VPC – task 2

1) Create one VPC,with 1 one public subnet and 1 private subnet.

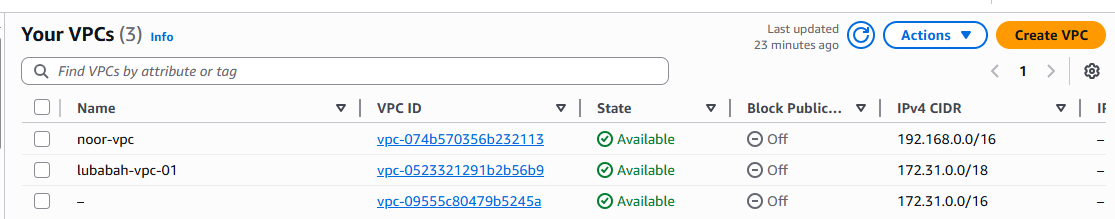
2) Enable VPC peering for cross region.

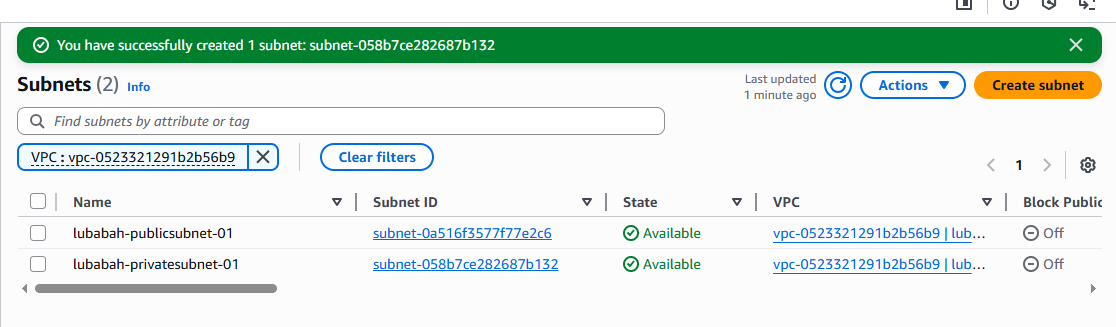
3) Enable VPC peering for cross account. (You can collaborate with your friend and do this task).

4) Setup VPC Transist gateway.

5) Setup VPC End Point.

1) Create one VPC,with 1 one public subnet and 1 private subnet.





2) Enable VPC peering for cross region.

Same region it is working because same VPC

When changing VPC we are unable to communicate

Come to the NV – peering connection – creat PC

Name: peering-nverginia-ohio

Requester is northvirginia

Accepter ohio and accepter VPC ID

Click on launch peering connection

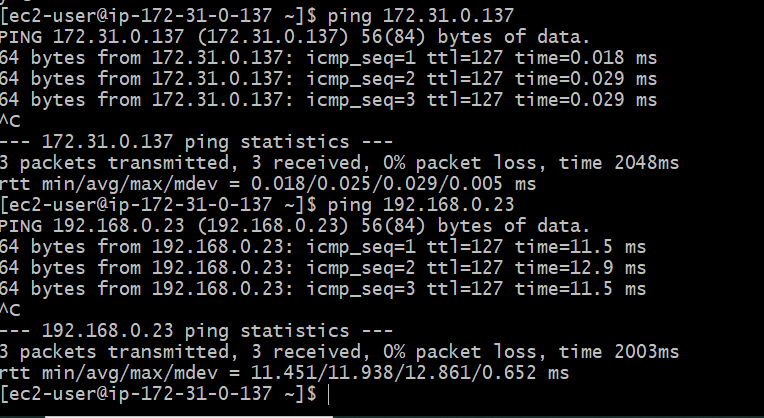
Then come to ohio region – peering connection

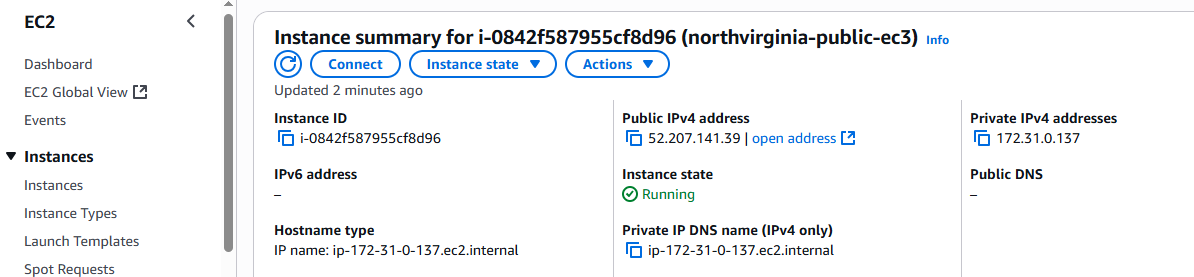
You can see here one request then just select this and go to action – accept requester – it will become active status.

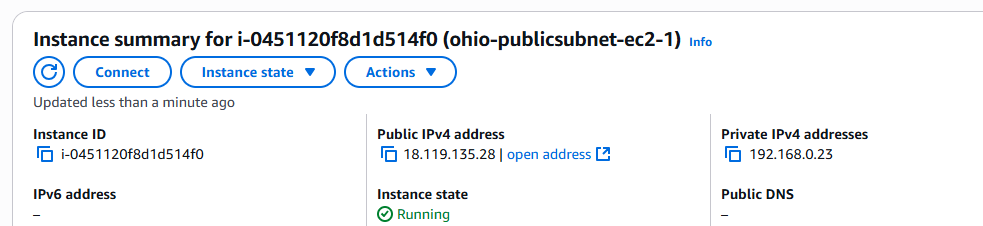
Then just go to north virgnia VPC and routtable – slect publicroute table bca we are using – routes- edit route – add route – here give the ohio cidr range – peering connection

Similarthing we have to configure in our ohio region route table also.

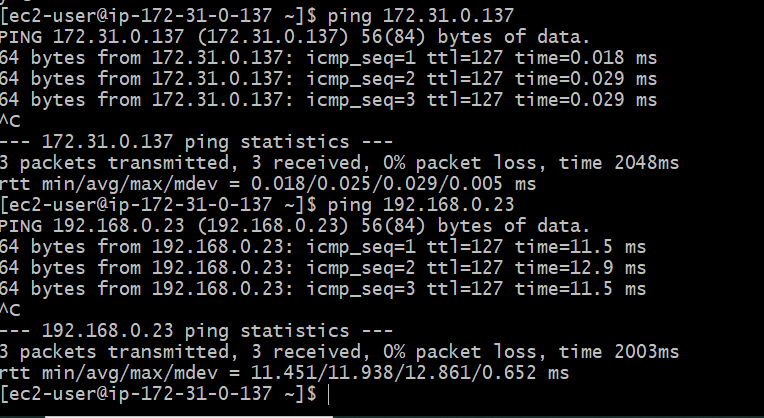
Go to ohio region vpc – routetable – publicroute bcz we are using – editroute – addroute – save





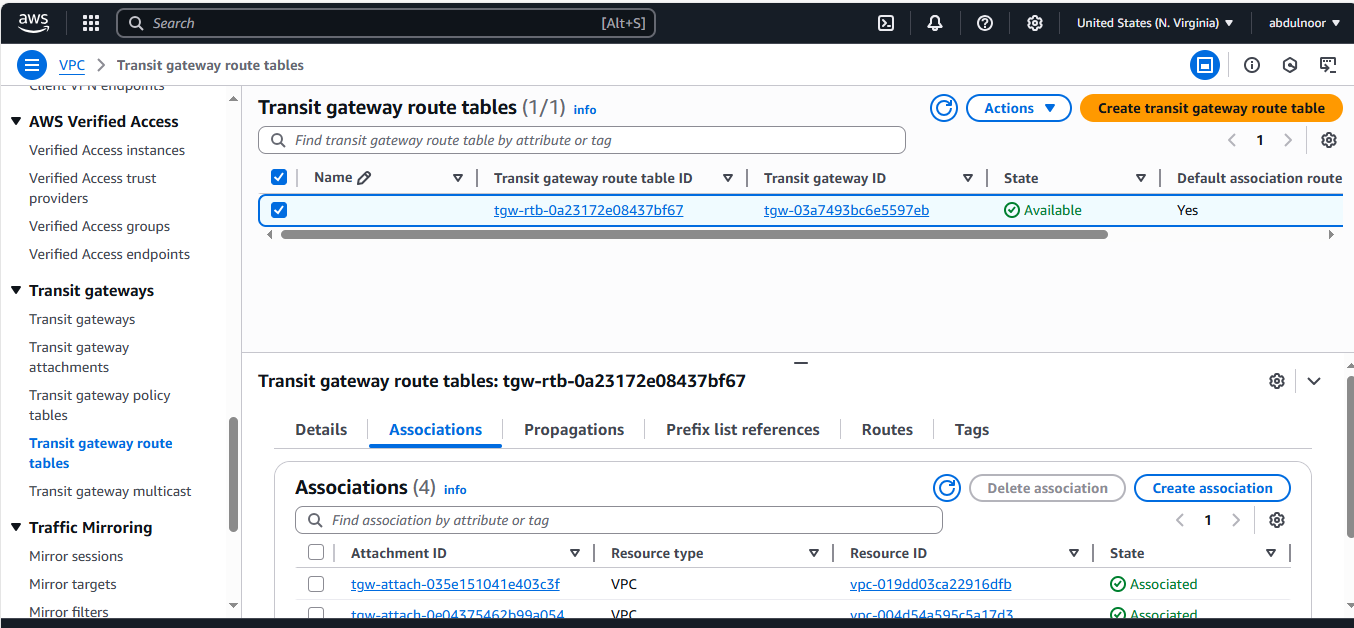


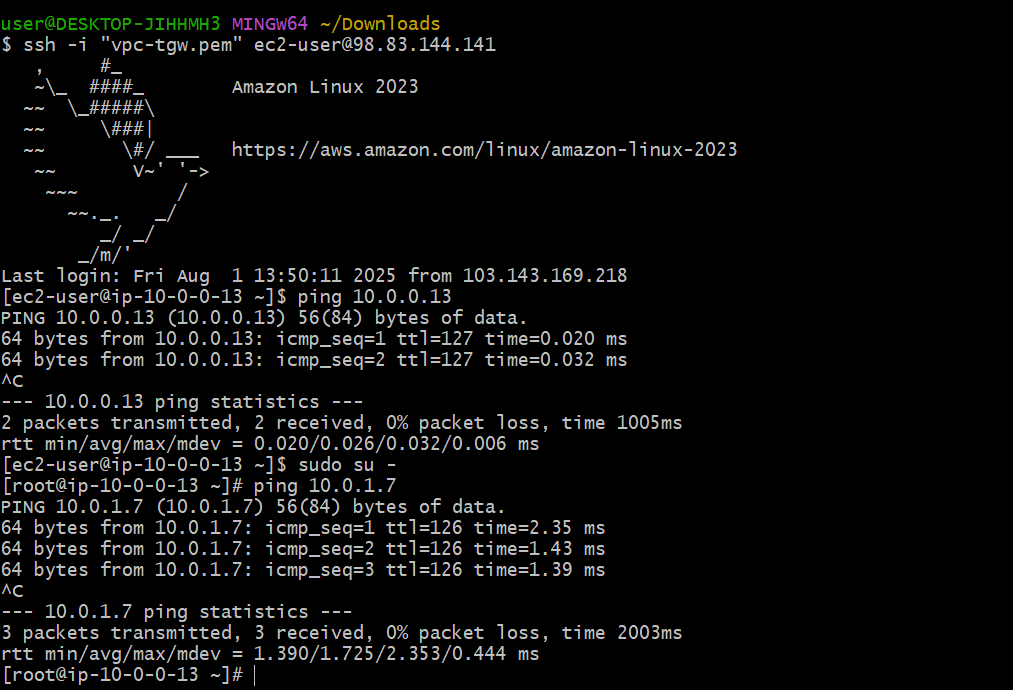
3) Enable VPC peering for cross account. (You can collaborate with your friend and do this task).

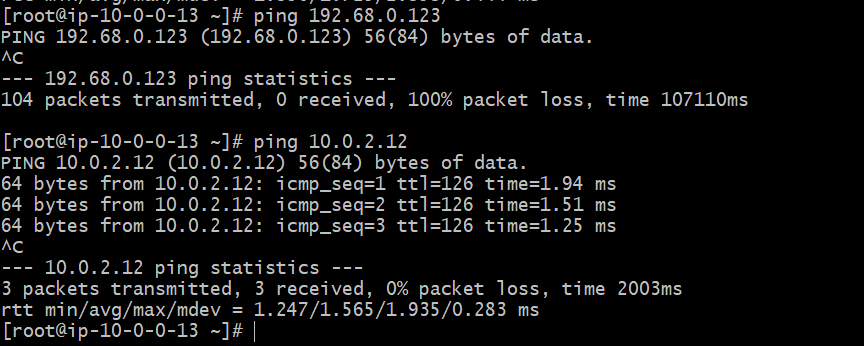


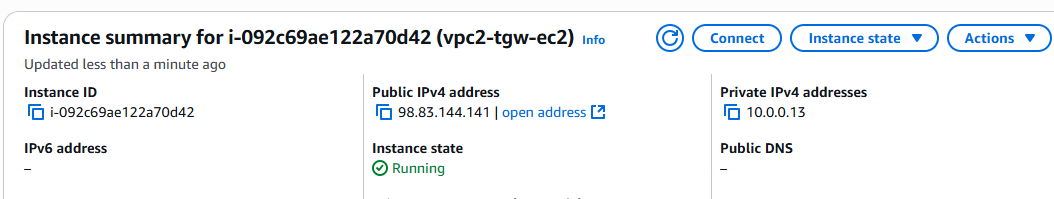
4) Setup VPC Transist gateway.

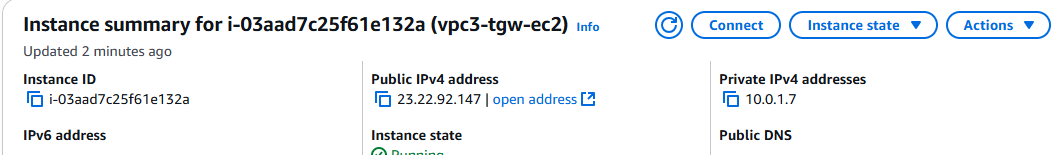












Executed internet is working with ec2 public one to ec2 three private id an ec2 four private id

5) Setup VPC End Point

To see the bucket s3 the command is **aws s3 ls** but if it’s not showing then first enter the command **aws configure** to start aws cli as below

The below black bordered box is just for information not related to this task points.

|  |
| --- |
|  |
|  |
| .aws file appears in root user only. That’s why we need to enter in root user. |
| Now enter into the .aws directory |
| Cd .aws/ |
|  |
| Now we are in .aws directory has **config** and credential file |
| Now read the config file |
| Cat config |
|  |
| Now read the credential file |
|  |

Now I can not access to my private ec2 because no IGW and NAT public iPs

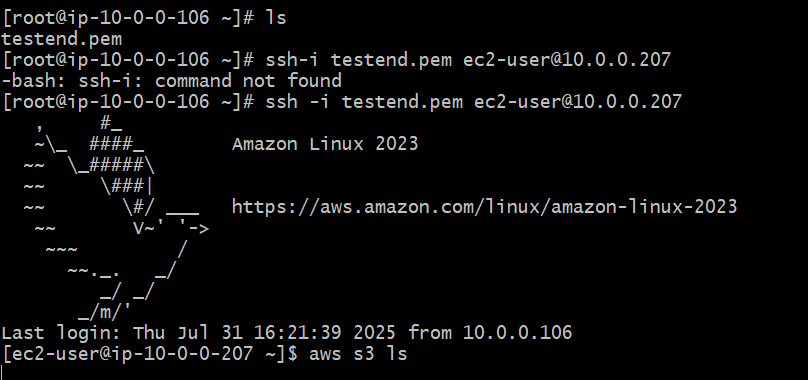
So to connect private ec2 copy the pemkey of public ec2 and create a new file and paste it

Cat endpoint-key copy it

And vi testend.pem

Paste it here and now execute the command

Ssh-i testend.pem ec2-user@private ec2 private ip enter here



Now execute to check the bucket of public ec2 in this private ec2 private ip

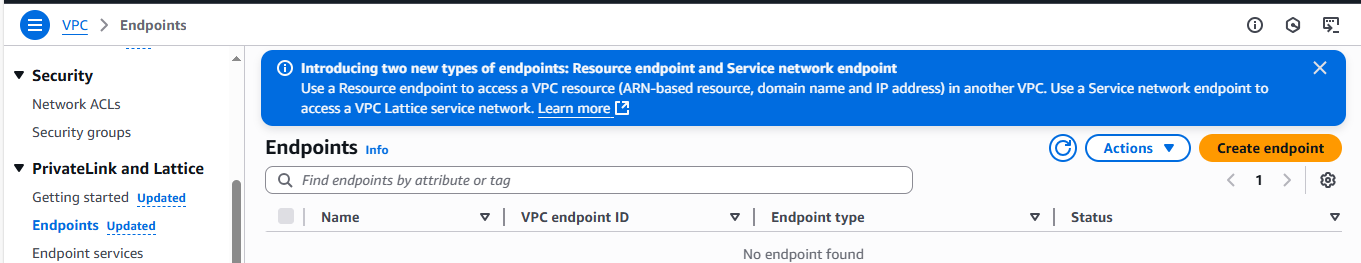
Command

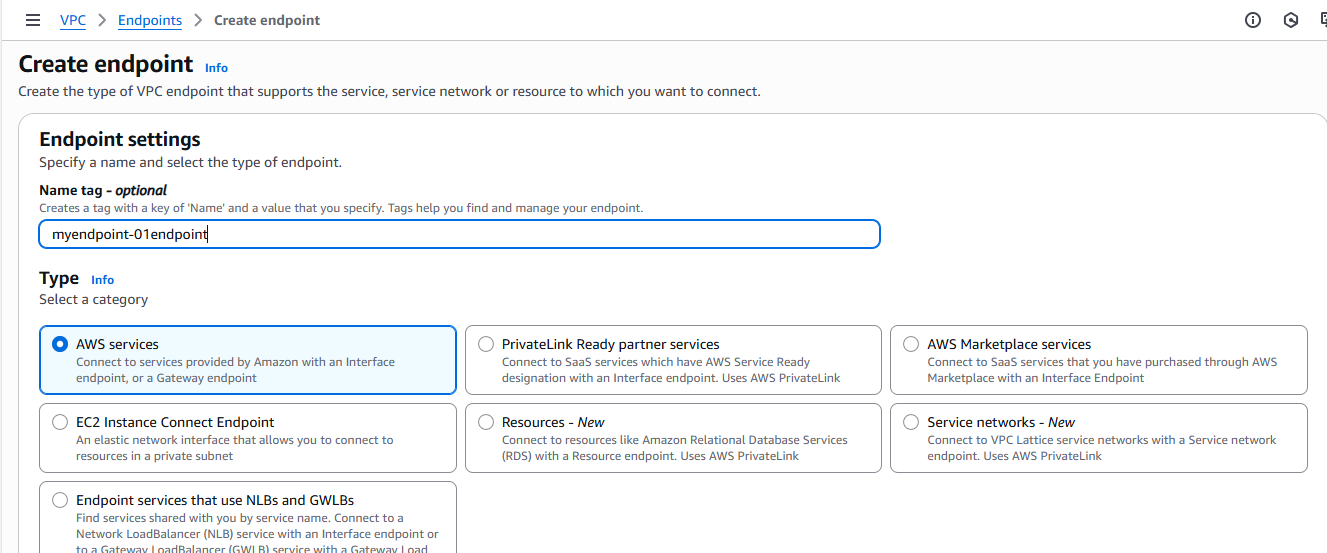
Aws s3 ls

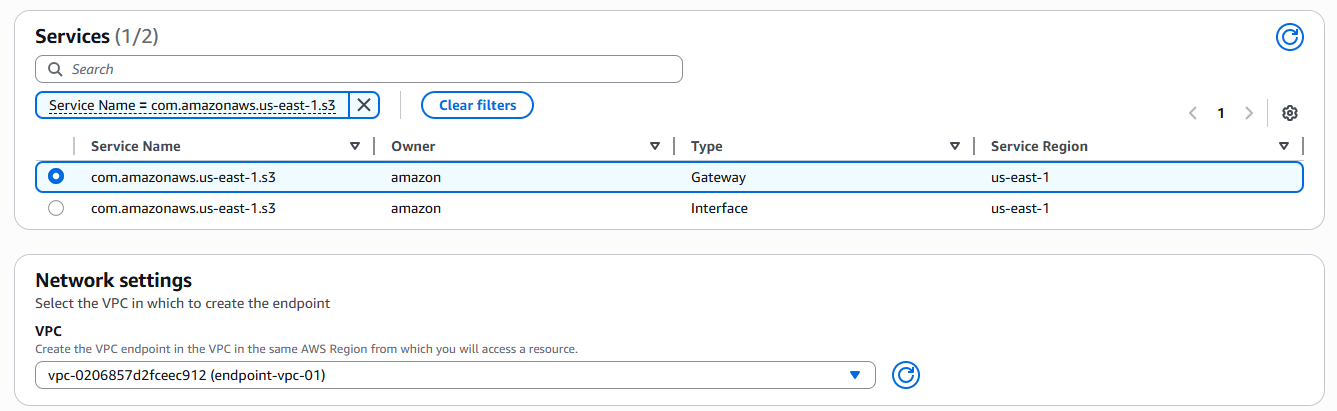
It will not show the bucket details because you don’t have connection of s3 bucket in this private ec2 private id.

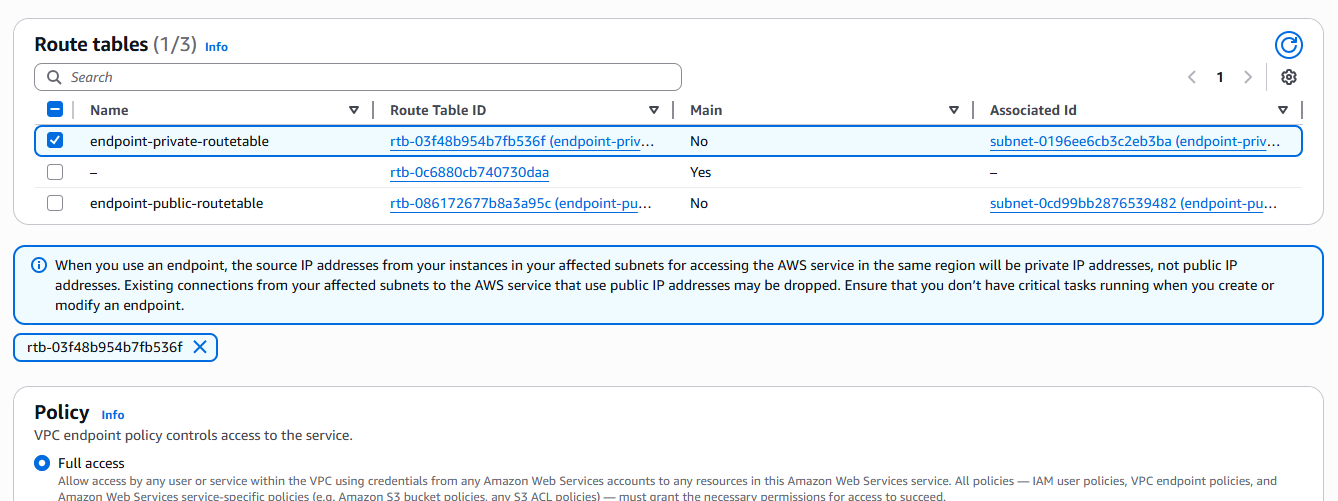
for this create ENDPOINT and attach to the private routing table.

Click on create

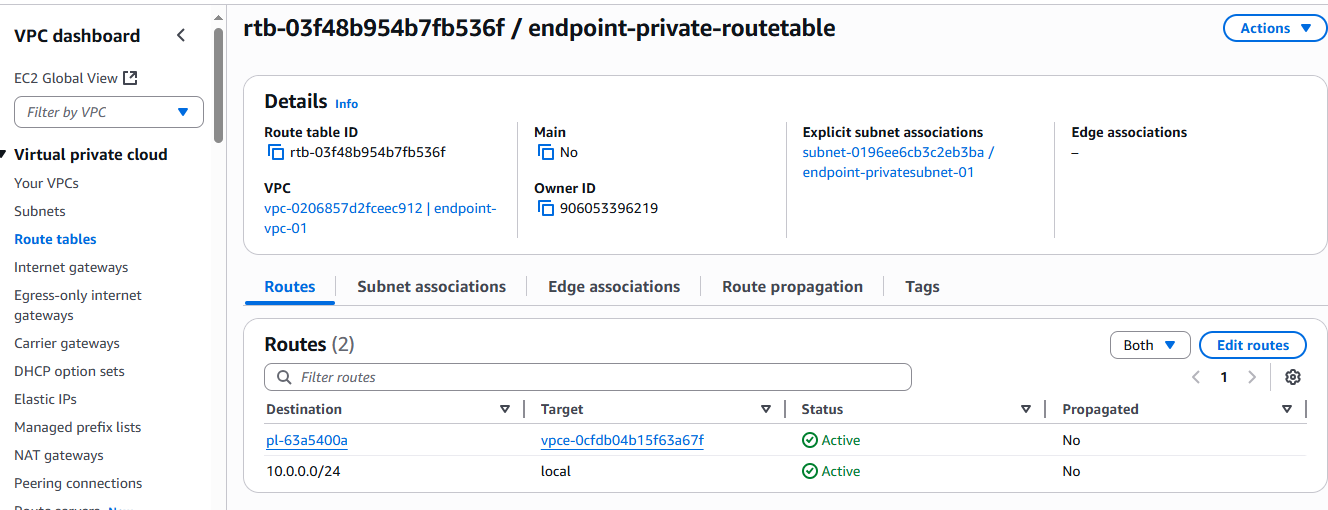


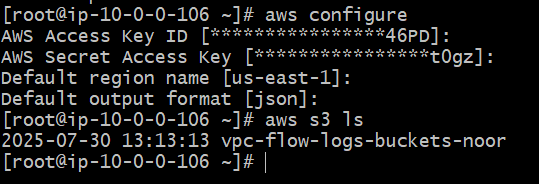






Go to vpc = private route tables create one private table but don’t assign the internet routes and in security group of private ec2 just assign ssh and don’t assign all traffic.





In the above appearing in private id of private instance without having internet with the help endpoint. Note: we can get the internet via pem key by copying and creating but we don’t get S3 bucket for this we have above steps.

Now enter into the root user to check your bucket

Sudo su –

Aws s3 ls