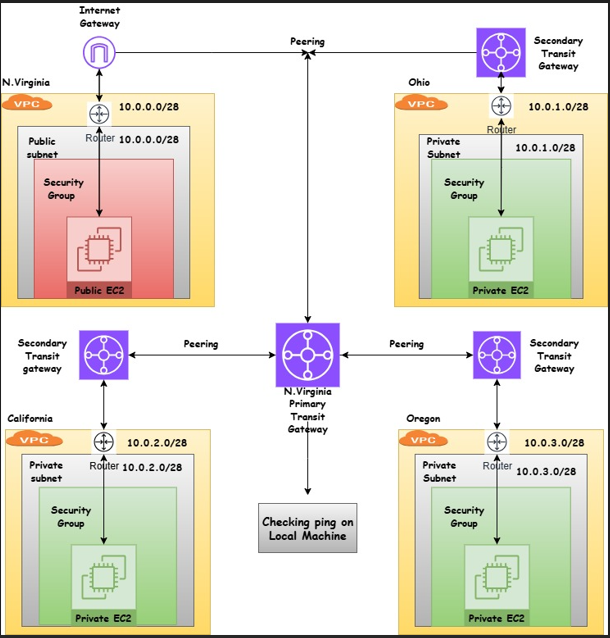
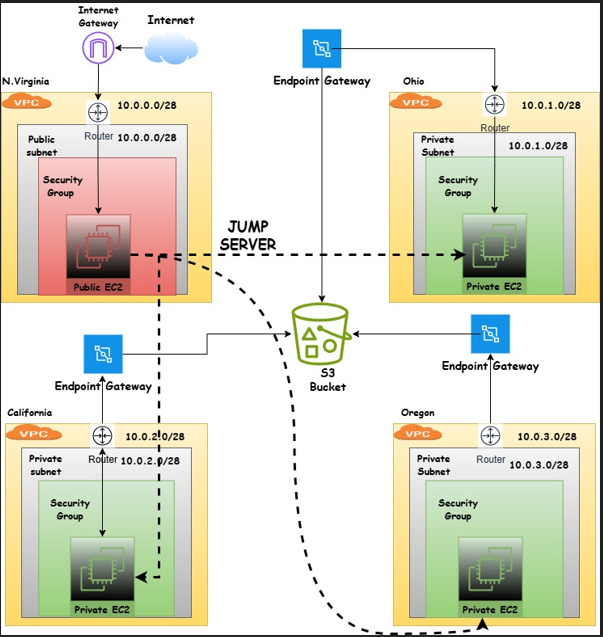
**Use Case: Setting up Transit Gateway and VPC Endpoints for a Multi-VPC Architecture**  
**Scenario:**  
 A large organization is migrating its on-premises infrastructure to the AWS cloud.  
 The organization's architecture involves multiple VPCs for different departments and applications, each requiring 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.

Prepare a document with all the screenshots and push it to a GitHub repo, then share the UR

* **Go to AWS console and select VPC in 4 regions**
* **Create 4 VPC in 4 regions**
* **CIDR range allocation for 4 VPC**

**Primary-1**

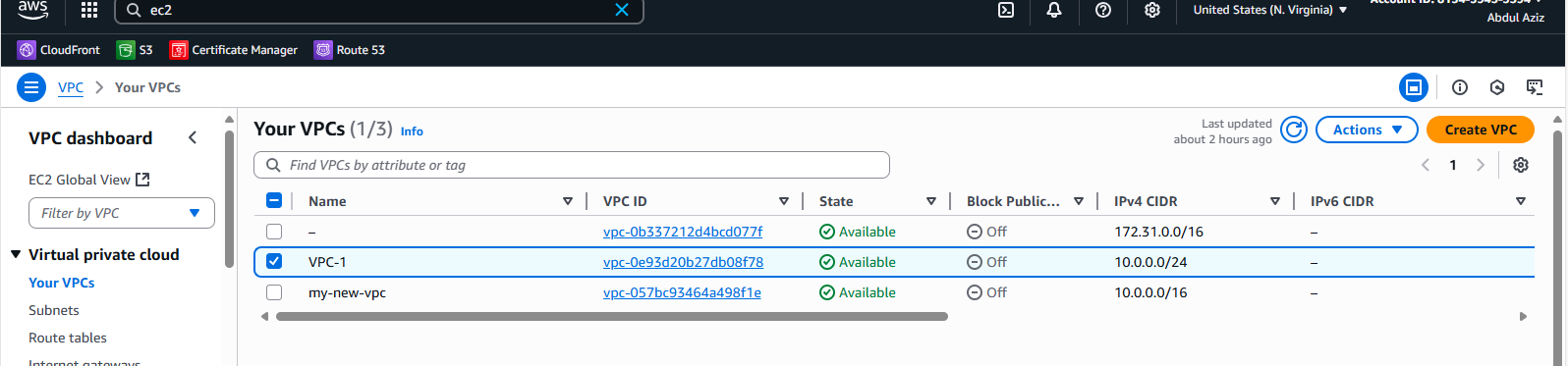
* Vpc1-us-east-1(10.0.0.0/28) & Pub-sub-(10.0.0.0/28)

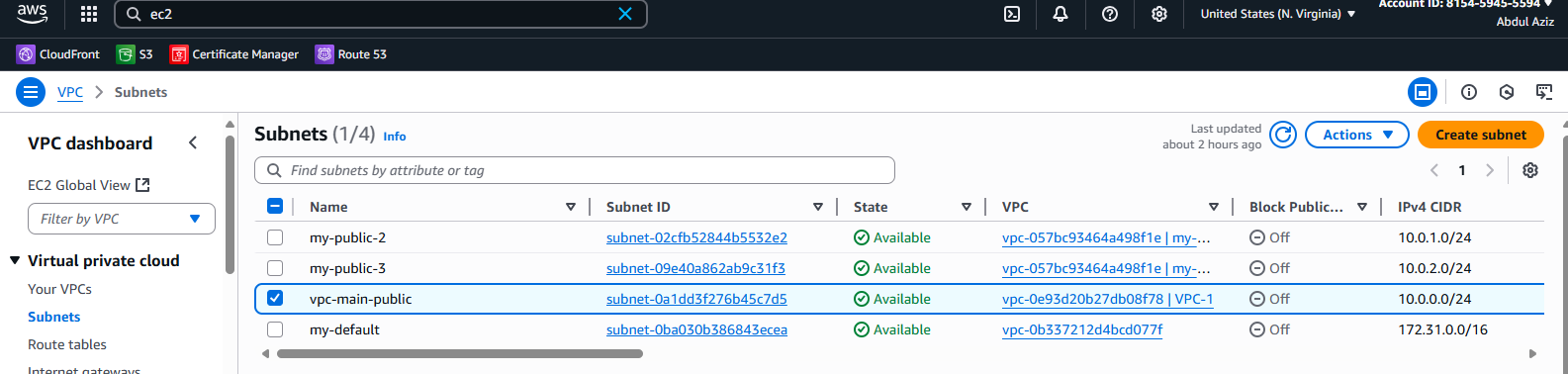
**Secondary-3**

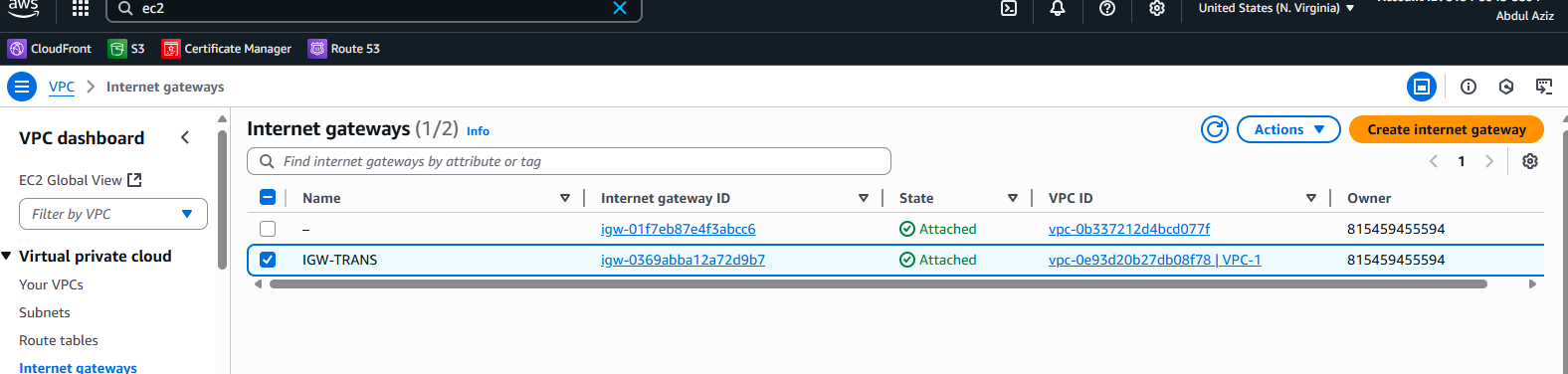
* Vpc2-us-east-2(10.0.1.0/28) & Pri-sub-(10.0.1.0/28)
* Vpc3-us-west-1(10.0.2.0/28) & pri-sub-(10.0.2.0/28)
* Vpc4-us-west-2(10.0.3.0/28) & Pri-sub-(10.0.3.0/28)

**Creating Primary VPC**

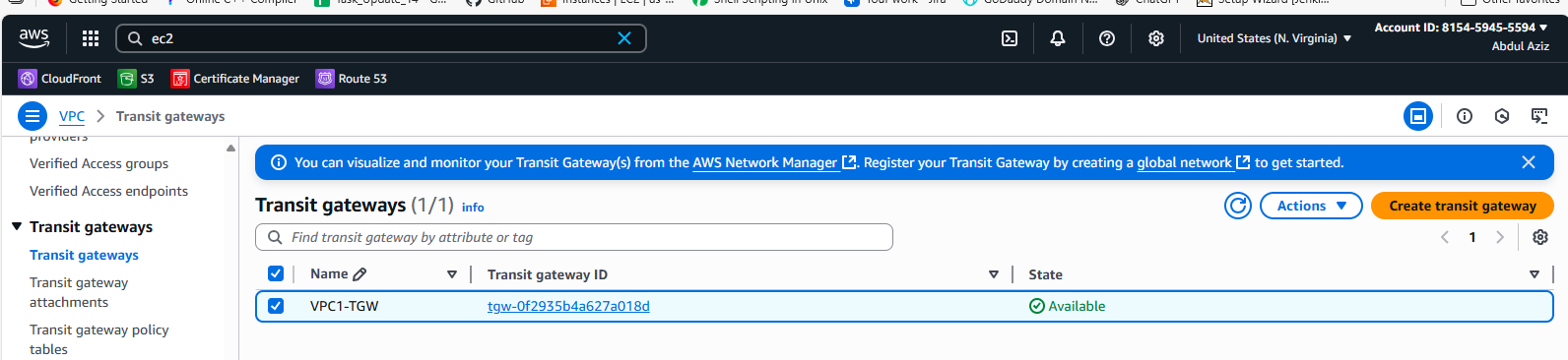
* **Vpc-us-east-1(10.0.0.1/16)**Go to vpc and create 1 vpc in us-east-1
* After Creating vpc1 ,create one subnet and attach internet gateway
* Attach Route table to vpc1 and associate subnet

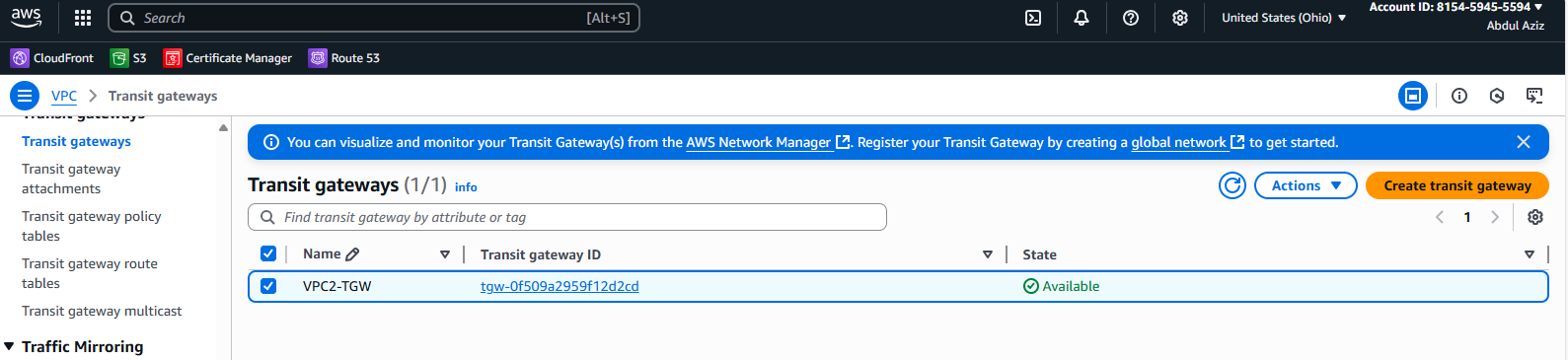
****

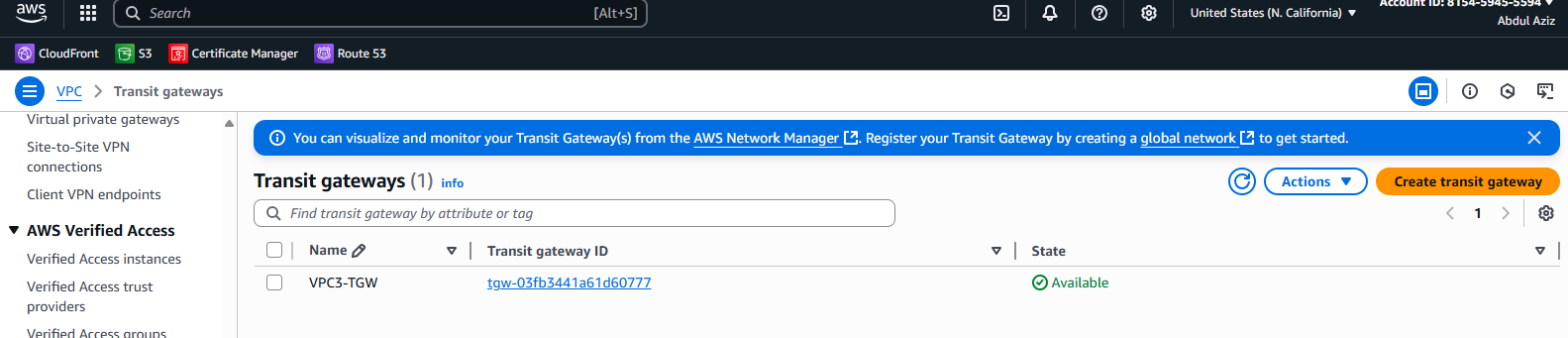
****

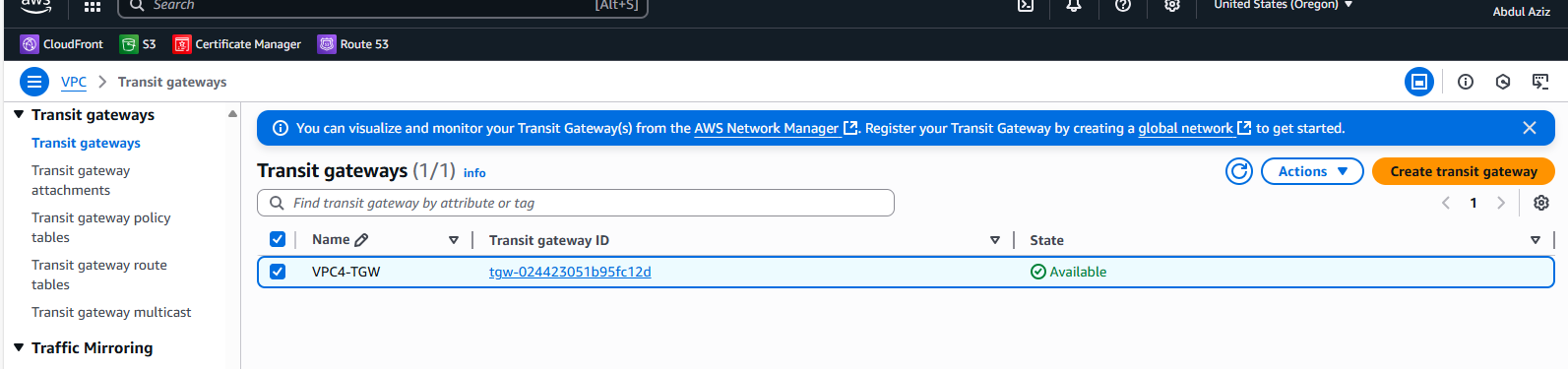
****

* Create vpc2 in other region
* Create subnets and do not attach IGW to these vpc2, vpc3 and vpc4
* Associate Route table to private subnets
* Similarly, follow the steps for vpc3 & 4 same as vpc2 in other regions.
* After all VPC’s are created then start to create separate Transit gateway for each VPC.

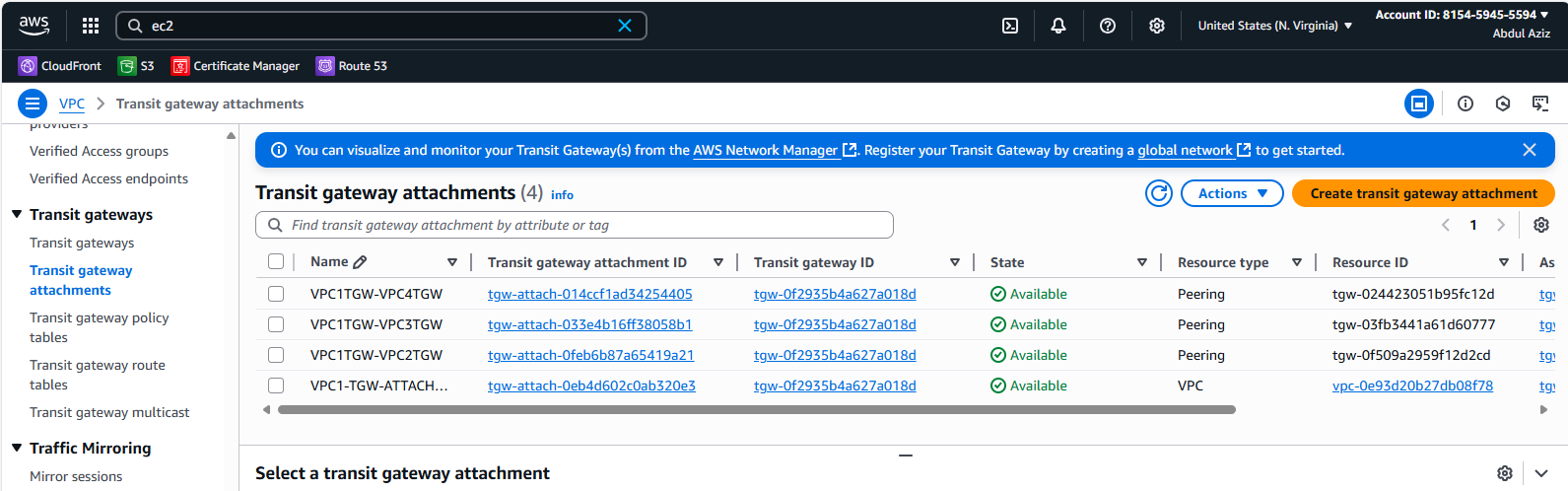
****

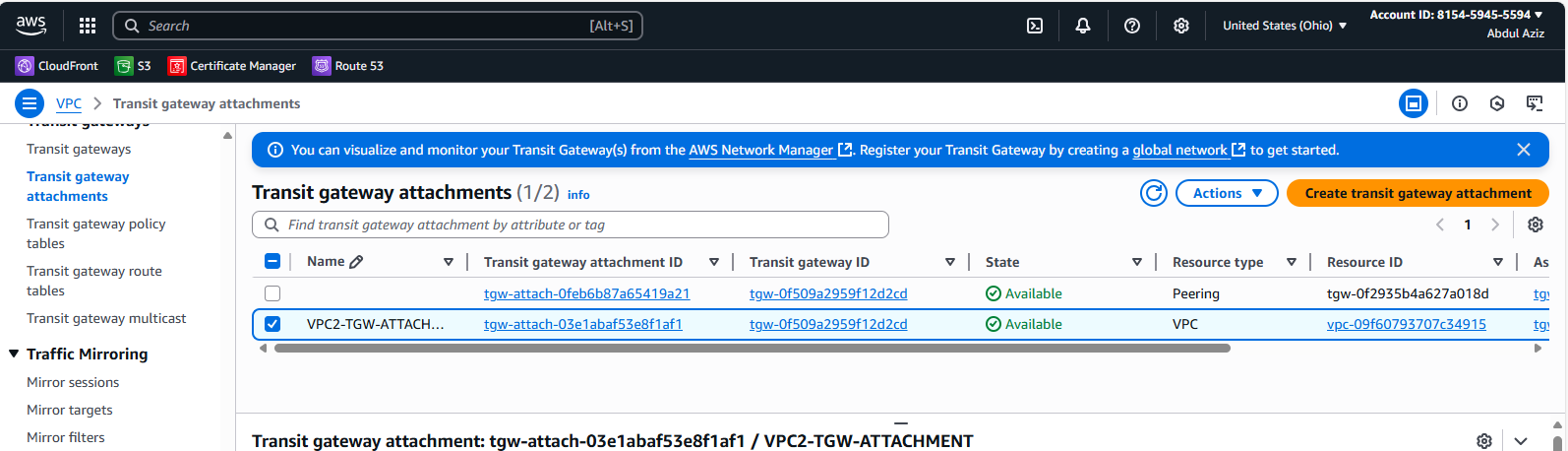
****

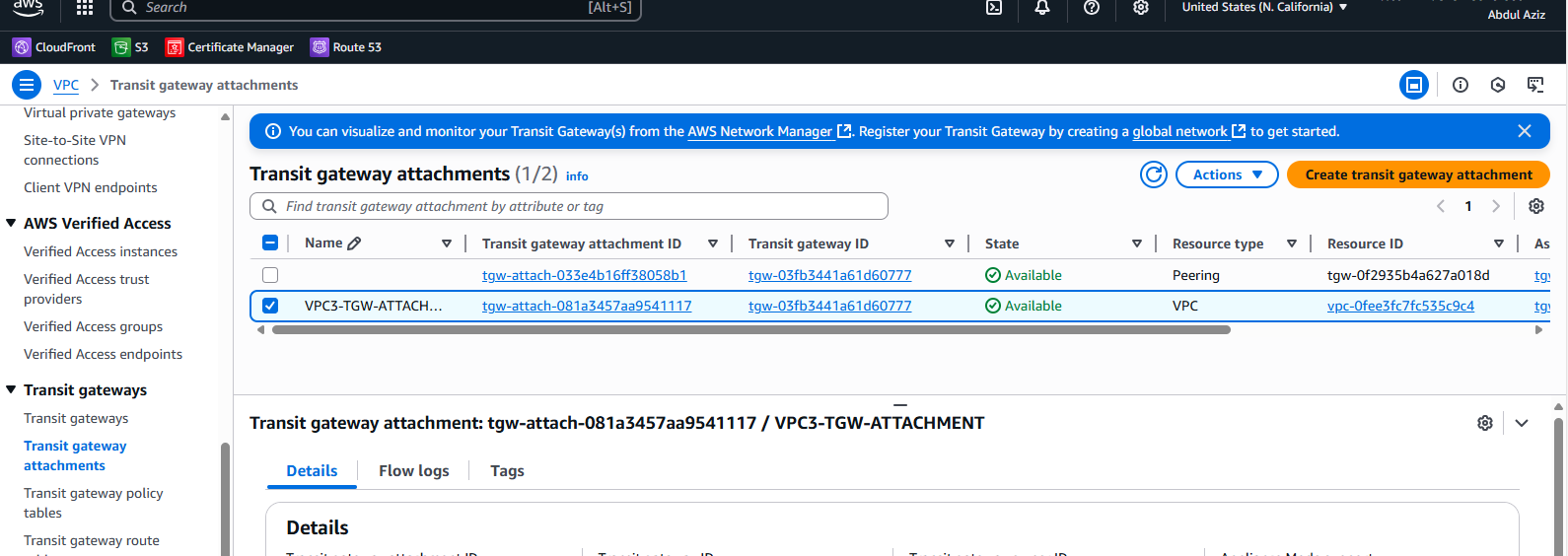
****

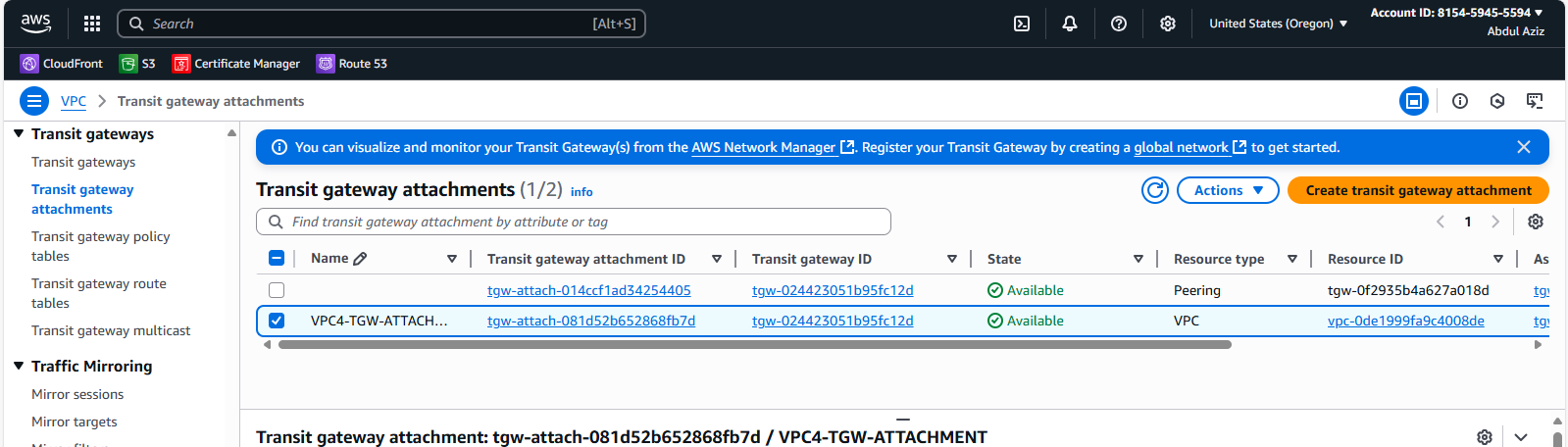
****

* Create transit gateway attachment peering for vpc1,vpc2,vpc3 and vpc4 i.e in 4 different regions.

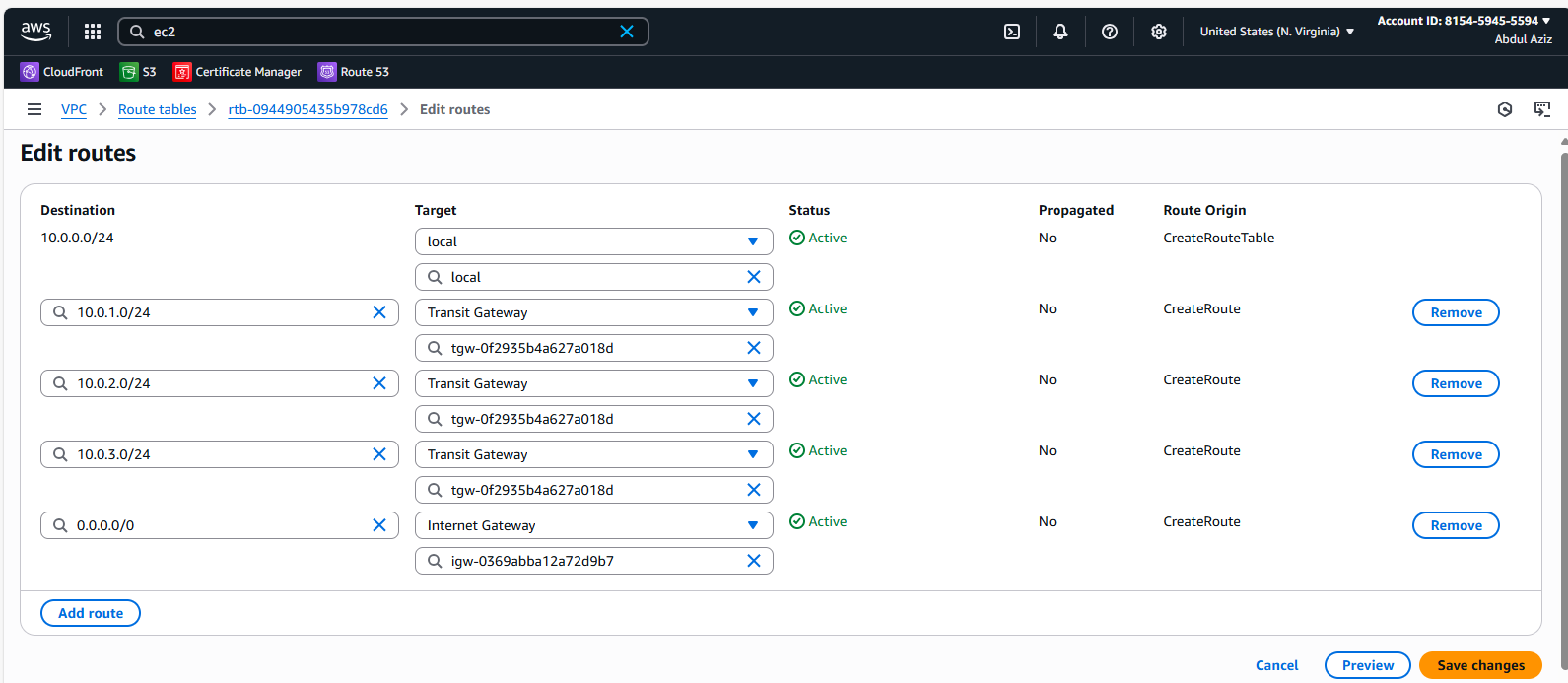








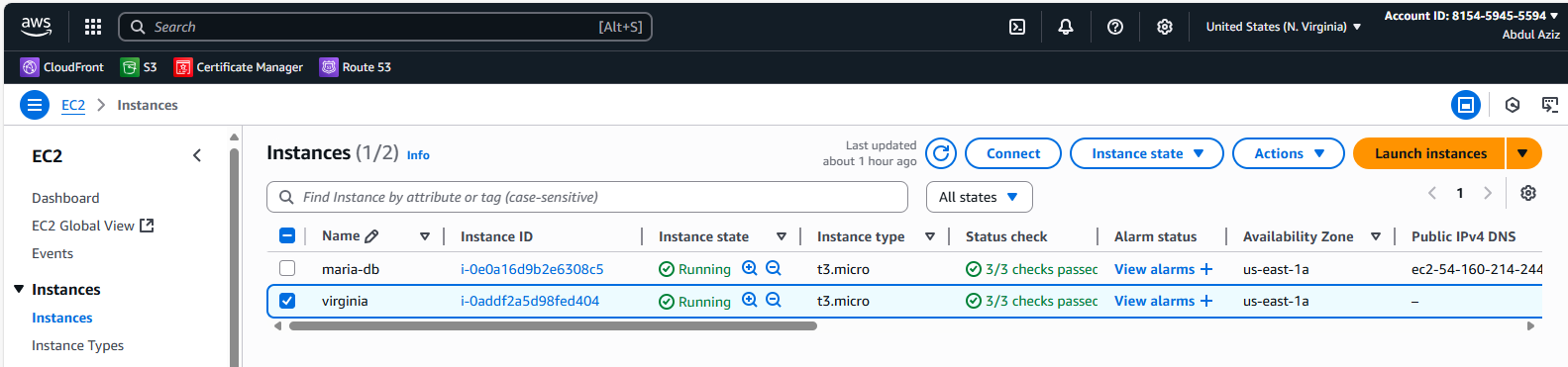
* In vpc route table attach vpc1, vpc2 ,vpc3 and vpc4 TGW with CIDR range.

****

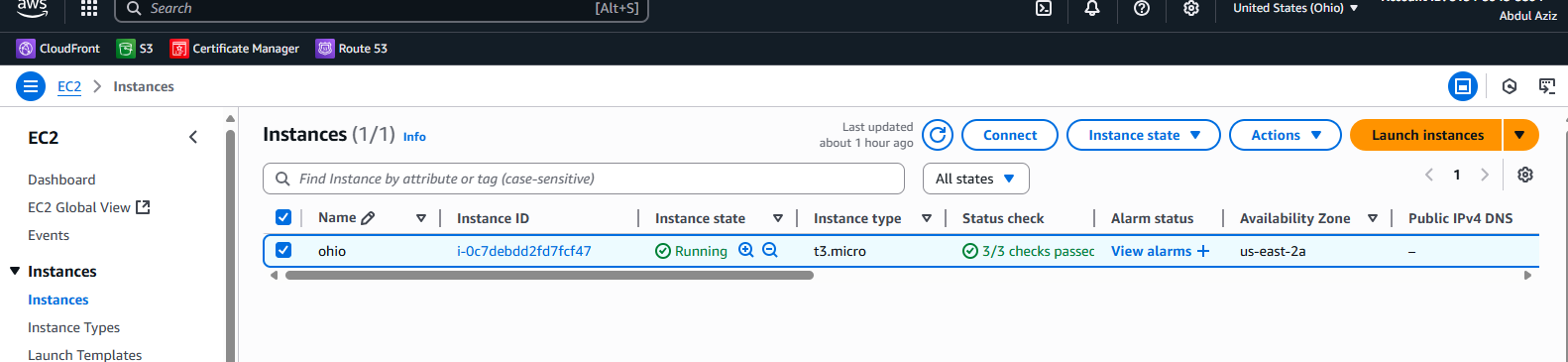
**Same as above in remaining 3 vpc’s**

* Now lunch 4 instances in 4 different regions.
* In primary instance enables the public and all secondary instances disable the public.

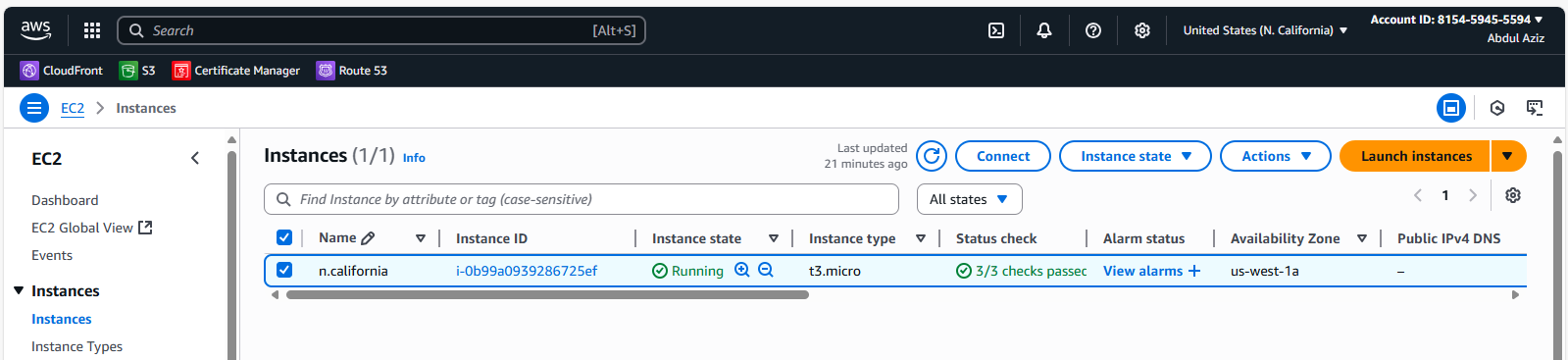
**Virginia region**

****

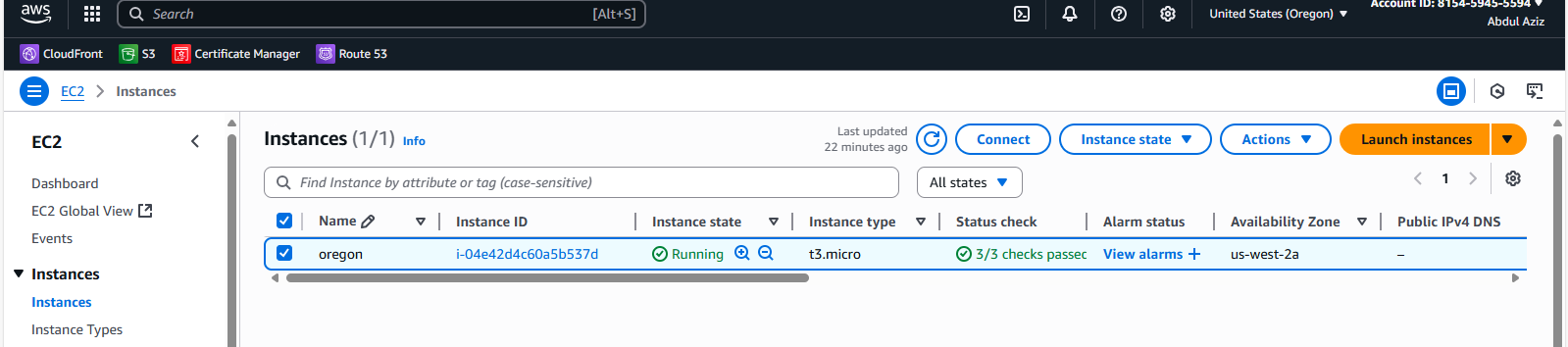
**Ohio region**

****

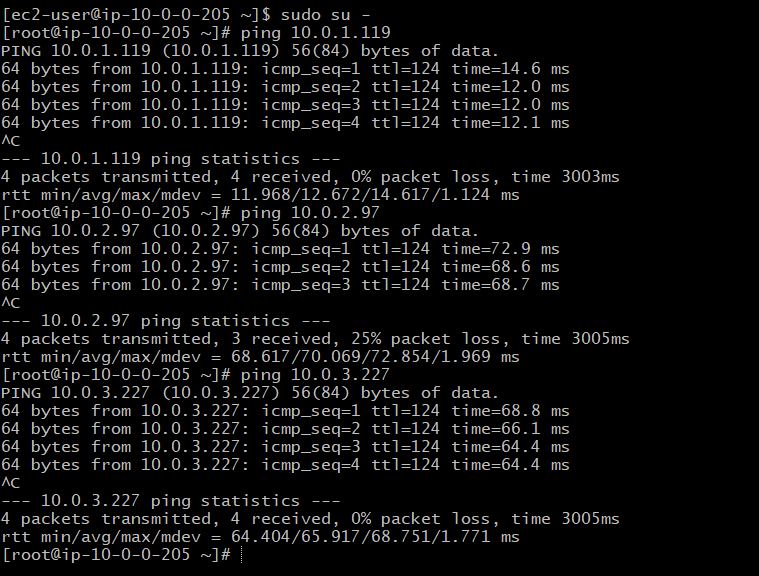
**California region**

****

**Oregon region**

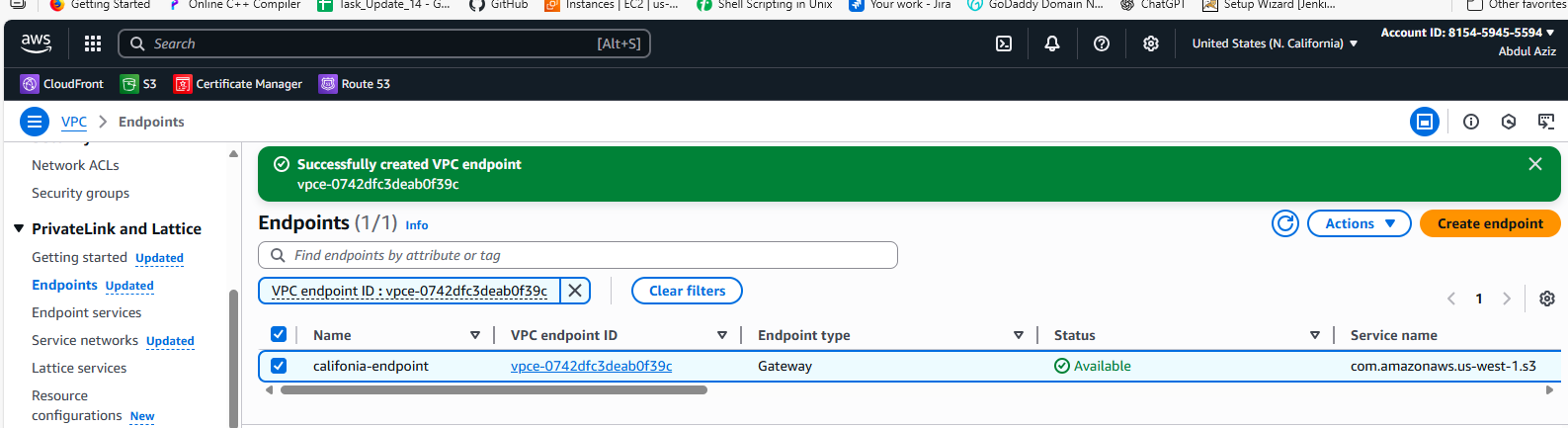
****

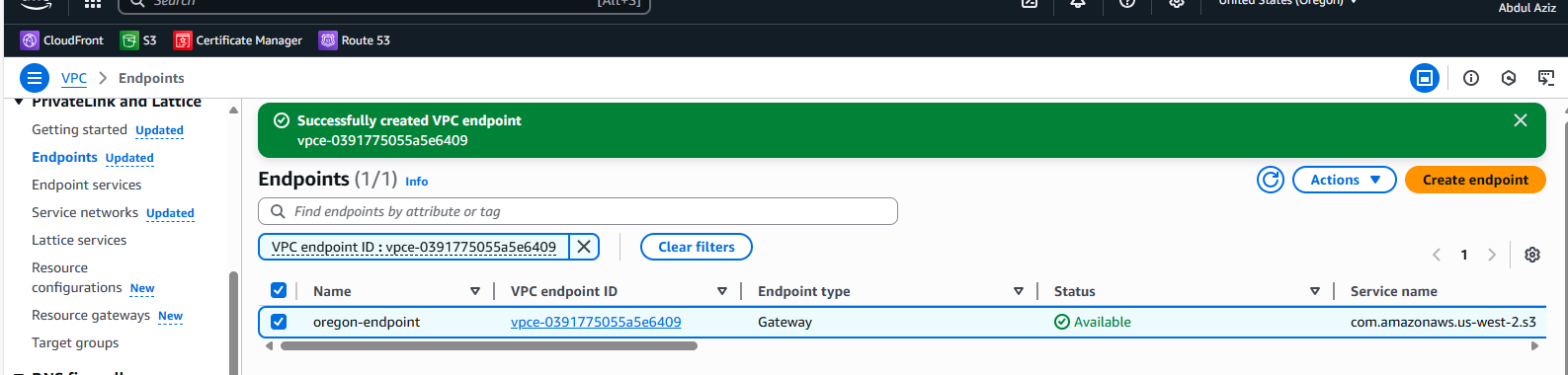
**Now we will ping the private ip address.**

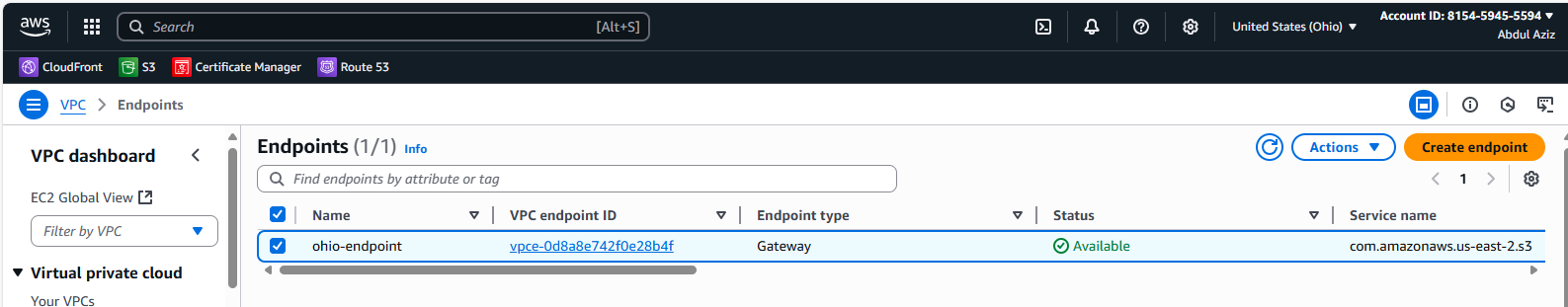
****

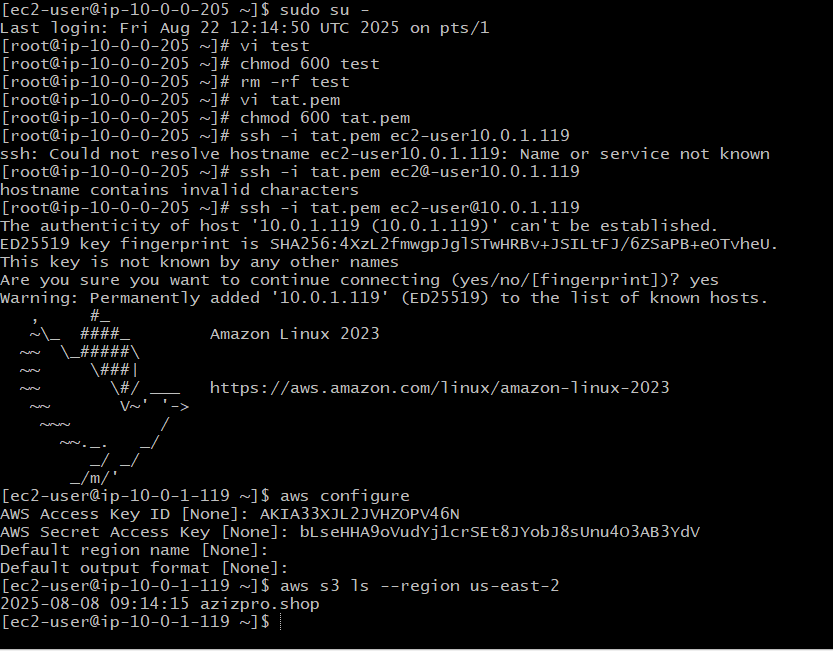
**I have done all in one image.**

Create endpoint in vpc2,vpc3 and vpc4  
•Which do not have public route table and attach s3

****

****

****

****

Similarly, procedure follow for remaining regions