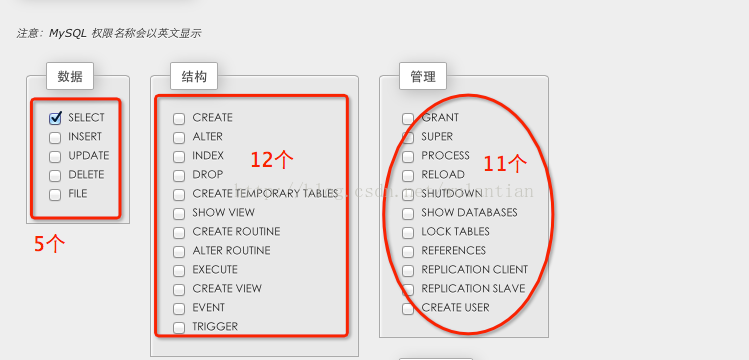
1、MySQL的用户权限



## MySQL权限级别

服务器>数据库>表>列，另外还有存储过程、视图和索引。

**MySQL权限列表：**

| **权  限** | **作用范围** | **作  用** |
| --- | --- | --- |
| **all** | 服务器 | 所有权限 |
| **select** | 表、列 | 选择行 |
| **insert** | 表、列 | 插入行 |
| **update** | 表、列 | 更新行 |
| **delete** | 表 | 删除行 |
| **create** | 数据库、表、索引 | 创建 |
| **drop** | 数据库、表、视图 | 删除 |
| **reload** | 服务器 | 允许使用flush语句 |
| **shutdown** | 服务器 | 关闭服务 |
| **process** | 服务器 | 查看线程信息 |
| **file** | 服务器 | 文件操作 |
| **grant option** | 数据库、表、存储过程 | 授权 |
| **references** | 数据库、表 | 外键约束的父表 |
| **index** | 表 | 创建/删除索引 |
| **alter** | 表 | 修改表结构 |
| **show databases** | 服务器 | 查看数据库名称 |
| **super** | 服务器 | 超级权限 |
| **create temporary tables** | 表 | 创建临时表 |
| **lock tables** | 数据库 | 锁表 |
| **execute** | 存储过程 | 执行 |
| **replication client** | 服务器 | 允许查看主/从/二进制日志状态 |
| **replication slave** | 服务器 | 主从复制 |
| **create view** | 视图 | 创建视图 |
| **show view** | 视图 | 查看视图 |
| **create routine** | 存储过程 | 创建存储过程 |
| **alter routine** | 存储过程 | 修改/删除存储过程 |
| **create user** | 服务器 | 创建用户 |
| **event** | 数据库 | 创建/更改/删除/查看事件 |
| **trigger** | 表 | 触发器 |
| **create tablespace** | 服务器 | 创建/更改/删除表空间/日志文件 |
| **proxy** | 服务器 | 代理成为其它用户 |
| **usage** | 服务器 | 没有权限 |

## MySQL授权命令

### 创建用户

CREATE USER 'username'@'host' IDENTIFIED BY 'password';

CREATE USER 'user'@'192.168.1.10' IDENTIFIED BY 'password';

CREATE USER 'user'@'%';   #不设置密码

说明：如果主机位使用%，那么将允许从任意主机登录；密码可以为空，若为空，则用户可以不需要密码登录服务器。

补充：主机名或者IP中可以使用%进行通配，如\*\*%.baidu.com\*\*;**192.168.1.%**

补充：如果即有字母，又有数字，则不进行匹配(防止恶意访问)

补充：IPv4地址可以使用掩码，如**192.168.0.0/255.255.0.0**  匹配整个B类地址

### 进行授权

GRANT privileges（权限） ON databasename.tablename TO 'username'@'host';

GRANT SELECT, INSERT, UPDATE, DELETE, CREATE, DROP ON *.* TO 'user'@'%';

如果授予所有权限，则可以使用ALL，所有数据库和所有表可以使用\*

注意：ALL并不包括GRANT OPTION权限（也不包括proxy权限），如果需要使本用户可以给其它用户授权，则可以使用如下语句：

GRANT GRANT OPTION ON *.* TO 'user'@'%';  或者：

GRANT privileges ON databasename.tablename TO 'username'@'host' WITH GRANT OPTION;

### 修改密码

SET PASSWORD FOR 'user'@'%' = PASSWORD('pass');

mysqladmin -u用户名 -p旧密码 password 新密码

### 取消授权

REVOKE privilege ON databasename.tablename FROM 'username'@'host';

REVOKE SELECT ON *.* FROM 'user'@'%';

### 删除用户

DROP USER 'username'@'host';

### 查看用户权限

查看当前用户权限：

show grants;

查看其它用户权限：

show grants for 'user'@'%';

### 用户重命名

RENAME USER 'user'@'%' TO 'dong'@'%';

### 刷新权限

flush privileges;

## MySQL权限说明

**all,服务器**

授予所有权限

**alter,表**

可以使用alter table来改变表的结构。alter table同时需要create和insert权限；重命名表需要旧表的alter和drop权限，新表的create和insert权限

**alter routine,存储过程**

更改和删除存储过程(过程和函数)

**create,数据库/表/索引**

允许创建新的数据库和表以及索引

**create routine,存储过程**

允许创建存储过程(过程和函数)

**create tablespace,服务器**

创建、更改或删除表空间和日志文件组

**create temporary tables,表**

使用create temporary table创建临时表。会话创建临时表后，不再对该表进行权限检查，创建会话可以对该表执行任何操作

**create user,服务器**

创建用户，允许使用alter user/create user/drop user/rename user/revoke all privileges语句对用户权限进行操作

**create view,视图**

创建视图，允许使用create view语句

**delete,表**

允许删除行

**drop,数据库/表/视图**

删除现有数据库、表和视图。在分区表使用alter table … drop partition语句，truncate table也需要drop权限。若将mysql库的drop权限授予用户，则该用户可以删除权限数据库

**event,数据库**

创建、更改、删除或查看事件调度程序的事件

**execute,存储过程**

执行存储过程(过程和函数)

**file,服务器**

允许使用load data infile和select … into outfile语句以及load\_file()函数。从5.7.17开始，create table语句中的data directory或者index directory选项也需要该权限

**grant option,数据库/表/存储过程**

授予其它用户或者从其它用户删除你所拥有的权限。 grant option权限使用户可以将其权限授予其他用户。具有不同特权和grant option权限的两个用户可以组合特权。

**index,表**

创建或删除索引。适用于现有表，如果你具有create权限，则可以在创建表语句中包含索引定义

**insert,表/列**

插入行。analyze table/optimize table/repair table表维护语句也需要该权限

**lock tables,数据库**

锁表。使用lock tables语句显示的锁定你拥有select权限的表，包括写入锁，可以防止其它他话读取锁定的表

**process,服务器**

显示线程信息。使用show processlist/mysqladmin processlist查看其它用户的线程，还可以使用show engine语句

**proxy,服务器**

代理权限。可以代理成为另一个用户

**references,数据库/表**

创建外键约束的父表需要该权限

**reload,服务器**

允许使用flush语句。同进还启用等效的mysqladmin命令：flush-hosts,flush-logs,flush-privileges,flush-status,flush-tables,flush-threads,refresh和reload

**replication client,服务器**

允许使用show master status/show slave status/show binary logs语句

**replication slave,服务器**

允许从服务器请求当前主服务器上的更新

**select,表/列**

选择行。其他读取列的语句也需要该权限，如delete或update语句中where子句指定的列

**show databases,服务器**

通过show databases语句查看数据库名称

**show view,视图**

通过show create view语句查看视图，与explain一起使用的视图也需要此权限

**shutdown,服务器**

使用shutdown语句，mysqladmin关闭以及mysql\_shutdown()函数

**super,服务器**

通过修改全局系统变量来启用配置更改。对某些系统变量，设置会话值也需要该权限。binlog\_format,sql\_log\_bin,sql\_log\_off  
全局事务特性更改  
启动和停止复制，包括组复制  
允许使用change master to和change replication filter语句  
二进制日志控制，purge binary logs和binlog语句  
执行视图或存储程序时启用授权ID  
允许使用create server,alter server和drop server语句  
允许使用mysqladmin debug命令  
启用innodb密钥轮换  
使用des\_encrypt()函数读取DES密钥文件  
使用版本令牌用户定义函数  
对非super帐户客户端连接的控制

使用kill语句或者mysqladmin kill命令终止属于其他用户的线程  
即使达到max\_connections控制的连接限制，服务器也会授受来自super客户端的连接  
即使使用了read\_only系统变量，也可以执行更新  
super客户端连接时，服务器不执行init\_connect系统变量内容  
处于脱机模式offline\_mode的服务器不会终止super客户端的连接，并接受来自super客户端的新连接  
如果启用二进制日志记录，可能还需要super权限创建或更改存储过程

**trigger,服务器**

触发器。创建、删除、执行、显示该表的触发器

**update,表/列**

更新行

**usage,服务器**

没有任何权限

2、查看用户权限

SELECT \* FROM mysql.user WHERE user='用户名'\G

SHOW GRANTS FOR '用户名'@'白名单';