

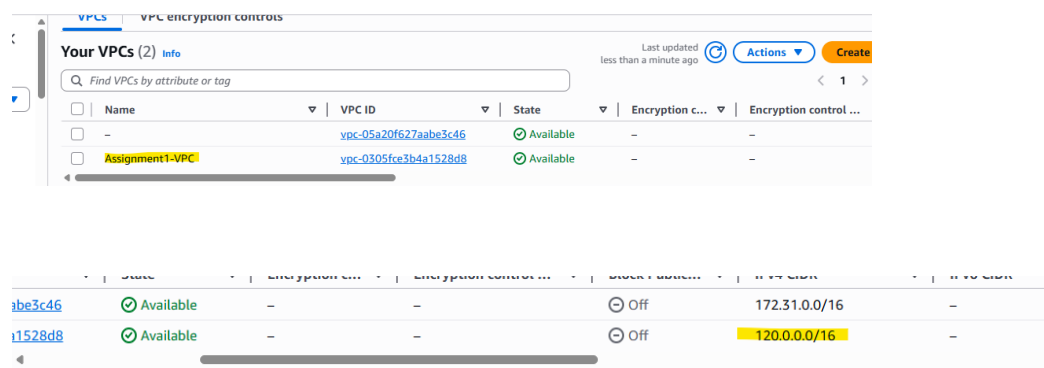
Assignment 1

Working for an organization, you are required to provide them with a safe and secure environment for the deployment of their resources. They might require different types of connectivity. Implement the following to fulfill the requirements of the company.

Tasks To Be Performed:

1. Create a VPC with 120.0.0.0/16 CIDR block.
2. Create 1 public subnet and 2 private subnets and make sure you connect a NAT gateway for internet connectivity to a private subnet

Step 1: Create VPC with the CIDR block 172.31.0.0/16

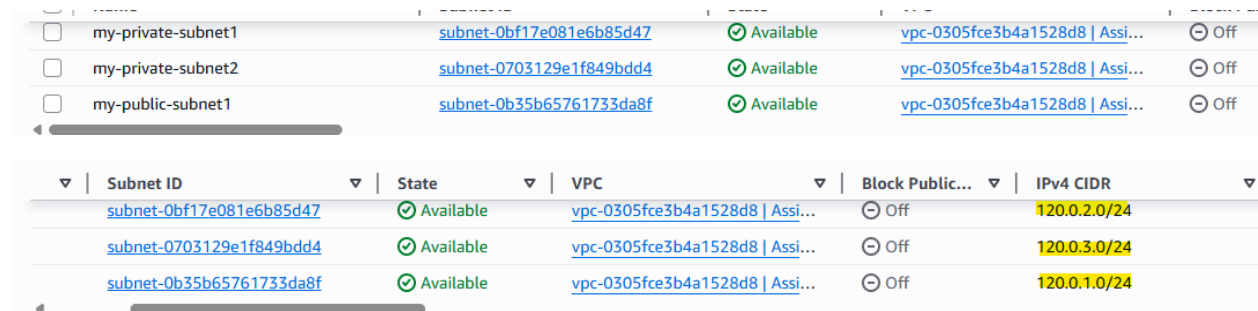


The screenshot shows the AWS VPC console. At the top, there's a section for 'Your VPCs (2)' with a search bar and a table. The table lists two VPCs: 'vpc-05a20f627aabe3c46' and 'vpc-0305fce3b4a1528d8'. The second VPC is highlighted. Below this, there's a table for subnets. It lists three subnets: 'subnet-0bf17e081e6b85d47', 'subnet-0703129e1f849bdd4', and 'subnet-0b35b65761733da8f'. The second subnet is highlighted.

Name	VPC ID	State	Encryption c...	Encryption control ...
-	vpc-05a20f627aabe3c46	Available	-	-
Assignment1-VPC	vpc-0305fce3b4a1528d8	Available	-	-

Name	VPC ID	State	Encryption c...	Encryption control ...
subnet-0bf17e081e6b85d47	vpc-0305fce3b4a1528d8	Available	-	-
subnet-0703129e1f849bdd4	vpc-0305fce3b4a1528d8	Available	-	-
subnet-0b35b65761733da8f	vpc-0305fce3b4a1528d8	Available	-	-

Step 2: Create 1 public subnet and 2 private subnets



The screenshot shows the AWS VPC console. At the top, there's a section for 'Your Subnets (3)' with a search bar and a table. The table lists three subnets: 'my-private-subnet1', 'my-private-subnet2', and 'my-public-subnet1'. The third subnet is highlighted. Below this, there's a table for subnets. It lists three subnets: 'subnet-0bf17e081e6b85d47', 'subnet-0703129e1f849bdd4', and 'subnet-0b35b65761733da8f'. The second subnet is highlighted.

Name	VPC ID	State	Encryption c...	Encryption control ...
my-private-subnet1	subnet-0bf17e081e6b85d47	Available	-	-
my-private-subnet2	subnet-0703129e1f849bdd4	Available	-	-
my-public-subnet1	subnet-0b35b65761733da8f	Available	-	-

Subnet ID	State	VPC	Block Public...	IPv4 CIDR
subnet-0bf17e081e6b85d47	Available	vpc-0305fce3b4a1528d8 Assi...	Off	120.0.2.0/24
subnet-0703129e1f849bdd4	Available	vpc-0305fce3b4a1528d8 Assi...	Off	120.0.3.0/24
subnet-0b35b65761733da8f	Available	vpc-0305fce3b4a1528d8 Assi...	Off	120.0.1.0/24

Step 3: Create the Internet Gateway and attach it to VPC

igw-044d84032e87567bc / Assignment-1-IGW

Actions

Details

Internet gateway ID
igw-044d84032e87567bc

State
Attached

VPC ID
vpc-0305fce3b4a1528d8
Assignment1-VPC

Owner
416946765337

Tags (1)

Manage tags

Search tags

< 1 >

Key

Value

Name

Assignment-1-IGW

Step 4: Create the route table for public subnet

rtb-05d954063d14db8d9 / public-rt

Actions

Details

Route table ID
rtb-05d954063d14db8d9

VPC
vpc-0305fce3b4a1528d8
Assignment1-VPC

Main
No

Owner ID
416946765337

Explicit subnet associations
-

Edge associations
-

Routes

Subnet associations

Edge associations

Route propagation

Tags

Routes (2)

Both

Edit routes

Filter routes

< 1 >

Destination

Target

Status

Propagated

Route Origin

0.0.0.0/0

igw-044d84032e87567bc

Active

No

Create Route

rtb-05d954063d14db8d9 / public-rt

Actions

Details

Route table ID
rtb-05d954063d14db8d9

VPC
vpc-0305fce3b4a1528d8 | Assignment1-VPC

Main
No

Owner ID
416946765337

Explicit subnet associations
subnet-0b35b65761733da8f / my-public-subnet1

Edge associations
-

Routes

Subnet associations

Edge associations

Route propagation

Tags

Explicit subnet associations (1)

Edit subnet associations

Find subnet association

< 1 >

Name

Subnet ID

IPv4 CIDR

IPv6 CIDR

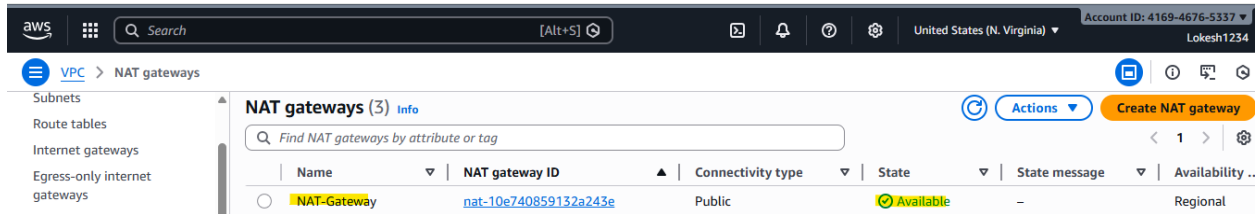
my-public-subnet1

subnet-0b35b65761733da8f

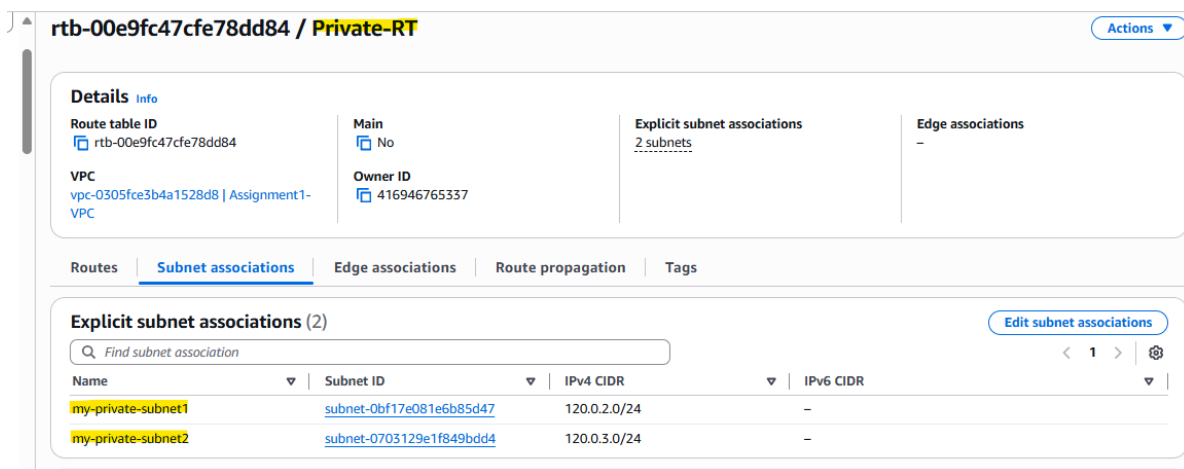
120.0.1.0/24

-

Step 5: Create a NAT gateway

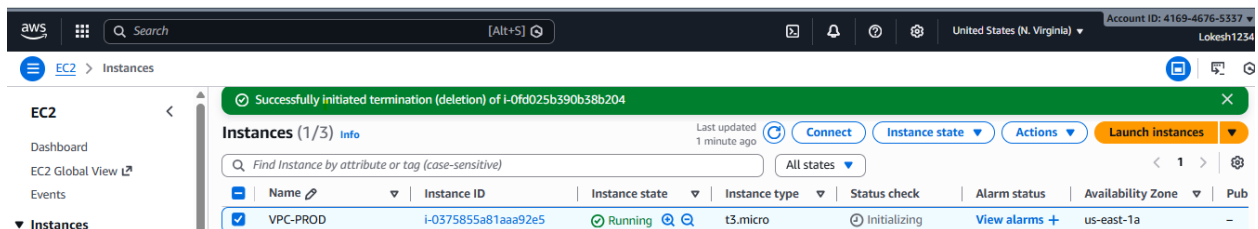


Step 6: Create private route table and associate them with private subnets to it.



Testing whether we can connect to the Internet through the public subnet

Create a EC2 instance and assign the VPC created use the public subnet assign auto assign public IP and launch the Ec2 instance



Connect from the outside using the ssh command to the Ec2 instance

And ping google.com

```
#
#-
#####
#####
#####
#####
V--' --> https://aws.amazon.com/linux/amazon-linux-2023
m/'
```

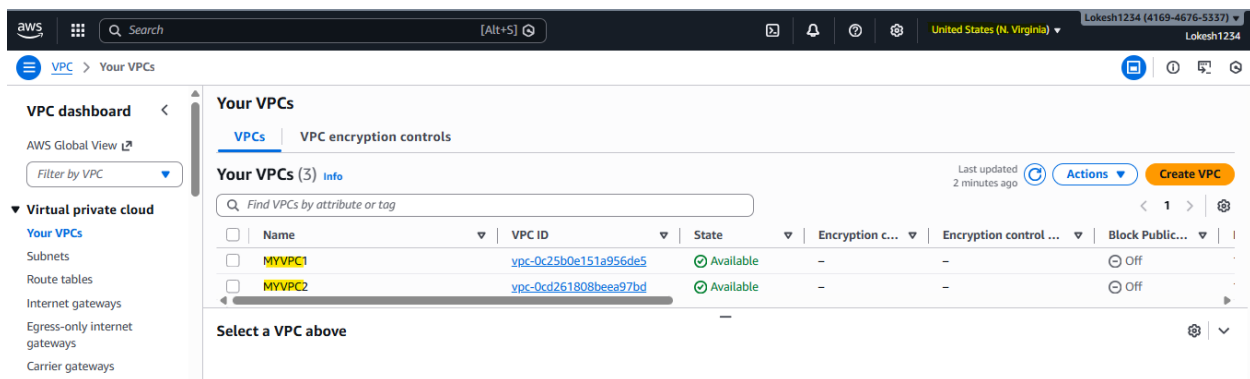
[ec2-user@ip-120-0-1-73 ~]\$ ping google.com
PING google.com (192.178.155.101) 56(84) bytes of data.
64 bytes from yuiadr-in-f101.1e100.net (192.178.155.101): icmp_seq=1 ttl=102 time=2.13 ms
64 bytes from yuiadr-in-f101.1e100.net (192.178.155.101): icmp_seq=2 ttl=102 time=2.16 ms
64 bytes from yuiadr-in-f101.1e100.net (192.178.155.101): icmp_seq=3 ttl=102 time=2.15 ms
64 bytes from yuiadr-in-f101.1e100.net (192.178.155.101): icmp_seq=4 ttl=102 time=2.17 ms
64 bytes from yuiadr-in-f101.1e100.net (192.178.155.101): icmp_seq=5 ttl=102 time=2.24 ms
64 bytes from yuiadr-in-f101.1e100.net (192.178.155.101): icmp_seq=6 ttl=102 time=2.14 ms
64 bytes from yuiadr-in-f101.1e100.net (192.178.155.101): icmp_seq=7 ttl=102 time=2.17 ms
64 bytes from yuiadr-in-f101.1e100.net (192.178.155.101): icmp_seq=8 ttl=102 time=2.16 ms
^C
--- google.com ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7012ms
rtt min/avg/max/mdev = 2.133/2.165/2.241/0.031 ms

Problem Statement:

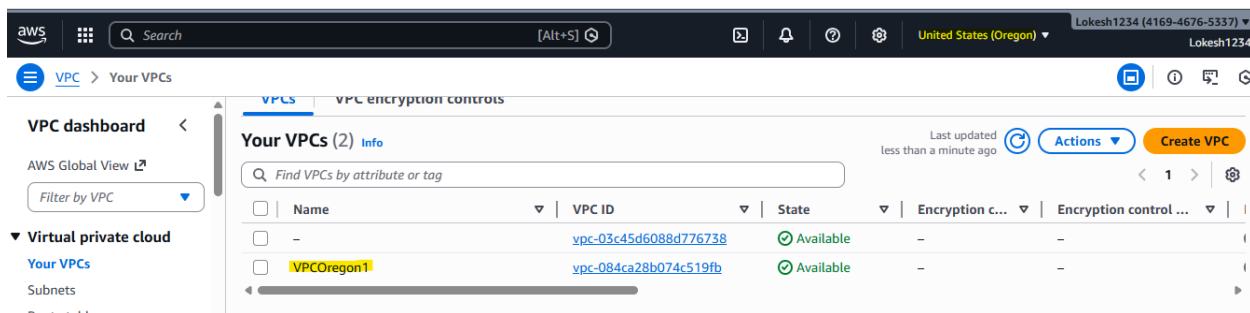
Working for an organization, you are required to provide them a safe and secure environment for the deployment of their resources. They might require different types of connectivity. Implement the following to fulfill the requirements of the company.

Tasks To Be Performed:

1. Create 2 VPCs in the North Virginia region named MYVPC1 and MYVPC2



2. Create one VPC in the Oregon region named VPCOregon1



3. Create a peering connection between MYVPC1 and MYVPC2

aws [Search] [Alt+S] United States (N. Virginia) Lokesh1234 (4169-4676-5337) Lokesh1234

VPC > Peering connections

Route tables
Internet gateways
Egress-only internet gateways
Carrier gateways
DHCP option sets
Elastic IPs
Managed prefix lists

Peering connections (1) info

Find peering connections by attribute or tag

Name	Peering connection ID	Status	Requester VPC	Accepter VPC
Peer-MYVPC1-MYVPC2	pcx-0099b59cbcd7266e7	Pending acceptance	vpc-0c25b0e151a956de5 / MY...	vpc-0cd261808beea97bd / MY...

aws [Search] [Alt+S] United States (N. Virginia) Lokesh1234 (4169-4676-5337) Lokesh1234

VPC > Peering connections

Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only internet gateways
Carrier gateways

Your VPC peering connection () has been established.
To send and receive traffic across this VPC peering connection, you must add a route to the peered VPC in one or more of your VPC route tables. [Modify my route tables now](#)

Peering connections (1) info

Find peering connections by attribute or tag

Name	Peering connection ID	Status	Requester VPC	Accepter VPC
Peer-MYVPC1-MYVPC2	pcx-0099b59cbcd7266e7	Active	vpc-0c25b0e151a956de5 / MY...	vpc-0cd261808beea97bd / MY..

4. Create a peering connection between MYVPC2 and VPCOregon1

Home | XORNET Chat-Gpt First Workflow - Loki... Full Stack Monitorin... Xoriant SPRP Kubernetes for the... Student Dashboard... Coin by Zerodha - B... All Bookmark

aws [Search] [Alt+S] United States (N. Virginia) Lokesh1234 (4169-4676-5337) Lokesh1234

VPC > Peering connections

Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only internet gateways
Carrier gateways
DHCP option sets
Elastic IPs

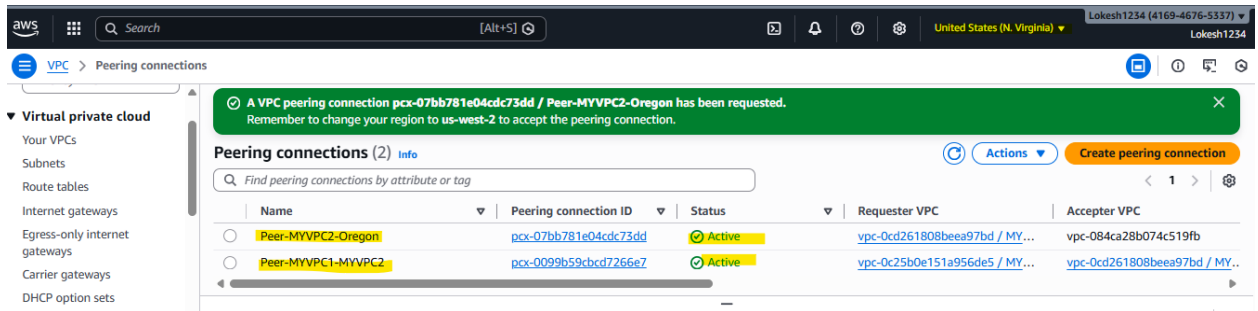
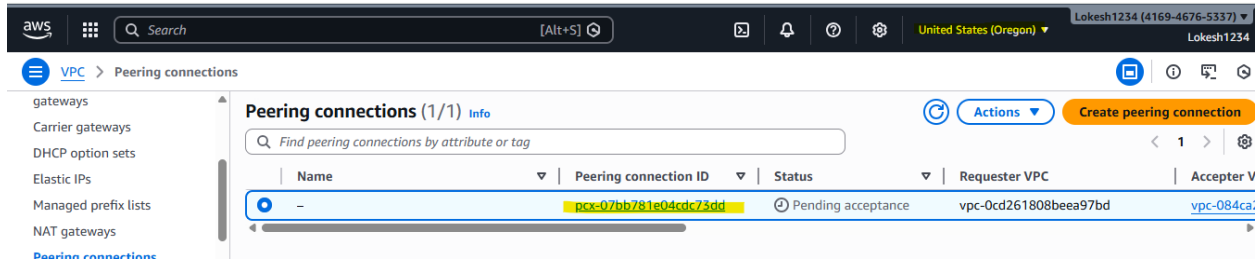
A VPC peering connection pcx-07bb781e04cdc73dd / Peer-MYVPC2-Oregon has been requested.
Remember to change your region to us-west-2 to accept the peering connection.

Peering connections (1/2) info

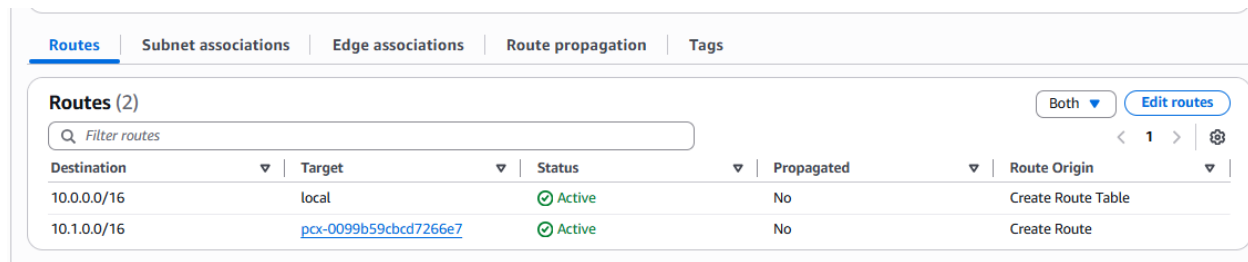
Find peering connections by attribute or tag

Name	Peering connection ID	Status	Requester VPC	Accepter VPC
Peer-MYVPC1-MYVPC2	pcx-0099b59cbcd7266e7	Active	vpc-0c25b0e151a956de5 / MY...	vpc-0cd261808beea97bd / MY..
Peer-MYVPC2-Oregon	pcx-07bb781e04cdc73dd	Pending acceptance	vpc-0cd261808beea97bd / MY...	vpc-084ca28b074c519fb

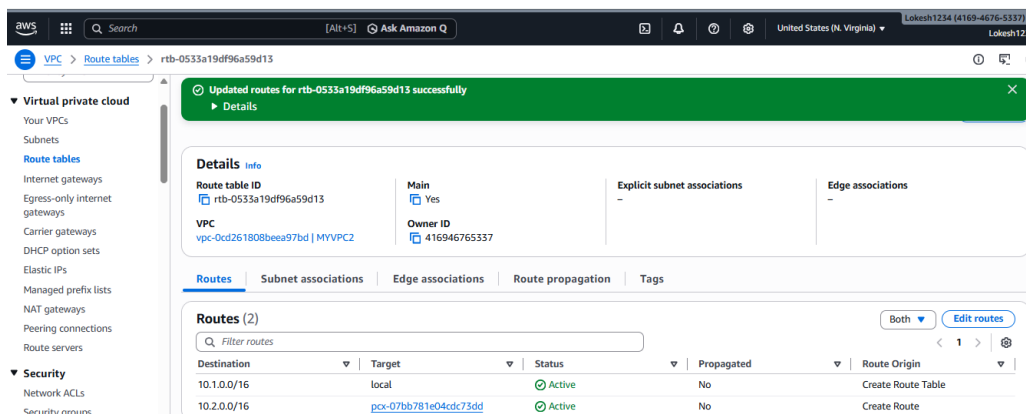
pcx-0099b59cbcd7266e7 / Peer-MYVPC1-MYVPC2



Create route table for the traffic flow on VPC1 and VPC2



Create route table to Oregon VPC from VPC2



aws

Search

[Alt+S]

United States (Oregon)

Lokesh1234 (4169-4676-5337)

Lokesh123

VPC > Route tables > rtb-0d4032cfe57dce1a3

Updated routes for rtb-0d4032cfe57dce1a3 successfully
Details

Route table ID

rtb-0d4032cfe57dce1a3

Main

Yes

Explicit subnet associations

-

Edge associations

-

VPC

vpc-084ca28b074c519fb | VPCOregon1

Owner ID

416946765337

Routes

Subnet associations

Edge associations

Route propagation

Tags

Routes (2)

Both Edit routes

Filter routes

Destination	Target	Status	Propagated	Route Origin
10.1.0.0/16	pcx-07bb781e04cdc73dd	Active	No	Create Route
10.2.0.0/16	local	Active	No	Create Route Table

VPC dashboard

AWS Global View

Filter by VPC

Virtual private cloud

Your VPCs

Subnets

Route tables

Internet gateways

Egress-only internet gateways

Carrier gateways

DHCP option sets

Elastic IPs

Managed prefix lists

Assignment 2

Working for an organization, you are required to provide them with a safe and secure environment for the deployment of their resources. They might require different types of connectivity. Implement the following to fulfill the requirements of the company.

Tasks To Be Performed:

1. Create 2 VPCs in the North Virginia region named MYVPC1 and MYVPC2
2. Create one VPC in the Oregon region named VPCOregon1
3. Create a peering connection between MYVPC1 and MYVPC2
4. Create a peering connection between MYVPC2 and VPCOregon1

Step1 : Create two VPC's one in N virginia and one in oregon

The first screenshot shows the AWS Management Console for the 'United States (N. Virginia)' region. The 'Your VPCs' page displays a table with two VPCs:

Name	VPC ID	State	Encryption c...	Encryption control ...	Block Public...
MYVPC1	vpc-05a20f627aabe3cd6	Available	-	-	Off
MYVPC2	vpc-0305f3e3b4a1528d8	Available	-	-	Off

The second screenshot shows the AWS Management Console for the 'United States (Oregon)' region. The 'Your VPCs' page displays a table with two VPCs:

Name	VPC ID	State	Encryption c...	Encryption control ...	Block Public...
MYVPC1	vpc-03c45d6088d776738	Available	-	-	Off
MYVPC2	vpc-0c07527785527d04c	Available	-	-	Off

Step 2: Create peering b/w VPC1 and VPC2

VPC → Peering Connections → Create

Name: Peering-VPC1-VPC2

Requester VPC: MYVPC1

Acceptor VPC: MYVPC2

Once the peering request is done from the N Virginia region accept the request for peering same on Oregon region.

Assignment 3

Problem Statement:

Working for an organization, you are required to provide them a safe and secure environment for the deployment of their resources. They might require different types of connectivity. Implement the following to fulfill the requirements of the company.

Tasks To Be Performed:

1. Create 2 EC2 instances in any public subnet of any VPC and name them Master and Client.
2. Using security groups, make sure that the Client instance can only be accessed (SSH) through the Master instance.

<input type="checkbox"/>	Client	i-09a04539a99cfc76d	Running	t3.micro	3/3 checks passed	View alarms +	us-east-1a	-
<input checked="" type="checkbox"/>	Master	i-06eed8725b934fd6a	Running	t3.micro	3/3 checks passed	View alarms +	us-east-1a	ec2-

-06eed8725b934fd6a (Master)

[Details](#) | [Status and alarms](#) | [Monitoring](#) | [Security](#) | [Networking](#) | [Storage](#) | [Tags](#)

Instance summary [Info](#)

Instance ID	Public IPv4 address	Private IPv4 addresses
i-06eed8725b934fd6a	3.236.129.242 open address	172.31.7.184

<input checked="" type="checkbox"/>	Client	i-09a04539a99cfc76d	Running	t3.micro	3/3 checks passed	View alarms +	us-east-1a	-
<input type="checkbox"/>	Master	i-06eed8725b934fd6a	Running	t3.micro	3/3 checks passed	View alarms +	us-east-1a	ec2-

i-09a04539a99cfc76d (Client)

Instance summary [Info](#)

Instance ID	Public IPv4 address	Private IPv4 addresses
i-09a04539a99cfc76d	-	172.31.4.176

Connect to the Master Ec2 using the public Ip

```

ec2-user@ip-172-31-7-184:~
C:\Users\lokesht> ssh -i "C:\Users\lokesht\Downloads\aws_prac2.pem" ec2-user@3.236.129.242

#_
~\_#####_      Amazon Linux 2023
~\_#####\
~\_###|
~\_#/_--- https://aws.amazon.com/linux/amazon-linux-2023
~\_V~' '--->
~\_./
~\_/m/'

Last login: Sun Jan 25 09:27:19 2026 from 49.37.171.188
[ec2-user@ip-172-31-7-184 ~]$

```

Copy the pem key to the linux m/c of master instance

```
PS C:\Users\lokesh_ht> scp -i "C:\Users\lokesh_ht\Downloads\aws_prac2.pem" "C:\Users\lokesh_ht\Downloads\aws_prac2.pem"
ec2-user@3.236.129.242:~/
aws_prac2.pem
100% 1834      7.5KB/s   00:00
PS C:\Users\lokesh_ht>
```

Change the permission for pem key

```
Last login: Sun Jan 25 09:45:50 2026 from 49.37.171.188
[ec2-user@ip-172-31-7-184 ~]$ chmod 400 aws_prac2.pem
[ec2-user@ip-172-31-7-184 ~]$
```

Connect to the Client Ec2 instance using the private key

```
[ec2-user@ip-172-31-7-184 ~]$ ssh -i aws_prac2.pem ec2-user@172.31.4.176
```

```
#_
~\ #####_      Amazon Linux 2023
~~ \#####\
~~ \###|
~~ \#/ --- https://aws.amazon.com/linux/amazon-linux-2023
~~ V~' '->
    NNNN
      .-.
     _/_/_/_/_
    _/m/'
```

```
Last login: Sun Jan 25 09:44:02 2026 from 172.31.7.184
[ec2-user@ip-172-31-4-176 ~]$
```

Assignment 4

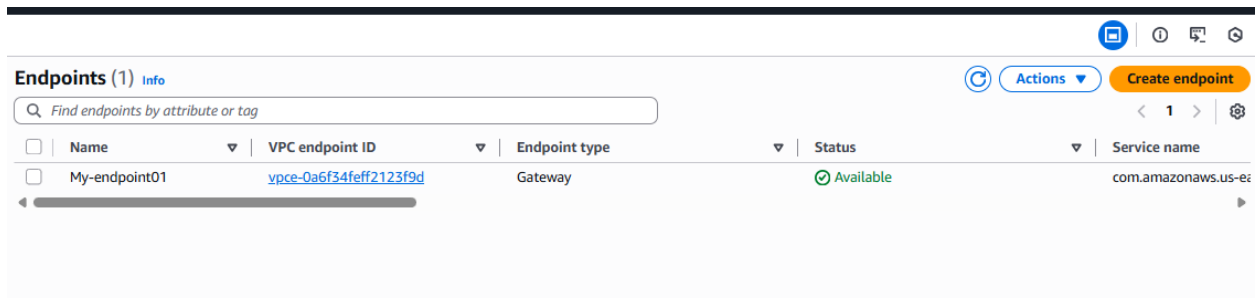
Problem Statement:

Working for an organization, you are required to provide them a safe and secure environment for the deployment of their resources. They might require different types of connectivity. Implement the following to fulfill the requirements of the company.

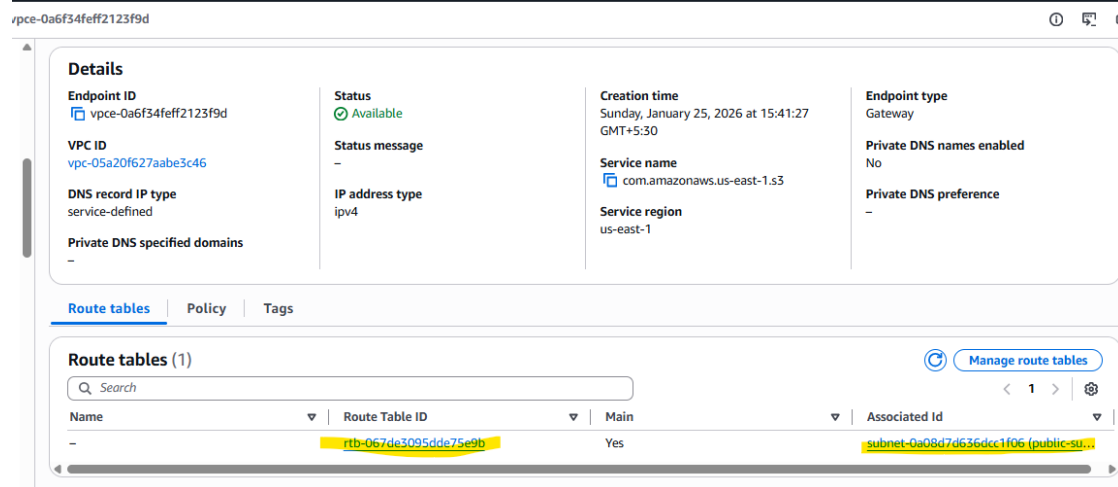
Tasks To Be Performed:

1. Create a VPC endpoint for a S3 bucket of your choice for secure access to the files.

Create a Gateway VPC Endpoint for S3



Choose the route tables associated with the subnets where your EC2 instances run.



Attach a policy (IAM-like JSON) to control access. Example: allow full S3 access:

```
{
  "Statement": [
    {
      "Action": "*",
      "Effect": "Allow",
      "Resource": "*",
      "Principal": "*"
    }
  ]
}
```

In the S3 bucket policy, restrict access to only requests coming via the VPC endpoint.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Principal": "*",
```

```
"Action": "s3:*",
"Effect": "Allow",
"Resource": [
  "arn:aws:s3:::my-secure-bucket",
  "arn:aws:s3:::my-secure-bucket/*"
],
"Condition": {
  "StringEquals": {
    "aws:SourceVpce": "vpce-1234567890abcdef0"
  }
}
}
```

Test Connectivity

```
An error occurred (AccessDenied) when calling the ListObjectsV2 operation: Access Denied
[ec2-user@ip-172-31-7-184 ~]$ [ec2-user@ip-172-31-7-184 ~]$ aws s3 ls s3://my-secure-bucket --region us-east-1
An error occurred (AccessDenied) when calling the ListObjectsV2 operation: Access Denied^C
```

Assignment 5

Problem Statement:

You work for XYZ Corporation and based on the expansion requirements of your corporation you have been asked to create and set up a distinct Amazon VPC for the production and development team. You are expected to perform the following tasks for the respective VPCs.

Production Network:

1. Design and build a 4-tier architecture.
2. Create 5 subnets out of which 4 should be private named app1, app2, dbcache and db and one should be public, named web.
3. Launch instances in all subnets and name them as per the subnet that they have been launched in.
4. Allow dbcache instance and app1 subnet to send internet requests.
5. Manage security groups and NACLs.

Development Network:

1. Design and build 2-tier architecture with two subnets named web and db and launch instances in both subnets and name them as per the subnet names.
2. Make sure only the web subnet can send internet requests.
3. Create peering connection between production network and development network.
4. Setup connection between db subnets of both production network and development network respectively.