Deploying Cisco Catalyst 8000V Using VM Templates

This chapter specifies the procedure for deploying Cisco Catalyst 8000V on Google Cloud Platform (GCP) by using VM templates, and contains the following sections detailing the various tasks in the procedure.

Create an SSH Key

The first task in the deployment procedure is to create an SSH key. SSH keys act as a method of authentication to access your Cisco Catalyst 8000V instance. When you create an SSH key, a public key and a private key are created in the .ssh directory.

RSA is the default key type until Cisco IOS XE 17.9.x. From Cisco IOS XE 17.10.1a, support for ED25519 key type is added.

To create an SSH key, perform the following steps. Enter the commands in a terminal server.

Step 1 Run the **ssh-keygen -t rsa -f** ~/.ssh/*keyfile* `[`-C *username*`]` command. Here,

~/.ssh/*keyfile* is the directory path and filename of the key, for example, `/users/joe/.ssh/mykey`.

-C *username* is the username that is added as a comment. This variable is optional.

Two key files, a private key and a public key, are created in the .ssh directory, for example, `mykey` and `mykey.pub`.

For more information on creating an SSH key, see Creating a new SSH key. See also Managing SSH keys in Metadata.

Example:

```
ssh-keygen -t rsa -f /users/joe/.ssh/mykey -C joe
```

Step 2 Run the **cat** ~/.ssh/[*keyfile_pub*] command. Here, *keyfile_pub* specifies the public key, for example, `mykey.pub`.

Example:

```
cat /users/joe/.ssh/mykey.pub
```

The system displays the contents of the public key. You will need this public key to create a VM instance.

Create a VPC Network

Before you begin

Learn about VPC networks. For information about VPC networks, see Virtual Private Cloud (VPC) Network Overview and Using VPC Networks.

Step 1 In the navigation pane of the Google Cloud Platform console, choose **VPC network** > **VPC Networks**.

Step 2 Choose **Create VPC Network**.

Step 3 Enter a **Name** for the network.

Step 4 Enter a **Description** for the network.

Step 5 Choose **Subnets** > **Add Subnet**.

Step 6 In the **New Subnet** dialog box, enter a **Name** for the subnet, for example, **`c8kvnet1`**.

Step 7 Choose the appropriate option from the **Region** drop-down list.

Step 8 Enter an **IP address range**, for example, enter 10.10.1.0/24 for the subnet address.

Step 9 Click **Done** to create the subnet.

To create multiple subnets for the VPC network, repeat step 5 to step 9.

Step 10 Click **Create** to create the VPC Network.

Create an External IP Address

To create an external IP address, you must reserve an IP address by performing the following steps. Only devices with external IP addresses can send and receive traffic directly to and from the network. Create the IP address to connect to a VM instance using an SSH session. For more information about IP addresses, see: IP Addresses.

Step 1 In the navigation pane of the Google Cloud Platform console, scroll down to **VPC Network**, and click **External IP Addresses**.

Step 2 Click **Reserve static address**. The following fields are displayed. The permissible values for these fields are listed in the following table:

Table 1: External IP Addresses Fields

Field	Value
Name	Enter a name (in lowercase) for this address.

Field	Value
Description	Enter a description for this address.
Network Service Tier	Premium: The premium tier gives a higher performance than the standard tier. To know more about network tiers in GCP, see Network Service Tiers Overview.
IP Version	The IP version of the instance. Choose **IPv4**.
Type	Choose **Regional**.
Region	Choose a location from the drop-down list, for example, **us-east2**.

Step 3 Click **Reserve** to reserve this IP address.

Create a VM Instance

Upload the VM Image

Perform the following steps to upload a custom Cisco Catalyst 8000V image that you'll use to deploy the VM.

Before you begin

To learn about VM instances in GCP, see Creating and Starting a VM Instance.

Step 1 In the navigation pane of the Google Cloud Platform console, choose **Compute Engine** and **VM Instances**.

Step 2 Click **Create Instance**.

Step 3 To create a new Cisco Catalyst 8000V VM instance by using a boot disk image, do one of the following:

- To create the VM instance using a public OS image, choose **OS Images**. Select the image from the list of images displayed.
- To create the VM instance using a defined list of trusted images, choose **Custom Images** and upload your image.

Configure the Properties for the VM

To configure the properties for your VM instance, perform the following steps in the Create Instance window.

Before you begin

Perform the Create a VM instance task.

Step 1 Specify the name for your VM in the **Name** field. Use only lowercase letters, for example, **`newtestvm`**.

Step 2 Choose the appropriate **Region** from the drop-down list.

Step 3 Specify the zone for your instance in the **Zone** field. The zone is often a data center with a region.

Step 4 Choose one of these machine types from the **Machine Type** drop-down list—n1-standard-2, n1-standard-4, or n1-standard-8. The machine type is associated with an image filename. For example, the 2vCPUs machine type for the Cisco Catalyst 8000V has the image filename n1-standard-2.

Step 5 (Optional) Click **Customize** to customize the number of cores (vCPUs), memory size, and GPUs for your VM instance.

Configure the DIsk Options for the VM

To configure the boot disk options for your VM instance, perform the following steps in the **Boot Disk** section in the **Create Instance** window.

Step 1 Click **Change**.

A pop-up window with the **Boot Disk** options is displayed.

Step 2 Click the **Custom Image** tab, and select the Cisco Catalyst 8000V image that you uploaded.

Step 3 From the **Boot disk** drop-down list, choose the persistent disk storage option for your VM. It is recommended that you choose the **SSD persistent disk** option.

Step 4 In the **Disk Size** field, enter the boot disk size in GB.

Step 5 Click **Select** to save all the disk options.

The name of the Cisco Catalyst 8000V image you selected is displayed in the **Boot disk** section.

Configure the Firewall and Networking Options

Perform the following steps to configure the firewall options and the networking options for your VM.

Step 1 In the **Identity and API Access** field, the default value is **Service account**. Do not change this value. This field specifies how your VM instance interacts with the other resources within your project.

Step 2 In the **Firewall** field, choose either **Allow HTTP traffic** or **Allow HTTPS traffic** to allow HTTP or HTTPS traffic to the VM.

Step 3 Click the **Networking** tab, and configure the following networking properties.

a) Click **Add interface**.
b) In the **Networking Interface** window, choose the default interface for your VM. For example, the default security group is 10.12.0.2.
c) Choose the first default interface for your VM.
d) From the **IP Forwarding** drop-down list, choose **On** to prevent the traffic from being blocked.
e) From the **Primary internal IP** drop-down list, choose **Ephemeral (automatic)**. This private IP address is obtained automatically from the selected subnet.
f) From the **External IP** drop-down list, choose **Ephemeral (automatic)**. The external IP address of each interface is either ephemeral or static. When you select the **Ephemeral (automatic)** option, you can use this public IP address when you start an SSH session from a terminal server. You can also choose to set a static address as this external IP address.

Step 4 Click **Done** to save the properties and go to the previous window.

Add an Additional Interface

Perform these steps to configure an additional interface when you deploy a Cisco Catalyst 8000V VM instance in GCP. This is an optional task. If you don't want to add another interface, proceed to Configuring the Security Properties section.

Step 1 Click **Add network interface** to add a second interface.

Note For every new interface that you add, you must create a new VPC.

Step 2 In the **Name** field, specify the name of the second interface.

Step 3 From the **Network** drop-down list, choose the network for your second interface..

Step 4 From the **Subnetwork** drop-down list, select the subnetwork.

Step 5 In the primary internal IP field, choose **Ephemeral (automatic)**. The private IP address is obtained automatically from the subnet you selected.

Step 6 In the external IP field, choose **None**.

Note If you have created the second or additional interface, you do not need a public IP address for this interface because you have already set an external IP address for your first interface.

Step 7 Click **Done**.

Configure the Security Options

Step 1 In the **Security** section, in the **Block Project-Wide SSH Keys** field, paste the SSH key from the public key that you created as described in Create an SSH Key.

Note The SSH key is an instance-wide SSH key. The settings are applicable only to this VM instance and not to the whole project.

Step 2 (Optional) To provide custom data, click **Management**.

Step 3 (Optional) Copy and paste the custom data in the **Startup Script** field. For more information on custom data, see the Day Zero Configuration chapter.

Step 4 Click **Create**.

The newly created Cisco Catalyst 8000V VM instance starts, and this process could take several minutes. To check whether the VM instance is up, click on your VM on the **Instances** page. Choose **Logs** > **Serial Port**. The status is indicated here.

Access the Cisco Catalyst 8000V CLI

SSH keys act as the authentication method to access your Cisco Catalyst 8000V instance. Apart from the RSA key type, Cisco Catalyst 8000V also supports the ED25519 key type from Cisco IOS XE 17.10.1a. To set up an SSH using the CLI, perform the following steps.

Before you begin

- Perfrom the Day 0 configuration as mentioned in the Day Zero Configuration chapter.
- Ensure that the Cisco Catalyst 8000V VM instance is up. This is required for you to access the Cisco Catalyst 8000V VM instance using an SSH session.

Note In the VM Instances window, the **SSH** tab is not enabled for a Cisco Catalyst 8000V VM. You must set up an SSH using the following commands.

SUMMARY STEPS

1. **ssh -i** ~/.ssh/[*keyfile*] *username@ instance-external-IP* .
2. **interface** *interface-name*
3. **ip address dhcp**
4. **speed <interface speed>**
5. **no negotiation auto**
6. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**ssh -i** ~/.ssh/[*keyfile*] *username@ instance-external-IP* . **Example:** `ssh -i /users/joe/.ssh/mykey.pub joe@10.0.0.2`	Logs into the Cisco Catalyst 8000V instance using an SSH session. Here, `~/.ssh/keyfile` represents the path and filename of the public key. After logging in, you can enter the Cisco IOS XE commands using the CLI.
Step 2	**interface** *interface-name* **Example:** `Router(config)# interface GigabitEthernet1`	Enters interface configuration mode. It is recommended that you perform the following steps to increase the interface's speed for each interface.
Step 3	**ip address dhcp** **Example:** `Router(config-if)# ip address dhcp`	Acquires an IP address on an interface from DHCP.
Step 4	**speed <interface speed>** **Example:** `Router(config-if)# speed 10000`	Sets the speed of the interface.

	Command or Action	Purpose
Step 5	**no negotiation auto** **Example:** `Router(config-if)# no negotiation auto`	Disables auto negotiation.
Step 6	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode. (Optional) Repeat steps 2 to 6 to increase the speed of the second interface of the Cisco Catalyst 8000V instance.

Configuring a Sample Feature

After you deploy Cisco Catalyst 8000V in GCP and access the CLI, you can configure the supported features. In this section, the following code sample shows how to configure an IPsec VPN on a Cisco Catalyst 8000V instance running on GCP.

```
crypto isakmp policy 1
 encr aes
 hash sha256
 authentication pre-share
 group 14
crypto isakmp key cisco123 address 0.0.0.0
crypto ipsec transform-set T1 esp-3des esp-md5-hmac
 mode transport
crypto ipsec profile P1
 set transform-set T1
interface Tunnel0
 ip address 10.0.0.2 255.255.255.0
 tunnel source GigabitEthernet1
 tunnel mode ipsec ipv4
 tunnel destination 198.51.100.253
 tunnel protection ipsec profile P1
end

ip route 6.6.6.6 255.255.255.255 Tunnel0
```