

DEBORAH BINYANYA

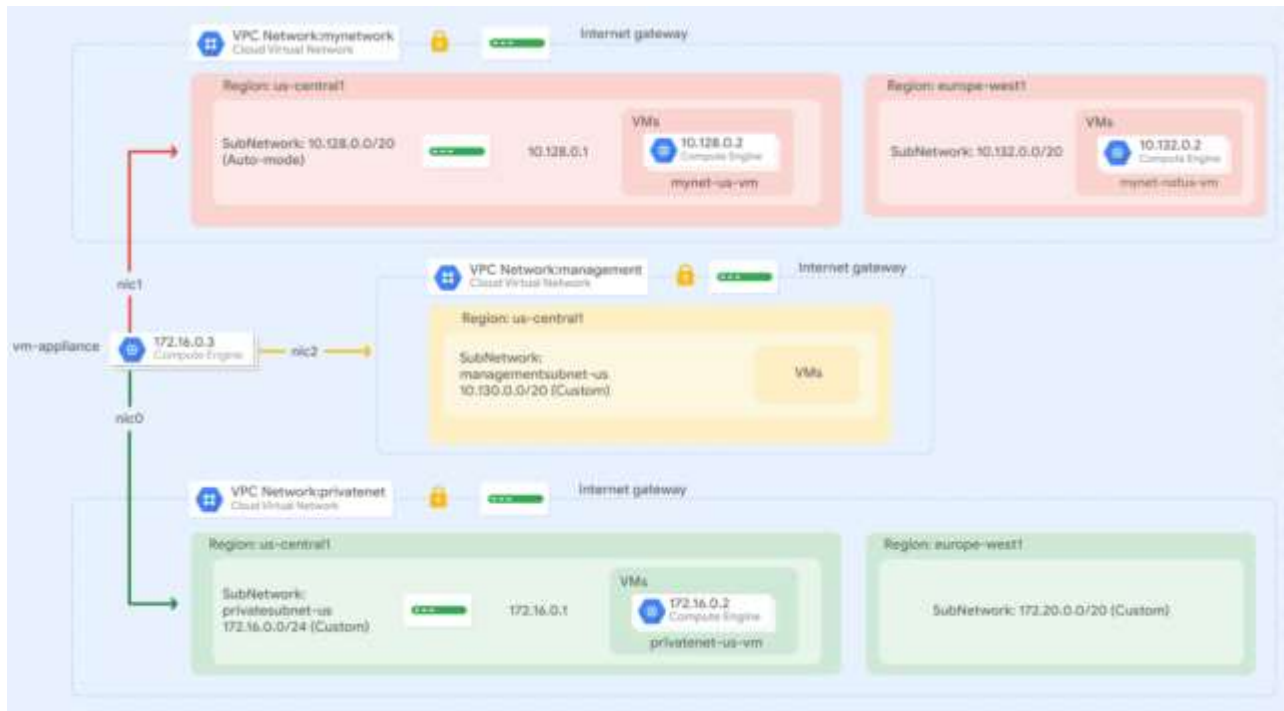
Table of Contents

LAB 1: WORKING WITH MULTIPLE VPC NETWORKS.....	2
Overview	2
Objectives	2
Setup and requirements	2
Task 1. Create custom mode VPC networks with firewall rules	4
Create the managementnet network	4
Create the privatenet network	9
Create the firewall rules for managementnet	13
Create the firewall rules for privatenet	18
Task 2. Create VM instances	19
Create the managementnet-us-vm instance	19
Create the privatenet-us-vm instance	24
Task 3. Explore the connectivity between VM instances	26
Ping the external IP addresses	26
Ping the internal IP addresses.....	28
Task 4. Create a VM instance with multiple network interfaces	30
Create the VM instance with multiple network interfaces.....	30
Explore the network interface details.....	34
Explore the network interface connectivity	38
Review.....	40

LAB 1: WORKING WITH MULTIPLE VPC NETWORKS

Overview

In this lab, you create several VPC networks and VM instances and test connectivity across networks. Specifically, you create two custom mode networks (**managementnet** and **privatenet**) with firewall rules and VM instances, as shown in this network diagram:



The **mynetwork** network, its firewall rules, and two VM instances (**mynet-notus-vm** and **mynet-us-vm**) have already been created for you in this Qwiklabs project.

Objectives

In this lab, you learn how to perform the following tasks:

- Create custom mode VPC networks with firewall rules
- Create VM instances using Compute Engine
- Explore the connectivity for VM instances across VPC networks
- Create a VM instance with multiple network interfaces

Setup and requirements

For each lab, you get a new Google Cloud project and set of resources for a fixed time at no cost.

1. Click the **Start Lab** button. If you need to pay for the lab, a pop-up opens for you to select your payment method. On the left is the **Lab Details** panel with the following:
 - The **Open Google Cloud console** button
 - Time remaining

- The temporary credentials that you must use for this lab
 - Other information, if needed, to step through this lab
2. Click **Open Google Cloud console** (or right-click and select **Open Link in Incognito Window** if you are running the Chrome browser).

The lab spins up resources, and then opens another tab that shows the **Sign in** page.

Tip: Arrange the tabs in separate windows, side-by-side.

Note: If you see the **Choose an account** dialog, click **Use Another Account**.

3. If necessary, copy the **Username** below and paste it into the **Sign in** dialog.

"Username"

You can also find the **Username** in the **Lab Details** panel.

4. Click **Next**.
5. Copy the **Password** below and paste it into the **Welcome** dialog.

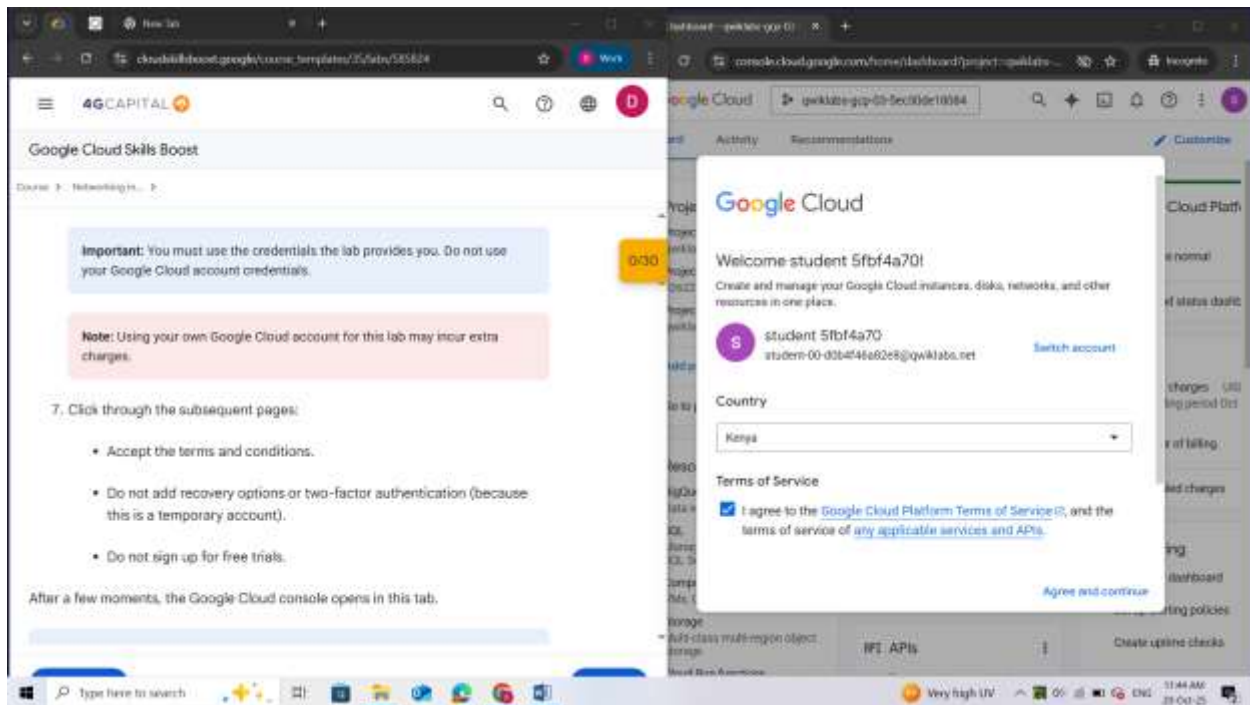
"Password"

You can also find the **Password** in the **Lab Details** panel.

6. Click **Next**.

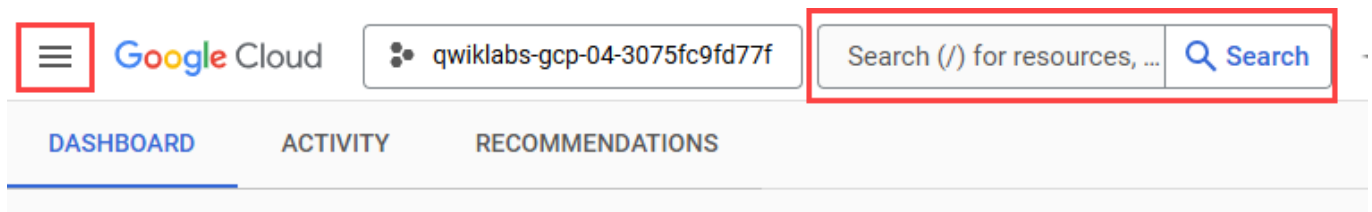
Important: You must use the credentials the lab provides you. Do not use your Google Cloud account credentials. **Note:** Using your own Google Cloud account for this lab may incur extra charges.

7. Click through the subsequent pages:
 - Accept the terms and conditions.
 - Do not add recovery options or two-factor authentication (because this is a temporary account).
 - Do not sign up for free trials.



After a few moments, the Google Cloud console opens in this tab.

Note: To view a menu with a list of Google Cloud products and services, click the **Navigation menu** at the top-left, or type the service or product name in the **Search** field.



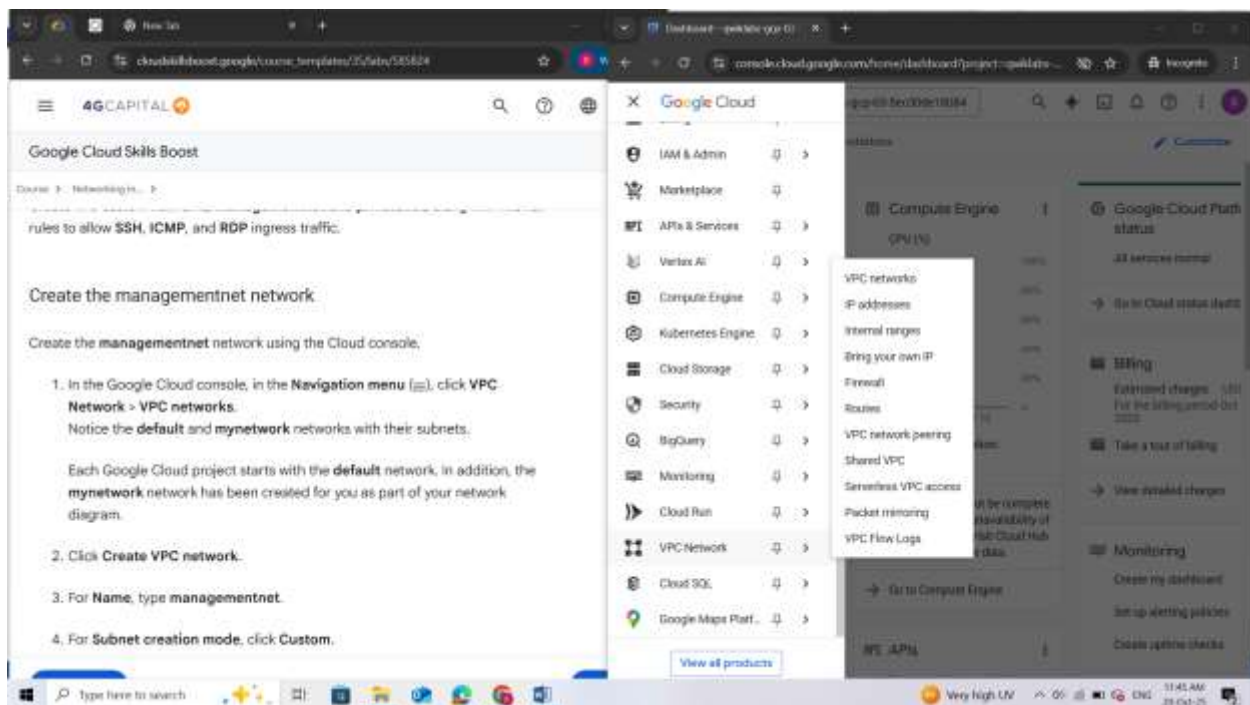
Task 1. Create custom mode VPC networks with firewall rules

Create two custom networks, **managementnet** and **privatenet**, along with firewall rules to allow **SSH**, **ICMP**, and **RDP** ingress traffic.

Create the managementnet network

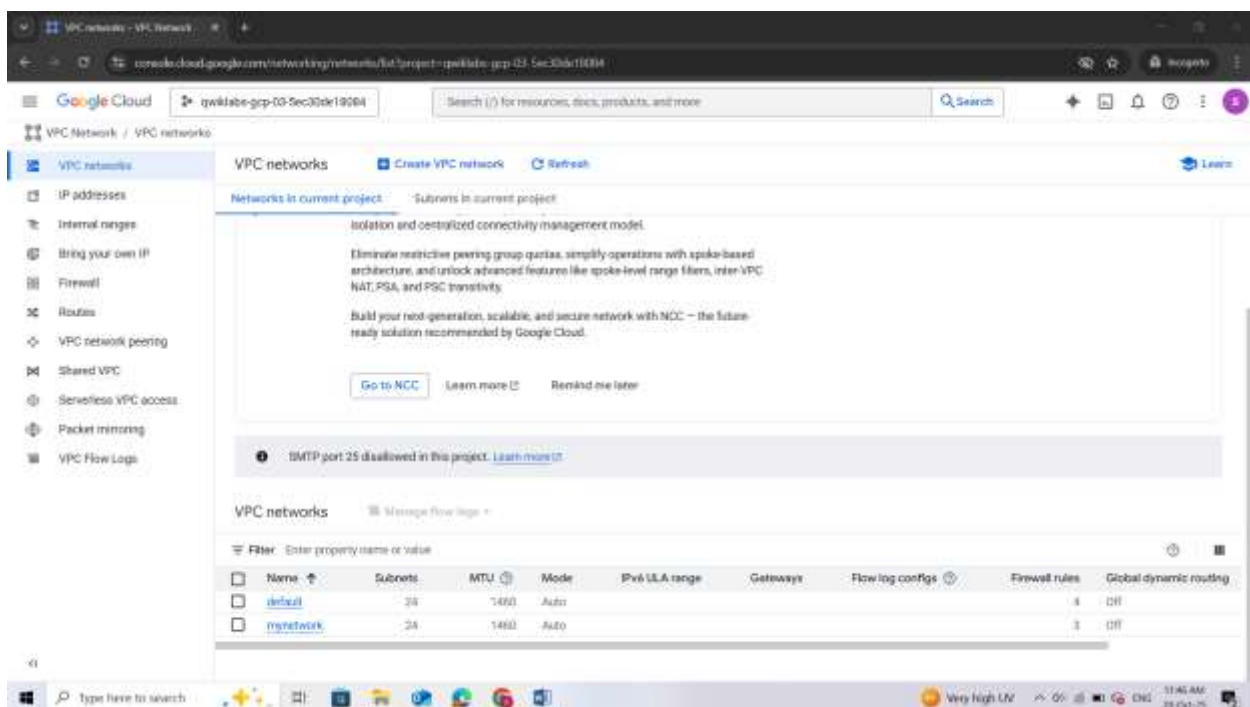
Create the **managementnet** network using the Cloud console.

1. In the Google Cloud console, in the **Navigation menu** (≡), click **VPC Network** > **VPC networks**.



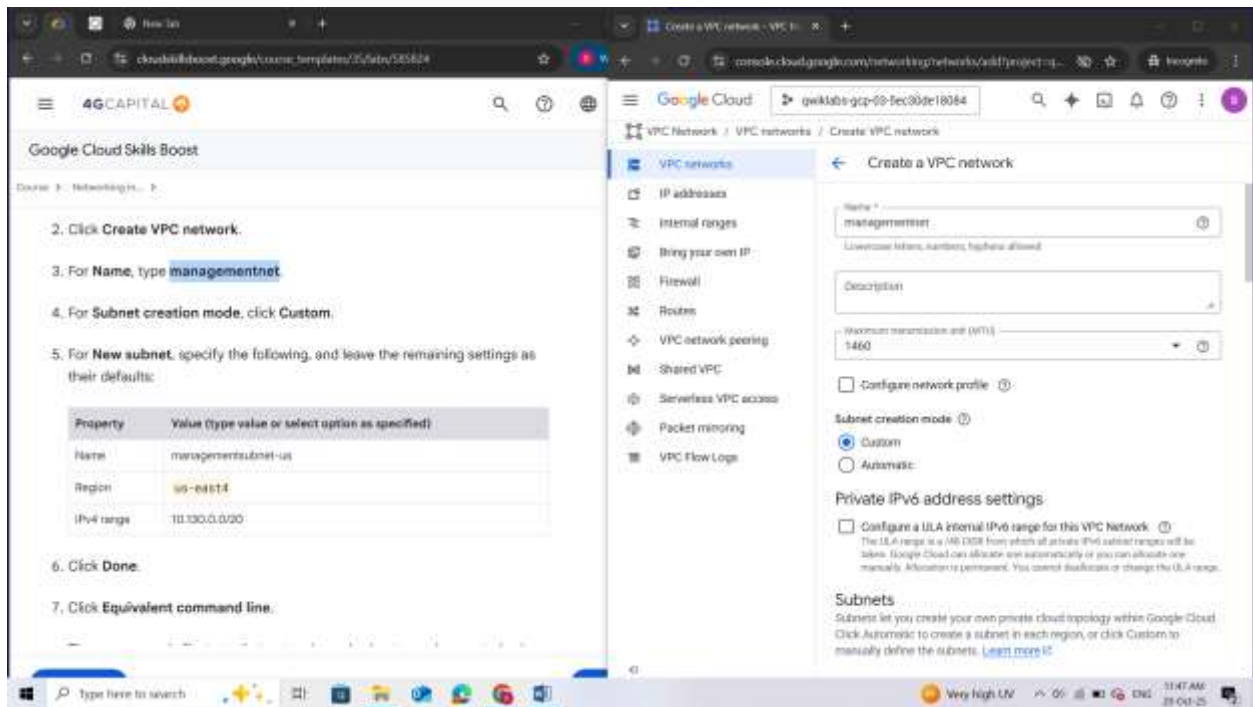
Notice the **default** and **mynetwork** networks with their subnets.

Each Google Cloud project starts with the **default** network. In addition, the **mynetwork** network has been created for you as part of your network diagram.



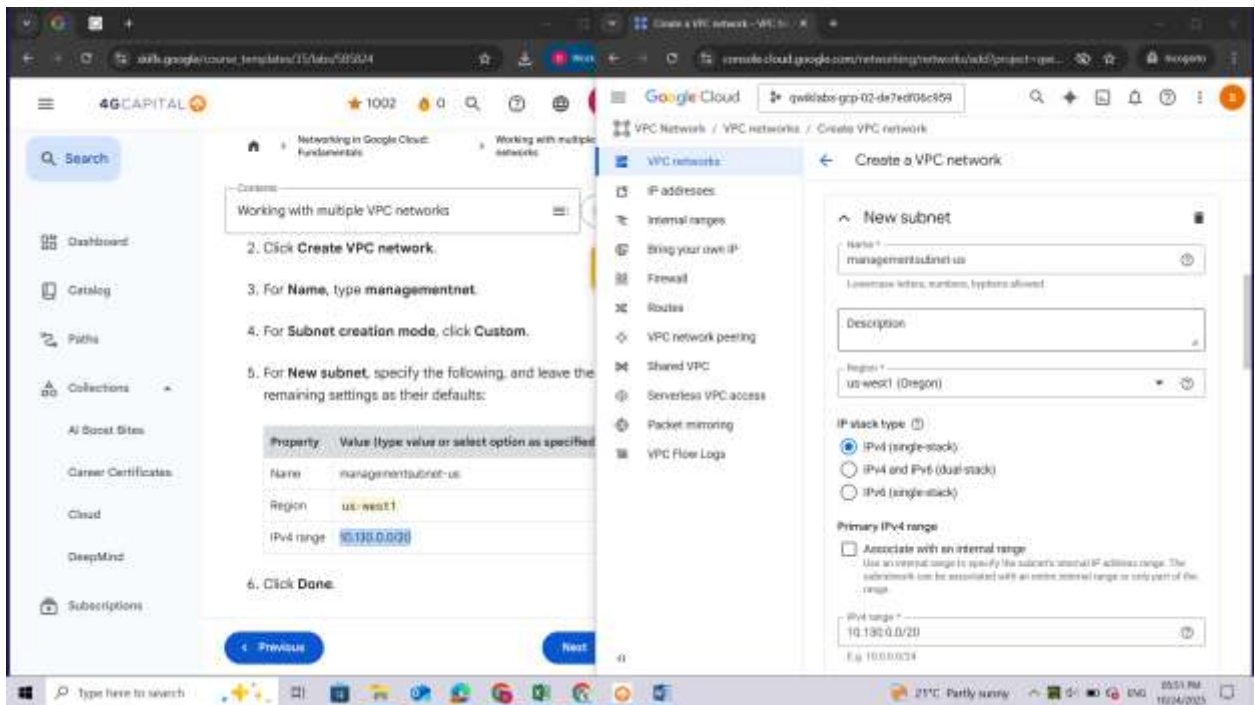
2. Click **Create VPC network**.
3. For **Name**, type **managementnet**.

4. For **Subnet creation mode**, click **Custom**.

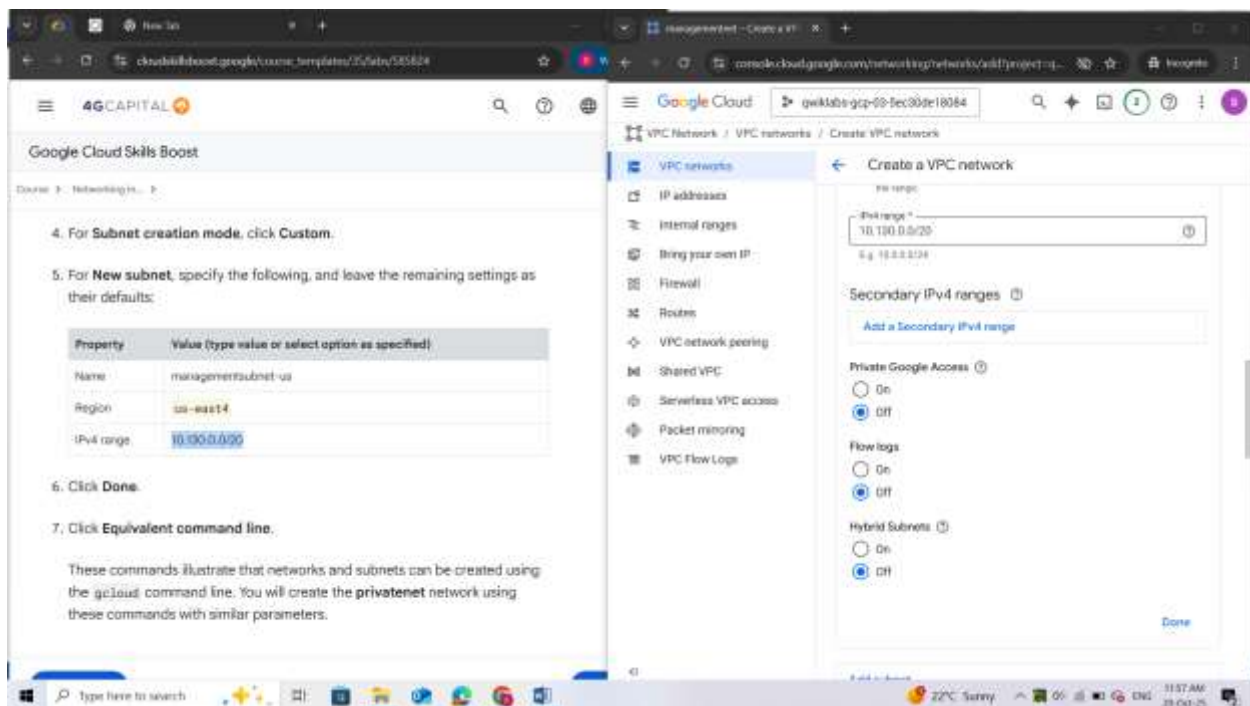


5. For **New subnet**, specify the following, and leave the remaining settings as their defaults:

Property	Value (type value or select option as specified)
Name	managementsubnet-us
Region	<filled at lab start>
IPv4 range	10.130.0.0/20



6. Click **Done**.



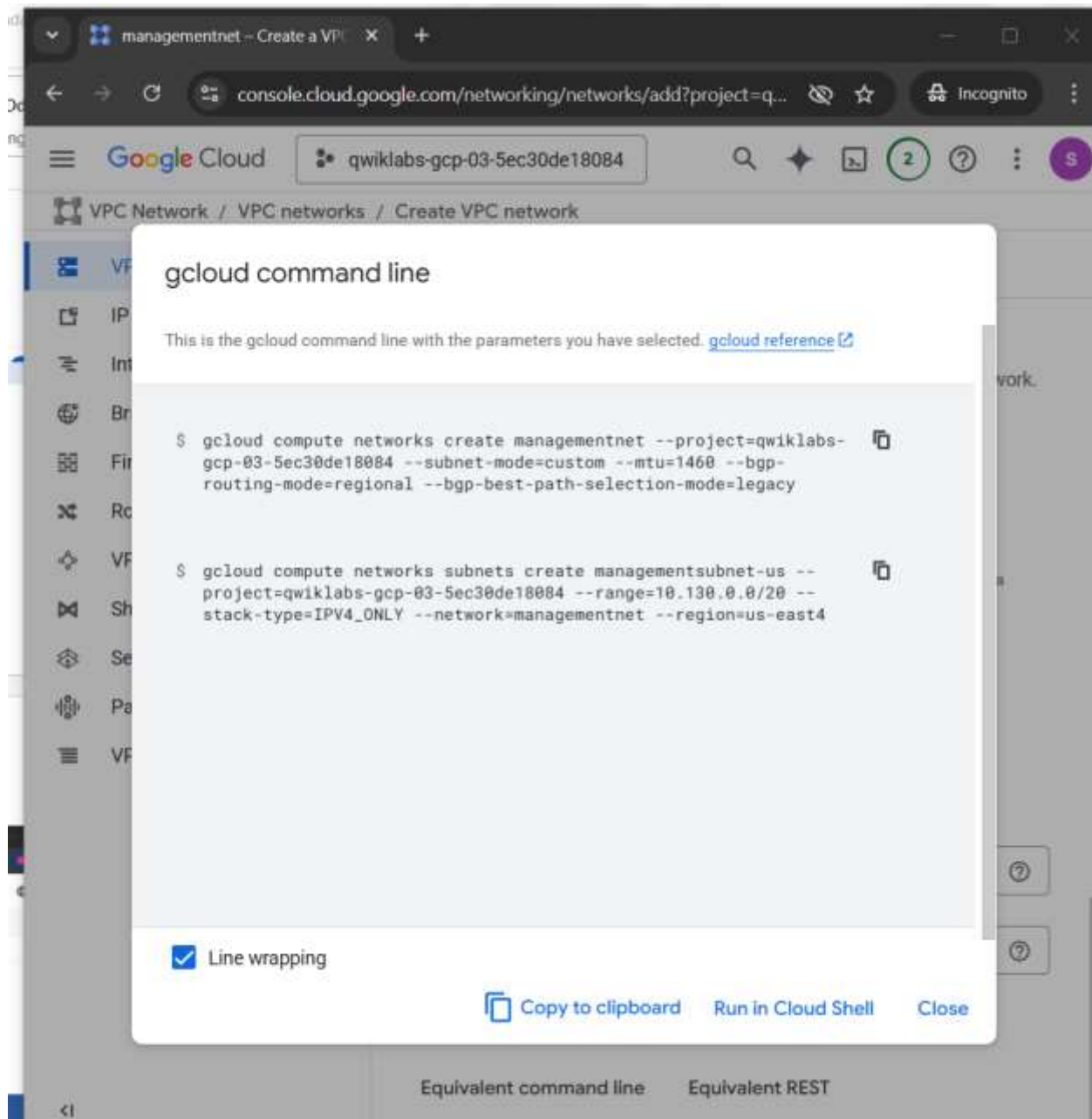
7. Click **Equivalent command line**.

The screenshot displays two browser windows. The left window, titled 'Google Cloud Skills Boost', shows a course page for 'Networking' with steps 4, 5, 6, and 7. Step 5 includes a table for subnet configuration:

Property	Value (type value or select option as specified)
Name	management-subnet-us
Region	us-east14
IPv4 range	10.100.0.0/20

The right window, titled 'Google Cloud', shows the 'Create a VPC network' page. The 'VPC networks' sidebar is active. The main configuration area shows 'Advanced dynamic routing configuration' with 'Dynamic routing mode' set to 'Regional' and 'Best path selection mode' set to 'Legacy (default)'. The 'DNS configuration (optional)' section shows 'Managed zone' and 'DNS server policy' dropdowns. 'Create' and 'Cancel' buttons are at the bottom.

These commands illustrate that networks and subnets can be created using the `gcloud` command line. You will create the **privatenet** network using these commands with similar parameters.




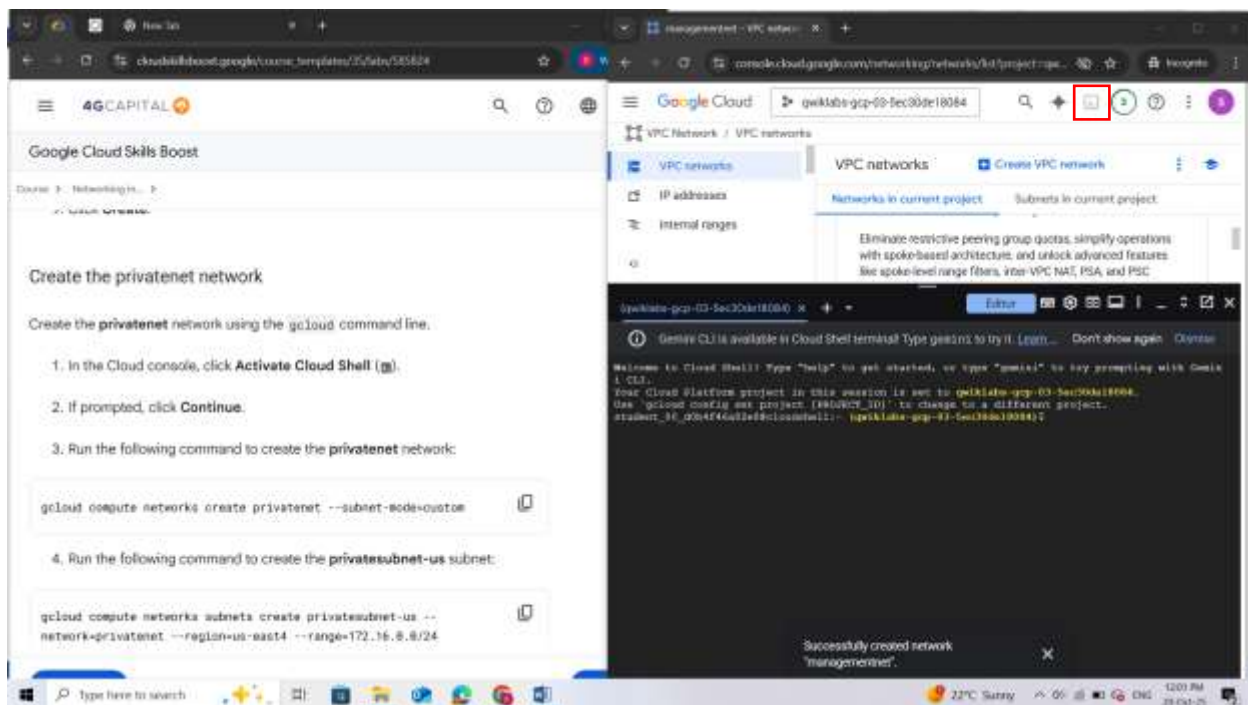
8. Click **Close**.

9. Click **Create**.

Create the privatenet network

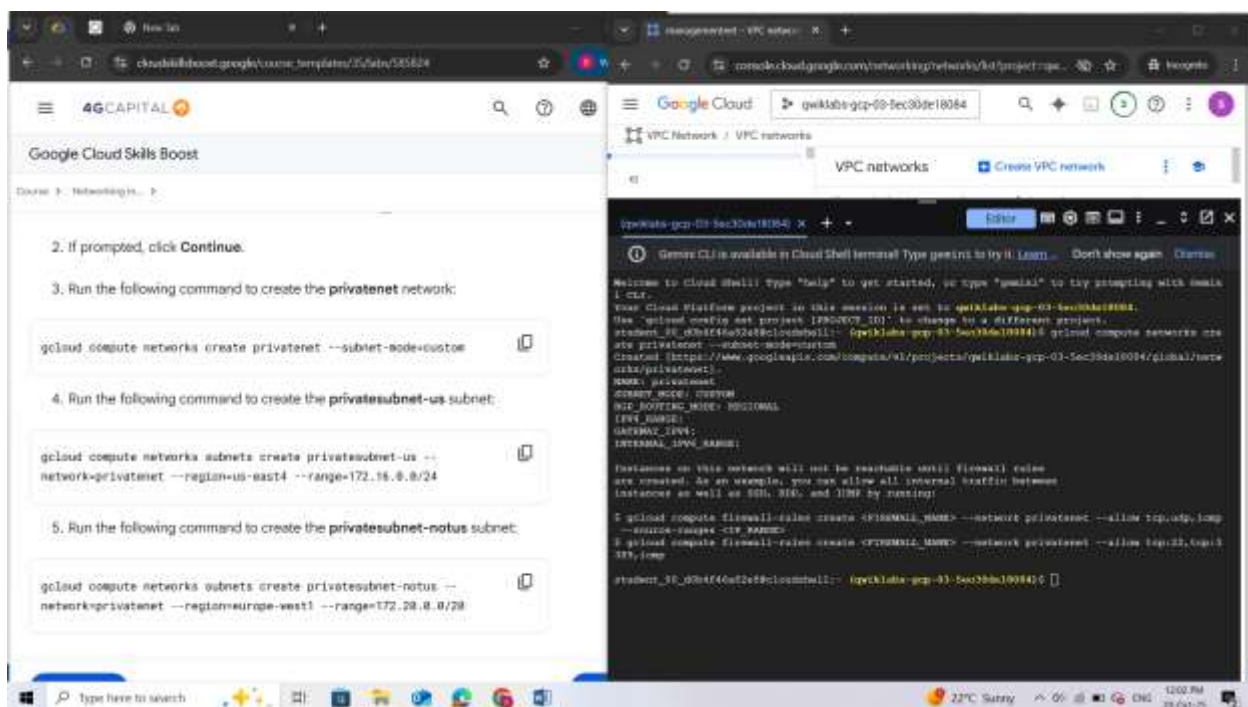
Create the **privatenet** network using the gcloud command line.

1. In the Cloud console, click **Activate Cloud Shell** ().
2. If prompted, click **Continue**.



3. Run the following command to create the **privatenet** network:

gcloud compute networks create privatenet --subnet-mode=custom

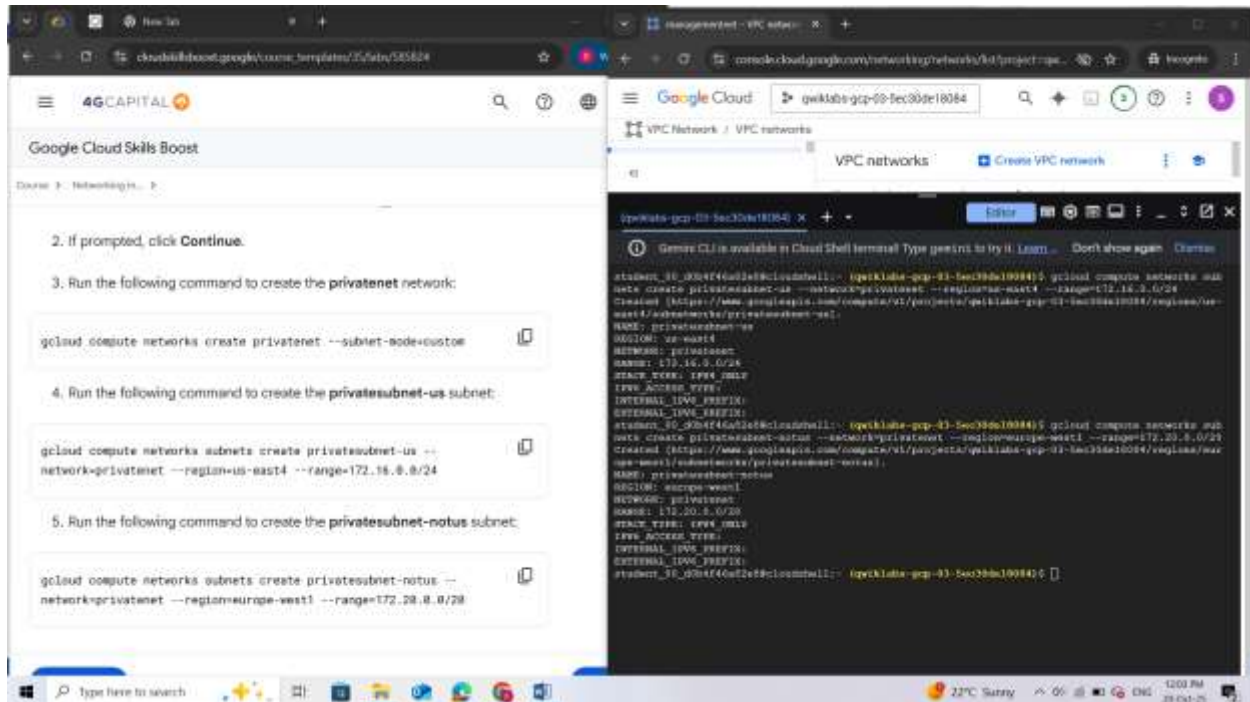


4. Run the following command to create the **privatesubnet-us** subnet:

gcloud compute networks subnets create privatesubnet-us --network=privatenet --region="filled at lab start" --range=172.16.0.0/24

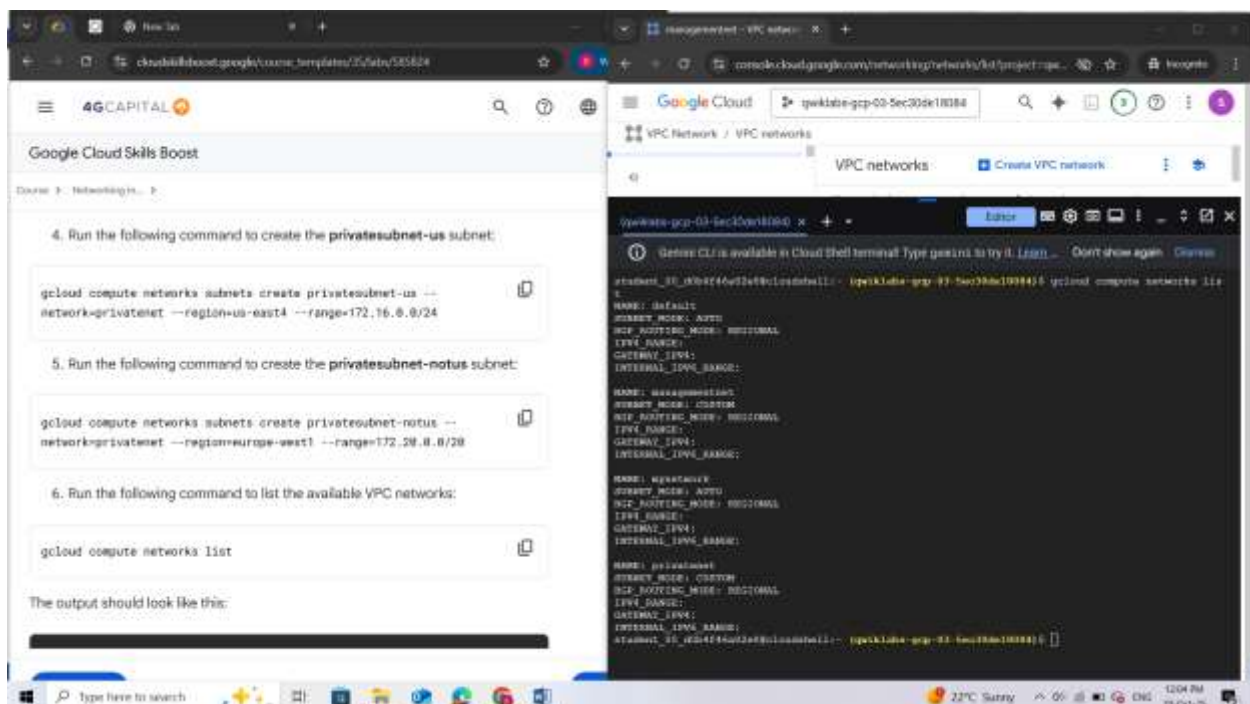
5. Run the following command to create the **privatesubnet-notus** subnet:

gcloud compute networks subnets create privatesubnet-notus --network=privatenet --region="filled at lab start" --range=172.20.0.0/20



6. Run the following command to list the available VPC networks:

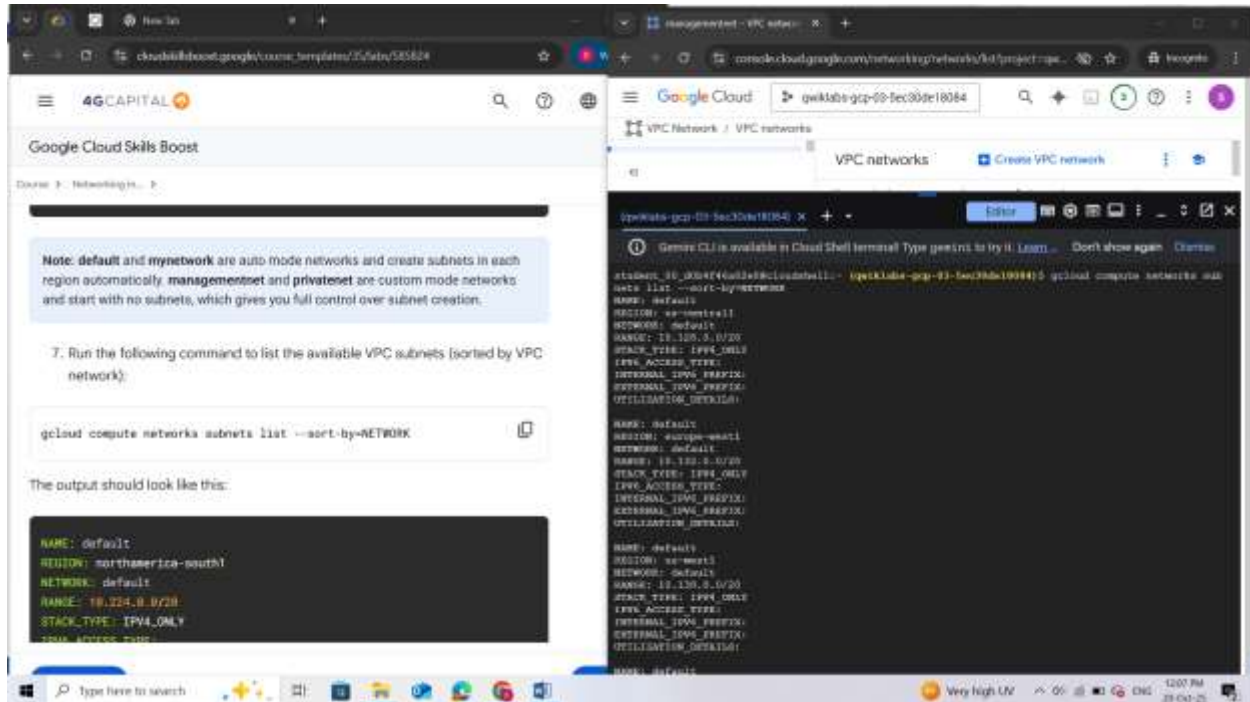
gcloud compute networks list



Note: *default* and *mynetwork* are auto mode networks and create subnets in each region automatically. *managementnet* and *privatenet* are custom mode networks and start with no subnets, which gives you full control over subnet creation.

7. Run the following command to list the available VPC subnets (sorted by VPC network):

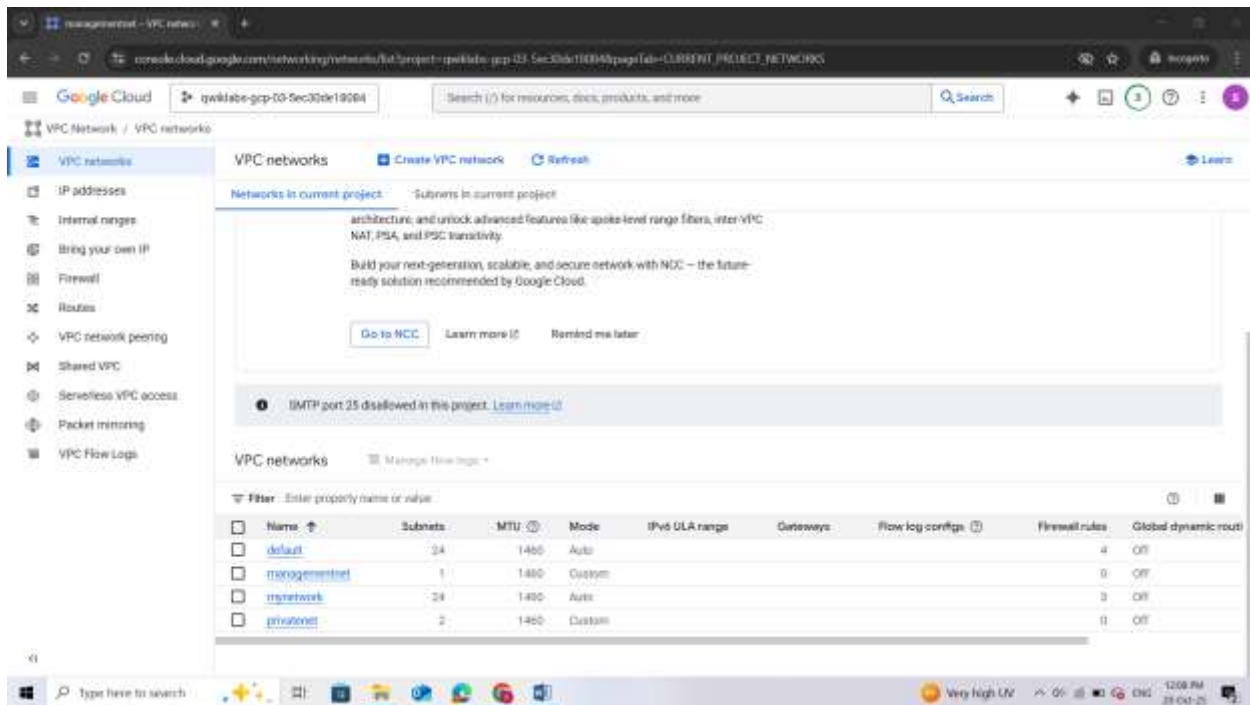
`gcloud compute networks subnets list --sort-by=NETWORK`



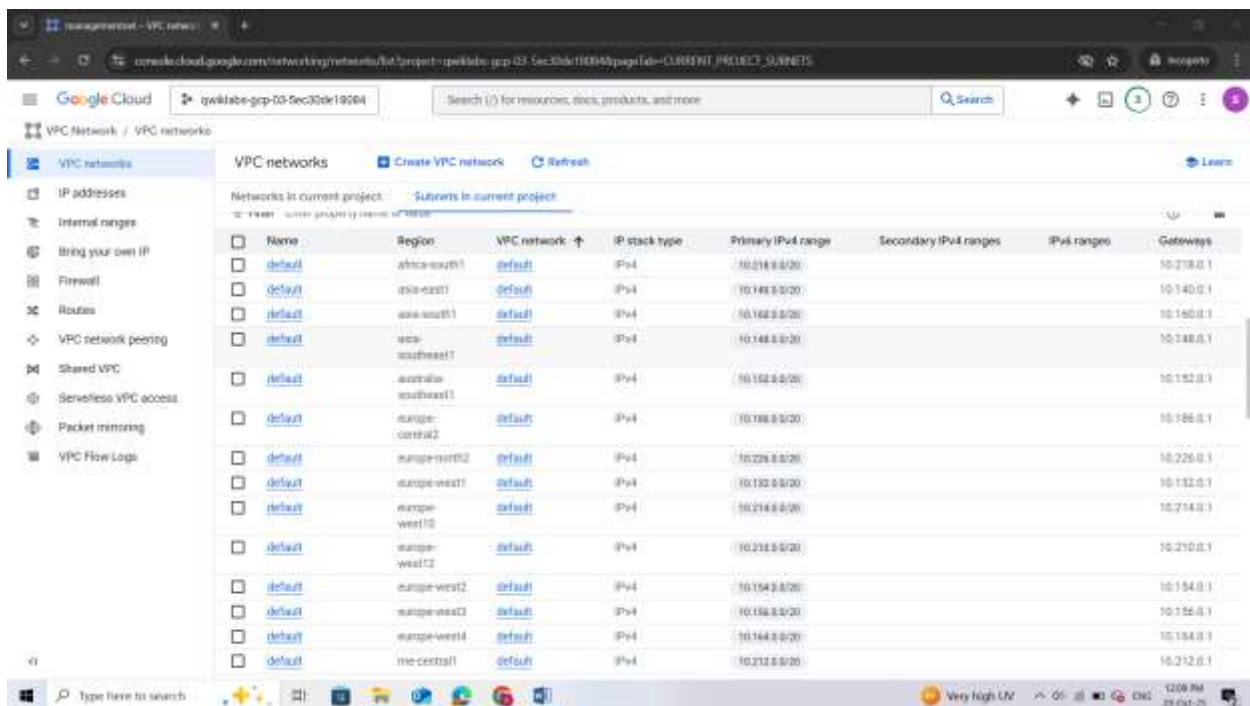
Note: As expected, the *default* and *mynetwork* networks have subnets in each region, because they are auto mode networks. The *managementnet* and *privatenet* networks only have the subnets that you created, because they are custom mode networks.

8. In the Cloud console, in the **Navigation menu** (≡), click **VPC Network > VPC networks**.
Verify that the same **networks** and **subnets** are listed in the Cloud console.

Networks:



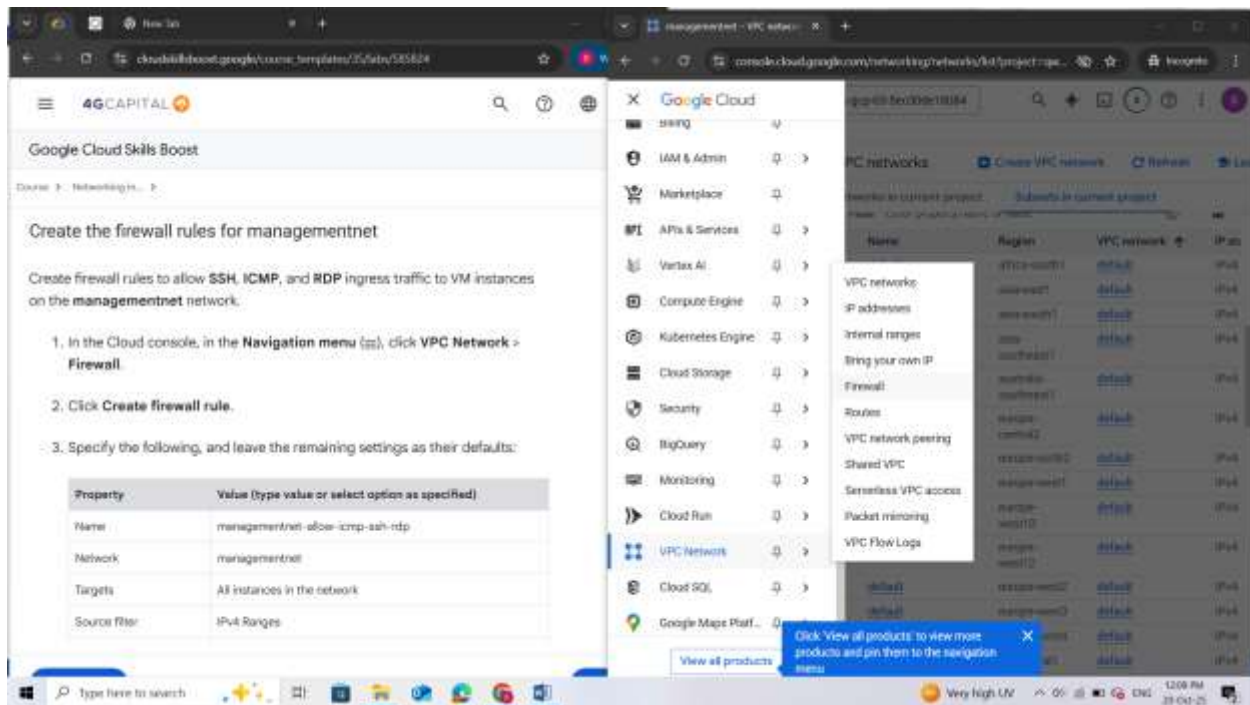
Subnets:



Create the firewall rules for managementnet

Create firewall rules to allow **SSH**, **ICMP**, and **RDP** ingress traffic to VM instances on the **managementnet** network.

1. In the Cloud console, in the **Navigation menu** () , click **VPC Network > Firewall**.



2. Click **Create firewall rule**.

3. Specify the following, and leave the remaining settings as their defaults:

Property	Value (type value or select option as specified)
Name	managementnet-allow-icmp-ssh-rdp
Network	managementnet
Targets	All instances in the network
Source filter	IPv4 Ranges
Source IPv4 ranges	0.0.0.0/0
Protocols and ports	Specified protocols and ports

Google Cloud

qwiklabs-gcp-03-5ec30de18084

3

Network Security

Create a firewall rule

Cloud Armor

DDoS Dashboard

Cloud Armor policies

Adaptive Protection

Cloud Armor Service Tier

Cloud IDS

IDS Dashboard

IDS Endpoints

IDS Threats

Cloud NGFW

Dashboard

Firewall policies

Threats

Firewall endpoints

Secure Access Connect

Realms Preview

Attachments

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

Name *

managementnet-allow-icmp-ssh-rdp

Lowercase letters, numbers, hyphens allowed

Description

Logs

Turning on firewall logs can generate a large number of logs which can increase costs in Logging. [Learn more](#)

On

Off

Network *

managementnet

Priority *

1000

Compare

Priority can be 0 - 65535

Direction of traffic

Ingress

Egress

Action on match

Google Cloud qwiklabs-gcp-03-5ec30de18084

Network Security

Create a firewall rule

Cloud Armor

- DDoS Dashboard
- Cloud Armor policies
- Adaptive Protection
- Cloud Armor Service Tier

Cloud IDS

- IDS Dashboard
- IDS Endpoints
- IDS Threats

Cloud NGFW

- Dashboard
- Firewall policies
- Threats
- Firewall endpoints

Secure Access Connect

- Realms **Preview**
- Attachments

Direction of traffic ?

☒ Ingress

☐ Egress

Action on match ?

☒ Allow

☐ Deny

Targets

All instances in the network

Source filter

IPv4 ranges

Source IPv4 ranges *

0.0.0.0/0 X for example, 0.0.0.0/0, 192.168.2.0/24

Second source filter

None

Destination filter

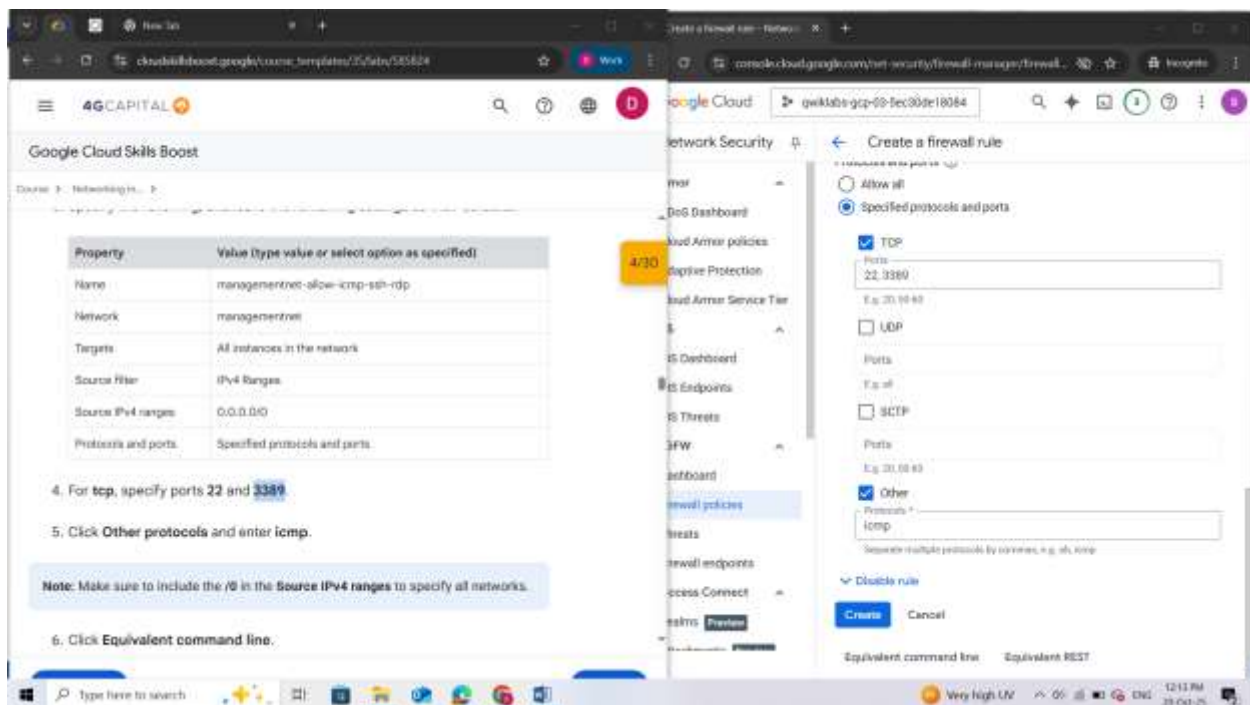
None

Protocols and ports ?

☐ Allow all

☒ Specified protocols and ports

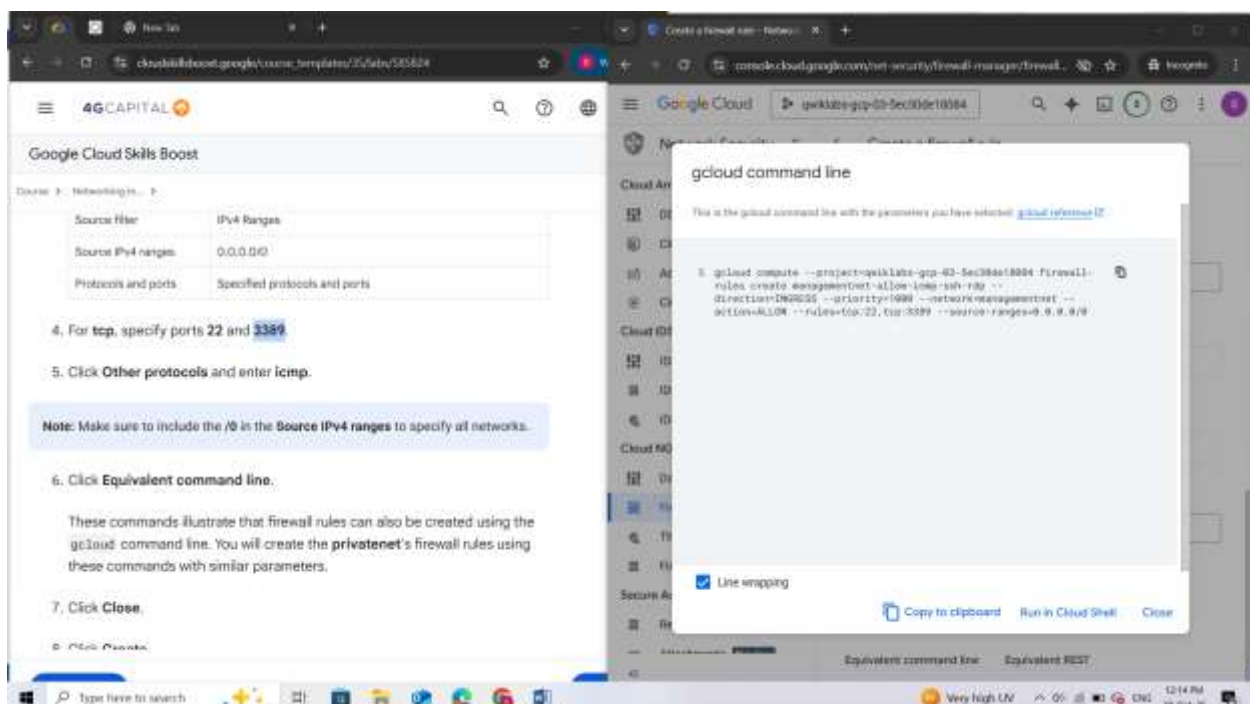
- For **tcp**, specify ports **22** and **3389**.
- Click **Other protocols** and enter **icmp**.



Note: Make sure to include the /0 in the **Source IPv4 ranges** to specify all networks.

6. Click **Equivalent command line**.

These commands illustrate that firewall rules can also be created using the gcloud command line. You will create the **privatenet**'s firewall rules using these commands with similar parameters.




7. Click **Close**.

8. Click **Create**.

Create the firewall rules for **privatenet**

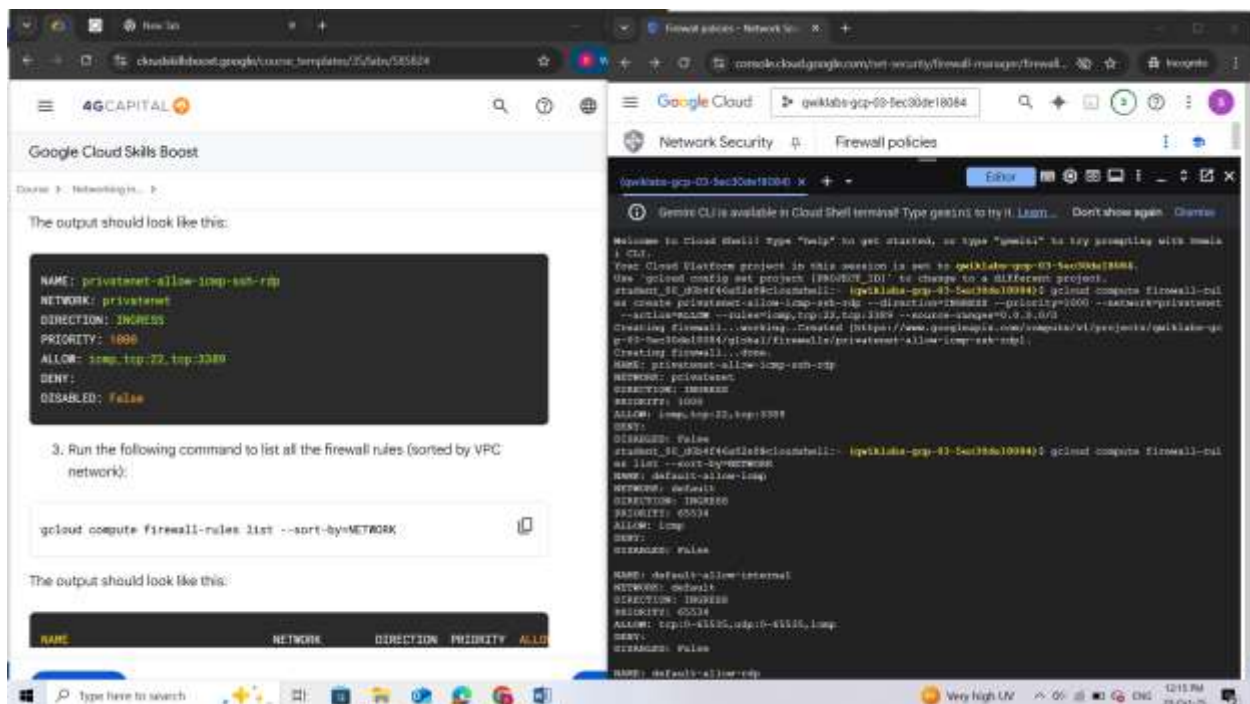
Create the firewall rules for **privatenet** network using the gcloud command line.

1. Return to **Cloud Shell**. If necessary, click **Activate Cloud Shell** ().
2. Run the following command to create the **privatenet-allow-icmp-ssh-rdp** firewall rule:


```
gcloud compute firewall-rules create privatenet-allow-icmp-ssh-rdp --direction=INGRESS --priority=1000 --network=privatenet --action=ALLOW --rules=icmp,tcp:22,tcp:3389 --source-ranges=0.0.0.0/0
```

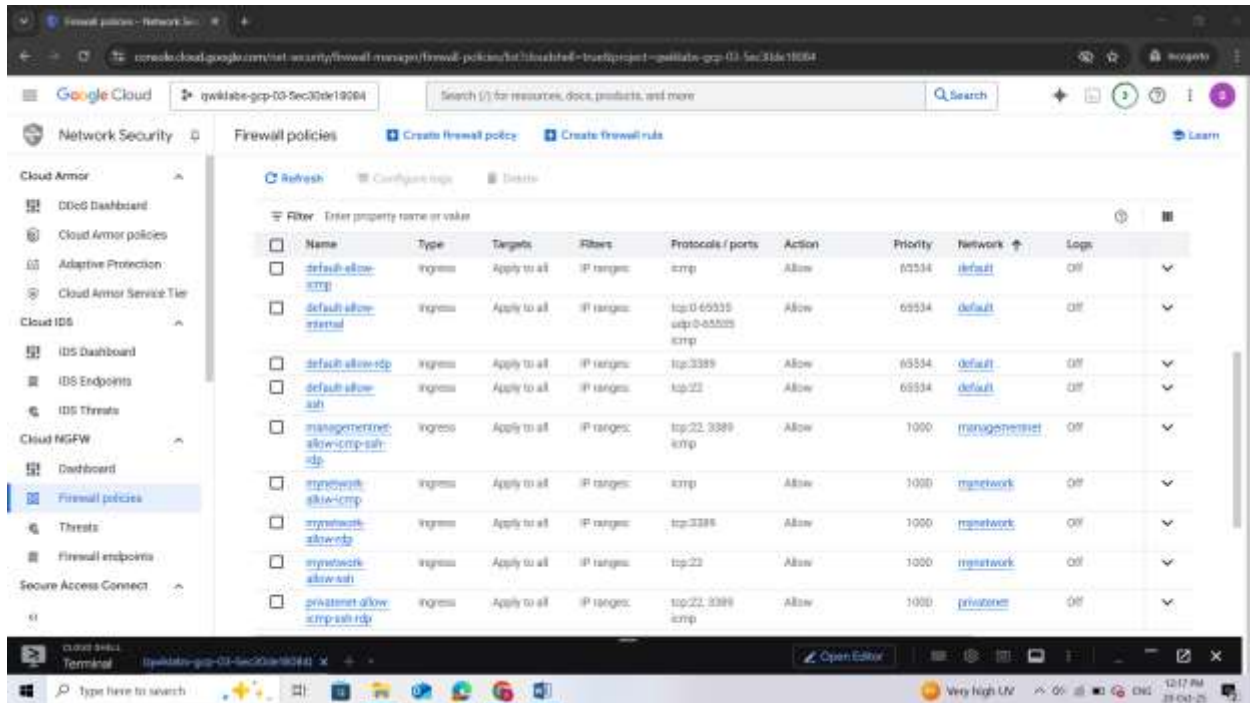
3. Run the following command to list all the firewall rules (sorted by VPC network):

```
gcloud compute firewall-rules list --sort-by=NETWORK
```



The firewall rules for **mynetwork** network have been created for you. You can define multiple protocols and ports in one firewall rule (**privatenet** and **managementnet**) or spread them across multiple rules (**default** and **mynetwork**).

4. In the Cloud console, on the **Navigation menu** (), click **VPC Network > Firewall**. Verify that the same firewall rules are listed in the Cloud console.



Task 2. Create VM instances

Create two VM instances:

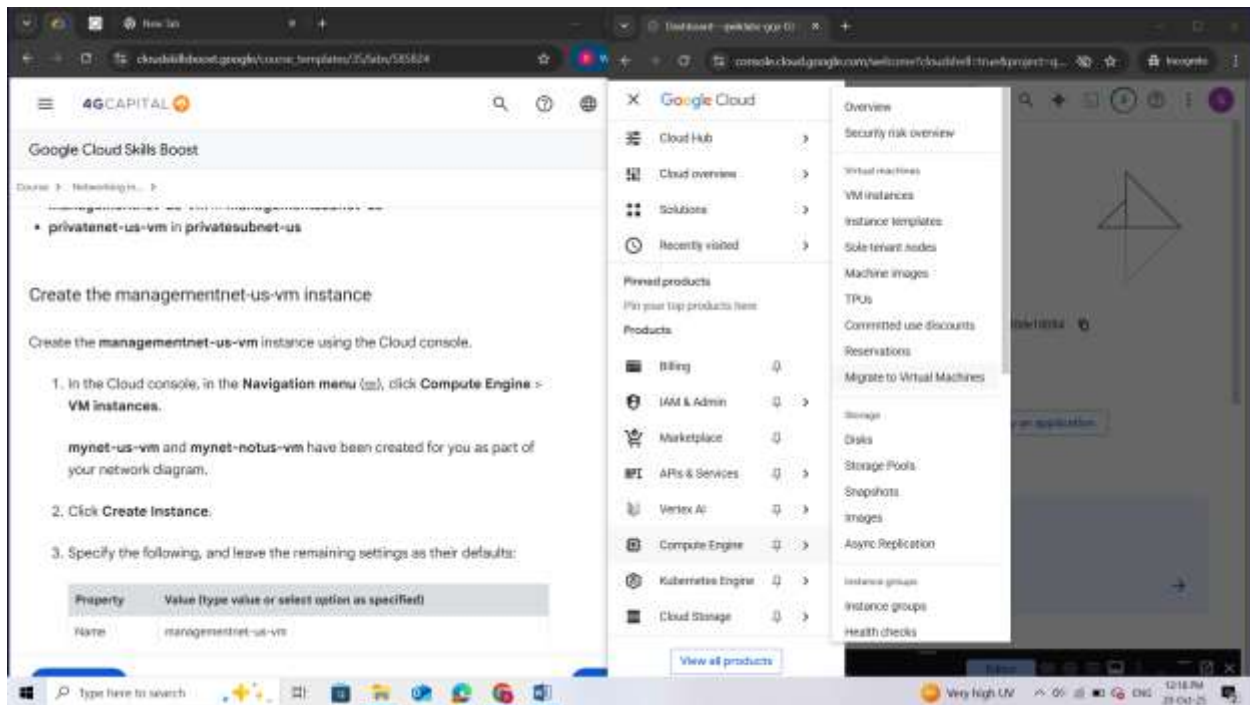
- **managementnet-us-vm** in **managementsubnet-us**
- **privatenet-us-vm** in **privatesubnet-us**

Create the **managementnet-us-vm** instance

Create the **managementnet-us-vm** instance using the Cloud console.

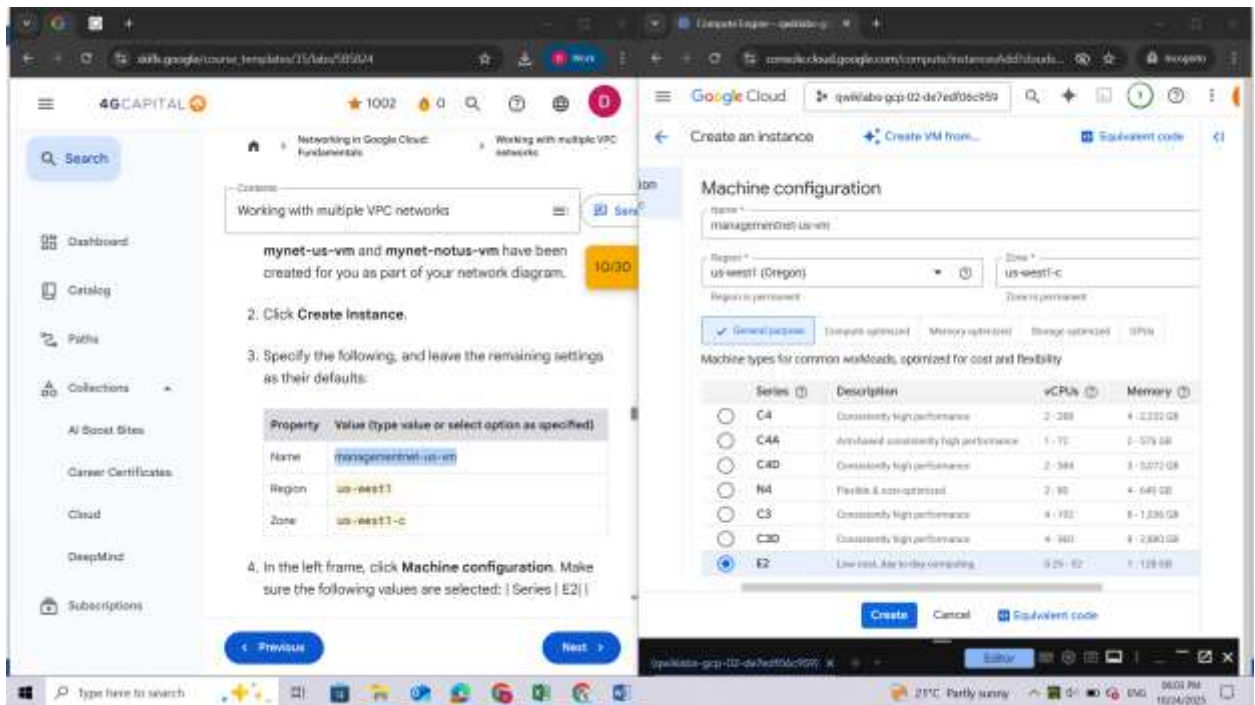
1. In the Cloud console, in the **Navigation menu** () , click **Compute Engine > VM instances**.

mynet-us-vm and **mynet-notus-vm** have been created for you as part of your network diagram.

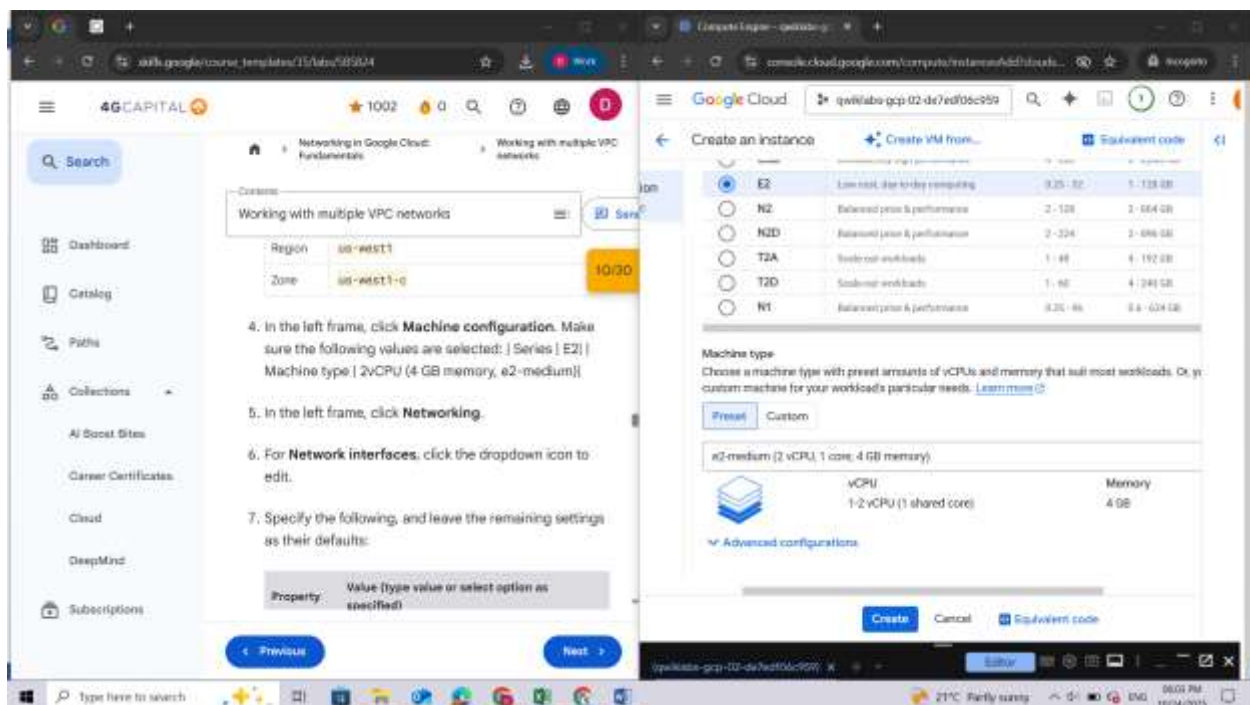


2. Click **Create Instance**.
3. Specify the following, and leave the remaining settings as their defaults:

Property	Value (type value or select option as specified)
Name	managementnet-us-vm
Region	<filled at lab start>
Zone	<filled at lab start>



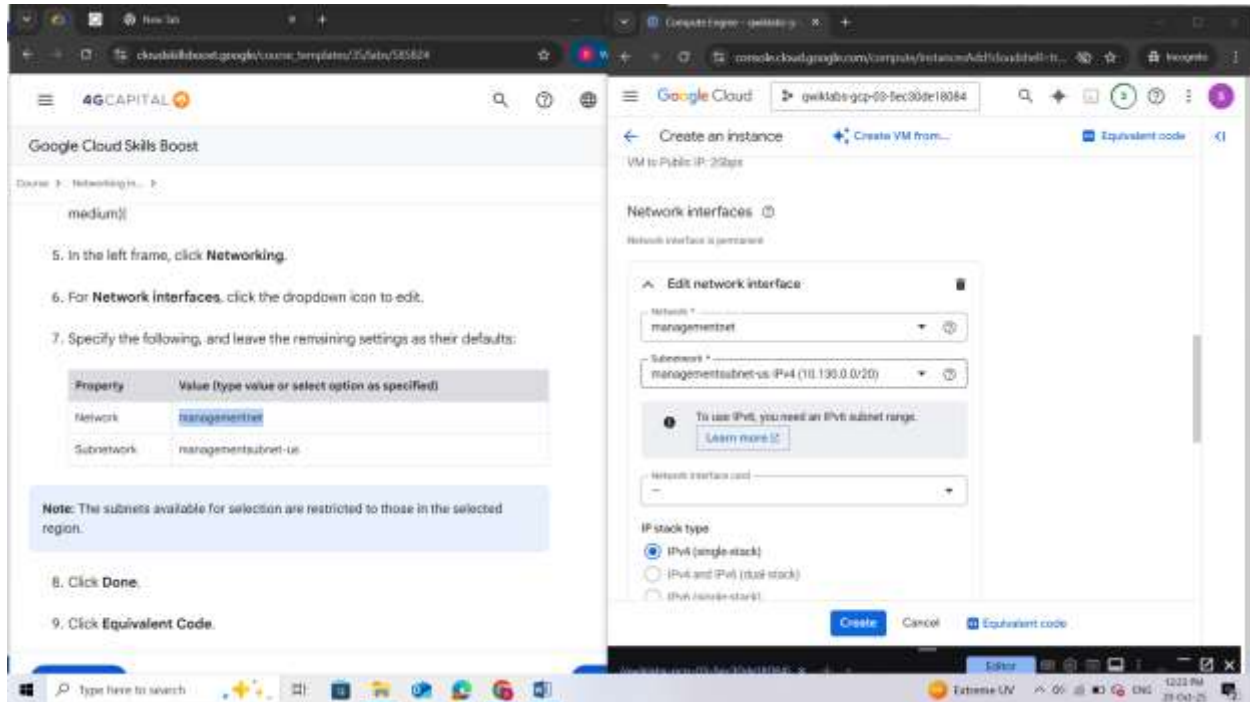
4. In the left frame, click **Machine configuration**. Make sure the following values are selected: | Series | E2 | | Machine type | 2vCPU (4 GB memory, e2-medium) |



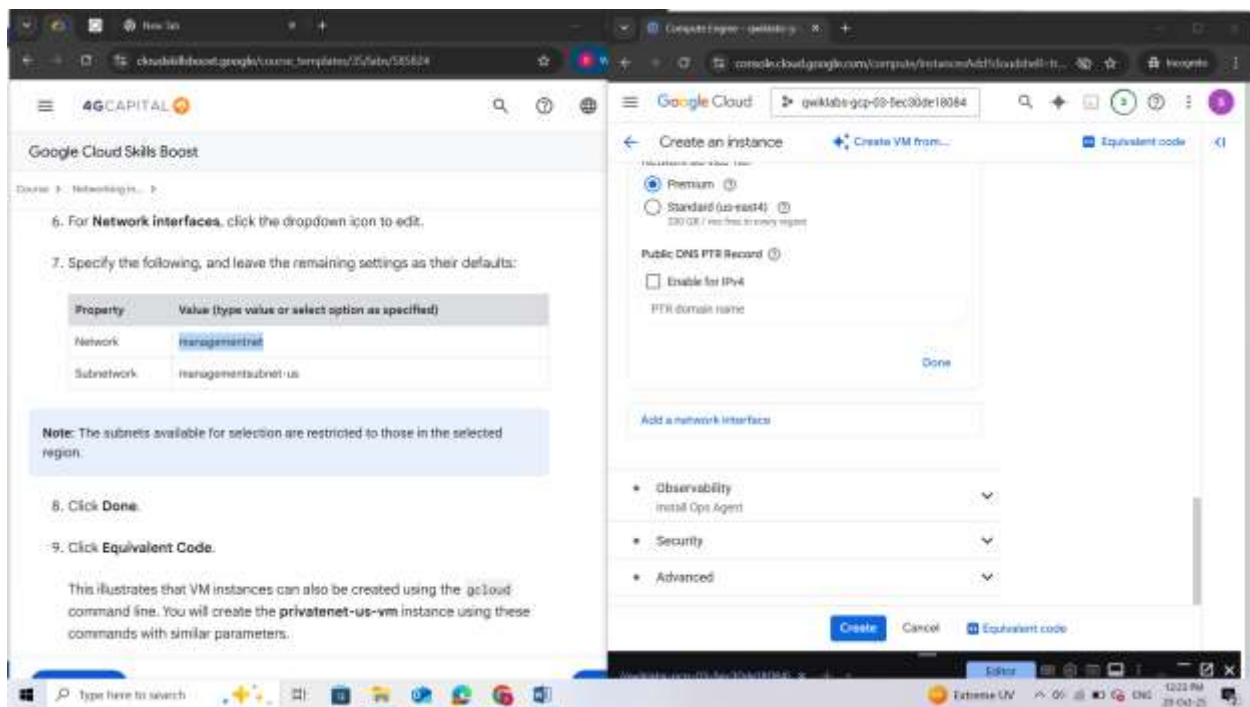
5. In the left frame, click **Networking**.
6. For **Network interfaces**, click the dropdown icon to edit.
7. Specify the following, and leave the remaining settings as their defaults:

Property	Value (type value or select option as specified)
Network	managementnet
Subnetwork	managementsubnet-us

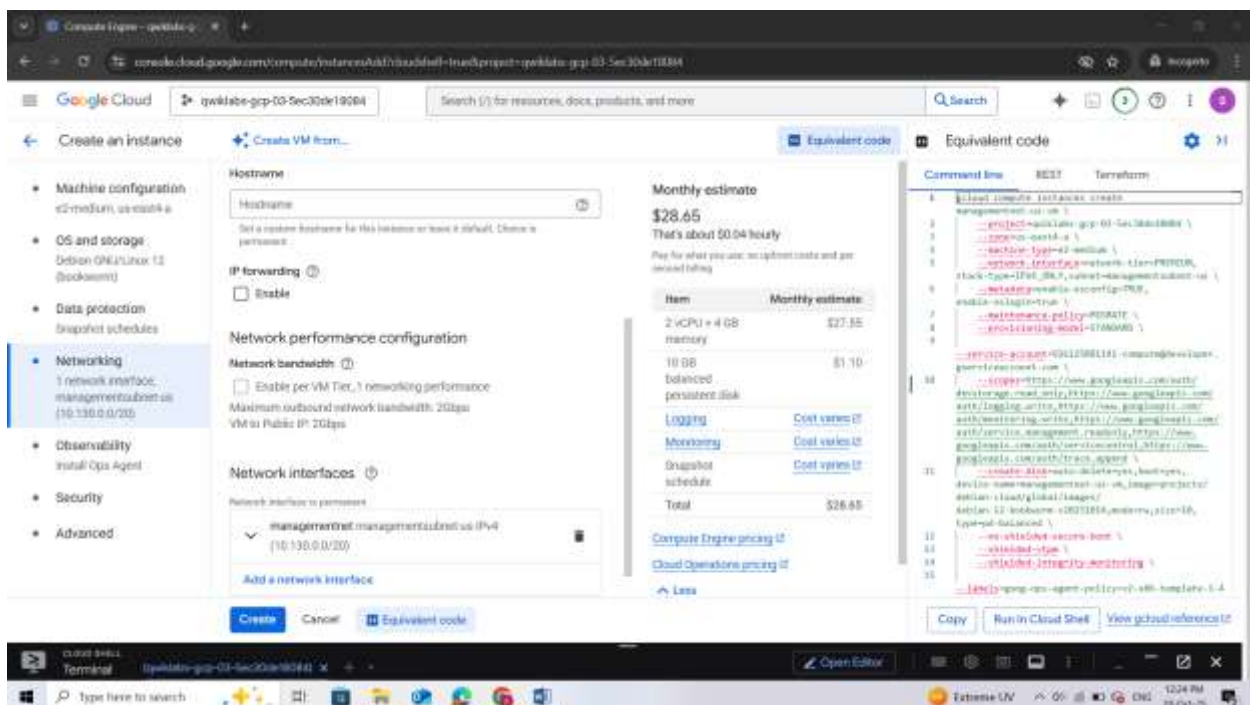
Note: The subnets available for selection are restricted to those in the selected region.



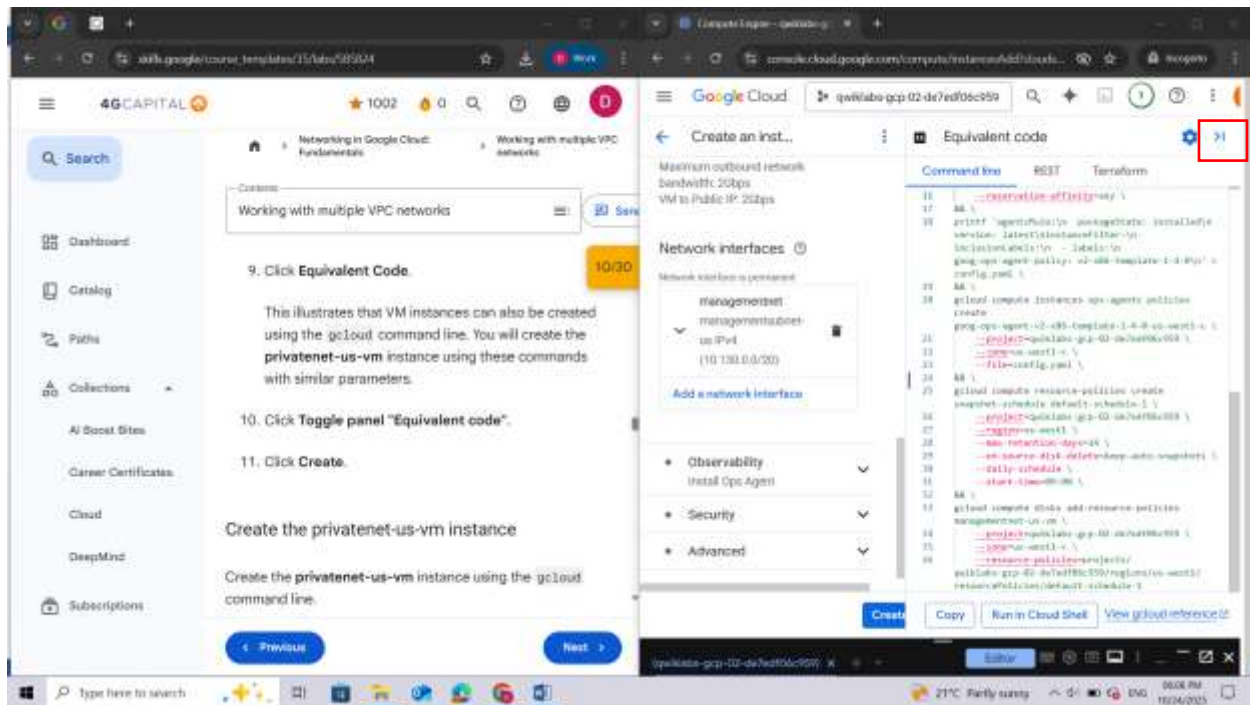
8. Click **Done**.
9. Click **Equivalent Code**.



This illustrates that VM instances can also be created using the gcloud command line. You will create the **privatenet-us-vm** instance using these commands with similar parameters.



10. Click Toggle panel "Equivalent code".



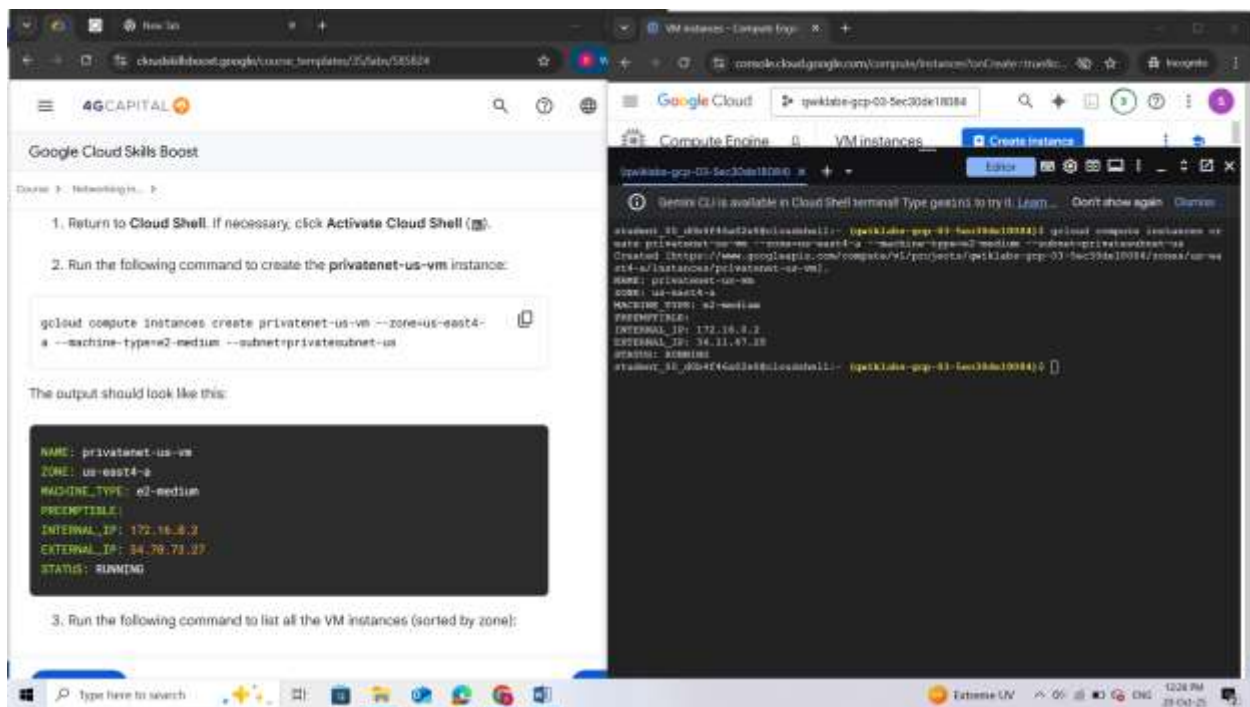
11. Click **Create**.

Create the privatenet-us-vm instance

Create the **privatenet-us-vm** instance using the gcloud command line.

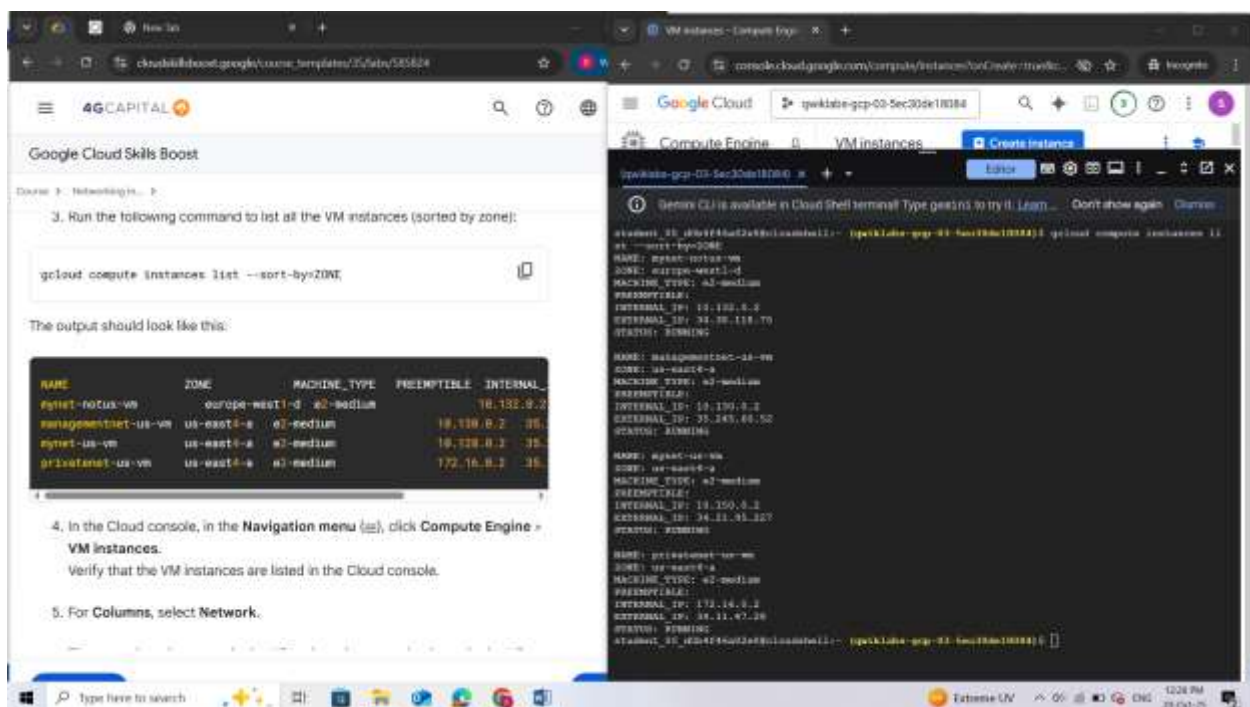
1. Return to **Cloud Shell**. If necessary, click **Activate Cloud Shell** (▶).
2. Run the following command to create the **privatenet-us-vm** instance:


gcloud compute instances create privatenet-us-vm --zone="filled at lab start" --machine-type=e2-medium --subnet=privatesubnet-us

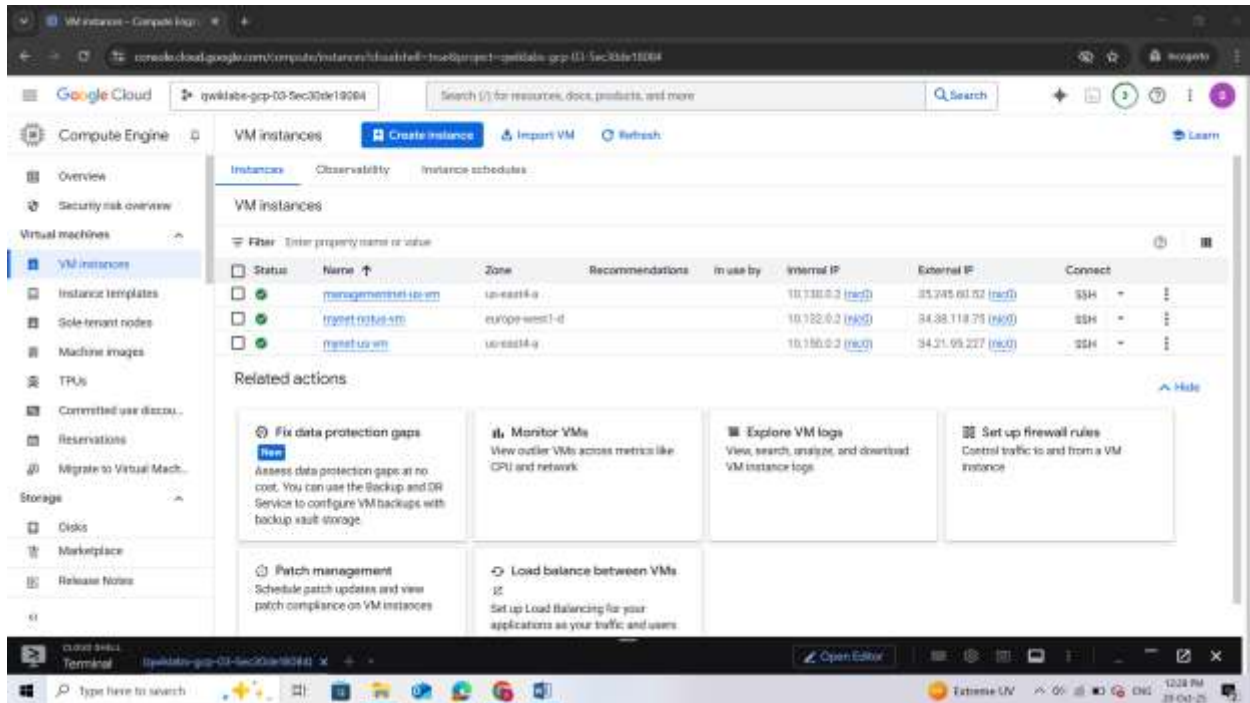


3. Run the following command to list all the VM instances (sorted by zone):

gcloud compute instances list --sort-by=ZONE



4. In the Cloud console, in the **Navigation menu** () , click **Compute Engine > VM instances**.
Verify that the VM instances are listed in the Cloud console.



5. For **Columns**, select **Network**.

There are three instances in the US and one instance that is not in the US. These instances are spread across three VPC networks (**managementnet**, **mynet**, and **privatenet**), with no instance in the same zone and network as another. In the next task, you explore the effect this has on internal connectivity.

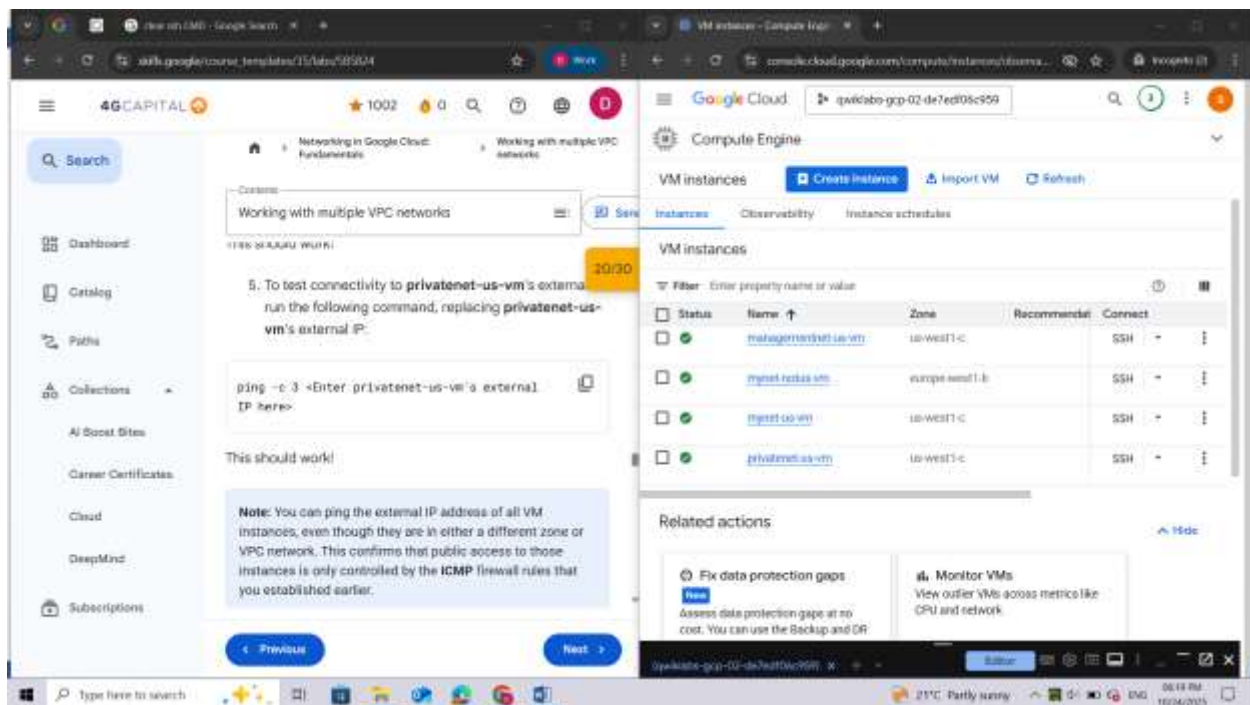
Task 3. Explore the connectivity between VM instances

Explore the connectivity between the VM instances. Specifically, determine the effect of having VM instances in the same zone versus having instances in the same VPC network.

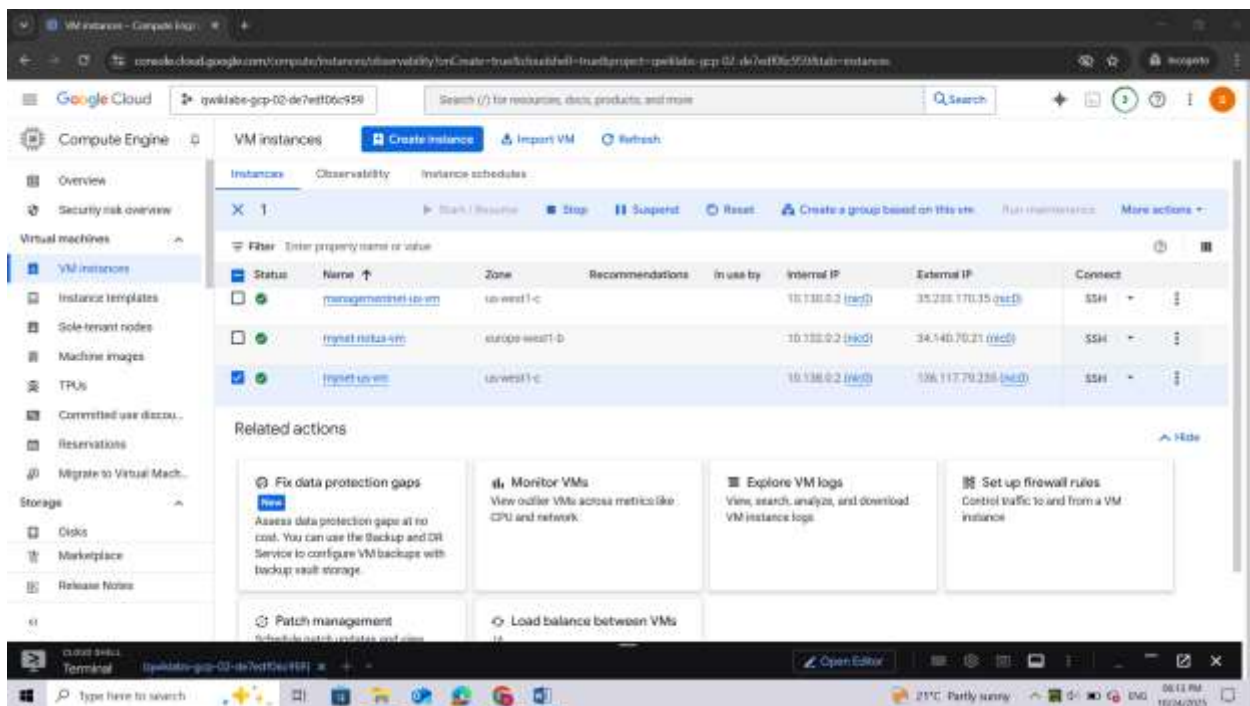
Ping the external IP addresses

Ping the external IP addresses of the VM instances to determine whether you can reach the instances from the public internet.

1. In the Cloud console, in the **Navigation menu**, click **Compute Engine > VM instances**. Note the external IP addresses for **mynet-notus-vm**, **managementnet-us-vm**, and **privatenet-us-vm**.



2. For **myinet-us-vm**, click **SSH** to launch a terminal and connect.



3. To test connectivity to **myinet-notus-vm**'s external IP, run the following command, replacing **myinet-notus-vm**'s external IP:

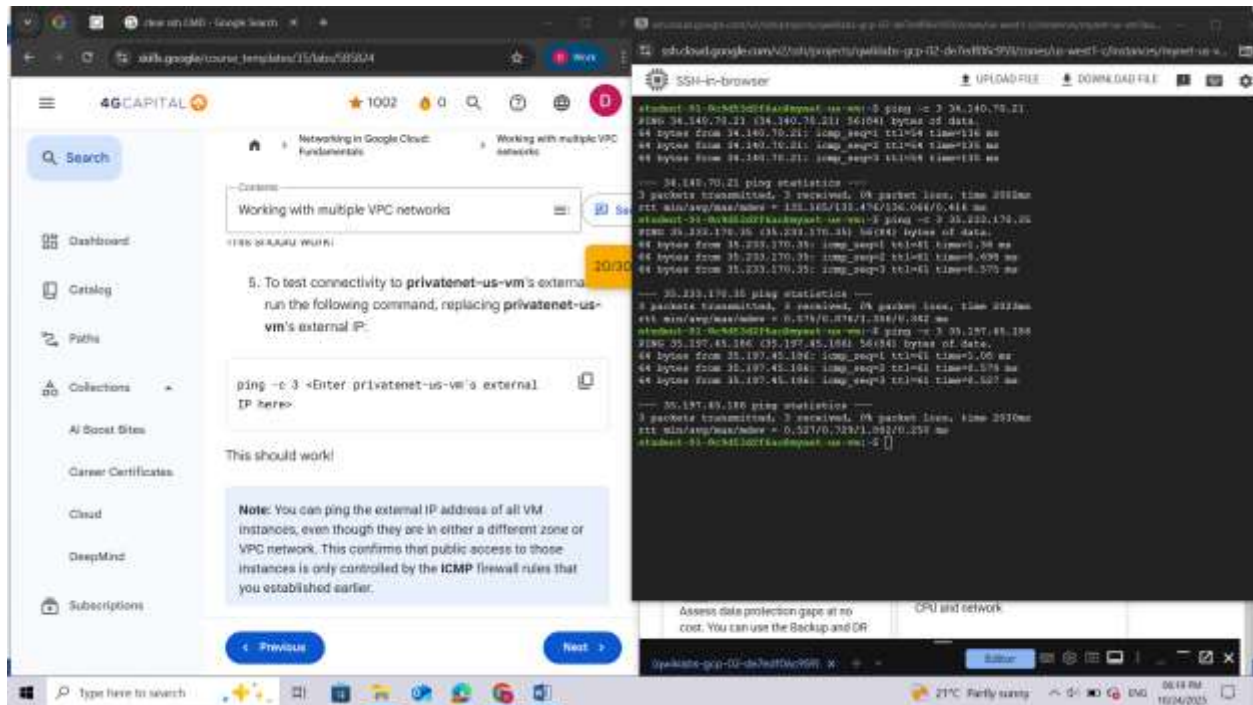
`ping -c 3 <Enter myinet-notus-vm's external IP here>`

- To test connectivity to **managementnet-us-vm**'s external IP, run the following command, replacing **managementnet-us-vm**'s external IP:

ping -c 3 <Enter managementnet-us-vm's external IP here>

- To test connectivity to **privatenet-us-vm**'s external IP, run the following command, replacing **privatenet-us-vm**'s external IP:

ping -c 3 <Enter privatenet-us-vm's external IP here>



Note: You can ping the external IP address of all VM instances, even though they are in either a different zone or VPC network. This confirms that public access to those instances is only controlled by the **ICMP** firewall rules that you established earlier.

Ping the internal IP addresses

Ping the internal IP addresses of the VM instances to determine whether you can reach the instances from within a VPC network.

Which instance(s) should you be able to ping from mynet-us-vm using internal IP addresses?

☐

managementnet-us-vm

☒

mynet-notus-vm

☐

privatenet-us-vm

1. In the Cloud console, in the **Navigation menu**, click **Compute Engine > VM instances**.
Note the internal IP addresses for **mynet-notus-vm**, **managementnet-us-vm**, and **privatenet-us-vm**.
2. Return to the **SSH** terminal for **mynet-us-vm**.
3. To test connectivity to **mynet-notus-vm**'s internal IP, run the following command, replacing **mynet-notus-vm**'s internal IP:

ping -c 3 <Enter mynet-notus-vm's internal IP here>

Note: You can ping the internal IP address of **mynet-notus-vm** because it is on the same VPC network as the source of the ping (**mynet-us-vm**), even though both VM instances are in separate zones, regions, and continents!

4. To test connectivity to **managementnet-us-vm**'s internal IP, run the following command, replacing **managementnet-us-vm**'s internal IP:

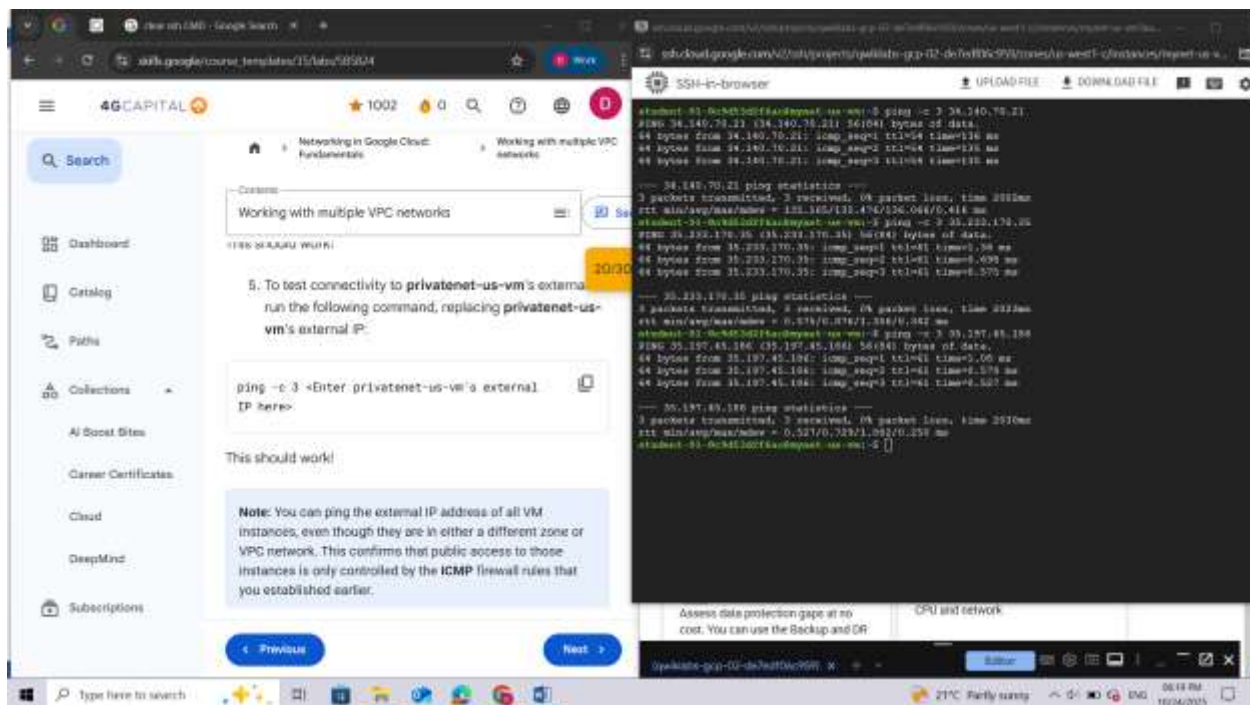
ping -c 3 <Enter managementnet-us-vm's internal IP here>

Note: This should not work, as indicated by a 100% packet loss!

5. To test connectivity to **privatenet-us-vm**'s internal IP, run the following command, replacing **privatenet-us-vm**'s internal IP:

ping -c 3 <Enter privatenet-us-vm's internal IP here>

Note: This should not work either, as indicated by a 100% packet loss! You cannot ping the internal IP address of **managementnet-us-vm** and **privatenet-us-vm** because they are in separate VPC networks from the source of the ping (**mynet-us-vm**), even though they are all in the same zone.



VPC networks are by default isolated private networking domains. However, no internal IP address communication is allowed between networks, unless you set up mechanisms such as VPC peering or VPN.

Task 4. Create a VM instance with multiple network interfaces

Every instance in a VPC network has a default network interface. You can create additional network interfaces attached to your VMs. Multiple network interfaces enable you to create configurations in which an instance connects directly to several VPC networks (up to 8 interfaces, depending on the instance's type).

Create the VM instance with multiple network interfaces

Create the **vm-appliance** instance with network interfaces in **privatesubnet-us**, **managementsubnet-us**, and **mynetwork**. The CIDR ranges of these subnets do not overlap, which is a requirement for creating a VM with multiple network interface controllers (NICs).

1. In the Cloud console, in the **Navigation menu**, click **Compute Engine > VM instances**.
2. Click **Create instance**.
3. Specify the following, and leave the remaining settings as their defaults:

Property	Value (type value or select option as specified)
Name	vm-appliance
Region	<filled at lab start>

Zone	<filled at lab start>
------	-----------------------

qwiklabs-gcp-02-de7edf06c959
7

[← Create an instance](#)
[Create VM from...](#)
[Equivalent code](#)

- Machine configuration**
e2-standard-4, us-west1-c
- OS and storage
Debian GNU/Linux 12 (bookworm)
- Data protection
Snapshot schedules
- Networking
1 network interface
- Observability
Install Ops Agent

Machine configuration

Name *
vm-appliance

Region *
us-west1 (Oregon) ?

Zone *
us-west1-c ?

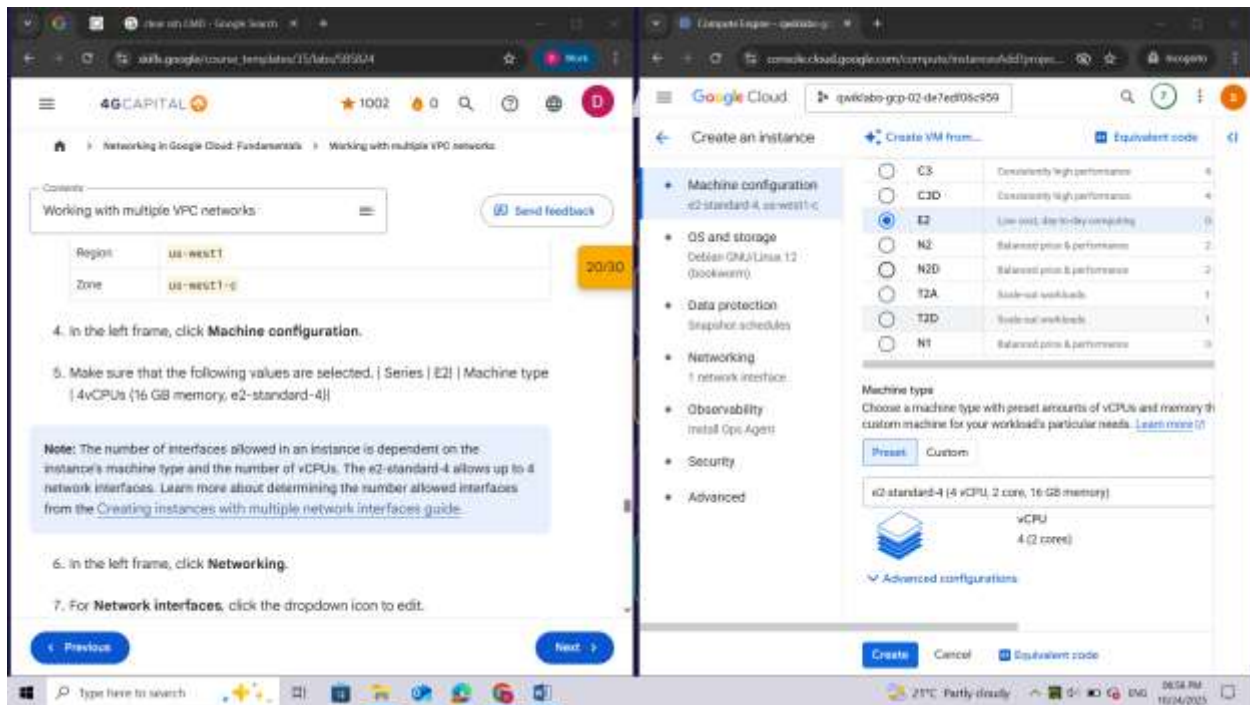
Region is permanent Zone is permanent

☒ General purpose
 ☐ Compute optimized
 ☐ Memory optimized
 ☐ Storage optimized

Machine types for common workloads, optimized for cost and flexibility

Series ?	Description	VM size
<input type="radio"/> C4	Consistently high performance	2 vCPUs (8 GB memory)
<input type="radio"/> E2	Cost-optimized	2 vCPUs (16 GB memory)

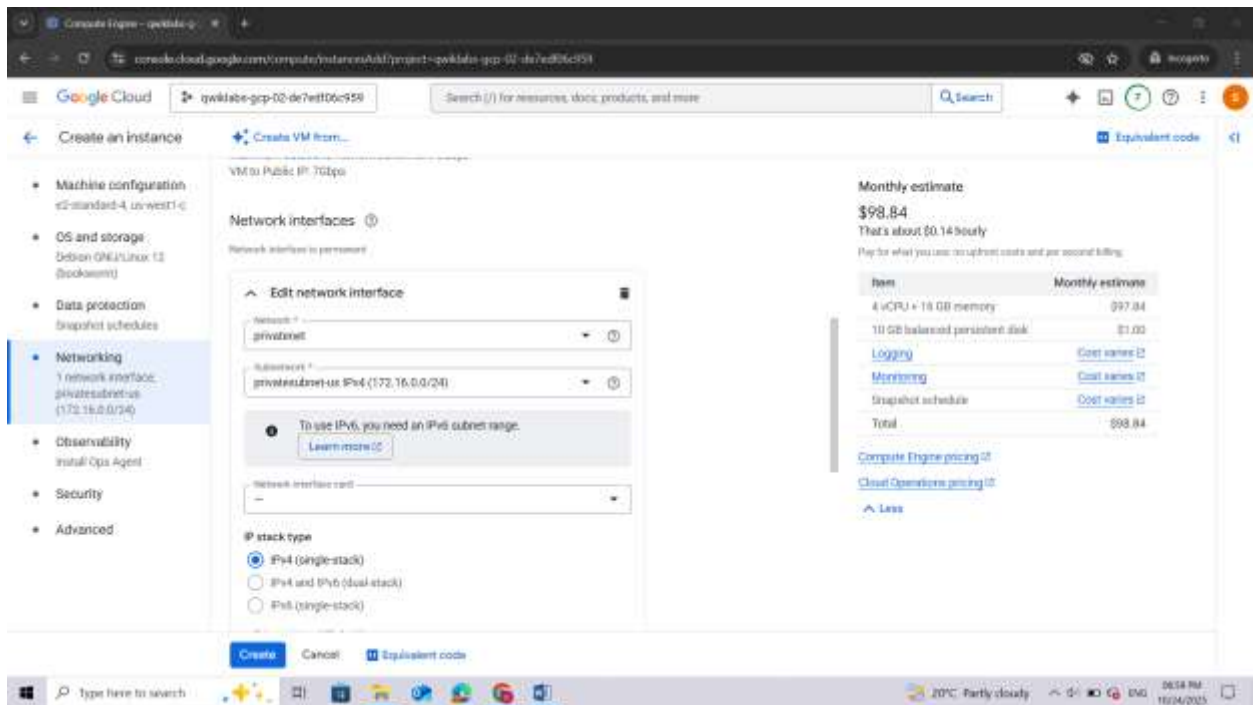
- In the left frame, click **Machine configuration**.
- Make sure that the following values are selected. | Series | E2 | | Machine type | 4vCPUs (16 GB memory, e2-standard-4) |



Note: The number of interfaces allowed in an instance is dependent on the instance's machine type and the number of vCPUs. The e2-standard-4 allows up to 4 network interfaces. Learn more about determining the number allowed interfaces from the [Creating instances with multiple network interfaces guide](#).

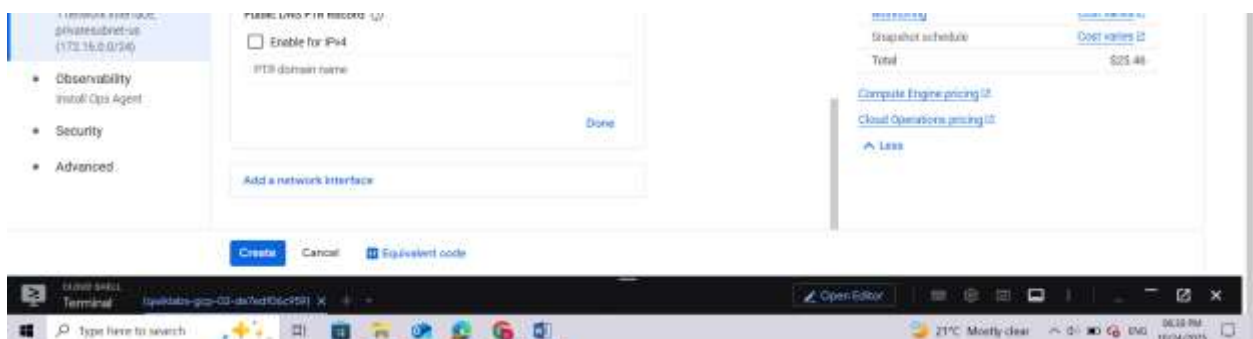
6. In the left frame, click **Networking**.
7. For **Network interfaces**, click the dropdown icon to edit.
8. Specify the following, and leave the remaining settings as their defaults:

Property	Value (type value or select option as specified)
Network	privatenet
Subnetwork	privatesubnet-us



9. Click **Done**.

10. Click **Add a network interface**.



11. Specify the following, and leave the remaining settings as their defaults:

Property	Value (type value or select option as specified)
Network	managementnet
Subnetwork	managementsubnet-us

12. Click **Done**.

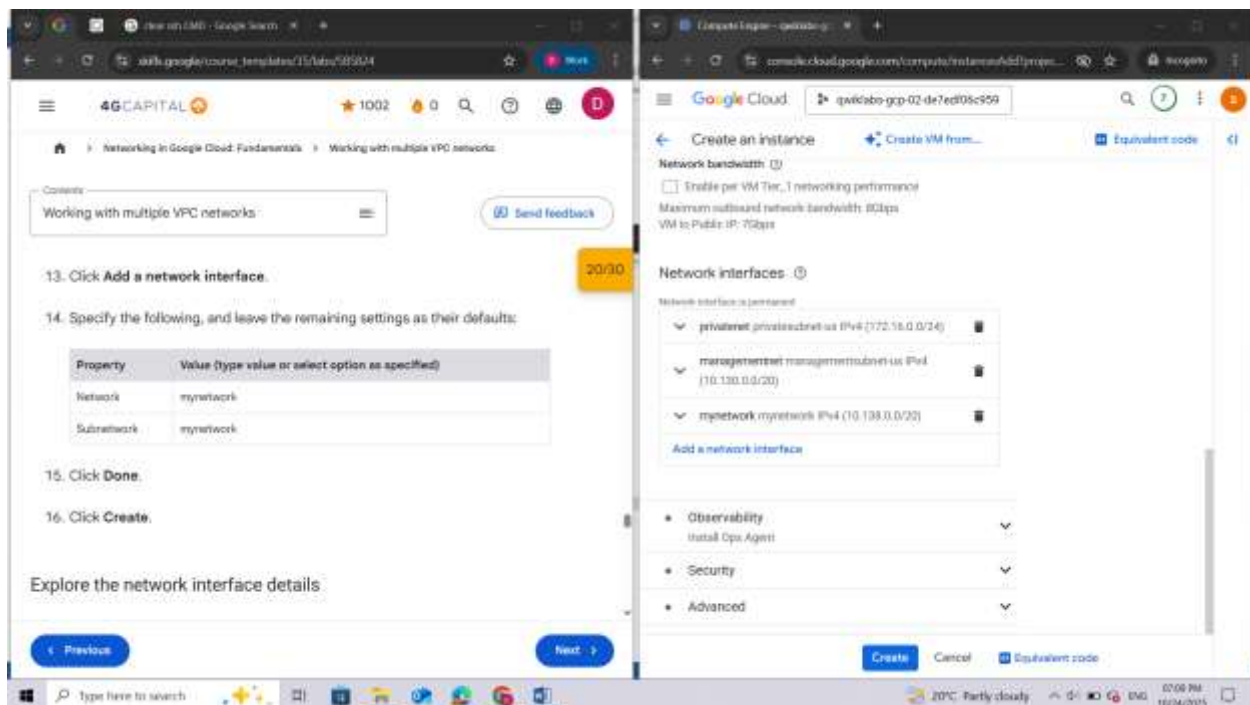
13. Click **Add a network interface**.

14. Specify the following, and leave the remaining settings as their defaults:

Property	Value (type value or select option as specified)
Network	mynetwork
Subnetwork	mynetwork

15. Click **Done**.

16. Click **Create**.



Explore the network interface details

Explore the network interface details of **vm-appliance** within the Cloud console and within the VM's terminal.

1. In the Cloud console, in the **Navigation menu**, click **Compute Engine > VM instances**.
2. To open the **Network interface details** page, in the **Internal IP** address of **vm-appliance**, click **nic0**.
3. Verify that **nic0** is attached to **privatesubnet-us**, is assigned an internal IP address within that subnet (172.16.0.0/24), and has applicable firewall rules.

The screenshot shows the Google Cloud console's 'Network interface details' page for the interface 'nic0'. The left sidebar lists various VPC network components. The main content area displays details for the selected network interface, including its name, network, subnetwork, primary internal IP address, and associated VM instance details. Below this, the 'Firewall and routes details' section shows a list of firewall rules.

Network interface details

Name	Network	Subnetwork	Primary internal IP address	Alias IP ranges	IP stack type	External IP address	Network Service Tier
nic0	privatenet	privatesubnet-us	172.16.0.4	—	IPv4	34.137.19.82	Premium

VM instance details

Name	Zone	Network tags	Service account	IP forwarding
vm-appliance	us-west1-c	None	275665775667-compute@developer.gserviceaccount.com	Off

Firewall and routes details

Filter: Enter property name or value

Name	Enforcement order	Type	Deployment scope	Rule priority	Source	Destination	Protocols and ports	Action
firewall	1	Hierarchical firewall policy	Global					
vpc firewall rules	2	VPC firewall rules	Global					

4. Click **nic0** and select **nic1**.

5. Verify that **nic1** is attached to **managementsubnet-us**, is assigned an internal IP address within that subnet (10.130.0.0/20), and has applicable firewall rules.

The screenshot shows the Google Cloud console's 'Network interface details' page for the interface 'nic1'. The left sidebar lists various VPC network components. The main content area displays details for the selected network interface, including its name, network, subnetwork, primary internal IP address, and associated VM instance details. Below this, the 'Firewall and routes details' section shows a list of firewall rules.

Network interface details

Name	Network	Subnetwork	Primary internal IP address	Alias IP ranges	IP stack type	External IP address	Network Service Tier
nic1	managenetnet	managementsubnet-us	10.130.0.3	—	IPv4	35.185.187.156	Premium

VM instance details

Name	Zone	Network tags	Service account	IP forwarding
vm-appliance	us-west1-c	None	275665775667-compute@developer.gserviceaccount.com	Off

Firewall and routes details

Filter: Enter property name or value

Name	Enforcement order	Type	Deployment scope	Rule priority	Source	Destination	Protocols and ports	Action
firewall	1	Hierarchical firewall policy	Global					
vpc firewall rules	2	VPC firewall rules	Global					

6. Click **nic1** and select **nic2**.

7. Verify that **nic2** is attached to **mynetwork**, is assigned an internal IP address within that subnet (10.128.0.0/20), and has applicable firewall rules. The subnet shown may differ depending on the region selected during VM creation.

The screenshot shows the Google Cloud console interface for the 'Network interface details' of a VM instance named 'vm-appliance'. The selected network interface is 'nic2'. The page displays the following details:

Network interface details

Name	Network	Subnetwork	Primary internal IP address	Alias IP ranges	IP stack type	External IP address	Network Service Tier
nic2	mynetwork	mynetwork	10.128.0.4	—	IPv4	34.160.82.52	Premium

VM instance details

Name	Zone	Network tag	Service account	IP forwarding
vm-appliance	us-west1-c	None	275865775867-compute@developer.gserviceaccount.com	Off

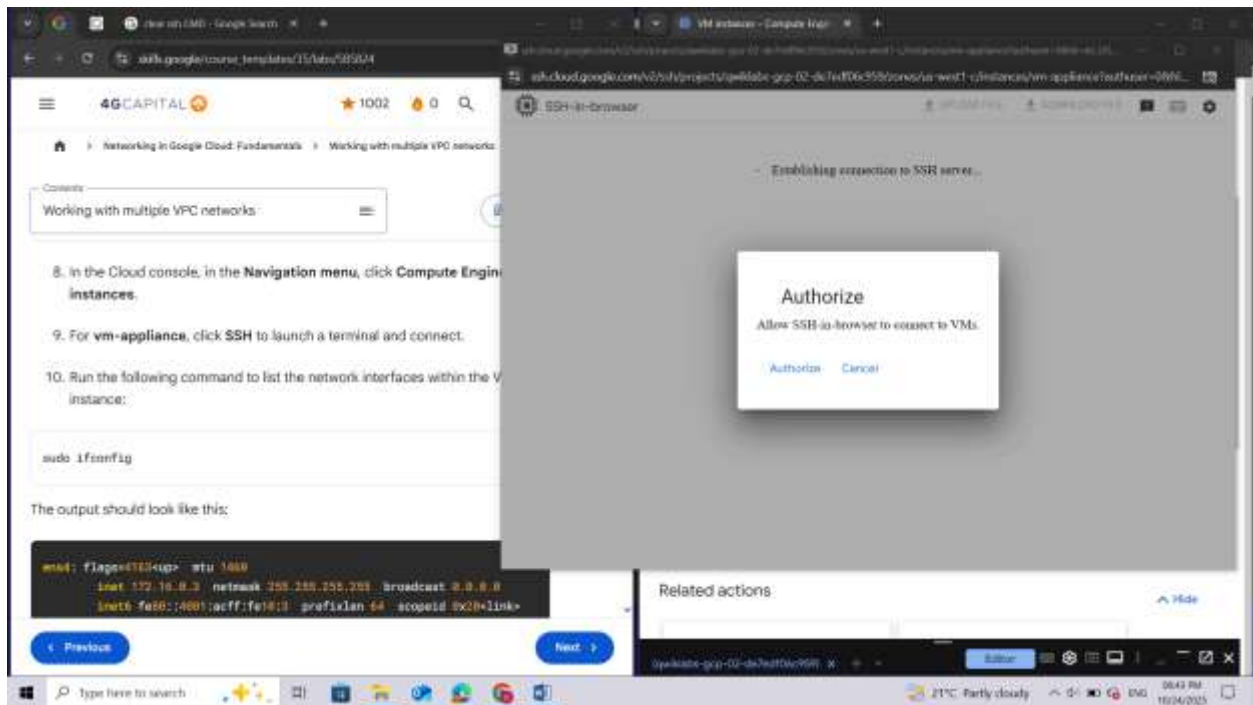
Firewall and routes details

Filter: Enter property name or value

Name	Enforcement order	Type	Deployment scope	Rule priority	Source	Destination	Protocols and ports	Action
firewall	1	Hierarchical firewall policy	Global					
vpc-firewall-rules	2	VPC firewall rules	Global					

Note: Each network interface has its own internal IP address so that the VM instance can communicate with those networks.

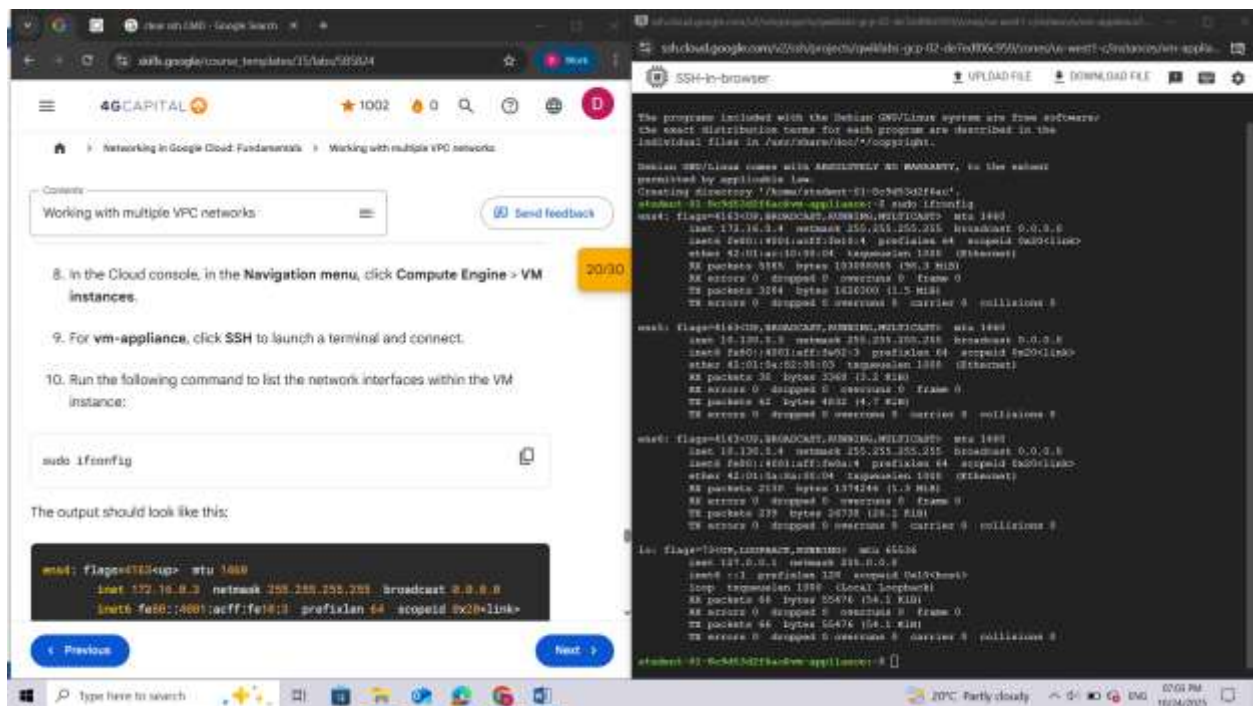
8. In the Cloud console, in the **Navigation menu**, click **Compute Engine > VM instances**.
9. For **vm-appliance**, click **SSH** to launch a terminal and connect.



10. Run the following command to list the network interfaces within the VM instance:

`sudo ifconfig`

Note: The `sudo ifconfig` command lists a Linux VM's network interfaces with the internal IP addresses for each interface.



Explore the network interface connectivity

Demonstrate that the **vm-appliance** instance is connected to **privatesubnet-us**, **managementsubnet-us**, and **mynetwork** by pinging VM instances on those subnets.

Which instance(s) should you be able to ping from vm-appliance using internal IP addresses?

☐

mynet-notus-vm

☒

mynet-us-vm

☒

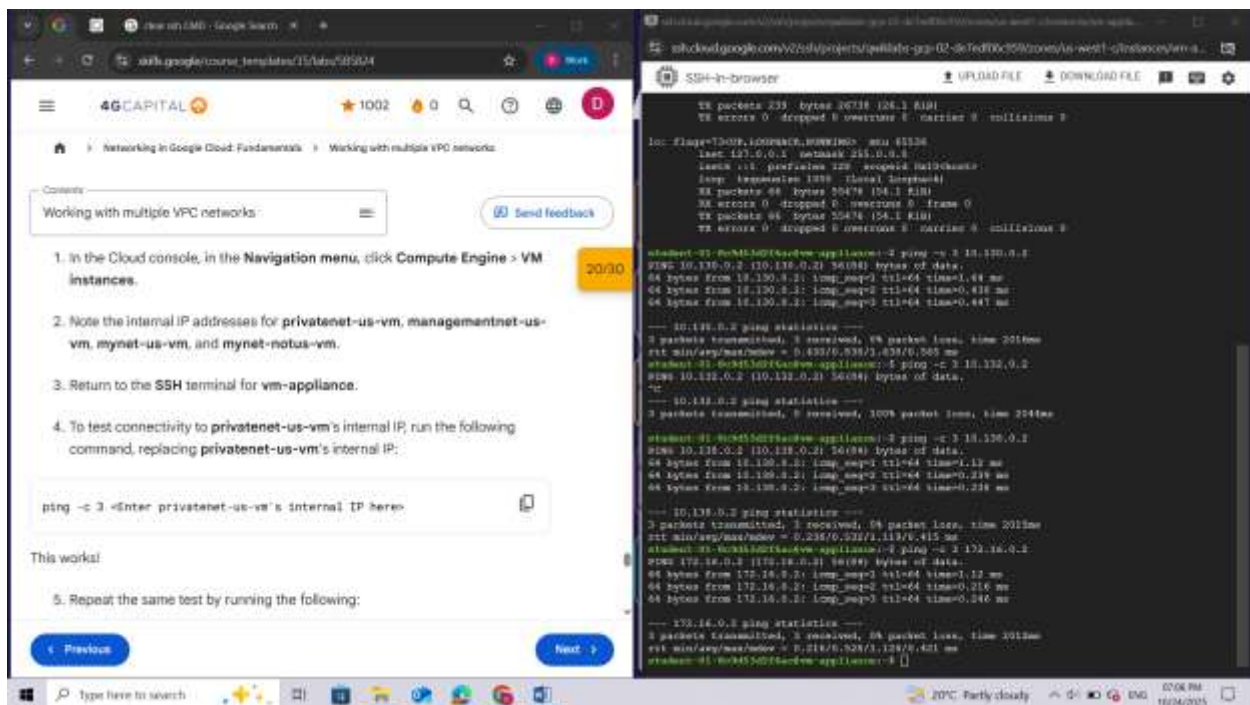
privatenet-us-vm

☒

managementnet-us-vm

1. In the Cloud console, in the **Navigation menu**, click **Compute Engine > VM instances**.
2. Note the internal IP addresses for **privatenet-us-vm**, **managementnet-us-vm**, **mynet-us-vm**, and **mynet-notus-vm**.
3. Return to the **SSH** terminal for **vm-appliance**.
4. To test connectivity to **privatenet-us-vm**'s internal IP, run the following command, replacing **privatenet-us-vm**'s internal IP:

ping -c 3 <Enter privatenet-us-vm's internal IP here>



5. Repeat the same test by running the following:

`ping -c 3 privatenet-us-vm`

Note: You can ping **privatenet-us-vm** by its name because VPC networks have an internal DNS service that allows you to address instances by their DNS names instead of their internal IP addresses. When an internal DNS query is made with the instance hostname, it resolves to the primary interface (nic0) of the instance. Therefore, this only works for **privatenet-us-vm** in this case.

```
student-01-8c9d53d2f6ac@vm-appliance:~$ ping -c 3 privatenet-us-vm
PING privatenet-us-vm.us-west1-c.c.qwiklabs-gcp-02-de7edf06c959.internal (172.16.0.2) 56(84)
bytes of data.
64 bytes from privatenet-us-vm.us-west1-c.c.qwiklabs-gcp-02-de7edf06c959.internal (172.16.0.
2): icmp_seq=1 ttl=64 time=0.924 ms
64 bytes from privatenet-us-vm.us-west1-c.c.qwiklabs-gcp-02-de7edf06c959.internal (172.16.0.
2): icmp_seq=2 ttl=64 time=0.237 ms
64 bytes from privatenet-us-vm.us-west1-c.c.qwiklabs-gcp-02-de7edf06c959.internal (172.16.0.
2): icmp_seq=3 ttl=64 time=0.304 ms
--- privatenet-us-vm.us-west1-c.c.qwiklabs-gcp-02-de7edf06c959.internal ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 0.237/0.528/1.139/0.403 ms
student-01-8c9d53d2f6ac@vm-appliance:~$
```

6. To test connectivity to **managementnet-us-vm**'s internal IP, run the following command, replacing **managementnet-us-vm**'s internal IP:

`ping -c 3 <Enter managementnet-us-vm's internal IP here>`

7. To test connectivity to **myynet-us-vm**'s internal IP, run the following command, replacing **myynet-us-vm**'s internal IP:

`ping -c 3 <Enter myynet-us-vm's internal IP here>`

- To test connectivity to **mynet-notus-vm**'s internal IP, run the following command, replacing **mynet-notus-vm**'s internal IP:

ping -c 3 <Enter mynet-notus-vm's internal IP here>

Note: This does not work! In a multiple interface instance, every interface gets a route for the subnet that it is in. In addition, the instance gets a single default route that is associated with the primary interface **ens4**. Unless manually configured otherwise, any traffic leaving an instance for any destination other than a directly connected subnet will leave the instance via the default route on **ens4**.

- To list the routes for **vm-appliance** instance, run the following command:

ip route

```
student-01-8c9d53d2f6ac@vm-appliance:~$ ip route
default via 172.16.0.1 dev ens4 proto dhcp src 172.16.0.4 metric 100
10.130.0.0/20 via 10.130.0.1 dev ens5 proto dhcp src 10.130.0.3 metric 100
10.130.0.1 dev ens5 proto dhcp scope link src 10.130.0.3 metric 100
10.138.0.0/20 via 10.138.0.1 dev ens6 proto dhcp src 10.138.0.4 metric 100
10.138.0.1 dev ens6 proto dhcp scope link src 10.138.0.4 metric 100
169.254.169.254 via 172.16.0.1 dev ens4 proto dhcp src 172.16.0.4 metric 100
172.16.0.0/24 via 172.16.0.1 dev ens4 proto dhcp src 172.16.0.4 metric 100
172.16.0.1 dev ens4 proto dhcp scope link src 172.16.0.4 metric 100
student-01-8c9d53d2f6ac@vm-appliance:~$
```

Note: The primary interface **ens4** gets the default route (default via 172.16.0.1 dev ens4), and all three interfaces, **ens4**, **ens5**, and **ens6**, get routes for their respective subnets. Because the subnet of **mynet-notus-vm** (10.132.0.0/20) is not included in this routing table, the ping to that instance leaves **vm-appliance** on **ens4** (which is on a different VPC network).

Learn more about how you can change this behavior by configuring policy routing from the [Creating instances with multiple network interfaces guide](#).

Review

In this lab, you created several custom mode VPC networks, firewall rules, and VM instances using the Cloud console and the gcloud command line. Then you tested the connectivity across VPC networks, which worked when pinging external IP addresses but not when pinging internal IP addresses. Thus you created a VM instance with three network interfaces and verified internal connectivity for VM instances that are on the subnets that are attached to the multiple interface VM.

End your lab

When you have completed your lab, click **End Lab**. Google Cloud Skills Boost removes the resources you've used and cleans the account for you.

4G CAPITAL

What do you want to learn today?

10020

Work

Search

DashboardCatalogPathsCollectionsAI Boost BitesCareer CertificatesCloudDeepMindSubscriptions

Contents

Working with multiple VPC networks

End Lab00:09:16

Caution: When you are in the console, do not deviate from the lab instructions. Doing so may cause your account to be blocked.
Learn more

Open Google Cloud console

Usernamestudent-81-8c9d332f6ac

PassworduvFiv#D5k4ZI

Project IDqwklaba-gcp-62-de7edf8c

PreviousNext

On stars, type a comment, and then click **Submit**.

The number of stars indicates the following:

- 1 star = Very dissatisfied
- 2 stars = Dissatisfied
- 3 stars = Neutral
- 4 stars = Satisfied
- 5 stars = Very satisfied

You can close the dialog box if you don't want to provide feedback.

For feedback, suggestions, or corrections, please use the **Support** tab.

Copyright 2022 Google LLC. All rights reserved. Google and the Google logo are trademarks of Google LLC. All other company and product names may be trademarks of the respective companies with which they are associated.

Lab instructions and tasks30/30

Overview

Setup and requirements

Task 1. Create custom vshard VPC networks with firewall rules

Task 2. Create VM instances

Task 3. Explore the connectivity between VM instances

Task 4. Create a VM instance with multiple

Type here to search

20°C Partly cloudy

07:08 PM16/04/2025