

## 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

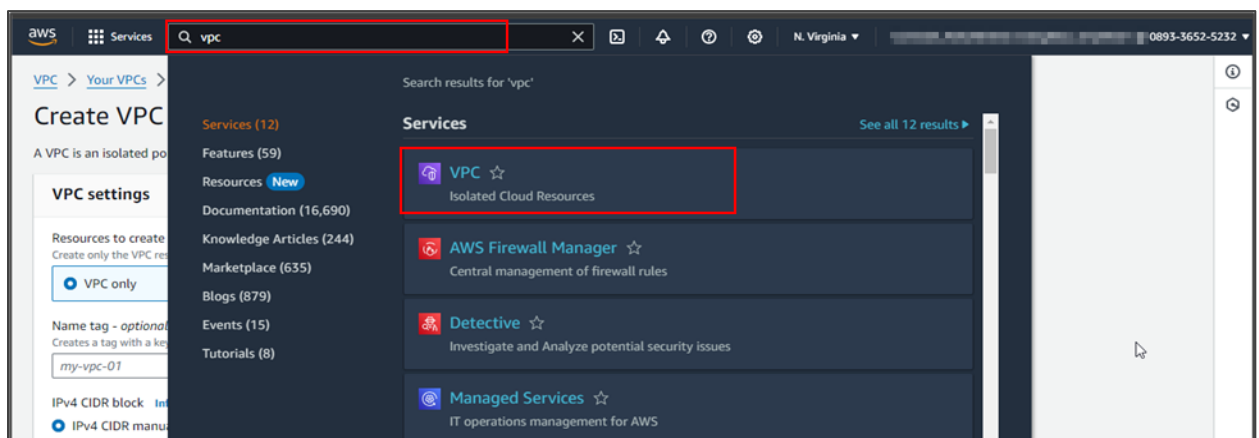
**Prerequisites:** None

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**

aws Services vpc

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.

**IPv4 CIDR block** [Info](#)

☒ IPv4 CIDR manual input  
☐ IPAM-allocated IPv4 CIDR block

**IPv4 CIDR**

CloudShell Feedback

© 2024, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

aws Services vpc

N. Virginia Corestack\_Role/darshan.mangaldas\_simplilearn @ 0893-3652-5232

**IPv4 CIDR**

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](#)

### 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.

No tags associated with the resource

You can add 50 more tags

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

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](#)

Default

**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.

No tags associated with the resource

[Add tag](#)  
You can add 50 more tags

[Cancel](#) [Create VPC](#)

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

**VPC dashboard** [x](#)

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](#)
- [Endpoints](#)

**You successfully created vpc-04c11fe17f74060d4** [x](#) [🔍](#)

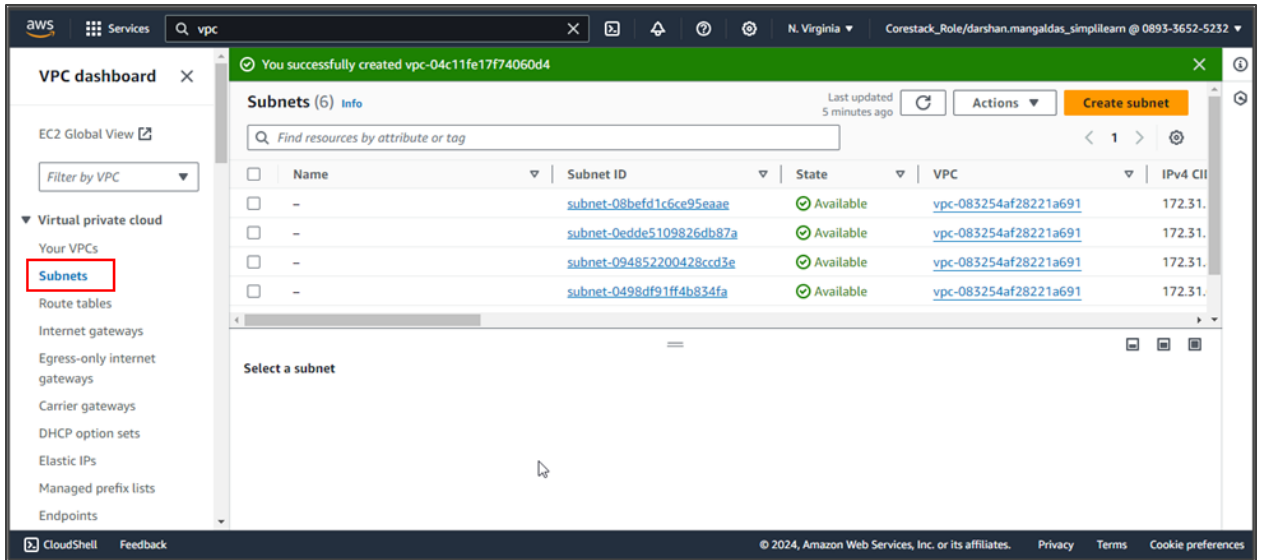
[VPC](#) > [Your VPCs](#) > vpc-04c11fe17f74060d4

**vpc-04c11fe17f74060d4** [Actions](#) [▼](#)

**Details** [Info](#)

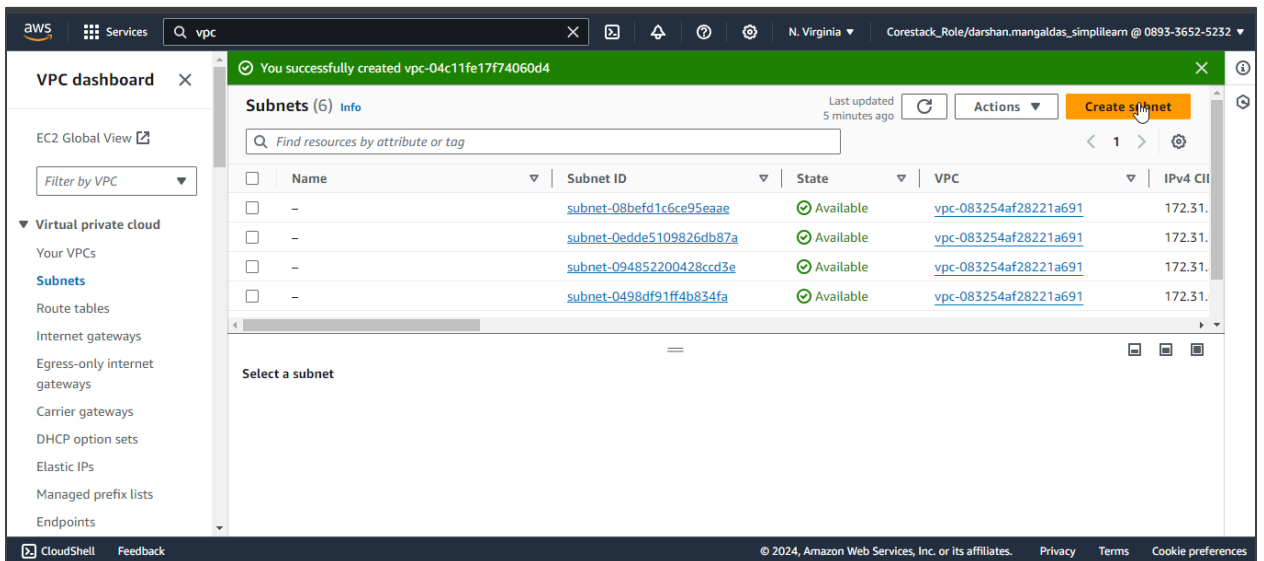
VPC ID <a href="#">vpc-04c11fe17f74060d4</a>	State <a href="#">🟢 Available</a>	DNS hostnames Disabled	DNS resolution Enabled
Tenancy Default	DHCP option set <a href="#">dopt-2b84eb51</a>	Main route table <a href="#">rtb-08938d78815fd65b5</a>	Main network ACL <a href="#">acl-0bc34c6807a3542fb</a>
Default 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 <a href="#">089336525232</a>	

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



## 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:

The screenshot shows the AWS Management Console interface for creating a subnet. The breadcrumb navigation indicates the path: VPC > Subnets > Create subnet. The main heading is 'Create subnet' with an 'Info' link. Below this, there are two main sections: 'VPC' and 'Subnet settings'. In the 'VPC' section, the 'VPC ID' is set to 'vpc-04c11fe17f74060d4'. Below it, the 'Associated VPC CIDRs' section shows 'IPv4 CIDRs' as '10.0.0.0/16'. The 'Subnet settings' section is partially visible, showing the instruction to 'Specify the CIDR blocks and Availability Zone for the subnet.'

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 screenshot shows the 'Subnet 1 of 1' configuration page. The 'Subnet name' field is set to 'private-subnet-1'. The 'Availability Zone' is set to 'US East (N. Virginia) / us-east-1a'. The 'IPv4 VPC CIDR block' is set to '10.0.0.0/16'. The 'IPv4 subnet CIDR block' is set to '10.0.0.0/20'. The 'Tags' section is expanded, showing a table with 'Key' and 'Value - optional' columns. The 'Subnet name' field is highlighted with a red box, and the 'Availability Zone' and 'IPv4 VPC CIDR block' fields are also highlighted with red boxes.

aws Services  N. Virginia Corestack\_Role/darshan.mangaldas\_simplilearn @ 0893-3652-5232

### Subnet 1 of 1

**Subnet name**  
Create a tag with a key of 'Name' and a value that you specify.  
  
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.

**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.

**IPv4 subnet CIDR block**  
 256 IPs

▼ **Tags - optional**

Key	Value - optional
<input type="text"/>	<input type="text"/>

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

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

aws Services  N. Virginia Corestack\_Role/darshan.mangaldas\_simplilearn @ 0893-3652-5232

**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
- Endpoints

**Subnets (1) Info** [Info](#) Last updated 1 minute ago

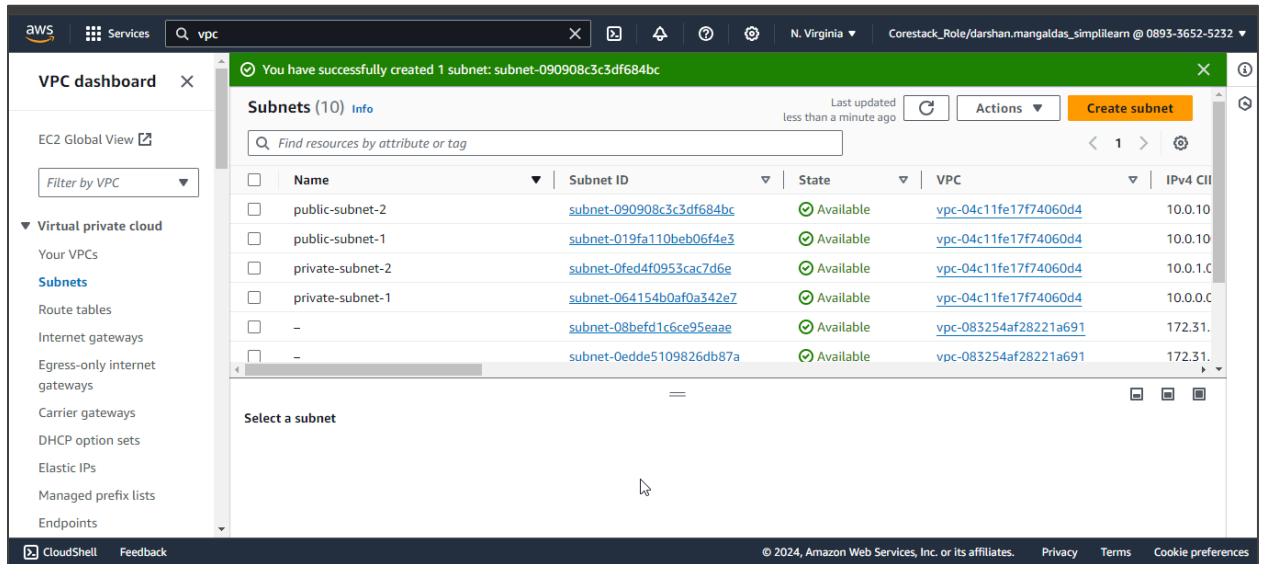
< 1 >

<input type="checkbox"/>	Name	Subnet ID	State	VPC	IPv4 CIDR
<input type="checkbox"/>	private-subnet-1	<a href="#">subnet-064154b0af0a342e7</a>	Available	<a href="#">vpc-04c11fe17f74060d4</a>	10.0.0.0/24

Select a subnet

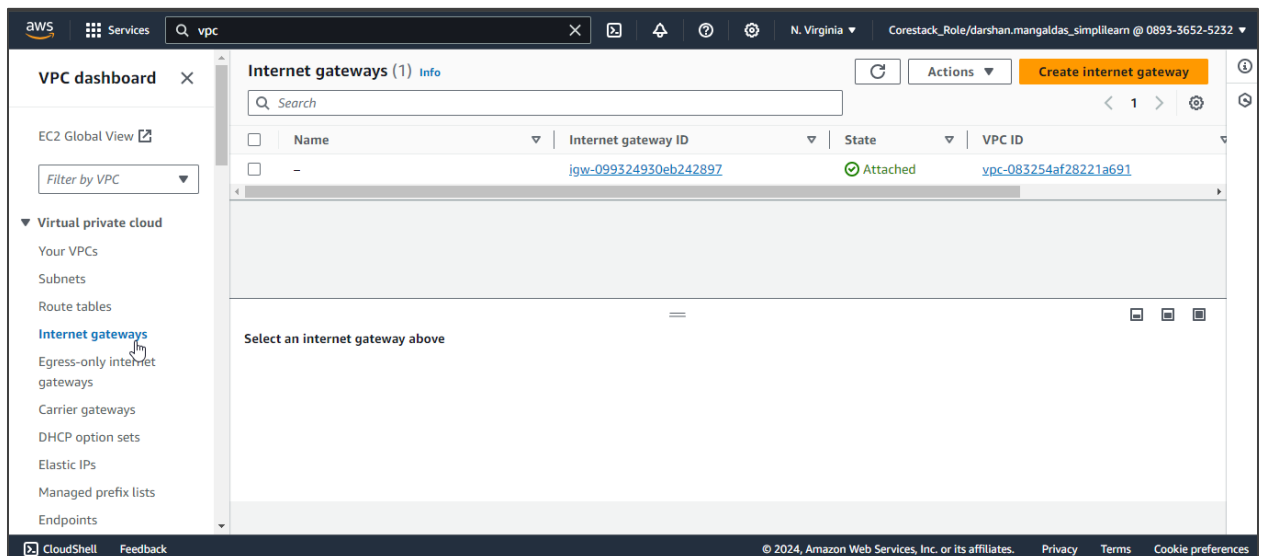
CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

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

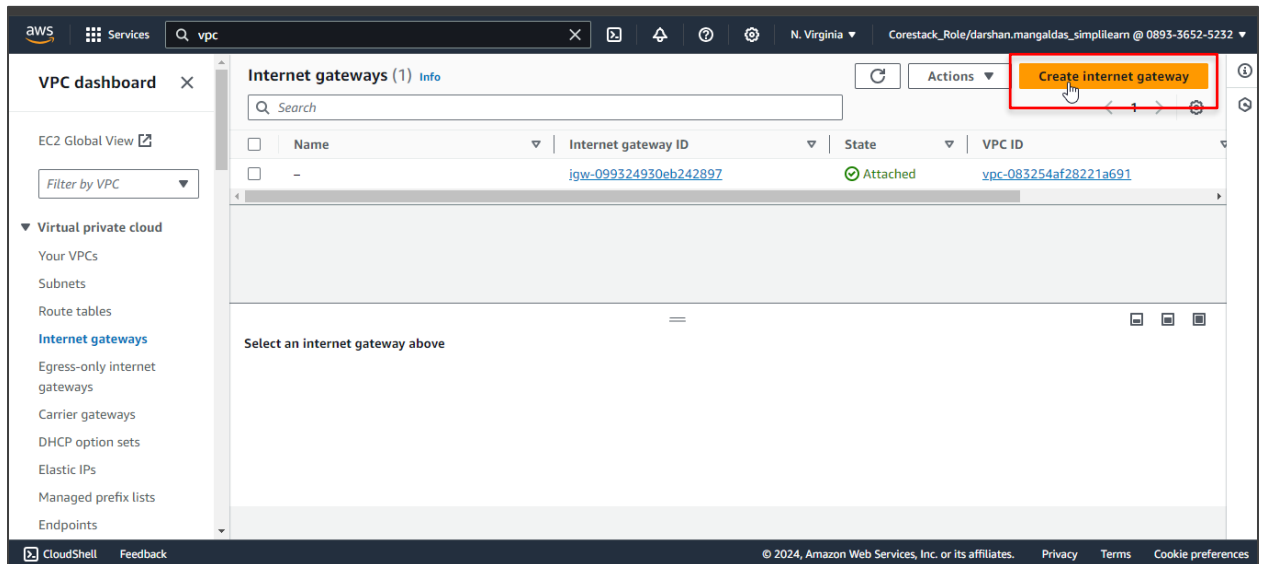


## Step 3: Deploy an internet gateway and attach it to the VPC

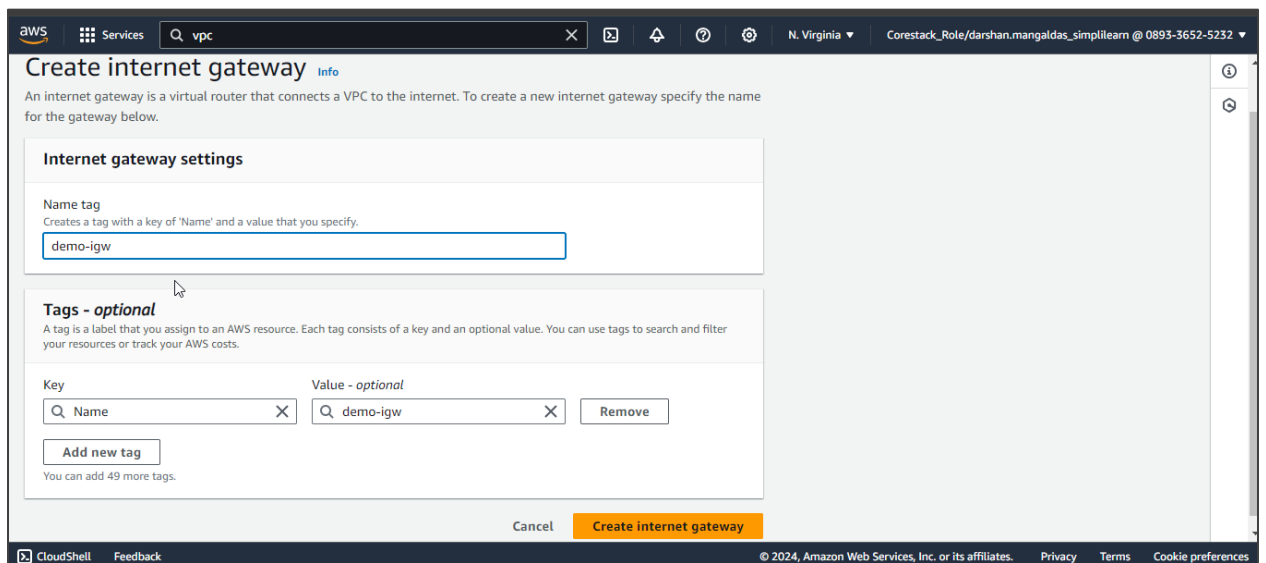
### 3.1 Click on the **Internet gateways** option on the VPC dashboard



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:

**Create internet gateway** Info

An internet gateway is a virtual router that connects a VPC to the internet. To create a new internet gateway specify the name for the gateway below.

**Internet gateway settings**

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

demo-igw

**Tags - optional**  
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: Name Value - optional: demo-igw

Remove

Add new tag

You can add 49 more tags.

Cancel **Create internet gateway**

The internet gateway is successfully created.

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

**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
- Endpoints

**igw-0295cdb7ec09ac262 / demo-igw**

**Details** Info

Internet gateway ID	State	VPC ID	Owner
igw-0295cdb7ec09ac262	Detached	-	089334

**Tags**

Search tags

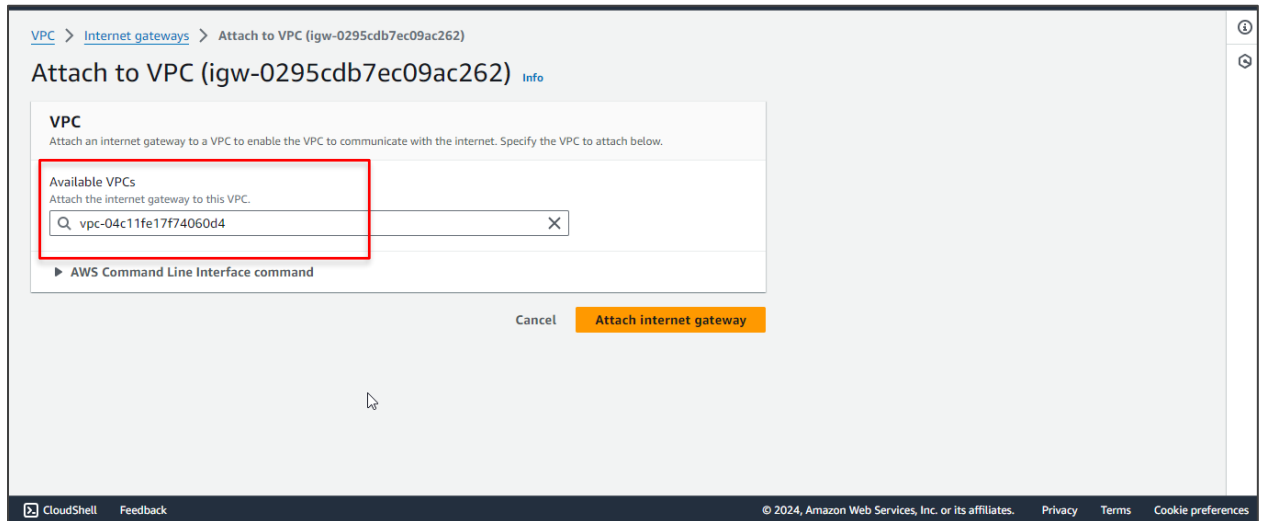
Key	Value
Name	demo-igw

Manage tags

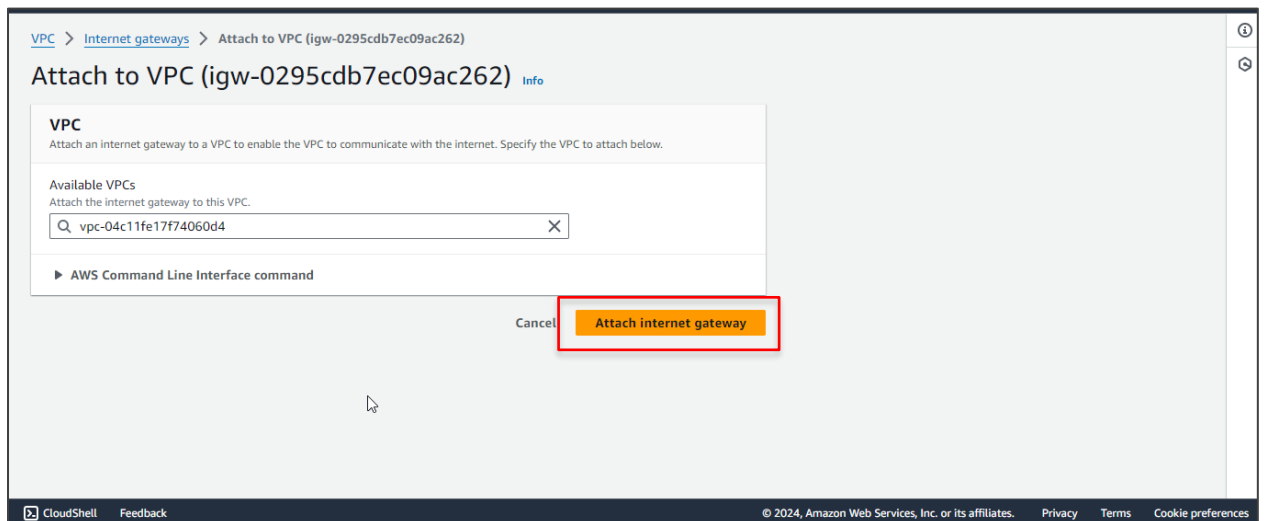
Actions ▲

- Attach to VPC**
- Detach from VPC
- Manage tags
- Delete

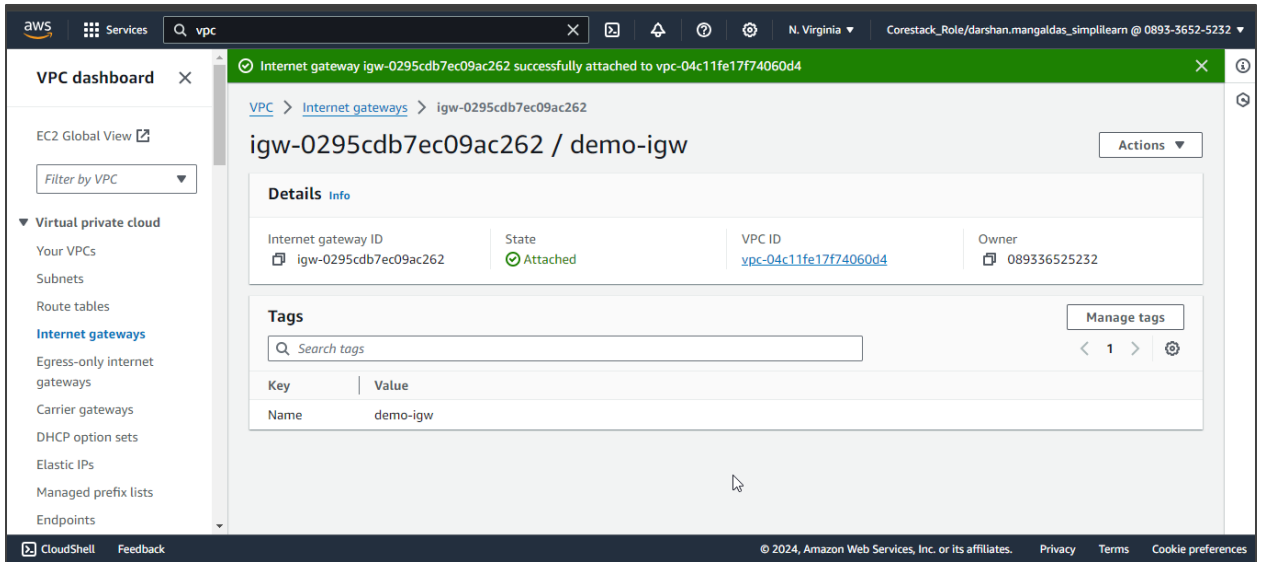
3.6 Select the created VPC from the drop-down list in the **Available VPCs** field as shown below:



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

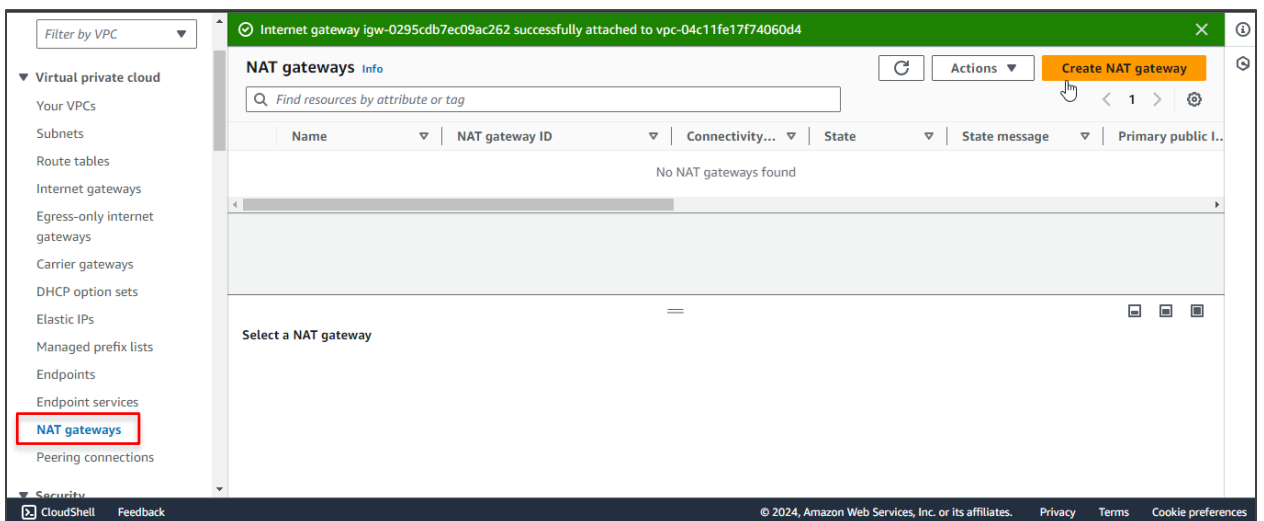


The internet gateway will be created as shown below:

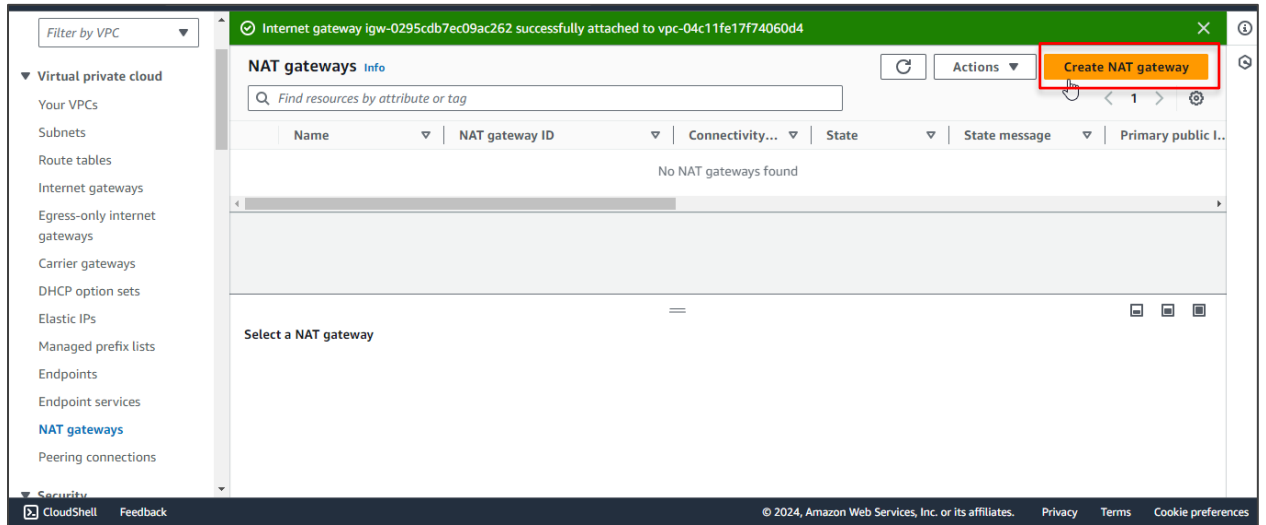


## Step 4: Provision a NAT gateway for outbound connectivity

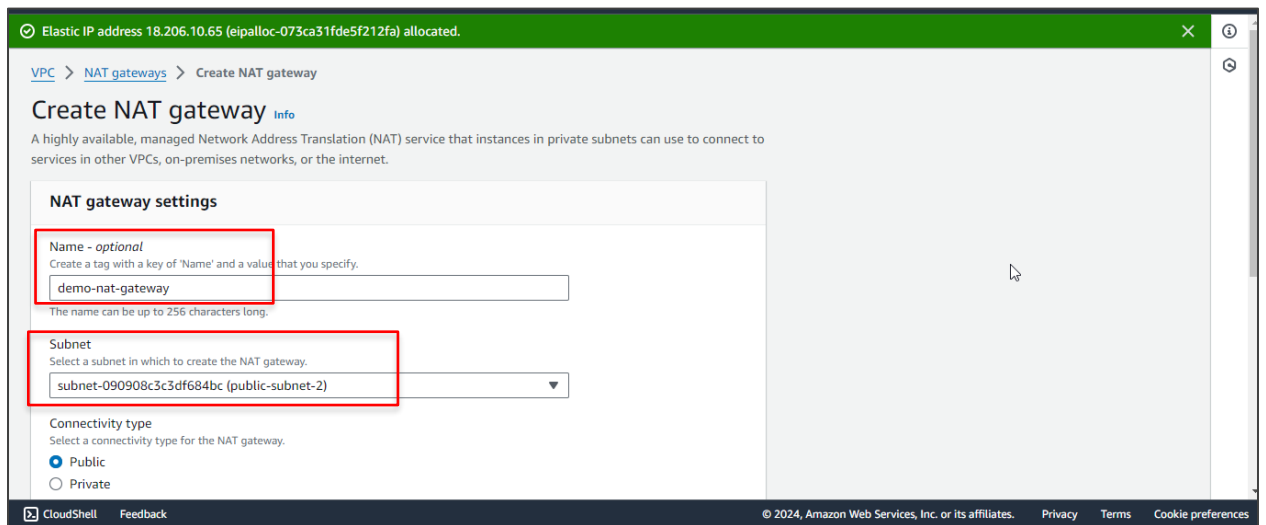
### 4.1 Click on the **NAT gateways** option in the VPC dashboard



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

Elastic IP address 18.206.10.65 (eipalloc-073ca31fde5f212fa) allocated.

☒ Public  
☐ Private

Elastic IP allocation ID [Info](#)  
Assign an Elastic IP address to the NAT gateway.  
eipalloc-073ca31fde5f212fa [Allocate Elastic IP](#)

► Additional settings [Info](#)

**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  
Name demo-nat-gateway Remove  
Add new tag  
You can add 49 more tags.

Cancel **Create NAT gateway**

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

The NAT gateway will be created as shown below:

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  
Endpoints

NAT gateway nat-0d7e5a09eab89551c | demo-nat-gateway was created successfully.

VPC > NAT gateways > nat-0d7e5a09eab89551c

nat-0d7e5a09eab89551c / demo-nat-gateway [Actions](#)

**Details**

NAT gateway ID nat-0d7e5a09eab89551c	Connectivity type Public	State Pending	State message <a href="#">Info</a> -
NAT gateway ARN arn:aws:ec2:us-east-1:089336525232:natgateway/nat-0d7e5a09eab89551c	Primary public IPv4 address -	Primary private IPv4 address -	Primary network interface ID -
VPC vpc-04c11fe17f74060d4	Subnet subnet-090908c3c3df684bc / public-subnet-2	Created Monday, June 24, 2024 at 17:25:41 GMT+5:30	Deleted -

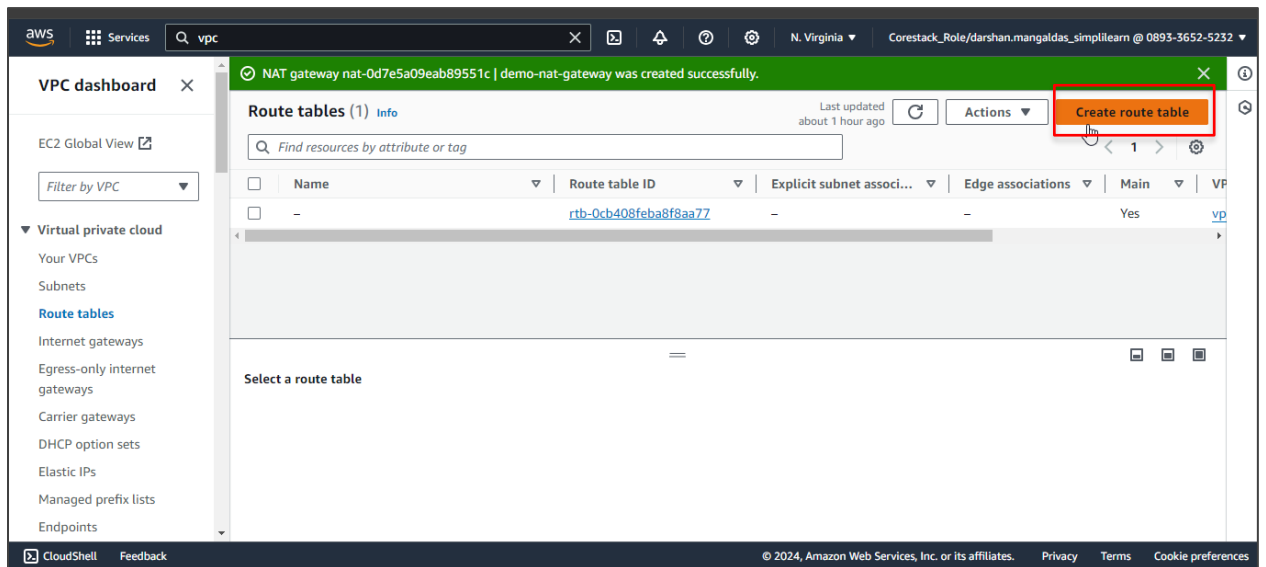
[Secondary IPv4 addresses](#) Monitoring Tags

Secondary IPv4 addresses [Edit secondary IPv4 address associations](#)

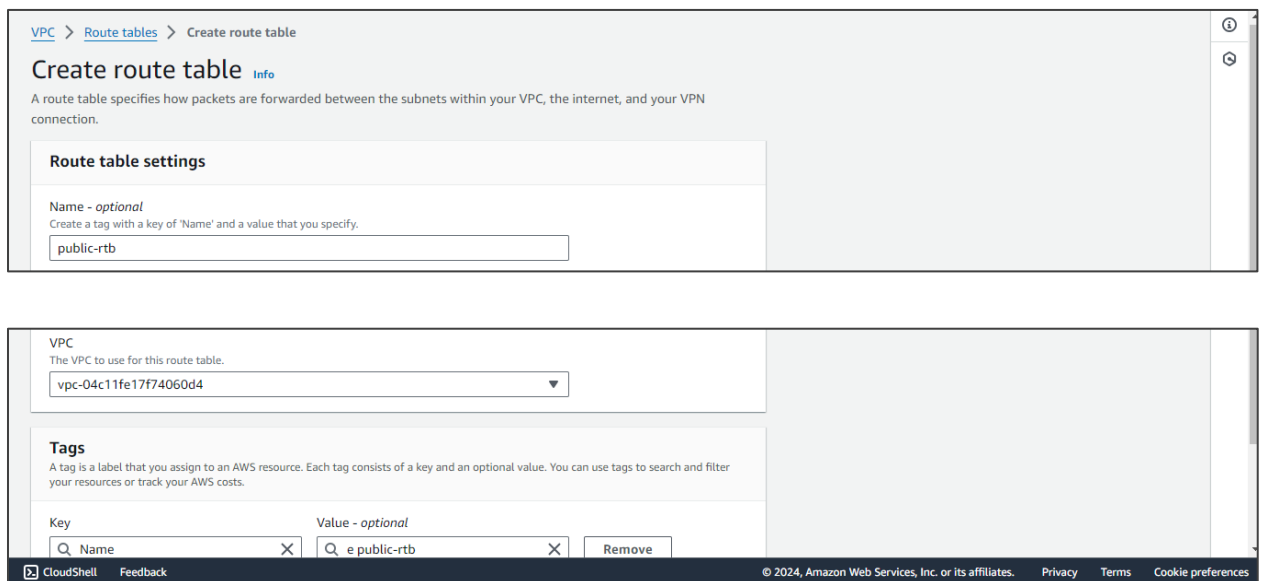
CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

## 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

**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:

You can add 49 more tags.

**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

**Route tables (1/4)** Info

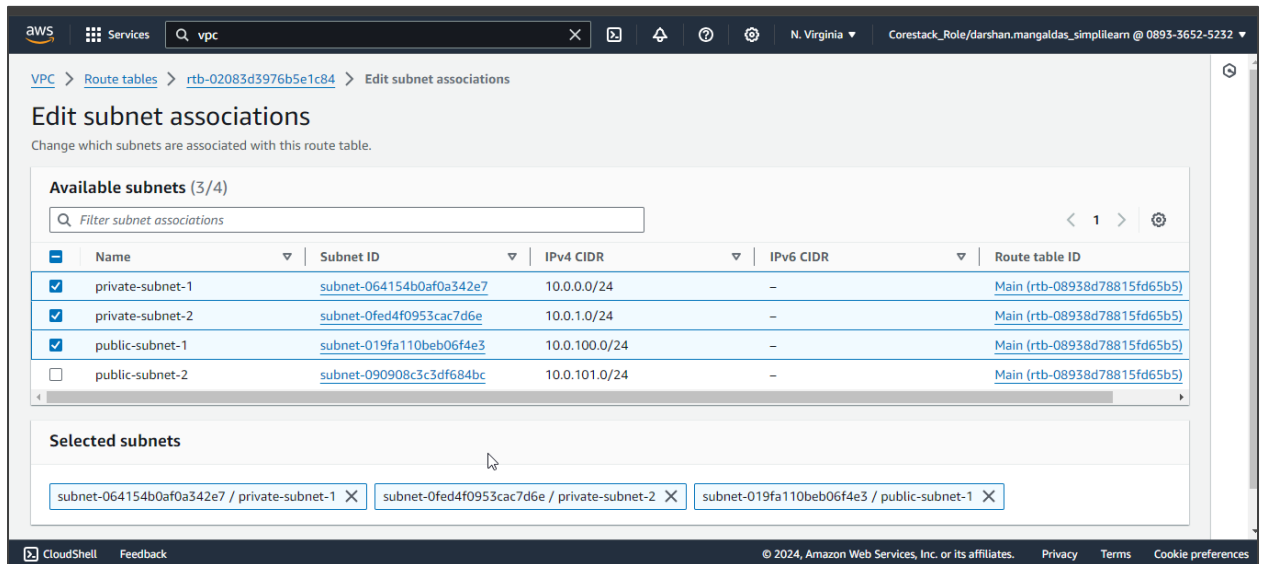
Name	Route table ID	Explicit subnet associ...	Edge associations	Main	VP
-	rtb-0cb408feba8f8aa77	-	-	Yes	vp
-	rtb-08938d78815fd65b5	-	-	Yes	vp
e public-rtb	rtb-00c8dd4df00429d5d	-	-	No	vp
private-rtb.	rtb-02083d3976b5e1c84	-	-	No	vp

**rtb-02083d3976b5e1c84 / private-rtb.**

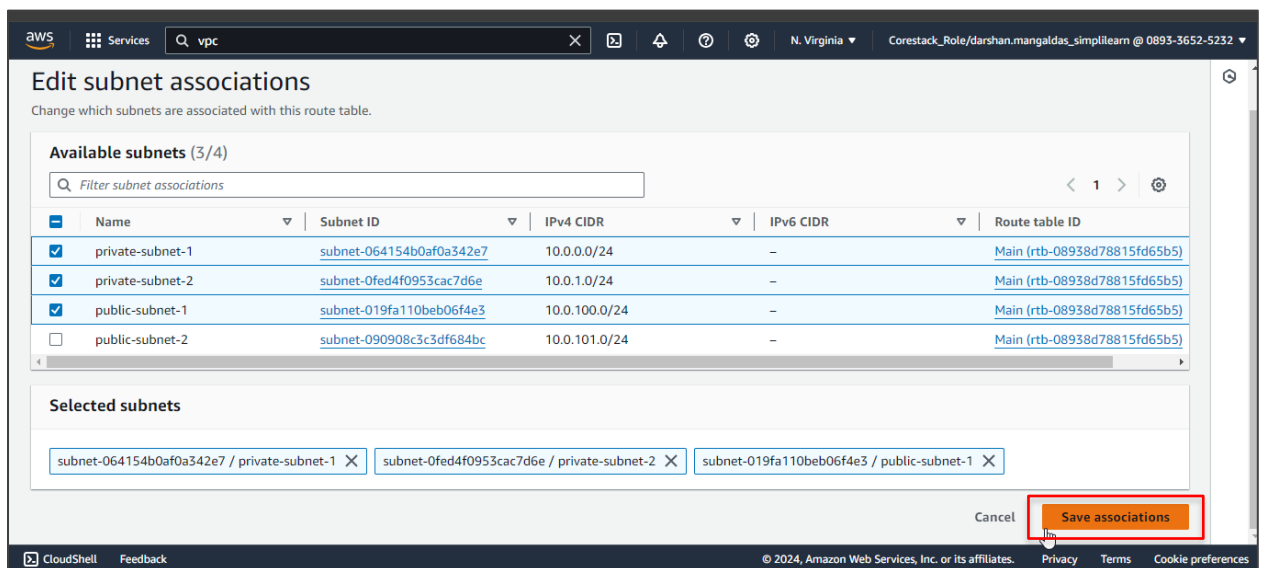
Details | Routes | **Subnet associations** | Edge associations | Route propagation | Tags

**Explicit subnet associations (0)**

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

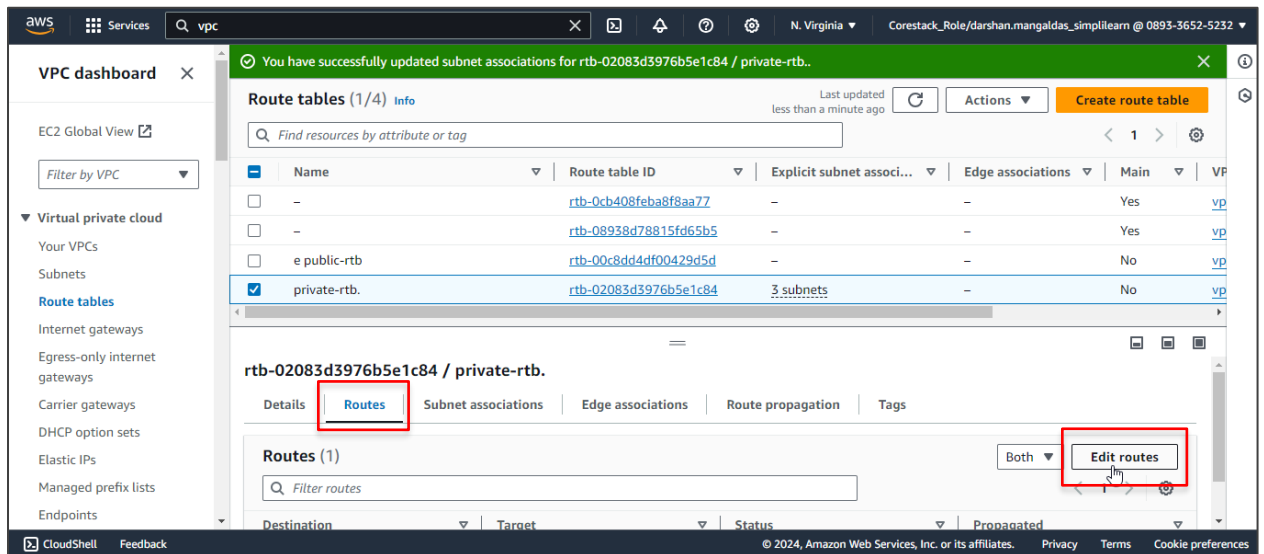


5.6 Once you have selected the three subnets, click on the **Save associations** button to save your configuration

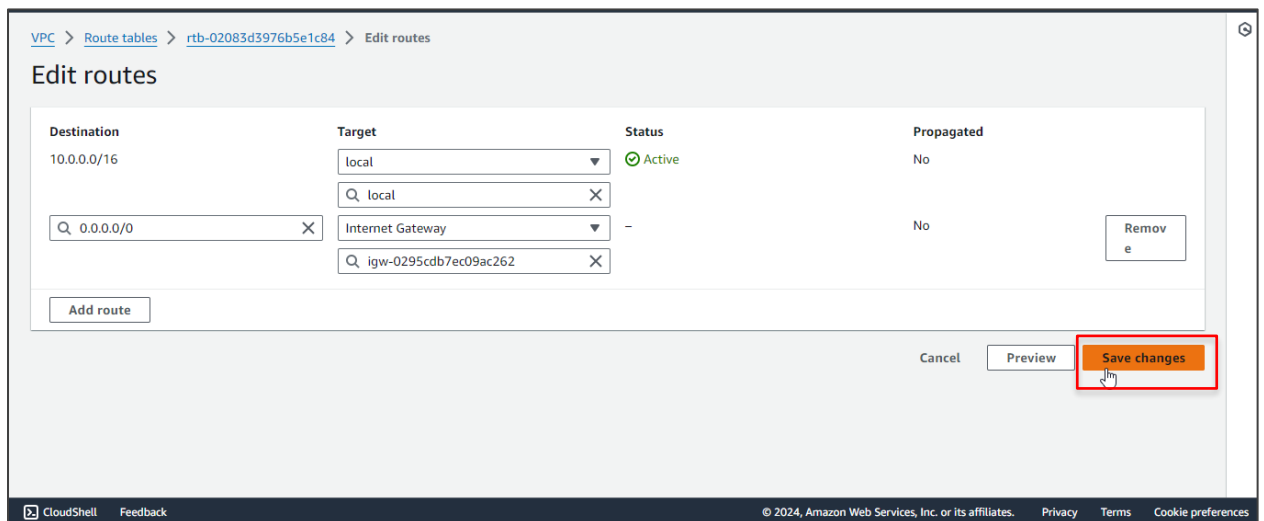




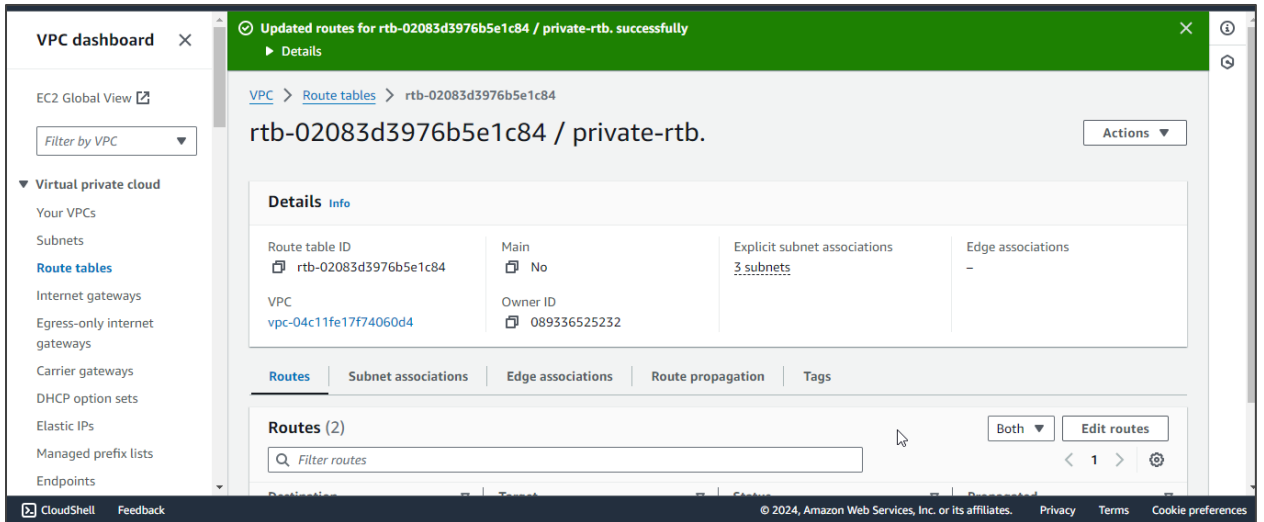
5.7 In the Route tables console, select the **public-rtb** route table, click on **Routes**, and then select **Edit Routes** to add routes for proper network traffic routing



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**



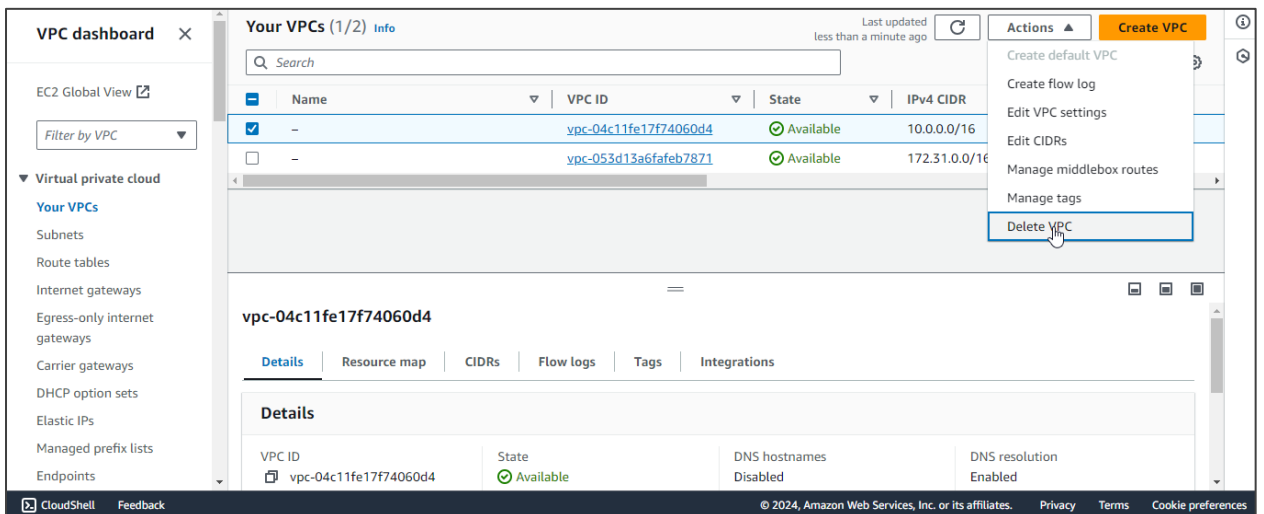
**Note:** Repeat this step to add a route to the **private-rtb**. The Destination should be 0.0.0.0/0. Select **NAT Gateway** and choose the gateway created in Step 4 as the **Target**. Finally, click **Save changes** to save the new route configuration.



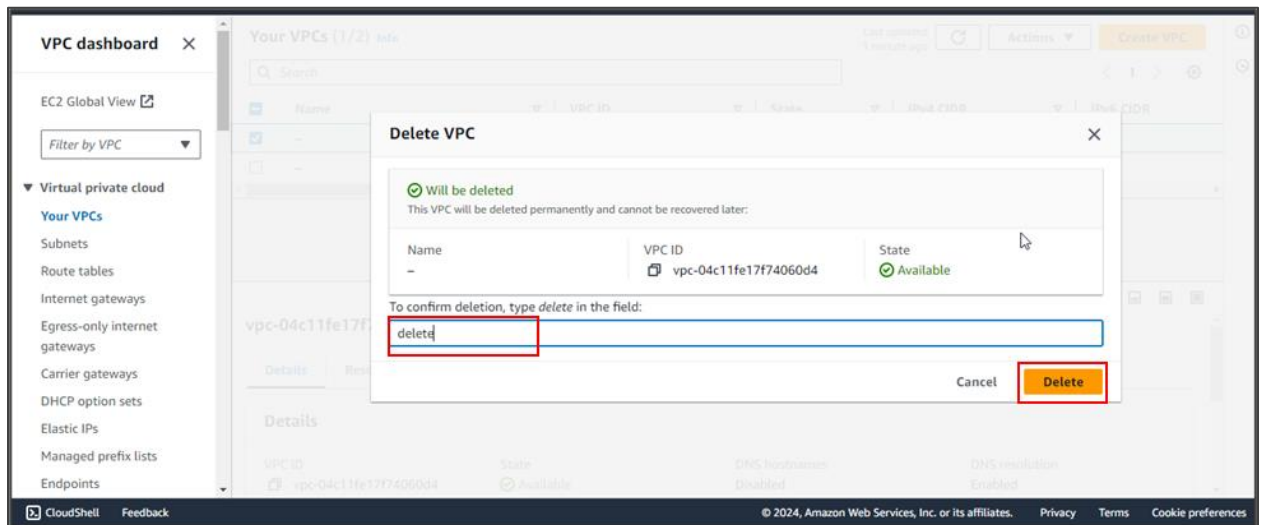
The traffic route for the **private-rtb** route table has also been added.

## Step 6: Delete the VPC

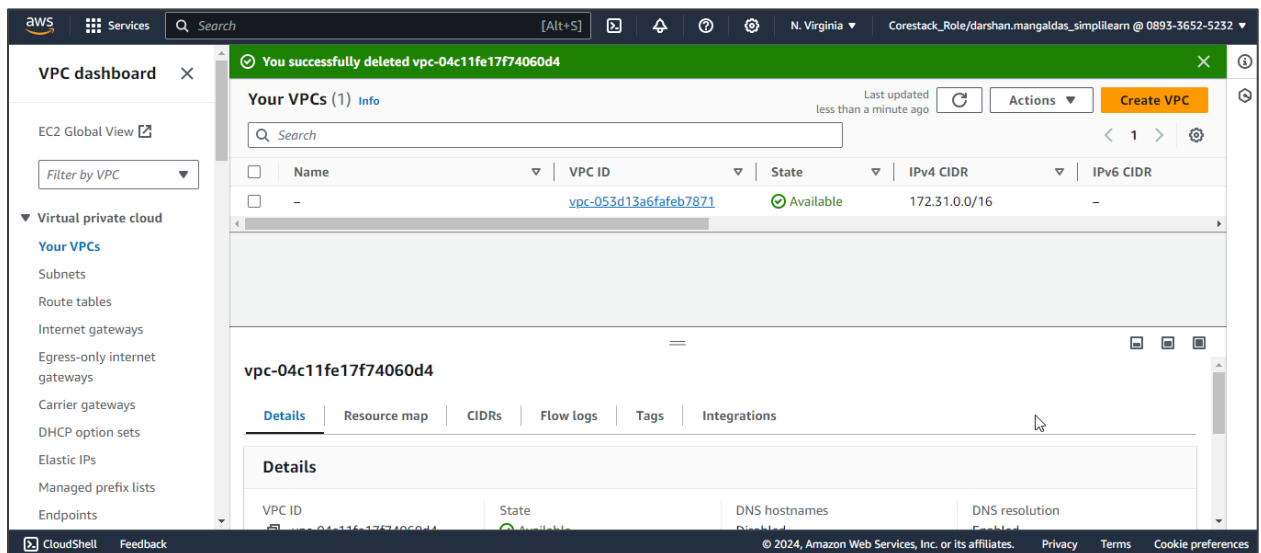
6.1 In the VPC dashboard, select the created VPC, click the **Actions** button, and select **Delete VPC**



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.