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: CHANDRU S

Department: INFORMATION TECHNOLOGY

Introduction

A Virtual Private Cloud (VPC) is a secure, isolated segment of a cloud provider's infrastructure that allows you to deploy and manage resources in a controlled environment. Establishing a VPC involves creating subnets, configuring routing, and implementing security measures to regulate traffic and access. This setup is crucial for applications that need secure internal communication while remaining accessible to external networks as required.

Objective

1. **Create a VPC:** Build a private, customizable network in the cloud tailored to your application's needs.
2. **Configure Subnets:** Design and deploy subnets within the VPC to segregate resources, such as public-facing and private instances.
3. **Set Up Routing:** Establish routing tables to facilitate seamless internal communication between subnets and enable external access when necessary.
4. **Implement Security:** Apply security groups and network ACLs to manage and restrict inbound and outbound traffic effectively.
5. **Ensure High Availability:** Distribute resources across multiple Availability Zones to improve fault tolerance and reliability.

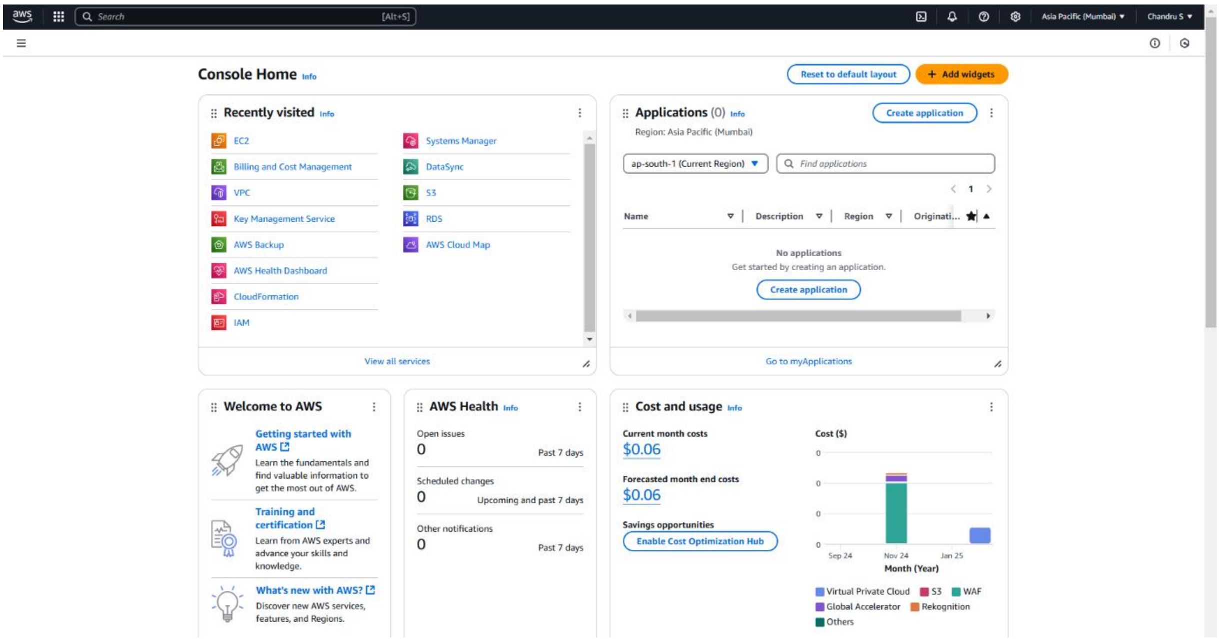
Importance

- 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:

Log in to the **AWS Management Console** using your credentials.



No applications

Get started by creating an application.

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

Learn from AWS experts and advance your skills and knowledge.

Discover new AWS services, features, and Regions.

Open issues 0 Past 7 days

Scheduled changes 0 Upcoming and past 7 days

Other notifications 0 Past 7 days

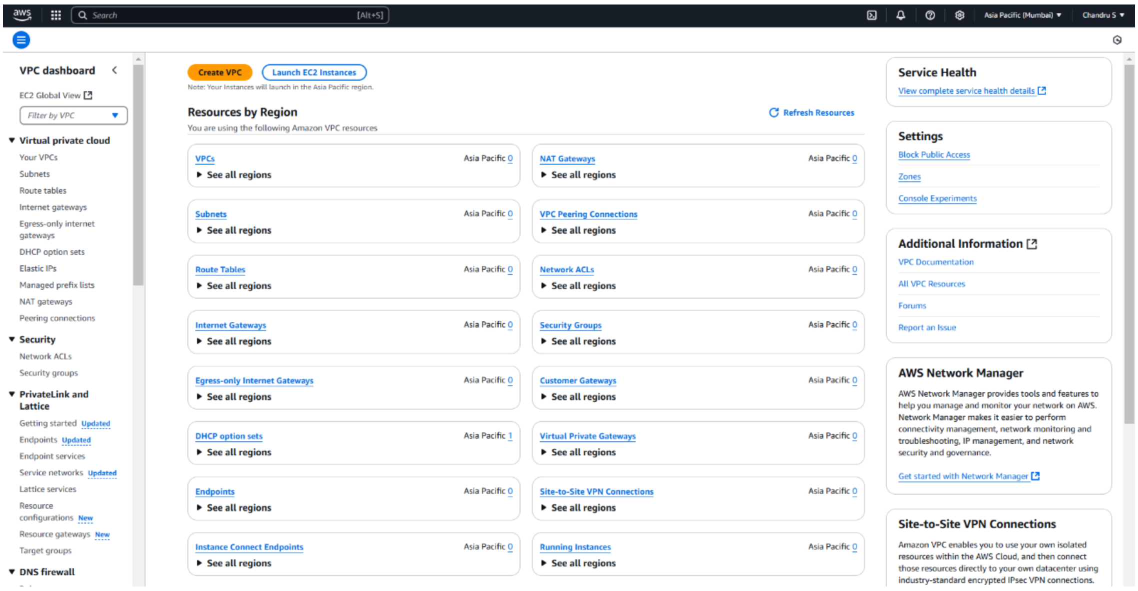
Current month costs $0.06

Forecasted month end costs $0.06

Step 2:

Navigate to the VPC Dashboard:

- In the Services menu, select VPC to access the dashboard.



Note: Your Instances will launch in the Asia Pacific region.

You are using the following Amazon VPC resources

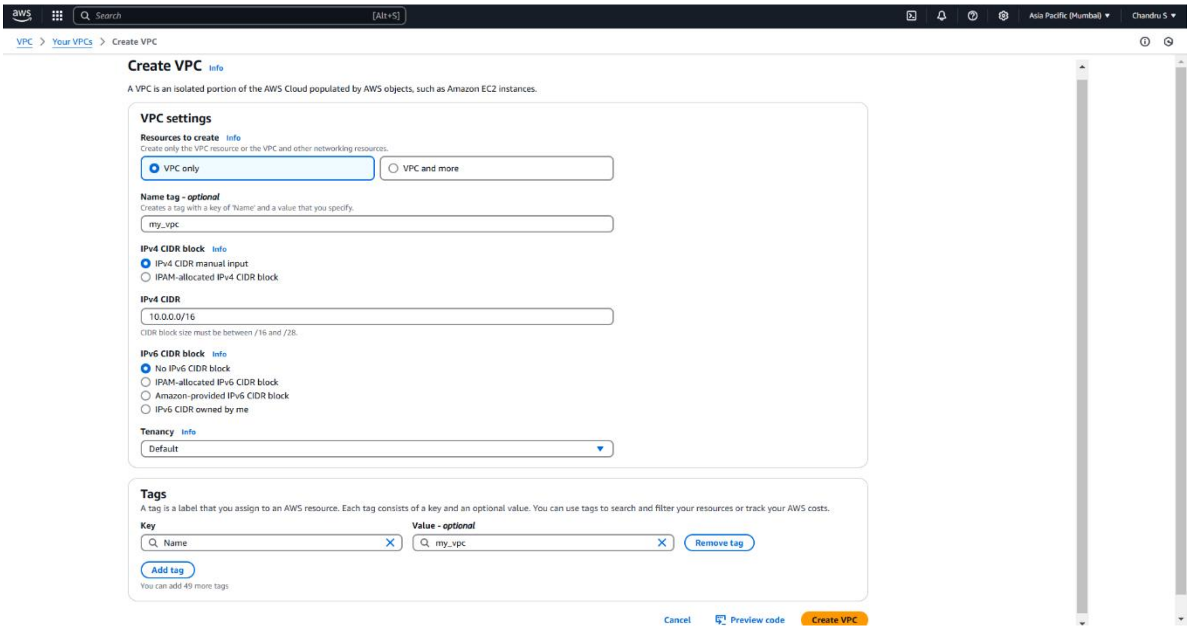
VPCs Asia Pacific 0 ▶ See all regions	NAT Gateways Asia Pacific 0 ▶ See all regions
Subnets Asia Pacific 0 ▶ See all regions	VPC Peering Connections Asia Pacific 0 ▶ See all regions
Route Tables Asia Pacific 0 ▶ See all regions	Network ACLs Asia Pacific 0 ▶ See all regions
Internet Gateways Asia Pacific 0 ▶ See all regions	Security Groups Asia Pacific 0 ▶ See all regions
Egress-only Internet Gateways Asia Pacific 0 ▶ See all regions	Customer Gateways Asia Pacific 0 ▶ See all regions
DHCP option sets Asia Pacific 1 ▶ See all regions	Virtual Private Gateways Asia Pacific 0 ▶ See all regions
Endpoints Asia Pacific 0 ▶ See all regions	Site-to-Site VPN Connections Asia Pacific 0 ▶ See all regions
Instance Connect Endpoints Asia Pacific 0 ▶ See all regions	Running Instances Asia Pacific 0 ▶ See all regions

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.

Amazon VPC enables you to use your own isolated resources within the AWS Cloud, and then connect those resources directly to your own datacenter using industry-standard encrypted IPsec VPN connections.

Create a VPC

- Click on "Your VPCs" in the left menu, then click "Create VPC."
- Specify the following:
  - **Name tag**: Enter a name for your VPC.
  - **IPv4 CIDR block**: Example: 10.0.0.0/16 (provides 65,536 IP addresses).
  - **IPv6 CIDR block**: (Optional).
  - **Tenancy**: Default is sufficient for most cases.



Create VPC

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

VPC settings

Resources to create
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

IPv4 CIDR block
● 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
● No IPv6 CIDR block
○ IPAM-allocated IPv6 CIDR block
○ Amazon-provided IPv6 CIDR block
○ IPv6 CIDR owned by me

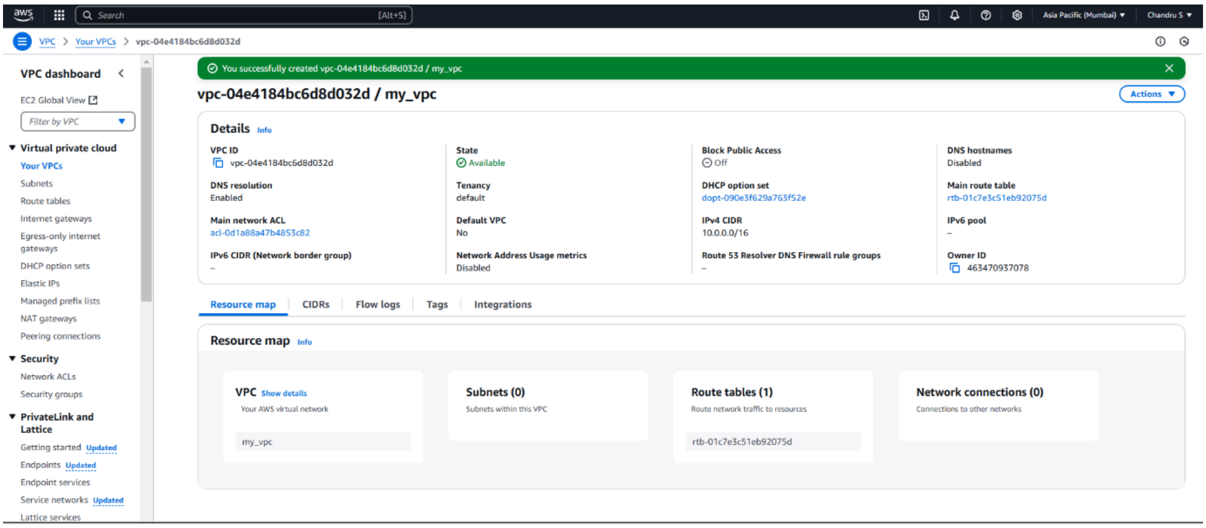
Tenancy
Default

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	my_vpc

Remove tag
Add tag
You can add 49 more tags

- Click "Create."



You successfully created vpc-04e4184bc6d8d032d / my_vpc

vpc-04e4184bc6d8d032d / my_vpc

Details

VPC ID vpc-04e4184bc6d8d032d	State Available	Block Public Access Off	DNS hostnames Disabled
DNS resolution Enabled	Tenancy default	DHCP option set dopt-090e3f629a763f52e	Main route table rtb-01c7e3c51eb92075d
Main network ACL acl-0d1a88a47b4853c82	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 463470937078

Resource map

VPC — Your AWS virtual network — my_vpc
Subnets (0) — Subnets within this VPC
Route tables (1) — Route network traffic to resources — rtb-01c7e3c51eb92075d
Network connections (0) — Connections to other networks

Step 3:

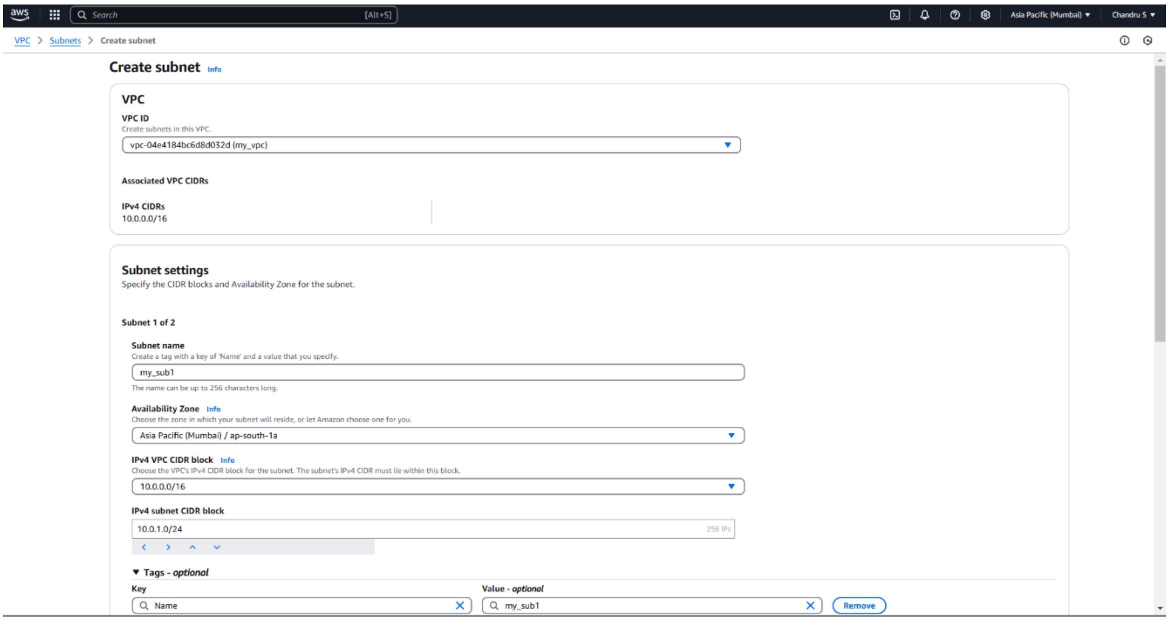
Create Subnets

You need at least two private subnets for internal communication:

1. Go to **Subnets** → Click **Create Subnet**.
2. Select the **VPC (my_vpc)** created earlier.
3. Create two subnets:

Subnet 1 (my_sub1)

- **IPv4 CIDR:** 10.0.1.0/24
- **Availability Zone:** ap-south-1a (example)



Create subnet Info

VPC

VPC ID
Create subnets in this VPC.
vpc-04e4184bc6d8d032d (my_vpc)

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_sub1
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.
Asia Pacific (Mumbai) / ap-south-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

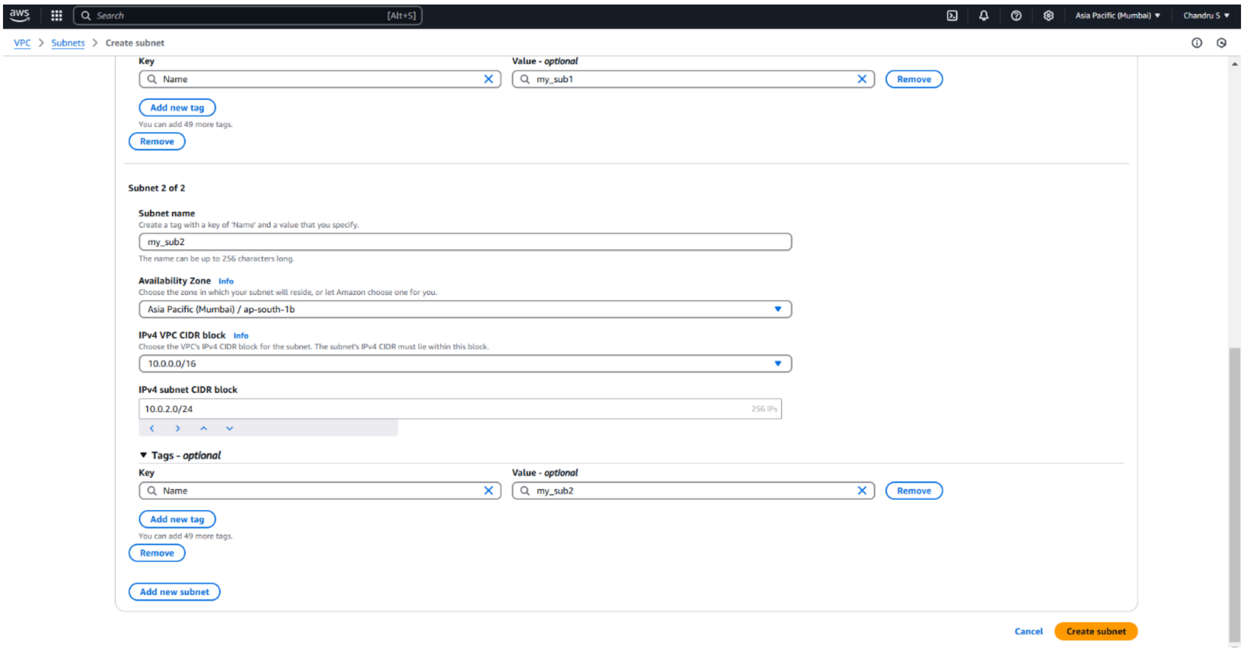
IPv4 subnet CIDR block
10.0.1.0/24 256 IPs

▼ Tags - *optional*

Key: Name
Value - *optional*: my_sub1

Subnet 2 (my_sub2)

- **IPv4 CIDR:** 10.0.2.0/24
- **Availability Zone:** ap-south-1b (example)



Key: Name
Value - *optional*: my_sub1

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.
my_sub2
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.
Asia Pacific (Mumbai) / ap-south-1b

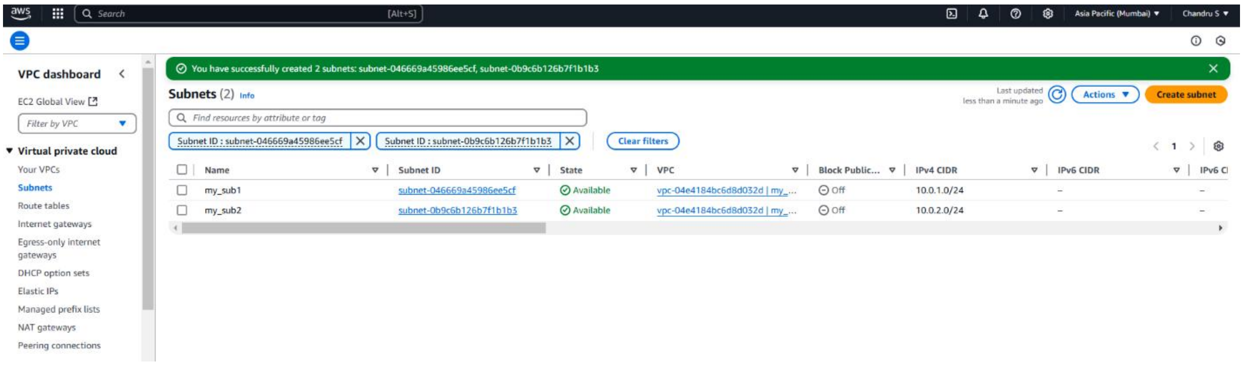
IPv4 VPC CIDR block Info
Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.
10.0.0.0/16

IPv4 subnet CIDR block
10.0.2.0/24 256 IPs

▼ Tags - *optional*
Key: Name
Value - *optional*: my_sub2

You can add 49 more tags.

Click **Create Subnet**.



You have successfully created 2 subnets: subnet-046669a45986ee5cf, subnet-0b9c6b126b7f1b1b3

Subnets (2) Info
Last updated less than a minute ago

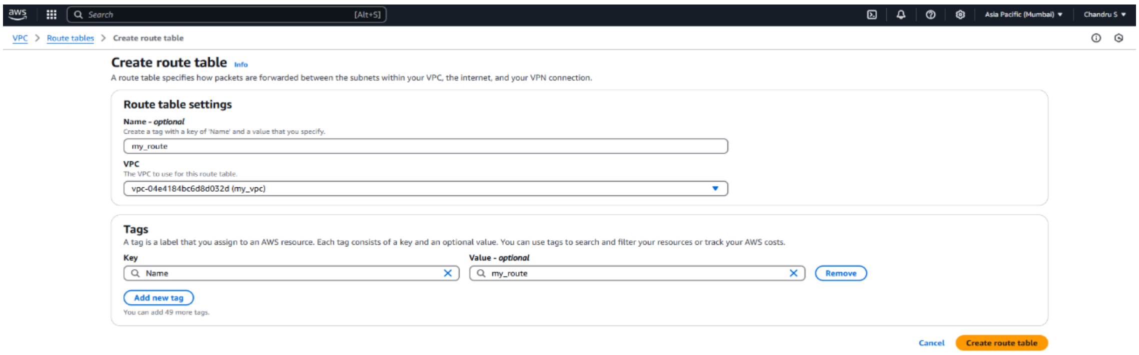
Subnet ID : subnet-046669a45986ee5cf
Subnet ID : subnet-0b9c6b126b7f1b1b3

	Name	Subnet ID	State	VPC	Block Public...	IPv4 CIDR	IPv6 CIDR	IPv6 C
□	my_sub1	subnet-046669a45986ee5cf	Available	vpc-04e4184bc6d8d032d | my_...	Off	10.0.1.0/24	–	–
□	my_sub2	subnet-0b9c6b126b7f1b1b3	Available	vpc-04e4184bc6d8d032d | my_...	Off	10.0.2.0/24	–	–

Step 4:

Configure Route Tables for Internal Communication

- Go to **Route Tables** → Click **Create Route Table.**
- Provide a Name (e.g., my_route).
- Select **my_vpc**



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

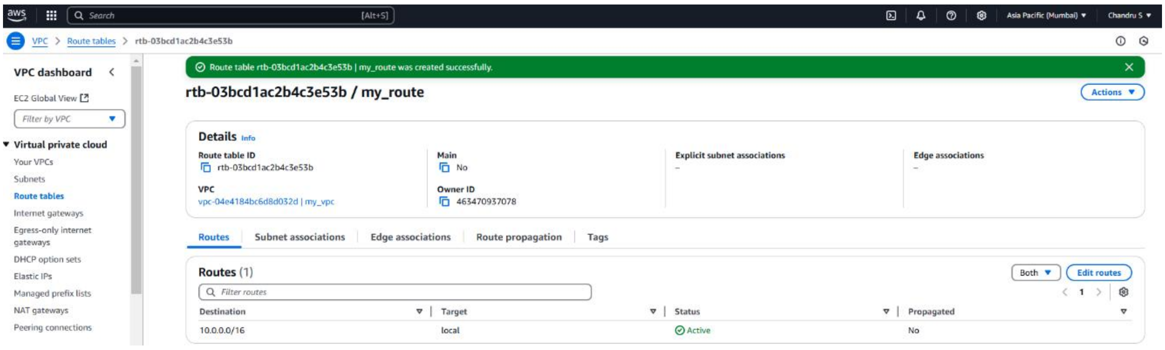
Name - *optional*
Create a tag with a key of 'Name' and a value that you specify.
my_route

VPC
The VPC to use for this route table.
vpc-04e4184bc6d8d032d (my_vpc)

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: Name
Value - *optional*: my_route

You can add 49 more tags.

- Click **Create route table**.



Route table rtb-03bcd1ac2b4c3e53b | my_route was created successfully.

rtb-03bcd1ac2b4c3e53b / my_route

Details

Route table ID: rtb-03bcd1ac2b4c3e53b
Main: No
Explicit subnet associations: –
Edge associations: –
VPC: vpc-04e4184bc6d8d032d | my_vpc
Owner ID: 463470937078

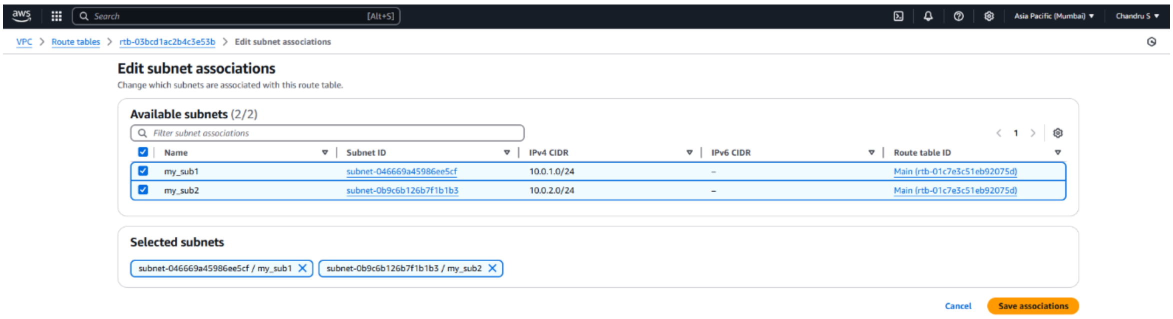
Routes (1)

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 **my_sub1** and **my_sub2**.


aws
Search [Alt+S]
Asia Pacific (Mumbai)
Chandru S
VPC > Route tables > rtb-03bcd1ac2b4c3e53b > Edit subnet associations
Filter subnet associations
Cancel
Save 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
☑	my_sub1	subnet-046669a45986ee5cf	10.0.1.0/24	–	Main (rtb-01c7e3c51eb92075d)
☑	my_sub2	subnet-0b9c6b126b7f1b1b3	10.0.2.0/24	–	Main (rtb-01c7e3c51eb92075d)

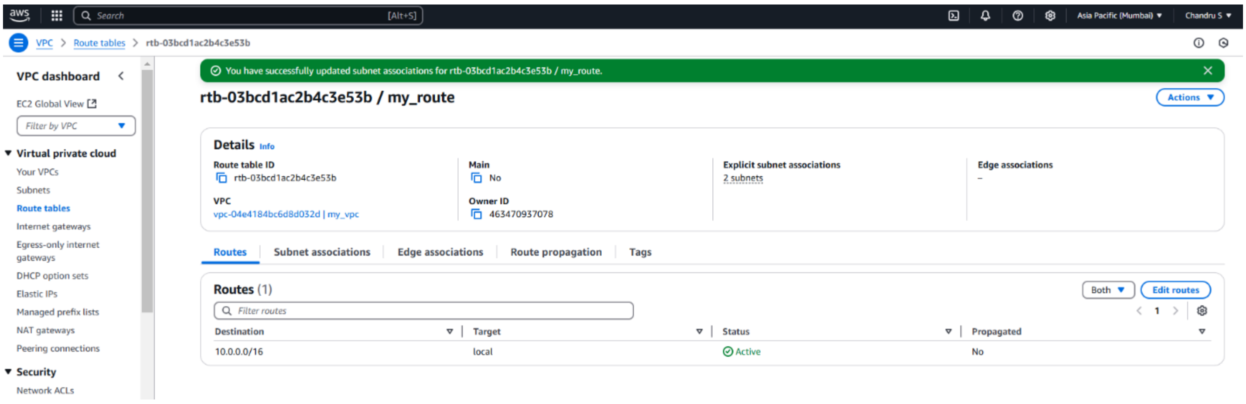
Selected subnets

subnet-046669a45986ee5cf / my_sub1 ✕
subnet-0b9c6b126b7f1b1b3 / my_sub2 ✕

- Click **Save associations**.

Step 6:

Default route (10.0.0.0/16 → local) is automatically added for internal communication.



You have successfully updated subnet associations for rtb-03bcd1ac2b4c3e53b / my_route.

rtb-03bcd1ac2b4c3e53b / my_route

Details

Route table ID: rtb-03bcd1ac2b4c3e53b
Main: No
Explicit subnet associations: 2 subnets
Edge associations: –
VPC: vpc-04e4184bc6d8d032d | my_vpc
Owner ID: 463470937078

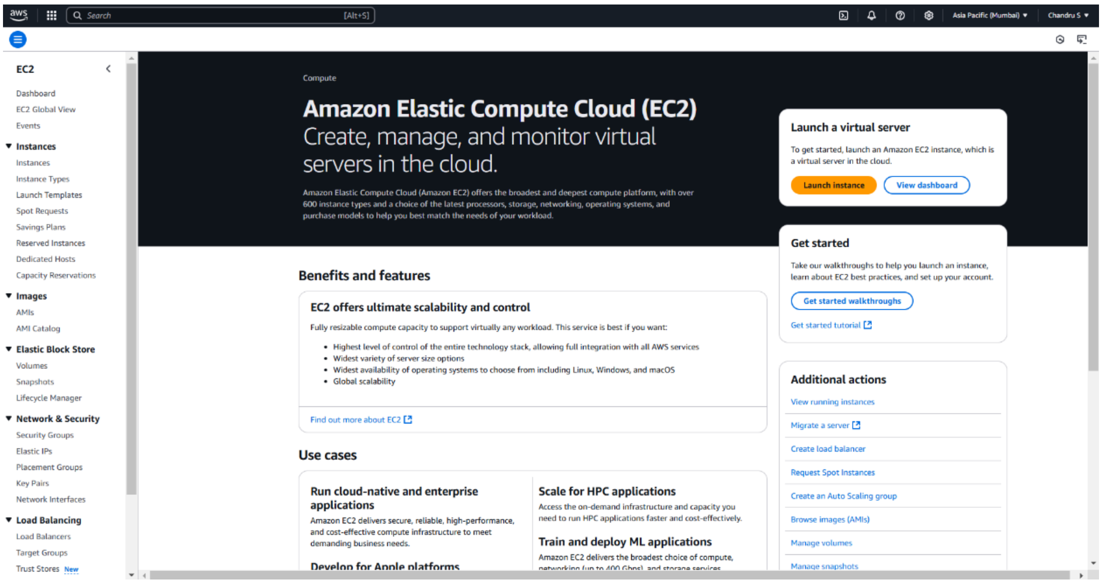
Routes (1)

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No

Step 7:

Launch Instances in Private Subnets

1. Go to **EC2 Dashboard** → Click **Launch Instance**.



Compute

Amazon Elastic Compute Cloud (EC2)

Create, manage, and monitor virtual servers in the cloud.

Amazon Elastic Compute Cloud (Amazon EC2) offers the broadest and deepest compute platform, with over 600 instance types and a choice of the latest processors, storage, networking, operating systems, and purchase models to help you best match the needs of your workload.

Launch a virtual server

To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.

Get started

Take our walkthroughs to help you launch an instance, learn about EC2 best practices, and set up your account.

Benefits and features

EC2 offers ultimate scalability and control

Fully resizable compute capacity to support virtually any workload. This service is best if you want:

- Highest level of control of the entire technology stack, allowing full integration with all AWS services
- Widest variety of server size options
- Widest availability of operating systems to choose from including Linux, Windows, and macOS
- Global scalability

Use cases

Run cloud-native and enterprise applications

Amazon EC2 delivers secure, reliable, high-performance, and cost-effective compute infrastructure to meet demanding business needs.

Develop for Apple platforms

Scale for HPC applications

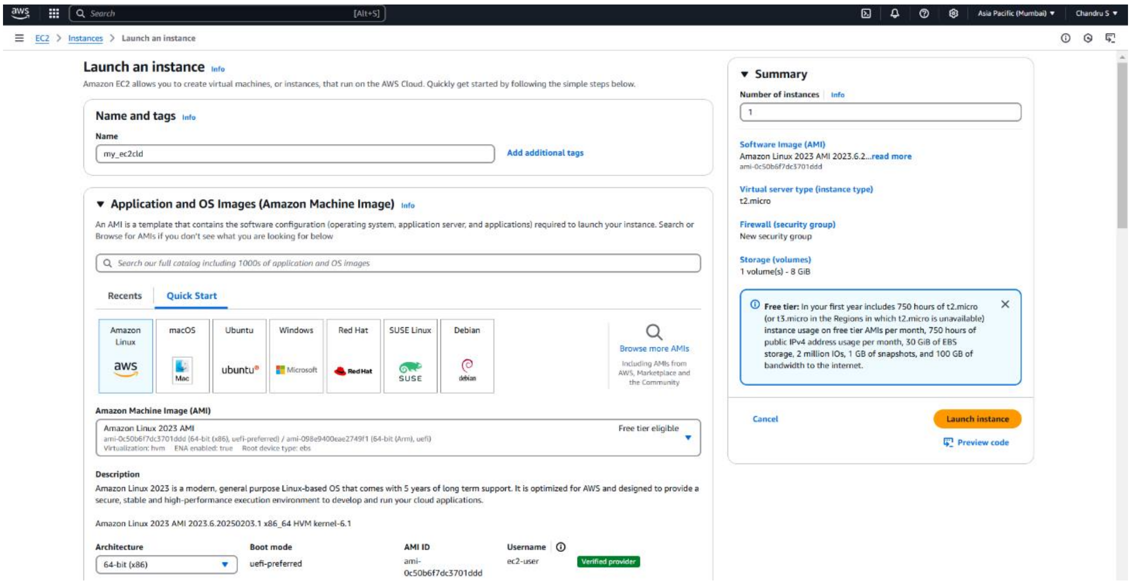
Access the on-demand infrastructure and capacity you need to run HPC applications faster and cost-effectively.

Train and deploy ML applications

Amazon EC2 delivers the broadest choice of compute, networking (up to 400 Gbps), and storage services

Additional actions

2. Select an AMI (Amazon Linux, Ubuntu, etc.).



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: my_ec2cld

▾ 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

Amazon Machine Image (AMI)

Amazon Linux 2023 AMI — Free tier eligible
ami-0c50b6f7dc3701ddd (64-bit (x86), uefi-preferred) / ami-098e9400eae2749f1 (64-bit (Arm), uefi)
Virtualization: hvm ENA enabled: true Root device type: ebs

Description

Amazon Linux 2023 is a modern, general purpose Linux-based OS that comes with 5 years of long term support. It is optimized for AWS and designed to provide a secure, stable and high-performance execution environment to develop and run your cloud applications.

Amazon Linux 2023 AMI 2023.6.20250203.1 x86_64 HVM kernel-6.1

Architecture	Boot mode	AMI ID	Username
64-bit (x86)	uefi-preferred	ami-0c50b6f7dc3701ddd	ec2-user Verified provider

▾ Summary

Number of instances: 1

Software Image (AMI)
Amazon Linux 2023 AMI 2023.6.2...read more
ami-0c50b6f7dc3701ddd

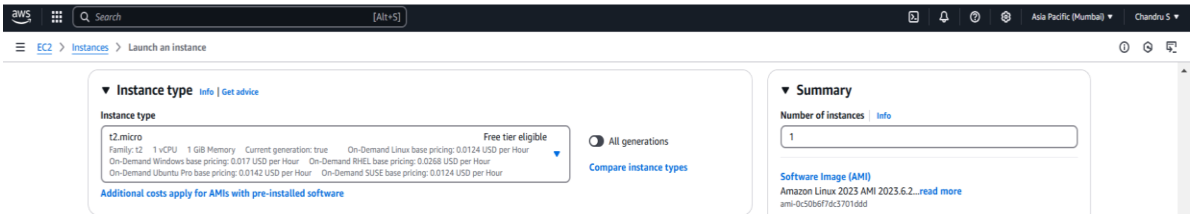
Virtual server type (instance type)
t2.micro

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 100 GB of bandwidth to the internet.

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



▼ Instance type

Instance type

t2.micro — Free tier eligible
Family: t2 1 vCPU 1 GiB Memory Current generation: true On-Demand Linux base pricing: 0.0124 USD per Hour
On-Demand Windows base pricing: 0.017 USD per Hour On-Demand RHEL base pricing: 0.0268 USD per Hour
On-Demand Ubuntu Pro base pricing: 0.0142 USD per Hour On-Demand SUSE base pricing: 0.0124 USD per Hour

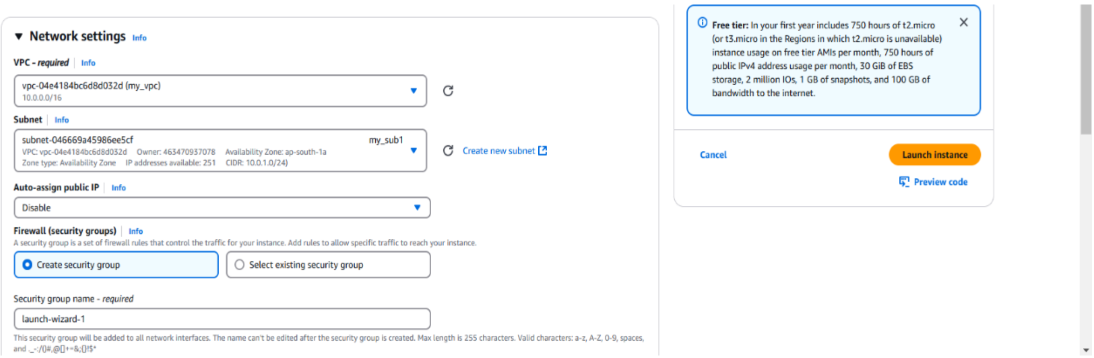
▼ Summary

Number of instances: 1

Software Image (AMI)
Amazon Linux 2023 AMI 2023.6.2...read more
ami-0c50b6f7dc3701ddd

4. Configure **Network settings**:

- Select **my_vpc**.
- Choose **my_sub1** or **my_sub2**.
- **Disable Auto-assign Public IP** to keep instances private.



▼ Network settings

VPC - *required*
vpc-04e4184bc6d8d032d (my_vpc)
10.0.0.0/16

Subnet
subnet-046669a45986ee5cf — my_sub1
VPC: vpc-04e4184bc6d8d032d Owner: 463470937078 Availability Zone: ap-south-1a
Zone type: Availability Zone IP addresses available: 251 CIDR: 10.0.1.0/24)

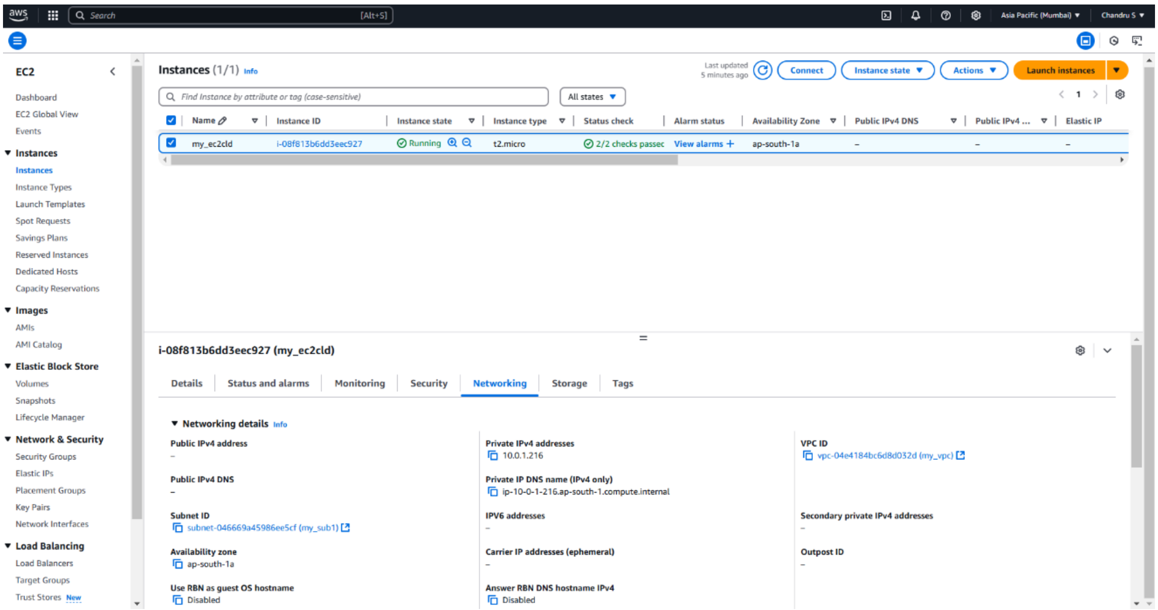
Auto-assign public IP
Disable

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*
launch-wizard-1
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 ._-:/()#,@[]+=&;{}!$*

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 100 GB of bandwidth to the internet.

5. Successfully launch instances in private subnets.



Instances (1/1)

☑	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP
☑	my_ec2cld	i-08f813b6dd3eec927	✓ Running	t2.micro	✓ 2/2 checks passec	View alarms +	ap-south-1a	–	–	–

i-08f813b6dd3eec927 (my_ec2cld)

▼ Networking details

Public IPv4 address: –

Public IPv4 DNS: –

Subnet ID: subnet-046669a45986ee5cf (my_sub1)

Availability zone: ap-south-1a

Use RBN as guest OS hostname: Disabled

Private IPv4 addresses: 10.0.1.216

Private IP DNS name (IPv4 only): ip-10-0-1-216.ap-south-1.compute.internal

IPV6 addresses: –

Carrier IP addresses (ephemeral): –

Answer RBN DNS hostname IPv4: Disabled

VPC ID: vpc-04e4184bc6d8d032d (my_vpc)

Secondary private IPv4 addresses: –

Outpost ID: –

Step 8:

Enable Internal Communication

- Instances within private subnets can communicate without an internet gateway.
- If internet access is required (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:

Your private network is now configured, and instances inside can securely communicate!
If additional configurations are needed (e.g., **VPN, Bastion Host, NAT Gateway**), let me know.

Outcome

By completing these steps, you will achieve:

- A fully isolated VPC, ensuring your resources are secure and separate from other networks.
- One or more subnets for your instances, including at least one public subnet capable of internet communication.
- Properly configured routing to enable seamless internal communication between subnets.