Deploying the Cloud APIC in Google Cloud

Creating a Project in Google Cloud for the Infra Tenant

This procedure describes how to create a project in Google Cloud, enable the appropriate APIs and services on the project, and assign appropriate permissions to the service account.

The tenant that will be created in these procedures will be referred to as the infra tenant.

Step 1 Log into your Google Cloud account.

Step 2 Create or use an existing project that will be used for Cisco Cloud APIC.

See Creating and managing projects in the Google Cloud documentation for those instructions.

If you are using an existing project, verify that there is no previous Cisco Cloud APIC deployment on this project. If there is a previous Cisco Cloud APIC deployment on this project, delete that existing deployment using the instructions in Deleting a Cisco Cloud APIC Deployment in Google Cloud, on page 10.

Step 3 Enable the appropriate APIs and services on your project.

a) In the Google Cloud GUI, navigate to the project that you created for Cisco Cloud APIC.
The **Dashboard** for your project is displayed.

b) In the search bar at the top of the **Dashboard**, search for **APIs & Services**, then click the result from that search to access the **APIs & Services** window.

c) In the **APIs & Services** window, click the **+ ENABLE APIS AND SERVICES** tab.

The **API Library** window appears.

d) In the **Search for APIs & Services** field, search for and enable the necessary services.

For each of the services in the list below:

1. Search for the API or service in the **Search for APIs & Services** field.
2. Click on the search result to display the page for that API or service.

3. Click the **ENABLE** button in that API or service page.

Following are the APIs and services that you must search for and enable:

- Compute Engine API
- Cloud Deployment Manager V2 API
- Cloud Logging API
- Cloud Pub/Sub API
- Cloud Resource Manager API
- Cloud Runtime Configuration API
- Identity and Access Management (IAM) API
- Service Usage API

Each API or service takes several minutes to enable. You will have to navigate back to the **APIs & Services** window after you enable each API or service.

Note that the following additional APIs and services should be enabled automatically when you enable all of the APIs and services listed above:

- IAM Service Account Credentials API
- Cloud OS Login API
- Recommender API

If they are not enabled automatically, enable them manually.

Step 4 Assign the appropriate permissions to the service account.

There are two types of service accounts:

- **Service account for the project**: This service account allows for the deployment of the Cisco Cloud APIC.
- **Service account for the user**: This service account communicates with the APIs. Instead of having a user login or password, this service account acts on behalf of the project and will create resources.

For this step, you will be assigning the appropriate permissions to the service account for the project.

a) In the Google Cloud GUI, navigate back to the **Dashboard** window for your Cisco Cloud APIC project.
b) In the left nav bar, click on **IAM & Admin**, then choose **IAM**.

The **IAM** window appears with several service accounts displayed.

c) Locate the appropriate service account for the deployment.

Locate the service account with the entry `Google APIs Service Agent` shown in the **Name** column (also listed with *<project_number>*`@cloudservices.gserviceaccount.com` in the **Principal** column).

This service account should have been created automatically when you enabled the APIs in the previous step. If this service account was not created automatically, follow these steps to create it manually:

1. Verify that the **PRINCIPALS** tab is selected in the **IAM** window.
2. Click **ADD** at the top part of the window.

3. In the **New Principals** field, enter the name for this service account:

   `<project_number>@cloudservices.gserviceaccount.com`

4. Click **SAVE**.

d) Add the necessary role entries for this service account.

You should see the following entry in the **Role** column for this service account:

- `Editor`

You will also have to add these additional roles for this service account:

- `Project IAM Admin`
- `Role Administrator`

To add the additional role entries for this service account:

1. Click the pencil icon on the row for this service account.

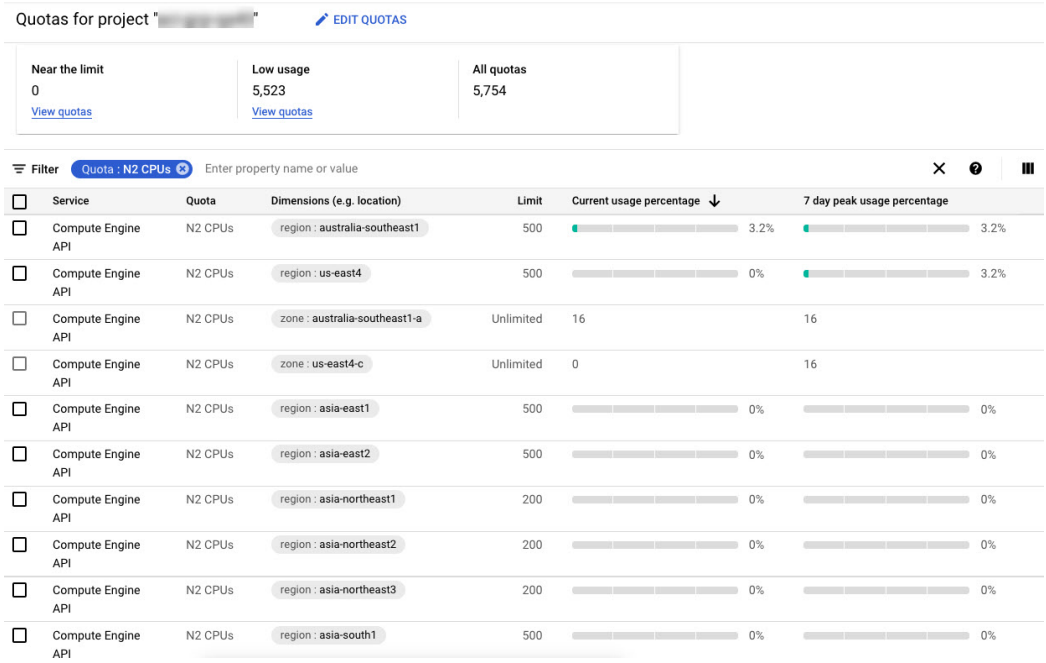
   The **Edit Permissions** window is displayed.

2. Click **+ ADD ANOTHER ROLE**, then search for and choose the `Project IAM Admin` role entry.
3. Click **+ ADD ANOTHER ROLE** again, then search for and choose the `Role Administrator` role entry.
4. Click **SAVE**.

   You are returned to the **IAM** window with the service accounts displayed.

Step 5 Verify that the Google Cloud account has N2 CPUs quota set to at least 16 in the region where the Cisco Cloud APIC is deployed, and that the quotas are currently not used.

If this is not the case, raise a case with Google Cloud to increase the quota limit.



Generating an SSH Key Pair in Linux or MacOS

These procedures describe how to generate an SSH public and private key pair in Linux or MacOS.

Step 1 On your Linux virtual machine or Mac, create a public and private key pair using `ssh-keygen`, directing the output to a file.

```
# ssh-keygen -t rsa -f ~/.ssh/capic-ssh-key -C admin
```

Step 2 Locate the public key file that you saved.

The public key file is saved in this file:

```
~/.ssh/capic-ssh-key.pub
```

Step 3 Open the public key file and copy the public key information from that file.

The public key information will be in this format:

```
ssh-rsa <public-key-string> admin
```

Verify that you've copied all of the necessary public key information, including the `ssh-rsa` text at the beginning and the `admin` text at the end.

Following is an example of the public key information that you would copy from the file:

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABABABgQC+0Aom7Mblv+w7yWE7QOPytvpankAdOsNWd7keptT6nAnr
S2UjHP0c0KC0jABEo7fL0hwQpwKmLRfHi0poQ3FAy7Oof6XcFJx5aCcCayrGDhm96HPbcPoXjhhg0Fufr4QyL9cWpbsKn9K1k
OhnIw+KQyaxCQS1D1wMsgREKMDrkdk5MZazqZC8haThaaAO/h+i+OQ9juo6N6QPUogHRZ+E9ztyGU/buU1/0vnvzTTinvw8aq
mTnPUQxNI6wZ2FpMH8JHiDQ924wIboAEq0tvidnElemG5wsQrwUghD7r1D9uWjI1rsfGAJL8mSIkWbXZFo+AqNlbE69Oa1TIL
```

```
2DfmgYQm3M+qWdzaZPI6i+Ap/dMgGKyy8M4VGFN0o+wbkzi1XdEbMpSEBxyuDtoB5H9T4Kov2yuH/RdqPMSSt+ZgNgBZgcl6S
HXlpSA0GmwyHljYNizo70UMI2JDJDmUc4vCNMgVRxWkNraCWYEZD5iMjnAtIiZvQGmZKQwBH0GY3XIc= admin
```

What to do next

Follow the instructions in Deploying the Cloud APIC in Google Cloud, on page 5 to continue the Google Cloud configuration process, which includes pasting the public key information into the Google Cloud deployment template.

Deploying the Cloud APIC in Google Cloud

Step 1 Log into your Google Cloud account for the Cisco Cloud APIC infra tenant.

Step 2 Navigate to the Google Cloud Marketplace.

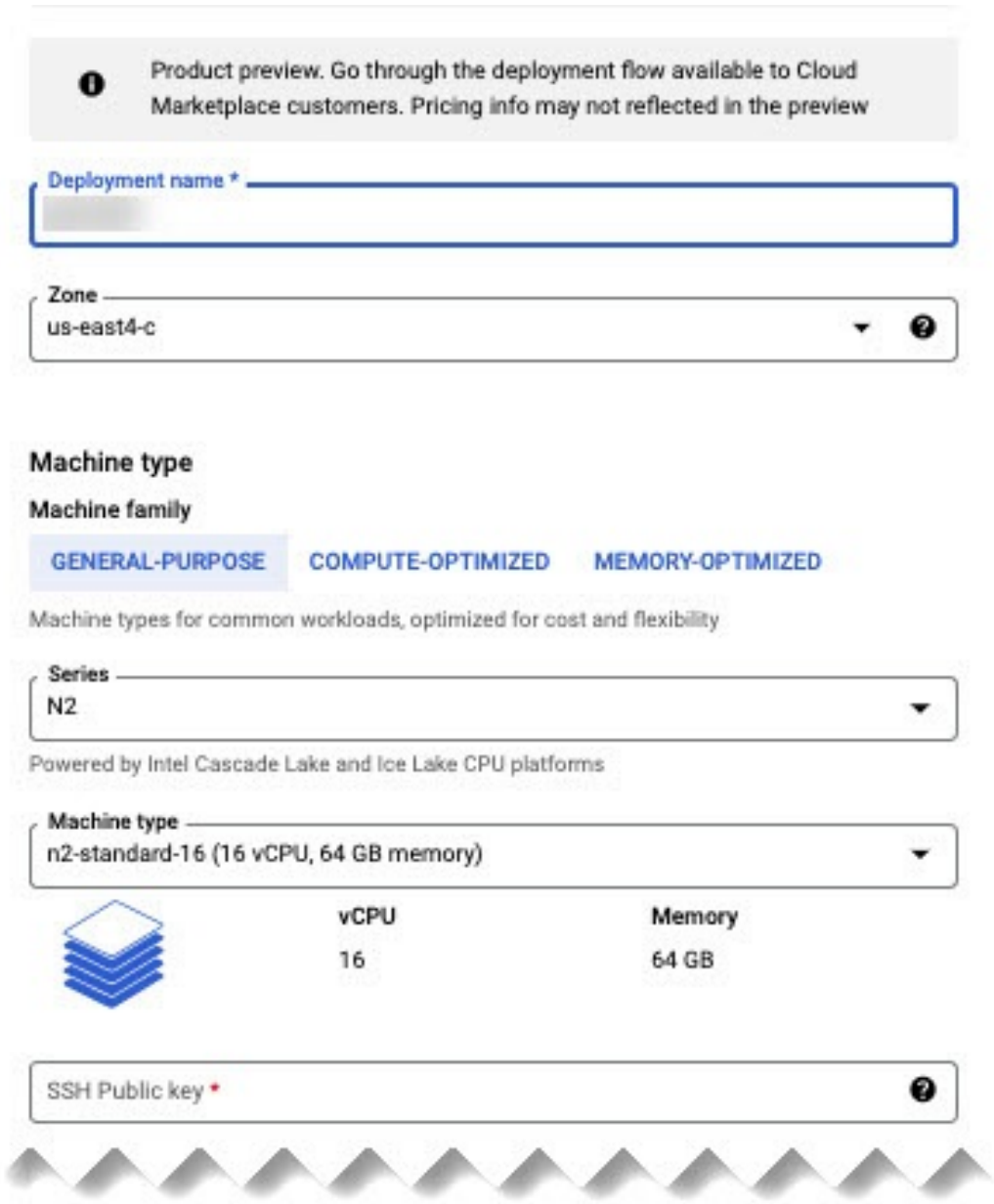
Step 3 In the search bar, search for:

```
Cisco Cloud APIC
```

and select the result from that search.

Step 4 In the **Cisco Cloud APIC** window in the Google Cloud Marketplace, click **LAUNCH**.

The **New Cisco Cloud APIC deployment** window appears.



Step 5 In the **New Cisco Cloud APIC deployment** window, enter the necessary information in the following fields:

- **Deployment name**: Enter a unique name for this Cisco Cloud APIC deployment.
- **Zone**: Select the zone where the Cisco Cloud APIC will be deployed.

  The Cisco Cloud APIC deployment will be supported in all zones that support the following:

  - **GENERAL PURPOSE** as the **Machine family**
  - **n2-standard-16** as the **Machine type**

  For more information, see:

https://cloud.google.com/compute/docs/general-purpose-machines#n2_machines

- **Machine type** section:
  - **Machine family**: Select the **GENERAL PURPOSE** tab if it is not already selected.
  - **Series**: Leave the default **N2** selection as-is.
  - **Machine type**: We recommend choosing the **n2-standard-16** option in this field.
  - **SSH Public key**: Enter the SSH public key to enable SSH access to the Cisco Cloud APIC. You will use this SSH key pair to log into the Cloud APIC.

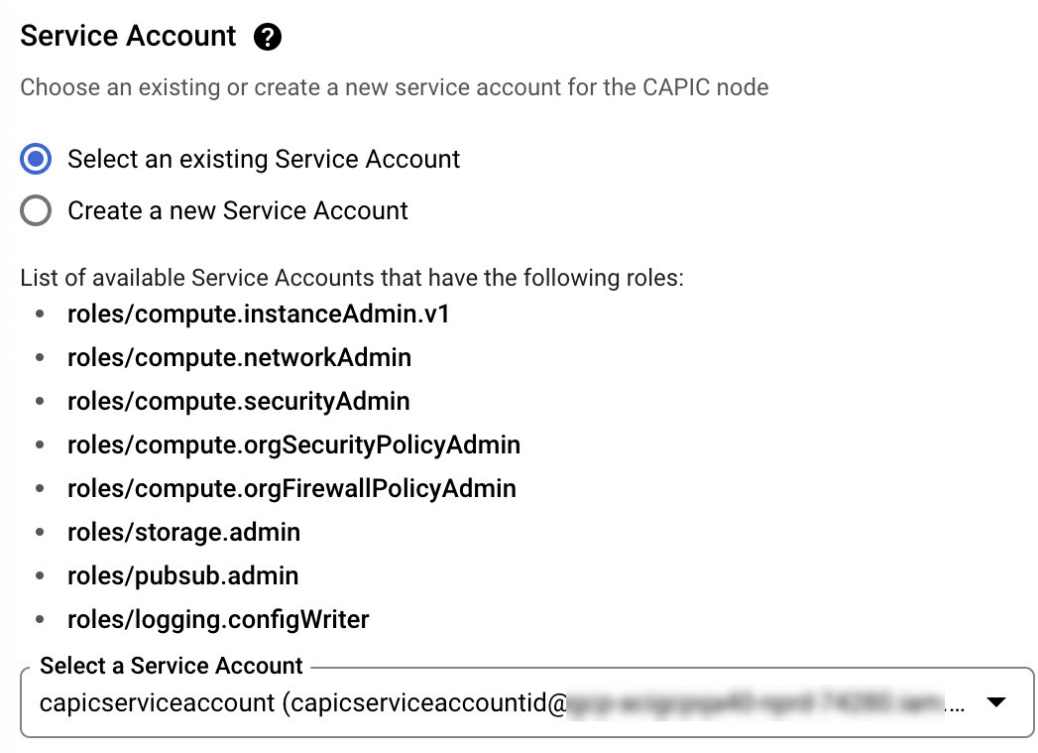
    Paste the public key information that you copied at the end of Generating an SSH Key Pair in Linux or MacOS, on page 4. Note that the **ssh-rsa** string should remain at the beginning of the public key string that you paste into this field. This SSH public key must be in the following format:

    ```
    ssh-rsa <ssh-public-key-string> <user-info>
    ```

  - **Service Account**: Choose an existing service account or create a new service account for the Cisco Cloud APIC deployment.
    - **Select an existing Service Account**: If you have an existing service account that you can use for the Cisco Cloud APIC deployment, we recommend that you use that existing service account.

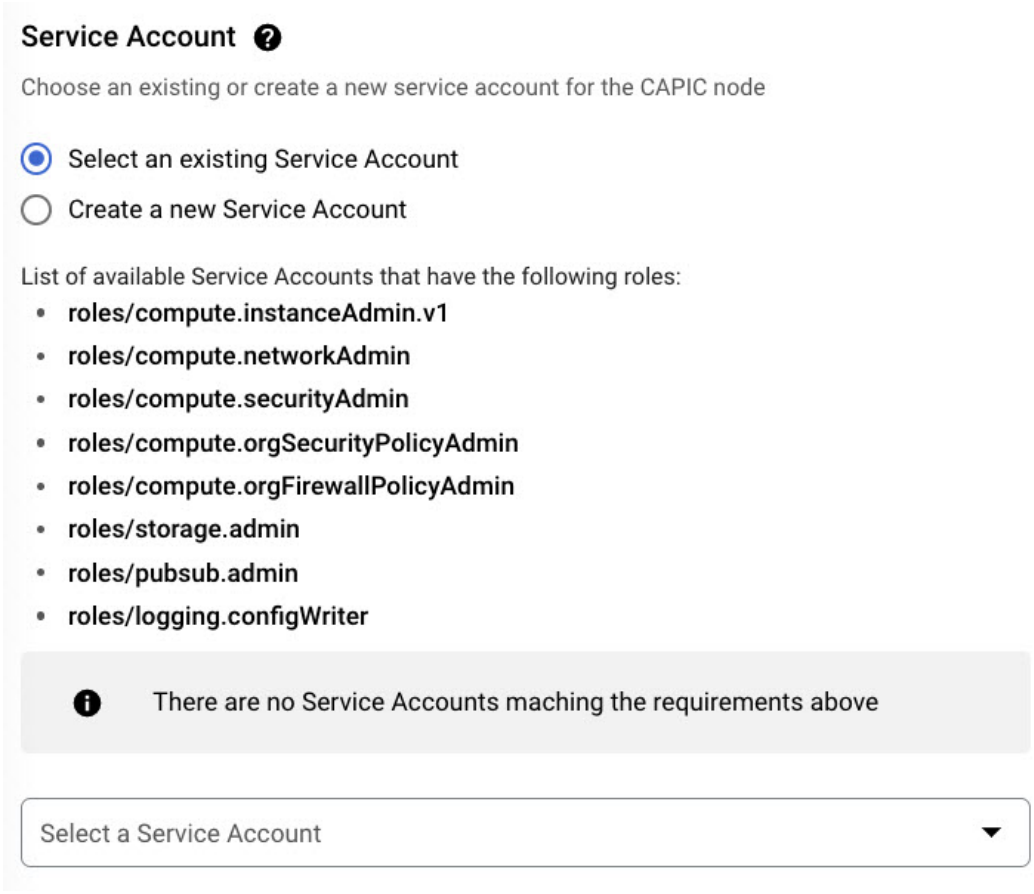
      Click the **Select an existing Service Account** option.

      - If you have an existing service account that you can use for this Cisco Cloud APIC deployment, you will see a screen similar to the following:



      Select the service account in the **Select a Service Account** field in this case.

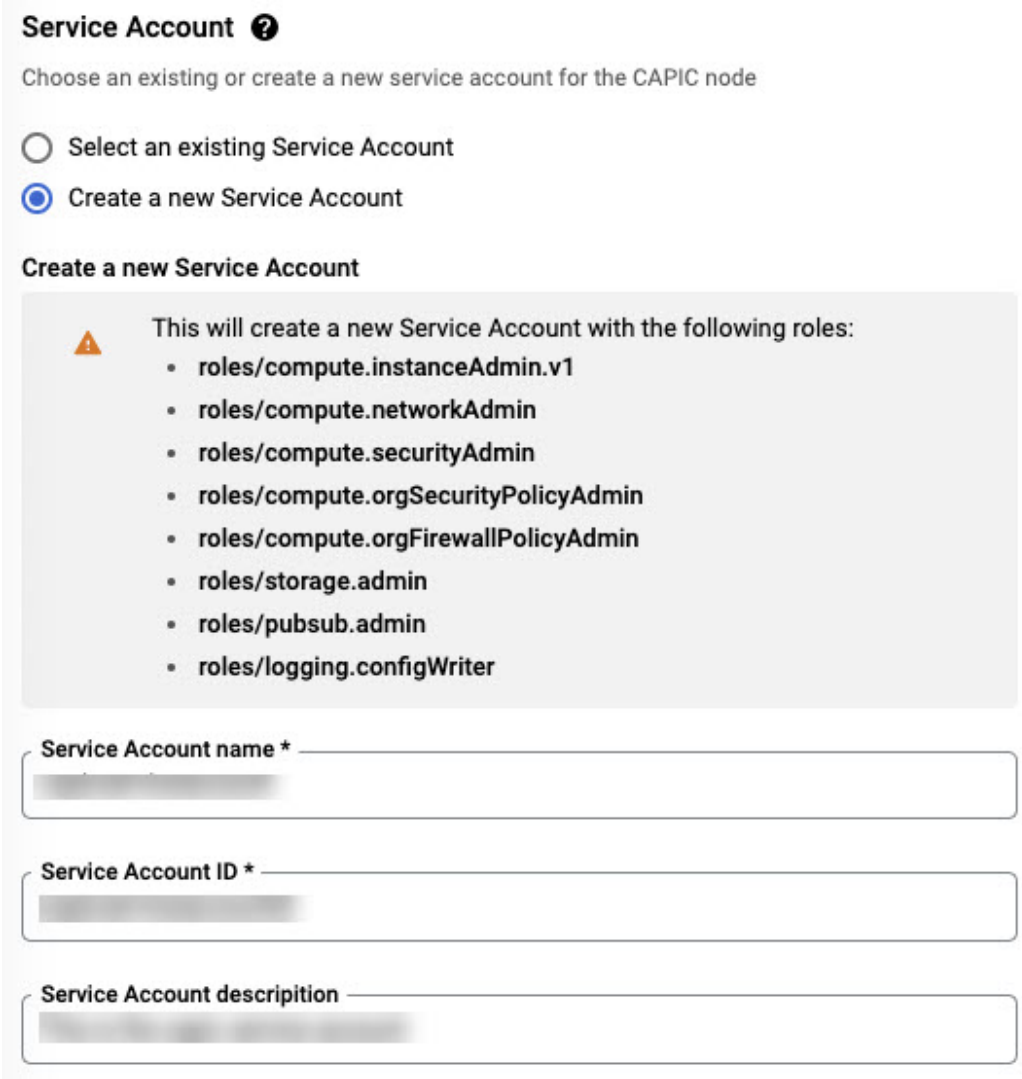
- If you do not have an existing service account that you can use for this Cisco Cloud APIC deployment, you will see a screen similar to the following:



  If you see this message, then you must create a new service account for this Cisco Cloud APIC deployment. Go to the **Create a new Service Account** option below for those instructions.

- **Create a new Service Account**: If you do not have an existing service account that you can use for the Cisco Cloud APIC deployment, click the **Create a new Service Account** option.

Deploying the Cloud APIC in Google Cloud



Enter the following information to create a new service account:

- **Service Account name**: Enter a unique name for this service account. The service account name must be between 1 and 100 characters.
- **Service Account ID**: Enter a unique ID for this service account. The service account ID must be between 6 and 30 characters, and must follow the following pattern:

  [a-z][a-z0-9]+[a-z0-9]

- **Service Account description**: Enter a description for this service account.

- **VPC subnet cidr**: Enter the subnet CIDR to create the subnet and launch the Cisco Cloud APIC from this subnet.

  This must be a valid CIDR in the form `x.x.x.x/24`. The subnet mask must be at least /24.

- **Admin user password**: Enter the password of the Cisco Cloud APIC admin user.

  The password should follow these rules:

- Contain eight or more characters
- At least one letter
- At least one number
- At least one special character

- **Remote Access**: Enter the external network allowed to access the Cisco Cloud APIC.

  This must be a valid IP CIDR in the form `x.x.x.x/xx`.

Step 6 Click the box at the bottom of the page to accept the Google Cloud terms, then click **DEPLOY**.

The **Deployment Manager** window appears. A messages saying that the Cisco Cloud APIC is being deployed will appear for roughly 5-10 minutes.

- Wait for the message saying that the Cisco Cloud APIC has been deployed before proceeding.
- Once you see that message, wait for roughly 10 additional minutes for the system to come to the operational state. You will not be able to log into the Cisco Cloud APIC using the password until the system comes to the operational state.

Note If you want to delete a Cisco Cloud APIC deployment in Google Cloud for any reason, see Deleting a Cisco Cloud APIC Deployment in Google Cloud, on page 10 for those procedures.

What to do next

This infra service account that you created with these procedures will be used for each of the user-tenant projects (managed tenants) to establish communication between the infra and user-tenant projects. Next, go to Configuring Cisco Cloud APIC Using the Setup Wizard to set up the cloud infrastructure configuration for your Cisco Cloud APIC, where the Cisco Cloud APIC deploys the required Google Cloud constructs.

Deleting a Cisco Cloud APIC Deployment in Google Cloud

These procedures assume that you have already deployed the Cisco Cloud APIC in Google Cloud using the procedures provided in Deploying the Cloud APIC in Google Cloud, on page 5, but now you want to delete that Cisco Cloud APIC deployment in Google Cloud.

If you want to delete a Cisco Cloud APIC deployment for any reason, you will need to delete all the resources that you created earlier before you can delete the deployment. Follow these procedures to delete a Cisco Cloud APIC deployment:

Step 1 If you have an external network deployed in Google Cloud for Cisco Cloud APIC, delete the configured external network.

Skip to Step 2, on page 11 if you do not have an external network deployed in Google Cloud for Cisco Cloud APIC.

a) In the left navigation bar in the Cisco Cloud APIC GUI, navigate to **Application Management** > **External Networks**.
b) In the **External Networks** window, click the box next to the configured external network, then choose **Actions** > **Delete External Network**.

Click **OK** in the confirmation window to delete the external network.

Step 2 If you have cloud routers deployed in any region, disable external connectivity first.

a) In the Cisco Cloud APIC GUI, click the Intent icon ( ).
b) In the **Workflows** area, click **Cloud APIC Setup**.
c) In the **Region Management** area, click **Edit Configuration**.

The **Region Management** page appears.

d) In the **Region Management** page, locate the **External Connectivity** area.

In the **External Connectivity** area, the box next to **Enable** should be checked at this point, indicating that external connectivity is currently enabled.

e) Click the box next to **Enable** to remove the check in the checkbox.

A confirmation window with the following message appears:

```
External Connectivity
Disabling External Connectivity will delete all Hub Networks and IPsec Tunnels, any Route
Leaks for External Networks will be disrupted.
```

f) Click **Confirm** in the confirmation window to disable external connectivity.
g) Click **Save and Continue**, then click **Done**.
h) In the Google Cloud portal, verify that the previously configured VPN connection was successfully deleted by clicking **Hybrid Connectivity** > **VPN**.

You should not see the previously configured VPN connection for your Cisco Cloud APIC in this window.

Step 3 Delete the firewall rules in Google Cloud.

a) In the Google Cloud portal, click **VPC network** > **Firewall**.
b) Click the box next to **Name** to select all of the firewall rules displayed in this window.
c) Click **DELETE**.

Click **DELETE** again in the confirmation window to delete these firewall rules.

Step 4 Delete the deployments in Google Cloud.

a) In the Google Cloud portal, navigate to the **Cloud Deployment Manager** page.
b) Click **GO TO CLOUD DEPLOYMENT MANAGER**.

Your Google Cloud deployments are displayed.

c) Click the box next to the deployment that you want to delete, then click **DELETE**.

In the confirmation window, leave the default setting as-is, where you will delete the deployment and all resources created by the deployment. Click **DELETE ALL** in the confirmation window to delete the deployment.

If the deletion fails, a message is displayed, describing which resource still exists that caused the deletion to fail. Locate and delete that resource in that case, then repeat the steps to delete the deployment.

Step 5 Verify that the current deployment is deleted completely before attempting to redeploy.

After you have deleted the current deployment, wait for roughly 10 minutes before redeploying the Cisco Cloud APIC.