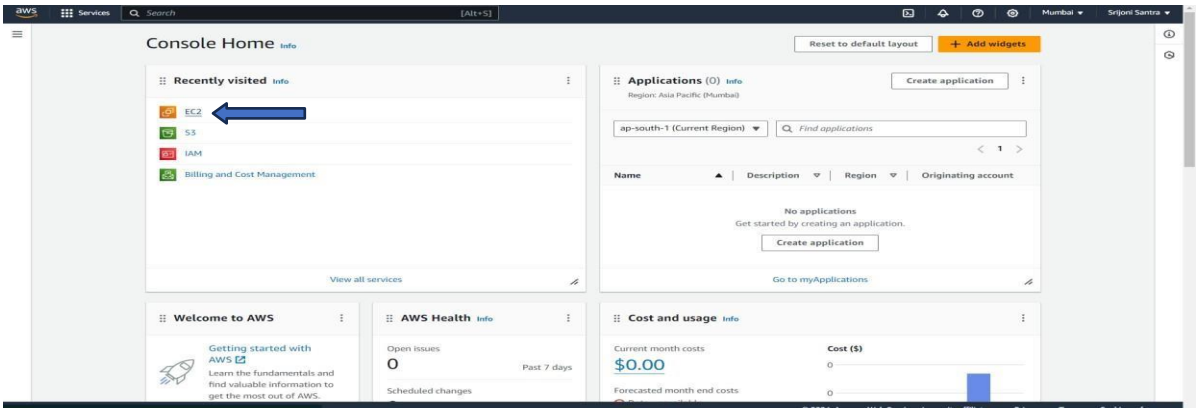
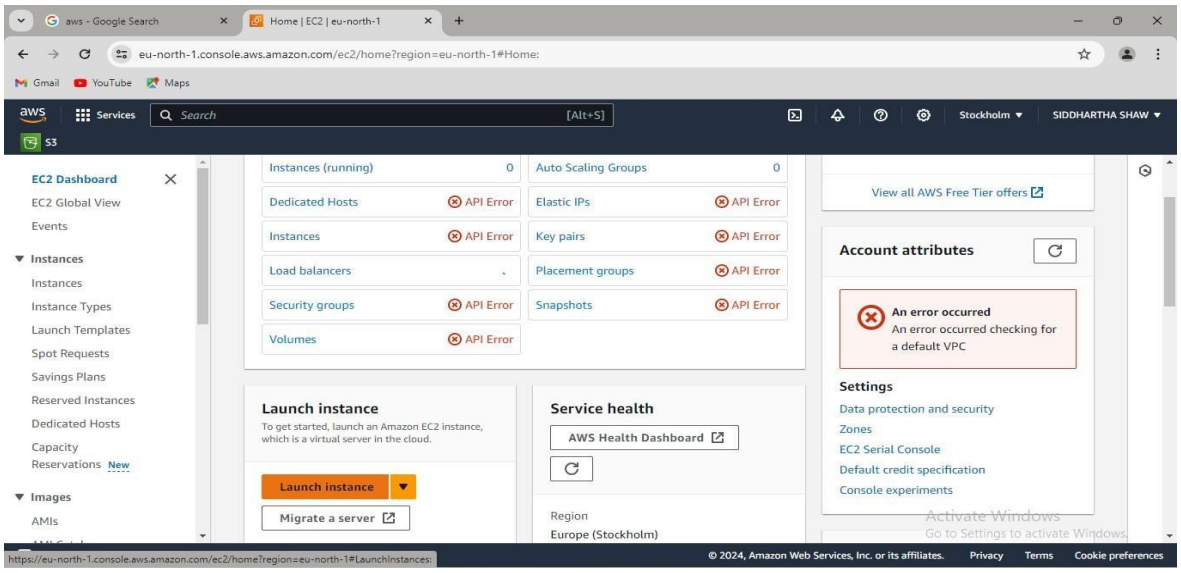
ASSIGNMENT-12

Problem Statement: Deploy and run the project in AWS without using port.

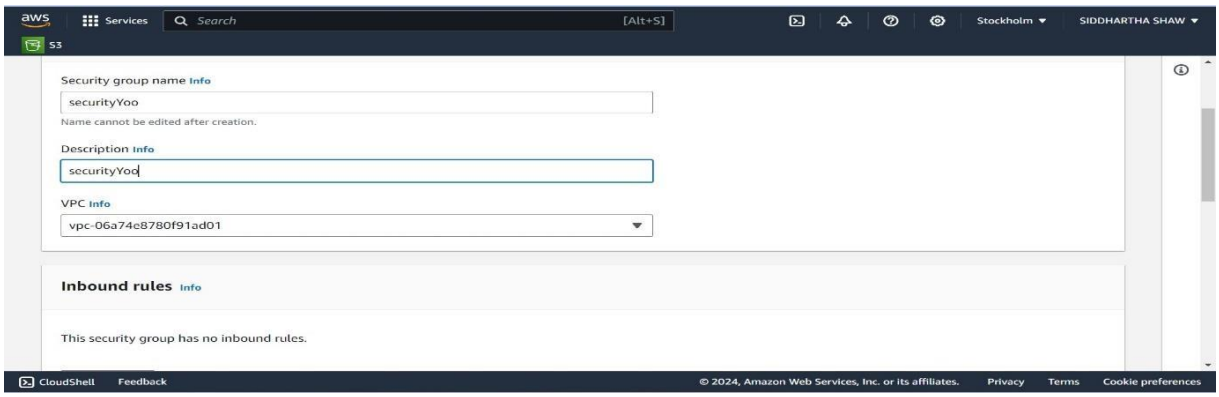
Step 1: Login to the console and click on **EC2**.



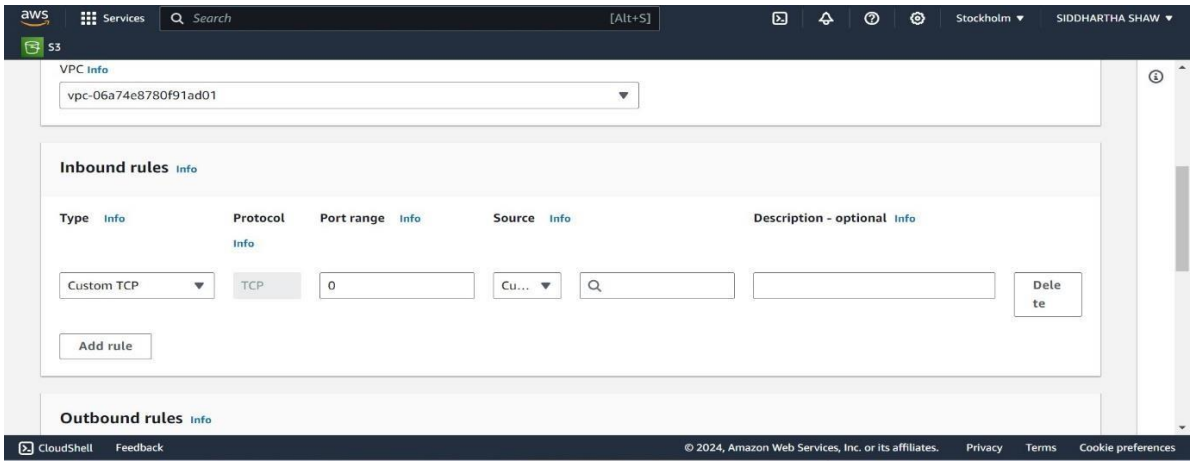
Step 2: Then click on Security Groups.

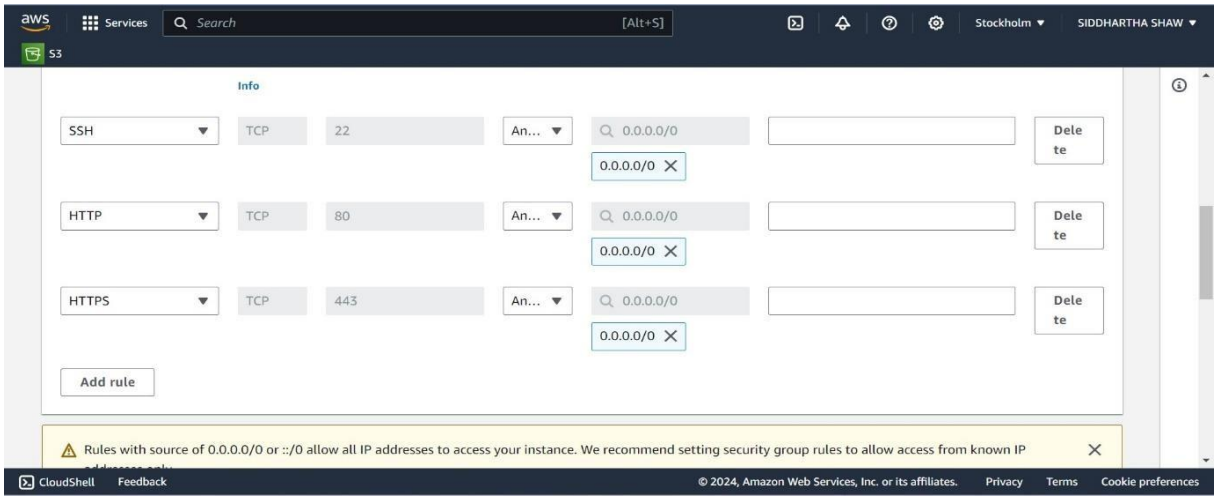


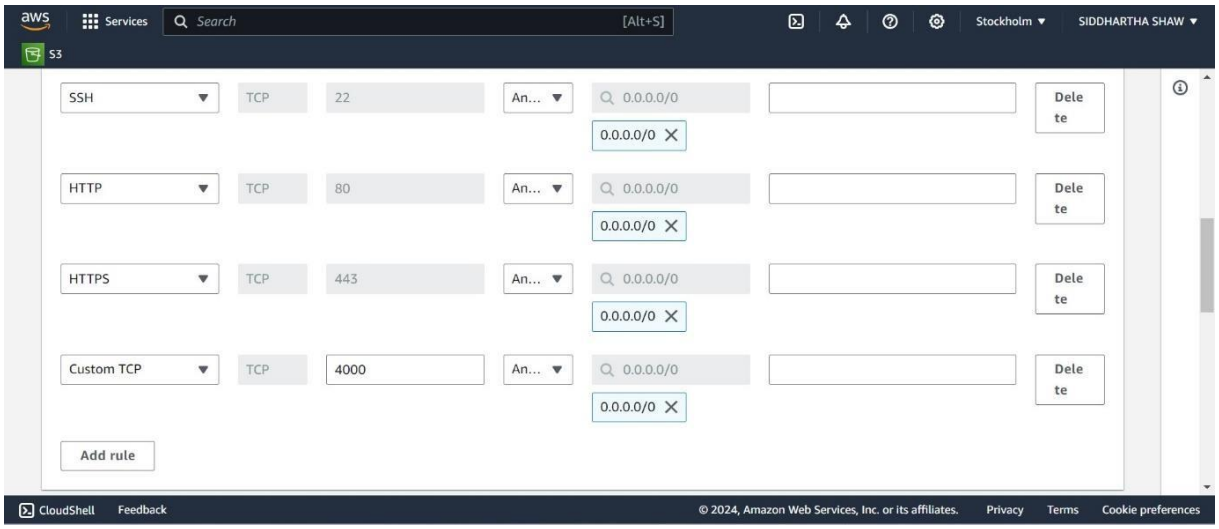
Step 3: Then go to the “Create Security group”



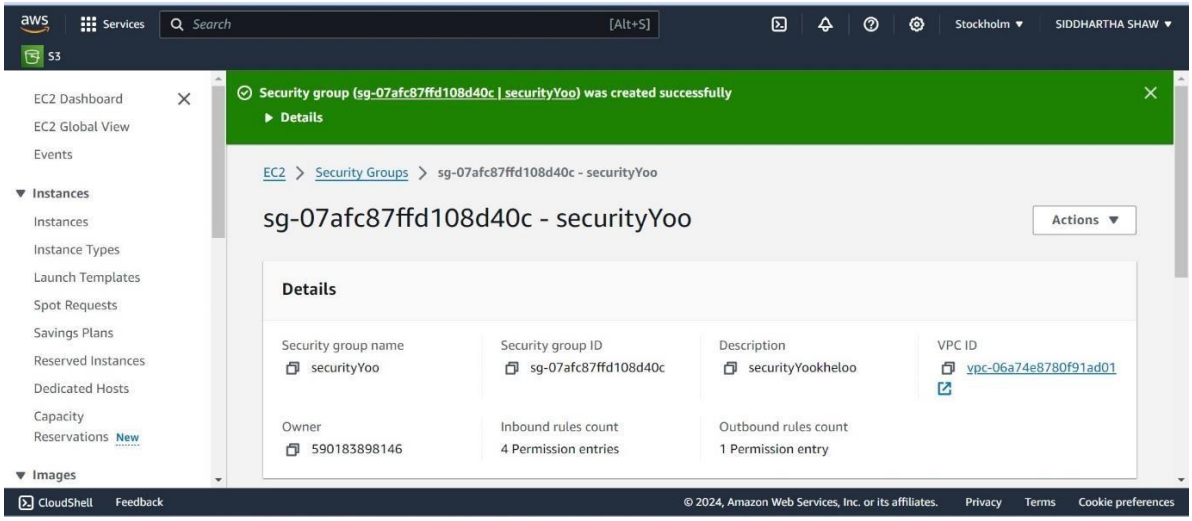
Step 4: Write security group name, add inbound rules and click on “Create security group”.



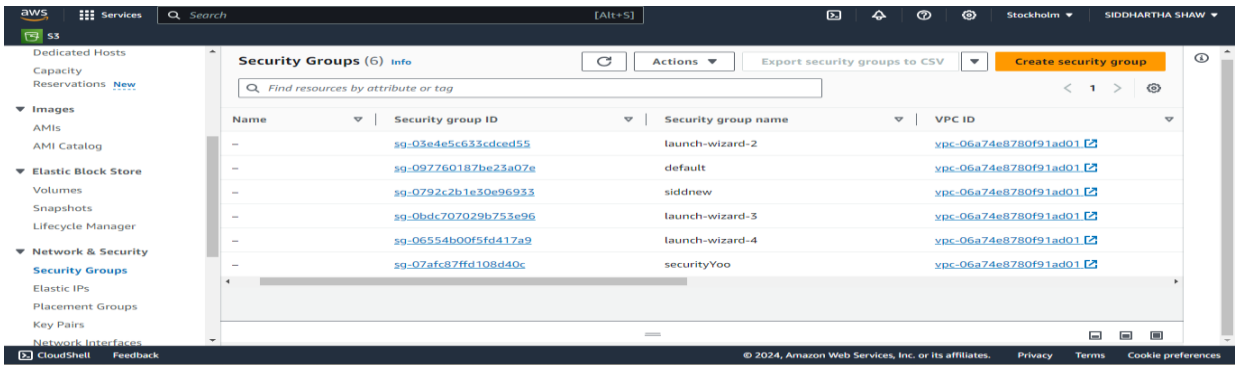




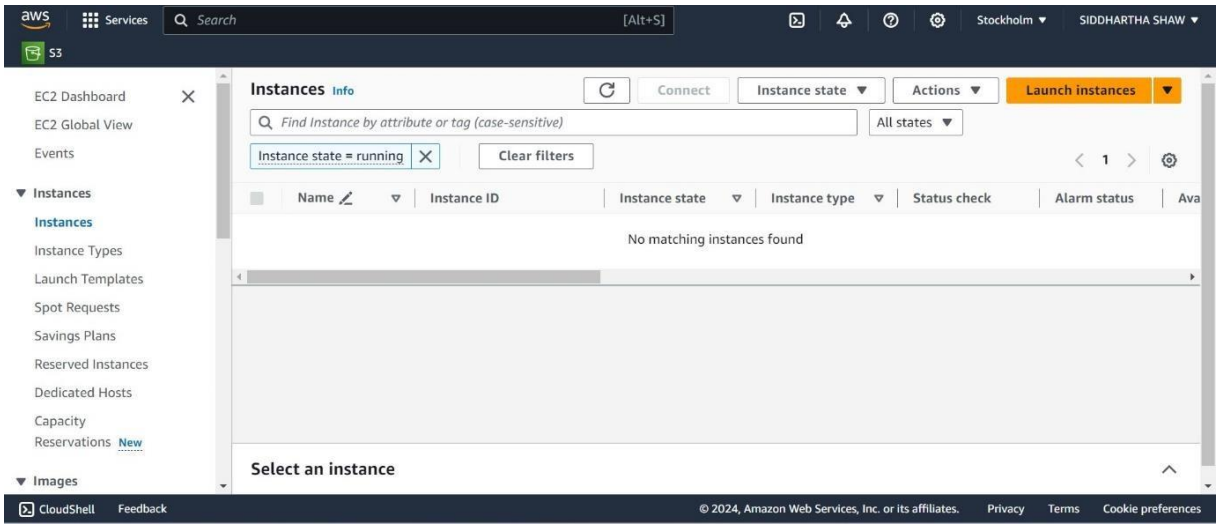
Step 5: after that security group is created successfully.

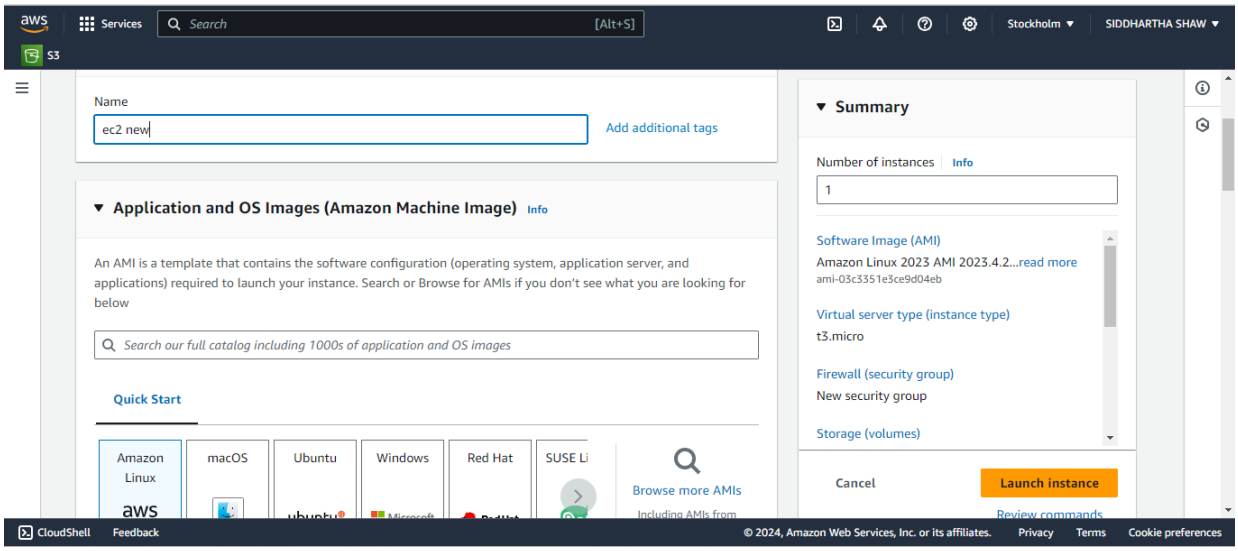


Step 6: Now check the security group activity whether its shows all port number or not.

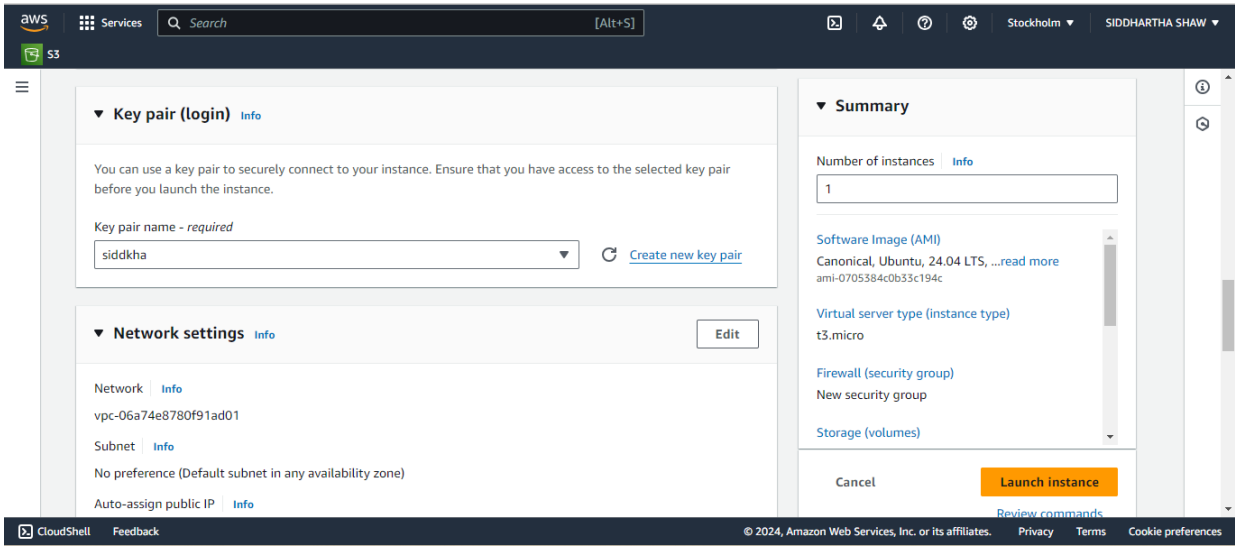

aws
Services
Search
[Alt+S]
S3
Stockholm
SIDDHARTHA SHAW
Dedicated Hosts
Capacity Reservations New
Images
AMIs
AMI Catalog
Elastic Block Store
Volumes
Snapshots
Lifecycle Manager
Network & Security
Security Groups
Elastic IPs
Placement Groups
Key Pairs
Network Interfaces
Security Groups (6) Info
Actions
Export security groups to CSV
Create security group
Find resources by attribute or tag
1
Name
Security group ID
Security group name
VPC ID
– sg-03e4e5c633cdced55 launch-wizard-2 vpc-06a74e8780f91ad01
– sg-097760187be23a07e default vpc-06a74e8780f91ad01
– sg-0792c2b1e30e96933 siddnew vpc-06a74e8780f91ad01
– sg-0bdc707029b753e96 launch-wizard-3 vpc-06a74e8780f91ad01
– sg-06554b00f5fd417a9 launch-wizard-4 vpc-06a74e8780f91ad01
– sg-07afc87ffd108d40c securityYoo vpc-06a74e8780f91ad01
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Step 7: The security group is created. Now go to the EC2 and click on “Launch Instances”.

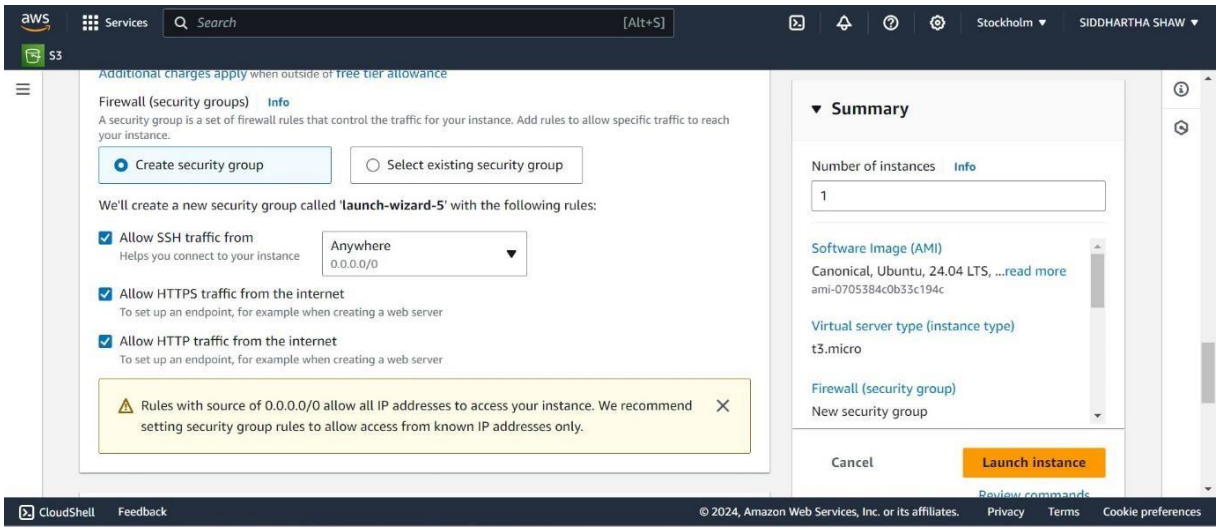




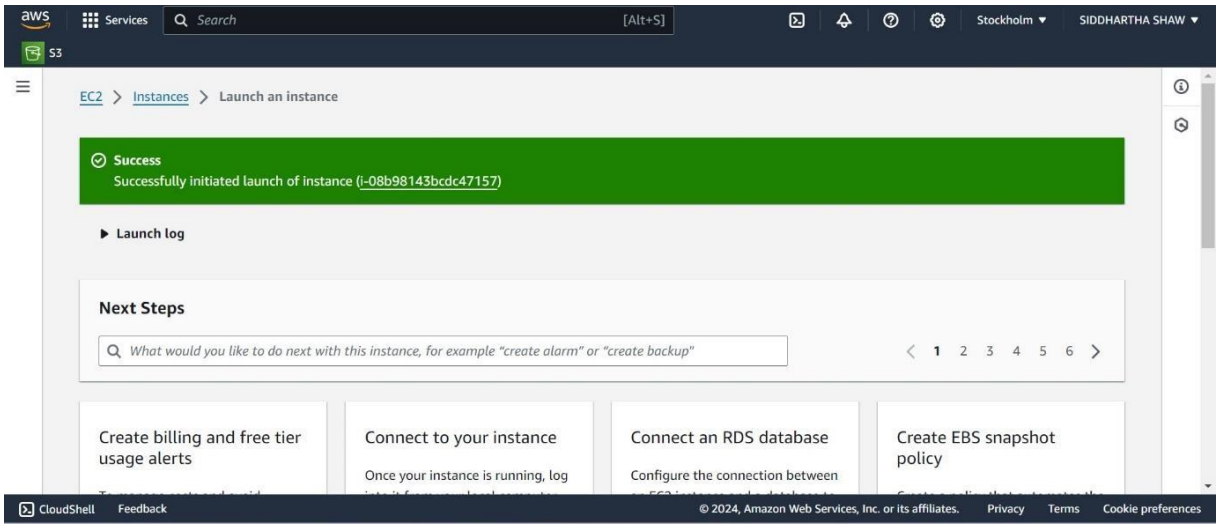
Step 8: search the existing key pair whether its already created.


aws
Services
Search
[Alt+S]
Stockholm
SIDDHARTHA SHAW
S3
Key pair (login) Info
You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.
Key pair name - required
siddkha
Create new key pair
Network settings Info
Edit
Network Info
vpc-06a74e8780f91ad01
Subnet Info
No preference (Default subnet in any availability zone)
Auto-assign public IP Info
Summary
Number of instances Info
1
Software Image (AMI)
Canonical, Ubuntu, 24.04 LTS, ...read more
ami-0705384c0b33c194c
Virtual server type (instance type)
t3.micro
Firewall (security group)
New security group
Storage (volumes)
Cancel
Launch instance
Review commands
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

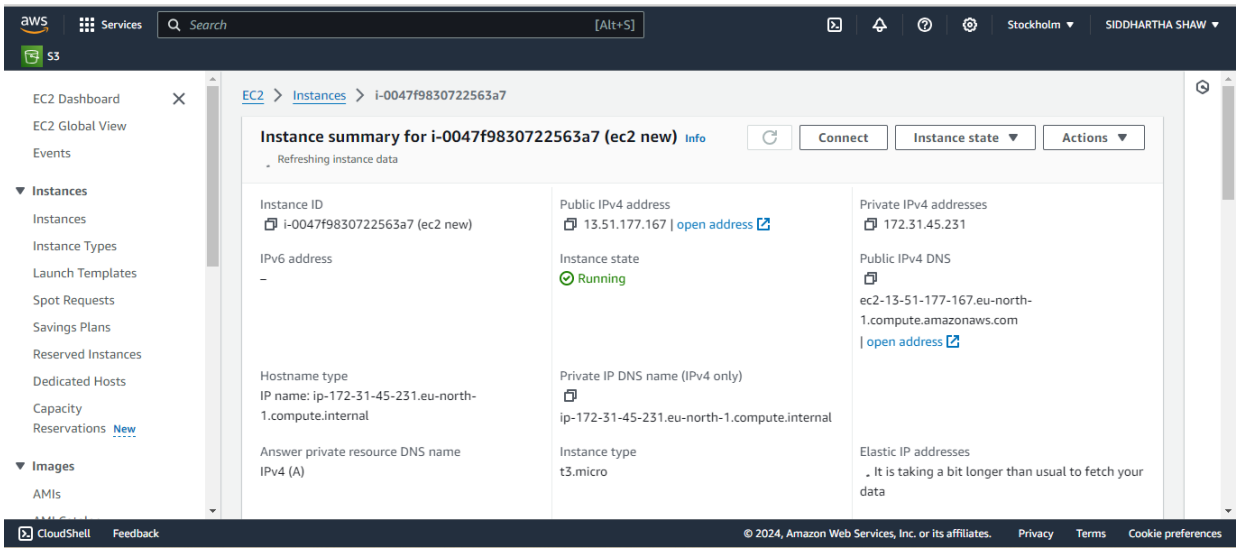
Step 9: select the SSH, HTTPS,HTTP and move it.



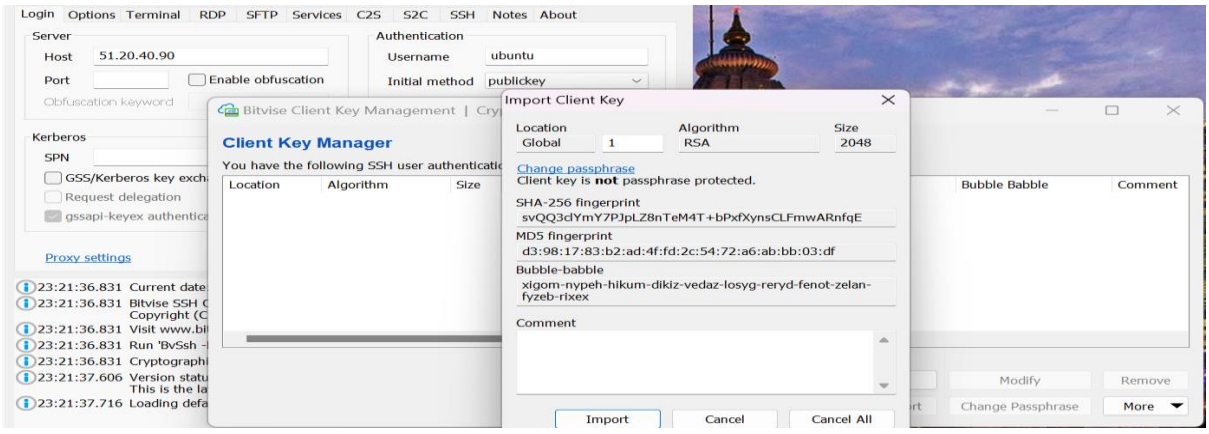
Step 10: after that the instance lunch successfully.



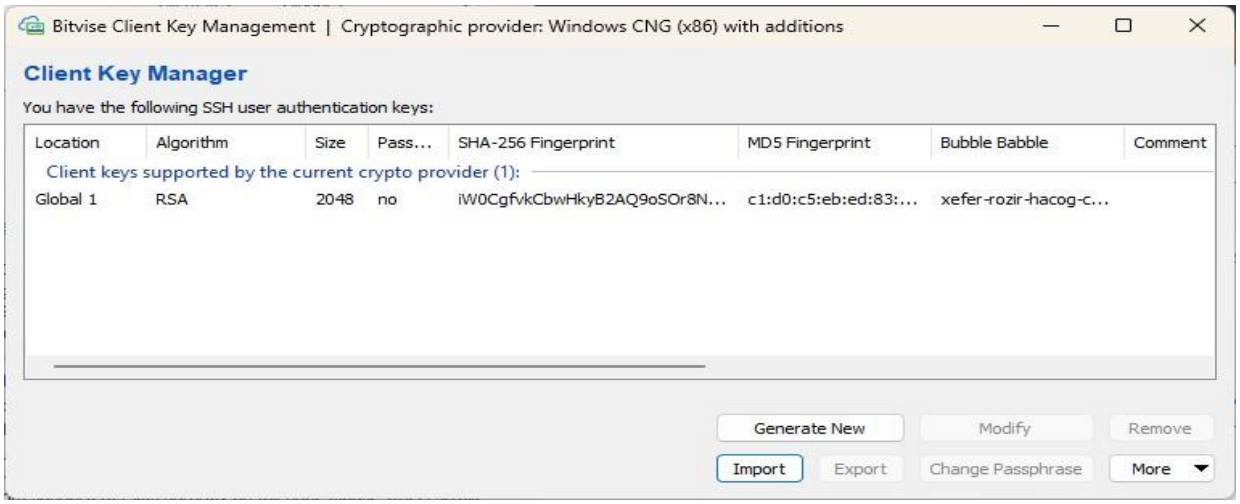
Step 11: Go back to the Instance, copy the "Public IPv4 address".



Step 12: In "Bitvise SSH Client", paste the "Public IPv4 address" in "Host" and under "Authentication tab" give the username as Ubuntu. Then click on "Client Key Manager".



Step 13: after that "bitwise ssh client" creation process done.



Step 14: steps of further processes which is done in **command pannle** in "bitwise ssh client".

a. Remove any previously selected key if any, then click on "Import" & select the key which instance was created.

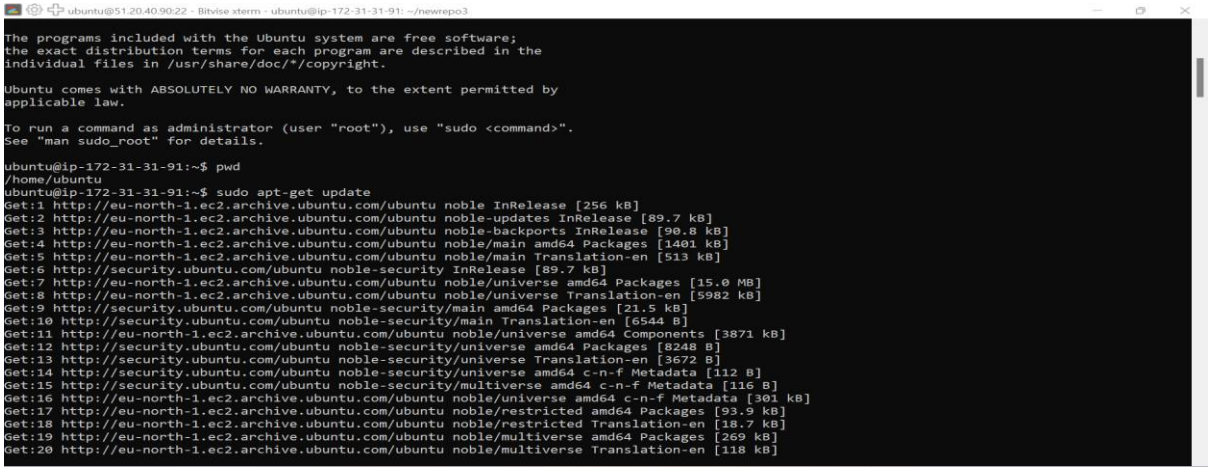
b. In "Bitvise SSH Client", click on "Log in".

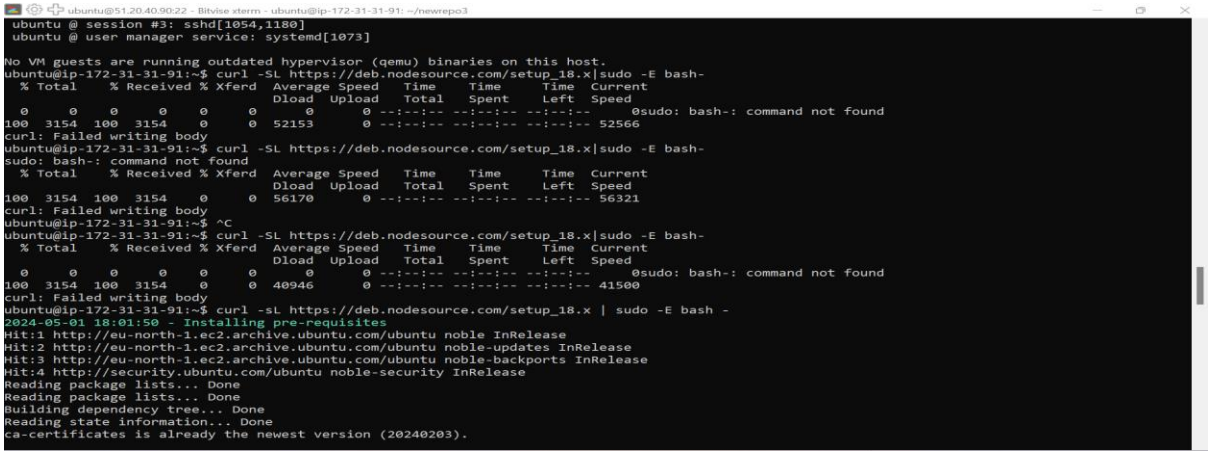
c. After successful "Log in" open a "New Terminal Console".

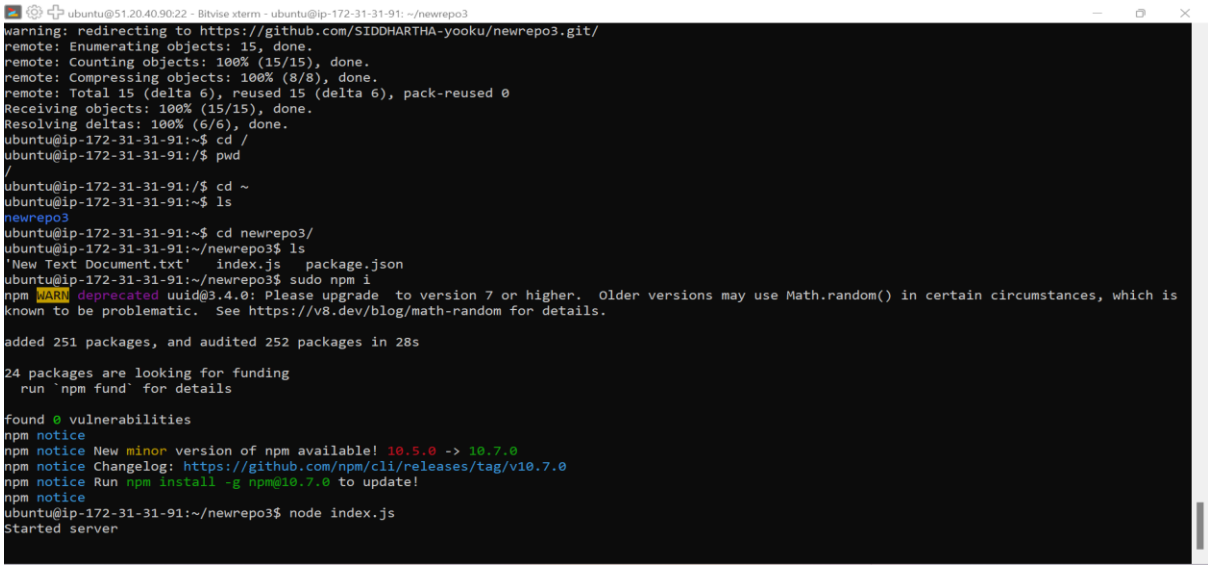
d. In the console, type the following commands in sequential order.

```
ubuntu@ip-172-31-27-221:~$ pwd
/home/ubuntu
ubuntu@ip-172-31-27-221:~$ sudo apt-get update
```

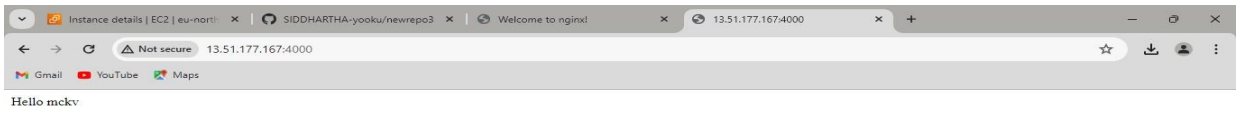
```
Fetched 30.7 MB in 6s (5382 kB/s)
Reading package lists... Done
ubuntu@ip-172-31-27-221:~$ sudo apt-get upgrade
```



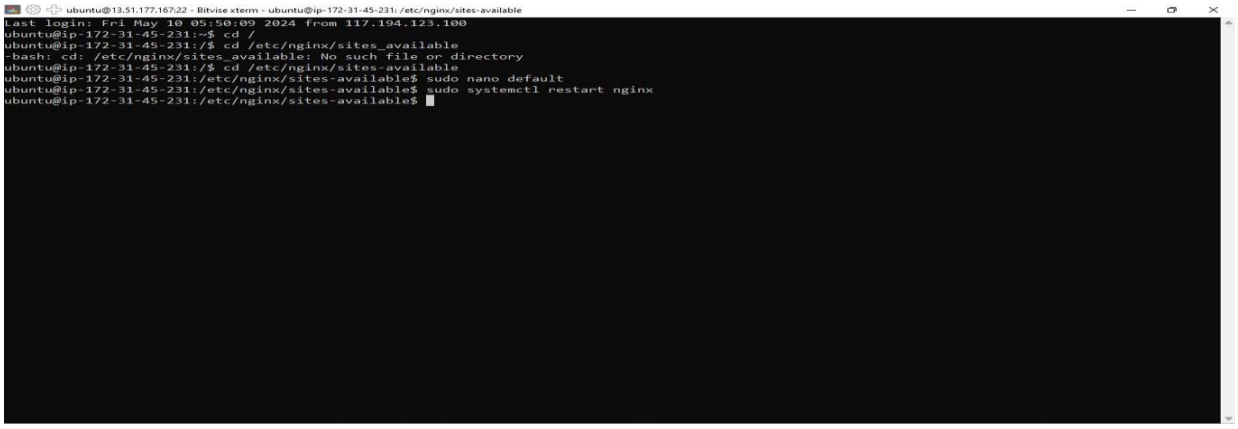




Step 15: after that we start the server and show that whether its running or not.



Step 16: Now we open another command pannle and go to the further process.



Step 17: Now type the commands and then go to the further steps--

In this step edit the **"location"** part only with -

location / { proxy_pass http://localhost:4000;

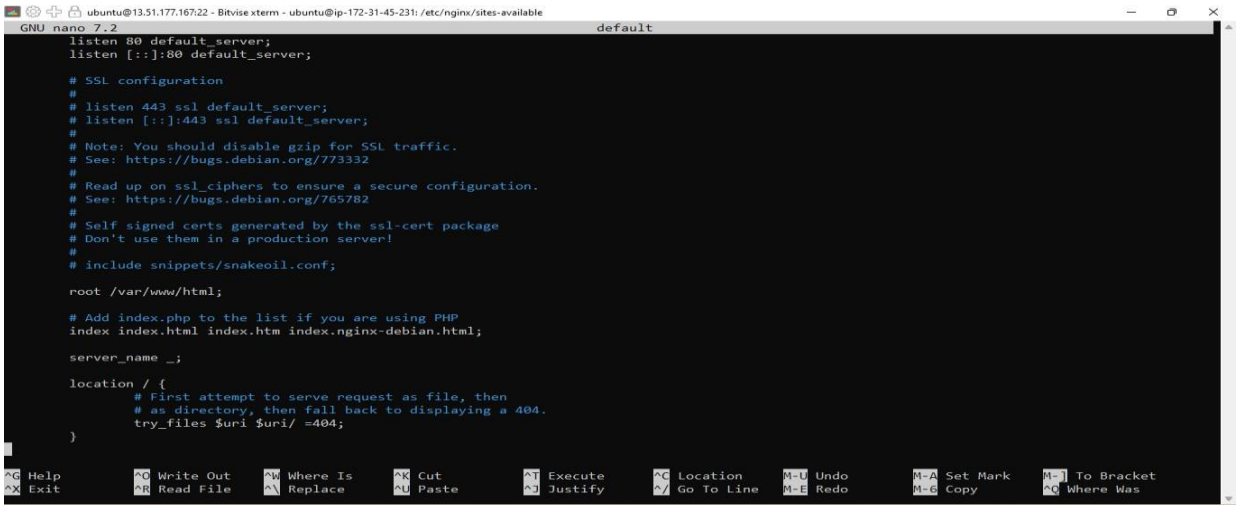
proxy_http_version 1.1;

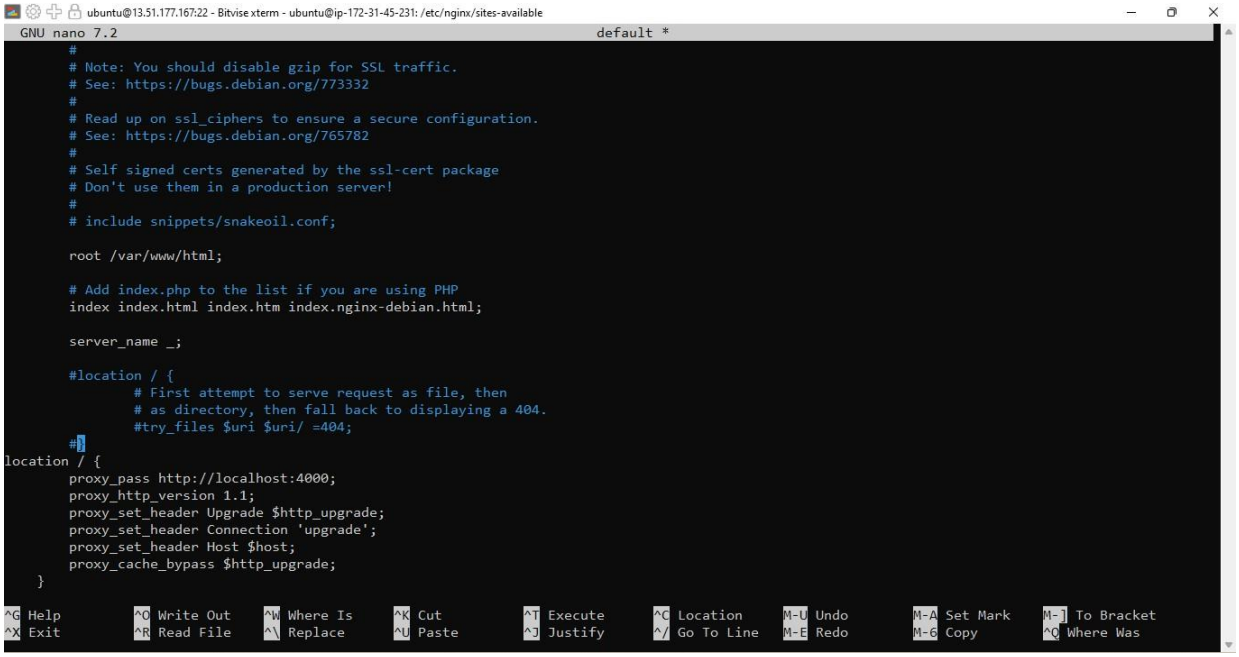
proxy_set_header Upgrade $http_upgrade;

proxy_set_header Connection 'upgrade';

proxy_set_header Host $host;

proxy_cache_bypass $http_upgrade; }





Step 18: Now we saw that after one more time copy the **ipv4 address** of instance its running without using port(4000).