恢复Linux系统里被删除的Ext3文件Linux认证考试 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/586/2021_2022__E6_81_A2_E5_A4_8DLinu_c103_586594.htm 1、Ext3文件系统结构的简单介绍 在Linux所用的Ext3文件系统中，文件是以块为单位存储的，默认情况下每个块的大小是1K，不同的块以块号区分。每个文件还有一个节点，节点中包含有文件所有者，读写权限，文件类型等信息。对于一个小于12个块的文件，在节点中直接存储文件数据块的块号。如果文件大于12个块，那么节点在12个块号之后存储一个间接块的块号，在这个间接块号所对应的块中，存储有256个文件数据块的块号（Ext2fs中每个块号占用4字节，这样一个块中所能存储的块号就是1024/4=256）。如果有更大的文件，那么还会在节点中出现二级间接块和三级间接块。 2、恢复被误删文件的方法 大多数Linux发行版都提供一个debugfs工具，可以用来对Ext3文件系统进行编辑操作。不过在使用这个工具之前，还有一些工作要做。 首先以只读方式重新挂载被误删的文件所在分区。使用如下命令：（假设文件在/usr分区）[pre]mount -r -n -o remount /usr[/pre] r表示只读方式挂载；-n表示不写入/etc/mtab，如果是恢复/etc上的文件，就加上这个参数。如果系统说xxx partion busy，可以用fuser命令查看一下是哪些进程使用这个分区上的文件：[pre]fuser -v -m /usr[/pre] 如果没有什么重要的进程，用以下命令停掉它们：[pre]fuser -k -v -m /usr[/pre] 然后就可以重新挂载这些文件系统了。 如果是把所有的文件统一安装在一个大的/分区当中，可以在boot提示符下用linux single进入单用户模式，尽量减少系统进程向硬盘写

入数据的机会，要不干脆把硬盘挂在别的机器上。另外，恢复出来的数据不要写到/上面，避免破坏那些有用的数据。如果机器上有dos/windows，可以写到这些分区上面：[pre]mount -r -n /dev/hda1 /mnt/had[/pre] 然后就可以执行debugfs：（假设Linux在 /dev/hda5） [pre]#debugfs /dev/hda5[/pre] 就会出现debugfs提示符debugfs： 使用lsdel命令可以列出很多被删除的文件的信息： [pre]debugfs：lsdel debugfs: 2692 0deleted inodes found. Inode Owner Mode Size Blocks Time 0deleted 164821 0 100600 8192 1/ 1 Sun May 13 19:22:46 2001 36137 0 100644 4 1/ 1 Tue Apr 24 10:11:15 2001 196829 0 100644 149500 38/ 38 Mon May 27 13:52:04 2001 debugfs:[/pre] 列出的文件有很多（这里找到2692个），第一字段是文件节点号，第二字段是文件所有者，第三字段是读写权限，接下来是文件大小，占用块数，删除时间。然后就可以根据文件大小和删除日期判断那些是我们需要的。比如我们要恢复节点是196829的文件： 可以先看看文件数据状态： [pre]debugfs：stat Inode: 196829 Type: regular Mode: 0644 Flags: 0x0 Version: 1 User: 0 Group: 0 Size: 149500 File ACL: 0 Directory ACL: 0 Links: 0 Blockcount: 38 Fragment: Address: 0 Number: 0 Size: 0 ctime: 0x31a9a574 -- Mon May 27 13:52:04 2001 atime: 0x31a21dd1 -- Tue May 21 20:47:29 2001 mtime: 0x313bf4d7 -- Tue Mar 5 08:01:27 2001 dtime: 0x31a9a574 -- Mon May 27 13:52:04 2001 BLOCKS: 594810 594811 594814 594815 594816 594817 ……. TOTAL: 38[/pre] 然后就可以用dump指令恢复文件： [pre]debugfs：dump /mnt/hda/01.sav[/pre] 这样就把文件恢复出来了。退出debugfs

：[pre]debugfs：quit[/pre] 另一种方法是手工编辑inode：[pre]debugfs：mi Mode [0100644] User ID [0] Group ID [0] Size [149500] Creation time [0x31a9a574] Modification time [0x31a9a574] Access time [0x31a21dd1] Deletion time [0x31a9a574] 0 Link count [0] 1 Block count [38] File flags [0x0] Reserved1 [0] File acl [0] Directory acl [0] Fragment address [0] Fragment number [0] Fragment size [0] Direct Block #0 [594810] Triple Indirect Block [0][/pre] 使用mi指令后每次显示一行信息以供编辑，其它行可以直接按回车表示确认，把deletion time改成0（未删除），Link count改成1。改好后退出debugfs：[pre]debugfs：quit[/pre] 然后用fsck检查/dev/hda5 fsck /dev/hda5，程序会说找到丢失的数据块，放在lost found里面。 