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 :Shalini D Department: IT

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

Introduction

Creating a Virtual Private Cloud (VPC) in the cloud involves defining a logically isolated network for your resources, dividing it into smaller segments called subnets (public and private), and configuring routing tables for internal communication. By establishing a VPC with an appropriate CIDR block, deploying instances in both public and private subnets, associating routing tables for traffic control, and ensuring security measures such as security groups and network ACLs, you enable secure and efficient internal communication between instances while isolating private instances from the internet. For additional resilience, distribute subnets across different availability zones.

Objectives

The objective of creating a Virtual Private Cloud (VPC) is to establish a secure, isolated network environment for your cloud resources, enabling seamless internal communication between instances in various subnets while maintaining strict control over traffic flow and security. This setup ensures that private instances are isolated from the internet, enhances security through controlled access, and supports scalable and resilient infrastructure by distributing subnets across multiple availability zones.

Importance

Creating a Virtual Private Cloud (VPC) is critically important because it provides a secure, isolated environment for managing your cloud resources. This ensures that sensitive data remains protected and private instances are not exposed to the internet, thereby reducing the risk of unauthorized access and potential cyber-attacks. Additionally, a VPC allows you to control and monitor traffic flow, enforce strict security policies, and optimize network performance. By using a VPC, you also achieve higher availability and fault tolerance by distributing subnets across multiple availability zones, ensuring that your infrastructure remains resilient and robust even in the face of failures or outages.

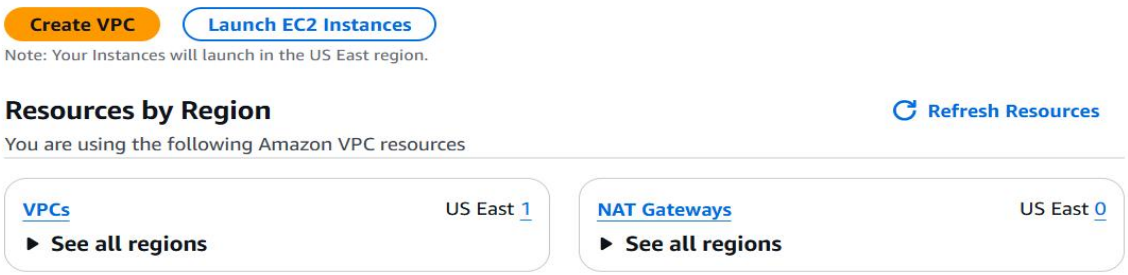
Step-by-Step Overview

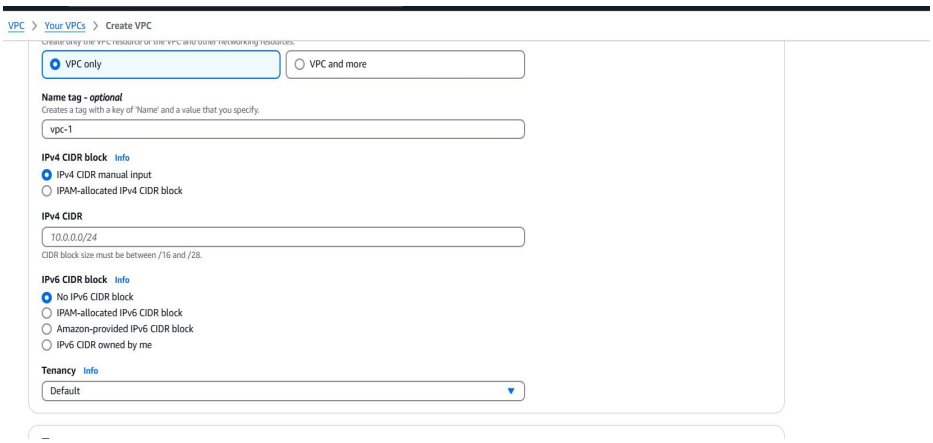
Step 1:

Navigate to the VPC Dashboard

Create a VPC

Click "Create."

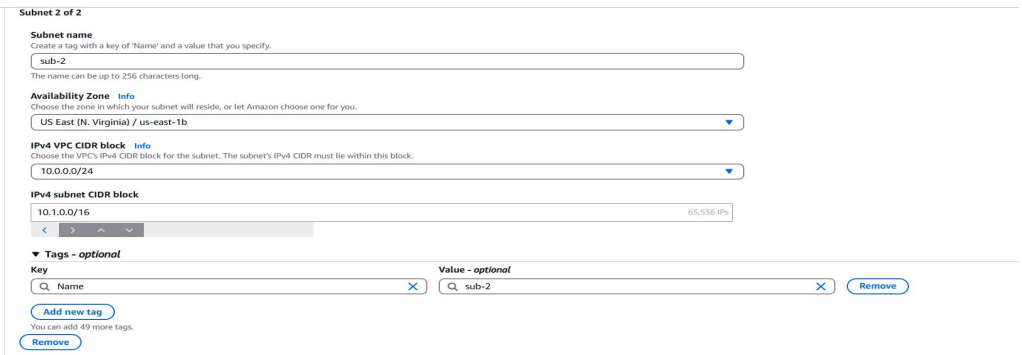




Step 2:

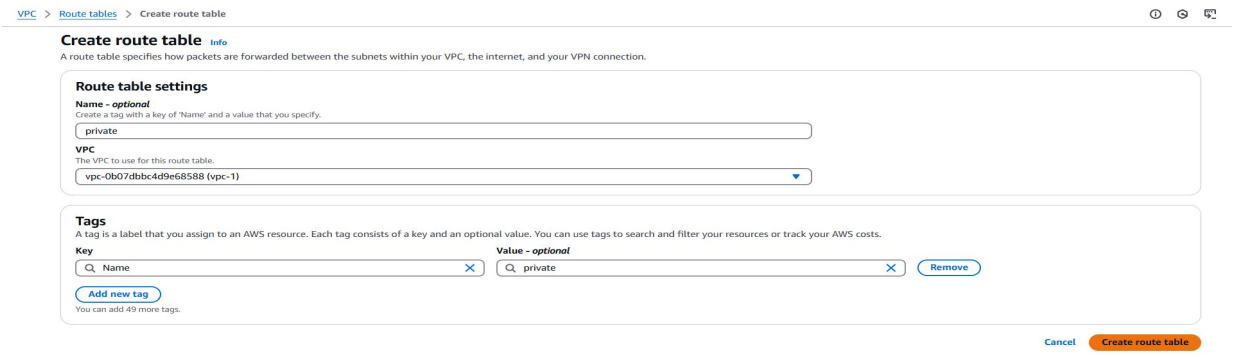
Create Subnets

Create two subnets:



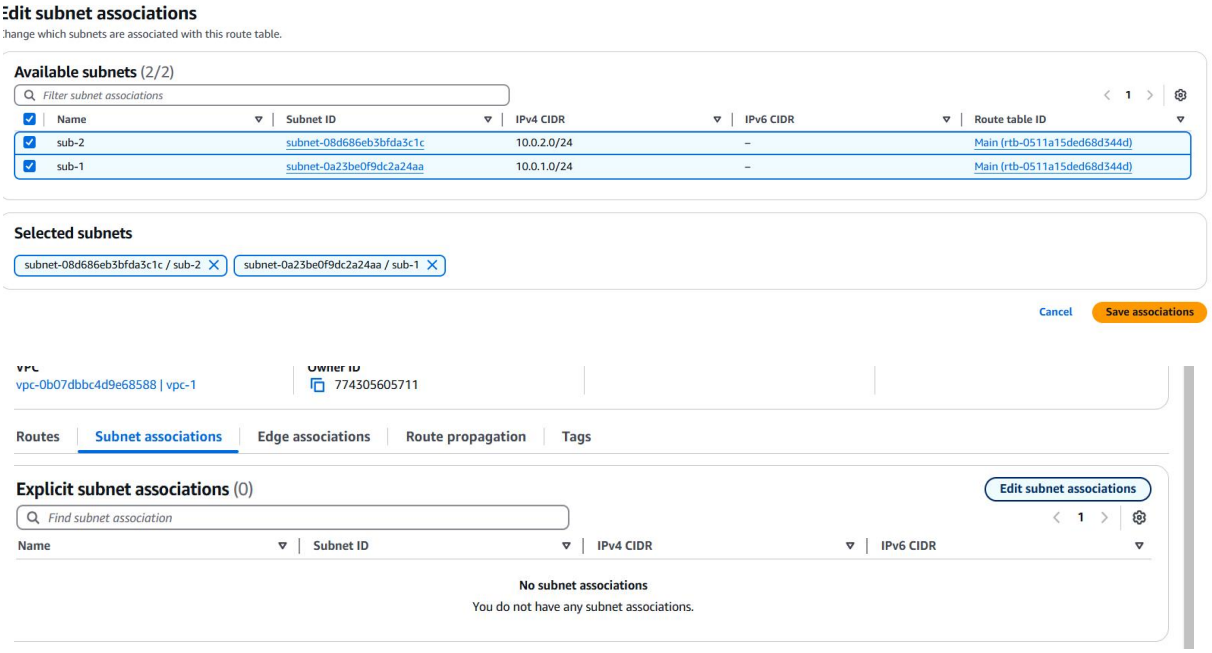
Step 3:

Configure Route Tables for Internal Communication



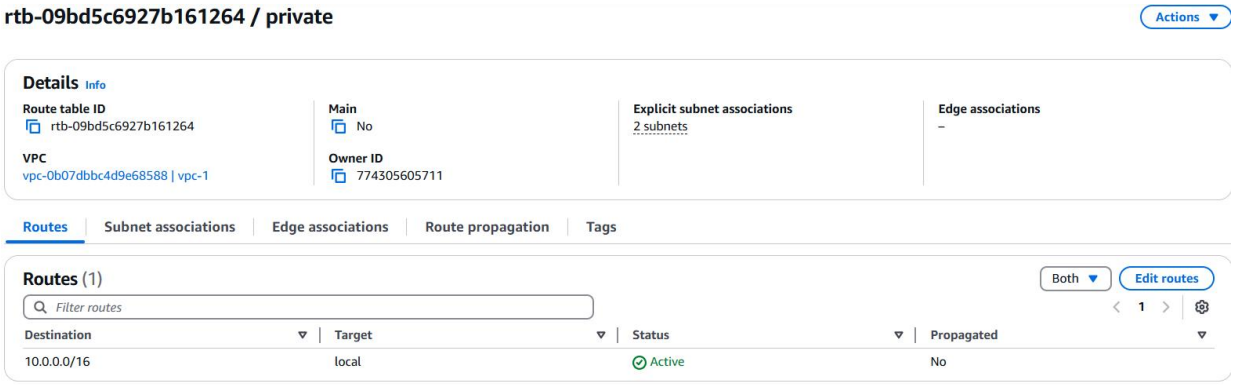
Step 4:

Associate the subnets:



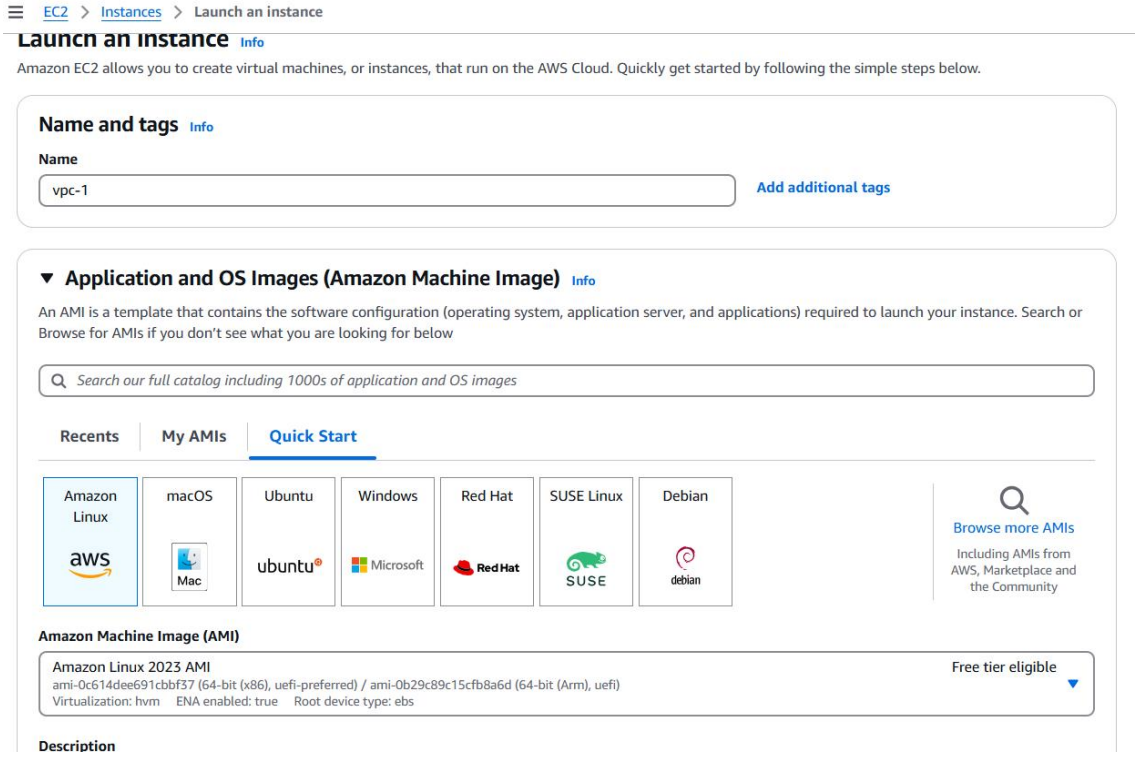
Step 6:

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



Step 7:

Launch Instances in Private Subnets



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.