Actividad noviembre 19 de 2024

Estructura del Taller

1. Conceptos básicos

Antes de comenzar, repasa estos conceptos:

* + Usuario: Identidad que se conecta a la base de datos.
  + Permisos: Conjunto de reglas que determinan qué puede hacer un usuario.
  + Rol: Grupo de permisos que se puede asignar a varios usuarios.
  + Host: Define desde dónde puede conectarse un usuario (local o remoto).

1. Ejercicios prácticos (teóricos)

Sigue los pasos con atención para imaginar o planificar cómo configurarías cada escenario.

Parte 1: Crear usuarios

Actividad 1: Crear usuarios con diferentes restricciones

Crea un usuario local (analista) que solo pueda conectarse desde el servidor.

**CREATE USER ‘analista’@’localhost’ IDENTIFIED BY ‘analista123’;**

Pregunta: ¿Por qué usarías localhost en lugar de %?

**Porque con el localhost se restringe a que solo se pueda conectar desde el localhost (servidor local) a la base de datos, en cambio con el % se declara que se puede conectar a la base de datos desde cualquier servidor, lo cual representa un riesgo de seguridad para la base de datos.**

Crea un usuario remoto (remoto) que pueda conectarse desde cualquier lugar.

Pregunta: ¿Qué riesgos puede tener esta configuración?

**CREATE USER ‘remoto’@’%’ IDENTIFIED BY ‘remoto123’;**

Parte 2: Otorgar permisos

Actividad 2: Permitir acceso limitado

Permitir al usuario analista consultar datos de una tabla específica (empleados).

**GRANT SELECT ON base\_de\_datos.empleados TO ‘analista’@’localhost’;**

Permitir al usuario remoto insertar y consultar datos.

**GRANT SELECT, INSERT ON base\_de\_datos.table TO ‘remoto’@’%’;**

Restricción adicional: Revoca el permiso de inserción al usuario remoto.

**REVOKE INSERT ON base\_de\_datos.table FROM 'remoto'@'%';**

Pregunta: ¿Qué sucede si remoto intenta insertar datos después de revocar el permiso?

**El usuario remoto no va a tener el permiso de insertar datos en la tabla.**

Parte 3: Uso de roles

Actividad 3: Crear y asignar roles

Crea un rol llamado lectura\_escritura con permisos para leer e insertar en cualquier tabla

**CREATE ROLE ‘lectura\_escritura’ ;**

**GRANT SELECT, INSERT ON \*.\* TO ‘lectura\_escritura’;**

Asigna el rol lectura\_escritura al usuario remoto.

**GRANT ‘lectura\_escritura’ TO ‘remoto’@’%’;**

Pregunta: Si eliminamos el rol, ¿los permisos del usuario remoto se mantienen?

**Si se elimina el rol también se eliminan los permisos al usuario, ya que se eliminan para todos los usuarios que se les haya asignado ese rol.**

Parte 4: Políticas avanzadas (conceptual)

Configura seguridad por filas: Imagina que solo deseas que analista pueda ver empleados con salarios menores a 6000.

Política conceptual:

CREATE POLICY analista\_policy ON empleados

FOR SELECT TO analista

USING (salario < 6000);

Pregunta: ¿Qué registros esperas que pueda ver analista después de aplicar esta política?

**El analista espera ver los registros en los cuales el salario sea menor a 6000.**