

## **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

# 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."

[Create VPC](#) [Launch EC2 Instances](#)

Note: Your Instances will launch in the US East region.

### Resources by Region

[Refresh Resources](#)

You are using the following Amazon VPC resources

[VPCs](#) US East [1](#)  
▶ [See all regions](#)

[NAT Gateways](#) US East [0](#)  
▶ [See all regions](#)

VPC > Your VPCs > Create VPC

Create only one VPC resource or the VPC and other networking resources.

☒ VPC only ☐ VPC and more

**Name tag - optional**  
Creates a tag with a key of 'Name' and a value that you specify.

**IPv4 CIDR block** [Info](#)  
☒ IPv4 CIDR manual input  
☐ IPAM-allocated IPv4 CIDR block

**IPv4 CIDR**  
  
CIDR block size must be between /16 and /28.

**IPv6 CIDR block** [Info](#)  
☒ No IPv6 CIDR block  
☐ IPAM-allocated IPv6 CIDR block  
☐ Amazon-provided IPv6 CIDR block  
☐ IPv6 CIDR owned by me

**Tenancy** [Info](#)

## Step 2:

### Create Subnets

Create two subnets:

Subnet 2 of 2

**Subnet name**  
Create a tag with a key of 'Name' and a value that you specify.  
  
The name can be up to 256 characters long.

**Availability Zone** [Info](#)  
Choose the zone in which your subnet will reside, or let Amazon choose one for you.

**IPv4 VPC CIDR block** [Info](#)  
Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.

**IPv4 subnet CIDR block**  
 65,536 IPs

**Tags - optional**

| Key                               | Value - optional                   |
|-----------------------------------|------------------------------------|
| <input type="text" value="Name"/> | <input type="text" value="sub-2"/> |

[Add new tag](#) [Remove](#)

You can add 49 more tags.

## Step 3:

### Configure Route Tables for Internal Communication

VPC > Route tables > Create route table

**Create route table** [Info](#)

A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.

**Route table settings**

**Name - optional**  
Create a tag with a key of 'Name' and a value that you specify.

private

**VPC**  
The VPC to use for this route table.

vpc-0b07dbbc4d9e68588 (vpc-1)

**Tags**  
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

**Key**

Q Name X

**Value - optional**

Q private X Remove

Add new tag

You can add 49 more tags.

Cancel Create route table

## Step 4:

### Associate the subnets:

#### Edit subnet associations

Change which subnets are associated with this route table.

**Available subnets (2/2)**

Filter subnet associations

|                                     | Name  | Subnet ID                | IPv4 CIDR   | IPv6 CIDR | Route table ID               |
|-------------------------------------|-------|--------------------------|-------------|-----------|------------------------------|
| <input checked="" type="checkbox"/> | sub-2 | subnet-08d686eb3bfda3c1c | 10.0.2.0/24 | -         | Main (rtb-0511a15ded68d344d) |
| <input checked="" type="checkbox"/> | sub-1 | subnet-0a23be0f9dc2a24aa | 10.0.1.0/24 | -         | Main (rtb-0511a15ded68d344d) |

**Selected subnets**

subnet-08d686eb3bfda3c1c / sub-2 X subnet-0a23be0f9dc2a24aa / sub-1 X

Cancel Save associations

**VPC**  
vpc-0b07dbbc4d9e68588 | vpc-1

**Owner ID**  
774305605711

**Routes** | **Subnet associations** | Edge associations | Route propagation | Tags

**Explicit subnet associations (0)**

Find subnet association

| Name | Subnet ID | IPv4 CIDR | IPv6 CIDR |
|------|-----------|-----------|-----------|
|------|-----------|-----------|-----------|

No subnet associations  
You do not have any subnet associations.

Edit subnet associations

## Step 6:

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

rtb-09bd5c6927b161264 / private

Actions

#### Details

Route table ID

rtb-09bd5c6927b161264

VPC

vpc-0b07dbbc4d9e68588 | vpc-1

Main

No

Owner ID

774305605711

Explicit subnet associations

2 subnets

Edge associations

–

Routes

Subnet associations

Edge associations

Route propagation

Tags

#### Routes (1)

Filter routes

Both

Edit routes

< 1 >

| Destination | Target | Status | Propagated |
|-------------|--------|--------|------------|
| 10.0.0.0/16 | local  | Active | No         |

## Step 7: Launch Instances in Private Subnets

EC2 > Instances > Launch an instance

### Launch an instance

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

#### Name and tags

Name

vpc-1

Add additional tags

#### Application and OS Images (Amazon Machine Image)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Search our full catalog including 1000s of application and OS images

Recents

My AMIs

Quick Start



Browse more AMIs  
Including AMIs from  
AWS, Marketplace and  
the Community

#### Amazon Machine Image (AMI)

Amazon Linux 2023 AMI  
ami-0c614dee691cbbf37 (64-bit (x86), uefi-preferred) / ami-0b29c89c15cfb8a6d (64-bit (Arm), uefi)  
Virtualization: hvm ENA enabled: true Root device type: ebs

Free tier eligible

Description

## 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.

