Linux系统下使用Lsof恢复误删除的文件 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/295/2021_2022_Linux_E7_B3_BB_E7_BB_c103_295999.htm 先介绍一些文件的基本概念， 文件实际上是一个指向inode的链接， inode链接包含了文件的所有属性， 比如权限和所有者， 数据块地址（文件存储在磁盘的这些数据块中）。 当你删除（rm）一个文件， 实际删除了指向inode的链接， 并没有删除inode的内容。 进程可能还在使用。 只有当inode的所有链接完全移去， 然后这些数据块将可以写入新的数据。 proc文件系统可以协助我们恢复数据。 每一个系统上的进程在/proc都有一个目录和自己的名字： 里面包含了一个fd（文件描述符）子目录（进程需要打开文件的所有链接）。 如果从文件系统中删除一个文件， 此处还有一个inode的引用： /proc/进程号/fd/文件描述符 接下来，你需要知道打开文件的进程号（pid）和文件描述符（fd）。 这些都可以通过lsof工具方便获得， lsof的意思是“ list open files， 列出（进程）打开的文件 ”。 然后你将可以从/proc拷贝出需要恢复的数据。 下面介绍在Fedora Core 5系统上使用lsof恢复误删的文件： 环境 主机： 使用微睦独立主机， 一台基于vmware的虚拟独立主机。 系统： Fedora Core 5 内核： 2.6.16-1.2122_FC5 lsof版本： [zhaoke@fedora5 ~]$ /usr/sbin/lsof -v lsof version information： revision： 4.77 预备工作： 如果你的系统没有安装lsof， 可以从作者网站或pbone获得。 恢复过程： 首先， 我们需要创建一个文本文件， 删除然后恢复： [zhaoke@fedora5 ~]$ man lsof | col -b > myfile 然后看一下文件内容： [zhaoke@fedora5 ~]$ less myfile 你可以看到lsof所有的文本

帮助信息。 现在按Ctrl-Z退出less命令， 然后在shell提示符下查看文件属性信息： [zhaoke@fedora5 ~]$ stat myfile File： `myfile ‘ Size： 116549 Blocks： 240 IO Block： 4096 regular file Device： fd00h/64768d Inode： 492686 Links： 1 Access： （0664/-rw-rw-r） Uid： （ 505/ zhaoke） Gid： （ 505/ zhaoke ） Access： 2006-11-20 12：59：38.000000000 0800 Modify： 2006-11-20 12：59：34.000000000 0800 Change： 2006-11-20 12 ：59：34.000000000 0800 没问题， 继续下面工作： [zhaoke@fedora5 ~]$ rm myfile [zhaoke@fedora5 ~]$ ls -l myfile ls ： myfile： No such file or directory [zhaoke@fedora5 ~]$ stat myfile stat： cannot stat `myfile ‘ ： No such file or directory myfile 文件删除了。 这时候， 你不要终止仍在使用文件的进程。 因为一旦终止， 文件将很难恢复。 现在我们开始找回数据， 首先用lsof查看一下： [zhaoke@fedora5 ~]$ lsof | grep myfile less 9104 zhaoke 4r REG 253，0 116549 492686 /home/zhaoke/myfile （0deleted） 第一个纵行是进程的名称（命令名）， 第二纵行是进程号（PID）， 第四纵行是文件描述符（r意思是普通文件）， 现在你知道9104进程仍有打开文件， 文件描述符是4. 那我们开始从/proc里面拷贝出数据。 你可能会考虑使用cp -a， 但实际上没有作用， 你将拷贝的是一个指向被删除文件的符号链接： [zhaoke@fedora5 ~]$ ls -l /proc/9104/fd/4 lr-x 1 zhaoke zhaoke 64 Nov 20 13：00 /proc/9104/fd/4 -> /home/zhaoke/myfile （0deleted） [zhaoke@fedora5 ~]$ cp -a /proc/9104/fd/4 myfile.wrong [zhaoke@fedora5 ~]$ ls -l myfile.wrong lrwxrwxrwx 1 zhaoke zhaoke 29 Nov 20 13：02 myfile.wrong -> /home/zhaoke/myfile （0deleted）

[zhaoke@fedora5 ~]$ file myfile.wrong myfile.wrong： broken symbolic link to `/home/zhaoke/myfile （0deleted）‘ [zhaoke@fedora5 ~]$ file /proc/9104/fd/4 /proc/9104/fd/4： broken symbolic link to `/home/zhaoke/myfile （0deleted）‘ 然后， 使用cp拷贝出数据： [zhaoke@fedora5 ~]$ cp /proc/9104/fd/4 myfile.saved 最后， 确认一下文件： [zhaoke@fedora5 ~]$ ls -l myfile.saved -rw-rw-r 1 zhaoke zhaoke 116549 Nov 20 13：03 myfile.saved [zhaoke@fedora5 ~]$ man lsof | col -b > myfile.new [zhaoke@fedora5 ~]$ cmp myfile.saved myfile.new