

## **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 : Nevesh Gokul M J

Department: CSE

# 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

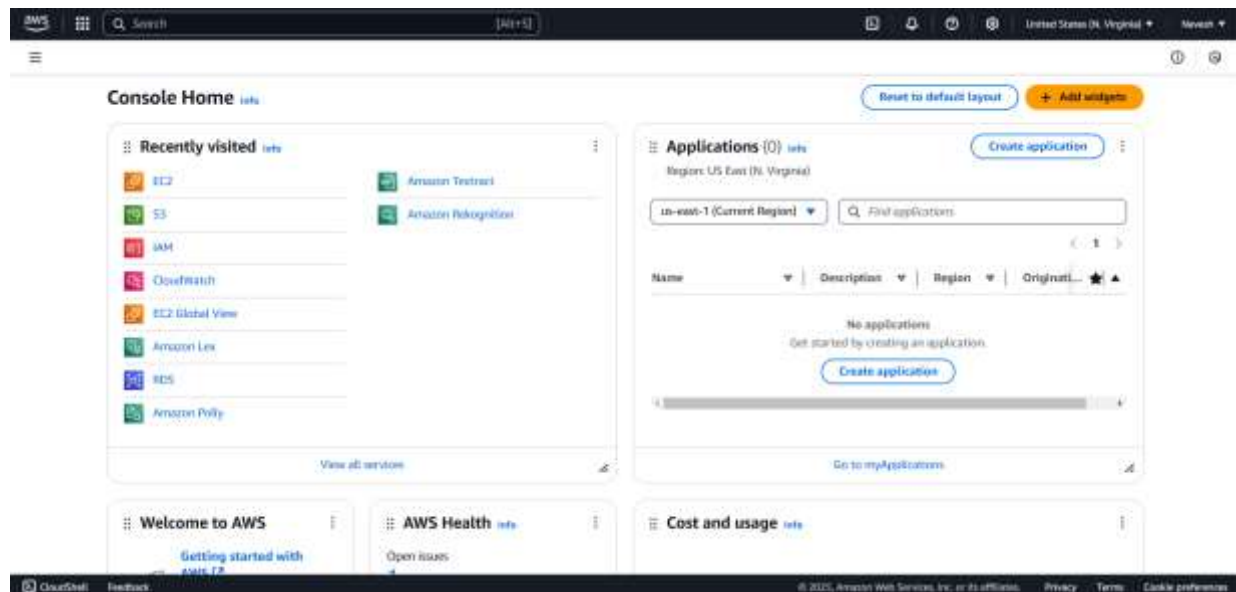
# Importance

- **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 subnet 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](#).
2. Enter your username and password to log in



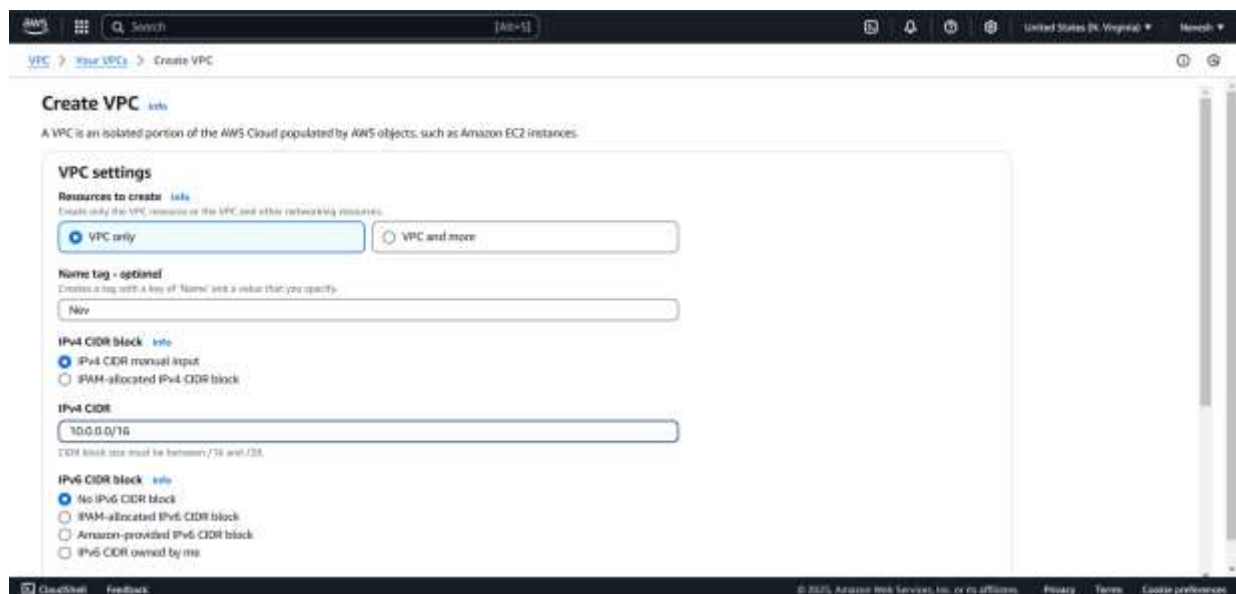
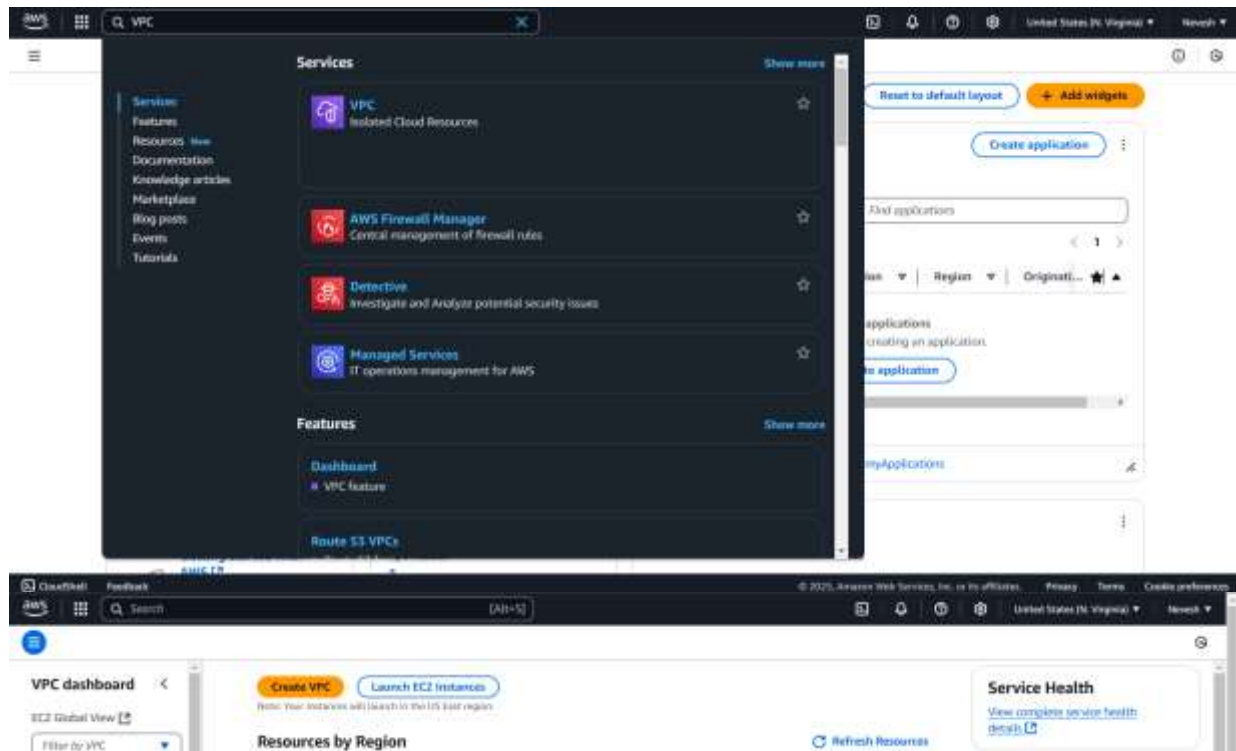
## Step 2:

### 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**

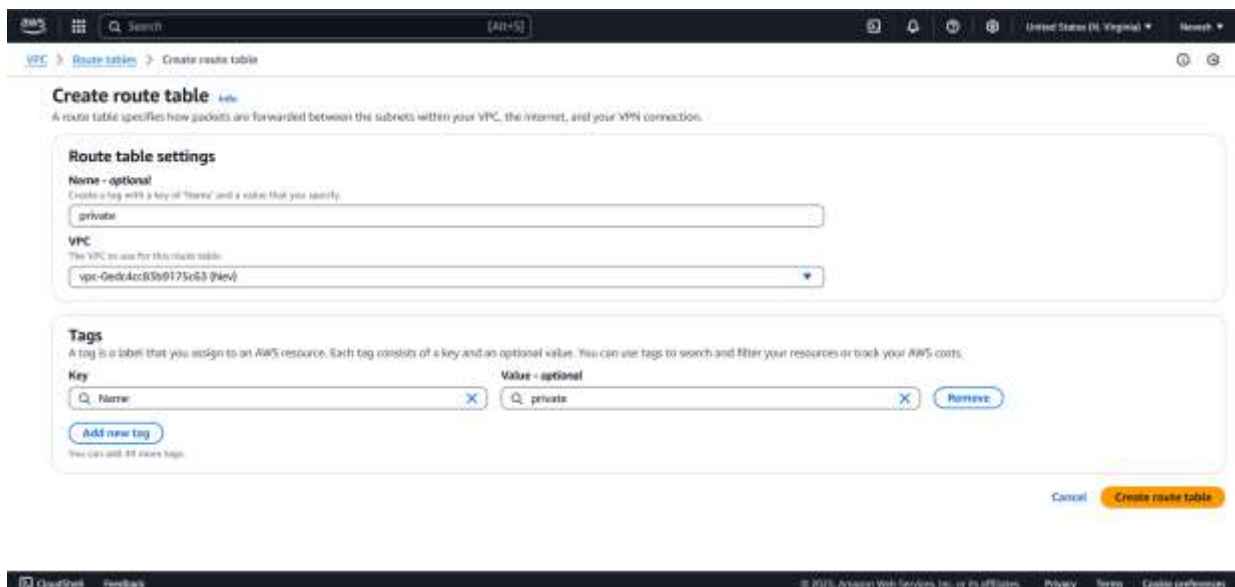
The screenshot shows the 'Create subnet' page in the AWS Management Console. The 'VPC' section shows 'VPC ID' as 'vpc-080d535548e526bb5 (New)'. The 'Associated VPC CIDRs' section shows 'IPv4 CIDRs' as '10.0.0.0/28'. The 'Subnet settings' section shows 'Subnet name' as 'sub-1' and 'Availability Zone' as 'us-east-1a'. The page includes a 'Create subnet' button and a 'Feedback' link.

The screenshot shows the 'Create subnet' page in the AWS Management Console. The 'VPC' section shows 'VPC ID' as 'vpc-080d535548e526bb5 (New)'. The 'Associated VPC CIDRs' section shows 'IPv4 CIDRs' as '10.0.0.0/28'. The 'Subnet settings' section shows 'Subnet name' as 'sub-2' and 'Availability Zone' as 'us-east-1a'. The page includes a 'Create subnet' button and a 'Feedback' link.

## 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.

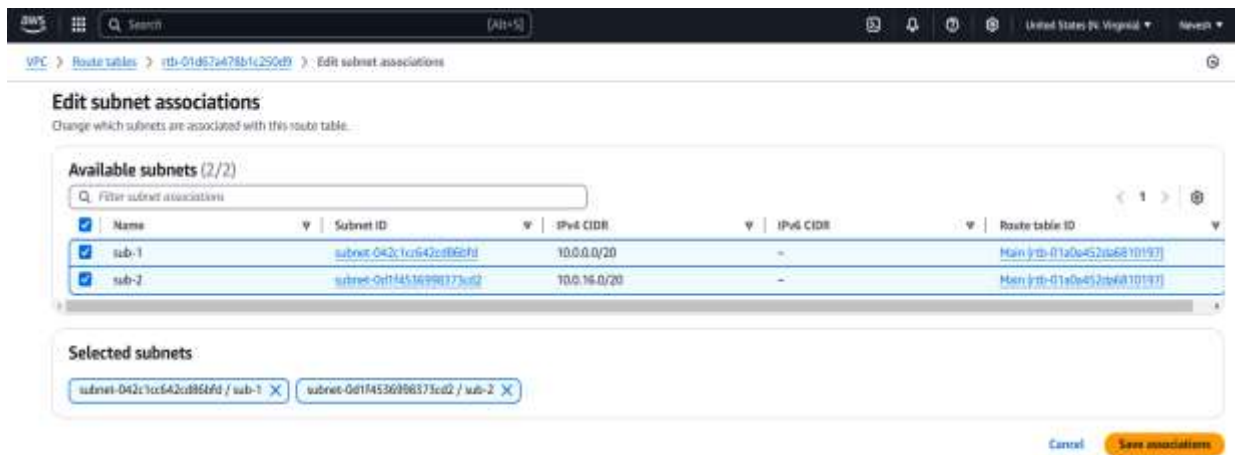
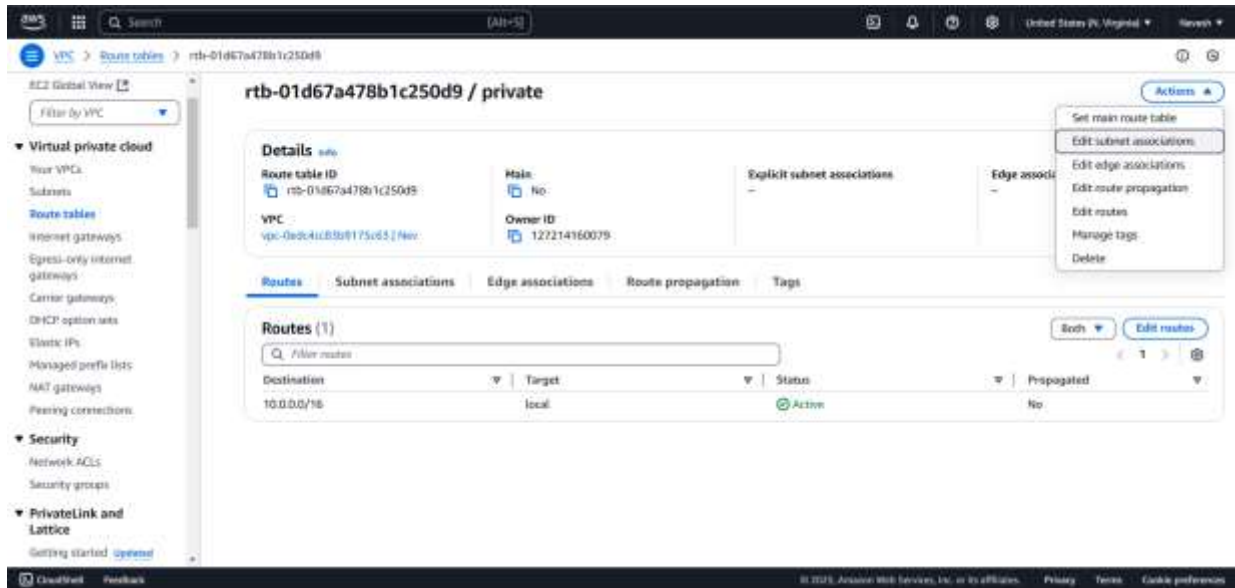


The screenshot shows the AWS Management Console interface for creating a new route table. The breadcrumb navigation at the top indicates the path: VPC > Route tables > Create route table. The main heading is 'Create route table' with a small 'Help' link. Below the heading is a descriptive sentence: 'A route table specifies how packets are forwarded between the subnets within your VPC, the Internet, and your VPN connection.' The form is divided into two main sections: 'Route table settings' and 'Tags'. In the 'Route table settings' section, there is a 'Name - optional' field with the value 'private' entered, and a 'VPC' dropdown menu showing 'vpc-GesdAcc809175c63 (New)'. The 'Tags' section includes a description of tags and a table with two columns: 'Key' and 'Value - optional'. One tag is already added with the key 'Name' and the value 'private'. There are buttons for 'Add new tag' and 'Remove'. At the bottom right of the form are 'Cancel' and 'Create route table' buttons. The footer of the console shows 'CloudFirst', 'Feedback', and copyright information for Amazon Web Services.

## Step 5:

### Associate the subnets:

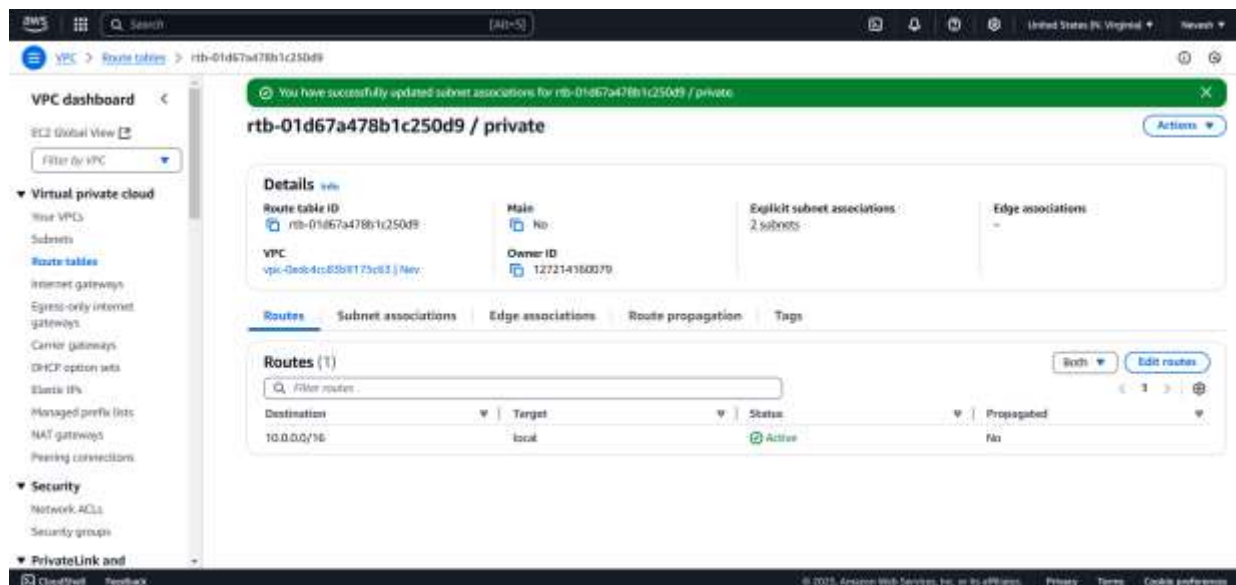
- Go to Subnet Associations → Click Edit subnet associations.
- Select Private-Subnet-A and Private-Subnet-B.
- Click Save associations.



## Step 6:

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

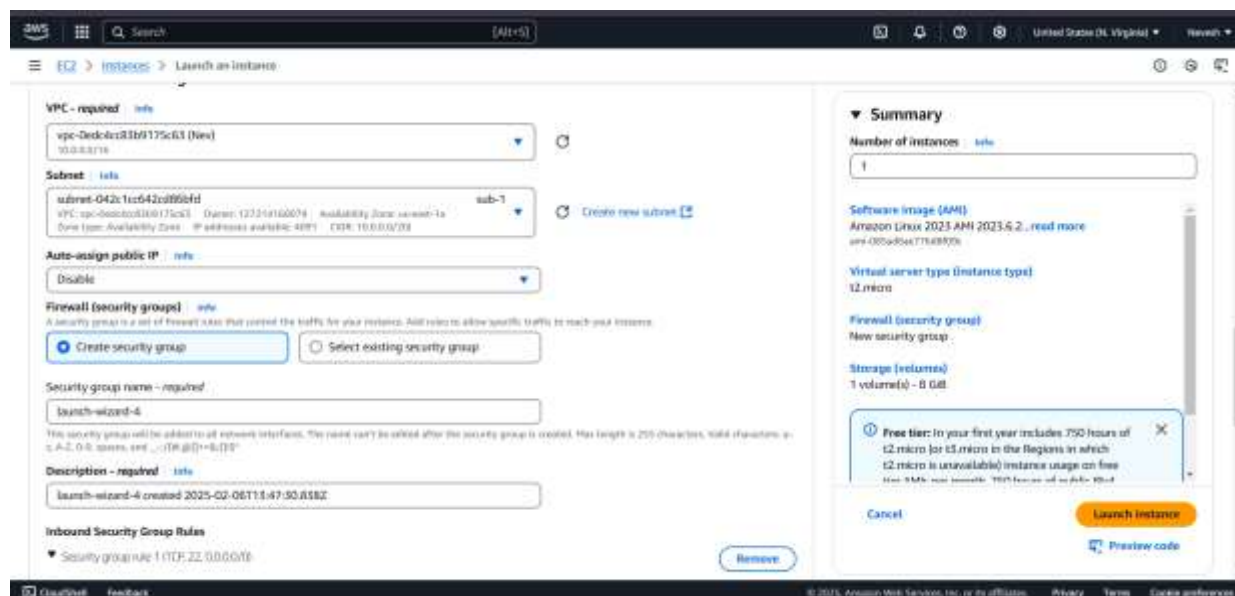
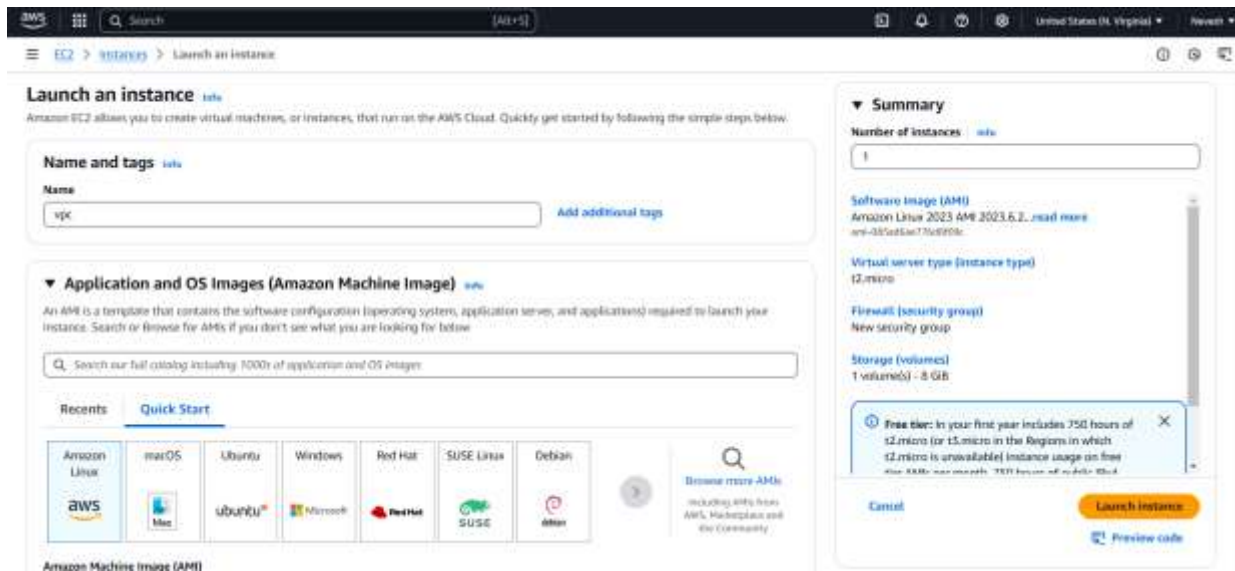




## Step 7:

### 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 subnet