AWS VPC Design – Step-by-Step Console Guide

Purpose

This document provides a step-by-step guide to creating an enterprise-grade VPC architecture in the AWS Console. Screenshot placeholders are included for audit, lab submission, or documentation purposes.

Task 1: Create VPC

1.Open AWS Console → VPC
2. Click Your VPCs → Create VPC
3. Name: Enterprise-VPC
4. CIDR: 10.0.0.0/16
5. Create VPC

Single VPC architecture

Minimum VPC CIDR size: /16

Exactly six subnets with unequal sizes

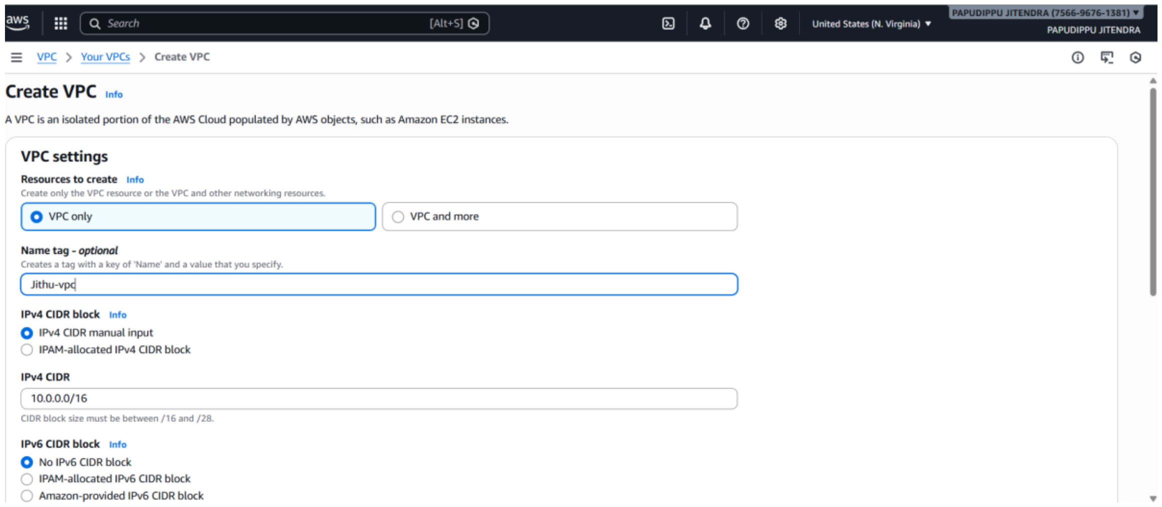
Subnets must be allocated largest to smallest

No overlapping CIDRs

Correct CIDR network boundaries only

Internet access must be explicit and controller

Security Groups and NACLs are out of scope


aws
Search [Alt+S]
United States (N. Virginia)
PAPUDIPPU JITENDRA (7566-9676-1381)
PAPUDIPPU JITENDRA
VPC > Your VPCs > Create VPC

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.
Jithu-vpc

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

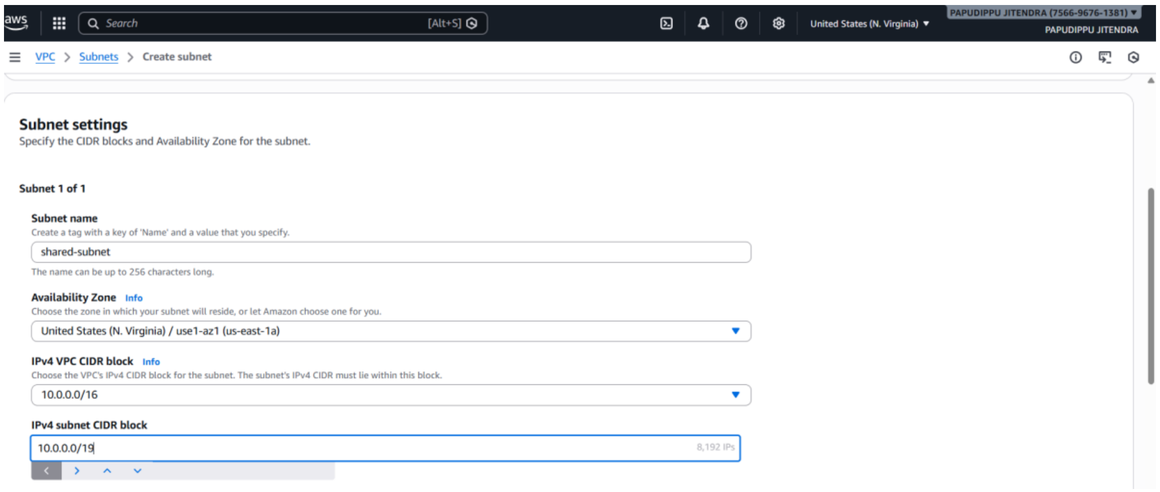
Task 2: Create Subnets

Create the following subnets in order:

Shared: 10.0.0.0/19
Platform: 10.0.32.0/20
App: 10.0.48.0/21
Web: 10.0.56.0/22
Edge: 10.0.60.0/23
Admin: 10.0.62.0/24

Subnet	Required IPs	CIDR
Shared	~8,192	/19
Platform	~4,096	/20
App	~2,048	/21
Web	~1,024	/22
Edge	~512	/23
Admin	~256	/24

Shared-subnet


aws
Search
[Alt+S]
United States (N. Virginia)
PAPUDIPPU JITENDRA (7566-9676-1381)
PAPUDIPPU JITENDRA
VPC > Subnets > Create subnet

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

Subnet 1 of 1

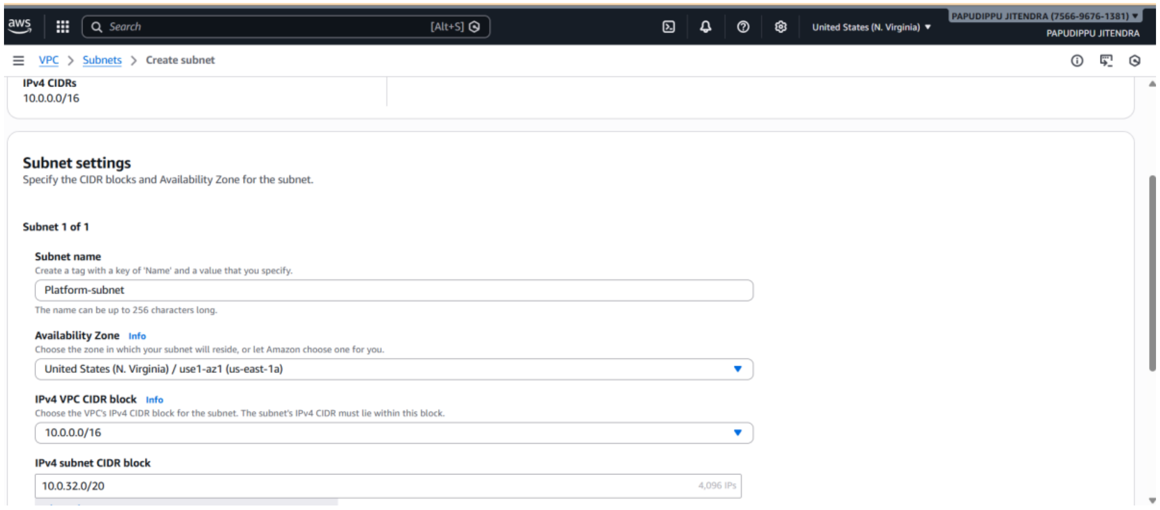
Subnet name
Create a tag with a key of 'Name' and a value that you specify.
shared-subnet
The name can be up to 256 characters long.

Availability Zone Info
Choose the zone in which your subnet will reside, or let Amazon choose one for you.
United States (N. Virginia) / use1-az1 (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

IPv4 subnet CIDR block
10.0.0.0/19 8,192 IPs

Platform-Subnet


Search [Alt+S]
United States (N. Virginia)
PAPUDIPPU JITENDRA (7566-9676-1381)
PAPUDIPPU JITENDRA
VPC > Subnets > Create subnet

IPv4 CIDRs
10.0.0.0/16

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

Subnet 1 of 1

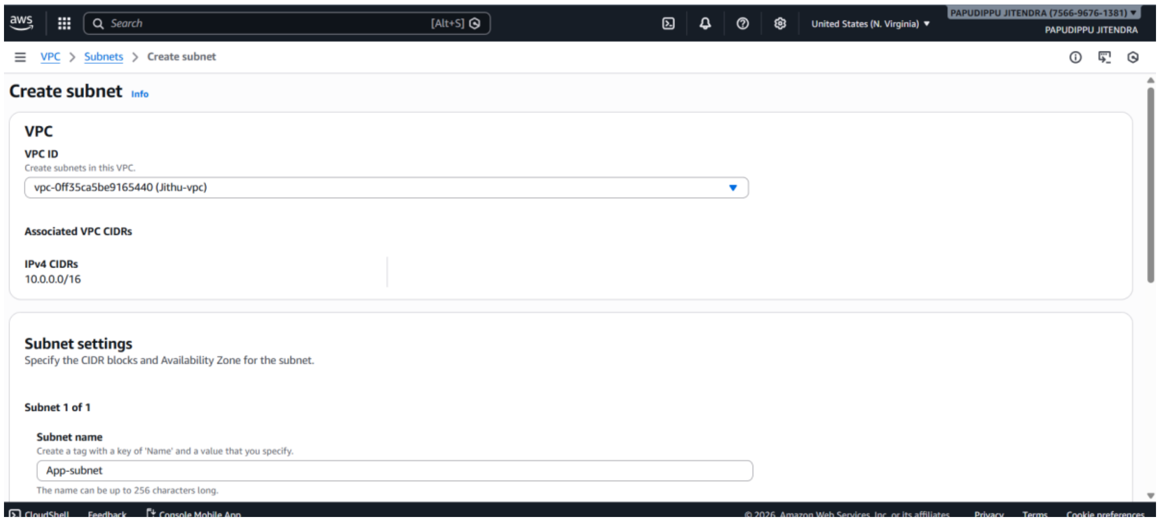
Subnet name
Create a tag with a key of 'Name' and a value that you specify.
Platform-subnet
The name can be up to 256 characters long.

Availability Zone Info
Choose the zone in which your subnet will reside, or let Amazon choose one for you.
United States (N. Virginia) / use1-az1 (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

IPv4 subnet CIDR block
10.0.32.0/20 4,096 IPs

App-subnet


Search [Alt+S]
United States (N. Virginia)
PAPUDIPPU JITENDRA (7566-9676-1381)
PAPUDIPPU JITENDRA
VPC > Subnets > Create subnet
CloudShell
Feedback
Console Mobile App
© 2026, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Create subnet Info

VPC
VPC ID
Create subnets in this VPC.
vpc-0ff35ca5be9165440 (Jithu-vpc)

Associated VPC CIDRs

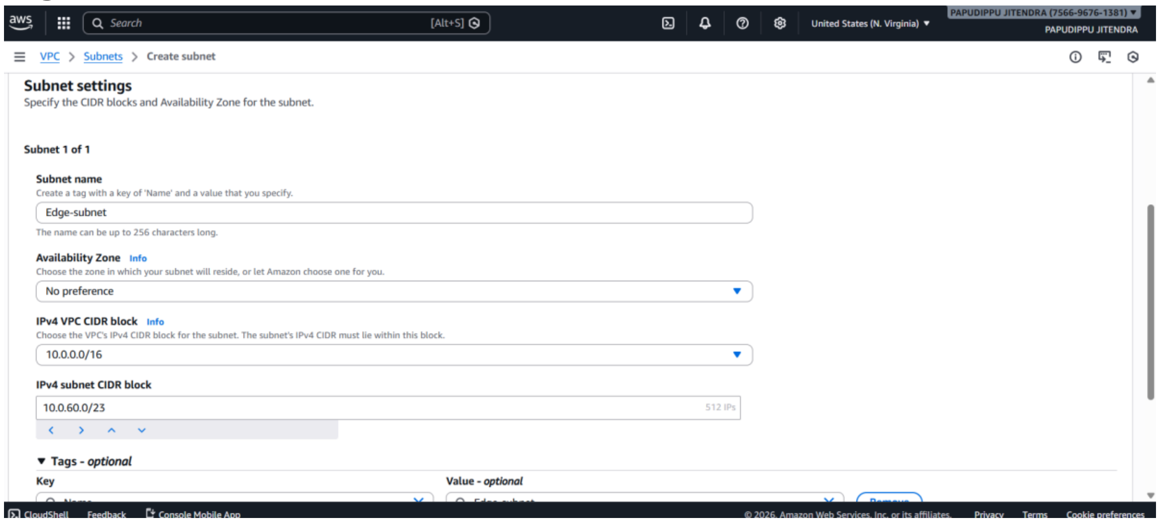
IPv4 CIDRs
10.0.0.0/16

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

Subnet 1 of 1

Subnet name
Create a tag with a key of 'Name' and a value that you specify.
App-subnet
The name can be up to 256 characters long.

Edge-Subnet:



VPC > Subnets > Create subnet

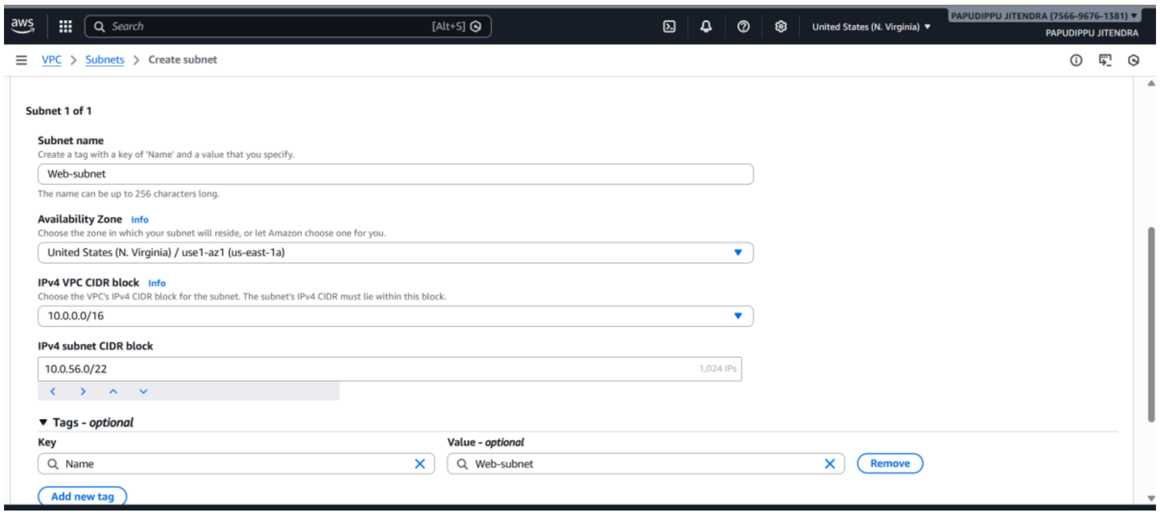
Subnet settings
Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

Subnet name: Edge-subnet
Availability Zone: No preference
IPv4 VPC CIDR block: 10.0.0.0/16
IPv4 subnet CIDR block: 10.0.60.0/23 (512 IPs)

Tags - optional

Web-Subnet:



VPC > Subnets > Create subnet

Subnet 1 of 1

Subnet name: Web-subnet
Availability Zone: United States (N. Virginia) / use1-az1 (us-east-1a)
IPv4 VPC CIDR block: 10.0.0.0/16
IPv4 subnet CIDR block: 10.0.56.0/22 (1,024 IPs)

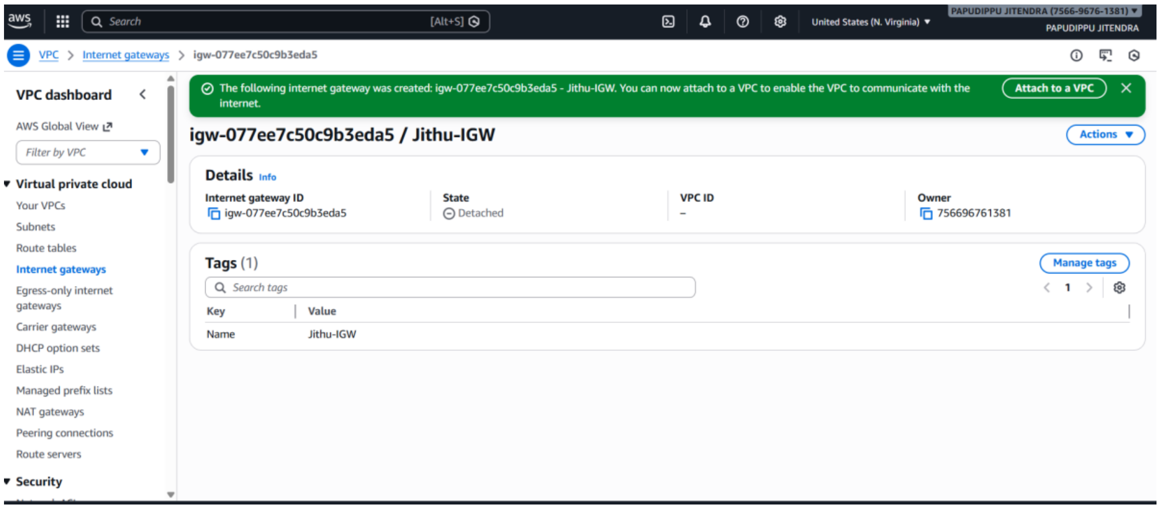
Tags - optional

Key	Value - optional
Name	Web-subnet

Task 3: Internet Gateway

1.Create Internet Gateway
2. Name: Enterprise-IGW
3. Attach to Enterprise-VPC

IGW is Created



The following internet gateway was created: igw-077ee7c50c9b3eda5 - Jithu-IGW. You can now attach to a VPC to enable the VPC to communicate with the internet.

igw-077ee7c50c9b3eda5 / Jithu-IGW

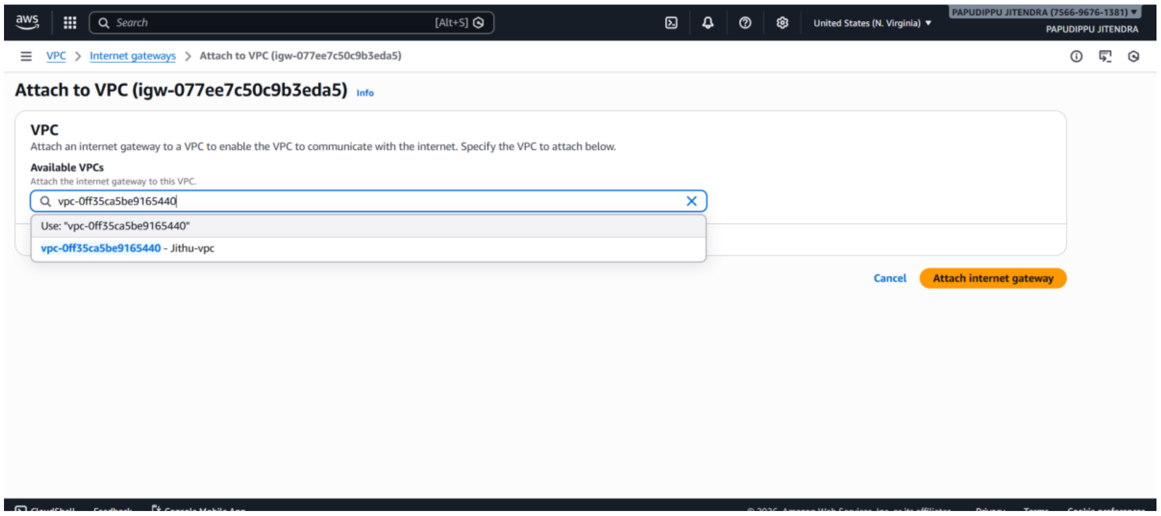
Details Info

Internet gateway ID	State	VPC ID	Owner
igw-077ee7c50c9b3eda5	Detached	–	756696761381

Tags (1)

Key	Value
Name	Jithu-IGW

IGW Attached to VPC

1. 

Search
[Alt+S]
United States (N. Virginia)
PAPUDIPPU JITENDRA (7566-9676-1381)
PAPUDIPPU JITENDRA
VPC > Internet gateways > Attach to VPC (igw-077ee7c50c9b3eda5)
Cancel
Attach internet gateway

Attach to VPC (igw-077ee7c50c9b3eda5) Info

VPC

Attach an internet gateway to a VPC to enable the VPC to communicate with the internet. Specify the VPC to attach below.

Available VPCs

Attach the internet gateway to this VPC.

vpc-0ff35ca5be9165440

Use: "vpc-0ff35ca5be9165440"

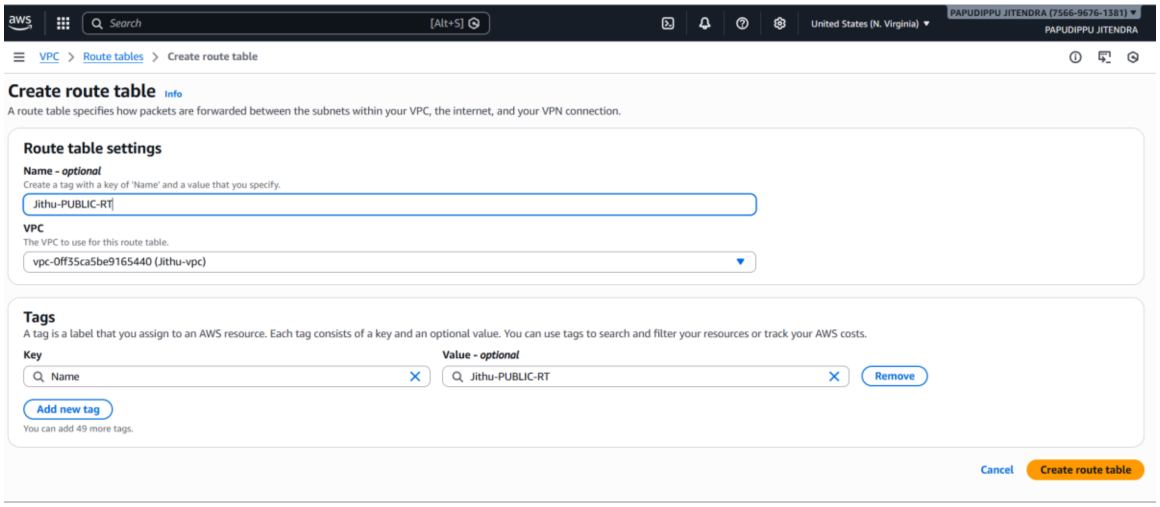
vpc-0ff35ca5be9165440 - Jithu-vpc

Task 4: Route Tables

Public-RT:
0.0.0.0/0 → IGW

Private-RT:
Local route only

Public Route Table


VPC > Route tables > Create route table

Create route table

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*: Jithu-PUBLIC-RT

VPC: vpc-0ff35ca5be9165440 (Jithu-vpc)

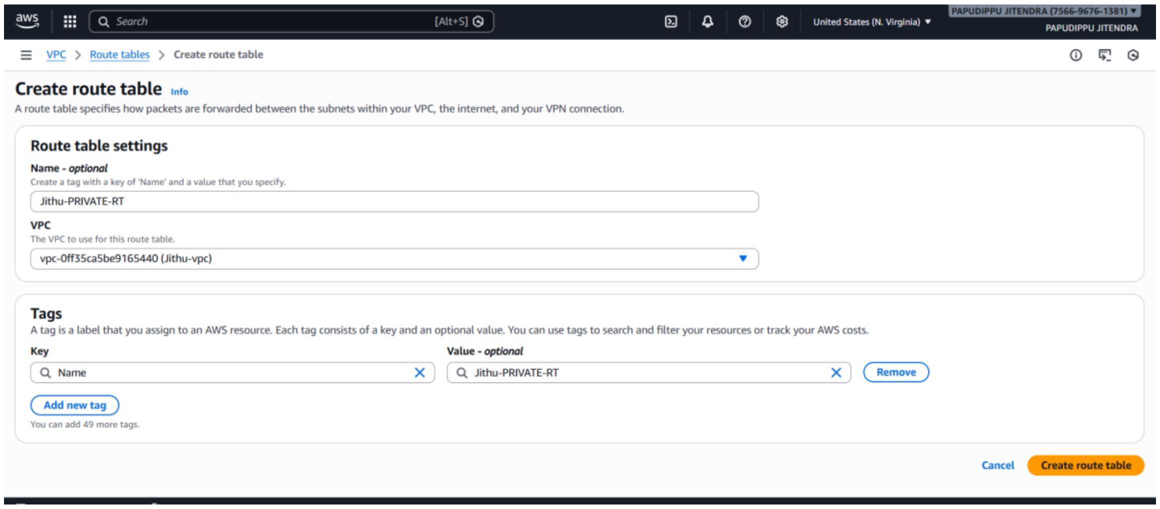
Tags

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	Value - *optional*
Name	Jithu-PUBLIC-RT

You can add 49 more tags.

Private-Route Table


VPC > Route tables > Create route table

Create route table

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*: Jithu-PRIVATE-RT

VPC: vpc-0ff35ca5be9165440 (Jithu-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.

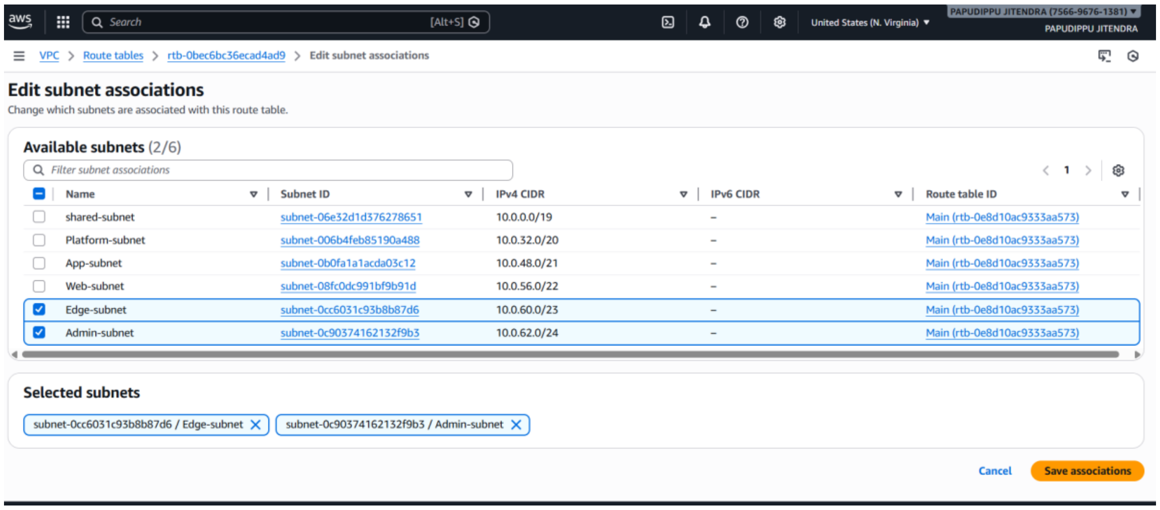
Key	Value - *optional*
Name	Jithu-PRIVATE-RT

You can add 49 more tags.

Task 5: Route Table Associations

Public-RT → Admin, Edge

Private-RT → Web, App, Platform, Shared



VPC > Route tables > rtb-0bec6bc36ecad4ad9 > Edit subnet associations

Edit subnet associations

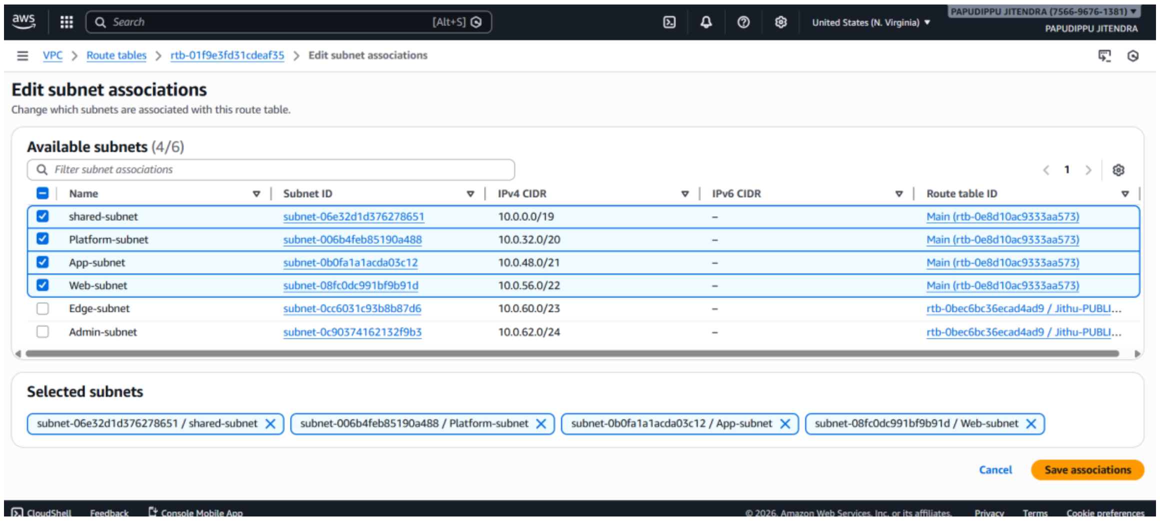
Change which subnets are associated with this route table.

Available subnets (2/6)

	Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
☐	shared-subnet	subnet-06e32d1d376278651	10.0.0.0/19	–	Main (rtb-0e8d10ac9333aa573)
☐	Platform-subnet	subnet-006b4feb85190a488	10.0.32.0/20	–	Main (rtb-0e8d10ac9333aa573)
☐	App-subnet	subnet-0b0fa1a1acda03c12	10.0.48.0/21	–	Main (rtb-0e8d10ac9333aa573)
☐	Web-subnet	subnet-08fc0dc991bf9b91d	10.0.56.0/22	–	Main (rtb-0e8d10ac9333aa573)
☑	Edge-subnet	subnet-0cc6031c93b8b87d6	10.0.60.0/23	–	Main (rtb-0e8d10ac9333aa573)
☑	Admin-subnet	subnet-0c90374162132f9b3	10.0.62.0/24	–	Main (rtb-0e8d10ac9333aa573)

Selected subnets

subnet-0cc6031c93b8b87d6 / Edge-subnet
subnet-0c90374162132f9b3 / Admin-subnet



VPC > Route tables > rtb-01f9e3fd31cdeaf35 > Edit subnet associations

Edit subnet associations

Change which subnets are associated with this route table.

Available subnets (4/6)

	Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
☑	shared-subnet	subnet-06e32d1d376278651	10.0.0.0/19	–	Main (rtb-0e8d10ac9333aa573)
☑	Platform-subnet	subnet-006b4feb85190a488	10.0.32.0/20	–	Main (rtb-0e8d10ac9333aa573)
☑	App-subnet	subnet-0b0fa1a1acda03c12	10.0.48.0/21	–	Main (rtb-0e8d10ac9333aa573)
☑	Web-subnet	subnet-08fc0dc991bf9b91d	10.0.56.0/22	–	Main (rtb-0e8d10ac9333aa573)
☐	Edge-subnet	subnet-0cc6031c93b8b87d6	10.0.60.0/23	–	rtb-0bec6bc36ecad4ad9 / Jithu-PUBLI...
☐	Admin-subnet	subnet-0c90374162132f9b3	10.0.62.0/24	–	rtb-0bec6bc36ecad4ad9 / Jithu-PUBLI...

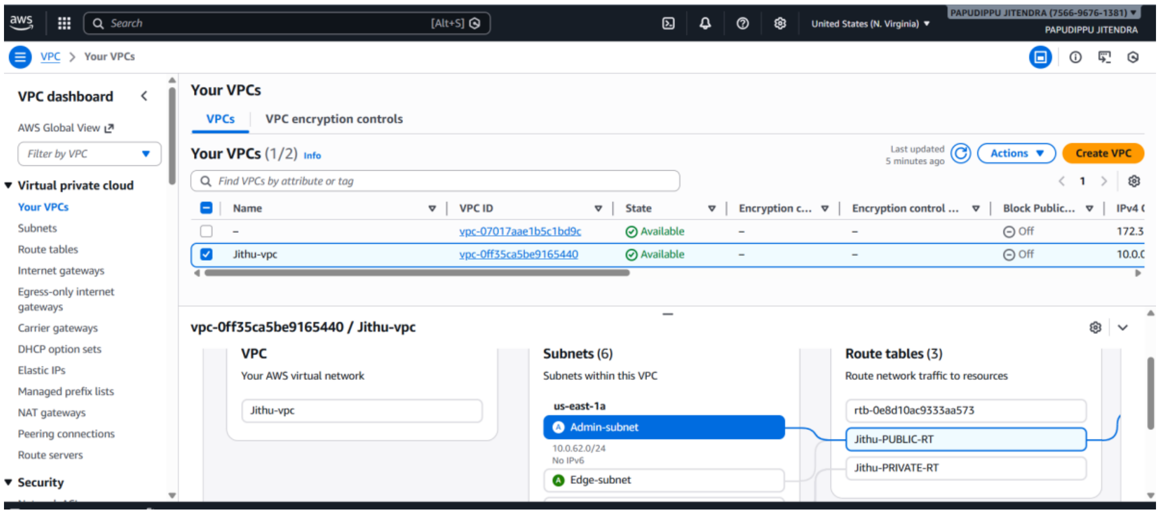
Selected subnets

subnet-06e32d1d376278651 / shared-subnet
subnet-006b4feb85190a488 / Platform-subnet
subnet-0b0fa1a1acda03c12 / App-subnet
subnet-08fc0dc991bf9b91d / Web-subnet

Task 6: Validation

Public subnets have internet access via IGW.
Private subnets have no default route and are isolated.
All subnets communicate internally via local routing.

Subnet with Public Route table



Your VPCs

Your VPCs (1/2) Info

Name	VPC ID	State	Encryption c...	Encryption control ...	Block Public...	IPv4 (
–	vpc-07017aae1b5c1bd9c	Available	–	–	Off	172.3
Jithu-vpc	vpc-0ff35ca5be9165440	Available	–	–	Off	10.0.(

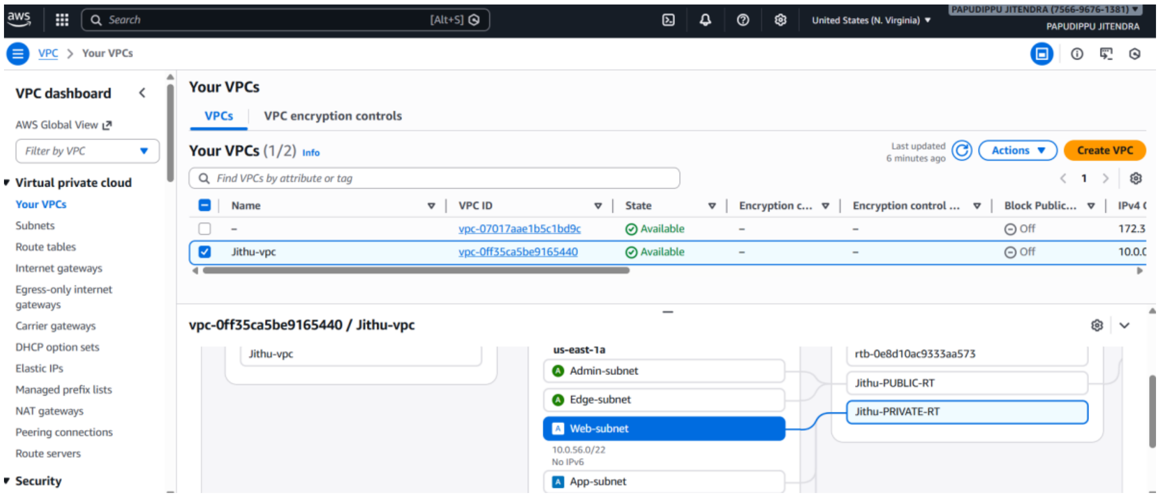
vpc-0ff35ca5be9165440 / Jithu-vpc

VPC
Your AWS virtual network
Jithu-vpc

Subnets (6)
Subnets within this VPC
us-east-1a
Admin-subnet
10.0.62.0/24
No IPv6
Edge-subnet

Route tables (3)
Route network traffic to resources
rtb-0e8d10ac9333aa573
Jithu-PUBLIC-RT
Jithu-PRIVATE-RT

Subnet with Private Route table



Your VPCs

Your VPCs (1/2) Info

Name	VPC ID	State	Encryption c...	Encryption control ...	Block Public...	IPv4 (
–	vpc-07017aae1b5c1bd9c	Available	–	–	Off	172.3
Jithu-vpc	vpc-0ff35ca5be9165440	Available	–	–	Off	10.0.(

vpc-0ff35ca5be9165440 / Jithu-vpc

Jithu-vpc

us-east-1a
Admin-subnet
Edge-subnet
Web-subnet
10.0.56.0/22
No IPv6
App-subnet

rtb-0e8d10ac9333aa573
Jithu-PUBLIC-RT
Jithu-PRIVATE-RT

Audit & Failure Scenarios

- Detaching IGW removes all internet access
- Associating private subnet with Public-RT exposes it
- Incorrect CIDR boundaries cause overlap and failure

Validation & Testing

This section validates that the VPC networking design behaves as intended based solely on **routing architecture**, without relying on security groups or NACLs.

7.1 Public Subnet Instance Validation

Test Scenario

An EC2 instance is launched in a public subnet (Admin or Edge subnet) with an assigned public IPv4 address.

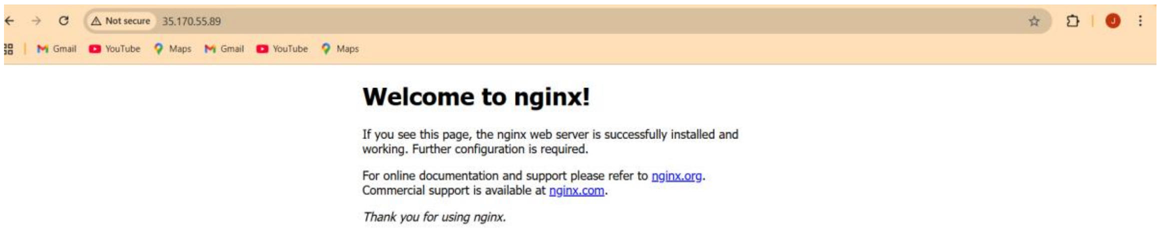
Observed Behavior

- The instance successfully accesses the internet
- Outbound traffic to external IP addresses is permitted
- Inbound access (e.g., HTTP/SSH) is reachable as configured

Reason

- The subnet is associated with the **Public Route Table**
- The route table contains the following entry:
- 0.0.0.0/0 → Internet Gateway (IGW)
- The presence of a public IP allows return traffic from the internet

Conclusion
Public subnets have intentional internet access through explicit routing to the Internet Gateway.



Welcome to nginx!

If you see this page, the nginx web server is successfully installed and working. Further configuration is required.

For online documentation and support please refer to nginx.org.
Commercial support is available at nginx.com.

Thank you for using nginx.

8. Failure Scenarios & Design Considerations

This section explains how AWS behaves under misconfiguration scenarios and how the current design mitigates operational and security risks.

8.1 Internet Gateway (IGW) Detached from VPC

Scenario

The Internet Gateway attached to the VPC is detached or deleted.

Observed Behavior

- All internet connectivity immediately stops
- Public subnets lose outbound and inbound internet access
- EC2 instances remain reachable only within the VPC

Reason

- The Internet Gateway is the only component that enables traffic between the VPC and the internet
- Even if a route table contains 0.0.0.0/0, traffic cannot exit the VPC without an attached IGW

Impact

- Public subnets effectively behave as private subnets
- Internal VPC communication remains unaffected

Conclusion

The IGW is a single, controlled point of internet access. Its removal enforces complete network isolation.

8.2 Private Subnet Associated with Public Route Table

Scenario

A private subnet is mistakenly associated with the Public Route Table.

Observed Behavior

- The subnet gains a default route to the Internet Gateway
- Instances in the subnet can access the internet
- The subnet becomes externally reachable if public IPs are assigned

Reason

- Route tables define network behavior

- Associating a subnet with a route table containing 0.0.0.0/0 → IGW makes it a public subnet

Impact

- Security boundary is violated
- Unintended exposure of internal services
- High-severity audit and compliance failure

Conclusion
Explicit route table associations are mandatory to prevent accidental exposure of private resources.

8.3 Incorrect CIDR Block Starting Address

Scenario

A subnet CIDR block is created using an incorrect network boundary (e.g., starting a /19 at an invalid IP).

Observed Behavior

- AWS rejects the subnet creation request
- Error indicates overlapping or invalid CIDR range

Reason

- CIDR blocks must start on correct binary boundaries
- Example: a /19 must start at multiples of 32 in the third octet
- Valid: 10.0.0.0/19
- Invalid: 10.0.5.0/19

Impact

- Subnet creation fails
- Network design cannot be deployed

Conclusion

Proper CIDR alignment is critical to prevent overlap and ensure predictable network segmentation.