# 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 :Harivasan S

Department: ADS



**Introduction**

A Virtual Private Cloud (VPC) is a secure, isolated segment within a cloud provider's infrastructure, allowing you to deploy resources in a controlled environment. Configuring a VPC involves setting up subnets, defining routing rules, and implementing security controls to regulate traffic and access. This architecture is crucial for applications that need protected internal communication while maintaining controlled external connectivity.

**Objectives**

1. Set Up a VPC: Create a dedicated cloud network tailored to your application's needs.

2. Define Subnets: Organize the VPC into subnets, separating public and private resources as needed.

3. Configure Routing: Establish routing tables to manage internal subnet communication and external connectivity.

4. Enhance Security: Apply security groups and network ACLs to regulate inbound and outbound traffic.

5. Optimize Availability: Distribute resources across multiple Availability Zones to improve reliability and fault tolerance.

# 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



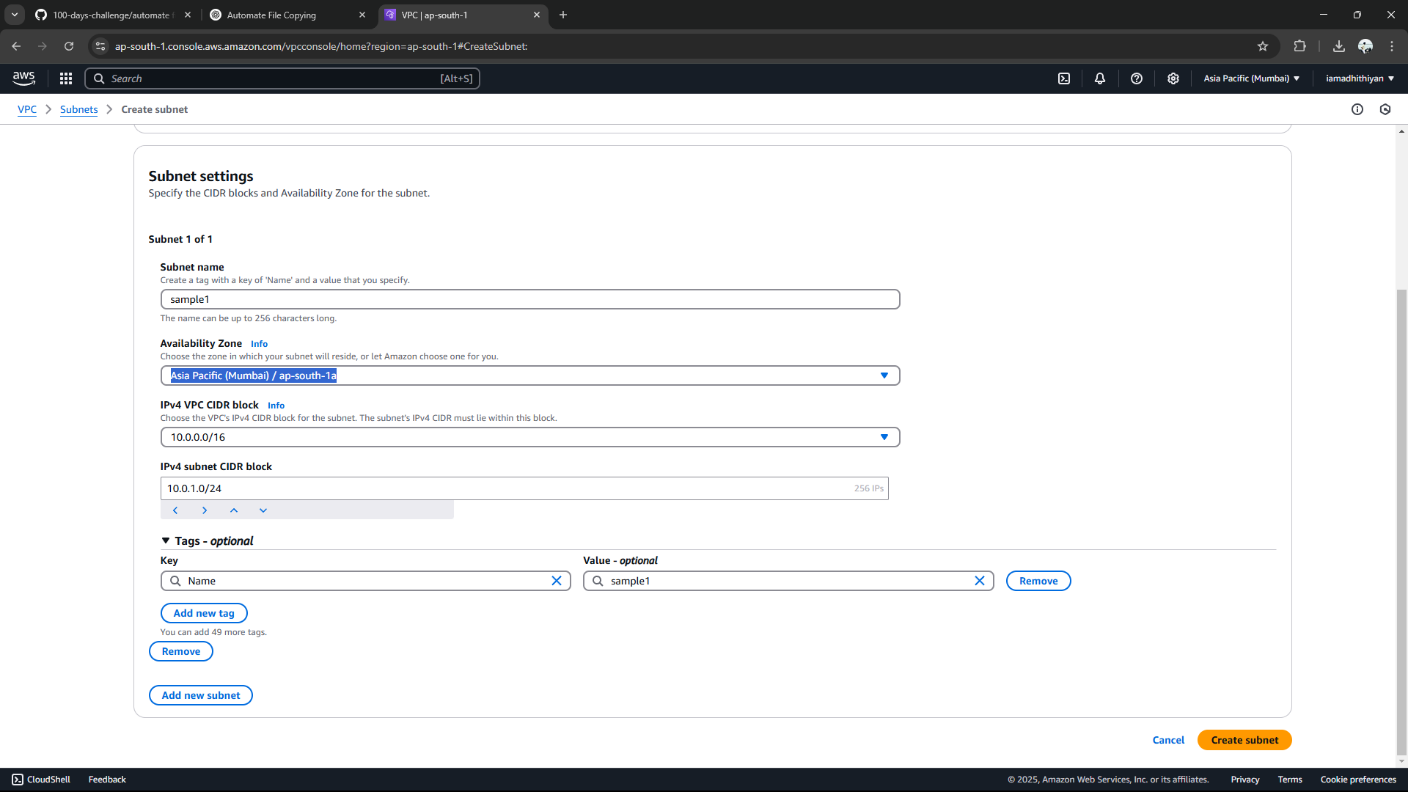
## Step 2:

**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:**

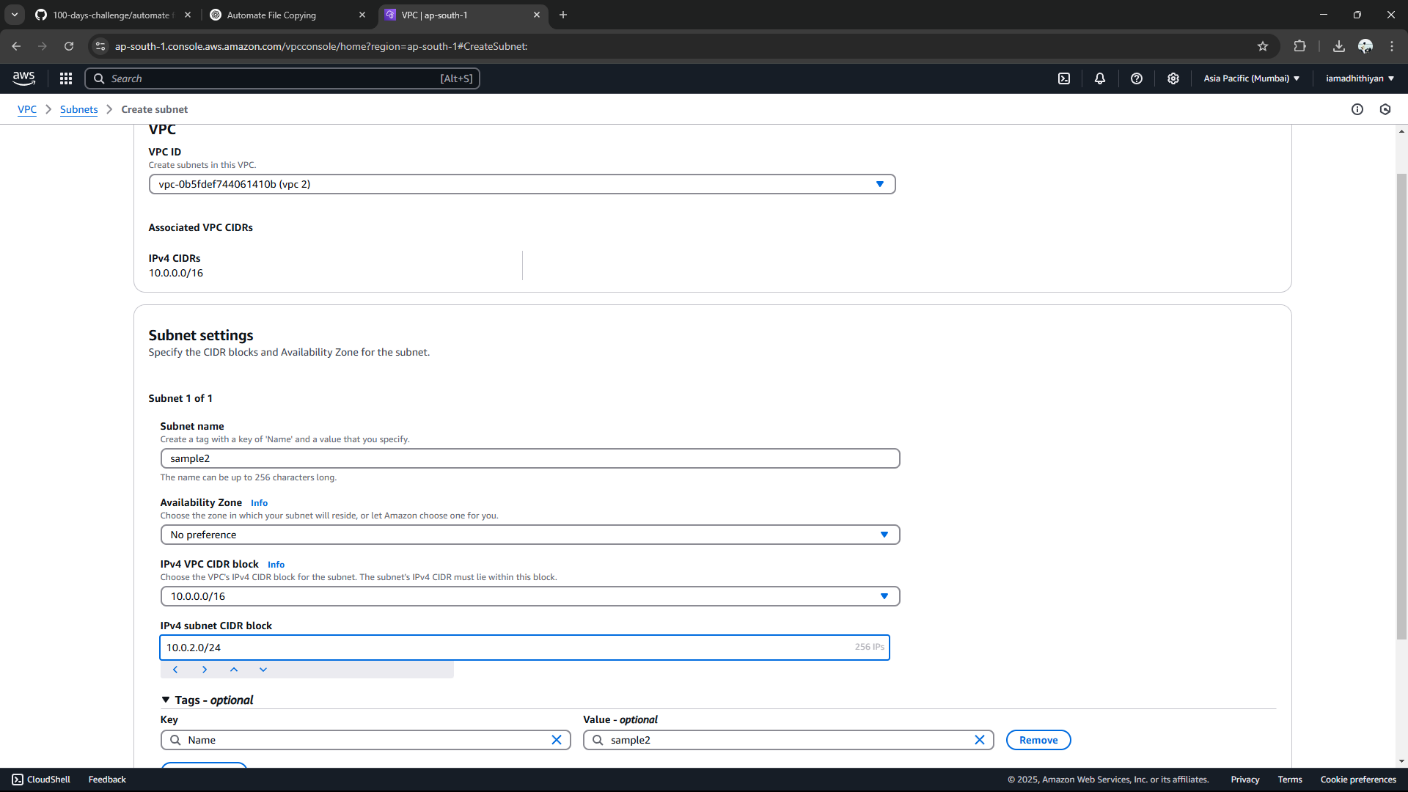
**Subnet 1 (Private-Subnet-A)**

**IPv4 CIDR: 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.

## 

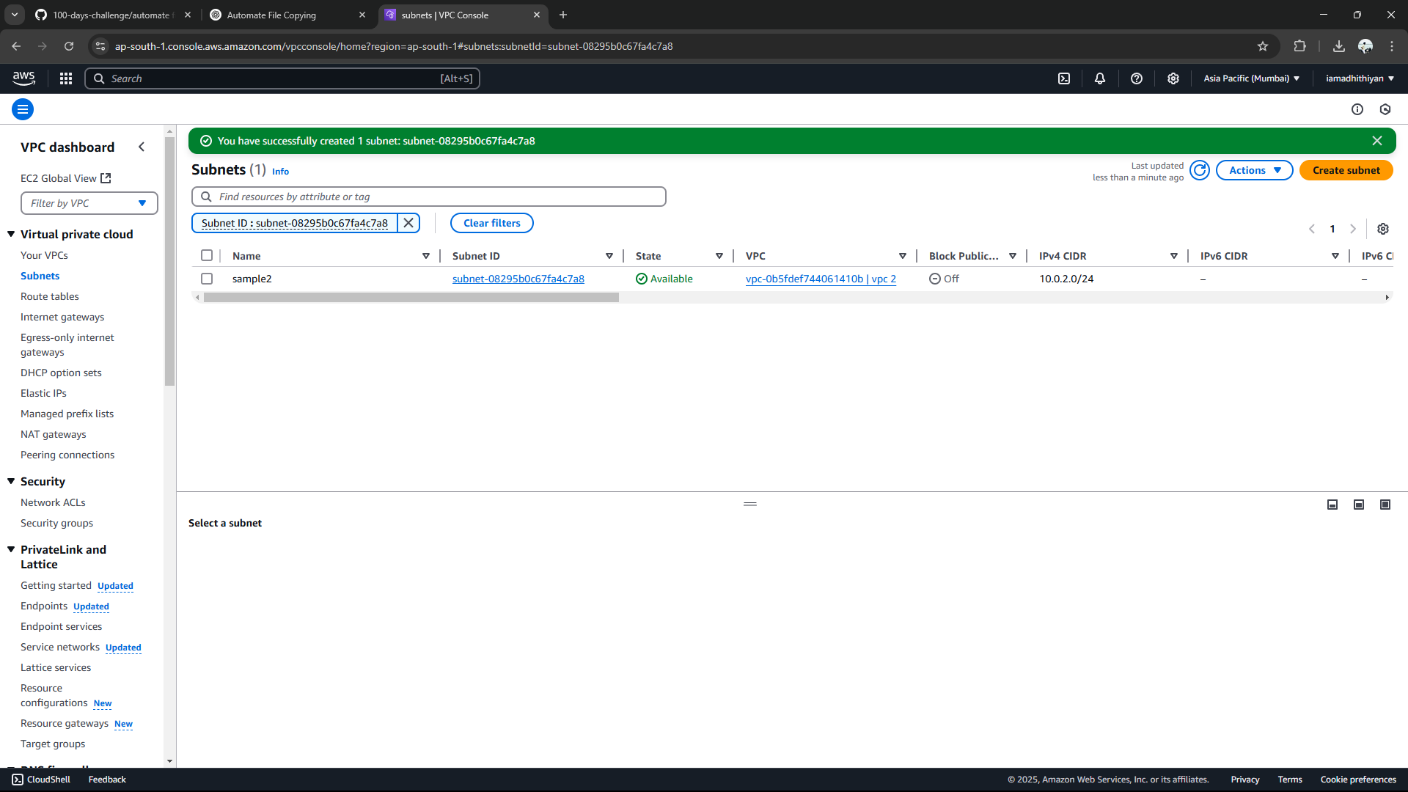
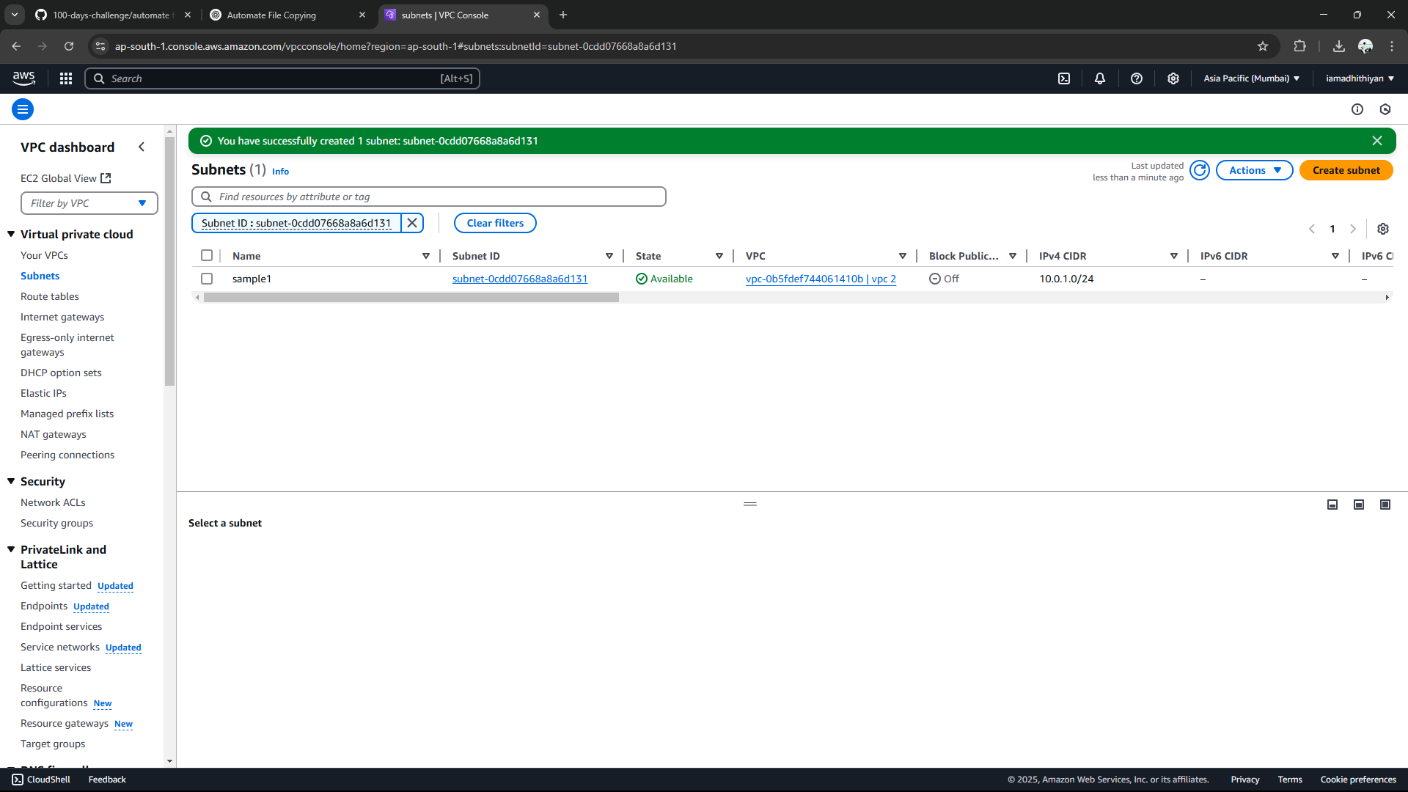
## Step 5:

**Associate the subnets:**

Go to Subnet Associations → Click Edit subnet associations.

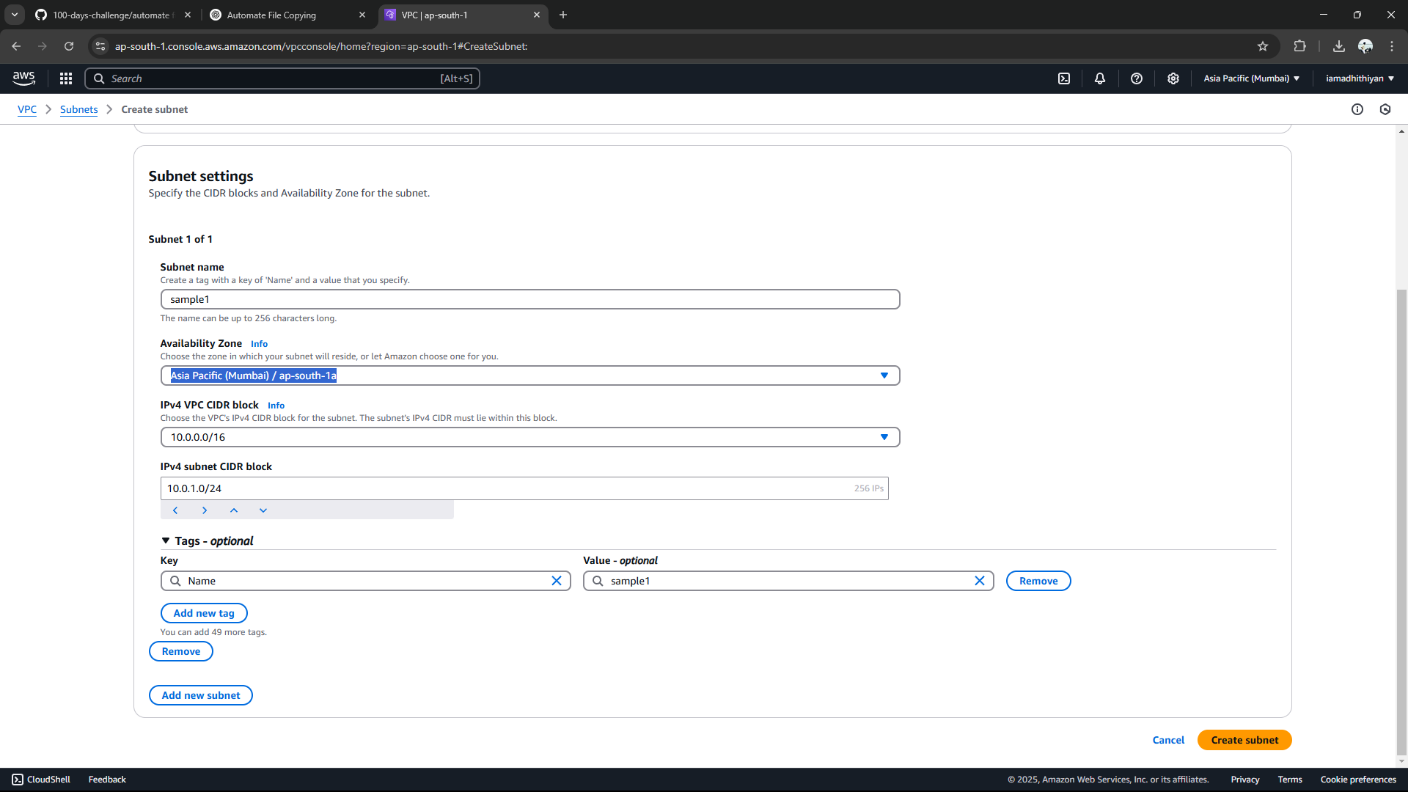
Select Private-Subnet-A and Private-Subnet-B.

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.).

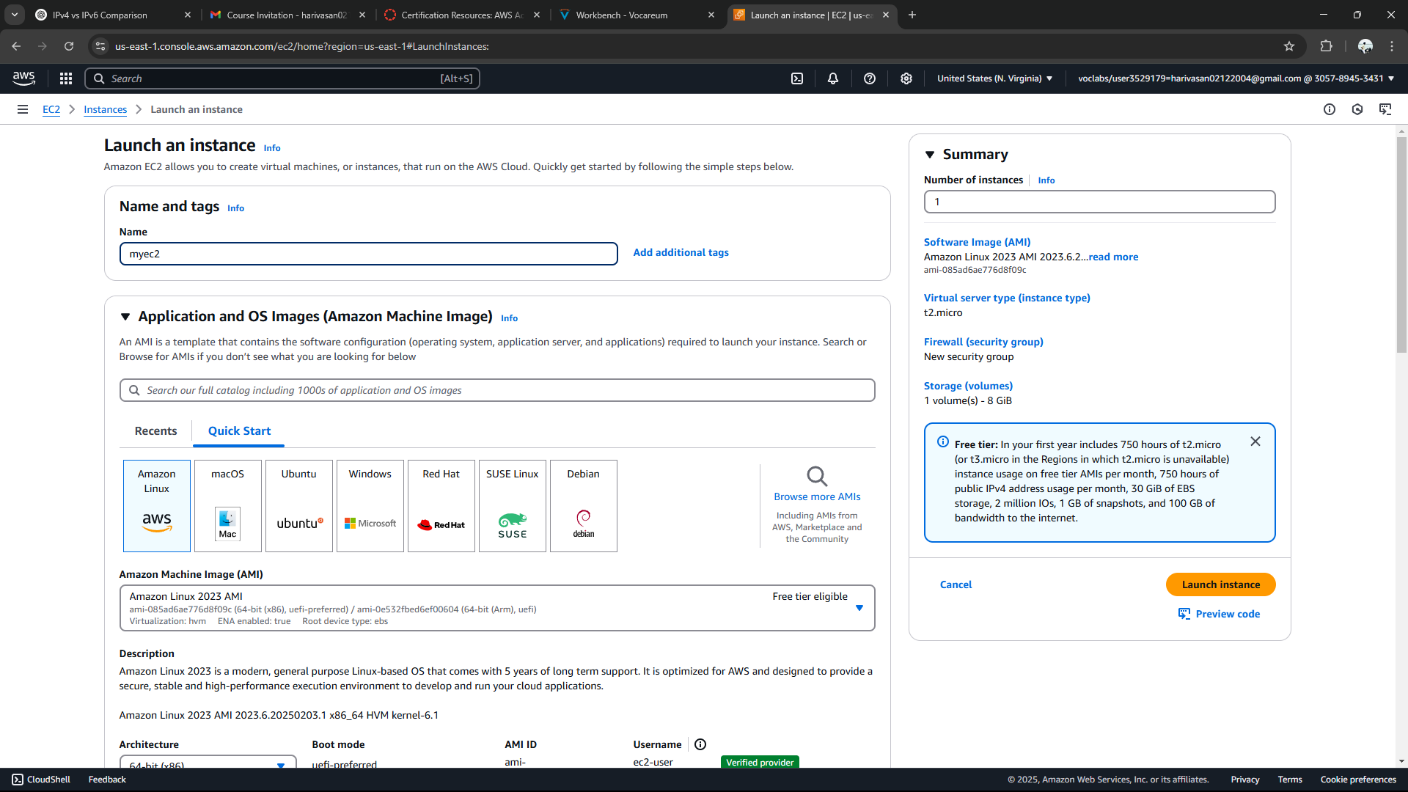
3. Choose an Instance Type (e.g., t2.micro).

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.

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.

**Expected Outcome:**

By completing these steps, you will have:

* A securely isolated VPC, separate from other networks.
* Multiple subnets for your instances, including at least one public subnet with internet connectivity.
* Well-configured routing to enable seamless internal communication between subnets.