# 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 : Mohamad riyas P

Department: IT



**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.
* 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](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.

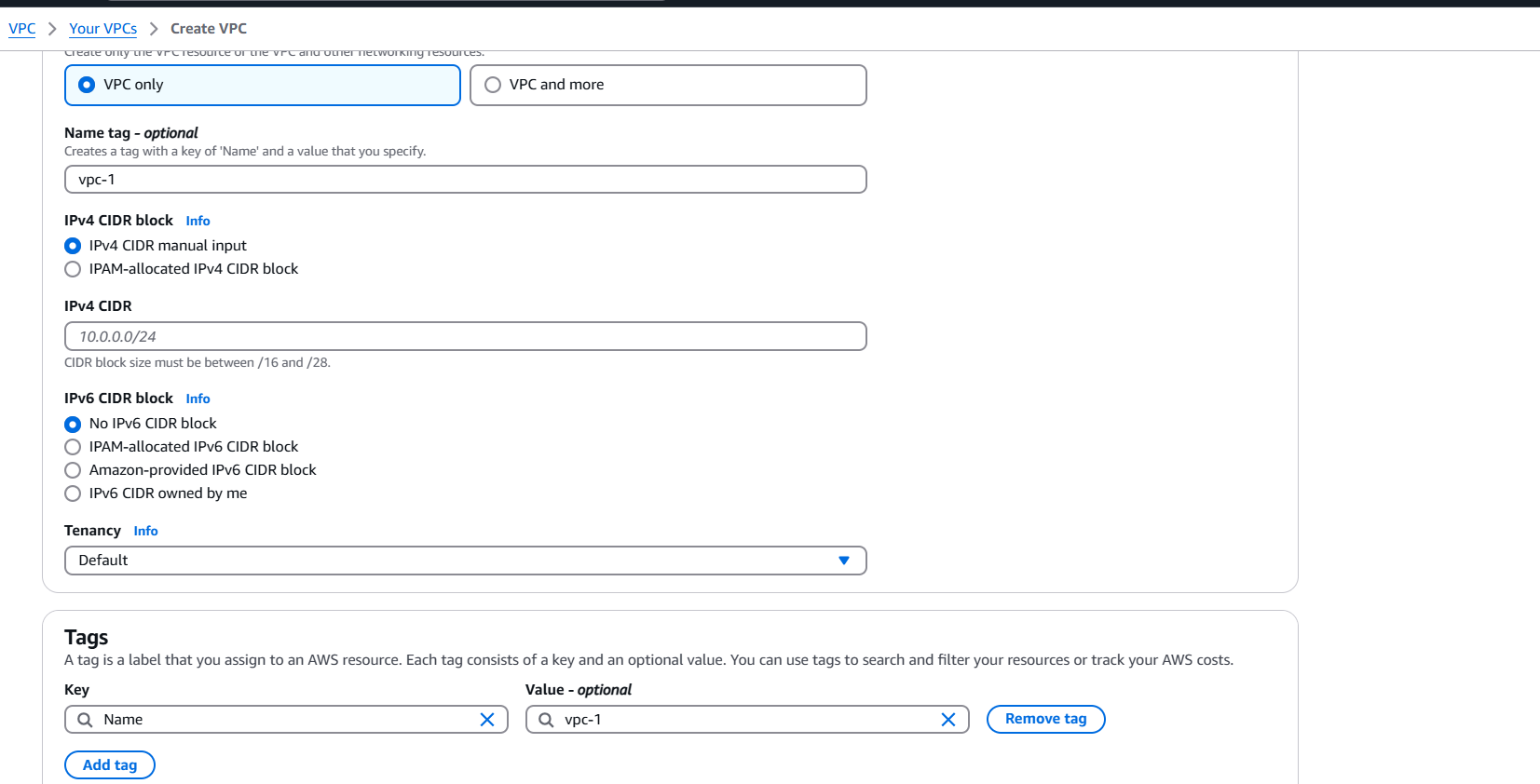
**Create a VPC**

* Click on "Your VPCs" in the left menu, then click "Create VPC."
* Specify the following:

Select only vpc

* + **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:**

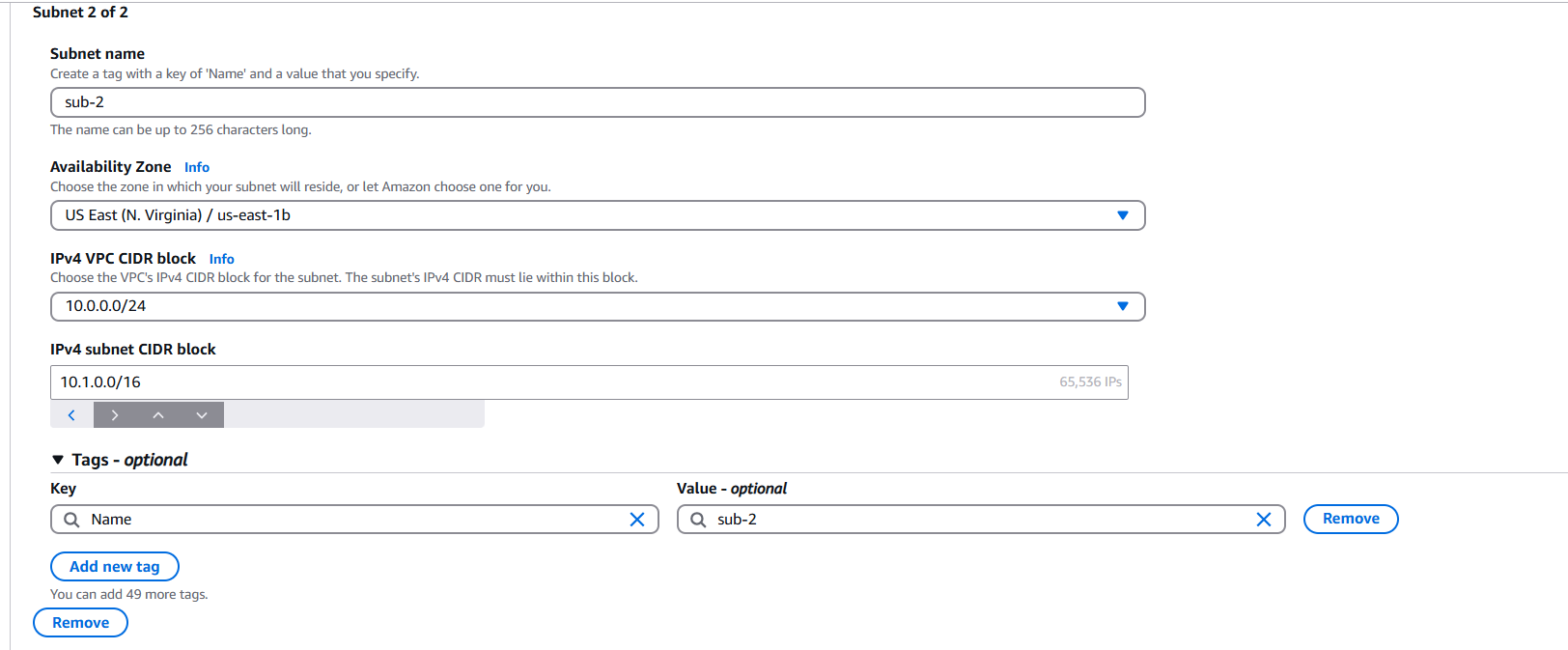
**Subnet 1 (Private-Subnet-A)**

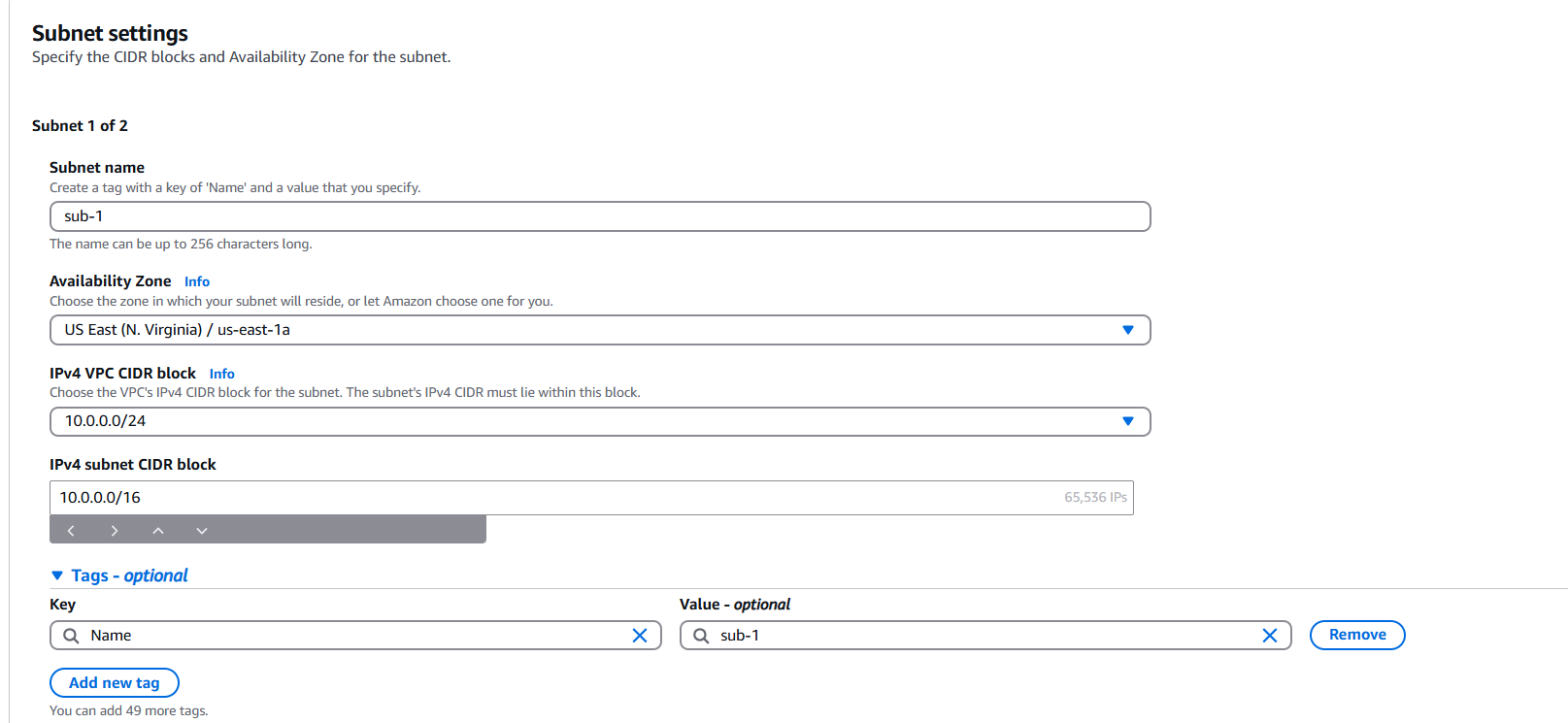
**IPv4 CIDR: 10.0.1.0/24**

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

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

**IPv4 CIDR: 10.0.2.0/24**





## 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.

## 

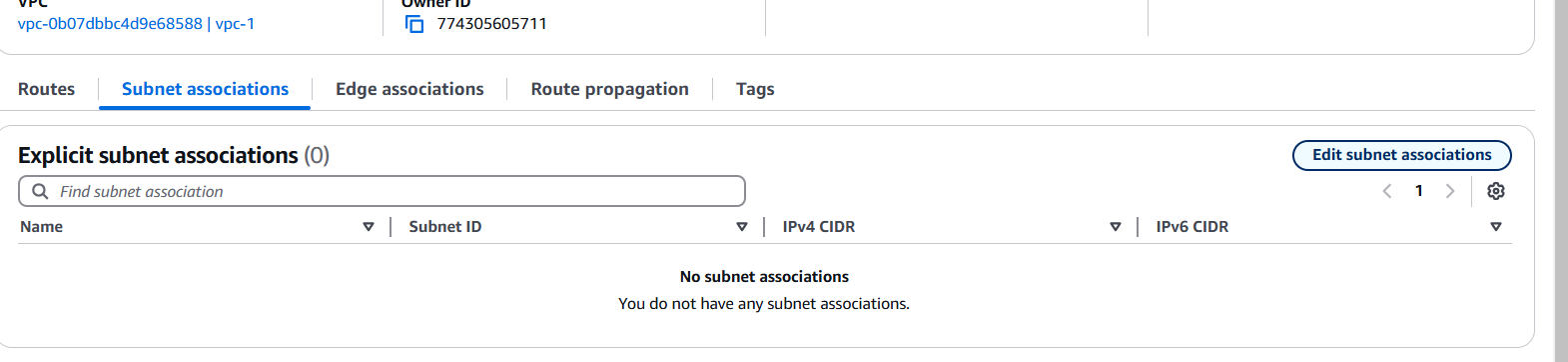
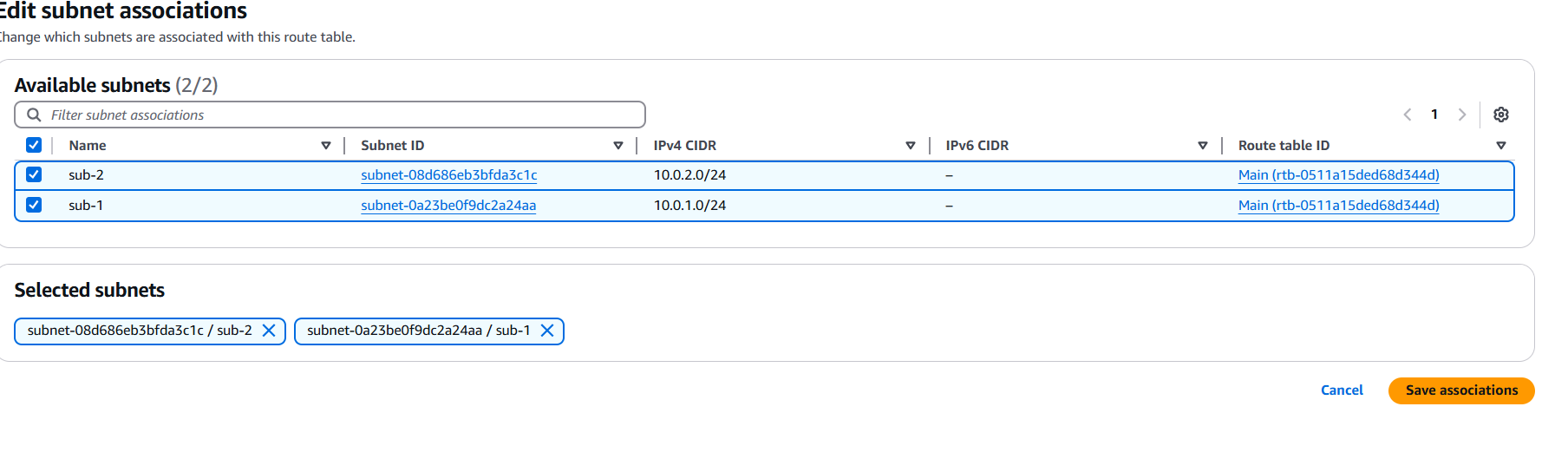
## Step 5:

**Associate the subnets:**

Go to Subnet Associations → Click Edit subnet associations.

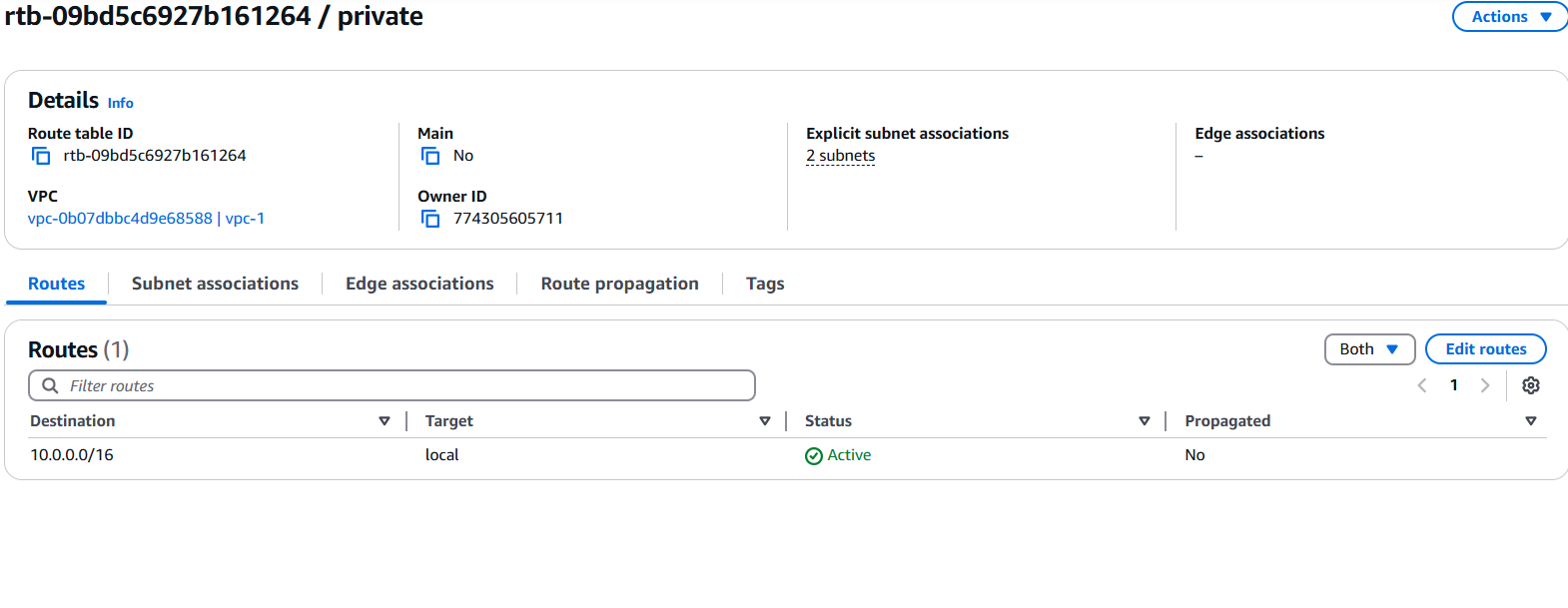
Select Private-Subnet-A and Private-Subnet-B.

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.).

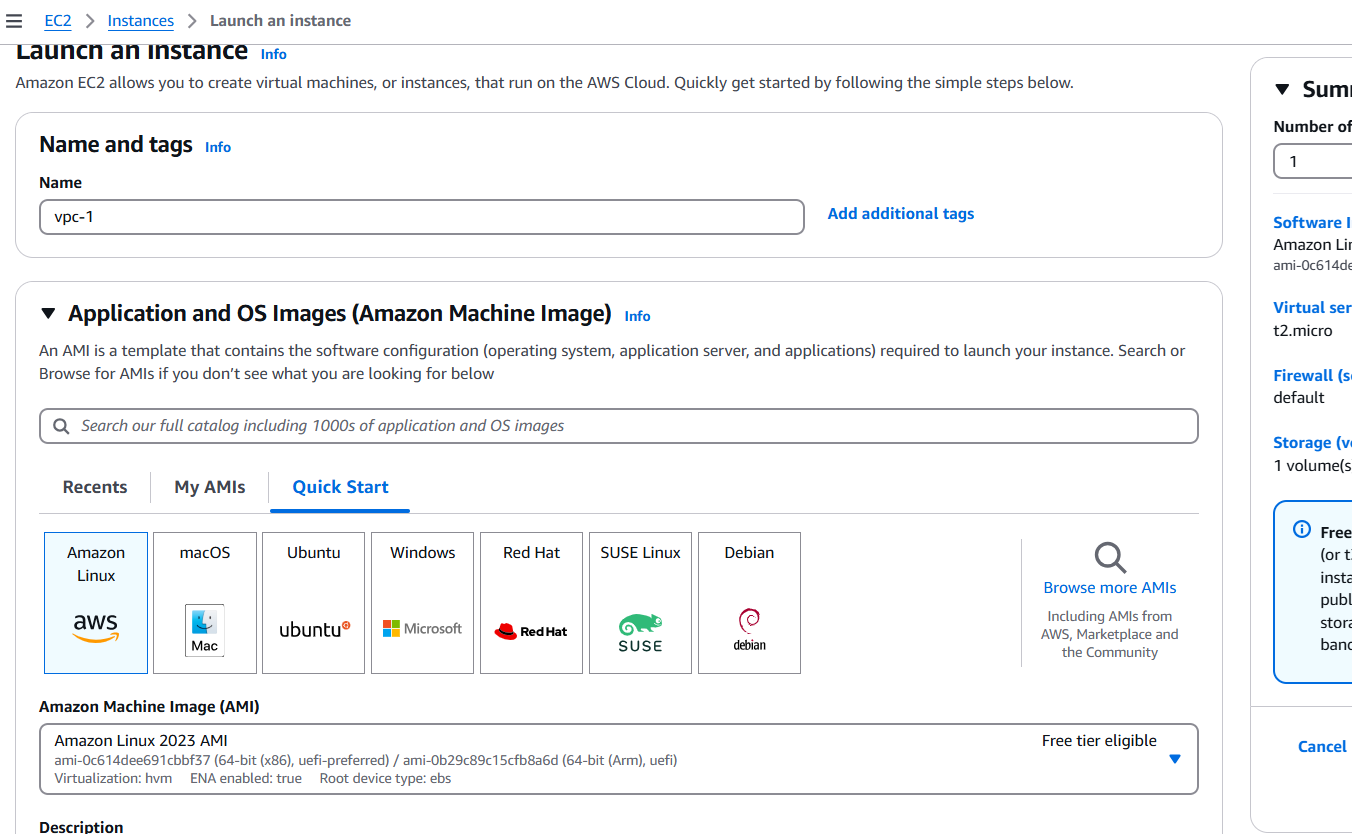
3. Choose an Instance Type (e.g., t2.micro).

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.

1.Create a Security Group:

Click the Create Security Group button.

In the Create Security Group form:

Name: Provide a name for the security group (e.g., MyVPCInstanceSG).

Description: Write a brief description (e.g., Security group for my VPC instance).

VPC: Select the VPC where you want this security group to be applied.

2. Add Inbound Rules:

Click Add Rule under the Inbound Rules section.

For example, to allow SSH access:

Type: Select SSH.

Protocol: Select TCP.

Port Range: Enter 22.

Source: You can select My IP to restrict SSH to your IP address or use 0.0.0.0/0 for global access (less secure).

You can add other rules as needed, like HTTP (80) or HTTPS (443).

3. Add Outbound Rules:

By default, the outbound rules allow all traffic. You can modify it as needed.

4. Review and Create:

Review the security group settings and click Create

This will attach the security group to your instance.

## 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.