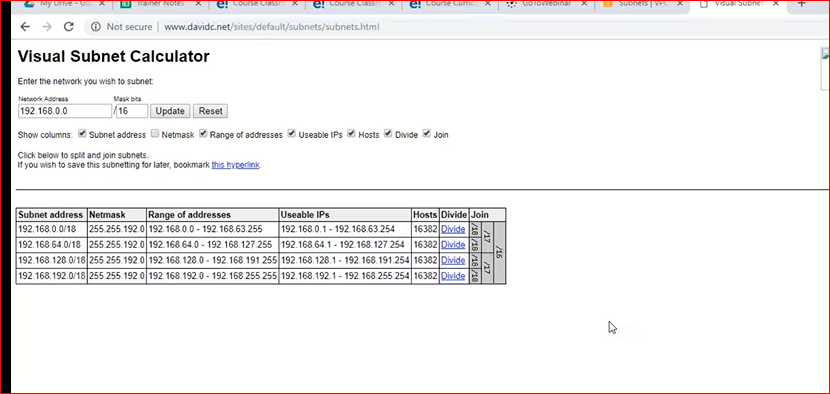
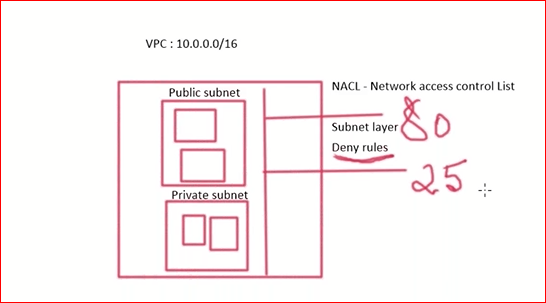
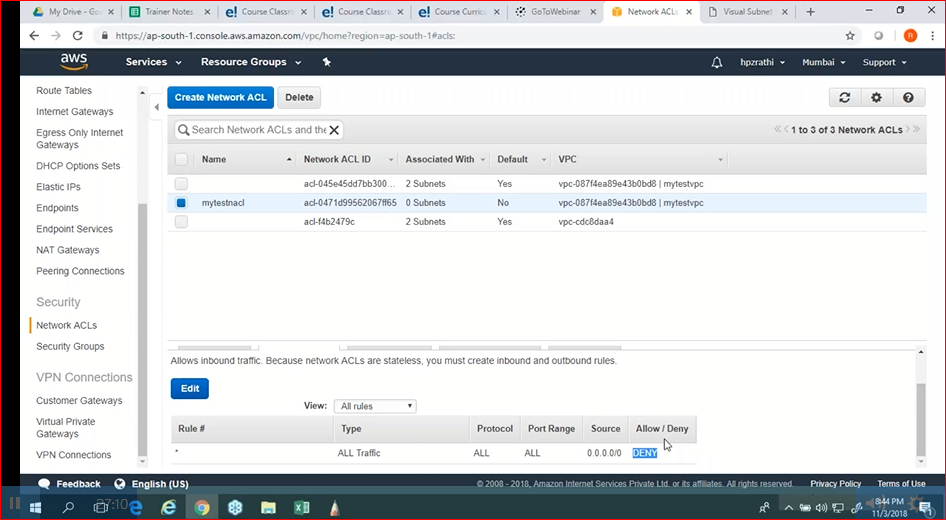
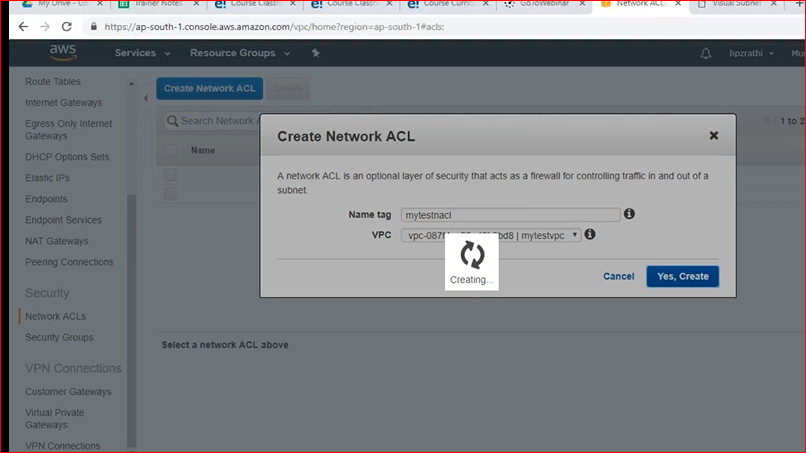
Module#3 Database Services



Revision

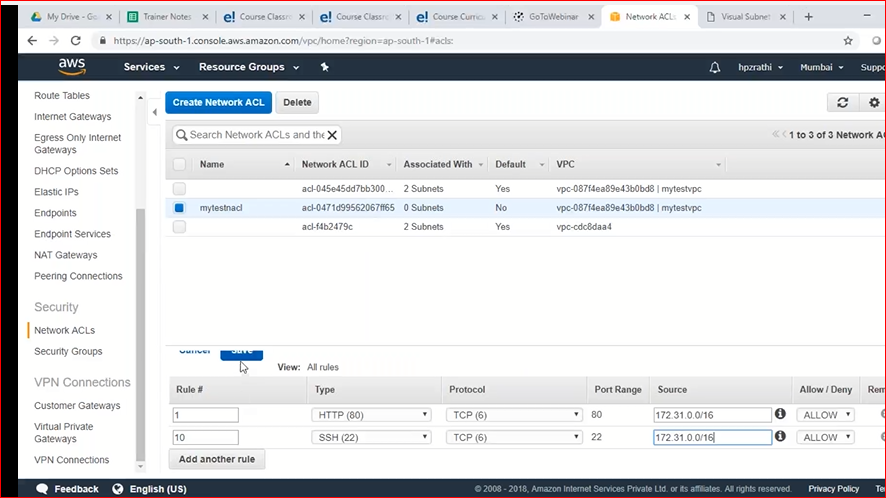
NACL



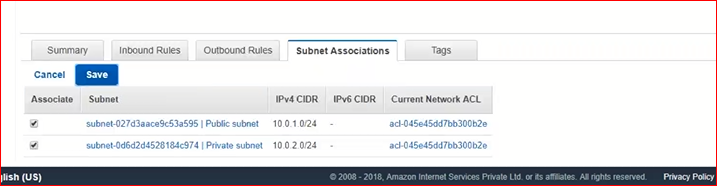


Default rule is Deny all the traffic

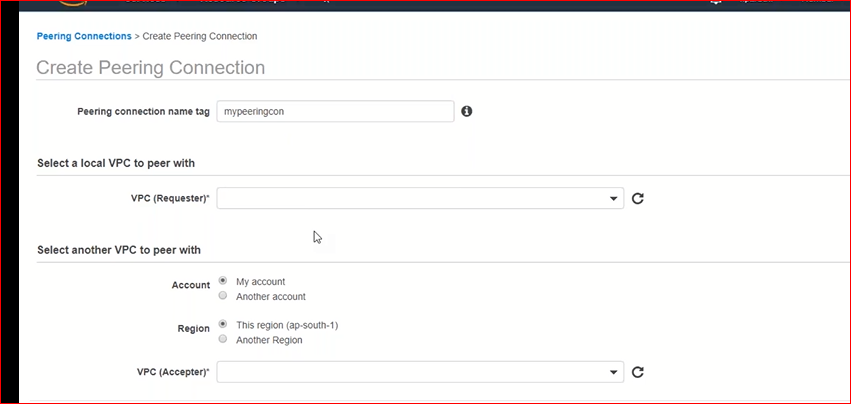
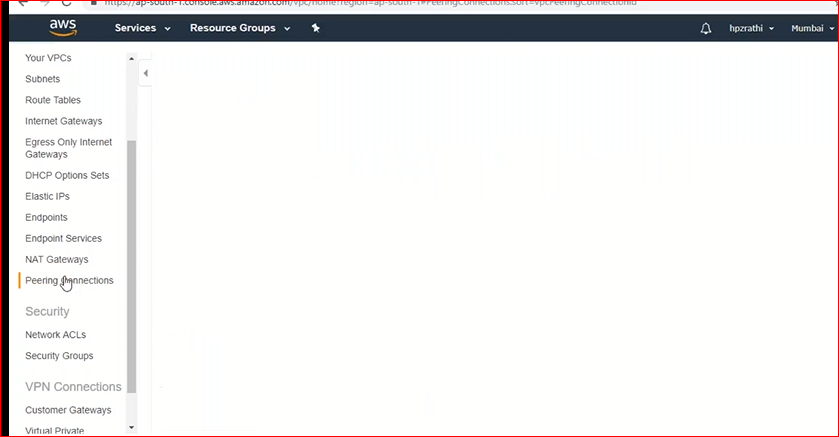
Create rules

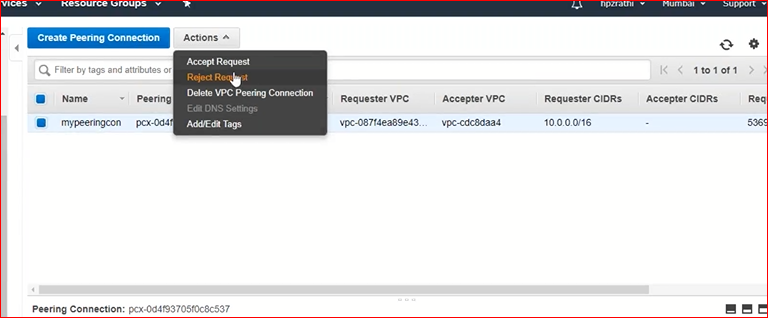
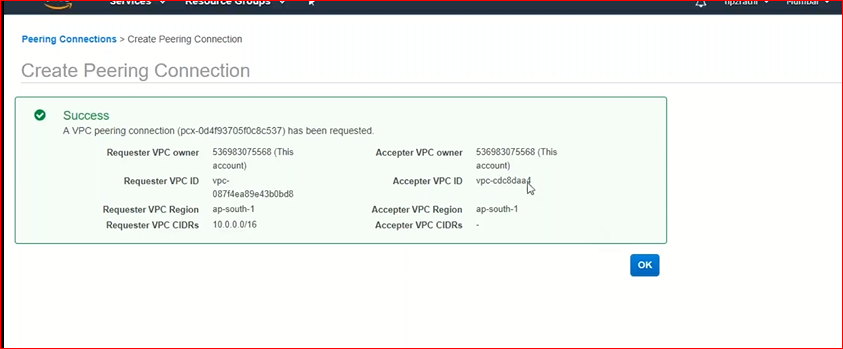
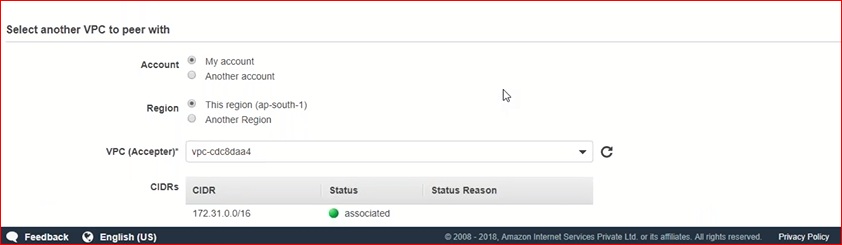


Now associate the subnet

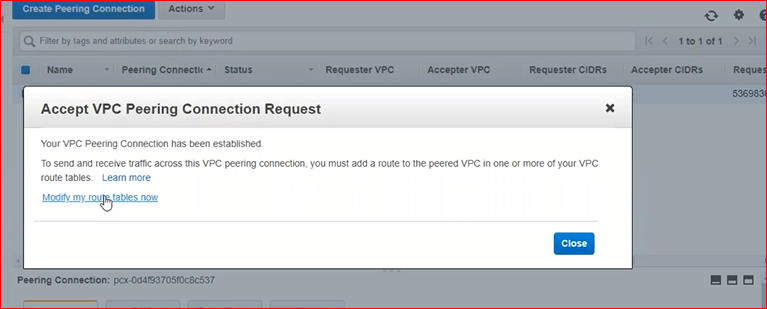


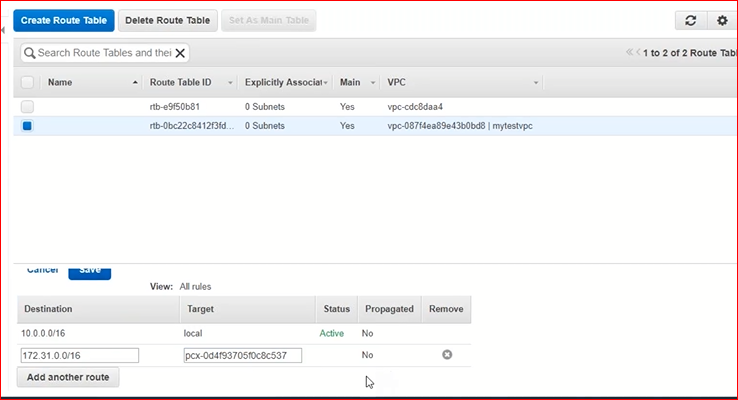
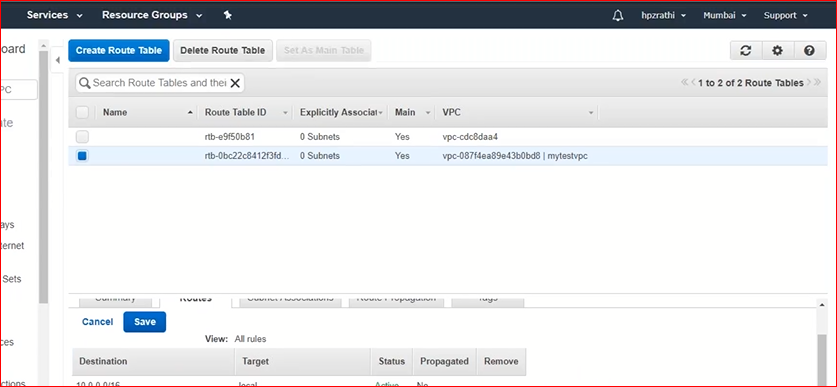
VPC Peering



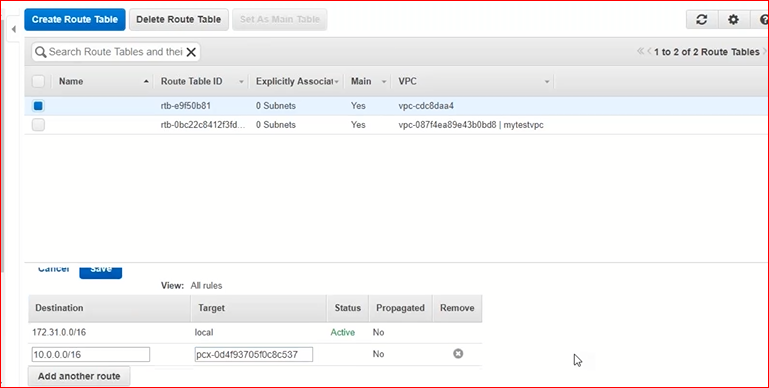


Modify the route tables

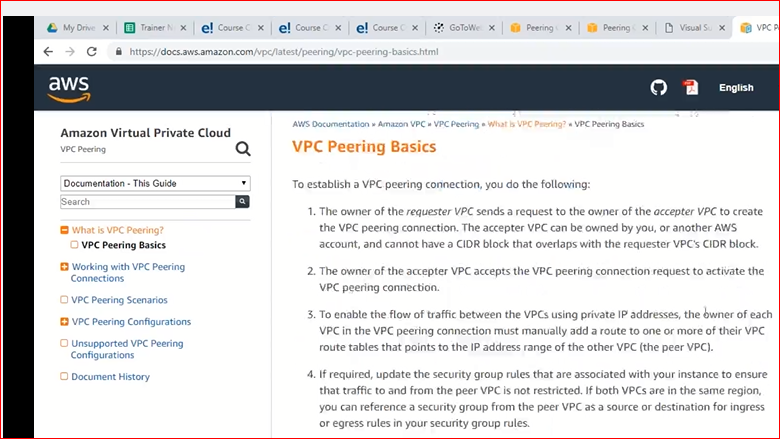




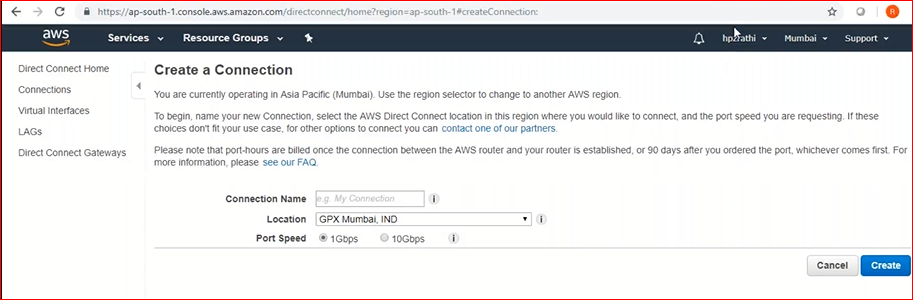
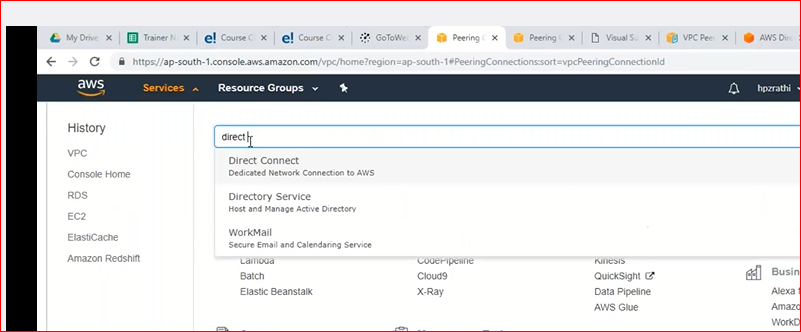
Do the same thing for default vpc



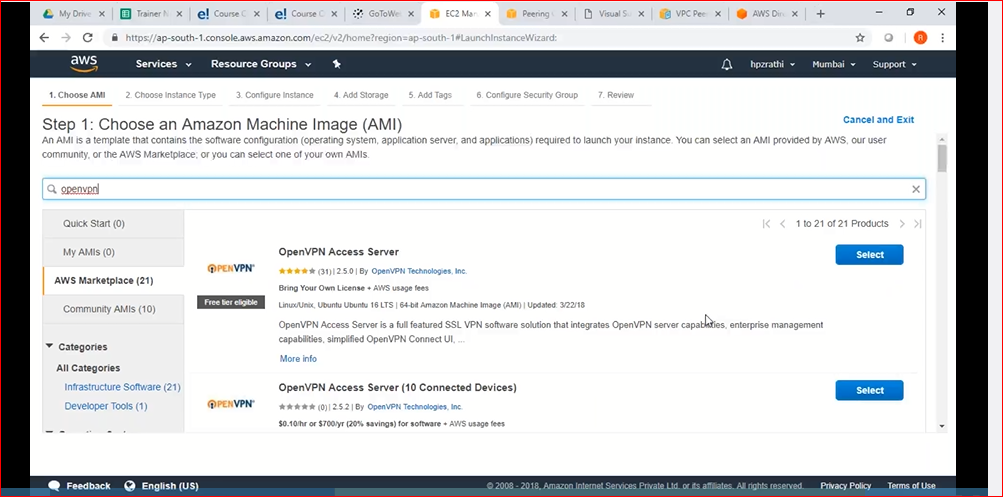
Add destination and target in route tables of each vpc



Direct connect

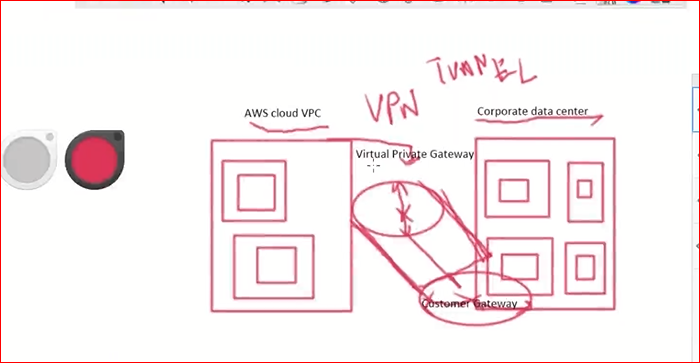


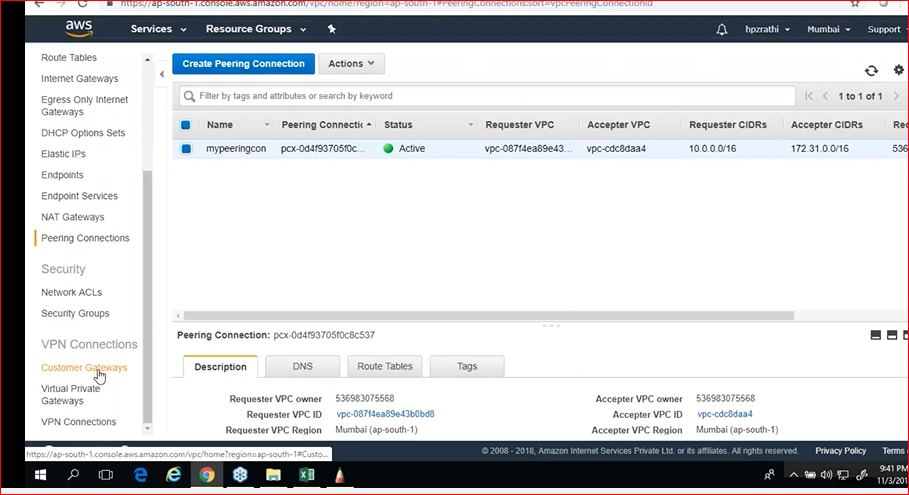
Open vpn



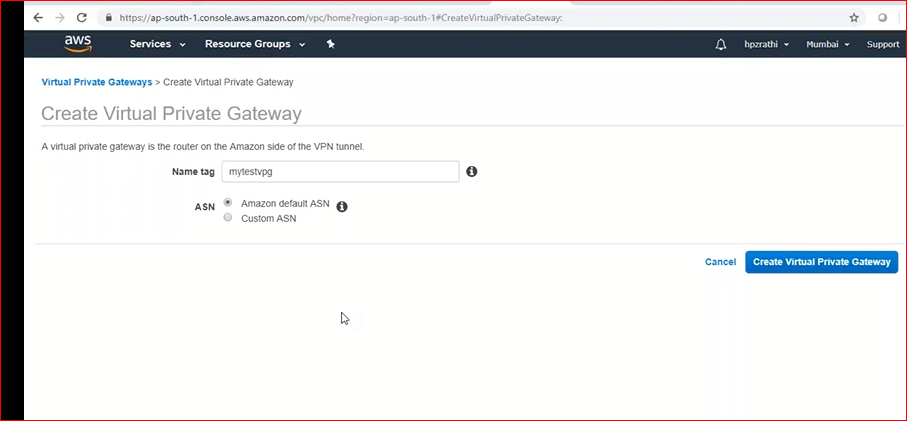
VPN Tunneling

Connect the routers

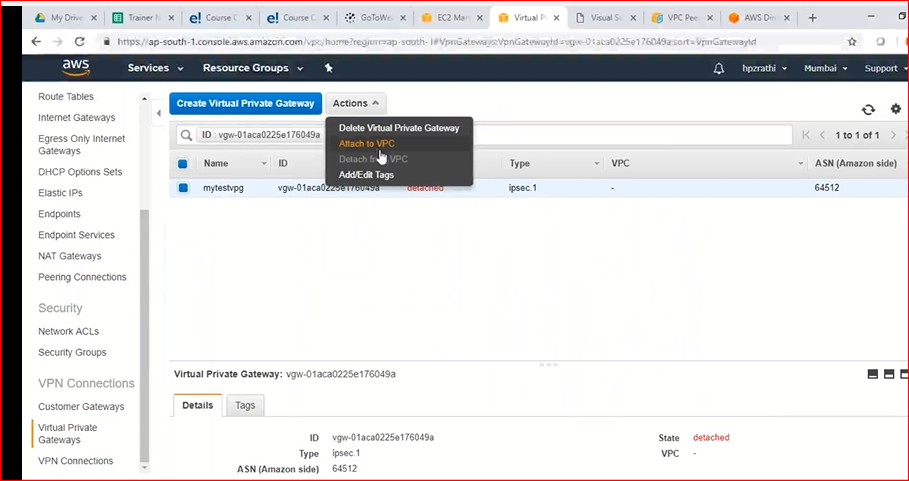


\\

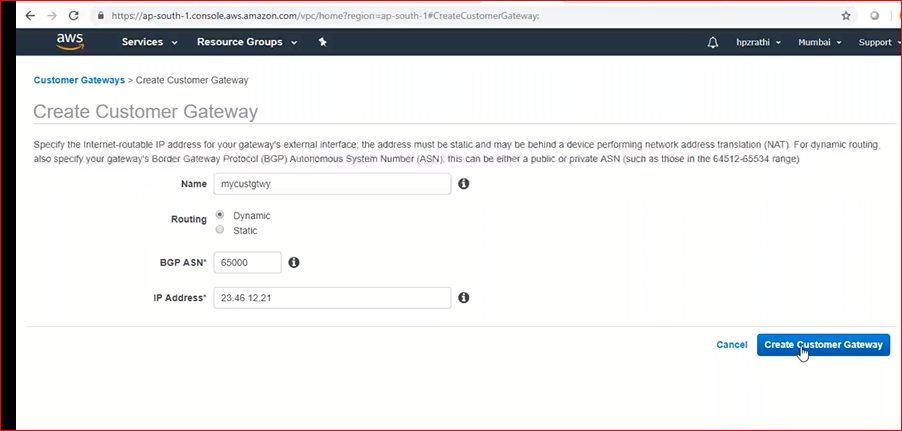
Step 1 create virtual private gateway



Now attach it to the VPC

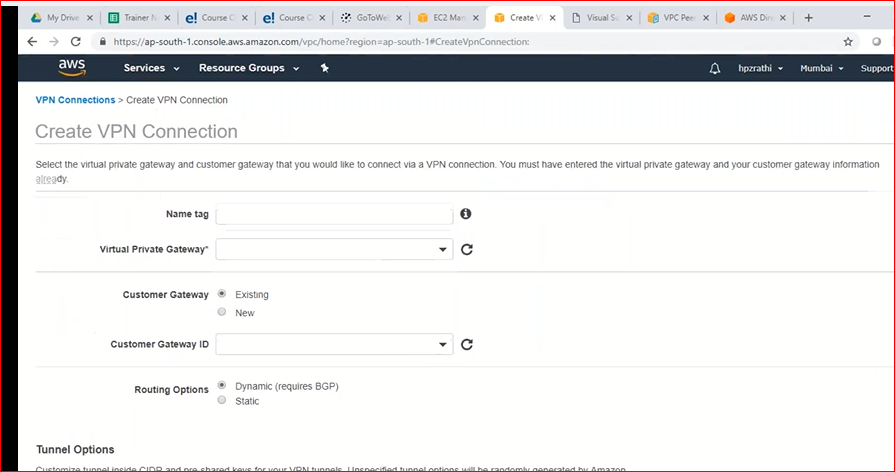


Create a customer gateway

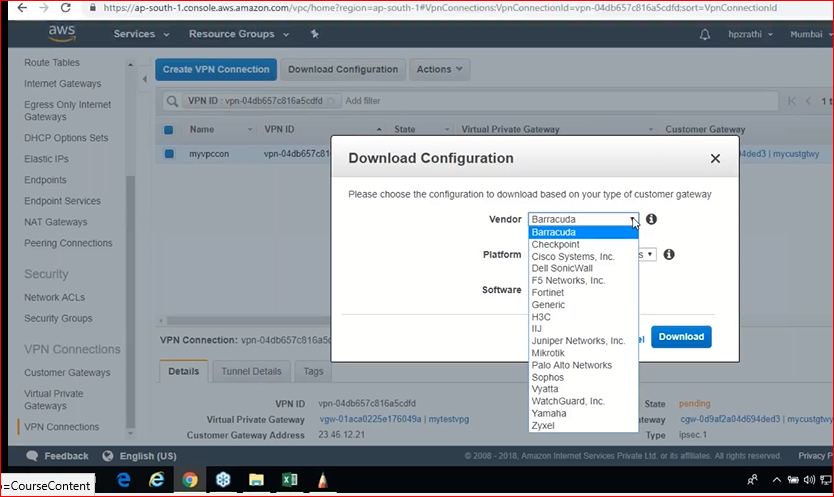


Get the configuration from ur network team,

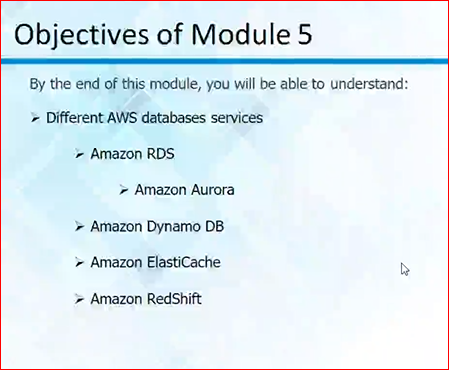
Now as both the routers are created next step is to create VPN tunnel or connection



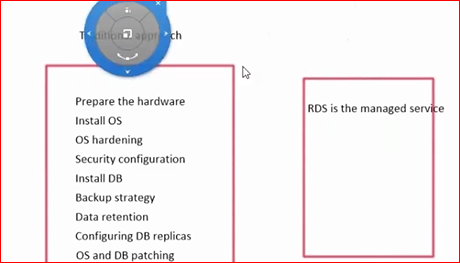
Now customer gateway has to initiate the tunnel, so u have to download the configuration



Select customer gateway attribute.

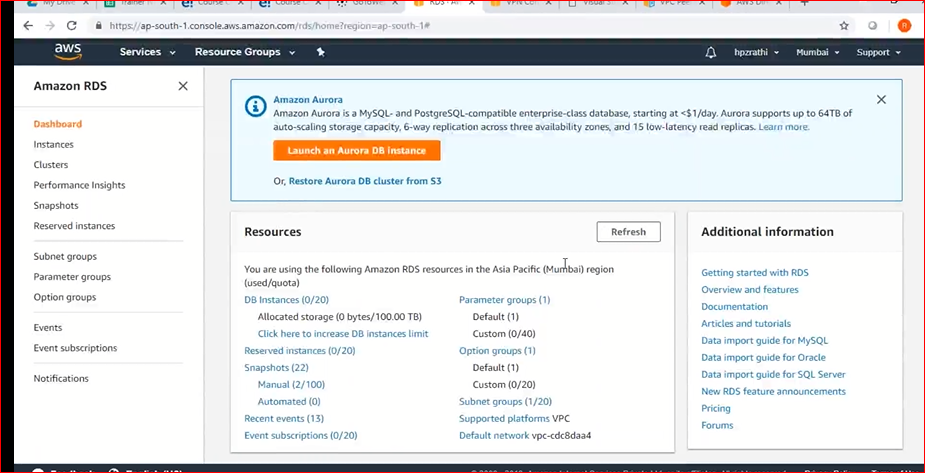


In traditional approach, one have to take care of

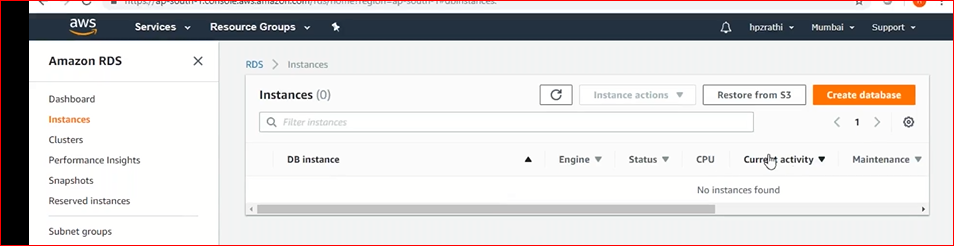


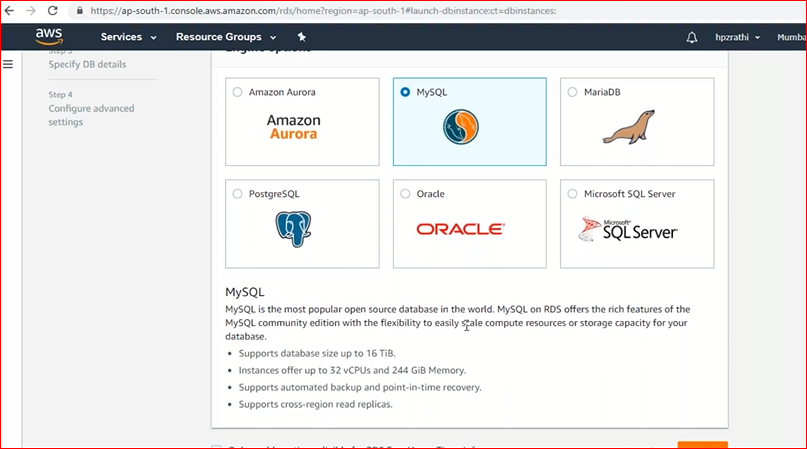
Create a DB instance

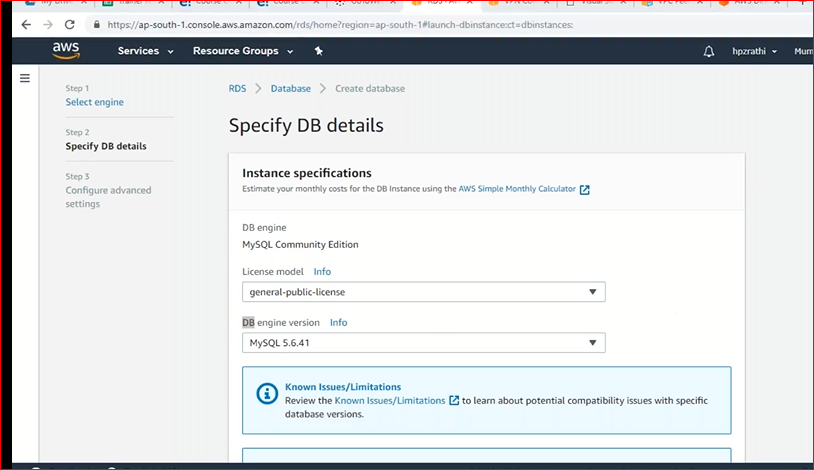
Search for RDS

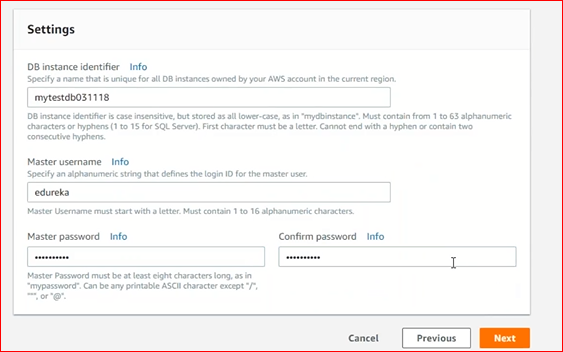
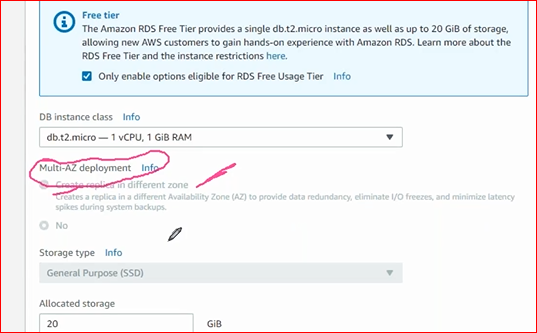


Click instances => created database

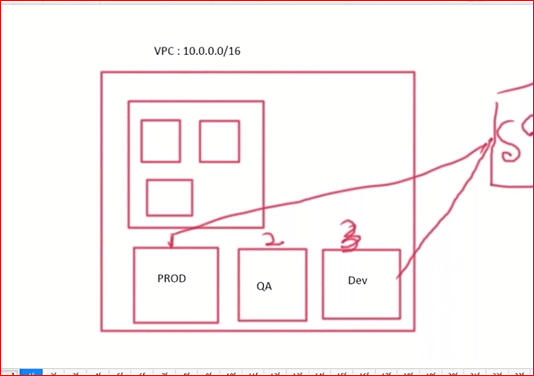


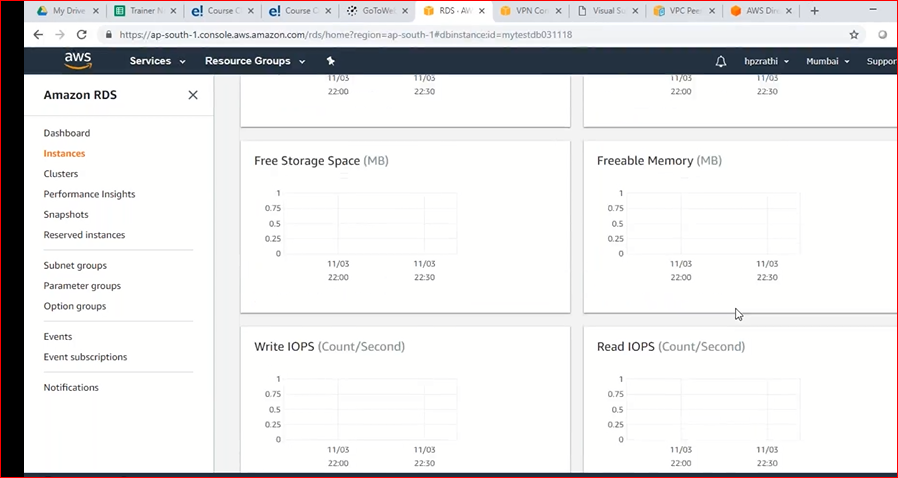




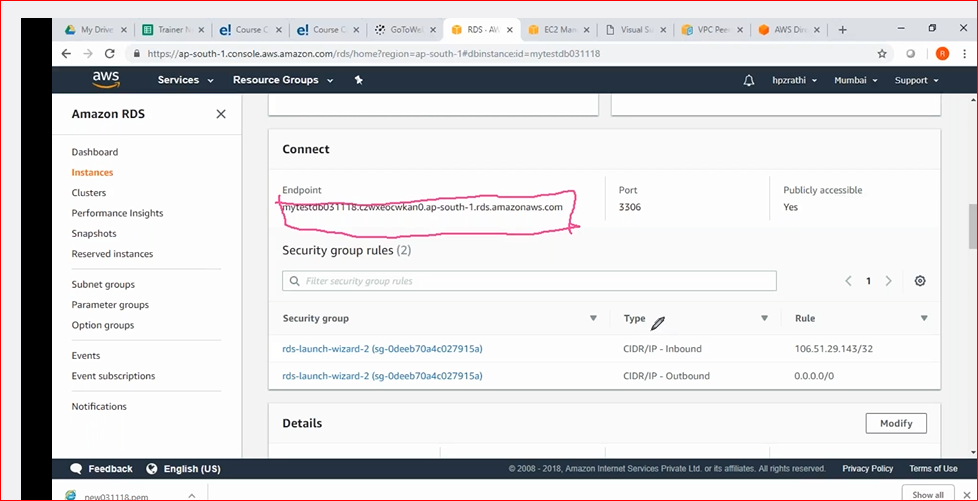


Subnet group

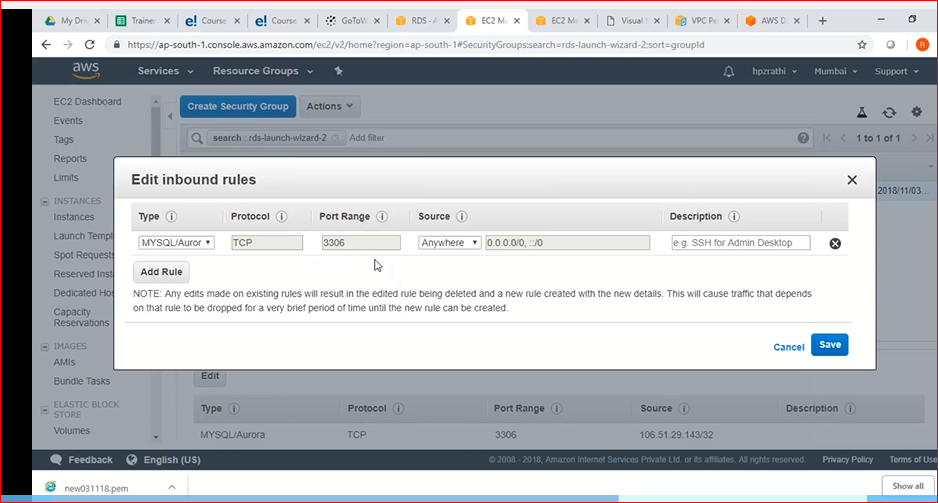


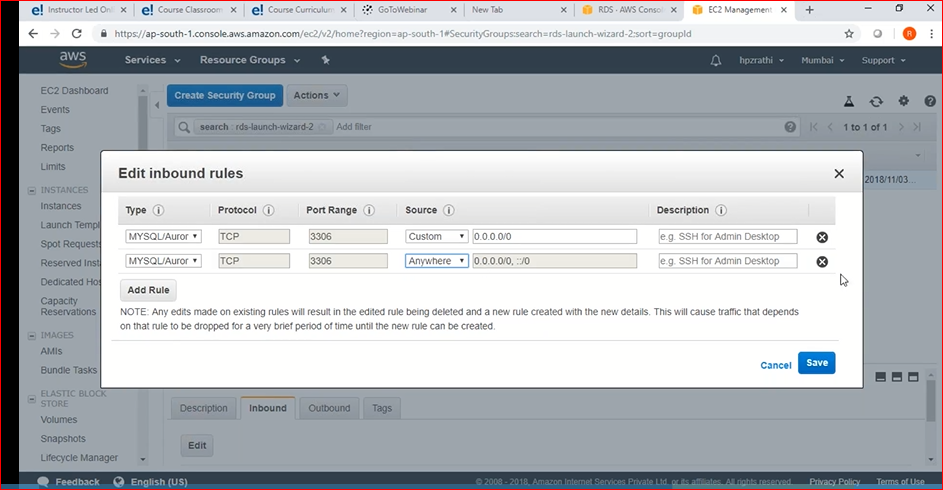


Launch EC2 and connect to DB



Configure security group





Go to EC2 instance and connect it

