.create</li> <li>- compute.networks.updatePolicy</li> <li>- compute.regionBackendServices.create</li> <li>- compute.regionBackendServices.get</li> <li>- compute.regionBackendServices.list</li> </ul>	To deploy HA pairs.

## AWS Marketplace pages for Cloud Manager and Cloud Volumes ONTAP

Several offerings are available in the AWS Marketplace for Cloud Manager and Cloud Volumes ONTAP. If need help understanding the purpose of each page, read the descriptions below.

In all cases, remember that you can't launch Cloud Volumes ONTAP in AWS from the AWS Marketplace. You need to launch it directly from Cloud Manager.

Goal	AWS Marketplace page to use	More information
Enable the use of Cloud Volumes ONTAP PAYGO, Cloud Tiering, Cloud Compliance, and other add-on services	<a href="#">Cloud Manager - Deploy &amp; Manage NetApp Cloud Data Services</a>	<p>This subscription enables charging for the PAYGO version of Cloud Volumes ONTAP 9.6 and later. It also enables charging for Cloud Tiering, Cloud Compliance, and other add-on services.</p> <p>You should subscribe to this offering when Cloud Manager prompts you and redirects you to the page. Cloud Manager prompts you in the Working Environment wizard or when you add new credentials in the Settings.</p> <p>This page doesn't enable you to launch Cloud Manager in AWS. That should be done from <a href="#">NetApp Cloud Central</a>, or alternatively using the AMI listed in row 3 of this table.</p>
Enable the use of Cloud Volumes ONTAP PAYGO, Cloud Tiering, Cloud Compliance, and other add-on services <i>using an annual contract</i>	<a href="#">Cloud Manager (Contracts) - Deploy &amp; Manage NetApp Cloud Data Services</a>	This subscription is an alternative to the subscription in the first row. It enables you to get an annual upfront payment for the listings. It's mostly for NetApp partners.
Deploy Cloud Manager from the AWS Marketplace using an AMI	<a href="#">Cloud Manager - Manual installation without access keys</a>	We recommend that you launch Cloud Manager in AWS from <a href="#">NetApp Cloud Central</a> , but you can launch it from this AWS Marketplace page, if you prefer.
Enable deployment of Cloud Volumes ONTAP PAYGO (9.5 or earlier)	<ul style="list-style-type: none"> <li>• <a href="#">Cloud Volumes ONTAP for AWS</a></li> <li>• <a href="#">Cloud Volumes ONTAP for AWS - High Availability</a></li> </ul>	<p>These AWS Marketplace pages enable you to subscribe to the single node or HA versions of Cloud Volumes ONTAP PAYGO for versions 9.5 and earlier.</p> <p>Starting with version 9.6, you need to subscribe through the AWS Marketplace page listed in row 1 of this table for PAYGO deployments.</p>

# Automate with the API and IaC tools

## Automation resources for infrastructure as code

Use the resources on this page to get help integrating Cloud Manager and Cloud Volumes ONTAP with your [infrastructure as code](#) (IaC).

DevOps teams use a variety of tools to automate the setup of new environments, which allows them to treat infrastructure as code. One such tool is Terraform. We have developed a Terraform provider that DevOps teams can use with Cloud Manager to automate and integrate Cloud Volumes ONTAP with infrastructure as code.

[View the netapp-cloudmmanager provider.](#)

### Related links

- [NetApp Cloud Blog: Using Cloud Manager REST APIs with Federated Access](#)
- [NetApp Cloud Blog: Cloud Automation with Cloud Volumes ONTAP and REST](#)
- [NetApp Cloud Blog: Automated Data Cloning for Cloud-Based Testing of Software Applications](#)
- [NetApp Blog: Infrastructure-As-Code \(IaC\) Accelerated with Ansible + NetApp](#)
- [NetApp thePub: Configuration Management & Automation with Ansible](#)
- [NetApp thePub: Roles for Ansible ONTAP use](#)

# Where to get help and find more information

You can get help and find more information about Cloud Manager and Cloud Volumes ONTAP through various resources, including videos, forums, and support.

- [NetApp Cloud Volumes ONTAP Support](#)

Access support resources to get help and troubleshoot issues with Cloud Volumes ONTAP.

- [Videos for Cloud Manager and Cloud Volumes ONTAP](#)

Watch videos that show you how to deploy and manage Cloud Volumes ONTAP and how to replicate data across your hybrid cloud.

- [Policies for Cloud Manager](#)

Download JSON files that include the permissions that Cloud Manager needs to perform actions in a cloud provider.

- [Cloud Manager API Developer Guide](#)

Read an overview of the APIs, examples of how to use them, and an API reference.

- Training for Cloud Volumes ONTAP

- [Cloud Volumes ONTAP Fundamentals](#)
- [Cloud Volumes ONTAP Deployment and Management for Azure](#)
- [Cloud Volumes ONTAP Deployment and Management for AWS](#)

- Technical reports

- [NetApp Technical Report 4383: Performance Characterization of Cloud Volumes ONTAP in Amazon Web Services with Application Workloads](#)
- [NetApp Technical Report 4671: Performance Characterization of Cloud Volumes ONTAP in Azure with Application Workloads](#)
- [NetApp Technical Report 4816: Performance Characterization of Cloud Volumes ONTAP for Google Cloud](#)

- SVM disaster recovery

SVM disaster recovery is the asynchronous mirroring of SVM data and configuration from a source SVM to a destination SVM. You can quickly activate a destination SVM for data access if the source SVM is no longer available.

- [Cloud Volumes ONTAP 9 SVM Disaster Recovery Preparation Express Guide](#)

Describes how to quickly configure a destination SVM in preparation for disaster recovery.

- [Cloud Volumes ONTAP 9 SVM Disaster Recovery Express Guide](#)

Describes how to quickly activate a destination SVM after a disaster, and then reactivate the source SVM.

- [FlexCache Volumes for Faster Data Access Power Guide](#)

Describes how to create and manage FlexCache volumes in the same cluster or different cluster as the origin volume for accelerating data access.

- [Security advisories](#)

Identify known vulnerabilities (CVEs) for NetApp products, including ONTAP. Note that you can remediate security vulnerabilities for Cloud Volumes ONTAP by following ONTAP documentation.

- [ONTAP 9 Documentation Center](#)

Access product documentation for ONTAP, which can help you as you use Cloud Volumes ONTAP.

- [NetApp Community: Cloud Data Services](#)

Connect with peers, ask questions, exchange ideas, find resources, and share best practices.

- [NetApp Cloud Central](#)

Find information about additional NetApp products and solutions for the cloud.

- [NetApp Product Documentation](#)

Search NetApp product documentation for instructions, resources, and answers.

# Earlier versions of Cloud Manager documentation

Documentation for previous releases of Cloud Manager is available in case you're not running the latest version.

- [Cloud Manager 3.8](#)
- [Cloud Manager 3.7](#)
- [Cloud Manager 3.6](#)
- [Cloud Manager 3.5](#)
- [Cloud Manager 3.4](#)
- [Cloud Manager 3.3](#)
- [Cloud Manager 3.2](#)

# 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](#)
- [Notice for the Cloud Backup Service](#)
- [Notice for Single File Restore](#)
- [Notice for Global File Cache](#)
- [Notice for Cloud Sync](#)
- [Notice for Cloud Tiering](#)
- [Notice for Cloud Compliance](#)

## **Copyright Information**

Copyright © 2021 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.