

Администрирование и безопасность

Зорина И.Г.

Учетные записи пользователей

В MySQL идентификация пользователей основана на комбинации имени пользователя и хоста, с которого подключается пользователь

Идентификатор пользователя:

`'<Значение столбца User>' ['@' <Значение столбца Host>']`

ПРИМЕР: `'anna'@'localhost'`



Регистрация пользователя

```
CREATE USER<идентификатор пользователя>  
[IDENTIFIED BY [PASSWORD]'<пароль>'];
```

- Если параметр **IDENTIFIED BY** не задан, то будет использоваться пустой пароль.
- Параметр **PASSWORD** необходимо указать в том случае, если вводится не реальный, а зашифрованный пароль.

ПРИМЕР:

```
CREATE USER 'anna'@'localhost' IDENTIFIED BY '123';
```

Установка пароля

```
SET PASSWORD [FOR <идентификатор пользов>]  
= PASSWORD ('<пароль>') ;
```

- Параметрами данной команды являются идентификатор учетной записи пользователя и новый пароль для этой записи.
 - Если не указать идентификатор пользователя, то изменится пароль пользователя, под которым выполняется команда
-



Система привилегий пользователя

Создание привилегии доступа в MySQL подразумевает определение следующих параметров:

- - идентификатор учетной записи пользователя, которому предоставляется привилегия;
 - - тип привилегии, т.е. тип операций, которые будут разрешены пользователю;
 - - область действия привилегии.
-



Типы привилегий

- ALL [PRIVILEGES] – предоставляет все привилегии;
 - ALTER – разрешает выполнение команд ALTER;
 - CREATE – разрешает выполнение команд CREATE;
 - CREATE USER – разрешает выполнение команд CREATE USER и DROP USER;
 - DELETE – разрешает выполнение команд DELETE;
 - DROP – разрешает выполнение команд DROP;
 - FILE – разрешает чтение и создание файлов на сервере;
 - INSERT – разрешает выполнение команд INSERT;
 - SELECT – разрешает выполнение команд SELECT;
 - UPDATE – разрешает выполнение команд UPDATE;
 - GRANT OPTION – разрешает назначать и отменять привилегии другим пользователям.
-



Область действия привилегии

- ***.*** - привилегия будет действовать глобально, т.е. на все базы данных;
- **<Имя базы данных>.*** - привилегия будет действовать для указанной базы данных;
- ***** - привилегия будет действовать для базы данных, которая в момент выполнения команды GRANT являлась текущей;
- **<Имя базы данных>. <Имя таблицы>** - привилегия будет действовать для указанной таблицы;
- Если требуется создать привилегию не для всей таблицы, а для отдельных столбцов, необходимо перечислить данные столбцы в скобках перед ключевым словом ON.

Предоставление привилегии

```
GRANT <тип привилегии>  
[ (<список столбцов>)] ON <область действия>  
TO <идентификатор пользователя>  
[WITH GRANT OPTION];
```

ПРИМЕР:

```
GRANT CREATE ON *.* TO 'anna'@'localhost';  
GRANT DROP ON sales.* TO 'anna'@'localhost';  
GRANT SELECT ON sales.product TO  
'anna'@'localhost';  
GRANT UPDATE (price) ON sales.product TO  
'anna'@'localhost';
```


Отмена привилегий

```
REVOKE <тип привилегии>  
[ (<список столбцов> ) ] ON <область действия>  
FROM <идентификатор пользователя>;
```

ПРИМЕР:

```
REVOKE CREATE ON *.* FROM 'anna'@'localhost' ;  
REVOKE DROP ON sales.* FROM  
'anna'@'localhost' ;  
REVOKE SELECT ON sales.product FROM  
'anna'@'localhost' ;  
REVOKE UPDATE (price) ON sales.product FROM  
'anna'@'localhost' ;
```

Просмотр привилегий

- Глобальные привилегии хранятся в таблице **user**.
- Привилегии, областью действия которых является отдельная база данных, хранятся в таблице **db**.
- Привилегии, относящиеся к отдельным таблицам, хранятся в таблице **tables_priv**.
- Привилегии для отдельных столбцов хранятся в таблице **columns_priv**.

