

Module 4 -VPC

CASE STUDY

Production Network:

1. Design and build a 4 tier architecture
2. Create 5 subnets out of which 4 should be private with names 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

→ Creation of VPC

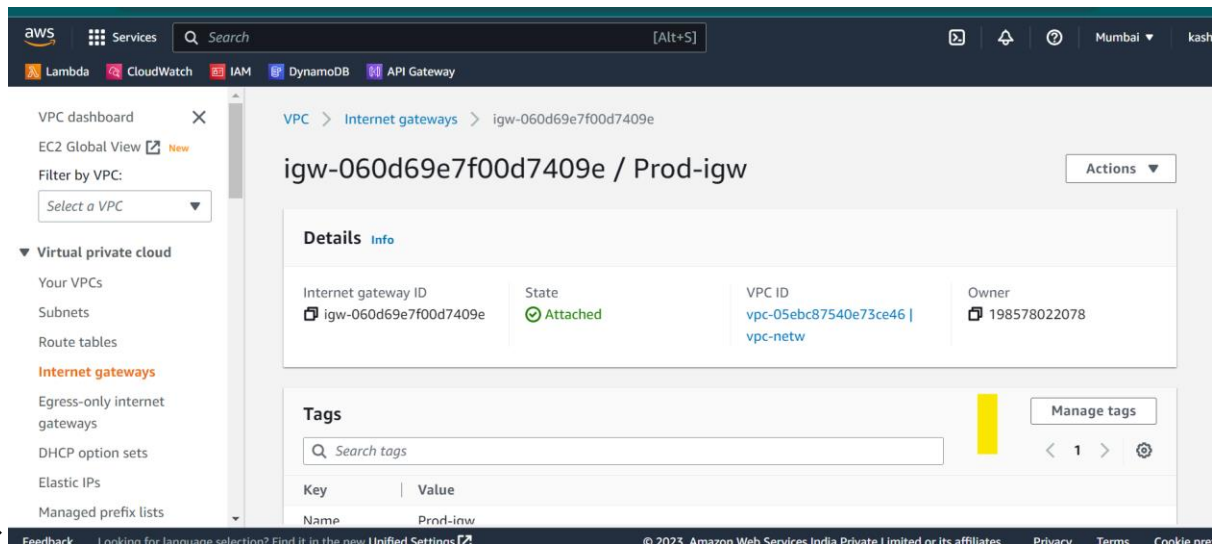
The screenshot displays the AWS VPC console. The top section shows the VPC details for 'vpc-05ebc87540e73ce46 / vpc-netw'. The details include:

- VPC ID: vpc-05ebc87540e73ce46
- State: Available
- Tenancy: Default
- Default VPC: No
- Network Address Usage metrics: Disabled
- DNS hostnames: Disabled
- DNS resolution: Enabled
- DHCP option set: dopt-0127b17658b277c29
- IPv4 CIDR: 10.10.0.0/16
- Main route table: rtb-03522246d3dcf470a
- Main network ACL: acl-0a1d7bd1b4c44312b
- IPv6 pool: -
- IPv6 CIDR (Network border group): -
- Owner ID: 198578022078

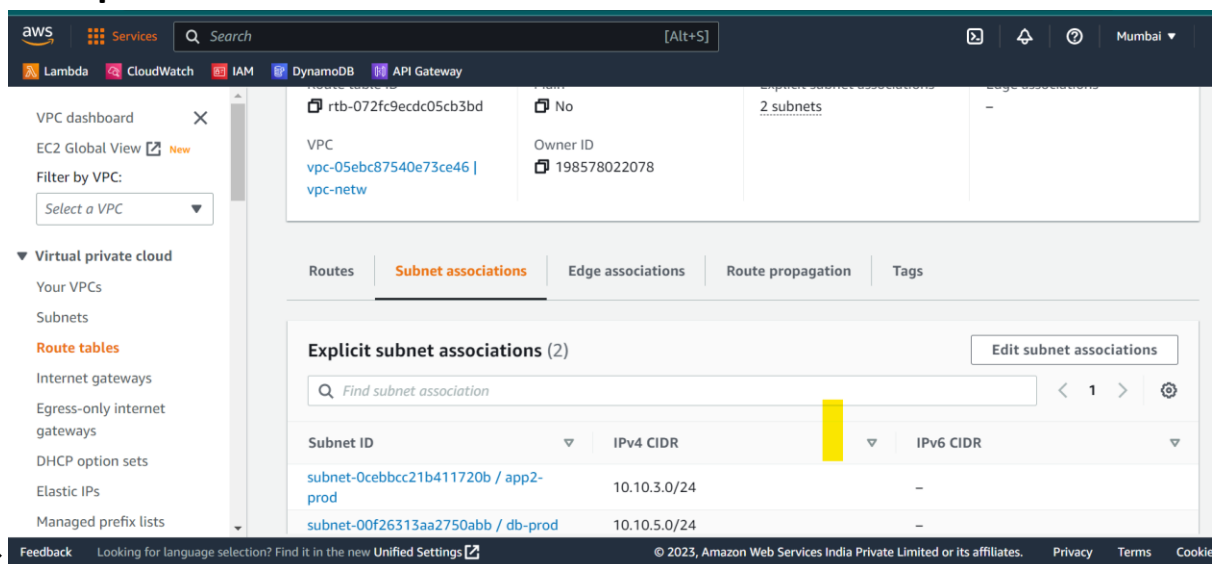
The bottom section shows the 'Subnets (8)' list. The subnets are:

| Name | Subnet ID | State | VPC | IPv4 CIDR |
|--------------|--------------------------|-----------|--------------------------------|----------------|
| dbcache-prod | subnet-0d7407c8e9e69113a | Available | vpc-05ebc87540e73ce46 vpc... | 10.10.4.0/24 |
| app1-Prod | subnet-0625da0b22ee7cb4c | Available | vpc-05ebc87540e73ce46 vpc... | 10.10.2.0/24 |
| app2-prod | subnet-0cebbcc21b411720b | Available | vpc-05ebc87540e73ce46 vpc... | 10.10.3.0/24 |
| - | subnet-0dec31e59c5d819ad | Available | vpc-0317a17da6df51281 | 172.31.16.0/24 |
| db-prod | subnet-00f26313aa2750abb | Available | vpc-05ebc87540e73ce46 vpc... | 10.10.5.0/24 |
| WEB-prod | subnet-00e18562557523aed | Available | vpc-05ebc87540e73ce46 vpc... | 10.10.1.0/24 |
| - | subnet-069dd5df06cc241ff | Available | vpc-0317a17da6df51281 | 172.31.32.0/24 |
| - | subnet-0749d5bc2810a3088 | Available | vpc-0317a17da6df51281 | 172.31.0.0/24 |

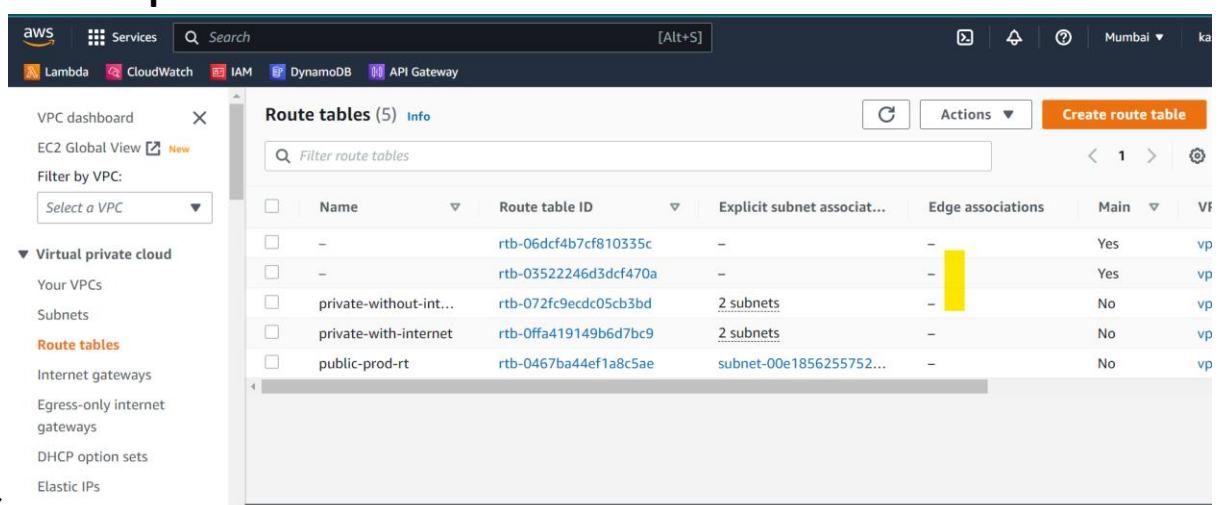
→ The creation of 5 subnets and WEB-prod is the only public subnet .



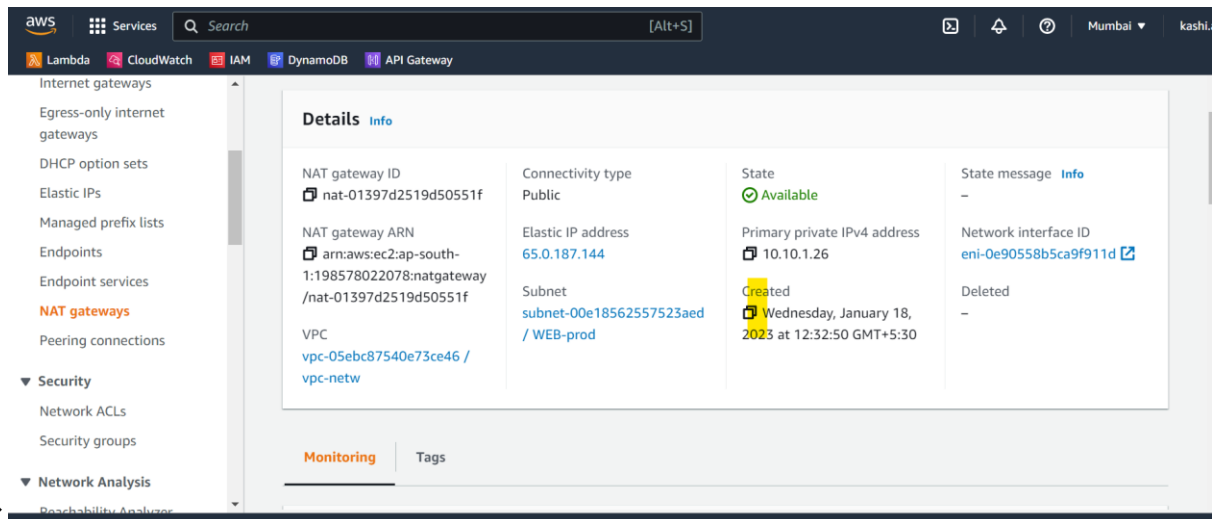
→ Internet gateway for Internet connection and attached to web-prod.



→ Route Table with internet and associated 2 subnets app2-prod and DB-prod



→ 3 Route tables are created and associated with subnets .

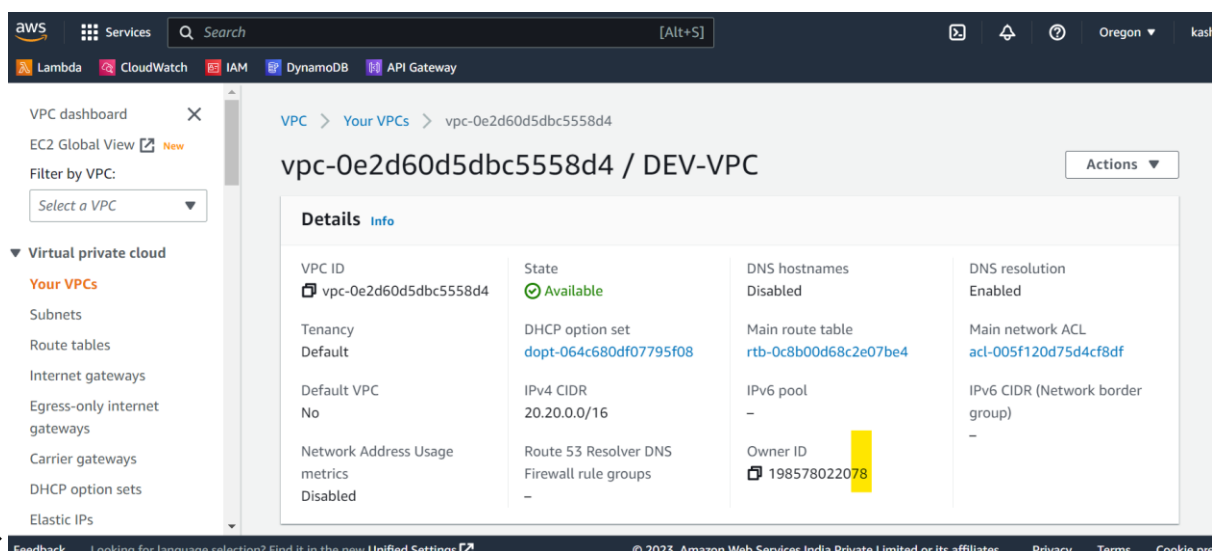


→ **NAT Gateway is created for web-prod(public) as to communicate with private instances once created .**

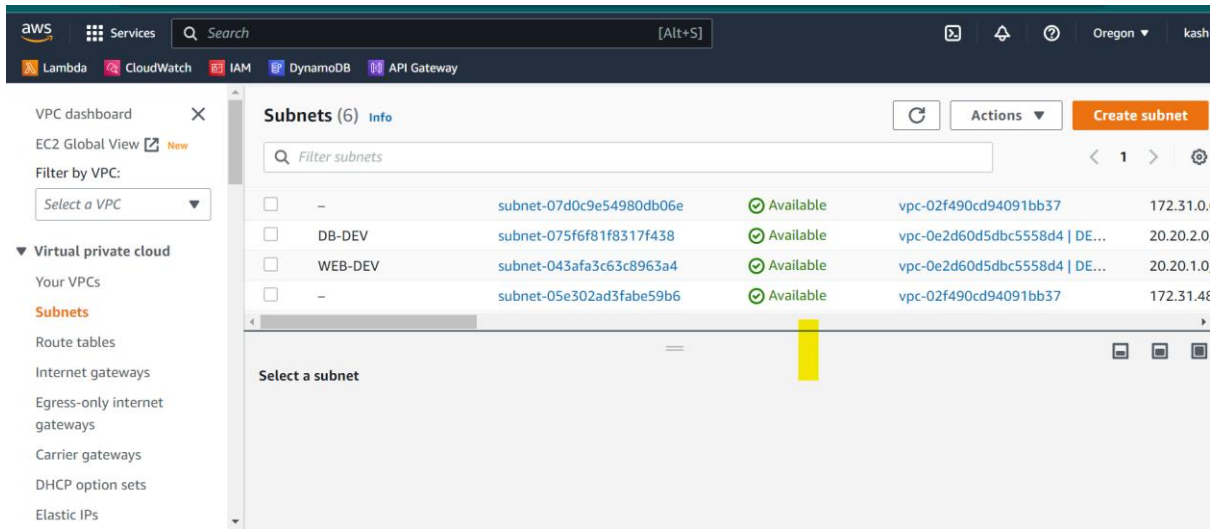
Development Network:

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 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

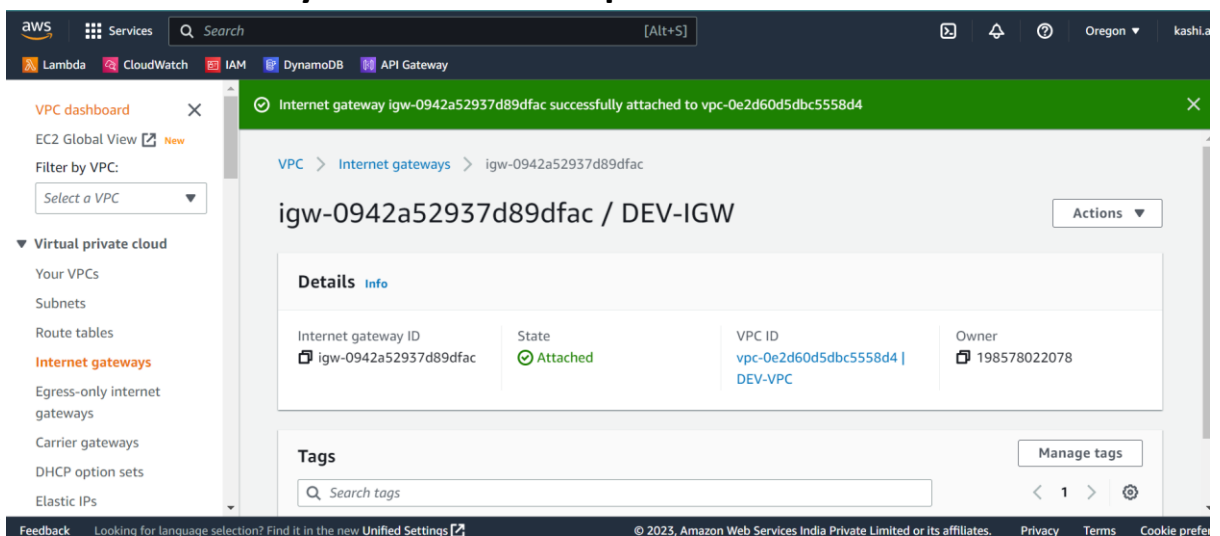
→ Created a VPC



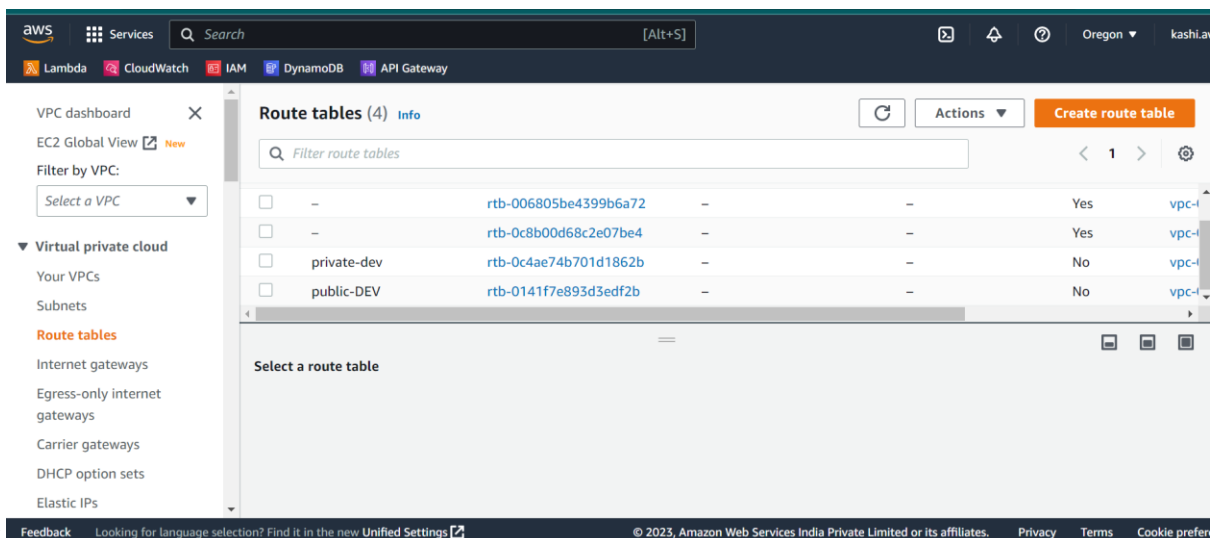
→ **WITH 2 subnets**



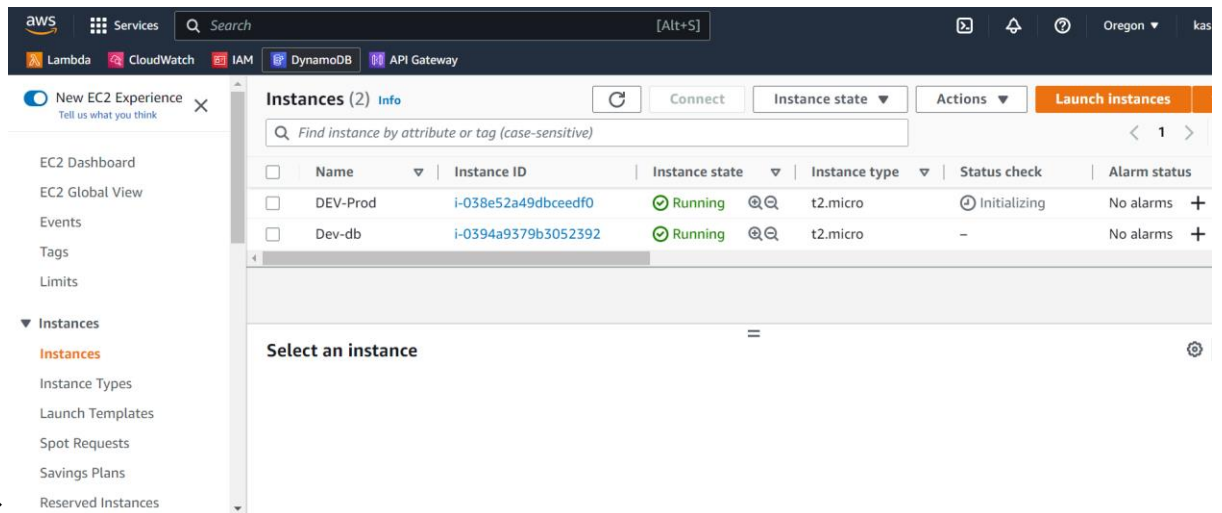
Internet Gateway with attached vpc



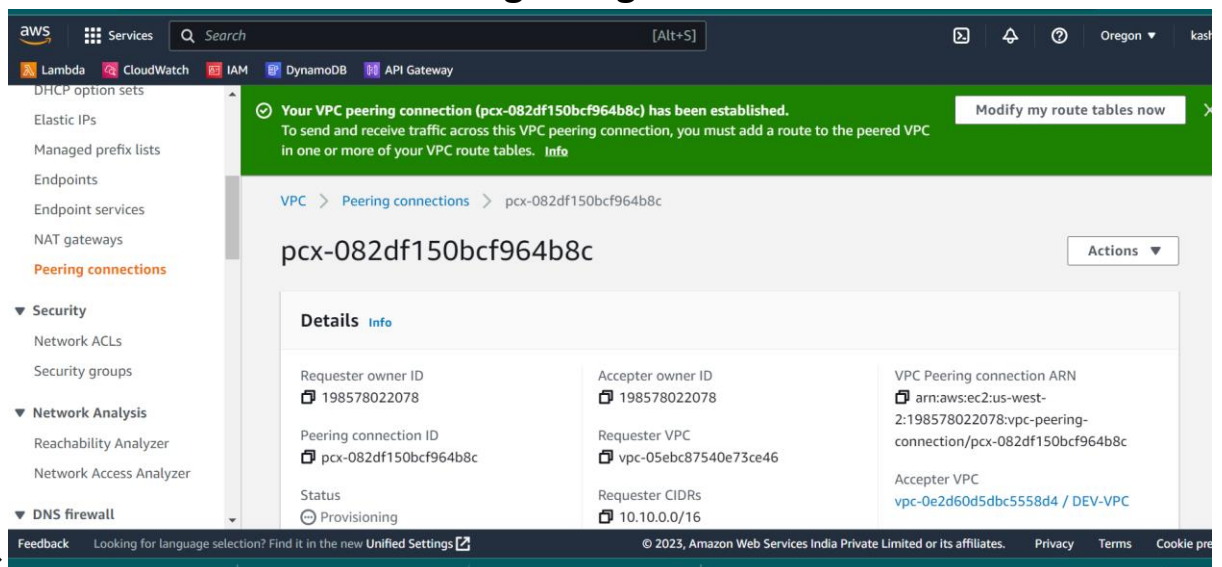
Route tables



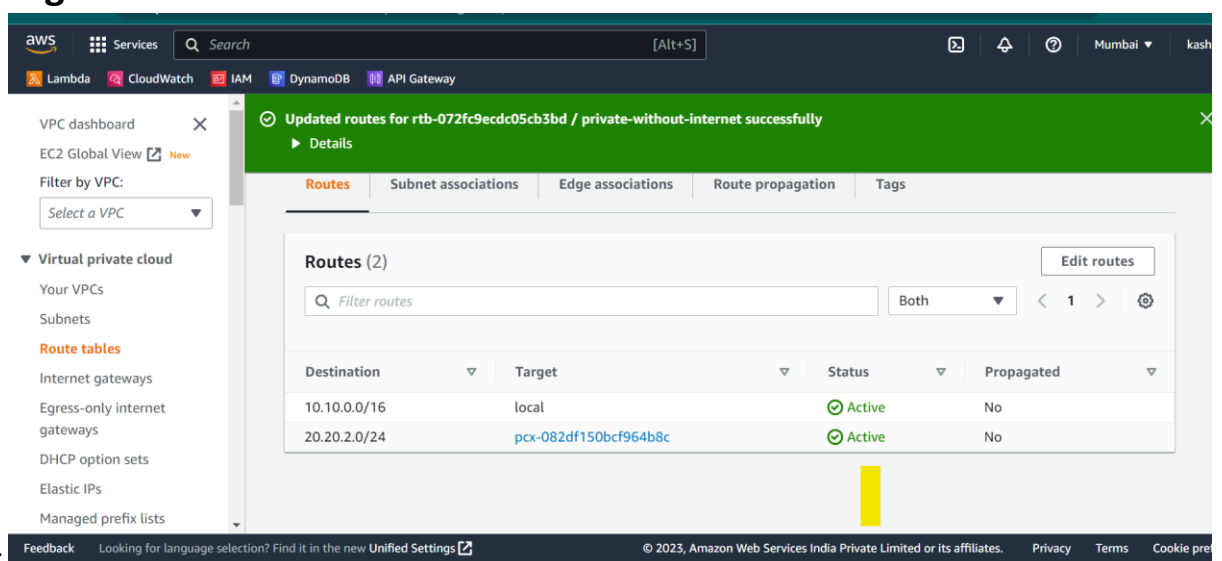
Public route table is associated with dev-prod subnet and connected with Internet Gateway



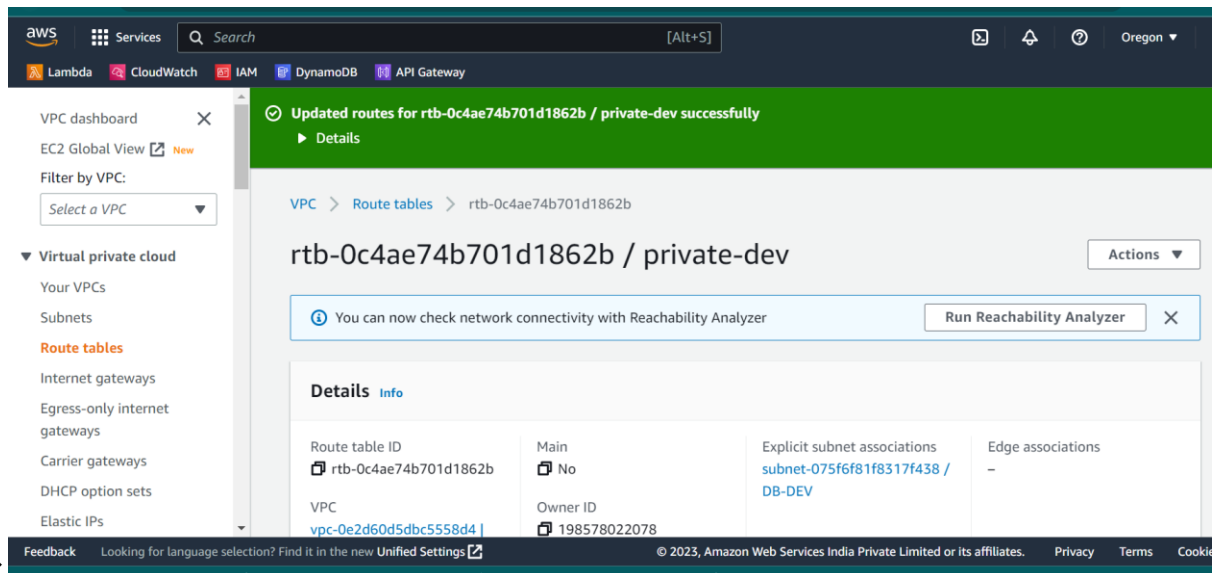
→
→ Instances are created in Oregon region



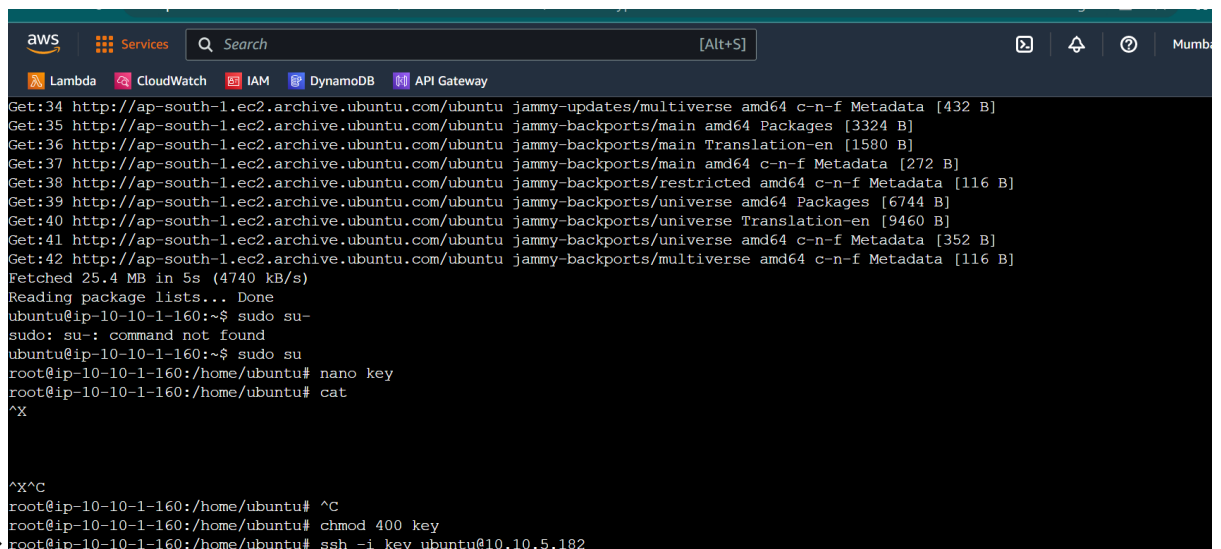
→
→ Created Peering connection between Oregon and Mumbai region and



→



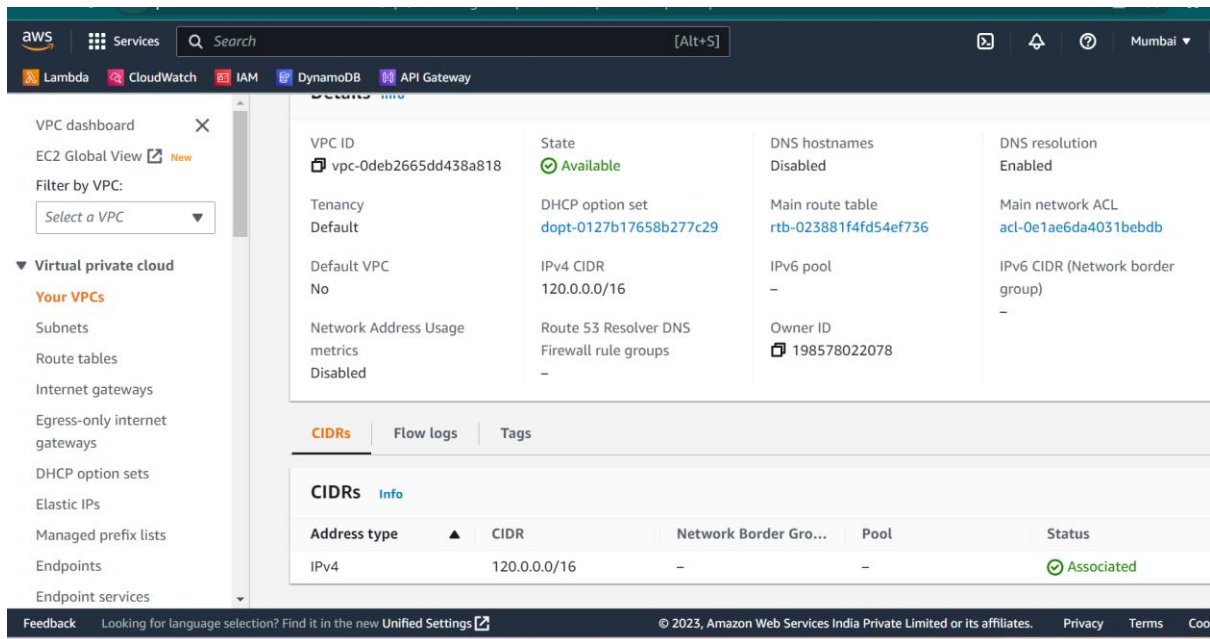
→ Route table is edited with the route



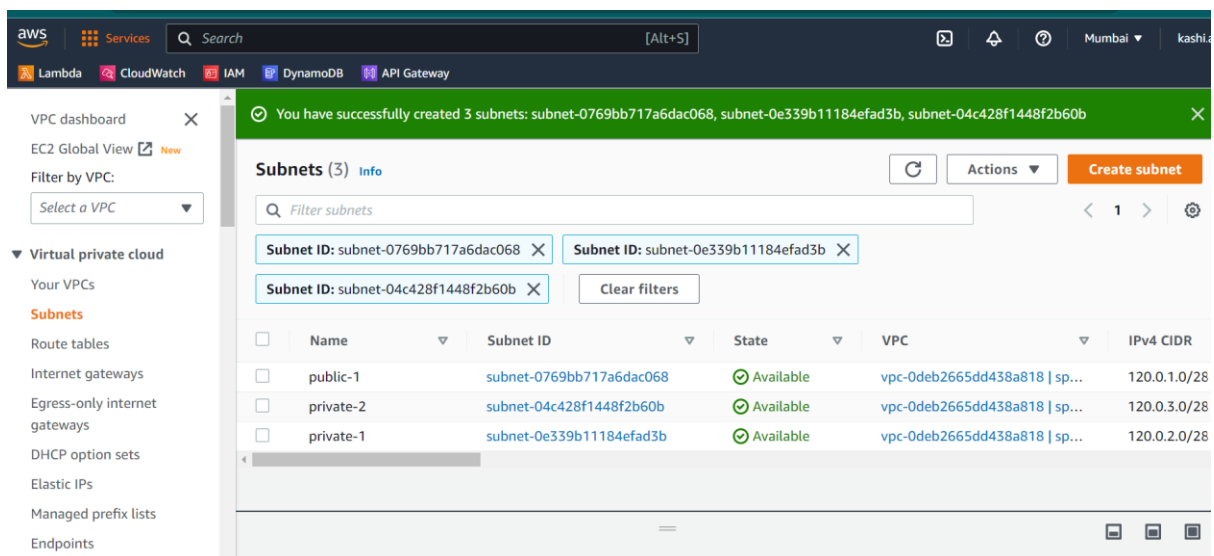
→ Same is checked by using ping for Oregon

Assignment -1

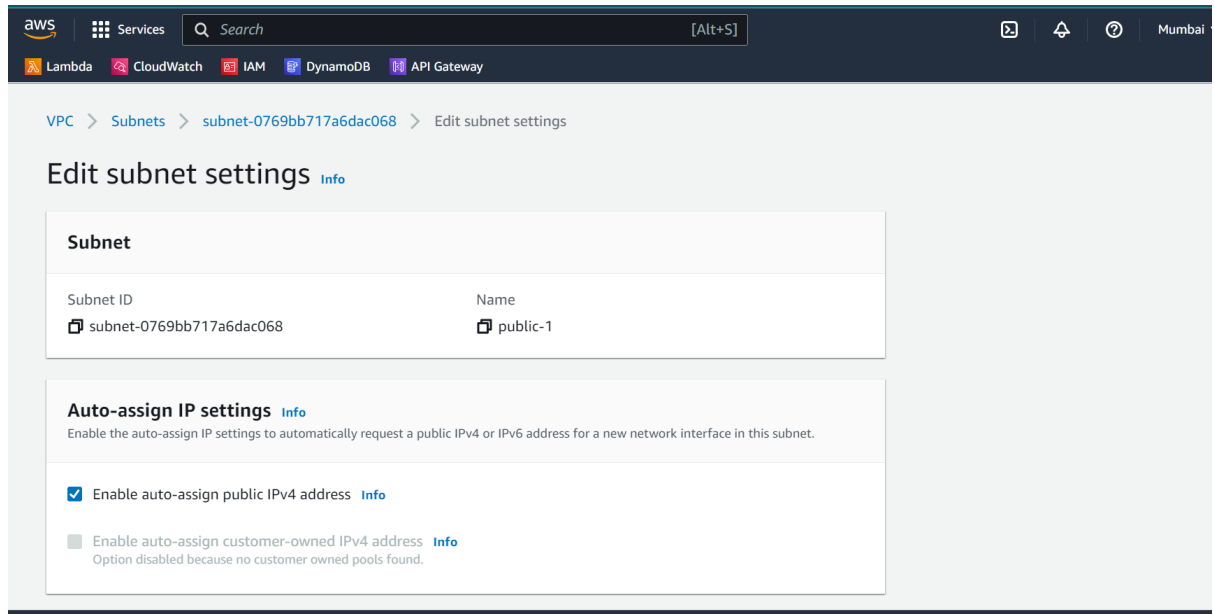
1. Create VPC With 120.0.0.0/16 CIDR Block



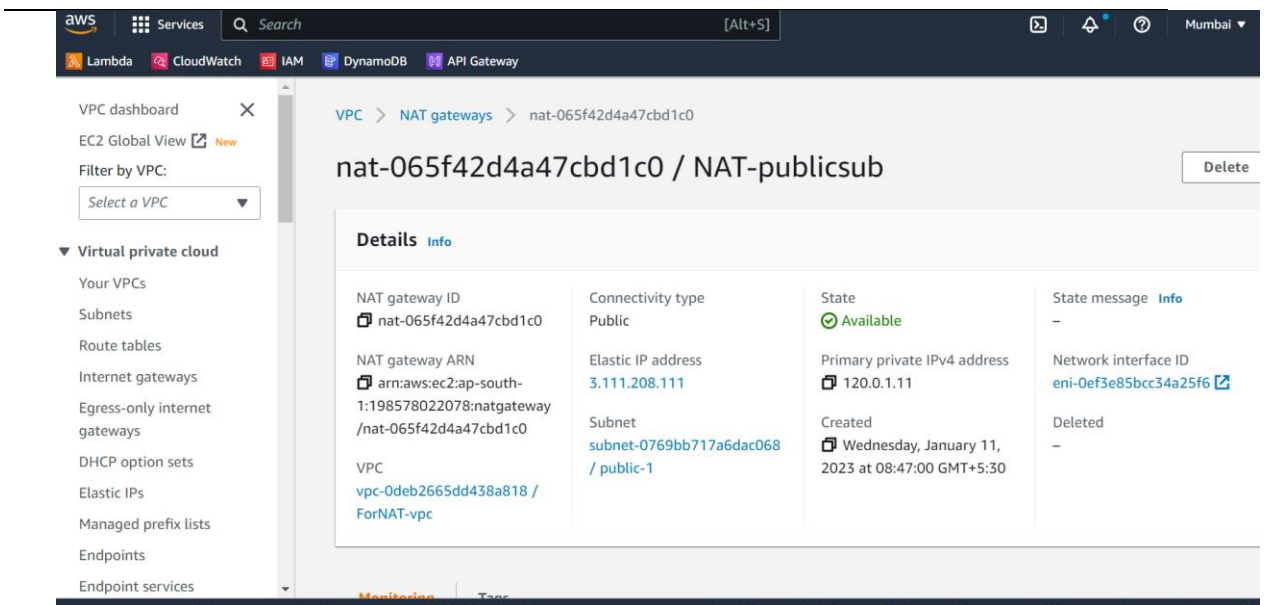
2.Create 1 public and 2 private subnet and NAT gateway for private subnet .



➔ 2 private and 1 public subnet are created with IPV4 CIDR



- ➔ The public subnet is enabled to receive IPV4 / IPV6 addresses publicly
- Creating NAT Gateway in the public subnet for the private subnets to communicate with internet.



VPC dashboard

EC2 Global View

Filter by VPC:

Virtual private cloud

Your VPCs

Subnets

Route tables

Internet gateways

Egress-only internet gateways

DHCP option sets

Elastic IPs

Managed prefix lists

Endpoints

Endpoint services

VPC > Your VPCs > vpc-0deb2665dd438a818

vpc-0deb2665dd438a818 / ForNAT-vpc

Actions

Details Info

| | | | |
|---|---|---|---|
| VPC ID vpc-0deb2665dd438a818 | State Available | DNS hostnames Disabled | DNS resolution Enabled |
| Tenancy Default | DHCP option set dopt-0127b17658b277c29 | Main route table rtb-023881f4fd54ef736 | Main network ACL acl-0e1ae6da4031bebdb |
| Default VPC No | IPv4 CIDR 120.0.0.0/16 | IPv6 pool - | IPv6 CIDR (Network border group) - |
| Network Address Usage metrics Disabled | Route 53 Resolver DNS Firewall rule groups - | Owner ID 198578022078 | |

CIDRs Flow logs Tags

Feedback Looking for language selection? Find it in the new Unified Settings

© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cooki

Your VPCs

Subnets

Route tables

Internet gateways

Egress-only internet gateways

DHCP option sets

Elastic IPs

Managed prefix lists

Endpoints

Endpoint services

| | | | | | | |
|--------------------------|------------------|-----------------------|-------------------------|---|----|------|
| <input type="checkbox"/> | rt-in-privateSub | rtb-0ba64b440d4303ddc | 2 subnets | - | No | vpc- |
| <input type="checkbox"/> | rt-in-pubSubnet | rtb-0065fe7b074b117c9 | subnet-0769bb717a6da... | - | No | vpc- |

Select a route table

See "man sudo_root" for details.

```
ubuntu@ip-120-0-1-5:~$ ping
ping: usage error: Destination address required
ubuntu@ip-120-0-1-5:~$ ping 120.0.2.7
PING 120.0.2.7 (120.0.2.7) 56(84) bytes of data.
64 bytes from 120.0.2.7: icmp_seq=1 ttl=64 time=0.732 ms
64 bytes from 120.0.2.7: icmp_seq=2 ttl=64 time=0.528 ms
64 bytes from 120.0.2.7: icmp_seq=3 ttl=64 time=0.447 ms
64 bytes from 120.0.2.7: icmp_seq=4 ttl=64 time=0.551 ms
64 bytes from 120.0.2.7: icmp_seq=5 ttl=64 time=0.538 ms
64 bytes from 120.0.2.7: icmp_seq=6 ttl=64 time=0.488 ms
64 bytes from 120.0.2.7: icmp_seq=7 ttl=64 time=0.497 ms
64 bytes from 120.0.2.7: icmp_seq=8 ttl=64 time=0.505 ms
64 bytes from 120.0.2.7: icmp_seq=9 ttl=64 time=0.530 ms
64 bytes from 120.0.2.7: icmp_seq=10 ttl=64 time=1.39 ms
^C
--- 120.0.2.7 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9217ms
rtt min/avg/max/mdev = 0.447/0.620/1.386/0.265 ms
ubuntu@ip-120-0-1-5:~$
```

i-082f6fab9c210faa3 (ec2-public)

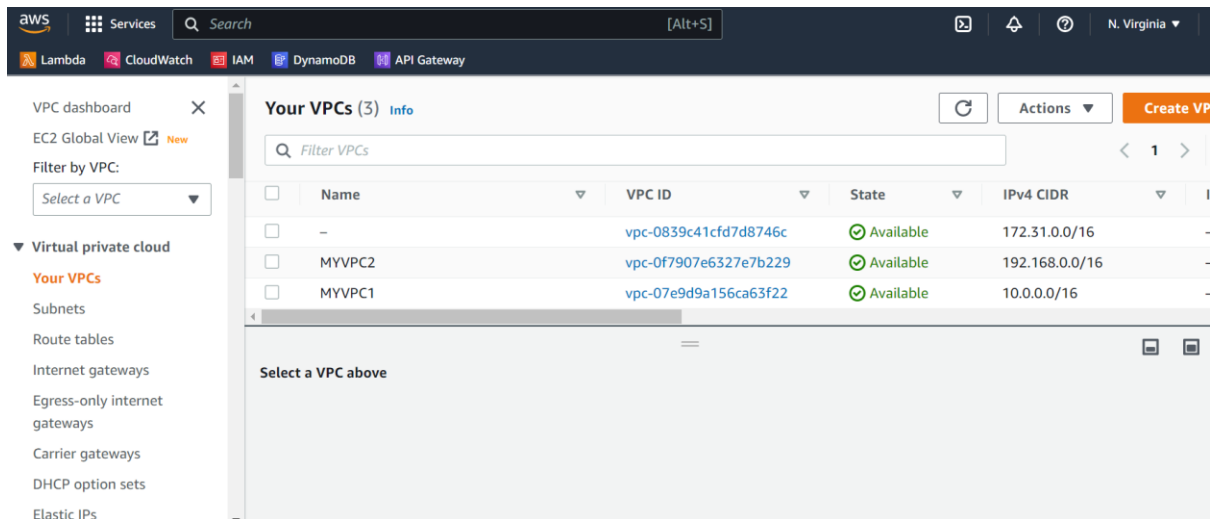
PublicIPs: 13.234.231.65 PrivateIPs: 120.0.1.5

Feedback Looking for language selection? Find it in the new Unified Settings

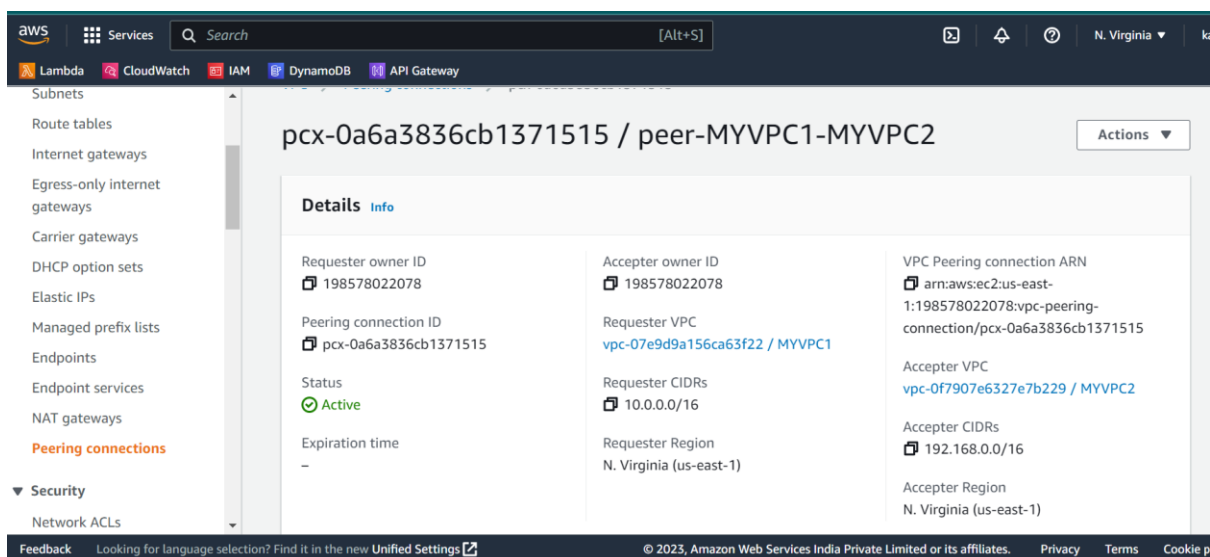
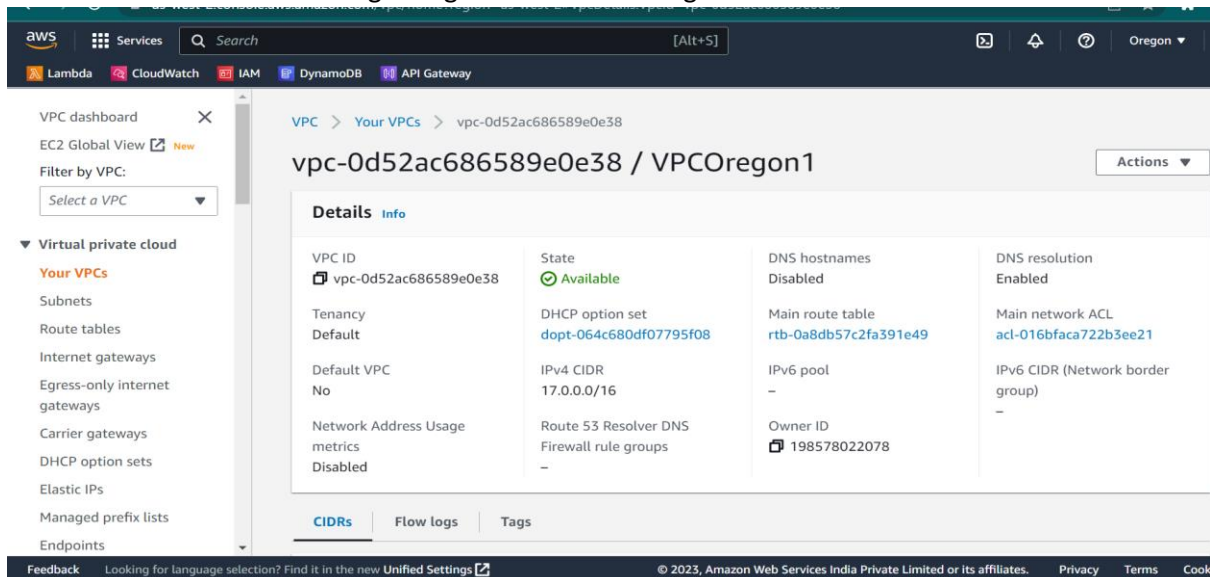
© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cooki

Assignment 2

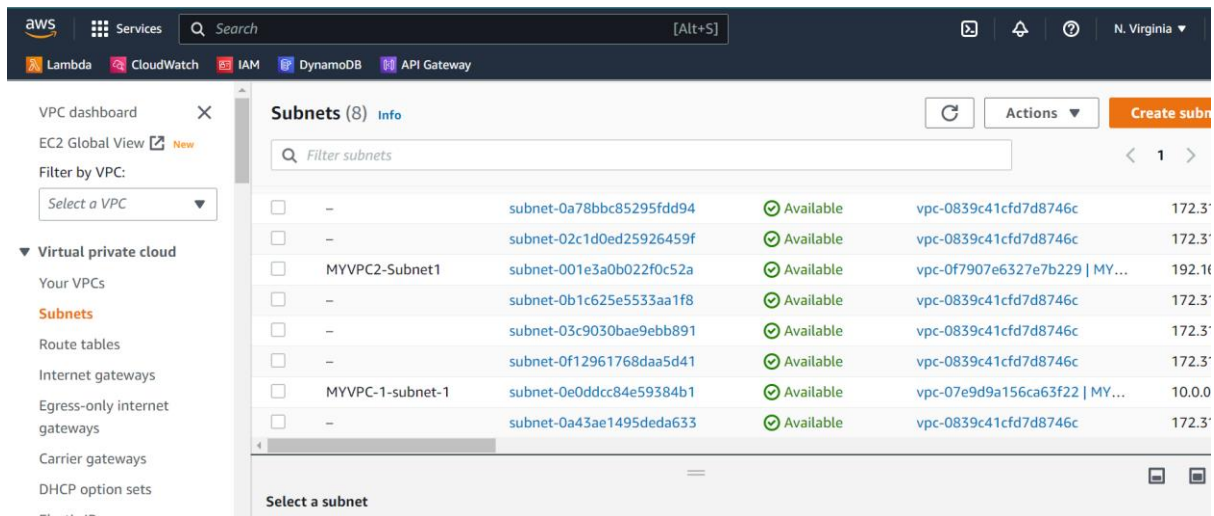
1. Creating 2 vpc in n.verginia MYVPC1 and MYVPCC2



2. Create one VPC in Oregon region named VPCOregon1



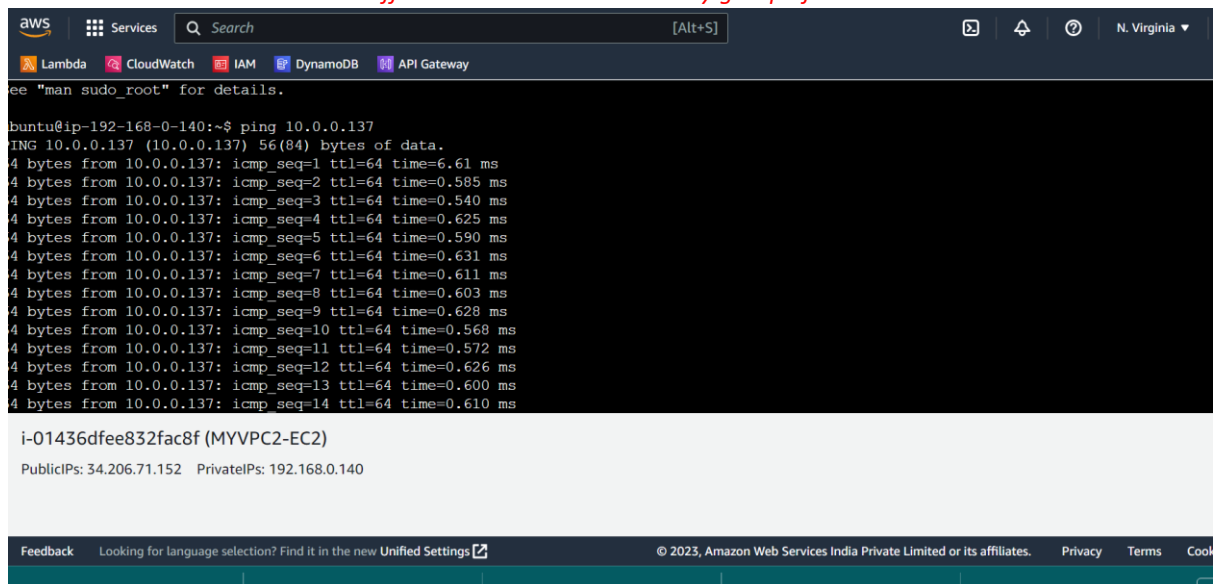
- ➔ Created 2 vpc MYVPC1 and MYVPC2 .
- ➔ Created subnet in both the VPC



- ➔ Created Internet Gateway and route table respectively and with the help of ping command done the communication between peers MYVPC1 and MYVPC2

ERROR Faced 1 – peering gateway connection was not done in the route table

ERROR Faced2 – ICMP traffic was allowed in the security group of the instances



➔

```
aws
Services
Search [Alt+S]
N. Virginia
Lambda CloudWatch IAM DynamoDB API Gateway

buntu@ip-10-0-0-137:~$ ping 192.168.0.140
PING 192.168.0.140 (192.168.0.140) 56(84) bytes of data.
4 bytes from 192.168.0.140: icmp_seq=1 ttl=64 time=1.26 ms
4 bytes from 192.168.0.140: icmp_seq=2 ttl=64 time=0.534 ms
4 bytes from 192.168.0.140: icmp_seq=3 ttl=64 time=0.595 ms
4 bytes from 192.168.0.140: icmp_seq=4 ttl=64 time=0.569 ms
4 bytes from 192.168.0.140: icmp_seq=5 ttl=64 time=0.578 ms
4 bytes from 192.168.0.140: icmp_seq=6 ttl=64 time=0.620 ms
4 bytes from 192.168.0.140: icmp_seq=7 ttl=64 time=0.573 ms
4 bytes from 192.168.0.140: icmp_seq=8 ttl=64 time=0.593 ms
4 bytes from 192.168.0.140: icmp_seq=9 ttl=64 time=0.578 ms
4 bytes from 192.168.0.140: icmp_seq=10 ttl=64 time=0.592 ms
4 bytes from 192.168.0.140: icmp_seq=11 ttl=64 time=0.559 ms
4 bytes from 192.168.0.140: icmp_seq=12 ttl=64 time=0.604 ms
4 bytes from 192.168.0.140: icmp_seq=13 ttl=64 time=0.544 ms
4 bytes from 192.168.0.140: icmp_seq=14 ttl=64 time=0.571 ms
4 bytes from 192.168.0.140: icmp_seq=15 ttl=64 time=0.590 ms

i-0484062cc13fe270d (MYVPC1-EC2)
PublicIPs: 3.216.132.185 PrivateIPs: 10.0.0.137

Feedback Looking for language selection? Find it in the new Unified Settings
© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms C
VPC-2.ppk ^ VP1.ppk ^ MYVPC2.pem ^ MYVPC1.pem ^
```

→
→ The connection is successful.