Setting up Transit Gateway and VPC Endpoints for a MultiVPC Architecture.

SCENARIO:

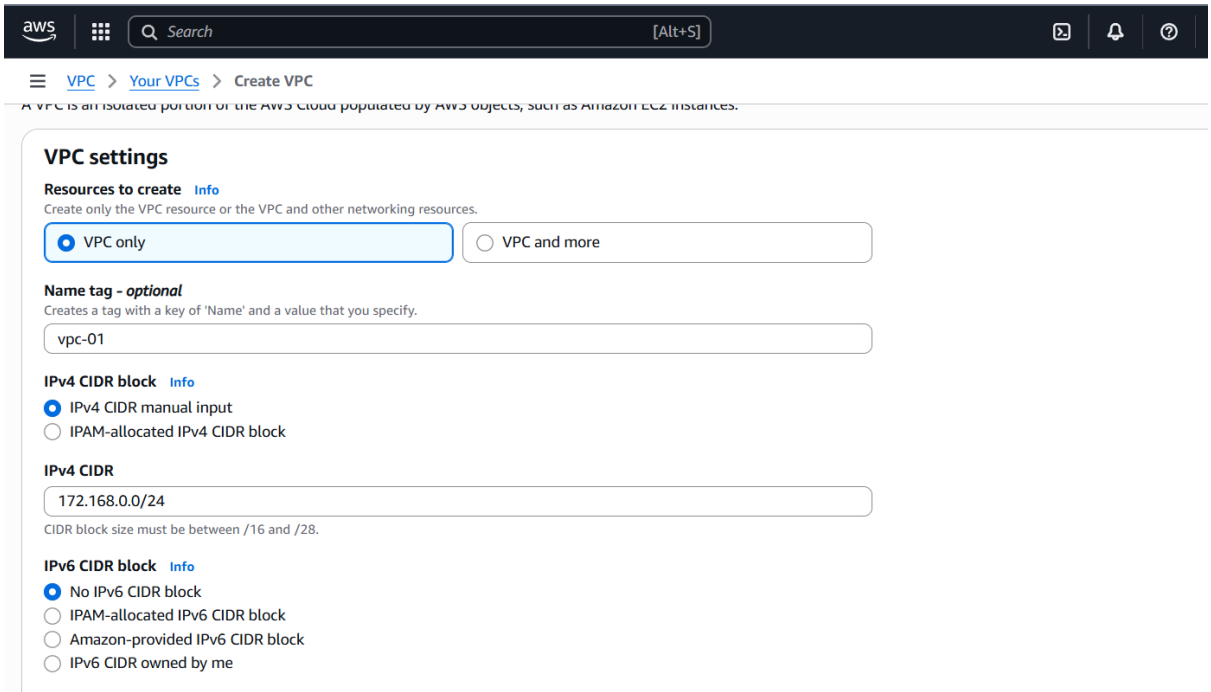
A large organization is migrating its on-premises infrastructure to the AWS cloud.

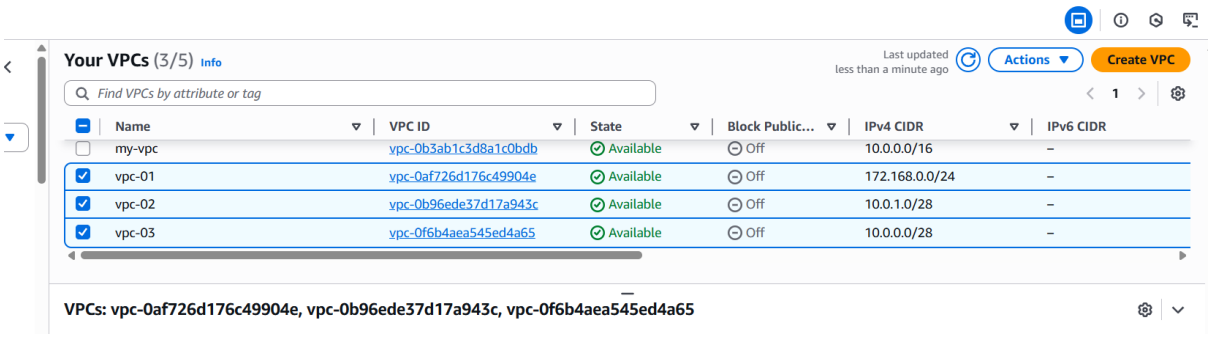
The organization's architecture involves multiple VPCs for different departments and applications, each requiring secure communication with centralized services and external resources.

The IT team needs to design and implement a scalable and efficient network

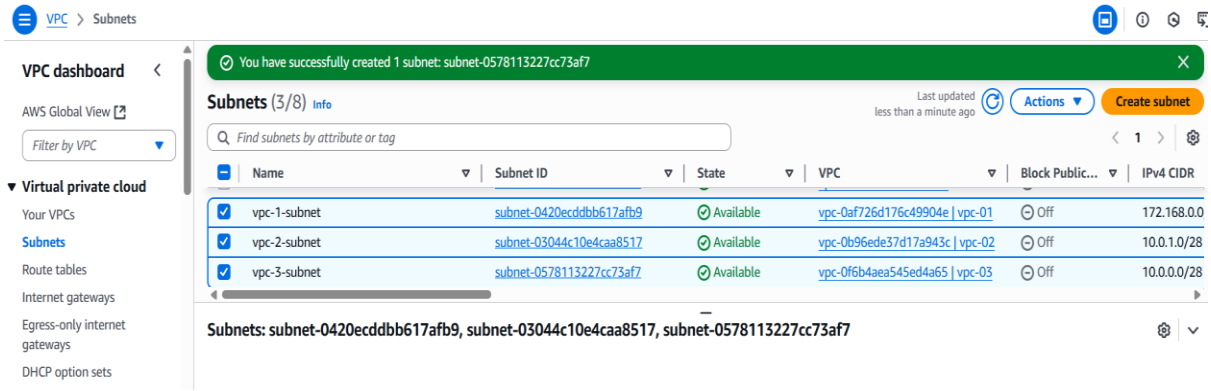
architecture to accommodate the organization's growth and ensure robust connectivity between VPCs and external services.

Create 3 VPC’s one for public and 2 for private.

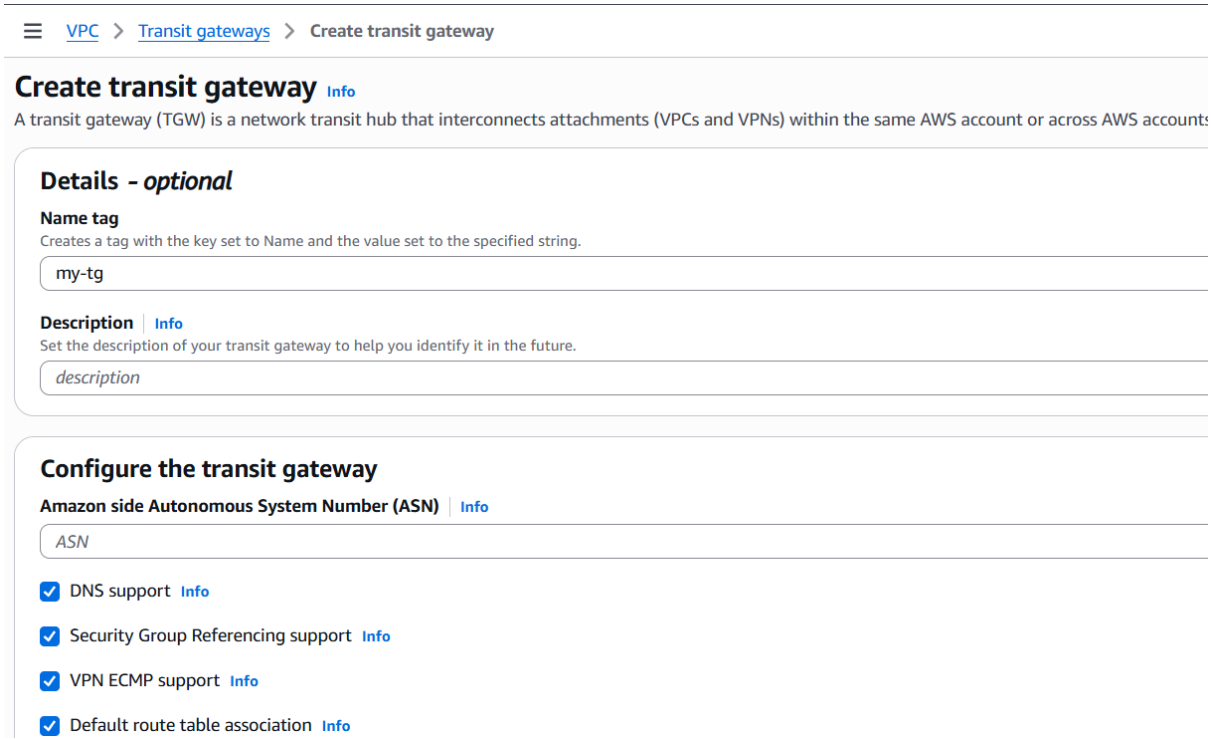




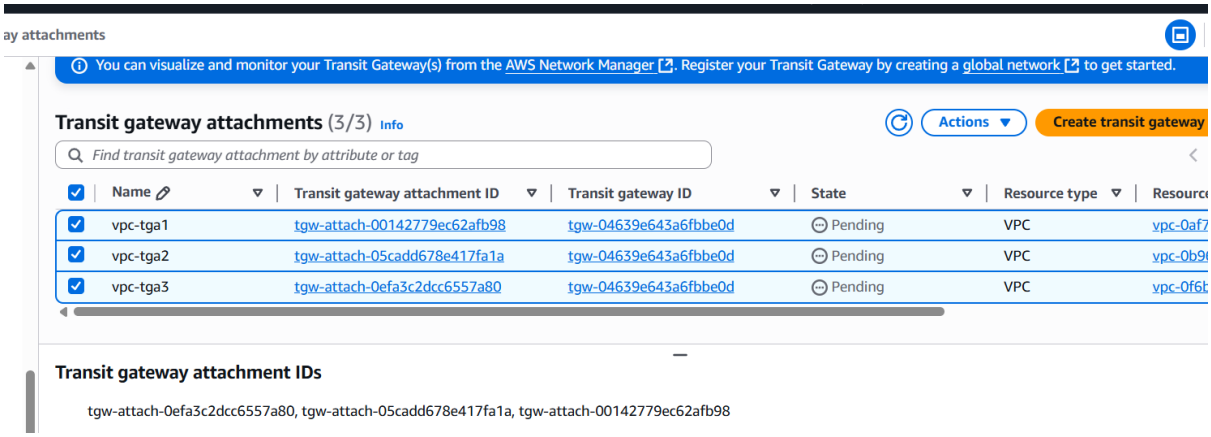
Create subnets for the vpc's that you are created.



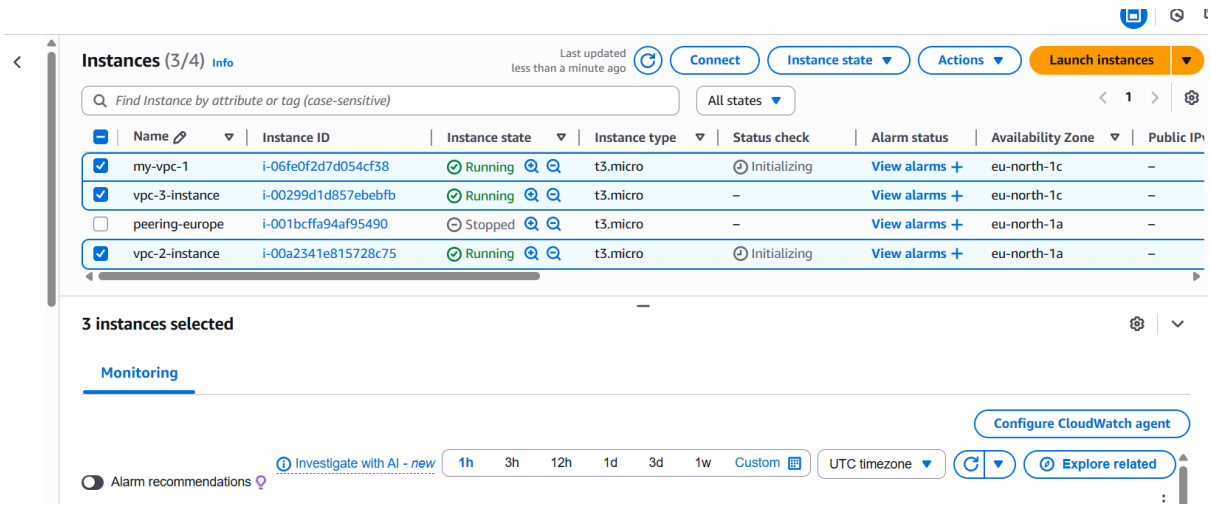
Create a transit gateway



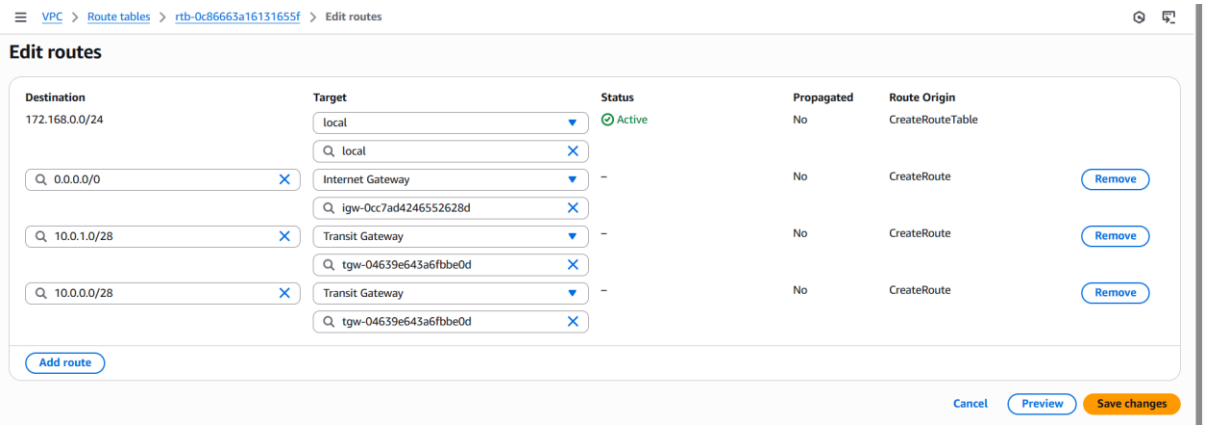
Create transit gateway attachments for three vpc’s. and give the subnet associations, for public subnet attach the internet gateway.



Create 3 instances with the 3 vpc’s.



Go to first subnet and edit routes add remaining two vpc’s cidr range .

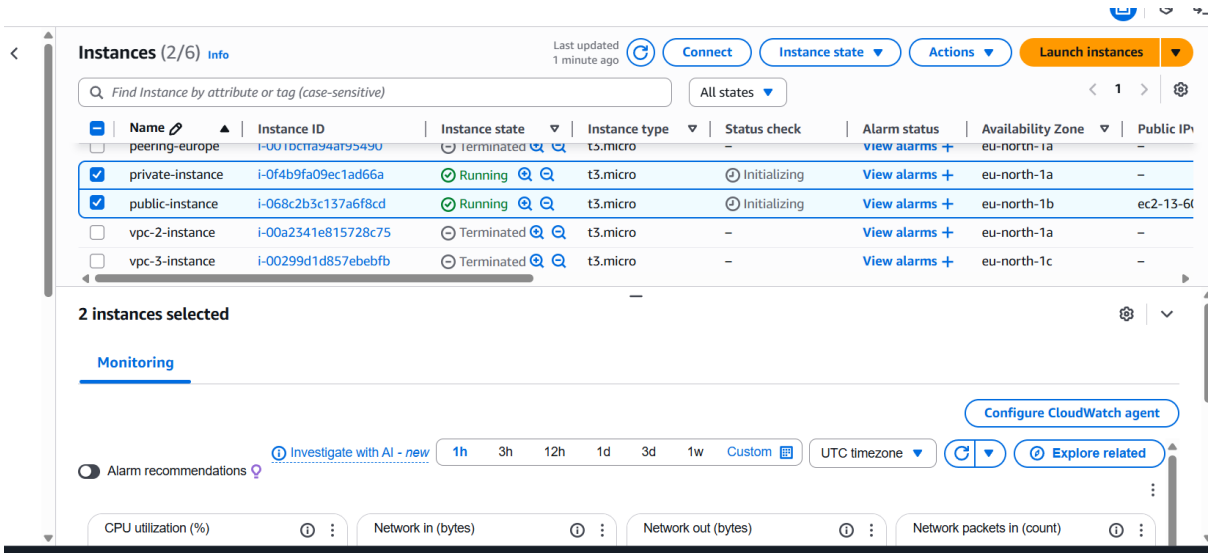


Login with public ip of 1 instance and from that public to ping another account's private ip address.

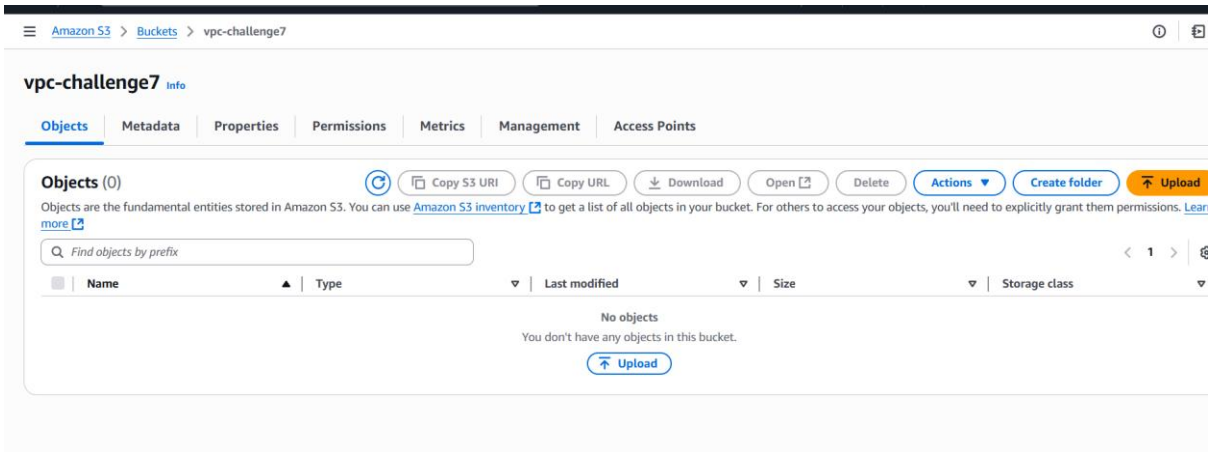
```
MUJJU SK@DESKTOP-LU541U4 MINGW64 ~/Downloads
$ ssh -i "AWS.pem" ec2-user@16.16.233.250
The authenticity of host '16.16.233.250 (16.16.233.250)' can't be established.
ED25519 key fingerprint is SHA256:ZHcPO387ISO1bgjyOsGYpr7tAnArYC3C2CN82dyoja4.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '16.16.233.250' (ED25519) to the list of known hosts.
   ,     #_
   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
[ec2-user@ip-10-0-0-5 ~]$ sudo su -
[root@ip-10-0-0-5 ~]# ping 172.168.0.161
PING 172.168.0.161 (172.168.0.161) 56(84) bytes of data.
64 bytes from 172.168.0.161: icmp_seq=41 ttl=126 time=0.629 ms
64 bytes from 172.168.0.161: icmp_seq=42 ttl=126 time=0.288 ms
64 bytes from 172.168.0.161: icmp_seq=43 ttl=126 time=0.290 ms
64 bytes from 172.168.0.161: icmp_seq=44 ttl=126 time=0.285 ms
64 bytes from 172.168.0.161: icmp_seq=45 ttl=126 time=0.302 ms
64 bytes from 172.168.0.161: icmp_seq=46 ttl=126 time=0.290 ms
64 bytes from 172.168.0.161: icmp_seq=47 ttl=126 time=0.291 ms
64 bytes from 172.168.0.161: icmp_seq=48 ttl=126 time=0.295 ms
```

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

Launch one public instance and one private instance using private subnet and public subnet.



Go to S3 and create a bucket.



Connect ssh with the public instance

```
MUJJU SK@DESKTOP-LU541U4 MINGW64 ~/Downloads
$ ssh -i "AWS.pem" ec2-user@ec2-13-60-99-219.eu-north-1.compute.amazonaws.com
   ,     #_
   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Wed Oct  1 09:37:02 2025 from 103.143.169.218
[ec2-user@ip-172-31-36-222 ~]$ sudo su -
Last login: Wed Oct  1 09:37:20 UTC 2025 on pts/1
[root@ip-172-31-36-222 ~]# aws --version
aws-cli/2.27.57 Python/3.9.23 Linux/6.1.150-174.273.amzn2023.x86_64 source/x86_64.amzn.2023
[root@ip-172-31-36-222 ~]#
```

Go to aws configure and give the security key and password .

```
[root@ip-172-31-36-222 ~]# aws configure
AWS Access Key ID [None]: AKIATNTADWLTSYF63H5C
AWS Secret Access Key [None]: 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
Default region name [None]: us-east-1
Default output format [None]: json
[root@ip-172-31-36-222 ~]# aws s3 ls
2025-09-29 10:11:05 bucketnew57
2025-09-29 11:34:52 n-virginia-bucket6
2025-10-01 09:35:38 vpc-challenge7
[root@ip-172-31-36-222 ~]#
```

Copy the pem key in local and create a file and paste the pem key in that file.

Add permission to that file chmod 400 test.pem

Ssh -i test.pem ec2-user@<private ip>

```
[root@ip-172-31-36-222 ~]# vi test.pem
[root@ip-172-31-36-222 ~]# chmod 400 test.pem
[root@ip-172-31-36-222 ~]# ssh -i test.pem ec2-user@172.31.36.222
The authenticity of host '172.31.36.222 (172.31.36.222)' can't be established.
ED25519 key fingerprint is SHA256:4w+Vu2FUk9B7oyo77R7k9udiFTt6LnLXKRf2teKboSE.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.31.36.222' (ED25519) to the list of known hosts.
   ,     #_
   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Wed Oct  1 09:38:21 2025 from 103.143.169.218
[ec2-user@ip-172-31-36-222 ~]$
```

After that aws configure.

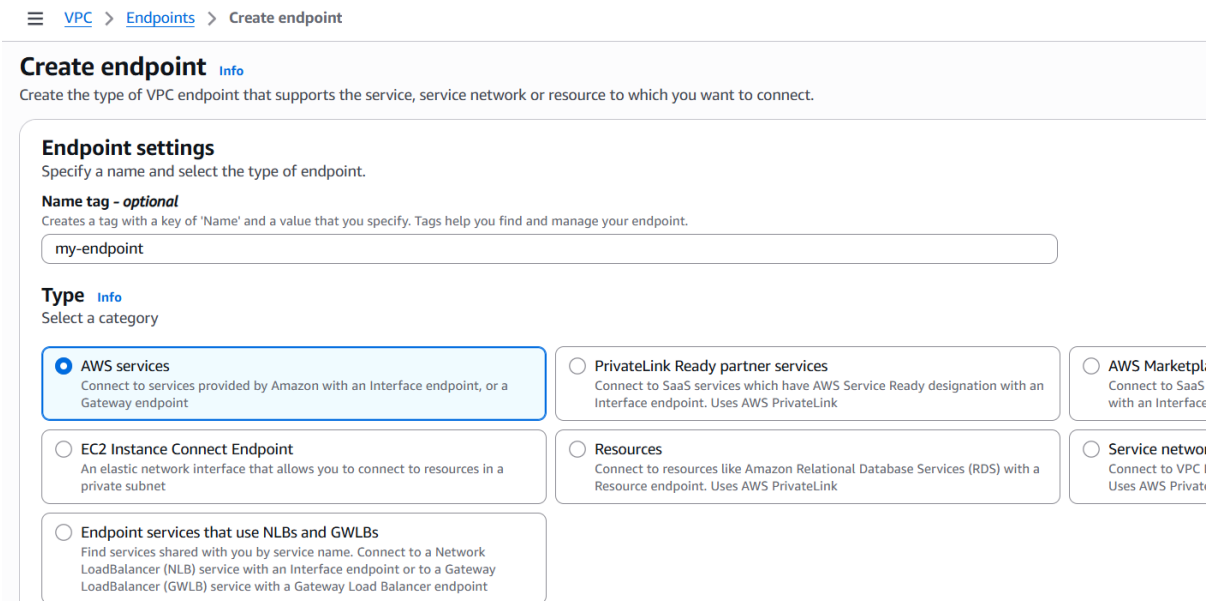
```
[ec2-user@ip-172-31-36-222 ~]$ aws configure
AWS Access Key ID [None]: AKIATNTADWLTSYF63H5C
AWS Secret Access Key [None]: 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
Default region name [None]: us-east-1
Default output format [None]: json
[ec2-user@ip-172-31-36-222 ~]$
```

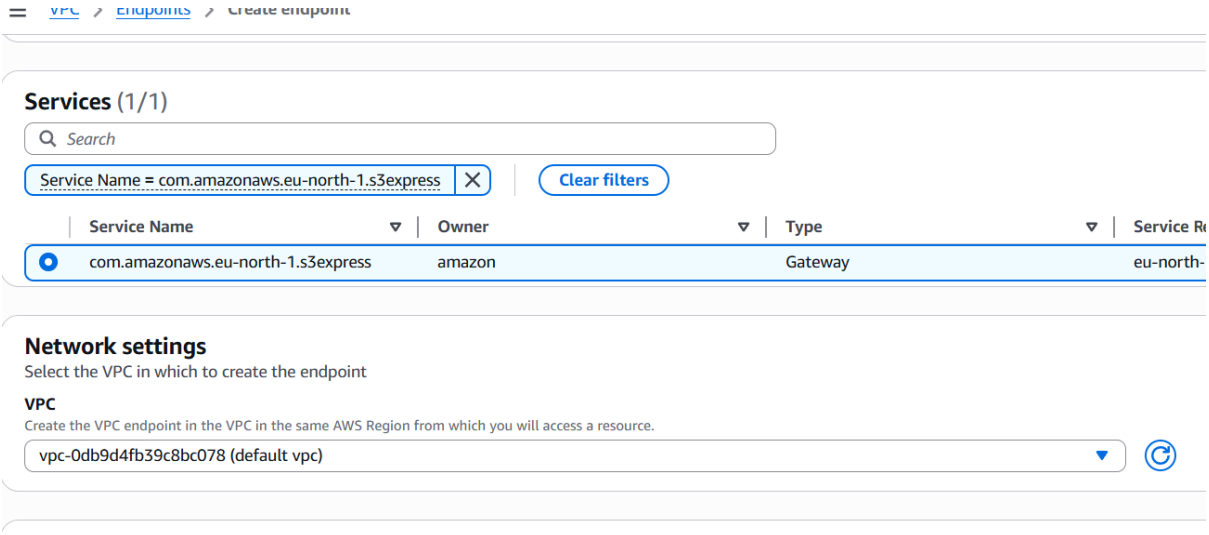
- Now go to vpc
- Navigate to end points
- Select aws service
- Then select s3 and end point type expres
- Then select gateway

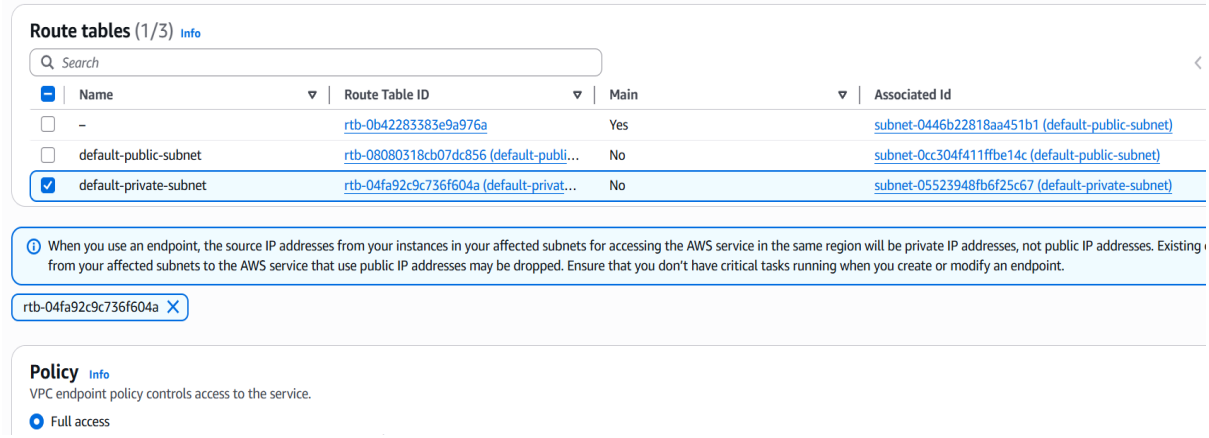
•Create end point the end point has been created

•Now you can acess the s3 from the private instance : aws s3 ls

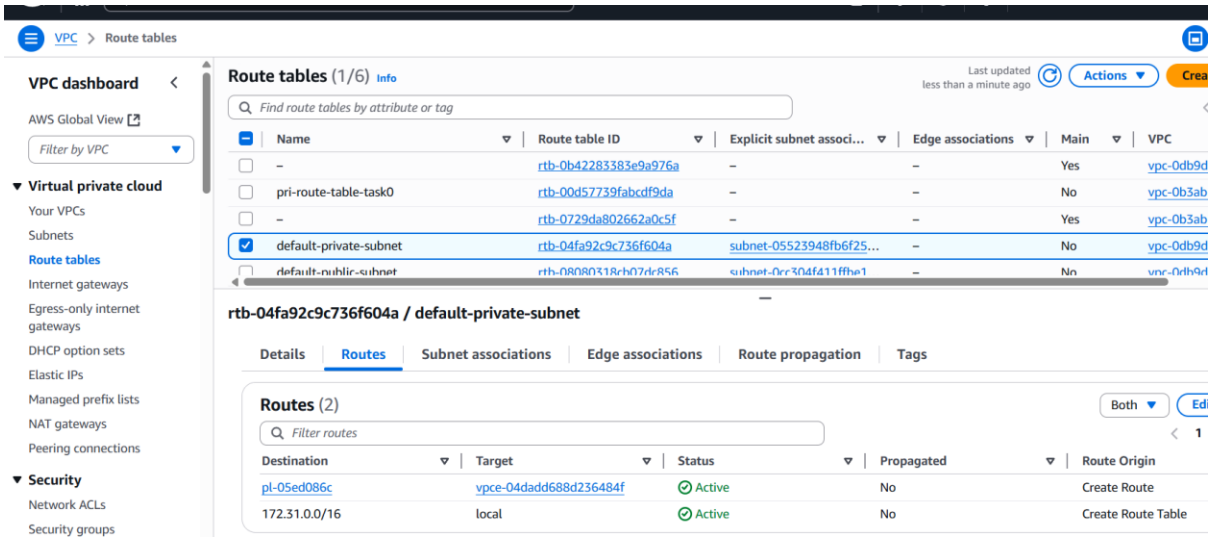
Create an end point.







If we see in the routetable the endpoint is created for private subnet.




```
[root@ip-172-31-36-222 ~]# aws configure
AWS Access Key ID [None]: AKIATNTADWLTSYF63H5C
AWS Secret Access Key [None]: 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
Default region name [None]: us-east-1
Default output format [None]: json
[root@ip-172-31-36-222 ~]# aws s3 ls
2025-09-29 10:11:05 bucketnew57
2025-09-29 11:34:52 n-virginia-bucket6
2025-10-01 09:35:38 vpc-challenge7
[root@ip-172-31-36-222 ~]#
```