# 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:** HARSHINI A **Department:** CSE

St. JOSEPH'S COLLEGE OF ENGINEERING | St. JOSEPH'S INSTITUTE OF TECHNOLOGY
AUTONOMOUS INSTITUTIONS, AFFILIATED TO ANNA UNIVERSITY

## *Introduction*

In cloud environments, securing internal communication is crucial for maintaining data integrity and minimizing exposure to the public internet. A Virtual Private Cloud (VPC) enables organizations to create isolated network environments with controlled access. This PoC demonstrates the process of setting up a **private network** in the cloud, creating **subnets**, and configuring **internal routing** for communication between instances.

## *Objectives*

1. Create a VPC with private and public subnets.

2. Configure routing tables to enable internal communication.

3. Deploy instances within the subnets and verify private communication.

4. Ensure no direct internet access for private subnets while allowing controlled outbound access.

## *Importance*

1. Security: Limits exposure to external threats by restricting internet access.

2. Performance: Reduces latency by keeping communication within the private network.

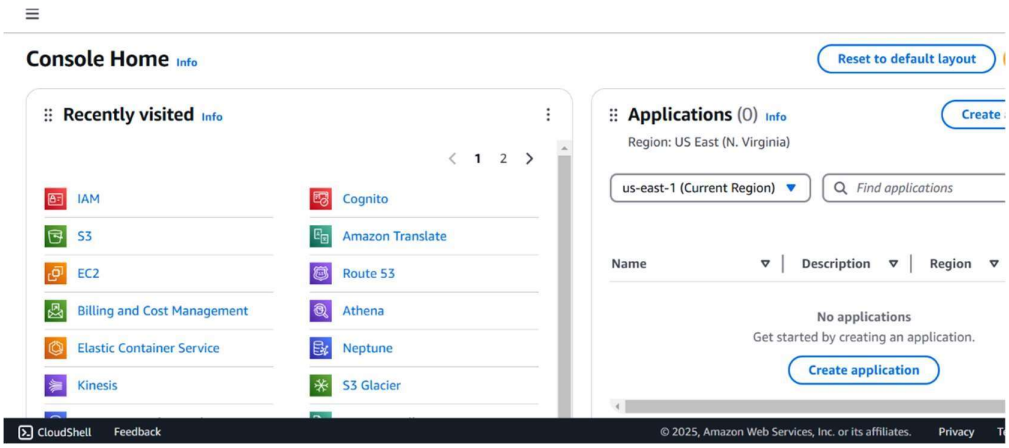
3. Compliance: Helps meet regulatory requirements for sensitive data handling.

4. Scalability: Allows better control over network traffic as workloads grow.

# Step-by-Step Overview

## Step 1:

1. Go to AWS Management Console
2. Enter your username and password to log in



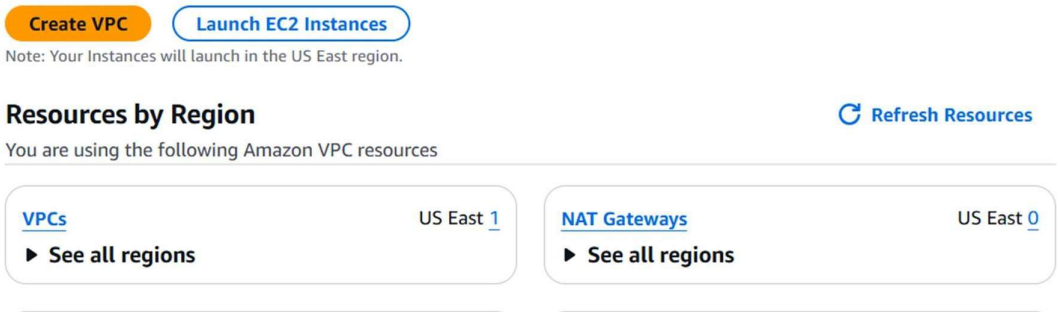

## Step 2:

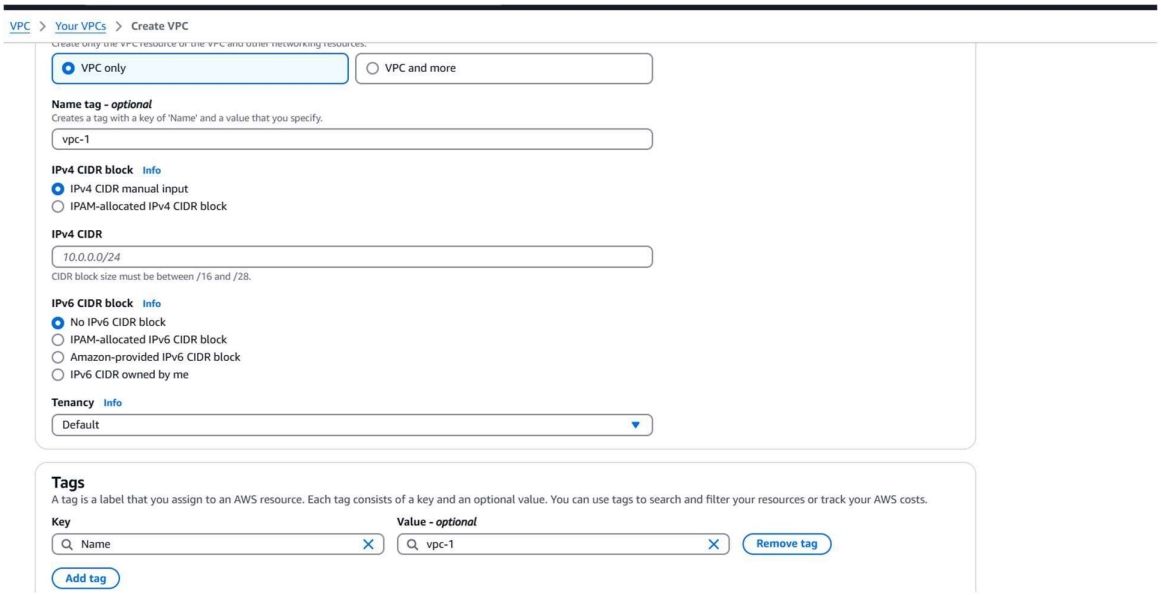
Navigate to the VPC Dashboard

- 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."




# Step 3:

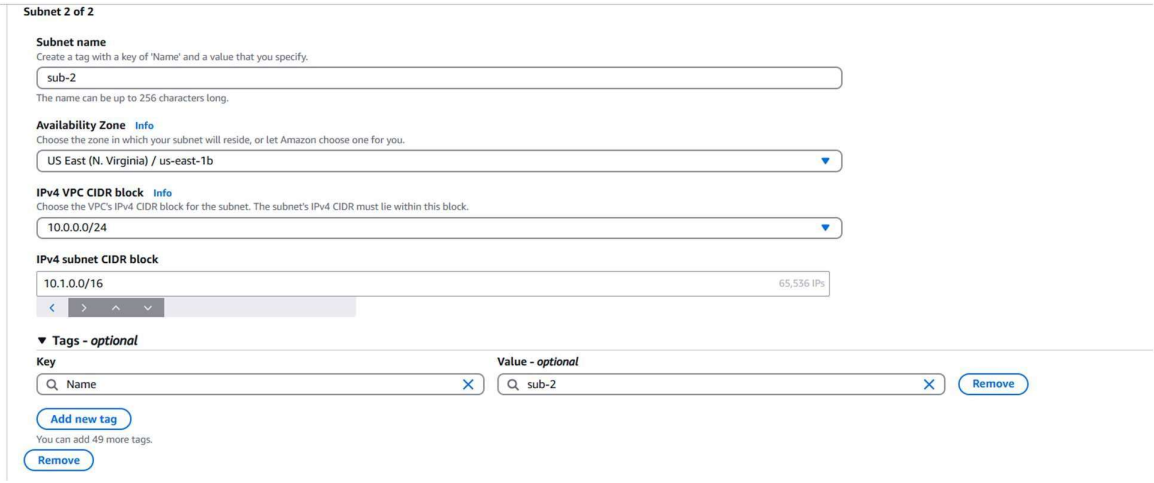
Create Subnets

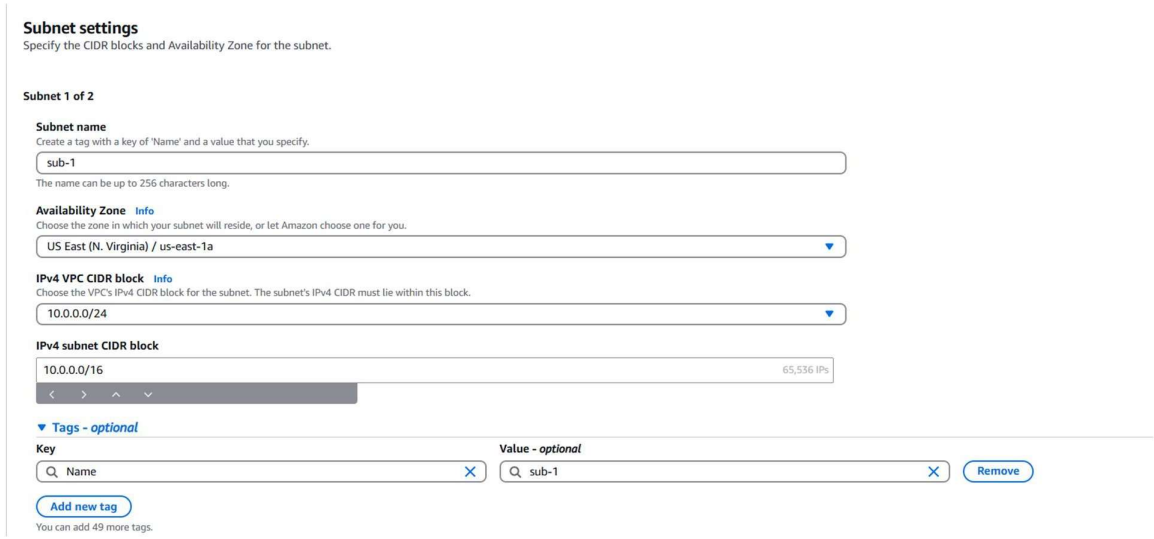
You need at least two private subnets for internal communication:

1. Go to Subnets → Click Create Subnet.
2. Select the VPC (MyPrivateVPC) you created earlier.
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
Availability Zone: us-east-2a (example)




# Step 4:

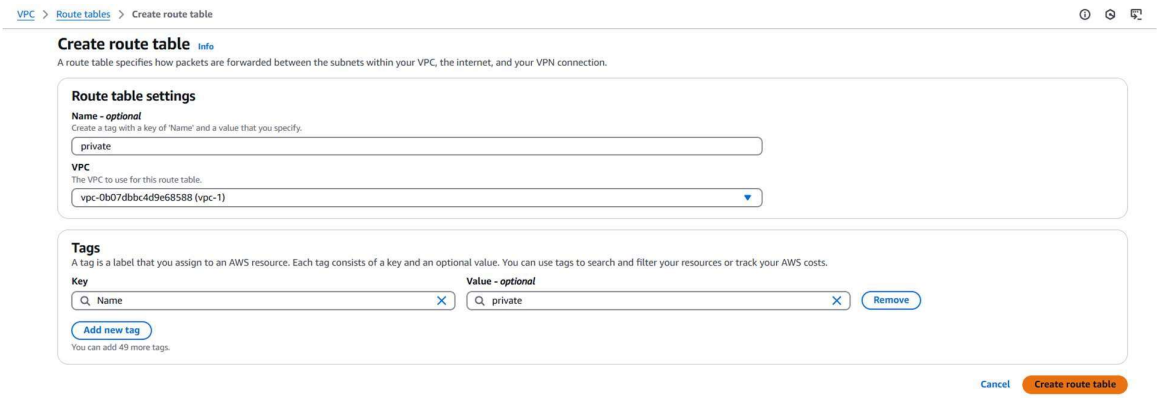
Configure Route Tables for Internal Communication

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

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

3. Select MyPrivateVPC.

4. Click Create.



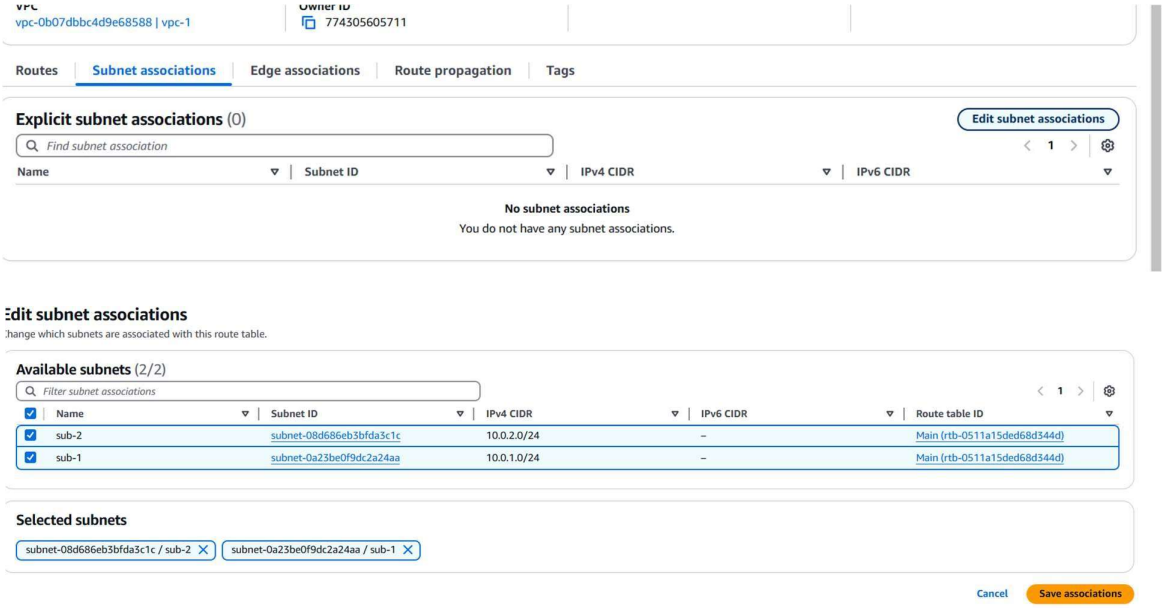

# Step 5:

Associate the subnets:

Go to Subnet Associations → Click Edit subnet associations.

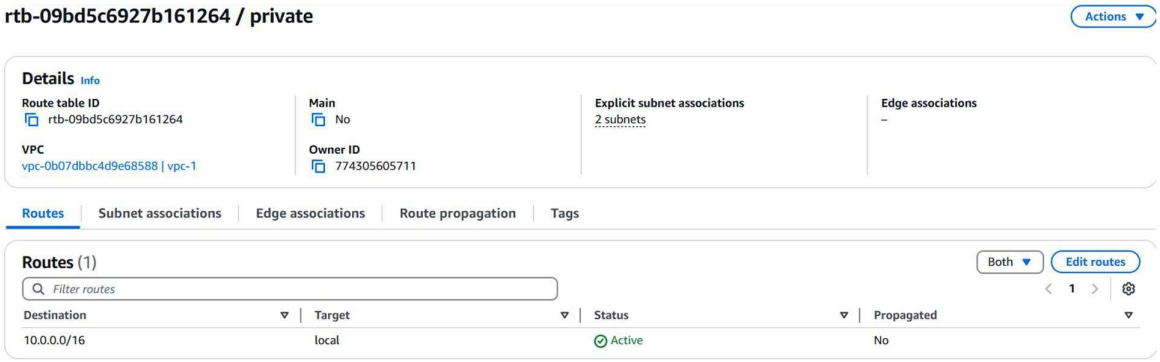
Select Private-Subnet-A and Private-Subnet-B.

Click Save associations.




# Step 6:

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




# Step 7:

Launch Instances in Private Subnets

1. Go to EC2 Dashboard → Launch Instance.

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

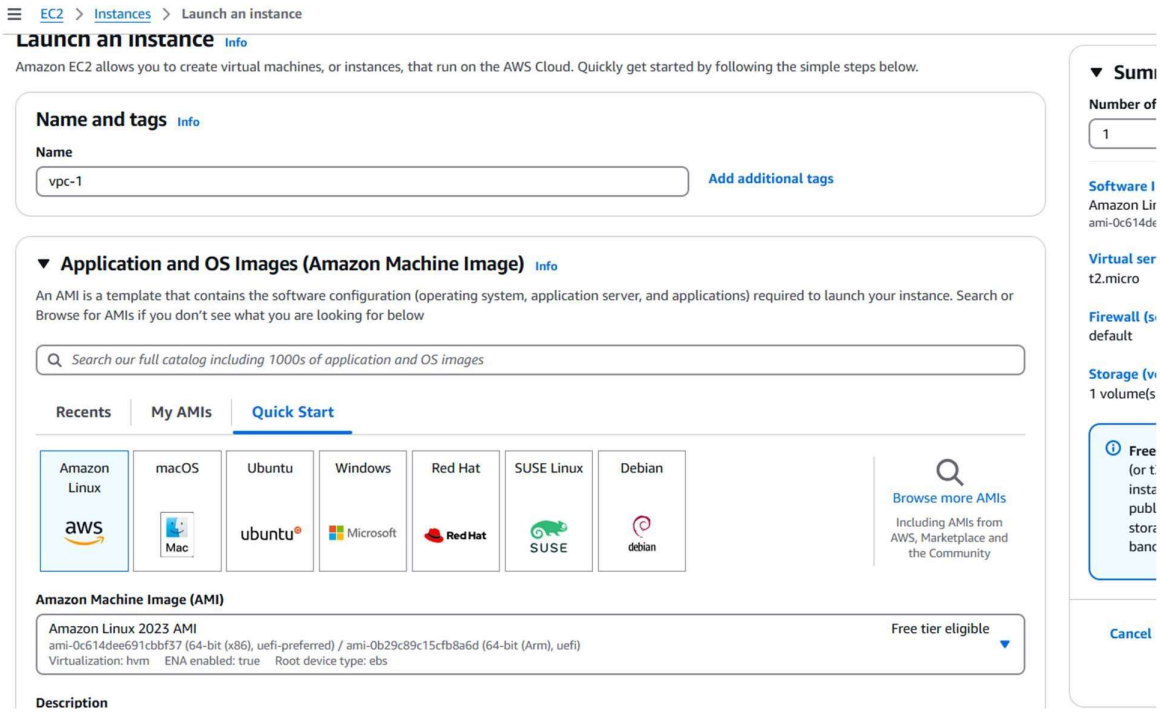
3. Choose an Instance Type (e.g., t2.micro).

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).

## *Outcome*

After following these steps, you will have:

1. The private instance should not have direct internet access.

2. Internal communication should work seamlessly between private subnets.

3. The public instance should be able to connect to the private instance using SSH.

4. Internet access for the private instance should be routed through the NAT Gateway (if configured).