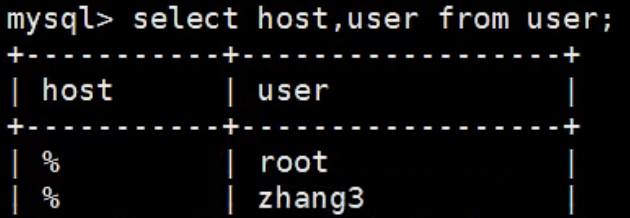
# 用户管理

## 创建用户

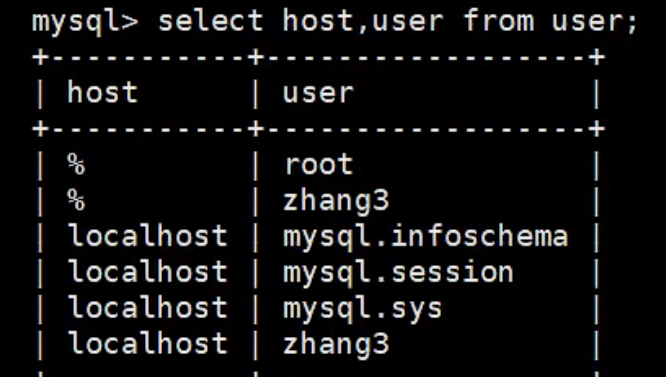


默认什么IP可以连接此数据库跟root用户一样



指定什么IP可以连接此数据库：





此时即使用户名一样也可以创建成功，因为支持的连接IP地址不一样。

由此可见user表是user与host字段联合起来作为主键

即建表时使用constraint xxx primary key（user，host）

然后登录



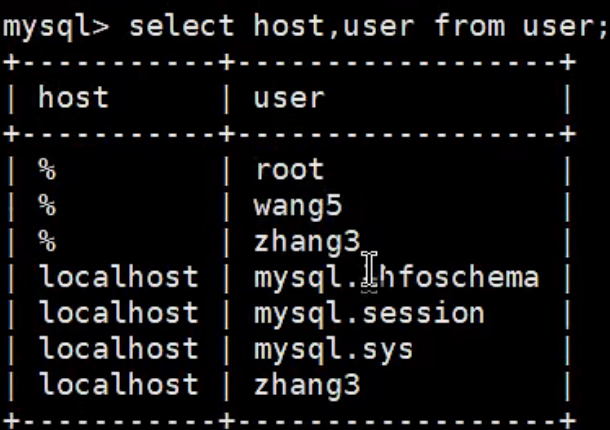


表非常少，因为普通用户权限很小

## 修改用户

就是修改user表中user字段值改名

可能用户名有一样的，所以直接匹配主键。

最后刷新一下，否则李四还没有被修改，因为是DML操作，而不是DDL操作



## 删除用户

特殊：可以直接使用drop指令删除



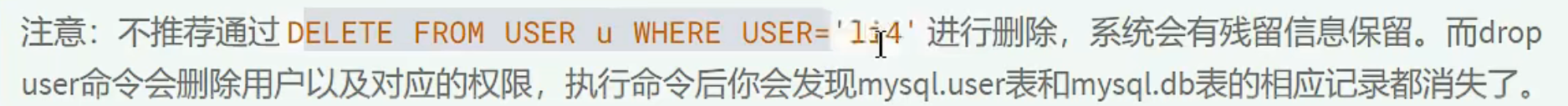
DDL操作，不需要flush



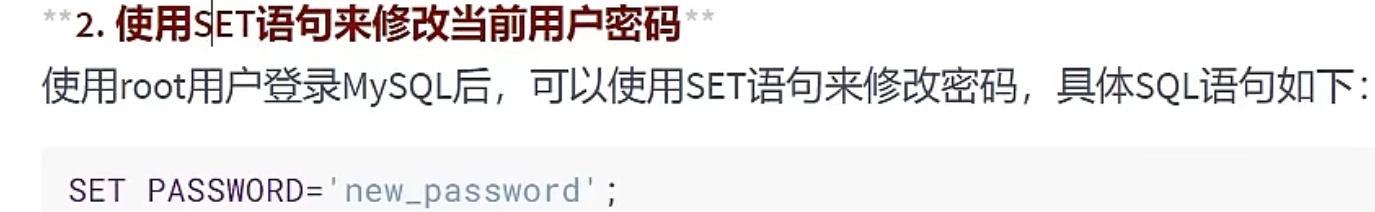
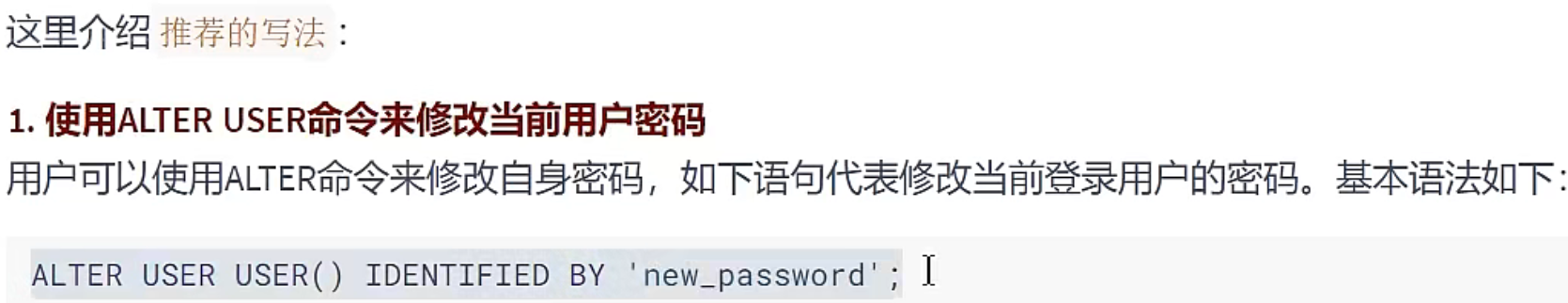
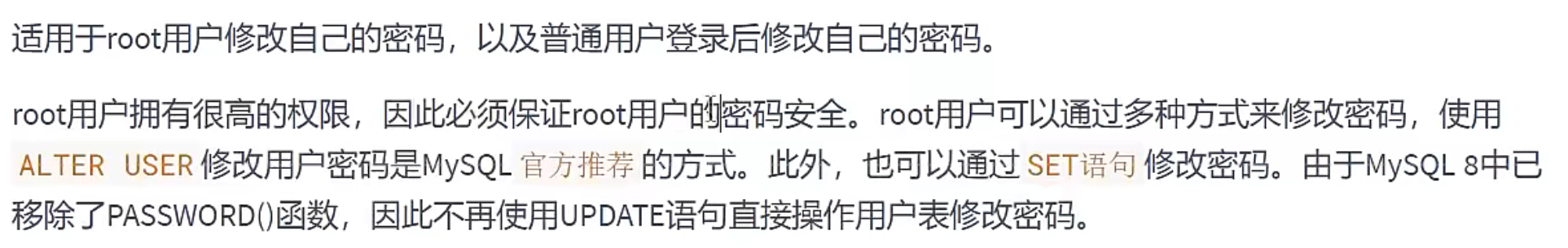
这种情况下默认删除与root用户相同host的那个用户

还可以DML删除表中此用户但是不推荐



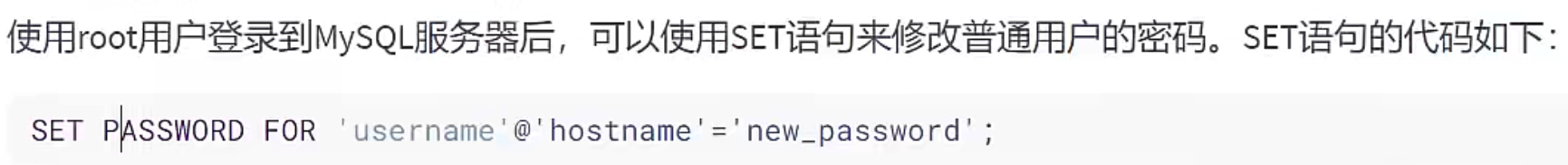


## 修改当前用户密码



## 修改指定用户密码

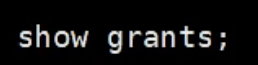
可以多个user中间逗号间隔



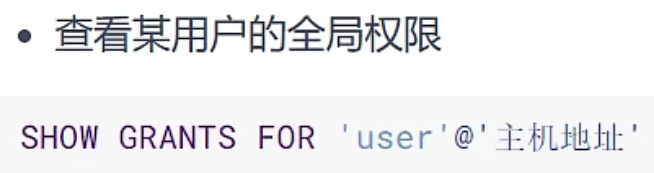
# 权限管理

## 查看权限

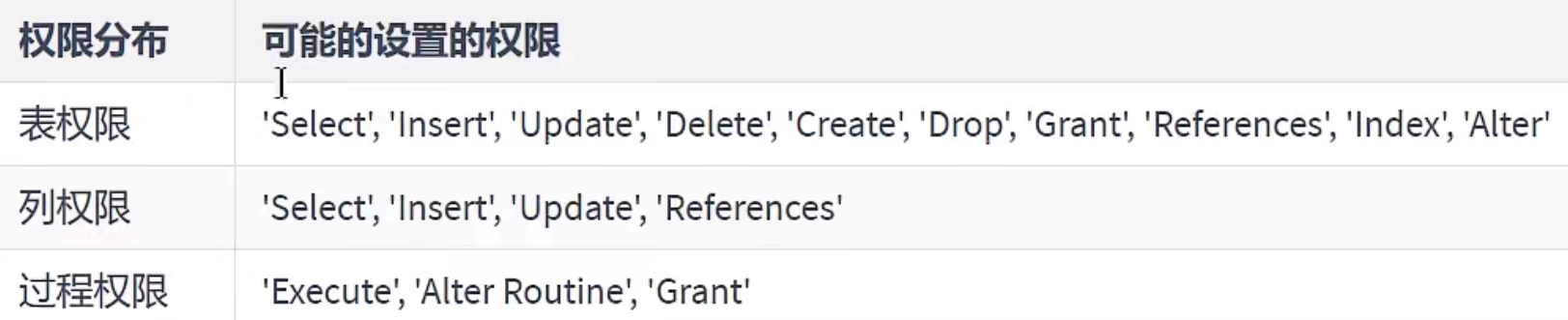
查看当前用户权限



root下



## 授予权限



使用grant（授予）关键字

grant 什么权限 on什么数据库/什么表/什么字段 to 用户名@登录此用户的IP



赋予所有权限给李四，但是李四不能将权限赋给别人



如果要李四可以赋给别人则



## 回收权限

root下

revoke（撤销）关键字

revoke 什么权限 on什么数据库/表/字段 from ‘谁’ @‘地址’



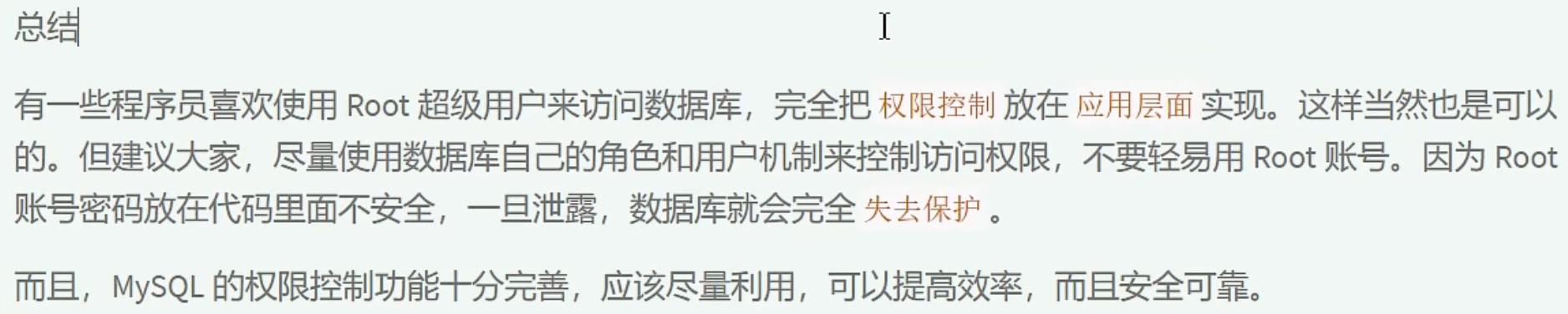
如果要回收跟root同级的用户的权限，则需要先赋予当前root用户system\_user权限



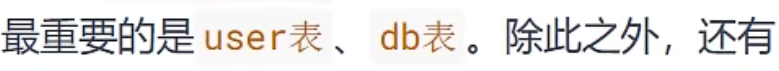
再去回收root同级用户权限

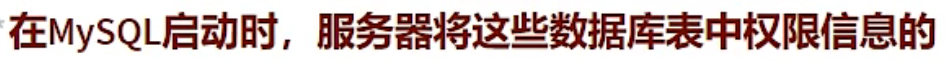


## 小结



# 权限表

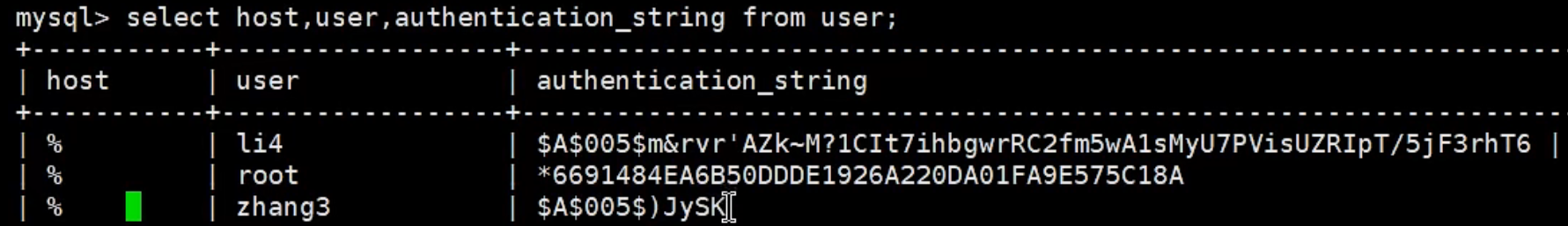




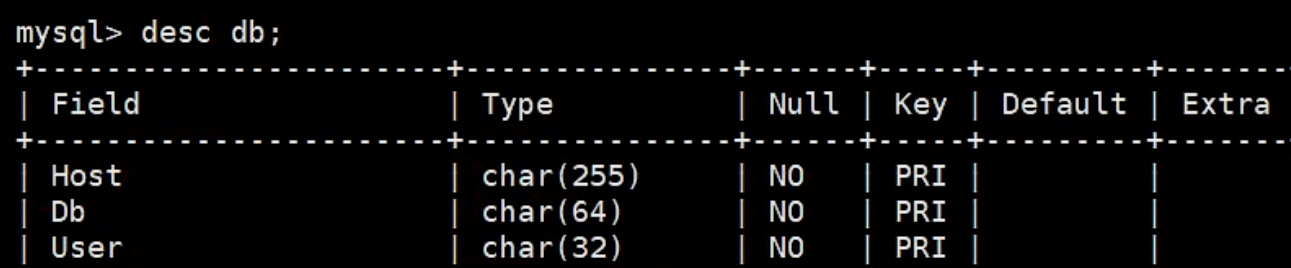
## user表

登陆的时候会去mysql数据库的user表中校验



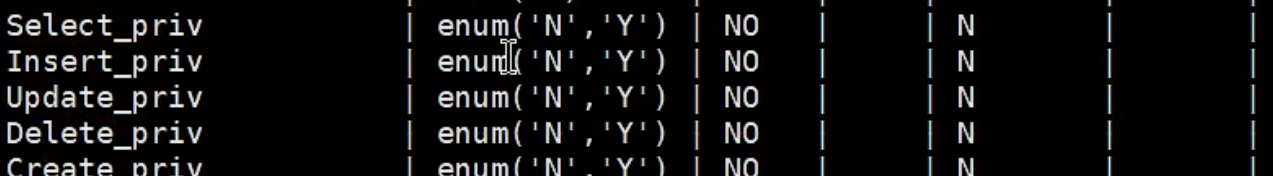


## db表



此表Host，User，Db三个字段为联合主键，存储了某个用户对不同数据库的权限。

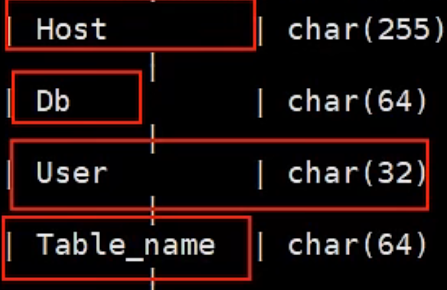
其他字段就是对某数据库的权限字段，值就是枚举，Y/N



## table\_priv表

存储的是用户对某张表的权限，此时User，Host，Db，Table\_name四个字段为联合主键，因为不同的数据库下可能有相同名称的表



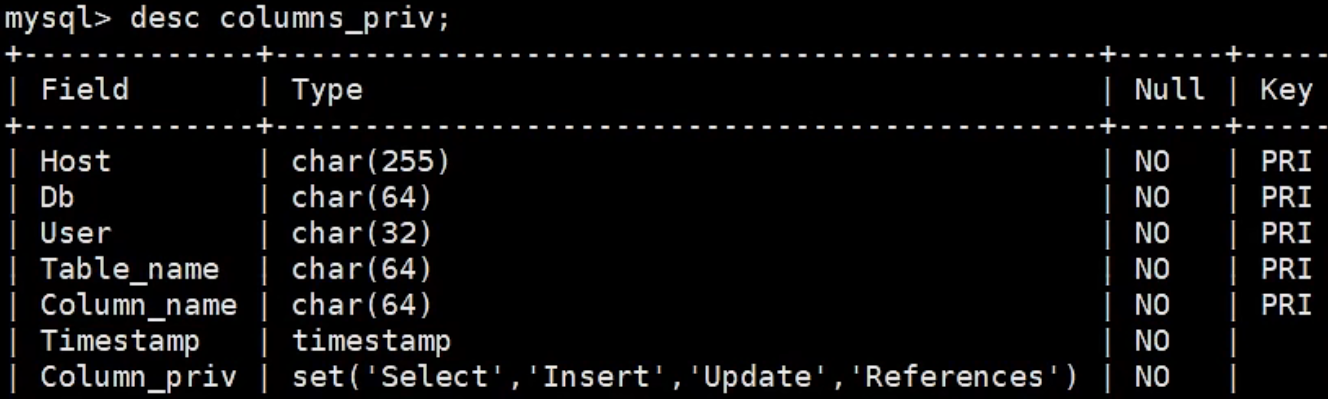


此时对表的权限是集合形式



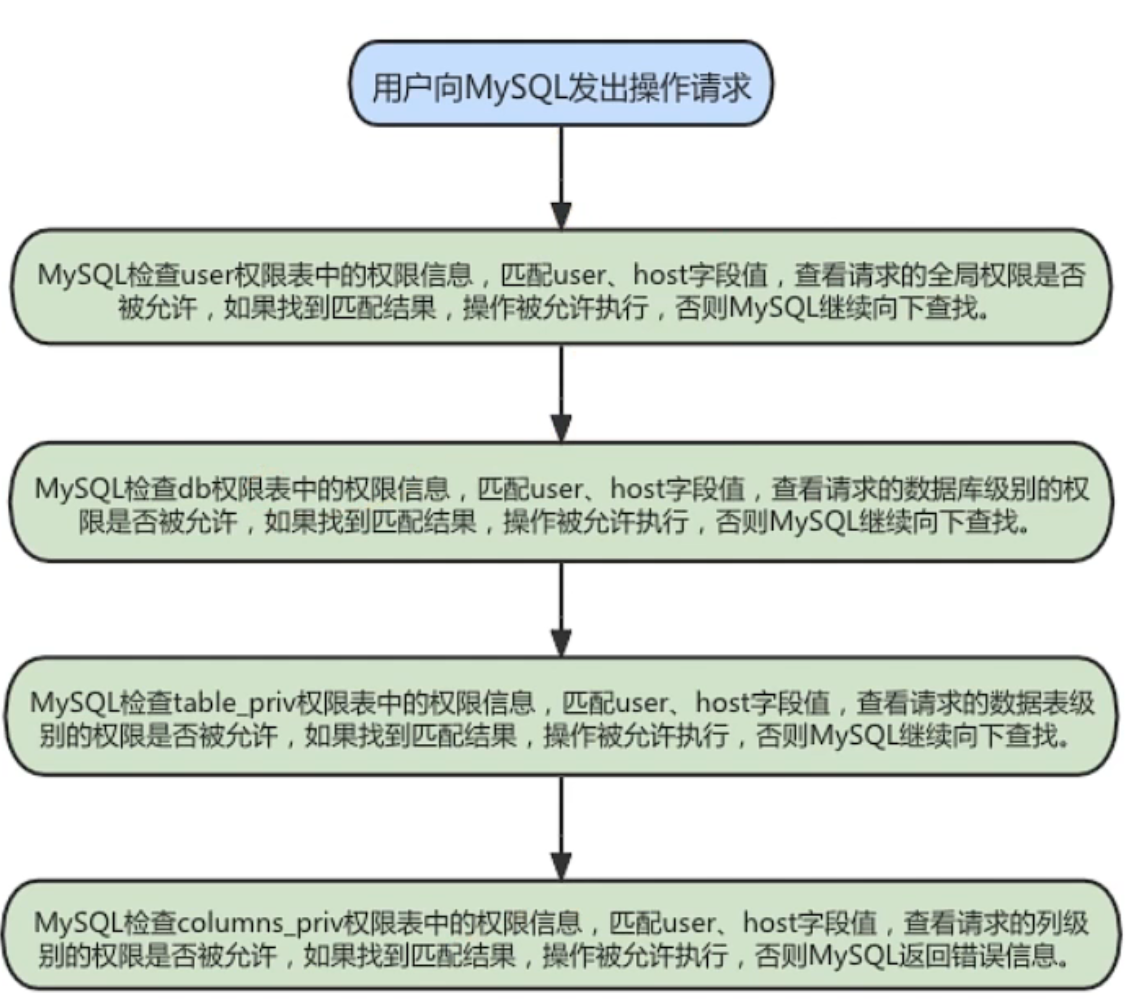
## columns\_priv表

使用Host，User，Db，Table\_name,Column\_name五个字段为联合主键。



权限仍然是集合形式

# 请求核实



# 8.0新特性角色管理

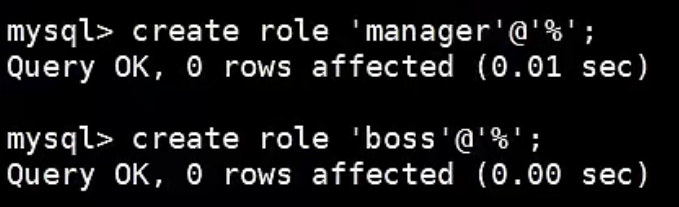
分配给用户权限时，除了grant具体权限，还可以创建一个角色，添加一些权限，然后将角色给不同的用户。

相当于将权限封装起来。不用每次都grant权限。

角色格式类似用户，也是名字+IP

## 创建角色

create role‘角色名’ @‘地址’



## 删除角色

跟删除用户一样drop role ‘用户名’ @‘ip地址’



## 给角色权限

跟赋予用户权限一样格式







## 回收角色权限

与回收用户角色格式一样



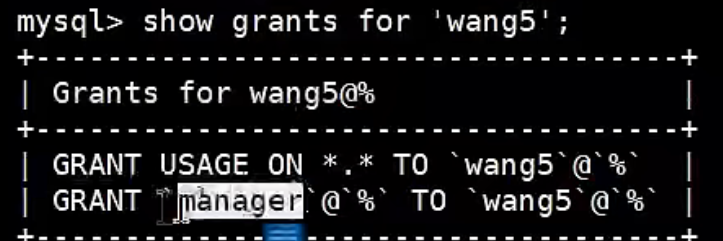
## 将角色授予用户

跟授予用户权限格式类似。

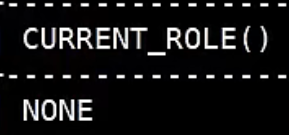
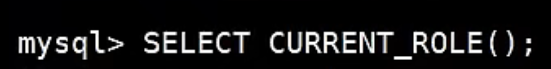
grant ‘角色名’ @‘IP地址’ to ‘用户’ @‘IP地址’



如果IP地址跟用户的不一样，此时用户的IP就被改为角色的IP



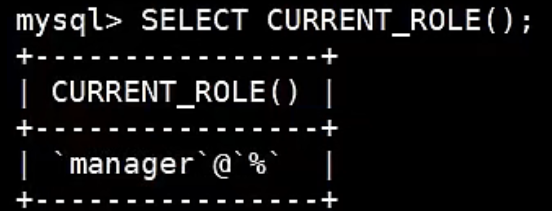
## 激活用户身上的角色



此时代表没有激活当前任何角色 current（当前的）

root下激活角色到某用户



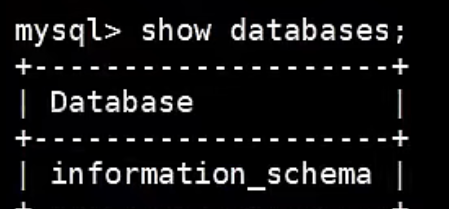


## 回收用户身上的角色

格式类似回收用户权限

root下





此时看不到任何数据库了。

## 设置强制角色

一旦设置后，所有用户默认都是这个角色，角色不可被删除（drop），也不可被从用户身上回收（revoke）

比如登录权限，所有用户都可以登录数据库