



Técnico en
< DESARROLLO DE SOFTWARE >

Bases de Datos III

(CC BY-NC-ND 4.0)
International

Attribution-NonCommercial-NoDerivatives 4.0



Atribución

Usted debe reconocer el crédito de una obra de manera adecuada, proporcionar un enlace a la licencia, e indicar si se han realizado cambios. Puede hacerlo en cualquier forma razonable, pero no de forma tal que sugiera que tiene el apoyo del licenciante o lo recibe por el uso que hace.



No Comercial

Usted no puede hacer uso del material con fines comerciales.



Sin obra derivada

Si usted mezcla, transforma o crea un nuevo material a partir de esta obra, no puede distribuir el material modificado.

No hay restricciones adicionales - Usted no puede aplicar términos legales ni medidas tecnológicas que restrinjan legalmente a otros hacer cualquier uso permitido por la licencia.

<http://creativecommons.org/licenses/by-nc-nd/4.0/>



Bases de Datos III

Unidad I

1. Gestiones sobre usuarios

MySQL implementa un sistema de control de acceso y privilegios sofisticados que le permite crear reglas integrales para el manejo de las operaciones del usuario, previniendo eficazmente el ingreso de usuarios no autorizados al sistema de base de datos.

El control de acceso de MySQL tiene dos etapas, cuando un usuario se conecta al servidor:

Verificación de Conexión: un usuario cada vez que se conecta al servidor de base de datos MySQL, necesita tener un usuario y contraseña válidos. Además, el host desde el que se conecta el cliente tiene que coincidir con el host ubicado en la tabla de permisos de MySQL.

Verificación de la Petición: una vez que se ha establecido correctamente una conexión, por cada declaración emitida por el cliente, MySQL comprueba si el cliente tiene suficientes privilegios para ejecutar esa declaración particular. MySQL tiene capacidad de comprobar un privilegio en la base de datos, tabla, y a nivel de campos entre otros.

En nuestro motor de base de datos existe una base de datos llamada mysql la cual es creada automáticamente por el instalador de MySQL. La base de datos mysql contiene cinco tablas de permisos principales. A menudo la manipulación de estas tablas se realiza indirectamente a través de los comandos **GRANT** y **REVOKE**.

Estas tablas son:

Tabla User: contiene la cuenta de usuario y columnas de sus privilegios globales. MySQL utiliza la tabla de usuario para aceptar o rechazar una conexión desde un host. Un privilegio otorgado en la tabla de usuario es eficaz para todas las bases de datos en el servidor MySQL.

Tabla db: contiene privilegios al nivel de la base de datos. MySQL utiliza la tabla db para determinar a qué base de datos un usuario puede acceder y desde que host lo puede realizar. Un privilegio otorgado a nivel de base de datos en la tabla db se aplica a todas las base de datos y todos los objetos pertenecientes a esa base de datos, por ejemplo, tablas, triggers, vistas, procedimientos almacenados, etc.

Table_priv y columns_priv: contiene los privilegios a nivel de tablas y privilegios a nivel de columnas. Un privilegio otorgado en la tabla table_priv aplica a la tabla y sus columnas, mientras que un privilegio otorgado en la tabla columns_priv sólo se aplica a una columna específica de una tabla.

Procs_priv: contiene los privilegios necesarios para el uso de funciones almacenadas y procedimientos almacenados.

1.1. Creación de cuentas de usuarios

En MySQL, puede especificar no sólo que puede conectarse a un servidor de base de datos, sino también de dónde. Por lo tanto una cuenta en MySQL se compone de nombre de usuario y el nombre de host en el que el usuario se conecta desde que se separó por @. Por ejemplo, si el usuario root se conecta desde el host mysqlgalileo.edu al servidor de base de datos, el nombre de la cuenta sería root@mysqlgalileo.edu.

Esto le permite configurar múltiples cuentas con el mismo nombre pero se conecta desde diferentes hosts y tienen diferentes privilegios. Además, usted tiene el control de la configuración de cuentas para conectarse desde alguna en específico o un conjunto amplio de host. El nombre de usuario y el host se almacenan en la tabla de permisos con el nombre del usuario.

Creación de cuentas mediante la sentencia “create user”

MySQL proporciona la sentencia CREATE USER para permitirle crear un nuevo usuario en un servidor de base de datos. La sintaxis de la sentencia CREATE USER es el siguiente:

```
CREATE USER user IDENTIFIED BY password
```

La cuenta de usuario con el formato 'nombre de usuario' @ 'host' es seguido por el nombre de usuario a crear, también se especifica la contraseña después de la cláusula IDENTIFIED BY. La contraseña debe ser en texto plano. MySQL cifrará la contraseña para usted cuando almacene los datos en la tabla usuario.

Por ejemplo, para crear un nuevo usuario dbadmin que se conecta desde localhost con la contraseña CrEate-User, se utiliza la sentencia CREATE USER de la siguiente manera:

```
1 CREATE USER dbadmin@localhost
2 IDENTIFIED BY 'CrEate-User'
```

Para permitir al usuario conectarse desde cualquier host se utiliza el símbolo %.

```
1 CREATE USER superadmin@%'
2 IDENTIFIED BY 'Secured'
```

El símbolo de porcentaje % tiene el mismo efecto cuando se utiliza por ejemplo con el operador LIKE, para permitir al usuario mysqladmin conectase desde cualquier host que utiliza mysqltutorial.org, el uso del símbolo de porcentaje es de la siguiente manera:

```
1 CREATE USER mysqladmin@'%.mysqltutorial.org'
2 IDENTIFIED by 'SecurePass704';
```

Creación de cuentas mediante la sentencia “insert”

Una forma menos común de crear usuarios es mediante la sentencia INSERT para insertar un nuevo registro en la tabla de permisos con el nombre del usuario. De esta manera, usted necesita utilizar la función de contraseña para cifrar la contraseña antes de insertar el registro en la tabla. Vea el siguiente ejemplo:

```
1 INSERT INTO user (host,user,password)
2 VALUES('localhost','dbadmin',PASSWORD('CrEate-User'));
```

1.2. Cambio de contraseña

Los cambios de contraseña en MySQL se pueden llevar a cabo de manera fácil y rápida únicamente hay que tomar en cuenta los siguientes aspectos:

- ¿Qué usuario utilizara para cambiar la contraseña?
- ¿Te has enterado de las aplicaciones relacionadas que actualmente están utilizando la cuenta MySQL cuya contraseña se está cambiando?
- Si cambia la contraseña sin una planificación adecuada, las aplicaciones van a perder la conexión con la base de datos y dejar de funcionar correctamente.

MySQL proporciona varias declaraciones que usted puede utilizar para cambiar o restablecer la contraseña de una cuenta de MySQL incluyendo la instrucción UPDATE, la sentencia SET PASSWORD y el comando GRANT USAGE.

Cambio de contraseña mediante la sentencia “update”

La primera forma de cambiar la contraseña es utilizar la instrucción UPDATE para actualizar la columna de usuario y host de la tabla de usuario ubicada en la base de datos mysql. Después de ejecutar la sentencia UPDATE, es necesario ejecutar la sentencia FLUSH PRIVILEGES para recargar los privilegios de la tabla de permisos en la base de datos mysql.

```
1 USE mysql;
2
3 UPDATE user
4 SET password = PASSWORD('Secret1970')
5 WHERE user = 'mysqltutorial' AND
6       host = 'mysqltutorial.org';
7
8 FLUSH PRIVILEGES;
```

Cambio de contraseña mediante la sentencia “set password”

La segunda forma de cambiar la contraseña es utilizando la sentencia SET PASSWORD. Utilizar la cuenta de MySQL en formato usuario @ host para actualizar la contraseña. Si necesita cambiar la contraseña de otras cuentas, es necesario tener al menos privilegios de UPDATE. No es necesario ejecutar la sentencia FLUSH PRIVILEGES para recargar privilegios de tabla de permisos.

```
1 SET PASSWORD FOR 'mysqltutorial'@'mysqltutorial.org' = PASSWORD('Secret1970');
```

Cambio de contraseña mediante la sentencia “grant usage”

La tercera forma de cambiar la contraseña es mediante la sentencia GRANT USAGE utilizando la sentencia IDENTIFIED BY. De este modo, se especifica la contraseña en texto plano en lugar del modo cifrado.

La siguiente declaración cambia la contraseña de la cuenta tutorial mysql utilizando la sentencia GRANT USAGE:

```
1 GRANT USAGE ON *.* TO mysqltutorial@mysqltutorial.org IDENTIFIED BY Secret1970
```


NOTA: En caso de que quiera restablecer la contraseña de la cuenta root de MySQL, es necesario reiniciar el servidor de base de datos MySQL, sin necesidad de utilizar la validación tabla de permisos

2. Privilegios

2.1. Asignar privilegios a usuarios

MySQL proporciona la sentencia GRANT MySQL que le permite otorgar privilegios de acceso a las cuentas de base de datos.

A continuación se muestra la sintaxis de la sentencia GRANT:

```
1 GRANT privileges (column_list)
2 ON [object_type] privilege_level
3 TO account [IDENTIFIED BY 'password']
4 [REQUIRE encryption]
5 WITH with_options
```

Ejemplos:

```
1 CREATE USER 'super'@'localhost' IDENTIFIED BY 'SecurePass1';
2
3 GRANT ALL ON *.* TO 'super'@'localhost' WITH GRANT OPTION;
```

La sentencia ON *.* significa todas las bases de datos y todos los objetos de las bases de datos. La única limitación del usuario super es que sólo se puede conectar con el servidor de base de datos del host local, que hace que el servidor MySQL sea más seguro.

También puede otorgar múltiples privilegios utilizando una sola sentencia GRANT. Por ejemplo, puede crear un usuario que puede ejecutar instrucciones INSERT, UPDATE y SELECT en la base de datos muestra los modelos clásicos con las siguientes declaraciones:

```
1 CREATE USER 'rfc'@'%' IDENTIFIED BY 'SecurePass3';
2
3 GRANT SELECT, UPDATE, DELETE ON classicmodels.* TO 'rfc'@'%';
```

En la siguiente tabla se muestran los privilegios que podemos utilizar en MySQL.

Privilege	Description
ALL [PRIVILEGES]	Grant all privileges at specified access level except GRANT OPTION
ALTER	Allow to use of ALTER TABLE statement
ALTER ROUTINE	Allow user to alter or drop stored routine
CREATE	Allow user to create database and table
CREATE ROUTINE	Allow user to create stored routine
CREATE TABLESPACE	Allow user to create, alter or drop tablespaces and log file groups
CREATE TEMPORARYTABLES	Allow user to create temporary table by using CREATE TEMPORARY TABLE

Privilege	Description
CREATE USER	Allow user to use the CREATE USER, DROP USER, RENAME USER, and REVOKE ALL PRIVILEGES statements.
CREATE VIEW	Allow user to create or modify view
DELETE	Allow user to use DELETE
DROP	Allow user to drop database, table and view
EVENT	Allow user to schedule events in Event Scheduler
EXECUTE	Allow user to execute stored routines
FILE	Allow user to read any file in the database directory.
GRANT OPTION	Allow user to have privileges to grant or revoke privileges from other accounts
INDEX	Allow user to create or remove indexes.
INSERT	Allow user to use INSERT statement
LOCK TABLES	Allow user to use LOCK TABLES on tables for which you have the SELECT privilege
PROCESS	Allow user to see all processes with SHOW PROCESSLIST statement.
PROXY	Enable user proxying
REFERENCES	Not implemented

Privilege	Description
RELOAD	Allow user to use FLUSH operations
REPLICATION CLIENT	Allow user to query to see where master or slave servers are
REPLICATION SLAVE	Allow user to use replicate slaves to read binary log events from the master.
SELECT	Allow user to use SELECT statement
SHOW DATABASES	Allow user to show all databases
SHOW VIEW	Allow user to use SHOW CREATE VIEW statement
SHUTDOWN	Allow user to use mysqladmin shutdown command
SUPER	Allow user to use other administrative operations such as CHANGE MASTER TO, KILL, PURGE BINARY LOGS, SET GLOBAL, and mysqladmin command
TRIGGER	Allow user to use TRIGGER operations.
UPDATE	Allow user to use UPDATE statement
USAGE	Equivalent to “no privileges”

2.2. Revocar privilegios a usuarios

Con el fin de revocar los privilegios de una cuenta, se utiliza la sentencia REVOKE. La sintaxis de declaración REVOKE es la siguiente:

```
1 REVOKE    privilege_type [(column_list)]    [, priv_type [(column_list)]]...
2 ON [object_type] privilege_level
3 FROM user [, user]...
```

Ejemplos:

Mostramos los privilegios que tiene un usuario.

```
1 SHOW GRANTS FOR 'rfc'@'localhost';
```

Se puede revocar el privilegio de UPDATE (actualizar datos) y DELETE (eliminar datos) de la cuenta rfc de la siguiente manera:

```
1 REVOKE UPDATE, DELETE ON classicmodels.* FROM 'rfc'@'localhost';
```

Podemos también quitar todos los privilegios que tiene el usuario rfc realizándolo de la siguiente forma:

```
1 REVOKE ALL PRIVILEGES, GRANT OPTION FROM 'rfc'@'localhost';
```

NOTA: El efecto de la declaración MySQL REVOKE depende del nivel de privilegio, tomando en cuenta las siguientes afirmaciones.

- Los cambios que se hacen a los privilegios globales sólo tienen efecto cuando el cliente se conecta al MySQL en las sesiones posteriores. Los cambios no se aplican a todas las cuentas vinculadas actuales.
- Se aplica el cambio de los privilegios de base de datos después de la siguiente instrucción USE.

- Cambios de tablas y columnas de privilegios se aplican a todas las consultas que se emiten después de realizar los cambios.

Referencias:

- <http://dev.mysql.com/doc/refman/5.1/en/user-names.html>
- <http://dev.mysql.com/doc/refman/5.1/en/adding-users.html>
- <http://dev.mysql.com/doc/refman/5.1/en/removing-users.html>
- <http://dev.mysql.com/doc/refman/5.1/en/user-resources.html>
- <http://dev.mysql.com/doc/refman/5.1/en/assigning-passwords.html>
- <http://dev.mysql.com/doc/refman/5.1/en/grant-table-structure.html>
- <http://dev.mysql.com/doc/refman/5.1/en/mysqldump.html>

Base de datos de ejemplo

- <http://www.mysqltutorial.org/mysql-sample-database.aspx>

Descargo de responsabilidad

La información contenida en este documento descargable en formato PDF o PPT es un reflejo del material virtual presentado en la versión online del curso. Por lo tanto, su contenido, gráficos, links de consulta, acotaciones y comentarios son responsabilidad exclusiva de su(s) respectivo(s) autor(es) por lo que su contenido no compromete al área de e-Learning del Departamento GES o al programa académico al que pertenece.

El área de e-Learning no asume ninguna responsabilidad por la actualidad, exactitud, obligaciones de derechos de autor, integridad o calidad de los contenidos proporcionados y se aclara que la utilización de este descargable se encuentra limitada de manera expresa para los propósitos educacionales del curso.

