NetApp

Google Cloud

Set up and administration

NetApp
April 04, 2023

Table of Contents

Google Cloud

Quick start to create a Connector in Google Cloud

Create a Connector in Google Cloud by choosing an installation option, setting up networking, preparing permissions, and more.

1 **Understand your installation options**

The standard way to create a Connector in Google Cloud is directly from BlueXP, but you can also create it using gcloud, or by manually installing the software on a pre-existing Linux host.

Learn more about your installation options.

2 **Set up networking**

Prepare the following for the Connector:

- A VPC and subnet
- A network connection to the networks where you're planning to create and manage working environments
- Outbound internet access to specific endpoints for day-to-day operations
- The IP address, credentials, and HTTPS certificate of a proxy server, if a proxy server is required for outbound internet

Learn more about networking requirements.

3 **Review host requirements**

The Connector software must run on a host that meets specific requirements. If you plan to manually install the Connector software on your own Linux host, then you should ensure that your host meets these requirements. If you're creating the Connector from BlueXP or by using gcloud, then these requirements are taken care of for you because the software is deployed from an image.

The key requirements are as follows:

- A dedicated host running CentOS or Red Hat Enterprise Linux
- 4 CPUs
- 14 GB of RAM
- Docker Engine

Learn more about these host requirements.

4 **Set up Google Cloud permissions**

Set up Google Cloud permissions for the installation option that you're planning to use:

- **Installation from BlueXP or gcloud**: Create a custom role and attach it to the user who will deploy the Connector. Create another custom role and assign it to a service account for the Connector VM instance.
- **Manual install**: Create a custom role and assign it to a service account for the Connector VM instance.

Follow step-by-step instructions for each of these options.

⑤ Enable Google Cloud APIs

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

- Cloud Deployment Manager V2 API
- Cloud Logging API
- Cloud Resource Manager API
- Compute Engine API
- Identity and Access Management (IAM) API

⑥ Create the Connector

Create the Connector using one of the available installation options:

- **From BlueXP**: Click the Connector drop-down, select **Add Connector** and follow the prompts.
- **Using gloud**: Use the `gcloud compute instances create` command.
- **Manual install**: Download the Connector software from the NetApp Support Site and run the installation script.

Follow step-by-step instructions for each of these options.

⑦ Provide BlueXP with permissions

If you manually installed the Connector software on your own Linux host, you need to provide BlueXP with the permissions that you previously set up.

Follow step-by-step instructions.

Connector installation options in Google Cloud

There are a few different ways to create a Connector in Google Cloud. Directly from BlueXP is the most common way.

The following installation options are available:

- Create the Connector directly from BlueXP (this is the standard option)

  This action launches a VM instance running Linux and the Connector software in a VPC of your choice.

- Create the Connector using gcloud

  This action also launches a VM instance running Linux and the Connector software.

- Download and manually install the software on your own Linux host

The installation option that you choose impacts how you prepare for installation. This includes how you provide BlueXP with the required permissions that it needs to authenticate and manage resources in Google Cloud.

Learn how to install the Connector in Google Cloud.

Set up Google Cloud networking

Set up your networking so the Connector can manage resources and processes within your hybrid cloud environment.

VPC and subnet

When you create the Connector, you need to specify the VPC and subnet where the Connector should reside.

Connections to target networks

A Connector requires a network connection to the location where you're planning to create and manage working environments.

Outbound internet access

The network location where you deploy the Connector must have an outbound internet connection.

Endpoints contacted during manual installation

If you plan to manually install the Connector on your own Linux host, the installer for the Connector requires access to the following URLs during the installation process:

- https://support.netapp.com
- https://mysupport.netapp.com
- https://cloudmanager.cloud.netapp.com/tenancy
- https://stream.cloudmanager.cloud.netapp.com
- https://cloudmanagerinfraprod.azurecr.io
- https://production-artifacts.cloudmanager.cloud.netapp.com
- https://*.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 contacted for day-to-day operations

The Connector requires outbound internet access to contact the following endpoints in order to manage resources and processes within your public cloud environment.

Endpoints	Purpose
https://www.googleapis.com/compute/v1/ https://cloudresourcemanager.googleapis.com/v1/projects https://www.googleapis.com/compute/beta https://storage.googleapis.com/storage/v1 https://www.googleapis.com/storage/v1 https://iam.googleapis.com/v1 https://cloudkms.googleapis.com/v1 https://www.googleapis.com/deploymentmanager/v2/projects	To manage resources in Google Cloud.
https://support.netapp.com	To obtain licensing information and to send AutoSupport messages to NetApp support.
https://*.api.bluexp.netapp.com https://api.bluexp.netapp.com https://*.cloudmanager.cloud.netapp.com https://cloudmanager.cloud.netapp.com	To provide SaaS features and services within BlueXP. ⓘ The Connector is currently contacting "cloudmanager.cloud.netapp.com" but it will start contacting "api.bluexp.netapp.com" in an upcoming release.
https://cloudmanagerinfraprod.azurecr.io https://*.blob.core.windows.net	To upgrade the Connector and its Docker components.

Related link

Prepare networking for user access to the BlueXP console

Proxy server

If your organization requires deployment of a proxy server for all outgoing internet traffic, obtain the following information about your HTTP or HTTPS proxy:

- IP address
- Credentials
- HTTPS certificate

Ports

There's no incoming traffic to the Connector, unless you initiate it or if the Connector is used as a proxy for AutoSupport messages.

- 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.
- Inbound connections over port 3128 are required if you deploy Cloud Volumes ONTAP systems in a subnet where an outbound internet connection isn't available.

IP address limitation

There's a possible conflict with IP addresses in the 172 range. Learn more about this limitation.

Review Connector host requirements for Google Cloud installs

The Connector software must run on a host that meets specific operating system requirements, RAM requirements, port requirements, and so on. If you plan to manually install the Connector, you should ensure that your host meets these requirements.

When you deploy the Connector from BlueXP or by using glcoud, the image includes the required OS and software components.

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

Supported operating systems
    • CentOS 7.6, 7.7, 7.8, and 7.9

    • Red Hat Enterprise Linux 7.6, 7.7, 7.8, 7.9, 8.6, and 8.7

    The host must be registered with Red Hat Subscription Management. If it's not registered, the host can't access repositories to update required 3rd-party software during Connector installation.

    The Connector is supported on English-language versions of these operating systems.

Hypervisor
    A bare metal or hosted hypervisor that is certified to run CentOS or Red Hat Enterprise Linux is required. Red Hat Solution: Which hypervisors are certified to run Red Hat Enterprise Linux?

CPU
    4 cores or 4 vCPUs

RAM
    14 GB

Google Cloud machine type
    An instance type that meets the CPU and RAM requirements above. We recommend n2-standard-4.

    The Connector is supported in Google Cloud on a VM instance with an OS that supports Shielded VM features

Disk space in /opt
    100 GiB of space must be available

Disk space in /var
    20 GiB of space must be available

Docker Engine

Docker Engine version 19.3.1 or later is required on the host before you install the Connector. View installation instructions

Set up Google Cloud permissions

Set up Google Cloud permissions so that you can use BlueXP to manage your data and storage infrastructure in Google Cloud.

You need to set up Google Cloud permissions as follows:

- If you are planning to create the Connector from BlueXP or by using gcloud, then you need to set up permissions for the Google Cloud user who will deploy the Connector VM.

- Set up permissions for the Connector by creating a role and granting the role to a service account.

  You'll associate this service account with the Connector VM so that BlueXP has the required permissions.

Depending on your configuration, you might need to complete the following steps as well:

- Set up permissions across projects
- Set up permissions for a shared VPC

Set up permissions to create the Connector from BlueXP or gcloud

Before you can deploy a Connector from BlueXP or by using gcloud, you need to ensure that your Google Cloud account has the correct permissions.

Steps

1. Create a custom role in Google Cloud:

   a. Create a YAML file that includes the following permissions:

   ```
   title: Connector deployment policy
   description: Permissions for the user who deploys the Connector from
   BlueXP
   stage: GA
   includedPermissions:
   - compute.disks.create
   - compute.disks.get
   - compute.disks.list
   - compute.disks.setLabels
   - compute.disks.use
   - compute.firewalls.create
   - compute.firewalls.delete
   - compute.firewalls.get
   - compute.firewalls.list
   - compute.globalOperations.get
   - compute.images.get
   ```

```
- compute.images.getFromFamily
- compute.images.list
- compute.images.useReadOnly
- compute.instances.attachDisk
- compute.instances.create
- compute.instances.get
- compute.instances.list
- compute.instances.setDeletionProtection
- compute.instances.setLabels
- compute.instances.setMachineType
- compute.instances.setMetadata
- compute.instances.setTags
- compute.instances.start
- compute.instances.updateDisplayDevice
- compute.machineTypes.get
- compute.networks.get
- compute.networks.list
- compute.networks.updatePolicy
- compute.projects.get
- compute.regions.get
- compute.regions.list
- compute.subnetworks.get
- compute.subnetworks.list
- compute.zoneOperations.get
- compute.zones.get
- compute.zones.list
- 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
- resourcemanager.projects.get
- compute.instances.setServiceAccount
- iam.serviceAccounts.list
```

b. From Google Cloud, activate cloud shell.

   c. Upload the YAML file that includes the required permissions.

   d. Create a custom role by using the `gcloud iam roles create` command.

   The following example creates a role named "connectorDeployment" at the project level:

   gcloud iam roles create connectorDeployment --project=myproject --file=connector-deployment.yaml

   Google Cloud docs: Creating and managing custom roles

2. Assign this custom role to the user who will deploy the Connector from BlueXP or by using gcloud.

   Google Cloud docs: Grant a single role

Result

The Google Cloud user now has the permissions required to create the Connector.

Set up permissions for the Connector

A service account is required to provide the Connector with the permissions that BlueXP needs to manage resources in Google Cloud. You need to associate this service account with the Connector VM.

Steps

1. Create a custom role in Google Cloud:

   a. Create a YAML file that includes the contents of the service account permissions for the Connector.

   b. From Google Cloud, activate cloud shell.

   c. Upload the YAML file that includes the required permissions.

   d. Create a custom role by using the `gcloud iam roles create` command.

   The following example creates a role named "connector" at the project level:

   gcloud iam roles create connector --project=myproject --file=connector.yaml

   Google Cloud docs: Creating and managing custom roles

2. Create a service account in Google Cloud:

   a. From the IAM & Admin service, click **Service Accounts > Create Service Account**.

   b. Enter service account details and click **Create and Continue**.

   c. Select the role that you just created.

   d. Finish the remaining steps to create the role.

   Google Cloud docs: Creating a service account

Result

The service account for the Connector VM is set up.

Set up permissions across projects

If you plan to deploy Cloud Volumes ONTAP systems in different projects than the project where the Connector resides, then you'll need to provide the Connector's service account with access to those projects.

For example, let's say the Connector is in project 1 and you want to create Cloud Volumes ONTAP systems in project 2. You'll need to grant access to the service account in project 2.

Steps

1. In the Google Cloud console, go to the IAM service and select the project where you want to create Cloud Volumes ONTAP systems.

2. On the **IAM** page, select **Grant Access** and provide the required details.

   - Enter the email of the Connector's service account.

   - Select the Connector's custom role.

   - Click **Save**.

For more details, refer to Google Cloud documentation

Set up shared VPC permissions

If you are using a shared VPC to deploy resources into a service project, then you'll need to prepare your permissions.

This table is for reference and your environment should reflect the permissions table when IAM configuration is complete.

Identity	Creator	Hosted in	Service project permissions	Host project permissions	Purpose
Google account to deploy the Connector	Custom	Service Project	Connector deployment policy	compute.networkUser	Deploying the Connector in the service project
Connector service account	Custom	Service project	Connector service account policy	• 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: BlueXP service account as serviceAccount.user	N/A	(Optional) For data tiering and Cloud Backup

Identity	Creator	Hosted in	Service project permissions	Host project permissions	Purpose
Google APIs service agent	Google Cloud	Service project	(Default) Editor	compute.networkUser	Interacts with Google Cloud APIs on behalf of deployment. Allows BlueXP to use the shared network.
Google Compute Engine default service account	Google Cloud	Service project	(Default) Editor	compute.networkUser	Deploys Google Cloud instances and compute infrastructure on behalf of deployment. Allows BlueXP 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 BlueXP create them for you. BlueXP 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 BlueXP create them for you. These permissions reside in the BlueXP 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.

Enable Google Cloud APIs

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

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

Google Cloud documentation: Enabling APIs

Create the Connector in Google Cloud

Create the Connector directly from the BlueXP web-based console, by using gcloud, or by installing the software on your own Linux host.

BlueXP

What you'll need

- The required Google Cloud permissions to create the Connector and a service account for the Connector VM.

  [Learn how to set up Google Cloud permissions](#)

- A VPC and subnet that meets networking requirements.

  [Learn about networking requirements](#)

- Details about a proxy server, if a proxy is required for internet access from the Connector.

Steps

1. Click the **Connector** drop-down and select **Add Connector**.

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

3. On the **Deploying a Connector** page, review the details about what you'll need. You have two options:

   a. Click **Continue** to prepare for deployment by using the in-product guide. Each step in the in-product guide includes the information that's contained on this page of the documentation.

   b. Click **Skip to Deployment** if you already prepared by following the steps on this page.

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

   ◦ 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.

   ◦ **Details**: 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.

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

5. Click **Add**.

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

Result

After the process is complete, the Connector is available for use from BlueXP.

gcloud

What you'll need

- The required Google Cloud permissions to create the Connector and a service account for the Connector VM.

  [Learn how to set up Google Cloud permissions](#)

- A VPC and subnet that meets networking requirements.

  [Learn about networking requirements](#)

Steps

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 Google Cloud 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=n2-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:

   https://*ipaddress*

5. After you log in, set up the Connector:

   a. Specify the BlueXP account to associate with the Connector.

      Learn about BlueXP accounts.

   b. Enter a name for the system.

Result

The Connector is now installed and set up with your BlueXP account.

Open a web browser and go to the BlueXP console to start using the Connector with BlueXP.

Manual install

What you'll need

- Root privileges to install the Connector.
- Details about a proxy server, if a proxy is required for internet access from the Connector.

  You have the option to configure a proxy server after installation but doing so requires restarting the Connector.

- A CA-signed certificate, if the proxy server uses HTTPS or if the proxy is an intercepting proxy.

About this task

- The installation installs the AWS command line tools (awscli) to enable recovery procedures from NetApp support.

  If you receive a message that installing the awscli failed, you can safely ignore the message. The Connector can operate successfully without the tools.

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

Steps

1. Verify that docker is enabled and running.

   ```
   sudo systemctl enable docker && sudo systemctl start docker
   ```

2. If the *http_proxy* or *https_proxy* system variables are set on the host, remove them:

   ```
   unset http_proxy
   unset https_proxy
   ```

If you don't remove these system variables, the installation will fail.

3. Download the Connector software from the NetApp Support Site, and then copy it to the Linux host.

   You should download the "online" Connector installer that's meant for use in your network or in the cloud. A separate "offline" installer is available for the Connector, but it's only supported with private mode deployments.

4. Assign permissions to run the script.

   ```
   chmod +x OnCommandCloudManager-<version>
   ```

   Where <version> is the version of the Connector that you downloaded.

5. Run the installation script.

   ```
   ./OnCommandCloudManager-<version> --proxy <HTTP or HTTPS proxy
   server> --cacert <path and file name of a CA-signed certificate>
   ```

   The --proxy and --cacert parameters are optional. If you have a proxy server, you will need to enter the parameter(s) as shown. The installer doesn't prompt you to provide information about a proxy.

   Here's an example of the command using both optional parameters:

   ```
   ./OnCommandCloudManager-V3.9.26 --proxy
   https://user:password@10.0.0.30:8080/ --cacert
   /tmp/cacert/certificate.cer
   ```

   --proxy configures the Connector to use an HTTP or HTTPS proxy server using one of the following formats:

   ◦ http://address:port
   ◦ http://username:password@address:port
   ◦ https://address:port
   ◦ https://username:password@address:port

   --cacert specifies a CA-signed certificate to use for HTTPS access between the Connector and the proxy server. This parameter is required only if you specify an HTTPS proxy server or if the proxy is an intercepting proxy.

6. Wait for the installation to complete.

   At the end of the installation, the Connector service (occm) restarts twice if you specified a proxy server.

7. Open a web browser from a host that has a connection to the Connector virtual machine and enter the following URL:

   https://*ipaddress*

8. After you log in, set up the Connector:

    a. Specify the BlueXP account to associate with the Connector.

    b. Enter a name for the system.

    c. Under **Are you running in a secured environment?** keep restricted mode disabled.

       You should keep restricted mode disabled because these steps describe how to use BlueXP in standard mode. You should enable restricted mode only if you have a secure environment and want to disconnect this account from BlueXP backend services. If that's the case, follow steps to get started with BlueXP in restricted mode.

    d. Click **Let's start**.

Result

The Connector is now installed and is set up with your BlueXP account.

What's next?

Provide BlueXP with the permissions that you previously setup.

Provide Google Cloud permissions to BlueXP

If you manually installed the Connector software on your own Linux host, you need to provide BlueXP with the permissions that you previously set up.

Learn how to set up these permissions.

These steps don't apply if you deployed the Connector directly from BlueXP or by using gcloud.

Steps

1. Go to the Google Cloud portal and assign the service account to the Connector VM instance.

   Google Cloud documentation: Changing the service account and access scopes for an instance

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

Result

BlueXP now has the permissions that it needs to perform actions in Google Cloud on your behalf.