# 分区

Linux下的设备存在/Dev 目录中

系统的第一块IDE接口硬盘称为/dev/hda

系统的第二块IDE接口硬盘称为/dev/hdb

系统的第一块SCSI接口硬盘称为/dev/sda

系统的第二块SCSI接口硬盘称为/dev/sdb

分区则使用数字编号

系统的第一块IDE接口硬盘的第一个分区称为/dev/hda1

系统的第二块IDE接口硬盘的第五个分区称为/dev/hdb5

系统的第一块SCSI接口硬盘的第一个分区称为/dev/sda1

系统的第二块SCSI接口硬盘的第五个分区称为/dev/sdb5

注意：数字编号1-4留给主分区或扩展分区使用，逻辑分区编号从5开始

SCSI SAS SATA USB接口硬盘的设备均以dev/sd开头

在Linux系统上划分了分区之后，还要在分区上创建文件系统。

Linux系统对分区的要求：

1. 至少要有/ 以及swap两个分区
2. Swap的作用：虚拟内存，swap分区大小=1.5\*物理内存容量
3. 建议设置独立的/boot分区

Linux引导分区存放系统引导文件，如Linux内核等，所有文件大小一般只有几十兆，因此该分区设置为100-200M

所有一般服务器分区方式为 / 、swap 、 /boot三个分区

linux操作系统自从开始启动至启动完毕需要经历几个不同的阶段，这几个阶段就叫做runlevel，同样，当linux操作系统关闭时也要经历另外几个不同的runlevel

进入每个runlevel都需要启动或关闭相应的一系列服务(services)，这些服务(services)以初始化脚本的方式放置于目录/etc/rc.d/rc?.d/或者/etc/rc?.d下面(?代表runlevel的对应序号)。

在大多数的linux发行版本中，通常有8个runlevel

多数的[桌面](http://baike.baidu.com/view/79807.htm)的linux系统缺省的runlevel是5，用户登陆时是图形界面，而多数的服务器版本的linux系统缺省的runlevel是3，用户登陆时是字符界面，runlevel 1和2除了调试之外很少使用，runlevel s和S并不是直接给用户使用，而是用来为Single user mode作准备。



# 目录

/bin 常用的二进制命令目录。比如ls cp mkdir等命令，和/usr/bin类似

/boot Linux内核及引导系统程序所需要文件的目录

/dev 设备文件目录 如声卡 硬盘

/etc 常用系统及二进制安装包配置文件默认路径和服务启动命令目录

/home 普通用户的家目录默认存放目录

/lib 库文件存放目录

/lost +found 在ext3文件系统中，当系统意外崩溃或机器意外关机，会产生一些文件碎片在这里。当系统在开机启动的过程中fsck工具会检查这里，并修复已经损坏的文件系统。当系统发生问题，可能会有文件被移动到这个目录里，可能需要用手工的方式来修复，或移动到文件的原先位置。

/mnt 一般用于临时挂载存储设备的挂载目录，如cdrom 、u盘等目录

/opt 表示的是可选择的意思，有些软件包也会被安装在这里，也就是自定义软件包，我们自己编译的软件包，就可以安装在这里，通过源码包安装的软件，可以通过./configure –prefix=/opt/目录，非必须这样，视习惯或规定而定

/proc 操作系统运行时，进程信息及内核信息（如CPU 内存信息等）存在这里。/proc目录伪装的文件系统的挂载目录，proc并不是真正的文件系统，它的定义参见/etc/fstab

/root Linux超级用户root目录

/sbin 大多是涉及系统管理的命令的存放，是超级用户权限root的可执行命令存放地，这个目录和/usr/sbin /usr/X11R6/sbin 或/usr/local/sbin目录是相似的

/tmp 临时文件目录，有时用户运行程序的时候，会产生临时文件。/tmp就用来存放临时文件的，权限比较特殊。/var/temp目录和这个相似

/usr 这个是系统存放程序的目录，比如命令、帮助文件等。这个目录下有很多的文件和目录。当我们安装一个Linux发行版官方提供的软件包时，大多安装在这个目录下。如果有涉及服务器配置文件的，会把配置文件安装在/etc中。/usr目录下包括涉及字体目录/usr/share/fonts 帮助目录 /usr/share/man 或/usr/share/doc。 普通用户可执行文件目录/usr/bin或/usr/local/bin 等 还有程序的头文件存放目录/usr/include

/var 这个目录的内容是经常变动的，看名字就知道，我们可以理解为vary的缩写，/var下有/var/log这个是用来存放系统日志的。/var/www目录是定义Apache服务器站点存放的目录 /var/lib用来存放一些库文件，比如mysql及mysql数据库的存放地。

重要的子目录

/etc/sysconfig/network-scripts/ifconfig-eth0 配置网络地址及网关等

/etc/resolv.conf 设置本机客户端的DNS

/etc/hosts 设置用户IP与名字对应表，相当于本地的ＤＮＳ

/etc/sysconfig/network 可修改机器名及网卡启动等配置

/etc/fstab 记录开机要mount的文件系统

/etc/inittab 设定系统启动时init进程将把系统设置成什么样的runlevel及加载相关的启动文件设置.

/etc/exports 设置NFS系统用的配置文件路径

/etc/init.d 这个目录是用来存放系统或者服务器以system V模式启动的脚本，这在以system V模式启动或初始化的系统中比较常见，比如centos redhat

/etc/Xinit.d 如果服务是通过xinit模式运行的，它的脚本要放在这个目录下，有些系统没有这个目录

/etc/profile 系统全局环境变量配置路径

/etc/sudoers 可以sudo命令的配置文件

/etc/syslog.conf 日志设置文件

/var/log/message 系统信息默认日志文件，

/var/log/secure 记录登入系统存取信息的文件 如pop3 ssh ftp等

/var/log/wtmp 记录登入者信息的文件

/proc/version 内核版本

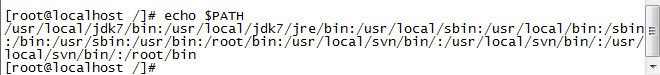
/proc/cpuinfo 处理器信息 如类型 厂家 型号等

/proc/devices 当前运行内核所配置的所有设备清单

/proc/interrupts 正在使用的中断 和曾经有多少个中断

/proc/loadavg 系统负载信息 uptime结果

PATH全局环境变量



每个路径用：隔开

加入全局变量好处：加入后，所有目录下的命令可以直接运行，系统会自动从这些目录去搜索你执行的命令，否则只能敲全路径执行

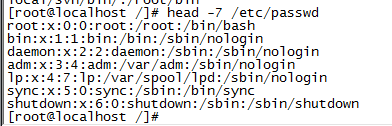
# 用户与用户组

Linux是一个多用户、多任务的操作系统。

虚拟用户：与真实普通用户分开，这类用户最大的特点是安装系统后默认就会存在的，且默认情况下不能登录系统，他们是系统正常运行不可缺少的，它们的存在主要是方便系统管理，满足相应的系统进程对文件属主的要求，如bin adm nobody等。由于服务器角色的不同，有部分用不到的系统服务被禁止开机执行，因此，在做系统安全优化时，被禁止开机启动了的服务对应的虚拟用户也是可以处理掉的（删除或注释）。

Sudo 是仅一次使用root权限 su 是长期使用root权限

使用head -7 只查看最前面7行



root: x:0:0: root: /root: /bin/bash

用户说明 用户家目录 shell解释器

UID GID范围是0-65535

用户说明：这个字段是对账户的描述说明

用户家目录：用户登录后首先进入的目录

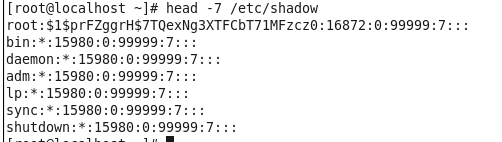
Shell解释器：当前用户登录后所使用的shell，默认shell是bash,如果不需要用户登录系统，可以通过usermod或者手动修改passwd文件，将该字段改为/sbin/nologin即可，大部分虚拟账户的这个字段都是/sbin/nologin，表示禁止登录。

UID范围

0 当用户UID为0时，表示这个账户为超级管理员账户，如果要增加一个系统管理员账户的话，只需将UID改为0即可

1-499 这个范围是保留给系统使用的UID，之所以这样划分，是为了防止人为建立账户的UID和系统UID冲突，虚拟账户UID都在这个范围内，其实，除0以为，其他UID在使用上没有区别

500-65535 普通账户UID，当使用useradd建立账户时，默认情况下UID从500开始，当然也可以指定UID



以：分成9部分

root:$1$prFZggrH$7TQexNg3XTFCbT71MFzcz0:16872:0:99999:7:::

第一个是账户名

第二个是密码

第三个是最近密码修改时间，从1970年1月1日起，到用户最近一次修改口令的天数

第四个是禁止修改密码的天数，从1970年1月1日起，到用户可以更改密码的天数，0 表示“可在任何时间修改”

第五个是用户必须修改口令的天数，从1970年1月1日起，到用户必须修改密码的天数，1 表示“永远都不能修改”

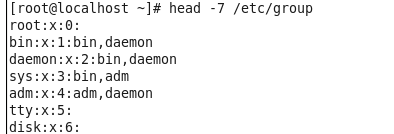
第六个是警告密码修改的期限，在用户密码过期前多少天提醒用户修改密码，-1 表示“没有警告”

第七个是不活动时间，在用户密码过期之后到禁用账户的天数，-1 表示“永远不会禁用”

第八个是失效时间，从1970年1月1日起，到用户被禁用的天数，-1 表示“该帐户被启用”

第九个是标志，保留字段

用户组



root:x:0:

账户：密码：GID:组成员（加入这个组的所有用户账户）



Usermode -a 用户组 用户 。把某个用户添加在组

-G把某个用户添加在组，且离开其他组

Yum的配置文件

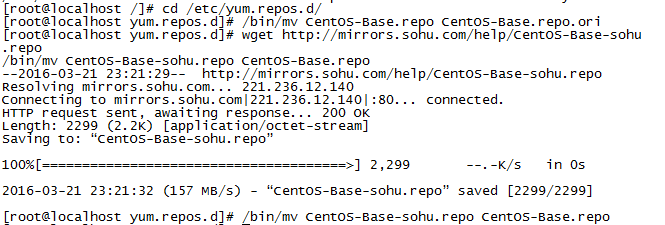
[root@localhost /]# vi /etc/yum.repos.d/CentOS-Base.repo

cd /etc/yum.repos.d/

/bin/mv CentOS-Base.repo CentOS-Base.repo.ori

wget <http://mirrors.sohu.com/help/CentOS-Base-sohu.repo>

/bin/mv CentOS-Base-sohu.repo CentOS-Base.repo



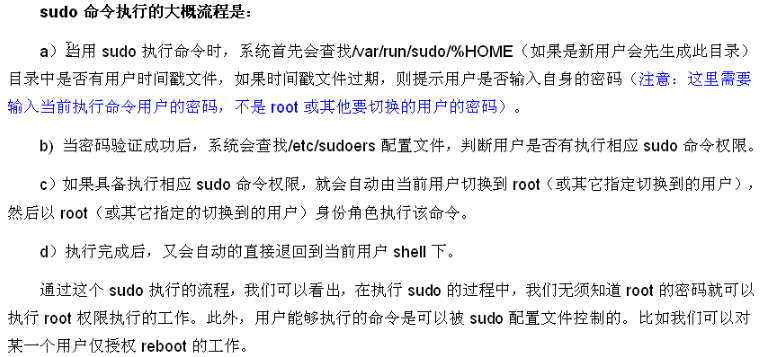
然后使用如下命令更新系统到最新

rpm –-import /etc/pki/rpm-gpg/RPM-GPG-KEY\*

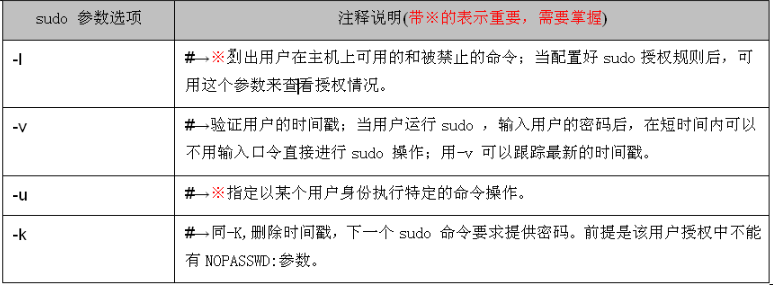
yum upgrade

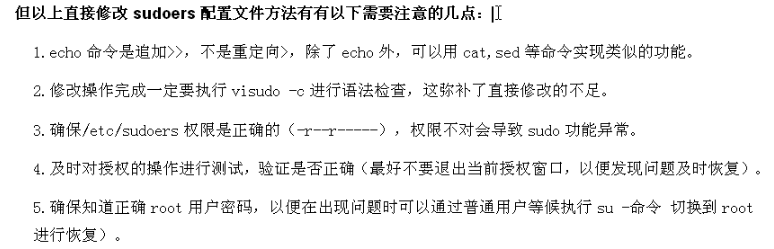
# Su和sudo区别

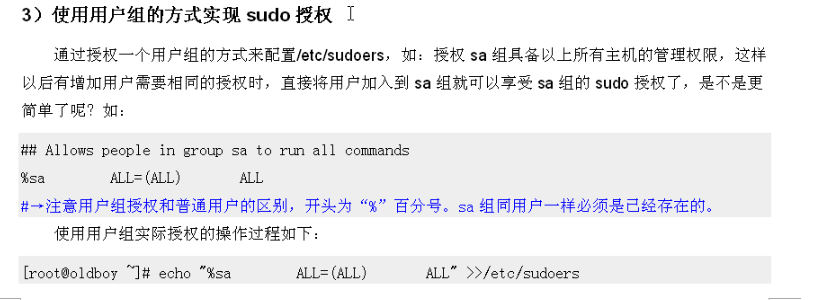
Su是直接切换到另一个账号，需要知道另一个账户的密码，sudo相当于另一个账户事先赋予它的一部分权限，切换过去不需要密码，且仅切换一次



能够完成上述流程中的权限控制，我们完全依赖/etc/sudoer这个配置文件，在默认的情况下，普通用户无法使用sudo，只要编辑/etc/sudoer文件加入用户的授权规则后才可以，这就需要visudo命令（更改/etc/sudoer配置文件的标准工作）。







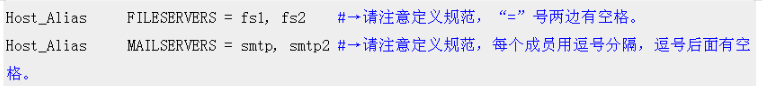
# sudoers文件配置

/etc/sudoers配置文件中的每一行就是一个规则，前面#说明是注释，当规则超过一行时，可以用\号来续行。

/etc/sudoers规则大致分2类，一类是别名定义，另一类是授权规则。别名定义不是必须的，但授权规则是必须的。

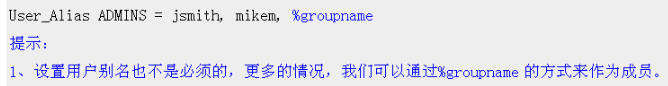
别名类型包括如下四种：

1. Host\_Alias定义主机别名



1. User\_Alias定义用户别名

别名成员可以是用户、用户组（用户组前面要加%号）



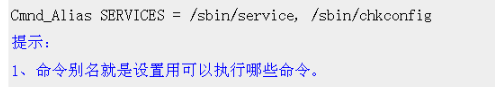
1. Runas\_Alias定义runas别名

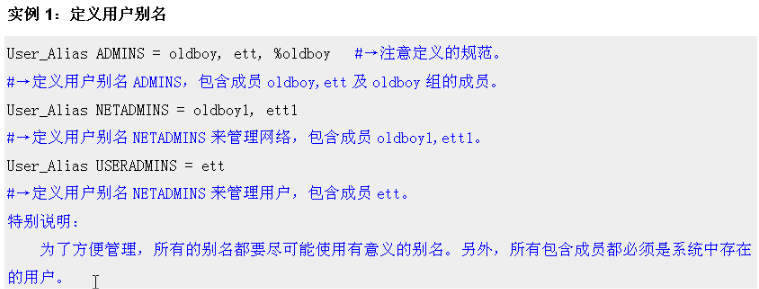
这个别名指定的是 用户身份，即sudo允许切换至的用户

Runas\_Alias定义的是某个系统用户可以执行sudo切换身份到runas\_Alias下包含的成员身份。



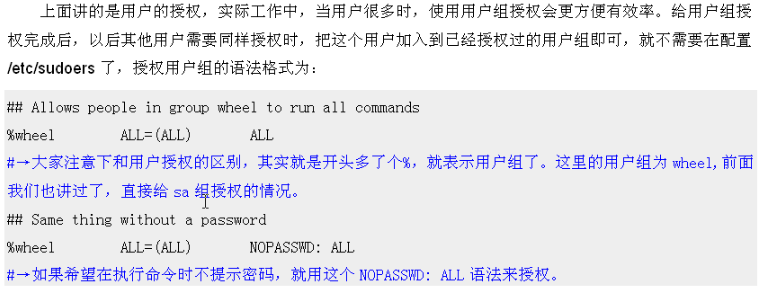
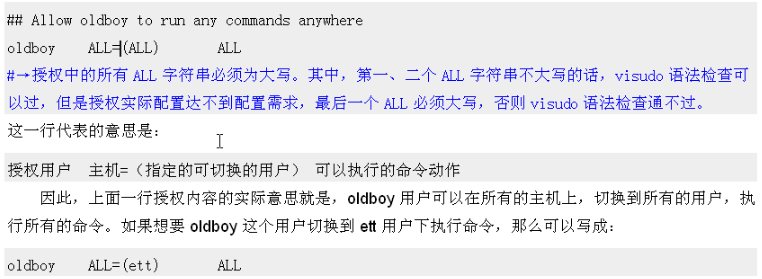
4．Cmnd\_Alias 定义命令别名



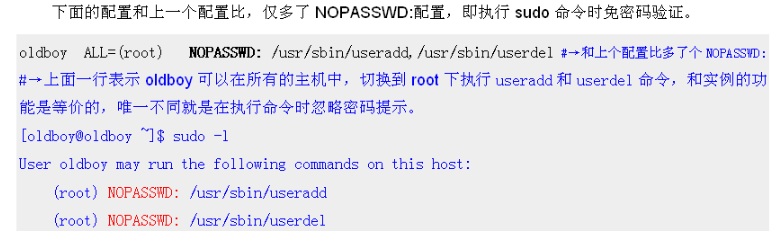
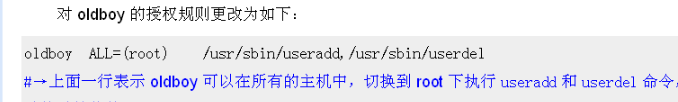


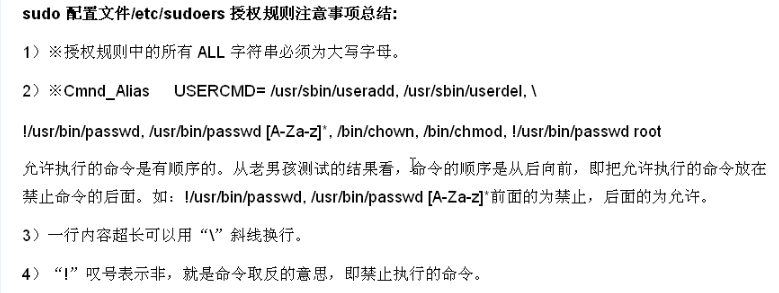
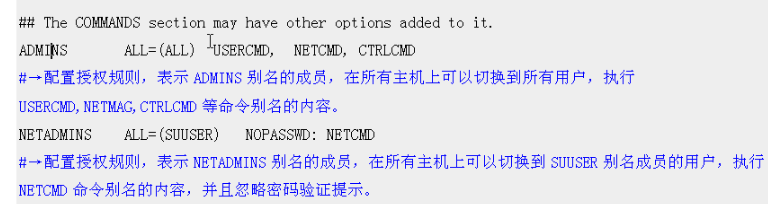
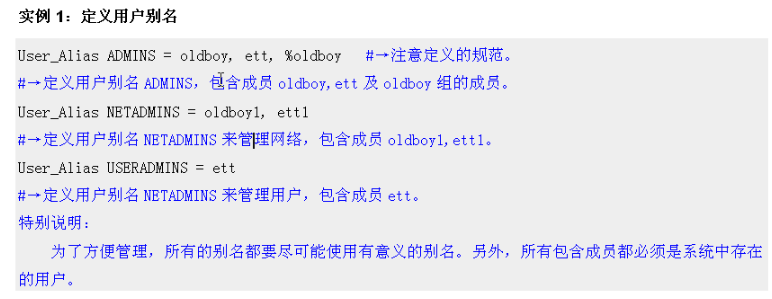


授权规则：



如果没有括号表示仅可以切换到root下执行相关命令，你如ALL







# 更改ssh登录配置

1. 更改前先备份



1. Port 2222 ssh默认端口为22 大家都知道 必须改掉

PermitEmptyPasswords no 不允许空密码登录

PermitRootLogin no 不允许root账户远程登录

UseDNS no 不使用DNS，表示是否对远程主机名进行反向解析，以检查该主机名是否与其IP真实对应

3./etc/init.d/sshd restart 重启sshd，保证配置生效

将普通用加入root组

相当于直接编辑/etc/sudoer，但用命令方式更安全



修改中文显示

1. 用root用户登录。输入【vi /etc/sysconfig/i18n】
2. 如果安装系统为中文系统，则修改【LANG=“zh\_CN.UTF-8”】

如果安装系统为英文系统，则修改【LANG=“en\_US.UTF-8”】

3.source /etc/sysconfig/il8n 使修改生效

# 服务器时间同步

echo '\*/5\*\*\*/usr/sbin/ntpdate time.windows.com>/dev/null 2>&1' >>/var/spool/cron/root



这个命令相当于写一个定时任务，相当于执行crontab –e 然后加入内容：\*/5\*\*\*/usr/sbin/ntpdate time.windows.com>/dev/null 2>&1保存退出

# 设置Sysctl.conf用以提高Linux的性能

Sysctl是一个允许您改变正在运行中的Linux系统的接口。它包含一些 TCP/IP 堆栈和虚拟内存系统的高级选项， 这可以让有经验的管理员提高引人注目的系统性能。用sysctl可以读取设置超过五百个系统变量。基于这点，sysctl(8) 提供两个功能：读取和修改系统设置。

查看所有可读变量：

% sysctl -a

读一个指定的变量，例如 kern.maxproc：

#表示进程（例如一个worker进程）可能同时打开的最大句柄数，直接限制最大并发连接数  
fs.file max = 999999

#1代表允许将状态为TIME-WAIT状态的socket连接重新用于新的连接。对于服务器来说有意义，因为有大量的TIME-WAIT状态的连接  
net.ipv4.tcp\_tw\_reuse = 1

#当keepalive启用时，TCP发送keepalive消息的频率。默认是2个小时。将其调小一些，可以更快的清除无用的连接  
net.ipv4.tcp\_keepalive\_time = 600

#当服务器主动关闭链接时，socket保持FN-WAIT-2状态的最大时间  
net.ipv4.tcp\_fin\_timeout = 30

#允许TIME-WAIT套接字数量的最大值。超过些数字，TIME-WAIT套接字将立刻被清除同时打印警告信息。默认是180000，过多的TIME-WAIT套接字会使webserver变慢  
net.ipv4.tcp\_max\_tw\_buckets = 5000

#UDP和TCP连接中本地端口（不包括连接的远端）的取值范围  
net.ipv4.ip\_local\_port\_range = 1024　　61000

#TCP接收/发送缓存的最小值、默认值、最大值  
net.ipv4.tcp\_rmem = 4096　　32768　　262142  
net.ipv4.tcp\_wmem = 4096　　32768　　262142

#当网卡接收的数据包的速度大于内核处理的速度时，会有一个队列保存这些数据包。这个参数就是这个队列的最大值。  
net.core.netdev\_max\_backlog = 8096

#内核套接字接收/发送缓存区的默认值  
net.core.rmem\_default = 262144  
net.core.wmem\_default = 262144

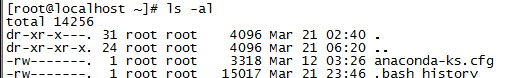
#内核套接字接收/发送缓存区的最大值  
net.core.rmem\_max = 2097152  
net.core.wmem\_max = 2097152

#解决TCP的SYN攻击。与性能无关  
net.ipv4.tcp\_syncookies = 1

#三次握手建立阶段SYN请求队列的最大长度，默认是1024。设置大一些可以在繁忙时将来不及处理的请求放入队列，而不至于丢失客户端的请求  
net.ipv4.tcp\_max\_syn\_backlog = 1024

Ls –l 可以查看文件，但不包括隐藏文件

Ls –al 可以查看所有文件 包括隐藏文件

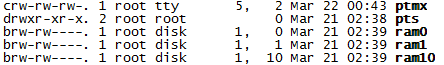


d 表示目录 –表示文件

l 表示是一个符号链接文件，实际上它指向另一个文件，可以通过ln –s 源文件名 新文件名 来创建

b,c表示区块设备和其他外围设备，是特殊类型文件(/dev下几乎都是这种文件)

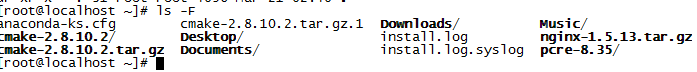
c是字符设备文件 b是块设备文件，如硬盘 光驱，这类文件用mknod创建 rm来删除



s p 这些文件关系到系统的数据结构和管道，很少见(/dev下几乎都是这种文件)

s是套接字文件

ls –F 这种命令格式可以很明显的显示出那些是目录那些是文件。目录后会跟 /



Linux下的扩展名没什么意思，只是为了兼容Windows 同时便于大家习惯

# 软连接 硬链接

硬链接：新建的文件是已经存在的文件的一个别名，当原文件删除时，新建的文件仍然可以使用. 默认不带参数的情况下，ln创建的都是硬链接

软链接：也称为符号链接，新建的文件以“路径”的形式来表示另一个文件，和Windows的快捷方式十分相似，新建的软链接可以指向不存在的文件.ln –s 创建软链接

软硬链接使用场景：

安装软件时由于文件名过长，但又想使用短文件名 就可以创软链接

硬件存储的快照功能，或者为备份数据创建多个硬链接，防止误删数据

目录不可以创建硬链接 但可以创建软链接

硬链接作用之一是允许一个文件拥有多个有效路劲名，这样用户就可以建立硬链接到重要的文件，以防止文件误删（快照就先当于建立一个硬链接），因为文件系统的原理是，只要文件的索引节点（Inode Index）还有一个以上的链接（仅仅删除该文件的指向），只删除其中一个链接并不影响索引节点本身和其他链接（即数据文件实体并未被删除），只要当最后一个链接被删除后，此时如果有新数据要存储到硬盘时，被删除文件的数据块及目录的链接才被释放，空间被新数据占用覆盖。此时数据无法找回。也就是说，在Linux中，删除文件的条件是与之相关的所有硬链接文件均被删除，硬链接相当于文件的另一个入口。

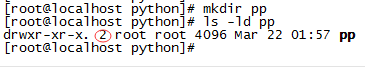
下面详细介绍一下硬链接和软连接之间的区别.

1.硬链接和原来的文件没有什么区别，而且共享一个 inode 号（文件在文件系统上的唯一标识）；而软链接不共享 inode，也可以说是个特殊的 inode，所以和原来的 inode 有区别。

2.若原文件删除了，则该软连接则不可以访问，而硬连接则是可以的。

3.由于符号链接的特性，导致其可以跨越磁盘分区，但硬链接不具备这个特性.

Linux下mkdir创建一个目录，它的硬链接数为2个 因为创建的目录本身是一个硬链接，其次新目录下的隐藏目录（点号）为创建的新目录的又一个硬链接，也算软链接，因此，硬链接为2个，查看方法为ls –ld 新目录

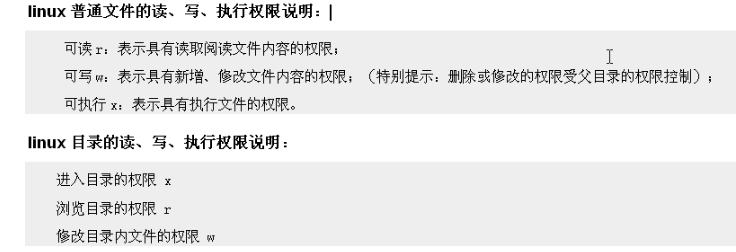


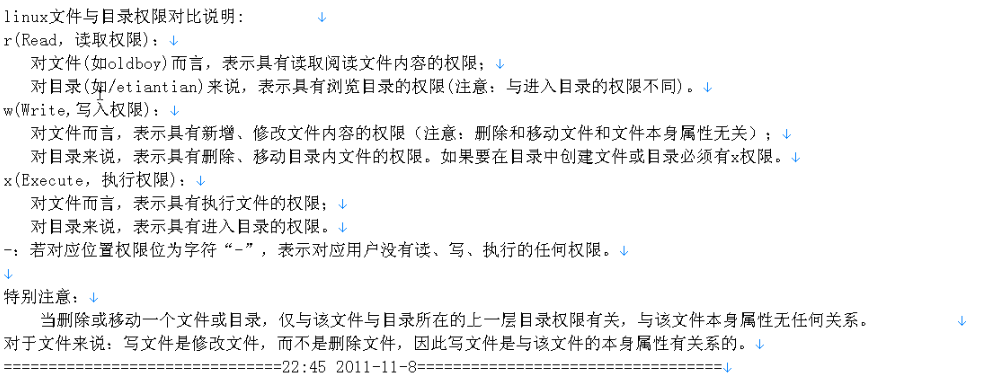
2就表示2个硬链接

inode 中文意思为索引节点，每个存储设备或存储设备的分区被格式化以后，都有2个部分，一部分是inode 另一部分是block。Block用来存储数据，inode就来存储这些数据信息的，这些信息包括文件大小、属主、权限等。

Inode为每一个文件进行信息索引，所以就有了inode的数值，操作系统根据指令，能通过inode值最快的找到相应的文件。ls –i 就可以看到inode的值

# 文件权限





W对于目录来说，具有删除、移动目录内的权限，但必须也有x权限

当删除或移动一个文件或目录时，仅与该文件与目录所在的上一层目录权限有关，与该文件本身属性无关，对于文件来说，写权限是修改文件而不是删除文件，因此写文件与该文件本身属性有关系的。

即使该文件权限为777也不一定能删除或移动，主要看上一层权限。

对于目录，可写 W 表示具有修改权限、移动或删除目录内的权限，但是必须同时有x权限才可以

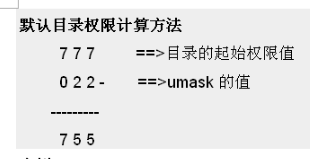
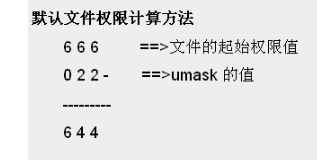
Chmod可以更改文件或目录权限，不加参数表示仅改变打开权限，如果想把目录及以下所有文件或子目录权限同时改变，需要加参数-R

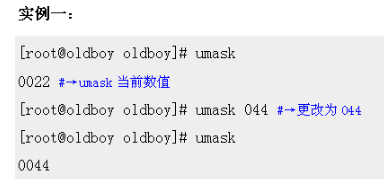
字符修改权限

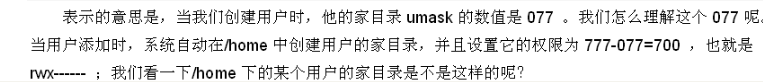


umask是通过八进制的数值来定义用户创建文件或目录的默认权限，umask表示的是禁止权限。对于文件来说，umask的设置是假定文件拥有八进制666权限上进行，文件的权限就是666减去umask的数值；

对于目录来说，umask的设置是假定文件拥有八进制777权限上进行，文件的权限就是777减去umask的数值。







有时会查看文件权限组与用户都会以数字显示，说明该文件曾经所属的用户与组都被删除了，

删用户可以用userdel –r 用户 连同家目录一起删除

# 权限重重点

**PS：有时候你发现用root权限都不能修改某个文件，大部分原因是曾经用chattr命令锁定该文件了。chattr命令的作用很大，其中一些功能是由**[**Linux**](http://www.ha97.com/category/linux)**内核版本来支持的，不过现在生产绝大部分跑的**[**linux**](http://www.ha97.com/tag/linux)**系统都是2.6以上内核了。通过chattr命令修改属性能够提高系统的安全性，但是它并不适合所有的目录。chattr命令不能保护/、/dev、/tmp、/var目录。lsattr命令是显示chattr命令设置的文件属性。**

这两个命令是用来查看和改变文件、目录属性的，与chmod这个命令相比，chmod只是改变文件的读写、执行权限，更底层的属性控制是由chattr来改变的。

chattr命令的用法：chattr [ -RVf ] [ -v version ] [ mode ] files…  
最关键的是在[mode]部分，[mode]部分是由+-=和[ASacDdIijsTtu]这些字符组合的，这部分是用来控制文件的  
属性。  
  
+ ：在原有参数设定基础上，追加参数。  
- ：在原有参数设定基础上，移除参数。  
= ：更新为指定参数设定。  
A：文件或目录的 atime (access time)不可被修改(modified), 可以有效预防例如手提电脑磁盘I/O错误的发生。  
S：硬盘I/O同步选项，功能类似sync。  
a：即append，设定该参数后，只能向文件中添加数据，而不能删除，多用于服务器日志文件安全，只有root才能设定这个属性。  
c：即compresse，设定文件是否经压缩后再存储。读取时需要经过自动解压操作。  
d：即no dump，设定文件不能成为dump程序的备份目标。  
i：设定文件不能被删除、改名、设定链接关系，同时不能写入或新增内容。i参数对于文件 系统的安全设置有很大帮助。  
j：即journal，设定此参数使得当通过mount参数：data=ordered 或者 data=writeback 挂 载的文件系统，文件在写入时会先被记录(在journal中)。如果filesystem被设定参数为 data=journal，则该参数自动失效。  
s：保密性地删除文件或目录，即硬盘空间被全部收回。  
u：与s相反，当设定为u时，数据内容其实还存在磁盘中，可以用于undeletion。  
各参数选项中常用到的是a和i。a选项强制只可添加不可删除，多用于日志系统的安全设定。而i是更为严格的安全设定，只有superuser (root) 或具有CAP\_LINUX\_IMMUTABLE处理能力（标识）的进程能够施加该选项。

**应用举例：**  
  
1、用chattr命令防止系统中某个关键文件被修改：  
# chattr +i /etc/resolv.conf

然后用mv /etc/resolv.conf等命令操作于该文件，都是得到Operation not permitted 的结果。vim编辑该文件时会提示W10: Warning: Changing a readonly file错误。要想修改此文件就要把i属性去掉： chattr -i /etc/resolv.conf

# lsattr /etc/resolv.conf  
会显示如下属性  
----i-------- /etc/resolv.conf

2、让某个文件只能往里面追加数据，但不能删除，适用于各种日志文件：  
# chattr +a /var/log/messages

# chown

利用 chown 可以将档案的拥有者加以改变。这个指令只有是由系统管理者(root)所使用，一般使用者没有权限可以改变别人的档案拥有者，也没有权限可以自己的档案拥有者改设为别人。只有系统管理者(root)才有这样的权限。

**命令参数：**

**必要参数:**

　　　　-c 显示更改的部分的信息

　　　　-f 忽略错误信息

　　　　-h 修复符号链接

　　　　-R 处理指定目录以及其子目录下的所有文件

　　　　-v 显示详细的处理信息

　　　　-deference 作用于符号链接的指向，而不是链接文件本身

**选择参数:**

　　　　--reference=<目录或文件> 把指定的目录/文件作为参考，把操作的文件/目录设置成参考文件/目录相同拥有者和群组

　　　　--from=<当前用户：当前群组> 只有当前用户和群组跟指定的用户和群组相同时才进行改变

　　　　--help 显示帮助信息

　　　　--version 显示版本信息

Chown –R [用户名] [文件或目录]

Chown –R [用户名：组名] [文件或目录] **改变拥有者和群组**

# Crond服务

crond的概念和crontab是不可分割的。crontab是一个命令，常见于Unix和类Unix的操作系统之中，用于设置周期性被执行的指令。该命令从标准输入设备读取指令，并将其存放于“crontab”文件中，以供之后读取和执行。

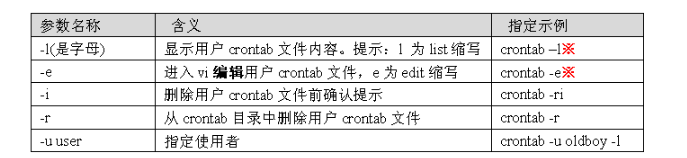
Crond是Linux中用来定期执行命令或指定程序任务的服务，一般情况下，安装完操作系统后，默认便会启动此任务调度任务。Crond服务会定期检查系统中是否有要执行的任务工作，如果有，则会根据预先默认的规则自动执行该任务工作。

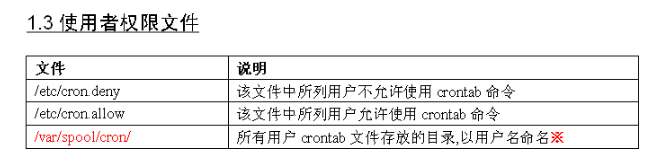
Linux任务调度的工作分以下2类：

1. 系统自身执行的工作：系统周期性执行的任务工作，如轮询系统日志，备份系统数据、清理缓存等
2. 用户执行的工作：某个用户定期要做的工作：如每隔10分钟和互联网时间进行时间同步，每晚10点备份站点数据等

**基本用法**

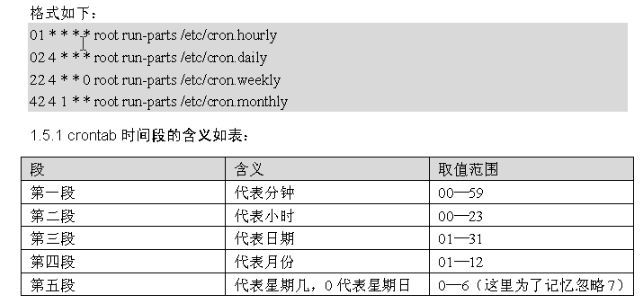
crontab -u //设定某个用户的cron服务   
　　crontab -l //列出某个用户cron服务的详细内容   
　　crontab -r //删除某个用户的cron服务   
　　crontab -e //编辑某个用户的cron服务

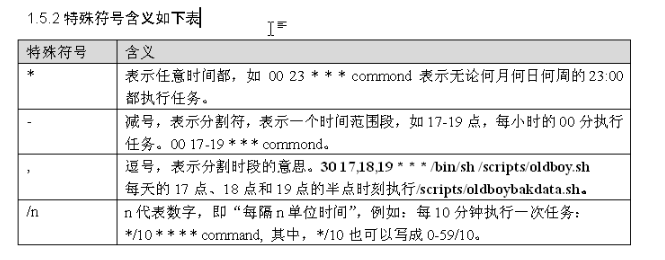


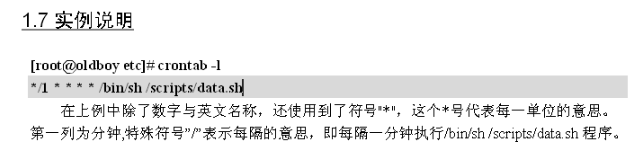


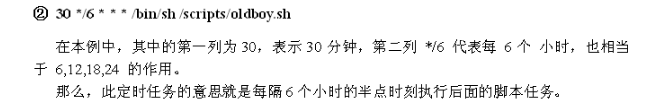
默认情况下，用户所建立的crontab文件存于/var/spool/cron中，其中crontab对应的文件名与用户名一致。

格式共分为七段，前五段为时间设置段，第六段为哪个用户执行crontab的（默认是当前用户），第七段为所用执行的命令段。

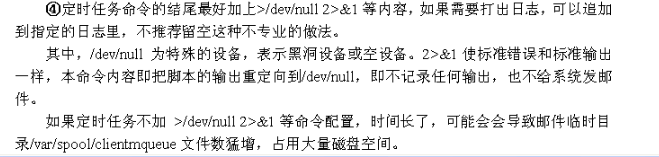


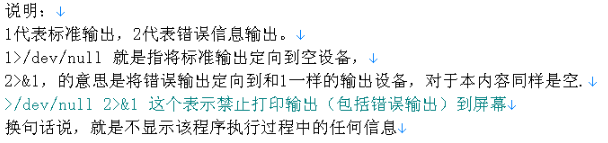




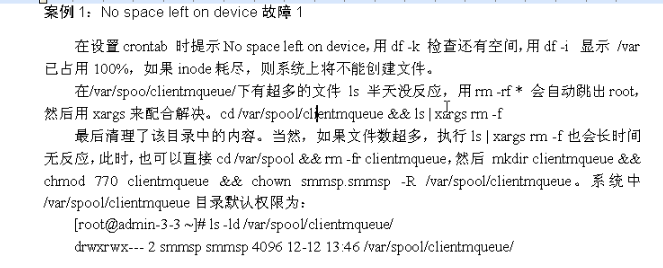




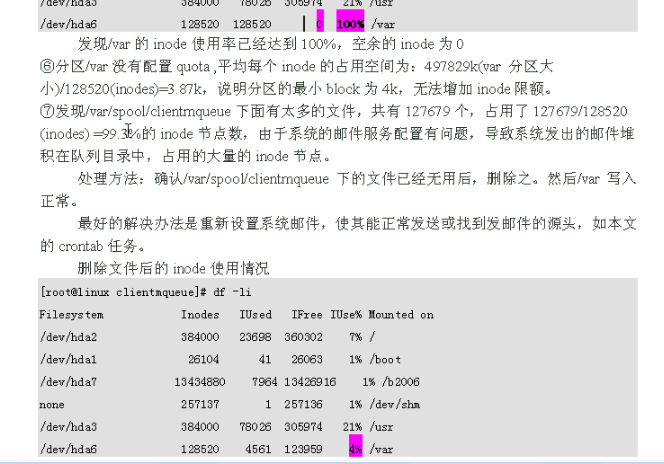
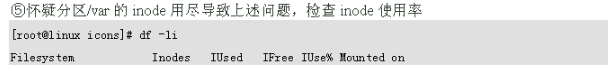
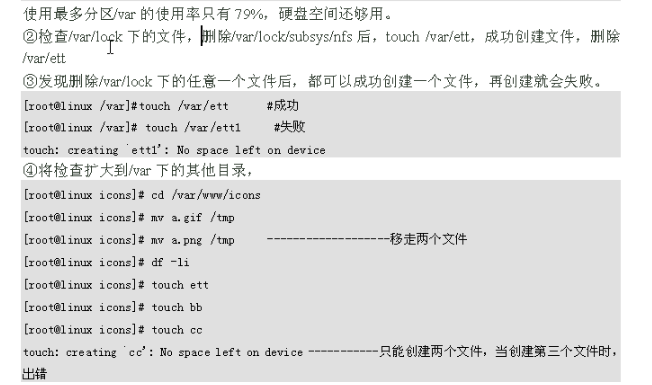


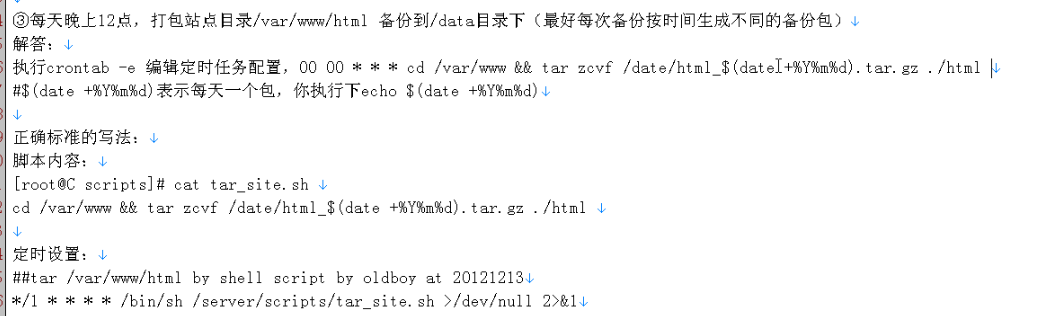


注：shell等脚本的执行方式才能加>/dev/null 2>&1

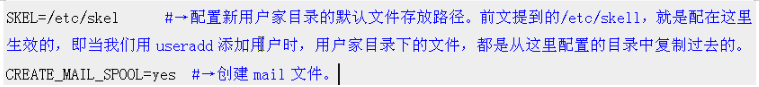
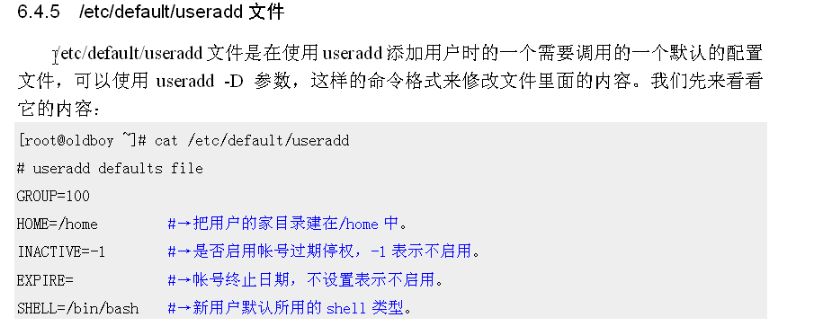
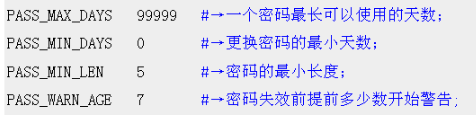
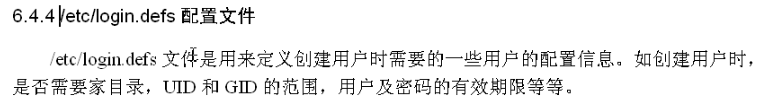
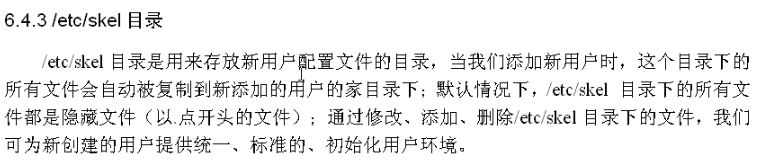
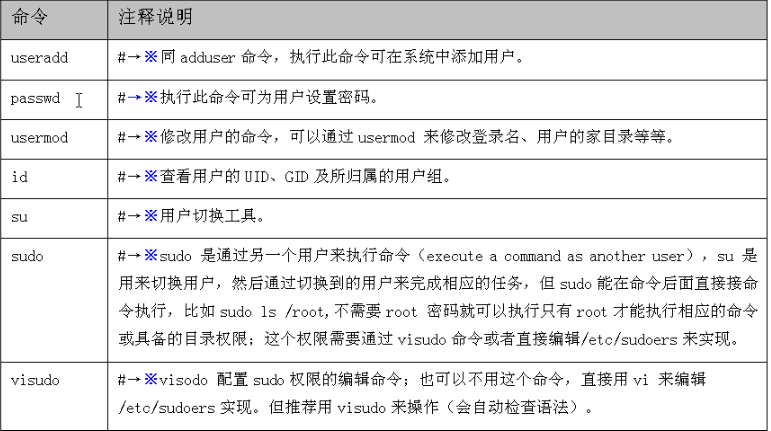




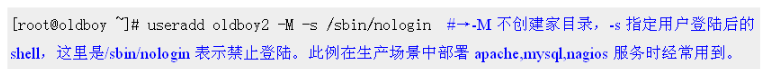
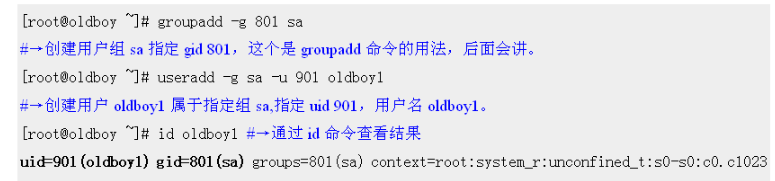


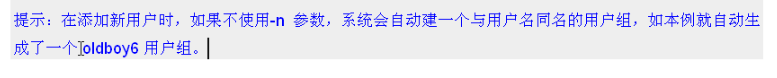
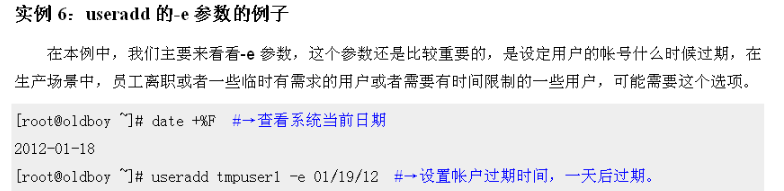


# 用户及用户组管理

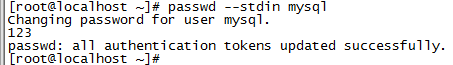
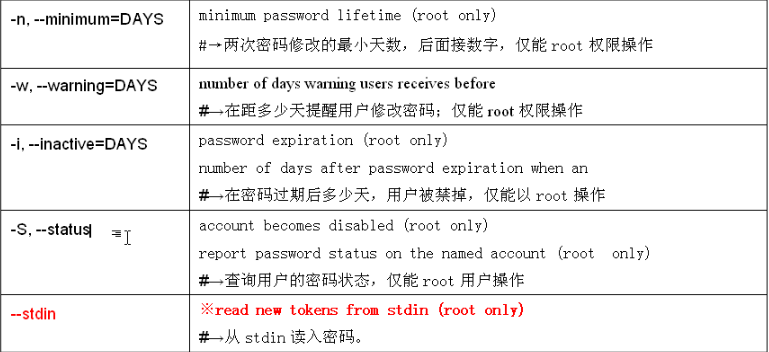
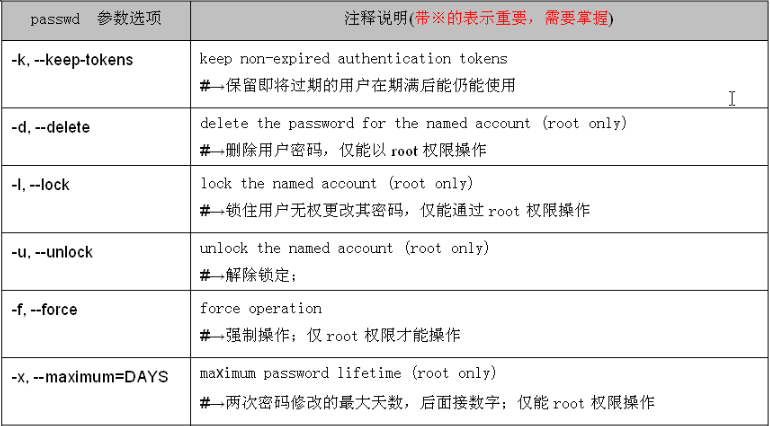


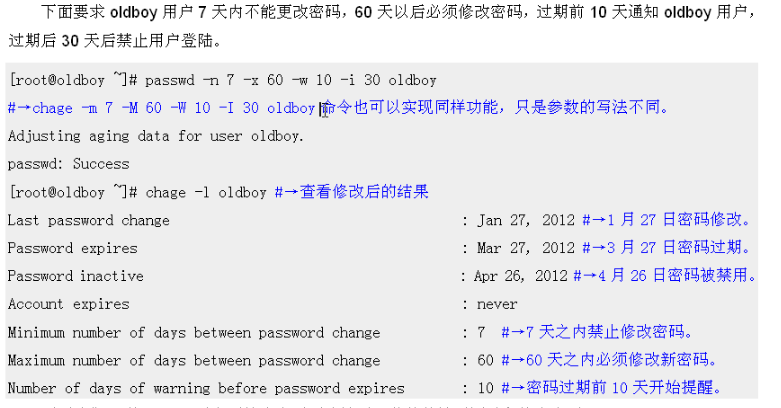
创建新用户属于哪个组





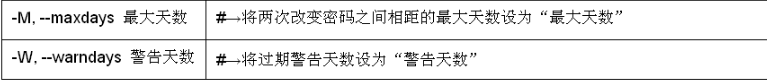
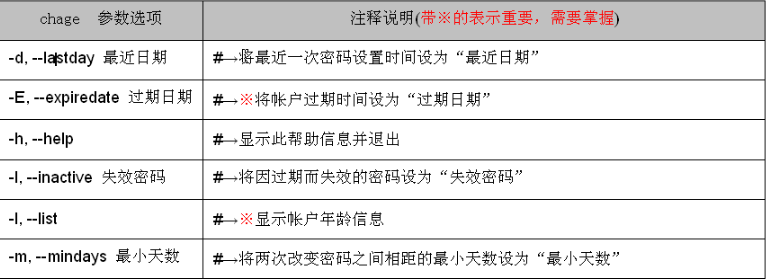
# Passwd命令





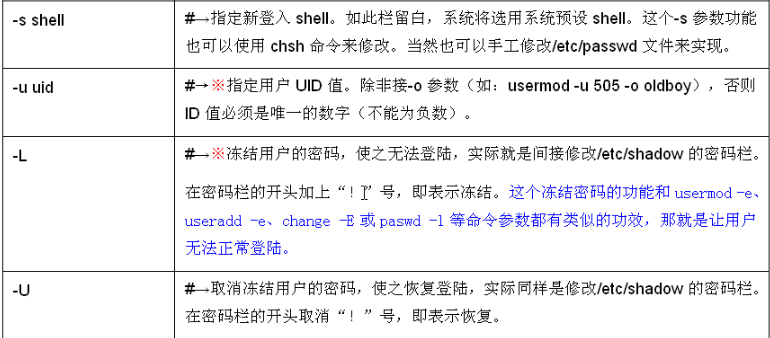
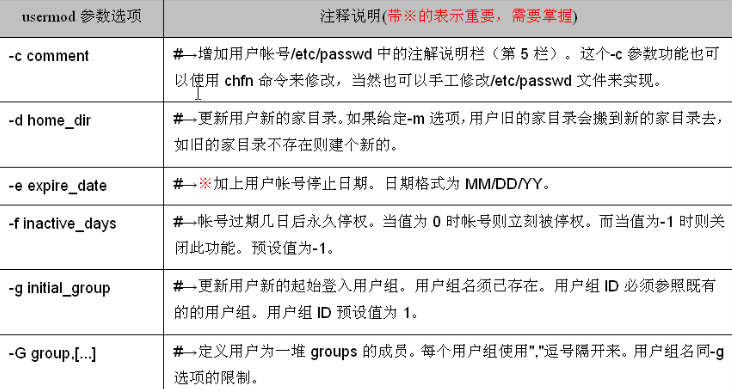
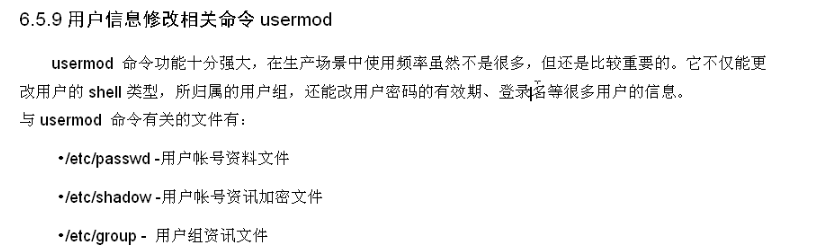
# Chage命令

chage是用来修改用户密码有效期限的



# Usermod命令

Usermod命令参数与useradd相似，不同在于useradd是添加用户，usermod是修改用户

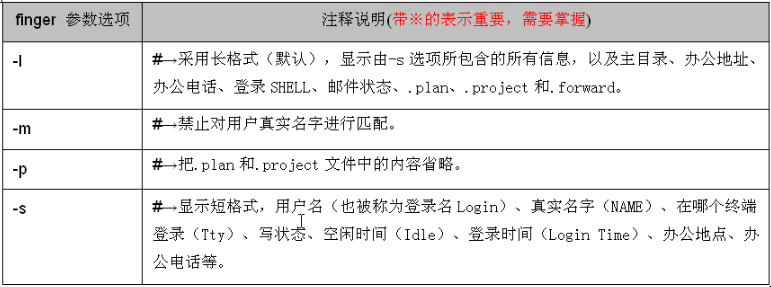


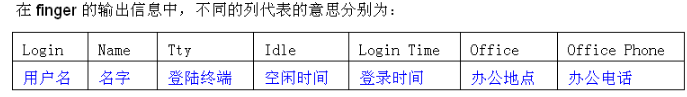
# 用户查询相关命令

1. id id命令是来查询用户的信息，比如用户归属哪个组 GID UID等等



1. finger 侧重于用户信息的查询，查询内容包括用户名 家目录 登录shell类型等





1. W命令显示已经登录的用户，并且都做了什么的信息，查看的信息与/var/run/utmp文件有关
2. Who显示哪些用户在登录，终端及登录时间 来源主机
3. Users仅显示哪些用户在登录
4. Last 显示已登录的用户列表及登录时间等，查看的信息与/var/log/wtmp和/var/log/btmp俩个文件有关
5. Lastlog 报告显示最近的所有系统用户的登录信息，查看信息与/var/log/lastlog文件有关
6. Groups 查看用户归属哪个组

newgrp命令

如果一个用户同时隶属于两个或两个以上分组，需要切换到其它用户组来执行一些操作，就用到了newgrp命令切换当前登陆所在组

命 令: newgrp   
功能说明：切换用户所在用户组命令 登入另一个群组。   
语　　法：newgrp [群组名称]

生产环境中，一般都用普通用户启动进程

Ps –ef |gerp mysql 查看属于mysql用户的进程

# 硬盘

