VPC-Peering

This project demonstrates the setup of a **VPC Peering connection** between two AWS regions: **Mumbai (ap-south-1)** and **Tokyo (ap-northeast-1)**. The Mumbai VPC has a **CIDR range of 10.0.0.0/16**, while the Tokyo VPC uses **192.0.0.0/16**.

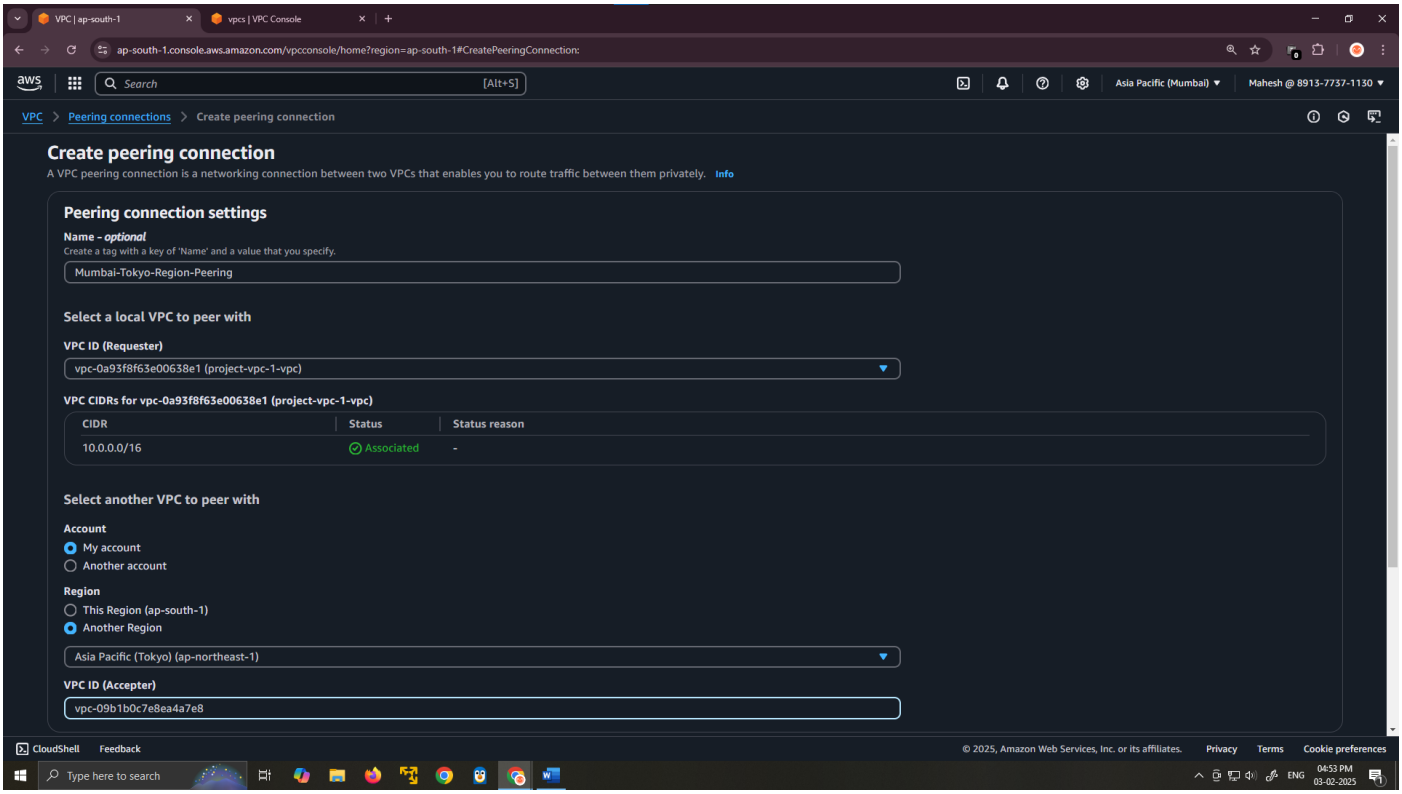
The process includes:

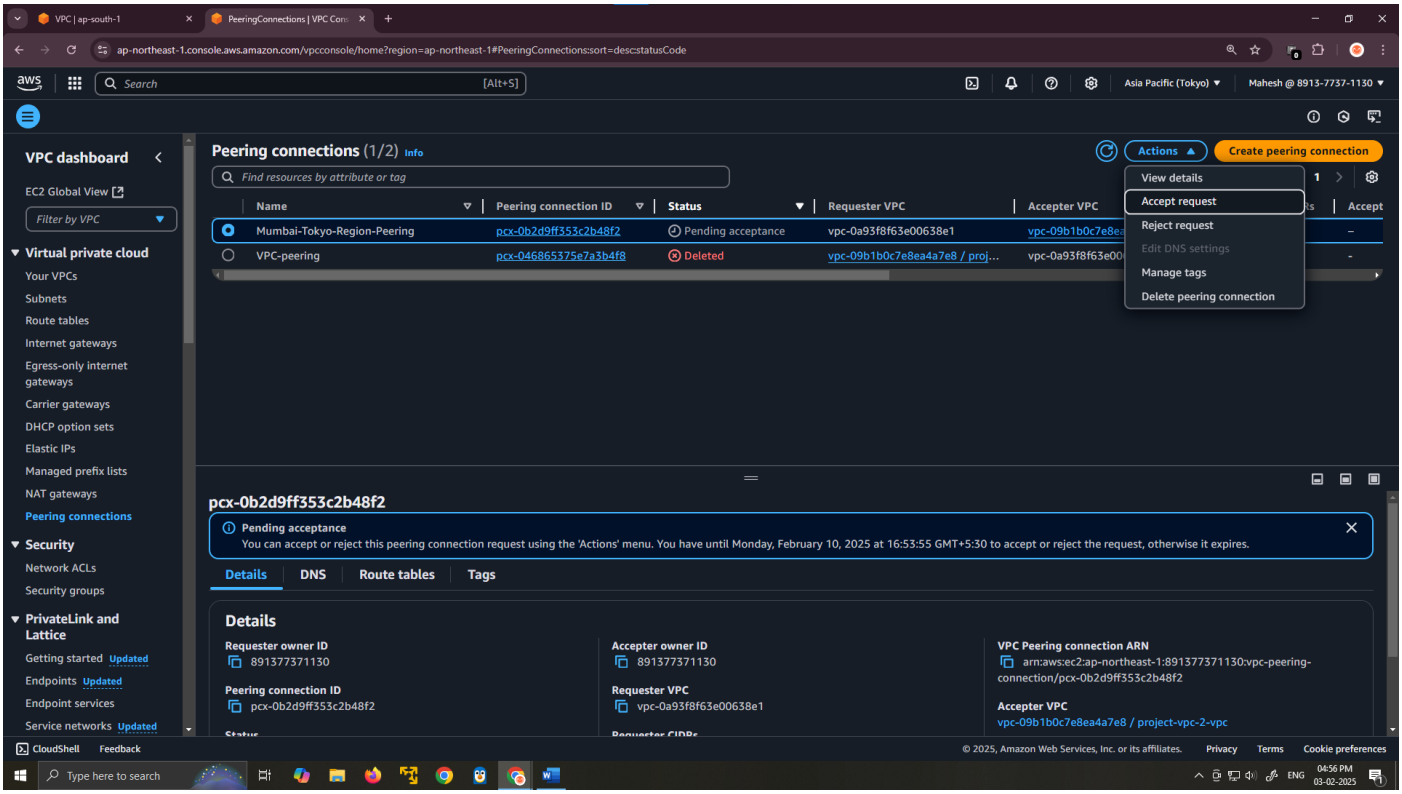
1. **Creating and accepting the VPC Peering Connection** between the two VPCs.
2. **Updating route tables** in both VPCs to allow cross-region communication.
3. **Configuring security groups** to permit ICMP (ping) and other necessary traffic.
4. **Testing connectivity** between instances in both regions using the ping command.

This setup enables secure, low-latency, and private communication between VPCs without using the public internet. 🚀

Step 1: Create a VPC Peering Connection

1. **Login to AWS Console** and navigate to **VPC Dashboard**.
2. In the **Mumbai region** (ap-south-1):
    - Go to **Peering Connections** → Click **Create Peering Connection**.
    - **Name tag:** Mumbai-Tokyo-Peering
    - **VPC Requester:** Select Mumbai VPC (10.0.0.0/16).
    - **VPC Accepter:** Choose **Another account or Another region**.
    - **Region:** Select Tokyo (ap-northeast-1).
    - **Accepter VPC ID:** Select Tokyo VPC (192.0.0.0/16).
    - Click **Create Peering Connection**.
3. Now, go to the **Tokyo region** (ap-northeast-1):
    - Navigate to **VPC Peering Connections**.
    - Select the **Peering Request** received from Mumbai VPC.
    - Click **Accept Request**.
4. **Verify Peering Connection:**
    - After accepting, the **status** of the peering connection should change to Active.





Step 2: Update Route Tables

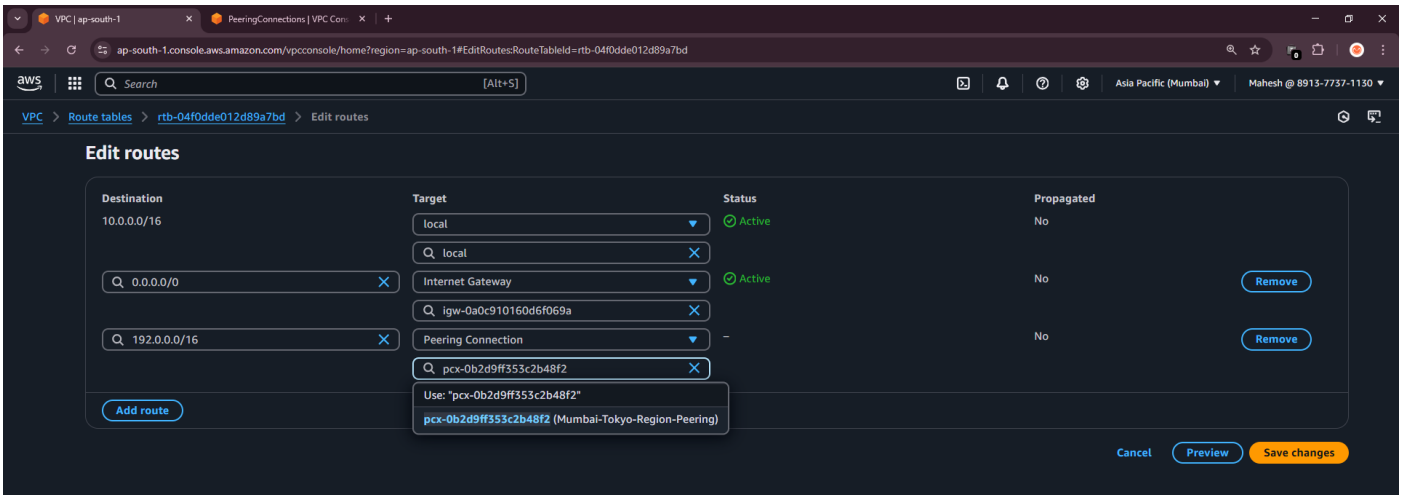
After establishing the VPC peering connection, you need to update the **route tables** in both VPCs to allow traffic to pass.

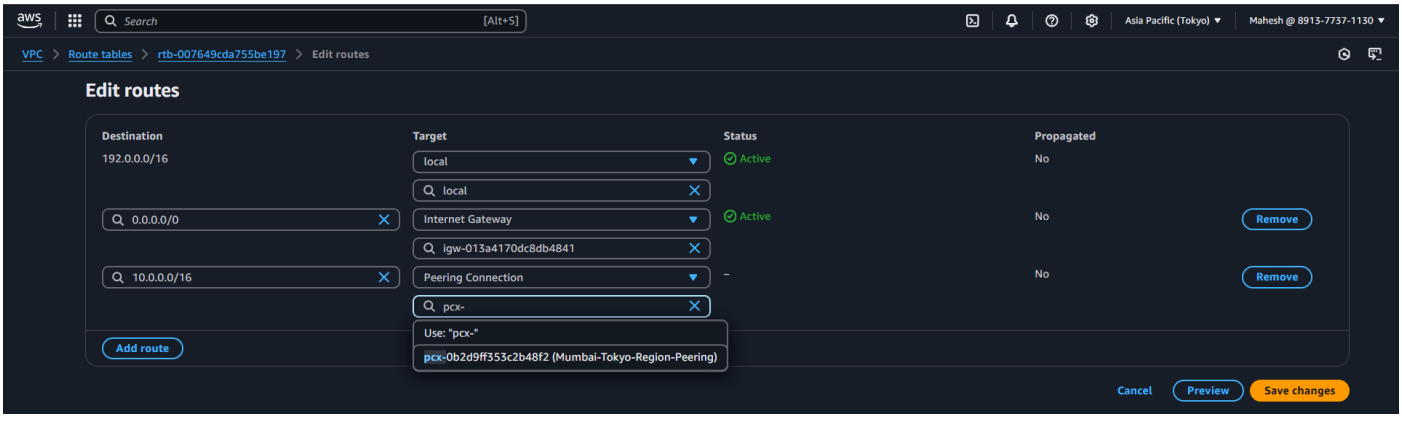
In Mumbai Region (ap-south-1)

1. Navigate to **VPC → Route Tables**.
2. Select the **Route Table** associated with your **Mumbai VPC (10.0.0.0/16)**.
3. Click on **Routes → Edit Routes**.
4. Add a new route:
    - **Destination:** 192.0.0.0/16 (Tokyo VPC CIDR)
    - **Target:** Select the **Peering Connection (pcx-xxxxxxxxxx)**.
5. Click **Save changes**.

In Tokyo Region (ap-northeast-1)

1. Navigate to **VPC → Route Tables**.
2. Select the **Route Table** associated with your **Tokyo VPC (192.0.0.0/16)**.
3. Click on **Routes → Edit Routes**.
4. Add a new route:
    - **Destination:** 10.0.0.0/16 (Mumbai VPC CIDR)
    - **Target:** Select the **Peering Connection (pcx-xxxxxxxxxx)**.
5. Click **Save changes**.





Step 3: Update Security Groups

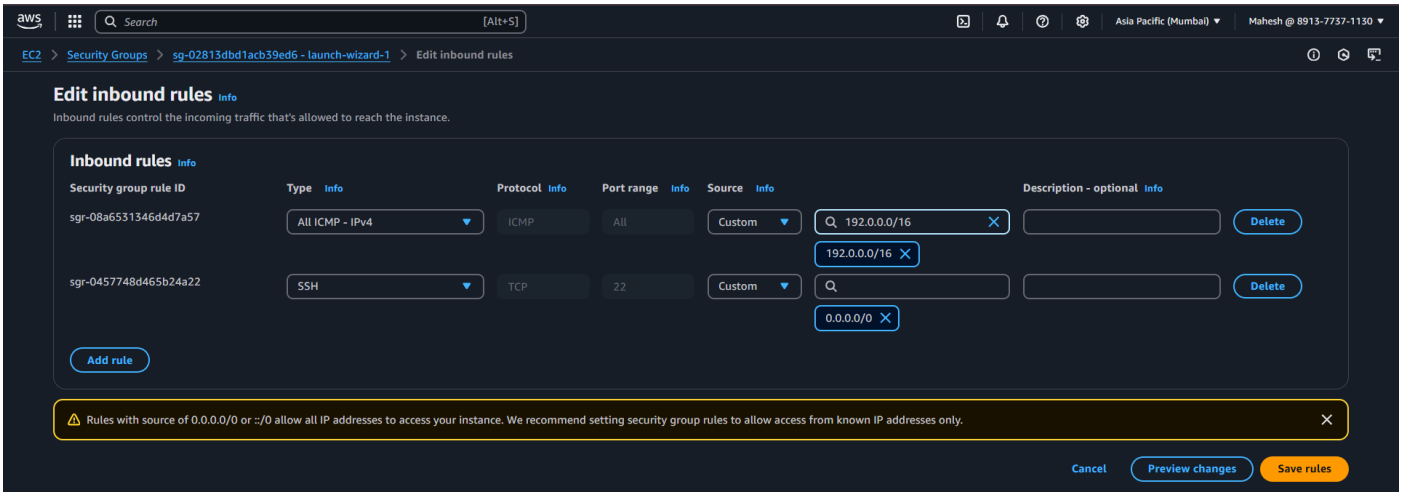
By default, security groups restrict all inbound and outbound traffic. You need to allow **ICMP (ping) and other necessary traffic**.

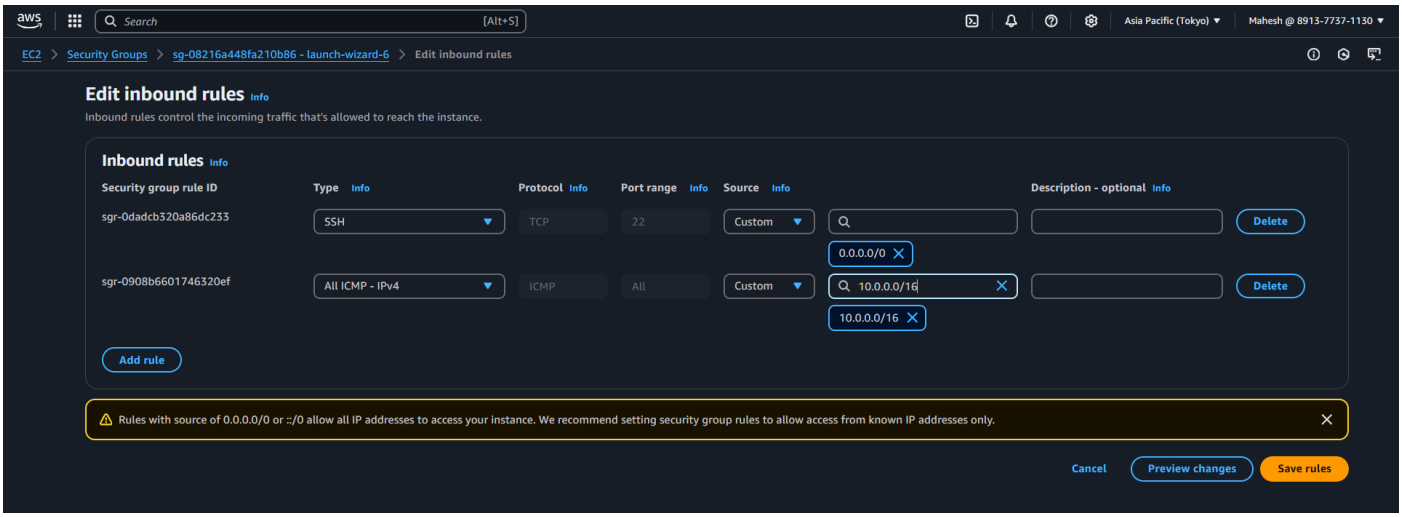
In Mumbai Region (ap-south-1)

1. Navigate to **EC2 → Security Groups**.
2. Select the **Security Group** associated with Mumbai VPC instances.
3. Go to the **Inbound rules** and click **Edit inbound rules**.
4. Add a new rule:
    - **Type:** All ICMP - IPv4
    - **Protocol:** ICMP
    - **Port Range:** All
    - **Source:** 192.0.0.0/16 (Tokyo VPC CIDR)
5. Click **Save rules**.

In Tokyo Region (ap-northeast-1)

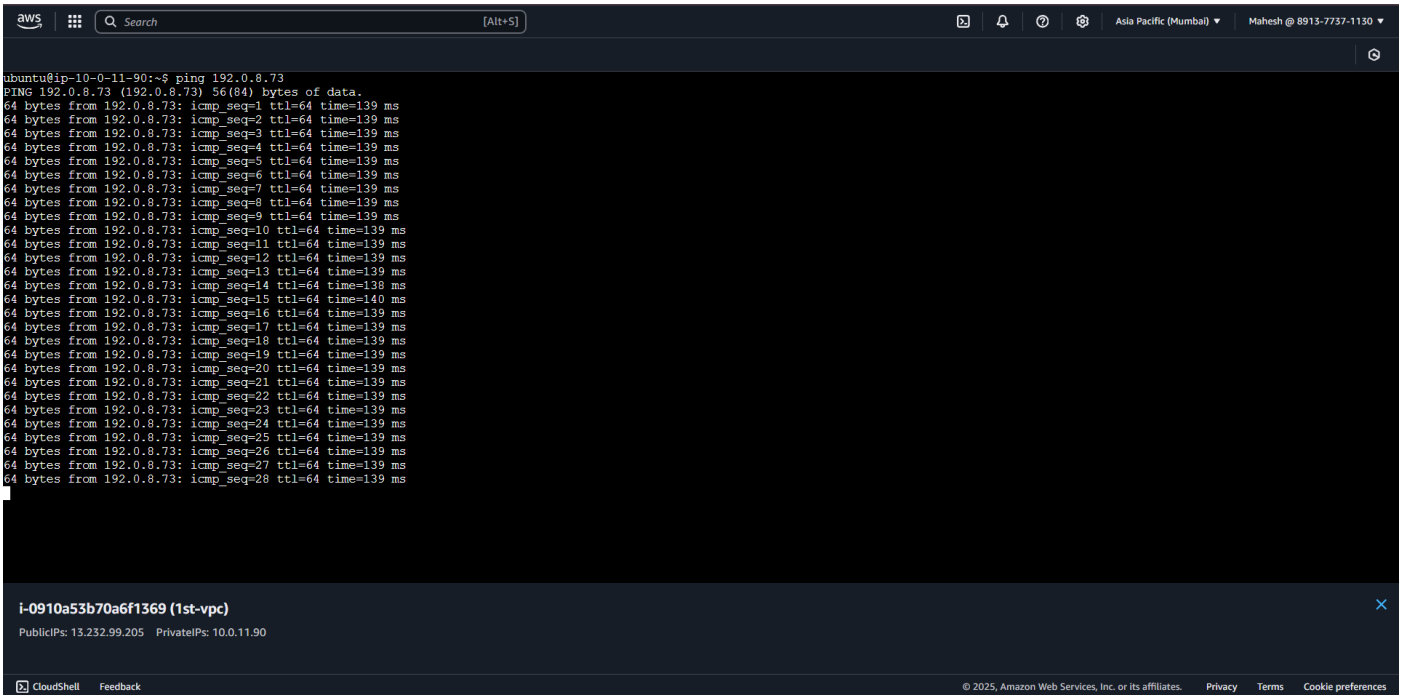
1. Navigate to **EC2 → Security Groups**.
2. Select the **Security Group** associated with Tokyo VPC instances.
3. Go to the **Inbound rules** and click **Edit inbound rules**.
4. Add a new rule:
    - **Type:** All ICMP - IPv4
    - **Protocol:** ICMP
    - **Port Range:** All
    - **Source:** 10.0.0.0/16 (Mumbai VPC CIDR)
5. Click **Save rules**.

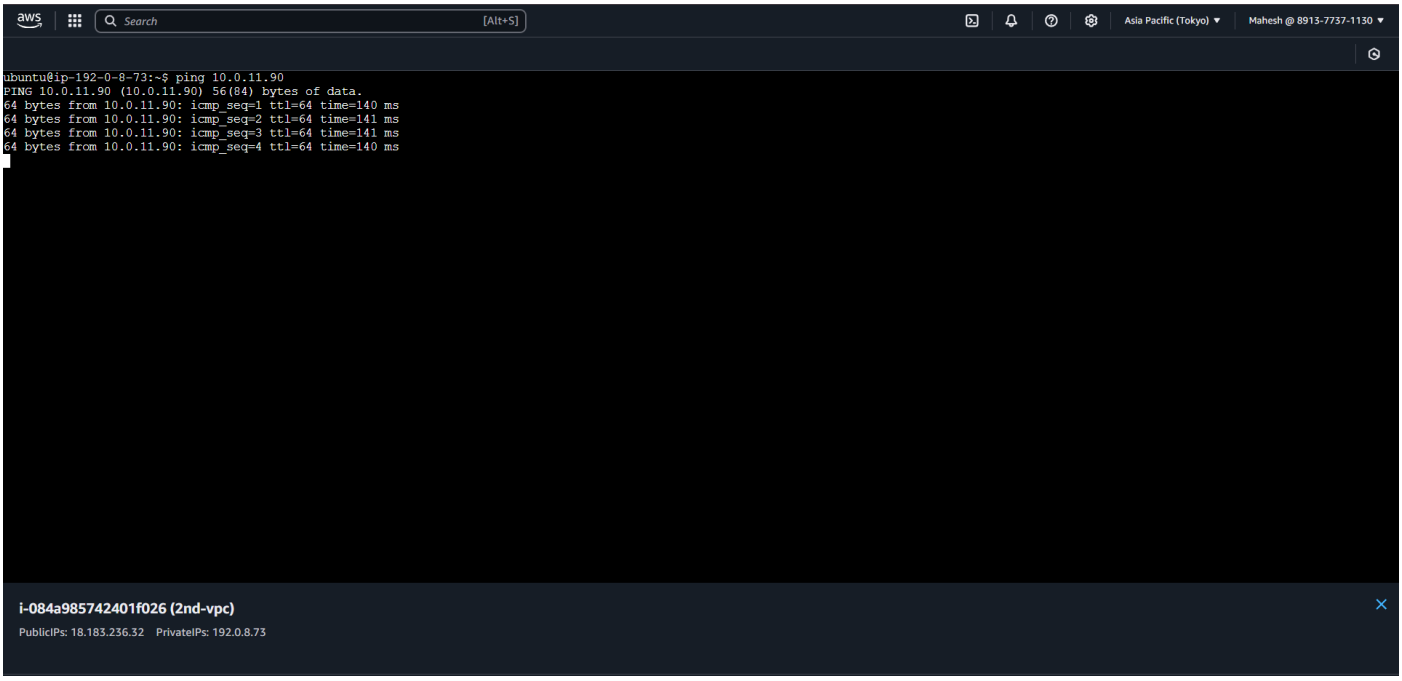




Test the Peering Connection.

1. SSH into an instance
2. ping Private IP of instance





If the **ping is successful**, your **VPC peering connection** is working!