

Instituto Politécnico Nacional

Escuela Superior de Cómputo

Materia: Bases de Datos

Grupo: 2CM6

Profesora: Erika Hernández Rubio

Alumnos:

Juan Daniel Castillo Reyes

Javier Said Naranjo Miranda

Práctica 9 "Permisos"

Contents

1	Introducción	1
2	Querys	3
3	Conclusión	4

1 Introducción

Para conservar la integridad de los datos y de las estructuras será conveniente que sólo algunos usuarios puedan realizar determinadas tareas, y que otras, que requieren mayor conocimiento sobre las estructuras de bases de datos y tablas, sólo puedan realizarse por un número limitado y controlado de usuarios.

Los conceptos de usuarios y privilegios están íntimamente relacionados.

No se pueden crear usuarios sin asignarle al mismo tiempo privilegios. De hecho, la necesidad de crear usuarios está ligada a la necesidad de limitar las acciones que tales usuarios pueden llevar a cabo.

MySQL permite definir diferentes usuarios, y además, asignar a cada uno determinados privilegios en distintos niveles o categorías de ellos.

En MySQL existen cinco niveles distintos de privilegios:

1. **Globales:** se aplican al conjunto de todas las bases de datos en un servidor. Es el nivel más alto de privilegio, en el sentido de que su ámbito es el más general.

2. **De base de datos:** se refieren a bases de datos individuales, y por extensión, a todos los objetos que contiene cada base de datos.
3. **De tabla:** se aplican a tablas individuales, y por lo tanto, a todas las columnas de esas tabla.
4. **De columna:** se aplican a una columna en una tabla concreta.
5. **De rutina:** se aplican a los procedimientos almacenados. Aún no hemos visto nada sobre este tema, pero en MySQL se pueden almacenar procedimientos consistentes en varias consultas SQL

Aunque en la versión 5.0.2 de MySQL existe una sentencia para crear usuarios(CREATE USER), en versiones anteriores se usa exclusivamente la sentencia GRANT para crearlos. La sintaxis simplificada que usaremos para GRANT es :

```
GRANT priv_type [(column_list)] [, priv_type [(column_list)]] ...
ON
TO user [IDENTIFIED BY [PASSWORD] 'password']
    [, user [IDENTIFIED BY [PASSWORD] 'password']] ...
```

Se muestra una lista de los posibles privilegios que puede tener un usuario.

1. **ALL PRIVILEGES:** Permite a un usuario de MySQL acceder a todas las bases de datos asignadas en el sistema.
2. **CREATE:** Permite crear nuevas tablas o bases de datos.
3. **DROP:** permite eliminar tablas o bases de datos.
4. **DELETE:** permite eliminar registros de tablas.
5. **INSERT:** permite insertar registros en tablas.
6. **SELECT:** permite leer registros en las tablas.
7. **UPDATE:** permite actualizar registros seleccionados en tablas.
8. **GRANT OPTION:** permite remover privilegios de usuarios.

Para revocar los privilegios se usa la sentencia REVOKE.

A continuación se muestra su sintaxis.

```
REVOKE priv_type [(column_list)] [, priv_type [(column_list)]] ...
ON
FROM user [, user] ...
```

Para eliminar usuarios se usa la sentencia DROP USER.

No se puede eliminar un usuario que tenga privilegios, es necesario revocar los privilegios antes de eliminar al usuario.

2 Querys

Código de la práctica de permisos

```
create database emprensa;  
use emprensa;
```

```
create database samss;  
use samss;  
desc club;
```

```
select user from mysql.user;  
create user 'ana'@'localhost' IDENTIFIED BY 'pato';
```

```
#punto 1  
grant all on sams.*To ana@localhost identified by 'pato';  
#punto 2  
grant all on sams.*To pedro@localhost identified by 'cuarzo';  
#punto 3  
grant all on sams.*To mary@localhost identified by 'diamante';  
#punto 4  
grant all on *.* to felipe@localhost identified by 'topaz' with grant option;  
#punto 5  
grant update(nombre, direccion, tel) on samss.club to asistente@localhost identified by  
#punto 6  
#primero usar database mysql  
revoke all on *.* from felipe@localhost;  
mysql -u -root -p root  
delete from user where user='felipe' and Host='localhost';  
flush privileges
```

```
#punto 7  
set password for ana@localhost = password("naranja");
```

```
#punto 8  
grant select on samss.*To fulano@localhost identified by 'lagarto';
```

```
#punto 9  
grant update on samss.club to sutano@localhost identified by 'lagartito';  
grant insert on samss.socio to sutano@localhost;
```

```
#punto 10  
cd C:\Program Files\MySQL\MySQL Server 5.6\bin  
mysqladmin ping
```

3 Conclusión

Los permisos son un elemento fundamental dentro de las bases de datos, ya que protegen la integridad de nuestros datos, además son considerados como uno de los niveles más básicos de seguridad dentro de un sistema informático.

Dentro de una organización permite delegar responsabilidades al momento de manipular una BD sin comprometer la información resguardada, la creación de usuarios es un proceso que todo administrador de bases de datos debe realizar de manera adecuada. Actualmente existen muchos SGBD con soporte para diferentes usuarios realizando conexiones a ellos, a tal grado que sistemas como PostgreSQL tiene todo un framework dedicado a la creación de usuarios y de permisos asignados a ellos.

Diferentes tipos de usuarios con diferentes permisos aparecerán casi siempre en cualquier base de datos por lo que la manipulación de estas técnicas estará presente en muchas ocasiones.