

Open in app ↗

Medium

 Search

Rahul Desharaj · Following

8 min read · Apr 19, 2024



Listen



Share



More

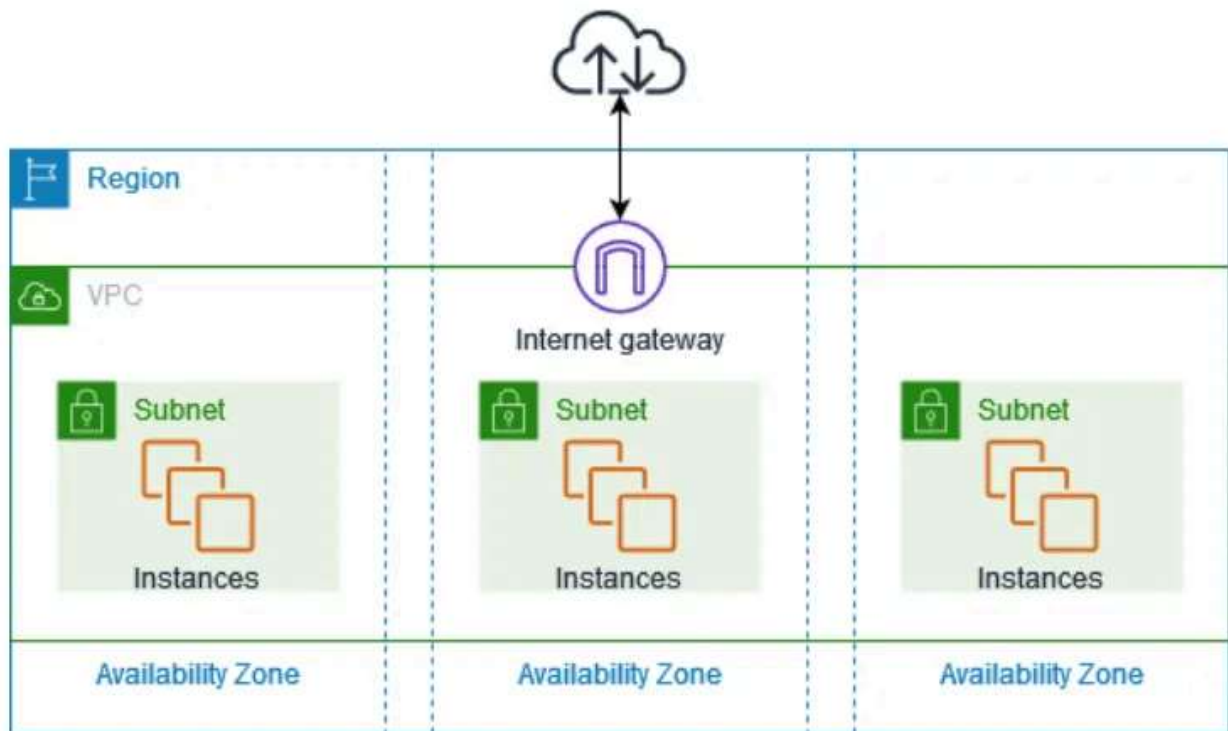
## What is VPC in AWS ? How to Create a VPC in AWS?

Amazon Virtual Private Cloud (Amazon VPC) enables you to launch AWS resources into a virtual network that you've defined. This virtual network closely resembles a traditional network that you'd operate in your own data center , with the benefits of using the scalable infrastructure of AWS.

### Why we need VPC ?

AWS VPC allows you to create a secure and isolated network for your resources, which provides a high level of security and control. This means that you can create your own private network, which is not accessible from the internet or other networks.

The following diagram shows an example VPC. The VPC has one subnet in each of the Availability Zones in the Region, EC2 instances in each subnet, and an internet gateway to allow communication between the resources in your VPC and the internet.



### AWS VPC Components:

**Subnet :** subnet is a range of IP addresses in your VPC. You can launch AWS resources into a specified subnet. Use a public subnet for resources that must be connected to the internet, and a private subnet for resources that won't be connected to the internet.

**Route Tables:** A route table is a set of rules that determines how traffic is directed in your VPC. You can create multiple route tables and assign them to different subnets to control the flow of traffic.

**Internet Gateway:** AWS component that provides a path for network traffic to travel between a Virtual Private Cloud (VPC) and the public internet. It acts as a bridge between the two networks, enabling inbound and outbound connections from resources within the VPC.

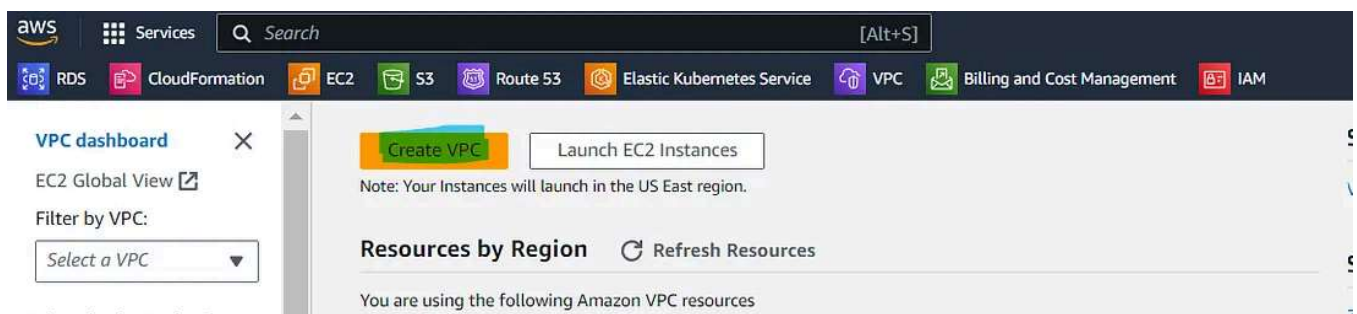
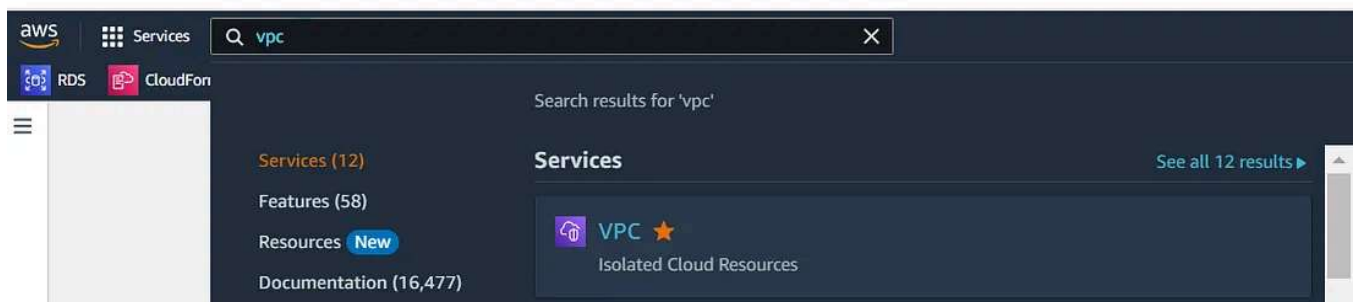
**NAT Gateway:** A network address translation (NAT) gateway enables instances in a private subnet to connect to the internet or other AWS services while preventing the internet from initiating connections with the instances.

**Security Groups:** Security groups act as a virtual firewall for your instances. You can create security groups to control inbound and outbound traffic for your instances. When you launch an instance in a VPC, you can assign up to five security groups to

the instance. Security groups act at the instance level, not the subnet level. Therefore, each instance in a subnet in your VPC could be assigned to a different set of security groups. If you don't specify a particular group at launch time, the instance is automatically assigned to the default security group for the VPC.

**Network Access Control Lists (NACLs):** NACLs are another layer of security that act as a firewall for subnets. You can use NACLs to control inbound and outbound traffic at the subnet level.

## Creating your own VPC:



If you clicked on the button “Create VPC” you will get following screen.

VPC > Your VPCs > Create VPC

## Create VPC [Info](#)

A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon EC2 instances.

### VPC settings

**Resources to create** [Info](#)  
Create only the VPC resource or the VPC and other networking resources.

☒ VPC only ☐ VPC and more

**Name tag - optional**  
Creates a tag with a key of 'Name' and a value that you specify.

medium

**IPv4 CIDR block** [Info](#)  
☒ IPv4 CIDR manual input  
☐ IPAM-allocated IPv4 CIDR block

**IPv4 CIDR**  
10.0.0.0/16  
CIDR block size must be between /16 and /28.

**IPv6 CIDR block** [Info](#)  
☒ No IPv6 CIDR block  
☐ IPAM-allocated IPv6 CIDR block  
☐ Amazon-provided IPv6 CIDR block  
☐ IPv6 CIDR owned by me

**Tenancy** [Info](#)

Now give your VPC name and your custom CIDR(Classless Inter Domain Routing) Range as I have given both parameters as you can see in below image.

After Click on the “Create VPC” following screen will appear.

VPC dashboard

EC2 Global View

Filter by VPC:  
Select a VPC

Virtual private cloud

Your VPCs

Subnets

Route tables

Internet gateways

Egress-only Internet gateways

Carrier gateways

DHCP option sets

Elastic IPs

Managed prefix lists

Endpoints

Endpoint services

NAT gateways

Peering connections

Security

Network ACLs

Security groups

You successfully created vpc-080976a64e0e230a3 / medium

VPC > Your VPCs > vpc-080976a64e0e230a3

vpc-080976a64e0e230a3 / medium [Actions](#)

**Details** [Info](#)

VPC ID vpc-080976a64e0e230a3	State <span>Available</span>	DNS hostnames Disabled	DNS resolution Enabled
Tenancy Default	DHCP option set dopt-0a257a4e6e3fc8bf3	Main route table rtb-030a83608787bc016	Main network ACL acl-0ad4221b2041f3f2f
Default VPC No	IPv4 CIDR 10.0.0.0/16	IPv6 pool -	IPv6 CIDR (Network border group) -
Network Address Usage metrics Disabled	Route 53 Resolver DNS Firewall rule groups -	Owner ID 100796962221	

[Resource map](#) [CIDRs](#) [Flow logs](#) [Tags](#) [Integrations](#)

**Resource map** [Info](#)

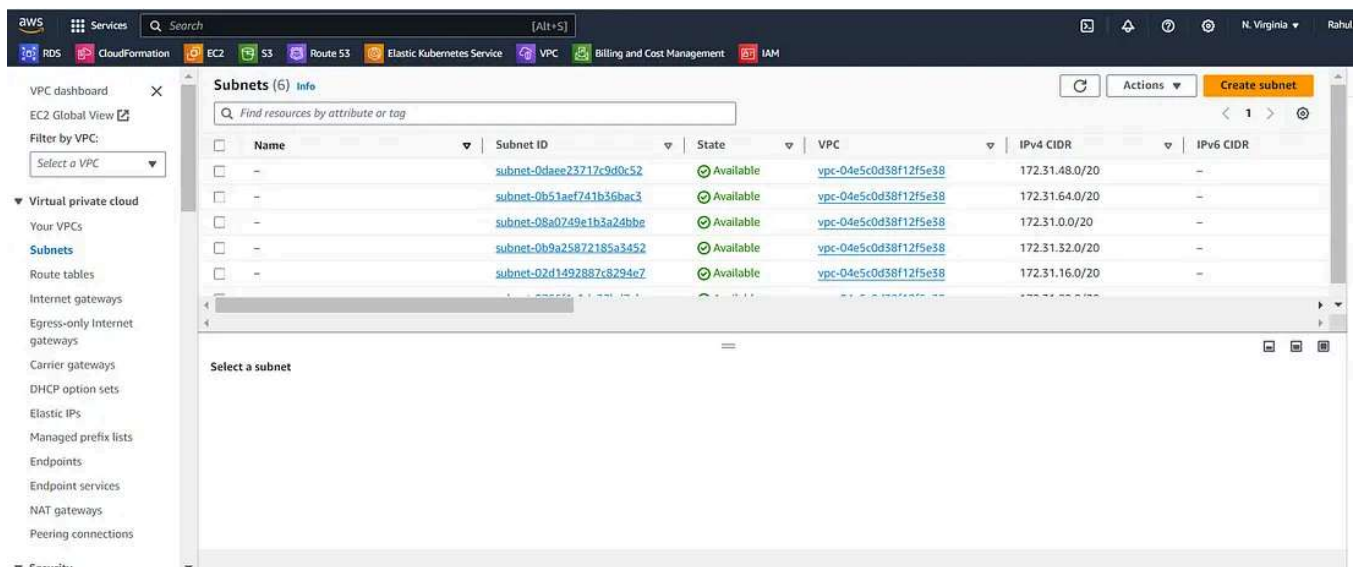
VPC [Show details](#)  
Your AWS virtual network  
medium

Subnets (0)  
Subnets within this VPC

Route tables (1)  
Route network traffic to resources  
rtb-030a83608787bc016

Network connections (0)  
Connections to other networks

**Step 2:** Click on the “Subnets” in the left-side pane, after that the following screen will appear.



**Step 2.1:** Click on the “Create Subnet” After that following screen will appear.

VPC > Subnets > Create subnet

## Create subnet [Info](#)

**VPC**

VPC ID  
Create subnets in this VPC.

Select a VPC

**Subnet settings**  
Specify the CIDR blocks and Availability Zone for the subnet.

Select a VPC first to create new subnets.

Add new subnet

Cancel Create subnet

**Step 2.2:** After selecting the “VPC ID” do the following things:

- Choose your custom “VPC ID” from the dropdown menu.
- Provide a subnet name.
- Select the desired Availability Zone (AZ) for the subnet.

- Fill in the subnet range.
- Click on “Create Subnet.”

For reference following are the screen shot of the steps.

VPC ID  
Create subnets in this VPC.  
vpc-0443a72887a5112eb (medium)

Associated VPC CIDRs  
IPv4 CIDRs  
10.0.0.0/16

Subnet settings  
Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

Subnet name  
Create a tag with a key of 'Name' and a value that you specify.  
public-subnet  
The name can be up to 256 characters long.

Availability Zone [Info](#)  
Choose the zone in which your subnet will reside, or let Amazon choose one for you.  
US East (N. Virginia) / us-east-1a

IPv4 VPC CIDR block [Info](#)  
Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.  
10.0.0.0/16

IPv4 subnet CIDR block  
10.0.1.0/24 256 IPs

VPC dashboard

EC2 Global View

Filter by VPC

Virtual private cloud

Your VPCs

Subnets

Route tables

Internet gateways

Egress-only Internet gateways

Carrier gateways

DHCP option sets

Elastic IPs

Managed prefix lists

You have successfully created 1 subnet: subnet-01879abe28adf827b

Subnets (1) [Info](#)

Find resources by attribute or tag

Subnet ID: subnet-01879abe28adf827b Clear filters

Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 CIDR	IPv6 CIDR association ID
public-subnet	subnet-01879abe28adf827b	Available	vpc-0443a72887a5112eb   med...	10.0.1.0/24	-	-

Select a subnet

Now create Private-subnet as well , please do follow same steps like above.

VPC dashboard

EC2 Global View

Filter by VPC

Virtual private cloud

Your VPCs

Subnets

Route tables

Internet gateways

Egress-only Internet gateways

Carrier gateways

DHCP option sets

Elastic IPs

Managed prefix lists

You have successfully created 1 subnet: subnet-0ecc434e5fad166fa

Subnets (1/2) [Info](#)

Find resources by attribute or tag

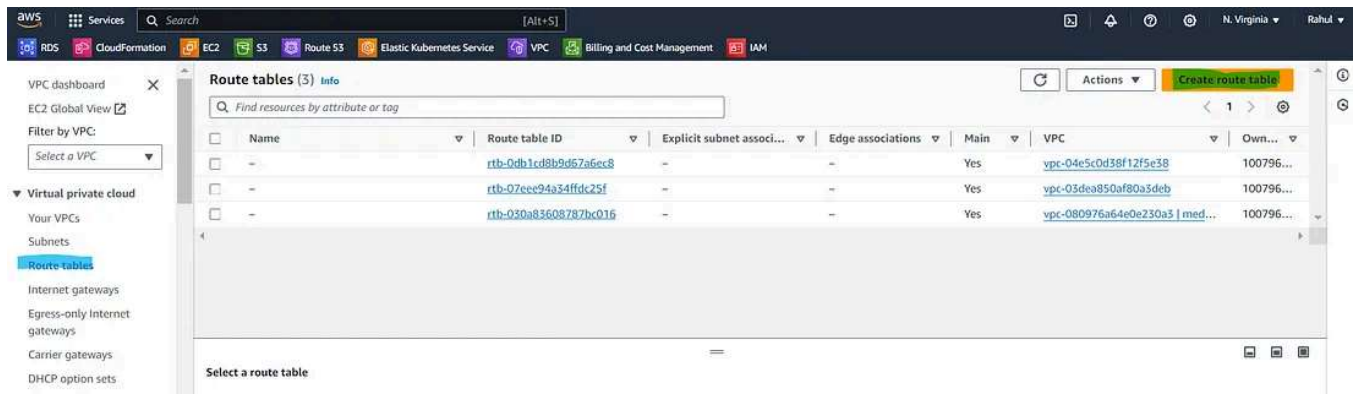
VPC: vpc-0443a72887a5112eb Clear filters

Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 CIDR	IPv6 CIDR association ID
public-subnet	subnet-01879abe28adf827b	Available	vpc-0443a72887a5112eb   med...	10.0.1.0/24	-	-
private-subnet	subnet-0ecc434e5fad166fa	Available	vpc-0443a72887a5112eb   med...	10.0.11.0/24	-	-

**Step 3:** Now create Route Table for that click on the “Route Tables” that is present on the left side window pane, after click on the “Route Tables” following screen will



appear.



### Step 3.1:

- Click on the orange “Create route table” button.
- Provide a name for the route table.
- Select the VPC for which you want to create the route table.
- Click the “Create route table” button.

For Reference following are the screenshot of the steps:

VPC > Route tables > Create route table

## Create route table [Info](#)

A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.

### Route table settings

**Name - optional**  
Create a tag with a key of 'Name' and a value that you specify.

**VPC**  
The VPC to use for this route table.

### Tags

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

**Key**

**Value - optional**

[Remove](#)

[Add new tag](#)

You can add 49 more tags.

[Cancel](#)
[Create route table](#)

After clicking on the “Create route table” following screen will appear.

Route table rtb-09957beea13a90ddf | my route table was created successfully.

VPC > Route tables > rtb-09957beea13a90ddf

### rtb-09957beea13a90ddf / my route table

**Details** [Info](#)

Route table ID rtb-09957beea13a90ddf	Main No	Explicit subnet associations -	Edge associations -
VPC vpc-080976a64e0e230a3   medium	Owner ID 100796962221		

**Routes** | Subnet associations | Edge associations | Route propagation | Tags

**Routes (1)**

[Both](#) [Edit routes](#)

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No

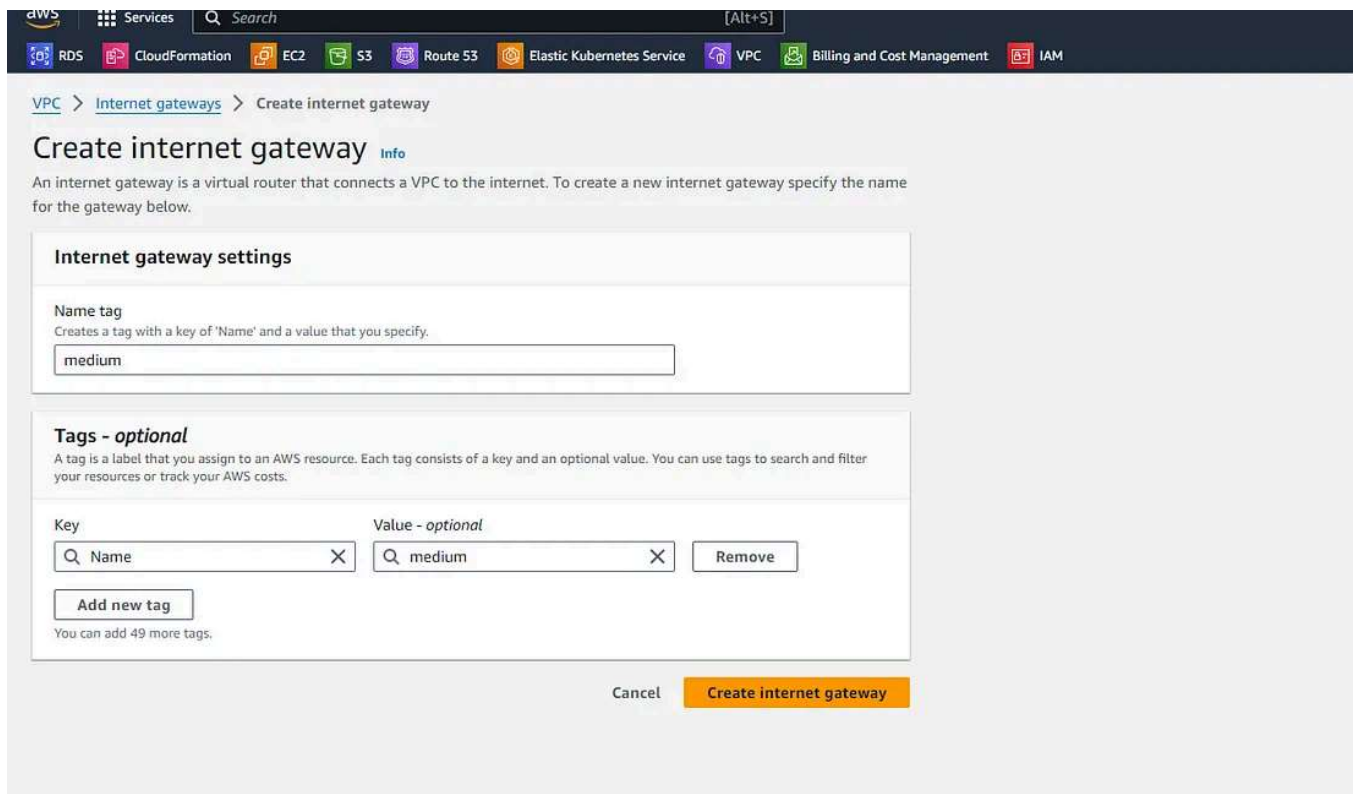
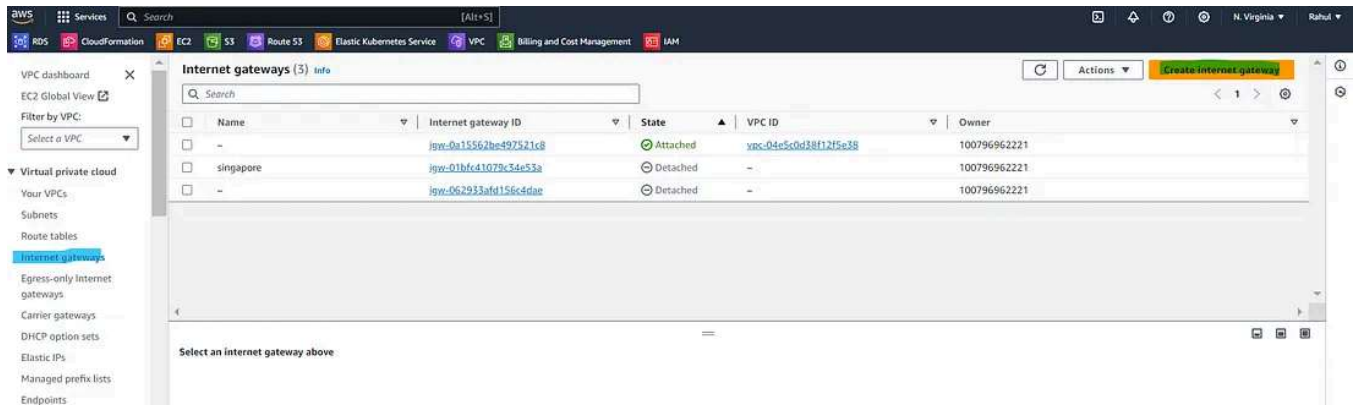
#### Step 4:

- Click on “Internet gateways.”
- Click the orange “Create Internet Gateway” button.
- Provide a name for the Internet gateway.

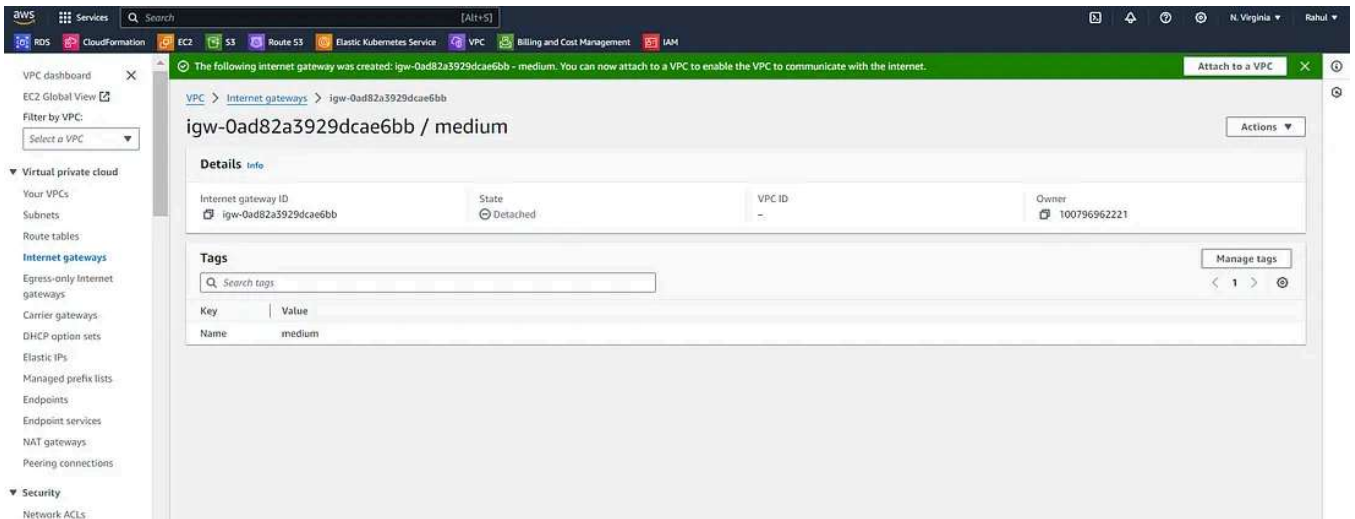


- Click on the “Create Internet Gateway” button.

For reference following are the screenshot of the steps:



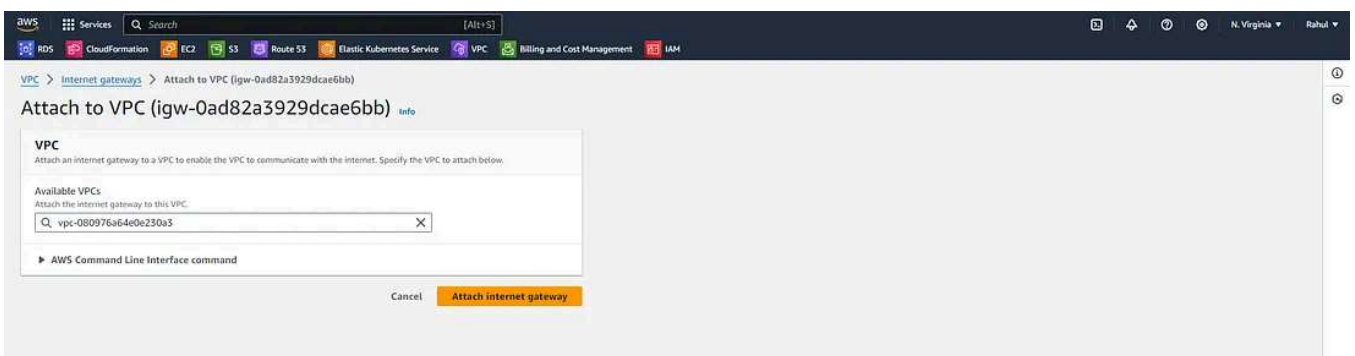
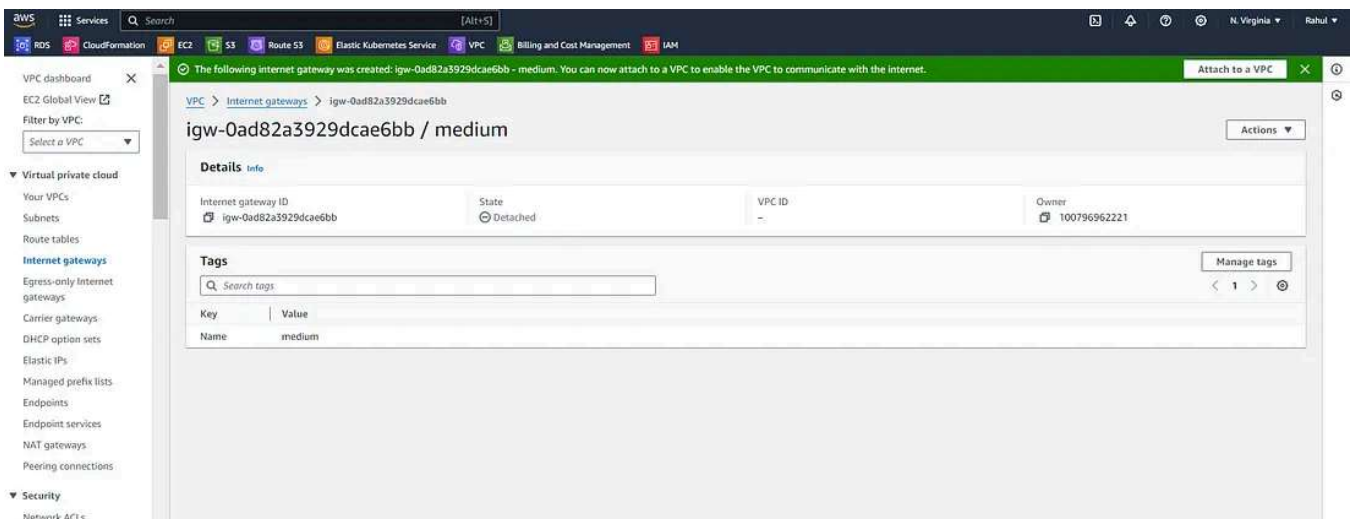
After clicking on the “Create Internet Gateway” button following screen will appear.



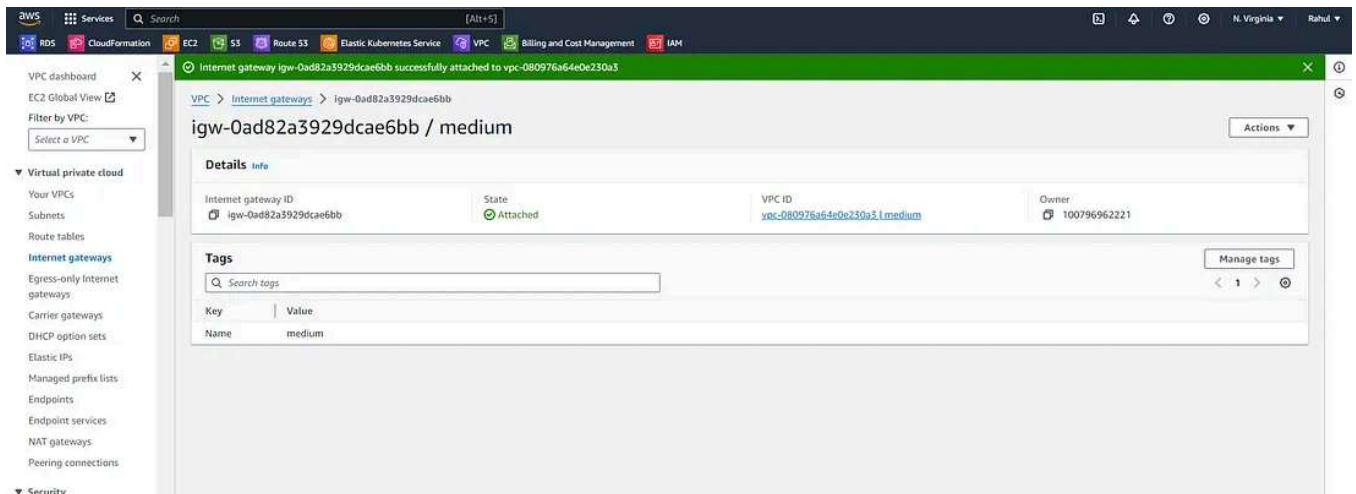
## Step 4.1:

- Click on the “Attach to a VPC” button in white.
- Alternatively, click on the “Action” button, then select “Attach to VPC.”
- Choose your VPC from the list.
- Click on the “Attach Internet Gateway” button.

Following are the screenshot of the above steps for reference:



After clicking on the “Attach internet gateway” following screen will appear.



**Step 5:** Configure the Route table with Internet gateway and subnet.

- Go to “Route Tables.”
- Select your desired route table.
- Click on the “Routes” tab.
- Click “Edit Routes.”
- Click “Add Route.”
- Enter the destination IP address CIDR value (e.g., 0.0.0.0/0) to communicate with any IP address or use CIDR range 0.0.0.0/0 for internet access.
- Select the target as “Internet Gateway.”
- Click “Save Changes.”
- Click “Subnet associations”
- Click “Edit subnet associations”
- Click on subnet “check box”
- Click on “Save Associations”

Following are the screenshots of the above steps for your reference:

The screenshot shows the AWS VPC dashboard. On the left, there's a navigation menu with options like 'Virtual private cloud', 'Subnets', 'Route tables', 'Internet gateways', etc. The main area displays 'Route tables (1/3) info'. A table lists three route tables: 'my route table-public', a private route table, and 'my route table-private'. The 'my route table-public' is selected, and its details are shown below. It has one route with destination '10.0.0.0/16' and target 'local', which is 'Active'.

Name	Route table ID	Explicit subnet associ...	Edge associations	Main	VPC	Owner ID
my route table-public	rtb-04b3fd5f62bde94f2	-	-	No	vpc-0443a72887a5112eb   med...	100796962221
-	rtb-0f69b8c8598554bb1	-	-	Yes	vpc-0443a72887a5112eb   med...	100796962221
my route table-private	rtb-0f69b8c8598554bb1	-	-	No	vpc-0443a72887a5112eb   med...	100796962221

Below the table, the details for 'rtb-04b3fd5f62bde94f2 / my route table-public' are shown. It has one route with destination '10.0.0.0/16' and target 'local', which is 'Active'.

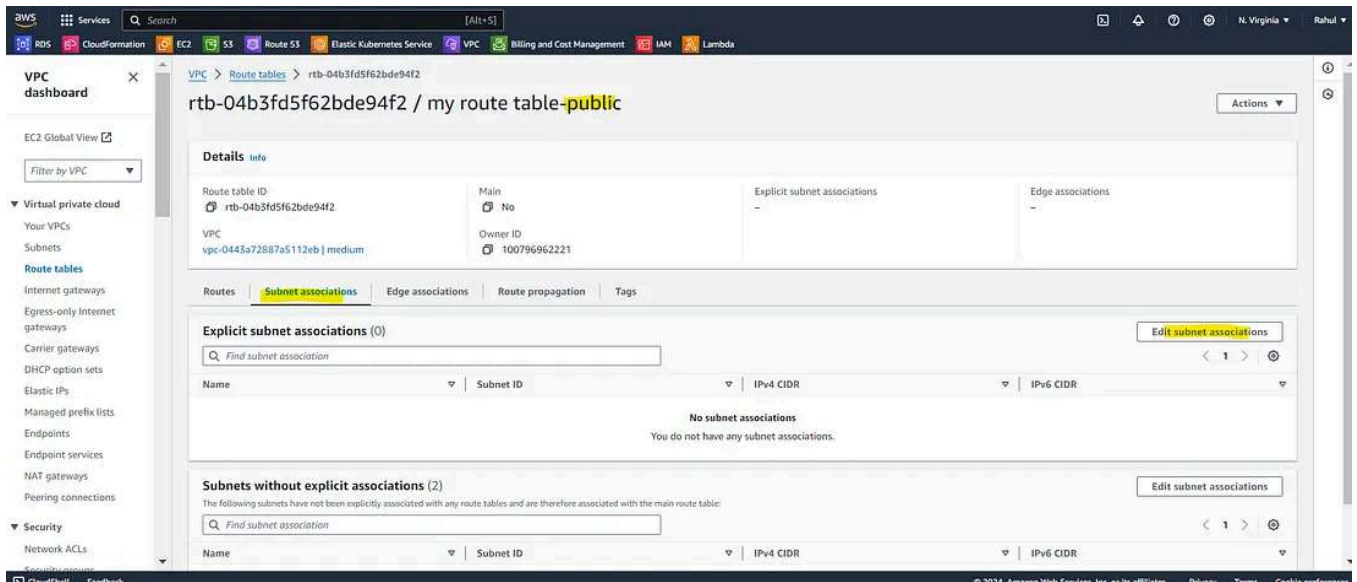
The screenshot shows the 'Edit routes' page for the selected route table. It displays a table with columns: Destination, Target, Status, and Propagated. There are two routes: one with destination '10.0.0.0/16' and target 'local' (Status: Active, Propagated: No), and another with destination '0.0.0.0/0' and target 'Internet Gateway' (Status: -, Propagated: No). There are buttons to 'Add route', 'Remove', 'Cancel', 'Preview', and 'Save changes'.

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No
0.0.0.0/0	Internet Gateway	-	No

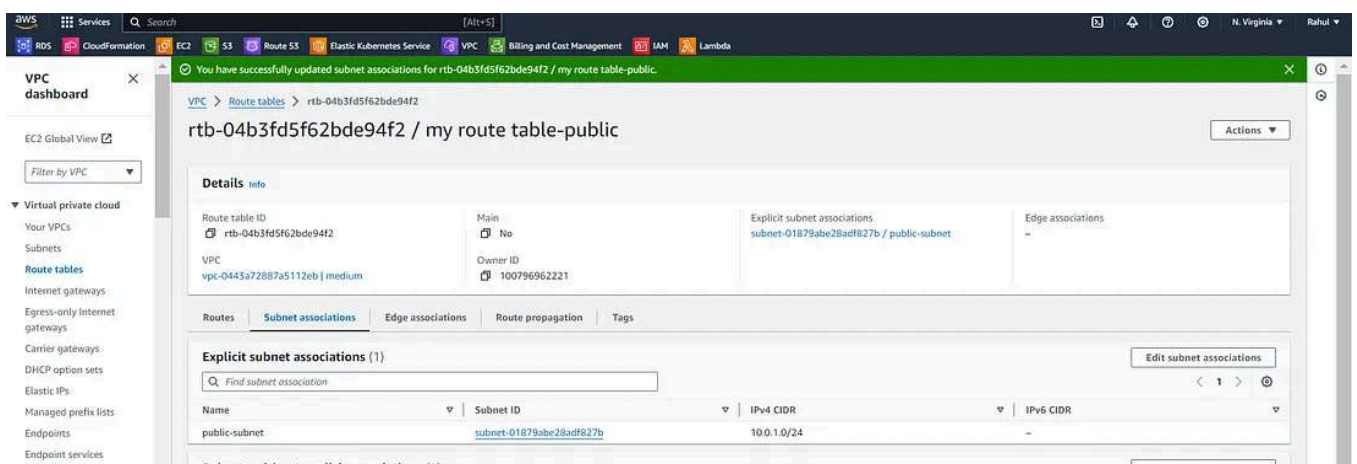
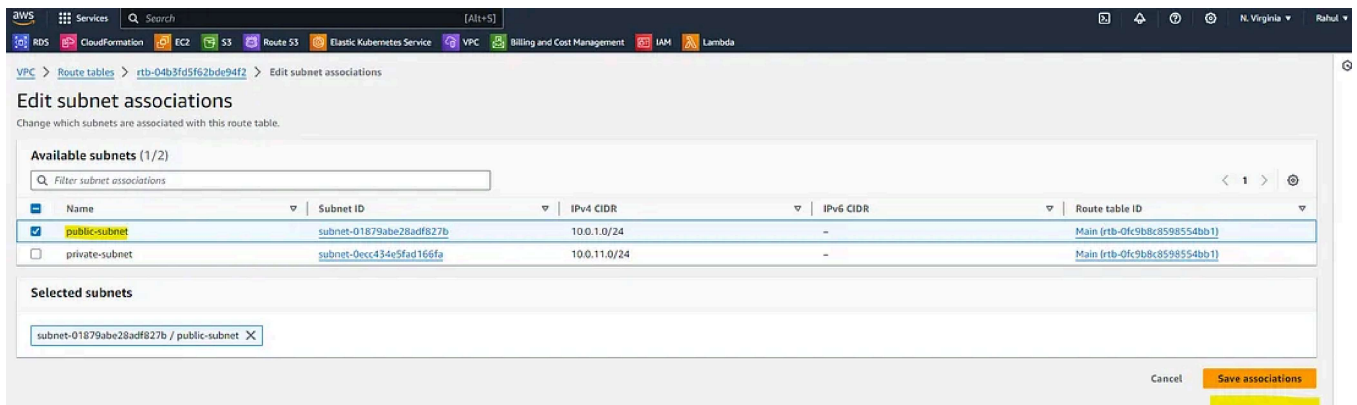
The screenshot shows the 'Details' page for the route table 'rtb-04b3fd5f62bde94f2 / my route table-public'. It displays a table with columns: Route table ID, Main, Explicit subnet associations, and Edge associations. The route table ID is 'rtb-04b3fd5f62bde94f2', the main is 'No', and the owner ID is '100796962221'. Below the table, the details for 'rtb-04b3fd5f62bde94f2 / my route table-public' are shown. It has two routes: one with destination '0.0.0.0/0' and target 'igw-0ee1c5baf3fe16915' (Status: Active, Propagated: No), and another with destination '10.0.0.0/16' and target 'local' (Status: Active, Propagated: No). There are buttons to 'Both', 'Edit routes', 'Cancel', 'Preview', and 'Save changes'.

Route table ID	Main	Explicit subnet associations	Edge associations
rtb-04b3fd5f62bde94f2	No	-	-

Below the table, the details for 'rtb-04b3fd5f62bde94f2 / my route table-public' are shown. It has two routes: one with destination '0.0.0.0/0' and target 'igw-0ee1c5baf3fe16915' (Status: Active, Propagated: No), and another with destination '10.0.0.0/16' and target 'local' (Status: Active, Propagated: No).



Now select a public subnet that has a direct route to the internet, allowing resources in that subnet to access the public internet.



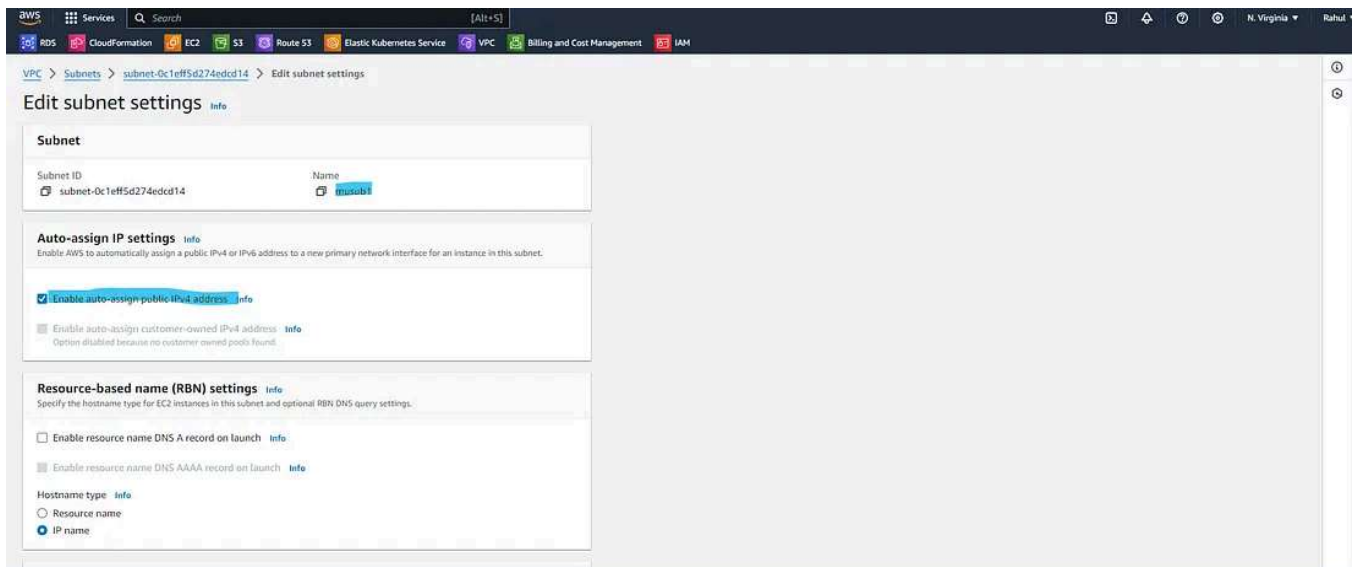
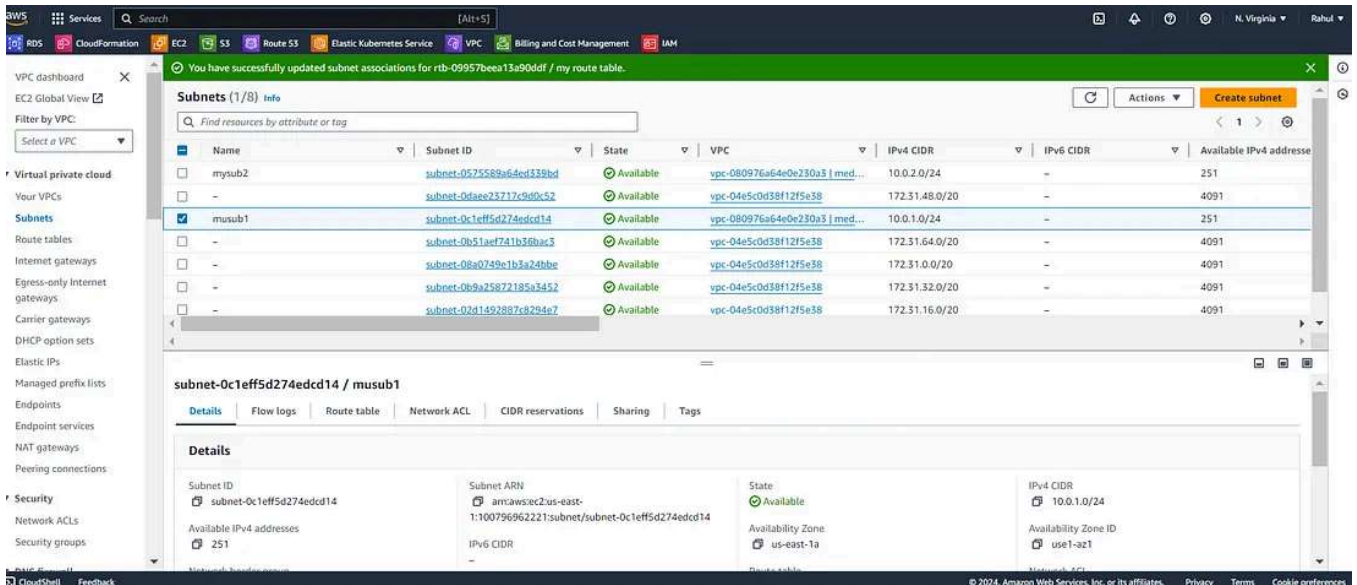
## Steps 6: Enable Public IP Configuration for Subnet

- Click on “Subnets” in the left-side window.
- Select your desired subnet.

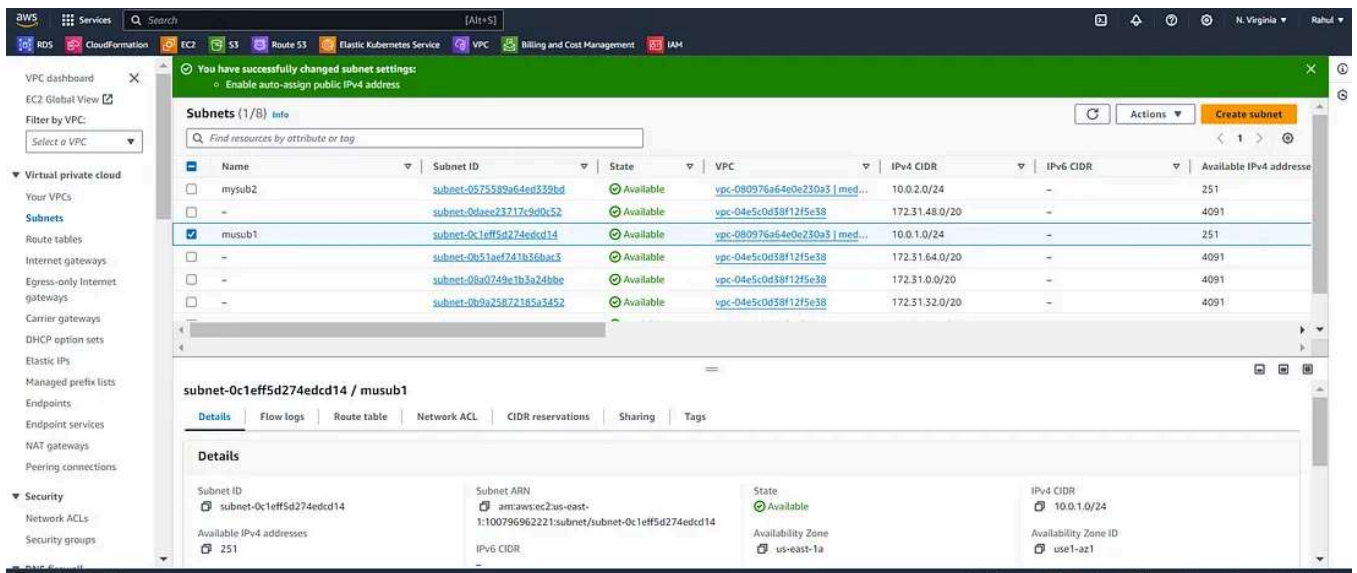


- Click on “Actions.”
- Choose “Edit Subnet Settings.”
- Check the box for “Enable auto assign public IPv4 address.”
- Click “Save.”

Following are the screenshots of the above steps for the reference:



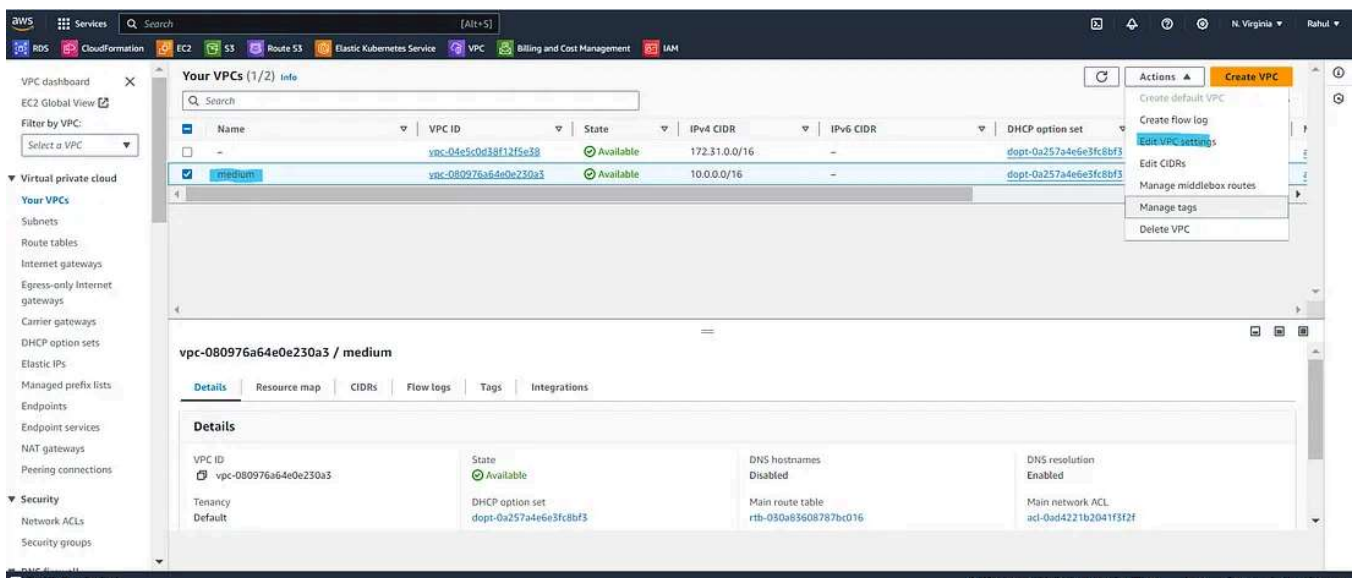


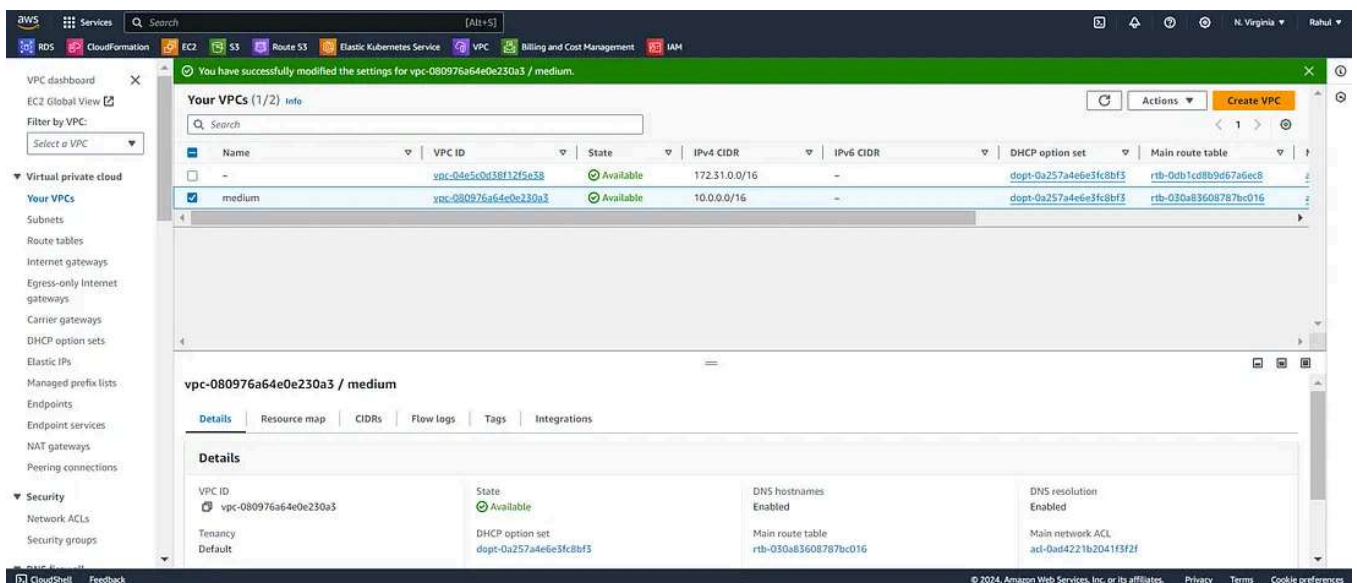
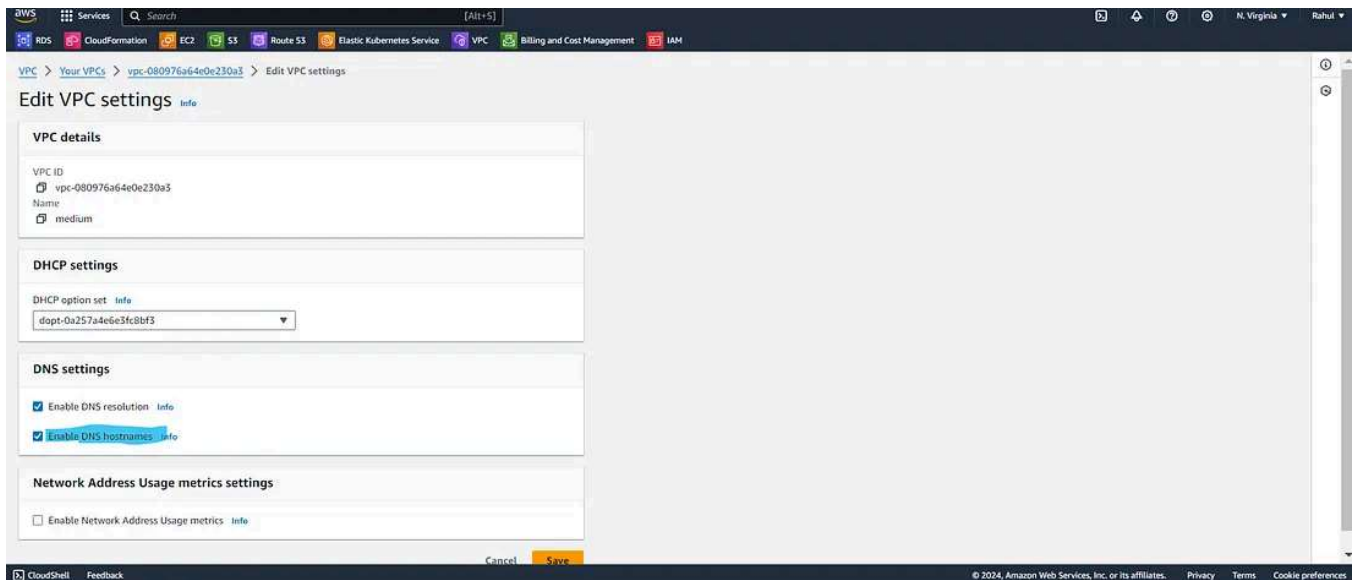


## Step 7: Enable DNS Hostname Resolution for VPC

- Click on “Your VPC.”
- Select your VPC.
- Click on “Actions.”
- Choose “Edit VPC Settings.”
- Check the box for “Enable DNS hostnames.”
- Click “Save.”

Following are the screenshot of above steps for reference:

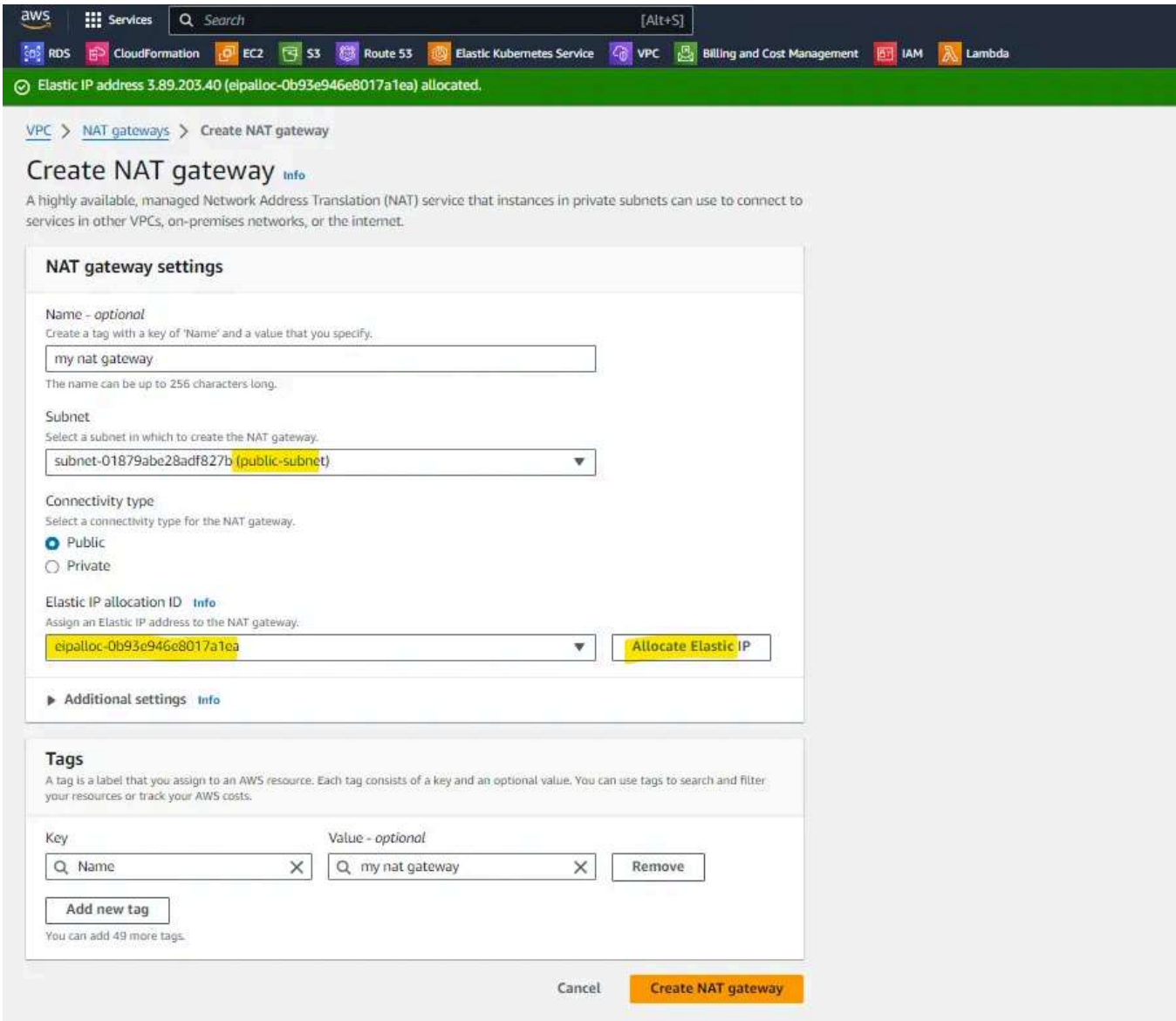
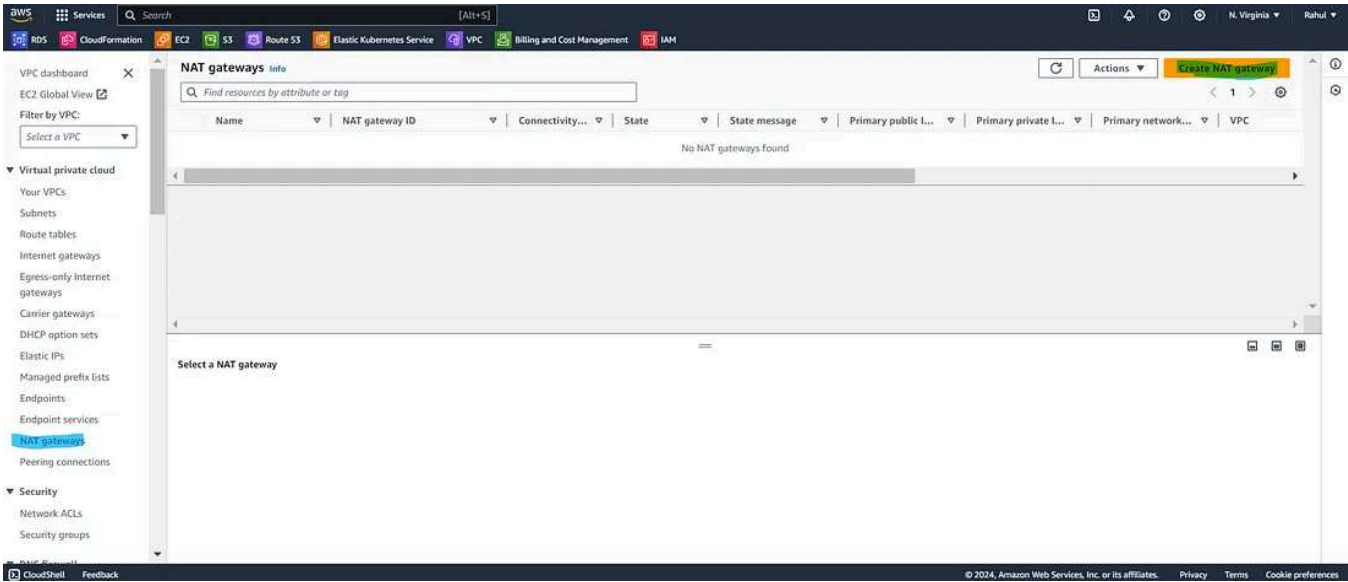


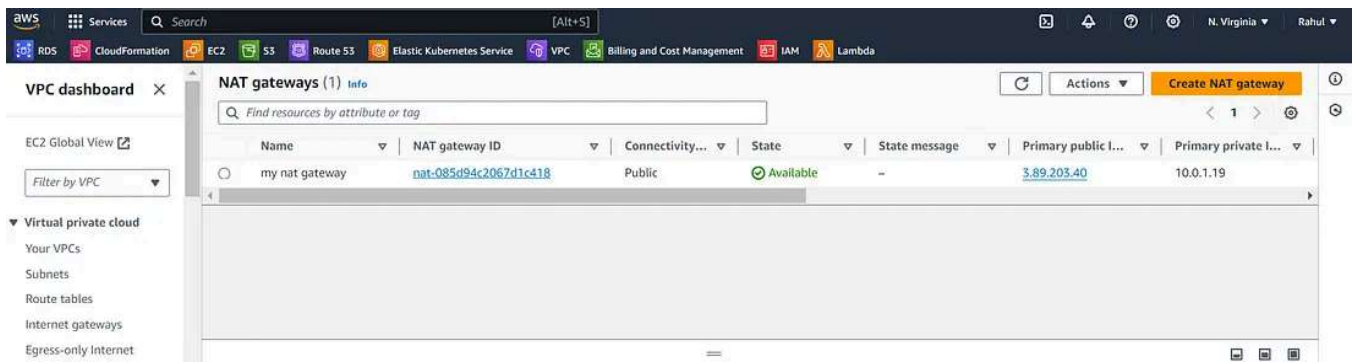


## Step 8:

- Click on “NAT Gateway”
- Click the orange “Create NAT Gateway” button.
- Provide a name for the NAT Gateway.
- Click on the “Create NAT Gateway” button.
- Make sure you select the Public Subnet.

For reference following are the screenshot of the steps:

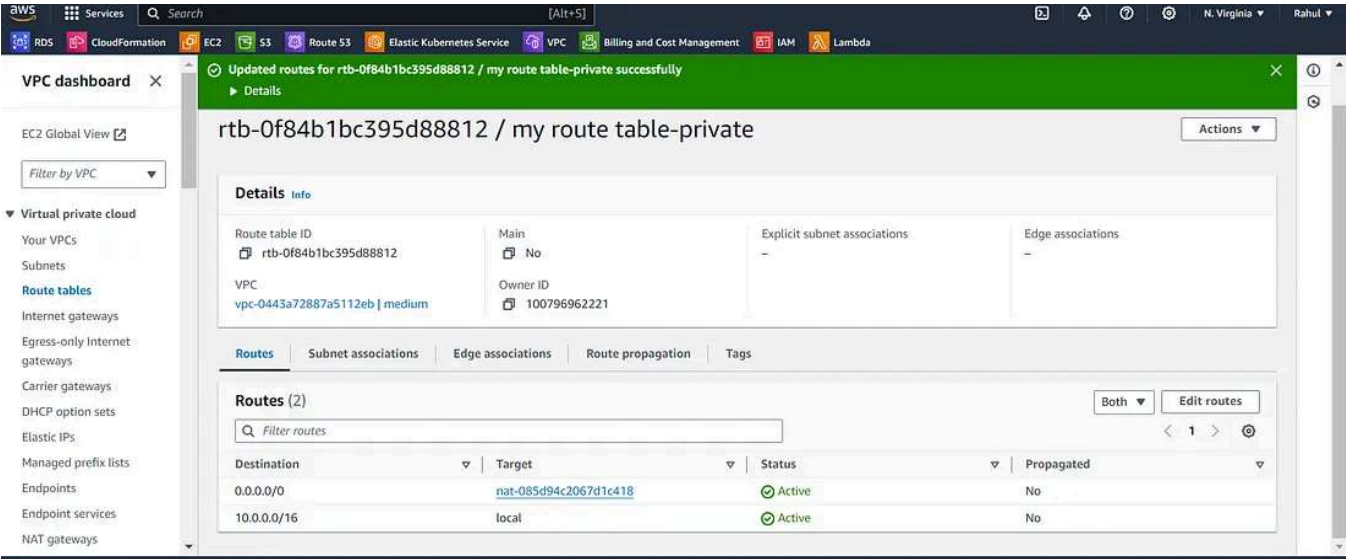
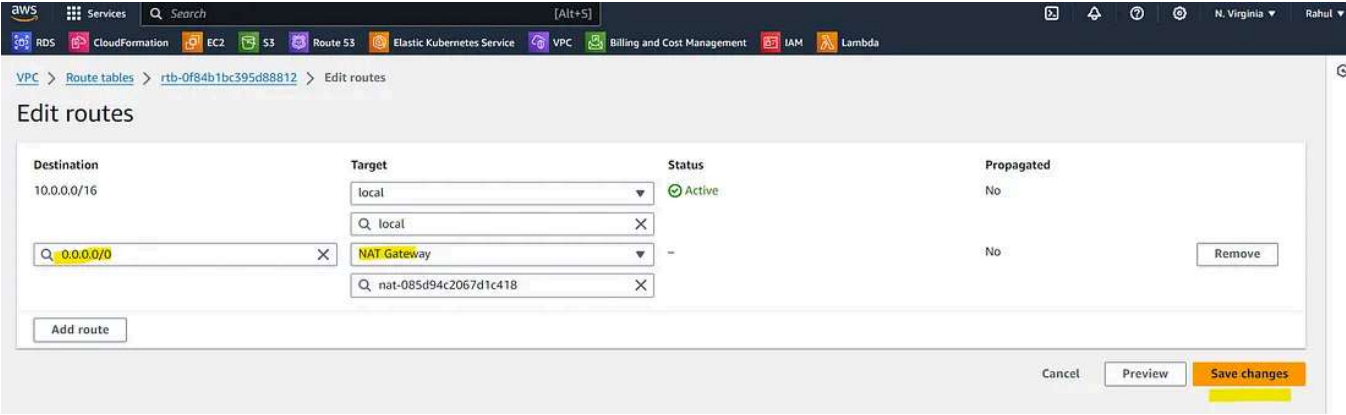
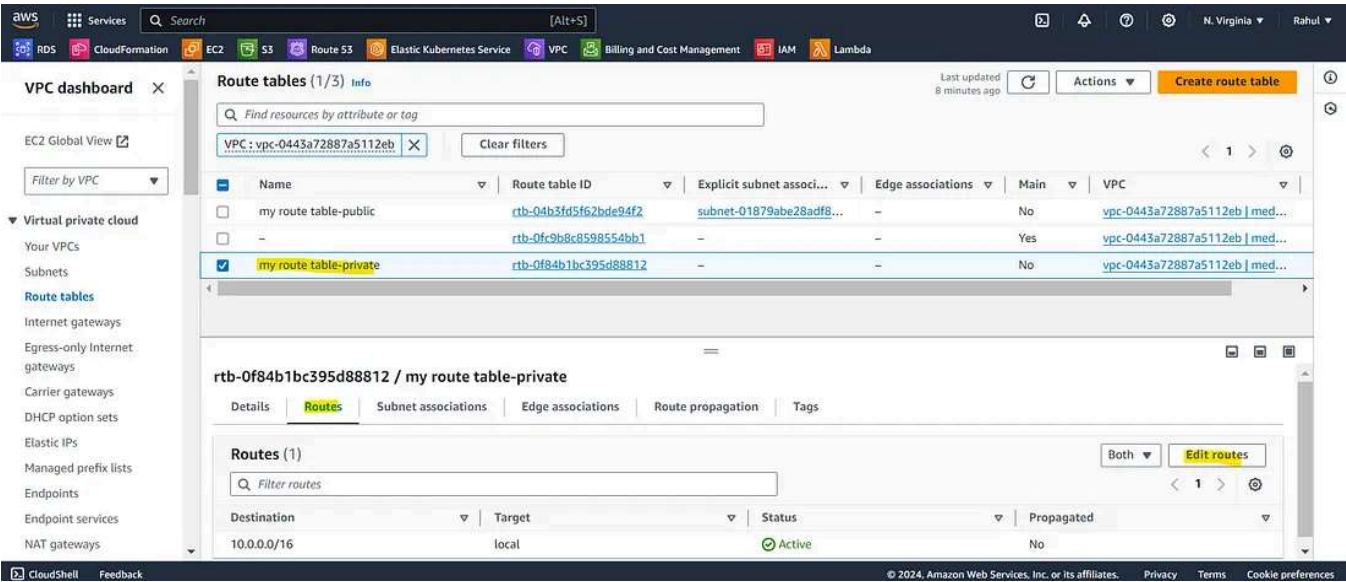




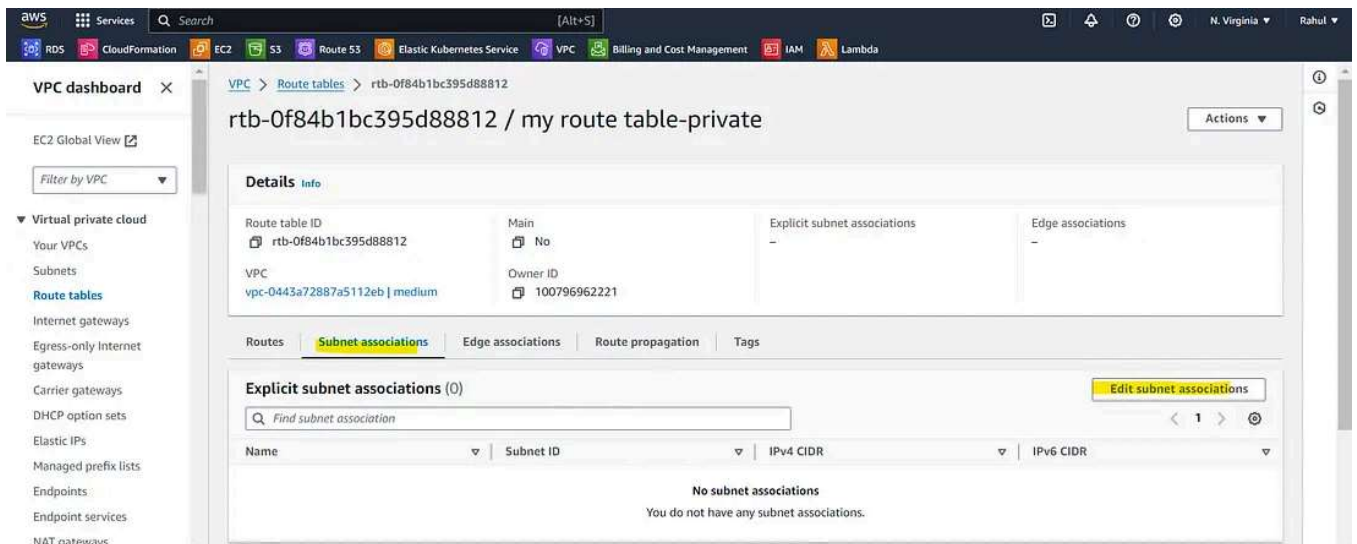
**Step 9: Configure the Route table with NAT Gate way and subnet.**

- Go to “Route Tables.”
- Select your desired route table.
- Click on the “Routes” tab.
- Click “Edit Routes.”
- Click “Add Route.”
- Select the target as “NAT Gateway.”
- Click “Save Changes.”
- Click “ Subnet associations”
- Click “Edit subnet associations”
- Click on subnet “check box”
- Click on “Save Associations”

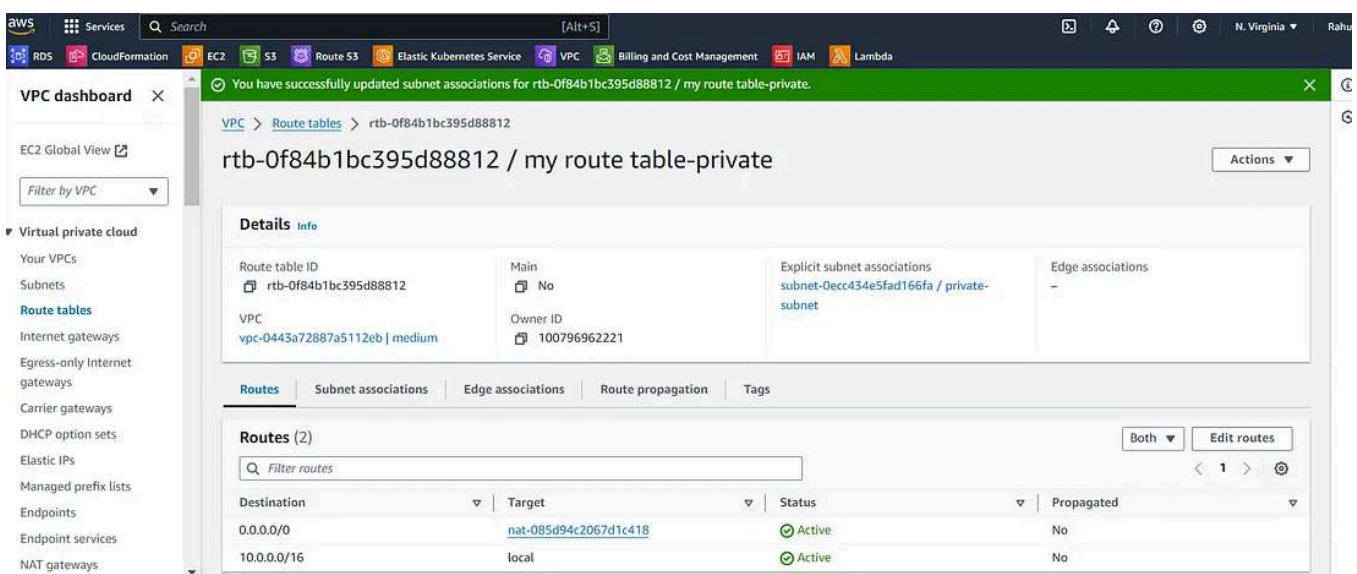
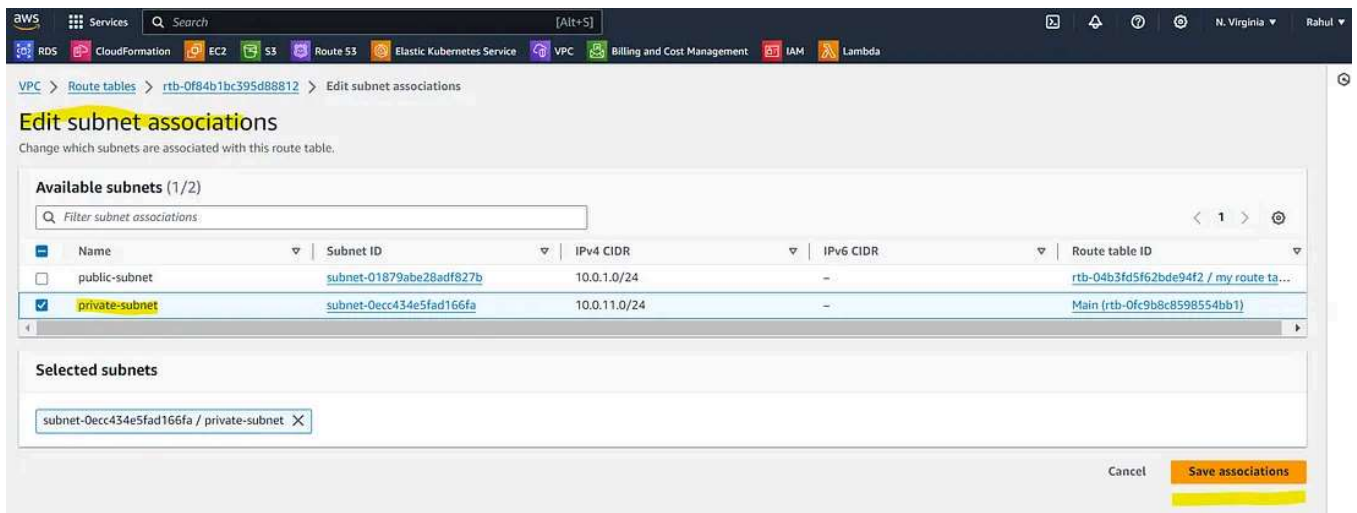
**Following are the screenshots of the above steps for your reference:**







Now select the private subnet and please see the screenshot as below.



By following these steps, you'll have successfully created a secure and tailored Virtual Private Cloud (VPC) in AWS, providing a robust foundation for your cloud-based applications and services.