## 数据恢复工具—extundelete

#### 1、源码安装

##### 1.1下载包

wget  http://zy-res.oss-cn-hangzhou.aliyuncs.com/server/extundelete-0.2.4.tar.bz2

##### 1.2配置yum源安装相关依赖包

yum -y install  bzip2  e2fsprogs-devel  e2fsprogs  gcc-c++ make

##### 1.3安装extundelete

tar -xvjf extundelete-0.2.4.tar.bz2 -C /usr/local/src

cd /usr/local/src/extundelete-0.2.4

./configure –prefix=/usr/local/extundelete

make && make install

ln -s /usr/local/extundelete/bin/extundelete /usr/local/bin/

#### 2、恢复数据

##### 2.1模拟环境

添加一块硬盘，格式化为ext3或ext4，导入数据，删除数据

extundelete只能恢复文件系统为ext3和ext4的文件

[root@localhost media]# ls

baseline cdrom.ko kylin lost+found openss-kylin3.2-8g openss-kylin3.2-8g.tar.gz sr\_mod.ko usb-storage.ko

[root@localhost media]# cd openss-kylin3.2-8g

[root@localhost openss-kylin3.2-8g]# ls

openssh-8.4p1-2.ky3.kb4.pg.x86\_64.rpm openssl-devel-1.1.1g-57.ky3.kb1.pg.x86\_64.rpm

openssh-askpass-8.4p1-2.ky3.kb4.pg.x86\_64.rpm openssl-perl-1.1.1g-57.ky3.kb1.pg.x86\_64.rpm

openssh-clients-8.4p1-2.ky3.kb4.pg.x86\_64.rpm openssl-static-1.1.1g-57.ky3.kb1.pg.x86\_64.rpm

openssh-server-8.4p1-2.ky3.kb4.pg.x86\_64.rpm pam\_ssh\_agent\_auth-0.9.3.1-2.ky3.kb4.pg.x86\_64.rpm

openssl-1.1.1g-57.ky3.kb1.pg.x86\_64.rpm perl-WWW-Curl-4.09-4.ky3.kb1.x86\_64.rpm

[root@localhost openss-kylin3.2-8g]# rm -rf ./\*

[root@localhost openss-kylin3.2-8g]#

##### 2.2 恢复前的准备工作

###### 2.2.1 卸载盘符或将盘符挂载为只读

umount /dev/sdb

mount -o remount,ro /dev/sdb

###### 2.2.2 查询要恢复的文件

[root@localhost ~]# extundelete /dev/sdb --inode 2

……

File name | Inode number | Deleted status

. 2

.. 2

lost+found 11

baseline 12

cdrom.ko 16

kylin 8193

openss-kylin3.2-8g 8194

openss-kylin3.2-8g.tar.gz 27

sr\_mod.ko 28

usb-storage.ko 29

[root@localhost ~]# extundelete /dev/sdb --inode 8194

…

File name | Inode number | Deleted status

. 8194

.. 2

openssh-askpass-8.4p1-2.ky3.kb4.pg.x86\_64.rpm 17 Deleted

pam\_ssh\_agent\_auth-0.9.3.1-2.ky3.kb4.pg.x86\_64.rpm18 Deleted

openssl-static-1.1.1g-57.ky3.kb1.pg.x86\_64.rpm 19 Deleted

perl-WWW-Curl-4.09-4.ky3.kb1.x86\_64.rpm 20 Deleted

openssl-devel-1.1.1g-57.ky3.kb1.pg.x86\_64.rpm 21 Deleted

openssl-1.1.1g-57.ky3.kb1.pg.x86\_64.rpm 22 Deleted

openssh-8.4p1-2.ky3.kb4.pg.x86\_64.rpm 23 Deleted

openssh-server-8.4p1-2.ky3.kb4.pg.x86\_64.rpm 24 Deleted

openssh-clients-8.4p1-2.ky3.kb4.pg.x86\_64.rpm 25 Deleted

openssl-perl-1.1.1g-57.ky3.kb1.pg.x86\_64.rpm 26 Deleted

找到Deleted status为Deleted的文件，就是刚刚删除的文件

##### 2.3 开始恢复

###### 2.3.1 恢复单个文件

[root@localhost ~]# cd /mnt/

[root@localhost mnt]# ls

\*该文件路径为挂载点的相对路径

eg：将盘符挂载至/media/目录下，删除文件所属目录为/media/openss-kylin3.2-8g/,此处就为openss-kylin3.2-8g/file（删除文件名）

[root@localhost mnt]# extundelete /dev/sdb --restore-file openss-kylin3.2-8g/perl-WWW-Curl-4.09-4.ky3.kb1.x86\_64.rpm

NOTICE: Extended attributes are not restored.

Loading filesystem metadata ... 8 groups loaded.

Loading journal descriptors ... 31 descriptors loaded.

Successfully restored file openss-kylin3.2-8g/perl-WWW-Curl-4.09-4.ky3.kb1.x86\_64.rpm

执行完成后会在当前目录下生成一个RECOVERED\_FILES的目录，该目录下会保存恢复的文件及目录

[root@localhost mnt]# ls

RECOVERED\_FILES

[root@localhost mnt]# cd RECOVERED\_FILES/

[root@localhost RECOVERED\_FILES]# ls

openss-kylin3.2-8g

[root@localhost RECOVERED\_FILES]# cd openss-kylin3.2-8g/

[root@localhost openss-kylin3.2-8g]# ls

perl-WWW-Curl-4.09-4.ky3.kb1.x86\_64.rpm

查看md5值校验

[root@localhost openss-kylin3.2-8g]# md5sum perl-WWW-Curl-4.09-4.ky3.kb1.x86\_64.rpm

Windows下查看md5值

D:\系统加固及升级\3.2\update-3.2-8\openssh>certutil -hashfile perl-WWW-Curl-4.09-4.ky3.2.x86\_64.rpm

###### 2.3.2 恢复目录

[root@localhost mnt]# extundelete /dev/sdb --restore-directory openss-kylin3.2-8g

NOTICE: Extended attributes are not restored.

Loading filesystem metadata ... 8 groups loaded.

Loading journal descriptors ... 31 descriptors loaded.

Searching for recoverable inodes in directory openss-kylin3.2-8g ...

10 recoverable inodes found.

Looking through the directory structure for deleted files ...

0 recoverable inodes still lost.

[root@localhost mnt]# ls

RECOVERED\_FILES

[root@localhost mnt]# cd RECOVERED\_FILES/

[root@localhost RECOVERED\_FILES]# ls

openss-kylin3.2-8g

[root@localhost RECOVERED\_FILES]# cd openss-kylin3.2-8g/

[root@localhost openss-kylin3.2-8g]# ls

openssh-8.4p1-2.ky3.kb4.pg.x86\_64.rpm openssl-devel-1.1.1g-57.ky3.kb1.pg.x86\_64.rpm

openssh-askpass-8.4p1-2.ky3.kb4.pg.x86\_64.rpm openssl-perl-1.1.1g-57.ky3.kb1.pg.x86\_64.rpm

openssh-clients-8.4p1-2.ky3.kb4.pg.x86\_64.rpm openssl-static-1.1.1g-57.ky3.kb1.pg.x86\_64.rpm

openssh-server-8.4p1-2.ky3.kb4.pg.x86\_64.rpm pam\_ssh\_agent\_auth-0.9.3.1-2.ky3.kb4.pg.x86\_64.rpm

openssl-1.1.1g-57.ky3.kb1.pg.x86\_64.rpm perl-WWW-Curl-4.09-4.ky3.kb1.x86\_64.rpm

###### 2.3.3 恢复所有文件及目录

[root@localhost mnt]# extundelete /dev/sdb --restore-all

NOTICE: Extended attributes are not restored.

Loading filesystem metadata ... 8 groups loaded.

Loading journal descriptors ... 31 descriptors loaded.

Searching for recoverable inodes in directory / ...

10 recoverable inodes found.

Looking through the directory structure for deleted files ...

0 recoverable inodes still lost.

[root@localhost mnt]# ls

RECOVERED\_FILES

[root@localhost mnt]# cd RECOVERED\_FILES/

[root@localhost RECOVERED\_FILES]# ls

openss-kylin3.2-8g

[root@localhost RECOVERED\_FILES]# cd openss-kylin3.2-8g/

[root@localhost openss-kylin3.2-8g]# ls

openssh-8.4p1-2.ky3.kb4.pg.x86\_64.rpm openssl-devel-1.1.1g-57.ky3.kb1.pg.x86\_64.rpm

openssh-askpass-8.4p1-2.ky3.kb4.pg.x86\_64.rpm openssl-perl-1.1.1g-57.ky3.kb1.pg.x86\_64.rpm

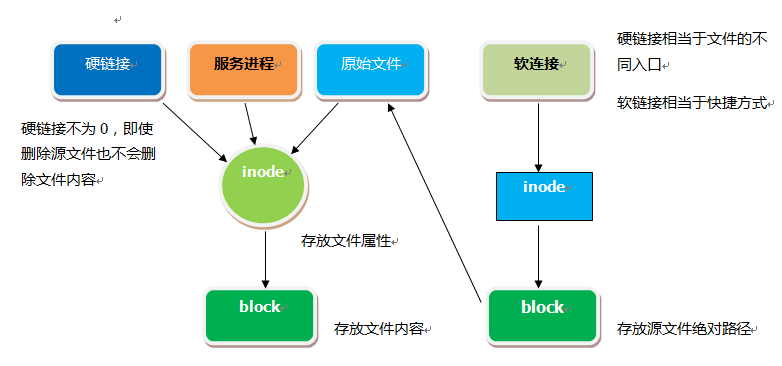
openssh-clients-8.4p1-2.ky3.kb4.pg.x86\_64.rpm openssl-static-1.1.1g-57.ky3.kb1.pg.x86\_64.rpm

openssh-server-8.4p1-2.ky3.kb4.pg.x86\_64.rpm pam\_ssh\_agent\_auth-0.9.3.1-2.ky3.kb4.pg.x86\_64.rpm

openssl-1.1.1g-57.ky3.kb1.pg.x86\_64.rpm perl-WWW-Curl-4.09-4.ky3.kb1.x86\_64.rpm

## 拓展-- Linux文件删除原理

#### 软链接和硬链接



硬链接--指向和源文件的同一inode

软链接—block里面写入的是源文件的绝对路径

硬链接只能指向文件

软链接可以指向文件或目录

#### 文件删除原理

i\_count是当前文件被调用的数量

i\_link是当前文件的硬链接数量

当执行rm命令时，只是将文件的i\_link -1，

当文件的i\_count和i\_link都为0时，文件才会被删除。此时文件被删除，但是inode和block数据块仍然存在（extundelete就是通过inode和block恢复文件的），等下一次继续写入数据时，新数据会占用inode（所以要恢复数据，需要第一时间卸载盘符，防止inode被占用block数据块被覆盖），文件才会被彻底删除