目录

1. 用户授权： 1

1.1 用户授权 1

1.2 用户授权案例 2

2. 授权库： 4

3. 撤销权限： 7

1. 用户授权：

1.1 用户授权

添加用户并设置权限及连接密码

命令格式：

grant 权限列表 on 库名 to 用户名@“客户端地址” identified by "密码" with grant option; #有授权权限，可选项

权限列表：

- all //所有权限
- usage //无权限
- select , update, insert //个别权限
- select, update (字段1, ... , 字段N) //指定字段

库名：

. //所有库所有表

库名.* // 一个库 userdb.*

库名.表名 //一张表 userdb.user

用户名：

授权时自定义 要有标识性 webuser

存储在mysql库的user表里

客户端地址：

% // 所有主机

192.168.4.% // 网段内的所有主机 192.168.4.1~254

192.168.4.1 // 1台主机

localhost // 数据库服务器本机

1.2 用户授权案例

案例 1：添加用户 mydba，对所有库，表有完全权限，允许从任何客户端连接，密码 123qqq...A，且有授权权限

```
[root@svr7 ~]# mysql -uroot -p'123qqq...A'
mysql> grant all on *.* to mydba@"%" identified by "123qqq...A" with grant option;
```

客户端 pc207 测试，-h 登录的服务器地址

```
[root@pc207 ~]# yum -y install mariadb
[root@pc207 ~]# mysql -h192.168.4.7 -umydba  -p'123qqq...A'
MySQL [(none)]> select user();                  #查看当前的登录用户
MySQL [(none)]> show grants;                    #查看当前登录用户mydba所拥有的权限
MySQL [(none)]> set password=password("456abc...A");  #客户端用户mydba修改自己的连接密码
MySQL [(none)]> exit
客户端pc207测试，成功
[root@pc207 ~]# mysql -h192.168.4.7 -umydba -p’  456abc...A’
```

虚拟机 svr7 操作，管理员修改授权用户 mydba 的连接密码

```
mysql> show grants for mydba@"%";       #管理员查看已有授权用户权限
mysql> set password for mydba@"%"=password("123qqq...A");
```

客户端 pc207 测试，成功

```
[root@pc207 ~]# mysql -h192.168.4.7 -umydba  -p123qqq...A
```

Pc207 主机测试权限拥有的所有权限(增删改查，授权权限)

```
MySQL [(none)]> show grants;
MySQL [(none)]> show databases;
MySQL [(none)]> drop database bbsdb;              #用户mydba删除bbsdb库
MySQL [(none)]> show databases;
MySQL [(none)]> create database bbsdb;  #用户mydba创建新的库bbsdb
```

```
MySQL [(none)]> create database bbsdb2;
```

Pc207主机：用户mydba可以给其他用户授权

```
MySQL [(none)]> grant all on db2.* to abc@"localhost" identified by "123qqq...A";
```

Svr7主机，abc用户测试登录

```
[root@svr7 ~]# mysql -uabc -p123qqq...A          #成功
mysql> exit
```

删除授权用户 mydba

```
[root@svr7 ~]# mysql -uroot -p123qqq...A
mysql> drop user mydba@"%";
```

案例 2：添加 admin 用户,允许从 192.168.4.0/24 网段连接，对 db3 库的 user 表有查询权限，密码 123qqq...A

主机 svr7 做授权，pc207 测试

```
[root@svr7 ~]# mysql -uroot -p123qqq...A
mysql> grant select on db3.user to admin@"192.168.4.%" identified by "123qqq...A";
        #创建失败
##给用户授权时，如果不是授予all的权限，当对应的库和表不存在时，必须有create权限
##给用户授权时，如果是授予all的权限，则对应的库和表可以不存在
mysql> grant create,select on db3.user to admin@"192.1668.4.%" identified by
"123qqq...A";
```

案例 3：添加 admin2 用户，允许从本机连接，允许对 db3 库的所有表有查询/更新/插入/删除记录权限，密码 123qqq...A

```
mysql> grant create,select,insert,update,delete on db3.* to admin2@"localhost"
identified by "123qqq...A";
```

新建db3库，前面的授权可以让admin,admin02用户对db3库下的表进行操作，但他们并不具备创建库的权限，需要管理员提前创建

```
mysql> create database  db3;
```

pc207：测试 admin 用户的权限

```
[root@pc207 ~]# mysql -h192.168.4.7  -uadmin  -p123qqq...A
MySQL [(none)]> show grants;                    #查看当前登录用户拥有的权限
MySQL [(none)]> create table db3.user(name char(10),sex enum("boy","girl"));
        #在db3库下，创建user表
MySQL [(none)]> insert into db3.user values("bob","boy");          #插入失败
MySQL [(none)]> exit
```

Svr7：测试 admin2 用户的权限，只能从本机登录

```
[root@svr7 ~]# mysql -uadmin2   -p123qqq...A
mysql> show grants;
mysql> use db3;
mysql> show tables;                                          #可以查看db3库下的所有表
mysql> insert into db3.user values("bob","boy"); #可以向db3库下的user表中，插入数据
mysql> select * from user;                                   #可以查询user表下的所有记录
mysql> create table user2(id int);                           #可以在db3库下创建新的表user2
```

2. 授权库：

mysql库记录授权信息,主要表如下：

- ✓ **user表**　记录已有的授权用户及权限 (all)
- ✓ **db表**　记录已有授权用户对数据库的访问权限
- ✓ **tables_priv表**　记录已有授权用户对表的访问权限
- ✓ **columns_priv表**　记录已有授权用户对字段的访问权限
- ✓ **查看表记录可以获取用户权限；也可以通过更新记录，修改用户权限**

mysql 库下 user 表中记录的是已经授权的用户和权限

```
[root@svr7 ~]# mysql -uroot -p123qqq...A
```

```
mysql> select user,host from mysql.user;
mysql> show grants for admin@"192.168.4.%";              #查看admin用户的权限
查看登录主机为:"192.168.4.%" 的admin用户,在user表的权限字段，admin用户在user表中的所有权限字段均为N,所以用户admin的权限信息，并不会被存储到user表中
mysql> select * from mysql.user where host="192.168.4.%" and user="admin" \G;
```

tables_priv 记录已有授权用户对表的访问权限

```
在tables_priv表中，查看用户admin的授权信息，\G 竖行显示
mysql> select * from mysql.tables_priv where user="admin"\G; #拥有查询和创建的权限
通过直接修改表tables_priv中的字段值，修改授权用户admin的权限
查看表结构，Table_priv字段记录表的权限，枚举类型，修改表用户权限时，只能在枚举类型的范围内选择
mysql> desc mysql.tables_priv\G;
...
set('Select','Insert','Update','Delete','Create','Drop','Grant','References','Index','Alter','Create View','Show view','Trigger')
...
给用户admin新增insert和update的权限
mysql> update mysql.tables_priv set Table_priv="select,create,insert,update" where user="admin" and Host="192.168.4.%";
mysql> flush privileges;     #刷新，让配置生效
通过查看tables_priv权限表，来查看用户admin的权限
mysql> select * from mysql.tables_priv where user="admin"\G;
...
Table_priv: Select,Insert,Update,Create
...
mysql> show grants for admin@"192.168.4.%"; #通过授权命令，查看用户admin的权限
```

mysql 库下的 db 表，记录已有授权用户对数据库的访问权限

```
查看mysql.db表的表结构，类型为enum的字段，值为Y 则代表拥有访问权限；值为N 则代表没有访问权限
mysql> desc mysql.db;
查询mysql库下db表中的，host,user,db字段的值，从哪个主机(host)登录的用户(user)，对哪个库(db)拥有访问
mysql> select host,user,db from mysql.db;
在mysql.db表中，查询admine2用户对db3库的访问权限
mysql> select * from mysql.db where db="db3"\G;
mysql> show grants for admin2@"localhost";       #通过授权命令，查看授权用户
通过修改mysql.db权限表，取消用户admin2，删除的权限
mysql> update mysql.db set Delete_priv="N" where user="admin2";
mysql> flush privileges;
在mysql.db表中，重新查询admin2用户对db3库的访问权限
mysql> select * from mysql.db where db="db3"\G;
         Delete_priv: N       #删除权限变为 N
mysql> show grants for admin2@"localhost";
```

columns_priv 表，记录已有授权用户对字段的访问权限

```
mysql> desc mysql.columns_priv;
查看columns_priv表中的所有数据，记录为空，没有设置用户对字段的访问权限
mysql> select * from mysql.columns_priv;
用户admin2用户授权，让用户仅对db3.user表的name字段有更新的权限
mysql> desc db3.user;
mysql> grant select,update(name) on db3.user to admin2@"localhost" identified by "123qqq...A";
再次查看columns_priv表中的所有数据，新增加了对字段的访问权限
mysql> select * from mysql.columns_priv;
```

```
mysql> show grants for admin2@"localhost";      通过授权命令查看admin2的权限
mysql> exit
```

3. 撤销权限：

revoke 权限列表 on 库名.表 from 用户名@"客户端地址";

```
[root@svr7 ~]# mysql -uroot -p123qqq...A
mysql> select host,user from mysql.user;            #查询授权用户的host和user字段
要取消某一个用户的权限，先查看用户的具体授权信息
mysql> show grants for admin@"192.168.4.%";
取消admin用户对db3.user表的更新和创建的权限
mysql> revoke update,create on db3.user from 'admin'@'192.168.4.%';
mysql> show grants for admin@"192.168.4.%";     #通过命令查看授权admin的权限信息
在mysql库的tables_priv表中，查看admin用户的权限
mysql> select * from mysql.tables_priv where user="admin" \G;
撤销db3库下，admin2用户对所有表的insert,update,delete的权限
mysql> select host,user from mysql.user;            #查询授权用户的host和user字段
mysql> show grants for admin2@'localhost';
mysql> select * from mysql.db where db="db3"\G;
mysql> revoke insert,update,delete on db3.* from admin2@"localhost";
mysql> select * from mysql.db where db="db3"\G;
mysql> show grants for admin2@'localhost';
取消admin2用户在db3库和db3库下的权限
mysql> show grants for admin2@"localhost";
mysql> revoke all on db3.* from admin2@"localhost";
mysql> revoke all on db3.user from admin2@"localhost"
mysql> show grants for admin2@"localhost";          #通过命令查看授权用户
admin2的权限信息，USAGE指没有权限，此时用户依然存在，可以登录，不能进行任何操作
```

彻底删除用户，不能再使用此用户登录数据库

```
mysql> drop user admin2@"localhost";
[root@svr7~]# mysql -uadmin2 -p123qqq...A                #登录失败
```