Visualize data in Amazon RDS (Relational Database Service) with QuickSight

In this project we will create a relational data base and connect it with Quicksight to visualize . Agenda is to learn how database can be managed with AWS

**IAM in AWS** means **Identity and Access Management**.

Think of it like a **security guard system** for AWS.
It helps you decide **"Who can do what"** in your AWS account.

**Example:**

- You (the account owner) are like the **house owner**.
- You can create **keys** (IAM Users) to give to other people (like friends, employees).
- Each key can open only certain **rooms** (services) depending on the rules you set (IAM Policies).

**Main parts of IAM:**

1. **IAM Users** → individual people or apps who need access.
2. **IAM Groups** → a collection of users (e.g., "Developers" group).
3. **IAM Roles** → temporary permissions that apps or services can use.
4. **IAM Policies** → the **rules** that define what actions are allowed or denied.

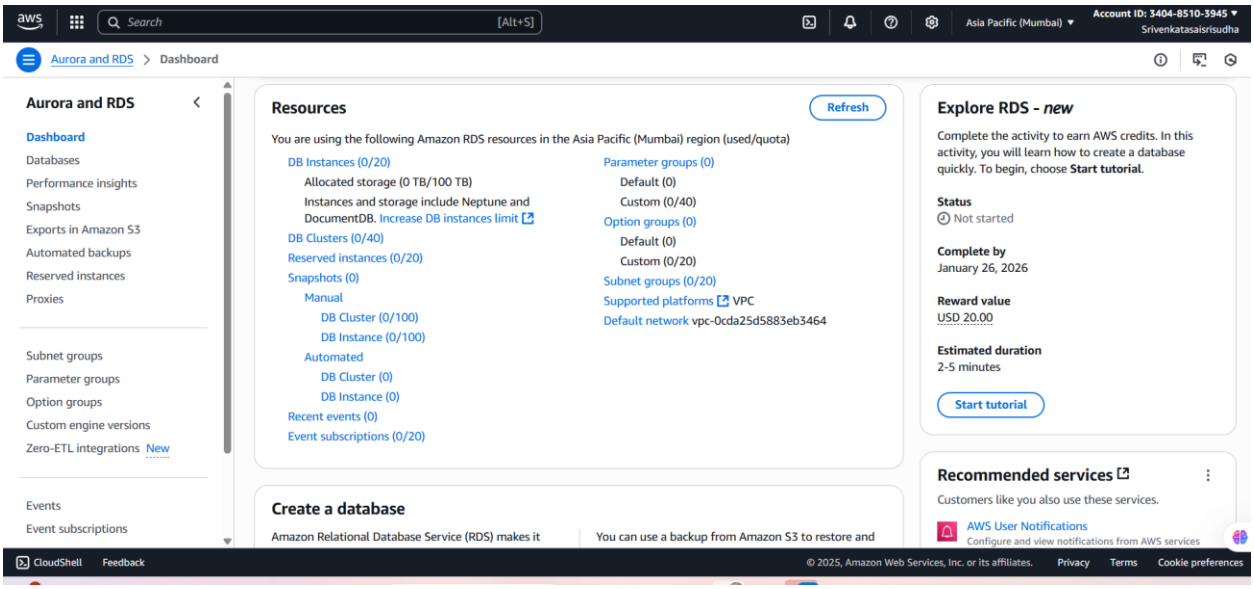
**Why is IAM important?**

- Keeps your AWS account **safe**.
- You don't have to share your **root account password** with everyone.
- You can give people **only the access they need** (nothing more).

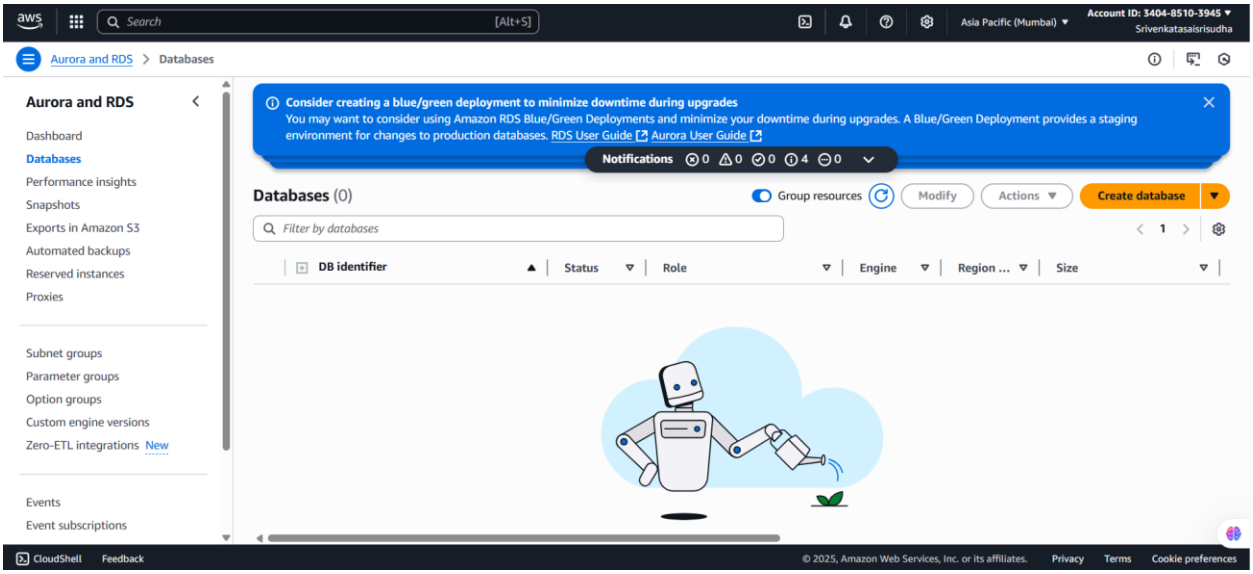
So, IAM = **a lock-and-key system for AWS services**

Step 1 :Create a database becz we want to connect with quicksight

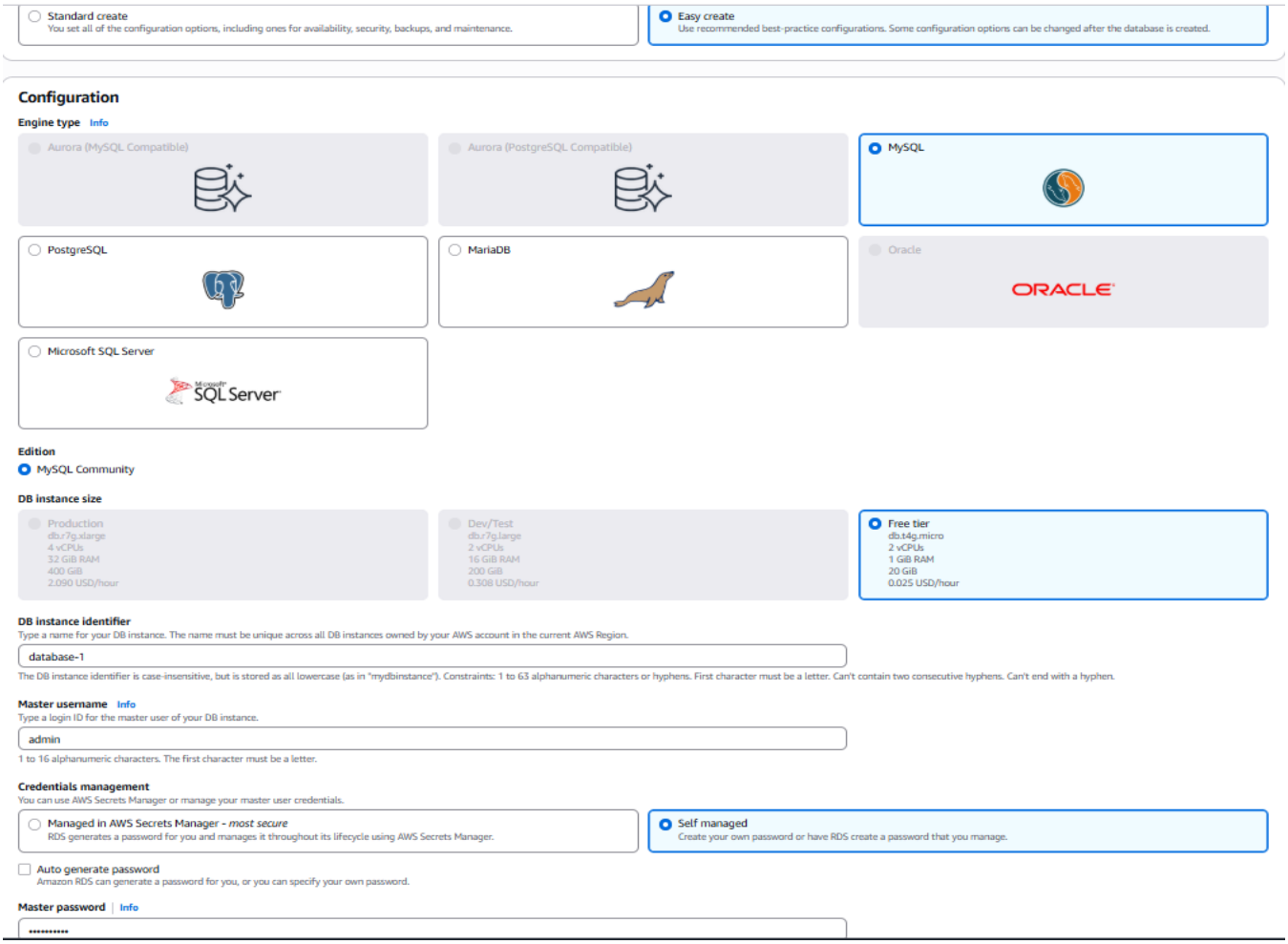
Search for RDS in the amazon console




Step 2: Go to database and create a database as shown in the figure




Step 3: Click on easy create and click on MySQL and free tire




Difference between SQL and MYsql

**SQL**

- Full form → **Structured Query Language**.
- It's a **language** used to talk to databases.
- Example: You can use SQL commands like:
    - SELECT * FROM students; → shows all students.
    - INSERT INTO students VALUES (1, 'Ramesh', 20); → adds a student.

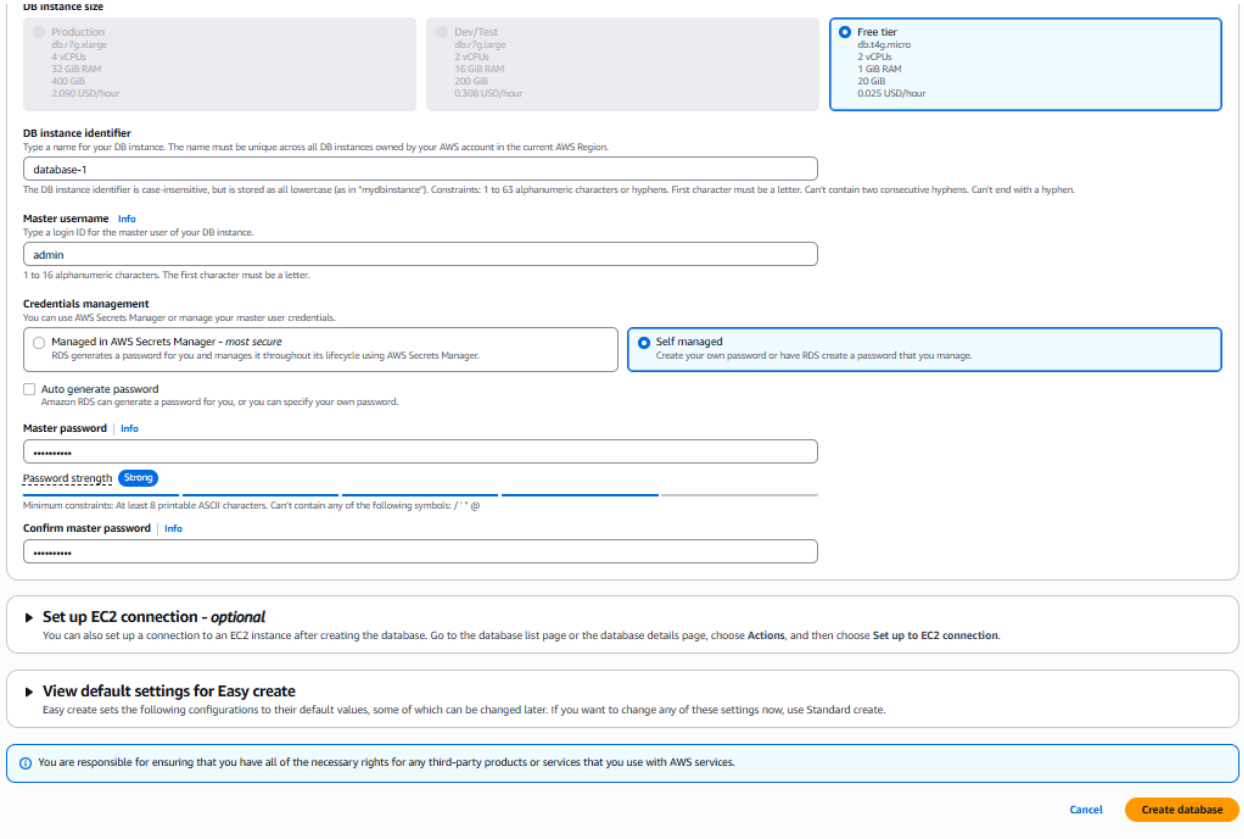
Think of SQL like **English for databases**.

**MySQL**

- MySQL is a **database software** (a system) where you can store your data.
- It uses **SQL language** to work.
- Example: You install MySQL → create a database → then use SQL commands to manage it.

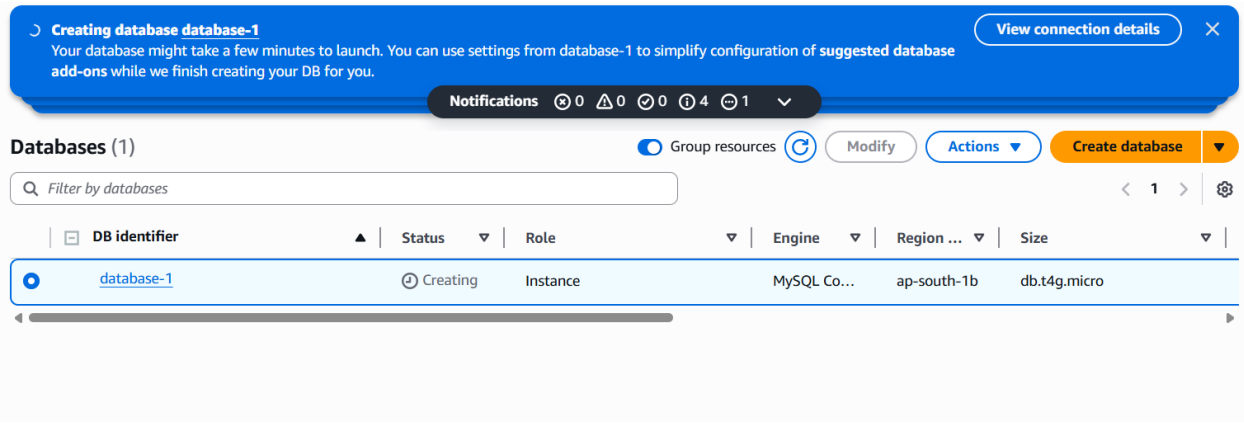
Think of MySQL like a **library**, and SQL is the **language you use to ask the librarian** for books.

Mysql is relational database management system and sql is a lang stands for structured query lang is used to manipulate mysql databases




Step 4: Click on create database

Now the database is created




So I created the database using aurora and RDS and quickly configured using easy create function

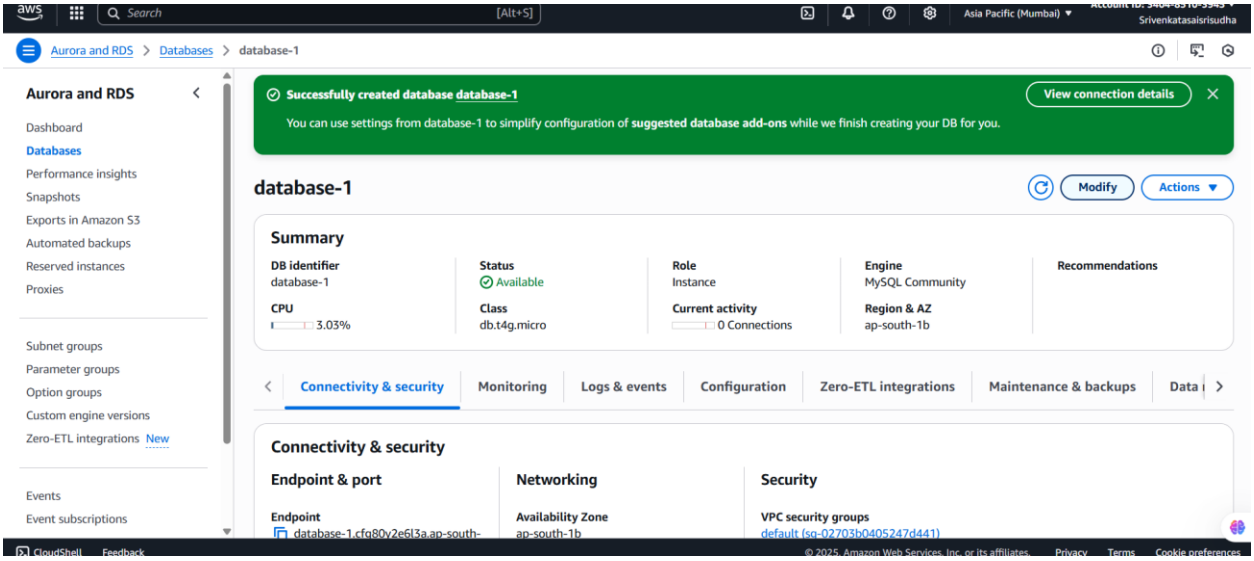
Now, we need to connect mysql workbench to enter data in-order to do that I need to connect with RDS instance

**RDS Instance**

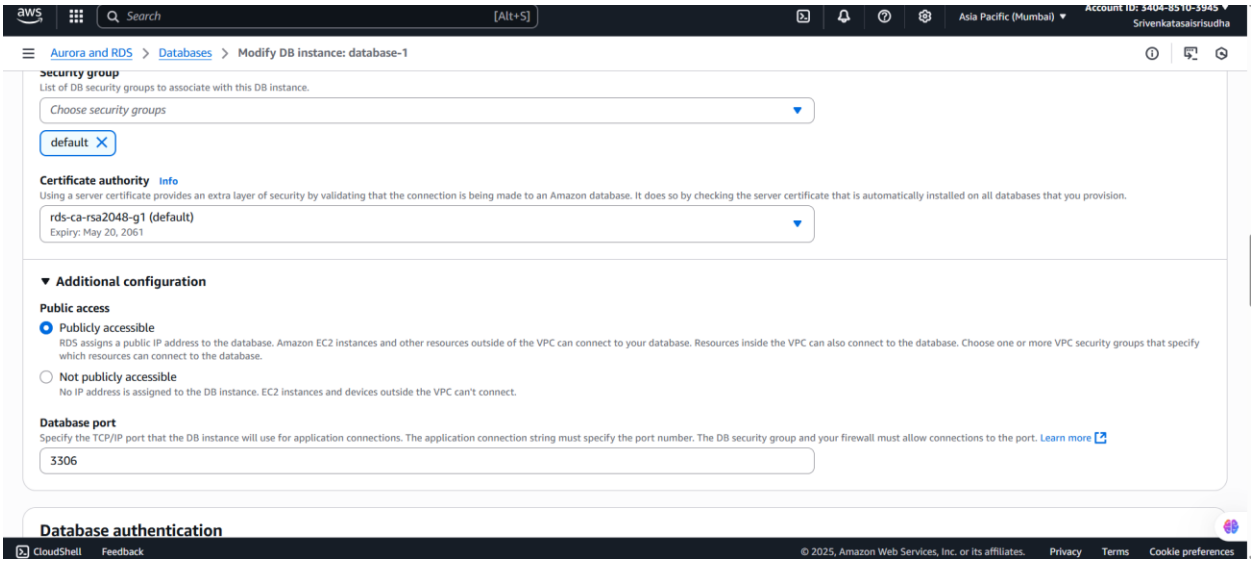
- An **RDS instance** is simply a **database server in the cloud** that AWS runs for you.

- Instead of you buying a computer, installing MySQL, keeping it secure, and taking backups... AWS does all that for you.

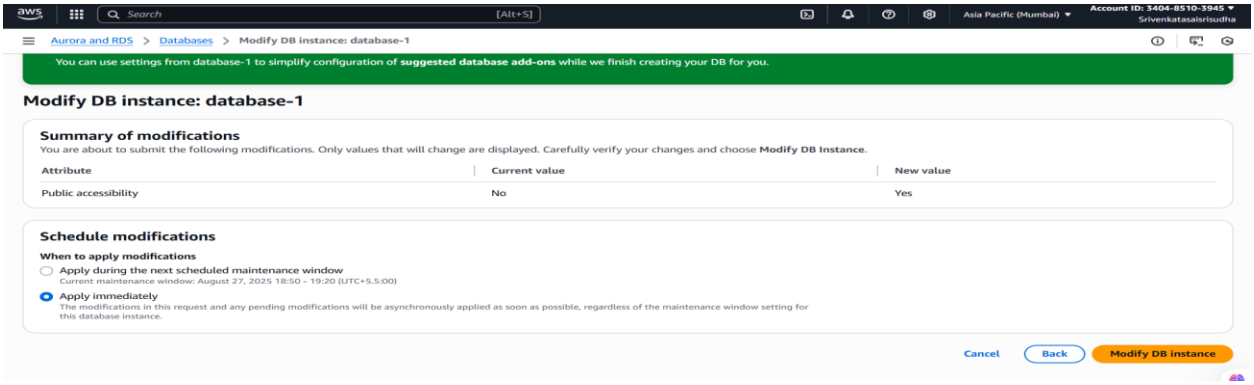
Step 5: Click on databases-1 and it shows like this




Step 6:Then click on modify  scroll down and click on publicly accessible

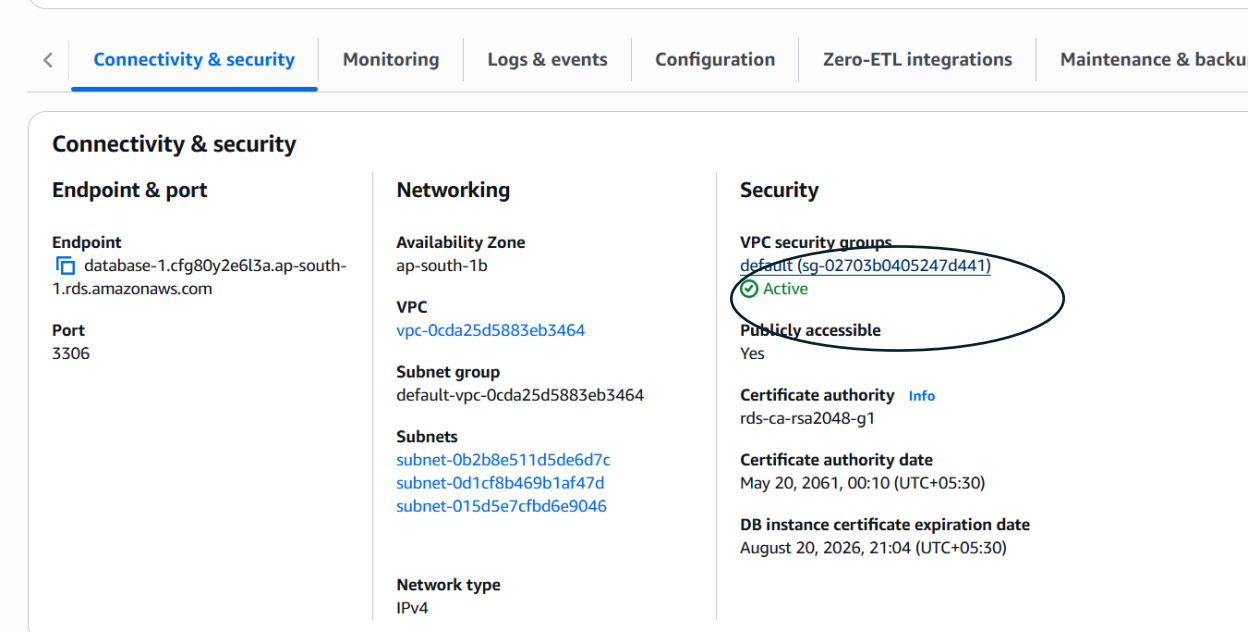



Step 7:Click on continue and apply immediately and modify DB instance

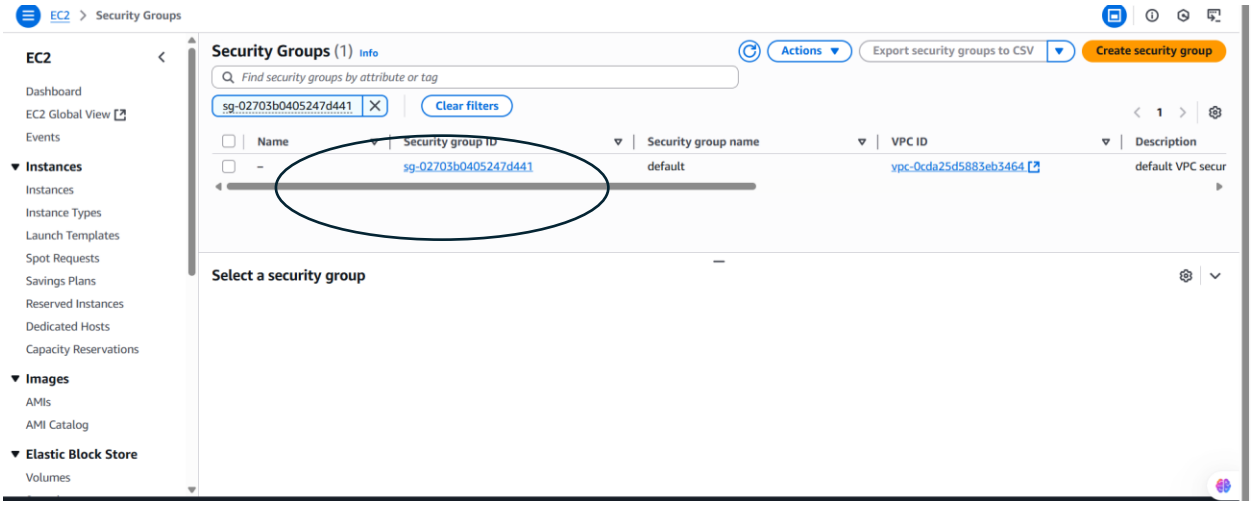


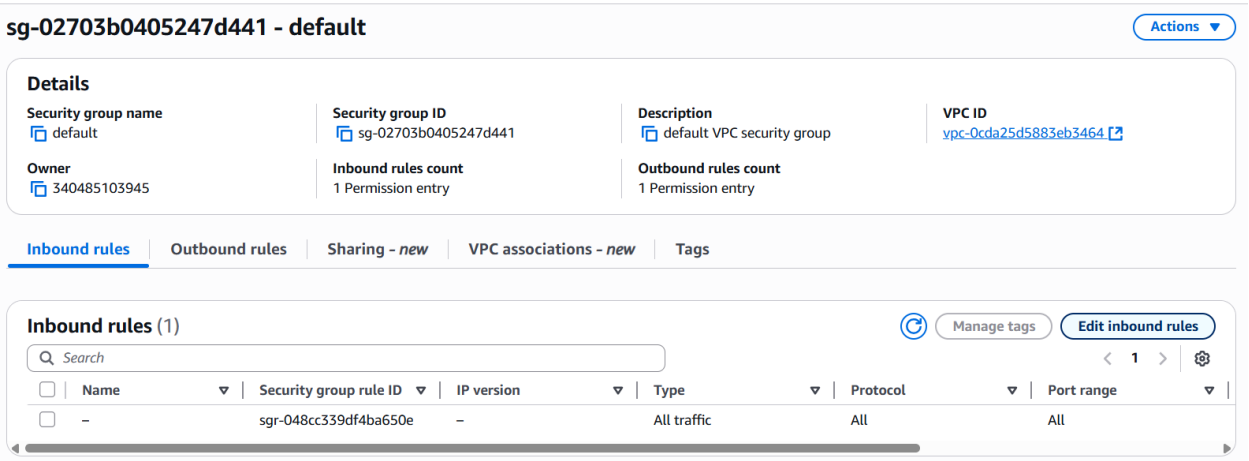
We made it public because MySQL workbench to connect to RDS instance.

Step 8: Now click on VPC Security groups




Step 9:Click on the group ID And click on edit inbound rules



Y do we need to edit inbound rules

We edit inbound rules to **decide who is allowed to knock on the door of our AWS server**.

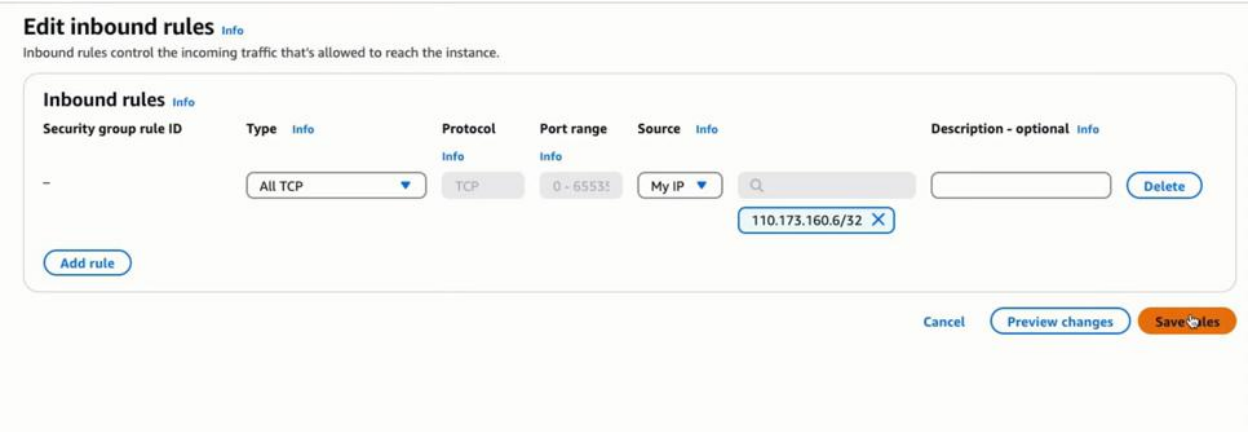
- If we don't edit → nobody can come in.
- If we allow too much → hackers can also enter.

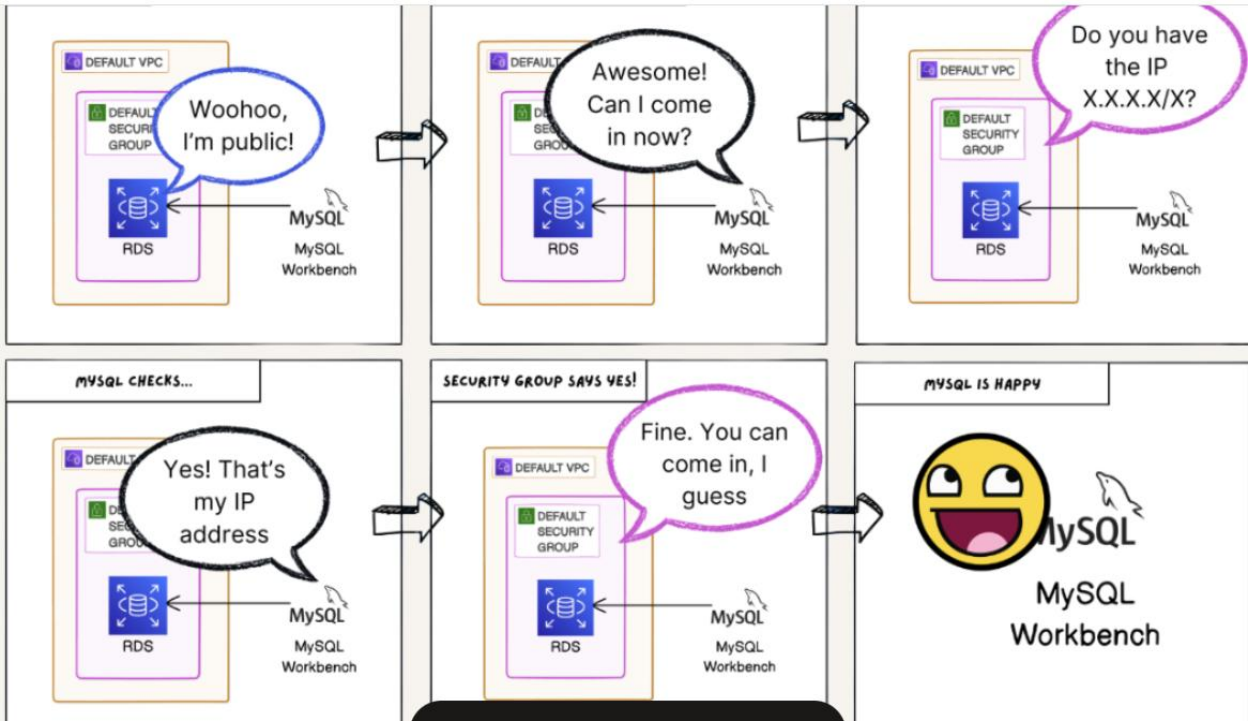
So we need to **edit carefully** → only the ports and IPs that we actually need.

Step 10:Add rule and click on all TCP and My IP, it allows all traffic from my IP Address

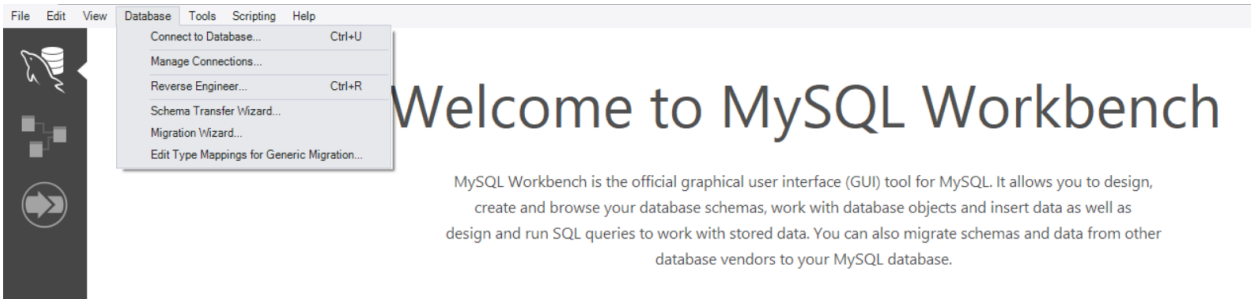
Step 11: click on save rules

I want sql workbench to have access to RDS instance when it is on my local machine

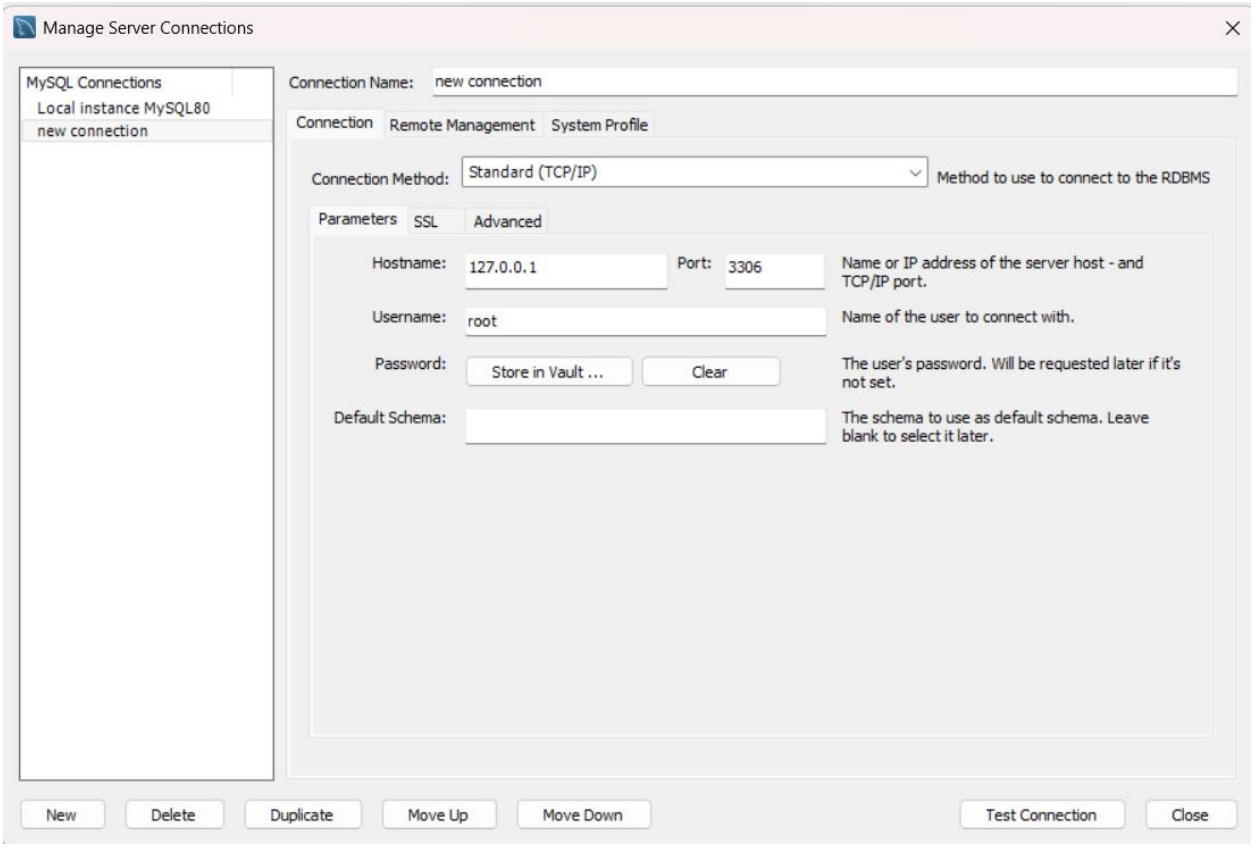


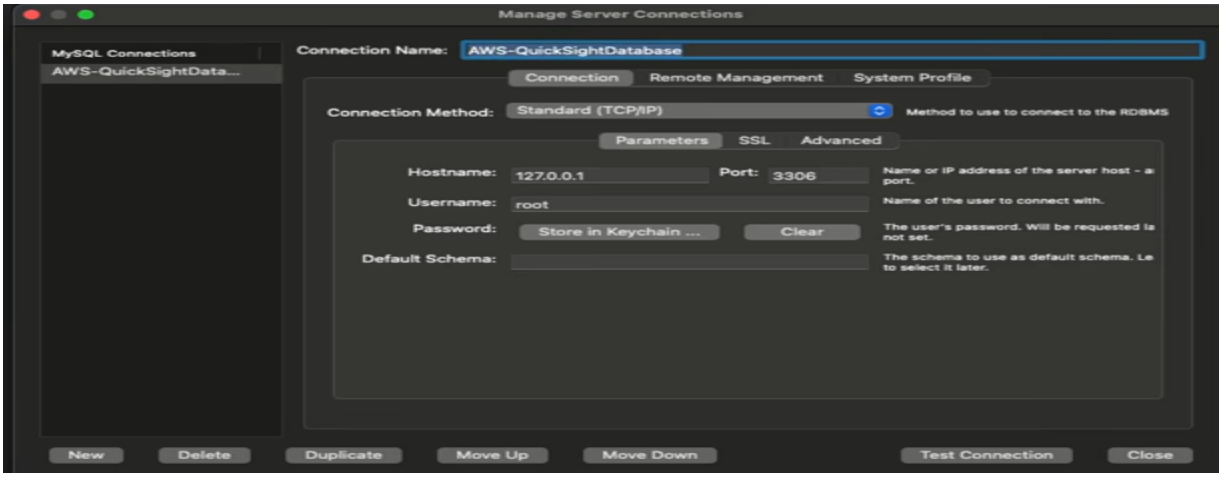

Step 12:Now go to Manage connections in MySQL Workbench



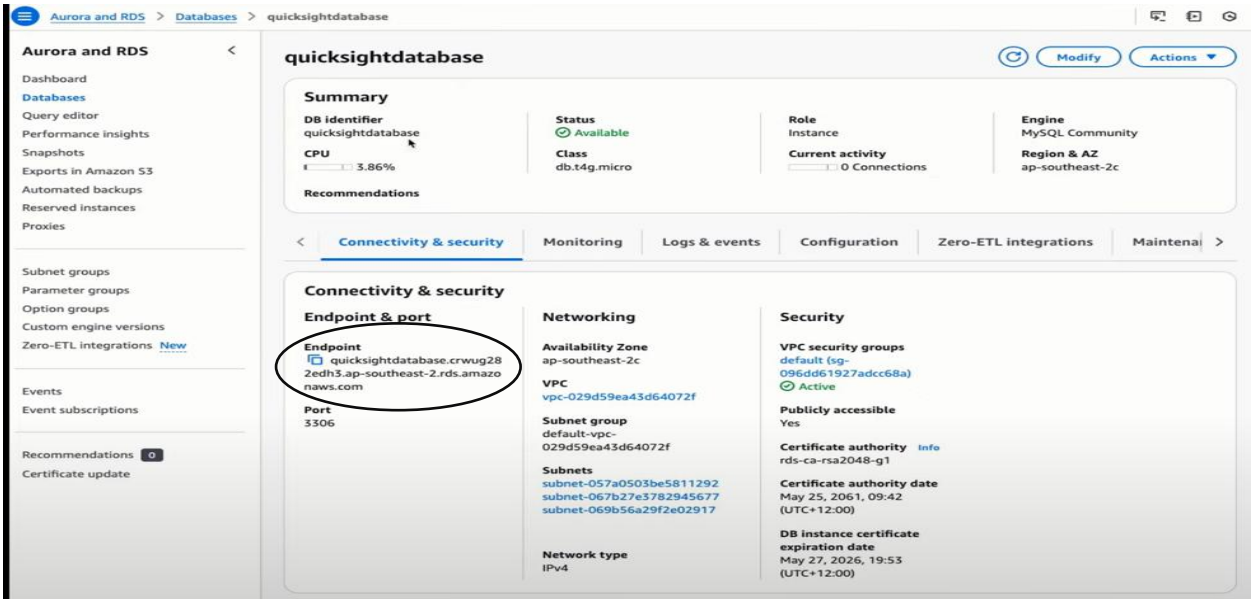

Step 13 :Select new and the below tab gets opened



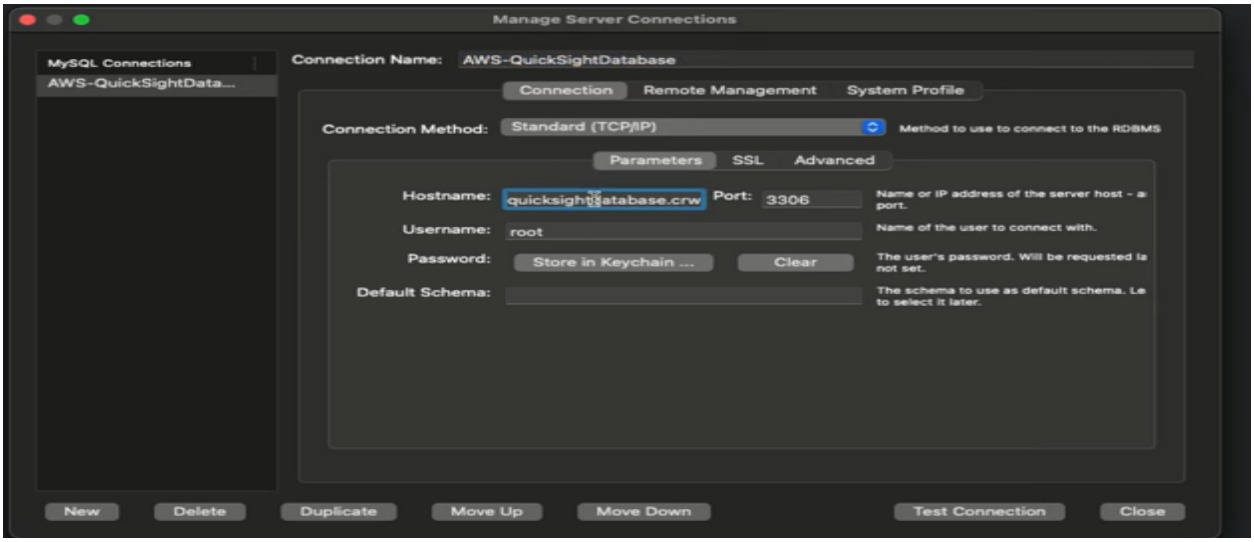

So the connection name is AWS-QuickSightDatabase



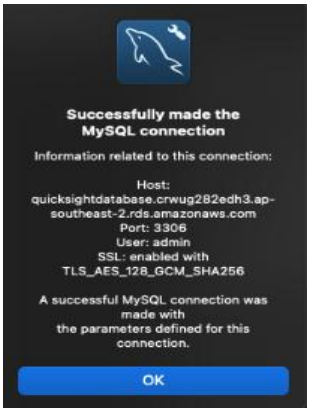

Step 14: And to get the connectivity, go to aurora and RDS and copy the link



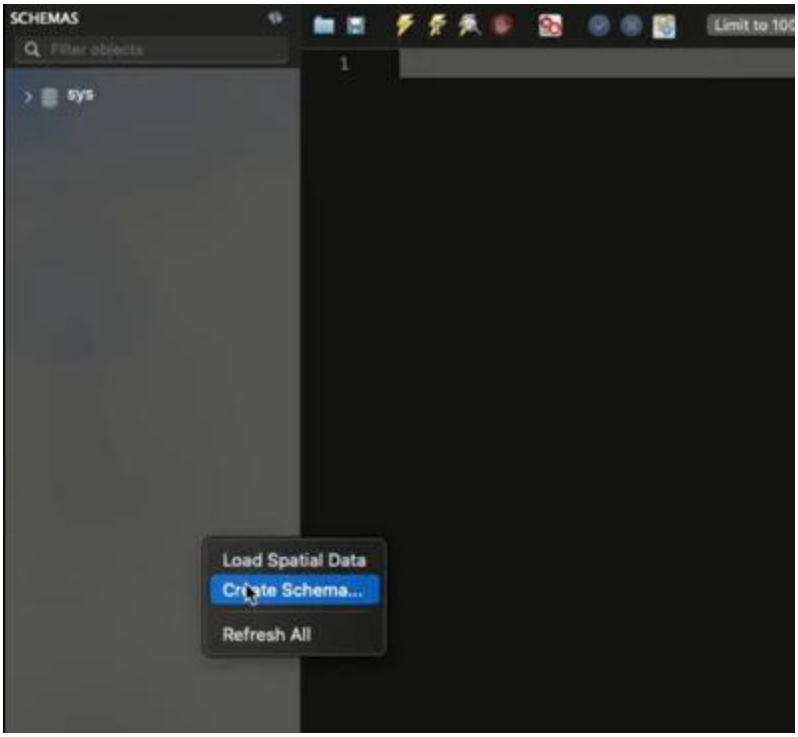

Step 15: Copy the link and paste under the Hostname



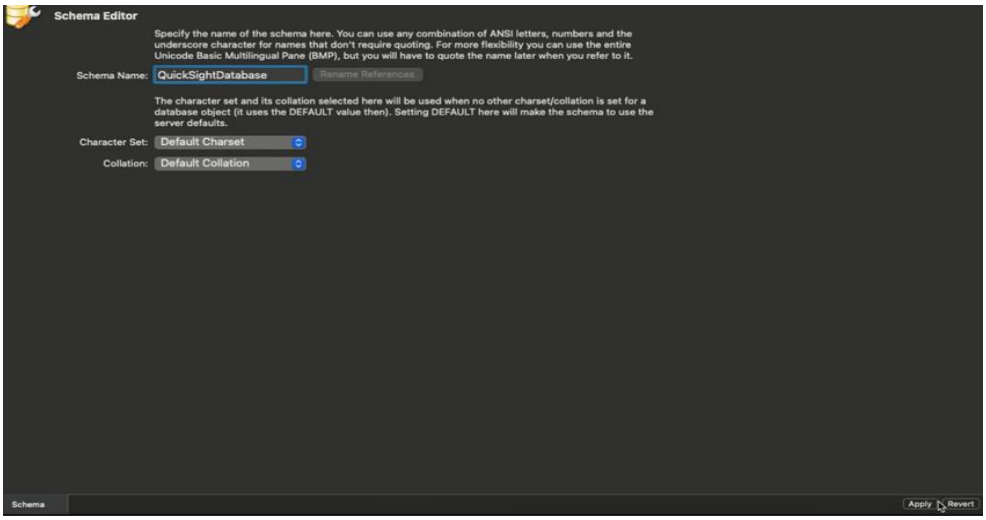

And the username and password will be the one we created in the step 3 remove root and add the username and click on store in keychain and write the password. Make sure the port is correct and then click on test connection.



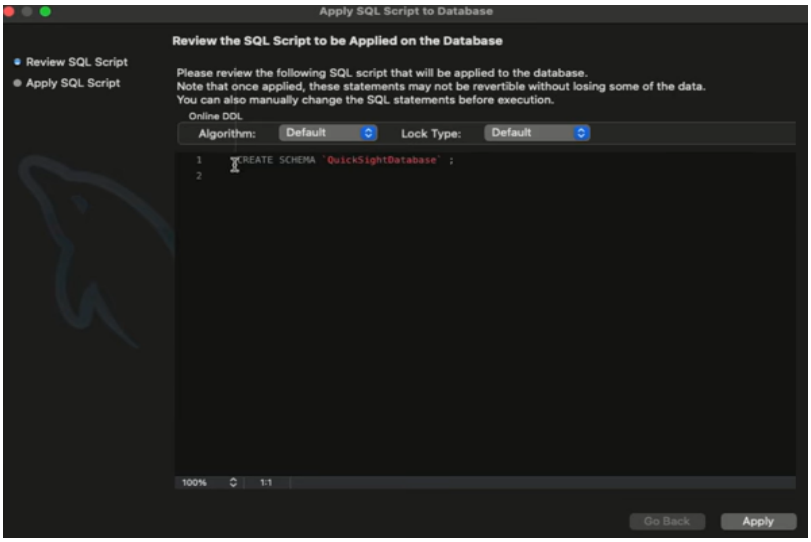
Step 16: Go to MySQL Connections and open under sys create new schema



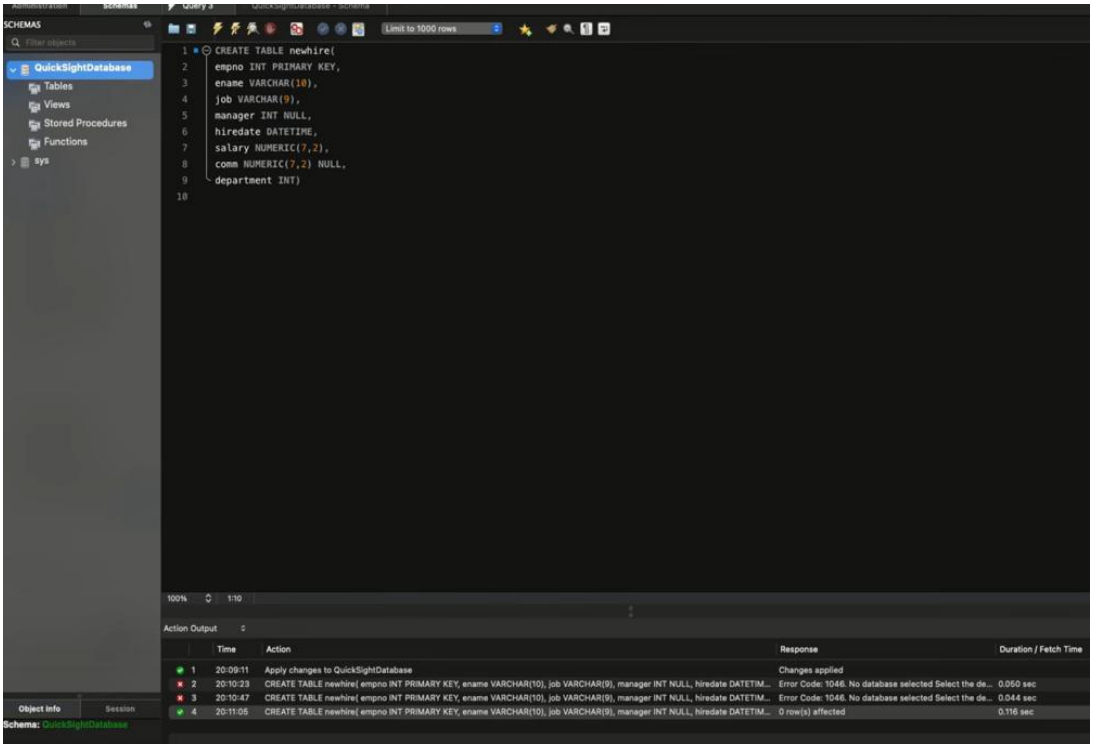

Step 17: Write the schema name as quicksightdatabase and click on apply



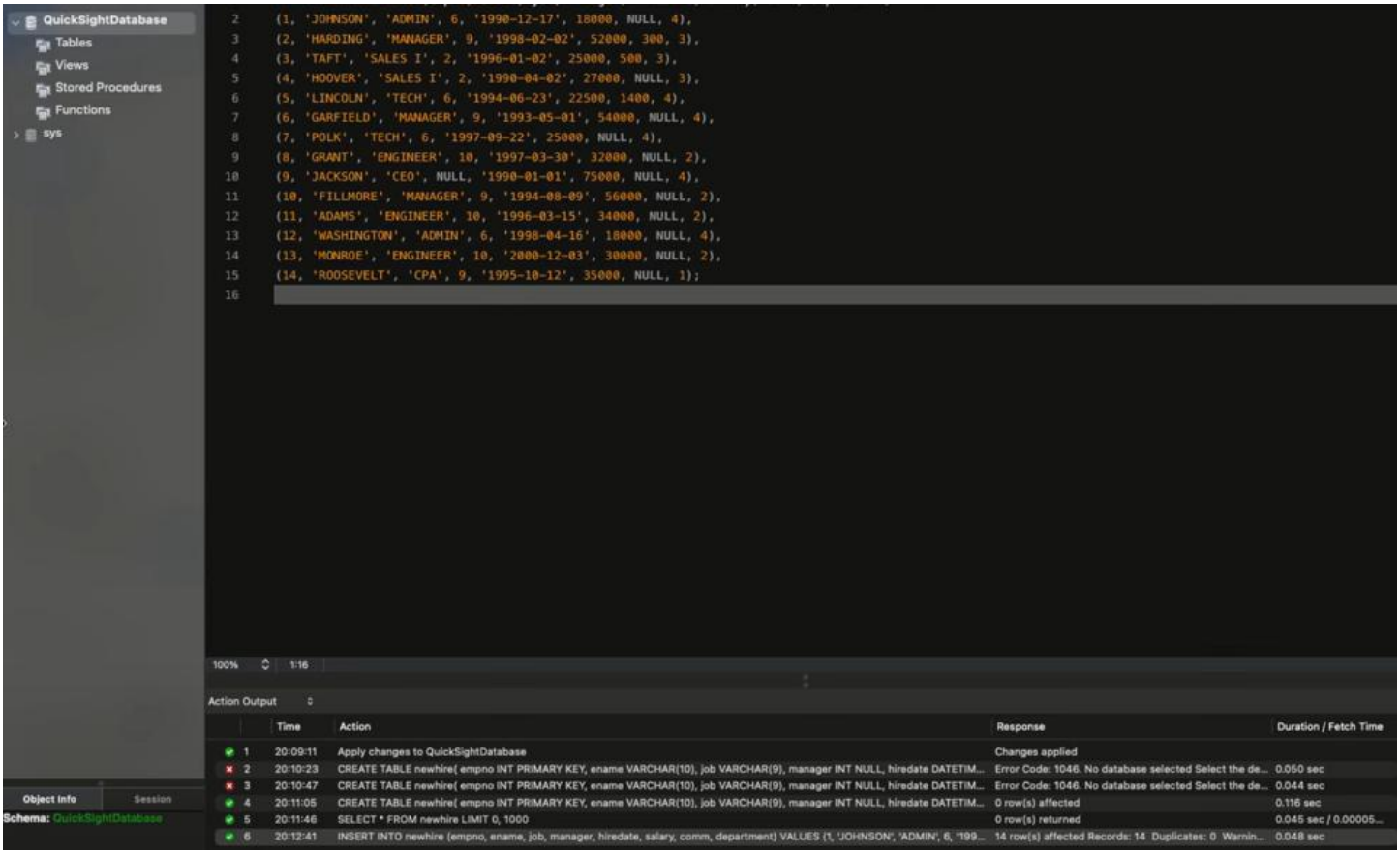

Step 18: Click Apply



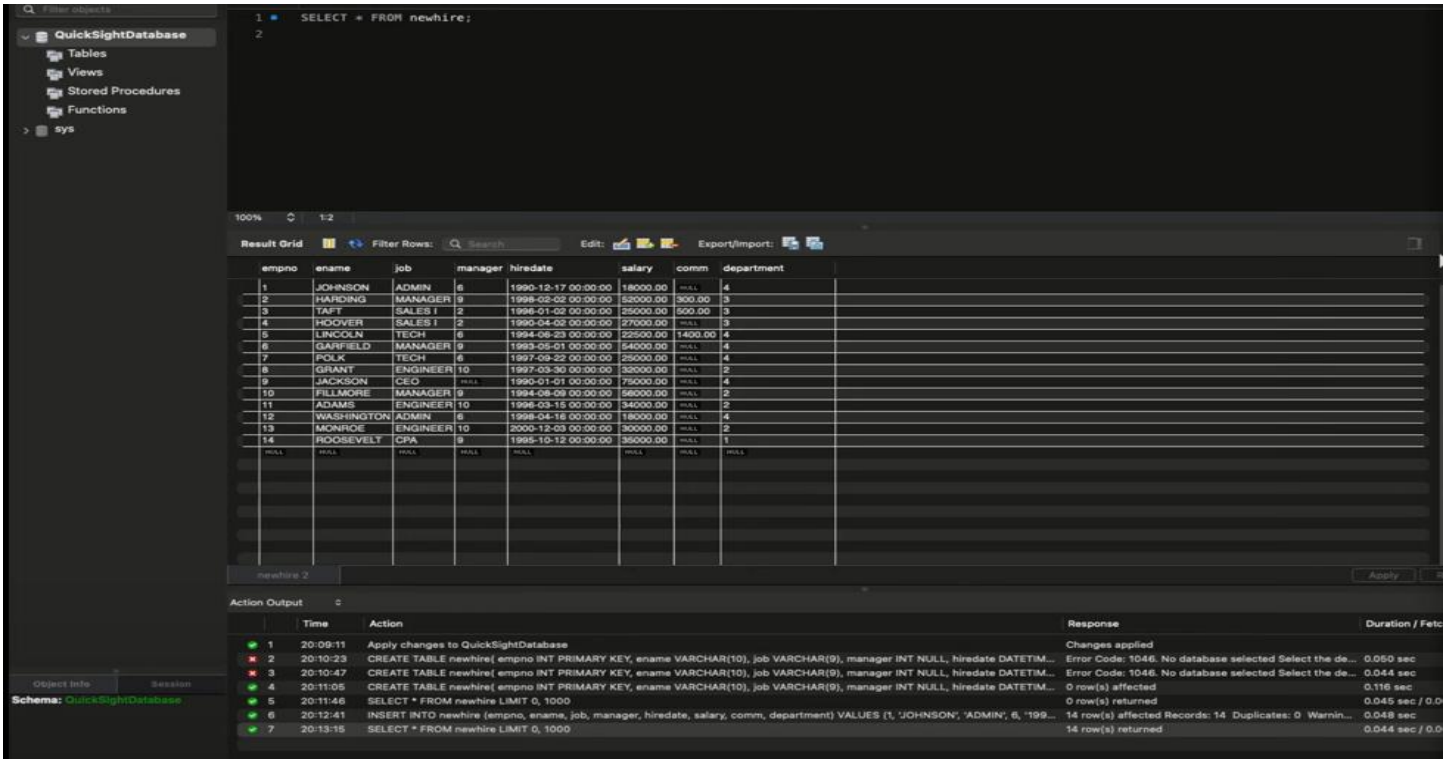

Step 19:Select the schema in which you want to enter the table and then write the query and run



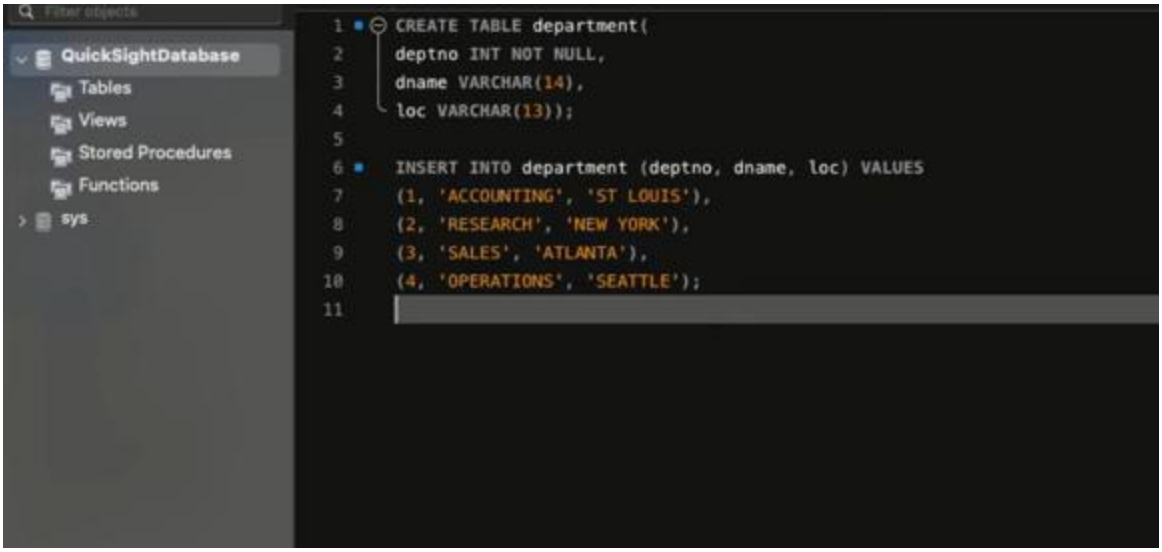

Step 20: Add the data into the table




And write the code select * from newhire to see the data we have inserted

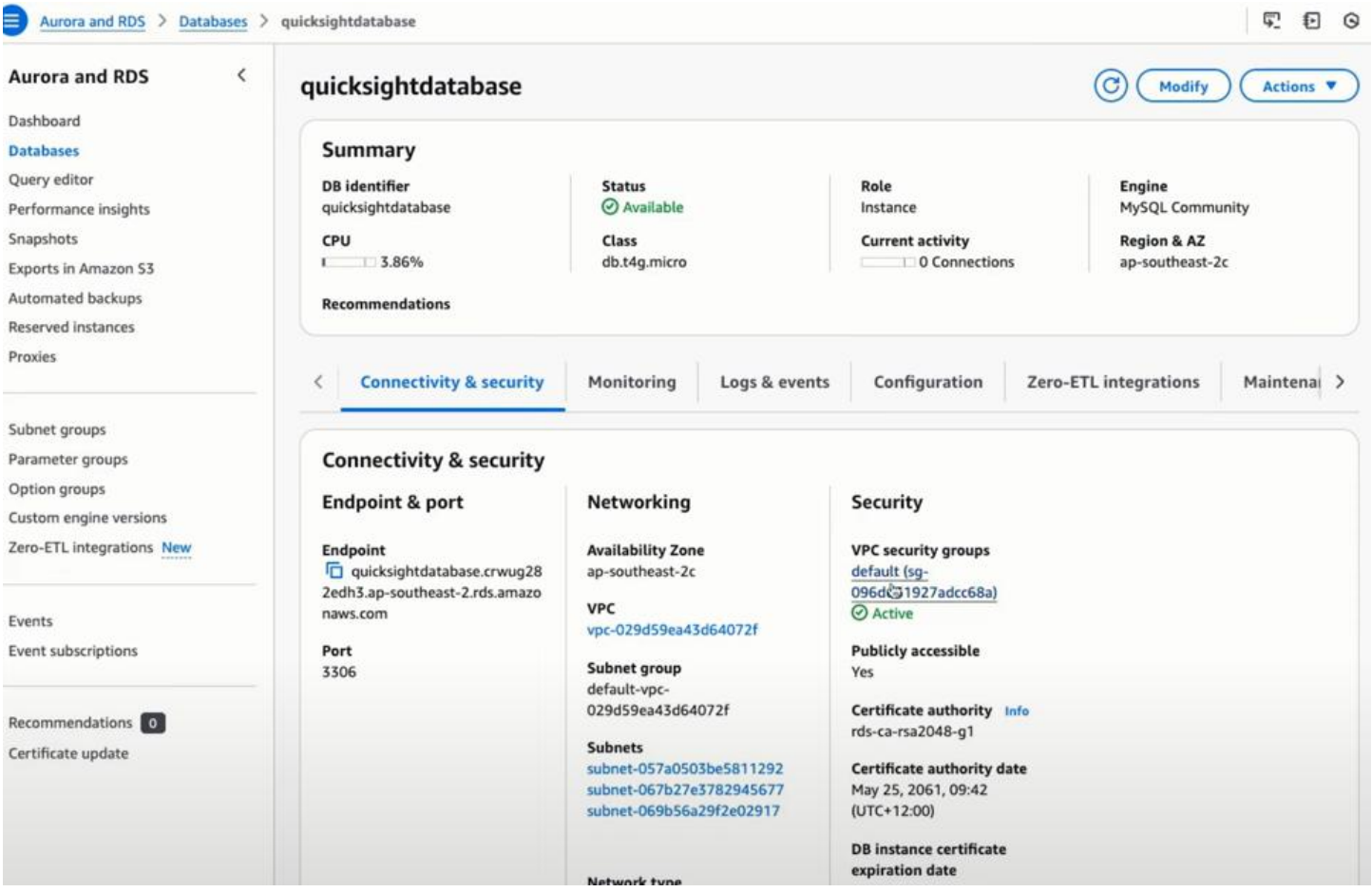



Step 21: Create other table with the code

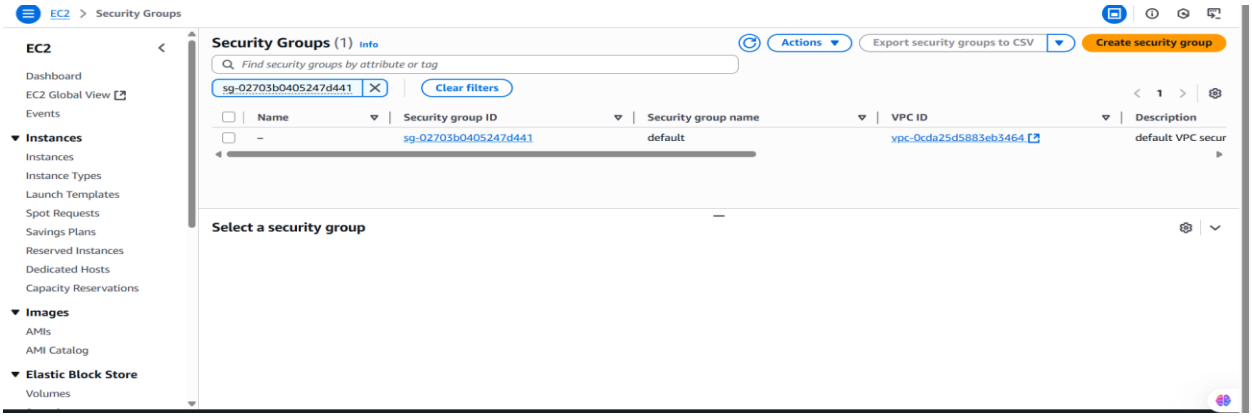


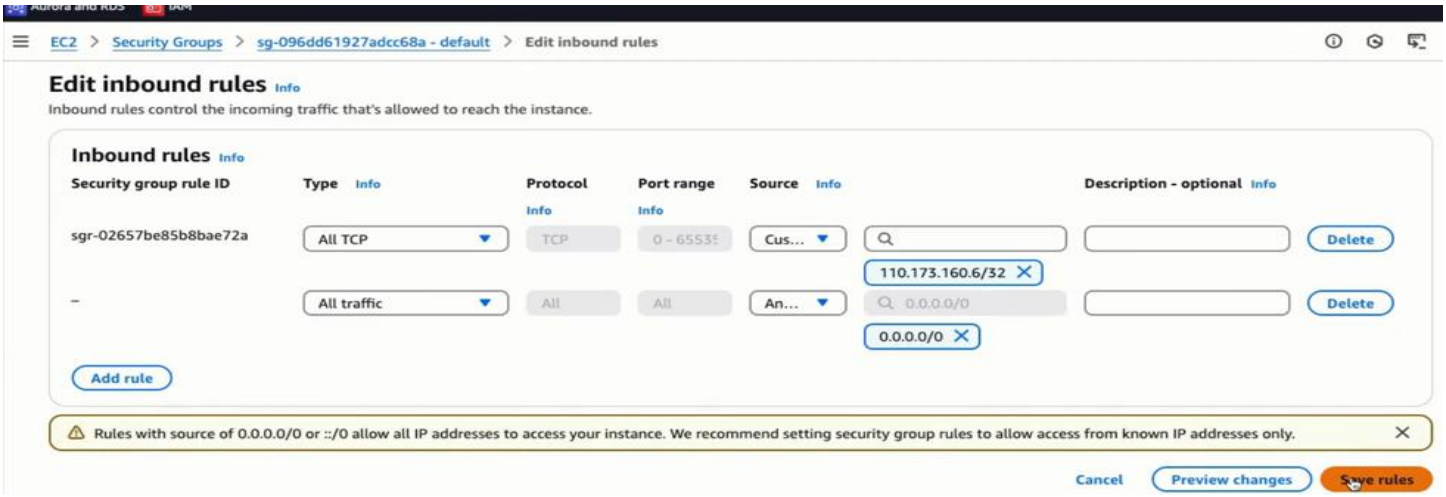

And do select * from department to see the rows

Step 22: We need to connect RDS to quicksight so we will edit the inbound rules,click on VPC security groups

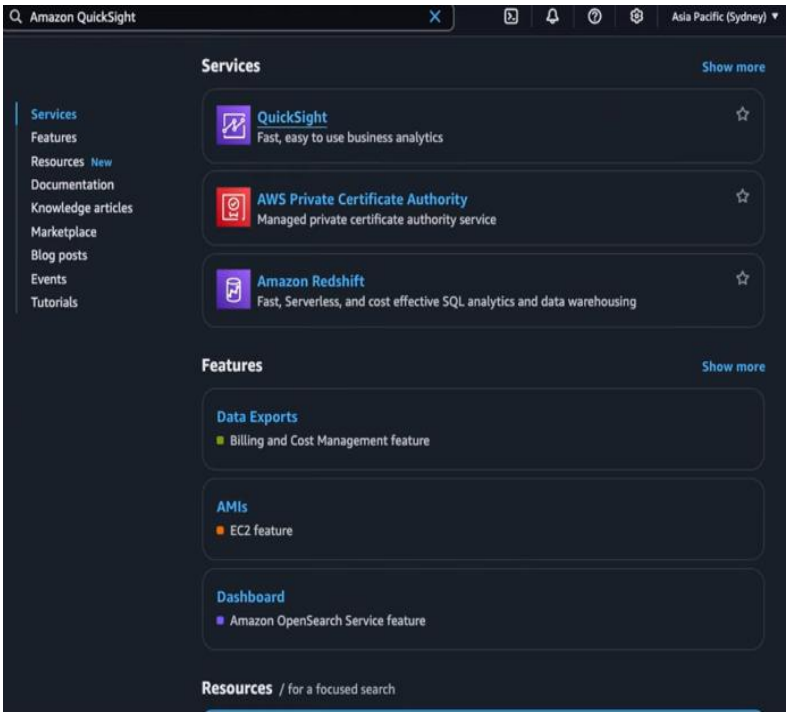



Step 23: Any Ip address any where should be able to access so we are giving the rules like that and save rules.

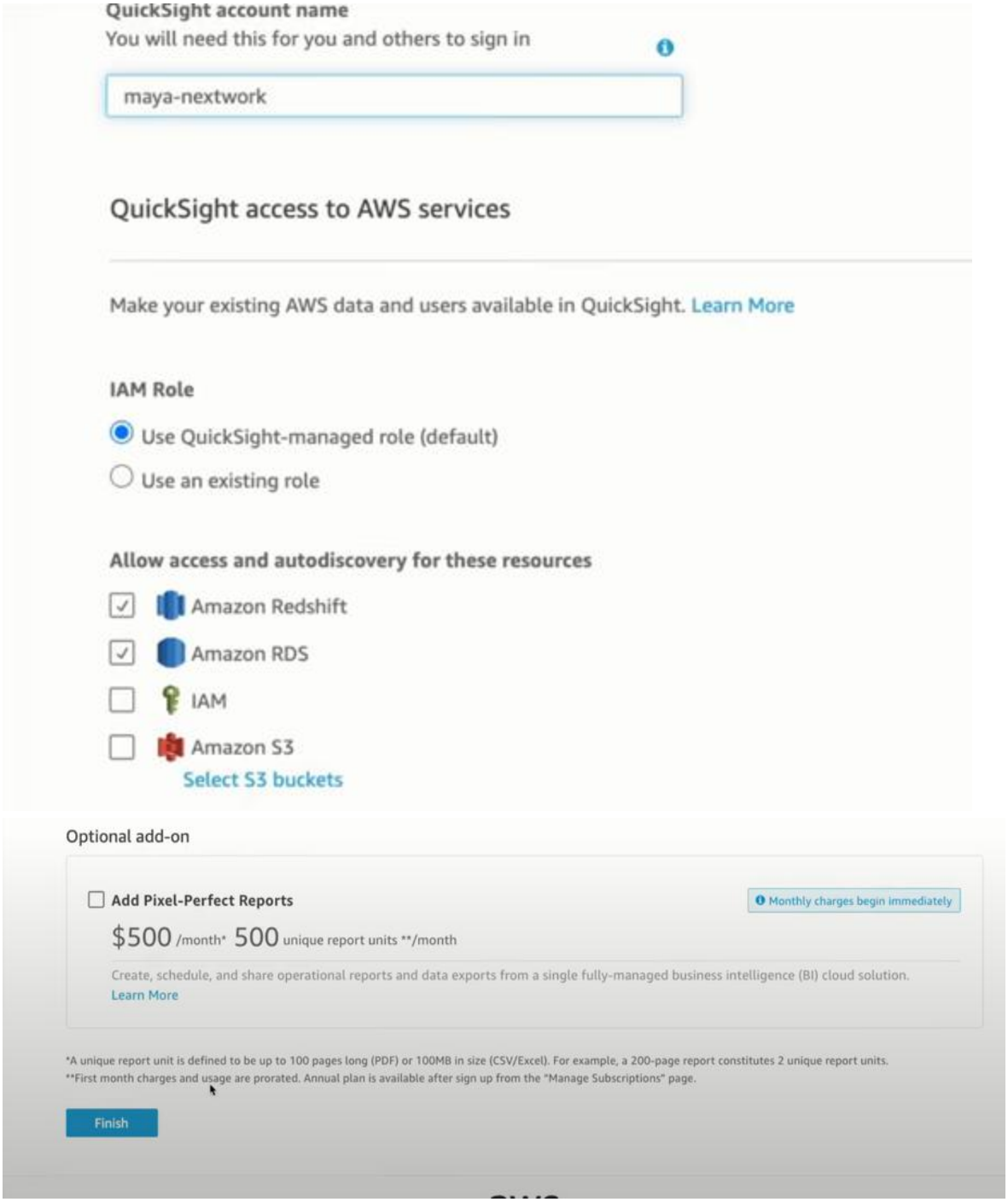



Now search for amazon quicksight.



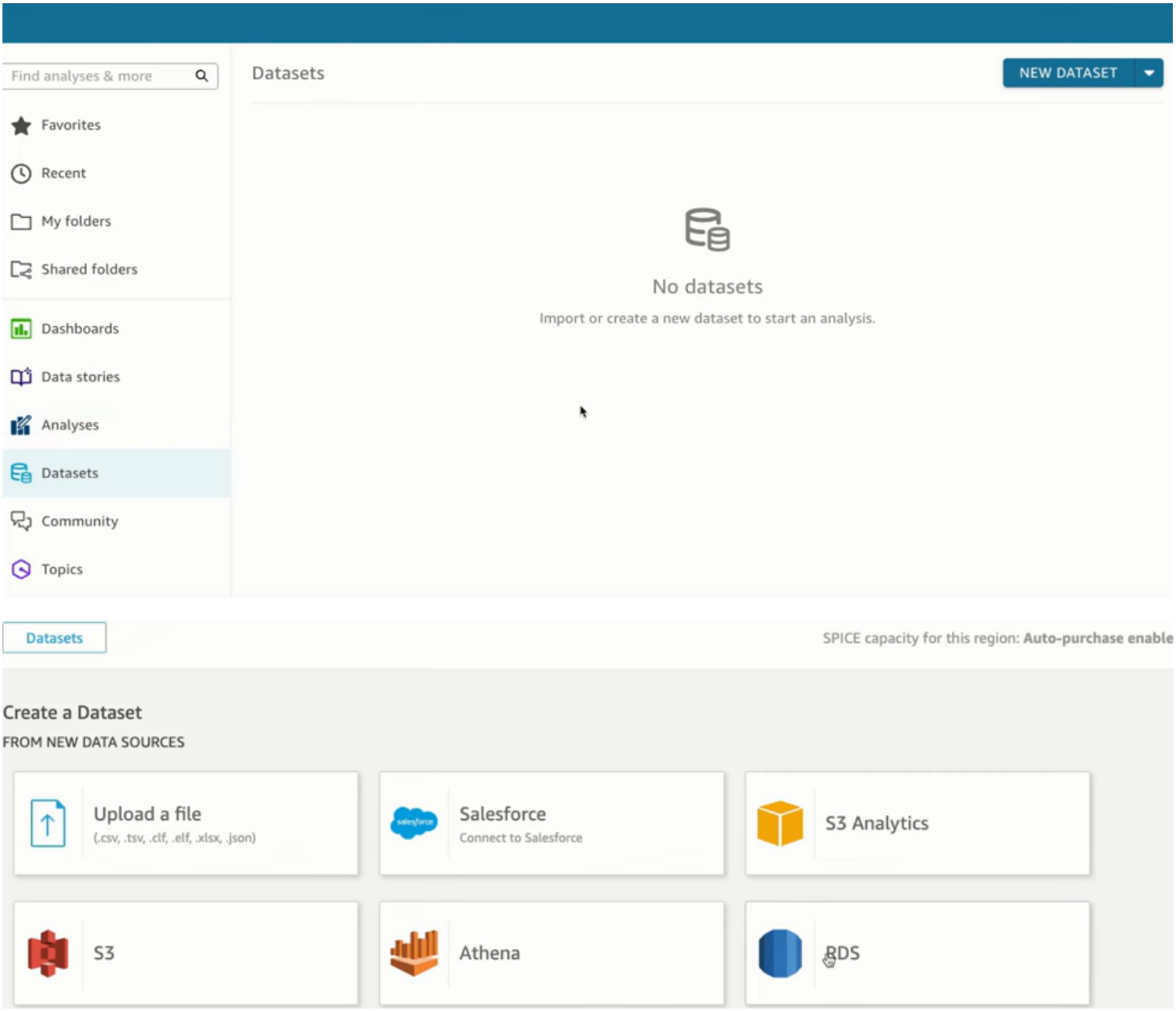

Step 24: While creating add the email and do and shown in the picture and click on Finish



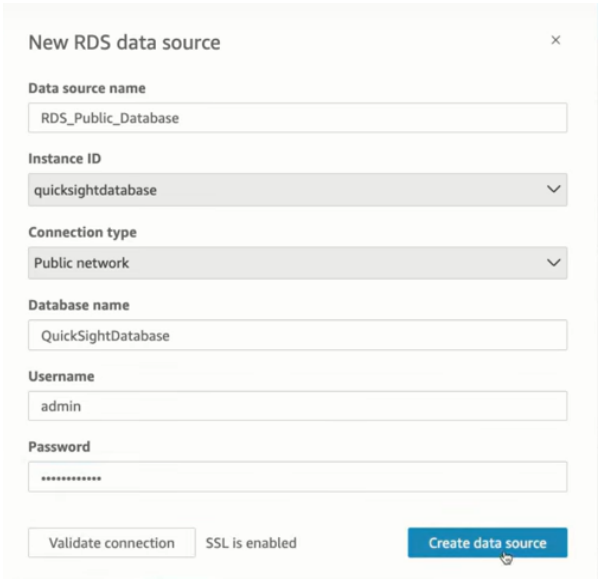




Step 25:As shown below go to new dataset and select RDS



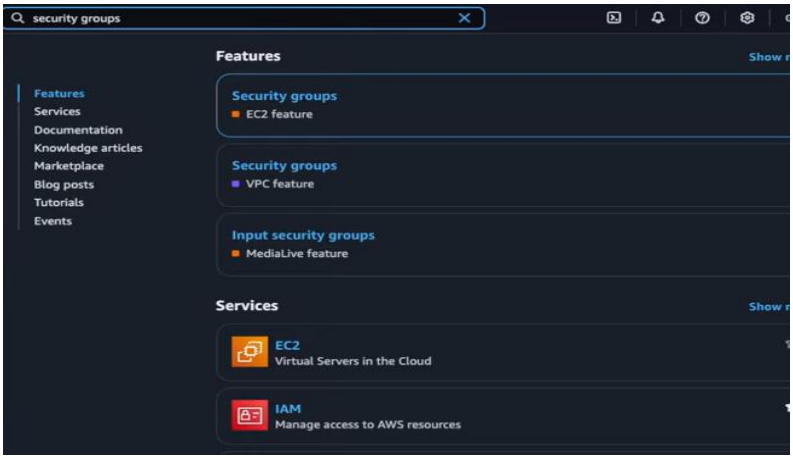

Step 26: username and password Step 3,validate the connection and create the data source



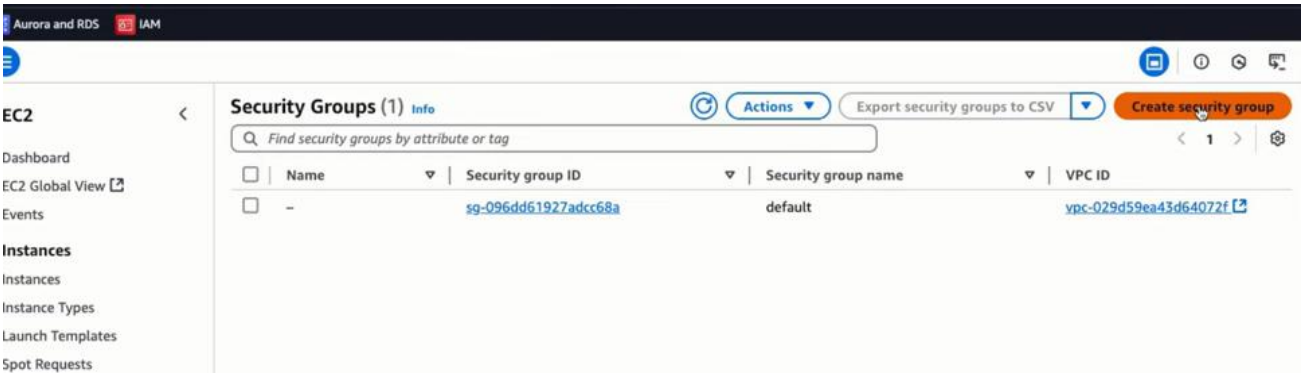
The problem here is any one can misuse as we have allowed the traffic , to make it secure we will create a security group for Quicksight to access the RDS instance.

Step 27: We will now create the new security group for quicksight and attach it with the new security group of quicksight.

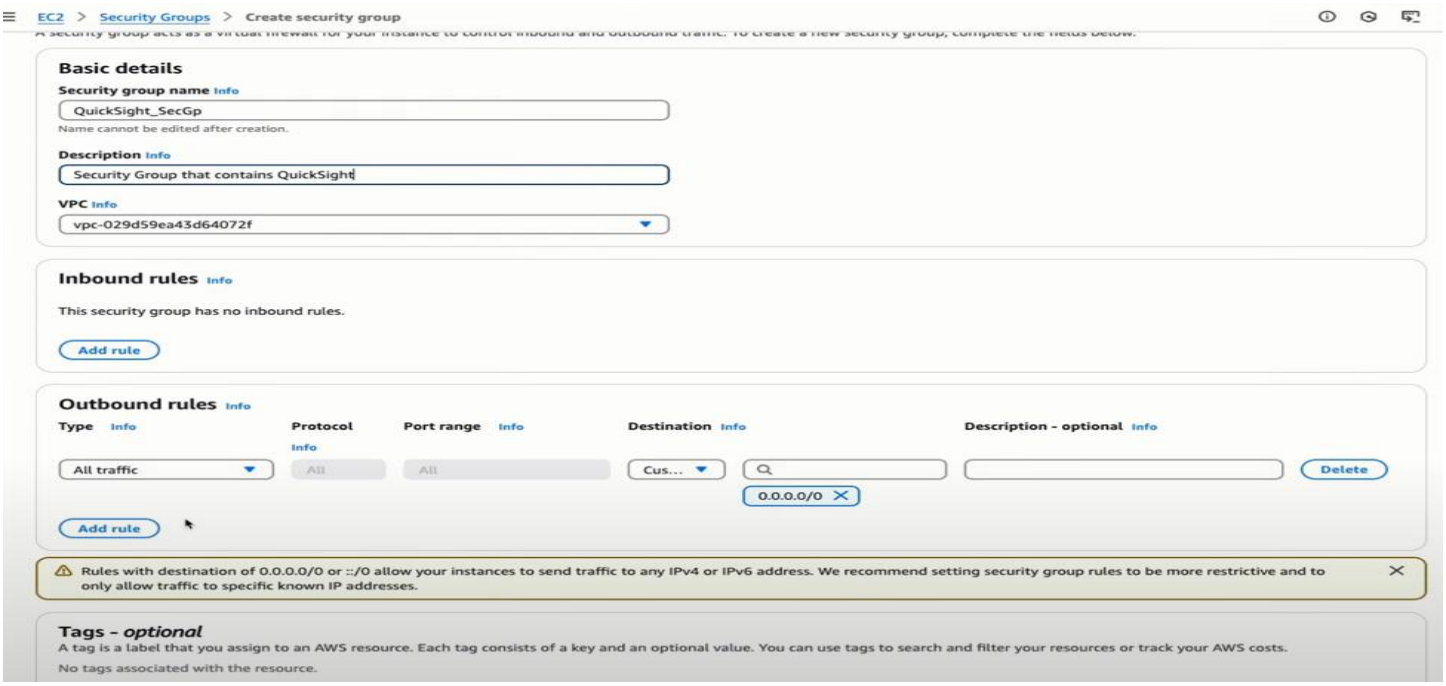
Step 28: Go to amazon console and search for security groups



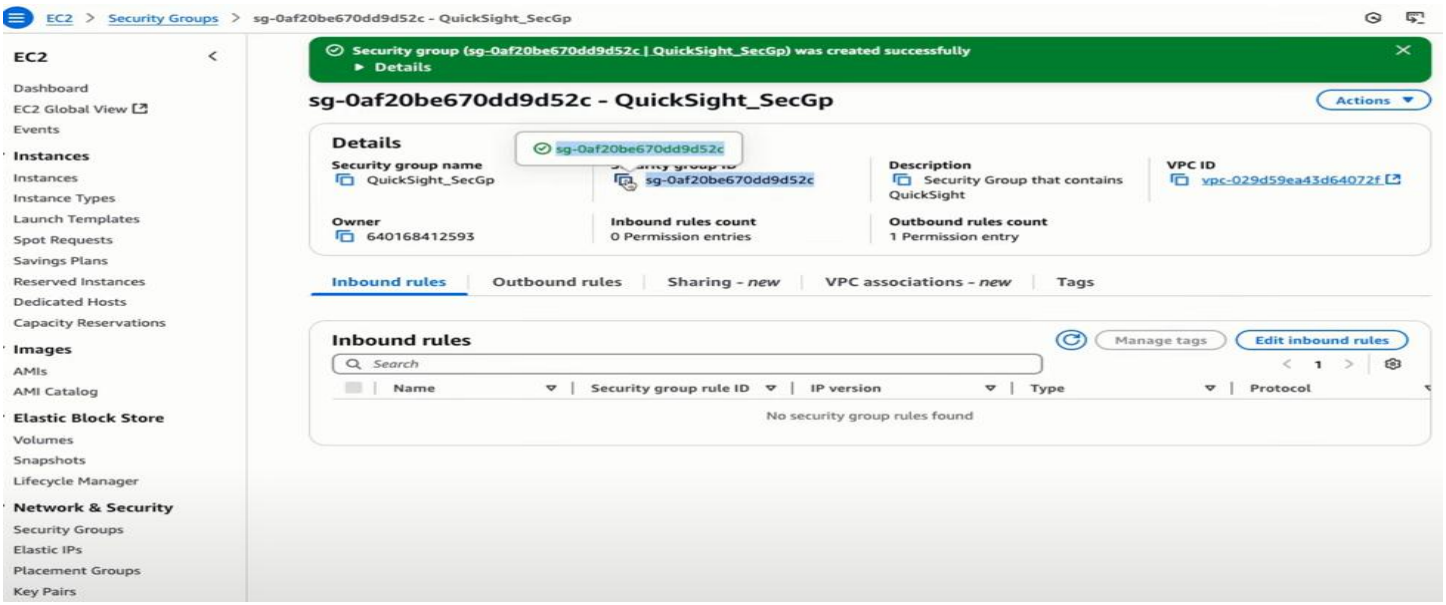

Step 29: Create a security group



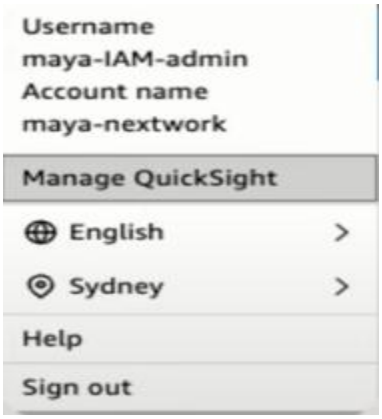

Step 30: Add group name description and keep same remaining and create a security group by hitting the buttom below



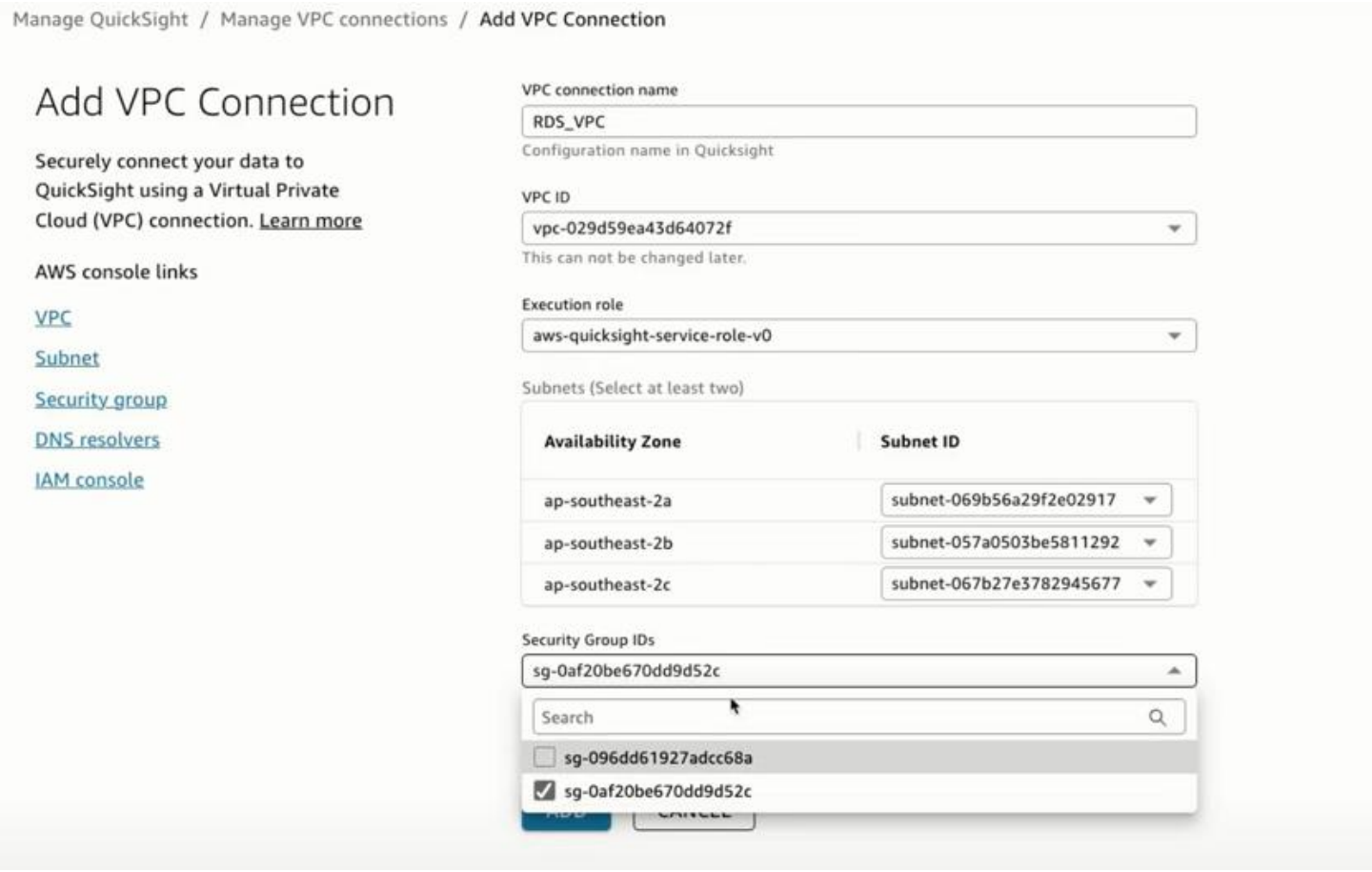

Step 31:Copy the security group ID




Step 32: Click on manage quicksight

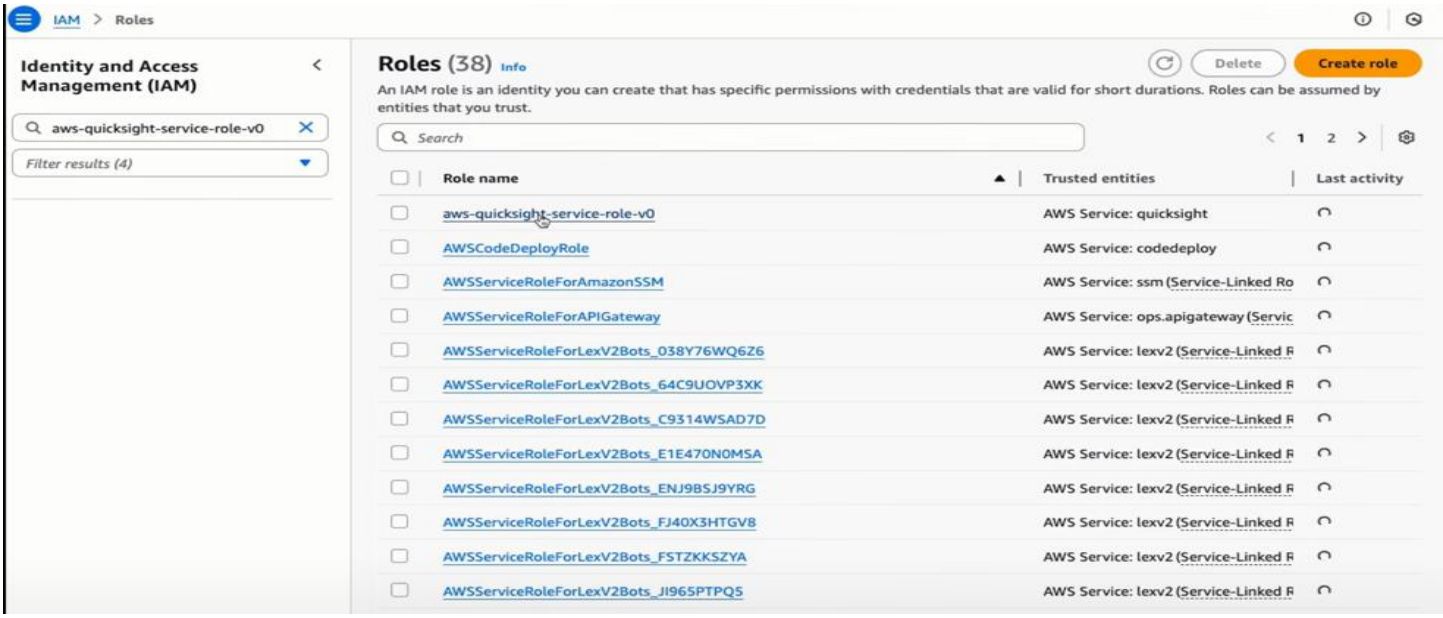


Step 33: paste the link happened from step 31,all these name id execution roles comes defaulty




It throws an error

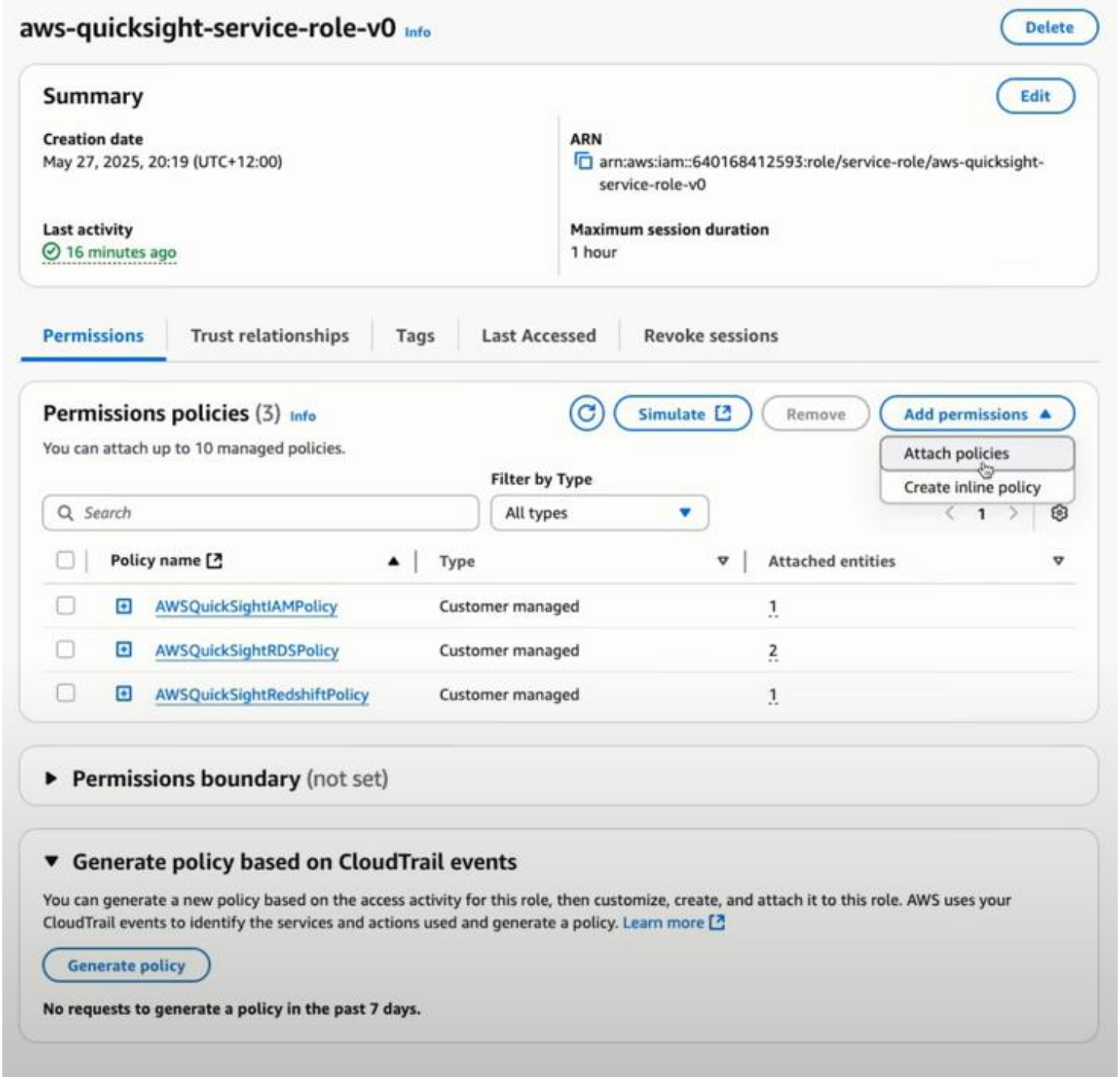
Step 34:



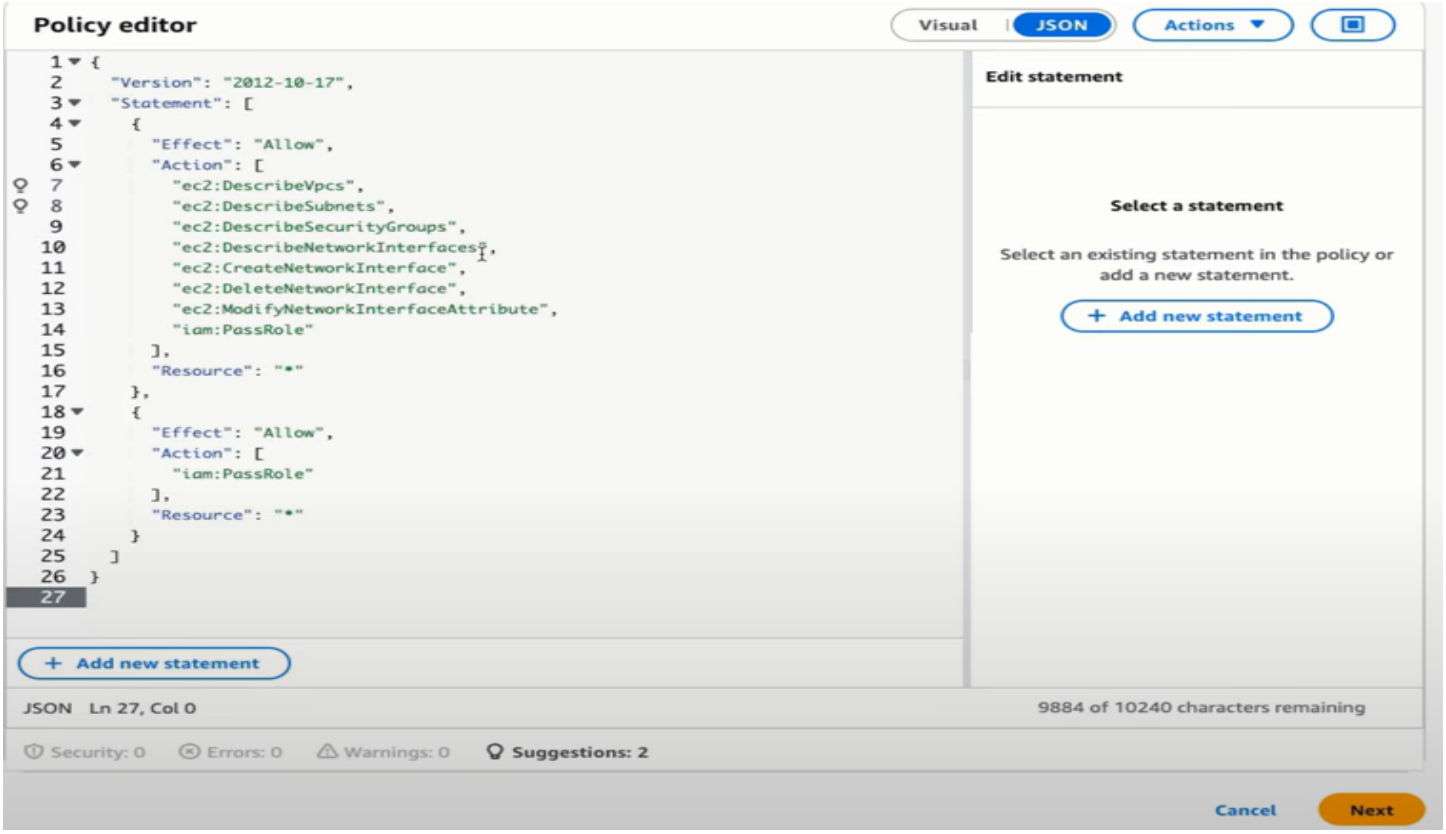
**Update role**

- Open a new tab to your AWS console and search for IAM
- In the left menu, select **Roles**
- In the Roles search bar, search for our role; aws-quicksight-service-role-v0

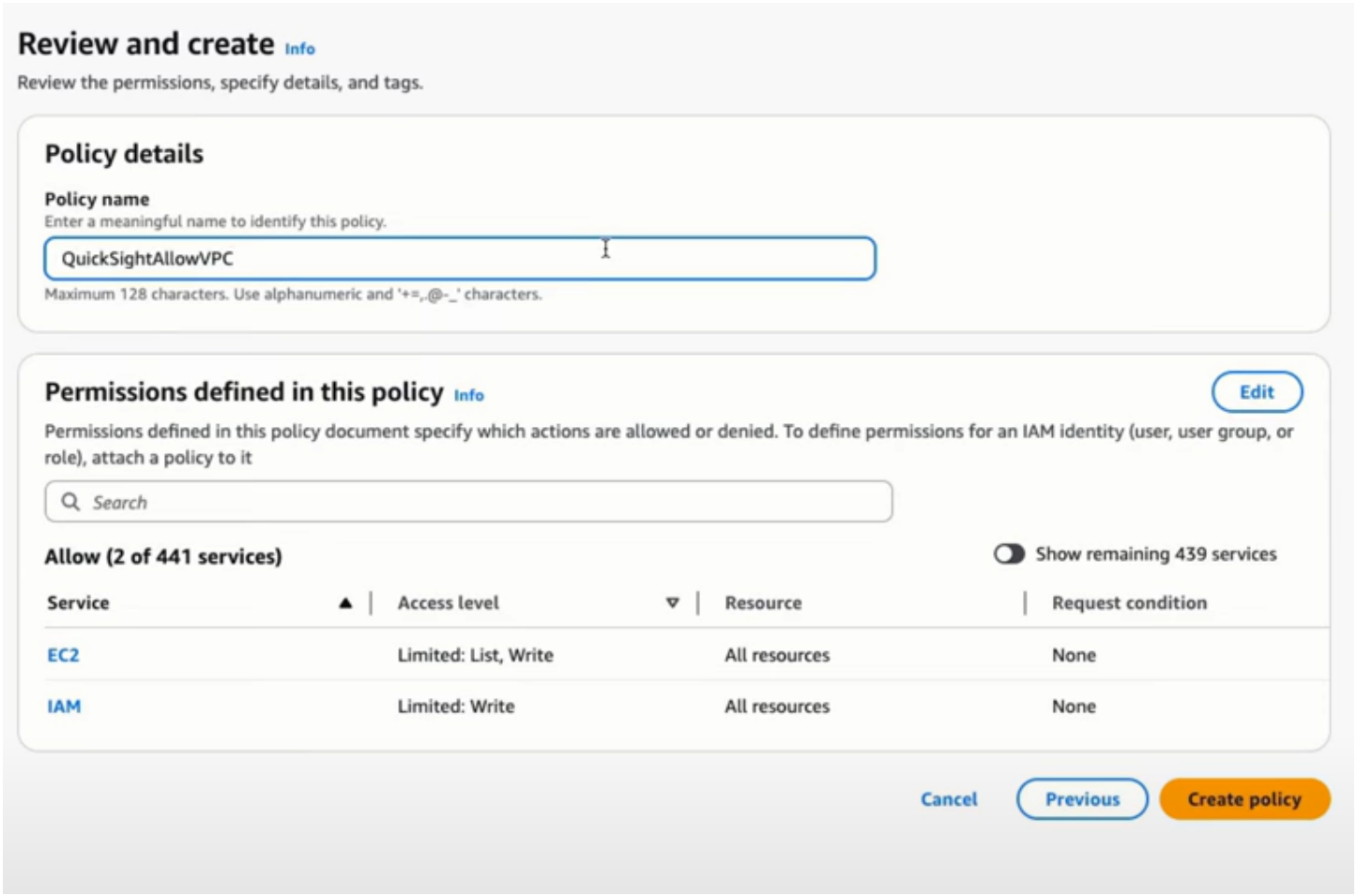
Step 35:click on inline policy



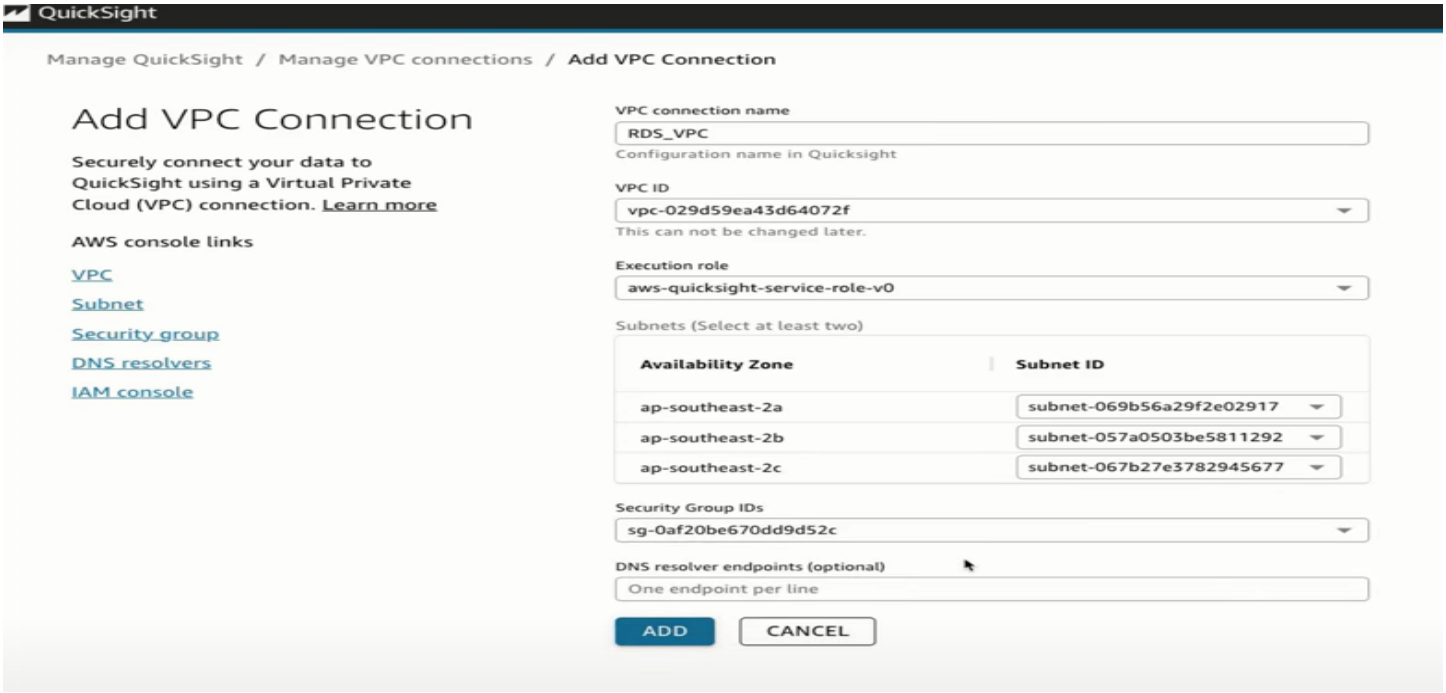
Step 36: change visual to json and add the code




Step 37:Add the policy name and create policy



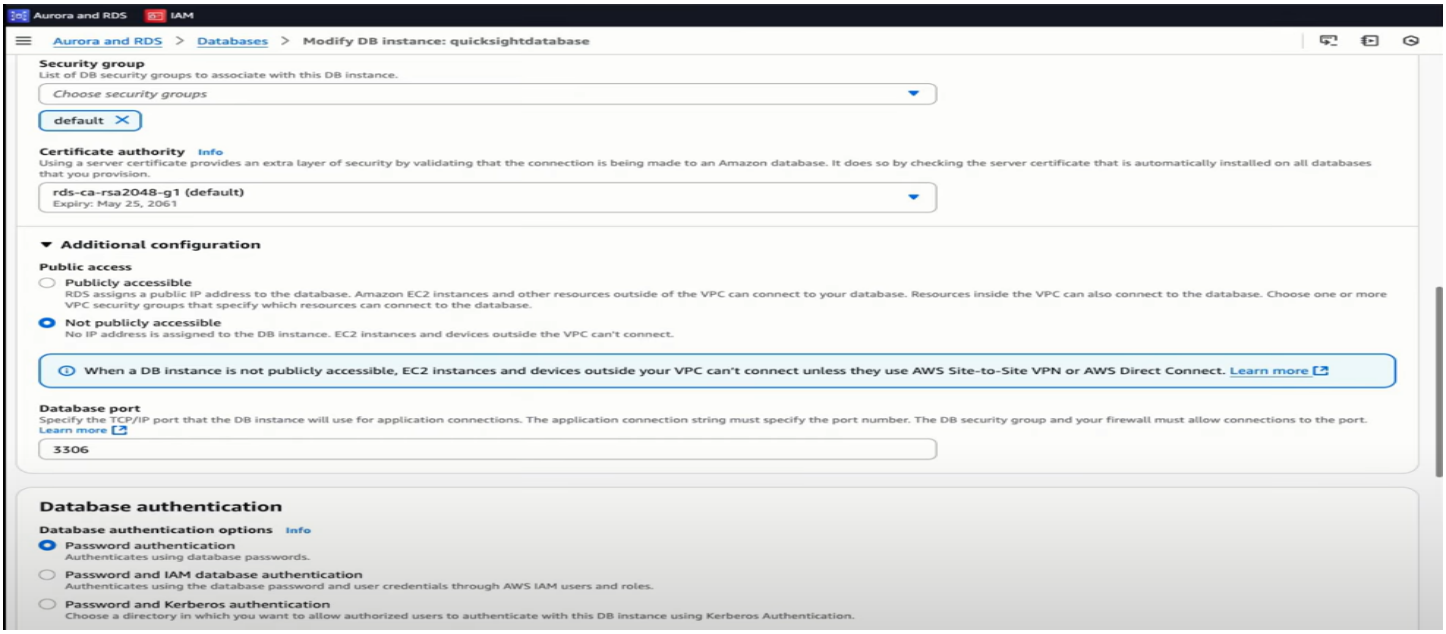
Step 38: We now have attached QuickSight to our new security group.



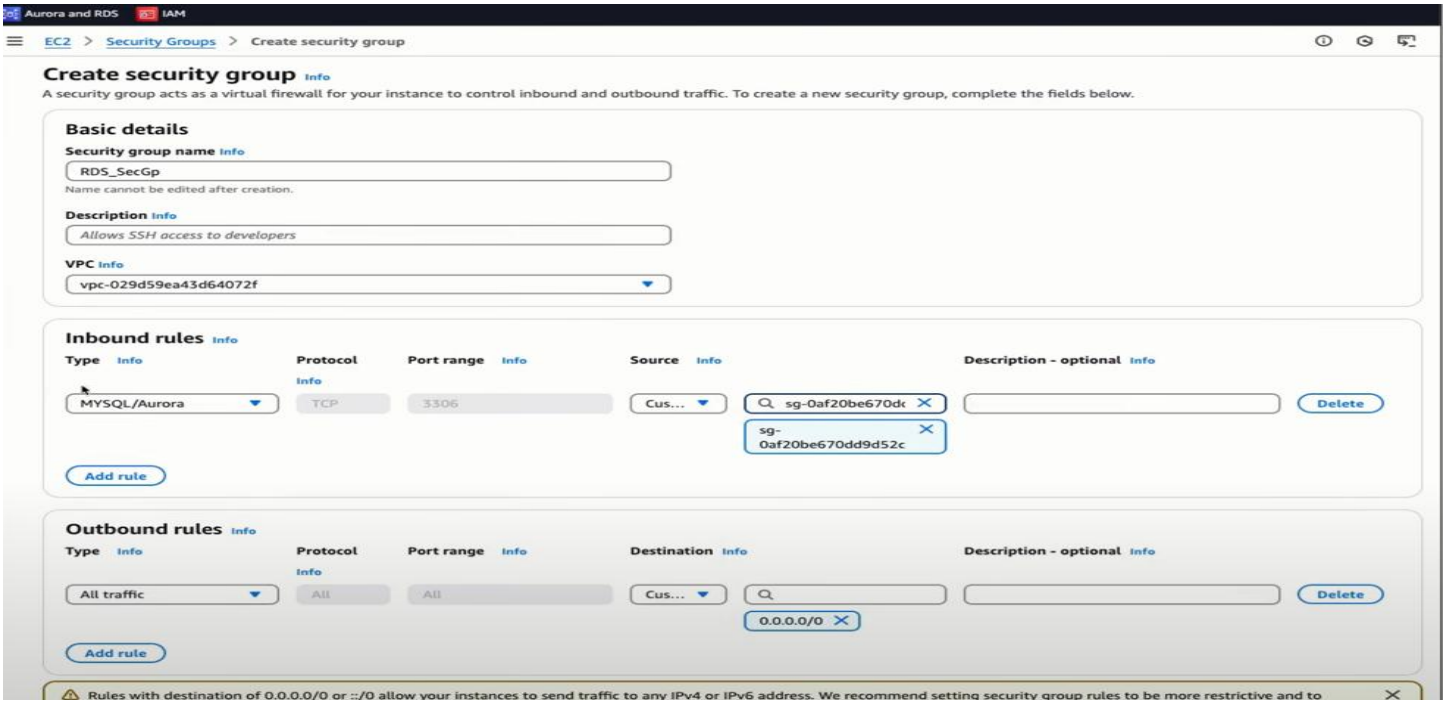

Step 39: Finally we added VPC Connection


Now let us make RDS Private

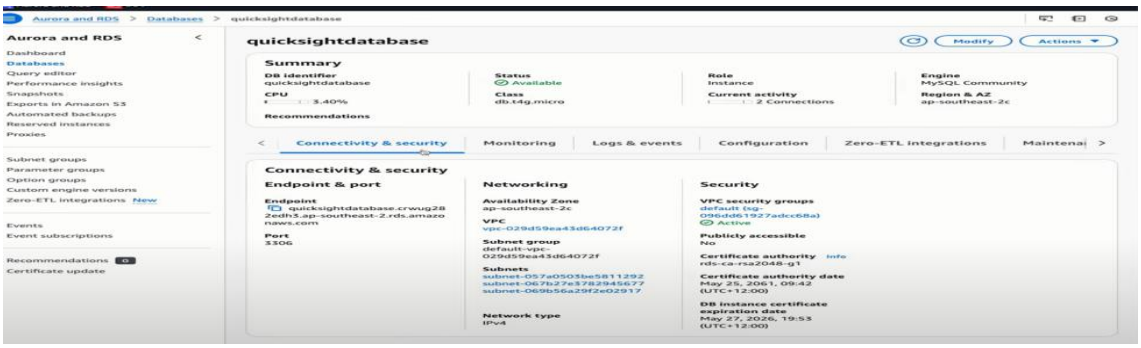
Step 40: Go to Amazon console->Databases->Modify->Additional configuration and make it Not publicly Assessible -> click continue -> Apply immediately ->modify DB instance



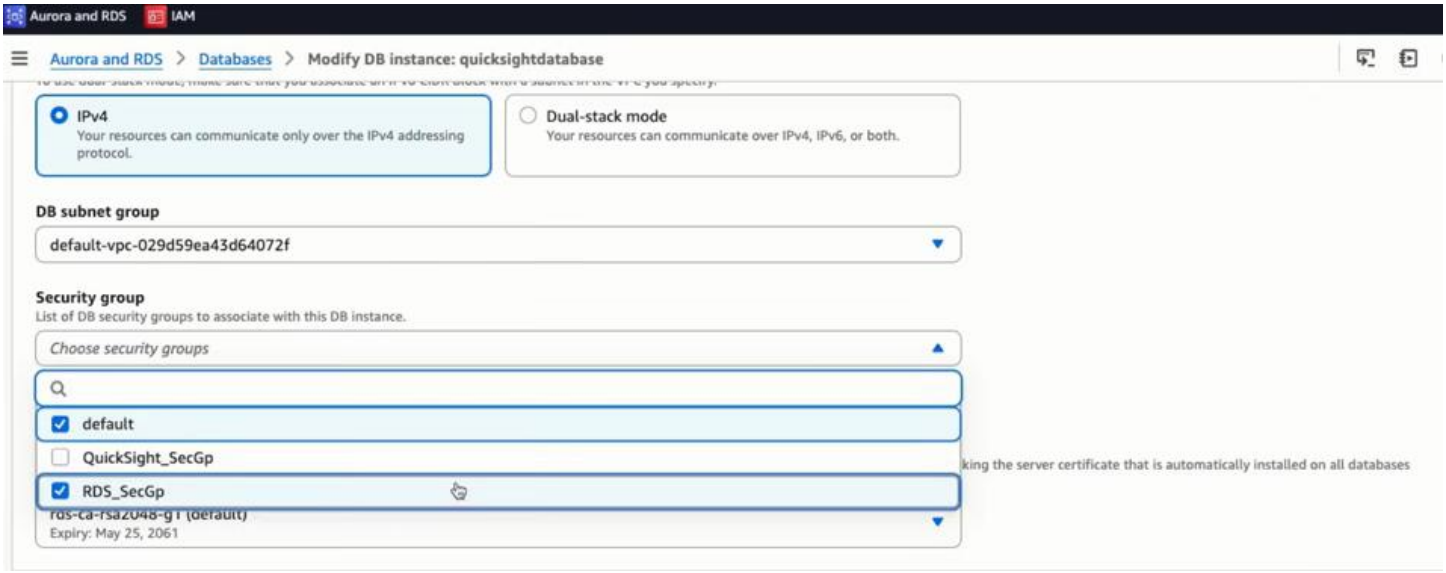

Step 41:Search for security groups and create one and description also




Step 42: Click on modify

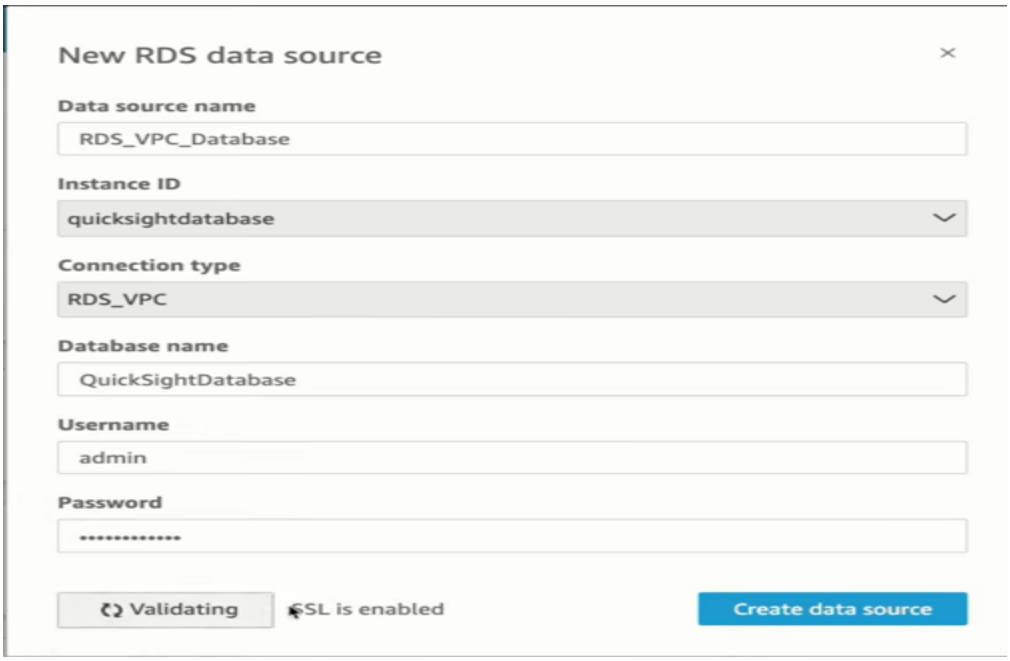



Step 43:

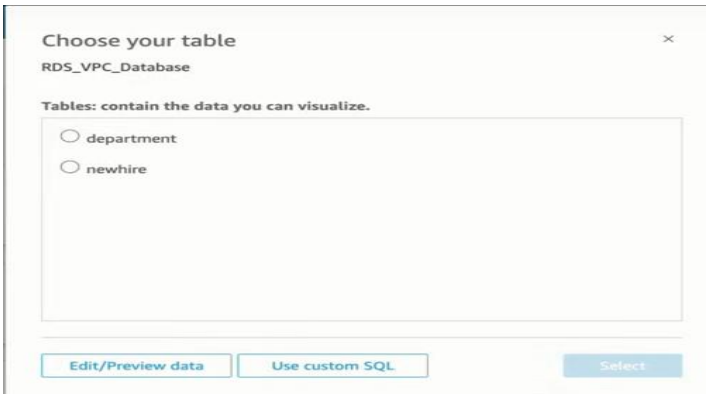



Click continue -> Apply immediately->Modify DB

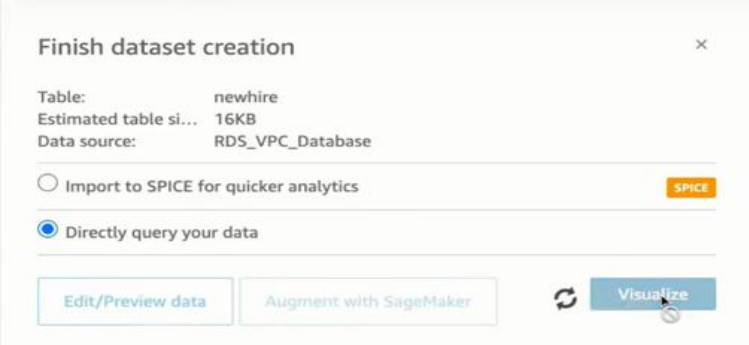
Step 44: Go to Quicksight and open databases and create a connection and click on RDS a dialogue box appears,we also need to validate and click on create the data source



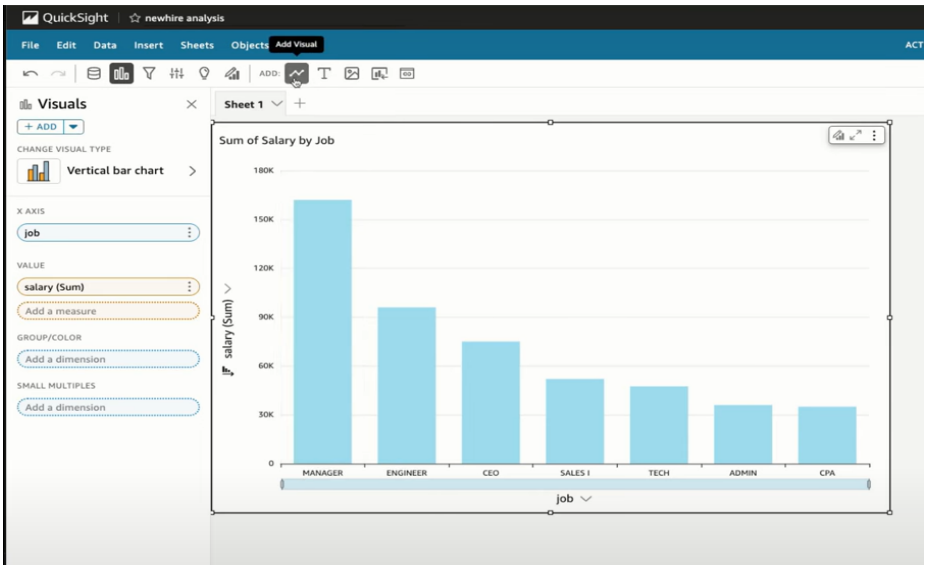

Step 45:



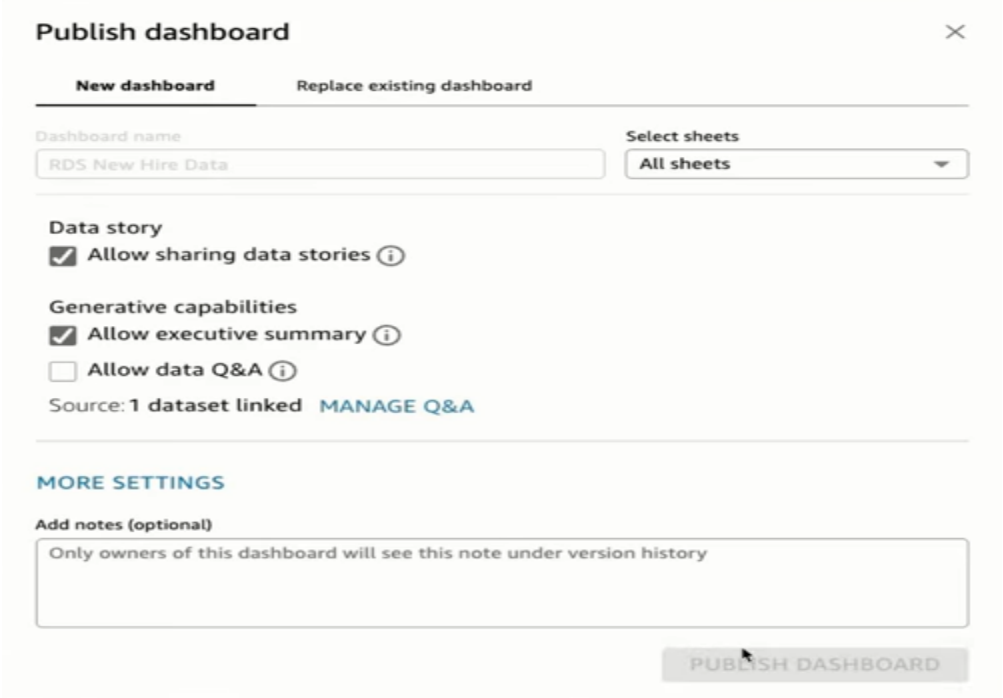
Step 46: Select the database as newhire and directly query your data and click on visualize




Step 47: The dashboard is ready

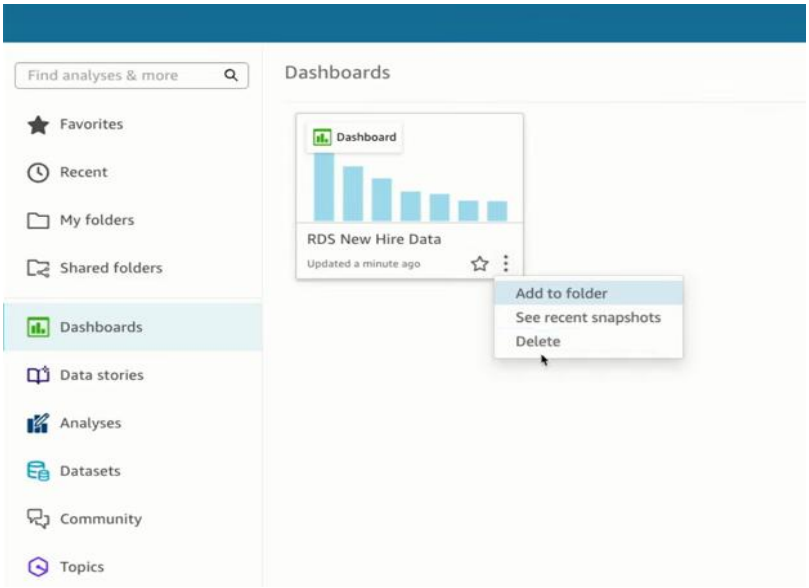



Step 48: Dashboard name as RDS New Hire Data and hit publish dashboard

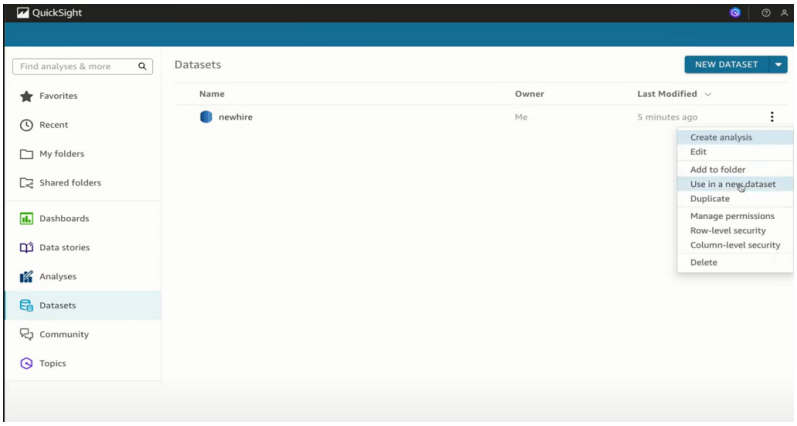


Delete All the items inorder to avoid extra charge.

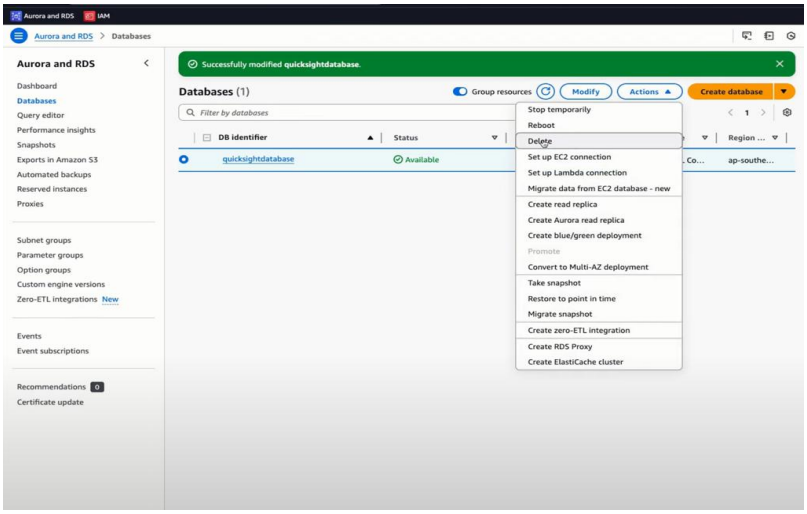
Step 1: Delete as shown in the figure



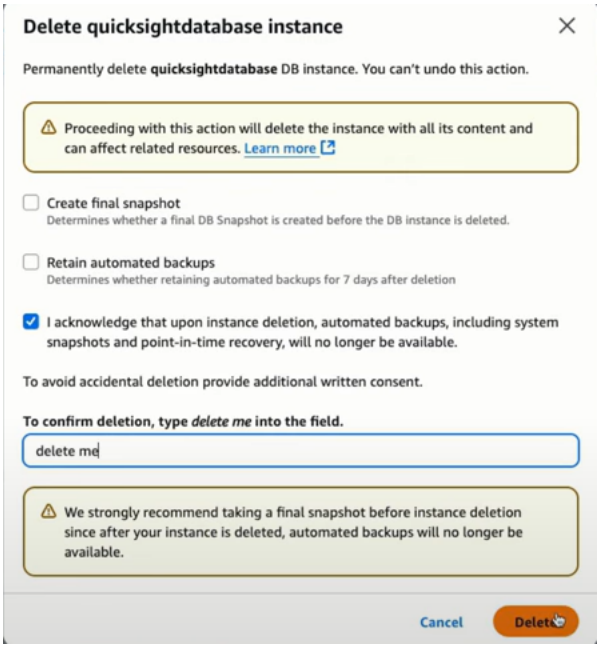

Step 2:Delete the dataset using delete option




Step 3: Go to RDS instance and delete

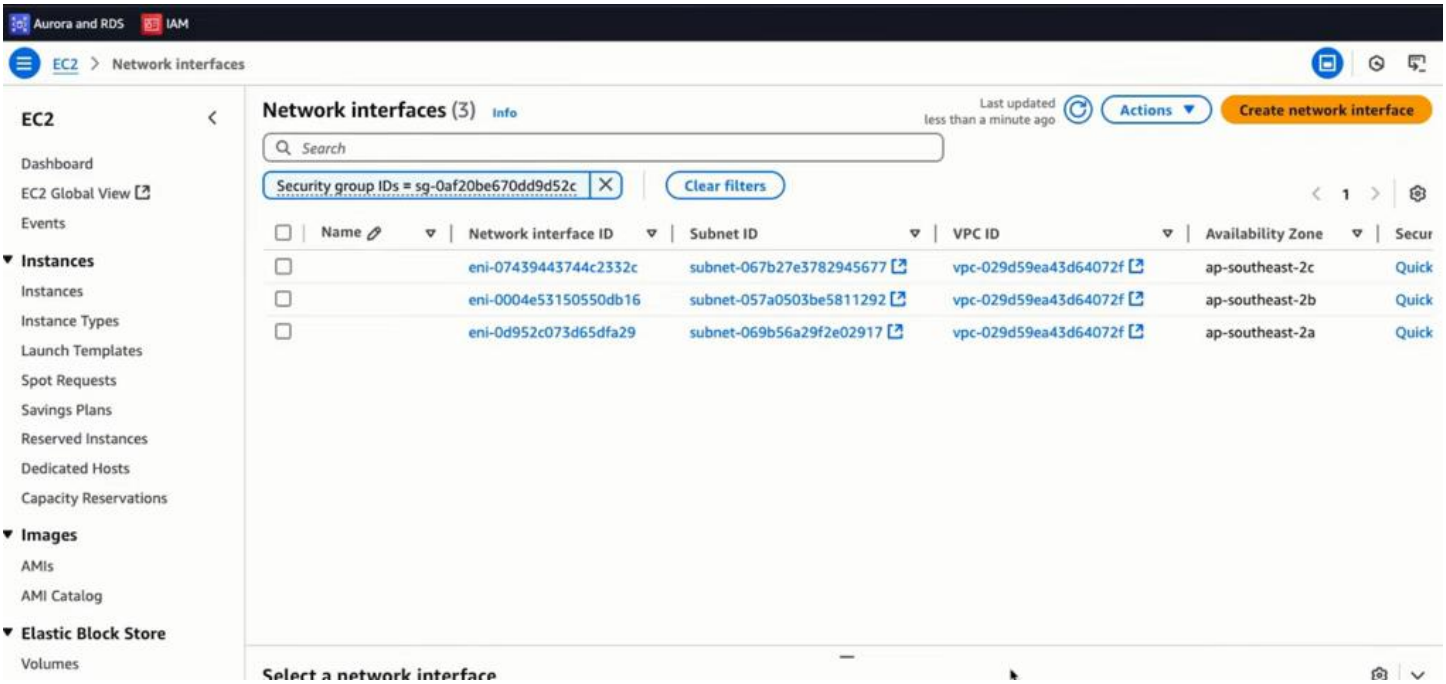



Step 4: follow all the steps

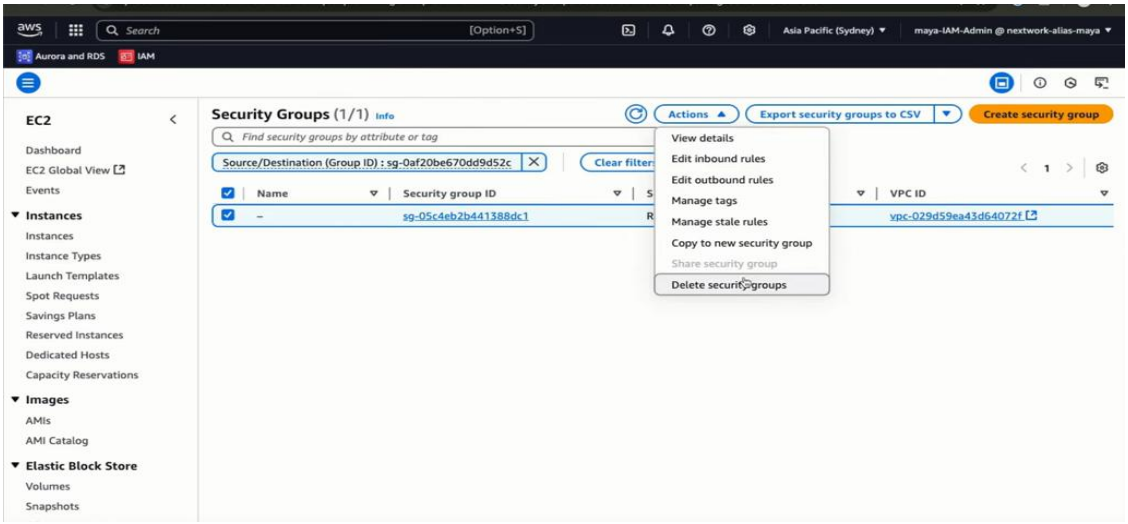



Step 5:Go to quicksight and manage quicksight on top right corner and delete it as shown in figure.

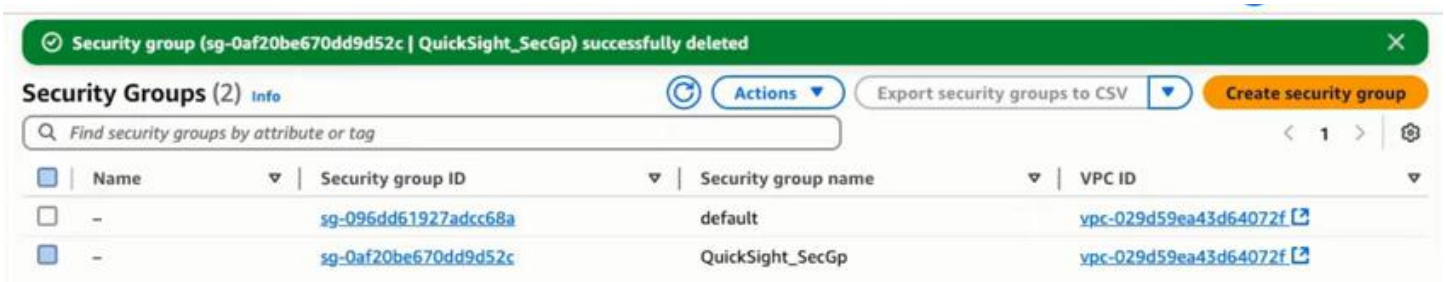

Step 6: Open Ec2 and delete all the 3 from clicking on actions and delete.



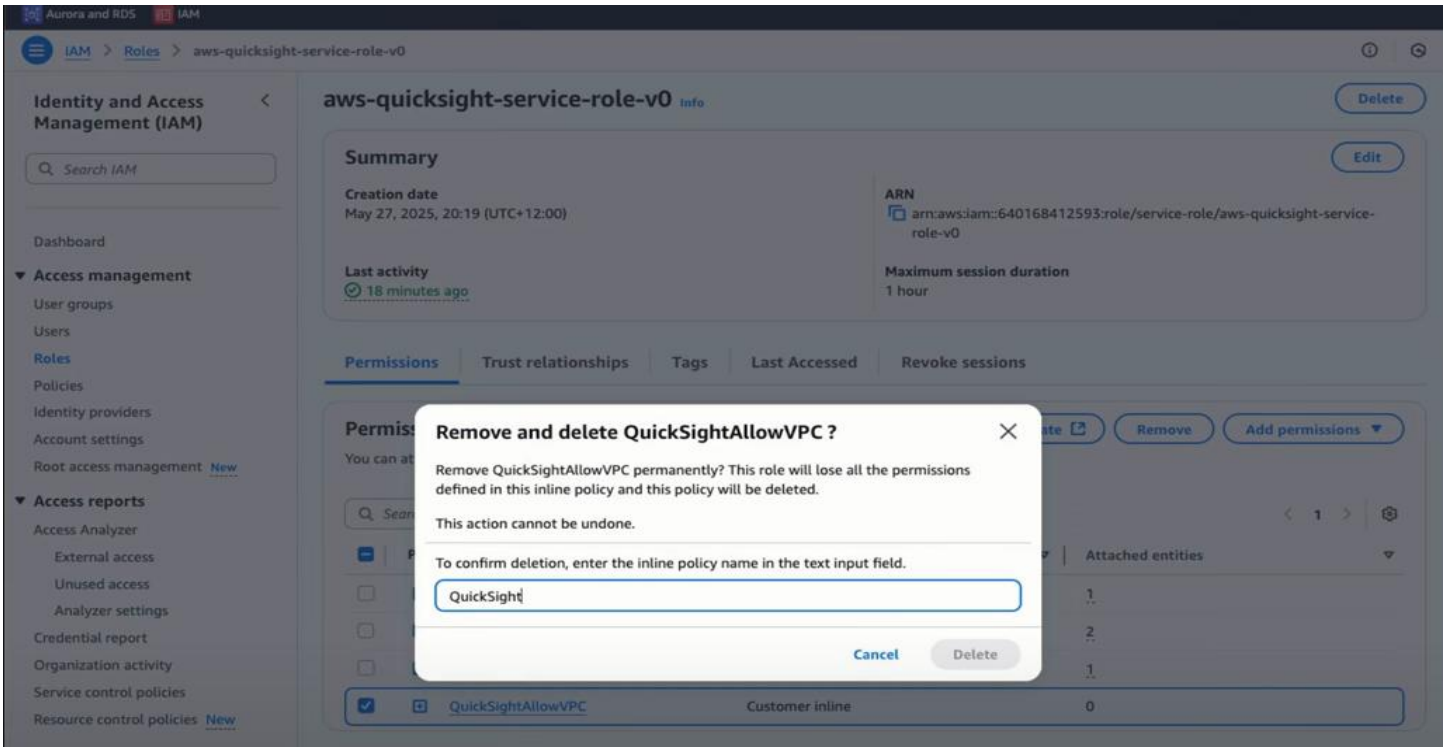
Step 7: Delete security groups



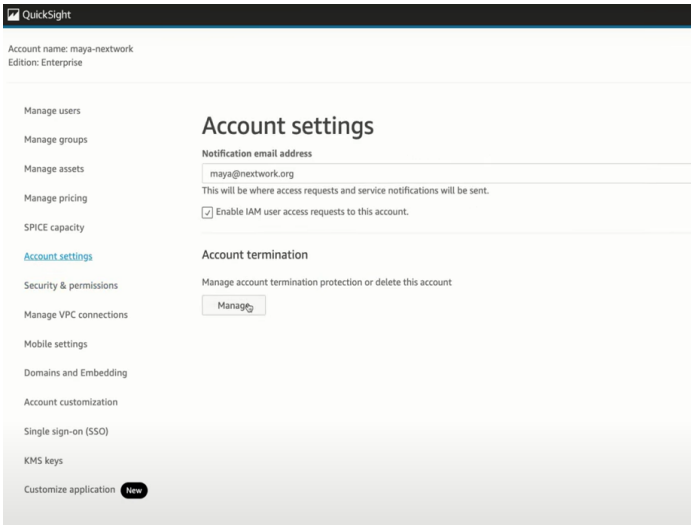

Step 8: delete the quicksight_secGp using actions



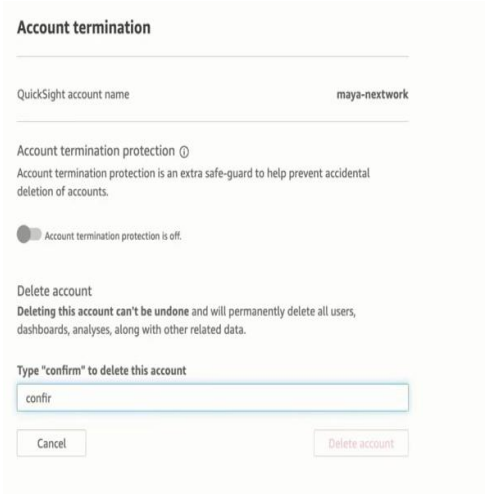

Step 9: Click on IAM Roles and in permission delete all after deleting this.



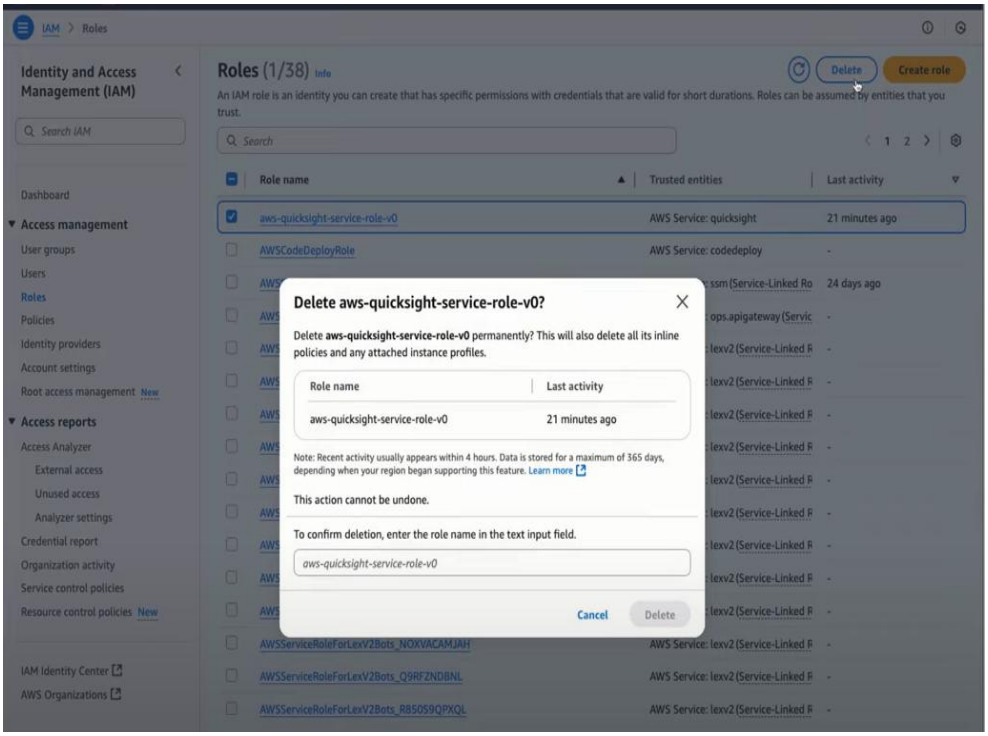
Step 10:Delete Quicksight account




Step 11: By confirming delete the account




Step 12:Go to IAM console and refresh if u still see it delete the account




Codes used:

SQL Data

CREATE TABLE newhire(

empno INT PRIMARY KEY,

ename VARCHAR(10),

job VARCHAR(9),

manager INT NULL,

hiredate DATETIME,

salary NUMERIC(7,2),

comm NUMERIC(7,2) NULL,

department INT)

SELECT * FROM newhire;

INSERT INTO newhire (empno, ename, job, manager, hiredate, salary, comm, department) VALUES

(1, 'JOHNSON', 'ADMIN', 6, '1990-12-17', 18000, NULL, 4),

```
(2, 'HARDING', 'MANAGER', 9, '1998-02-02', 52000, 300, 3),
(3, 'TAFT', 'SALES I', 2, '1996-01-02', 25000, 500, 3),
(4, 'HOOVER', 'SALES I', 2, '1990-04-02', 27000, NULL, 3),
(5, 'LINCOLN', 'TECH', 6, '1994-06-23', 22500, 1400, 4),
(6, 'GARFIELD', 'MANAGER', 9, '1993-05-01', 54000, NULL, 4),
(7, 'POLK', 'TECH', 6, '1997-09-22', 25000, NULL, 4),
(8, 'GRANT', 'ENGINEER', 10, '1997-03-30', 32000, NULL, 2),
(9, 'JACKSON', 'CEO', NULL, '1990-01-01', 75000, NULL, 4),
(10, 'FILLMORE', 'MANAGER', 9, '1994-08-09', 56000, NULL, 2),
(11, 'ADAMS', 'ENGINEER', 10, '1996-03-15', 34000, NULL, 2),
(12, 'WASHINGTON', 'ADMIN', 6, '1998-04-16', 18000, NULL, 4),
(13, 'MONROE', 'ENGINEER', 10, '2000-12-03', 30000, NULL, 2),
(14, 'ROOSEVELT', 'CPA', 9, '1995-10-12', 35000, NULL, 1);

SELECT * FROM newhire;

CREATE TABLE department(
deptno INT NOT NULL,
dname VARCHAR(14),
loc VARCHAR(13));

INSERT INTO department (deptno, dname, loc) VALUES
(1, 'ACCOUNTING', 'ST LOUIS'),
(2, 'RESEARCH', 'NEW YORK'),
(3, 'SALES', 'ATLANTA'),
(4, 'OPERATIONS', 'SEATTLE');

SELECT * FROM department;
```

To Create inline policy in JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeNetworkInterfaces",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "iam:PassRole"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:PassRole"
      ],
      "Resource": "*"
    }
  ]
}
```