## Lab 7-02: Using AWS Secrets Manager for Storing and Rotating Database Credentials

### Service Introduction

AWS Secrets Manager is a service that helps you protect access to your applications, services, and IT resources without the upfront cost and complexity of managing your own Hardware Security Module (HSM) infrastructure. Secrets Manager enables you to rotate, manage, and retrieve database credentials, API keys, and other secrets throughout their lifecycle.

### Problem

You are managing multiple databases with credentials hard-coded in the application code. This practice poses a security risk and makes it difficult to rotate credentials regularly, which is necessary to maintain security best practices and compliance requirements.

### Solution

Utilize AWS Secrets Manager to store and manage your database credentials securely. Secrets Manager can automatically rotate the credentials according to a specified schedule, ensuring that your applications always use up-to-date credentials without manual intervention. This enhances security by reducing the risk of exposing credentials and simplifying the management of sensitive information.

#### Task 1: Create a New Secret in Secrets Manager (with Secret Rotation)

|  |
| --- |
| 1. Navigate to **AWS Secrets Manager** by searching for and selecting Secrets Manager in the top search bar. 2. Under **Get started** on the right, click **Store a new secret.**      1. Under **Secret type,** select **Credentials** for Amazon RDS database. 2. Under Credentials > User name, enter a username. 3. Under Credentials > Password, enter your password. 4. Under Database, select the listed database. 5. Click **Next.**      1. Under Secret name and description > Secret name, enter NewDbSecrets. 2. Under Description, enter Username and password for MySQL DB.      1. Click **Next.**      1. Configure Rotation 2. Under Configure automatic rotation, move the slider to the right to turn on Automatic rotation. 3. Under Rotation schedule, ensure Schedule expression builder is selected and set the schedule:  * Time unit: Select Days. * Days: Enter 30.      1. Uncheck **Rotate immediately when the secret is stored** to ensure the next rotation follows your set schedule. 2. Under **Rotation function**, ensure that **Create a rotation function** is selected. 3. Next to SecretsManager, type in the listed default name (since a function name is required), and click **Next.** 4. Scroll down to review the settings, and click **Store.**      1. This process may take a few moments; you might need to refresh the page to see the secret. |

#### Task 2: Create a Reference to the Secret in the CloudFormation Template

|  |
| --- |
| 1. In the new tab's search bar at the top of the AWS portal, type and select CloudFormation.      1. Click on the stack name starting with cfst.      1. Click on the Resources tab and review the configuration. 2. Click on the Template tab and scroll down until you see the Database configuration portion; note the hardcoded username and password. 3. In the upper right corner, click on **Update**.      1. Under Prerequisite - Prepare template > Prepare template, select Edit in Application composer. 2. Under Edit template in Application Composer, click **Edit in Application Composer.**      1. Under template1, scroll down until you see the Database configuration. 2. Highlight MasterUsername: username and MasterUserPassword: password (lines 146 and 147) and replace with the following secrets code:   MasterUsername: '{{resolve:secretsmanager:NewDbSecrets:SecretString:username}}'  MasterUserPassword: '{{resolve:secretsmanager:NewDbSecrets:SecretString:password}}'  **Note:** If you need to, fix the spacing to ensure it aligns with the rest of the code. |

#### Task 3: Update CloudFormation Stack

|  |
| --- |
| 1. Navigate to the **Secrets Manager** tab. 2. In the upper right corner, click Store a new secret: Note that the resolve:secretsmanager:NewDbSecrets:SecretString: username/password string from the secrets code is pulling the RDS database user name and password listed. 3. Navigate back to **the AWS CloudFormation Designer** tab. 4. In the upper left corner, click on the Validate template icon (the checkmark icon). 5. Next to the checkmark icon, click on the **Create stack** icon. 6. Click **Next** until you get to the Review page.      1. Scroll down to Changes and confirm the database Replacement setting is set to True. 2. **Click Next;** the creation may take between 5-10 minutes.      1. After a few minutes, refresh the page until the UPDATE\_IN\_PROGRESS changes to CREATE\_COMPLETE.      1. Navigate to the Template tab and scroll down until you see the Database configuration portion. 2. Confirm the MasterUsername: username and MasterUserPassword: password was updated with the secrets code. 3. Navigate back to the Secrets Manager tab. 4. Click on **NewDbSecrets.** 5. Scroll down to the Rotation configuration section and verify that the Rotation schedule is set to 30 days and that the Lambda rotation function is active. |