【删库不跑路】—Linux系统自杀实验 rm -rf /* 及如何抢救和预防

原创

置顶 姬无力 于 2021-04-28 22:43:06 发布 15744 收藏 146
文章标签： 运维 linux 系统恢复 自杀实验

本文链接：https://blog.csdn.net/weixin_42350212/article/details/115703709

事情是这样的

想必大家都听说过一个笑话：一个程序员去公司面试，面试官让他随便写个shell脚本看看

结果程序员在公司机器上写了个简单的 rm -rf /*

今天博主好奇到无聊，想看看到底会有什么效果呢。

就拿了一台不用的废弃虚拟机系统玩了一把。

在这里跟大家，汇报一下战果：

大家一定注意谨慎：玩完之后，绝大部分数据无法恢复，系统会基本完全崩溃状态，

建议在废弃的机器上玩可以，正式环境千万不要，另外大家写删除命令的时候，也一定要小心

Linux机器准备

首先找了台好久不用的虚拟机，回到根目录下，直接执行rm -rf * ；

然后就开始看到系统开始从根目录开始删除

开始报一些无法删除的错误

```
[root@fea3 opt]# cd /
[root@fea3 /]# rm -rf *
rm: cannot remove `boot': Device or resource busy
rm: cannot remove `dev/pts/ptmx': Operation not permitted
rm: cannot remove `dev/shm': Device or resource busy
rm: cannot remove `misc': Device or resource busy
rm: cannot remove `net': Device or resource busy
```


因为一些正在运转的misc net等硬件文件 无法删除

当我们误操作的时候，发现这些rm： cannot remove...，就赶紧中止还有得救

相关路径解读

boot：启动路径，部分文件，正在运行删不掉。

misc net：硬件相关运行中，不允许删除。

dev/shm：

`/dev`:目录下一般都是一些设备硬件文件，例如磁盘、内存、摄像头、网卡等等。
`/dev/shm`： 这个目录是linux下一个利用内存虚拟出来的一个目录，这个目录中的文件都是保存在内存中，而不是磁盘上。

其大小是非固定的，即不是预先分配好的内存来存储的。(shm == shared memory)

dev/pts/ptmx

ptmx 虚拟终端相关文件 系统不让删除

```
[root@open-falcon pts]# ll
total 0
c--------- 1 root root 5, 2 Apr  2 14:28 ptmx
[root@open-falcon pts]# _
```

Linux终端：

另外sys目录下的一些系统文件包括，

挂载的磁盘信息等，root也是没有权限删除的，

其余的文件夹 opt mnt home root等等 统统被删除

Linux挣扎了一下：sys/block的块设备不让删除、

nfs文件系统的缓存、挂载记录、锁等不让删除

rm -rf /* 运行完之后

删除完成之后，我们在根目录下看一下：

ls 命令已经没有了，这是因为存放命令的/bin目录下的所有二进制命令文件都被删除了，

包括 yum pwd 等等统统没有了，只有cd命令还在，

这是因为cd命令并不在/bin下

whereis cd :查看一下，cd在/usr/bin目录下

```
[root@fea3 /]# ls
-bash: /bin/ls: No such file or directory
[root@fea3 /]# cd ..
[root@fea3 /]# cd boot/
[root@fea3 boot]# ls
-bash: /bin/ls: No such file or directory
[root@fea3 boot]# yum
-bash: yum: command not found
[root@fea3 boot]# ls
-bash: /bin/ls: No such file or directory
[root@fea3 boot]# cd ..
[root@fea3 /]# ls
-bash: /bin/ls: No such file or directory
[root@fea3 /]# pwd
/
[root@fea3 /]# cd /dev/
pts/ shm/
[root@fea3 /]# cd /
.autofsck     boot/         misc/         proc/         var/
.autorelabel  dev/          net/          sys/
[root@fea3 /]# cd /_
```

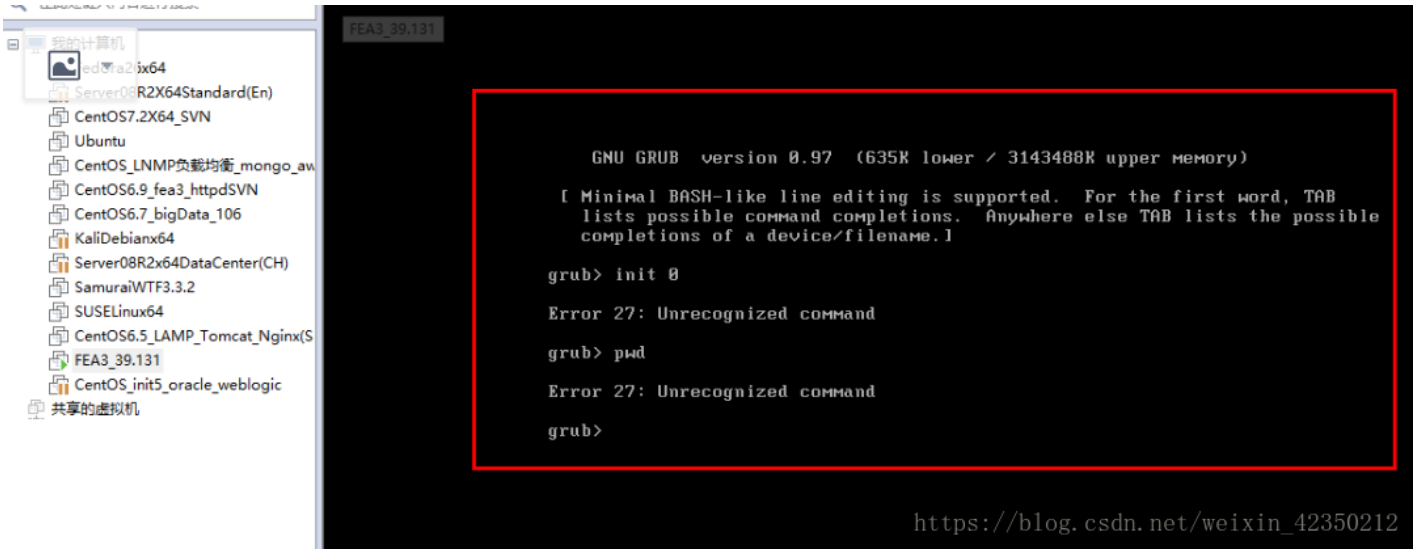

可以看到根目录下 只剩下/boot的启动文件夹。

硬件相关的misc net dev

sys系统相关文件夹

这是给我们下次启动时 进行启动牵引，牵引到grub界面 之后，由

于系统中所有的东西都被我们删除了，所以就卡死在grub界面 无法进内核。



抢救及预防措施

这个命令是极其危险的，所以一旦误操作

1、中止命令

首先，在意识到命令执行时，立即按Ctrl+C 终止命令。尽可能的保护系统文件。

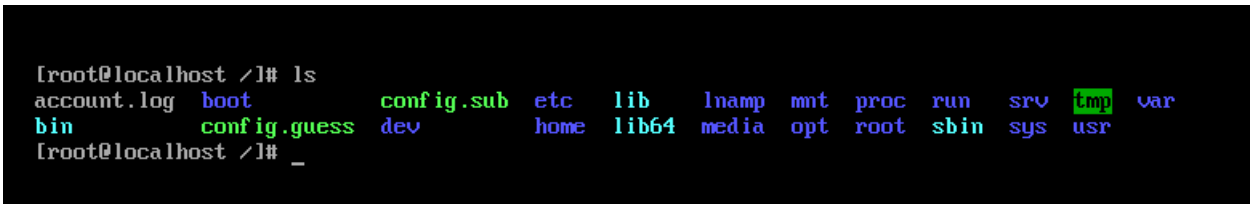
2、不要退出当前shell，不要重启

因为，我们不清楚，到底有哪些文件被删除了。

我们总会下意识的觉得，重启下就好了。这个时候千万不要重启，因为一重启，你可能无法再进入系统，连最后抢救的机会都没有了。

3、系统文件夹迁移

系统根目录下，大体就是这几个文件夹。



像/bin /sbin :主要是存储一些命令的文件夹。如果被删除了，我们可以通过从其他的服务器，将/bin目录，压缩，拷到当前服务器解压，进行替换。

4、系统快照

这是一个非常实用的方法。我们可以定时做系统快照，例如：每天凌晨2点，对系统做一个快照；也可以每逢比较重大的系统更新或者服务搭建之后，做一个快照。

这样，当我们误操作之后，就会有一个回退的备份。

5、命令重写

可以将rm -rf 重写，构造一个回收站，可以参考博主的这篇博文：

“你的rm -rf /*，我接盘了“——刚毕业的运维小姐姐总误删文件，我送了她一个命令行版 “回收站”

推荐阅读

【资源推荐】

- **渗透测试专用系统**
- kali-linux-e17-2019.1a-amd64.iso系统镜像
- https://download.csdn.net/download/weixin_42350212/15834456
- kali-linux-2018.4-amd64 操作系统
- https://download.csdn.net/download/weixin_42350212/13733164
- manjaro-xfce-17.1.7-stable-x86_64.iso系统镜像
- https://download.csdn.net/download/weixin_42350212/15834405
- WiFi专用渗透系统 nst-32-11992.x86_64.iso操作系统镜像
- https://download.csdn.net/download/weixin_42350212/15808682
- Parrot-security-4.1_amd64.iso 操作系统镜像
- https://download.csdn.net/download/weixin_42350212/15808365
- manjaro-xfce-17.1.7-stable-x86_64 操作系统
- https://download.csdn.net/download/weixin_42350212/13733286
- cyborg-hawk-linux-v-1.1 操作系统
- https://download.csdn.net/download/weixin_42350212/13733159
-
- **渗透测试相关工具**
- **渗透测试实战专栏**
- 【kali常用工具】上网行为监控工具
- https://download.csdn.net/download/weixin_42350212/13985799

- 【kali常用工具】抓包工具Charles Windows64位 免费版
- https://download.csdn.net/download/weixin_42350212/15898652
- 【kali常用工具】图印工具stamp.zip
- https://download.csdn.net/download/weixin_42350212/14980915
- 【kali常用工具】brutecrack工具[WIFIPR中文版]及wpa/wpa2字典
- https://download.csdn.net/download/weixin_42350212/13721381
- 【kali常用工具】EWSA 5.1.282-破包工具
- https://download.csdn.net/download/weixin_42350212/13704097
- 【kali常用工具】Realtek 8812AU KALI网卡驱动及安装教程
- https://download.csdn.net/download/weixin_42350212/13703770
- 【kali常用工具】无线信号搜索工具_kali更新
- https://download.csdn.net/download/weixin_42350212/13703729
- 【kali常用工具】inssider信号测试软件_kali常用工具
- https://download.csdn.net/download/weixin_42350212/13703705
- 【kali常用工具】MAC地址修改工具 保护终端不暴露
- https://download.csdn.net/download/weixin_42350212/13703597
- 【kali常用工具】脚本管理工具 php和jsp页面 接收命令参数 在服务器端执行
- https://download.csdn.net/download/weixin_42350212/13754997

- **Java实现照片GPS定位【完整脚本】**
- https://download.csdn.net/download/weixin_42350212/20024262
- **Python实现照片GPS定位【完整脚本】**
- https://download.csdn.net/download/weixin_42350212/19776215
- **女神忘记相册密码 python20行代码打开【完整脚本】**
- https://download.csdn.net/download/weixin_42350212/19871942
- **python修改证件照底色、大小、背景、抠图【完整源码】**
- https://download.csdn.net/download/weixin_42350212/19815306

python实战

- **【python实战】前女友婚礼，python破解婚礼现场的WIFI，把名称改成了**
- **【python实战】前女友发来加密的 “520快乐.pdf“，我用python破解开之后，却发现**
- **【python实战】昨晚，我用python帮隔壁小姐姐P证件照 自拍，然后发现...**
- **【python实战】女友半夜加班发自拍 python男友用30行代码发现惊天秘密**
- **【python实战】python你TM太皮了——区区30行代码就能记录键盘的一举一动**
- **【python实战】女神相册密码忘记了，我只用Python写了20行代码~~~**

【pygame开发实战开发30例 完整源码】

- https://download.csdn.net/download/weixin_42350212/15836285

【pygame游戏开发专栏，获取完整源码+教程】

- **一起来学pygame吧 游戏开发30例（二）——塔防游戏**
- **一起来学pygame吧 游戏开发30例（四）——俄罗斯方块小游戏**
- **渗透测试实战专栏**
- **Windows AD/Exchange管理专栏**
- **Linux高性能服务器搭建**
- **PowerShell自动化专栏**

CSDN官方学习推荐↓↓↓

- **CSDN出的Python全栈知识图谱，太强了，推荐给大家！**