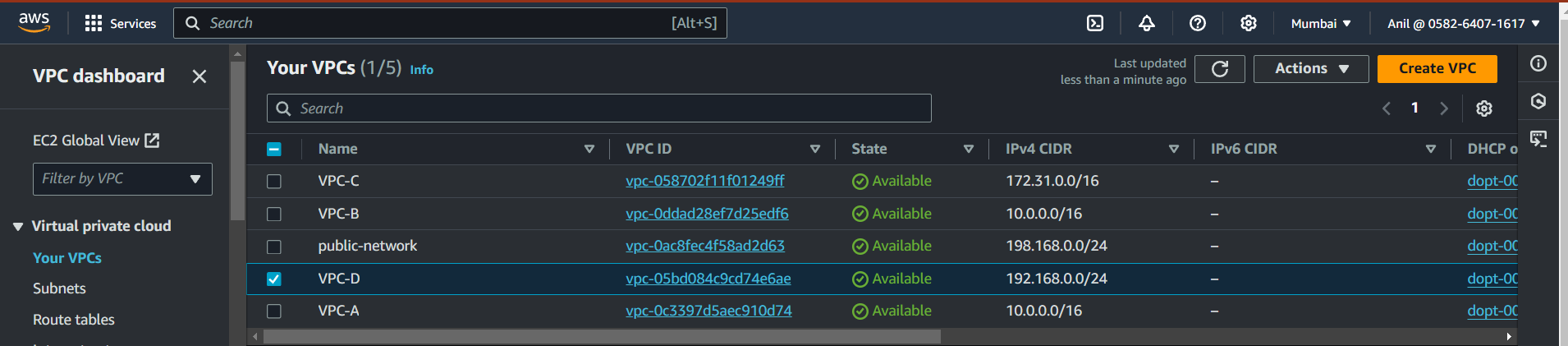
Step 1: Create VPCs in 4 Regions

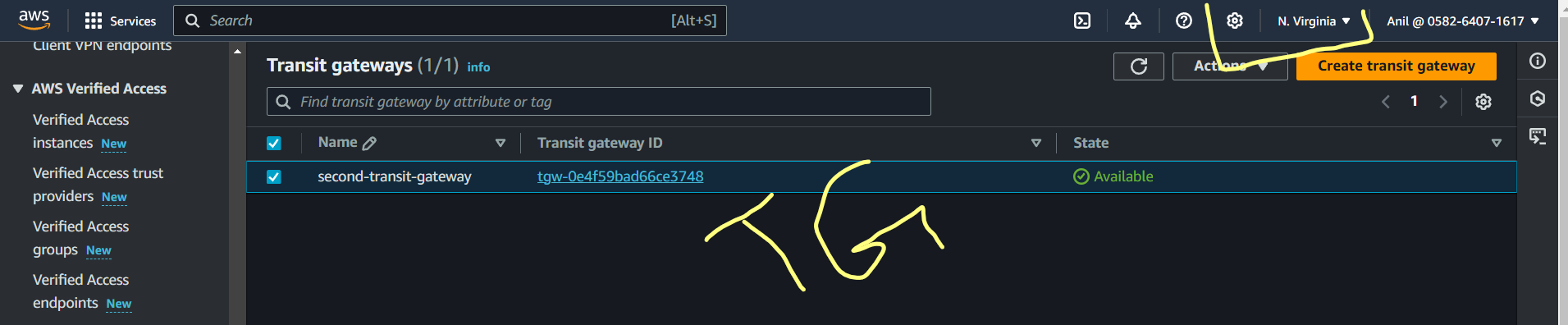
For Each Region:

1. Log into AWS Management Console.
   * Navigate to VPC Dashboard.
2. Create a New VPC:
   * In the VPC Dashboard, click Create VPC.
   * Select VPC with a Single Public Subnet option (you can modify this later).
   * Enter a unique CIDR block for each VPC:
     + Region 1: 10.0.0.0/16
     + Region 2: 10.1.0.0/16
     + Region 3: 10.2.0.0/16
     + Region 4: 10.3.0.0/16
   * Click Create.

**

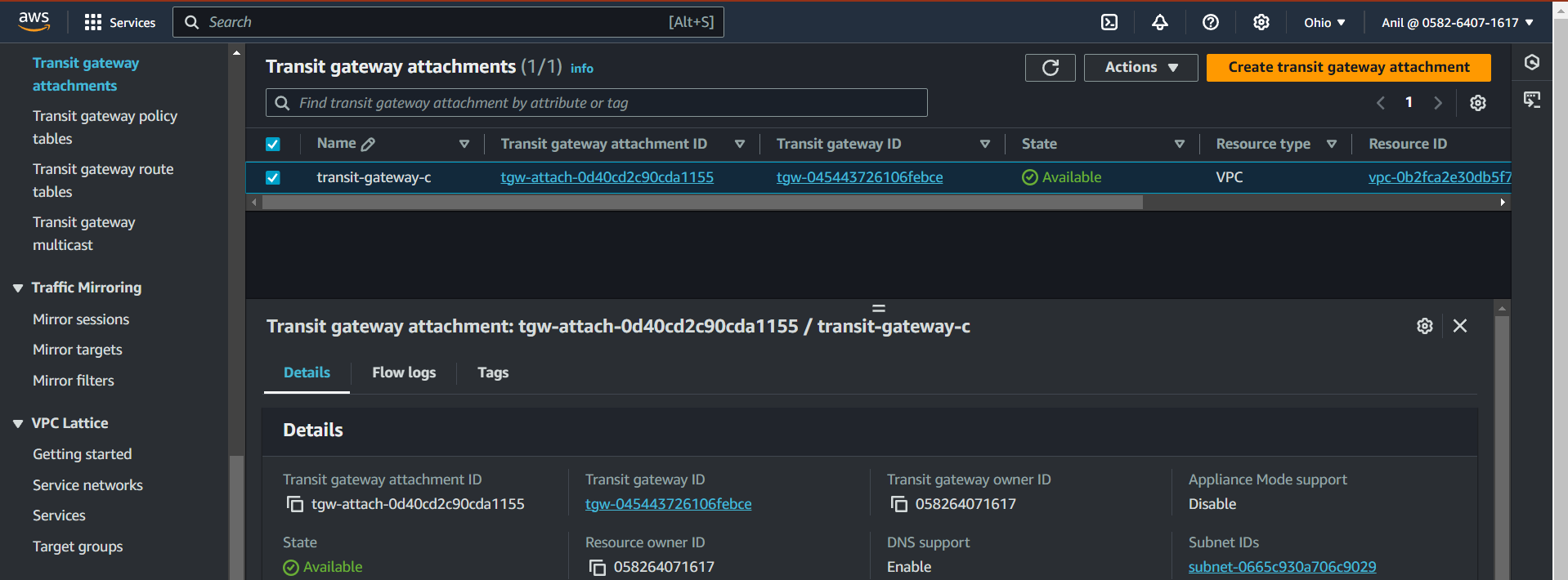
Step 2: Set up Transit Gateway (TGW) in Each Region

1. Navigate to AWS Transit Gateway (TGW):
   * Go to VPC Dashboard > Transit Gateways.
2. Create a Transit Gateway in Each Region:
   * For each region, click Create Transit Gateway.
   * Provide a name (e.g., TGW-Region1).
   * Set up an Autonomous System Number (ASN) (for internal BGP routing) or use default.
   * Leave other settings as default and click Create.
3. Verify the Transit Gateway is available in each region.

**

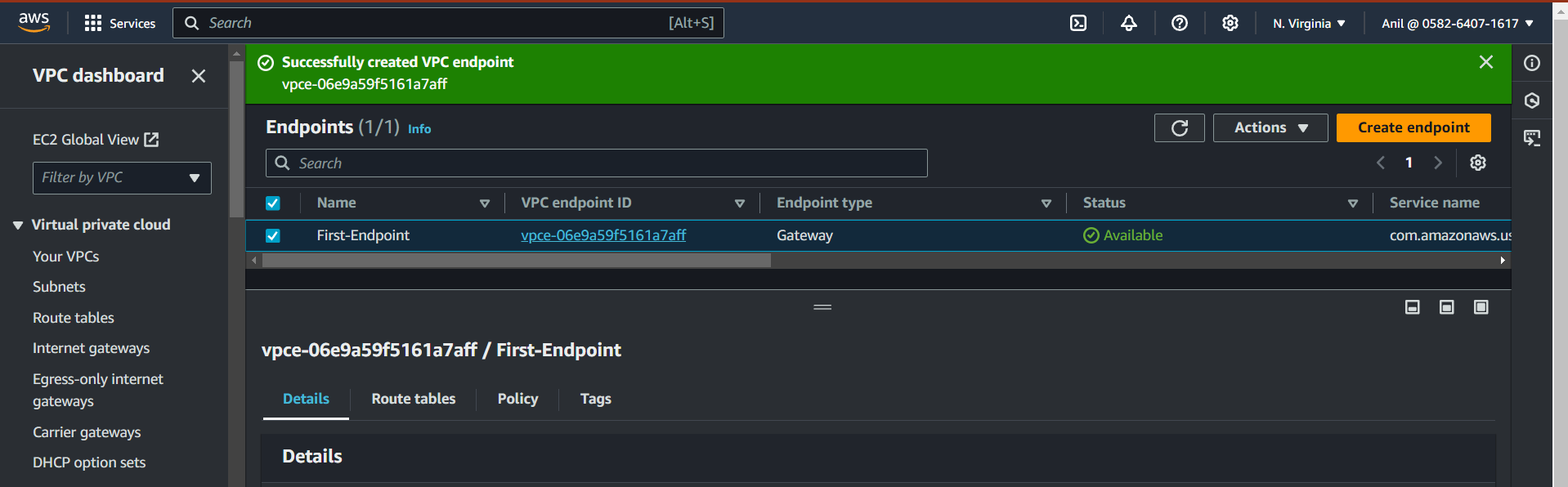
Step 3: Attach VPCs to Transit Gateway

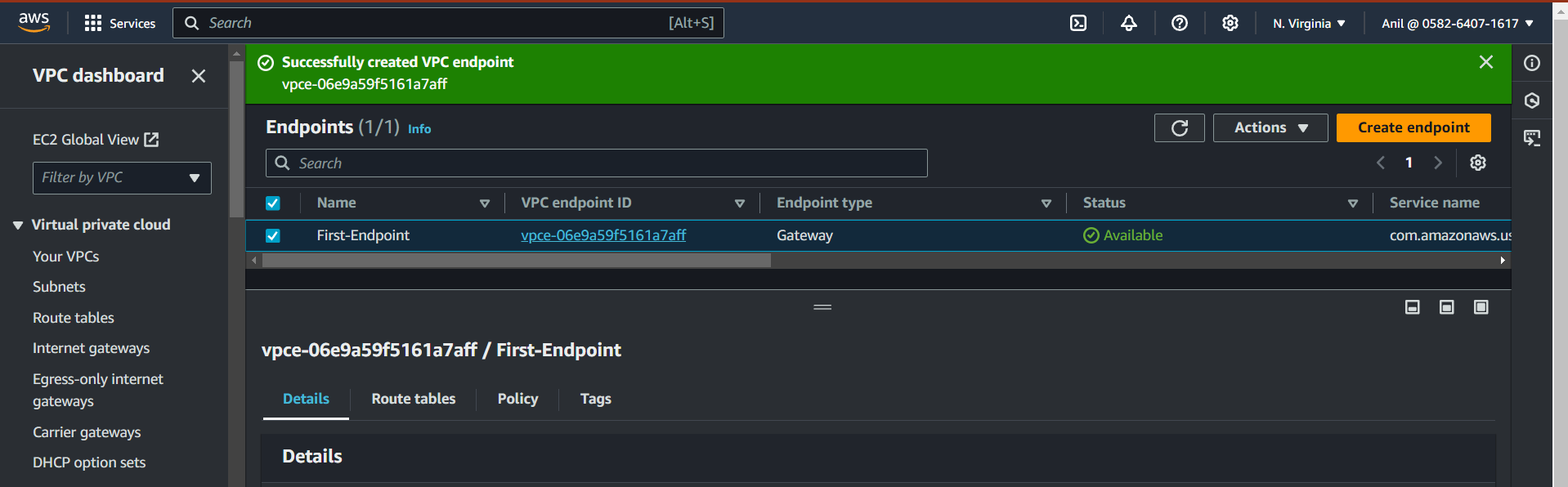
1. Go to Transit Gateway Attachments in the VPC Console.
2. Create an Attachment for Each VPC:
   * For each VPC in each region, click Create Transit Gateway Attachment.
   * Select the respective VPC, Subnet, and Transit Gateway.
   * Repeat for every VPC in each region, ensuring that VPCs are attached to the correct region’s TGW.
3. Configure routing in each VPC’s route tables to route traffic through the TGW for inter-region communication.
   * Add routes for remote VPC CIDRs using the Transit Gateway as the target.

**

* + VPC in Region 1 (CIDR 10.0.0.0/16):
    - Add routes to 10.1.0.0/16, 10.2.0.0/16, and 10.3.0.0/16 through the Transit Gateway.
  + VPC in Region 2 (CIDR 10.1.0.0/16):
    - Add routes to 10.0.0.0/16, 10.2.0.0/16, and 10.3.0.0/16 through the Transit Gateway.

Repeat this for all VPCs.

**



Step 4: Set up VPC Endpoints for Secure Access to AWS Services

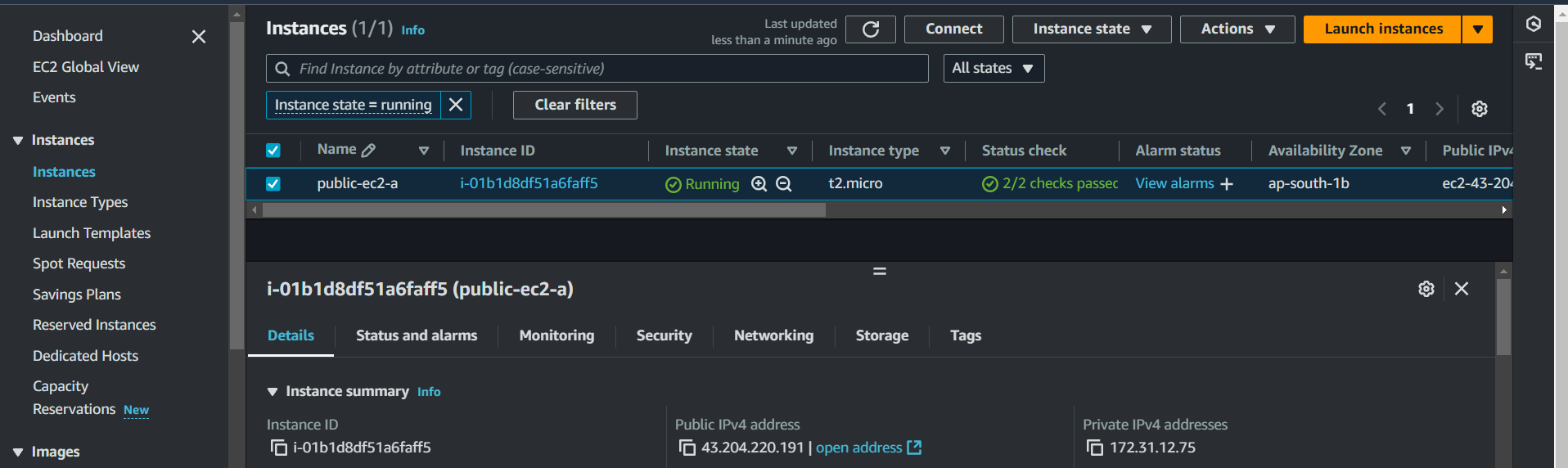
1. Choose the Service to Access:
   * VPC endpoints are used to access AWS services privately
   * For example, to access S3 securely, you need to set up a Gateway VPC Endpoint for S3.
2. Create VPC Endpoint for Each Service:
   * Go to VPC Console > Endpoints.
   * Click Create Endpoint.
   * Choose the service to access (e.g., com.amazonaws.us-east-1.s3 for S3).
   * Select VPC and choose the subnet(s) to associate the endpoint.
   * If you need to use PrivateLink for specific services, you can create Interface Endpoints instead.
3. Configure Security Groups:
   * Ensure that security groups for your EC2 instances and endpoint services allow the required traffic (e.g., S3 traffic).
4. Repeat for other services you need to access through endpoints, such as DynamoDB, SQS, SNS, etc.

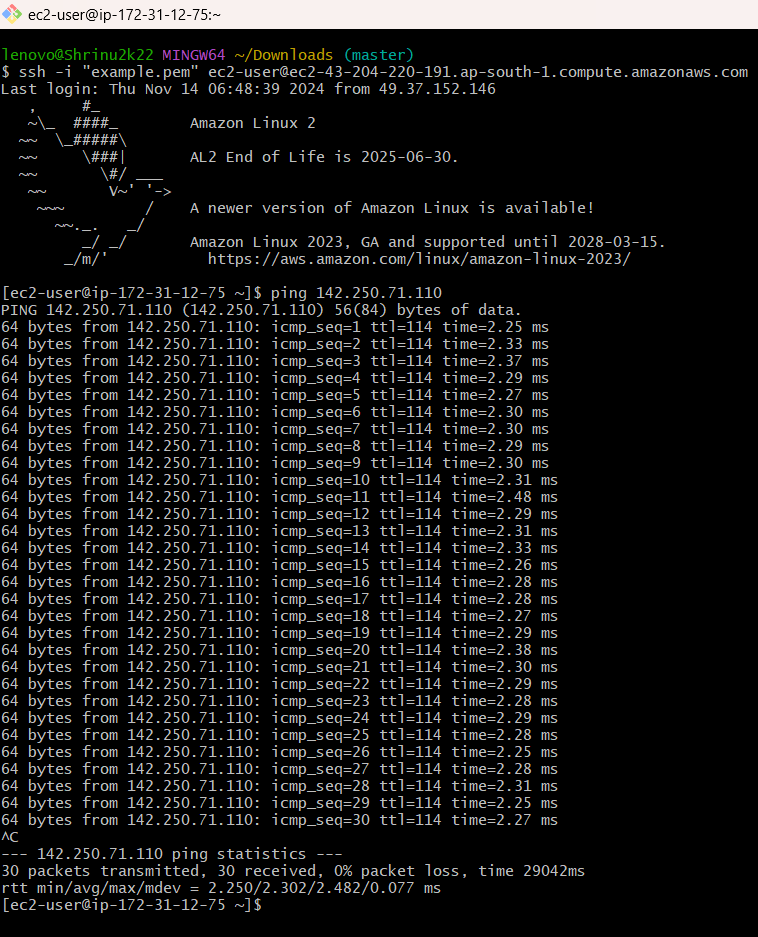
Step 5: Ensure Cross-Region Communication Using TGW Peering

1. Peering Transit Gateways Across Regions:
   * Navigate to Transit Gateway > Peering.
   * Click Create Peering Connection.
   * Select the Transit Gateways you want to peer across regions (e.g., TGW-Region1 with TGW-Region2).
   * Repeat the peering setup between all required regions.
   * After the peering is established, update the Transit Gateway route tables to allow routing between regions.

Step 6: Test the Configuration

1. Test EC2 Instances:
   * Launch EC2 instances in each VPC and ensure that they are properly configured with the correct security groups.
   * Test ping or SSH/RDP between instances across different VPCs using private IPs.

**

**