# 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 :Jai Riyaz G Department: ADS



**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.

**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

Step-by-Step Overview

## Step 1:

* 1. Go to [AWS Management Console](https://aws.amazon.com/console/).
  2. Enter your username and password to log in



## Step 2:

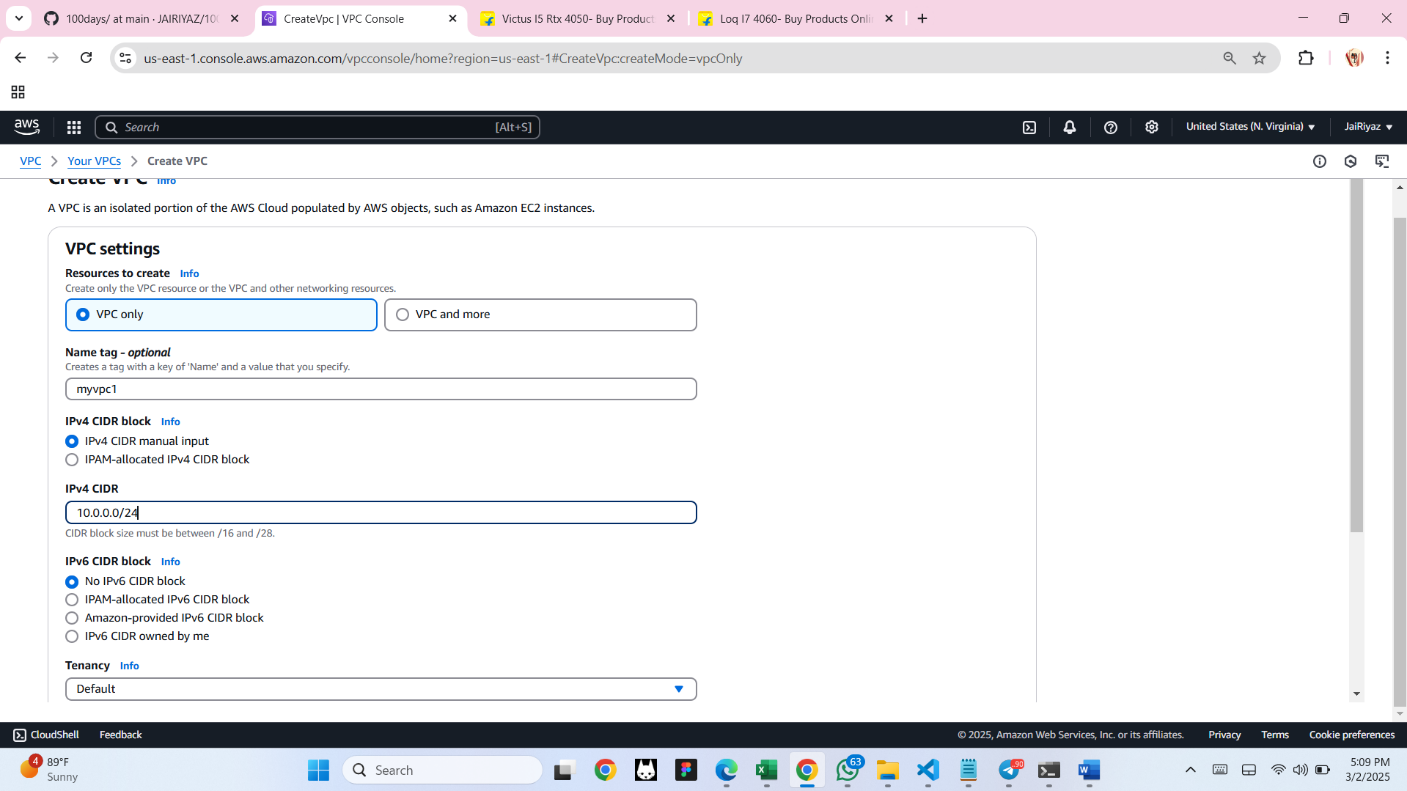
**Navigate to the VPC Dashboard**

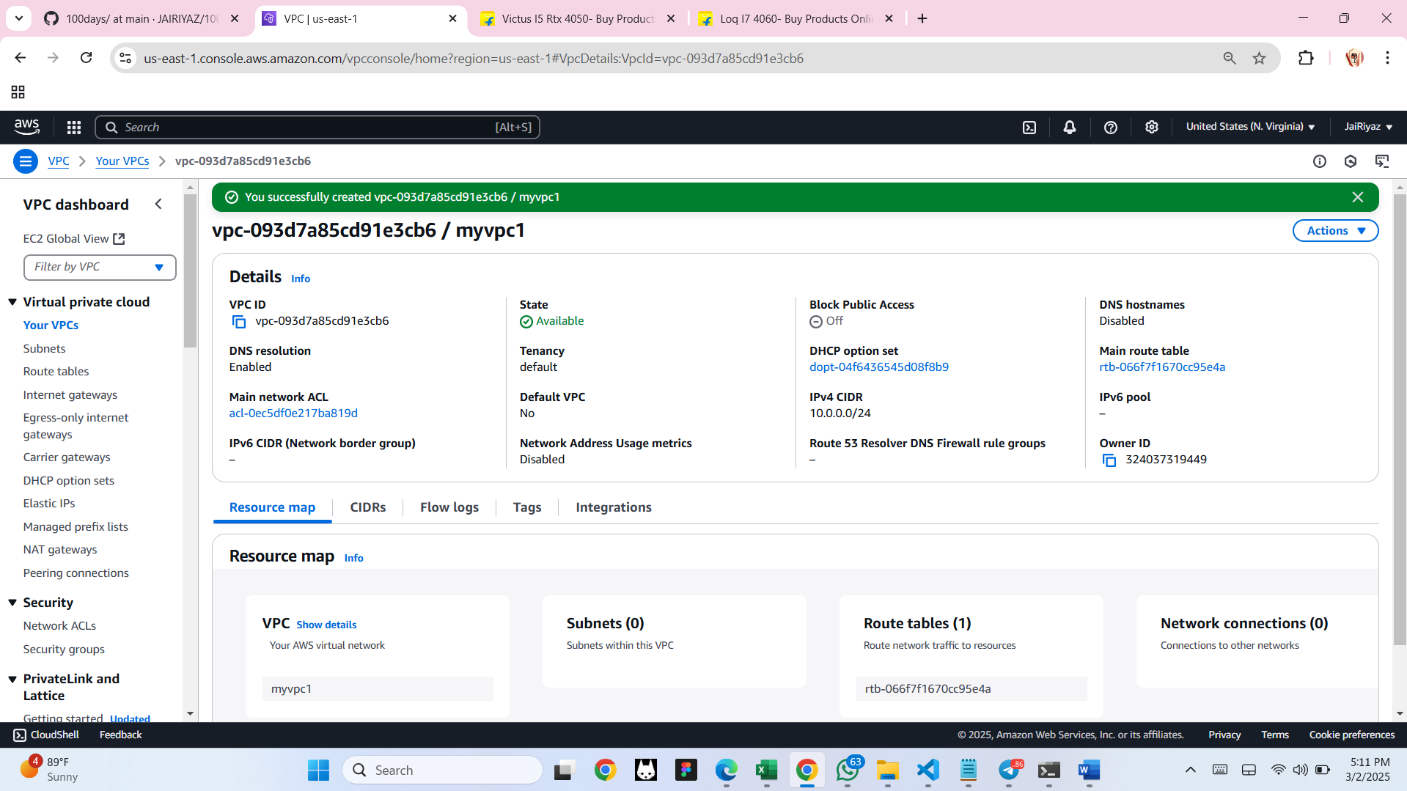
* In the Services menu, select "VPC" to access the VPC Dashboard.

**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.**

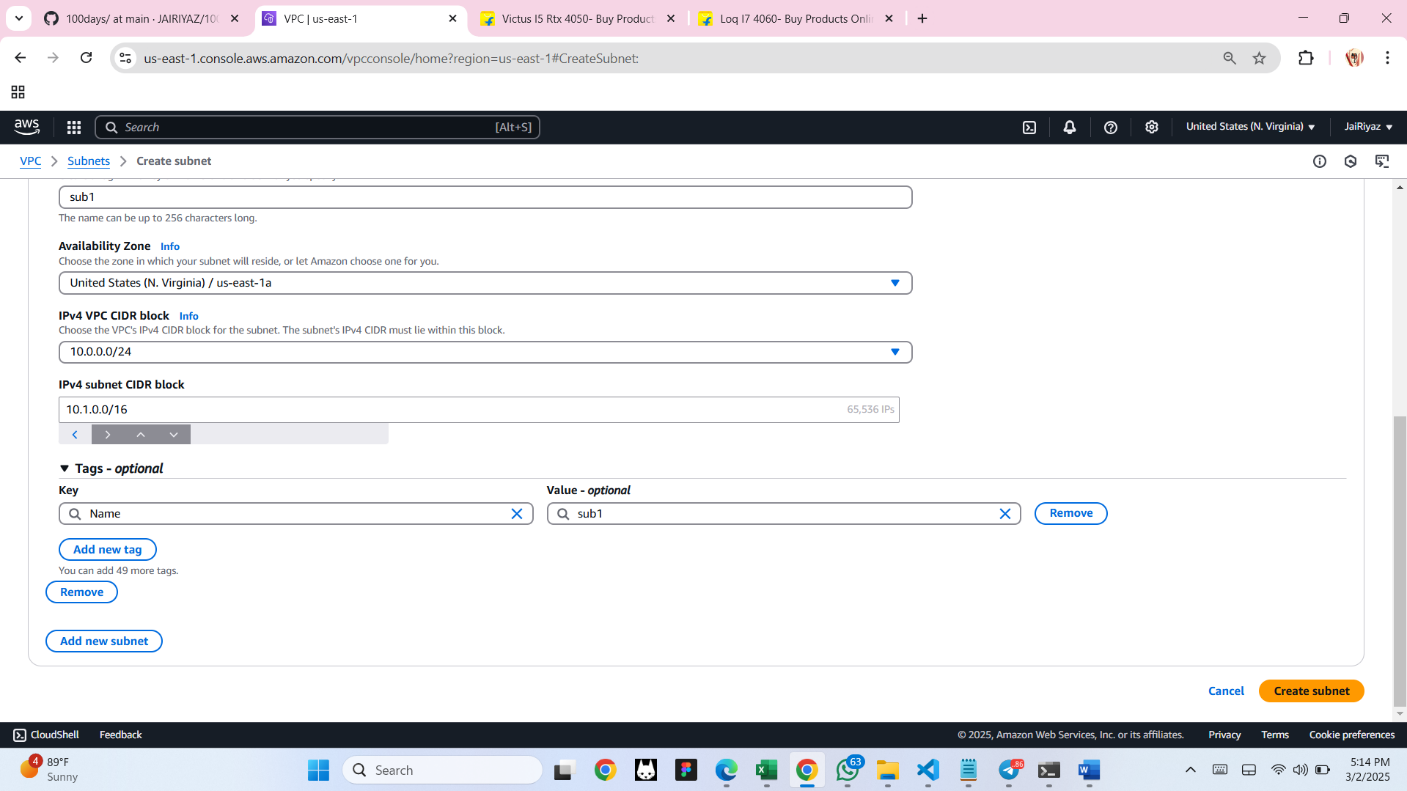
**3. Create two subnets:**

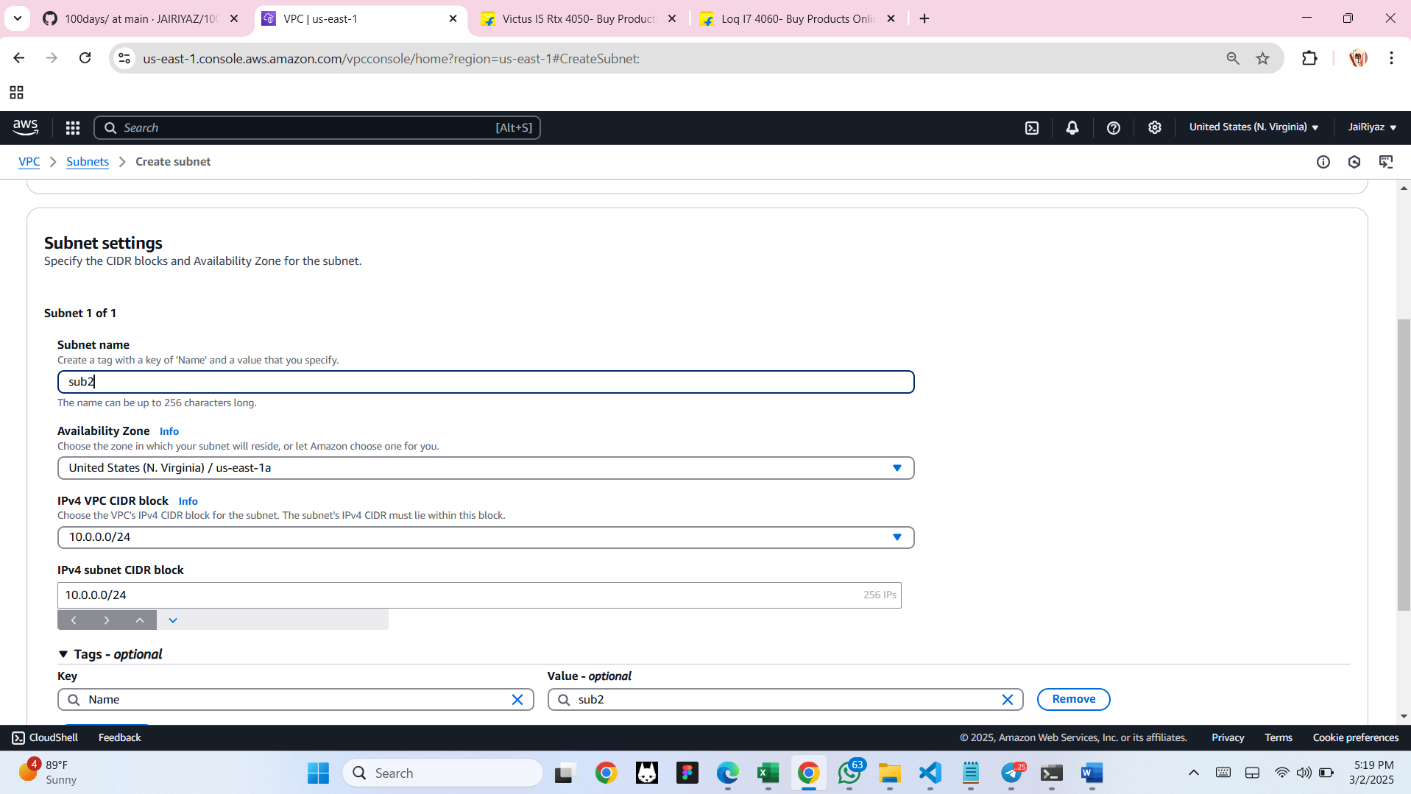
**Subnet 1 (Private-Subnet-A)**

**IPv4 CIDR:**

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

**Subnet 2 (Private-Subnet-B)**



**IPv4 CIDR:** 

## 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.

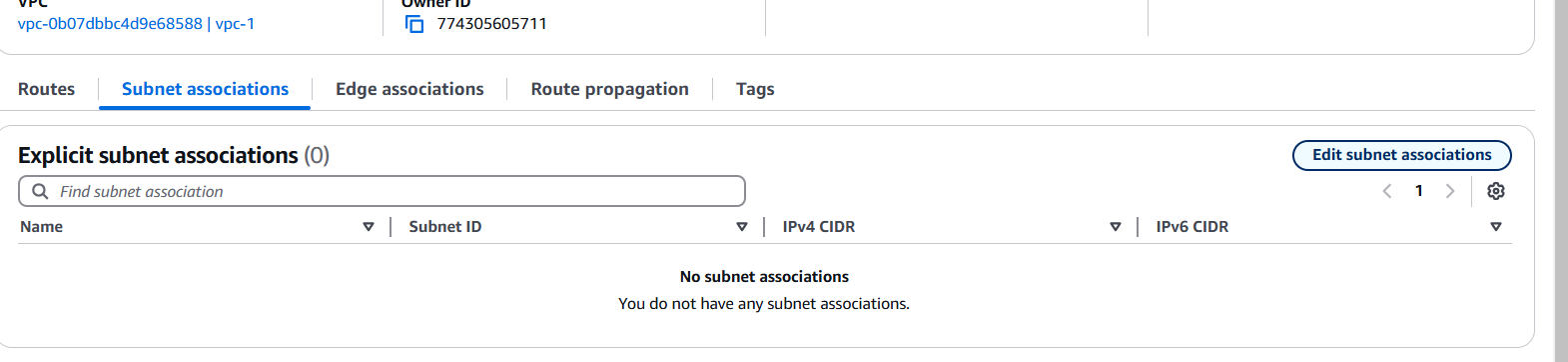
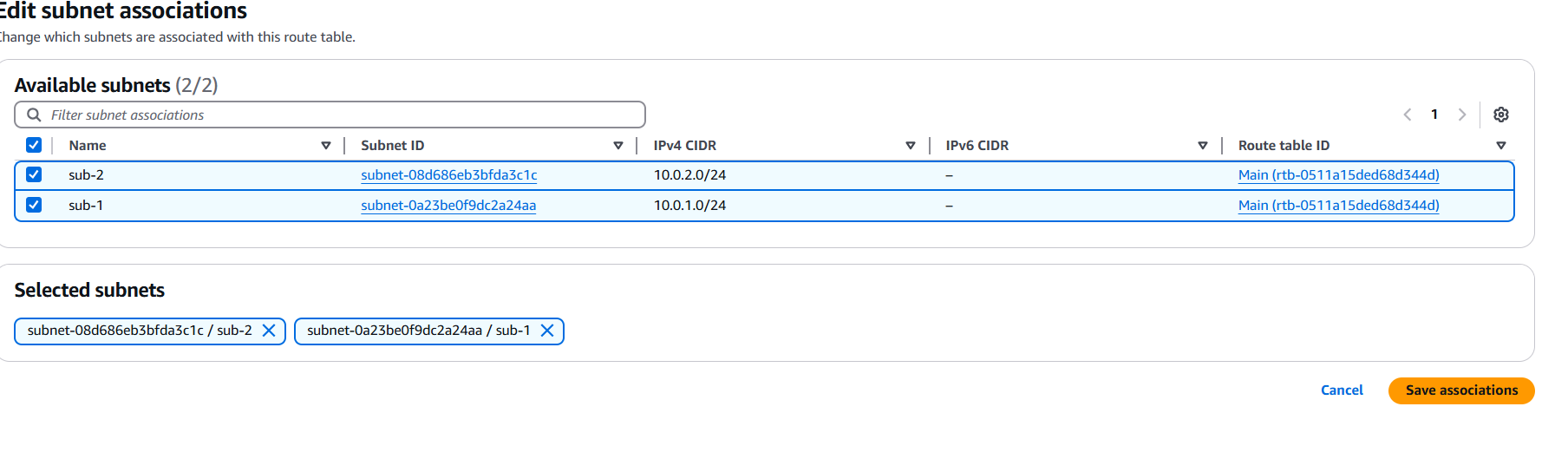
## Step 5:

**Associate the subnets:**

Go to Subnet Associations → Click Edit subnet associations.

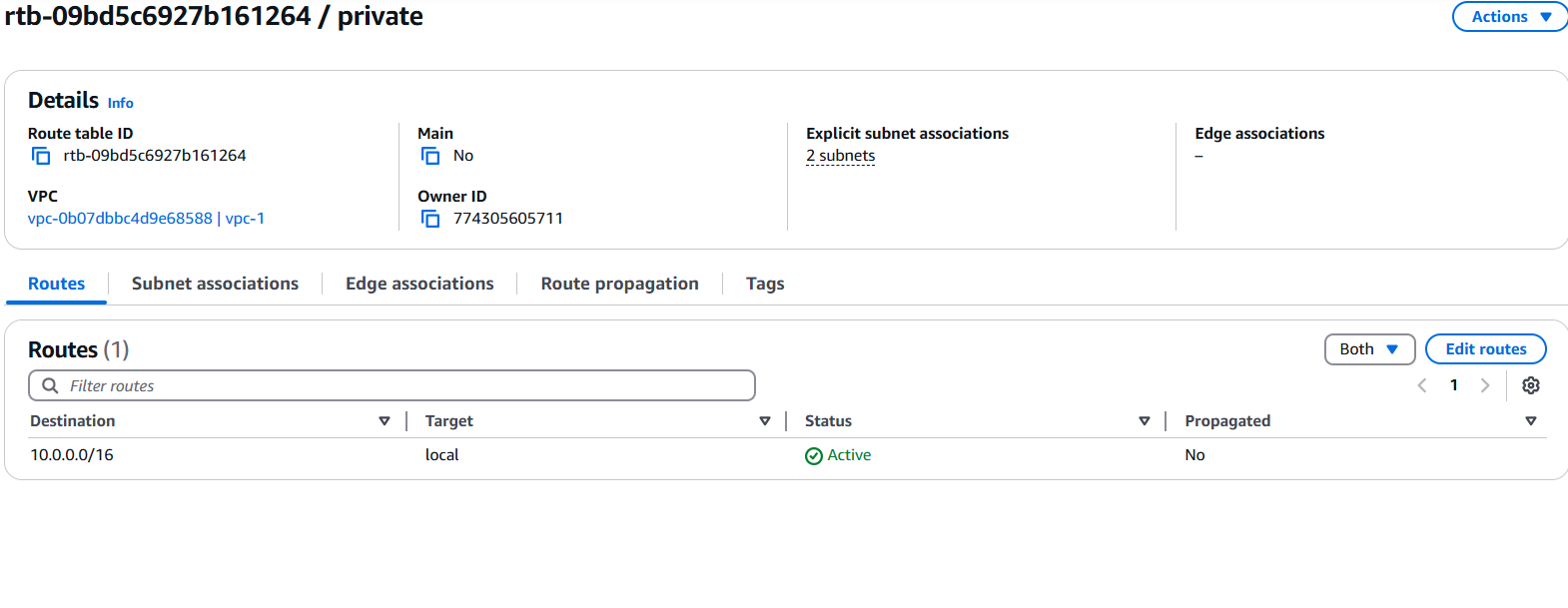
Select Private-Subnet-A and Private-Subnet-B.

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).

## Step 9:

Now, your private network is set up, and instances inside can communicate securely! Let me know if you need extra configurations like VPN, Bastion Host, or NAT setup.

**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.