HSBC

Infosys
Navigate your next

Lab Guide for Introduce Compute Services from GCP

CONTENTS

Day-6 Assignments

Contents

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.

Internal

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:

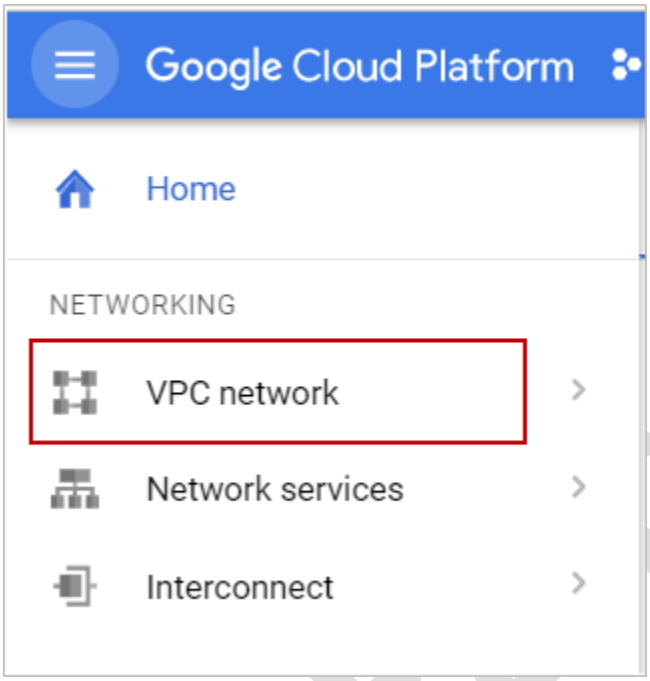
Panchama wants to configure network and subnet to create a private cloud topology in GCP in which instances under VPC can also access GCP products and services.

VPC creation using Google cloud platform console

Step 1:

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

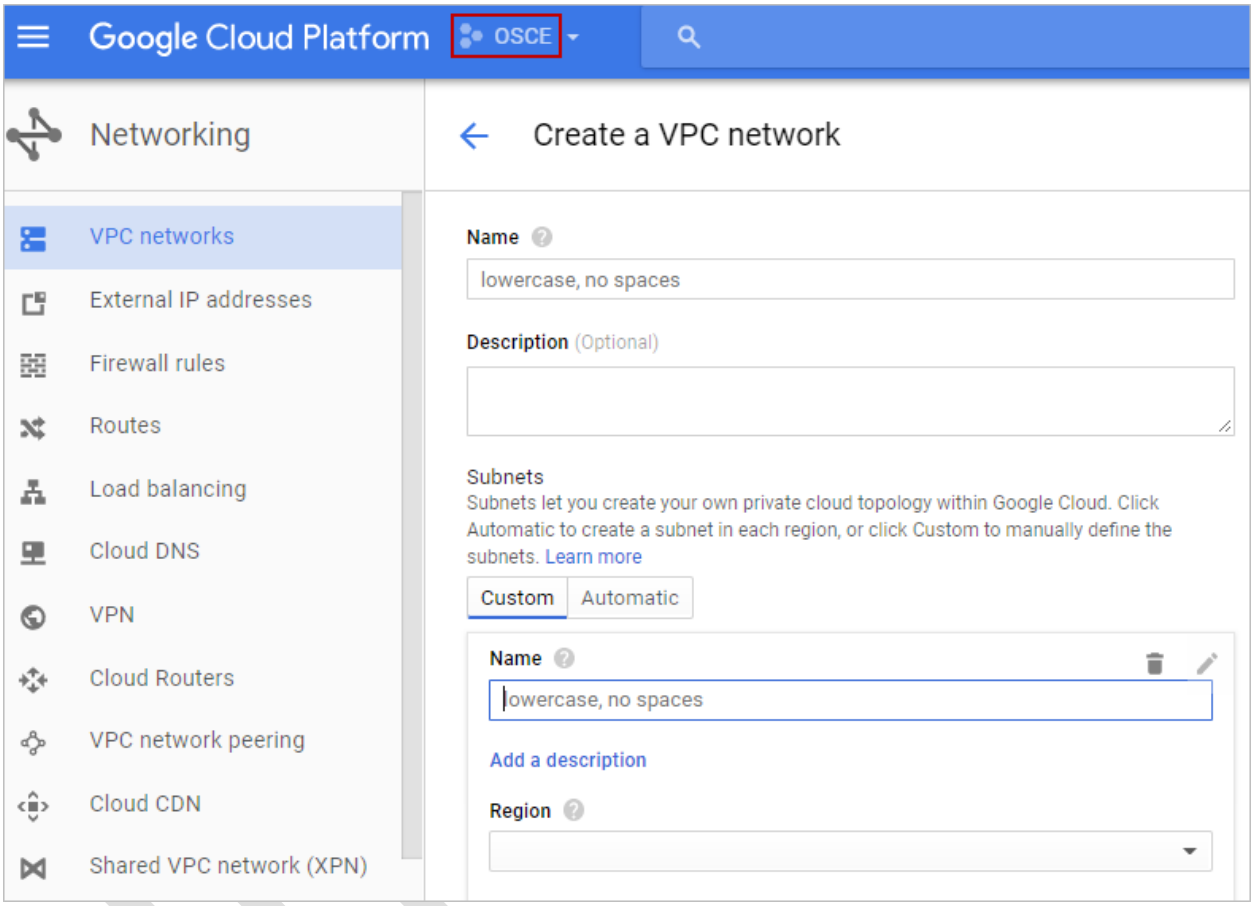
Internal



Step 2:

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

Internal



Step 3:

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

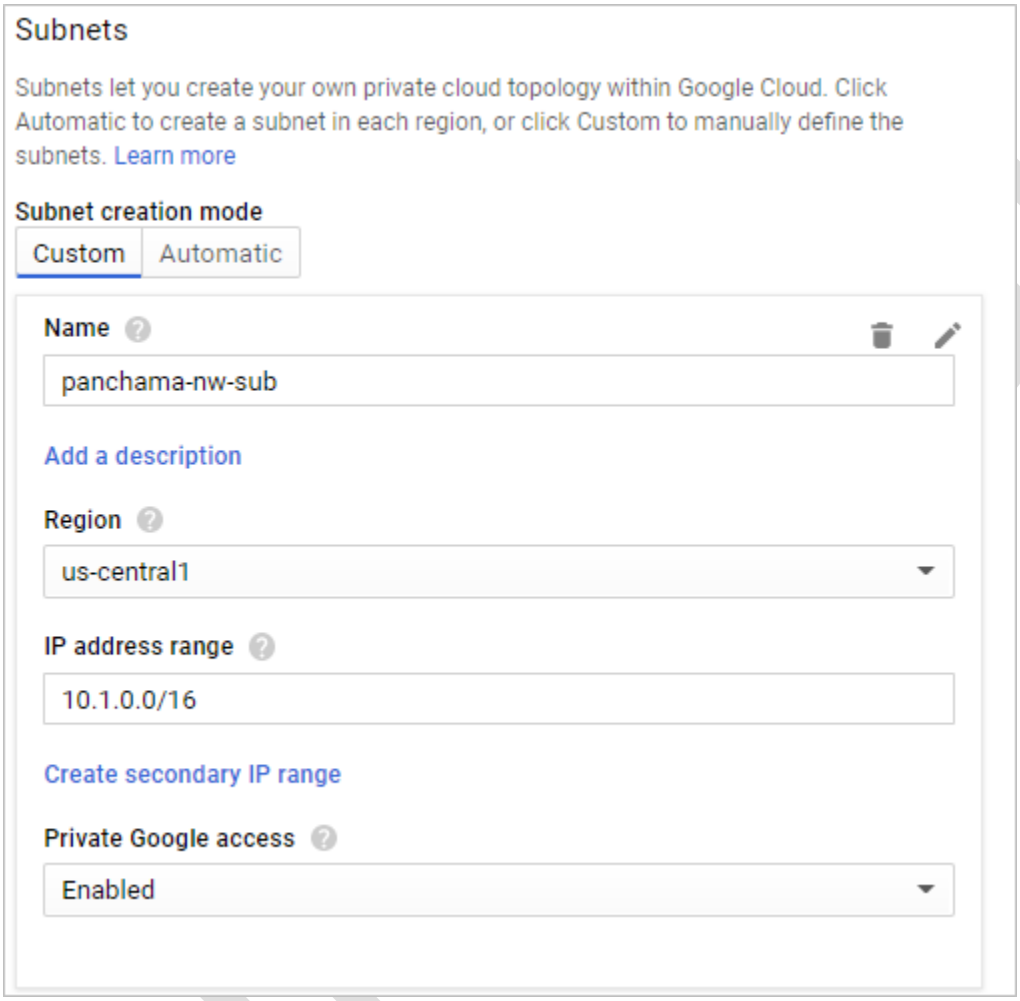
Step 4: Describe network

Give a unique name to network as shown below.

Step 5:

Define subnet by providing the following values as shown below.

Internal



Name: *Provide a unique name to subnet.*

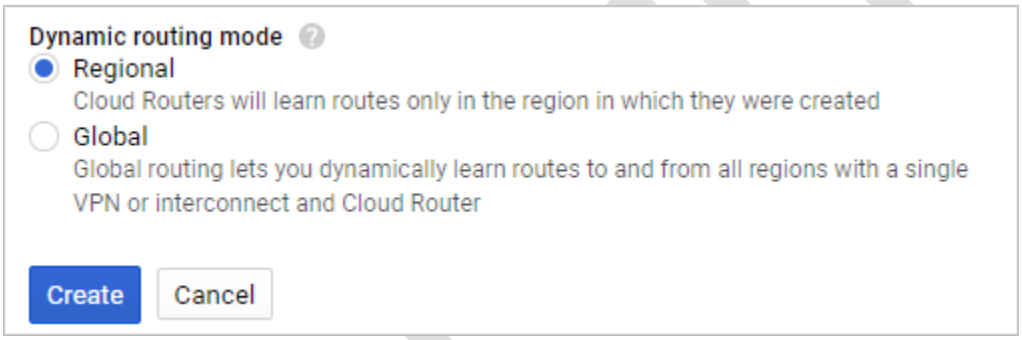
Region: *Panchama has decided to deploy their application in North America as their region. Hence selected the nearest proximity region of "us-central1".*

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.*



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

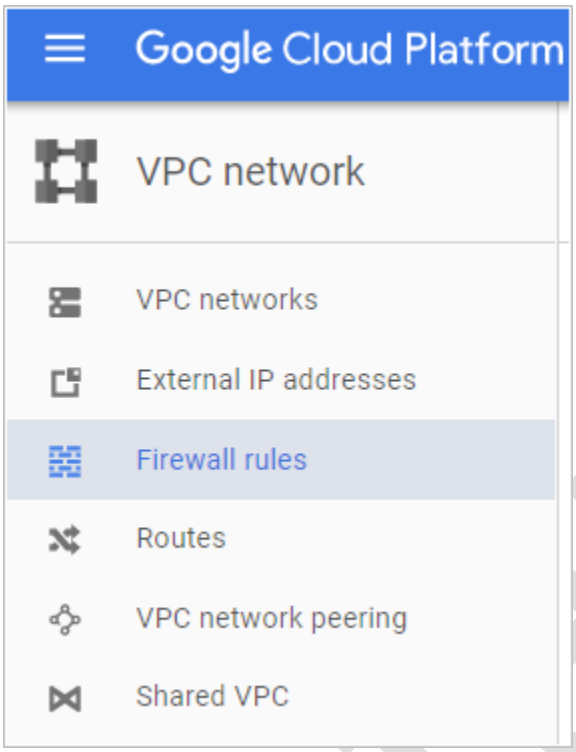
Demo steps:

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.

Internal



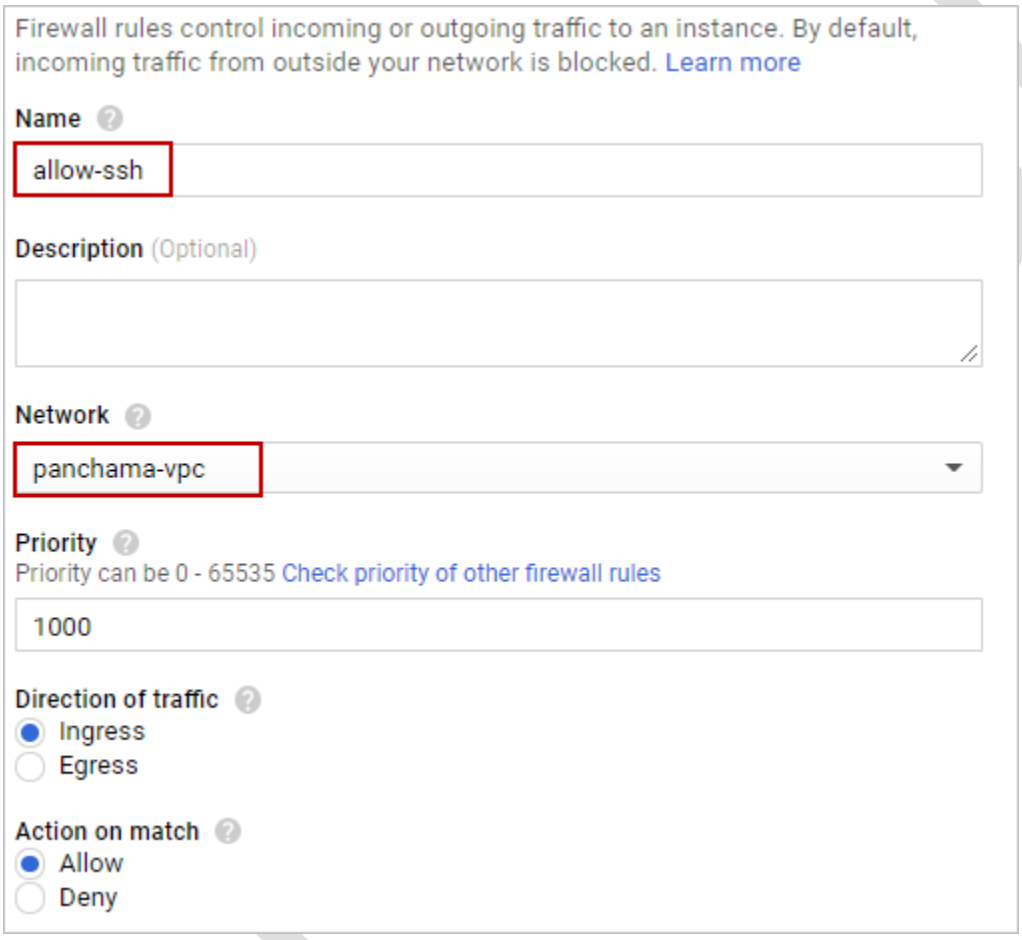
Step 2:

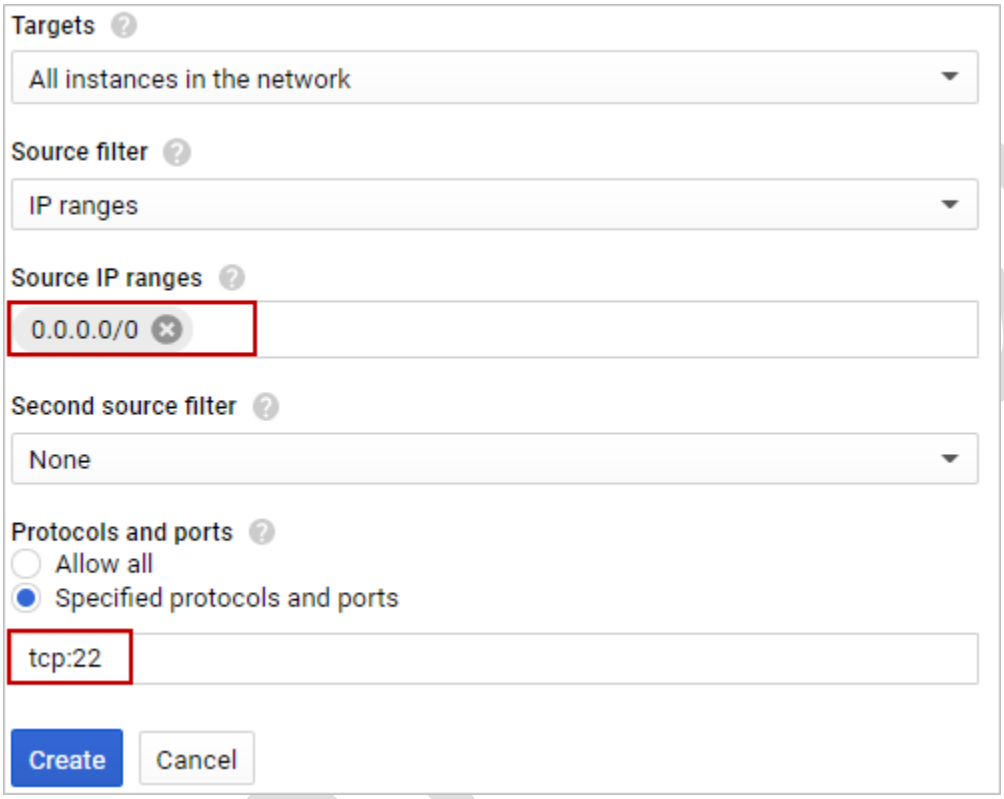
*Click on **create firewall rule** as shown*

Internal

Step 3:

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





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

Name	Targets	Source filters	Protocols / ports	Action	Priority	Network
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.

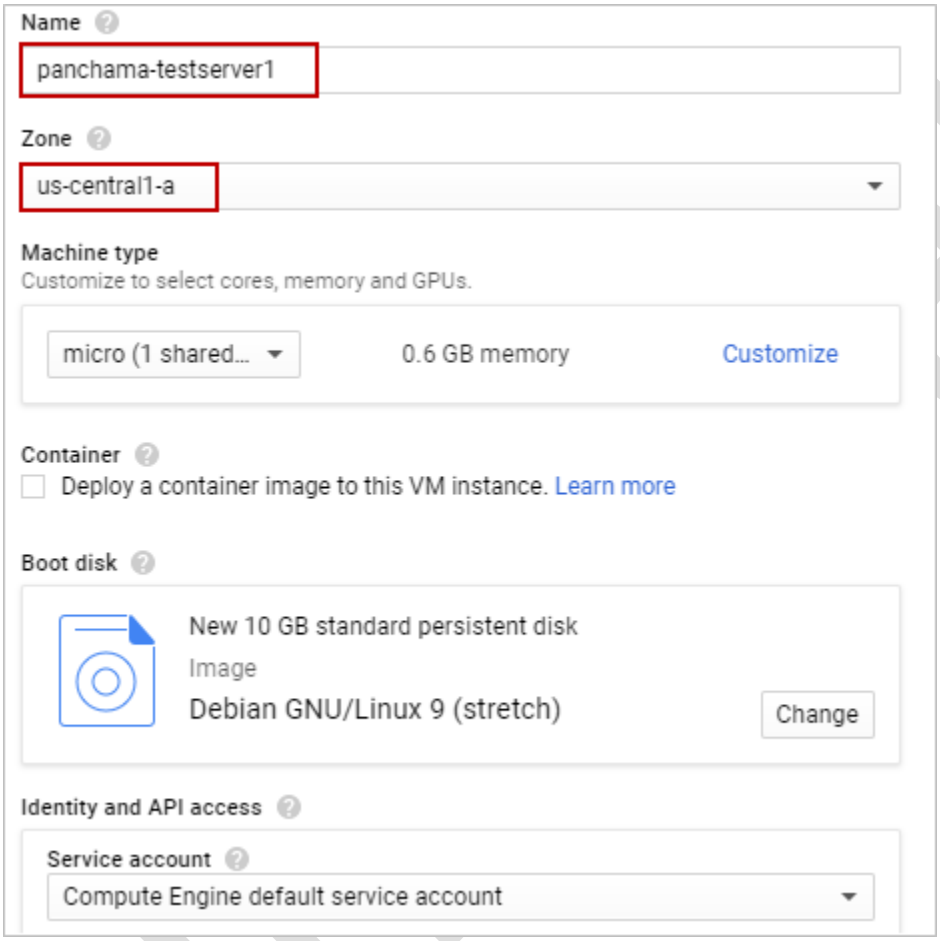
Instance *is to be created in your desired project by selecting the custom netwok under "Management, disk, Networking, access and security"*

Step 4:

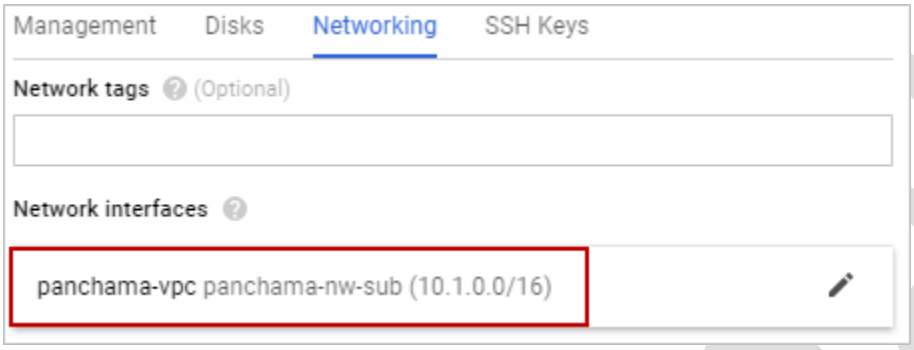
Navigate to ***Compute Engine*** *and create instance by specifying below details.*

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

Internal

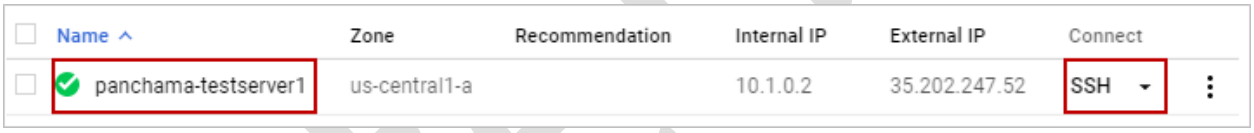


2. Choose the network, created in the previous steps.

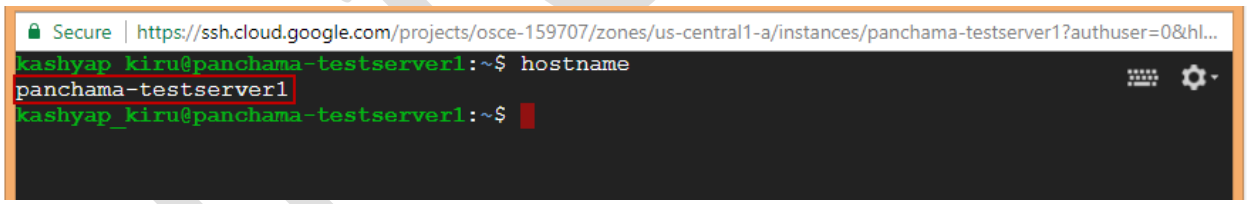


Step 6:

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



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



Internal

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.

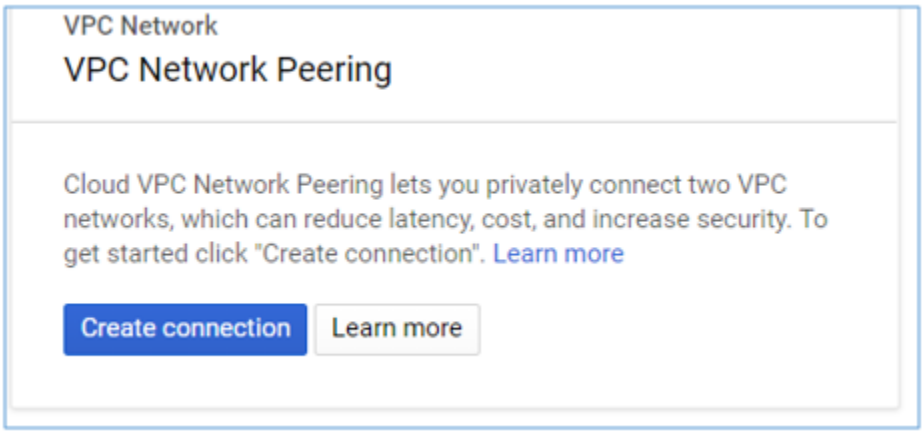
- *Name of the network: peer-vpc-1*
- *Name of the subnet: public-subnet-1*
- *CIDR: 10.0.0.0/24*

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

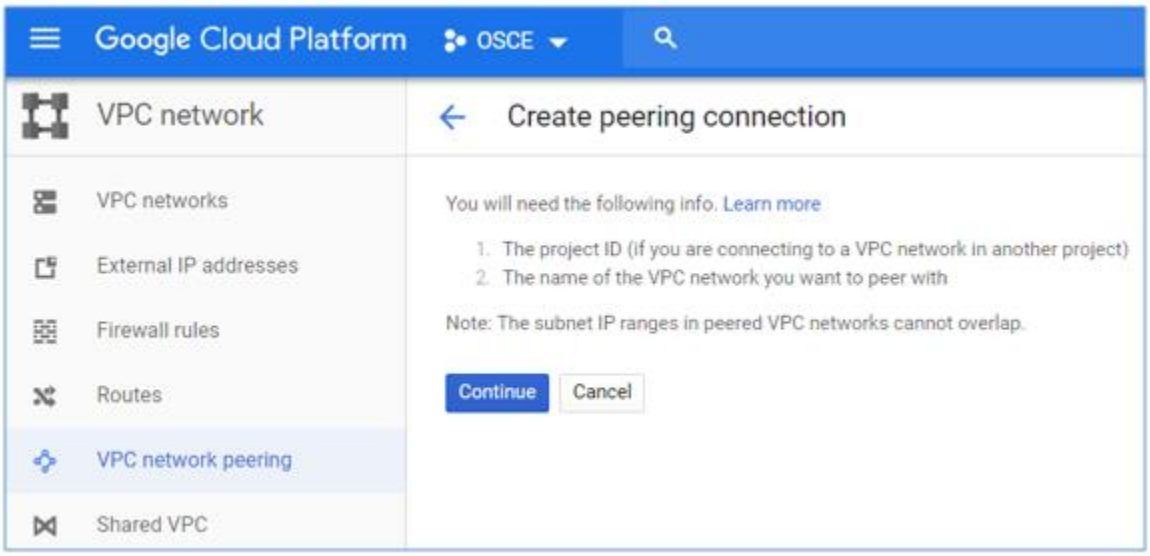
- *Name of the network: peer-vpc-2*
- *Name of the subnet: public-subnet-2*
- *CIDR: 192.168.0.0/24*

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

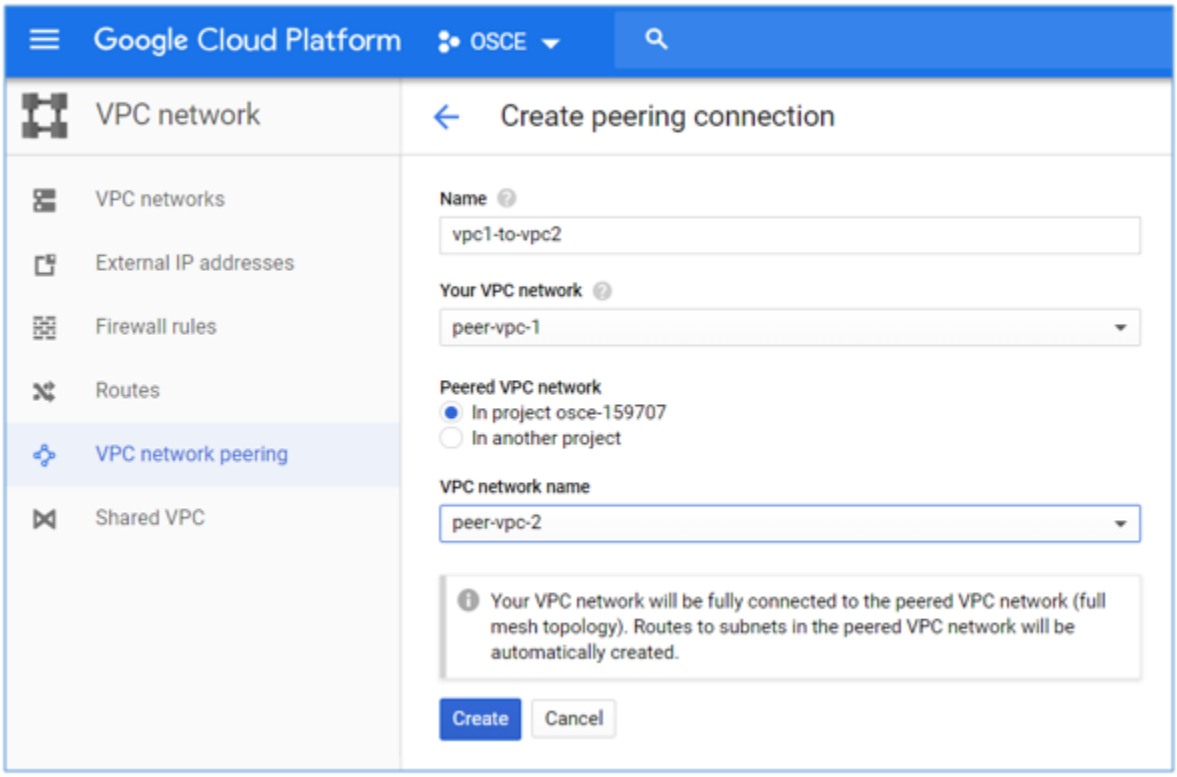
Internal



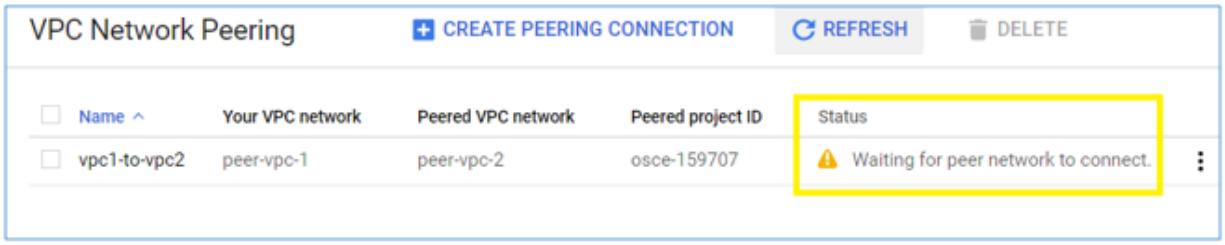
Click “continue”.



Create a connection from vpc1-to-vpc2.

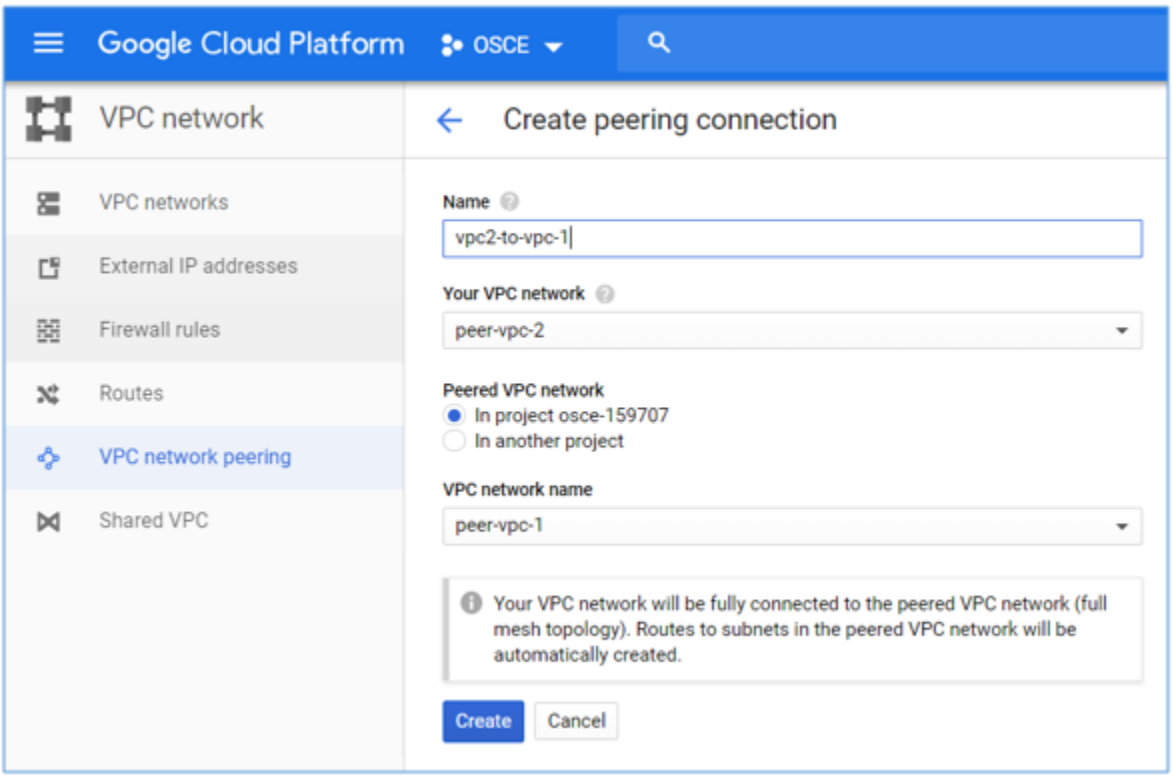


Observer the status of the network peering connection.

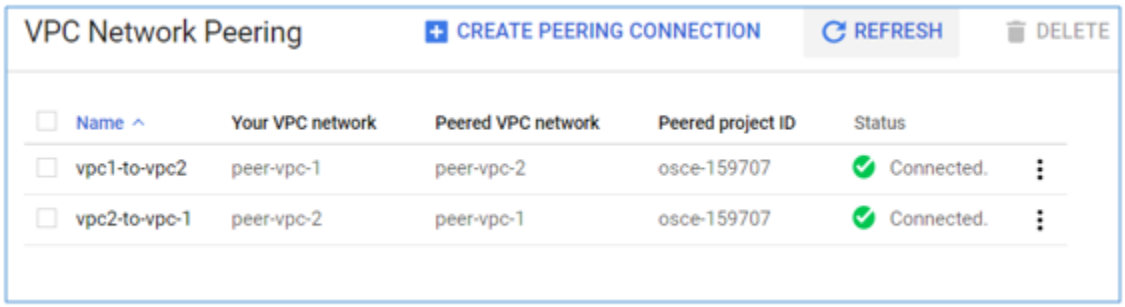


Create the peering connection from vpc2-to-vpc1

Internal


Google Cloud Platform
OSCE
VPC network
Create peering connection
VPC networks
External IP addresses
Firewall rules
Routes
VPC network peering
Shared VPC
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.



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.

Interna