# 1、CentOS7下安装mysql5.7

## 一、安装YUM Repo

1、由于CentOS 的yum源中没有mysql，需要到mysql的官网下载yum repo配置文件。

下载命令：

wget https://dev.mysql.com/get/mysql57-community-release-el7-9.noarch.rpm

2、然后进行repo的安装：

rpm -ivh mysql57-community-release-el7-9.noarch.rpm

执行完成后会在/etc/yum.repos.d/目录下生成两个repo文件mysql-community.repo mysql-community-source.repo

## 二、使用yum命令即可完成安装

注意：必须进入到 /etc/yum.repos.d/目录后再执行以下脚本

1、安装命令：

yum install mysql-server

2、启动msyql：

systemctl start mysqld #启动MySQL

3、获取安装时的临时密码（在第一次登录时就是用这个密码）：

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

4、倘若没有获取临时密码，则

4.1、删除原来安装过的mysql残留的数据

rm -rf /var/lib/mysql

4.2.再启动mysql

systemctl start mysqld #启动MySQL

## 三、登录：

1、方式一（已验证）：

mysql -u root -p

然后输入密码（刚刚获取的临时密码）

2、方式二（未验证）：

进入mysql数据库

root@test:/home# mysql -uroot -proot   <uroot是用户名，proot是密码>

如：

root@test:/home# mysql -root -XXXX

3、若登录不了，则进行以下配置，跳过登录验证

3.1、重置密码的第一步就是跳过MySQL的密码认证过程，方法如下：

3.2、vim /etc/my.cnf(注：windows下修改的是my.ini)

在文档内搜索mysqld定位到[mysqld]文本段：

/mysqld(在vim编辑状态下直接输入该命令可搜索文本内容)

在[mysqld]后面任意一行添加“skip-grant-tables”用来跳过密码验证的过程，如下图所示：

3.3、保存文档并退出：

#:wq

3.4、接下来我们需要重启MySQL：

## 四、登录成功后修改密码

1、注意：这里会进行密码强度校验（密码设置时必须包含大小写字母、特殊符号、数字，并且长度大于8位）

2、如不满足以上条件则会报错，如下图：

密码策略问题异常信息：

ERROR 1819 (HY000): Your password does not satisfy the current policy requirements

3、解决办法：

3.1、查看 mysql 初始的密码策略，

输入语句 “ SHOW VARIABLES LIKE 'validate\_password%'; ” 进行查看，

如下图：

3.2、首先需要设置密码的验证强度等级，设置 validate\_password\_policy 的全局参数为 LOW 即可，

输入设值语句 “ set global validate\_password\_policy=LOW; ” 进行设值，

3.3、当前密码长度为 8 ，如果不介意的话就不用修改了，按照通用的来讲，设置为 6 位的密码，设置 validate\_password\_length 的全局参数为 6 即可，

输入设值语句 “ set global validate\_password\_length=6; ” 进行设值，

3.4、现在可以为 mysql 设置简单密码了，只要满足六位的长度即可，

输入修改语句 “ ALTER USER 'root'@'localhost' IDENTIFIED BY '123456'; ” 可以看到修改成功，表示密码策略修改成功了！！！

3.5、注：在默认密码的长度最小值为 4 ，由 大/小写字母各一个 + 阿拉伯数字一个 + 特殊字符一个，

只要设置密码的长度小于 3 ，都将自动设值为 4 ，

3.6、关于 mysql 密码策略相关参数；

1）、validate\_password\_length  固定密码的总长度；

2）、validate\_password\_dictionary\_file 指定密码验证的文件路径；

3）、validate\_password\_mixed\_case\_count  整个密码中至少要包含大/小写字母的总个数；

4）、validate\_password\_number\_count  整个密码中至少要包含阿拉伯数字的个数；

5）、validate\_password\_policy 指定密码的强度验证等级，默认为 MEDIUM；

关于 validate\_password\_policy 的取值：

LOW：只验证长度；

1/MEDIUM：验证长度、数字、大小写、特殊字符；

2/STRONG：验证长度、数字、大小写、特殊字符、字典文件；

6）、validate\_password\_special\_char\_count 整个密码中至少要包含特殊字符的个数；

## 五、修改密码

1、方式一（已验证）：

ALTER USER 'root'@'localhost' IDENTIFIED BY '@abcd123456';

2、方式二（未验证）

set password=password("yourpassword");

## 六、开启远程控制

MySQL默认是没有开启远程控制的，必须添加远程访问的用户，即默认是只能自己访问，别的机器是访问不了的。

1、方式一（已验证）：

　   1.1、连接服务器: mysql -u root -p

　　1.2、看当前所有数据库：show databases;

　　1.3、进入mysql数据库：use mysql;

　　1.4、查看mysql数据库中所有的表：show tables;

　　1.5、查看user表中的数据：select Host, User,Password from user;

　　1.6、修改user表中的Host:   update user set Host='%' where User='root';

                说明： % 代表任意的客户端,可替换成具体IP地址。

　　1.7、最后刷新一下：flush privileges;

       1.8、注意：一定要记得在写sql的时候要在语句完成后加上" ; "

2、方式二（未验证）：

1、使用 grant 命令

grant all privileges on 数据库名.表名 to 创建的用户名(root)@"%" identified by "密码";

2、格式说明：

数据库名.表名 如果写成\*.\*代表授权所有的数据库 flush privileges; #刷新刚才的内容

如：

grant all privileges on \*.\* to root@"113.123.123.1" identified by "123456789";

@ 后面是访问mysql的客户端IP地址（或是 主机名） % 代表任意的客户端，如果填写 localhost 为本地访问（那此用户就不能远程访问该mysql数据库了）

## 七、其他配置

1、设置安全选项：

mysql\_secure\_installation

2、关闭MySQL

systemctl stop mysqld

3、重启MySQL

systemctl restart mysqld

4、查看MySQL运行状态

systemctl status mysqld

5、设置开机启动

systemctl enable mysqld

6、关闭开机启动

systemctl disable mysqld

7、配置默认编码为utf8：

vi /etc/my.cnf #添加 [mysqld] character\_set\_server=utf8 init\_connect='SET NAMES utf8'

其他默认配置文件路径：

配置文件：/etc/my.cnf 日志文件：/var/log//var/log/mysqld.log 服务启动脚本：/usr/lib/systemd/system/mysqld.service socket文件：/var/run/mysqld/mysqld.pid

8、查看版本

select version();

# 2、安装Redis

## 1.获取redis资源

　　wget http://download.redis.io/releases/redis-5.0.8.tar.gz

## 2.解压

　　tar xzvf redis-5.0.8.tar.gz

## 3.安装

1、cd redis-5.0.8

2、make

报错没有gcc执行yum install gcc-c++

make  distclean   清除之前编译失败的文件

　　3、cd src

　　make install PREFIX=/usr/local/redis

## 4.移动配置文件到安装目录下

　　cd ../

　　mkdir /usr/local/redis/etc

　　mv redis.conf /usr/local/redis/etc

## 5.配置redis为后台启动

vi /usr/local/redis/etc/redis.conf //将**daemonize no** 改成daemonize yes

redis-cli设置密码 config set requirepass

## 6.将redis加入到开机启动

vi /etc/rc.local //在里面添加内容：/usr/local/redis/bin/redis-server /usr/local/redis/etc/redis.conf (意思就是开机调用这段开启redis的命令，给/usr/local/redis/etc/redis.conf执行权限)

## 7.开启redis

　　/usr/local/redis/bin/redis-server /usr/local/redis/etc/redis.conf

常用命令

　　redis-server /usr/local/redis/etc/redis.conf //启动redis

　　pkill redis  //停止redis

　　卸载redis：

　　　　rm -rf /usr/local/redis //删除安装目录

　　　　rm -rf /usr/bin/redis-\* //删除所有redis相关命令脚本

　　　　rm -rf /root/download/redis-4.0.4 //删除redis解压文件夹

## 8-启动redis:

两种方式：

redis-server &

加上`&`号使redis以后台程序方式运行

或者是

redis-server

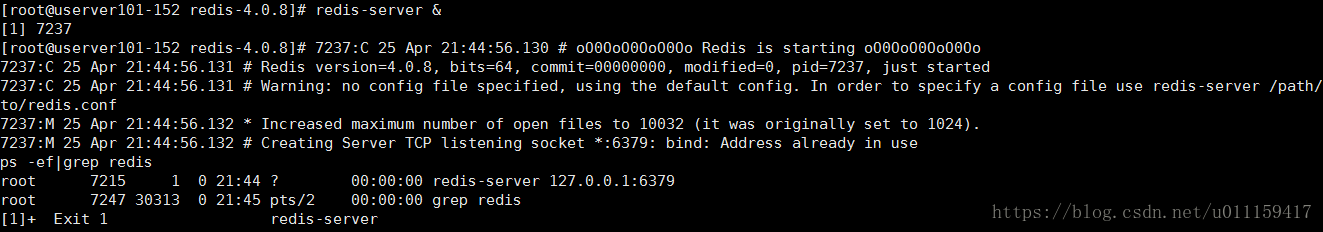
## 9-检测后台进程是否存在

ps -ef |grep redis

## 10-检测6379端口是否在监听

netstat -lntp | grep 6379

有时候会报异常



原因: Redis已经启动

解决: 关掉Redis,重启即可

1. redis-cli shutdown
2. redis-server

然后你就能看到Redis愉快的运行了.

# 3、阿里云部署edis连接不上问题

在redis配置文件中修改bind参数：bind 0.0.0.0，关闭保护模式：

protected-mode no

启动redis配置：./redis-server ../redis.conf   (配置文件位置)。

如果还不行，注释所有bind参数重启redis服务。

注意防火墙设置打开相应的端口，阿里云后台管理也要开放redis端口。

# 4、阿里云服务器被挖矿

CPU内存过高，经常端口禁用

清除的过程

使用top已经知道了进程号，接下来看看位置，命令ls -l proc/{进程号}/exe

sysupdate、networkservice都在/etc/目录下

到etc下，除了sysupdate、networkservice 同时还有sysguard、update.sh，除了update.sh其余的都是二进制文件，应该就是挖矿的主程序以及守护程序了。

找到了源头update.sh，接下来分析下这个脚本。

恩。。。我们有时间再写分析过程，这里先直接给出解决方案。

删除定时任务

rm /var/spool/cron/root 或crontab -r

1

杀掉进程 删除文件

首先杀进程，kill -9 {进程号}，然后删除文件

直接删除sysupdate你会发现无法删除，因为一般病毒会使用chattr +i命令，我们使用chattr -i sysupdate，然后再 rm -f sysupdate 即可正常删除。

同理删除networkservice、sysguard、update.sh、config.json。

/root/.ssh/authorized\_keys 删除或修复 rm-rf /root/.ssh/authorized\_keys

如果你被攻破的是root用户(或者被攻破的用户权限较大),你可能还需要

修复SELinux

病毒脚本首先就会尝试关闭SELinux子系统，我们可以使用getenforce命令查看SELinux状态。

如果你想要重新打开，可以修改/etc/selinux/config文件将SELINUX=disabled改为SELINUX=enforcing，然后重新启动服务器。

wget命令和curl命令会被改为wge和cur，这样用着很变扭，改回来

mv /bin/wge /bin/wget

mv /bin/cur /bin/curl

mv /usr/bin/wge /usr/bin/wget

mv /usr/bin/cur /usr/bin/curl

恢复防火墙配置

这里给出病毒脚本修改的iptables配置的语句，方便读者修复

iptables -F

iptables -X

iptables -A OUTPUT -p tcp --dport 3333 -j DROP

iptables -A OUTPUT -p tcp --dport 5555 -j DROP

iptables -A OUTPUT -p tcp --dport 7777 -j DROP

iptables -A OUTPUT -p tcp --dport 9999 -j DROP

iptables -I INPUT -s 43.245.222.57 -j DROP

service iptables reload

# 5、RedisDesktopManager连不上设置密码后的redis

背景：我是在自己机器上装的redis，使用的是虚拟机，系统是linux 版本是centeros-6.7

在使用这个连接redis的时候，发现连接不上。

第一步：在自己的本机外面试下能不能连接上虚拟机，打开cmd，使用 ping 192.168.65.128  （192.168.65.128这个为虚拟机的ip地址 查看虚拟机的ip地址：命令 ifconfig）

如果能ping的通，这个没问题，表示外部可以访问得到。访问不到可以，把虚拟机的防火墙给关了，最省事，命令： service iptables stop

第二步：在redis的配置文件里面，是否把bind 127.0.0.1 给注释掉，如果没有，连接不上

第三步：在redis的配置文件里面，是否把本地保护模式给关闭，如果没有，连接不上，关闭方式：protected-mode no

如果你没有设置密码，应该是可以连接上了。如果你设置了密码，请看下面：

1：在redis的配置文件（redis.conf）里面设置了requirepass  表示连接的密码

如果还是连接不上，你首先在你虚拟机里面登录上redis的客户端 进入到src目录层级下面。

和启动redis一样，命令： ./redis-cli

进入到客户端之后：命令：auth 123456（你设置的密码）

看一下是否ok。

我之前在这里踩了坑，明明我的配置文件里面设置了访问密码，却没有生效，为了保险起见，还是再来看下，密码是否生效了

如果ok,那就没有问题，如果出现了错误，说你密码没有设置，那就直接用命令设置：config set requirepass 123456(这个为你设置的访密码)

然后再试下命令 auth 123456（出现ok就好了）