

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 : Sharon J Christopher

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

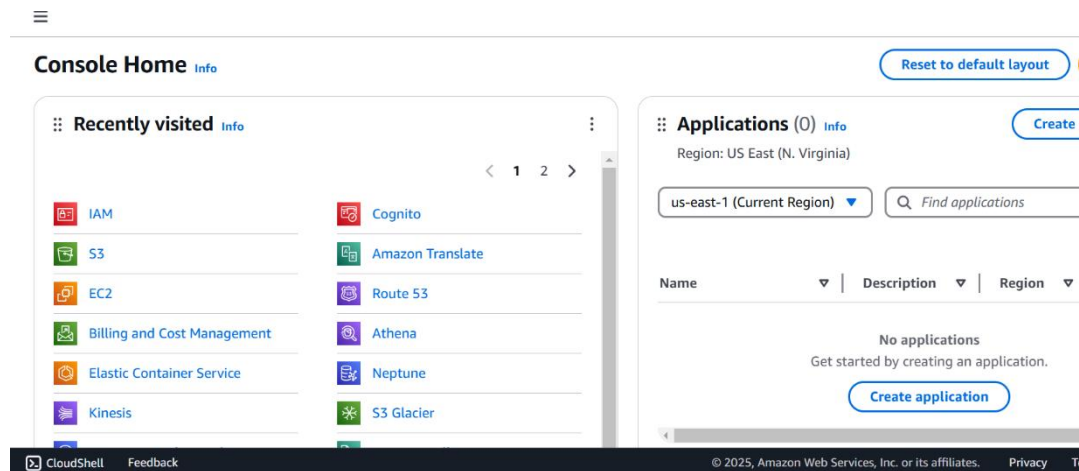
Importance

- **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 subnetwork 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
---	---

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.

vpc1

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

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

aws [Search] [Alt+S] United States (N. Virginia) sharon

VPC > Subnets > Create subnet

Create subnet info

VPC
Create subnets in this VPC.
vpc-0537adca20a03dad6 (vpc1)

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.

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

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

aws [Search] [Alt+S] United States (N. Virginia) sharon

VPC dashboard < EC2 Global View [?] Filter by VPC

▼ 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
Network ACLs
Security groups

▼ PrivateLink and

You have successfully created 2 subnets: subnet-0345a088949ab2f7b, subnet-0ad1ef7c5378b268
Last updated less than a minute ago [Actions] [Create subnet]

Subnets (2) info

Find resources by attribute or tag

Subnet ID : subnet-0345a088949ab2f7b Subnet ID : subnet-0ad1ef7c5378b268 Clear filters

<input type="checkbox"/>	Name	Subnet ID	State	VPC	Block Public...	IPv4 CIDR
<input type="checkbox"/>	subnet2	subnet-0ad1ef7c5378b268	Available	vpc-0537adca20a03dad6 vpc1	Off	10.0.2.0/24
<input type="checkbox"/>	subnet1	subnet-0345a088949ab2f7b	Available	vpc-0537adca20a03dad6 vpc1	Off	10.0.1.0/24

Select a subnet

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.

aws

Search

[Alt+S]

United States (N. Virginia)

sharon

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.

VPC
The VPC to use for this route table.

vpc-0537adca20a03dad6 (vpc1)

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	Value - optional	
<input type="text" value="Name"/>	<input type="text" value="routetable"/>	Remove
Add new tag		

You can add 49 more tags.

[Cancel](#) [Create route table](#)

CloudShell Feedback

© 2025, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

✔ Route table rtb-0c5fc70e51d32c6f3 | routetable was created successfully.

[Actions](#)

rtb-0c5fc70e51d32c6f3 / routetable

Details [Info](#)

Route table ID rtb-0c5fc70e51d32c6f3	Main No	Explicit subnet associations -	Edge associations -
VPC vpc-0537adca20a03dad6 vpc1	Owner ID 779846806994		

[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

© 2025, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

Step 5:

Associate the subnets:

Go to Subnet Associations → Click Edit subnet associations.

Select Private-Subnet-A and Private-Subnet-B.

Click Save associations.

Subnet associations

Explicit subnet associations (0)

Find subnet association

No subnet associations
You do not have any subnet associations.

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-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 subnet-0a23be0f9dc2a24aa / sub-1

Cancel Save 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

Main
No

Owner ID
774305605711

Explicit subnet associations
2 subnets

Edge associations
–

Routes

Routes (1)

Filter routes

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No

Step 7:

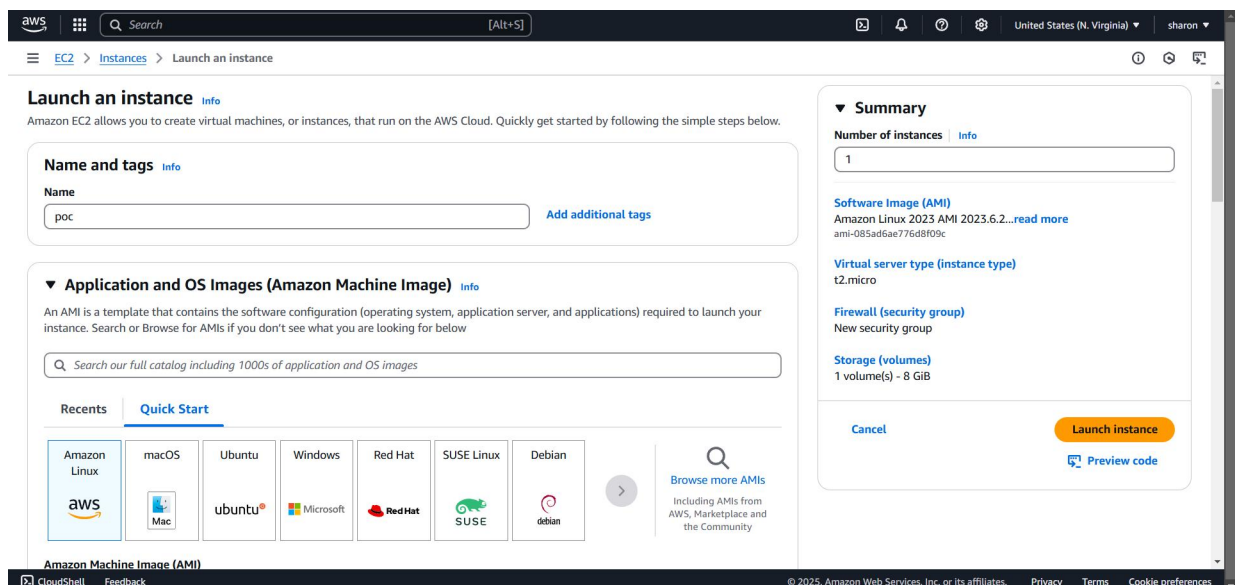
Launch Instances in Private Subnets

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).



▼
Network settings
Info

VPC - required
Info

vpc-0537adca20a03dad6 (vpc1)
10.0.0.0/16

Subnet
Info

subnet-0345a088949ab2f7b
VPC: vpc-0537adca20a03dad6 Owner: 779846806994 Availability Zone: us-east-1a
Zone type: Availability Zone IP addresses available: 251 CIDR: 10.0.1.0/24

subnet1

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-10

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 characters. Valid characters: a-z, A-Z, 0-9, spaces, and ._-:/()#,@[]+=&;{}!\$*

Description - required
Info

launch-wizard-10 created 2025-02-06T04:15:49.049Z

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.

Instance summary for i-0ad24aeb7b5fefa6 (poc) [Info](#)

Updated less than a minute ago

[Refresh](#)
[Connect](#)
[Instance state ▼](#)
[Actions ▼](#)

Instance ID i-0ad24aeb7b5fefa6	Public IPv4 address -	Private IPv4 addresses 10.0.1.102
IPv6 address -	Instance state Running	Public IPv4 DNS -
Hostname type IP name: ip-10-0-1-102.ec2.internal	Private IP DNS name (IPv4 only) ip-10-0-1-102.ec2.internal	Elastic IP addresses -
Answer private resource DNS name -	Instance type t2.micro	AWS Compute Optimizer finding Opt-in to AWS Compute Optimizer for recommendation s. Learn more
Auto-assigned IP address -	VPC ID vpc-0537adca20a03dad6 (vpc1)	Auto Scaling Group name -
IAM Role -	Subnet ID subnet-0345a088949ab2f7b (subnet1)	Managed false
IMDSv2 Required	Instance ARN arn:aws:ec2:us-east-1:779846806994:instance/i-0ad24aeb7b5fefa6	
Operator -		

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.

