### Centos普通用户启动redis服务

**为了保证生产环境服务器的安全，在工作中有一个规范，要求我们运行的服务都要求以非登陆的普通用户运行，从而防止程序本身的漏洞被利用被黑客提权！**

**首先注明，我的redis目录为，根据自己的redis目录做修改：/usr/local/redis-5.0.2**

建立用户组： groupadd redis

建立普通用户： useradd redis -M -g redis -s /sbin/nologin

拓展useradd知识：

 -d 指定用户家目录（默认是/home目录下）

 -M 禁止创建用户家目录（常配合非登陆用户使用）

 -s 指定shell类型 （默认是/bin/bash ，/sbin/nologin 为禁止登陆）

#创建redis运行时的pid目录（默认是/var/run/但是仅限root用户创建，如果普通用户运行的，必须在其下自创目录，并chown授权）

mkdir -pv /var/run/redis && chown –R redis:redis /var/run/redis

#新建日志文件

mkdir -pv /var/log/redis/ && chown -R redis:redis /var/log/redis/

#新建redis数据目录，并且授权给redis用户为所有权

mkdir -pv /usr/local/redis/data/ && chown -R redis:redis /usr/local/redis/data/

#拷贝配置文件到redis的目录

cp /usr/local/redis-5.0.2/redis.conf /usr/local/redis/

注意：我们的appendonly.aof文件默认是644权限，其他用户只读。所以修改普通用户前，看看该文件在哪个路径下，并且检查是否chown redis了，也可以给他直接加w权限，但是为了安全不推荐。如果该文件没权限，修改后会启动redis失败，报错如下。



所以最好更改下redis所属的用户：chown –R redis:redis “这里是redis的源码目录”

修改redis.conf 配置文件，登陆密码和端口什么的根据自己的需要配置，这里我配置的是9379端口：

port 9379

pidfile /var/run/redis/redis\_9379.pid

logfile "/var/log/redis/redis.log"

dir "/usr/local/redis/data"

新增redis开机启动文件

vim /usr/lib/systemd/system/redis.service

指定普通用户运行，全靠我们的开启启动文件进行配置 ，wq保存后。

[Unit]

#redis服务自启动

Description=redis-server

After=network.target

[Service]

User=redis

Group=redis

Type=forking

PIDFile=/var/run/redis/redis\_9379.pid

ExecStart=/usr/local/redis-5.0.2/src/redis-server /usr/local/redis/redis9379.conf

PrivateTmp=true

[Install]

WantedBy=multi-user.target

执行:

 systemctl darmon-reload

 service redis restart

正常情况如下图所示：



使用：ps aux|grep redis

可以看到已经是用redis用户启动了

