# Лабораторная работа 21. Привилегии MySQL

Цель: получение представления о системе привилегий пользователей MySQL.

Привилегии SELECT, INSERT, UPDATE и DELETE позволяют выполнять операции над строками таблиц баз данных.

Для операторов SELECT привилегия SELECT требуется только в том случае, если они действительно извлекают строки из таблицы..

Привилегия INDEX позволяет создавать или уничтожать (удалять) индексы.

Привилегия ALTER позволяет использовать команду ALTER TABLE.

Привилегии CREATE и DROP позволяют создавать новые базы данных и таблицы или уничтожать (удалять) существующие базы данных и таблицы. Заметим, что в случае, если пользователю предоставляется привилегия DROP по отношению к базе данных mysql, он может уничтожить базу данных, в которой хранятся привилегии доступа в MySQL!

Привилегия GRANT позволяет вам предоставлять другим пользователям привилегии, которыми обладаете вы сами.

Привилегия FILE дает вам право читать и записывать файлы на сервере с помощью операторов LOAD DATA INFILE и SELECT ... INTO OUTFILE. Любой пользователь, которому предоставлена такая привилегия, имеет право прочитать или записать любой файл, который может прочитать или записать сервер MySQL.

**Задание 1.** Запустить MySQL. Выполняя соответствующие команды (см. примеры табл. 1), определите, какие привилегии доступны для пользователя.

Таблица 1 – Привилегии

| Привилегия | Пример запроса |
| --- | --- |
| ALTER Alter\_priv | ALTER TABLE t1 CHANGE a b INTEGER; |
| DELETE Delete\_priv | DELETE FROM somelog WHERE user = 'jcole'; |
| INDEX Index\_priv | CREATE INDEX part\_of\_name ON customer (name(10)); |
| INSERT Insert\_priv | INSERT INTO tbl\_name (col1,col2) VALUES(col2\*2,15); |
| SELECT Select\_priv | (см. лабораторную работу в 5 семестре) |
| UPDATE Update\_priv | UPDATE persondata SET age=age\*2, age=age+1; |
| CREATE Create\_priv | CREATE TABLE t40 (c CHAR(20)); |
| DROP Drop\_priv | DROP TABLE t40; |
| GRANT Grant\_priv | (см. ниже) |
| FILE | LOAD DATA INFILE 'data.txt' INTO TABLE db2.my\_table; (надо сначала создать текстовый файл с данными, где поля разделены символами табуляции) |

Привилегия GRANT

Новых пользователей можно добавлять, используя команду GRANT:

GRANT ALL PRIVILEGES ON \*.\* TO monty@localhost

 IDENTIFIED BY 'some\_pass' WITH GRANT OPTION;

 GRANT ALL PRIVILEGES ON \*.\* TO monty@"%"

 IDENTIFIED BY 'some\_pass' WITH GRANT OPTION;

GRANT RELOAD,PROCESS ON \*.\* TO admin@localhost;

 GRANT USAGE ON \*.\* TO dummy@localhost;

Эти команды GRANT создают трех новых пользователей:

monty - Полноценный суперпользователь - он может подсоединяться к серверу откуда угодно, но должен использовать для этого пароль some\_pass. Обратите внимание на то, что надо применить операторы GRANT как для monty@localhost, так и для monty@"%". Если не добавить запись с localhost, запись анонимного пользователя для localhost, которая создается при помощи mysql\_install\_db, будет иметь преимущество при подсоединении с локального компьютера, так как в ней указано более определенное значение для поля Host, и она расположена раньше в таблице user.

admin - Пользователь, который может подсоединяться с localhost без пароля; ему назначены административные привилегии RELOAD и PROCESS. Эти привилегии позволяют пользователю запускать команды mysqladmin reload, mysqladmin refresh и mysqladmin flush-\*, а также mysqladmin processlist. Ему не назначено никаких привилегий, относящихся к базам данных (их можно назначить позже, дополнительно применив оператор GRANT).

dummy - Пользователь, который может подсоединяться к серверу без пароля, но только с локального компьютера. Все глобальные привилегии установлены в значение 'N'-тип привилегии USAGE, который позволяет создавать пользователей без привилегий. Предполагается, что относящиеся к базам данных привилегии будут назначены позже.

В приведенном ниже примере добавляется пользователь custom, который может подсоединяться с компьютеров localhost, server.domain и whitehouse.gov. Он хочет получать доступ к базе данных bankaccount только с компьютера localhost, к базе данных expenses - только с whitehouse.gov, и к базе данных customer - со всех трех компьютеров, а также использовать пароль stupid при подсоединении со всех трех компьютеров.

**Задание 2.**

Чтобы задать привилегии пользователя при помощи оператора GRANT, выполните следующие команды:

shell> mysql --user=root mysql

mysql> GRANT SELECT,INSERT,UPDATE,DELETE,CREATE,DROP

 -> ON bankaccount.\*

 -> TO custom@localhost

 -> IDENTIFIED BY 'stupid';

mysql> GRANT SELECT,INSERT,UPDATE,DELETE,CREATE,DROP

 -> ON expenses.\*

 -> TO custom@whitehouse.gov

 -> IDENTIFIED BY 'stupid';

mysql> GRANT SELECT,INSERT,UPDATE,DELETE,CREATE,DROP

 -> ON customer.\*

 -> TO custom@'%'

 -> IDENTIFIED BY 'stupid';

Привилегии для пользователя custom назначаются потому, что этот пользователь хочет получать доступ к MySQL как с локального компьютера через сокеты Unix, так и с удаленного компьютера whitehouse.gov через протокол TCP/IP.

**Задание 3.**

Чтобы задать привилегии пользователя путем непосредственного внесения изменений в таблицы назначения привилегий, выполните следующие команды (обратите внимание на команду FLUSH PRIVILEGES в конце примера):

shell> mysql --user=root mysql

mysql> INSERT INTO user (Host,User,Password)

 -> VALUES('localhost','custom',PASSWORD('stupid'));

mysql> INSERT INTO user (Host,User,Password)

 -> VALUES('server.domain','custom',PASSWORD('stupid'));

mysql> INSERT INTO user (Host,User,Password)

 -> VALUES('whitehouse.gov','custom',PASSWORD('stupid'));

mysql> INSERT INTO db

 -> (Host,Db,User,Select\_priv,Insert\_priv,Update\_priv,Delete\_priv,

 -> Create\_priv,Drop\_priv)

 -> VALUES

 -> ('localhost','bankaccount','custom','Y','Y','Y','Y','Y','Y');

mysql> INSERT INTO db

 -> (Host,Db,User,Select\_priv,Insert\_priv,Update\_priv,Delete\_priv,

 -> Create\_priv,Drop\_priv)

 -> VALUES

 -> ('whitehouse.gov','expenses','custom','Y','Y','Y','Y','Y','Y');

mysql> INSERT INTO db

 -> (Host,Db,User,Select\_priv,Insert\_priv,Update\_priv,Delete\_priv,

 -> Create\_priv,Drop\_priv)

 -> VALUES('%','customer','custom','Y','Y','Y','Y','Y','Y');

mysql> FLUSH PRIVILEGES;

Первые три оператора INSERT добавляют в таблицу user записи, которые позволят пользователю custom подключаться с различных компьютеров с указанным паролем, но не дают ему никаких привилегий (все привилегии установлены в принятое по умолчанию значение 'N'). Следующие три оператора INSERT добавляют записи в таблицу db, в которой назначаются привилегии для пользователя custom по отношению к базам данных bankaccount, expenses и customer, но только если доступ осуществляется с определенных компьютеров. Как обычно, после внесения изменений непосредственно в таблицы назначения привилегий серверу необходимо дать команду на перезагрузку этих таблиц (при помощи FLUSH PRIVILEGES), чтобы внесенные изменения вступили в силу.

Если необходимо предоставить определенному пользователю доступ с любого компьютера к определенному домену, можно воспользоваться оператором GRANT следующим образом:

mysql> GRANT ...

 -> ON \*.\*

 -> TO myusername@"%.mydomainname.com"

 -> IDENTIFIED BY 'mypassword';

Чтобы сделать то же самое путем непосредственного внесения изменений в таблицы назначения привилегий, выполните следующие действия:

mysql> INSERT INTO user VALUES ('%.mydomainname.com', 'myusername',

 -> PASSWORD('mypassword'),...);

mysql> FLUSH PRIVILEGES;

Можно также воспользоваться программой MySQL Query Browser, xmysqladmin, mysql\_webadmin и даже xmysql, чтобы вставить, обновить или изменить значения в таблицах назначения привилегий. Эти утилиты можно найти в каталоге Contrib веб-сайта.

**Контрольные вопросы:**

1. Какие существуют привилегии в MySQL?

2. Как создать пользователя MySQL?

3. Что означают символы %, \* и @ в команде Grant?