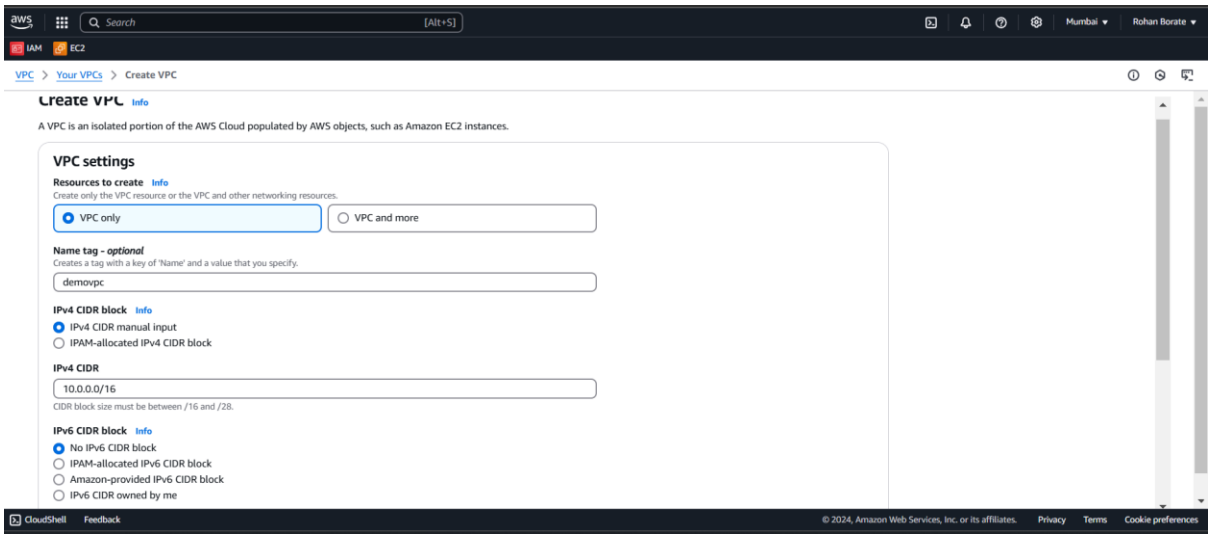
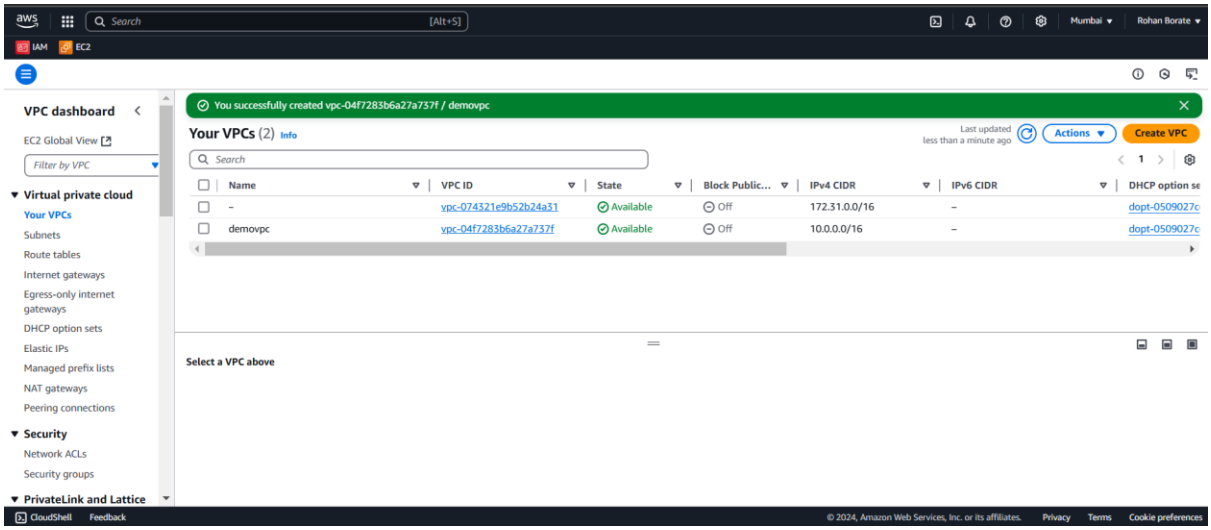
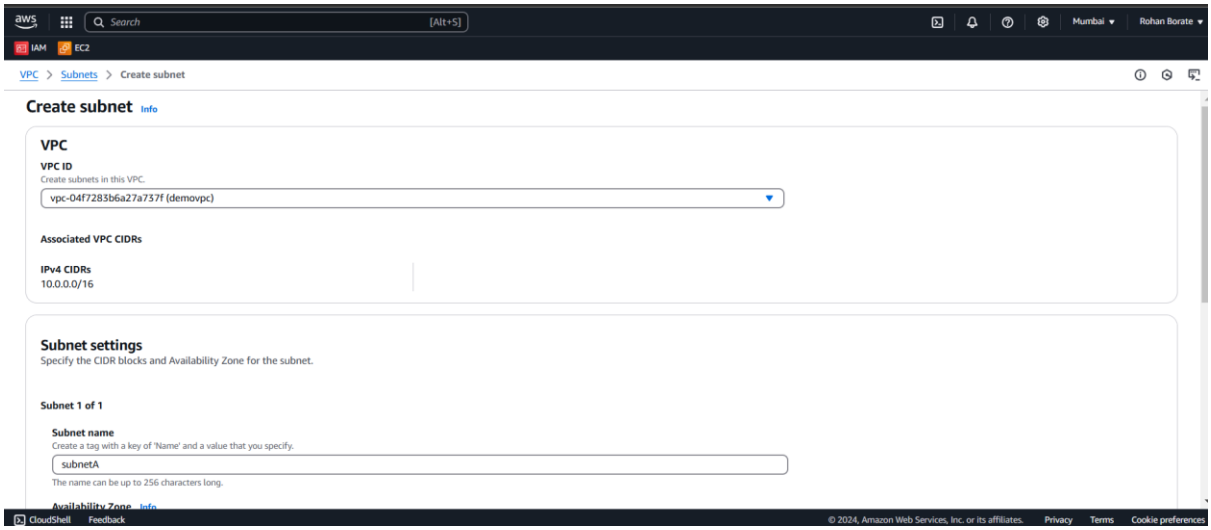
NACL_and_SecurityGroups

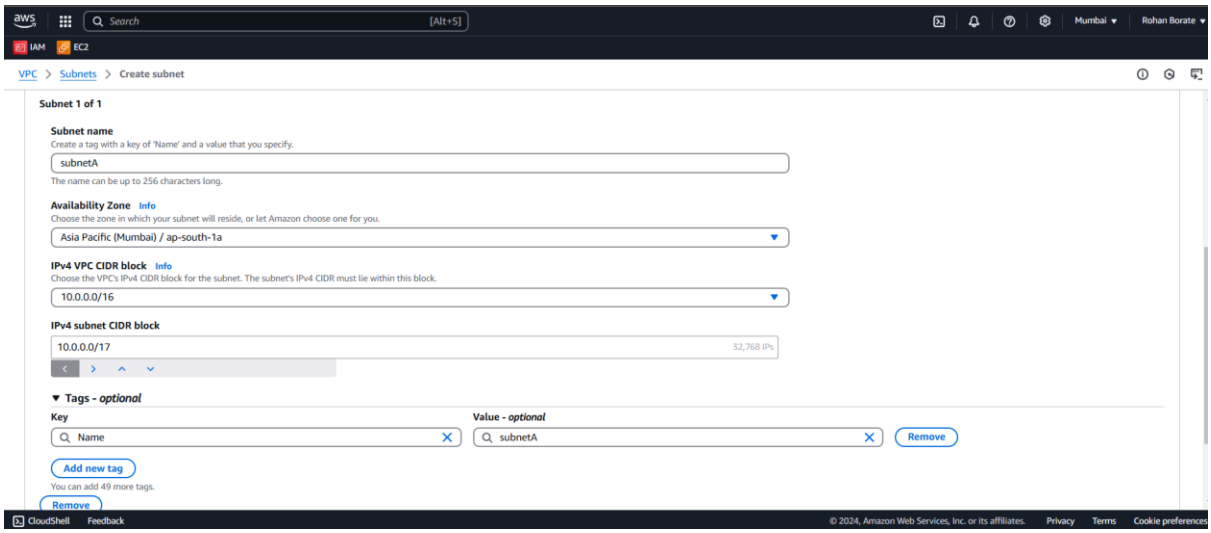
Create a VPC → demovpc

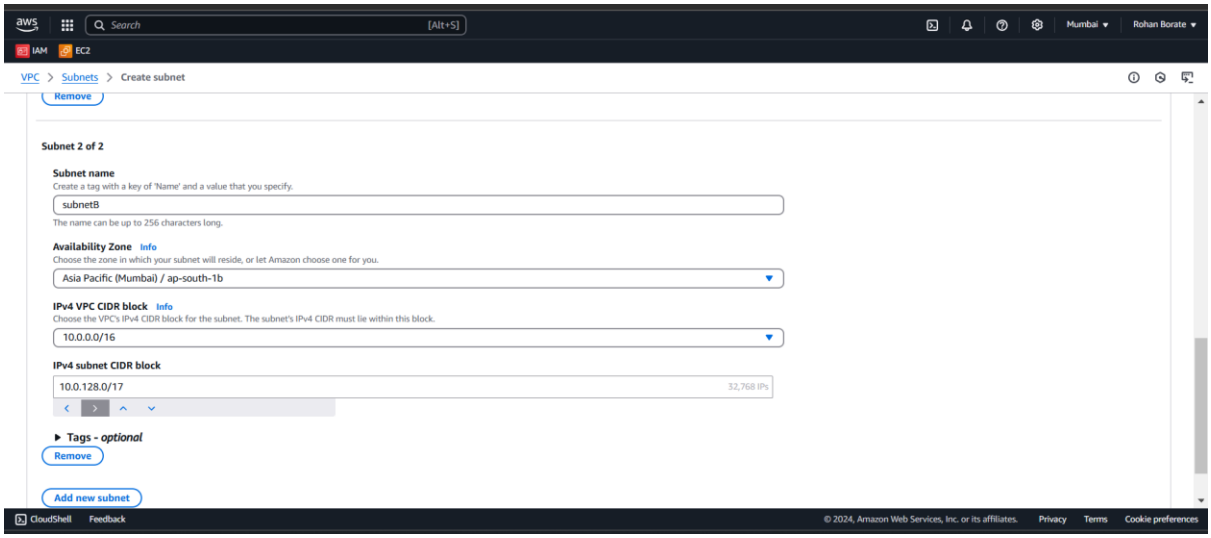


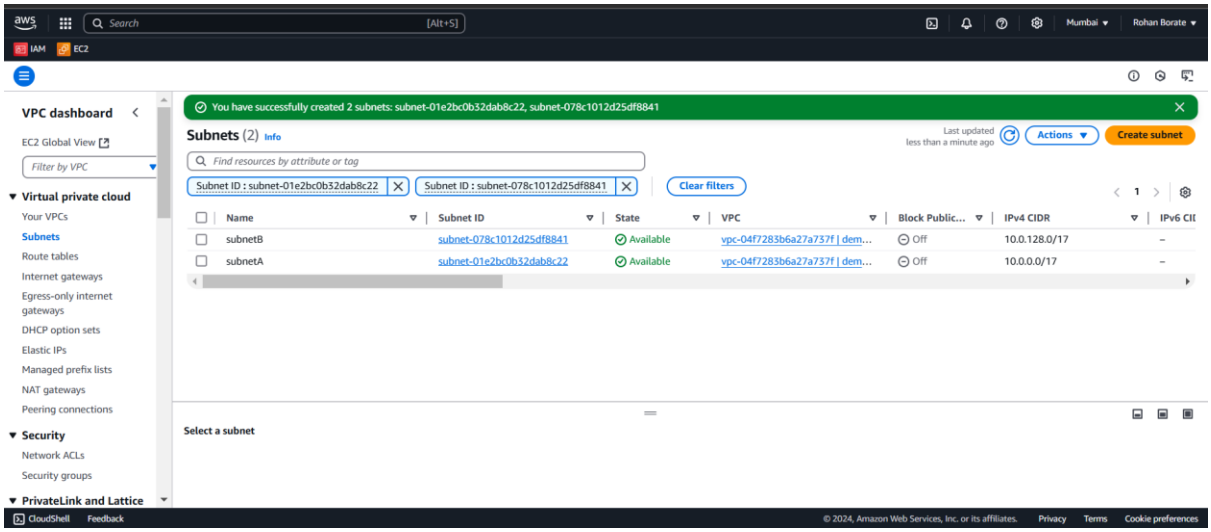


Create two subnet one private subnet and one public subnet in demovpc

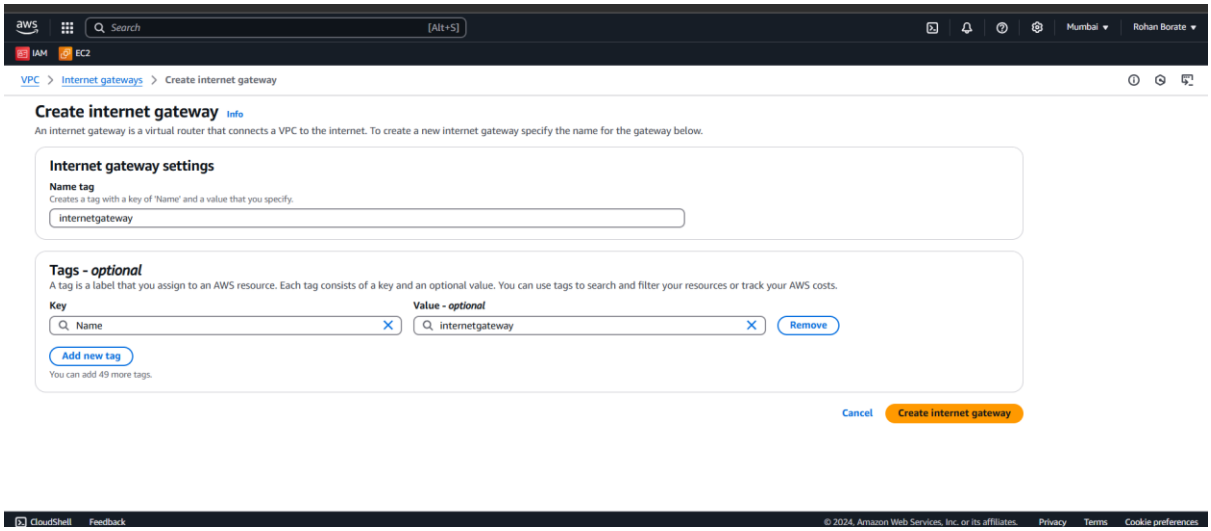




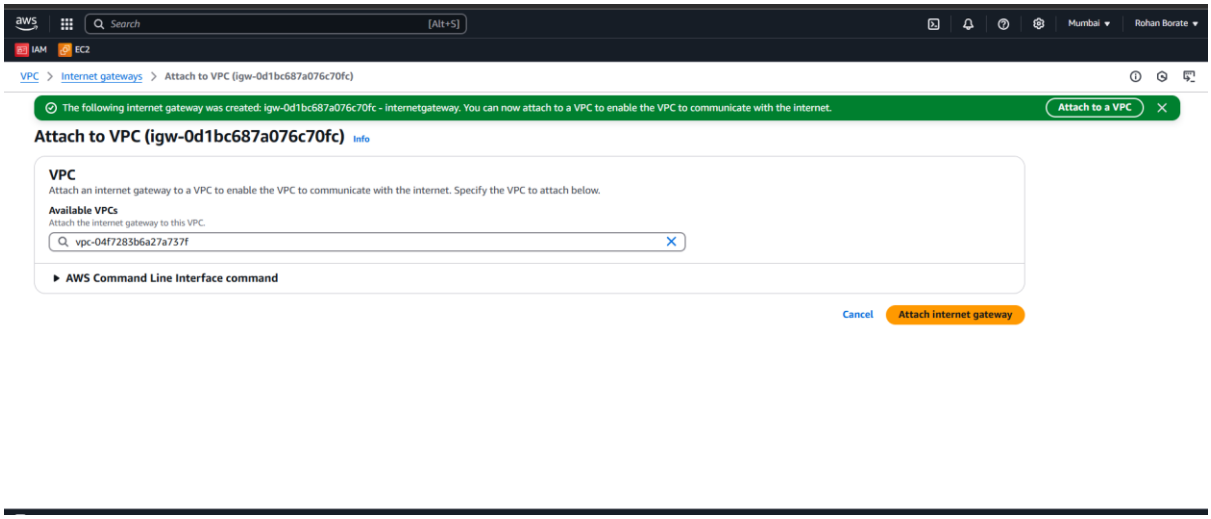




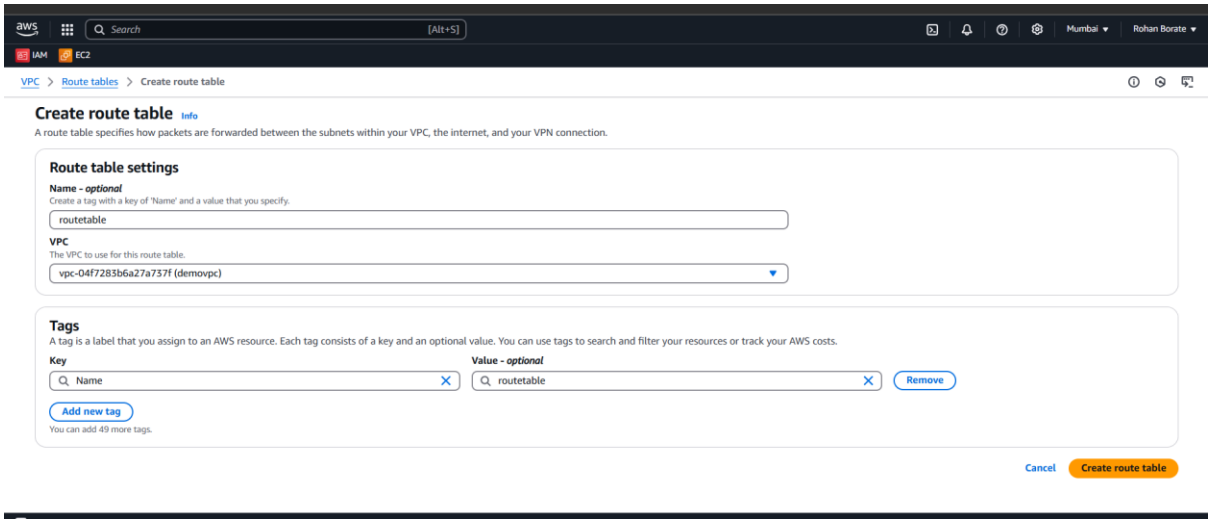
Create internet gateway



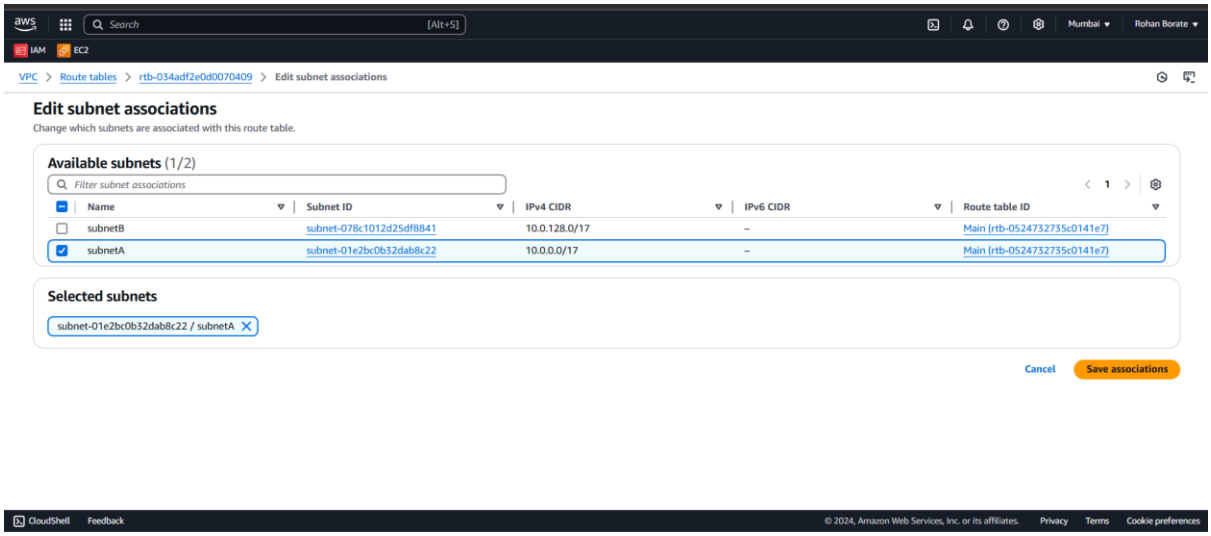
Attach internet gateway to vpc

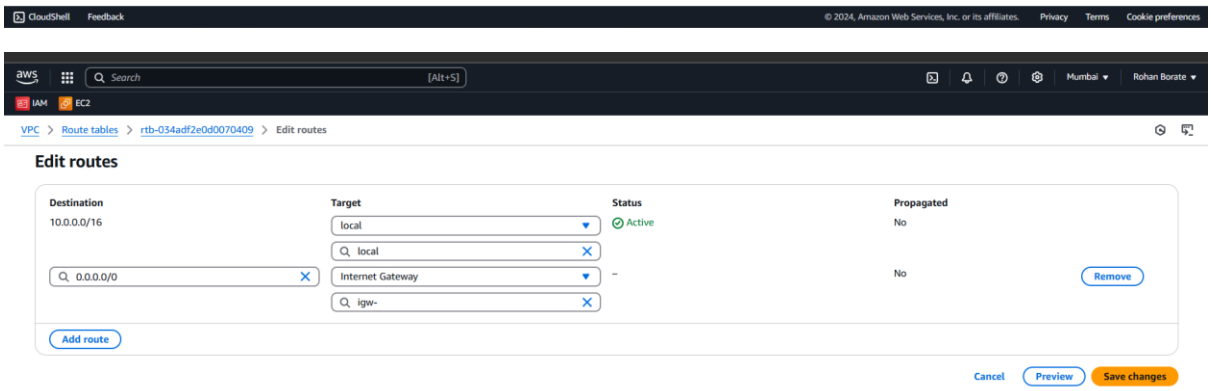


Create routetable with demo vpc

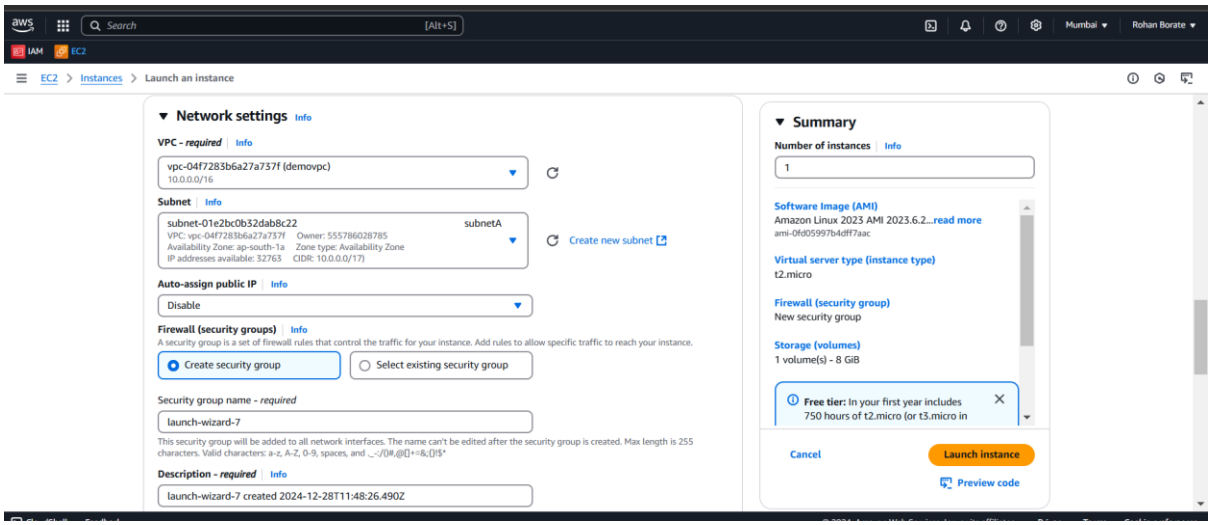


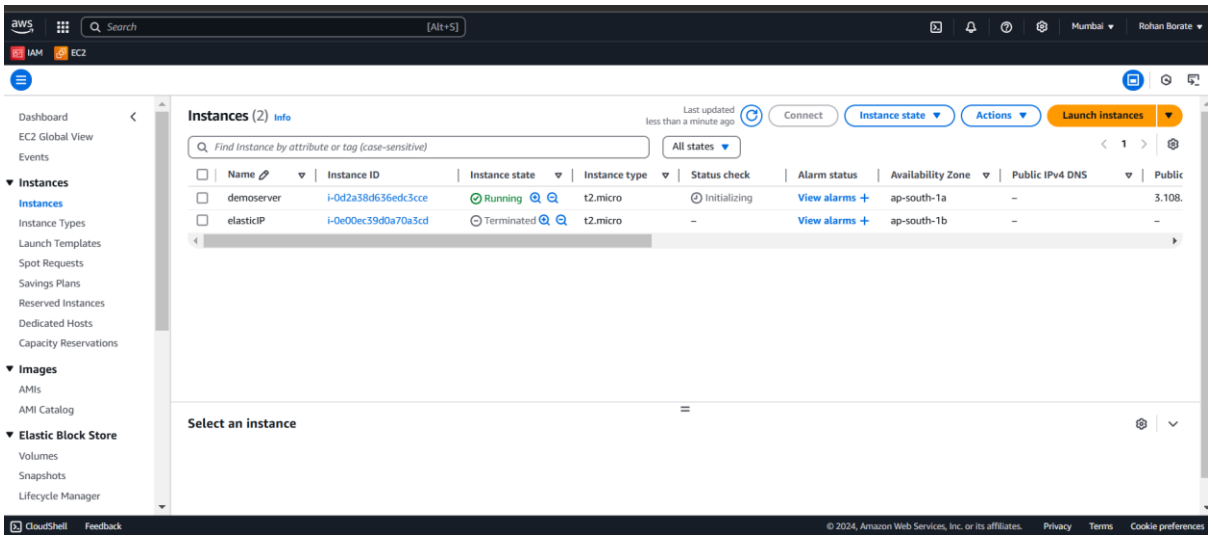
Edit routetable assosciate subnet and add internet gateway routing



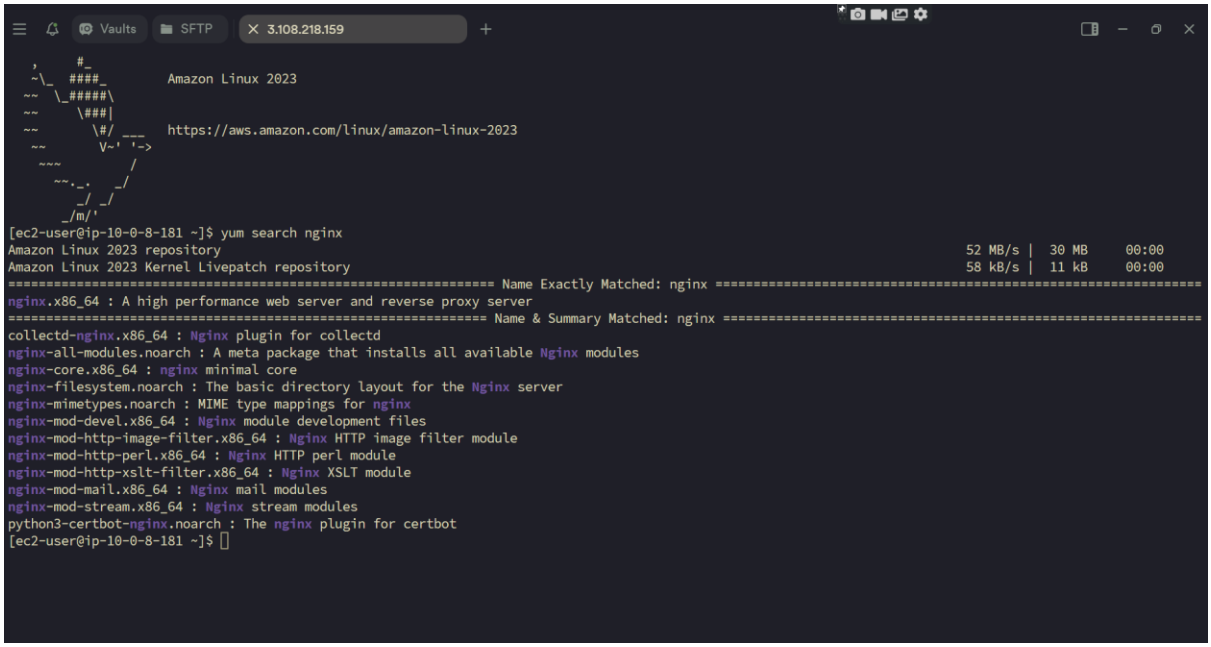


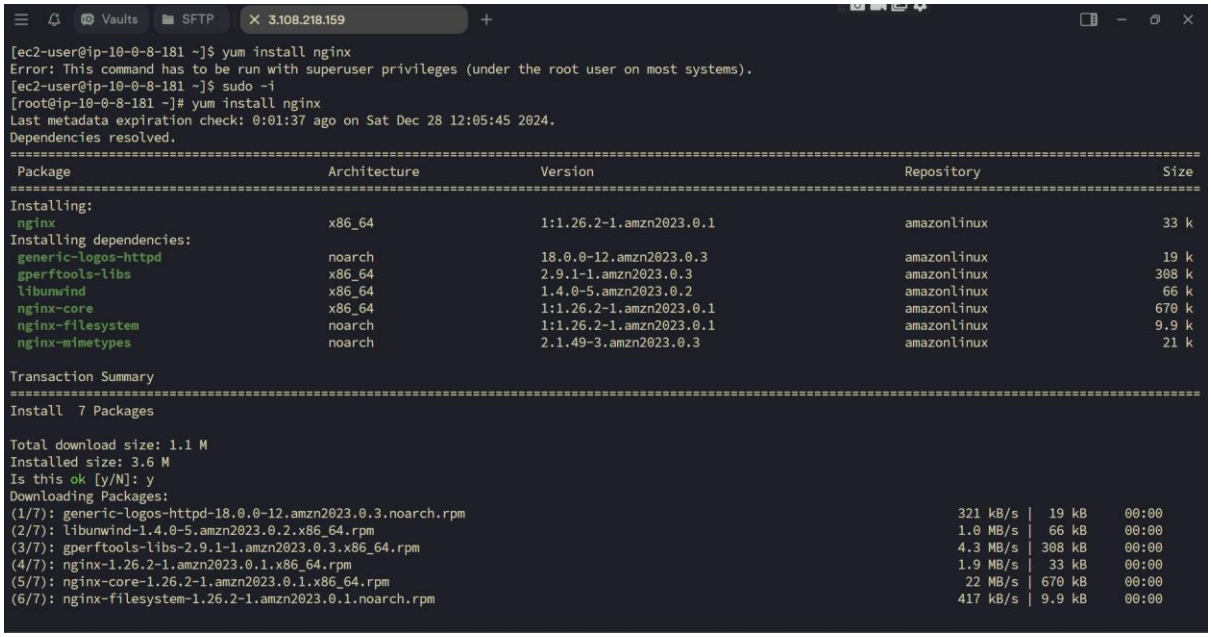
Create an instance in that VPC in subnetA which is public subnet .because we have assosciate it routetable where internet gateway is also added



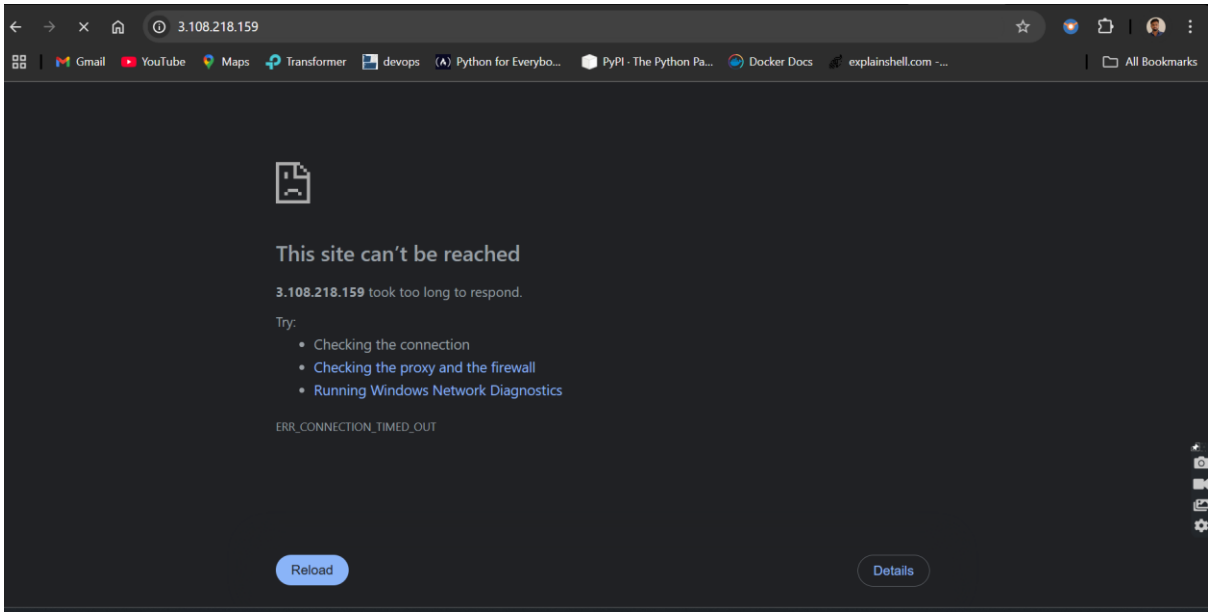


Connect to that create EC2 instance (demoserver) and install nginix on that instance

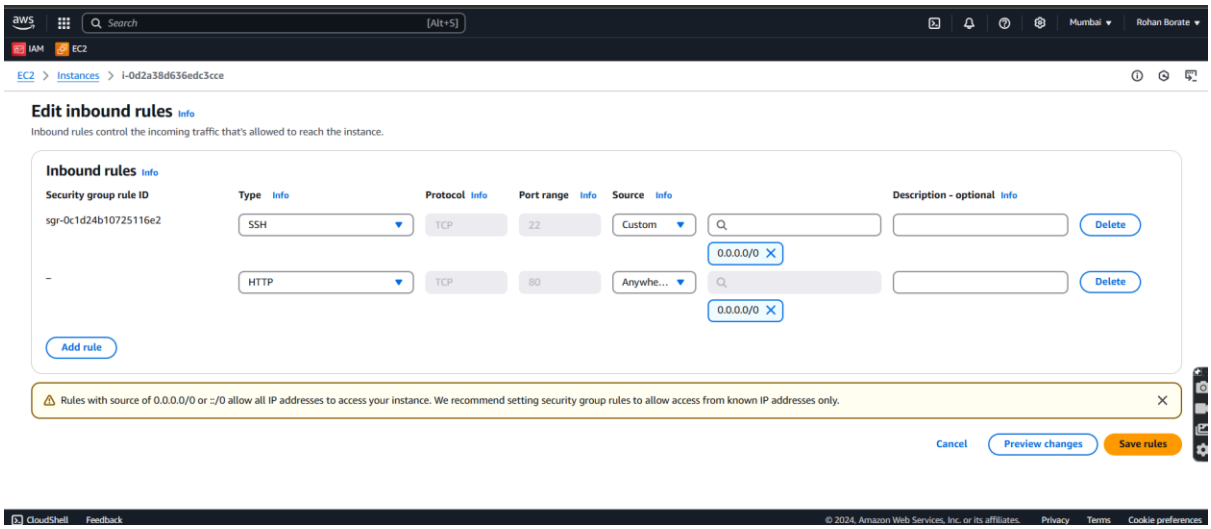




Start the nginx and check It is running , with port 80

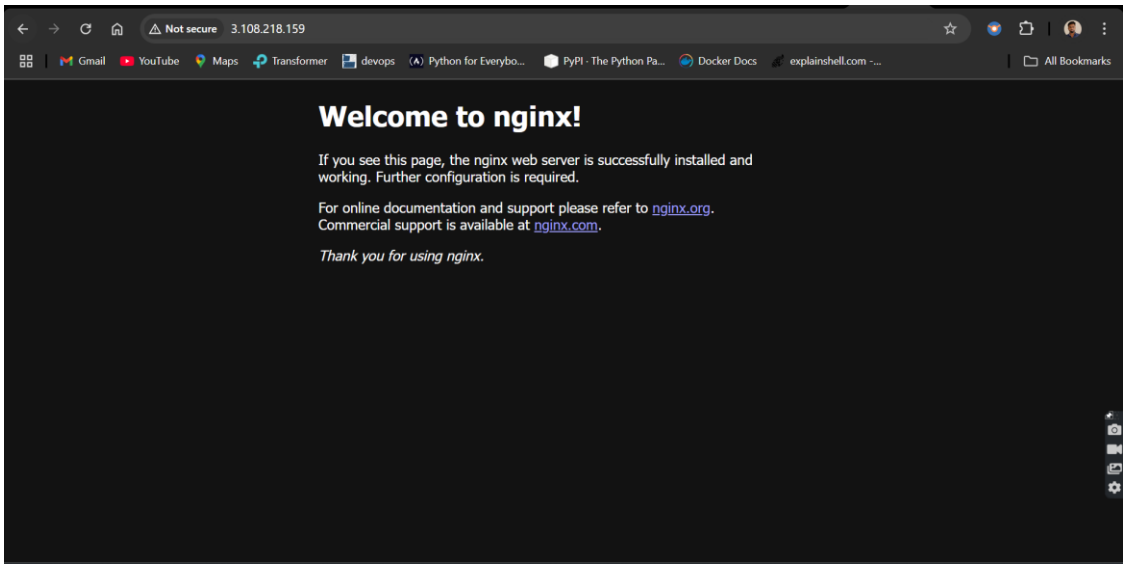


Enable port 80 in security group inbound rules



Now check nginx is accessible as we are enable port 80 , through the security group

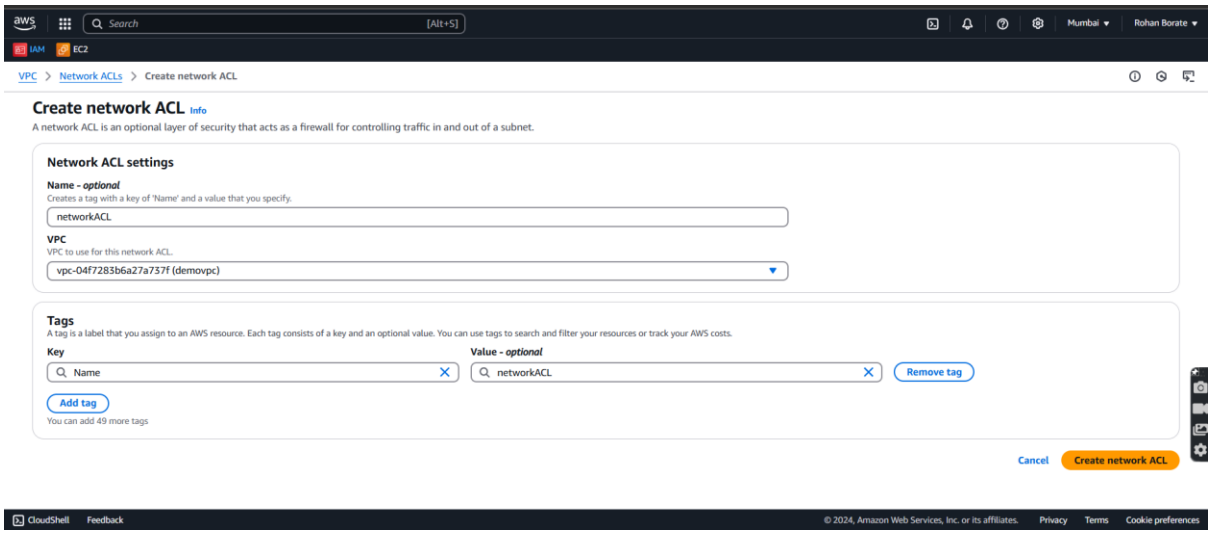
Here we are enabling the security through the security group



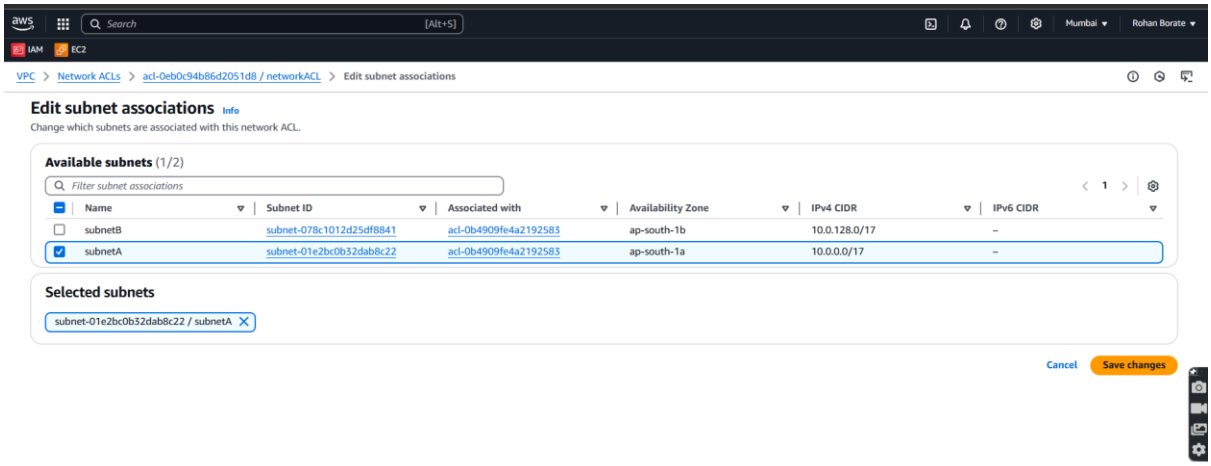
Now go to the NACL and denied port 80 ,

Basically NACL used to allow and denied specific ports and IP

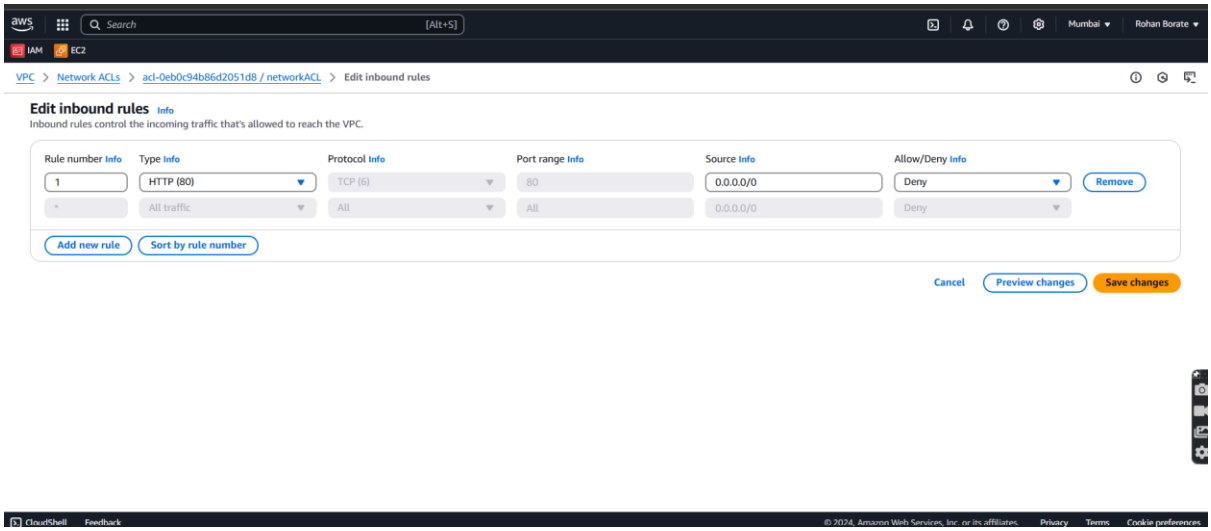
Create NACL



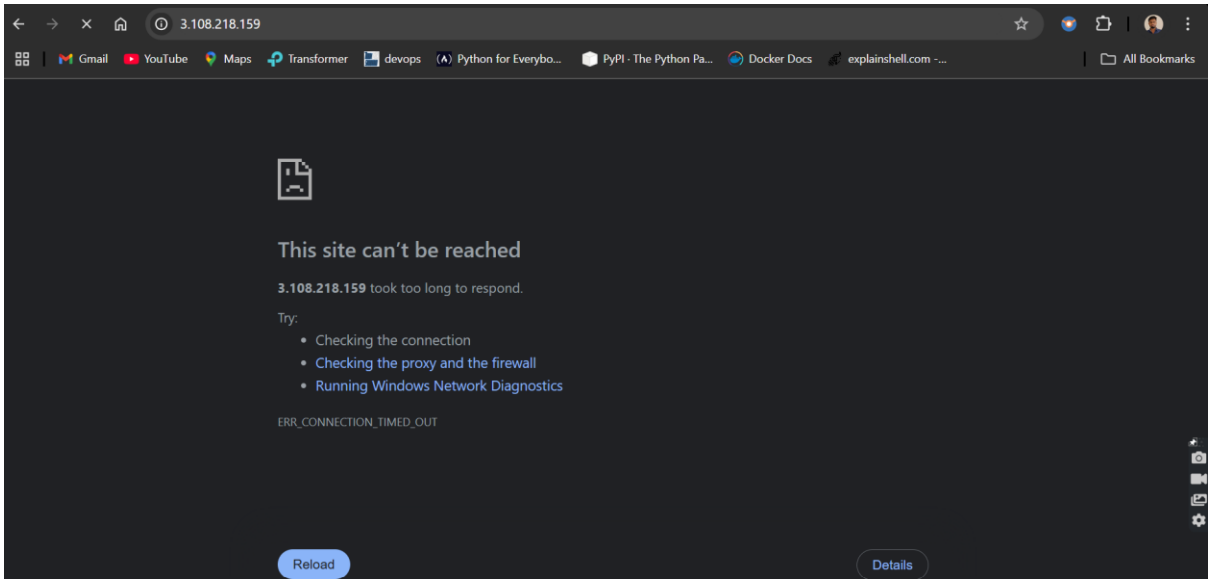
Assosciate subnetA to NACL



Denied port 80 in NACL inbound rule

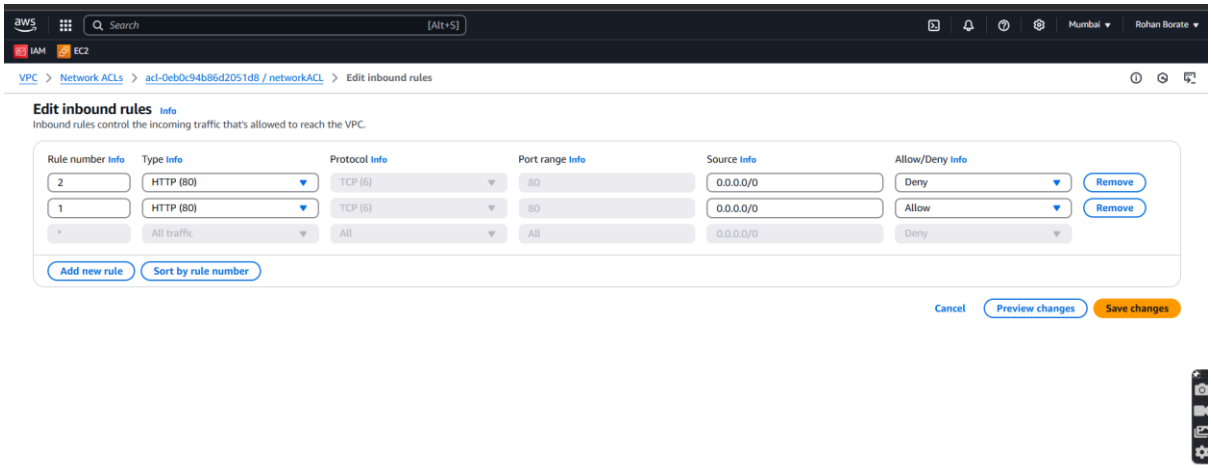


Now check nginx is accessible through port 80 , in security groups port 80 is enabled , but we have denied port 80 in NACL , NACL works at subnet level , so nginx should not be accessible



NACL works on the rule , means priority from low to high , 1 is highest priority

We can check now this by adding new rule which is allowing port 80 with giving high priority than other rule which is denying this port 80



Check nginx is available , it should be accessible