Lesson 08 Demo 01

Deploying and Managing a VPC with Public and Private Subnets in AWS

Objective: To deploy and manage a resilient VPC with public and private subnets across multiple availability zones in AWS, ensuring proper routing and connectivity for failover and disaster recovery testing

Tools required: AWS Account

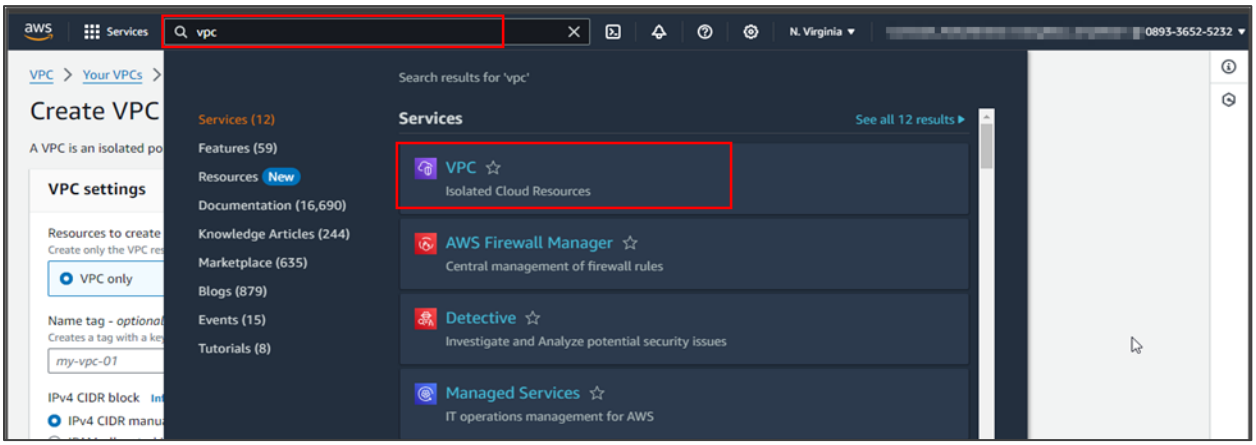
Prerequisites: None

Steps to be followed:

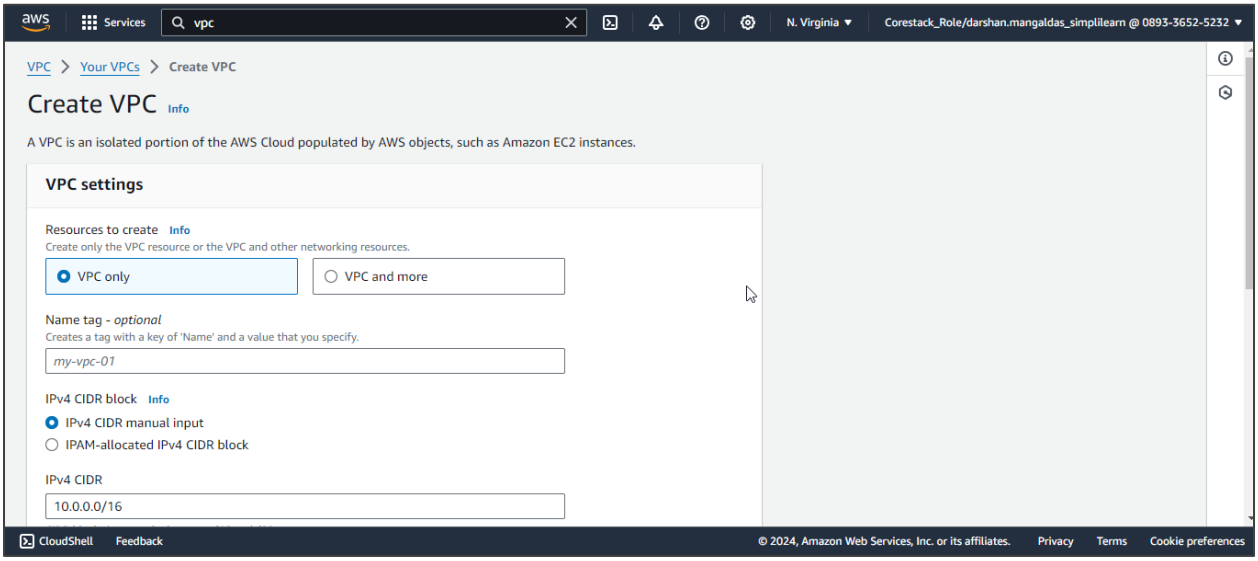
1. Create a new VPC in the US-East-1 region
2. Create public and private subnets in three different availability zones
3. Deploy an internet gateway and attach it to the VPC
4. Provision a NAT Gateway for outbound connectivity
5. Configure the route tables to route traffic
6. Delete the VPC

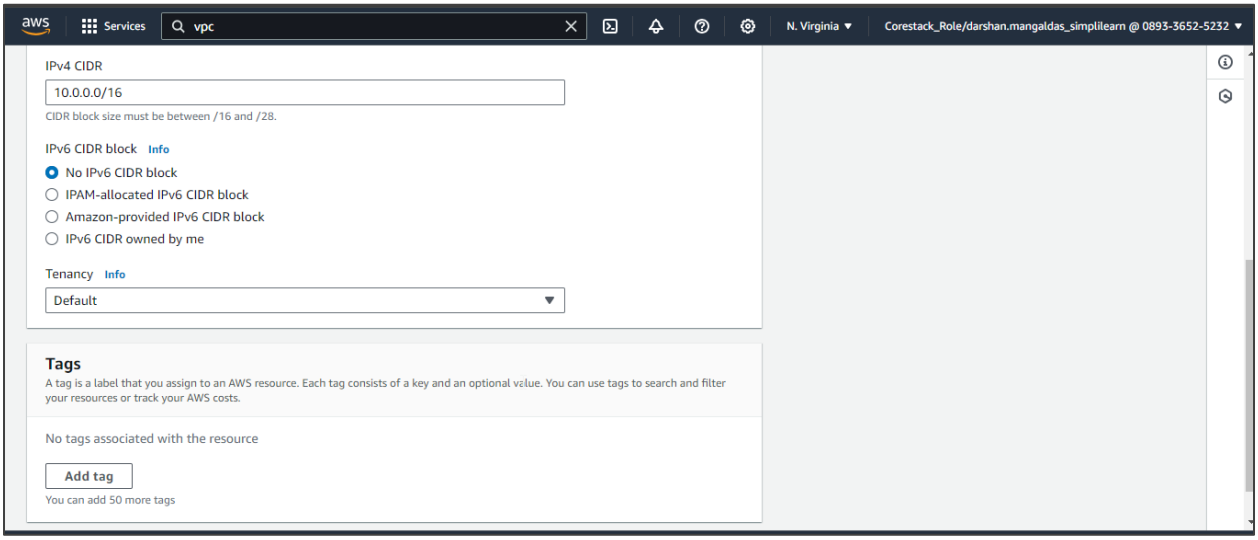
Step 1: Create a new VPC in the US-East-1 region

1.1 Log into the AWS console, enter **vpc** in the search field, and select the **VPC** service

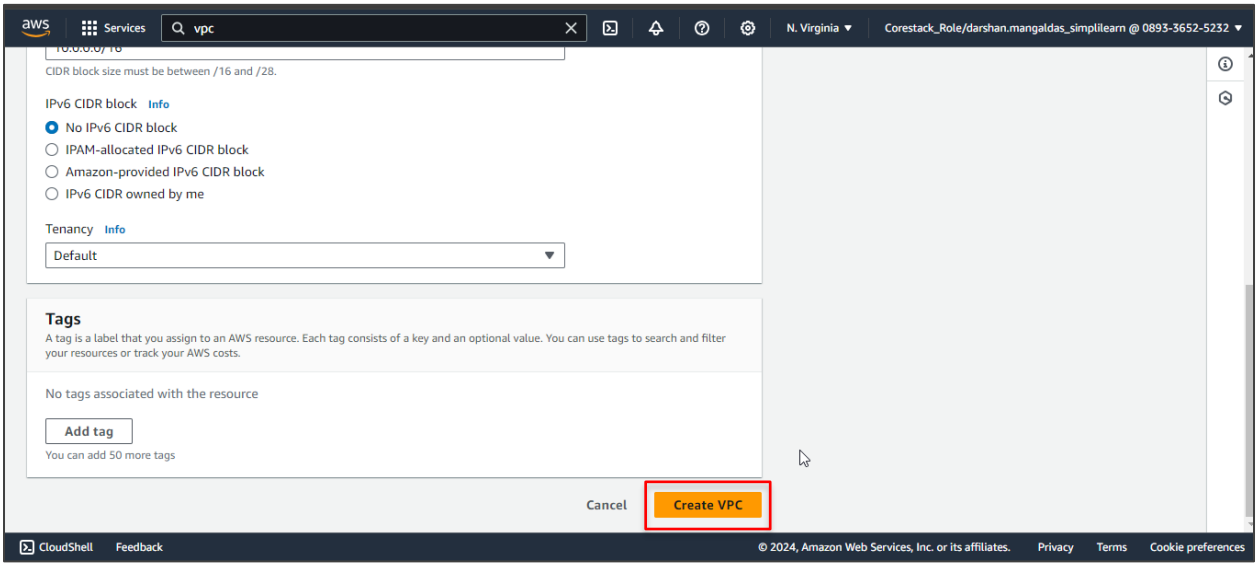


1.2 In the **Create VPC** page, select the **VPC only** option, enter the **Name tag** as **demo-vpc,** and set the IPv4 CIDR block to **IPv4 CIDR manual input** and IPv4 CIDS to **10.0.0.0/16**

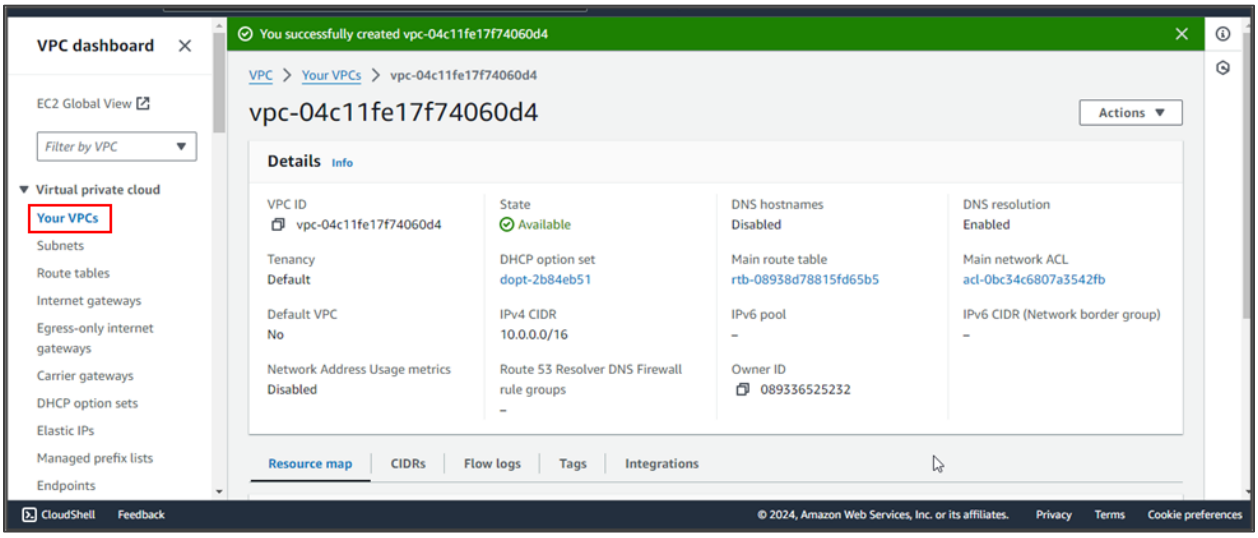


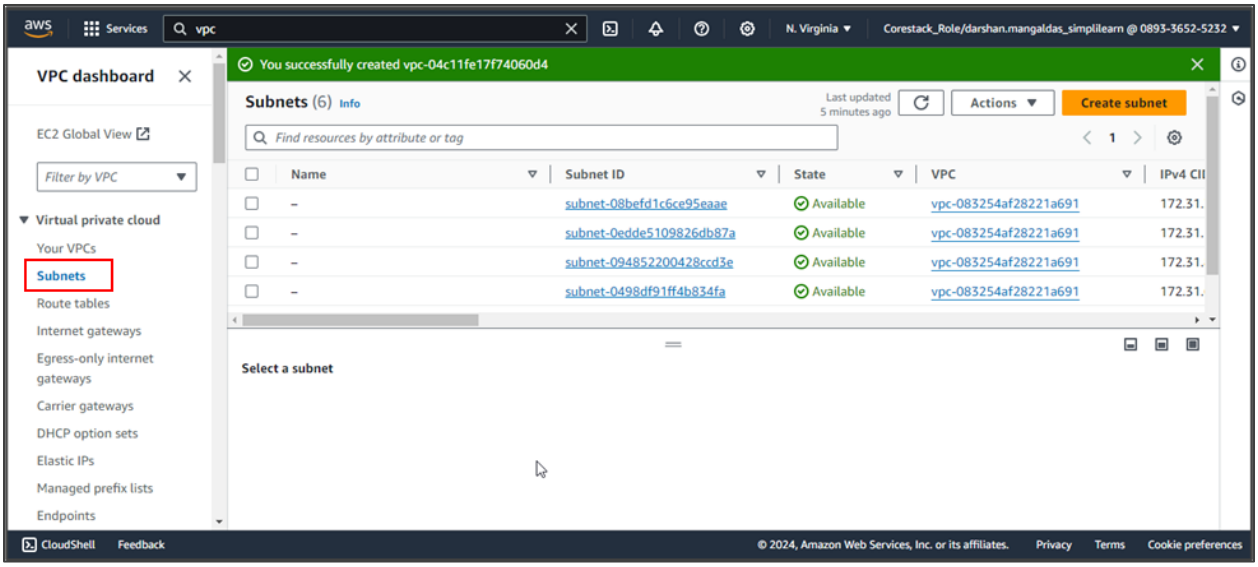


1.3 Select **Create VPC** and leave all the other settings as default



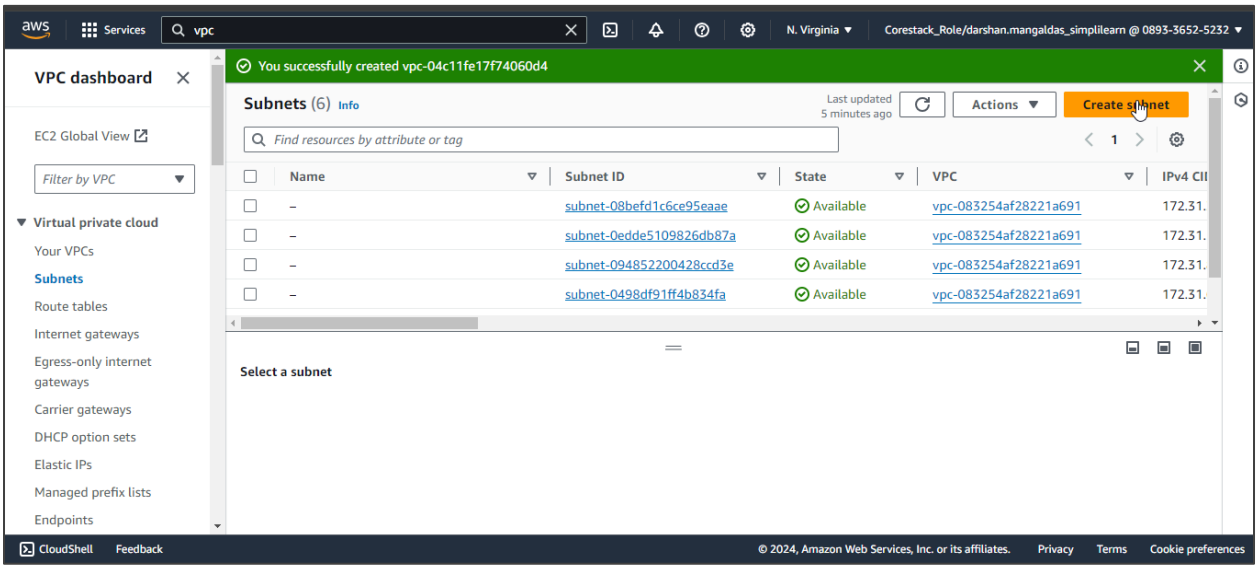
The VPC and subnet will be created successfully as shown below:



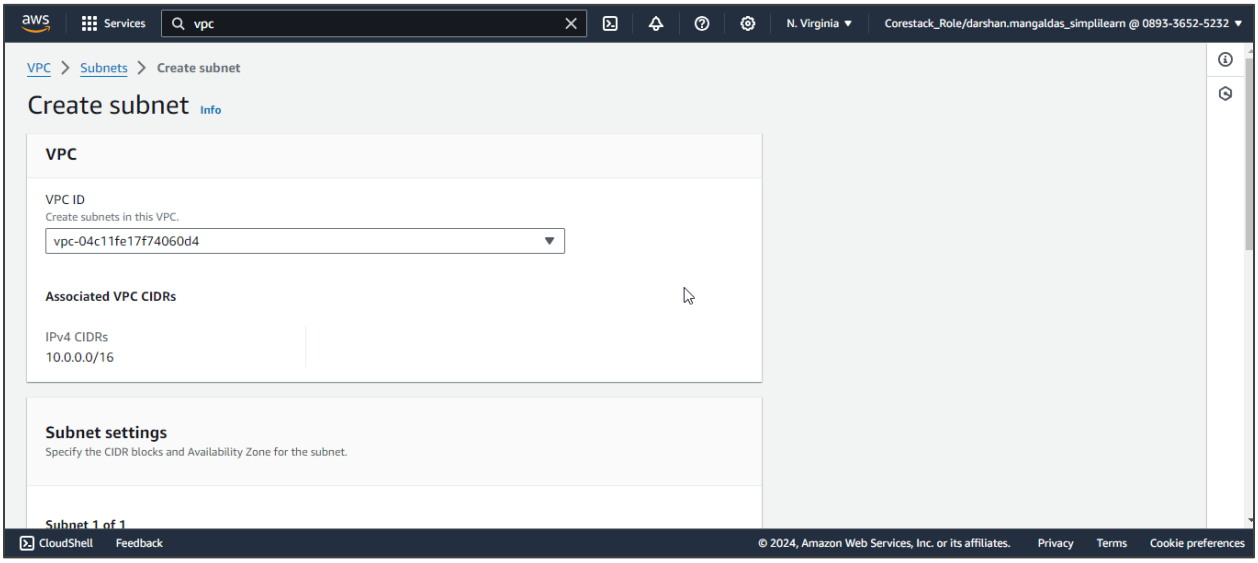


Step 2: Create public and private subnets in three different availability zones

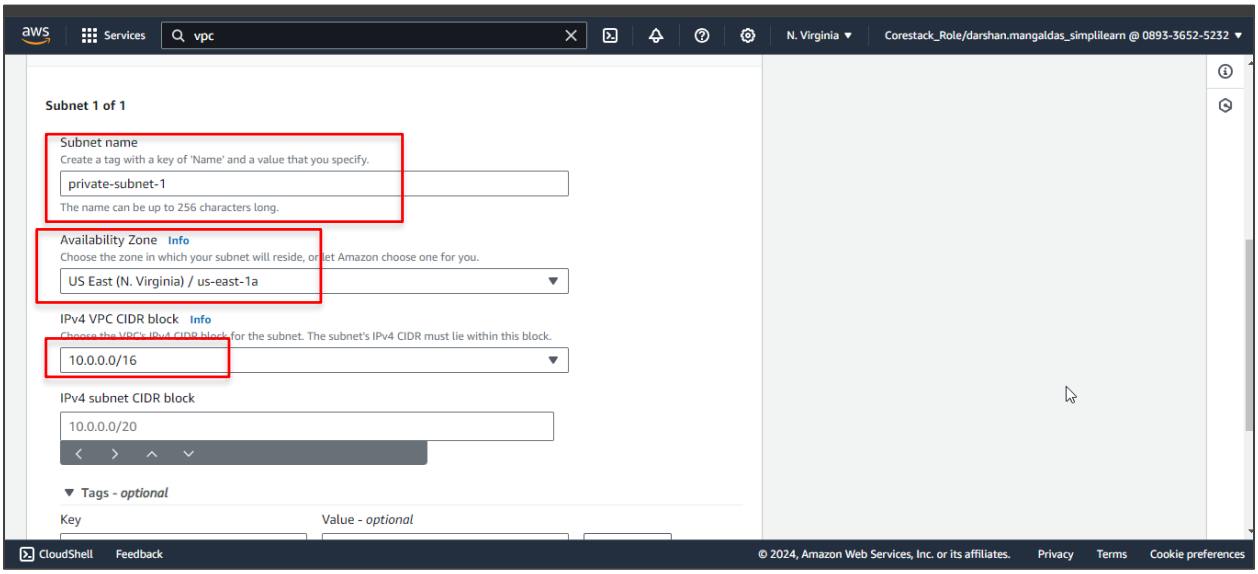
2.1 Click on the **Create subnet** button

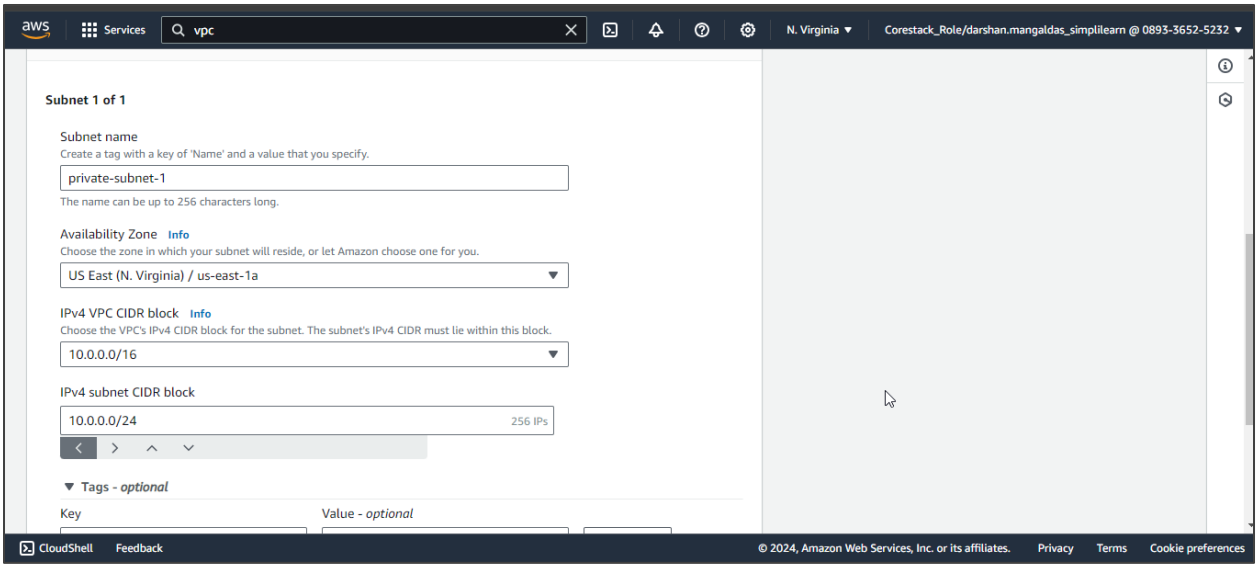


2.2 Select the **VPC ID** as shown below:

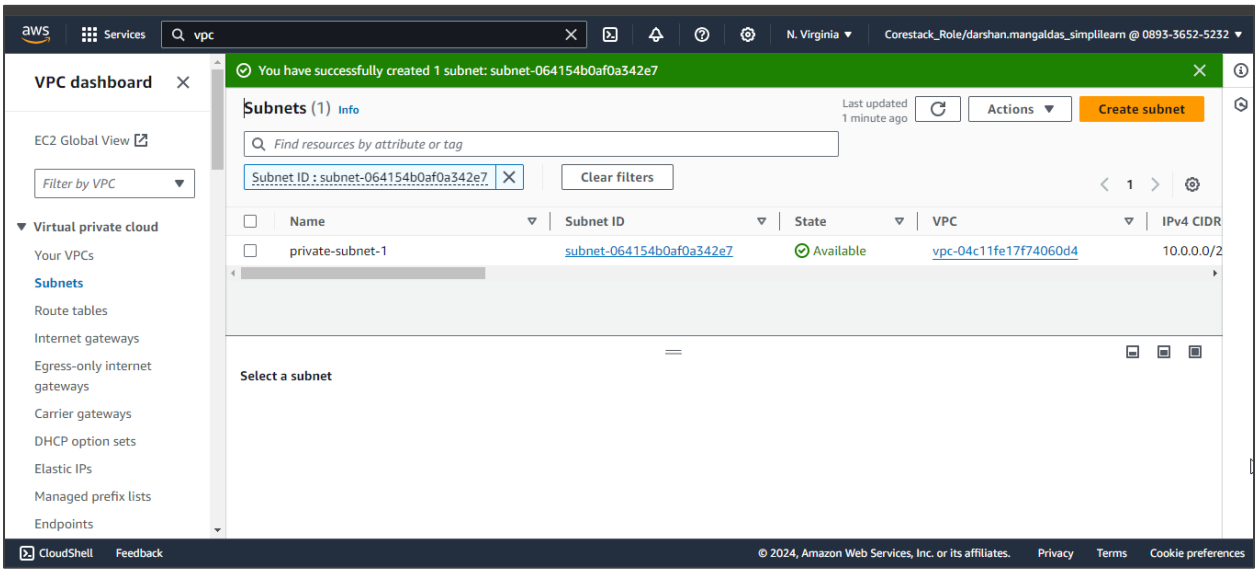


2.3 Enter the **Subnet name** as **private-subnet-1**, **Availability Zone** as **us-east-1a**, and **IPv4** as **10.0.0.0/16** as shown below:

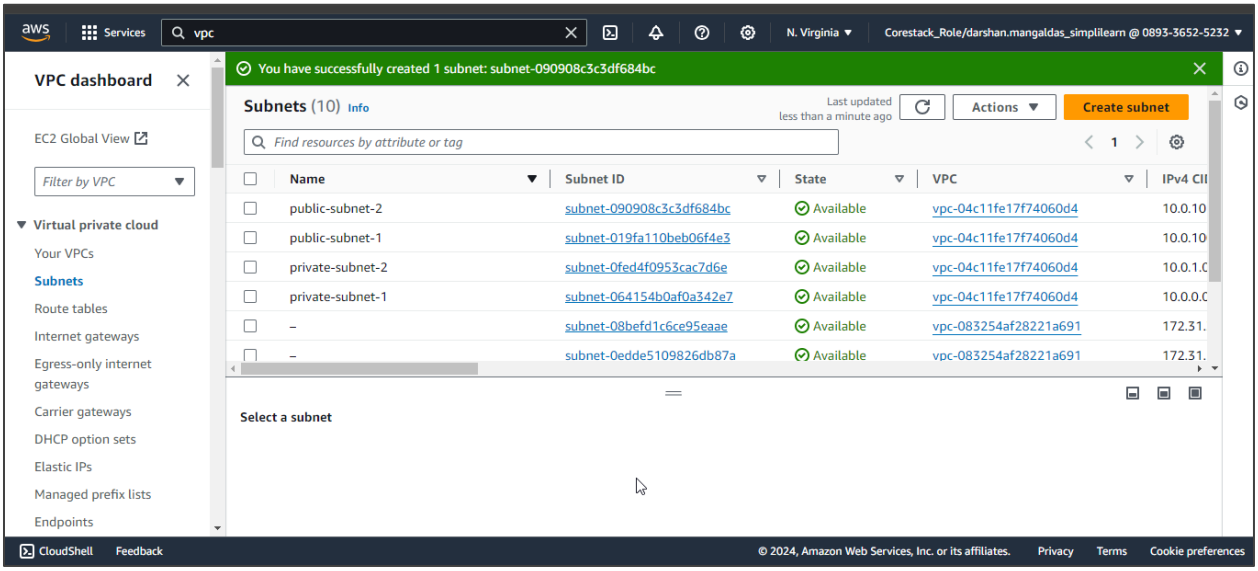




The required **subnet** will be created successfully as shown below:

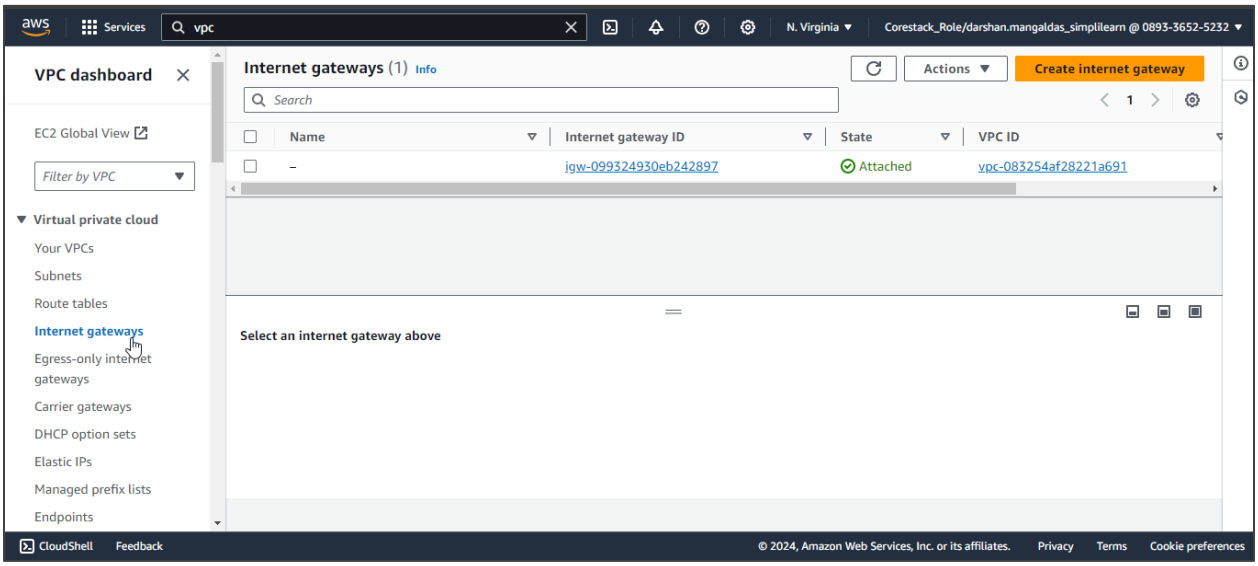


Similarly, create three more subnets with different names and regions following the above steps

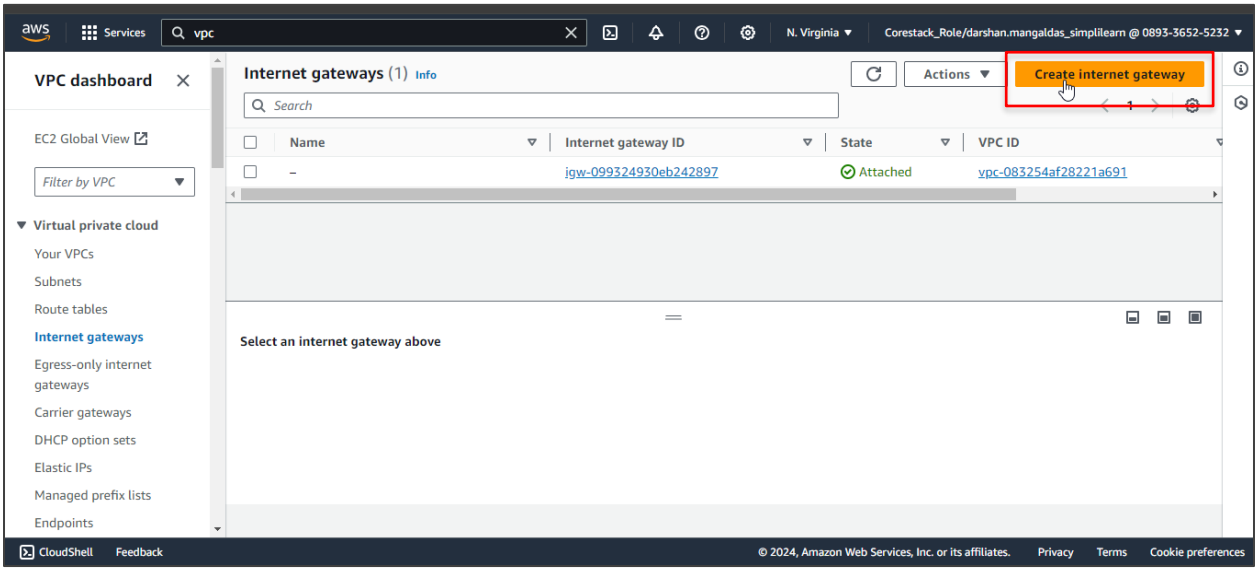


Step 3: Deploy an internet gateway and attach it to the VPC

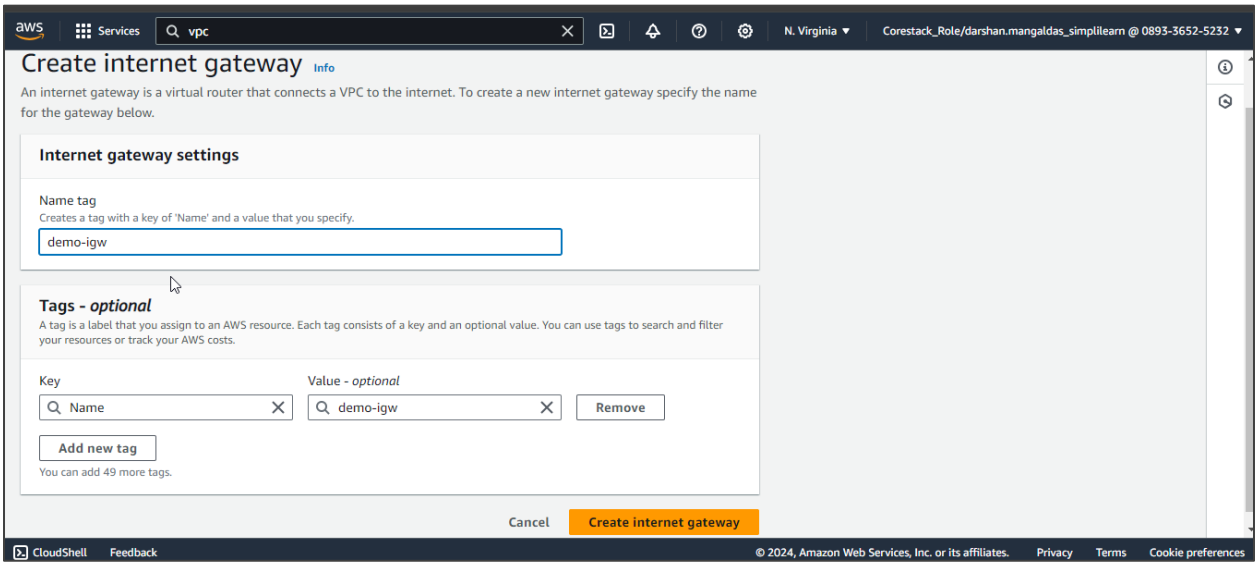
3.1 Click on the **Internet gateways** option on the VPC dashboard



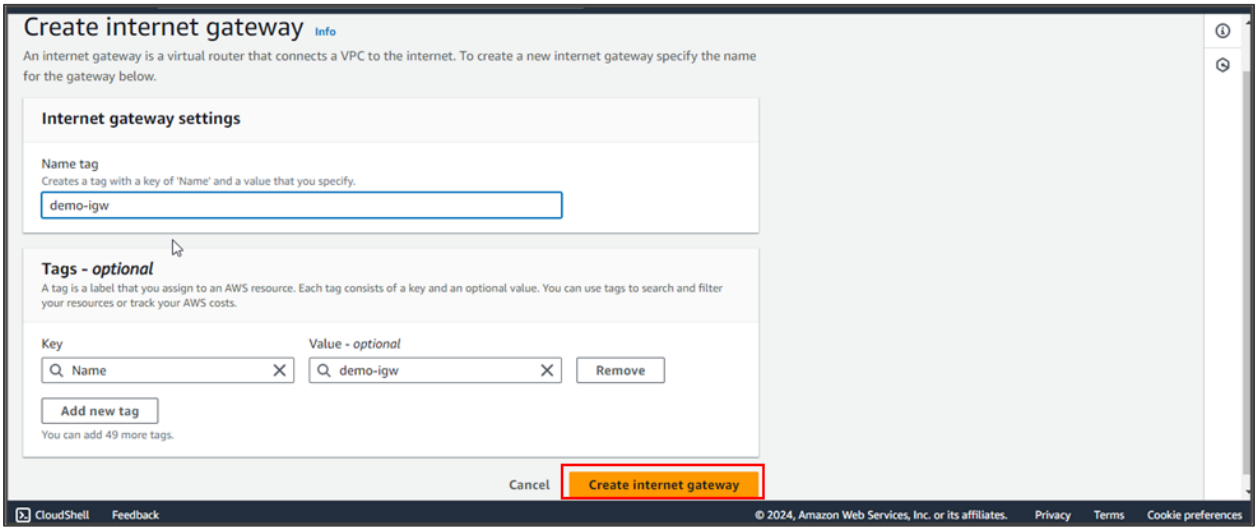
3.2 Click on the **Create internet gateway** button as shown below:



3.3 Enter **demo-igw** in the **Name tag** field

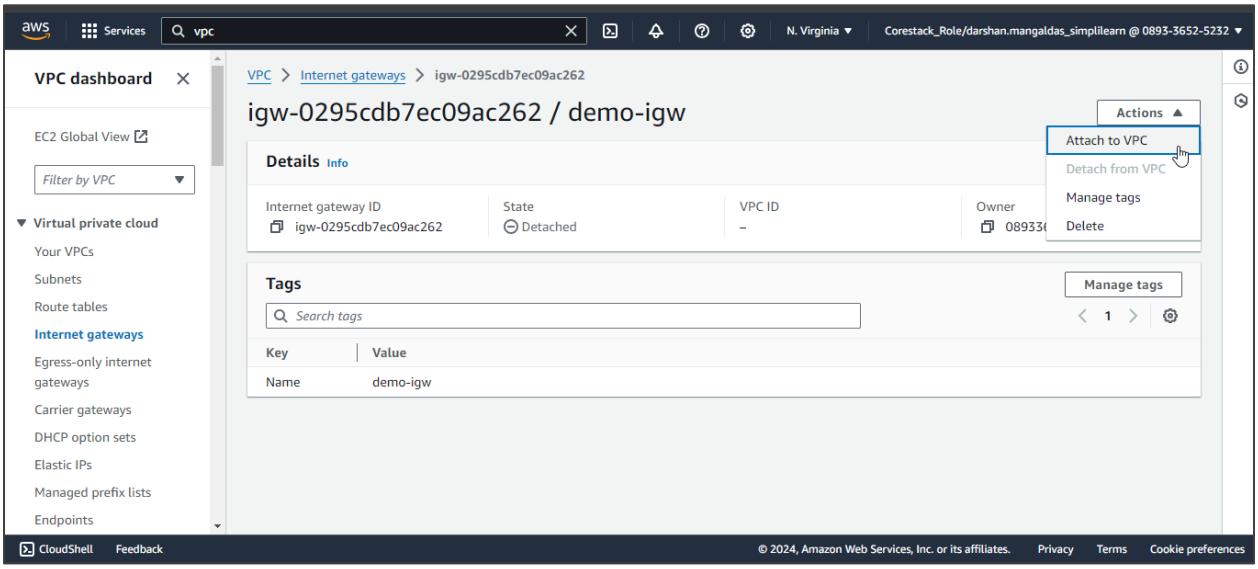


3.4 Click on the **Create internet gateway** button as shown below:

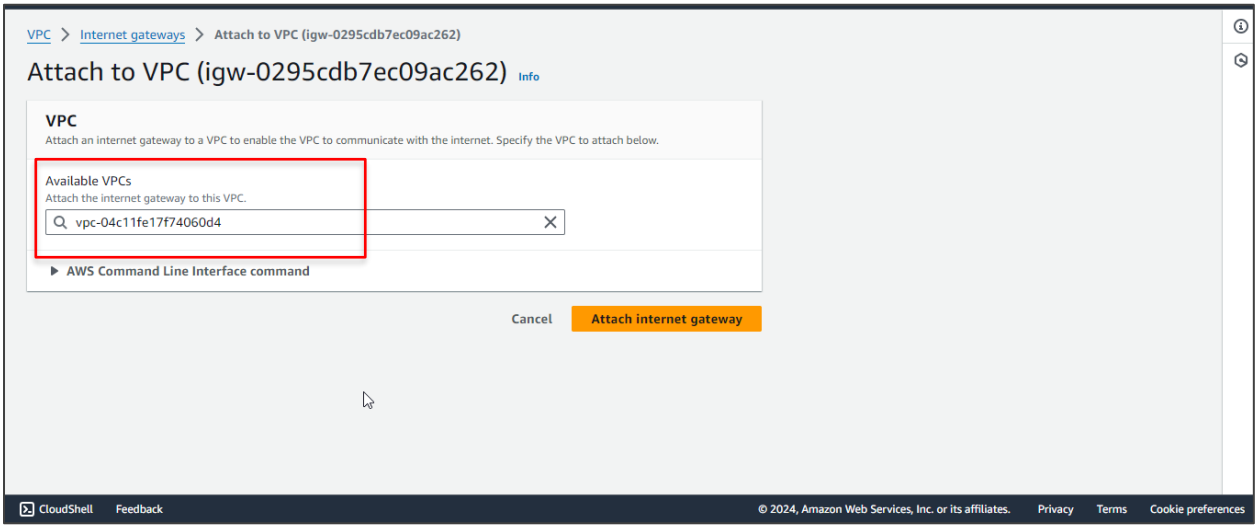


The internet gateway is successfully created.

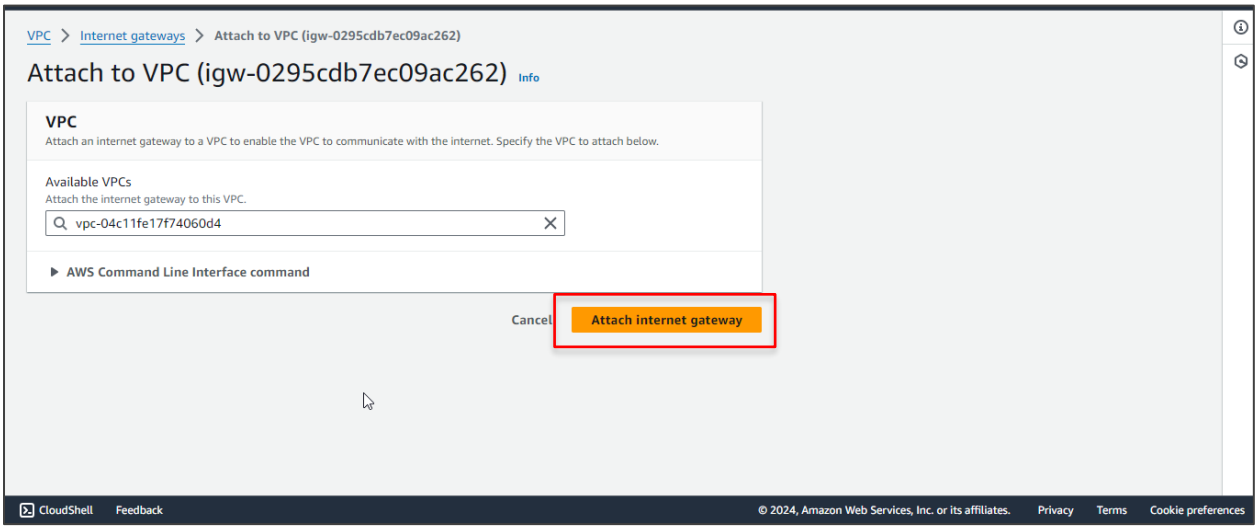
3.5 Click on the **Attach to VPC** option under the **Actions** tab as shown below:



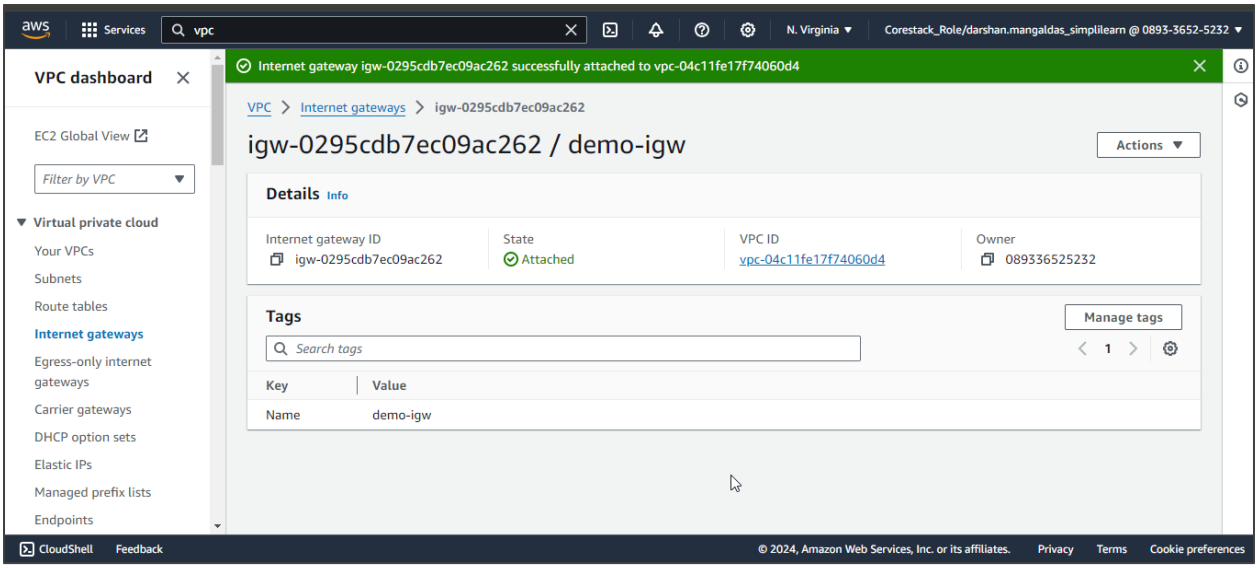
3.6 Select the created VPC from the drop-down list in the **Available VPCs** field as shown below:



3.7 Click on the **Attach internet gateway** button

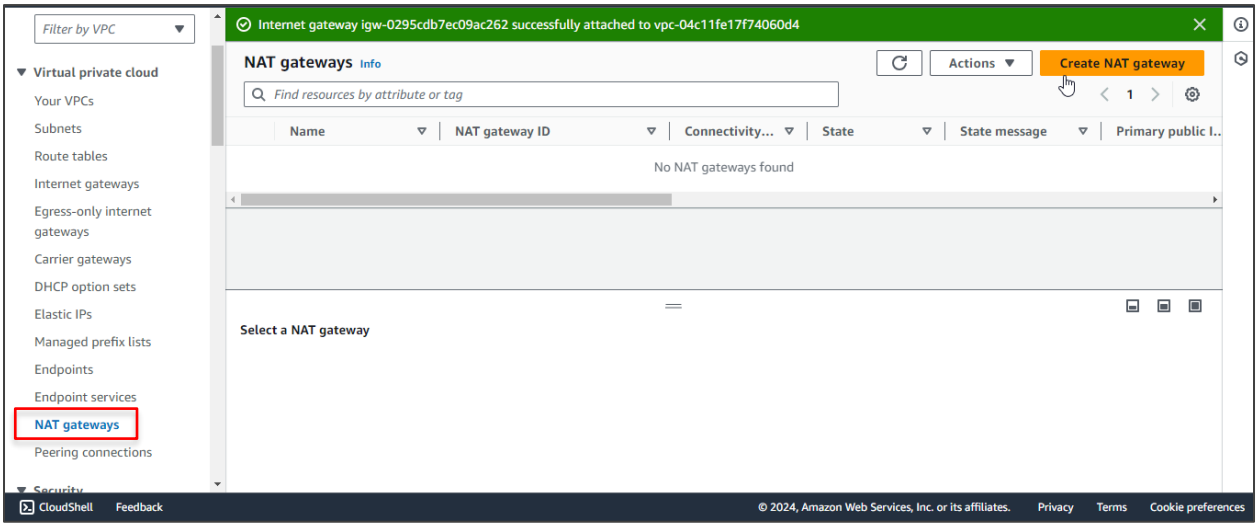


The internet gateway will be created as shown below:

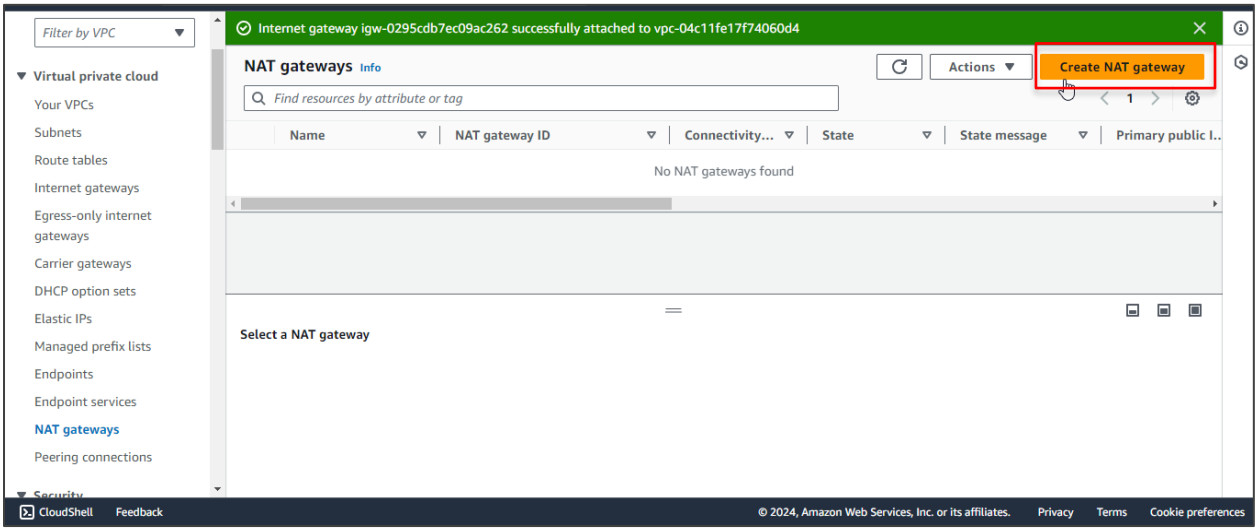


Step 4: Provision a NAT gateway for outbound connectivity

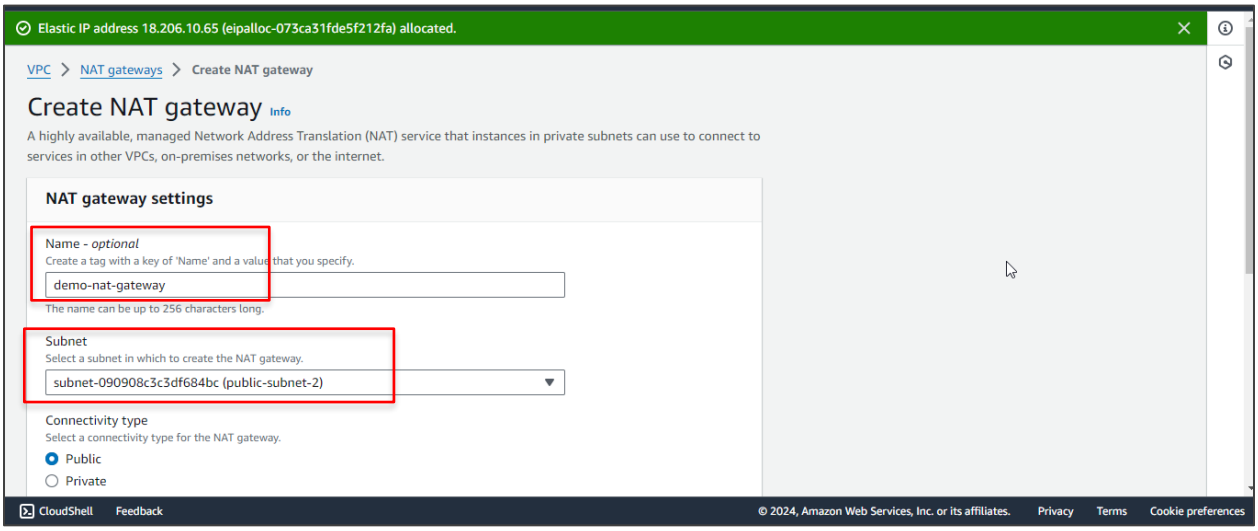
4.1 Click on the **NAT gateways** option in the VPC dashboard



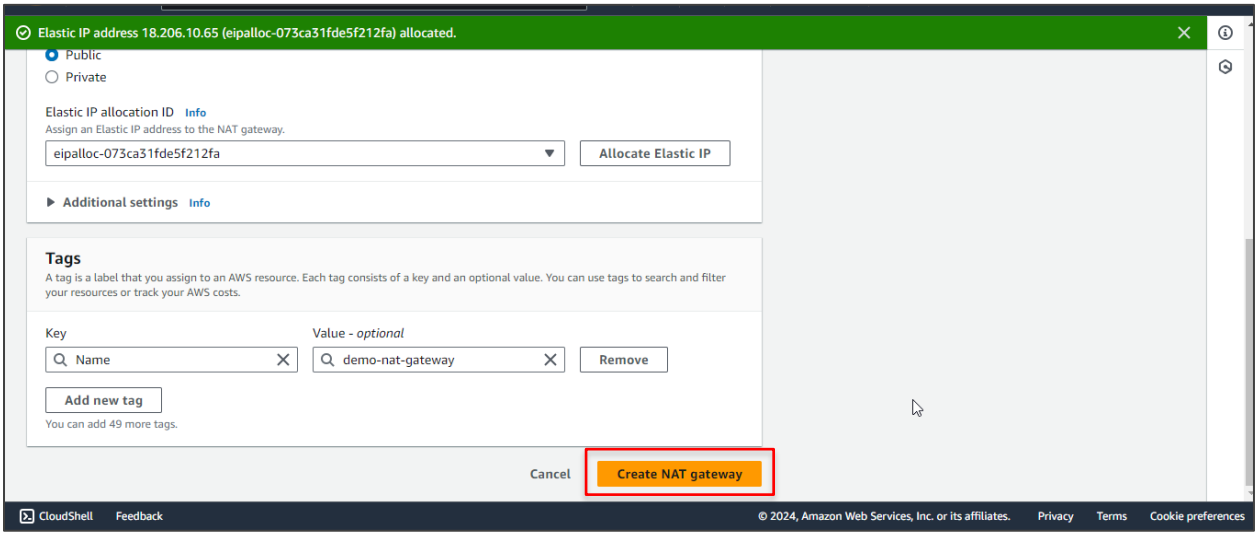
4.2 Click on the **Create NAT gateway** button as shown below:



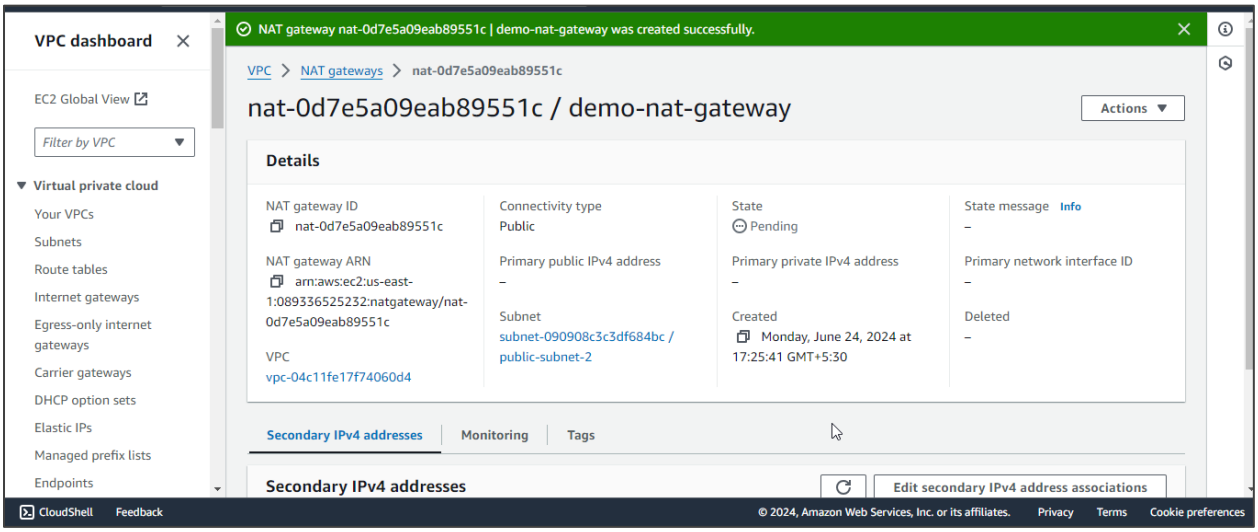
4.3 Enter **demo-nat-gateway** in the **Name** field, select **public-subnet-2** from the **Subnet** option, and in the **Connectivity type** field, select **Public** as shown below:



4.4 Click on the **Create NAT gateway** button

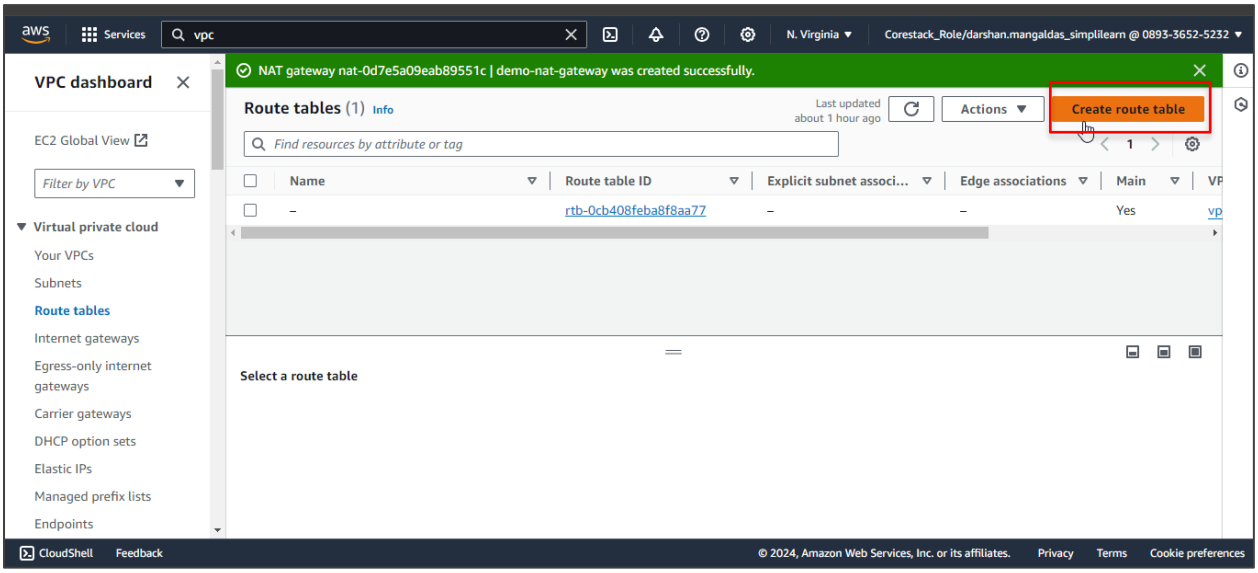


The **NAT gateway** will be created as shown below:

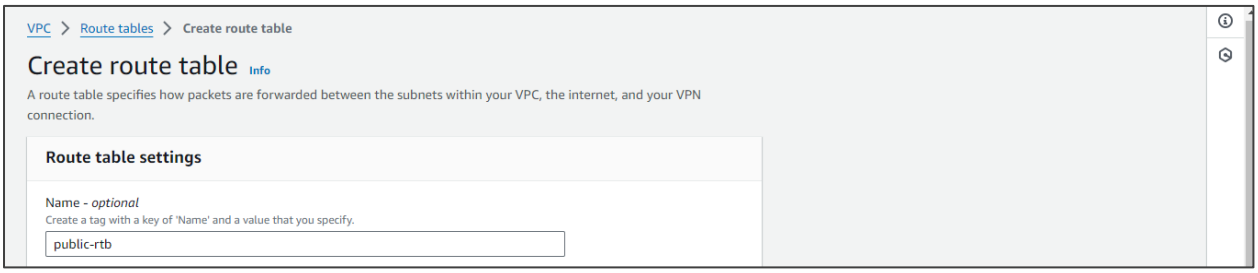


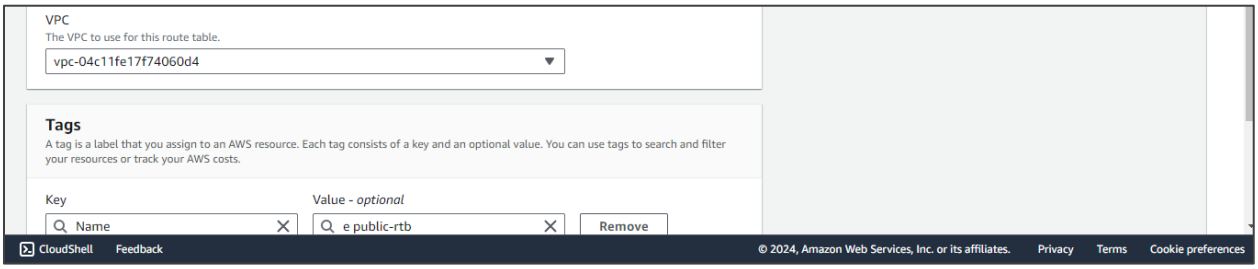
Step 5: Configure the route tables to route traffic

5.1 In the VPC console, select **Route tables** from the left navigation panel and click the **Create route table** button

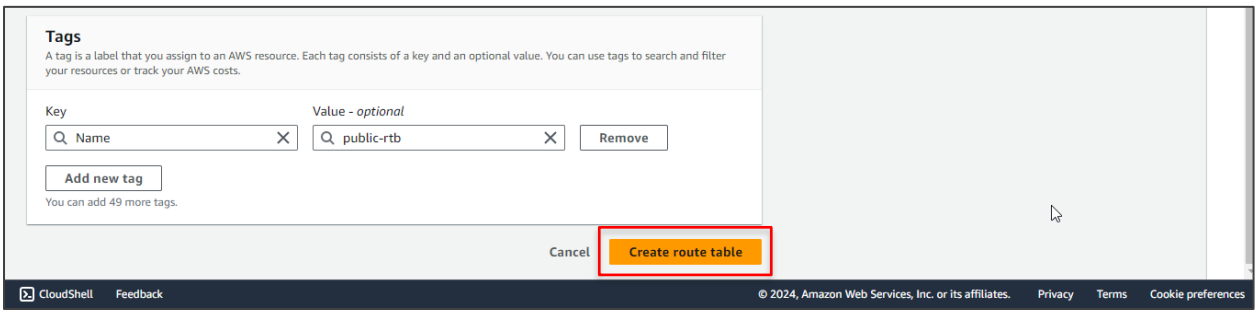


5.2 Name the route table **public-rtb**, and select the **VPC** created in step 1



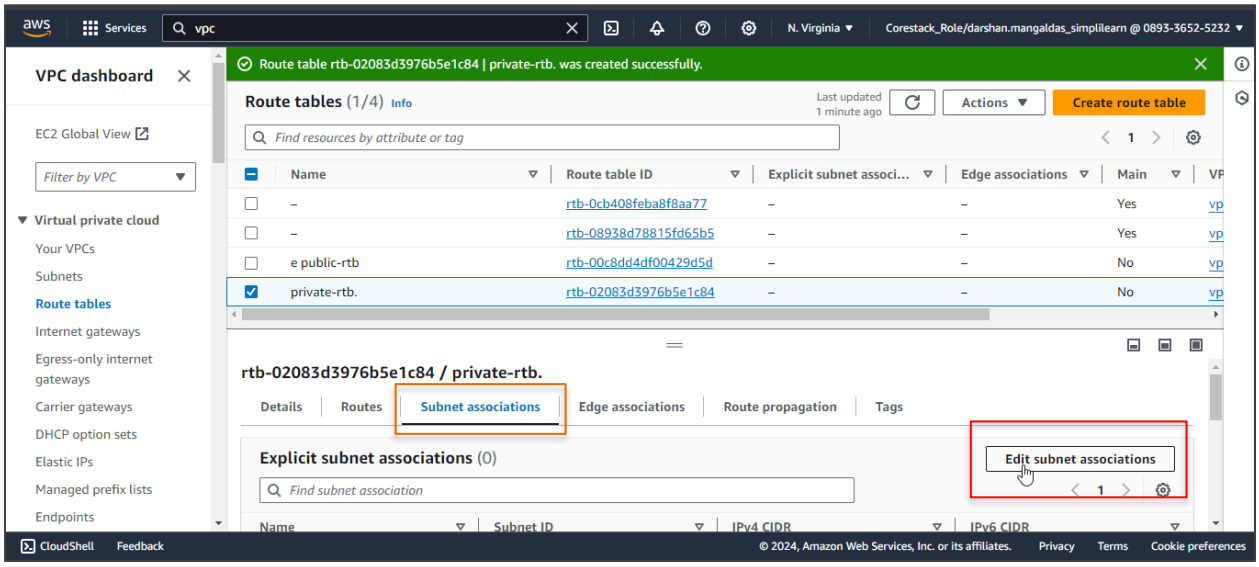


5.3 Click the **Create route table** button to create your first route table

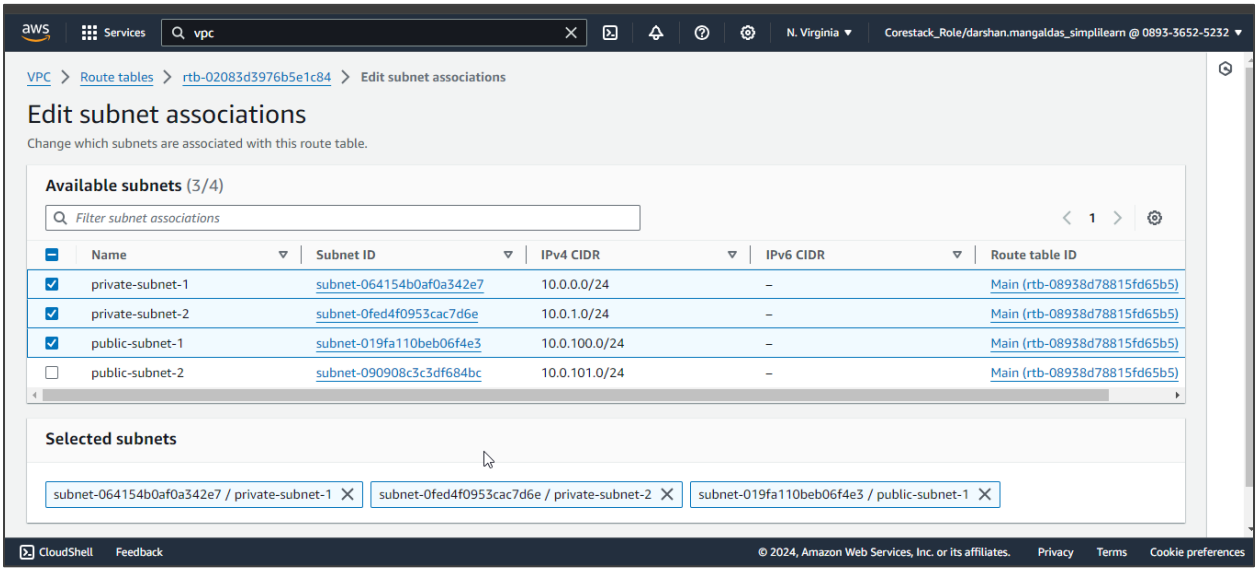


Note: Repeat the above task to create a second route table; name the second table **private rtb**. Select the same VPC created in step 1. Click the **Create route table** button to create the second route table.

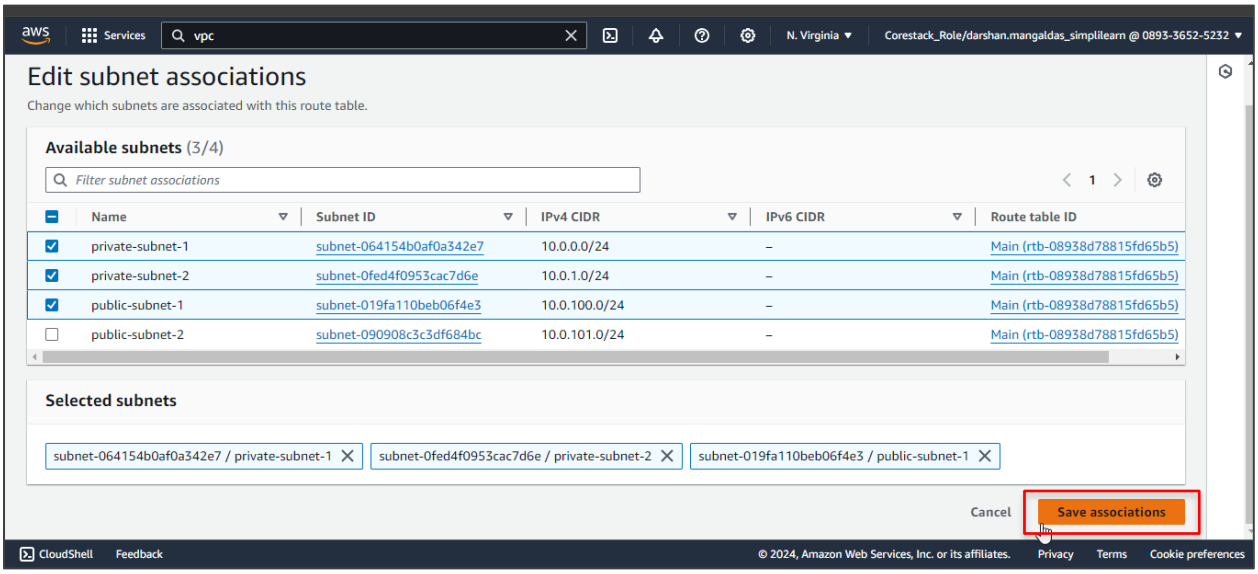
5.4 In the Route tables console, select the **public-rtb** route table, go to the **Subnet associations** tab, and click the **Edit subnet associations** button



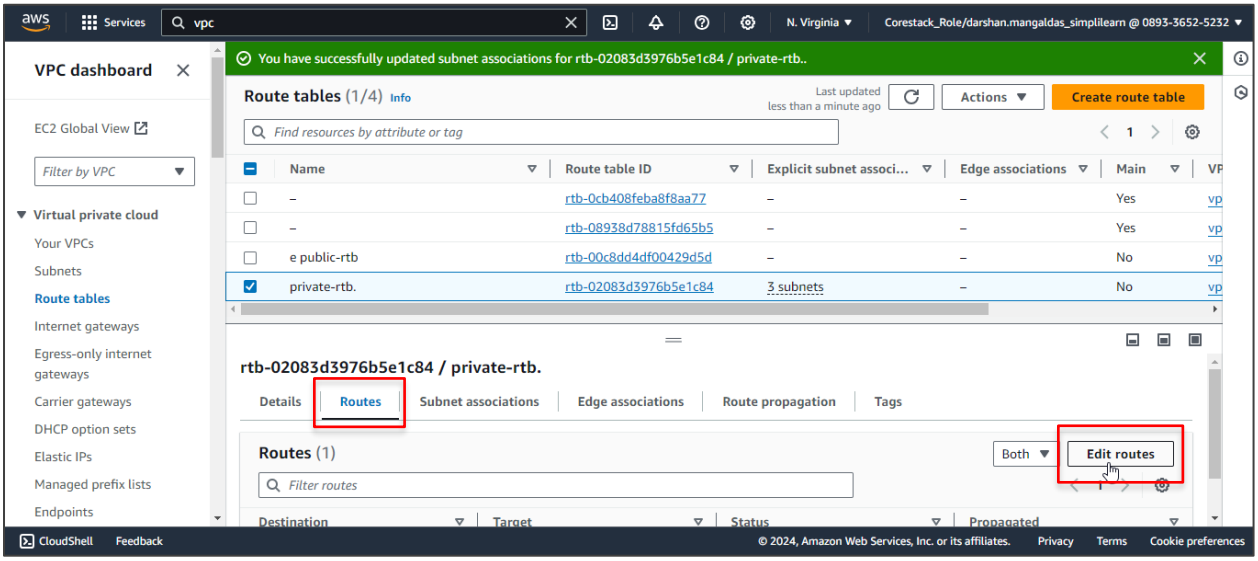
5.5 Select the three subnets that you created in Step 2 from the list of available subnets



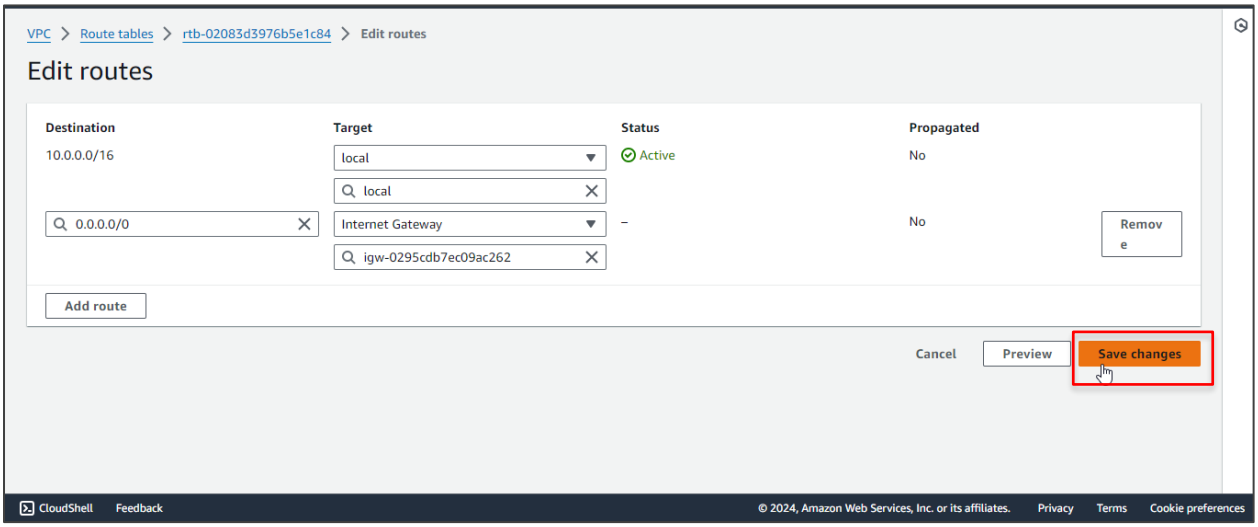
5.6 Once you have selected the three subnets, click on the **Save associations** button to save your configuration



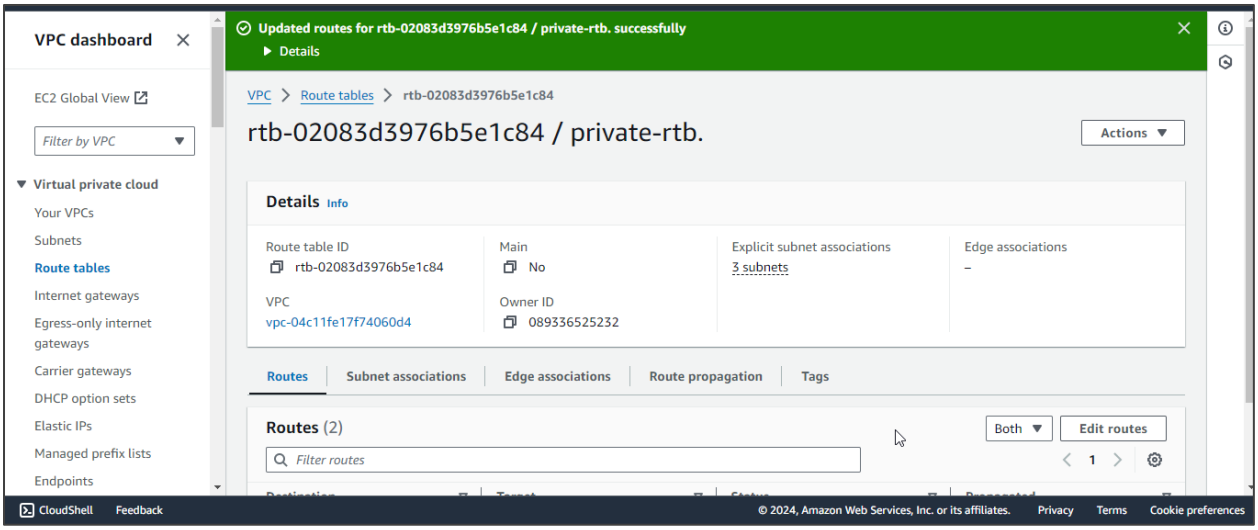
5.7 In the Route tables console, select the **public-rtb** route table, click on **Routes**, and then select **Edit Routes** to add routes for proper network traffic routing



5.8 In the Edit routes window, click the **Add route** button, enter **0.0.0.0/0** as the new route destination, select **Internet Gateway** and the gateway created in Step 3 as the **Target**, and then click **Save changes**



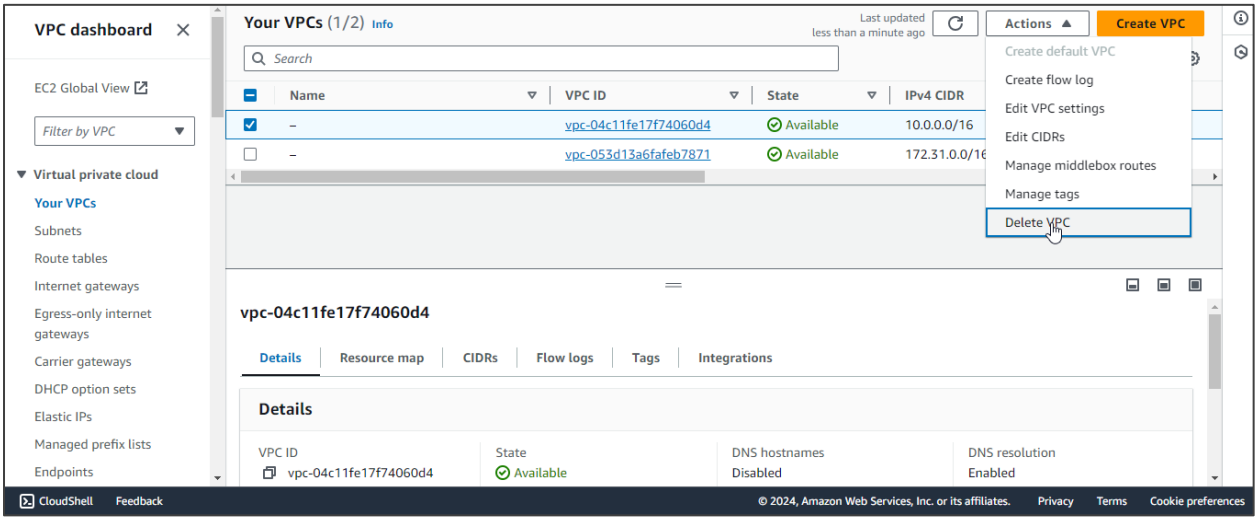
Note: Repeat this step to add a route to the **private-rtb**. The Destination should be 0.0.0.0/0. Select **NAT Gateway** and choose the gateway created in Step 4 as the **Target**. Finally, click **Save changes** to save the new route configuration.



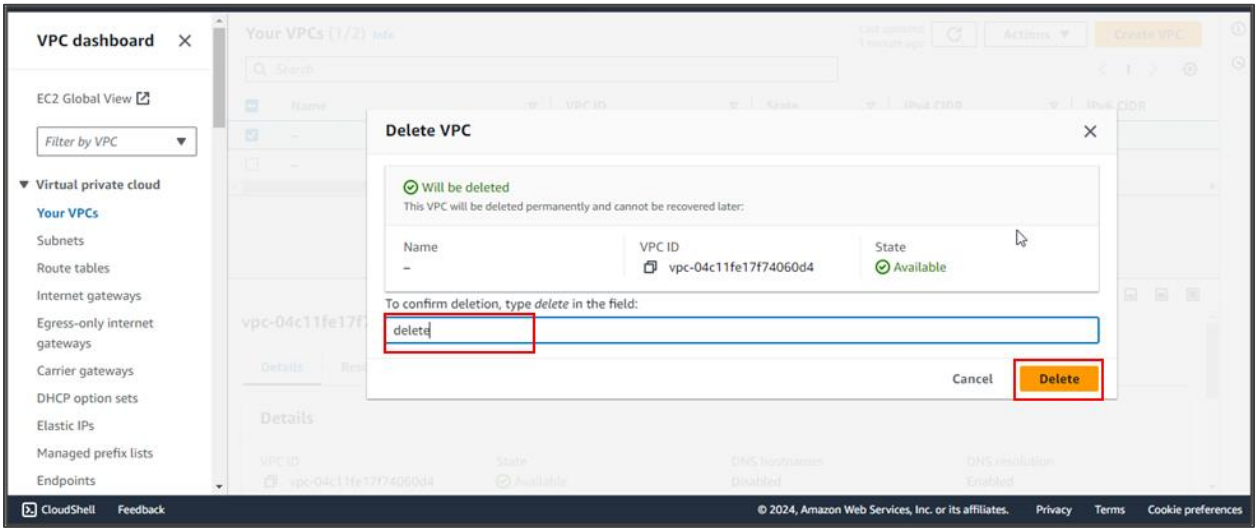
The traffic route for the **private-rtb** route table has also been added.

Step 6: Delete the VPC

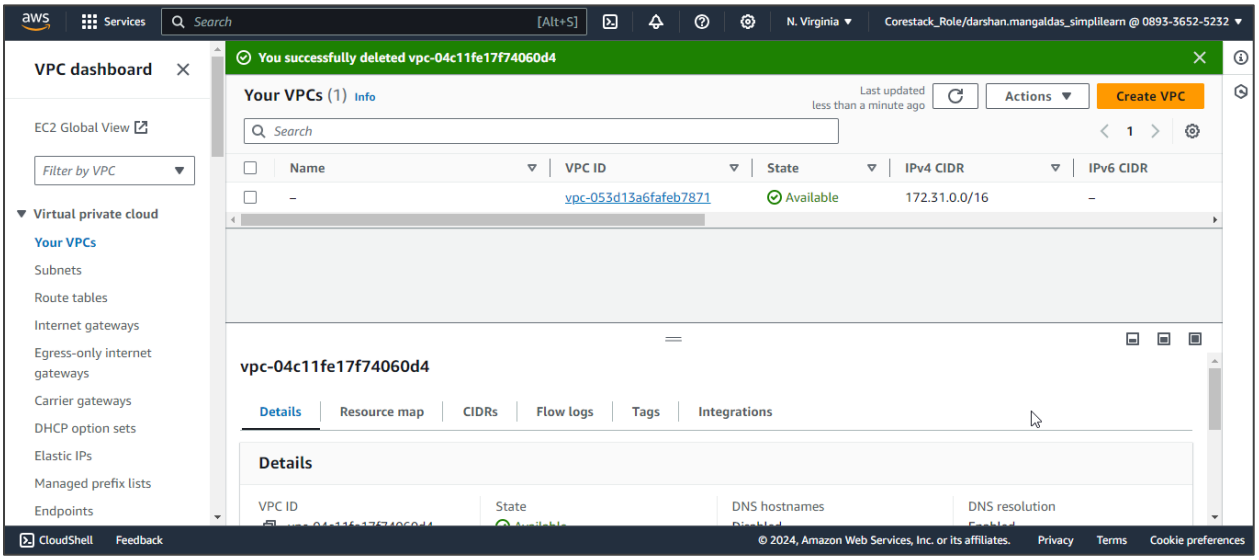
6.1 In the VPC dashboard, select the created VPC, click the **Actions** button, and select **Delete VPC**



6.2 Enter **delete** in the given text field and click on **Delete** to confirm the deletion of the VPC and related AWS resources



The VPC is successfully deleted.



By following these steps, you have successfully deployed and managed a VPC with public and private subnets across multiple availability zones in AWS, ensuring proper routing and connectivity. This setup provides a resilient and scalable infrastructure, ready for testing failover and disaster recovery scenarios.