

The goal of this document is to show a database available in a cloud environment. The project should be built from these indications.

The usage of a cloud database requires an Amazon AWS account.

Scalability:

RDS virtualization could be scaled, creating different SCHEMAS, or DATABASES instances, for different Application services.

The following contents is presented in this document.

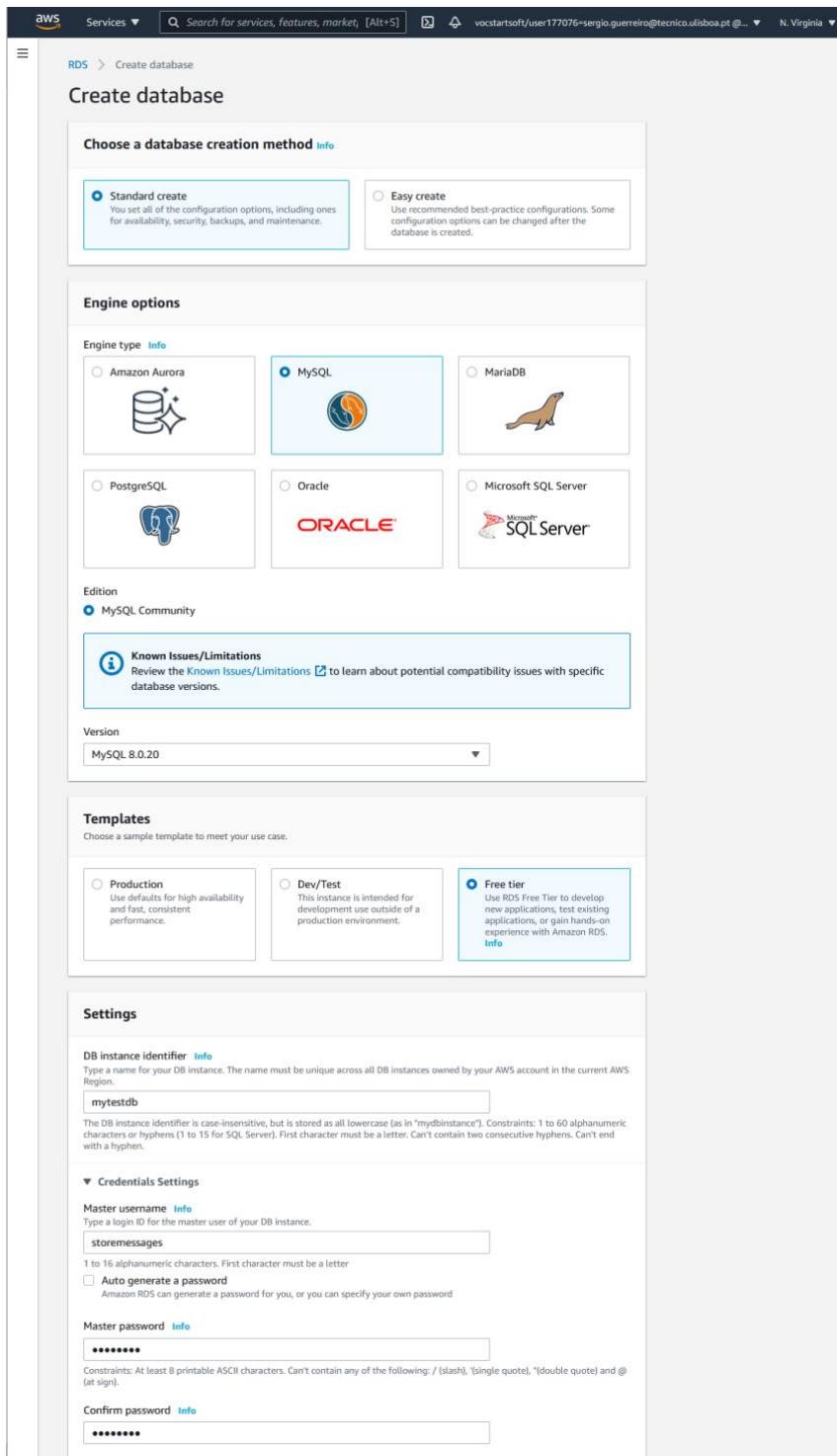
Contents

- A. Create an AWS RDS Database, accessing it, and inserting data: example of.....2

A. Create an AWS RDS Database, accessing it, and inserting data: example of

The goal of this section is to exemplify how to create your own cloud database in AWS, to access its contents through a database workbench, and then creating a JAVA microservice to consume Kafka messages that are then inserted in the cloud database.

1. Go to your AWS account console and click on Database RDS -> My SQL and select the following configurations in step 2:



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.

- 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

New instance classes are available for specific engine versions. [Info](#)

Include previous generation classes

Storage

Storage type [Info](#)
 General Purpose (SSD)

Allocated storage
 20 GiB
 (Minimum: 20 GiB, Maximum: 16 384 GiB) Higher allocated storage may improve IOPS performance.

Storage autoscaling [Info](#)
 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.

Maximum storage threshold [Info](#)
 Charges will apply when your database autoscales to the specified threshold
 1000 GiB
 Minimum: 21 GiB, Maximum: 16 384 GiB

Availability & durability

Multi-AZ deployment [Info](#)

- Do not create a standby instance
- Create a standby instance (recommended for production usage)
 Creates a standby in a different Availability Zone (AZ) to provide data redundancy, eliminate I/O freezes, and minimize latency spikes during system backups.

Connectivity

Virtual private cloud (VPC) [Info](#)
 VPC that defines the virtual networking environment for this DB instance.
Default VPC (vpc-3413dd49)

Only VPCs with a corresponding DB subnet group are listed.

Subnet group [Info](#)
 DB subnet group that defines which subnets and IP ranges the DB instance can use in the VPC you selected.
default

Public access [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 a VPC security group to allow access to your database. Ensure that the security group rules allow the appropriate incoming traffic.

Choose existing
 Choose existing VPC security groups

Create new
 Create new VPC security group

Existing VPC security groups
 Choose VPC security groups
 launch-wizard-5 X default X

Availability Zone [Info](#)
 No preference

Additional configuration

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 (not available for this version)
 Choose a directory in which you want to allow authorized users to authenticate with this DB instance using Kerberos Authentication.

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

Database options

Initial database name [Info](#)
 If you do not specify a database name, Amazon RDS does not create a database.

DB parameter group [Info](#)

Option group [Info](#)

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.

⚠ Please note that automated backups are currently supported for InnoDB storage engine only. If you are using MyISAM, refer to details [here](#).

Backup retention period [Info](#)
Choose the number of days that RDS should retain automatic backups for this instance.

Backup window [Info](#)
Select the period for which you want automated backups of the database to be created by Amazon RDS.
 Select window
 No preference

Copy tags to snapshots

Monitoring

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

Log exports

Select the log types to publish to Amazon CloudWatch Logs

Error log
 General log
 Slow query log

IAM role

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

ⓘ 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.

Hint: Later, check if your VPC configuration allows connections from anywhere in the internet. Choose the VPC Security groups and edit the configuration similarly with:

The screenshot shows the AWS EC2 Services dashboard with the 'Resource Groups' tab selected. Under 'SECURITY GROUPS', there is one entry: 'Security Group: sg-671f0033'. The 'Inbound' tab is selected, showing two rules: 'All traffic' on port All from Source 0.0.0.0/0. The 'Description' column indicates it's the 'default VPC security group'.

2. You can now check if the database is started.
3. Use your MySQL database client (for example MySQL workbench), connect to your RDS AWS database and execute the following scripts:

```
DROP DATABASE IF EXISTS collectedMSGs;
CREATE DATABASE IF NOT EXISTS collectedMSGs;
```

```
USE collectedMSGs;
DROP TABLE IF EXISTS Message;

CREATE TABLE Message( offset INTEGER PRIMARY KEY,
    groupId VARCHAR(100) NOT NULL,
    contentKey VARCHAR(100),
    contentValue VARCHAR(1000));
```