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

aws

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

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

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

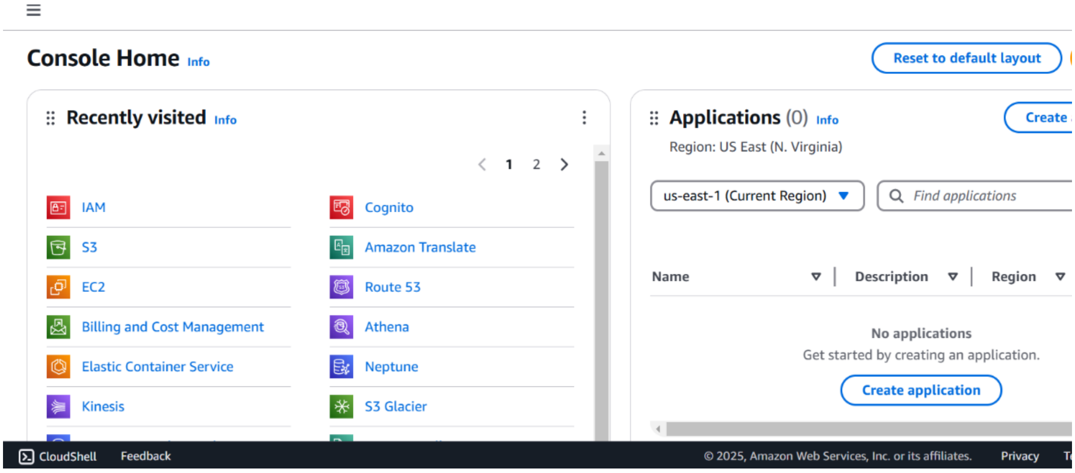
- Security: A VPC allows you to maintain a secure environment, isolating your resources from public internet exposure while enabling controlled access.
- Customization: You can tailor the network architecture to meet specific needs, such as private IP addressing and subnetwork segmentation.
- Cost Efficiency: 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



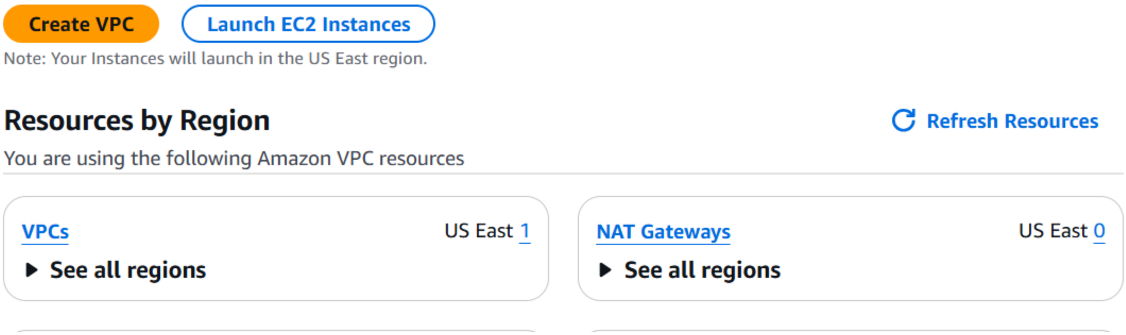
Step 2:

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."



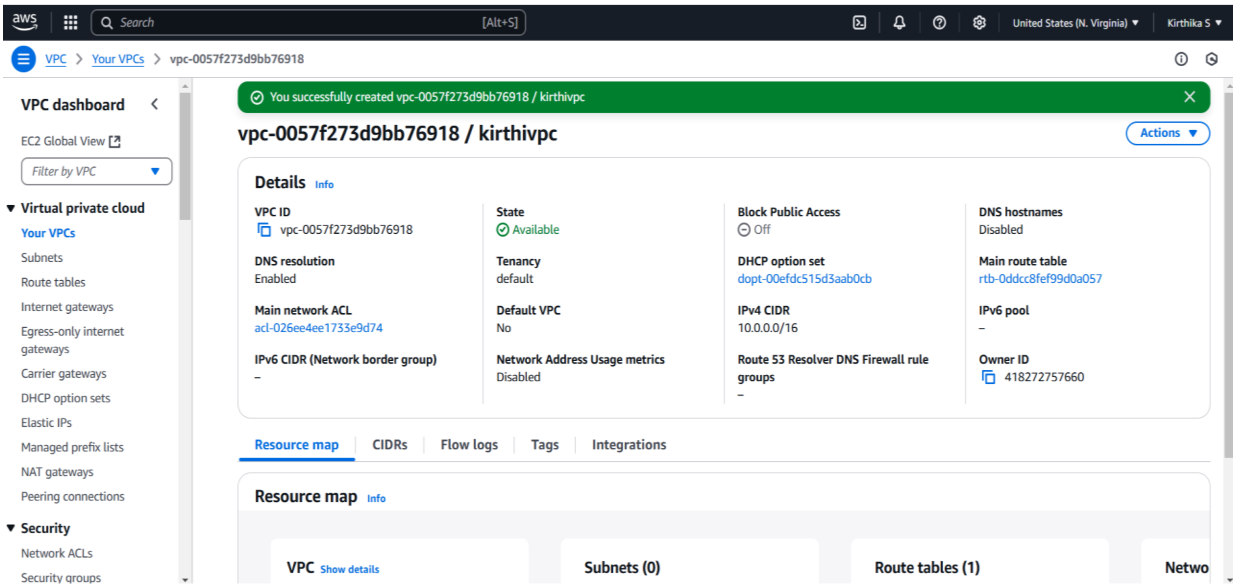
Note: Your Instances will launch in the US East region.

Resources by Region

You are using the following Amazon VPC resources

VPCs US East 1

NAT Gateways US East 0



You successfully created vpc-0057f273d9bb76918 / kirthivpc

vpc-0057f273d9bb76918 / kirthivpc

Details

VPC ID: vpc-0057f273d9bb76918

State: Available

Block Public Access: Off

DNS hostnames: Disabled

DNS resolution: Enabled

Tenancy: default

DHCP option set: dopt-00efdc515d3aab0cb

Main route table: rtb-0ddcc8fef99d0a057

Main network ACL: acl-026ee4ee1733e9d74

Default VPC: No

IPv4 CIDR: 10.0.0.0/16

IPv6 pool: –

IPv6 CIDR (Network border group): –

Network Address Usage metrics: Disabled

Route 53 Resolver DNS Firewall rule groups: –

Owner ID: 418272757660

Resource map

VPC

Subnets (0)

Route tables (1)

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:

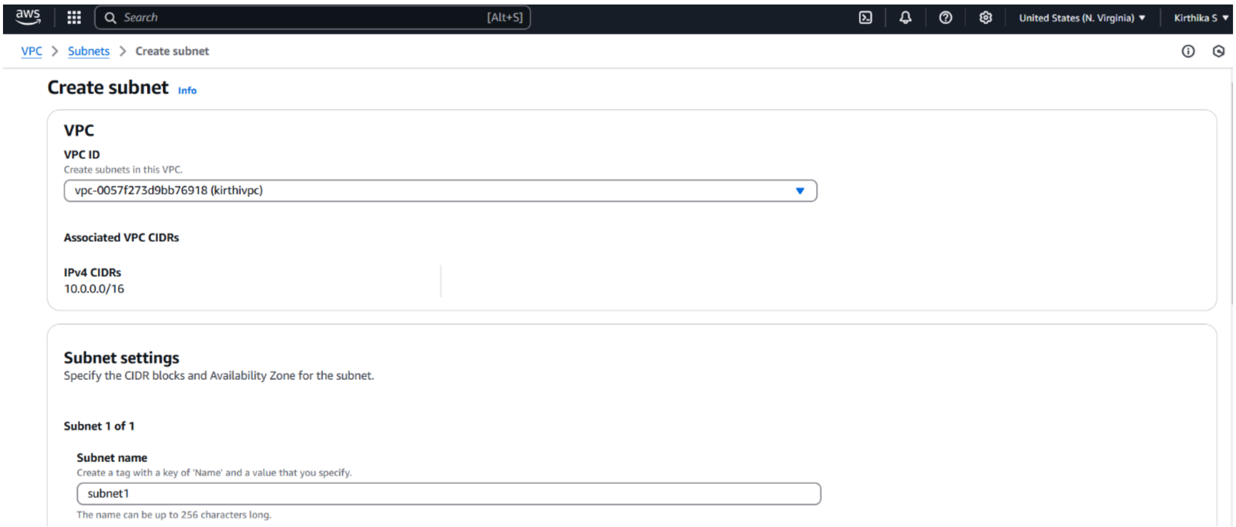
Subnet 1 (Private-Subnet-A)

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



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.

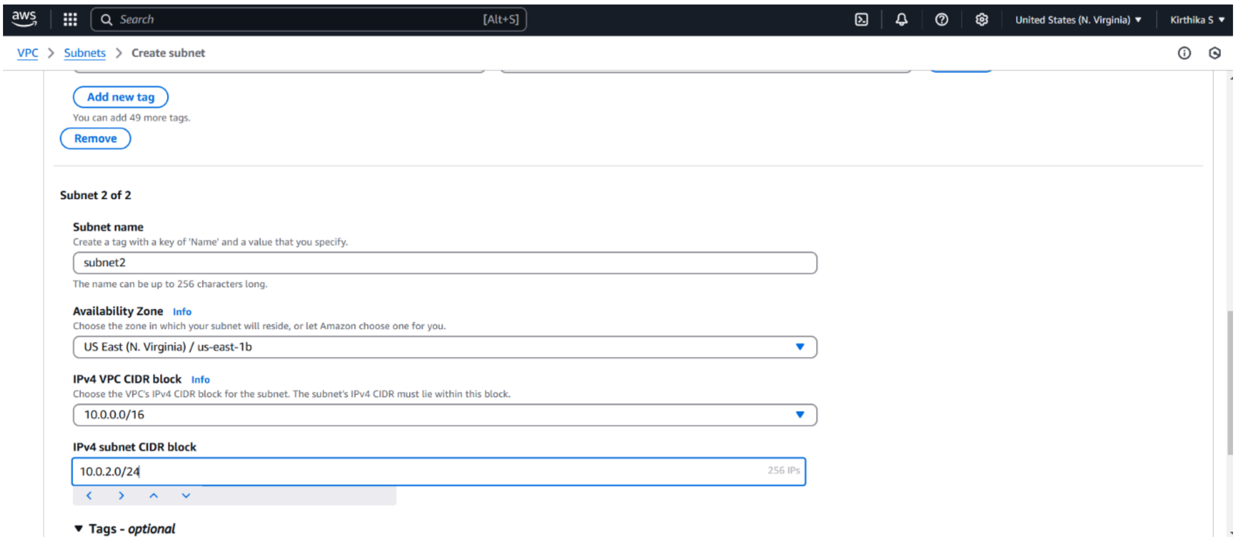
Subnet 1 of 1

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.



You can add 49 more tags.

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

▼ Tags - *optional*

Step 4:

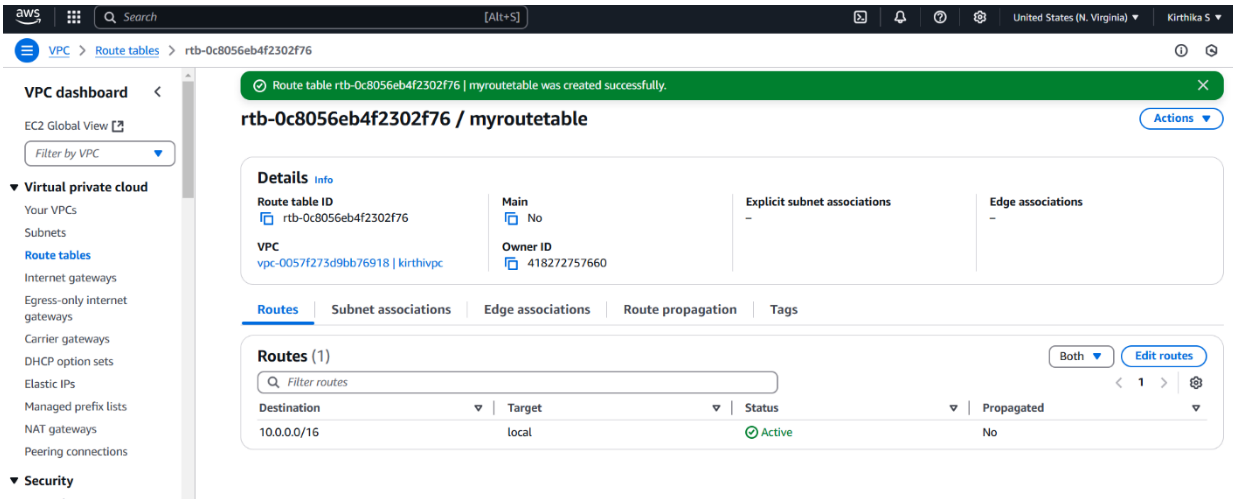
Configure Route Tables for Internal Communication

1. Go to Route Tables → Click Create Route Table.

2. Name it (e.g., PrivateRouteTable).

3. Select MyPrivateVPC.

4. Click Create.



Route table rtb-0c8056eb4f2302f76 | myroutetable was created successfully.

rtb-0c8056eb4f2302f76 / myroutetable

Details

Route table ID: rtb-0c8056eb4f2302f76

VPC: vpc-0057f273d9bb76918 | kirthivpc

Main: No

Owner ID: 418272757660

Explicit subnet associations: –

Edge associations: –

Routes (1)

Destination	Target	Status	Propagated
10.0.0.0/16	local	✓ Active	No

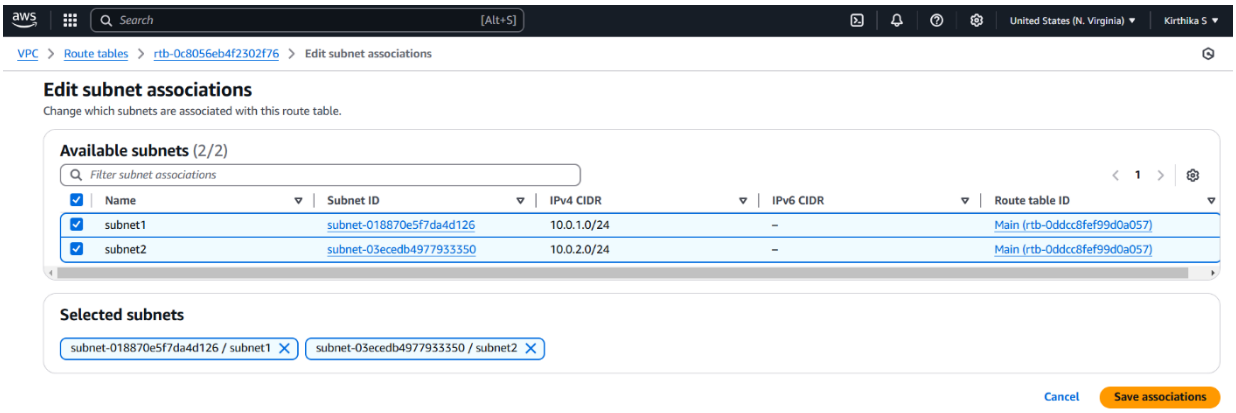
Step 5:

Associate the subnets:

Go to Subnet Associations → Click Edit subnet associations.

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

Click Save associations.



VPC > Route tables > rtb-0c8056eb4f2302f76 > Edit subnet associations

Edit subnet associations

Change which subnets are associated with this route table.

Available subnets (2/2)

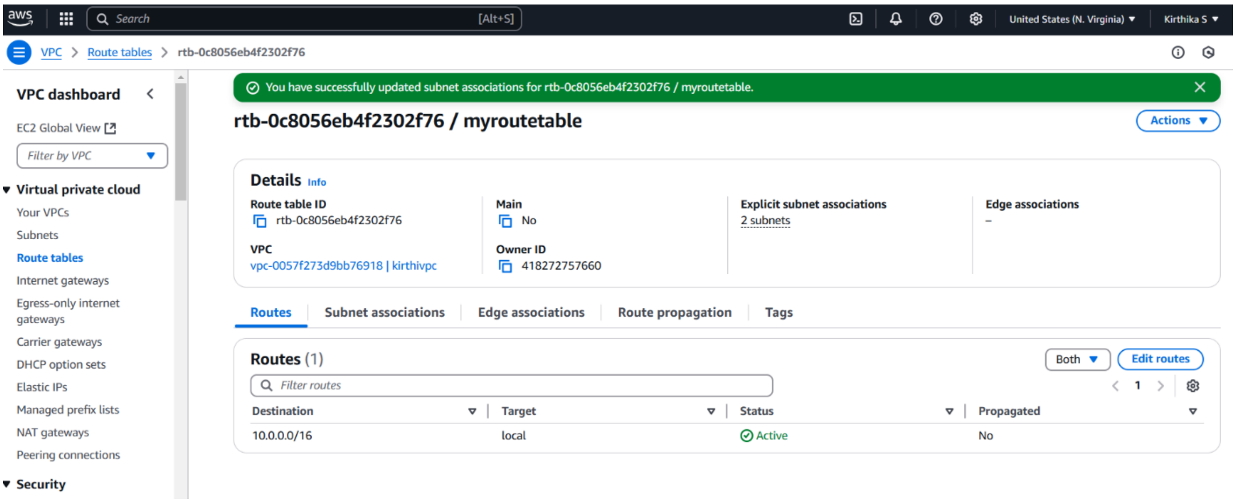
☑	Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
☑	subnet1	subnet-018870e5f7da4d126	10.0.1.0/24	–	Main (rtb-0ddcc8fef99d0a057)
☑	subnet2	subnet-03ecedb4977933350	10.0.2.0/24	–	Main (rtb-0ddcc8fef99d0a057)

Selected subnets

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

Step 6:

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



VPC > Route tables > rtb-0c8056eb4f2302f76

You have successfully updated subnet associations for rtb-0c8056eb4f2302f76 / myroutetable.

rtb-0c8056eb4f2302f76 / myroutetable

Details Info

Route table ID: rtb-0c8056eb4f2302f76

Main: No

Explicit subnet associations: 2 subnets

Edge associations: –

VPC: vpc-0057f273d9bb76918 | kirthivpc

Owner ID: 418272757660

Routes (1)

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.).

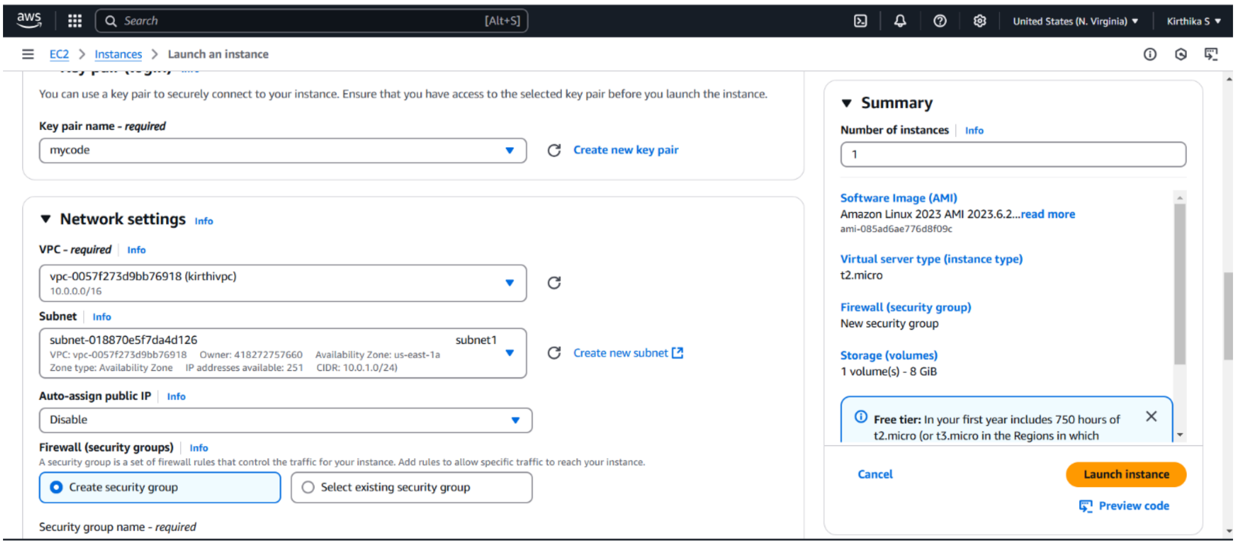
3. Choose an Instance Type (e.g., t2.micro).

4. Under Network settings:

Select MyPrivateVPC.

Select Private Subnet-A or Private-Subnet-B.

Disable Auto-assign Public IP (to keep it private).



You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - *required*: mycode

Network settings

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

Subnet: subnet-018870e5f7da4d126 subnet1
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: Disable

Firewall (security groups)
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*

Number of instances: 1

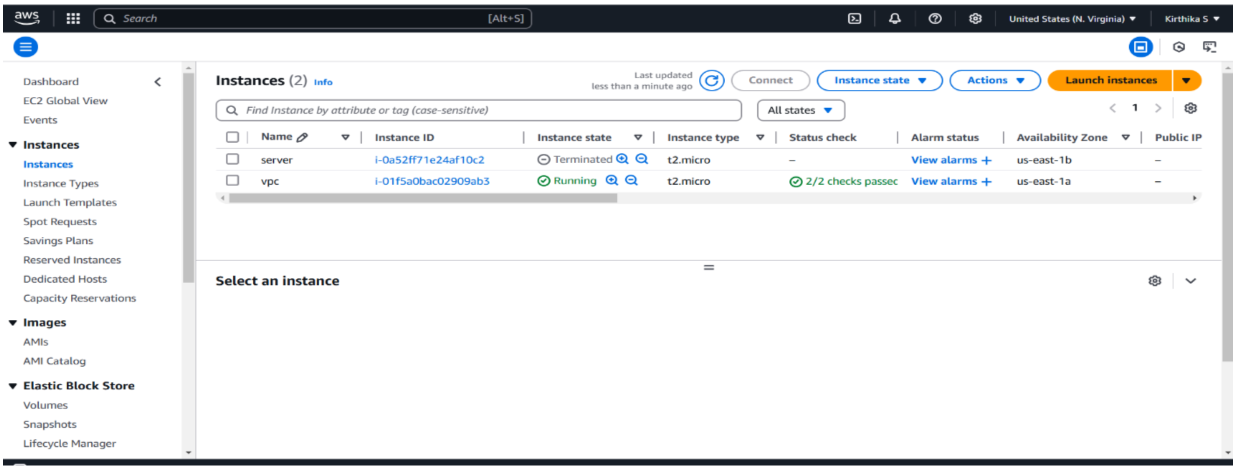
Software Image (AMI)
Amazon Linux 2023 AMI 2023.6.2...read more
ami-085ad6ae776d8f09c

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



Instances (2)

Last updated less than a minute ago

□	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IP
□	server	i-0a52ff71e24af10c2	Terminated	t2.micro	–	View alarms +	us-east-1b	–
□	vpc	i-01f5a0bac02909ab3	Running	t2.micro	2/2 checks passec	View alarms +	us-east-1a	–

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.