Cross-Region VPC Peering

This document explains the entire setup of **Cross-Region VPC Peering** between:

- **Region A:** Asia Pacific (Singapore) ap-southeast-1
- **Region B:** Europe (Ireland) eu-west-1

---

1. Project Overview

This project demonstrates how to create two vpc's in different regions/accounts and set up secure communication via peering test with ec2 instances.

---

2. Architecture Summary

Region A: Asia Pacific (Singapore) ap-southeast-1

- VPC-A CIDR: 10.0.0.0/16
- Subnet-A: 10.0.0.0/17
- EC2-A Private IP: 10.0.63.38

Region B: Europe (Ireland) eu-west-1

- VPC-B CIDR: 172.16.0.0/16
- Subnet-B: 172.16.0.0/17
- EC2-B Private IP: 172.16.88.161

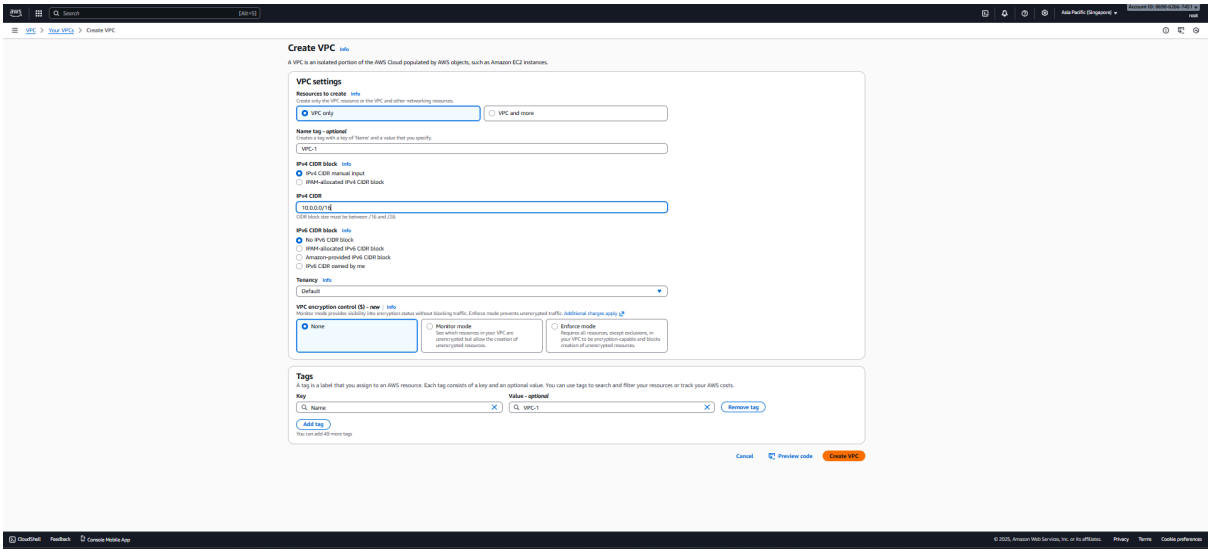
Connection

- VPC Peering initiated from Singapore → accepted in Ireland
- Route tables updated on both sides
- Security groups configured to allow ICMP/SSH

3. Step-by-Step Implementation

Step 1: Create VPC in Singapore (Region A)

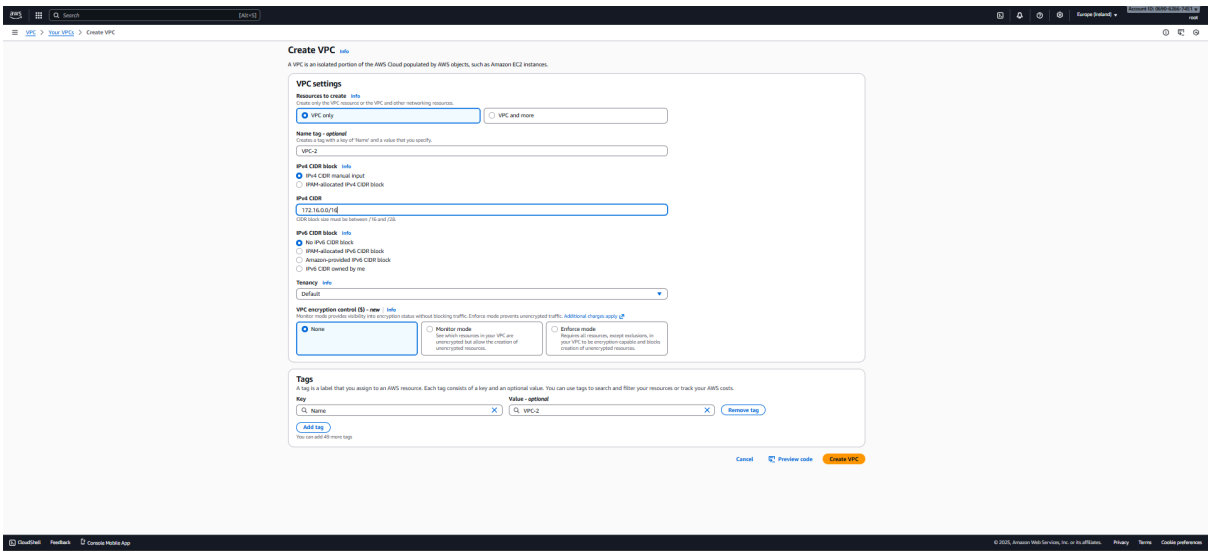
1. Go to **AWS Console →VPC Dashboard > Your VPCs > Create VPC**
2. Enter:
    - Name: VPC-1
    - CIDR: 10.0.0.0/16
3. Click **Create VPC**.



Snapshot: Singapore VPC creation

Step 2: Create VPC in Ireland (Region B)

1. Switch region to **Europe (Ireland)**
2. Create a new VPC:
    - Name: VPC-2
    - CIDR: 172.16.0.0/16
3. Click **Create VPC**.



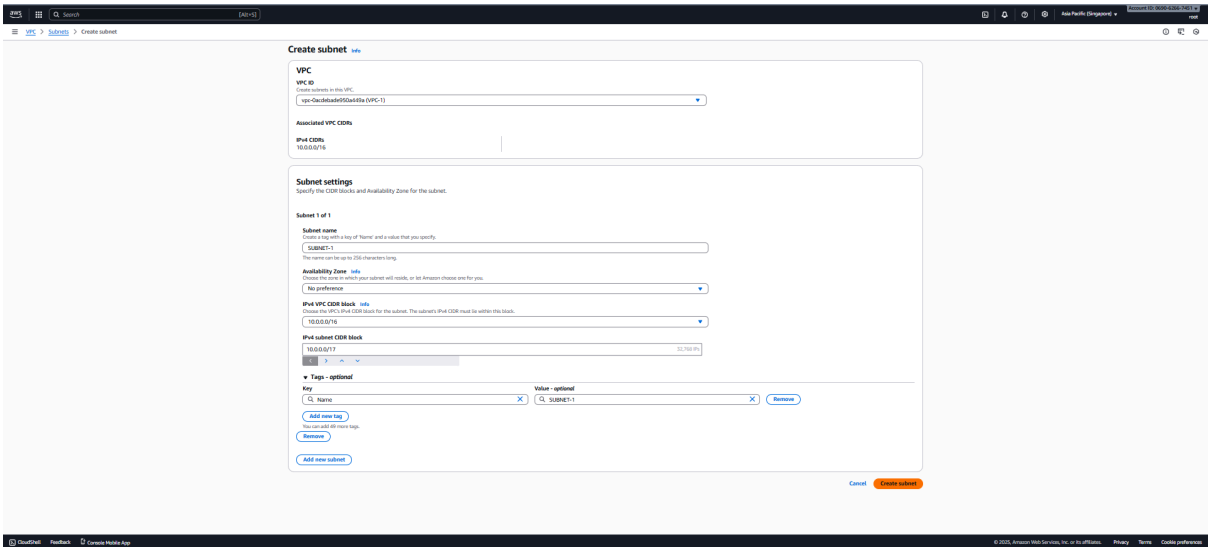
Snapshot: Ireland VPC creation

Step 3: Create Subnets

Singapore Subnet-1

AWS Console → VPC → Subnets → Create Subnet

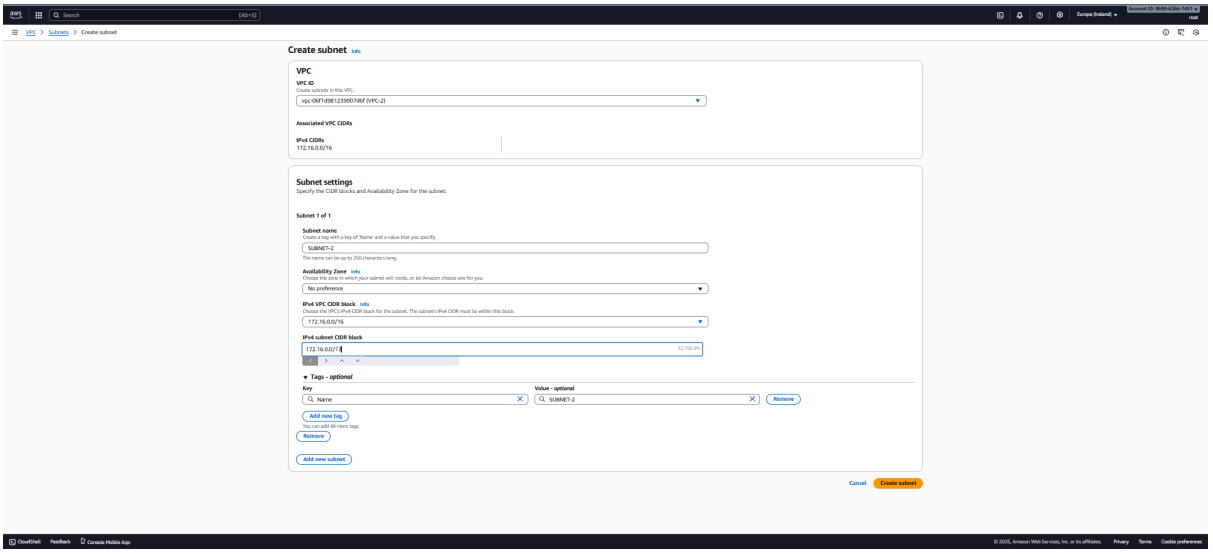
- CIDR: 10.0.0.0/17
- AZ: (any available zone)(optional)



Snapshot: Subnet creation

Ireland Subnet-2

- CIDR: 172.16.0.0/17
- AZ: (any available zone)(optional)



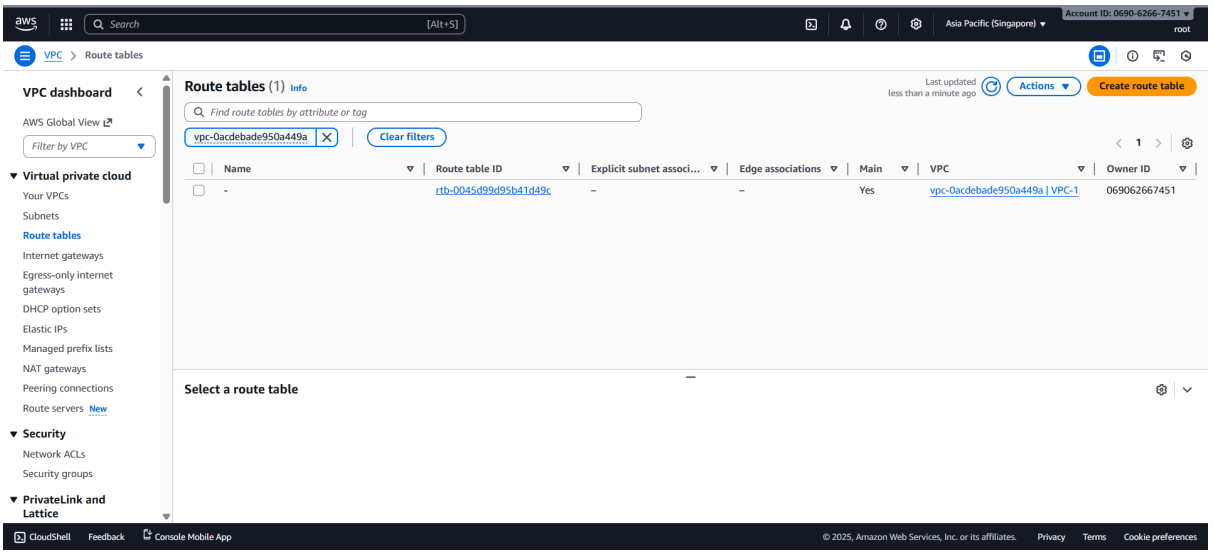
Snapshot: Subnet creation

Step 4: Create Route Tables

Region A Route Table

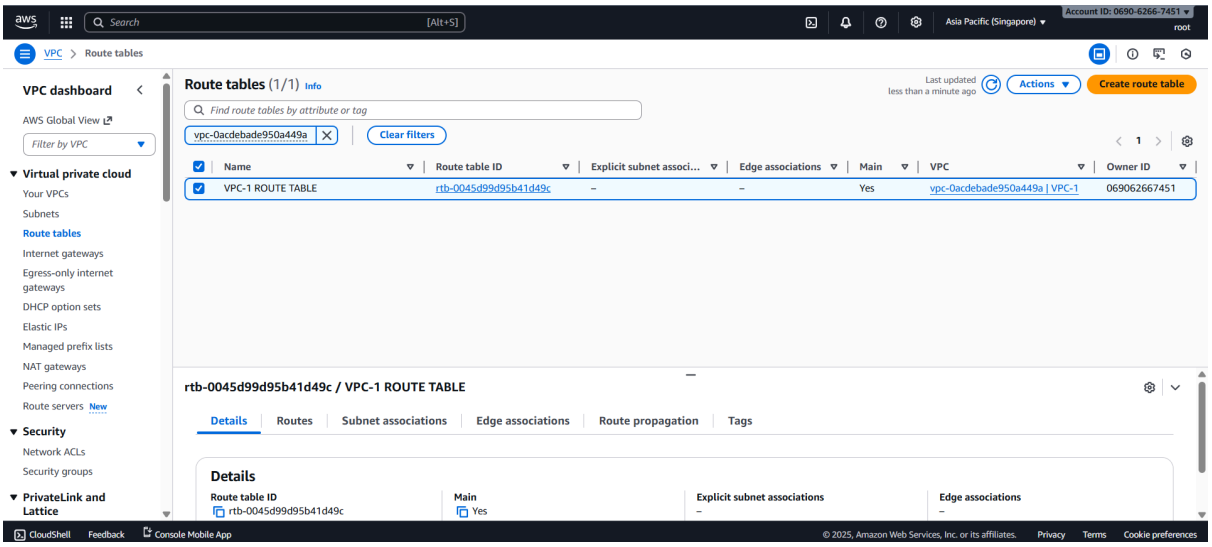
VPC Dashboard → Route Tables

1. Filtered the route tables by **VPC-1**, so only VPC-1–related route tables were visible.



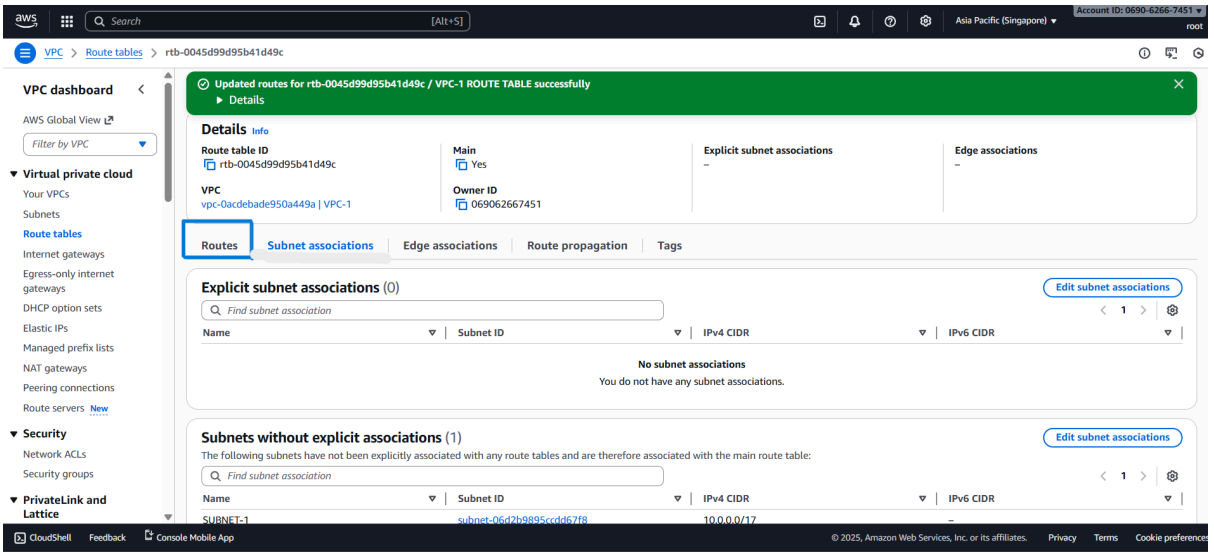
Snapshot: Filtering the route tables by **VPC-1**

2. Selected the default route table and **renamed it** to:
   VPC-1 ROUTE TABLE



Snapshot: Renaming the Root Table

3. Opened the route table → **Routes** tab → **Edit Routes**.

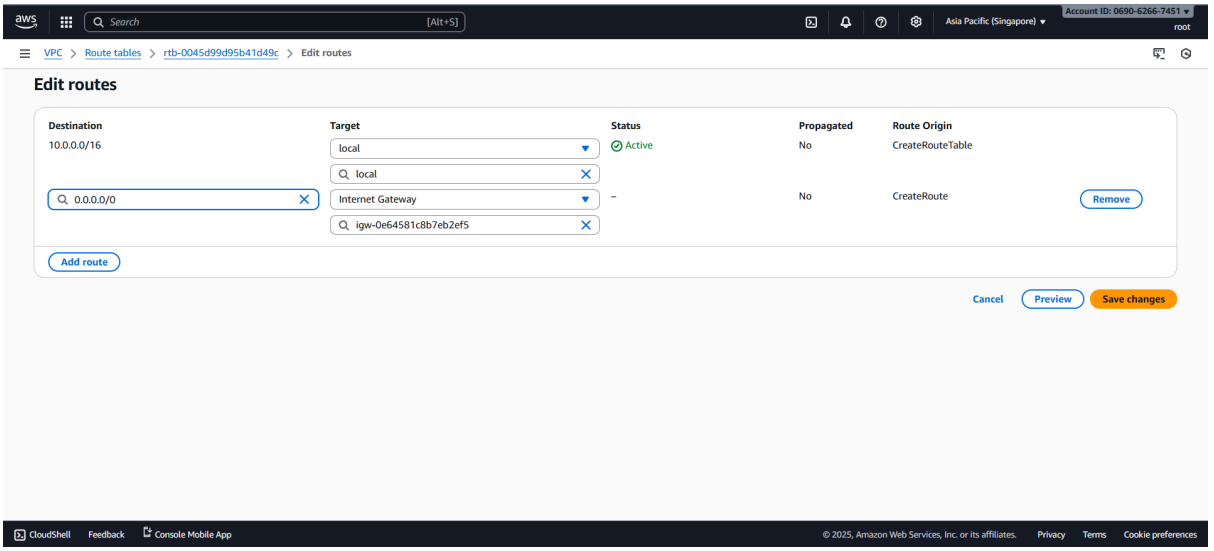


Snapshot: Root tab

4. Added a new route for communication with Region B:

   - **Destination:** 0.0.0.0/0
   - **Target:** Internet Gateway

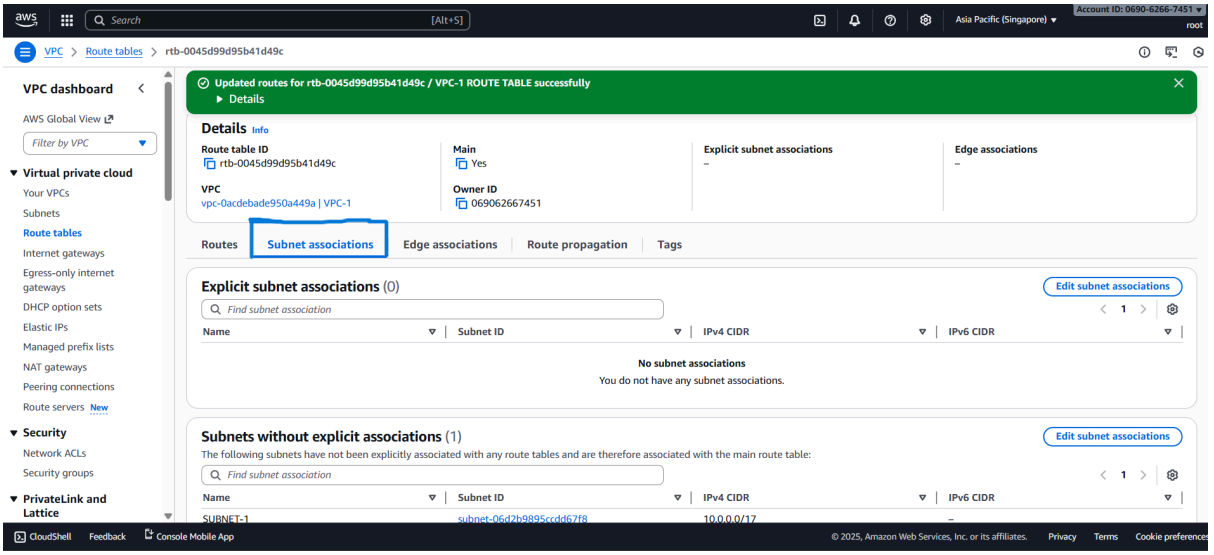
Saved changes.



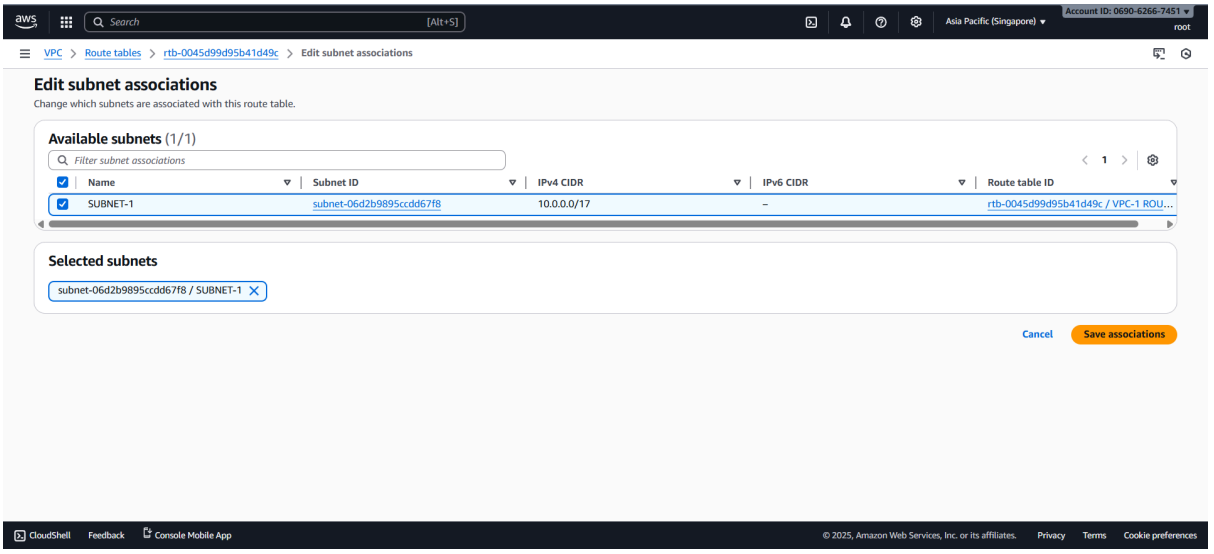
Snapshot : Edit Routes

5. Under **Subnet Associations** tab:

- Edit subnet associations
- Selected **SUBNET-1 (10.0.0.0/17)**
- Saved.



Snapshot: Subnet Associations Tab



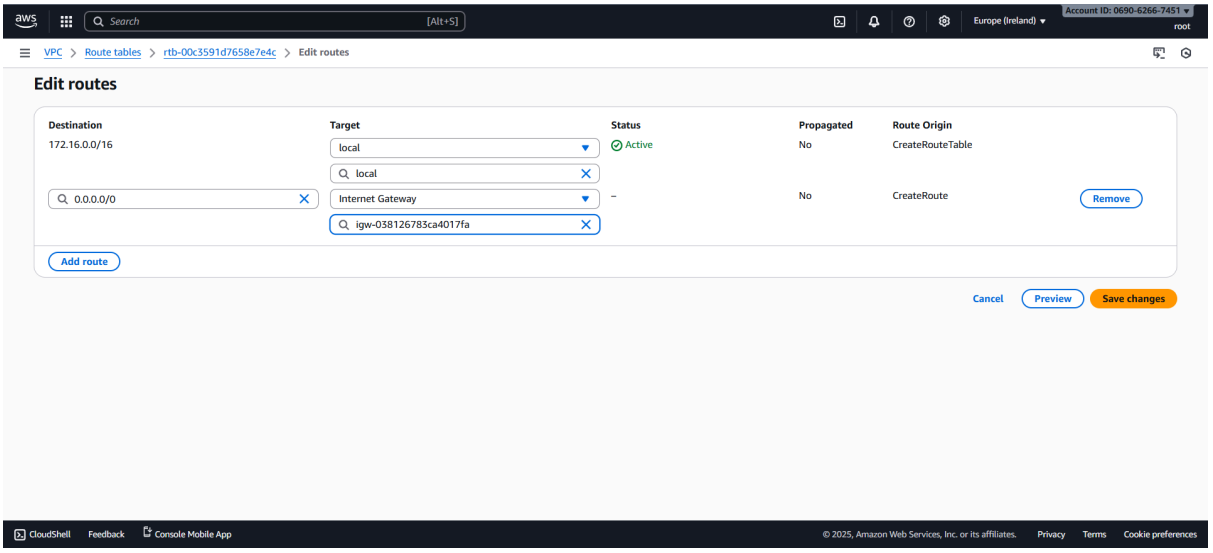
Snapshot: Edit Subnet Associations

Region B Route Table

1. Filtered all route tables by **VPC-2** so only route tables belonging to this VPC were shown.

2. Selected the main route table and renamed it to:
   VPC-2 ROUTE TABLE

3. Opened the route table → **Routes** tab → clicked **Edit Routes**.



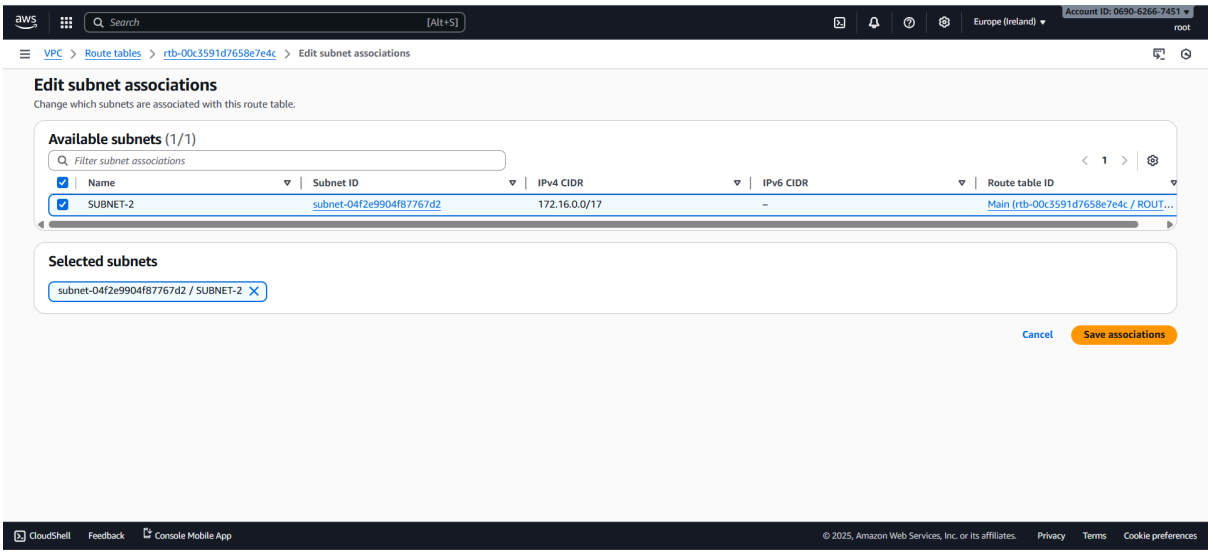
Snapshot: Snapshot :Edit Routes

4. Added a new route for communication with Region A:

   - **Destination:** 0.0.0.0/0
   - **Target:** Internet Gateway
   - Saved the route.

5. Opened the **Subnet Associations** tab:

   - Clicked **Edit subnet associations**
   - Selected **Subnet-B (172.16.0.0/17)**
   - Saved.

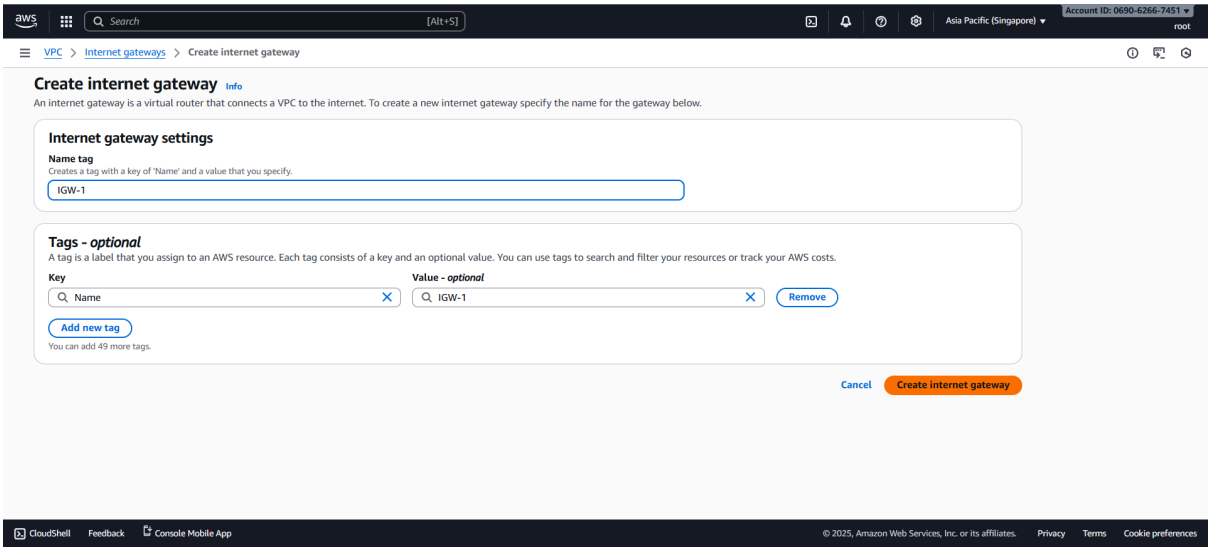


Snapshot: Edit Subnet Associations

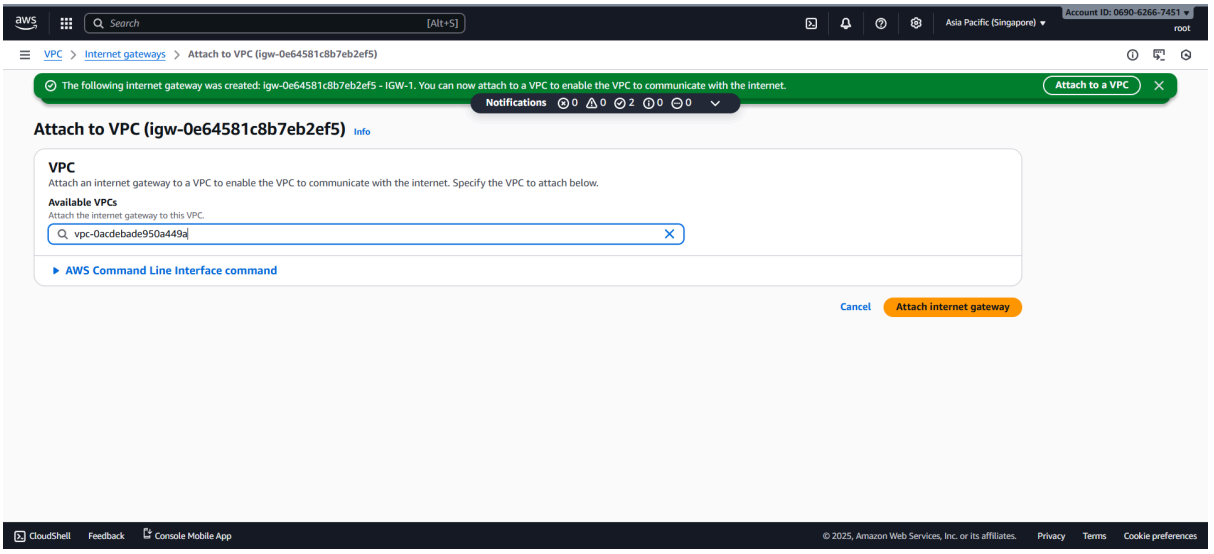
Step 5: Create Internet Gateway (IGW)

Region A IGW

- Create IGW → Attach to VPC-1Snapshot: Edit Subnet Associations



Snapshot: Create Internet Gateway



Snapshot: Attach to VPC

Region B IGW

- Create IGW → Attach to VPC-B
  (same as above procedure)

---

4. Create EC2 Instances

AWS Console → Services → EC2 → Instances → Launch Instances

1. Name the Instance

2. Choose Application & OS Image (AMI)

- Select Amazon Linux.
- AMI: Amazon Linux 2023 kernel-6.1 AMI

3. Select Instance Type

- Recommended: t3.micro or t2.micro (Free-tier eligible).

4. Configure Key Pair

- Create a new key pair for SSH access.

5. Configure Network Settings

- Select the appropriate VPC → choose VPC-1.
- Enable Auto-assign Public IP.

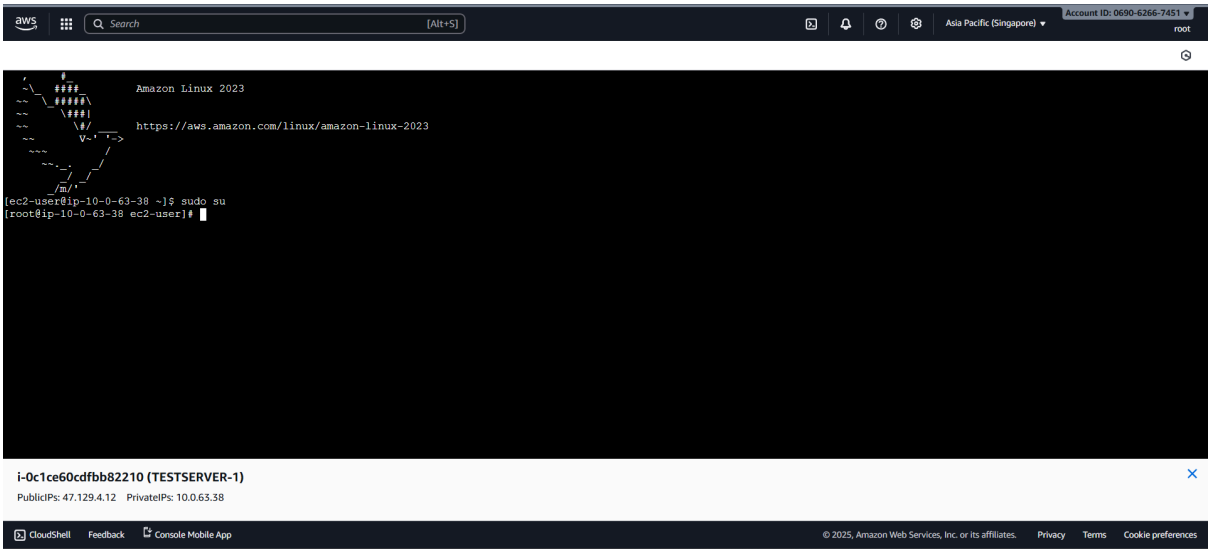
6. Configure Firewall (Security Group)

- Create a new security group.
- Provide a security group name.
- Set Type: All traffic .

7. Launch Instance

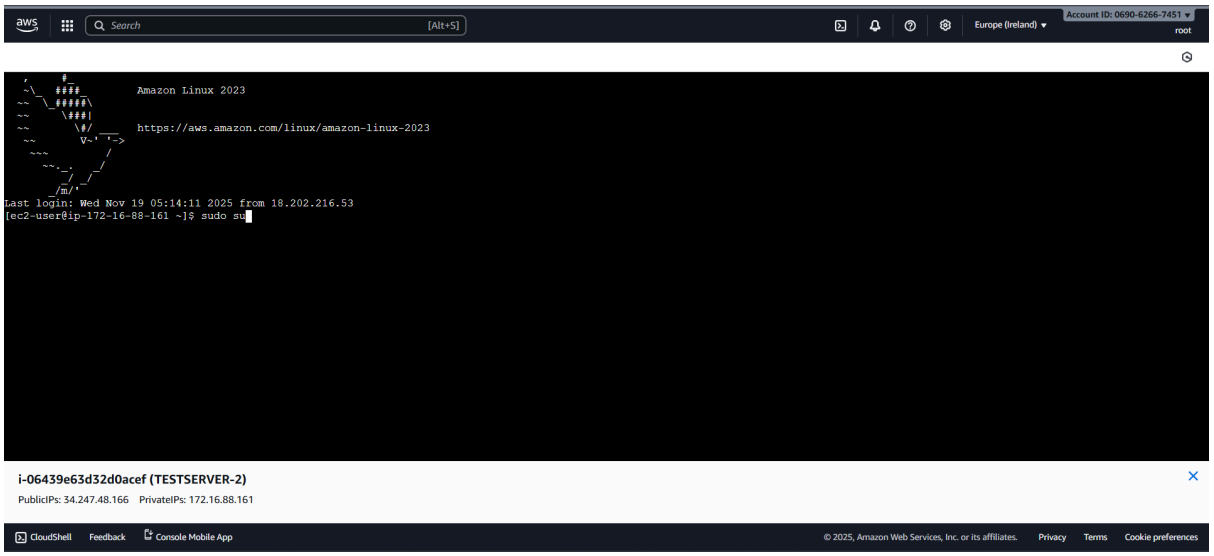
- Review all settings and click Launch Instance.

TESTSERVER-1 (Singapore)



Snapshot: Testserver-1

TESTSERVER-2 (Ireland)



Snapshot: Testserver-2

5. Create VPC Peering Connection

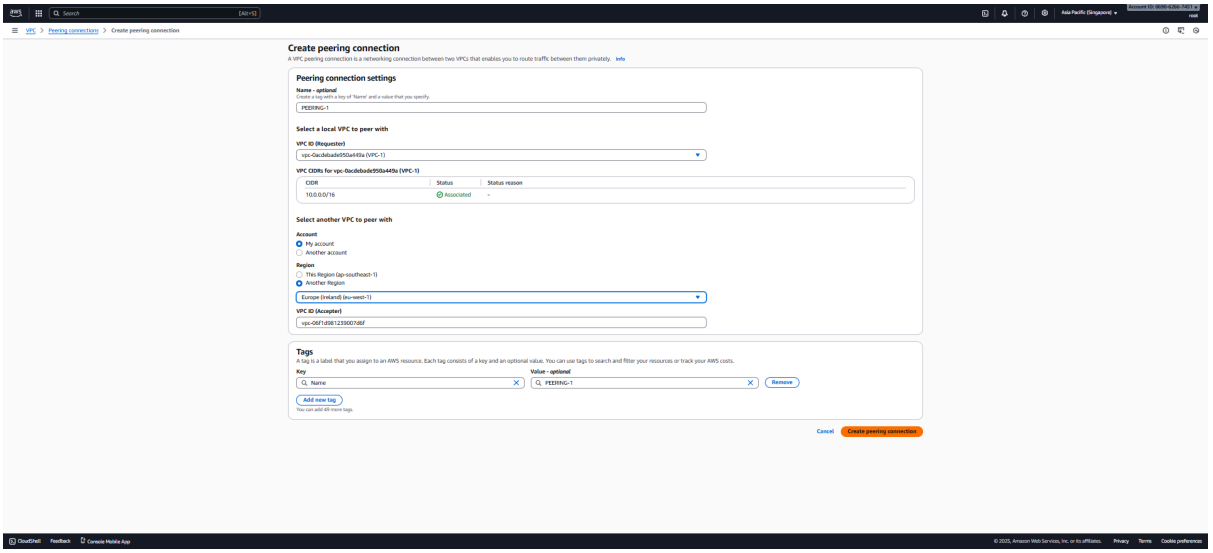
AWS Console → VPC → Peering Connections → Create Peering Connection

Steps to Create the Peering Connection

Step 1: Open the Peering Creation Page

1. Go to **VPC Dashboard**
2. In the left menu, click **Peering Connections**
3. Click **Create Peering Connection**

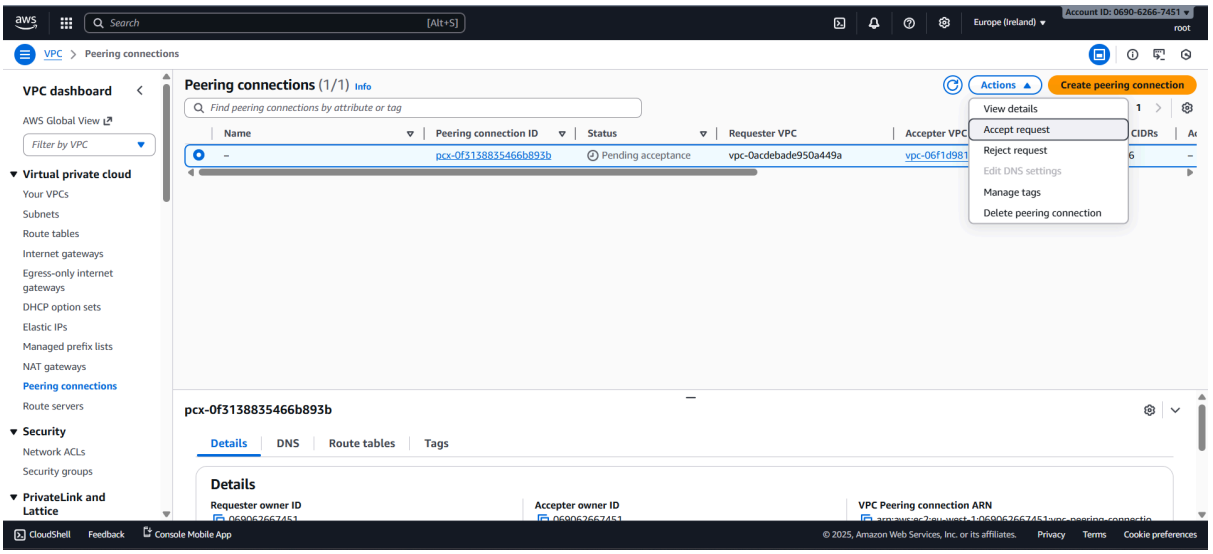
Step 1 — Initiate Peering Request from Singapore



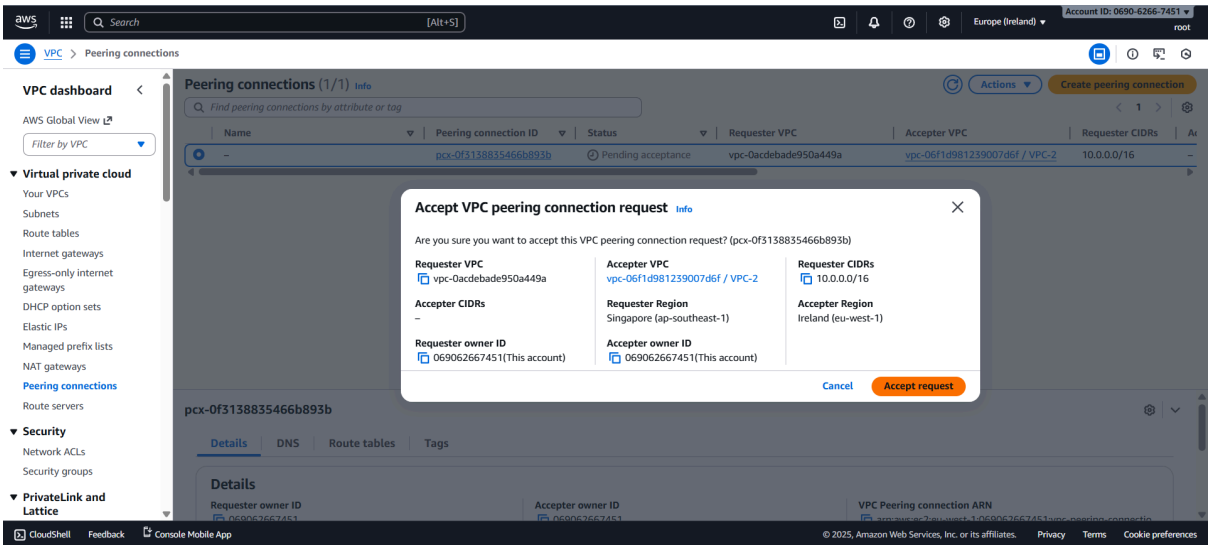
Snapshot: Initiating Peering Request

Step 2 — Accept Peering in Ireland

- Switch region → Ireland
- Accept peering request



Snapshot: Accepting Peering Request



Snapshot: Accepting Peering Request

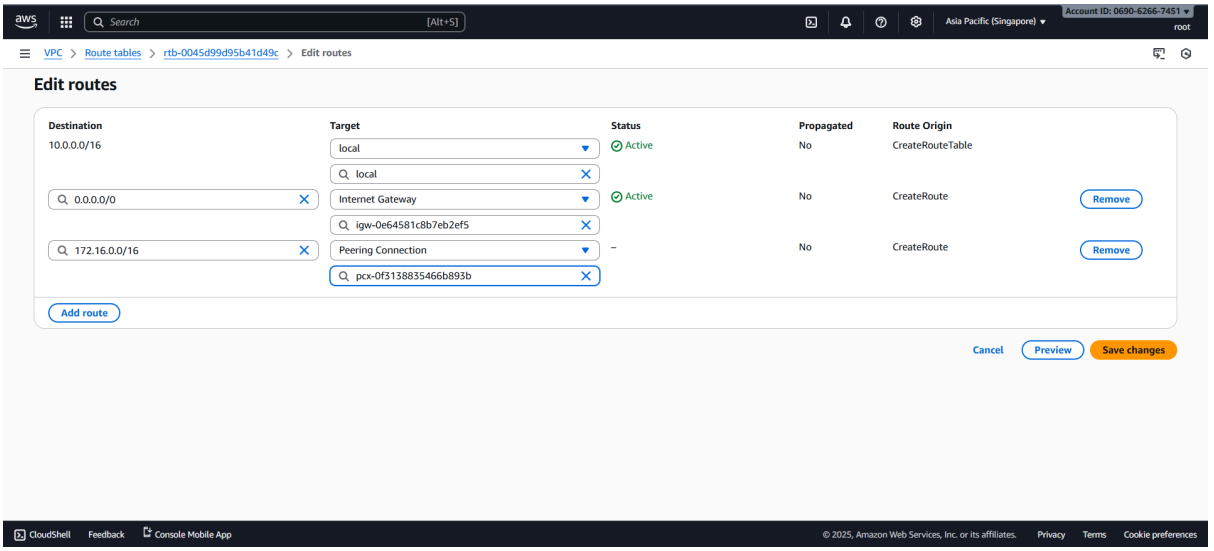
6. Update Route Tables

After the peering is active, update the routes.

Singapore Route Table (RT-A)

Add route:

- Destination: 172.16.0.0/16
- Target: Peering Connection



Snapshot: Updating Route Tables

Ireland Route Table (RT-B)

Add route:

- Destination: 10.0.0.0/16
- Target: Peering IConnection

---

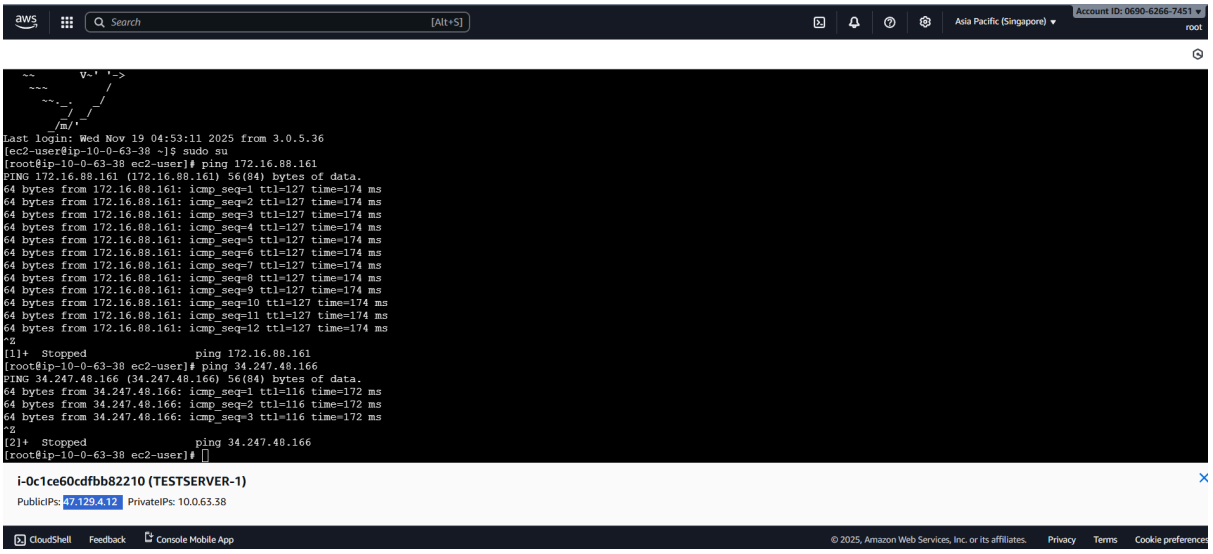
7. Test Private Connectivity

SSH into EC2-A and run:

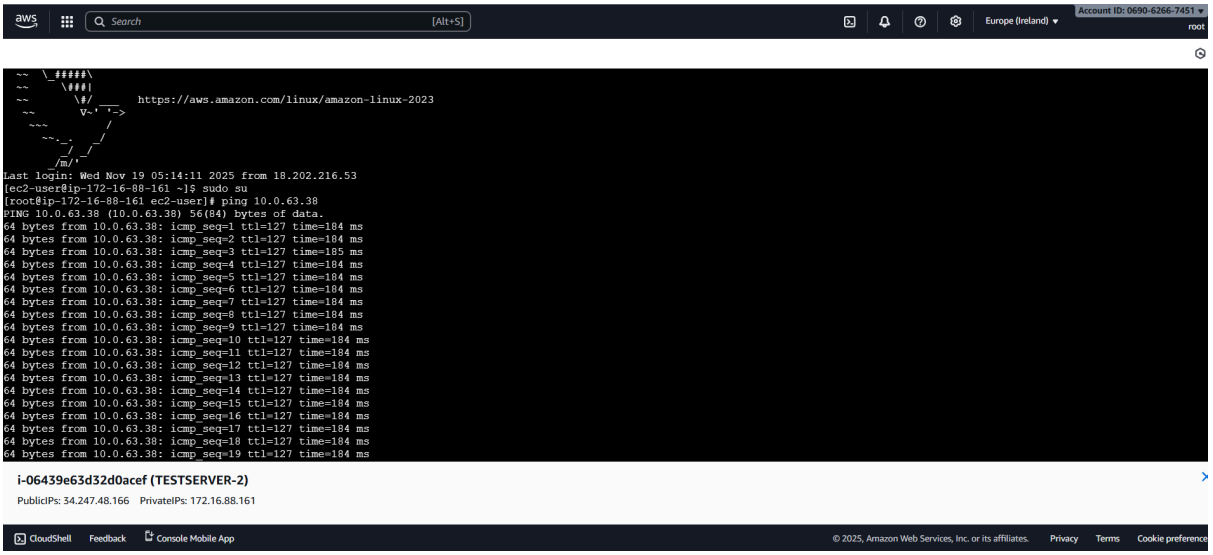
ping 172.16.88.161

SSH into EC2-B and run:

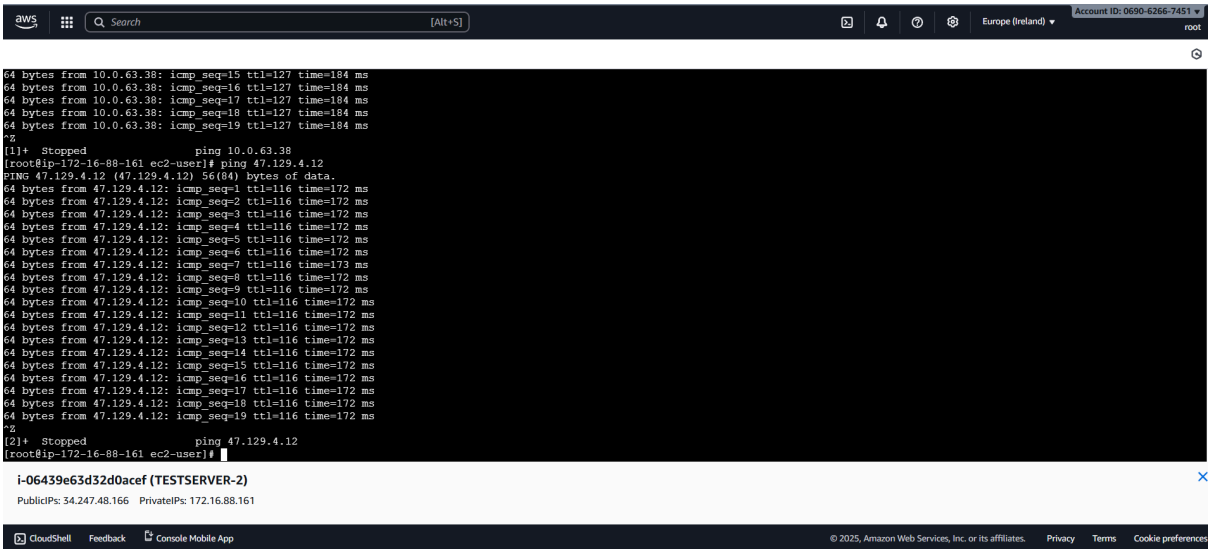
ping 10.0.63.38



Snapshot: Testing Private Connectivity



Snapshot: Testing Private Connectivity



Snapshot: Testing Private Connectivity

8. Final Outcome

By completing this setup:

- Both EC2 instances communicate privately across regions