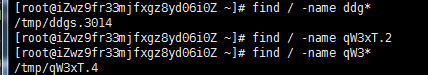
# 找出挖矿工具

执行

find / -name ddg\*

find / -name qW3\*

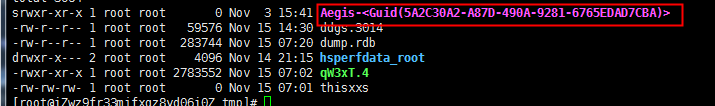


如果出现这两个东西则表示被挖矿了

进入这些工具下的目录

cd /tmp

输入 ll 后会出现可疑的东西



再输入

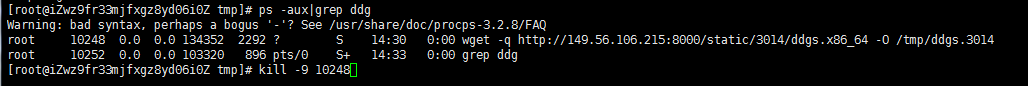
find / –name Aegis-\*



# 清理挖矿工具

输入

ps -aux|grep ddg



杀掉他

kill -9 10248

同样步骤

ps -aux|grep qW3xT.2

执行删除命令

rm -rf /tmp/ddgs.3014

rm -rf /tmp/qW3xT.4

rm –rf /tmp/Aegis-<Guid(5A2C30A2-A87D-490A-9281-6765EDAD7CBA)>

rm –rf /usr/local/aegis/Aegis-<Guid(5A2C30A2-A87D-490A-9281-6765EDAD7CBA)>

清理完成

出现阿里云服务器被挖矿时,有可能是阿里云开放了redis的6379端口,redis是不用密码就可以链接的,把redis设置一下密码.

如果还是不行就直接重装系统