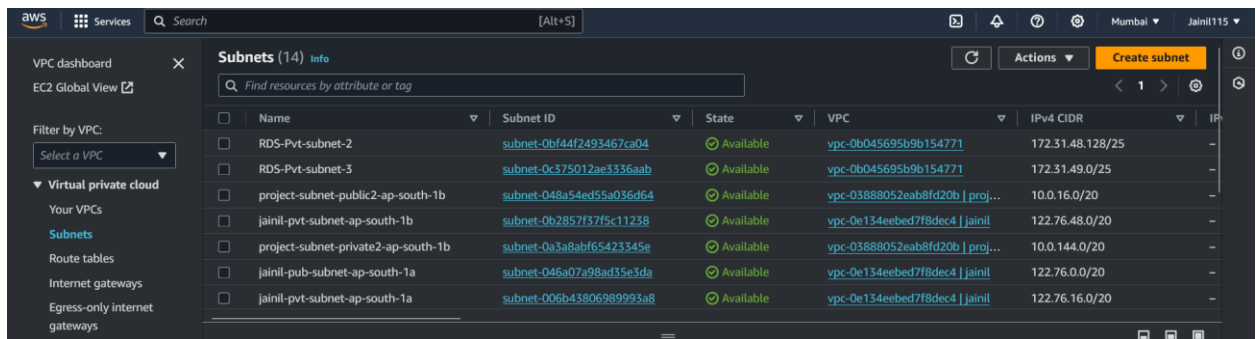


TASK 2: Subnet Configuration:

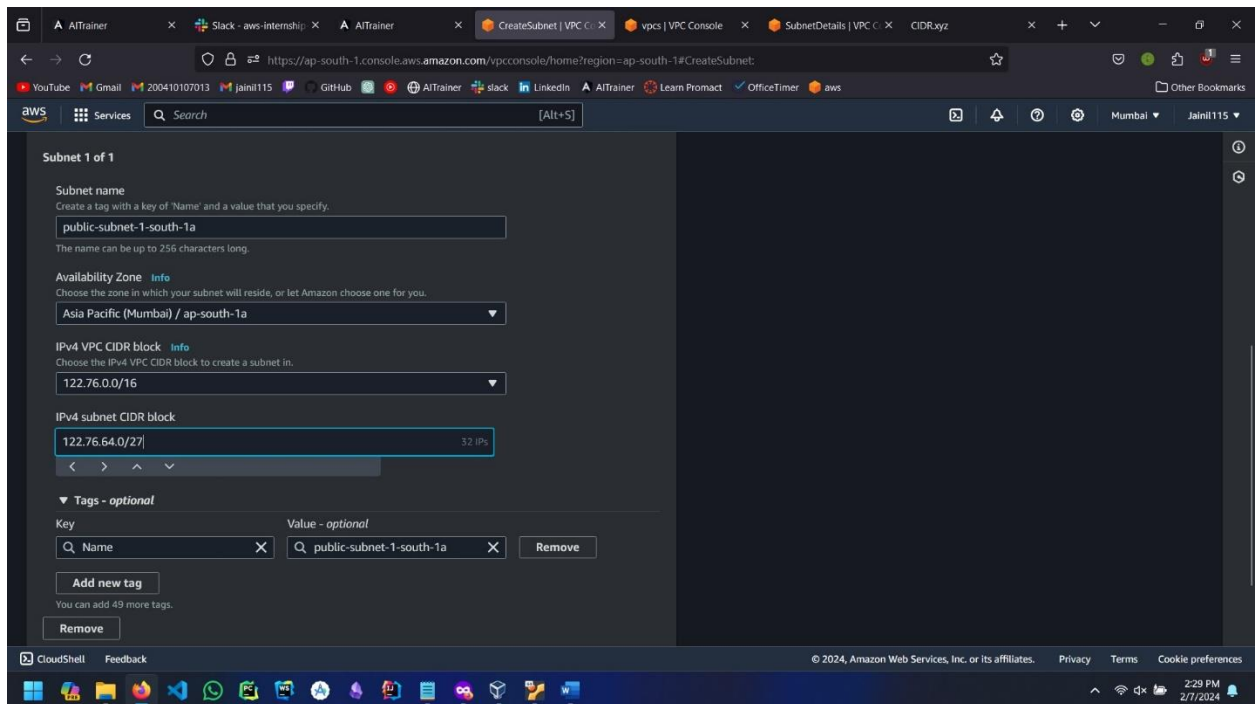
1. Configure one subnet as a public subnet and the other as a private subnet.
2. Launch an EC2 instance in each subnet. The EC2 instance in the public subnet should be reachable from the Internet.

We need to create 2 new subnets. Steps to create 2 new subnet:

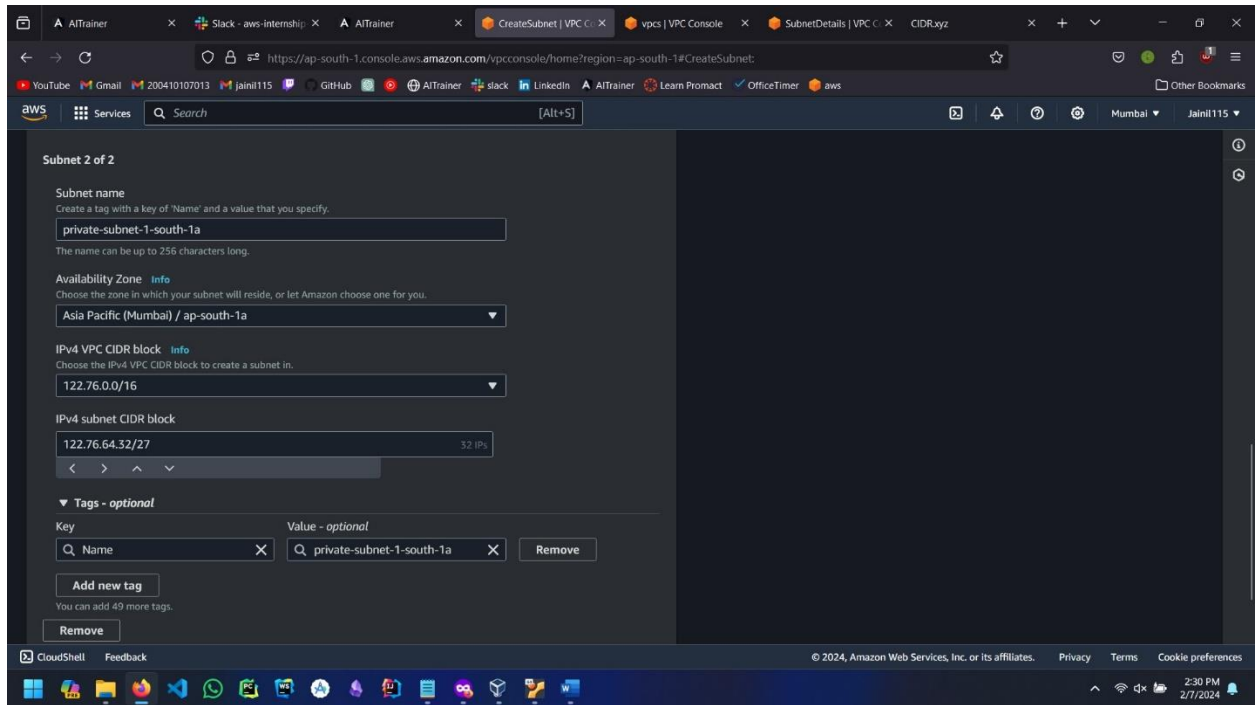
1. In VPC dashboard and click on Subnets. Then click on create subnet.



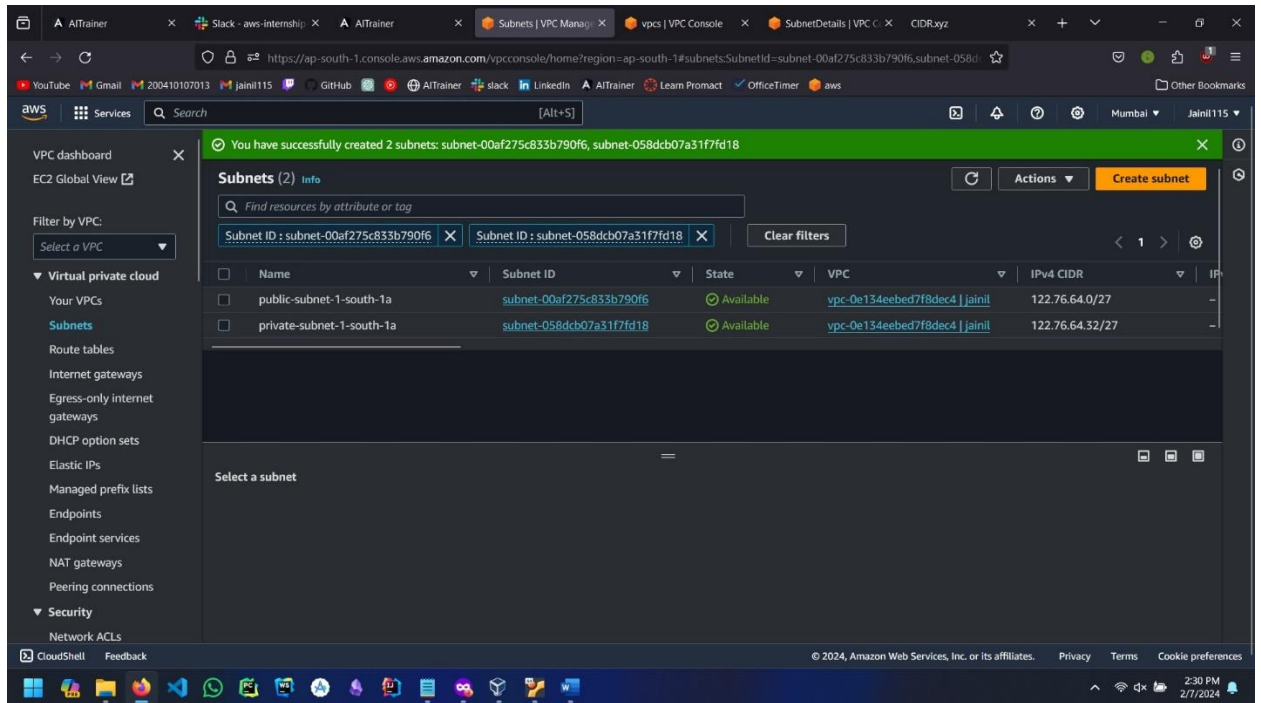
2. Under subnet setting fill out the following:
 - i. Subnet name: public-subnet-1-south-1a
 - ii. Availability zone: ap-south-1a
 - iii. IPv4 VPC CIDR block: 122.76.0.0/16
 - iv. IPv4 subnet CIDR block: 122.76.64.0/27



3. And then click on add subnet. And enter the following details in under subnet setting:
 - i. Subnet name: private-subnet-1-south-1a
 - ii. Availability zone: ap-south-1a
 - iii. IPv4 VPC CIDR block: 122.76.0.0/16
 - iv. IPv4 subnet CIDR block: 122.76.64.32/27

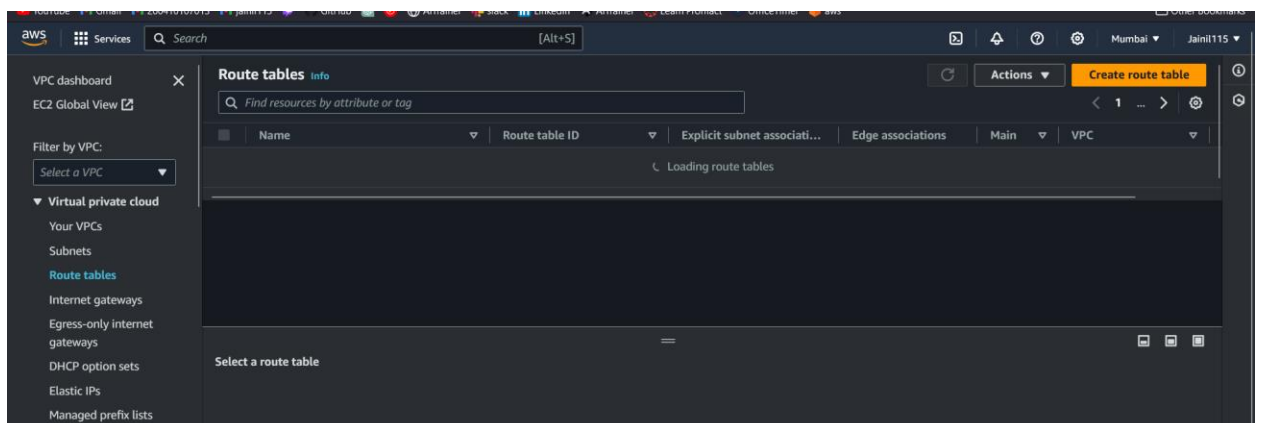


4. Then click on Create subnet. Now you will be able to see the subnets were successfully created.

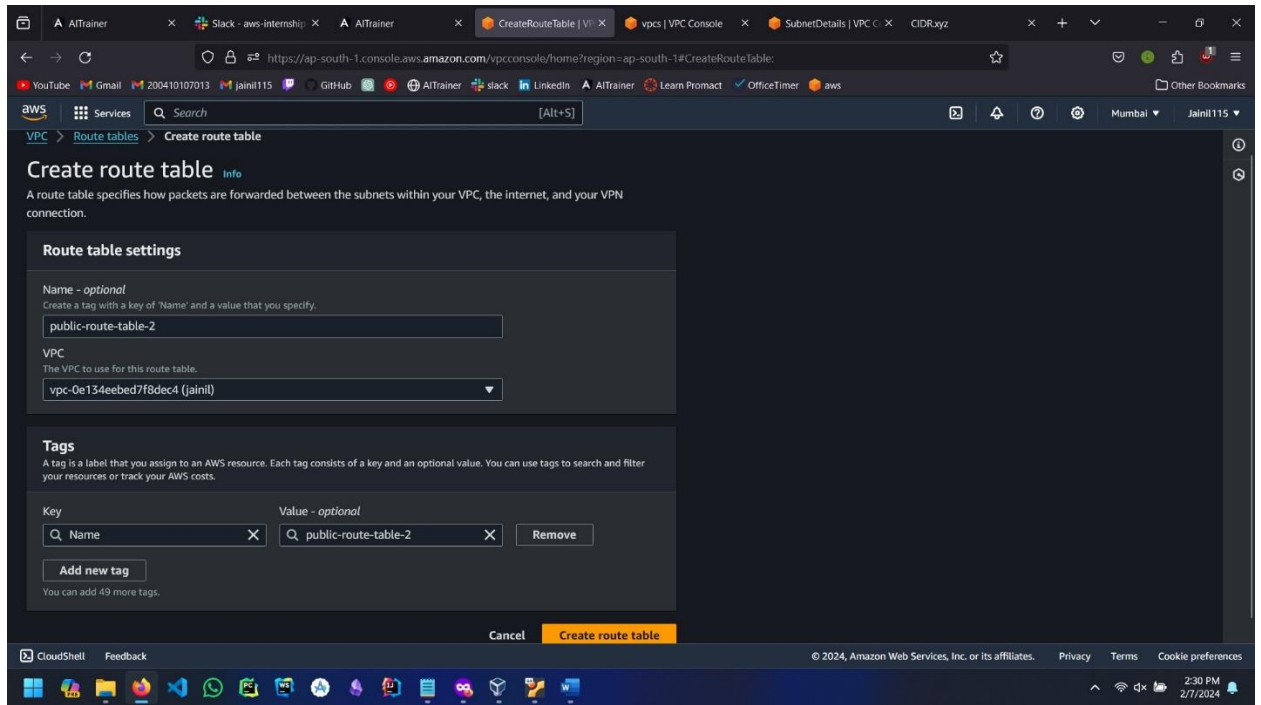


Now we need to create route tables. Here are the steps to create route table:

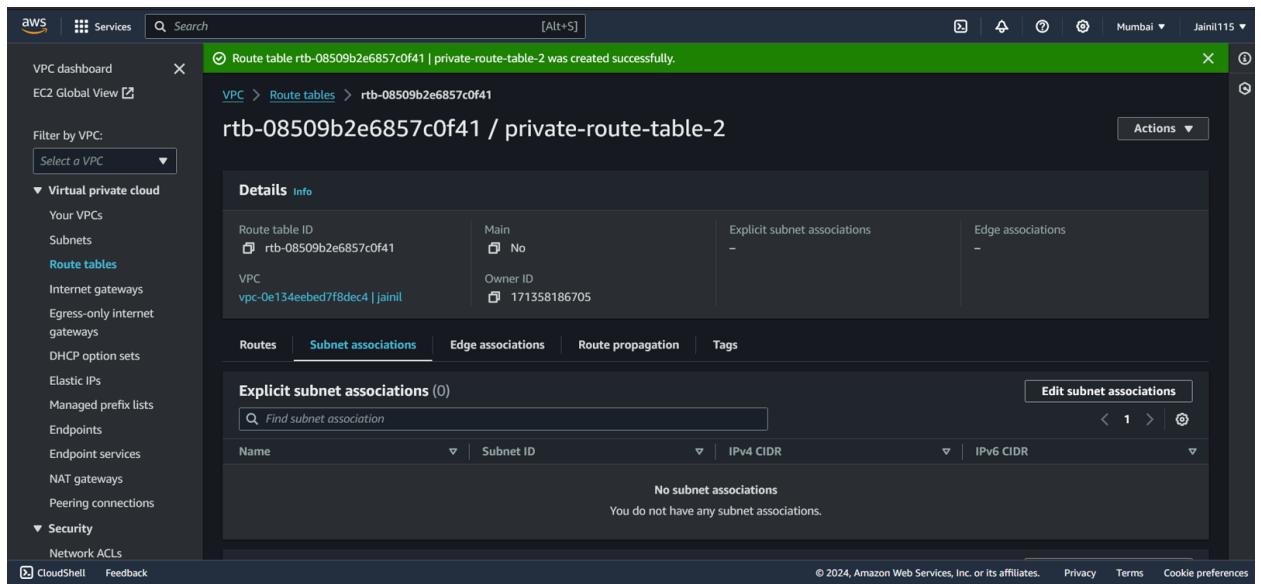
1. Now we need to create public route table by going to VPC dashboard and click on route table and click on create route table.



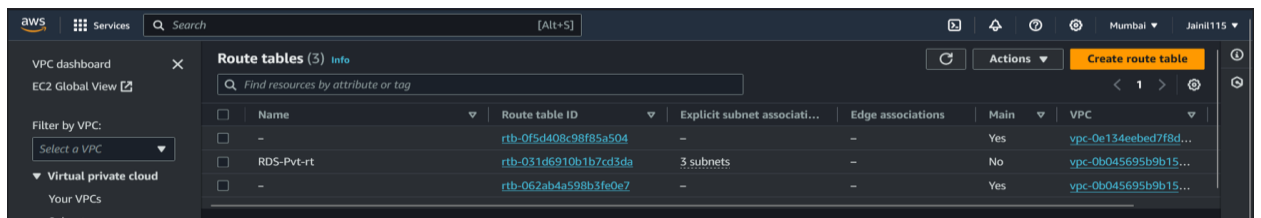
2. Fill out the route table setting:
 - i. Name: public-route-table-2
 - ii. VPC: vpc-0e134eebed7f8dec4 (jainil)



3. Then click on Create route table. Now you will be able to see the public-route-table-2.



4. Now go to route tables again, and click on create route table.



5. Fill out the route table setting:

- i. Name: private-route-table-2
- ii. VPC: vpc-0e134eebed7f8dec4 (jainil)

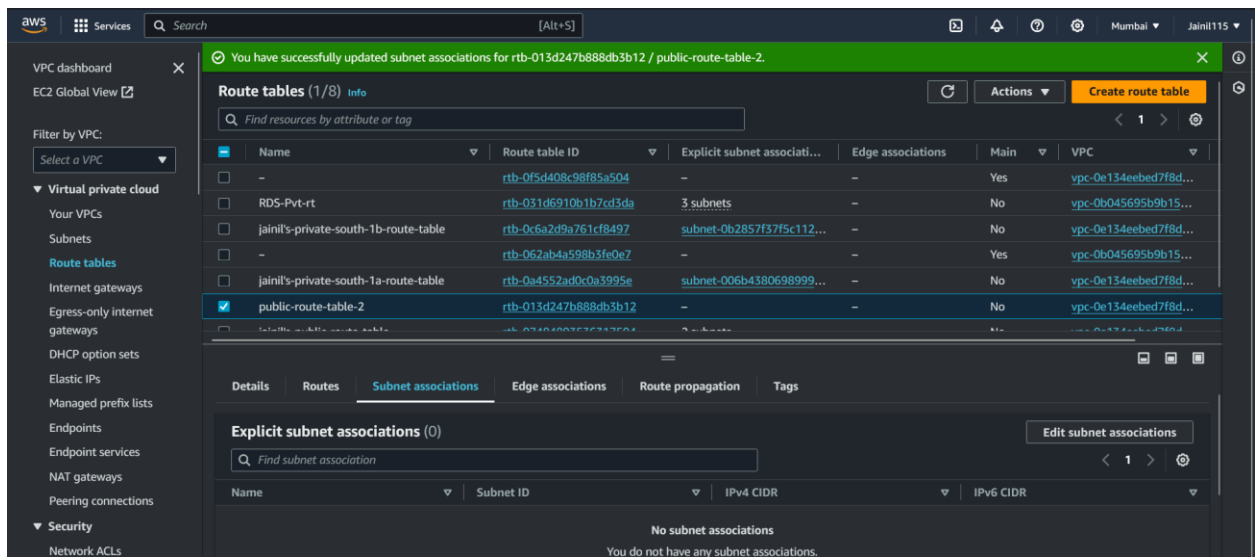
The screenshot shows the 'Create route table' page in the AWS Management Console. The 'Route table settings' section has the 'Name' field set to 'private-route-table-2' and the 'VPC' dropdown set to 'vpc-0e134eebed7f8dec4 (jainil)'. The 'Tags' section shows a tag with key 'Name' and value 'private-route-table-2'.

6. Then click on Create route table. Now you will be able to see the private-route-table-2.

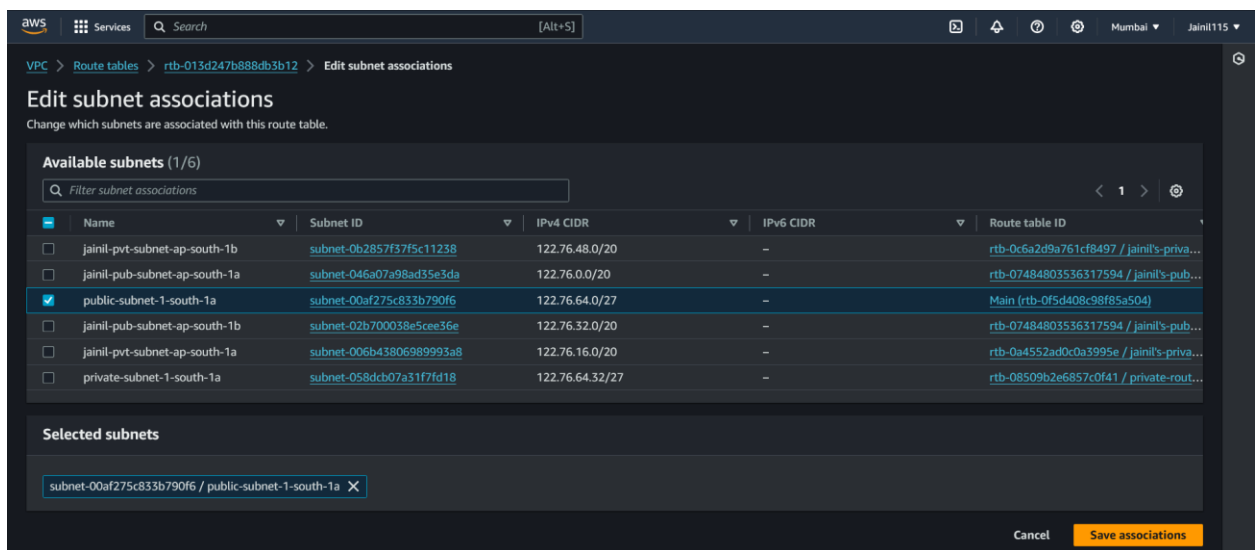
The screenshot shows the 'Route table rtb-08509b2e6857c0f41 / private-route-table-2' page in the AWS Management Console. The page displays details such as Route table ID, VPC, and Owner ID. The 'Subnet associations' tab is selected, showing 'Explicit subnet associations (0)'.

Now associate subnets with route table. Following are the steps to associate subnets to route table:

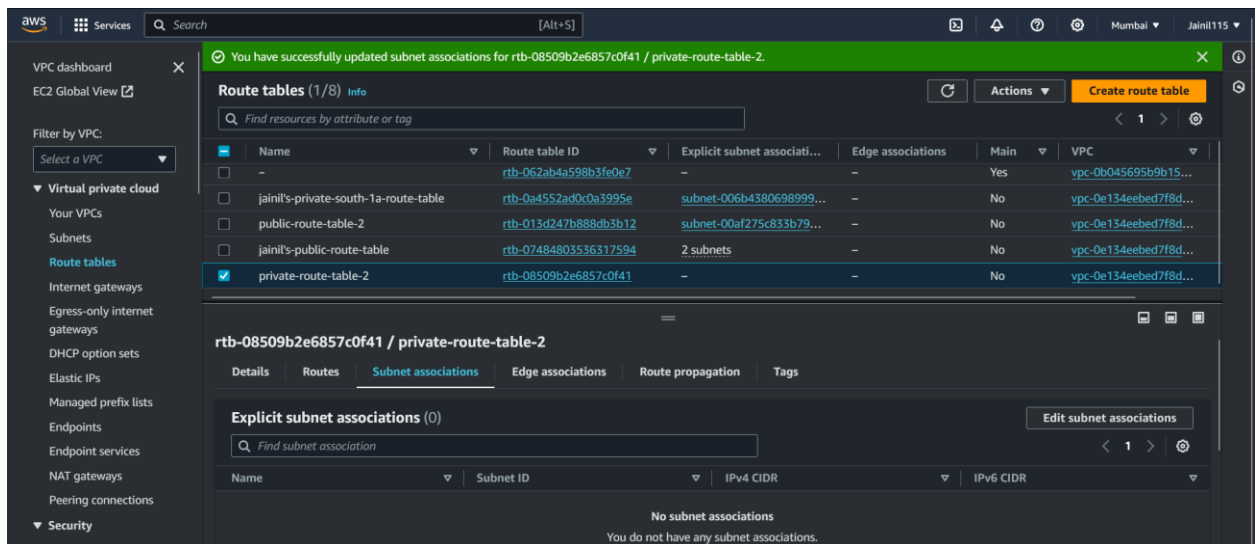
1. Go to Route tables and select public-route-table-2 and click on subnet associations.



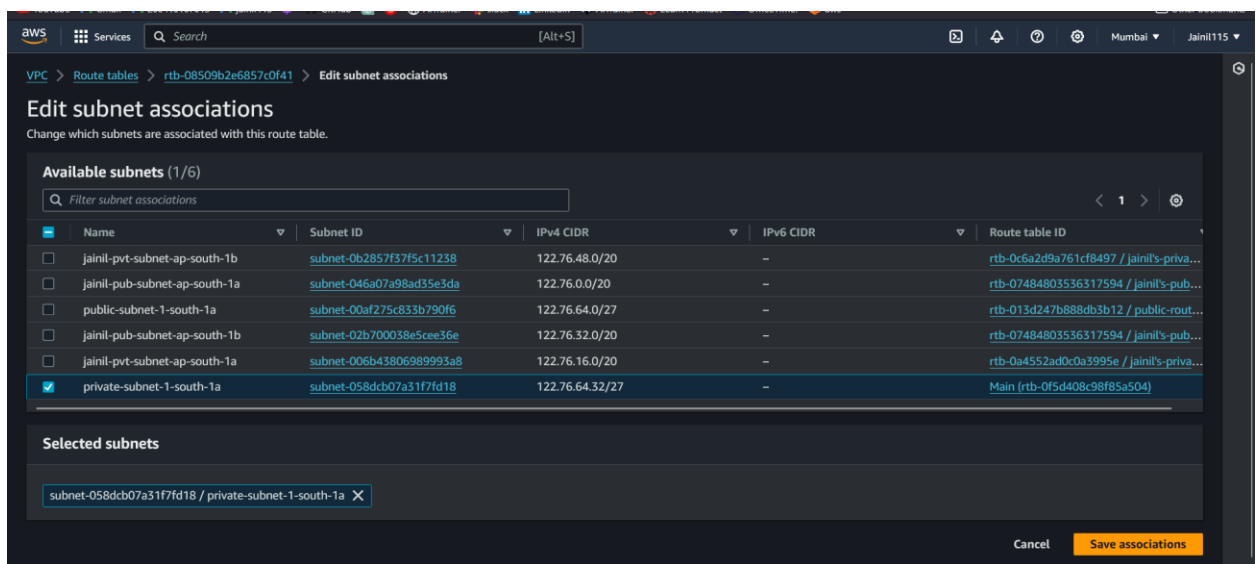
- Now click on edit subnet associations. And then select public-subnet-1-south-1a and click on Save associations.



- Now go to Route tables again and select private-route-table-2 and click on subnet associations.



- Then click on edit subnet associations. Then select private-subnet-1-south-1a and click on save associations.



Now add Internet-Gateway to public subnet.

- To add internet gateway to public subnet, go to Route tables and select public-route-table-2 and click on routes.

Route tables (1/8)

Name	Route table ID	Explicit subnet associati...	Edge associations	Main	VPC
-	rtb-062ab4a598b3fe0e7	-	-	Yes	vpc-0b045695b9b15...
jainil's-private-south-1a-route-table	rtb-0a4552ad0c0a3995e	subnet-006b4380698999...	-	No	vpc-0e134eebed7f8d...
public-route-table-2	rtb-013d247b888db3b12	subnet-00af275c833b79...	-	No	vpc-0e134eebed7f8d...
jainil's-public-route-table	rtb-07484803536317594	2 subnets	-	No	vpc-0e134eebed7f8d...
private-route-table-2	rtb-08509b2e6857c0f41	subnet-058dcb07a31f7fd...	-	No	vpc-0e134eebed7f8d...

rtb-013d247b888db3b12 / public-route-table-2

Routes (1)

Destination	Target	Status	Propagated
122.76.0.0/16	local	Active	No

- Now click on edit routes. Then click on add routes and then select the Internet Gateway and select the igw-073ebc5961480814 (jainil's igw) in target (created in previous task and is already attached to the current VPC) and set destination to 0.0.0.0/0 and click on save changes.

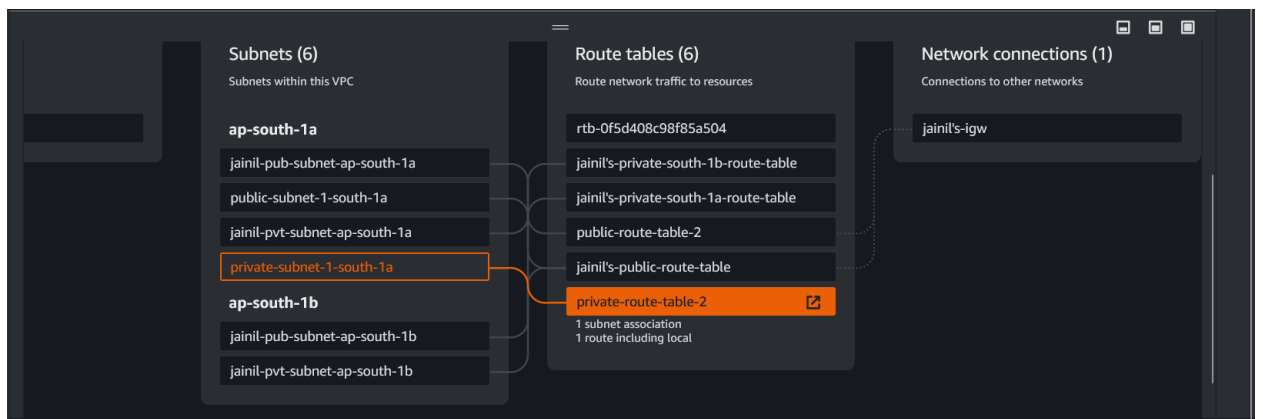
Edit routes

Destination	Target	Status	Propagated
122.76.0.0/16	local	Active	No
0.0.0.0/0	Internet Gateway	-	No
	igw-073ebc5961480814		

Add route

Cancel Preview **Save changes**

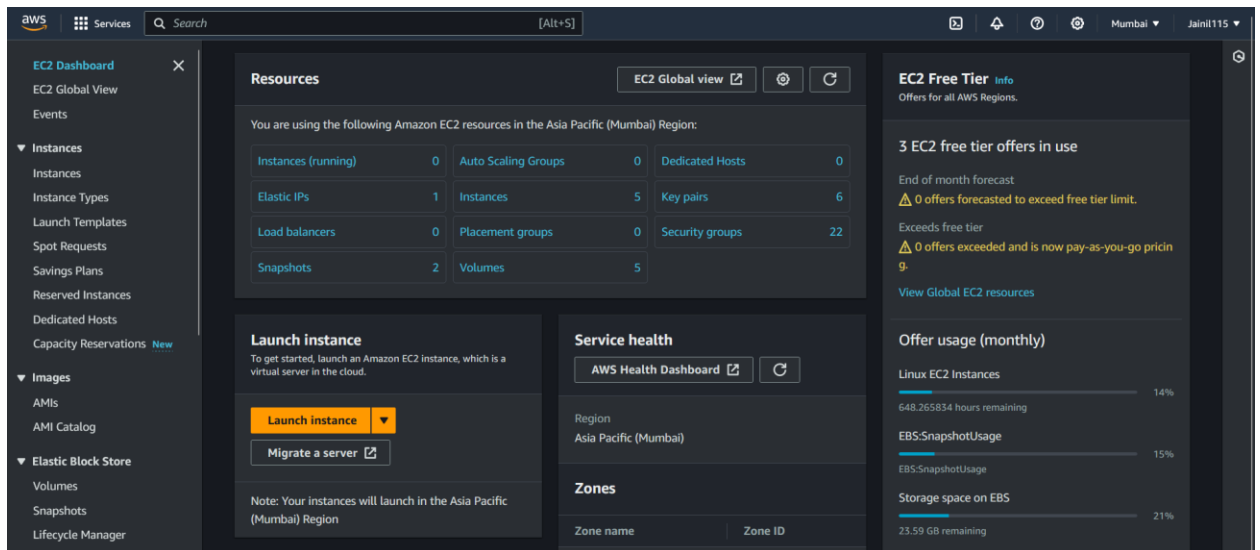
Now go to VPC. And check the Resource map to confirm that all the subnet's are associated with their appropriate route tables.



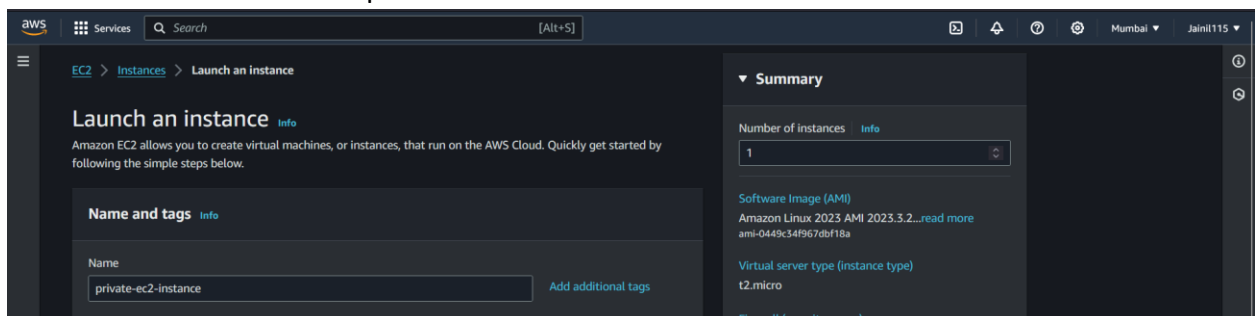
Steps to launch an EC2 instance in each subnet. The EC2 instance in the public subnet should be reachable from the Internet.:

Steps to create private ec2 instance:

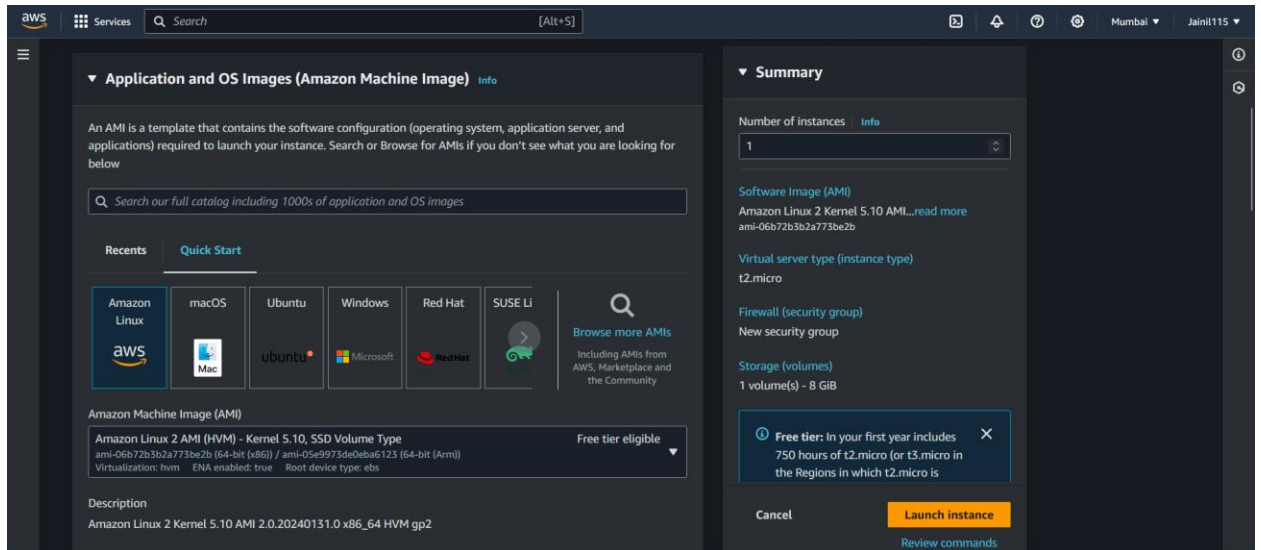
1. To create EC2 instance tab and click on launch EC2 instance.



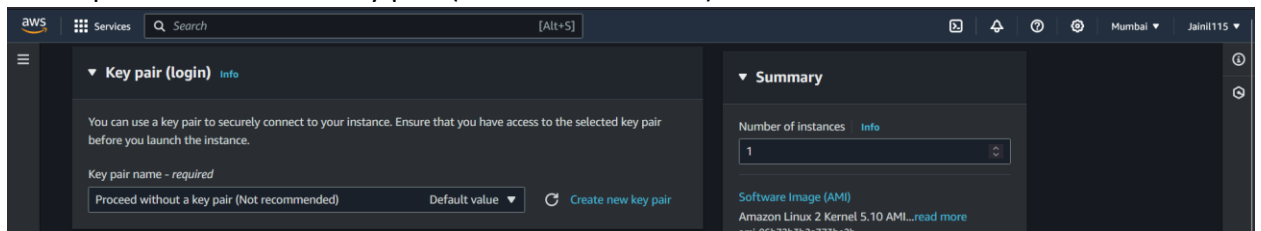
2. Enter the name of instance private-ec2-instance.



3. Select Amazon Linux 2 in AMI template.

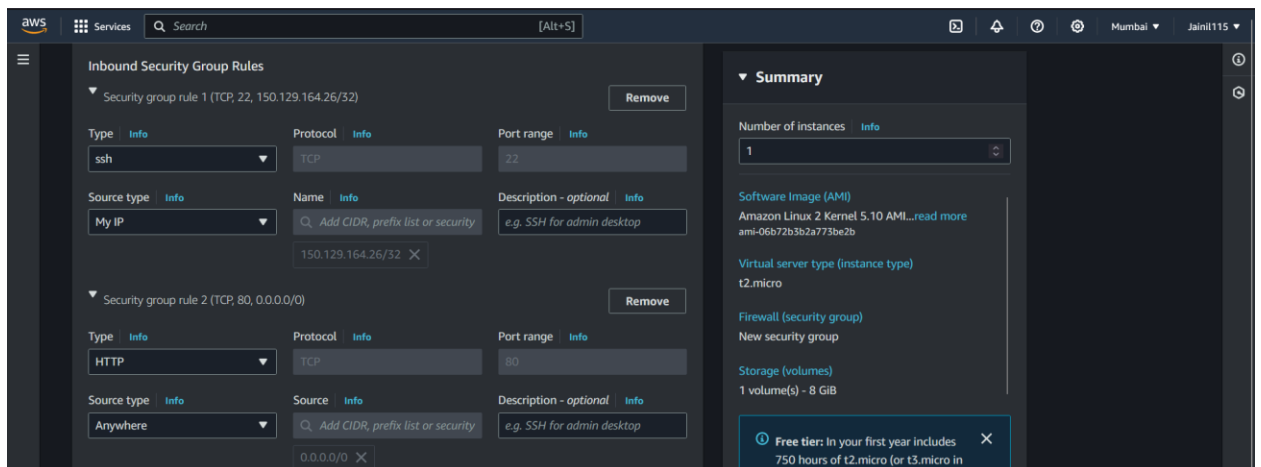
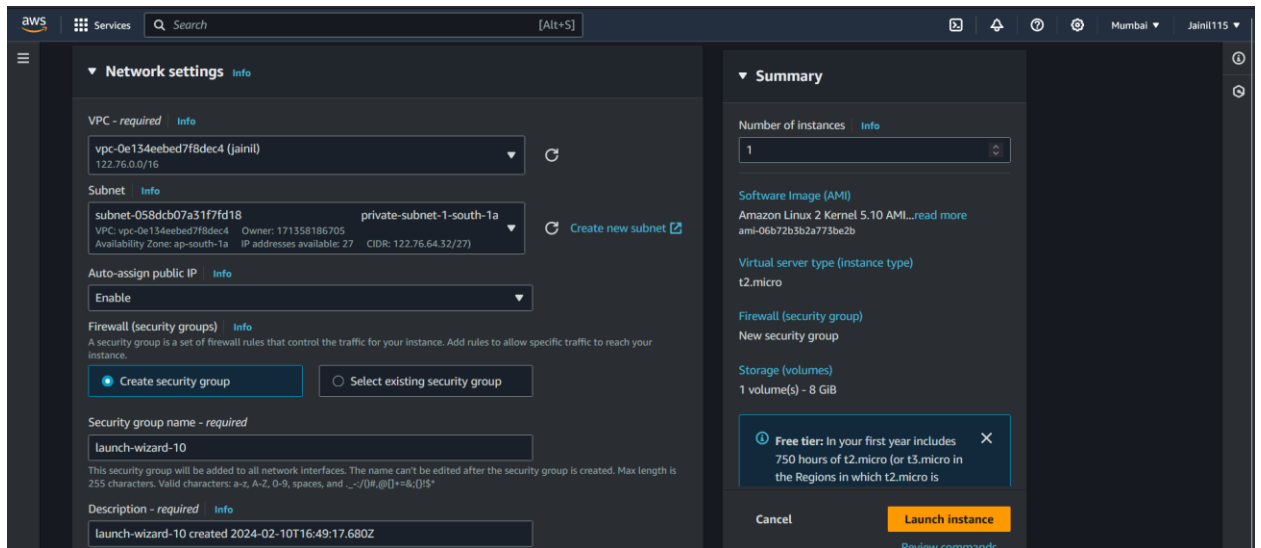


4. Select proceed without a key pair (Not recommended).

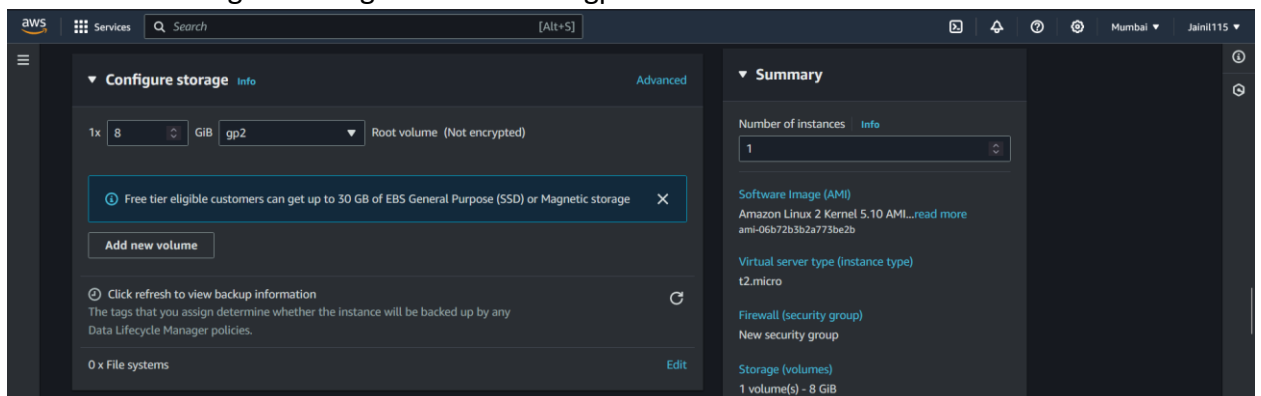


5. Now click on edit in Network setting. Then enter the following details:

- i. VPC: vpc-0e134eebed7f8dec4 (jainil)
- ii. Subnet: private-subnet-1-south-1a
- iii. Auto-Assign IP: Enable
- iv. Firewall (Security Groups): Create security group
- v. Security group name: launch-wizard-10 (Automatically created)
- vi. Description: launch-wizard-10 created 2024-02-10T16:49:17.680Z (Automatically created)
- vii. In inbound security group Rules: Under SSH select MY IP.
- viii. Add a http inbound rule and add source type anywhere (to test if it is accessible).



- Then inside configure storage select 8GiB of gp2 root volume.



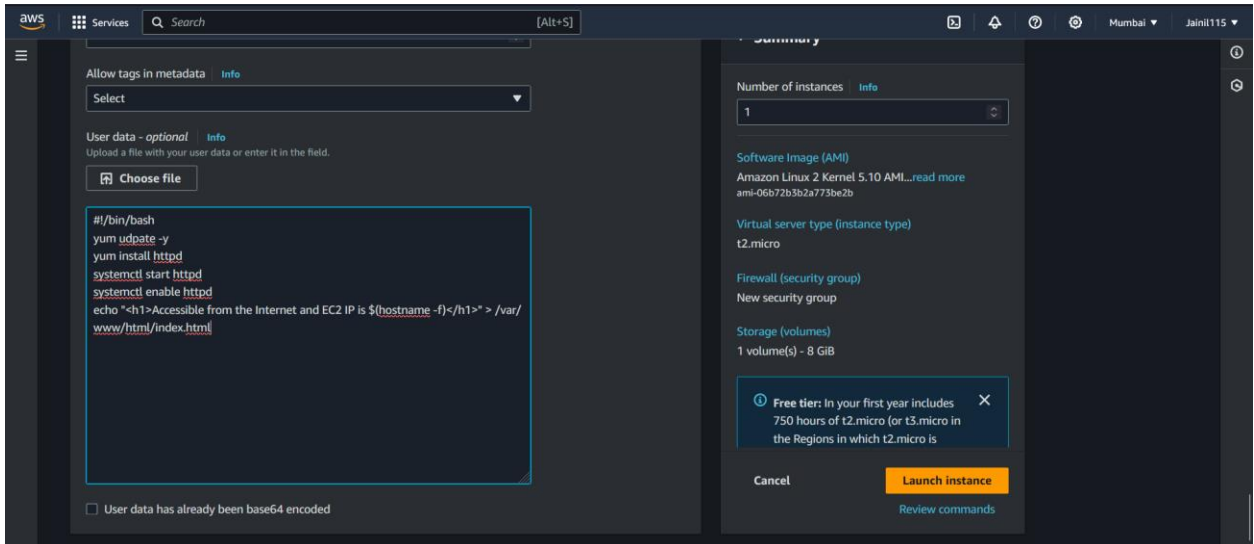
- Under advanced details scroll down to bottom and enter the following User data. And Click on Launch Instance.

```
#!/bin/bash
yum update -y
```

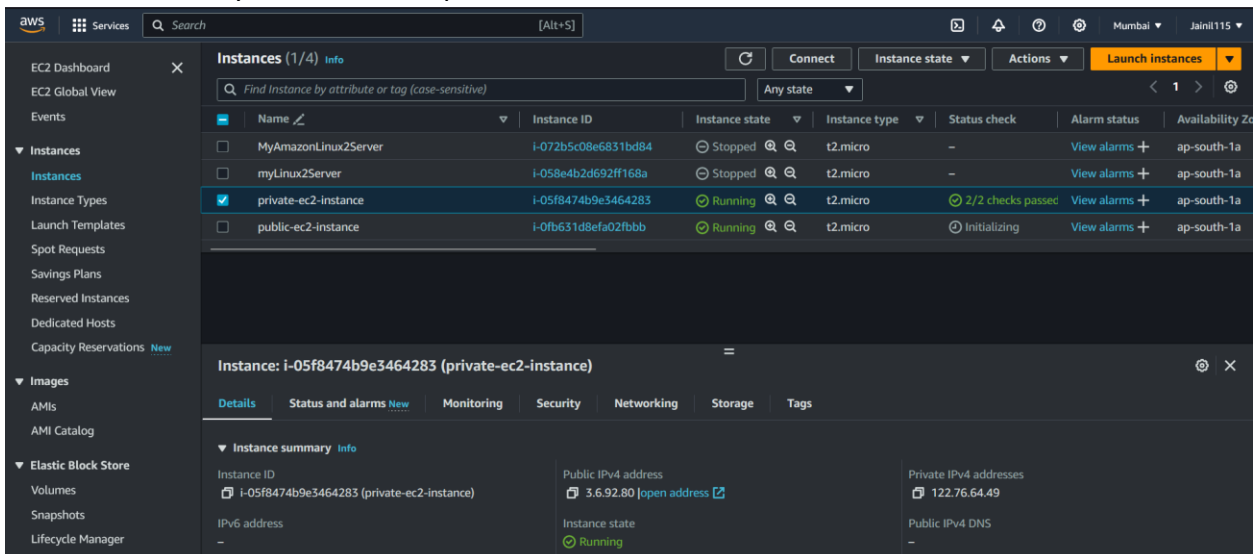
```

yum install httpd
systemctl start httpd
systemctl enable httpd
echo "<h1>Accessible from the Internet and EC2 IP is $(hostname -f)</h1>" >
/var/www/html/index.html

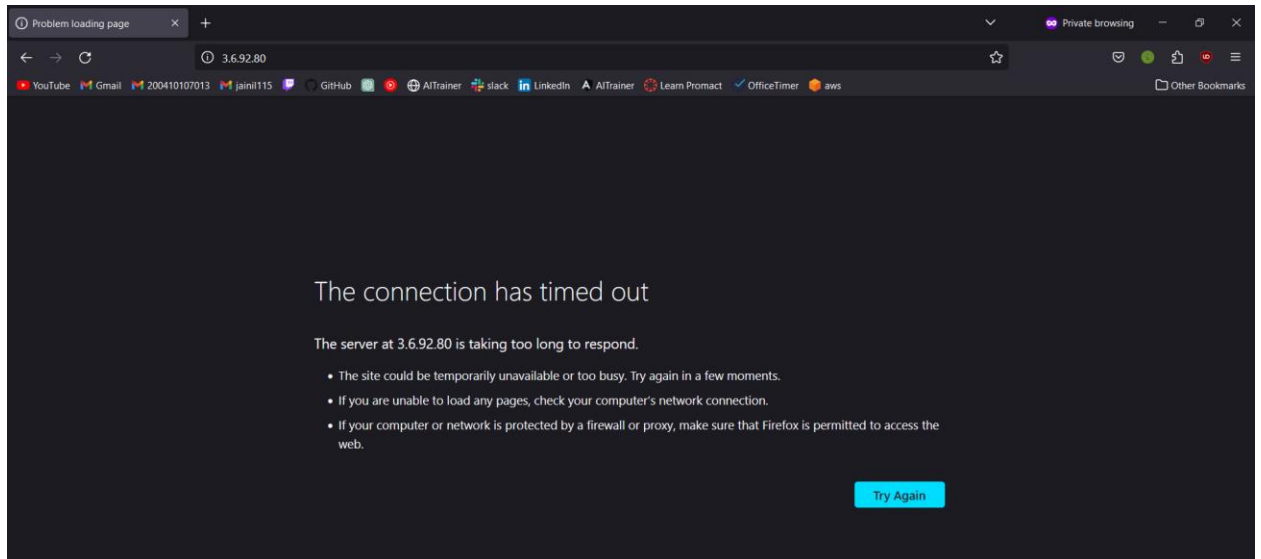
```



8. Now in instances you can see the private-ec2-instance is created.

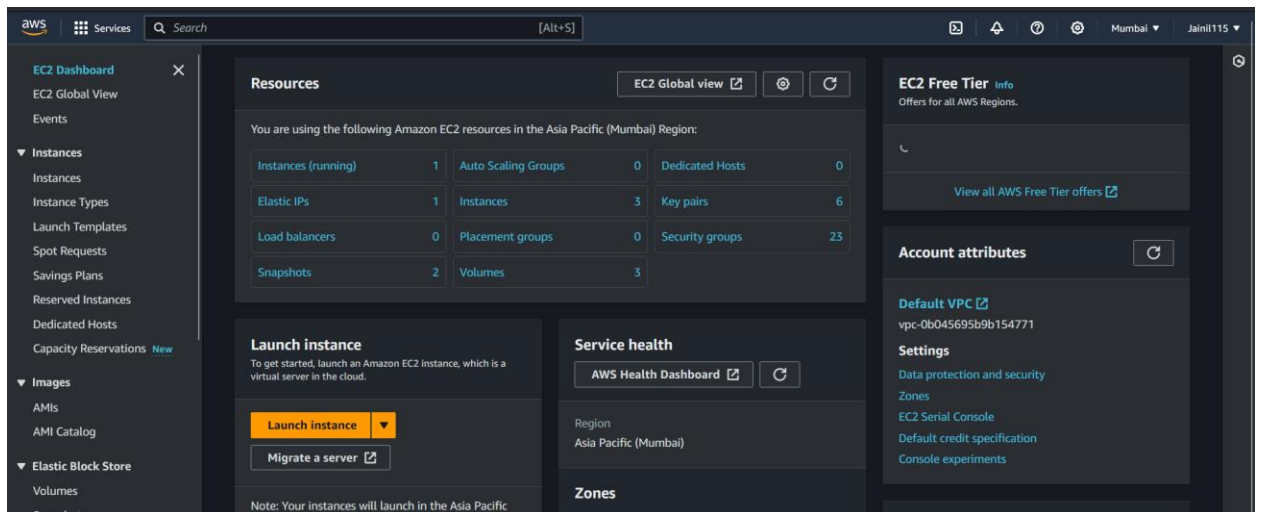


9. Now enter the public ip address in a web browser to check if it is accessible from the internet.

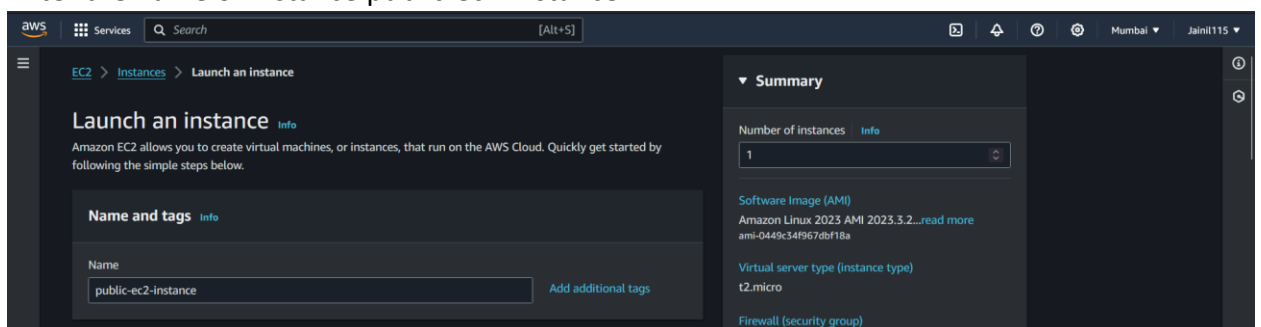


Steps to create public ec2 instance:

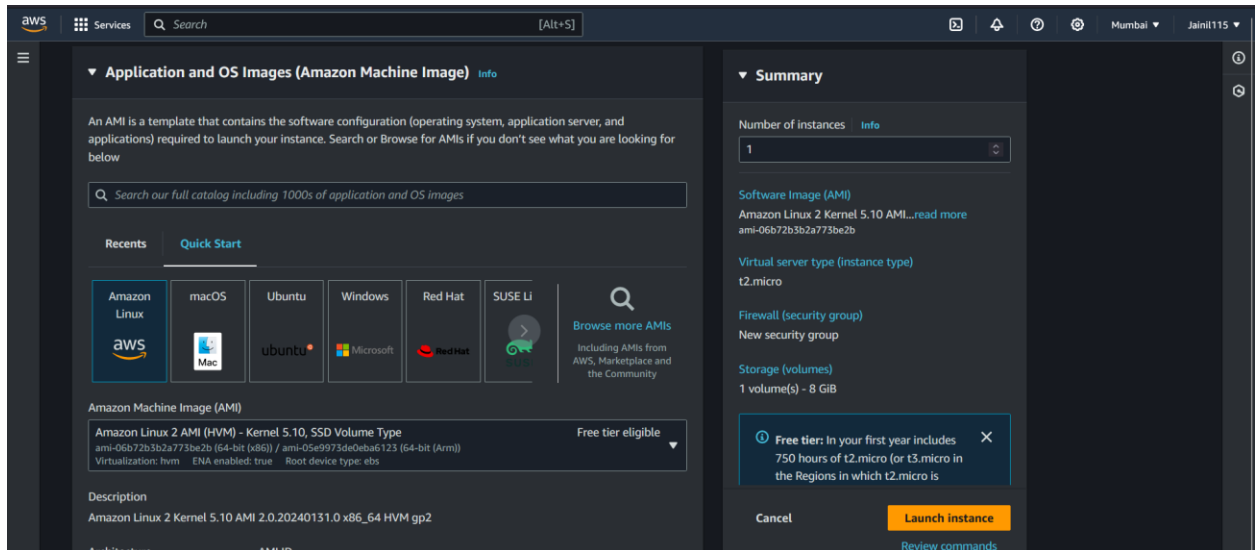
1. To create EC2 Dashboard and click on launch EC2 instance.



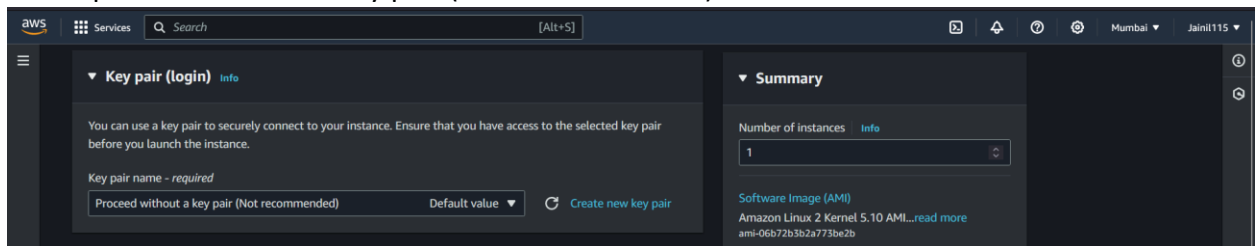
2. Enter the name of instance public-ec2-instance.



3. Select Amazon Linux 2 in AMI template.



4. Select proceed without a key pair (Not recommended).



5. Now click on edit in Network setting. Then enter the following details:
 - i. VPC: vpc-0e134eebed7f8dec4 (jainil)
 - ii. Subnet: public-subnet-1-south-1a
 - iii. Auto-Assign IP: Enable
 - iv. Firewall (Security Groups): Create security group
 - v. Security group name: launch-wizard-11 (Automatically created)
 - vi. Description: launch-wizard-11 created 2024-02-10T17:08:23.180Z (Automatically created)
 - vii. In inbound security group Rules: Under SSH select MY IP.
 - viii. Add a http inbound rule and add source type anywhere (to test if it is accessible).

Network settings

VPC - required
vpc-0e134eebed7f8dec4 (jainil)
122.76.0.0/16

Subnet
subnet-00af275c833b790f6 public-subnet-1-south-1a
VPC: vpc-0e134eebed7f8dec4 Owner: 171358186705
Availability Zone: ap-south-1a IP addresses available: 27 CIDR: 122.76.64.0/27

Auto-assign public IP
Enable

Firewall (security groups)
A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.
☒ Create security group ☐ Select existing security group

Security group name - required
launch-wizard-11
This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and _-./[!@#%&*~`^'\"/>
Description - required
launch-wizard-11 created 2024-02-10T17:08:23.180Z

Summary

Number of instances
1

Software Image (AMI)
Amazon Linux 2 Kernel 5.10 AMI...read more
ami-06b72b3b2a773be2b

Virtual server type (instance type)
t2.micro

Firewall (security group)
New security group

Storage (volumes)
1 volume(s) - 8 GiB

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is

Cancel Launch instance Review commands

Inbound Security Group Rules

Security group rule 1 (TCP, 22, 150.129.164.26/32) Remove

Type ssh Protocol TCP Port range 22
Source type My IP Name 150.129.164.26/32 Description - optional e.g. SSH for admin desktop

Security group rule 2 (TCP, 80, 0.0.0.0/0) Remove

Type HTTP Protocol TCP Port range 80
Source type Anywhere Source 0.0.0.0/0 Description - optional e.g. SSH for admin desktop

Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

Summary

Number of instances
1

Software Image (AMI)
Amazon Linux 2 Kernel 5.10 AMI...read more
ami-06b72b3b2a773be2b

Virtual server type (instance type)
t2.micro

Firewall (security group)
New security group

Storage (volumes)
1 volume(s) - 8 GiB

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is

Cancel Launch instance Review commands

6. Then inside configure storage select 8GiB of gp2 root volume.

Configure storage

1x 8 GiB gp2 Root volume (Not encrypted)

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage

Add new volume

Click refresh to view backup information
The tags that you assign determine whether the instance will be backed up by any Data Lifecycle Manager policies.

0 x File systems Edit

Summary

Number of instances
1

Software Image (AMI)
Amazon Linux 2 Kernel 5.10 AMI...read more
ami-06b72b3b2a773be2b

Virtual server type (instance type)
t2.micro

Firewall (security group)
New security group

Storage (volumes)
1 volume(s) - 8 GiB

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is

7. Under advanced details scroll down to bottom and enter the following User data. And Click on Launch Instance.

```
#!/bin/bash
```

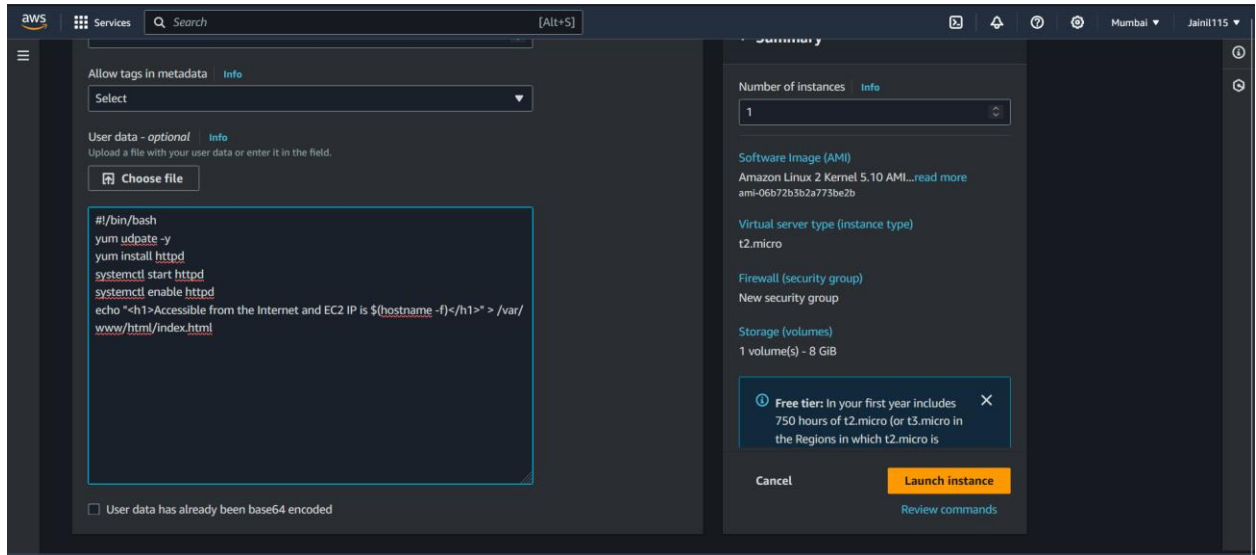
```
yum update -y
```

```
yum install -y httpd
```

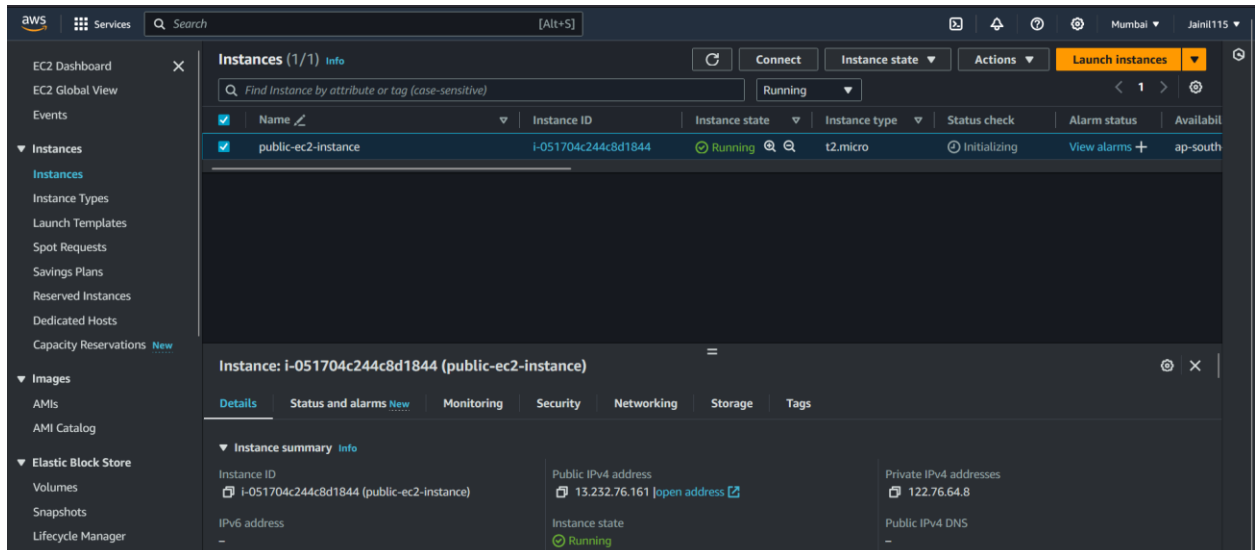
```
systemctl start httpd
```

```
systemctl enable httpd
```

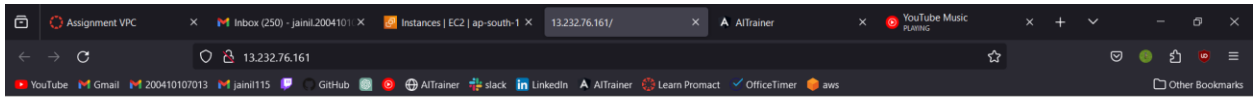
```
echo "<h1>Accessible from the Internet and EC2 IP is $(hostname -f)</h1>" >  
/var/www/html/index.html
```



8. Now in instances you can see the public-ec2-instance is created.



9. Now enter the public ip address 13.232.76.161 (I have deleted the instance) in a web browser to check if it is accessible from the internet.



Accessible from the Internet and EC2 IP is ip-122-76-64-8.ap-south-1.compute.internal