# Cloud Manager and Cloud Volumes ONTAP documentation

## Cloud Manager 3.7

NetApp
October 23, 2024

# Table of Contents

# Cloud Manager and Cloud Volumes ONTAP documentation

Cloud Manager enables you to deploy and manage NetApp Cloud Volumes ONTAP, which is a data management solution that provides protection, visibility, and control for your cloud-based workloads.

## BlueXP

NetApp BlueXP extends and enhances the capabilities that were provided through Cloud Manager.

Go to the BlueXP documentation

## Discover what's new

- What's new in Cloud Manager
- What's new in Cloud Volumes ONTAP

## Get started

- Get started in AWS
- Get started in Azure
- Get started in Google Cloud Platform
- Find supported configurations for Cloud Volumes ONTAP
- Review networking requirements for Cloud Manager
- Review networking requirements for Cloud Volumes ONTAP for AWS
- Review networking requirements for Cloud Volumes ONTAP for Azure
- Review networking requirements for Cloud Volumes ONTAP for GCP
- Plan your Cloud Volumes ONTAP configuration

## Automate with APIs

- API Developer Guide
- Automation samples

## 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 3.7

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 3.6
What's new in 3.5
What's new in 3.4

#### Cloud Manager 3.7.5 update (16 Dec 2019)

This update includes the following enhancements:

- Cloud Volumes ONTAP 9.7
- Cloud Compliance for Cloud Volumes ONTAP

##### Cloud Volumes ONTAP 9.7

Cloud Volumes ONTAP 9.7 is now available in AWS, Azure, and Google Cloud Platform.

See what's new in Cloud Volumes ONTAP 9.7.

##### Cloud Compliance for Cloud Volumes ONTAP

Cloud Compliance is a data privacy and compliance service for Cloud Volumes ONTAP in AWS and Azure. Using Artificial Intelligence (AI) driven technology, Cloud Compliance helps organizations understand data context and identify sensitive data across Cloud Volumes ONTAP systems.

Cloud Compliance is currently available as a Controlled Availability release.

Learn more about Cloud Compliance.

#### Cloud Manager 3.7.5 (3 Dec 2019)

Cloud Manager 3.7.5 includes the following enhancements.

- High write speed for Cloud Volumes ONTAP in GCP
- On-prem ONTAP clusters as persistent storage for Kubernetes
- Latest Trident version for Kubernetes
- Support for Azure general-purpose v2 storage accounts
- Prefixes in Azure storage account names using APIs

#### High write speed for Cloud Volumes ONTAP in GCP

You can now enable high write speed on new and existing Cloud Volumes ONTAP systems in Google Cloud Platform. High write speed is a good choice if fast write performance is required for your workload.

- Learn how to choose a write speed
- Learn how to change write speed on existing systems

#### On-prem ONTAP clusters as persistent storage for Kubernetes

Cloud Manager now enables you to use on-premises ONTAP clusters as persistent storage for containers. Similar to Cloud Volumes ONTAP, Cloud Manager automates the deployment of NetApp Trident and the connects ONTAP to Kubernetes clusters.

After adding a Kubernetes cluster to Cloud Manager, you can connect it to your on-premises ONTAP clusters from the Working Environments page:

Learn how to get started.

#### Latest Trident version for Kubernetes

Cloud Manager now installs a more recent version of Trident (version 19.07.1) when you connect a working environment to a Kubernetes cluster.

#### Support for Azure general-purpose v2 storage accounts

When you deploy new Cloud Volumes ONTAP systems in Azure, the storage accounts that Cloud Manager creates for diagnostics and data tiering are now general-purpose v2 storage accounts.

#### Prefixes in Azure storage account names using APIs

You can now add a prefix to the names of the Azure storage accounts that Cloud Manager creates for Cloud Volumes ONTAP. Just use the *storageAccountPrefix* parameter when you deploy a new Cloud Volumes ONTAP system in Azure.

See the API Developer Guide for more details about using APIs.

### Cloud Manager 3.7.4 (6 Oct 2019)

Cloud Manager 3.7.4 includes the following enhancements.

- Support for Azure NetApp Files
- Cloud Volumes ONTAP for GCP enhancements
- Backup to S3 enhancement
- Encryption of boot and root disks in AWS
- Support for the AWS Bahrain region
- Support for the Azure UAE North region

#### Support for Azure NetApp Files

You can now view and create NFS volumes for Azure NetApp Files directly from Cloud Manager. This enhancement continues our goal to help you manage your cloud storage from a single interface.

Learn how to get started.

This feature requires new permissions as shown in the latest Cloud Manager policy for Azure.

```
"Microsoft.NetApp/netAppAccounts/read",
"Microsoft.NetApp/netAppAccounts/capacityPools/read",
"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/write",
"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/read",
"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/delete"
```

#### Cloud Volumes ONTAP for GCP enhancements

Cloud Manager 3.7.4 enables the following enhancements to Cloud Volumes ONTAP for Google Cloud Platform:

**Pay-as-you-go subscriptions in the GCP Marketplace**

You can now pay for Cloud Volumes ONTAP as you go by subscribing to Cloud Volumes ONTAP in the Google Cloud Platform Marketplace.

Google Cloud Platform Marketplace: Cloud Manager for Cloud Volumes ONTAP

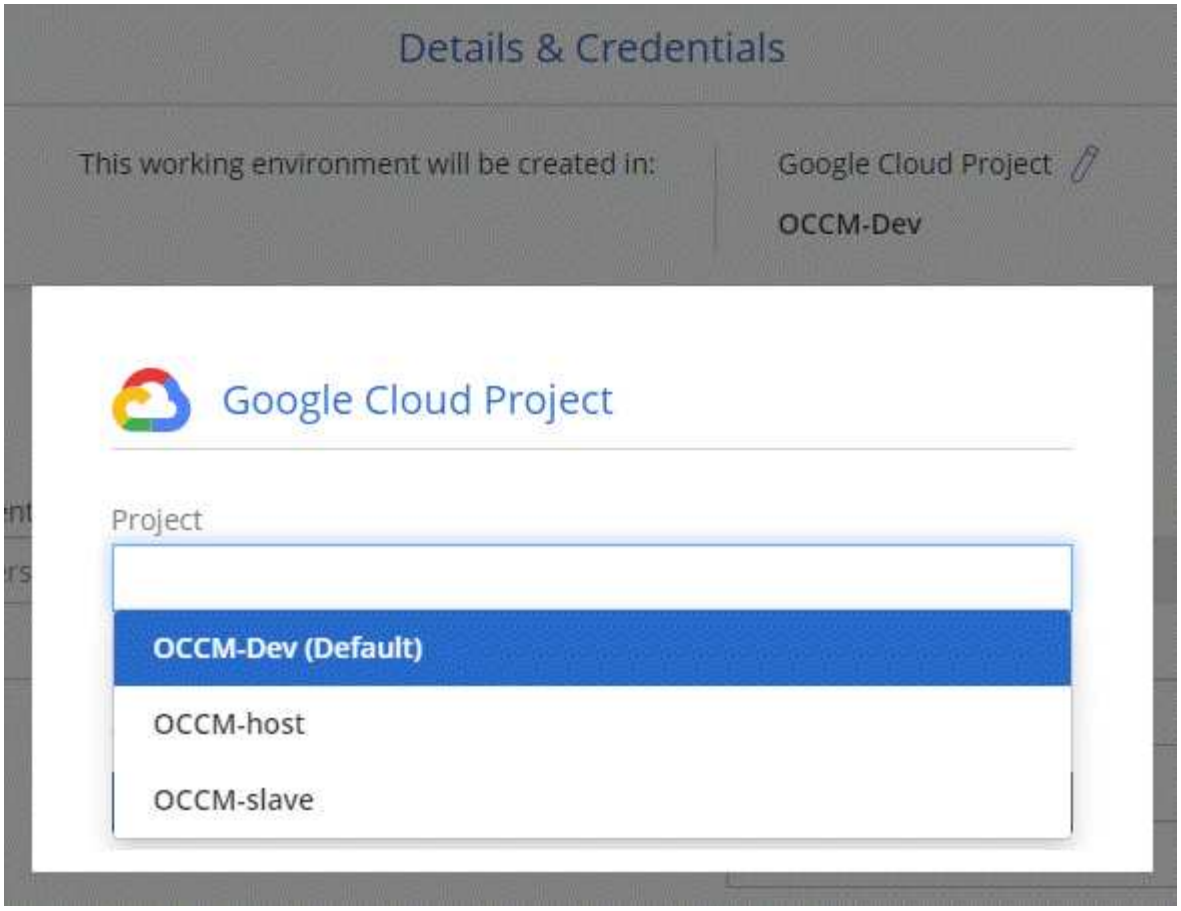
**Shared VPC**

Cloud Manager and Cloud Volumes ONTAP are now supported in a Google Cloud Platform shared VPC.

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 Cloud Manager and Cloud Volumes ONTAP virtual machine instances in a *service project*. Google Cloud documentation: Shared VPC overview.

**Multiple Google Cloud projects**

Cloud Volumes ONTAP no longer needs to be in the same project as Cloud Manager. Add the Cloud Manager service account and role to additional projects and then you can choose from those projects you deploy Cloud Volumes ONTAP.




For more details about setting up the Cloud Manager service account, see step 4b on this page.

**Customer-managed encryption keys when using Cloud Manager APIs**

While Google Cloud Storage always encrypts your data before it's written to disk, you can use Cloud Manager APIs to create a new 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.

Refer to the API Developer Guide for details about using the "GcpEncryption" parameters.

This feature requires new permissions as shown in the latest Cloud Manager policy for GCP:

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

#### Backup to S3 enhancement

You can now delete the backups for existing volumes. Previously, you could only delete the backups for volumes that had been deleted.

Learn more about Backup to S3.

#### Encryption of boot and root disks in AWS

When you enable data encryption using the AWS Key Management Service (KMS), the boot and root disks for Cloud Volumes ONTAP are now 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.

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

#### Support for the AWS Bahrain region

Cloud Manager and Cloud Volumes ONTAP are now supported in the AWS Middle East (Bahrain) region.

#### Support for the Azure UAE North region

Cloud Manager and Cloud Volumes ONTAP are now supported in the Azure UAE North region.

View all supported regions.

### Cloud Manager 3.7.3 update (15 Sept 2019)

Cloud Manager now enables you to back up data from Cloud Volumes ONTAP to Amazon S3.

#### Backup to S3

Backup to S3 is an add-on service for Cloud Volumes ONTAP that delivers fully-managed backup and restore capabilities for protection, and long-term archive of your cloud data. Backups are stored in S3 object storage, independent of volume Snapshot copies used for near-term recovery or cloning.

Learn how to get started.

This feature requires an update to the Cloud Manager policy. The following VPC endpoint permissions are now required:

```
"ec2:DescribeVpcEndpoints",
"ec2:CreateVpcEndpoint",
"ec2:ModifyVpcEndpoint",
"ec2:DeleteVpcEndpoints"
```

### Cloud Manager 3.7.3 (11 Sept 2019)

Cloud Manager 3.7.3 includes the following enhancements.

- Discovery and management of Cloud Volumes Service for AWS
- New subscription required in the AWS Marketplace
- Support for AWS GovCloud (US-East)

#### Discovery and management of Cloud Volumes Service for AWS

Cloud Manager now enables you to discover the cloud volumes in your Cloud Volumes Service for AWS subscription. After discovery, you can add additional cloud volumes directly from Cloud Manager. This enhancement provides a single pane of glass from which you can manage your NetApp cloud storage.

Learn how to get started.

#### New subscription required in the AWS Marketplace

A new subscription is available in the AWS Marketplace. This one-time subscription is required to deploy Cloud Volumes ONTAP 9.6 PAYGO (except for your 30-day free trial system). The subscription also enables us to offer add-on features for Cloud Volumes ONTAP PAYGO and BYOL. You'll be charged from this subscription for every Cloud Volumes ONTAP PAYGO system that you create and each add-on feature that you enable.

Starting with version 9.6, this new subscription method replaces the two existing AWS Marketplace subscriptions for Cloud Volumes ONTAP PAYGO to which you previously subscribed. You still need subscriptions through the existing AWS Marketplace pages when deploying Cloud Volumes ONTAP BYOL.

Learn more about each AWS Marketplace page.

#### Support for AWS GovCloud (US-East)

Cloud Manager and Cloud Volumes ONTAP are now supported in the AWS GovCloud (US-East) region.

### General Availability of Cloud Volumes ONTAP in GCP (3 Sept 2019)

Cloud Volumes ONTAP is now generally available in Google Cloud Platform (GCP) when you bring your own license (BYOL). A pay-as-you-go promotion is also available. The promotion offers free licenses for an unlimited number of systems and will expire at the end of September 2019.

- Learn how to get started in GCP
- View supported configurations

### Cloud Manager 3.7.2 (5 Aug 2019)

- FlexCache licenses
- Kubernetes storage classes for iSCSI
- Management of inodes
- Support for the Hong Kong region in AWS
- Support for the Australia Central regions in Azure

#### FlexCache licenses

Cloud Manager now 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.

#### Kubernetes storage classes for iSCSI

When you connect Cloud Volumes ONTAP to a Kubernetes cluster, Cloud Manager now creates two additional Kubernetes storage classes that you can use with iSCSI Persistent Volumes:

- **netapp-file-san**: For binding iSCSI Persistent Volumes to single-node Cloud Volumes ONTAP systems
- **netapp-file-redundant-san**: For binding iSCSI Persistent Volumes to Cloud Volumes ONTAP HA pairs

#### Management of inodes

Cloud Manager now 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.

> Cloud Manager monitors inode usage only when the Capacity Management Mode is set to automatic (this is the default setting).

#### Support for the Hong Kong region in AWS

Cloud Manager and Cloud Volumes ONTAP are now supported in the Asia Pacific (Hong Kong) region in AWS.

#### Support for the Australia Central regions in Azure

Cloud Manager and Cloud Volumes ONTAP are now supported in the following Azure regions:

- Australia Central
- Australia Central 2

See the full list of supported regions.

### Update on backing up and restoring (15 July 2019)

Starting with the 3.7.1 release, Cloud Manager no longer supports downloading a backup and using it to restore your Cloud Manager configuration. You need to follow these steps to restore Cloud Manager.

### Cloud Manager 3.7.1 (1 July 2019)

- This release primarily includes bug fixes.
- It does include one enhancement: Cloud Manager now installs a NetApp Volume Encryption (NVE) license on each Cloud Volumes ONTAP system that is registered with NetApp Support (both new and existing systems).
  - Adding NetApp Support Site accounts to Cloud Manager
  - Registering pay-as-you-go systems
  - Setting up NetApp Volume Encryption

> Cloud Manager does not install the NVE license on systems that reside in the China region.

### Cloud Manager 3.7 update (16 June 2019)

Cloud Volumes ONTAP 9.6 is now available in AWS, Azure, and in Google Cloud Platform as a private preview. To join the private preview, send a request to ng-Cloud-Volume-ONTAP-preview@netapp.com.

See what's new in Cloud Volumes ONTAP 9.6

### Cloud Manager 3.7 (5 June 2019)

- Support for upcoming Cloud Volumes ONTAP 9.6 release

- NetApp Cloud Central accounts
- Backup and restore with the Cloud Backup Service

#### Support for upcoming Cloud Volumes ONTAP 9.6 release

Cloud Manager 3.7 includes support for the upcoming Cloud Volumes ONTAP 9.6 release. The 9.6 release includes a private preview of Cloud Volumes ONTAP in Google Cloud Platform. We'll update the release notes when 9.6 is available.

#### NetApp Cloud Central accounts

We've enhanced how you manage your cloud resources. Each Cloud Manager system will be associated with a *NetApp Cloud Central account*. The account enables multi-tenancy and is planned for other NetApp cloud data services in the future.

In Cloud Manager, a Cloud Central account is a container for your Cloud Manager systems and the *workspaces* in which users deploy Cloud Volumes ONTAP.

Learn how Cloud Central accounts enable multi-tenancy.

Cloud Manager needs access to *https://cloudmanager.cloud.netapp.com* in order to connect to the Cloud Central account service. Open this URL on your firewall to ensure that Cloud Manager can contact the service.

#### Integrating your system with Cloud Central accounts

Some time after you upgrade to Cloud Manager 3.7, NetApp will choose specific Cloud Manager systems to integrate with Cloud Central accounts. During this process, NetApp creates an account, assigns new roles to each user, creates workspaces, and places existing working environments in those workspaces. There's no disruption to your Cloud Volumes ONTAP systems.

If you have questions, refer to this FAQ.

#### Backup and restore with the Cloud Backup Service

The NetApp Cloud Backup Service for Cloud Volumes ONTAP delivers fully-managed backup and restore capabilities for protection and long-term archive of your cloud data. You can integrate the Cloud Backup Service with Cloud Volumes ONTAP for AWS. Backups created by the service are stored in AWS S3 object storage.

Learn more about the Cloud Backup Service.

To get started, install and configure the backup agent and then start backup and restore operations. If you need help, we encourage you to contact us by using the chat icon in Cloud Manager.

This manual process is no longer supported. The Backup to S3 feature was integrated into Cloud Manager in the 3.7.3 release.

## 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.

### Cloud Manager should remain running at all times

Cloud Manager is a key component in the health and billing of Cloud Volumes ONTAP. If Cloud Manager is powered down, Cloud Volumes ONTAP systems will shut down after losing communication with Cloud Manager for longer than 4 days.

### Shared Linux hosts are not supported

Cloud Manager is not supported on a host that is shared with other applications. The host must be a dedicated host.

### Cloud Manager does not 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.

### Active Directory not supported by default with new installations of Cloud Manager

Starting with version 3.4, new installations of Cloud Manager do not support using your organization's Active Directory authentication for user management. If needed, NetApp can help you set up Active Directory with Cloud Manager. Click the chat icon in the lower right of Cloud Manager to get assistance.

### Limitations with the AWS GovCloud (US) region

- Cloud Manager must be deployed in the AWS GovCloud (US) region if you want to launch Cloud Volumes ONTAP instances in the AWS GovCloud (US) region.
- When deployed in the AWS GovCloud (US) region, Cloud Manager cannot discover ONTAP clusters in a NetApp Private Storage for Microsoft Azure configuration or a NetApp Private Storage for SoftLayer configuration.

### Cloud Manager does not set up iSCSI volumes

When you create a volume in Cloud Manager using the Storage System View, you can choose the NFS or CIFS protocol. You must use OnCommand System Manager to create a volume for iSCSI.

### Storage Virtual Machine (SVM) limitation

Cloud Volumes ONTAP supports one data-serving SVM and one or more SVMs used for disaster recovery. The one data-serving SVM spans the entire Cloud Volumes ONTAP system (HA pair or single node).

Cloud Manager does not provide any setup or orchestration support for SVM disaster recovery. It also does not

support storage-related tasks on any additional SVMs. You must use System Manager or the CLI for SVM disaster recovery.

# Concepts

## Cloud Manager and Cloud Volumes ONTAP overview

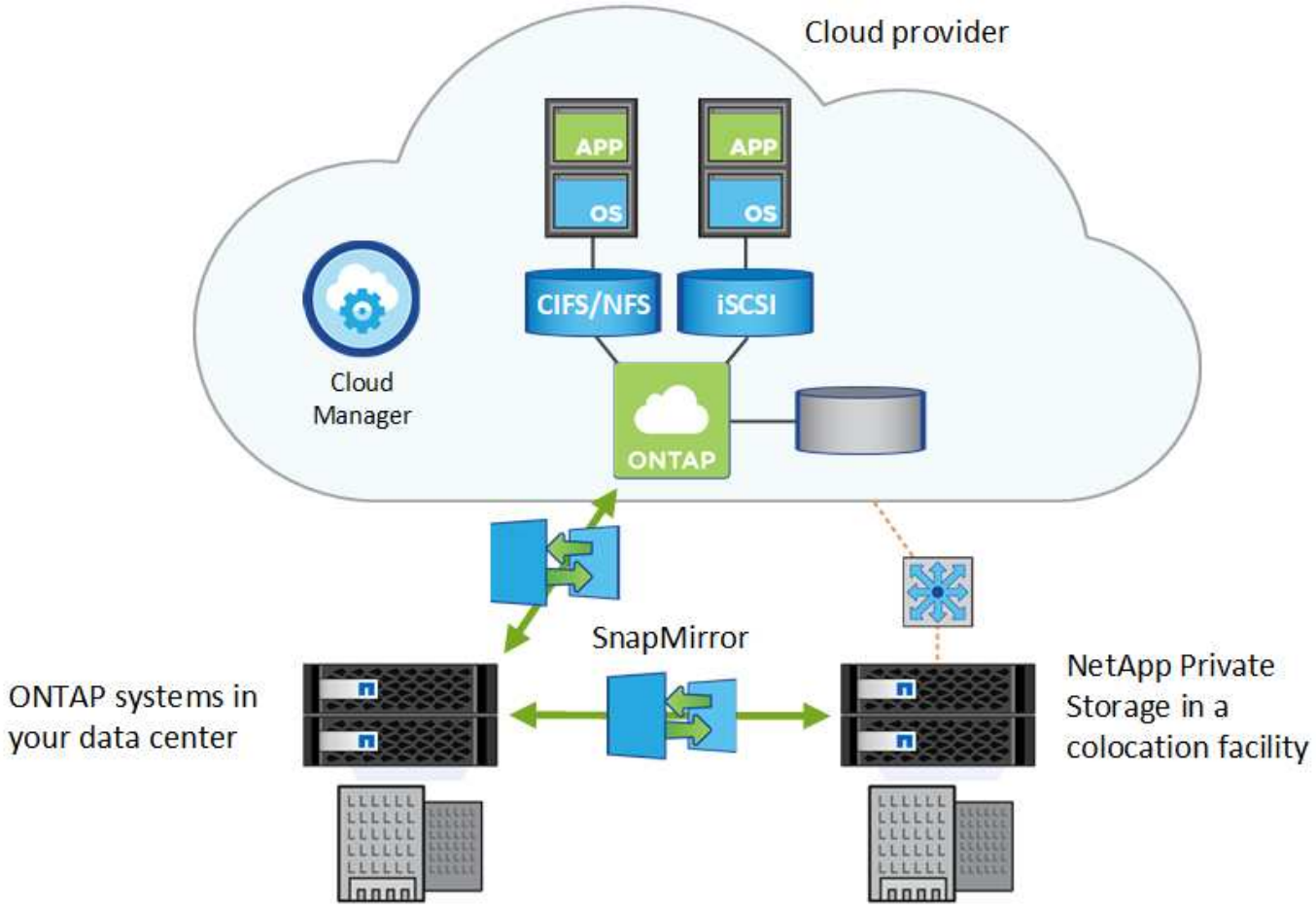
Cloud Manager enables you to deploy Cloud Volumes ONTAP, which provides enterprise-class features for your cloud storage, and to easily replicate data across hybrid clouds built on NetApp.

### Cloud Manager

Cloud Manager was built with simplicity in mind. It guides you through Cloud Volumes ONTAP setup in a few steps, eases data management by offering simplified storage provisioning and automated capacity management, enables drag-and-drop data replication across a hybrid cloud, and more.

Cloud Manager is required to deploy and manage Cloud Volumes ONTAP, but it can also discover and provision storage for on-premises ONTAP clusters. This provides a central point of control for your cloud and on-premises storage infrastructure.

You can run Cloud Manager in the cloud or in your network—it just needs a connection to the networks in which you want to deploy Cloud Volumes ONTAP. The following image shows Cloud Manager and Cloud Volumes ONTAP running in a cloud provider. It also shows data replication across a hybrid cloud.




Learn more about Cloud Manager

### Cloud Volumes ONTAP

Cloud Volumes ONTAP is a software-only storage appliance that runs the ONTAP data management software in the cloud. You can use Cloud Volumes ONTAP for production workloads, disaster recovery, DevOps, file shares, and database management.

Cloud Volumes ONTAP extends enterprise storage to the cloud 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 replication
  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.
- 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.

Licenses for ONTAP features are included with Cloud Volumes ONTAP.

View supported Cloud Volumes ONTAP configurations

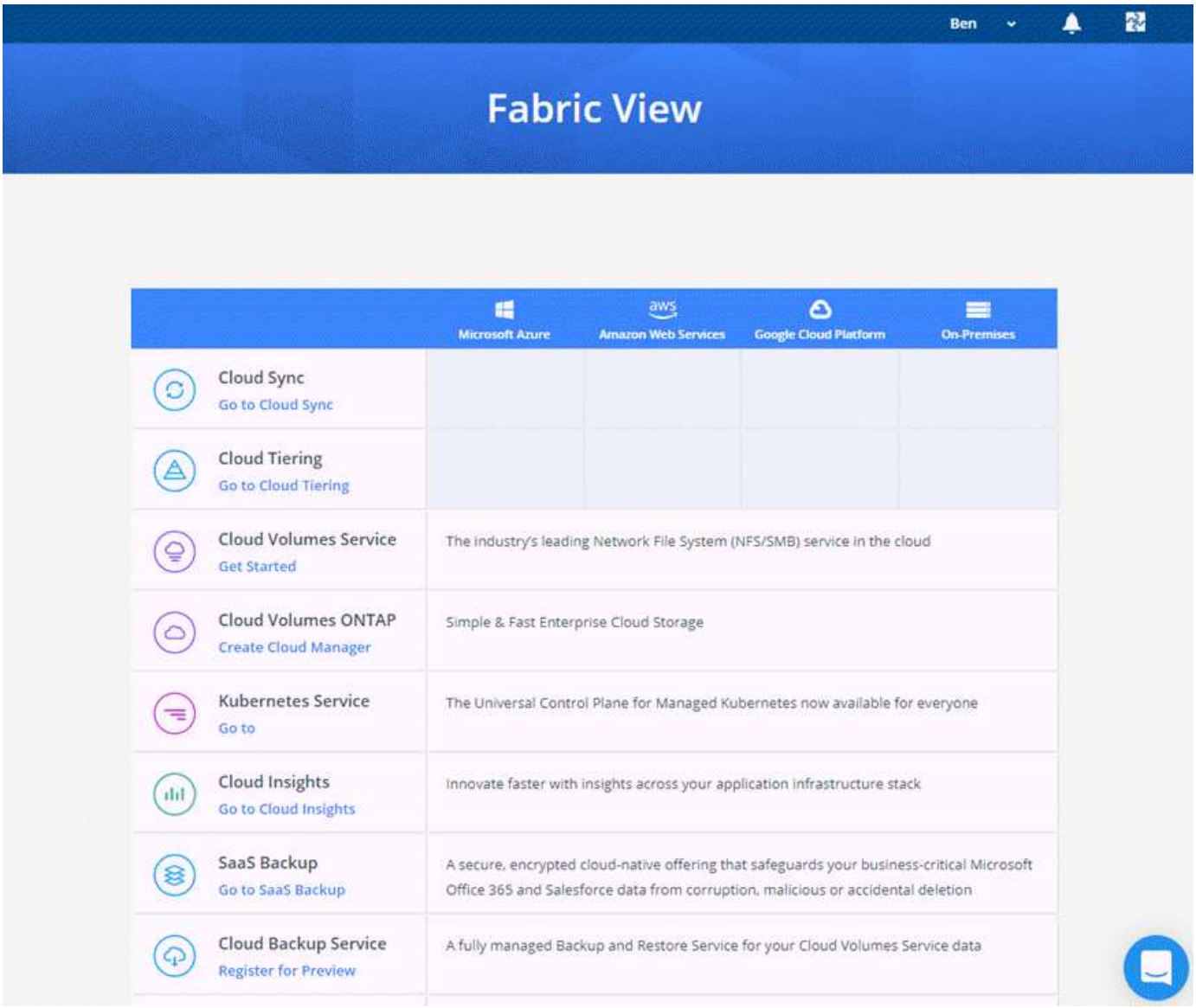
Learn more about Cloud Volumes ONTAP

## NetApp Cloud Central

NetApp Cloud Central provides a centralized location to access and manage NetApp cloud data services. These services enable you to run critical applications in the cloud, create automated DR sites, back up your SaaS data, and effectively migrate and control data across multiple clouds.

Cloud Manager's integration with NetApp Cloud Central provides several benefits, including a simplified deployment experience, a single location to view and manage multiple Cloud Manager systems, and centralized user authentication.

With centralized user authentication, you can use the same set of credentials across Cloud Manager systems and between Cloud Manager and other data services, such as Cloud Sync. It's also easy to reset your password if you forgot it.




# Cloud Central accounts

Each Cloud Manager system is associated with a *NetApp Cloud Central account*. A Cloud Central account provides multi-tenancy and enables you to organize users and resources in isolated workspaces.

A Cloud Central account enables multi-tenancy:

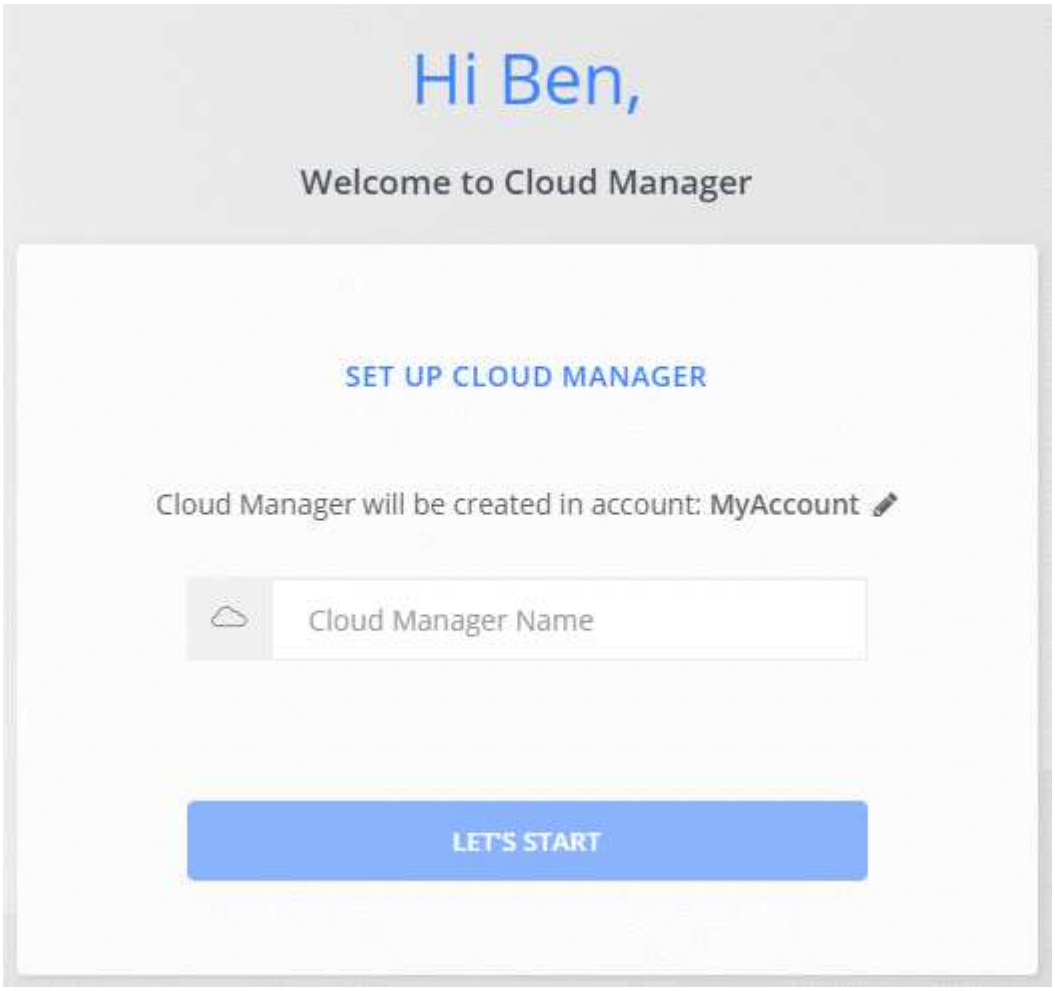
- A single Cloud Central account can include multiple Cloud Manager systems that serve different business needs.

  Because users are associated with the Cloud Central account, there's no need to configure users for each individual Cloud Manager system.

- Within each Cloud Manager system, 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 deploy Cloud Manager, you select the Cloud Central account to associate with the system:




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

For step-by-step instructions, see Setting up the Cloud Central account.

Cloud Manager needs access to *https://cloudmanager.cloud.netapp.com* in order to connect to the Cloud Central account service. Open this URL on your firewall to ensure that Cloud Manager can contact the service.

## Users, workspaces, and service connectors

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, and service connectors that are associated with the account.

**Users**

These 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.

**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

**Service connectors**

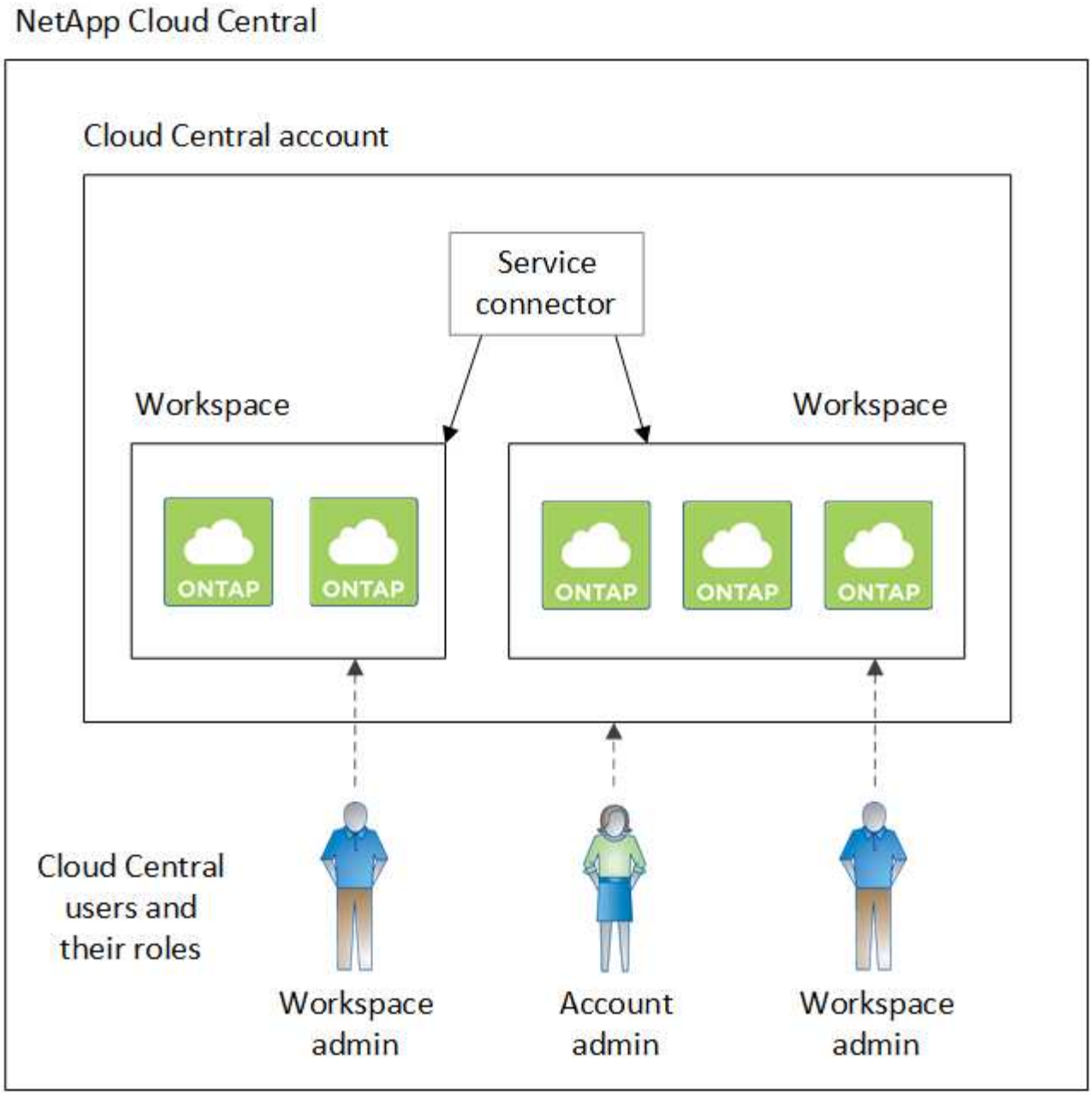
A service connector is part of Cloud Manager. It runs much of the Cloud Manager software (like the user interface), except for a few Cloud Central services that it connects to (auth0 and Cloud Central accounts). The service connector runs on the virtual machine instance that was deployed in your cloud provider, or on an on-prem host that you configured.

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

## Examples

The following example shows an account that uses two workspaces to create isolated environments for Cloud Volumes ONTAP systems. For example, one workspace might be for a staging environment, while the other is for a production environment.

Cloud Manager 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.




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 Cloud Central 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 service connectors. This might happen if you have systems in separate regions or in separate cloud providers.

Again, Cloud Manager 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.

## FAQ for integration with Cloud Central accounts

Some time after you upgrade to Cloud Manager 3.7, NetApp will choose specific Cloud Manager systems to integrate with Cloud Central accounts. This FAQ can answer questions that you might have about the process.

#### How long does the process take?

Just a few minutes.

#### Will Cloud Manager be unavailable?

No, you can still access your Cloud Manager system.

#### What about Cloud Volumes ONTAP?

There's no disruption to your Cloud Volumes ONTAP systems.

#### What happens during this process?

NetApp does the following during the integration process:

1. Creates a new Cloud Central account and associates it with your Cloud Manager system.
2. Assigns new roles to each existing user:
    - Cloud Manager Admins become Account Admins
    - Tenant Admins and Working Environment Admins become Workspace Admins
3. Creates workspaces that replace existing tenants.
4. Places your working environments in those workspaces.
5. Associates the service connector with all workspaces.

#### Does it matter where I installed my Cloud Manager system?

No. NetApp will integrate systems with Cloud Central accounts no matter where they reside, whether that's in AWS, Azure, or on your premises.

# Cloud provider accounts

## AWS accounts and permissions

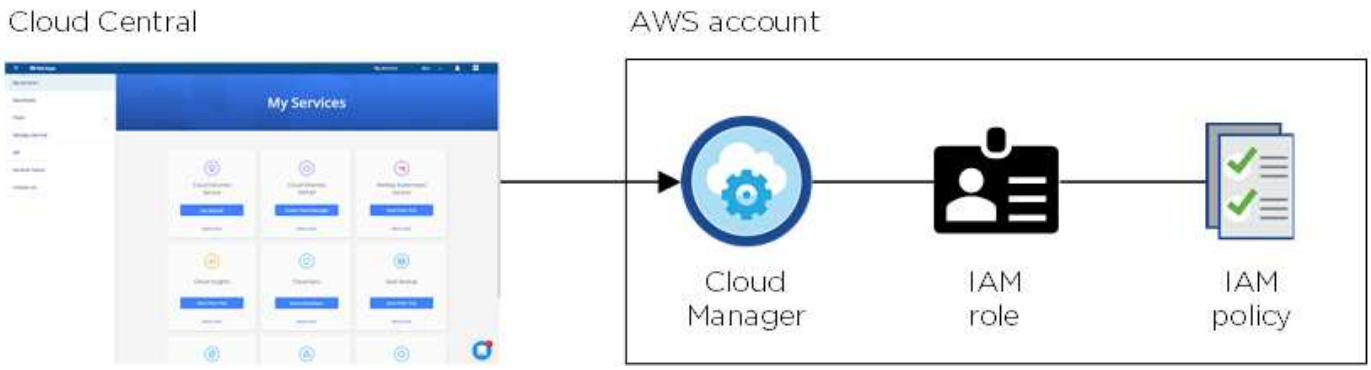
Cloud Manager enables you to choose the AWS account in which you want to deploy a Cloud Volumes ONTAP system. You can deploy all of your Cloud Volumes ONTAP systems in the initial AWS account, or you can set up additional accounts.

#### The initial AWS account

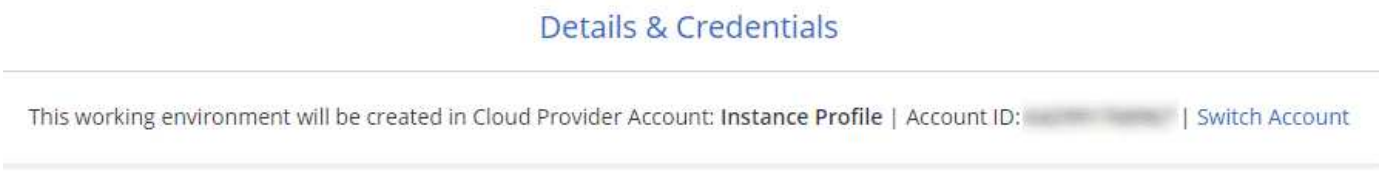
When you deploy Cloud Manager from NetApp Cloud Central, you need to use an AWS account that has permissions to launch the Cloud Manager instance. The required permissions are listed in the NetApp Cloud Central policy for AWS.

When Cloud Central launches the Cloud Manager 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 deploy and

manage Cloud Volumes ONTAP in that AWS account. Review how Cloud Manager uses the permissions.

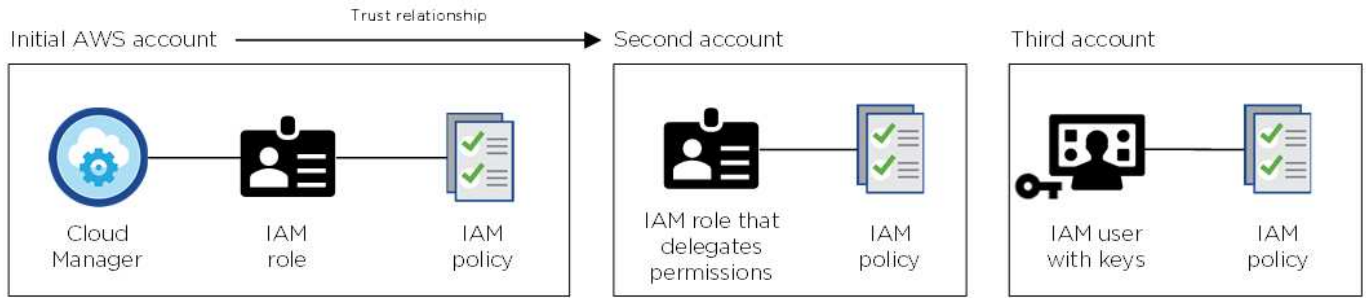



Cloud Manager selects this cloud provider account by default when you create a new working environment:



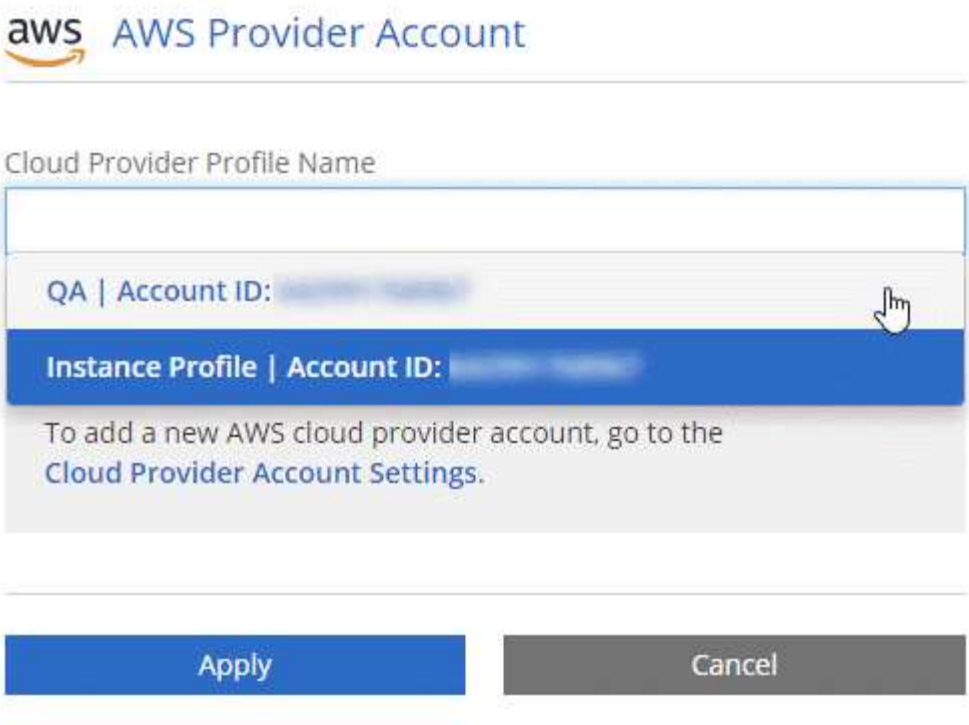

### Additional AWS accounts

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 cloud provider accounts 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 account, you can switch to it when creating a new working environment:




### What about Marketplace deployments and on-prem deployments?

The sections above describe the recommended deployment method from NetApp Cloud Central. You can also deploy Cloud Manager in AWS from the AWS Marketplace and you can install Cloud Manager 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.

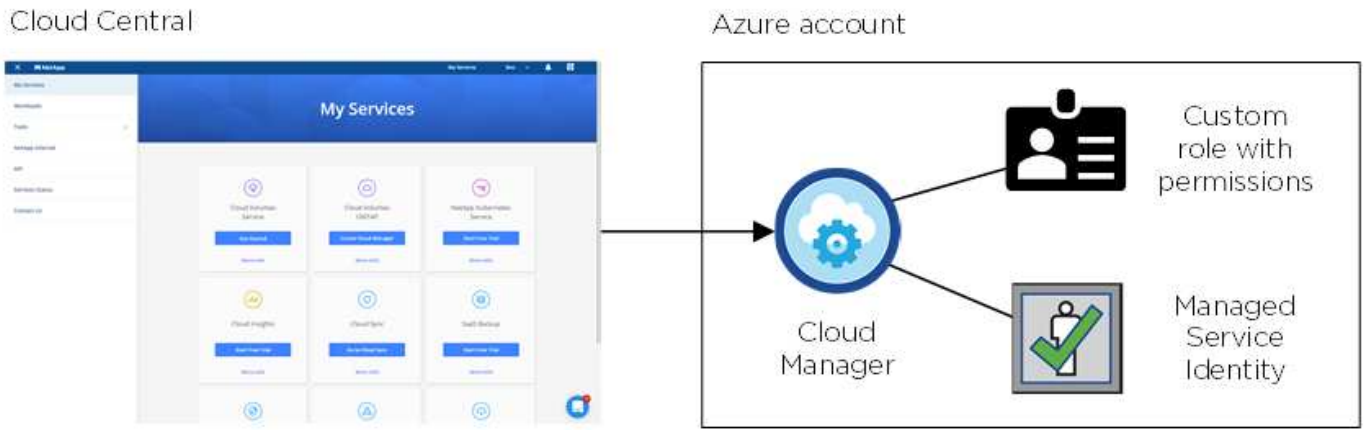
## Azure accounts and permissions

Cloud Manager enables you to choose the Azure account in which you want to deploy a Cloud Volumes ONTAP system. You can deploy all of your Cloud Volumes ONTAP systems in the initial Azure account, or you can set up additional accounts.

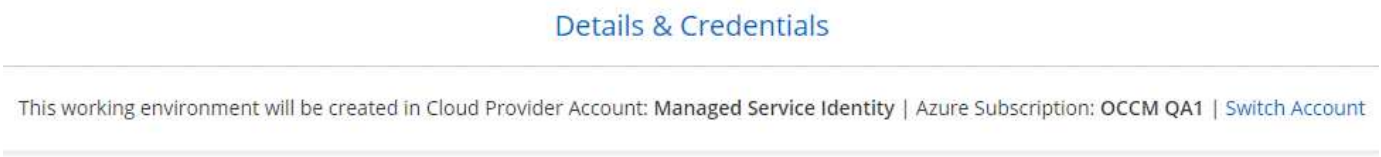
#### The initial Azure account

When you deploy Cloud Manager from NetApp Cloud Central, you need to use an Azure account that has permissions to deploy the Cloud Manager virtual machine. The required permissions are listed in the NetApp Cloud Central policy for Azure.

When Cloud Central deploys the Cloud Manager virtual machine in Azure, it enables a system-assigned managed identity on the Cloud Manager virtual machine, creates a custom role, and assigns it to the virtual machine. The role provides Cloud Manager with permissions to deploy and manage Cloud Volumes ONTAP in that Azure subscription. Review how Cloud Manager uses the permissions.




Cloud Manager selects this cloud provider account by default when you create a new working environment:




**Additional Azure subscriptions for the initial account**

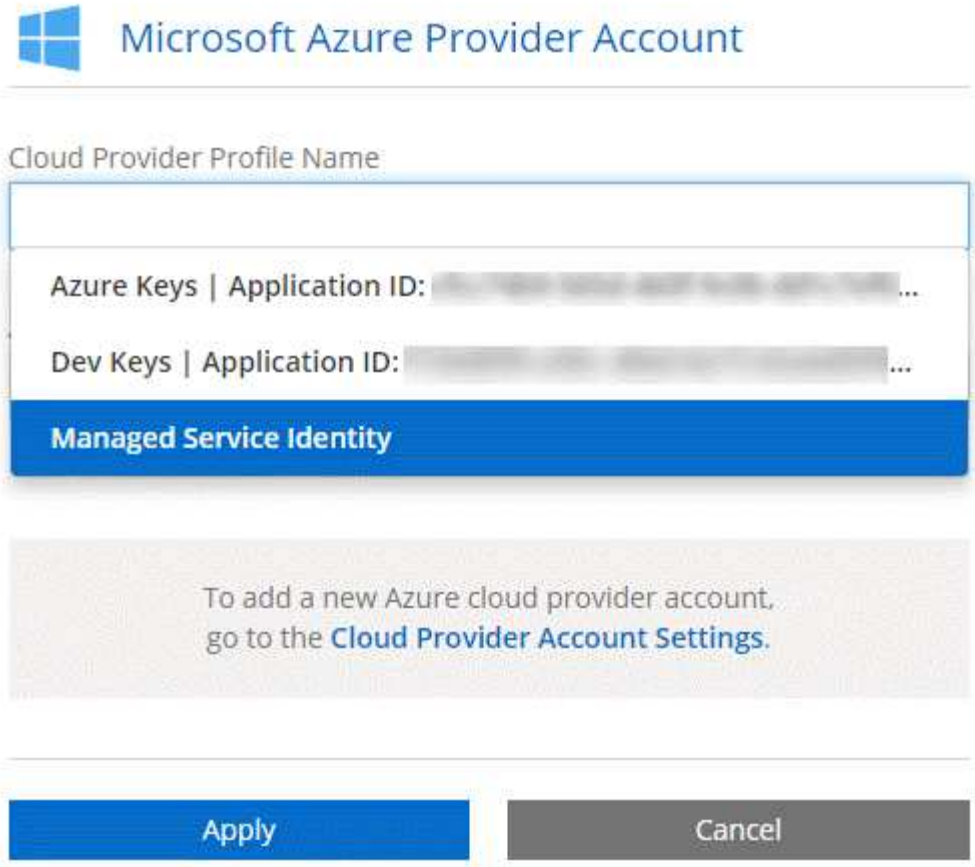
The managed identity is associated with the subscription in which you launched Cloud Manager. If you want to select a different Azure subscription, then you need to associate the managed identity with those subscriptions.

**Additional Azure accounts**

If you want to deploy Cloud Volumes ONTAP in different Azure accounts, 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 cloud provider accounts to Cloud Manager by providing details about the AD service principal.

After you add another account, you can switch to it when creating a new working environment:




### What about Marketplace deployments and on-prem deployments?

The sections above describe the recommended deployment method from NetApp Cloud Central. You can also deploy Cloud Manager in Azure from the Azure Marketplace, and you can install Cloud Manager 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 Cloud Manager, and then provide permissions for any additional accounts.

For on-premises deployments, you can't set up a managed identity for the Cloud Manager system, but you can provide permissions just like you would for additional accounts.

## 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. Google Cloud accounts that you add to Cloud Manager are used to enable data tiering.

#### Project and permissions for Cloud Manager

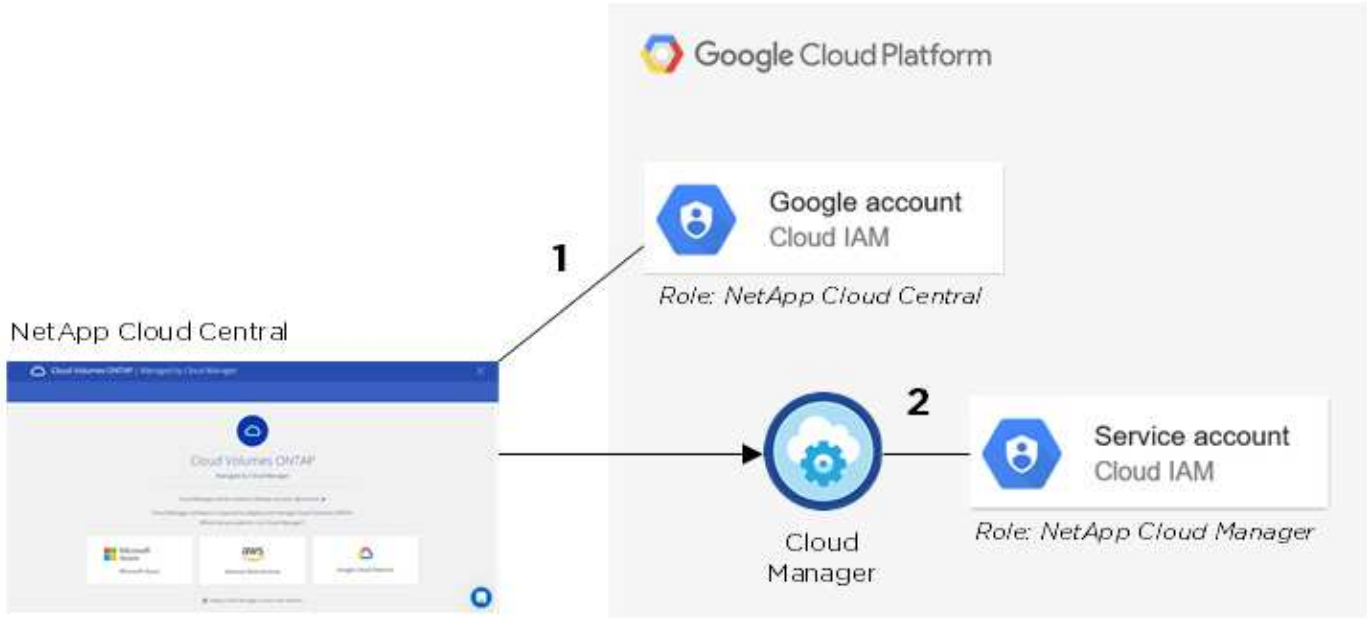
Before you can deploy Cloud Volumes ONTAP in Google Cloud, you must first deploy Cloud Manager in a Google Cloud project. Cloud Manager can't be running on your premises, or in a different cloud provider.

Two sets of permissions must be in place before you deploy Cloud Manager from NetApp Cloud Central:

1. You need to deploy Cloud Manager using a Google account that has permissions to launch the Cloud Manager VM instance from Cloud Central.
2. When deploying Cloud Manager, 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 Cloud Manager, or in a different project. To deploy Cloud Volumes ONTAP in a different project, you need to first add the Cloud Manager service account and role to that project.

- Learn how to set up the Cloud Manager service account (see step 4).
- Learn how to deploy Cloud Volumes ONTAP in GCP and select a project.

### Account for data tiering

Adding a Google Cloud account to Cloud Manager is required to enable data tiering on a Cloud Volumes ONTAP 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.

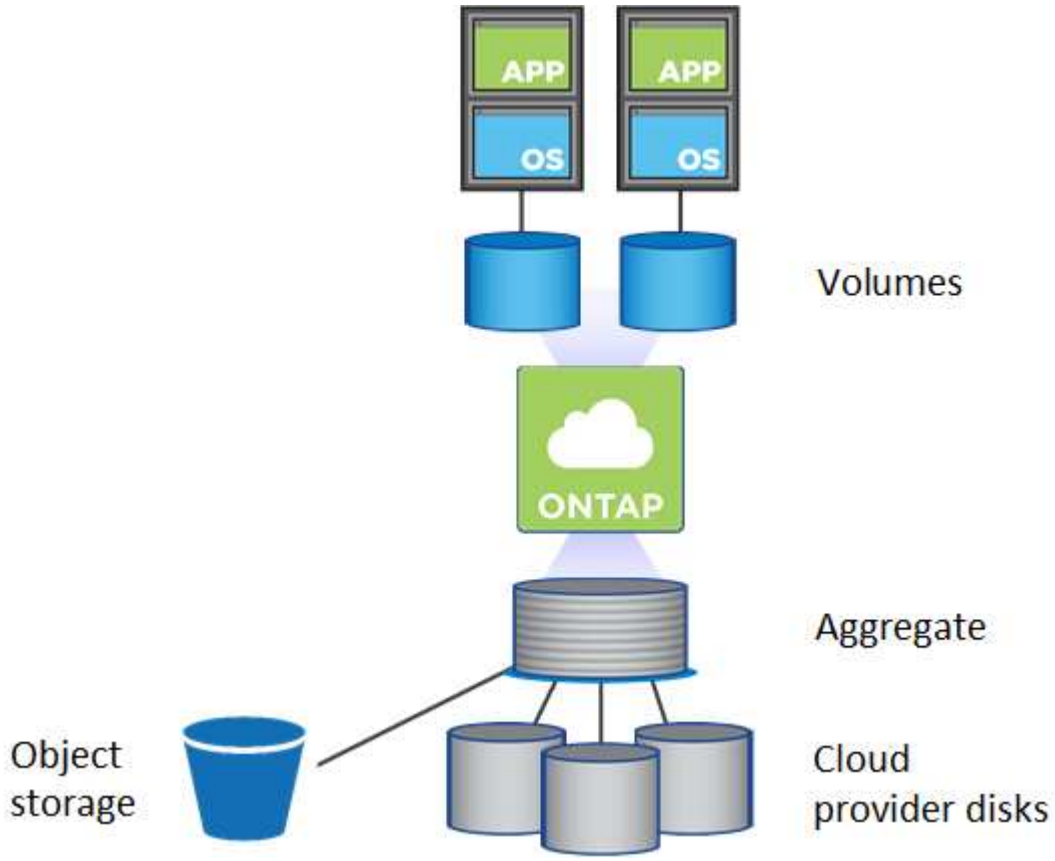
# Storage

## Disks and aggregates

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

### 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

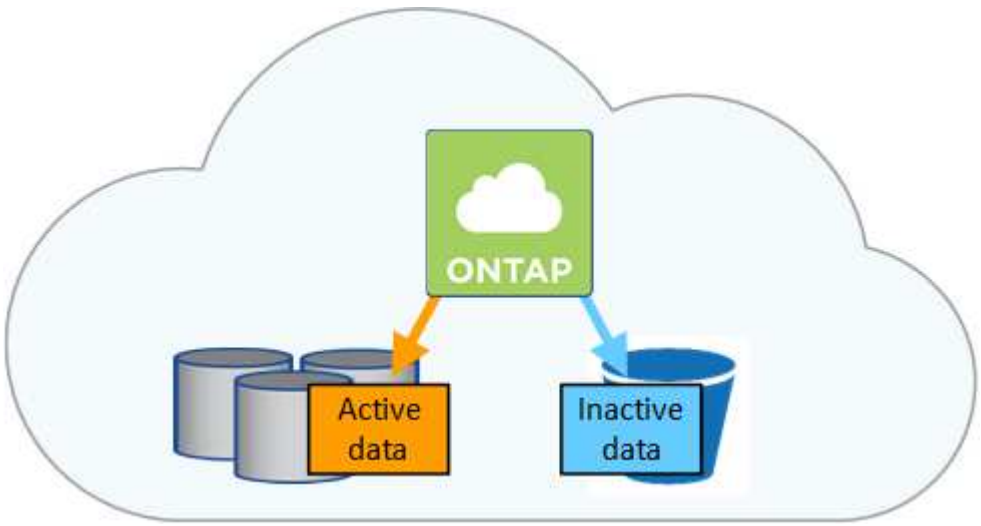
- Google Cloud Platform documentation: Storage Options
- Review storage limits for Cloud Volumes ONTAP in GCP

#### 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 do not 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. Changing a system's tiering level enables you to choose a different S3 storage class.

#### 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.

#### Tiering levels

If you don't plan to access the inactive data, you can reduce your storage costs by changing a system's tiering level to one of the following: *Intelligent Tiering*, *One-Zone Infrequent Access*, or *Standard-Infrequent Access*. When you change the tiering level, inactive data starts in the Standard storage class and moves 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 tiering level. Learn more about Amazon S3 storage classes.

Changing the tiering level is possible after you create the system. For details, see Tiering inactive data to low-cost object storage.

The tiering level is system wide—it is 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. Changing a system's tiering level enables you to choose a different Azure storage tier.

#### 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.

### Tiering levels

If you don't plan to access the inactive data, you can reduce your storage costs by changing a system's tiering level to the Azure *cool* storage tier. When you change the tiering level, inactive data starts in the hot storage tier and moves 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 tiering level. Learn more about Azure Blob storage access tiers.

Changing the tiering level is possible after you create the system. For details, see Tiering inactive data to low-cost object storage.

The tiering level is system wide—it is 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.

### Tiering levels

No other GCP storage classes are supported at this time.

## 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.

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.

**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 might experience longer cooling times.

### 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 cannot be returned to AWS or Azure in this scenario.

- If an aggregate contains no volumes for more than 12 hours, Cloud Manager deletes it.

#### 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.

## 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.

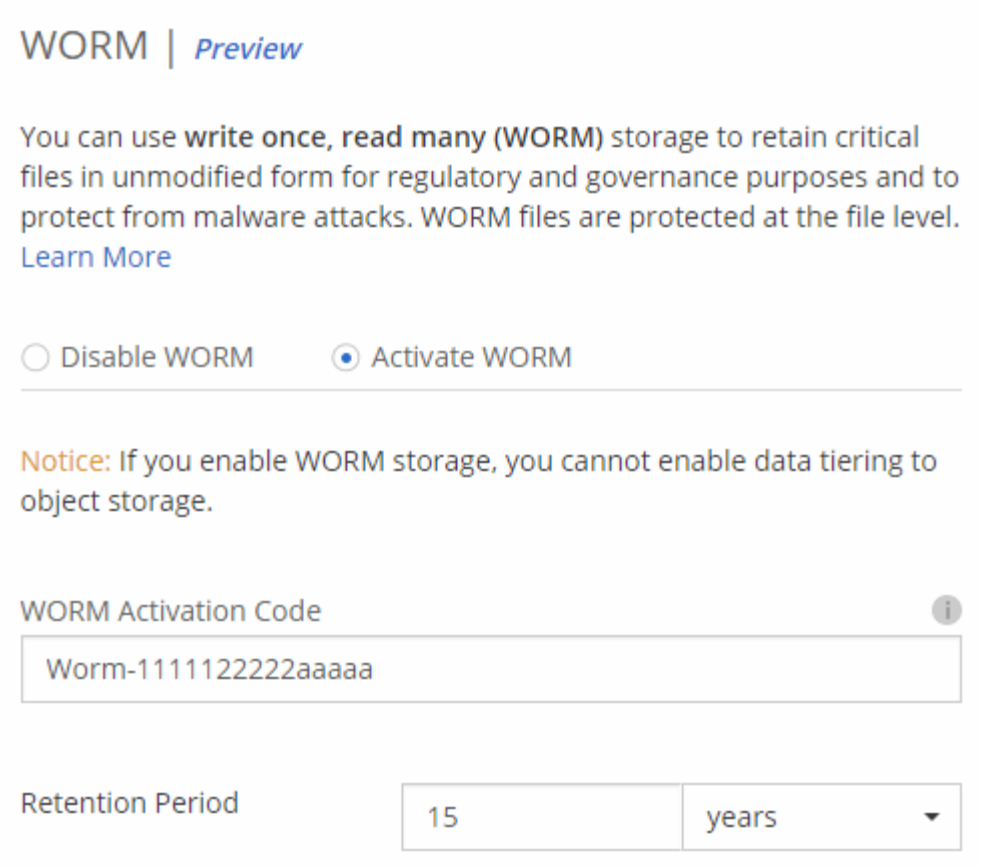
After the retention period has elapsed, you are responsible for deleting any files that you no longer need.

#### 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:




**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 cannot be enabled.

# 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.

#### 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.

## Cloud Volumes ONTAP HA in 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.

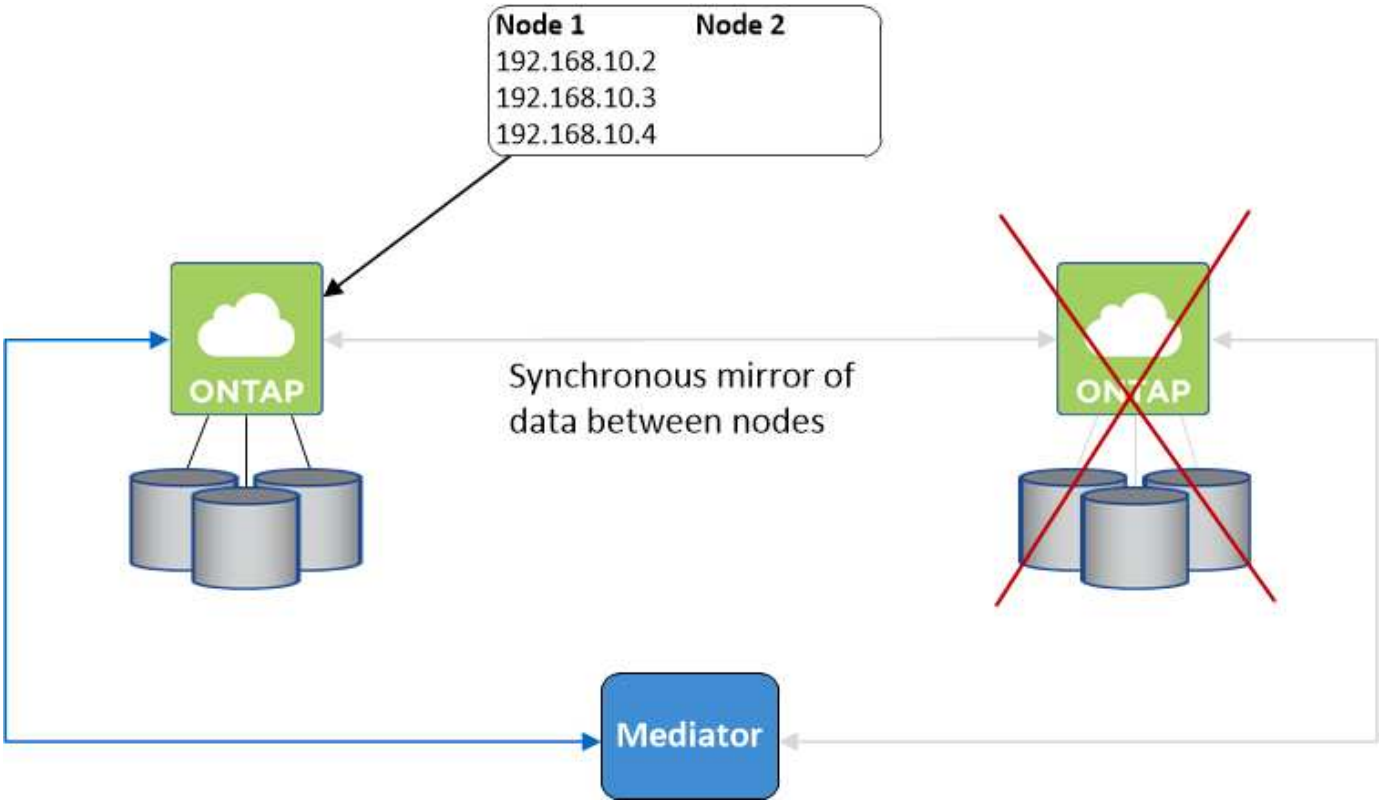
#### Storage takeover and giveback for iSCSI

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.

#### Storage 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

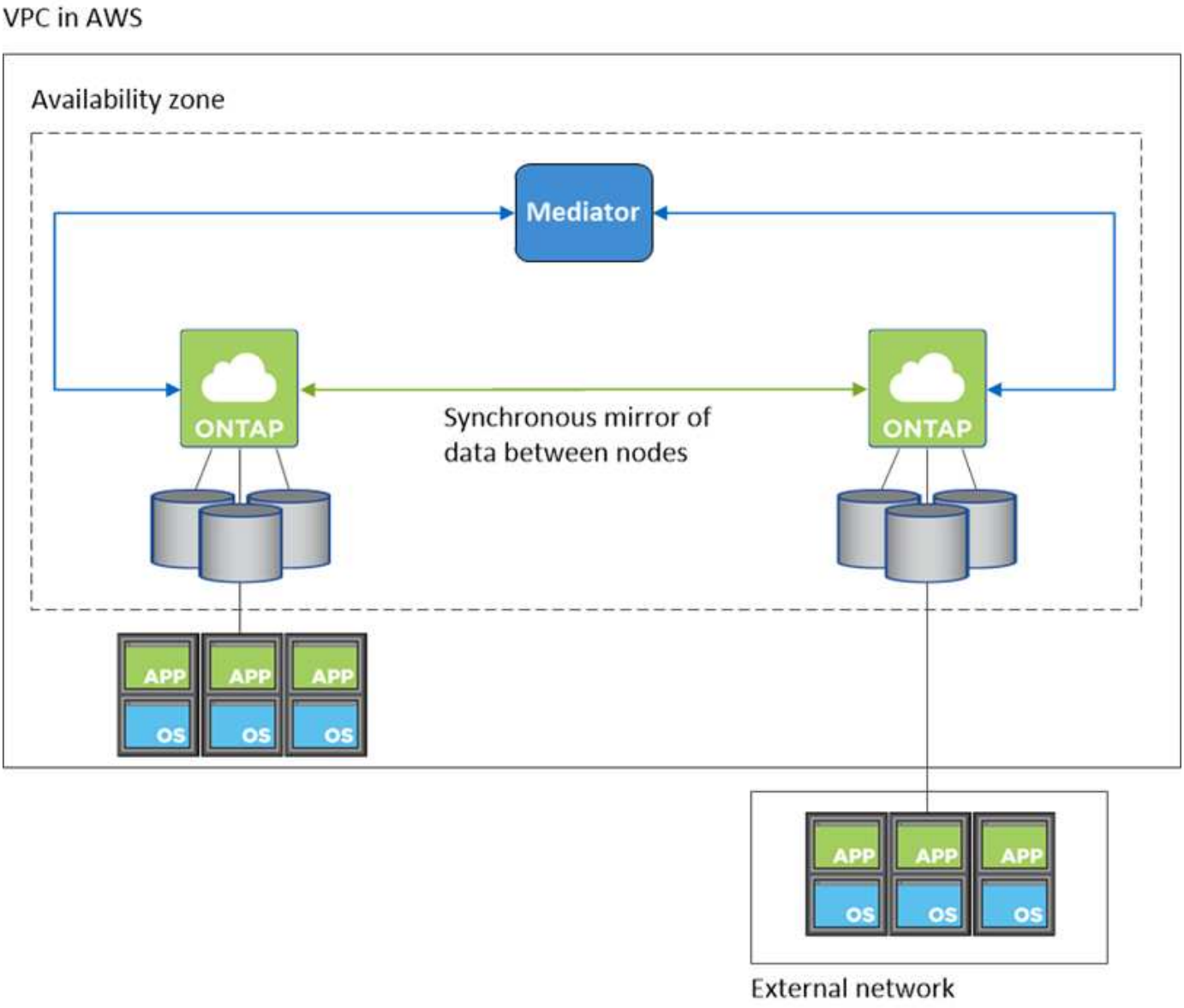
Deploying an HA configuration in a single Availability Zone (AZ) can ensure high availability of your data if an instance that runs a Cloud Volumes ONTAP node fails. All data is natively accessible from outside of the VPC.

> 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.



#### Storage 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 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.

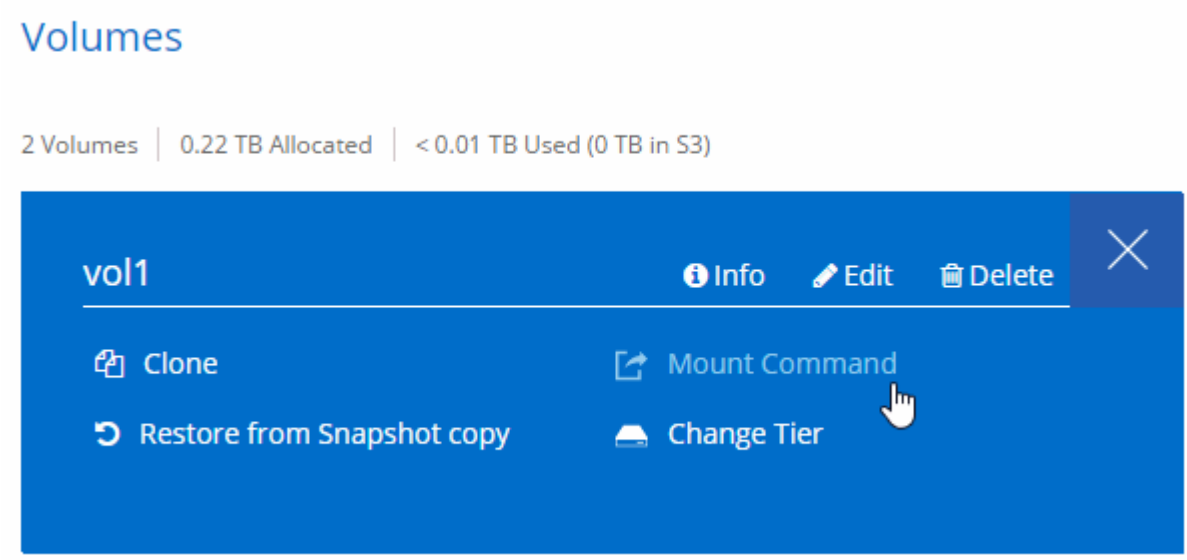
For more details about Cloud Volumes ONTAP performance, see Performance.

#### 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:

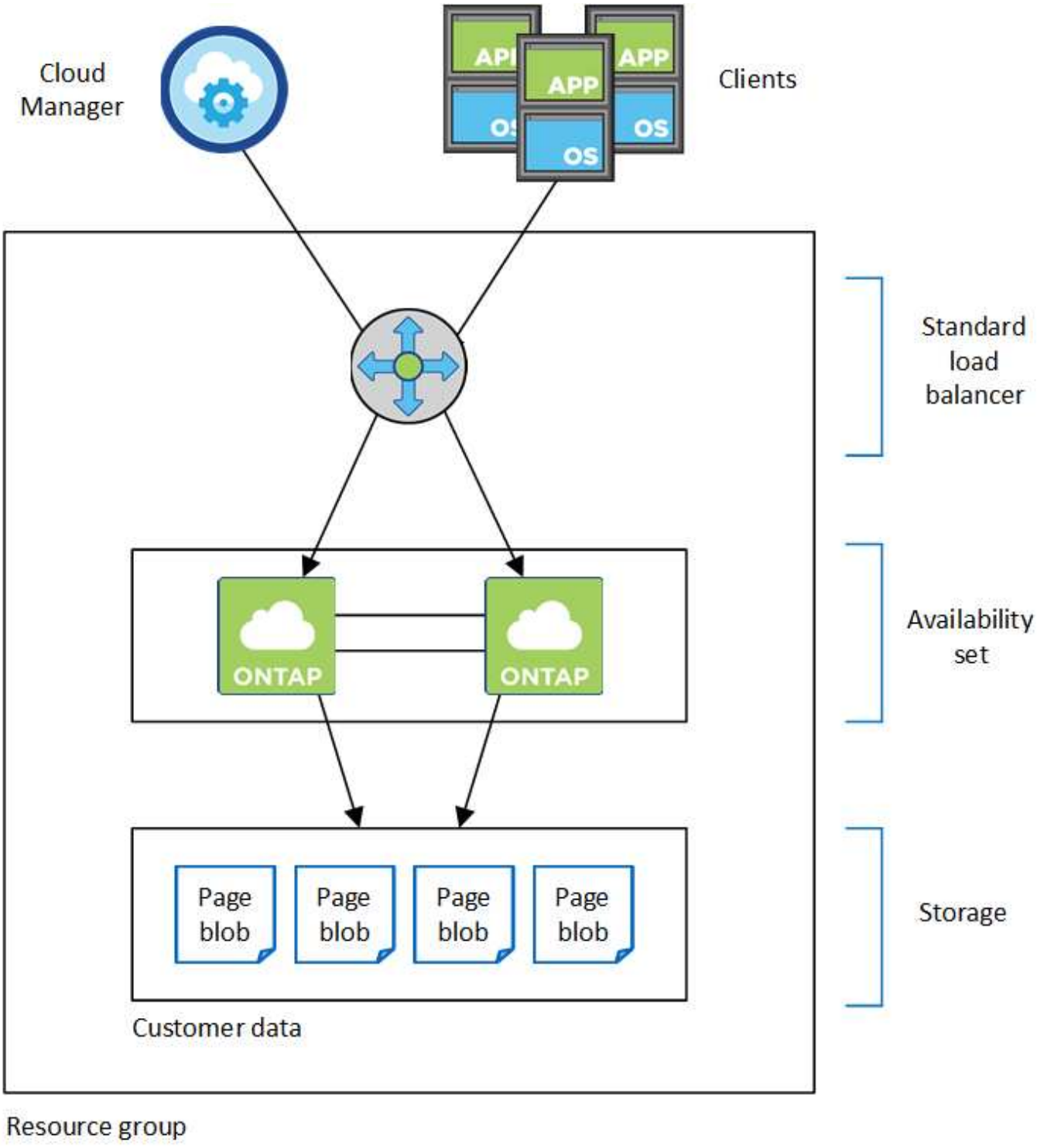



## High-availability pairs in Azure

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:




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:

- Two 90 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 128 GB Standard HDD disks for saving cores (one per node)

### 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.

### 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 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.

# Evaluating

You can evaluate Cloud Volumes ONTAP before you pay for the software.

A 30-day free trial of a single-node Cloud Volumes ONTAP system is available from NetApp Cloud Central. There are no hourly software charges, but infrastructure charges still apply. A free trial automatically converts to a paid hourly subscription when it expires.

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.

# Licensing

Each Cloud Volumes ONTAP BYOL system must have a license installed with an active subscription. If an active license is not installed, the Cloud Volumes ONTAP system shuts itself down after 30 days. Cloud Manager simplifies the process by managing licenses for you and by notifying you before they expire.

### License management for a new system

When you create a BYOL system, Cloud Manager prompts you for a 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 cannot 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 Installing license files on Cloud Volumes ONTAP BYOL systems.

### License expiration

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 do not 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 cannot 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 Installing license files on Cloud Volumes ONTAP BYOL systems.

# 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 Volume Encryption (starting with Cloud Volumes ONTAP 9.5)
- AWS Key Management Service
- Azure Storage Service Encryption
- Google Cloud Platform default encryption

You can use NetApp Volume Encryption with native AWS, Azure, or GCP encryption, which encrypt data at the hypervisor level.

#### NetApp Volume Encryption

NetApp Volume Encryption (NVE) is a software-based technology for encrypting data at rest one volume at a time. Data, Snapshot copies, and metadata are encrypted. Access to the data is given by a unique XTS-AES-256 key, one per volume.

Cloud Volumes ONTAP supports NetApp Volume Encryption with an external key management server. An Onboard Key Manager is not supported. You can find the supported key managers in the NetApp

Interoperability Matrix Tool under the **Key Managers** solution.

You can enable NetApp Volume Encryption on a new or existing volume by using the CLI or System Manager. Cloud Manager does not support NetApp Volume Encryption. For instructions, see Encrypting volumes with NetApp Volume Encryption.

#### 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.

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

#### 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.

Refer to the API Developer Guide for details about using the "GcpEncryption" parameters.

## 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

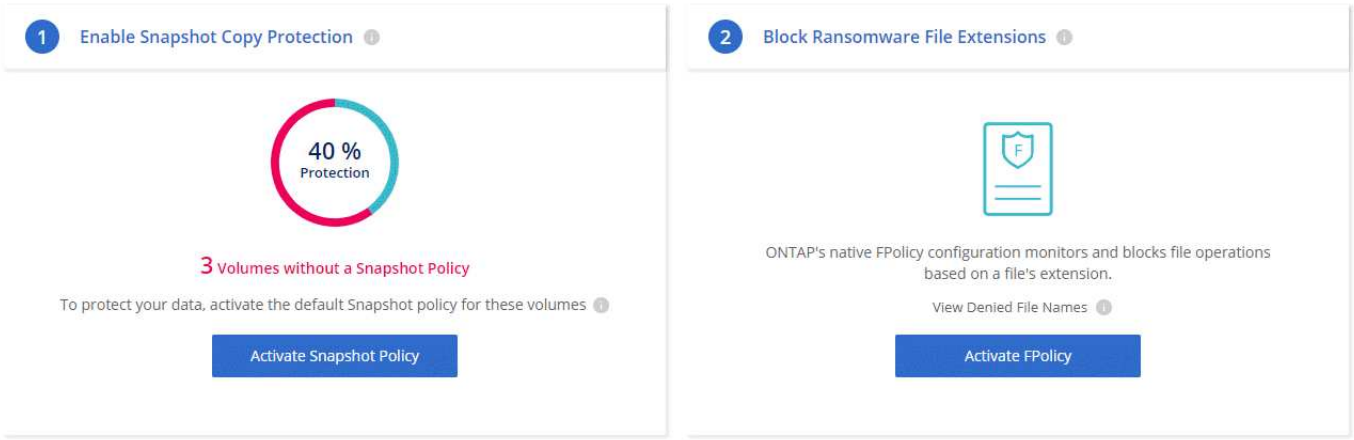
Ransomware attacks can cost a business time, resources, and reputation. Cloud Manager enables you to implement the NetApp solution for ransomware, which provides effective tools for visibility, detection, and

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.




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.

For Cloud Volumes ONTAP for AWS, refer to NetApp Technical Report 4383: Performance Characterization of Cloud Volumes ONTAP in Amazon Web Services with Application Workloads.

For Cloud Volumes ONTAP for Microsoft Azure, refer to NetApp Technical Report 4671: Performance Characterization of Cloud Volumes ONTAP in Azure with Application Workloads.

# Get started

## Deployment overview

Before you get started, you might want to better understand your options for deploying Cloud Manager and Cloud Volumes ONTAP.

### Cloud Manager installation

Cloud Manager software is required to deploy and manage Cloud Volumes ONTAP. You can deploy Cloud Manager in any of the following locations:

- Amazon Web Services (AWS)
- Microsoft Azure
- Google Cloud Platform

  Cloud Manager must be in Google Cloud Platform when deploying Cloud Volumes ONTAP in GCP.

- IBM Cloud
- In your own network

How you deploy Cloud Manager depends on which location you choose:

| Location for Cloud Manager | How to deploy Cloud Manager |
|---|---|
| AWS | 1. Deploy Cloud Manager from NetApp Cloud Central (recommended)<br>2. Deploy from the AWS Marketplace<br>3. Download and install the software on a Linux host |
| AWS C2S | Deploy Cloud Manager from the AWS Intelligence Community Marketplace |
| Azure generally available region | 1. Deploy Cloud Manager from NetApp Cloud Central (recommended)<br>2. Deploy from the Azure Marketplace<br>3. Download and install the software on a Linux host |
| Azure Government | Deploy Cloud Manager from the Azure US Government Marketplace |
| Azure Germany | Download and install the software on a Linux host |
| Google Cloud Platform | 1. Deploy Cloud Manager from NetApp Cloud Central (recommended)<br>2. Download and install the software on a Linux host<br>ⓘ You can’t deploy Cloud Manager in Google Cloud from the GCP Marketplace |

| Location for Cloud Manager | How to deploy Cloud Manager |
|---|---|
| IBM Cloud | Download and install the software on a Linux host |
| On-premises network | Download and install the software on a Linux host |

### Cloud Manager setup

You might want to perform additional setup after you install Cloud Manager, such as adding additional cloud provider accounts, installing an HTTPS certificate, and more.

- Setting up your Cloud Central account
- Adding AWS accounts to Cloud Manager
- Adding Azure accounts to Cloud Manager
- Installing an HTTPS certificate
- Setting up the AWS KMS

### Cloud Volumes ONTAP deployment

After you get Cloud Manager up and running, you can start deploying Cloud Volumes ONTAP in your cloud provider.

Getting started in AWS, Getting started in Azure, and Getting started in GCP provide instructions for getting Cloud Volumes ONTAP up and running quickly. For additional help, refer to the following:

- Supported configurations for Cloud Volumes ONTAP 9.7 in AWS
- Supported configurations for Cloud Volumes ONTAP 9.7 in Azure
- Supported configurations for Cloud Volumes ONTAP 9.7 in GCP
- Planning your configuration
- Launching Cloud Volumes ONTAP in AWS
- Launching Cloud Volumes ONTAP in Azure
- Launching Cloud Volumes ONTAP in GCP

# Getting started with Cloud Volumes ONTAP in AWS

Get started with Cloud Volumes ONTAP by setting up AWS and then launching Cloud Manager software from NetApp Cloud Central. A 30-day free trial is available for the first Cloud Volumes ONTAP system that you launch in AWS.

**Set up your networking**

a. Enable outbound internet access from the target VPC so Cloud Manager and Cloud Volumes ONTAP can contact several endpoints.

   This step is important because Cloud Manager can't deploy Cloud Volumes ONTAP without outbound internet access. If you need to limit outbound connectivity, refer to the list of endpoints for Cloud Manager and Cloud Volumes ONTAP.

b. 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.

### Provide the required AWS permissions

When you deploy Cloud Manager from NetApp Cloud Central, you need to use an AWS account that has permissions to deploy the instance.

a. Go to the AWS IAM console and create a policy by copying and pasting the contents of the NetApp Cloud Central policy for AWS.
b. Attach the policy to the IAM user.

### Subscribe from the AWS Marketplace

Subscribe to Cloud Manager from the AWS Marketplace to ensure that there's no disruption of service after your free trial of Cloud Volumes ONTAP ends. You'll be charged from this subscription for every Cloud Volumes ONTAP PAYGO system that you create and each add-on feature that you enable.

If you're launching Cloud Volumes ONTAP by bringing your own license (BYOL), then you'll need to subscribe to that offering in the AWS Marketplace.

### Launch Cloud Manager from NetApp Cloud Central

Cloud Manager software is required to deploy and manage Cloud Volumes ONTAP. It takes just a few minutes to launch a Cloud Manager instance from Cloud Central.

### Launch Cloud Volumes ONTAP using Cloud Manager

Once Cloud Manager is ready, just click Create, select the type of system that you would like to launch, and complete the steps in the wizard. After 25 minutes, your first Cloud Volumes ONTAP system should be up and running.

Watch the following video for a walk through of these steps:

► https://docs.netapp.com/us-en/occm37//media/video_getting_started_aws.mp4 *(video)*

**Related links**

- Evaluating
- Networking requirements for Cloud Manager
- Networking requirements for Cloud Volumes ONTAP in AWS
- Security group rules for AWS
- Adding AWS accounts to Cloud Manager

- What Cloud Manager does with AWS permissions
- Launching Cloud Volumes ONTAP in AWS
- Launching Cloud Manager from the AWS Marketplace

# Getting started with Cloud Volumes ONTAP in Azure

Get started with Cloud Volumes ONTAP by setting up Azure and then deploying Cloud Manager software from NetApp Cloud Central. Separate instructions are available to deploy Cloud Manager in Azure US Government regions and in Azure Germany regions.

### Set up your networking

Enable outbound internet access from the target VNet so Cloud Manager and Cloud Volumes ONTAP can contact several endpoints.

This step is important because Cloud Manager cannot deploy Cloud Volumes ONTAP without outbound internet access. If you need to limit outbound connectivity, refer to the list of endpoints for Cloud Manager and Cloud Volumes ONTAP.

### Provide the required Azure permissions

When you deploy Cloud Manager from NetApp Cloud Central, you need to use an Azure account that has permissions to deploy the Cloud Manager virtual machine.

a. Download the NetApp Cloud Central policy for Azure.
b. Modify the JSON file by adding your Azure subscription ID to the "AssignableScopes" field.
c. Use the JSON file to create a custom role in Azure named *Azure SetupAsService*.

   Example: **az role definition create --role-definition C:\Policy_for_Setup_As_Service_Azure.json**

d. From the Azure portal, assign the custom role to the user who will deploy Cloud Manager from Cloud Central.

### Launch Cloud Manager from NetApp Cloud Central

Cloud Manager software is required to deploy and manage Cloud Volumes ONTAP. It takes just a few minutes to launch a Cloud Manager instance from Cloud Central.

### Launch Cloud Volumes ONTAP using Cloud Manager

Once Cloud Manager is ready, just click Create, select the type of system that you would like to deploy, and complete the steps in the wizard. After 25 minutes, your first Cloud Volumes ONTAP system should be up and running.

**Related links**

- Evaluating
- Networking requirements for Cloud Manager
- Networking requirements for Cloud Volumes ONTAP in Azure
- Security group rules for Azure
- Adding Azure accounts to Cloud Manager
- What Cloud Manager does with Azure permissions
- Launching Cloud Volumes ONTAP in Azure
- Launching Cloud Manager from the Azure Marketplace

# Getting started with Cloud Volumes ONTAP in Google Cloud Platform

Get started with Cloud Volumes ONTAP by setting up GCP and then deploying Cloud Manager software from NetApp Cloud Central.

Cloud Manager must be installed in Google Cloud Platform in order to deploy Cloud Volumes ONTAP in GCP.

**Set up your networking**

Enable outbound internet access from the target VPC so Cloud Manager and Cloud Volumes ONTAP can contact several endpoints.

This step is important because Cloud Manager can't deploy Cloud Volumes ONTAP without outbound internet access. If you need to limit outbound connectivity, refer to the list of endpoints for Cloud Manager and Cloud Volumes ONTAP.

**Set up GCP permissions and projects**

Make sure that two sets of permissions are in place:

a. Ensure that the GCP user who deploys Cloud Manager from NetApp Cloud Central has the permissions in the Cloud Central 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.

b. 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 Cloud Manager VM in step 6.

   - 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 2a.

   - Create a GCP service account and apply the custom role that you just created.

- 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.

### 3 Set up GCP for data tiering

Two requirements must be met to tier cold data from Cloud Volumes ONTAP 9.7 to low-cost object storage (a Google Cloud Storage bucket):

a. Create a service account that has the predefined Storage Admin role and the Cloud Manager service account as a user.

   You'll need to select this service account later when you create a Cloud Volumes ONTAP working environment. This service account is different from the service account that you created in step 2.

b. Configure the Cloud Volumes ONTAP subnet for Private Google Access.

If you want to use data tiering with Cloud Volumes ONTAP 9.6, then follow these steps.

### 4 Enable Google Cloud APIs

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

- Cloud Deployment Manager V2 API
- Cloud Resource Manager API
- Compute Engine API
- Stackdriver Logging API

### 5 Subscribe from the GCP Marketplace

Subscribe to Cloud Volumes ONTAP from the GCP Marketplace to ensure that there's no disruption of service after your free trial ends. You'll be charged from this subscription for every Cloud Volumes ONTAP PAYGO system that you create.

### 6 Launch Cloud Manager from NetApp Cloud Central

Cloud Manager software is required to deploy and manage Cloud Volumes ONTAP. It takes just a few minutes to launch a Cloud Manager instance in GCP from Cloud Central.

When you choose GCP as the cloud provider, you're prompted by Google to log in to your account and to grant permissions. Clicking "Allow" grants access to the compute APIs needed to deploy Cloud Manager.

### 7 Launch Cloud Volumes ONTAP using Cloud Manager

Once Cloud Manager is ready, just click Create, select the type of system that you would like to deploy, and

complete the steps in the wizard. After 25 minutes, your first Cloud Volumes ONTAP system should be up and running.

**Related links**

- Evaluating
- Networking requirements for Cloud Manager
- Networking requirements for Cloud Volumes ONTAP in GCP
- Firewall rules for GCP
- What Cloud Manager does with GCP permissions
- Launching Cloud Volumes ONTAP in GCP
- Downloading and installing the Cloud Manager software on a Linux host

# Set up Cloud Manager

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

Each Cloud Manager system is associated with a *NetApp Cloud Central account*. Set up the Cloud Central account associated with your Cloud Manager system so a user can access Cloud Manager and deploy Cloud Volumes ONTAP systems in workspaces. Just add a user or add multiple users and workspaces.

The account is maintained in Cloud Central, so any changes that you make are available to other Cloud Manager systems and to other NetApp cloud data services. Learn more about how Cloud Central accounts work.

### 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 the workspaces.

**Steps**

1. Click **Account Settings**.


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

**After you finish**

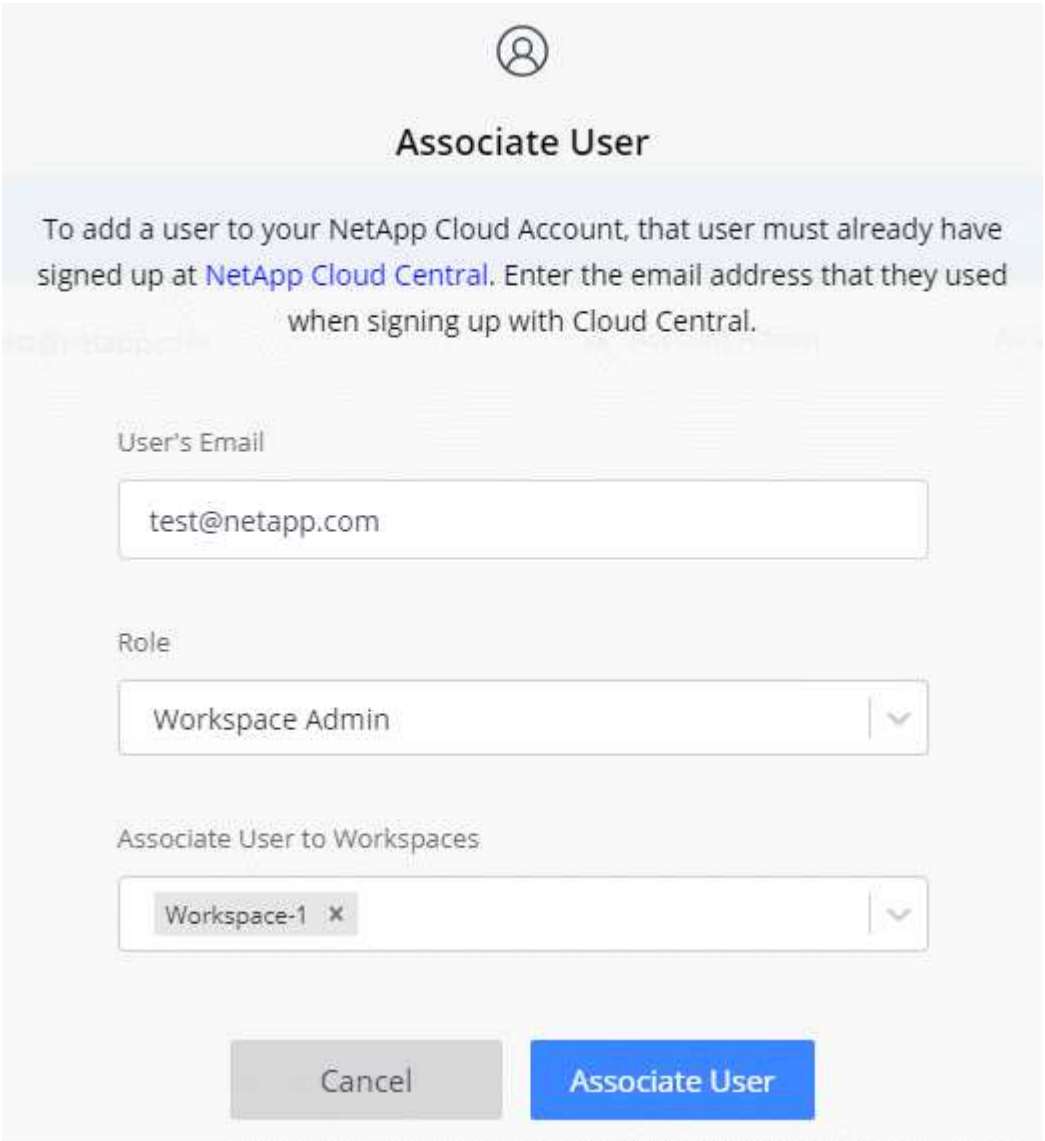
You can now associate users and service connectors with the workspace.

### 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 has not already done so, ask the user to go to NetApp Cloud Central and create an account.
2. In Cloud Manager, click **Account Settings**.
3. In 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.
5. If you selected Workspace Admin, select one or more workspaces to associate with that user.




6. Click **Associate User**.

#### Result

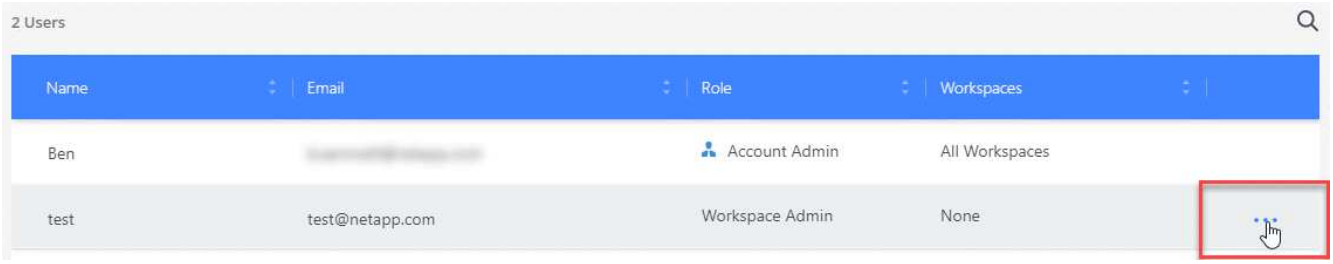
The user should receive an email from NetApp Cloud Central titled "Account Association." The email includes the information needed to access Cloud Manager.

### 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. Click **Account Settings**.
2. Click the action menu in the row that corresponds to the user.




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 service connector was also associated with the workspaces.

### Associating service connectors with workspaces

A service connector is part of the Cloud Manager system. It runs on the virtual machine instance that was deployed in your cloud provider, or on an on-prem host that you configured. You need to associate this service connector with workspaces so Workspace Admins can access those workspaces from Cloud Manager.

If you only have Account Admins, then associating the service 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 service connectors.

#### Steps

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

#### Result

Workspace Admins can now access the associated workspaces, as long as the user was also associated with the workspace.

## Setting up and adding AWS accounts to Cloud Manager

If you want to deploy Cloud Volumes ONTAP in different AWS accounts, then you need to provide the required permissions and add the details to Cloud Manager. 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 deploy Cloud Manager from Cloud Central, Cloud Manager automatically adds the AWS account in which you deployed Cloud Manager. An initial account is not added if you manually installed the Cloud Manager software on an existing system. Learn about AWS accounts and permissions.

### Choices

- Granting permissions by providing AWS keys
- Granting permissions by assuming IAM roles in other accounts

### 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 Cloud Manager 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 Cloud Manager 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 Cloud Manager instance resides and select the IAM role that is attached to the instance.
   a. Click **Trust Relationships > Edit trust relationship**.
   b. Add 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 accounts to Cloud Manager

After you provide an AWS account with the required permissions, you can add the account to Cloud Manager. This enables you to launch Cloud Volumes ONTAP systems in that account.

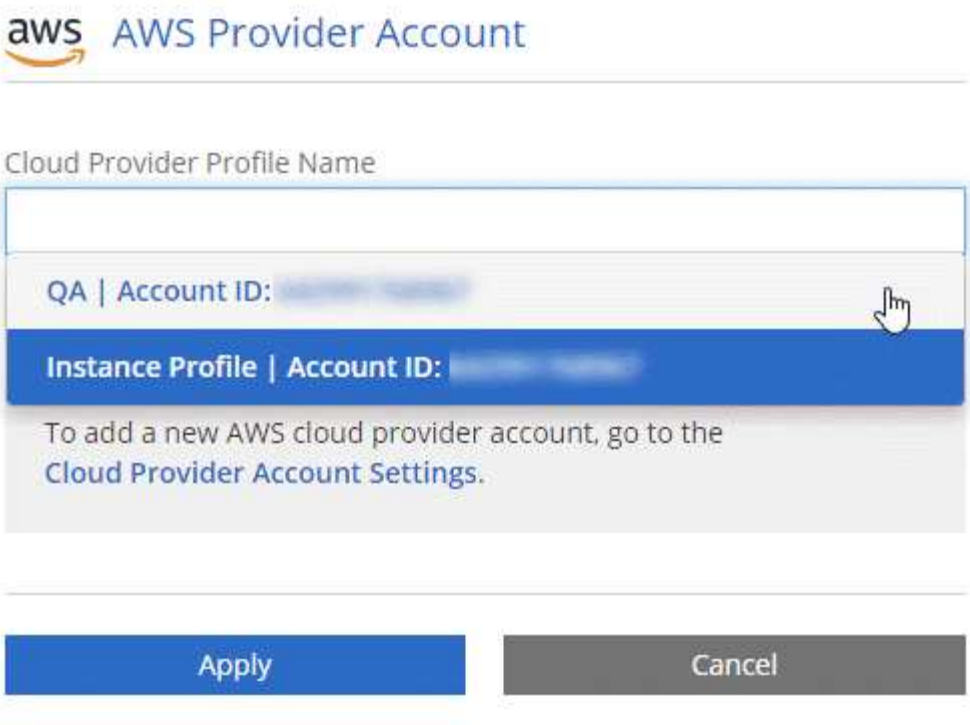
**Steps**

1. In the upper right of the Cloud Manager console, click the Settings icon, and select **Cloud Provider & Support Accounts**.


2. Click **Add New Account** and select **AWS**.
3. Choose whether you want to provide AWS keys or the ARN of a trusted IAM role.
4. Confirm that the policy requirements have been met and then click **Create Account**.

**Result**

You can now switch to another account from the Details and Credentials page when creating a new working environment:




## Setting up and adding Azure accounts to Cloud Manager

If you want to deploy Cloud Volumes ONTAP in different Azure accounts, then you need to provide the required permissions to those accounts and then add details about the accounts to Cloud Manager.

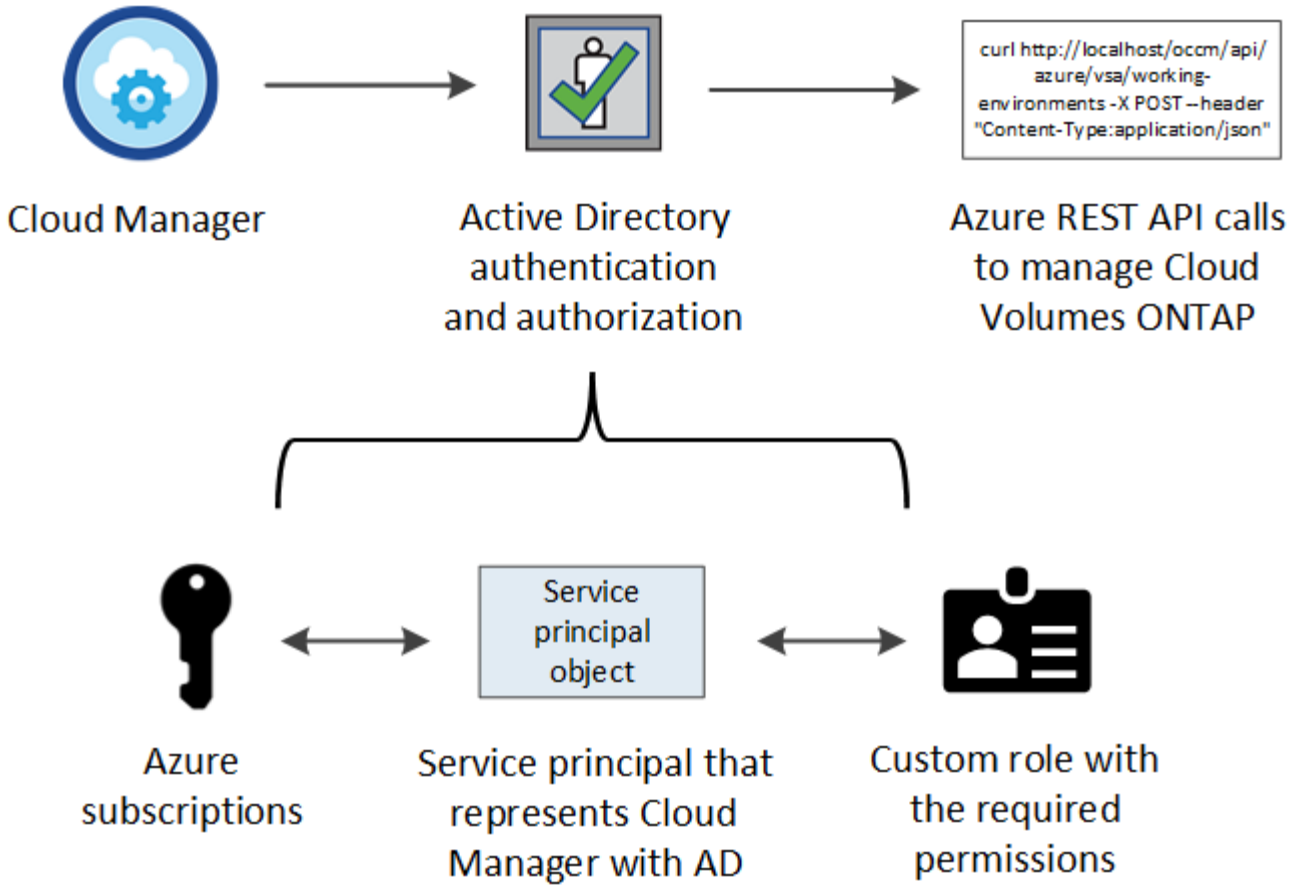
When you deploy Cloud Manager from Cloud Central, Cloud Manager automatically adds the Azure account in which you deployed Cloud Manager. An initial account is not added if you manually installed the Cloud Manager software on an existing system. Learn about Azure accounts and permissions.

### 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

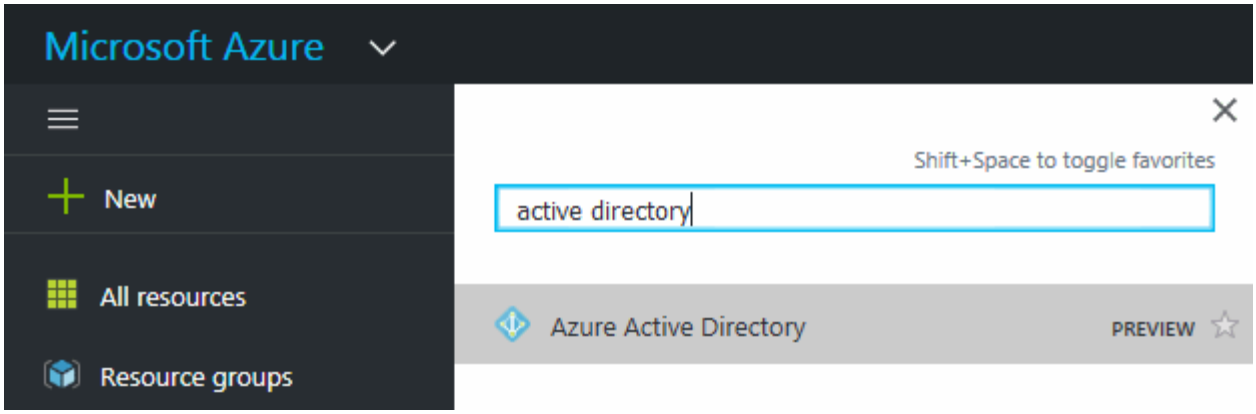
Create an Azure Active Directory (AD) application and service principal that Cloud Manager can use for role-based access control.

**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**: Select **Web** and then enter any URL—for example, https://url
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-c25fbzzzzzzz",
      "/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",
      "/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
      ```

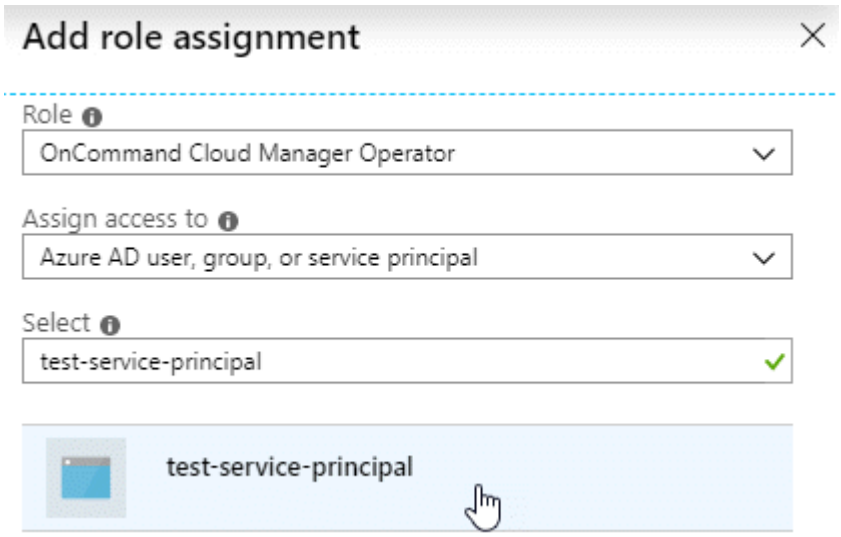
   c. Use the JSON file to create a custom role in Azure.

      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_3.7.4.json**

You should now have a custom role called *OnCommand 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 **OnCommand 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).




   g. Select the application and click **Save**.

      The service principal for Cloud Manager now has the required Azure permissions for that subscription.

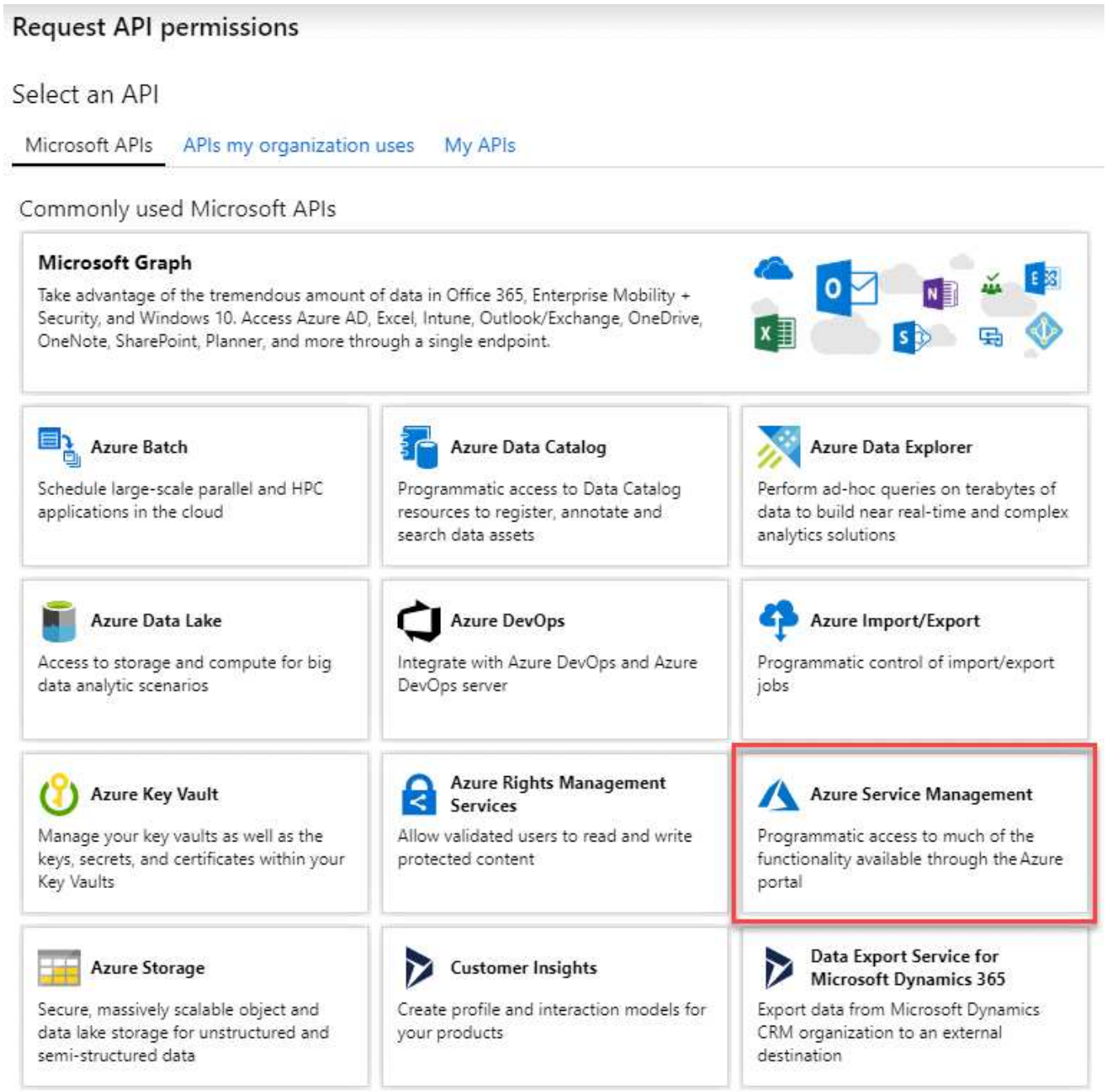
      If you want to deploy Cloud Volumes ONTAP from multiple Azure subscriptions, then you must bind the service principal to each of those subscriptions. Cloud Manager enables you to select the subscription that you want to use when deploying Cloud Volumes ONTAP.

#### Adding Windows Azure Service Management API permissions

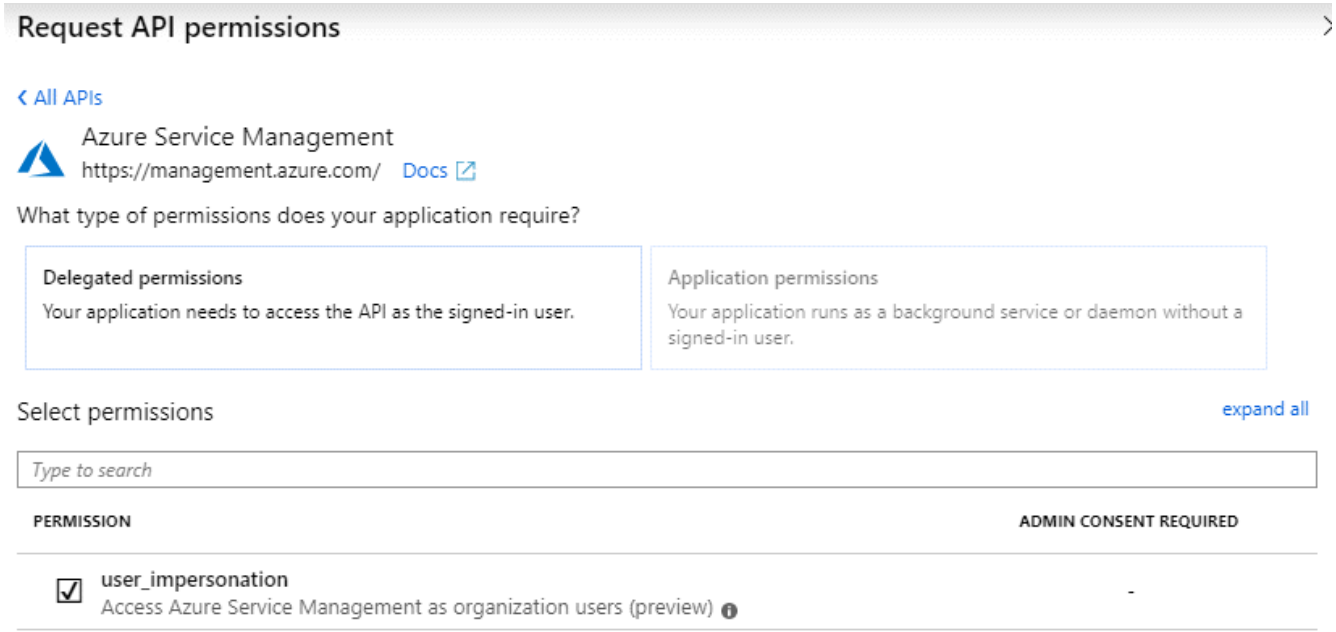
The service principal must have "Windows Azure Service Management API" permissions.

**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**.




4. Click **Access Azure Service Management as organization users** and then click **Add permissions**.

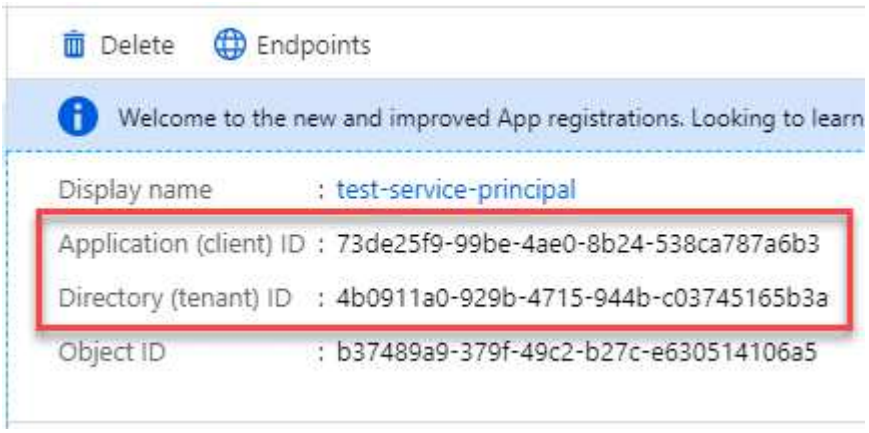



#### Getting the application ID and directory ID

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**.




#### 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.


**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 accounts to Cloud Manager

After you provide an Azure account with the required permissions, you can add the account to Cloud Manager. This enables you to launch Cloud Volumes ONTAP systems in that account.

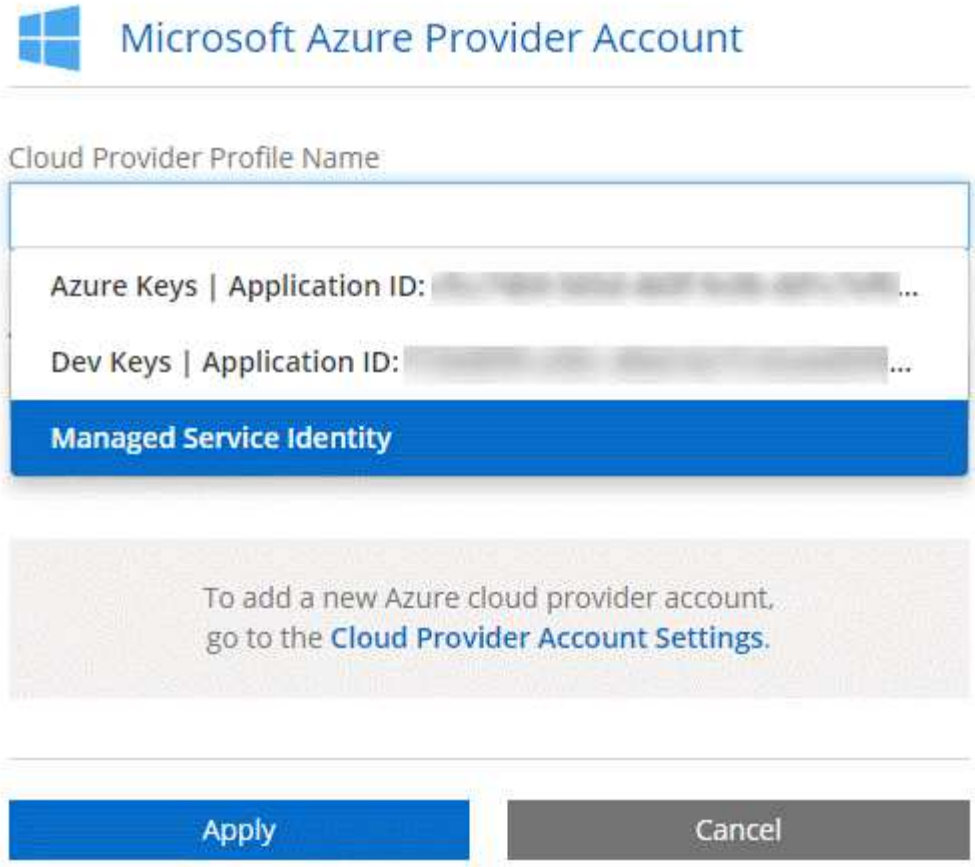
**Steps**

1. In the upper right of the Cloud Manager console, click the Settings icon, and select **Cloud Provider & Support Accounts**.


2. Click **Add New Account** and select **Microsoft Azure**.
3. Enter information about the Azure Active Directory service principal that grants the required permissions:
   - Application ID: See Getting the application ID and directory ID.
   - Tenant ID (or Directory ID): See Getting the application ID and directory ID.
   - Application Key (the client secret): See Creating a client secret.
4. Confirm that the policy requirements have been met and then click **Create Account**.

**Result**

You can now switch to another account from the Details and Credentials page when creating a new working environment:




### Associating additional Azure subscriptions with a managed identity

Cloud Manager enables you to choose the Azure account and 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 Cloud Manager from NetApp Cloud Central. When you deployed Cloud Manager, Cloud Central created the OnCommand Cloud Manager Operator role and assigned it to the Cloud Manager 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 systems.
3. Click **Access control (IAM)**.
   a. Click **Add** > **Add role assignment** and then add the permissions:
      - Select the **OnCommand Cloud Manager Operator** role.

        OnCommand 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.

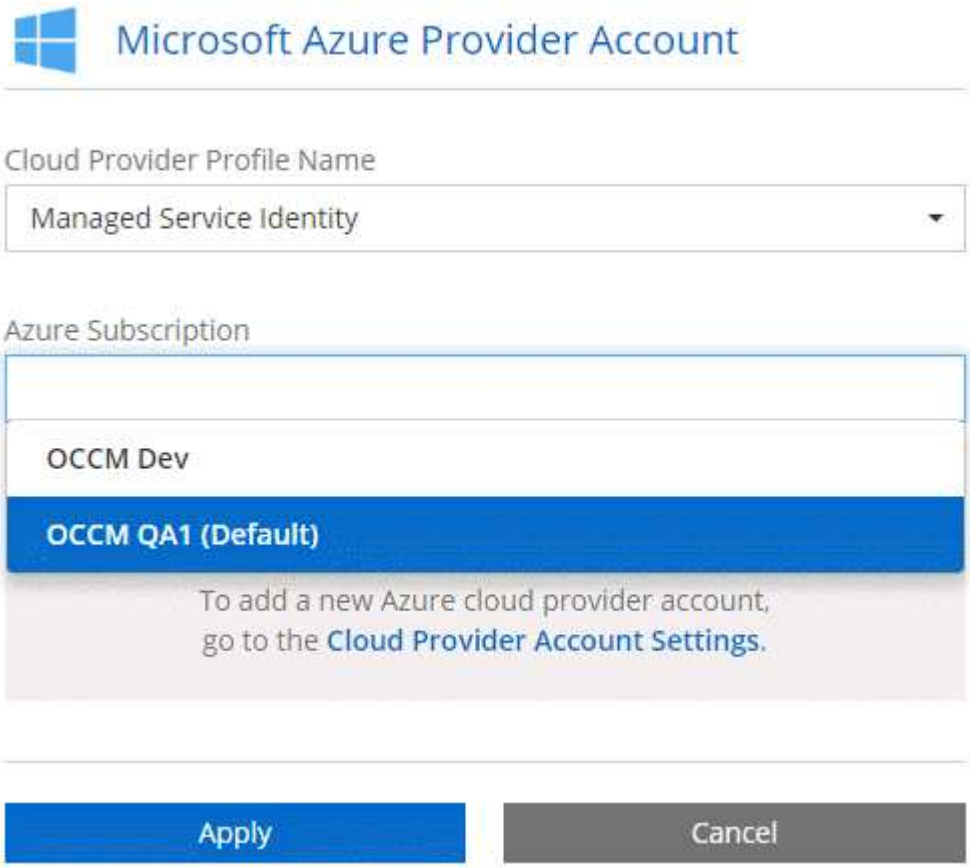
      - Assign access to a **Virtual Machine**.

- Select the subscription in which the Cloud Manager virtual machine was created.
- Select the Cloud Manager 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.




## Setting up and adding GCP accounts to Cloud Manager

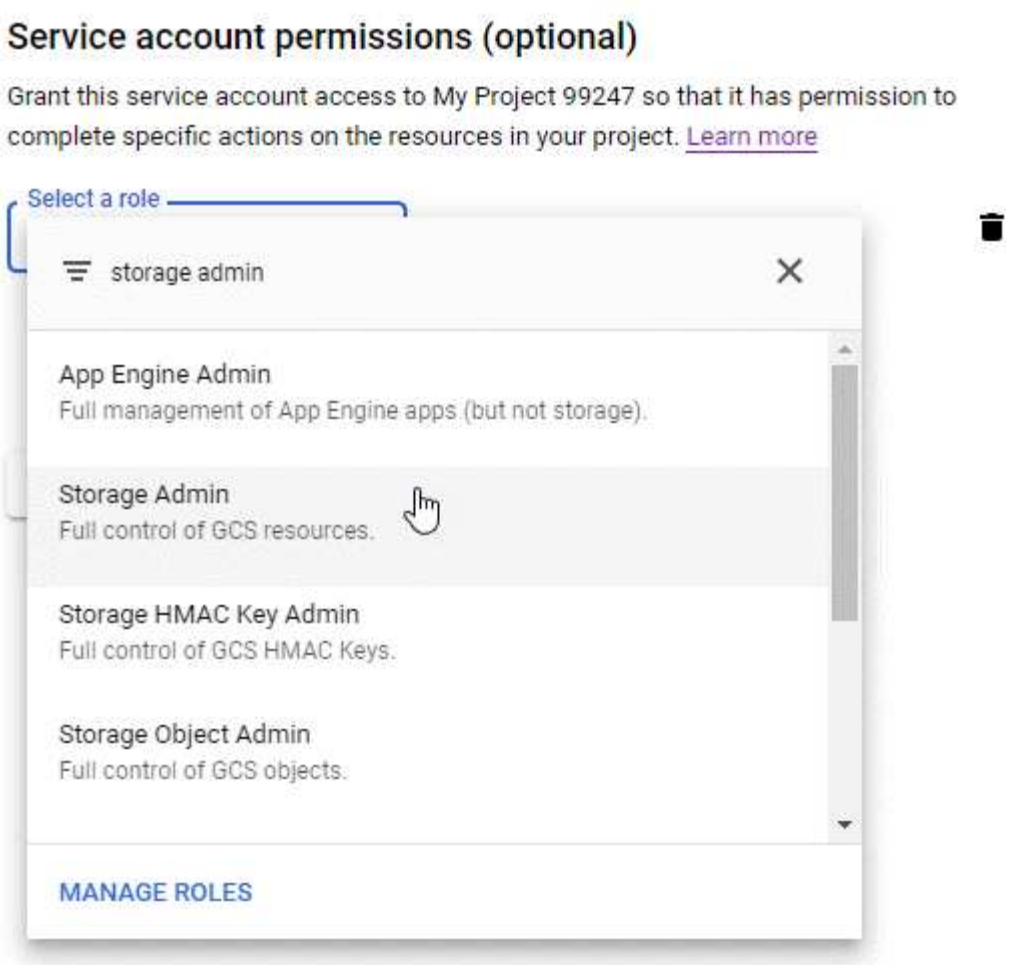
If you want to enable data tiering on a Cloud Volumes ONTAP system, you need to provide Cloud Manager with a storage access key for a service account that has Storage Admin permissions. Cloud Manager uses the access keys to set up and manage a Cloud Storage bucket for data tiering.

### Setting up a service account and access keys for Google Cloud Storage

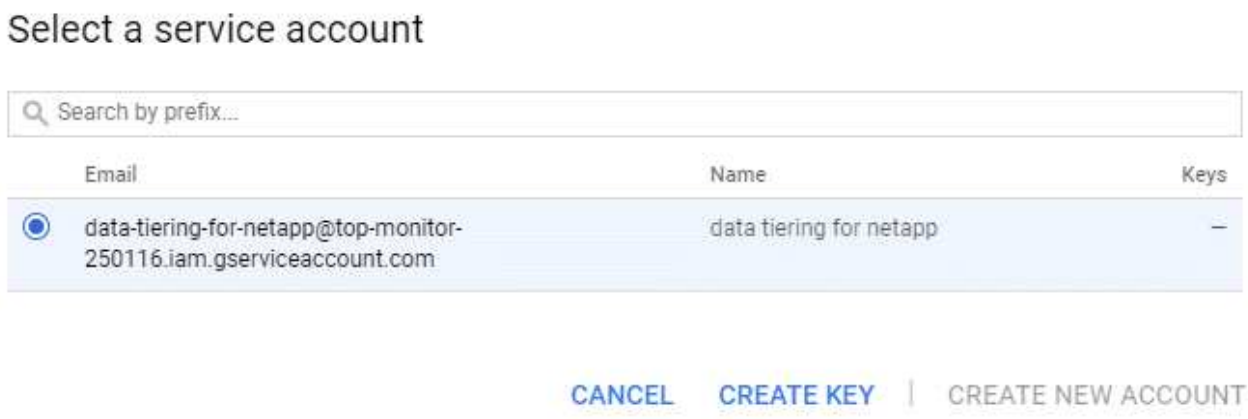
A service account enables Cloud Manager to authenticate and access Cloud Storage buckets used for data tiering. The keys are required so that Google Cloud Storage knows who is making the request.

**Steps**

1. Open the GCP IAM console and create a service account that has the Storage Admin role.




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.




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.

**Steps**

1. In the upper right of the Cloud Manager console, click the Settings icon, and select **Cloud Provider & Support Accounts**.


2. Click **Add New Account** and select **GCP**.
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 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.

[] | *https://img.youtube.com/vi/V2fLTyztqYQ/maxresdefault.jpg*

**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 **Cloud Provider & Support Accounts**.

3. Click **Add New Account** 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

## Installing 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.

**Steps**

1. In the upper right of the Cloud Manager console, click the Settings icon, and select **HTTPS Setup**.

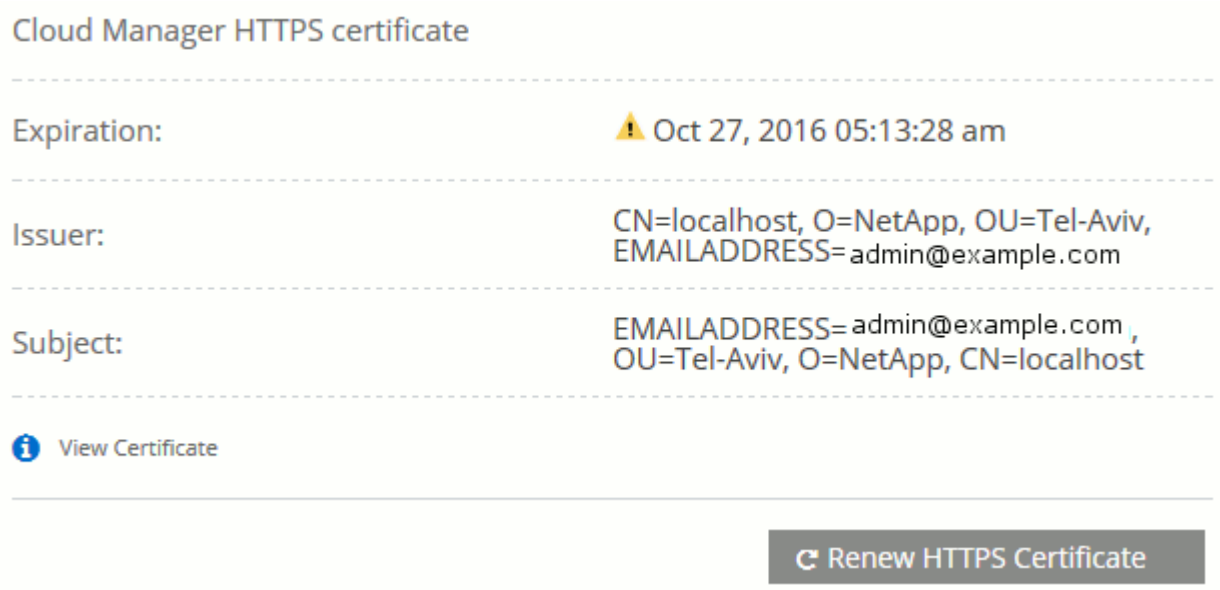

2. In the HTTPS Setup page, install a certificate by generating a certificate signing request (CSR) or by installing your own CA-signed certificate:

| Option | Description |
|---|---|
| Generate a CSR | a. Enter the host name or DNS of the Cloud Manager host (its Common Name), and then click **Generate CSR**.<br><br>Cloud Manager displays a certificate signing request.<br><br>b. Use the CSR to submit an SSL certificate request to a CA.<br><br>The certificate must use the Privacy Enhanced Mail (PEM) Base-64 encoded X.509 format.<br><br>c. Copy the contents of the signed certificate, paste it in the Certificate field, and then click **Install**. |

| Option | Description |
| --- | --- |
| Install your own CA-signed certificate | a. Select **Install CA-signed certificate**.<br>b. Load both the certificate file and the private key and then click **Install**.<br>The certificate must use the Privacy Enhanced Mail (PEM) Base-64 encoded X.509 format. |

**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:




## 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.

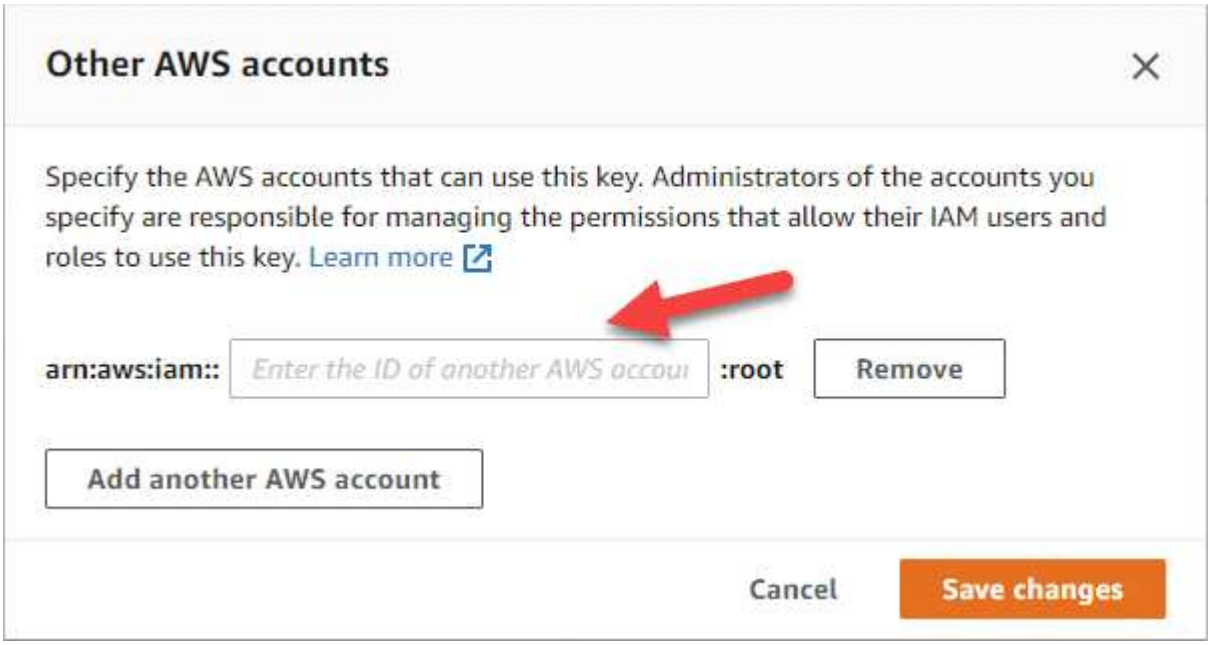
   AWS Documentation: Editing Keys

3. If the CMK is in a different AWS account, complete the following steps:
   a. Go to the KMS console from the account where the CMK resides.
   b. Select the key.
   c. In the **General configuration** pane, copy the ARN of the key.

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

   d. 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.


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

# Network requirements

## Networking requirements for Cloud Manager

Set up your networking so that Cloud Manager can deploy Cloud Volumes ONTAP systems in AWS, Microsoft Azure, or Google Cloud Platform. 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, Cloud Manager prompts you to specify the proxy during setup. You can also specify the proxy server from the Settings page. Refer to Configuring Cloud Manager to use a proxy server.

### Connection to target networks

Cloud Manager requires a network connection to the VPCs and VNets in which you want to deploy Cloud Volumes ONTAP.

For example, if you install Cloud Manager 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

Cloud Manager requires outbound internet access to deploy and manage Cloud Volumes ONTAP. Outbound internet access is also required when accessing Cloud Manager from your web browser and when running the Cloud Manager installer on a Linux host.

The following sections identify the specific endpoints.

#### Endpoints to manage Cloud Volumes ONTAP in AWS

Cloud Manager requires outbound internet access to contact the following endpoints when deploying and managing Cloud Volumes ONTAP in AWS:

| Endpoints | Purpose |
|---|---|
| AWS services (amazonaws.com):<br>• CloudFormation<br>• Elastic Compute Cloud (EC2)<br>• Key Management Service (KMS)<br>• Security Token Service (STS)<br>• Simple Storage Service (S3)<br>The exact endpoint depends on the region in which you deploy Cloud Volumes ONTAP. Refer to AWS documentation for details. | Enables Cloud Manager to deploy and manage Cloud Volumes ONTAP in AWS. |
| https://api.services.cloud.netapp.com:443 | API requests to NetApp Cloud Central. |
| https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com | Provides access to software images, manifests, and templates. |

| Endpoints | Purpose |
| --- | --- |
| https://cognito-idp.us-east-1.amazonaws.com<br>https://cognito-identity.us-east-1.amazonaws.com | Enables Cloud Manager to access and download manifests, templates, and Cloud Volumes ONTAP upgrade images. |
| https://kinesis.us-east-1.amazonaws.com | Enables NetApp to stream data from audit records. |
| https://cloudmanager.cloud.netapp.com | Communication with the Cloud Manager service, which includes Cloud Central accounts. |
| https://netapp-cloud-account.auth0.com | Communication with NetApp Cloud Central for centralized user authentication. |
| https://w86yt021u5.execute-api.us-east-1.amazonaws.com/production/whitelist | Used to add your AWS account ID to the list of allowed users for Backup to S3. |
| https://support.netapp.com/aods/asupmessage<br>https://support.netapp.com/asupprod/post/1.0/postAsup | Communication with NetApp AutoSupport. |
| https://support.netapp.com/svcgw<br>https://support.netapp.com/ServiceGW/entitlement | Communication with NetApp for system licensing and support registration. |
| https://ipa-signer.cloudmanager.netapp.com | Enables Cloud Manager to generate licenses (for example, a FlexCache license for Cloud Volumes ONTAP) |
| https://packages.cloud.google.com/yum<br>https://github.com/NetApp/trident/releases/download/ | Required to connect Cloud Volumes ONTAP systems with a Kubernetes cluster. The endpoints enable installation of NetApp Trident. |
| Various third-party locations, for example:<br>• https://repo1.maven.org/maven2<br>• https://oss.sonatype.org/content/repositories<br>• https://repo.typesafe.org<br>Third-party locations are subject to change. | During upgrades, Cloud Manager downloads the latest packages for third-party dependencies. |

#### Endpoints to manage Cloud Volumes ONTAP in Azure

Cloud Manager requires outbound internet access to contact the following endpoints when deploying and managing Cloud Volumes ONTAP in Microsoft Azure:

| Endpoints | Purpose |
| --- | --- |
| https://management.azure.com<br>https://login.microsoftonline.com | Enables Cloud Manager to deploy and manage Cloud Volumes ONTAP in most Azure regions. |
| https://management.microsoftazure.de<br>https://login.microsoftonline.de | Enables Cloud Manager to deploy and manage Cloud Volumes ONTAP in the Azure Germany regions. |

| Endpoints | Purpose |
| --- | --- |
| https://management.usgovcloudapi.net<br>https://login.microsoftonline.com | Enables Cloud Manager to deploy and manage Cloud Volumes ONTAP in the Azure US Gov regions. |
| https://api.services.cloud.netapp.com:443 | API requests to NetApp Cloud Central. |
| https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com | Provides access to software images, manifests, and templates. |
| https://cognito-idp.us-east-1.amazonaws.com<br>https://cognito-identity.us-east-1.amazonaws.com<br>https://sts.amazonaws.com | Enables Cloud Manager to access and download manifests, templates, and Cloud Volumes ONTAP upgrade images. |
| https://kinesis.us-east-1.amazonaws.com | Enables NetApp to stream data from audit records. |
| https://cloudmanager.cloud.netapp.com | Communication with the Cloud Manager service, which includes Cloud Central accounts. |
| https://netapp-cloud-account.auth0.com | Communication with NetApp Cloud Central for centralized user authentication. |
| https://mysupport.netapp.com | Communication with NetApp AutoSupport. |
| https://support.netapp.com/svcgw<br>https://support.netapp.com/ServiceGW/entitlement | Communication with NetApp for system licensing and support registration. |
| https://ipa-signer.cloudmanager.netapp.com | Enables Cloud Manager to generate licenses (for example, a FlexCache license for Cloud Volumes ONTAP) |
| https://packages.cloud.google.com/yum<br>https://github.com/NetApp/trident/releases/download/ | Required to connect Cloud Volumes ONTAP systems with a Kubernetes cluster. The endpoints enable installation of NetApp Trident. |
| Various third-party locations, for example:<br>• https://repo1.maven.org/maven2<br>• https://oss.sonatype.org/content/repositories<br>• https://repo.typesafe.org<br>Third-party locations are subject to change. | During upgrades, Cloud Manager downloads the latest packages for third-party dependencies. |

#### Endpoints to manage Cloud Volumes ONTAP in GCP

Cloud Manager requires outbound internet access to contact the following endpoints when deploying and managing Cloud Volumes ONTAP in GCP:

| Endpoints | Purpose |
| --- | --- |
| https://www.googleapis.com | Enables Cloud Manager to contact Google APIs for deploying and managing Cloud Volumes ONTAP in GCP. |
| https://api.services.cloud.netapp.com:443 | API requests to NetApp Cloud Central. |

| Endpoints | Purpose |
| --- | --- |
| https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com | Provides access to software images, manifests, and templates. |
| https://cognito-idp.us-east-1.amazonaws.com<br>https://cognito-identity.us-east-1.amazonaws.com<br>https://sts.amazonaws.com | Enables Cloud Manager to access and download manifests, templates, and Cloud Volumes ONTAP upgrade images. |
| https://kinesis.us-east-1.amazonaws.com | Enables NetApp to stream data from audit records. |
| https://cloudmanager.cloud.netapp.com | Communication with the Cloud Manager service, which includes Cloud Central accounts. |
| https://netapp-cloud-account.auth0.com | Communication with NetApp Cloud Central for centralized user authentication. |
| https://mysupport.netapp.com | Communication with NetApp AutoSupport. |
| https://support.netapp.com/svcgw<br>https://support.netapp.com/ServiceGW/entitlement | Communication with NetApp for system licensing and support registration. |
| https://ipa-signer.cloudmanager.netapp.com | Enables Cloud Manager to generate licenses (for example, a FlexCache license for Cloud Volumes ONTAP) |
| https://packages.cloud.google.com/yum<br>https://github.com/NetApp/trident/releases/download/ | Required to connect Cloud Volumes ONTAP systems with a Kubernetes cluster. The endpoints enable installation of NetApp Trident. |
| Various third-party locations, for example:<br>• https://repo1.maven.org/maven2<br>• https://oss.sonatype.org/content/repositories<br>• https://repo.typesafe.org<br>Third-party locations are subject to change. | During upgrades, Cloud Manager downloads the latest packages for third-party dependencies. |

#### 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 |
| --- | --- |
| The Cloud Manager host | You must enter the host's IP address from a web browser to load the Cloud Manager console.<br><br>Depending on your connectivity to your cloud provider, you can use the private IP or a public IP assigned to the host:<br><br>• A private IP works if you have a VPN and direct connect access to your virtual network<br>• A public IP works in any networking scenario<br><br>In any case, you should secure network access by ensuring that security group rules allow access from only authorized IPs or subnets. |
| https://auth0.com<br>https://cdn.auth0.com<br>https://netapp-cloud-account.auth0.com<br>https://services.cloud.netapp.com | Your web browser connects to these endpoints for centralized user authentication through NetApp Cloud Central. |
| https://widget.intercom.io | For in-product chat that enables you to talk to NetApp cloud experts. |

#### Endpoints to install Cloud Manager on a Linux host

The Cloud Manager installer 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

### Ports and security groups

- If you deploy Cloud Manager from Cloud Central or from the marketplace images, refer to the following:
  - Security group rules for Cloud Manager in AWS
  - Security group rules for Cloud Manager in Azure
  - Firewall rules for Cloud Manager in GCP
- If you install Cloud Manager on an existing Linux host, see Cloud Manager host requirements.

## Networking requirements for Cloud Volumes ONTAP in AWS

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

### General AWS networking 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.

**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.

## AWS networking requirements for Cloud Volumes ONTAP HA 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.

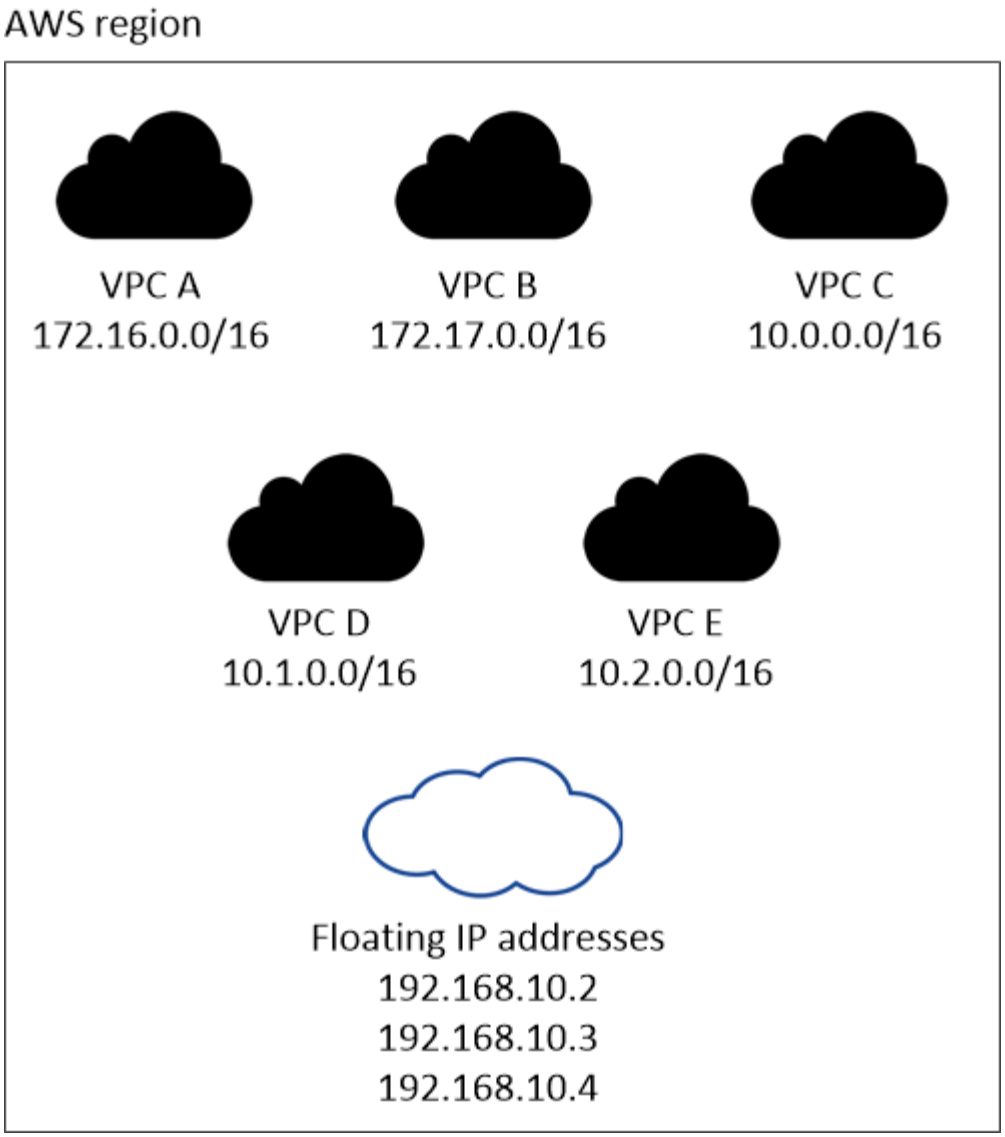
One floating IP address is for cluster management, one is for NFS/CIFS data on node 1, and one is for NFS/CIFS data on node 2. A fourth floating IP address for SVM management is optional.

> ⓘ 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.




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 configuration

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

## Sample VPC configurations

To better understand how you can deploy Cloud Manager and Cloud Volumes ONTAP in AWS, you should review the most common VPC configurations.

- A VPC with public and private subnets and a NAT device
- A VPC with a private subnet and a VPN connection to your network

#### A VPC with public and private subnets and a NAT device

This VPC configuration includes public and private subnets, an internet gateway that connects the VPC to the internet, and a NAT gateway or NAT instance in the public subnet that enables outbound internet traffic from the private subnet. In this configuration, you can run Cloud Manager in a public subnet or private subnet, but the public subnet is recommended because it allows access from hosts outside the VPC. You can then launch Cloud Volumes ONTAP instances in the private subnet.

Instead of a NAT device, you can use an HTTP proxy to provide internet connectivity.

For more details about this scenario, refer to AWS Documentation: Scenario 2: VPC with Public and Private Subnets (NAT).

The following graphic shows Cloud Manager running in a public subnet and single node systems running in a private subnet:

#### A VPC with a private subnet and a VPN connection to your network

This VPC configuration is a hybrid cloud configuration in which Cloud Volumes ONTAP becomes an extension of your private environment. The configuration includes a private subnet and a virtual private gateway with a VPN connection to your network. Routing across the VPN tunnel allows EC2 instances to access the internet through your network and firewalls. You can run Cloud Manager in the private subnet or in your data center. You would then launch Cloud Volumes ONTAP in the private subnet.

You can also use a proxy server in this configuration to allow internet access. The proxy server can be in your data center or in AWS.

If you want to replicate data between FAS systems in your data center and Cloud Volumes ONTAP systems in AWS, you should use a VPN connection so that the link is secure.

For more details about this scenario, refer to AWS Documentation: Scenario 4: VPC with a Private Subnet Only and AWS Managed VPN Access.

The following graphic shows Cloud Manager running in your data center and single node systems running in a private subnet:

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

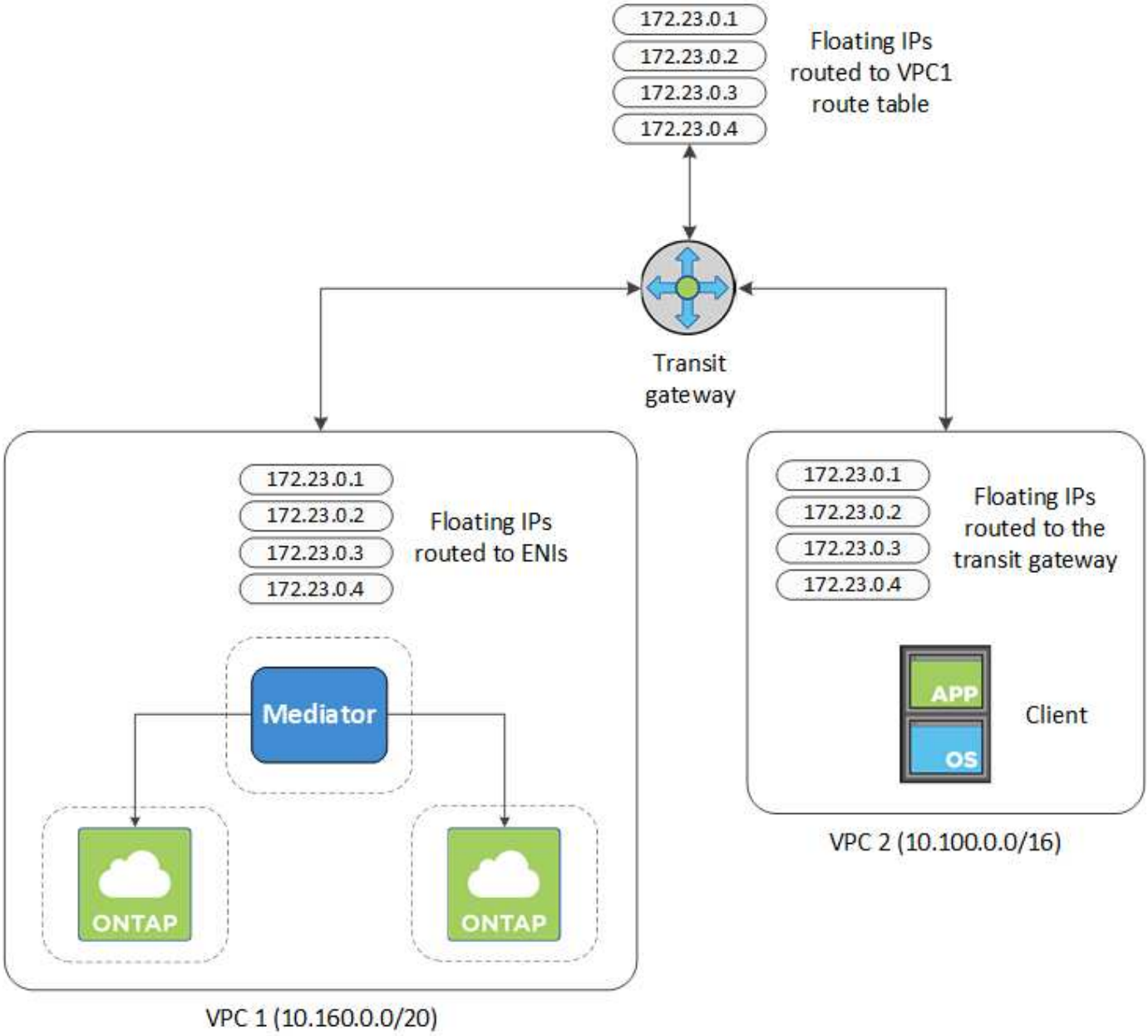
Set up an AWS transit gateway to enable access to an HA pair's floating IP addresses from outside the VPC where the HA pair resides.

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.

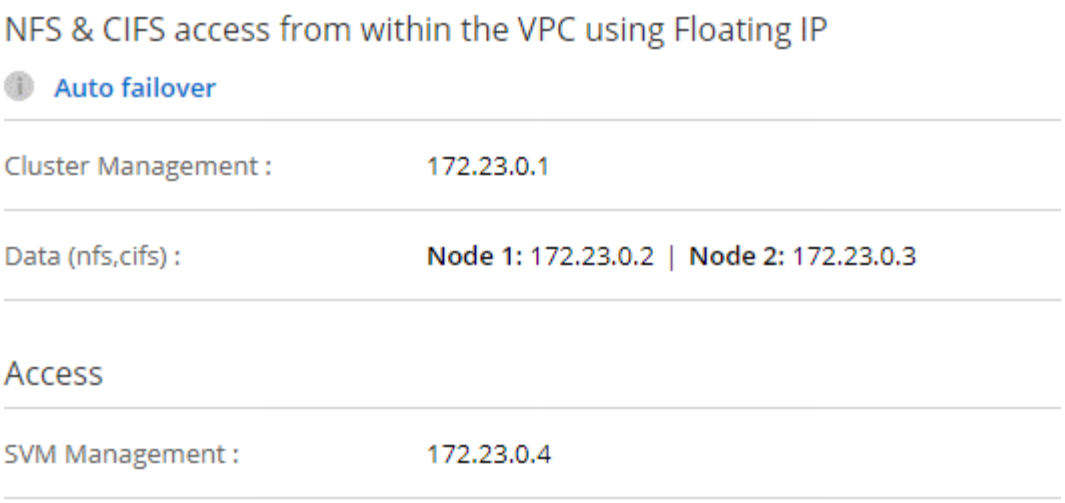



The following steps illustrate how to set up a similar configuration.

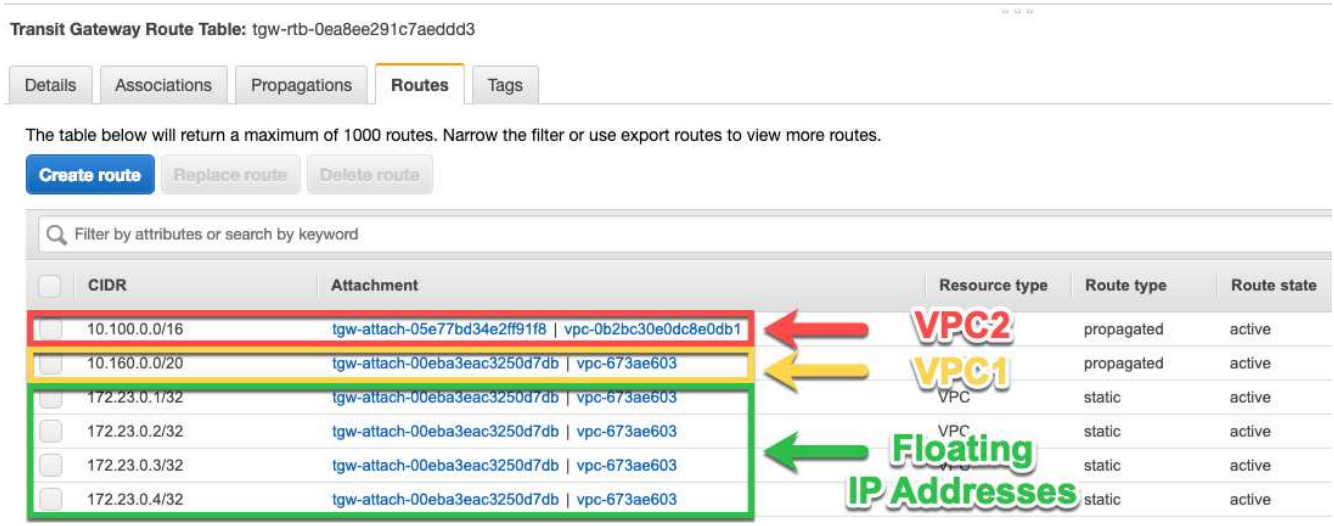
**Steps**

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:

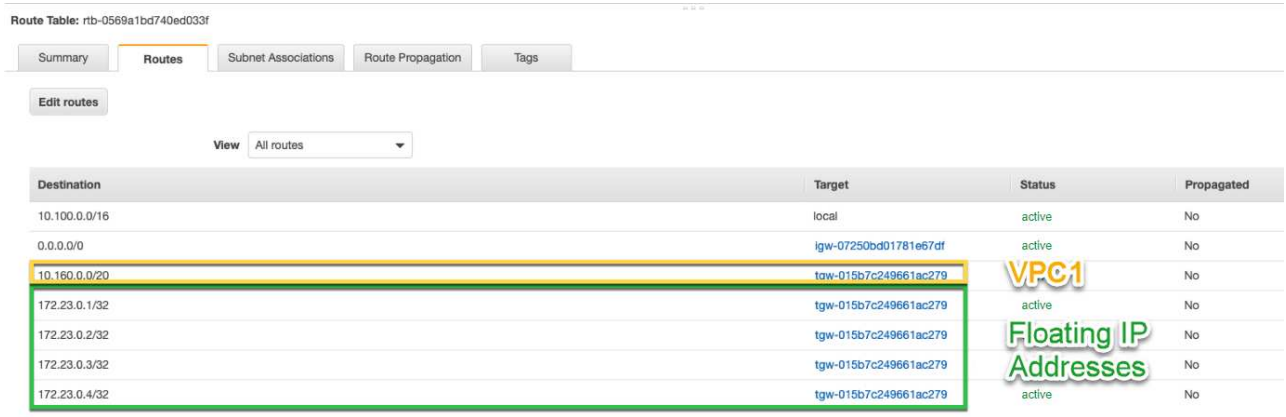



The following sample image shows the route table for the transit gateway. It includes routes to the CIDR blocks of the two VPCs and four floating IP addresses used by Cloud Volumes ONTAP.




3. Modify the route table of VPCs that need to access the floating IP addresses.
   a. Add route entries to the floating IP addresses.
   b. Add a route entry to the CIDR block of the VPC where the HA pair resides.

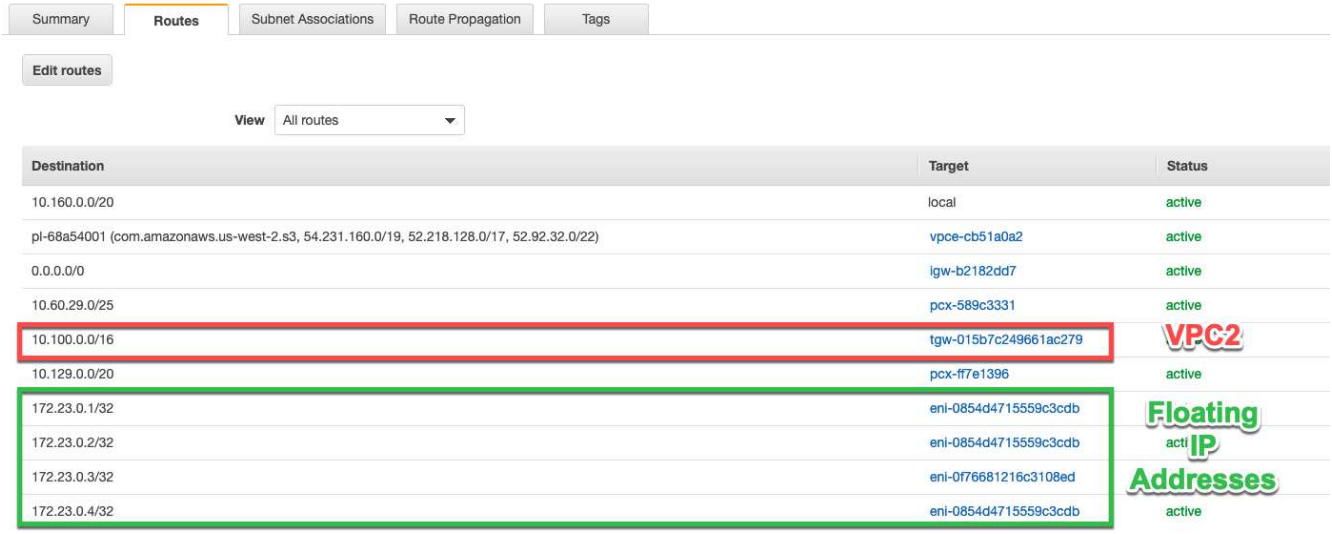
      The following sample image shows the route table for VPC 2, which includes routes to VPC 1 and the floating IP addresses.




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.

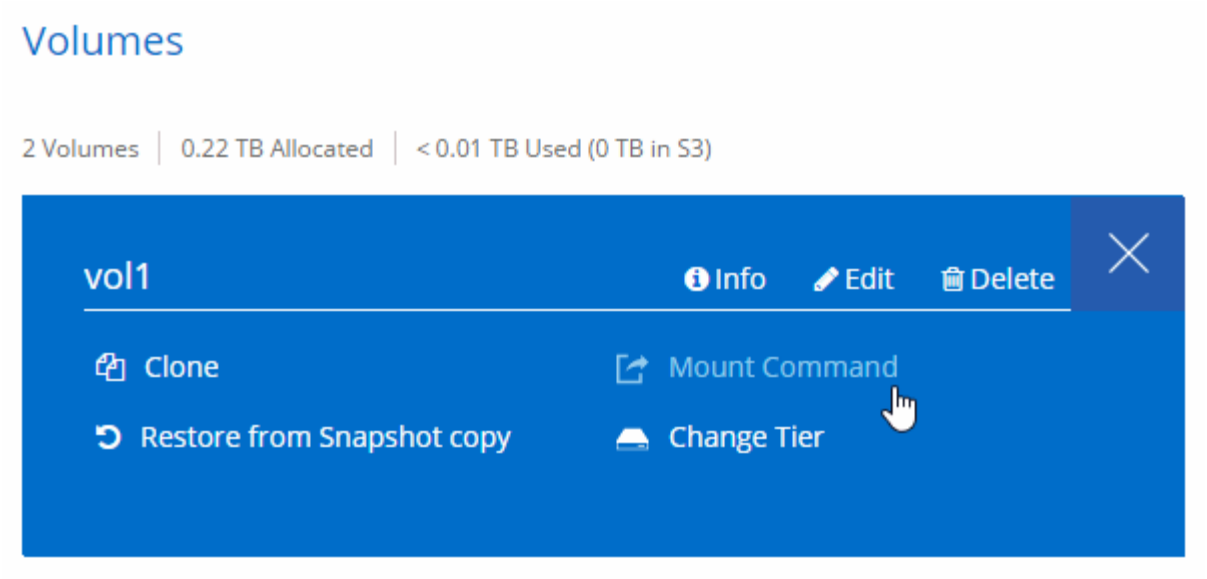
   This step is important because it completes the routing between the VPCs.

   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.




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**.




**Related links**

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

## Networking requirements for Cloud Volumes ONTAP in Azure

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

### 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

### 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.

### 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.

## Networking requirements for Cloud Volumes ONTAP in GCP

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

**Shared VPC**

Cloud Manager and Cloud Volumes ONTAP are supported in a Google Cloud Platform shared VPC.

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 Cloud Manager and Cloud Volumes ONTAP virtual machine instances in a *service project*. Google Cloud documentation: Shared VPC overview.

The only requirement is to provide the following permissions to the Cloud Manager service account in the shared VPC host project:

compute.firewalls.*
compute.networks.*
compute.subnetworks.*

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

**Number of IP addresses**

Cloud Manager allocates 5 IP addresses to Cloud Volumes ONTAP in GCP.

Note that Cloud Manager doesn't create an SVM management LIF for Cloud Volumes ONTAP in GCP.

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

**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 GCP firewall rules.

**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. 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.

# Additional deployment options

## Cloud Manager host requirements

If you install Cloud Manager on your own host, then you must verify support for your configuration, which includes operating system requirements, port requirements, and so on.

You can install Cloud Manager on your own host in GCP, but not in your on-premises network. Cloud Manager must be installed in GCP in order to deploy Cloud Volumes ONTAP in GCP.

**A dedicated host is required**

Cloud Manager is not supported on a host that is shared with other applications. The host must be a dedicated host.

**Supported AWS EC2 instance types**

- t2.medium
- t3.medium (recommended)
- m4.large

- m5.xlarge
- m5.2xlarge
- m5.4xlarge
- m5.8xlarge

**Supported Azure VM sizes**

A2, D2 v2, or D2 v3 (based on availability)

**Supported GCP machine types**

A machine type with at least 2 vCPUs and 4 GB of memory.

**Supported operating systems**

- CentOS 7.2
- CentOS 7.3
- CentOS 7.4
- CentOS 7.5
- Red Hat Enterprise Linux 7.2
- Red Hat Enterprise Linux 7.3
- Red Hat Enterprise Linux 7.4
- Red Hat Enterprise Linux 7.5

  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 Cloud Manager installation.

  Cloud Manager 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?

**CPU**

2.27 GHz or higher with two cores

**RAM**

4 GB

**Free disk space**

50 GB

**Outbound internet access**

Outbound internet access is required when installing Cloud Manager and when using Cloud Manager to deploy Cloud Volumes ONTAP. For a list of endpoints, see Networking requirements for Cloud Manager.

**Ports**

The following ports must be available:

- 80 for HTTP access

- 443 for HTTPS access
- 3306 for the Cloud Manager database
- 8080 for the Cloud Manager API proxy

  If other services are using these ports, Cloud Manager installation fails.

  > There is a potential conflict with port 3306. If another instance of MySQL is running on the host, it uses port 3306 by default. You must change the port that the existing MySQL instance uses.

  You can change the default HTTP and HTTPS ports when you install Cloud Manager. You cannot change the default port for the MySQL database. If you change the HTTP and HTTPS ports, you must ensure that users can access the Cloud Manager web console from a remote host:

  - Modify the security group to allow inbound connections through the ports.
  - Specify the port when you enter the URL to the Cloud Manager web console.

## Installing Cloud Manager on an existing Linux host

The most common way to deploy Cloud Manager is from Cloud Central or from a cloud provider's marketplace. But you have the option to download and install the Cloud Manager software on an existing Linux host in your network or in the cloud.

> You can install Cloud Manager on your own host in GCP, but not in your on-premises network. Cloud Manager must be installed in GCP in order to deploy Cloud Volumes ONTAP in GCP.

**Before you begin**

- 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 Cloud Manager installation.
- The Cloud Manager installer accesses several URLs during the installation process. You must ensure that outbound internet access is allowed to those endpoints. Refer to Networking requirements for Cloud Manager.

**About this task**

- Root privileges are not required to install Cloud Manager.
- Cloud Manager 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. Cloud Manager can operate successfully without the tools.

- The installer that is available on the NetApp Support Site might be an earlier version. After installation, Cloud Manager automatically updates itself if a new version is available.

**Steps**

1. Review networking requirements:
   - Networking requirements for Cloud Manager
   - Networking requirements for Cloud Volumes ONTAP in AWS

- Networking requirements for Cloud Volumes ONTAP in Azure
- Networking requirements for Cloud Volumes ONTAP in GCP

2. Review Cloud Manager host requirements.
3. Download the 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.

4. Assign permissions to execute the script.

   **Example**

   ```
   chmod +x OnCommandCloudManager-V3.7.0.sh
   ```

5. Run the installation script:

   ```
   ./OnCommandCloudManager-V3.7.0.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 Cloud Manager 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.

6. Unless you specified the silent parameter, type **Y** to continue the script, and then enter the HTTP and HTTPS ports when prompted.

   If you change the HTTP and HTTPS ports, you must ensure that users can access the Cloud Manager web console from a remote host:

   - Modify the security group to allow inbound connections through the ports.
   - Specify the port when you enter the URL to the Cloud Manager web console.

     Cloud Manager is now installed. At the end of the installation, the Cloud Manager service (occm) restarts twice if you specified a proxy server.

7. 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 Cloud Manager host. For example, if Cloud Manager 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 Cloud Manager host.

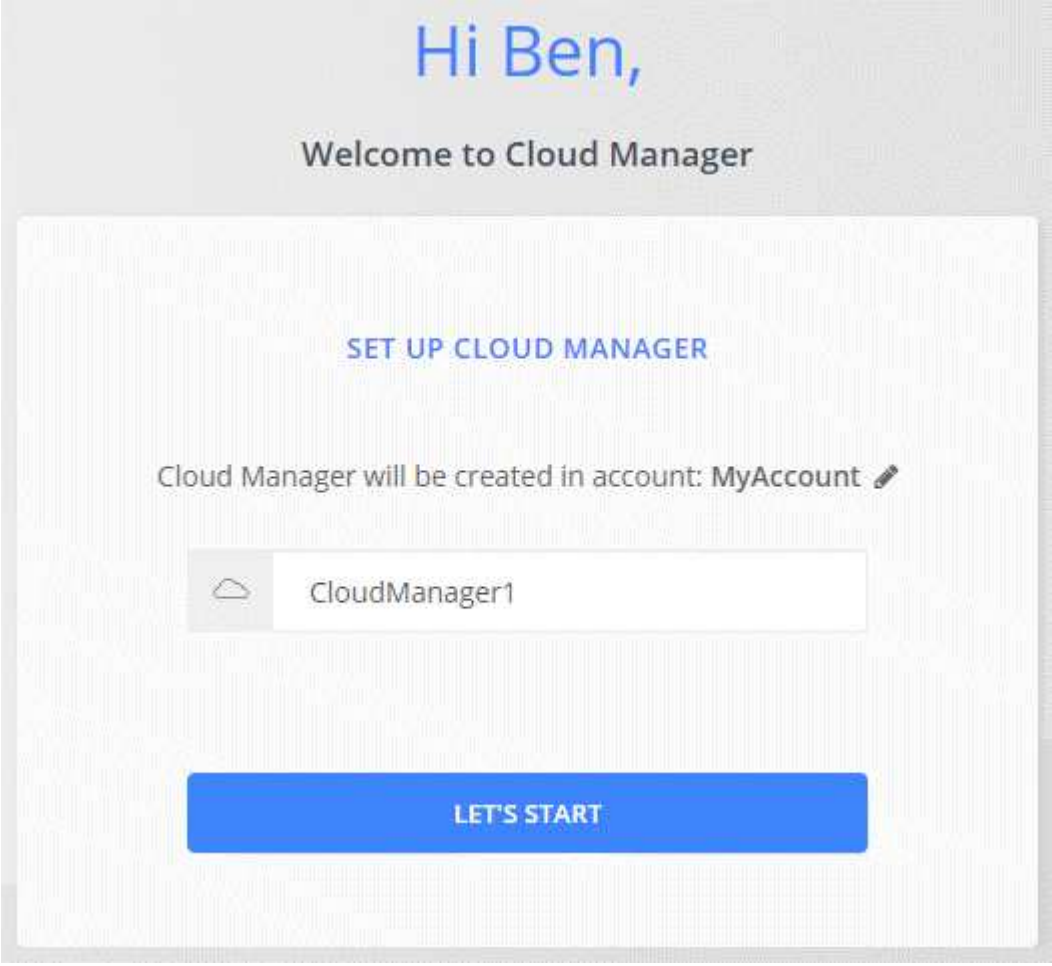
   *port* is required if you changed the default HTTP (80) or HTTPS (443) ports. For example, if the HTTPS

port was changed to 8443, you would enter https://*ipaddress*:8443

8. Sign up at NetApp Cloud Central or log in.
9. After you log in, set up Cloud Manager:
   a. Specify the Cloud Central account to associate with this Cloud Manager system.

      Learn about Cloud Central accounts.

   b. Enter a name for the system.




**After you finish**

Set up permissions so Cloud Manager can deploy Cloud Volumes ONTAP in your cloud provider:

- 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 Cloud Manager 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.

## Launching Cloud Manager from the AWS Marketplace

It's best to launch Cloud Manager in AWS using NetApp Cloud Central, but you can launch it from the AWS Marketplace, if needed.

If you launch Cloud Manager from the AWS Marketplace, Cloud Manager is still integrated with NetApp Cloud Central. Learn more about the integration.

### About this task

The following 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 is not possible using the **Launch from Website** action.

### Steps

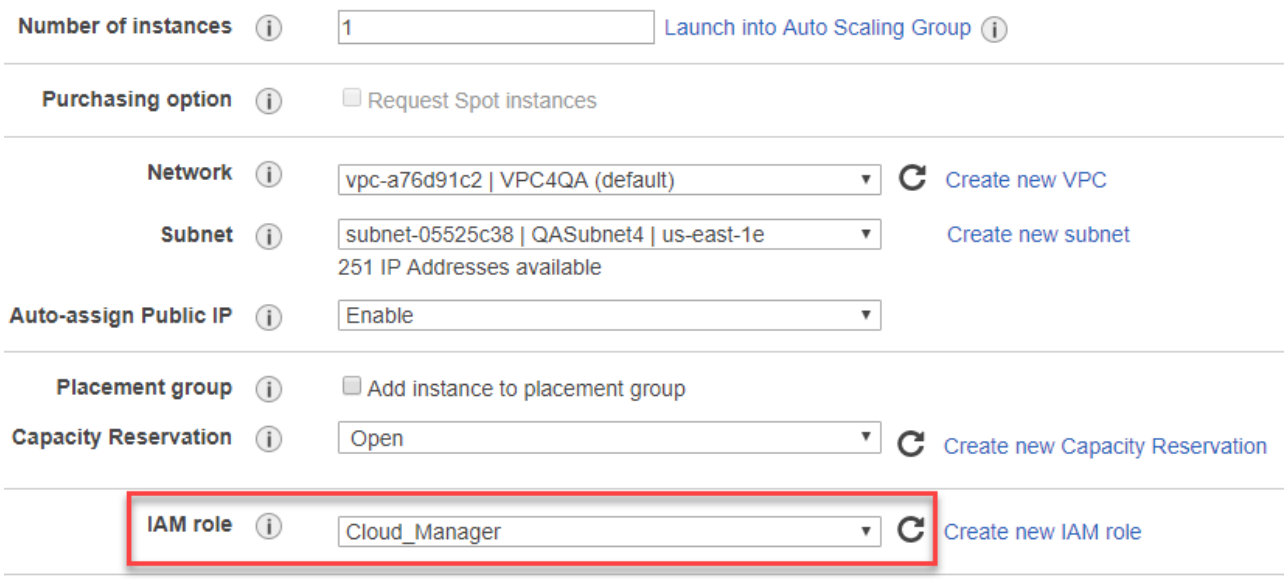
1. Create an IAM policy and role for the EC2 instance:
   a. Download the Cloud Manager IAM policy from the following location:

      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. Subscribe from the AWS Marketplace to ensure that there's no disruption of service after your free trial of Cloud Volumes ONTAP ends. 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.
3. Now go to the Cloud Manager page on the AWS Marketplace to deploy Cloud Manager from an AMI.
4. On the Marketplace page, click **Continue to Subscribe** and then click **Continue to Configuration**.
5. Change any of the default options and click **Continue to Launch**.
6. Under **Choose Action**, select **Launch through EC2** and then click **Launch**.
7. Follow the prompts to configure and deploy the instance:
   - **Choose Instance Type**: Depending on region availability, choose one of the supported instance types (t3.medium is recommended).

     Review the list of supported instance types.

   - **Configure Instance**: Select a VPC and subnet, the IAM role that you created in step 1, and other configuration options that meet your requirements.




- **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 Cloud Manager instance: SSH, HTTP, and HTTPS.
- **Review**: Review your selections and click **Launch**.

  AWS launches the software with the specified settings. The Cloud Manager instance and software should be running in approximately five minutes.

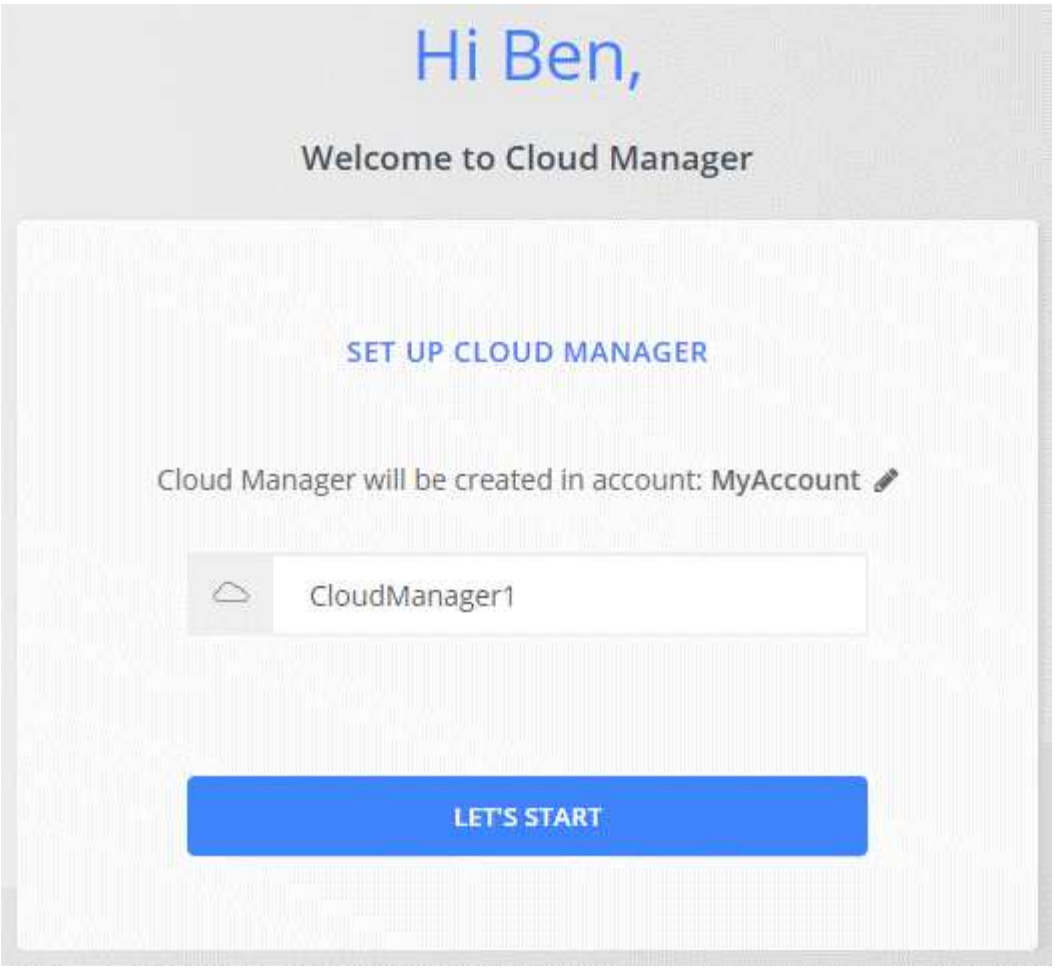
8. Open a web browser from a host that has a connection to the Cloud Manager virtual machine and enter the following URL:

   http://*ipaddress*:80

9. After you log in, set up Cloud Manager:
   a. Specify the Cloud Central account to associate with this Cloud Manager system.

      Learn about Cloud Central accounts.

   b. Enter a name for the system.




**Result**

Cloud Manager is now installed and set up.

## Deploying Cloud Manager from the Azure Marketplace

It is best to deploy Cloud Manager in Azure using NetApp Cloud Central, but you can deploy it from the Azure Marketplace, if needed.

Separate instructions are available to deploy Cloud Manager in Azure US Government regions and in Azure Germany regions.

If you deploy Cloud Manager from the Azure Marketplace, Cloud Manager is still integrated with NetApp Cloud Central. Learn more about the integration.

### Deploying Cloud Manager in Azure

You need to install and set up Cloud Manager so you can use it to launch Cloud Volumes ONTAP in Azure.

**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 one of the recommended virtual machine sizes: A2, D2 v2, or D2 v3 (based on availability).
- For the network security group, Cloud Manager requires inbound connections using SSH, HTTP, and HTTPS.

  Learn more about security group rules for Cloud Manager.

- Under **Management**, enable **System assigned managed identity** for Cloud Manager by selecting **On**.

  This setting is important because a managed identity allows the Cloud Manager 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 Cloud Manager software should be running in approximately five minutes.

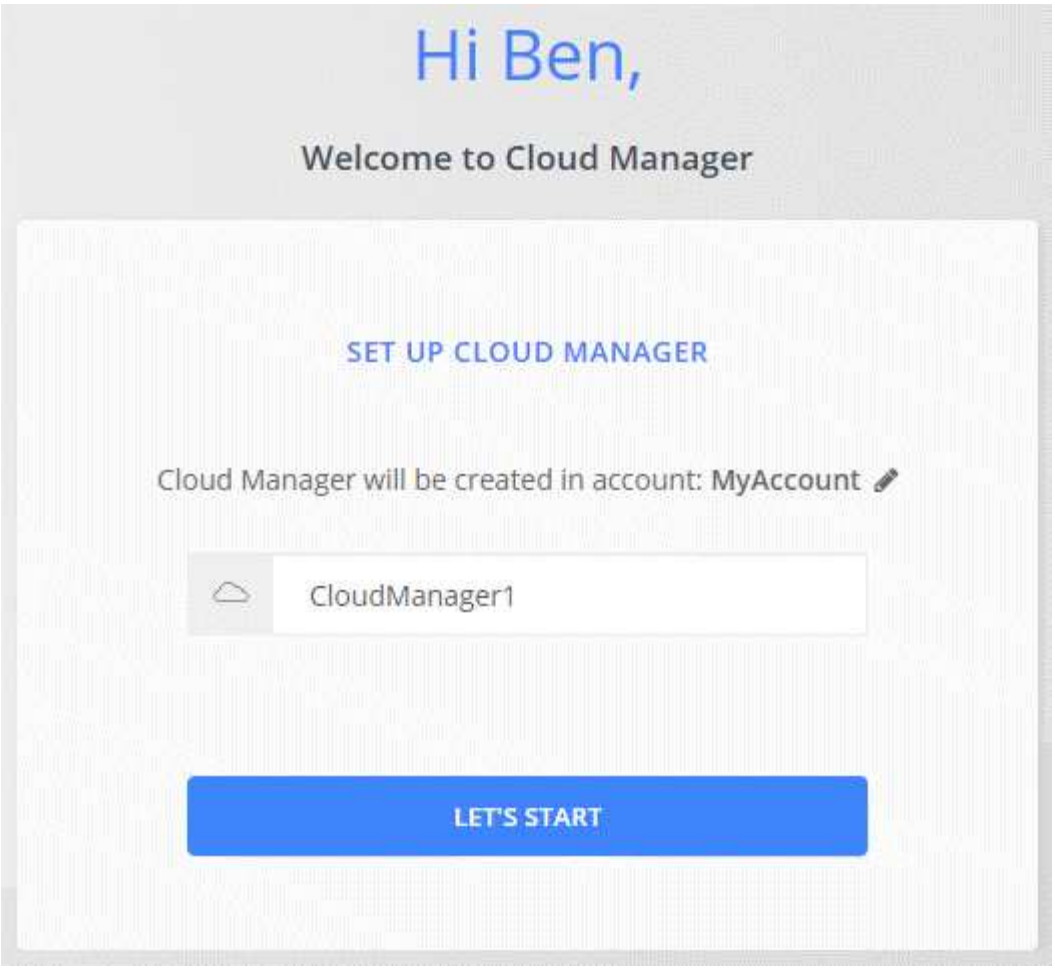
5. Open a web browser from a host that has a connection to the Cloud Manager virtual machine and enter the following URL:

   http://*ipaddress*:80

6. After you log in, set up Cloud Manager:
   a. Specify the Cloud Central account to associate with this Cloud Manager system.

      Learn about Cloud Central accounts.

   b. Enter a name for the system.




**Result**

Cloud Manager is now installed and set up. You must grant Azure permissions before users can deploy Cloud Volumes ONTAP in Azure.

### Granting Azure permissions to Cloud Manager

When you deployed Cloud Manager 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 Cloud Manager 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-c25fbzzzzzzz",
      "/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",
      "/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"

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_3.7.4.json**

   You should now have a custom role called OnCommand Cloud Manager Operator that you can assign to the Cloud Manager virtual machine.

2. Assign the role to the Cloud Manager 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 **OnCommand Cloud Manager Operator** role.

        OnCommand 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 Cloud Manager virtual machine was created.
      - Select the Cloud Manager 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**

Cloud Manager now has the permissions that it needs to deploy and manage Cloud Volumes ONTAP in Azure.

## Deploying Cloud Manager in an Azure US Government region

To get Cloud Manager up and running in a US Government region, first deploy Cloud Manager from the Azure Government Marketplace. Then provide the permissions that Cloud Manager needs to deploy and manage Cloud Volumes ONTAP systems.

For a list of supported Azure US Government regions, see Cloud Volumes Global Regions.

### Deploying Cloud Manager from the Azure US Government Marketplace

Cloud Manager is available as an image in the Azure US Government Marketplace.

**Steps**

1. Ensure that the Azure Government Marketplace is enabled in your subscription:
   a. Log into the portal as an Enterprise Administrator.
   b. Navigate to **Manage**.
   c. Under **Enrollment Details**, click the pencil icon next to **Azure Marketplace**.

d. Select **Enabled**.

e. Click **Save**.

Microsoft Azure Documentation: Azure Government Marketplace

2. Search for OnCommand Cloud Manager in the Azure US Government portal.
3. Click **Create** and follow the steps to configure the virtual machine.

   Note the following as you configure the virtual machine:

   - Cloud Manager can perform optimally with either HDD or SSD disks.
   - You should choose one of the recommended virtual machine sizes: A2, D2 v2, or D2 v3 (based on availability).
   - For the network security group, it is best to choose **Advanced**.

     The **Advanced** option creates a new security group that includes the required inbound rules for Cloud Manager. If you choose Basic, refer to Security group rules for the list of required rules.

4. On the summary page, review your selections and click **Create** to start the deployment.

   Azure deploys the virtual machine with the specified settings. The virtual machine and Cloud Manager software should be running in approximately five minutes.

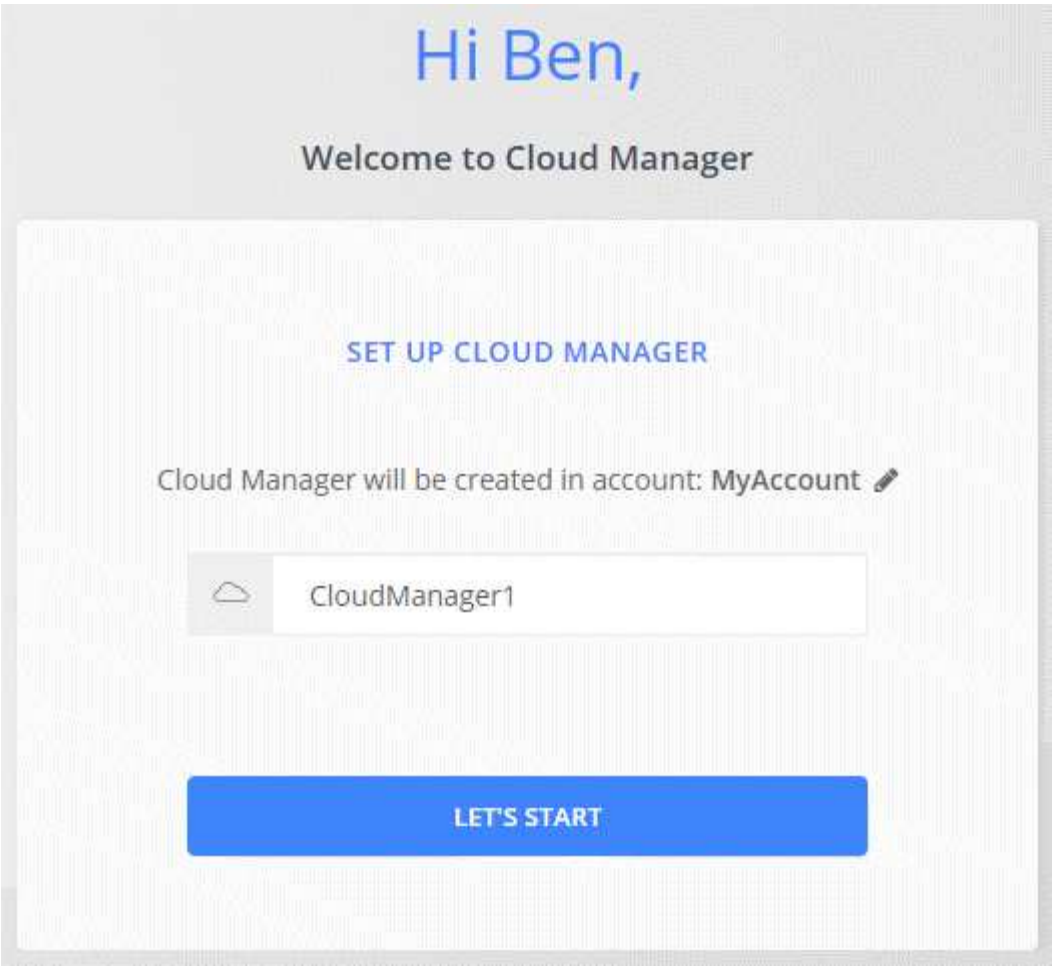
5. Open a web browser from a host that has a connection to the Cloud Manager virtual machine and enter the following URL:

   http://*ipaddress*:80

6. After you log in, set up Cloud Manager:
   a. Specify the Cloud Central account to associate with this Cloud Manager system.

      Learn about Cloud Central accounts.

   b. Enter a name for the system.




**Result**

Cloud Manager is now installed and set up. You must grant Azure permissions before users can deploy Cloud Volumes ONTAP in Azure.

### Granting Azure permissions to Cloud Manager using a managed identity

The easiest way to provide permissions is by enabling a managed identity on the Cloud Manager virtual machine and then by assigning the required permissions to the virtual machine. If preferred, an alternative way is to grant Azure permissions using a service principal.

**Steps**

1. Enable a managed identity on the Cloud Manager virtual machine:
   a. Navigate to the Cloud Manager virtual machine and select **Identity**.
   b. Under **System Assigned**, click **On** and then click **Save**.
2. 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-c25fbzzzzzzz",
"/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",
"/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"

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_3.7.4.json**

You should now have a custom role called OnCommand Cloud Manager Operator that you can assign to the Cloud Manager virtual machine.

3. Assign the role to the Cloud Manager 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**, click **Add role assignment**, and then add the permissions:
      - Select the **OnCommand Cloud Manager Operator** role.

        OnCommand 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 Cloud Manager virtual machine was created.
      - Type the name of the virtual machine and then select it.
      - Click **Save**.
   d. If you want to deploy Cloud Volumes ONTAP from additional subscriptions, switch to that subscription and then repeat these steps.

**Result**

Cloud Manager now has the permissions that it needs to deploy and manage Cloud Volumes ONTAP in Azure.

## Installing Cloud Manager in an Azure Germany region

The Azure Marketplace is not available in the Azure Germany regions, so you must download the Cloud Manager installer from the NetApp Support Site and install it on an existing Linux host in the region.

**Steps**

1. Review networking requirements for Azure.
2. Review Cloud Manager host requirements.
3. Download and install Cloud Manager.
4. Grant Azure permissions to Cloud Manager using a service principal.

**After you finish**

Cloud Manager is now ready to deploy Cloud Volumes ONTAP in the Azure Germany region, just like any other region. However, you might want to perform additional setup first.

# Keeping Cloud Manager up and running

## Cloud Manager should remain running at all times.

Cloud Manager is a key component in the health and billing of Cloud Volumes ONTAP. If Cloud Manager is powered down, Cloud Volumes ONTAP systems will shut down after losing communication with Cloud Manager for longer than 4 days.

# Deploy Cloud Volumes ONTAP

## Before you create Cloud Volumes ONTAP systems

Before you use Cloud Manager to create and manage Cloud Volumes ONTAP systems, your Cloud Manager administrator should have prepared networking and installed and set up Cloud Manager.

The following conditions should exist before you start deploying Cloud Volumes ONTAP:

- Networking requirements were met for Cloud Manager and Cloud Volumes ONTAP.
- Cloud Manager has permissions to perform operations in your chosen cloud provider.
- For AWS, you subscribed to the appropriate AWS Marketplace page:
  - If you want to deploy a PAYGO system, or enable an add-on feature: The Cloud Manager (for Cloud Volumes ONTAP) page.
  - If you want to deploy a BYOL system: The single node or HA page in the AWS Marketplace.
- Cloud Manager was installed.

**Related links**

- Getting started in AWS
- Getting started in Azure
- Getting started in GCP
- Setting up Cloud Manager

## Logging in to Cloud Manager

You can log in to Cloud Manager from any web browser that has a connection to the Cloud Manager system. You should log in using a NetApp Cloud Central user account.

**Steps**

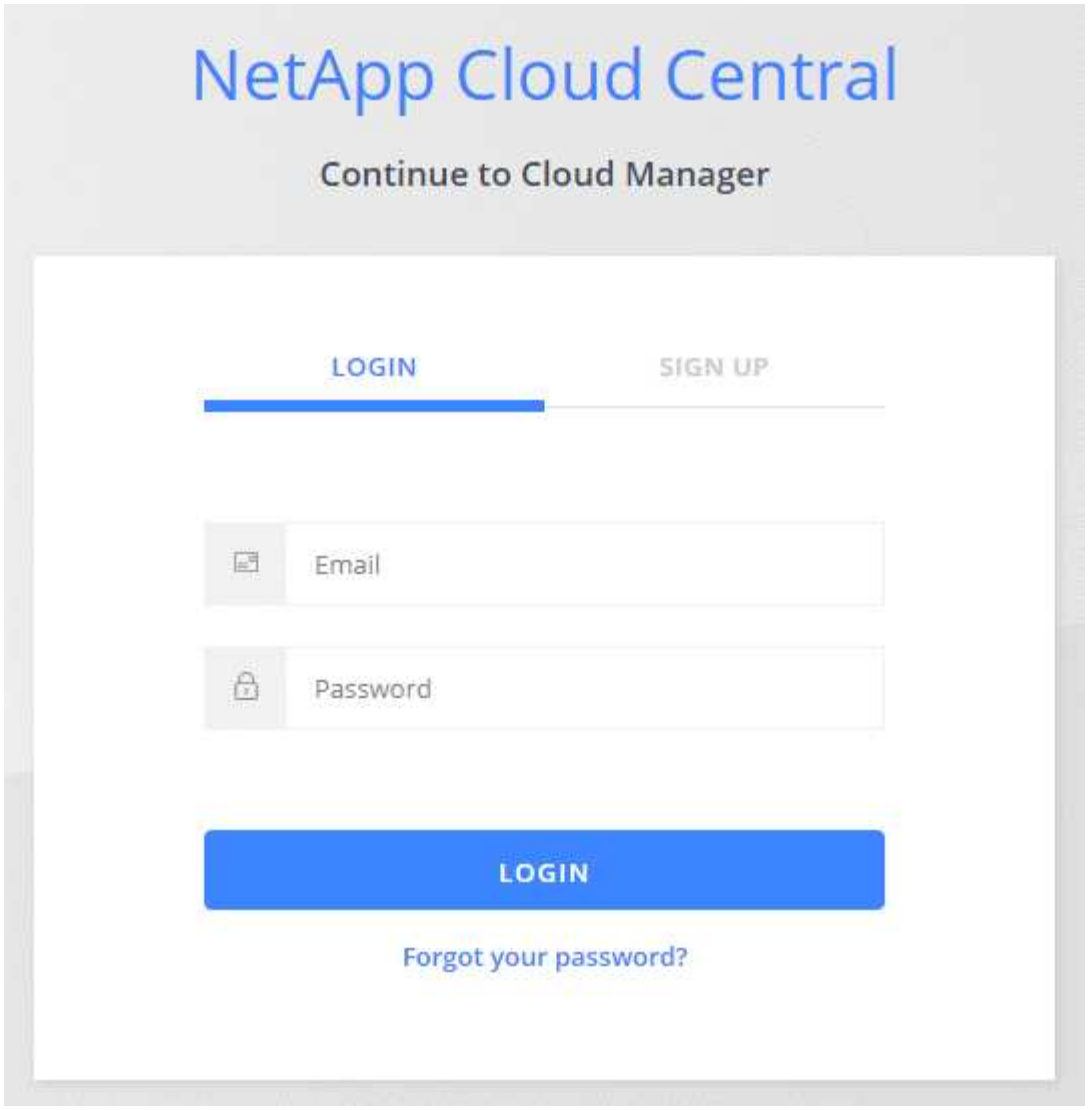
1. Open a web browser and log in to NetApp Cloud Central.

   This step should automatically direct you to the Fabric View. If it doesn't, then click **Fabric View**.

2. Select the Cloud Manager system that you want to access.

   If you don't see any systems listed, make sure that the Account Admin added you to the Cloud Central Account associated with the Cloud Manager system.

3. Log in to Cloud Manager using your NetApp Cloud Central credentials.




# Planning your Cloud Volumes ONTAP configuration

When you deploy Cloud Volumes ONTAP, 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 9.7 in AWS
- Supported configurations for Cloud Volumes ONTAP 9.7 in Azure
- Supported configurations for Cloud Volumes ONTAP 9.7 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 9.7 in AWS
- Storage limits for Cloud Volumes ONTAP 9.7 in Azure
- Storage limits for Cloud Volumes ONTAP 9.7 in GCP

## Choosing a write speed

Cloud Manager enables you to choose a write speed setting for single node Cloud Volumes ONTAP systems. 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.

#### Difference between normal write speed and high write speed

When you choose normal write speed, data is written directly to disk, thereby reducing the likelihood of data loss in the event of an unplanned system outage.

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, AWS EBS volume performance 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.

#### Recommendations when using high write speed

If you enable high write speed, you should ensure write protection at the application layer.

## 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.

## AWS planning

Plan your deployment of Cloud Volumes ONTAP in AWS by sizing your system and reviewing the network information that you need to enter.

- Sizing your system in AWS
- AWS network information worksheet

### 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:

[] | *https://img.youtube.com/vi/GELcXmOuYPw/maxresdefault.jpg*

### 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 | |

## Azure planning

Plan your deployment of Cloud Volumes ONTAP in Azure by sizing your system and reviewing the network information that you need to enter.

- Sizing your system in Azure

- Azure network information worksheet

### 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: Introduction to Microsoft Azure Storage.

#### 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

### 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) | |

## GCP planning

Plan your deployment of Cloud Volumes ONTAP in Google Cloud Platform by sizing your system and reviewing the network information that you need to enter.

- Sizing your system in GCP
- GCP network information worksheet

### 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.

| GCP information | Your value |
|---|---|
| Region | |
| Zone | |
| VPC network | |
| Subnet | |
| Firewall policy (if using your own) | |

# 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.

**Steps**

1. In the upper right of the Cloud Manager console, click the Settings icon.


2. Click **Support Dashboard**.

   Your system ID appears in the top right.

   **Example**


# Enabling Flash Cache on Cloud Volumes ONTAP

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 is effective for random read-intensive workloads, including databases, email, and file services.

## Limitations

- Compression must be disabled on all volumes to take advantage of the Flash Cache performance improvements.
- Cache rewarming after a reboot is not supported with Cloud Volumes ONTAP.

## Enabling Flash Cache on Cloud Volumes ONTAP in AWS

Flash Cache is supported with Cloud Volumes ONTAP Premium and BYOL in AWS.

**Steps**

1. Select one of the following EC2 instance types with a new or existing Cloud Volumes ONTAP Premium or BYOL system:
   - c5d.4xlarge
   - c5d.9xlarge
   - r5d.2xlarge
2. Disable compression 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.

## Enabling Flash Cache on Cloud Volumes ONTAP in Azure

Flash Cache is supported with Cloud Volumes ONTAP BYOL on single node systems.

**Steps**

1. Select the Standard_L8s_v2 VM type with a single node Cloud Volumes ONTAP BYOL system in Azure.
2. Disable compression 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.

# Launching Cloud Volumes ONTAP in AWS

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

## Subscribing from the AWS Marketplace

Subscribe from the AWS Marketplace to pay for Cloud Volumes ONTAP as you go or so you can deploy Cloud Volumes ONTAP BYOL.

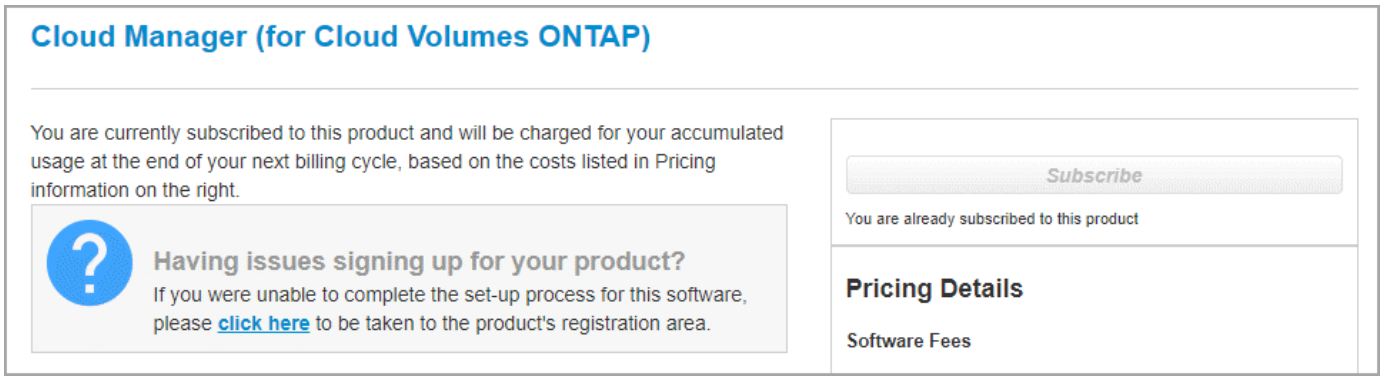
### Subscribing for PAYGO

Subscribe from the AWS Marketplace to ensure that there's no disruption of service after your free trial of Cloud Volumes ONTAP ends. 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.

The following video shows the subscription process:

► https://docs.netapp.com/us-en/occm37//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, AWS shows 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 the subscription. If you see the message shown below, click the **click here** link to go to Cloud Central and complete the process.




### Subscribing for BYOL

If you're launching Cloud Volumes ONTAP by bringing your own license (BYOL), then you'll need to subscribe to that offering in the AWS Marketplace.

Learn more about each AWS Marketplace page.

## Launching a single 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 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 Working Environments page, click **Create Cloud Volumes ONTAP** and follow the prompts.
2. **Define Your Working Environment**: Select **Amazon Web Services** and **Cloud Volumes ONTAP**.
3. **Details and Credentials**: Optionally change the AWS account and marketplace 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:

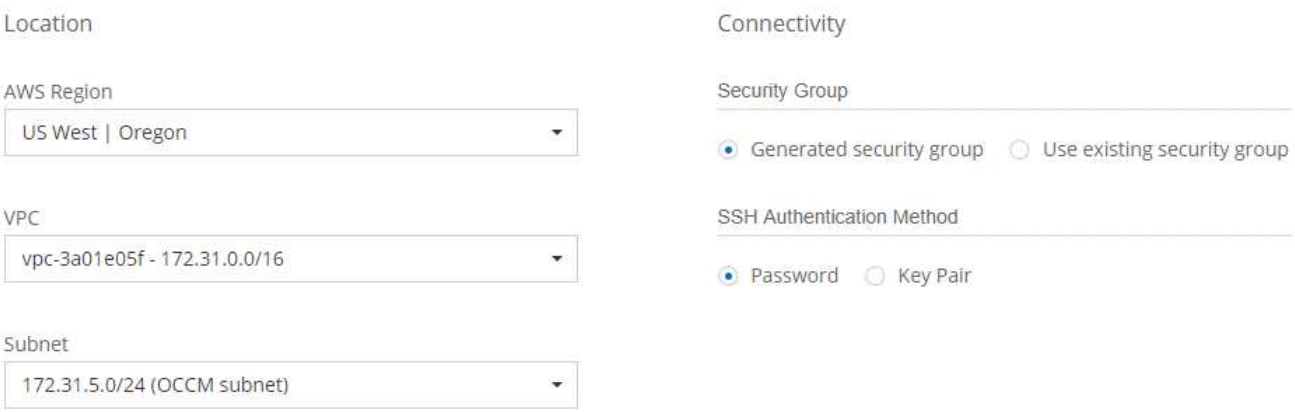
| Field | Description |
|---|---|
| Account | You can choose a different account if you added additional AWS accounts to Cloud Manager. |
| Marketplace Subscription | Select a different subscription if you want to change the AWS account from which you get charged. To add a new subscription, go to the offering in the AWS Marketplace. |
| 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. |
| Add tags | 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.<br><br>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.<br><br>For information about tags, refer to AWS Documentation: Tagging your Amazon EC2 Resources. |
| Credentials | 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. |

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 Backup to S3.
- Learn more about Cloud Compliance.

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

   The following image shows the page filled out:




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 9.4 RC1 and 9.4 GA is available. The update does not occur from one release to another—for example, from 9.3 to 9.4.

11. **Underlying Storage Resources**: Choose settings for the initial aggregate: a disk type, a size for each disk, and whether S3 tiering should be enabled.

    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.

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.

    Learn more about WORM storage.

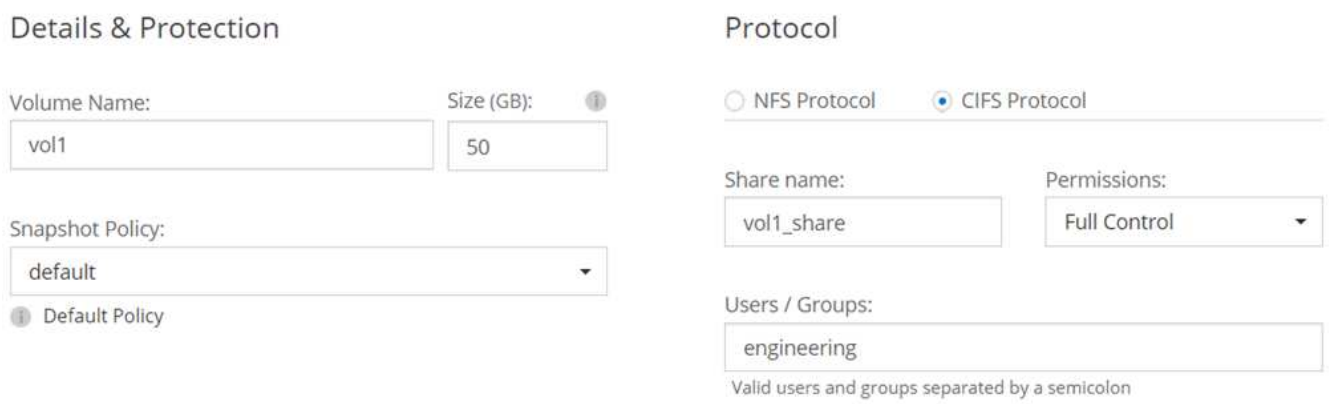
13. **Create Volume**: Enter details for the new volume or click **Skip**.

    You might skip this step if you want to create a volume for iSCSI. Cloud Manager sets up volumes for NFS and CIFS only.

    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. |

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




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.<br>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.<br>If you configure AWS Managed Microsoft AD as the AD server for Cloud Volumes ONTAP, you should enter **OU=Computers,OU=corp** in this field. |
| DNS Domain | The DNS domain for the Cloud Volumes ONTAP storage virtual machine (SVM). In most cases, the domain is the same as the AD domain. |
| NTP Server | Select **Use Active Directory Domain** to configure an NTP server using the Active Directory DNS. If you need to configure an NTP server using a different address, then you should use the API. See the Cloud Manager API Developer Guide for details. |

15. **Usage Profile, Disk Type, and Tiering Policy**: Choose whether you want to enable storage efficiency features and edit the S3 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 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 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 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.

**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 Working Environments page, click **Create Cloud Volumes ONTAP** and follow the prompts.
2. **Define Your Working Environment**: Select **Amazon Web Services** and **Cloud Volumes ONTAP HA**.
3. **Details and Credentials**: Optionally change the AWS account and marketplace 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:

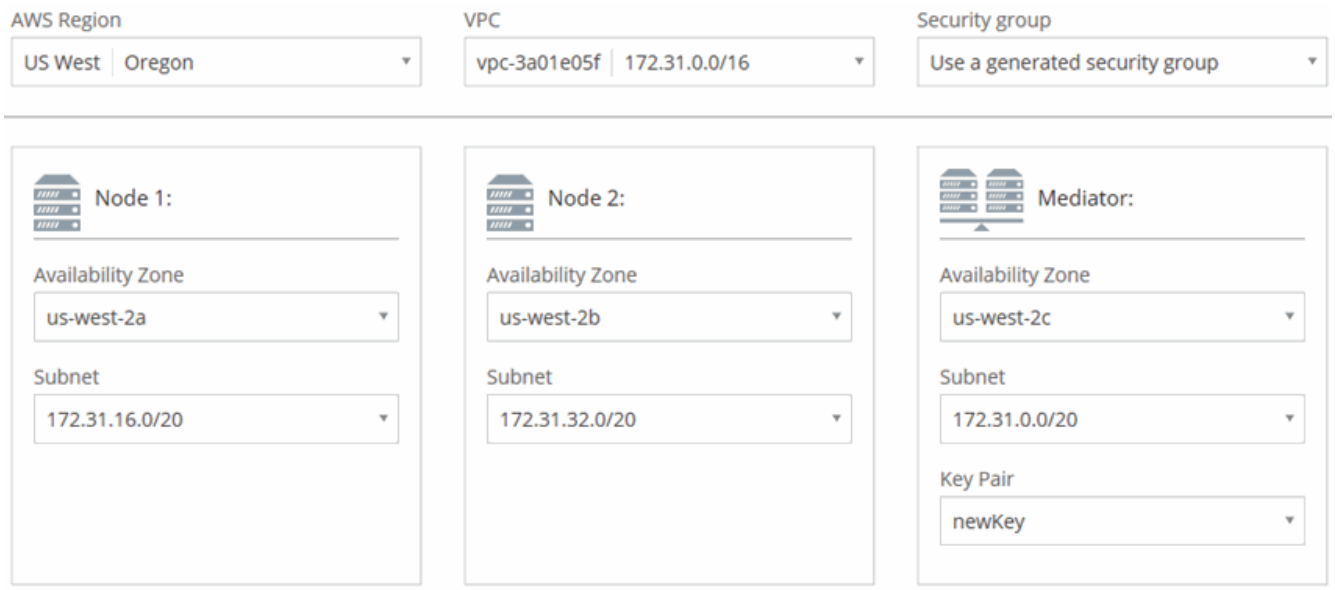
| Field | Description |
| --- | --- |
| Account | You can choose a different account if you added additional AWS accounts to Cloud Manager. |

| Field | Description |
|---|---|
| Marketplace Subscription | Select a different subscription if you want to change the AWS account from which you get charged. To add a new subscription, go to the offering in the AWS Marketplace. |
| 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. |
| Add tags | 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.<br><br>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.<br><br>For information about tags, refer to AWS Documentation: Tagging your Amazon EC2 Resources. |
| Credentials | 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. |

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 Backup to S3.
   - Learn more about Cloud Compliance.
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:



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 9.4 RC1 and 9.4 GA is available. The update does not occur from one release to another—for example, from 9.3 to 9.4.

15. **Underlying Storage Resources**: Choose settings for the initial aggregate: a disk type, a size for each disk, and whether S3 tiering should be enabled.

    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.

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

    Learn more about WORM storage.

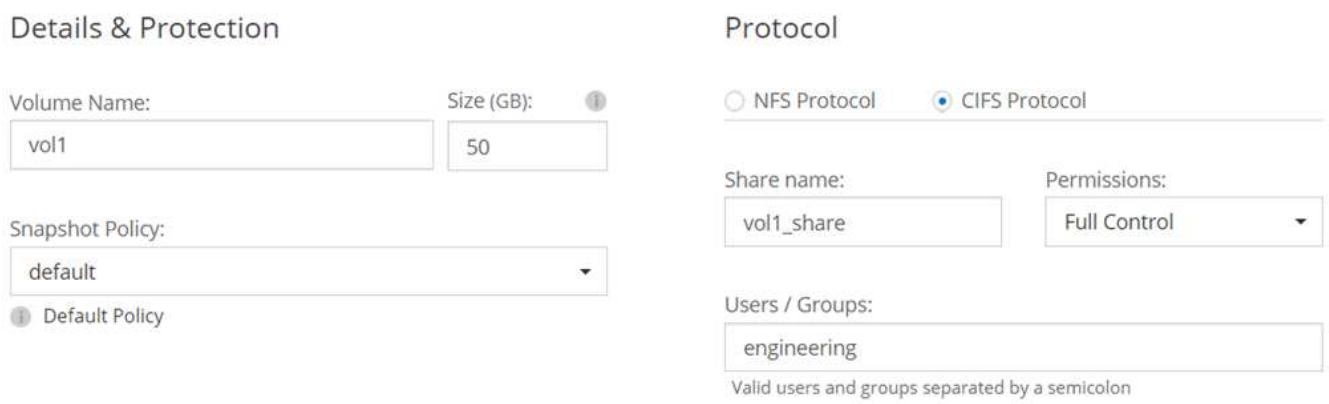
17. **Create Volume**: Enter details for the new volume or click **Skip**.

    You might skip this step if you want to create a volume for iSCSI. Cloud Manager sets up volumes for NFS and CIFS only.

    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. |

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




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.<br>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.<br>If you configure AWS Managed Microsoft AD as the AD server for Cloud Volumes ONTAP, you should enter **OU=Computers,OU=corp** in this field. |
| DNS Domain | The DNS domain for the Cloud Volumes ONTAP storage virtual machine (SVM). In most cases, the domain is the same as the AD domain. |
| NTP Server | Select **Use Active Directory Domain** to configure an NTP server using the Active Directory DNS. If you need to configure an NTP server using a different address, then you should use the API. See the Cloud Manager API Developer Guide for details. |

19. **Usage Profile, Disk Type, and Tiering Policy**: Choose whether you want to enable storage efficiency features and edit the S3 tiering policy, if needed.

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

20. **Review & Approve**: Review and confirm your selections.
    a. Review details about the configuration.
    b. Click **More information** to review details about support and the AWS resources that 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.

# 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**

- Make sure that your Azure account has the required permissions, especially if you upgraded from a previous release and are deploying an HA system for the first time.

  The latest permissions are in the NetApp Cloud Central policy for Azure.

- You should have chose 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.

**Steps**

1. On the Working Environments page, click **Create Cloud Volumes ONTAP** and follow the prompts.
2. **Define Your Working Environment**: Select **Microsoft Azure** and then choose a single node or HA pair.
3. **Details and Credentials**: Optionally change the Azure account or 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 |
| --- | --- |
| Switch Account | You can choose a different account or subscription if you set them up and added them to Cloud Manager. |

| 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 | If you uncheck **Use Default**, you can enter the name of a new resource group. If you want to use an existing resource group, then you must use the API. |
| Tags | Tags are metadata for your Azure resources. Cloud Manager adds the tags to the Cloud Volumes ONTAP system and each Azure resource associated with the system.<br><br>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.<br><br>For information about tags, refer to Microsoft Azure Documentation: Using tags to organize your Azure resources. |
| Credentials | 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. |

4. **Services**: Keep Cloud Compliance enabled or disable it if you don't want to use it with this Cloud Volumes ONTAP system.

   Learn more about Cloud Compliance.

5. **Location & Connectivity**: Select a location and security group and select the checkbox to confirm network connectivity between Cloud Manager and the target location.
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**: Shelect 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 9.5 RC1 and 9.5 GA is available. The update does not occur from one release to another—for example, from 9.4 to 9.5.

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.

    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.

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

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

    Learn more about write speed.

    Learn more about WORM storage.

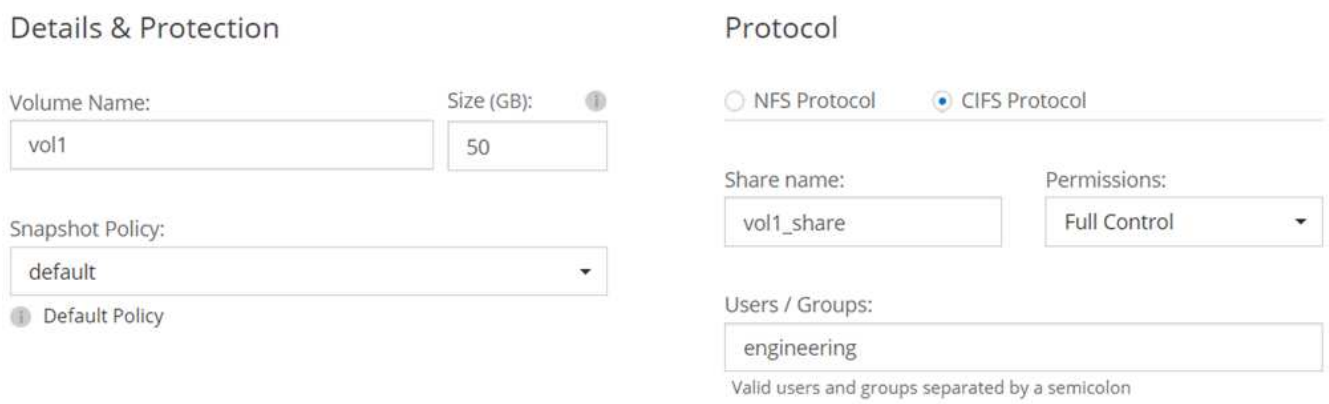
12. **Create Volume**: Enter details for the new volume or click **Skip**.

    You should skip this step if you want to use iSCSI. Cloud Manager enables you to create volumes for NFS and CIFS only.

    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. |

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




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.<br>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.<br><br>To configure Azure AD Domain Services as the AD server for Cloud Volumes ONTAP, you should enter **OU=AADDC Computers** or **OU=AADDC Users** in this field.<br>Azure Documentation: Create an Organizational Unit (OU) in an Azure AD Domain Services managed domain |
| DNS Domain | The DNS domain for the Cloud Volumes ONTAP storage virtual machine (SVM). In most cases, the domain is the same as the AD domain. |
| NTP Server | Select **Use Active Directory Domain** to configure an NTP server using the Active Directory DNS. If you need to configure an NTP server using a different address, then you should use the API. See the Cloud Manager API Developer Guide for details. |

14. **Usage Profile, Disk Type, and Tiering Policy**: Choose whether you want to enable storage efficiency features and change the 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 Azure 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 Cloud Volumes ONTAP in GCP

You can launch a single node Cloud Volumes ONTAP system in GCP by creating a working environment.

**Before you begin**

- You should have chose 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.

**Steps**

1. On the Working Environments page, click **Create Cloud Volumes ONTAP** and follow the prompts.
2. **Define Your Working Environment**: Click **Continue**.
3. **Subscribe to Cloud Volumes ONTAP**: If you're prompted, subscribe to Cloud Volumes ONTAP in the GCP Marketplace.

   The following video shows the subscription process:

   ► https://docs.netapp.com/us-en/occm37//media/video_subscribing_gcp.mp4 *(video)*

4. **Details & Credentials**: Select a project, specify a cluster name, optionally add labels, and then specify credentials.

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

| Field | Description |
| --- | --- |
| Google Cloud Project | Select the project where you want Cloud Volumes ONTAP to reside. The default project is the project where Cloud Manager resides.<br><br>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.<br><br>This is the service account that you set up for Cloud Manager, as described in step 4b on this page. |
| 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. |
| Add Labels | 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.<br><br>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.<br><br>For information about labels, refer to Google Cloud Documentation: Labeling Resources. |
| Credentials | 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. |

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 9.5 RC1 and 9.5 GA is available. The update does not occur from one release to another—for example, from 9.4 to 9.5.

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

   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.

    Learn more about write speed.

    Learn more about WORM storage.

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

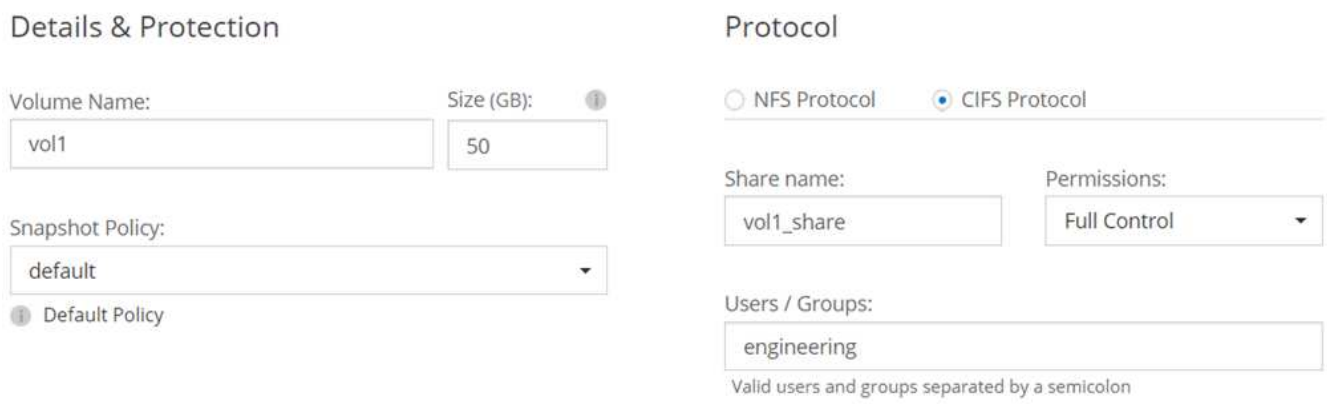
    You should skip this step if you want to use iSCSI. Cloud Manager enables you to create volumes for NFS and CIFS only.

    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. |

| Field | Description |
| --- | --- |
| Snapshot Policy | A Snapshot copy policy specifies the frequency and number of automatically created NetApp Snapshot copies. A NetApp Snapshot copy is a point-in-time file system image that has no performance impact and requires minimal storage. You can choose the default policy or none. You might choose none for transient data: for example, tempdb for Microsoft SQL Server. |

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




12. **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.<br>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 **Use Active Directory Domain** to configure an NTP server using the Active Directory DNS. If you need to configure an NTP server using a different address, then you should use the API. See the Cloud Manager API Developer Guide for details. |

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

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

14. **Google Cloud Platform Account for Data Tiering**: Set up data tiering by providing interoperable storage access keys for a Google Cloud Platform account. Click **Skip** to disable data tiering.

    The keys enable Cloud Manager to set up a Cloud Storage bucket for data tiering. For more details, see Setting up and adding GCP accounts to Cloud Manager.

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.

# Registering pay-as-you-go systems

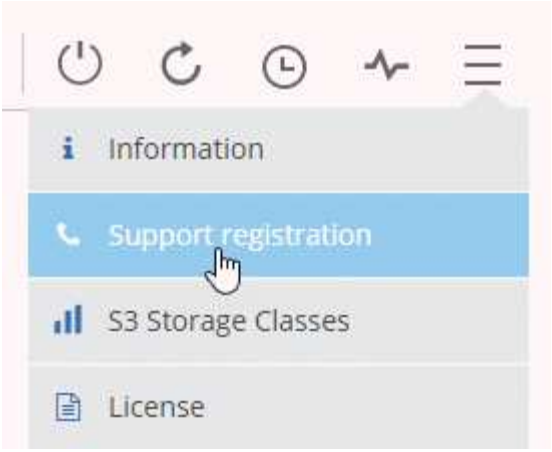
Support from NetApp is included with Cloud Volumes ONTAP Explore, Standard, and Premium systems, but you must first activate support by registering the systems with NetApp.

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



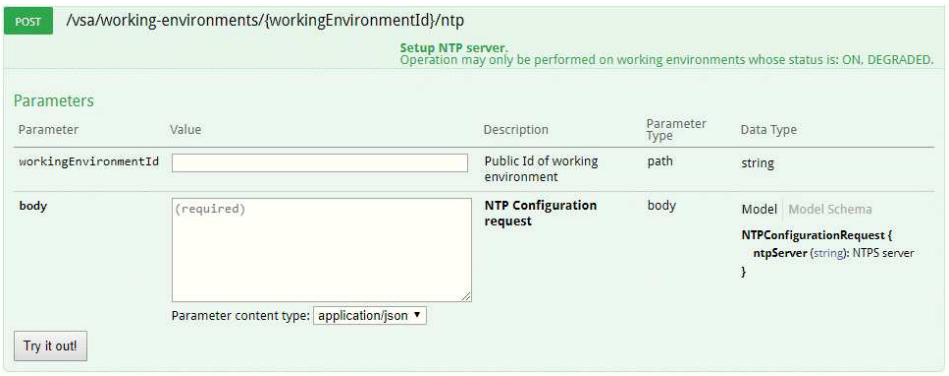

4. Select a NetApp Support Site account and click **Register**.

**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 |
|---|---|
| Synchronize the system time using NTP | Specifying an NTP server synchronizes the time between the systems in your network, which can help prevent issues due to time differences.<br><br>Specify an NTP server using the Cloud Manager API or from the user interface when you set up a CIFS server.<br><br>• Modifying the CIFS server<br>• Cloud Manager API Developer Guide<br><br>For example, here's the API for a single-node system in AWS:<br><br>  |

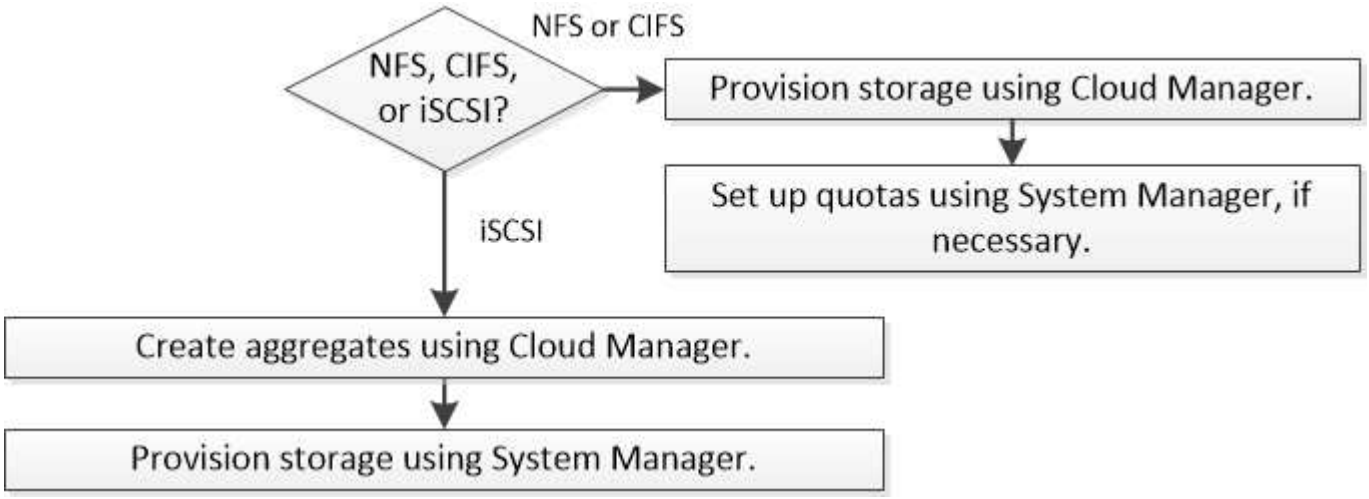
| Task | Description |
| --- | --- |
| Optional: Configure AutoSupport | AutoSupport proactively monitors the health of your system and automatically sends messages to NetApp technical support by default.<br><br>If the Account Admin added a proxy server to Cloud Manager before you launched your instance, Cloud Volumes ONTAP is configured to use that proxy server for AutoSupport messages.<br><br>You should test AutoSupport to ensure that it can send messages. For instructions, see the System Manager Help or the ONTAP 9 System Administration Reference. |
| Optional: Configure EMS | 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.<br><br>You can configure EMS using the CLI. For instructions, see the ONTAP 9 EMS Configuration Express Guide. |
| Optional: Create an SVM management network interface (LIF) for HA systems in multiple AWS Availability Zones | A storage virtual machine (SVM) management network interface (LIF) is required if you want to use SnapCenter or SnapDrive for Windows with an HA pair. The SVM management LIF must use a *floating* IP address when using an HA pair across multiple AWS Availability Zones.<br><br>Cloud Manager prompts you to specify the floating IP address when you launch the HA pair. If you did not specify the IP address, you can create the SVM Management LIF yourself from System Manager or the CLI. The following example shows how to create the LIF from the CLI:<br><br>`network interface create -vserver svm_cloud -lif svm_mgmt -role data -data-protocol none -home-node cloud-01 -home-port e0a -address 10.0.2.126 -netmask 255.255.255.0 -status-admin up -firewall -policy mgmt` |
| Optional: Change the backup location of configuration files | Cloud Volumes ONTAP automatically creates configuration backup files that contain information about the configurable options that it needs to operate properly.<br><br>By default, Cloud Volumes ONTAP backs up the files to the Cloud Manager 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.<br><br>You can change the backup location using the CLI. See the ONTAP 9 System Administration Reference. |

# Provision storage

## Provisioning storage

You can provision additional NFS and CIFS storage for your Cloud Volumes ONTAP systems from Cloud Manager by managing volumes and aggregates. If you need to create iSCSI storage, you should do so from System Manager.

> 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 or CIFS from Cloud Manager.

#### 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 Working Environments 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 **Add New Volume**. |

| Action | Steps |
| --- | --- |
| Create a new volume on a specific aggregate | a. Click the menu icon, and then click **Advanced > Advanced allocation**.<br>b. Click the menu for an aggregate.<br>c. Click **Create volume**. |

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. |

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

| Field | Description |
| --- | --- |
| Organizational Unit | The organizational unit within the AD domain to associate with the CIFS server. The default is CN=Computers.<br>• To configure AWS Managed Microsoft AD as the AD server for Cloud Volumes ONTAP, you should enter **OU=Computers,OU=corp** in this field.<br>• To configure Azure AD Domain Services as the AD server for Cloud Volumes ONTAP, you should enter **OU=AADDC Computers** or **OU=AADDC Users** in this field.<br>Azure Documentation: Create an Organizational Unit (OU) in an Azure AD Domain Services managed domain |
| DNS Domain | The DNS domain for the Cloud Volumes ONTAP storage virtual machine (SVM). In most cases, the domain is the same as the AD domain. |
| NTP Server | Select **Use Active Directory Domain** to configure an NTP server using the Active Directory DNS. If you need to configure an NTP server using a different address, then you should use the API. See the Cloud Manager API Developer Guide 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 Working Environments 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 Working Environments 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**.

## Provisioning iSCSI LUNs

If you want to create iSCSI LUNs, you need to do so from System Manager.

#### Before you begin

- The Host Utilities must be installed and set up on the hosts that will connect to the LUN.
- You must have recorded the iSCSI initiator name from the host. You need to supply this name when you create an igroup for the LUN.
- Before you create volumes in System Manager, you must ensure that you have an aggregate with sufficient space. You need to create aggregates in Cloud Manager. For details, see Creating aggregates.

#### About this task

These steps describe how to use System Manager for version 9.3 and later.

#### Steps

1. Log in to System Manager.
2. Click **Storage > LUNs**.
3. Click **Create** and follow the prompts to create the LUN.

4. Connect to the LUN from your hosts.

   For instructions, see the Host Utilities documentation for your operating system.

### 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.


# Tiering inactive data to low-cost object storage

You can reduce storage costs by combining an SSD or HDD performance tier for hot data

with an object storage capacity tier for inactive data. For a high-level overview, see Data tiering overview.

To set up data tiering, you simply 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 add a GCP account to Cloud Manager and configure the subnet for Private Google Access. 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.

## 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 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

- You need to add a Google Cloud Platform account to Cloud Manager by entering storage access keys for a service account. The keys enable Cloud Manager to set up a Cloud Storage bucket for data tiering. For instructions, see Setting up and adding GCP accounts to Cloud Manager.
- 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.

## Tiering data from read-write volumes

Cloud Volumes ONTAP can tier inactive data on read-write volumes to cost-effective object storage, freeing up the performance tier for hot data.

### Steps

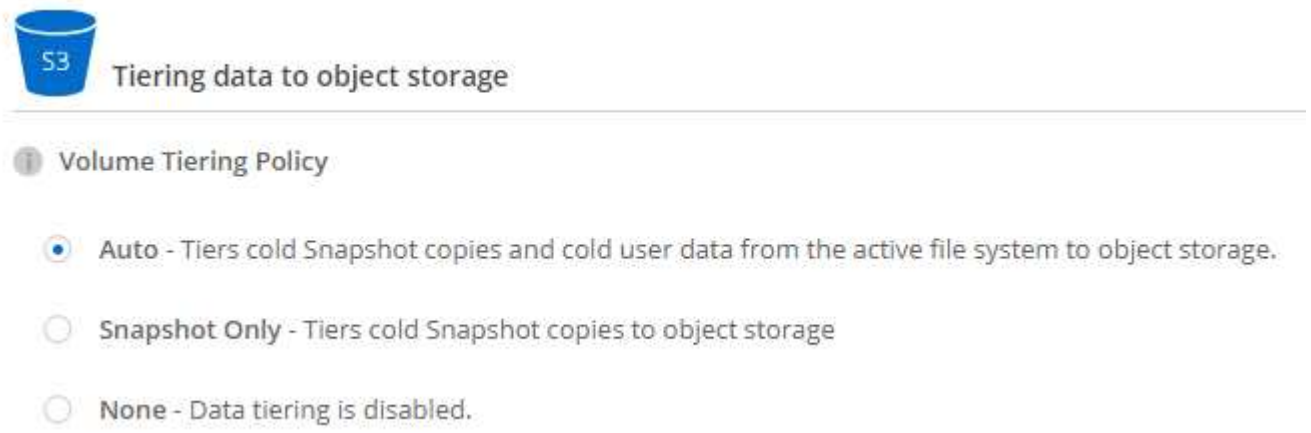
1. In the working environment, create a new volume or change the tier of an existing volume:

| Task | Action |
| --- | --- |
| Create a new volume | Click **Add New Volume**. |
| Modify an existing volume | Select the volume and click **Change Disk Type & Tiering Policy**. |

2. Select the Snapshot Only policy or the Auto policy.

   For a description of these policies, see Data tiering overview.

   **Example**




   Cloud Manager creates a new aggregate for the volume if a data tiering-enabled aggregate does not already exist.

   If you prefer to create aggregates yourself, you can enable data tiering on aggregates when you create them.

## 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 Working Environments 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**

For help with replicating data, see Replicating data to and from the cloud.

### Changing the tiering level in AWS or Azure

When you enable data tiering, Cloud Volumes ONTAP tiers inactive data to the S3 *Standard* storage class in AWS or to the *hot* storage tier in Azure. After you deploy Cloud Volumes ONTAP, you can reduce your storage costs by changing the tiering level for inactive data that has not 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 tiering level.

You can't change the tiering level in GCP because only the *Regional* storage class is supported at this time.

**About this task**

The tiering level is system wide—it is not per volume.

In AWS, you can change the tiering level so inactive data moves to one of the following storage classes after 30 days of inactivity:

- Intelligent Tiering
- Standard-Infrequent Access
- One Zone-Infrequent Access

In Azure, you can change the tiering level so inactive data moves to the *cool* storage tier after 30 days of inactivity.

For more information about how tiering levels work, see Data tiering overview.

**Steps**

1. From the working environment, click the menu icon and then click **S3 Storage Classes** or **Blob Storage Tiering**.
2. Choose the tiering level and then click **Save**.

# Using ONTAP as persistent storage for Kubernetes

Cloud Manager can automate the deployment of NetApp Trident on Kubernetes clusters so you can use ONTAP as persistent storage for containers. This works with Cloud Volumes ONTAP and on-prem ONTAP clusters.

Before you complete these steps, you need to create a Cloud Volumes ONTAP system or discover an on-premises ONTAP cluster from Cloud Manager.

If you deploy Kubernetes clusters using the NetApp Kubernetes Service, Cloud Manager can automatically discover the clusters from your NetApp Cloud Central account. If that's the case, skip the first two steps and start with step 3.

### 1 Verify network connectivity

a. A network connection must be available between Cloud Manager and the Kubernetes clusters, and from

the Kubernetes clusters to ONTAP systems.

b. Cloud Manager needs an outbound internet connection to access the following endpoints when installing Trident:

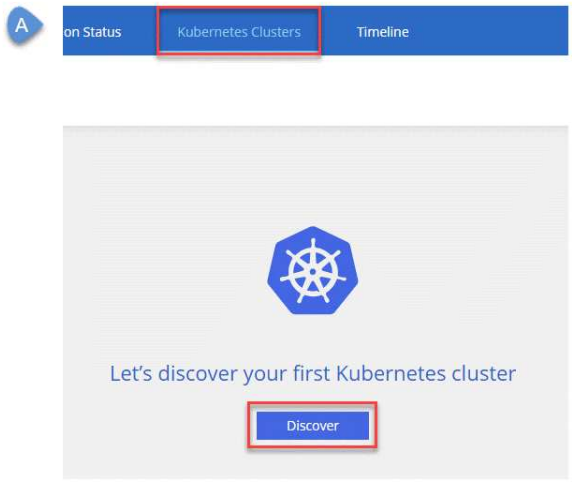
   https://packages.cloud.google.com/yum
   https://github.com/NetApp/trident/releases/download/

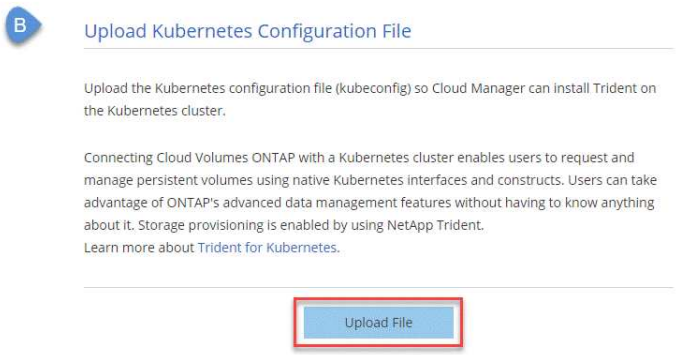
   Cloud Manager installs Trident on a Kubernetes cluster when you connect a working environment to the cluster.

### Upload Kubernetes configuration files to Cloud Manager

For each Kubernetes cluster, the Account Admin needs to upload a configuration file (kubeconfig) that is in YAML format. After you upload the file, Cloud Manager verifies connectivity to the cluster and saves an encrypted copy of the kubeconfig file.

Click **Kubernetes Clusters > Discover > Upload File** and select the kubeconfig file.

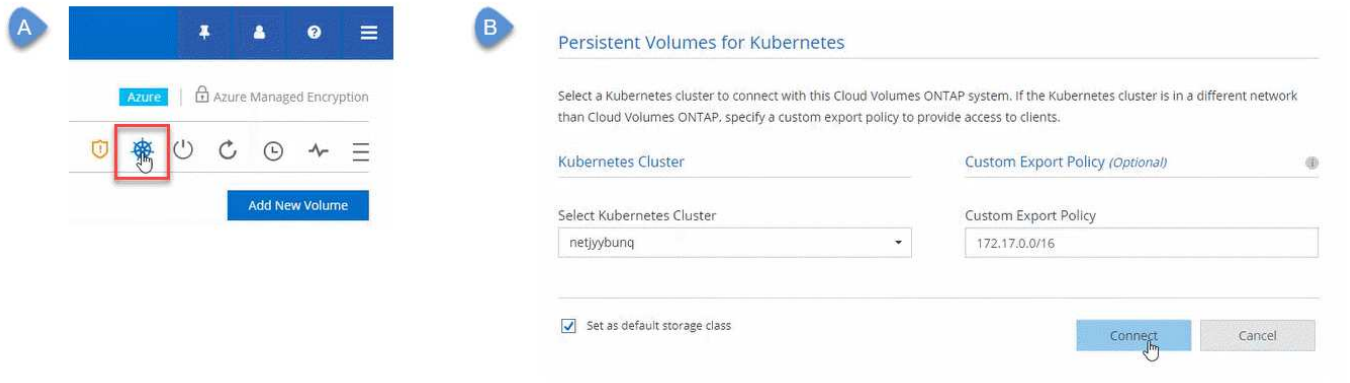



### Connect your working environments to Kubernetes clusters

From the working environment, click the Kubernetes icon and follow the prompts. You can connect different clusters to different ONTAP systems and multiple clusters to the same ONTAP system.

You have the option to set the NetApp storage class as the default storage class for the Kubernetes cluster. When a user creates a persistent volume, the Kubernetes cluster can use connected ONTAP systems as the backend storage by default.




## 4 Start provisioning Persistent Volumes

Request and manage Persistent Volumes using native Kubernetes interfaces and constructs. Cloud Manager creates four Kubernetes storage classes that you can use when provisioning Persistent Volumes:

- **netapp-file**: for binding Persistent Volumes to single-node ONTAP systems
- **netapp-file-san**: for binding iSCSI Persistent Volumes to single-node ONTAP systems
- **netapp-file-redundant**: for binding Persistent Volumes to ONTAP HA pairs
- **netapp-file-redundant-san**: for binding iSCSI Persistent Volumes to ONTAP HA pairs

Cloud Manager configures Trident to use the following provisioning options by default:

- Thin volumes
- The default Snapshot policy
- Accessible Snapshot directory

Learn more about provisioning your first volume with Trident for Kubernetes

### What are the trident_trident volumes?

Cloud Manager creates a volume on the first ONTAP system that you connect to a Kubernetes cluster. The name of the volume is appended with "_trident_trident." ONTAP uses this volume to connect to the Kubernetes cluster. You should not delete these volumes.

### What happens when you disconnect or remove a Kubernetes cluster?

Cloud Manager enables you to disconnect individual ONTAP systems from a Kubernetes cluster. When you disconnect a system, you can no longer use that ONTAP system as persistent storage for containers. Existing Persistent Volumes are not deleted.

After you disconnect all systems from a Kubernetes cluster, you can also remove the entire Kubernetes configuration from Cloud Manager. Cloud Manager does not uninstall Trident when you remove the cluster and it does not delete any Persistent Volumes.

Both of these actions are available through APIs only. We plan to add the actions to the interface in a future release.
Click here for details about the APIs.

# Encrypting volumes with NetApp Volume Encryption

NetApp Volume Encryption (NVE) is a software-based technology for encrypting data at rest one volume at a time. Data, Snapshot copies, and metadata are encrypted. Access to the data is given by a unique XTS-AES-256 key, one per volume.

**About this task**

- 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 does not install the NVE license on systems that reside in the China region.

- At this time, Cloud Volumes ONTAP supports NetApp Volume Encryption with an external key management server. An Onboard Key Manager is not supported.
- You need to set up NetApp Volume Encryption from the ONTAP CLI.

  You can then use either the CLI or System Manager to enable encryption on specific volumes. Cloud Manager does not support NetApp Volume Encryption from its user interface and from its APIs.

Learn more about supported encryption technologies.

**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

4. Create a new encrypted volume or convert an existing unencrypted volume using either the CLI or System Manager.
   - CLI:
     - For new volumes, use the **volume create** command with the -encrypt parameter.

       ONTAP 9 NetApp Encryption Power Guide: Enabling encryption on a new volume

     - For existing volumes, use the **volume encryption conversion start** command.

       ONTAP 9 NetApp Encryption Power Guide: Enabling encryption on an existing volume with the volume encryption conversion start command

   - System Manager:
     - For new volumes, click **Storage > Volumes > Create > Create FlexVol** and then select **Encrypted**.

       ONTAP 9 Cluster Management using System Manager: Creating FlexVol volumes

     - For existing volumes, select the volume, click **Edit**, and then select **Encrypted**.

       ONTAP 9 Cluster Management using System Manager: Editing volume properties

# 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 Working Environments page, double-click the Cloud Volumes ONTAP working environment on which you want to manage volumes.
2. Manage your volumes:

| Task | Action |
|---|---|
| View information about a volume | Select a volume, and then click **Info**. |
| Edit a volume (read-write volumes only) | a. Select a volume, and then click **Edit**.<br>b. Modify the volume's Snapshot policy, NFS access control list, or share permissions, and then click **Update**.<br>If you need custom Snapshot policies, you can create them by using System Manager. |

| Task | Action |
| --- | --- |
| Clone a volume | a. Select a volume, and then click **Clone**.<br>b. Modify the clone name as needed, and then click **Clone**.<br><br>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.<br><br>To learn more about FlexClone volumes, see the ONTAP 9 Logical Storage Management Guide. |
| Restore data from a Snapshot copy to a new volume | a. Select a volume, and then click **Restore from Snapshot copy**.<br>b. Select a Snapshot copy, enter a name for the new volume, and then click **Restore**. |
| Create a Snapshot copy on demand | a. Select a volume, and then click **Create a Snapshot copy**.<br>b. Change the name, if needed, and then click **Create**. |
| Get the NFS mount command | a. Select a volume, and then click **Mount Command**.<br>b. Click **Copy**. |
| Change the underlying disk type | a. Select a volume, and then click **Change Disk Type & Tiering Policy**.<br>b. Select the disk type, and then click **Change**.<br><br>Cloud Manager moves the volume to an existing aggregate that uses the selected disk type or it creates a new aggregate for the volume. |
| Change the tiering policy | a. Select a volume, and then click **Change Disk Type & Tiering Policy**.<br>b. Click **Edit Policy**.<br>c. Select a different policy and click **Change**.<br><br>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. |
| Enable or disable sync to S3 for a volume | Select a volume and then click **Sync to S3** or **Delete Sync Relationship**.<br><br>The sync to S3 feature must be enabled before you can use these options. For instructions, see Syncing data to AWS S3 |

| Task | Action |
| --- | --- |
| Delete a volume | a. Select a volume, and then click **Delete**.<br>b. Click **Delete** again to confirm. |

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

| Task | Action |
| --- | --- |
| View information about an aggregate | Select an aggregate and click **Info**. |
| Create a volume on a specific aggregate | Select an aggregate and click **Create volume**. |
| Add disks to an aggregate | a. Select an aggregate and click **Add AWS disks** or **Add Azure disks**.<br>b. Select the number of disks that you want to add and click **Add**.<br>All disks in an aggregate must be the same size. |
| Delete an aggregate | a. Select an aggregate that does not contain any volumes and click **Delete**.<br>b. Click **Delete** again to confirm. |

## 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.<br><br>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.<br>If you configure AWS Managed Microsoft AD as the AD server for Cloud Volumes ONTAP, you should enter **OU=Computers,OU=corp** in this field. |
| DNS Domain | The DNS domain for the Cloud Volumes ONTAP storage virtual machine (SVM). In most cases, the domain is the same as the AD domain. |
| NTP Server | Select **Use Active Directory Domain** to configure an NTP server using the Active Directory DNS. If you need to configure an NTP server using a different address, then you should use the API. See the Cloud Manager API Developer Guide for details. |

3. Click **Save**.

#### Result

Cloud Volumes ONTAP updates the CIFS server with the changes.

## Moving a volume to avoid capacity issues

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

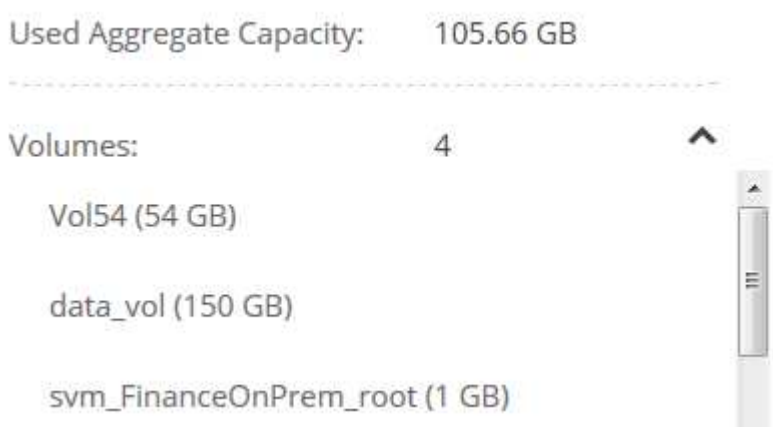
If Cloud Manager cannot provide recommendations for moving a volume to avoid capacity issues, you must identify the volumes that you need to move and whether you should move them to another aggregate on the same system or to another system.

**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.




   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.

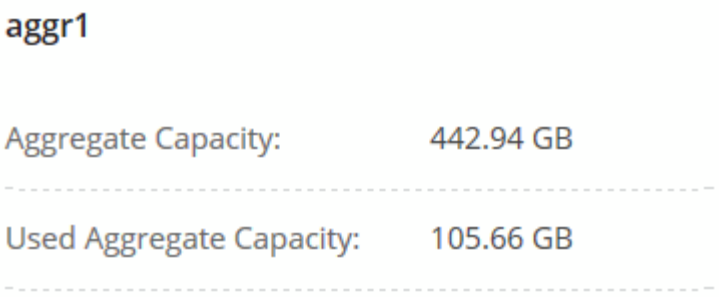
**About this task**

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).




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.

# Replicate and protect data

# Discovering and managing 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 these clusters enables you to easily replicate data across your hybrid cloud environment directly from Cloud Manager.

## Discovering ONTAP clusters

Discovering an ONTAP cluster in Cloud Manager enables you to provision storage and replicate data across your hybrid cloud.

### Before you begin

You must have 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 Cloud Manager host must allow outbound HTTPS access through port 443.

  If Cloud Manager is in AWS, 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 Cloud Manager host.

### Steps

1. On the Working Environments page, click **Discover** and select **ONTAP Cluster**.
2. 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.



3. On the Details page, enter a name and description for the working environment, and then click **Go**.

### Result

Cloud Manager discovers the cluster. You can now create volumes, replicate data to and from the cluster, and launch OnCommand System Manager to perform advanced tasks.

## Provisioning volumes on ONTAP clusters

Cloud Manager enables you to provision NFS and CIFS volumes on ONTAP clusters.

### Before you begin

NFS or CIFS must be set up on the cluster. You can set up NFS and CIFS using System Manager or the CLI.

### About this task

You can create volumes on existing aggregates. You cannot create new aggregates from Cloud Manager.

**Steps**

1. On the Working Environments 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. |
| 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. |
| Usage Profile | Usage profiles define the NetApp storage efficiency features that are enabled for a volume. |
| 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. |

# 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.

## 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 10000, 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

1. On the Working Environments 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 Working Environments page, view the replication status for all working environments in the

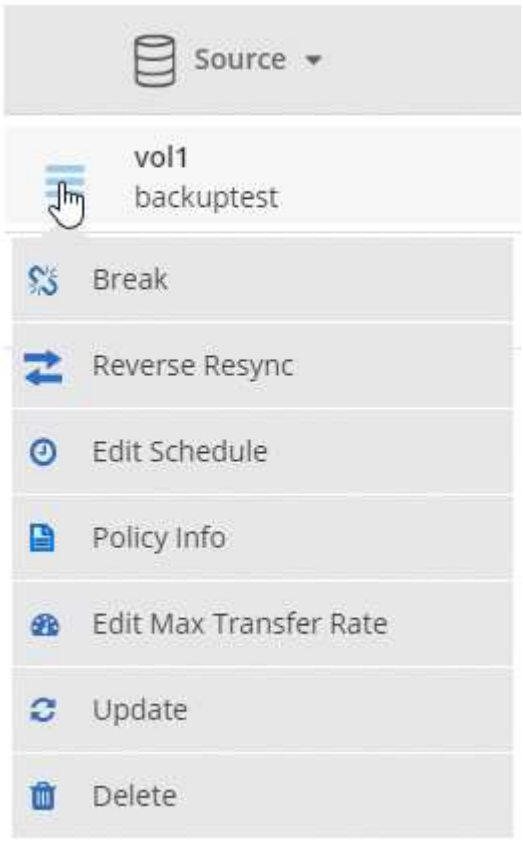
workspace or for a specific working environment:

| Option | Action |
| --- | --- |
| All working environments in the workspace | At the top of Cloud Manager, click **Replication Status**. |
| A specific working environment | Open the working environment and click **Replications**. |

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 | Breaks the relationship between the source and destination volumes, and activates the destination volume for data access.<br><br>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.<br><br>For information about configuring a destination volume for data access and reactivating a source volume, see the ONTAP 9 Volume Disaster Recovery Express Guide. |
| Resync | Reestablishes a broken relationship between volumes and resumes data replication according to the defined schedule.<br><br>When you resynchronize the volumes, the contents on the destination volume are overwritten by the contents on the source volume.<br><br>To perform a reverse resync, which resynchronizes the data from the destination volume to the source volume, see the ONTAP 9 Volume Disaster Recovery Express Guide. |
| Reverse Resync | 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.<br><br>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. |
| 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.

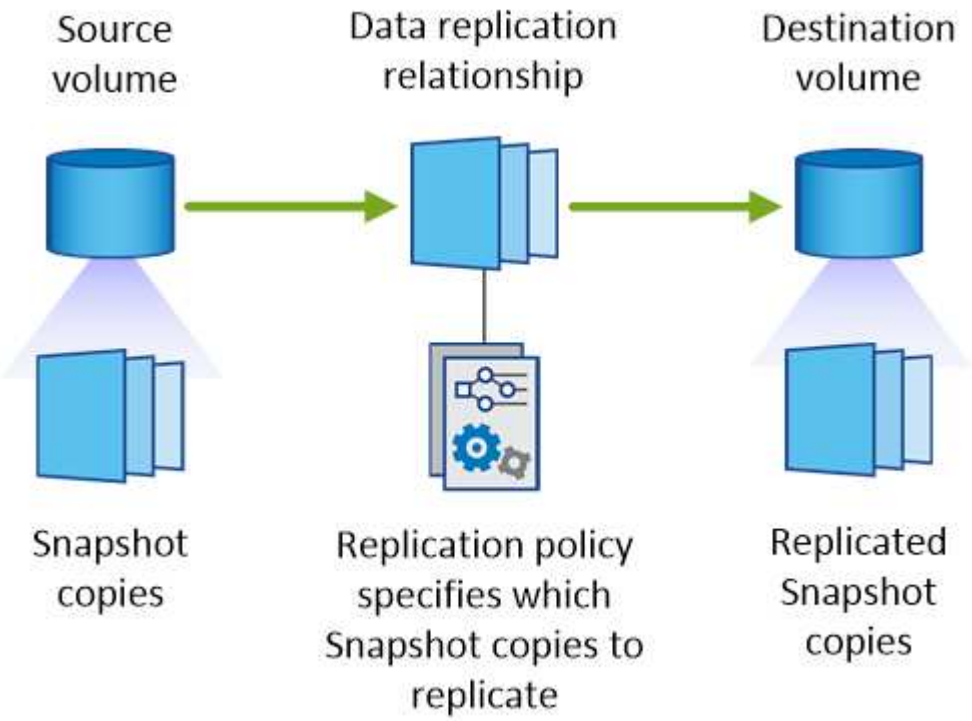
### What replication policies do

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.

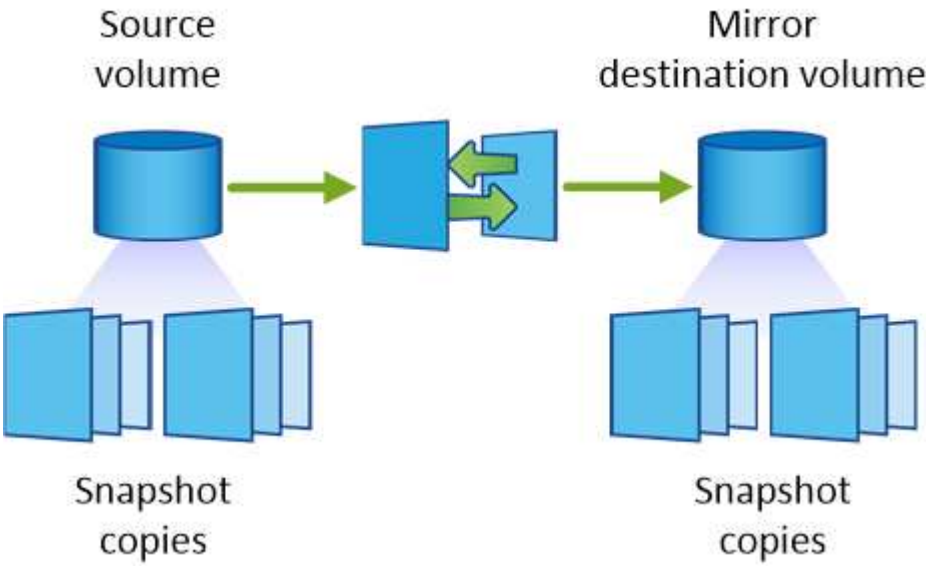
- A *Backup* policy replicates specific Snapshot copies to a destination volume and typically retains them for a longer period of time than you would on the source volume.

  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.

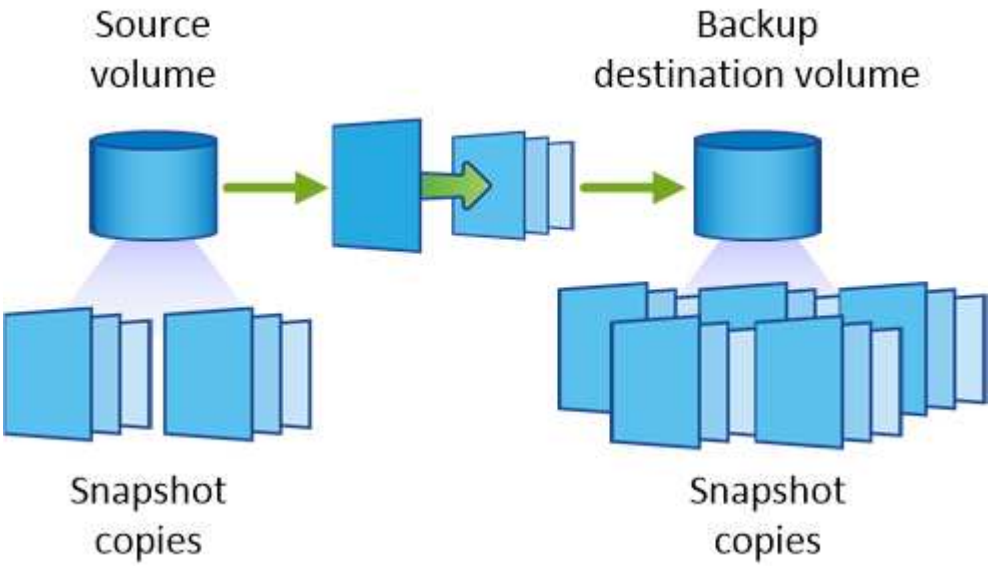
- A *Mirror and Backup* policy provides both disaster recovery and long-term retention.

  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.

# Backing up data to Amazon S3

Backup to S3 is an add-on feature for Cloud Volumes ONTAP that delivers fully-managed backup and restore capabilities for protection, and long-term archive of your cloud data. Backups are stored in S3 object storage, independent of volume Snapshot copies used for near-term recovery or cloning.

When you enable Backup to S3, the service performs a full backup of your data. All additional backups are incremental, which means that only changed blocks and new blocks are backed up.

Go to NetApp Cloud Central for pricing details.

Note that you must use Cloud Manager for all backup and restore operations. Any actions taken directly from ONTAP or from Amazon S3 results in an unsupported configuration.

## Quick start

Get started quickly by following these steps or scroll down to the remaining sections for full details.

**Verify support for your configuration**

Verify the following:

- Cloud Volumes ONTAP 9.4 or later is running in a supported AWS region: N. Virginia, Oregon, Ireland, Frankfurt, or Sydney
- You have subscribed to the new Cloud Manager Marketplace offering
- TCP port 5010 is open for outbound traffic on the security group for Cloud Volumes ONTAP (it's open by default)
- TCP port 8088 is open for outbound traffic on the security group for Cloud Manager (it's open by default)
- The following endpoint is accessible from Cloud Manager:

  https://w86yt021u5.execute-api.us-east-1.amazonaws.com/production/whitelist

- There's room for Cloud Manager to allocate up to two interface VPC endpoints in the VPC (the AWS limit

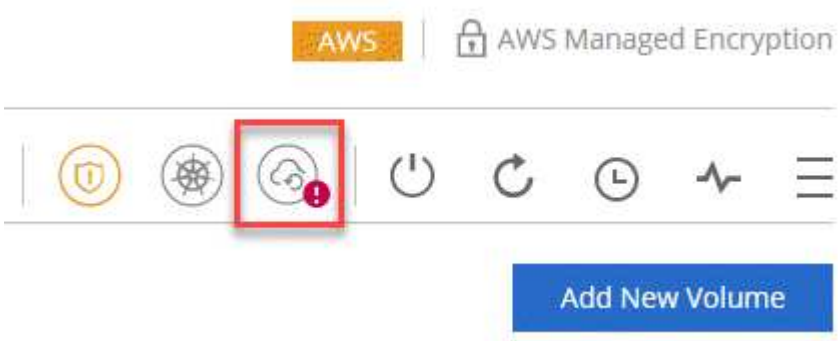
per VPC is 20)

- Cloud Manager has permission to use the VPC endpoint permissions listed in the latest Cloud Manager policy:

```
"ec2:DescribeVpcEndpoints",
"ec2:CreateVpcEndpoint",
"ec2:ModifyVpcEndpoint",
"ec2:DeleteVpcEndpoints"
```

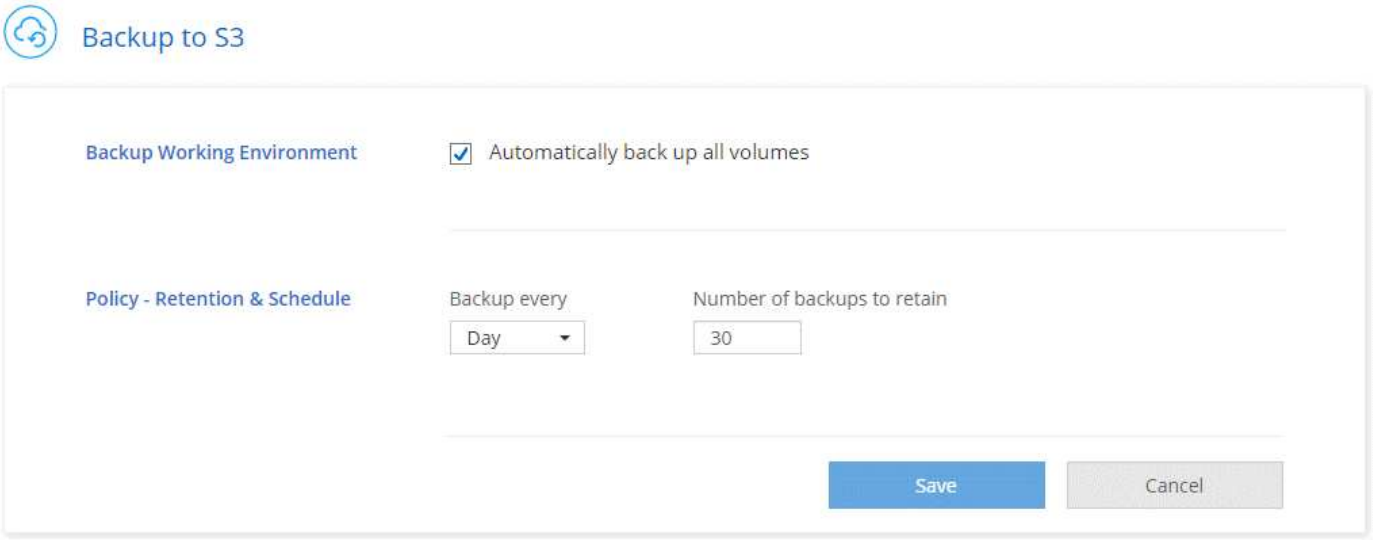
**Enable Backup to S3 on your new or existing system**

- New systems: The Backup to S3 feature is enabled by default in the working environment wizard. Be sure to keep the option enabled.
- Existing systems: Open the working environment, click the backup settings icon and enable backups.



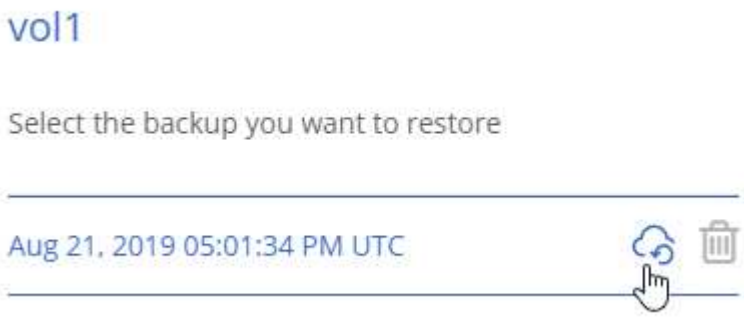

**If needed, modify the backup policy**

The default policy backs up volumes every day and retains 30 backup copies of each volume. If needed, you can change the number of backup copies to retain.




**Restore your data, as needed**

At the top of Cloud Manager, click **Backup & Restore**, select a volume, select a backup, and then restore data from the backup to a new volume.




## 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**

Backup to S3 is supported with Cloud Volume ONTAP 9.4 and later.

**Supported AWS regions**

Backup to S3 is supported with Cloud Volumes ONTAP in the following AWS regions:

- US East (N. Virginia)
- US West (Oregon)
- EU (Ireland)
- EU (Frankfurt)
- Asia Pacific (Sydney)

### AWS permissions required

The IAM role that provides Cloud Manager with permissions must include the following:

```
"ec2:DescribeVpcEndpoints",
"ec2:CreateVpcEndpoint",
"ec2:ModifyVpcEndpoint",
"ec2:DeleteVpcEndpoints"
```

### AWS subscription requirement

Starting with the 3.7.3 release, a new Cloud Manager subscription is available in the AWS Marketplace. This subscription enables deployments of Cloud Volumes ONTAP 9.6 and later PAYGO systems and the Backup to S3 feature. You need to subscribe to this new Cloud Manager subscription before you enable Backup to S3. Billing for the Backup to S3 feature is done through this subscription.

### Port requirements

- TCP port 5010 must be open for outbound traffic from Cloud Volumes ONTAP to the backup service.
- TCP port 8088 must be open for outbound traffic on the security group for Cloud Manager.

  These ports are already open if you used the predefined security groups. But if you used your own, then you'll need to open these ports.

### Outbound internet access

Ensure that the following endpoint is accessible from Cloud Manager:
https://w86yt021u5.execute-api.us-east-1.amazonaws.com/production/whitelist

Cloud Manager contacts this endpoint to add your AWS account ID to the list of allowed users for Backup to S3.

### Interface VPC endpoints

When you enable the Backup to S3 feature, Cloud Manager creates an interface VPC endpoint in the VPC where Cloud Volumes ONTAP is running. This *backup endpoint* connects to the NetApp VPC where Backup to S3 is running. If you restore a volume, Cloud Manager creates an additional interface VPC endpoint—the *restore endpoint*.

Any additional Cloud Volumes ONTAP systems in the VPC use these two VPC endpoints.

The default limit for interface VPC endpoints is 20 per VPC. Make sure that your VPC hasn't reached the limit before you enable the feature.

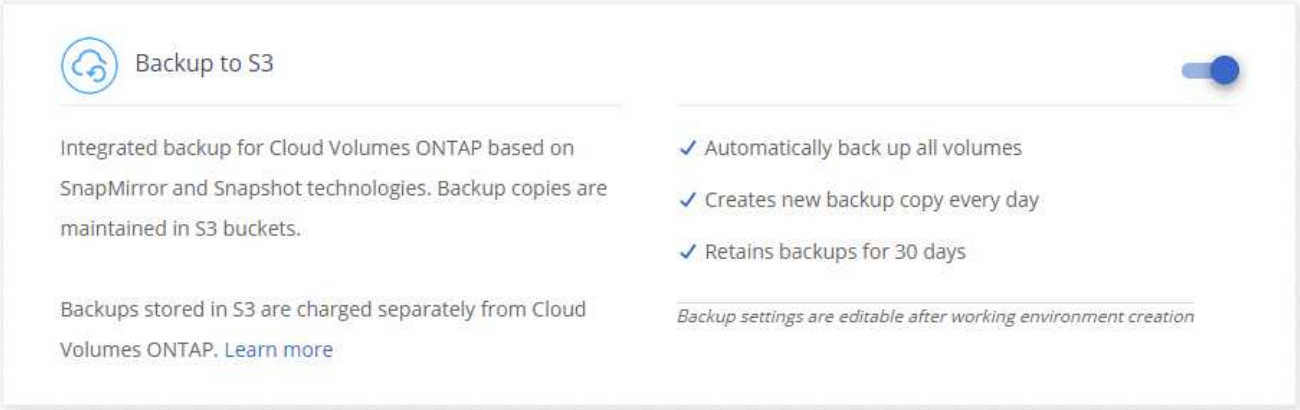
## Enabling backups to S3 on a new system

The Backup to S3 feature 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 Backup to S3 page, leave the feature enabled and click **Continue**.




5. Complete the pages in the wizard to deploy the system.

**Result**

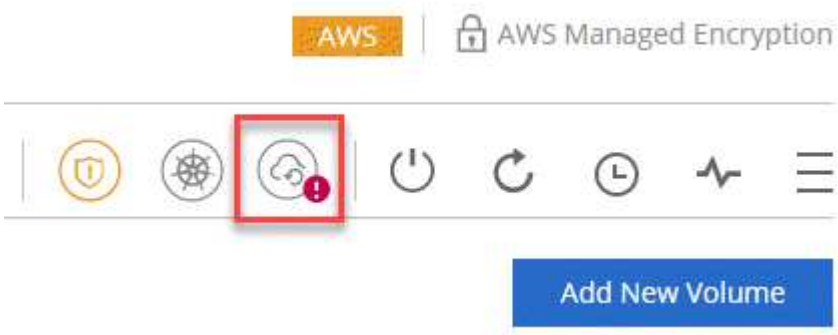
The Backup to S3 feature is enabled on the system and backs up volumes every day and retains 30 backup copies. Learn how to modify backup retention.

## Enabling backups to S3 on an existing system

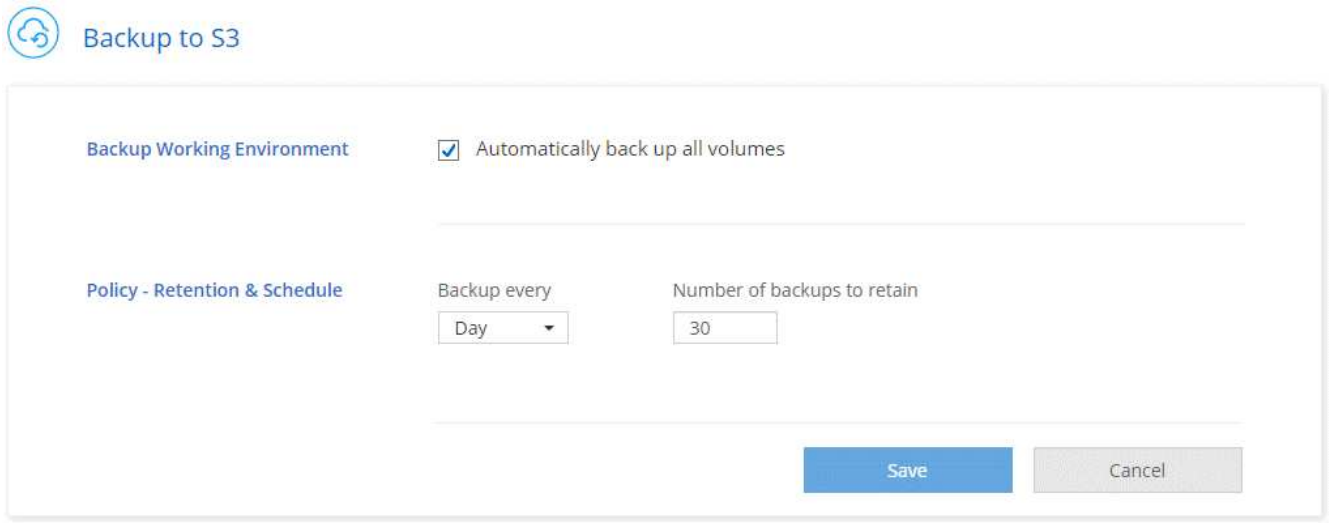
You can enable backups to S3 on an existing Cloud Volumes ONTAP system, as long as you are running a supported configuration. For details, see Requirements.

**Steps**

1. Open the working environment.
2. Click the backup settings icon.




3. Select **Automatically back up all volumes**.
4. Choose your backup retention and then click **Save**.




**Result**

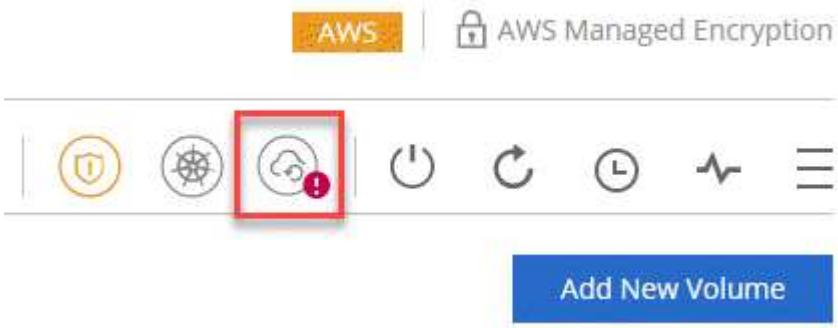
The Backup to S3 feature starts taking the initial backups of each volume.

## Changing the backup retention

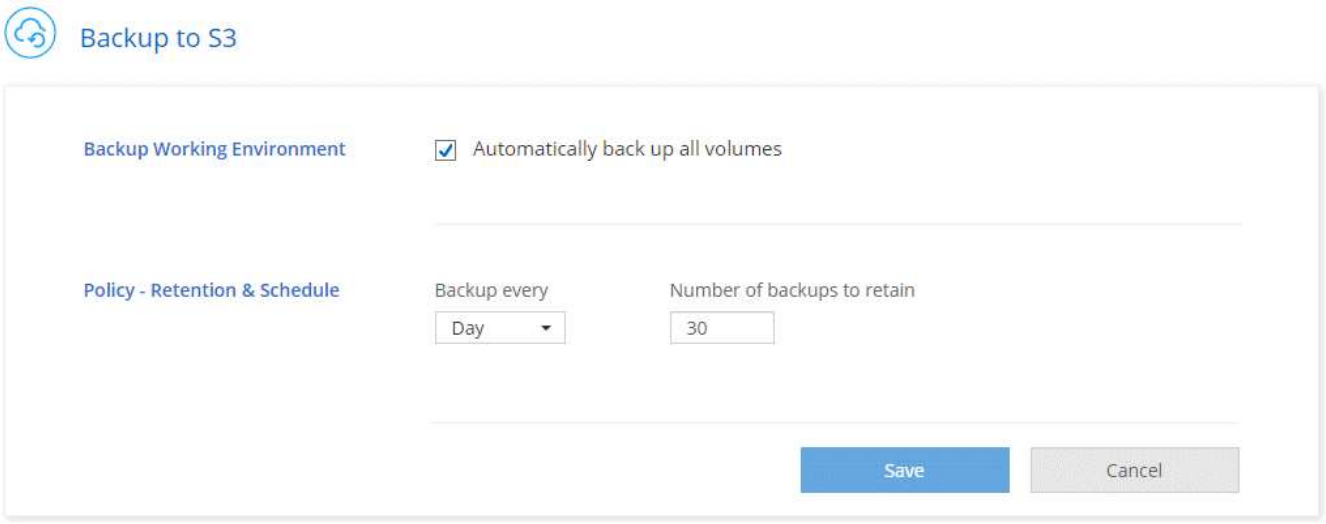
The default policy backs up volumes every day and retains 30 backup copies of each volume. You can change the number of backup copies to retain.

**Steps**

1. Open the working environment.
2. Click the backup settings icon.




3. Change the backup retention and then click **Save**.



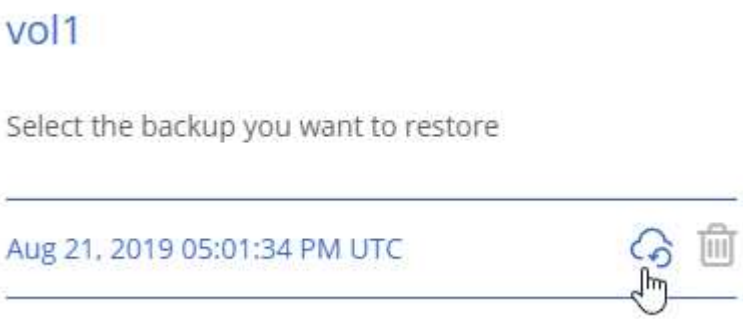

## Restoring a volume

When you restore data from a backup, Cloud Manager performs a full volume restore to a *new* volume. You can restore the data to the same working environment or to a different working environment.

### Steps

1. At the top of Cloud Manager, click **Backup & Restore**.
2. Select the volume that you want to restore.


3. Find the backup that you want to restore from and click the restore icon.



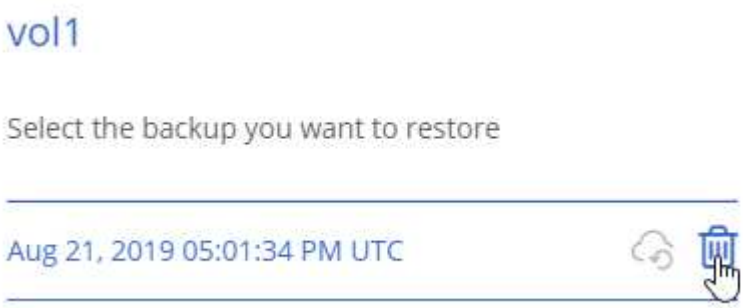

4. Select the working environment to which you want to restore the volume.
5. Enter a name for the volume.
6. Click **Restore**.

## Deleting backups

All backups are retained in S3 until you delete them from Cloud Manager. Backups are not deleted when you delete a volume or when you delete the Cloud Volumes ONTAP system.

**Steps**

1. At the top of Cloud Manager, click **Backup & Restore**.
2. Select a volume.
3. Find the backup that you want to delete and click the delete icon.



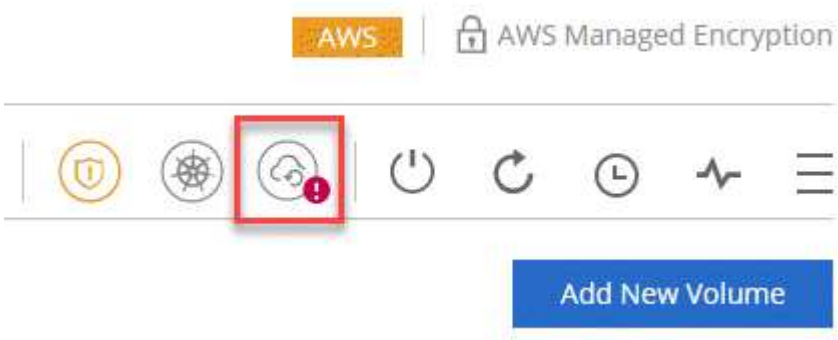

4. Confirm that you want to delete the backup.

## Disabling backups to S3

Disabling backups to S3 disables backups of each volume on the system. Any existing backups will not be deleted.

**Steps**

1. Open the working environment.
2. Click the backup settings icon.




3. Disable **Automatically back up all volumes** and then click **Save**.

## How Backup to S3 works

The following sections provide more information about the Backup to S3 feature.

### Where backups reside

Backup copies are stored in a NetApp-owned S3 bucket, in the same region where the Cloud Volumes ONTAP system is located.

### Backups are incremental

After the initial full backup of your data, all additional backups are incremental, which means that only changed blocks and new blocks are backed up.

### Backups are taken at midnight

Daily backups start just after midnight each day. 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 instances from other Cloud Manager systems.

### The backup policy is system wide

The number of backups to retain are defined at the system level. You can't set a different policy for each volume on the system.

### Security

Backup data is secured with AES-256 bit encryption at-rest and TLS 1.2 HTTPS connections in-flight.

Data travels across secured Direct Connect links to the service, and is protected at rest by AES 256-bit encryption. The encrypted data is then written to cloud using HTTPS TLS 1.2 connections. Data also travels to Amazon S3 only through secure VPC endpoint connections, so no traffic is sent across the internet.

Each user is assigned a tenant key, in addition to an overall encryption key owned by the service. This requirement is similar to needing a pair of keys to open a customer safe in a bank. All keys, as cloud credentials, are stored securely by the service and are restricted to only certain NetApp personnel responsible for maintaining the service.

### Limitations

- If you use any of the following instance types, a Cloud Volumes ONTAP system can back up a maximum of 20 volumes to S3:
  - m4.xlarge
  - m5.xlarge
  - r4.xlarge
  - r5.xlarge
- Volumes that you create outside of Cloud Manager aren't automatically backed up to S3.

  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 backup these volumes, you would need to disable Backup to S3 and then enable it again.

- When you restore data from a backup, Cloud Manager performs a full volume restore to a *new* volume. This new volume isn't automatically backed up to S3.

  If you want to backup volumes created from a restore operation, you would need to disable Backup to S3 and then enable it again.

- You can back up volumes that are 50 TB in size or less.
- Backup to S3 can maintain up to 245 total backups of a volume.
- WORM storage is not supported on a Cloud Volumes ONTAP system when backup to S3 is enabled.

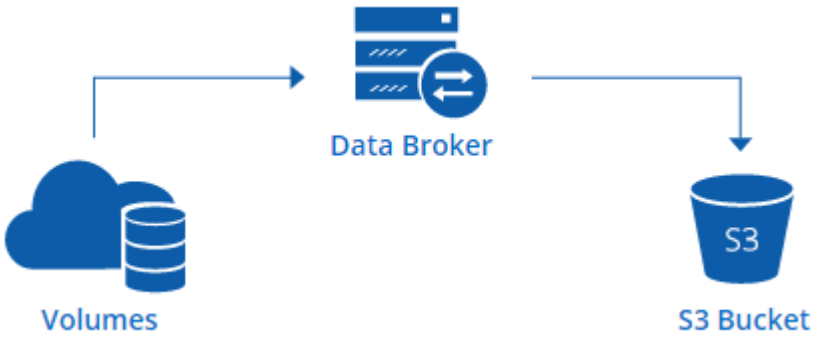
# Syncing data to Amazon S3

You can sync data from ONTAP volumes to an Amazon S3 bucket by integrating a working environment with NetApp Cloud Sync. You can then use the synced data as a secondary copy or for data processing using AWS services like EMR and Redshift.

## How the sync to S3 feature works

You can integrate a working environment with the Cloud Sync service at any time. When you integrate a working environment, the Cloud Sync service syncs data from the selected volumes to a single S3 bucket. The integration works with Cloud Volumes ONTAP working environments, as well as ONTAP clusters that are on-premises or part of a NetApp Private Storage (NPS) configuration.

To sync the data, the service launches a data broker instance in your VPC. Cloud Sync uses one data broker per working environment to sync data from volumes to an S3 bucket. After the initial sync, the service syncs any changed data once per day at midnight.




If you want to perform advanced Cloud Sync actions, go directly to the Cloud Sync service. From there, you can perform actions such as syncing from S3 to an NFS server, choosing different S3 buckets for volumes, and modifying schedules.

### 14-day free trial

If you are a new Cloud Sync user, your first 14 days are free. After the free trial ends, you must pay for each *sync relationship* at an hourly rate or by purchasing licenses. Each volume that you sync to an S3 bucket is considered a sync relationship. You can set up both payment options directly from Cloud Sync in the License

Settings page.

### How to get help

Use the following options for any support related to the Cloud Manager sync to S3 feature or for Cloud Sync in general:

- General product feedback: ng-cloudsync-contact@netapp.com
- Technical Support options:
  - NetApp Cloud Sync Communities
  - In-product chat (lower-right corner of Cloud Manager)

## Integrating a working environment with the Cloud Sync service

If you want to sync volumes to Amazon S3 directly from Cloud Manager, then you must integrate the working environment with the Cloud Sync service.

[] | *https://img.youtube.com/vi/3hOtLs70_xE/maxresdefault.jpg*

### Steps

1. Open a working environment and click **Sync to S3**.
2. Click **Sync** and follow the prompts to sync your data to S3.

You cannot sync data protection volumes to S3. The volumes must be writable.

## Managing volume sync relationships

After you integrate a working environment with the Cloud Sync service, you can sync additional volumes, stop syncing a volume, and remove the integration with Cloud Sync.

### Steps

1. On the Working Environments page, double-click the working environment on which you want to manage sync relationships.
2. If you want to enable or disable sync to S3 for a volume, select the volume and then click **Sync to S3** or **Delete Sync Relationship**.
3. If you want to delete all sync relationships for a working environment, click the **Sync to S3** tab and then click **Delete Sync**.

   This action does not delete synced data from the S3 bucket. If the data broker is not being used in any other sync relationships, then the Cloud Sync service deletes the data broker.

# Gain insight into data privacy

## Learn about Cloud Compliance

Cloud Compliance is a data privacy and compliance service for Cloud Volumes ONTAP in AWS and Azure. Using Artificial Intelligence (AI) driven technology, Cloud Compliance helps organizations understand data context and identify sensitive data across Cloud Volumes ONTAP systems.

Cloud Compliance is currently available as a Controlled Availability release.

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)

### Cost

Cloud Compliance is an add-on service for Cloud Volumes ONTAP provided by NetApp at no extra cost. Activating Cloud Compliance requires deploying a cloud instance, which you will be charged for by your cloud provider. There are no charges for data ingress or egress because data doesn't flow outside of the network.

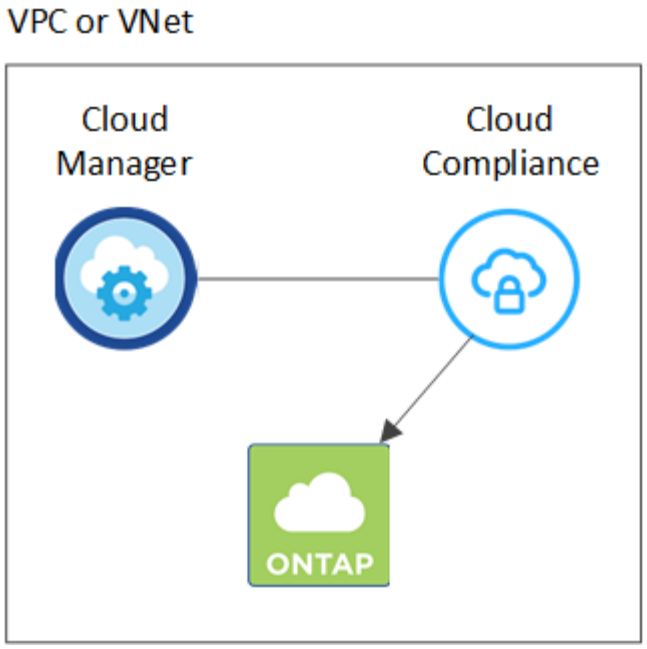
### How Cloud Compliance works

At a high-level, Cloud Compliance works like this:

1. You enable Cloud Compliance on one or more Cloud Volumes ONTAP systems.
2. Cloud Compliance scans the data using an AI learning process.
3. In Cloud Manager, you click **Compliance** and use the provided dashboard and reporting tools to help you in your compliance efforts.

### The Cloud Compliance instance

When you enable Cloud Compliance on one or more Cloud Volumes ONTAP systems, Cloud Manager deploys a Cloud Compliance instance in the same VPC or VNet as the first Cloud Volumes ONTAP system in the request.




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 io1 disk.

  In regions where m5.4xlarge isn't available, Cloud Compliance runs on an m4.4xlarge instance instead.

- 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 Cloud Manager system.
- Upgrades of Cloud Compliance software is automated—you don't need to worry about it.

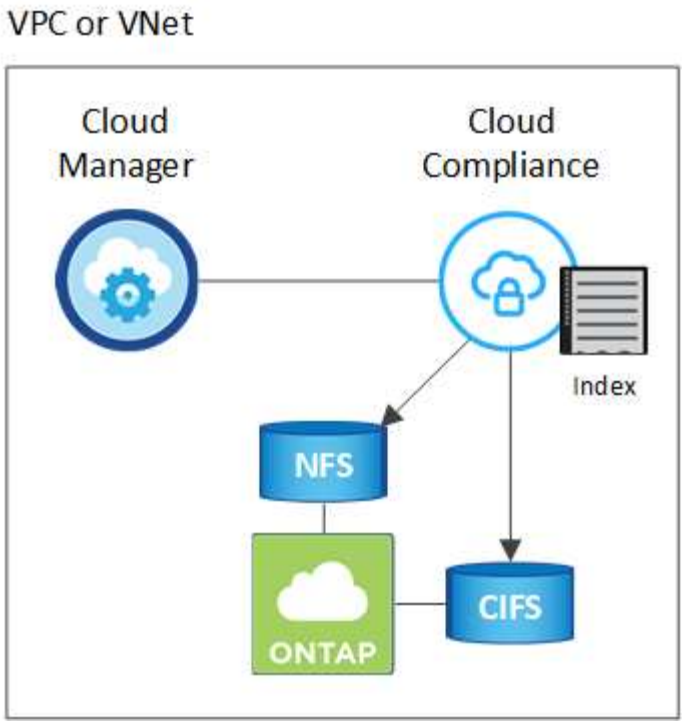
The instance should remain running at all times because Cloud Compliance continuously scans the data on Cloud Volumes ONTAP systems.

## How scans work

After you enable Cloud Compliance, it immediately starts scanning your data to identify personal and sensitive data.

Cloud Compliance connects to Cloud Volumes ONTAP 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.

Cloud Compliance scans the unstructured data on each volume for a range of personal information. 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, and data categories.




After the initial scan, Cloud Compliance continuously scans each volume to detect incremental changes (this is why it's important to keep the instance running).

You can turn scans on and off at the working environment level, but not at the volume level. Learn how.

## Information that Cloud Compliance indexes

Cloud Compliance collects, indexes, and assigns categories to unstructured 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.

**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 private IP address and a security group that enables inbound HTTP connections from Cloud Manager. This connection enables you to access the Cloud Compliance dashboard from the Cloud Manager interface.

Outbound rules are completely open. The instance connects to Cloud Volumes ONTAP systems and to the internet through a proxy from Cloud Manager. Internet access is needed to upgrade the Cloud Compliance software and to send usage metrics.

If you have strict networking requirements, learn about the endpoints that Cloud Compliance contacts.

The indexed data never leaves the Cloud Compliance instance—the data isn't relayed outside of your virtual network and it isn't sent to Cloud Manager.

### User access to compliance information

Cloud Manager Admins can view compliance information for all working environments.

Workspace Admins can 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.

Learn more about Cloud Manager roles.

# Getting started with Cloud Compliance for Cloud Volumes ONTAP

Complete a few steps to get started with Cloud Compliance for Cloud Volumes ONTAP in AWS or Azure.

### Quick start

Get started quickly by following these steps or scroll down to the remaining sections for full details.

**Verify that your configuration can meet the requirements**

- Ensure that the Cloud Compliance instance will have outbound internet access.

  Cloud Manager deploys the instance in the same VPC or VNet as the first Cloud Volumes ONTAP system in the request.

- Ensure that users can access the Cloud Manager interface from a host that has a direct connection to AWS or Azure, or from a host that's inside the same network as the Cloud Compliance instance (the instance will have a private IP address).
- Ensure that you can keep the Cloud Compliance instance running.

**Enable Cloud Compliance on Cloud Volumes ONTAP**

- New working environments: Be sure to keep Cloud Compliance enabled when you create the working environment (it's enabled by default).
- Existing working environments: Click **Compliance**, optionally edit the list of working environments, and click **Show Compliance Dashboard**.

**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.
- 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** > **CIFS Scan Status** > **Edit CIFS Credentials** and provide the credentials. The credentials can be read-only, but providing admin credentials ensures that Cloud Compliance can read data that requires elevated permissions.

**Ensure connectivity between Cloud Manager and Cloud Compliance**

- The security group for Cloud Manager must allow inbound and outbound traffic over port 80 to and from the Cloud Compliance instance.
- If your AWS network doesn't use a NAT or proxy for internet access, then the security group for Cloud Manager must allow inbound traffic over TCP port 3128 from the Cloud Compliance instance.

## Reviewing prerequisites

Review the following prerequisites to make sure that you have a supported configuration before you enable Cloud Compliance. You'll need to ensure connectivity between components after you enable Cloud Compliance. That's covered below.

### Enable outbound internet access

Cloud Compliance requires outbound internet access. If your virtual network uses a proxy server for internet access, ensure that the Cloud Compliance instance has outbound internet access to contact the following endpoints:

| Endpoints | Purpose |
|---|---|
| https://cloudmanager.cloud.netapp.com | Communication with the Cloud Manager service, which includes Cloud Central accounts. |
| https://netapp-cloud-account.auth0.com | Communication with NetApp Cloud Central for centralized user authentication. |

| Endpoints | Purpose |
| --- | --- |
| https://cloud-compliance-support-netapp.s3.us-west-1.amazonaws.com<br>https://hub.docker.com | Provides access to software images, manifests, and templates. |
| https://kinesis.us-east-1.amazonaws.com | Enables NetApp to stream data from audit records. |
| https://cognito-idp.us-east-1.amazonaws.com<br>https://cognito-identity.us-east-1.amazonaws.com | Enables Cloud Compliance to access and download manifests and templates, and to send logs and metrics. |

**Verify web browser connectivity to Cloud Compliance**

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.

If you're accessing Cloud Manager from a public IP address, then your web browser probably isn't running on a host inside the network.

**Keep Cloud Compliance running**

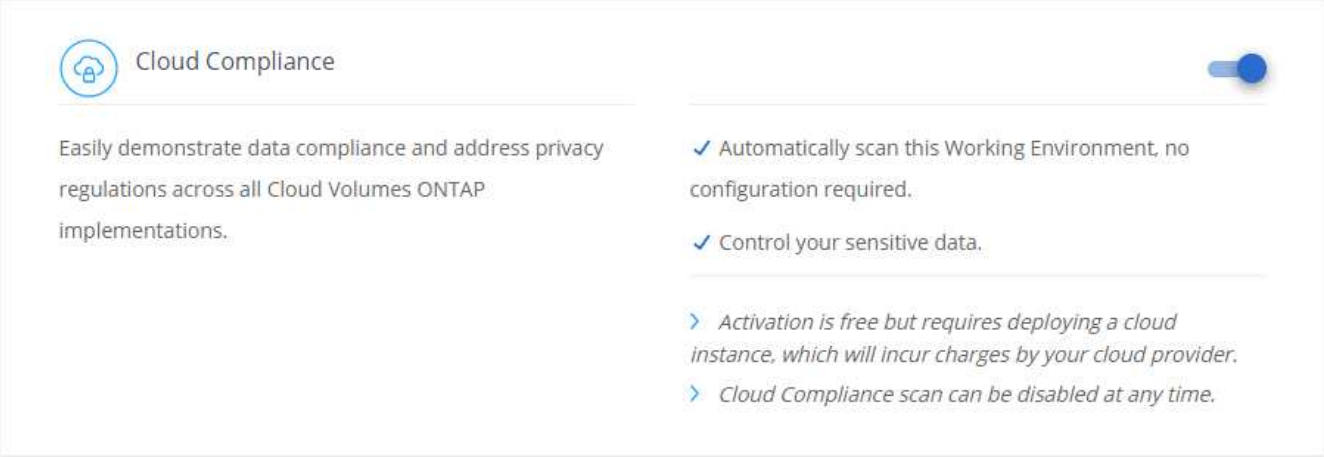
The Cloud Compliance instance needs to stay on to continuously scan your data.

## Enabling Cloud Compliance on a new working environment

Cloud Compliance 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 Cloud Compliance enabled and click **Continue**.




5. Complete the pages in the wizard to deploy the system.

For help, see Launching Cloud Volumes ONTAP in AWS and Launching Cloud Volumes ONTAP in Azure.

**Result**

Cloud Compliance is enabled on the Cloud Volumes ONTAP system. If this the first time that you enabled Cloud Compliance, Cloud Manager deploys the Cloud Compliance instance in your cloud provider. As soon as the instance is available, it starts scanning data as its written to each volume that you create.

## Enabling Cloud Compliance on existing working environments

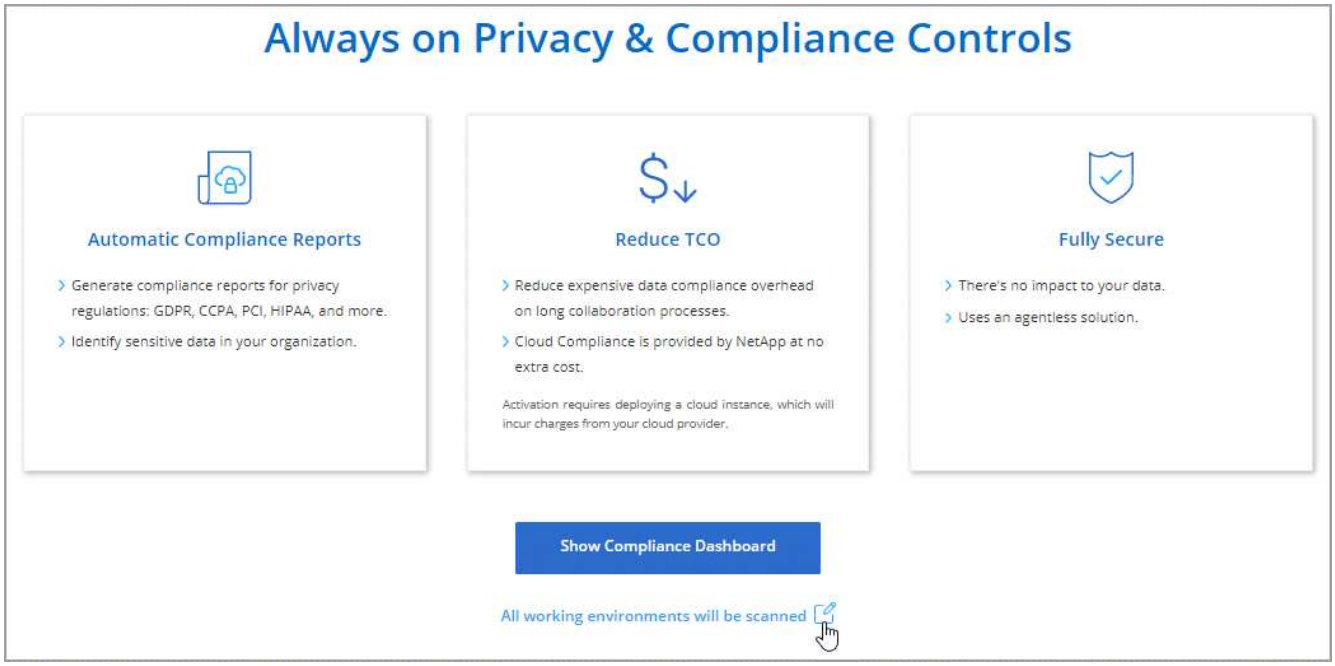
Enable Cloud Compliance on your existing Cloud Volumes ONTAP systems from the **Compliance** tab in Cloud Manager.

Another option is to enable Cloud Compliance from the **Working Environments** tab by selecting each working environment individually. That'll take you longer to complete, unless you have just one system.

**Steps for multiple working environments**

1. At the top of Cloud Manager, click **Compliance**.
2. If you want to enable Cloud Compliance on specific working environments, click the edit icon.

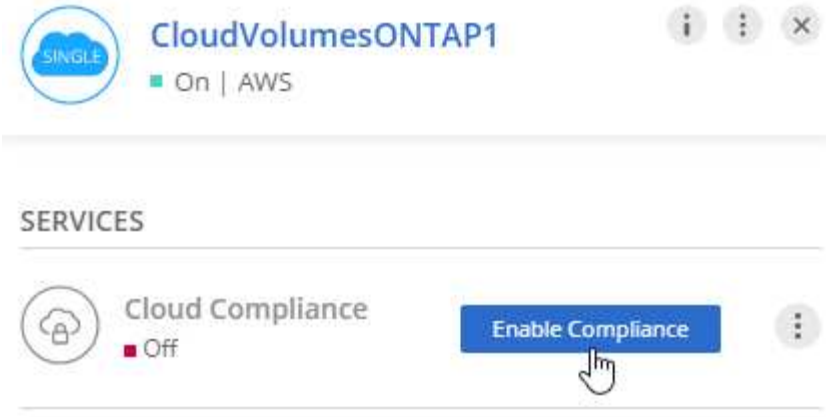
   Otherwise, Cloud Manager is set to enable Cloud Compliance on all working environments to which you have access.




3. Click **Show Compliance Dashboard**.

**Steps for a single working environment**

1. At the top of Cloud Manager, click **Working Environments**.
2. Select a working environment.
3. In the pane on the right, click **Enable Compliance**.




**Result**

If this the first time that you enabled Cloud Compliance, Cloud Manager deploys the Cloud Compliance instance in your cloud provider.

Cloud Compliance starts scanning the data on each working environment. Data 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 on Cloud Volumes ONTAP 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**

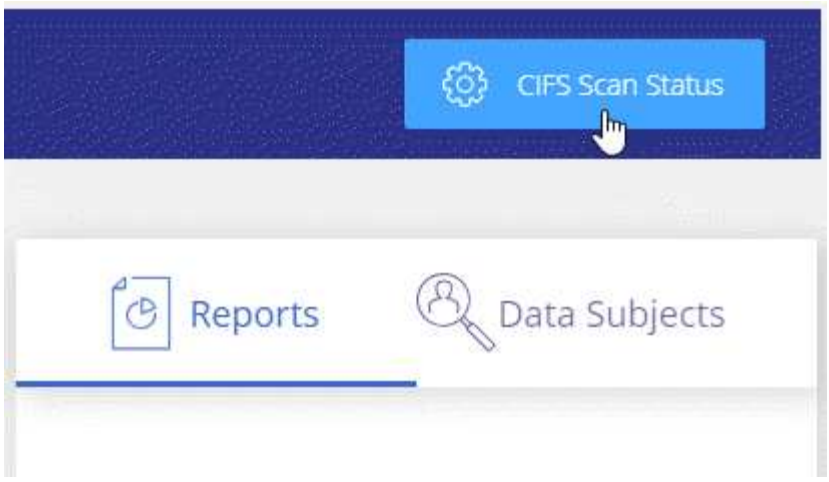
1. Make sure that there's a network connection between the Cloud Compliance instance and each Cloud Volumes ONTAP subnet.

   Cloud Manager deploys the Cloud Compliance instance in the same VPC or VNet as the first Cloud Volumes ONTAP system in the request. So this step is important if some Cloud Volumes ONTAP systems are in different subnets or virtual networks.

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. In the top right, click **CIFS Scan Status**.




c. For each Cloud Volumes ONTAP system, 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.


## Verifying that Cloud Manager can access Cloud Compliance

Ensure connectivity between Cloud Manager and Cloud Compliance so you can view the compliance insights that Cloud Compliance found.

**Steps**

1. Make sure that the security group for Cloud Manager allows inbound and outbound traffic over port 80 to and from the Cloud Compliance instance.

   This connection enables you to view information in the Compliance tab.

2. If your AWS network doesn't use a NAT or proxy for internet access, modify the security group for Cloud Manager to allow inbound traffic over TCP port 3128 from the Cloud Compliance instance.

   This is required because the Cloud Compliance instance uses Cloud Manager as a proxy to access the internet.

   This port is open by default on all new Cloud Manager instances, starting with version 3.7.5. It's not open on Cloud Manager instances created prior to that version.

# Gaining visibility and control of private data

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.

## Personal data

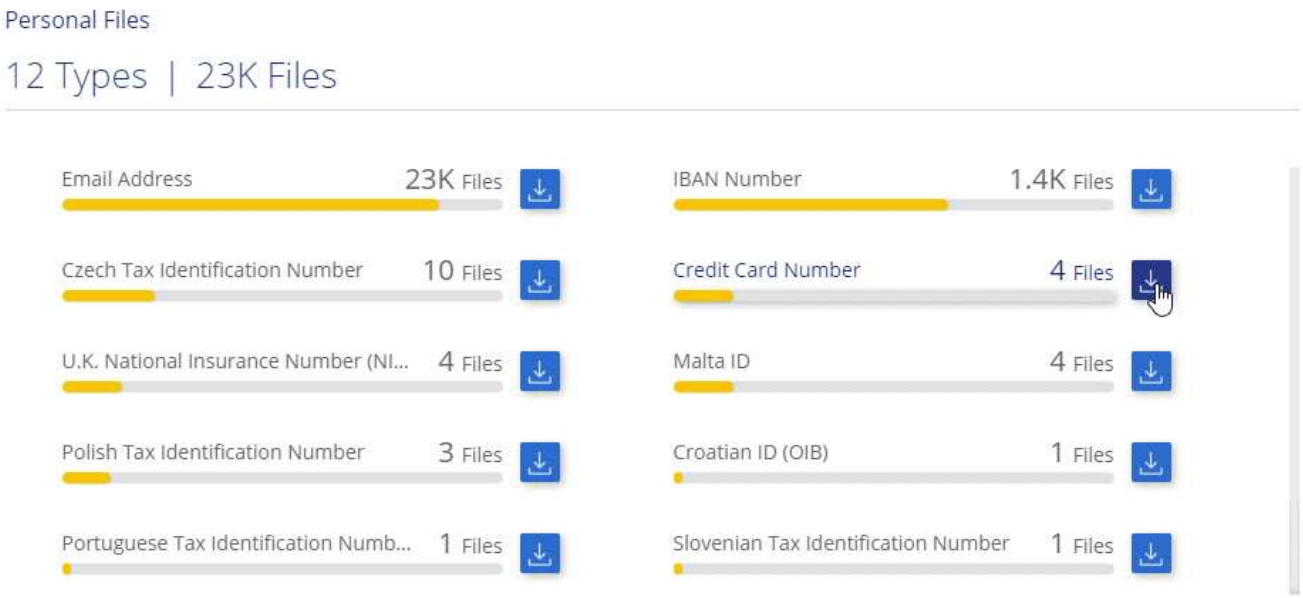
Cloud Compliance automatically identifies specific words, strings, and patterns (Regex) inside the data. For example, Personal Identification Information (PII), credit card numbers, social security numbers, bank account numbers, and more. See the full list.

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 list below shows when Cloud Compliance uses proximity validation.

### Viewing files that contain personal data

#### Steps

1. At the top of Cloud Manager, click **Compliance**.
2. Download the details for one of the top 2 file types directly from the main screen, or click **View All** and then download the list for any of the personal data types that were found.




### 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.

| Type | Identifier | Proximity validation? |
|---|---|---|
| General | Email address | No |
| | Credit card number | No |
| | IBAN number (International Bank Account Number) | No |
| | IP address | Yes |
| National Identifiers | Belgian ID (Numero National) | Yes |
| | Bulgarian ID (Unified Civil Number) | Yes |
| | Cyprus Tax Identification Number (TIC) | Yes |
| | Danish Tax Identification Number (CPR) | Yes |
| | Estonian ID (Isikukood) | Yes |
| | Finnish ID (henkilötunnus) | Yes |
| | French Tax Identification Number (SPI) | Yes |
| | German Tax Identification Number (Steuerliche Identifikationsnummer) | Yes |
| | Hungarian Tax Identification Number (Adóazonosító jel) | Yes |
| | Irish ID (PPS) | Yes |
| | Israeli ID | Yes |
| | Italian ID (Codice Fiscale) | Yes |
| | Latvian Tax Identification Number | Yes |
| | Lithuanian ID (Asmens kodas) | Yes |
| | Luxembourg ID | Yes |
| | Malta ID | Yes |
| | Netherlands ID (BSN) | Yes |
| | Polish Tax Identification Number | Yes |
| | Portuguese Tax Identification Number (NIF) | Yes |
| | Romanian Tax Identification Number | Yes |
| | Slovakian Tax Identification Number | Yes |
| | Slovenian Tax Identification Number | Yes |
| | South African ID | Yes |
| | Spanish Tax Identification Number | Yes |
| | Swedish Tax Identification Number | Yes |
| | U.K. National Insurance Number (NINO) | Yes |
| | USA Social Security Number (SSN) | Yes |

## 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.

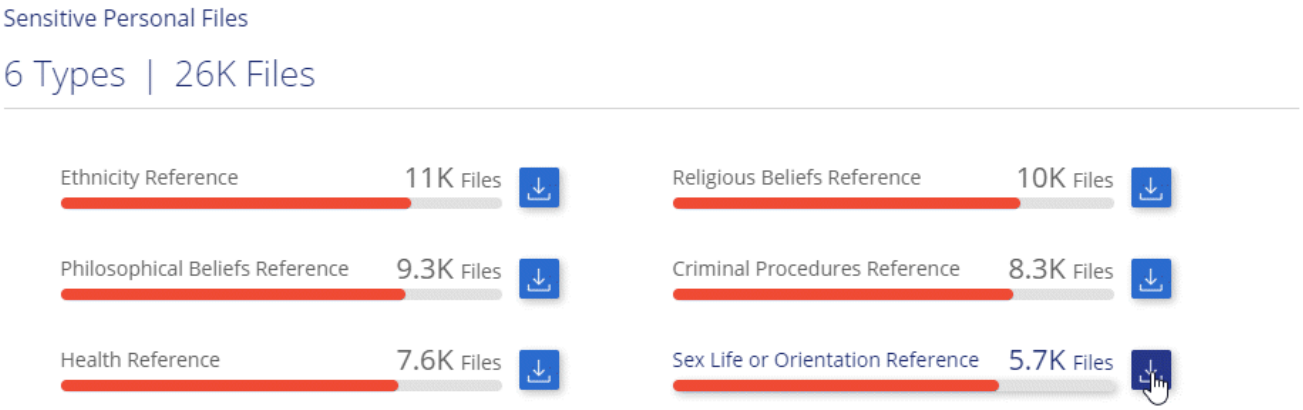
For example, one sensitive GDPR data category is ethnic origin. Because of its NLP abilities, Cloud Compliance can distinguish the difference between a sentence that reads "George is Mexican" (indicating sensitive data as specified in article 9 of the GDPR), versus "George is eating Mexican food."

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. Download the details for one of the top 2 file types directly from the main screen, or click **View All** and then download the list for any of the sensitive personal data types that were found.




### 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.

**Philosophical Beliefs Reference**

Data concerning a natural person's philosophical beliefs.

**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.

## 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.

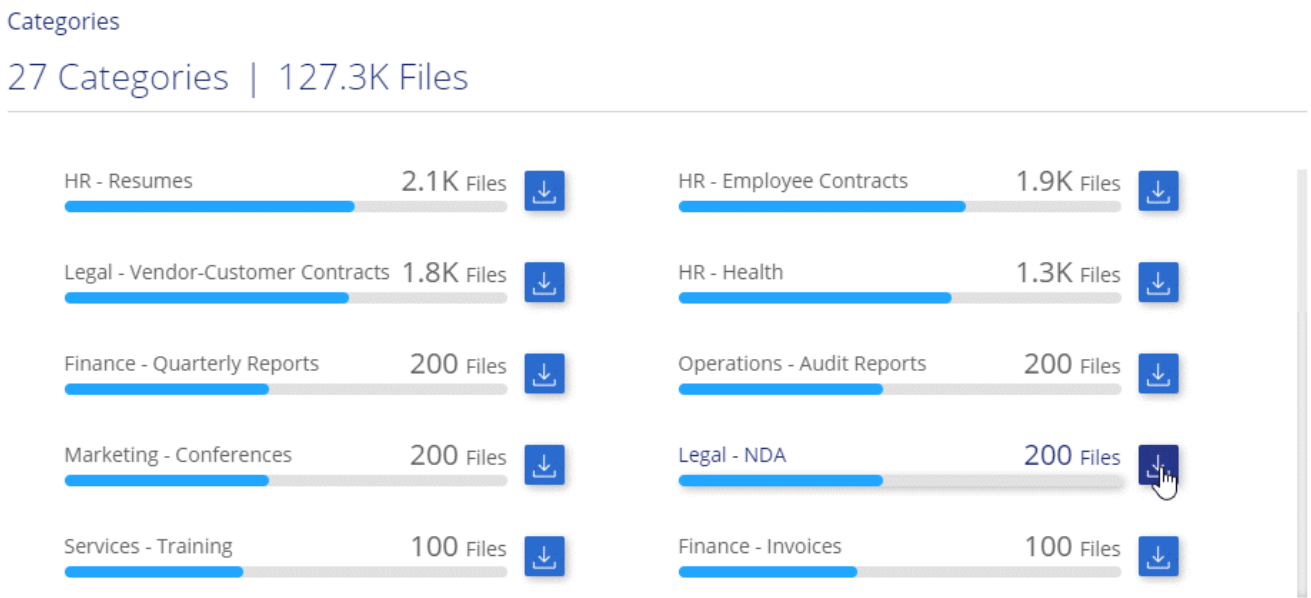
Categories can help you understand what's happening with your data by showing you the type of information that you have. For example, a category like resumes or employee contracts can include sensitive data. When you download the CSV report, you might find that employee contracts are stored in an unsecure 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. Download the details for one of the top 4 file types directly from the main screen, or click **View All** and then download the list for any of the categories.




### Types of categories

Cloud Compliance categorizes your data as follows:

**Finance**

- Balance Sheets
- Purchase Orders
- Invoices
- Quarterly Reports

**HR**

- Background Check
- Compensation Plans
- Employee Contracts
- Employee Review
- Health
- Resumes

**Legal**

- NDA
- Vendor-Customer contracts

**Marketing**

- Campaigns
- Conferences

**Operations**

- Audit Reports

**Sales**

- Sales Orders

**Services**

- RFI
- RFP
- Training

**Support**

- Complaints and Tickets

**Other**

- Archive Files
- Audio
- CAD Files
- Code
- Executables
- Images

## File types

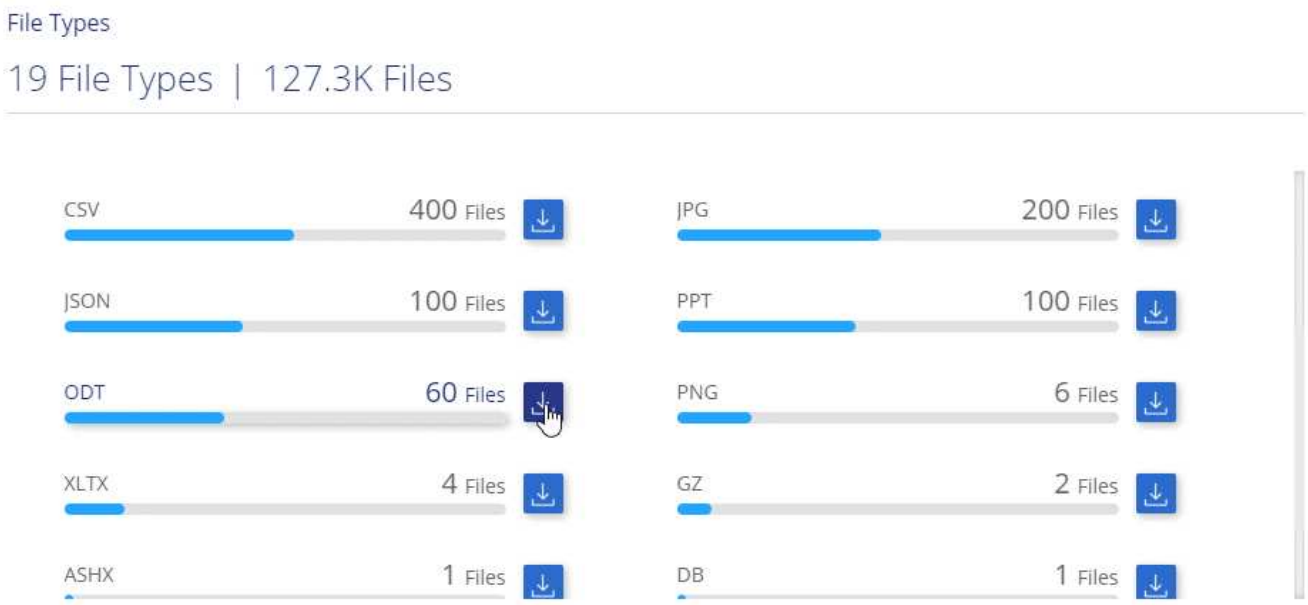
Cloud Compliance takes the data that it scanned and breaks it down by file type. Cloud Compliance can display all file types found in the scans.

Reviewing your file types can help you control your sensitive data because you might find that certain file types are not stored correctly. 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. Download the details for one of the top 4 file types directly from the main screen, or click **View All** and then download the list for any of the file types.




## 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% |

### What's included in each file list report (CSV file)

The dashboard enables you 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 (support for more will be added later).

Each file list includes the following information:

- File name
- Location type
- Location
- File path
- File type
- 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. The files only appear in the CSV reports.

# Viewing the 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.

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.

The report includes the following information:

**Compliance status**

A severity score (see below for more details) 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**

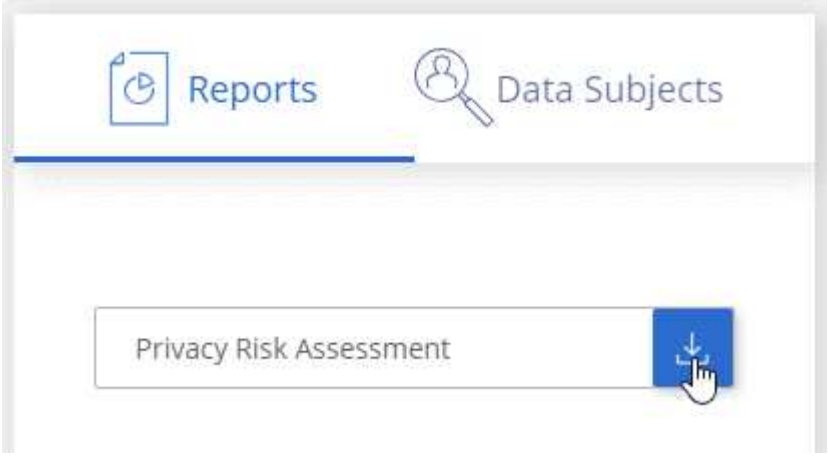
The number of people by location for which national identifiers were found.

## 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% |

| Severity score | Logic |
|---|---|
| 4 | Three of the variables are larger than 3% |
| 5 | One of the variables are larger 6% |
| 6 | Two of the variables are larger 6% |
| 7 | Three of the variables are larger 6% |
| 8 | One of the variables are larger 15% |
| 9 | Two of the variables are larger 15% |
| 10 | Three of the variables are larger 15% |

# 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 that has 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 or 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.

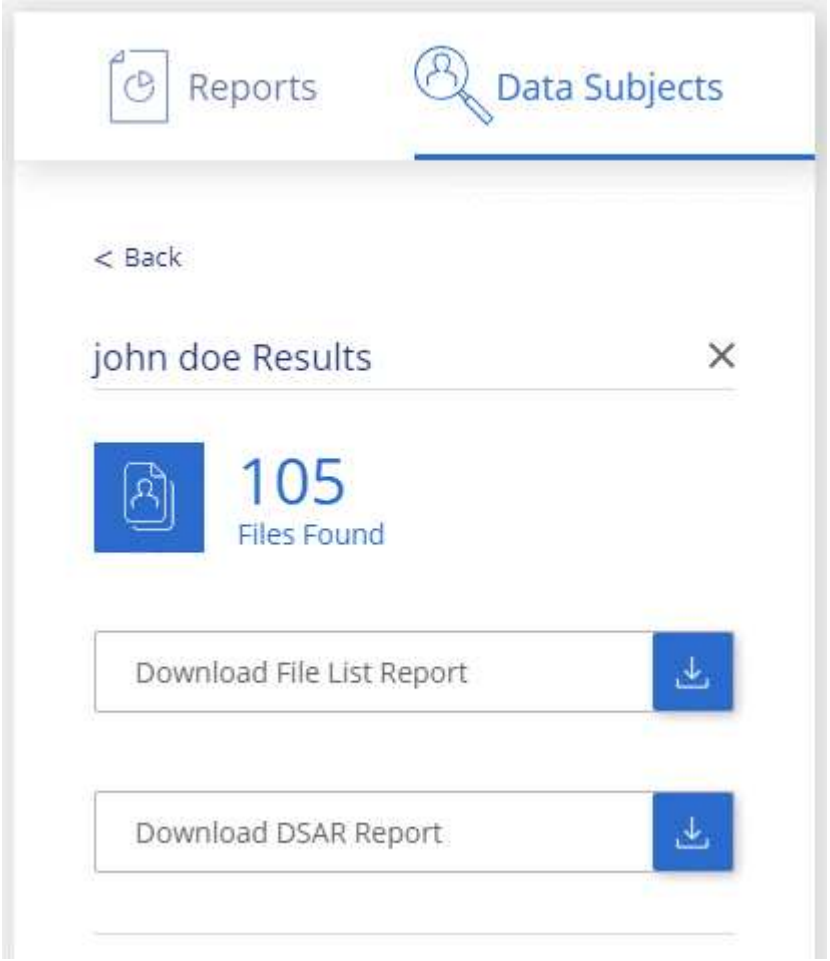
Only English is supported when searching for the names of data subjects. Support for more languages will be added later.

**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*:




4. Choose one of the available options:
   - **Download File List Report**: A list of the files that contain information on the data subject.

     If there are more than 10,000 results, only the top 10,000 appear in the report (support for more will be added later).

   - **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.

# Disabling Cloud Compliance

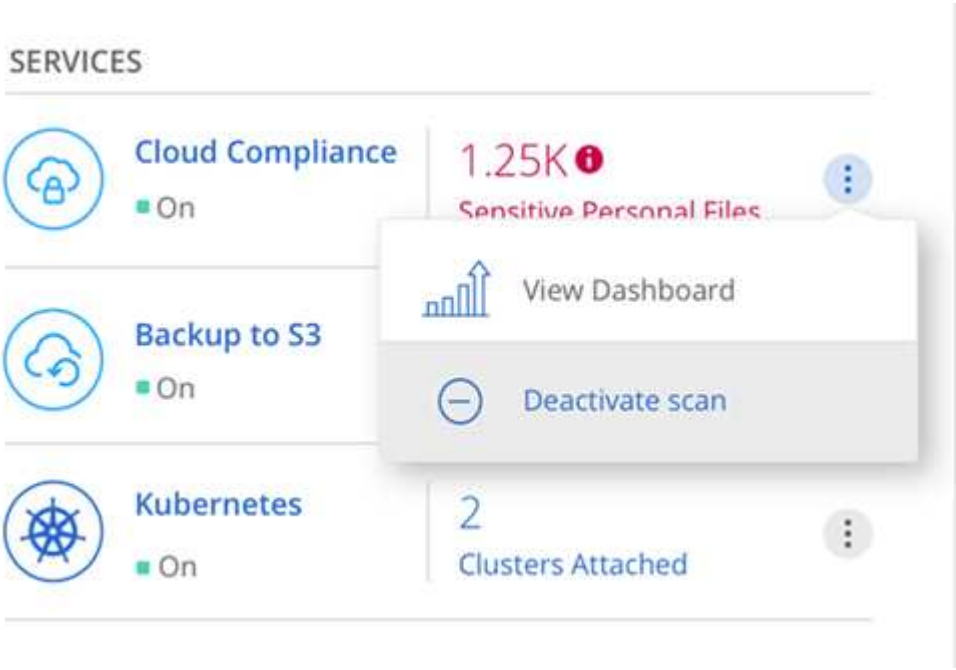
If you need to, you can stop Cloud Compliance from scanning one or more working environments. You can also delete the Cloud Compliance instance if you no longer want to use Cloud Compliance with your Cloud Volumes ONTAP systems.

## Deactivating compliance scans for a working environment

When you deactivate scans, Cloud Compliance no longer scans the data on the system and it removes the indexed compliance insights from the Cloud Compliance instance (the data from the working environment itself isn't deleted).

**Steps**

1. At the top of Cloud Manager, click **Working Environments**.
2. Select the working environment.
3. In the right panel, click the action icon for the Cloud Compliance service and select **Deactivate scan**.




## Deleting the Cloud Compliance instance

You can delete the Cloud Compliance instance if you no longer want to use Cloud Compliance with Cloud Volumes ONTAP. Deleting the instance also deletes the associated disks where the indexed data resides.

**Step**

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 new NetApp cloud offering. Using Artificial Intelligence (AI) driven technology, Cloud Compliance helps organizations understand data context and identify sensitive data across your Cloud

Volumes ONTAP systems hosted in AWS or Azure.

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, 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, 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. Currently Cloud Compliance scans data managed by Cloud Volumes ONTAP.

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 Cloud Volumes ONTAP instances. It then scans the data on Cloud Volumes ONTAP and indexes the data insights found.

Learn more about how Cloud Compliance works.

## How much does Cloud Compliance cost?

Cloud Compliance is offered as part of Cloud Volumes ONTAP and doesn't require any additional costs.

Additional costs might be required in the future for customized capabilities.

Cloud Compliance requires deployment of an instance in your cloud provider, for which you'll be charged by your cloud provider.

## 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.

**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 io1 disk.

  In regions where m5.4xlarge isn't available, Cloud Compliance runs on an m4.4xlarge instance instead.

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.

## How do I enable Cloud Compliance?

You can enable Cloud Compliance when you create a new working environment. You can enable it on existing working environments from the **Compliance** tab (on first activation only) 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 Working Environments 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-premise ONTAP storage?

No. Cloud Compliance is currently available as part of Cloud Manager and supports Cloud Volumes ONTAP. We're planning to support Cloud Compliance with additional cloud offerings such as Cloud Volumes Service and Azure NetApp Files.

## Can Cloud Compliance send notifications to my organization?

No, but you can download status reports that you can share internally in your organization.

## Can I customize the service to my organization's need?

Cloud Compliance provides out-of-the-box insights to your data. These insights can be extracted and used for your organization's needs.

## 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.

Learn more.

# Administer Cloud Volumes ONTAP

## 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 OnCommand System Manager

You might need to perform some Cloud Volumes ONTAP tasks from OnCommand 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

1. From the Working Environments page, double-click the Cloud Volumes ONTAP system that you want to manage with System Manager.
2. Click the menu icon, and then click **Advanced > System Manager**.
3. Click **Launch**.

   System Manager loads in a new browser tab.

4. 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.

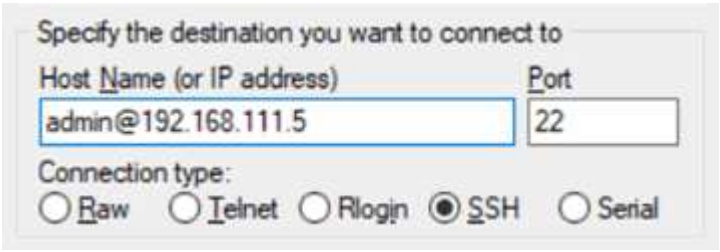
When deployed in multiple AZs, Cloud Volumes ONTAP HA configurations use a floating IP address for the cluster management interface, which means external routing is not available. You must connect from a host that is part of the same routing domain.

#### Steps

1. In Cloud Manager, identify the IP address of the cluster management interface:
   a. On the Working Environments page, select the Cloud Volumes ONTAP system.
   b. Copy the cluster management IP address that appears in the right pane.
2. Use SSH to connect to the cluster management interface IP address using the admin account.

   **Example**

   The following image shows an example using PuTTY:




3. At the login prompt, enter the password for the admin account.

   **Example**

```
Password: ********
COT2::>
```

# Updating Cloud Volumes ONTAP software

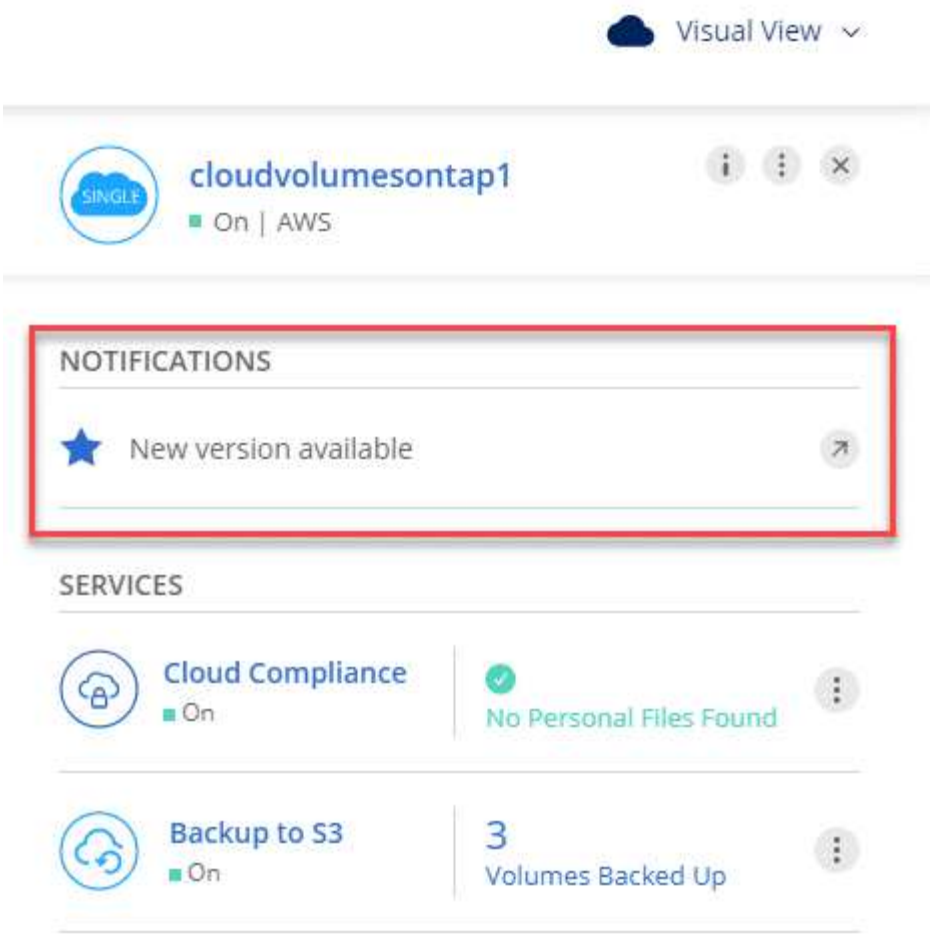
Cloud Manager includes several options that you can use to upgrade to the current Cloud Volumes ONTAP release or to downgrade Cloud Volumes ONTAP to an earlier release. You should prepare Cloud Volumes ONTAP systems before you upgrade or downgrade the software.

## Software updates 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.

## Ways to update Cloud Volumes ONTAP

Cloud Manager displays a notification in Cloud Volumes ONTAP working environments when a new version of Cloud Volumes ONTAP is available:




You can start the upgrade process from this notification, which automates the process by obtaining the software image from an S3 bucket, installing the image, and then restarting the system. 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.

**Advanced options for software updates**

Cloud Manager also provides the following advanced options for updating Cloud Volumes ONTAP software:

- Software updates using an image on an external URL

  This option is helpful if Cloud Manager cannot access the S3 bucket to upgrade the software, if you were provided with a patch, or if you want to downgrade the software to a specific version.

  For details, see Upgrading or downgrading Cloud Volumes ONTAP by using an HTTP or FTP server.

- Software updates using the alternate image on the system

  You can use this option to downgrade to the previous version by making the alternate software image the default image. This option is not available for HA pairs.

  For details, see Downgrading Cloud Volumes ONTAP by using a local image.

# Preparing to update Cloud Volumes ONTAP software

Before performing an upgrade or downgrade, you must verify that your systems are ready and make any required configuration changes.

- Planning for downtime
- Reviewing version requirements
- Verifying that automatic giveback is still enabled
- Suspending SnapMirror transfers
- Verifying that aggregates are online

### 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.

### Reviewing version requirements

The version of ONTAP that you can upgrade or downgrade to varies based on the version of ONTAP currently running on your system.

To understand version requirements, refer to ONTAP 9 Documentation: Cluster update requirements.

### 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

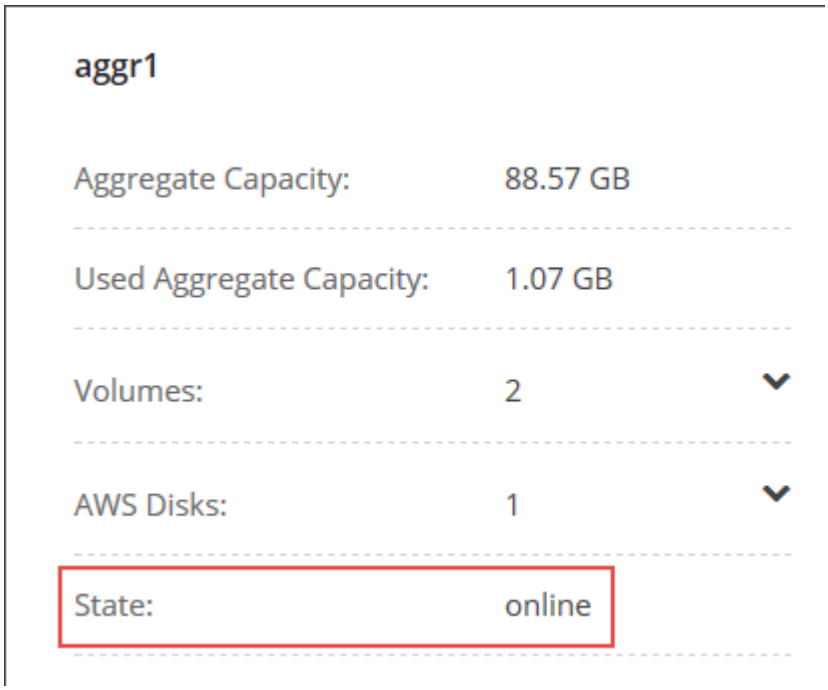
Aggregates for Cloud Volumes ONTAP must be online before you update the software. Aggregates should be online in most configurations, but if they are not, then you should bring them online.

**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.




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.

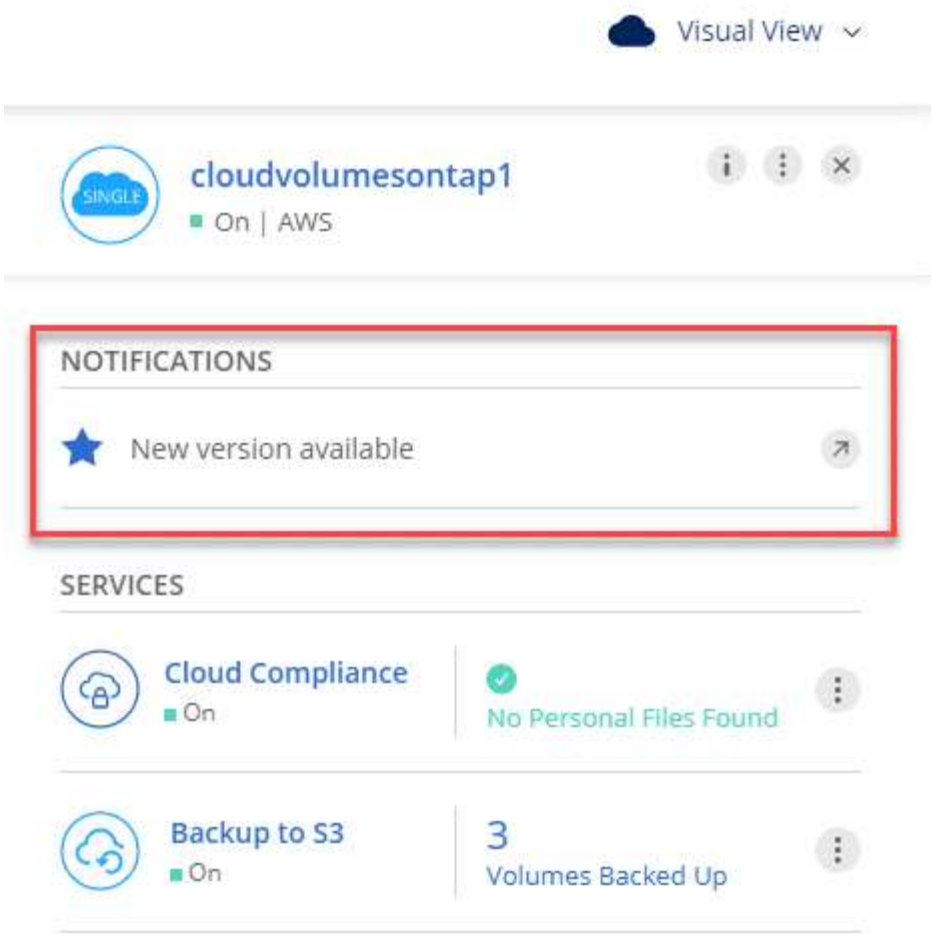
**Before you begin**

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

**Steps**

1. Click **Working Environments**.
2. Select a working environment.

   A notification appears in the right pane if a new version is available:




3. If a new version is available, click **Upgrade**.
4. In the Release Information page, click the link to read the Release Notes for the specified version, and then select the **I have read…** check box.
5. In the End User License Agreement (EULA) page, read the EULA, and then select **I read and approve the EULA**.
6. In the Review and Approve page, read the important notes, select **I understand…**, and then click **Go**.

**Result**

Cloud Manager starts the software upgrade. You can perform actions on the working environment once the software update is complete.

**After you finish**

If you suspended SnapMirror transfers, use System Manager to resume the transfers.

## Upgrading or downgrading 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 update from Cloud Manager. You might use this option if Cloud Manager cannot access the S3 bucket to upgrade the software or if you want to downgrade 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.

## Downgrading Cloud Volumes ONTAP by using a local image

Transitioning Cloud Volumes ONTAP to an earlier release in the same release family (for example, 9.5 to 9.4) is referred to as a downgrade. You can downgrade without assistance when downgrading new or test clusters, but you should contact technical support if you want to downgrade a production cluster.

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. You can use this option to downgrade to the previous version of Cloud Volumes ONTAP, if you are experiencing issues with the current image.

#### About this task

This downgrade process is available for single Cloud Volumes ONTAP systems only. It is not available for HA pairs.

#### 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 instances as your storage needs change. For example, you can change between pay-as-you-go configurations, change the instance or VM type, and move to an alternate subscription.

## Installing license files on Cloud Volumes ONTAP BYOL systems

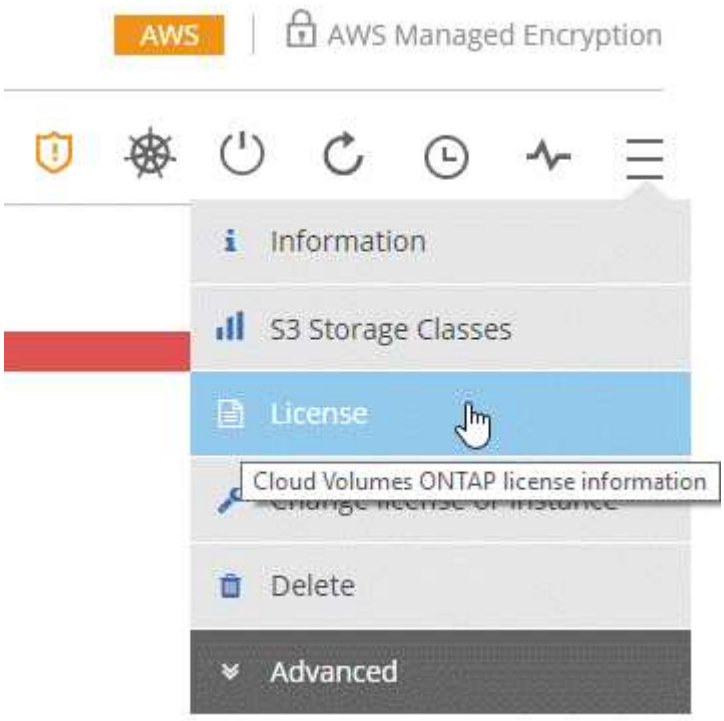
If Cloud Manager cannot obtain a BYOL license file from NetApp, you can obtain the file yourself and then manually upload the file to Cloud Manager so it can install the license on the Cloud Volumes ONTAP system.

**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.
4. In Cloud Manager, open the Cloud Volumes ONTAP BYOL working environment.
5. Click the menu icon and then click **License**.




6. Click **Upload License File**.

7. Click **Upload** and then select the file.

**Result**

Cloud Manager installs the new license file on the Cloud Volumes ONTAP system.

## 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

- 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**

1. 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. If you are using a pay-as-you-go configuration, you can optionally choose a different license.
3. 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**

1. 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 move between a pay-as-you-go subscription and a BYOL subscription or between a single Cloud Volumes ONTAP system and an HA pair, you can 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 your AWS Marketplace subscription

Change the AWS Marketplace subscription for your Cloud Volumes ONTAP system if you want to change the AWS account from which you get charged.

**Steps**

1. If you haven't already done so, add a new subscription from the Cloud Manager offering in the AWS Marketplace.
2. From the working environment in Cloud Manager, click the menu icon, and then click **Marketplace Subscription**.
3. Select a subscription from the drop-down list.
4. Click **Save**.

## Changing write speed to normal or high

The default write speed for Cloud Volumes ONTAP is normal. You can change to high write speed if fast write performance is required for your workload. 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.

  For single node systems, I/O is interrupted.

  For HA pairs, the change is nondisruptive. HA pairs continue to serve data.

**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.

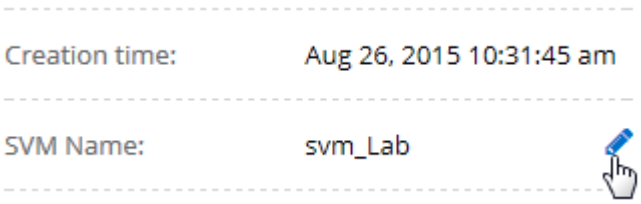
3. Click **Save**, review the confirmation message, and then click **Proceed**.

## Modifying the storage virtual machine name

Cloud Manager automatically names the storage virtual machine (SVM) for Cloud Volumes ONTAP. You can modify the name of the SVM if you have strict naming standards. For example, you might want it to match how you name the SVMs for your ONTAP clusters.

**Steps**

1. From the working environment, click the menu icon, and then click **Information**.
2. Click the edit icon to the right of the SVM name.




3. In the Modify SVM Name dialog box, modify the SVM 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.


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.

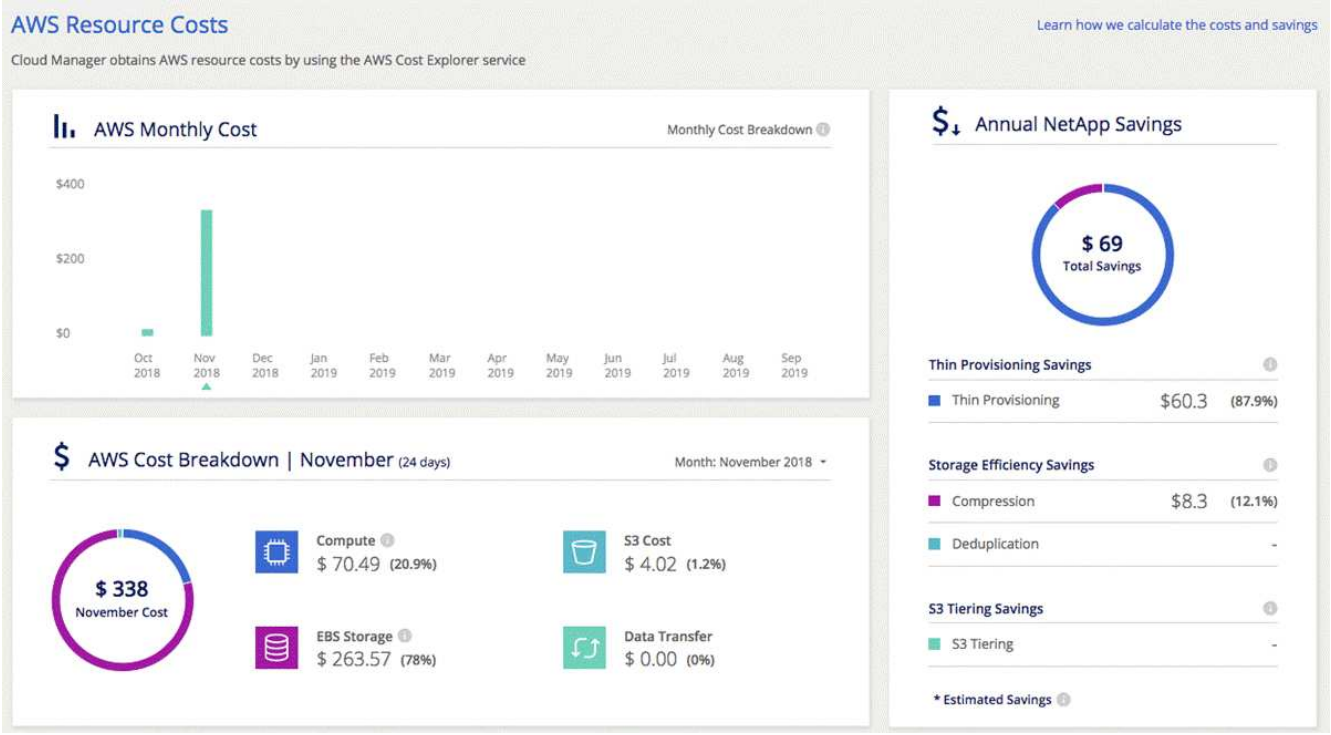
   b. Activate the **WorkingEnvironmentId** tag.

   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 Working Environments 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:

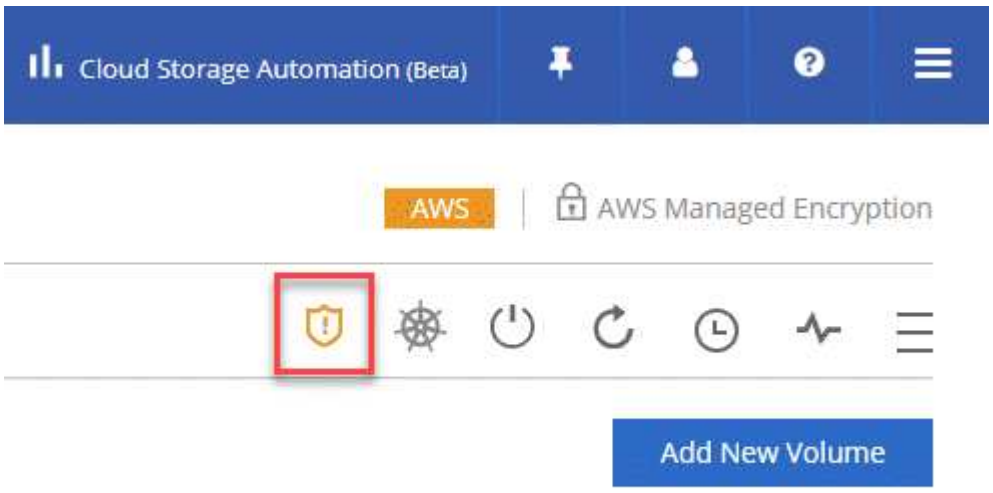



# Improving protection against ransomware

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.

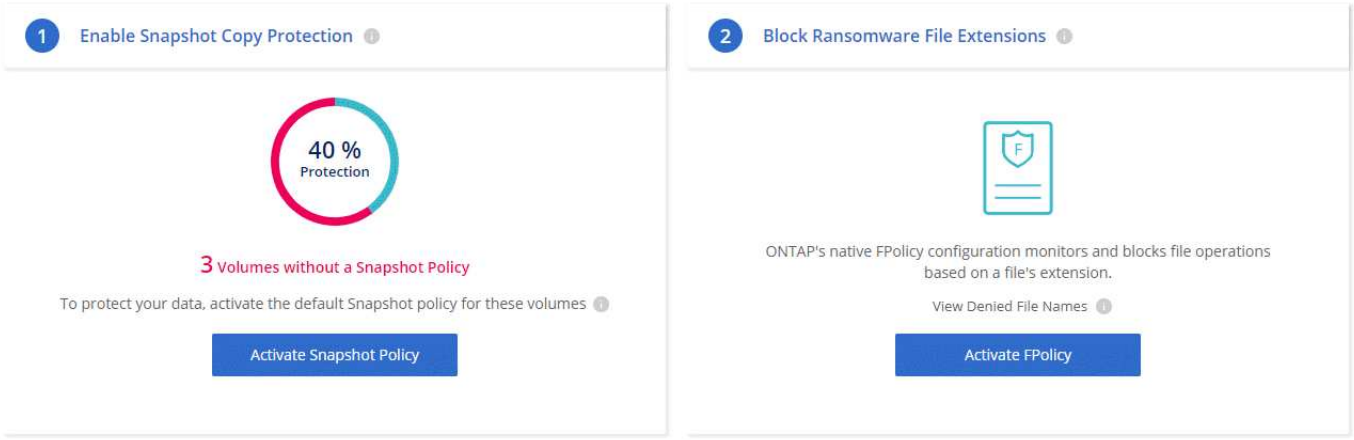



2. Implement the NetApp solution for ransomware:
   a. Click **Activate Snapshot Policy**, if you have volumes that do not have a Snapshot policy enabled.

NetApp Snapshot technology provides the industry's best solution for ransomware remediation. The key to a successful recovery is restoring from uninfected backups. Snapshot copies are read-only, which prevents ransomware corruption. They can also provide the granularity to create images of a single file copy or a complete disaster recovery solution.

b. Click **Activate FPolicy** to enable ONTAP's FPolicy solution, which can block file operations based on a file's extension.

   This preventative solution improves protection from ransomware attacks by blocking common ransomware file types.




# 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 Working Environments page, click **Discover** and select **Cloud Volumes ONTAP**.
2. Select the cloud provider in which the system resides.
3. On the Region page, choose the region where the instances are running, and then select the instances.
4. 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.

# 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.

# Administer Cloud Manager

## Updating Cloud Manager

You can update Cloud Manager to the latest version or with a patch that NetApp personnel shared with you.

### Enabling automatic updates

Cloud Manager can automatically update itself when a new version is available. This ensures that you are running the latest version.

#### About this task

Cloud Manager automatically updates at 12:00 midnight if no operations are running.

#### Steps

1. In the upper right of the Cloud Manager console, click the Settings icon, and select **Cloud Manager Settings**.
2. Select the checkbox under Automatic Cloud Manager Updates and then click **Save**.

### Updating Cloud Manager to the latest version

You should enable automatic updates to Cloud Manager, but you can always do a manual update directly from the web console. Cloud Manager obtains the software update from a NetApp-owned S3 bucket in AWS.

#### Before you begin

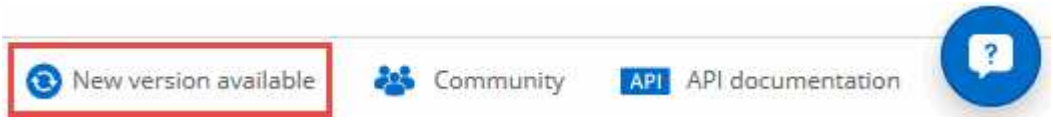
You should have reviewed what is new in the release to identify new requirements and changes in support.

#### About this task

The software update takes a few minutes. Cloud Manager will not be available during the update.

#### Steps

1. Check whether a new version is available by looking at the lower-right corner of the console:




2. If a new version is available, click **Timeline** to determine whether any tasks are in progress.

   If any tasks are in progress, wait for them to finish before you proceed to the next step.

3. In the lower-right of the console, click **New version available**.
4. On the Cloud Manager Software Update page, click **Update** next to the version that you want.
5. Complete the confirmation dialog box, and then click **OK**.

#### Result

Cloud Manager starts the update process. You can log in to the console after a few minutes.

## Updating Cloud Manager with a patch

If NetApp shared a patch with you, you can update Cloud Manager with the supplied patch directly from the Cloud Manager web console.

### About this task

The patch update typically takes a few minutes. Cloud Manager will not be available during the update.

### Steps

1. In the upper right of the Cloud Manager console, click the Settings icon, and select **Software Update**.


2. Click the link to update Cloud Manager with the supplied patch.


3. Complete the confirmation dialog box and then click **OK**.
4. Select the patch that you were provided.

### Result

Cloud Manager applies the patch. You can log in to the console after a few minutes.

# Managing workspaces and users in the Cloud Central account

After you perform initial setup, you might need to later manage users, workspaces, and service connectors.

Learn more about how Cloud Central accounts work.

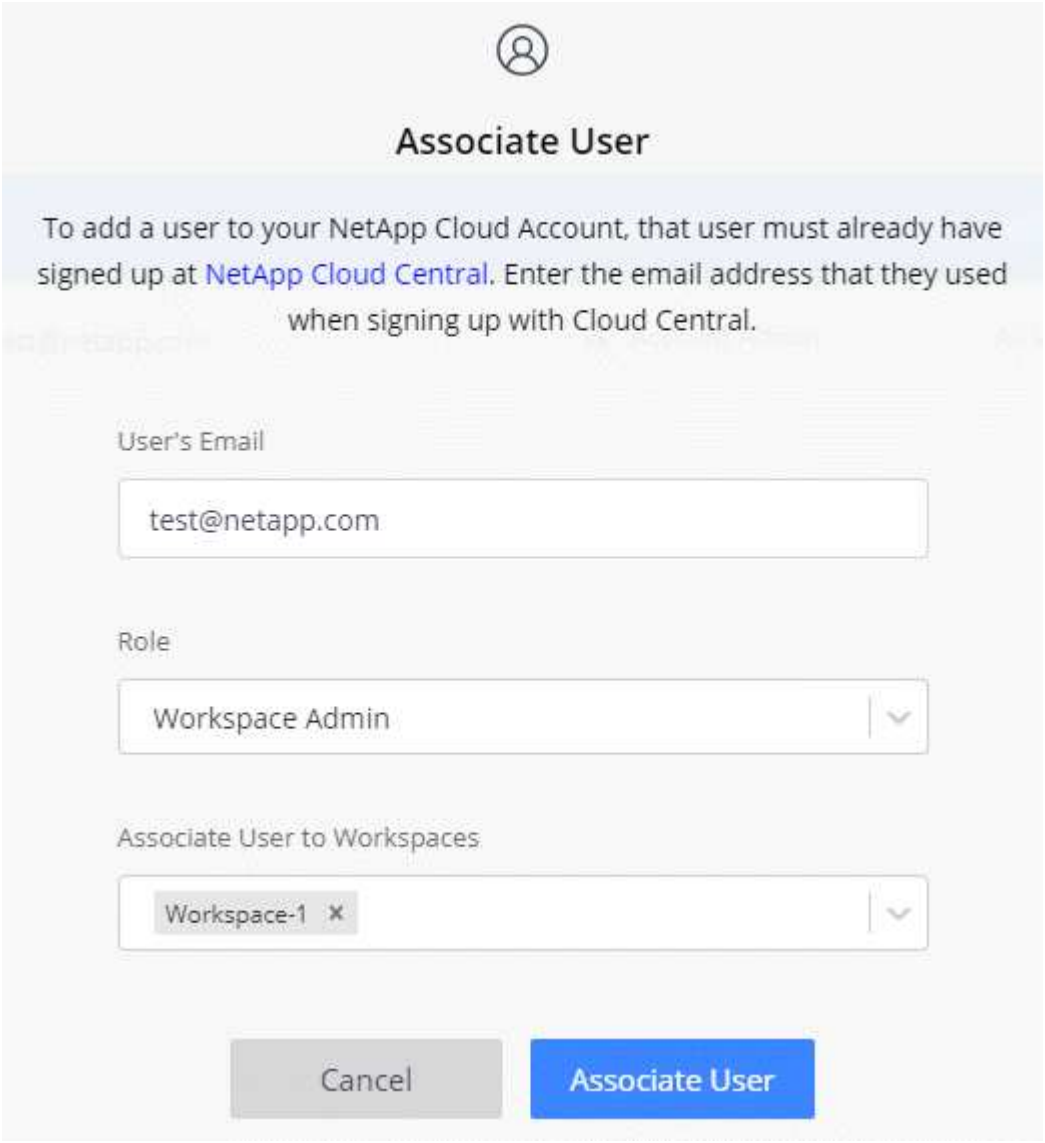
## Adding users

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 has not already done so, ask the user to go to NetApp Cloud Central and create an account.
2. In Cloud Manager, click **Account Settings**.
3. In 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.

5. If you selected Workspace Admin, select one or more workspaces to associate with that 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.

**Result**

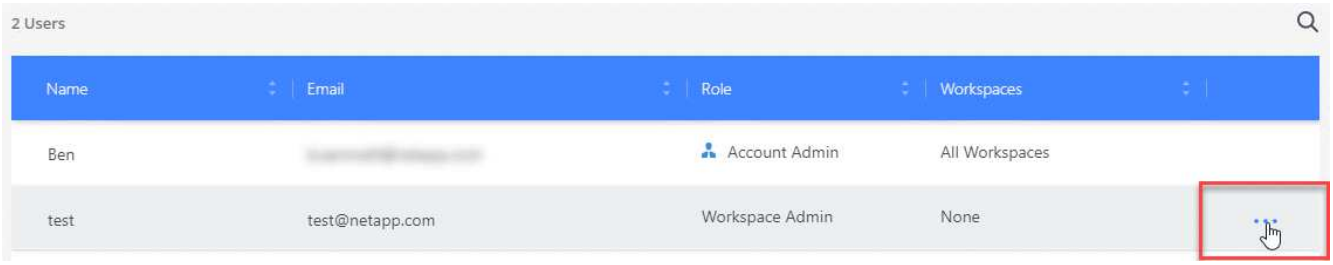
The user should receive an email from NetApp Cloud Central titled "Account Association." The email includes the information needed to access Cloud Manager.

## Removing users

Disassociating a user makes it so they can no longer access the resources in a Cloud Central account.

**Steps**

1. Click **Account Settings**.
2. Click the action menu in the row that corresponds to the user.




3. Click **Disassociate User** and click **Disassociate** to confirm.

**Result**

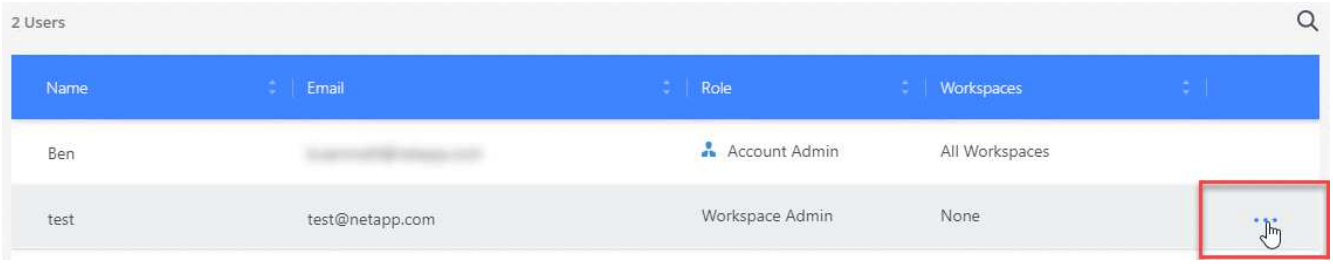
The user can no longer access the resources in this Cloud Central account.

## 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. Click **Account Settings**.
2. Click the action menu in the row that corresponds to the user.




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 service 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. Click **Account Settings**.
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 service connector's workspaces

You need to associate the service connector with workspaces so Workspace Admins can access those workspaces from Cloud Manager.

If you only have Account Admins, then associating the service 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 service connectors.

**Steps**

1. Click **Account Settings**.
2. Click **Service Connector**.
3. Click **Manage Workspaces** for the service connector that you want to associate.
4. Select the workspaces to associate with the service connector and click **Apply**.

# 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 Working Environments page at any time.

# Configuring Cloud Manager to use a proxy server

When you first deploy Cloud Manager, it prompts you to enter a proxy server if the system does not have internet access. You can also manually enter and modify the proxy from Cloud Manager's settings.

**About this task**

If your corporate policies dictate that you use a proxy server for all HTTP communication to the internet, then you must configure Cloud Manager to use that proxy server. The proxy server can be in the cloud or in your network.

When you configure Cloud Manager to use a proxy server, Cloud Manager, Cloud Volumes ONTAP, and the HA mediator all use the proxy server.

**Steps**

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


2. 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 does not 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 do not 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.

# 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.

# Restoring Cloud Manager

Your NetApp Cloud Central account makes it easy for you to restore a Cloud Manager configuration. The account is a service running in Cloud Central so the users, workspaces, and service connectors that you associated with the account are always accessible. Even if your Cloud Manager system was accidentally deleted.

Starting with the 3.7.1 release, Cloud Manager no longer supports downloading a backup and using it to restore your configuration. You need to follow these steps to restore Cloud Manager.

**Steps**

1. Deploy a new Cloud Manager system in your existing Cloud Central account.

   Deployment options

2. Add your cloud provider accounts and NetApp Support Site accounts to Cloud Manager.

   This step gets Cloud Manager ready so you can create additional Cloud Volumes ONTAP systems in your cloud provider.

   It's important to complete this step if you used AWS keys to deploy an existing Cloud Volumes ONTAP system that you want to discover on this new Cloud Manager system. Cloud Manager needs the AWS keys to properly discover and manage Cloud Volumes ONTAP.

   - Adding AWS accounts to Cloud Manager
   - Adding Azure accounts to Cloud Manager
   - Adding NetApp Support Site accounts to Cloud Manager

3. Rediscover your working environments: Cloud Volumes ONTAP systems, on-premises clusters, and NetApp Private Storage for Cloud configurations.
   - Adding existing Cloud Volumes ONTAP systems to Cloud Manager
   - Discovering ONTAP clusters

**Result**

Your Cloud Manager configuration is now restored with your accounts, settings, and working environments.

# Uninstalling Cloud Manager

Cloud Manager includes an uninstallation script that you can use to uninstall the software to troubleshoot issues or to permanently remove the software from the host.

**Steps**

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.

# Provision volumes for file services

## Managing volumes for Azure NetApp Files

View and create NFS volumes for Azure NetApp Files directly from Cloud Manager.

### Setting up your configuration

Your configuration needs to meet a few requirements before you can manage volumes for Azure NetApp Files from Cloud Manager.

1. Azure NetApp Files must be set up by completing the following from the Azure portal:
   - Register for Azure NetApp Files
   - Create a NetApp account
   - Set up a capacity pool
   - Delegate a subnet to Azure NetApp Files
2. Cloud Manager must be set up as follows:
   - Cloud Manager must be running in Azure, in the account where Azure NetApp Files was set up.
   - The Cloud Manager virtual machine must receive permissions through a managed identity.

     If you deployed Cloud Manager from Cloud Central, then you're all set. Cloud Central automatically enables a system-assigned managed identity on the Cloud Manager virtual machine.

     If you deployed Cloud Manager from the Azure Marketplace, then you should have followed instructions to enable a managed identity.

   - The Azure role assigned to the Cloud Manager virtual machine must include the permissions listed in the latest Cloud Manager policy for Azure:

```
"Microsoft.NetApp/netAppAccounts/read",
"Microsoft.NetApp/netAppAccounts/capacityPools/read",
"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/write",
"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/read",
"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/delete"
```

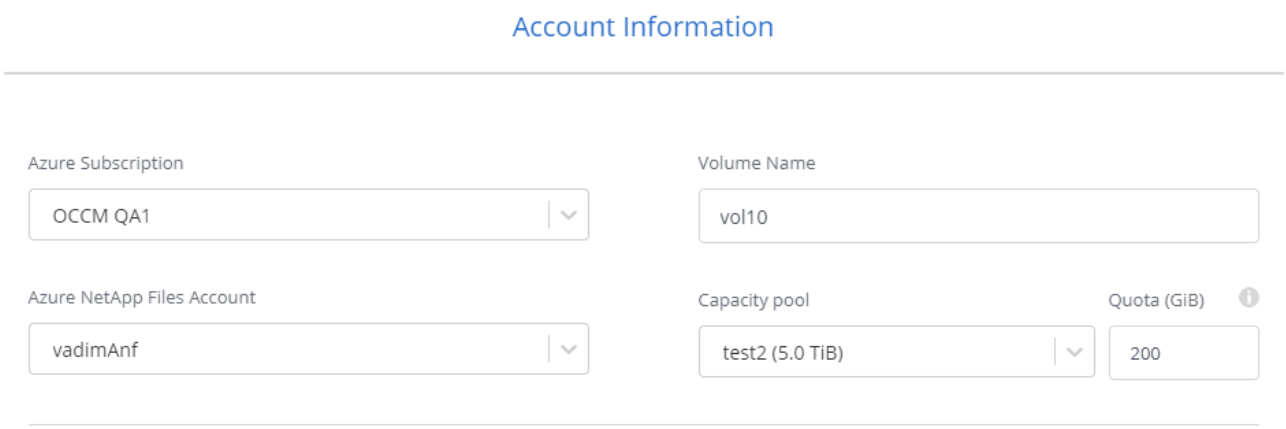
When your configuration is set up, Cloud Manager automatically displays Azure NetApp Files on the Working Environments page:

## Creating volumes

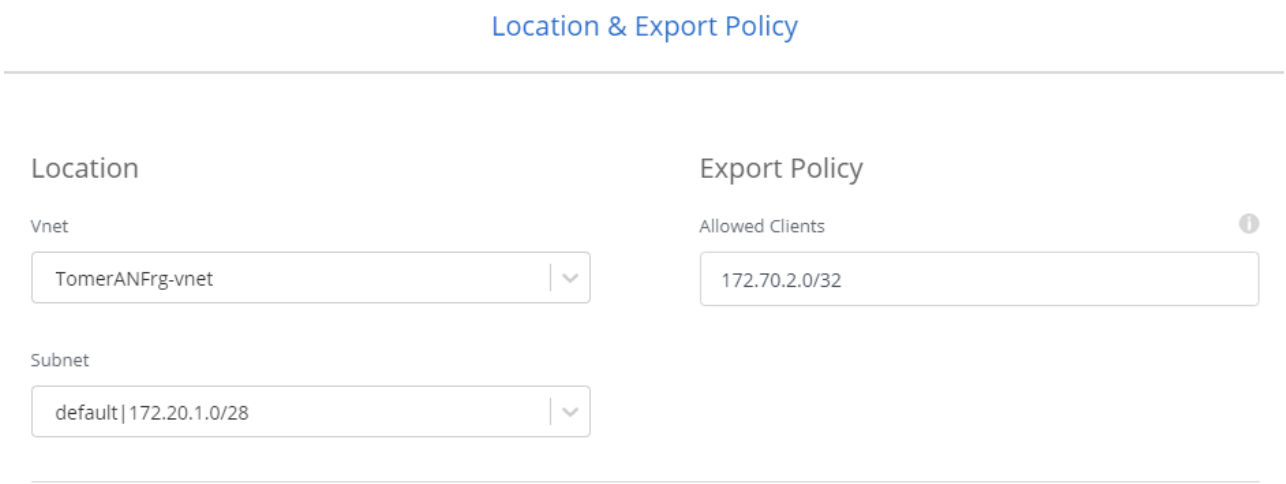
Cloud Manager enables you to create NFSv3 volumes for Azure NetApp Files.

**Steps**

1. Open the working environment.
2. Click **Add New Volume**.
3. Enter basic details about the volume in the **Account Information** page:
   a. Select an Azure subscription and Azure NetApp Files account.
   b. Enter a name for the volume.
   c. Select a capacity pool and specify a quota, which is the amount of logical storage that's allocated to the volume.




4. Fill out the **Location & Export Policy** page:
   a. Select a VNet and subnet.
   b. Configure an export policy to control access to the volume.



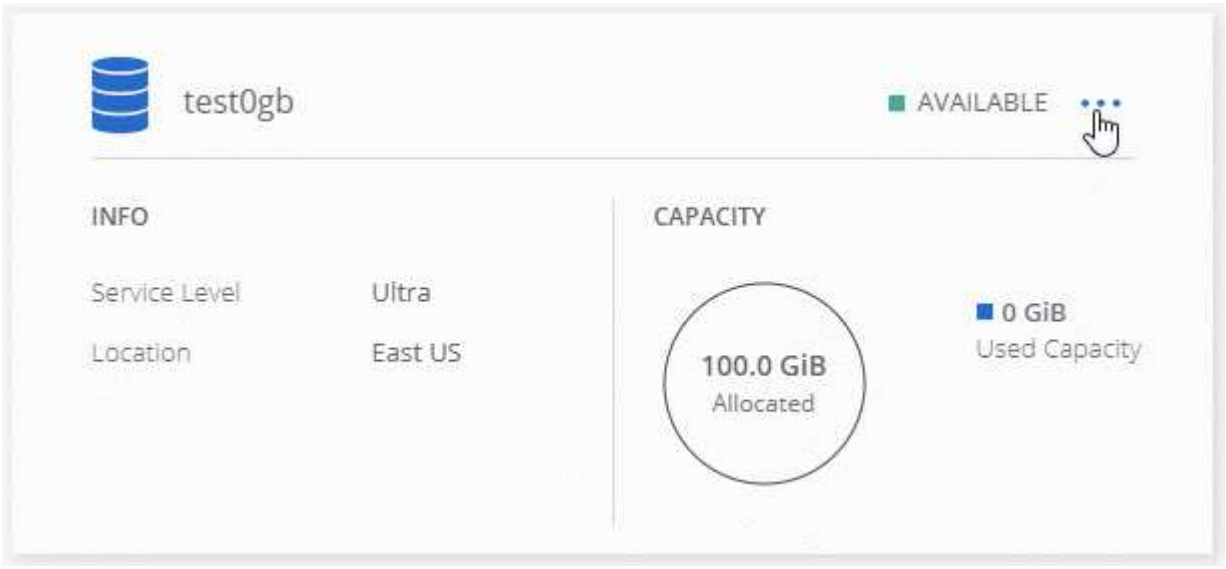

5. Click **Go**.

## Getting a volume's mount path

Copy the mount path for a volume so you can mount the volume to a Linux machine.

**Steps**

1. Open the working environment.
2. Hover over the volume and click the menu.




3. Click **Mount Command**.


4. Copy the mount path and use the copied text to mount the volume to a Linux machine.

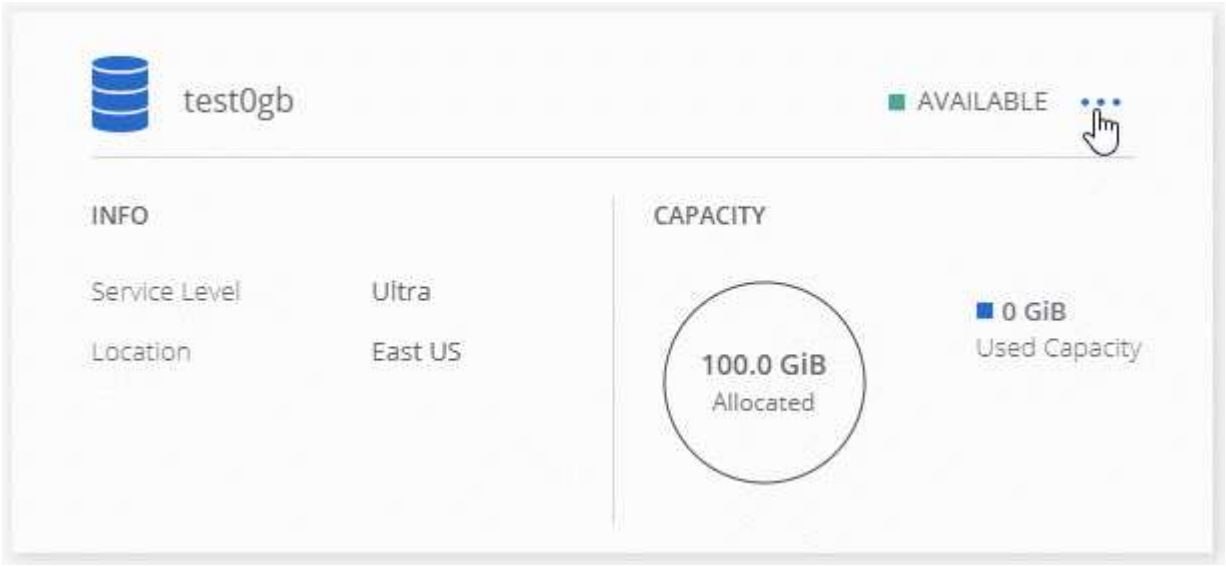
## Deleting volumes

Delete the volumes that you no longer need.

**Steps**

1. Open the working environment.

2. Hover over the volume and click the menu.




3. Click **Delete**.
4. Confirm that you want to delete the volume.

### Getting help

Use the Cloud Manager chat for general service questions.

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.

Cloud Manager provides a local AutoSupport download under the **Support Dashboard** menu option. This 7z file contains an Azure debug file to show inbound and outbound communication to your Azure NetApp Files account.

### Limitations

- Cloud Manager doesn't support SMB volumes.
- Cloud Manager doesn't enable you to manage capacity pools or volume snapshots.
- You can create volumes with an initial size and single export policy. Editing a volume must be done from the Azure NetApp Files interface in the Azure portal.
- Cloud Manager doesn't support data replication to or from Azure NetApp Files.

### Related links

- NetApp Cloud Central: Azure NetApp Files
- Azure NetApp Files documentation

# Managing Cloud Volumes Service for AWS

Cloud Manager enables you to discover the NFS cloud volumes in your Cloud Volumes

Service for AWS subscription. After discovery, you can add additional NFS cloud volumes directly from Cloud Manager.

Cloud Manager does not support SMB or dual-protocol volumes with Cloud Volumes Service for AWS.

## Before you get started

- Cloud Manager enables discovery of *existing* Cloud Volumes Service for AWS subscriptions. 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 and provision your first volume from Cloud Volumes Service before you can discover the region 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.

## Discovering your Cloud Volumes Service for AWS subscription

To get started, you need to discover the cloud volumes in an AWS region. You can discover additional regions later.

**Steps**

1. On the Working Environments page, click **Discover**.
2. Select **Cloud Volumes Service for AWS**.
3. Provide information about your Cloud Volumes Service subscription:
   a. Select the AWS region where your cloud volumes reside.
   b. Enter the Cloud Volumes API key and secret key. For instructions, refer to Cloud Volumes Service for AWS documentation.
   c. Click **Go**.

**Result**

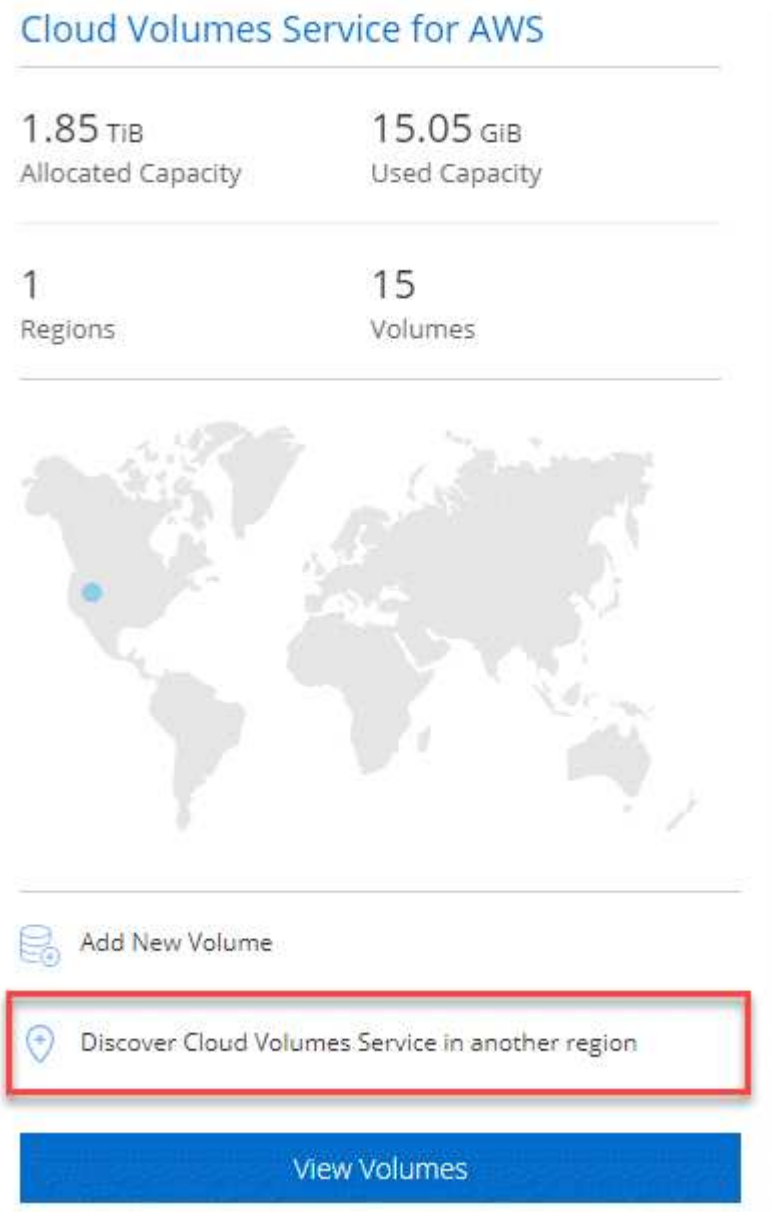
Cloud Manager should now display your Cloud Volumes Service for AWS configuration on the Working Environments page.

## Discovering additional regions

If you have cloud volumes in additional regions, you need to discover each individual region.

**Steps**

1. On the Working Environments page, select the working environment (but don't open it by double-clicking).
2. In the right pane, click **Discover Cloud Volumes Service in another region**.




3. Provide information about your Cloud Volumes Service subscription:
   a. Select the AWS region where your cloud volumes reside.
   b. Enter the Cloud Volumes API key and secret key. For instructions, refer to Cloud Volumes Service for AWS documentation.
   c. Click **Go**.

**Result**

Cloud Manager discovers information about the cloud volumes in the selected region.

## Creating cloud volumes

Cloud Manager enables you to create NFSv3 cloud volumes. You can only create cloud volumes with an initial size and single export policy. Editing the volume must be done from the Cloud Volume Service user interface.

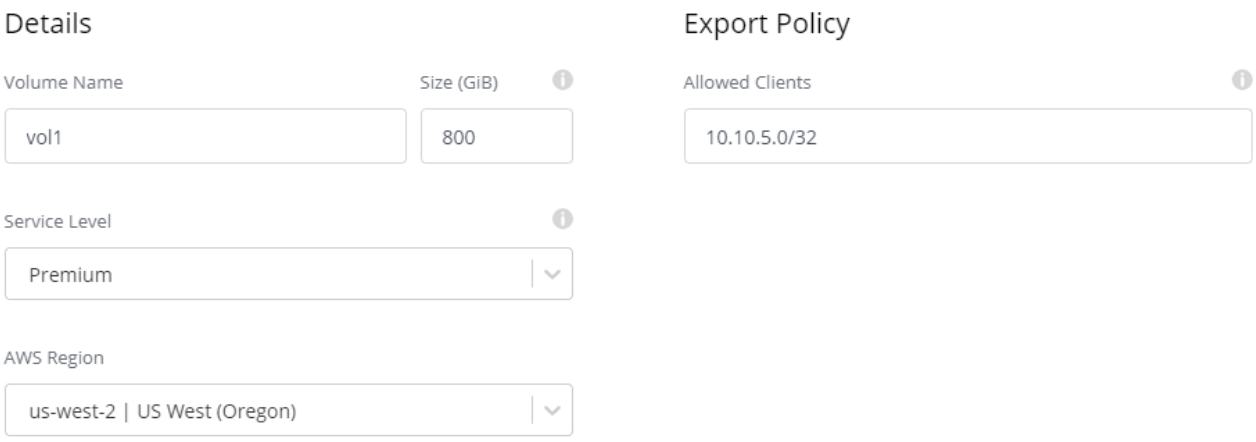
1. Open the working environment.
2. Click **Add New Volume**.
3. Enter details about the volume:
   a. Enter a name for the volume.
   b. Specify a size within the range of 100 GiB to 90,000 GiB (equivalent to 88 TiBs).

      Cloud Manager displays volumes in GiB, while the Cloud Volumes Service displays volumes in GB.

   c. Specify a service level: Standard, Premium, or Extreme.

      Learn more about these service levels.

   d. Choose a region. You can create the volume in a region that Cloud Manager has discovered.
   e. Restrict client access by specifying an IP address or Classless Inter-Domain Routing (CIDR).




4. Click **Go**.

## Deleting cloud volumes

Delete the cloud volumes that you no longer need.

**Steps**

1. Open the working environment.
2. Hover over the volume and click the menu. Click **Delete**.

3. Confirm that you want to delete the volume.

## 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 does not support SMB or dual-protocol volumes.
- You can only create cloud volumes with an initial size and single export policy. Editing the volume must be done from the Cloud Volume Service user interface.
- Cloud Manager doesn’t support data replication to or from a Cloud Volumes Service for AWS subscription.
- Removing your Cloud Volumes Service for AWS subscription from Cloud Manager isn’t supported. There are no charges to discover a region from Cloud Manager.

## Related links

- NetApp Cloud Central: Cloud Volumes Service for AWS
- NetApp Cloud Volumes Service for AWS documentation

# APIs and automation

## Automation samples 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.

DevOps teams use a variety of tools to automate the setup of new environments, which allows them to treat infrastructure as code. Two such tools are Ansible and Terraform. We have developed Ansible and Terraform samples that DevOps team can use with Cloud Manager to automate and integrate Cloud Volumes ONTAP with infrastructure as code.

View the automation samples.

For example, you can use sample Ansible playbooks to deploy Cloud Manager and Cloud Volumes ONTAP, create an aggregate, and create a volume. Modify the samples for your environment or create new playbooks based on the samples.

**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

# Reference

## Frequently asked questions: Integrating Cloud Manager with NetApp Cloud Central

When upgrading from Cloud Manager 3.4 or earlier, NetApp will choose specific Cloud Manager systems to integrate with NetApp Cloud Central, if they are not already integrated. This FAQ can answer questions that you might have about the process.

### What is NetApp Cloud Central?

NetApp Cloud Central provides a centralized location to access and manage NetApp cloud data services. These services enable you to run critical applications in the cloud, create automated DR sites, back up your SaaS data, and effectively migrate and control data across multiple clouds.

### Why is NetApp integrating my Cloud Manager system with Cloud Central?

Cloud Manager's integration with NetApp Cloud Central provides several benefits, including a simplified deployment experience, a single location to view and manage multiple Cloud Manager systems, and centralized user authentication.

### What happens during the integration process?

NetApp migrates all local user accounts in your Cloud Manager system to the centralized user authentication available in Cloud Central.

### How does centralized user authentication work?

With centralized user authentication, you can use the same set of credentials across Cloud Manager systems and between Cloud Manager and other data services, such as Cloud Sync. It's also easy to reset your password if you forget it.

### Do I need to sign up for a Cloud Central user account?

NetApp will create a Cloud Central user account for you when we integrate your Cloud Manager system with Cloud Central. You simply need to reset your password to complete the registration process.

### What if I already have a Cloud Central user account?

If the email address that you use to log in to Cloud Manager matches the email address for a Cloud Central user account, then you can log right in to your Cloud Manager system.

### What if my Cloud Manager system has multiple user accounts?

NetApp migrates all local user accounts to Cloud Central user accounts. Every user needs to reset his or her password.

### What if I have a user account that uses the same email address across multiple Cloud Manager systems?

You just need to reset your password once and then you can use the same Cloud Central user account to log in to each Cloud Manager system.

### What if my local user account uses an invalid email address?

Resetting your password requires a valid email address. Contact us through the chat icon that is available in the lower right of the Cloud Manager interface.

### What if I have automation scripts for Cloud Manager APIs?

All APIs are backwards compatible. You will need to update scripts that use passwords, if you change your password when you reset it.

### What if my Cloud Manager system uses LDAP?

If your system uses LDAP, NetApp cannot automatically integrate the system with Cloud Central. You need to manually perform the following steps:

1. Deploy a new Cloud Manager system from NetApp Cloud Central.
2. Set up LDAP with the new system.
3. Discover existing Cloud Volumes ONTAP systems from the new Cloud Manager system.
4. Delete the old Cloud Manager system.

### Does it matter where I installed my Cloud Manager system?

No. NetApp will integrate systems with Cloud Central no matter where they reside, whether that's in AWS, Azure, or on your premises.

The only exception is the AWS Commercial Cloud Services Environment.

# Security group rules for AWS

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

## Rules for Cloud Manager

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

#### Inbound rules for Cloud Manager

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

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

### Outbound rules for Cloud Manager

The predefined security group for Cloud Manager 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 Manager 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 Cloud Manager.

The source IP address is the Cloud Manager 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 |

| Service | Protocol | Port | Destination | Purpose |
|---|---|---|---|---|
| API calls and AutoSupport | HTTPS | 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 Cloud Volumes ONTAP

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

### Inbound rules for Cloud Volumes ONTAP

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 |

| Protocol | Port | Purpose |
|---|---|---|
| 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 for Cloud Volumes ONTAP

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 | 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) | 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 | 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 | 18600–18699 | Node management LIF | Destination servers | NDMP copy |
| SMTP | TCP | 25 | Node management LIF | Mail server | SMTP alerts, can be used for AutoSupport |
| SNMP | TCP | 161 | Node management LIF | Monitor server | Monitoring by SNMP traps |
| | UDP | 161 | Node management LIF | Monitor server | Monitoring by SNMP traps |
| | TCP | 162 | Node management LIF | Monitor server | Monitoring by SNMP traps |
| | UDP | 162 | Node management LIF | Monitor server | Monitoring by SNMP traps |
| SnapMirror | TCP | 11104 | Intercluster LIF | ONTAP intercluster LIFs | Management of intercluster communication sessions for SnapMirror |
| | TCP | 11105 | Intercluster LIF | ONTAP intercluster LIFs | SnapMirror data transfer |
| Syslog | UDP | 514 | Node management LIF | Syslog server | Syslog forward messages |

## Rules for 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 Cloud Manager |

### 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 | Cloud Manager 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 |

# Security group rules for Azure

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

## Rules for Cloud Manager

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

#### Inbound rules for Cloud Manager

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

| Port | Protocol | Purpose |
|---|---|---|
| 22 | SSH | Provides SSH access to the Cloud Manager host |
| 80 | HTTP | Provides HTTP access from client web browsers to the Cloud Manager web console |
| 443 | HTTPS | Provides HTTPS access from client web browsers to the Cloud Manager web console |

#### Outbound rules for Cloud Manager

The predefined security group for Cloud Manager 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 Manager 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 Manager.

The source IP address is the Cloud Manager 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 | HTTPS | 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 Cloud Volumes ONTAP

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 |

| Priority and name | Port and protocol | Source and destination | Description |
|---|---|---|---|
| 1005 inbound_161-162 _tcp | 161-162 TCP | Any to Any | Simple network management protocol |
| 1006 inbound_161-162 _udp | 161-162 UDP | Any to Any | Simple network management protocol |
| 1007 inbound_443 | 443 TCP | Any to Any | HTTPS access to the System Manager web console using the IP address of the cluster management LIF |
| 1008 inbound_445 | 445 TCP | Any to Any | Microsoft SMB/CIFS over TCP with NetBIOS framing |
| 1009 inbound_635_tcp | 635 TCP | Any to Any | NFS mount |
| 1010 inbound_635_udp | 635 UDP | Any to Any | NFS mount |
| 1011 inbound_749 | 749 TCP | Any to Any | Kerberos |
| 1012 inbound_2049_tcp | 2049 TCP | Any to Any | NFS server daemon |
| 1013 inbound_2049_udp | 2049 UDP | Any to Any | NFS server daemon |
| 1014 inbound_3260 | 3260 TCP | Any to Any | iSCSI access through the iSCSI data LIF |
| 1015 inbound_4045-4046_tcp | 4045-4046 TCP | Any to Any | NFS lock daemon and network status monitor |
| 1016 inbound_4045-4046_udp | 4045-4046 UDP | Any to Any | NFS lock daemon and network status monitor |
| 1017 inbound_10000 | 10000 TCP | Any to Any | Backup using NDMP |
| 1018 inbound_11104-11105 | 11104-11105 TCP | Any to Any | SnapMirror data transfer |
| 3000 inbound_deny _all_tcp | Any port TCP | Any to Any | Block all other TCP inbound traffic |
| 3001 inbound_deny _all_udp | Any port UDP | Any to Any | Block all other UDP inbound traffic |

| Priority and name | Port and protocol | Source and destination | Description |
|---|---|---|---|
| 65000 AllowVnetInBound | Any port Any protocol | VirtualNetwork to VirtualNetwork | Inbound traffic from within the VNet |
| 65001 AllowAzureLoad BalancerInBound | Any port Any protocol | AzureLoadBalancer to Any | Data traffic from the Azure Standard Load Balancer |
| 65500 DenyAllInBound | Any port Any protocol | Any to Any | Block all other inbound traffic |

**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.

| Priority and name | Port and protocol | Source and destination | Description |
|---|---|---|---|
| 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 AllowAzureLoad BalancerInBound | 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 for Cloud Volumes ONTAP

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 | 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) | 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 | Data LIF (NFS, CIFS) | Active Directory forest | LDAP |
| | 445 | TCP | Data LIF (NFS, CIFS) | Active Directory forest | Microsoft SMB/CIFS over TCP with NetBIOS framing |
| | 464 | TCP | Data LIF (NFS, CIFS) | Active Directory forest | Kerberos V change & set password (SET_CHANGE) |
| | 464 | UDP | Data LIF (NFS, CIFS) | Active Directory forest | Kerberos key administration |
| | 749 | TCP | Data LIF (NFS, CIFS) | Active Directory forest | Kerberos V change & set password (RPCSEC_GSS) |
| DHCP | 68 | UDP | Node management LIF | DHCP | DHCP client for first-time setup |
| DHCPS | 67 | UDP | Node management LIF | DHCP | DHCP server |

| Service | Port | Protocol | Source | Destination | Purpose |
|---|---|---|---|---|---|
| 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 |

# Firewall rules for GCP

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

## Rules for Cloud Manager

The firewall rules for Cloud Manager requires both inbound and outbound rules.

#### Inbound rules for Cloud Manager

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

| Protocol | Port | Purpose |
|---|---|---|
| SSH | 22 | Provides SSH access to the Cloud Manager host |
| HTTP | 80 | Provides HTTP access from client web browsers to the Cloud Manager web console |

| Protocol | Port | Purpose |
|---|---|---|
| HTTPS | 443 | Provides HTTPS access from client web browsers to the Cloud Manager web console |

### Outbound rules for Cloud Manager

The predefined firewall rules for Cloud Manager 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 Cloud Manager 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 Cloud Manager.

The source IP address is the Cloud Manager 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 | HTTPS | 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 |

## Rules for Cloud Volumes ONTAP

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

### Inbound rules for Cloud Volumes ONTAP

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 |
| 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 for Cloud Volumes ONTAP

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 | 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) | 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 | 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 | 18600–18699 | Node management LIF | Destination servers | NDMP copy |
| SMTP | TCP | 25 | Node management LIF | Mail server | SMTP alerts, can be used for AutoSupport |
| SNMP | TCP | 161 | Node management LIF | Monitor server | Monitoring by SNMP traps |
| | UDP | 161 | Node management LIF | Monitor server | Monitoring by SNMP traps |
| | TCP | 162 | Node management LIF | Monitor server | Monitoring by SNMP traps |
| | UDP | 162 | Node management LIF | Monitor server | Monitoring by SNMP traps |
| SnapMirror | TCP | 11104 | Intercluster LIF | ONTAP intercluster LIFs | Management of intercluster communication sessions for SnapMirror |
| | TCP | 11105 | Intercluster LIF | ONTAP intercluster LIFs | SnapMirror data transfer |
| Syslog | UDP | 514 | Node management LIF | Syslog server | Syslog forward messages |

# 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 you're not sure which page you need to use, read below and we'll direct you to the right page based on your goal.

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 deployment of Cloud Volumes ONTAP PAYGO for versions 9.6 and later | Cloud Manager (for Cloud Volumes ONTAP) | This AWS Marketplace page enables charging for the PAYGO version of Cloud Volumes ONTAP 9.6 and later. It also enables charging for Cloud Volumes ONTAP add-on features.<br><br>This page does not enable you to launch Cloud Manager in AWS. That should be done from NetApp Cloud Central, or alternatively using the AMI listed in row 4 of this table. |
| Enable add-on features for Cloud Volumes ONTAP (PAYGO or BYOL) | | |
| Enable deployment of Cloud Volumes ONTAP using a license that I purchased from NetApp (BYOL) | • Cloud Volumes ONTAP for AWS (BYOL)<br>• Cloud Volumes ONTAP for AWS - High Availability (BYOL) | These AWS Marketplace pages enable you to subscribe to the single node or HA versions of Cloud Volumes ONTAP BYOL. |
| Deploy Cloud Manager from the AWS Marketplace using an AMI | NetApp Cloud Manager (for NetApp Cloud Volumes ONTAP) | We recommend that you launch Cloud Manager in AWS from NetApp Cloud Central, but you can launch it from this AWS Marketplace page, if you prefer. |
| Enable deployment of Cloud Volumes ONTAP PAYGO (9.5 or earlier) | • Cloud Volumes ONTAP for AWS<br>• Cloud Volumes ONTAP for AWS - High Availability | 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.<br><br>Starting with version 9.6, you need to subscribe through the AWS Marketplace page listed in row 1 of this table for PAYGO deployments. |

# 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 |
| --- | --- |
| "ec2:StartInstances",<br>"ec2:StopInstances",<br>"ec2:DescribeInstances",<br>"ec2:DescribeInstanceStatus",<br>"ec2:RunInstances",<br>"ec2:TerminateInstances",<br>"ec2:ModifyInstanceAttribute", | Launches a Cloud Volumes ONTAP instance and stops, starts, and monitors the instance. |
| "ec2:DescribeInstanceAttribute", | Verifies that enhanced networking is enabled for supported instance types. |
| "ec2:DescribeRouteTables",<br>"ec2:DescribeImages", | Launches a Cloud Volumes ONTAP HA configuration. |
| "ec2:CreateTags", | Tags every resource that Cloud Manager creates with the "WorkingEnvironment" and "WorkingEnvironmentId" tags. Cloud Manager uses these tags for maintenance and cost allocation. |
| "ec2:CreateVolume",<br>"ec2:DescribeVolumes",<br>"ec2:ModifyVolumeAttribute",<br>"ec2:AttachVolume",<br>"ec2:DeleteVolume",<br>"ec2:DetachVolume", | Manages the EBS volumes that Cloud Volumes ONTAP uses as back-end storage. |
| "ec2:CreateSecurityGroup",<br>"ec2:DeleteSecurityGroup",<br>"ec2:DescribeSecurityGroups",<br>"ec2:RevokeSecurityGroupEgress",<br>"ec2:AuthorizeSecurityGroupEgress",<br>"ec2:AuthorizeSecurityGroupIngress",<br>"ec2:RevokeSecurityGroupIngress", | Creates predefined security groups for Cloud Volumes ONTAP. |
| "ec2:CreateNetworkInterface",<br>"ec2:DescribeNetworkInterfaces",<br>"ec2:DeleteNetworkInterface",<br>"ec2:ModifyNetworkInterfaceAttribute", | Creates and manages network interfaces for Cloud Volumes ONTAP in the target subnet. |
| "ec2:DescribeSubnets",<br>"ec2:DescribeVpcs", | Gets the list of destination subnets and security groups, which is needed when creating a new working environment for Cloud Volumes ONTAP. |
| "ec2:DescribeDhcpOptions", | Determines DNS servers and the default domain name when launching Cloud Volumes ONTAP instances. |
| "ec2:CreateSnapshot",<br>"ec2:DeleteSnapshot",<br>"ec2:DescribeSnapshots", | Takes snapshots of EBS volumes during initial setup and whenever a Cloud Volumes ONTAP instance is stopped. |
| "ec2:GetConsoleOutput", | Captures the Cloud Volumes ONTAP console, which is attached to AutoSupport messages. |
| "ec2:DescribeKeyPairs", | Obtains the list of available key pairs when launching instances. |

| Actions | Purpose |
| --- | --- |
| "ec2:DescribeRegions", | Gets a list of available AWS regions. |
| "ec2:DeleteTags",<br>"ec2:DescribeTags", | Manages tags for resources associated with Cloud Volumes ONTAP instances. |
| "cloudformation:CreateStack",<br>"cloudformation:DeleteStack",<br>"cloudformation:DescribeStacks",<br>"cloudformation:DescribeStackEvents",<br>"cloudformation:ValidateTemplate", | Launches Cloud Volumes ONTAP instances. |
| "iam:PassRole",<br>"iam:CreateRole",<br>"iam:DeleteRole",<br>"iam:PutRolePolicy",<br>"iam:CreateInstanceProfile",<br>"iam:DeleteRolePolicy",<br>"iam:AddRoleToInstanceProfile",<br>"iam:RemoveRoleFromInstanceProfile",<br>"iam:DeleteInstanceProfile", | Launches a Cloud Volumes ONTAP HA configuration. |
| "iam:ListInstanceProfiles",<br>"sts:DecodeAuthorizationMessage",<br>"ec2:AssociateIamInstanceProfile",<br>"ec2:DescribeIamInstanceProfileAssociations",<br>"ec2:DisassociateIamInstanceProfile", | Manages instance profiles for Cloud Volumes ONTAP instances. |
| "s3:GetBucketTagging",<br>"s3:GetBucketLocation",<br>"s3:ListAllMyBuckets",<br>"s3:ListBucket" | Obtains information about AWS S3 buckets so Cloud Manager can integrate with the NetApp Data Fabric Cloud Sync service. |
| "s3:CreateBucket",<br>"s3:DeleteBucket",<br>"s3:GetLifecycleConfiguration",<br>"s3:PutLifecycleConfiguration",<br>"s3:PutBucketTagging",<br>"s3:ListBucketVersions", | Manages the S3 bucket that a Cloud Volumes ONTAP system uses as a capacity tier. |
| "kms:List*",<br>"kms:Describe*" | Obtains information about keys from the AWS Key Management Service. |
| "ce:GetReservationUtilization",<br>"ce:GetDimensionValues",<br>"ce:GetCostAndUsage",<br>"ce:GetTags" | Obtains AWS cost data for Cloud Volumes ONTAP. |
| "ec2:CreatePlacementGroup",<br>"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. |

## 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",<br>"Microsoft.Compute/locations/vmSizes/read",<br>"Microsoft.Compute/operations/read",<br>"Microsoft.Compute/virtualMachines/instanceView/read",<br>"Microsoft.Compute/virtualMachines/powerOff/action",<br>"Microsoft.Compute/virtualMachines/read",<br>"Microsoft.Compute/virtualMachines/restart/action",<br>"Microsoft.Compute/virtualMachines/start/action",<br>"Microsoft.Compute/virtualMachines/deallocate/action",<br>"Microsoft.Compute/virtualMachines/vmSizes/read",<br>"Microsoft.Compute/virtualMachines/write", | Creates Cloud Volumes ONTAP and stops, starts, deletes, and obtains the status of the system. |
| "Microsoft.Compute/images/write",<br>"Microsoft.Compute/images/read", | Enables Cloud Volumes ONTAP deployment from a VHD. |
| "Microsoft.Compute/disks/delete",<br>"Microsoft.Compute/disks/read",<br>"Microsoft.Compute/disks/write",<br>"Microsoft.Storage/checknameavailability/read",<br>"Microsoft.Storage/operations/read",<br>"Microsoft.Storage/storageAccounts/listkeys/action",<br>"Microsoft.Storage/storageAccounts/read",<br>"Microsoft.Storage/storageAccounts/regeneratekey/action",<br>"Microsoft.Storage/storageAccounts/write"<br>"Microsoft.Storage/storageAccounts/delete",<br>"Microsoft.Storage/usages/read", | Manages Azure storage accounts and disks, and attaches the disks to Cloud Volumes ONTAP. |
| "Microsoft.Network/networkInterfaces/read",<br>"Microsoft.Network/networkInterfaces/write",<br>"Microsoft.Network/networkInterfaces/join/action", | Creates and manages network interfaces for Cloud Volumes ONTAP in the target subnet. |
| "Microsoft.Network/networkSecurityGroups/read",<br>"Microsoft.Network/networkSecurityGroups/write",<br>"Microsoft.Network/networkSecurityGroups/join/action", | Creates predefined network security groups for Cloud Volumes ONTAP. |

| Actions | Purpose |
| --- | --- |
| "Microsoft.Resources/subscriptions/locations/read",<br>"Microsoft.Network/locations/operationResults/read",<br>"Microsoft.Network/locations/operations/read",<br>"Microsoft.Network/virtualNetworks/read",<br>"Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read",<br>"Microsoft.Network/virtualNetworks/subnets/read",<br>"Microsoft.Network/virtualNetworks/subnets/virtualMachines/read",<br>"Microsoft.Network/virtualNetworks/virtualMachines/read",<br>"Microsoft.Network/virtualNetworks/subnets/join/action",<br> | Gets network information about regions, the target VNet and subnet, and adds Cloud Volumes ONTAP to VNets. |
| "Microsoft.Network/virtualNetworks/subnets/write",<br>"Microsoft.Network/routeTables/join/action",<br> | Enables VNet service endpoints for data tiering. |
| "Microsoft.Resources/deployments/operations/read",<br>"Microsoft.Resources/deployments/read",<br>"Microsoft.Resources/deployments/write",<br> | Deploys Cloud Volumes ONTAP from a template. |
| "Microsoft.Resources/deployments/operations/read",<br>"Microsoft.Resources/deployments/read",<br>"Microsoft.Resources/deployments/write",<br>"Microsoft.Resources/resources/read",<br>"Microsoft.Resources/subscriptions/operationresults/read",<br>"Microsoft.Resources/subscriptions/resourceGroups/delete",<br>"Microsoft.Resources/subscriptions/resourceGroups/read",<br>"Microsoft.Resources/subscriptions/resourcegroups/resources/read",<br>"Microsoft.Resources/subscriptions/resourceGroups/write",<br> | Creates and manages resource groups for Cloud Volumes ONTAP. |
| "Microsoft.Compute/snapshots/write",<br>"Microsoft.Compute/snapshots/read",<br>"Microsoft.Compute/disks/beginGetAccess/action"<br> | Creates and manages Azure managed snapshots. |
| "Microsoft.Compute/availabilitySets/write",<br>"Microsoft.Compute/availabilitySets/read",<br> | Creates and manages availability sets for Cloud Volumes ONTAP. |
| "Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/read",<br>"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/write"<br> | Enables programmatic deployments from the Azure Marketplace. |

| Actions | Purpose |
| --- | --- |
| "Microsoft.Network/loadBalancers/read",<br>"Microsoft.Network/loadBalancers/write",<br>"Microsoft.Network/loadBalancers/delete",<br>"Microsoft.Network/loadBalancers/backendAddressPools/read",<br>"Microsoft.Network/loadBalancers/backendAddressPools/join/action",<br>"Microsoft.Network/loadBalancers/frontendIPConfigurations/read",<br>"Microsoft.Network/loadBalancers/loadBalancingRules/read",<br>"Microsoft.Network/loadBalancers/probes/read",<br>"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",<br>"Microsoft.Authorization/roleAssignments/write",<br>"Microsoft.Web/sites/*" | Manages failover for HA pairs. |

## 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<br>- compute.disks.createSnapshot<br>- compute.disks.delete<br>- compute.disks.get<br>- compute.disks.list<br>- compute.disks.setLabels<br>- compute.disks.use | To create and manage disks for Cloud Volumes ONTAP. |
| - compute.firewalls.create<br>- compute.firewalls.delete<br>- compute.firewalls.get<br>- compute.firewalls.list | To create firewall rules for Cloud Volumes ONTAP. |
| - compute.globalOperations.get | To get the status of operations. |
| - compute.images.get<br>- compute.images.getFromFamily<br>- compute.images.list<br>- compute.images.useReadOnly | To get images for VM instances. |
| - compute.instances.attachDisk<br>- compute.instances.detachDisk | To attach and detach disks to Cloud Volumes ONTAP. |
| - compute.instances.create<br>- compute.instances.delete | To create and delete Cloud Volumes ONTAP VM instances. |
| - compute.instances.get | To list VM instances. |

| Actions | Purpose |
| --- | --- |
| - compute.instances.getSerialPortOutput | To get console logs. |
| - compute.instances.list | To retrieve the list of instances in a zone. |
| - compute.instances.setDeletionProtection | To set deletion protection on the instance. |
| - compute.instances.setLabels | To add labels. |
| - compute.instances.setMachineType | To change the machine type for Cloud Volumes ONTAP. |
| - compute.instances.setMetadata | To add metadata. |
| - compute.instances.setTags | To add tags for firewall rules. |
| - compute.instances.start<br>- compute.instances.stop<br>- compute.instances.updateDisplayDevice | To start and stop Cloud Volumes ONTAP. |
| - compute.machineTypes.get | To get the numbers of cores to check qoutas. |
| - compute.projects.get | To support multi-projects. |
| - compute.snapshots.create<br>- compute.snapshots.delete<br>- compute.snapshots.get<br>- compute.snapshots.list<br>- compute.snapshots.setLabels | To create and manage persistent disk snapshots. |
| - compute.networks.get<br>- compute.networks.list<br>- compute.regions.get<br>- compute.regions.list<br>- compute.subnetworks.get<br>- compute.subnetworks.list<br>- compute.zoneOperations.get<br>- compute.zones.get<br>- compute.zones.list | To get the networking information needed to create a new Cloud Volumes ONTAP virtual machine instance. |
| - deploymentmanager.compositeTypes.get<br>- deploymentmanager.compositeTypes.list<br>- deploymentmanager.deployments.create<br>- deploymentmanager.deployments.delete<br>- deploymentmanager.deployments.get<br>- deploymentmanager.deployments.list<br>- deploymentmanager.manifests.get<br>- deploymentmanager.manifests.list<br>- deploymentmanager.operations.get<br>- deploymentmanager.operations.list<br>- deploymentmanager.resources.get<br>- deploymentmanager.resources.list<br>- deploymentmanager.typeProviders.get<br>- deploymentmanager.typeProviders.list<br>- deploymentmanager.types.get<br>- deploymentmanager.types.list | To deploy the Cloud Volumes ONTAP virtual machine instance using Google Cloud Deployment Manager. |

| Actions | Purpose |
| --- | --- |
| - logging.logEntries.list<br>- logging.privateLogEntries.list | To get stack log drives. |
| - resourcemanager.projects.get | To support multi-projects. |
| - storage.buckets.create<br>- storage.buckets.delete<br>- storage.buckets.get<br>- storage.buckets.list | To create and manage a Google Cloud Storage bucket for data tiering. |
| - cloudkms.cryptoKeyVersions.useToEncrypt<br>- cloudkms.cryptoKeys.get<br>- cloudkms.cryptoKeys.list<br>- cloudkms.keyRings.list | To use customer-managed encryption keys from the Cloud Key Management Service with Cloud Volumes ONTAP. |

# Default configurations

Details about how Cloud Manager and Cloud Volumes ONTAP are configured by default can help you administer the systems.

## Default configuration for Cloud Manager on Linux

If you need to troubleshoot Cloud Manager or your Linux host, it might help to understand how Cloud Manager is configured.

- If you deployed Cloud Manager from NetApp Cloud Central (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 Cloud Manager image is Red Hat Enterprise Linux 7.4 (HVM).

    The operating system does not include a GUI. You must use a terminal to access the system.
- The Cloud Manager 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
  - Java

- Kubectl
- MySQL
- Tridentctl
- Wget

## 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.

- Cloud Volumes ONTAP is available as a single-node system in AWS, Azure, and GCP, and as an HA pair in AWS and Azure.
- Cloud Manager creates one data-serving SVM when it deploys Cloud Volumes ONTAP. Using multiple data-serving SVMs is not supported.
- 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, 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 Cloud Manager using HTTPS.

  When logged in to Cloud Manager, the backups are accessible from https://ipaddress/occm/offboxconfig/

- 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<br>The Account Admin can modify this value from the Settings page. |
| Security style | NTFS for CIFS volumes<br>UNIX for NFS volumes |
| Space guarantee style | none |
| UNIX permissions (NFS only) | 777 |

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

## Boot and root data for Cloud Volumes ONTAP

In addition to the storage for user data, Cloud Manager also purchases cloud storage for boot and root data on each Cloud Volumes ONTAP system.

### AWS

- Two General Purpose SSD disks:
  - One 140 GB disk for root data (one per node)
  - 9.6 and later: One 86 GB disk for boot data (one per node)
  - 9.5 and earlier: One 45 GB disk for boot data (one per node)
- 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)

- Two Premium SSD disks:
  - One 90 GB disk for boot data
  - One 140 GB disk for root data
- One Azure snapshot for each boot disk and root disk

### Azure (HA pairs)

- Two 90 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 128 GB Standard HDD disks for saving cores (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 216 GB Standard persistent disk for saving cores
- One GCP snapshot each for the boot disk and root disk

**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.

# Roles

The Account Admin and Workspace Admin roles provide specific permissions to users.

| Task | Account Admin | Workspace Admin |
|---|---|---|
| Manage working environments | Yes | Yes, for associated workspaces |
| View data replication status | Yes | Yes, for associated workspaces |
| View the timeline | Yes | Yes, for associated workspaces |
| Delete working environments | Yes | No |
| Connect Kubernetes clusters to Cloud Volumes ONTAP | Yes | No |
| Receive the Cloud Volumes ONTAP report | Yes | No |
| Manage Cloud Central accounts | Yes | No |
| Manage cloud provider accounts | Yes | No |

| Task | Account Admin | Workspace Admin |
|---|---|---|
| Modify Cloud Manager settings | Yes | No |
| View and manage the Support Dashboard | Yes | No |
| Remove working environments from Cloud Manager | Yes | No |
| Update Cloud Manager | Yes | No |
| Install an HTTPS certificate | Yes | No |
| Set up Active Directory | Yes | No |

**Related links**

- Setting up workspaces and users in the Cloud Central account
- Managing workspaces and users in the Cloud Central account

# 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.

- 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
- 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.es how to quickly activate a destination SVM after a disaster, and then reactivate the source SVM.

- 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 Cloud Volumes ONTAP Support

  Access support resources to get help and troubleshoot issues with 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 are not running the latest version.

Cloud Manager 3.6

# 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 3.7.4
- Notice for Cloud Manager 3.7.1
- Notice for Cloud Manager 3.7
- Notice for the Cloud Backup Service

## Copyright information



## Trademark information