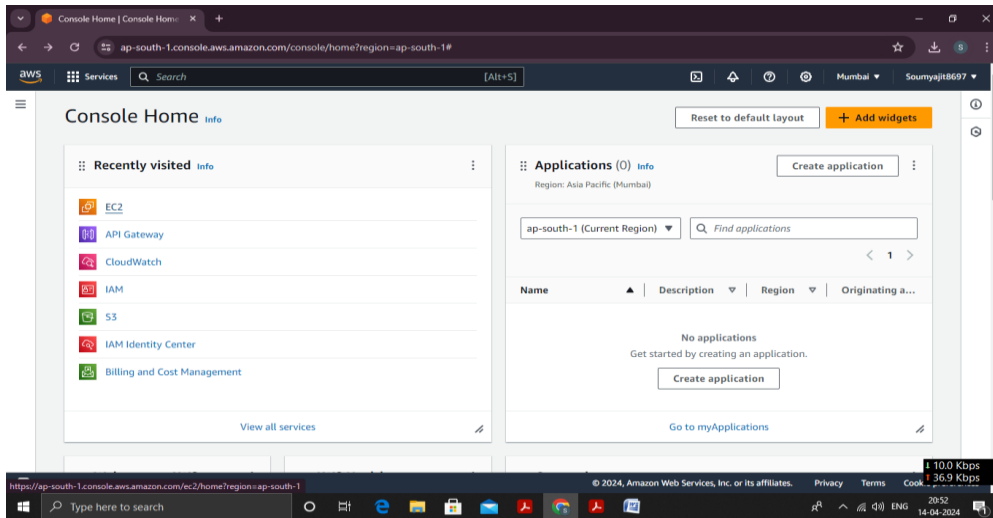


Assignment:-10

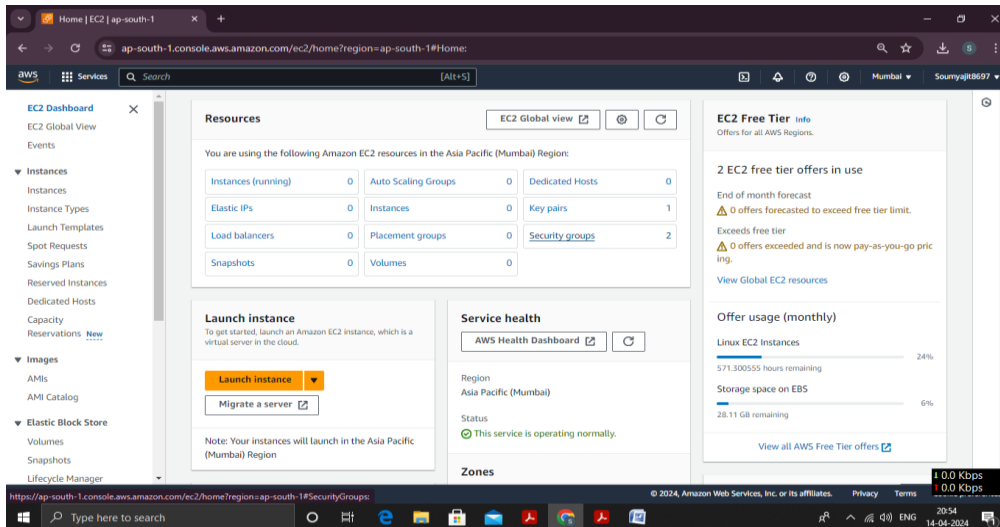
Problem Statement: Deploy a project from GitHub to EC2 by creating a new security group and user data.

Procedure:

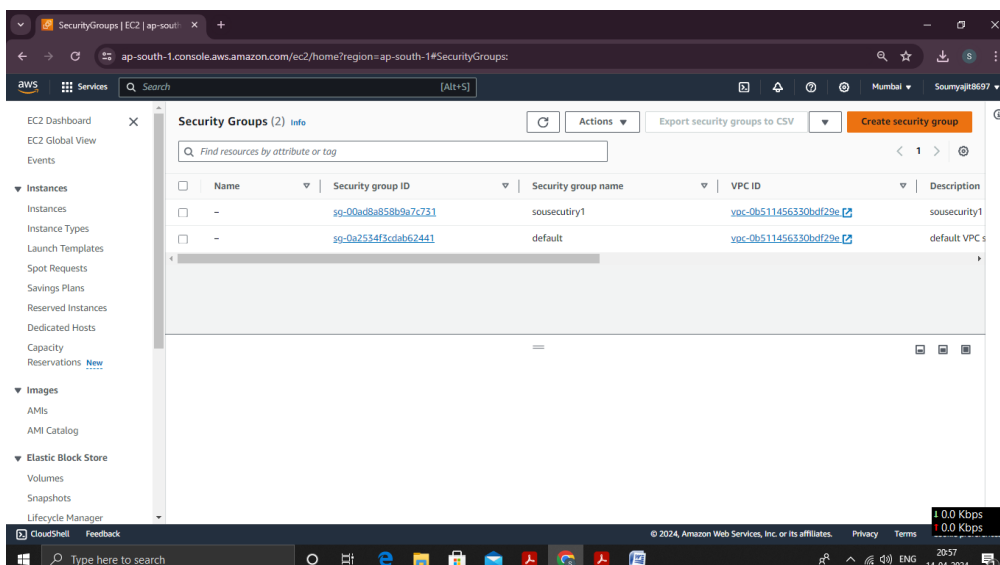
1. Access your AWS console and search for EC2, then proceed to click on the first option.



2. Now, Click on "Security Groups".



3. Now click on "Create security Group".



4. Fill up the name and description (same as name) of the security group.

Create security group

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

Basic details

Security group name [info](#)
sousecurityEC2
Name cannot be edited after creation.

Description [info](#)
sousecurityEC2

VPC [info](#)
vpc-0b511456330bdf29e

Inbound rules [info](#)

This security group has no inbound rules.

5. Now, scroll down to Inbound Rules and click on “Add rule”. First set the type as Custom TCP, port number as 4000 and select first option in CIDR blocks i.e. “0.0.0.0/0” .

Inbound rules [info](#)

Type	Protocol	Port range	Source	Description - optional
Custom TCP	TCP	4000	Anyw... 0.0.0.0/0	

Add rule

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

Outbound rules [info](#)

Type	Protocol	Port range	Destination	Description - optional
All traffic	All	All	Custom 0.0.0.0/0	

Add rule

6. Click on “Add rule” again and set type as “SSH” and select first option in CIDR blocks. Repeat this two more times and add rules of type “HTTP” and “HTTPS”.

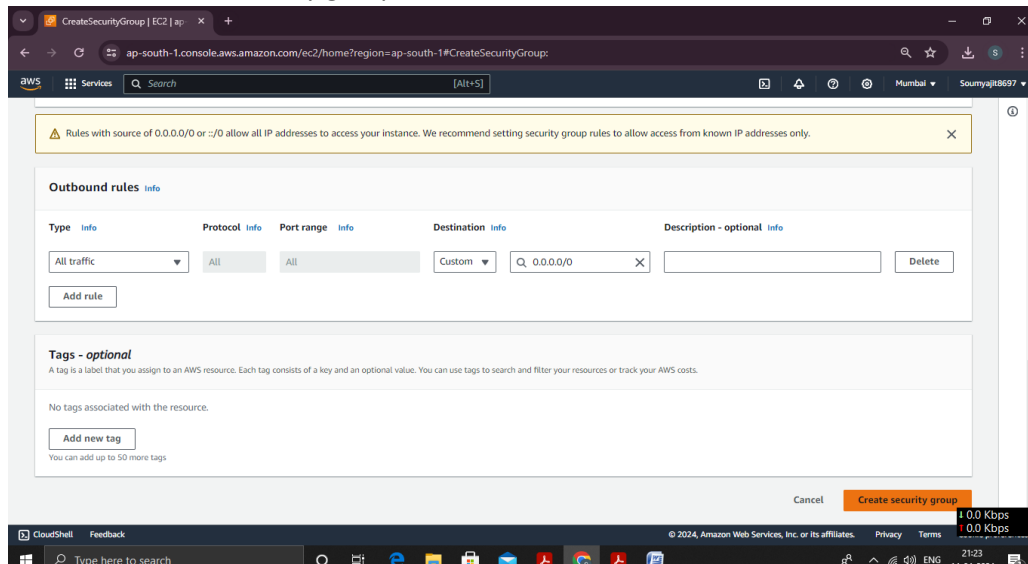
Inbound rules [info](#)

Type	Protocol	Port range	Source	Description - optional
Custom TCP	TCP	4000	Anyw... 0.0.0.0/0	
SSH	TCP	22	Anyw... 0.0.0.0/0	
HTTP	TCP	80	Anyw... 0.0.0.0/0	
HTTPS	TCP	443	Anyw... 0.0.0.0/0	

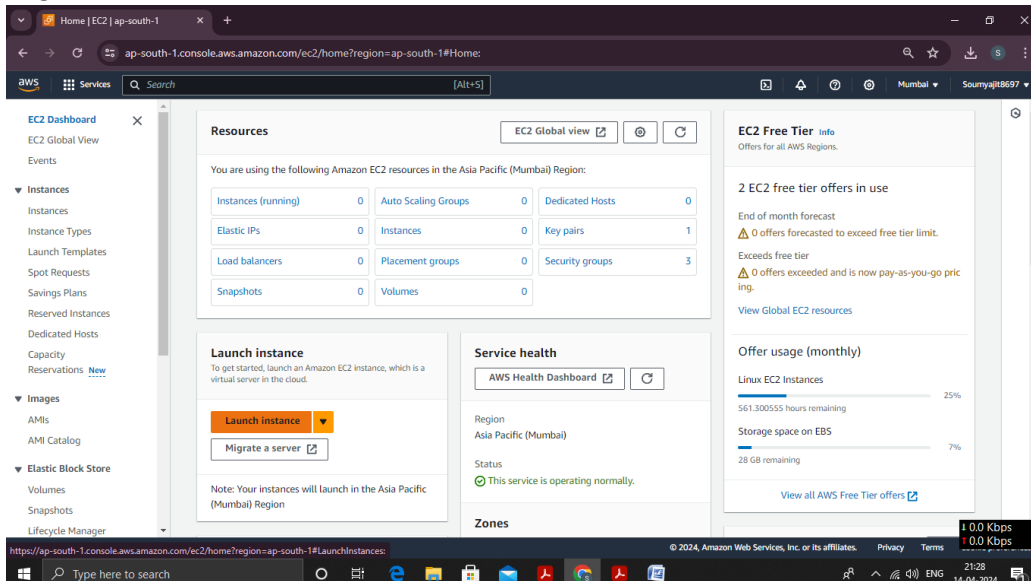
Add rule

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

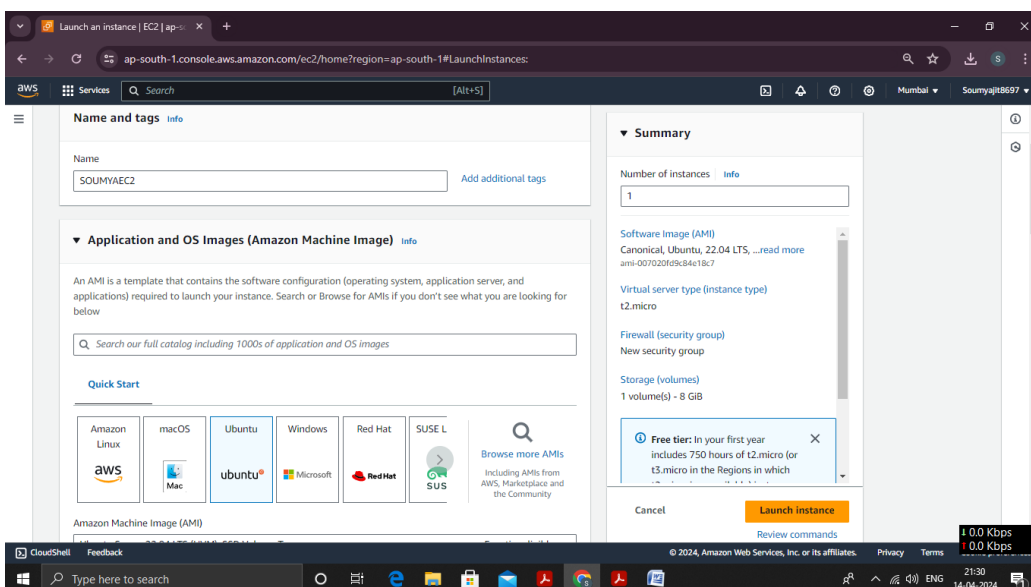
7. Then click on “Create security group”.



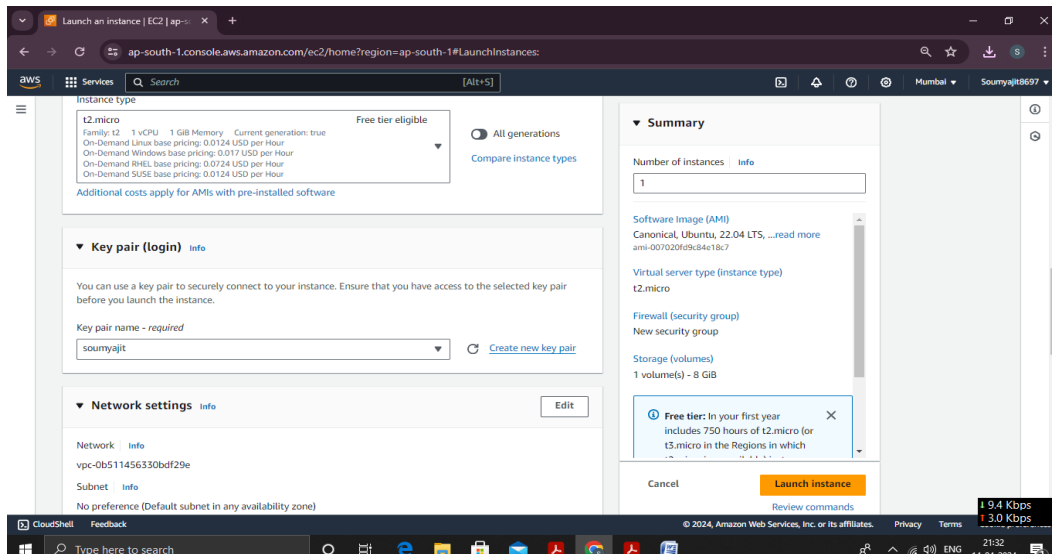
8. Now, go to EC2 dashboard and click on “Launch instance”.



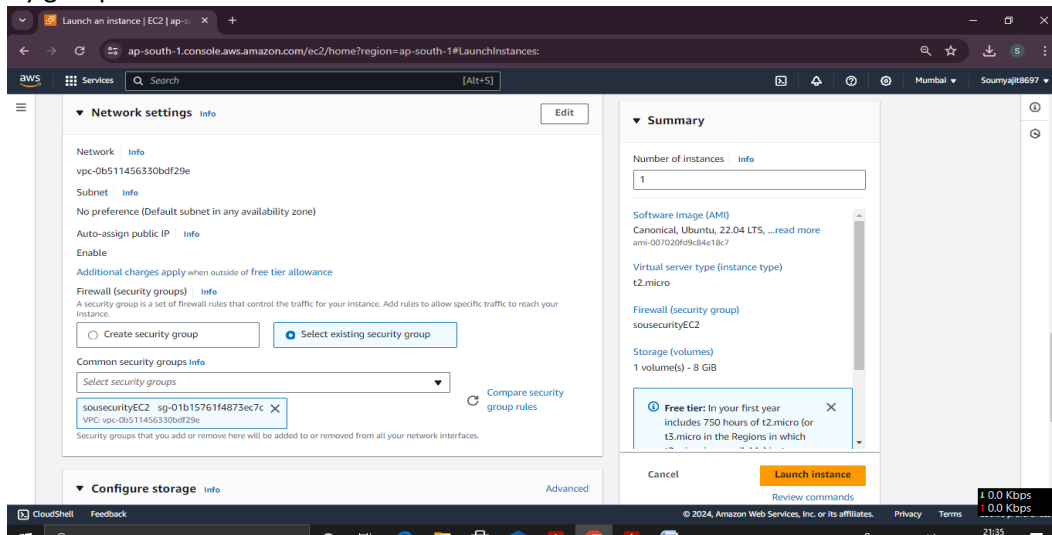
9. Fill up the instance name and select Ubuntu as the AMI.



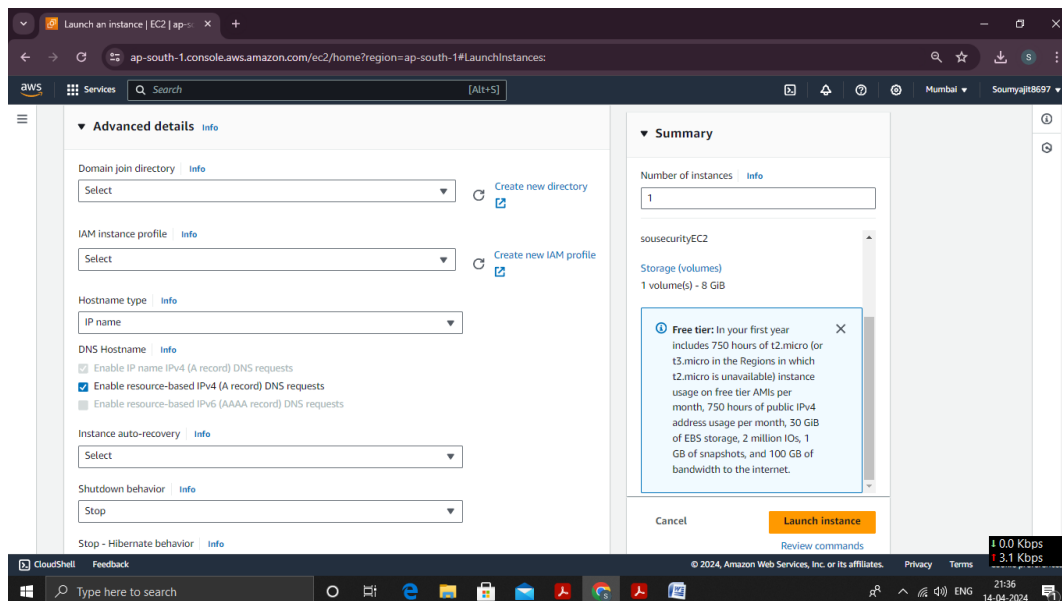
10. Select an existing keypair or create a new one.



11. Now, from Network settings option select “Existing security group” and select the newly created security group.



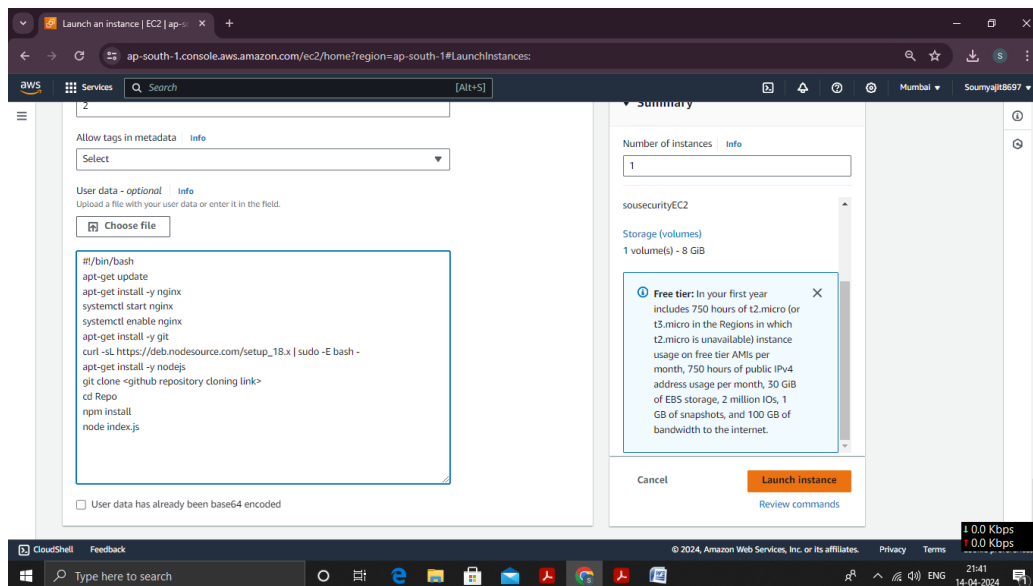
12. Expand the “Advanced details” section.



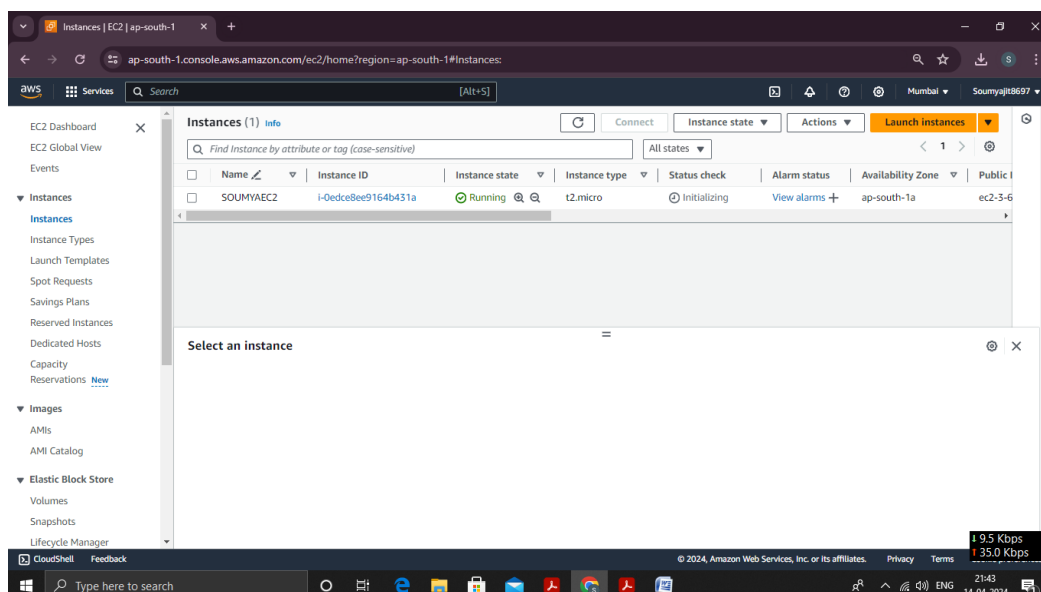
13. Scroll down to the “User data” section and add the following script:

```
#!/bin/bash
apt-get update
apt-get install -y nginx
systemctl start nginx
systemctl enable nginx
apt-get install -y git
curl -sL https://deb.nodesource.com/setup_18.x | sudo -E bash -
apt-get install -y nodejs
git clone <github repository cloning link>
cd Repo
npm install
node index.js
```

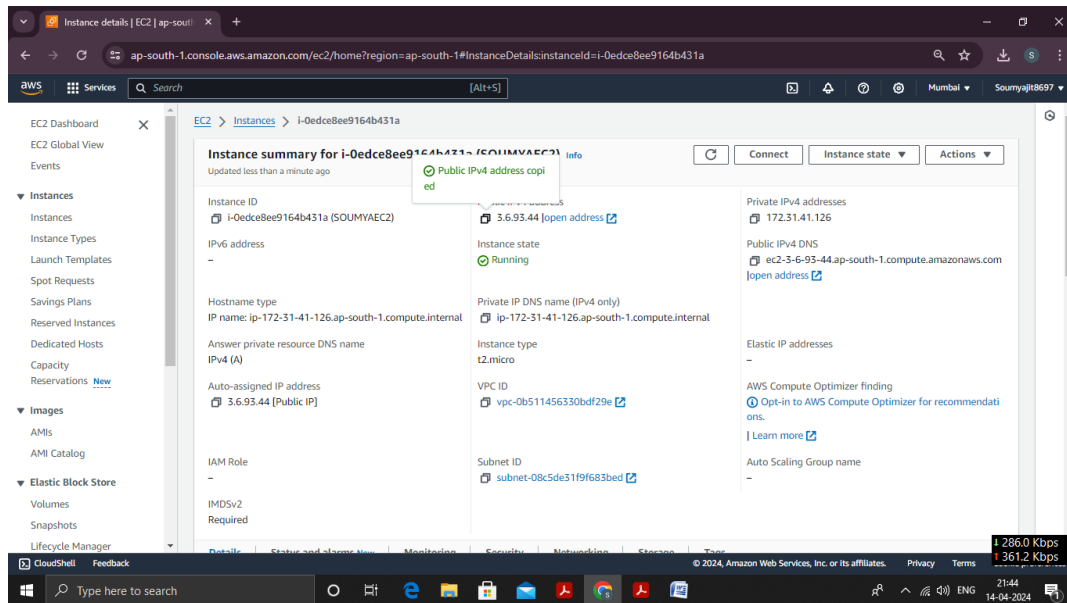
14. Then click on “Launch instance”.



15. Now go to “Instances” and click on the instance id of the newly created instance.



16. Copy the public IPv4 address.



17. Open a new incognito tab and paste the IPv4 address copied then we can see the page “Welcome to nginx!” and add “:4000” to the end of public IPv4 address . This will display our intended website.

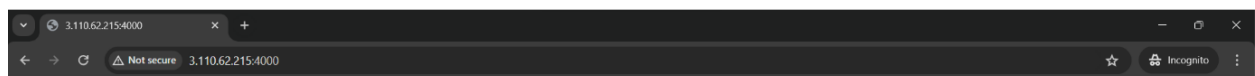


Welcome to nginx!

If you see this page, the nginx web server is successfully installed and working. Further configuration is required.

For online documentation and support please refer to nginx.org.
Commercial support is available at nginx.com.

Thank you for using nginx.



Hello