

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 :Nantha Krishnan.G.K.

Department: AML

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

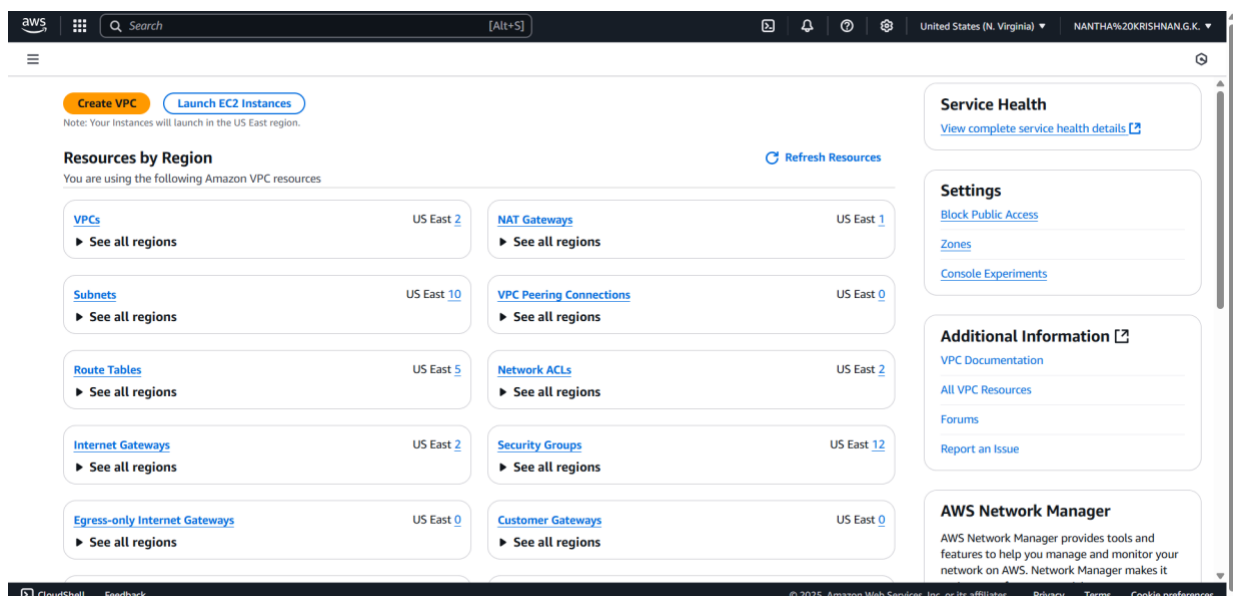
Step 2:

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 [Info](#)

A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon EC2 instances.

VPC settings

Resources to create [Info](#)
Create only the 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.

my-vpc-01

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

IPv4 CIDR
10.0.0.0/16
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 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

VPC > Subnets > Create subnet

VPC

VPC ID

Create subnets in this VPC.

vpc-089f9d4dfa6ca852f (my-vpc-01)

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 2

Subnet name

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

my-subnet-01

The name can be up to 256 characters long.

Availability Zone

Choose the zone in which your subnet will reside, or let Amazon choose one for you.

US East (N. Virginia) / us-east-1a

aws

Search

[Alt+S]

United States (N. Virginia)

NANTHA%20KRISHNAN.G.K.

VPC > Subnets > Create subnet

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.

my-subnet-02

The name can be up to 256 characters long.

Availability Zone

Choose the zone in which your subnet will reside, or let Amazon choose one for you.

US East (N. Virginia) / us-east-1a

IPv4 VPC CIDR block

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

10.0.16.0/20

4,096 IPs

Tags - optional

Key

Value - optional

Q Name X

Q my-subnet-02 X

Remove

Add new tag

CloudShell

Feedback

© 2025, Amazon Web Services, Inc. or its affiliates.

Privacy

Terms

Cookie preferences

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 'private-routetable' and 'VPC' with a dropdown menu showing 'vpc-089f9d4dfa6ca852f (my-vpc-01)'. The 'Tags' section includes a description of tags and a table with one entry: Key 'Name' and Value 'private-routetable'. There are buttons for 'Add new tag', 'Remove', 'Cancel', and 'Create route table'.

Step 5:

Associate the subnets:

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

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

Explicit subnet associations (0) [Edit subnet associations](#)

Find subnet association

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)

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
<input checked="" type="checkbox"/> my-subnet-02	subnet-083877f7201160306	10.0.16.0/20	-	Main (rtb-03e3b4ea8906536bb)
<input checked="" type="checkbox"/> my-subnet-01	subnet-081df2d1e3b508bdd	10.0.4.0/23	-	Main (rtb-03e3b4ea8906536bb)

Selected subnets

subnet-081df2d1e3b508bdd / my-subnet-01 subnet-083877f7201160306 / my-subnet-02

[Cancel](#) [Save associations](#)

Step 6:

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

Details [Info](#)

Route table ID rtb-0a5e3b0662be61f90	Main No	Explicit subnet associations 2 subnets	Edge associations -
VPC vpc-089f9d4dfa6ca852f my-vpc-01	Owner ID 423623830296		

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

Routes (1) [Both](#) [Edit routes](#)

Filter 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).

Launch an instance [Info](#)

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 [Info](#)

Name
myec2 [Add additional tags](#)

Application and OS Images (Amazon Machine Image) [Info](#)

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 **Quick Start**

Amazon Linux macOS Ubuntu Windows Red Hat SUSE Linux Debian

[Browse more AMIs](#)
Including AMIs from AWS, Marketplace and the Community

Summary

Number of instances [Info](#)
1

Software Image (AMI)
Amazon Linux 2023 AMI 2023.6.2...[read more](#)
ami-085ad5ae776d8f09c

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 t2.micro is unavailable) instance usage on free tier AMIs per month, 750 hours of public IPv4

[Cancel](#) [Launch instance](#) [Preview code](#)

Network settings [Info](#)

VPC - required [Info](#)

vpc-089f9d4dfa6ca852f (my-vpc-01)
10.0.0.0/16

Subnet [Info](#)

subnet-083877f7201160306 my-subnet-02
VPC: vpc-089f9d4dfa6ca852f Owner: 423623830296 Availability Zone: us-east-1a
Zone type: Availability Zone IP addresses available: 4091 CIDR: 10.0.16.0/20

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

launch-wizard-11

This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 (a-z, A-Z, 0-9, spaces, and ._-:/()#,@[]+=&:{}!\$*)

Description - required [Info](#)

launch-wizard-11 created 2025-02-06T15:12:09.803Z

Inbound Security Group Rules

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 Secure & Isolated VPC** – A Virtual Private Cloud (VPC) that is isolated from other networks, ensuring security and control over your cloud environment.

✅ **Structured Subnet Configuration** – One or more subnets within the VPC, including:

- At least **one public subnet** that can communicate with the internet.
- **Private subnets** (if configured) to host internal resources like databases and backend services.

✅ **Proper Routing & Connectivity** – Correctly configured route tables to enable:

- **Internal communication** between subnets for seamless data exchange.

- **Internet access** for instances in public subnets through an **Internet Gateway (IGW)**.
- **Private subnet internet access** (if required) via a **NAT Gateway**.



Enhanced Security Measures (Optional) –

- Security Groups and Network ACLs for traffic control.
- VPC Peering or Transit Gateway for cross-VPC communication.
- Elastic IP and Bastion Host for secure remote access.

