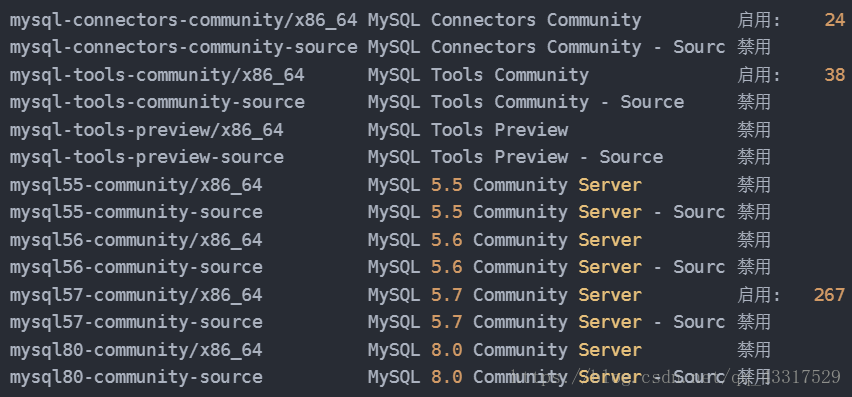
# 安装

1、打开Centos操作系统，下载mysql的repo源并安装，执行命令：

rpm -Uvh http://dev.mysql.com/get/mysql57-community-release-el7-9.noarch.rpm （不是链接）

2、查看可用的mysql版本以及禁用/启用情况：

yum repolist all | grep mysql



3、修改源文件,禁用5.7,启用8.0

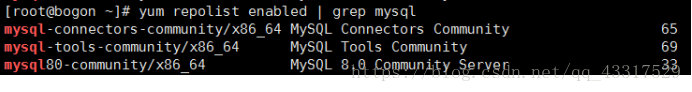
vim /etc/yum.repos.d/mysql-community.repo

把里面的8.0enabled改为1就可以了，其他的版本改为0



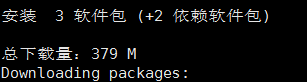
4、修改完之后查看可用版本

yum repolist enabled | grep mysql (显示8.0即为成功)



5、8.0版本启用后,安装Mysql

yum install -y mysql-community-server (380M左右,过程会稍微有些慢，耐心等待）



6、安装完成之后,启动mysql

systemctl start mysqld

7、开机启动设置

systemctl enable mysqld

systemctl daemon-reload

8、查看随机生成的密码,注意记住密码

grep ‘temporary password’ /var/log/mysqld.log

sudo grep 'temporary password' /var/log/mysqld.log

9、登录Mysql,输入原始生成的随机密码

mysql -uroot -p

10、改变mysql密码策略 ( 密码强度默认为中等，大小写字母、数字、特殊符号，只有修改成功后才能修改配置再设置更简单的密码 )

set global validate\_password.policy=0;

set global validate\_password.length=1;

11、修改root密码

ALTER USER ‘root’@‘localhost’ IDENTIFIED BY ‘new pwd’;(单引号和分号不能省，一定记住密码)

12、退出mysql,重新启动即可生效，安装成功。

退出命令：quit

# 密码修改

MySQL8.0和MySQL5.7具有众多不同之处，此处不赘述。这里，只简单讲讲在安装过程中遇到的问题之一和解决办法：  
**MySQL8.0安装完成之后的默认密码是多少？如何修改初始密码？**

**1 启动MySQL服务**

启动MySQL服务的命令：

shell> sudo service mysqld start

Starting mysqld:[ OK ]

检查MySQL服务器的运行状态：

shell> sudo service mysqld status

● mysqld.service - MySQL Server

Loaded: loaded (/usr/lib/systemd/system/mysqld.service; enabled; vendor preset: disabled)

Active: active (running) since Sun 2018-06-03 18:31:51 CST; 6min ago

Docs: man:mysqld(8)

http://dev.mysql.com/doc/refman/en/using-systemd.html

Process: 5281 ExecStartPre=/usr/bin/mysqld\_pre\_systemd (code=exited, status=0/SUCCESS)

Main PID: 5299 (mysqld)

Status: "SERVER\_OPERATING"

CGroup: /system.slice/mysqld.service

└─5299 /usr/sbin/mysqld

Jun 03 18:31:50 {your-server-name} systemd[1]: Starting MySQL Server...

Jun 03 18:31:51 {your-server-name} systemd[1]: Started MySQL Server.

以上信息表示MySQL服务启动成功。

**2 MySQL默认密码和修改密码**

在启动MySQL服务的时候，主要会发生以下4件事

* MySQL Server初始化并启动起来；
* MySQL的data文件夹中生成SSL证书和key文件；
* 密码验证组件被安装并且生效；
* 创建一个超级管用户*'root'@'localhost‘*。超级用户设置的密码被保存在错误日志文件中，可以通过以下命令查看：
* shell> sudo grep 'temporary password' /var/log/mysqld.log
* 2018-06-03T10:15:57.448920Z 5 [Note] [MY-010454] [Server] A temporary password is generated for root@localhost: 0xxXxxXx?xXX

通过默认密码登录MySQL服务器，并马上修改密码(**强烈建议**)！！！。  
用默认密码(0xxXxxXx?xXX)登录：

shell> mysql -uroot -p

修改密码：

mysql> ALTER USER 'root'@'localhost' IDENTIFIED BY '\*{your-password}\*';

退出MySQL并用新密码重新登录，然后就可以在MySQL中尽情发挥想象了。

# 修改登陆域

1，登进MySQL之后，

2，输入以下语句，进入mysql库：

use mysql

3，更新域属性，'%'表示允许外部访问：

update user set host='%' where user ='root';

4，执行以上语句之后再执行：

FLUSH PRIVILEGES;

5，再执行授权语句：

GRANT ALL PRIVILEGES ON \*.\* TO 'root'@'%'WITH GRANT OPTION;

然后外部就可以通过账户密码访问了。

6，其它说明：

FLUSH PRIVILEGES; 命令本质上的作用是：

将当前user和privilige表中的用户信息/权限设置从mysql库(MySQL数据库的内置库)中提取到内存里。

MySQL用户数据和权限有修改后，希望在"不重启MySQL服务"的情况下直接生效，那么就需要执行这个命令。

通常是在修改ROOT帐号的设置后，怕重启后无法再登录进来，那么直接flush之后就可以看权限设置是否生效。

而不必冒太大风险。

三、可能存在的其它问题：

执行完之后，再用Navicat连接mysql，报错如下：

Client does not support authentication protocol requested by server；

报错原因：

mysql8.0 引入了新特性 caching\_sha2\_password；这种密码加密方式Navicat 12以下客户端不支持；

Navicat 12以下客户端支持的是mysql\_native\_password 这种加密方式；

解决方案：

1，用如下语句查看MySQL当前加密方式

select host,user,plugin from user;

查询结果

+-----------+------------------+-----------------------+

| host | user | plugin |

+-----------+------------------+-----------------------+

| % | root | caching\_sha2\_password |

| localhost | mysql.infoschema | mysql\_native\_password |

| localhost | mysql.session | mysql\_native\_password |

| localhost | mysql.sys | mysql\_native\_password |

+-----------+------------------+-----------------------+

看第一行，root加密方式为caching\_sha2\_password。

2，使用命令将他修改成mysql\_native\_password加密模式：

update user set plugin='mysql\_native\_password' where user='root';

再次连接的时候，就成功了。

四、如果还连接不上

通过以上操作后，依然无法连接上，问题可能出在了防火墙上。

1，MySQL部署在实体服务器上解决方案如下：

a.开放MySQL的端口号，默认端口号是3306。

b.直接关闭防火墙（慎重操作，不建议。当然测试玩的话就随意了。。。。）

2，MySQL部署在云计算机上的方案如下：

a.以阿里云为例，找到实例，设置安全组，开放端口号即可。

————————————————

版权声明：本文为CSDN博主「lemon\_cake」的原创文章，遵循 CC 4.0 BY-SA 版权协议，转载请附上原文出处链接及本声明。

原文链接：https://blog.csdn.net/h996666/article/details/80921913