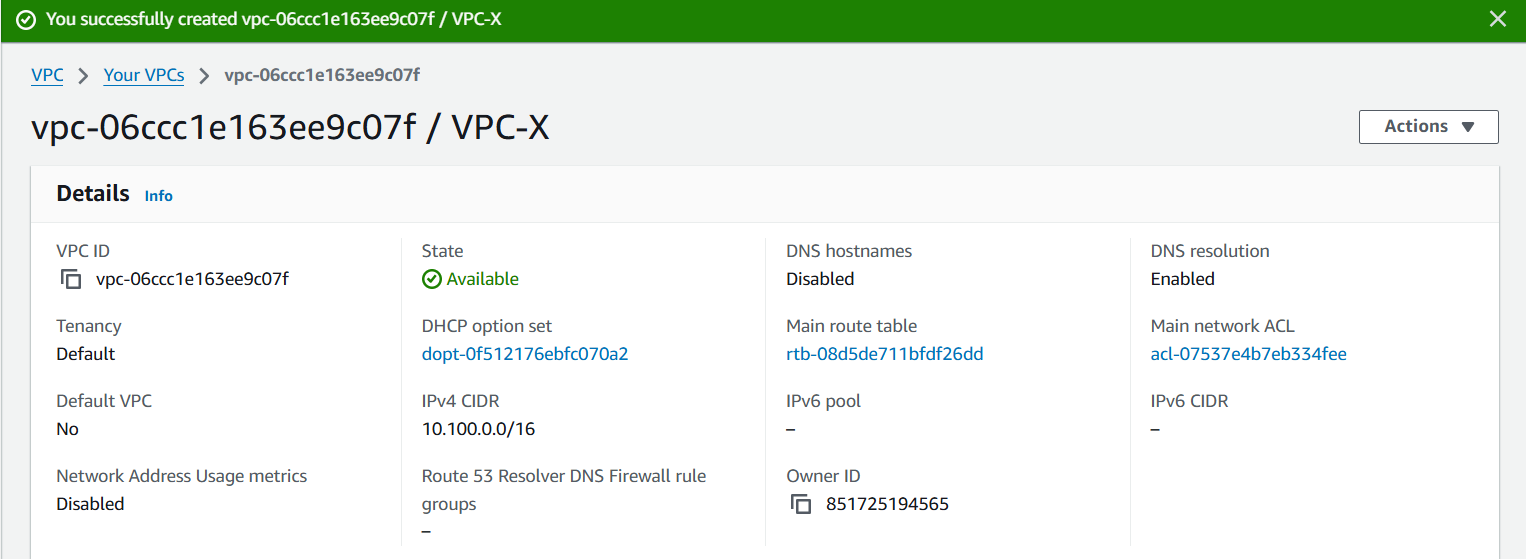
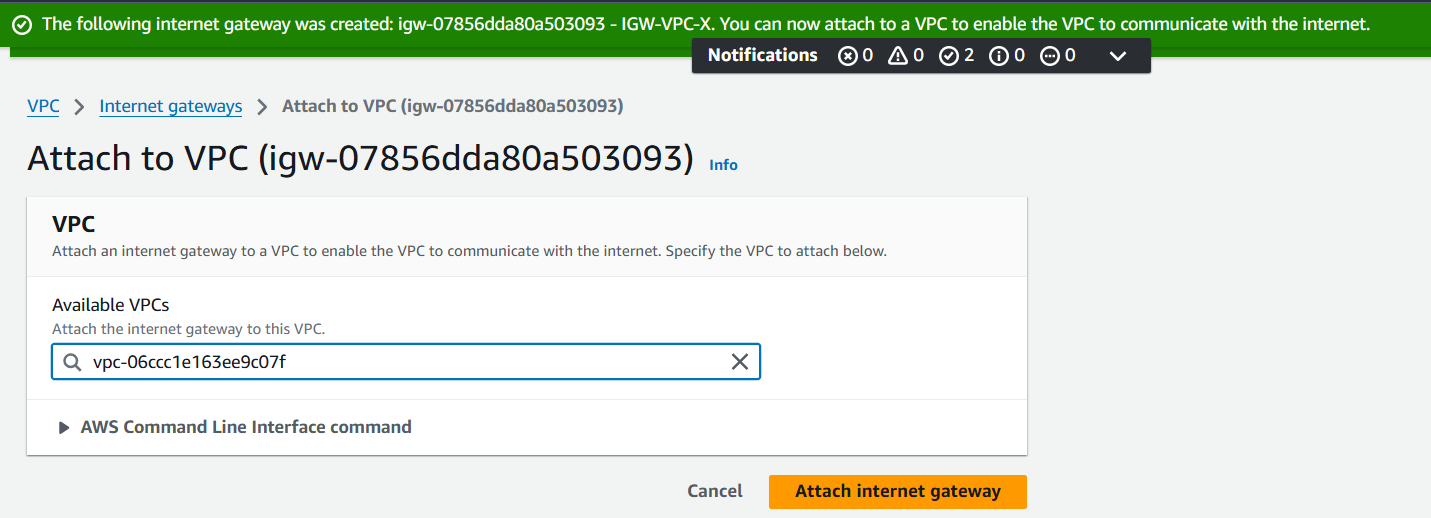
TASK 19- VPC PEERING

**VPC Peering** is a secure, direct network connection between two VPCs that allows instances in each VPC to communicate as if they were within the same network

STEP 1- CREATED VPC-X

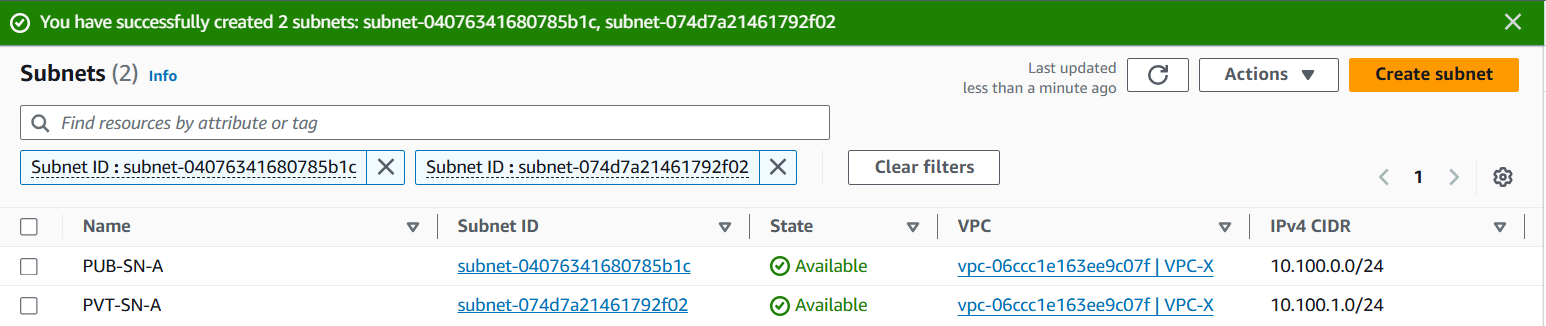


STEP 2- ATTACHED IGW TO IT

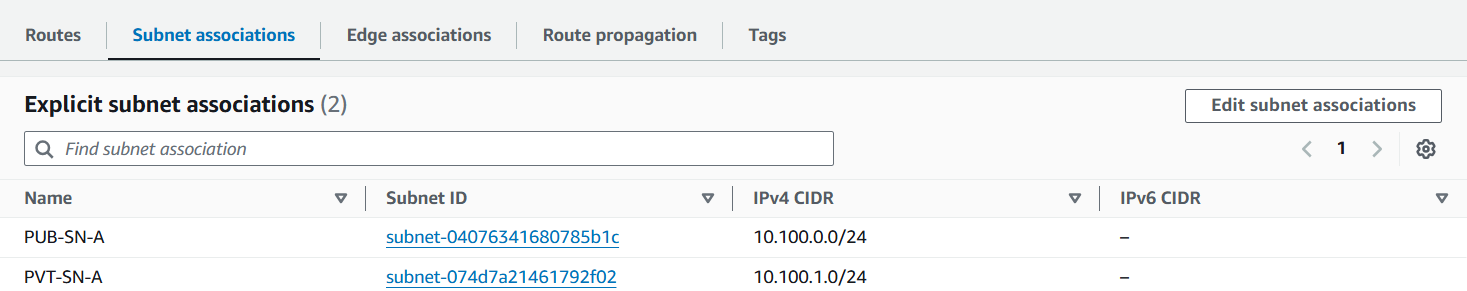


Ensure Non-Overlapping CIDR Ranges: Both VPCs must have unique, non-overlapping CIDR ranges for the VPC Peering connection to work.

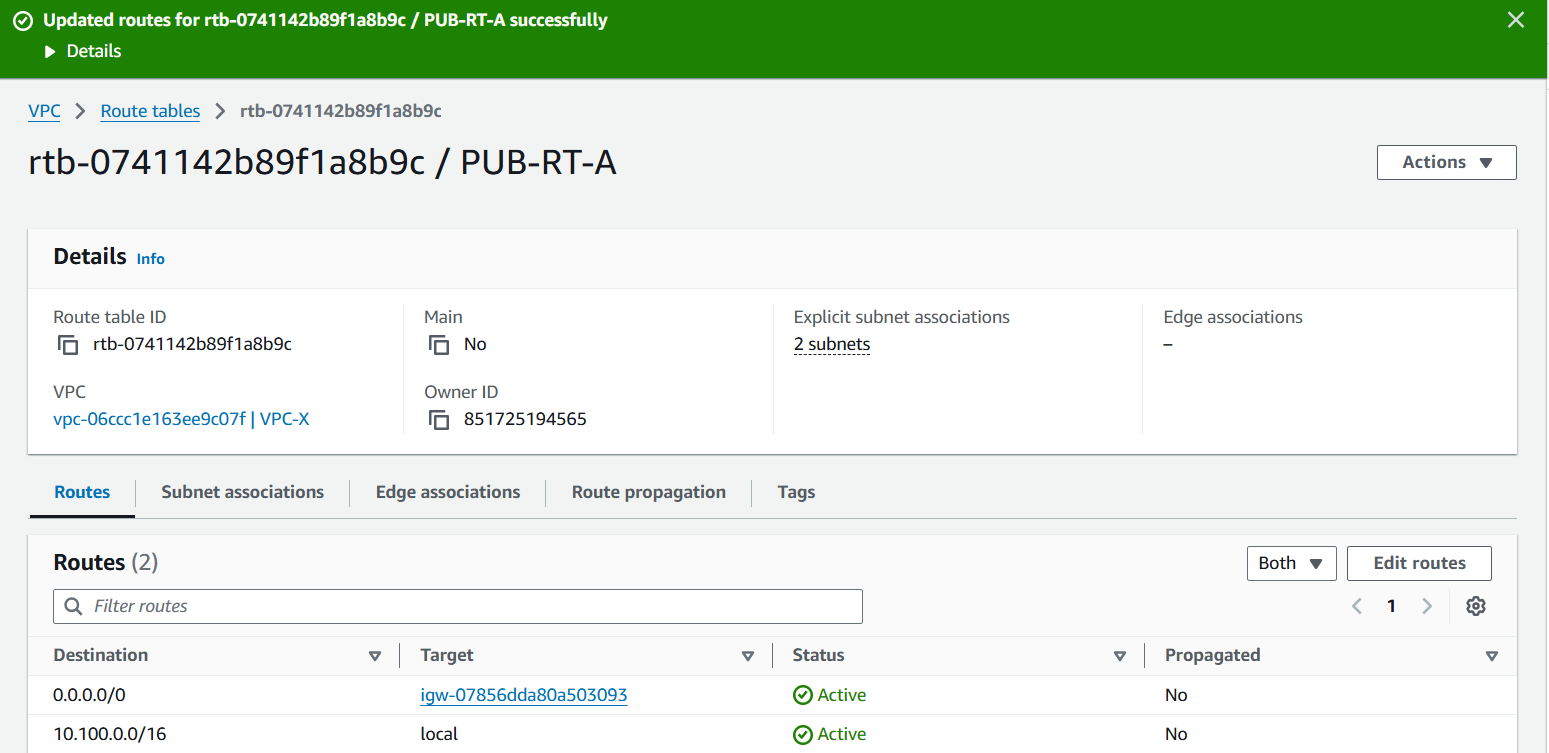
STEP 3- CREATED SUBNETS NAMED PUB-SN-A/PVT-SN-A



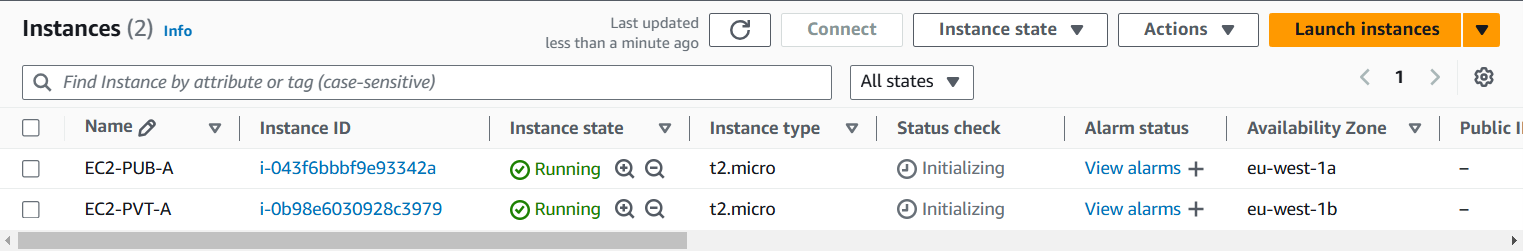
STEP 4- SUBNET ASSOCIATION



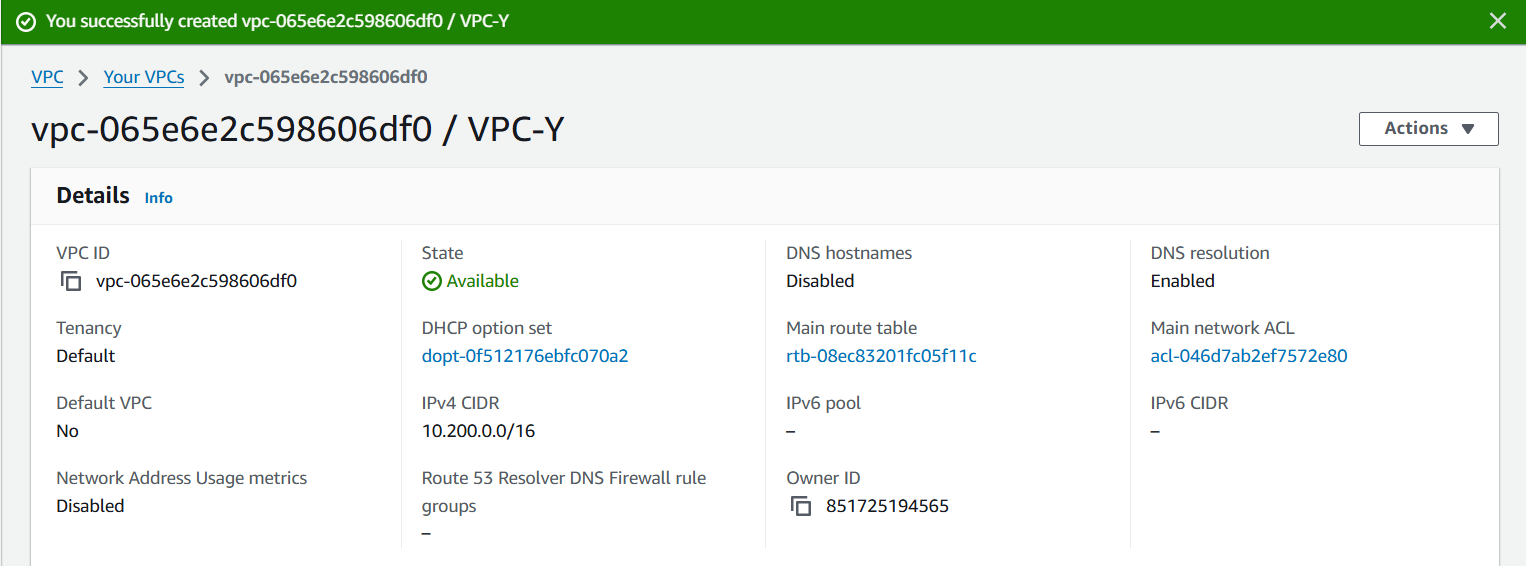
STEP 5- ROUTES UPDATED



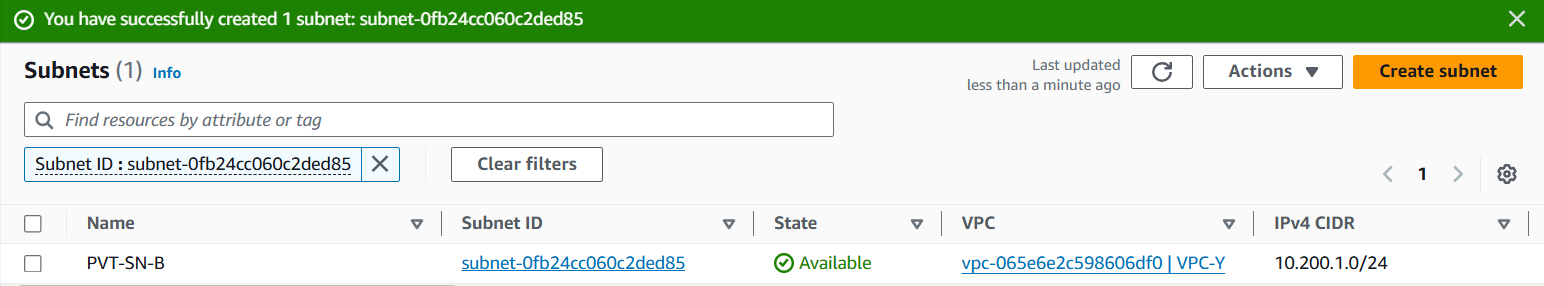
STEP 6- LAUNCHED TWO EC2 INSTANCES IN VPC-X, DIFFERENT SUBNETS/AZ.



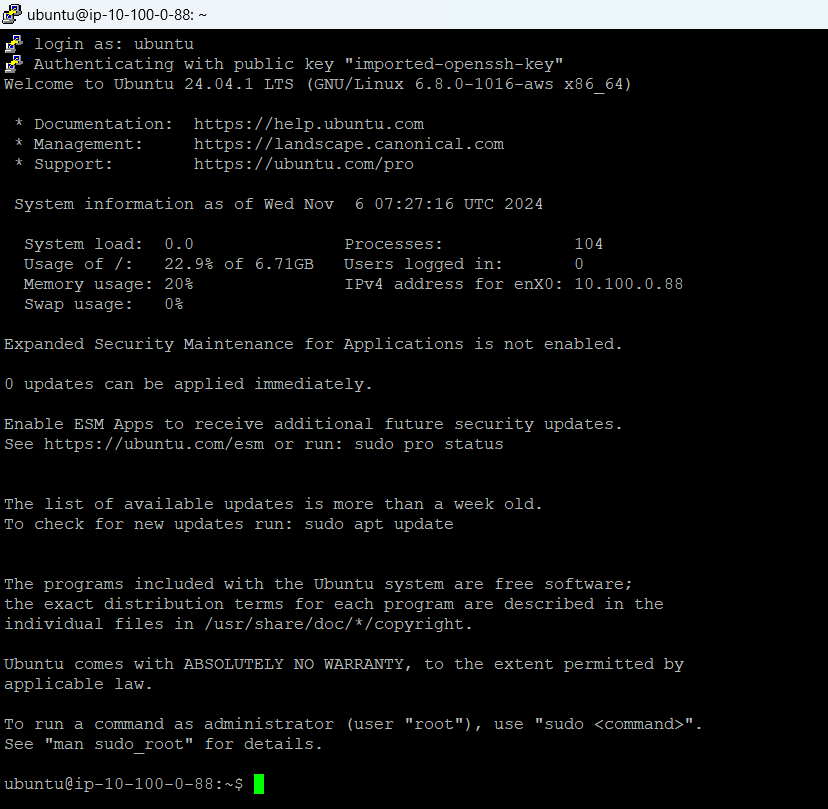
STEP 7- CREATED VPC-Y



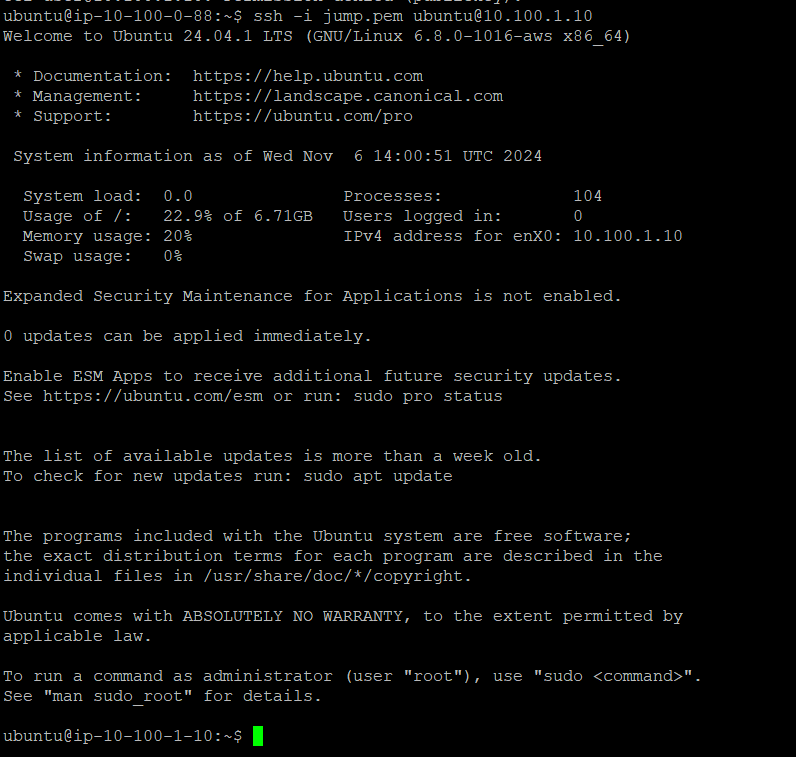
STEP8- CREATED PVT-SN-B



STEP 9- CHECKED INTERNET CONNECTION ON EC2-PUB-A USING PUTTY

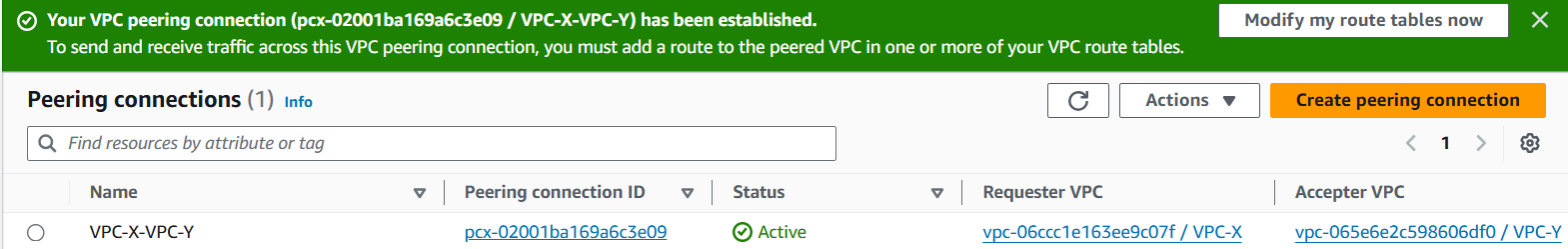


STEP 10- JUMPED FROM EC2-PUB-2 TO EC2-PVT-A



PEM KEY WAS SAVED IN JUMP.PEM FILE, AND JUMPED USING COMMAND ssh -i jump.pem [ubuntu@10.100.1.0](mailto:ubuntu@10.100.1.0)

STEP 11- PEERING ESTABLISHED BY ACCEPTING REQUEST

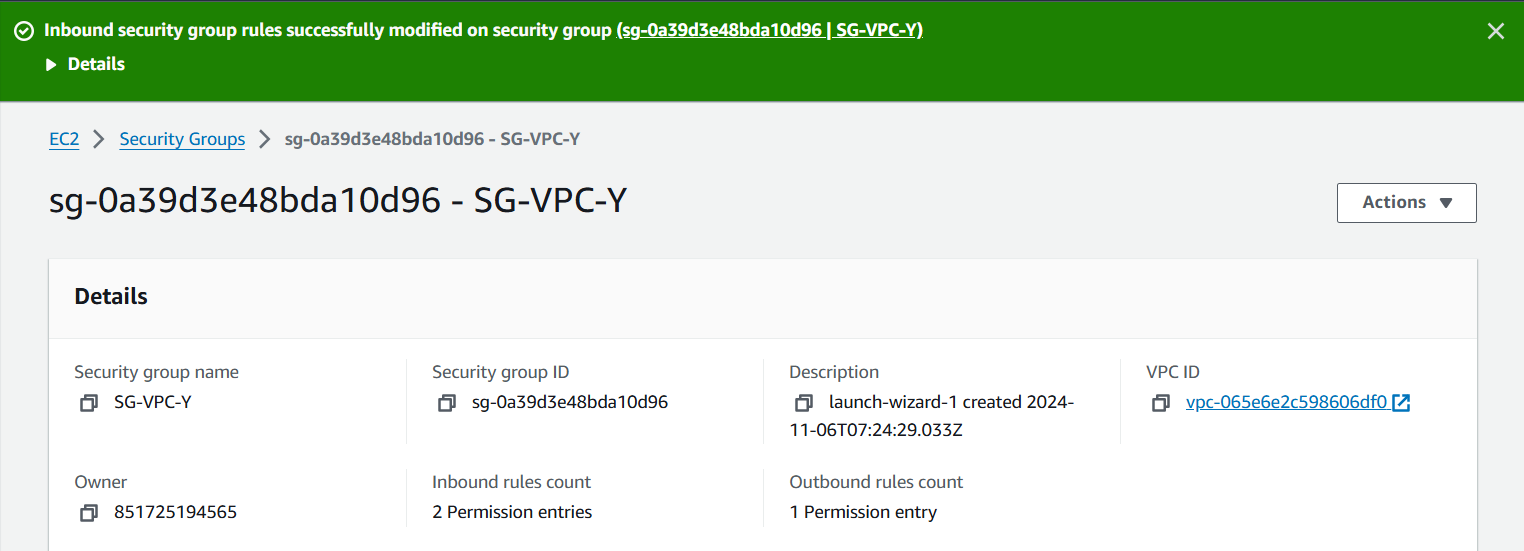


Set Up VPC Peering: Create a VPC Peering connection between the two VPCs. Accept the request if they are in different accounts.

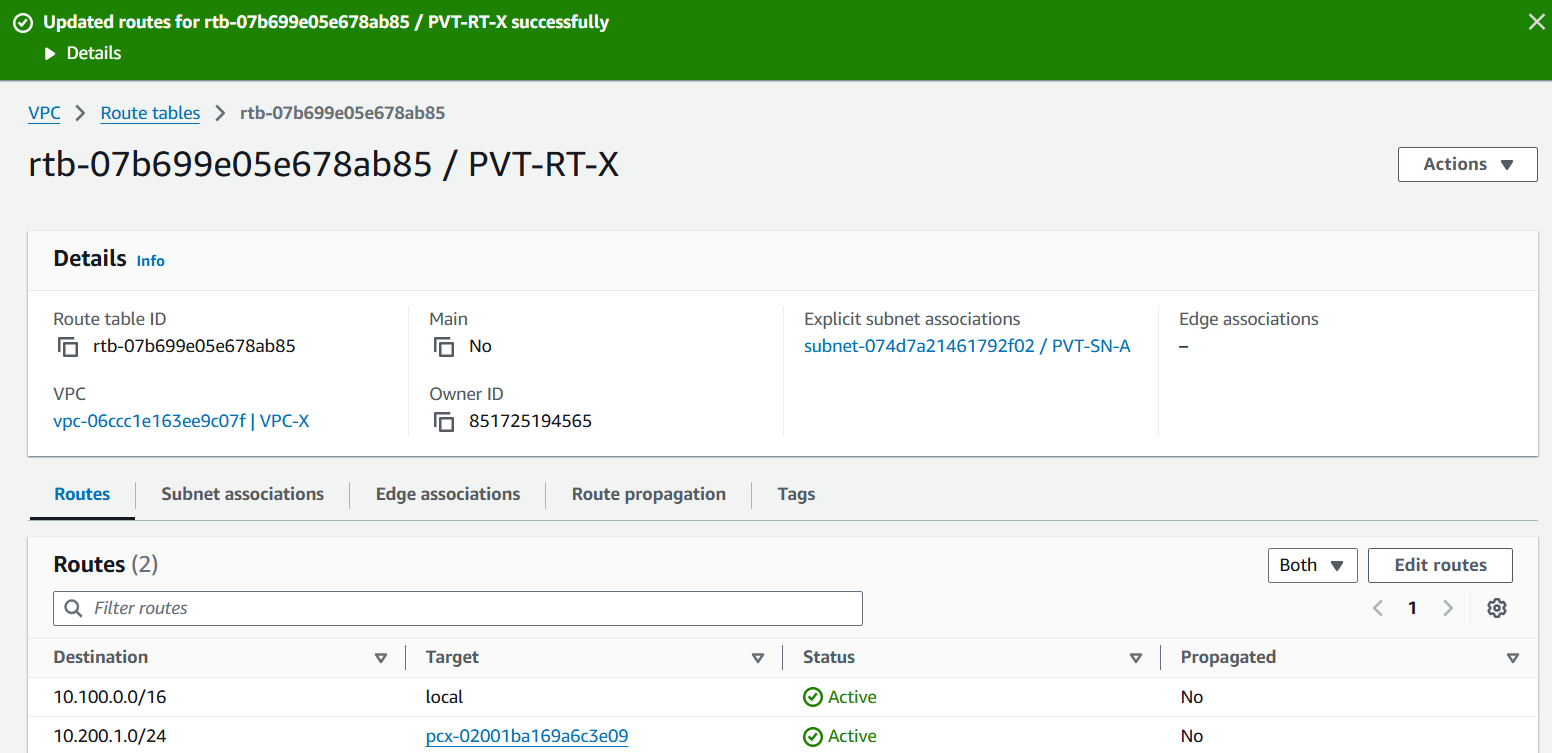
Update Route Tables: In each VPC, update the route tables of the private subnets:

* Add routes pointing to the CIDR block of the other VPC.
* Target the VPC Peering connection as the destination.

STEP 12 – INBOUND RULES MODIFIED IN SG

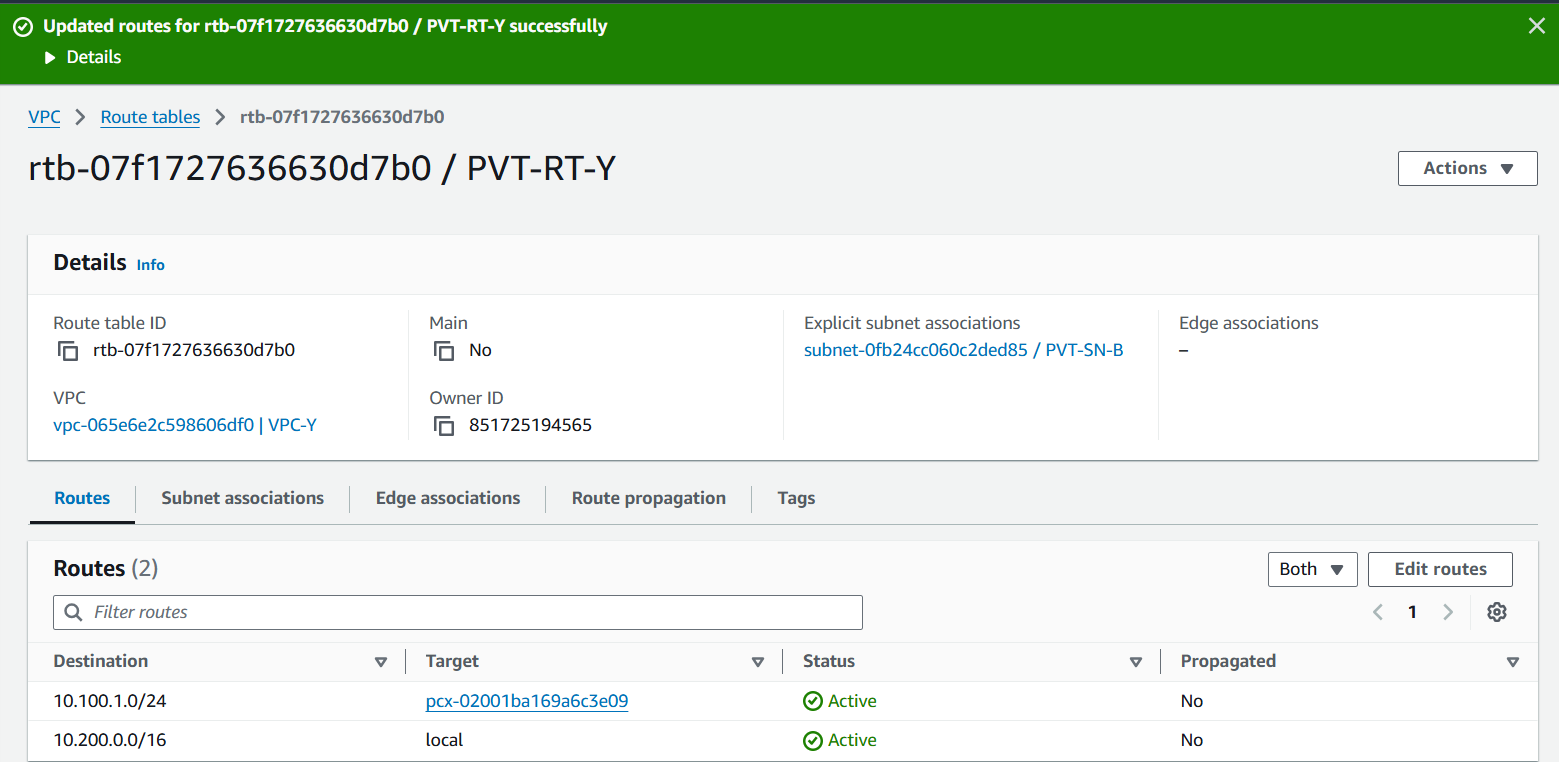


STEP 13- ROUTES EDITED FOR BOTH VPC’S CREATED

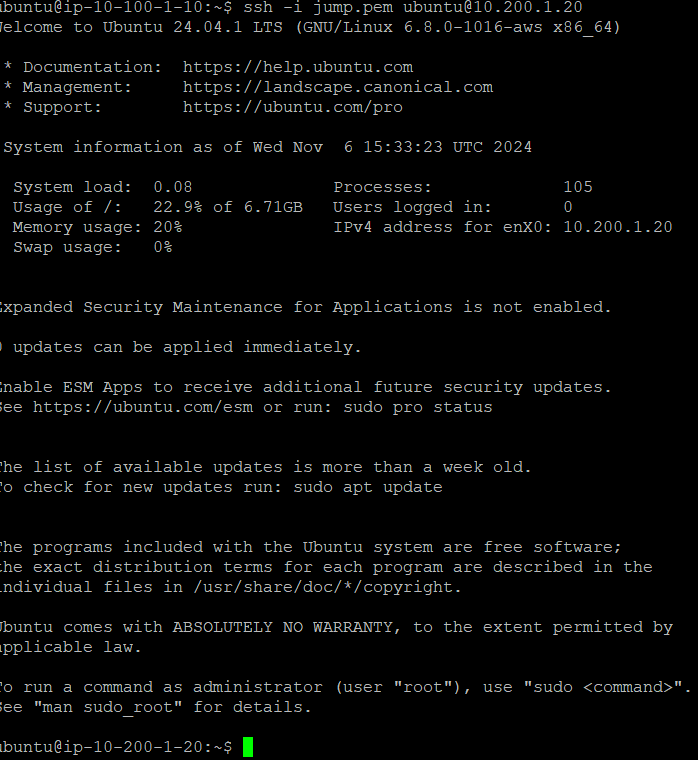


Modify Security Groups: Update security group rules in each VPC to allow traffic from the other VPC's CIDR range.

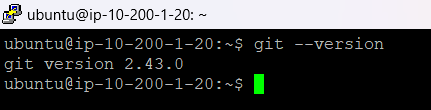
STEP 14- THE RELEVANT CIDR RANGE OF SUBNETS WAS USED FOR AUTHENTICATION



STEP 15- SUCCESSFULLY JUMPED FROM EC2-PVT-A TO EC2-PVT-B



STEP 16- INSTALLED GIT TO CHECK INTERNET CONNECTION



STEP 17- EXIT FROM 10.200.1.20 TO 10.100.1.0 TO 10.100.0.88

