

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:CHELSIAH M

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

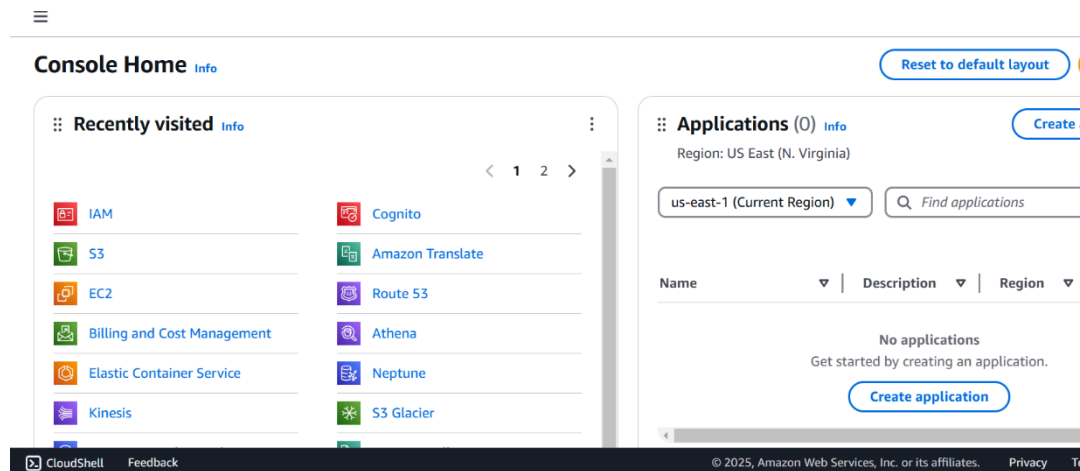
Importance

- **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."

[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 displays the AWS Management Console interface for a VPC. The top navigation bar shows the AWS logo, a search bar, and the current region (United States (N. Virginia)) and user (Kirthika S). The left sidebar contains the navigation menu with categories like Virtual private cloud, Security, and Network. The main content area shows the details of the VPC `vpc-0057f273d9bb76918 / kirthivpc`. A green notification bar at the top indicates that the VPC was successfully created. The details section is organized into a grid with the following information:

Details	
VPC ID vpc-0057f273d9bb76918	State Available
DNS resolution Enabled	Tenancy default
Main network ACL acl-026ee4ee1733e9d74	Default VPC No
IPv6 CIDR (Network border group) -	Network Address Usage metrics Disabled
Block Public Access Off	DHCP option set dopt-00efdc515d3aab0cb
DNS hostnames Disabled	IPv4 CIDR 10.0.0.0/16
Main route table rtb-0ddcc8fef99d0a057	Route 53 Resolver DNS Firewall rule groups -
IPv6 pool -	Owner ID 418272757660

Below the details, there are tabs for **Resource map**, **CIDRs**, **Flow logs**, **Tags**, and **Integrations**. The **Resource map** tab is active, showing a visual representation of the VPC resources: VPC (with a link to show details), Subnets (0), Route tables (1), and Network interfaces (0).

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 breadcrumb navigation is 'VPC > Subnets > Create subnet'. The page title is 'Create subnet' with an 'info' link. The 'VPC' section shows 'VPC ID' as 'vpc-0057f273d9bb76918 (kirthivpc)' and 'Associated VPC CIDRs' as 'IPv4 CIDRs 10.0.0.0/16'. The 'Subnet settings' section has a subtitle 'Specify the CIDR blocks and Availability Zone for the subnet.' and 'Subnet 1 of 1'. The 'Subnet name' field contains 'subnet1'.

Create subnet [info](#)

VPC

VPC ID
Create subnets in this VPC.
vpc-0057f273d9bb76918 (kirthivpc) ▼

Associated VPC CIDRs

IPv4 CIDRs
10.0.0.0/16

Subnet settings
Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

Subnet name
Create a tag with a key of 'Name' and a value that you specify.
subnet1
The name can be up to 256 characters long.

The screenshot shows the 'Create subnet' page in the AWS Management Console for Subnet 2. The breadcrumb navigation is 'VPC > Subnets > Create subnet'. The page title is 'Create subnet' with an 'info' link. The 'Add new tag' button is visible. The 'Subnet 2 of 2' section shows 'Subnet name' as 'subnet2'. The 'Availability Zone' is 'US East (N. Virginia) / us-east-1b'. The 'IPv4 VPC CIDR block' is '10.0.0.0/16'. The 'IPv4 subnet CIDR block' is '10.0.2.0/24' with a '256 IPs' indicator. The 'Tags - optional' section is collapsed.

[Add new tag](#)
You can add 49 more tags.
[Remove](#)

Subnet 2 of 2

Subnet name
Create a tag with a key of 'Name' and a value that you specify.
subnet2
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.
US East (N. Virginia) / us-east-1b ▼

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.
10.0.0.0/16 ▼

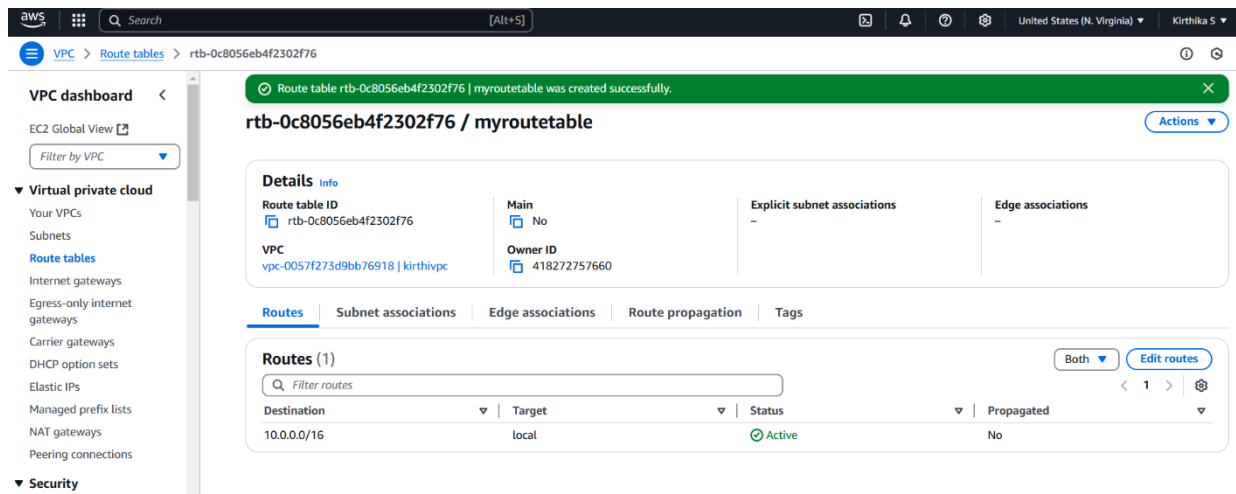
IPv4 subnet CIDR block
10.0.2.0/24 256 IPs
< > ^ v

▼ **Tags - optional**

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.

Edit subnet associations
Change which subnets are associated with this route table.

Available subnets (2/2)

<input checked="" type="checkbox"/>	Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
<input checked="" type="checkbox"/>	subnet1	subnet-018870e5f7da4d126	10.0.1.0/24	-	Main (rtb-0ddcc8fef99d0a057)
<input checked="" type="checkbox"/>	subnet2	subnet-03ecedb4977933350	10.0.2.0/24	-	Main (rtb-0ddcc8fef99d0a057)

Selected subnets

subnet-018870e5f7da4d126 / subnet1 subnet-03ecedb4977933350 / subnet2

Step 6:

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

Virtual private cloud

EC2 Global View

▼ Virtual private cloud

- Your VPCs
- Subnets
- Route tables**
- Internet gateways
- Egress-only internet gateways
- Carrier gateways
- DHCP option sets
- Elastic IPs
- Managed prefix lists
- NAT gateways
- Peering connections

Security

rtb-0c8056eb4f2302f76 / myroutetable

Details

Route table ID rtb-0c8056eb4f2302f76	Main <input checked="" type="checkbox"/> No	Explicit subnet associations 2 subnets	Edge associations -
VPC vpc-0057f273d9bb76918 kirthivpc	Owner ID 418272757660		

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

Routes (1)

Destination	Target	Status	Propagated
10.0.0.0/16	local	<input checked="" type="checkbox"/> 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).

Key pair name - required
mycode

▼ Network settings info

VPC - required info
vpc-0057f273d9bb76918 (kirthivpc)
10.0.0.0/16

Subnet info
subnet-018870e5f7da4d126
VPC: vpc-0057f273d9bb76918 Owner: 418272757660 Availability Zone: us-east-1a
Zone type: Availability Zone IP addresses available: 251 CIDR: 10.0.1.0/24

Auto-assign public IP info
Disable

Firewall (security groups) info
A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.
Create security group Select existing security group

Security group name - required

▼ Summary

Number of instances info
1

Software Image (AMI)
Amazon Linux 2023 AMI 2023.6.2...read more
ami-085ad6ae776d8f09c

Virtual server type (instance type)
t2.micro

Firewall (security group)
New security group

Storage (volumes)
1 volume(s) - 8 GiB

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which

Cancel Launch instance Preview code

Instances (2) info

Find Instance by attribute or tag (case-sensitive)

All states

	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IP
<input type="checkbox"/>	server	i-0a52ff71e24af10c2	Terminated	t2.micro	-	View alarms +	us-east-1b	-
<input type="checkbox"/>	vpc	i-01f5a0bac02909ab3	Running	t2.micro	2/2 checks passed	View alarms +	us-east-1a	-

Select an instance

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.

