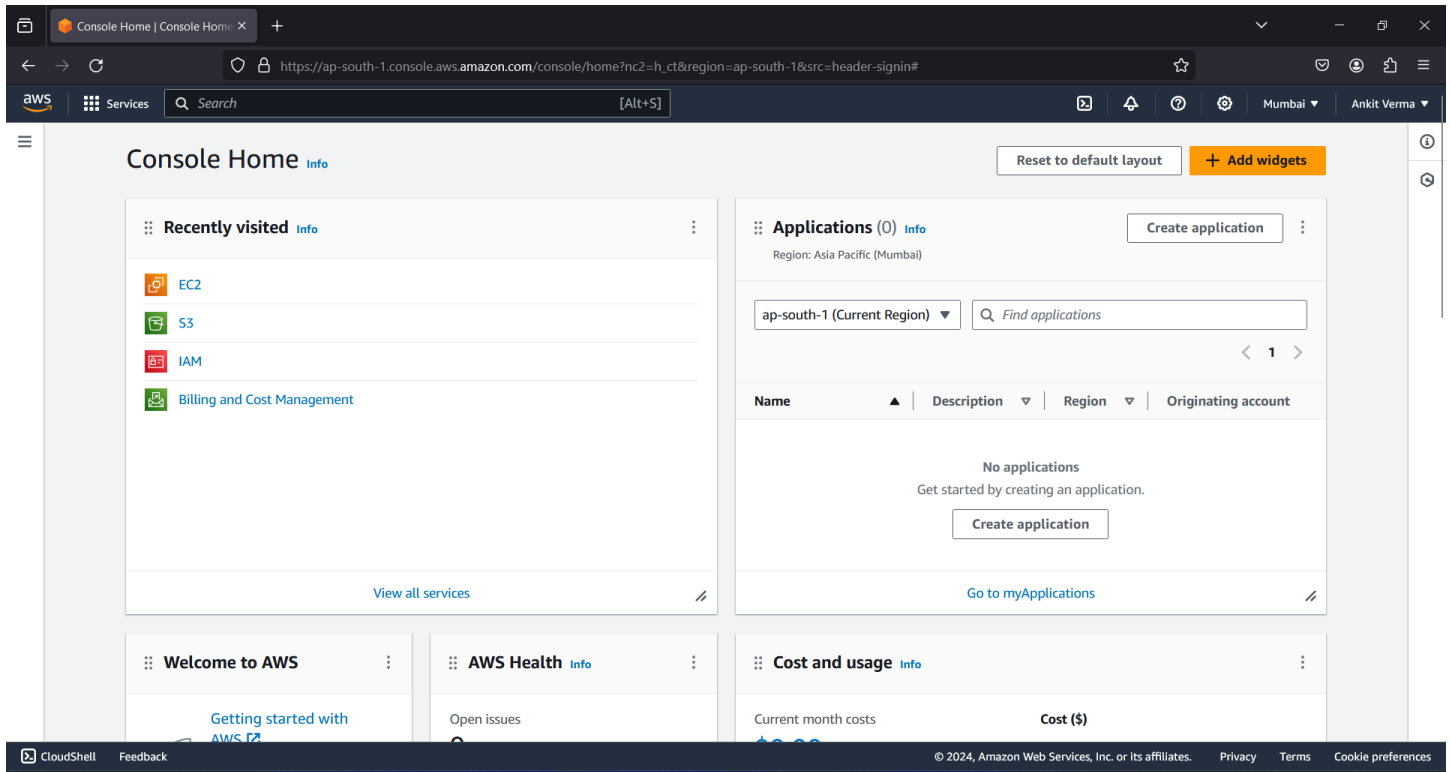


Assignment: 9

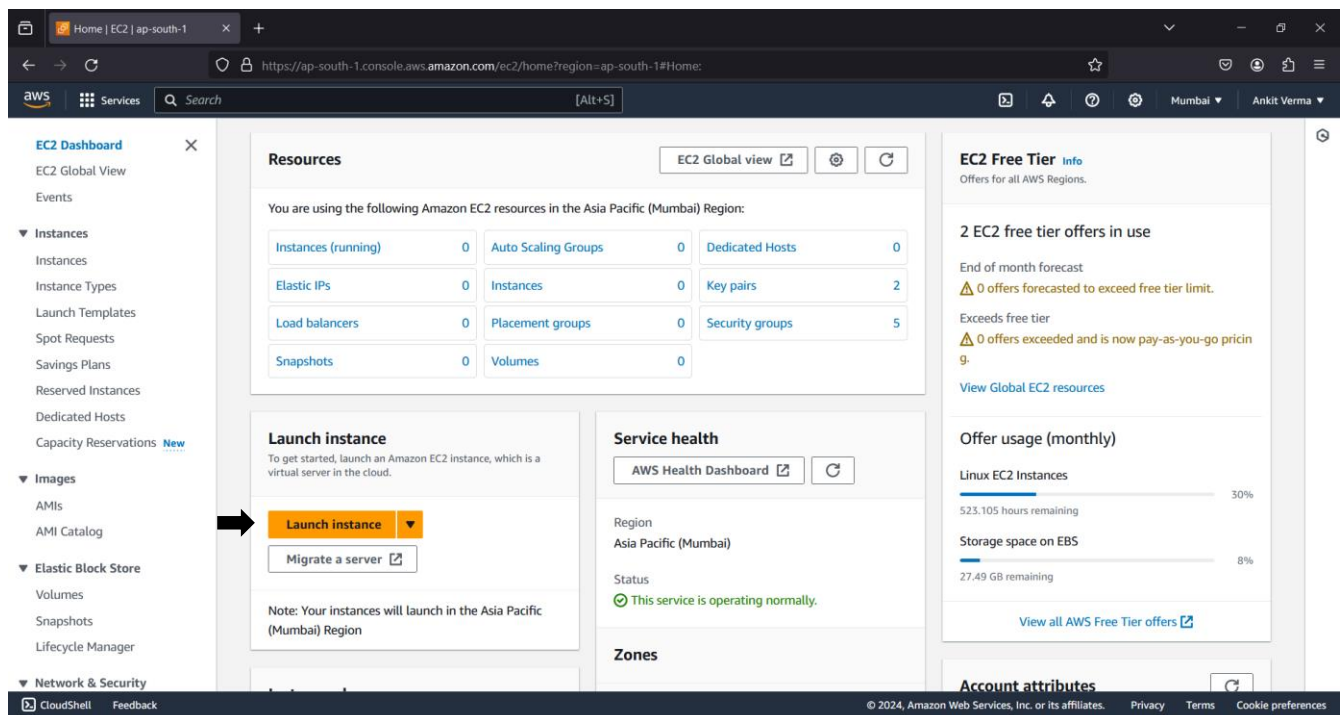
Problem Statement: Deploy a project from GitHub to EC2.

» The steps to deploy the project:-

Step 1: Select EC2.



Step 2: Click on 'Launch Instance'.



Step 3: Give a unique name to the instance and select Ubuntu.

The screenshot shows the AWS Management Console 'Launch an instance' page. The 'Name' field is set to 'Assg9'. The 'Application and OS Images' section shows 'Ubuntu' selected as the AMI. The 'Summary' section on the right shows 'Number of instances' as 1, 'Software Image (AMI)' as Canonical, Ubuntu, 22.04 LTS, 'Virtual server type (instance type)' as t2.micro, 'Firewall (security group)' as New security group, and 'Storage (volumes)' as 1 volume(s) - 8 GiB. A 'Launch instance' button is visible at the bottom right.

Step 4: Select the key from the list or create a new one.

The screenshot shows the AWS Management Console 'Launch an instance' page. The 'Key pair (login)' section shows a dropdown menu with 'key2' selected. The 'Summary' section on the right shows 'Number of instances' as 1, 'Software Image (AMI)' as Canonical, Ubuntu, 22.04 LTS, 'Virtual server type (instance type)' as t2.micro, 'Firewall (security group)' as New security group, and 'Storage (volumes)' as 1 volume(s) - 8 GiB. A 'Launch instance' button is visible at the bottom right.

Step 5: Check all the 3 check boxes. Then click on Launch Instance.

Launch an instance | EC2 | ap-south-1

https://ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#LaunchInstances:

Services Search [Alt+S]

Mumbai Ankit Verma

Network Info

vpc-04d3f0c91f9f1eefc

Subnet Info

No preference (Default subnet in any availability zone)

Auto-assign public IP Info

Enable

Additional charges apply when outside of free tier allowance

Firewall (security groups) Info

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

We'll create a new security group called 'launch-wizard-5' with the following rules:

- ☒ Allow SSH traffic from
Helps you connect to your instance
Anywhere
0.0.0.0/0
- ☒ Allow HTTPS traffic from the internet
To set up an endpoint, for example when creating a web server
- ☒ Allow HTTP traffic from the internet
To set up an endpoint, for example when creating a web server

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 Info

1

Software Image (AMI)

Canonical, Ubuntu, 22.04 LTS, ...read more
ami-007020fd9c84e18c7

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 unavailable) instance usage on free

Cancel Launch instance Review commands

CloudShell Feedback

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Step 6: Click on instance id to enter into the instance.

Instances | EC2 | ap-south-1

https://ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#Instances:

Services Search [Alt+S]

Mumbai Ankit Verma

Instances (1) Info

Find Instance by attribute or tag (case-sensitive) All states

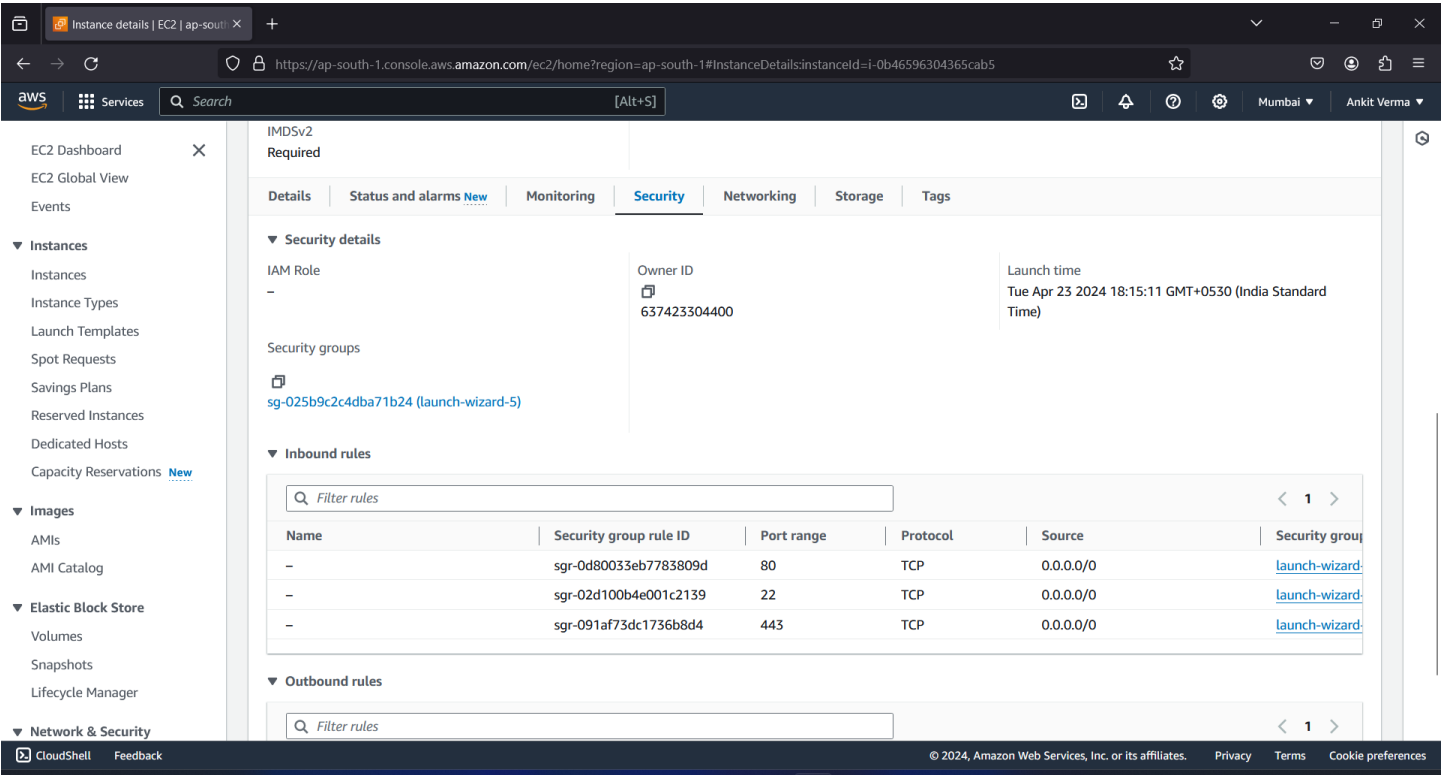
	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
<input type="checkbox"/>	Assg9	i-0b46596304365cab5	Running	t2.micro	Initializing	View alarms	ap-south-1a	ec2-43-205-212-98

Select an instance

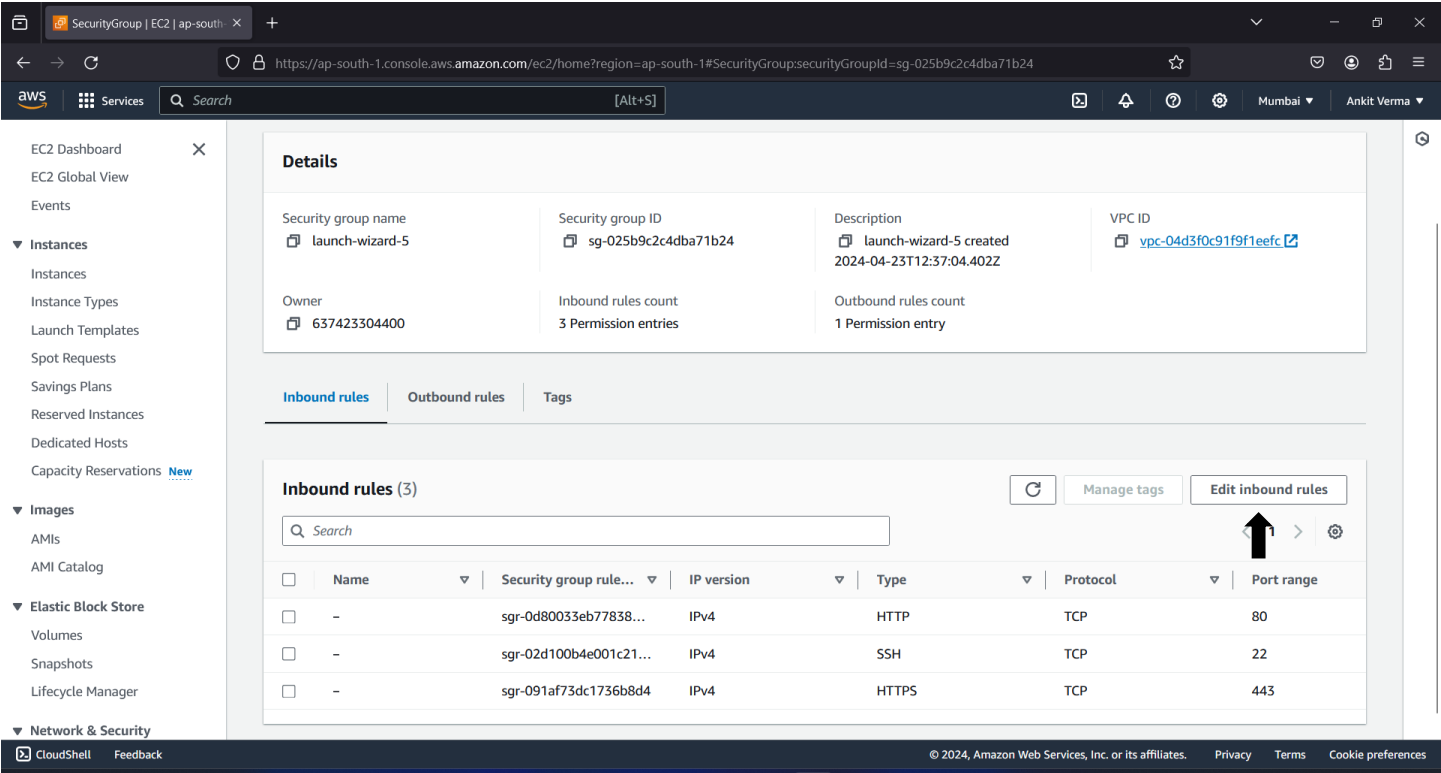
CloudShell Feedback

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

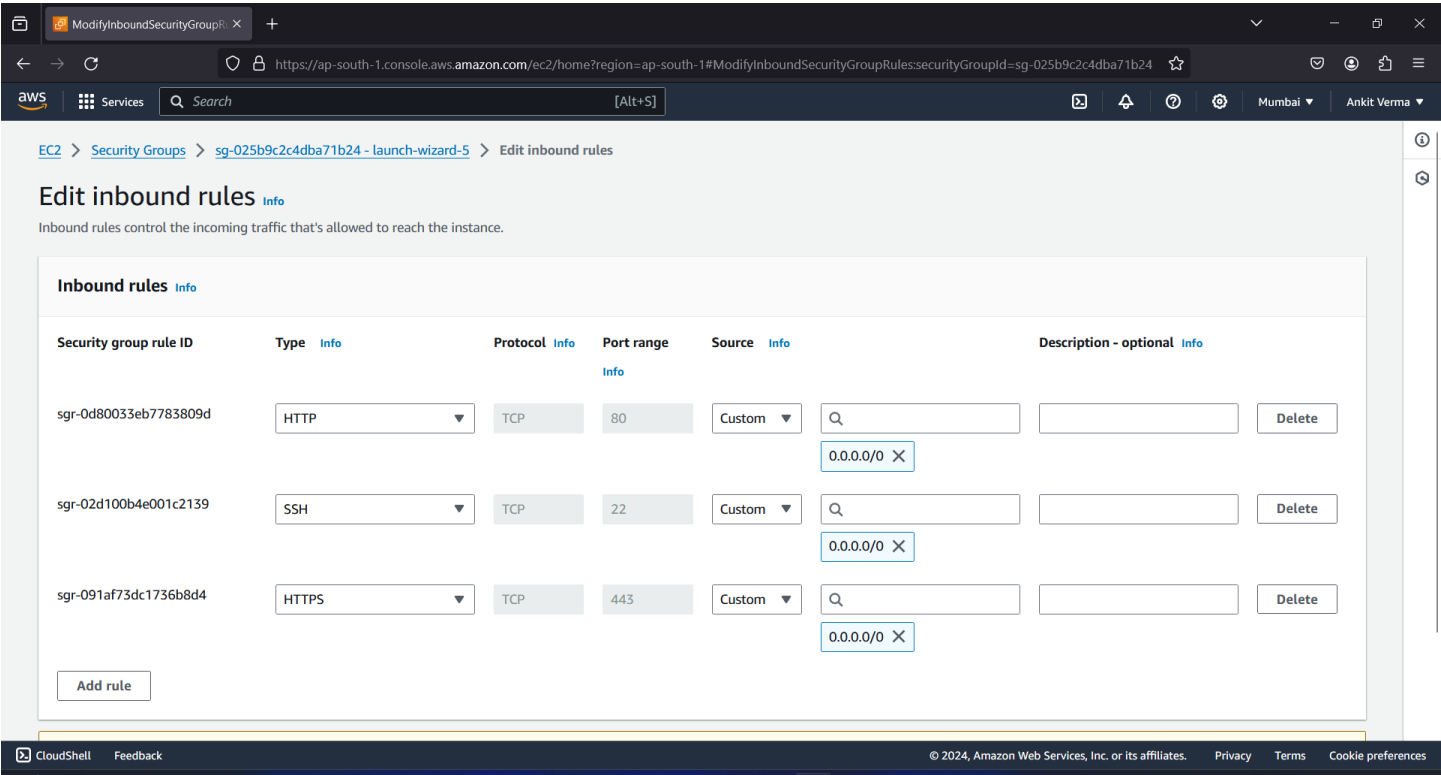
Step 7: Select the Security option & Click on the security group ID.



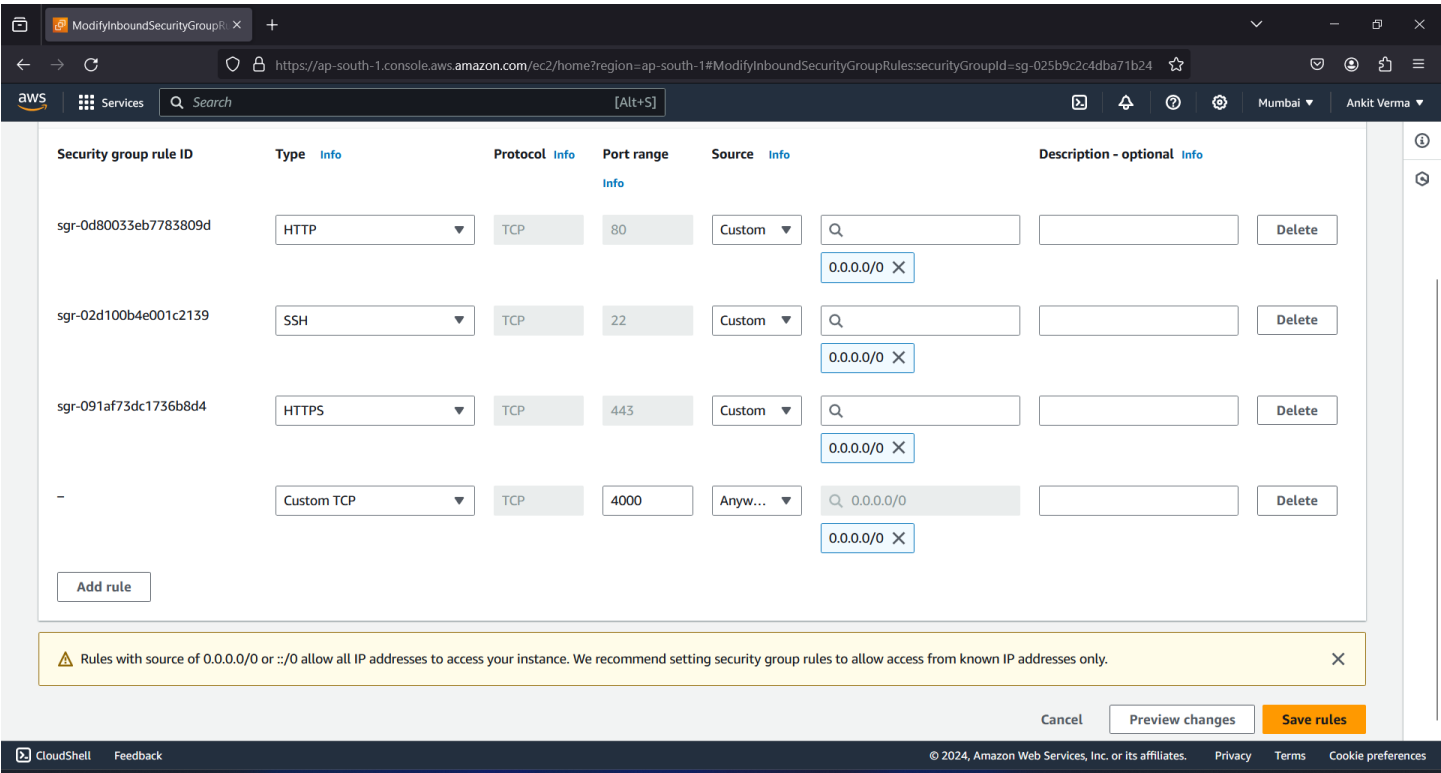
Step 8: Click on Edit Inbound Rules.



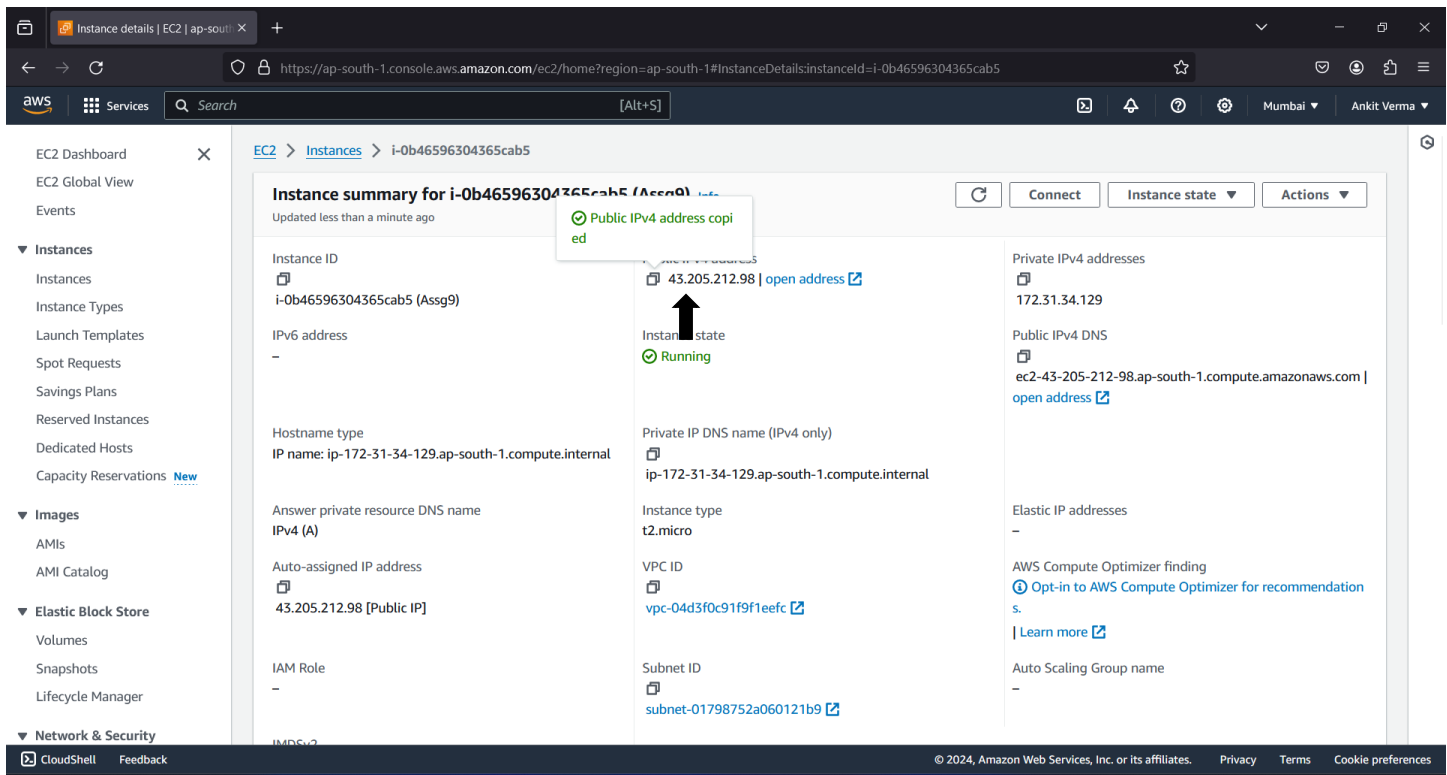
Step 9: Click on Add Rules.



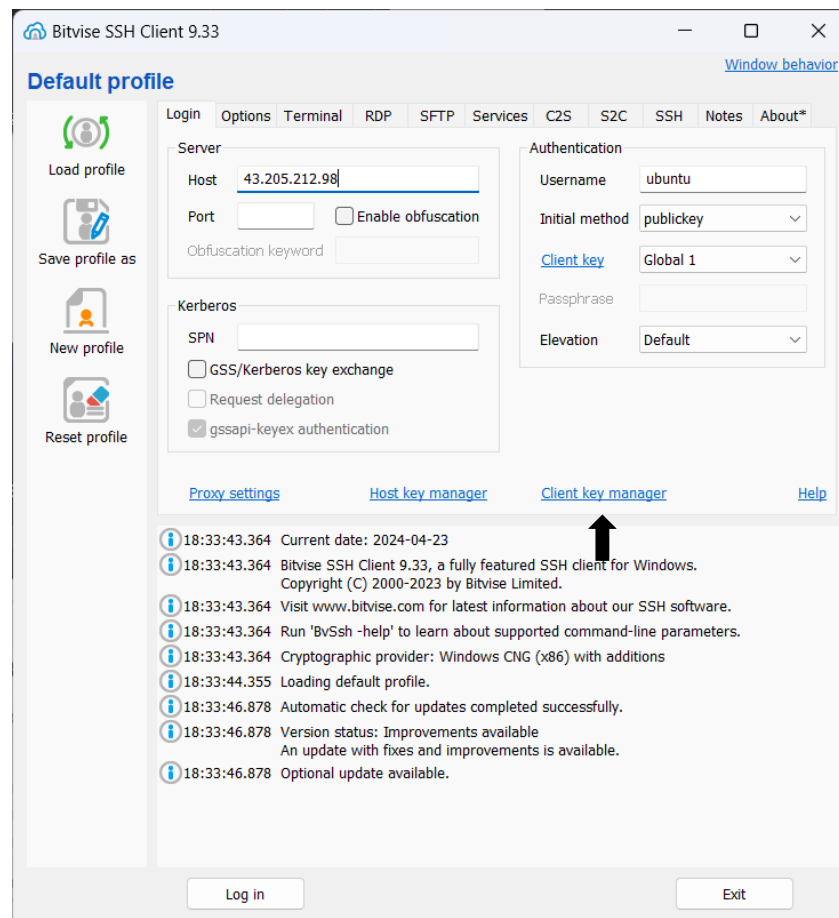
Step 10: Give the port no. 4000, in source info give 0.0.0.0/0. Then click on Save Rules.



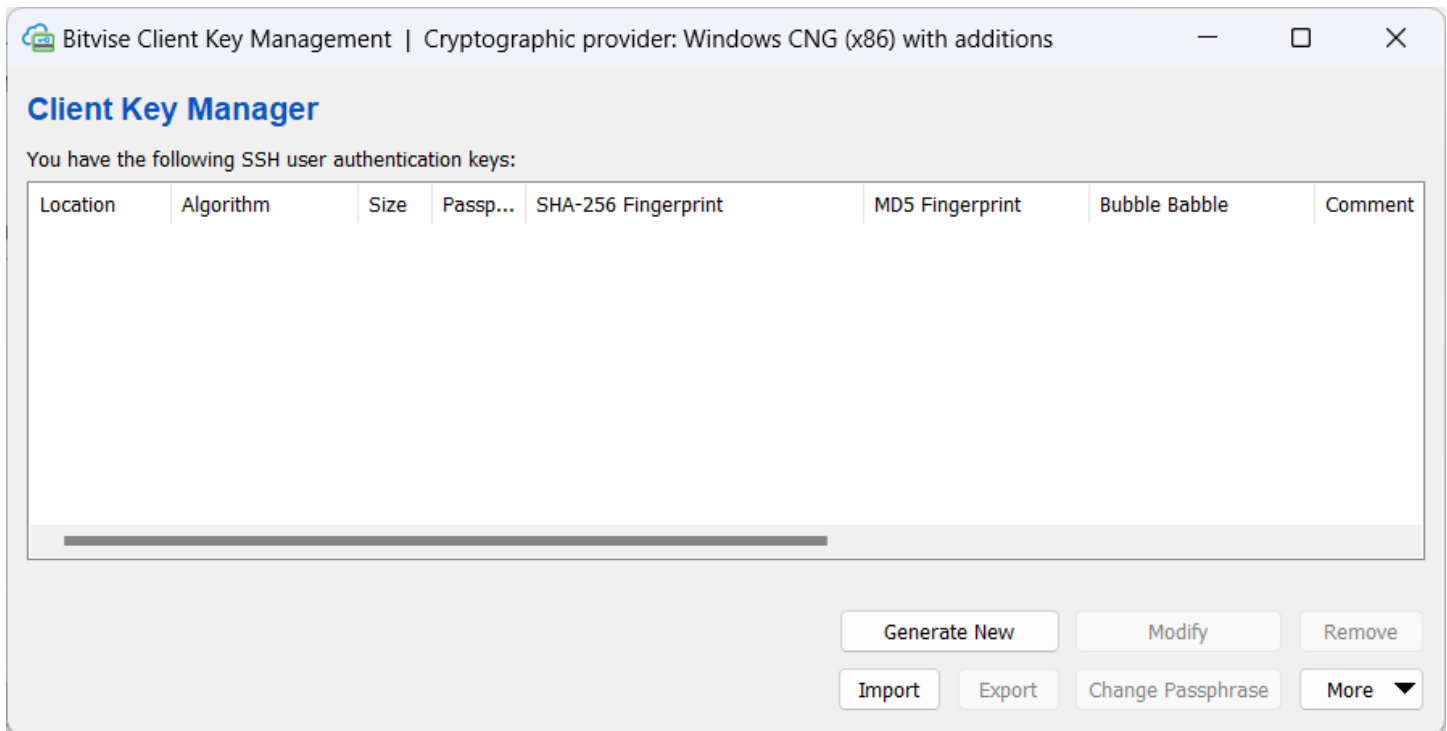
Step 11: Go back into the instance and copy the Public IPv4 Address.



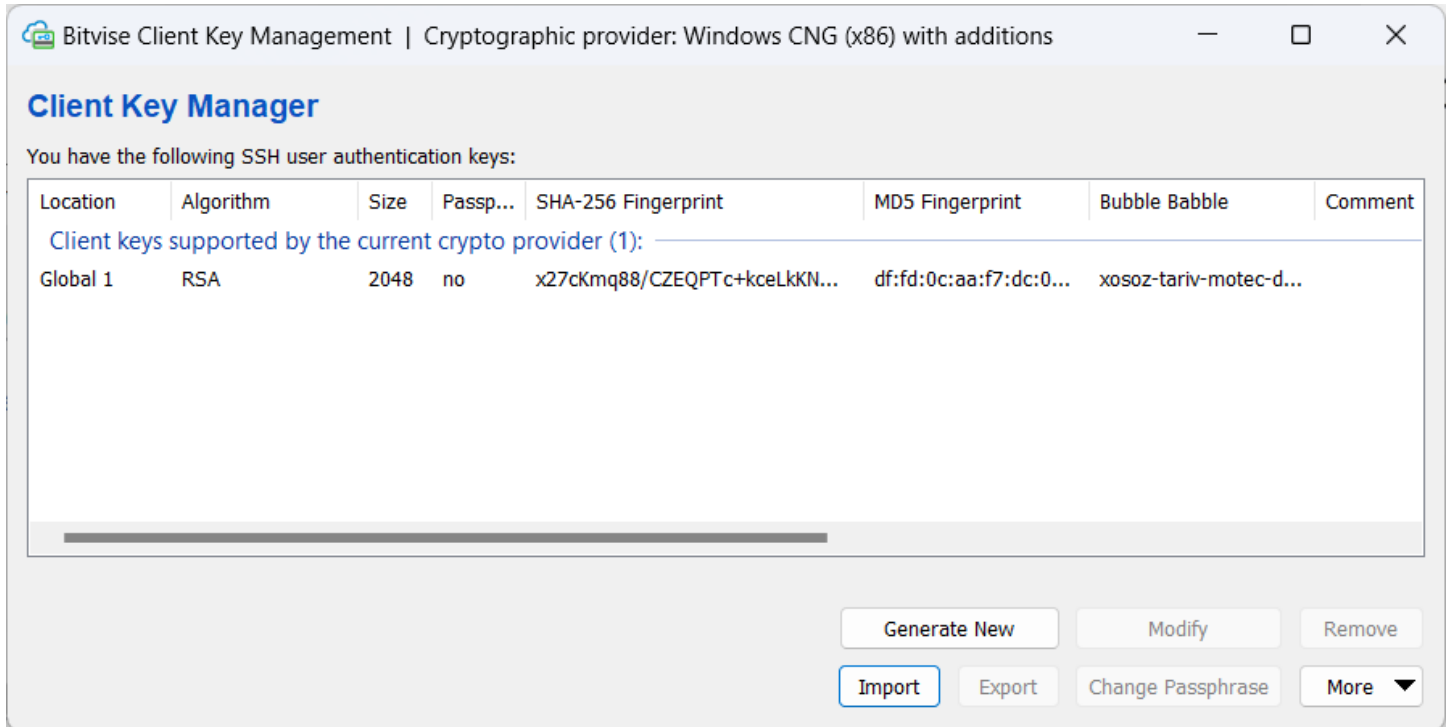
Step 12: Paste the address under the host tab. Under the Authentication tab, give the username as ubuntu, Initial method as publickey. Then click on Client Key Manager.



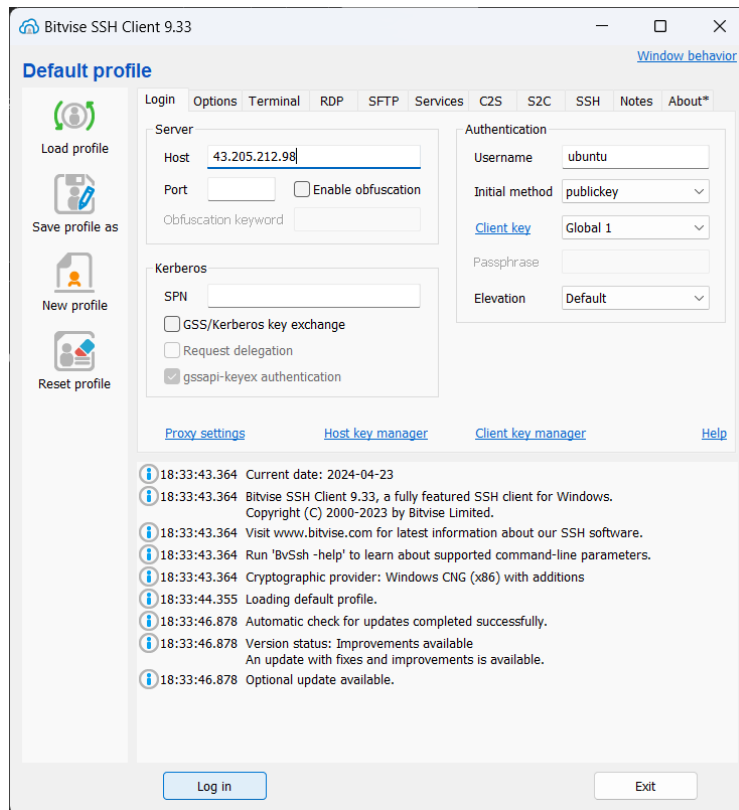
Step 13: Remove any previously selected key if any, the click on Import.



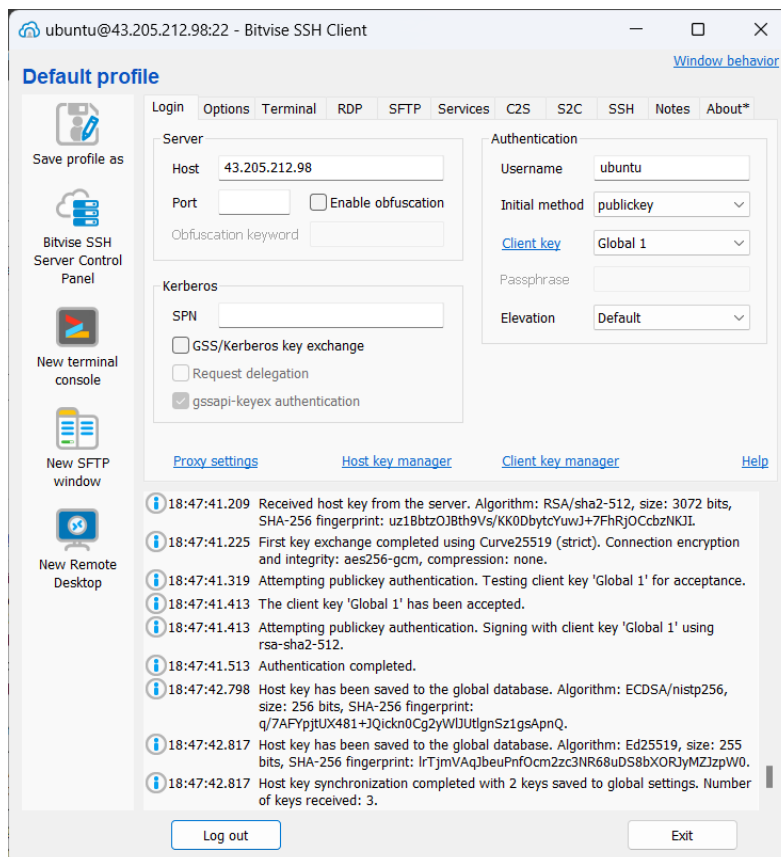
Step 14: Select the key using which instance was created. Then close the window.



Step 15: Then click “Log in”.



Step 16: Open a new terminal by clicking on New Terminal Console.



Step 17: In the console type the following commands in sequential order:

```
ubuntu@43.205.212.98:22 - Bitvise xterm - ubuntu@ip-172-31-34-129: ~  
  
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by  
applicable law.  
  
To run a command as administrator (user "root"), use "sudo <command>".  
See "man sudo_root" for details.  
  
ubuntu@ip-172-31-34-129:~$ pwd  
/home/ubuntu  
ubuntu@ip-172-31-34-129:~$ sudo apt-get update
```

```
ubuntu@43.205.212.98:22 - Bitvise xterm - ubuntu@ip-172-31-34-129: ~  
  
n-en [162 kB]  
Get:35 http://security.ubuntu.com/ubuntu jammy-security/universe amd64 c-n-  
f Metadata [16.8 kB]  
Get:36 http://security.ubuntu.com/ubuntu jammy-security/multiverse amd64 Pa  
ckages [37.2 kB]  
Get:37 http://security.ubuntu.com/ubuntu jammy-security/multiverse Translat  
ion-en [7588 B]  
Get:38 http://security.ubuntu.com/ubuntu jammy-security/multiverse amd64 c-  
n-f Metadata [260 B]  
Fetched 31.0 MB in 6s (5360 kB/s)  
Reading package lists... Done  
ubuntu@ip-172-31-34-129:~$ sudo apt-get upgrade
```

```
ubuntu@43.205.212.98:22 - Bitvise xterm - ubuntu@ip-172-31-34-129: ~  
  
systemctl restart systemd-networkd.service  
systemctl restart systemd-resolved.service  
systemctl restart systemd-udevd.service  
systemctl restart unattended-upgrades.service  
systemctl restart user@1000.service  
  
No containers need to be restarted.  
  
No user sessions are running outdated binaries.  
  
No VM guests are running outdated hypervisor (qemu) binaries on this host.  
ubuntu@ip-172-31-34-129:~$ sudo apt-get install nginx
```

```
ubuntu@43.205.212.98:22 - Bitvise xterm - ubuntu@ip-172-31-34-129: ~
systemctl restart unattended-upgrades.service
systemctl restart user@1000.service

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
ubuntu@ip-172-31-34-129:~$ nginx -v
nginx version: nginx/1.18.0 (Ubuntu)
ubuntu@ip-172-31-34-129:~$ curl -SL https://deb.nodesource.com/setup_16.x|sudo -E bash -
```

```
ubuntu@43.205.212.98:22 - Bitvise xterm - ubuntu@ip-172-31-34-129: ~
Get:4 https://deb.nodesource.com/node_16.x nodistro InRelease [12.1 kB]
Hit:5 http://security.ubuntu.com/ubuntu jammy-security InRelease
Get:6 https://deb.nodesource.com/node_16.x nodistro/main amd64 Packages [7462 B]
Fetched 19.6 kB in 1s (19.9 kB/s)
Reading package lists... Done
2024-04-23 13:35:23 - Repository configured successfully. To install Node.js, run: apt-get install n
odejs -y
ubuntu@ip-172-31-34-129:~$ sudo apt install nodejs
```

```
ubuntu@43.205.212.98:22 - Bitvise xterm - ubuntu@ip-172-31-34-129: ~
No containers need to be restarted.

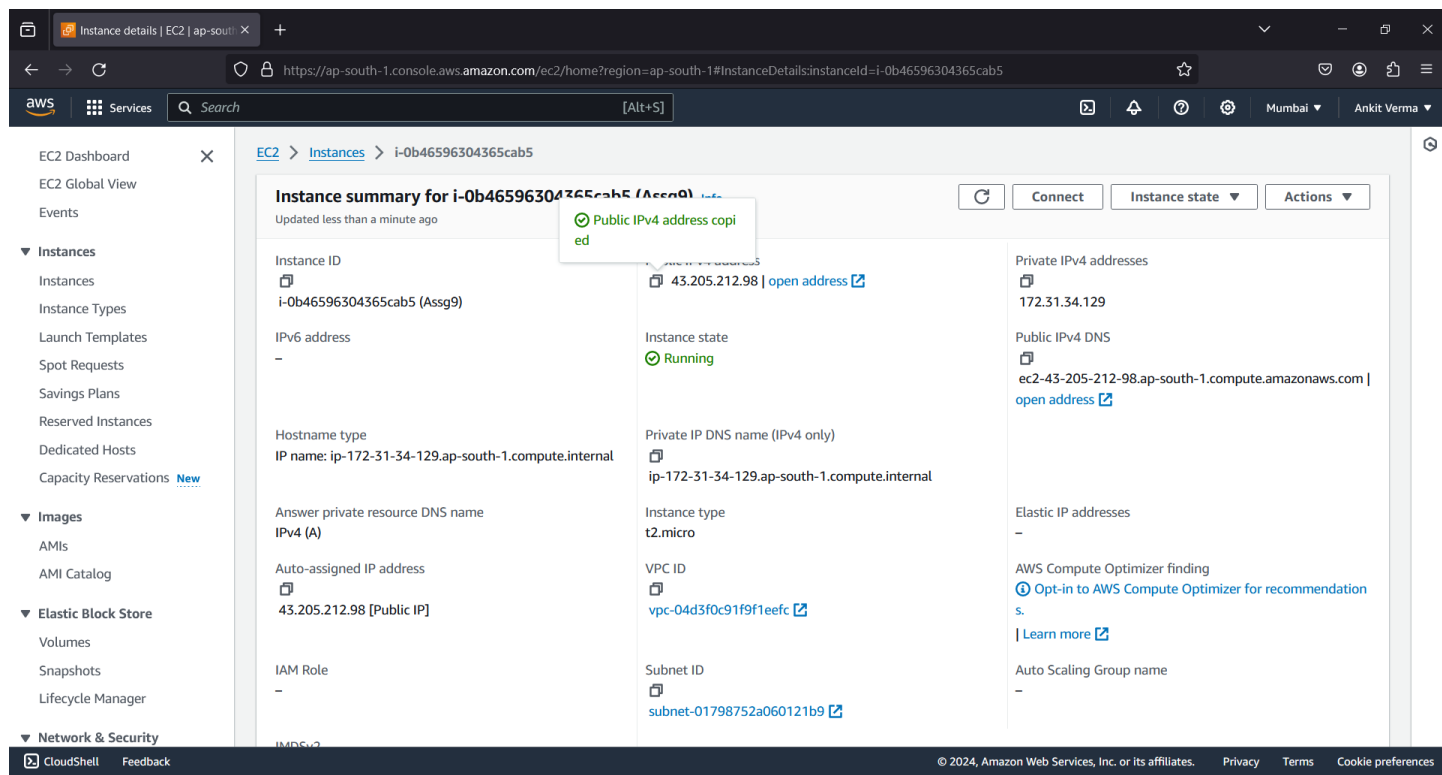
No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
ubuntu@ip-172-31-34-129:~$ node -v
v16.20.2
ubuntu@ip-172-31-34-129:~$
```

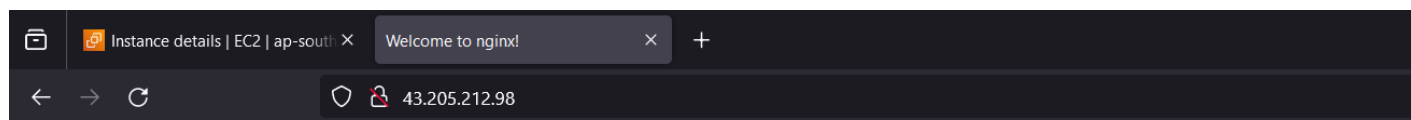
```
ubuntu@43.205.212.98:22 - Bitvise xterm - ubuntu@ip-172-31-34-129: ~/repo007/Repo07
ubuntu@ip-172-31-34-129:~/repo007$ git clone https://github.com/ankit11exe/Repo07.git
Cloning into 'Repo07'...
remote: Enumerating objects: 6, done.
remote: Counting objects: 100% (6/6), done.
remote: Compressing objects: 100% (6/6), done.
remote: Total 6 (delta 0), reused 0 (delta 0), pack-reused 0
Receiving objects: 100% (6/6), 48.75 KiB | 4.88 MiB/s, done.
ubuntu@ip-172-31-34-129:~/repo007$ cd Repo07
ubuntu@ip-172-31-34-129:~/repo007/Repo07$ npm install
npm WARN deprecated uuid@3.4.0: Please upgrade to version 7 or higher. Older versions may use Math
```

```
ubuntu@43.205.212.98:22 - Bitvise xterm - ubuntu@ip-172-31-34-129: ~/repo007/Repo07
npm notice
npm notice New major version of npm available! 8.19.4 -> 10.5.2
npm notice Changelog: https://github.com/npm/cli/releases/tag/v10.5.2
npm notice Run npm install -g npm@10.5.2 to update!
npm notice
ubuntu@ip-172-31-34-129:~/repo007/Repo07$ npm -v
8.19.4
ubuntu@ip-172-31-34-129:~/repo007/Repo07$ node index.js
Started server
```

Step 18: From the Public IPv4 Address click Open Address.



Step 19: Nginx window will open. Now add :4000 at the end of the IPv4 Address.



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.

Step 20: The Nodejs file content will be visible.

