**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 NA

1.Create Production VPC (cidr - 10.10.0.0/16)

**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.

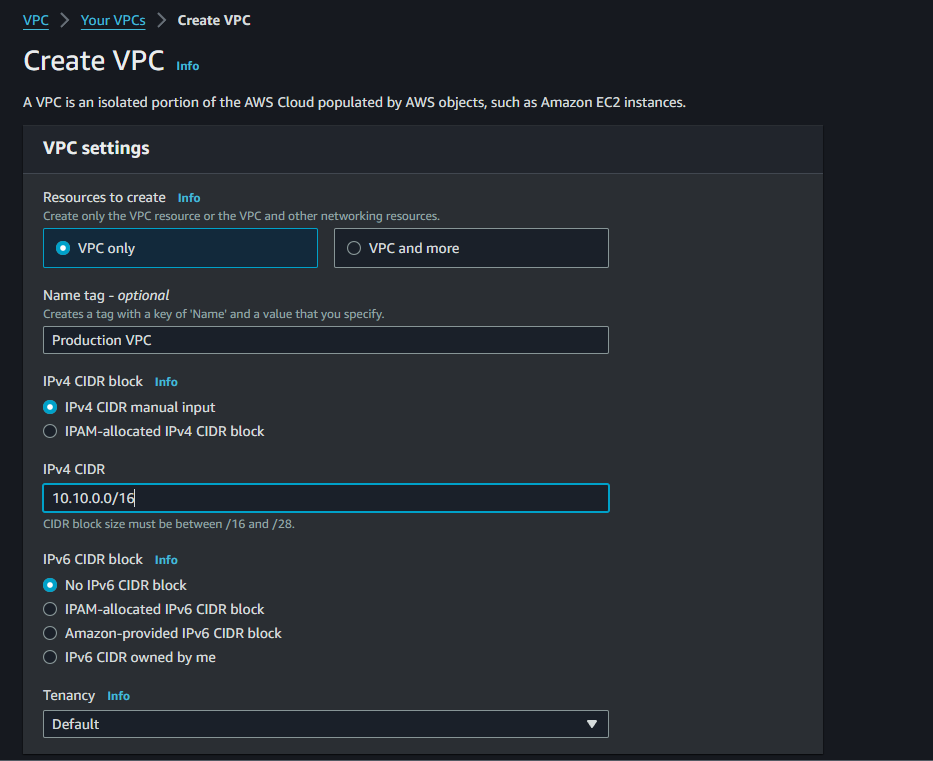
4. Setup connection between db subnets of both production network and development network respectively.

**Step by step demonstration:**

**Note:** I have performed all the tasks through AWS console. You can use Cloud formation/Terraform/CLI for resource creation.

There are EC2 instances which have been created on private subnets so directly we can't perform SSH. For making connections I used the Jump server/Bastion host concept. You may refer to any youtube video for explanation:

1.Create Production VPC (cidr - 10.10.0.0/16)



2. Create 5 Subnets in it

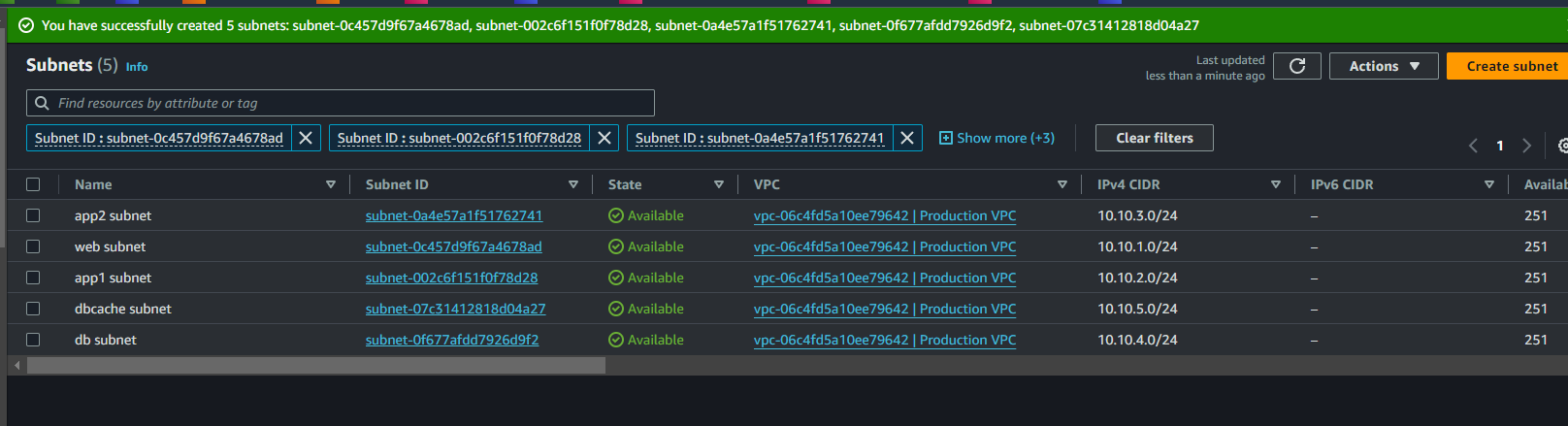
- web subnet [public] (cidr - 10.10.1.0/24)

- app1 subnet [private] (cidr - 10.10.2.0/24)

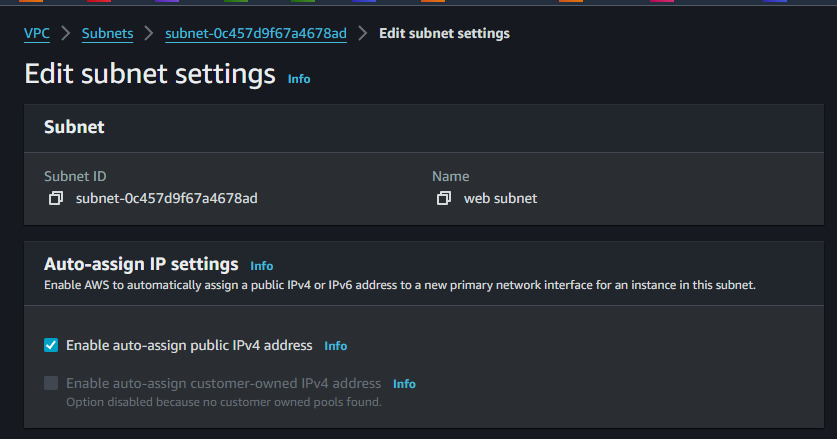
- app2 subnet [private] (cidr - 10.10.3.0/24)

- db subnet [private] (cidr - 10.10.4.0/24)

- dbcache subnet [private] (cidr - 10.10.5.0/24)



- Select web subnet > Go to Action > Edit Subnet setting > Enable Auto Assign IPv4.



3. Create Internet Gateway (Prod-IGW) and attach it to Prod VPC.



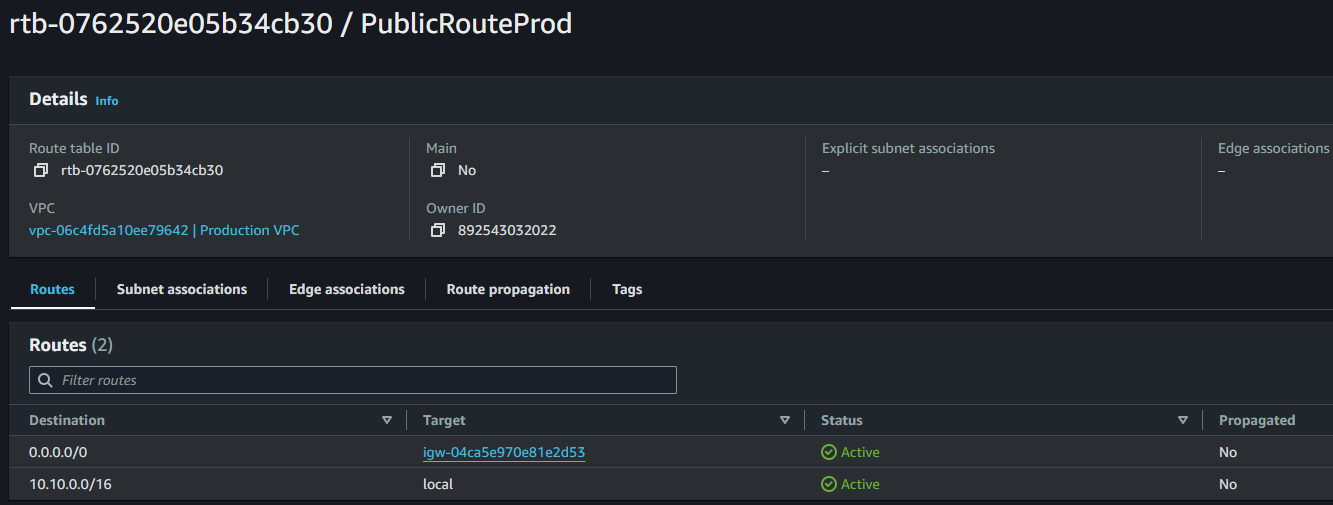
4. Create Public Route Table

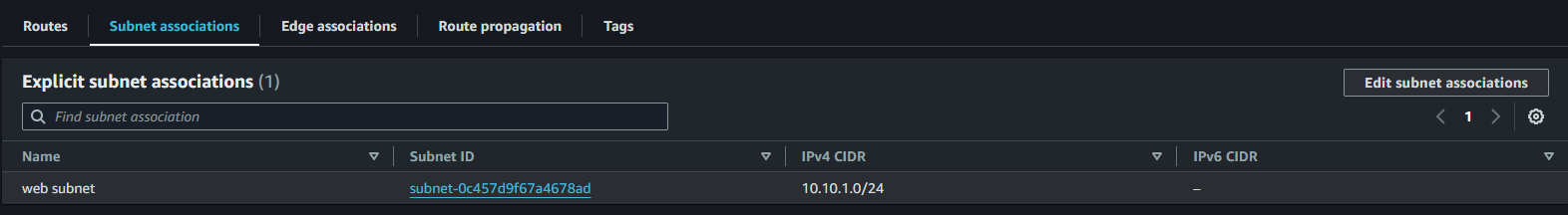
- edit routes

- destination - 0.0.0.0/0

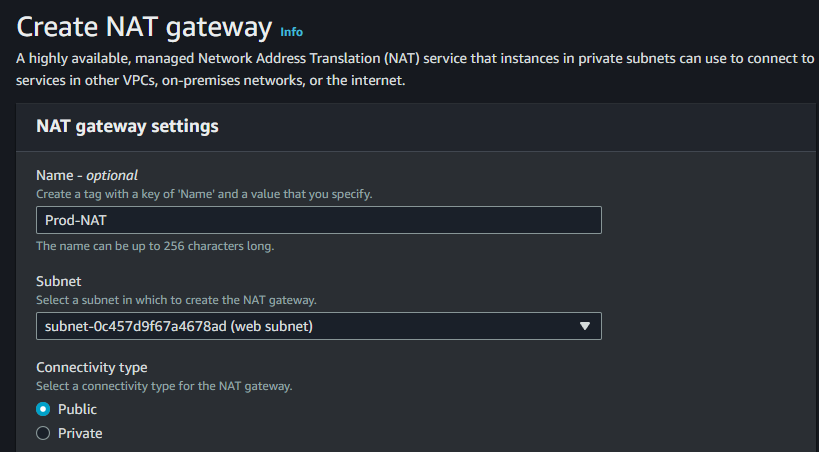
- target - internet gateway (Prod-IGW)

- subnet association - web subnet





5. Create NAT Gateway [in web subnet] (Prod-NAT)



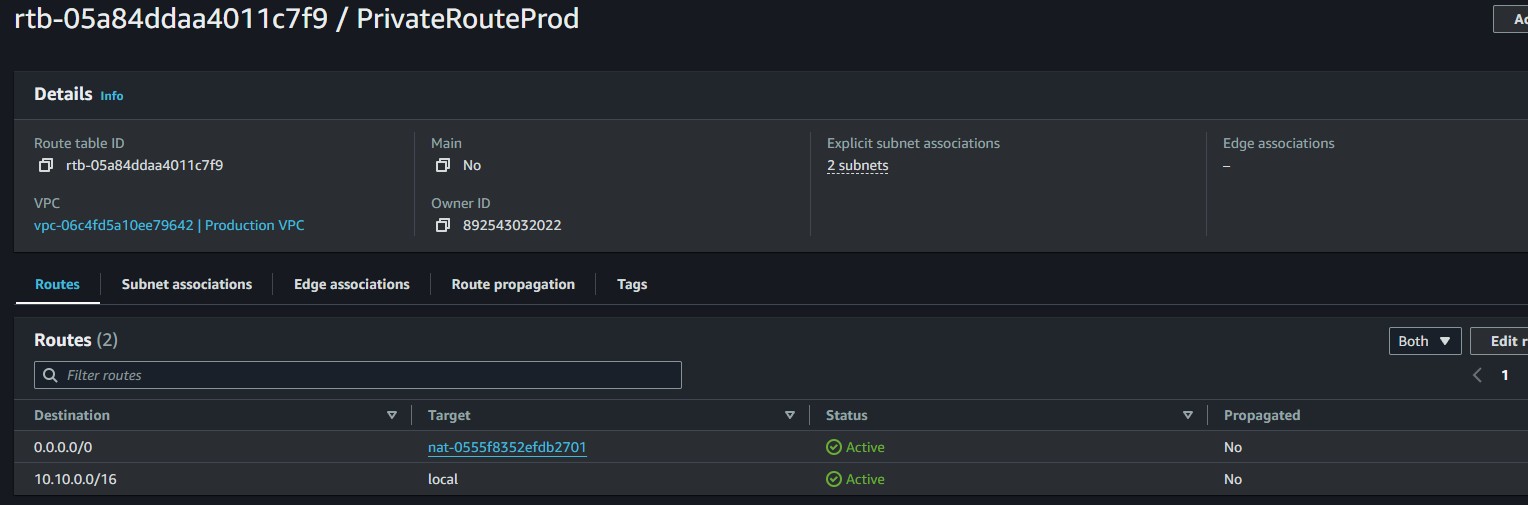
6. Create Private Route Table

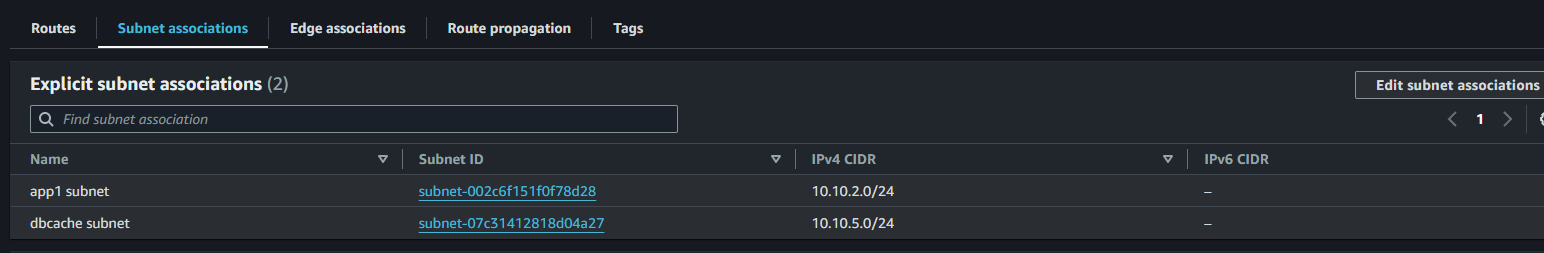
- edit routes

- destination - 0.0.0.0/0

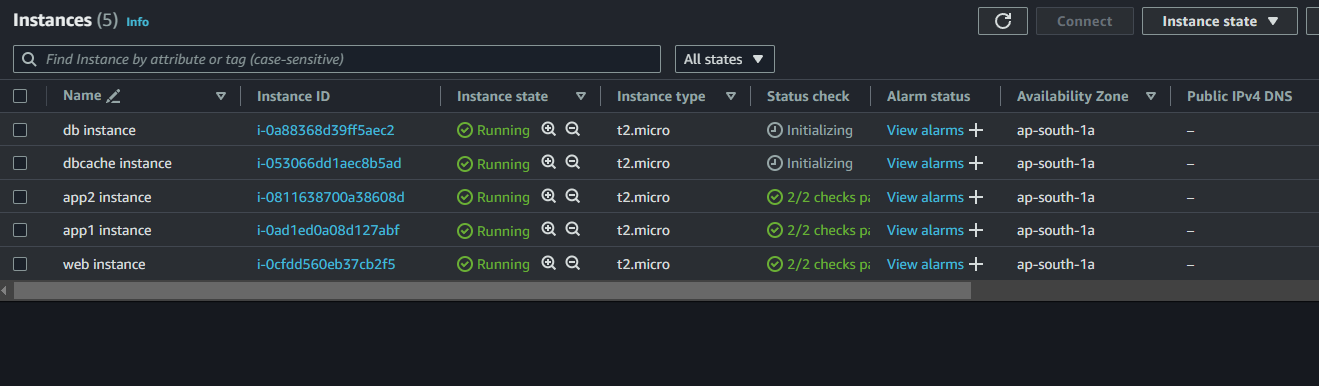
- target - nat gateway (Prod-NAT)

- subnet association - app1 subnet and dbcache subnet

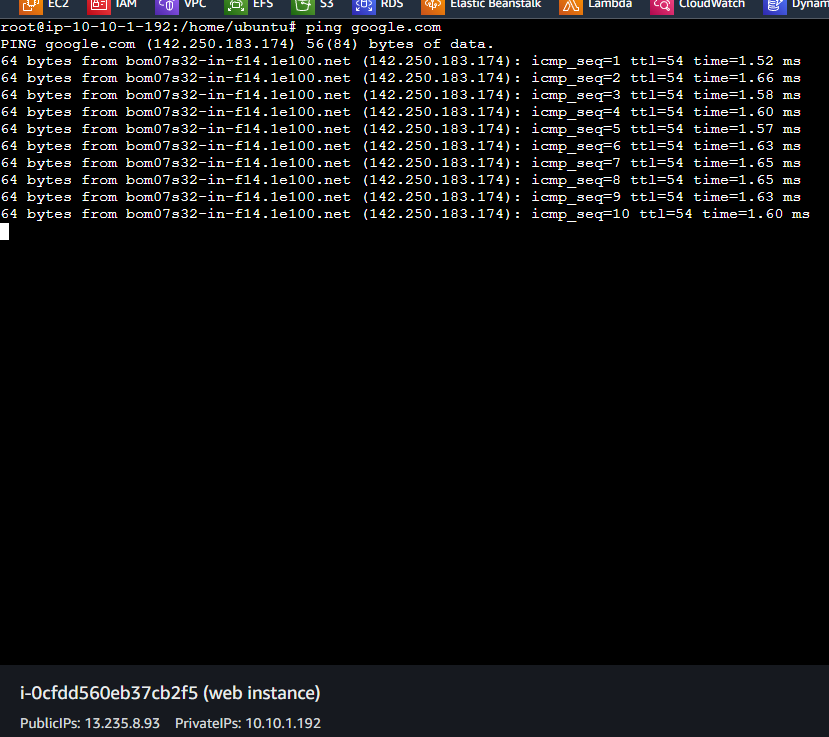




7. Launch ec2 instances in all subnets of Production VPC and name them as per name of your subnets.

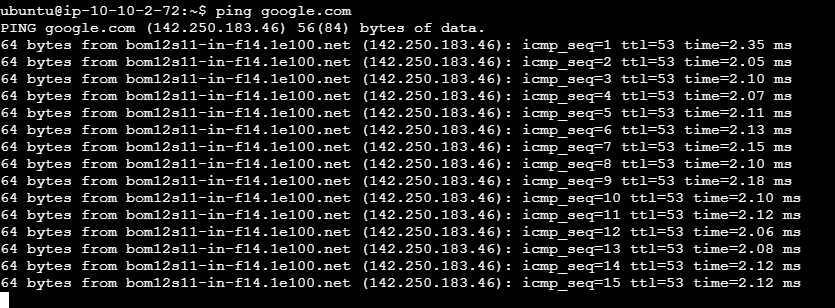


8. Connect to your web instance and check the internet connectivity ( ping google.com )

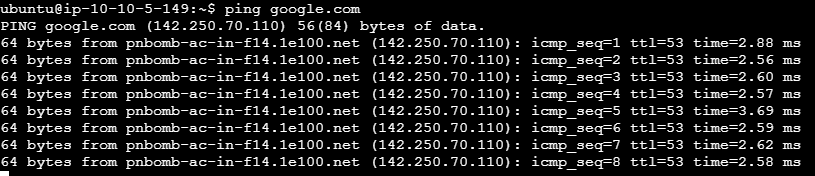


9. Connect to your app1/dbcache instance and check the internet connectivity [ connect by bastion/jump server method ] ( ping google.com )

App1 instance:



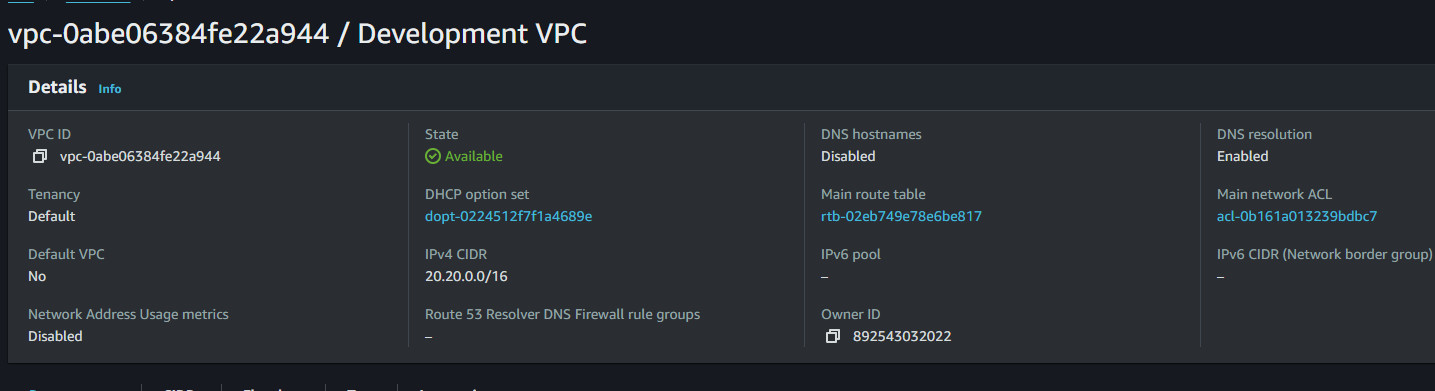
DB cache instance:



Note - make sure in the security group of the resources enabled ALL TRAFFIC from ANYWHERE source.

---------------------------------------------------------------------------------------------------------------------------------------

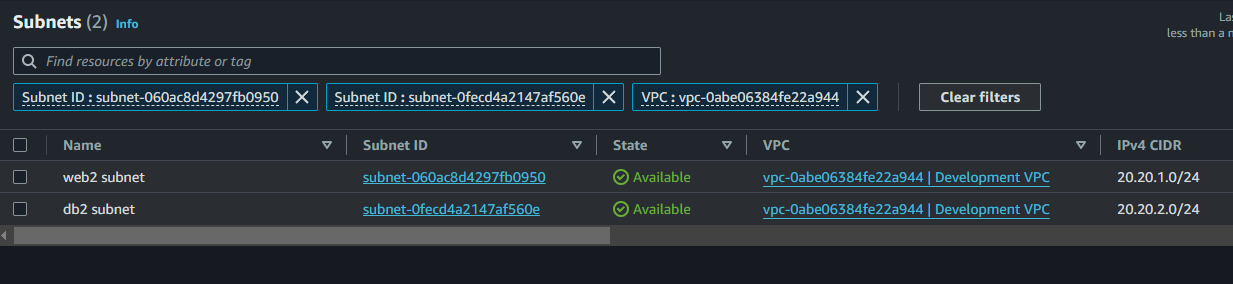
10.Create Development VPC (cidr - 20.20.0.0/16)



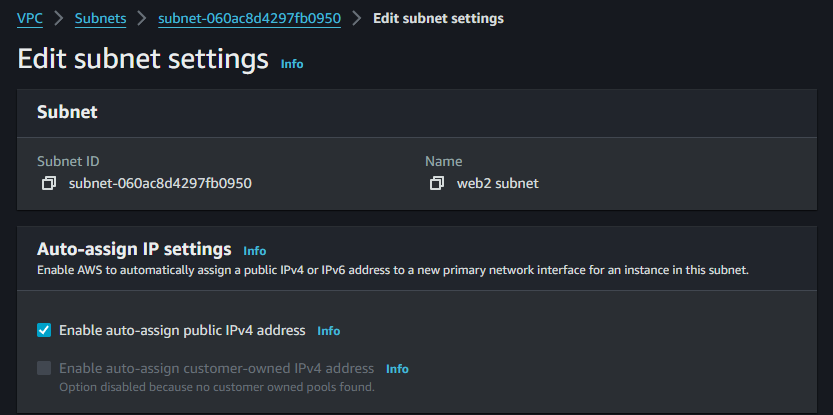
11. Create 2 Subnets in it

- web2 subnet [public] (cidr - 20.20.1.0/24)

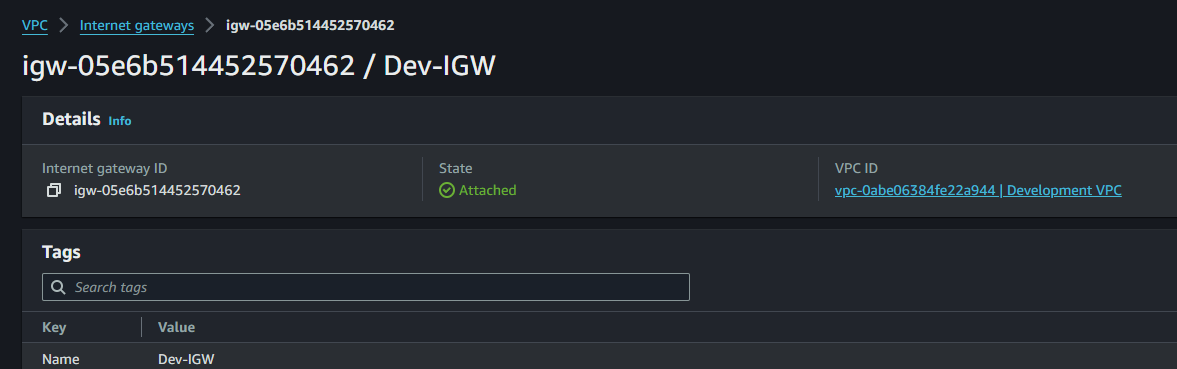
- db2 subnet [private] (cidr - 20.20.2.0/24)



- Select web2 subnet > Go to Action > Edit Subnet setting > Enable Auto Assign IPv4.



12. Create Internet Gateway (Dev-IGW) and attach it to Dev VPC.



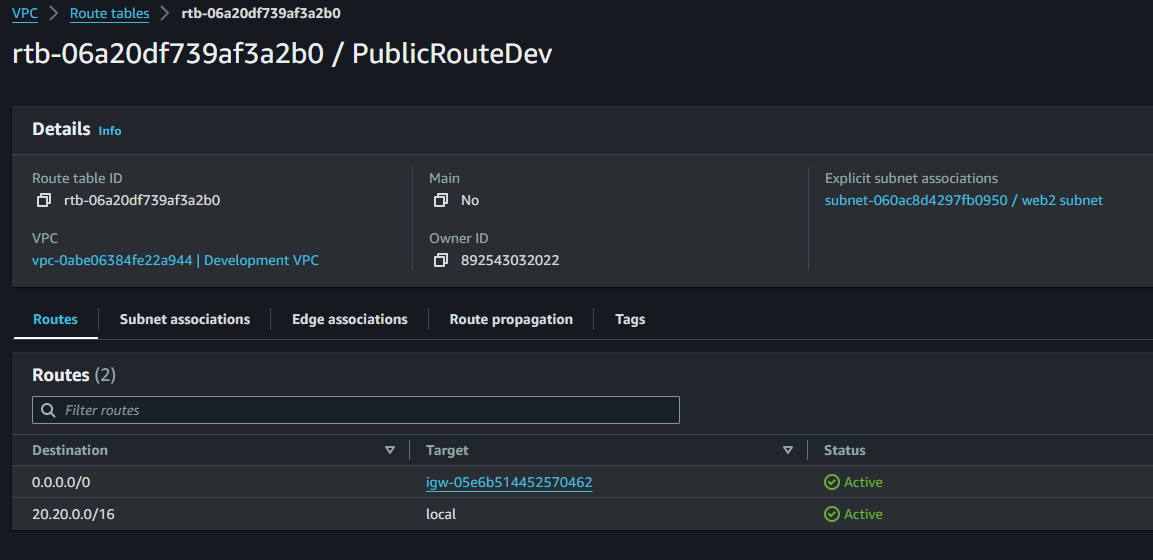
13. Create Public Route Table

- edit routes

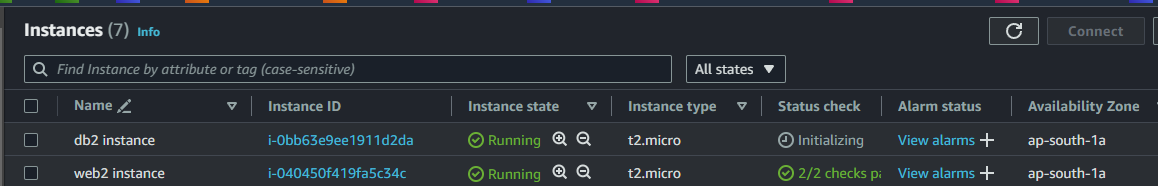
- destination - 0.0.0.0/0

- target - internet gateway (Dev-IGW)

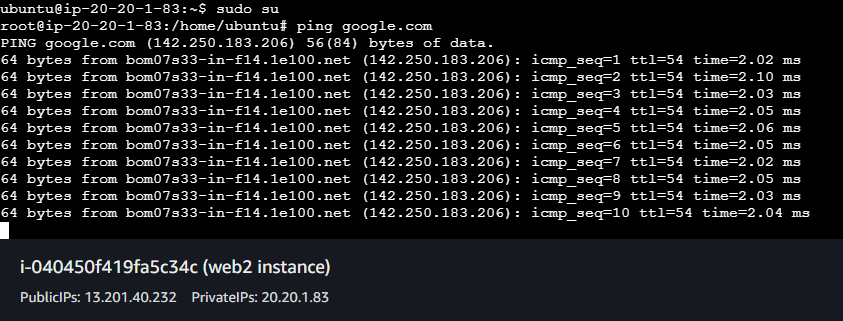
- subnet association - web2 subnet



14. Launch ec2 instances in all subnets of Development VPC and name them as per name of your subnets.



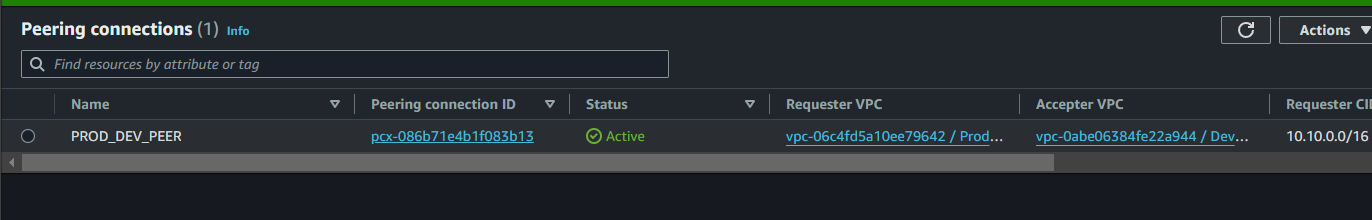
15. Connect to your web2 instance and check the internet connectivity ( ping google.com )



Note - make sure in the security group of the resources enabled ALL TRAFFIC from ANYWHERE source.

---------------------------------------------------------------------------------------------------------------------------------------

16. Create Peering connection (PROD\_DEV\_PEER) between Production VPC and Development VPC, also accept the peering request.



17. Create 2 Route Tables-

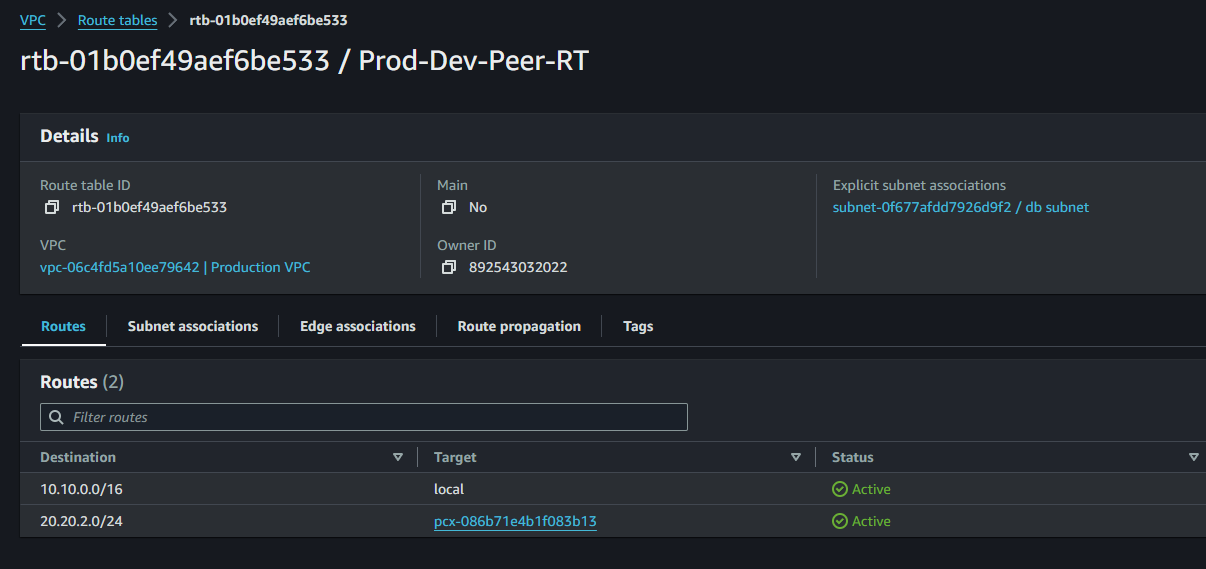
a. Prod-Dev-Peer-RT and attach to Production VPC.

- edit the routes

- destination - 20.20.2.0/24 [ cidr of db2 subnet of dev network ]

- target - peering connection (PROD\_DEV\_PEER)

- subnet association - db subnet



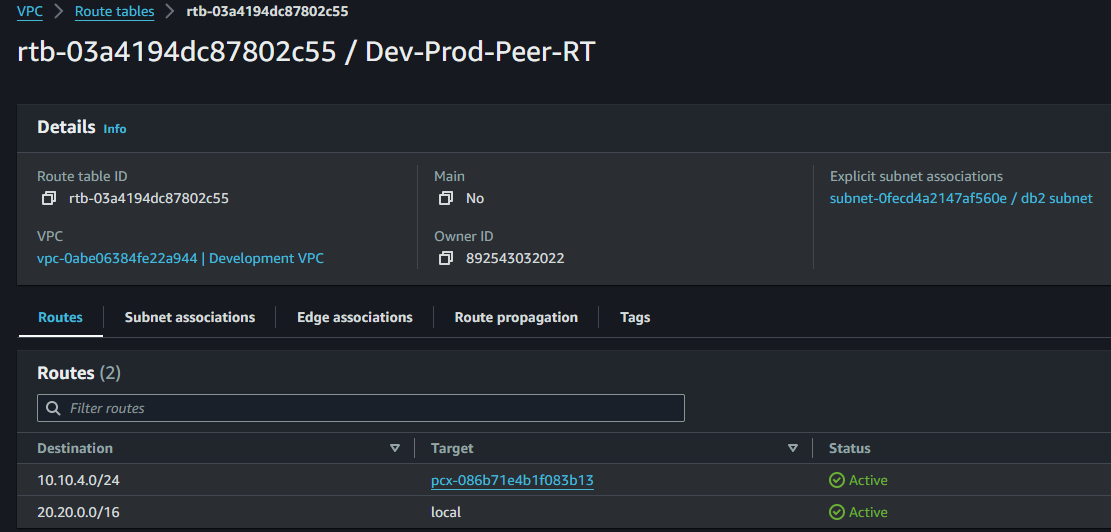
b. Dev-Prod-Peer-RT and attach to Development VPC.

- edit the routes

- destination - 10.10.4.0/24 [ cidr of db subnet of prod network ]

- target - peering connection (PROD\_DEV\_PEER)

- subnet association - db2 subnet



18. Then connect to your db instance and then ping private ip of db2 instance ( you will be able to see the network packet transfer)

