Google Cloud

Set up and administration

NetApp
March 31, 2022

Table of Contents

Google Cloud

Required permissions for the Connector in Google Cloud

Cloud Manager requires permissions to perform actions in your cloud provider. These permissions are included in the policies provided by NetApp. You might want to understand what Cloud Manager does with these permissions.

The Cloud Manager policy for GCP includes the permissions that Cloud Manager needs to deploy and manage Cloud Volumes ONTAP.

Actions	Purpose
- compute.disks.create - compute.disks.createSnapshot - compute.disks.delete - compute.disks.get - compute.disks.list - compute.disks.setLabels - compute.disks.use	To create and manage disks for Cloud Volumes ONTAP.
- compute.firewalls.create - compute.firewalls.delete - compute.firewalls.get - compute.firewalls.list	To create firewall rules for Cloud Volumes ONTAP.
- compute.globalOperations.get	To get the status of operations.
- compute.images.get - compute.images.getFromFamily - compute.images.list - compute.images.useReadOnly	To get images for VM instances.
- compute.instances.attachDisk - compute.instances.detachDisk	To attach and detach disks to Cloud Volumes ONTAP.
- compute.instances.create - compute.instances.delete	To create and delete Cloud Volumes ONTAP VM instances.
- compute.instances.get	To list VM instances.
- compute.instances.getSerialPortOutput	To get console logs.
- compute.instances.list	To retrieve the list of instances in a zone.
- compute.instances.setDeletionProtection	To set deletion protection on the instance.
- compute.instances.setLabels	To add labels.
- compute.instances.setMachineType - compute.instances.setMinCpuPlatform	To change the machine type for Cloud Volumes ONTAP.
- compute.instances.setMetadata	To add metadata.
- compute.instances.setTags	To add tags for firewall rules.

Actions	Purpose
- compute.instances.start - compute.instances.stop - compute.instances.updateDisplayDevice	To start and stop Cloud Volumes ONTAP.
- compute.machineTypes.get	To get the numbers of cores to check qoutas.
- compute.projects.get	To support multi-projects.
- compute.snapshots.create - compute.snapshots.delete - compute.snapshots.get - compute.snapshots.list - compute.snapshots.setLabels	To create and manage persistent disk snapshots.
- compute.networks.get - compute.networks.list - compute.regions.get - compute.regions.list - compute.subnetworks.get - compute.subnetworks.list - compute.zoneOperations.get - compute.zones.get - compute.zones.list	To get the networking information needed to create a new Cloud Volumes ONTAP virtual machine instance.
- deploymentmanager.compositeTypes.get - deploymentmanager.compositeTypes.list - deploymentmanager.deployments.create - deploymentmanager.deployments.delete - deploymentmanager.deployments.get - deploymentmanager.deployments.list - deploymentmanager.manifests.get - deploymentmanager.manifests.list - deploymentmanager.operations.get - deploymentmanager.operations.list - deploymentmanager.resources.get - deploymentmanager.resources.list - deploymentmanager.typeProviders.get - deploymentmanager.typeProviders.list - deploymentmanager.types.get - deploymentmanager.types.list	To deploy the Cloud Volumes ONTAP virtual machine instance using Google Cloud Deployment Manager.
- logging.logEntries.list - logging.privateLogEntries.list	To get stack log drives.
- resourcemanager.projects.get	To support multi-projects.
- storage.buckets.create - storage.buckets.delete - storage.buckets.get - storage.buckets.list - storage.buckets.update	To create and manage a Google Cloud Storage bucket for data tiering.

Actions	Purpose
- cloudkms.cryptoKeyVersions.useToEncrypt - cloudkms.cryptoKeys.get - cloudkms.cryptoKeys.list - cloudkms.keyRings.list	To use customer-managed encryption keys from the Cloud Key Management Service with Cloud Volumes ONTAP.
- compute.instances.setServiceAccount - iam.serviceAccounts.actAs - iam.serviceAccounts.getIamPolicy - iam.serviceAccounts.list - storage.objects.get - storage.objects.list	To set a service account on the Cloud Volumes ONTAP instance. This service account provides permissions for data tiering to a Google Cloud Storage bucket.
- compute.addresses.list - compute.backendServices.create - compute.networks.updatePolicy - compute.regionBackendServices.create - compute.regionBackendServices.get - compute.regionBackendServices.list	To deploy HA pairs.
- compute.subnetworks.use - compute.subnetworks.useExternalIp - compute.instances.addAccessConfig	To enable Cloud Data Sense.
- container.clusters.get - container.clusters.list	To discover Kubernetes clusters running in Google Kubernetes Engine.

Create a Connector in Google Cloud 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. Learn about other ways to deploy a Connector.

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 permissions

Before you can deploy a Connector, 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 the Connector 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.

   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 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.

Service Account	Creator	Hosted in	Service project permissions	Host project permissions	Purpose
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. Cloud Manager will create a deployment in the host project which contains the VPC0 firewall rule if no rule is specified.
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. These permissions reside in the Cloud Manager service account .yaml file. If you are deploying an HA pair using a shared VPC, these permissions will be used to create the firewall rules for VPC1, 2 and 3. For all other deployments, these permissions will also be used to create rules for VPC0.
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

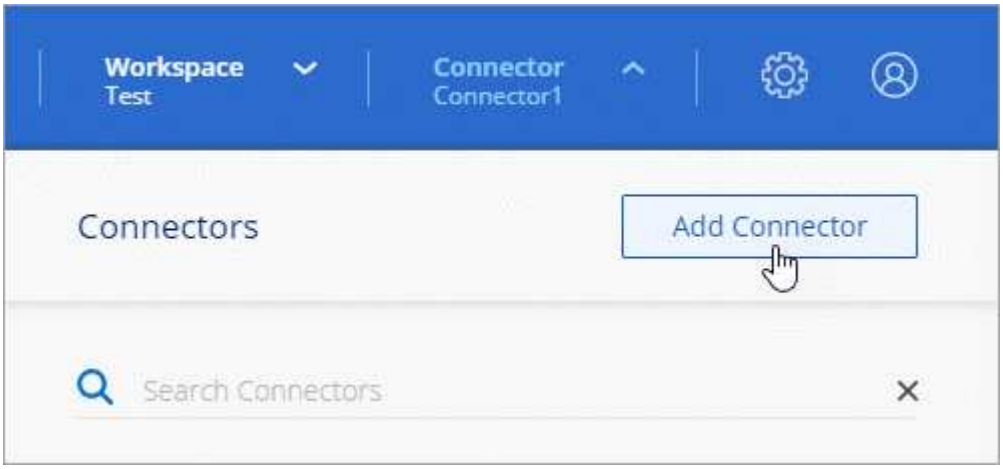
Create a Connector in Google Cloud directly from the Cloud Manager user interface or by using gcloud.

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.

Cloud Manager

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.

gcloud

1. Log in to the gcloud SDK using your preferred methodology.

   In our examples, we'll use a local shell with the gcloud SDK installed, but you could use the native Google Cloud Shell in the GCP console.

   For more information about the Google Cloud SDK, visit the Google Cloud SDK documentation page.

2. Verify that you are logged in as a user who has the required permissions that are defined in the section above:

   ```
   gcloud auth list
   ```

   The output should show the following where the * user account is the desired user account to be logged in as:

   ```
   Credentialed Accounts
   ACTIVE  ACCOUNT
        some_user_account@domain.com
   *    desired_user_account@domain.com
   To set the active account, run:
    $ gcloud config set account `ACCOUNT`
   Updates are available for some Cloud SDK components. To install
   them,
   please run:
   $ gcloud components update
   ```

3. Run the `gcloud compute instances create` command:

   ```
   gcloud compute instances create <instance-name>
     --machine-type=n1-standard-4
     --image-project=netapp-cloudmanager
     --image-family=cloudmanager
     --scopes=cloud-platform
     --project=<project>
     --service-account=<<service-account>
     --zone=<zone>
     --no-address
     --tags <network-tag>
     --network <network-path>
     --subnet <subnet-path>
     --boot-disk-kms-key <kms-key-path>
   ```

instance-name

The desired instance name for the VM instance.

project

(Optional) The project where you want to deploy the VM.

service-account

The service account specified in the output from step 2.

zone

The zone where you want to deploy the VM

no-address

(Optional) No external IP address is used (you need a cloud NAT or proxy to route traffic to the public internet)

network-tag

(Optional) Add network tagging to link a firewall rule using tags to the Connector instance

network-path

(Optional) Add the name of the network to deploy the Connector into (for a Shared VPC, you need the full path)

subnet-path

(Optional) Add the name of the subnet to deploy the Connector into (for a Shared VPC, you need the full path)

kms-key-path

(Optional) Add a KMS key to encrypt the Connector's disks (IAM permissions also need to be applied)

For more information about these flags, visit the Google Cloud compute SDK documentation.

Running the command deploys the Connector using the NetApp golden image. The Connector instance and software should be running in approximately five minutes.

4. Open a web browser from a host that has a connection to the Connector instance and enter the following URL:

   http://*ipaddress*:80

5. After you log in, set up the Connector:
   a. Specify the NetApp account to associate with the Connector.

      Learn about NetApp accounts.

   b. Enter a name for the system.

Result

The Connector is now installed and set up with your NetApp account. Cloud Manager will automatically use this Connector when you create new working environments. But if you have more than one Connector, you'll need to switch between them.