Lab 1: Setting up the Networking Layer in AWS

Task1: create your own vpc with following task

* Create vpc from scratch
* Create two vpc named prod-vpc and dev-vpc
* Each vpc should have 2 public subnet and 2 private subnets
* Create internet gateway, NAT gateway, Route table and define routes & define subnet association

### Theory:

#### Virtual Private Cloud (VPC):

A Virtual Private Cloud (VPC) is a private, isolated section of a public cloud. It allows organizations to use cloud resources securely while being completely separated from other users.

* Purpose: VPCs help organizations securely host applications, databases, and other resources in the cloud.
* Key Feature: Network segmentation. This divides the network into smaller parts (subnets) for better organization and security.

#### Subnets (Public and Private):

Subnets are smaller sections of a VPC, created to group resources based on their purpose and security needs.

* Public Subnet: A public subnet is directly accessible to the Internet. Resources placed here, like web servers, can be accessed by users worldwide. These subnets must connect to an Internet Gateway to enable Internet access.
* Private Subnet: A private subnet is isolated and cannot be accessed directly from the Internet. Resources like databases are placed here. To access the Internet, private subnets use a NAT Gateway for outbound-only traffic.

#### Routing Table:

A routing table is a set of rules that guides network traffic in a VPC. It tells data packets where to go next, whether it’s another subnet, an Internet Gateway, or a NAT Gateway.

* Purpose: Routing tables ensure that each subnet knows how to send and receive traffic properly.

#### Internet Gateway:

An Internet Gateway is like the main gate of your VPC that connects your network to the Internet.

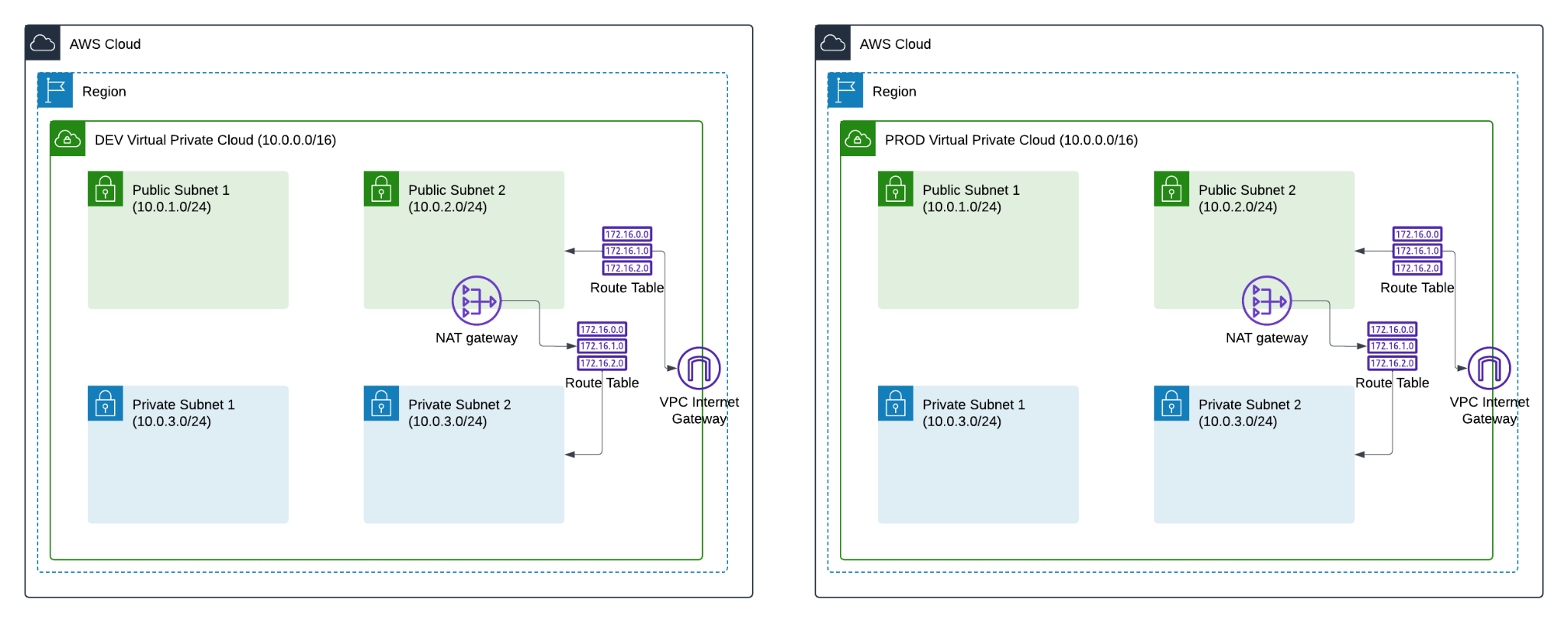
* Purpose: It allows public resources, like web servers in public subnets, to communicate with the Internet.
* Features:
  + Handles two-way traffic (inbound and outbound).
  + Only works with public subnets.

#### NAT Gateway:

A NAT (Network Address Translation) Gateway is used to enable Internet access for private subnets while keeping them hidden from external users.

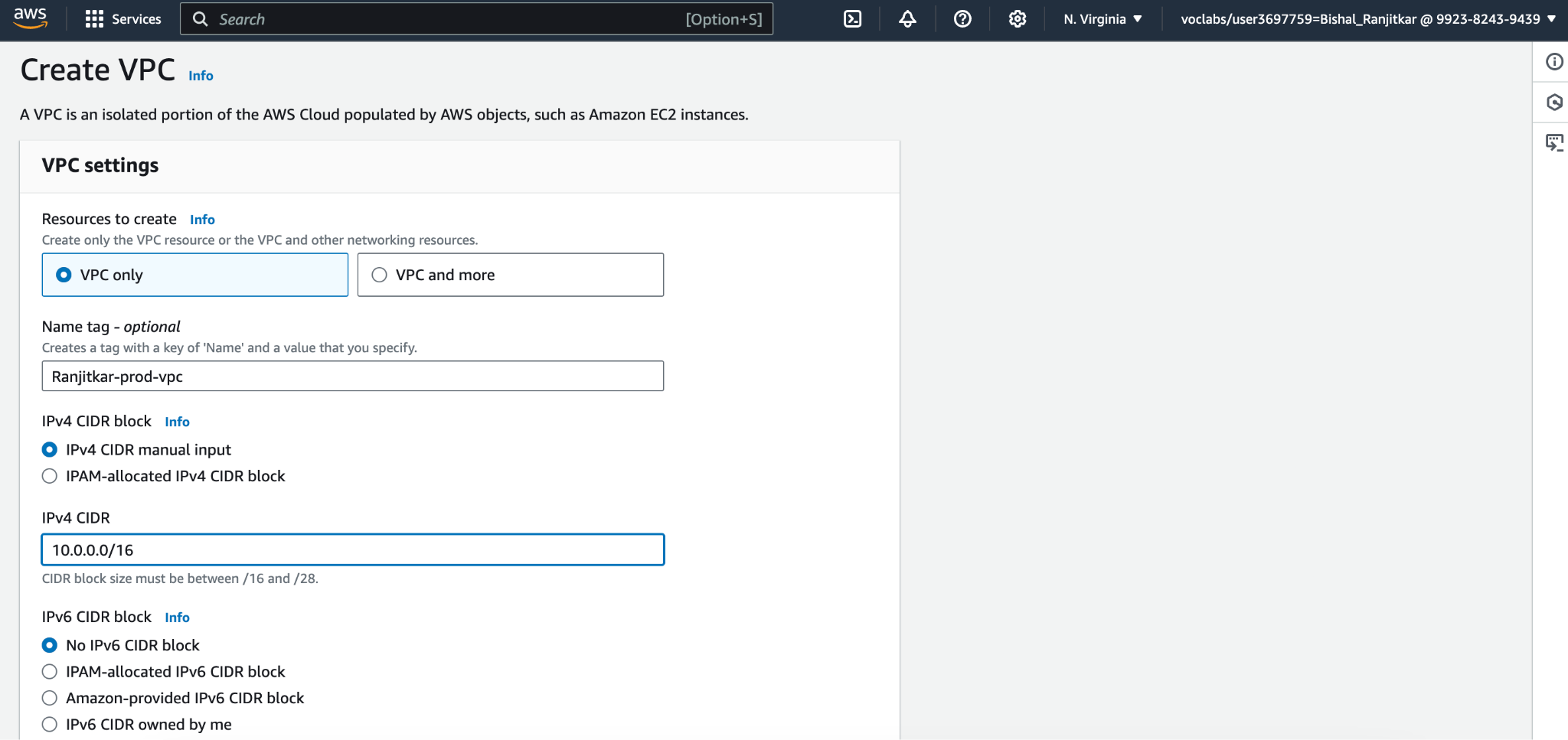
* Purpose: It allows resources in private subnets to download updates or access the Internet without exposing them to external users.
* How it Works:
  + Outbound traffic is translated and sent to the Internet.
  + Inbound traffic is blocked to maintain security.

Architecture design for Production VPC and DEV VPC:

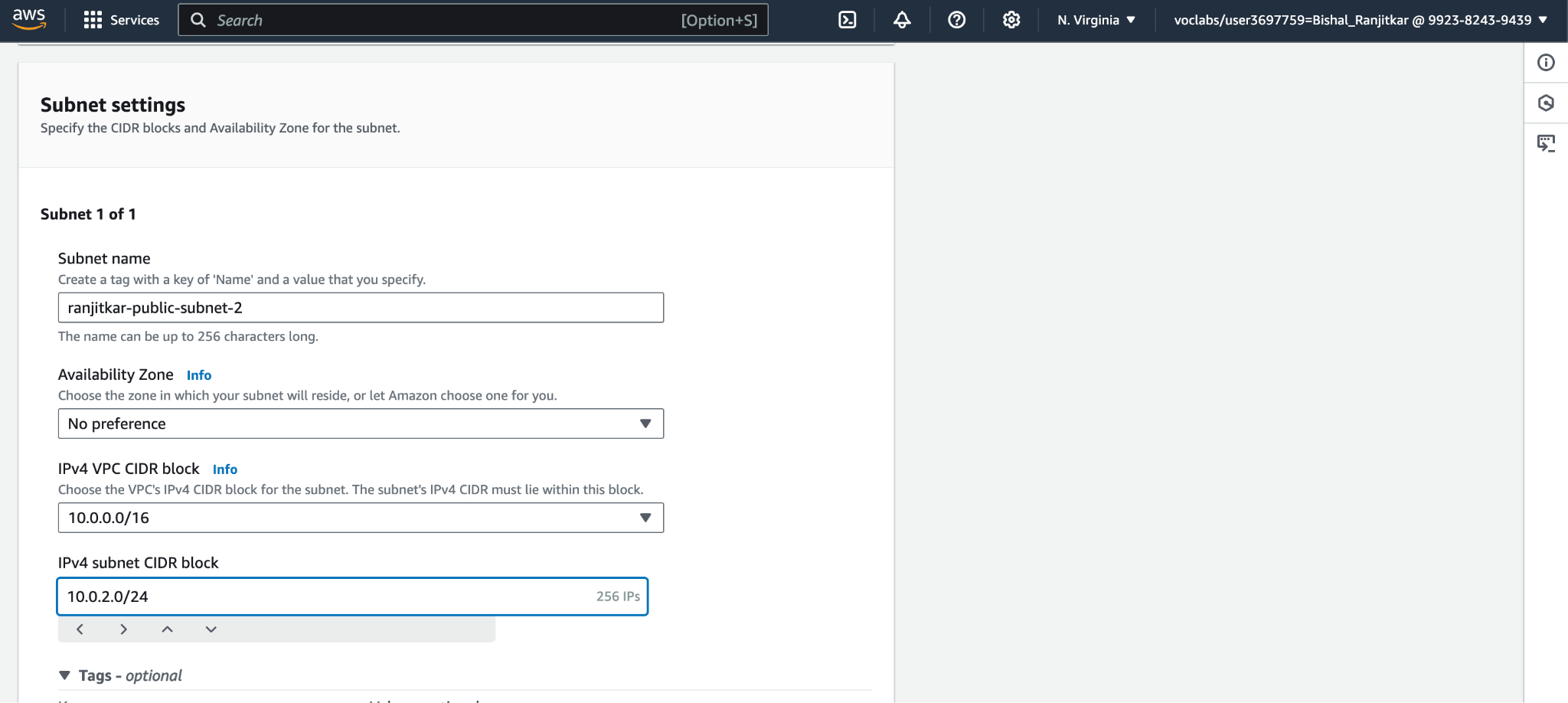


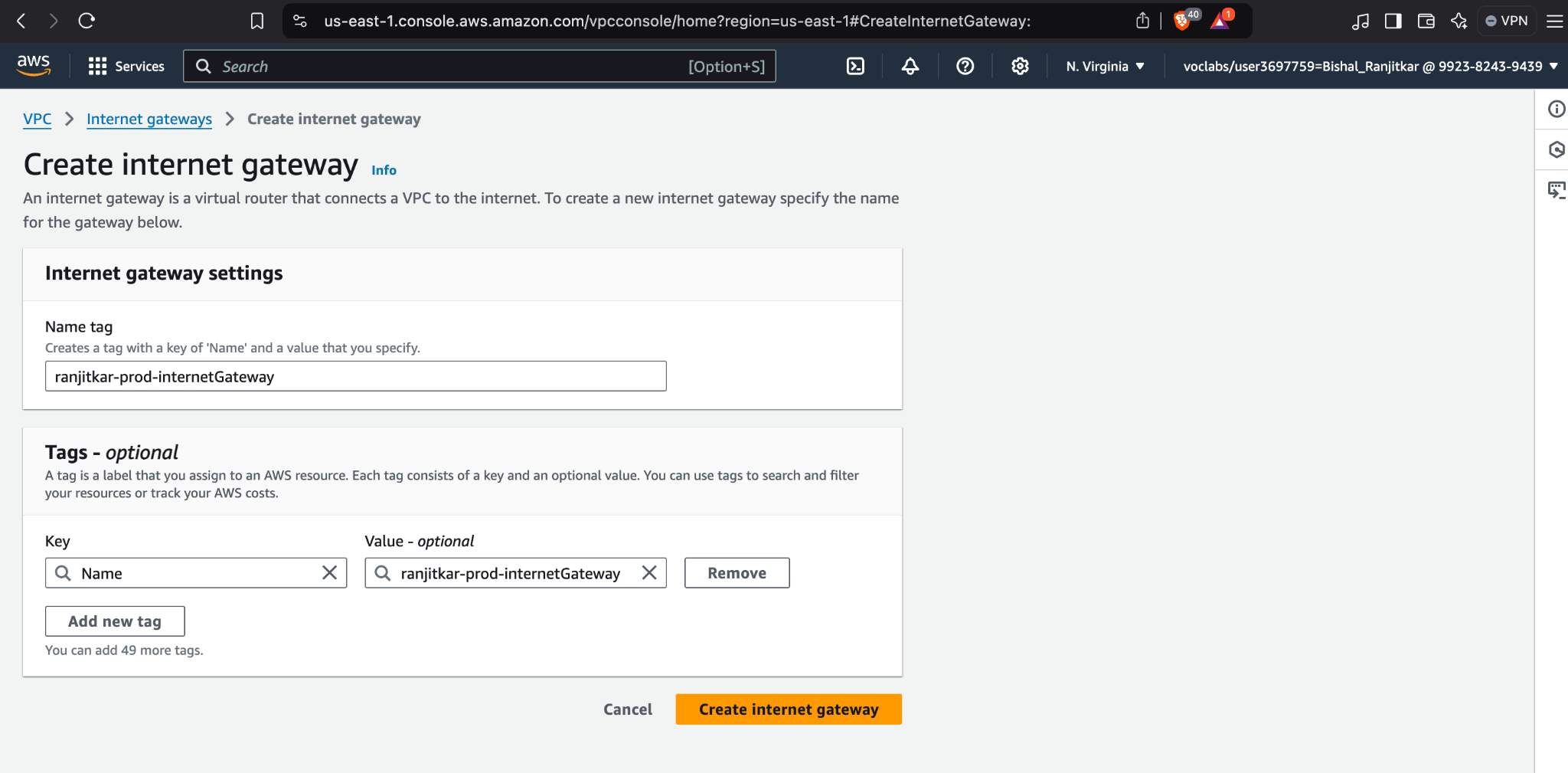
Steps for production vpc :

1. Login into AWS and go to VPC. click on your VPC and create VPC. insert name of VPC (Ranjitkar-prod-vpc) and CIRD(10.0.0.0/16)

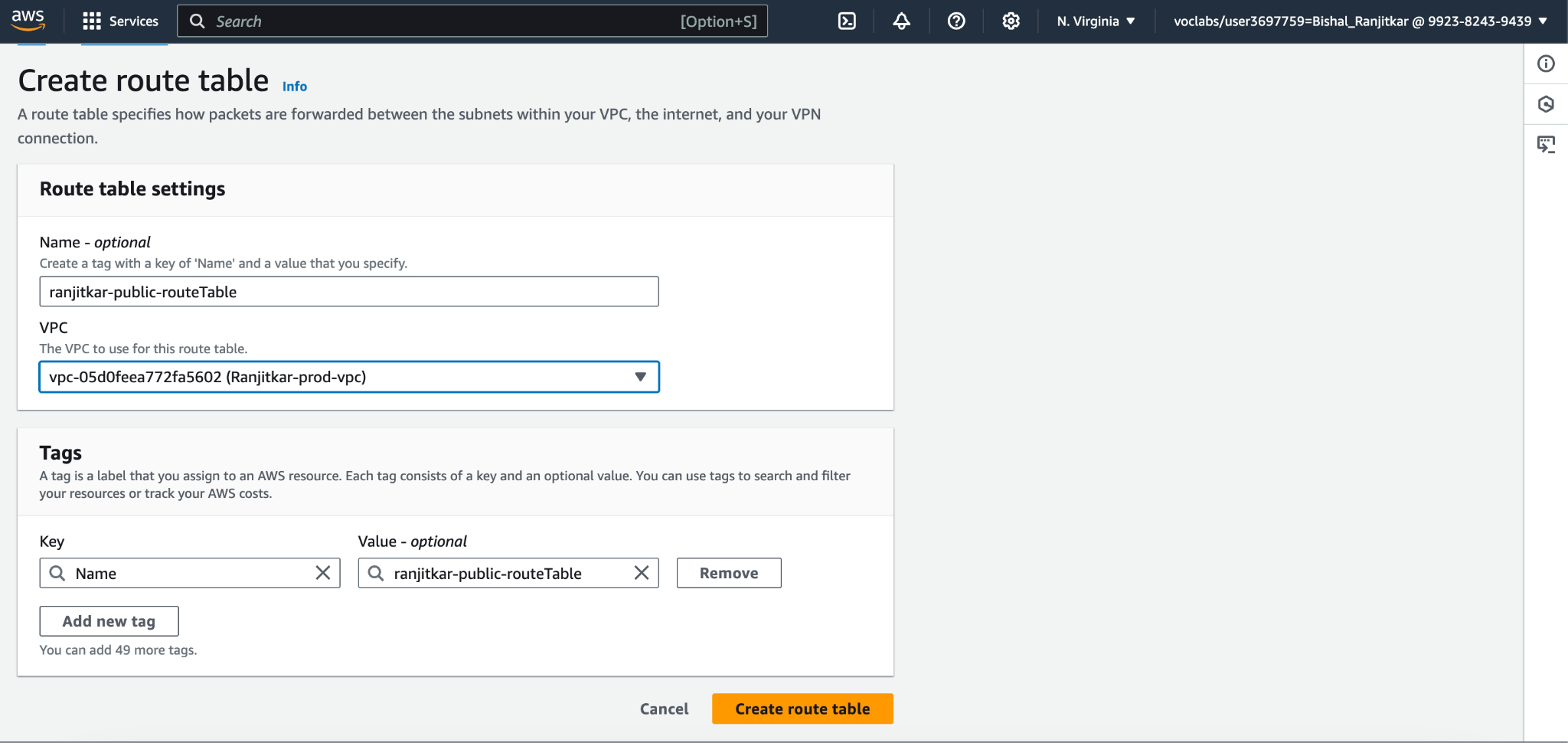


Step 2: create two public subnet(ranjitkar-public-subnet-1, ranjitkar-public-subnet-2) and two private subnet (ranjitkar-private-subnet-1,ranjitkar-private-subnet-2 ). Insert details like name of subnet and CIDR(10.0.1.0/24, 10.0.2.0/24, 10.0.3.0/24, 10.0.4.0/24)

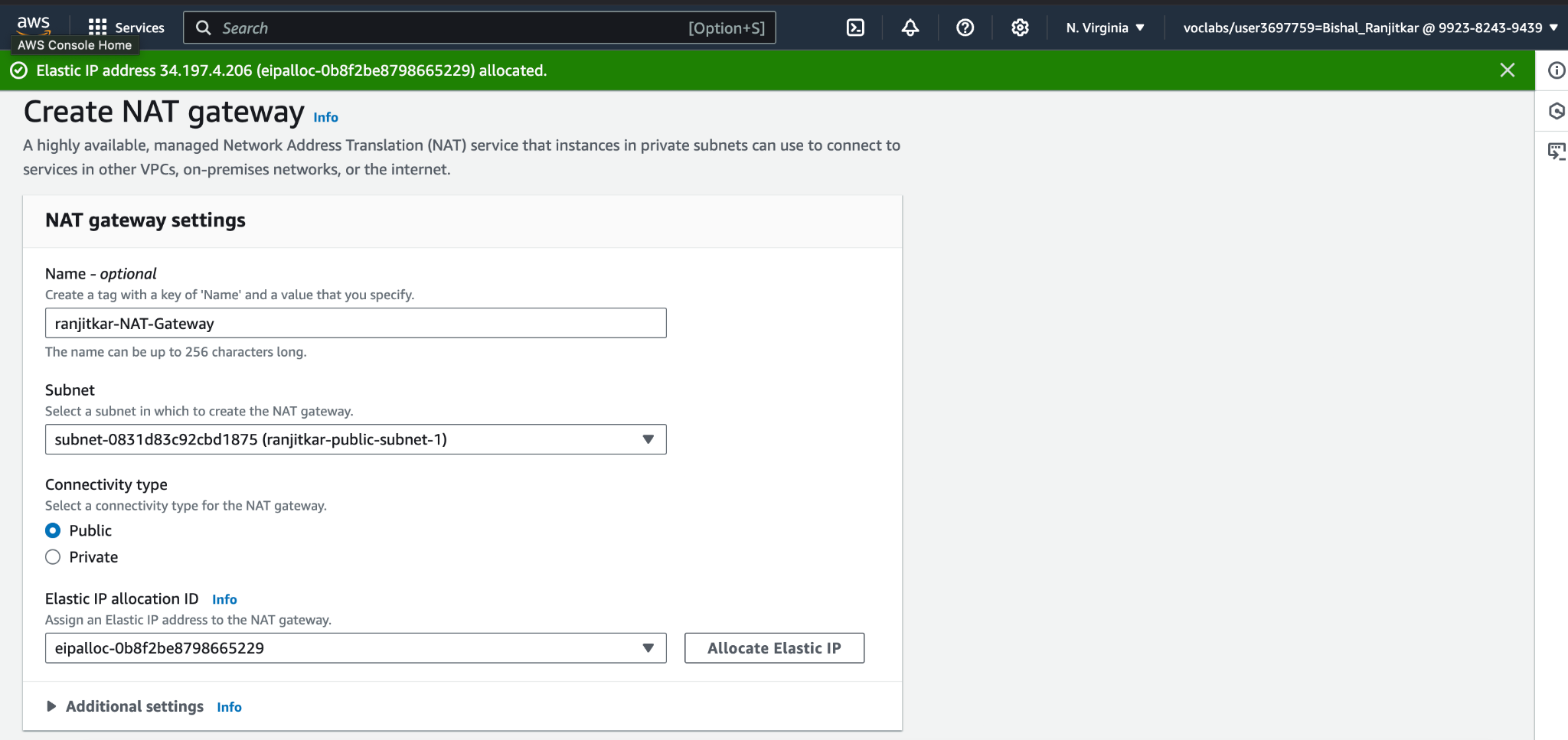


Step 3: create internet gateway (ranjitkar-prod-internetGateway)and attach it to VPC(ranjitkar-prod-vpc)

Step 4: create route table for public subnet. For public subnet create route table insert name (ranjitkar-public-routeTable) and vpc. Then go to edit routes, click add route and insert ip address(0.0.0.0/0) and internet gateway.then go to edit subnet associations and check ranjitkar-public-subnet-1 and ranjitkar-public-subnet-2

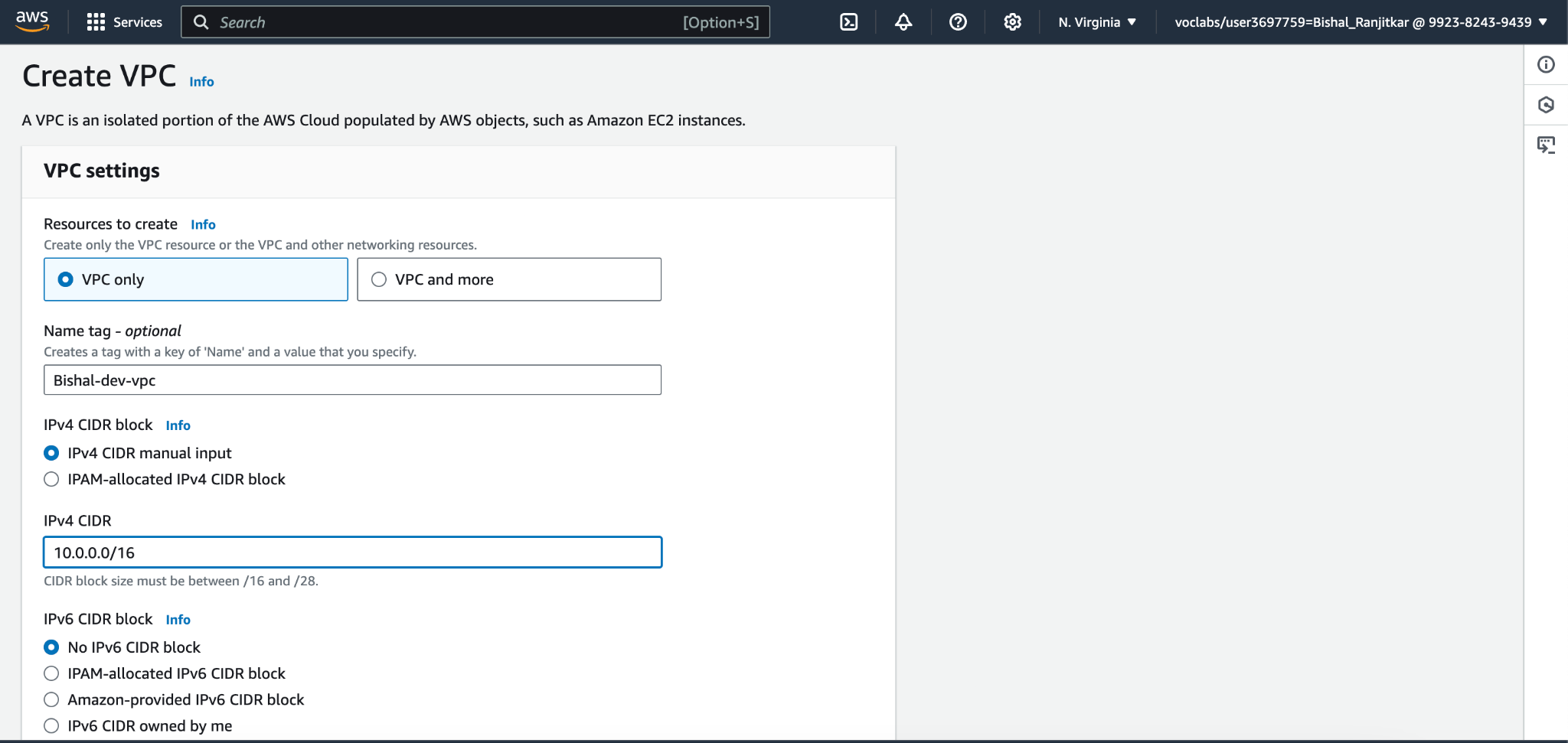


Step5: create NAT gateway (ranjitkar-NAT-Gateway).insert name,subnet and click allocate elastic IP.go to route table check ranjitkar-private-routeTable edit routes insert CIDR (0.0.0.0/0) and nat gateway.

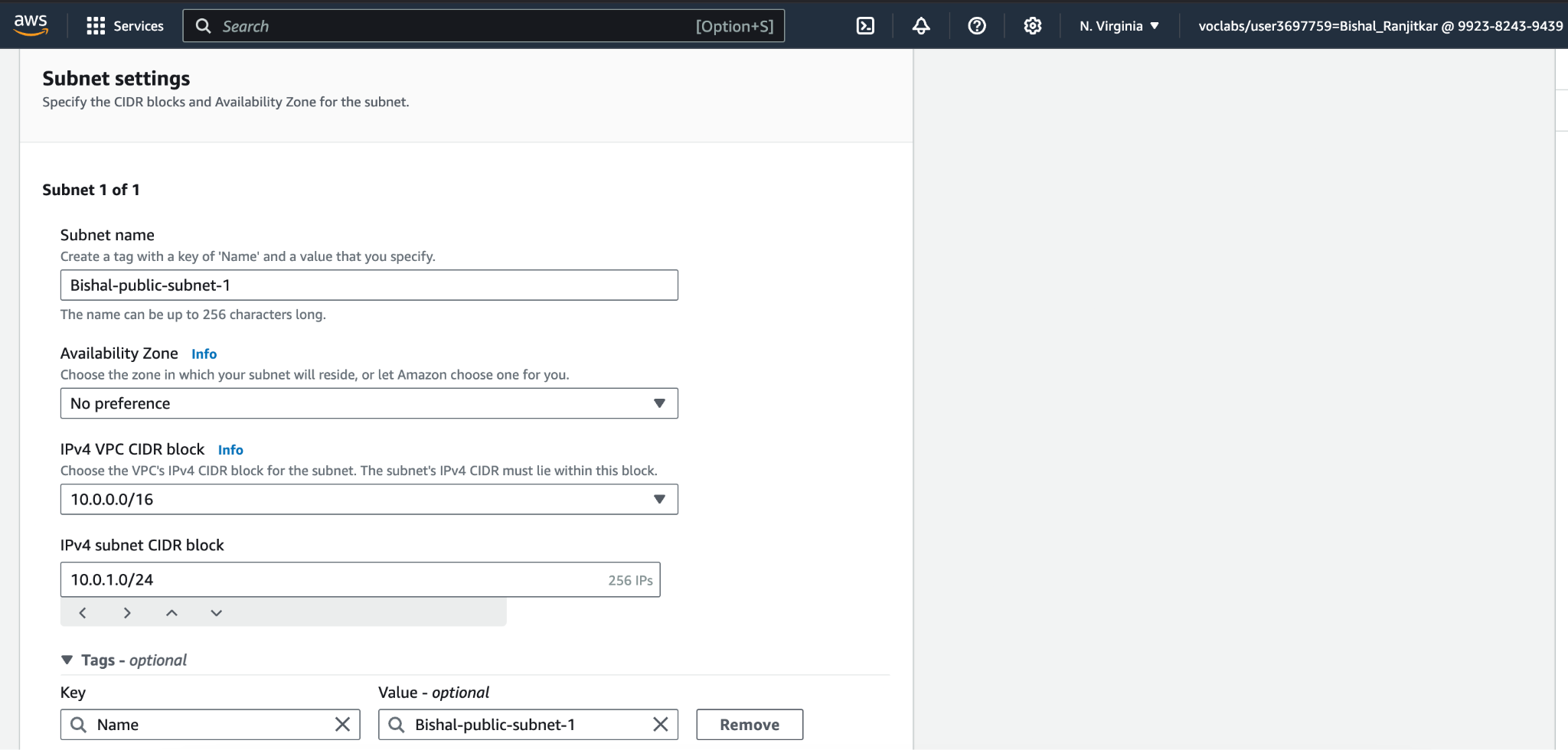


Steps for developer vpc :

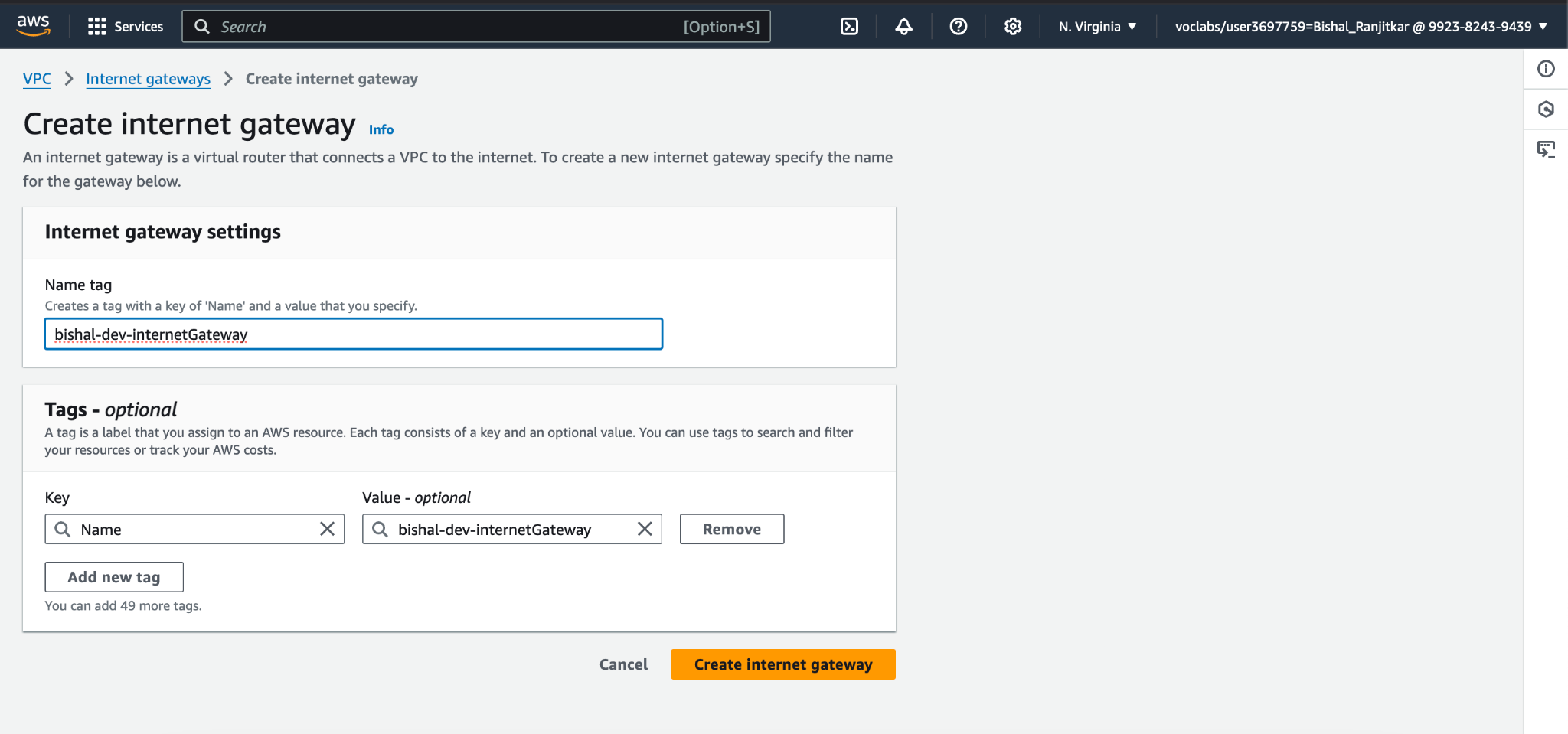
1. Login into AWS and go to VPC. click on your VPC and create VPC. insert name of VPC (Bishal-dev-vpc) and CIRD(10.0.0.0/16)



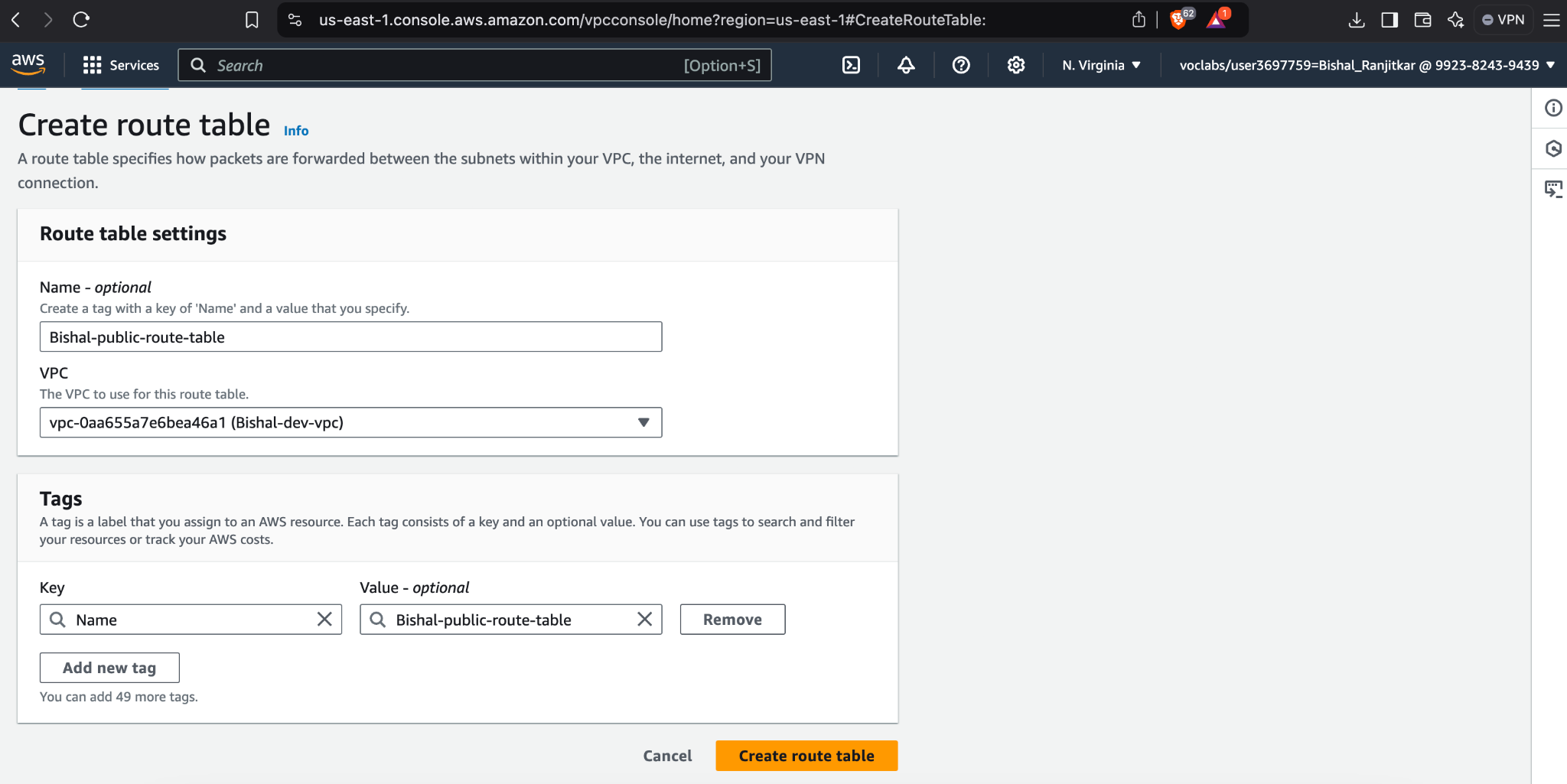
Step 2: create two public subnet(Bishal-public-subnet-1, Bishal-public-subnet-2) and two private subnet (Bishal-private-subnet-1,Bishalr-private-subnet-2 ). Insert details like name of subnet and CIDR(10.0.1.0/24, 10.0.2.0/24, 10.0.3.0/24, 10.0.4.0/24)



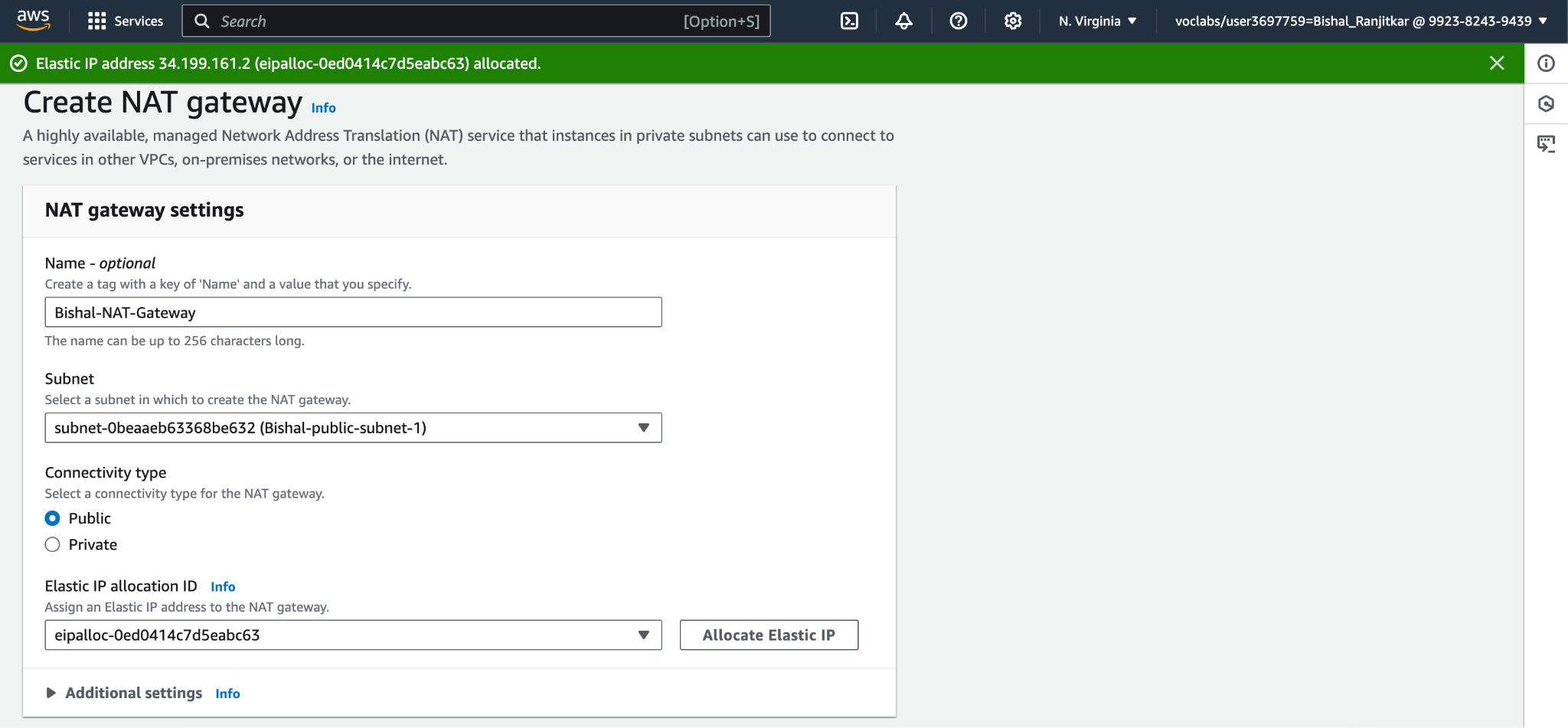
Step 3: create internet gateway (Bishal-dev-internetGateway)and attach it to VPC(Bishal-dev-vpc)



Step 4: create route table for public subnet. For public subnet create route table insert name (bishal-public-routeTable) and vpc. Then go to edit routes, click add route and insert ip address(0.0.0.0/0) and internet gateway.then go to edit subnet associations and check bishal-public-subnet-1 and bishal-public-subnet-2



Step5: create NAT gateway (bishal-NAT-Gateway).insert name,subnet and click allocate elastic IP.go to route table, check bishal-private-routetable and click edit routes insert CIDR (0.0.0.0/0) and nat gateway.



### **Conclusion**

We created two VPCs named prod-vpc and dev-vpc. Each VPC has 2 public subnets and 2 private subnets.

We set up:

1. Internet Gateway for internet access in public subnets.
2. NAT Gateway for private subnets to access the internet securely.
3. Route Tables to manage traffic and linked them to the right subnets.
4. Network ACLs (NACLs) to control inbound and outbound traffic for better security.

This setup is secure, organized, and ready for production and development use.