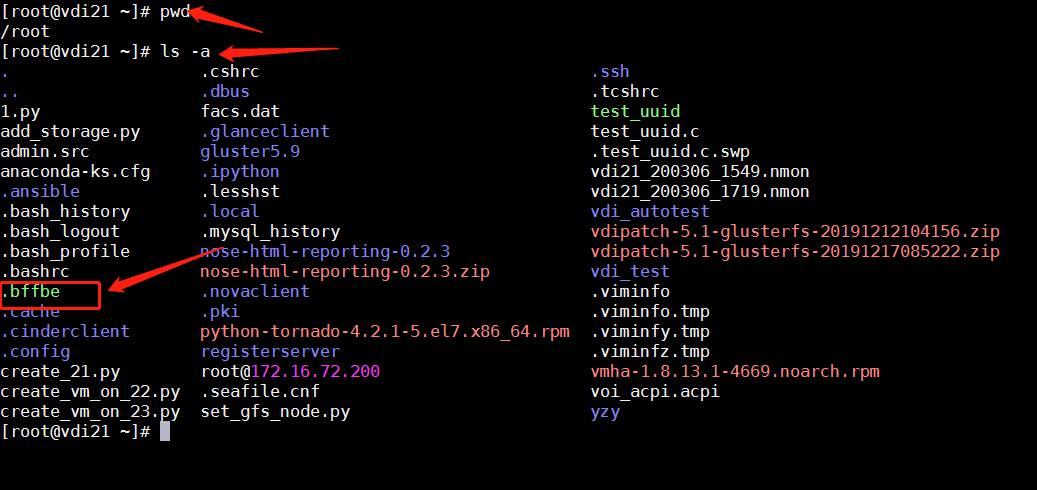
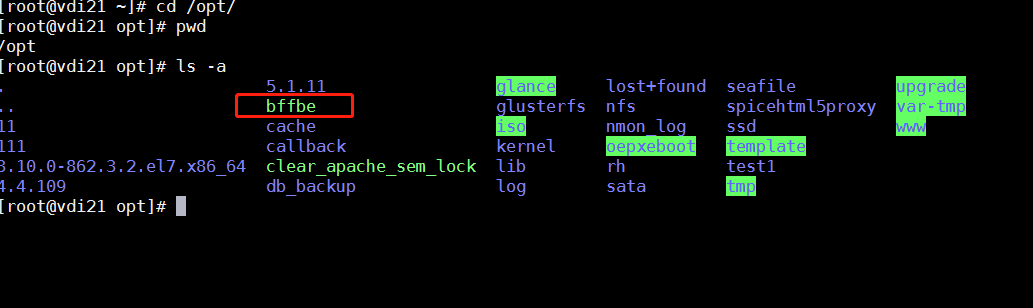
# Bffbe 病毒查杀办法

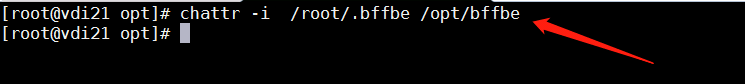
**1，病毒文件路径**



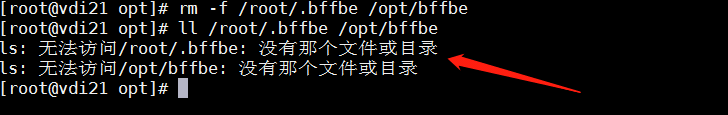


**2，删除病毒文件**

1. Chattr –i 修改文件属性

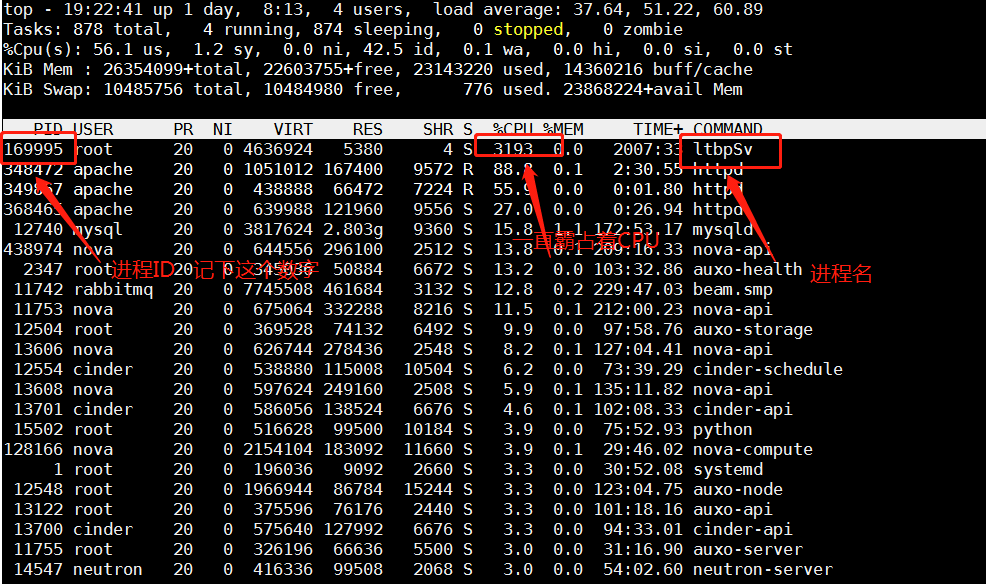


1. ，rm –f 删除病毒文件



1. **处理病毒进程**

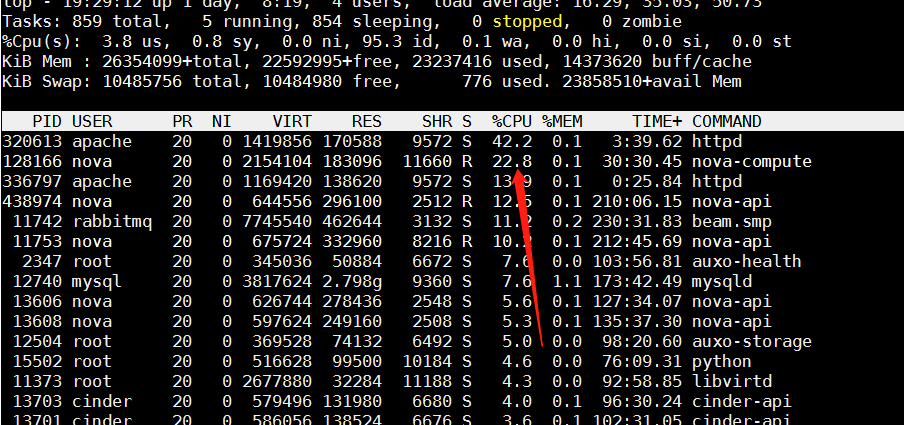
1，top命令查看病毒进程



1. kill -9 干掉169995



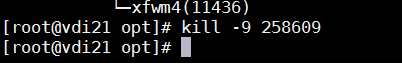
1. 检查



1. **还有守护进程的。用pstree -p |more查看。（注意这个鬼）**



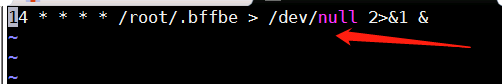


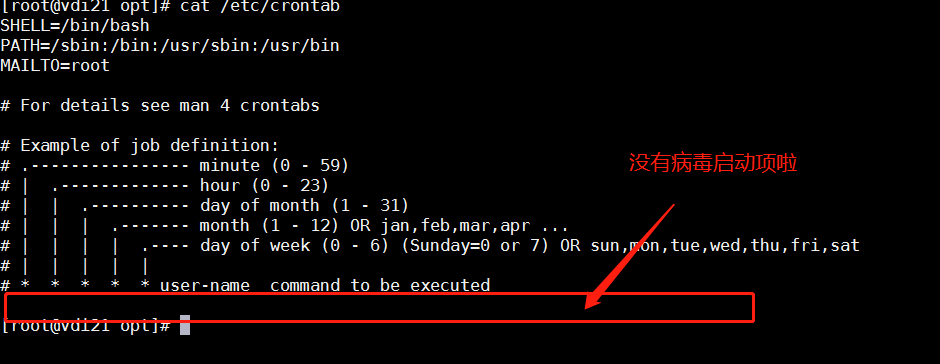


1. 开始干掉病毒的启动器.

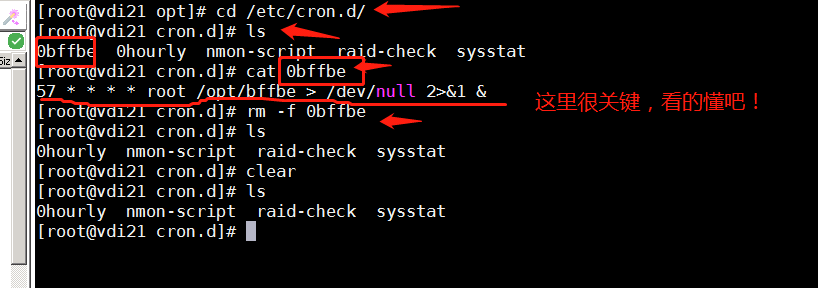
1,干掉计划任务 crontab –e 整个动作一定要快



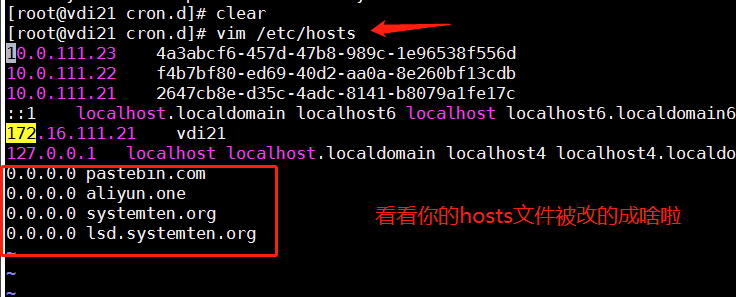
2，看着代码就知道是啥意思啦。dd删除这一行，保存修改(命令模式 按 ：x)



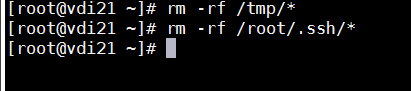
3，还没有完哦，还有隐藏的启动项



4.vim /etc/hosts 编辑hosts文件，还是用dd 删 ： x 保存

****

5，清除隐患



杀毒完成。

最后：

杀毒后几个建议

1. passwd修改操作系统登录密码。
2. redis服务开启密码验证。
3. sshd 修改端口。

/var/log/cron

/查ssh登陆的ip