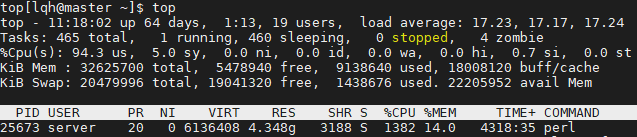
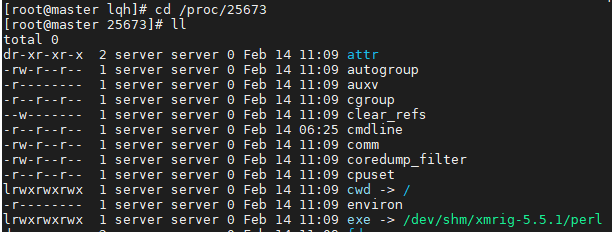
服务器计算资源异常报告

1. 异常发现与解决

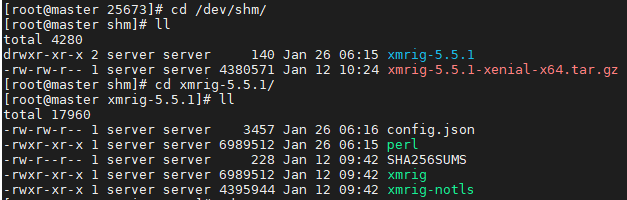
top命令查看进程，发现异常如下（单个进程占用了master节点上所有计算资源）



进一步查看PID为25673进程的对应命令，发现执行命令来自/dev/shm/xmrig-5.5.1程序文件夹（门罗币挖矿软件）下



该挖矿软件文件夹中内容如下



kill -9命令直接终止挖矿进程，恢复正常

1. 异常原因追溯

该挖矿软件所有者为server，但server并不在我们课题组的用户列表内，怀疑其可能是工程师调试时创建的临时账户，密码设立不完善，而被人恶意暴力破解登录。

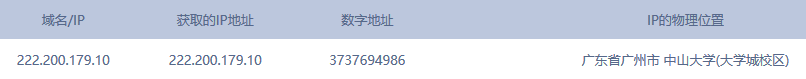
查询server用户最近登录的时间、登录IP地址如下所示，其登录IP为202.116.118.166（2020.1.26）和222.200.179.10（2020.2.14）



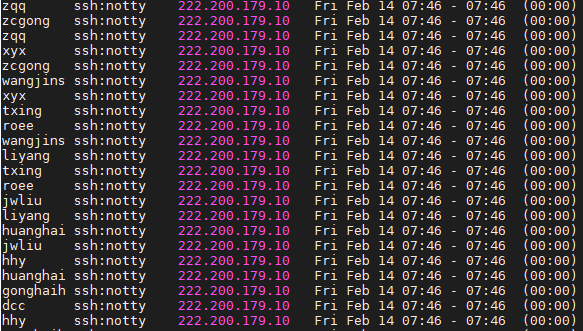
对这两个IP地址进行IP地址查询，结果如下所示（均为校内ip地址）

由xc师兄向网络信息中心咨询后知，202开头的ip地址为北校区科技楼wjc老师所有，222开头的ip地址可能为经过中大VPN转发后的ip地址。





进一步查看被阻止的登录记录，发现该222开头的ip地址还存在尝试暴力破解我们课题组服务器对应账号密码的行为，仅在今日（2020.2.14）上午就尝试了多达4200余次。





1. 解决措施
   1. 再次提醒课题组内其他成员将密码修改成不易被暴力破解的形式
   2. 及时清理无用账户，避免不安全的登录（已删除t99、server等账户）
   3. 彻底删除挖矿软件，并对相应文件夹设置权限
   4. 可安装专用屏蔽SSH暴力破解行为的软件，或直接封禁ip
   5. 必要时可向学校或网警报告，其涉嫌[非法侵入计算机系统罪](https://baike.baidu.com/item/%E9%9D%9E%E6%B3%95%E4%BE%B5%E5%85%A5%E8%AE%A1%E7%AE%97%E6%9C%BA%E4%BF%A1%E6%81%AF%E7%B3%BB%E7%BB%9F%E7%BD%AA)（刑法285条）