Security

Nov 14, 2011

Chapter 21

http://dev.mysql.com/doc/refman/5.5/en/privilege-system.html

Security

- Secrecy
- Integrity
- Availablity

Security

- Security Policy

- Security mechanism
  - access rights
  - privileges

phpMyAdmin

User *'chadd'@'%'* : Edit Privileges

Global privileges (Check All / Uncheck All)

Note: MySQL privilege names are expressed in English

Data

- [x] SELECT
- [x] INSERT
- [x] UPDATE
- [x] DELETE
- [x] FILE

Structure

- [x] CREATE
- [x] ALTER
- [x] INDEX
- [x] DROP
- [x] CREATE TEMPORARY TABLES
- [x] CREATE VIEW
- [x] SHOW VIEW
- [x] CREATE ROUTINE
- [x] ALTER ROUTINE
- [x] EXECUTE

Administration

- [x] GRANT
- [x] SUPER
- [x] PROCESS
- [x] RELOAD
- [x] SHUTDOWN
- [x] SHOW DATABASES
- [x] LOCK TABLES
- [x] REFERENCES
- [x] REPLICATION CLIENT
- [x] REPLICATION SLAVE
- [x] CREATE USER

Also: Resource Limits

12.7.1.3. GRANT Syntax

http://dev.mysql.com/doc/refman/5.5/en/grant.html

```
GRANT
    priv_type [(column_list)]
      [, priv_type [(column_list)]] ...
    ON [object_type] priv_level
    TO user_specification [, user_specification] ...
    [REQUIRE {NONE | ssl_option [[AND] ssl_option] ...}]
    [WITH with_option ...]

with_option:
    GRANT OPTION
  | MAX_QUERIES_PER_HOUR count
  | MAX_UPDATES_PER_HOUR count
  | MAX_CONNECTIONS_PER_HOUR count
  | MAX_USER_CONNECTIONS count
```

Privilege	
ALL [PRIVILEGES]	Grant all privileges at specified access level except GRANT OPTION
ALTER	Enable use of ALTER TABLE
ALTER ROUTINE	Enable stored routines to be altered or dropped
CREATE	Enable database and table creation
CREATE ROUTINE	Enable stored routine creation
CREATE TABLESPACE	Enable tablespaces and log file groups to be created, altered, or dro
CREATE TEMPORARY TABLES	Enable use of CREATE TEMPORARY TABLE
CREATE USER	Enable use of CREATE USER, DROP USER, RENAME USER, and REVOI
CREATE VIEW	Enable views to be created or altered
DELETE	Enable use of DELETE
DROP	Enable databases, tables, and views to be dropped
EVENT	Enable use of events for the Event Scheduler
EXECUTE	Enable the user to execute stored routines
FILE	Enable the user to cause the server to read or write files
GRANT OPTION	Enable privileges to be granted to or removed from other accounts
INDEX	Enable indexes to be created or dropped
INSERT	Enable use of INSERT
LOCK TABLES	Enable use of LOCK TABLES on tables for which you have the SELEC
PROCESS	Enable the user to see all processes with SHOW PROCESSLIST

Examples

```
CREATE USER 'jeffrey'@'localhost' IDENTIFIED BY 'mypass';
GRANT ALL ON db1.* TO 'jeffrey'@'localhost';
GRANT SELECT ON db2.invoice TO 'jeffrey'@'localhost';
GRANT USAGE ON *.* TO 'jeffrey'@'localhost' WITH MAX_QUERIES_PER_HOUR 90;
```

```
create database PUNetID_test;

create USER 'PUNetID'@'%' IDENTIFIED BY 'XXXXXX';
grant all on PUNetID_test.* to 'PUNetID'@'%';
grant all on PUNetID_AssignmentOne.* to 'PUNetID'@'%';

grant SELECT on chadd_test.* to 'PUNetID'@'%';

grant FILE on *.* to 'PUNetID'@'%';

grant TRIGGER on PUNetID_test.* to 'PUNetID'@'%';

grant PROCESS on *.* to 'PUNetID'@'%';
```

Opposite of Grant...

12.5.1.5. REVOKE Syntax

```
REVOKE
    priv_type [(column list)]
      [, priv type [(column list)]] ...
    ON [object_type] priv_level
    FROM user [, user] ...

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

Other types of security

- Encryption
- SSL certificate
- Digital Signature