Lab Work​

Task 1. Creating the custom-vpc-1​

​

In Cloud Shell, run the following command to create a custom VPC named cloud associated with your Google Cloud project:​

​

gcloud compute networks create custom-vpc-1 --subnet-mode custom.​

Run the following to enable SSH and icmp:​

gcloud compute firewall-rules create vpc1-firewall --network custom-vpc-1 --allow tcp:22

Creating firewall...working..Created [<https://www.googleapis.com/compute/v1/projects/olagt-381100/global/firewalls/vpc1-firewall>].

Creating firewall...done.

NAME: vpc1-firewall

NETWORK: custom-vpc-1

DIRECTION: INGRESS

PRIORITY: 1000

ALLOW: tcp:22

DENY:

DISABLED: False

Create a subnet within this VPC:​

gcloud compute networks subnets create vpc1-subnet-east --network custom-vpc-1 --range 10.0.1.0/24 --region us-east1​

​

Task 2. Creating the custom-vpc-2​

Create the custom-vpc-2:​

gcloud compute networks create custom-vpc-2 --subnet-mode custom

gcloud compute firewall-rules create vpc2-firewall --network custom-vpc-2 --allow tcp:22,icmp​

gcloud compute networks subnets create vpc2-subnet-east --network custom-vpc-2 --range 10.0.2.0/24 --region us-east1​

Task 3. Creating virtual machine instance with multiple network interfaces​

Create a virtual machine instance with multiple network interfaces:​

gcloud compute instances create vm1 --machine-type=n1-standard-4 --zone=us-east1-b --network-interface subnet=vpc1-subnet-east --network-interface subnet=vpc2-subnet-east --no-address​

​

Task 4. Creating another virtual machine instance​

Now create another instance in the same subnetwork which is used in the secondary interface for the first instance so that you can test the connectivity:​

gcloud compute instances create vm2 --machine-type=n1-standard-1 --zone=us-east1-b --subnet=vpc2-subnet-east​

GO TO VM INSTANCE ON GCP

CLICK THE SSH ON VM1

WHEN SSH OPEN AND COMPLETELY LOAD

ENTER ; ip a

ENTER; ping -c 3 (vm2 ip addresss) 10.0.2.3

**Lab Work​**

**Task 1. Creating the custom-vpc-1​**

**In Cloud Shell, run the following command to create a custom VPC named cloud associated with your Google Cloud project:​**

gcloud compute networks create custom-vpc-1 --subnet-mode custom

Created [<https://www.googleapis.com/compute/v1/projects/olagt-381100/global/networks/custom-vpc-1>].

NAME: custom-vpc-1

SUBNET\_MODE: CUSTOM

BGP\_ROUTING\_MODE: REGIONAL

IPV4\_RANGE:

GATEWAY\_IPV4:

Instances on this network will not be reachable until firewall rules

are created. As an example, you can allow all internal traffic between

instances as well as SSH, RDP, and ICMP by running:

$ gcloud compute firewall-rules create <FIREWALL\_NAME> --network custom-vpc-1 --allow tcp,udp,icmp --source-ranges <IP\_RANGE>

$ gcloud compute firewall-rules create <FIREWALL\_NAME> --network custom-vpc-1 --allow tcp:22,tcp:3389,icmp

**Run the following to enable SSH and icmp:​**

gcloud compute firewall-rules create vpc1-firewall --network custom-vpc-1 --allow tcp:22

Created [<https://www.googleapis.com/compute/v1/projects/olagt-381100/global/networks/custom-vpc-2>].

NAME: custom-vpc-2

SUBNET\_MODE: CUSTOM

BGP\_ROUTING\_MODE: REGIONAL

IPV4\_RANGE:

GATEWAY\_IPV4:

Instances on this network will not be reachable until firewall rules

are created. As an example, you can allow all internal traffic between

instances as well as SSH, RDP, and ICMP by running:

$ gcloud compute firewall-rules create <FIREWALL\_NAME> --network custom-vpc-2 --allow tcp,udp,icmp --source-ranges <IP\_RANGE>

$ gcloud compute firewall-rules create <FIREWALL\_NAME> --network custom-vpc-2 --allow tcp:22,tcp:3389,icmp

**Create a subnet within this VPC:​**

gcloud compute networks subnets create vpc1-subnet-east --network custom-vpc-1 --range 10.0.1.0/24 --region us-east1​-b

**Task 2. Creating the custom-vpc-2​**

**Create the custom-vpc-2:​**

gcloud compute networks create custom-vpc-2 --subnet-mode custom

gcloud compute firewall-rules create vpc2-firewall --network custom-vpc-2 --allow tcp:22,icmp​

gcloud compute networks subnets create vpc2-subnet-east --network custom-vpc-2 --range 10.0.2.0/24 --region us-east1​

**Task 3. Creating virtual machine instance with multiple network interfaces​**

**Create a virtual machine instance with multiple network interfaces:​**

gcloud compute instances create vm1 --machine-type=n1-standard-4 --zone=us-east1-b --network-interface subnet=vpc1-subnet-east --network-interface subnet=vpc2-subnet-east 10.0.1.0/24 -address​

​**Task 4. Creating another virtual machine instance​**

**Now create another instance in the same subnetwork which is used in the secondary interface for the first instance so that you can test the connectivity:​**

gcloud compute instances create vm2 --machine-type=n1-standard-1 --zone=us-east1-b --subnet=vpc2-subnet-east

**Task 5. Verify you can connect​**

Now do a few exercises to test the connection to your VMs.​

Switch back to the Cloud console and navigate to Compute Engine > VM instances.​

Click the SSH button corresponding to the vm1 instance. This opens an SSH connection to the instance in a new window.​

In the SSH window of vm1, type the following commands, replacing with the IP address from the last command you ran, to use an ICMP echo against vm2.:​

**ping -c 3 <vm2-internal-ip-address>​**

**Task 6. Troubleshooting​**

Troubleshooting tasks:​

Check firewall rules to see that they allow connectivity to the VM secondary interface.​

You can check by looking at the firewall rules for the network that is attached to the secondary interface by either visiting Cloud Console and clicking the appropriate VPC network or by using the following gcloud command:​

**gcloud compute firewall-rules list --filter='network:\[NETWORK\\_NAME\]'​**

Check if you are trying to connect to a secondary interface from an Internet address or from outside of the secondary interface's network.​

You can only connect to an interface's internal IP from within its net

​