User & Privilege Access

Adaptation of the lecture of Mr. Heng Sotharith

Content

- Privileges provided by MySQL
- Grant command
- Revoke command
- Create user command
- Set password command
- Drop user command
- Rename user command

Privileges provided by MySQL

- Level of operation for privilege
  - Administrative privilege: for managing operations of MySQL server.
  - Database privilege: privileges apply to database and its objects.
  - Privilege for database objects (tables, indexes, views, and stored routines): privileges apply to objects of a database.

Privileges provided by MySQL

- Information about account privileges is stored in the user, db, host, tables_priv, columns_priv, and procs_priv tables in the mysql database.

Privilege	Grant Table Column	Context
ALL [PRIVILEGES]	Synonym for "all privileges"	Server administration
ALTER	Alter_priv	Tables
ALTER ROUTINE	Alter_routine_priv	Stored routines
CREATE	Create_priv	Databases, tables, or indexes
CREATE ROLE	Create_role_priv	Server administration
CREATE ROUTINE	Create_routine_priv	Stored routines
CREATE TABLESPACE	Create_tablespace_priv	Server administration
CREATE TEMPORARY TABLES	Create_tmp_table_priv	Tables
CREATE USER	Create_user_priv	Server administration
CREATE VIEW	Create_view_priv	Views
DELETE	Delete_priv	Tables
DROP	Drop_priv	Databases, tables, or views

Privileges provided by MySQL (cont.)

Privilege	Grant Table Column	Context
DROP ROLE	Drop_role_priv	Server administration
EVENT	Event_priv	Databases
EXECUTE	Execute_priv	Stored routines
FILE	File_priv	File access on server host
GRANT OPTION	Grant_priv	Databases, tables, or stored routines
INDEX	Index_priv	Tables
INSERT	Insert_priv	Tables or columns
LOCK TABLES	Lock_tables_priv	Databases
PROCESS	Process_priv	Server administration
PROXY	See proxies_priv table	Server administration
REFERENCES	References_priv	Databases or tables
RELOAD	Reload_priv	Server administration
REPLICATION CLIENT	Repl_client_priv	Server administration
REPLICATION SLAVE	Repl_slave_priv	Server administration
SELECT	Select_priv	Tables or columns

Privileges provided by MySQL (cont.)

Privilege	Grant Table Column	Context
SHOW DATABASES	Show_db_priv	Server administration
SHOW VIEW	Show_view_priv	Views
SHUTDOWN	Shutdown_priv	Server administration
SUPER	Super_priv	Server administration
TRIGGER	Trigger_priv	Tables
UPDATE	Update_priv	Tables or columns
USAGE	Synonym for “no privileges”	Server administration

Grant command

- To grant privilege to MySQL account.
- Create account if it is not exist.
- To execute this command, user must have global **GRANT** privilege and the privilege that you are granting.

Syntax:

GRANT *priv_type* [(*column_list*)] [, *priv_type* [(*column_list*)]] ...
ON [*object_type*] {*tbl_name* | * | *.* | *db_name*.*}
TO *user* [IDENTIFIED BY [PASSWORD] '*password*']
[, *user* [IDENTIFIED BY [PASSWORD] '*password*']] ...
[REQUIRE NONE | [{SSL| X509}] [CIPHER '*cipher*' [AND]] [ISSUER '*issuer*' [AND]] [SUBJECT '*subject*']]
[WITH *with_option* [*with_option*] ...]

Grant command (cont.)

- ***Global Privilege:***

  - Privileges are administrative or apply to all database on a given server.
  - These privileges are store in the **mysql.user** table.

Example:

```
GRANT ALL ON *.* TO 'someuser'@'somehost';
GRANT SELECT, INSERT ON *.* TO 'someuser'@'somehost';
GRANT USAGE ON *.* TO 'jeffrey'@'localhost' WITH
                    MAX_QUERIES_PER_HOUR 90;
```

Grant command (cont.)

- ***Database Privilege:***

  - Privileges are apply to all objects in a given database.
  - Theses privileges are stored in **mysql.db** tables.

Example:

```
GRANT ALL ON mydb.* TO 'someuser'@'somehost';
GRANT SELECT, INSERT ON mydb.* TO 'someuser'@'somehost';
```

Grant command (cont.)

- ***Table Privilege:***
  - Privileges are apply to all column in a given table.
  - Theses privileges are stored in **mysql.tables_priv** table.

Priv_type:

SELECT, INSERT, UPDATE, DELETE, CREATE, DROP, INDEX, ALTER, GRANT OPTION.

Example:

```
GRANT ALL ON mydb.mytbl TO 'someuser'@'somehost';
GRANT SELECT, INSERT ON mydb.mytbl TO
'someuser'@'somehost';
```

Grant command (cont.)

- ***Column Privilege:***
  - Privileges are apply to a single column in a given table.
  - Theses privileges are stored in **mysql.column_priv** table.

Priv_type:

SELECT, INSERT, UPDATE

Example:

GRANT SELECT (col1), INSERT (col1,col2) ON mydb.mytbl TO 'someuser'@'somehost';

Grant command (cont.)

- ***Routine Privilege:***

  - CREATE ROUTINE, ALTER ROUTINE, EXECUTE apply to stored routines.
  - Theses privileges can be granted at global and database level.
  - Theses privileges are stored in **mysql.procs_priv** table.

Example:

```
GRANT ALTER ROUTINE ON mydb.* TO 'someuser'@'somehost';
```

Grant command (cont.)

- ***Setting resource limit*** : limits for individual accounts on use of these server resources:

- The number of queries an account can issue per hour
- The number of updates an account can issue per hour
- The number of times an account can connect to the server per hour
- The number of simultaneous connections to the server by an account

Examples:

```
CREATE USER 'francis'@'localhost' IDENTIFIED BY 'frank'
WITH MAX_QUERIES_PER_HOUR 20
MAX_UPDATES_PER_HOUR 10
MAX_CONNECTIONS_PER_HOUR 5
MAX_USER_CONNECTIONS 2;
```

Or

```
ALTER USER 'jeffrey'@'localhost'
  WITH MAX_QUERIES_PER_HOUR 500 MAX_UPDATES_PER_HOUR 100;
```

Revoke command

- To revoke privilege from MySQL account.
- To use the first ***REVOKE*** syntax, you must have the ***GRANT OPTION*** privilege, and you must have the privileges that you are revoking.

Syntax:

REVOKE *priv_type* [(*column_list*)] [, *priv_type* [(*column_list*)]] ...
ON [*object_type*] {*tbl_name* | * | *.* | *db_name*.*}
FROM *user* [, *user*] ...

Revoke ALL command

- To revoke all privileges.
- To use this REVOKE syntax, you must have the global CREATE USER privilege or the UPDATE privilege for the mysql database.

Syntax:

REVOKE ALL PRIVILEGES, **GRANT OPTION** FROM *user* [, *user*] ...

Create user command

- MySQL account information are store *mysql* database.
- To use this command you need to have *create user* privilege
- It creates a new row in table *mysql.user* with no privilege

Syntax:

CREATE USER *user_specification* [, *user_specification*] ...

user_specification:

user [IDENTIFIED BY [PASSWORD] '***password***']

Create user command (cont.)

Example:

- No password:

CREATE USER 'jeffrey'@'localhost';

- Password required:

CREATE USER 'jeffrey'@'localhost' IDENTIFIED BY 'mypass';

- Or:

CREATE USER 'jeffrey'@'localhost' IDENTIFIED BY PASSWORD *90E462C37378CED12064BB3388827D2BA3A9B689';

- Assign password or set password with ALTER USER

ALTER USER 'jeffrey'@'localhost' IDENTIFIED BY

Set password command

- Assign password to an existing user account.
- Must have a ***UPDATE*** privilege for ***mysql*** database to run this command.
- With no "***For user***" clause, it sets password for current user. Any client who successfully connects to the server could run this command.
- Use ALTER USER instead

Syntax:

```
SET PASSWORD [FOR user] = {
        PASSWORD('cleartext password')
            | OLD_PASSWORD('cleartext password')
            | 'encrypted password'
        }
```

Set password command (cont.)

Example:
SET PASSWORD FOR 'bob'@'%.example.org' =
PASSWORD('cleartext password');
or
UPDATE mysql.user SET Password=PASSWORD('cleartext password')
WHERE User='bob' AND Host='%.example.org';
FLUSH PRIVILEGES;
or
GRANT USAGE ON *.* TO; 'bob'@'%.example.org' IDENTIFIED BY 'cleartext password'
Or
ALTER USER 'bob'@'%.example.org' IDENTIFIED BY 'cleartext password'

Drop user command

- To remove one or more MySQL account.
- To execute this command, user must have global **CREATE** or **DELETE** user privilege.

Syntax:

DROP USER *user* [, *user*] …

Example:

```
DROP USER 'jeffrey'@'localhost';
```

Rename user command

- To rename existing MySQL account.
- To execute this command, user must have global **CREATE** or **UPDATE** user privilege.

Syntax:

RENAME USER *old_user* **TO** *new_user* [, *old_user* TO *new_user*] ...

Example:

```
RENAME USER 'jeffrey'@'localhost' TO 'jeff'@'127.0.0.1';
```