Set up a Connector

Cloud Manager

NetApp
November 10, 2020

Table of Contents

Set up a Connector

Learn about Connectors

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

When a Connector is required

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

- Cloud Volumes ONTAP
- On-premises ONTAP clusters
- Cloud Compliance
- Kubernetes
- Backup to Cloud
- Monitoring
- On-prem tiering
- Global File Cache
- Amazon S3 bucket discovery

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

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

Supported locations

A Connector is supported in the following locations:

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

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

Connectors should remain running

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

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

How to create a Connector

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

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

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

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

Permissions

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

Permissions to create a Connector

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

View policies for each cloud provider.

Permissions for the Connector instance

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

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

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

View policies for each cloud provider.

When to use multiple Connectors

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

Here are a few examples:

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

When to switch between Connectors

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

Learn how to switch between Connectors.

The local user interface

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

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

Learn how to access the local UI.

Connector upgrades

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

Networking requirements for the Connector

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

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

Connection to target networks

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

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

Outbound internet access

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

The following sections identify the specific endpoints.

Endpoints to manage resources in AWS

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

Endpoints	Purpose
AWS services (amazonaws.com): • CloudFormation • Elastic Compute Cloud (EC2) • Key Management Service (KMS) • Security Token Service (STS) • Simple Storage Service (S3) The exact endpoint depends on the region in which you deploy Cloud Volumes ONTAP. Refer to AWS documentation for details.	Enables the Connector 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.
https://repo.cloud.support.netapp.com	Used to download Cloud Manager dependencies.
http://repo.mysql.com/	Used to download MySQL.
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com https://sts.amazonaws.com https://cloud-support-netapp-com-accelerated.s3.amazonaws.com	Enables the Connector to access and download manifests, templates, and Cloud Volumes ONTAP upgrade images.
https://cloudmanagerinfraprod.azurecr.io	Access to software images of container components for an infrastructure that's running Docker and provides a solution for service integrations with Cloud Manager.
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.

Endpoints	Purpose
https://support.netapp.com/aods/asupmessage https://support.netapp.com/asupprod/post/1.0/postAsup	Communication with NetApp AutoSupport.
https://support.netapp.com/svcgw https://support.netapp.com/ServiceGW/entitlement https://eval.lic.netapp.com.s3.us-west-1.amazonaws.com https://cloud-support-netapp-com.s3.us-west-1.amazonaws.com	Communication with NetApp for system licensing and support registration.
https://client.infra.support.netapp.com.s3.us-west-1.amazonaws.com https://cloud-support-netapp-com-accelerated.s3.us-west-1.amazonaws.com https://trigger.asup.netapp.com.s3.us-west-1.amazonaws.com	Enables NetApp to collect information needed to troubleshoot support issues.
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 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: • https://repo1.maven.org/maven2 • https://oss.sonatype.org/content/repositories • https://repo.typesafe.com Third-party locations are subject to change.	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
https://management.azure.com https://login.microsoftonline.com	Enables Cloud Manager to deploy and manage Cloud Volumes ONTAP in most Azure regions.
https://management.microsoftazure.de https://login.microsoftonline.de	Enables Cloud Manager to deploy and manage Cloud Volumes ONTAP in the Azure Germany regions.
https://management.usgovcloudapi.net 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://repo.cloud.support.netapp.com	Used to download Cloud Manager dependencies.
http://repo.mysql.com/	Used to download MySQL.
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com https://sts.amazonaws.com https://cloud-support-netapp-com-accelerated.s3.amazonaws.com	Enables the Connector to access and download manifests, templates, and Cloud Volumes ONTAP upgrade images.
https://cloudmanagerinfraprod.azurecr.io	Access to software images of container components for an infrastructure that's running Docker and provides a solution for service integrations with Cloud Manager.
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 https://support.netapp.com/ServiceGW/entitlement https://eval.lic.netapp.com.s3.us-west-1.amazonaws.com https://cloud-support-netapp-com.s3.us-west-1.amazonaws.com	Communication with NetApp for system licensing and support registration.

Endpoints	Purpose
https://client.infra.support.netapp.com.s3.us-west-1.amazonaws.com https://cloud-support-netapp-com-accelerated.s3.us-west-1.amazonaws.com https://trigger.asup.netapp.com.s3.us-west-1.amazonaws.com	Enables NetApp to collect information needed to troubleshoot support issues.
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 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.
*.blob.core.windows.net	Required for HA pairs when using a proxy.
Various third-party locations, for example: • https://repo1.maven.org/maven2 • https://oss.sonatype.org/content/repositories • https://repo.typesafe.com Third-party locations are subject to change.	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
https://www.googleapis.com	Enables the Connector 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.
https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com	Provides access to software images, manifests, and templates.
https://repo.cloud.support.netapp.com	Used to download Cloud Manager dependencies.
http://repo.mysql.com/	Used to download MySQL.

Endpoints	Purpose
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com https://sts.amazonaws.com https://cloud-support-netapp-com-accelerated.s3.amazonaws.com	Enables the Connector to access and download manifests, templates, and Cloud Volumes ONTAP upgrade images.
https://cloudmanagerinfraprod.azurecr.io	Access to software images of container components for an infrastructure that's running Docker and provides a solution for service integrations with Cloud Manager.
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 https://support.netapp.com/ServiceGW/entitlement https://eval.lic.netapp.com.s3.us-west-1.amazonaws.com https://cloud-support-netapp-com.s3.us-west-1.amazonaws.com	Communication with NetApp for system licensing and support registration.
https://client.infra.support.netapp.com.s3.us-west-1.amazonaws.com https://cloud-support-netapp-com-accelerated.s3.us-west-1.amazonaws.com https://trigger.asup.netapp.com.s3.us-west-1.amazonaws.com	Enables NetApp to collect information needed to troubleshoot support issues.
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 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.

Endpoints	Purpose
Various third-party locations, for example: • https://repo1.maven.org/maven2 • https://oss.sonatype.org/content/repositories • https://repo.typesafe.com Third-party locations are subject to change.	During upgrades, Cloud Manager downloads the latest packages for third-party dependencies.

Endpoints to install the Connector on a Linux host

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

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

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

Endpoints accessed from your web browser when using the local UI

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

Endpoints	Purpose
The Connector host	You must enter the host's IP address from a web browser to load the Cloud Manager console. Depending on your connectivity to your cloud provider, you can use the private IP or a public IP assigned to the host: • A private IP works if you have a VPN and direct connect access to your virtual network • A public IP works in any networking scenario 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 https://cdn.auth0.com https://netapp-cloud-account.auth0.com 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.

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

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 Connector host
HTTP	80	Provides HTTP access from client web browsers to the local user interface and connections from Cloud Compliance
HTTPS	443	Provides HTTPS access from client web browsers to the local user interface

Protocol	Port	Purpose
TCP	3128	Provides the Cloud Compliance instance with internet access, if your AWS network doesn't use a NAT or proxy

Outbound rules

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

Basic outbound rules

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

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

Advanced outbound rules

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

The source IP address is the Connector host.

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

Service	Protocol	Port	Destination	Purpose
API calls	TCP	3000	ONTAP cluster management LIF	API calls to ONTAP
	TCP	8088	Backup to S3	API calls to Backup to S3
DNS	UDP	53	DNS	Used for DNS resolve by Cloud Manager
Cloud Compliance	HTTP	80	Cloud Compliance instance	Cloud Compliance for Cloud Volumes ONTAP

Rules for the Connector in Azure

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

Inbound rules

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 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

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 Connector host
HTTP	80	Provides HTTP access from client web browsers to the local user interface
HTTPS	443	Provides HTTPS access from client web browsers to the local user interface

Outbound rules

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

Basic outbound rules

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

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

Advanced outbound rules

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

The source IP address is the Connector host.

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

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

Result

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

Creating a Connector in AWS

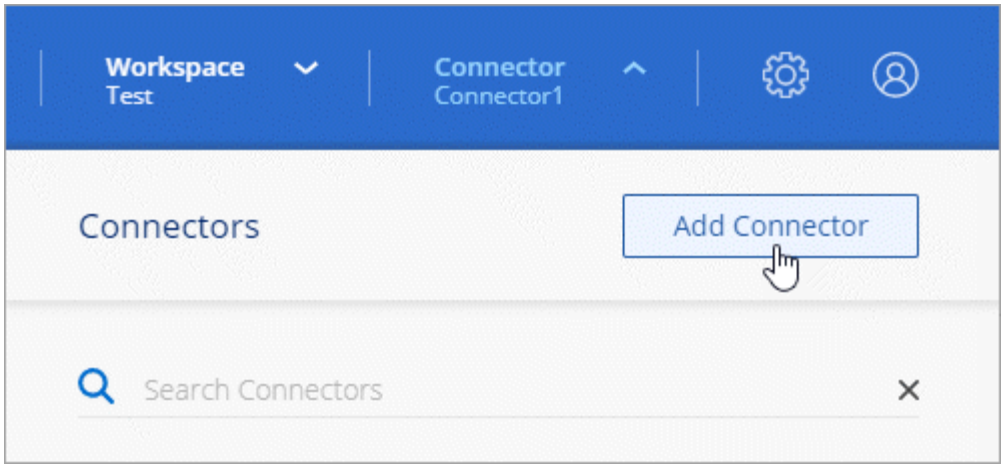
Cloud Manager enables you to create a Connector in AWS directly from its user interface.

What you'll need

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

Steps

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



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

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

   Learn more about networking requirements for the Connector.

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

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

6. Click **Create**.

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

After you finish

You need to associate a Connector with workspaces so Workspace Admins can use those Connectors to create Cloud Volumes ONTAP systems. If you only have Account Admins, then associating the Connector with workspaces isn't required. Account Admins have the ability to access all workspaces in

Cloud Manager by default. Learn more.

Creating a Connector in Azure from Cloud Manager

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

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

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

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

Setting up Azure permissions to create a Connector

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

Steps

1. Create a custom role using the Azure policy for the Connector:
   a. Download the Azure policy for the Connector.

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

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

      Example

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

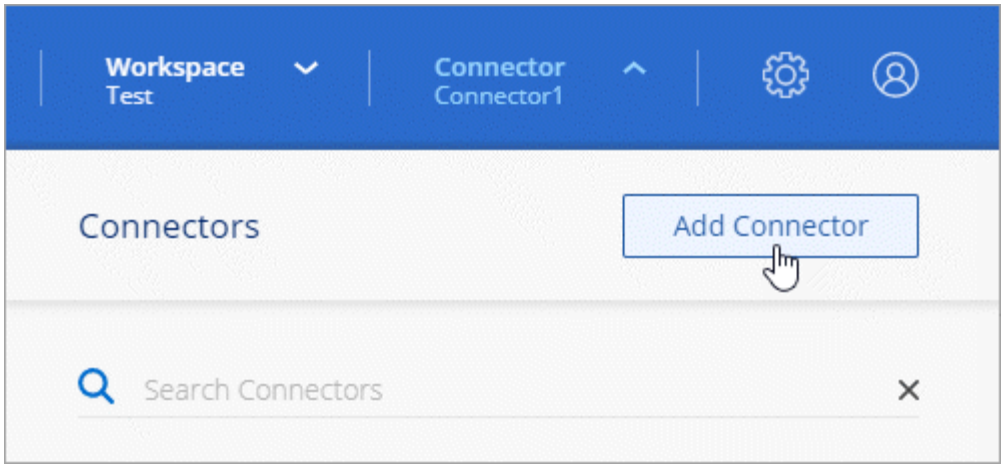
Cloud Manager enables you to create a Connector in Azure directly from its user interface.

What you'll need

- The required permissions for your Azure account.
- An Azure subscription.
- A VNet and subnet in your Azure region of choice.

Steps

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



2. Click **Let's Start**.
3. Choose **Microsoft Azure** as your cloud provider.

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

   Learn more about networking requirements for the Connector.

4. Review what you'll need and click **Continue**.
5. If you're prompted, log in to your Microsoft account, which should have the required permissions to create the virtual machine.

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

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

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

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

7. Click **Create**.

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

After you finish

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

Creating a Connector in GCP from Cloud Manager

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

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

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

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

Setting up GCP permissions to create a Connector

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

Steps

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

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

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

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

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

   The permissions contained in this YAML file are different than the permissions in step 2a.

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

c. If you want to deploy Cloud Volumes ONTAP in other projects, grant access by adding the service account with the Cloud Manager role to that project. You'll need to repeat this step for each project.

Result

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

Enabling Google Cloud APIs

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

Step

1. Enable the following Google Cloud APIs in your project.
   - Cloud Deployment Manager V2 API
   - Cloud Logging API
   - Cloud Resource Manager API
   - Compute Engine API
   - Identity and Access Management (IAM) API

Creating a Connector in GCP

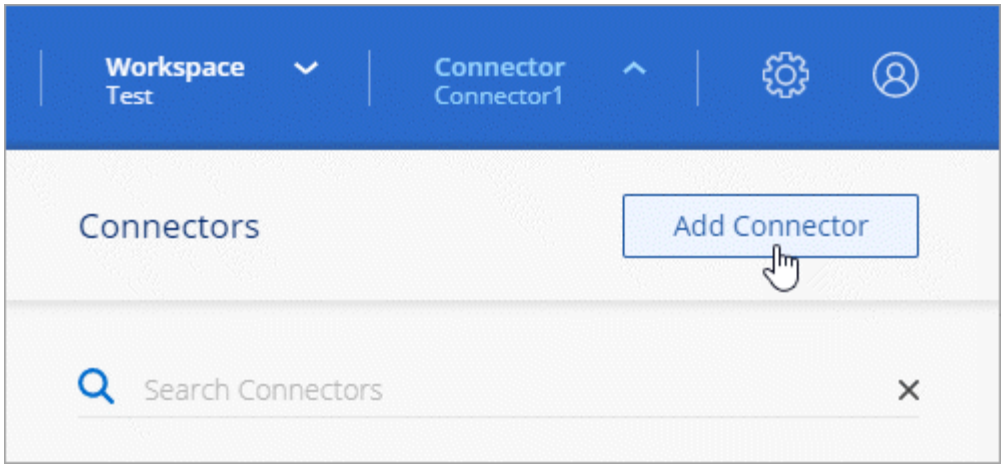
Cloud Manager enables you to create a Connector in GCP directly from its user interface.

What you'll need

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

Steps

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



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

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

   Learn more about networking requirements for the Connector.

4. Review what you'll need and click **Continue**.
5. If you're prompted, log in to your Google account, which should have the required permissions to create the virtual machine instance.

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

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

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

7. Click **Create**.

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

After you finish

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