Creating Secure VPC

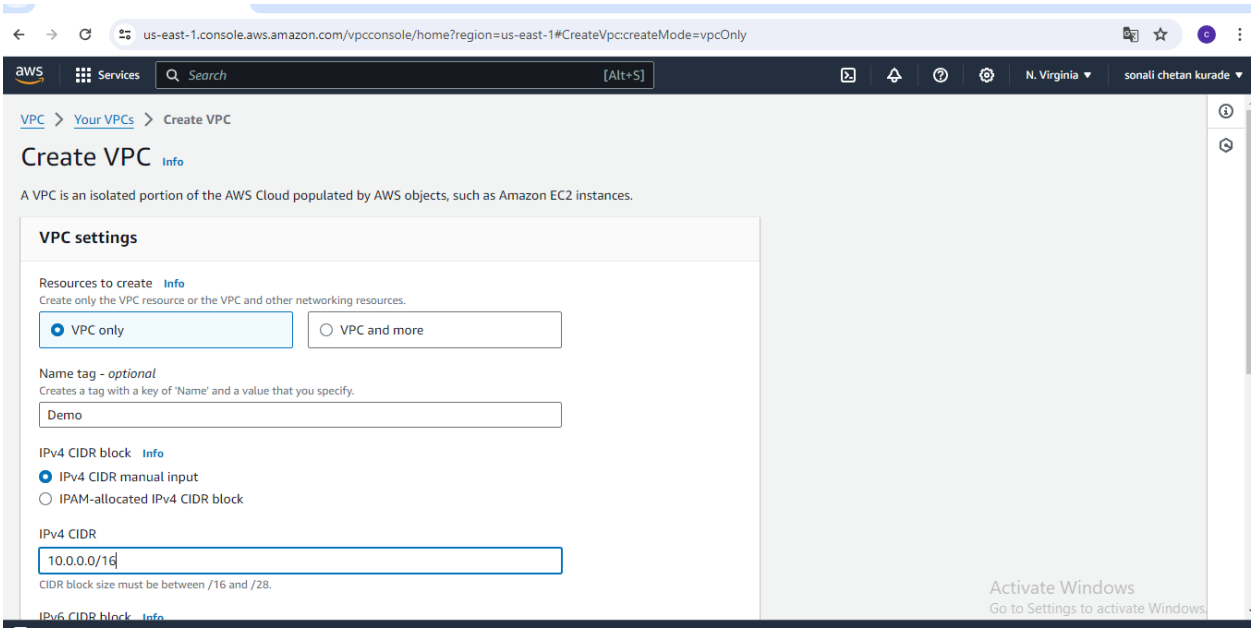
Amazon Virtual Private Cloud is a commercial cloud computing service that provides a virtual private cloud, by provisioning a logically isolated section of Amazon Web Services Cloud. Enterprise customers can access the Amazon Elastic Compute Cloud over an IPsec based virtual private network.

Step1 : Logging In to the Amazon Web Services Console

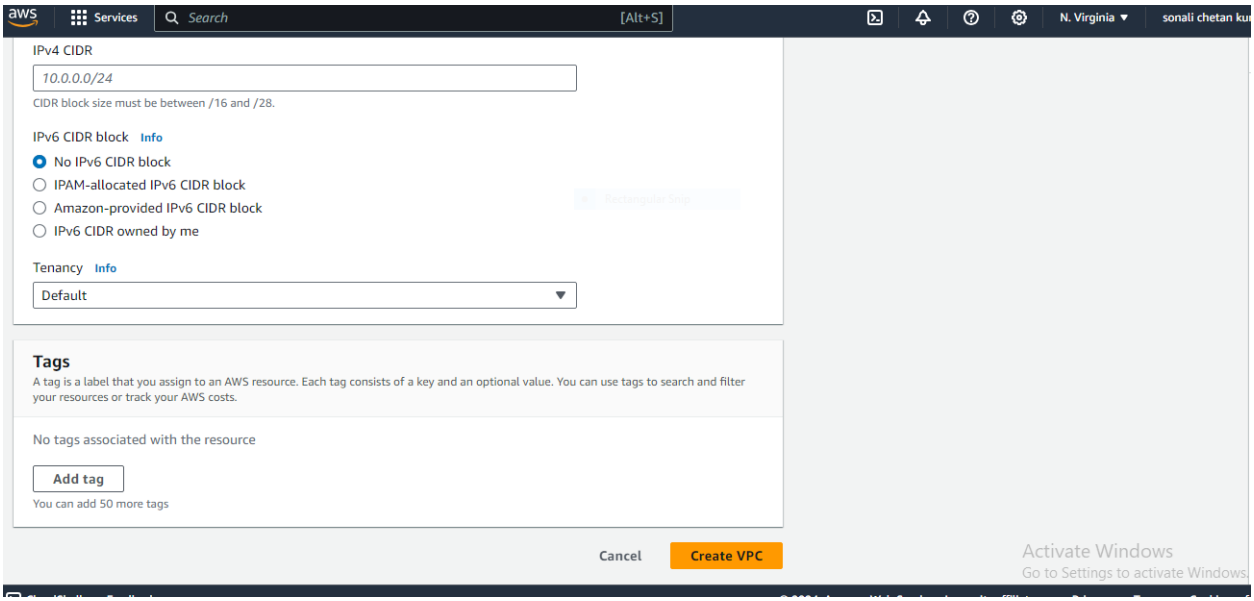
login to your AWS account using your credentials.

Step 2: Create VPC

1. In the AWS Management Console search bar, enter VPC, and click the VPC result under Services:
2. To start creating VPC, in the left down side, Click on **Your VPC** to Create VPC:
2. Enter VPC name and IPV4 CIDR Range Click on create VPC

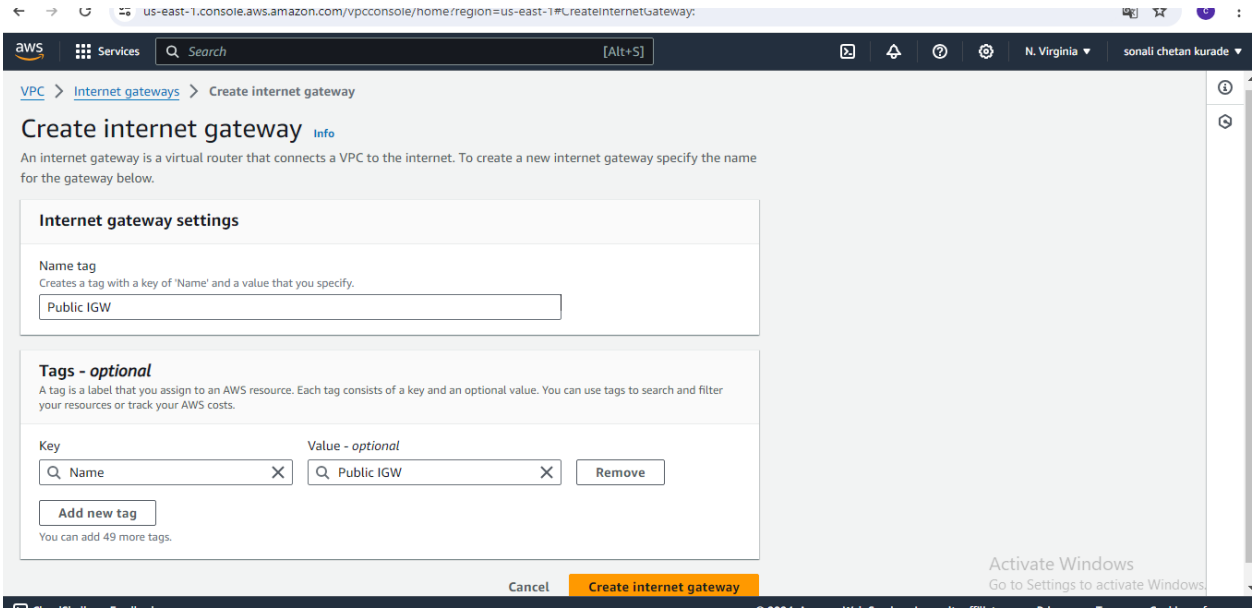


2. Click on below button create VPC



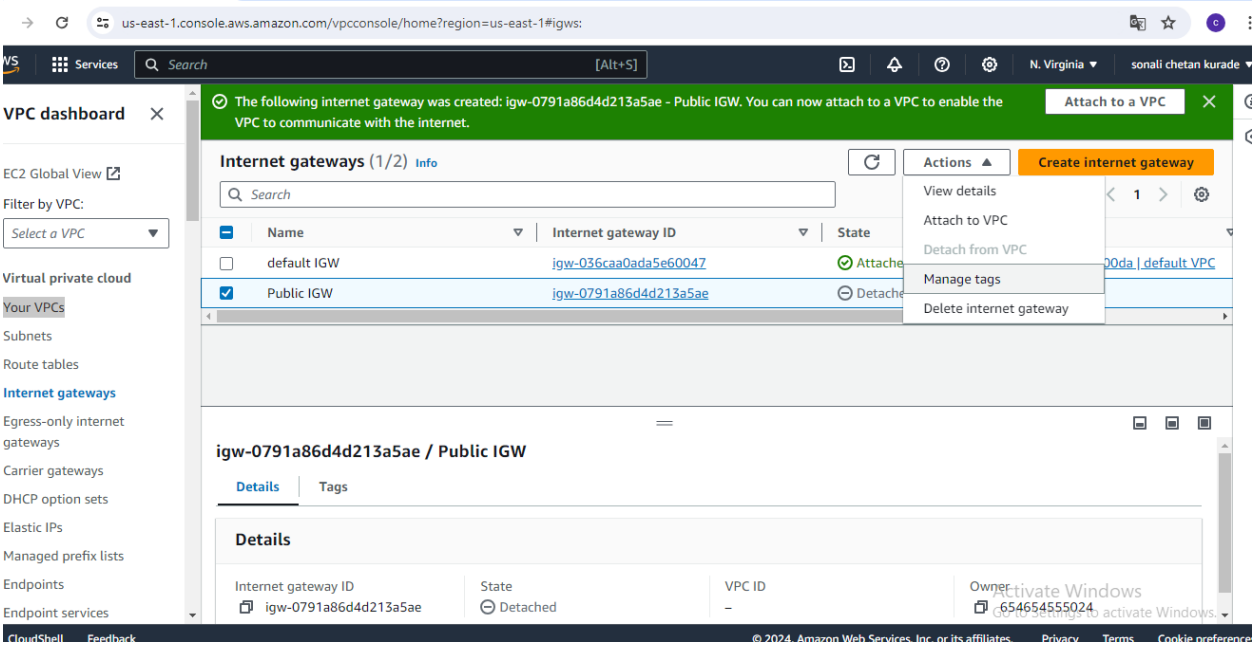
Step 3 : Create IGW

1. To start creating IGW , in the left down side, click Create Internet Gateway:
2. Give name to internet Gateway and click on create internet gateway

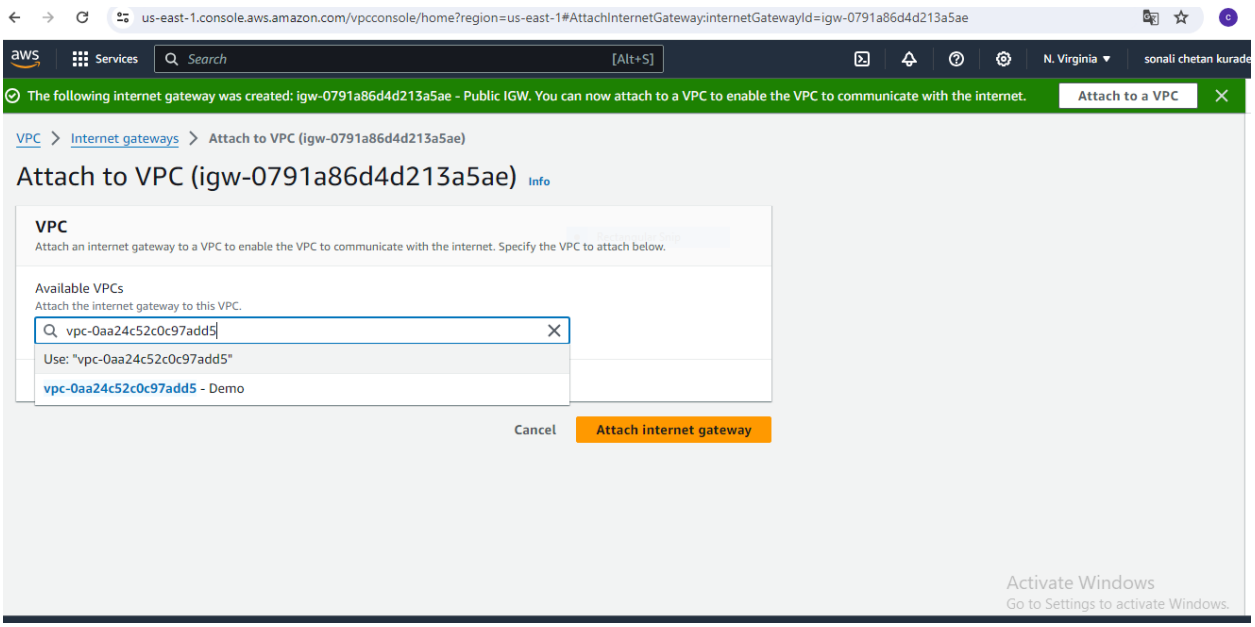


Step 4 : Attach Your IGW to VPC

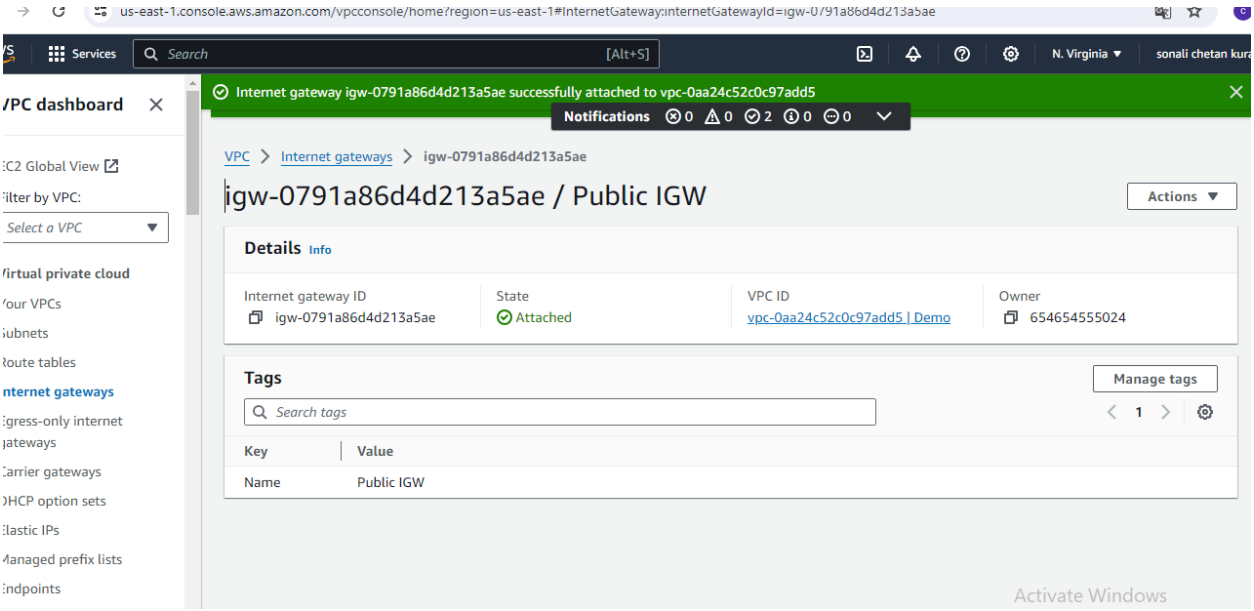
- Select IGW Which you have created recently and Click on **Action** and select option **Attach to VPC**



- Select VPC and click on **Attach internet gateway**

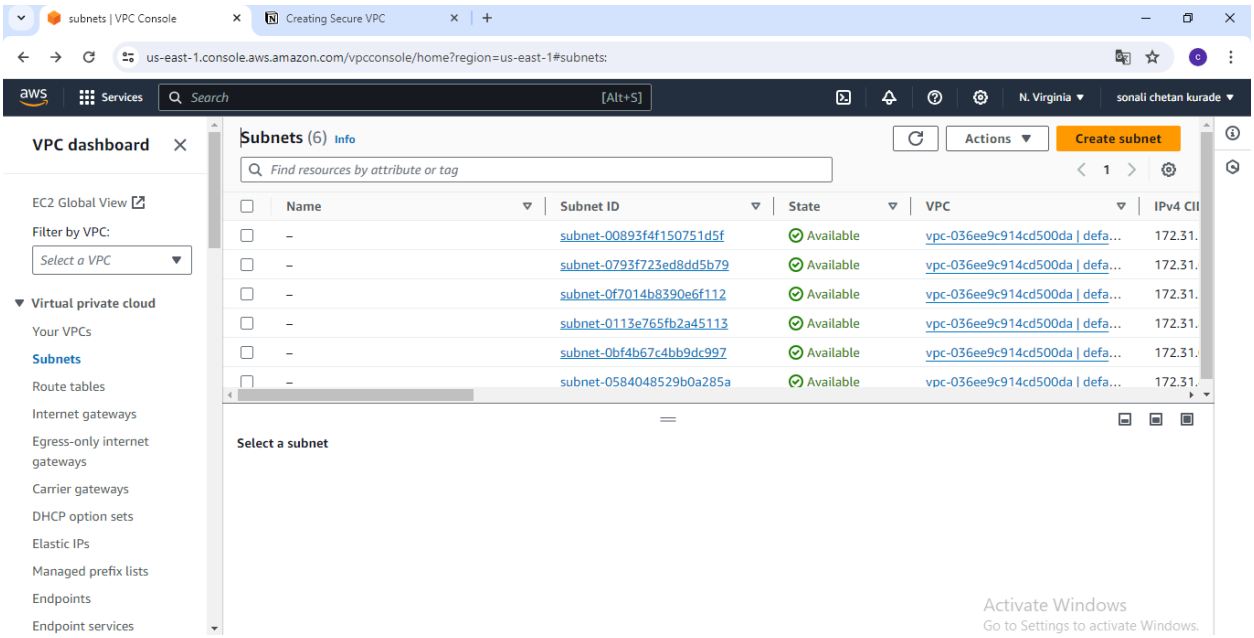


- IGW is attached successfully

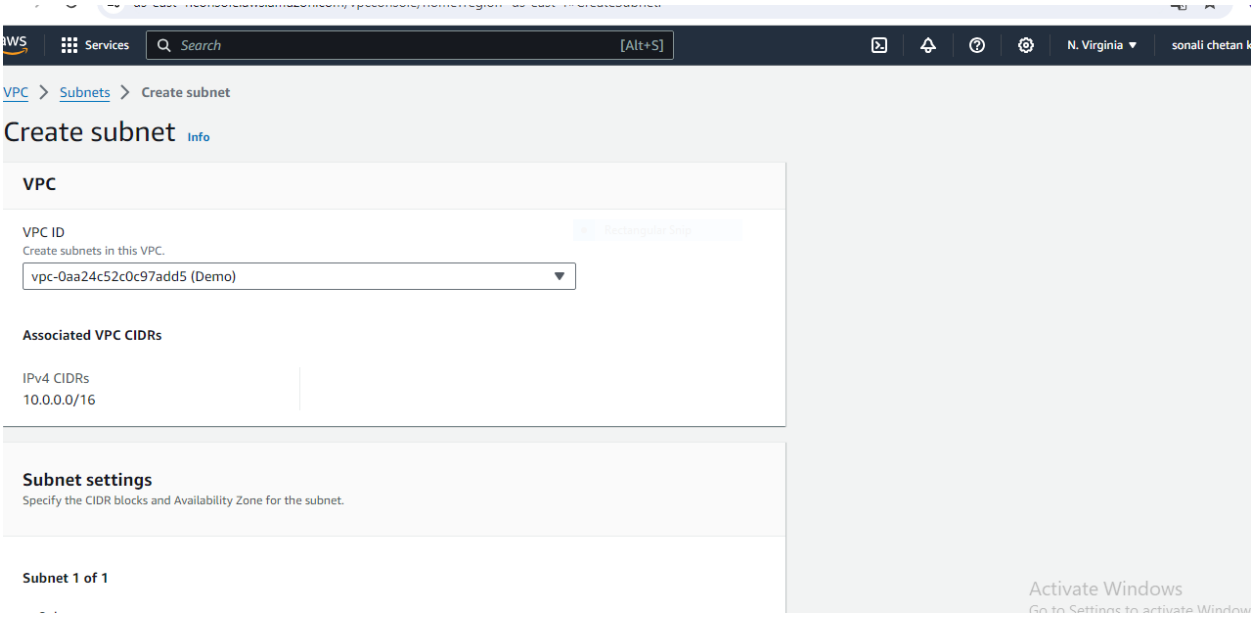


Step 4 : Create Subnet

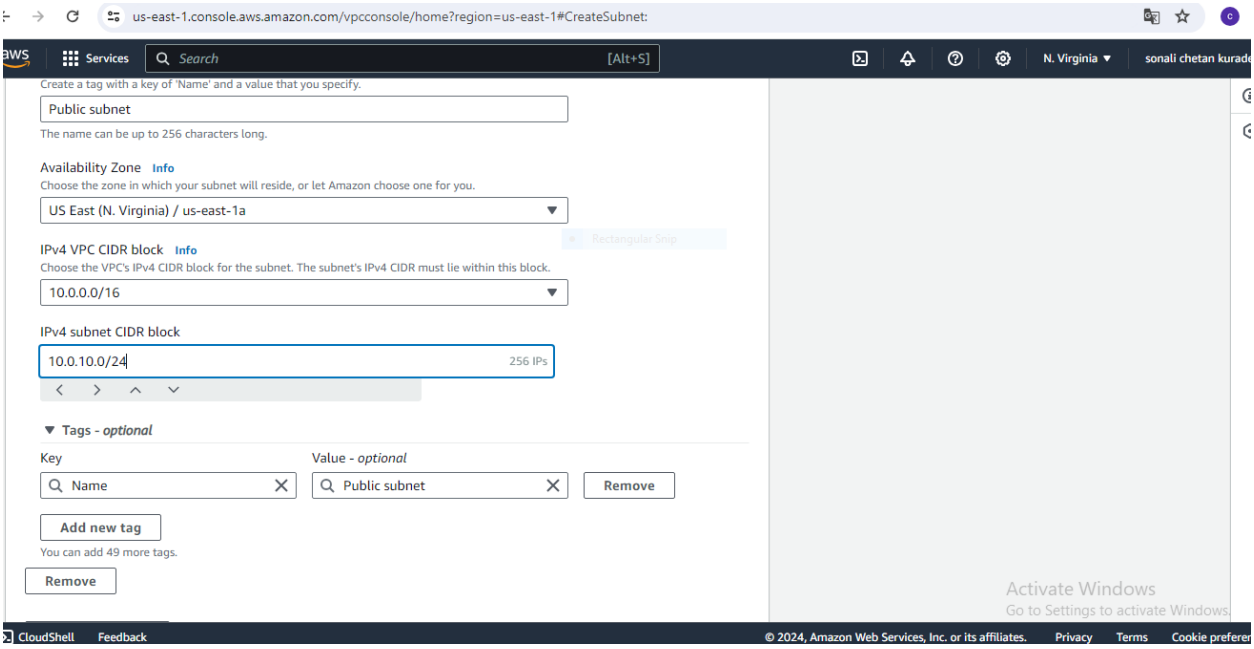
- To start creating subnet , in the left down side, click on Create **subnets**:



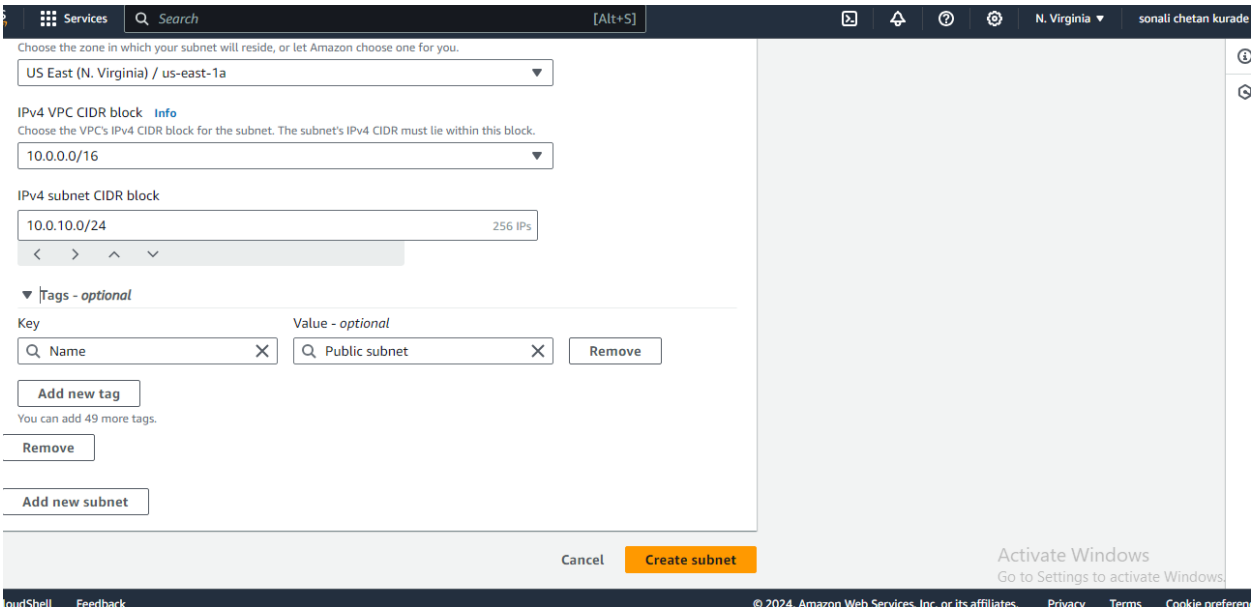
- Click on **Create Subnet** and select newly created vpc



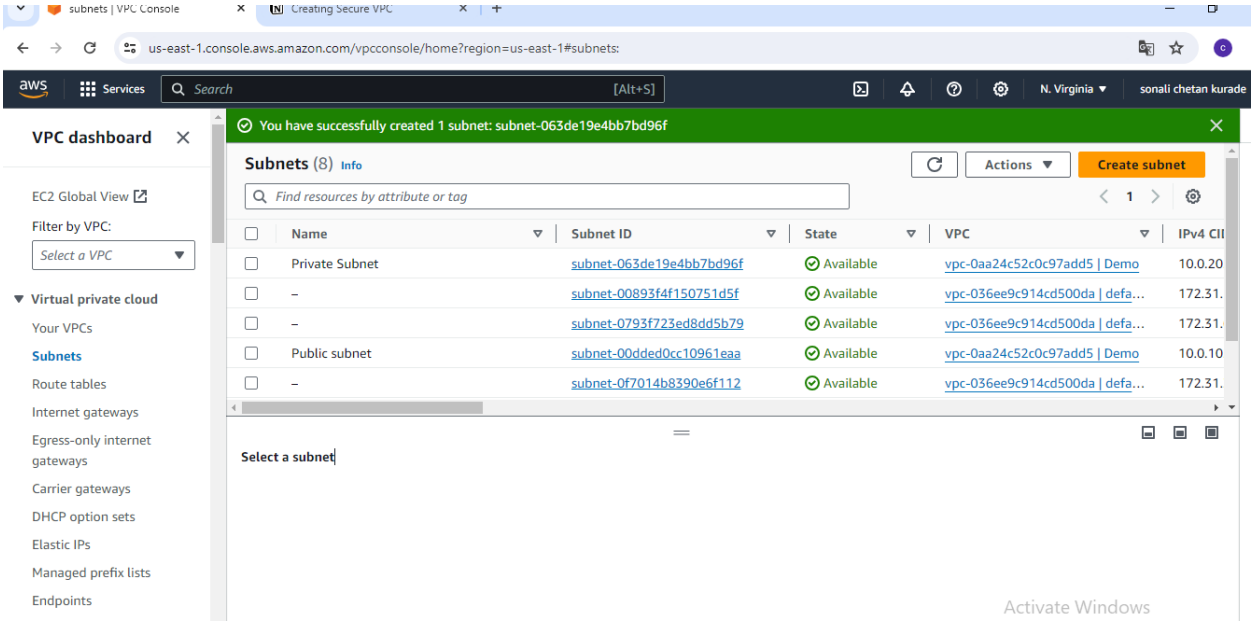
- Give name for that subnet and Select availability zone and enter the CIDR range



- Click on Create subnet

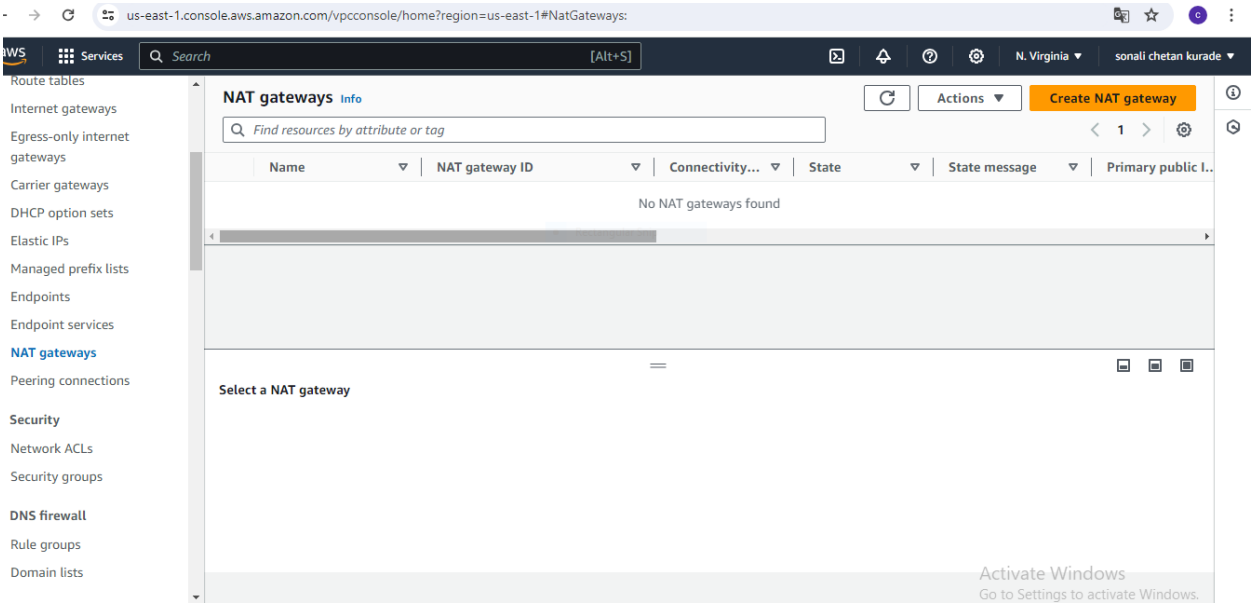


- Create another subnet that is private subnet same like above procedure.
- Finally two subnet is created

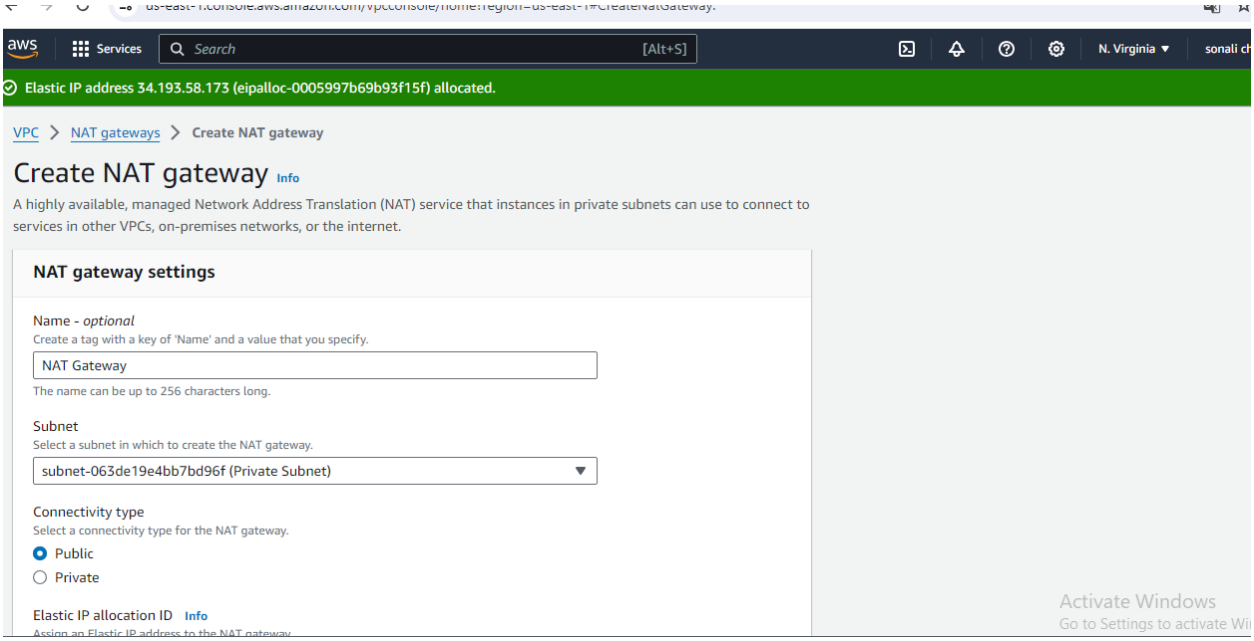


Step 5: Create NAT Gateway

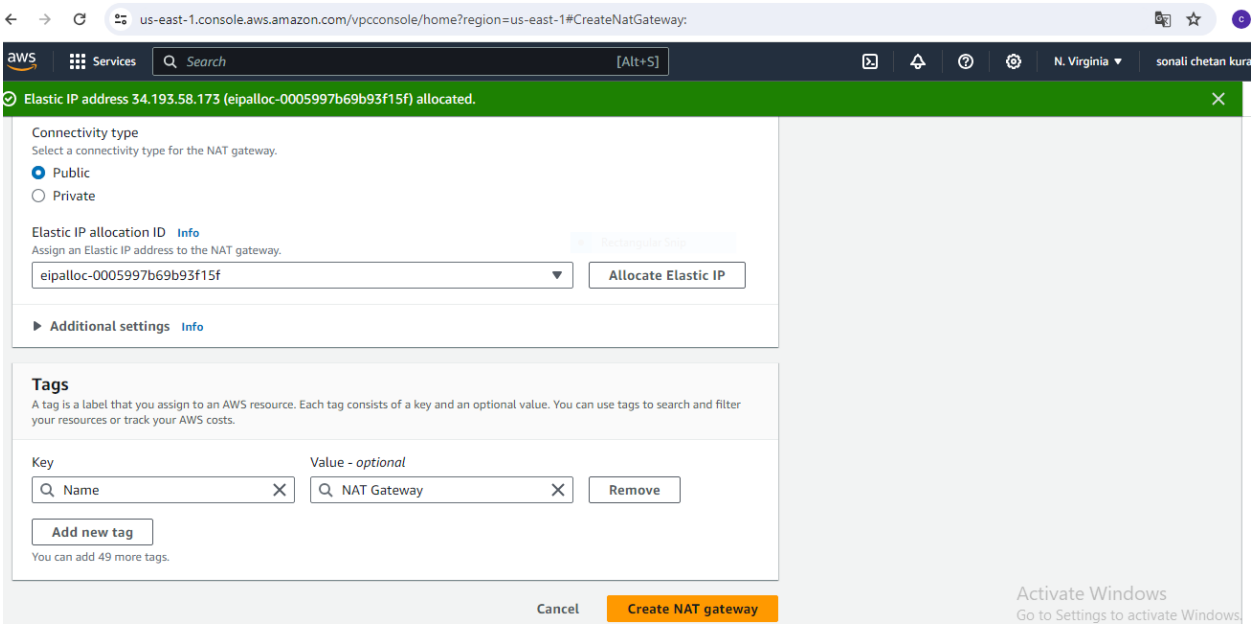
- To start creating NAT Gateway , in the left down side, click on Create **NAT Gateways**:



- Click on create **NAT Gateway** give name for that and select private subnet

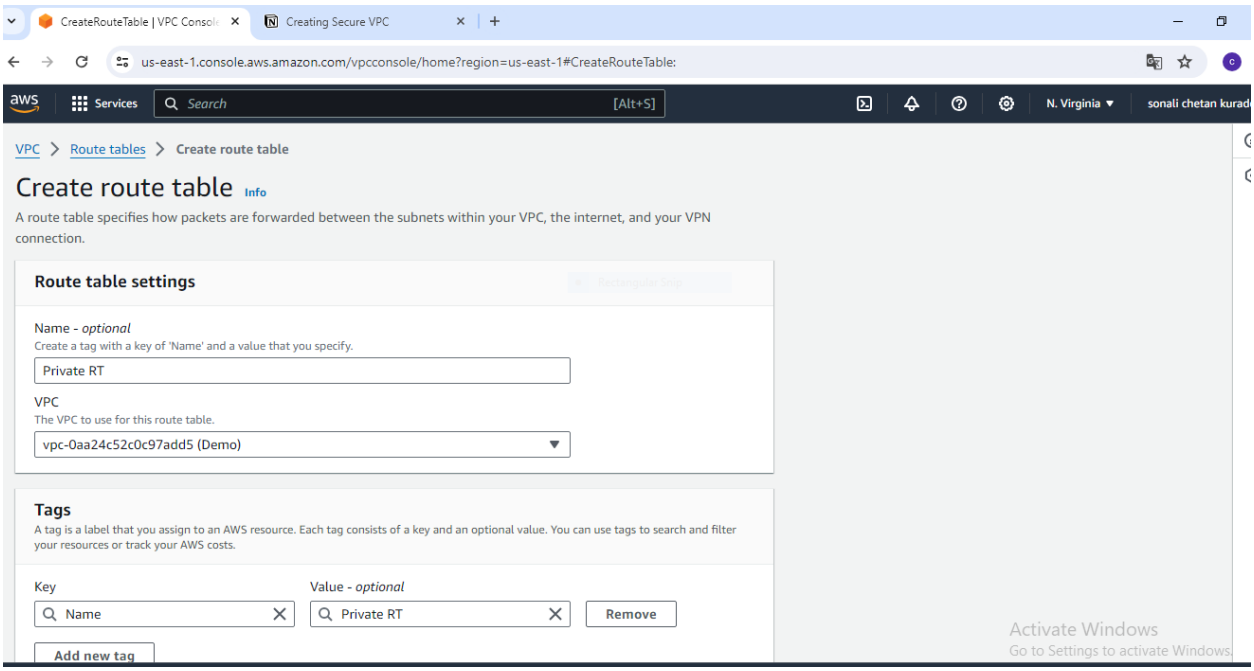


- Allocate Elastic IP and click on create NAT gateway

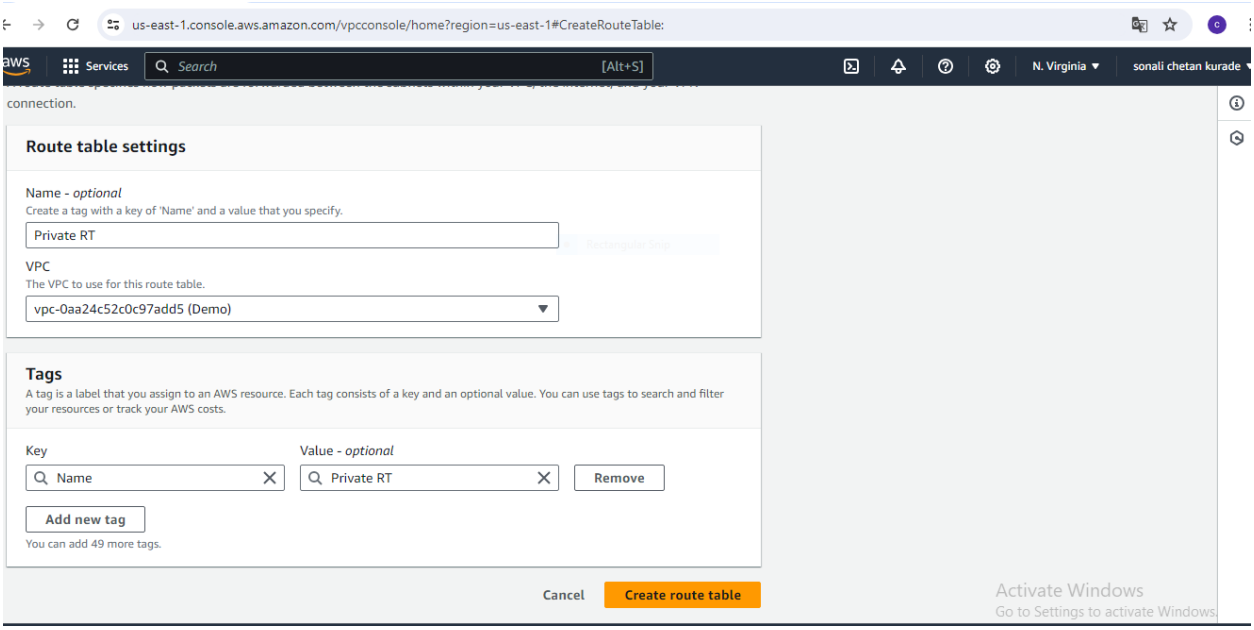


Step 6: Create Route table

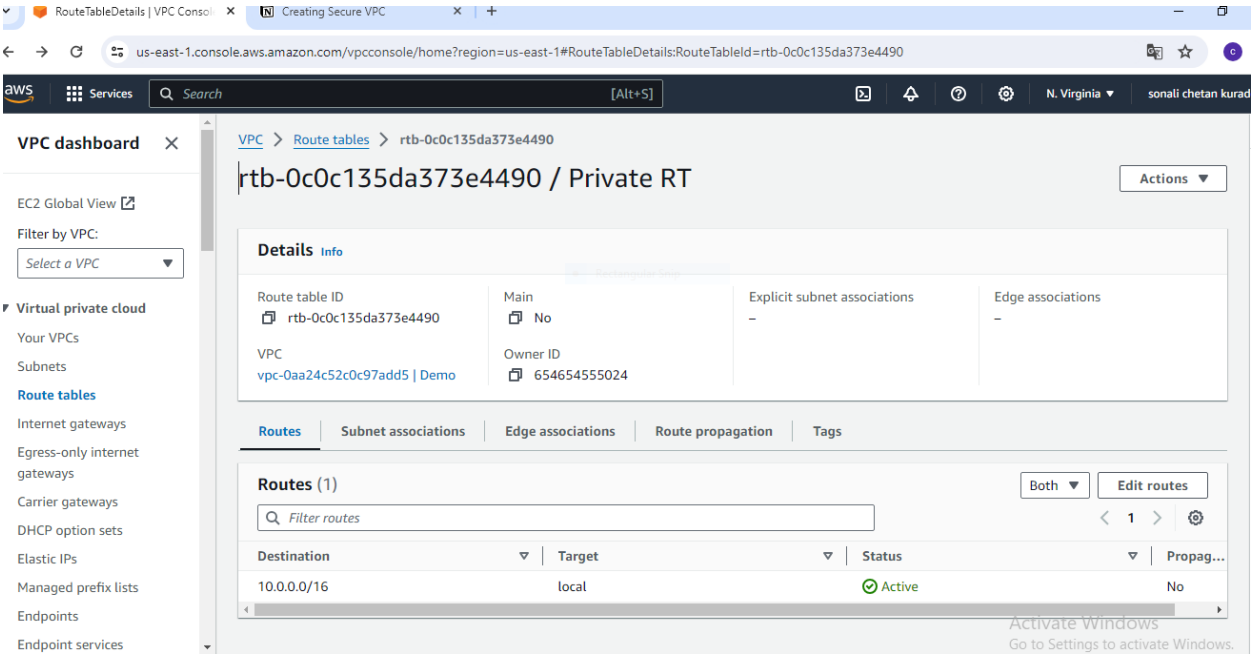
- To start creating Route table, in the left down side, click on Create **Route Table** :



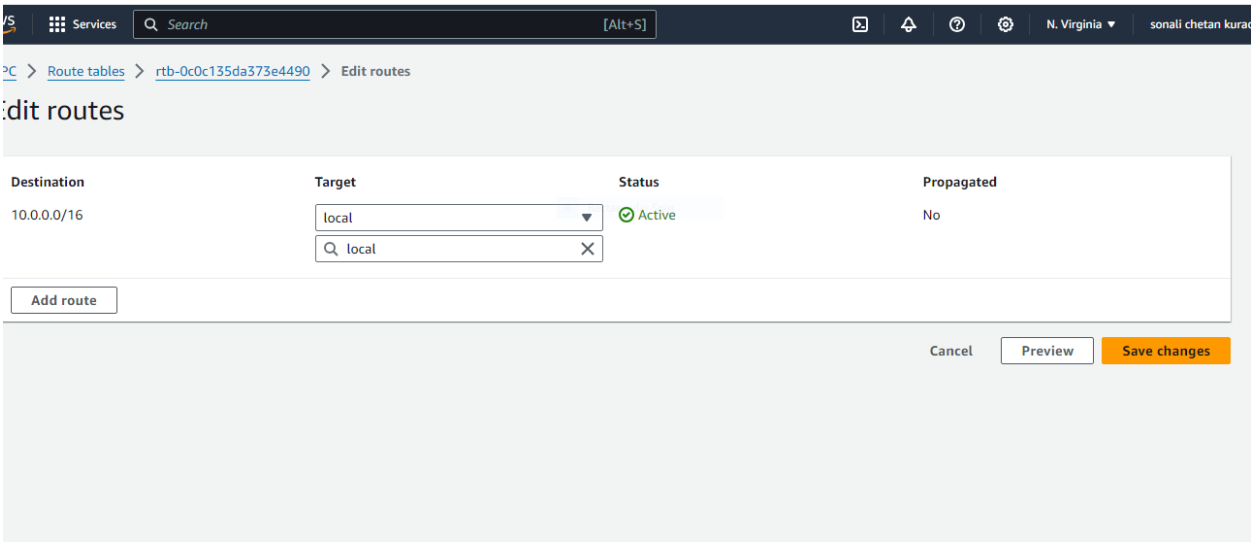
- Select Vpc and Click on **Create route table**



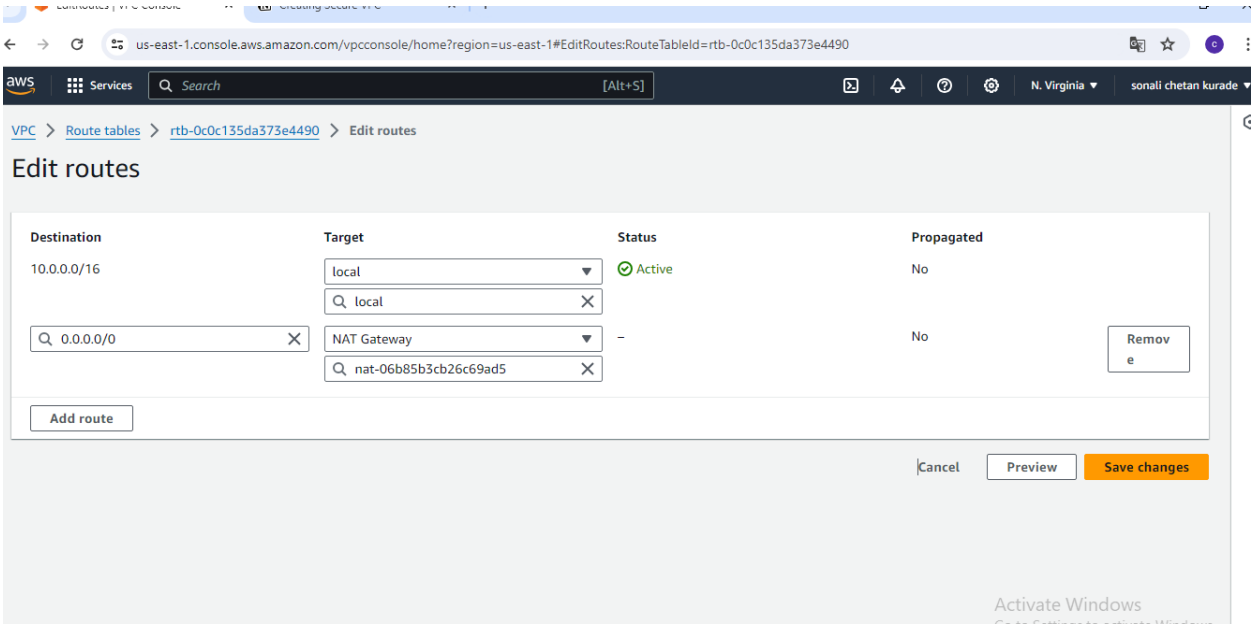
- Route table is created successfully. Same ways you have to create two route tables and add route to it.



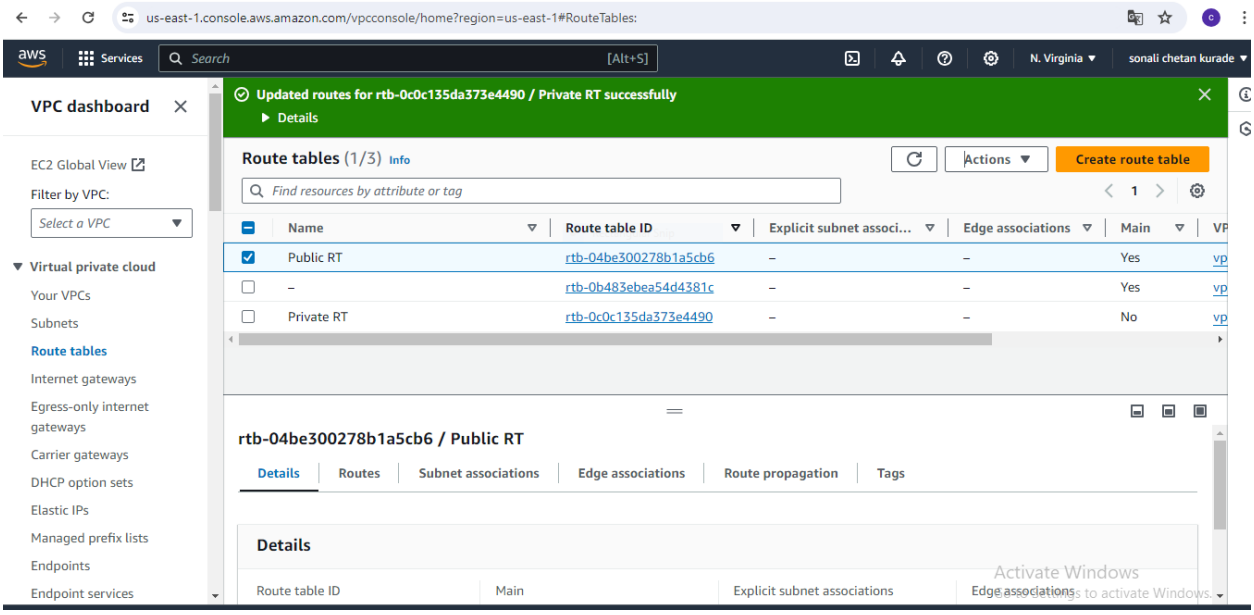
- To add the Route in route table go inside the route table and select option **Edit route**



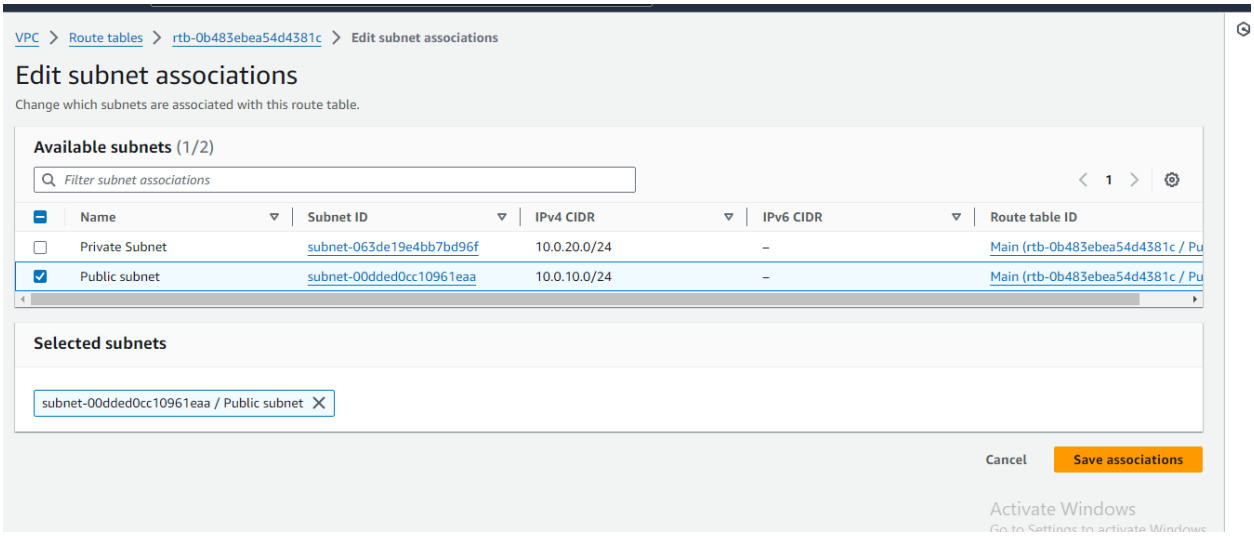
- Click on **Add Route** add route into it.
- select destination 0.0.0.0/0 (anywhere) and target is NAT gateway in private route table
- select destination 0.0.0.0/0 (anywhere) and target is Internet gateway in public route table



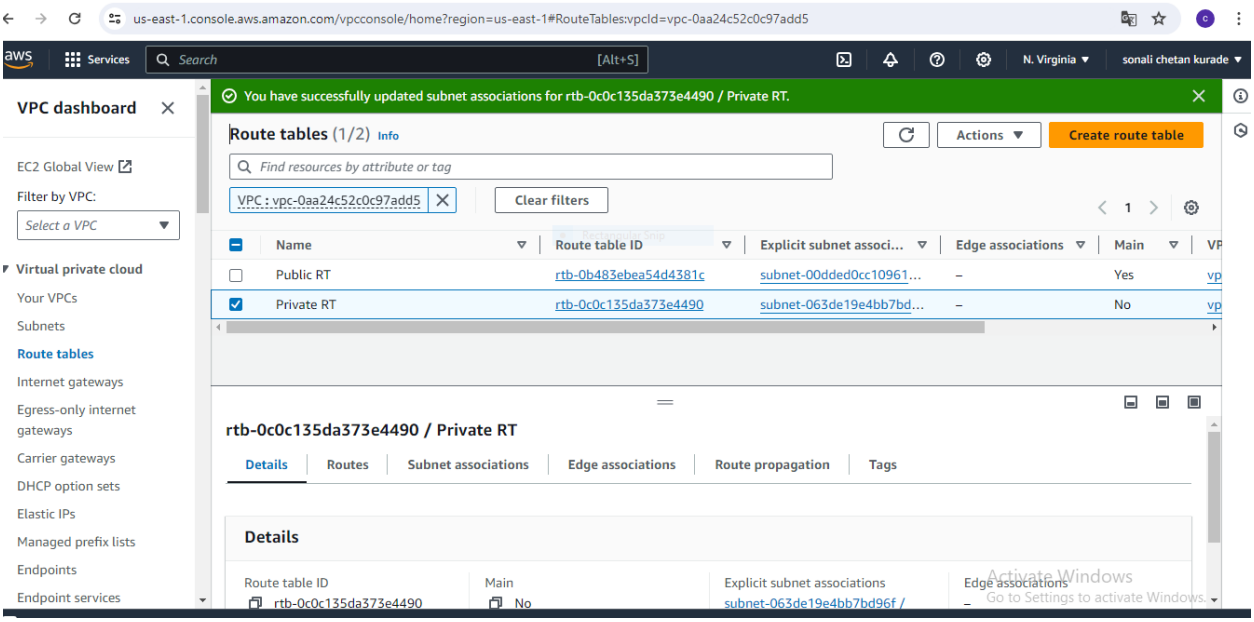
- Attach Route table to Subnet



- Click on Action and select the option **Edit Subnet Asociation select the subnet**

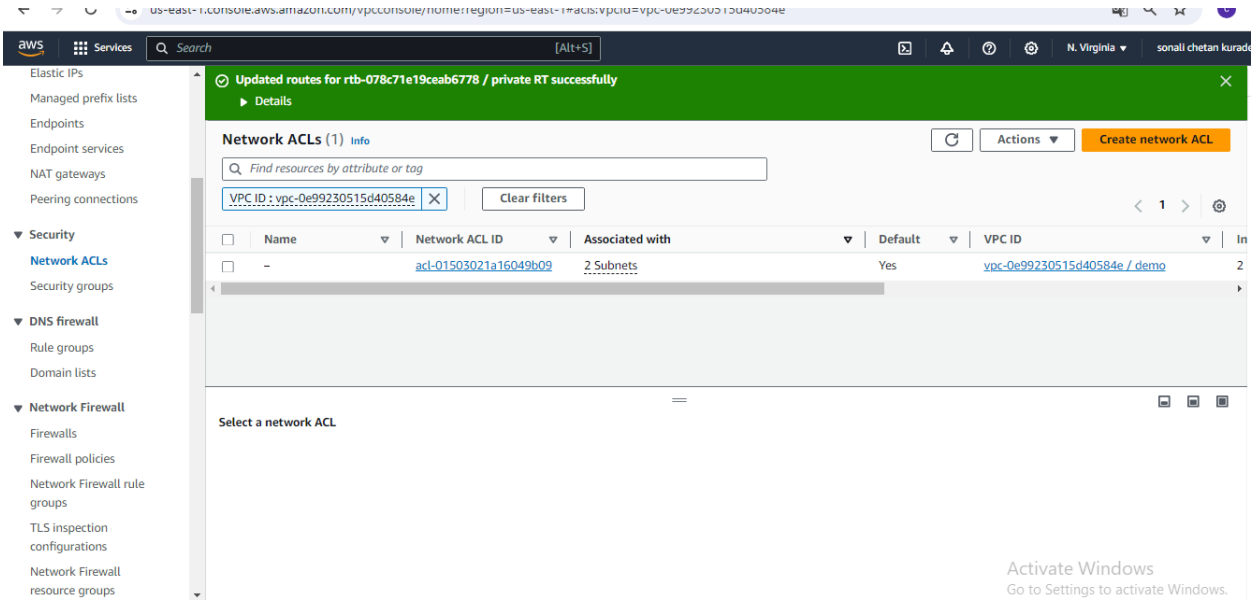


- Attached successfully

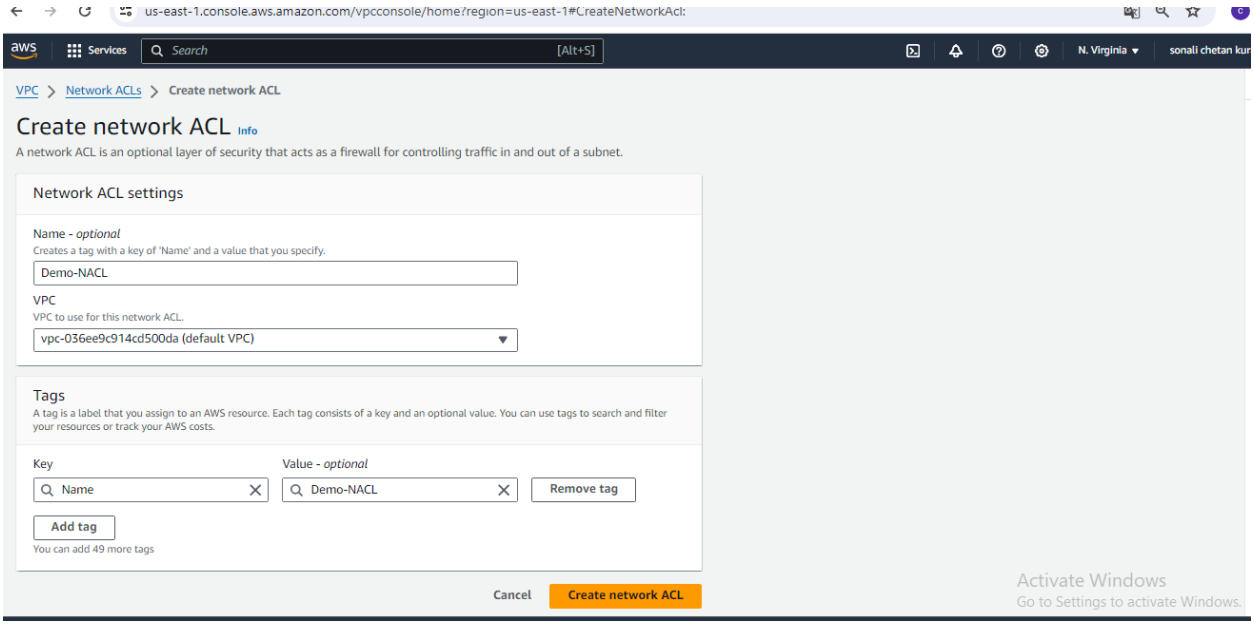


Step 7: Creating NACL

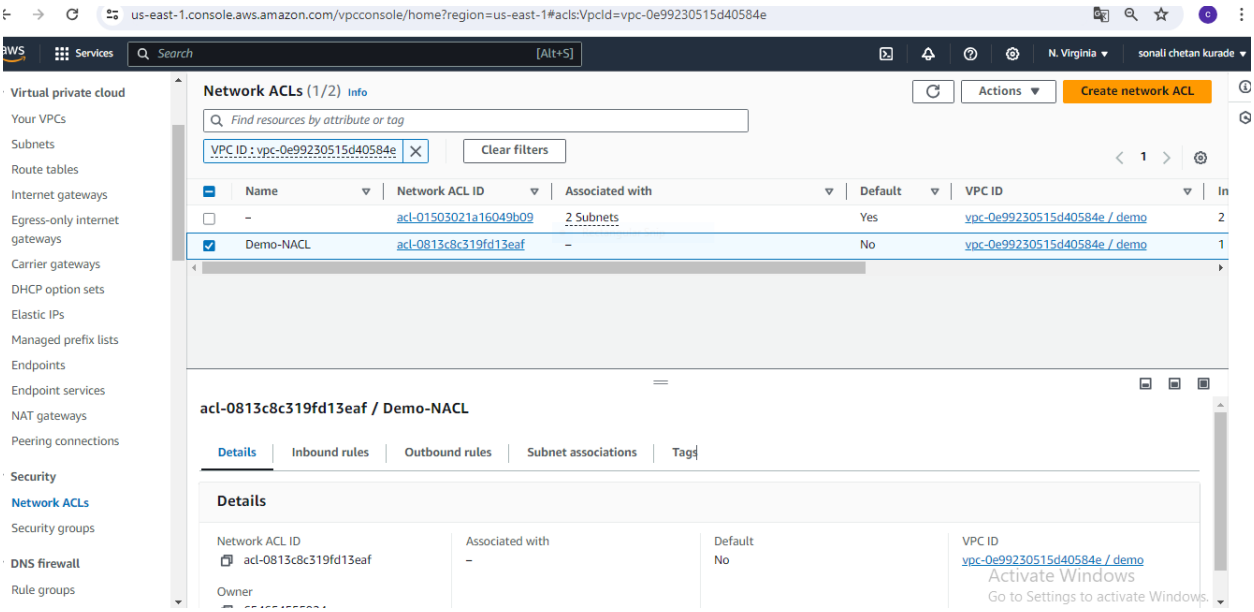
- To start creating NACL, in the left down side, click on **Network ACL.** Click on **Create Network ACL**



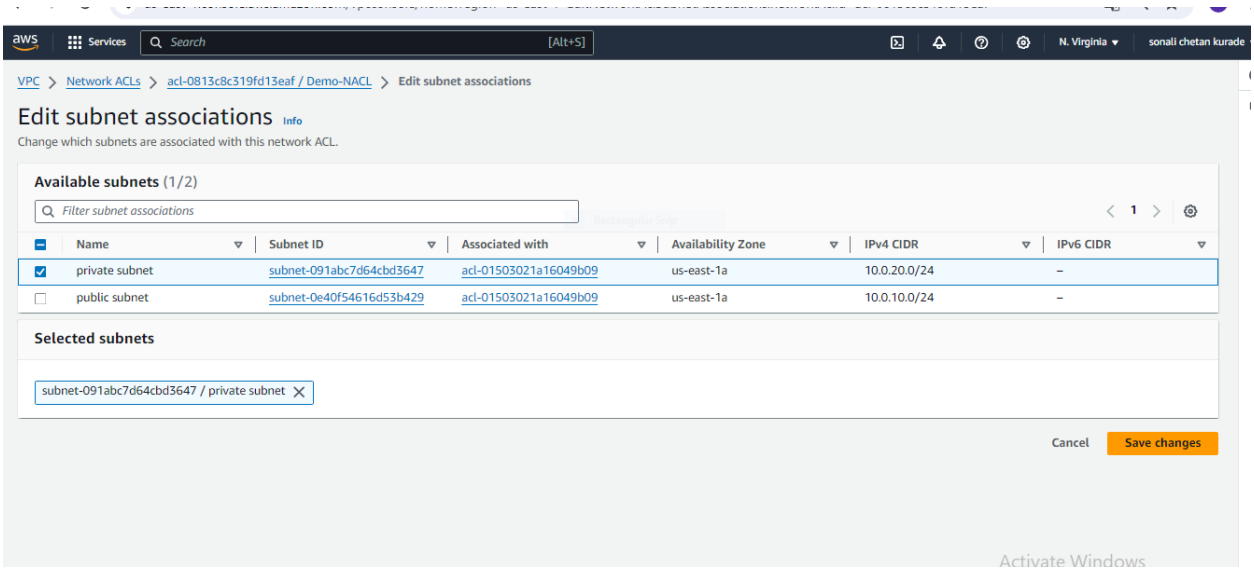
- Enter the details like Name and VPC and click on **Create network ACL**



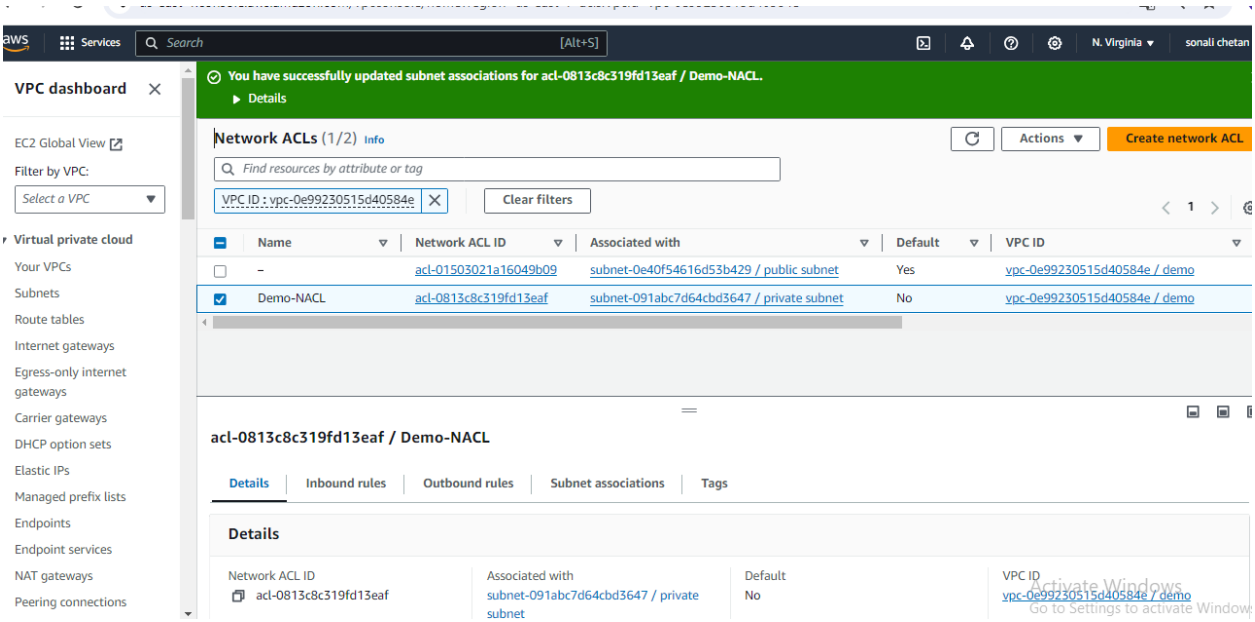
- Attach this NACL to Private subnet. Select NACL which we have created previously and click on **action.** Select the option **Edit subnet association.**



- Select private subnet and click on **save changes**



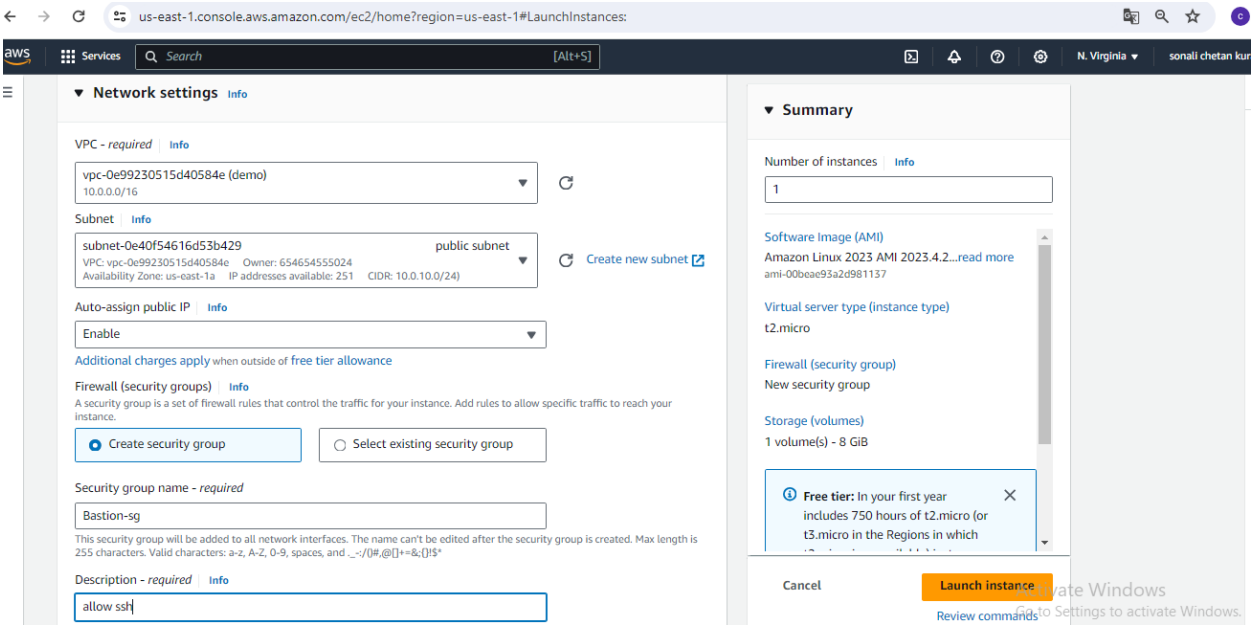
- subnet Association is completed successfully



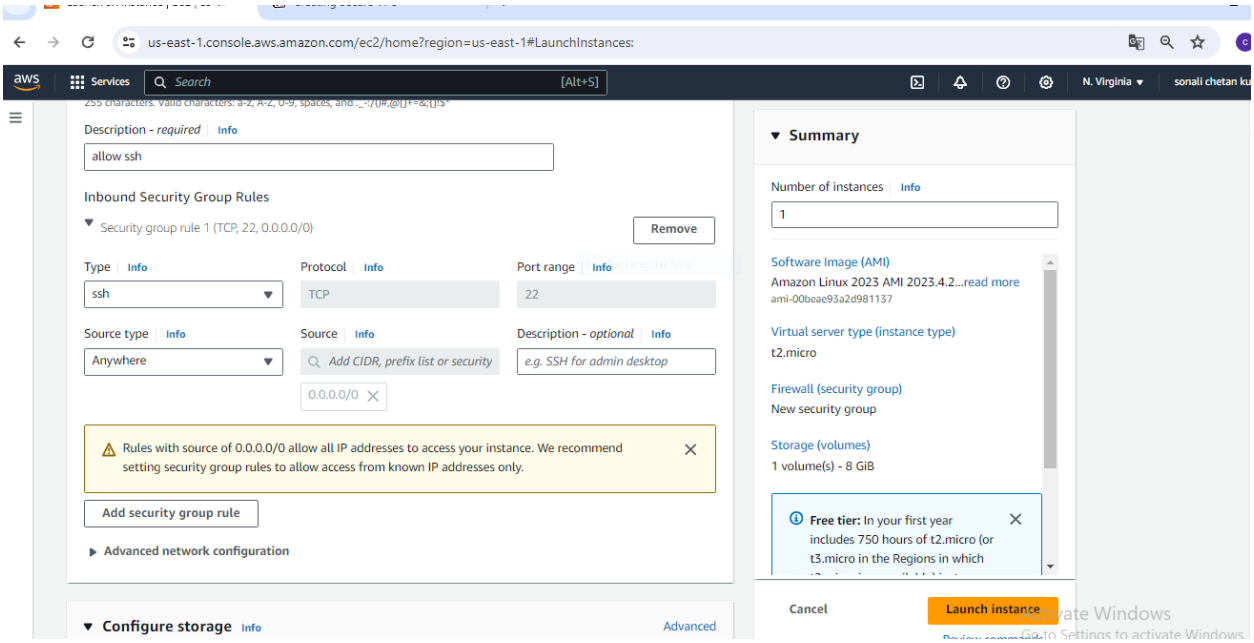
Step 8: Creating Bastion host

- In the AWS Management Console search bar, enter EC2, and click the EC2 result under Services:
- To start creating Bastion host, in the left down side, click on **Instances.** Click on **Launch Instance**
- Give the name **bastion** and select the Image

- Select the key Pair
- Click on Edit Network
- Select the VPC and public Subnet
- Enable the **Auto-assign public IP**
- Create a Security Group. Give name to that security group (bastion-sg)and and description

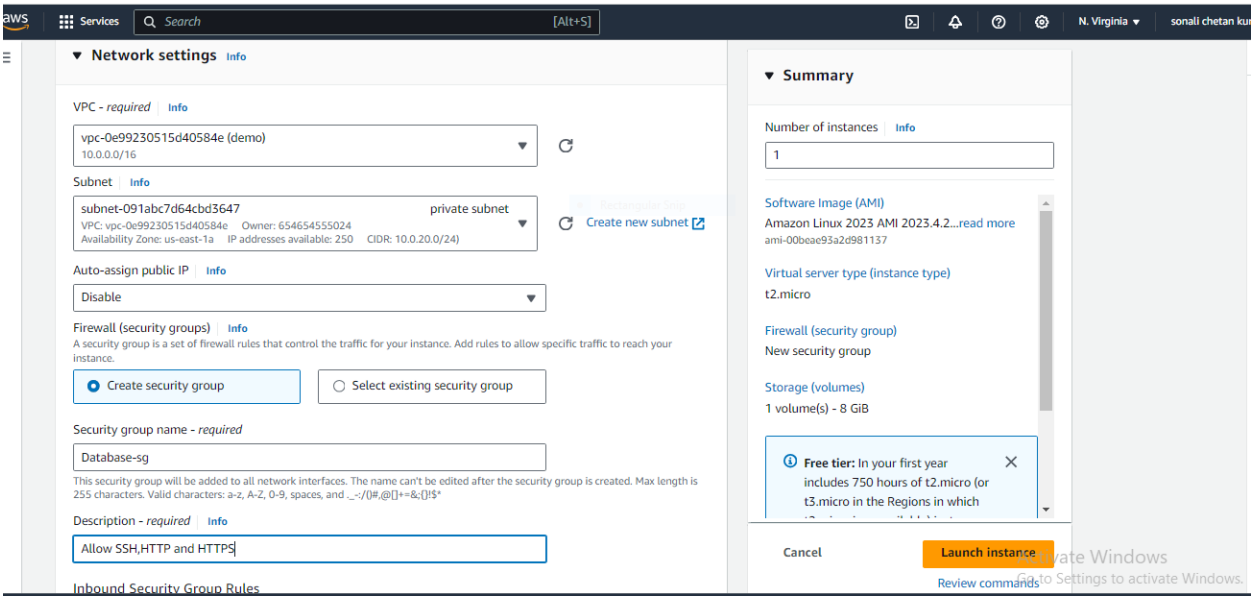


- Add the inbound rule and click on **launch instance** to launch instance.

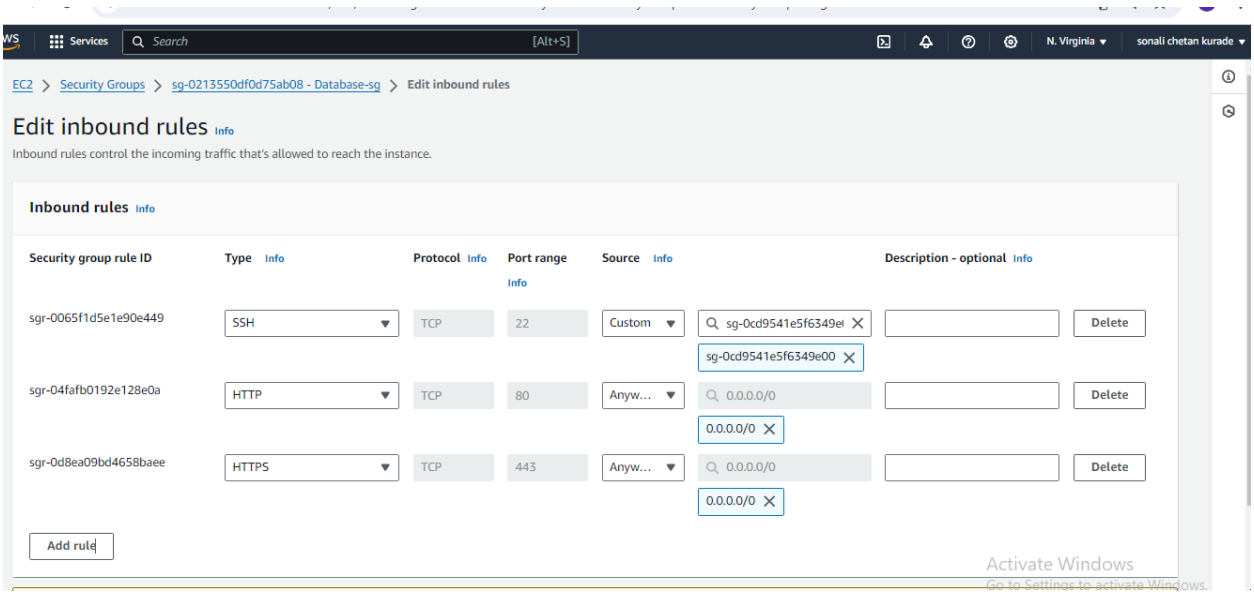


Step 9 : Creating Database Server

- In the AWS Management Console search bar, enter EC2, and click the EC2 result under Services:
- To start creating Bastion host, in the left down side, click on **Instances.** Click on **Launch Instance**
- Give the name **Database** and select the Image
- Select the key Pair
- Click on Edit Network
- Select the VPC and private Subnet
- Disable the **Auto-assign public IP**
- Create a Security Group. Give name to that security group(database-sg) and and description



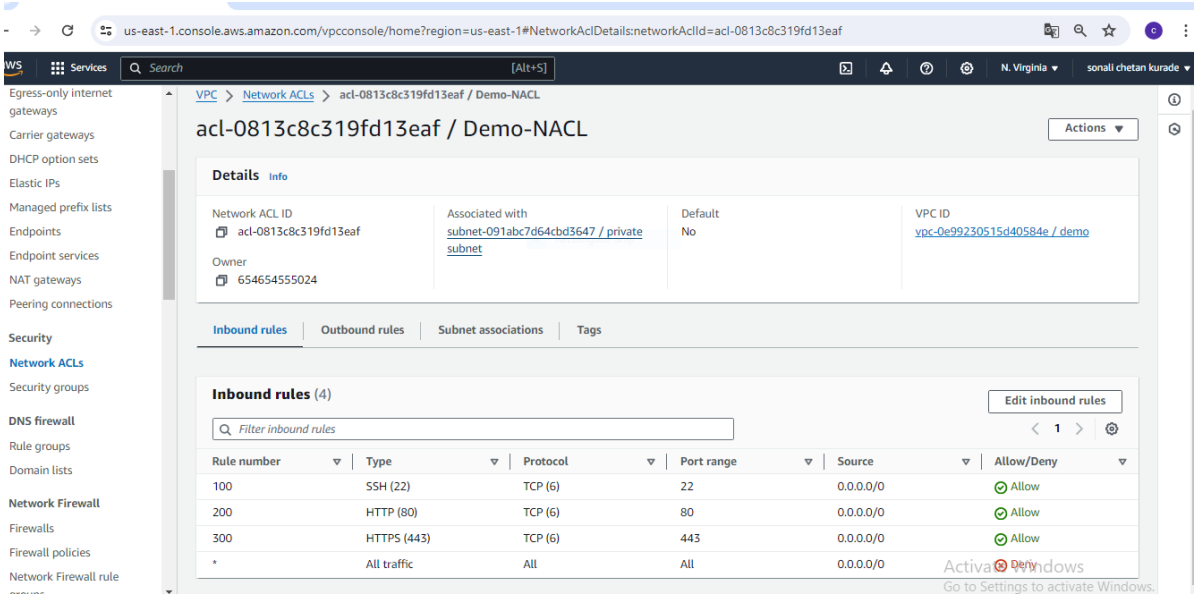
- Add the Inbound rule ssh,http,https and click on **launch instance**



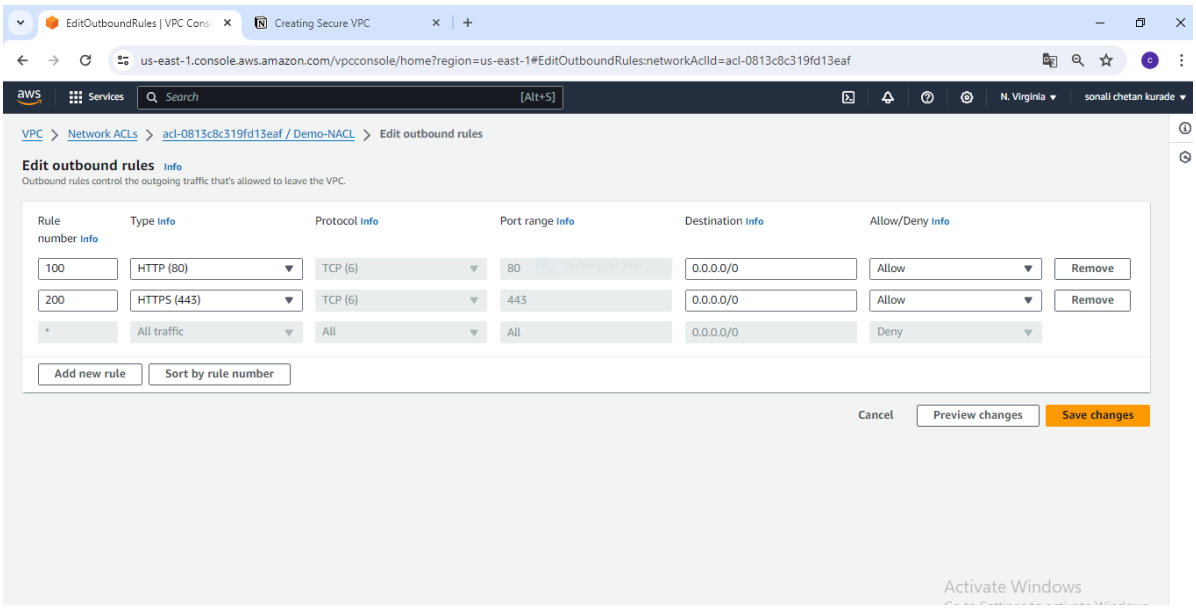
Step 10 : Add the Inbound and Outbound Rules to in NACL

- In the left down side, click on **Network ACL.** Select the NACL which we have created.

- And add inbound rule and click edit inbound rule after adding the rule click on save changes
    - ssh
    - http
    - https



- And add outbound rule
    - http
    - https


EditOutboundRules | VPC Cons
Creating Secure VPC
us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#EditOutboundRules:networkAclId=acl-0813c8c319fd13eaf
aws
Services
Search
[Alt+S]
N. Virginia
sonali chetan kurade
VPC > Network ACLs > acl-0813c8c319fd13eaf / Demo-NACL > Edit outbound rules
Edit outbound rules Info
Outbound rules control the outgoing traffic that's allowed to leave the VPC.
Rule number Info
Type Info
Protocol Info
Port range Info
Destination Info
Allow/Deny Info
100
HTTP (80)
TCP (6)
80
0.0.0.0/0
Allow
Remove
200
HTTPS (443)
TCP (6)
443
0.0.0.0/0
Allow
Remove
*
All traffic
All
All
0.0.0.0/0
Deny
Add new rule
Sort by rule number
Cancel
Preview changes
Save changes
Activate Windows