

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

Screenshot of the AWS Aurora and RDS Dashboard showing the Resources section. It lists DB Instances (0/20), DB Clusters (0/40), and Snapshots (0). A sidebar on the left shows navigation links for Aurora and RDS, including Dashboard, Databases, Performance insights, Snapshots, Exports in Amazon S3, Automated backups, Reserved instances, Proxies, Subnet groups, Parameter groups, Option groups, Custom engine versions, Zero-ETL integrations, Events, and Event subscriptions.

Explore RDS - new

Complete the activity to earn AWS credits. In this activity, you will learn how to create a database quickly. To begin, choose [Start tutorial](#).

Status
Not started

Complete by
January 26, 2026

Reward value
USD 20.00

Estimated duration
2-5 minutes

[Start tutorial](#)

Create a database

Amazon Relational Database Service (RDS) makes it easy to set up, manage, and scale relational databases in the cloud. You can use a backup from Amazon S3 to restore and

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

Screenshot of the AWS Aurora and RDS Databases page. A modal window titled "Consider creating a blue/green deployment to minimize downtime during upgrades" provides information about RDS Blue/Green Deployments. Below the modal, the "Databases (0)" section is visible, featuring a search bar, a "Create database" button, and a table header with columns for DB identifier, Status, Role, Engine, Region ..., and Size. A cartoon robot icon is centered on the page.

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

Standard create
You set all of the configuration options, including ones for availability, security, backups, and maintenance.

Easy create
Use recommended best-practice configurations. Some configuration options can be changed after the database is created.

Configuration

Engine type [Info](#)

<input type="radio"/> Aurora (MySQL Compatible)	<input type="radio"/> Aurora (PostgreSQL Compatible)	<input checked="" type="radio"/> MySQL
<input type="radio"/> PostgreSQL	<input type="radio"/> MariaDB	<input type="radio"/> Oracle
<input type="radio"/> Microsoft SQL Server		

Edition
 MySQL Community

DB instance size

<input type="radio"/> Production db.r7g.xlarge 4 vCPUs 32 GiB RAM 400 GiB 2.090 USD/hour	<input type="radio"/> Dev/Test db.r7g.large 2 vCPUs 16 GiB RAM 200 GiB 0.308 USD/hour	<input checked="" type="radio"/> Free tier db.t4g.micro 2 vCPUs 1 GiB RAM 20 GiB 0.025 USD/hour
---	--	--

DB instance identifier
Type a name for your DB instance. The name must be unique across all DB instances owned by your AWS account in the current AWS Region.

The DB instance identifier is case-insensitive, but is stored as all lowercase (as in "mydbinstance"). Constraints: 1 to 63 alphanumeric characters or hyphens. First character must be a letter. Can't contain two consecutive hyphens. Can't end with a hyphen.

Master username [Info](#)
Type a login ID for the master user of your DB instance.

1 to 16 alphanumeric characters. The first character must be a letter.

Credentials management
You can use AWS Secrets Manager or manage your master user credentials.

<input type="radio"/> Managed in AWS Secrets Manager - most secure RDS generates a password for you and manages it throughout its lifecycle using AWS Secrets Manager.	<input checked="" type="radio"/> Self managed Create your own password or have RDS create a password that you manage.
--	--

Auto generate password
Amazon RDS can generate a password for you, or you can specify your own password.

Master password [Info](#)

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

DB instance size

Production db.r7g.xlarge 4 vCPUs 32 GiB RAM 400 GiB 2.090 USD/hour	Dev/Test db.r7g.large 2 vCPUs 16 GiB RAM 200 GiB 0.508 USD/hour	Free tier db.t4g.micro 2 vCPUs 1 GiB RAM 20 GiB 0.025 USD/hour
---	--	---

DB instance identifier
Type a name for your DB instance. The name must be unique across all DB instances owned by your AWS account in the current AWS Region.

Master username [Info](#)
Type a login ID for the master user of your DB instance.

Credentials management
You can use AWS Secrets Manager or manage your master user credentials.

Managed in AWS Secrets Manager - most secure
RDS generates a password for you and manages it throughout its lifecycle using AWS Secrets Manager.

Self managed
Create your own password or have RDS create a password that you manage.

Auto generate password
Amazon RDS can generate a password for you, or you can specify your own password.

Master password [Info](#)

Password strength Strong
Minimum constraints: At least 8 printable ASCII characters. Can't contain any of the following symbols: / " @

Confirm master password [Info](#)

► Set up EC2 connection - **optional**
You can also set up a connection to an EC2 instance after creating the database. Go to the database list page or the database details page, choose **Actions**, and then choose **Set up to EC2 connection**.

► View default settings for Easy create
Easy create sets the following configurations to their default values, some of which can be changed later. If you want to change any of these settings now, use Standard create.

You are responsible for ensuring that you have all of the necessary rights for any third-party products or services that you use with AWS services.

[Cancel](#) [Create database](#)

Step 4: Click on create database

Now the database is created

Creating database database-1
Your database might take a few minutes to launch. You can use settings from database-1 to simplify configuration of suggested database add-ons while we finish creating your DB for you.

View connection details [X](#)

Notifications 0 0 0 0 1 1 [▼](#)

Databases (1)

Group resources [C](#) [Modify](#) [Actions ▾](#) [Create database](#) [▼](#)

Filter by databases

DB identifier	Status	Role	Engine	Region ...	Size
database-1	Creating	Instance	MySQL Co...	ap-south-1b	db.t4g.micro

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

The screenshot shows the 'Connectivity & security' tab of the AWS RDS console. It displays the following information:

Endpoint & port	Networking	Security
Endpoint database-1.cfg80y2e6l3a.ap-south-1.rds.amazonaws.com	Availability Zone ap-south-1b	VPC security groups default (sg-02703b0405247d441) Active
Port 3306	VPC vpc-0cda25d5883eb3464	Publicly accessible Yes
	Subnet group default-vpc-0cda25d5883eb3464	Certificate authority Info rds-ca-rsa2048-g1
	Subnets subnet-0b2b8e511d5de6d7c subnet-0d1cf8b469b1af47d subnet-015d5e7cfbd6e9046	Certificate authority date May 20, 2061, 00:10 (UTC+05:30)
	Network type IPv4	DB instance certificate expiration date August 20, 2026, 21:04 (UTC+05:30)

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

The screenshot shows the 'Security Groups' section of the AWS EC2 console. A specific security group, 'sg-02703b0405247d441 - default', is selected and highlighted with a large oval.

Security Groups (1) Info

Name	Security group ID	Security group name	VPC ID	Description
-	sg-02703b0405247d441	default	vpc-0cda25d5883eb3464	default VPC secur

sg-02703b0405247d441 - default

Details

Security group name	Security group ID	Description	VPC ID
checkbox default	checkbox sg-02703b0405247d441	checkbox default VPC security group	checkbox vpc-0cda25d5883eb3464
Owner	Inbound rules count	Outbound rules count	
checkbox 340485103945	1 Permission entry	1 Permission entry	

Inbound rules

Name	Security group rule ID	IP version	Type	Protocol	Port range
-	sgr-048cc339df4ba650e	-	All traffic	All	All

Why 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

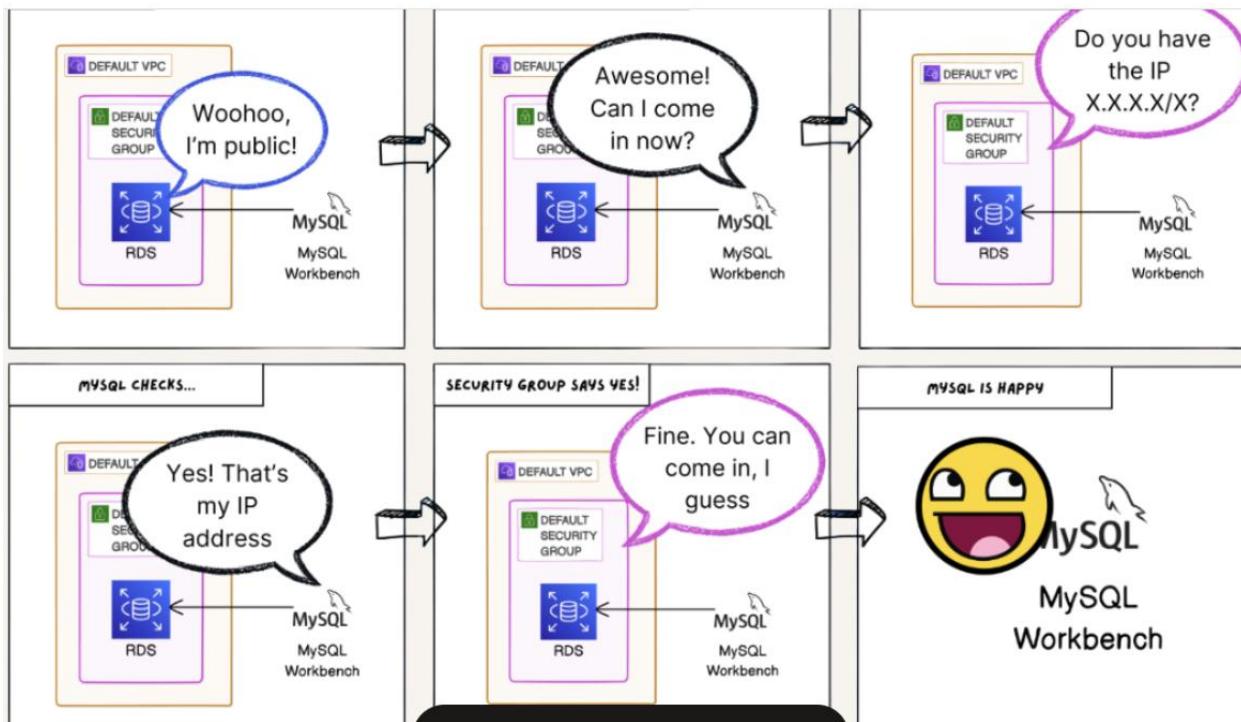
I want sql workbench to have access to RDS instance when it is on my local machine

Edit inbound rules Info

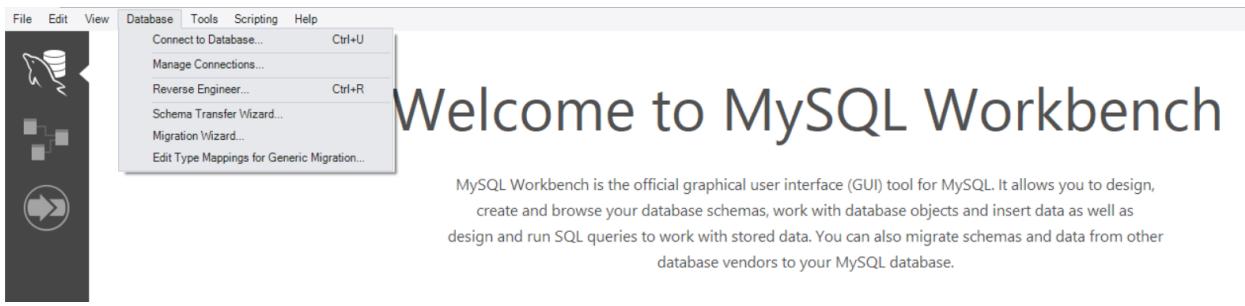
Inbound rules control the incoming traffic that's allowed to reach the instance.

Security group rule ID	Type	Protocol	Port range	Source	Description - optional
-	All TCP	TCP	0 - 65535	My IP	110.173.160.6/32

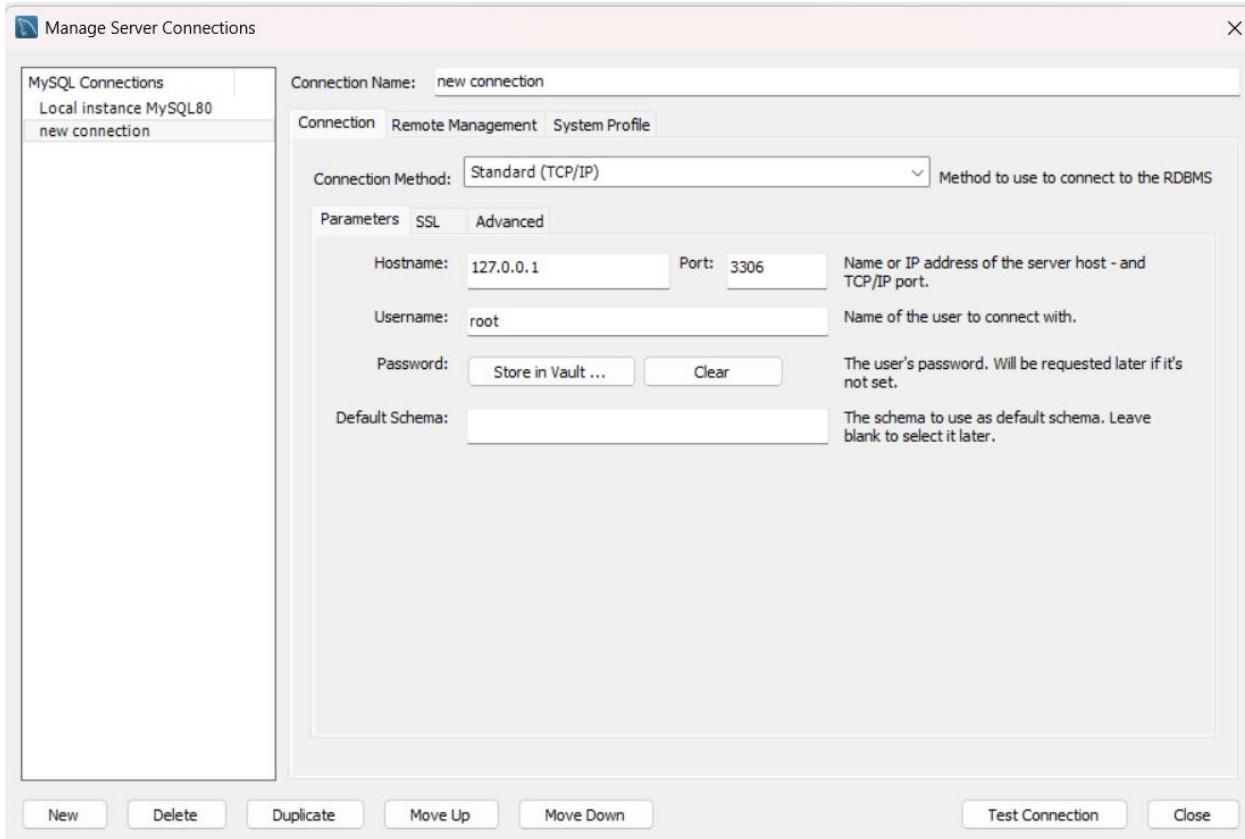
Add rule Cancel Preview changes **Save** Changes



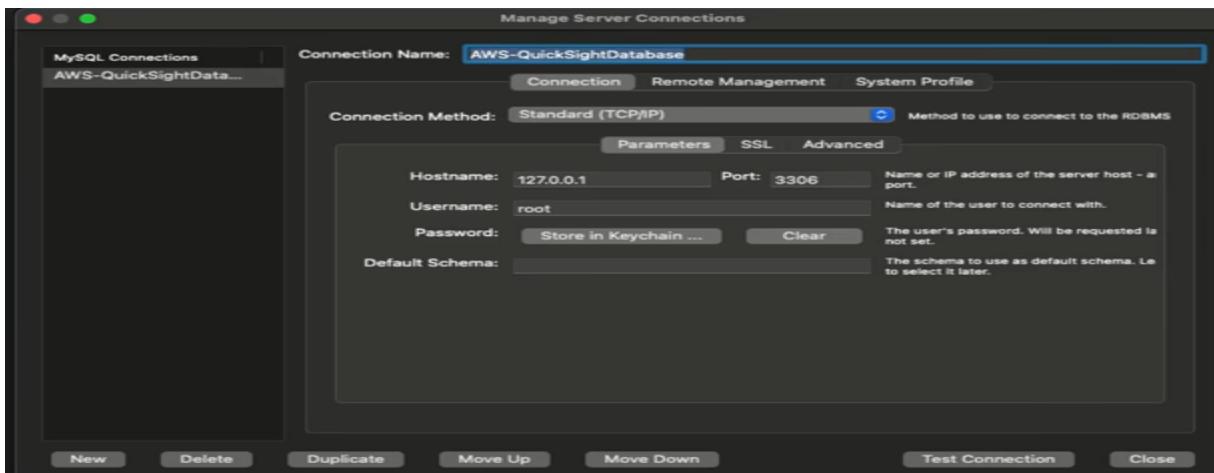
Step 12: Now go to Manage connections in MySQL Workbench



Step 13 :Select new and the below tab gets opened



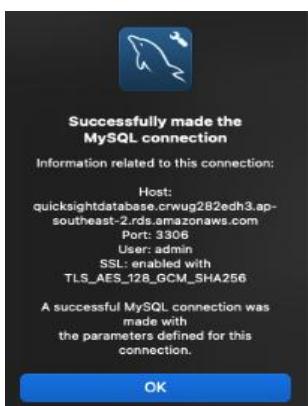
So the connection name is AWS-QuickSightDatabase



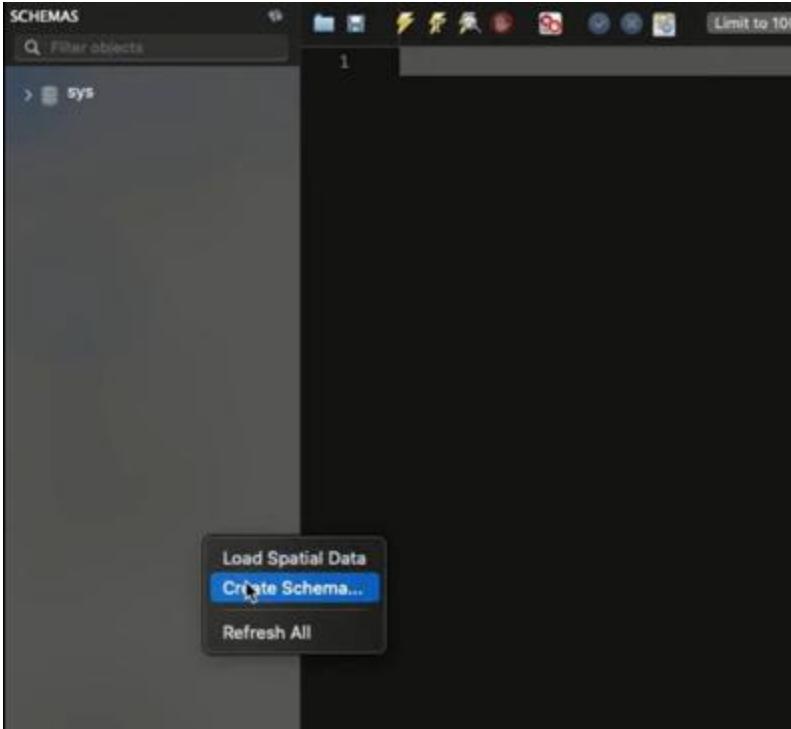
Step 14: And to get the connectivity, go to aurora and RDS and copy the link

Step 15: Copy the link and paste under the Hostname

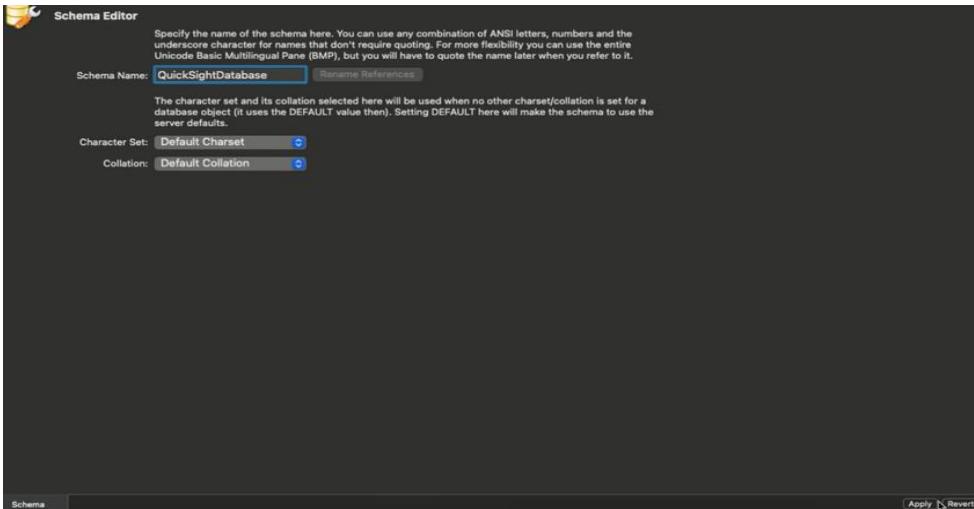
And the username and password will be the one we created in the step 3 remove root and add the username and click on store in keychain and write the password. Make sure the port is correct and then click on test connection.



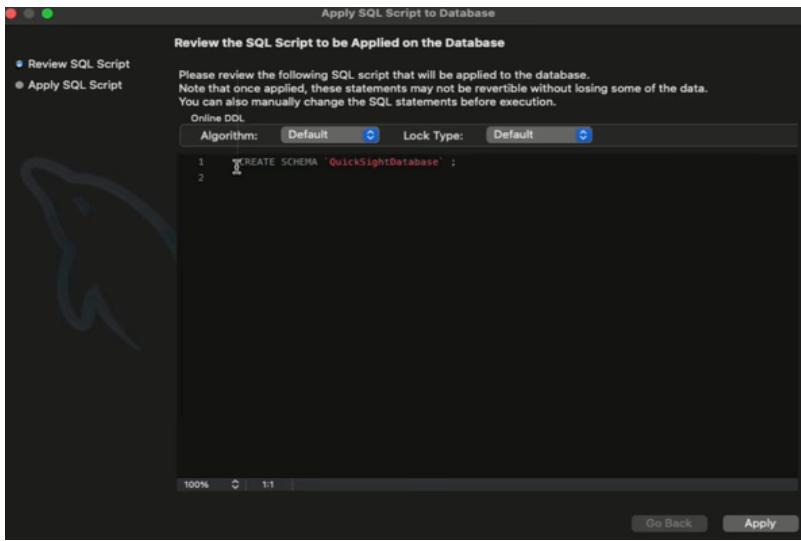
Step 16: Go to MySQL Connections and open under sys create new schema



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

Action	Time	Response	Duration / Fetch Time
1. Apply changes to QuickSightDatabase	20:09:11	Changes applied	0.050 sec
2. CREATE TABLE newhire	20:10:23	Error Code: 1046. No database selected Select the de...	0.044 sec
3. CREATE TABLE newhire	20:10:47	Error Code: 1046. No database selected Select the de...	0.044 sec
4. CREATE TABLE newhire	20:11:05	0 row(s) affected	0.116 sec

Step 20: Add the data into the table

QuickSightDatabase

- Tables
- Views
- Stored Procedures
- Functions
- sys

```

2   (1, 'JOHNSON', 'ADMIN', 6, '1990-12-17', 18000, NULL, 4),
3   (2, 'HARDING', 'MANAGER', 9, '1998-02-02', 52000, 300, 3),
4   (3, 'TAFT', 'SALES I', 2, '1996-01-02', 25000, 500, 3),
5   (4, 'HOOVER', 'SALES I', 2, '1990-04-02', 27000, NULL, 3),
6   (5, 'LINCOLN', 'TECH', 6, '1994-06-23', 22500, 1400, 4),
7   (6, 'GARFIELD', 'MANAGER', 9, '1993-05-01', 54000, NULL, 4),
8   (7, 'POLK', 'TECH', 6, '1997-09-22', 25000, NULL, 4),
9   (8, 'GRANT', 'ENGINEER', 10, '1997-03-30', 32000, NULL, 2),
10  (9, 'JACKSON', 'CEO', NULL, '1990-01-01', 75000, NULL, 4),
11  (10, 'FILLMORE', 'MANAGER', 9, '1994-08-09', 56000, NULL, 2),
12  (11, 'ADAMS', 'ENGINEER', 10, '1996-03-15', 34000, NULL, 2),
13  (12, 'WASHINGTON', 'ADMIN', 6, '1998-04-16', 18000, NULL, 4),
14  (13, 'MONROE', 'ENGINEER', 10, '2000-12-03', 30000, NULL, 2),
15  (14, 'ROOSEVELT', 'CPA', 9, '1995-10-12', 35000, NULL, 1);
16

```

Action Output 0

	Time	Action	Response	Duration / Fetch Time
1	20:09:11	Apply changes to QuickSightDatabase	Changes applied	
2	20:10:23	CREATE TABLE newhire(empno INT PRIMARY KEY, ename VARCHAR(10), job VARCHAR(9), manager INT NULL, hiredate DATETIME, salary DECIMAL(7,2), comm DECIMAL(5,2), department INT NULL)	Error Code: 1046. No database selected Select the de... 0.050 sec	
3	20:10:47	CREATE TABLE newhire(empno INT PRIMARY KEY, ename VARCHAR(10), job VARCHAR(9), manager INT NULL, hiredate DATETIME, salary DECIMAL(7,2), comm DECIMAL(5,2), department INT NULL)	Error Code: 1046. No database selected Select the de... 0.044 sec	
4	20:11:05	CREATE TABLE newhire(empno INT PRIMARY KEY, ename VARCHAR(10), job VARCHAR(9), manager INT NULL, hiredate DATETIME, salary DECIMAL(7,2), comm DECIMAL(5,2), department INT NULL)	0 row(s) affected 0.116 sec	
5	20:11:46	SELECT * FROM newhire LIMIT 0, 1000	0 row(s) returned 0.045 sec / 0.00005...	
6	20:12:41	INSERT INTO newhire (empno, ename, job, manager, hiredate, salary, comm, department) VALUES (1, 'JOHNSON', 'ADMIN', 6, '1990-12-17', 18000, NULL, 4)	14 row(s) affected Records: 14 Duplicates: 0 Warnings: 0 0.048 sec	

Object Info Session Schema: QuickSightDatabase

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

QuickSightDatabase

- Tables
- Views
- Stored Procedures
- Functions
- sys

```

1  SELECT * FROM newhire;
2

```

Result Grid

empno	ename	job	manager	hiredate	salary	comm	department
1	JOHNSON	ADMIN	6	1990-12-17 00:00:00	18000.00	NULL	4
2	HARDING	MANAGER	9	1998-02-02 00:00:00	52000.00	300.00	3
3	TAFT	SALES I	2	1996-01-02 00:00:00	25000.00	500.00	3
4	HOOVER	SALES I	2	1990-04-02 00:00:00	27000.00	NULL	5
5	LINCOLN	TECH	6	1994-08-09 00:00:00	22500.00	1400.00	4
6	GARFIELD	MANAGER	9	1993-03-30 00:00:00	56000.00	NULL	4
7	POLK	TECH	6	1997-09-22 00:00:00	25000.00	NULL	4
8	GRANT	ENGINEER	10	1997-03-30 00:00:00	32000.00	NULL	2
9	JACKSON	CEO	NULL	1990-01-01 00:00:00	75000.00	NULL	4
10	FILLMORE	MANAGER	9	1994-08-09 00:00:00	56000.00	NULL	2
11	ADAMS	ENGINEER	10	1996-03-15 00:00:00	34000.00	NULL	2
12	WASHINGTON	ADMIN	6	1998-04-16 00:00:00	18000.00	NULL	4
13	MONROE	ENGINEER	10	2000-12-03 00:00:00	30000.00	NULL	2
14	ROOSEVELT	CPA	9	1995-10-12 00:00:00	35000.00	NULL	1
NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL

newhire 2

Action Output 0

	Time	Action	Response	Duration / Fetch Time
1	20:09:11	Apply changes to QuickSightDatabase	Changes applied	
2	20:10:23	CREATE TABLE newhire(empno INT PRIMARY KEY, ename VARCHAR(10), job VARCHAR(9), manager INT NULL, hiredate DATETIME, salary DECIMAL(7,2), comm DECIMAL(5,2), department INT NULL)	Error Code: 1046. No database selected Select the de... 0.050 sec	
3	20:10:47	CREATE TABLE newhire(empno INT PRIMARY KEY, ename VARCHAR(10), job VARCHAR(9), manager INT NULL, hiredate DATETIME, salary DECIMAL(7,2), comm DECIMAL(5,2), department INT NULL)	Error Code: 1046. No database selected Select the de... 0.044 sec	
4	20:11:05	CREATE TABLE newhire(empno INT PRIMARY KEY, ename VARCHAR(10), job VARCHAR(9), manager INT NULL, hiredate DATETIME, salary DECIMAL(7,2), comm DECIMAL(5,2), department INT NULL)	0 row(s) affected 0.116 sec	
5	20:11:46	SELECT * FROM newhire LIMIT 0, 1000	0 row(s) returned 0.045 sec / 0.0...	
6	20:12:41	INSERT INTO newhire (empno, ename, job, manager, hiredate, salary, comm, department) VALUES (1, 'JOHNSON', 'ADMIN', 6, '1990-12-17', 18000, NULL, 4)	14 row(s) affected Records: 14 Duplicates: 0 Warnings: 0 0.048 sec	
7	20:13:18	SELECT * FROM newhire LIMIT 0, 1000	14 row(s) returned 0.044 sec / 0.0...	

Object Info Session Schema: QuickSightDatabase

Step 21: Create other table with the code

```

1 • CREATE TABLE department(
2     deptno INT NOT NULL,
3     dname VARCHAR(14),
4     loc VARCHAR(13));
5
6 • INSERT INTO department (deptno, dname, loc) VALUES
7     (1, 'ACCOUNTING', 'ST LOUIS'),
8     (2, 'RESEARCH', 'NEW YORK'),
9     (3, 'SALES', 'ATLANTA'),
10    (4, 'OPERATIONS', 'SEATTLE');
11

```

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

Aurora and RDS > Databases > quicksightdatabase

Summary		Actions	
DB identifier	quicksightdatabase	Status	Available
CPU	3.86%	Role	Instance
Class	db.t4g.micro	Current activity	0 Connections
Engine: MySQL Community			
Region & AZ: ap-southeast-2c			

Connectivity & security

Endpoint & port	Networking	Security
Endpoint: quicksightdatabase.crwug28.zeidh3.ap-southeast-2.rds.amazonaws.com	Availability Zone: ap-southeast-2c VPC: vpc-029d59ea43d64072f Subnet group: default-vpc-029d59ea43d64072f Subnets: subnet-057a0503be5811292, subnet-067b27e3782945677, subnet-069b56a29f2e02917	VPC security groups: default (sg-096d1927adcc68a) Active: Yes Publicly accessible: Yes Certificate authority: rds-ca-rsa2048-g1 Certificate authority date: May 25, 2061, 09:42 (UTC+12:00) DB instance certificate expiration date

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

The screenshot shows the AWS EC2 console under the 'Security Groups' section. A single security group named 'default' is listed. The table includes columns for Name, Security group ID, Security group name, VPC ID, and Description. The 'Actions' dropdown and 'Create security group' button are visible at the top right.

The screenshot shows the 'Edit inbound rules' page for the 'default' security group. It lists two rules:

- Rule 1: Type: All TCP, Protocol: TCP, Port range: 0 - 65535, Source: Cus... (110.173.160.6/32), Description: (empty)
- Rule 2: Type: All traffic, Protocol: All, Port range: All, Source: An... (0.0.0.0/0), Description: (empty)

A warning message at the bottom states: "⚠ Rules with source of 0.0.0.0/0 or ::/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only." Buttons for 'Cancel', 'Preview changes', and 'Save rules' are at the bottom right.

Now search for amazon quicksight.

The screenshot shows the AWS search results for 'Amazon QuickSight'. The search bar at the top contains 'Q. Amazon QuickSight'. Below it, there are sections for 'Services', 'Features', and 'Resources'.

- Services:**
 - QuickSight: Fast, easy to use business analytics
 - AWS Private Certificate Authority: Managed private certificate authority service
 - Amazon Redshift: Fast, Serverless, and cost effective SQL analytics and data warehousing
- Features:**
 - Data Exports: Billing and Cost Management feature
 - AMIs: EC2 feature
 - Dashboard: Amazon OpenSearch Service feature
- Resources:** / for a focused search

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

QuickSight account name

You will need this for you and others to sign in



maya-nextwork

QuickSight access to AWS services

Make your existing AWS data and users available in QuickSight. [Learn More](#)

IAM Role

- Use QuickSight-managed role (default)
- Use an existing role

Allow access and autodiscovery for these resources

- Amazon Redshift
- Amazon RDS
- IAM
- Amazon S3

[Select S3 buckets](#)

Optional add-on

- Add Pixel-Perfect Reports

Monthly charges begin immediately

\$500 /month* 500 unique report units **/month

Create, schedule, and share operational reports and data exports from a single fully-managed business intelligence (BI) cloud solution.

[Learn More](#)

*A unique report unit is defined to be up to 100 pages long (PDF) or 100MB in size (CSV/Excel). For example, a 200-page report constitutes 2 unique report units.

**First month charges and usage are prorated. Annual plan is available after sign up from the "Manage Subscriptions" page.

[Finish](#)

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

Find analyses & more NEW DATASET

Favorites

Recent

My folders

Shared folders

Dashboards

Data stories

Analyses

Datasets

Community

Topics

Datasets

No datasets

Import or create a new dataset to start an analysis.

Datasets

SPICE capacity for this region: Auto-purchase enable

Create a Dataset

FROM NEW DATA SOURCES

 Upload a file
.csv, .tsv, .clf, .elf, .xlsx, .json

 Salesforce
Connect to Salesforce

 S3 Analytics

 S3

 Athena

 RDS

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

New RDS data source X

Data source name

Instance ID

Connection type

Database name

Username

Password

SSL is enabled

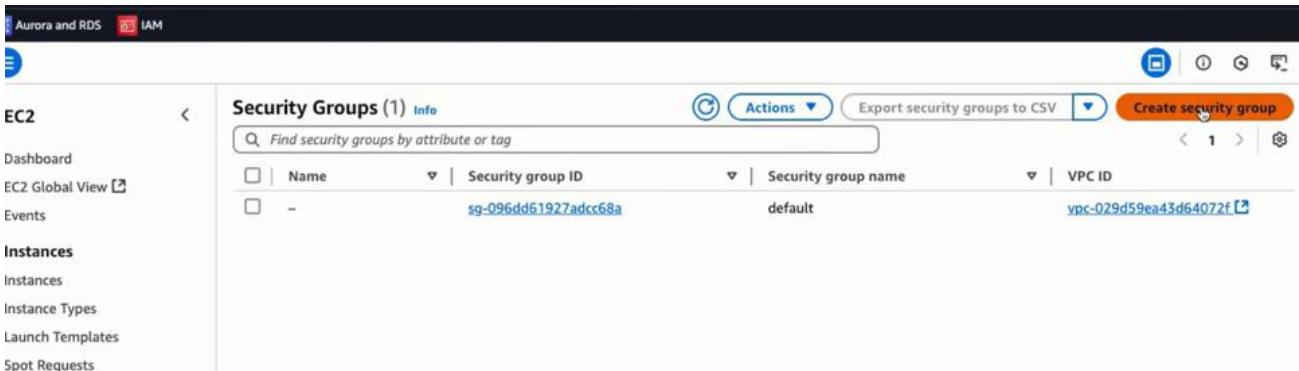
The problem here is any one can misuse as we have allowed the traffic , to make it secure we will create a security group for Quicksight to access the RDS instance.

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 button below

EC2 > Security Groups > Create security group

A security group acts as a virtual firewall for your instance to control incoming and outgoing traffic. To create a new security group, complete the fields below.

Basic details

Security group name [Info](#)

Name cannot be edited after creation.

Description [Info](#)

VPC Info

Inbound rules

This security group has no inbound rules.

[Add rule](#)

Outbound rules

Type	Protocol	Port range	Destination	Description - optional
All traffic	All	All	Cus... <input type="text" value="0.0.0.0/0"/> X	Delete

[Add rule](#)

⚠️ Rules with destination of 0.0.0.0/0 or ::/0 allow your instances to send traffic to any IPv4 or IPv6 address. We recommend setting security group rules to be more restrictive and to only allow traffic to specific known IP addresses.

Tags - optional

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

No tags associated with the resource.

Step 31: Copy the security group ID

EC2 > Security Groups > sg-0af20be670dd9d52c - QuickSight_SecGp

Security group (sg-0af20be670dd9d52c | QuickSight_SecGp) was created successfully

sg-0af20be670dd9d52c - QuickSight_SecGp

Details

Security group name	sg-0af20be670dd9d52c
Owner	640168412593
Inbound rules count	0 Permission entries
Outbound rules count	1 Permission entry

Inbound rules | **Outbound rules** | **Sharing - new** | **VPC associations - new** | **Tags**

Inbound rules

Name	Security group rule ID	IP version	Type	Protocol
No security group rules found				

[Actions](#)

Step 32: Click on manage quicksight

Username
maya-IAM-admin

Account name
maya-nextwork

Manage QuickSight

- [English](#)
- [Sydney](#)

Help

Sign out

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

Manage QuickSight / Manage VPC connections / Add VPC Connection

Add VPC Connection

Securely connect your data to QuickSight using a Virtual Private Cloud (VPC) connection. [Learn more](#)

AWS console links

- [VPC](#)
- [Subnet](#)
- [Security group](#)
- [DNS resolvers](#)
- [IAM console](#)

VPC connection name: RDS_VPC

VPC ID: vpc-029d59ea43d64072f

Execution role: aws-quicksight-service-role-v0

Subnets (Select at least two)

Availability Zone	Subnet ID
ap-southeast-2a	subnet-069b56a29f2e02917
ap-southeast-2b	subnet-057a0503be5811292
ap-southeast-2c	subnet-067b27e3782945677

Security Group IDs

sg-0af20be670dd9d52c
Search
<input type="checkbox"/> sg-096dd61927adcc68a
<input checked="" type="checkbox"/> sg-0af20be670dd9d52c

It throws an error

Step 34:

IAM > Roles

Identity and Access Management (IAM)

aws-quicksight-service-role-v0

Filter results (4)

Roles (38) [Info](#)

An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

Role name	Trusted entities	Last activity
aws-quicksight-service-role-v0	AWS Service: quicksight	...
AWSCodeDeployRole	AWS Service: codedeploy	...
AWSServiceRoleForAmazonSSM	AWS Service: ssm (Service-Linked Role)	...
AWSServiceRoleForAPIGateway	AWS Service: ops.apigateway (Service-Linked Role)	...
AWSServiceRoleForLexV2Bots_038Y76WQ6Z6	AWS Service: lexv2 (Service-Linked Role)	...
AWSServiceRoleForLexV2Bots_64C9UOVP3XK	AWS Service: lexv2 (Service-Linked Role)	...
AWSServiceRoleForLexV2Bots_C9314WSAD7D	AWS Service: lexv2 (Service-Linked Role)	...
AWSServiceRoleForLexV2Bots_E1E47ONOMSA	AWS Service: lexv2 (Service-Linked Role)	...
AWSServiceRoleForLexV2Bots_ENJ9BSJ9YRG	AWS Service: lexv2 (Service-Linked Role)	...
AWSServiceRoleForLexV2Bots_FJ40X3HTGV8	AWS Service: lexv2 (Service-Linked Role)	...
AWSServiceRoleForLexV2Bots_FSTZKKSZYA	AWS Service: lexv2 (Service-Linked Role)	...
AWSServiceRoleForLexV2Bots_JI965PTPQ5	AWS Service: lexv2 (Service-Linked Role)	...

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

aws-quicksight-service-role-v0 [Info](#) [Delete](#) [Edit](#)

Summary

Creation date
May 27, 2025, 20:19 (UTC+12:00)

ARN
 arn:aws:iam::640168412593:role/service-role/aws-quicksight-service-role-v0

Last activity
 16 minutes ago

Maximum session duration
1 hour

[Permissions](#) [Trust relationships](#) [Tags](#) [Last Accessed](#) [Revoke sessions](#)

Permissions policies (3) [Info](#) [C](#) [Simulate](#) [Remove](#) [Add permissions ▲](#)

You can attach up to 10 managed policies.

Filter by Type
 Search [All types](#)

<input type="checkbox"/>	Policy name	Type	Attached entities
<input type="checkbox"/>	AWSQuickSightIAMPolicy	Customer managed	1
<input type="checkbox"/>	AWSQuickSightRDSPolicy	Customer managed	2
<input type="checkbox"/>	AWSQuickSightRedshiftPolicy	Customer managed	1

[Attach policies](#) [Create inline policy](#)

[◀](#) [1](#) [▶](#) [⚙️](#)

▶ **Permissions boundary (not set)**

▼ **Generate policy based on CloudTrail events**

You can generate a new policy based on the access activity for this role, then customize, create, and attach it to this role. AWS uses your CloudTrail events to identify the services and actions used and generate a policy. [Learn more ↗](#)

[Generate policy](#)

No requests to generate a policy in the past 7 days.

Step 36: change visual to json and add the code

The screenshot shows the AWS IAM Policy Editor interface. On the left, there is a code editor window titled "Policy editor" containing the following JSON code:

```

1  {
2      "Version": "2012-10-17",
3      "Statement": [
4          {
5              "Effect": "Allow",
6              "Action": [
7                  "ec2:DescribeVpcs",
8                  "ec2:DescribeSubnets",
9                  "ec2:DescribeSecurityGroups",
10                 "ec2:DescribeNetworkInterfaces",
11                 "ec2:CreateNetworkInterface",
12                 "ec2:DeleteNetworkInterface",
13                 "ec2:ModifyNetworkInterfaceAttribute",
14                 "iam:PassRole"
15             ],
16             "Resource": "*"
17         },
18         {
19             "Effect": "Allow",
20             "Action": [
21                 "iam:PassRole"
22             ],
23             "Resource": "*"
24         }
25     ]
26 }
27

```

Below the code editor, there is a button labeled "+ Add new statement". At the bottom of the editor, it says "JSON Ln 27, Col 0" and "9884 of 10240 characters remaining".

On the right side of the interface, there is a panel titled "Edit statement" with the sub-section "Select a statement". It contains the instruction "Select an existing statement in the policy or add a new statement." and a button labeled "+ Add new statement".

At the bottom right of the interface, there are buttons for "Cancel" and "Next".

Step 37: Add the policy name and create policy

The screenshot shows the "Review and create" step of the policy creation wizard.

Review and create Info

Review the permissions, specify details, and tags.

Policy details

Policy name
Enter a meaningful name to identify this policy.

Maximum 128 characters. Use alphanumeric and '+=_,-.' characters.

Permissions defined in this policy Info

Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it.

Allow (2 of 441 services)

Service	▲ Access level	▼ Resource	Request condition
EC2	Limited: List, Write	All resources	None
IAM	Limited: Write	All resources	None

Show remaining 439 services

Create policy

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

The screenshot shows the 'Add VPC Connection' page. At the top, there's a header with the QuickSight logo and navigation links: 'Manage QuickSight / Manage VPC connections / Add VPC Connection'. The main title is 'Add VPC Connection'. Below it, a sub-instruction reads: 'Securely connect your data to QuickSight using a Virtual Private Cloud (VPC) connection. [Learn more](#)'. On the left, there's a sidebar titled 'AWS console links' with links to 'VPC', 'Subnet', 'Security group', 'DNS resolvers', and 'IAM console'. The main form area has several input fields:

- 'VPC connection name': 'RDS_VPC'
- 'VPC ID': 'vpc-029d59ea43d64072f' (with a note: 'This can not be changed later.')
- 'Execution role': 'aws-quicksight-service-role-v0'
- 'Subnets (Select at least two)':

Availability Zone	Subnet ID
ap-southeast-2a	subnet-069b56a29f2e02917
ap-southeast-2b	subnet-057a0503be5811292
ap-southeast-2c	subnet-067b27e3782945677
- 'Security Group IDs': 'sg-0af20be670dd9d52c'
- 'DNS resolver endpoints (optional)': 'One endpoint per line' (with a note: 'One endpoint per line'))

At the bottom right are 'ADD' and 'CANCEL' buttons.

Step 39: Finally we added VPC Connection

The screenshot shows the 'Manage VPC connections' page. At the top, there's a header with the QuickSight logo and navigation links: 'Manage QuickSight / Manage VPC connections'. The main title is 'Manage VPC connections'. On the right, there's a large blue 'ADD VPC CONNECTION' button. Below the title, there's a table listing existing VPC connections:

VPC connection name	VPC ID	VPC connection ARN	Security Gro...	DNS resolvers	Status	Ac...
RDS_VPC	vpc-029d59ea43d64072f	arn:aws:quicksight:ap-s...	sg-0af20be6...		UNAVAILABLE	:

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

Security group
List of DB security groups to associate with this DB instance.

Certificate authority [Info](#)
Using a server certificate provides an extra layer of security by validating that the connection is being made to an Amazon database. It does so by checking the server certificate that is automatically installed on all databases that you provision.

Additional configuration

Public access

- Publicly accessible**
RDS assigns a public IP address to the database. Amazon EC2 instances and other resources outside of the VPC can connect to your database. Resources inside the VPC can also connect to the database. Choose one or more VPC security groups that specify which resources can connect to the database.
- Not publicly accessible**
No IP address is assigned to the DB instance. EC2 instances and devices outside the VPC can't connect.

When a DB instance is not publicly accessible, EC2 instances and devices outside your VPC can't connect unless they use AWS Site-to-Site VPN or AWS Direct Connect. [Learn more](#)

Database port
Specify the TCP/IP port that the DB instance will use for application connections. The application connection string must specify the port number. The DB security group and your firewall must allow connections to the port.

Learn more [\[?\]](#)

3306

Database authentication

Database authentication options [Info](#)

- Password authentication**
Authenticates using database passwords.
- Password and IAM database authentication**
Authenticates using the database password and user credentials through AWS IAM users and roles.
- Password and Kerberos authentication**
Choose a directory in which you want to allow authorized users to authenticate with this DB instance using Kerberos Authentication.

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

Create security group [Info](#)

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

Basic details

Security group name [Info](#)
RDS_SecGp
Name cannot be edited after creation.

Description [Info](#)
Allows SSH access to developers

VPC [Info](#)
vpc-029d59ea43d64072f

Inbound rules [Info](#)

Type	Protocol	Port range	Source	Description - optional
MySQL/Aurora	TCP	3306	Cus... <input type="button" value="Delete"/>	sg-0af20be670dc <input type="button" value="Delete"/>
			Cus... <input type="button" value="Delete"/>	sg-0af20be670dd9d52c <input type="button" value="Delete"/>

Add rule

Outbound rules [Info](#)

Type	Protocol	Port range	Destination	Description - optional
All traffic	All	All	Cus... <input type="button" value="Delete"/>	0.0.0.0/0 <input type="button" value="Delete"/>

Add rule

Rules with destination of 0.0.0.0/0 or ::/0 allow your instances to send traffic to any IPv4 or IPv6 address. We recommend setting security group rules to be more restrictive and to

Step 42: Click on modify

Summary

DB Identifier quicksightdatabase

CPU 3.40%

Status Available

Class db.t4g.micro

Role Instance

Current activity 2 Connections

Engine MySQL Community

Region & AZ ap-southeast-2c

Recommendations

Connectivity & security

Endpoint & port

Endpoint quicksightdatabase.crwug28aws.com

Port 3306

Networking

Availability Zone ap-southeast-2c

VPC vpc-029d59ea43d64072f

Subnet group default-vpc-029d59ea43d64072f

Subnets

- subnet-057ad503a5811292
- subnet-057ad503a5811292
- subnet-069b56a29f2e02917

Network type IPv4

Security

VPC security groups

- default (sg-0af20be670dd9d52c)
- Active

Publicly accessible

Certificate authority [Info](#)
rds-ca-rsa2048-g1

Certificate authority date May 27, 2026, 19:55 (UTC+12:00)

DB instance certificate
Expiration date: May 27, 2026, 19:55 (UTC+12:00)

Step 43:

Aurora and RDS IAM

Aurora and RDS > Databases > Modify DB instance: quicksightdatabase

IPv4
Your resources can communicate only over the IPv4 addressing protocol.

Dual-stack mode
Your resources can communicate over IPv4, IPv6, or both.

DB subnet group
default-vpc-029d59ea43d64072f

Security group
List of DB security groups to associate with this DB instance.

Choose security groups

Q default

RDS_SecGp

RDS-CA-RSA2048-g1 (default)
Expiry: May 25, 2061

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

New RDS data source

Data source name
RDS_VPC_Database

Instance ID
quicksightdatabase

Connection type
RDS_VPC

Database name
QuickSightDatabase

Username
admin

Password

Validating SSL is enabled Create data source

Step 45:

Choose your table

RDS_VPC_Database

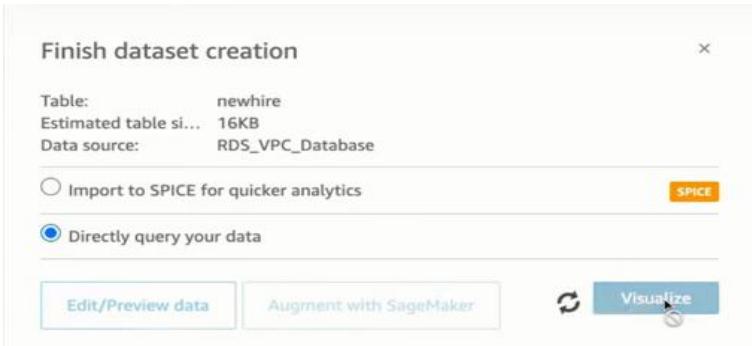
Tables: contain the data you can visualize.

department

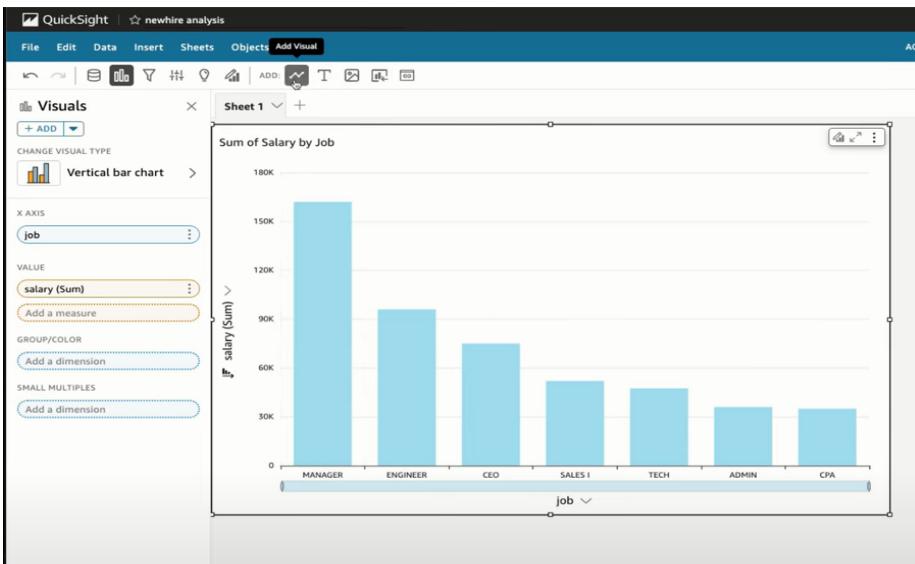
newhire

Edit/Preview data Use custom SQL Select

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

New dashboard Replace existing dashboard

Dashboard name: RDS New Hire Data

Select sheets: All sheets

Data story: Allow sharing data stories

Generative capabilities:

- Allow executive summary
- Allow data Q&A

Source: 1 dataset linked [MANAGE Q&A](#)

MORE SETTINGS

Add notes (optional)

Only owners of this dashboard will see this note under version history

PUBLISH DASHBOARD

Delete All the items inorder to avoid extra charge.

Step 1: Delete as shown in the figure

The screenshot shows the AWS QuickSight interface. On the left, there's a sidebar with navigation links: Favorites, Recent, My folders, Shared folders, Dashboards, Data stories, Analyses, Datasets, Community, and Topics. The 'Dashboards' link is currently selected. In the main area, there's a list of dashboards. One dashboard titled 'RDS New Hire Data' is selected, and a context menu is open over it. The menu options are: Add to folder, See recent snapshots, and Delete. The 'Delete' option is highlighted with a cursor.

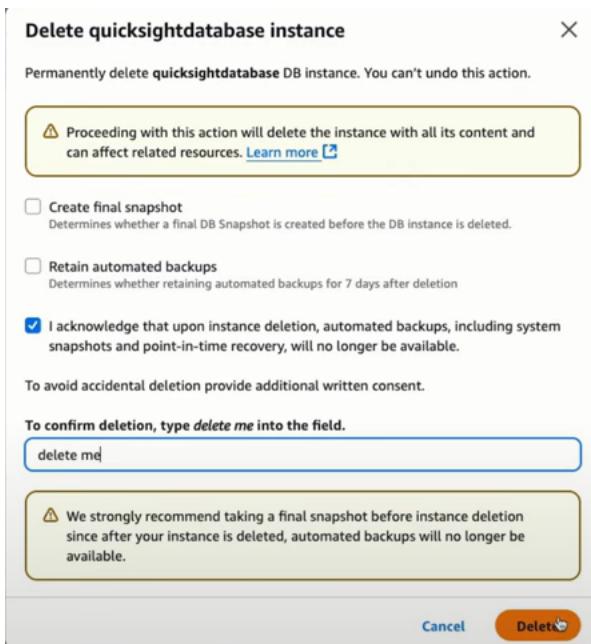
Step 2: Delete the dataset using delete option

This screenshot shows the AWS QuickSight interface with the 'Datasets' link selected in the sidebar. A list of datasets is displayed, with one dataset named 'newhire' selected. A context menu is open over this dataset, showing options like Create analysis, Edit, Add to folder, Use in a new dataset, Duplicate, Manage permissions, Row-level security, Column-level security, and Delete. The 'Delete' option is highlighted.

Step 3: Go to RDS instance and delete

This screenshot shows the AWS Aurora and RDS interface. The left sidebar includes links for Aurora and RDS, Databases, Query editor, Performance insights, Snapshots, Exports in Amazon S3, Automated backups, Reserved instances, Proxies, Subnet groups, Parameter groups, Option groups, Custom engine versions, Zero-ETL integration, Events, Event subscriptions, and Recommendations. The 'Databases' link is selected. In the main area, the 'Databases' section shows a single database named 'quicksightdatabase' with an 'Available' status. A context menu is open over this database, listing actions such as Stop temporarily, Reboot, Delete, Set up EC2 connection, Set up Lambda connection, Migrate data from EC2 database - new, Create read replica, Create Aurora read replica, Create blue/green deployment, Promote, Convert to Multi-AZ deployment, Take snapshot, Restore to point in time, Migrate snapshot, Create zero-ETL integration, Create RDS Proxy, and Create ElastiCache cluster. The 'Delete' option is highlighted.

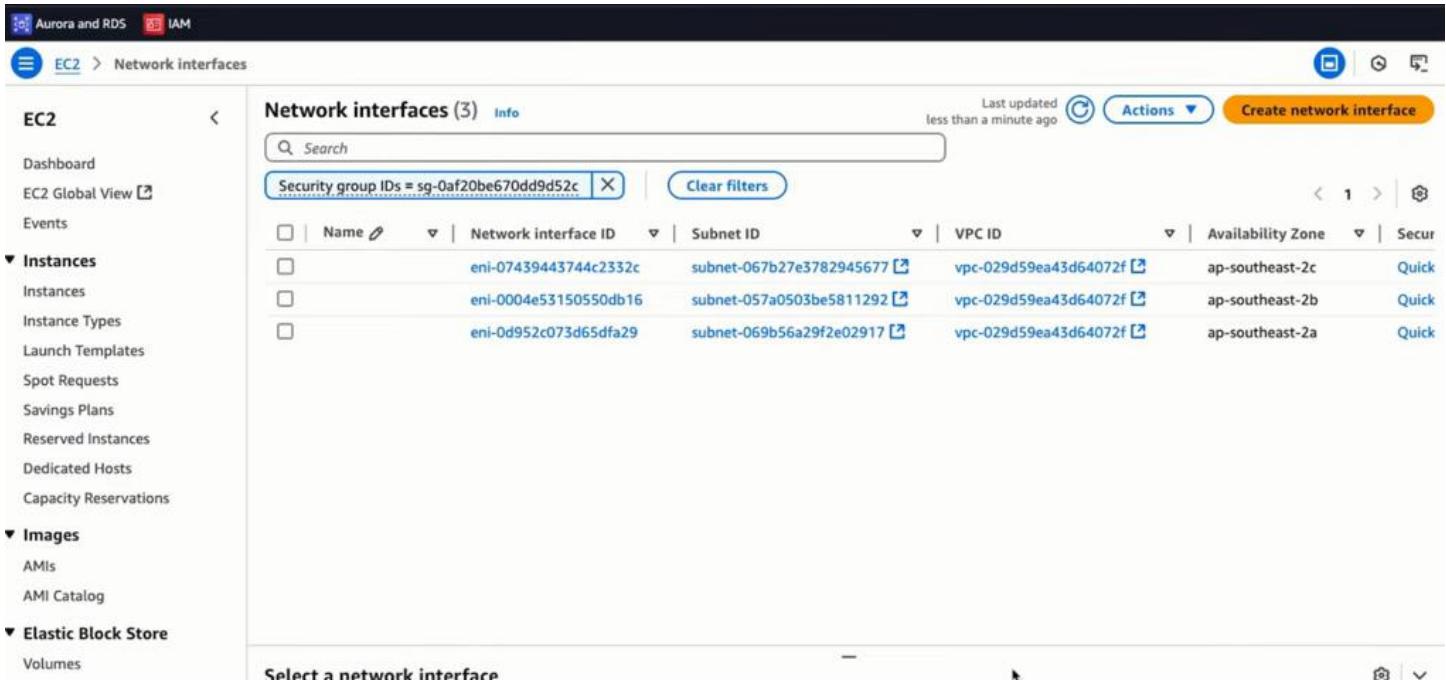
Step 4: follow all the steps



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

The screenshot shows the AWS EC2 Security Groups page. A context menu is open over a selected security group named "sg-05c4eb2b441388dc1". The menu options include: View details, Edit inbound rules, Edit outbound rules, Manage tags, Manage stale rules, Copy to new security group, Share security group, and Delete security groups.

Step 8: delete the quicksight_secGp using actions

The screenshot shows the AWS Security Groups page. A green success message at the top states: "Security group (sg-0af20be670dd9d52c | QuickSight_SecGp) successfully deleted". Below it, the table lists two security groups: "default" and "QuickSight_SecGp".

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

The screenshot shows the AWS IAM Roles page. A modal dialog box is displayed, asking "Remove and delete QuickSightAllowVPC ?". It explains that removing the role will permanently delete it and all its permissions. A text input field asks to "To confirm deletion, enter the inline policy name in the text input field." The user has typed "QuickSight" into this field. The dialog includes "Cancel" and "Delete" buttons.

Step 10: Delete Quicksight account

The screenshot shows the 'Account settings' page in the QuickSight console. The left sidebar lists various account management options. Under 'Account termination', it says 'Manage account termination protection or delete this account' and has a 'Manage' button. The main area shows 'Notification email address' set to 'maya@nextwork.org'. A note below it says 'This will be where access requests and service notifications will be sent.' There is also a checked checkbox for 'Enable IAM user access requests to this account.' The status 'Account termination protection is off.' is displayed.

Step 11: By confirming delete the account

The screenshot shows a confirmation dialog titled 'Account termination'. It displays the 'QuickSight account name' as 'maya-nextwork'. Below it, 'Account termination protection' is shown as 'off'. A note states: 'Account termination protection is an extra safe-guard to help prevent accidental deletion of accounts.' A message at the bottom says 'Delete account' and 'Deleting this account can't be undone and will permanently delete all users, dashboards, analyses, along with other related data.' A text input field contains 'confir'. At the bottom are 'Cancel' and 'Delete account' buttons.

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

The screenshot shows the AWS IAM Roles page with a modal dialog titled "Delete aws-quicksight-service-role-v0?". The dialog asks if the user wants to permanently delete the role, noting it will also delete all inline policies and any attached instance profiles. It displays the role name "aws-quicksight-service-role-v0" and its last activity (21 minutes ago). A note at the bottom states that recent activity usually appears within 4 hours. The "Delete" button is highlighted in blue.

Role name	Trusted entities	Last activity
aws-quicksight-service-role-v0	AWS Service: quicksight	21 minutes ago
AWSCodeDeployRole	AWS Service: codedeploy	-
AWSLambdaBasicExecutionRole	AWS Lambda (Service-Linked Role)	24 days ago
AWSLambdaContainerOptimizerRole	AWS Lambda Container Optimizer (Service-Linked Role)	-
AWSLambdaEventSourceMappingRole	AWS Lambda Event Source Mapping (Service-Linked Role)	-
AWSLambdaFunctionV2InvokerRole	AWS Lambda Function V2 Invoker (Service-Linked Role)	-
AWSLambdaLayerVersionRole	AWS Lambda Layer Version (Service-Linked Role)	-
AWSLambdaLogDeliveryRole	AWS Lambda Log Delivery (Service-Linked Role)	-
AWSLambdaPowerInvokeRole	AWS Lambda Power Invoke (Service-Linked Role)	-
AWSLambdaPowerInvokeRoleForV2Bots	AWS Lambda Power Invoke for V2 Bots (Service-Linked Role)	-
AWSLambdaPowerInvokeRoleForLexV2Bots	AWS Lambda Power Invoke for Lex V2 Bots (Service-Linked Role)	-
AWSLambdaPowerInvokeRoleForLexV2Jobs	AWS Lambda Power Invoke for Lex V2 Jobs (Service-Linked Role)	-

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": "*"
```

```
    }
```

```
  ]
```

```
}
```