



# **Get started with Cloud Manager**

## Cloud Manager

NetApp  
September 09, 2021

This PDF was generated from [https://docs.netapp.com/us-en/occm/concept\\_overview.html](https://docs.netapp.com/us-en/occm/concept_overview.html) on September 09, 2021. Always check docs.netapp.com for the latest.

# Table of Contents

- Get started with Cloud Manager . . . . . 1
  - Learn about Cloud Manager . . . . . 1
  - Getting started checklist . . . . . 2
  - Signing up to NetApp Cloud Central . . . . . 4
  - Logging in to Cloud Manager . . . . . 5
  - Set up a Cloud Central account . . . . . 6
  - Set up a Connector . . . . . 15
  - Where to go next . . . . . 36

# Get started with Cloud Manager

## Learn about Cloud Manager

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

### Features

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

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

[Learn more about Cloud Manager.](#)

### Supported object storage providers

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

### Cost

Cloud Manager software is free of charge from NetApp.

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

### How Cloud Manager works

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

#### Software-as-a-service

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

#### NetApp Cloud Central

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

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

## Connectors

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

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

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

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

## Getting started checklist

This checklist describes what's needed to get up and running with Cloud Manager.

### A NetApp Cloud Central login

You need to sign up to [NetApp Cloud Central](#) so you can access Cloud Manager and other cloud services.

### Network access from a web browser to several endpoints

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

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

### A network location for a Connector

After logging in to Cloud Manager, an Account Admin will need to deploy a *Connector* in a cloud provider or in your on-premises network. The Connector enables Cloud Manager to manage resources and processes within your public cloud environment. A Connector isn't required for Azure NetApp Files, Cloud Volumes Service, or Cloud Sync, but it is required for all other services and features in Cloud Manager. [Learn more about Connectors and how they work.](#)

- The network location must have an outbound internet connection.

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

[View the specific endpoints that the Connector contacts.](#)

- There's no incoming traffic to the Connector, unless you initiate it.

HTTP (80) and HTTPS (443) provide access to the local UI, which you'll use in rare circumstances. SSH (22) is only needed if you need to connect to the host for troubleshooting.

## Cloud provider permissions

You need an account that has permissions to deploy the Connector in your cloud provider directly from Cloud Manager.



There are alternative ways to create a Connector. You also have the option to create a Connector from the [AWS Marketplace](#), [Azure Marketplace](#), or to [manually install the software](#).

Location	High-level steps	Detailed steps
AWS	<ol style="list-style-type: none"><li>1. Use a JSON file that includes the required permissions to create an IAM policy in AWS.</li><li>2. Attach the policy to the IAM user who will create the Connector from Cloud Manager.</li><li>3. When you create the Connector, provide Cloud Manager with the AWS access key and secret key for the IAM user that has the required permissions.</li></ol>	<a href="#">Click here to view detailed steps.</a>
Azure	<ol style="list-style-type: none"><li>1. Use a JSON file that includes the required permissions to create a custom role in Azure.</li><li>2. Assign the role to the user who will create the Connector from Cloud Manager.</li><li>3. When you create the Connector, log in with the Microsoft account that has the required permissions (the login prompt that is owned and hosted by Microsoft).</li></ol>	<a href="#">Click here to view detailed steps.</a>
Google Cloud	<ol style="list-style-type: none"><li>1. Use a YAML file that includes the required permissions to create a custom role in Google Cloud.</li><li>2. Attach that role to the user who will create the Connector from Cloud Manager.</li><li>3. If you plan to use Cloud Volumes ONTAP, set up a service account that has the required permissions.</li><li>4. Enable Google Cloud APIs.</li><li>5. When you create the Connector, log in with the Google account that has the required permissions (the login prompt is owned and hosted by Google).</li></ol>	<a href="#">Click here to view detailed steps.</a>

## Networking for individual services

Now that your setup is complete, you're ready to start using the services available from Cloud Manager. Note that each service has its own networking requirements. Refer to the following pages for more details.

- [Cloud Volumes ONTAP for AWS](#)
- [Cloud Volumes ONTAP for Azure](#)
- [Cloud Volumes ONTAP for GCP](#)
- [Data replication between ONTAP systems](#)
- [Cloud Data Sense for Cloud Volumes ONTAP, on-premises ONTAP, or Azure NetApp Files](#)
- [Cloud Data Sense for Amazon S3](#)
- [Cloud Data Sense for generic S3 object storage](#)
- [Cloud Data Sense for non-NetApp NFS or CIFS file shares](#)
- [Cloud Data Sense for databases](#)
- [Cloud Data Sense for OneDrive accounts](#)
- [On-prem ONTAP clusters](#)
  - [Data tiering from ONTAP clusters to Amazon S3](#)
  - [Data tiering from ONTAP clusters to Azure Blob storage](#)
  - [Data tiering from ONTAP clusters to Google Cloud Storage](#)
  - [Data tiering from ONTAP clusters to StorageGRID](#)
  - [Data backup from ONTAP clusters to Amazon S3 or Azure Blob storage](#)

## Signing up to NetApp Cloud Central

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



You can use single sign-on to log in using credentials from your corporate directory (federated identity). To learn more, go to the [Cloud Central Help Center](#) and then click **Cloud Central sign-in options**.

### Steps

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

## Log In to NetApp Cloud Central

---

Already signed up? [Login](#)

*\*optional*

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

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

### Result

You now have an active Cloud Central user login.

## Logging in to Cloud Manager

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



You can use single sign-on to log in using credentials from your corporate directory (federated identity). To learn more, go to the [Cloud Central Help Center](#) and then click **Cloud Central sign-in options**.

### Steps

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



[Continue to Cloud Manager](#)

## Log In to NetApp Cloud Central

---

Don't have an account yet? [Sign Up](#)

LOGIN

[Forgot your password?](#)

## Set up a Cloud Central account

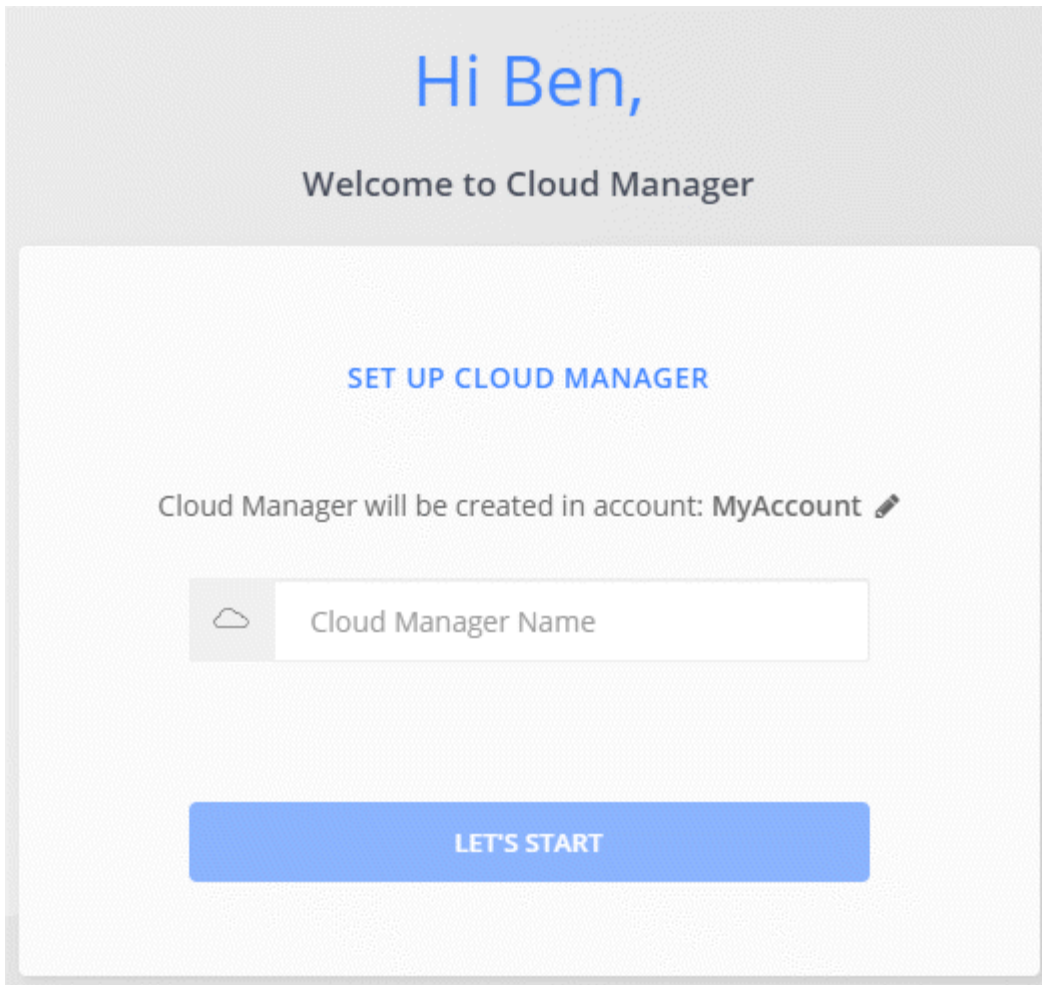
### Account settings: users, workspaces, Connectors, and subscriptions

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

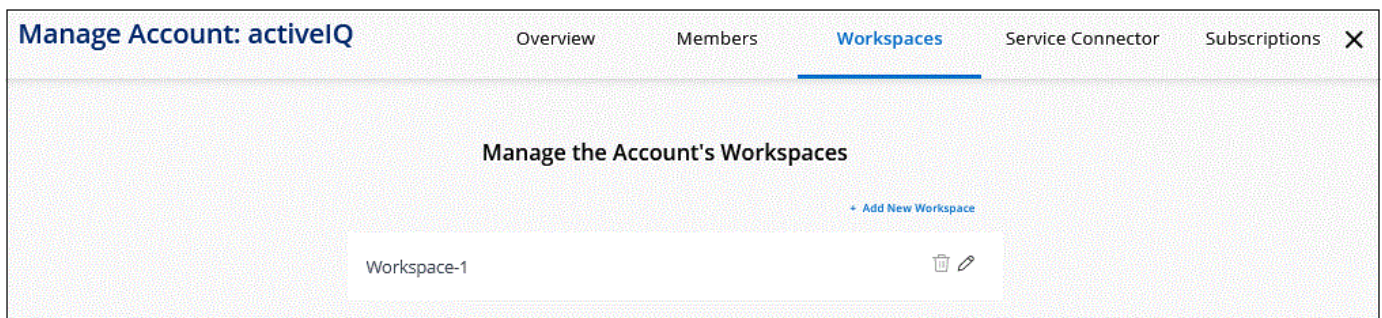
For example, multiple users can deploy and manage Cloud Volumes ONTAP systems in isolated environments called *workspaces*. These workspaces are invisible to other users, unless they are shared.

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





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



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

## Account Settings

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

## Overview

The Overview page shows the Account Name and the Account ID. You may need to provide your Account ID when registering some services. This page also includes some Cloud Manager configuration options.

## Members

The members 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.
- *Compliance Viewer*: Can only view Cloud Data Sense compliance information and generate reports for systems that they have permission to access.
- *SnapCenter Admin*: Can use the SnapCenter Service to create application consistent backups and restore data using those backups. *This service is currently in Beta.*

## Workspaces

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

A working environment represents a storage system:

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

## Connectors

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

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

## Subscriptions

These are the NetApp subscriptions associated with the selected account.

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

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

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

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

## Examples

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

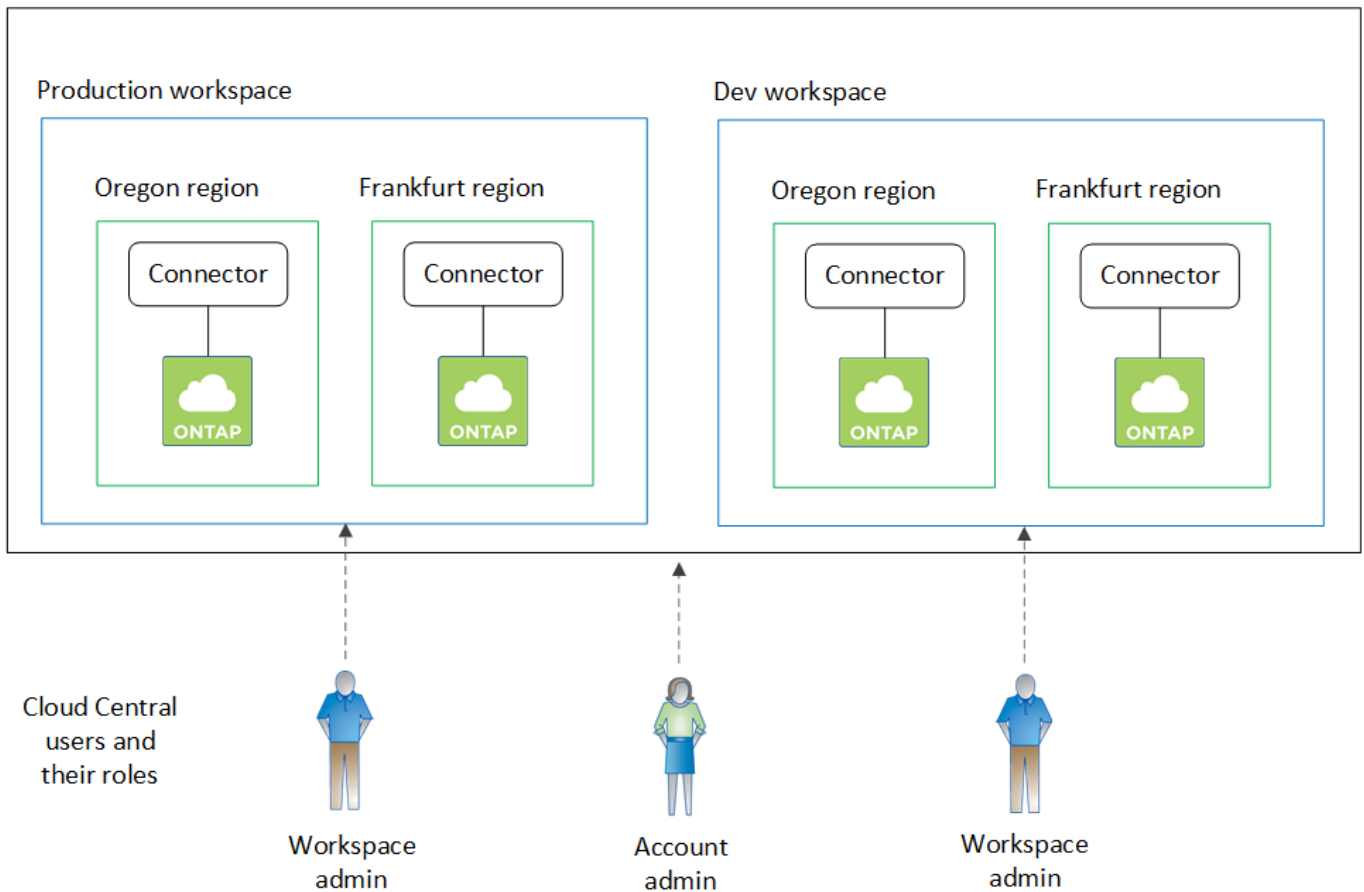


In both example images that follow, the Connector and the Cloud Volumes ONTAP systems don't actually reside *in* the NetApp Cloud Central account—they're running in a cloud provider. This is a conceptual representation of the relationship between each component.

### Example 1

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

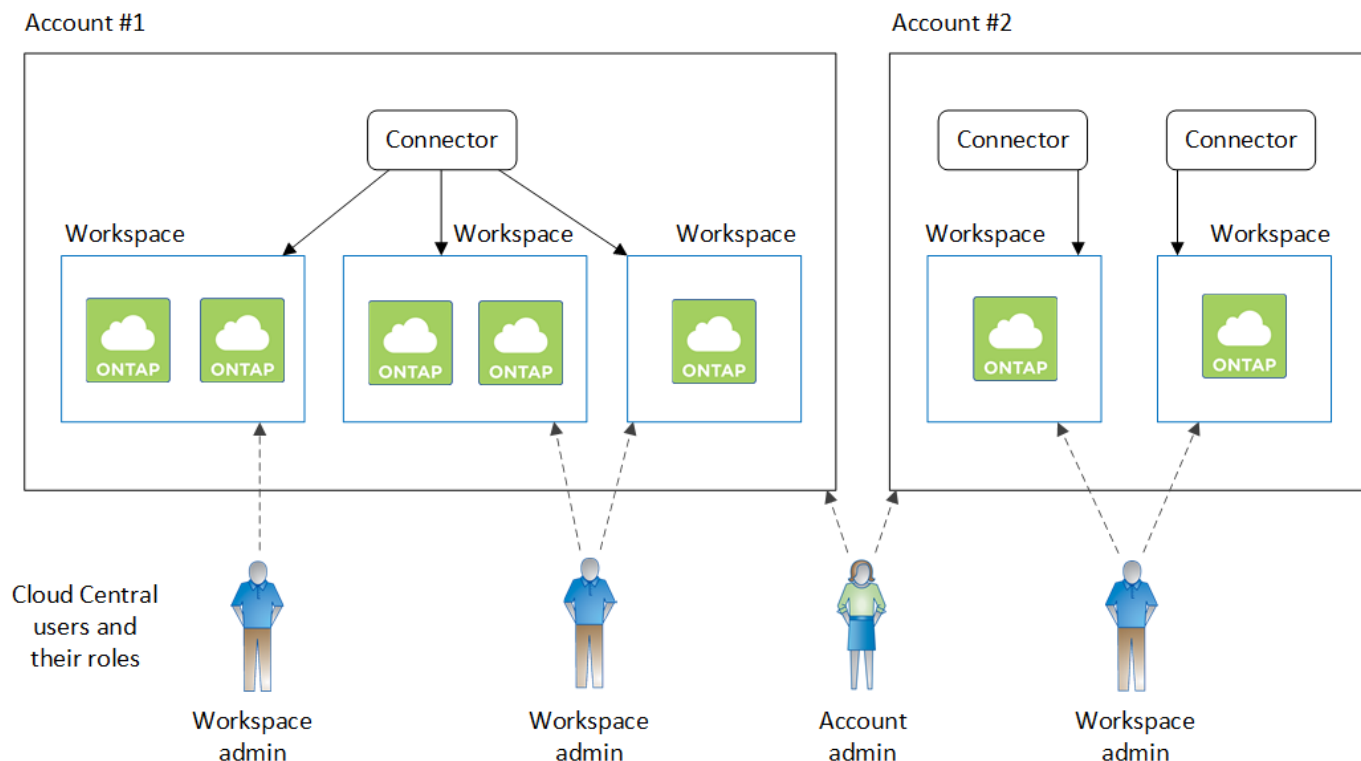
#### Account



### Example 2

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

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



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

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

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

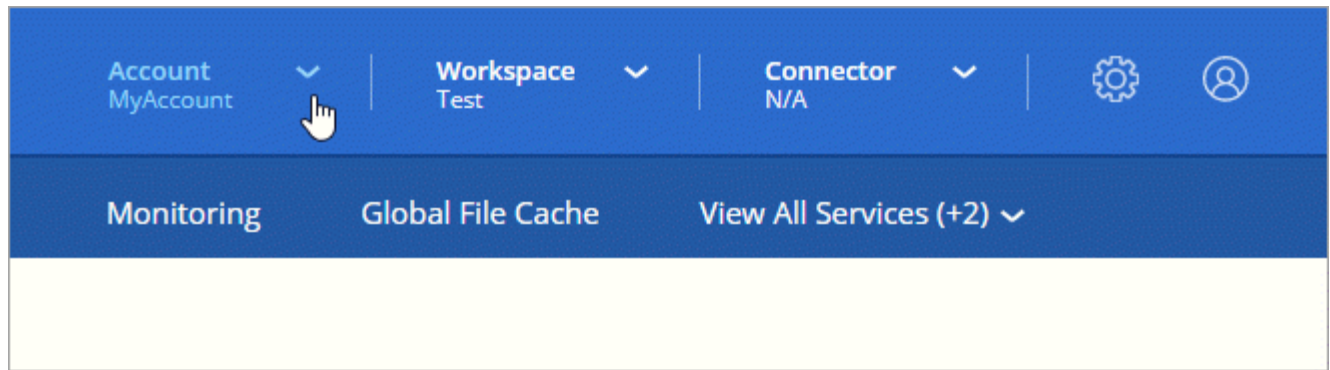
Set up your Cloud Central account so users can access Cloud Manager and access the working environments in a workspace. Just add a single user or add multiple users and workspaces.

### Adding workspaces

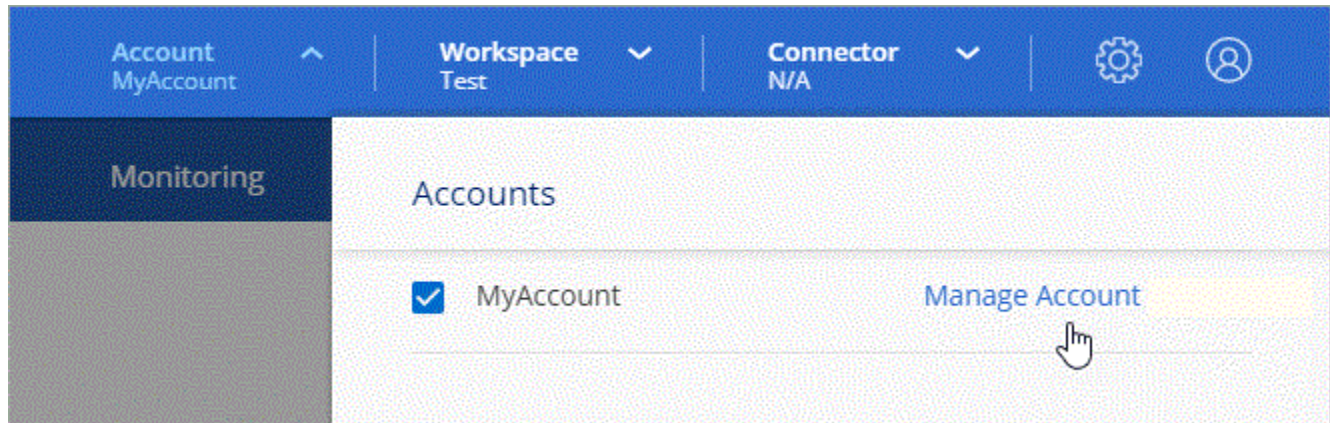
In Cloud Manager, workspaces enable you to isolate a set of working environments from other working environments and from other users. For example, you can create two workspaces and associate separate users with each workspace.

#### Steps

1. From the top of [Cloud Manager](#), click the **Account** drop-down.



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



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

### After you finish

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

### Adding users

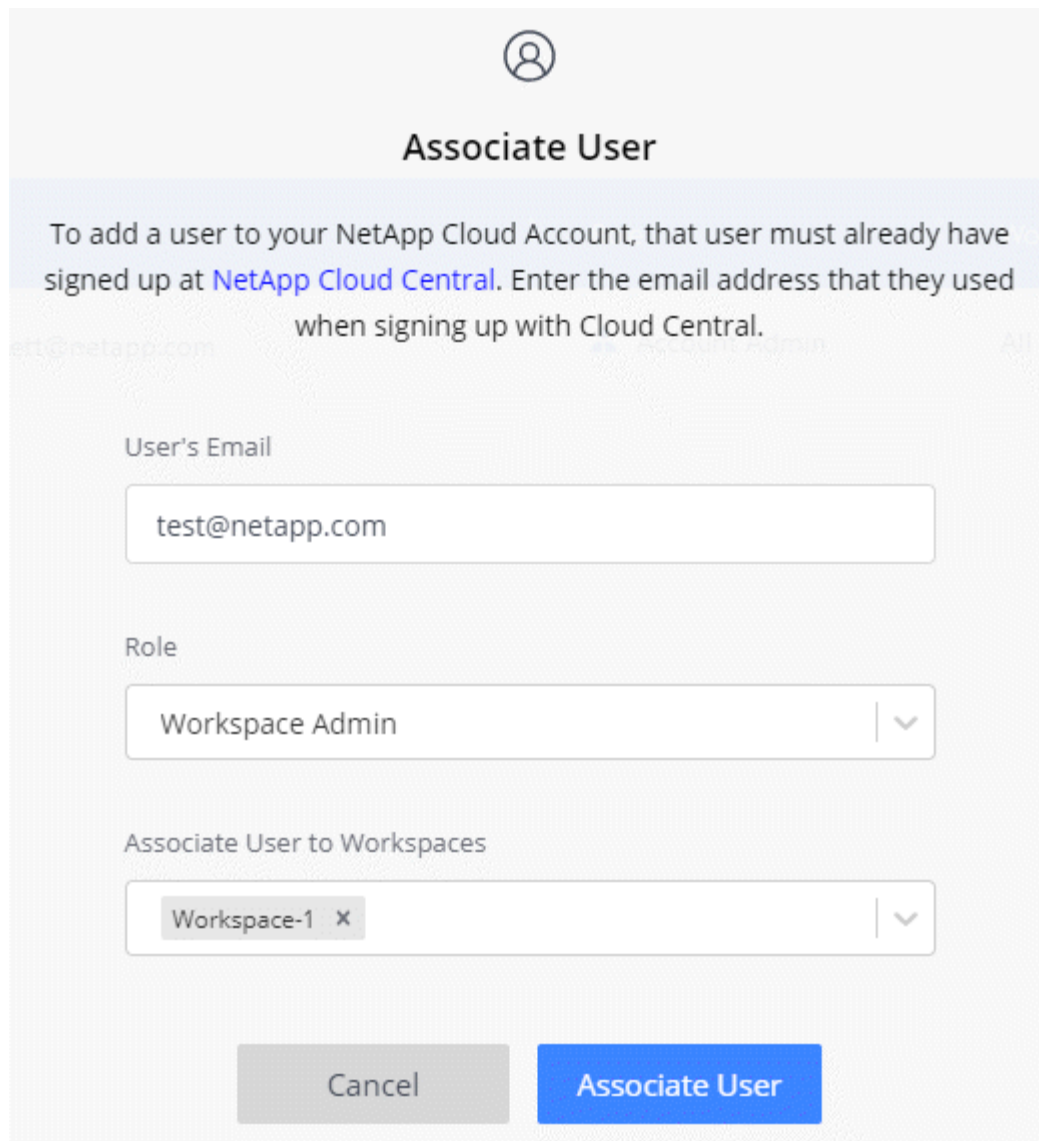
Associate Cloud Central users with the Cloud Central account so those users can create and manage working environments in Cloud Manager.

### Steps


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



3. From the Members tab, click **Associate User**.
4. Enter the user's email address and select a role for the user:
  - **Account Admin**: Can perform any action in Cloud Manager.
  - **Workspace Admin**: Can create and manage resources in assigned workspaces.
  - **Compliance Viewer**: Can only view Cloud Data Sense governance and compliance information and generate reports for workspaces that they have permission to access.
  - **SnapCenter Admin**: Can use the SnapCenter Service to create application consistent backups and restore data using those backups. This service is currently in Beta.
5. If you selected an account other than Account Admin, select one or more workspaces to associate with that user.



The image shows a modal dialog box titled "Associate User" with a user icon at the top. The main text explains that to add a user to a NetApp Cloud Account, the user must have signed up at NetApp Cloud Central and provides the email address used. The form contains three fields: "User's Email" with the value "test@netapp.com", "Role" with a dropdown menu showing "Workspace Admin", and "Associate User to Workspaces" with a dropdown menu showing "Workspace-1". At the bottom are "Cancel" and "Associate User" buttons.



### Associate User

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

User's Email

test@netapp.com

Role

Workspace Admin

Associate User to Workspaces

Workspace-1

Cancel Associate User

6. Click **Associate**.

#### Result

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

#### Associating Workspace Admins with workspaces

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

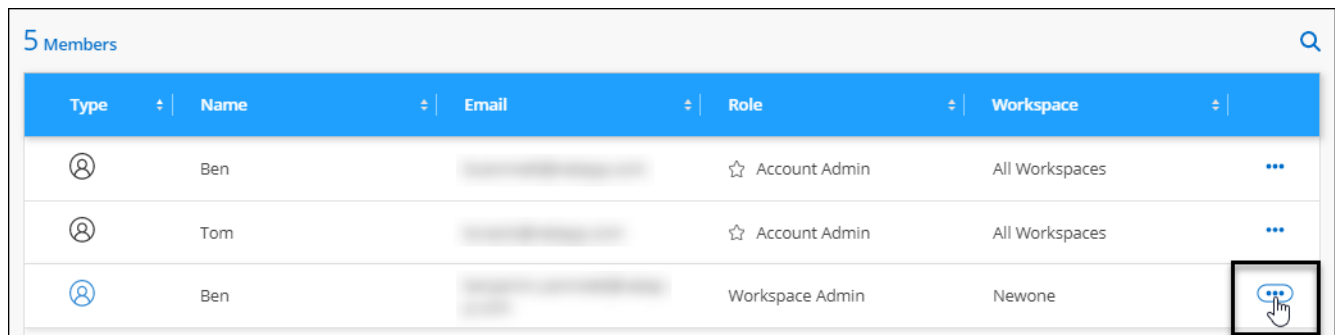
#### Steps

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





2. From the Members tab, 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 Connector was also associated with the workspaces.

## Associating Connectors with workspaces

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

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

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

## Steps

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





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

### Result

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

### What's next?

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

## Set up a Connector

### Learn about Connectors

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

### When a Connector is required

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

- Cloud Volumes ONTAP
- On-premises ONTAP clusters
- Cloud Data Sense
- Kubernetes
- Cloud Backup
- Monitoring
- Tiering on-prem data
- Global File Cache
- Amazon S3 bucket discovery
- Amazon FSx for ONTAP advanced management features

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



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

## Supported locations

A Connector is supported in the following locations:

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



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

## Connectors should remain running

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

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

## How to create a Connector

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

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

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

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

## Permissions

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

## Permissions to create a Connector

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

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

## Permissions for the Connector instance

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

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

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

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

## When to use multiple Connectors

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

Here are a few examples:

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

## Using multiple Connectors with the same working environment

You can manage a working environment with multiple Connectors at the same time for disaster recovery purposes. If one Connector goes down, you can switch to the other Connector to immediately manage the working environment.

To set up this configuration:

1. [Switch to another Connector](#)
2. Discover the existing working environment.
  - [Adding existing Cloud Volumes ONTAP systems to Cloud Manager](#)
  - [Discovering ONTAP clusters](#)
3. Set the [Capacity Management Mode](#) to **Manual** on any additional Connectors.

Only the main Connector should be set to **Automatic Mode**. If you switch to another Connector for DR purposes, then you can change the Capacity Management Mode as needed.

## When to switch between Connectors

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

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

## The local user interface

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

- [Setting a proxy server](#)
- Installing a patch (you'll typically work with NetApp personnel to install a patch)
- Downloading AutoSupport messages (usually directed by NetApp personnel when you have issues)

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

## Connector upgrades

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

## Networking requirements for the Connector

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



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

## Connection to target networks

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

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

## Possible conflict with IP addresses in the 172 range

If your network has a subnet configured in the 172 range, then you might experience connectivity failures from Cloud Manager. [Learn more about this known issue.](#)

## Outbound internet access

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

The following sections identify the specific endpoints.

### Endpoints to manage resources in AWS

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



If your VPC uses a network access control list (ACL) to filter traffic, then make sure that you enable these endpoints for both outbound and inbound traffic.

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

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

### Endpoints to manage resources in Azure

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

Endpoints	Purpose
<a href="https://management.azure.com">https://management.azure.com</a> <a href="https://login.microsoftonline.com">https://login.microsoftonline.com</a>	Enables Cloud Manager to deploy and manage Cloud Volumes ONTAP in most Azure regions.
<a href="https://management.microsoftazure.de">https://management.microsoftazure.de</a> <a href="https://login.microsoftonline.de">https://login.microsoftonline.de</a>	Enables Cloud Manager to deploy and manage Cloud Volumes ONTAP in the Azure Germany regions.
<a href="https://management.usgovcloudapi.net">https://management.usgovcloudapi.net</a> <a href="https://login.microsoftonline.com">https://login.microsoftonline.com</a>	Enables Cloud Manager to deploy and manage Cloud Volumes ONTAP in the Azure US Gov regions.
<a href="https://api.services.cloud.netapp.com:443">https://api.services.cloud.netapp.com:443</a>	API requests to NetApp Cloud Central.
<a href="https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com">https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com</a>	Provides access to software images, manifests, and templates.

Endpoints	Purpose
<a href="https://cognito-idp.us-east-1.amazonaws.com">https://cognito-idp.us-east-1.amazonaws.com</a> <a href="https://cognito-identity.us-east-1.amazonaws.com">https://cognito-identity.us-east-1.amazonaws.com</a> <a href="https://sts.amazonaws.com">https://sts.amazonaws.com</a> <a href="https://cloud-support-netapp-com-accelerated.s3.amazonaws.com">https://cloud-support-netapp-com-accelerated.s3.amazonaws.com</a>	Enables the Connector to access and download manifests, templates, and Cloud Volumes ONTAP upgrade images.
<a href="https://cloudmanagerinfraprod.azurecr.io">https://cloudmanagerinfraprod.azurecr.io</a> <a href="https://*.blob.core.windows.net">*.blob.core.windows.net</a>	Access to software images of container components for an infrastructure that's running Docker and provides a solution for service integrations with Cloud Manager.
<a href="https://kinesis.us-east-1.amazonaws.com">https://kinesis.us-east-1.amazonaws.com</a>	Enables NetApp to stream data from audit records.
<a href="https://cloudmanager.cloud.netapp.com">https://cloudmanager.cloud.netapp.com</a>	Communication with the Cloud Manager service, which includes Cloud Central accounts.
<a href="https://netapp-cloud-account.auth0.com">https://netapp-cloud-account.auth0.com</a>	Communication with NetApp Cloud Central for centralized user authentication.
<a href="https://support.netapp.com:443">support.netapp.com:443</a> <a href="https://mysupport.netapp.com">https://mysupport.netapp.com</a>	Communication with NetApp AutoSupport. Note that the Connector communicates with <a href="https://support.netapp.com:443">support.netapp.com:443</a> , which redirects to <a href="https://mysupport.netapp.com">https://mysupport.netapp.com</a> .
<a href="https://support.netapp.com/svcgw">https://support.netapp.com/svcgw</a> <a href="https://support.netapp.com/ServiceGW/entitlement">https://support.netapp.com/ServiceGW/entitlement</a> <a href="https://eval.lic.netapp.com.s3.us-west-1.amazonaws.com">https://eval.lic.netapp.com.s3.us-west-1.amazonaws.com</a> <a href="https://cloud-support-netapp-com.s3.us-west-1.amazonaws.com">https://cloud-support-netapp-com.s3.us-west-1.amazonaws.com</a>	Communication with NetApp for system licensing and support registration.
<a href="https://client.infra.support.netapp.com.s3.us-west-1.amazonaws.com">https://client.infra.support.netapp.com.s3.us-west-1.amazonaws.com</a> <a href="https://cloud-support-netapp-com-accelerated.s3.us-west-1.amazonaws.com">https://cloud-support-netapp-com-accelerated.s3.us-west-1.amazonaws.com</a> <a href="https://trigger.asup.netapp.com.s3.us-west-1.amazonaws.com">https://trigger.asup.netapp.com.s3.us-west-1.amazonaws.com</a>	Enables NetApp to collect information needed to troubleshoot support issues.
<a href="https://ipa-signer.cloudmanager.netapp.com">https://ipa-signer.cloudmanager.netapp.com</a>	Enables Cloud Manager to generate licenses (for example, a FlexCache license for Cloud Volumes ONTAP)
<a href="https://*.blob.core.windows.net">*.blob.core.windows.net</a>	Required for HA pairs when using a proxy.
<p>Various third-party locations, for example:</p> <ul style="list-style-type: none"> <li><a href="https://repo1.maven.org/maven2">https://repo1.maven.org/maven2</a></li> <li><a href="https://oss.sonatype.org/content/repositories">https://oss.sonatype.org/content/repositories</a></li> <li><a href="https://repo.typesafe.com">https://repo.typesafe.com</a></li> </ul> <p>Third-party locations are subject to change.</p>	During upgrades, Cloud Manager downloads the latest packages for third-party dependencies.

## Endpoints to manage resources in GCP

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

Endpoints	Purpose
<a href="https://www.googleapis.com">https://www.googleapis.com</a>	Enables the Connector to contact Google APIs for deploying and managing Cloud Volumes ONTAP in GCP.
<a href="https://api.services.cloud.netapp.com:443">https://api.services.cloud.netapp.com:443</a>	API requests to NetApp Cloud Central.
<a href="https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com">https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com</a>	Provides access to software images, manifests, and templates.
<a href="https://cognito-idp.us-east-1.amazonaws.com">https://cognito-idp.us-east-1.amazonaws.com</a> <a href="https://cognito-identity.us-east-1.amazonaws.com">https://cognito-identity.us-east-1.amazonaws.com</a> <a href="https://sts.amazonaws.com">https://sts.amazonaws.com</a> <a href="https://cloud-support-netapp-com-accelerated.s3.amazonaws.com">https://cloud-support-netapp-com-accelerated.s3.amazonaws.com</a>	Enables the Connector to access and download manifests, templates, and Cloud Volumes ONTAP upgrade images.
<a href="https://cloudmanagerinfraproduct.azurecr.io">https://cloudmanagerinfraproduct.azurecr.io</a> <a href="https://blob.core.windows.net">*.blob.core.windows.net</a>	Access to software images of container components for an infrastructure that's running Docker and provides a solution for service integrations with Cloud Manager.
<a href="https://kinesis.us-east-1.amazonaws.com">https://kinesis.us-east-1.amazonaws.com</a>	Enables NetApp to stream data from audit records.
<a href="https://cloudmanager.cloud.netapp.com">https://cloudmanager.cloud.netapp.com</a>	Communication with the Cloud Manager service, which includes Cloud Central accounts.
<a href="https://netapp-cloud-account.auth0.com">https://netapp-cloud-account.auth0.com</a>	Communication with NetApp Cloud Central for centralized user authentication.
<a href="https://support.netapp.com:443">support.netapp.com:443</a> <a href="https://mysupport.netapp.com">https://mysupport.netapp.com</a>	Communication with NetApp AutoSupport. Note that the Connector communicates with <a href="https://support.netapp.com:443">support.netapp.com:443</a> , which redirects to <a href="https://mysupport.netapp.com">https://mysupport.netapp.com</a> .
<a href="https://support.netapp.com/svcgw">https://support.netapp.com/svcgw</a> <a href="https://support.netapp.com/ServiceGW/entitlement">https://support.netapp.com/ServiceGW/entitlement</a> <a href="https://eval.lic.netapp.com.s3.us-west-1.amazonaws.com">https://eval.lic.netapp.com.s3.us-west-1.amazonaws.com</a> <a href="https://cloud-support-netapp-com.s3.us-west-1.amazonaws.com">https://cloud-support-netapp-com.s3.us-west-1.amazonaws.com</a>	Communication with NetApp for system licensing and support registration.
<a href="https://client.infra.support.netapp.com.s3.us-west-1.amazonaws.com">https://client.infra.support.netapp.com.s3.us-west-1.amazonaws.com</a> <a href="https://cloud-support-netapp-com-accelerated.s3.us-west-1.amazonaws.com">https://cloud-support-netapp-com-accelerated.s3.us-west-1.amazonaws.com</a> <a href="https://trigger.asup.netapp.com.s3.us-west-1.amazonaws.com">https://trigger.asup.netapp.com.s3.us-west-1.amazonaws.com</a>	Enables NetApp to collect information needed to troubleshoot support issues.
<a href="https://ipa-signer.cloudmanager.netapp.com">https://ipa-signer.cloudmanager.netapp.com</a>	Enables Cloud Manager to generate licenses (for example, a FlexCache license for Cloud Volumes ONTAP)



Endpoints	Purpose
<p>Various third-party locations, for example:</p> <ul style="list-style-type: none"> <li>• <a href="https://repo1.maven.org/maven2">https://repo1.maven.org/maven2</a></li> <li>• <a href="https://oss.sonatype.org/content/repositories">https://oss.sonatype.org/content/repositories</a></li> <li>• <a href="https://repo.typesafe.com">https://repo.typesafe.com</a></li> </ul> <p>Third-party locations are subject to change.</p>	<p>During upgrades, Cloud Manager downloads the latest packages for third-party dependencies.</p>

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

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

- <http://dev.mysql.com/get/mysql-community-release-el7-5.noarch.rpm>
- <https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm>
- <https://s3.amazonaws.com/aws-cli/awscli-bundle.zip>
- [\\*.blob.core.windows.net](http://*.blob.core.windows.net)

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

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

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

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

Endpoints	Purpose
https://widget.intercom.io	For in-product chat that enables you to talk to NetApp cloud experts.

## Ports and security groups

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

### Rules for the Connector in AWS

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

#### Inbound rules

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

#### Outbound rules

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

#### Basic outbound rules

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

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

#### Advanced outbound rules

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



The source IP address is the Connector host.

Service	Protocol	Port	Destination	Purpose
Active Directory	TCP	88	Active Directory forest	Kerberos V authentication
	TCP	139	Active Directory forest	NetBIOS service session
	TCP	389	Active Directory forest	LDAP
	TCP	445	Active Directory forest	Microsoft SMB/CIFS over TCP with NetBIOS framing
	TCP	464	Active Directory forest	Kerberos V change & set password (SET_CHANGE)
	TCP	749	Active Directory forest	Active Directory Kerberos V change & set password (RPCSEC_GSS)
	UDP	137	Active Directory forest	NetBIOS name service
	UDP	138	Active Directory forest	NetBIOS datagram service
	UDP	464	Active Directory forest	Kerberos key administration
API calls and AutoSupport	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 Data Sense	HTTP	80	Cloud Data Sense instance	Cloud Data Sense for Cloud Volumes ONTAP

### Rules for the Connector in Azure

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

### Inbound rules

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

### Outbound rules

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

## Basic outbound rules

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

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

## Advanced outbound rules

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



The source IP address is the Connector host.

Service	Port	Protocol	Destination	Purpose
Active Directory	88	TCP	Active Directory forest	Kerberos V authentication
	139	TCP	Active Directory forest	NetBIOS service session
	389	TCP	Active Directory forest	LDAP
	445	TCP	Active Directory forest	Microsoft SMB/CIFS over TCP with NetBIOS framing
	464	TCP	Active Directory forest	Kerberos V change & set password (SET_CHANGE)
	749	TCP	Active Directory forest	Active Directory Kerberos V change & set password (RPCSEC_GSS)
	137	UDP	Active Directory forest	NetBIOS name service
	138	UDP	Active Directory forest	NetBIOS datagram service
	464	UDP	Active Directory forest	Kerberos key administration
API calls and AutoSupport	443	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 the Connector in GCP

The firewall rules for the Connector requires both inbound and outbound rules.

## Inbound rules

Protocol	Port	Purpose
SSH	22	Provides SSH access to the Connector host

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

## Outbound rules

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

### Basic outbound rules

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

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

### Advanced outbound rules

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



The source IP address is the Connector host.

Service	Protocol	Port	Destination	Purpose
Active Directory	TCP	88	Active Directory forest	Kerberos V authentication
	TCP	139	Active Directory forest	NetBIOS service session
	TCP	389	Active Directory forest	LDAP
	TCP	445	Active Directory forest	Microsoft SMB/CIFS over TCP with NetBIOS framing
	TCP	464	Active Directory forest	Kerberos V change & set password (SET_CHANGE)
	TCP	749	Active Directory forest	Active Directory Kerberos V change & set password (RPCSEC_GSS)
	UDP	137	Active Directory forest	NetBIOS name service
	UDP	138	Active Directory forest	NetBIOS datagram service
	UDP	464	Active Directory forest	Kerberos key administration
API calls and AutoSupport	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

## Creating a Connector in AWS from Cloud Manager

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

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

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



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

### Setting up AWS permissions to create a Connector

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

#### Steps

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

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



For IAM user permissions for Amazon FSx for ONTAP, see [Create an FSx for ONTAP working environment](#).

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

#### Result

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

### Creating a Connector in AWS

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

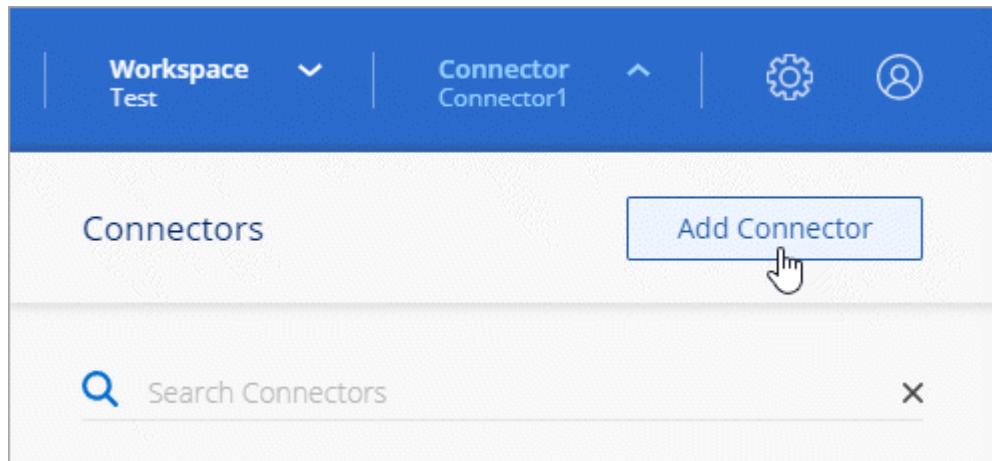
#### What you'll need

- An AWS access key and secret key for an IAM user who has the [required permissions](#) to create a Connector.
- A VPC, subnet, and keypair in your AWS region of choice.
- If you don't want Cloud Manager to automatically create an IAM role for the Connector, then you'll need to create your own [using this policy](#).

These permissions are for the Connector instance. It's a different set of permissions than what's provided in the first bullet above.

## Steps

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



2. Choose **Amazon Web Services** as your cloud provider and click **Continue**.

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

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

3. Follow the steps in the wizard to create the Connector:

- **Get Ready:** Review what you'll need.
- **AWS Credentials:** Specify the AWS access key and secret key that meet permissions requirements and then select your region.
- **Details:** Enter a name for the instance, specify tags, and choose whether you want Cloud Manager to create a new role that has the required permissions, or if you want to select an existing role that you set up with [the required permissions](#).
- **Network:** Specify a VPC, subnet, and key pair for the instance, choose whether to enable a public IP address, and optionally specify a proxy configuration.
- **Security Group:** Choose whether to create a new security group or whether to select an existing security group that allows inbound HTTP, HTTPS, and SSH access.



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

- **Review:** Review your selections to verify that your set up is correct.

4. Click **Add**.

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

## After you finish

You need to associate a Connector with workspaces so Workspace Admins can use those Connectors to create Cloud Volumes ONTAP systems. If you only have Account Admins, then associating the Connector with

workspaces isn't required. Account Admins have the ability to access all workspaces in Cloud Manager by default. [Learn more](#).

## Creating a Connector in Azure from Cloud Manager

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

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

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



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

### Setting up Azure permissions to create a Connector

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

#### Steps

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



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

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

#### Example

```
"AssignableScopes": [  
  "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz"  
],
```

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

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

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

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

2. Assign the role to the user who will deploy the Connector from Cloud Manager:
  - a. Open the **Subscriptions** service and select the user's subscription.



- b. Click **Access control (IAM)**.
- c. Click **Add > Add role assignment** and then add the permissions:
  - Select the **Azure SetupAsService** role.



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

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

## Result

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

## Creating a Connector in Azure

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

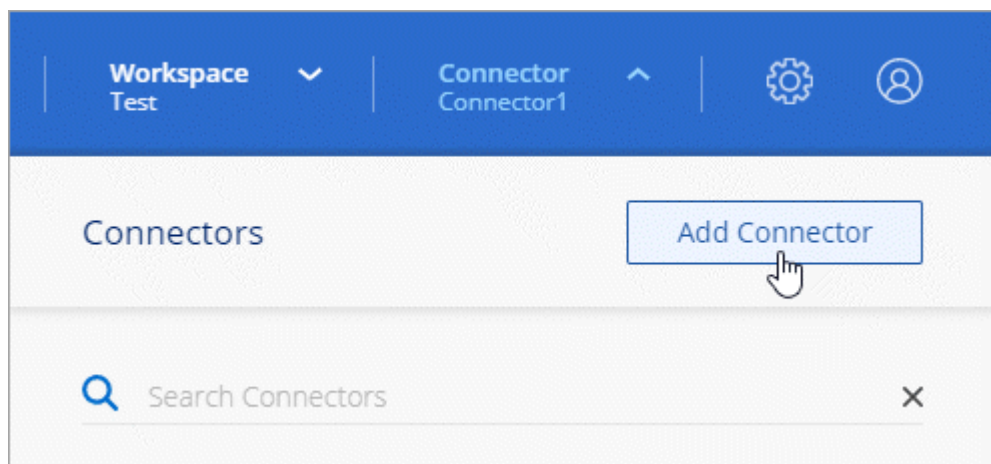
### What you'll need

- The [required permissions](#) for your Azure account.
- An Azure subscription.
- A VNet and subnet in your Azure region of choice.
- If you don't want Cloud Manager to automatically create an Azure role for the Connector, then you'll need to create your own [using this policy](#).

These permissions are for the Connector instance. It's a different set of permissions than what's provided in the first bullet above.

### Steps

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



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

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

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

3. Follow the steps in the wizard to create the Connector:

- **Get Ready:** Review what you'll need.
- If you're prompted, log in to your Microsoft account, which should have the required permissions to create the virtual machine.

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



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

- **VM Authentication:** Choose an Azure subscription, a location, a new resource group or an existing resource group, and then choose an authentication method.
- **Details:** Enter a name for the instance, specify tags, and choose whether you want Cloud Manager to create a new role that has the required permissions, or if you want to select an existing role that you set up with [the required permissions](#).

Note that you can choose the subscriptions associated with this role. Each subscription that you choose provides the Connector with permissions to deploy Cloud Volumes ONTAP in those subscriptions.

- **Network:** Choose a VNet and subnet, whether to enable a public IP address, and optionally specify a proxy configuration.
- **Security Group:** Choose whether to create a new security group or whether to select an existing security group that allows inbound HTTP, HTTPS, and SSH access.



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

- **Review:** Review your selections to verify that your set up is correct.

4. Click **Add**.

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

### After you finish

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

## Creating a Connector in GCP from Cloud Manager

An Account Admin needs to deploy a *Connector* before you can use most Cloud Manager

features. [Learn when a Connector is required](#). The Connector enables Cloud Manager to manage resources and processes within your public cloud environment.

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

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



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

## Setting up GCP permissions to create a Connector

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

### Steps

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

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

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

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

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

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

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

### Result

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

### Shared VPC Permissions

If you are using a shared VPC to deploy resources into a service project, then the following permissions are required. This table is for reference and your environment should reflect the permissions table when IAM configuration is complete.

Service Account	Creator	Hosted in	Service project permissions	Host project permissions	Purpose
Cloud Manager service account	Custom	Service project	<ul style="list-style-type: none"> <li>• <a href="#">The permissions found in this .yaml file</a></li> </ul>	<ul style="list-style-type: none"> <li>• compute.networkUser</li> <li>• deploymentmanager.editor</li> </ul>	Deploying and maintaining Cloud Volumes ONTAP and services in the service project
Cloud Volumes ONTAP service account	Custom	Service project	<ul style="list-style-type: none"> <li>• storage.admin</li> <li>• member: Cloud Manager service account as serviceAccount.user</li> </ul>	N/A	(Optional) For data tiering and Cloud Backup
Google APIs service agent	GCP	Service project	<ul style="list-style-type: none"> <li>• (Default) Editor</li> </ul>	<ul style="list-style-type: none"> <li>• compute.networkUser</li> </ul>	Interacts with GCP APIs on behalf of deployment. Allows Cloud Manager to use the shared network.
Google Compute Engine default service account	GCP	Service project	<ul style="list-style-type: none"> <li>• (Default) Editor</li> </ul>	<ul style="list-style-type: none"> <li>• compute.networkUser</li> </ul>	Deploys GCP instances and compute infrastructure on behalf of deployment. Allows Cloud Manager to use the shared network.

#### Notes:

1. deploymentmanager.editor is only required at the host project if you are not passing firewall rules to the deployment and are choosing to let Cloud Manager create them for you.
2. firewall.create and firewall.delete are only required if you are not passing firewall rules to the deployment and are choosing to let Cloud Manager create them for you.
3. For data tiering, the tiering service account must have the serviceAccount.user role on the service account, not just at the project level. Currently if you assign serviceAccount.user at the project level, the permissions don't show when you query the service account with getIAMPolicy.

## Enabling Google Cloud APIs

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

### Step

1. [Enable the following Google Cloud APIs in your project.](#)
  - Cloud Deployment Manager V2 API
  - Cloud Logging API
  - Cloud Resource Manager API
  - Compute Engine API

- Identity and Access Management (IAM) API

## Creating a Connector in GCP

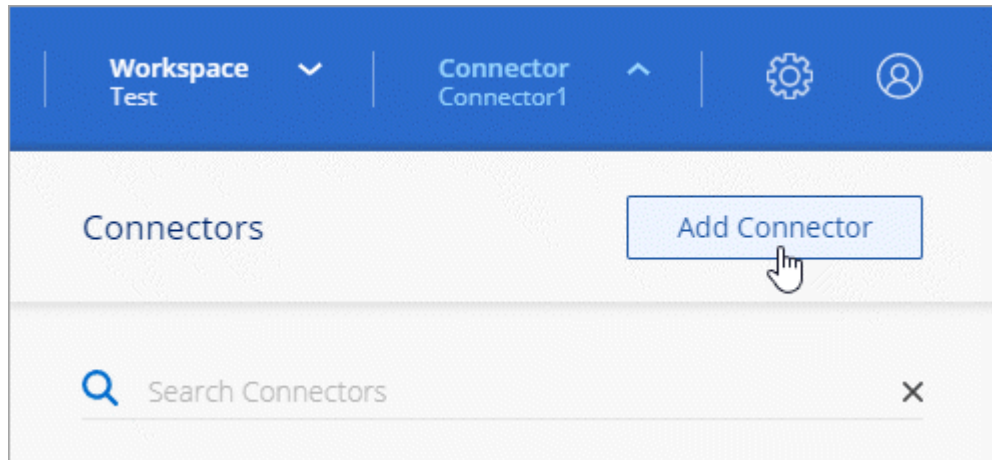
Cloud Manager enables you to create a Connector in GCP directly from its user interface.

### What you'll need

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

### Steps

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



2. Choose **Google Cloud Platform** as your cloud provider.

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

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

3. Follow the steps in the wizard to create the Connector:
  - **Get Ready:** Review what you'll need.
  - If you're prompted, log in to your Google account, which should have the required permissions to create the virtual machine instance.

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

- **Basic Settings:** Enter a name for the virtual machine instance, specify tags, select a project, and then select the service account that has the required permissions (refer to the section above for details).
- **Location:** Specify a region, zone, VPC, and subnet for the instance.
- **Network:** Choose whether to enable a public IP address and optionally specify a proxy configuration.
- **Firewall Policy:** Choose whether to create a new firewall policy or whether to select an existing firewall

policy that allows inbound HTTP, HTTPS, and SSH access.



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

- **Review:** Review your selections to verify that your set up is correct.

4. Click **Add**.

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

### After you finish

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

## Where to go next

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

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

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

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

## Copyright Information

Copyright © 2021 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means-graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system-without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

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

## Trademark Information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.