超全！Linux 誤刪文件恢復命令及方法

網絡安全編程與黑客程序員 前天

作者：漠效

https://blog.csdn.net/GX_1_11_real/article/details/84571303

前言

無論在哪個系統中，刪除文件都是必須謹慎的操作。

因為如果不小心刪除了重要文件，就會導致個人或公司出現重大的損失。

類似於windows系統誤刪了文件，可以使用一些軟件進行恢復操作。Linux也是有幾款軟件可以做到誤刪恢復的。

注意事項：雖然有軟件可以對誤刪的數據進行恢復，但是完全恢復數據的概率並不是百分百的。

因此，使用rm命令刪除文件的時候，一定要小心；重要的數據一定要有備份；並且恢復刪除的數據前，刪除文件的目錄內不能往進存放新東西，否則覆蓋掉的信息無法找回。

下面介紹的就是對Linux中誤刪文件的恢復操作。

1、lsof

原理：

這個命令實際上並不能直接用來恢復文件，不過它可以列出被各種進程打開的文件信息。

配合其他命令，從/proc目錄下的信息中恢復“文件已刪除，但進程仍保持打開該文件的狀態”的文件。

/proc目錄是掛載的是在內存中所映射的一塊區域，當我們對這些文件進行讀取和寫入時，實際上是在從內存中獲取相關信息。

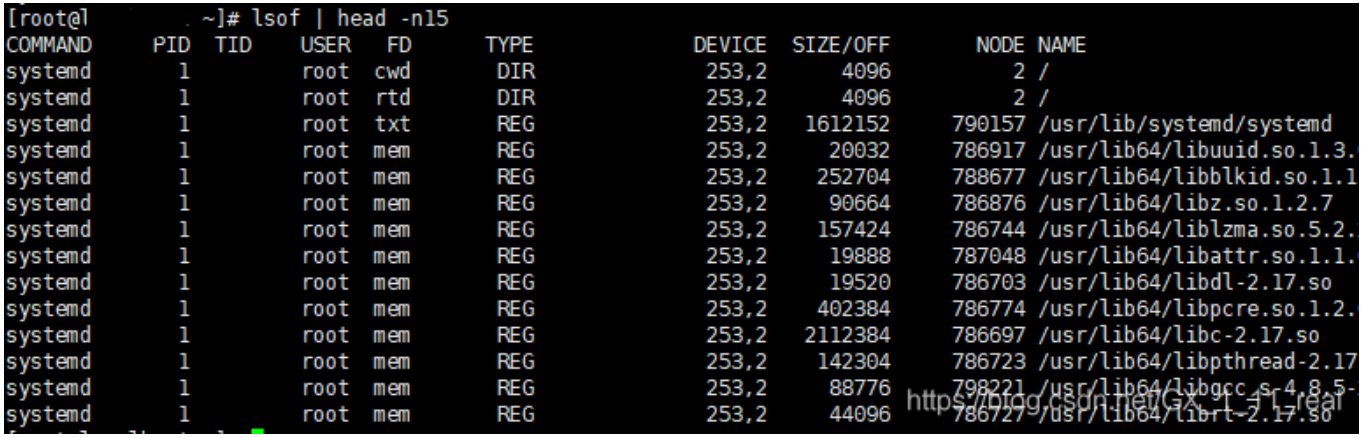
因此，當我們對文件進行讀取或寫入時(即有進程正使用文件時)，哪怕硬盤中的該文件已刪除，還可以從內存中的信息恢復文件。

注意：
必須以root用戶的權限運行，因為lsof需要訪問核心內存和各種文件。

只能恢復“文件已刪除，但進程仍保持打開該文件的狀態”的文件。

如果誤刪了目錄，目錄中的其他文件未被進程打開，沒有進行使用的文件將無法使用此方法恢復。

lsof輸出信息的意義：



COMMAND	进程的PID(进程标识符)
USER	进程所有者
FD	用来识别该文件(文件描述符)
DEVICE	指定磁盘的名称
SIZE	文件的大小
NODE	索引节点(文件在磁盘上的标识)
NAME	打开文件的确切名称

最常用参数:

-c	显示某进程现在打开的文件
-p	显示哪些文件被某pid进程打开
-g	显示归属某gid的进程情况
-d	显示目录下被进程开启的文件
-d	显示使用fd为4的进程
-i:80	显示打开80端口的进

恢復文件操作

環境：

在/mnt下有一些文件，其中一個文件train.less正在被查看，然後另一個終端將其刪除

【1】lsof查看

查看正在使用刪除文件的進程號

```
lsof /mnt
```

```
[root@          mnt]# lsof /mnt/
COMMAND   PID USER   FD   TYPE DEVICE SIZE/OFF    NODE NAME
bash    30694 root  cwd    DIR 253,17        0 1313234 /mnt/ferris/static (deleted)
bash    30701 root  cwd    DIR 253,17     4096       2 /mnt
less    31284 root  cwd    DIR 253,17        0 1313234 /mnt/ferris/static (deleted)
less    31284 root    4r   REG 253,17      358 1313235 /mnt/ferris/static/train.less (deleted)
lsof    31297 root  cwd    DIR 253,17     4096       2 /mnt
lsof    31298 root  cwd    DIR 253,17     4096       2 /mnt
```

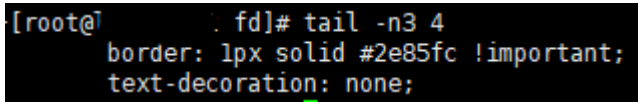
```
[root@l          mnt]# ll /mnt
总用量 24
drwx------ 2 root root 16384 8月  25 18:35 lost+found
drwxr-xr-x 2 root root  4096 9月  15 19:10 nfs01
```

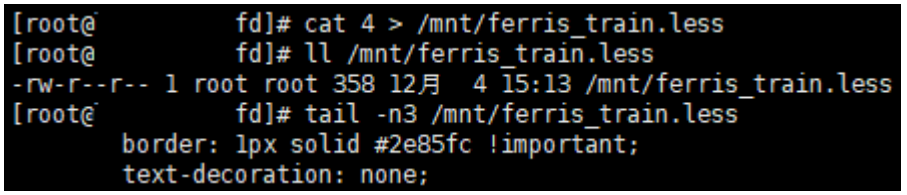
【2】恢復

切換到/proc下，刪除文件對應的進程的pid下的文件描述符中的目錄中；將對應的內容重定向或cp到其他文件中

重點關注：PID與FD

```
cd /proc/31284/fd/
 cat 4 > /mnt/ferris_train.less
```





2、extundelete

原理：

使用存儲在分區日誌中的信息，嘗試恢復已從ext3或ext4的分區中刪除的文件

優點：

相比於ext3grep只能恢復ext3文件系統的文件，其適用範圍更廣，恢復速度更快

extundelete官方地址(官方文檔)：

http://extundelete.sourceforge.net

extundelete下載地址：

http://downloads.sourceforge.net/project/extundelete/extundelete/0.2.4/extundelete-0.2.4.tar.bz2

(最新版本的extundelete是0.2.4，於2013年1月發布)

注意：

- 在數據刪除之後，要卸載被刪除數據所在的磁盤或是分區
- 如果是系統根分區遭到誤刪除，就要進入單用戶模式,將根分區以只讀的方式掛載,盡可能避免數據被覆蓋
- 數據被覆蓋後無法找回
- 恢復仍有一定的機率失敗，平時應對重要數據作備份，小心使用rm

安裝

1、依賴安裝

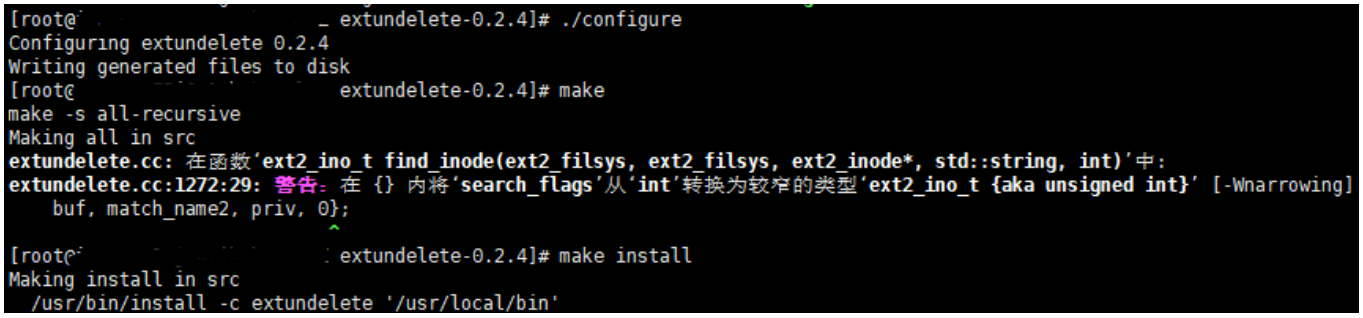
```
centos安装操作
yum install e2fsprogs-devel   e2fsprogs* gcc*

```

```
ubuntu安装操作
apt-get install build-essential  e2fslibs-dev  e2fslibs-dev
```

2、編譯安裝

```
wget http://downloads.sourceforge.net/project/extundelete/extundelete/0.2.4
tar xf  extundelete-0.2.4.tar.bz2
cd  extundelete-0.2.4
./configure
make
make install
```




```
cd /root/extundelete-0.2.4/src
```

```
[root@iZ2zeas52j0wtihsh815l9Z extundelete-0.2.4]# cd src/
[root@iZ2zeas52j0wtihsh815l9Z src]# ll
总用量 4664
-rw-r--r-- 1 ats  ats    22324 1月   3 2013 block.c
-rw-r--r-- 1 ats  ats     1170 1月   3 2013 block.h
-rw-r--r-- 1 ats  ats    24976 12月 31 2012 cli.cc
-rwxr-xr-x 1 root root 1323536 11月 29 12:58 extundelete
-rw-r--r-- 1 root root   49336 11月 29 12:58 extundelete-block.o
-rw-r--r-- 1 ats  ats    61470 1月   4 2013 extundelete.cc
-rw-r--r-- 1 root root  350496 11月 29 12:58 extundelete-cli.o
-rw-r--r-- 1 root root 1904408 11月 29 12:58 extundelete-extundelete.o
-rw-r--r-- 1 ats  ats     3425 12月 31 2012 extundelete.h
-rw-r--r-- 1 root root  850408 11月 29 12:58 extundelete-insertionops.o
-rw-r--r-- 1 ats  ats     1440 1月   3 2013 extundelete-priv.h
-rw-r--r-- 1 ats  ats    12176 12月 31 2012 insertionops.cc
-rw-r--r-- 1 ats  ats      229 11月  3 2012 jfs_compat.h
-rw-r--r-- 1 ats  ats    30742 12月 31 2012 kernel-jbd.h
-rw-r--r-- 1 root root   45769 11月 29 12:58 Makefile
-rw-r--r-- 1 ats  ats     1399 12月 31 2012 Makefile.am
-rw-r--r-- 1 ats  ats    51372 1月   4 2013 Makefile.in
```



```
extundelete -v
```

```
[root@          ~]# extundelete -v
extundelete version 0.2.4
libext2fs version 1.42.9
Processor is little endian.
```

執行make命令會在src目錄下生成extundelete可執行文件，可在此直接執行恢復命令。

執行make install會將程序安裝在/usr/local/bin/下

恢復文件操作

執行extundelete命令的當前目錄必須是可寫的。

1、查看要恢復文件的分區的文件系統

```
df  -Th
```

```
[root@          ~]# df -Th
文件系统        类型      容量  已用  可用 已用% 挂载点
/dev/vda2       ext4       20G  8.9G  9.6G   49% /
devtmpfs        devtmpfs  3.9G     0  3.9G    0% /dev
tmpfs           tmpfs     3.9G     0  3.9G    0% /dev/shm
tmpfs           tmpfs     3.9G  329M  3.5G    9% /run
tmpfs           tmpfs     3.9G     0  3.9G    0% /sys/fs/cgroup
/dev/vda1       ext4      190M   92M   85M   52% /boot
tmpfs           tmpfs     783M     0  783M    0% /run/user/0
/dev/vdb1       ext4       99G   61M   94G    1% /mnt
```

2、對要恢復文件的分區解除掛載

```
umount /mnt
```

```
[root@localhost ~]# umount /mnt
[root@localhost ~]# lsblk
NAME   MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
vda    253:0    0   20G  0 disk
├─vda1 253:1    0  200M  0 part /boot
└─vda2 253:2    0 19.8G  0 part /
vdb    253:16   0  100G  0 disk
└─vdb1 253:17   0  100G  0 part
```

3、查看可以恢復的數據

指定誤刪文件的分區進行查找

最後一列標記為Deleted的文件，即為刪除了的文件

```
extundelete /dev/vdb1 --inode 2 （根分区的inode值是2）
```

```
File name                                       | Inode number | Deleted status
.                                                 2
..                                                2
ferris                                            1310721        Deleted
nfs01                                             4718593        Deleted
test2.txt                                         12             Deleted
ferris_train.less                                 15             Deleted
.ferris_train.less.swp                            13             Deleted
ferris_train.less~                                14             Deleted
```

4、恢復單個目錄

指定要恢復的目錄名

如果是空目錄，則不會恢復

```
extundelete /dev/vdb1 --restore-directory  ferris
```

```
[root@    ~]# extundelete /dev/vdb1 --restore-directory ferris
NOTICE: Extended attributes are not restored.
Loading filesystem metadata ... 800 groups loaded.
Loading journal descriptors ... 576 descriptors loaded.
Searching for recoverable inodes in directory ferris ...
22 recoverable inodes found.
Looking through the directory structure for deleted files ...
1 recoverable inodes still lost.
```

```
[root@    ~]# cd RECOVERED_FILES/
[root@    RECOVERED_FILES]# ls
ferris
[root@    RECOVERED_FILES]# cd ferris/
[root@    ferris]# ls
build.sh  local.sh  readme.md  server.conf  static  widget
```

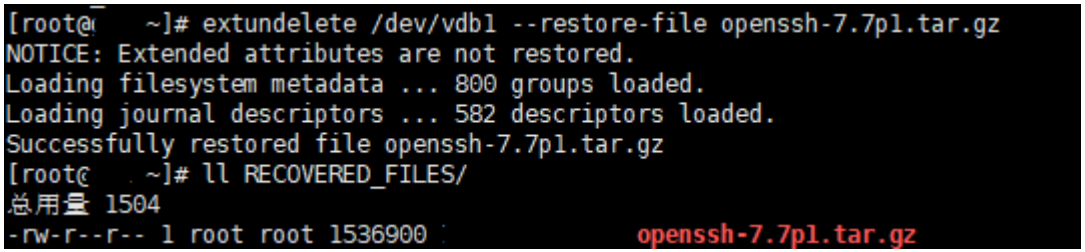
當執行恢復文件的命令後，會在執行命令的當前的目錄下生成RECOVERED_FILES目錄，恢復的文件都會放入此目錄中。如未生成目錄，即為失敗。

5、恢復單個文件

指定要恢復的文件名

如果幾k大小的小文件，有很大機率恢復失敗

```
extundelete /dev/vdb1 --restore-file openssh-7.7p1.tar.gz
```



6、恢復全部刪除的文件

無需指定文件名或目錄名，恢復全部刪除的數據

extundelete /dev/vdb1 --restore-all

喜歡此內容的人還喜歡

windows下遠程不落地上線的方式

雷神眾測

Linux系統安全-SELinux入門

謝公子學安全

組策略限制3389登錄的繞過方式

瀟湘信安