第 4 章　用户和用户组管理

Linux 和其他类 UNIX 系统一样是一个多用户、多任务操作系统。多用户特性允许多人在 Linux 中创建独立的账户来确保用户个人数据的安全性。而多任务机制允许多个用户同时登录，使用系统的软硬件资源。

本章分别从命令行和图形界面两个层次对普通用户、根用户以及用户组的设置与管理进行了介绍，并对用户管理常见问题进行了分析。用户和用户组管理是 Linux 系统管理的基础，也是实现 Linux 系统安全的重要手段。良好的用户和用户组管理可以为进一步扩展 Linux 系统应用提供强有力的支持。

在 Linux 操作系统中，每一个用户都有一个惟一的身份标识，称为用户 ID(UID)。每一个用户至少需要属于一个用户组。用户组是由系统管理员创建，由多个用户组成的用户群体。每一个用户组也有一个惟一的身份标识，称为用户组 ID。不同的用户和用户组对系统拥有不同的权限。对文件或目录的访问以及对程序的执行都需要调用者拥有相符合的身份，同样一个正被执行的程序也相应地继承了调用者的所有权限。

Linux 用户被划分为两类：一类是根用户(root 用户)也称为超级用户，一类是普通用户。根用户是系统的所有者，对系统拥有最高的权力，可以对所有文件、目录进行访问，执行系统中的所有程序而不管文件、目录和程序的所有者同意与否。普通用户的权限由系统管理员创建时赋予。通常普通用户只能管理自己的属主文件或组内共享及完全共享的文件。根用户与 Windows 系统中的 Administrator 地位相当，但根用户在 Linux 系统中是惟一的，且不允许重新命名。

4.1　普通用户的管理

用户管理的基本任务包括添加新用户、删除用户，修改用户属性以及对现有用户的访问参数进行设置。与此密切相关的文件包括/etc/passwd、/etc/shadow 以及/home 目录。虽然 Red Hat Enterprise Linux 提供了图形化工具可以完成这些任务，但大多数管理员更习惯从命令行界面中执行管理操作。

4.1.1　添加新用户

系统中一个合法的用户应该具有用户名、真实姓名、密码、登录环境等用户信息。与此相对应，添加一个新用户通常系统需要完成以下几项操作。

（1）设置用户名称及密码。

（2）设置用户的 UID。系统在/etc/passwd 文件中查找目前使用的大于 500 的 UID 的最大编号，加 1 后赋予当前的新用户；若目前还没有大于 500 的编号，则将 500 赋予该用户。

（3）添加该新用户的用户组。每一个用户都会属于一个或多个用户组。系统在添加新用户时默认添加的用户组名与新用户名相同，同时会赋予该用户组一个 GID，通常 GID 的编号与 UID 的编号相同。

（4）创建以新用户的用户名为名称的主目录。在大多数系统中，用户的主目录都被创建在同一个特定目录下，例如/home。各用户对自己的主目录有完全的读、写、执行权限，其他用户只能依据该目录的权限进行访问。

（5）设定用户的 shell 环境，默认是/bin/bash。

（6）设定用户的失效时间，默认是 99999 天后。

（7）设定失效前发出警告的天数，默认是失效前 7 天。

在 Red Hat Enterprise Linux 5 的安装过程中，系统会自动创建若干默认的标准用户（Standard Users），其中除了 root 代表系统管理者之外，其余账号都是系统账号。系统账号是应用程序在运行过程中所具有的权限。有关标准用户的详细说明如表 4-1 所示。

表 4-1 Linux系统标准用户说明

用户名	用户ID	用户组ID	用户所在组	用户主目录	使用的Shell
root	0	0	root	/root	/bin/bash
bin	1	1	bin	/bin	/sbin/nologin
daemon	2	2	daemon	/sbin	/sbin/nologin
adm	3	4	adm	/var/adm	/sbin/nologin
lp	4	7	lp	/var/spool/lpd	/sbin/nologin
sync	5	0	sync	/sbin	/bin/sync
shutdown	6	0	shutdown	/sbin	/sbin/shutdown
halt	7	0	halt	/sbin	/sbin/halt
mail	8	12	mail	/var/spool/mail	/sbin/nologin
news	9	13	news	/etc/news	
uucp	10	14	uucp	/var/spool/uucp	/sbin/nologin
operator	11	0	operator	/root	/sbin/nologin
games	12	100	games	/usr/games	/sbin/nologin
gopher	13	30	gopher	/var/gopher	/sbin/nologin
ftp	14	50	FTP User	/var/ftp	/sbin/nologin
nobody	99	99	Nobody	/	/sbin/nologin
rpm	37	37		/var/lib/rpm	/sbin/nologin
dbus	81	81	System message bus	/	/sbin/nologin
avahi	70	70	Avahi daemon	/	/sbin/nologin
mailnull	47	47		/var/spool/mqueue	/sbin/nologin
smmsp	51	51		/var/spool/mqueue	/sbin/nologin
nscd	28	28	NSCD Daemon	/	/sbin/nologin
vcsa	69	69	virtual console memory owner	/dev	/sbin/nologin
haldaemon	68	68	HAL daemon	/	/sbin/nologin
rpc	32	32	Portmapper RPC user	/	/sbin/nologin
rpcuser	29	29	RPC Service User	/var/lib/nfs	/sbin/nologin
nfsnobody	65534	65534	Anonymous NFS User	/var/lib/nfs	/sbin/nologin
sshd	74	74	Privilege-separated SSH	/var/empty/sshd	/sbin/nologin
pcap	77	77		/var/arpwatch	/sbin/nologin
ntp	38	38		/etc/ntp	/sbin/nologin
gdm	42	42		/var/gdm	/sbin/nologin
apache	48	48	Apache	/var/www	/sbin/nologin
distcache	94	94	Distcache	/	/sbin/nologin
postgres	26	26	PostgreSQL Server	/var/lib/pgsql	/bin/bash
mysql	27	27	MySQL Server	/var/lib/mysql	/bin/bash
dovecot	97	97	dovecot	/usr/libexec/dovecot	/sbin/nologin
webalizer	67	67	Webalizer	/var/www/usage	/sbin/nologin
squid	23	23		/var/spool/squid	/sbin/nologin
named	25	25	Named	/var/named	/sbin/nologin
xfs	43	43	X Font Server	/etc/X11/fs	/sbin/nologin
sabayon	86	86	Sabayon user	/home/sabayon	/sbin/nologin

管理员可以使用 useradd 或 adduser 命令来添加一个新的用户。在 Red Hat Enterprise Linux 5 中通过查看 adduser 和 useradd 这两个命令的文件信息,可以看出其功能是完全相同的：

```
#ls –l /usr/sbin/useradd   /usr/sbin/adduser
lrwxrwxrwx 1 root root 7 07-12 07:05 /usr/sbin/adduser->useradd    //链接文件
-rwxr-x---   1 root root 74512 01-17 03:50 /usr/sbin/useradd          //普通文件
```

可以看出，adduser 命令只是 useradd 命令的一个链接文件，如此设计只是为了方便用户的使用。useradd 程序通常在/usr/sbin 目录中，命令格式为：

```
useradd [-c comment] [-d home_dir]
        [-e expire_date] [-f inactive_time]
        [-g initial_group] [-G group[,...]]
        [-m [-k skeleton_dir] | -M] [-s shell]
        [-u uid [ -o]] [-n] [-r] login
useradd -D [-g default_group] [-b default_home]
        [-f default_inactive] [-e default_expire_date]
        [-s default_shell]
```

不带-D 参数时，useradd 命令用来指定新账户的设定值，如果没有指定则使用系统的默认值。useradd 可使用的选项为：

- -c comment：用户的注释说明。
- -d home_dir：用户每次登录系统时所使用的登录目录，可以用来取代默认的/home/username 主目录。
- -e expire_date：账号失效日期。日期的指定格式为 MM/DD/YY。
- -f inactive_days：设定从账号过期到永久停用的天数。当值为 0 时帐号到期后会立即被停用。而当值为-1 时，账号不会被停用，系统默认值为-1。
- -g initial_group：用户默认的用户组或默认的组 ID。该用户组或组 ID 必须是已经存的，其默认组 ID 值为 100，即属于 users 组。
- -G group,[...] ：设定该用户为若干用户组的成员。每个用户组使用“，”分隔，且不可以夹杂空格。组名与-g 选项的限制相同，且-g 的设定值为用户的第一用户组。
- -m：用户目录如不存在则自动建立。若使用-k 选项，则 skeleton_dir 目录内的文档会复制至此用户目录中，同时/etc/skel 目录下的文档也会复制过去。任何在 skeleton_dir 或者/etc/skel 中的目录也同样会在该用户目录下一一建立。-k 和-m 的默认值是不建立目录以及不复制任何文档。
- -M：不建立用户主目录，使用/etc/login.defs 系统文件对用户进行设定。
- -n：系统默认用户组名称与用户名称相同。打开此选项将取消此默认设定。
- -r：此参数是用来建立系统账号。系统账号的 UID 是比定义在/etc/login.defs 中的 UID_MIN 小的值，UID_MIN 的默认值是 500。
- -shell default_shell：指定用户的登录 shell，系统默认为/bin/bash。
- -u uid：用户的 UID 值。该数值在系统中必须唯一，且数字不可为负值。0～499 传统上预留给系统账号使用。

注意：“useradd -r”命令所建立的账号不会创建用户主目录，也不会依据/etc/login.defs 对用户进行设置。如果想创建用户主目录，须额外指定-m 参数。

带参数-D 且配合其他选项，useradd 可以对系统的默认值进行重新设定。如不带任何其他选项，则显示当前的默认值，如下所示：

```
#useradd  -D
GROUP=100
HOME=/home
```

```
INACTIVE=-1
EXPIRE=
SHELL=/bin/bash
SKEL=/etc/skel
CREATE_MAIL_SPOOL=no
```

例如修改 useradd 命令的默认值，命令行如下：

```
//修改 useradd 命令使用的 shell 的默认值为“/bin/csh”
#useradd –D –s /bin/csh
#useradd –D                    //显示默认值
GROUP=100
HOME=/home
INACTIVE=-1
EXPIRE=
SHELL=/bin/csh                 //默认 Shell 已改为/bin/csh
SKEL=/etc/skel
CREATE_MAIL_SPOOL=no
```

例如添加一新用户 student2，UID 为 502，用户组 ID 为 100（users 用户组的标识符是 100），用户目录为/home/student2，用户的默认 Shell 为/bin/bash，账号的失效日期为 2007 年 10 月 30 日，其命令行为：

```
#useradd student2  –u  550 –d  /home/student  -s  /bin/bash  -e  10/30/07  –g  100
//新添加用户的用户信息存储在/etc/passwd 和/etc/shadow 文件尾行，使用 tail 命令可以查看指定的行
#tail -1 /etc/passwd              //显示/etc/passwd 文件最后一行内容
student2:x:550:100::/home/student2:/bin/bash
#tail -1 /etc/shadow              //显示/etc/shadow 文件最后一行内容
student2:!!:13707:099999:7: :13816:
```

如果新添加的用户名已经存在，那么执行 useradd 命令后，系统会提示用户已存在：

```
#useradd student2
useradd: user student2 exists
```

4.1.2　解析/etc/passwd 文件

/etc/passwd 文件存储着用户的相关信息，包括用户名、密码、主目录位置等。根用户对该文件有读和写的权限，普通用户只有读权限。Linux2.0 以上版本为了增强系统的安全性，采用了用户基本信息与密码分开存储的方法，密码已不存放在/etc/passwd 文件中，而是转存到了同目录下的/etc/shadow 文件中，其原来存放密码的位置用“x”标识。/etc/passwd 存储的信息格式如下：

```
Username:encypted password:UID:GID:full name:home directory:login shell
```

其中共分 7 个字段，各字段之间用“:”分隔。利用 cat 命令查看/etc/passwd 文件内容如下：

```
#cat  /etc/passwd
root:x:0:0:root:/root:/bin/bash                  //根用户的设置项,UID 为 0,属于 root 组，登录 Shell 为/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin                 //该用户在/bin 下有许多命令，且主目录为/bin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin     //该用户可以控件一些打印功能，包括移或清除 lp 日志、打印假脱机文
                                             //件等工作。lp 的主目录是/var/spool/lpd
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
```

```
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin //该用户可以管理电子邮件。Mail 组有使用/var/spool/mail 文件的权限
news:x:9:13:news:/etc/news:                    //该用户可以对 Internet 新闻服务进行管理
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin    //该用户管理匿名 ftp 服务
nobody:x:99:99:Nobody:/:/sbin/nologin
rpm:x:37:37::/var/lib/rpm:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
avahi:x:70:70:Avahi daemon:/:/sbin/nologin
mailnull:x:47:47::/var/spool/mqueue:/sbin/nologin
smmsp:x:51:51::/var/spool/mqueue:/sbin/nologin
nscd:x:28:28:NSCD Daemon:/:/sbin/nologin
vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin
haldaemon:x:68:68:HAL daemon:/:/sbin/nologin
rpc:x:32:32:Portmapper RPC user:/:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
pcap:x:77:77::/var/arpwatch:/sbin/nologin
ntp:x:38:38::/etc/ntp:/sbin/nologin
gdm:x:42:42::/var/gdm:/sbin/nologin
apache:x:48:48:Apache:/var/www:/sbin/nologin   //该用户管理 http 服务
distcache:x:94:94:Distcache:/:/sbin/nologin
postgres:x:26:26:PostgreSQL Server:/var/lib/pgsql:/bin/bash
mysql:x:27:27:MySQL Server:/var/lib/mysql:/bin/bash   //该用户管理 mysql 数据库
dovecot:x:97:97:dovecot:/usr/libexec/dovecot:/sbin/nologin
webalizer:x:67:67:Webalizer:/var/www/usage:/sbin/nologin
squid:x:23:23::/var/spool/squid:/sbin/nologin
named:x:25:25:Named:/var/named:/sbin/nologin
xfs:x:43:43:X Font Server:/etc/X11/fs:/sbin/nologin
sabayon:x:86:86:Sabayon user:/home/sabayon:/sbin/nologin
yang:x:500:500:yang:/home/yang:/bin/bash       //系统安装时创建的普通用户
teacher:x:501:501::/home/teacher:/bin/bash     //管理员自行添加的用户
```

可以使用 vipw 命令直接编辑/etc/passwd 文件。vipw 命令功能上相当于“ vi /etc/passwd”命令，但比直接使用 vi 命令更安全。在用 vipw 命令编辑 passwd 文件时将自动对该文件加锁，编辑结束自动解锁，从而保证了数据的一致性。

其中列出了所有的用户信息，每个用户占用一行，各字段含义如下：

（1）用户名：用户名是用户在系统中的标识，通常长度不超过 8 个字符，由字母、数字、下划线或句点组成。

（2）密码：该字段存放加密后的用户密码。由于现在的系统大多采用 shadow 技术，该字段通常只存放一个特殊的字符“x”，真正的密码已转移到/etc/shadow 文件中。

如果该字段的第一个字母是“#”，如下例所示，表示该用户已被停用，即系统暂时不再允许该用户登录，但该用户的用户信息及相应的主目录及属主文件仍保存在系统中，并没有被系统删除。

```
yang:x:500:500:yang:/home/yang:/bin/bash
# teacher:x:501:501::/home/teacher:/bin/bash
```

（3）用户标识号(UID)：UID 是用户在系统中的唯一标识号，必须是整数，通常和用户名一一对应。

当有多个用户名对应同一个 UID 时，系统会把它们视为同一用户。

UID 标识号的取值范围是 0～65535。0～499 一般由系统自己保留，其中“0”由根用户占用，新增用户的 UID 和 GID 需要大于等于 500。

（4）用户组标识号(GID)：该字段记录用户所属的用户组。用户组的具体定义可以查看/etc/group 文件。

（5）个人信息描述：该字段记录用户的真实姓名、电话、地址、邮编等个人信息。各项之间用“，”分隔，该字段内容可以为空。

（6）登录目录：该目录是用户录登系统后的默认目录，通常就是用户的主目录，一般在/home 下。根用户登录系统后默认的登录目录是/root。

（7）登录 Shell：用户以文本方式登录系统后需要启动一个 Shell 进程。Shell 是用户和 Linux 内核之间的接口程序，负责将用户的操作传递给内核，所以 Shell 也被称为命令解释器。在 Linux 系统中有多种 Shell 可以使用，各 Shell 之间略有差别，常用的包括 sh(Bourne Shell)、csh(C Shell)、ksh(Korn Shell)、tcsh(TENEX/TOPS-20 type C Shell)、 bash(Bourne Again Shell)等。其中 C shell 可以提供方便的用户界面设计，语法与 C 语言很相似，而 Korn Shell 兼有 C shell 和 Bourne Shell 的优点。

无论是普通用户还是根用户，登录系统后都会进入该字段指定的命令解释器状态下，用户输入的每一个命令都将被这个命令解释器翻译执行。

该字段也可以指定为一个特定的程序，此时用户登录后只能执行该程序。程序执行结束，用户就自动退出了系统。

4.1.3　解析/etc/shadow 文件

由于普通用户可以读取/etc/passwd 文件，因此密码直接保存在该文件中是极不安全的，很可能会被别有用心的人获取并破译。目前的操作系统在密码保护方面大多采用了 Shadow Passwords 及 MD5 口令保护功能。Shadow Passwords 技术，即影子密码，是将加密的口令放在了另一个文件/etc/shadow 中，并且对/etc/shadow 文件设置严格的权限，只有根用户可以读取该文件。/etc/shadow 文件中存储的信息格式如下：

```
Username:Encypted password:Number of days:Minimum password life:Maximum password life:Warning period:Disable account:Account expiration:Reserved
```

其中共分 9 个字段，各字段之间用“:”分隔。利用 cat 命令查看/etc/shasow 文件内容如下：

```
#cat /etc/shadow
root:$1$f9.s.ENV$9PcgRNEuspQsWgG8vX.8V/:13698:0:99999:7:::  //根用户已设置密码,帐户 99999 天后失效,
                                                            //失效前 7 天系统会给出警告
bin:*:13698:0:99999:7:::
daemon:*:13698:0:99999:7:::
adm:*:13698:0:99999:7:::
lp:*:13698:0:99999:7:::
sync:*:13698:0:99999:7:::
shutdown:*:13698:0:99999:7:::
halt:*:13698:0:99999:7:::
mail:*:13698:0:99999:7:::
news:*:13698:0:99999:7:::
uucp:*:13698:0:99999:7:::
operator:*:13698:0:99999:7:::
games:*:13698:0:99999:7:::
```

```
gopher:*:13698:0:99999:7:::
ftp:*:13698:0:99999:7:::                    //ftp 用户，目前已禁止该用户登录
nobody:*:13698:0:99999:7:::
rpm:!!:13698:0:99999:7:::
dbus:!!:13698:0:99999:7:::
avahi:!!:13698:0:99999:7:::
mailnull:!!:13698:0:99999:7:::
smmsp:!!:13698:0:99999:7:::
nscd:!!:13698:0:99999:7:::
vcsa:!!:13698:0:99999:7:::
haldaemon:!!:13698:0:99999:7:::
rpc:!!:13698:0:99999:7:::
rpcuser:!!:13698:0:99999:7:::
nfsnobody:!!:13698:0:99999:7:::
sshd:!!:13698:0:99999:7:::
pcap:!!:13698:0:99999:7:::
ntp:!!:13698:0:99999:7:::
gdm:!!:13698:0:99999:7:::
apache:!!:13698:0:99999:7:::                //http 用户，未启用，暂无法登录
distcache:!!:13698:0:99999:7:::
postgres:!!:13698:0:99999:7:::
mysql:!!:13698:0:99999:7:::                 //mysql 用户，未启用，暂无法登录
dovecot:!!:13698:0:99999:7:::
webalizer:!!:13698:0:99999:7:::
squid:!!:13698:0:99999:7:::
named:!!:13698:0:99999:7:::
xfs:!!:13698:0:99999:7:::
sabayon:!!:13698:0:99999:7:::
yang:$1$9y0JsfWl$fW4uZTnP6r7hLykdf7jQ71:13698:0:99999:7:::
teacher::13698:0:99999:7:::                 //设置用户 teacher 密码为空
```

其中列出了所有有效用户的密码信息，每个用户占用一行，一行分 9 个字段，分别表示用户名、密码、从 1970 年到上次修改密码的天数、密码必须连续使用的天数，密码有效期、密码失效前告警的天数、从密码过期到彻底停用的天数、账号失效日期，最后一段作为保留字段，详情见表 4-2。从/etc/shadow 文件和/etc/passwd 文件的对比中可以看出，其每行记录所记载的用户信息是一一对应的。

表 4-2 /ect/shadow项说明

序号	字段	描述
1	Username	用户的登录名
2	Encypted password	已加密的密码
3	Number of days	从1970年1月1日到上次修改密码的天数。
4	Minimum password life	至少在设定的天数内密码是不能修改的。
5	Maximum password life	在设定的天数之后必须重新设置密码。
6	Warning period	在密码失效前，提前提醒用户密码即将失效的天数。
7	Disable account	设定密码过期之后，如果该账号仍没有被使用，则停用该账号的天数。
8	Account expiration	设定账号失效的时间。如果到这个时间还没有使用该账号，用户将不能以该账号身份登录。时间的格式可以是YYYY-MM-DD也可以是距1970年1月1日的天数。
9	Reserved	系统保留

注意：MD5(Message Digest v5) 是密码学中经典算法之一，经常应该于数字签名技术。MD5 可以接受任意长度的字符串，并根据输入的字符串产生一组 128 位的信息摘要。从理论上讲，两组不同的字符串输入是不可能得到相同的输出，

所以 MD5 可以有效保护用户的口令安全。

4.1.4　修改用户的账号

修改用户的账号包括更改用户的用户名、密码、主目录、所属用户组和登录 Shell 等信息。

1. 修改用户基本信息

修改用户的基本信息可以使用 usermod 命令，其命令格式为：

```
usermod [-c comment] [-d home_dir [ -m]]
        [-e expire_date] [-f inactive_time]
        [-g initial_group] [-G group[,...]]
        [-l login_name] [-s shell]
        [-u uid [ -o]] login
```

usermod 命令会参照命令行上指定的选项对用户账号进行修改。下列为 usermod 可用的选项。

- -c comment：更新用户的注释信息。
- -d home_dir：更新用户的登录目录。如果指定了-m 选项，则旧目录中的内容会复制到新的目录中。如果新目录不存在则自动创建。
- -e expire_date：更新用户账号停用日期。其日期格式为 MM/DD/YY。
- -f inactive_days：设定账号失效到永久停用的天数，当值为 0 时账号到期后立刻被停用。而当值为-1 时则关闭此功能。默认值为-1。
- -g initial_group：更新用户的起始登录的用户组，即第一用户组。用户组名必须是已经存在，且默认值为 users 组。
- -G group,[...]：更新用户所属的用户组。通常一个用户可以属于多个用户组，成为多个用户组的成员。每个用户组名之间必须用“，”分隔，如果用户当前所在的用户组不在此例中，则会从该当前用户组中删除此用户。
- -l login_name：变更用户登录时的名称为 login_name。
- -s shell：指定用户新的登录 shell。如果此项留白，系统将选用默认的 Shell。
- -u uid：更新用户的 UID 值 。该值修改后，用户目录树下所有的文件、目录的用户 UID 值会自动改变，但放在用户主目录外的文件、目录的 UID 值则需要用户手动更新。

例如：

```
#usermod   -d   /home/student2   -s   /bin/ksh   -g users student
```

此命令将用户的登录目录改为/home/student2，用户的登录 Shell 改为 ksh，用户所在的组改为 users 和 student。

密码管理是用户管理的一项重要内容。用户在刚创建账号时如果没有设定密码，该账号是被系统锁定的，用户无法用该账号登录。只有为其指定密码（即使密码为空）才能激活账号。

2. 修改用户密码

指定和修改用户密码的命令是 passwd。根用户不仅可以修改自己的密码，还可以修改其他用户密码。普通用户则只能修改自己的密码。passwd 命令格式为：

```
passwd   [-k] [-l][-u][-f][-d][-n mindays][-x maxdays][-w warndays]
         [-i inactivedyas][-S][--stdin][username]
```

- -k：表示只有密码过期才需要用户重新设定密码。
- -l：通过在用户的密码字段前加前缀“！”，对用户进行锁定。锁定的用户无法登录系统，该命令只有根用户有权使用。例如锁定 student 用户，使其不能登录的命令为：

```
#passwd  -l  student
```

- --stdin：表示从标准输入重新读入密码，该标准输入也可为一管道。
- -u：该参数与-l 相反，是对锁定的用户进行解锁操作。该操作会删除密码字段前的“！”，使用户可以重新登录系统。对于口令为空的用户，系统原则上是不允许解锁的，需配合使用-f 参数，才能强制解锁。
- -d：快速删除用户的密码。该命令只对根用户有效。例如删除 student 用户的密码可以执行下面的命令：

```
#passwd  -d  student
```

- -n：设定最短的密码有效期。
- -x：设定最长的密码有效期。
- -w：设定密码过期前，提前发出警报的天数。
- -i：设定密码过期到账号停用的天数。
- -S：显示指定用户当前密码状态。

其中 username 的默认值为当前用户，即用户名为空，则修改当前用户的密码。设定新密码需输入旧密码进行验证，如果验证不正确则不允许修改。新密码需连续输入两次，如果两次的输入一致，则新密码生效，例如：

```
$passwd
Changing password for user student
Changing password for student
(current) UNIX password:
passwd: authentication token manipulation error          //不能提供合法的旧密码，验证失败
$passwd
Changing password for user student
Changing password for student
(current) UNIX password:
New password:
Retype new password:
passwd: all authentication tokens updated successfully.  //两次输入一致，密码生效
```

如果是根用户修改普通用户的密码，则无需知道该普通用户的原始密码，例如：

```
#passwd  student
Changing password for user student
New UNIX password:
Retype new UNIX password:
passwd: all authentication tokens updated successfully
```

密码应是字母、数字以及符号的组合，不应小于 5 个字符长，密码过短或是过于简单系统会提示其是弱口令。如果用户执意要将弱口令设为密码只需继续输入，例如：

```
#passwd  student
Changing password for user student
New UNIX password:                                       //仅输入 3 位密码
BAD PASSWORD: it is  WAY too short                       //密码过短
Retype new UNIX password:
passwd: all authentication tokens updated successfully   //虽然密码过短但已生效
#passwd  student
Changing password for user student
New UNIX password:
BAD PASSWORD: it is too simplistic/systematic            //密码过于简单
```

```
Retype new UNIX password:
passwd: all authentication tokens updated successfully      //虽然密码过于简单但已生效
```

4.1.5　删除用户

当不允许用户再次登录本系统时，可以将该用户从系统中删除。准备删除的用户如果已经登录，则必须退出系统才能删除。与添加用户的操作相反，删除用户时系统需要修改/etc/passwd、/etc/shadow、/etc/group 文件中的对应条目，还需删除用户的主目录及所属文件。userdel 命令格式如下：

```
userdel   [-r]   login
```

如果不带选项“-r”，则只删除用户在系统中的账户信息，用户的主目录及相关文件依然保留在系统中。使用选项“-r”，则可将用户主目录下的文档全部删除。同时该用户放在其他位置的文档也会被一一找出并删除。例如：

```
userdel   -r   student
```

执行该命令后，系统将删除 student 账号，同时删除 student 的主目录、邮件及相关属主文档。删除用户前应检查系统是否还有该用户的相关进程正在执行。如果存在该用户的进程，则需等待其执行完毕或直接终止该用户进程。例如，可以使用 ps 或 top 命令对进程进行查看，使用 kill 命令终止该用户进程：

```
#ps   -aux   |   grep   “student”
student   4001   0.0   0.5   4712   666   ?   S   12:15   0:00   studentproc
#kill   4001
```

用 crontab 命令查看是否还有该用户设定的定时任务，如果有则进行删除。

```
#crontab   -u   student   -r
```

4.1.6　用户的临时禁用

如果不想删除用户，只是临时禁止该用户登录系统，可以通过对/etc/password 或/etc/shadow 文件的修改来实现。例如，可以直接修改/etc/password 文件中希望禁用的用户记录行，在该用户行的行首添加“#”。也可以修改/etc/shadow 文件中的密码字段，在希望禁用的用户所对应密码字段前添加“*”或“!”。如果想重新启用该账户，只需恢复上面所做的操作。

例如，在前面的/etc/passwd 文件中，对用户 yang 临时禁用：

```
#yang:x:500:500:yang:/home/yang:/bin/bash
```

例如，在前面的/etc/shadow 文件中，对用户 teacher 临时禁用：

```
teacher:*$1$v4pzr72Z$wBrJyro1SI622P4nI.UJE.:13698:0:99999:7:::
```

4.1.7　用户缺省配置文件/etc/login.defs

/etc/login.defs 文件中存储的是用户的缺省设置。useradd 命令和【User Manager】窗口都是通过读取该文件来获得新账户的默认值。可以使用带“-D”选项的 useradd 命令修改这些值，也可以直接手工编辑该文件。该文件的具体内容和相关注解如下：

```
# *REQUIRED*
#     Directory where mailboxes reside, _or_ name of file, relative to the
#     home directory.    If you _do_ define both, MAIL_DIR takes precedence.
#     QMAIL_DIR is for Qmail
#
#QMAIL_DIR Maildir
```

```
MAIL_DIR /var/spool/mail                    //用户初始的信箱建立在该目录下
#MAIL_FILE .mail
# Password aging controls:
#
#PASS_MAX_DAYS Maximum number of days a password may be used.
#PASS_MIN_DAYS Minimum number of days allowed between password changes.
#PASS_MIN_LEN Minimum acceptable password length.
#PASS_WARN_AGE Number of days warning given before a password expires.
#
PASS_MAX_DAYS 99999          //设置口令可以使用 99999 天
PASS_MIN_DAYS 0              //设置密码可以连续使用的天数，0 表示可以一直使用
PASS_MIN_LEN  5              //设置密码的最小长度为 5
PASS_WARN_AGE 7              //设置密码失效前 7 天开始报警
#
# Min/max values for automatic uid selection in useradd
#
UID_MIN  500                 //设置自动生成的 UID 的最小值 500
UID_MAX  60000               //设置自动生成的 UID 的最大值 60000
#
# Min/max values for automatic gid selection in groupadd
#
GID_MIN  500                 //设置自动生成的 GID 的最小值 500
GID_MAX  60000               //设置自动生成的 GID 的最大值 60000
#
# If defined, this command is run when removing a user.
# It should remove any at/cron/print jobs etc. owned by
# the user to be removed (passed as the first argument).
#
#USERDEL_CMD /usr/sbin/userdel_local
#
# If useradd should create home directories for users by default
# On RH systems, we do. This option is overridden with the -m flag on
# useradd command line.
#
CREATE_HOME     yes          //设定自动创建主目录
# The permission mask is initialized to this value. If not specified,
# the permission mask will be initialized to 022.
UMASK           077          //设定新建文件或目录的权限是 077
# This enables userdel to remove user groups if no members exist.
#
USERGROUPS_ENAB yes          //设定如果组内成员为空则自动删除该用户组
```

其中以“#”开头的行为注释行，空行和注释行都会被系统忽略。“#”通常用来屏蔽系统暂不使用的功能，若需启用相应功能可将其行首的“#”删除。所有其他行均包括一对关键字和设置值，可以直接修改设置值从而改变系统默认值。不带其他选项使用“useradd　-D”命令也可以查看系统默认设置。

4.1.8　使用 newusers 命令批量添加用户

管理员有时需要一次性创建大量用户账号，例如新学期开学或成立新的部门。如果仍采用 useradd

命令逐一创建不仅浪费时间而且在录入期间也很可能产生错误。通常在此情况下利用脚本程序可以完成批量用户的添加和修改。

例如编写 Shell 程序实现系统自动创建 20 个用户。用户名为 student1~student20，用户组为 users。程序中主要用到变量赋值语句、命令替换语句、循环语句以及流过滤语句 awk。具体操作步骤如下：

（1）使用 tail 命令查看/etc/passwd 和/etc/shadow 文件格式

```
#tail   -1   /etc/passwd
teacher:x:500:500:teacher:/home/teacher:/bin/bash
#tail   -1   /etc/shadow
teacher: :13707:0:99999:7:::
```

（2）根据上述查看情况编写脚本程序

```
#!/bin/sh
i=1
//提取最大的用户 ID 号
awk 'BEGIN { FS= ":" ; }   { print $3 } ' /etc/passwd > uid_list   //将 passwd 文件中的第三列暂存到 uid_list 文件中
temp=` tail -1 uid_list `                                          //该处使用后引号，提取 uid_list 文件中的最后一行
while [   $i   -le   20   ]
do
    //创建新用户的主目录
   mkdir   /home/student${i}
   temp=$(($i+1))
   //在/etc/passwd 和/etc/shadow 文件中添加新的用户信息
   echo   "student${i}:x:${temp}:100:student${i}:/home/student${i}:/bin/bash">>/etc/passwd
   echo   "student${i}: :13707:0:099999:7:::">>/etc/shadow
   i=$(($i+1))
done
```

对于不熟悉程序编写的读者，Red Hat Enterprise Linux 5 也提供了创建大量用户账号的工具——newuser 和 chpasswd。newusers 命令能够用一个含有用户名和密码的用户信息文件来生成和修改大量的账号。这个用户信息文件必须具有与/etc/passwd 文件相同的格式，且每个账号的用户名和用户 ID 必须不同。密码字段可以为空或输入“x”。建立上例中所需的用户信息文件如下：

```
#vi   /new_account
student1:x:501:100: :/home/student1:/bin/bash
student2:x:501:100: :/home/student2:/bin/bash
student3:x:501:100: :/home/student3:/bin/bash
student4:x:501:100: :/home/student4:/bin/bash
…   ...
```

将所建立的用户信息文件/new_account 输出给 newusers 命令可以完成新用户的批量自动建立，命令行如下：

```
#newusers < /new_account
```

（3）通过查看/etc/passwd 文件和/home 目录，可以看到新用户已经被添加，并且相应的主目录也已经创建：

```
#tail -20 /etc/passwd
student1:x:501:100: :/home/student1:/bin/bash
student2:x:501:100: :/home/student2:/bin/bash
student3:x:501:100: :/home/student3:/bin/bash
student4:x:501:100: :/home/student4:/bin/bash
…   ...
#ls /home
```

```
student1 student2 student3 student4 student5 student6 student7 student8 student9 student10
student11 student12 student13 student14 student15 student16 student17 student18 student19 student20
teacher yang
```

（4）创建批量用户的密码也可采用如上所述的方法。首先建立用户的密码文件：

```
#vi /password_account
student1:ijl335u
student2:4jslfjkl
student3:ijl335u
student4:4jslfjkl
…
```

将编辑好的密码文件传输给 chpasswd 命令，完成用户密码的批量设置：

```
#chpasswd < /password_account
```

（5）完成以上步骤后，就可以使用这些账号来登录系统。

4.2　根用户的管理

在 Red Hat Enterprise Linux 5 系统中，首要的管理员用户被称为根用户。该用户对系统拥有完全的控制权，可以对系统做任何的设置和更改，其权力远远大于普通用户。因此该用户一般也被称为 Super User，即超级用户。由于根用户对系统的使用不会受到任何限制和约束，非法用户以 root 身份登录系统或者经验不足的 Linux 用户使用 root 账号所做的误操作，都有可能会对系统造成严重的后果。因此根用户的账号安全显得格外重要。在 Red Hat Enterprise Linux 5 系统安装过程中，除创建根用户外，还会创建系统默认的普通用户。在不是绝对必要的情况下，最好不要用 root 账号登录系统。

4.2.1　修改 root 密码

由于根用户的特殊性，修改根用户的密码也需格外慎重，可以使用 passwd 命令进行修改：

```
#passwd root
Changing password for user root
New password:
Retype new password:
passwd: all authentication tokens updated successfully
```

root 密码的安全至关重要，密码的设置尽量不要基于单词，最好是字母、数字和符号的组合，否则很容易被暴力破解。

4.2.2　使用 su 命令切换为 root

当用户以普通账号登录系统后，由于缺少管理权限无法对系统进行重新设置。利用 su 命令可临时切换为 root 身份：

```
$whoami    //显示当前用户的用户名
teacher
$su        //切换为根用户
Password:
#whoami    //显示当前用户的用户名
root
```

当完成相关的系统设置之后，利用 exit 命令则可以返回普通用户身份，如果要切换到其他用户，可以在 su 命令后加上其他用户的账号名，并输入该账号的密码：

```
$whoami
teacher
$su              //切换到根用户
Password:
#whoami
root
#exit            //返回到用户 teacher
$whoami
teacher
$su student   //切换到 student 用户
Password:
$whoami
student
```

4.2.3　root 密码丢失的处理

由于对系统的许多配置必须由 root 来完成，root 密码丢失会导致系统配置无法进行，从而使系统失去系统管理员的控制。

1. 使用 passwd 命令重新设置 root 密码

Linux 系统可以运行在多种模式下，其中单用户模式不需要用户输入密码即可进入。丢失 root 密码的用户可以以单用户模式进入系统，使用 passwd 命令对密码进行重新设置。操作步骤如下：

（1）当系统启动时，按回车键进入 GRUB 界面，如图 4.1 所示。若安装了多个系统，则在菜单中会显示多个系统引导选项。用上下光标键选中要启动的系统，按回车键直接启动系统，按“e”键可以对启动命令进行编辑，按“a”键可以修改内核的启动参数，按“c”键直接进入 GRUB 命令行。选择“Red Hat Enterprise Linux Server”，并按“e”键进入命令菜单编辑状态。

（2）如图 4.2 例出了目前系统启动时可用的命令选项。其中按“e”键可以对命令行进行编辑，按“b”键启动该命令行，按“c”进入 GRUB 命令行，按“o”在选定行下添加一新行，按“O”在选定行前添加一新行，按“d”键对指定行进行删除，按 ESC 返回主菜单。选择“module /vmlinuz-2.6.18-8.el5xen ”,并按“e”键，进入命令行编辑菜单。

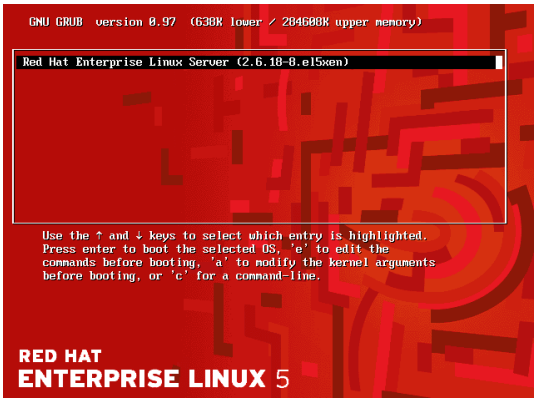

图 4.1 系统选项菜单

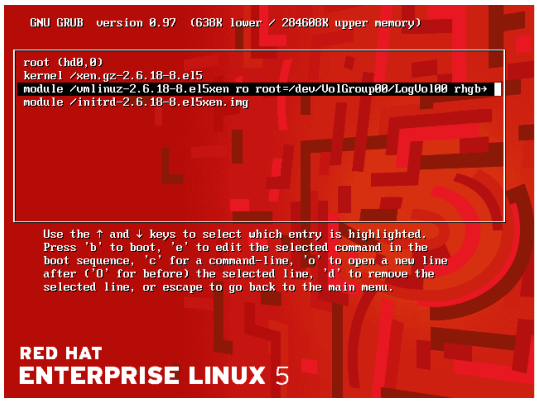

图 4.2 命令行选项菜单

（3）在命令编辑菜单中输入“single”，设定系统以单用户模式启动。返回上一级菜单并按“b”

键启动系统。

（4）系统启动成功后，利用 passwd 命令重新设置 root 密码。

（5）重新启动系统，用新设置的密码登录。

2. 直接删除 root 密码

由于 Linux 密码文件存放在/etc/shadow 文件中，通过对该文件的修改也可以重新设定 root 密码。步骤如下：

（1）用光盘引导系统，并在启动菜单中选择 Linux Rescue 模式。Linux Rescue 模式会自动搜索存在的 Linux 文件系统，找到后自动挂载到/mnt/sysimage 目录下，如图 4.3 所示。

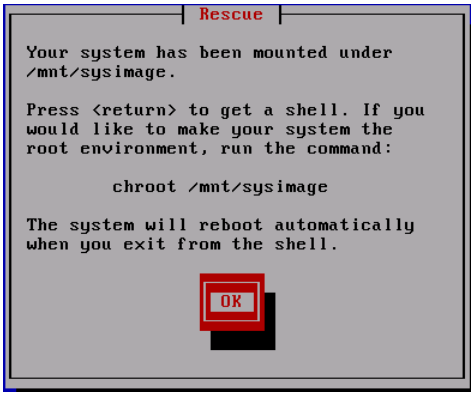

图 4.3 Linux 文件系统被挂载到/mnt/sysimage 目录下

（2）用 vi 打开/etc/shadow 文件，按“x”键逐一删除 root 行中密码字段的内容，并存盘退出。

```
#vi /etc/passwd
root::13698:0:99999:7:::      //删除密码字段的字符串
bin:*:13698:0:99999:7:::
daemon:*:13698:0:99999:7:::
…  ...
```

（3）重新启动系统并用 root 登录，此时 root 密码为空。进入系统后利用 passwd 命令重新设置根用户密码。

4.3　用户组的管理

用户组的管理主要涉及用户组的添加、修改、删除等操作。该操作与系统中的/etc/group 文件和/etc/gshadow 文件密切相关。

4.3.1　添加新用户组

在 Linux 系统中，每个账号都会属于一个用户组。账号的管理应以“组”为单位进行，即先把希望具有相同权限的用户分到同一个用户组，然后再对该用户组的权限进行指定，以此来对用户进行统一管理。

在 Red Hat Enterprise Linux 5 安装过程中，系统除了要自动创建默认的标准账号外，也会自动创建默认的标准用户组（Standard Groups）账号。除了 root 组是用来组织管理者之外，其他的账号都是提供

给应用程序在执行时使用。标准用户组说明如表 4-3 所示。

表 4-3 Linux标准用户组说明

用户组的名称	用户组的标识号	用户组成员列表 （列表中多个用户间用“，”分隔）
root	0	root
bin	1	root,bin,daemon
daemon	2	root,bin,daemon
sys	3	root,bin,adm
adm	4	root,adm,daemon
tty	5	
disk	6	root
lp	7	daemon,lp
mem	8	
kmem	9	
wheel	10	root
mail	12	mail
news	13	news
uucp	14	uucp
man	15	
games	20	
gopher	30	
dip	40	
ftp	50	
lock	54	
nobody	99	
users	100	
rpm	37	
dbus	81	
utmp	22	
utempter	35	
avahi	70	
mailnull	47	
smmsp	51	
nscd	28	
floppy	19	
vcsa	69	
haldaemon	68	
rpc	32	
rpcuser	29	
nfsnobody	65534	
sshd	74	
pcap	77	
ntp	38	
slocate	21	
gdm	42	
apache	48	
distcache	94	
postgres	26	
mysql	27	
dovecot	97	
webalizer	67	
squid	23	
named	25	
xfs	43	
sabayon	86	

screen	84	

用户组可以使用 groupadd 命令进行添加，其命令格式如下：

```
groupadd [-g GID [-o]] [-r] [-f]  [-K KEY=VALUE]  group
```

groupadd 命令会参照命令行上指定的选项对用户组进行设定。下列为 groupadd 可用的选项:

- -g GID：组的 GID，除非使用了-o 选项，否则该值在系统中必须惟一，且不能为负。该值应大于 499 且大于系统中已存的在任何组的 GID 值。其中 0～499 是系统预留。
- -r：创建小于 500 的系统组。若不指定-g 选项，则按递减顺序从小于 500 的可用值中挑选。
- -f：如果所定义的组已经存在，则退出并显示成功信息。如果同时指定了-g 和-f 选项，而-g 所指定的组已经存在，则忽略-g 的值，重新指定新的值。
- -o：允许指定不惟一的 GID，即用新的标识号取代原用户组标识号。
- -K KEY=VALUE：重载/etc/login.defs 中的默认值，例如用 GID_MIN 对用户组标识号最小值进行设定，用 GID_MAX 对用户组标识号最大值进行设定。

例如，添加一个新的用户组 student，GID 为 502，命令行如下：

```
#groupadd  -g  502  student
#tail  -1  /etc/group
student:x:502:
```

在 Red Hat Enterprise Linux 中，添加用户可以使用 useradd 或 adduser 命令，但用户组的添加不存在 addgroup 命令。如果需要，可自行创建一个名为 addgroup 的链接命令，链接到 groupadd 命令：

```
#ln /usr/sbin/groupadd    /usr/sbin/addgroup
```

4.3.2　修改用户组属性

修改用户组属性的命令是 groupmod，其命令格式如下：

```
groupmod [-g GID [-o]]  [-n new group name]  group
```

groupmod 命令会参照命令行上指定的选项对用户组属性进行修改。下列为 groupmod 可用的选项：

- -g GID：为用户组指定新的 GID，除非使用了-o 选项，否则该值在系统中必须惟一，且不能为负。但该选项并不能对文件的 GID 自动更新，文件的 GID 必须用户手动修改。
- -n：更改用户组的名称。

例如修改 teacher 用户组的组标识号为 503，命令行为：

```
#groupmod  -g  503  teacher
```

例如将 teacher 用户组的组标识号改为 550,用户组名称改为 director,命令行为：

```
#groupmod  -g  550  -n  director  teacher
```

一个用户同时可以属于多个用户组。但用户登录系统后，默认只属于一个用户组，可以使用 newgrp 命令使用户在多个用户组之间进行切换，其命令格式为：

```
Newgrp [-] [group]
```

其中选项[-]用于重新加载用户工作环境。如果不带[-]选项，则在切换用户组时，用户的工作环境（包括当前工作目录等）不会改变。

4.3.3　删除用户组

在创建用户账号时，系统会自动创建该账号所属的用户组。但在删除用户账号时，用户组不会自动删除。删除用户组可以使用 groupdel 命令完成。其命令格式如下：

```
groupdel group
```

例如删除 teacher 用户组可以使用如下命令：

```
#groupdel   teacher
```

如果希望删除的用户组中仍有用户登录系统，则无法删除该用户组。必须等该用户组的所有用户退出系统才能正常删除，例如：

```
$whoami
teacher
$groupdel   teacher
groupdel: cannot remove user's primary group.
```

4.3.4　解析/etc/group 文件

用户组文件位于/etc/group，其中存放用户组的账号信息。用户组的添加、删除、和修改实际上就是对该文件的的更新。该文件的内容任何用户都可以读取，但只有根用户可以修改：

```
#ls -l /etc/group
-rw-r--r-- 1 root root 735 Jul 20 07:10 /etc/group
```

/etc/group 文件中每一行对应一个用户组，用“:”分隔成四个字段，各字段说明如表 4-4 所示

表 4-4 /etc/group文件各字段说明

字段	说明
Group_name	用户组的名称。
Encrypted_password	用户组的密码，由于安全原因，相应内容已转到gshadow文件中，在此仅用“x”占位。
GID	用户组标识号，该数字在系统中必须唯一，且不能为负，0～499系统预留。
User_list	组成员列表。

文件/etc/group 内容及相关说明如下：

```
#cat /etc/group
root:x:0:root                    //root 用户组，组成员只有 root，GID 为 0
bin:x:1:root,bin,daemon
daemon:x:2:root,bin,daemon       //守护进程用户组，组成员包括 root,bin,daemon，GID 为 2
sys:x:3:root,bin,adm
adm:x:4:root,adm,daemon
tty:x:5:
disk:x:6:root
lp:x:7:daemon,lp mem:x:8:
kmem:x:9:
wheel:x:10:root
mail:x:12:mail
news:x:13:news
uucp:x:14:uucp
man:x:15:
games:x:20:                      //安装 x-windows 服务需要该组
gopher:x:30:
dip:x:40:
ftp:x:50:                        //ftp 用户组，GID 为 50
lock:x:54:
nobody:x:99:
users:x:100:student3,student4    //普通 users 用户组，GID 为 100，组成员包括 student3,student4,创建普通用户时
                                 //若不指定组则默认为 users 组
rpm:x:37:
```

```
dbus:x:81:
utmp:x:22:
utempter:x:35:
avahi:x:70:
mailnull:x:47:
smmsp:x:51:
nscd:x:28:
floppy:x:19:
vcsa:x:69:
haldaemon:x:68:
rpc:x:32:
rpcuser:x:29:
nfsnobody:x:65534:
sshd:x:74:
pcap:x:77:
ntp:x:38:
slocate:x:21:
gdm:x:42:
apache:x:48:
distcache:x:94:
postgres:x:26:                    //安装 postgres 数据库服务器时使用
mysql:x:27:                       //安装 mysql 服务器时使用
dovecot:x:97:
webalizer:x:67:
squid:x:23:                       //安装代理服务器 squid 时使用
named:x:25:                       //安装 DNS 服务器时使用
xfs:x:43:
sabayon:x:86:
screen:x:84:
teacher:x:500:teacher,director    //teacher 用户的 GID 为 500,组成员包括 teacher ,director
```

注意：与 vipw 命令相类似，可以使用 vigr 命令直接编辑 group 文件。vigr 命令功能上相当于“ vi /etc/group”命令，但比直接使用 vi 命令更安全。在用 vigr 命令打开 group 文件时，系统会自动对 group 文件加锁，编辑结束自动解锁，从而保证了数据的一致性。

4.3.5　解析/etc/gshadow 文件

在 Red Hat Enterprise Linux 5 中，用户组密码的保护机制与用户密码的保护机制一样采用了 Shadow Password 技术。加密后的用户组密码信息保存在了/etc/gshadow 文件中。gshadow 文件只有 root 用户可以读取，文件中每行定义一个用户组的信息，行中各字段用“:”分隔。文件/etc/gshadow 内容及相关说明如下：

```
#cat /etc/gshadow
root:::root                       //root 用户组，组成员只有 root，组密码为空
bin:::root,bin,daemon
daemon:::root,bin,daemon
sys:::root,bin,adm
adm:::root,adm,daemon
tty:::
disk:::root
```

```
lp:::daemon,lp
mem:::
kmem:::
wheel:::root
mail:::mail
news:::news
uucp:::uucp
man:::
games:::
gopher:::
dip:::
ftp:::                              //ftp 用户组，组成员为空，密码为空
lock:::
nobody:::
users:::student3,student4          //普通用户组，组密码为空
rpm:x::
dbus:x::
utmp:x::
utempter:x::
avahi:x::
mailnull:x::
smmsp:x::
nscd:x::
floppy:x::
vcsa:x::
haldaemon:x::
rpc:x::
rpcuser:x::
nfsnobody:x::
sshd:x::
pcap:x::
ntp:x::
slocate:x::
gdm:x::
apache:x::                          //apache 服务的密码设置项
distcache:x::
postgres:x::
mysql:x::                           //mysql 数据库的密码设置项
dovecot:x::
webalizer:x::
squid:x::
named:x::                           //域名服务器的密码设置项
xfs:x::
sabayon:x::
screen:x::
teacher:!!::
student:!::                    //用户组 student 已停用
```

从 gshadow 文件内容可以看出，每行共分四个字段，各字段内容定义如表 4-5 所示。

表 4-5 gshadow文件各字段说明

字段	说明
Group_name	用户组的名称。
Encrypted_password	用户组的密码，该字段用于保存加密后的口令。
Group administrators	用户组的管理员账号，管理员可以对该组进行增、删、改等操作。
User_list	组成员列表，列表中多个用户间用“,”分隔。

4.4　用户和用户组的图形化管理

Red Hat Enterprise Linux 5 是一种多用户的企业级 Linux 产品，除了提供命令行方式外，Red Hat Enterprise Linux 5 还提供了图形化的管理程序来简化用户和用户组管理。

4.4.1　添加新用户

在 Red Hat Enterprise Linux 5 中内置了名为“用户管理者”的图形化工具，可以方便地对用户和用户组进行管理。启动该工具可以单击 【系统】|【管理】|【用户和组群】，弹出【用户管理者】窗口，其中包括【用户】和【组群】两个选项卡，如图 4.4 所示。添加一个新用户步骤如下：

（1）在打开的【用户管理者】窗口中默认显示【用户】选项卡，其中列出了现有的用户列表，但该列表只包含管理员自行添加的用户，系统默认的标准账号并不会显示。列表中列出了【用户名】、【用户 ID】、【主组群】、【全名】、【登录 Shell】、【主目录】等信息，分别与/etc/passwd 文件的对应字段相一致。单击【添加用户】按钮，弹出【创建新用户】对话框，如图 4.5 所示。

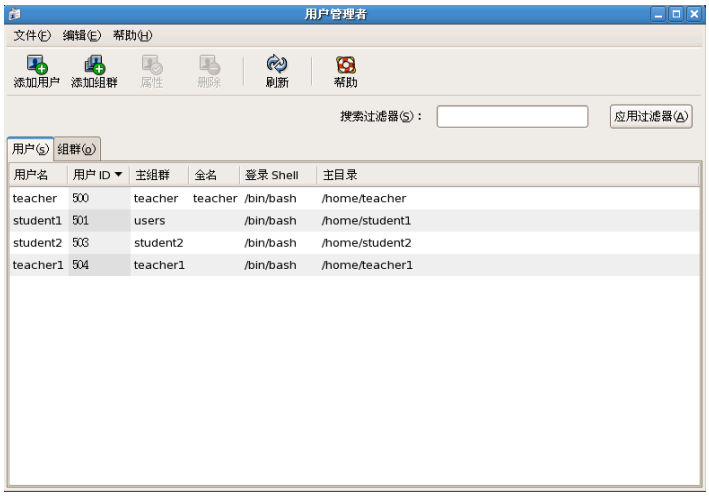

图 4.4　【用户管理者】窗口

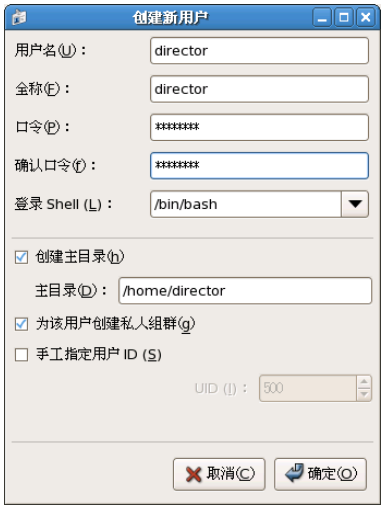

图 4.5【创建新用户】对话框

（2）在【用户名】文本框中输入要创建的用户名；在【全称】文本框中输入用户的全名；在【口令】和【确认口令】文本框中输入密码，密码必须和【口令】文本框中的输入一致并且不少于 6 个字符；在【登录 Shell】文本框中选择用户使用的 Shell；用户的默认主目录是“/home/用户名”，可以根据需要在【主目录】文本框中进行修改。如果点选【为用户创建私人组群】，则创建该新用户的同时会创建以该用户名为名称的新的用户组。取消【为用户创建私人组群】选项，则新建用户默认属于 user 用户组。通过【手工指定 ID】选项可以指定用户的标识号，不建议指定值小于 500。

（3）设置完成后，单击【确定】按钮，返回【用户管理者】窗口，新添加的用户已经显示在列表

中。

4.4.2　修改用户属性

用户属性的修改可以通过如图 4.4 所示的【用户管理者】窗口来完成。修改用户属性步骤如下：

（1）选择待修改用户，单击【属性】按钮，弹出【用户属性】对话框如图 4.6 所示。【用户属性】窗口包括【用户数据】、【账号信息】、【口令信息】、【组群】4 个选项卡，默认显示【用户数据】选项卡。在【用户数据】选项卡中可以修改用户名、全称、口令、主目录和登录 Shell 等信息。

（2）单击【账号信息】选项卡，如图 4.7 所示，用户可以设置账号过期的时间，时间格式为 YYYY-MM-DD。点选【本地口令被锁】复选框，可以对账号临时锁定，禁止该用户登录系统。

图 4.6 设置用户的【用户数据】

图 4.7 设置用户的【账号信息】

（3）单击【口令信息】选项卡，如图 4.8 所示，可以对口令过期进行设定。包括允许口令连续使用的天数，需要更换口令的天数，更换口令前发出警告的天数以及从口令过期到账号停用的天数。

（4）单击【组群】选项卡，如图 4.9 所示，可以设置该用户所属的用户组。列表中列出了系统中现有的用户组。由于一个用户可以属于多个用户组，所以可以在列表中选取多个用户组。但用户的主用户组，即第一用户组只有一个。

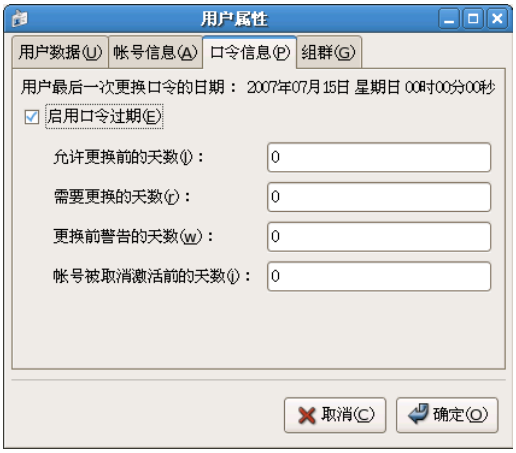

图 4.8 设置用户的【口令信息】

图 4.9　设置用户的【组群】

（5）单击【确定】按钮，完成用户属性信息的修改，返回如图 4.4 所示的【用户管理者】窗口。

4.4.3　删除用户

在如图 4.4 所示的【用户管理者】窗口中选择待删除用户，单击工具栏中的【删除】按钮，系统会询问是否该用户的主目录、邮件和临时文件一同删除，可以根据需要对用户数据进行有保留的删除。

4.4.4　添加新用户组

在【用户管理者】窗口中添加一个新用户组，步骤如下：

（1）在如图 4.4 所示的【用户管理者】窗口中选择【组群】选项卡，打开【组群】管理界面，如图 4.10 所示。列表中列出了管理者自行添加的所有用户组。每个用户组列出了【组群名】、【组群 ID】和【组群成员】信息。

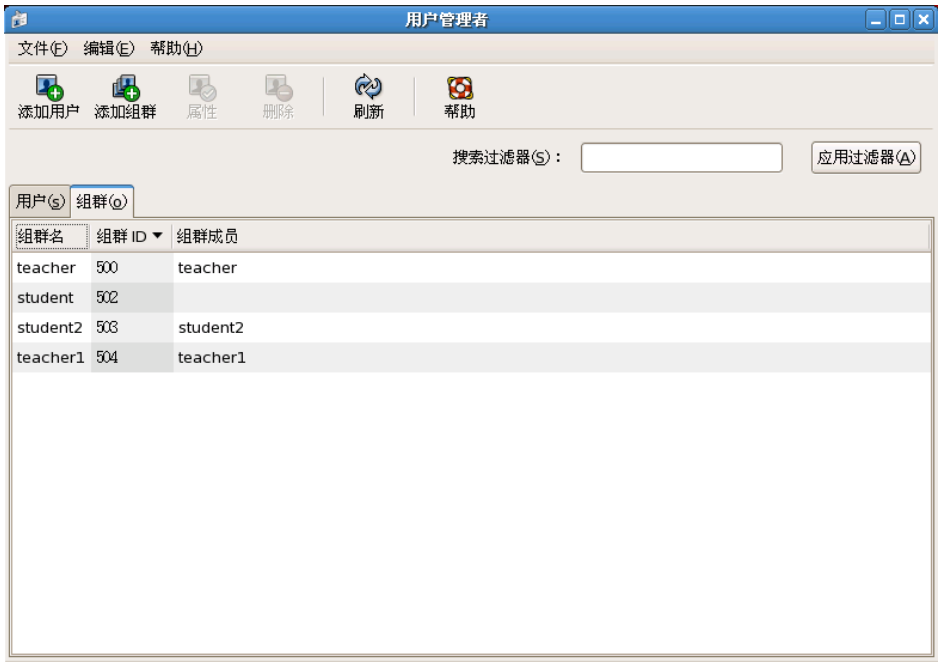

图 4.10【组群】选项卡窗口

（2）单击工具栏中的【添加组群】按钮，弹出【创建新组群】对话框，如图 4.11 所示，填入组群名称，单击确定即可添加完毕。若需指定组群 ID，也可选择【手工指定组群 ID】选项，不建议指定值小于 500。

图 4.11【创建新组群】对话框

图 4.12 设置【组群属性】

（3）单击【确定】按钮，完成新用户组的添加，返回如图 4.4 所示的【用户管理者】窗口。

4.4.5　修改用户组

修改用户组只需要在如图 4.4 所示的【用户管理者】窗口中选择【组群】，单击【属性】按钮，可以弹出【组群属性】对话框，如图 4.12 所示。在【组群数据】选项卡中可以设置用户组的名称，在【组群用户】选项卡中可以选择属于该用户组的成员。

4.4.6　删除用户组

在如图 4.4 所示的【用户管理者】窗口中选择【组群】，选定待删除用户组，单击工具栏中的【删除】按钮，完成用户组的删除。若待删除用户组的组成员不为空，则无法完成删除。

4.5 用户和用户组管理常见问题

用户和用户组管理是 Linux 系统管理中极为重要的环节，管理不当就可能出现账号锁定、无法登录等诸多问题并留下大量的安全隐患。本节将主要介绍用户管理中常见的一些问题并对系统安全提出一些建议。

4.5.1　对/etc/shadow 文件的编辑导致用户密码丢失

当用户尝试修改密码时，如果有人正在编辑/etc/shadow 文件，有可能导致该用户修改的密码失效。例如系统管理员正在使用 VI 编辑/etc/shadow 文件，此时用户 teacher 同时修改了用户密码。用户 teacher 在 /etc/shadow 的记录行未修改前为：

```
teacher:$1$v4pzr72Z$wBrJyro1SI622P4nI.UJE.:13698:0:99999:7:::
```

使用 passwd 命令修改密码后，teacher 用户在/etc/shadow 文件的记录行变为：

```
teacher: $1$9y0JsfWI$fW4uZTnP6r7hLykdf7jQ71.:13698:0:99999:7:::
```

用户 teacher 在系统管理员完成对/etc/shadow 文件的编辑、存盘退出前成功地修改了密码，此时系统管理员保存文件时系统会提示：

```
WARNING：The file has been changed since reading it !!!
Do you really want to write to it(y / n)?
```

如果系统管理员此时回答 y，用户 teacher 就会丢失他新设定的密码。用户 teacher 的/etc/shadow 行就会恢复成原来的值：

```
teacher:$1$v4pzr72Z$wBrJyro1SI622P4nI.UJE.:13698:0:99999:7:::
```

所以修改/etc/passwd 或/etc/shadow 时一定要谨慎。应当尽量使用命令来修改，而不是编辑该文件。

4.5.2　/etc/nologin 文件引起普通用户无法登录

/etc/nologin 文件给系统管理员提供了一种在 Linux 系统维护期间禁止用户登录的方式。为了提高系统的安全性和防止数据的不同步现象，系统管理员在对系统进行维护时，通常建立 0 字节的/etc/nologin 文件，如果存在/etc/nologin 文件，非 root 用户的登录尝试会失败。建立/etc/nologin 文件命令行如下：

```
touch　/etc/nologin
```

这种保护机制也被应用到系统的关机、重启等环节中。通常系统在关闭时要自动创建 nologin 文件，禁止所有用户登录，然后处理相关程序的退出停止工作，并在即将关闭系统前删除/etc/nologin 文件。如果系统在还未正常删除/etc/nologin 文件前出现突然断电停机等情况，就会出现因 nologin 文件未删除而引起的普通用户无法登录现象。此时只需根用户登录系统并删除 nologin 文件，问题即可解决。建议用户在使用系统过程中，不要采用直接关闭电源等不正常手段关闭系统。不正常关闭系统会对系统造成严重的损害。

注意：SSH 由于不查看/etc/nologin 文件，即使/etc/nologin 文件存在，使用 SSH 仍可登录系统。

4.5.3　账户到期或密码失效引起用户无法登录

账户到期或密码失效都会使用户无法登录系统，可以使用 chage 命令查看账户密码的有效期。命令 chage 的命令行格式为：

```
chage [选项] 用户名
```

表 4-6 给出了 chage 选项的定义。

表 4-6 chage选项定义

选项	定义	说明
-d, --lastday	最近日期	将最近一次密码设置时间设为“最近日期”
-E, --expiredate	过期日期	设置账户的过期时间
-h, --help	选项帮助	显示帮助信息并退出
-I, --inactive	密码失效天数	设置从密码过期到账户登录禁用的天数
-l, --list	当前设置	显示账户时效信息
-m, --mindays	最小天数	设置将两次改变密码之间相距的最小天数
-M, --maxdays	最大天数	设置两次改变密码之间相距的最大天数
-W, --warndays	警告天数	设置密码过期之前，向用户发出“密码将过期”警告的天数

例如使用“-l”选项显示 student1 用户的密码时效设置如下：

```
#chage　-l　student1
最近一次密码修改时间　　　　　　　　　：　7 月　21, 2007
密码过期时间　　　　　　　　：7 月　23, 2007
密码失效时间　　　　　　　　：从不
```

```
帐户过期时间                                    ：7 月  29, 2007
两次改变密码之间相距的最小天数          ：0
两次改变密码之间相距的最大天数          ：99999
在密码过期之前警告的天数      ：7
```

当 student1 用户 2007 年 7 月 23 日之后登录系统，系统会强行要求用户修改密码。如果用户未能在 2007 年 7 月 29 日之前修改密码，则会因为账号失效而导致无法登录系统。

4.5.4　用户和用户组管理的安全防范措施

系统管理员可以通过 who 和 last 命令来查询当前系统登录用户和用户历史登录情况。对于可疑用户和非法登录用户应及时采取措施。

查询当前系统中登录的用户，可以使用 who 命令，如下：

```
#who
student1 pts / 0       2007-7-22 11:17 (192.168.21.3)
student2 pts / 1       2007-7-22 16:17 (192.168.3.58)
```

查询最近的使用者登录时间，可以使用 last 命令。last 会列出最近一个月的用户登录曰志，last 的命令行如下：

```
#last
student1 pts/0    192.168.21.3      Sun Jul   22 19:16     still logged in
student2 pts/1    192.168.3.58      Sun Jul   22 18:35     still logged in
student2 pts/0    192.168.21.3      Fri Jul   15 05:56 - crash (1+12:47)
wtmp begins Sun Jul 15 22:03:31 2007
```

从前几节的学习中，可以看到 Linux 系统中提供了一些预置账号，而用户可能根本不需要这些账号。如果用户确实不需要这些账号，可以将其删掉。因为这些账号名是公开的，很容易受到攻击。用下面的命令删除一些不必要的用户：

```
#userdel   adm
#userdel   lp
#userdel   sync
#userdel   shutdown
#userdel   halt
#userdel   news
#userdel   uucp
#userdel   operator
#userdel   gopher
#userdel   ftp          //如果安装了匿名 ftp 服务，请不要删除
//一些用不到的用户组也可以删除
#groupdel   adm
#groupdel   lp
#groupdel   news
#groupdel   uucp
#groupdel   dip
#groupdel   pppusors
#groupdel   popusers   //如果安装了 POP 服务器，请不要删除
#groupdel   slipusers
```

4.5.5　账号管理的常用命令

1. id 命令

用于显示用户当前的 uid、gid 和用户所属的组列表。

```
#id  root
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel)
context=root:system_r:unconfined_t:SystemLow-SystemHigh
```

2. whoami 命令

用于显示当前用户的名称。

```
#whoami
root
```

3. groups 命令

用于显示指定用户所属的用户组。如果未指定用户则显示当前用户所属的组

```
#groups
root bin daemon sys adm disk wheel
```

显示根用户所属的用户组分别为 root、bin、daemon、sys、adm、disk 和 wheel。这与/etc/group 文件中所标记内容一致：

```
#cat  /etc/group  |  grep root
root:x:0:root
bin:x:1:root,bin,daemon
daemon:x:2:root,bin,daemon
sys:x:3:root,bin,adm
adm:x:4:root,adm,daemon
disk:x:6:root
wheel:x:10:root
```

4. newgrp 命令

```
#groups              //显示当前用户所属的用户组
root bin daemon sys adm disk wheel
#id  root            //显示根用户的组信息，当前用户的主组群是 root
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel)
context=root:system_r:unconfined_t:SystemLow-SystemHigh
#newgrp bin      // 改变当前用户的主组群为 bin 用户组
uid=0(root) gid=1(bin) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel)
context=root:system_r:unconfined_t:SystemLow-SystemHigh
//不指定转换的用户组时，系统默认转换为用户的私有组
#newgrp
#id
uid=0(root)gid=0(root)groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel)
context=root:system_r:unconfined_t:SystemLow-SystemHigh
//用户的主组群已变更为 root
```

5. finger 命令

用于查找并显示用户息。

```
#finger  -l  root
Login: root                          Name: root
Directory: /root                     Shell: /bin/bash
```

```
On since 日　7 月 22 19:57 (CST) on pts/1 from :0.0
New mail received 一　7 月 23 04:03 2007 (CST)
      Unread since 五　7 月 20 02:36 2007 (CST)
No Plan.
```

6. who 命令

显示当前登录用户的用户名、登录终端、登录时间以及登录地址。

```
#who
root      pts/1          2007-07-22 19:44 (:0.0)
teacher   pts/0          2007-07-22 10:27 (ns2)
```

7. w 命令

用于显示当前登录的所有用户的信息。

```
#w
06:48:11 up 11:22,  1 user,  load average: 0.05, 0.06, 0.07
USER     TTY      FROM              LOGIN@   IDLE   JCPU   PCPU WHAT
root     pts/1    :0.0              19:57    0.00s  3.02s  0.10s w
```

8. cnfn 命令

修改用户的基本信息。执行该命令系统会进入交互式，依次询问用户的真实姓名、办公室住址、办公电话和家庭电话。

```
#cnfin  teacher1
Changing finger information for teacher1
Name [ ]:yang
Office [ ]: 5 Zhongguanchu St. Beijing
Office Phone [ ]: 010-68913699
Home Phone [ ]: 010-68953428
#finger  teacher
Login: teacher1                         Name: yang
Directory: /home/teacher1                    Shell: /bin/bash
Office: 5 Zhongguanchu St. Beijing  Office Phone: 010-68913699
Home Phone: 010-68953428
Never logged in.
No mail.
No Plan.
```

9．write 命令

使用 write 命令，可以将信息实时传递给登录的用户或终端。通过在命令行指定用户或终端可以控制信息发往何处，不带任何选项使用该命令，会将信息发送给所有登录的用户。

```
#write  student1
System will shutdown soon!
```

用户 student1 会收到：

```
Message form root @bit.edu.cn on pts/0 at 16:55…
System will shutdown soon!
EOF
```

4.5.6　创建用户共享目录

Red Hat Enterprise Linux 可以利用用户组来组织用户进而加强系统的安全性。在/etc/passwd 配置文

件中，每个用户的 UID 通常与其 GID 是一致的。但有些时候有些用户可能属于一个公共部门，也可能正在从事一个公共项目。通过创建一个共同的组和一个共享目录，可以使这个组的所有成员自由读取共享目录中所输入的文件。

例如项目组成员 student1、student2、student3 需要创建一个公共目录用于存放项目开发中的文件。可以将这些用户组织到一个公共组并创建一个共享目录。通过设置 SGID 位，允许该组中的任何用户把文件复制到共享目录中，并允许该组其他成员可以读取共享目录中的所有文件。具体操作步骤如下：

（1）使用 groupadd 命令创建一个公共组。

```
#groupadd   student
```

（2）使用 useradd 命令创建 student1、student2 和 student3 账号，并要给每个用户分配一个密码.

```
#useradd   student1   -g   student                    //添加 student1 用户，并指定为 student 组
#passwd   student1
Changing password for user student1
New UNIX password:
Retype new UNIX password:
passwd: all authentication tokens updated successfully
#useradd   student2   -g   student                  //添加 student2 用户，并指定为 student 组
#passwd   student2
Changing password for user student2
New UNIX password:
Retype new UNIX password:
passwd: all authentication tokens updated successfully
#useradd   student3   -g   student                  //添加 student3 用户，并指定为 student 组
#passwd   student3
Changing password for user student3
New UNIX password:
Retype new UNIX password:
passwd: all authentication tokens updated successfully
```

（3）创建一个名为/home/student 的新共享目录。对于拥有这个目录的用户和组，使用 chmod 770 /home/student 命令给这个目录分配读、写和执行权限(rwx)。

```
#mkdir   /home/student
#chmod   770   /home/student
```

（4）在共享目录上配置 SGID 位，这使得拥有这个目录的组中的所有用户都能够拥有所有权级权限。

```
#chmod   g+s   /home/student
```

（5）使用 chgrp 命令为这个目录设置所有权。

```
#chgrp   student   /home/student
```