

Deploying Cisco Catalyst 8000V by Using the GCP Console

This chapter specifies the procedure for deploying Cisco Catalyst 8000V on Google Cloud Platform (GCP) by using the GCP Console. The GCP Console is a web-based graphical user interface (GUI) that enables the deployment of Cisco Catalyst 8000V instances manually.

- Guidelines for Deploying Cisco Catalyst 8000V, on page 1
- Create an SSH Key, on page 2
- Create a VPC Network, on page 3
- Create an External IP Address, on page 3
- Deploy the Cisco Catalyst 8000V Instance, on page 4
- Access the Cisco Catalyst 8000V CLI, on page 7
- Configure a Sample Feature, on page 9

Guidelines for Deploying Cisco Catalyst 8000V

Before you deploy a Cisco Catalyst 8000V instance, see these guidelines and recommendations.

Restrictions

- You can choose the gVNIC option only if you're using an N4 instance. If you've deployed Cisco Catalyst 8000V in GCP by using N1 or N2 instance series, you cannot resize your existing VMs to N4 instance series due to the variation in disks.
- If you use the Infrastructure Manager through public worker pools to run the Terraform that is used for the VM deployment, your permissions might restrict the usage of public pools, especially if you use VPC Service Controls. To overcome this issue, use Google Cloud Build, which allows the creation of private worker pools with your own security and configuration. Use this method to deploy VMs if the standard GUI launch option is restricted.

  Download the Cisco Catalyst 8000V Terraform through the Command-Line Deployment option and add the private worker pool option in the Terraform deployment script. First, manually deploy the Cisco Catalyst 8000V instance via CLI and then add the worker pool parameters.

Guidelines

- A maximum transmission unit (MTU) is the size, in bytes, of the largest possible IP packet, including IP headers, layer 4 protocol headers, and layer 4 data, that can fit inside an Ethernet frame.

  When using gvNIC-based instances, the MTU of the GCP VPC will be inherited by the guest VM, that is, Cisco Catalyst 8000V. If the GCP VPC MTU is set below 1500 bytes, Cisco Catalyst 8000V uses this MTU value. If the GCP VPC MTU is set above 1500 bytes, Cisco Catalyst 8000V uses an MTU ranging from 1500 bytes up to the configured MTU of the VPC.

  For Cisco Catalyst 8000V deployments in SD-WAN mode that utilize bootstrap configuration from vManage, it is important that the configured MTU matches the GCP VPC MTU, especially when the VPC MTU is less than 1500 bytes. Any mismatch in MTU values could lead to deployment failures.

  To configure the MTU settings, see Maximum transmission unit.

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.

Procedure

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

A Virtual Private Cloud (VPC) network is a virtual version of a physical network that is implemented in the cloud service provider. Create a VPC network to provide connectivity to your VM instance.

Before you begin

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

Procedure

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 In the **Name** field, specify a name for the network.

Step 4 In the **Description** field, provide 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.

Procedure

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.
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.

Deploy the Cisco Catalyst 8000V Instance

This section specifies the overall deployment process for creating a Cisco Catalyst 8000V instance by using the GCP Console. See each of these sections to view the deployment workflow in detail.

Choose the Machine Configuration

Perform these steps to set the machine configuration for a VM instance.

Before you begin

- Billing must be enabled for your GCP account.
- Familiarize yourself with the basic concepts of creating a VM instance. For more information, see Creating and Starting a VM Instance.

Procedure

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

Step 2 In the **VM Instances** page, click the **Create Instance** button.

Step 3 Set these machine configurations:

Field	Description
Name	Specify the name for your VM in this field. Use only lowercase letters, for example, **`newtestvm`**.
Region	Choose the appropriate region from the drop-down list.

Field	Description
Zone	Specify the zone for your instance in this field. The zone is often a data center within a region.

Step 4 In the Machine Type area, choose one of these two settings:

- **Preset**: The preset amounts of vCPUs and memory will be selected.
- **Custom**: Choose this option to customize the number of cores (vCPUs), memory size, and GPUs for the VM instance.

Step 5 Choose the required machine type from the **Machine Type** drop-down list.

The machine type from a machine family determines the resources available to that instance. Each machine family is further organized into machine series and predefined machine types within each series. For example, within the N2 machine series in the general-purpose machine family, you can select the n2-standard-4 machine type.

To view the list of supported machine types and instances, see Supported Instance Types for Google Cloud Platform.

Step 6 Configure the **CPU Platform** and **Visible Core Count** settings, if applicable.

Configure the OS and Storage Properties

Perform these steps to configure the OS and storage properties for the VM instance.

Procedure

Step 1 In the Web UI, from the left navigation pane, choose **OS and storage**.

The system displays the OS details such as the image name, size, license type, and so on.

Step 2 To modify any of these options, choose **Change**.

Step 3 In the **Boot disk** pop-up window, configure the boot disk options.

Step 4 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 the **Public Images** tab. Select the image from the list of images displayed.
- To create the VM instance using a defined list of trusted images, choose the **Custom Images** tab and select the Cisco Catalyst 8000V image.

Note
If you chose the N4 instance family under Machine Type, you must choose a Cisco Catalyst 8000V 17.18.1 or later image only.

Step 5 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 6 In the **Disk Size** field, enter the boot disk size in GB.

Configure the Firewall and Networking Options

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

Procedure

Step 1 In the left navigation page, choose **Networking**.

Step 2 In the **Firewall** field, select either **Allow HTTP traffic**, **Allow HTTPS traffic**, or **Allow Load Balancer Health Checks** radio button.

Step 3 Optionally, choose a **Network Tag** for your instance. To learn more about tags, see Manage Tags for Resources.

Step 4 From the **Hostname** field, set a hostname for your VM instance, if required.

Step 5 From the **IP Forwarding** drop-down list, choose **On** to prevent the traffic from being blocked.

Step 6 Under **Network Interfaces**, configure these settings:

a) **Network**: Choose the network in the region where you want to deploy the Cisco Catalyst 8000V instance. You must create the network before you create the Cisco Catalyst 8000V instance. Ensure that at least one subnet is associated to that network. For more information about networks, see Virtual Private Cloud Network Overview.

b) **Subnetwork**: Choose the subnet that is associated with the selected Network (VPC). This subnet acts as the first Network Interface (nic0) of the Cisco Catalyst 8000V instance.

c) **Network Interface Card**: Choose the network interface card for the instance from this drop-down list. You can choose the gVNIC option only if you're using an N4 instance. If you've deployed Cisco Catalyst 8000V in GCP by using N1 or N2 instance series, you cannot resize your existing VMs to N4 instance series due to the variation in disks.

d) **IP Stack Type**: Choose **IPv4 and IPv6 (dual-stack)** or **IPv6 (single-stack)**.

e) **Alias IP Range**: Configure this field if you want to assign multiple internal IP addresses to the VM instance.

Step 7 (Optional) To add an interface, click the **Add a Network Interface** option.

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.

Procedure

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

Perform these steps to configure the SSH option for the VM instance. If required, add a startup script to customize the boot options for the instance.

Procedure

Step 1 In the left navigation pane, choose **Security**.

Step 2 In the **VM Access** area, in the **SSH Keys** field, paste the SSH key from the public key that you created as described in Create an SSH Key.

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

Step 3 In the **Advanced** area, add your startup configuration by copying and pasting the startup configuration information in the **Startup script** field.

If the startup script is not specified, the default configuration is applied.

Step 4 Click **Create**.

The newly created Cisco Catalyst 8000V VM instance starts. This process could take several minutes. To verify that the VM instance is running, click your VM on the **Instances** page. Choose **Logs** > **Serial Port**. The status appears in this page.

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 these 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.

Procedure

Step 1 **ssh -i** ~/.ssh/[*keyfile*] *username@ instance-external-IP* .

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.

Example:

```
ssh -i /users/joe/.ssh/mykey.pub joe@10.0.0.2
```

Step 2 **interface** *interface-name*

Enters interface configuration mode.

Example:

```
Router(config)# interface GigabitEthernet1
```

It is recommended that you perform the following steps to increase the interface's speed for each interface.

Step 3 **ip address dhcp**

Acquires an IP address on an interface from DHCP.

Example:

```
Router(config-if)# ip address dhcp
```

Step 4 **speed <interface speed>**

Sets the speed of the interface.

Example:

```
Router(config-if)# speed 10000
```

Step 5 **no negotiation auto**

Disables auto negotiation.

Example:

```
Router(config-if)# no negotiation auto
```

Step 6 **exit**

Exits the interface configuration mode.

Example:

```
Router(config-if)# exit
```

(Optional) Repeat steps 2 to 6 to increase the speed of the second interface of the Cisco Catalyst 8000V instance.

Configure 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
```