

Resumen tema 5: SQL como DCL.

1. Introducción al Lenguaje de Control de Datos (DCL):

- **Definición:**

El DCL (Data Control Language) es un conjunto de comandos de SQL proporcionados por los sistemas gestores de bases de datos (SGBD) para gestionar el acceso y control de datos.

- **Objetivo principal:** Administrar usuarios, roles y privilegios en bases de datos multiusuario.

- **Comandos principales:**

- **GRANT:** Permite conceder permisos específicos a usuarios o roles para ejecutar operaciones como lectura, escritura o modificación.
- **REVOKE:** Revoca permisos previamente concedidos.

2. Usuarios y Límites de Uso:

- **Usuarios en el catálogo de MySQL:**

- Los usuarios se gestionan mediante la tabla `mysql.user`, donde se almacenan los privilegios, hashes de contraseñas y configuraciones de seguridad.
- Comandos relevantes:
 - **SELECT * FROM mysql.user;** : Consulta usuarios y sus detalles.
 - **SHOW GRANTS FOR [usuario];** : Muestra los privilegios asignados a un usuario.

- **Creación y eliminación de usuarios:**

- **Crear usuario:** `CREATE USER usuario@servidor IDENTIFIED BY 'contraseña';`
- **Eliminar usuario:** `DROP USER usuario;`
 - **Nota:** Antes de eliminar un usuario, es importante gestionar los objetos que haya creado para evitar que queden huérfanos.

- **Limitaciones de uso:**

- Parámetros configurables para evitar abusos o ataques de denegación de servicio:
 - **MAX_QUERIES_PER_HOUR:** Número de consultas por hora.
 - **MAX_UPDATES_PER_HOUR:** Número de actualizaciones por hora.
 - **MAX_CONNECTIONS_PER_HOUR:** Conexiones máximas por hora.
 - **MAX_USER_CONNECTIONS:** Conexiones simultáneas permitidas.
 - **MAX_STATEMENT_TIME:** Tiempo máximo de ejecución de sentencias.
- **Seguridad adicional:**
 - **FAILED_LOGIN_ATTEMPTS** y **PASSWORD_LOCK_TIME:** Configuran bloqueo de cuentas tras intentos fallidos.
 - **PASSWORD_EXPIRE_INTERVAL:** Fuerza el cambio periódico de contraseñas.

3. Gestión de Privilegios:

- **Tipos de privilegios en MySQL:**

- **Administrativos:** Aplican globalmente al servidor (e.g., `ALL PRIVILEGES`, `CREATE USER`).
- **De base de datos:** Permisos específicos sobre una base de datos (e.g., `SELECT`, `INSERT`).
- **De objetos:** Aplica a tablas, vistas, índices, etc. (e.g., `ALTER`, `REFERENCES`).

- **Asignación de privilegios:**

- **Comando GRANT:**
`GRANT tipo_privilegio ON base_datos.tabla TO usuario;`
 - **WITH GRANT OPTION:** Permite al usuario otorgar sus privilegios a otros (restringir su uso para evitar problemas de seguridad).
 - **FLUSH PRIVILEGES:** Actualiza los permisos aplicados.
- **Revocación de privilegios:**
 - **Comando REVOKE:**
`REVOKE tipo_privilegio ON base_datos.tabla FROM usuario;`

4. Grupos de Permisos y Límites (Roles y Perfiles):

- **Roles:**
 - Un rol es una agrupación de privilegios que facilita la administración.
 - **Creación y gestión:**
 - Crear un rol:
`CREATE ROLE nombre_rol;`
 - Asignar privilegios a un rol:
`GRANT privilegio ON base_datos.tabla TO nombre_rol;`
 - Asignar roles a usuarios:
`GRANT nombre_rol TO usuario;`
- **Perfiles:**
 - Configuraciones avanzadas que establecen límites como tiempo de conexión, número máximo de consultas y uso de memoria.
 - **Nota:** Los perfiles no están disponibles en la versión comunitaria de MySQL, como la incluida en XAMPP.

Ejemplos Prácticos Incluidos en el Documento:

1. Crear un usuario con limitaciones específicas:
`CREATE OR REPLACE USER usuario@localhost IDENTIFIED BY 'contraseña'
WITH MAX_USER_CONNECTIONS 5
MAX_UPDATES_PER_HOUR 50;`
2. Crear un usuario con caducidad de contraseña:
`CREATE OR REPLACE USER usuario IDENTIFIED BY 'contraseña'
PASSWORD EXPIRE INTERVAL 90 DAY;`
3. Modificar restricciones de un usuario:
`ALTER USER usuario@localhost WITH MAX_USER_CONNECTIONS 50;`
4. Retirar caducidad de contraseñas:
`ALTER USER usuario@localhost PASSWORD EXPIRE NEVER;`