Placement Empowerment Program

Cloud Computing and DevOps Centre

Set a private network in cloud – Create a VPC with subnets for your instances. Configure routing for internal communication between subnets

Name :Renita A
Department: ECE

Introduction

A Virtual Private Cloud (VPC) is a secure and isolated portion of a cloud provider's infrastructure where you can deploy your resources in a controlled environment. Setting up a VPC involves creating subnets, configuring routing, and implementing security measures to manage traffic and access. This setup is essential for applications that require secure internal communication while being accessible to external networks when necessary.

Objectives

1. **Create a VPC**: Establish a private network in the cloud that suits your application requirements.
2. **Configure Subnets**: Design and implement subnets within the VPC for different types of instances (e.g., public and private).
3. **Set Up Routing**: Configure routing tables to enable internal communication between subnets and external access as required.
4. **Implement Security**: Use security groups and network ACLs to control inbound and outbound traffic to your instances.
5. **Ensure High Availability**: Distribute resources across multiple Availability Zones to enhance resilience

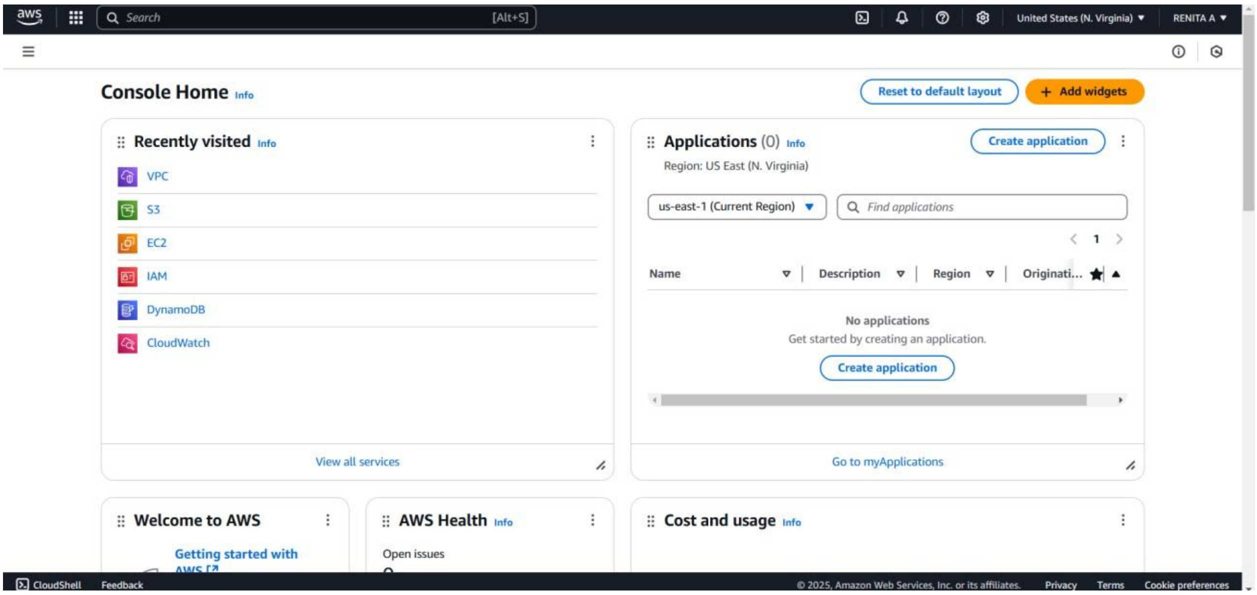
Importance

- Security: A VPC allows you to maintain a secure environment, isolating your resources from public internet exposure while enabling controlled access.

- Customization: You can tailor the network architecture to meet specific needs, such as private IP addressing and subnetwork segmentation.

- Cost Efficiency: Efficiently using cloud resources helps in managing costs associated with data transfer and resource allocation.

- Scalability: Easily scale your infrastructure to accommodate growing workloads without compromising security or performance.



No applications

Get started by creating an application.

- Control: Gain complete control over the networking environment, including IP address ranges, routing, and access controls.

Step-by-Step Overview

Step 1:

1. Go to AWS Management Console.

2. Enter your username and password to log in

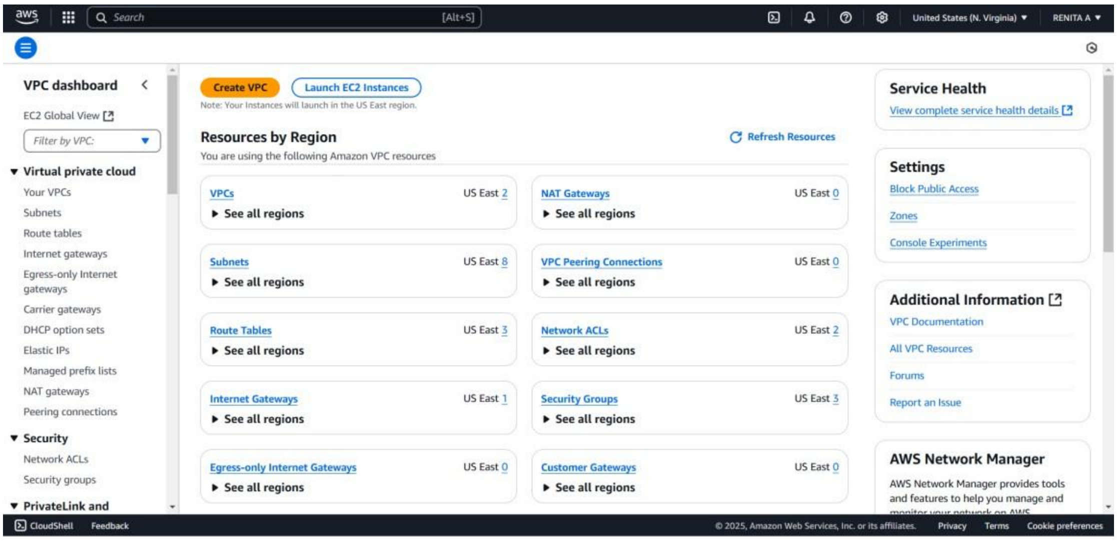
Step 2:

Navigate to the VPC Dashboard

- In the Services menu, select "VPC" to access the VPC Dashboard.
-

Create a VPC

- Click on "Your VPCs" in the left menu, then click "Create VPC." • Specify the following:
    - **Name tag**: A name for your VPC.
    - **IPv4 CIDR block**: E.g., 10.0.0.0/16 (this gives you 65,536 IP addresses).
    - **IPv6 CIDR block**: (Optional).
    - **Tenancy**: Default is usually sufficient.
- Click "Create."



Note: Your Instances will launch in the US East region.

You are using the following Amazon VPC resources

AWS Network Manager provides tools and features to help you manage and monitor your network on AWS

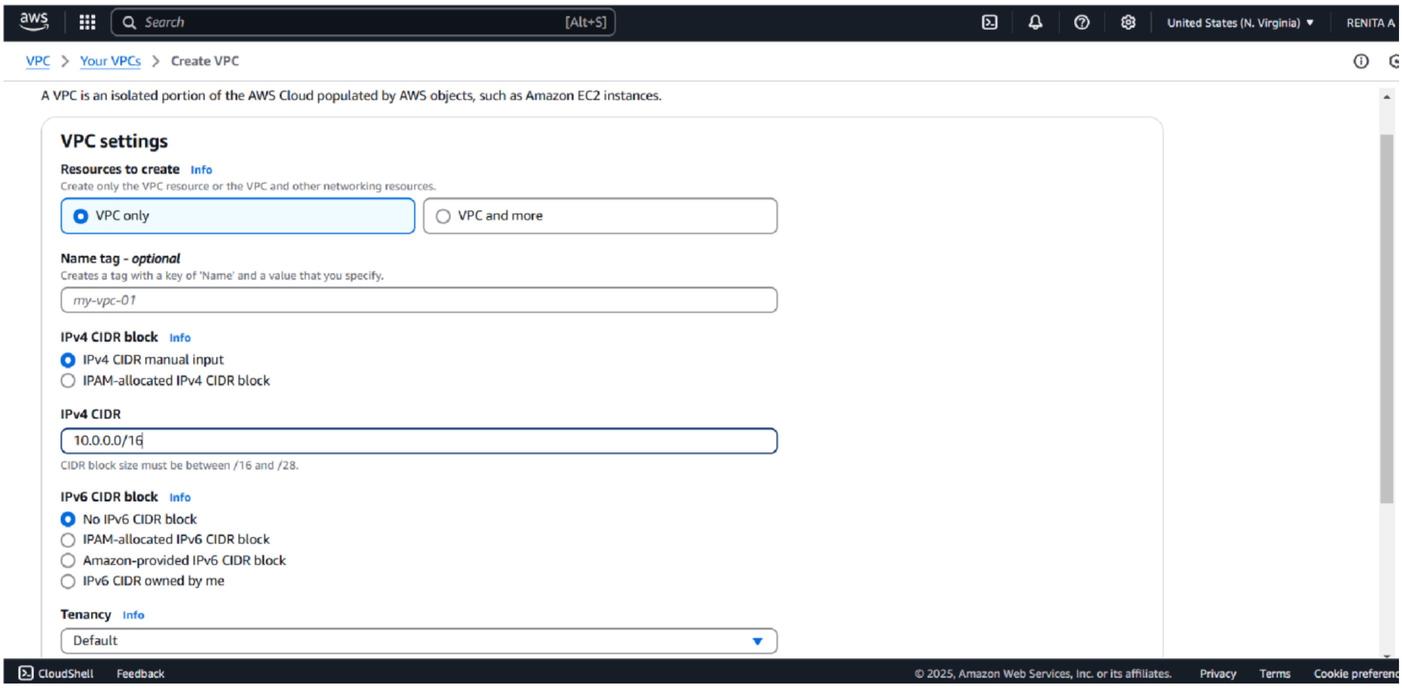
Step 3:

Create Subnets

You need at least two private subnets for internal communication:

1. Go to Subnets → Click Create Subnet.

2. Select the VPC (MyPrivateVPC) you created earlier.


aws
Search
[Alt+S]
United States (N. Virginia) ▾
RENITA A
VPC > Your VPCs > Create VPC
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferenc

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.

my-vpc-01

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

Default ▾

3. Create two subnets:

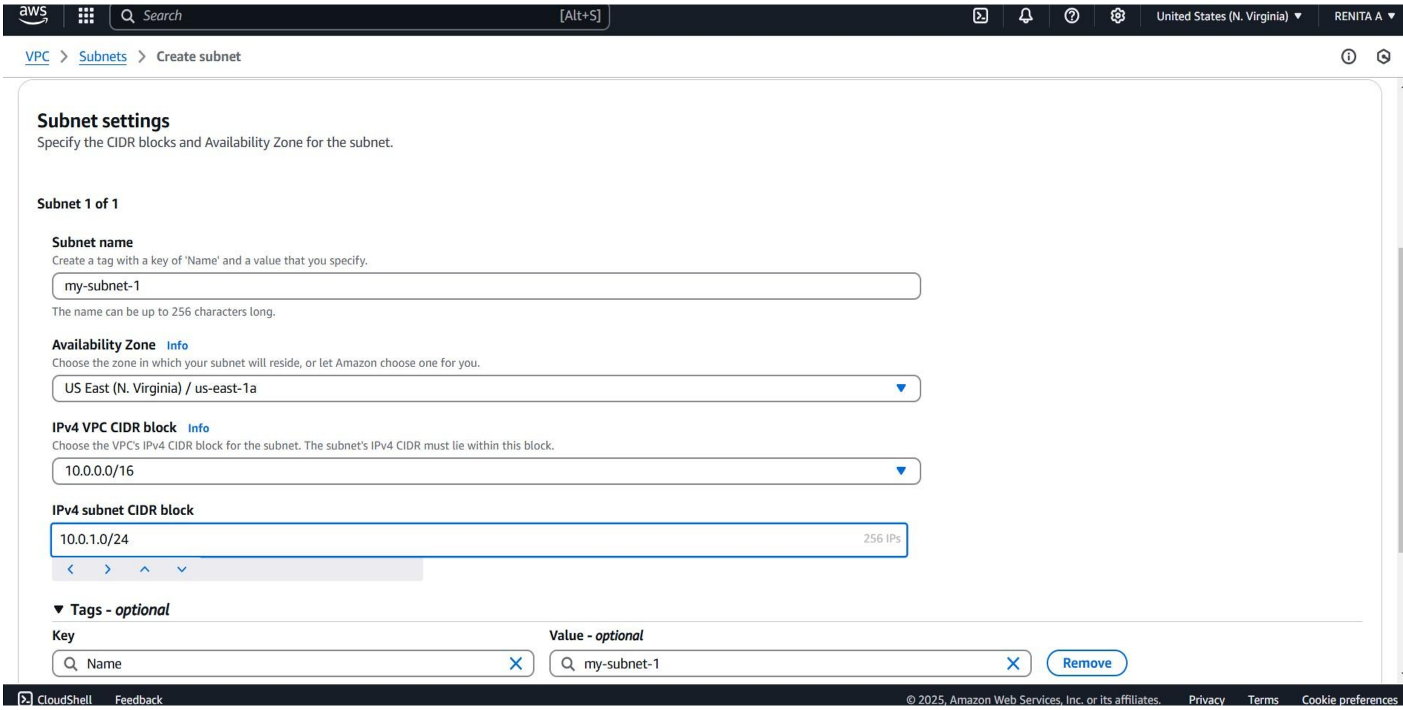
Subnet 1 (Private-Subnet-A)

IPv4 CIDR: 10.0.1.0/24

Availability Zone: us-east-1a (example)

Subnet 2 (Private-Subnet-B)

IPv4 CIDR: 10.0.2.0/24



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.

my-subnet-1

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

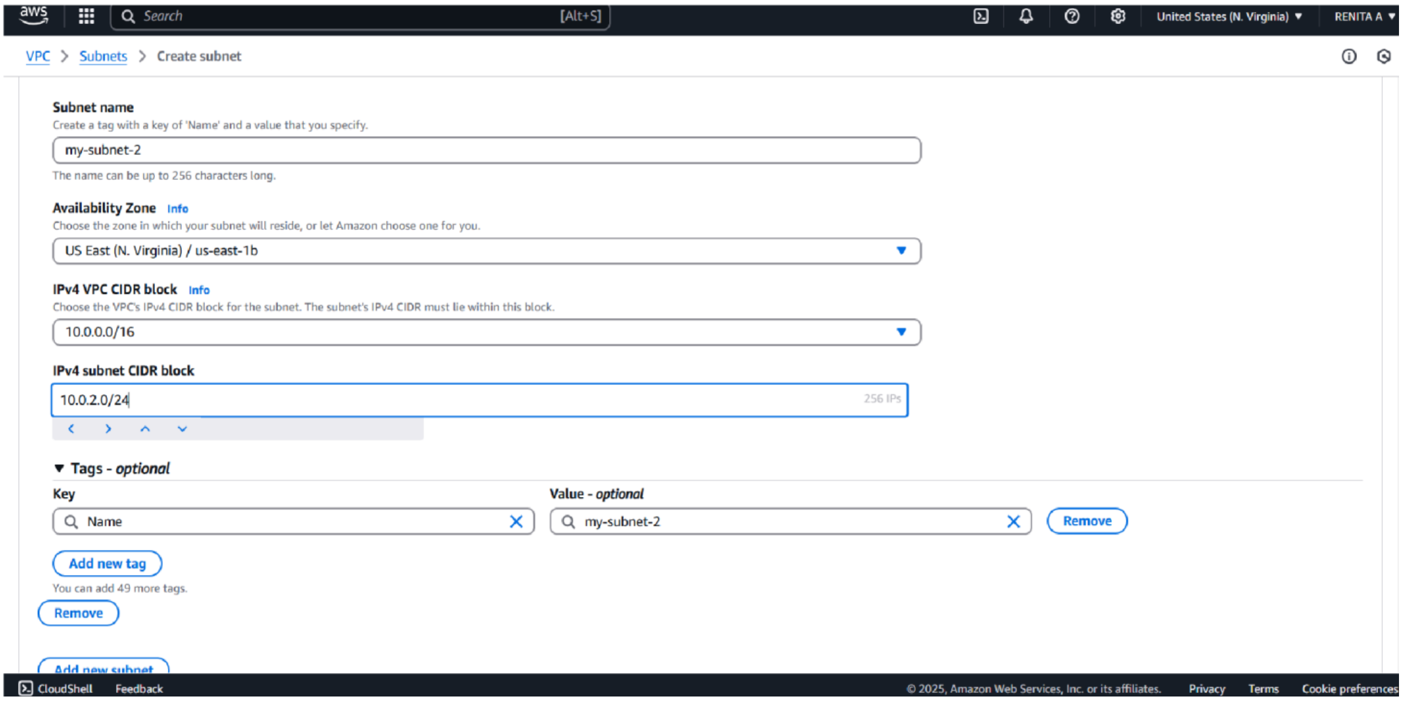
10.0.1.0/24 256 IPs

▼ Tags - *optional*

Key	Value - *optional*
Name	my-subnet-1

.

Step 4:



Subnet name
Create a tag with a key of 'Name' and a value that you specify.
my-subnet-2
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-1b

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
10.0.2.0/24 256 IPs

▼ Tags - *optional*

Key	Value - *optional*
Name	my-subnet-2

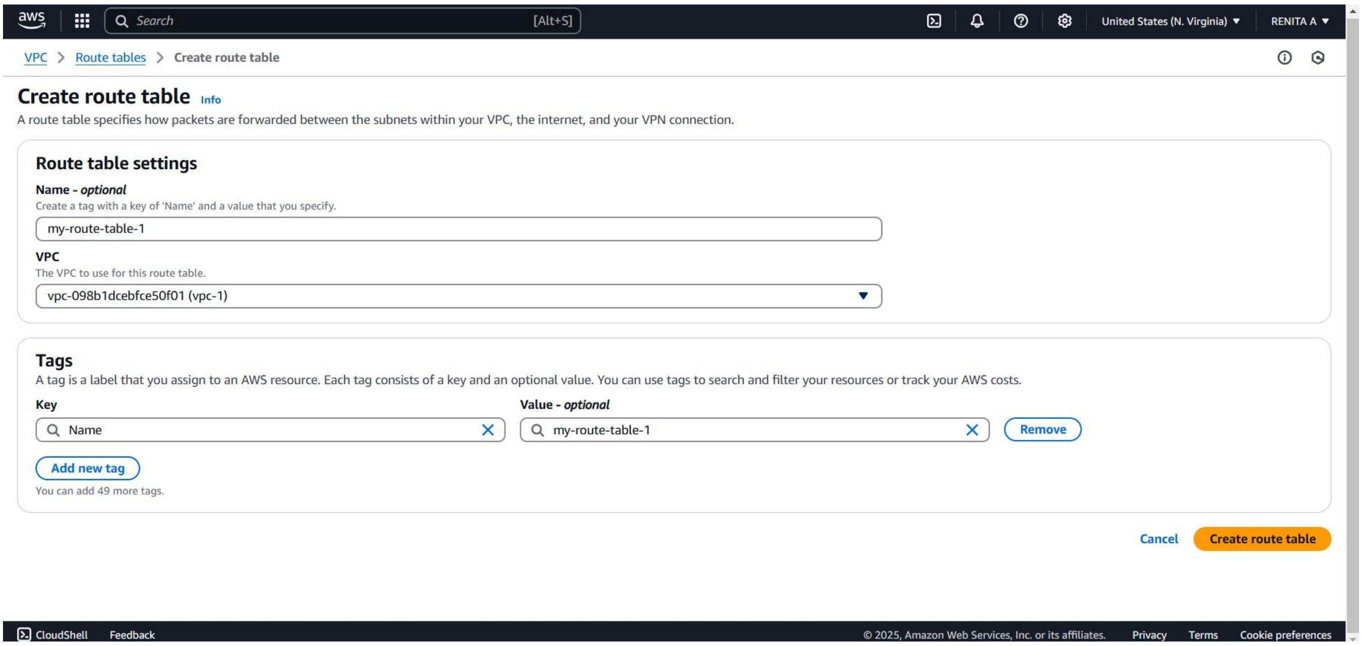
Configure Route Tables for Internal Communication

1. Go to Route Tables → Click Create Route Table.

2. Name it (e.g., PrivateRouteTable).

3. Select MyPrivateVPC.

4. Click Create.



aws
Search [Alt+S]
United States (N. Virginia) ▼
RENITA A ▼
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.
my-route-table-1
VPC
The VPC to use for this route table.
vpc-098b1dcebfce50f01 (vpc-1)

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	my-route-table-1

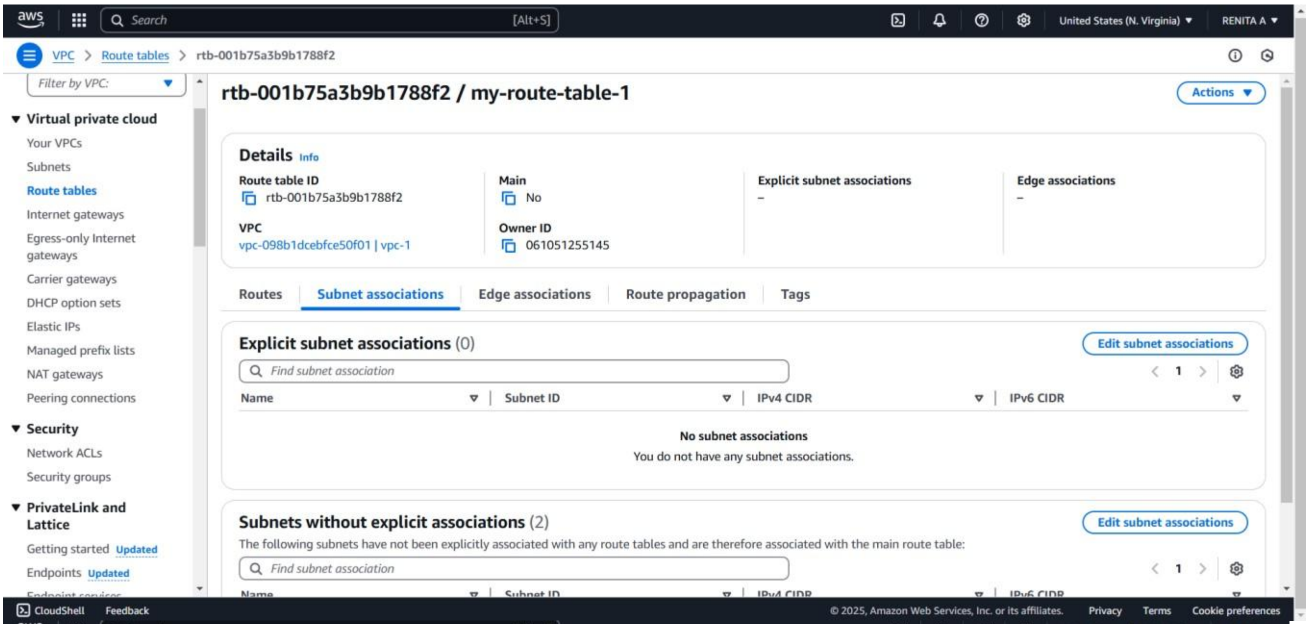
Step 5:

Associate the subnets:

Go to Subnet Associations → Click Edit subnet associations.

Select Private-Subnet-A and Private-Subnet-B.

Click Save associations.



VPC > Route tables > rtb-001b75a3b9b1788f2

rtb-001b75a3b9b1788f2 / my-route-table-1

Details Info

Route table ID	Main	Explicit subnet associations	Edge associations
rtb-001b75a3b9b1788f2	No	–	–
VPC	Owner ID		
vpc-098b1dcebfce50f01 | vpc-1	061051255145		

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

Explicit subnet associations (0)

Find subnet association

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR

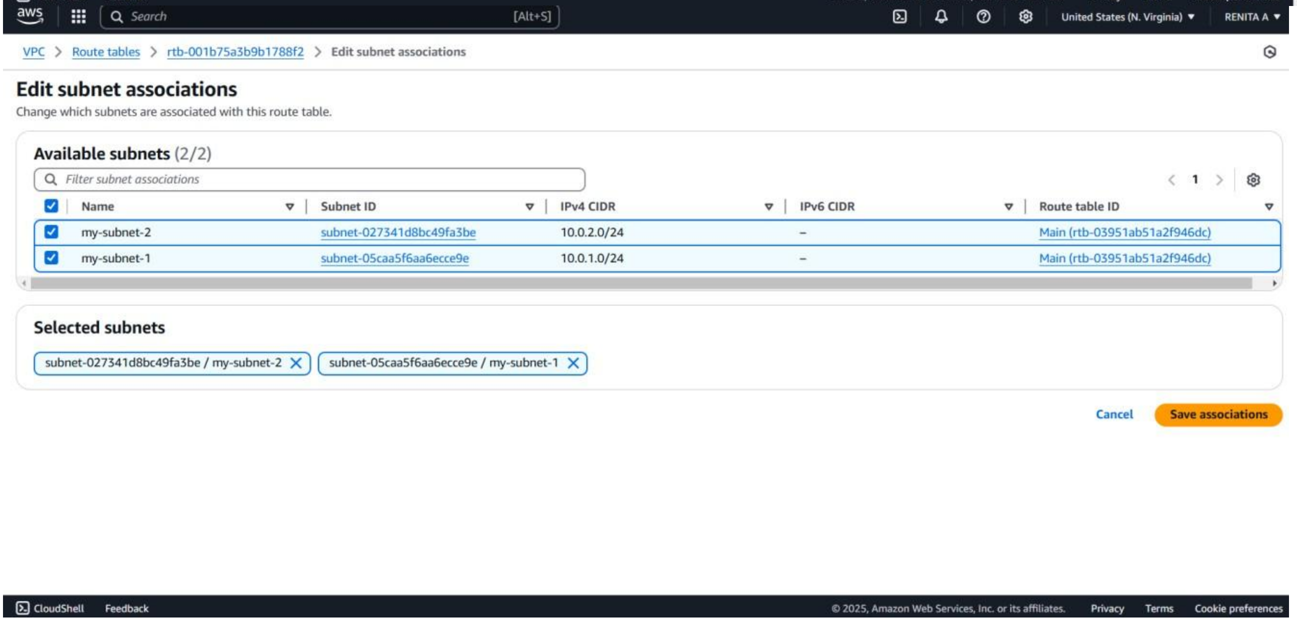
No subnet associations

You do not have any subnet associations.

Subnets without explicit associations (2)

The following subnets have not been explicitly associated with any route tables and are therefore associated with the main route table:

Find subnet association



VPC > Route tables > rtb-001b75a3b9b1788f2 > Edit subnet associations

Edit subnet associations

Change which subnets are associated with this route table.

Available subnets (2/2)

Filter subnet associations

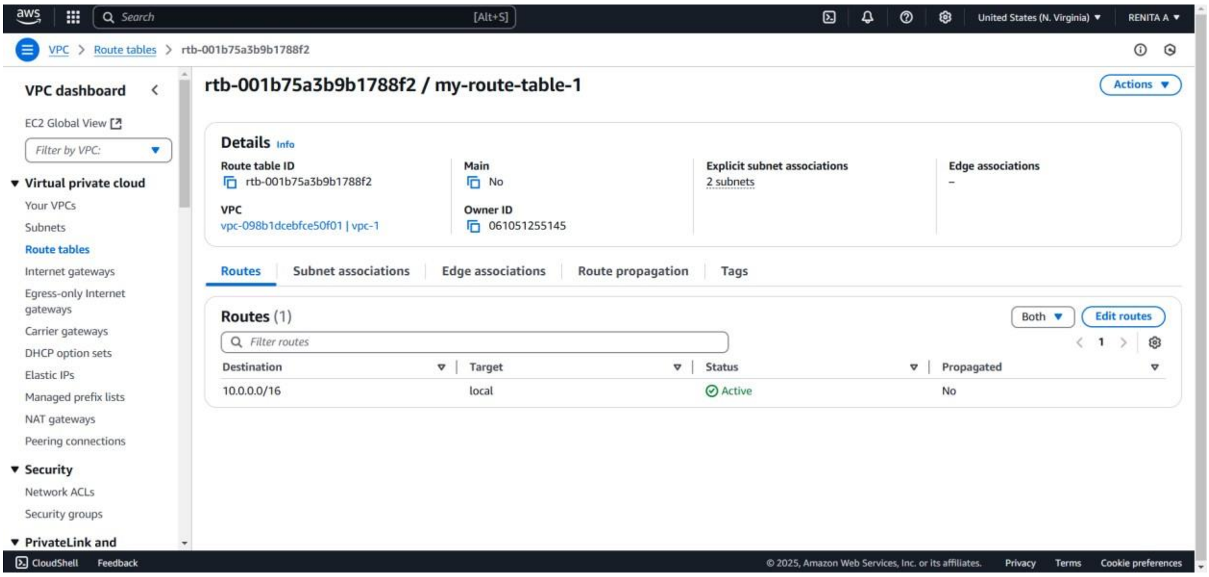
☑	Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
☑	my-subnet-2	subnet-027341d8bc49fa3be	10.0.2.0/24	–	Main (rtb-03951ab51a2f946dc)
☑	my-subnet-1	subnet-05caa5f6aa6ecce9e	10.0.1.0/24	–	Main (rtb-03951ab51a2f946dc)

Selected subnets

subnet-027341d8bc49fa3be / my-subnet-2 ✕ subnet-05caa5f6aa6ecce9e / my-subnet-1 ✕

Step 6:

Default route: 10.0.0.0/16 → local (Automatically added).



rtb-001b75a3b9b1788f2 / my-route-table-1

Details Info

Route table ID	Main	Explicit subnet associations	Edge associations
rtb-001b75a3b9b1788f2	No	2 subnets	–

VPC	Owner ID
vpc-098b1dcebfce50f01 | vpc-1	061051255145

Routes (1)

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No

Step 7:

Launch Instances in Private Subnets

1. Go to EC2 Dashboard → Launch Instance.

2. Select an AMI (Amazon Linux, Ubuntu, etc.).

3. Choose an Instance Type (e.g., t2.micro).

4. Under Network settings:

Select MyPrivateVPC.

Select Private Subnet-A or Private-Subnet-B.

Disable Auto-assign Public IP (to keep it private).

Step 8:

Enable Internal Communication

Instances inside the private subnets can communicate without an internet gateway.

If instances need internet access (for updates, etc.), configure a NAT Gateway in a Public Subnet.

Use Security Groups to allow inbound traffic only from internal sources (e.g., allow SSH from 10.0.0.0/16).

Step 9:

Now, your private network is set up, and instances inside can communicate securely!

Outcome

After following these steps, you will have:

- A VPC that is isolated from other networks.
- One or more subnets for your instances, with at least one public subnet that can communicate with the Internet.
- Proper routing configured for internal communication between subnets.