Taller Autodirigido: Administración y Seguridad en MySQL

Contexto del Ejercicio

La administración y seguridad de bases de datos es un aspecto fundamental en cualquier sistema informático, ya que garantiza la integridad, disponibilidad y confidencialidad de la información. En este taller autodirigido, los estudiantes realizarán una serie de ejercicios prácticos para instalar y configurar MySQL, gestionar usuarios y permisos, aplicar medidas de seguridad y manejar técnicas de encriptación de datos.

A lo largo de este taller, asumirás el rol de un administrador de bases de datos en una empresa que necesita implementar un sistema seguro de gestión de información. Se te pedirá que instales MySQL, configures usuarios y privilegios adecuados, protejas el acceso a la base de datos, y apliques técnicas de encriptación para garantizar la seguridad de los datos sensibles.

Objetivo

Al finalizar este taller, el estudiante será capaz de instalar y configurar MySQL, administrar usuarios y privilegios, aplicar medidas de seguridad y manejar técnicas de encriptación de datos.

Parte 1: Instalación y Configuración de MySQL

1. Descargar e instalar MySQL

Accede a la página oficial de MySQL: https://dev.mysql.com/downloads/

Descarga e instala MySQL Community Server.

Durante la instalación, configura la autenticación con contraseña segura y selecciona MySQL Server como servicio.

2. Configuración inicial de MySQL

Define el usuario `root` con una contraseña segura.

Configura MySQL como un servicio en Windows para que se inicie automáticamente.

Ajusta los permisos en la carpeta de datos para restringir el acceso.

Verifica la instalación ejecutando el siguiente comando en MySQL:

```
SELECT VERSION();
```

Parte 2: Creación de Base de Datos y Tablas

1. Crear una Base de Datos

Ejecuta los siguientes comandos en MySQL:

```
CREATE DATABASE seguridad_mysql;
SHOW DATABASES;
USE seguridad_mysql;
```

2. Crear una Tabla de Usuarios

Dentro de la base de datos `seguridad_mysql`, ejecuta:

```
CREATE TABLE usuarios (
   id INT AUTO_INCREMENT PRIMARY KEY,
   nombre VARCHAR(50),
   email VARCHAR(100),
   password_hash VARCHAR(255)
);
```

Parte 3: Gestión de Usuarios y Privilegios

1. Crear un Usuario con Permisos Limitados

Ejecuta el siguiente comando para crear un usuario:

```
CREATE USER 'adminuser'@'localhost' IDENTIFIED BY 'Admin123!';
```

2. Asignar Privilegios

Otorga permisos sobre la base de datos `seguridad_mysql`:

```
GRANT SELECT, INSERT, UPDATE ON seguridad_mysql.* TO 'adminuser'@'localhost';
```

Verifica los privilegios del usuario:

```
SHOW GRANTS FOR 'adminuser'@'localhost';
```

Para eliminar permisos:

```
REVOKE INSERT, UPDATE ON seguridad_mysql.* FROM 'adminuser'@'localhost';
```

Para eliminar un usuario:

```
DROP USER 'adminuser'@'localhost';
```

Parte 4: Seguridad en Bases de Datos

1. Habilitar autenticación segura

Verifica el método de autenticación de los usuarios:

SELECT user, host, plugin FROM mysql.user;

2. Configurar el Firewall de MySQL

Bloquea accesos remotos no deseados en Windows:

New-NetFirewallRule -DisplayName "Bloquear MySQL 3306" -Direction Inbound -Protocol TCP -LocalPort 3306 -Action Block

Parte 5: Manejo de Contraseñas y Encriptación

1. Almacenar Contraseñas de Forma Segura

Inserta una contraseña encriptada usando `SHA2`:

INSERT INTO usuarios (nombre, email, password_hash)
VALUES ('usuario1', 'usuario1@example.com', SHA2('MiClaveSegura!', 256));

Evaluación del Taller

1. ¿Qué aprendiste en cada sección del taller?

2. ¿Qué dificultades encontraste y cómo las resolviste?

3. ¿Qué medidas de seguridad adicionales aplicarías en un entorno empresarial real?