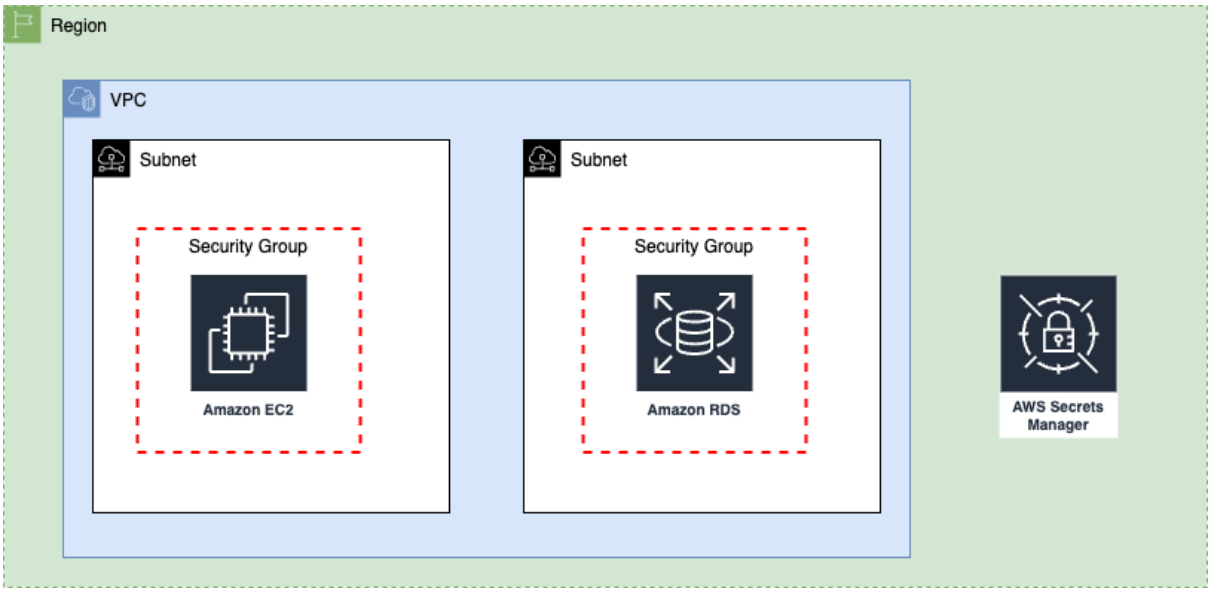
Lab - Securing Application Credentials with AWS Secrets Manager



Resumen del Lab: Securing Application Credentials with AWS Secrets Manager

Este lab me enseñó a usar AWS Secrets Manager, una herramienta clave para almacenar y gestionar información sensible de forma segura, como credenciales de bases de datos o claves API. En lugar de dejar estas credenciales en archivos de configuración o código fuente (algo muy inseguro), Secrets Manager cifra y almacena esta información, permitiendo acceder a ella solo cuando es necesario. Además, aprendí a rotar secretos automáticamente, lo que ayuda a reducir el riesgo de que se filtren o comprometan.

El objetivo principal fue crear, gestionar y rotar secretos, conectarme a una base de datos usando las credenciales almacenadas, y verificar que todo funcionaba correctamente. Esto es súper útil en entornos reales porque mejora la seguridad sin complicar demasiado el proceso.

Detalles relevantes

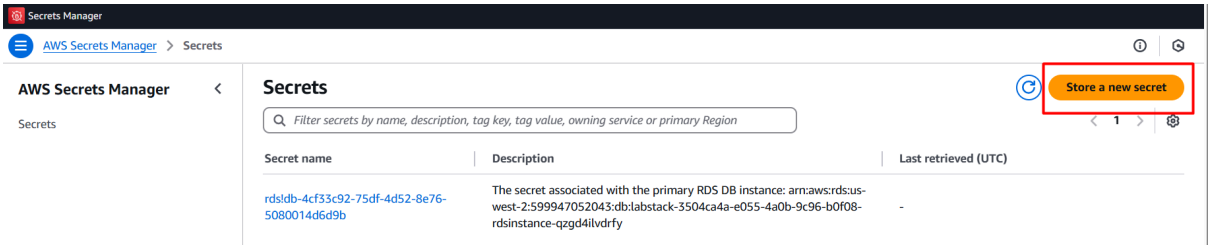
1. **Crear un secreto para credenciales de base de datos**

Qué hice?

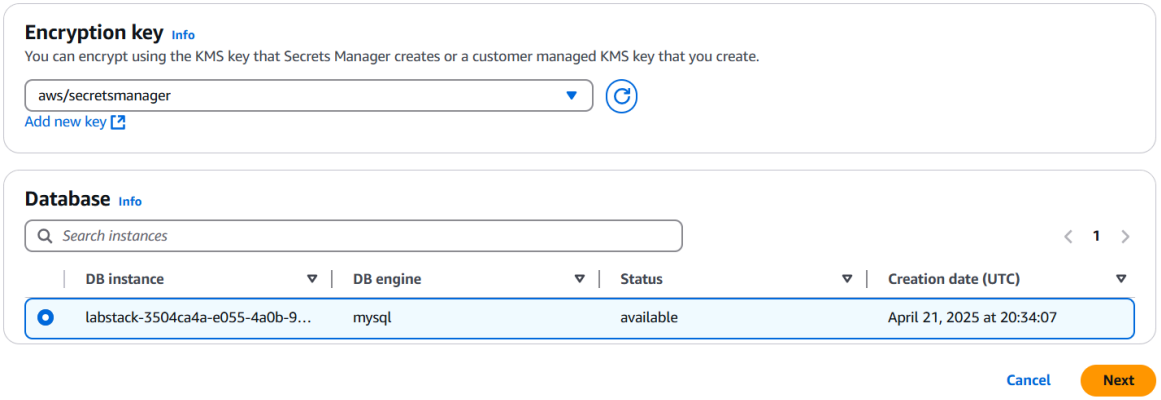
Creé un secreto en AWS Secrets Manager para almacenar las credenciales de una base de datos RDS.

Cómo lo hice?

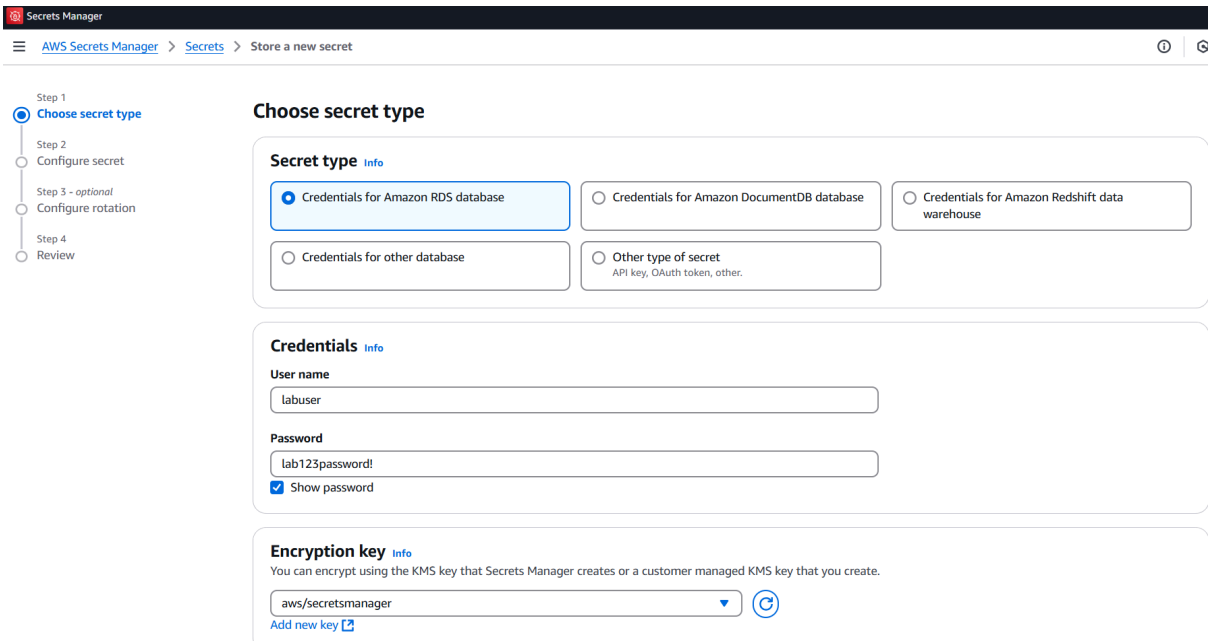
- Fui al servicio Secrets Manager desde la consola de AWS.
- Seleccioné Store a new secret y elegí Credentials for Amazon RDS database.



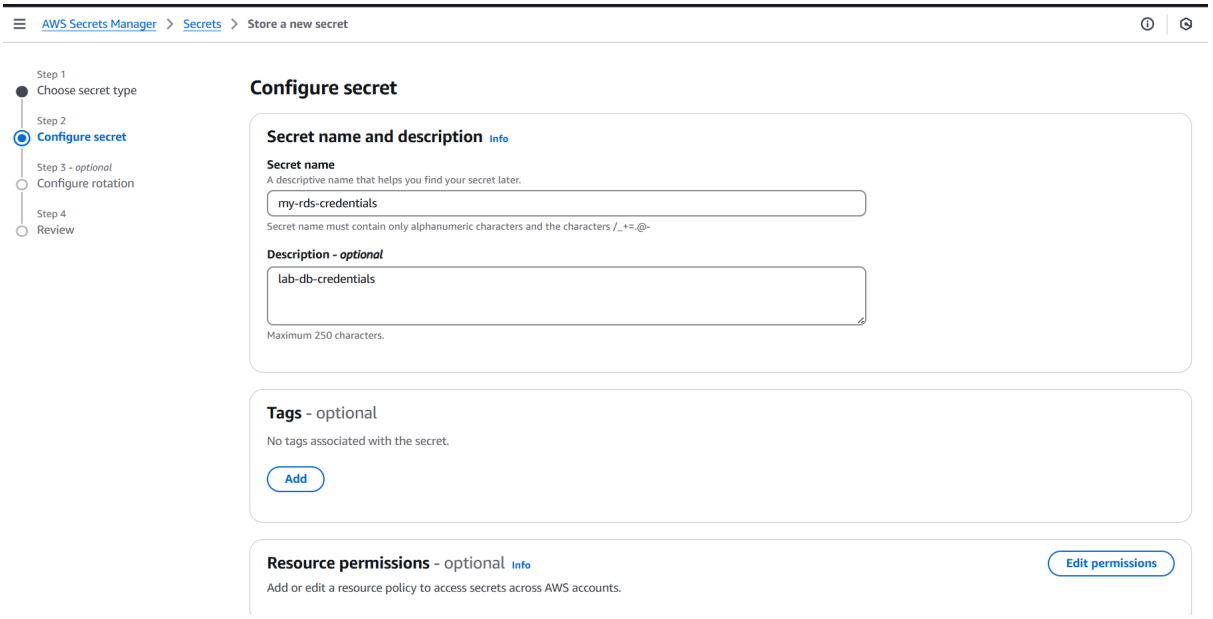
- Ingresé los datos de ejemplo:
  - Username: labuser
  - Password: lab123password!
  - Database: Usé el ID de la instancia RDS proporcionado.

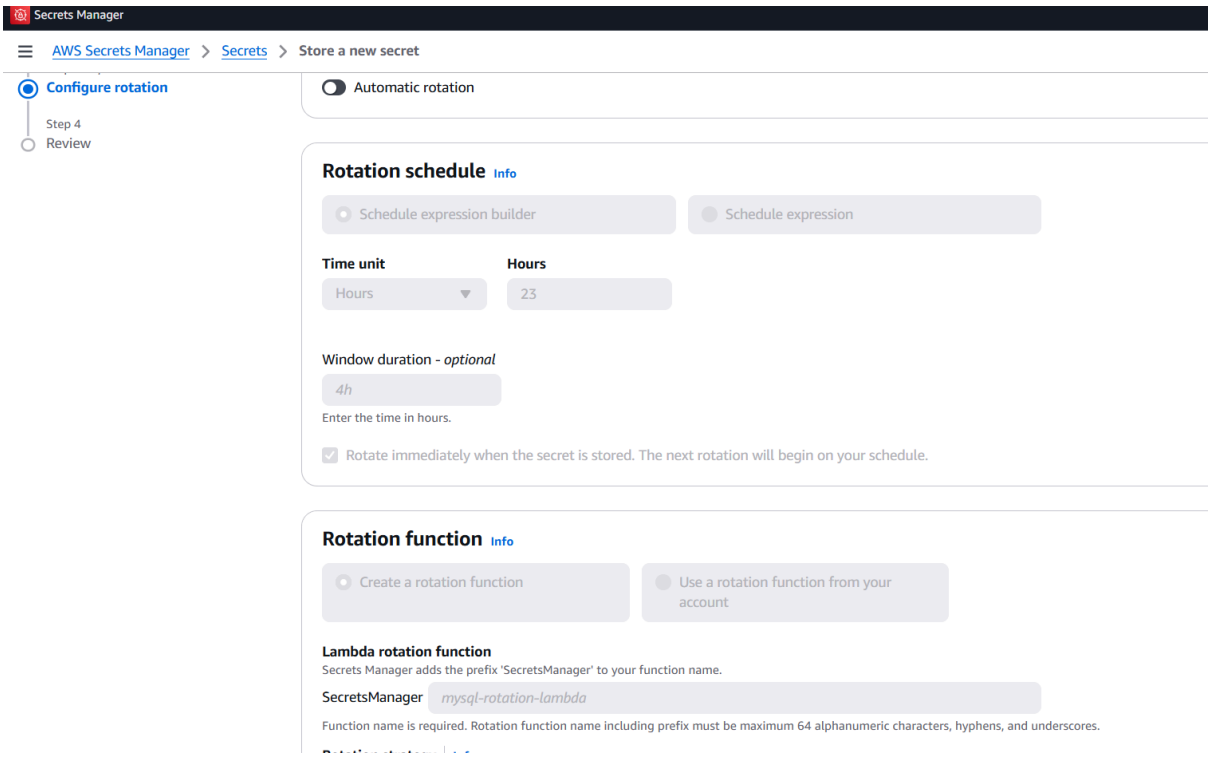


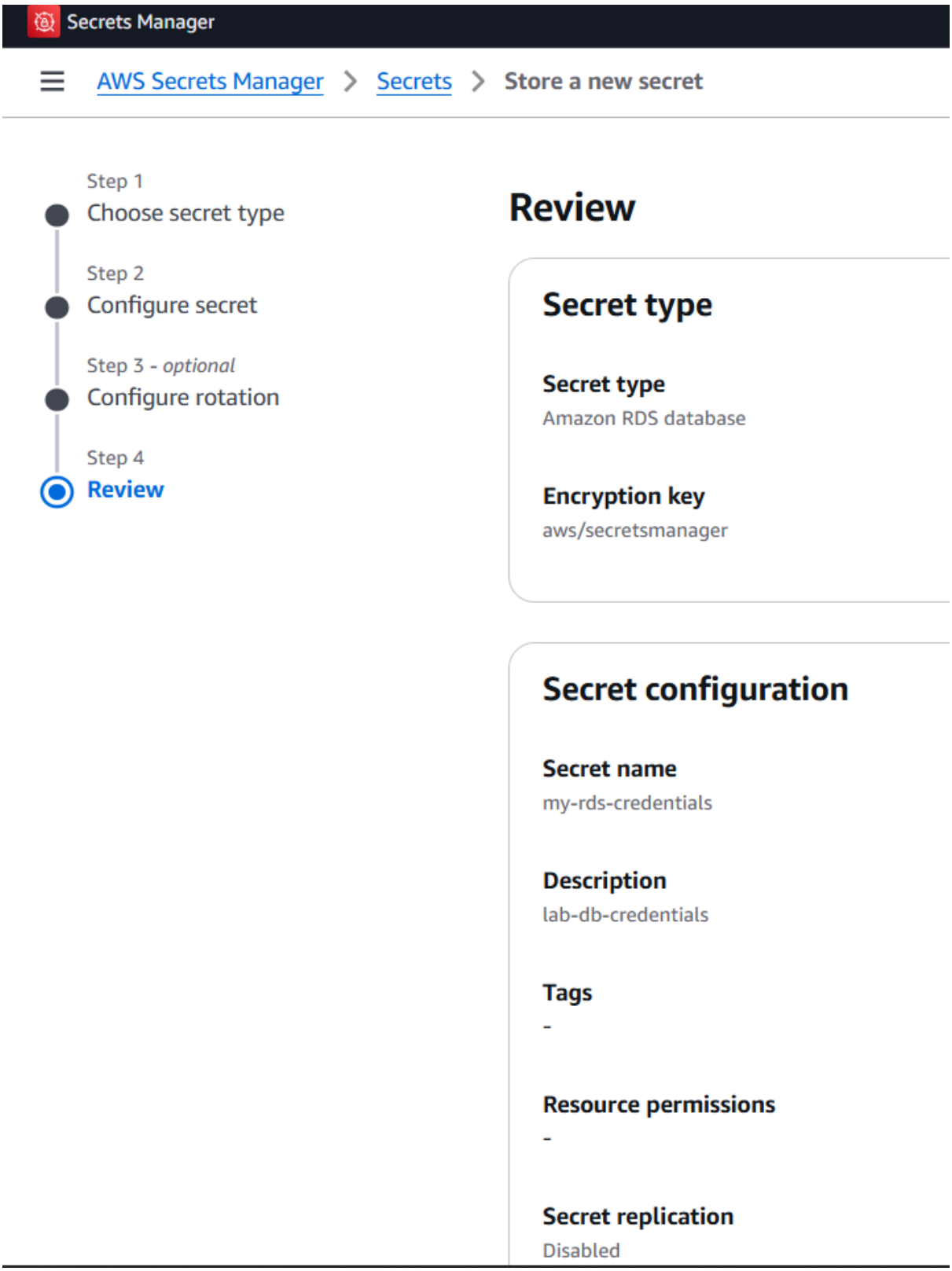
- Elegí la clave de cifrado por defecto (aws/secretsmanager) para simplificar el proceso.

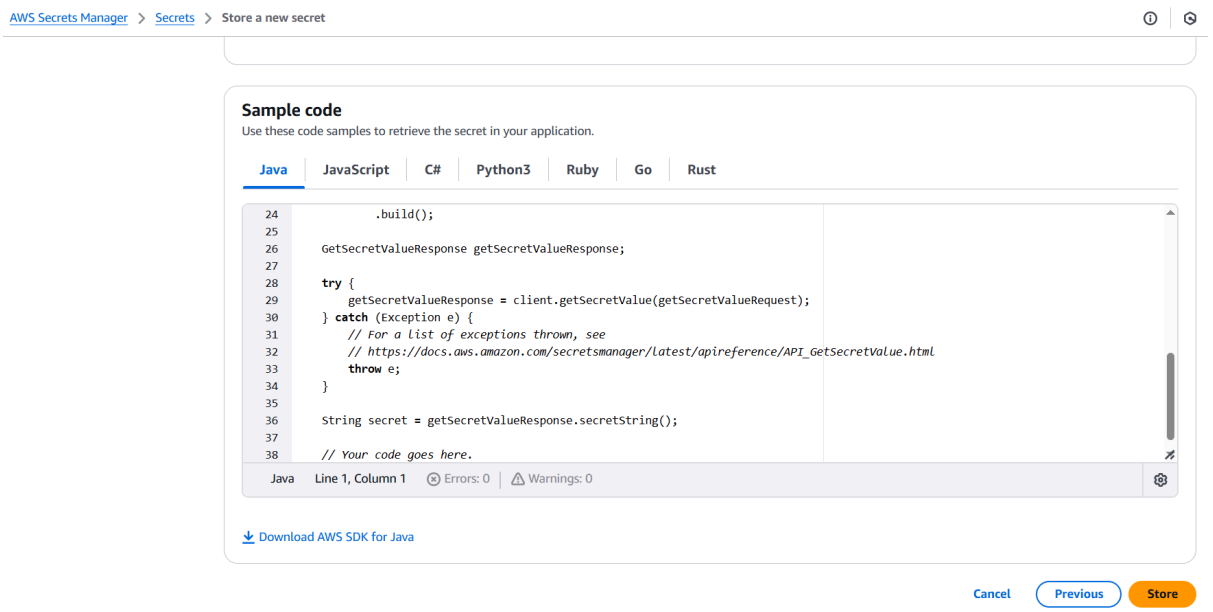


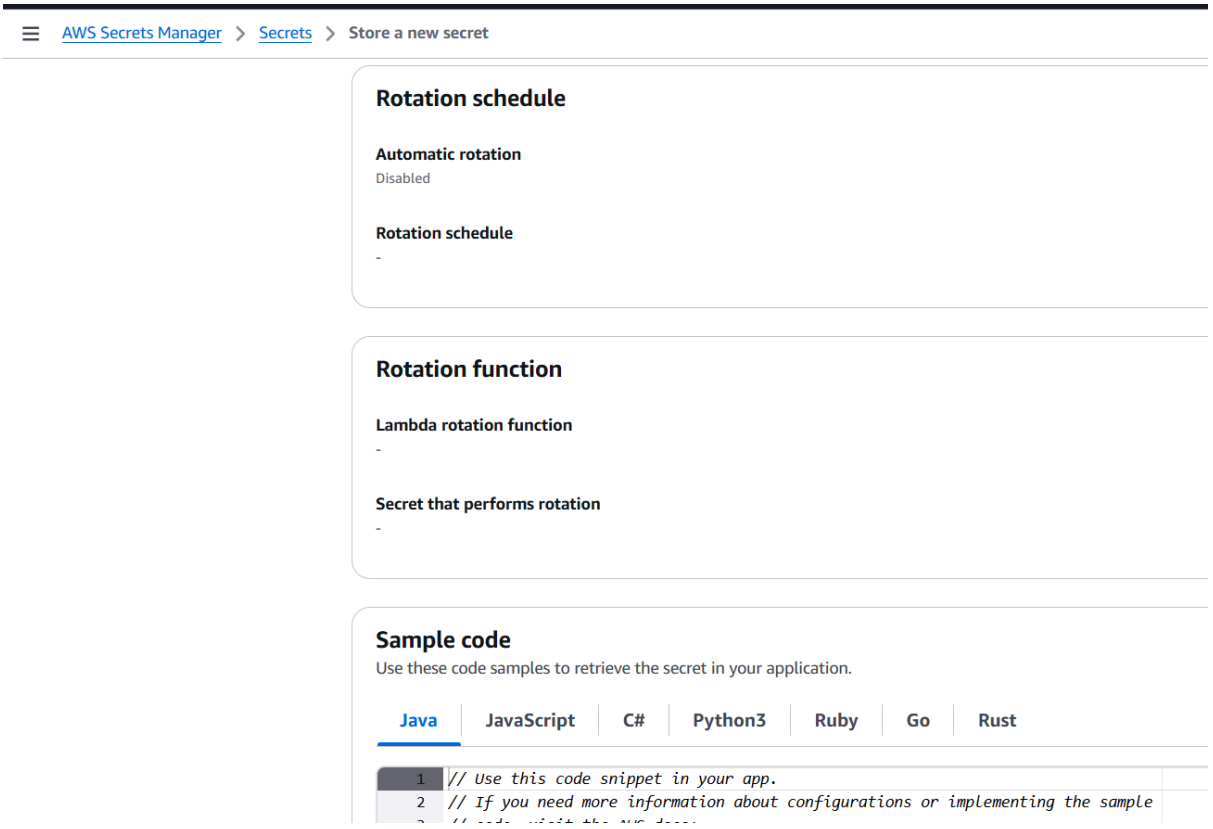
- Le puse un nombre descriptivo al secreto: my-rds-credentials.

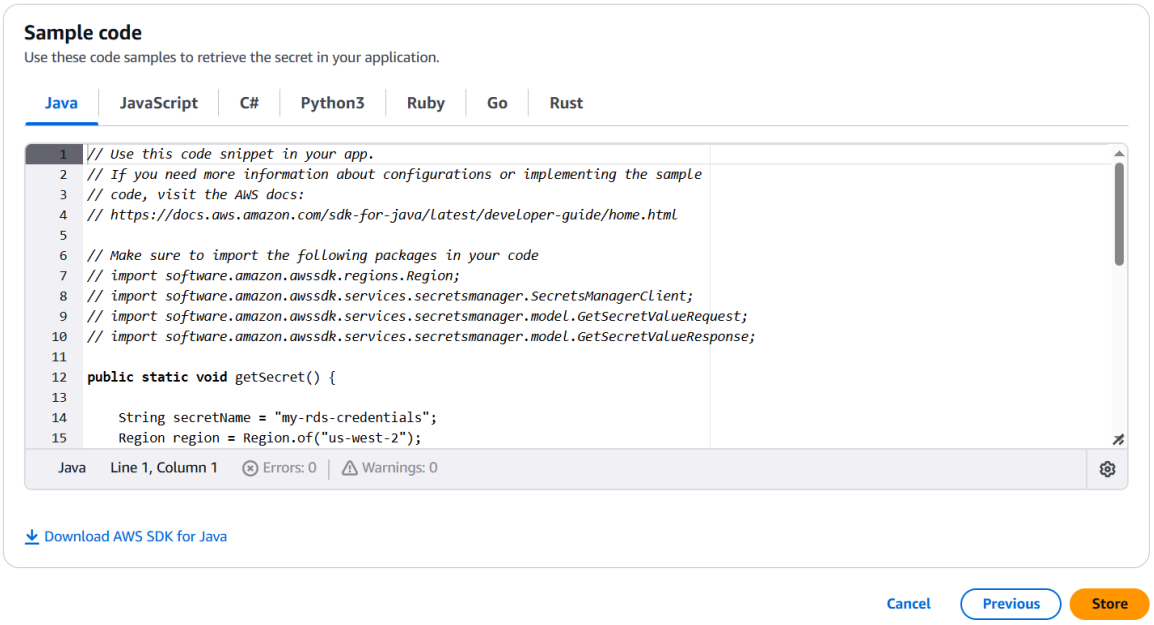


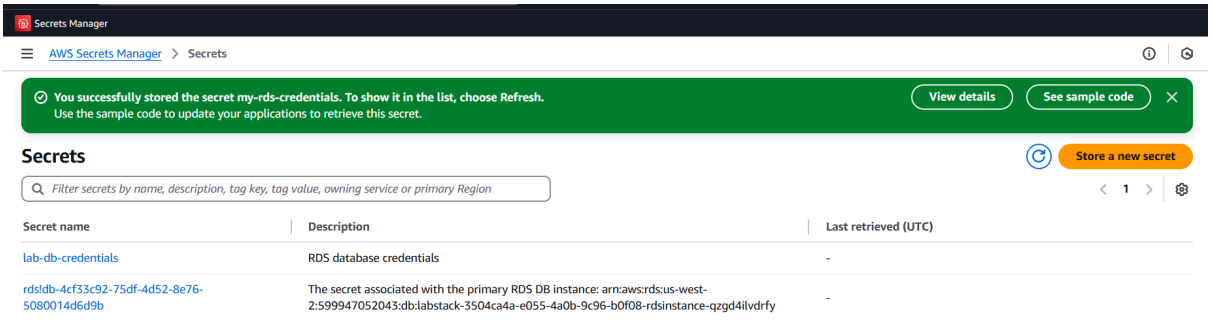

Secrets Manager
AWS Secrets Manager > Secrets > Store a new secret
Configure rotation
Step 4
Review
Automatic rotation
Rotation schedule Info
Schedule expression builder
Schedule expression
Time unit
Hours
Hours
23
Window duration - optional
4h
Enter the time in hours.
Rotate immediately when the secret is stored. The next rotation will begin on your schedule.
Rotation function Info
Create a rotation function
Use a rotation function from your account
Lambda rotation function
Secrets Manager adds the prefix 'SecretsManager' to your function name.
SecretsManager
mysql-rotation-lambda
Function name is required. Rotation function name including prefix must be maximum 64 alphanumeric characters, hyphens, and underscores.


Secrets Manager
AWS Secrets Manager
Secrets
Store a new secret
Step 1
Choose secret type
Step 2
Configure secret
Step 3 - optional
Configure rotation
Step 4
Review
Review
Secret type
Secret type
Amazon RDS database
Encryption key
aws/secretsmanager
Secret configuration
Secret name
my-rds-credentials
Description
lab-db-credentials
Tags
-
Resource permissions
-
Secret replication
Disabled


AWS Secrets Manager > Secrets > Store a new secret
Sample code
Use these code samples to retrieve the secret in your application.
Java
JavaScript
C#
Python3
Ruby
Go
Rust
.build();
GetSecretValueResponse getSecretValueResponse;
try {
getSecretValueResponse = client.getSecretValue(getSecretValueRequest);
} catch (Exception e) {
// For a list of exceptions thrown, see
// https://docs.aws.amazon.com/secretsmanager/latest/apireference/API_GetSecretValue.html
throw e;
}
String secret = getSecretValueResponse.secretString();
// Your code goes here.
Java Line 1, Column 1 Errors: 0 Warnings: 0
Download AWS SDK for Java
Cancel
Previous
Store


AWS Secrets Manager > Secrets > Store a new secret
Rotation schedule
Automatic rotation
Disabled
Rotation schedule
-
Rotation function
Lambda rotation function
-
Secret that performs rotation
-
Sample code
Use these code samples to retrieve the secret in your application.
Java
JavaScript
C#
Python3
Ruby
Go
Rust
// Use this code snippet in your app.
// If you need more information about configurations or implementing the sample





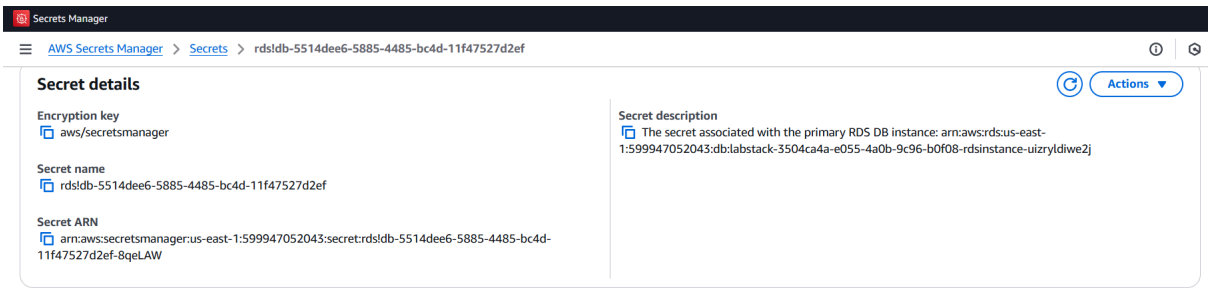
Por qué es importante?
Este paso es fundamental porque muestra cómo almacenar credenciales de forma segura. La clave de cifrado garantiza que nadie pueda ver los secretos sin permisos adecuados.

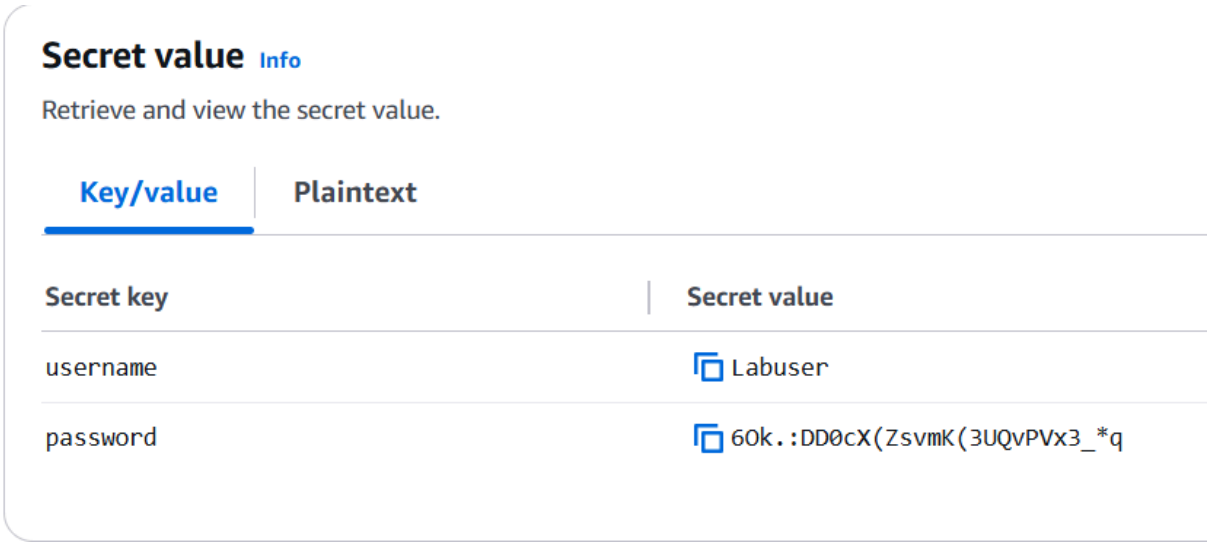
2. Conectar a la base de datos usando el secreto

Qué hice?
Recuperé las credenciales del secreto y me conecté a la base de datos RDS usando el cliente MySQL.

Cómo lo hice?

- Desde Secrets Manager, seleccioné el secreto creado (my-rds-credentials) y usé la opción Retrieve secret value para obtener las credenciales.





- Accedí a la instancia EC2 mediante Session Manager y ejecuté estos comandos:
  - sudo yum install mariadb

```
sh-4.2$ sudo yum install mariadb
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
amzn2-core                                                                      | 3.6 kB  00:00:00
Resolving Dependencies
--> Running transaction check
---> Package mariadb.x86_64 1:5.5.68-1.amzn2.0.1 will be installed
--> Finished Dependency Resolution

Dependencies Resolved

================================================================================================
 Package              Arch             Version                     Repository              Size
================================================================================================
Installing:
 mariadb              x86_64           1:5.5.68-1.amzn2.0.1        amzn2-core             8.8 M

Transaction Summary
================================================================================================
Install  1 Package

Total download size: 8.8 M
Installed size: 49 M
Is this ok [y/d/N]: Y
Downloading packages:
mariadb-5.5.68-1.amzn2.0.1.x86_64.rpm                                           | 8.8 MB  00:00:00
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Installing : 1:mariadb-5.5.68-1.amzn2.0.1.x86_64                                            1/1
  Verifying  : 1:mariadb-5.5.68-1.amzn2.0.1.x86_64                                            1/1

Installed:
  mariadb.x86_64 1:5.5.68-1.amzn2.0.1
```


```
Total download size: 8.8 M
Installed size: 49 M
Is this ok [y/d/N]: Y
Downloading packages:
mariadb-5.5.68-1.amzn2.0.1.x86_64.rpm
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Installing : 1:mariadb-5.5.68-1.amzn2.0.1.x86_64
  Verifying  : 1:mariadb-5.5.68-1.amzn2.0.1.x86_64

Installed:
  mariadb.x86_64 1:5.5.68-1.amzn2.0.1
```


```
Complete!
```

  - mysql -u Labuser -p -h labstack-3504ca4a-e055-4a0b-9c96-b0f08-rdsinstance-uizryldiwe2j.cwjug4nygjc8.us-east-1.rds.amazonaws.com -P 3306

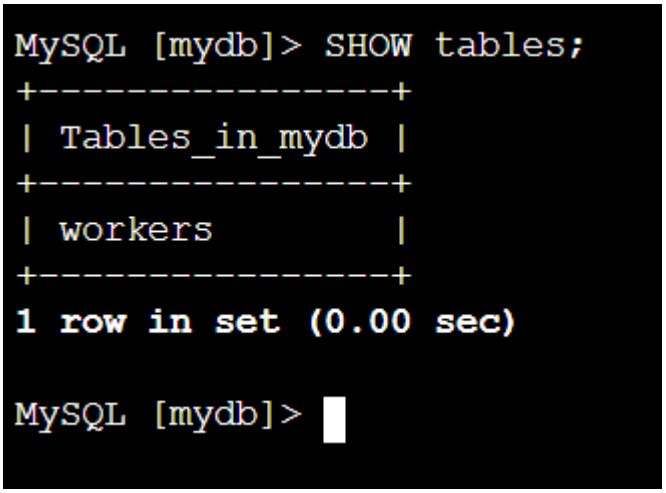
copia y pegar cuando pida la contraseña.→ 6Ok.:DD0cX(ZsvmK(3UQvPVx3_*q

- Resultado : Me conecté exitosamente a la base de datos y creé una tabla llamada workers para probar la conexión.

```
sh-4.2$ mysql -u Labuser -p -h labstack-3504ca4a-e055-4a0b-9c96-b0f08-rdsinstance-uizryldi
we2j.cwjug4nygjc8.us-east-1.rds.amazonaws.com -P 3306
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 35
Server version: 8.0.40 Source distribution

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]>
```

```
MySQL [(none)]> SHOW databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mydb               |
| mysql              |
| performance_schema |
| sys                |
+--------------------+
5 rows in set (0.01 sec)

MySQL [(none)]>
```

```
MySQL [(none)]> USE mydb;
Database changed
MySQL [mydb]> CREATE TABLE workers
    -> (
    ->     worker_id INT,
    ->     first_name VARCHAR(50) not null,
    ->     last_name VARCHAR(50),
    ->     birth_date DATE,
    ->     salary DOUBLE not null
    -> );
Query OK, 0 rows affected (0.08 sec)

MySQL [mydb]>
```



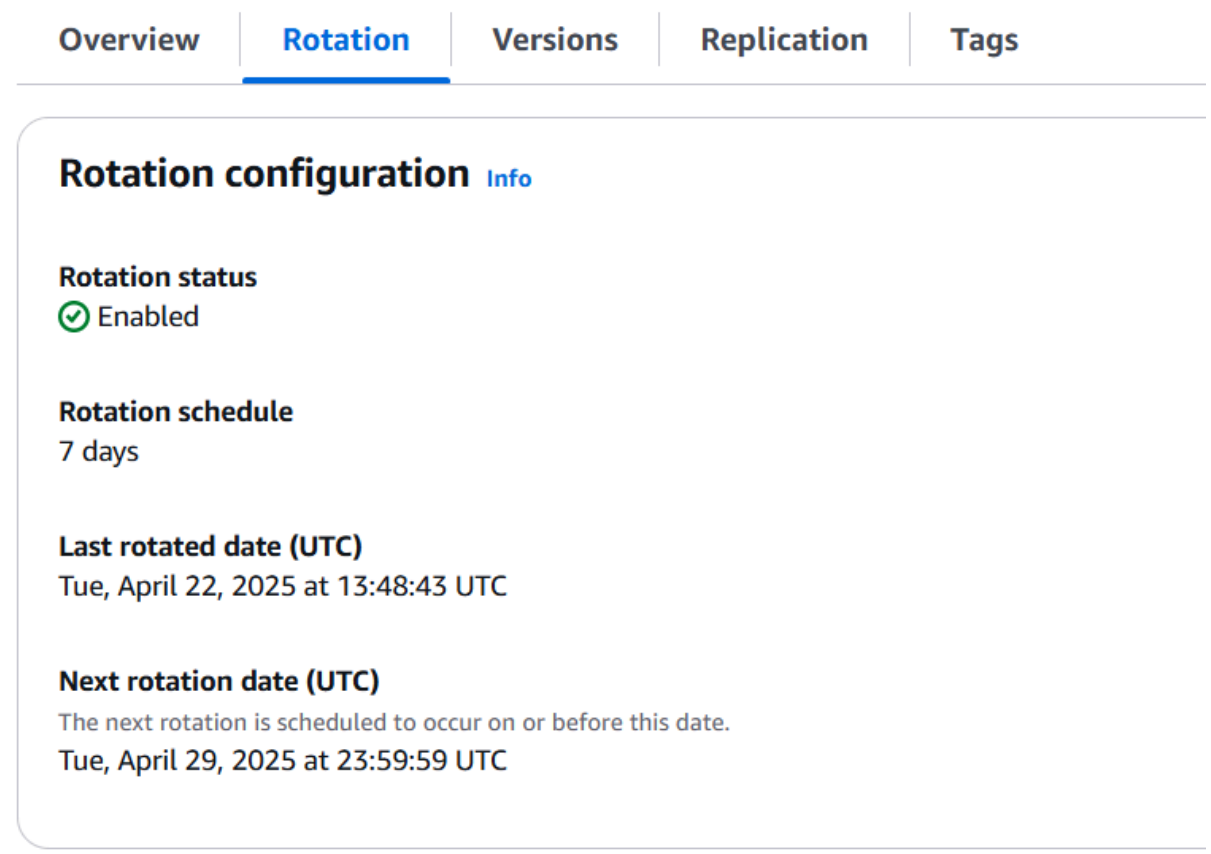
Por qué es importante : Este paso demuestra cómo recuperar secretos de forma segura y usarlos en aplicaciones o scripts sin exponerlos directamente.

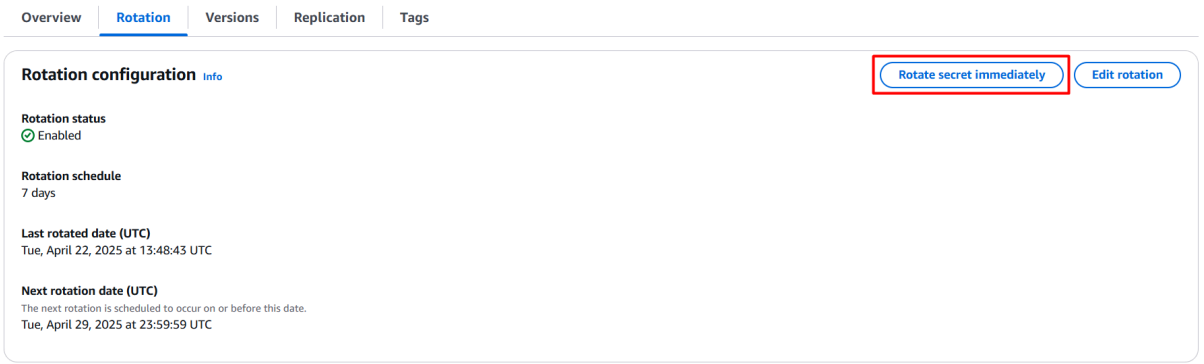
3. Rotar el secreto

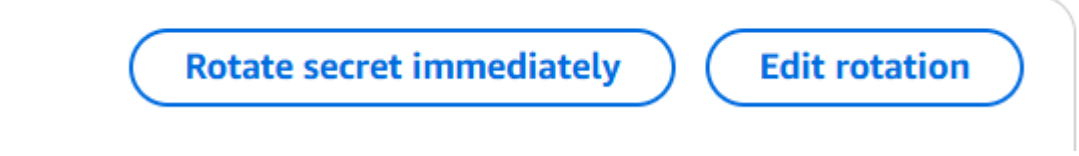
Qué hice?
Simulé una situación de emergencia rotando el secreto manualmente para generar una nueva contraseña.

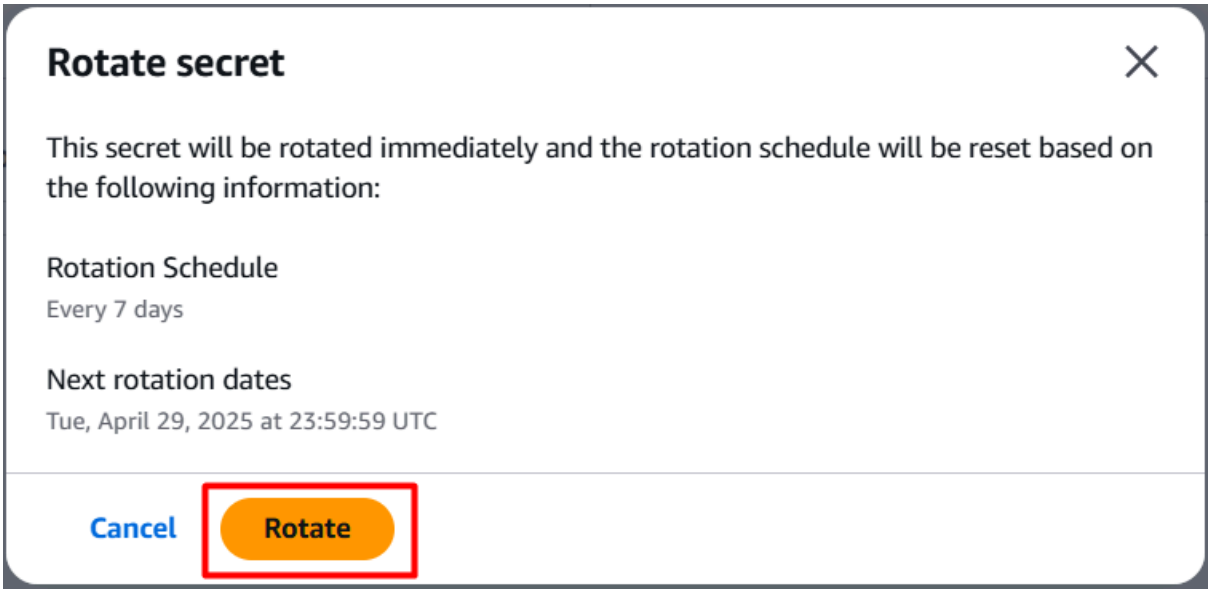
Cómo lo hice?

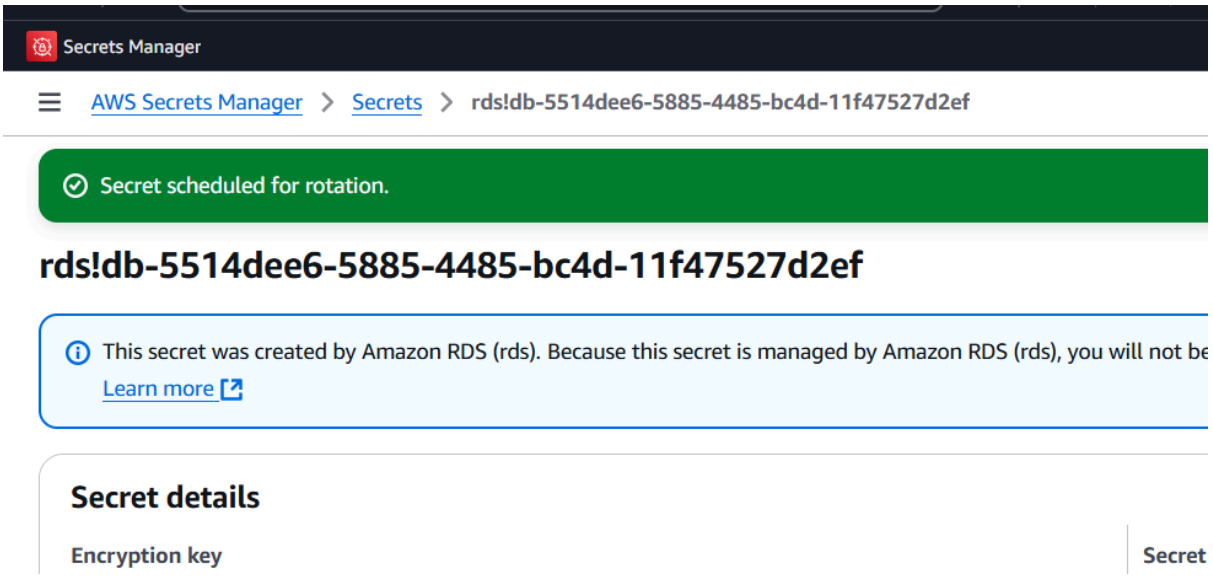
- En Secrets Manager, seleccioné el secreto (my-rds-credentials) y fui a la pestaña Rotation .
- Elegí Rotate secret immediately para generar una nueva contraseña.
- Confirmé la rotación y recuperé el nuevo valor del secreto.
- Probé la nueva contraseña conectándome nuevamente a la base de datos.


Overview
Rotation
Versions
Replication
Tags
Rotation configuration Info
Rotation status
Enabled
Rotation schedule
7 days
Last rotated date (UTC)
Tue, April 22, 2025 at 13:48:43 UTC
Next rotation date (UTC)
The next rotation is scheduled to occur on or before this date.
Tue, April 29, 2025 at 23:59:59 UTC

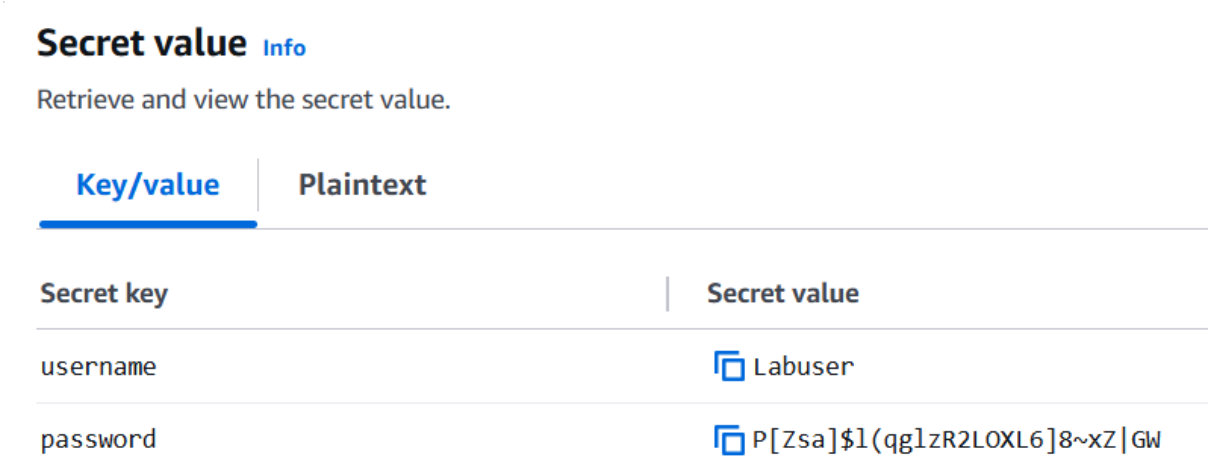

Overview
Rotation
Versions
Replication
Tags
Rotation configuration Info
Rotate secret immediately
Edit rotation
Rotation status
Enabled
Rotation schedule
7 days
Last rotated date (UTC)
Tue, April 22, 2025 at 13:48:43 UTC
Next rotation date (UTC)
The next rotation is scheduled to occur on or before this date.
Tue, April 29, 2025 at 23:59:59 UTC


Rotate secret immediately
Edit rotation

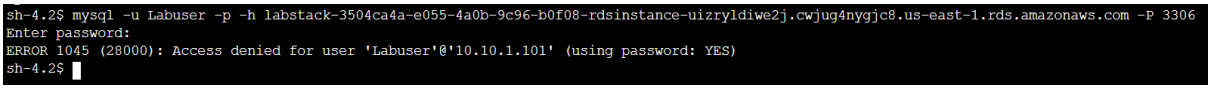


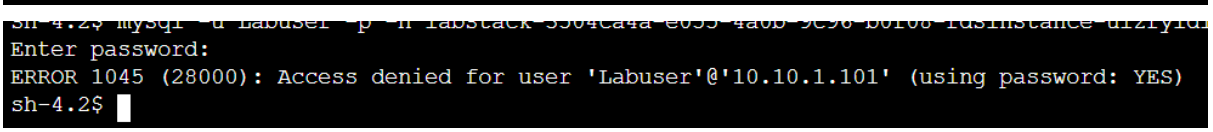


Esperamos unos minutos para que se actualice.



La contraseña ha cambiado e intento iniciar otra vez y no me deja.



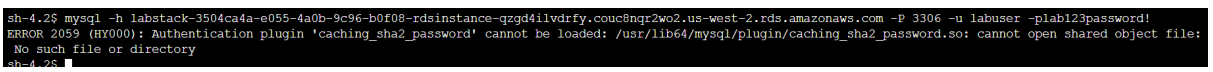


Por qué es importante?
La rotación de secretos es una práctica esencial para minimizar riesgos si una contraseña se filtra. AWS Secrets Manager automatiza este proceso, lo que facilita mucho la vida.

Aspectos destacados

- Seguridad: Almacenar credenciales en Secrets Manager es mucho más seguro que dejarlas en código o archivos de configuración.
- Automatización: Secrets Manager puede rotar secretos automáticamente, lo que reduce el trabajo manual y los errores humanos.
- Flexibilidad: Puedo almacenar cualquier tipo de dato sensible, no solo credenciales de bases de datos (por ejemplo, claves API o SSH keys).

Error → Solución



Me aparece un error que indica que no tiene instalado ni configurado correctamente el plugin caching_sha2_password, que es necesario para conectarte a la base de datos RDS de AWS. Este plugin es un método de

autenticación utilizado por MySQL 8.2, y parece que tu cliente MySQL actual no lo soporta.

Al final lo hice de nuevo y no tuve problemas.

Conclusión

En este lab aprendí a usar AWS Secrets Manager para almacenar, recuperar y rotar secretos de forma segura. Es una herramienta poderosa que puede mejorar significativamente la seguridad de mis aplicaciones y bases de datos. Además, la integración con servicios como RDS y EC2 hace que sea fácil de implementar en proyectos reales.

Ahora puedo decir con confianza que entiendo cómo proteger credenciales sensibles y evitar problemas de seguridad relacionados con ellas.