Challenge -2

--------------------------------------------------------------------------------------------

**Use Case: Setting up Transit Gateway and VPC Endpoints for a Multi-VPC Architecture**  
**Scenario:**  
 A large organization is migrating its on-premises infrastructure to the AWS cloud.  
 The organization's architecture involves multiple VPCs for different departments and applications, each requiring secure communication with centralized services and external resources.  
 The IT team needs to design and implement a scalable and efficient network architecture to accommodate the organization's growth and ensure robust connectivity between VPCs and external services.  
**Objectives:**

* Design and deploy a scalable network architecture using AWS Transit Gateway to simplify network connectivity between multiple VPCs.
* Configure VPC endpoints to securely access AWS services without internet gateways or NAT gateways, ensuring data privacy and minimizing exposure to external threats.

**Note:**

* Create 4 VPCs in 4 different regions and set up Transit Gateway.
* Do not use default VPCs.

**Step1: 4 Different IP Address**

**1.) VPC-A (N. Virginia, us-east-1) 🡪 10.0.0.0/16**

**2.) VPC-B (OHIO -us-east-2) → 172.16.0.0/16**

**3). VPC-C (California, us-west-1) 🡪192.168.0.0/16**

**4.) VPC-D (Oregon, us-west-2) → 100.64.0.0/16**

**Step2: Create 4 VPCS in Different regions**

**Go to VPC Console 🡪 Create VPC 🡪 VPC Settings 🡪 VPC Only 🡪 Name**

**VPC-1 N.Virginia 🡪 IPv4 CIDR 🡪 10.0.0.0/8 🡪 Create VPC**

**Subnets:**

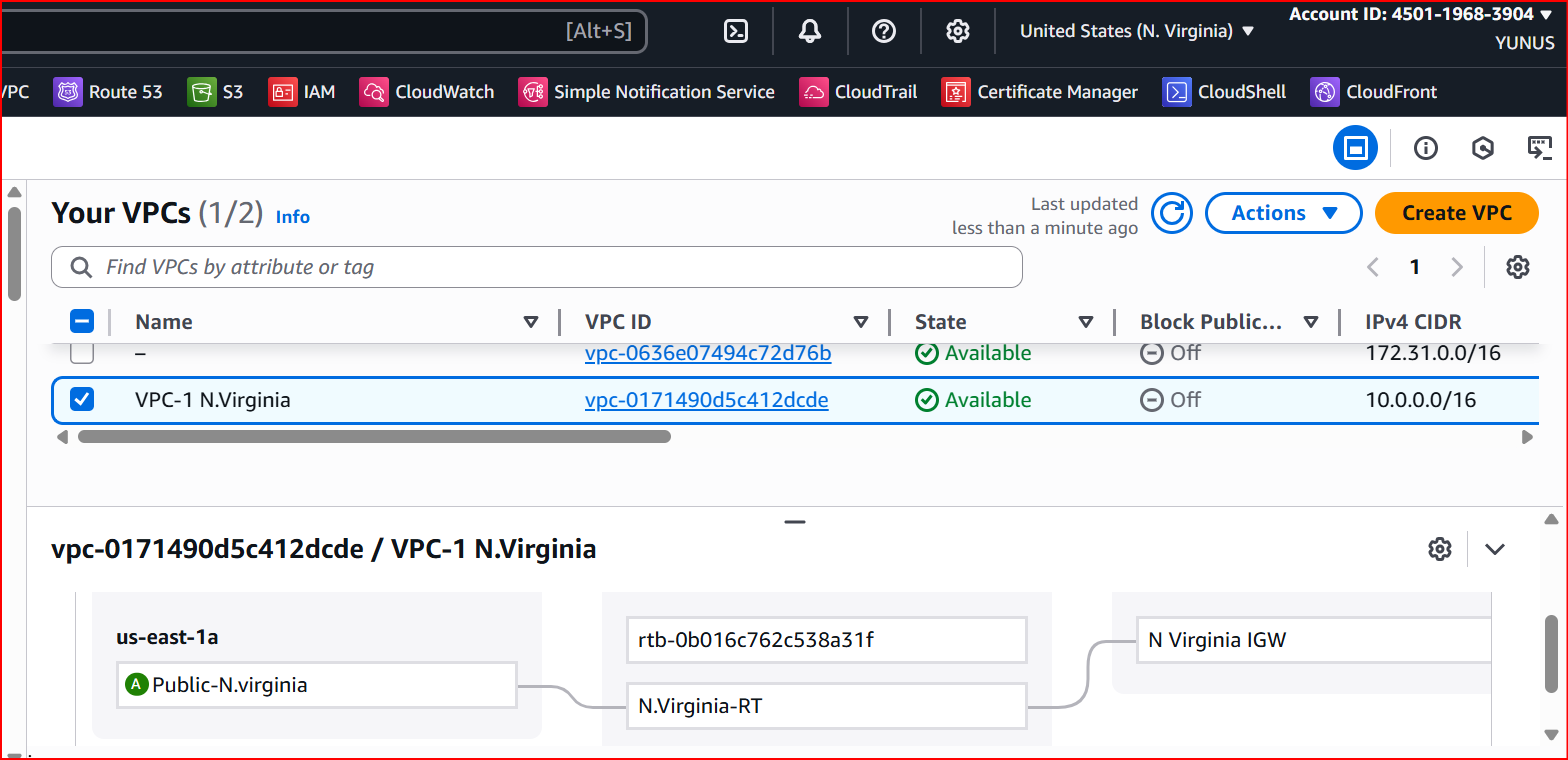
**Create 4 Private subnets in different regions**

**Route Tables:**

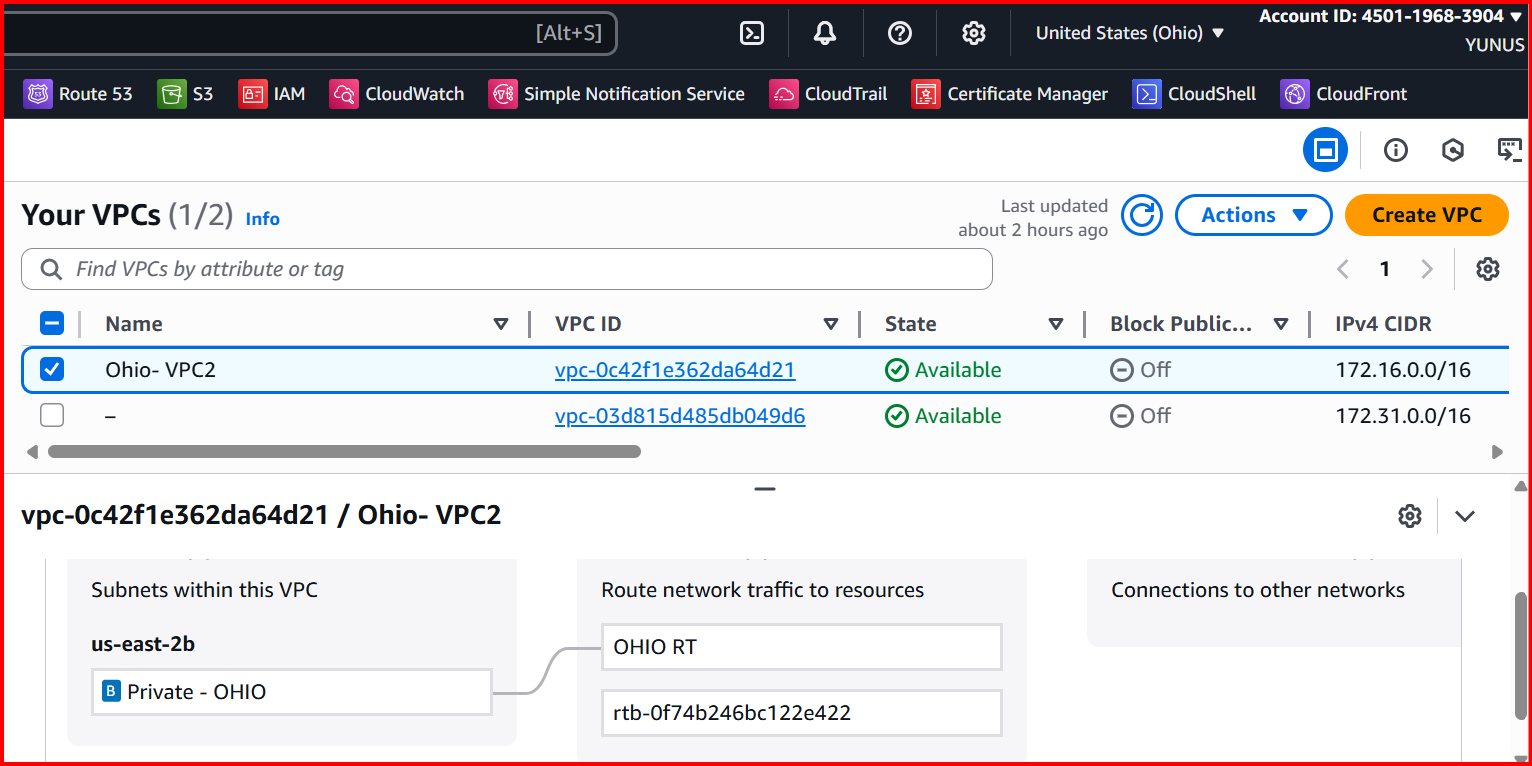
**Create a 4 Route Table for each set of subnets and associate them**

**Attached IGW to One VPC (N.Virginia)**

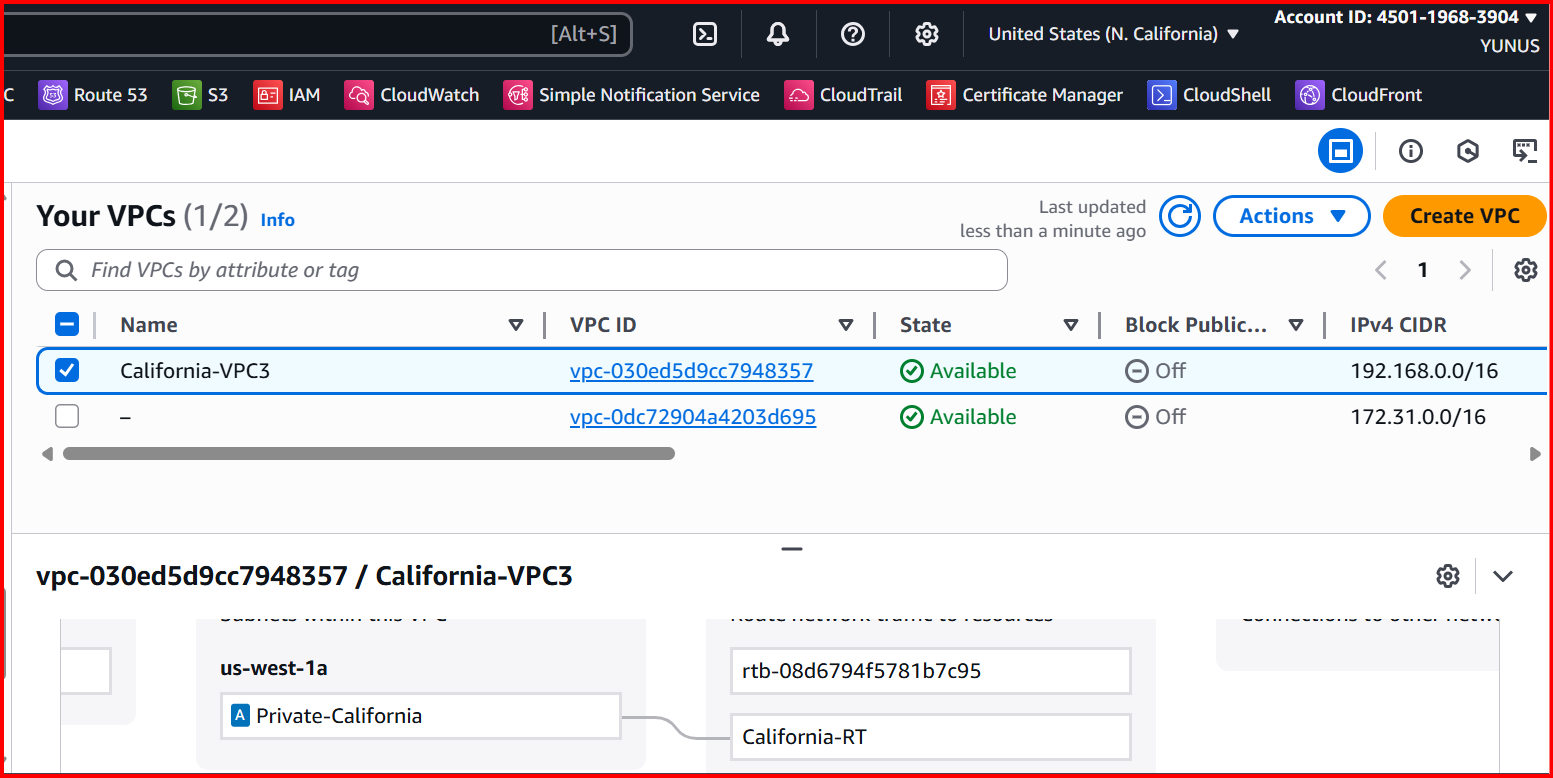
* 1. **VPC I have attached IGW**

****

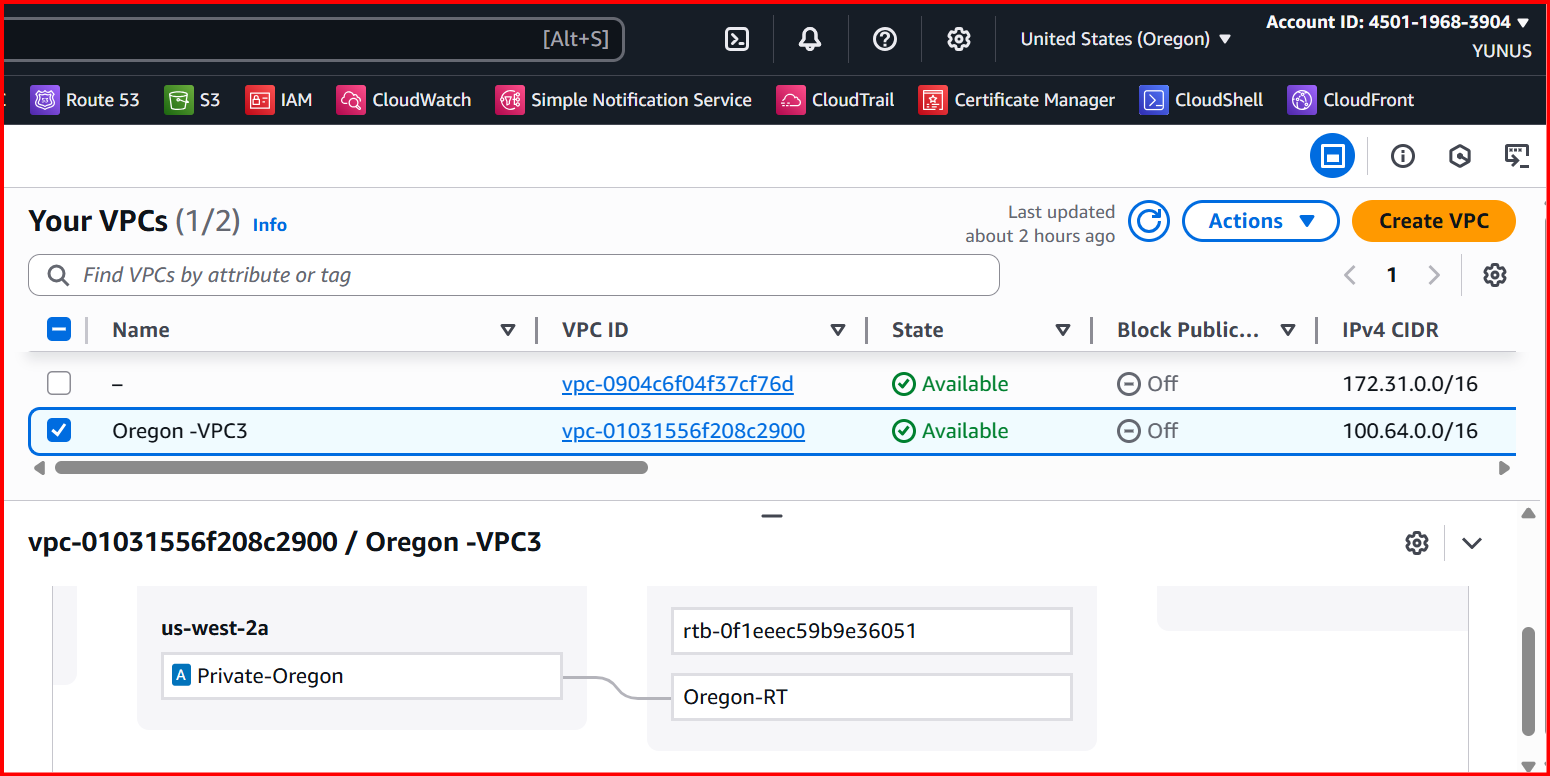
* 1. **VPC2 NO IGW**



* 1. **VPC3 NO IGW**

****

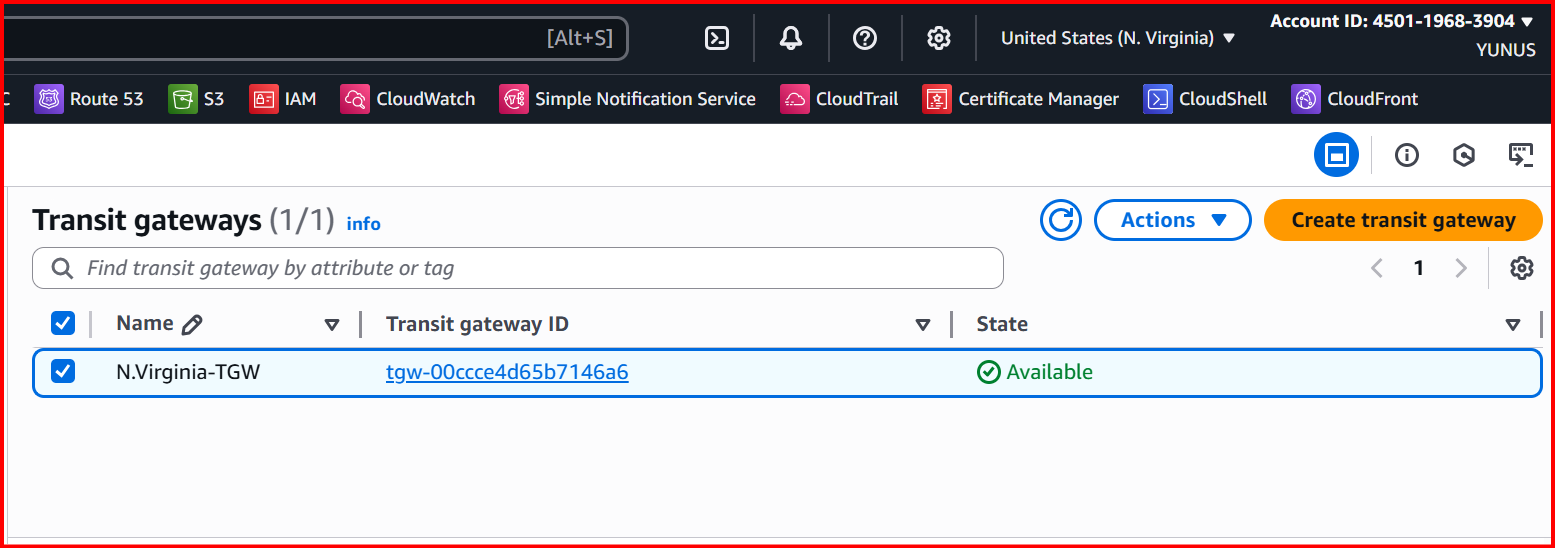
**4.VPC NO IGW**

****

**Step 3: Create Transit Gateways:**

**a. Create a Transit Gateway**

**VPC Console → Transit Gateways → Create transit gateway**

****

**b. Attach Each VPC to the Regional Transit Gateway**

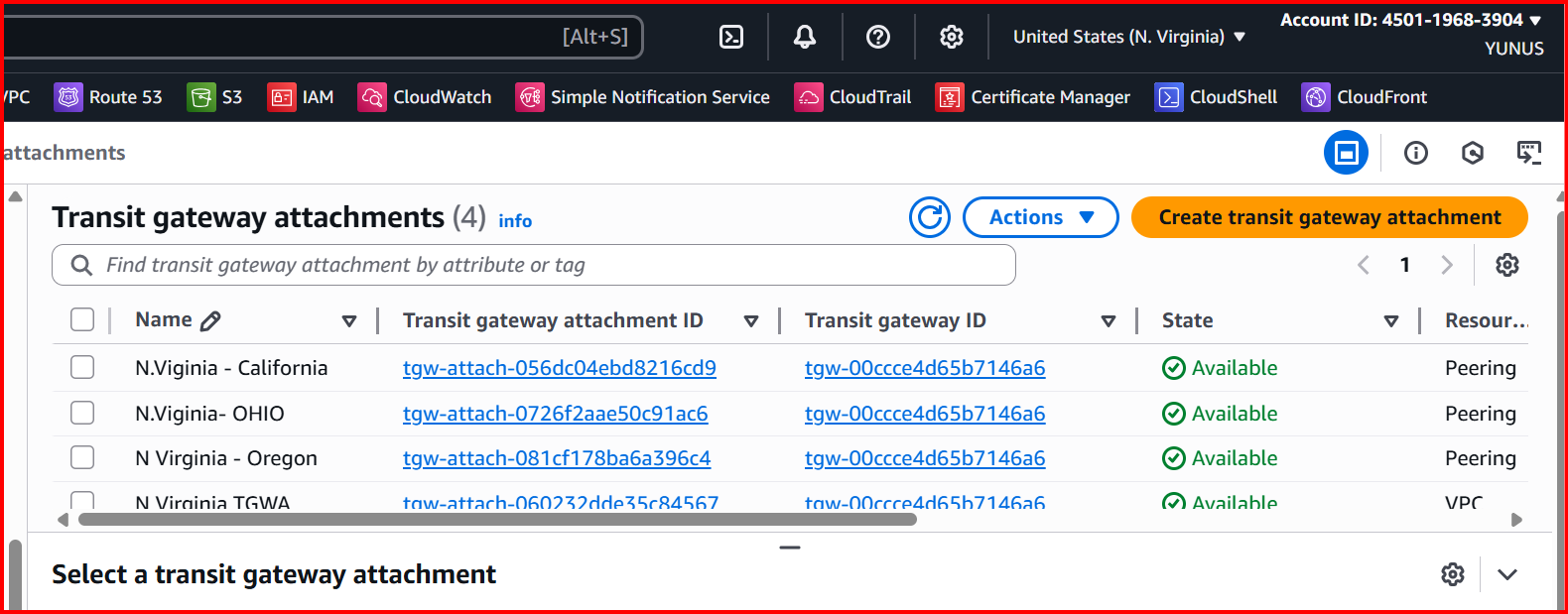
**Go to Transit Gateway Attachments → Create transit gateway attachment**

**Attachment type: VPC**

**Choose VPC: Select the regional VPC**

**Subnets: Select private subnets**

**Create attachment.**

****

**c. Associate VPC Attachment with TGW Route Table**

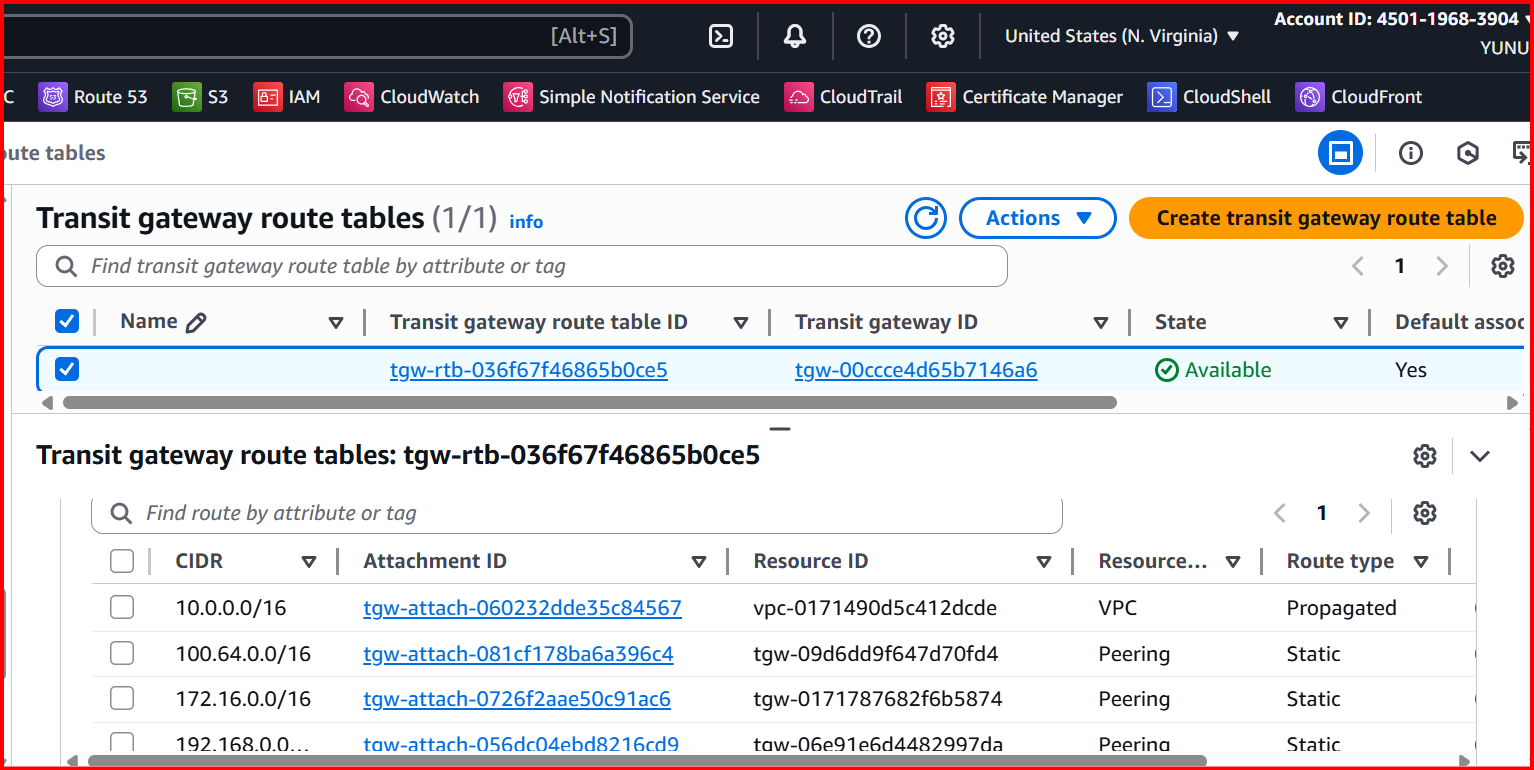
**Navigate: Transit Gateway Route Tables**

**Select TGW’s route table**

**Choose Associations → Create association**

**Pick the VPC attachment.**

**d. Update VPC Route Tables**

****

**Region A (Requester):**

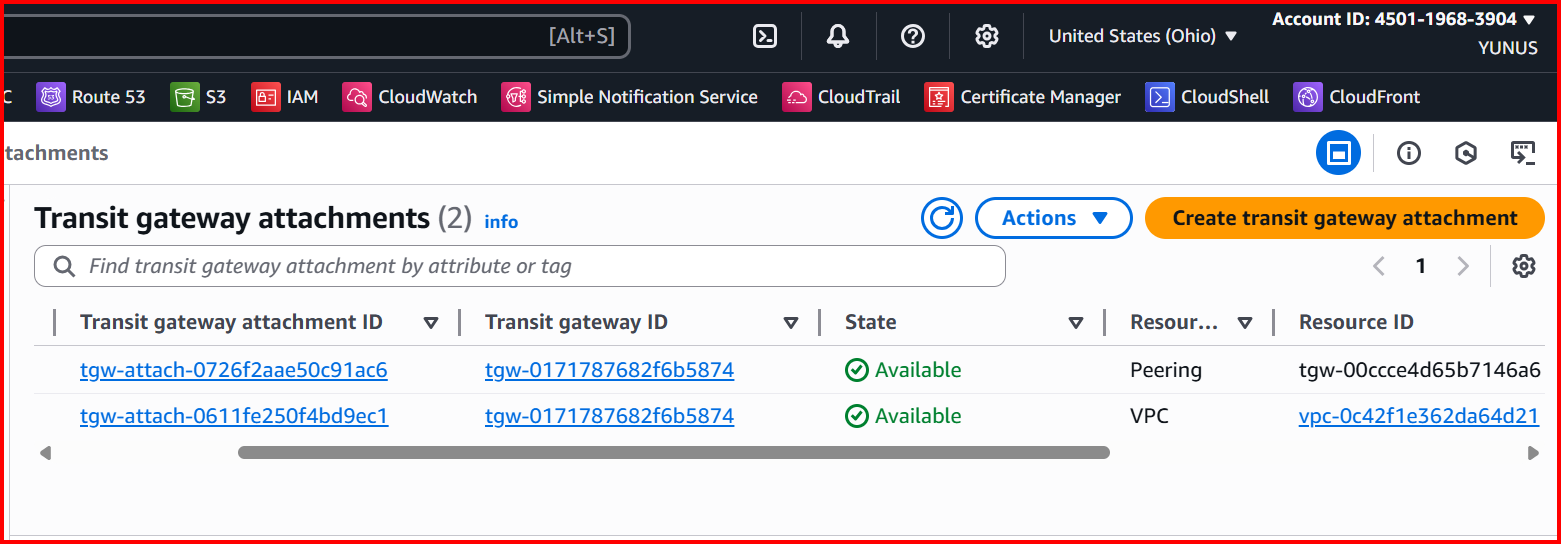
* **VPC Console → Transit Gateway Attachments → Create**
* **Type: Peering connection**
* **TGW ID: TGW-US-E1**
* **Target Region: us-west-2**
* **Peer TGW ID: TGW-Ohio**

**Region B (Accepter):**

* **VPC Console → Transit Gateway Attachments**
* **Accept the pending peering request.**

**Route Tables:**

* **Associate the peering attachment with TGW route tables in both regions.**
* **Enable route propagation (or add static routes).**

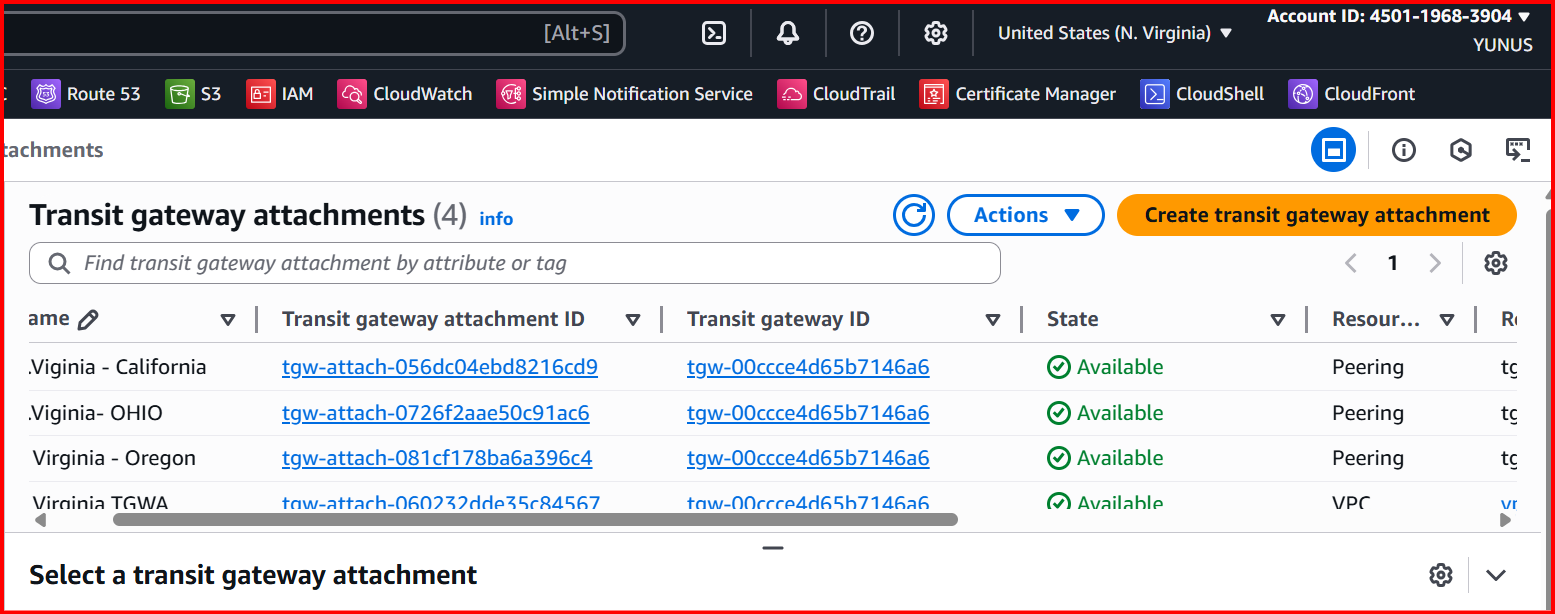
****

**Check the Peering**

**Accept Peering Attachment (Accepter Side)**

1. **Switch to the peer region’s console (e.g.,Ohio-region).**
2. **Go to Transit Gateway Attachments.**
3. **You’ll see a pending peering request.**
4. **Select it → Actions → Accept.**

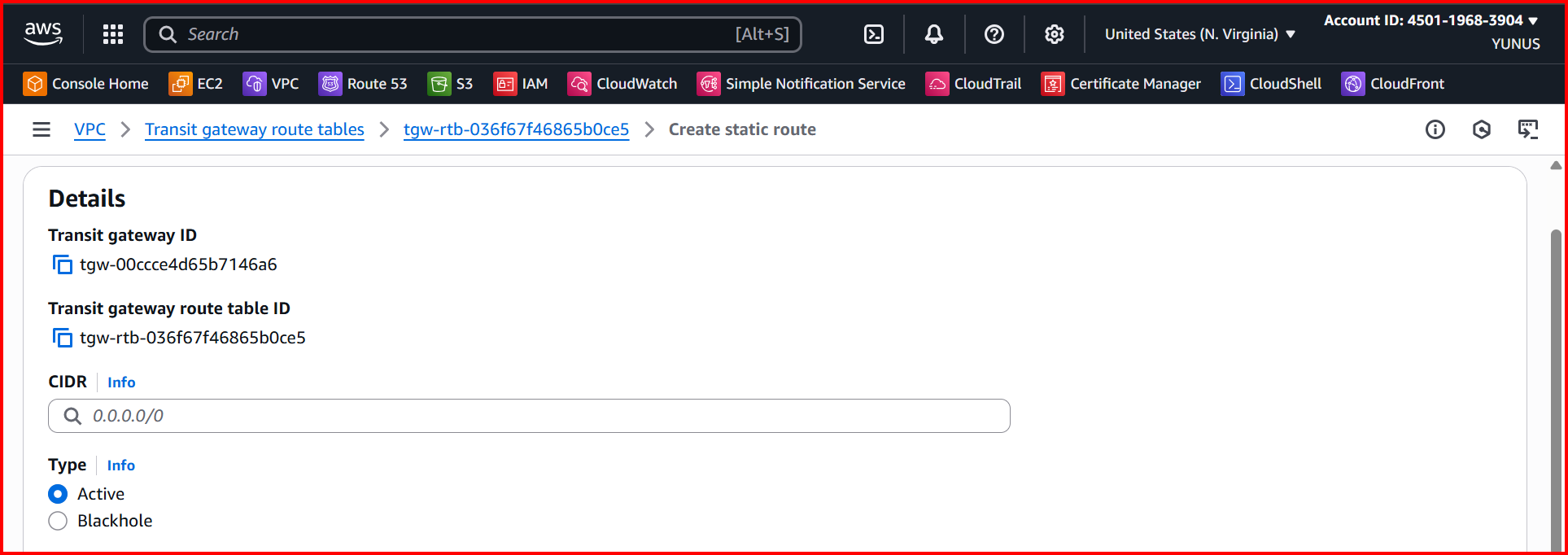
* **Similarly configure with the vpc3 and vpc4 and**
* **also configure the same with all the Regions with one to all**

****

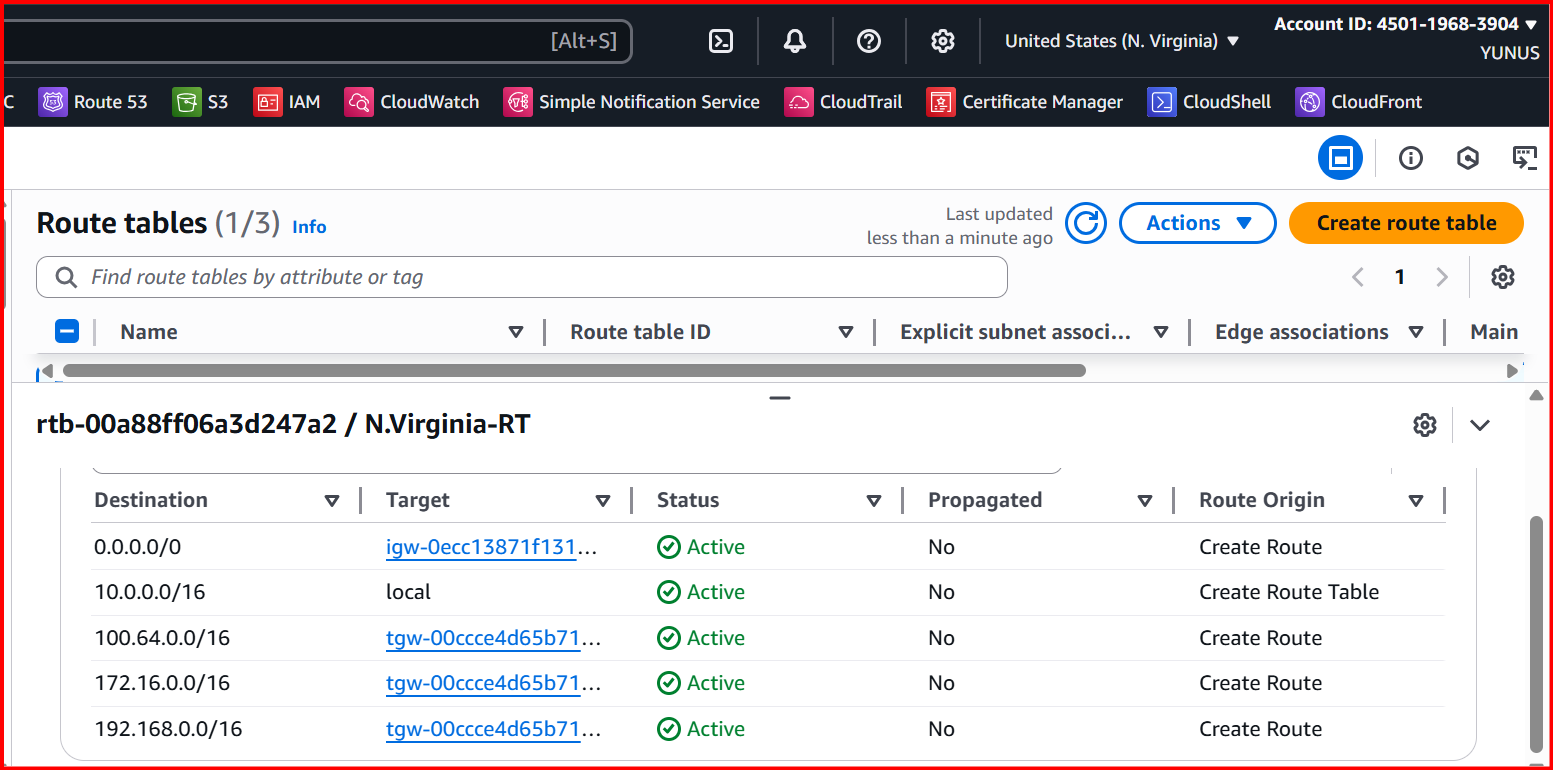
**Configure TGW Route Tables**

* **After the peering is active, you must update TGW route tables so traffic can flow.**

1. **In each TGW’s Route Table, add routes for the remote VPC CIDRs.**

****

**Update VPC Route Tables in all regions**

****

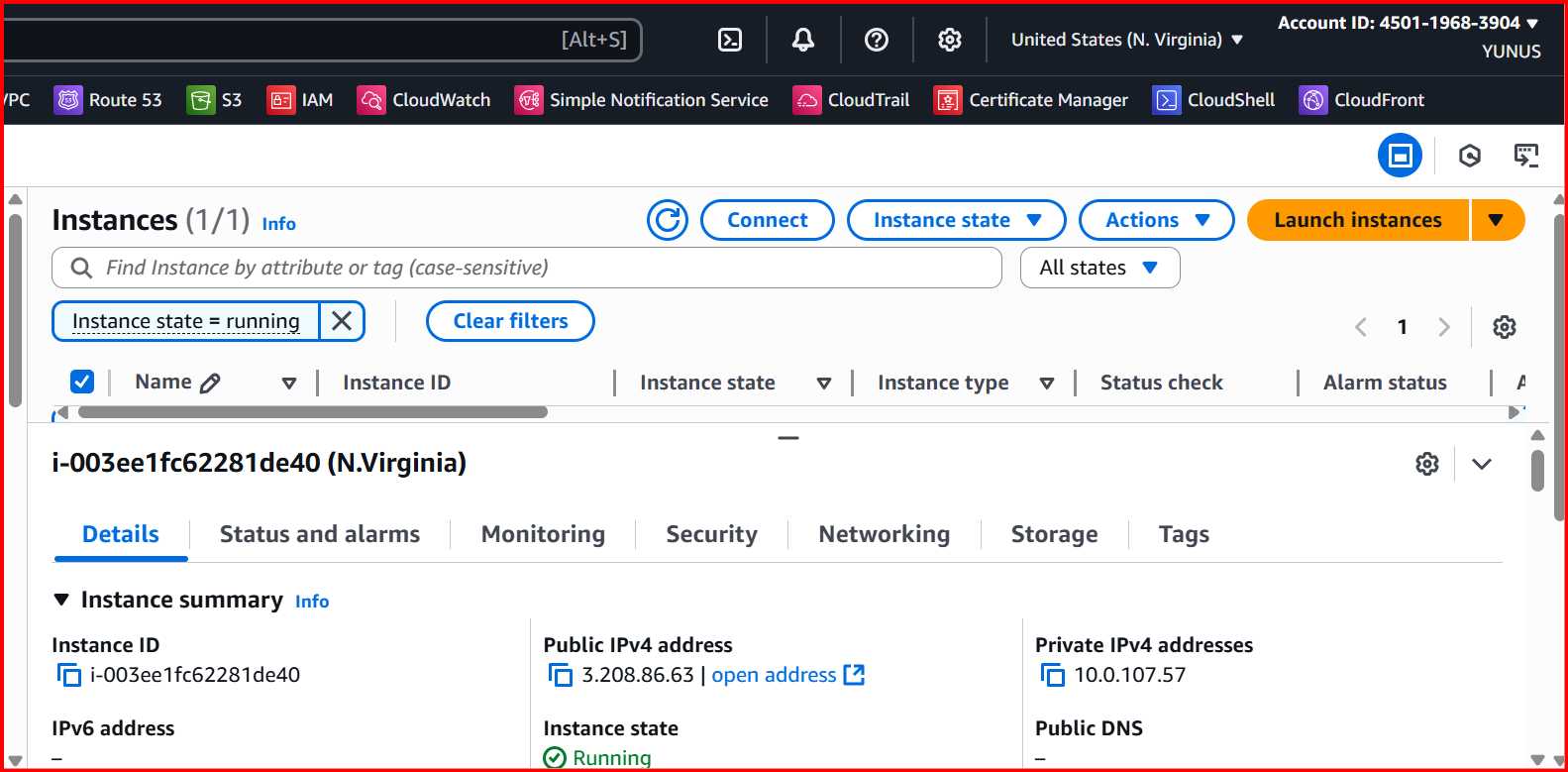
**Create 4 Instance in different regions**

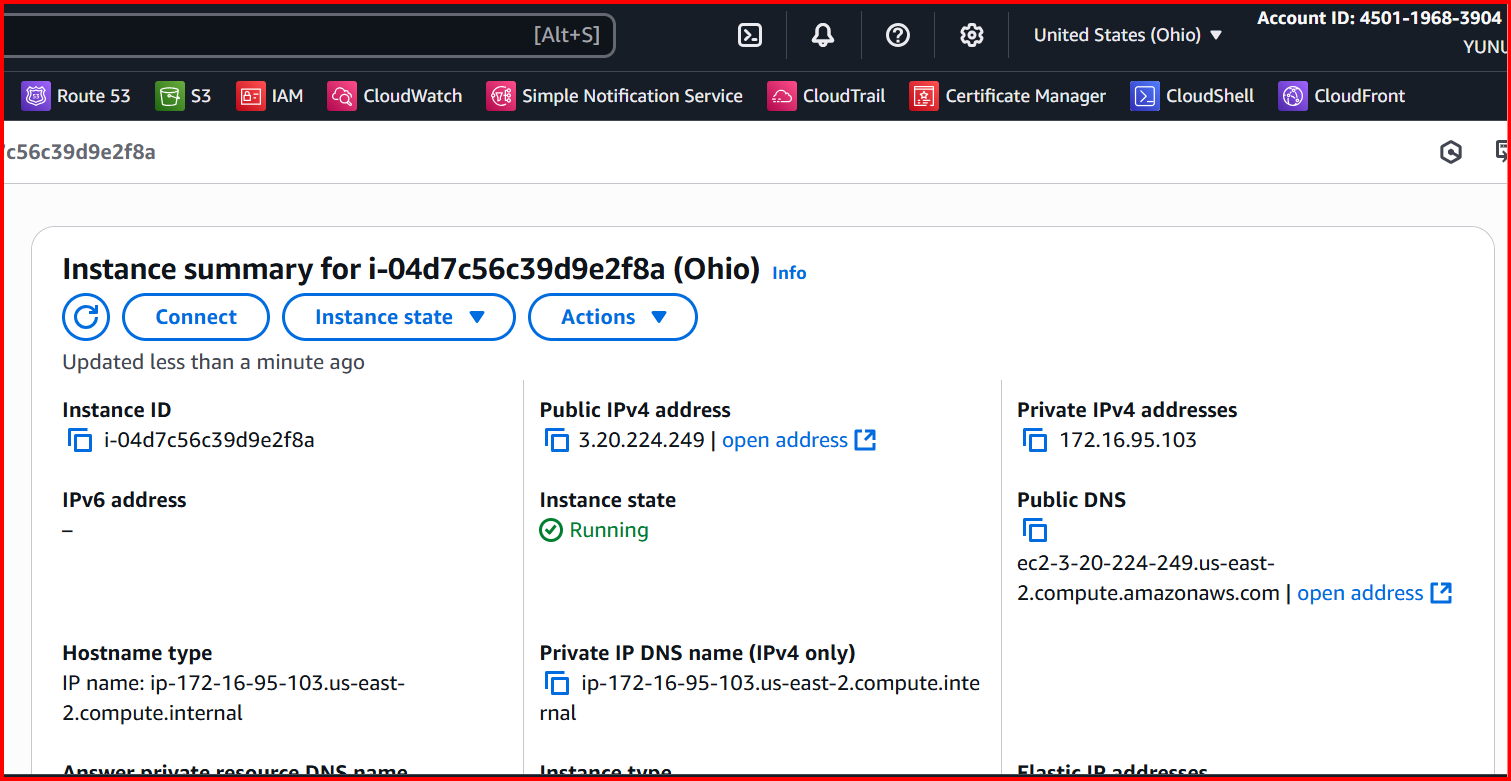
**EC2 connectivity:**

**Launch 1 EC2 in each VPC in public subnet- - Vpc-1-( N.Virginia)**

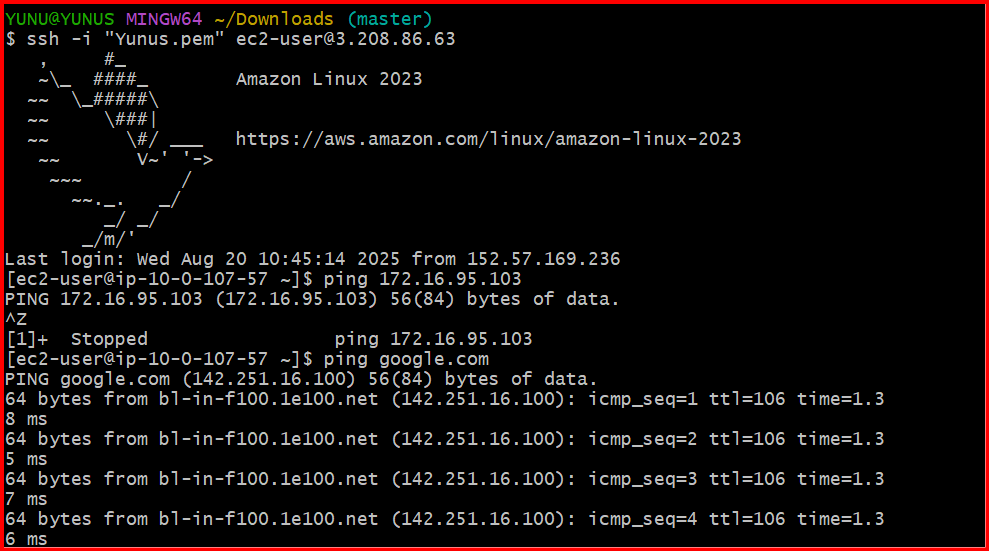
**Remaining all Launch 1 EC2 in each VPC private subnet.**

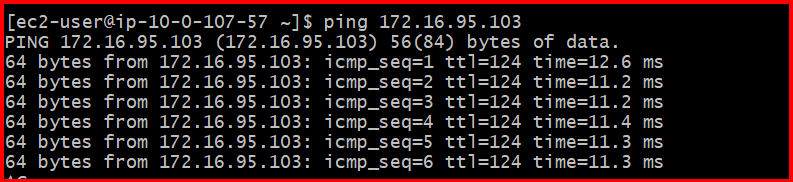
**From Virginia EC2 → ping Ohio EC2’s private IP.**

****

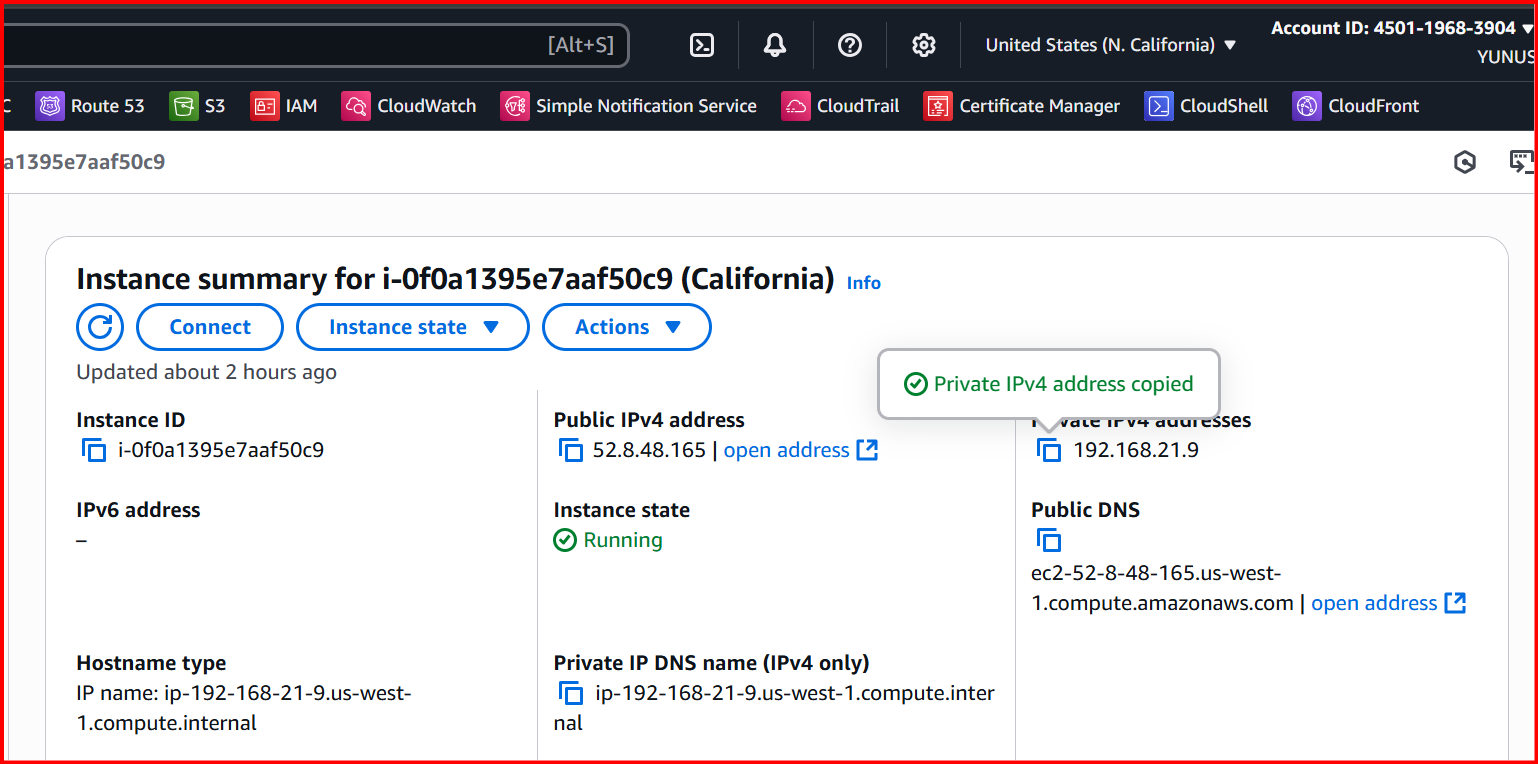
****

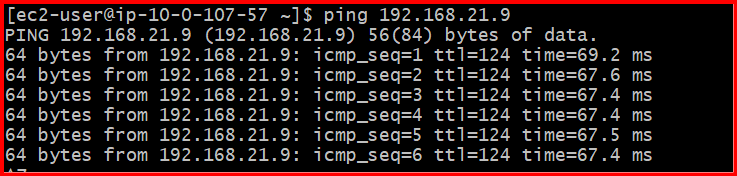
**Ping Virginia to Ohio**

****

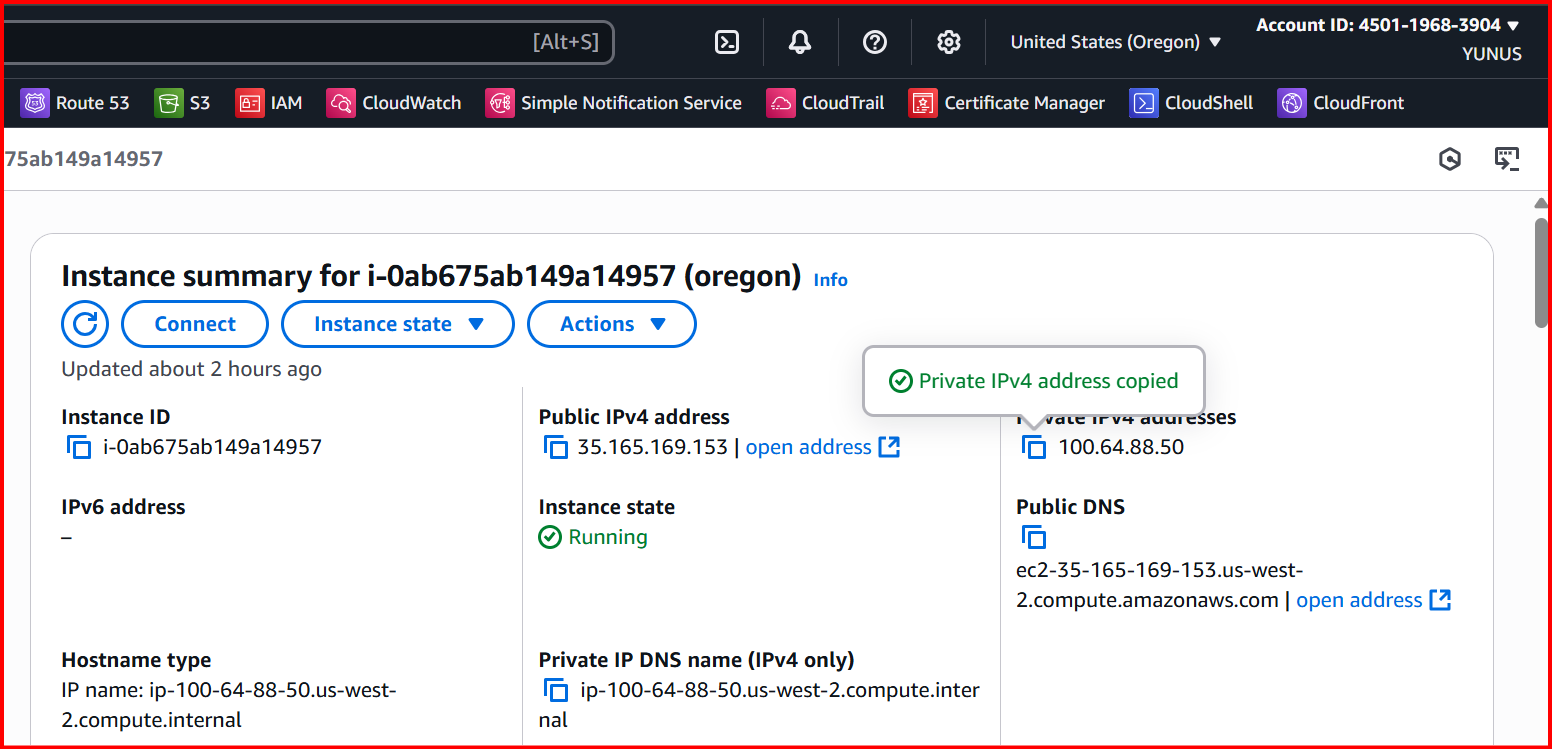
****

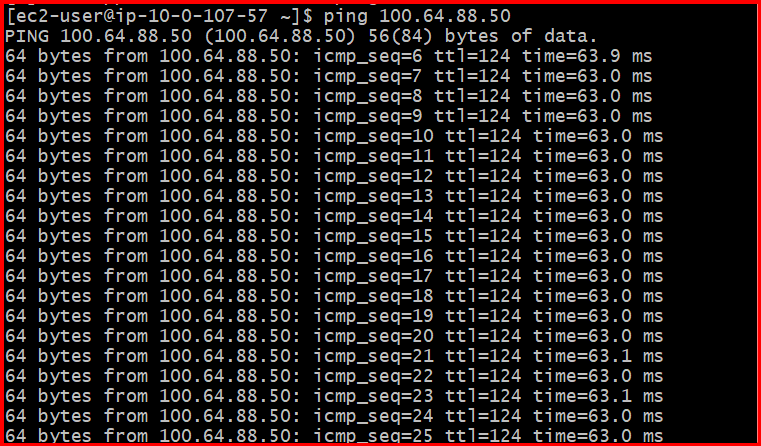
**Ping Virginia to California**

****

****

**Ping Virginia to Oregon**

****

****

**Configure VPC endpoints to securely access AWS services without internet gateways or NAT gateways, ensuring data privacy and minimizing exposure to external threats.**

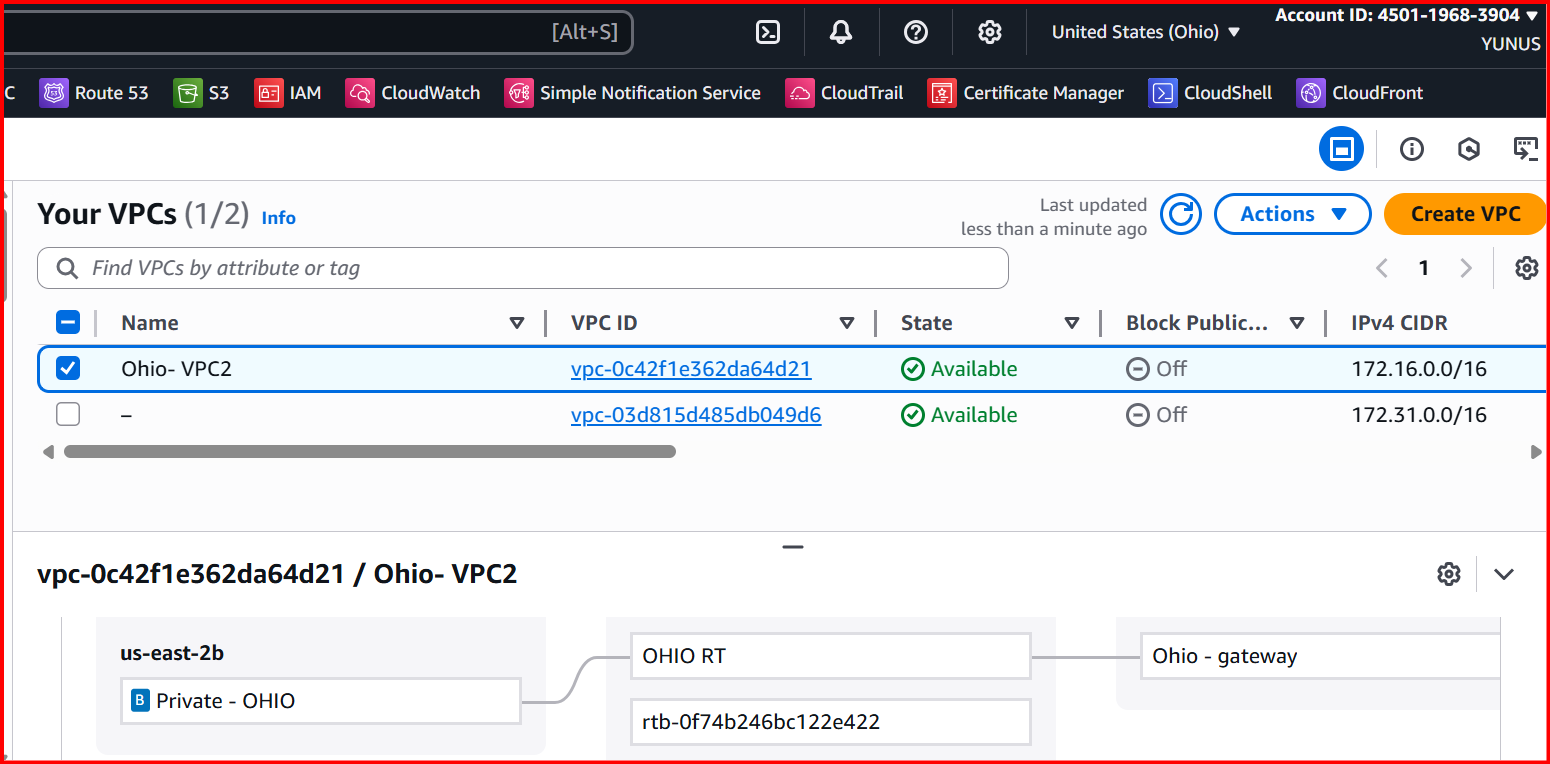
**Configure VPC Endpoints (Private access to AWS services)**

**For each VPC → Go to Endpoints → Create Endpoint.**

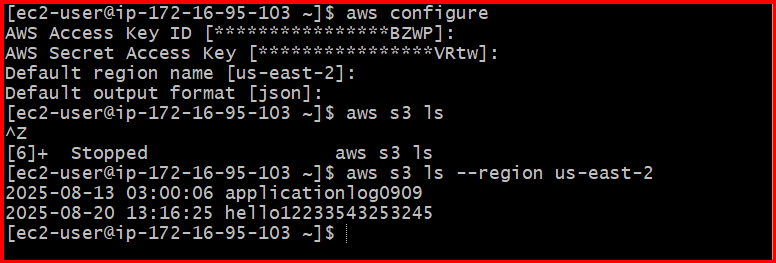
**Choose services:**

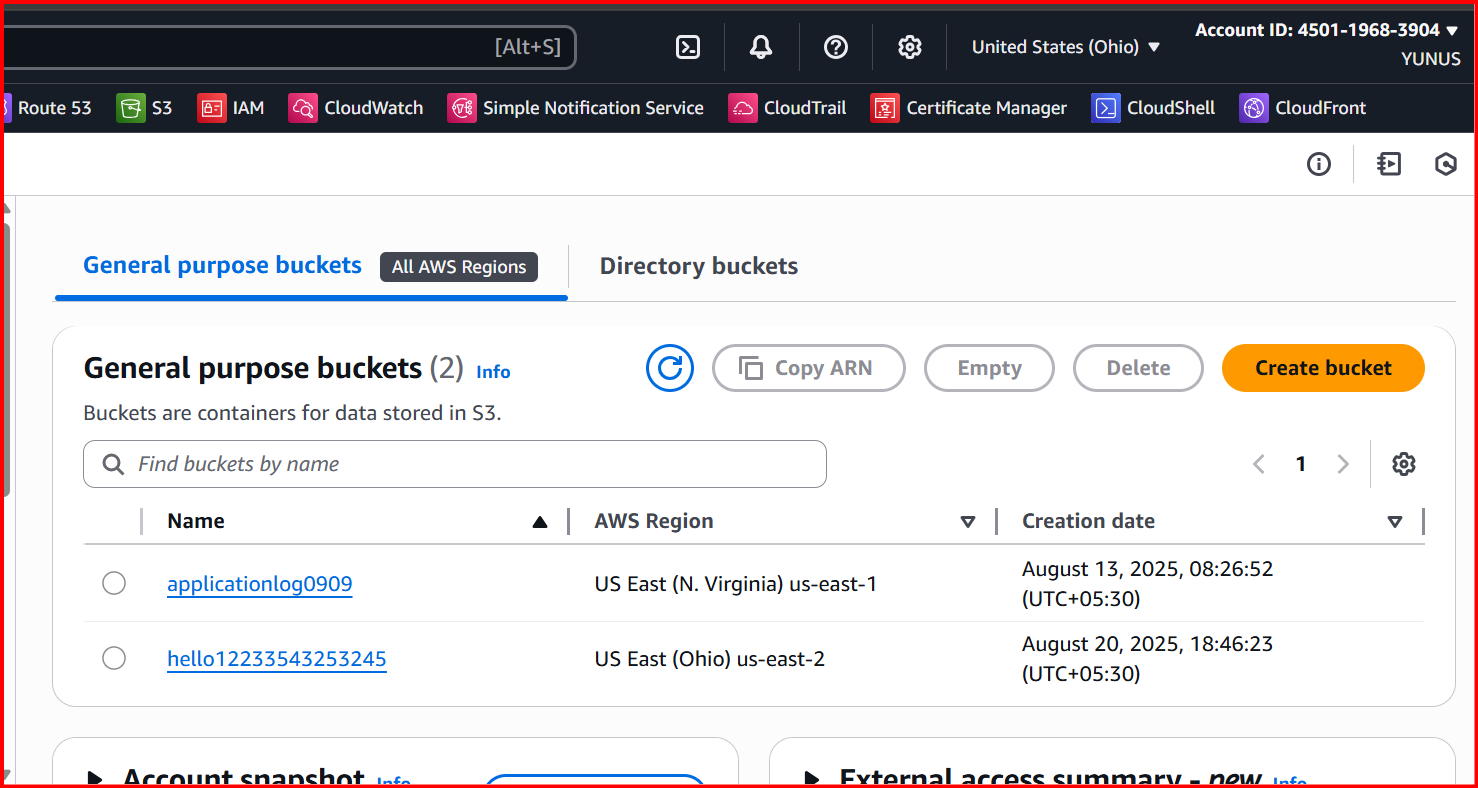
* **Gateway Endpoint: S3**

**Create an S3 endpoint in Ohio**

****

**Aws configure**

****

****

**Simlarly Configure in Other regions and Verify.**