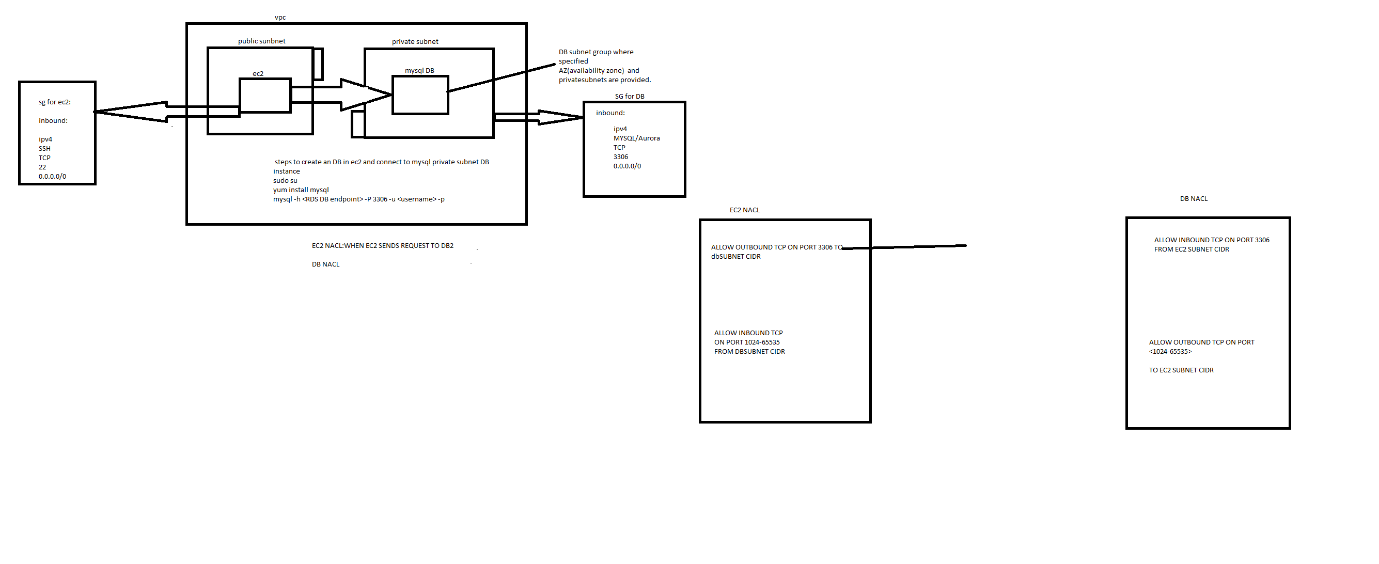
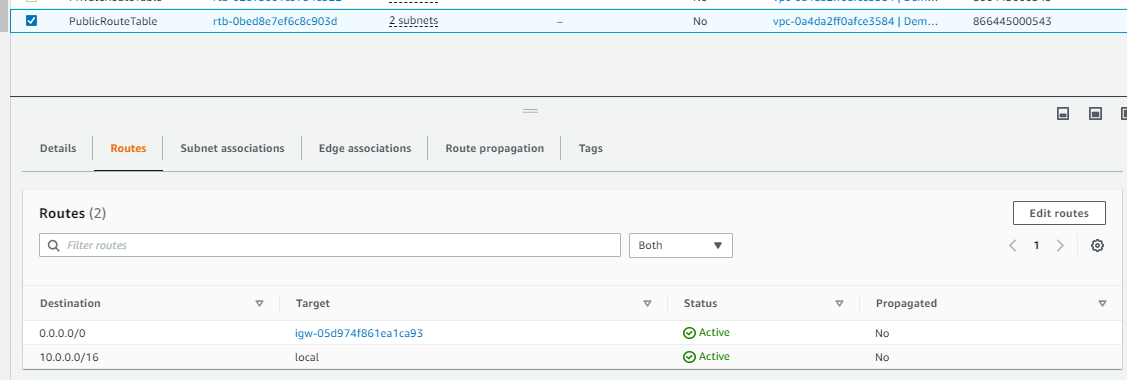
**vpc creation and connecting RDS(mqsql) in private subnet from different vpc Ec2 instance and public/private subnet of same vpc Ec2 instance & VPC Endpoints & VPC Flow logs with Athena**

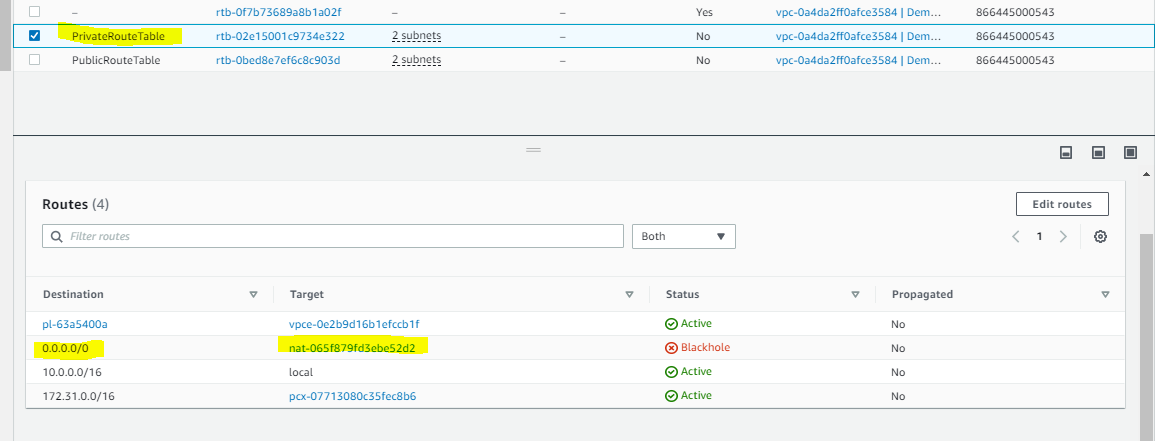


1.Created an vpc with 2 public subnets and 2 private subnets

2.Attach an IGW(internet gateway) to VPC

3.Created 2 route tables.one for public and other for private and associated the corresponding subnets.

4.Routetable of public is provided with IGW and an NAT gateway is created as public and adding NAT to route table of private subnet to access 0.0.0.0/0



5.RDS instance is created in private subnet ip by creating an

DB subnet group

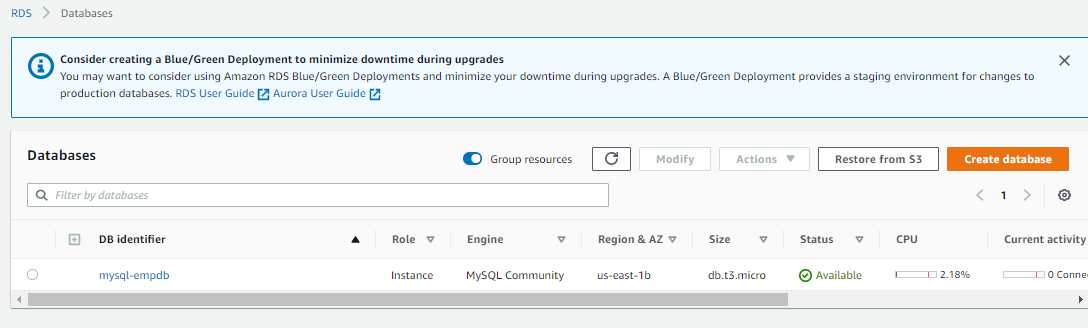
To create a new subnet group, give it a name and a description, and choose an existing VPC. You will then be able to add subnets related to that VPC.

Availability Zones

Choose the Availability Zones that include the subnets you want to add.

Subnets

Choose the subnets that you want to add. The list includes the subnets in the selected Availability Zones.



6.created an ec2 instance in public subnet

And install mysql db

sudo yum install mysql

7.created NACL’s for

1.Ec2 instnaces that is public subnet.

2. DB nacl for private subnet

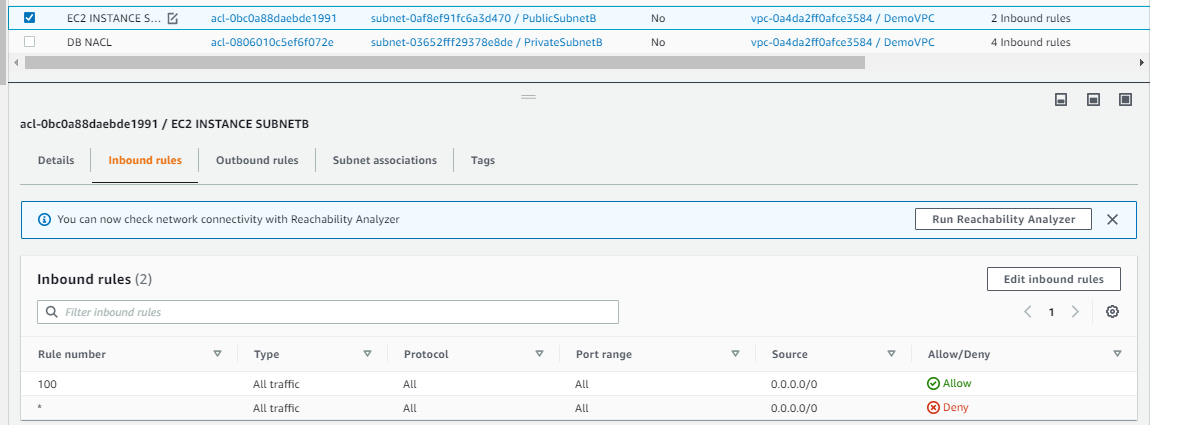
3.created an peering connection with default vpc and created vpc(DemoVPC)

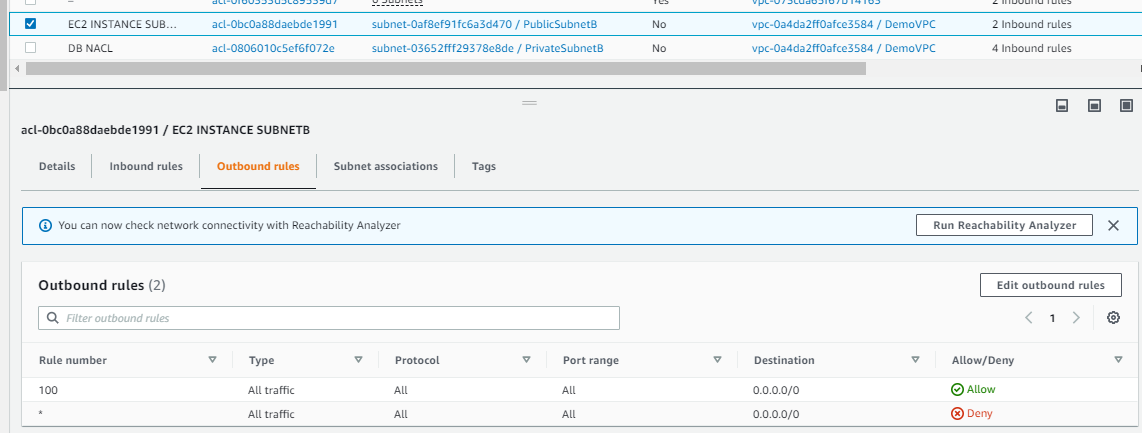
**\*\*\*\* for vpc peering to work we need to**

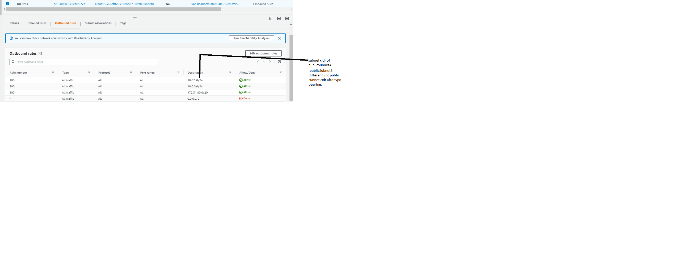
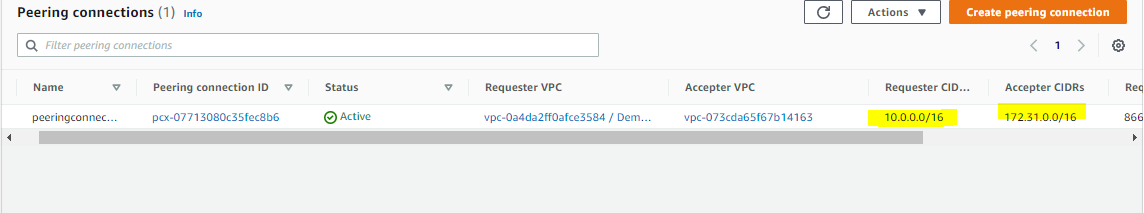
**To send and receive traffic across this VPC peering connection, you must add a route to the peered VPC in one or more of your VPC route tables**

**DEFAULTVPC(ROUTE TABLE OF THIS NEED TO ACCEPT CONNECTIONS FROM DEMOVPC)**

**DEMOVPC(ROUTE TABLE OF THIS NEED TO ACCEPT CONNECTIONS FROM DEFAULTVPC)**





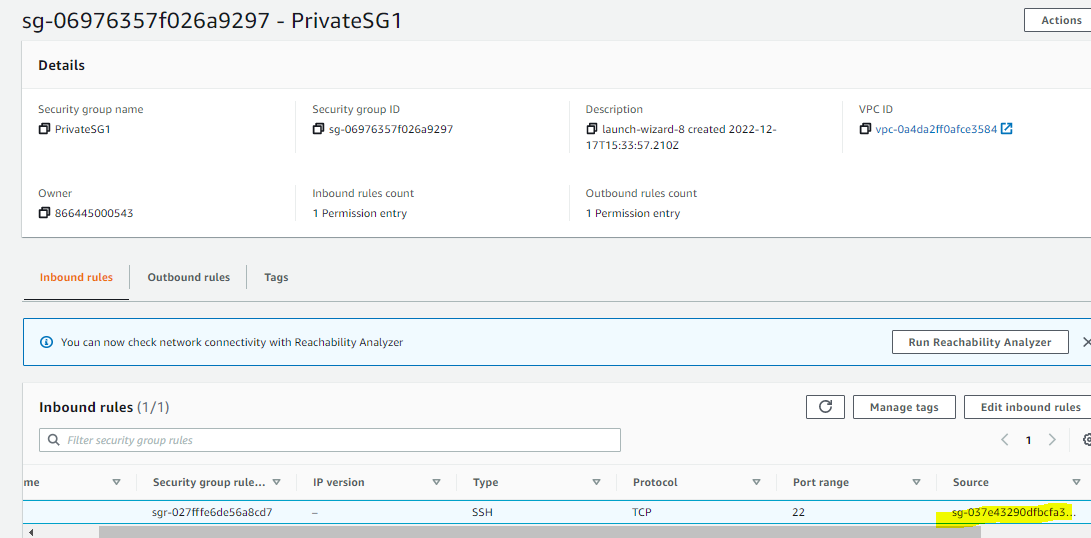


8.connect to ec2 instance from an baston host and connect to an private host

Below need to executed in baston host.

Baston host SG will allow SSH to 22 from anyip

But for private instance inbound rules baston host security group can only to SSH as below.



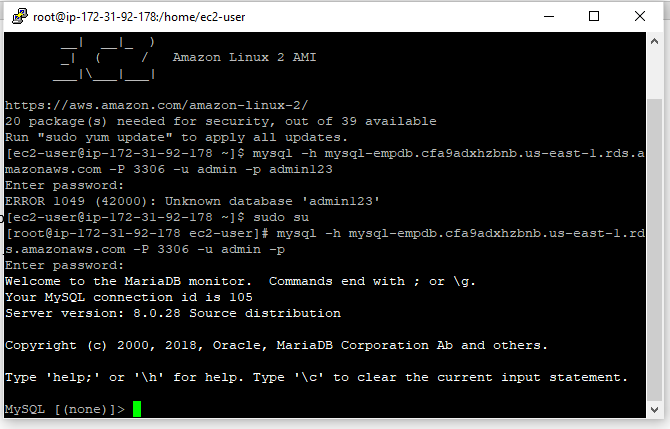
ssh ec2-user@<privateip of ec2> -i <pem file location of private ec2 instance>

once it is connected install sql and try to connect to RDS instance in private subnet.

SG for ec2 instance need to allow SSH access and for RDS instance SG it should allow TCP access to

3306 port.

mysql -h <hostname of RDS instance> -P 3306 -u <username> -p<password>



**Endpoints**

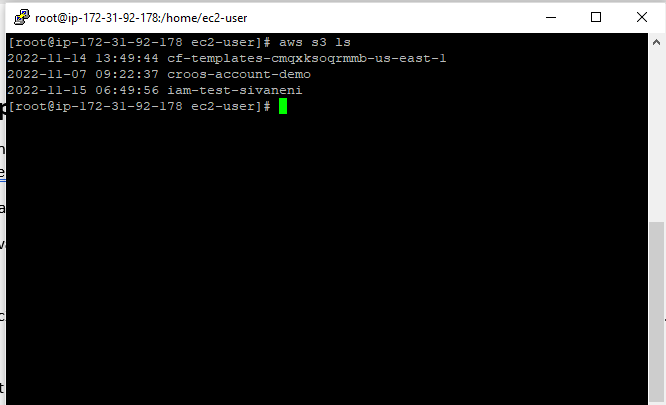
To connect to an aws services throw NAT🡪IGW🡪s3/dynamo DB we can create an endpoint and it can be Gateway or interface type.

Interface Type:need to explicitly associate an SG and subnet

Gateway type:need to select the associated route table only and no need of creating new SG

The ec2 instance need to have an IAM role to assume s3 readonlyaccess and attach the role to Ec2.

That it now we can connect our private ec2 instance to aws amazon s3 throw endpoint.



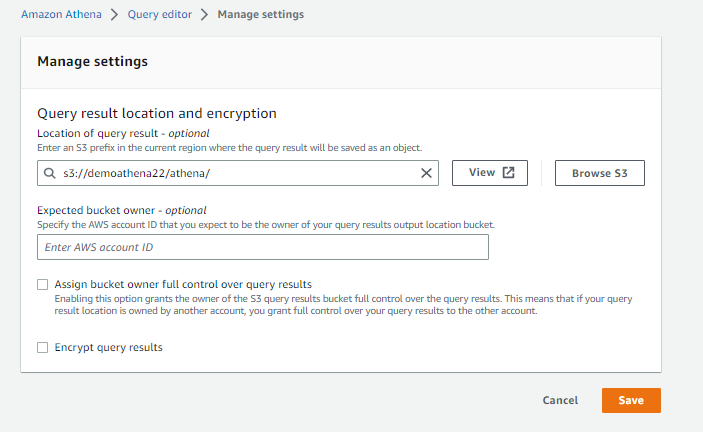
**Analyzing vpc flow logs Athena:**

<https://docs.aws.amazon.com/athena/latest/ug/vpc-flow-logs.html>

To analyize the traffic and check the source ip’s (‘Accept)’(‘/reject’)

1.Create an flow log and provide an s3 bucket

2.create an another bucket for Athena in the current region where the query result will be saved as an object.



3.Query the flow logs from Athena throw below commands

The marked yellow was the s3 bucket created in step-1 to analyze flowlogs.

CREATE EXTERNAL TABLE IF NOT EXISTS `vpc\_flow\_logs` ( `version` int, `account\_id` string, `interface\_id` string, `srcaddr` string, `dstaddr` string, `srcport` int, `dstport` int, `protocol` bigint, `packets` bigint, `bytes` bigint, `start` bigint, `end` bigint, `action` string, `log\_status` string, `vpc\_id` string, `subnet\_id` string, `instance\_id` string, `tcp\_flags` int, `type` string, `pkt\_srcaddr` string, `pkt\_dstaddr` string, `region` string, `az\_id` string, `sublocation\_type` string, `sublocation\_id` string, `pkt\_src\_aws\_service` string, `pkt\_dst\_aws\_service` string, `flow\_direction` string, `traffic\_path` int ) PARTITIONED BY (`date` date) ROW FORMAT DELIMITED FIELDS TERMINATED BY ' ' LOCATION 's3://cloudwatchbuc22/AWSLogs/866445000543/vpcflowlogs/us-east-1/' TBLPROPERTIES ("skip.header.line.count"="1")

To query particular date flow logs alter the table with below query

ALTER TABLE vpc\_flow\_logs ADD PARTITION (`date`='2022-12-19') LOCATION 's3://cloudwatchbuc22/AWSLogs/866445000543/vpcflowlogs/us-east-1/2022/12/19/'

<notes_vpc.txt>