St. JOSEPH'S
GROUP OF INSTITUTIONS
OMR, CHENNAI - 119

aws

Placement Empowerment Program

Cloud Computing and DevOps Centre

Set Up a Private Network in the Cloud : Create a Virtual Private Cloud (VPC) with subnets for your instances. Configure routing for internal communication between subnets.

Name: Saravana Krishnan J

Department: IT

St. JOSEPH'S COLLEGE OF ENGINEERING | St. JOSEPH'S INSTITUTE OF TECHNOLOGY
AUTONOMOUS INSTITUTIONS, AFFILIATED TO ANNA UNIVERSITY

Introduction

The goal of this Proof of Concept (PoC) was to set up a **Private Network in the Cloud** by creating a **Virtual Private Cloud (VPC)** in AWS, configuring **subnets**, and ensuring **internal communication** between instances within the VPC. This setup focused on isolating cloud resources in a private network, providing a secure environment for communication, and making sure that only internal traffic is allowed, without exposing resources to the public internet.

In this PoC, we created a **private subnet** where EC2 instances could communicate with each other without direct exposure to external networks.

Overview

In this PoC, we:

1. **Created a VPC** in AWS, which serves as the isolated private network.

2. **Created a private subnet** inside the VPC where EC2 instances can reside, ensuring no direct access from the public internet.

3. **Set up routing** to allow communication between the instances within the same VPC and subnet.

4. Launched **EC2 instances** in the private subnet and verified their ability to communicate internally using their private IP addresses.

The setup is designed to simulate a secure cloud environment where resources can interact securely without being exposed to external traffic.

Objective

The primary objectives of this PoC were:

1. **Establish a Private Network**: Set up a private VPC and subnets for cloud resources to reside in, ensuring they are isolated from the public internet.

2. **Internal Communication**: Ensure that EC2 instances within the private subnet can communicate with each other using their private IPs.

3. **Security**: Maintain internal communication only within the VPC, preventing direct exposure of instances to the public internet.

4. **Simplify Management**: Organize cloud resources into subnets for easier management and scaling, with clear routing between them.

Importance

1. **Security**: By placing EC2 instances in a private subnet and ensuring that no public IP is assigned, the resources are isolated from external traffic. This is crucial for keeping sensitive data and services protected.

2. **Cost Efficiency**: Using internal communication and private subnets can help reduce costs related to public internet access and data transfer.

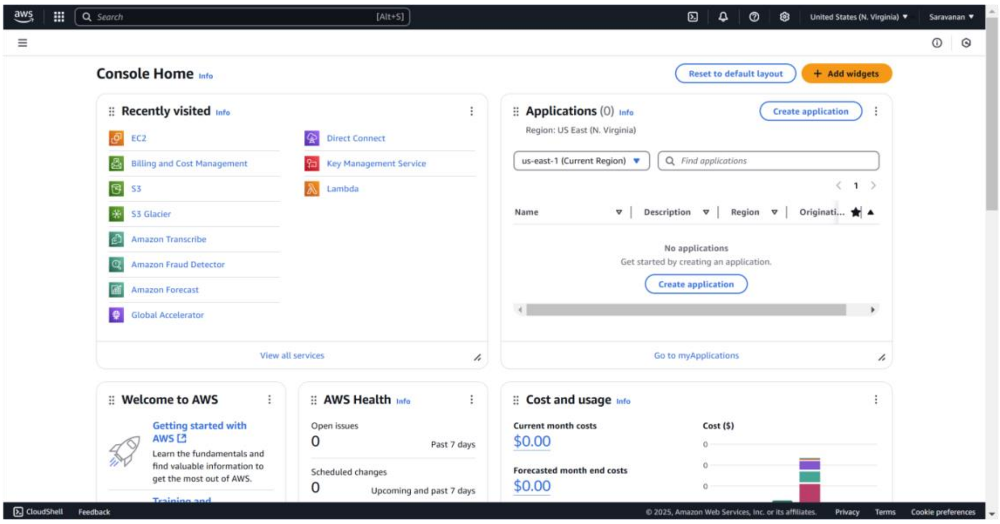
3. **Flexibility**: This setup provides a foundation for building more complex cloud infrastructures, such as multi-tier applications where only backend servers (databases, app servers) are private, while frontend servers may be public.

Step-by-Step Overview

Step 1:

1. Go to AWS Management Console.

2. Enter your username and password to log in.



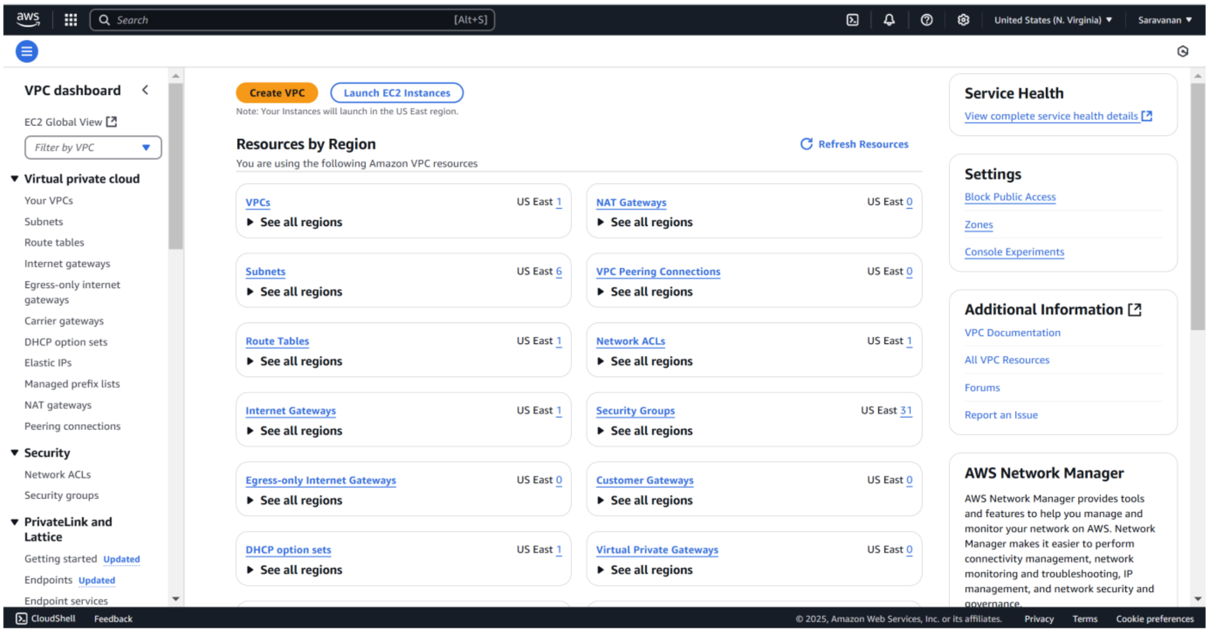
No applications

Get started by creating an application.

Learn the fundamentals and find valuable information to get the most out of AWS.

Step 2:

In the **VPC Dashboard**, click the **Create VPC** button.



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

You are using the following Amazon VPC resources

AWS Network Manager provides tools and features to help you manage and monitor your network on AWS. Network Manager makes it easier to perform connectivity management, network monitoring and troubleshooting, IP management, and network security and governance.

Step 3:

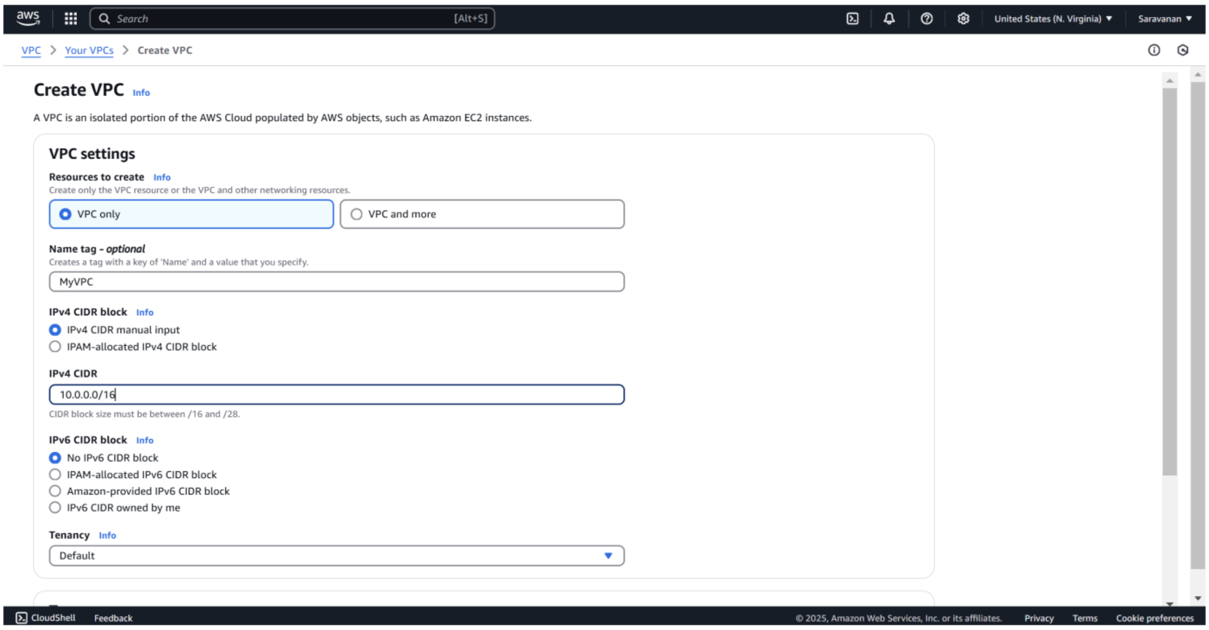
In the VPC creation wizard, select **VPC only**.

Name tag: Enter MyVPC .

IPv4 CIDR block: Enter 10.0.0.0/16 (this defines the IP range for your VPC).

Tenancy: Leave it as **Default**.

Click **Create VPC**.


aws
Search [Alt+S]
United States (N. Virginia) ▾
Saravanan ▾
VPC > Your VPCs > Create VPC
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

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.
MyVPC

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
Default ▾

Step 4:

In the **VPC Dashboard**, click on **Subnets** in the left-hand menu.

Click the **Create subnet** button.

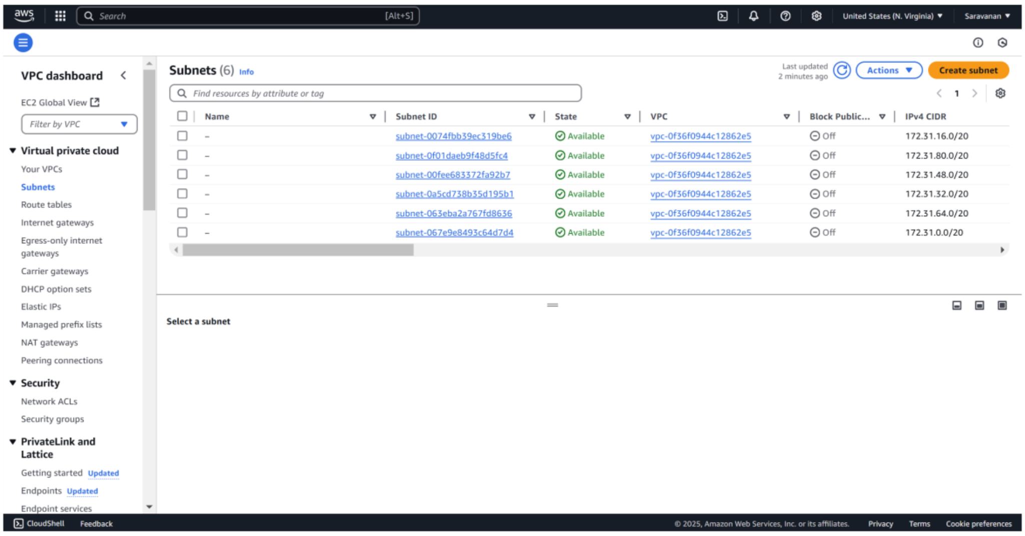
VPC: Select MyVPC (the one you just created).

Subnet name: Enter Private-Subnet.

Availability Zone: Pick any (e.g., us-east-1a or any zone from your region).

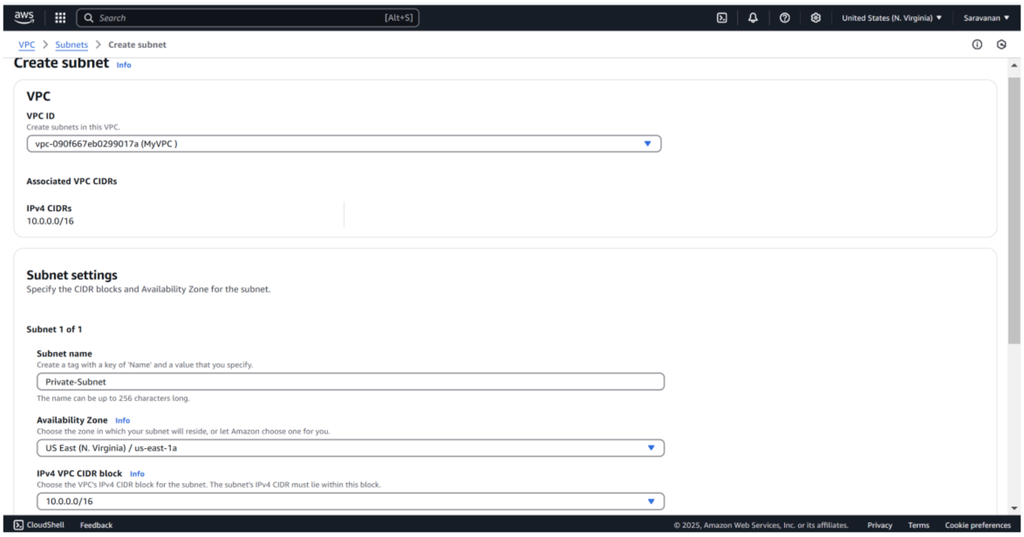
IPv4 CIDR block: Enter 10.0.1.0/24 (this is a smaller range within the VPC's IP range).

Click **Create subnet**.



Subnets (6) Info

Name	Subnet ID	State	VPC	Block Public...	IPv4 CIDR
–	subnet-0074fbb39ec319be6	Available	vpc-0f36f0944c12862e5	Off	172.31.16.0/20
–	subnet-0f01daeb9f48d5fc4	Available	vpc-0f36f0944c12862e5	Off	172.31.80.0/20
–	subnet-00fee683372fa92b7	Available	vpc-0f36f0944c12862e5	Off	172.31.48.0/20
–	subnet-0a5cd738b35d195b1	Available	vpc-0f36f0944c12862e5	Off	172.31.32.0/20
–	subnet-063eba2a767fd8636	Available	vpc-0f36f0944c12862e5	Off	172.31.64.0/20
–	subnet-067e9e8493c64d7d4	Available	vpc-0f36f0944c12862e5	Off	172.31.0.0/20


VPC > Subnets > Create subnet
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Create subnet Info

VPC

VPC ID
Create subnets in this VPC.
vpc-090f667eb0299017a (MyVPC)

Associated VPC CIDRs

IPv4 CIDRs
10.0.0.0/16

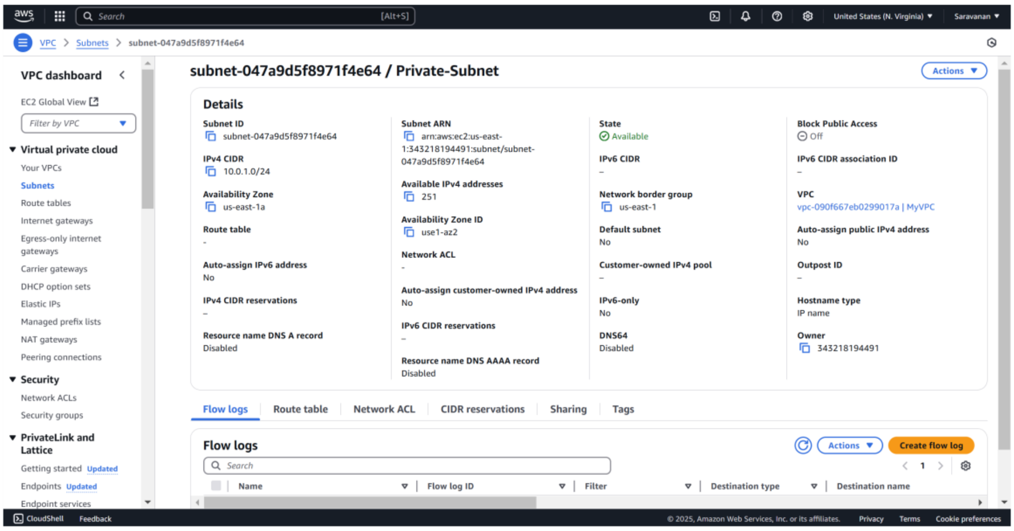
Subnet settings
Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

Subnet name
Create a tag with a key of 'Name' and a value that you specify.
Private-Subnet
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-1a

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



subnet-047a9d5f8971f4e64 / Private-Subnet

Details

Subnet ID subnet-047a9d5f8971f4e64	Subnet ARN arn:aws:ec2:us-east-1:343218194491:subnet/subnet-047a9d5f8971f4e64	State Available	Block Public Access Off
IPv4 CIDR 10.0.1.0/24	Available IPv4 addresses 251	IPv6 CIDR –	IPv6 CIDR association ID –
Availability Zone us-east-1a	Availability Zone ID use1-az2	Network border group us-east-1	VPC vpc-090f667eb0299017a | MyVPC
Route table -	Network ACL -	Default subnet No	Auto-assign public IPv4 address No
Auto-assign IPv6 address No	Auto-assign customer-owned IPv4 address No	Customer-owned IPv4 pool –	Outpost ID –
IPv4 CIDR reservations –	IPv6 CIDR reservations –	IPv6-only No	Hostname type IP name
Resource name DNS A record Disabled	Resource name DNS AAAA record Disabled	DNS64 Disabled	Owner 343218194491

Flow logs

Name	Flow log ID	Filter	Destination type	Destination name

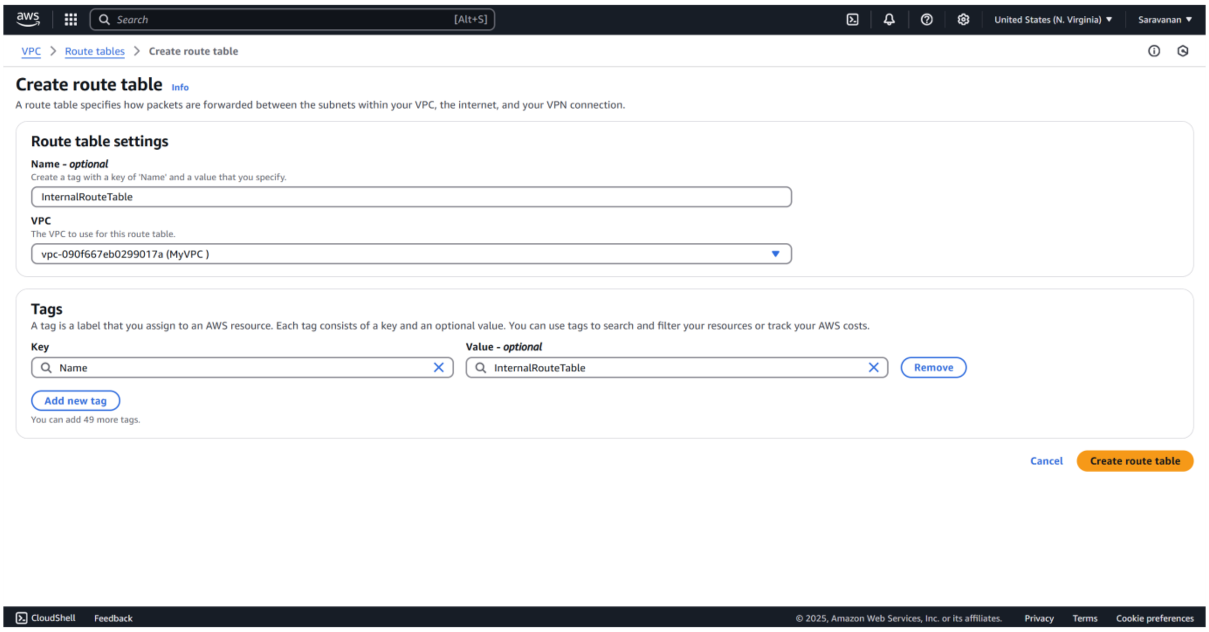
Step 5:

In the **VPC Dashboard**, click on **Route Tables** in the left-hand menu. Click **Create route table**.

Name tag: Enter InternalRouteTable.

VPC: Select MyVPC (the one you created earlier).

Click **Create route table**.



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

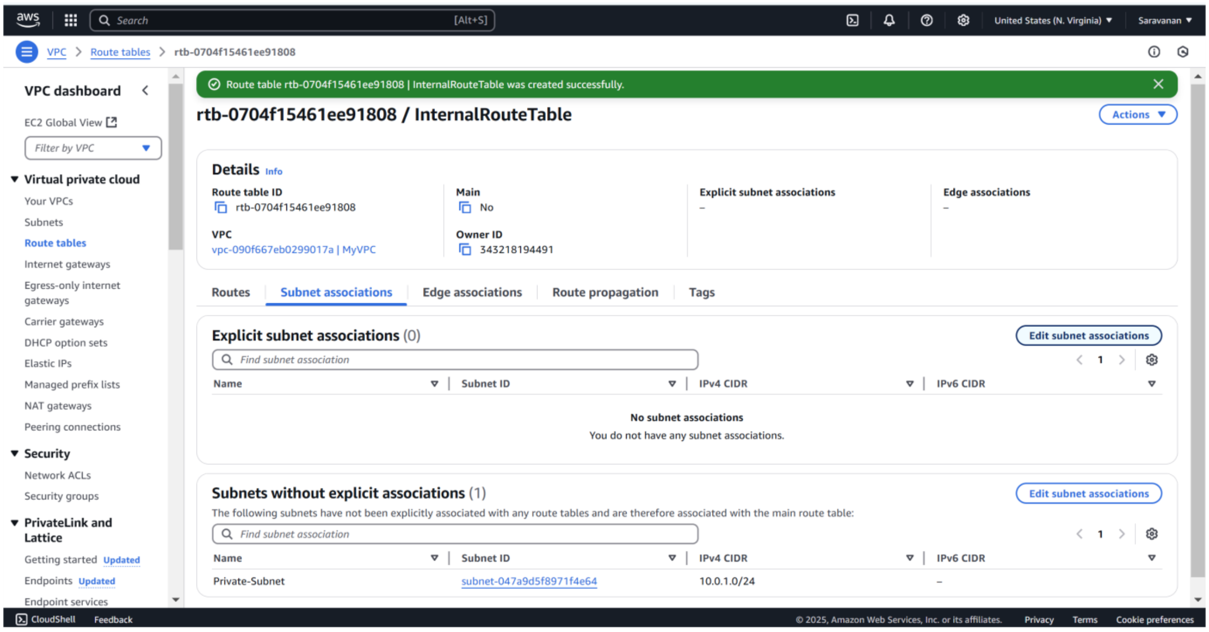
Name - *optional*
Create a tag with a key of 'Name' and a value that you specify.
InternalRouteTable

VPC
The VPC to use for this route table.
vpc-090f667eb0299017a (MyVPC)

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*
Name	InternalRouteTable



VPC > Route tables > rtb-0704f15461ee91808

Route table rtb-0704f15461ee91808 | InternalRouteTable was created successfully.

rtb-0704f15461ee91808 / InternalRouteTable

Details Info

Route table ID: rtb-0704f15461ee91808
Main: No
Explicit subnet associations: –
Edge associations: –
VPC: vpc-090f667eb0299017a | MyVPC
Owner ID: 343218194491

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

Explicit subnet associations (0)

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR

No subnet associations
You do not have any subnet associations.

Subnets without explicit associations (1)

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

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
Private-Subnet	subnet-047a9d5f8971f4e64	10.0.1.0/24	–

Step 6:

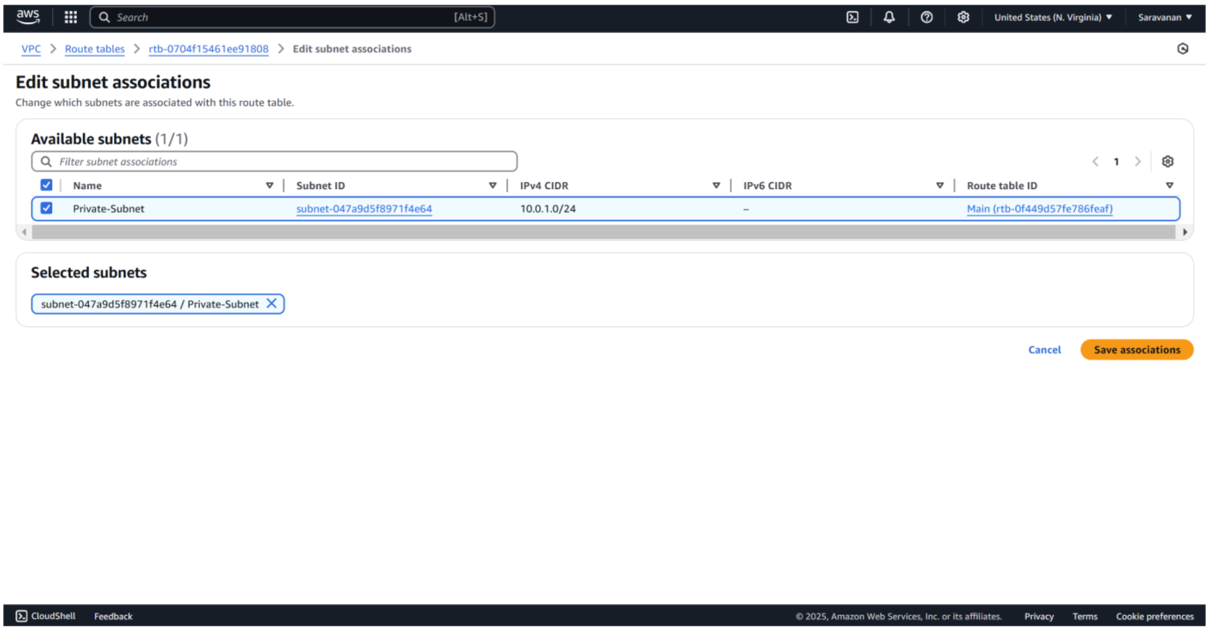
Select the InternalRouteTable you just created.

Go to the **Subnet Associations** tab (it’s near the bottom).

Click **Edit subnet associations**.

Select Private-Subnet (the subnet you created earlier).

Click **Save associations**.



VPC > Route tables > rtb-0704f15461ee91808 > Edit subnet associations

Edit subnet associations

Change which subnets are associated with this route table.

Available subnets (1/1)

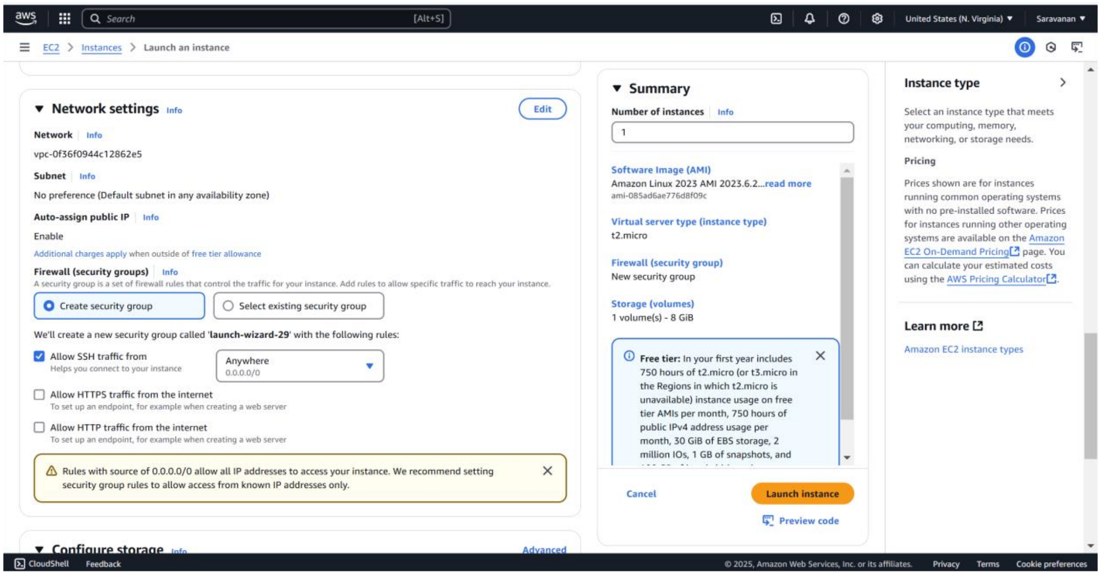
☑	Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
☑	Private-Subnet	subnet-047a9d5f8971f4e64	10.0.1.0/24	–	Main (rtb-0f449d57fe786feaf)

Selected subnets

subnet-047a9d5f8971f4e64 / Private-Subnet ✕

Step 7:

To launch a new EC2 instance in your private subnet, go to the EC2 Dashboard, click **Launch Instance**, and fill in the details: Name it "Private-Instance", choose an Amazon Linux 2 AMI (or another free-tier eligible image), select the **t2.micro** instance type, and either choose an existing key pair or create a new one for SSH access. Under **Network settings**, select your **MyVPC** and **Private-Subnet**, and make sure **Auto-assign Public IP** is disabled to keep it private. Leave all other settings as default, then click **Launch Instance**.


aws
Search [Alt+S]
United States (N. Virginia) ▼
Saravanan ▼
EC2 > Instances > Launch an instance
Edit
Cancel
Launch instance
Preview code
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

▼ Network settings Info

Network Info
vpc-0f36f0944c12862e5

Subnet Info
No preference (Default subnet in any availability zone)

Auto-assign public IP Info
Enable

Additional charges apply when outside of free tier allowance

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

We'll create a new security group called 'launch-wizard-29' with the following rules:

☑ Allow SSH traffic from — Anywhere 0.0.0.0/0
Helps you connect to your instance

□ Allow HTTPS traffic from the internet
To set up an endpoint, for example when creating a web server

□ Allow HTTP traffic from the internet
To set up an endpoint, for example when creating a web server

⚠ Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

▼ Configure storage Info — Advanced

▼ 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 t2.micro is unavailable) instance usage on free tier AMIs per month, 750 hours of public IPv4 address usage per month, 30 GiB of EBS storage, 2 million IOs, 1 GB of snapshots, and

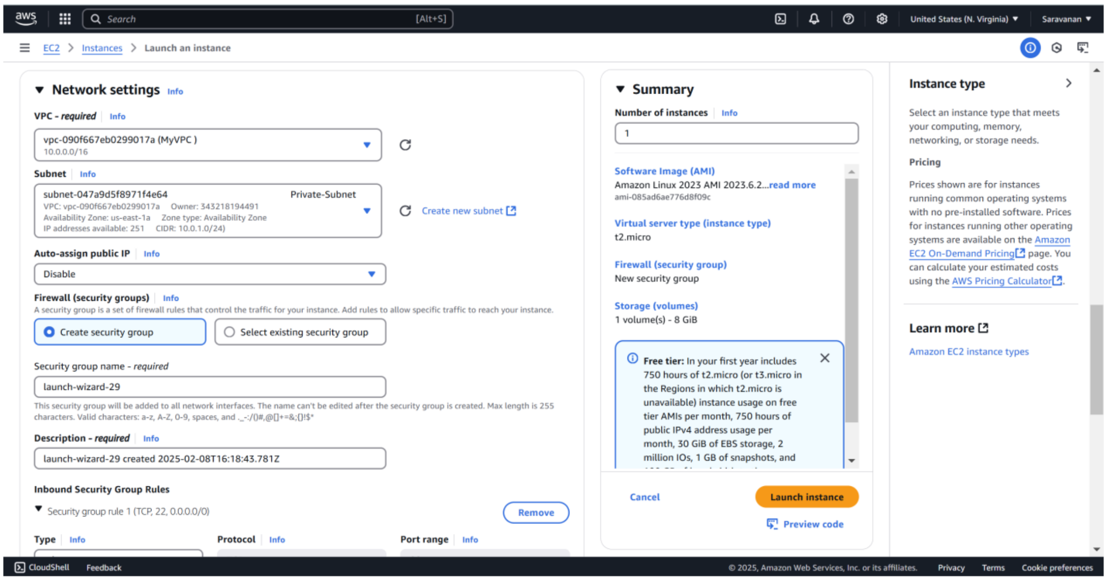
Instance type

Select an instance type that meets your computing, memory, networking, or storage needs.

Pricing

Prices shown are for instances running common operating systems with no pre-installed software. Prices for instances running other operating systems are available on the Amazon EC2 On-Demand Pricing page. You can calculate your estimated costs using the AWS Pricing Calculator.

Learn more
Amazon EC2 instance types



▼ Network settings Info

VPC - *required* Info
vpc-090f667eb0299017a (MyVPC)
10.0.0.0/16

Subnet Info
subnet-047a9d5f8971f4e64 Private-Subnet
VPC: vpc-090f667eb0299017a Owner: 343218194491
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*
launch-wizard-29
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-29 created 2025-02-08T16:18:43.781Z

Inbound Security Group Rules

▼ Security group rule 1 (TCP, 22, 0.0.0.0/0)

Type Info | Protocol Info | Port range Info

▼ 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 t2.micro is unavailable) instance usage on free tier AMIs per month, 750 hours of public IPv4 address usage per month, 30 GiB of EBS storage, 2 million IOs, 1 GB of snapshots, and

Instance type

Select an instance type that meets your computing, memory, networking, or storage needs.

Pricing

Prices shown are for instances running common operating systems with no pre-installed software. Prices for instances running other operating systems are available on the Amazon EC2 On-Demand Pricing page. You can calculate your estimated costs using the AWS Pricing Calculator.

Learn more
Amazon EC2 instance types

Step 8: Verify Internal Communication

1. **Find the private IP of your instance**:

   Go to the **EC2 Dashboard**.

   Select your instance in Private-Subnet.

   Note the **Private IPv4 address** (e.g., 10.0.1.x).

2. **Ping the Private IP**:

   If you have only one instance, you can skip this. If you have multiple instances in the private subnet, SSH into one instance and try pinging the private IP of the other instance.

Outcome

By completing this PoC of setting up a Private Network in AWS, you will:

1. Deploy a VPC with a private subnet to isolate cloud resources securely from the public internet.

2. Launch EC2 instances within the private subnet and ensure internal communication between them using private IPs.

3. Configure routing tables to enable efficient communication within the VPC while maintaining the isolation of private resources.

4. Implement security groups to allow only internal traffic between instances while restricting external access.

5. Gain practical experience in designing secure cloud architectures and foundational AWS services like VPC, EC2, and private networking.