ANALYTICS SYSTEMS ENGINEERING (MSDS 436)

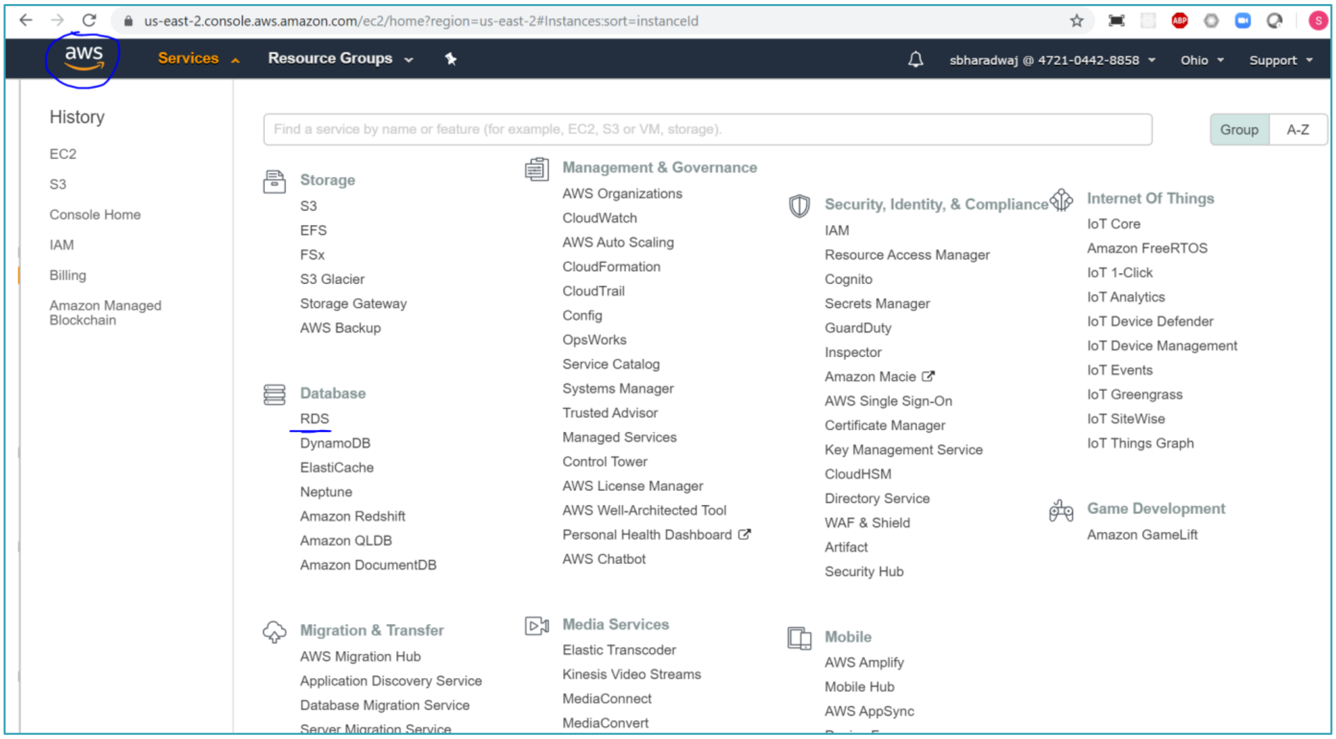
EXERCISE 2

shreenidhi.bharadwaj@northwestern.edu | ChristopherFiore2015@u.northwestern.edu

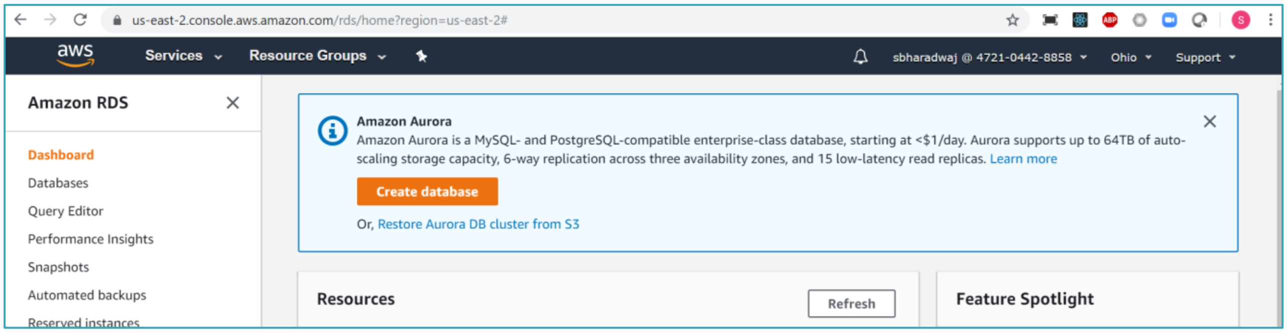
CONTENTS

CREATE POSTGRESQL DATABASE IN AWS

1. Go to AWS services and click on RDS (Relational Databases)



2. Click on Create Database and choose Standard Create > Amazon Aurora > Postgres Edition.



us-east-2.console.aws.amazon.com/rds/home?region=us-east-2#

Amazon RDS

- Dashboard
- Databases
- Query Editor
- Performance Insights
- Snapshots
- Automated backups
- Reserved instances

Amazon Aurora

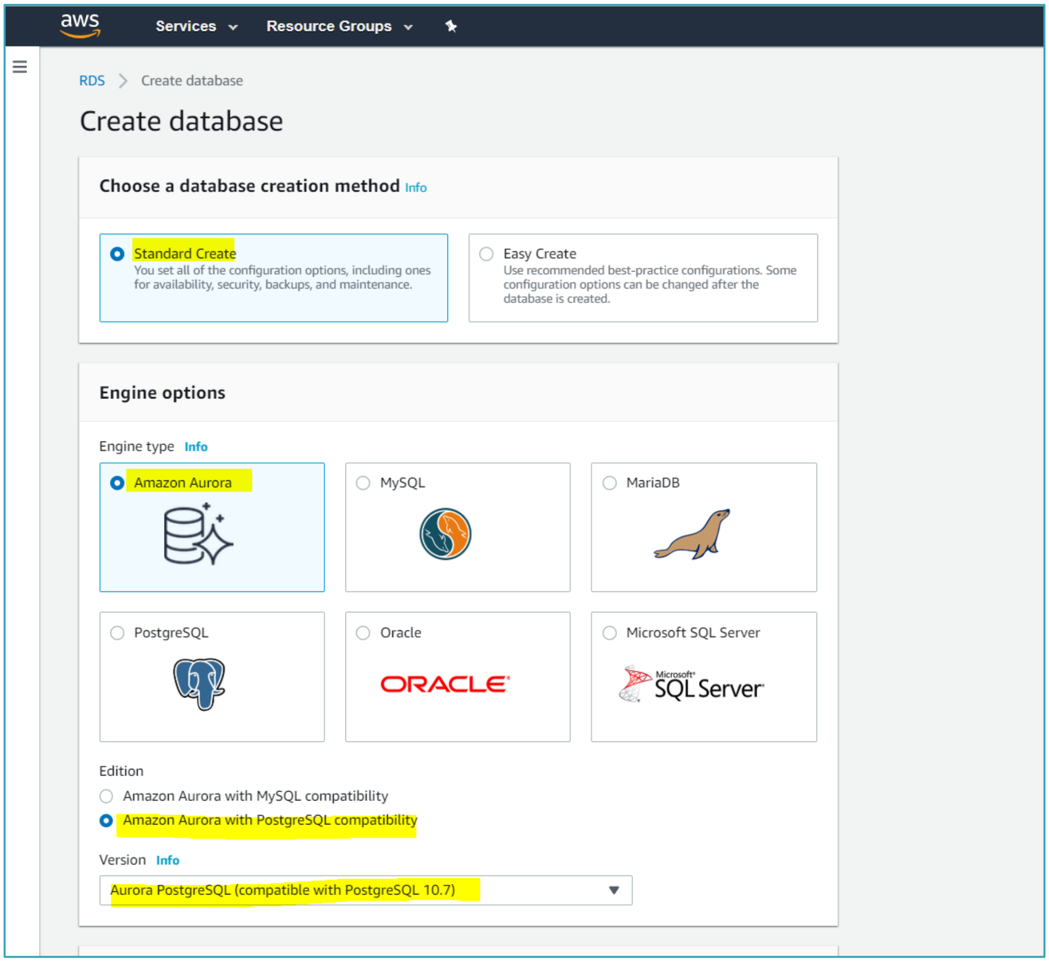
Amazon Aurora is a MySQL- and PostgreSQL-compatible enterprise-class database, starting at <$1/day. Aurora supports up to 64TB of auto-scaling storage capacity, 6-way replication across three availability zones, and 15 low-latency read replicas. Learn more

Create database

Or, Restore Aurora DB cluster from S3

Resources — Refresh

Feature Spotlight



RDS > Create database

Create database

Choose a database creation method Info

● 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.

Engine options

Engine type Info

● Amazon Aurora
○ MySQL
○ MariaDB
○ PostgreSQL
○ Oracle
○ Microsoft SQL Server

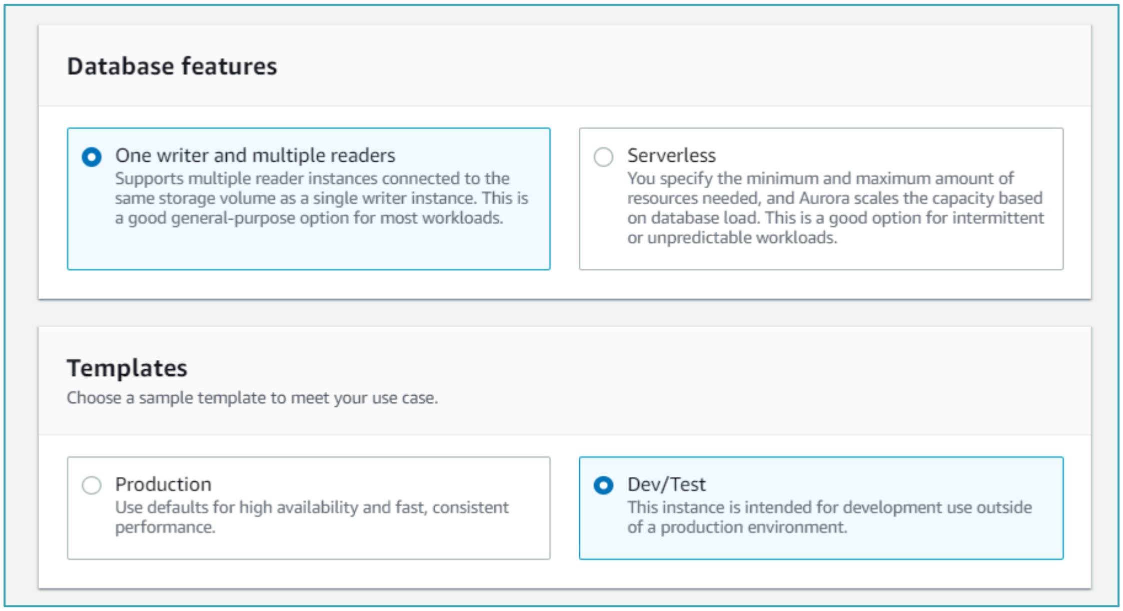
Edition

○ Amazon Aurora with MySQL compatibility
● Amazon Aurora with PostgreSQL compatibility

Version Info

Aurora PostgreSQL (compatible with PostgreSQL 10.7)

3. Scroll down, to select **One writer and multiple readers & Dev/Test**



Database features

● One writer and multiple readers
Supports multiple reader instances connected to the same storage volume as a single writer instance. This is a good general-purpose option for most workloads.

○ Serverless
You specify the minimum and maximum amount of resources needed, and Aurora scales the capacity based on database load. This is a good option for intermittent or unpredictable workloads.

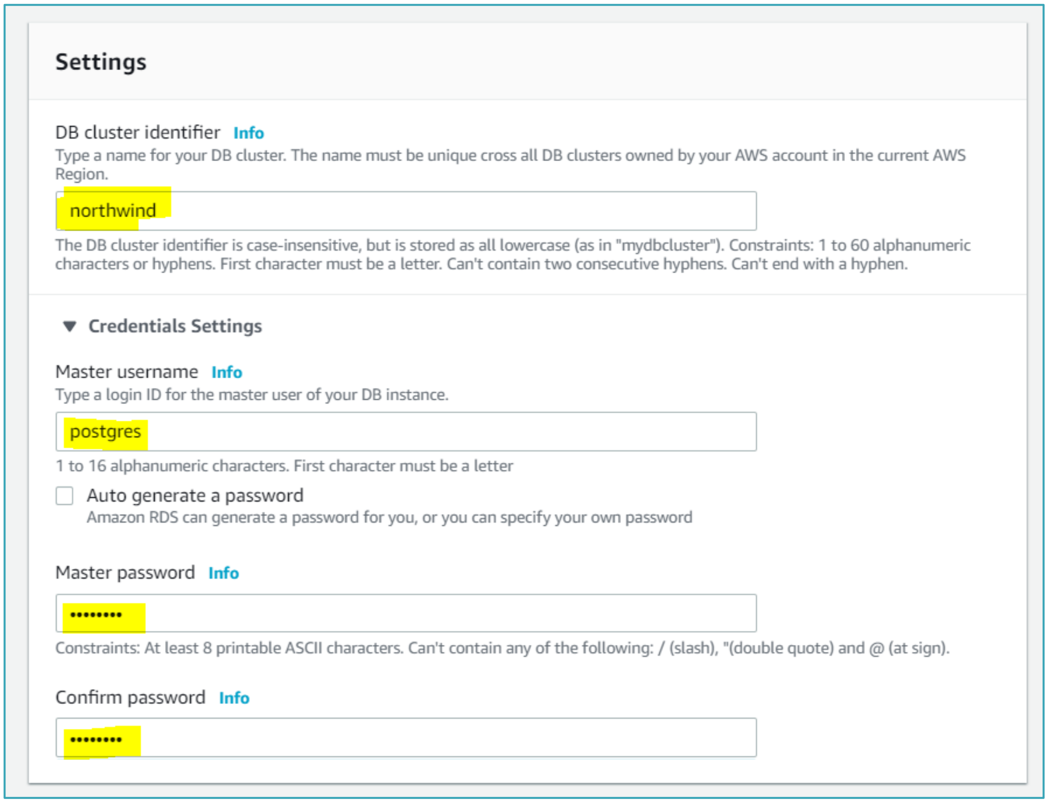
Templates

Choose a sample template to meet your use case.

○ Production
Use defaults for high availability and fast, consistent performance.

● Dev/Test
This instance is intended for development use outside of a production environment.

4. Scroll down to provide **database name (northwind), username (postgres) & password (rootroot)**



Settings

DB cluster identifier Info
Type a name for your DB cluster. The name must be unique cross all DB clusters owned by your AWS account in the current AWS Region.

northwind

The DB cluster identifier is case-insensitive, but is stored as all lowercase (as in "mydbcluster"). Constraints: 1 to 60 alphanumeric characters or hyphens. First character must be a letter. Can't contain two consecutive hyphens. Can't end with a hyphen.

▼ Credentials Settings

Master username Info
Type a login ID for the master user of your DB instance.

postgres

1 to 16 alphanumeric characters. First character must be a letter

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

Master password Info

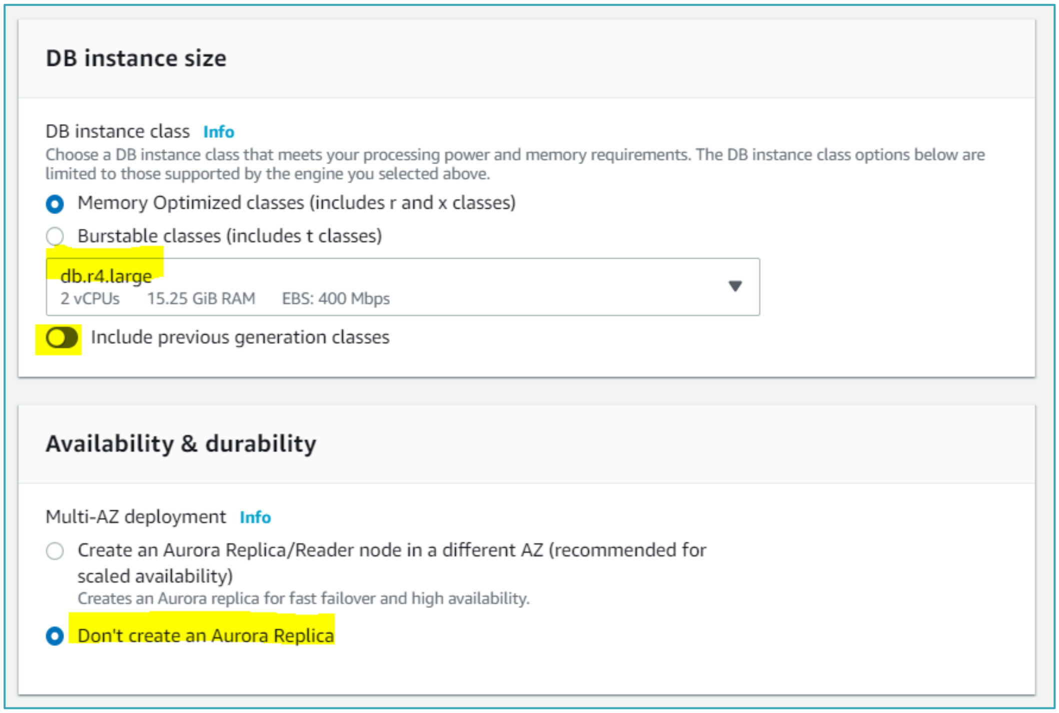
••••••••

Constraints: At least 8 printable ASCII characters. Can't contain any of the following: / (slash), "(double quote) and @ (at sign).

Confirm password Info

••••••••

5. Scroll down to Select **'db.r4. large'** as instance size & **don't create an Aurora Replica**



DB instance size

DB instance class Info

Choose a DB instance class that meets your processing power and memory requirements. The DB instance class options below are limited to those supported by the engine you selected above.

● Memory Optimized classes (includes r and x classes)

○ Burstable classes (includes t classes)

db.r4.large
2 vCPUs 15.25 GiB RAM EBS: 400 Mbps

Include previous generation classes

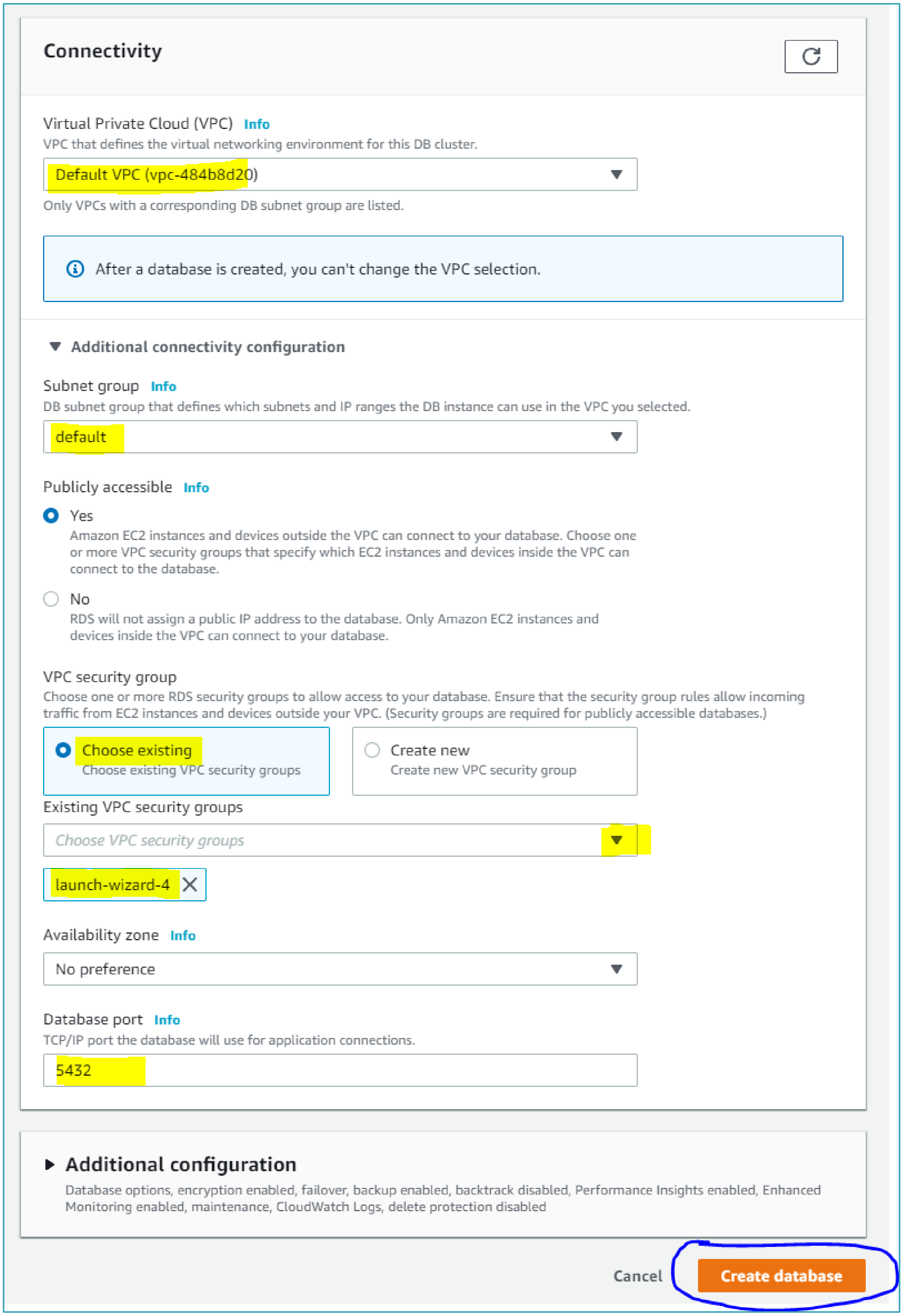
Availability & durability

Multi-AZ deployment Info

○ Create an Aurora Replica/Reader node in a different AZ (recommended for scaled availability)
Creates an Aurora replica for fast failover and high availability.

● Don't create an Aurora Replica

6. Scroll down and Select **Default VPC**, Your Existing **VPC Security group, and** Click on **Create database**



Connectivity

Virtual Private Cloud (VPC) Info

VPC that defines the virtual networking environment for this DB cluster.

Default VPC (vpc-484b8d20) ▼

Only VPCs with a corresponding DB subnet group are listed.

ⓘ After a database is created, you can't change the VPC selection.

▼ Additional connectivity configuration

Subnet group Info

DB subnet group that defines which subnets and IP ranges the DB instance can use in the VPC you selected.

default ▼

Publicly accessible Info

● Yes

Amazon EC2 instances and devices outside the VPC can connect to your database. Choose one or more VPC security groups that specify which EC2 instances and devices inside the VPC can connect to the database.

○ No

RDS will not assign a public IP address to the database. Only Amazon EC2 instances and devices inside the VPC can connect to your database.

VPC security group

Choose one or more RDS security groups to allow access to your database. Ensure that the security group rules allow incoming traffic from EC2 instances and devices outside your VPC. (Security groups are required for publicly accessible databases.)

● Choose existing
Choose existing VPC security groups

○ Create new
Create new VPC security group

Existing VPC security groups

Choose VPC security groups ▼

launch-wizard-4 ✕

Availability zone Info

No preference ▼

Database port Info

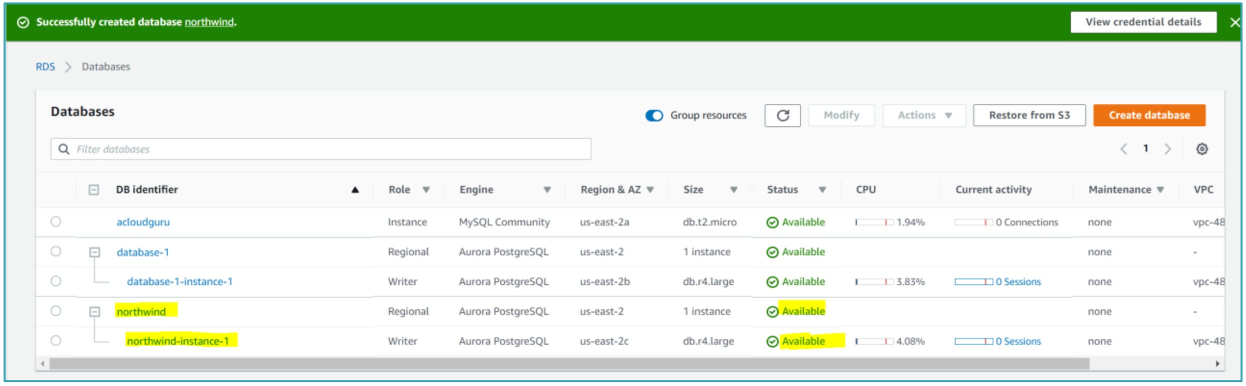
TCP/IP port the database will use for application connections.

5432

▶ Additional configuration

Database options, encryption enabled, failover, backup enabled, backtrack disabled, Performance Insights enabled, Enhanced Monitoring enabled, maintenance, CloudWatch Logs, delete protection disabled

7. It takes few moments to create the database, Once created, you get a success/Available message

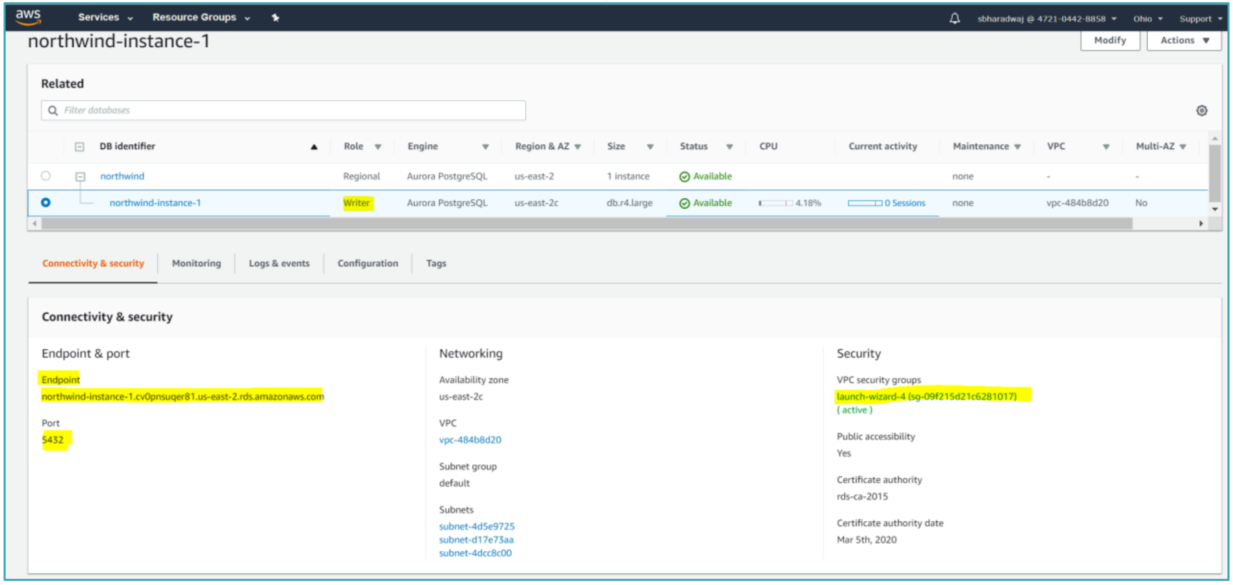


Successfully created database northwind.

Databases

	DB identifier	Role	Engine	Region & AZ	Size	Status	CPU	Current activity	Maintenance	VPC
○	acloudguru	Instance	MySQL Community	us-east-2a	db.t2.micro	Available	1.94%	0 Connections	none	vpc-48
○	database-1	Regional	Aurora PostgreSQL	us-east-2	1 instance	Available			none	-
○	database-1-instance-1	Writer	Aurora PostgreSQL	us-east-2b	db.r4.large	Available	3.83%	0 Sessions	none	vpc-48
○	northwind	Regional	Aurora PostgreSQL	us-east-2	1 instance	Available			none	-
○	northwind-instance-1	Writer	Aurora PostgreSQL	us-east-2c	db.r4.large	Available	4.08%	0 Sessions	none	vpc-48

8. Once your database status is **available** click on writer instance. Make a note of Endpoint/port (ex: northwind-instance-1.cv0pnsuqer81.us-east-2.rds.amazonaws.com/5432) & Click on VPC security Group (e.g. Launch-wizard-4)



northwind-instance-1

Related

	DB identifier	Role	Engine	Region & AZ	Size	Status	CPU	Current activity	Maintenance	VPC	Multi-AZ
○	northwind	Regional	Aurora PostgreSQL	us-east-2	1 instance	Available			none	-	-
●	northwind-instance-1	Writer	Aurora PostgreSQL	us-east-2c	db.r4.large	Available	4.18%	0 Sessions	none	vpc-484b8d20	No

Connectivity & security

Endpoint & port

Endpoint
northwind-instance-1.cv0pnsuqer81.us-east-2.rds.amazonaws.com

Port
5432

Networking

Availability zone
us-east-2c

VPC
vpc-484b8d20

Subnet group
default

Subnets
subnet-4d5e9725
subnet-d17e73aa
subnet-4dcc8c00

Security

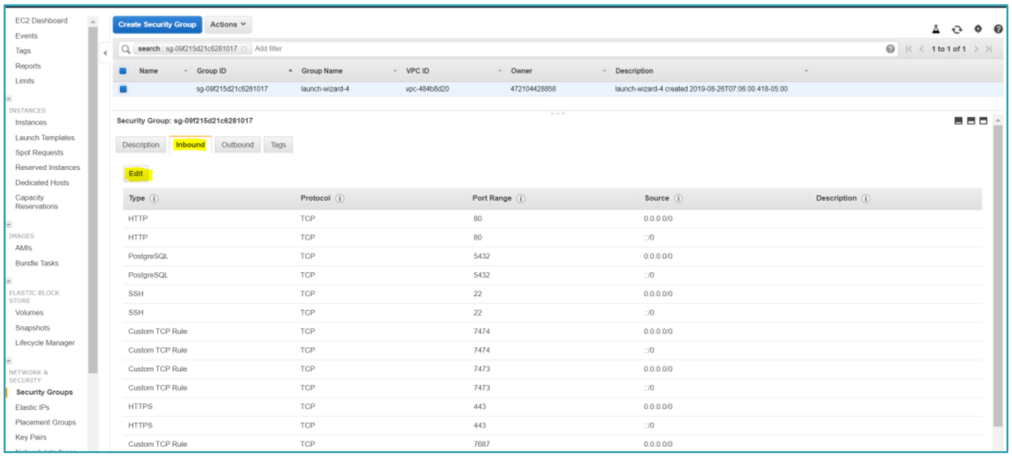
VPC security groups
launch-wizard-4 (sg-09f215d21c6281017)
(active)

Public accessibility
Yes

Certificate authority
rds-ca-2015

Certificate authority date
Mar 5th, 2020

9. Select **Inbound** tab. Click **Edit**.

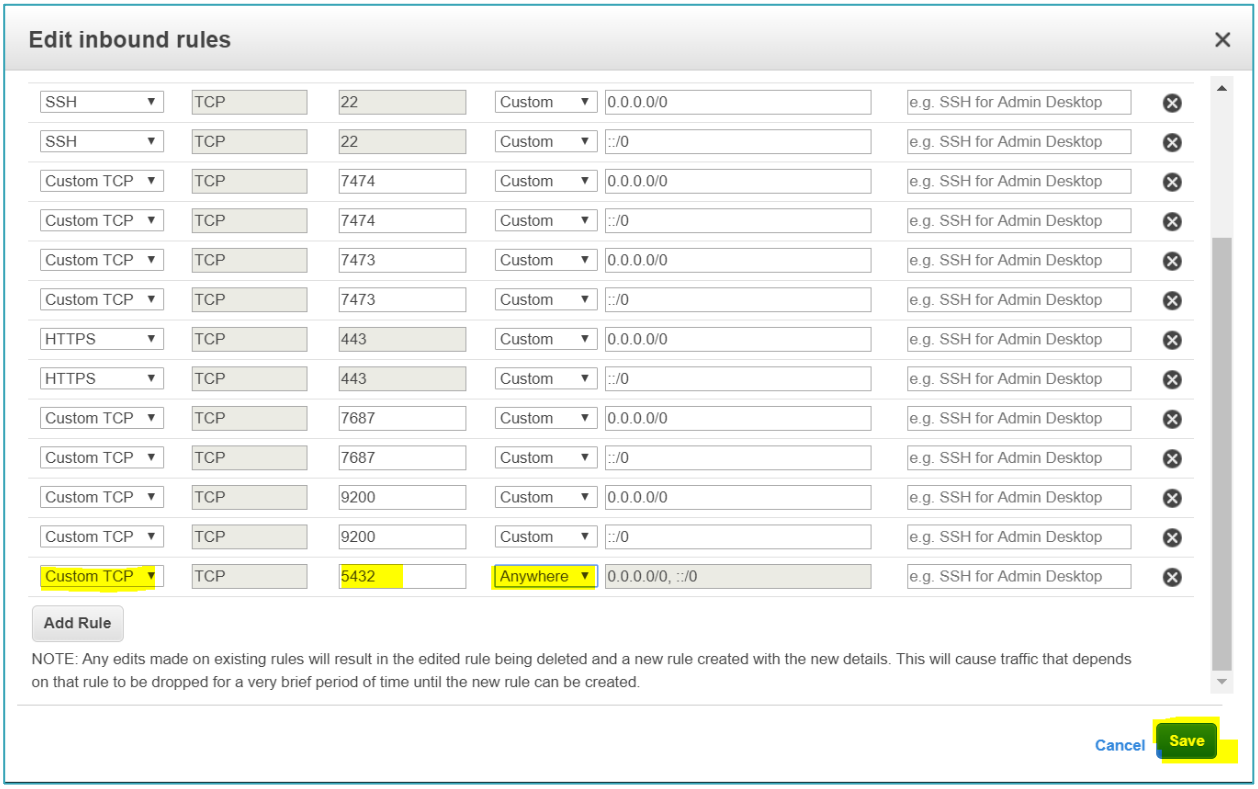


Name	Group ID	Group Name	VPC ID	Owner	Description
	sg-09f215d21c6281017	launch-wizard-4	vpc-484b8d20	472104428858	launch-wizard-4 created 2019-08-26T07:06:00.418-05:00

Security Group: sg-09f215d21c6281017

Type	Protocol	Port Range	Source	Description
HTTP	TCP	80	0.0.0.0/0	
HTTP	TCP	80	::/0	
PostgreSQL	TCP	5432	0.0.0.0/0	
PostgreSQL	TCP	5432	::/0	
SSH	TCP	22	0.0.0.0/0	
SSH	TCP	22	::/0	
Custom TCP Rule	TCP	7474	0.0.0.0/0	
Custom TCP Rule	TCP	7474	::/0	
Custom TCP Rule	TCP	7473	0.0.0.0/0	
Custom TCP Rule	TCP	7473	::/0	
HTTPS	TCP	443	0.0.0.0/0	
HTTPS	TCP	443	::/0	
Custom TCP Rule	TCP	7687	0.0.0.0/0	

10. Add new rule as shown below by clicking **Add Rule**. Once added, Click **Save** & Confirm the addition



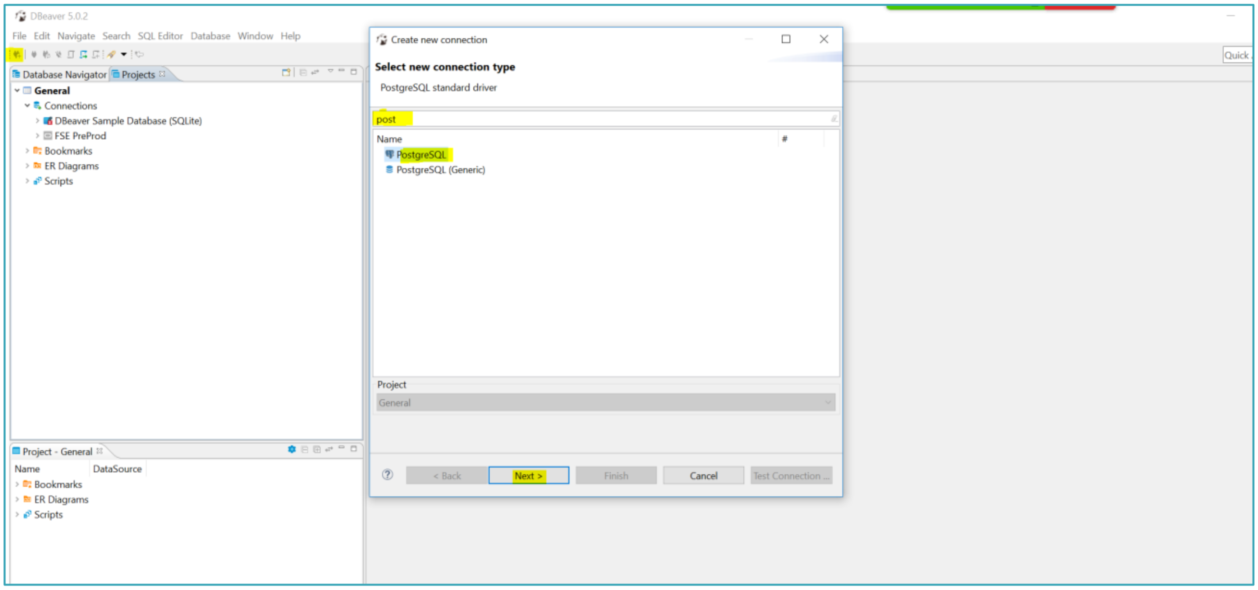
Edit inbound rules

SSH	TCP	22	Custom	0.0.0.0/0	e.g. SSH for Admin Desktop
SSH	TCP	22	Custom	::/0	e.g. SSH for Admin Desktop
Custom TCP	TCP	7474	Custom	0.0.0.0/0	e.g. SSH for Admin Desktop
Custom TCP	TCP	7474	Custom	::/0	e.g. SSH for Admin Desktop
Custom TCP	TCP	7473	Custom	0.0.0.0/0	e.g. SSH for Admin Desktop
Custom TCP	TCP	7473	Custom	::/0	e.g. SSH for Admin Desktop
HTTPS	TCP	443	Custom	0.0.0.0/0	e.g. SSH for Admin Desktop
HTTPS	TCP	443	Custom	::/0	e.g. SSH for Admin Desktop
Custom TCP	TCP	7687	Custom	0.0.0.0/0	e.g. SSH for Admin Desktop
Custom TCP	TCP	7687	Custom	::/0	e.g. SSH for Admin Desktop
Custom TCP	TCP	9200	Custom	0.0.0.0/0	e.g. SSH for Admin Desktop
Custom TCP	TCP	9200	Custom	::/0	e.g. SSH for Admin Desktop
Custom TCP	TCP	5432	Anywhere	0.0.0.0/0, ::/0	e.g. SSH for Admin Desktop

Add Rule

NOTE: Any edits made on existing rules will result in the edited rule being deleted and a new rule created with the new details. This will cause traffic that depends on that rule to be dropped for a very brief period of time until the new rule can be created.

11. Open DBeaver (client) installed on your laptop & Search for PostgreSQL, Select & click **Next**.



Select new connection type

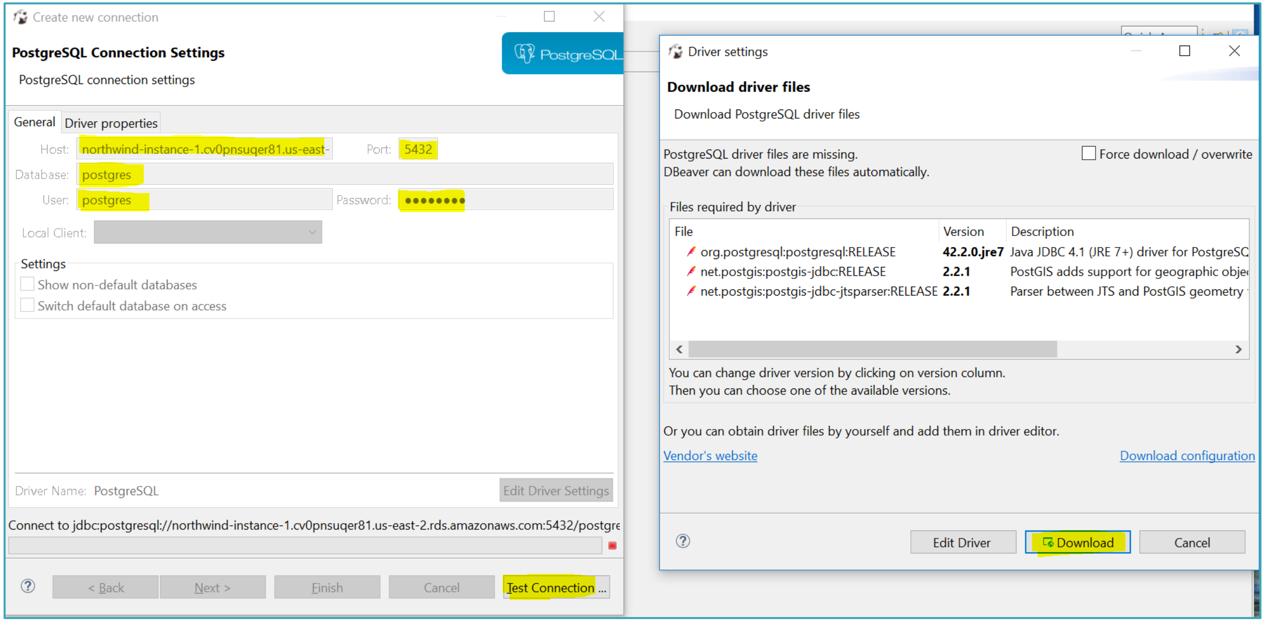
PostgreSQL standard driver

post

Name	#
PostgreSQL	
PostgreSQL (Generic)	

Project: General

12. Provide hostname, port, database, username & password and click on Test Connection.



PostgreSQL Connection Settings

PostgreSQL connection settings

Host: northwind-instance-1.cv0pnsuqer81.us-east- Port: 5432

Database: postgres

User: postgres Password: ••••••••

Settings

□ Show non-default databases

□ Switch default database on access

Driver Name: PostgreSQL

Connect to jdbc:postgresql://northwind-instance-1.cv0pnsuqer81.us-east-2.rds.amazonaws.com:5432/postgre

Download driver files

Download PostgreSQL driver files

PostgreSQL driver files are missing.
DBeaver can download these files automatically.

□ Force download / overwrite

Files required by driver

File	Version	Description
org.postgresql:postgresql:RELEASE	42.2.0.jre7	Java JDBC 4.1 (JRE 7+) driver for PostgreSC
net.postgis:postgis-jdbc:RELEASE	2.2.1	PostGIS adds support for geographic obje
net.postgis:postgis-jdbc-jtsparser:RELEASE	2.2.1	Parser between JTS and PostGIS geometry

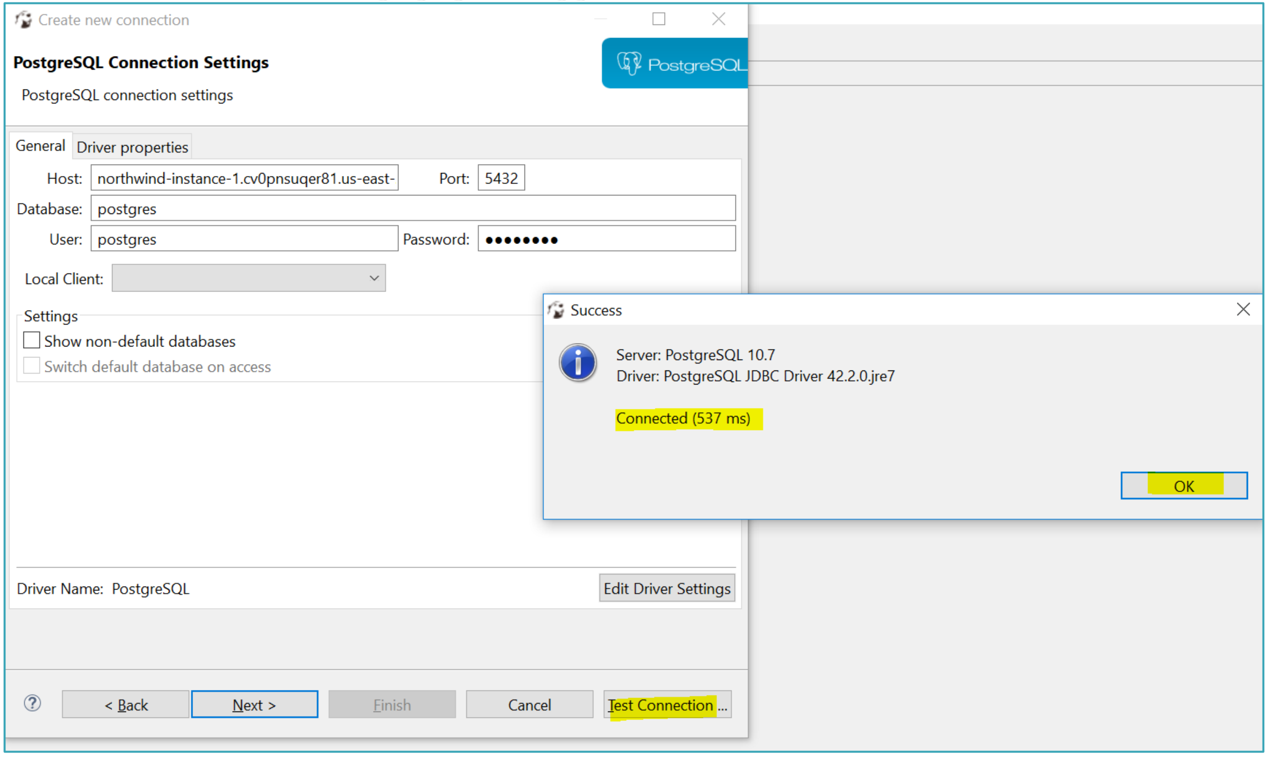
You can change driver version by clicking on version column.
Then you can choose one of the available versions.

Or you can obtain driver files by yourself and add them in driver editor.

Vendor's website

Download configuration

13. Connection confirmation popup will appear. Click on Next > Next > Finish



PostgreSQL Connection Settings

PostgreSQL connection settings

Host: northwind-instance-1.cv0pnsuqer81.us-east- Port: 5432

Database: postgres

User: postgres Password: ••••••••

Settings

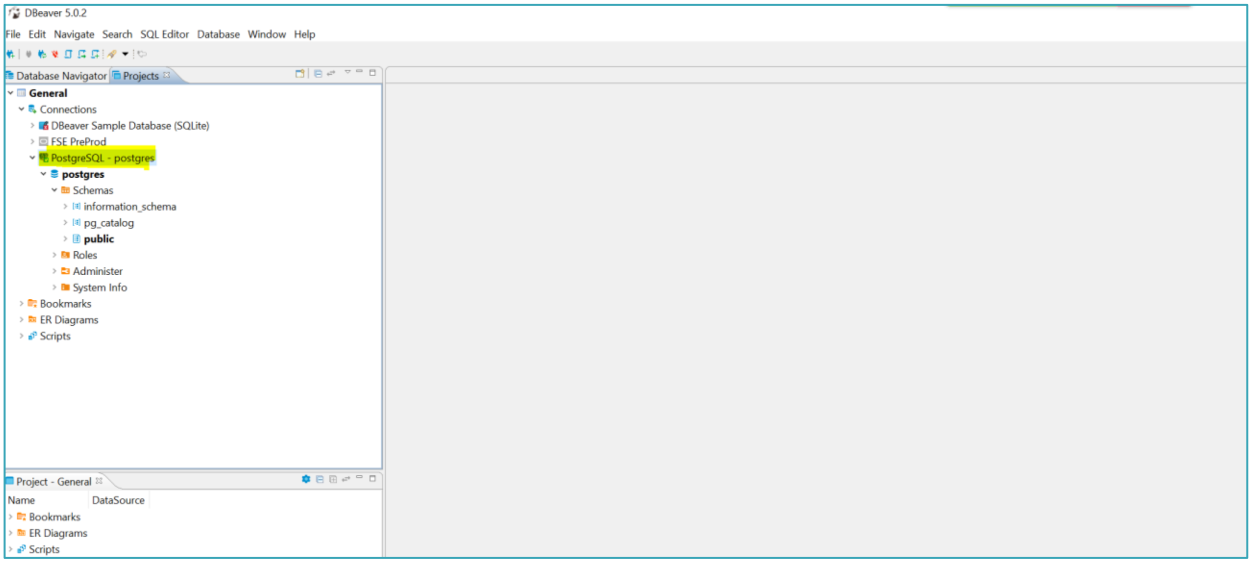
□ Show non-default databases

□ Switch default database on access

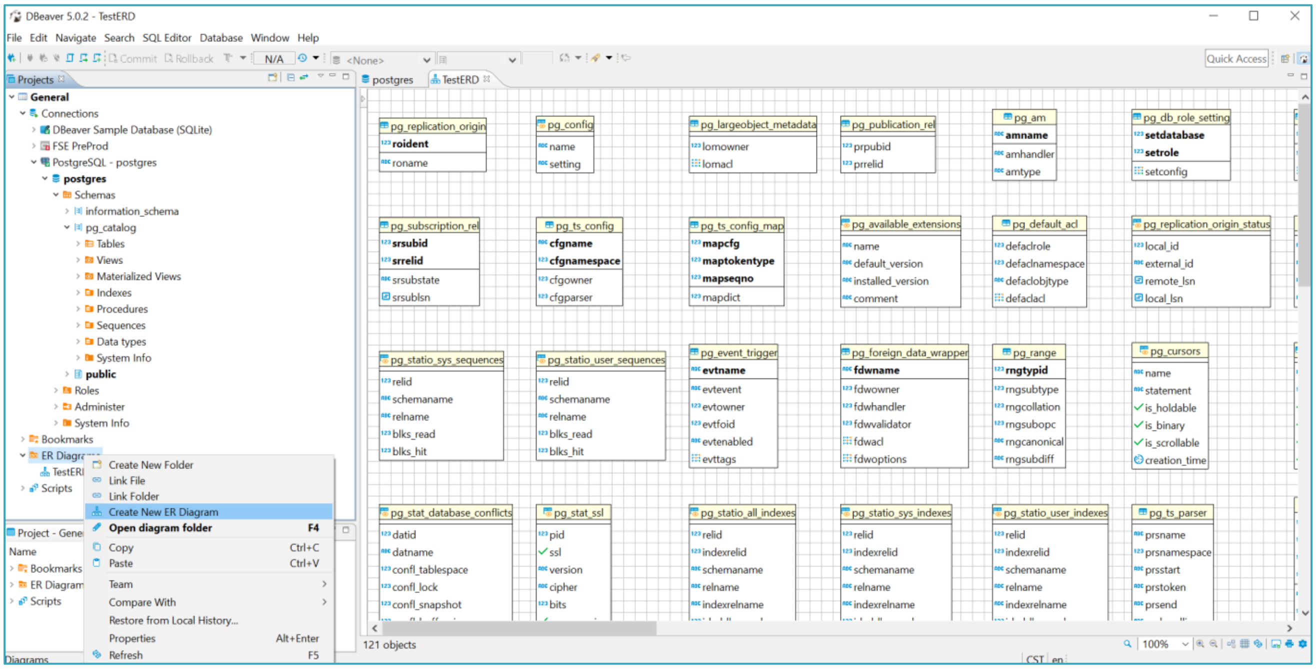
Driver Name: PostgreSQL

Server: PostgreSQL 10.7
Driver: PostgreSQL JDBC Driver 42.2.0.jre7

Connected (537 ms)



Note PostgreSQL installation is now complete. To generate ER diagram for a schema



CREATE REDSHIFT CLUSTER IN AWS

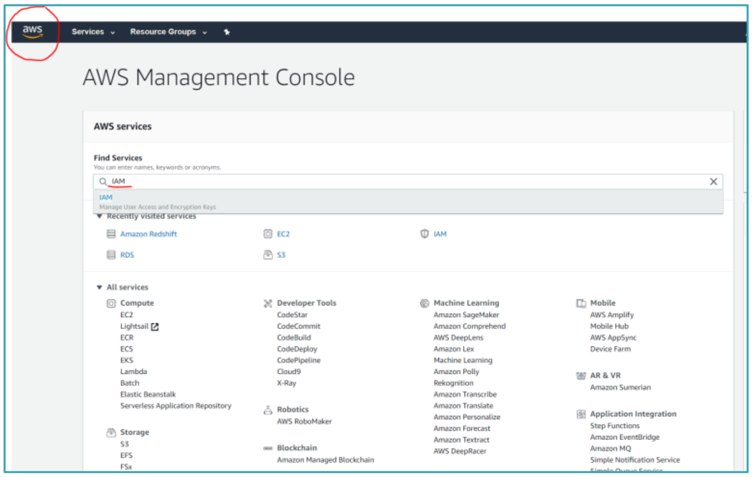
For creating Redshift cluster and querying the underlying dataset from S3, we will need to follow the below mentioned steps

A. Add access roles to access Redshift
B. Add IAM policy for Redshift query editor

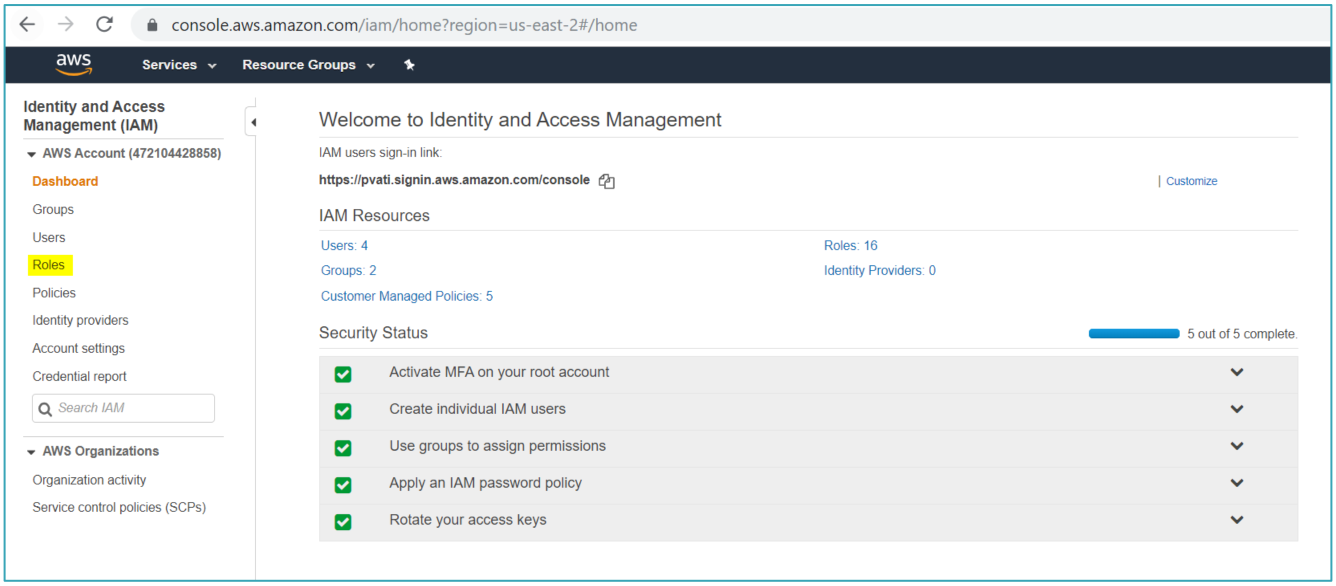
C. Create Redshift cluster
D. Execute sample query using query editor for verifying the install

A. Add access roles to access Redshift

1. Go to AWS services and click on IAM Console



2. Once in IAM dashboard, In the navigation pane, choose **Roles**



Welcome to Identity and Access Management

IAM users sign-in link:

https://pvati.signin.aws.amazon.com/console

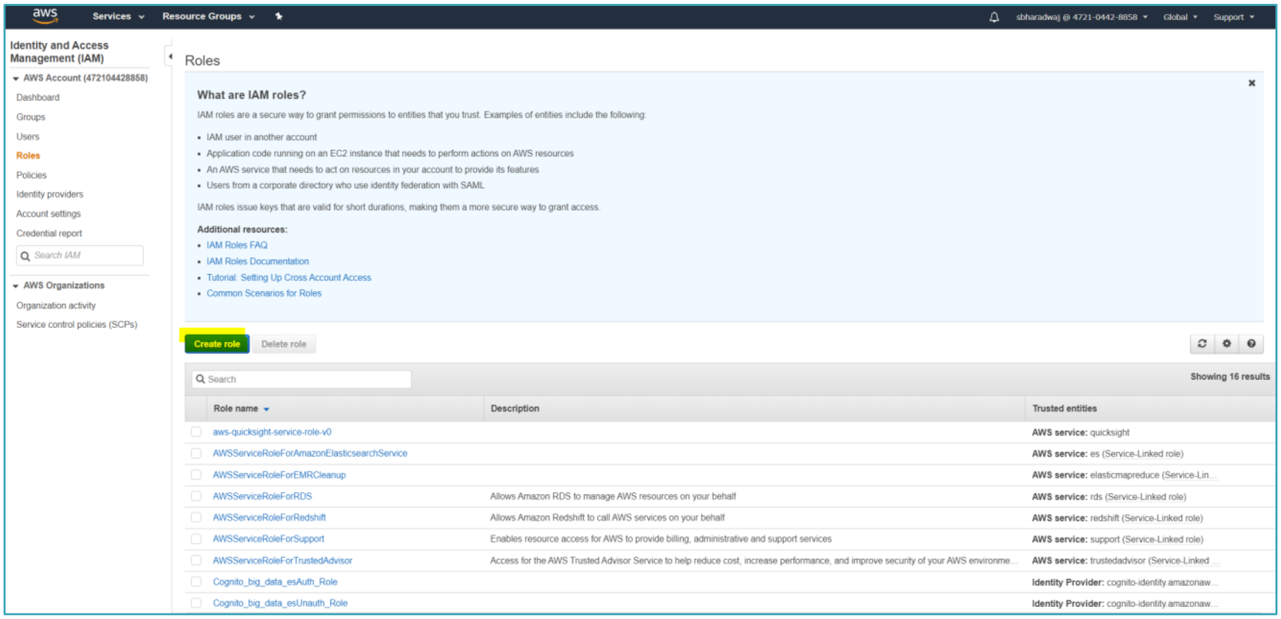
IAM Resources

Users: 4	Roles: 16
Groups: 2	Identity Providers: 0
Customer Managed Policies: 5	

Security Status — 5 out of 5 complete.

- ✓ Activate MFA on your root account
- ✓ Create individual IAM users
- ✓ Use groups to assign permissions
- ✓ Apply an IAM password policy
- ✓ Rotate your access keys

3. Choose **Create Role**



Roles

What are IAM roles?

IAM roles are a secure way to grant permissions to entities that you trust. Examples of entities include the following:

- IAM user in another account
- Application code running on an EC2 instance that needs to perform actions on AWS resources
- An AWS service that needs to act on resources in your account to provide its features
- Users from a corporate directory who use identity federation with SAML

IAM roles issue keys that are valid for short durations, making them a more secure way to grant access.

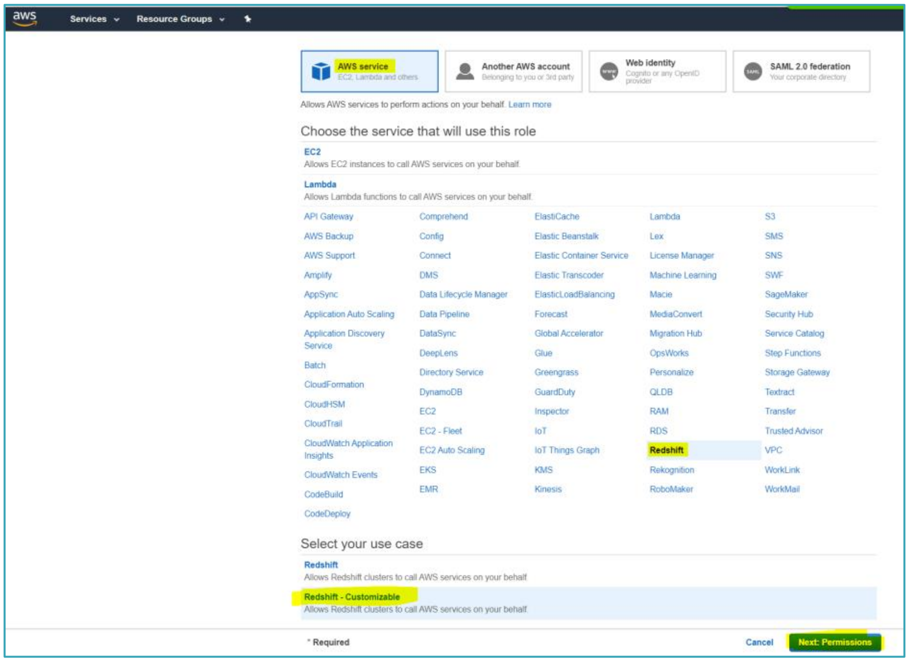
Additional resources:

- IAM Roles FAQ
- IAM Roles Documentation
- Tutorial: Setting Up Cross Account Access
- Common Scenarios for Roles

Showing 16 results

Role name	Description	Trusted entities
aws-quicksight-service-role-v0		**AWS service:** quicksight
AWSServiceRoleForAmazonElasticsearchService		**AWS service:** es (Service-Linked role)
AWSServiceRoleForEMRCleanup		**AWS service:** elasticmapreduce (Service-Lin...
AWSServiceRoleForRDS	Allows Amazon RDS to manage AWS resources on your behalf	**AWS service:** rds (Service-Linked role)
AWSServiceRoleForRedshift	Allows Amazon Redshift to call AWS services on your behalf	**AWS service:** redshift (Service-Linked role)
AWSServiceRoleForSupport	Enables resource access for AWS to provide billing, administrative and support services	**AWS service:** support (Service-Linked role)
AWSServiceRoleForTrustedAdvisor	Access for the AWS Trusted Advisor Service to help reduce cost, increase performance, and improve security of your AWS environme...	**AWS service:** trustedadvisor (Service-Linked ...
Cognito_big_data_esAuth_Role		**Identity Provider:** cognito-identity.amazonaw...
Cognito_big_data_esUnauth_Role		**Identity Provider:** cognito-identity.amazonaw...

4. Choose **AWS service**, and then choose **Redshift.** Under **Select your use case**, choose **Redshift - Customizable** and then choose **Next: Permissions**.



Allows AWS services to perform actions on your behalf. Learn more

Choose the service that will use this role

EC2
Allows EC2 instances to call AWS services on your behalf.

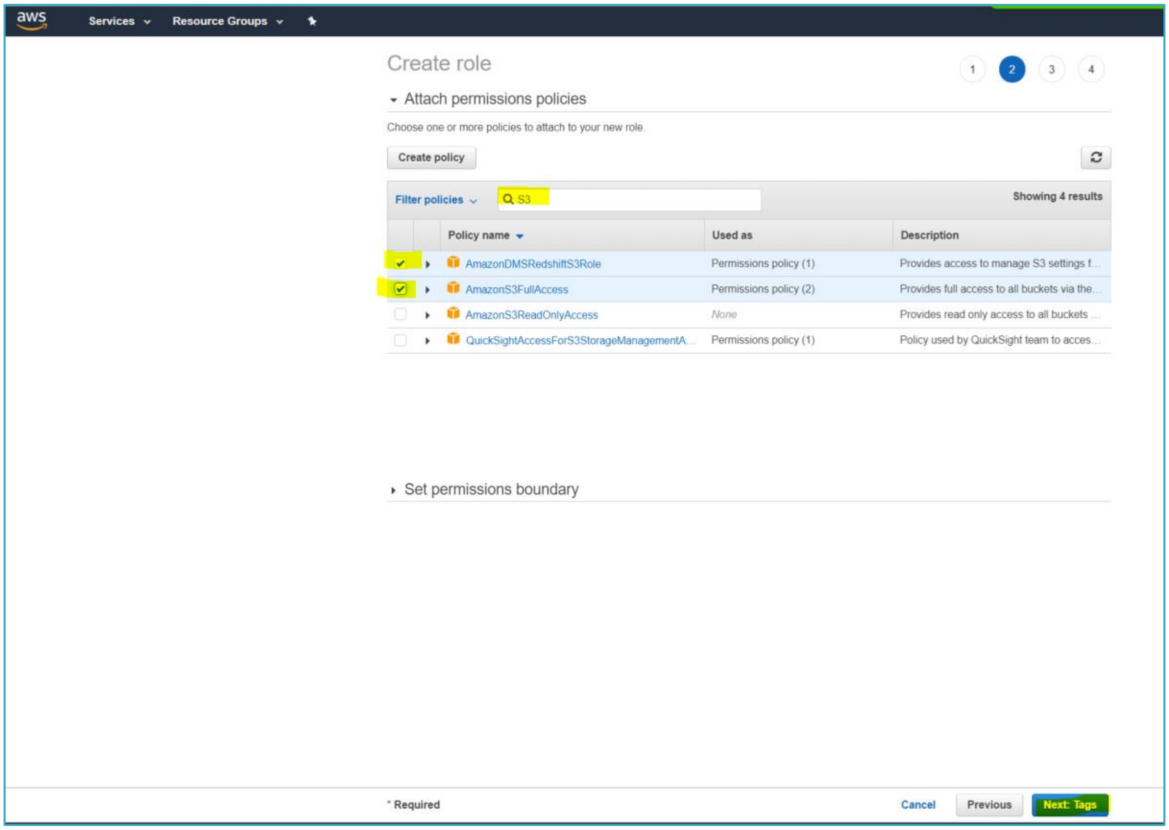
Lambda
Allows Lambda functions to call AWS services on your behalf.

Select your use case

Redshift
Allows Redshift clusters to call AWS services on your behalf

Redshift - Customizable
Allows Redshift clusters to call AWS services on your behalf

5. The **Attach permissions policy** page appears. Search for S3 policies & select AmazonDMSRedshiftS3Role & AmazonS3FullAccess & then Click **Next: Tags**



Create role

1 2 3 4

Attach permissions policies

Choose one or more policies to attach to your new role.

Create policy

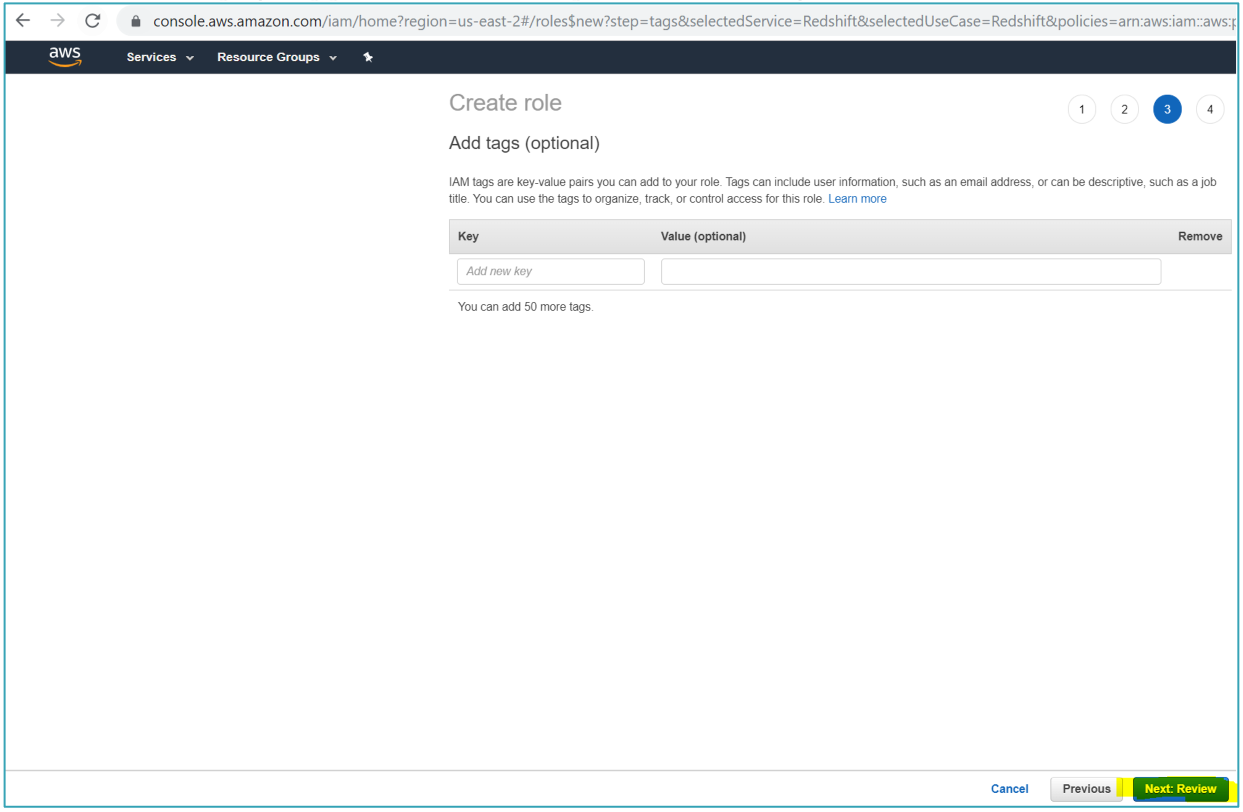
Filter policies S3 Showing 4 results

		Policy name	Used as	Description
☑	▸	AmazonDMSRedshiftS3Role	Permissions policy (1)	Provides access to manage S3 settings f...
☑	▸	AmazonS3FullAccess	Permissions policy (2)	Provides full access to all buckets via the...
□	▸	AmazonS3ReadOnlyAccess	None	Provides read only access to all buckets ...
□	▸	QuickSightAccessForS3StorageManagementA...	Permissions policy (1)	Policy used by QuickSight team to acces...

Set permissions boundary

* Required

6. The **Add tags** page appears. You can optionally add tags. Choose **Next: Review.**



console.aws.amazon.com/iam/home?region=us-east-2#/roles$new?step=tags&selectedService=Redshift&selectedUseCase=Redshift&policies=arn:aws:iam::aws:p

Create role

1 2 3 4

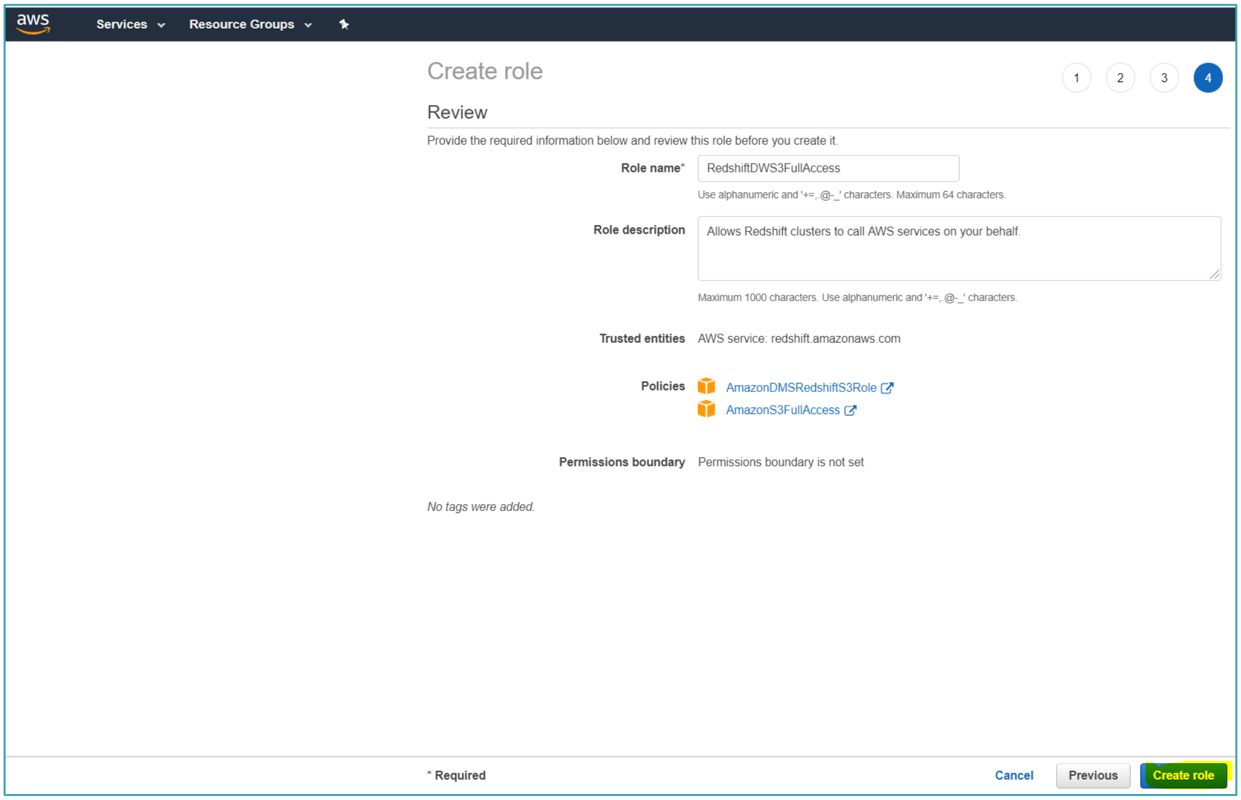
Add tags (optional)

IAM tags are key-value pairs you can add to your role. Tags can include user information, such as an email address, or can be descriptive, such as a job title. You can use the tags to organize, track, or control access for this role. Learn more

Key	Value (optional)	Remove
Add new key		

You can add 50 more tags.

7. For **Role name**, type a name for your role, for example **`RedshiftDWS3FullAccess`.** Choose **Create role**.



Create role

Review

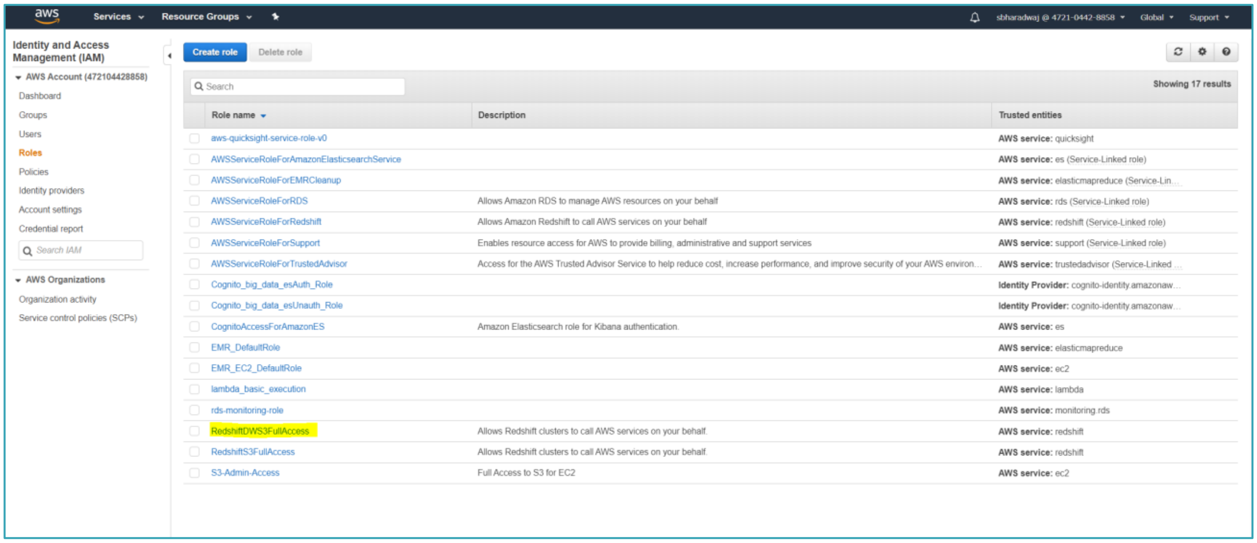
Provide the required information below and review this role before you create it.

Role name*	RedshiftDWS3FullAccess Use alphanumeric and '+=,.@-_' characters. Maximum 64 characters.
Role description	Allows Redshift clusters to call AWS services on your behalf. Maximum 1000 characters. Use alphanumeric and '+=,.@-_' characters.
Trusted entities	AWS service: redshift.amazonaws.com
Policies	AmazonDMSRedshiftS3Role AmazonS3FullAccess
Permissions boundary	Permissions boundary is not set

No tags were added.

* Required

8. Confirm, New Role is successfully added.

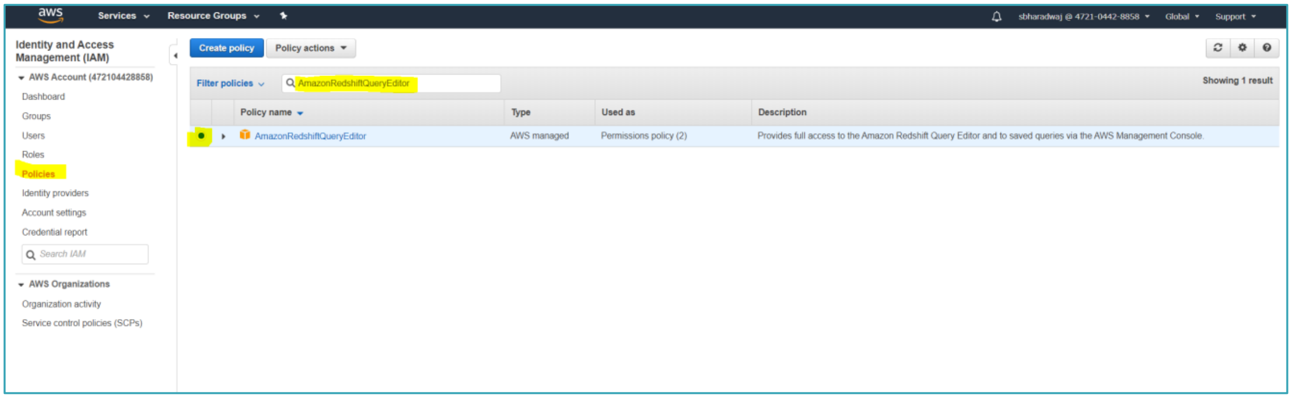


Showing 17 results

Role name	Description	Trusted entities
aws-quicksight-service-role-v0		**AWS service:** quicksight
AWSServiceRoleForAmazonElasticsearchService		**AWS service:** es (Service-Linked role)
AWSServiceRoleForEMRCleanup		**AWS service:** elasticmapreduce (Service-Lin...
AWSServiceRoleForRDS	Allows Amazon RDS to manage AWS resources on your behalf	**AWS service:** rds (Service-Linked role)
AWSServiceRoleForRedshift	Allows Amazon Redshift to call AWS services on your behalf	**AWS service:** redshift (Service-Linked role)
AWSServiceRoleForSupport	Enables resource access for AWS to provide billing, administrative and support services	**AWS service:** support (Service-Linked role)
AWSServiceRoleForTrustedAdvisor	Access for the AWS Trusted Advisor Service to help reduce cost, increase performance, and improve security of your AWS environ...	**AWS service:** trustedadvisor (Service-Linked ...
Cognito_big_data_esAuth_Role		**Identity Provider:** cognito-identity.amazonaw...
Cognito_big_data_esUnauth_Role		**Identity Provider:** cognito-identity.amazonaw...
CognitoAccessForAmazonES	Amazon Elasticsearch role for Kibana authentication.	**AWS service:** es
EMR_DefaultRole		**AWS service:** elasticmapreduce
EMR_EC2_DefaultRole		**AWS service:** ec2
lambda_basic_execution		**AWS service:** lambda
rds-monitoring-role		**AWS service:** monitoring.rds
RedshiftDWS3FullAccess	Allows Redshift clusters to call AWS services on your behalf.	**AWS service:** redshift
RedshiftS3FullAccess	Allows Redshift clusters to call AWS services on your behalf.	**AWS service:** redshift
S3-Admin-Access	Full Access to S3 for EC2	**AWS service:** ec2

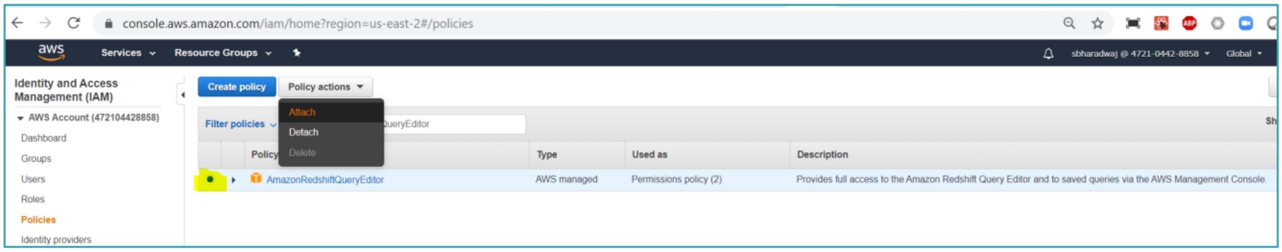
B. Add IAM policy for Redshift Query Editor

1. In the navigation menu, click on policies and Search for "AmazonRedshiftQueryEditor" policy



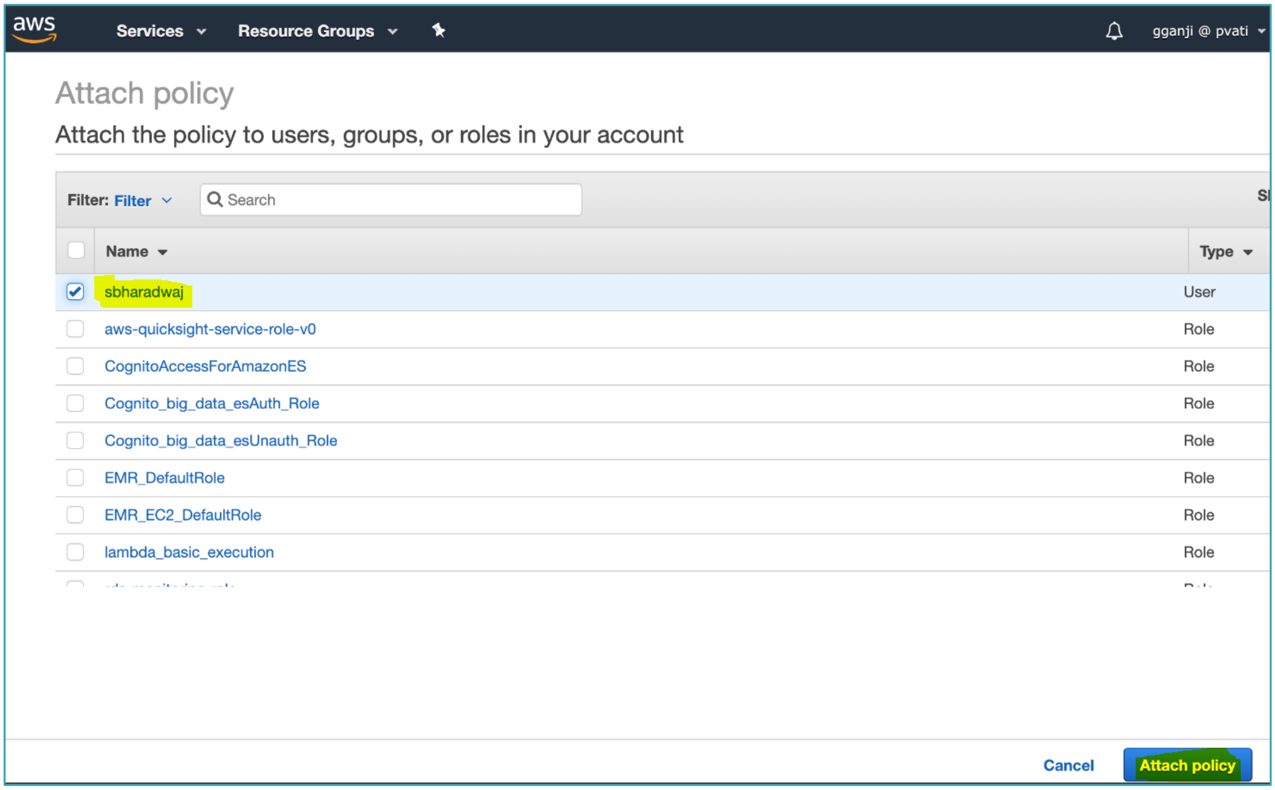
Policy name	Type	Used as	Description
AmazonRedshiftQueryEditor	AWS managed	Permissions policy (2)	Provides full access to the Amazon Redshift Query Editor and to saved queries via the AWS Management Console.

2. Select “AmazonRedshiftQueryEditor” policy & Click on “**Policy actions**” & select **Attach**



Policy	Type	Used as	Description
AmazonRedshiftQueryEditor	AWS managed	Permissions policy (2)	Provides full access to the Amazon Redshift Query Editor and to saved queries via the AWS Management Console.

3. In the Attach policy window, select the user ids & click **Attach policy**

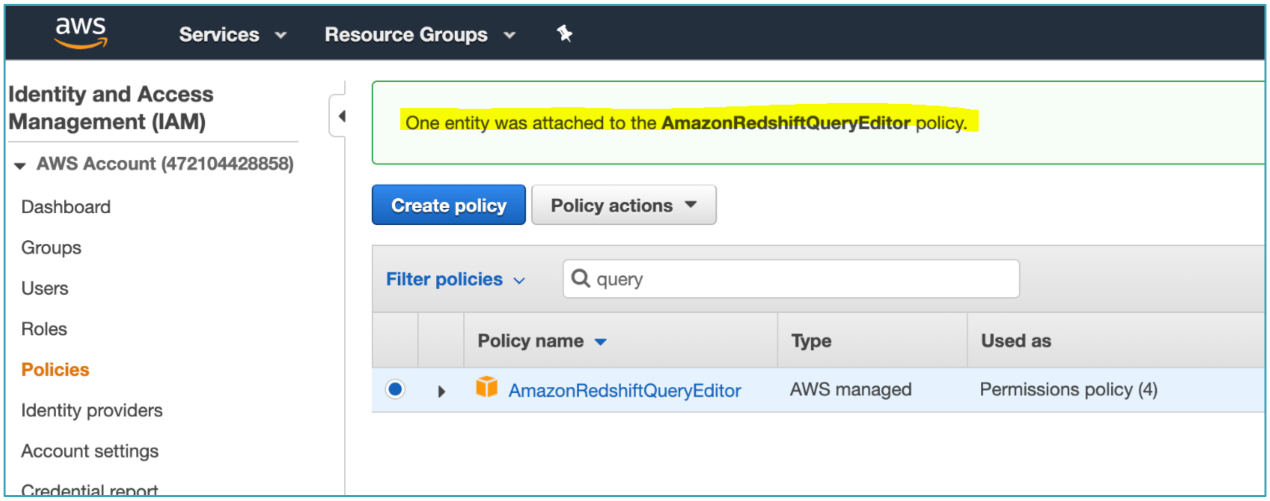


Attach policy

Attach the policy to users, groups, or roles in your account

	Name	Type
☑	sbharadwaj	User
□	aws-quicksight-service-role-v0	Role
□	CognitoAccessForAmazonES	Role
□	Cognito_big_data_esAuth_Role	Role
□	Cognito_big_data_esUnauth_Role	Role
□	EMR_DefaultRole	Role
□	EMR_EC2_DefaultRole	Role
□	lambda_basic_execution	Role

4. Confirm the policy attachment to user

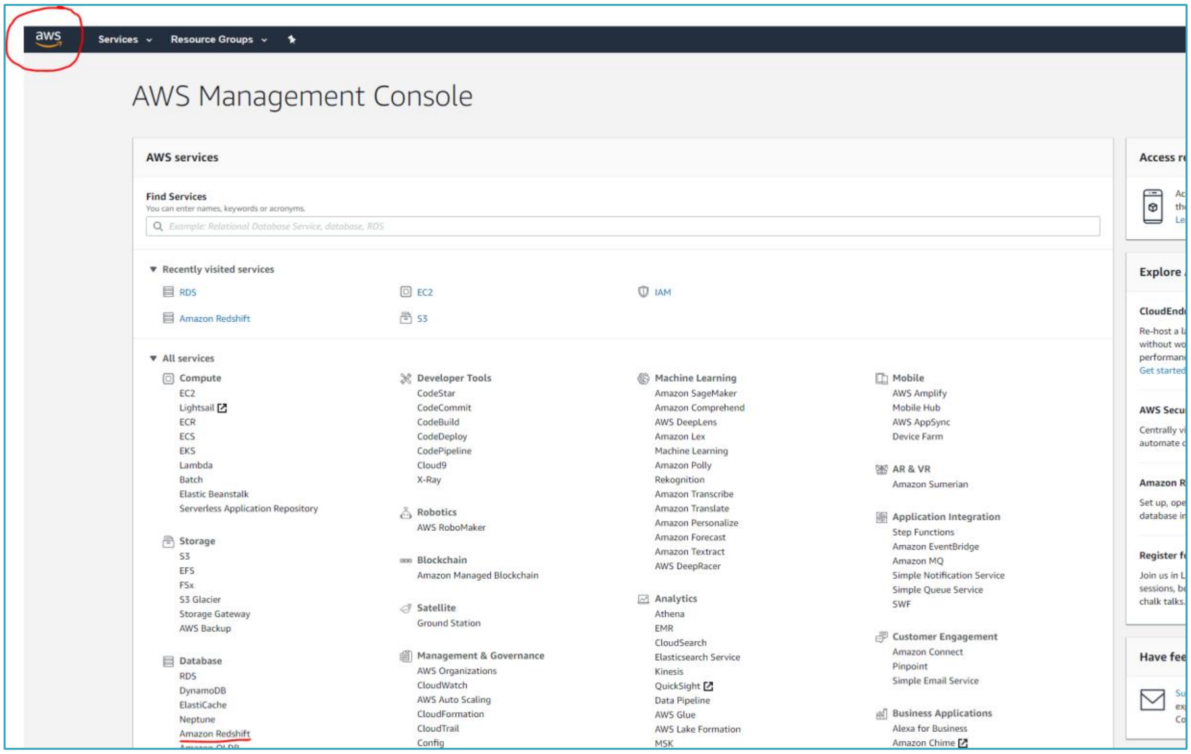


One entity was attached to the **AmazonRedshiftQueryEditor** policy.

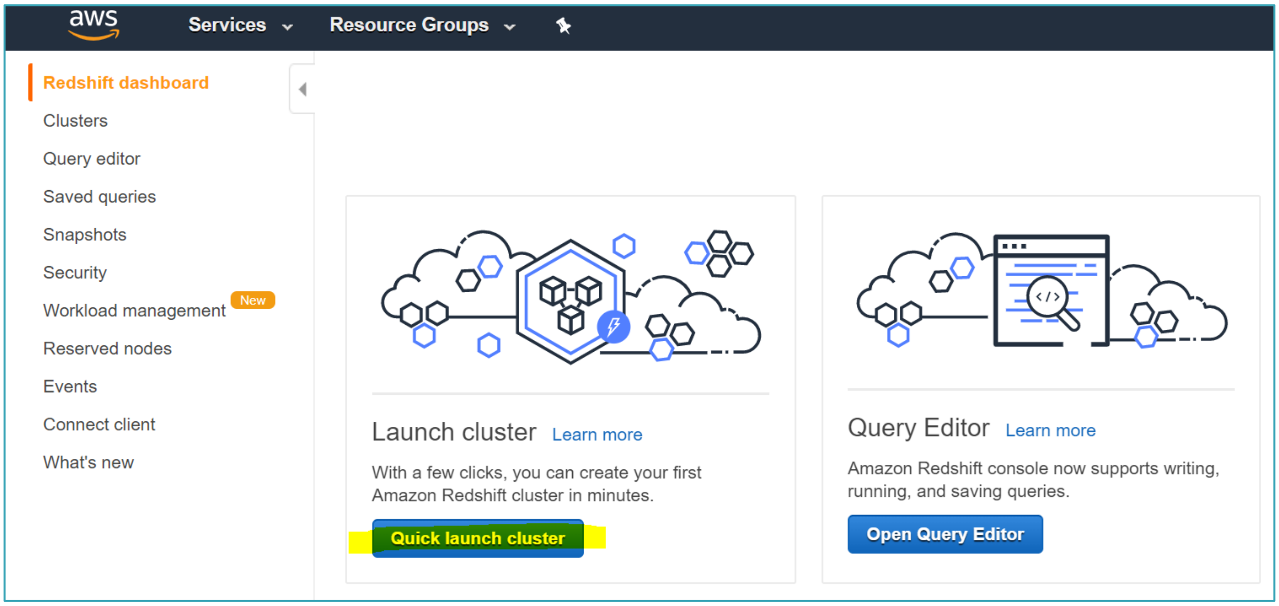
		Policy name	Type	Used as
●	▸	AmazonRedshiftQueryEditor	AWS managed	Permissions policy (4)

C. Create Redshift Cluster

1. Go to AWS services and click on Amazon Redshift (Datawarehouse)



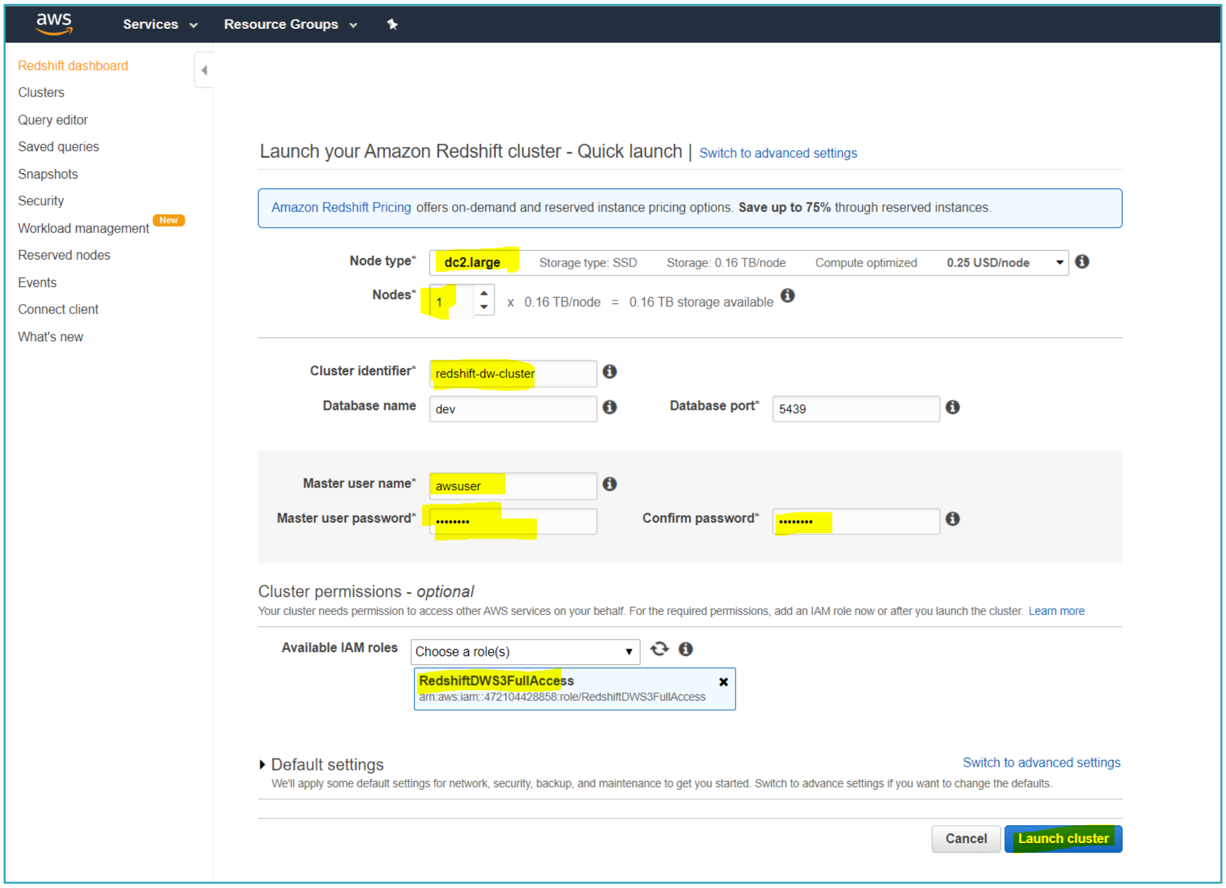
2. Click on **Quick launch cluster**



With a few clicks, you can create your first Amazon Redshift cluster in minutes.

Amazon Redshift console now supports writing, running, and saving queries.

3. Provide the details as shown below. Note that this will only add 1 node/machine in the cluster. If you need more than one update the number of nodes accordingly. Select the role that was added in previous steps & click **Launch cluster.** Choose password as Root1234 or something simple.



Launch your Amazon Redshift cluster - Quick launch | Switch to advanced settings

Amazon Redshift Pricing offers on-demand and reserved instance pricing options. **Save up to 75%** through reserved instances.

Node type* dc2.large Storage type: SSD Storage: 0.16 TB/node Compute optimized 0.25 USD/node

Nodes* 1 x 0.16 TB/node = 0.16 TB storage available

Cluster identifier* redshift-dw-cluster

Database name dev

Database port* 5439

Master user name* awsuser

Master user password* ••••••••

Confirm password* ••••••••

Cluster permissions - *optional*

Your cluster needs permission to access other AWS services on your behalf. For the required permissions, add an IAM role now or after you launch the cluster. Learn more

Available IAM roles Choose a role(s)

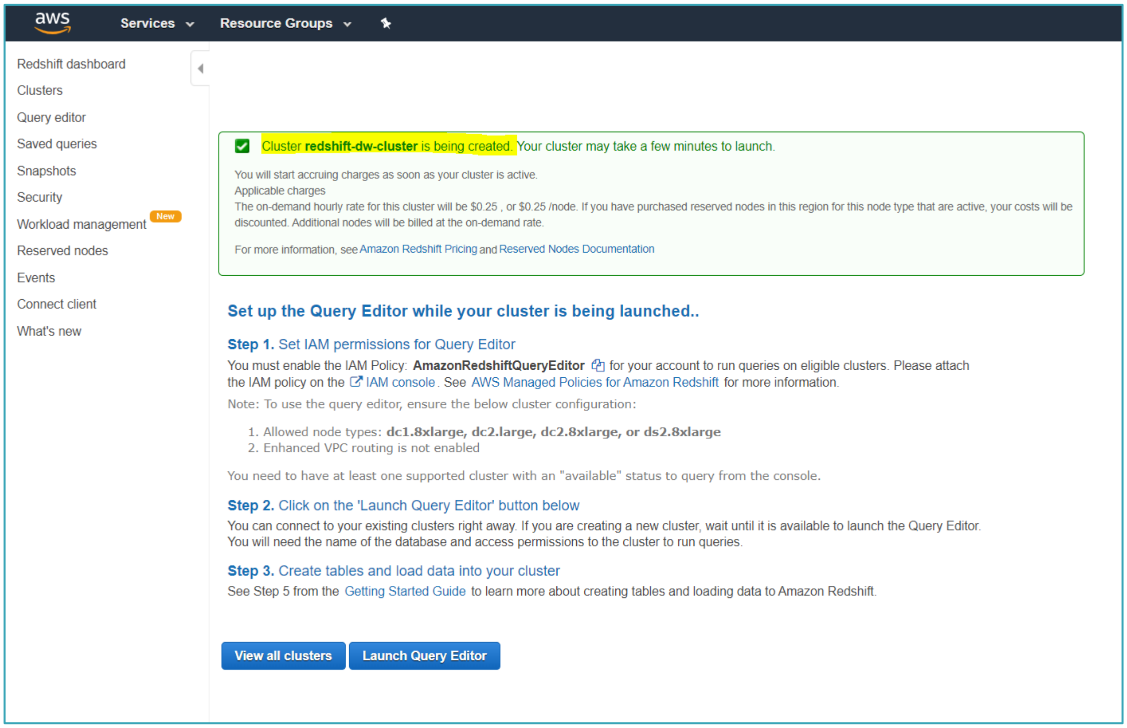
RedshiftDWS3FullAccess
arn:aws:iam::472104428858:role/RedshiftDWS3FullAccess

Default settings

Switch to advanced settings

We'll apply some default settings for network, security, backup, and maintenance to get you started. Switch to advance settings if you want to change the defaults.

4. Confirm the cluster has been launched successfully.



☑ Cluster **redshift-dw-cluster** is being created. Your cluster may take a few minutes to launch.

You will start accruing charges as soon as your cluster is active.
Applicable charges
The on-demand hourly rate for this cluster will be $0.25 , or $0.25 /node. If you have purchased reserved nodes in this region for this node type that are active, your costs will be discounted. Additional nodes will be billed at the on-demand rate.

For more information, see Amazon Redshift Pricing and Reserved Nodes Documentation

Set up the Query Editor while your cluster is being launched..

Step 1. Set IAM permissions for Query Editor

You must enable the IAM Policy: **AmazonRedshiftQueryEditor** for your account to run queries on eligible clusters. Please attach the IAM policy on the IAM console. See AWS Managed Policies for Amazon Redshift for more information.

Note: To use the query editor, ensure the below cluster configuration:

1. Allowed node types: **dc1.8xlarge, dc2.large, dc2.8xlarge, or ds2.8xlarge**
2. Enhanced VPC routing is not enabled

You need to have at least one supported cluster with an "available" status to query from the console.

Step 2. Click on the 'Launch Query Editor' button below

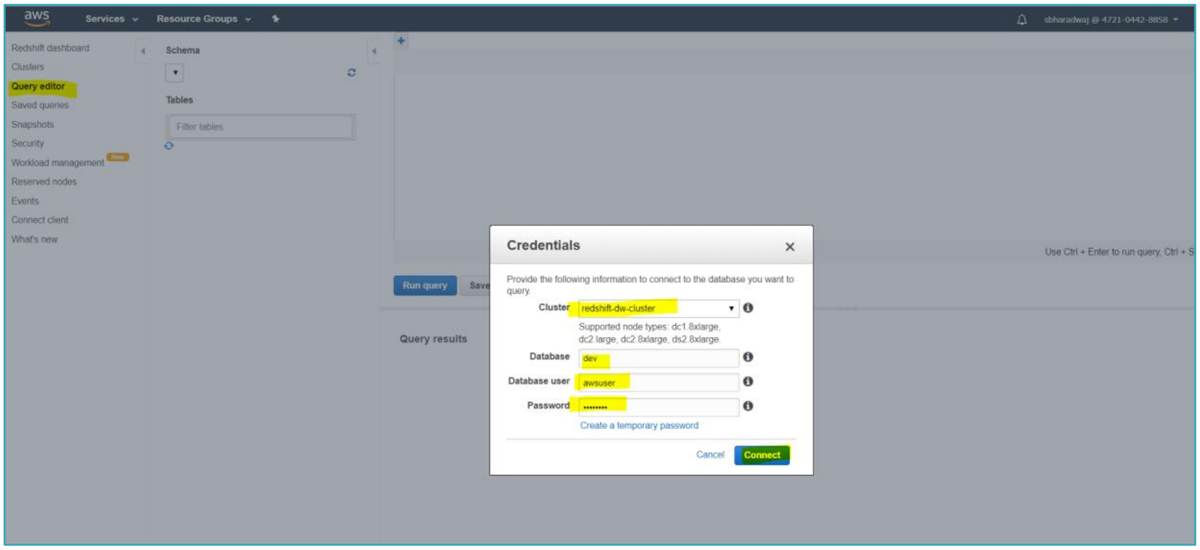
You can connect to your existing clusters right away. If you are creating a new cluster, wait until it is available to launch the Query Editor. You will need the name of the database and access permissions to the cluster to run queries.

Step 3. Create tables and load data into your cluster

See Step 5 from the Getting Started Guide to learn more about creating tables and loading data to Amazon Redshift.

D. Query using Query Editor

1. Once the cluster gets created, click on **Open Query Editor** from the navigation menu



Credentials

Provide the following information to connect to the database you want to query.

Cluster: redshift-dw-cluster

Supported node types: dc1.8xlarge, dc2.large, dc2.8xlarge, ds2.8xlarge.

Database: dev

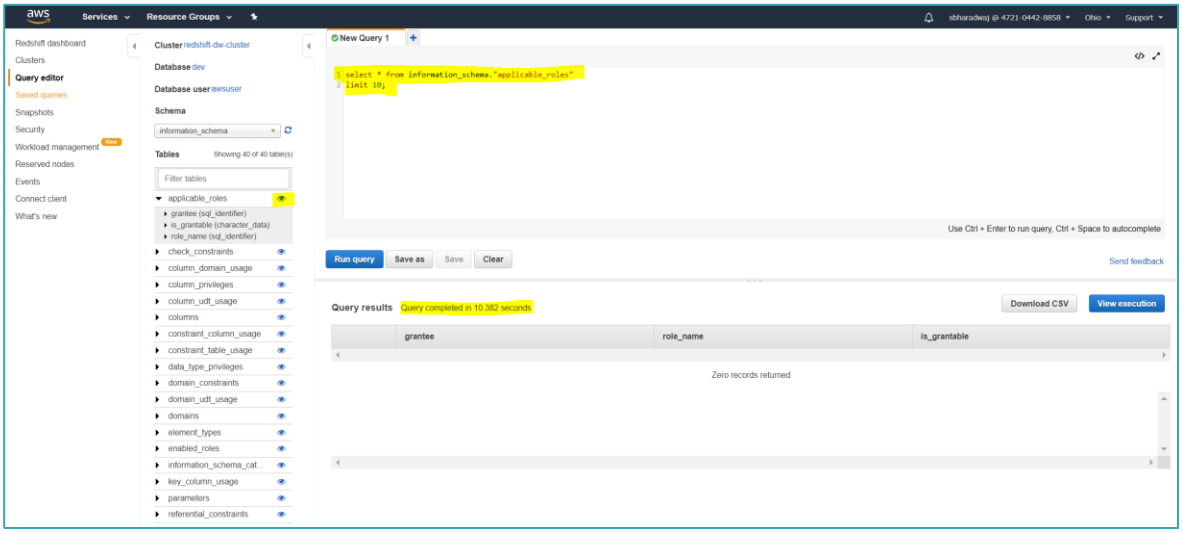
Database user: awsuser

Password: ••••••••

Create a temporary password

Cancel | Connect

2. Run sample query



Cluster redshift-dw-cluster

Database dev

Database user awsuser

Schema: information_schema

Tables — Showing 40 of 40 table(s)

- applicable_roles
  - grantee (sql_identifier)
  - is_grantable (character_data)
  - role_name (sql_identifier)
- check_constraints
- column_domain_usage
- column_privileges
- column_udt_usage
- columns
- constraint_column_usage
- constraint_table_usage
- data_type_privileges
- domain_constraints
- domain_udt_usage
- domains
- element_types
- enabled_roles
- information_schema_cat...
- key_column_usage
- parameters
- referential_constraints

```
select * from information_schema."applicable_roles"
limit 10;
```

Query results — Query completed in 10.382 seconds

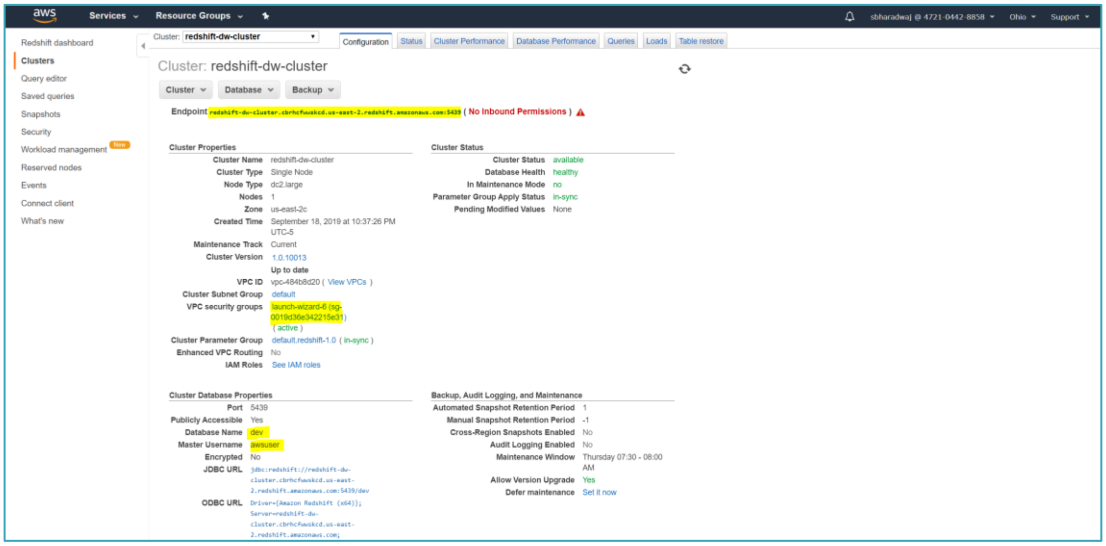
grantee	role_name	is_grantable

Zero records returned

Note: Amazon Redshift installation is now complete.

<u>CONNECT TABLEAU TO REDSHIFT</u>

1. Login to AWS console and have 5439 port added to your VPC security group. Copy the Endpoint {redshift-dw-cluster.cbrhcfwwskcd.us-east-2.redshift.amazonaws.com} which will be added to Tableau as server. Make a note of the Database Name and Master Username



Cluster: redshift-dw-cluster

Endpoint redshift-dw-cluster.cbrhcfwwskcd.us-east-2.redshift.amazonaws.com:5439 (No Inbound Permissions)

Cluster Properties

Cluster Name	redshift-dw-cluster
Cluster Type	Single Node
Node Type	dc2.large
Nodes	1
Zone	us-east-2c
Created Time	September 18, 2019 at 10:37:26 PM UTC-5
Maintenance Track	Current
Cluster Version	1.0.10013 Up to date
VPC ID	vpc-484b8d20 (View VPCs)
Cluster Subnet Group	default
VPC security groups	launch-wizard-6 (sg-0019d36e342215e31) (active)
Cluster Parameter Group	default.redshift-1.0 (in-sync)
Enhanced VPC Routing	No
IAM Roles	See IAM roles

Cluster Status

Cluster Status	available
Database Health	healthy
In Maintenance Mode	no
Parameter Group Apply Status	in-sync
Pending Modified Values	None

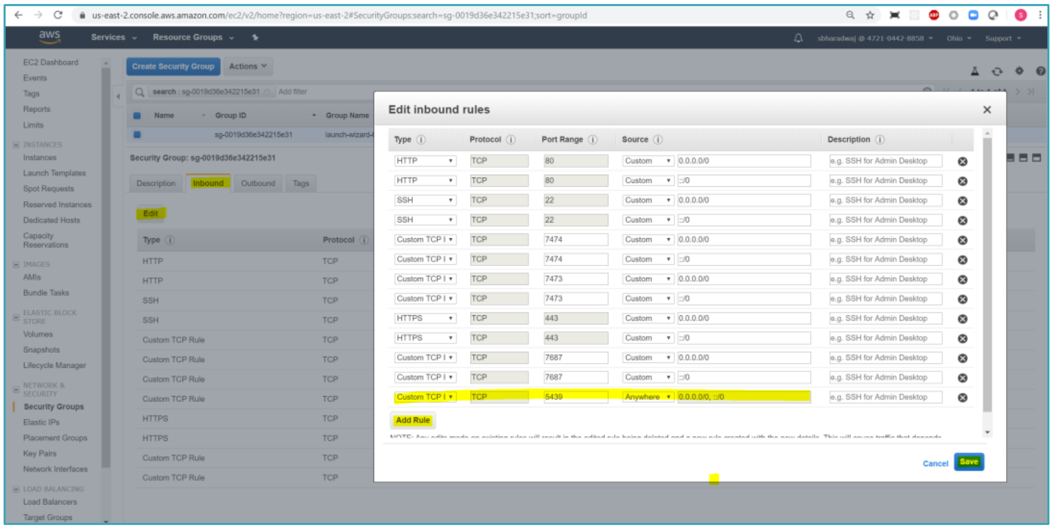
Cluster Database Properties

Port	5439
Publicly Accessible	Yes
Database Name	dev
Master Username	awsuser
Encrypted	No
JDBC URL	jdbc:redshift://redshift-dw-cluster.cbrhcfwwskcd.us-east-2.redshift.amazonaws.com:5439/dev
ODBC URL	Driver={Amazon Redshift (x64)}; Server=redshift-dw-cluster.cbrhcfwwskcd.us-east-2.redshift.amazonaws.com;

Backup, Audit Logging, and Maintenance

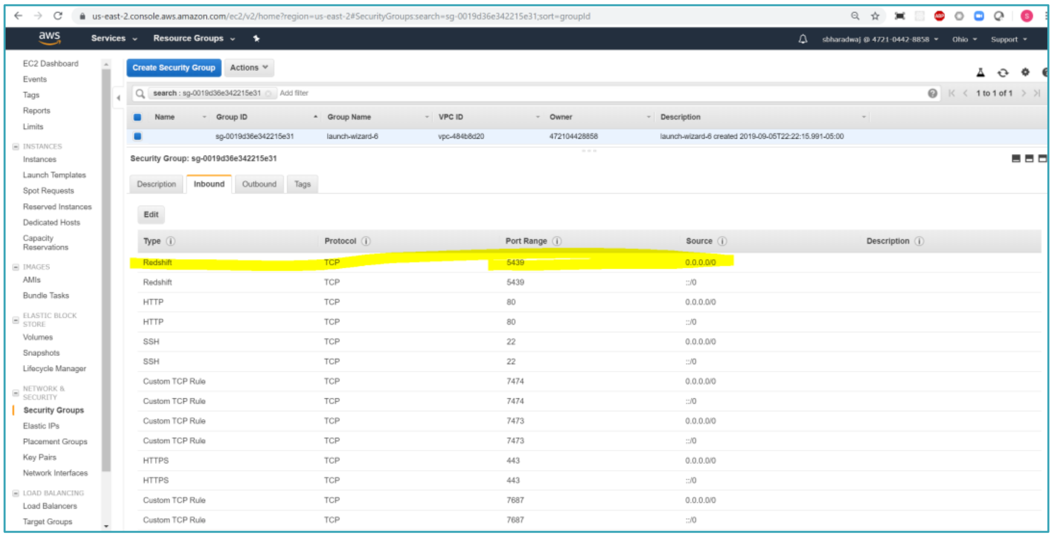
Automated Snapshot Retention Period	1
Manual Snapshot Retention Period	-1
Cross-Region Snapshots Enabled	No
Audit Logging Enabled	No
Maintenance Window	Thursday 07:30 - 08:00 AM
Allow Version Upgrade	Yes
Defer maintenance	Set it now

2. Click on the VPC Security Group and navigate to the Inbound tab and click on Edit and Add Rule and click Save


us-east-2.console.aws.amazon.com/ec2/v2/home?region=us-east-2#SecurityGroups:search=sg-0019d36e342215e31;sort=groupId
aws
Services
Resource Groups
sbharadwaj @ 4721-0442-8858
Ohio
Support
Create Security Group
Actions
Description
Inbound
Outbound
Tags
Edit
Add Rule
Cancel
Save

Edit inbound rules

Type	Protocol	Port Range	Source		Description
HTTP	TCP	80	Custom	0.0.0.0/0	e.g. SSH for Admin Desktop
HTTP	TCP	80	Custom	::/0	e.g. SSH for Admin Desktop
SSH	TCP	22	Custom	0.0.0.0/0	e.g. SSH for Admin Desktop
SSH	TCP	22	Custom	::/0	e.g. SSH for Admin Desktop
Custom TCP I	TCP	7474	Custom	0.0.0.0/0	e.g. SSH for Admin Desktop
Custom TCP I	TCP	7474	Custom	::/0	e.g. SSH for Admin Desktop
Custom TCP I	TCP	7473	Custom	0.0.0.0/0	e.g. SSH for Admin Desktop
Custom TCP I	TCP	7473	Custom	::/0	e.g. SSH for Admin Desktop
HTTPS	TCP	443	Custom	0.0.0.0/0	e.g. SSH for Admin Desktop
HTTPS	TCP	443	Custom	::/0	e.g. SSH for Admin Desktop
Custom TCP I	TCP	7687	Custom	0.0.0.0/0	e.g. SSH for Admin Desktop
Custom TCP I	TCP	7687	Custom	::/0	e.g. SSH for Admin Desktop
Custom TCP I	TCP	5439	Anywhere	0.0.0.0/0, ::/0	e.g. SSH for Admin Desktop

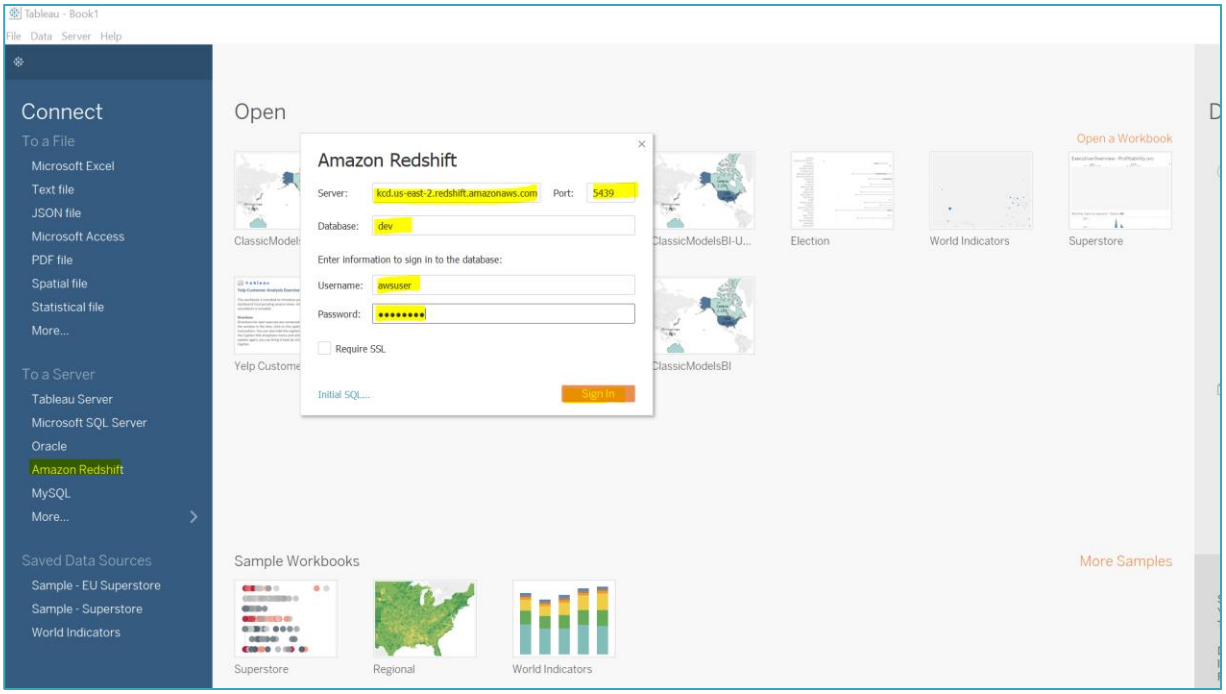


Name	Group ID	Group Name	VPC ID	Owner	Description
	sg-0019d36e342215e31	launch-wizard-6	vpc-484b8d20	472104428858	launch-wizard-6 created 2019-09-05T22:22:15.991-05:00

Security Group: sg-0019d36e342215e31

Type	Protocol	Port Range	Source	Description
Redshift	TCP	5439	0.0.0.0/0	
Redshift	TCP	5439	::/0	
HTTP	TCP	80	0.0.0.0/0	
HTTP	TCP	80	::/0	
SSH	TCP	22	0.0.0.0/0	
SSH	TCP	22	::/0	
Custom TCP Rule	TCP	7474	0.0.0.0/0	
Custom TCP Rule	TCP	7474	::/0	
Custom TCP Rule	TCP	7473	0.0.0.0/0	
Custom TCP Rule	TCP	7473	::/0	
HTTPS	TCP	443	0.0.0.0/0	
HTTPS	TCP	443	::/0	
Custom TCP Rule	TCP	7687	0.0.0.0/0	
Custom TCP Rule	TCP	7687	::/0	

3. Open Tableau click on 'Amazon Redshift' under server options. Add Server details to connect to AWS Redshift instance.



Amazon Redshift

Server: kcd.us-east-2.redshift.amazonaws.com Port: 5439

Database: dev

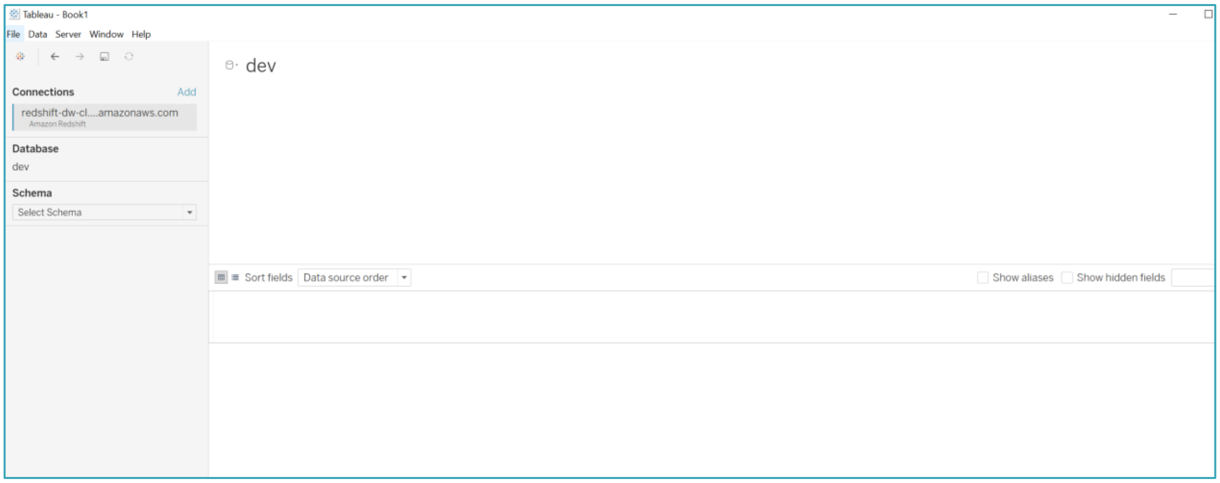
Enter information to sign in to the database:

Username: awsuser

Password: ●●●●●●●●

□ Require SSL

Initial SQL... Sign In



Connections: redshift-dw-cl....amazonaws.com (Amazon Redshift)

Database: dev

Schema: Select Schema

Tableau is now connected to Amazon Redshift.

End of Exercise 2.