

## Lab 2.1

From Cloud console, create a VPC named "auto-vpc" with auto-mode enabled,

34 subnets each with a /20 CIDR block.

Name ↑	Region	Subnets	MTU ?	Mode	Internal IP ranges	External IP ranges	Secondary
▶ auto-vpc		34	1460	Auto	None		
▶ default		34	1460	Auto	None		

How many subnets created? And how many routes created for this VPC? Can you delete any of these routes?

34 subnets each with a /20 CIDR block. 35 routes each with a /20 CIDR block. one of them is default for public access. no can't delete any of these routes.

From Cloud console, create a VPC named "custom-vpc" with auto-mode disabled and create two subnets. How many routes created for this VPC?

3 routes tables

Name ↑	Region	Subnets	MTU ?	Mode	Internal IP ranges	External IP ranges	Secondary
▶ auto-vpc		34	1460	Auto	None		
▼ custom-vpc		2	1460	Custom	None		
	us-east1	custom-vpc-n1			10.0.1.0/24	None	None
	asia-east2	custom-vpc-n2			10.0.2.0/24	None	None
▶ default		34	1460	Auto	None		

Using gcloud tool list all available VPCs and list subnets of each VPC.

```

mohamed@DevOps:~$ gcloud compute networks list
NAME          SUBNET_MODE  BGP_ROUTING_MODE  IPV4_RANGE  GATEWAY_IPV4  FLAGS
auto-vpc      AUTO        config            REGIONAL
custom-vpc    CUSTOM      config            REGIONAL
default       AUTO        config            REGIONAL

mohamed@DevOps:~$ gcloud compute networks subnets list
NAME          NETWORK  SUBNET_MODE  IPV4_RANGE  GATEWAY_IPV4  FLAGS
auto-vpc      auto-vpc  config       10.0.0.0/24  10.0.0.1
custom-vpc    custom-vpc  config       10.0.1.0/24  10.0.1.1
custom-vpc    custom-vpc  config       10.0.2.0/24  10.0.2.1
default       default    config       10.0.0.0/24  10.0.0.1

Argument NAME is deprecated. Use --filter="NAME"
--network = NETWORK
Only show subnetworks of a specific network

```

```

mohamed@DevOps:~$ gcloud compute networks subnets list --filter="custom-vpc"
NAME                REGION    NETWORK    RANGE        STACK_TYPE  IPV6_ACCESS_TYPE  INTERNAL_IPV6_PREFIX  EXTERNAL_I
custom-vpc-n1       us-east1  custom-vpc 10.0.1.0/24   IPV4_ONLY
custom-vpc-n2       asia-east2 custom-vpc 10.0.2.0/24   IPV4_ONLY

mohamed@DevOps:~$ gcloud compute networks subnets list --filter="auto-vpc"
NAME                REGION    NETWORK    RANGE        STACK_TYPE  IPV6_ACCESS_TYPE  INTERNAL_IPV6_PREFIX  EX
auto-vpc            us-central1  auto-vpc 10.128.0.0/20  IPV4_ONLY
auto-vpc            europe-west1  auto-vpc 10.132.0.0/20  IPV4_ONLY
auto-vpc            us-west1     auto-vpc 10.138.0.0/20  IPV4_ONLY
auto-vpc            asia-east1   auto-vpc 10.140.0.0/20  IPV4_ONLY
auto-vpc            us-east1     auto-vpc 10.142.0.0/20  IPV4_ONLY
auto-vpc            asia-northeast1 auto-vpc 10.146.0.0/20  IPV4_ONLY
auto-vpc            asia-southeast1 auto-vpc 10.148.0.0/20  IPV4_ONLY
auto-vpc            us-east4     auto-vpc 10.150.0.0/20  IPV4_ONLY
auto-vpc            australia-southeast1 auto-vpc 10.152.0.0/20  IPV4_ONLY
auto-vpc            europe-west2 auto-vpc 10.154.0.0/20  IPV4_ONLY
auto-vpc            europe-west3 auto-vpc 10.156.0.0/20  IPV4_ONLY
auto-vpc            southamerica-east1 auto-vpc 10.158.0.0/20  IPV4_ONLY
auto-vpc            asia-south1  auto-vpc 10.160.0.0/20  IPV4_ONLY

```

## In two different ways, How would you block internet access from you vpc?

By default, incoming traffic from outside your network is blocked create firewall rules to deny incoming traffic from outside

## Create a firewall rule to allow incoming SSH requests from internet to all instances in your vpc.

Filter Enter property name or value										
<input type="checkbox"/>	Name	Type	Targets	Filters	Protocols / ports	Action	Priority	Network ↑	Logs	Hit count
<input type="checkbox"/>	firewall-allow-in-ssh	Ingress	Apply to all	IP ranges	tcp:22	Allow	200	custom-vpc	Off	

## Modify the previous firewall rule to allow only ssh requests coming through Google

35.235.240.0/20. This range is the pool of IP addresses used by IAP

Filter Enter property name or value										
<input checked="" type="checkbox"/>	Name	Type	Targets	Filters	Protocols / ports	Action	Network ↑	Logs	Hit count	
<input checked="" type="checkbox"/>	firewall-allow-in-ssh	Ingress	Apply to all	IP ranges: 35.235.240.0/20	tcp:22	Allow	custom-vpc	Off		—

## lab 2.2

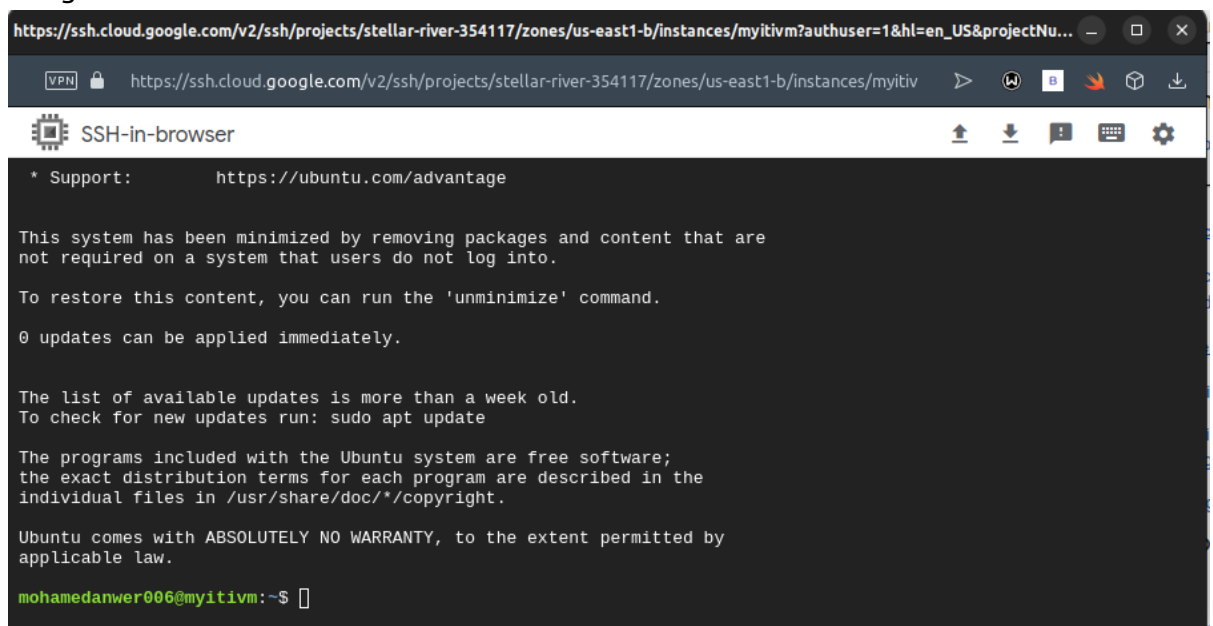
### Create a VM with public ip then:

VM instances are highly configurable virtual machines for running workloads on Google infrastructure. [Learn more](#)

**Filter** Enter property name or value

<input type="checkbox"/>	Status	Name ↑	Zone	Recommendations	Connect
<input type="checkbox"/>	✓	myitvm	us-east1-b		SSH ▾ ⋮

- In two different ways, SSH into this VM.
  - using web browser.



- using gcloud

gcloud will create a ssh key and add it to vm error happens because the firewall rule was set to allow only ssh from googl IAP range

```

mohamed@DevOps:~$ gcloud compute ssh --zone=us-east1-b "myitvm" --project="stellar-river-354117"
WARNING: The private SSH key file for gcloud does not exist.
WARNING: The public SSH key file for gcloud does not exist.
WARNING: You do not have an SSH key for gcloud.
WARNING: SSH keygen will be executed to generate a key.
Generating public/private rsa key pair.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/mohamed/.ssh/google_compute_engine
Your public key has been saved in /home/mohamed/.ssh/google_compute_engine.pub
The key fingerprint is:
SHA256:27klETSudo80c7L+9nJ/2LETuXZhL8m5kgTMTnuliQE mohamed@DevOps
The key's randomart image is:
+----[RSA 3072]----+
|
|
|
|
|
|
|
|
|
|
+----[SHA256]-----+
Updating project ssh metadata...Updated [https://www.googleapis.com/compute/v1/projects/stellar-river-354117].
Updating project ssh metadata...done.
Waiting for SSH key to propagate.
ssh: connect to host 34.73.138.3 port 22: Connection timed out
ERROR: (gcloud.compute.ssh) Could not SSH into the instance. It is possible that your SSH key has not propagated
ct, verify that the firewall and instance are set to accept ssh traffic.

```

### fix it

```

mohamed@DevOps:~$ gcloud compute ssh --zone=us-east1-b "myitvm" --project="stellar-river-354117"
Warning: Permanently added 'compute.1137526506727790836' (ED25519) to the list of known hosts.
Welcome to Ubuntu 22.04 LTS (GNU/Linux 5.15.0-1010-gcp x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

This system has been minimized by removing packages and content that are
not required on a system that users do not log into. To restore this content,
you can run the 'unminimize' command.

0 updates can be applied immediately.
The list of available updates is more than a week old.
To check for new updates run: sudo apt update

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
mohamed@myitvm:~$

```

- Enforce SSH into this VM to be IAP protected.

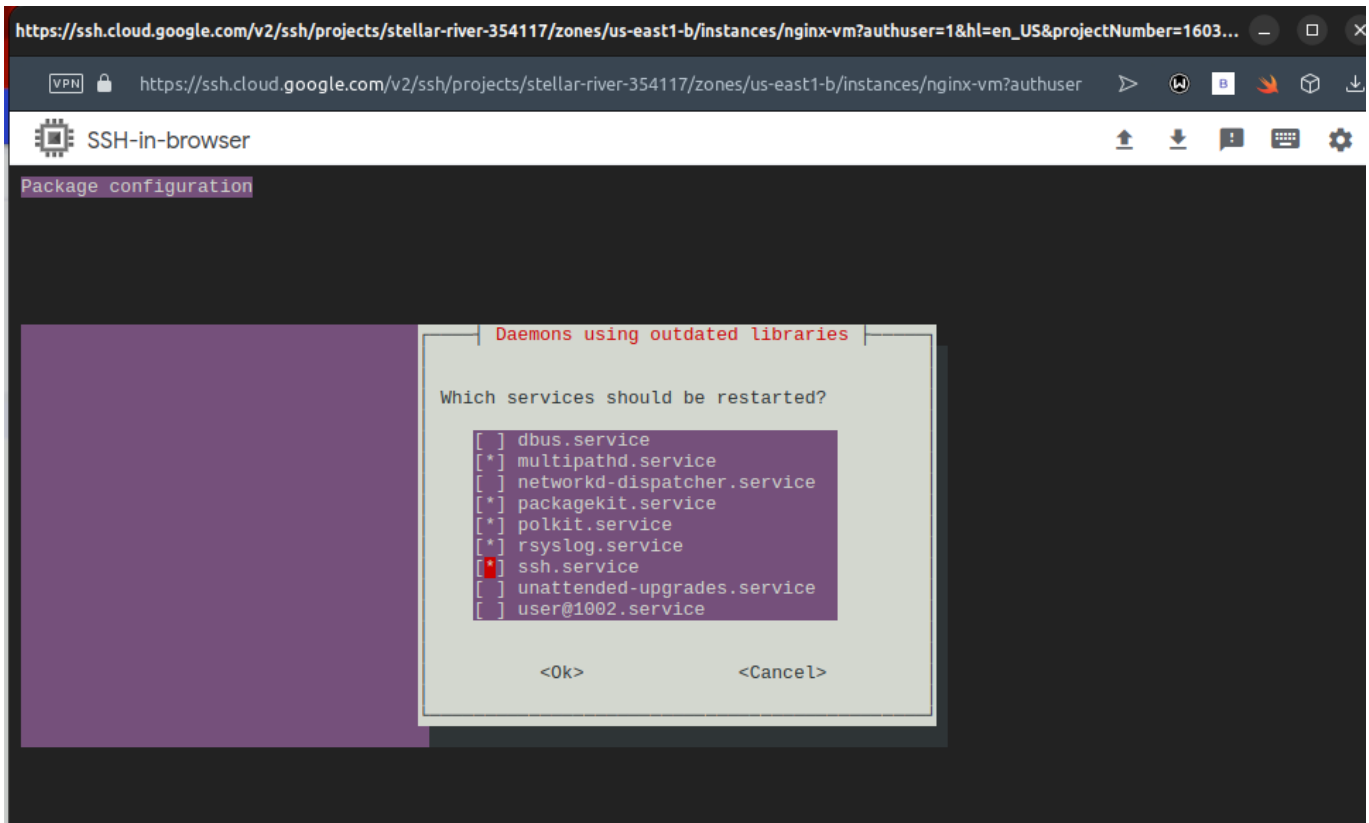
35.235.240.0/20. This range is the pool of IP addresses used by IAP

Filter Enter property name or value ?									
<input checked="" type="checkbox"/>	Name	Type	Targets	Filters	Protocols / ports	Action	Network ↑	Logs	Hit count ?
<input checked="" type="checkbox"/>	firewall-allow-in-ssh	Ingress	Apply to all	IP ranges: 35.23!	tcp:22	Allow	custom-vpc	Off	—

## Create a VM without public ip then:

- SSH into this vm and update system packages.

```
sudo apt update && sudo apt upgrade -y
```



- Setup Nginx Web Server and test your setup.

```
sudo apt install nginx -y
sudo systemctl enable --now nginx
```

changed the default page content and test it from browser.



- Create a custom image from this VM named "custom-img-nginx".

Machine images + CREATE MACHINE IMAGE REFRESH DELETE

A machine image contains a VM's properties, metadata, permissions, and data from all its attached disks. You can use a machine image to create, backup, or restore a VM. [Learn more](#)

**Filter** Enter property name or value

<input type="checkbox"/>	Status	Name ↑	Source instance	Machine type	Storage location	Creation time
<input type="checkbox"/>	✓	custom-img-nginx	nginx-vm	e2-small	us	Jun 23, 2022, 4:33:42 PM UTC+02:00