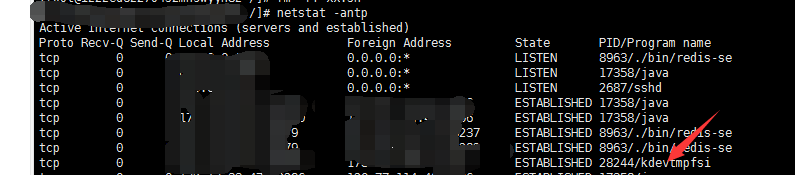
# **一. 错误信息**

先上阿里云上的报警信息。有个最大的问题是：****top命令查看自己服务器CPU运行情况，会发现kdevtmpfsi的进程，CPU使用率为100%****，第一次删除干净了kdevtmpfsi程序，没曾想几分钟以后，就出现了第二个警告。使用netstat -antp命令查看端口使用情况，又出现了kdevtmpfsi如图三所示

netstat -antp







# **二.解决问题**

一般出现kdevtmpfsi病毒都会伴有定时任务，就会出现我上面说的处理一次后，又会继续出现，反反复复处理不干净。

## **1.首先停掉kdevtmpfsi的程序**

ps aux



删除掉与kdevtmpfsi相关的进程

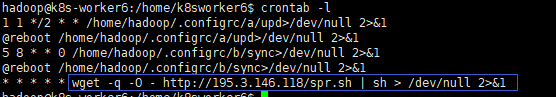
kill -9 20267kill -9 20367

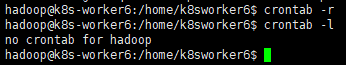
* 1
* 2

## **2.删除Linux下的异常定时任务**

crontab -l 查看定时任务

crontab -r 表示删除用户的定时任务，当执行此命令后，所有用户下面的定时任务会被删除





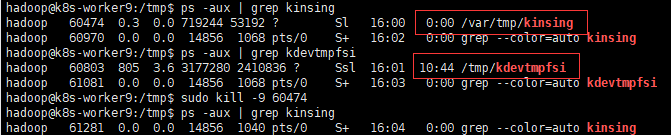
## **3.结束kdevtmpfsi进程及端口占用**

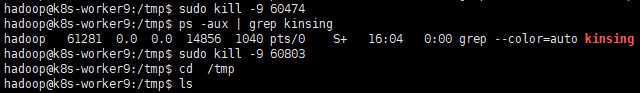
netstat -antp

* 1

找到kdevtmpfsi端口 我这里是28244 一中第三张图可以看到。不要直接杀掉，因为有守护线程还会重启。

ps -aux | grep kinsingps -aux | grep kdevtmpfsi





kill -9 28244kill -9 28829

* 1
* 2

## **4.删除掉kdevtmpfsi的相关文件**

cd /tmplsrm -rf kdevtmpfsi rm -rf /var/tmp/kinsing

最后自己可以再检查一下是否还有kdevtmpfsi的相关文件，有的话就继续删除

find / -name kdevtmpfsi

find / -name kinsing

# **三.怎么预防处理这个病毒**

最根本的原因是自己的redis 6379配置不当导致的。大家可以参考阿里云的Redis服务安全加固  
[阿里Redis服务安全加固](https://help.aliyun.com/knowledge_detail/37447.html?spm=a2c4g.11186631.2.2.828c1848kuRv6p)

https://help.aliyun.com/knowledge\_detail/37447.html?spm=a2c4g.11186631.2.2.828c1848kuRv6p

您的点赞，是我更新的动力！  
如有错误，还望指正