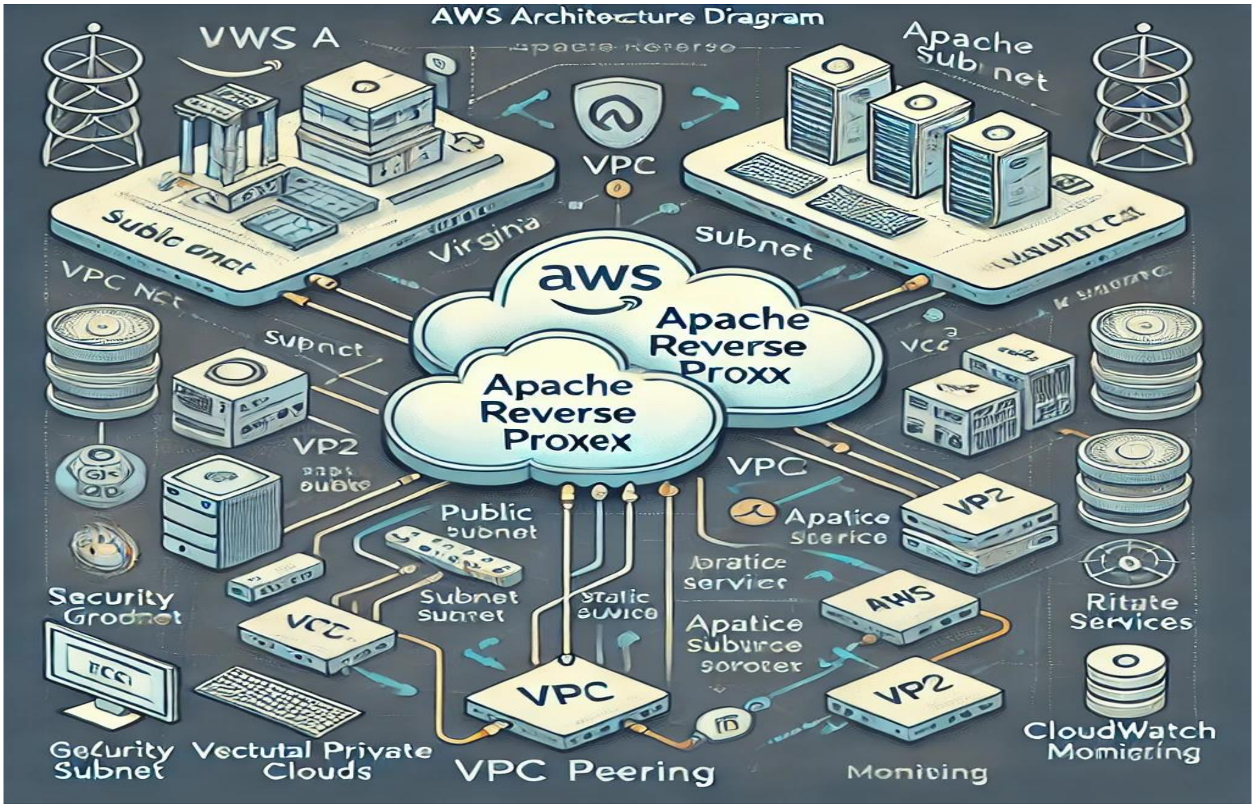
cprime

VPC Peering and Apache Reverse Proxy-Based Application Hosting



NAME : T MANOJ

EMPID : LYAKE2KHS

Introduction

This project aims to establish a robust networking infrastructure by creating a VPC peering connection between two Virtual Private Clouds (VPCs). The objective is to enable secure and efficient communication between VPCs while hosting a static web application. The application will leverage Apache HTTP Server for reverse proxy configuration, ensuring optimal routing and performance. This project also focuses on delivering high availability, scalability, and secure application access.

Project Overview

This project establishes VPC peering between two Virtual Private Clouds (VPCs) with application hosting and reverse proxy configuration using Apache. The application will have:

- **Seamless communication** between VPC A and VPC B via VPC peering.
- **High availability** and **scalability** for the hosted application.
- **Reverse proxy setup** using Apache HTTP Server for efficient routing and load management.
- **Static web application hosting** using HTML and CSS.

VPC Configurations

- **VPC A (Virginia):**
    - CIDR: 27.50.0.0/16
    - Public Subnet: 27.50.10.128/24
    - Private Subnet: 27.50.20.128/24
- **VPC B (OHIO):**
    - CIDR: 27.60.10.0/16
    - Public Subnet: 27.50.10.0/24
    - Private Subnet: 27.50.20.0/24

Key Components

1. **VPC Peering Connection**

a. Establish peering between VPC A and VPC B.
b. Update route tables to allow traffic flow between VPCs.

2. **Application Hosting**

a. Deploy HTML/CSS-based static web application on EC2 instances.
b. Configure security groups for HTTP/HTTPS access.

3. **Apache Reverse Proxy Configuration**
a. Install and configure Apache HTTP Server on EC2 instances.
b. Enable proxy modules and configure virtual hosts for routing.
4. **Testing and Validation**
a. Verify connectivity between VPCs through peering.
b. Test application accessibility and reverse proxy routing.
5. **Security and Monitoring**
a. Implement IAM roles and security best practices.
b. Set up CloudWatch for monitoring application and server health.

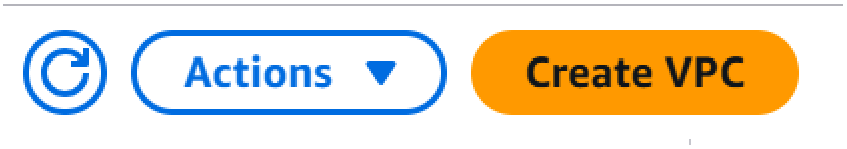
Deliverables

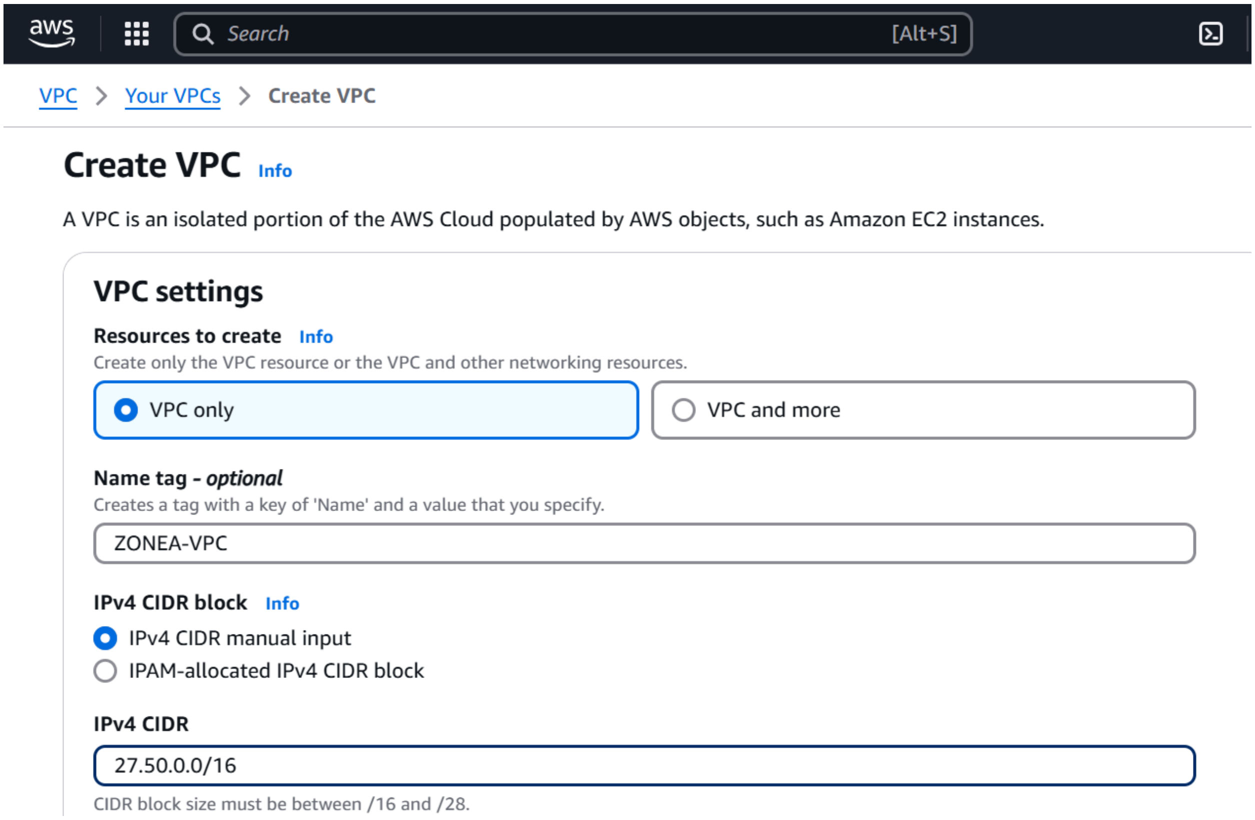
- Functional VPC peering connection.
- Accessible web application hosted on EC2 instances.
- Fully configured Apache reverse proxy.
- Documentation of configurations and processes.

Step-by-Step Implementation

Step 1: Set Up VPC A (Virginia Region)

1. **Create VPC A:**
    a. CIDR: 27.50.0.0/16
    b. Enable DNS Hostnames





Create VPC Info

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

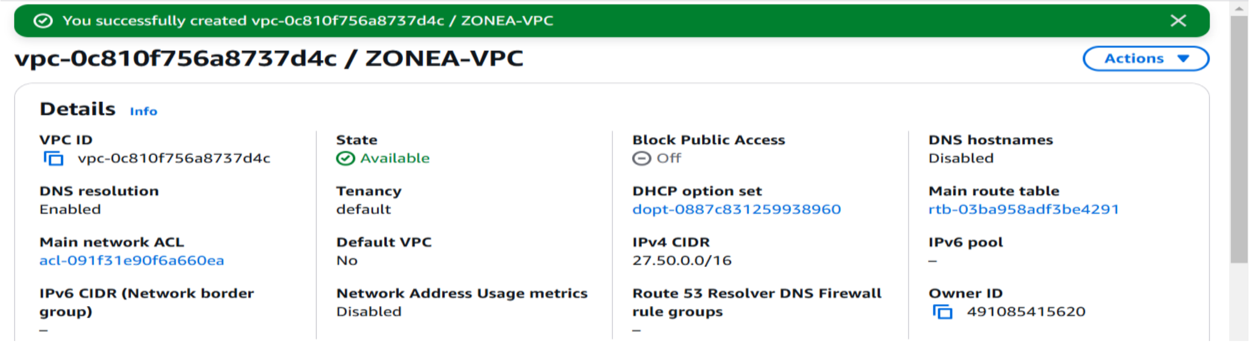
VPC settings

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.
ZONEA-VPC

IPv4 CIDR block Info
● IPv4 CIDR manual input
○ IPAM-allocated IPv4 CIDR block

IPv4 CIDR
27.50.0.0/16
CIDR block size must be between /16 and /28.

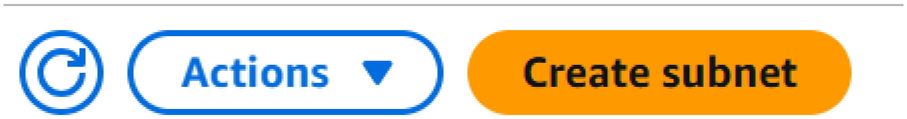

You successfully created vpc-0c810f756a8737d4c / ZONEA-VPC

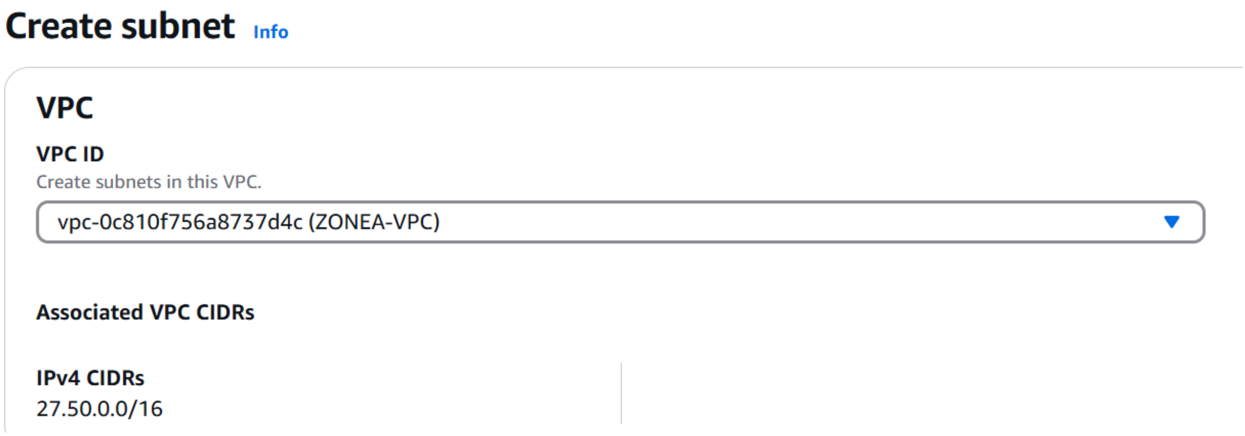
vpc-0c810f756a8737d4c / ZONEA-VPC

Details Info

VPC ID vpc-0c810f756a8737d4c	State Available	Block Public Access Off	DNS hostnames Disabled
DNS resolution Enabled	Tenancy default	DHCP option set dopt-0887c831259938960	Main route table rtb-03ba958adf3be4291
Main network ACL acl-091f31e90f6a660ea	Default VPC No	IPv4 CIDR 27.50.0.0/16	IPv6 pool –
IPv6 CIDR (Network border group) –	Network Address Usage metrics Disabled	Route 53 Resolver DNS Firewall rule groups –	Owner ID 491085415620

2. **Create Subnets:**
   a. Public Subnet (pubsub-a): 27.50.10.128/24
   b. Private Subnet (privsub-a): 27.50.20.128/24





Create subnet Info

VPC

VPC ID

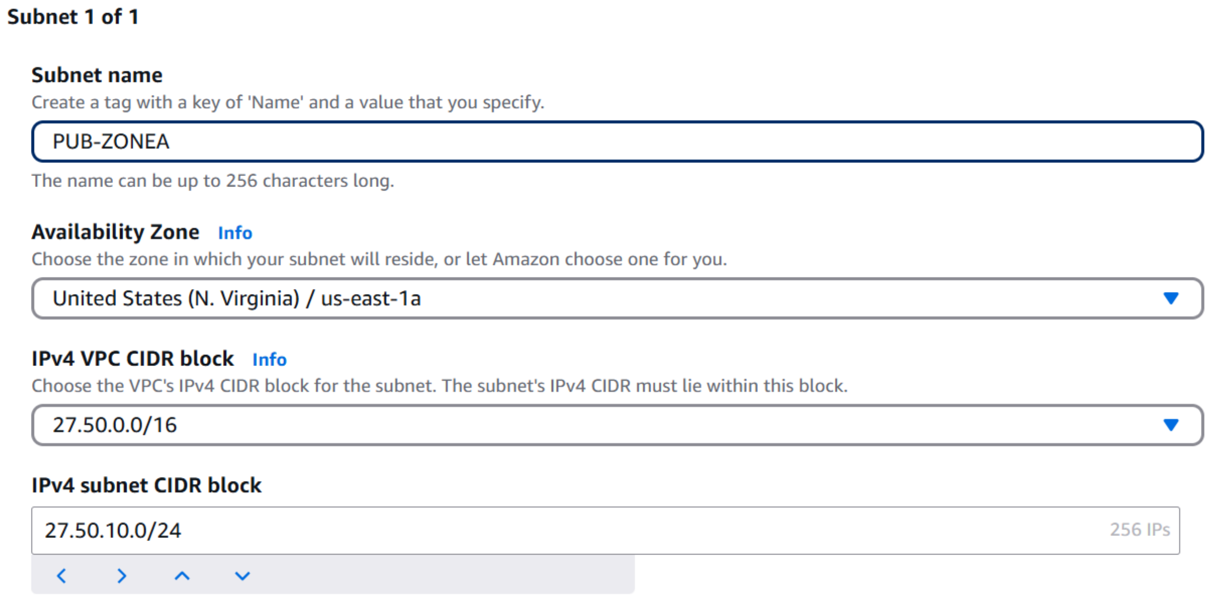
Create subnets in this VPC.

vpc-0c810f756a8737d4c (ZONEA-VPC)

Associated VPC CIDRs

IPv4 CIDRs

27.50.0.0/16



Subnet 1 of 1

Subnet name

Create a tag with a key of 'Name' and a value that you specify.

PUB-ZONEA

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) / us-east-1a

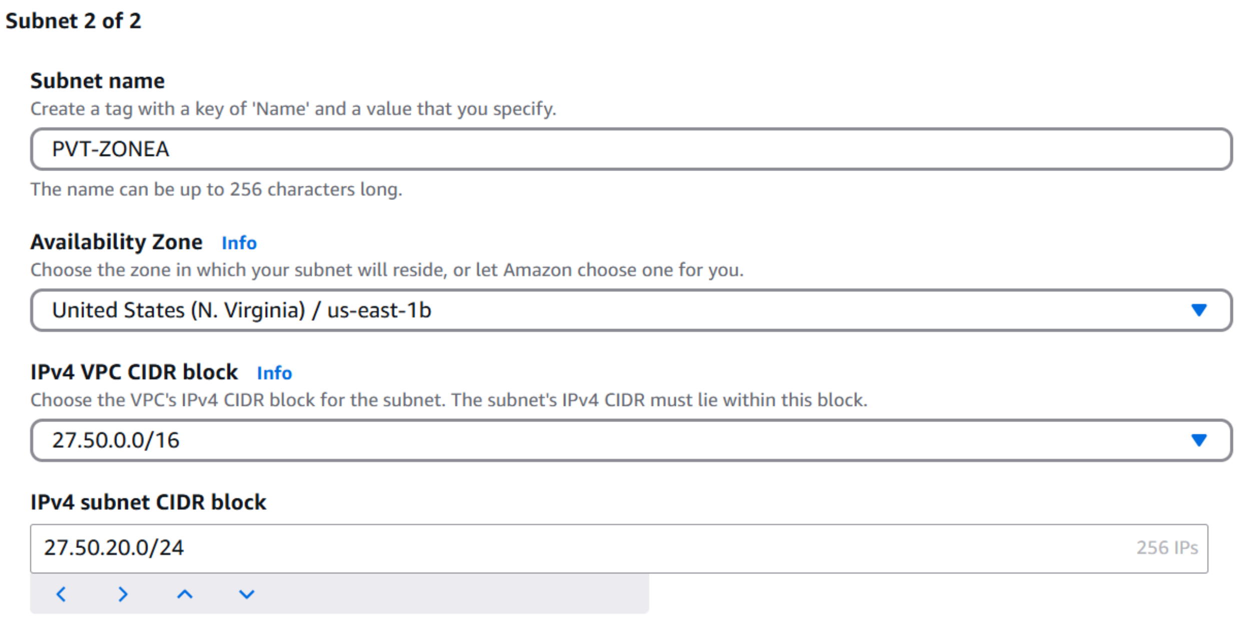
IPv4 VPC CIDR block Info

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

27.50.0.0/16

IPv4 subnet CIDR block

27.50.10.0/24 256 IPs



Subnet 2 of 2

Subnet name

Create a tag with a key of 'Name' and a value that you specify.

PVT-ZONEA

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) / us-east-1b ▼

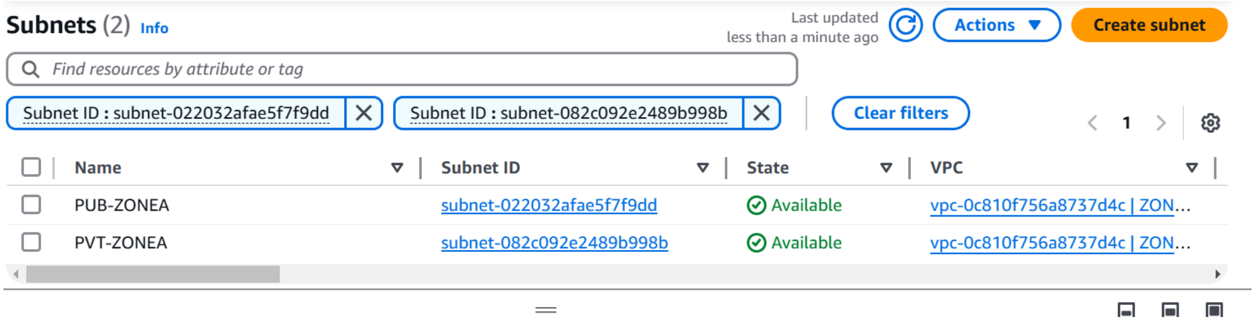
IPv4 VPC CIDR block Info

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

27.50.0.0/16 ▼

IPv4 subnet CIDR block

27.50.20.0/24 256 IPs



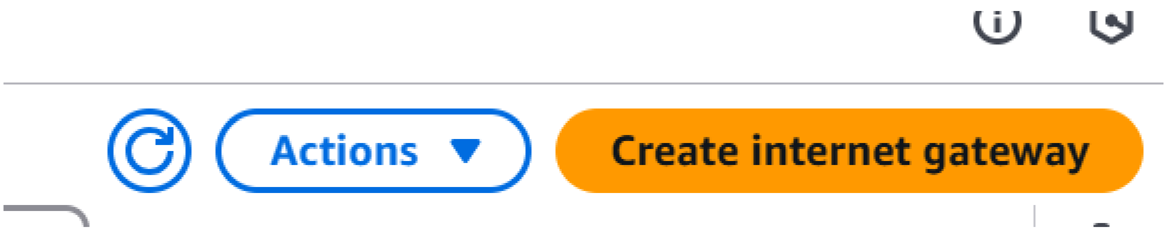
Subnets (2) Info

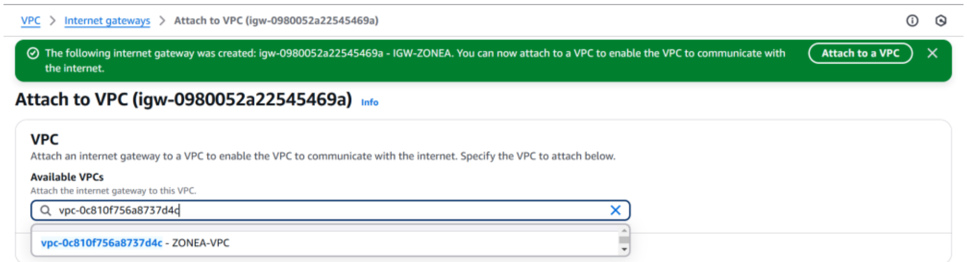
Last updated less than a minute ago

Subnet ID : subnet-022032afae5f7f9dd ✕ Subnet ID : subnet-082c092e2489b998b ✕

□	Name	Subnet ID	State	VPC
□	PUB-ZONEA	subnet-022032afae5f7f9dd	✓ Available	vpc-0c810f756a8737d4c | ZON…
□	PVT-ZONEA	subnet-082c092e2489b998b	✓ Available	vpc-0c810f756a8737d4c | ZON…

3. **Create & Attach Internet Gateway:**
    a. Name: igw-a
    b. Attach to VPC A





VPC > Internet gateways > Attach to VPC (igw-0980052a22545469a)

The following internet gateway was created: igw-0980052a22545469a - IGW-ZONEA. You can now attach to a VPC to enable the VPC to communicate with the internet.

Attach to VPC (igw-0980052a22545469a) Info

VPC

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

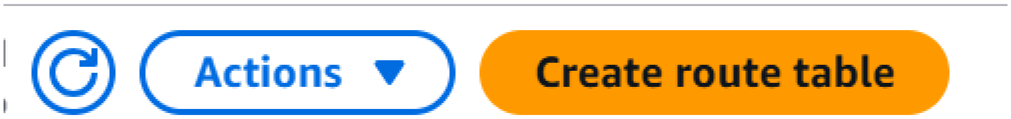
Available VPCs

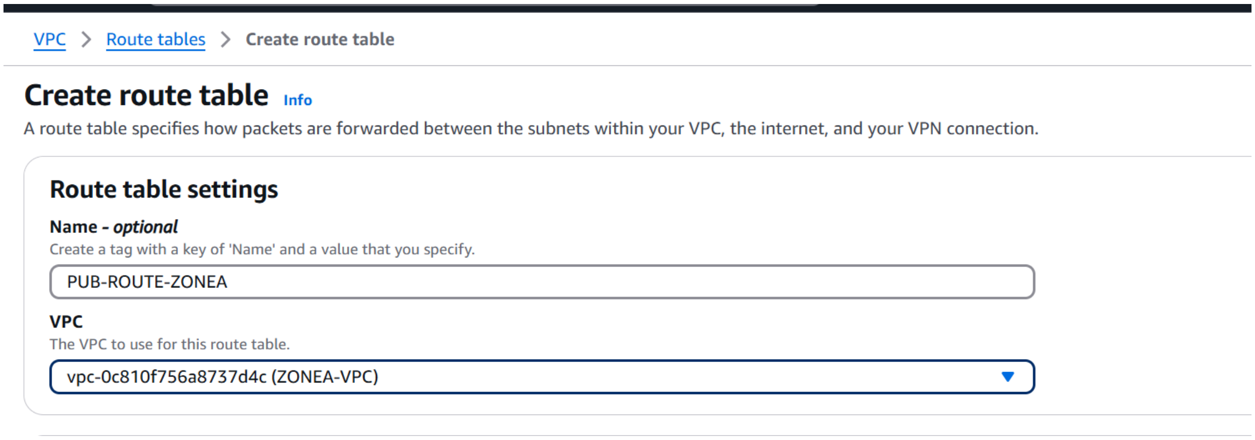
Attach the internet gateway to this VPC.

vpc-0c810f756a8737d4c

vpc-0c810f756a8737d4c - ZONEA-VPC

4. **Create Route Tables:**
   a. **pubrt-a:** Route 0.0.0.0/0 → igw-a
   b. **privrt-a:** No internet route
   c. Associate appropriately with subnets





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*

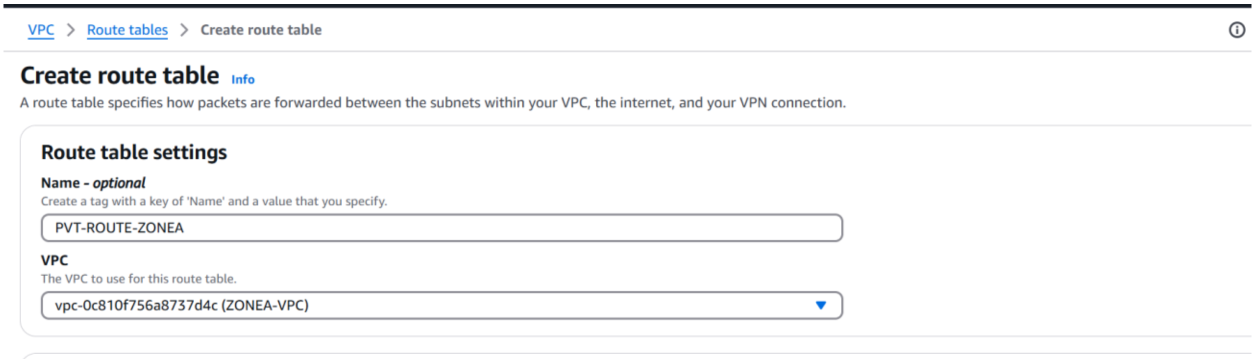
Create a tag with a key of 'Name' and a value that you specify.

PUB-ROUTE-ZONEA

VPC

The VPC to use for this route table.

vpc-0c810f756a8737d4c (ZONEA-VPC)



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.

PVT-ROUTE-ZONEA

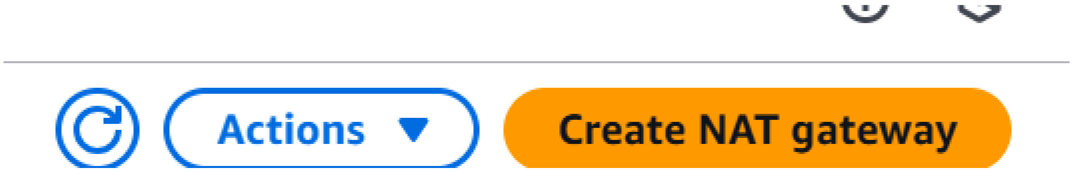
VPC

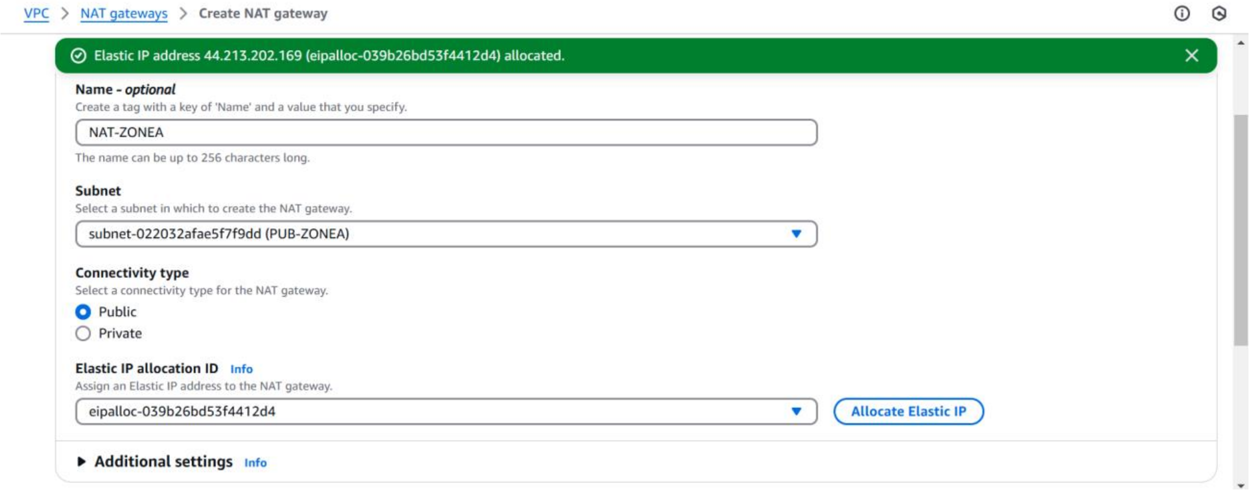
The VPC to use for this route table.

vpc-0c810f756a8737d4c (ZONEA-VPC)

5. **Create NAT Gateway:**
   a. Attach to pubsub-a with Elastic IP

b. Route 0.0.0.0/0 → NAT in privrt-a




VPC > NAT gateways > Create NAT gateway

Elastic IP address 44.213.202.169 (eipalloc-039b26bd53f4412d4) allocated.

Name - *optional*
Create a tag with a key of 'Name' and a value that you specify.
NAT-ZONEA
The name can be up to 256 characters long.

Subnet
Select a subnet in which to create the NAT gateway.
subnet-022032afae5f7f9dd (PUB-ZONEA)

Connectivity type
Select a connectivity type for the NAT gateway.
● Public
○ Private

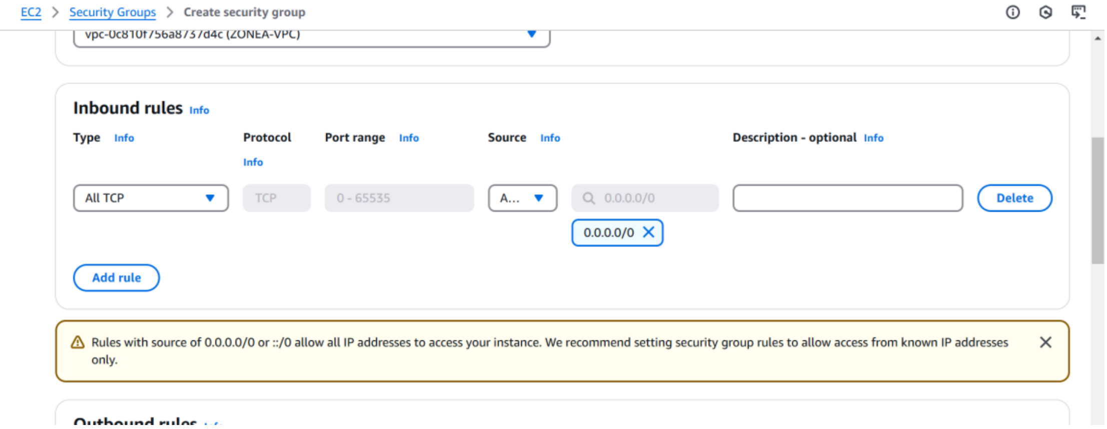
Elastic IP allocation ID Info
Assign an Elastic IP address to the NAT gateway.
eipalloc-039b26bd53f4412d4

▸ **Additional settings** Info

6. Security Groups:

a. **pubsg-a:** Allow all TCP (0.0.0.0/0)

b. **privsg-a:** Allow all TCP from 27.50.10.128/24


EC2 > Security Groups > Create security group

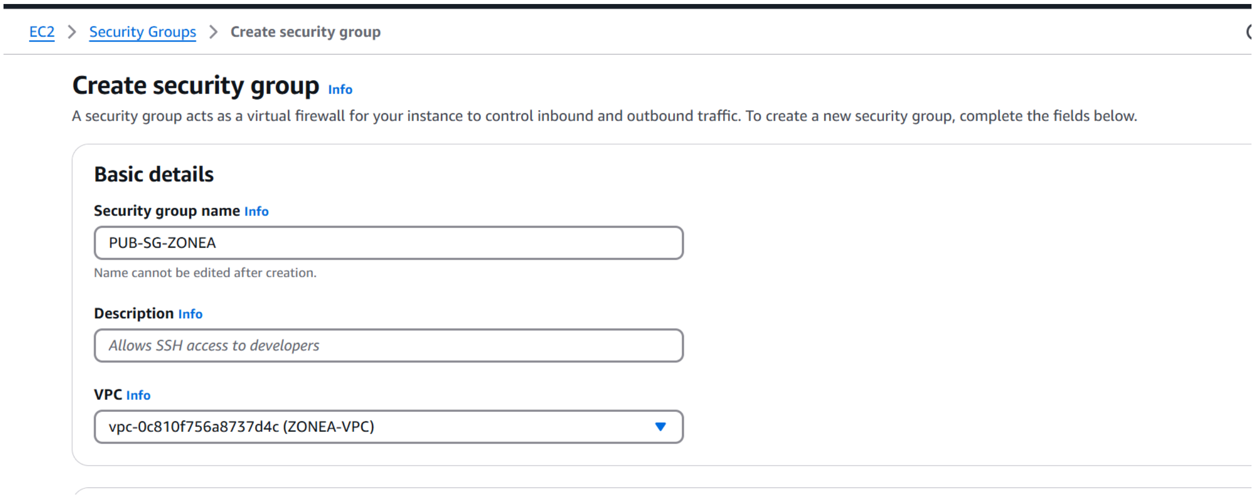
vpc-0c810f756a8737d4c (ZONEA-VPC)

Inbound rules Info

Type	Protocol	Port range	Source		Description - optional
All TCP	TCP	0 - 65535	A...	0.0.0.0/0 0.0.0.0/0	

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

Outbound rules



EC2 > Security Groups > Create security group

Create security group Info

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

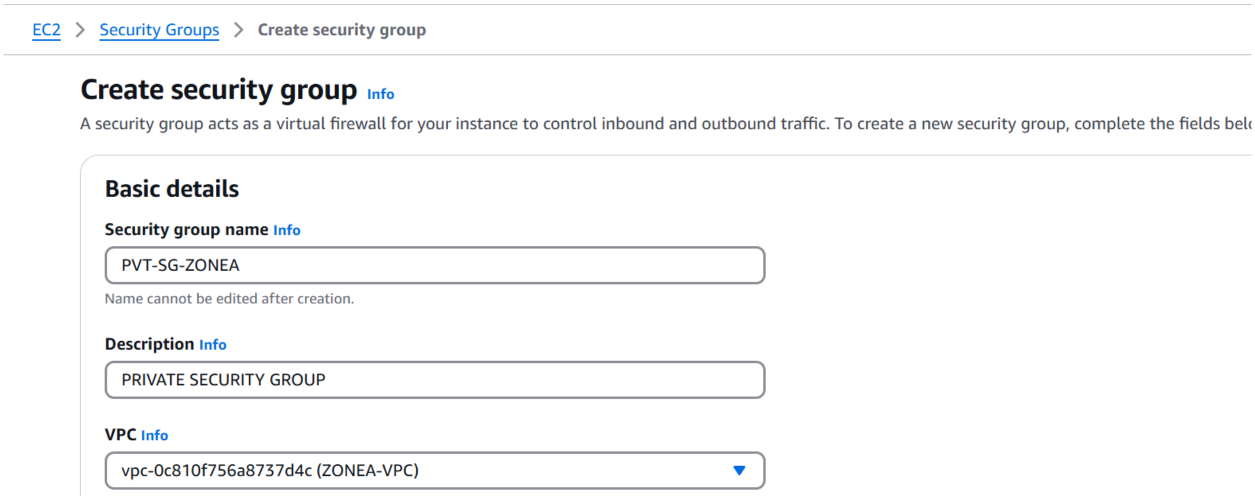
Basic details

Security group name Info: PUB-SG-ZONEA

Name cannot be edited after creation.

Description Info: *Allows SSH access to developers*

VPC Info: vpc-0c810f756a8737d4c (ZONEA-VPC)



EC2 > Security Groups > Create security group

Create security group Info

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields bel

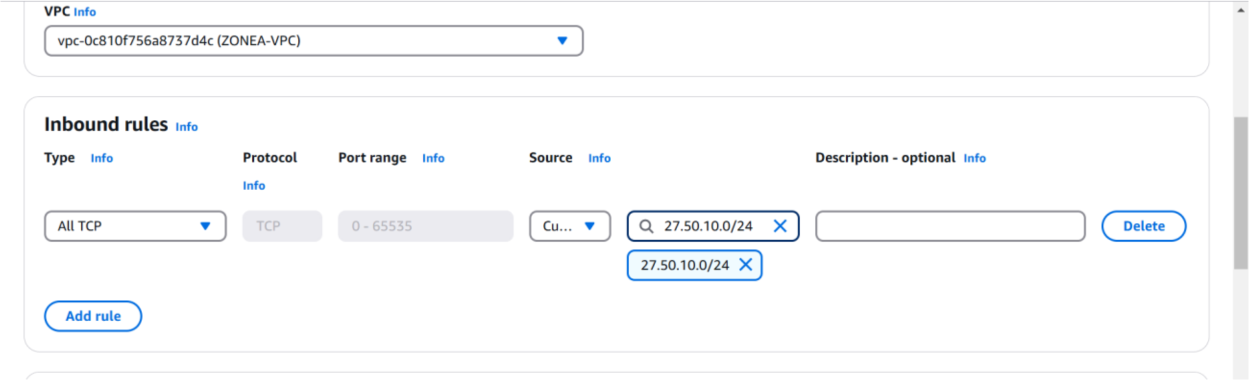
Basic details

Security group name Info: PVT-SG-ZONEA

Name cannot be edited after creation.

Description Info: PRIVATE SECURITY GROUP

VPC Info: vpc-0c810f756a8737d4c (ZONEA-VPC)

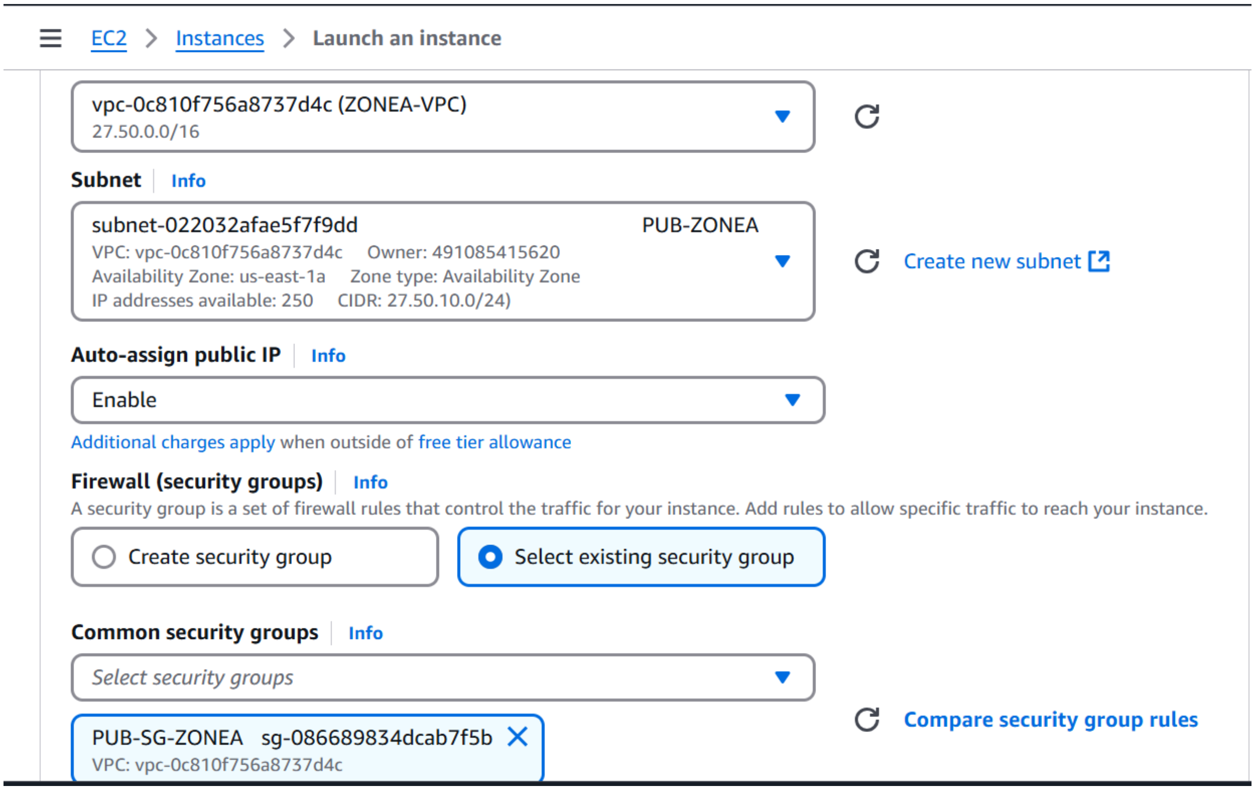


VPC Info: vpc-0c810f756a8737d4c (ZONEA-VPC)

Inbound rules Info

Type Info	Protocol Info	Port range Info	Source Info		Description - optional Info	
All TCP	TCP	0 - 65535	Cu...	27.50.10.0/24 27.50.10.0/24		Delete

7. **Launch EC2 Instances:**
    a. **Public EC2 (pubec2-a):** Debian, attach pubsub-a, enable public IP
    b. **Private EC2 (privec2-a):** Debian, attach privsub-a



EC2 > Instances > Launch an instance

vpc-0c810f756a8737d4c (ZONEA-VPC)
27.50.0.0/16

Subnet | Info

subnet-022032afae5f7f9dd PUB-ZONEA
VPC: vpc-0c810f756a8737d4c Owner: 491085415620
Availability Zone: us-east-1a Zone type: Availability Zone
IP addresses available: 250 CIDR: 27.50.10.0/24)

Create new subnet

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.

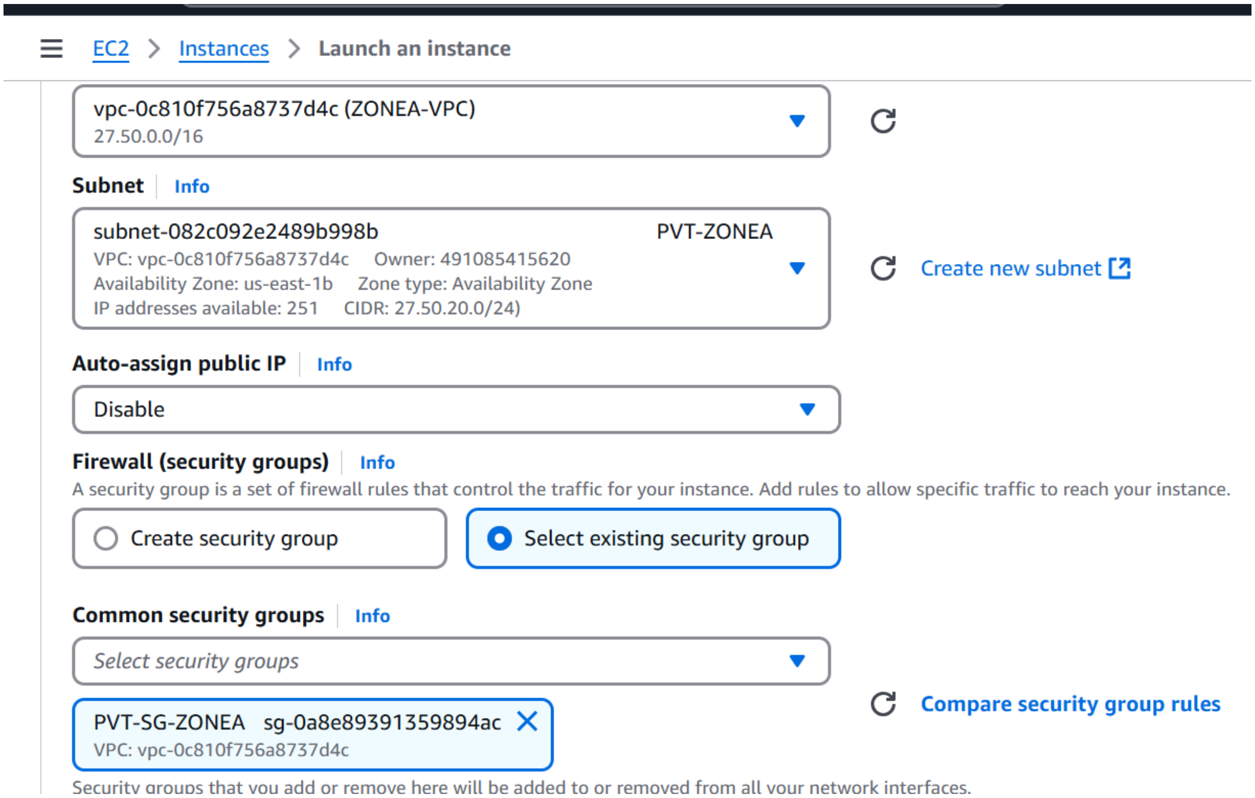
○ Create security group ● Select existing security group

Common security groups | Info

Select security groups

Compare security group rules

PUB-SG-ZONEA sg-086689834dcab7f5b ✕
VPC: vpc-0c810f756a8737d4c



EC2 > Instances > Launch an instance

vpc-0c810f756a8737d4c (ZONEA-VPC)
27.50.0.0/16

Subnet | Info

subnet-082c092e2489b998b PVT-ZONEA
VPC: vpc-0c810f756a8737d4c Owner: 491085415620
Availability Zone: us-east-1b Zone type: Availability Zone
IP addresses available: 251 CIDR: 27.50.20.0/24)

Create new subnet

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

Common security groups | Info

Select security groups

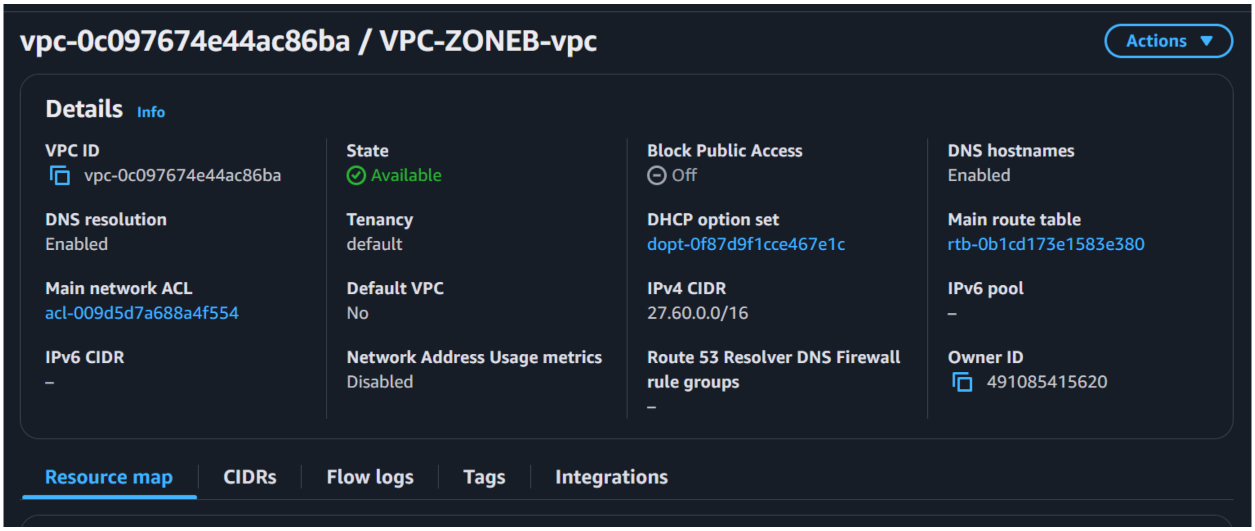
Compare security group rules

PVT-SG-ZONEA sg-0a8e89391359894ac ✕
VPC: vpc-0c810f756a8737d4c

Security groups that you add or remove here will be added to or removed from all your network interfaces.

Step 2: Set Up VPC B

1. **Create VPC B:**
   a. CIDR: 27.60.10.0/16



vpc-0c097674e44ac86ba / VPC-ZONEB-vpc

Details Info

VPC ID
vpc-0c097674e44ac86ba

State
Available

Block Public Access
Off

DNS hostnames
Enabled

DNS resolution
Enabled

Tenancy
default

DHCP option set
dopt-0f87d9f1cce467e1c

Main route table
rtb-0b1cd173e1583e380

Main network ACL
acl-009d5d7a688a4f554

Default VPC
No

IPv4 CIDR
27.60.0.0/16

IPv6 pool
–

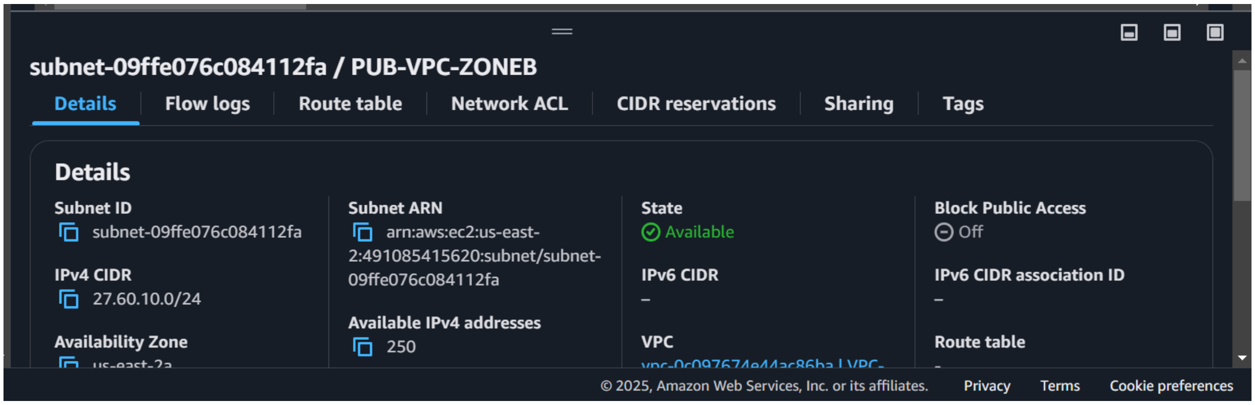
IPv6 CIDR
–

Network Address Usage metrics
Disabled

Route 53 Resolver DNS Firewall rule groups
–

Owner ID
491085415620

2. **Create Subnets:**
   a. Public Subnet (pubsub-b): 27.50.10.0/24
   b. Private Subnet (privsub-b): 27.50.20.0/24



subnet-09ffe076c084112fa / PUB-VPC-ZONEB

Details

Subnet ID
subnet-09ffe076c084112fa

Subnet ARN
arn:aws:ec2:us-east-2:491085415620:subnet/subnet-09ffe076c084112fa

State
Available

Block Public Access
Off

IPv4 CIDR
27.60.10.0/24

IPv6 CIDR
–

IPv6 CIDR association ID
–

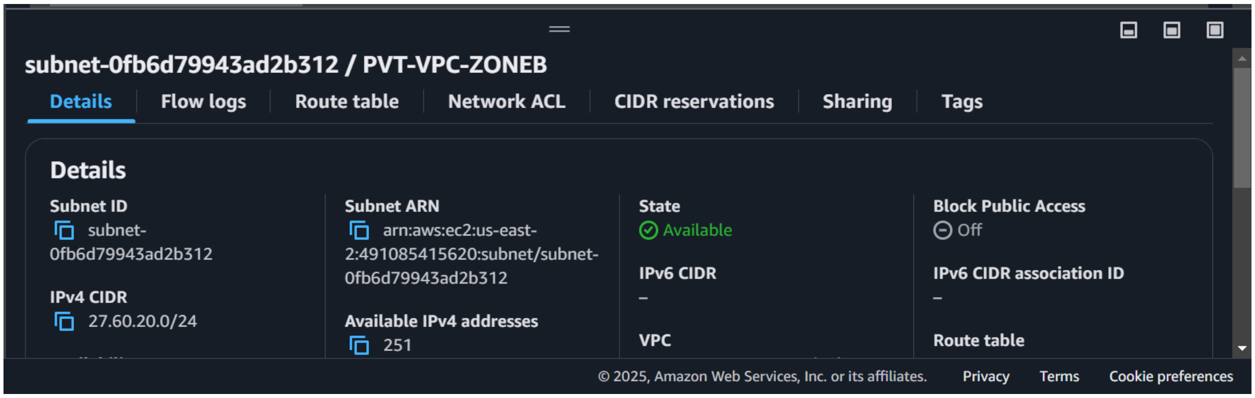
Availability Zone
us-east-2a

Available IPv4 addresses
250

VPC
vpc-0c097674e44ac86ba | VPC-

Route table
-

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



subnet-0fb6d79943ad2b312 / PVT-VPC-ZONEB

Details

Subnet ID
subnet-0fb6d79943ad2b312

IPv4 CIDR
27.60.20.0/24

Subnet ARN
arn:aws:ec2:us-east-2:491085415620:subnet/subnet-0fb6d79943ad2b312

Available IPv4 addresses
251

State
Available

IPv6 CIDR
–

VPC

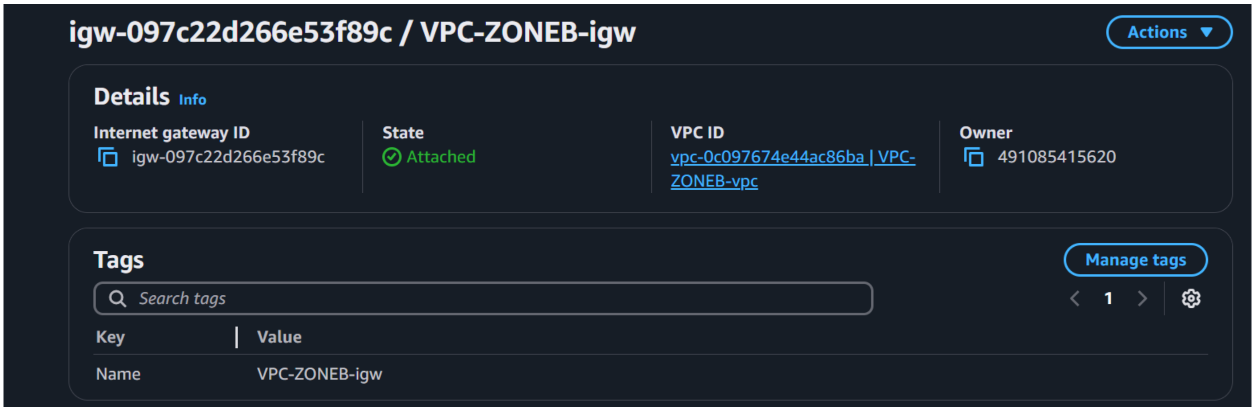
Block Public Access
Off

IPv6 CIDR association ID
–

Route table

© 2025, Amazon Web Services, Inc. or its affiliates.

3. **Internet Gateway:**
   a. Name: igw-b
   b. Attach to VPC B



igw-097c22d266e53f89c / VPC-ZONEB-igw

Details

Internet gateway ID
igw-097c22d266e53f89c

State
Attached

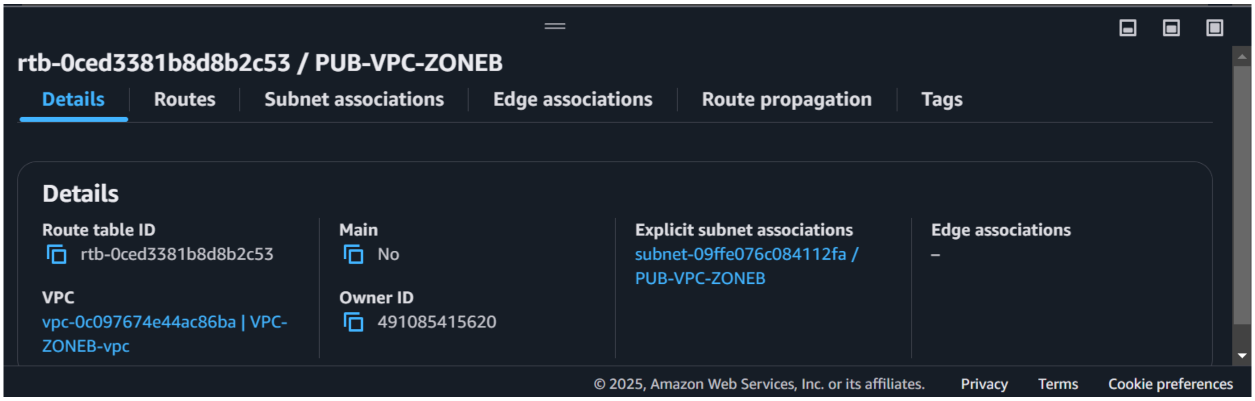
VPC ID
vpc-0c097674e44ac86ba | VPC-ZONEB-vpc

Owner
491085415620

Tags

Key	Value
Name	VPC-ZONEB-igw

4. **Route Tables:**
   a. **pubrt-b:** Route 0.0.0.0/0 → igw-b
   b. **privrt-b:** No internet route



rtb-0ced3381b8d8b2c53 / PUB-VPC-ZONEB

Details

Route table ID
rtb-0ced3381b8d8b2c53

VPC
vpc-0c097674e44ac86ba | VPC-ZONEB-vpc

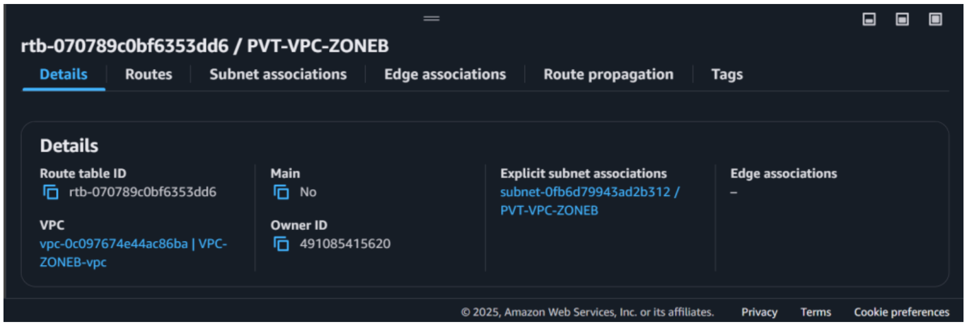
Main
No

Owner ID
491085415620

Explicit subnet associations
subnet-09ffe076c084112fa / PUB-VPC-ZONEB

Edge associations
–

© 2025, Amazon Web Services, Inc. or its affiliates.



rtb-070789c0bf6353dd6 / PVT-VPC-ZONEB

Details

Route table ID
rtb-070789c0bf6353dd6

VPC
vpc-0c097674e44ac86ba | VPC-ZONEB-vpc

Main
No

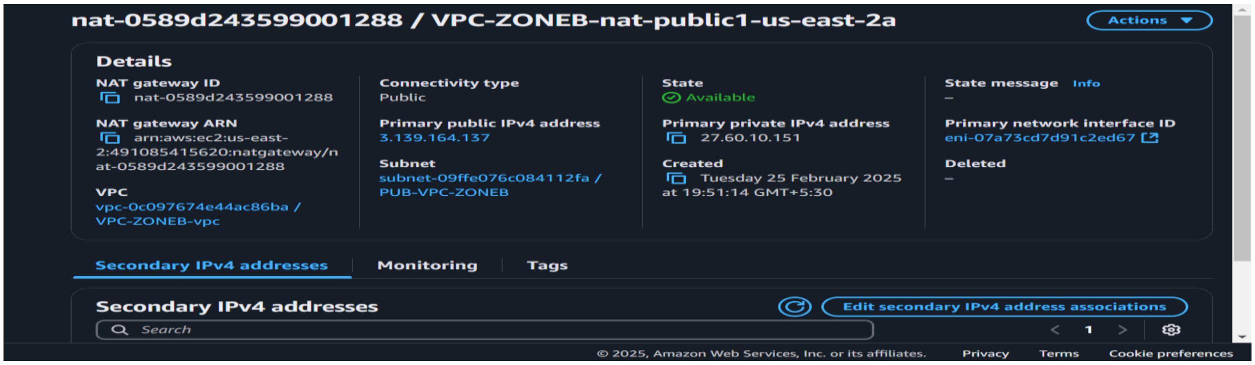
Owner ID
491085415620

Explicit subnet associations
subnet-0fb6d79943ad2b312 / PVT-VPC-ZONEB

Edge associations
–

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

5. **NAT Gateway:**
    a. Attach to pubsub-b with Elastic IP
    b. Route 0.0.0.0/0 → NAT in privrt-b



nat-0589d243599001288 / VPC-ZONEB-nat-public1-us-east-2a

Details

NAT gateway ID
nat-0589d243599001288

NAT gateway ARN
arn:aws:ec2:us-east-2:491085415620:natgateway/nat-0589d243599001288

VPC
vpc-0c097674e44ac86ba / VPC-ZONEB-vpc

Connectivity type
Public

Primary public IPv4 address
3.139.164.137

Subnet
subnet-09ffe076c084112fa / PUB-VPC-ZONEB

State
Available

Primary private IPv4 address
27.60.10.151

Created
Tuesday 25 February 2025 at 19:51:14 GMT+5:30

State message Info
–

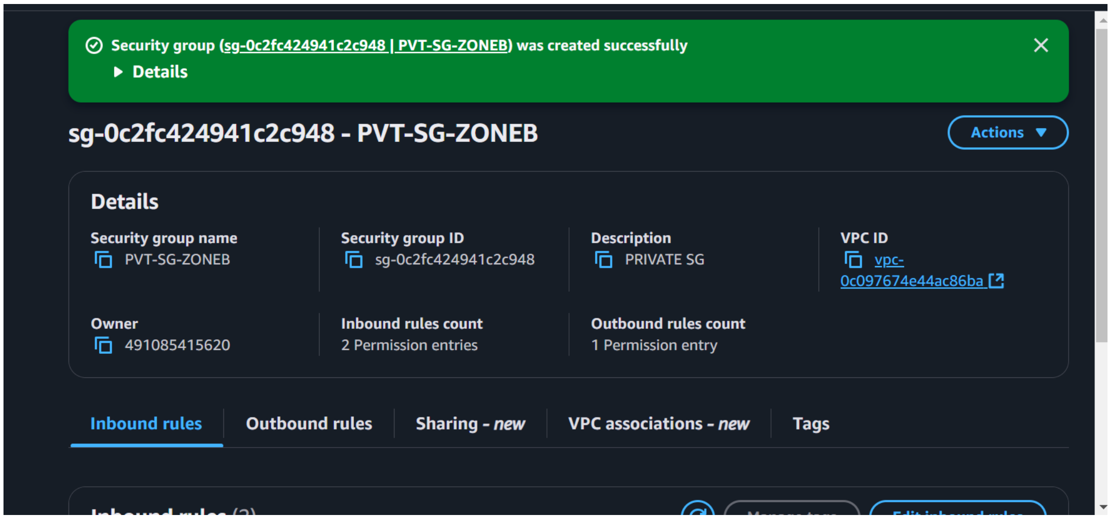
Primary network interface ID
eni-07a73cd7d91c2ed67

Deleted
–

Secondary IPv4 addresses

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

6. **Security Groups:**
    a. **pubsg-b:** Allow all TCP (0.0.0.0/0)
    b. **privsg-b:** Allow ICMP, SSH, HTTP from 27.50.20.128/24



Security group (sg-0c2fc424941c2c948 | PVT-SG-ZONEB) was created successfully
Details

sg-0c2fc424941c2c948 - PVT-SG-ZONEB

Details

Security group name
PVT-SG-ZONEB

Security group ID
sg-0c2fc424941c2c948

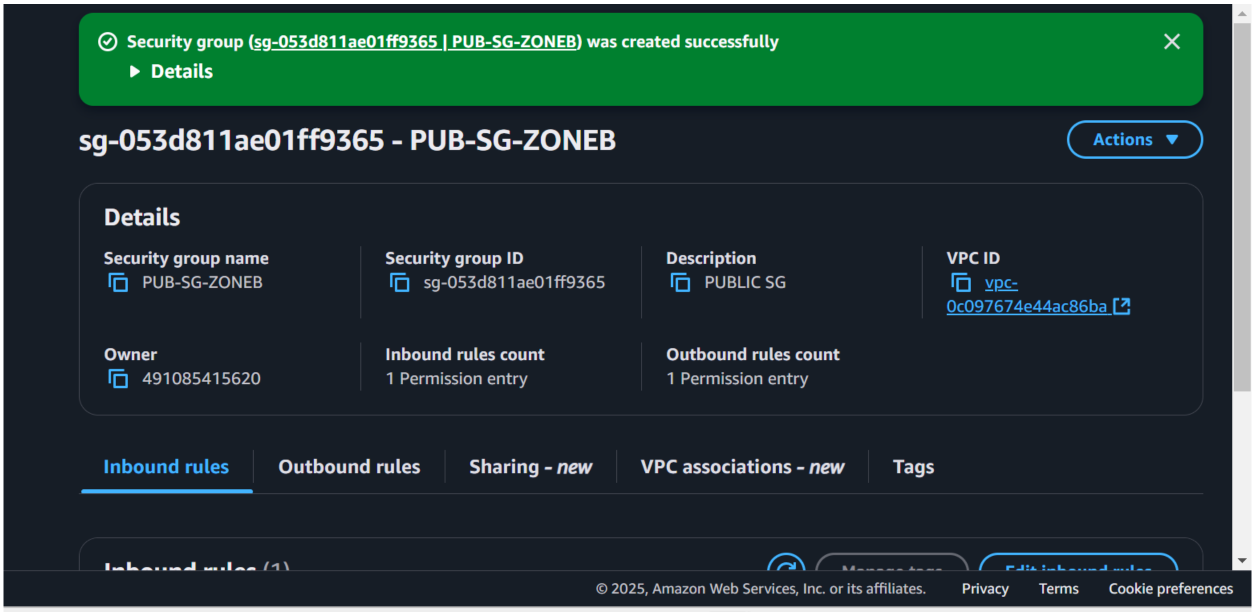
Description
PRIVATE SG

VPC ID
vpc-0c097674e44ac86ba

Owner
491085415620

Inbound rules count
2 Permission entries

Outbound rules count
1 Permission entry


Security group (sg-053d811ae01ff9365 | PUB-SG-ZONEB) was created successfully

▶ Details

sg-053d811ae01ff9365 - PUB-SG-ZONEB

Details

Security group name: PUB-SG-ZONEB

Security group ID: sg-053d811ae01ff9365

Description: PUBLIC SG

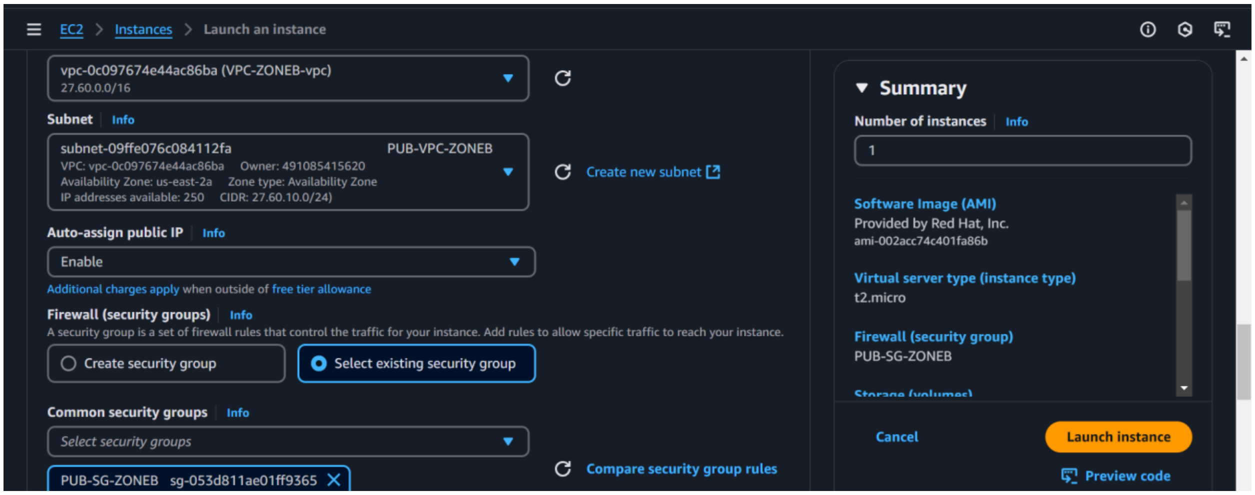
VPC ID: vpc-0c097674e44ac86ba

Owner: 491085415620

Inbound rules count: 1 Permission entry

Outbound rules count: 1 Permission entry

7. **Launch EC2 Instances:**
   a. **Public EC2 (pubec2-b):** Debian, attach pubsub-b
   b. **Private EC2 (privec2-b):** Debian, attach privsub-b


EC2 > Instances > Launch an instance

VPC: vpc-0c097674e44ac86ba (VPC-ZONEB-vpc) 27.60.0.0/16

Subnet: subnet-09ffe076c084112fa PUB-VPC-ZONEB
VPC: vpc-0c097674e44ac86ba Owner: 491085415620
Availability Zone: us-east-2a Zone type: Availability Zone
IP addresses available: 250 CIDR: 27.60.10.0/24)

Auto-assign public IP: Enable

Additional charges apply when outside of free tier allowance

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

Common security groups: Select security groups

PUB-SG-ZONEB sg-053d811ae01ff9365 ✕

Summary

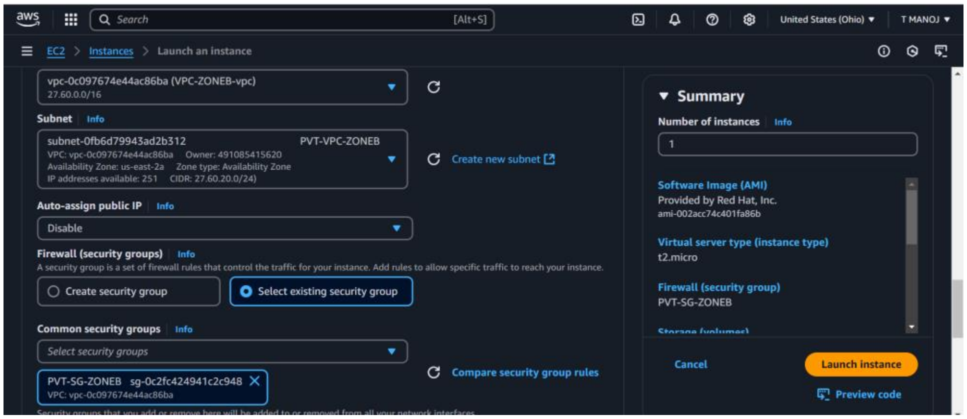
Number of instances: 1

Software Image (AMI): Provided by Red Hat, Inc. ami-002acc74c401fa86b

Virtual server type (instance type): t2.micro

Firewall (security group): PUB-SG-ZONEB

Storage (volumes)



vpc-0c097674e44ac86ba (VPC-ZONEB-vpc)
27.60.0.0/16

Subnet Info

subnet-0fb6d79943ad2b312 PVT-VPC-ZONEB
VPC: vpc-0c097674e44ac86ba Owner: 491085415620
Availability Zone: us-east-2a Zone type: Availability Zone
IP addresses available: 251 CIDR: 27.60.20.0/24)

Create new subnet

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

Common security groups Info

Select security groups

PVT-SG-ZONEB sg-0c2fc424941c2c948
VPC: vpc-0c097674e44ac86ba

Compare security group rules

Security groups that you add or remove here will be added to or removed from all your network interfaces.

▼ Summary

Number of instances Info

1

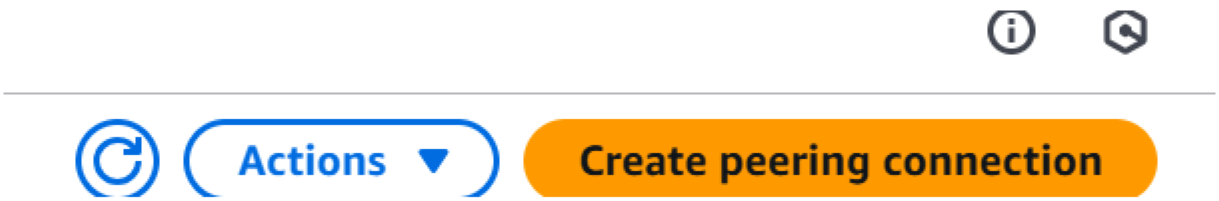
Software Image (AMI)
Provided by Red Hat, Inc.
ami-002acc74c401fa86b

Virtual server type (instance type)
t2.micro

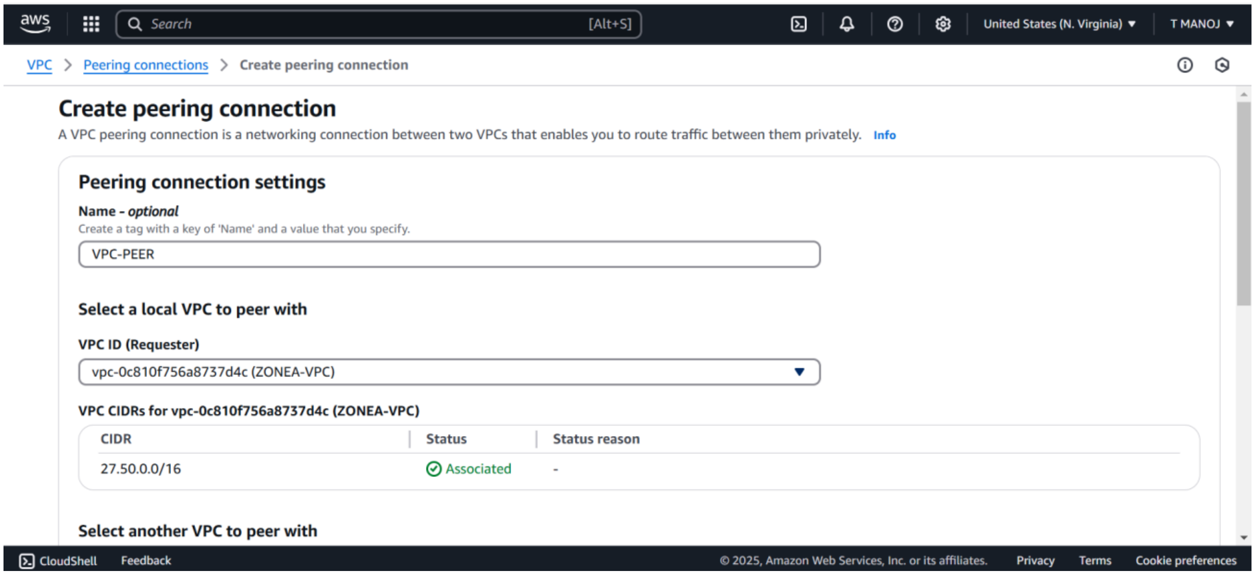
Firewall (security group)
PVT-SG-ZONEB

Storage (volumes)

Step 3: VPC Peering Setup



1. **Create Peering Connection:**
    a. **Requester:** VPC A
    b. **Accepter:** VPC B
    c. Accept peering in VPC B console



aws
Search [Alt+S]
United States (N. Virginia) ▾
T MANOJ ▾
VPC > Peering connections > Create peering connection

Create peering connection

A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them privately. Info

Peering connection settings

Name - *optional*

Create a tag with a key of 'Name' and a value that you specify.

VPC-PEER

Select a local VPC to peer with

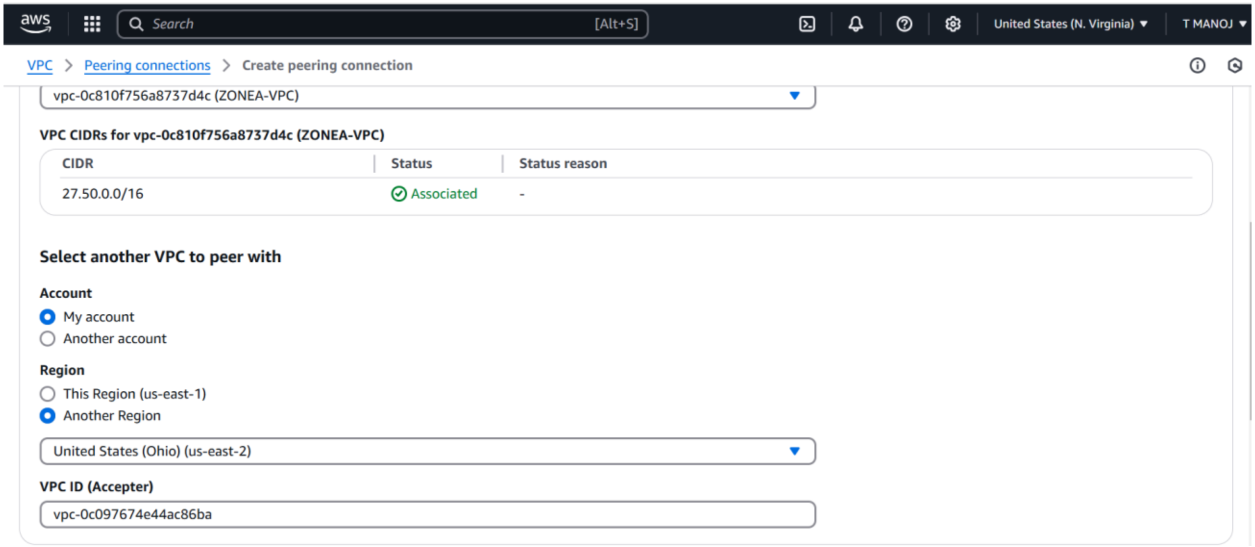
VPC ID (Requester)

vpc-0c810f756a8737d4c (ZONEA-VPC)

VPC CIDRs for vpc-0c810f756a8737d4c (ZONEA-VPC)

CIDR	Status	Status reason
27.50.0.0/16	✓ Associated	-

Select another VPC to peer with


aws
Search
[Alt+S]
United States (N. Virginia) ▾
T MANOJ ▾
VPC > Peering connections > Create peering connection

vpc-0c810f756a8737d4c (ZONEA-VPC) ▾

VPC CIDRs for vpc-0c810f756a8737d4c (ZONEA-VPC)

CIDR	Status	Status reason
27.50.0.0/16	✓ Associated	-

Select another VPC to peer with

Account

● My account
○ Another account

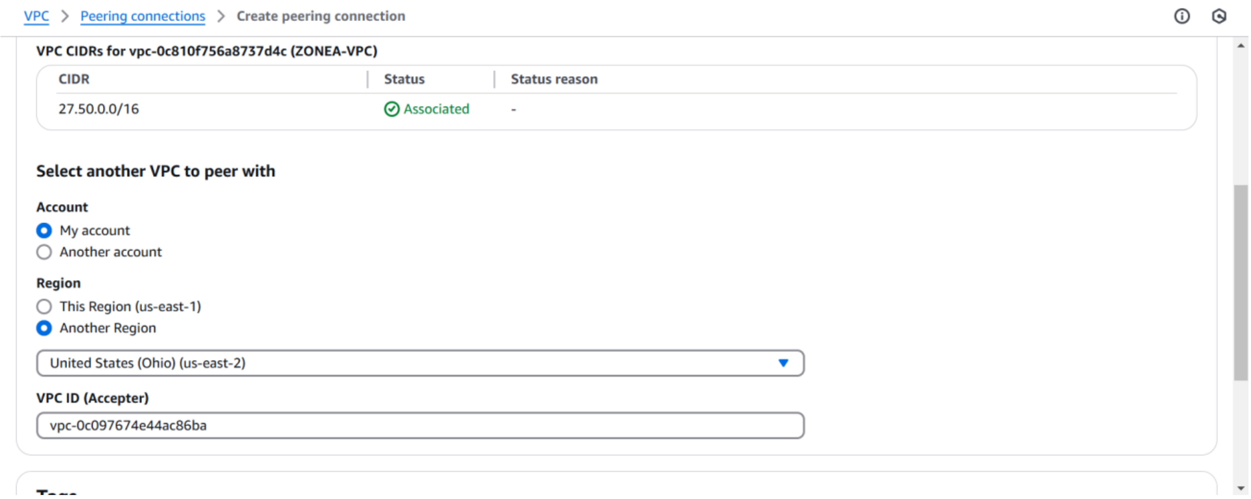
Region

○ This Region (us-east-1)
● Another Region

United States (Ohio) (us-east-2) ▾

VPC ID (Accepter)

vpc-0c097674e44ac86ba



VPC CIDRs for vpc-0c810f756a8737d4c (ZONEA-VPC)

CIDR	Status	Status reason
27.50.0.0/16	✓ Associated	-

Select another VPC to peer with

Account

● My account
○ Another account

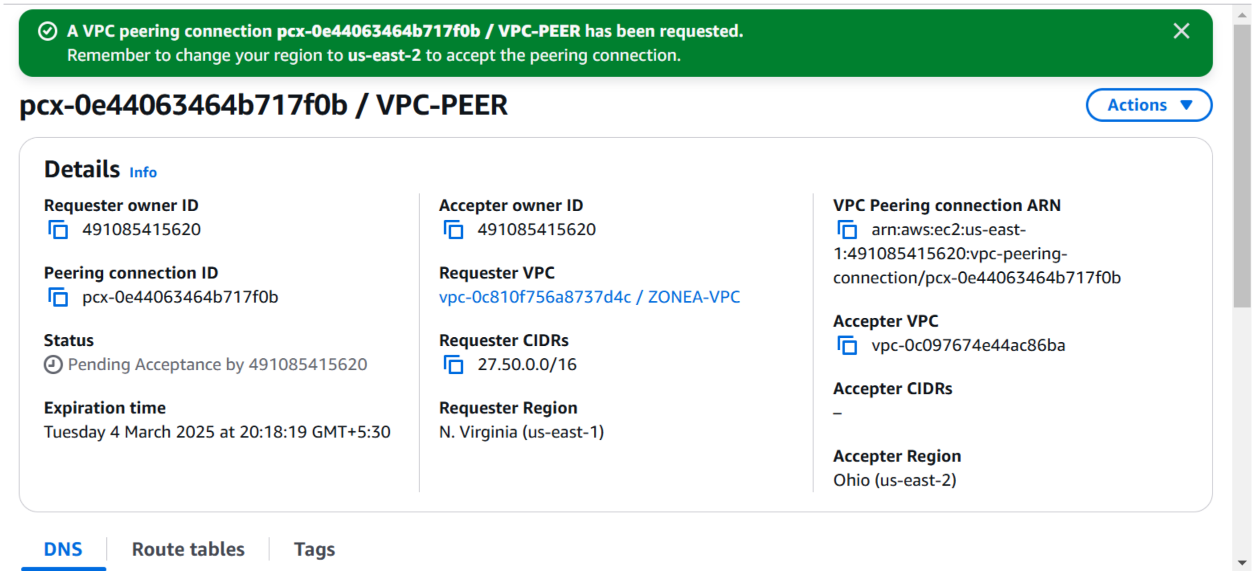
Region

○ This Region (us-east-1)
● Another Region

United States (Ohio) (us-east-2) ▾

VPC ID (Accepter)

vpc-0c097674e44ac86ba



A VPC peering connection **pcx-0e44063464b717f0b / VPC-PEER** has been requested.
Remember to change your region to **us-east-2** to accept the peering connection.

pcx-0e44063464b717f0b / VPC-PEER

Details

Requester owner ID
491085415620

Peering connection ID
pcx-0e44063464b717f0b

Status
Pending Acceptance by 491085415620

Expiration time
Tuesday 4 March 2025 at 20:18:19 GMT+5:30

Accepter owner ID
491085415620

Requester VPC
vpc-0c810f756a8737d4c / ZONEA-VPC

Requester CIDRs
27.50.0.0/16

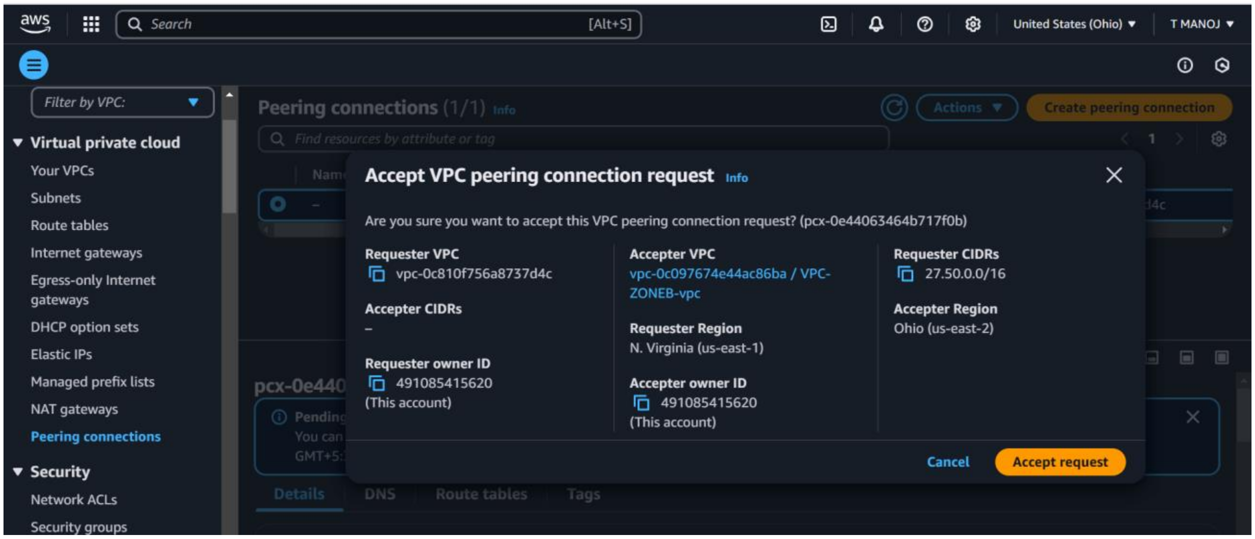
Requester Region
N. Virginia (us-east-1)

VPC Peering connection ARN
arn:aws:ec2:us-east-1:491085415620:vpc-peering-connection/pcx-0e44063464b717f0b

Accepter VPC
vpc-0c097674e44ac86ba

Accepter CIDRs
–

Accepter Region
Ohio (us-east-2)



Accept VPC peering connection request

Are you sure you want to accept this VPC peering connection request? (pcx-0e44063464b717f0b)

Requester VPC
vpc-0c810f756a8737d4c

Accepter CIDRs
–

Requester owner ID
491085415620
(This account)

Accepter VPC
vpc-0c097674e44ac86ba / VPC-ZONEB-vpc

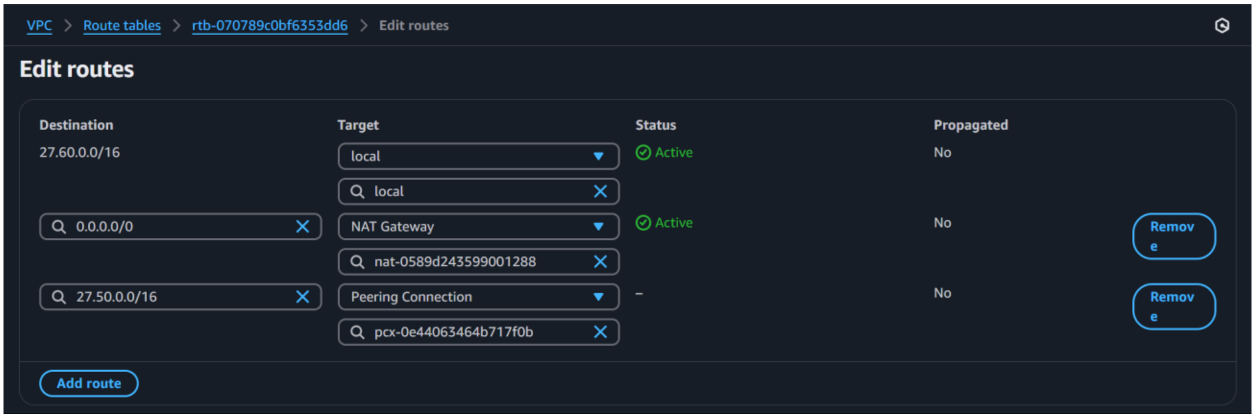
Requester Region
N. Virginia (us-east-1)

Accepter owner ID
491085415620
(This account)

Requester CIDRs
27.50.0.0/16

Accepter Region
Ohio (us-east-2)

2. **Update Route Tables:**
   a. **VPC A (privrt-a):** Add 27.60.10.0/16 → Peering Connection
   b. **VPC B (privrt-b):** Add 27.50.0.0/16 → Peering Connection

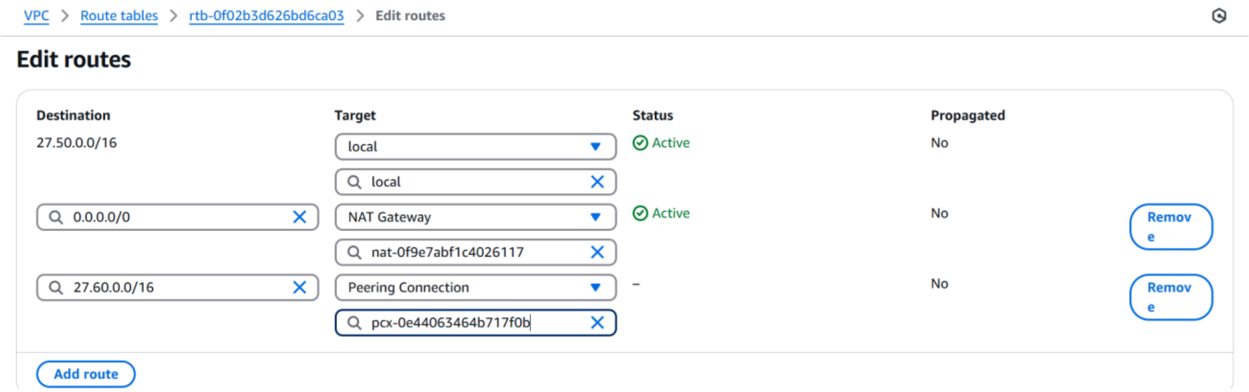


VPC > Route tables > rtb-070789c0bf6353dd6 > Edit routes

Edit routes

Destination	Target	Status	Propagated	
27.60.0.0/16	local local	✓ Active	No	
0.0.0.0/0	NAT Gateway nat-0589d243599001288	✓ Active	No	Remove
27.50.0.0/16	Peering Connection pcx-0e44063464b717f0b	–	No	Remove

Add route



VPC > Route tables > rtb-0f02b3d626bd6ca03 > Edit routes

Edit routes

Destination	Target	Status	Propagated	
27.50.0.0/16	local local	✓ Active	No	
0.0.0.0/0	NAT Gateway nat-0f9e7abf1c4026117	✓ Active	No	Remove
27.60.0.0/16	Peering Connection pcx-0e44063464b717f0b	–	No	Remove

Add route

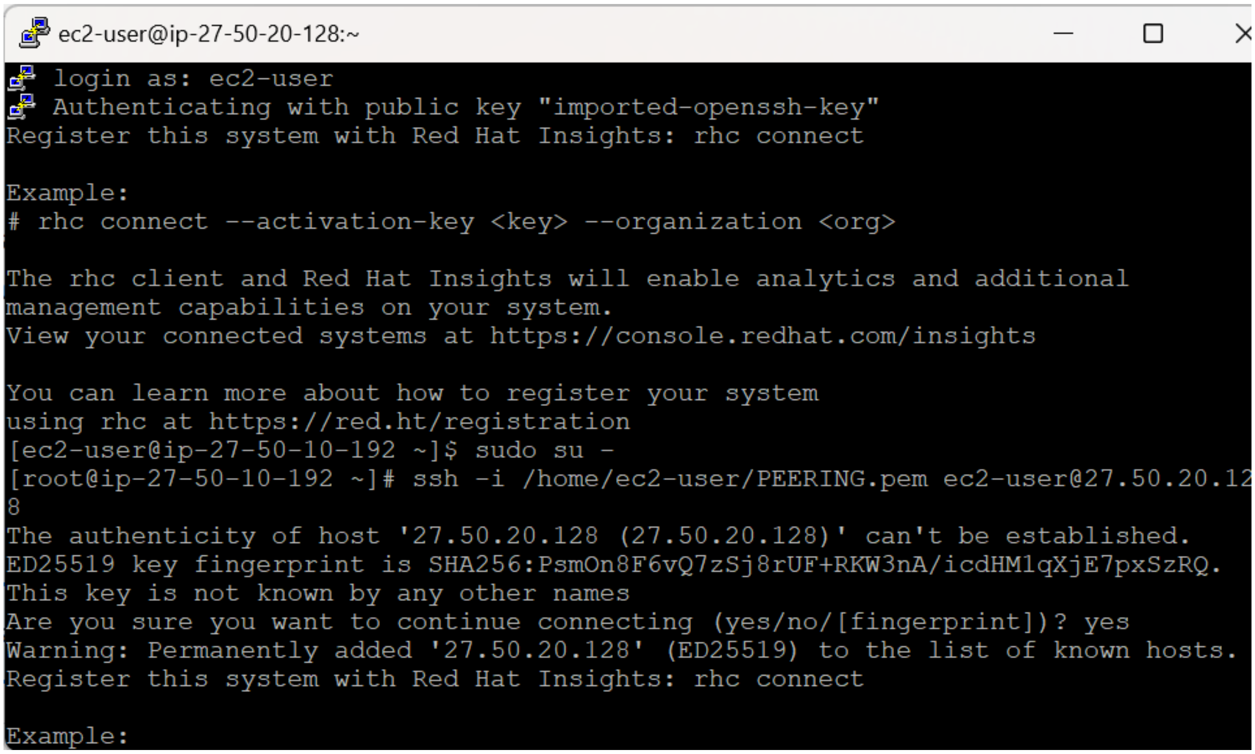
Step 4: Application Hosting

1. HOME Page (pubec2-a)

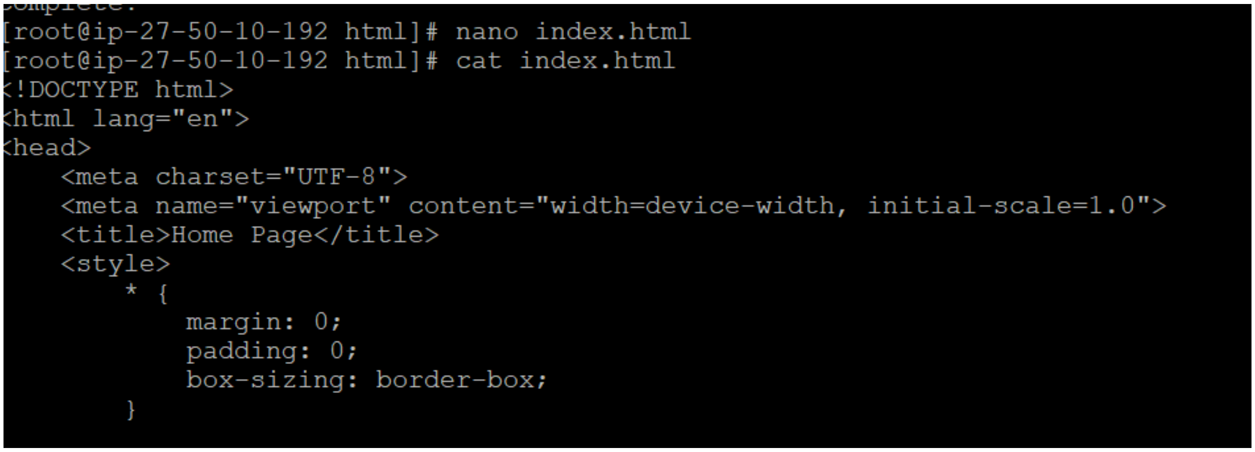
- Install Apache:

```
sudo apt update && sudo apt install -y apache2
sudo systemctl enable apache2
sudo systemctl start apache2
```

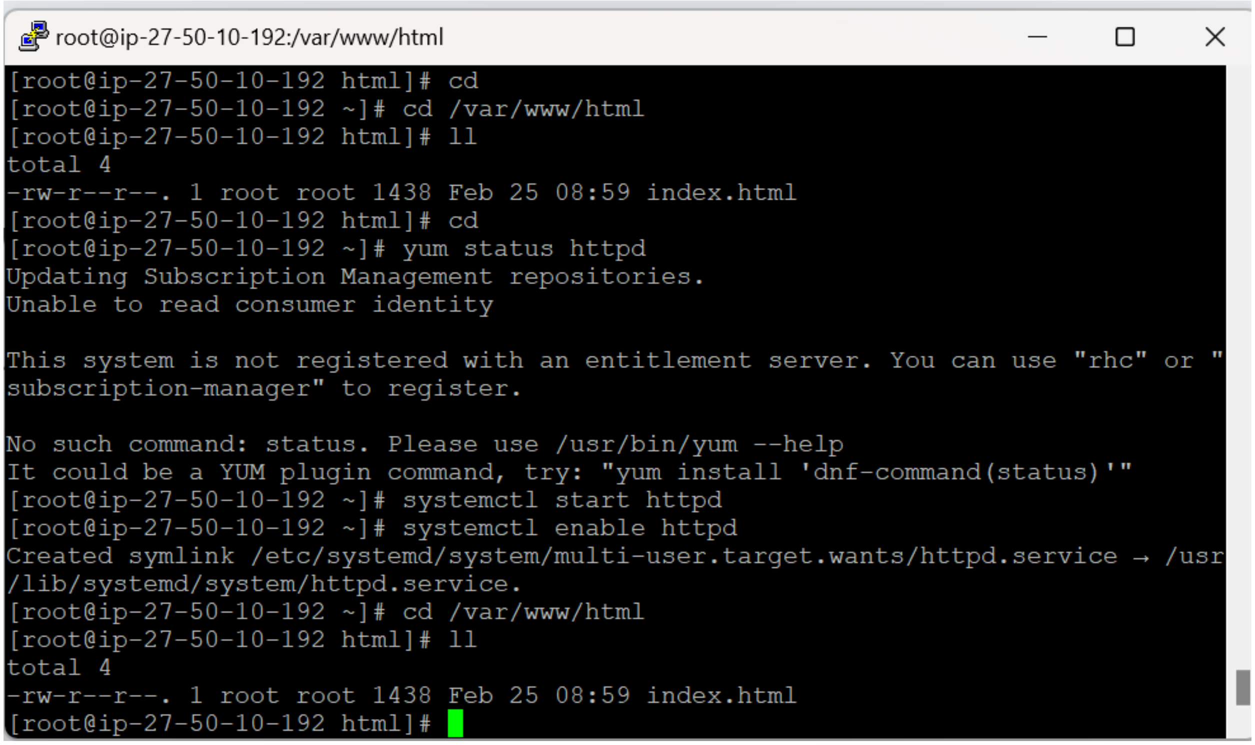
- Place `index.html` (Landing Page) in `/var/www/html/`.



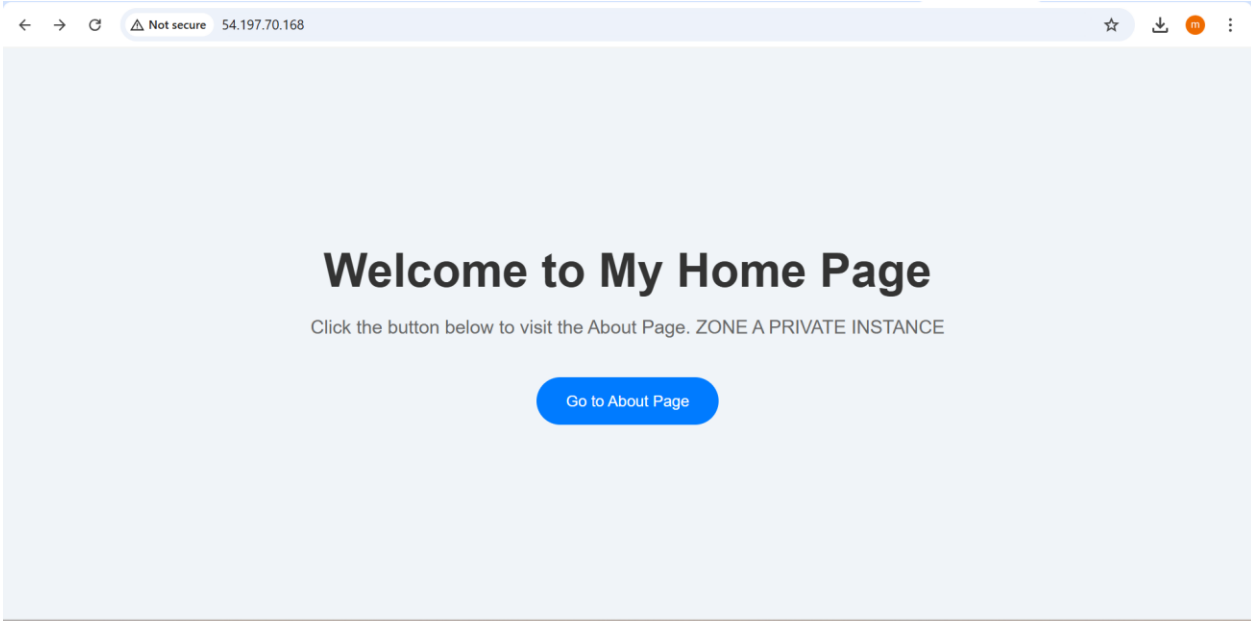
```
ec2-user@ip-27-50-20-128:~
login as: ec2-user
Authenticating with public key "imported-openssh-key"
Register this system with Red Hat Insights: rhc connect

Example:
# rhc connect --activation-key <key> --organization <org>

The rhc client and Red Hat Insights will enable analytics and additional
management capabilities on your system.
View your connected systems at https://console.redhat.com/insights

You can learn more about how to register your system
using rhc at https://red.ht/registration
[ec2-user@ip-27-50-10-192 ~]$ sudo su -
[root@ip-27-50-10-192 ~]# ssh -i /home/ec2-user/PEERING.pem ec2-user@27.50.20.12
8
The authenticity of host '27.50.20.128 (27.50.20.128)' can't be established.
ED25519 key fingerprint is SHA256:PsmOn8F6vQ7zSj8rUF+RKW3nA/icdHM1qXjE7pxSzRQ.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '27.50.20.128' (ED25519) to the list of known hosts.
Register this system with Red Hat Insights: rhc connect

Example:
```



```
Complete!
[root@ip-27-50-10-192 html]# nano index.html
[root@ip-27-50-10-192 html]# cat index.html
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Home Page</title>
    <style>
        * {
            margin: 0;
            padding: 0;
            box-sizing: border-box;
        }
```



```
[root@ip-27-50-10-192 html]# cd
[root@ip-27-50-10-192 ~]# cd /var/www/html
[root@ip-27-50-10-192 html]# ll
total 4
-rw-r--r--. 1 root root 1438 Feb 25 08:59 index.html
[root@ip-27-50-10-192 html]# cd
[root@ip-27-50-10-192 ~]# yum status httpd
Updating Subscription Management repositories.
Unable to read consumer identity

This system is not registered with an entitlement server. You can use "rhc" or "
subscription-manager" to register.

No such command: status. Please use /usr/bin/yum --help
It could be a YUM plugin command, try: "yum install 'dnf-command(status)'"
[root@ip-27-50-10-192 ~]# systemctl start httpd
[root@ip-27-50-10-192 ~]# systemctl enable httpd
Created symlink /etc/systemd/system/multi-user.target.wants/httpd.service → /usr
/lib/systemd/system/httpd.service.
[root@ip-27-50-10-192 ~]# cd /var/www/html
[root@ip-27-50-10-192 html]# ll
total 4
-rw-r--r--. 1 root root 1438 Feb 25 08:59 index.html
[root@ip-27-50-10-192 html]#
```



Welcome to My Home Page

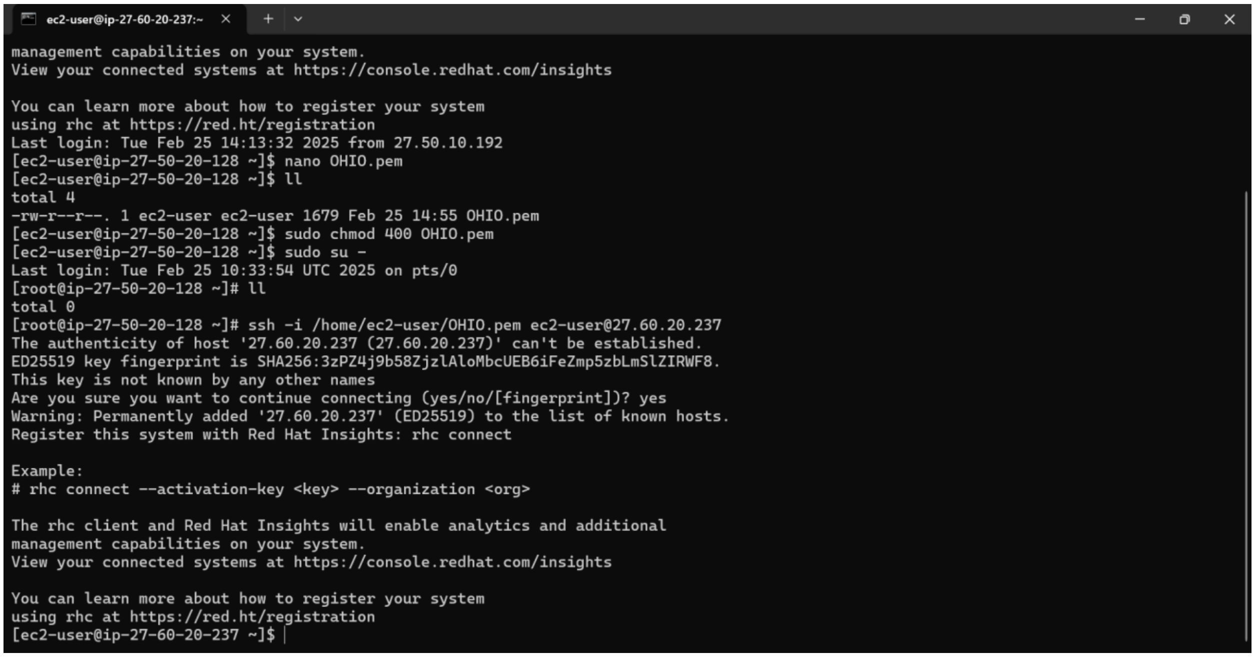
Click the button below to visit the About Page. ZONE A PRIVATE INSTANCE

2. Login Page (privec2-a)

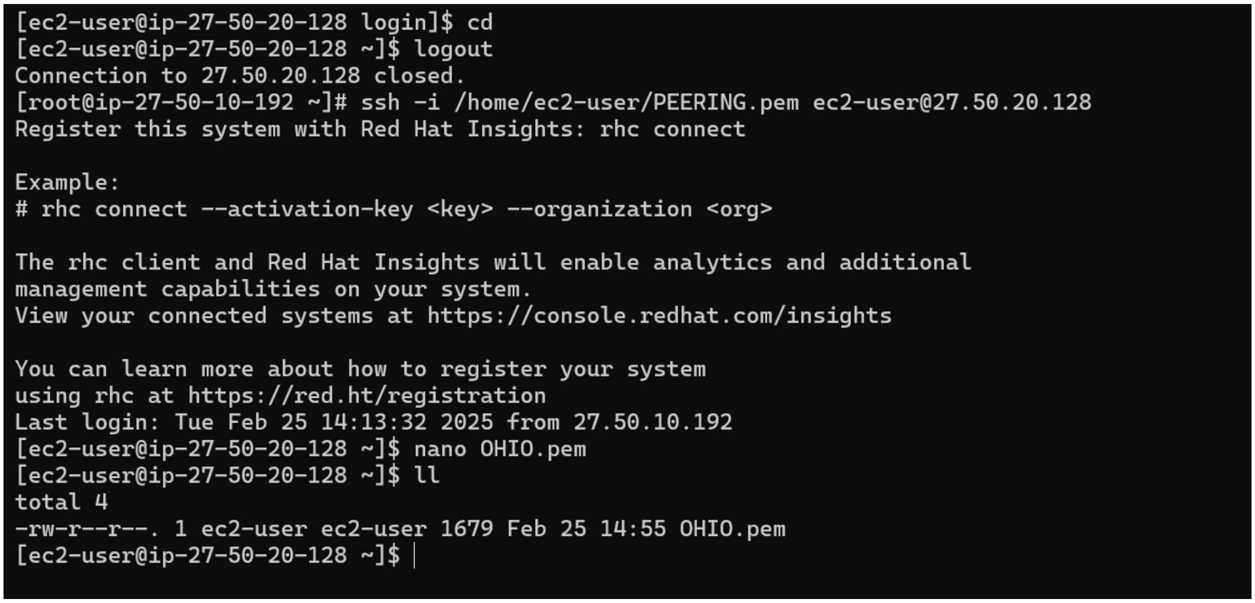
- SSH via pubec2-a:

```
ssh -i my-key.pem admin@<Private-IP>
```

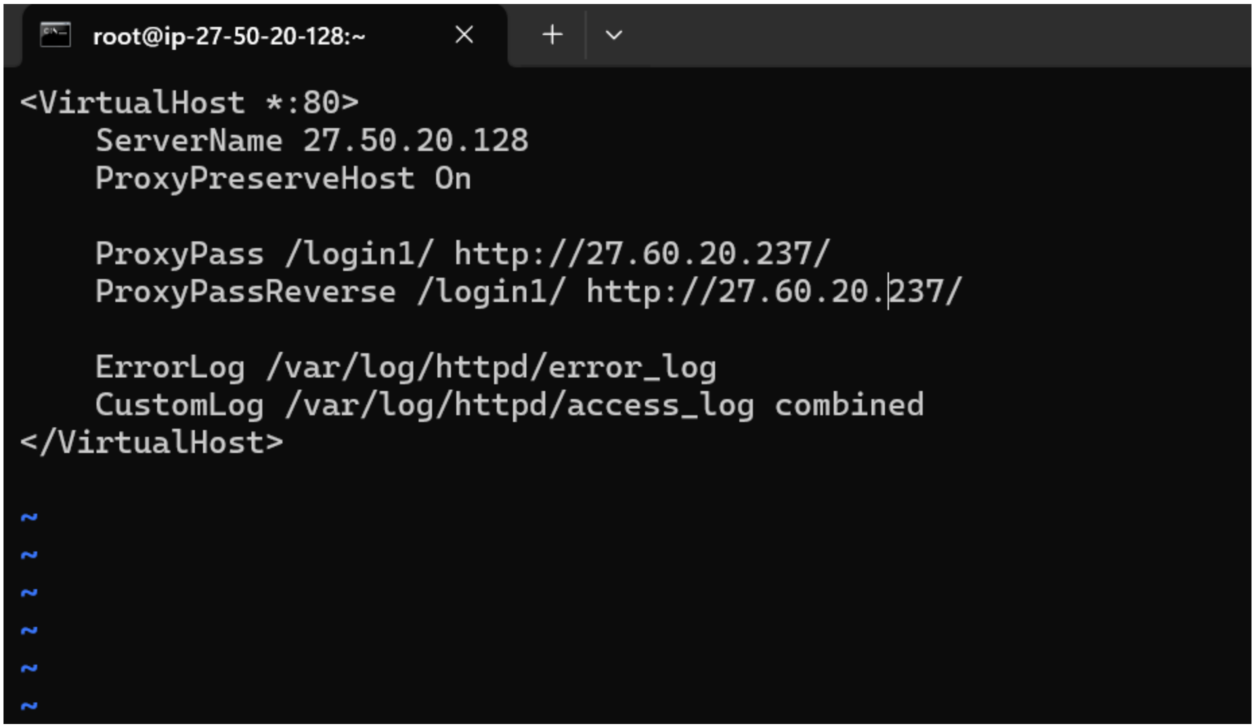
- Install Apache and add `index.html` (Login Page).



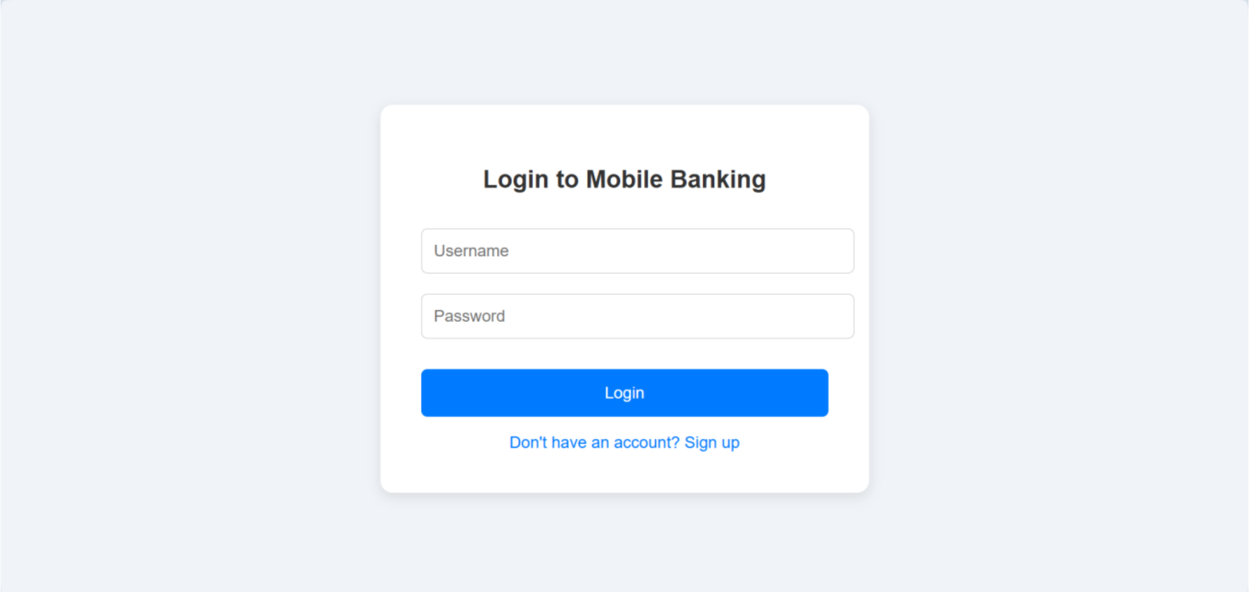
```
management capabilities on your system.
View your connected systems at https://console.redhat.com/insights

You can learn more about how to register your system
using rhc at https://red.ht/registration
Last login: Tue Feb 25 14:13:32 2025 from 27.50.10.192
[ec2-user@ip-27-50-20-128 ~]$ nano OHIO.pem
[ec2-user@ip-27-50-20-128 ~]$ ll
total 4
-rw-r--r--. 1 ec2-user ec2-user 1679 Feb 25 14:55 OHIO.pem
[ec2-user@ip-27-50-20-128 ~]$ sudo chmod 400 OHIO.pem
[ec2-user@ip-27-50-20-128 ~]$ sudo su -
Last login: Tue Feb 25 10:33:54 UTC 2025 on pts/0
[root@ip-27-50-20-128 ~]# ll
total 0
[root@ip-27-50-20-128 ~]# ssh -i /home/ec2-user/OHIO.pem ec2-user@27.60.20.237
The authenticity of host '27.60.20.237 (27.60.20.237)' can't be established.
ED25519 key fingerprint is SHA256:3zPZ4j9b58ZjzlAloMbcUEB6iFeZmp5zbLmSlZIRWF8.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '27.60.20.237' (ED25519) to the list of known hosts.
Register this system with Red Hat Insights: rhc connect

Example:
# rhc connect --activation-key <key> --organization <org>

The rhc client and Red Hat Insights will enable analytics and additional
management capabilities on your system.
View your connected systems at https://console.redhat.com/insights

You can learn more about how to register your system
using rhc at https://red.ht/registration
[ec2-user@ip-27-60-20-237 ~]$ 
```



```
[ec2-user@ip-27-50-20-128 login]$ cd
[ec2-user@ip-27-50-20-128 ~]$ logout
Connection to 27.50.20.128 closed.
[root@ip-27-50-10-192 ~]# ssh -i /home/ec2-user/PEERING.pem ec2-user@27.50.20.128
Register this system with Red Hat Insights: rhc connect

Example:
# rhc connect --activation-key <key> --organization <org>

The rhc client and Red Hat Insights will enable analytics and additional
management capabilities on your system.
View your connected systems at https://console.redhat.com/insights

You can learn more about how to register your system
using rhc at https://red.ht/registration
Last login: Tue Feb 25 14:13:32 2025 from 27.50.10.192
[ec2-user@ip-27-50-20-128 ~]$ nano OHIO.pem
[ec2-user@ip-27-50-20-128 ~]$ ll
total 4
-rw-r--r--. 1 ec2-user ec2-user 1679 Feb 25 14:55 OHIO.pem
[ec2-user@ip-27-50-20-128 ~]$ 
```



```
<VirtualHost *:80>
    ServerName 27.50.20.128
    ProxyPreserveHost On

    ProxyPass /login1/ http://27.60.20.237/
    ProxyPassReverse /login1/ http://27.60.20.237/

    ErrorLog /var/log/httpd/error_log
    CustomLog /var/log/httpd/access_log combined
</VirtualHost>

~
~
~
~
~
~
```

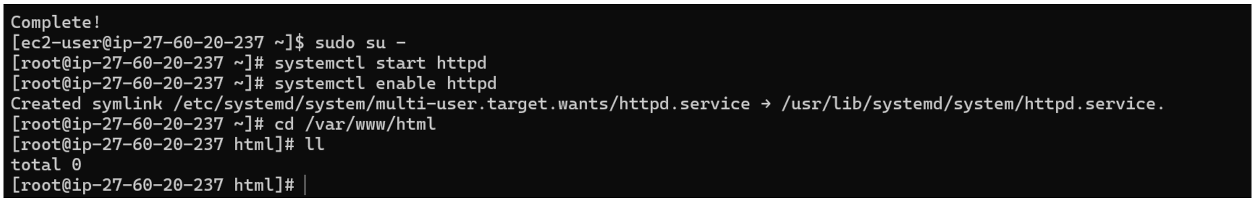


3. MOBILE Banking Page (privec2-b)

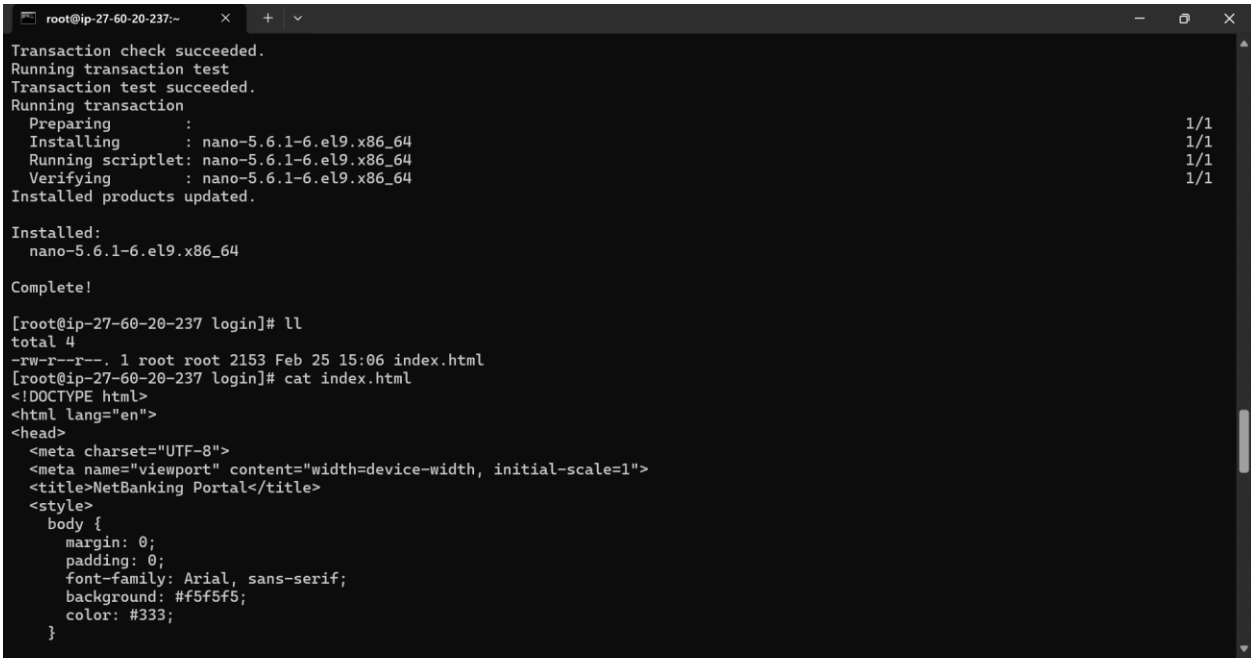
- SSH via privec2-a:

```
ssh -i my-key.pem admin@<Private-IP>
```

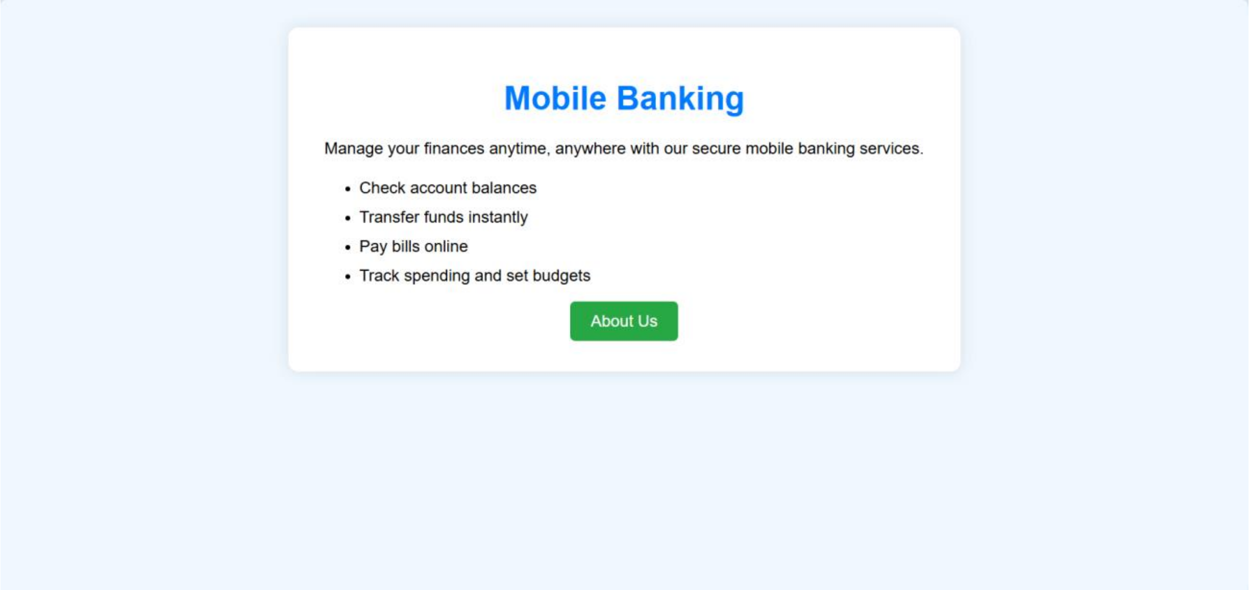
- Install Apache and add `index.html` (Net Banking Page).



```
Complete!
[ec2-user@ip-27-60-20-237 ~]$ sudo su -
[root@ip-27-60-20-237 ~]# systemctl start httpd
[root@ip-27-60-20-237 ~]# systemctl enable httpd
Created symlink /etc/systemd/system/multi-user.target.wants/httpd.service → /usr/lib/systemd/system/httpd.service.
[root@ip-27-60-20-237 ~]# cd /var/www/html
[root@ip-27-60-20-237 html]# ll
total 0
[root@ip-27-60-20-237 html]# 
```



```
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing        :                                                                                                 1/1
  Installing       : nano-5.6.1-6.el9.x86_64                                                                         1/1
  Running scriptlet: nano-5.6.1-6.el9.x86_64                                                                         1/1
  Verifying        : nano-5.6.1-6.el9.x86_64                                                                         1/1
Installed products updated.

Installed:
  nano-5.6.1-6.el9.x86_64

Complete!

[root@ip-27-60-20-237 login]# ll
total 4
-rw-r--r--. 1 root root 2153 Feb 25 15:06 index.html
[root@ip-27-60-20-237 login]# cat index.html
<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <title>NetBanking Portal</title>
  <style>
    body {
      margin: 0;
      padding: 0;
      font-family: Arial, sans-serif;
      background: #f5f5f5;
      color: #333;
    }
```



Mobile Banking

Manage your finances anytime, anywhere with our secure mobile banking services.

- Check account balances
- Transfer funds instantly
- Pay bills online
- Track spending and set budgets

Final Architecture :

```
      Internet
        |
   +------------------+
   |  Public EC2    |          ---> Hosts Landing Page
   | (27.50.10.128)  |
   +------------------+
           |
   +------------------+    VPC Peering    +------------------+
   |  Private EC2 (A) | ------------------> |  Private EC2 (B) |
   | (27.50.20.128)  |               | (27.60.20.0)    |
   +------------------+               +------------------+
     (Login Page)                   (Net Banking Page)
```

Advantages

- **Improved Network Connectivity:** Seamless data transfer and communication between VPC A and VPC B without the need for internet gateways.
- **Cost-Effective:** Reduces the need for VPN or direct connect solutions, minimizing operational costs.
- **Enhanced Security:** Traffic between VPCs remains on the AWS network, providing a secure connection with controlled access via security groups and route tables.
- **Scalability:** The architecture allows for easy expansion, supporting additional applications or services as needed.

Conclusion

This project successfully establishes a secure and efficient network infrastructure by implementing VPC peering and hosting a static web application. The reverse proxy configuration using Apache ensures optimal routing and load management, enhancing application performance. By leveraging AWS best practices for security, scalability, and monitoring, the solution not only meets current application hosting needs but also lays a strong foundation for future expansions.