

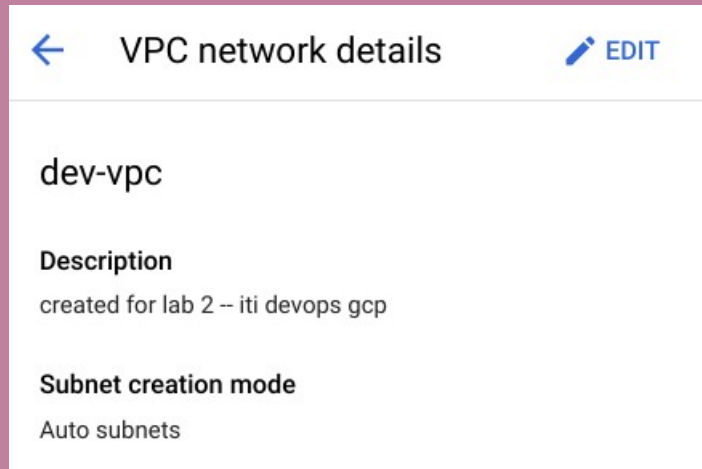
Name: Hadi Lotfy
Host: Andrew Anter
Project Name: hadi-lotfy-project
Project Number: 96418353483
Project ID: hadi-lotfy-project




Lab2

1. Create a VPC with the automatic mode called "dev-vpc" and another one called "prod-vpc" with 2 subnets:
 - subneta => region -> us-east1, cidr -> 10.1.0.0/16
 - subnetb => region -> asia-east1, cidr -> 192.168.1.0/24
 2. Can we edit the vpc subnets after the creation?
 3. Can you delete routes from "dev-vpc" region us-central1
 4. Create all required firewall rules to allow your localhost to ssh and curl all instances in subneta
 5. Block the internet reachability from dev-vpc
 6. Create instance "server-1" in subneta with automation, apache installation and home page with txt "Hello GCP, this is \$your_name"
 7. Create instance "server-2" in subnetb which can ping "server-1" but can access to the internet
- * note: all servers are linux based

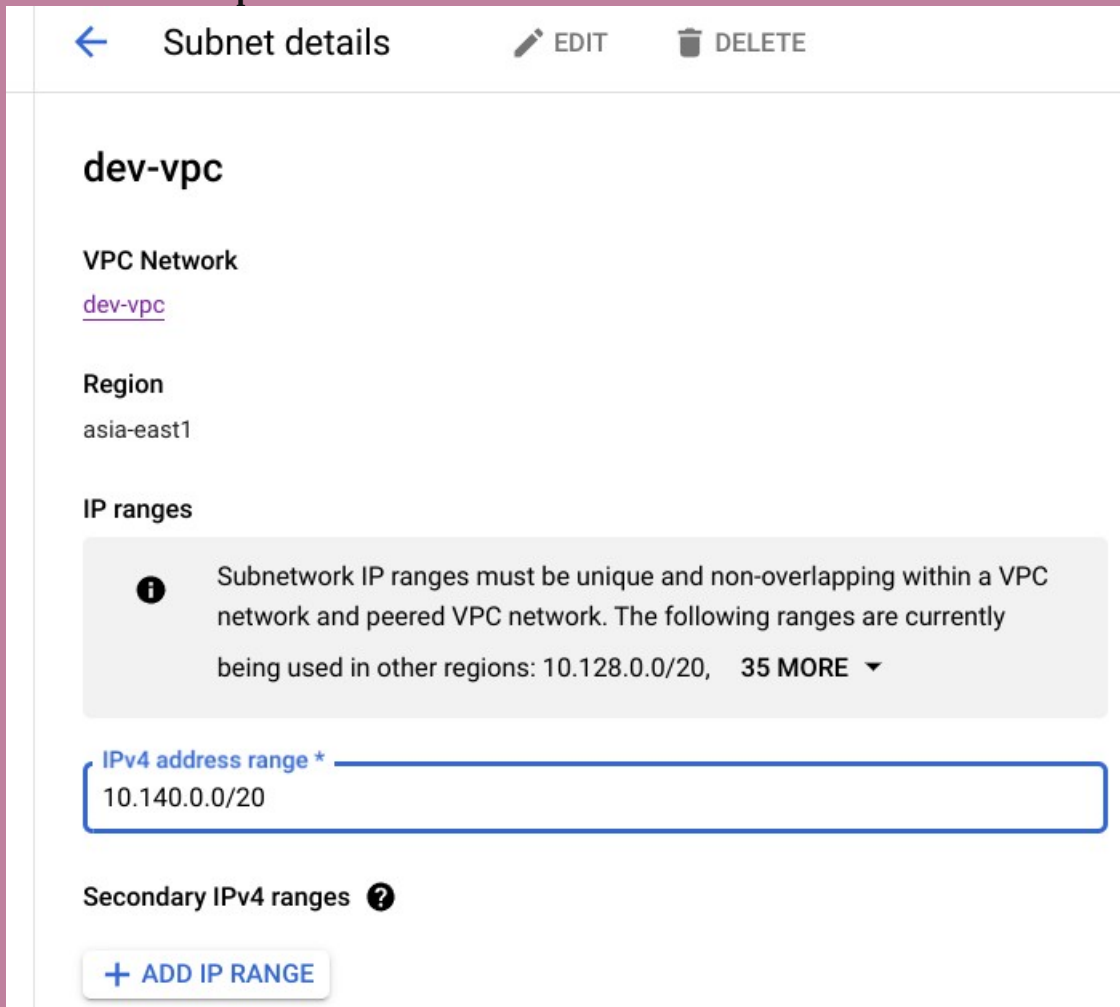
C2 General

q. what about region "us-east-7" that exists only in the default vpc subnets but cannot create a subnet there in my vpc ?

1. Create two VPCs**1. Create a VPC with the automatic mode called “dev-vpc”****2. and another one called “prod-vpc” with 2 subnets:****1. subnet-a ==> region (us-east1), CIDR (10.1.0.0/16)****2. subnet-b ==> region (asia-east1), CIDR (192.168.1.0/24)**

VPC networks							
 Filter Enter property name or value							
Name 	Subnets	MTU 	Mode	Internal IP ranges	Gateways	Firewall rules	Global dynamic routing
default	38	1460	Auto			4	Off
dev-vpc	37	1460	Auto			1	Off
prod-vpc	2	1460	Custom			1	Off

2. Can we edit the vpc subnets after creation ?



Subnet details EDIT DELETE

dev-vpc

VPC Network
[dev-vpc](#)

Region
asia-east1

IP ranges

i Subnetwork IP ranges must be unique and non-overlapping within a VPC network and peered VPC network. The following ranges are currently being used in other regions: 10.128.0.0/20, [35 MORE](#) ▼

IPv4 address range *

Secondary IPv4 ranges **?**

[+ ADD IP RANGE](#)

Yes we can edit it, but the name, vpc, and region cannot be changed (at least from the console)

3. Can you delete routes from “dev-vpc” region us-central1

I cannot delete subnet routes

(but can delete static routes freely that are children of the vpc not the subnet.)

4. Create all required firewall rules to allow your localhost to ssh and curl all instances in subnet-a.

The screenshot shows the 'Firewall rule details' page for a rule named 'subnet-a-ssh-http-https-allowance'. The rule is configured to allow SSH, HTTP, and HTTPS traffic to Subnet-A. The description is 'Allow SSH,HTTP(s) to Subnet-A'. The logs are turned off. The network is 'prod-vpc'. The priority is 1000. The direction is 'Ingress'. The action on match is 'Allow'. The source filters are set to '0.0.0.0/0' and the destination filters are set to '10.1.0.0/16'. The protocols and ports are 'tcp:22', 'tcp:80', and 'tcp:443'. The enforcement is 'Enabled' and the insights are 'None'.

Firewall rule details [EDIT](#)

subnet-a-ssh-http-https-allowance

Description
Allow SSH,HTTP(s) to Subnet-A

Logs [?](#)
Off
[view in Logs Explorer](#)

Network
prod-vpc

Priority
1000

Direction
Ingress

Action on match
Allow

Action on match
Allow

Source filters
IP ranges 0.0.0.0/0

Destination filters
IP ranges 10.1.0.0/16

Protocols and ports
tcp:22
tcp:80
tcp:443

Enforcement
Enabled

Insights
None

5. Block the internet reachability from dev-vpc using a firewall rule to block internet reachability.

The screenshot shows a list of firewall rules. The first rule is selected, with a checkbox checked. The rule name is 'block-internet-reachability'. The direction is 'Egress'. The action is 'Apply to all'. The IP ranges are '0.0.0.0/0'. The direction is 'all'. The action is 'Deny'. The priority is 1000. The network is 'dev-vpc'. The logs are 'Off'.

☒ [block-internet-reachability](#) Egress Apply to all IP ranges: 0.0.0.0/0 all Deny 1000 dev-vpc Off

Another way of doing so is by deleting the “default internet route from the vpc.

The screenshot shows the 'Route details' page for a route named 'default-route-204e3408ffb192ab'. The route is a static route to the Internet. The network is 'dev-vpc'. The route type is 'Static'. The IP version is 'IPv4'. The destination IP address range is '0.0.0.0/0'. A confirmation dialog is shown, asking if the user is sure they want to delete the route from all regions. The dialog has 'CANCEL' and 'DELETE' buttons.

Route details [DELETE](#)

default-route-204e3408ffb192ab

Description
Default route to the Internet.

Network
dev-vpc

Route type
Static

IP version
IPv4

Destination IP address range
0.0.0.0/0

Delete a route
Are you sure you want to delete route "default-route-204e3408ffb192ab" from all regions?
[CANCEL](#) [DELETE](#)

6. Create instance “server-1” in subnet-a with automation for apache installation and home page with txt “Hello GCP, this is “Hadi Lotfy”.

Automation

Startup script

```
#!/bin/bash
sudo yum install httpd -y
sudo bash -c 'echo "<h1>Hello GCP, This is Hadi Lotfy</h1>" >>
/var/www/html/index.html'
sudo systemctl enable --now httpd
```

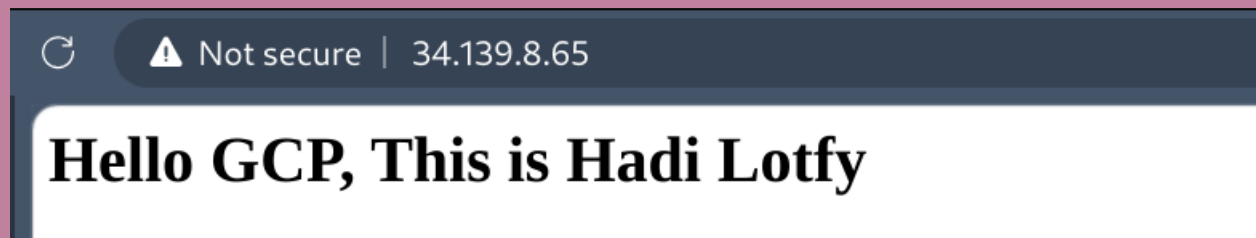
You can choose to specify a startup script that will run when your instance boots up or

lab-2-server-1 [EDIT](#) [RESET](#) [OPERATIONS](#) [HELP ASSISTANT](#) [LEARN](#)

DETAILS OBSERVABILITY OS INFO SCREENSHOT

Network interfaces

Internal IP address	Alias IP ranges	IP stack type	External IP address	Network tier	IP forwarding
2		IPv4	34.139.8.65 (Ephemeral)	Premium	Off



7. Create instance “server-2” in subnet-b which can ping “server-1” but can not access to the internet.

Filter Enter property name or value						
<input type="checkbox"/>	Status	Name ↑	Zone	Recommendations	In use by	Internal IP
<input type="checkbox"/>	✓	lab-2-server-1	us-east1-b			10.1.0.2 (nic0)
<input type="checkbox"/>	✓	lab-2-server-2	asia-east1-b			192.168.1.2 (nic0)

Fire wall rules to prevent internet access and to allow ping to subnet-a instances.

<input type="checkbox"/>	Name ↓	Enforcement order	Type	Deployment scope	Rule priority	Targets	Source	Destination	Protocols and ports	Action
<input type="checkbox"/>	vpc-firewall-rules	1	VPC firewall rules	Global						
<input type="checkbox"/>	subnet-b-deny-internet-access		Egress firewall rule	Global	1001	Apply to all	IPv4 ranges: 192.168.1.0/24	IPv4 ranges: 0.0.0.0/0	all	Deny
<input type="checkbox"/>	subnet-b-allow-ping-subnet-a		Egress firewall rule	Global	1000	Apply to all	IPv4 ranges: 192.168.1.0/24	IPv4 ranges: 10.1.0.0/16	icmp	Allow