Cloud Essentials

Project Solution

Problem Statement:

John is a newbie to the cloud computing domain; he is exploring AWS and is comfortable with creating most of the AWS services. However, he struggles in creating a Virtual Private Cloud (VPC) using the console in the AWS platform. He would need you to assist him in creating a Virtual Private Cloud. While creating a VPC make sure that you:

• Create an Amazon VPC using the VPC wizard, and it should be displayed on the dashboard

• Associate an Elastic IP address with it

• Explore various resources of VPC such as Internet Gateway, NAT Gateway, Subnets, Security Groups

• Launch a NAT Gateway so that internet access is provided to private resources

• Introduce a Public subnet for resources facing the internet such as a web server and a Private subnet for resources at the back end such as database server

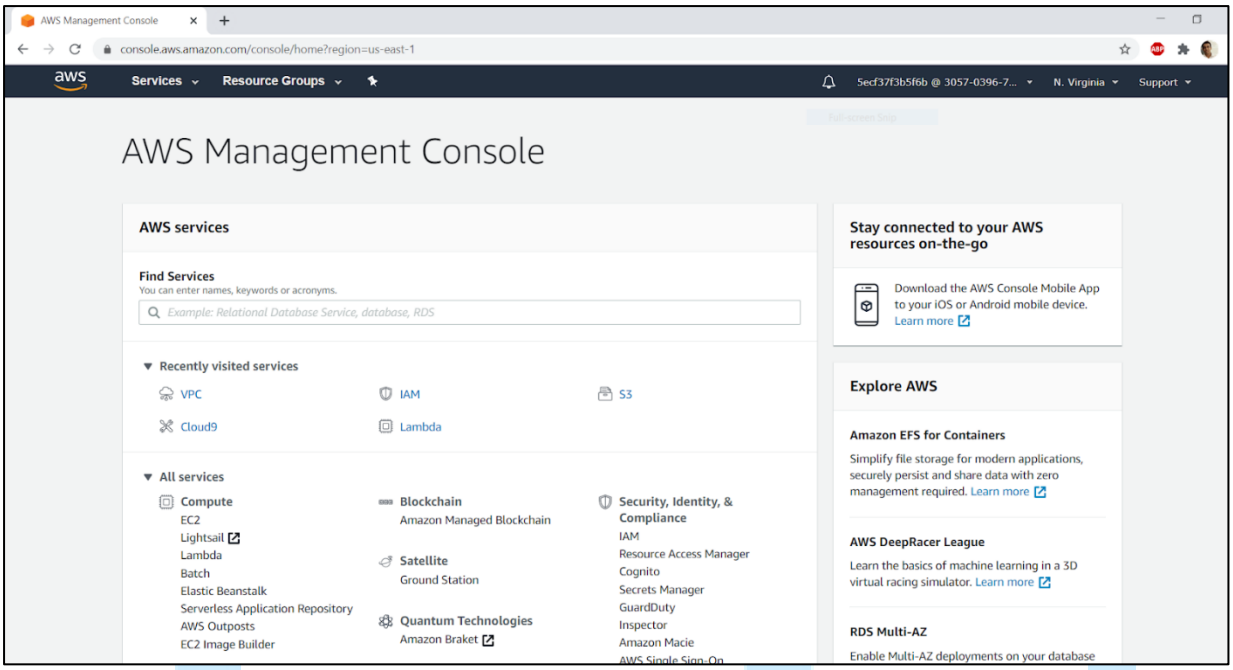
• Define security groups with appropriate inbound rules

• Ensure proper routes and corresponding Route tables entries specifying the traffic moving out of the subnet

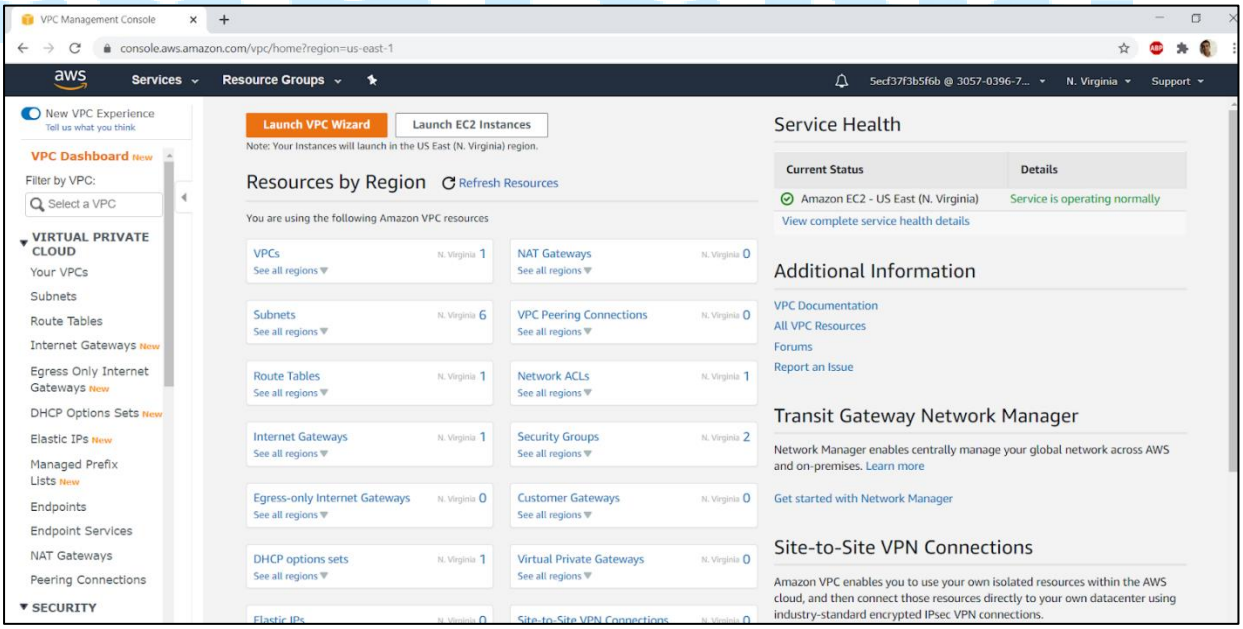
• Make use of Network ACLs for controlling inbound and outbound traffic in the VPC

Solution Steps:

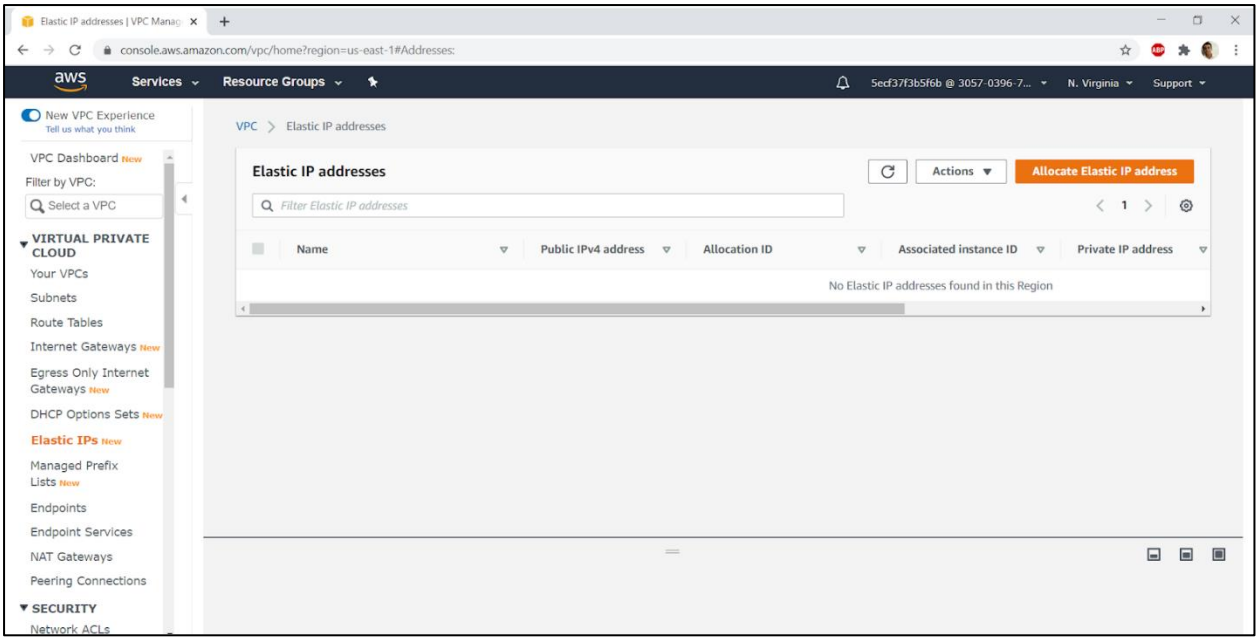
Step 1: Login to the **AWS Management Console** and navigate to **VPC** from the Services Menu.

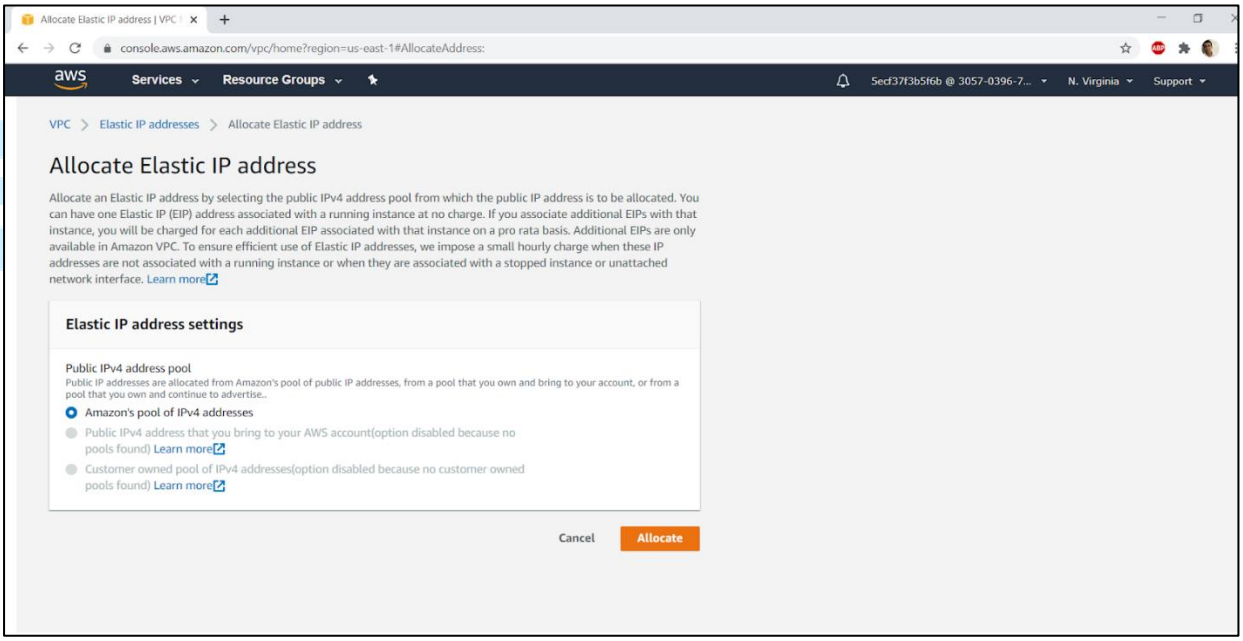


Step 2: First, we will create a static IP address i.e. the Elastic IP Address.
On the left navigation menu click **Elastic Ips.**

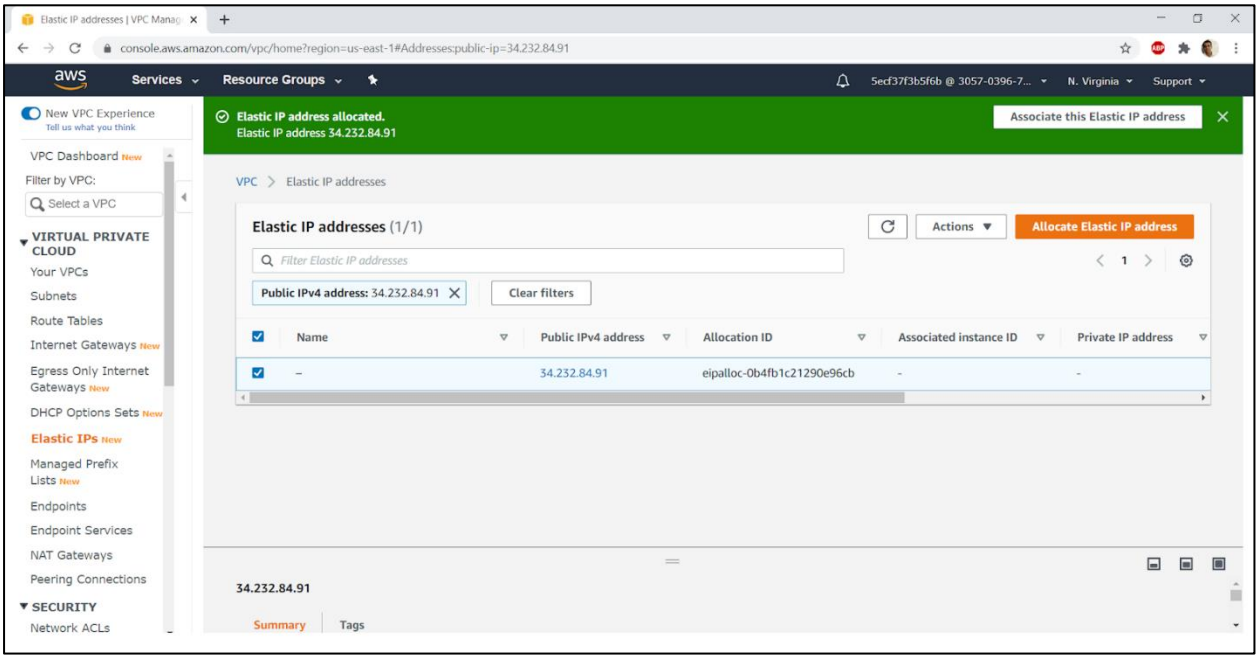


Step 3: Next ,we click on **Allocate Elastic IP address** and then click **Allocate** on the next page.

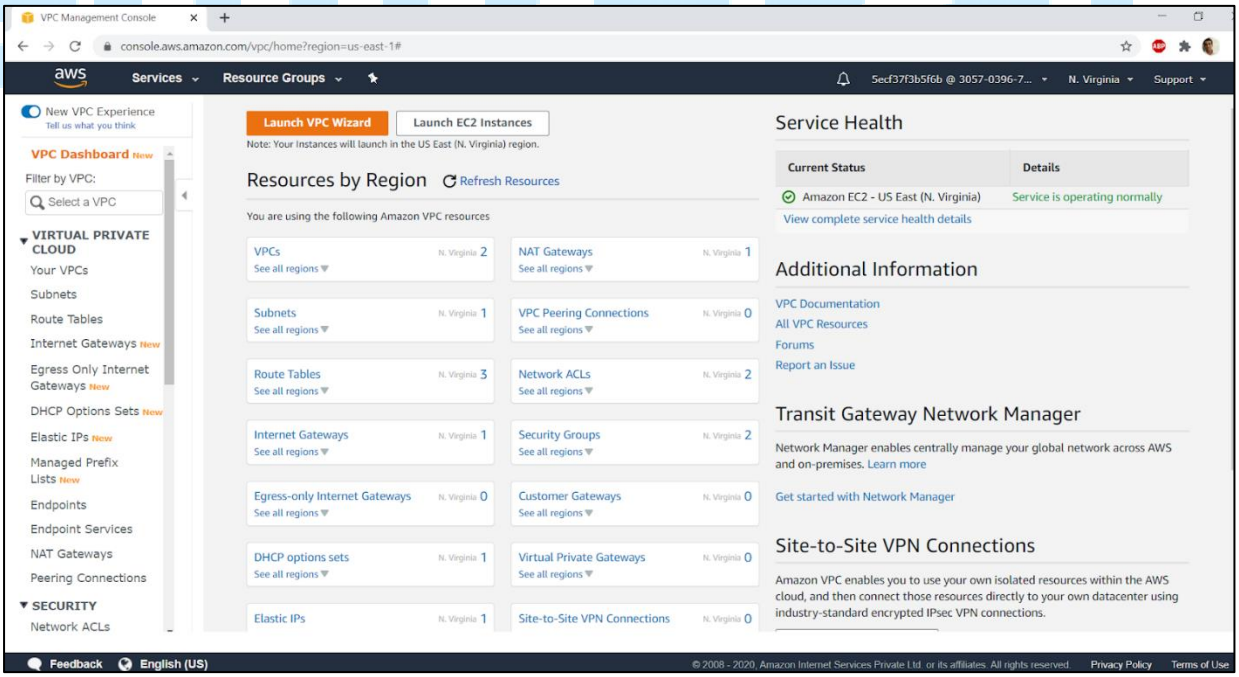

Elastic IP addresses | VPC Manag
console.aws.amazon.com/vpc/home?region=us-east-1#Addresses:
aws
Services
Resource Groups
5ecf37f3b5f6b @ 3057-0396-7...
N. Virginia
Support
New VPC Experience
Tell us what you think
VPC Dashboard New
Filter by VPC:
Select a VPC
VIRTUAL PRIVATE CLOUD
Your VPCs
Subnets
Route Tables
Internet Gateways New
Egress Only Internet Gateways New
DHCP Options Sets New
Elastic IPs New
Managed Prefix Lists New
Endpoints
Endpoint Services
NAT Gateways
Peering Connections
SECURITY
Network ACLs
VPC > Elastic IP addresses
Elastic IP addresses
Actions
Allocate Elastic IP address
Filter Elastic IP addresses
1
Name
Public IPv4 address
Allocation ID
Associated instance ID
Private IP address
No Elastic IP addresses found in this Region


Allocate Elastic IP address | VPC
console.aws.amazon.com/vpc/home?region=us-east-1#AllocateAddress:
aws
Services
Resource Groups
5ecf37f3b5f6b @ 3057-0396-7...
N. Virginia
Support
VPC > Elastic IP addresses > Allocate Elastic IP address
Allocate Elastic IP address
Allocate an Elastic IP address by selecting the public IPv4 address pool from which the public IP address is to be allocated. You can have one Elastic IP (EIP) address associated with a running instance at no charge. If you associate additional EIPs with that instance, you will be charged for each additional EIP associated with that instance on a pro rata basis. Additional EIPs are only available in Amazon VPC. To ensure efficient use of Elastic IP addresses, we impose a small hourly charge when these IP addresses are not associated with a running instance or when they are associated with a stopped instance or unattached network interface. Learn more
Elastic IP address settings
Public IPv4 address pool
Public IP addresses are allocated from Amazon's pool of public IP addresses, from a pool that you own and bring to your account, or from a pool that you own and continue to advertise..
Amazon's pool of IPv4 addresses
Public IPv4 address that you bring to your AWS account(option disabled because no pools found) Learn more
Customer owned pool of IPv4 addresses(option disabled because no customer owned pools found) Learn more
Cancel
Allocate

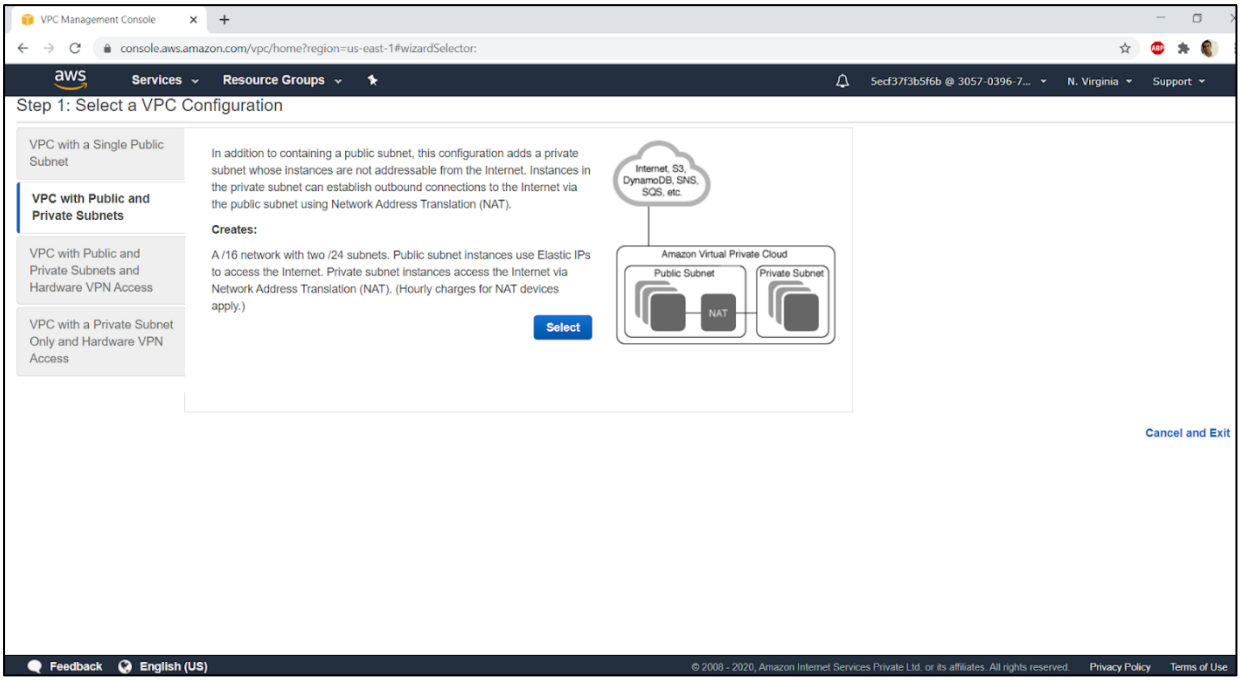
Step 4: An Elastic IP address will be assigned and is ready to use.



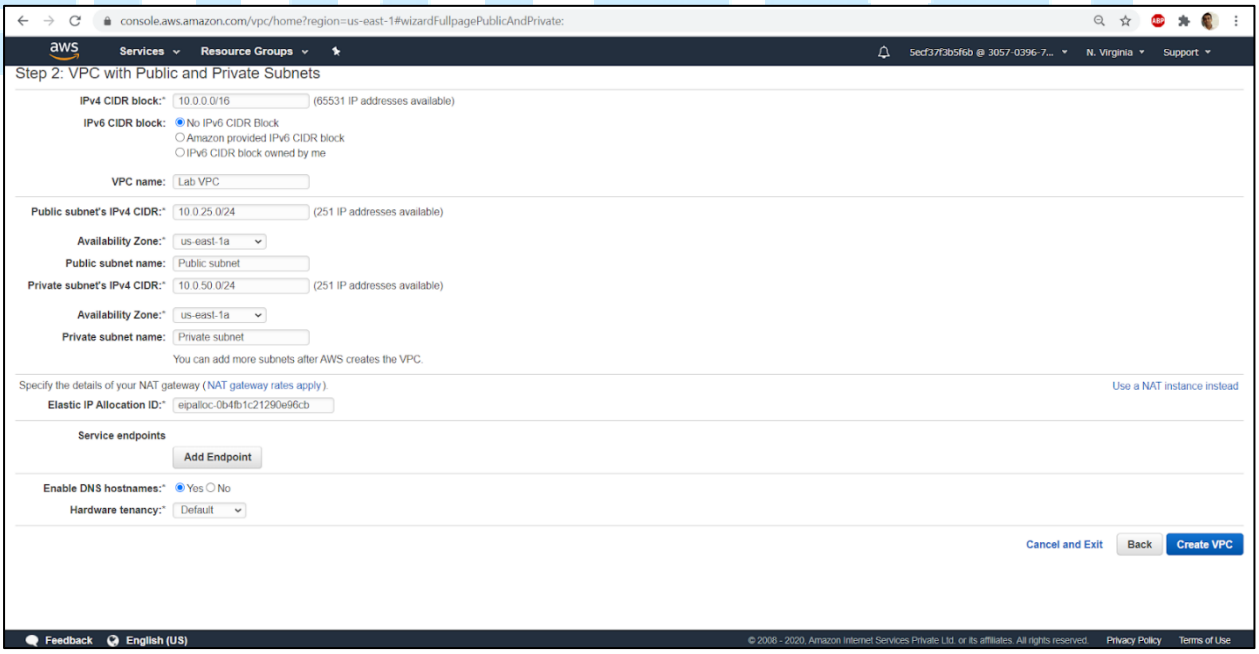
Step 5: Once done, we go back to the VPC page and click on the **Launch VPC Wizard** to create a VPC.



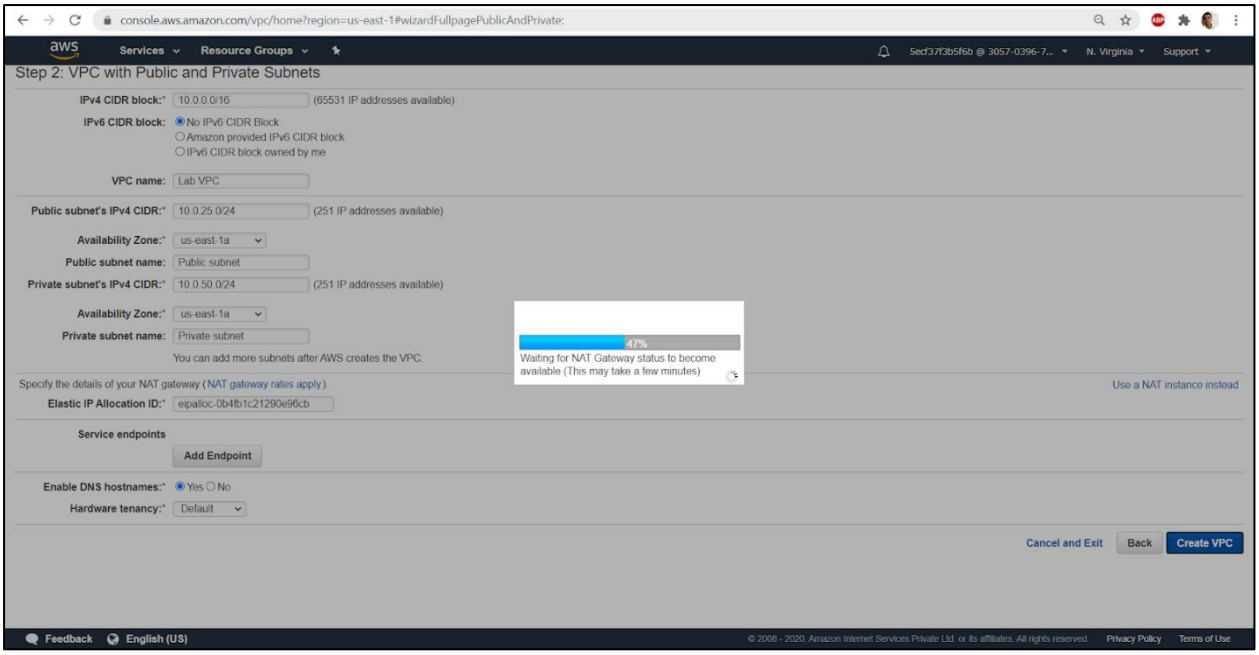
Step 6: From the list of given options, we select **VPC with Public and Private Subnets** and proceed.



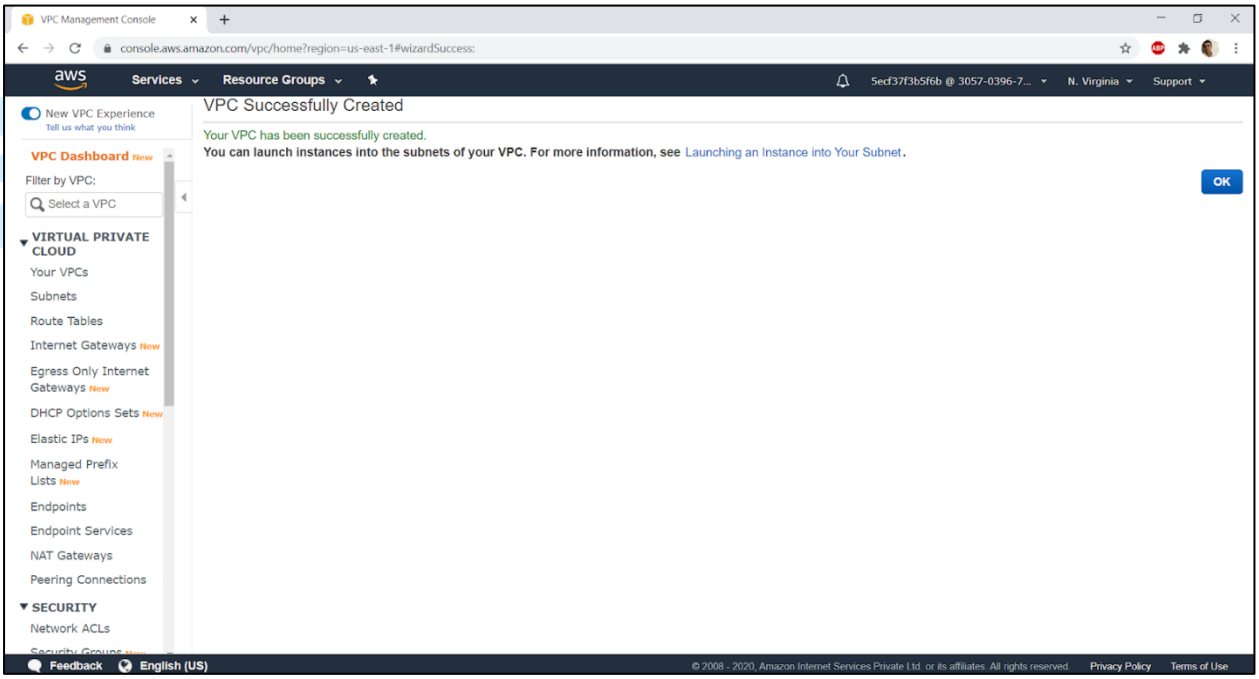
Step 7: On the next step, we fill in the relevant details such as VPC name, Public subnet IPv4 CIDR and its Availability Zone and Private subnet IPv4 CIDR and its Availability zone, Elastic IP address that we created in the earlier steps etc. and click on **Create VPC**.



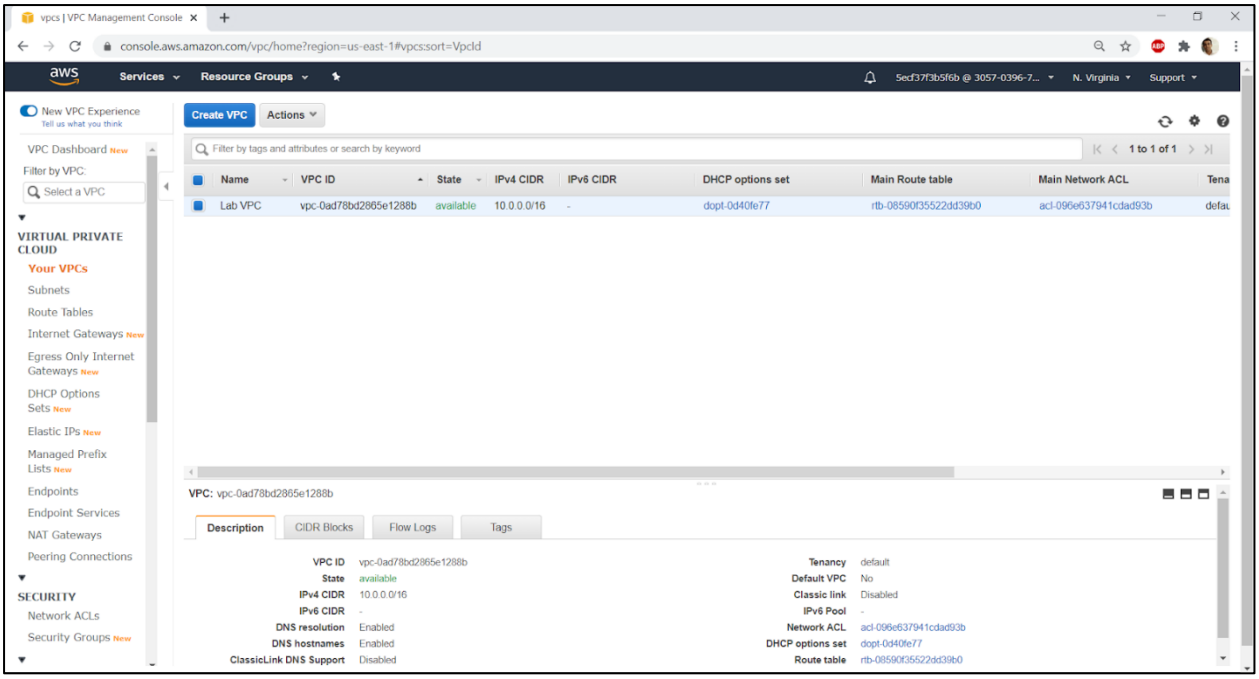
Step 8: A status windows is displayed that shows the current progress of creation of required resources.



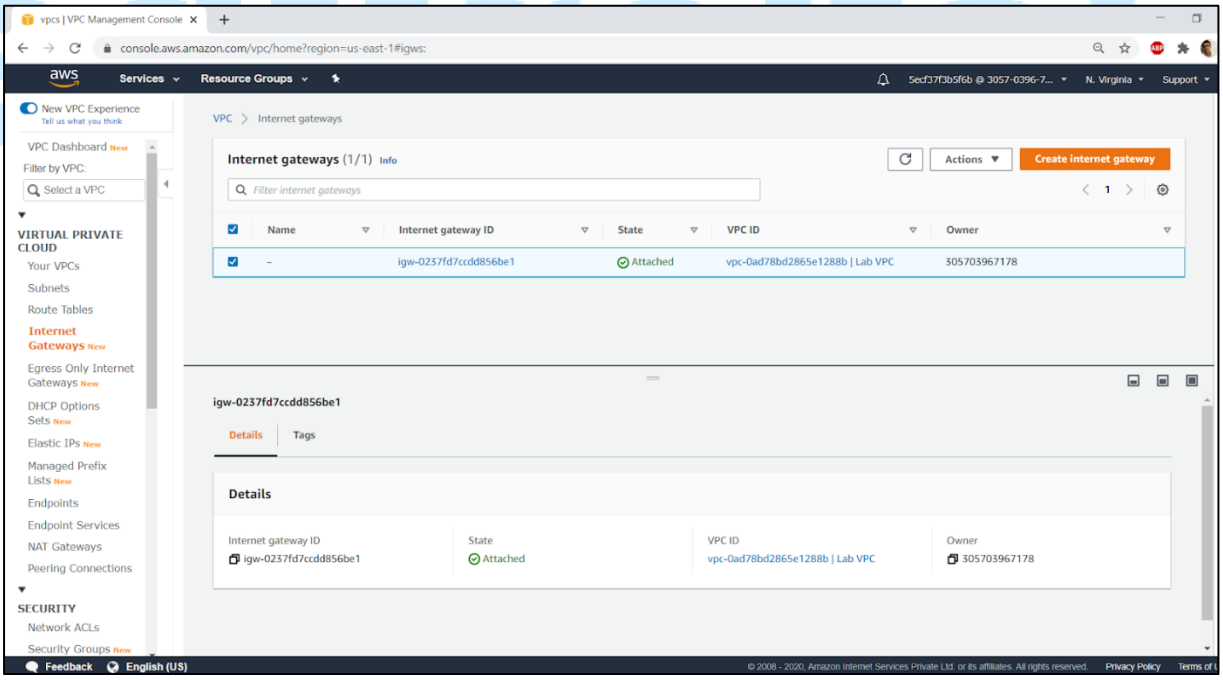
Step 9: Once done we get a VPC Successfully created message and the VPC is created in AWS.



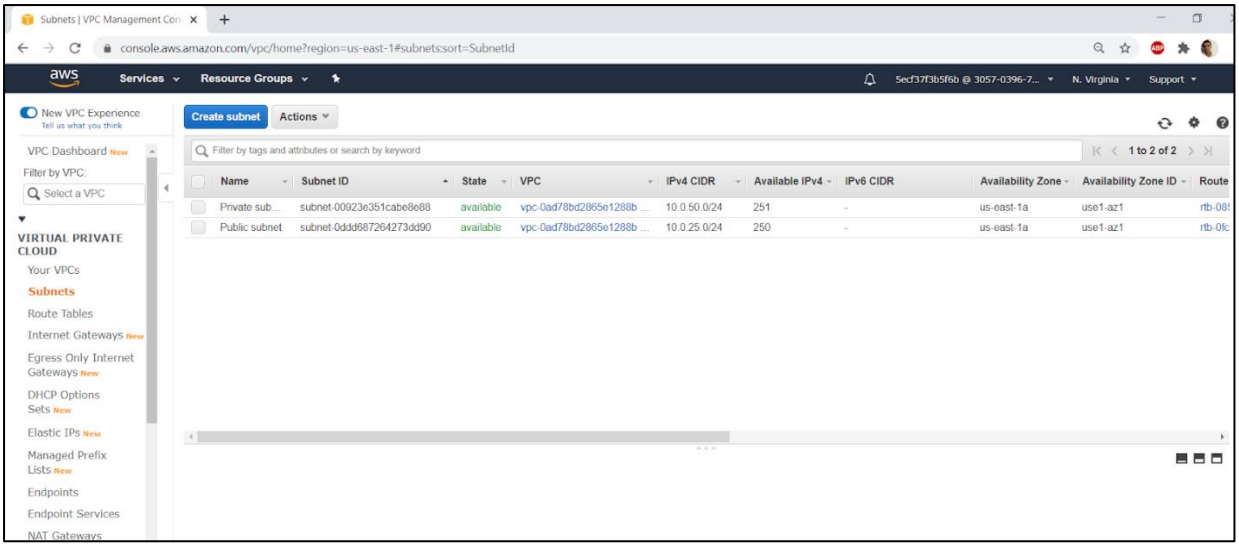
- We can verify that from the VPC Dashboard that lists the VPC details and has a VPC ID which we can note for future references.



Step 10: Select the VPC created and click on the **Internet Gateways** on the left navigation pane. We will see that an internet gateway is attached to the VPC which will allows the VPC to connect to the internet.



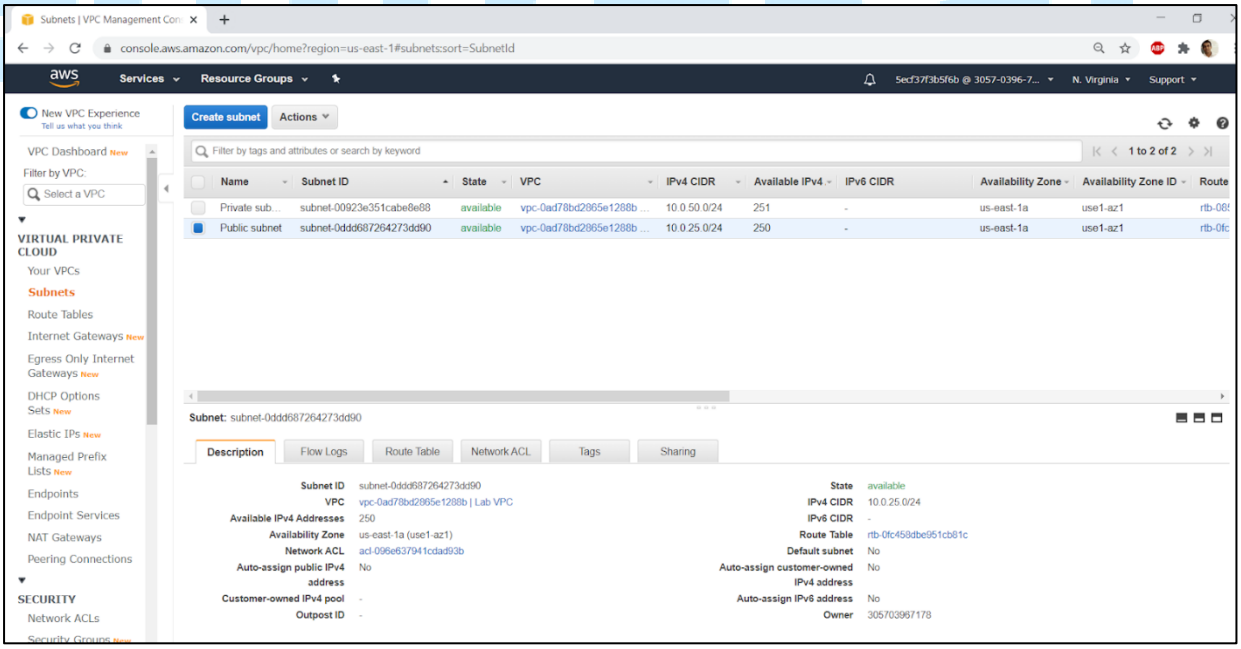
Step 11: Next , click on the **Subnets** on the left navigation pane.
We will notice that a Public Subnet and the Private Subnets are created for our VPC . It has a VPC ID which we can match with the VPC ID that we noted earlier for verification.



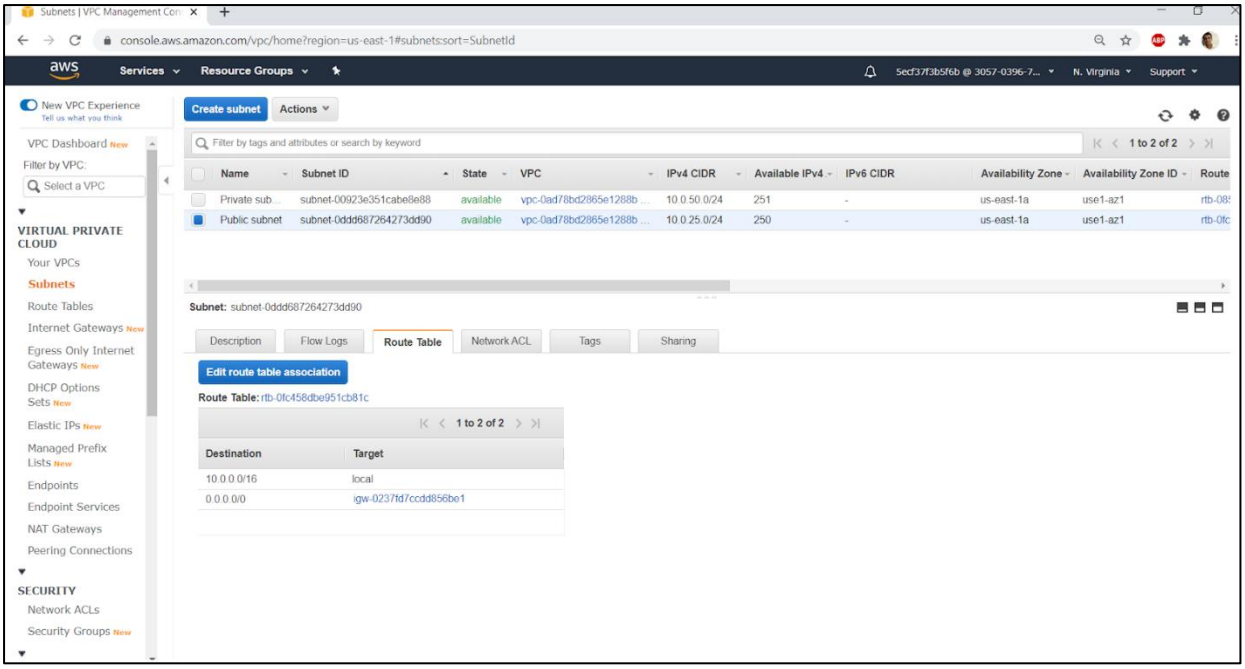
Step 12: We can now explore Public Subnet by selecting it and navigating through the below tabs.

The details include

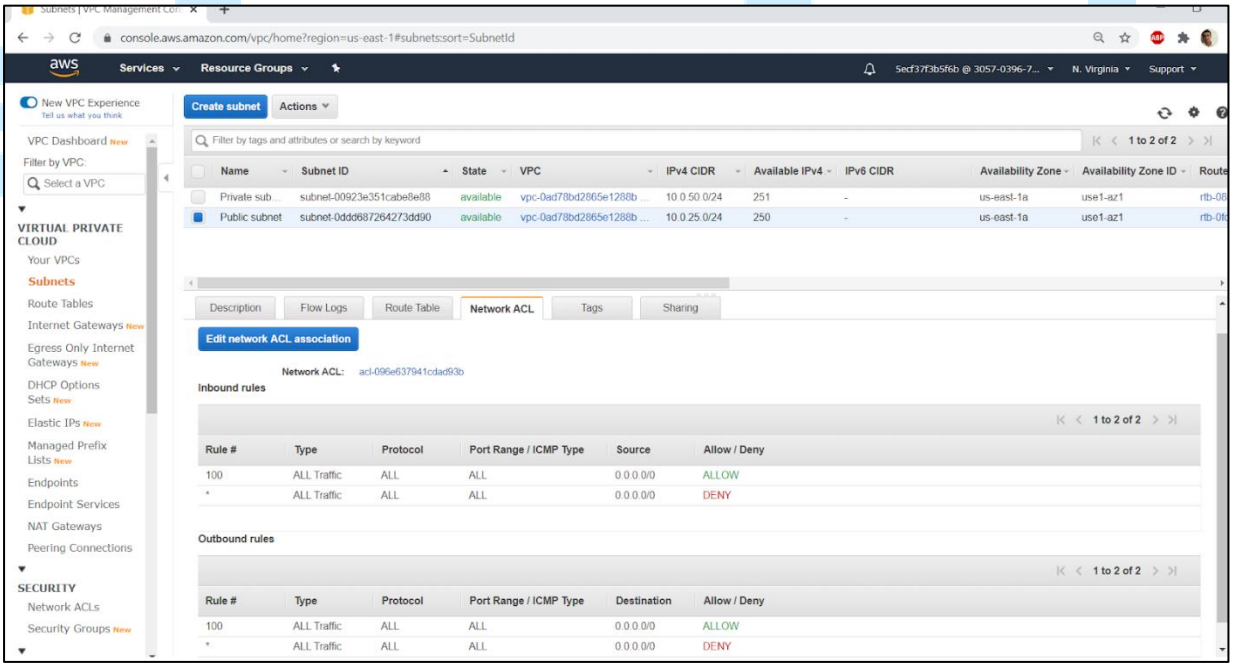
- **Description**
- **Flow Logs**
- **Route Table**
- **Network ACL**
- **Tags**



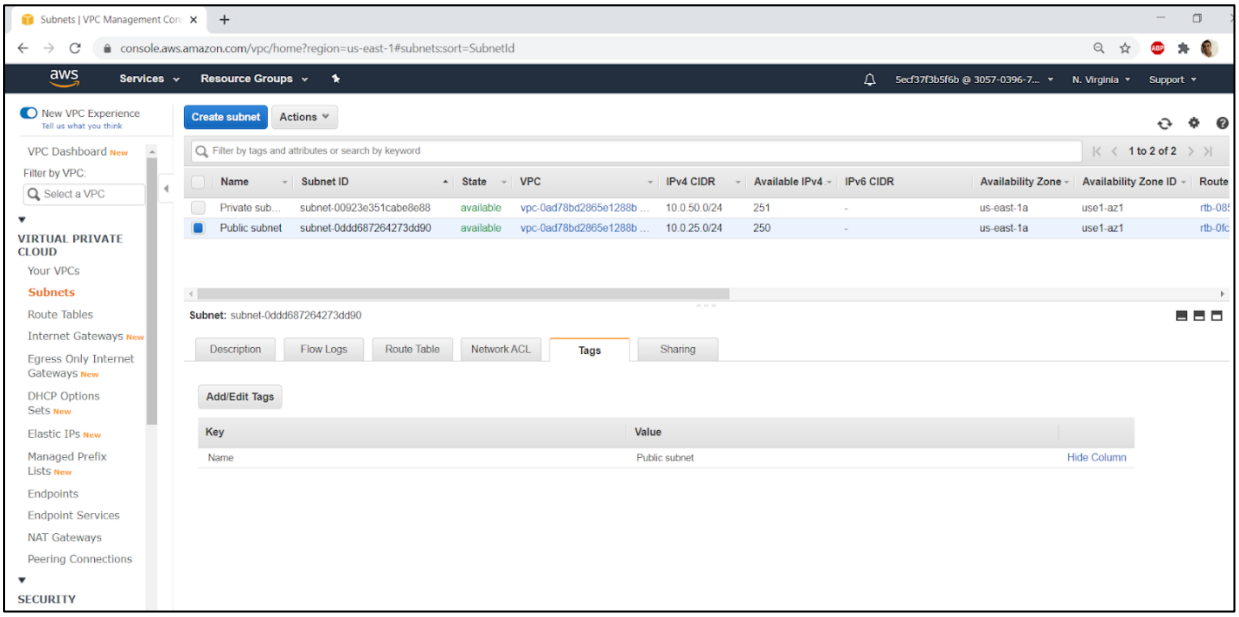
Step 13: On the Route table, we can see destination and find that an internet gateway is attached to the subnet.



Step 14: On the Network ACL, we can check the security layer that controls the traffic flowing in and out of the subnet.



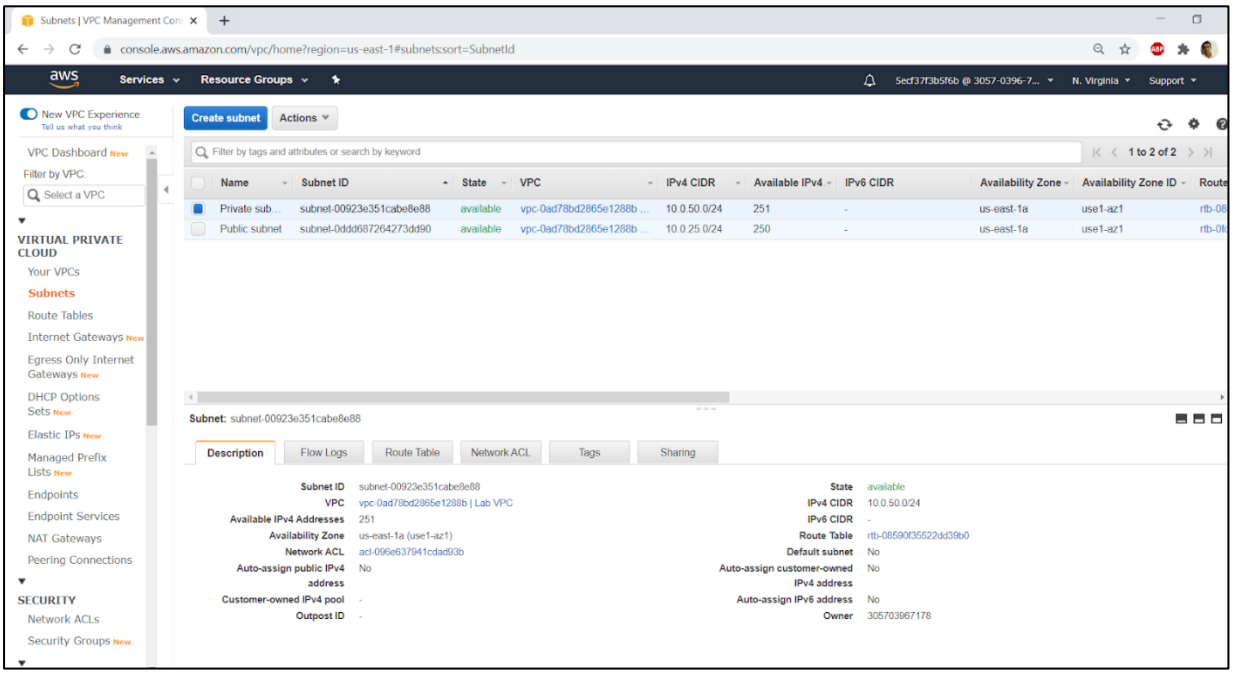
Step 15: On the Tags tab, we can check the tag name that we assign to the subnet.



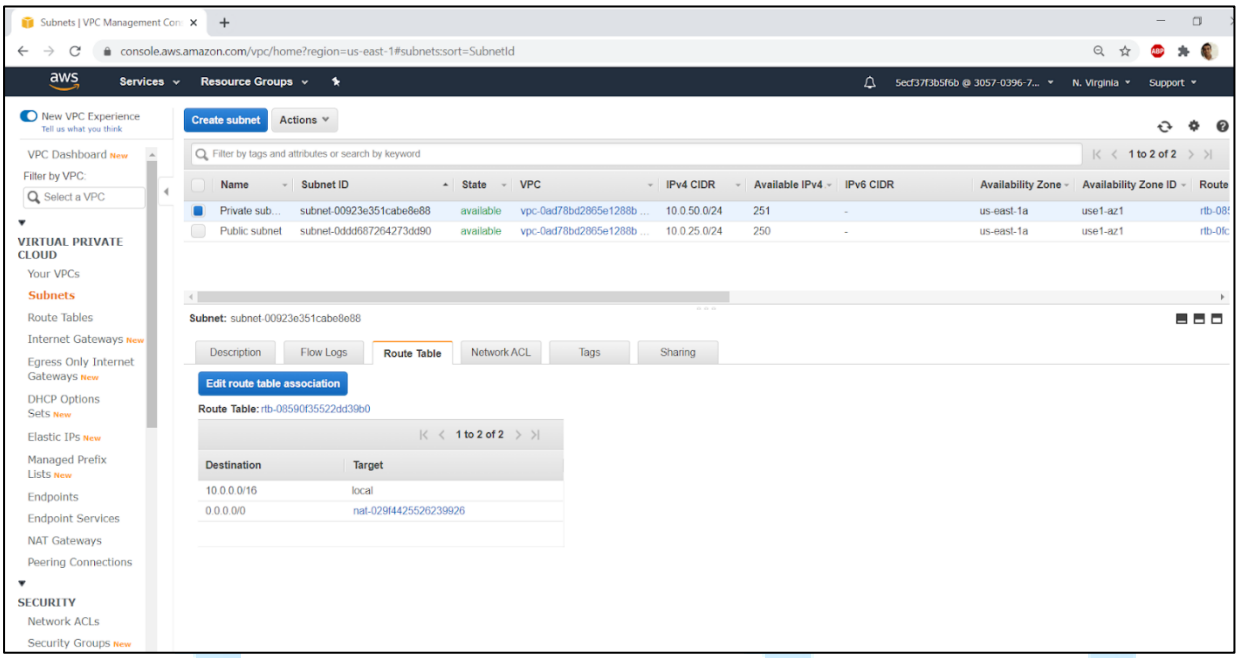
Step 16: We can now explore Private Subnet by selecting it and navigating through the below tabs.

The details include

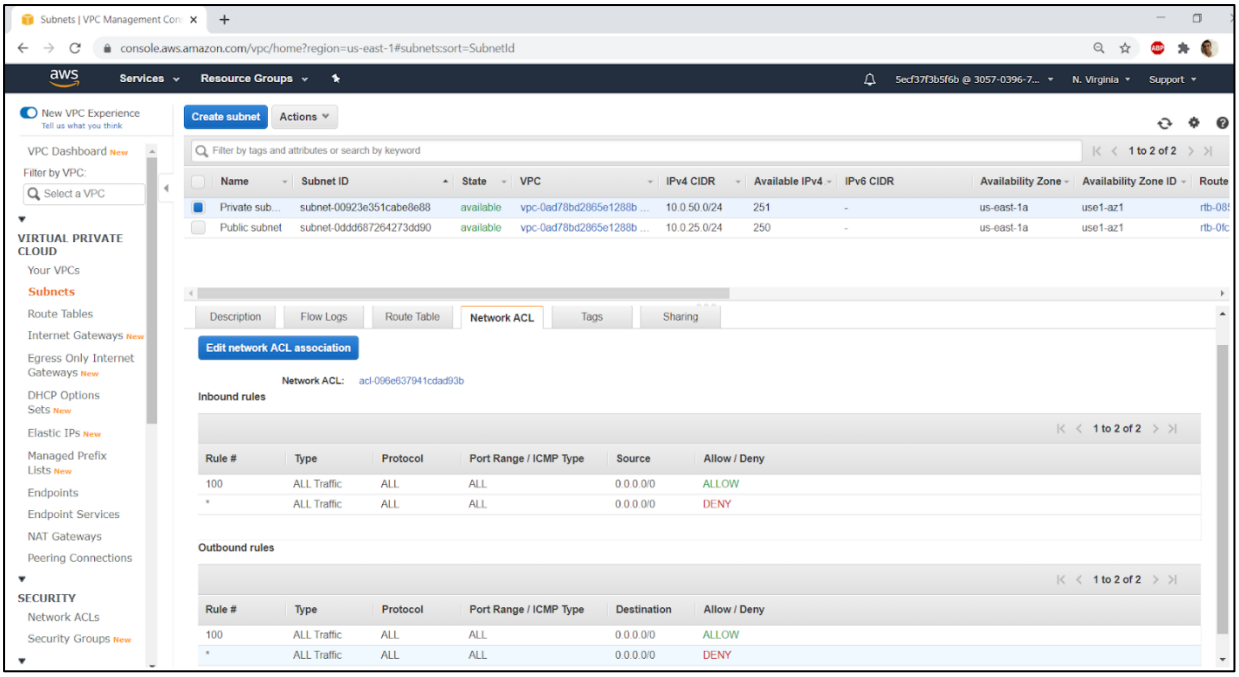
- **Description**
- **Flow Logs**
- **Route Table**
- **Network ACL**
- **Tags**



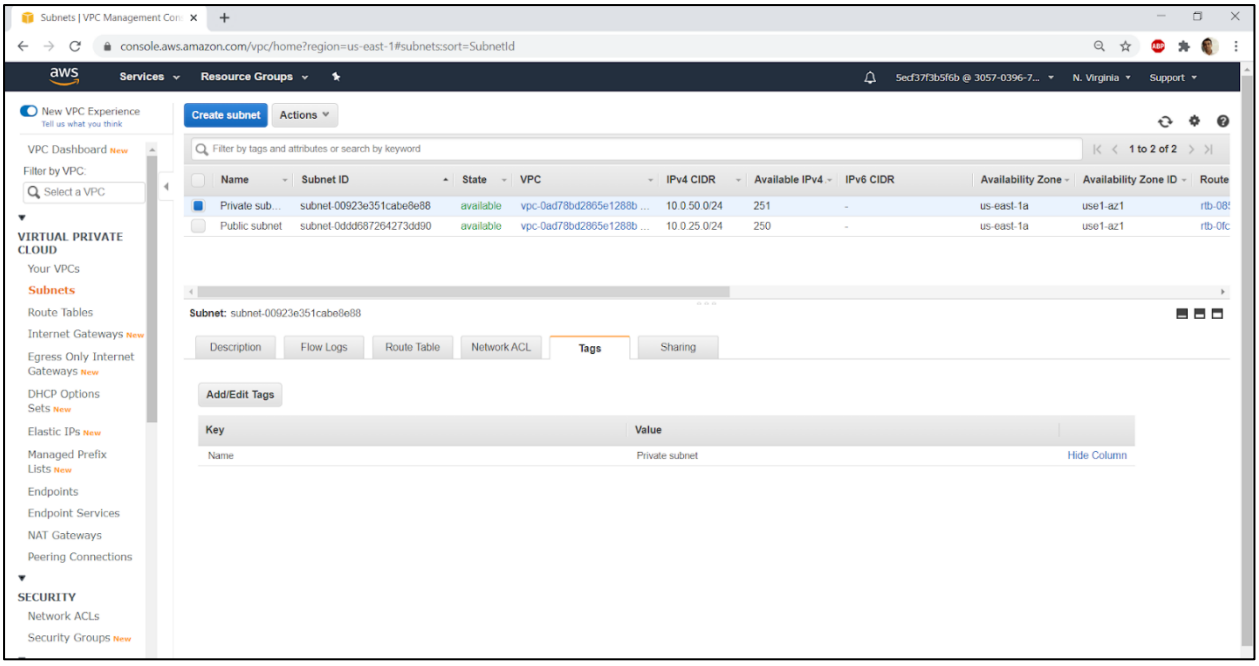
Step 17: On the Route table tab, we can find the route table entry and see destination and target attached with the same.



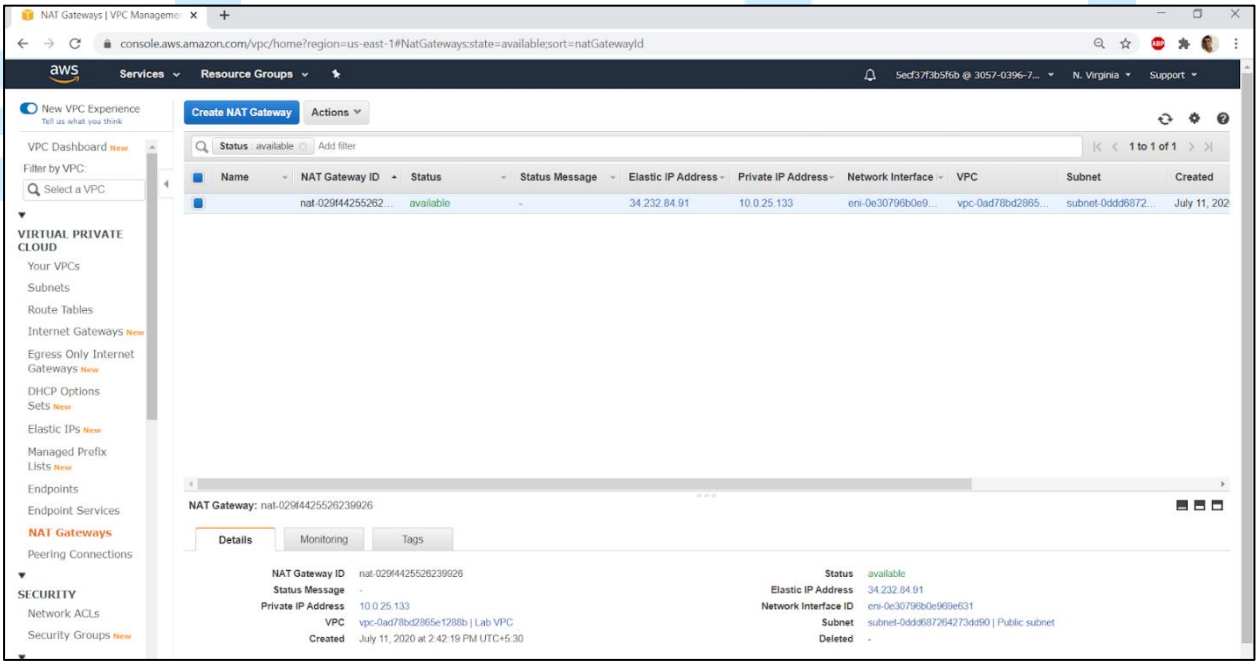
Step 18: On the Network ACL, we can check the security layer that controls the traffic flowing in and out of the subnet.



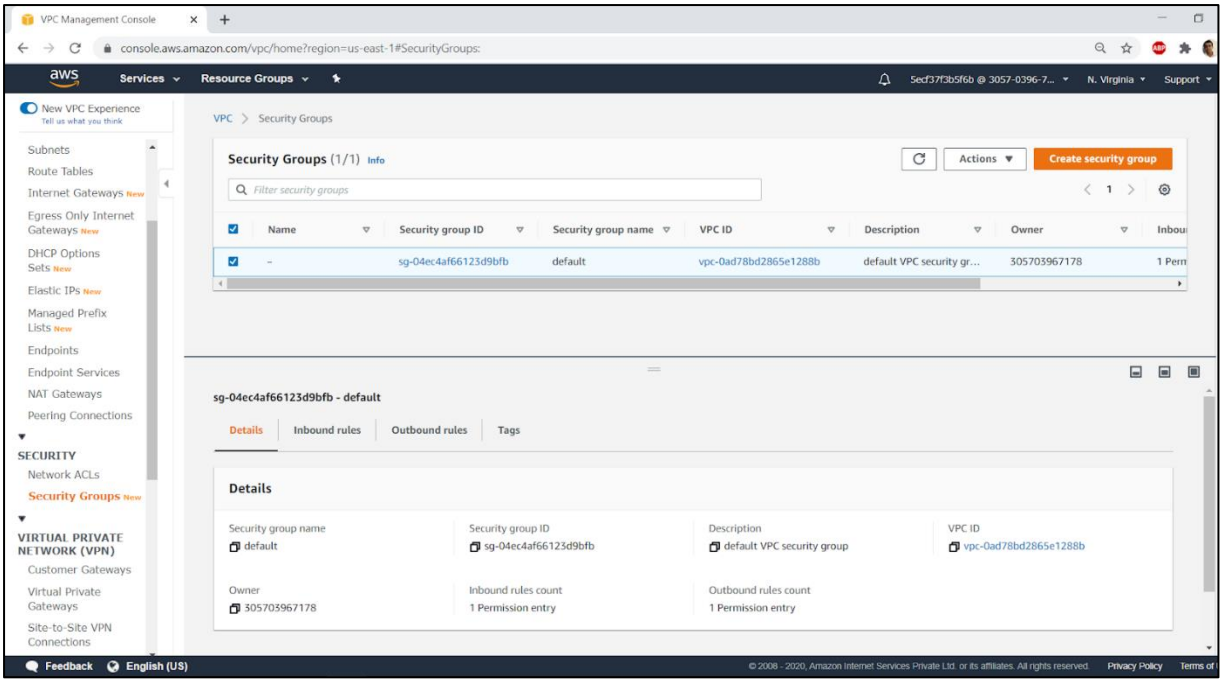
- On the Tags tab, we can check the tag name that we assign to the subnet.



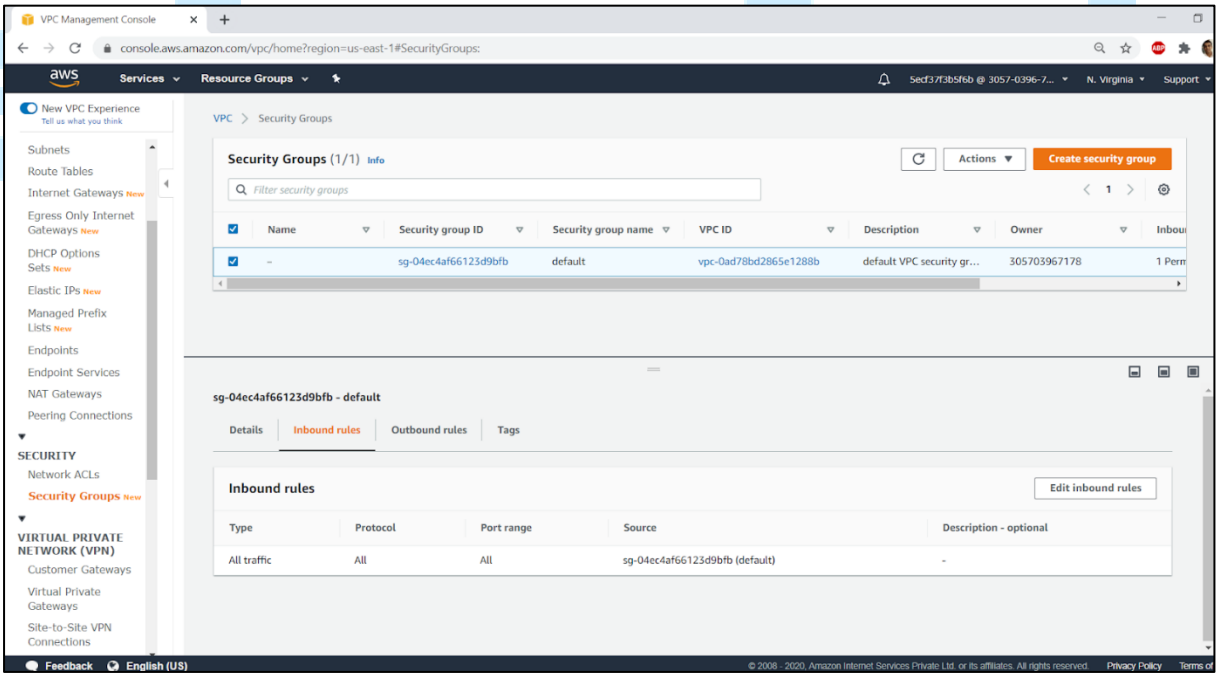
Step 19: Next , click on the **NAT Gateways** on the left navigation pane and check the status is available.It allows resources in the private subnet to connect to the internet.



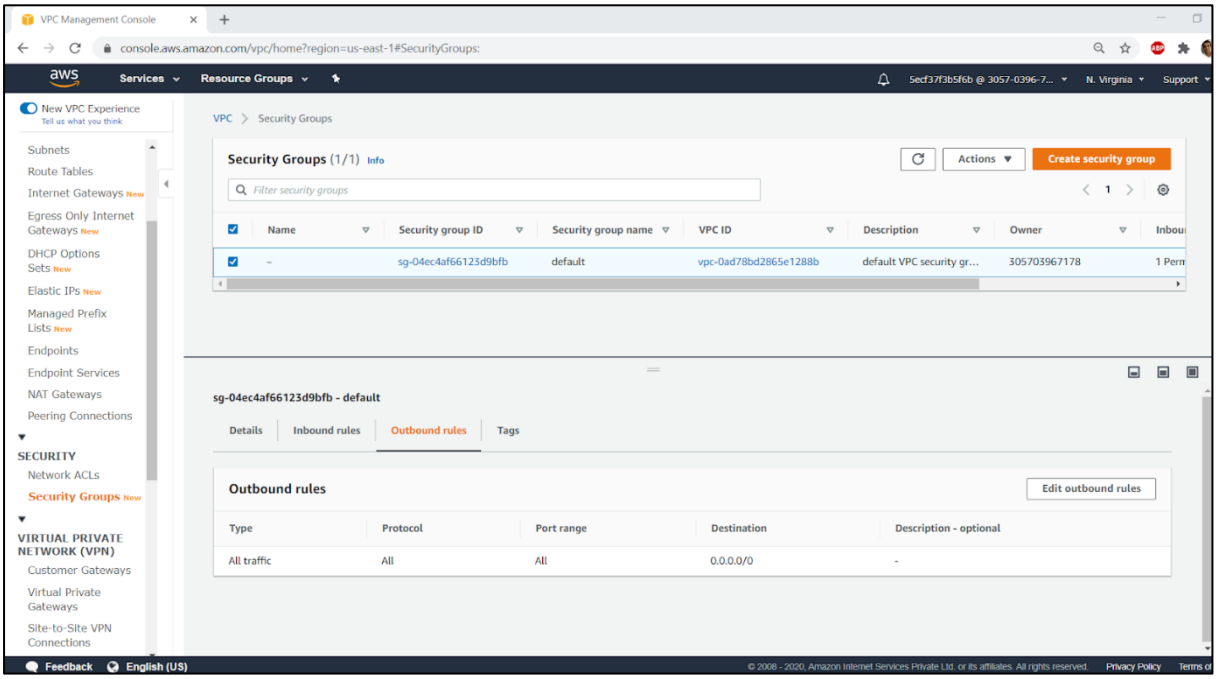
Step 20: Finally, we verify the security group , by clicking on the **Security Groups** in the left navigation pane. We can check the Security group ID and the associated VPC ID, it matches with the VPC created.



- Next we check the Inbound rules and Outbound rules in the below tabs to check the incoming and outgoing traffic to the provisioned resources.



- By default, the security group, permits all traffic to the resources, which can be edited as required from the edit option.



Evaluation Criteria:

Total Marks: – 100 Marks

Distribution:

• Create an Amazon VPC using the VPC wizard, and it should be displayed on the dashboard – 20 Marks

• Associate an Elastic IP address with it – 20 Marks

• Explore various resources of VPC such as Internet Gateway, NAT Gateway, Subnets, Security Groups – 10 Marks

• Launch a NAT Gateway so that internet access is provided to private resources – 10 Marks

• Introduce a Public subnet for resources facing the internet such as a web server and a Private subnet for resources at the back end such as database server – 10 Marks

• Define security groups with appropriate inbound rules – 10 Marks

• Ensure proper routes and corresponding Route tables entries specifying the traffic moving out of the subnet – 10 Marks

• Make use of Network ACLs for controlling inbound and outbound traffic in the VPC – 10 Marks