Creating a Connector in GCP from Cloud Manager

Cloud Manager

Ben Cammett, Felix melligan
September 08, 2021

Table of Contents

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	• The permissions found in this .yaml file	• compute.networkUser • deploymentmanager.editor	Deploying and maintaining Cloud Volumes ONTAP and services in the service project
Cloud Volumes ONTAP service account	Custom	Service project	• storage.admin • member: Cloud Manager service account as serviceAccount.user	N/A	(Optional) For data tiering and Cloud Backup
Google APIs service agent	GCP	Service project	• (Default) Editor	• compute.networkUser	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	• (Default) Editor	• compute.networkUser	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

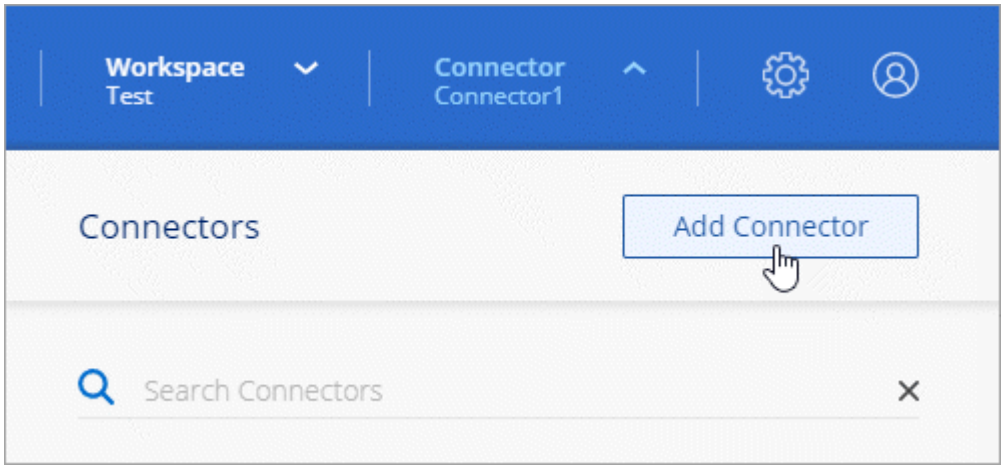
Cloud Manager enables you to create a Connector in GCP directly from its user interface.

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.