AWS CLOUD SOLUTIONS PROJECT 1

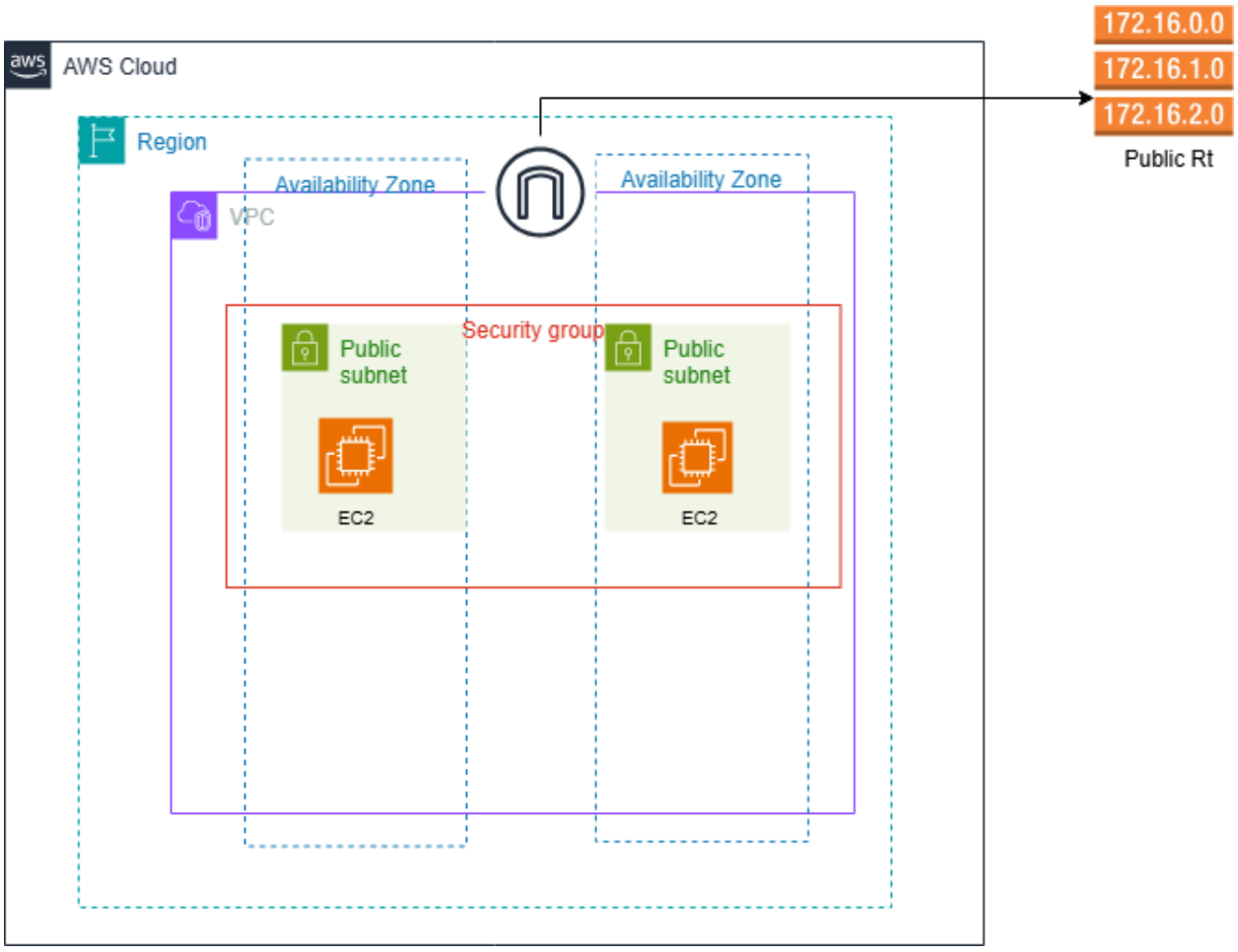
Setting up a Virtual Private Cloud (VPC) and launching of EC2 Instances On AWS Cloud.

This project shows a detailed step-by-by process of setting up a VPC, creating subnets, configuring a route table, security groups and NACL on AWS cloud.

This project validates my knowledge and skills in the following areas on AWS cloud.

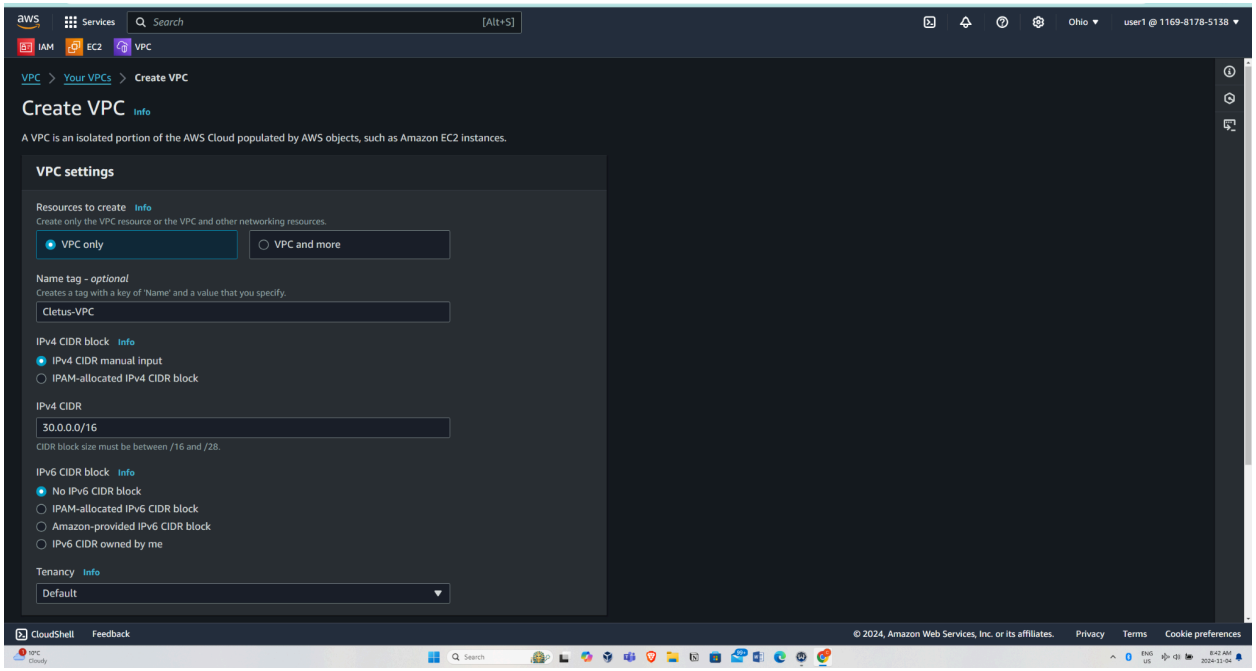
1. AWS infrastructure
2. IP Address (Cidr block)
3. Subnet
4. Virtual Machines (EC2)
5. Network Traffic
6. Security (SG and NACL)

Below is the architectural diagram of this project:



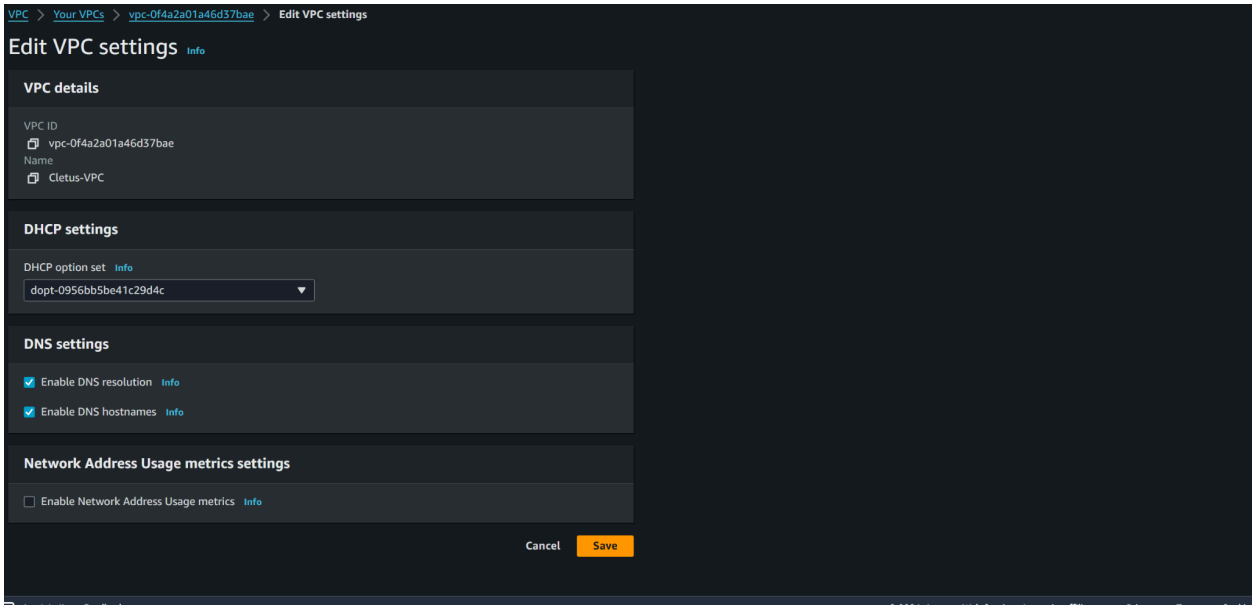
Step 1

Setting up a VPC (Virtual Private Cloud)



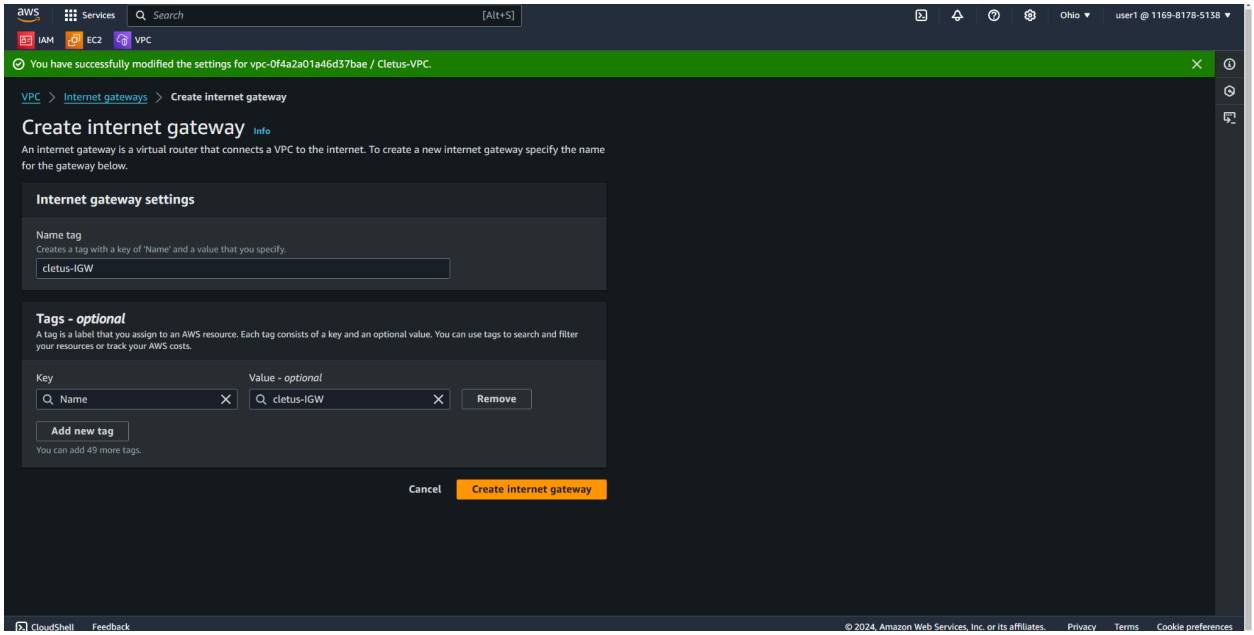
Step 1b

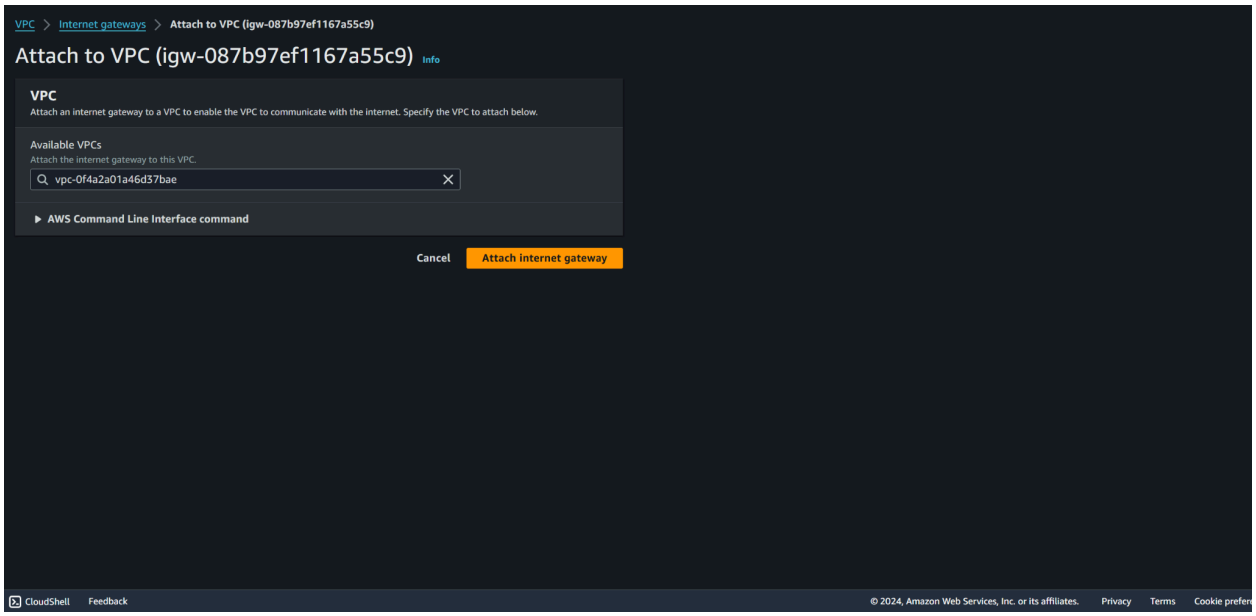
Configure your VPC settings by enabling DNS host names, which would allow resources provisioned within this subnet especially servers to have a DNS host name. This function is vital when routing traffic with Route53 Service



Step 2

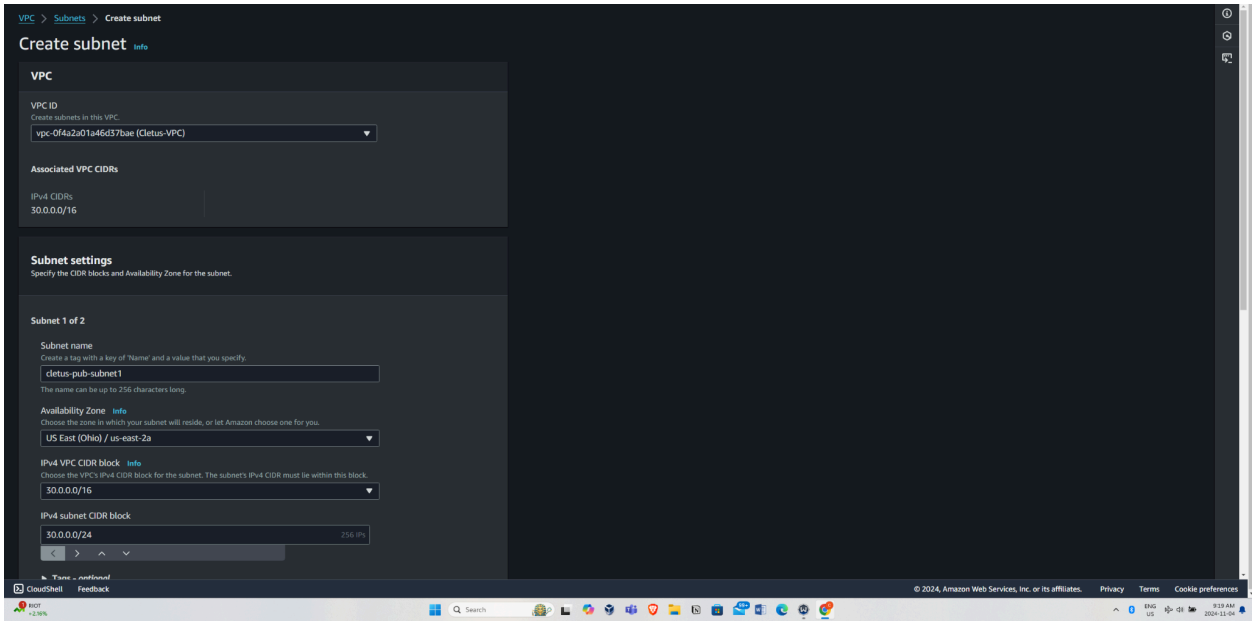
Creating and attaching an internet gateway (IGW) to make the VPC accessible to the internet

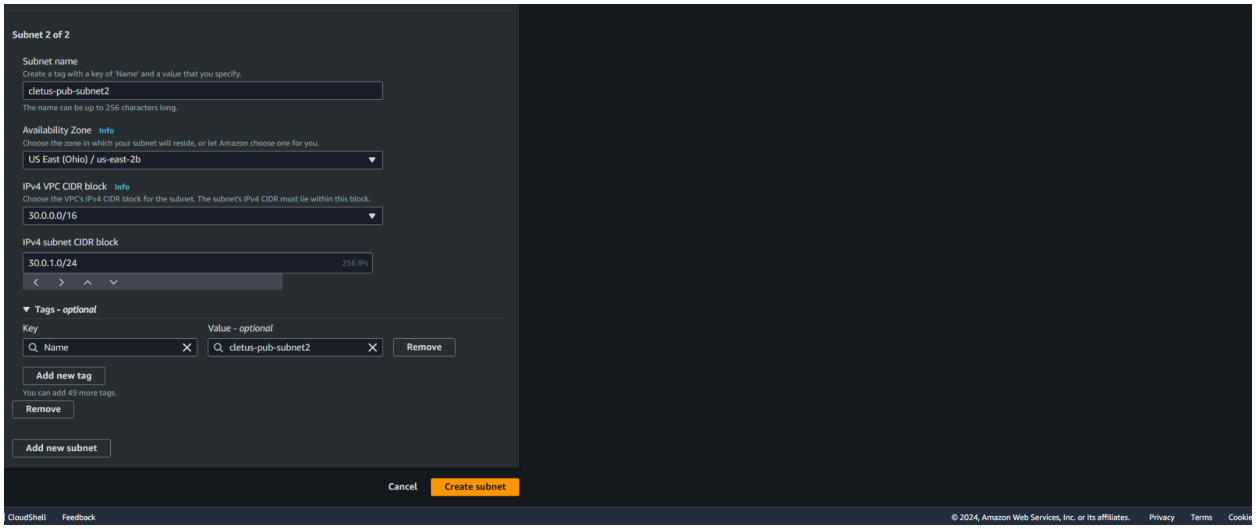




Step 3

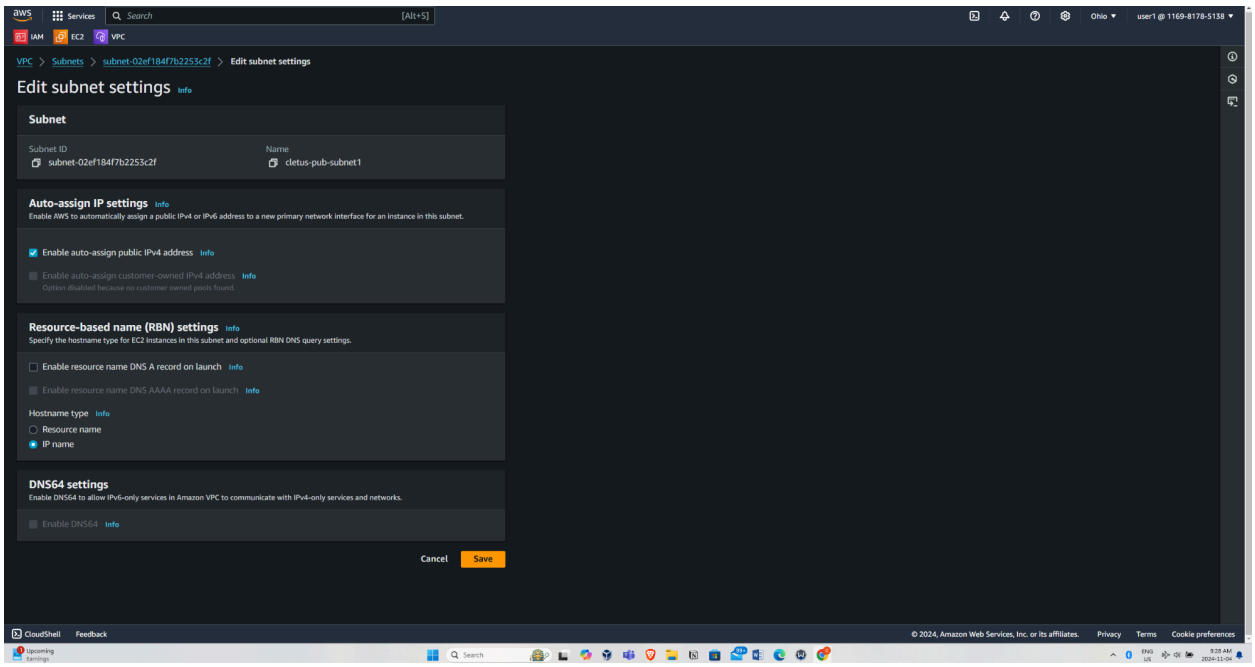
Creating two public subnets and keep them in different availability zones





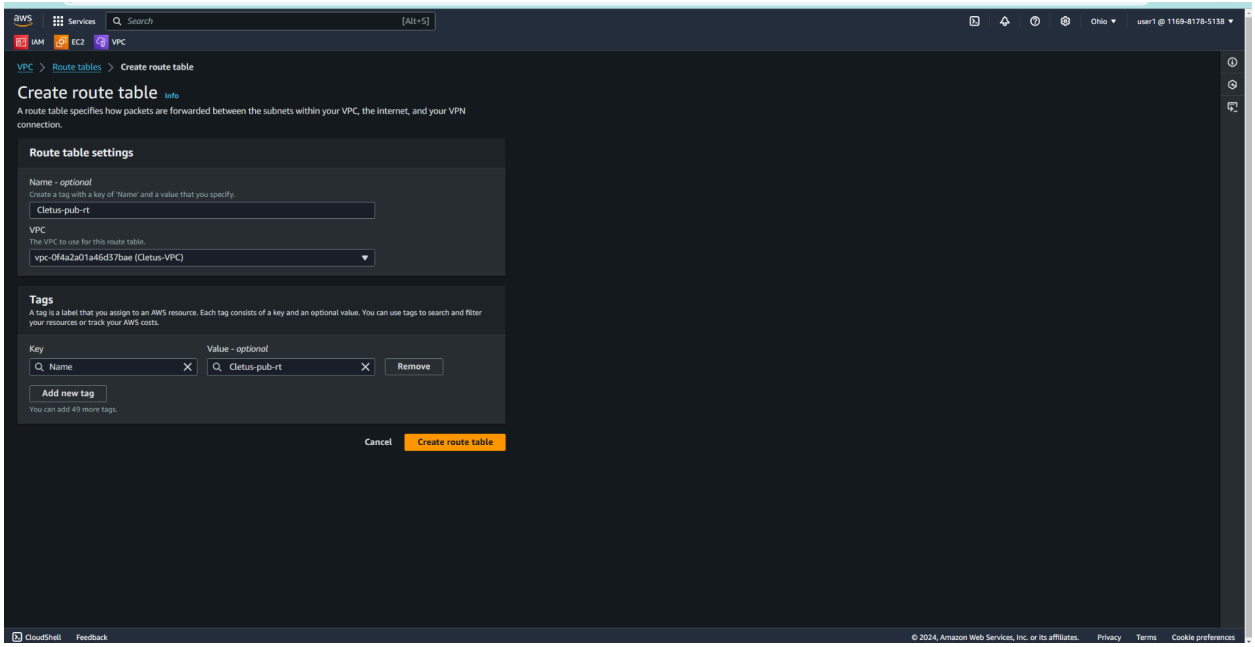
Step 3b

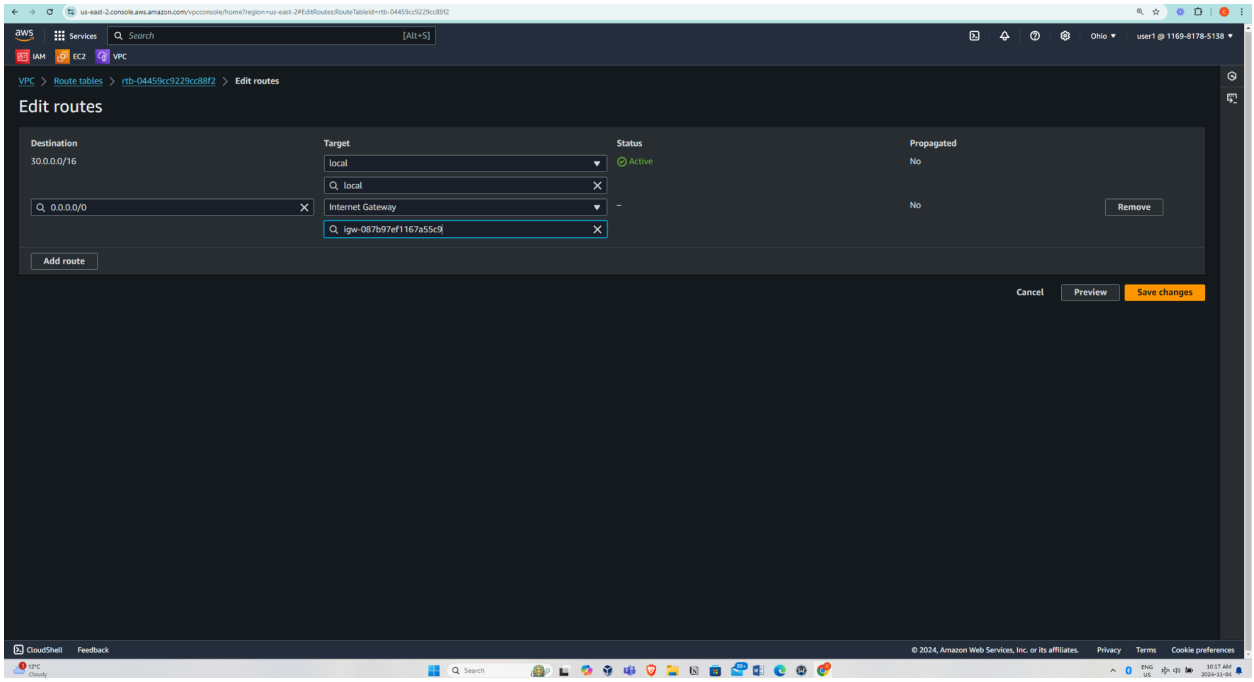
Edit your subnet settings and enable auto-assign public address. This setting would allow resources launched within this subnet to be assigned public IP addresses dynamically. This is a public subnet which means resources within this subnet need to be accessible to the internet. So having a public IP address is very vital.



Step 4

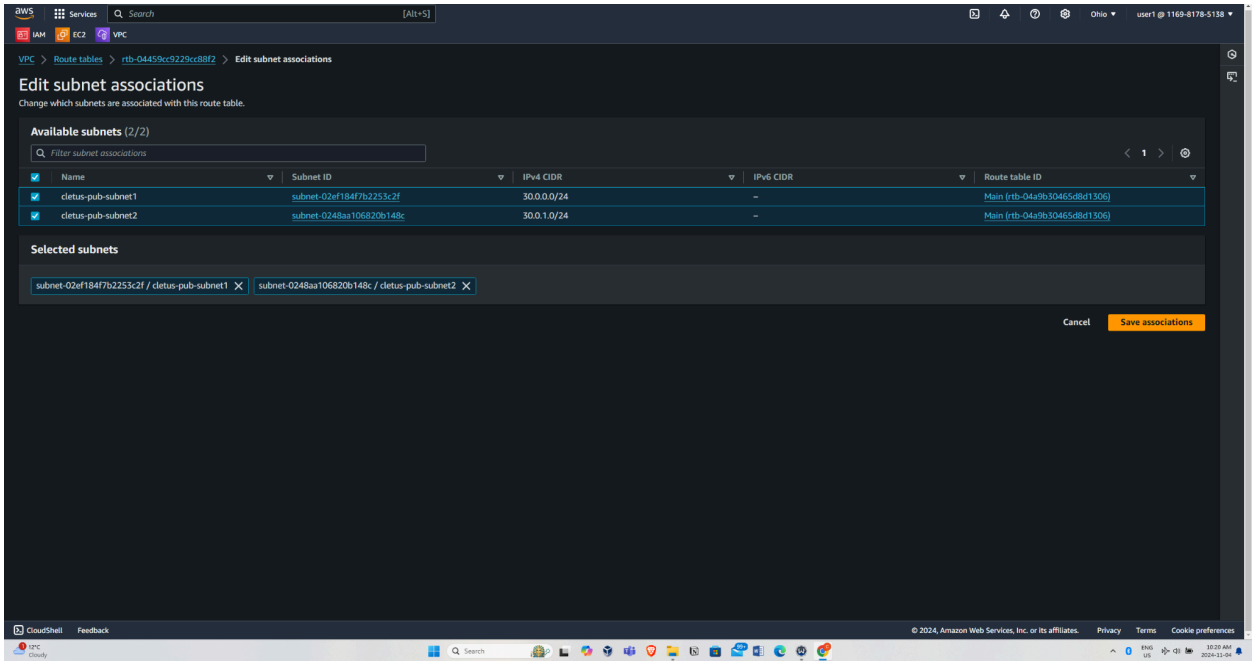
Create a public route table and associate the subnets to the newly created public route table which has a route pointing to the internet gateway.





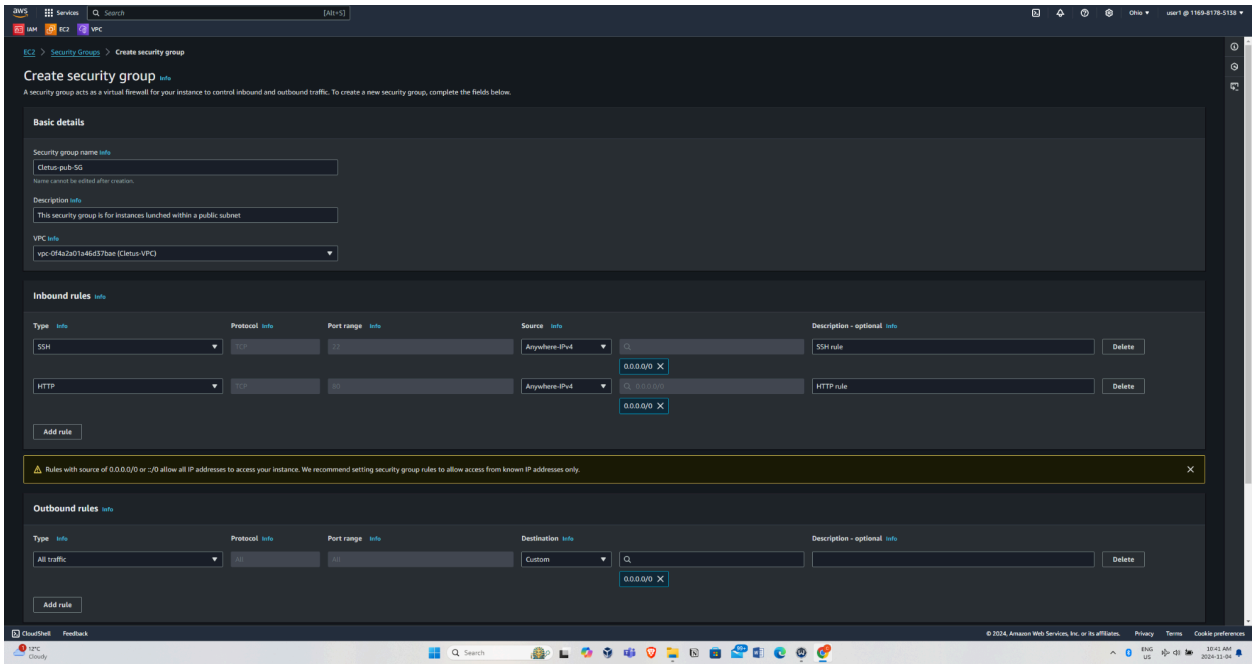
Step 4b

Associating Subnets.



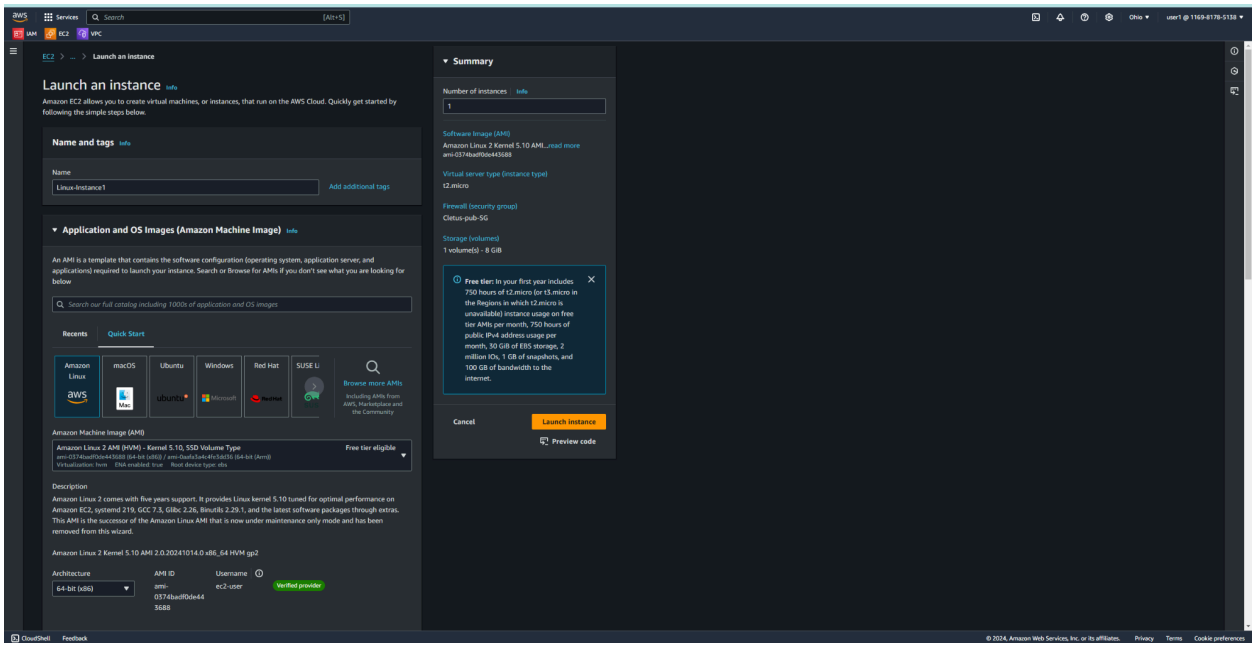
Step 5

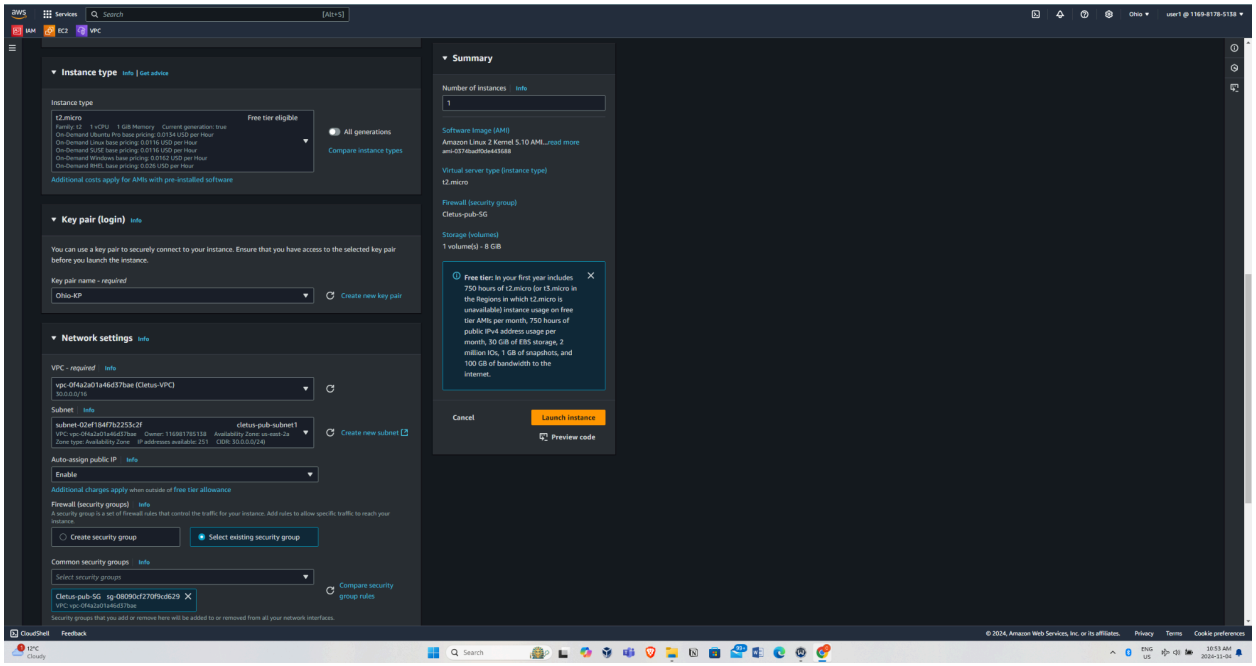
Create a security group (SG) and configure inbound rules to allow SSH and HTTP traffic. The SG dictates the Egress and Ingress traffic at the instance level.

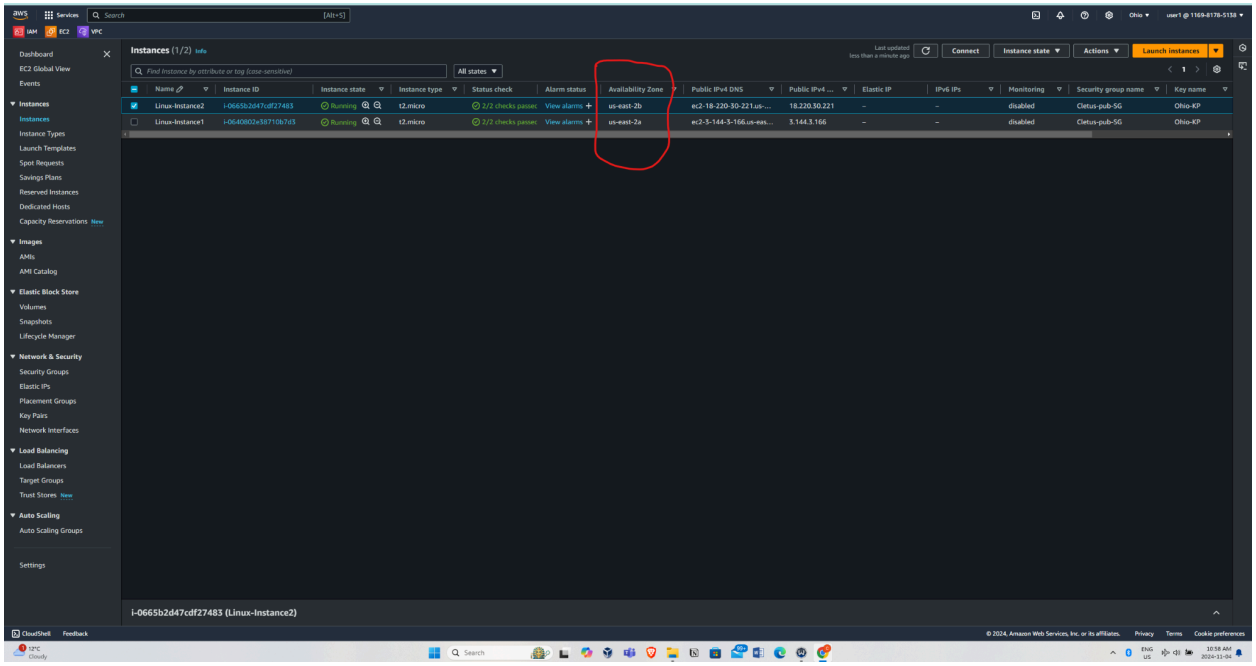


Step 6

Launch 2 instances within the VPC (cletus-VPC) and keep each of them in our public subnets. That is, one in cletus-pub-subnet1 and the other in cletus-pub-subnet2.

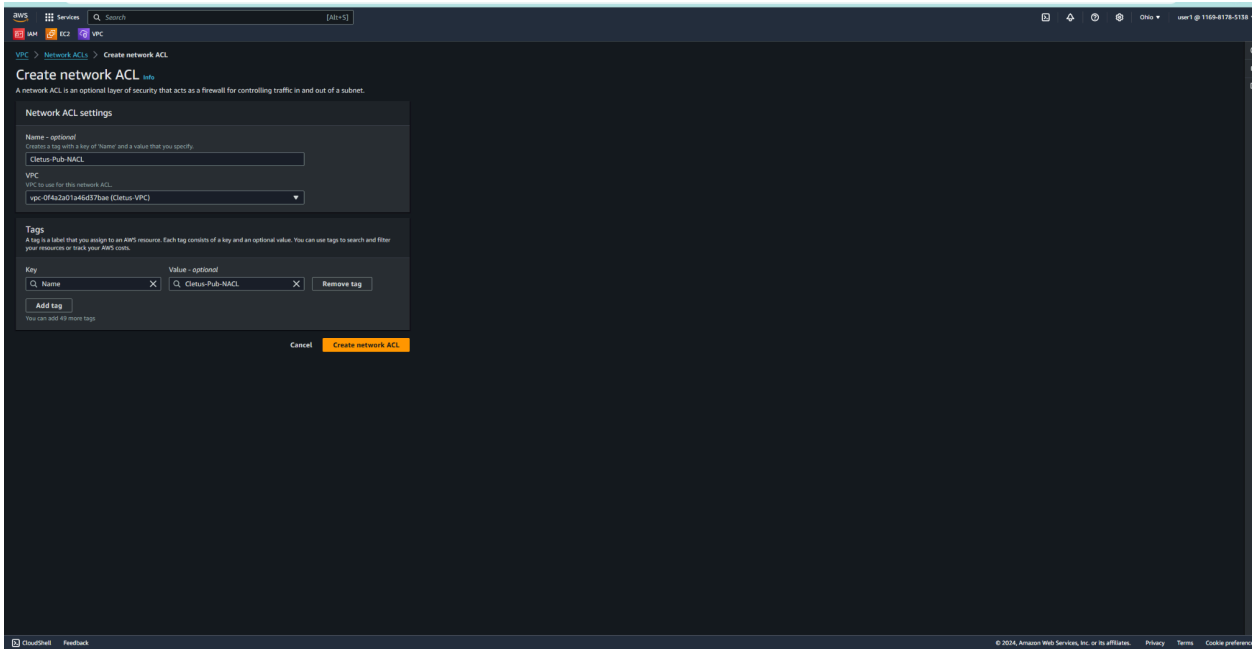



Instance type
Key pair (login)
Network settings
Summary
Launch instance
Cancel


Instances (1/2)
Linux-Instance2
Linux-Instance1
i-0665b2d47cdf27483 (Linux-Instance2)

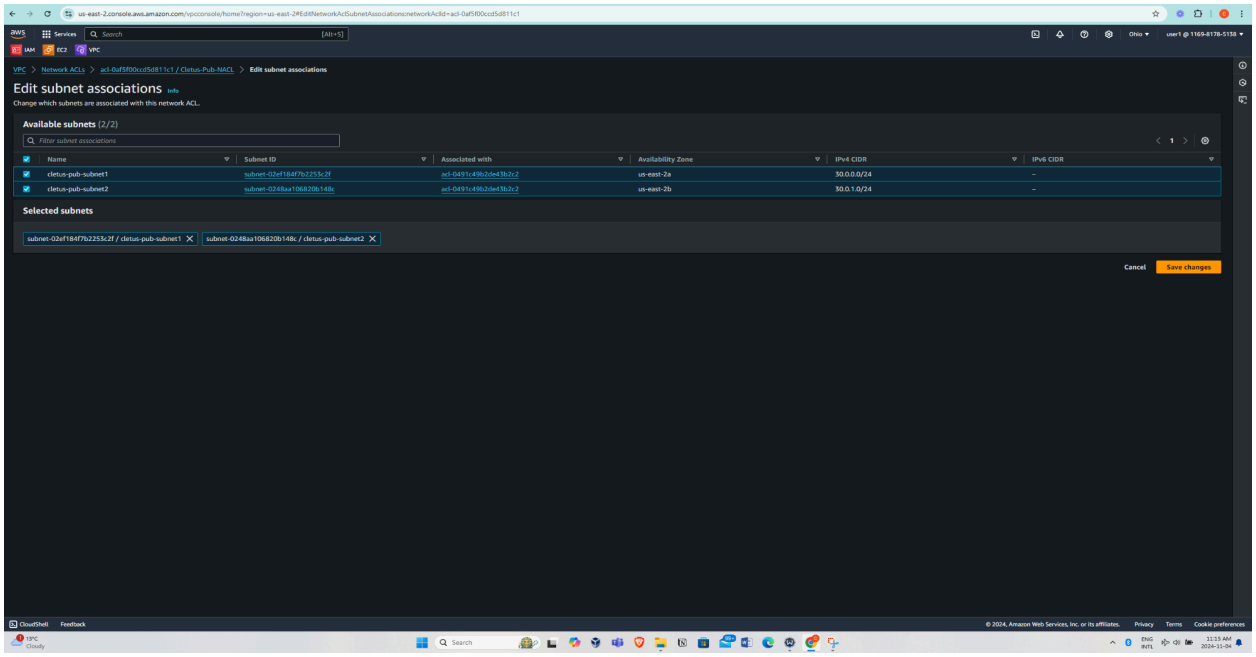
Step 7

Create and configure a Network Access Control List (NACL). To enhance the security of the infrastructure, I need to implement NACL which dictates the Ingress and Egress traffic at the subnet level. This is just like a firewall that allows or denies traffic based on set rules. Also, This is similar to a SG. The difference is that a SG is only effective at the Instance level while NACL is effective at the subnet level.



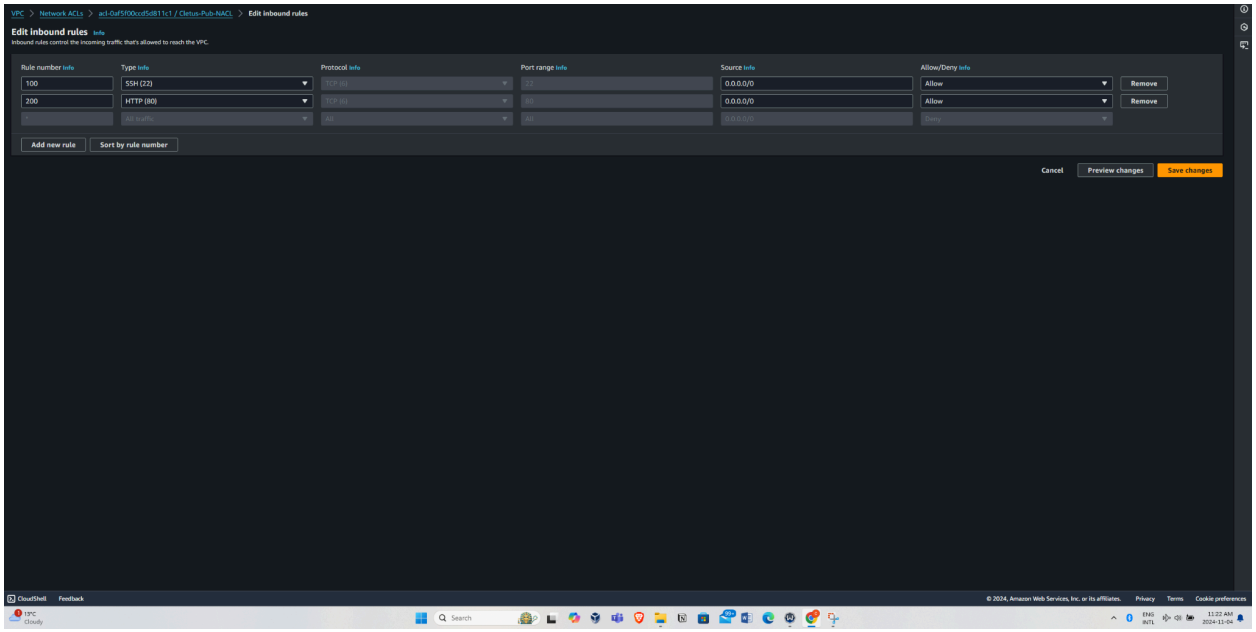
Step 7b

Associate the public subnets.

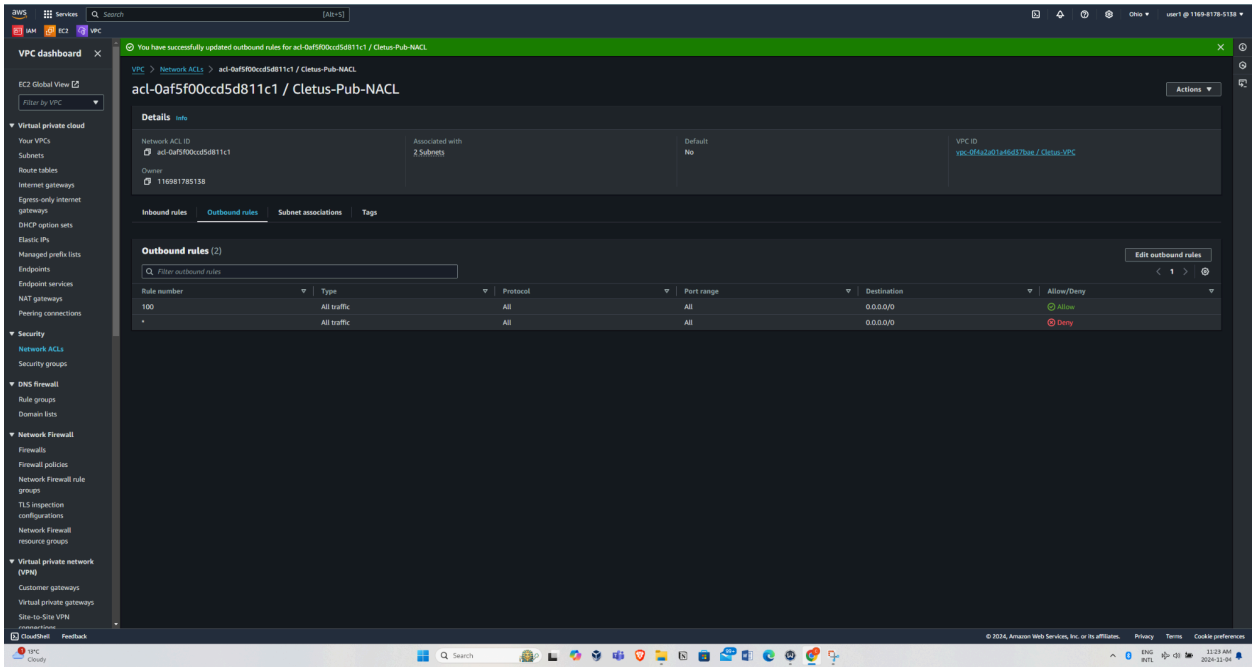


Step 7c

Configure inbound rule to allow traffic from port 22(SSH) and port 80 (HTTP)



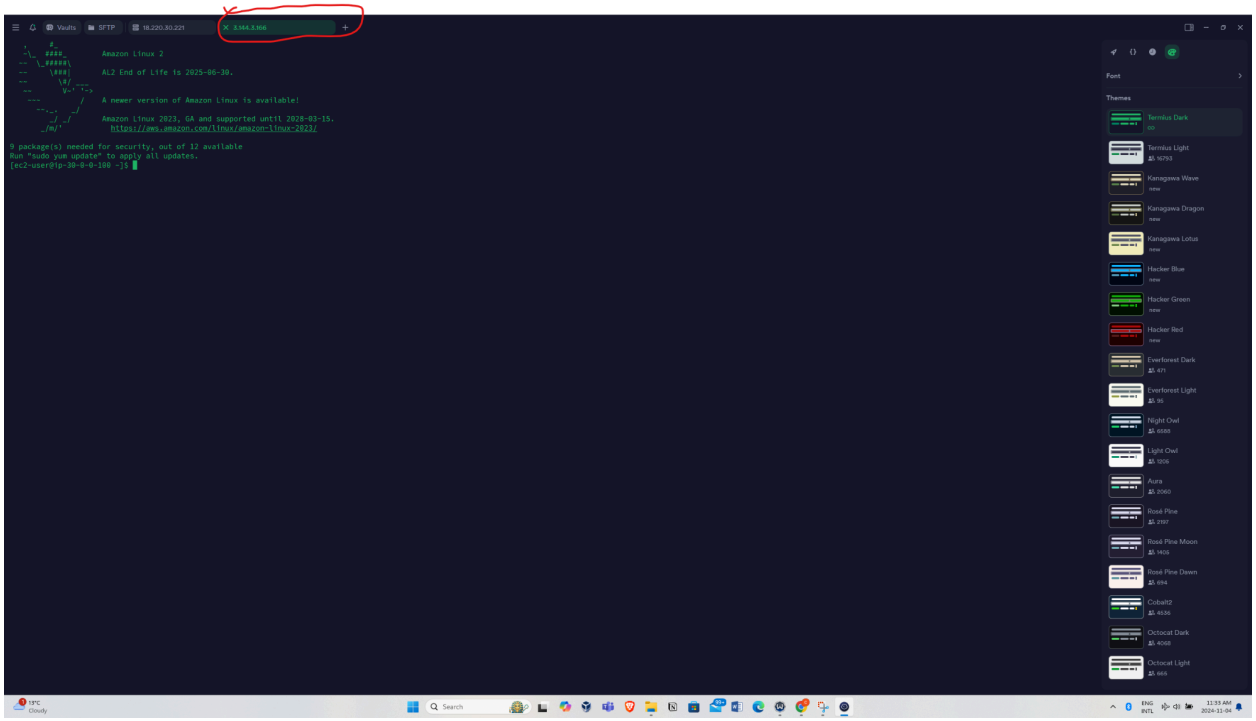
Configure outbound rules to allow all traffic.



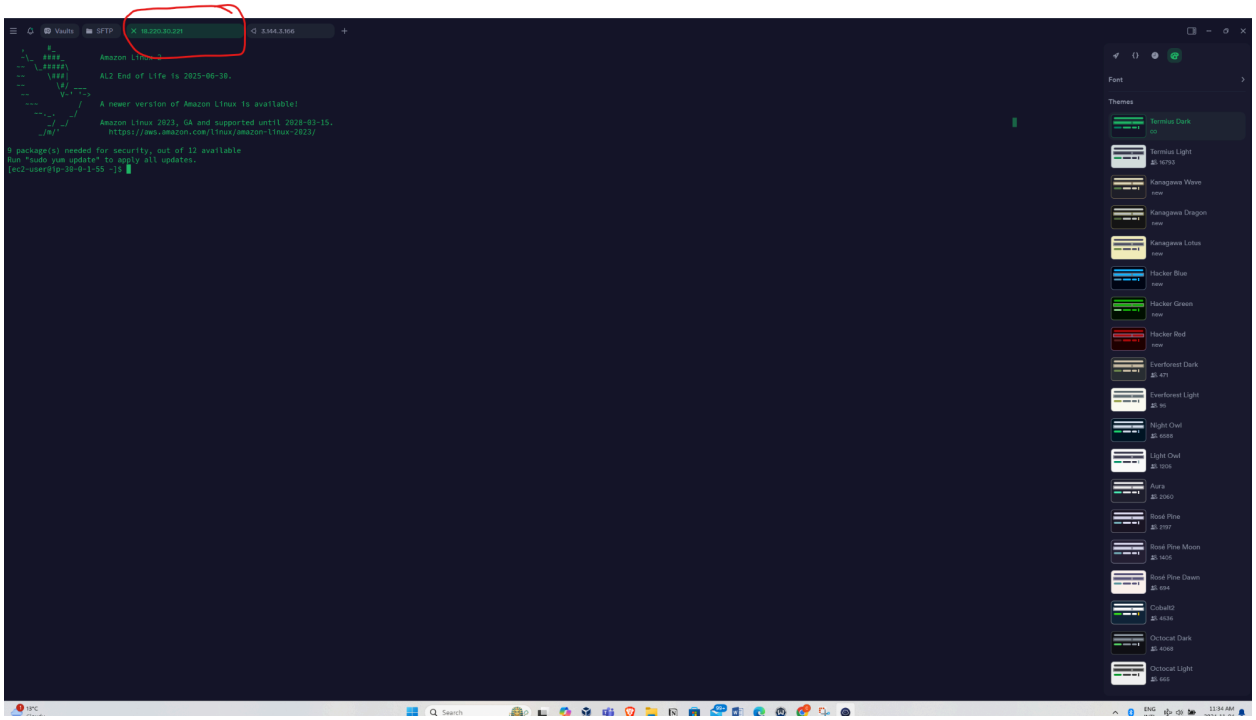
Step 8

Validating The instances can be accessible via the internet by connecting remotely with SSH.

Instance1



Instance2



Resource Map of what i have done so far in this project