1. 系统痕迹命令
2. 概述

系统中有些重要的痕迹日志文件，保存了很多重要的痕迹信息，如哪个用户登录了，何时登录何时退出等。这些文件是不能用vim打开的，即不能编辑的，只能通过对应的命令来查看。如/var/log/wtmp, /var/run/utmp, /var/log/btmp等等

1. w

w命令显示系统中正在登陆的用户信息，查看的痕迹日志时/var/run/utmp。会显示用户名称，登陆的终端名，开机时间，持续时间，系统在1分钟，5分钟，15分钟前的平均负载。

终端的名称：

tty1 – 6： 本地字符终端（alt + F1-6切换）

tty7: 本地图形终端（alt+ctrl+F7切换，需安装图形界面）

pts/0-255: 远程终端

IDLE： 用户闲置时间

JCPU: 所有进程占用的CPU时间

PCPU：当前进程占用的CPU时间

WHAT：用户正在进行的操作

1. who

与w命令类似，显示更加简单的内容，也是查看/var/run/utmp日志，查看当前正在登陆的用户。

1. last

查看系统所有登录过的用户信息，包括之前的，查看的是/var/log/wtmp日志文件。

1. lastlog

查看系统中所有用户最后一次登录时间，查看的是/var/log/lastlog日志文件。可以看到很多伪用户，这是Linux系统启动时所需的用户，不能删除的。

1. lastb

查看错误登录的信息，查看的是/var/log/btmp日志。

1. 挂载命令
2. mount命令

Linux中所有的存储设备都需要挂载使用，mount命令用于挂载，直接调用mount命令时，作用是查询系统中已经挂载的设备，返回如下内容，表示sda3设备挂载在 根目录/下，文件系统为ext4，读写权限位rw（读与写）：

/dev/sda3 on / type ext4(rw)

mount -a

根据配置文件 /etc/fstab 中的内容，自动挂载。

mount [-t 文件系统] [-L 卷标名] [-o 特殊选项] 设备文件名 挂载点

文件系统： 如ext3, ext4, iso9660

卷标名： 挂载指定卷标的分区，而不是安装设备文件名挂载

特殊选项： 可以指定挂载的额外选项， 如读写权限，同步异步等等，不过不设置就是默认的选项。注意，这些特殊权限一般情况下不要修改，不然会造成系统的崩溃。如下所示：

exec / noexec 执行/ 不执行，设定是否允许在文件系统中执行可执行文件，默认是exec。

remount: 重新挂载已经挂载的文件系统，用于修改特殊权限。

atime/noatime: 更新访问时间/不更新，在访问分区文件时，是否更新文件的访问时间，默认是更新。

async/sync： 异步/同步，默认是异步

auto/noauto : mount -a 执行时，是否会自动安装/etc/fstab文件内容自动挂载，默认是自动。

defaults : 默认值，相当于 rw, suid, dev, exec, auto, nouser, async

rw / ro : 读写/只读， 读写权限，默认是rw

suid / nosuid : 是否具有SUID和SGID权限，默认是有。

user / nouser : 文件系统是否允许普通用户挂载，默认是不允许，只有root可以挂载分区。

userquota : 写入代表文件系统支持用户磁盘配额，默认不支持

grpquota : 写入代表文件系统支持组磁盘配额，默认不支持。

举例如下所示：

mount -o remount,noexec /boot

重新挂载/boot分区，取消里面的执行权限

1. 挂载光盘

挂载光盘需要指定光盘的设备文件名，不同版本的Linux，设备文件名不同。在Centos5.x之前的系统，光盘设备文件名是 /dev/hdc，因为之前默认只有两块硬盘，因此第三块就是光盘。随着存储性能的发展，需要更多的存储设备，因此Centos6.x之后的系统中，光盘设备文件名是/dev/sr0开始的。同时，每个系统中都会有一个软链接/dev/cdrom，链接着第一个光盘，也可以作为光盘的设备文件名，但是最好还是用源文件的名称，因为在宕机情况下，软链接是不生效的，源文件名称是最好的。

mount -t iso9660 /dev/sr0 /mnt/cdrom/

-t 表示文件系统是光盘iso9660，这是光盘的固定系统，是默认的可省略；后面是设备文件名和挂载目录。

出现mount: block device /dev/sr0 is write-protected, mounting read-only 表示挂载成功，因为光盘就是一次性写入的。查看光盘中的内容，直接进入挂载点查看即可。

用完光盘记得卸载，物理机中如果不卸载，光驱是弹不出来的；虚拟机中的虚拟光驱有很大几率坏掉，需要移除该光驱，添加新的光驱。卸载时首先要退出光盘目录，才能够正常卸载。

umount /dev/sr0

umount /mnt/cdrom

卸载设备文件名或者挂载点都可以，因为已经连接到一起了。

注意！！！挂载一定要挂载到空目录上，如果挂载到一个有文件的目录上，那么原有的文件是不会删除的，也是无法搜索到的，相当于之前的目录与里面的文件Block时绑定的，当目录与设备文件挂载后，原有的目录中的文件是不会删除的，白白占用了存储空间。当卸载掉设备后，原有的文件又会和目录进行绑定，又能够通过该目录获取到这些文件了。

1. 挂载U盘

U盘和硬盘是共用设备文件名的，因此U盘的文件名是随着硬盘数量浮动的，首先要查询U盘的名称。通过如下命令查询系统能够识别的存储设备：

fdisk -l

查询到U盘文件名/dev/sdb1后，创建空目录/mnt/usb，将U盘挂载到该目录下，-t是文件系统格式vfat， 同时对于中文编码的问题，还需要指定 -o 为中文编码：

mount -t vfat -o iocharset=utf8 /dev/sdb1 /mnt/usb

Linux中要想显示中文，需要两个条件：

1. 安装了中文编码和中文字体
2. 操作终端需要支持中文显示

在VMWare终端中是不支持中文编码的，即使我们修改了编码为中文也只能显示乱码，因为该终端没有中文字体和编码，且不支持中文。而我们使用Xshell远程终端是Windows下的程序，支持中文显示，因此使用Xshell来挂载。

卸载 使用umount 命令即可：

umount /mnt/usb

1. 挂在NTFS分区

Linux一般是无法识别NTFS分区的，即使识别了，也只能读数据而不能写数据。

1. Linux驱动的加载顺序
2. 驱动直接放入系统内核之中，系统能够直接识别这些驱动，这种驱动主要是系统启动加载时必须的驱动，数量非常少。
3. 驱动以模块的形式放入硬盘中，大多数驱动以这种方式保存。以.ko结尾的扩展名文件都是驱动文件，在/lib/moduls/3.10.0-862.el7.x86\_64/kernel中。这种方式效率比较高，内核在需要驱动时可以直接从硬盘中掉用，方便快捷易存储。
4. 驱动可以被Linux识别，但是系统认为这种驱动一般不常用，默认不加载，如果要加载，需要重新编译内核，NTFS文件系统的驱动就是这种情况。
5. 硬件无法被Linux识别，需要手动安装驱动。
6. 使用插件安装NTFS

下载NTFS-3G插件到Linux服务器上，编译安装NTFS-3G插件之前，要保证gcc编译器已经安装了，安装步骤不赘述。