

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 : Priyanka Mary A
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

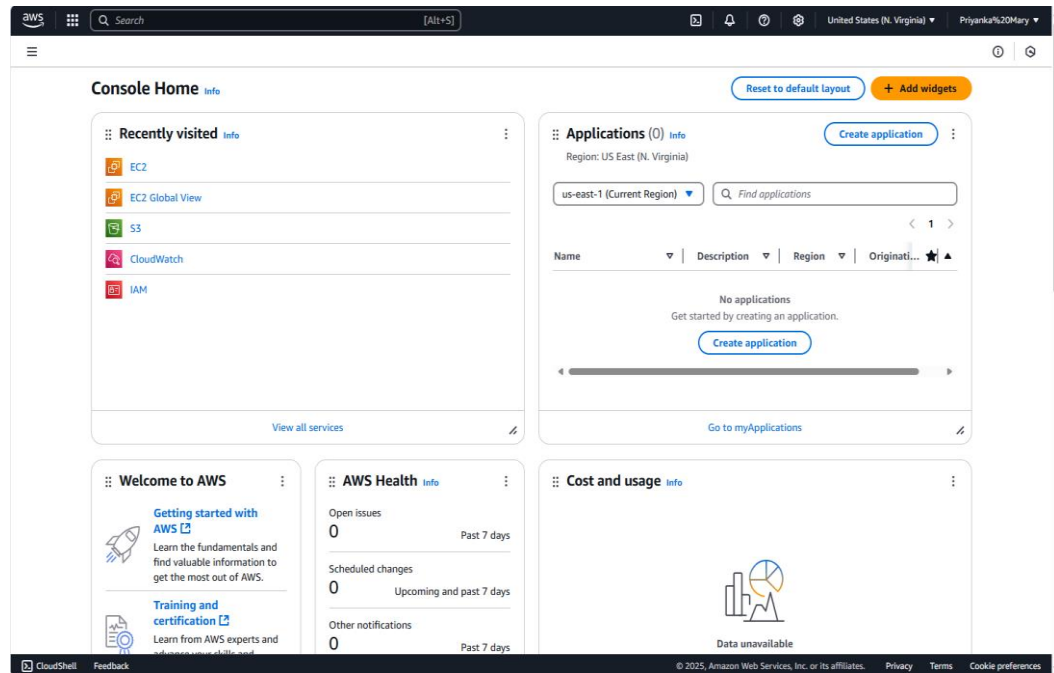
Importance

- **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



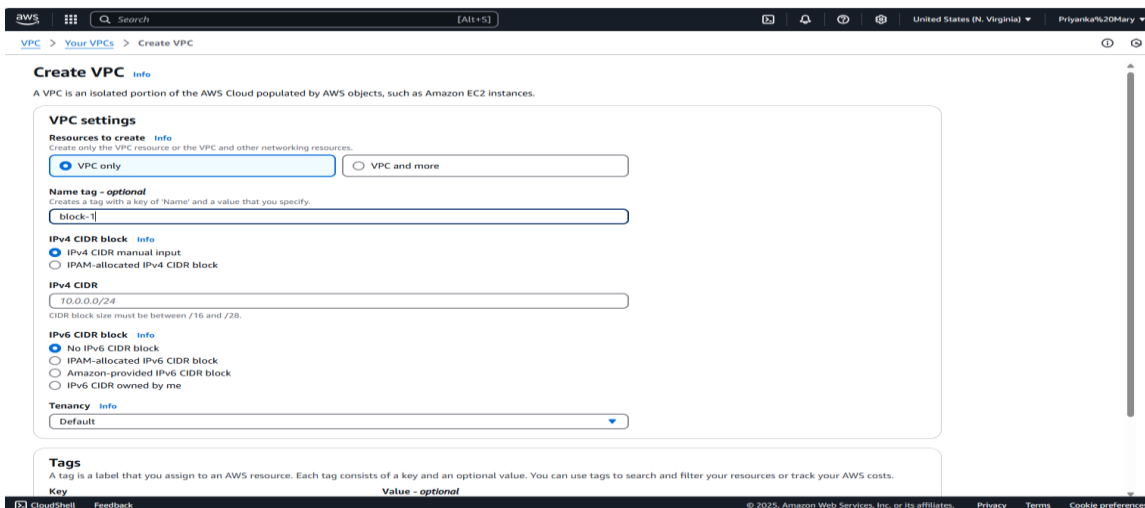
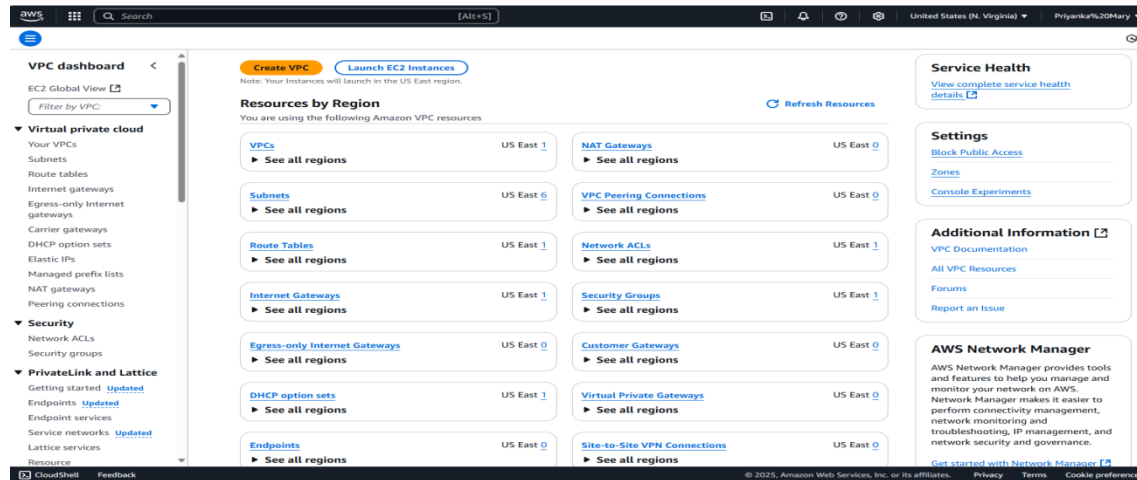
Step 2:

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 for 'Subnet 1 of 2'. The page is titled 'Subnet settings' and instructs the user to 'Specify the CIDR blocks and Availability Zone for the subnet.' The form includes the following fields:

- Subnet name:** A text input field containing 'sub-1'.
- Availability Zone:** A dropdown menu showing 'US East (N. Virginia) / us-east-1a'.
- IPv4 VPC CIDR block:** A dropdown menu showing '10.0.0.0/16'.
- IPv4 subnet CIDR block:** A text input field containing '10.0.0.0/24' with a '256 IPs' indicator.
- Tags - optional:** A section with a table for adding tags. The table has two columns: 'Key' and 'Value - optional'. A tag is added with 'Name' as the key and 'sub-1' as the value. There are buttons for 'Add new tag', 'Remove', and 'Add new subnet'.

The screenshot shows the 'Create subnet' page in the AWS Management Console for 'Subnet 2 of 2'. The page is titled 'Subnet settings' and instructs the user to 'Specify the CIDR blocks and Availability Zone for the subnet.' The form includes the following fields:

- Subnet name:** A text input field containing 'sub-2'.
- Availability Zone:** A dropdown menu showing 'US East (N. Virginia) / us-east-1b'.
- IPv4 VPC CIDR block:** A dropdown menu showing '10.0.0.0/16'.
- IPv4 subnet CIDR block:** A text input field containing '10.0.0.0/24' with a '256 IPs' indicator.
- Tags - optional:** A section with a table for adding tags. The table has two columns: 'Key' and 'Value - optional'. A tag is added with 'Name' as the key and 'sub-2' as the value. There are buttons for 'Add new tag', 'Remove', and 'Add new subnet'.

At the bottom right of the page, there are two buttons: 'Cancel' and 'Create subnet'.

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 an 'Info' link. Below this, a descriptive sentence states: 'A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.'

The 'Route table settings' section contains two fields: 'Name - optional' with the value 'PrivateRouteTable' and 'VPC' with a dropdown menu showing 'vpc-0d20b6efa0s2ee4b3 (block-1)'. Below this is the 'Tags' section, which includes a 'Key' field with 'Name' and a 'Value - optional' field with 'PrivateRouteTable'. A 'Remove' button is next to the value field, and an 'Add new tag' button is at the bottom left of the tags section. At the bottom right of the form, there are 'Cancel' and 'Create route table' buttons.

Step 5:

Associate the subnets:

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

aws Search [Alt+S] United States (N. Virginia) Priyanka%20Mary

VPC > Route tables > rtb-09b060c09a52c4b07 > Edit subnet associations

Edit subnet associations

Change which subnets are associated with this route table.

Available subnets (2/2)

Filter subnet associations

<input checked="" type="checkbox"/>	Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
<input checked="" type="checkbox"/>	sub-2	subnet-011bfbbefdf10abec	10.0.1.0/24	-	Main (rtb-0ae56547f933e2dd3)
<input checked="" type="checkbox"/>	sub-1	subnet-0029087b67c623b6a	10.0.2.0/24	-	Main (rtb-0ae56547f933e2dd3)

Selected subnets

subnet-011bfbbefdf10abec / sub-2 X subnet-0029087b67c623b6a / sub-1 X

Cancel Save associations

aws Search [Alt+S] United States (N. Virginia) Priyanka%20Mary

VPC > Route tables > rtb-09b060c09a52c4b07

rtb-09b060c09a52c4b07 / PrivateRouteTable

Actions

Details info

Route table ID rtb-09b060c09a52c4b07

VPC vpc-0d20b6efa0a2ee4b3 | block-1

Main No

Owner ID 850995557027

Explicit subnet associations -

Edge associations -

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.

Subnets without explicit associations (2)

The following subnets have not been explicitly associated with any route tables and are therefore associated with the main route table:

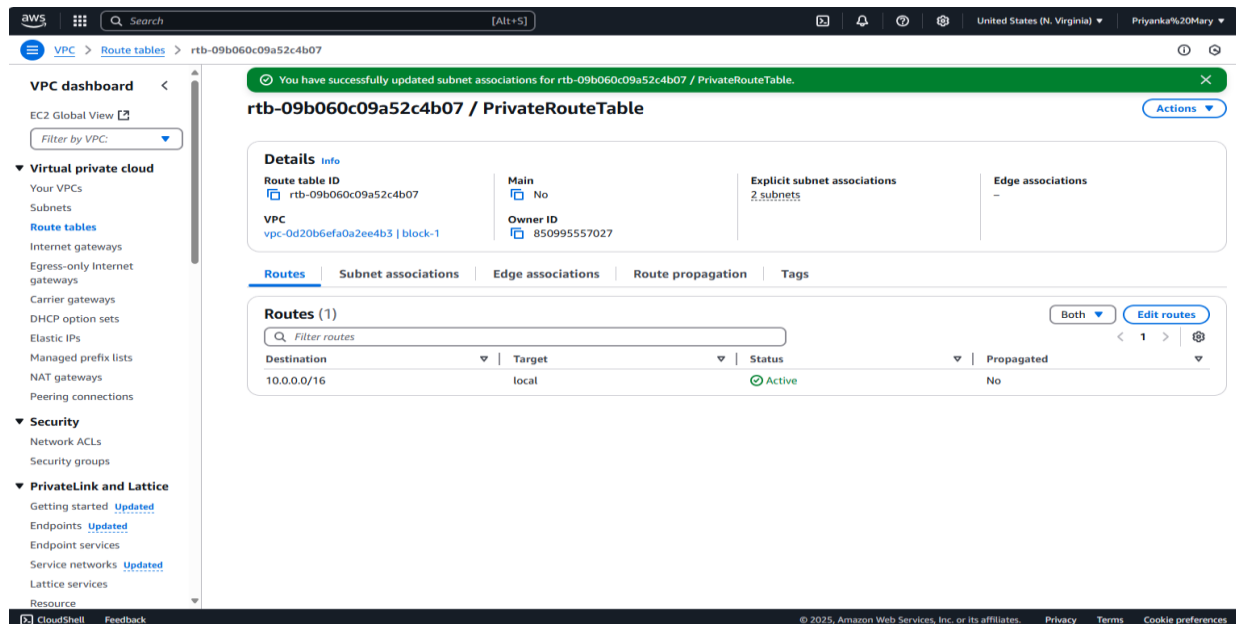
Find subnet association

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
sub-2	subnet-011bfbbefdf10abec	10.0.1.0/24	-
sub-1	subnet-0029087b67c623b6a	10.0.2.0/24	-

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Step 6:

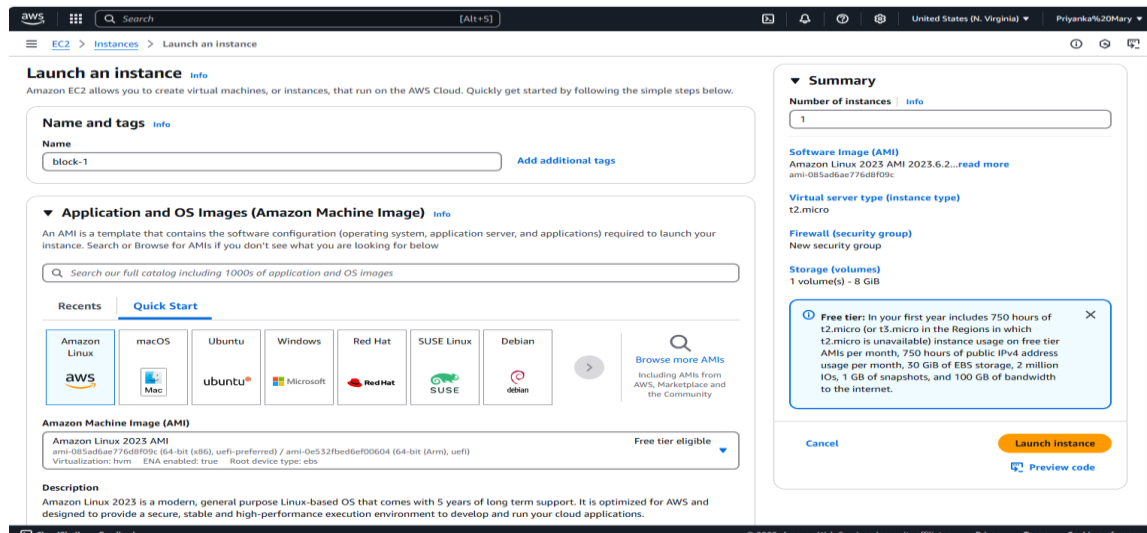
Default route: 10.0.0.0/16 → local (Automatically added).



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 subnets.

