Cisco CSR 1000v Deployment Guide for Google Cloud Platform

First Published: 2018-07-18

Last Modified: 2019-07-31

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2018-2019 Cisco Systems, Inc. All rights reserved.

CONTENTS

CHAPTER 1 **Deploying Cisco CSR 1000v on Google Cloud Platform** 1

Overview of Cisco CSR 1000v on Google Cloud Platform 1

Prerequisites for Deploying Cisco CSR 1000v on Google Cloud Platform 1

Google Cloud Platform Resources 2

Cisco CSR 1000v with Two Network Interfaces—Example 2

Licensing for a Cisco CSR 1000v on Google Cloud Platform 3

Bring Your Own License Model 3

CHAPTER 2 **How to Deploy a Cisco CSR 1000v on Google Cloud Platform** 5

Create an SSH Key 5

Create a VPC Network 6

Create an External IP Address 6

Create Firewall Rules 7

Create a VM Instance 8

Create Routes 10

Access the Cisco CSR 1000v CLI 10

Configuring IPsec VPN for a Cisco CSR 1000v on Google Cloud Platform 11

CHAPTER 3 **Deploy a CSR 1000v by Using a Solution Template** 13

Create an SSH Key 13

Create a VPC Network 14

Deploy the CSR Solution Template 14

CHAPTER 4 **Deploying a Cisco CSR 1000v VM Using Custom Data** 21

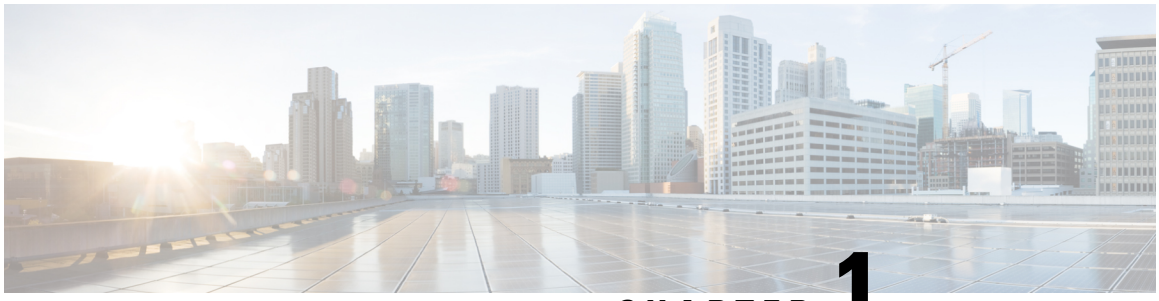
Editing the Custom Data 21

Configuring the IOS Configuration Property 22

Configuring the Scripts Property 22
Configuring the Script Credentials Property 23
Configuring the Python package Property 24
Configuring the License property 24
Accessing the Custom Data 25
Verifying the Custom Data Configuration 26

CHAPTER 5 **Usage Guidelines for Custom Routes** 29
Introduction to Custom Routes 29
Custom Routes in the Same VPC Network 29
Routing Between VPC Networks or On-Premises Networks 29

CHAPTER 6 **Cisco CSR 1000v Deployment Guidelines and Best Practices** 31
Differences Between CSR 1000v Deployments 31
Best Practices and Caveats 32
Other Related Resources 32



CHAPTER 1

Deploying Cisco CSR 1000v on Google Cloud Platform

- Overview of Cisco CSR 1000v on Google Cloud Platform, on page 1
- Prerequisites for Deploying Cisco CSR 1000v on Google Cloud Platform, on page 1
- Google Cloud Platform Resources, on page 2
- Cisco CSR 1000v with Two Network Interfaces—Example, on page 2
- Licensing for a Cisco CSR 1000v on Google Cloud Platform, on page 3

Overview of Cisco CSR 1000v on Google Cloud Platform

The Cisco Cloud Services Router (CSR) 1000V is a virtual router running Cisco IOS XE. Most Cisco IOS XE features are available on the Cisco CSR 1000V.

You can choose to deploy Cisco CSR 1000V software on new or existing infrastructure, such as a VPC network.

The following VPN features are supported on the Cisco CSR 1000V: IPsec, DMVPN, FlexVPN, Easy VPN, and SSLVPN. You can use dynamic routing protocols, such as EIGRP, OSPF, and BGP.

You can secure, inspect, and audit network traffic with the application-aware Zone-Based Firewall. You can also use IP SLA and Application Visibility and Control (AVC) to detect performance issues, fingerprint application flows, and export detailed flow data.

Prerequisites for Deploying Cisco CSR 1000v on Google Cloud Platform

The following are prerequisites when deploying a Cisco CSR 1000v on Google Cloud Platform (GCP):

- You must have a user account or subscription with Google Cloud Platform.
- Several resources must be deployed before, or during, the deployment of the Cisco CSR 1000v.
- To obtain full traffic throughput, you must obtain a software license for the Cisco CSR 1000v. Otherwise, throughput is limited to 1 Mbps.

Google Cloud Platform Resources

To deploy a Cisco CSR 1000V on Google Cloud Platform (GCP), you must create a project with the following resources: virtual machines, interfaces, VPC networks, routes, public IP addresses, firewall rules, and storage. Resources that exist in different projects can only connect through an external network. For more information on projects, see The Project resource, and Creating and Managing Projects in the Google Cloud Platform (GCP) resource hierarchy.

The following list is a summary of some of the resources that are used by a project for the Cisco CSR 1000V on Google Cloud Platform:

- Virtual Private Cloud (VPC) network—connects VM instances and has subnets with defined IP addresses.
- VM instance—created from a boot disk image. For example, n1-standard-2 (2 vCPUs, 7.5 GB RAM, 2 virtual Network Interface Cards (vNICs)).
- Subnet—includes a subnet route, which is the next hop IP address. The next hop IP address defines a communication path to and from the resources for the subnet.
- Firewall rules—security rules for the VPC network.
- Routes—a route maps an IP address range to a destination. This route allows the VPC network to send packets to the correct destination for an IP address. For more information, see Routes Overview.
- Storage—persistence disk storage that is used to hold disk or container images for VM instances. For more information, see Storage Options.
- Interfaces—You can assign a public IP address to each network interfaces of a Cisco CSR 1000v VM. (Usually, a public IP address is assigned to the first interface.) All Cisco CSR 1000v VM interfaces are in a private subnet. You can assign the IP address of each private interface using the **ip dhcp address** command in the interface configuration. Alternatively, you can assign a static IP address using the **ip address** command (for example, `ip address 1.1.1.1 255.255.255.0`). If you use a static IP address, ensure that the IP address is the same as the IP address assigned by GCP. Later, to view some details about the interface, use the **show ip interface brief** command.

Supported Instance Types

The following instance types are supported for this deployment:

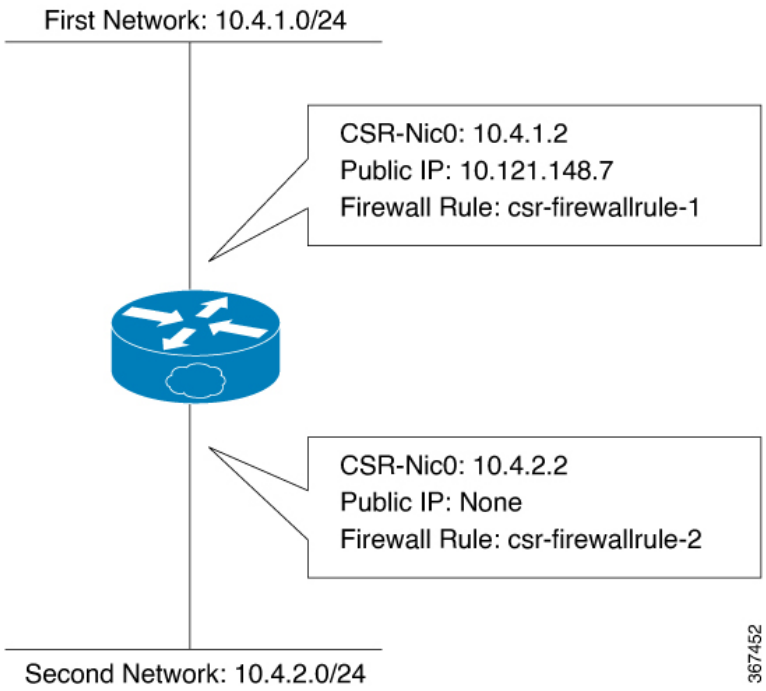
- N1-standard-8
- N1-standard-4
- N1-standard-2

Cisco CSR 1000v with Two Network Interfaces—Example

This example shows a topology diagram that results after deploying a Cisco CSR 1000v on GCP.

The Cisco CSR 1000v VM was created from image "n1-Standard-2" and has two interfaces and two vCPUs. This Cisco CSR 1000v has a public IP address of 40.121.148.7 for the interface of the first subnet (NIC0). The firewall rule "csr-firewallrule-1" is assigned to this interface.

Note Create a firewall rule to allow traffic to pass in a custom VPC network. (Without a firewall rule, by default, all traffic is blocked.)



Licensing for a Cisco CSR 1000v on Google Cloud Platform

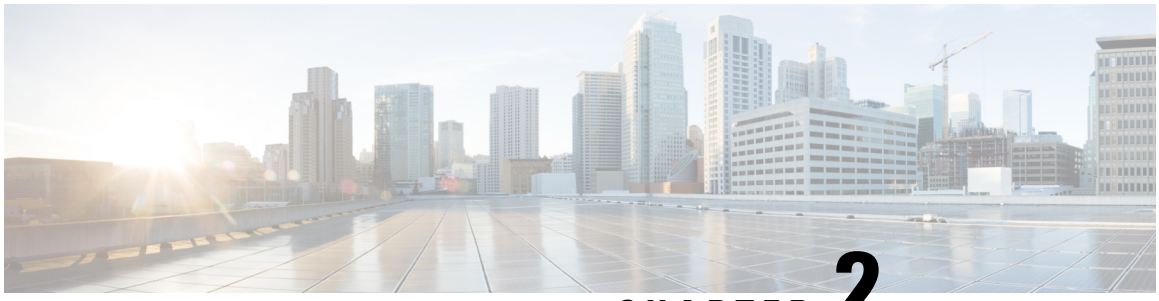
The Cisco CSR 1000v on GCP supports the following license model:

Bring Your Own License Model

The Bring Your Own License (BYOL) licensing model, for the Cisco CSR 1000v on GCP, supports the following two types of license:

- Cisco Software License (CSL)—uses a traditional Product Authorization Key (PAK) licensing model. For further information on using a PAK, see Cisco Software Licensing (CSL).
- Cisco Smart Licensing—assigns a license to Cisco CSR1000v instances dynamically. This allows you to manage licenses across different CSR1000v instances without having to lock each license to a specific CSR1000v UDI serial number. For more information on Cisco Smart Licensing, see Smart Licensing.

The cost of licensing using BYOL in GCP, includes the cost of a GCP instance and the cost of a Cisco CSR 1000v license.



CHAPTER 2

How to Deploy a Cisco CSR 1000v on Google Cloud Platform

Deploying a Cisco CSR 1000v on Google Cloud Platfrom involves these tasks:

- Create an SSH Key, on page 5
- Create a VPC Network, on page 6
- Create an External IP Address, on page 6
- Create Firewall Rules, on page 7
- Create a VM Instance, on page 8
- Create Routes, on page 10
- Access the Cisco CSR 1000v CLI, on page 10
- Configuring IPsec VPN for a Cisco CSR 1000v on Google Cloud Platform, on page 11

Create an SSH Key

To create an SSH key, which is required to access a Cisco CSR 1000v VM instance, perform the following steps. Enter the commands at a terminal server.

Step 1 Execute **ssh-keygen -t rsa -f** ~/.ssh/*keyfile* [-C *username*]

~/.ssh/*keyfile* - Directory path and filename of the key. Example: `/users/joe/.ssh/mykey`.

-C *username* - Username, which is added as a comment. This variable is optional.

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

For more information on creating an SSH key, see *Creating a new SSH key* in the Google Cloud Platform documentation. See also Managing SSH keys in Metadata.

Example:

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

Step 2 **cat** ~/.ssh/[*keyfile_pub*]

keyfile_pub specifies the public key; for example, `mykey.pub`.

Example:

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, on page 8.

Create a VPC Network

Before you begin

To learn about VPC networks, see: Virtual Private Cloud (VPC) Network Overview and Using VPC Networks.

Step 1 From the navigation pane in the Google Cloud Platform console, scroll down to **VPC network** and select **VPC networks**.

Step 2 Click **Create VPC Network**.

Step 3 Enter a **Name** for the network. **CREATE VPC NETWORK**.

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

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

Step 6 In the New Subnet dialog box, Enter a **Name** for the subnet. For example, `csrnet1`.

Step 7 Select the appropriate option in the **Region** field.

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 steps 5 to 9.

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

Create an External IP Address

To create an external IP address, you reserve an IP address by performing the following steps. You can later use the IP address to connect to a VM instance using an SSH session.

Step 1 From the navigation menu in the Google Cloud Platform Console, scroll down to "VPC network" and select "External IP Addresses".

For more information about IP addresses, see: IP Addresses.

Step 2 Click **Reserve static address**.

These are the field names and permissible values:

Table 1: External IP Addresses Fields

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

Field	Value
Network Service Tier	premium The premium tier gives a higher performance than the standard tier.
IP Version	IPv4
Type	Regional
Region	Select a location. Example: "us-east2".

Step 3 Click **Reserve**.

Reserves this IP address.

Create Firewall Rules

To enable traffic to pass to a VM instance, you must create a firewall rule by performing the following steps. For more information on firewall rules, refer to "Firewalls" in VPC Networking and Firewalls.

Note After creating a firewall rule, you can change only some of its values. The following properties cannot be changed: "Network" (that is, the network to which the rule originally applied), "Priority", "Direction of traffic," and "Action on match". Therefore, in future you may need to delete the original rule and replace it with a new rule.

Step 1 From the navigation menu in the Google Cloud Platform Console, scroll down to "VPC network" and select "Firewall Rules".

Step 2 Click "CREATE FIREWALL RULE".

Enter the specified values for the following fields:

Table 2: Firewall Rules Fields

Field	Value
Network	Default.
Priority	1000 Values: 0–65535. Default: 1000. A lower value results in a higher priority being assigned to this rule.
Traffic Direction	Ingress. Values: Ingress, Egress.

Field	Value
Action on Match	Allow. Values: Allow, Deny.
Targets	All instances in the network. Values: "All instances in the network", "Specified target tags", "Specified service account".
Region	Select a location. Example: "us-east2".
Source Filters (optional)	Choose to filter the traffic using up to four different source filter types. For example, if you choose to specify a source IP range, you can enter 0.0.0.0/0 to select any IP address.
Source IP Ranges	0.0.0.0/0 (selects all IP ranges in the network).
Protocols and Ports	A protocol and port range String multiple protocol and port ranges together. For example: "icmp", "udp:4789-4790", "tcp:0-6553".

Step 3 Click **Create**.

Creates a firewall rule. To add another firewall rules, repeat the previous steps.

Create a VM Instance

Perform the following steps to deploy a Cisco CSR 1000v VM instance on Google Cloud Platform.

For more information, see: Creating and Starting a VM Instance.

Step 1 Click **Compute Engine** and **VM Instances**.

Step 2 Click **CREATE INSTANCE**.

Select a boot disk to create a new CSR 1000v VM instance (from "OS Images" or custom images) and enter values for the following fields.

Step 3 Specify the name for your VM ins the **Name** field. You can

Name for your VM, using only lowercase letters. Example: "newtestvm".

Step 4 Specify the **Region**.

Step 5 Specify the **Zone**. The zone is often a data center with a region.

Step 6 Select the **Machine type**. Select one of the following options from the drop-down list: **`n1-standard-2`**, **`n1-standard-4`**, **`n1-standard-8`**. The machine type is associated with an image filename. For example, the 2vCPUs machine type for the Cisco CSR 1000v has an image filename of "n1-standard-2".

Step 7 (Optional) Click **Customize** to select the number of cores(vCPUs), memory size, and GPUs.

Step 8 In the **Boot disk** section, click **Change**.

Step 9 Select a Cisco CSR 1000v image. See the Marketplace to select the CSR 1000v image.

Step 10 In the Boot Disk window, for the **Boot disk** type, select **SSD persistent disk**.

Step 11 Click **Select**.

In the **Create an Instance** window, the name of the previously selected image appears in the **Boot disk** section.

Note In the **Identity and API Access** section, do not change the value of the **Service account**.

Step 12 Select **Allow default access**.

Step 13 In the **Firewall** section, select either: **Allow HTTP traffic** or **Allow HTTPS traffic**.

Step 14 Click **Management, disks, networking, SSH keys**.

Step 15 Click **Networking**.

Step 16 Click **Add interface**.

Step 17 In the Networking Interfaces dialog box, select the default interface. For example, the default security group is 10.142.0.0/20.

Step 18 In the Networking Interface window, select the first default interface.

Step 19 Set **IP Forwarding** to **On**. This setting prevents the traffic from being blocked.

Step 20 Set **Primary internal IP** to Ephemeral (automatic). This private IP address is obtained automatically from the selected subnet.

Step 21 Set **External IP** to Ephemeral (automatic).

Specify Ephemeral (automatic). Later, you can use this public IP address when you start an SSH session from a terminal server. You may also choose to specify this External IP address as static. The external IP address of each interface is either ephemeral or static.

Step 22 Click **Done**.

Step 23 (Optional) Click **Add network interface** to add a second interface.

This step is optional. If you do not want to add a second interface, go to step 31 "SSH Keys".

Step 24 Enter **Name** to specify the name of the second interface.

Step 25 Select a **Network**.

Step 26 Select a **Subnetwork**.

Step 27 For the primary internal IP, select **Ephemeral (automatic)**. The private IP address is obtained automatically from the selected subnet.

Step 28 For the external IP, select **None**.

For the second interface, you can select **None**. You do not need a public IP address on this interface as you previously set an external IP address on the first interface.

Step 29 Click **Done**.

Step 30 In the **SSH Keys** section, paste the SSH key from the public key that you created earlier in the Create an SSH Key, on page 5 section.

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 31 Click **Create**.

The newly created Cisco CSR 1000v VM instance boots up, and may take 5 to 10 minutes. To check whether the VM instance is up, click the Cisco CSR 1000v name and under **Logs**, click **Serial Port**. If you see, for example, "Adding eth0 entry", it indicates that the instance is still booting up.

Create Routes

Perform the following steps to create each route for traffic in the VPC network.

Step 1 Under "VPC Network", select **Routes**.

The "Route details" window opens.

Step 2 Click **CREATE ROUTE**.

Enter the specified values for the fields:

Table 3: Route Fields

Field	Value
Name	Enter a name (in lowercase) for this address. Example: "northboundtosouthbound".
Description	Enter a description for this address. Example: "Route to Linux".
Network	Name of the VPC network. Example: "csrnet220".
Destination IP range	Example: 10.12.1.0/24.
Next hop	Enter a value for the "Next hop" destination, using one of the following fields: Instance, Gateway, or IP address. Example (IP address): 10.11.1.2.

Step 3 Click **Create**.

Creates a route.

Access the Cisco CSR 1000v CLI

This task describes how to access the CLI of the Cisco CSR 1000v VM using SSH and how to increase the speed of the interfaces.

Before you begin

Before accessing the Cisco CSR 1000v VM instance using an SSH session, the Cisco CSR 1000v VM instance must be up.

Note In the "VM instances" window, the SSH tab is not enabled for a Cisco CSR 1000v VM. You must, therefore, set up an SSH using CLI commands, which are described in the table at the Procedure section.

Procedure

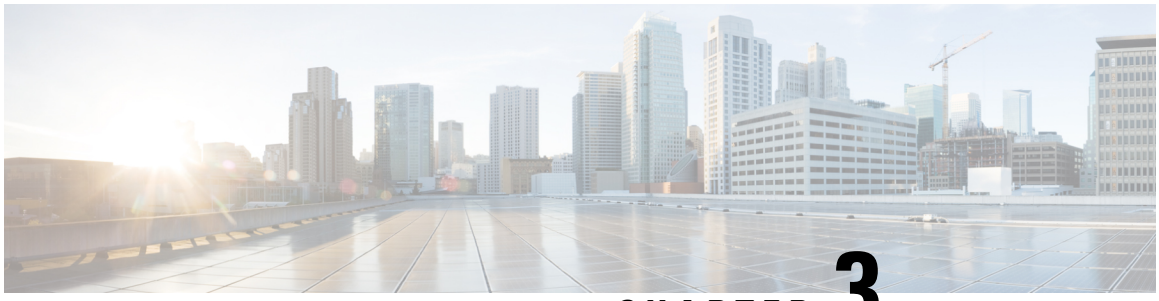
	Command or Action	Purpose
Step 1	In a terminal server, enter the following command: **ssh -i** ~/.ssh/[*keyfile*] *username@ instance-external-IP* . **Example:** `ssh -i /users/joe/.ssh/mykey.pub joe@10.0.0.2`	Logs into the Cisco CSR 1000v using an SSH session. ~/.ssh/keyfile represents the path and filename of the public key. After logging in, you can enter Cisco IOS XE commands using the CLI.
Step 2	**interface** *interface-name* **Example:** `Router(config)# interface GigabitEthernet1`	Enters interface configuration mode. (The following steps are recommended in order to increase the speed to 10 Gbps 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 10000** **Example:** `Router(config-if)# speed 10000`	Set speed to 10 Gbps.
Step 5	**no negotiation auto** **Example:** `Router(config-if)# no negotiation auto`	Disables autonegotiation.
Step 6	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode.
Step 7	Repeat steps 2 to 6 to increase the speed for the second interface of the Cisco CSR 1000v.	

Configuring IPsec VPN for a Cisco CSR 1000v on Google Cloud Platform

This example shows the configuration of an IPsec VPN on a Cisco CSR 1000v 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
```



CHAPTER 3

Deploy a CSR 1000v by Using a Solution Template

You can deploy a CSR 1000v router in Google Cloud Platform (GCP) in two ways: by using a VM instance, or by using a solution template. This chapter specifies how you can deploy a CSR 1000v solution template and the configuration of the associated resources in the service provider's cloud.

- Create an SSH Key, on page 13
- Create a VPC Network, on page 14
- Deploy the CSR Solution Template, on page 14

Create an SSH Key

To create an SSH key, which is required to access a Cisco CSR 1000v VM instance, perform the following steps. Enter the commands at a terminal server.

Step 1 Execute **ssh-keygen -t rsa -f** ~/.ssh/*keyfile* [-C *username*]

~/.ssh/*keyfile* - Directory path and filename of the key. Example:`/users/joe/.ssh/mykey`.

-C *username* - Username, which is added as a comment. This variable is optional.

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

For more information on creating an SSH key, see *Creating a new SSH key* in the Google Cloud Platform documentation. See also Managing SSH keys in Metadata.

Example:

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

Step 2 **cat** ~/.ssh/[*keyfile_pub*]

keyfile_pub specifies the public key; for example, `mykey.pub`.

Example:

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, on page 8.

Create a VPC Network

Before you begin

To learn about VPC networks, see: Virtual Private Cloud (VPC) Network Overview and Using VPC Networks.

Step 1 From the navigation pane in the Google Cloud Platform console, scroll down to **VPC network** and select **VPC networks**.

Step 2 Click **Create VPC Network**.

Step 3 Enter a **Name** for the network. **CREATE VPC NETWORK**.

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

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

Step 6 In the New Subnet dialog box, Enter a **Name** for the subnet. For example, `csrnet1`.

Step 7 Select the appropriate option in the **Region** field.

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.

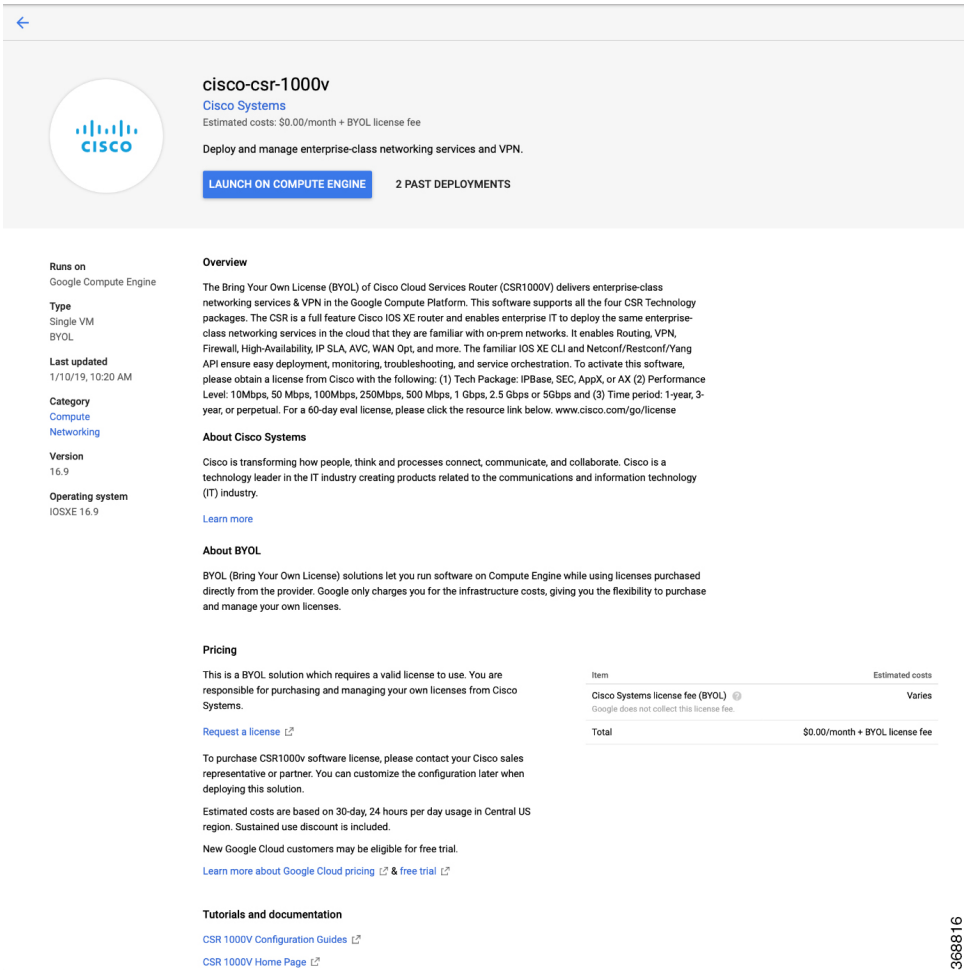
To create multiple subnets for the VPC network, repeat steps 5 to 9.

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

Deploy the CSR Solution Template

Step 1 Go to the Google Marketplace and search for Cisco CSR100v. Select the CSR Template.

Figure 1: Select CSR Deployment Template



Step 2 Click **Launch On Compute Engine**.

Step 3 In the New Cisco 1000v Deployment screen, provide the following details:

a) **Deployment name**: This field is filled by default, and displays the cisco-csr1000v-‘deployment number’

b) **Instance Name**: The name of the CSR 1000v instance in text format. You must follow the GCP naming pattern for successful deployment. The name of the instance must be a combination of regex '(?:[a-z](?:[-a-z0-9]{0,61}[a-z0-9])?)'">)

c) **Username**: Specify the username that is used to access the CSR 1000v instance.

d) **Instance SSH Key**: Specify the public key to be used for SSHing into the instance. To know how to create an ssh-key, see SSH-Key.

e) **Zone**: Select the zone where the CSR 1000v is deployed from the drop-down list.

f) **Machine Type**: Select the size of the CSR 1000v that you want to deploy. For more information on CSR 1000v sizes, see MachineTypes.

Bootdisk

g) **Bootdisk type**: By default, the SSD Persistent disk is selected. Cisco recommends that you use the default Boot disk type.

h) **Boot disk size in GB**: The default value is 10 GB. Cisco recommends that you use the default Boot disk size.

Networking

i) **Network (VPC)**: Select the network in the region where you want to deploy the CSR 1000v instance. You must create the Network (VPC) before you create the CSR 1000v instance. Ensure that at least one subnet is associated to that Network (VPC). For more information about VPC networks, see Virtual Private Cloud Network Overview and Using VPC Networks.

j) **Subnetwork**: Select the subnet that is associated with the selected Network (VPC). This subnet acts as the first Network Interface (nic0) of the CSR instance.

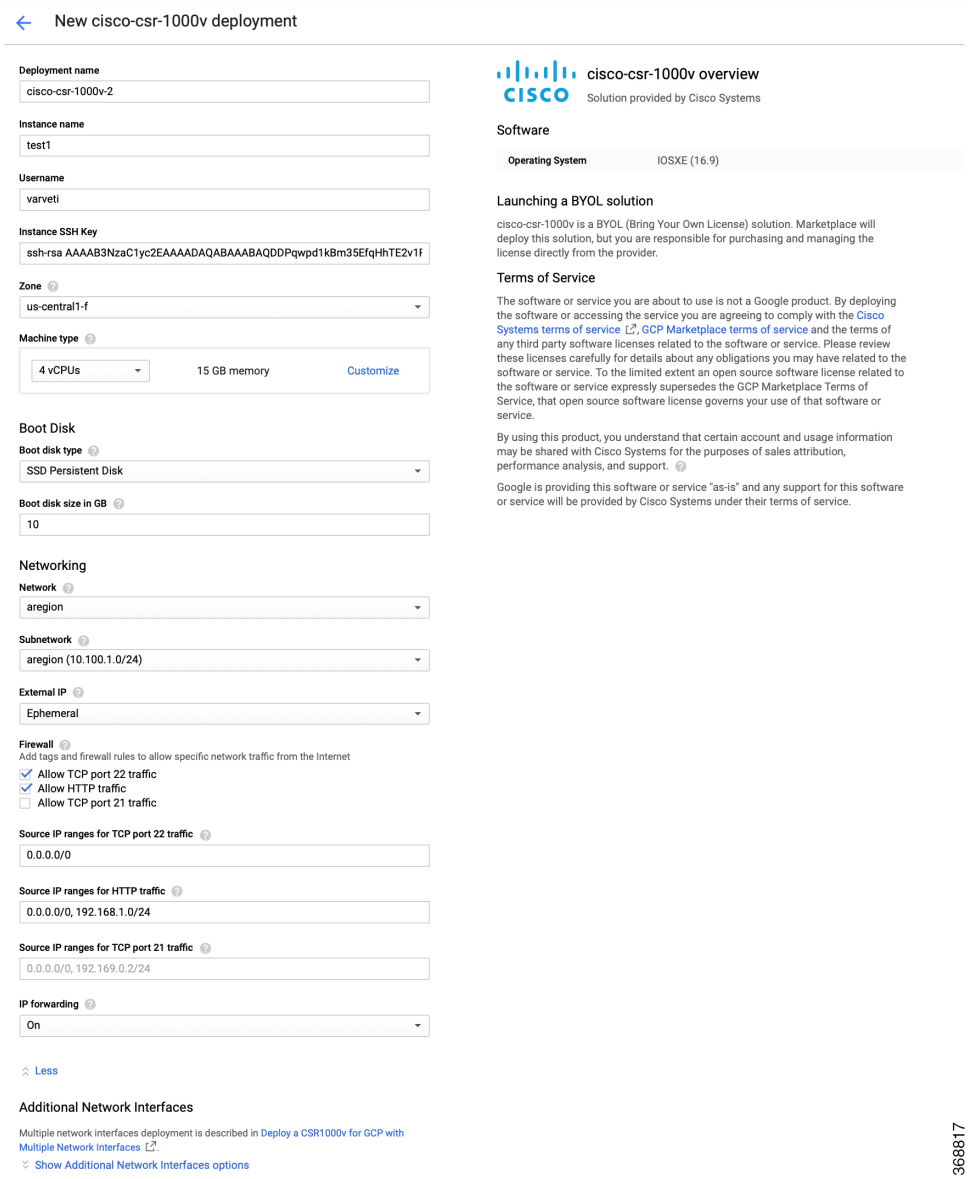
k) **ExternalIP**: The public IP address that you must use to SSH into the CSR 1000v instance. This can be static, Ephemeral (Dynamic) and None. For more information about IP addresses, see IP Addresses.

l) **Firewall**: The firewall wall rule associated to the VPC Network.With the current Solution Template, you can use TCP ports 21, 22, 80. You can also create additional Firewall rules. For more information on firewall rules, see Firewalls in VPC Networking and Firewalls.

Note You can also specify source ranges for firewalls rules.

m) **IP Forwarding**: The default value to allow traffic between interfaces on the CSR 1000v instance. By default, the value for IP Forwarding is ON.

Figure 2: New CSR 1000v Deployment Screen



n) **Additional Network Interfaces**: Configure this field if you want to configure additional interfaces. By default, the value of this field is 0. To add additional interfaces, specify additional interfaces that are needed for the CSR 1000v instance. Select the additional network interfaces based on the machine type. For more information on deployment of instance with multiple interfaces in GCP, see Creating Instances With Multiple Network Interfaces.

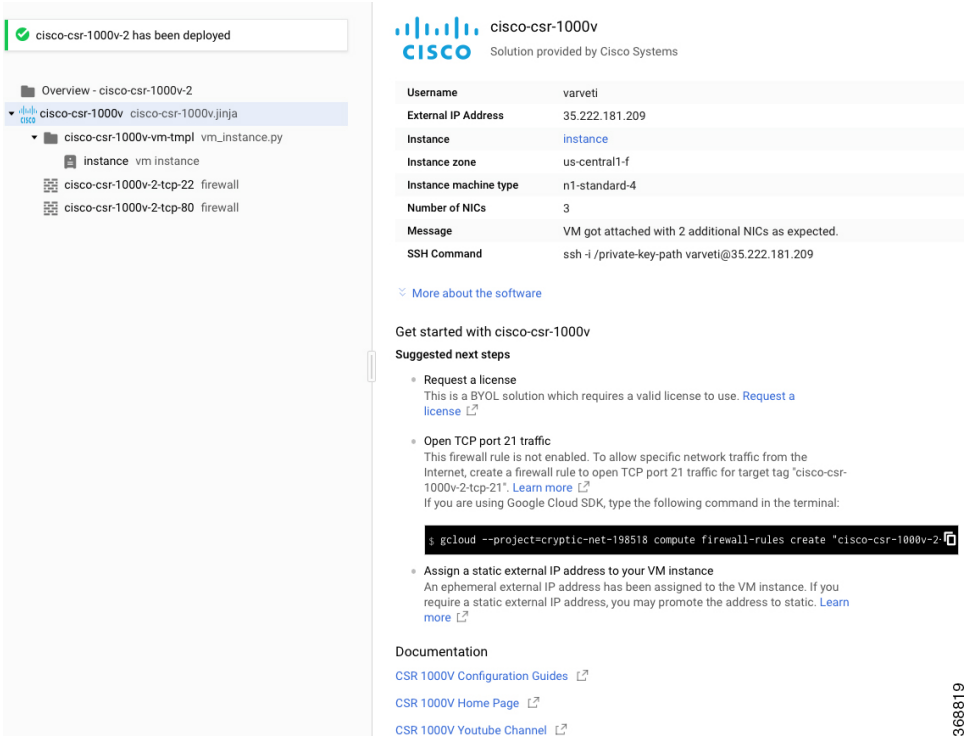
Figure 3: Additional Network Interfaces

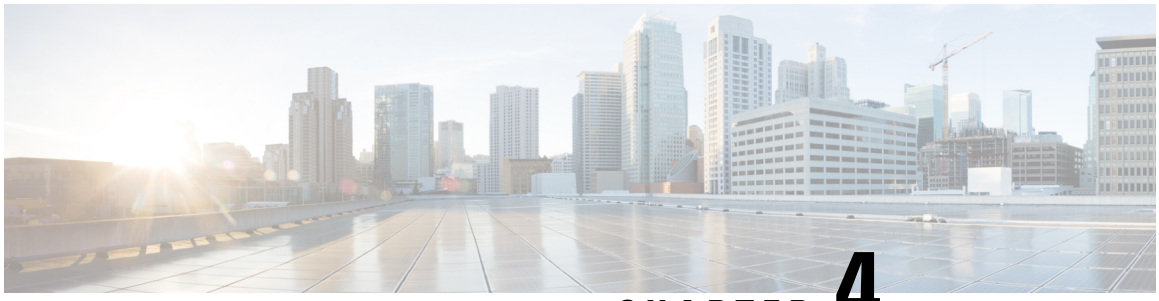
Note For the deployment to be successful, even if you do not require all the additional interfaces, you must select the Additional Network Interfaces option. This is a known issue where Google brings up to 8 interfaces, and you must fill in all the eight interfaces.

For example, in the following image, even though two additional NICs were selected, note that the 7 additional interfaces are configured with the networks and subnets present in region where the CSR 1000v instance is deployed.

After successful deployment, the system displays a message that the CSR instance has been deployed.

Figure 4: Verify successful deployment





CHAPTER 4

Deploying a Cisco CSR 1000v VM Using Custom Data

When you deploy a Cisco CSR 1000v Virtual Machine instance on Google Cloud Platform, you can optionally choose to use the **Startup Script** section on the VM creation console to provide custom data. You can also use the CLI to access the custom data to achieve various automation goals. The custom data in GCP allows you to run Cisco IOS XE configuration commands, install Python packages in guestshell on Day0, run scripts in guestshell on Day0, and provide licensing information to boot the CSR 1000v instance with a desired technology package.

Releases Supported

You can deploy a Cisco CSR 1000v VM using a custom data only on Cisco IOS XE Gibraltar 16.12.1 or later releases.

- Editing the Custom Data, on page 21
- Accessing the Custom Data, on page 25
- Verifying the Custom Data Configuration, on page 26

Editing the Custom Data

To edit the custom data, configure the following properties:

- IOS configuration
- Scripts
- Script credentials
- Python package
- Licensing

You can place the properties in a file in any order. The following property descriptions specify dependencies between the properties, if any. See the example bootstrap files at: https://github.com/csr1000v/customdata-examples.

After defining the custom data properties, you can access the startup script or the custom data file using the CLI as described in the *Accessing the Custom Data* section.

Configuring the IOS Configuration Property

If you want to bootstrap the IOS configuration on Day0, configure the IOS Configuration property. See the following IOS configuration example:

```
Section: IOS configuration
hostname CSR1
interface  GigabitEthernet1
description “static IP address config”
ip address 10.0.0.1 255.255.255.0
interface GigabitEthernet2
description “DHCP based IP address config”
ip address dhcp
```

After the first line that reads `Section: IOS configuration`, you can enter a list of Cisco IOS XE configuration commands that you want to execute, on the Cisco CSR 1000v router.

When you run this command, the preceding IOS configuration is applied to the CSR 1000v router running on GCP, on Day0.

Configuring the Scripts Property

Scripts property helps you automate the deployment of your CSR1000v instance. If you want to run a Python or a Bash script on Day0 under the guestshell context, provide the public URL and arguments of the python or the bash script in Scripts property.

A script must include a piece of code that includes the shebang (!) character in the first line of the script. This line tells Cisco IOS-XE which script interpreter (Python or Bash) you must use to parse the script code. For example, the first line of a Python script can contain `#!/usr/bin/env python`, while the first line of a Bash script can contain `#!/bin/bash`. This line allows the Python or the Bash script to run as executable code in a Linux environment.

When you execute the script, the script runs in the guestshell container of the Cisco CSR 1000v instance. To access the guestshell container, use the **guestshell** EXEC mode command. For more information on guestshell command, see the Programmability Configuration Guide.

To configure the Scripts property, use the following format:

```
Section: scripts
public_url <arg1> <arg2>
```

In this script, the first line of the property should read `Section: Scripts`.

In the second line of the property, enter the URL of the script and the script's arguments. The script can be either a Python or a Bash script. The script is run in guestshell in the first boot when you upload the custom data file, when you create the CSR1000v instance.

To view more examples of the scripts, see "scripts" at: https://github.com/csr1000v/customdata-examples. Also, refer to the following examples:

Example 1

```
Section: Script
https://raw.githubusercontent.com/csr1000v/customdata-
examples/master/scripts/smartLicensingConfigurator.py --idtoken "<token_string>" --throughput
 <throughput_value>
```

The two lines in the scripts property retrieve the `smartLicensingConfigurator.py` script from the `customdata-examples` repository at the specified URL. The script runs in the guestshell container of the Cisco CSR 1000v with the arguments `idtoken` and `throughput`.

Example 2

```
Section: Scripts
ftp://10.11.0.4/dir1/dir2/script.py -a arg1 -s arg2
```

These two lines in the Scripts property retrieve the `script.py` script from the FTP server with the IP address 10.11.0.4, and runs the script with the `./script.py -a arg1 -s arg2` Bash command in the guestshell container of the Cisco CSR 1000v instance using arguments arg1 and arg2.

Note If a script in the Scripts property requires a Python package that is not included in the standard CentOS Linux release (the CentOS Linux release that is currently used by the guestshell is CentOS Linux release 7.1.1503), you must include information about the Python package in the Python package property. For more information, see: Configuring the Python package Property, on page 24.

Before you access the custom data and run the Bash or the Python script, Cisco recommends that you test the URL that you intend to use, using the Scripts property. You can test `ftp://10.11.0.4/dir1/dir2/script.py -a arg1 -s arg2` by first running the curl software tool to download the script file. In the guestshell, enter the curl command as shown in the following example:

```
curl -m 30 --retry 5 --user username:password
ftp://10.11.0.4/dir1/dir2/script_needs_credentials.py.
```

If the curl command is successful, a copy of the Python script is downloaded, which verifies whether the URL is correct.

Configuring the Script Credentials Property

If you have specified an FTP server in the Script property, and the server requires a username and password credentials, specify the credentials using the Script credentials property.

Note If you can access the FTP server anonymously, you need not use the Script credentials property.

Configure the Scripts property with a URL and parameters that match those in the Script credentials property. To configure the Script credentials property, use the following format:

```
Section: Script credentials
public_url <username> <password>
```

Example

```
Section: Script credentials

ftp://10.11.0.4/dir1/dir2/script1.py userfoo foospass
```

The second line in the Script credentials property specifies the values of the username (`userfoo`) and password (`foospass`) credentials for the python script `script1.py`.

Include the name of the FTP server that is also in the Scripts property. An example line in the Scripts property is: `ftp://10.11.0.4/dir1/dir2/script1.py -a arg1 -s arg2`. See example 2 in Configuring the Scripts Property, on page 22.

Configuring the Python package Property

If a Python package is required by a script in the Scripts property and it is not part of the standard CentOS Linux release 7.1.1503, you must include information about the package in the Python package property. By including the Python package property in the bootstrap file, you ensure that the Cisco CSR 1000v downloads and installs the required Python package before the custom data file that you specified in the Scripts property.

Configure Python Package Property

To configure the Python package property, use the following format:

```
Section: Python package
package_name [ version ] [ sudo ] { [ pip_arg1 [ ..[ pip_arg9] ] ] }
```

The arguments: *version*, **sudo**, and *pip_arg1* to *pip_arg9* are optional. You must put the arguments to the pip command between "{" and "}" braces.

If you specify the *version* argument, a specific version number is downloaded.

If you specify the *sudo* argument, the package is downloaded as a sudo user.

Configuration Examples

Example 1

```
Section: Python package

ncclient 0.5.2
```

In this example, the second line of the Python package property specifies that the *package_name* is "ncclient" and the *version* is "0.5.2". When the bootstrap file is uploaded, version 0.5.2 of the ncclient package is installed in the guestshell container of the Cisco CSR 1000v.

Example 2

```
Section: Python package

csr_gcp_ha 3.0.0 sudo {--user}
```

In this example, the second line of the Python package property specifies that the *package_name* is "csr_gcp_ha" and the *version* is "3.0.0". When the bootstrap file is uploaded, version 3.0.0 of the csr_gcp_ha package is installed in the guestshell container of the Cisco CSR 1000v. The following command is executed as a sudo user: `pip install csr_gcp_ha=3.0.0 --user`.

Configuring the License property

Configure the license property to specify the license technology level for the Cisco CSR 1000v instance.

- Enter the first line of the property in the format: `Section: License`.
- Enter the second line of the property, which specifies the tech level of the license, using the following format: **TechPackage:***tech_level* .

Note Ensure there are no spaces between "TechPackage:" and the *tech_level*. The possible *tech_level* values include: ax, security, appx, or ipbase.

Ensure that *tech_level* is in lowercase.

Configuration Example

```
Section: License

TechPackage:security
```

Accessing the Custom Data

To run the custom data as a file by using the CLI, execute the following script:

Accessing the custom data file using the CLI

To run the custom data as a file by using the CLI, execute the following script:

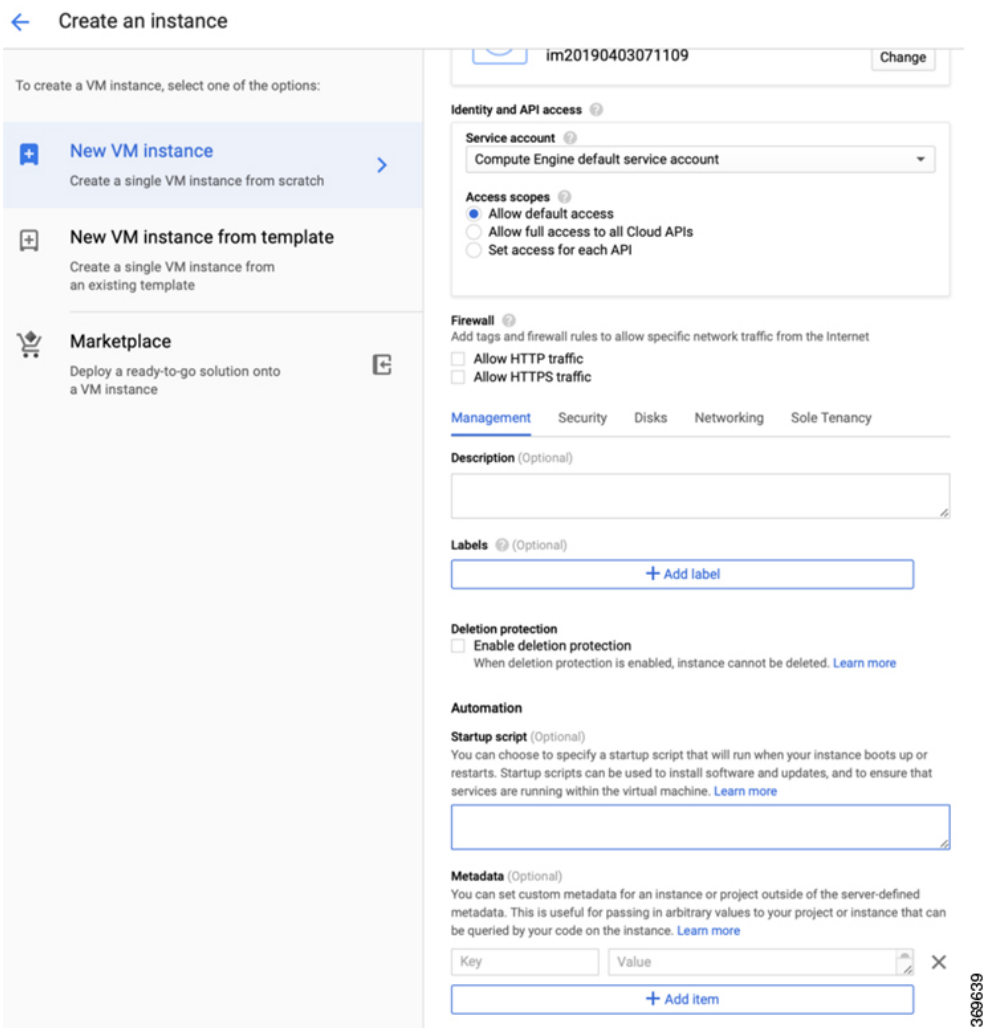
```
gcloud compute instances create <vm_name> --metadata-from-file=startup-script=Customdata.txt
 --image  <image_name>
```

When you execute this command, a Cisco CSR 1000v VM is created. The router is configured using the commands in the file: "Customdata.txt".

Accessing the custom data from the console

To access the custom data from the console, log in to the GCP console. Click **Compute Engine**, and select **Create an Instance**.

On the New VM instance screen, click **Management** > **Startup Script**.



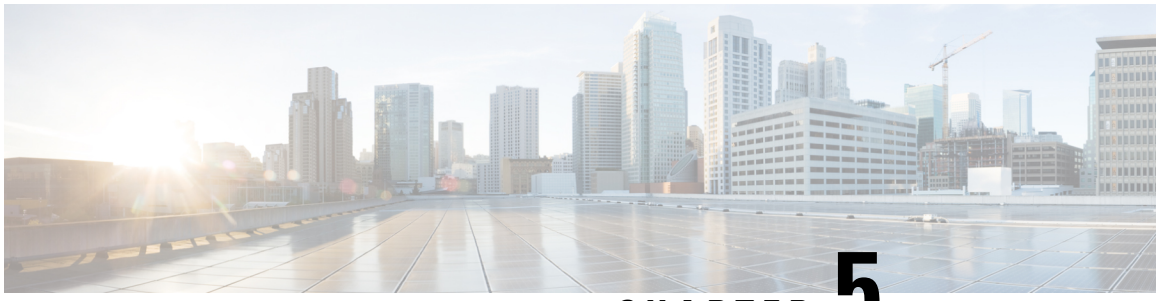
The startup script specified in this field runs every time you bootup or restart your CSR 1000v instance.

Verifying the Custom Data Configuration

After you run the custom data script, the VM is created and the configuration commands are executed. To verify the same, use the following commands and scripts:

- **show version**: To help determine if the license property worked, in Cisco IOS XE CLI on the CSR 1000v, enter the **show version** command. For example, the output displays a reference to the security license.
- To see if errors occurred after running commands in the scripts property, look at the `customdata.log` file in the `/bootflash/<cloud>/` directory. The *scriptname*.log file stores any output that is sent to STDOUT by the script.
- To verify whether the Python property worked, enter the `pip freeze | grep <package-name>` command from the Guestshell to view the currently installed Python packages. Here, *package-name* refers to the package that you are specifically searching for.

- To verify the Cisco IOS XE commands in the IOS Configuration property, run the **show running-configuration** command.



CHAPTER 5

Usage Guidelines for Custom Routes

- Introduction to Custom Routes, on page 29
- Custom Routes in the Same VPC Network, on page 29
- Routing Between VPC Networks or On-Premises Networks, on page 29

Introduction to Custom Routes

When a Cisco CSR 1000v is deployed in a VPC network, a route is created for each subnet to which the Cisco CSR 1000v is connected. For example, if you deploy a Cisco CSR 1000v in GCP with two subnets, then each subnet has an associated route.

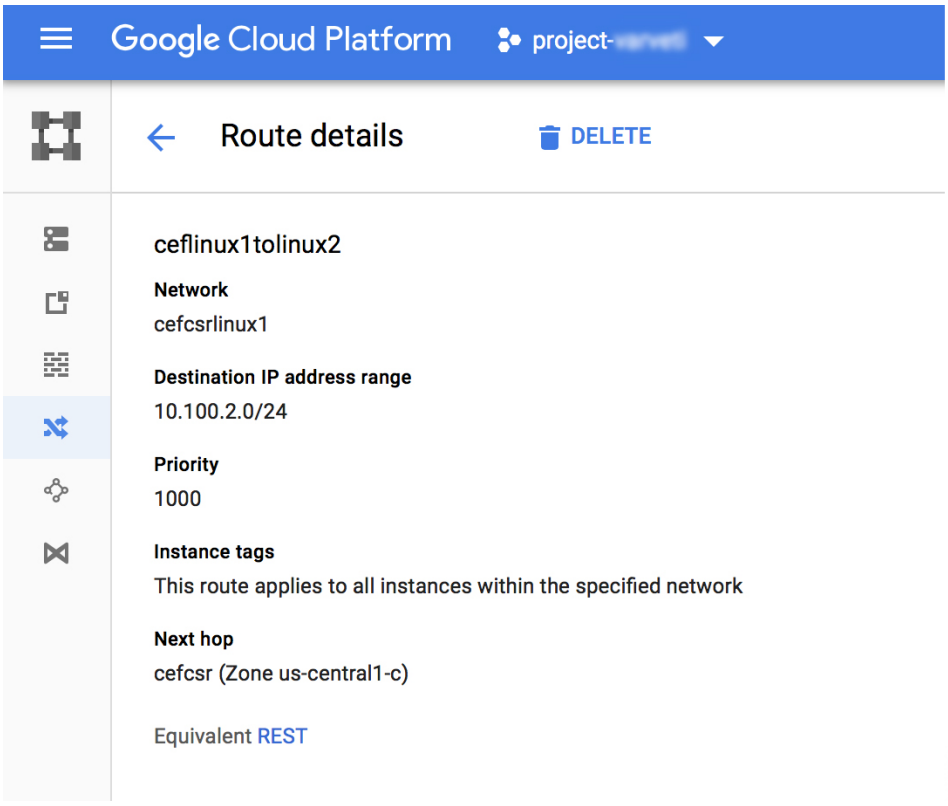
Custom Routes in the Same VPC Network

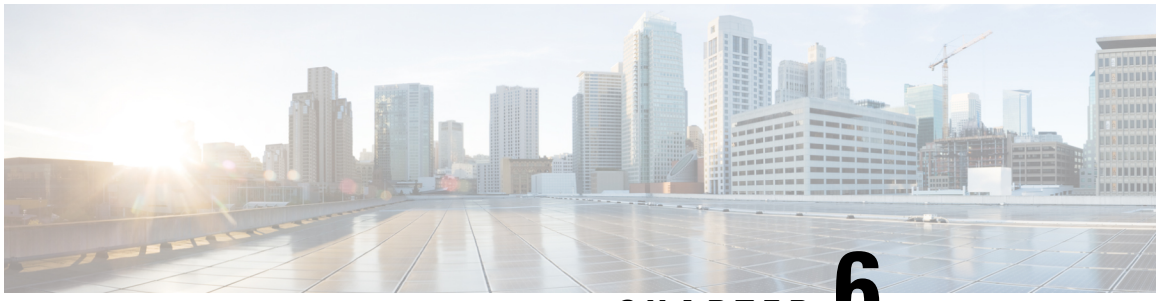
By default, the GCP network infrastructure provides a basic routing service which interconnects all the subnets within a VPC network. By default, packets are blocked between subnets, unless firewall rules are changed to allow them to pass.

Routing Between VPC Networks or On-Premises Networks

To connect two VPC networks or to connect a VPC network to an on-premises network, you must create a route to specify the Cisco CSR 1000v as the next hop router to each remote network. To force traffic through the Cisco CSR 1000v, add a route (default route or specific destination route) that points to the Cisco CSR 1000v.

For example, the following route was added with a destination IP address pointing to the Cisco CSR 1000v. The "Next hop" refers to the Cisco CSR 1000v VM instance "cefcsr".


Google Cloud Platform
project-
Route details
DELETE
ceflinux1tolinux2
Network
cefcsrlinux1
Destination IP address range
10.100.2.0/24
Priority
1000
Instance tags
This route applies to all instances within the specified network
Next hop
cefcsr (Zone us-central1-c)
Equivalent REST
367429



CHAPTER 6

Cisco CSR 1000v Deployment Guidelines and Best Practices

- Differences Between CSR 1000v Deployments , on page 31
- Best Practices and Caveats, on page 32
- Other Related Resources, on page 32

Differences Between CSR 1000v Deployments

The differences between deploying Cisco CSR 1000v on Microsoft Azure, Amazon Web Services (AWS), and Google Cloud Platform (GCP) are shown in the following table:

Table 4: Differences Between Deployments of Cisco CSR 1000v on Microsoft Azure, Amazon Web Services, and Google Cloud Platform

Function	Microsoft Azure	Amazon Web Services	Google Cloud Platform
Number of Interfaces	1, 2, 4, or 8.	3 or more.	1, 2, 4, or 8.
Multiple IP addresses	Multiple IP addresses per vNIC.	Multiple IP addresses per vNIC.	Multiple IP addresses per vNIC.
GRE tunnel	Not Supported.	Supported.	Not Supported.
Routing Redundancy	Supported through two CSR instances.	Supported through two CSR instances.	Not Supported.
Attachment or Detachment of an interface on the running Cisco CSR 1000v.	Not Supported	Supported	Not supported
Overlapping IP subnets in different VPC networks.	Supported.	Supported.	Supported.

Best Practices and Caveats

1. When a Cisco CSR 1000v VM is deleted, not all the resources for the VM are deleted. When you create a new Cisco CSR 1000v with the same name as before, the previous resources may be reused. If you do not want to reuse these resources, manually remove these individual resources or create a new Cisco CSR 1000v with a different name.

Other Related Resources

The Cisco CSR 1000v on Microsoft Azure supports DMVPN, AWS, and GCP. For further information on DMVPN, see the Cisco Dynamic Multipoint VPN Configuration Guide.