

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 :Jai Riyaz G

Department: ADS

Introduction

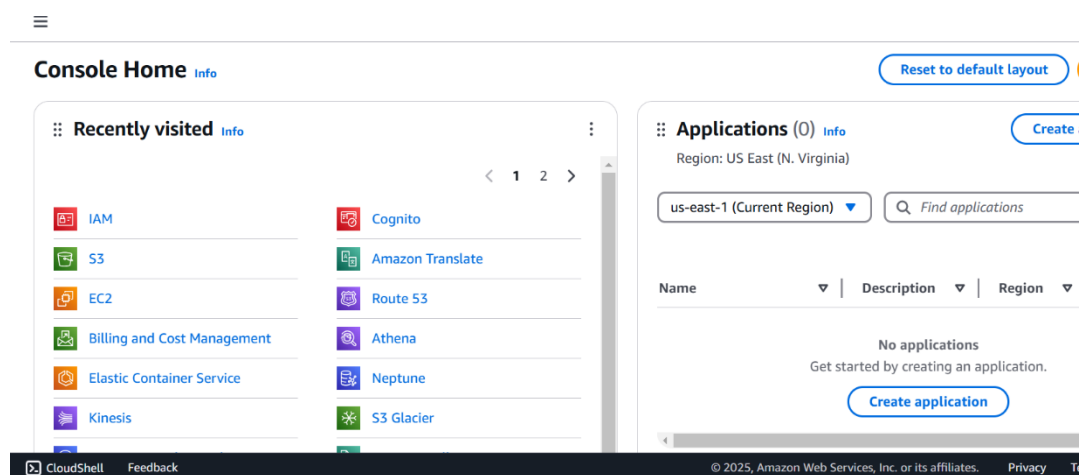
A Virtual Private Cloud (VPC) is a secure and isolated portion of a cloud provider's infrastructure where you can deploy your resources in a controlled environment. Setting up a VPC involves creating subnets, configuring routing, and implementing security measures to manage traffic and access.

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

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."

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

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

Resources by Region

[Refresh Resources](#)

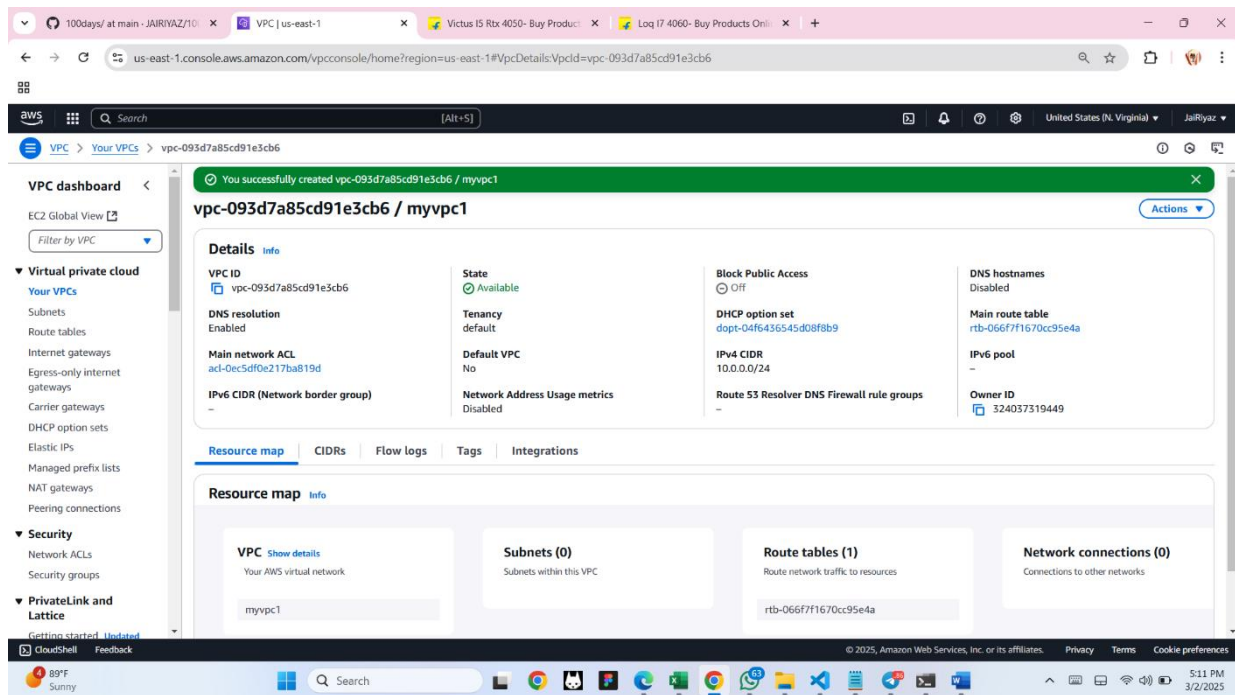
You are using the following Amazon VPC resources

[VPCs](#)US East [1](#)[► See all regions](#)[NAT Gateways](#)US East [0](#)[► See all regions](#)

The screenshot shows the AWS Management Console interface for creating a new VPC. The browser address bar indicates the URL is `us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#CreateVpccreateMode=vpcOnly`. The console header shows the user is logged in as 'JaiRiyaz' in the 'United States (N. Virginia)' region. The main content area is titled 'VPC settings' and includes the following sections:

- Resources to create:** Two radio buttons are present: 'VPC only' (which is selected) and 'VPC and more'.
- Name tag - optional:** A text input field containing the value 'myvpc1'.
- IPv4 CIDR block:** Two radio buttons are present: 'IPv4 CIDR manual input' (selected) and 'IPAM-allocated IPv4 CIDR block'.
- IPv4 CIDR:** A text input field containing the value '10.0.0.0/24'. Below this field, a note states: 'CIDR block size must be between /16 and /28.'
- IPv6 CIDR block:** Three radio buttons are present: 'No IPv6 CIDR block' (selected), 'IPAM-allocated IPv6 CIDR block', and 'Amazon-provided IPv6 CIDR block'.
- Tenancy:** A dropdown menu set to 'Default'.

The footer of the console shows the copyright notice '© 2025, Amazon Web Services, Inc. or its affiliates.' and links for 'Privacy', 'Terms', and 'Cookie preferences'. The system tray at the bottom of the screen shows the date and time as '5:09 PM 3/2/2025'.



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:

Availability Zone: us-east-1a (example)

Subnet 2 (Private-Subnet-B)

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

89°F Sunny 5:14 PM 3/2/2025

us-east-1.console.aws.amazon.com/vpccconsole/home?region=us-east-1#CreateSubnet:

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.

vpc

vpc-0b07dbbc4d9e68588 | vpc-1

owner id

774305605711

Routes

Subnet associations

Edge associations

Route propagation

Tags

Explicit subnet associations (0)

Edit subnet associations

Find subnet association

Name

Subnet ID

IPv4 CIDR

IPv6 CIDR

No subnet associations
You do not have any subnet associations.

Edit subnet associations

Change which subnets are associated with this route table.

Available subnets (2/2)

Filter subnet associations

☒

sub-2

subnet-08d686eb3bfd3c1c

10.0.2.0/24

-

Main (rtb-0511a15ded68d344d)

☒

sub-1

subnet-0a23be0f9dc2a24aa

10.0.1.0/24

-

Main (rtb-0511a15ded68d344d)

Selected subnets

subnet-08d686eb3bfd3c1c / sub-2

subnet-0a23be0f9dc2a24aa / sub-1

Cancel

Save associations

Step 6:

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

rtb-09bd5c6927b161264 / private Actions ▼

Details Info
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) Both ▼ Edit routes

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No

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.

