

Lab Guide for Introduce Compute Services from GCP

CONTENTS

Day-6 Assignments

Contents

Lab Guide for Introduce Compute Services from GCP	1
CONTENTS	1
Assignment 1: Create a VPC network with custom subnets.....	2
Assignment 2: Adding firewall rule and instance within the secure network.....	8
Assignment 3: Networking 101	15
Assignment 4: Creating a network peering connection between two VPCs.....	15

Context

This document contains assignments to be completed as part of the hands on session for the course

Guidelines

- The lab guide has been designed to give hands on experience to map the concepts learnt in the theory session with real life business oriented case studies/assignments.

Day-6 Assignments

Assignment 1: Create a VPC network with custom subnets

Highlights:

Virtual Private Cloud is a global resource.

Subnets are limited to regions

Routes in VPC networks are applicable within the project.

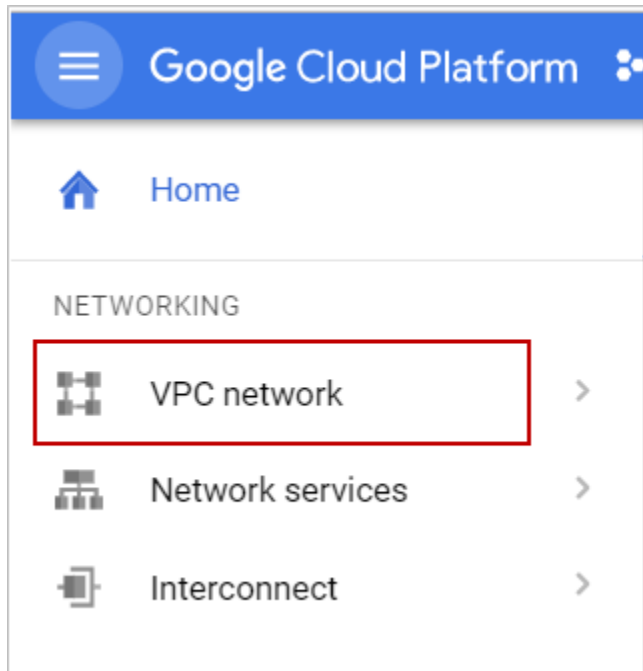
Demo steps:

Panchama wants to configure network and subnet to create a private cloud topology in GCP in which instances under VPC can also access GCP products and services.

VPC creation using Google cloud platform console

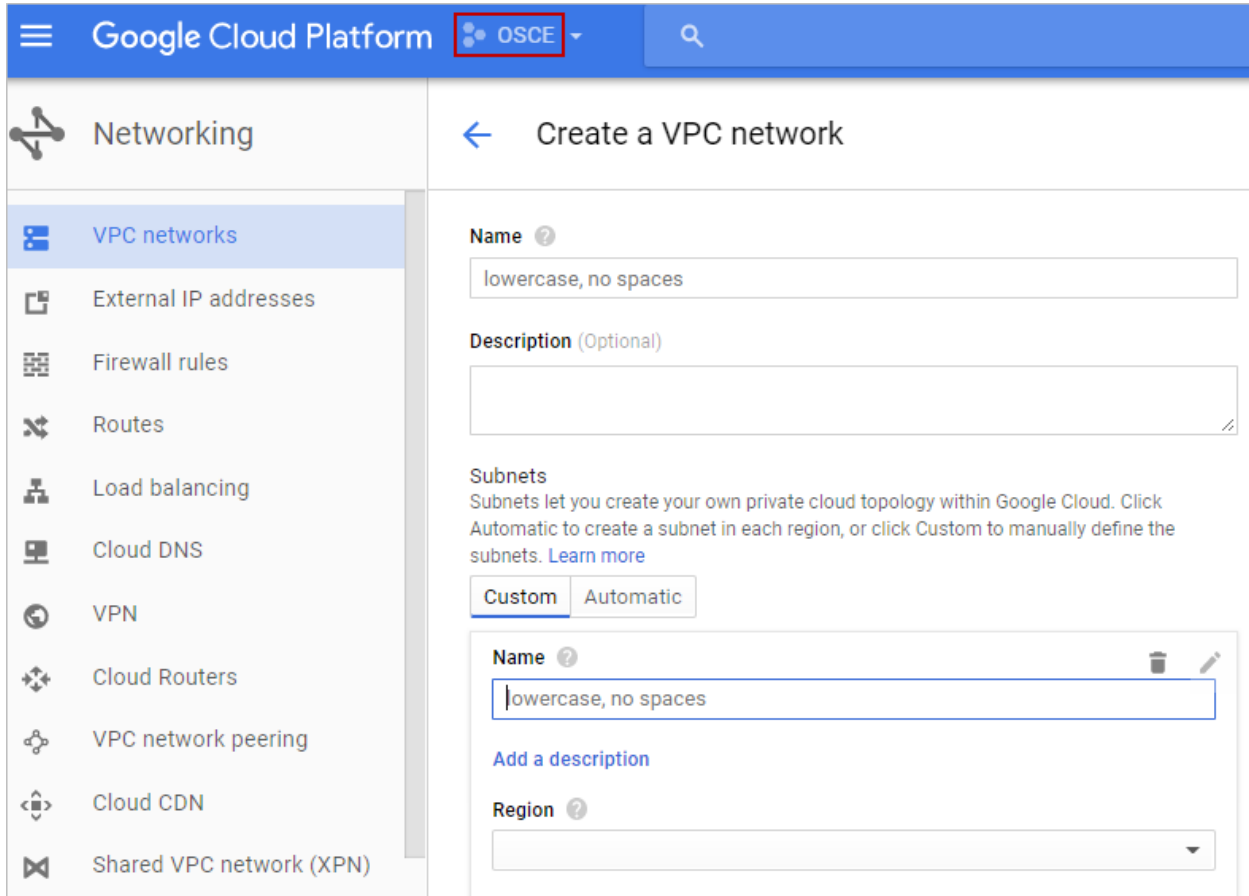
Step 1:

Navigate to VPC network under Networking in google cloud platform console as shown below:



Step 2:

Select **VPC networks** of project **OSCE** as shown below.



Google Cloud Platform OSCE

Networking

- VPC networks
- External IP addresses
- Firewall rules
- Routes
- Load balancing
- Cloud DNS
- VPN
- Cloud Routers
- VPC network peering
- Cloud CDN
- Shared VPC network (XPN)

Create a VPC network

Name ?
lowercase, no spaces

Description (Optional)

Subnets
Subnets let you create your own private cloud topology within Google Cloud. Click Automatic to create a subnet in each region, or click Custom to manually define the subnets. [Learn more](#)

Custom Automatic

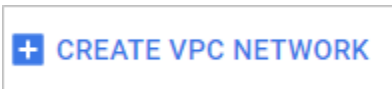
Name ?
lowercase, no spaces

Add a description

Region ?

Step 3:

Click on **Create VPC network** in the VPC networks dashboard.



Step 4: Describe network

Give a unique name to network as shown below.

Name ?

Description (Optional)

Step 5:

Define subnet by providing the following values as shown below.

Subnets

Subnets let you create your own private cloud topology within Google Cloud. Click Automatic to create a subnet in each region, or click Custom to manually define the subnets. [Learn more](#)

Subnet creation mode

Custom
Automatic

Name ?

panchama-nw-sub

Add a description

Region ?

us-central1

IP address range ?

10.1.0.0/16

Create secondary IP range

Private Google access ?

Enabled

Name: Provide a unique name to subnet.

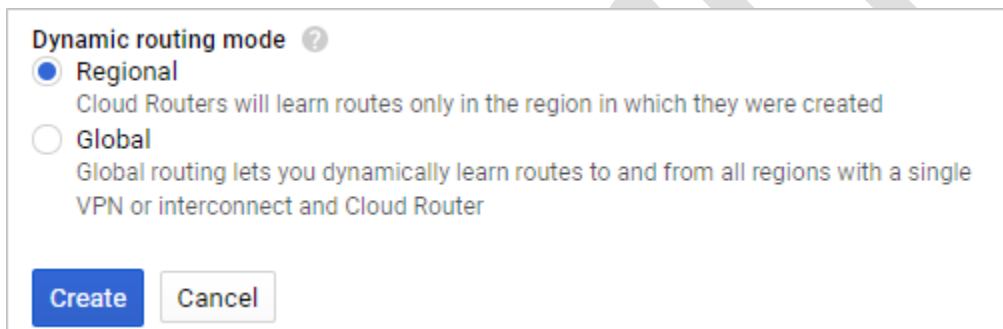
Region: Panchama has decided to deploy their application in North America as their region. Hence selected the nearest proximity region of "us-central1".

IP address: Choose an IP address range in Classless Inter-Domain Routing(CIDR) notation.

Private Google Access: Enabling accessibility of instance for Google services without setting external IP address.

Step 6:

Select **Dynamic Routing** mode as Regional and click create as shown below.



Dynamic routing mode ?

☒ **Regional**
Cloud Routers will learn routes only in the region in which they were created

☐ **Global**
Global routing lets you dynamically learn routes to and from all regions with a single VPN or interconnect and Cloud Router

Create **Cancel**

You can **verify the custom network and subnet** by navigating to VPC networks page.

Name	Region	Subnets	Mode	IP addresses ranges	Gateways	Firewall Rules	Global dynamic routing
panchama-vpc		1	Custom			0	Off
	us-central1	panchama-nw-sub		10.1.0.0/16	10.1.0.1		

At this point, the network has routes to the internet and to any instances. To enable the connectivity for the resources in VPCs, appropriate firewall rules to be added.

In next section, you will learn how to add firewall to secure your VPC configuration.

Assignment 2: Adding firewall rule and instance within the secure network

Highlights:

Firewall rules are added to dedicated network in the project

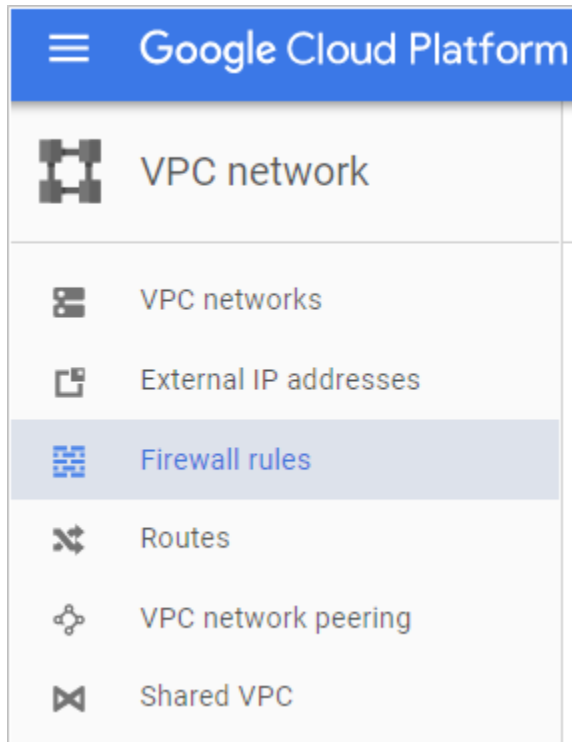
Default rules are created for auto-type networks

Demo steps:

Firewalls let you to determine the traffic that can be allowed or denied to or from instances based on IP addresses, protocols and ports. In our demonstration, will add SSH protocol to enable connectivity for the instance inside VPC network.

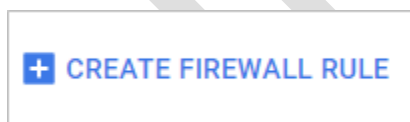
Step 1:

Navigate to the VPC networks and select "firewall rules" as shown below.



Step 2:

Click on **create firewall rule** as shown



Step 3:

Provide unique name to Firewall and select Panchama's Network as mentioned below.

Firewall rules control incoming or outgoing traffic to an instance. By default, incoming traffic from outside your network is blocked. [Learn more](#)

Name ?

allow-ssh

Description (Optional)

Network ?

panchama-vpc

Priority ?

Priority can be 0 - 65535 [Check priority of other firewall rules](#)

1000

Direction of traffic ?

☒ Ingress

☐ Egress

Action on match ?

☒ Allow

☐ Deny

Targets ?
 All instances in the network

Source filter ?
 IP ranges

Source IP ranges ?
 0.0.0.0/0

Second source filter ?
 None

Protocols and ports ?
☐ Allow all
☒ Specified protocols and ports
 tcp:22

Create Cancel

Upon creation, you can verify the protocol in firewall rules page.

Name	Targets	Source filters	Protocols / ports	Action	Priority	Network v
allow-ssh	Apply to all	IP ranges: 0.0.0.0/0	tcp:22	Allow	1000	panchama-vpc

To verify the connectivity, Panchama wants to deploy the resources inside VPC.

***Instance** is to be created in your desired project by selecting the custom network under "Management, disk, Networking, access and security"*

Step 4:

*Navigate to **Compute Engine** and create instance by specifying below details.*

- 1. Provide valid name and select the appropriate zone where your network is established*

Name ?


Zone ?

Machine type
Customize to select cores, memory and GPUs.

0.6 GB memory
[Customize](#)

Container ?
☐ Deploy a container image to this VM instance. [Learn more](#)

Boot disk ?



New 10 GB standard persistent disk
Image
Debian GNU/Linux 9 (stretch)

Change

Identity and API access ?


Service account ?

2. Choose the network, created in the previous steps.

Management Disks **Networking** SSH Keys



Network tags ? (Optional)

Network interfaces ?

panchama-vpc panchama-nw-sub (10.1.0.0/16) 

Step 6:

You can verify the instance from instance page as shown below.

<input type="checkbox"/>	Name ^	Zone	Recommendation	Internal IP	External IP	Connect
<input checked="" type="checkbox"/>	panchama-testserver1	us-central1-a		10.1.0.2	35.202.247.52	SSH  

You can connect using console "SSH" and verify the instance as shown below:

```
Secure | https://ssh.cloud.google.com/projects/osce-159707/zones/us-central1-a/instances/panchama-testserver1?authuser=0&hl...
kashyap_kiru@panchama-testserver1:~$ hostname
panchama-testserver1
kashyap_kiru@panchama-testserver1:~$
```

Assignment 3: Networking 101

Please refer to the instructions in the below link and try out.

<https://codelabs.developers.google.com/codelabs/cloud-networking-101/index.html?index=..%2F..index#0>

Assignment 4: Creating a network peering connection between two VPCs

Objective: In this demonstration, you will learn to create VPC Network Peering connection between two custom mode VPCs.

Create a custom mode VPC with one subnet with the below parameters.

- *Name of the network: peer-vpc-1*
- *Name of the subnet: public-subnet-1*
- *CIDR: 10.0.0.0/24*

Create another custom mode VPC with one subnet with the below parameters.

- *Name of the network: peer-vpc-2*
- *Name of the subnet: public-subnet-2*
- *CIDR: 192.168.0.0/24*

Navigate to VPC Network Peering in the console and select "Create connection".

VPC Network

VPC Network Peering

Cloud VPC Network Peering lets you privately connect two VPC networks, which can reduce latency, cost, and increase security. To get started click "Create connection". [Learn more](#)

Create connection

Learn more

Click "continue".

Google Cloud Platform

OSCE

VPC network

VPC networks

External IP addresses

Firewall rules

Routes

VPC network peering

Shared VPC

Create peering connection

You will need the following info. [Learn more](#)

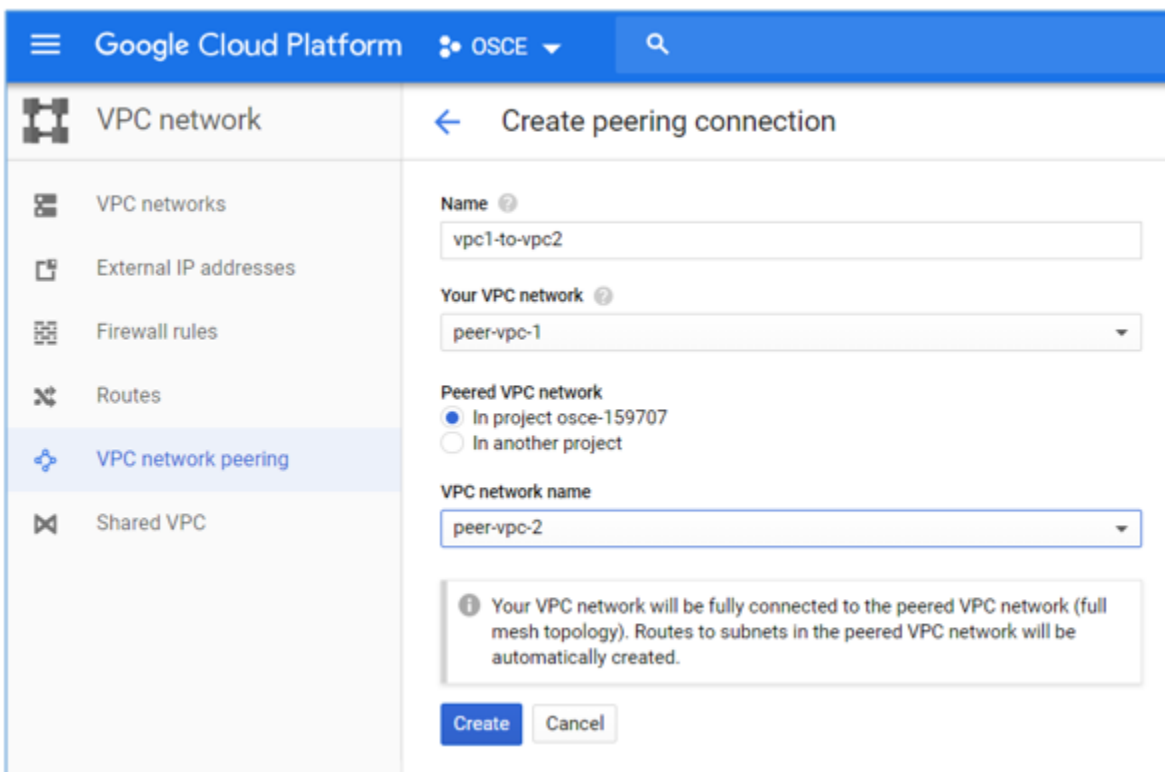
- The project ID (if you are connecting to a VPC network in another project)
- The name of the VPC network you want to peer with

Note: The subnet IP ranges in peered VPC networks cannot overlap.

Continue

Cancel

Create a connection from vpc1-to-vpc2.




The screenshot shows the Google Cloud Platform console interface. The top navigation bar includes the Google Cloud Platform logo, the project name 'OSCE', and a search icon. The left sidebar lists various network-related services: VPC networks, External IP addresses, Firewall rules, Routes, VPC network peering (which is highlighted), and Shared VPC. The main content area is titled 'Create peering connection'. It contains the following fields and options:

- Name:** A text input field containing 'vpc1-to-vpc2'.
- Your VPC network:** A dropdown menu showing 'peer-vpc-1'.
- Peered VPC network:** Two radio button options: 'In project osce-159707' (which is selected) and 'In another project'.
- VPC network name:** A dropdown menu showing 'peer-vpc-2'.

Below these fields is an informational message: 'Your VPC network will be fully connected to the peered VPC network (full mesh topology). Routes to subnets in the peered VPC network will be automatically created.' At the bottom of the form are two buttons: 'Create' and 'Cancel'.

Observer the status of the network peering connection.

VPC Network Peering				
<div> + CREATE PEERING CONNECTION REFRESH DELETE </div>				
<input type="checkbox"/> Name ^	Your VPC network	Peered VPC network	Peered project ID	Status
<input type="checkbox"/> vpc1-to-vpc2	peer-vpc-1	peer-vpc-2	osce-159707	<div>  Waiting for peer network to connect. </div>

Create the peering connection from vpc2-to-vpc1

Google Cloud Platform

OSCE

VPC network

VPC networks

External IP addresses

Firewall rules

Routes

VPC network peering

Shared VPC

Create peering connection

Name [?]

vpc2-to-vpc-1

Your VPC network [?]

peer-vpc-2

Peered VPC network

☒ In project osce-159707
 ☐ In another project

VPC network name



peer-vpc-1

Your VPC network will be fully connected to the peered VPC network (full mesh topology). Routes to subnets in the peered VPC network will be automatically created.

Create

Cancel

Now, the connection is complete and successful.

VPC Network Peering				
+ CREATE PEERING CONNECTION REFRESH DELETE				
<input type="checkbox"/> Name ^	Your VPC network	Peered VPC network	Peered project ID	Status
<input type="checkbox"/> vpc1-to-vpc2	peer-vpc-1	peer-vpc-2	osce-159707	 Connected. <div>⋮</div>
<input type="checkbox"/> vpc2-to-vpc-1	peer-vpc-2	peer-vpc-1	osce-159707	 Connected. <div>⋮</div>

Now, the services can be shared between the VPCs.

Note: If connection is removed from either side, peering will be disconnected

Summary

Learnt to establish VPC network peering connection between two VPCs to share the services between them.