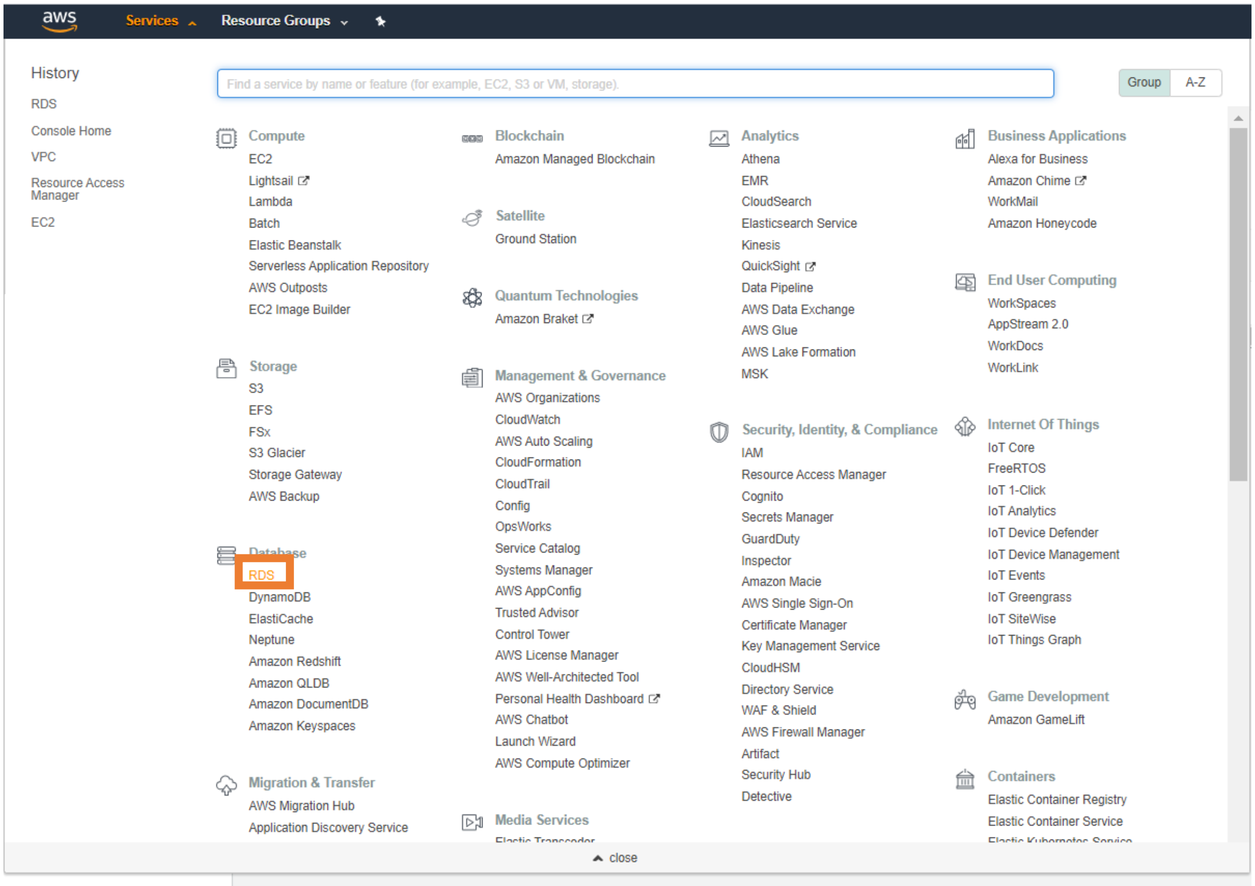
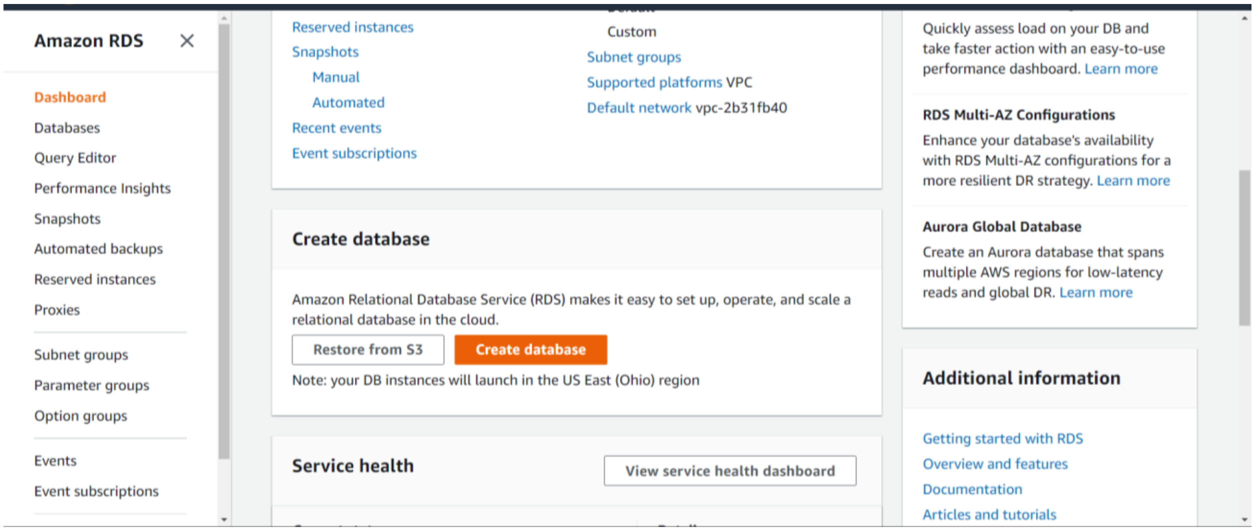
AWS Corporate Account RDS Instructions:

Spin up a Postgres RDS instance:

1. Sign in to your IAM user for revature-training.
2. Go to Services:



3. Select RDS.
4. On the next screen scroll down to *Create Database.*

5. 

Amazon RDS ✕

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

Subnet groups
Parameter groups
Option groups

Events
Event subscriptions

Reserved instances
Snapshots
Manual
Automated
Recent events
Event subscriptions

Custom
Subnet groups
Supported platforms VPC
Default network vpc-2b31fb40

Quickly assess load on your DB and take faster action with an easy-to-use performance dashboard. Learn more

RDS Multi-AZ Configurations
Enhance your database's availability with RDS Multi-AZ configurations for a more resilient DR strategy. Learn more

Aurora Global Database
Create an Aurora database that spans multiple AWS regions for low-latency reads and global DR. Learn more

Create database

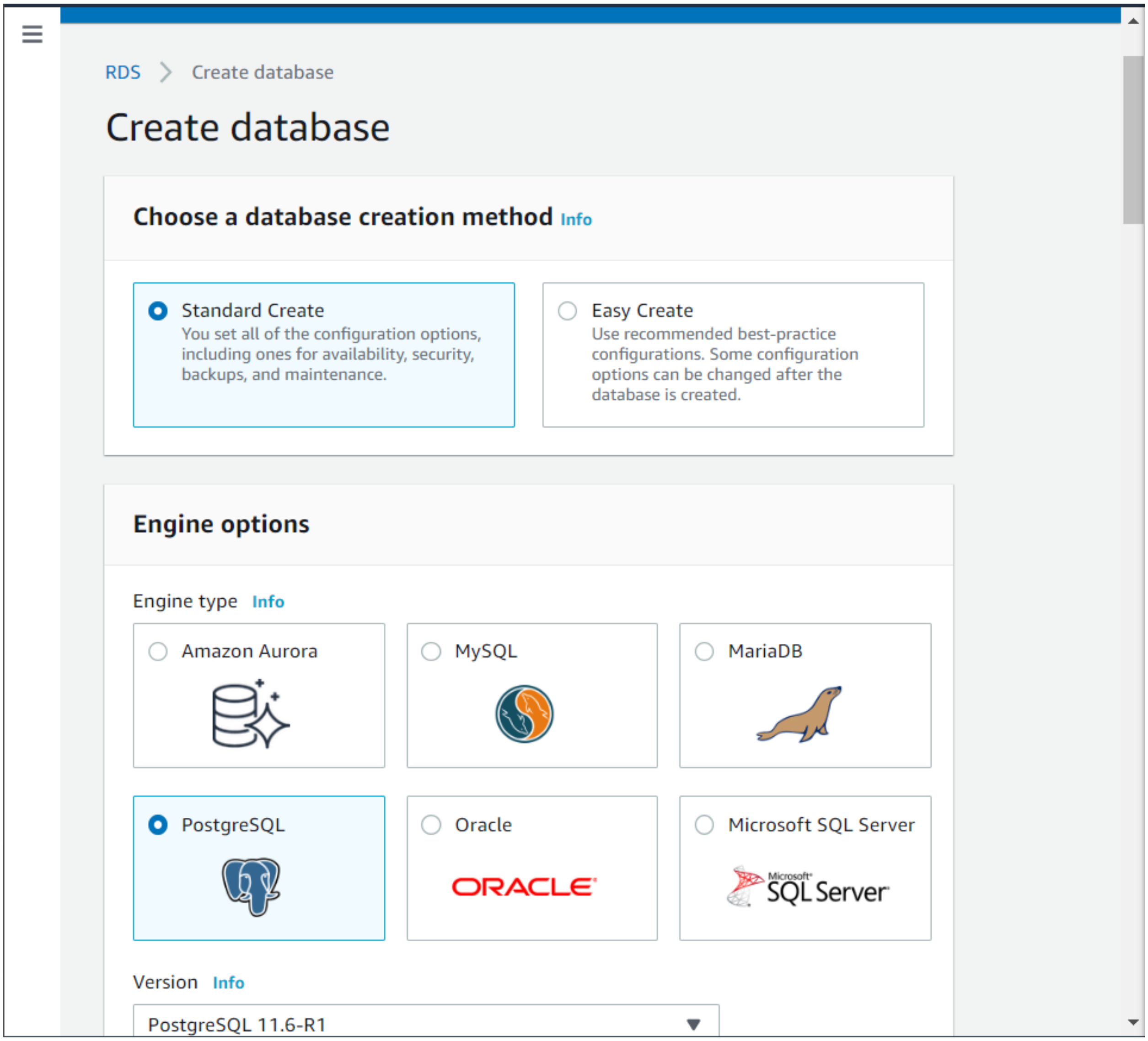
Amazon Relational Database Service (RDS) makes it easy to set up, operate, and scale a relational database in the cloud.

Note: your DB instances will launch in the US East (Ohio) region

Service health

Additional information

Getting started with RDS
Overview and features
Documentation
Articles and tutorials

6. 

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

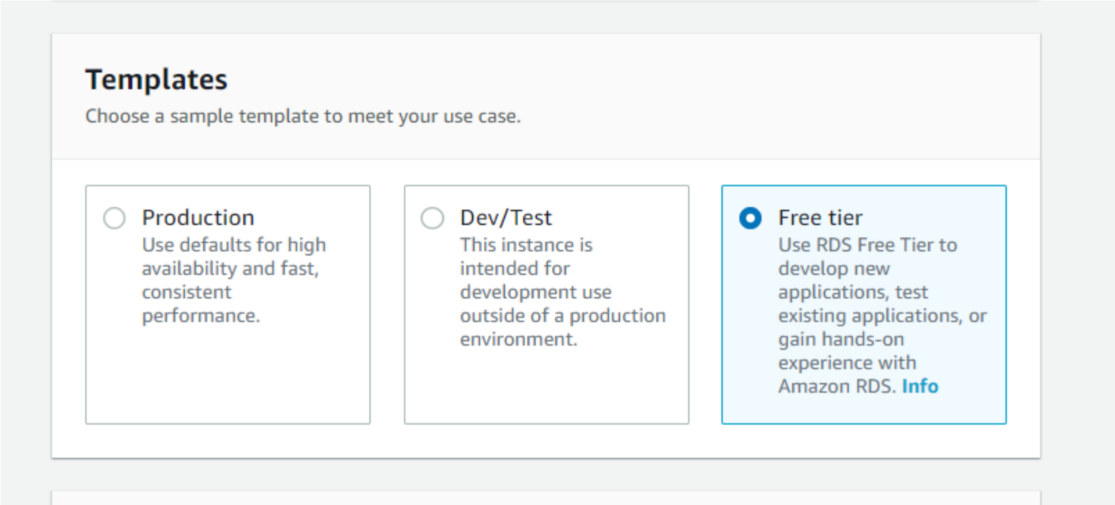
Engine type Info

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

Version Info

PostgreSQL 11.6-R1 ▼

7. Then select only enable free-tier options.



Templates

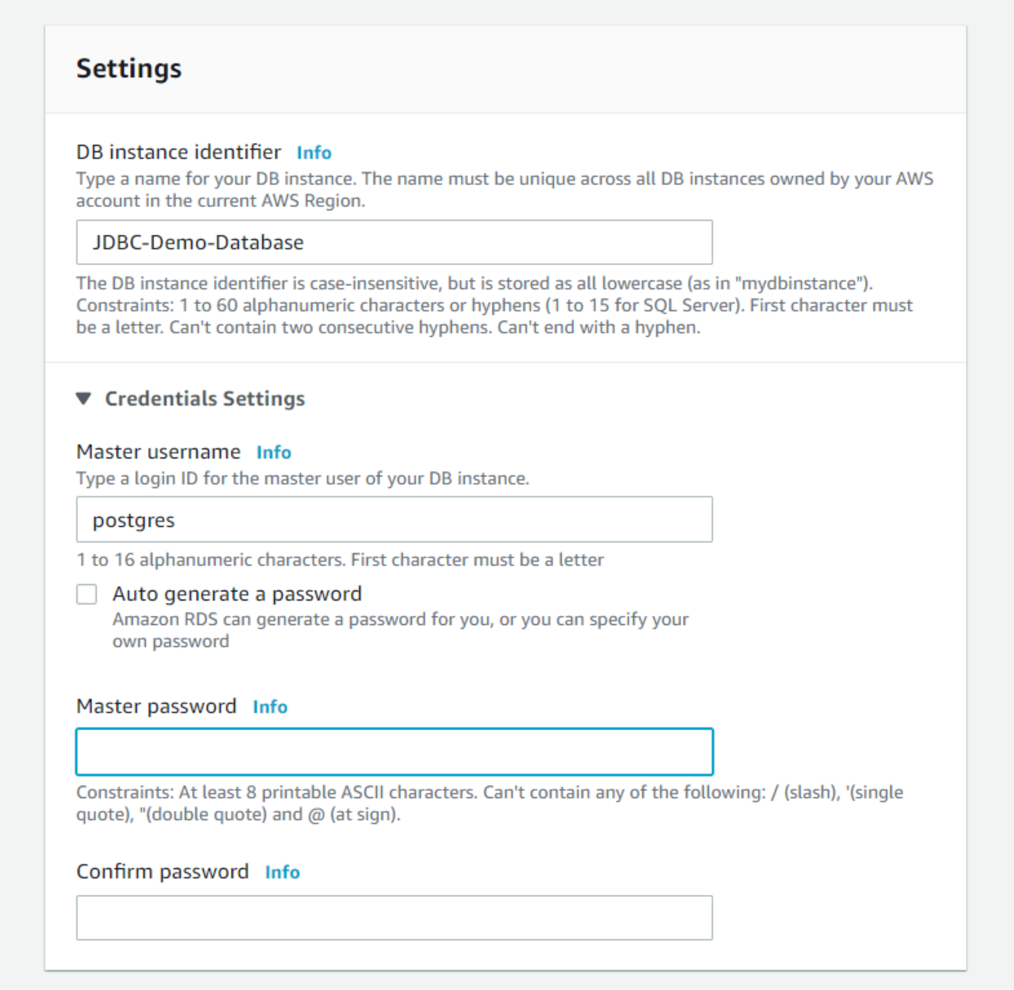
Choose a sample template to meet your use case.

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

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

● Free tier
Use RDS Free Tier to develop new applications, test existing applications, or gain hands-on experience with Amazon RDS. Info

8. Then decide on your DB instance's name and master credentials. **Be sure and remember this info.**



Settings

DB instance identifier Info

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.

JDBC-Demo-Database

The DB instance identifier is case-insensitive, but is stored as all lowercase (as in "mydbinstance"). Constraints: 1 to 60 alphanumeric characters or hyphens (1 to 15 for SQL Server). 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

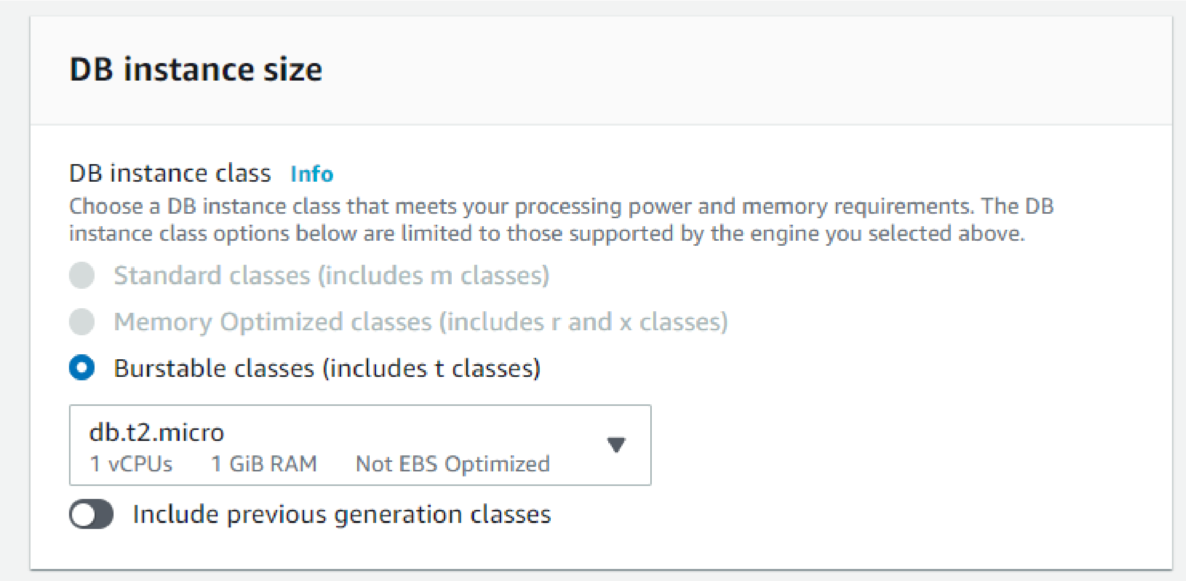
□ Auto generate a password
Amazon RDS can generate a password for you, or you can specify your own password

Master password Info

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

Confirm password Info

9. Leave defaults for the DB instance size- there is only one free tier option:



DB instance size

DB instance class

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.

○ Standard classes (includes m classes)

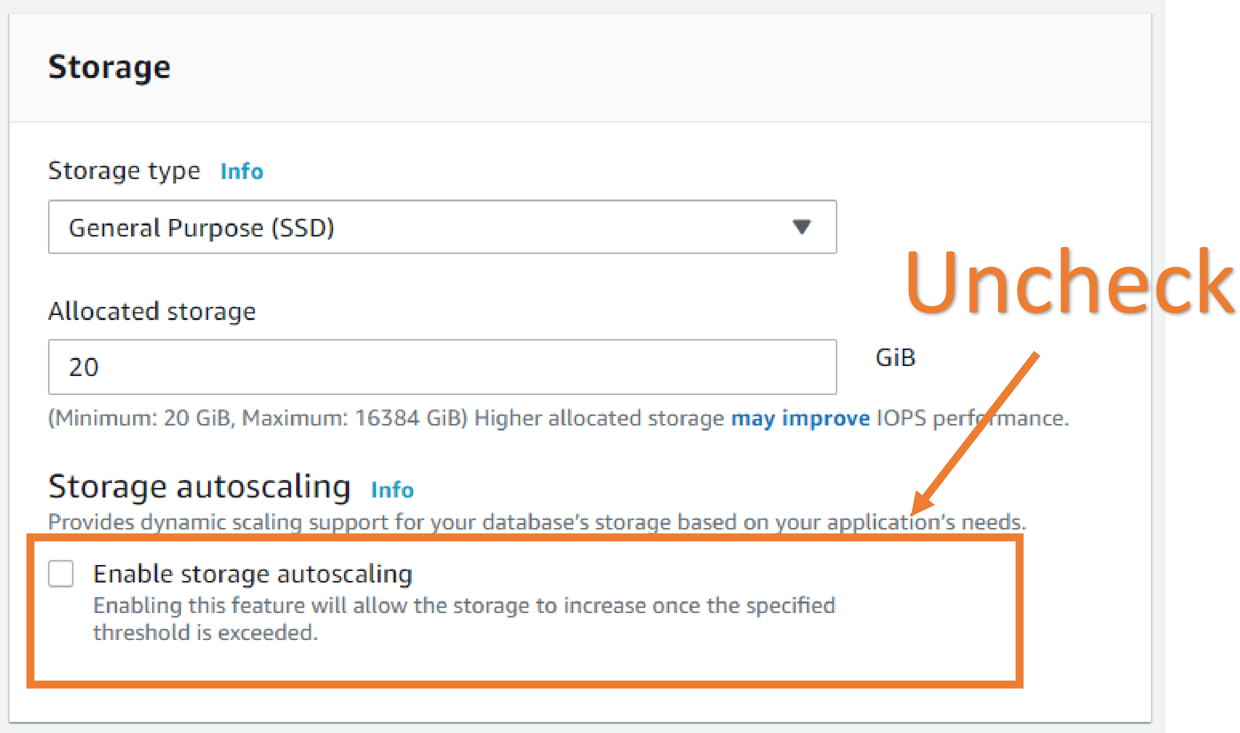
○ Memory Optimized classes (includes r and x classes)

● Burstable classes (includes t classes)

db.t2.micro
1 vCPUs 1 GiB RAM Not EBS Optimized ▼

Include previous generation classes

10. **This is important disable autoscaling! Uncheck the box:**



Storage

Storage type

General Purpose (SSD) ▼

Allocated storage

20 GiB

(Minimum: 20 GiB, Maximum: 16384 GiB) Higher allocated storage **may improve** IOPS performance.

Storage autoscaling

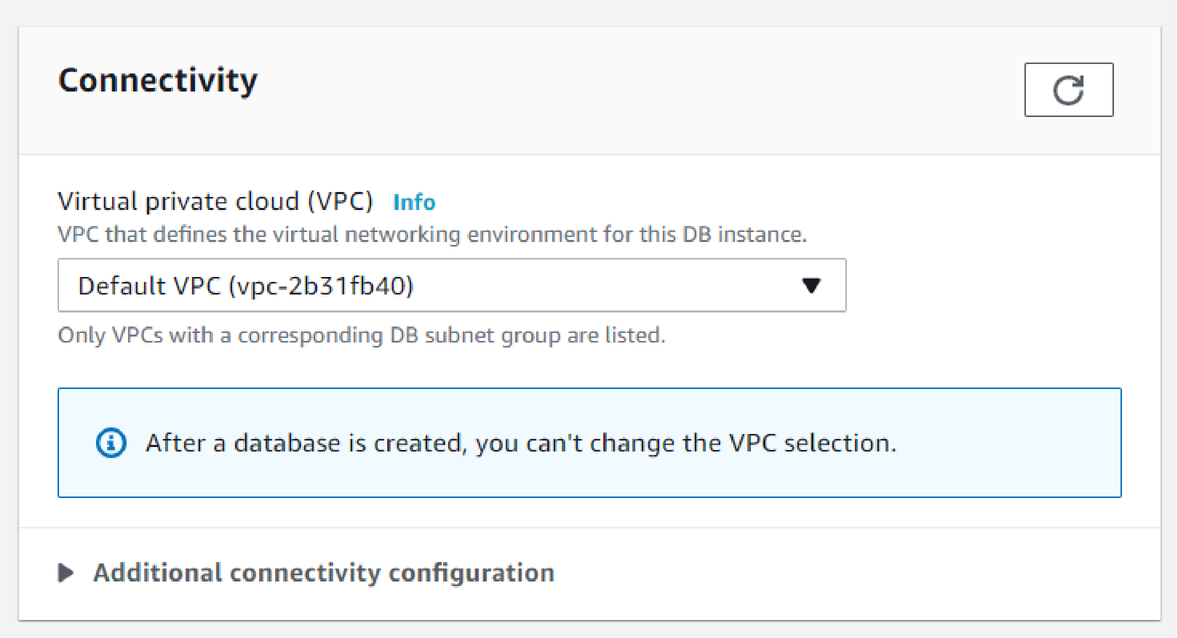
Provides dynamic scaling support for your database's storage based on your application's needs.

□ Enable storage autoscaling
Enabling this feature will allow the storage to increase once the specified threshold is exceeded.

Uncheck

11. **The Connectivity section will be a bit different than what you would do on a personal AWS.**

    a. **Leave Default VPC (vpc-someset of characters).**

b. 

Connectivity

Virtual private cloud (VPC) Info

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

Default VPC (vpc-2b31fb40) ▼

Only VPCs with a corresponding DB subnet group are listed.

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

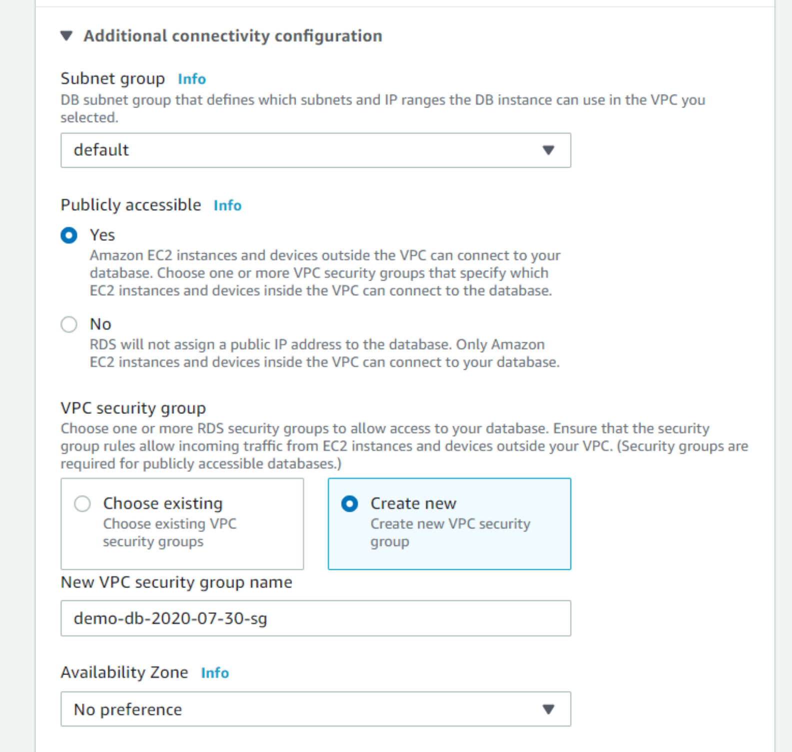
▶ Additional connectivity configuration

c. Then choose **Additional connectivity configuration…**

   i. Subnet group remains default.

   ii. Select **YES** for publicly accessible.

   iii. Then *Create new* VPC security group. And simply choose a unique name. You can leave the default port - 5432.



▼ 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

New VPC security group name

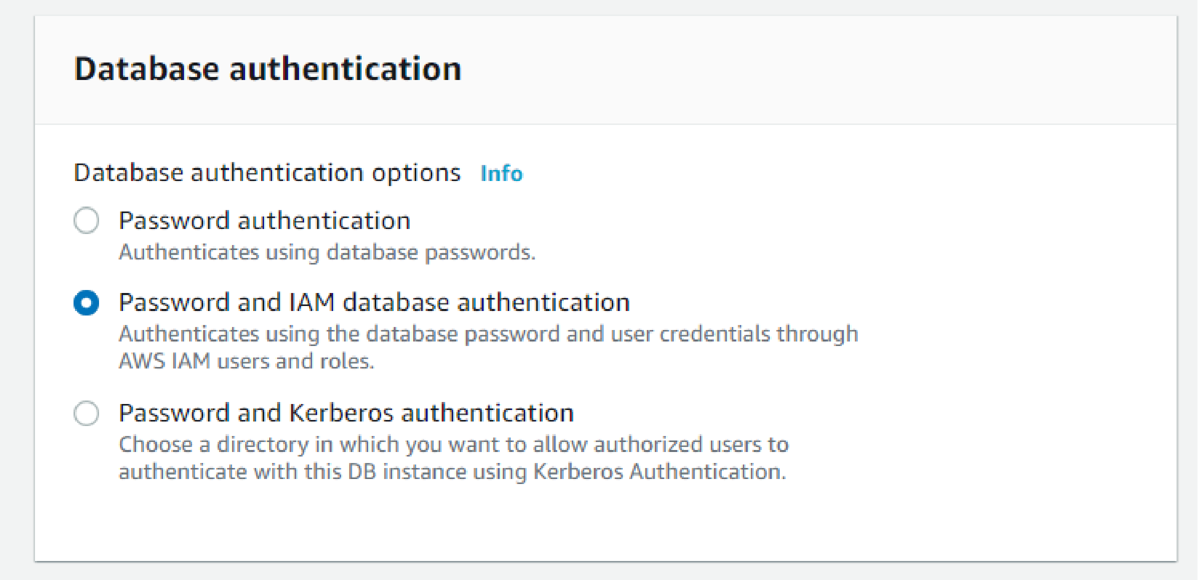
demo-db-2020-07-30-sg

Availability Zone Info

No preference ▼

Note: Upon creating an instance for the second time, you may find this option is not available. Select the previous security group you used and then after setting up the database go to the later instructions on modifying access to your RDS.

d. Then for database authentication be sure and check ***Password and IAM database authentication.***



Database authentication

Database authentication options Info

○ Password authentication
Authenticates using database passwords.

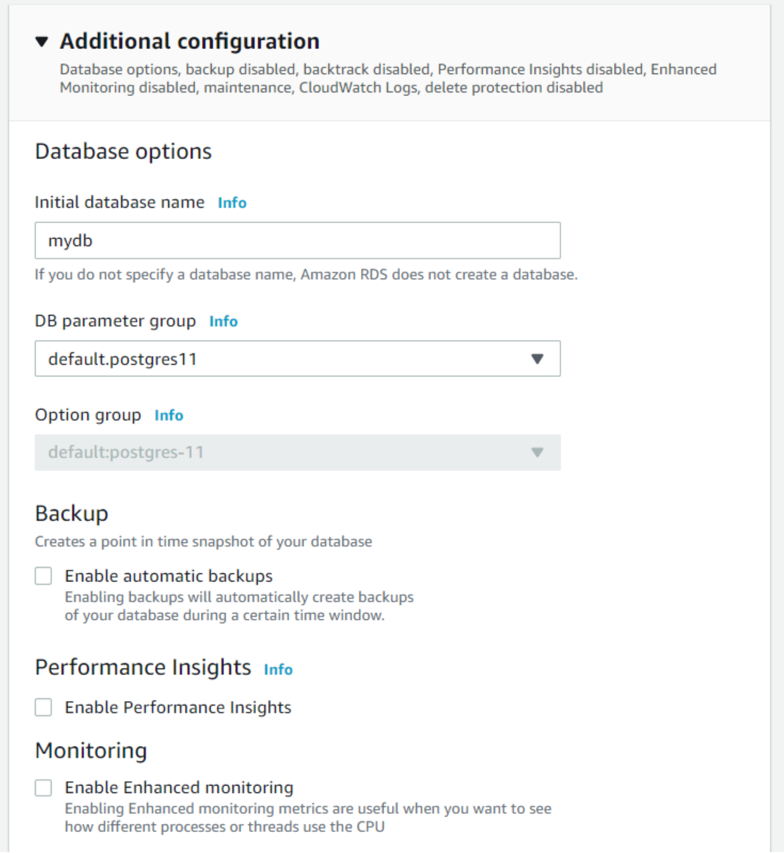
● Password and IAM database authentication
Authenticates using the database password and user credentials through AWS IAM users and roles.

○ Password and Kerberos authentication
Choose a directory in which you want to allow authorized users to authenticate with this DB instance using Kerberos Authentication.

e. Then select **Additional configuration:**

   i. **Then you can specify a name for your database and leave the default parameter group.**

   ii. **Disable Backup, Performance Insights, and Monitoring**



▼ Additional configuration
Database options, backup disabled, backtrack disabled, Performance Insights disabled, Enhanced Monitoring disabled, maintenance, CloudWatch Logs, delete protection disabled

Database options

Initial database name Info
mydb
If you do not specify a database name, Amazon RDS does not create a database.

DB parameter group Info
default.postgres11 ▼

Option group Info
default:postgres-11 ▼

Backup
Creates a point in time snapshot of your database

□ Enable automatic backups
Enabling backups will automatically create backups of your database during a certain time window.

Performance Insights Info

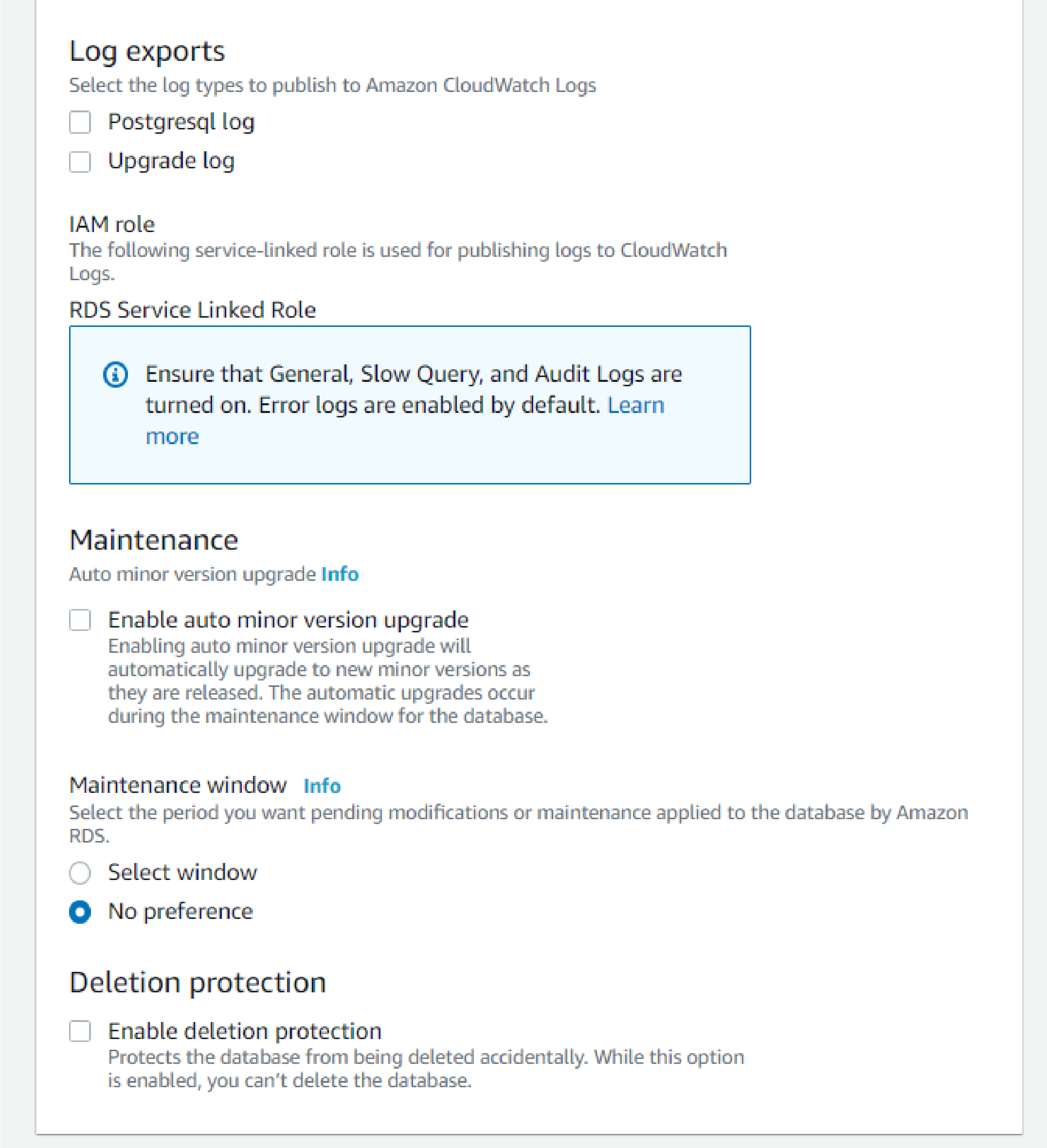
□ Enable Performance Insights

Monitoring

□ Enable Enhanced monitoring
Enabling Enhanced monitoring metrics are useful when you want to see how different processes or threads use the CPU

iii. Then ***disable*** the **Log Exports , Maintenance,** and **deletion protection**:

-



Log exports

Select the log types to publish to Amazon CloudWatch Logs

□ Postgresql log

□ Upgrade log

IAM role

The following service-linked role is used for publishing logs to CloudWatch Logs.

RDS Service Linked Role

ⓘ Ensure that General, Slow Query, and Audit Logs are turned on. Error logs are enabled by default. Learn more

Maintenance

Auto minor version upgrade Info

□ Enable auto minor version upgrade
Enabling auto minor version upgrade will automatically upgrade to new minor versions as they are released. The automatic upgrades occur during the maintenance window for the database.

Maintenance window Info

Select the period you want pending modifications or maintenance applied to the database by Amazon RDS.

○ Select window

● No preference

Deletion protection

□ Enable deletion protection
Protects the database from being deleted accidentally. While this option is enabled, you can't delete the database.

Finally, your you can proceed to create the instance!

You should see your database instance in the *Creating* status for several minutes. Eventually, you will see your database's status change to *Available.* At this point you may start to create connections and manage your database.

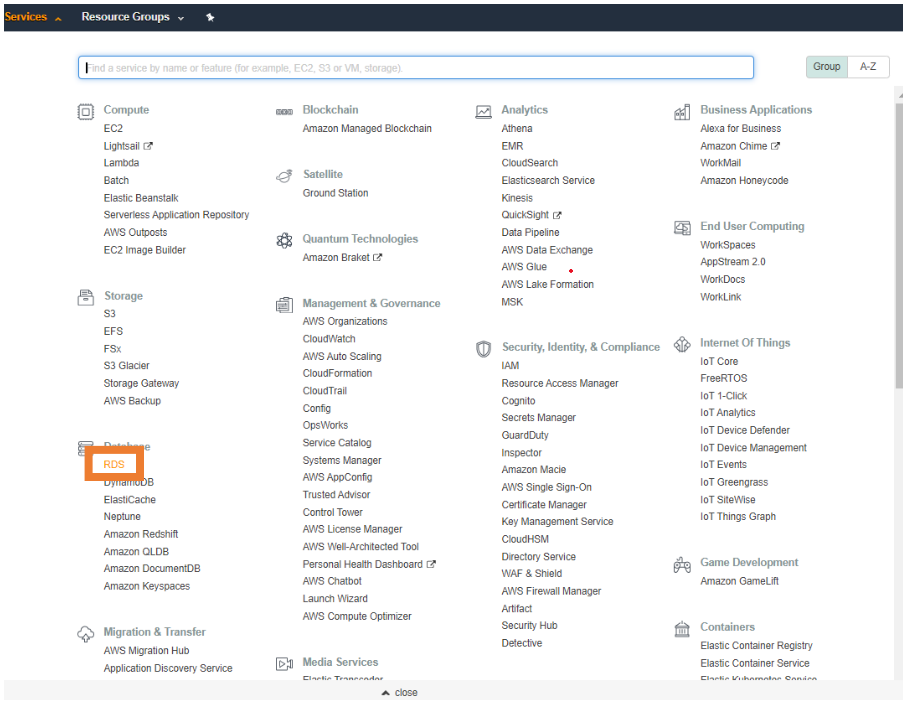
To find out details about the status of your database after exiting. Log back in and navigate to

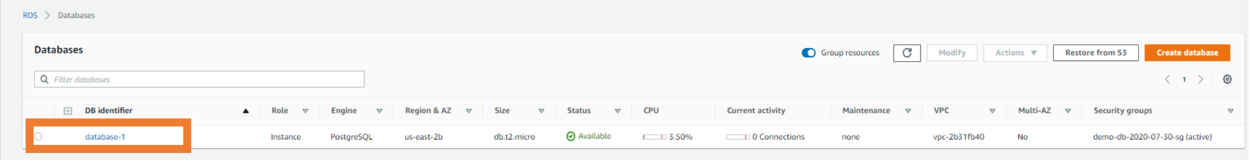
Services>RDS>Databases and select your database instance

When you are finished with your database you can remove it.

Upon Finishing:

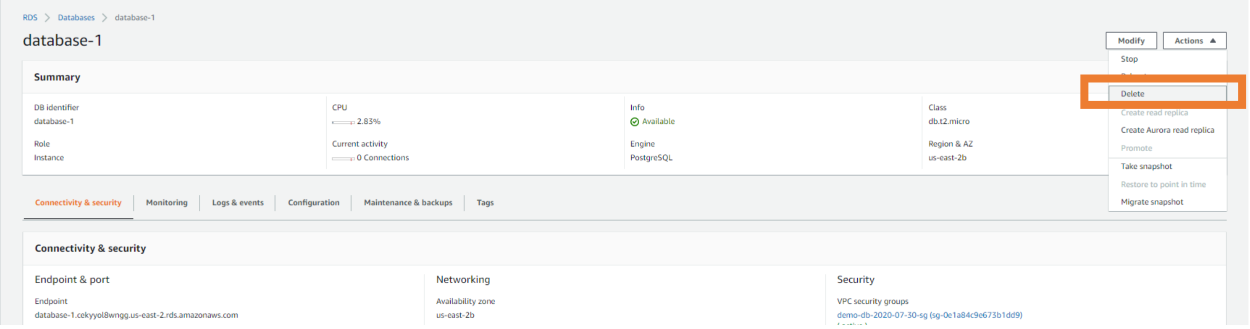
1. Navigate to Databases page. Go to Services> RDS>Databases :





DB identifier	Role	Engine	Region & AZ	Size	Status	CPU	Current activity	Maintenance	VPC	Multi-AZ	Security groups
database-1	Instance	PostgreSQL	us-east-2b	db.t2.micro	Available	3.50%	0 Connections	none	vpc-2b31fb40	No	demo-db-2020-07-30-sg (active)

2. Then select the instance ^^.
3. Finally click on the Actions dropdown menu and select Delete:



Summary

DB identifier
database-1

Role
Instance

CPU
2.83%

Current activity
0 Connections

Info
Available

Engine
PostgreSQL

Class
db.t2.micro

Region & AZ
us-east-2b

Connectivity & security

Endpoint & port

Endpoint
database-1.cekyyol8wngg.us-east-2.rds.amazonaws.com

Networking

Availability zone
us-east-2b

Security

VPC security groups
demo-db-2020-07-30-sg (sg-0e1a84c9e673b1dd9)

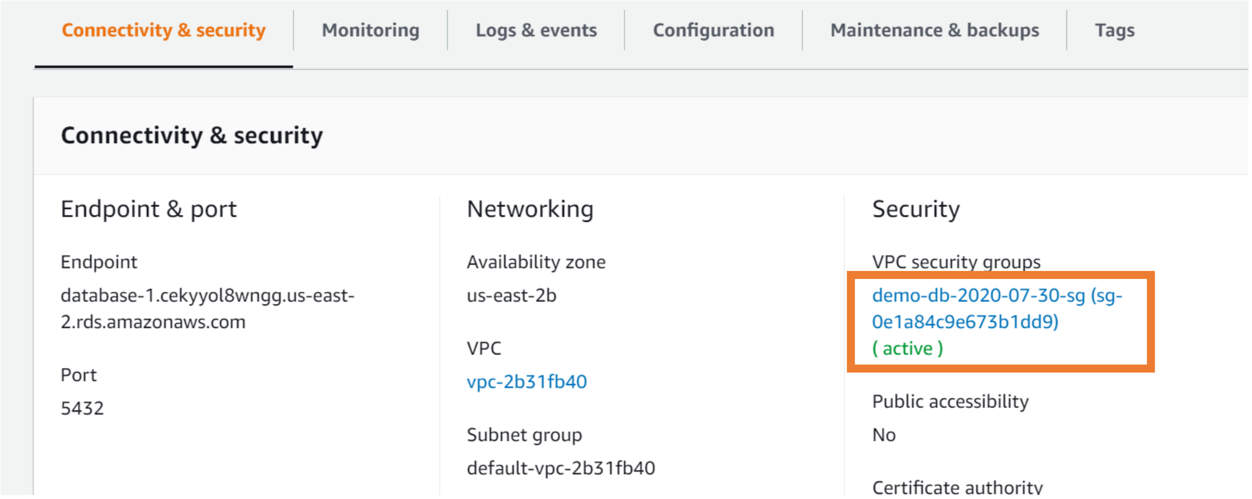
Nice work!

Modifying Access to AWS RDS

There may be circumstances where you are using an existing security group or you need to modify the rules associated with the security group that is associated with your RDS. Perhaps you need to change who has access to your database.

To do this navigate to your database page (the same page from which you will eventually delete your database).

Select the *Connectivity & security tab.* Click on the security group from there.



Connectivity & security | Monitoring | Logs & events | Configuration | Maintenance & backups | Tags

Connectivity & security

Endpoint & port

Endpoint
database-1.cekyyol8wngg.us-east-2.rds.amazonaws.com

Port
5432

Networking

Availability zone
us-east-2b

VPC
vpc-2b31fb40

Subnet group
default-vpc-2b31fb40

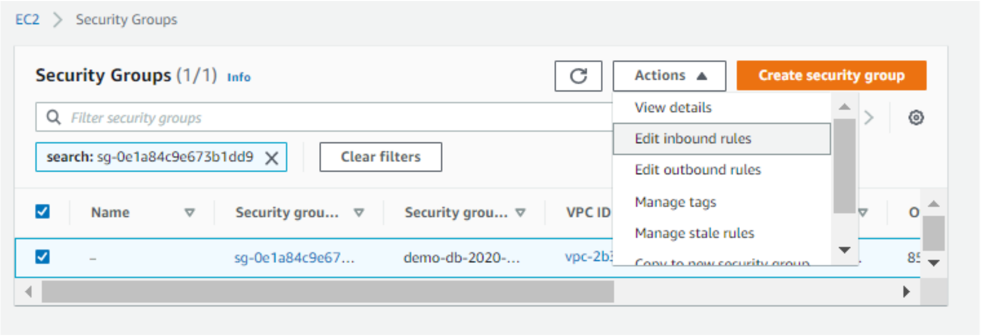
Security

VPC security groups
demo-db-2020-07-30-sg (sg-0e1a84c9e673b1dd9)
(active)

Public accessibility
No

Certificate authority

This will bring you to the Security Group page. From here make sure that your security groups is selected and then go to actions. Select edit inbound rules.



EC2 > Security Groups

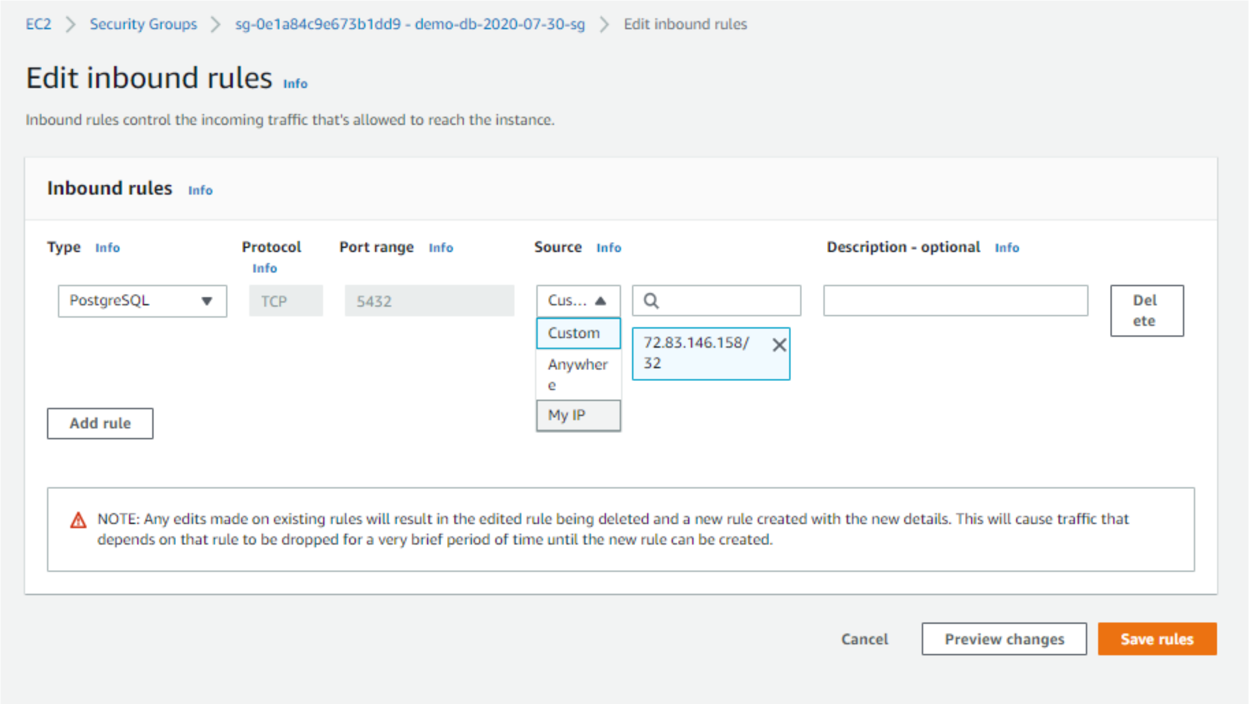
Security Groups (1/1) Info

☑	Name	Security grou...	Security grou...	VPC ID
☑	–	sg-0e1a84c9e67...	demo-db-2020-...	vpc-2b3

Now depending on your circumstances, you can add a rule to enable you to connect from another IP in addition to the current rule that exists or you can replace your previous inbound rule with another one.

You should ensure that the type matches PostgreSQL and its set to TCP and the port of your database.

Then for source, select either custom or MYIP depending on whether you are setting this up for yourself to connect from the current IP or somewhere else.



EC2 > Security Groups > sg-0e1a84c9e673b1dd9 - demo-db-2020-07-30-sg > Edit inbound rules

Edit inbound rules Info

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

Inbound rules Info

Type Info	Protocol Info	Port range Info	Source Info		Description - optional Info
PostgreSQL	TCP	5432	Custom	72.83.146.158/32	

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.

When you are finished select save rules. You should be able to connect from any IP for which there is an inbound rule.

Additionally, you should make sure to navigate back to this page and delete any inbound rules from IPs that are not or no longer associated with an IP address you specifically know. For instance, if you want to allow your associates to connect to the database you can add their IPs here, but you should delete them as soon as you are finished with the example.