第8章用户和组群账户管理

人民邮电出版社
POSTS & TELECOM PRESS

8.1 用户账户管理

8.2 组群账户管理

8.3 账户相关文件或目录

8.4 用户和组群维护命令

8.5 实现账户安全

在Linux系统中，用户账户是登录系统的唯一凭证，其中root用户是系统的最高管理者，该用户的UID是0级，与用户和组账户相关的配置文件有/etc/passwd、/etc/shadow、/etc/group和/etc/gshadow。

在Linux系统中可以使用chage命令管理用户口令的时效，防止用户口令由于长时间使用而导致泄漏。

8.1 用户账户管理

本节主要讲述Linux系统下用户账户的分类、与用户账户有关的配置文件/etc/passwd和/etc/shadow以及如何使用“用户管理者”和字符命令管理用户账户。

8.1.1 Linux用户账户概述

用户在Linux系统中是分角色的，由于角色不同，每个用户的权限和所能完成的操作任务也不同。而在实际的管理工作中，用户的角色是通过UID（用户ID号）来标识的，每个用户的UID都是不同的。

在Linux系统中主要有root用户、虚拟用户和普通用户这3类用户。

1．root用户

root用户是Linux系统的内置用户，在系统中的权限最高，普通用户无法执行的操作，root用户都可以操作，所以也被称之为超级管理用户。在系统中的每个文件、目录和进程都归属于某一个用户，没有用户许可，除root用户外的其它普通用户无法进行操作。

2．虚拟用户

这类用户也被称为伪用户或假用户，这类用户不具有登录系统的能力，但却是系统运行不可缺少的用户，比如bin，daemon，adm，ftp以及mail等用户账户，这类用户都是Linux系统的内置用户。

3．普通用户

这类用户是由系统管理员创建，并且能登录Linux系统。只能操作自己目录内的文件，权限有限。

8.1.2 Linux用户账户配置文件

谈到用户，就不得不谈用户管理、用户配置文件以及用户查询和管理的控制工具。用户管理主要是通过修改用户配置文件完成的，使用用户管理控制工具的最终目的也是为了修改用户配置文件。

1. /etc/passwd文件

/etc/passwd是系统识别用户的一个文件，Linux系统中所有的用户都记录在该文件中。

（1）/etc/passwd文件内容

任何用户都可以读取该文件内容，在/etc/passwd文件中，每一行表示的是一个用户账户信息，一行有7个段位，每个段位用“:”分隔，下面是/etc/passwd文件的部分内容。

zhangsan:x:1000:1000:张三:/home/zhangsan:/bin/bash

表8-1　/etc/passwd文件各字段的含义

字　　段	含　　义
用户名	也称为登录名，在系统内用户名应该具有唯一性。在本例中，zhangsan就是用户名
口令	存放加密的口令，在本例中看到的是一个x，其实口令已被映射到/etc/shadow文件中了
用户标识号	在系统内用一个整数标识用户ID号，每个用户的UID都是唯一的，root用户的UID是0，普通用户的UID默认从1000开始，本例中的用户zhangsan的UID是1000
组群标识号	在系统内用一个整数标识用户所属的组群的ID号，每个组群的GID都是唯一的
用户名全称	用户名描述，可以不设置。在本例中，zhangsan用户的用户名全称是“张三”
主目录	用户登录系统后首先进入的目录，zhangsan用户的主目录是/home/zhangsan
登录Shell	用户使用的Shell类型，Fedora 17系统默认使用的Shell是bash

（2）用户UID的概述

UID是用户的ID值，在系统中每个用户的UID值是唯一的，更确切地说每个用户都要对应一个唯一的UID。Linux系统用户的UID值是一个正整数，初始值从0开始，在Fedora 17系统中的最大默认值是60000。

在Linux系统中，root的UID是0，拥有系统最高权限。UID的唯一性关系到系统的安全，比如在/etc/passwd文件中把用户zhangsan的UID改为0后，zhangsan这个用户会被确认为root用户，当用这个账户登录到系统后，可以进行所有root用户才能执行的操作。

UID是确认用户权限的标识，用户登录系统所处的角色是通过UID来实现的，而不是用户名。

2. /etc/shadow文件

/etc/shadow文件是/etc/passwd文件的影子文件，这个文件并不是由/etc/passwd文件产生，这两个文件是对应互补的。/etc/shadow文件内容包括用户及被加密的口令及其他/etc/passwd不能包括的信息，比如用户账户的有效期限等。

/etc/shadow文件的内容包括9个段位，每个段位之间用“:”分隔。

zhangsan:6E/xvWMmh$rhYLQwwffEqIudVLFzMlvkb0iN4.0
Oluk6H.UovEYN0/99dVoHXcaCNGZZkFY1S3QHYgm7e6JPzEew6
ybmN4e0:16364:0:99999:7:::

表8-2　/etc/shadow文件各字段的含义

字　　段	含　　义
用户名	这里的用户名和/etc/passwd中的用户名是相同的
加密口令	口令已经加密，如果有些用户在这里显示的是“!!”，则表示这个用户还没有设置口令，不能登录到系统
用户最后一次更改口令的日期	从1970年1月1日算起到最后一次修改口令的时间间隔（天数）
口令允许更换前的天数	如果设置为0，则禁用此功能。该字段是指用户可以更改口令的天数
口令需要更换的天数	如果设置为0，则禁用此功能。该字段是指用户必须更改口令的天数
口令更换前警告的天数	用户登录系统后，系统登录程序提醒用户口令将要过期
账户被取消激活前的天数	表示用户口令过期多少天后，系统会禁用此用户，也就是说系统会不让此用户登录，也不会提示用户过期，是完全禁用的
用户账户过期日期	指定用户账户禁用的天数（从1970年的1月1日开始到账户被禁用的天数），如果这个字段的值为空，账户永久可用
保留字段	目前为空，以备将来Linux系统发展时用

8.1.3 图形界面下用户账户的设置

1. 显示Linux系统用户

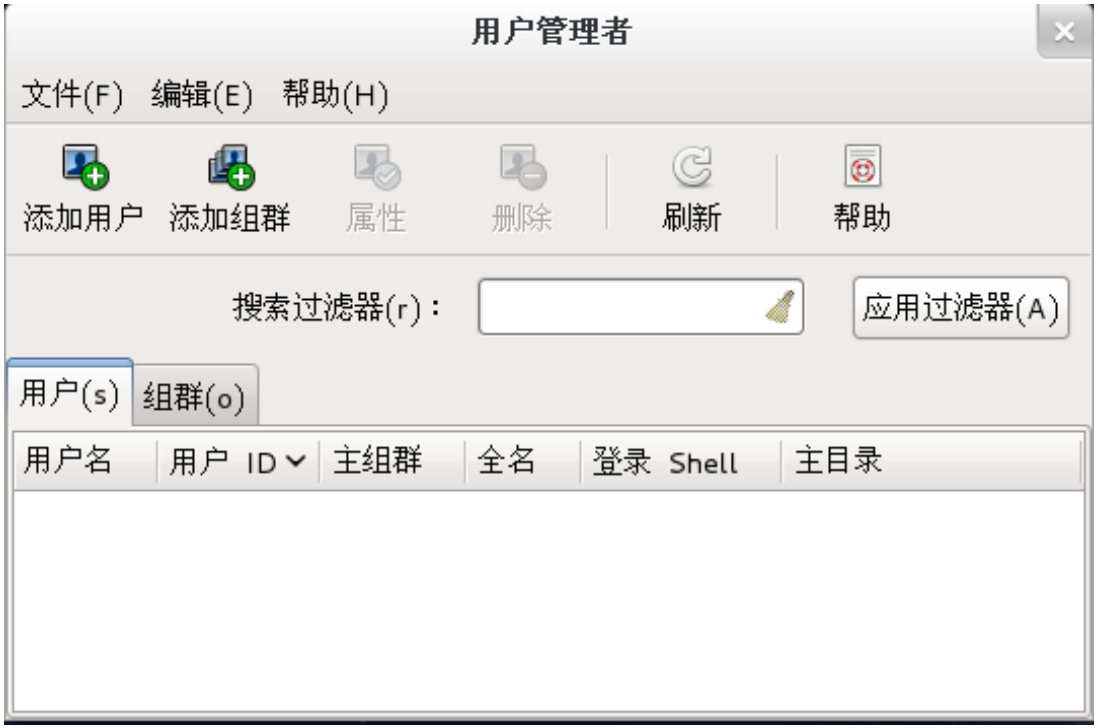

图8-1 “用户管理者”界面

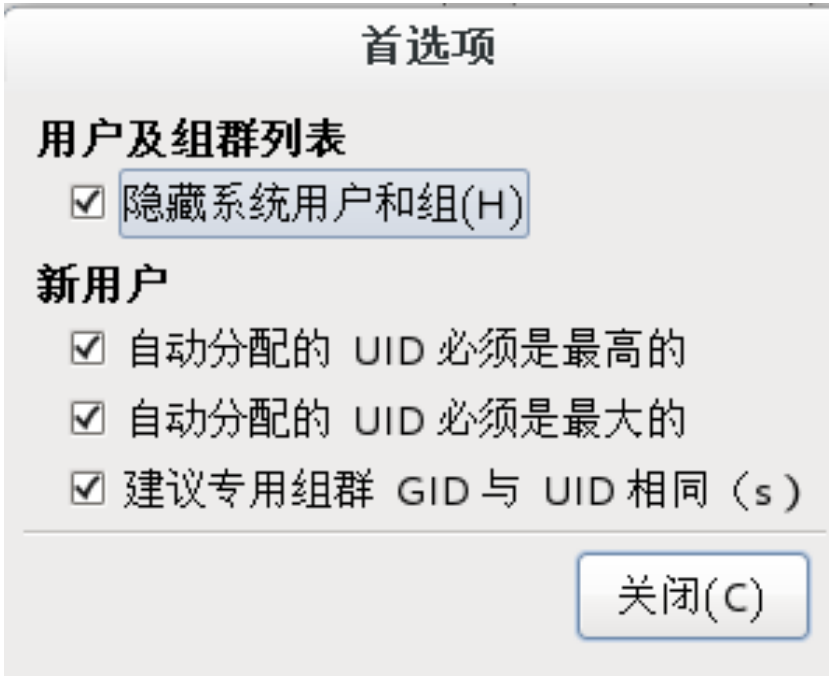
首选项
用户及组群列表
隐藏系统用户和组(H)
新用户
自动分配的 UID 必须是最高的
自动分配的 UID 必须是最大的
建议专用组群 GID 与 UID 相同（s）
关闭(C)

图8-2 “首选项”对话框

图8-3　显示系统用户界面

2. 创建用户账户

图8-4 “添加新用户”对话框

3. 修改用户账户属性

（1）**用户数据**:显示添加用户时配置的基本用户信息。使用这个选项卡改变用户的全称、口令、主目录或登录Shell。

（2）**账户信息**:如果想让用户账户在某一固定日期过期，选择“启用账户过期”选项，并在文本框内输入过期日期。选择“本地密码被锁”选项来锁住用户账户，从而使用户无法登录系统。

（3）**密码信息**:这个选项卡显示了用户口令最后一次被更改的日期。若要强制用户在一定天数之后改变密码，可以选择“启用密码过期”选项，并且设置口令允许更换前的天数、口令需要更换的天数、口令更改前警告的天数以及账户被取消激活前的天数。

（4）**组群**:选择让用户加入的组群以及用户的主要组群。如图8-8所示，用户zhangsan属于wheel和zhangsan组群，主组群是zhangsan。


用户属性
用户数据(U)
帐号信息(A)
密码信息(P)
组群(G)
用户名(N)：
zhangsan
全称(F)：
张三
密码（w）：
*****
确认密码（m）：
*****
主目录(H)：
/home/zhangsan
登录 Shell (L)：
/bin/bash
取消(C)
确定(O)

图8-5 “用户数据”选项卡

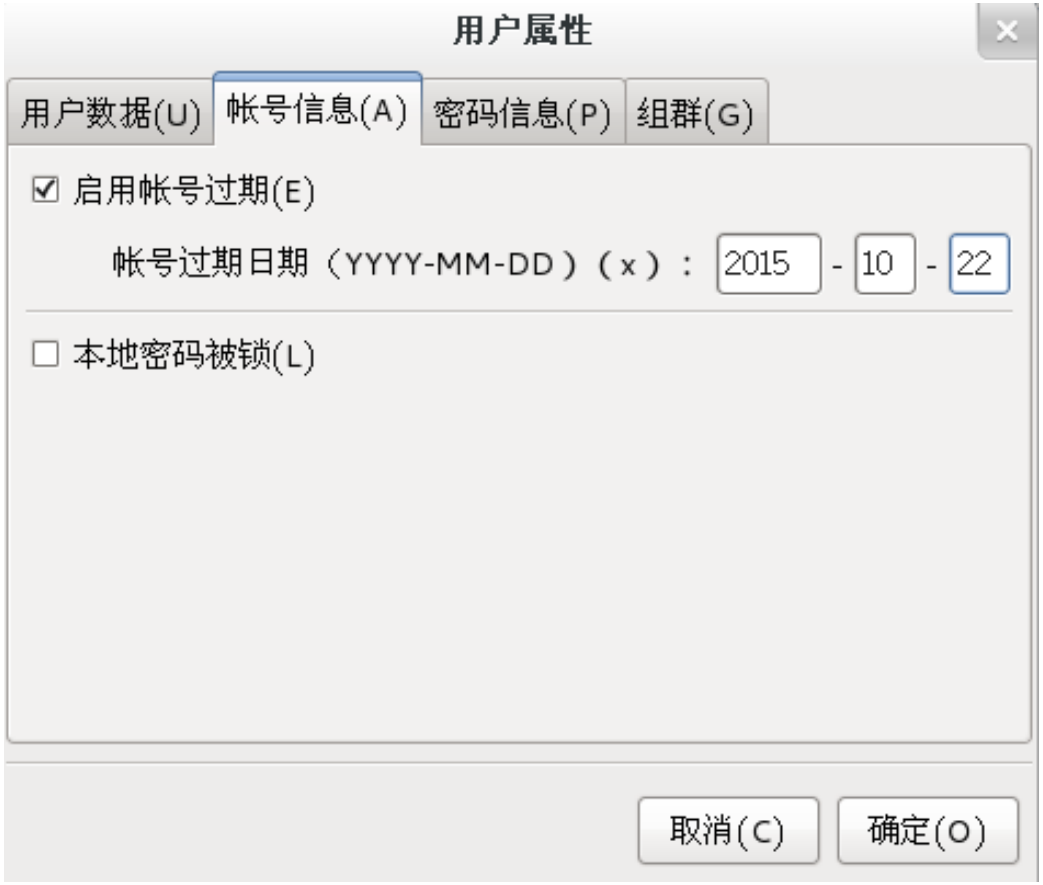
用户属性
用户数据(U)
帐号信息(A)
密码信息(P)
组群(G)
启用帐号过期(E)
帐号过期日期（YYYY-MM-DD）（x）：
2015
-
10
-
22
本地密码被锁(L)
取消(C)
确定(O)

图8-6　“账户信息”选项卡

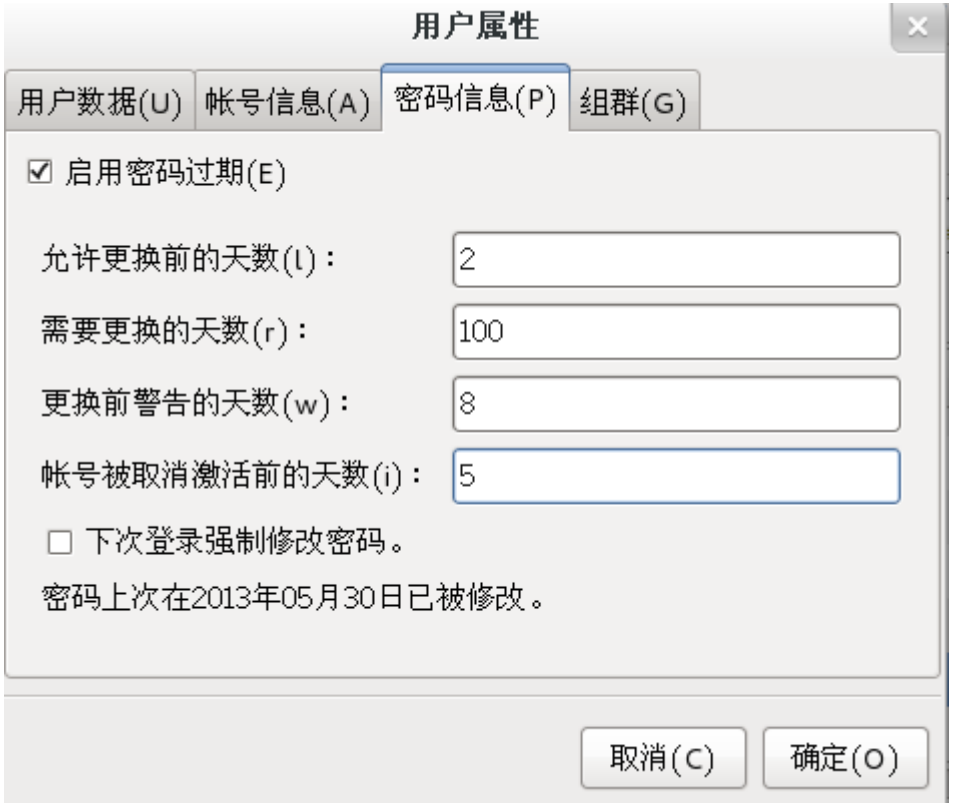
用户属性
用户数据(U)
帐号信息(A)
密码信息(P)
组群(G)
启用密码过期(E)
允许更换前的天数(l)：
2
需要更换的天数(r)：
100
更换前警告的天数(w)：
8
帐号被取消激活前的天数(i)：
5
下次登录强制修改密码。
密码上次在2013年05月30日已被修改。
取消(C)
确定(O)

图8-7　“密码信息”选项卡

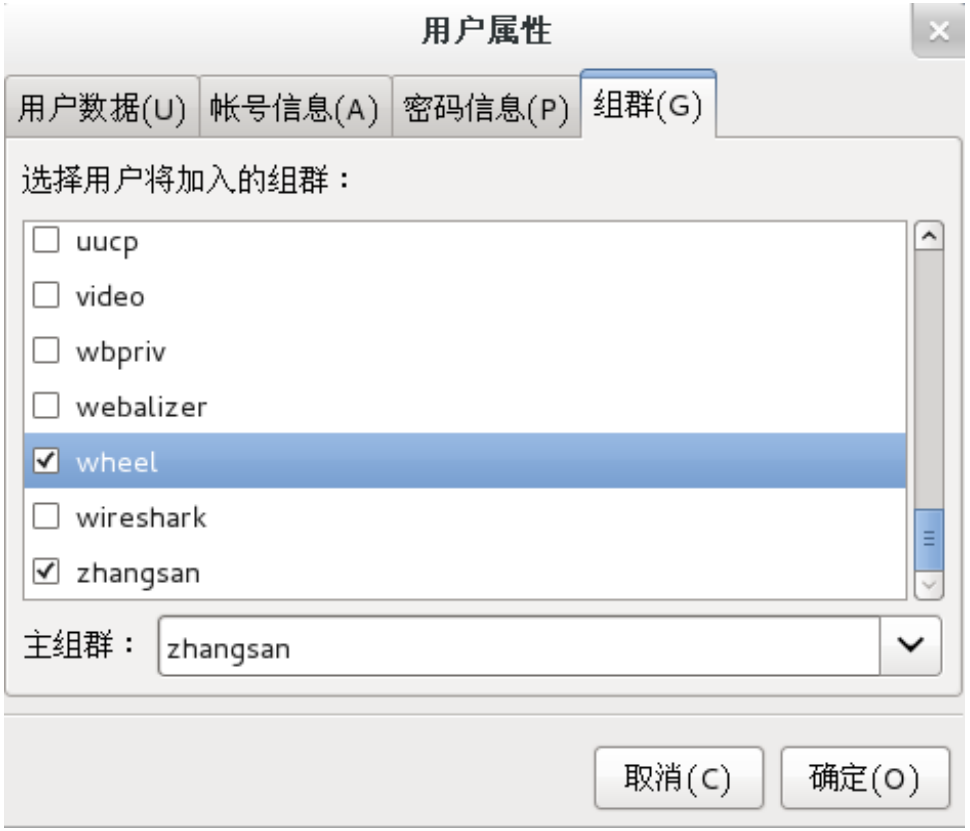
用户属性
用户数据(U)
帐号信息(A)
密码信息(P)
组群(G)
选择用户将加入的组群：
uucp
video
wbpriv
webalizer
wheel
wireshark
zhangsan
主组群：
zhangsan
取消(C)
确定(O)

图8-8 “组群”选项卡

4. 删除用户账户

图8-9 “用户删除确认”对话框

8.1.4 字符界面下用户账户的设置

在Linux系统字符界面下创建、修改以及删除用户账户主要使用useradd，usermod和userdel这3个命令，其结果与使用“用户管理者”工具一样。

1. 创建用户账户

创建用户账户就是在系统中创建一个新账户，然后为新账户分配用户UID、用户组群、主目录和登录Shell等资源，新创建的用户账户默认是被锁定的，无法使用，需要使用passwd命令设置密码以后才能使用。

使用useradd命令可以在Linux系统下创建用户账户。

命令语法：

```
useradd  [-u uid [-o]][-g 组群名][-G组群名,...]
         [-d home][-s shell][-c comment]
         [-m [-k template]][-f inactive]
         [-e expire ][-p passwd][-M][-n][-r]
         [-l][用户名]
useradd  -D [-g 组群名][-b base][-s shell]
            [-f inactive][-e expire ]
```

【例8.1】 创建用户账户zhangsan并设置口令。

```
[root@PC-LINUX ~]# useradd zhangsan
[root@PC-LINUX ~]# cat /etc/passwd|grep zhangsan
zhangsan:x:1000:1000::/home/zhangsan:/bin/bash
//查看/etc/passwd文件，可以看到已经创建了用户zhangsan
[root@PC-LINUX ~]# passwd zhangsan
更改用户 zhangsan 的密码 。
新的 密码：                          //在此设置用户zhangsan的口令
重新输入新的 密码：                  //重复设置用户zhangsan的口令
passwd：所有的身份验证令牌已经成功更新。
```

【例8.2】 对用户账户设置口令和不设置口令的比较。

```
[root@PC-LINUX ~]# useradd lisi
[root@PC-LINUX ~]# useradd wangwu
//创建用户lisi和wangwu
[root@PC-LINUX ~]# passwd wangwu
更改用户 wangwu 的密码 。
新的 密码：                          //在此设置用户wangwu的口令
重新输入新的 密码：                  //重复设置用户wangwu的口令
[root@PC-LINUX ~]# cat /etc/passwd|grep lisi
lisi:x:1001:1001::/home/lisi:/bin/bash
[root@PC-LINUX ~]# cat /etc/shadow|grep lisi
lisi:!!:15493:0:99999:7:::
```

//查看/etc/shadow文件，可以看到在用户lisi的口令字段上显示的是“!!”，表示该用户还没有设置口令，不能直接登录到Linux系统

```
[root@PC-LINUX ~]# cat /etc/passwd|grep wangwu
wangwu:x:1002:1002::/home/wangwu:/bin/bash
[root@PC-LINUX ~]# cat /etc/shadow|grep wangwu
wangwu:$6$KiAI6cI.$p/kEL0heCQBGdEH6/XoSh30Utke6Tx8IJAtVKiBnM1oDIQlwp.JciW1limKz1NmVKP7.0BZ9pF1LcfEzxprpk1:15493:0:99999:7:::
```

//查看/etc/shadow文件，可以看到在用户wangwu的口令字段上显示的是加密的口令，表示该用户已经设置口令，能直接登录到Linux系统

【例8.3】 创建用户moon，并设置该用户UID为1510。

```
[root@PC-LINUX ~]# useradd -u 1510 moon
[root@PC-LINUX ~]# cat /etc/passwd|grep moon
moon:x:1510:1004::/home/moon:/bin/bash
//查看/etc/passwd文件，可以看到用户moon的UID是1510
```

【例8.4】 创建用户newuser，并设置该用户主目录为/home/www。

```
[root@PC-LINUX ~]# useradd -d /home/www newuser
[root@PC-LINUX ~]# cat /etc/passwd|grep newuser
newuser:x:1003:1003::/home/www:/bin/bash
//查看/etc/passwd文件，可以看到用户newuser的主目录是/home/www
[root@PC-LINUX ~]# ls -l /home
总用量 20
drwx------. 4 lisi     lisi     4096 6月   3 05:42 lisi
drwx------. 4 moon     moon     4096 6月   3 05:51 moon
drwx------. 4 wangwu   wangwu   4096 6月   3 05:42 wangwu
drwx------. 4 newuser  newuser  4096 6月   3 05:49 www
drwx------. 4 zhangsan zhangsan 4096 6月   3 05:39 zhangsan
//用户newuser的主目录/home/www在创建用户时已经创建了
```

【例8.5】 创建用户pp，并指定该用户是属于组群root的成员。

```
[root@PC-LINUX ~]# useradd -g root pp
[root@PC-LINUX ~]# cat /etc/passwd|grep pp
pp:x:1004:0::/home/pp:/bin/bash
//查看/etc/passwd文件，可以看到pp用户GID字段为0，0为root组群的GID
[root@PC-LINUX ~]# id pp
uid=1004(pp) gid=0(root) 组=0(root)
//使用id命令，可以看到用户pp的主要组群是root
```

【例8.6】 创建用户abc，并设置该用户的Shell类型是/bin/ksh。

```
[root@PC-LINUX ~]# useradd -s /bin/ksh abc
[root@PC-LINUX ~]# cat /etc/passwd|grep abc
abc:x:1005:1005::/home/abc:/bin/ksh
//查看/etc/passwd文件，可以看到用户abc的Shell类型是/bin/ksh
```

2. 修改用户账户

使用usermod命令能更改用户的Shell类型、所属的用户组群、用户口令的有效期，还能更改用户的登录名。

命令语法：

```
usermod [-u uid [-o]][-g 组群名]
        [-G 组群名,...]
        [-d 主目录 [-m]] [-s shell]
        [-c 注释][-l 新登录名]
        [-f 失效日][-e 过期日][-p 密码]
        [-L|-U][用户名]
```

【例8.7】 修改用户zhangsan的主目录为/home/kkk，并手动创建/home/kkk目录。

```
[root@PC-LINUX ~]# usermod -d /home/kkk zhangsan
[root@PC-LINUX ~]# cat /etc/passwd|grep zhangsan
zhangsan:x:1000:1000::/home/kkk:/bin/bash
//查看/etc/passwd文件，可以看到用户zhangsan的主目录已经更改为/home/kkk
[root@PC-LINUX ~]# mkdir /home/kkk
//必须使用mkdir命令创建/home/kkk目录，这样用户zhangsan才能使用该主目录
```

【例8.8】 修改用户wangwu的主目录为/home/opop，并自动创建/home/opop目录。

```
[root@PC-LINUX ~]# ls /home
abc  kkk  lisi  moon  pp  wangwu  www  zhangsan
[root@PC-LINUX ~]# cat /etc/passwd|grep wangwu
wangwu:x:1002:1002::/home/wangwu:/bin/bash
//查看/home目录和/etc/passwd文件内容，可以看到用户wangwu的当前主目录是/home/wangwu
[root@PC-LINUX ~]# usermod -d /home/opop -m wangwu
[root@PC-LINUX ~]# ls /home
abc  kkk  lisi  moon  opop  pp  www  zhangsan
[root@PC-LINUX ~]# cat /etc/passwd|grep wangwu
wangwu:x:1002:1002::/home/opop:/bin/bash
//查看/home目录和/etc/passwd文件内容，可以看到用户wangwu的主目录自动由/home/wangwu改为/home/opop
```

【例8.9】 修改用户wangwu的登录名为zhaoliu。

```
[root@PC-LINUX ~]# usermod -l zhaoliu wangwu
[root@PC-LINUX ~]# cat /etc/passwd|grep zhaoliu
zhaoliu:x:1002:1002::/home/opop:/bin/bash
```

//查看/etc/paswd文件，可以看到用户wangwu的新登录名为zhaoliu

【例8.10】 修改用户zhangsan的用户名全称为张三。

```
[root@PC-LINUX ~]# usermod -c 张三 zhangsan
[root@PC-LINUX ~]# cat /etc/passwd|grep zhangsan
zhangsan:x:1000:1000:张三:/home/kkk:/bin/bash
```

//查看/etc/passwd文件，可以看到用户zhangsan的用户名全称为张三

【例8.11】 修改用户zhangsan在口令过期后20天就禁用该账户。

```
[root@PC-LINUX ~]# cat /etc/shadow|grep zhangsan
zhangsan:$6$faBBno4V$YqUY.YiJV1O4lyu4TXGGt/ikooQlgmnuPdJDVn
YvyPNRD4CZWcEL0Du7aG71igJhWF5QhXumJgcXYSNzPwvc2/:15493
:0:99999:7:::
//用户zhangsan在口令过期后几天禁用该账户默认是没有设置的
[root@PC-LINUX ~]# usermod -f 20 zhangsan
[root@PC-LINUX ~]# cat /etc/shadow|grep zhangsan
zhangsan:$6$faBBno4V$YqUY.YiJV1O4lyu4TXGGt/ikooQlgmnuPdJDVn
YvyPNRD4CZWcEL0Du7aG71igJhWF5QhXumJgcXYSNzPwvc2/:15493
:0:99999:7:20::
//查看/etc/passwd文件，可以看到用户zhangsan将在口令过期后20天就禁
用该账户
```

【例8.12】 修改用户sun所属的组群为root，该组群必须事先存在。

```
[root@PC-LINUX ～]# usermod -g root sun
[root@PC-LINUX ～]# cat /etc/passwd|grep sun
sun:x:1050:0:太阳:/home/sun:/bin/bash
```

//查看/etc/passwd文件，可以看到用户sun所属的组群是root，组群root的GID是0

【例8.13】 锁住用户zhangsan口令，使口令无效。

```
[root@PC-LINUX ~]# usermod -L zhangsan
[root@PC-LINUX ~]# passwd -S zhangsan
zhangsan LK 2012-06-02 0 99999 7 20 (密码已被锁定。)
```

//查看用户zhangsan口令状态，可以看到该用户口令已经锁住，该用户不能在系统上登录，但是却可以从其他用户账户切换到该账户

【例8.14】 解除用户zhangsan口令锁住。

```
[root@PC-LINUX ~]# usermod -U zhangsan
[root@PC-LINUX ~]# passwd -S zhangsan
zhangsan PS 2012-06-02 0 99999 7 20 (密码已设置，使用 SHA512 算法。)
```

//查看用户zhangsan口令状态，可以看到该用户口令已经解锁

【例8.15】 修改用户zhangsan账户的过期日期是2012年12月12号。

```
[root@PC-LINUX ~]# cat /etc/shadow|grep zhangsan
zhangsan:$6$faBBno4V$YqUY.YiJV1O4lyu4TXGGt/ikooQlgmnuPdJDVn
YvyPNRD4CZWcEL0Du7aG71igJhWF5QhXumJgcXYSNzPwvc2/:15493:
0:99999:7:20::
[root@PC-LINUX ~]# usermod -e 12/12/2012 zhangsan
[root@PC-LINUX ~]# cat /etc/shadow|grep zhangsan
zhangsan:$6$faBBno4V$YqUY.YiJV1O4lyu4TXGGt/ikooQlgmnuPdJDVn
YvyPNRD4CZWcEL0Du7aG71igJhWF5QhXumJgcXYSNzPwvc2/:15493:
0:99999:7:20:15686:
```

//查看/etc/shadow文件，可以看到用户zhangsan的账户过期日期已经更改

【例8.16】 修改用户zhangsan的Shell类型为/bin/ksh。

```
[root@PC-LINUX ~]# cat /etc/passwd|grep zhangsan
zhangsan:x:1000:1000:张三:/home/kkk:/bin/bash
[root@PC-LINUX ~]# usermod -s /bin/ksh zhangsan
[root@PC-LINUX ~]# cat /etc/passwd|grep zhangsan
zhangsan:x:1000:1000:张三:/home/kkk:/bin/ksh
//查看/etc/shadow文件，可以看到用户zhangsan的Shell类型已经更改为/bin/ksh
```

3. 删除用户账户

使用userdel命令可以在Linux系统下删除用户账户。

命令语法：

userdel [-r][用户名]

【例8.17】 删除用户lisi。

```
[root@PC-LINUX ~]# userdel lisi
[root@PC-LINUX ~]# cat /etc/passwd|grep lisi
```

//查看/etc/passwd文件，已经查询不到关于用户lisi的数据，说明该账户已经删除

```
[root@PC-LINUX ~]# ls /home/
abc  kkk  lisi  moon  opop  pp  www  zhangsan
```

//使用userdel命令删除用户账户并不会删除该用户主目录

【例8.18】 删除用户moon，并且在删除该用户的同时一起删除主目录。

```
[root@PC-LINUX ~]# ls /home
abc  kkk  lisi  moon  opop  pp  www  zhangsan
```

//用户moon的主目录为/home/moon

```
[root@PC-LINUX ~]# userdel -r moon
[root@PC-LINUX ~]# ls /home
abc  kkk  lisi  opop  pp  www  zhangsan
```

//查看/home目录的内容，可以看到用户moon的主目录随该用户一起删除了

8.2 组群账户管理

本节主要讲述Linux系统下与组群账户有关的配置文件/etc/group和/etc/gshadow以及如何使用“用户管理者”和字符命令管理组群账户。

8.2.1 Linux组群账户配置文件

具有某种共同特征的用户集合就是用户组群，用户组群配置文件主要有/etc/group和/etc/gshadow，其中/etc/gshadow是/etc/group的加密信息文件。

1. /etc/group文件

/etc/group文件是用户组群的配置文件，内容包括用户和用户组群，并且能显示出用户是归属哪个用户组群或哪几个用户组群。

（1）/etc/group文件内容

/etc/group文件的内容包括用户组群名、用户组群口令、GID及该用户组群所包含的用户，每个用户组群都有一条记录。一行有4个段位，每个段位用“:”分隔，下面是/etc/group文件的部分内容。

zhangsan:x:1000:

表8-3　/etc/group文件各字段的含义

字　　段	含　　义
组群名	用户组群名称，如组群名root
组群口令	存放加密的密码，在上面示例中我们看到的是一个x，其实口令已被映射到/etc/gshadow 文件中
组群标识号	在系统内用一个整数标识组群GID，每个组群的GID都是唯一的，默认普通组群的GID从1000开始，如root组群GID是0
组群成员	属于这个组群的成员，如root组群的成员有root用户

（2）组群GID的概述

组群GID和UID类似，是一个从0开始的正整数，GID为0的组群是root组群。

Fedora 17系统会预留1000个GID号给系统虚拟用户组群使用，创建的新组群GID是从1000开始的。

2. /etc/gshadow文件

/etc/gshadow文件是/etc/group的加密文件，比如用户组群管理口令就是存放在这个文件中。这两个文件是对应互补的。/etc/gshadow文件中每个用户组群都有一条记录。一行有4个段位，每个段位之间用“:”分隔。

shanghai:!!::

beijing:6E/xvWMmh$rhYLQwwffEqIudVLFzMlv1::ou

表8-4　/etc/gshadow文件各字段的含义

字　　段	含　　义
组群名	组群的名称
组群口令	口令已经加密，如果有些组群在这里显示的是“!”，表示这个组群没有口令。上面示例中组群**shanghai**没有口令，组群**beijing**已设置口令
组群管理者	组群的管理者，有权在该组群中添加、删除用户
组群成员	属于该组群的用户成员列表，如有多个用户用“，”分隔。上面示例中**beijing**组群的成员是**ou**

8.2.2 图形界面下组群账户的设置

1. 创建组群账户

图8-10 “添加新组群”对话框

2. 修改组群账户属性

图8-11 “组群数据”选项卡

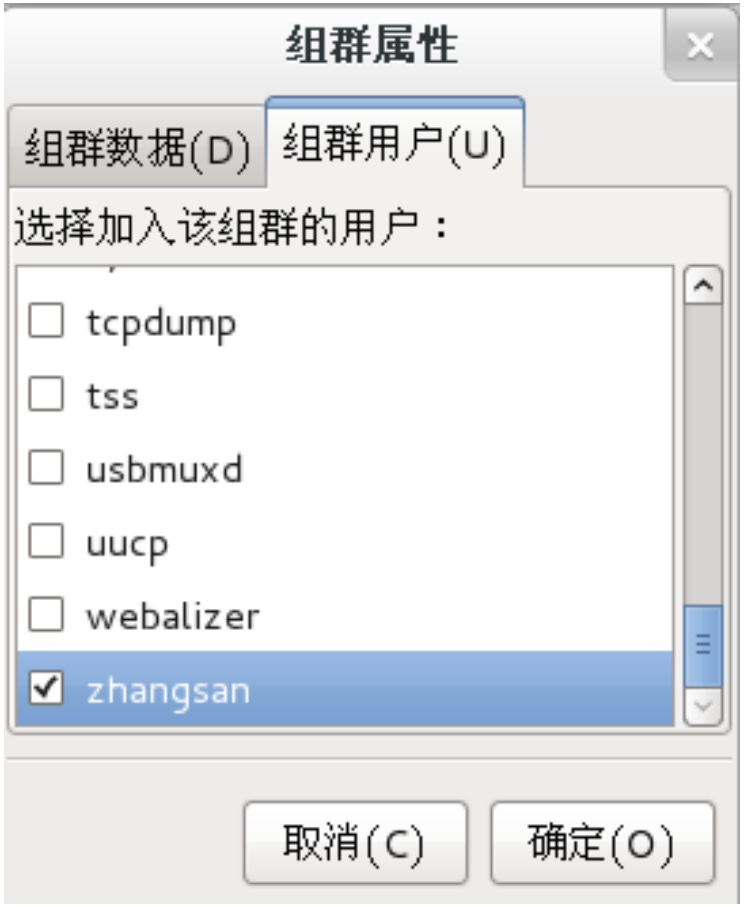

图8-12　“组群用户”选项卡

3. 删除组群账户

如果某个用户账户的主组群是该组群时，不能删除该组群。

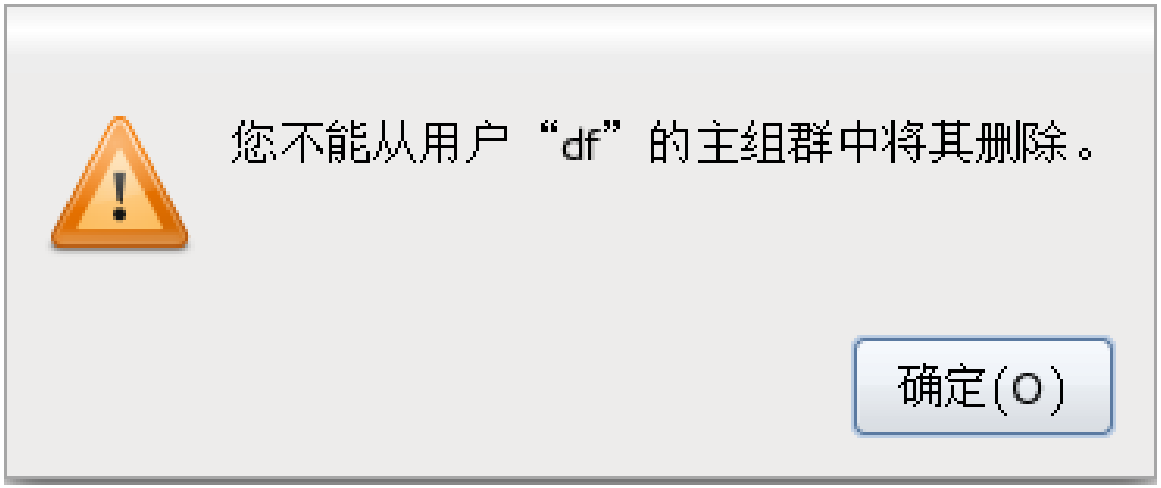

图8-13　“无法删除组群”对话框

当没有任何用户账户的主组群是该组群时，能删除该组群。

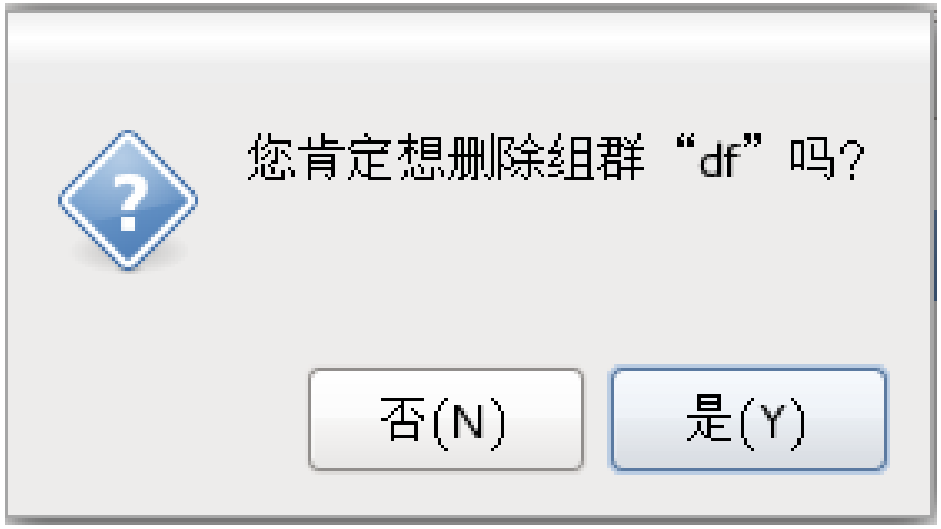

图8-14　“删除组群确认”对话框

8.2.3 字符界面下组群账户的设置

在Linux系统字符界面下创建、修改以及删除组群账户主要使用groupadd，groupmod和groupdel这3个命令，其结果与使用“用户管理者”工具一样。

1. 创建组群账户

使用groupadd命令可以在Linux系统下创建组群账户。

命令语法：

groupadd [-g gid [-o]] [-f] [组群名]

【例8.19】 创建名为china的组群。

```
[root@PC-LINUX ~]# groupadd china
[root@PC-LINUX ~]# cat /etc/group|grep china
china:x:1006:
```

//查看文件/etc/group，可以看到已经创建了组群china，组群GID是1006

【例8.20】 创建名为ou的组群，并且设置该组群GID为1800。

```
[root@PC-LINUX ~]# groupadd -g 1800 ou
[root@PC-LINUX ~]# cat /etc/group|grep ou
ou:x:1800:
```

//查看文件/etc/group，可以看到已经创建了组群ou，组群GID是1800

【例8.21】 创建名为chinese的系统组群。

```
[root@PC-LINUX ~]# groupadd -r chinese
[root@PC-LINUX ~]# cat /etc/group|grep chinese
chinese:x:982:
```

//查看/etc/group文件，可以看到系统组群chinese的GID是982，是小于1000的

2. 修改组群账户

使用groupmod命令可以在Linux系统下修改组群账户，如组群名称、GID等。

命令语法：

groupmod [-g <组群识别码> <-o>]
[-n <新组群名称>][组群名称]

【例8.22】 将组群ou的GID修改为1900。

```
[root@PC-LINUX ~]# groupmod -g 1900 ou
[root@PC-LINUX ~]# cat /etc/group|grep ou
ou:x:1900:
```

//查看文件/etc/group，可以看到组群ou的GID已经更改为1900

【例8.23】 修改组群ou的新组群名称为shanghai。

```
[root@PC-LINUX ~]# groupmod -n shanghai ou
[root@PC-LINUX ~]# cat /etc/group|grep shanghai
shanghai:x:1900:
```

//查看/etc/group文件，可以通过原来的GID看到组群ou的名称已经更改为shanghai

3. 删除组群账户

使用groupdel命令可以在Linux系统下删除组群账户。

命令语法：

groupdel [组群名称]

【例8.24】 删除组群shanghai。

```
[root@PC-LINUX ~]# groupdel shanghai
[root@PC-LINUX ~]# cat /etc/group|grep shanghai
```

//查看/etc/group文件，可以看到当前组群shanghai已经不存在

8.3 账户相关文件或目录

在创建、修改和删除账户时，涉及到众多的相关文件和目录，如/etc/skel目录、/etc/login.defs文件和/etc/default/useradd文件。下面分别进行介绍。

8.3.1 /etc/skel目录

/etc/skel目录是存放用户启动文件的目录，这个目录由root用户管理，当管理员创建新用户时，这个目录下的文件会自动复制到新创建的用户的主目录下。

/etc/skel目录下的文件都是隐藏文件，也就是类似“.file”格式的，可以通过添加、修改和删除/etc/skel目录下的文件，来为用户提供一个统一、标准和默认的用户环境。

8.3.2 /etc/login.defs配置文件

/etc/login.defs文件规定了创建新用户时的一些默认设置，比如创建用户时是否需要主目录、UID和GID的范围、用户账户口令的期限等，这个文件可以通过root用户来修改。

8.3.3 /etc/default/useradd文件

/etc/default/useradd文件是在使用useradd命令创建用户账户时的规则文件。

8.4 用户和组群维护命令

在日常工作中经常需要对Linux系统用户和组群账户进行维护和管理，下面就介绍这些维护命令。

8.4.1 账户维护命令

在平时的工作中对账户进行维护主要用到passwd，gpasswd，chfn，chsh，su，pwck以及newgrp等众多命令。

1. passwd命令

使用passwd命令可以设置或修改用户的口令，普通用户和超级权限用户都可以运行passwd。普通用户只能更改自己的用户口令，root用户可以设置或修改任何用户的口令。如果passwd命令后面不接任何选项或用户名，则表示修改当前用户的口令。

命令语法：

passwd [选项] [用户名]

【例8.25】 设置用户it的口令。

```
[root@PC-LINUX ~]# passwd it
更改用户 it 的密码 。
新的 密码：                          //在此输入用户it的口令
重新输入新的 密码：                    //在此重复输入用户it的口令
passwd：所有的身份验证令牌已经成功更新。
```

【例8.26】 设置当前用户的口令。

```
[root@PC-LINUX ~]# passwd
更改用户 root 的密码 。
新的 密码：                          //在此输入当前用户的口令
重新输入新的 密码：                    //再次输入当前用户的口令
passwd：所有的身份验证令牌已经成功更新。
```

【例8.27】 锁住用户it的口令。

```
[root@PC-LINUX ~]# passwd -l it
锁定用户 it 的密码 。
passwd: 操作成功
//用户it锁住以后不能登录到系统，但是可以用su命令从其他用户切换到用户it
[root@PC-LINUX ~]# passwd -S it
it LK 2012-06-02 0 99999 7 -1 (密码已被锁定。)
//查看用户口令状态，可以看到用户it的口令是锁住的
[root@PC-LINUX ~]# cat /etc/shadow|grep it
it:!!$6$/4sUM8yo$pRRuww3238PwFCv2o3T7JWMjAN0FA.zkGzhUBWshHCK0DX2k1udSXa9w8Y.HQ1hjcvG8laKrmFHGjYZfNZmYm1:15493:0:99999:7:::
//查看/etc/shadow文件，可以看到用户it口令锁住以后在口令字段前有“!!”
```

【例8.28】 解锁用户it口令。

```
[root@PC-LINUX ~]# passwd -u it
解锁用户 it 的密码。
passwd: 操作成功
//已经成功解锁用户it，重新设置用户口令也可以解锁用户
[root@PC-LINUX ~]# passwd -S it
it PS 2012-06-02 0 99999 7 -1 (密码已设置，使用 SHA512 算法。)
//查看用户口令状态，可以看到用户it的口令已经解锁
[root@PC-LINUX ~]# cat /etc/shadow|grep it
it:$6$/4sUM8yo$pRRuww3238PwFCv2o3T7JWMjAN0FA.zkGzhUBWsh
HCK0DX2k1udSXa9w8Y.HQ1hjcvG8laKrmFHGjYZfNZmYm1:15493:0:9
9999:7:::
//查看/etc/shadow文件，可以看到用户it口令解锁以后口令字段前的“!!”
没有了
```

【例8.29】 删除用户it的口令。

```
 [root@PC-LINUX ~]# cat /etc/shadow|grep it
rtkit:!!:15493::::::
it:$6$/4sUM8yo$pRRuww3238PwFCv2o3T7JWMjAN0FA.zkGzhUBWshHCK0DX2k1udSXa9w8Y.HQ1hjcvG8laKrmFHGjYZfNZmYm1:15493:0:99999:7:::
//查看/etc/shadow文件，可以看到用户it设置过口令
[root@PC-LINUX ~]# passwd -d it
清除用户的密码 it。
passwd: 操作成功
[root@PC-LINUX ~]# cat /etc/shadow|grep it
it::15493:0:99999:7:::
//查看/etc/shadow文件，可以看到用户it的口令已经没有了
```

2. gpasswd

使用gpasswd命令可以设置一个组群的组群密码，或是在组群中添加、删除用户。

命令语法：

gpasswd [-r|-R][组群名]

gpasswd [选项][用户名][组群名]

【例8.30】 把用户it添加到kk组群中。

```
[root@PC-LINUX ~]# gpasswd -a it kk
Adding user it to group kk
[root@PC-LINUX ~]# cat /etc/group|grep kk
kk:x:1002:it
//在/etc/group文件中可以看到kk组群中有用户it
```

【例8.31】 从kk组群中删除用户it。

```
[root@PC-LINUX ~]# gpasswd -d it kk
Removing user it from group kk
[root@PC-LINUX ~]# cat /etc/group|grep kk
kk:x:1002:
//在/etc/group文件中可以看到kk组群中已经没有用户it了
```

【例8.32】 设置kk组群的口令。

```
[root@PC-LINUX ~]# gpasswd kk
Changing the password for group kk
New Password:                    //在此输入组群kk的口令
Re-enter new password:           //在此重复输入组群kk的口令
[root@PC-LINUX ~]# cat /etc/gshadow|grep kk
kk:$6$LyMEB/59ARw/CdN$Gw8ln2/Vi3vUhzdCvbNInSioUDNcUOWpDuk
bMIeuGq8hjWWnVJWaa6BlFzYa6wdvuBkaVK7Cwkbmq0Vd8./0t1::
//在/etc/gshadow文件中可以看到组群kk已经设置口令
```

【例8.33】 取消kk组群密码。

```
[root@PC-LINUX ~]# gpasswd -r kk
[root@PC-LINUX ~]# cat /etc/gshadow|grep kk
kk:::
//在/etc/gshadow文件中可以看到组群kk已经不存在了
```

3. chfn命令

使用chfn命令可以更改用户全名、办公室地址、电话等信息。

命令语法：

chfn [-f full-name] [-o office] [-p office-phone] [-h home-phone] [-u] [-v] [用户名]

【例8.34】 更改用户newuser的信息。

```
[root@PC-LINUX ~]# chfn newuser
Changing finger information for newuser.
Name []: 新用户
Office []: 人事部
Office Phone []: 12345678
Home Phone []: 11223344

Finger information changed.
//在交互式界面上输入用户newuser的信息
[root@PC-LINUX ~]# cat /etc/passwd|grep newuser
newuser:x:1003:1003:新用户,人事部,12345678,11223344
:/home/www:/bin/bash
//查看/etc/passwd文件，可以看到用户newuser的信息
```

【例8.35】 设置用户it的办公地址是财务室。

```
[root@PC-LINUX ~]#chfn -o 财务室 it
Changing finger information for it.
Finger information changed.
[[root@PC-LINUX ~]# cat /etc/passwd|grep it
it:x:1020:1020:,财务室:/home/it:/bin/bash
//查看/etc/passwd文件，可以看到用户it的办公地址是财务室
```

【例8.36】 设置用户it的用户名全称为挨梯。

```
[root@PC-LINUX ～]# chfn -f 挨梯 it
Changing finger information for it.
Finger information changed.
[root@PC-LINUX ～]# cat /etc/passwd|grep it
it:x:1020:1020:挨梯,财务室:/home/it:/bin/bash
//查看/etc/passwd文件，可以看到用户it的用户名全称为挨梯
```

4. chsh命令

使用chsh命令可以更改用户账户的Shell类型。

命令语法：

chsh [-s Shell类型][-l][用户名]

【例8.37】 列出当前系统中所有支持的Shell类型。

```
[root@PC-LINUX ~]# chsh -l
/bin/sh
/bin/bash
/sbin/nologin
/bin/tcsh
/bin/csh
/bin/zsh
//列出Fedora 17系统上支持的所有Shell类型
```

【例8.38】 更改用户wangwu所用的Shell类型为/bin/sh。

```
[root@PC-LINUX ～]# chsh -s /bin/sh wangwu
Changing shell for wangwu.
Shell changed.
[root@PC-LINUX ～]# cat /etc/passwd|grep wangwu
wangwu:x:1002:1002::/home/wangwu:/bin/sh
//查看/etc/passwd文件，可以看到用户wangwu的Shell类型已经更改为
/bin/sh
```

【例8.39】 更改当前用户wangwu的Shell类型为/bin/bash。

```
[root@PC-LINUX ～]# chsh wangwu
Changing shell for wangwu.
New shell [/bin/sh]: /bin/bash                    //在此输入Shell类型，比如/bin/bash
Shell changed.
```

5. su命令

使用su命令可以切换到其他用户账户进行登录。

命令语法：

su［选项］［用户］

【例8.40】 从用户root切换到用户it登录系统。

```
[root@PC-LINUX ~]# su - it
[it@PC-LINUX ~]$
//从用户root切换到普通用户不需要输入用户it的口令
```

【例8.41】 从用户it切换到用户root登录系统。

```
[it@PC-LINUX ~]$ su root
口令：                                    //在此输入用户root的口令
[root@PC-LINUX ~]#
//从普通用户切换到root用户需要输入root用户的口令
```

6. pwck命令

使用pwck命令可以校验用户配置文件/etc/passwd 和/etc/shadow内容是否合法和完整。

命令语法：

pwck

【例8.42】检验用户配置文件/etc/passwd和/etc/shadow文件内容是否合法和完整。

[root@PC-LINUX ～]# rm -rf /home/it

//删除用户it的主目录/home/it

[root@PC-LINUX ～]# pwck

user adm：directory /var/adm does not exist

user uucp：directory /var/spool/uucp does not exist

user gopher：directory /var/gopher does not exist

user it：directory /home/it does not exist

pwck：无改变

//可以看到用户it的主目录/home/it不存在

7. newgrp命令

使用newgrp命令可以让用户账户以另一个组群的身份进行登录。

命令语法：

newgrp［组群名］

【例8.43】 将用户ab以组群ou的身份登录系统。

```
[ab@PC-LINUX root]$ id
uid=1008(ab) gid=1005(ab) 组=1005(ab),1006(ou)
//当前用户ab分别属于组群ab和ou的成员，是以ab组群的身份登录系统的
[ab@PC-LINUX root]$ newgrp ou
[ab@PC-LINUX root]$ id
uid=1008(ab) gid=1006(ou) 组=1006(ab),1005(ou)
//现在用户ab是以ou组群的身份登录系统
```

8.4.2 账户信息显示

在平时的工作中要显示账户的信息主要用到finger，groups，id，w以及who等众多命令。

1. finger命令

使用finger命令可以显示用户账户的信息。

命令语法：

finger [选项][用户名]

【例8.44】 显示所有用户的登录信息。

```
[root@PC-LINUX ~]# finger
Login    Name        Tty      Idle  Login Time   Office     Office Phone   Host
newuser  新用户      pts/0           May 30 13:27 人事部     12345678
(192.168.0.200)
root     root        *:0             May 30 08:34                        (:0)
root     root        pts/1           May 30 09:11                        (192.168.0.200)
```

【例8.45】 显示用户newuser的信息。

```
[root@PC-LINUX ~]#finger newuser
Login: newuser                          Name: 新用户
Directory: /home/www                    Shell: /bin/bash
Office: 人事部, 12345678                Home Phone: 11223344
Never logged in.
No mail.
No Plan.
```

//从结果信息可以看出用户newuser的办公地址是人事部，用户名全称是新用户，Shell类型是/bin/bash，主目录是/home/www

2. groups 命令

使用groups命令可以显示指定用户账户的组群成员身份。

命令语法：

groups [用户名]

【例8.46】 查看用户ab是属于哪些组群的成员。

```
[root@PC-LINUX ~]# groups ab
ab : ab ou
//可以看到用户ab是属于ab组群和ou组群的用户
```

3. id命令

使用id命令可以显示用户的ID以及该用户所属组群的GID。

命令语法：

id [选项][用户名]

【例8.47】 查询用户ab的UID、GID 以及归属组群的情况。

```
[root@PC-LINUX ～]# id ab
uid=1008(ab) gid=1005(ab) 组=1005(ab),1006(ou)
```

//用户ab的UID是1008，默认组群是ab，默认用户组群的GID是1005，归属于ab和ou组群

【例8.48】 显示用户ab所属主组群的GID。

```
[root@PC-LINUX ～]# id -g ab
1005
```

//可以看到用户ab所属主组群的GID是1005

【例8.49】 显示用户ab所属组群的GID。

```
[root@PC-LINUX ～]# id -G ab
1005 1006
```

//可以看到用户ab所属组群的GID是1005和1006

【例8.50】 显示用户ab的UID。

```
[root@PC-LINUX ～]# id -u ab
1008
```

//可以看到用户ab的UID是1008

4. w命令

使用w命令可以详细查询已登录当前计算机的用户。

命令语法：

w

【例8.51】 显示已登录当前计算机的用户详细信息。

```
[root@PC-LINUX ~]# w
 13:08:30 up  4:40,  2 users,  load average: 3.17, 0.87, 0.36
USER     TTY      FROM              LOGIN@   IDLE   JCPU   PCPU WHAT
root     :0       :0                08:34   ?xdm?   4:13   0.84s gdm-session-wor
root     pts/1    192.168.0.200     09:11    0.00s  2.80s  0.44s w
//显示已登录当前计算机的用户root详细信息
```

5. who命令

使用who命令可以显示已登录当前计算机用户的简单信息。

命令语法：

who [-Himqsw] [--version][am i][记录文件]

【例8.52】 显示已登录当前计算机用户的简单信息。

```
[root@PC-LINUX ~]# who
root     :0           2013-05-30 08:34 (:0)
root     pts/1        2013-05-30 09:11 (192.168.0.200)
//显示已登录当前计算机的用户root的简单信息
```

8.5 实现账户安全

在Linux系统中可以使用chage命令管理用户口令的时效，防止用户口令由于长时间使用而导致泄漏，或是被黑客破解口令而受到攻击。

命令语法：

chage [选项][用户名]

表8-5　　chage命令选项含义

含　义	选　项	描　述
两次改变密码之间相距的最小天数	-m days	指定用户必须改变口令所间隔的最少天数。如果值为0，口令码就不会过期
两次改变密码之间相距的最大天数	-M days	指定口令有效的最多天数。当该选项指定的天数加上“-d”选项指定的天数小于当前的日期，用户在使用该账户前就必须改变口令
最近一次密码修改时间	-d days	指定自从1970年1月1日起，口令被改变的天数
密码失效时间	-I days	指定口令过期后，账户被锁前不活跃的天数。如果值为0，账户在口令过期后就不会被锁
账户过期时间	-E date	指定账户被锁的日期，日期格式为YYYY-MM-DD。若不用日期，也可以使用自1970年1月1日后经过的天数
在密码过期之前警告的天数	-W days	指定口令过期前要警告用户的天数

【例8.53】 设置用户shanghai两次改变密码之间相距的最小天数为2天。

```
[root@PC-LINUX ~]# cat /etc/shadow|grep shanghai
shanghai:$6$4BPUKYr9$VFFar9mJgn10Uim3BX1sjfauL2duGa36mdI4
BoowWM63wtk.q9CbGXGbJhUA7ocCuv18GlWX2F8bHuUH0oNZC.:15
493:0:99999:7:::
[root@PC-LINUX ~]# chage -m 2 shanghai
[root@PC-LINUX ~]# cat /etc/shadow|grep shanghai
shanghai:$6$4BPUKYr9$VFFar9mJgn10Uim3BX1sjfauL2duGa36mdI4
BoowWM63wtk.q9CbGXGbJhUA7ocCuv18GlWX2F8bHuUH0oNZC.:15
493:2:99999:7:::
```

【例**8.54**】 设置用户**shanghai**两次改变密码之间相距的最大天数为**10**天。

```
[root@PC-LINUX ~]# chage -M 10 shanghai
[root@PC-LINUX ~]# cat /etc/shadow|grep shanghai
shanghai:$6$4BPUKYr9$VFFar9mJgn10Uim3BX1sjfauL2duGa36mdI4BowWM63wtk.q9CbGXGbJhUA7ocCuv18GIWX2F8bHuUH0oNZC.:15493:2:10:7:::
```

【例**8.55**】 设置用户**shanghai**在密码过期之前警告的天数为**1**天。

```
[root@PC-LINUX ~]# chage -W 1 shanghai
[root@PC-LINUX ~]# cat /etc/shadow|grep shanghai
shanghai:$6$4BPUKYr9$VFFar9mJgn10Uim3BX1sjfauL2duGa36mdI4BowWM63wtk.q9CbGXGbJhUA7ocCuv18GIWX2F8bHuUH0oNZC.:15493:2:10:1:::
```

【例8.56】 设置用户**shanghai**密码失效时间为**10**天。

```
[root@PC-LINUX ~]# chage -I 10 shanghai
[root@PC-LINUX ~]# cat /etc/shadow|grep shanghai
shanghai:$6$4BPUKYr9$VFFar9mJgn10Uim3BX1sjfauL2duGa36mdI4B
oowWM63wtk.q9CbGXGbJhUA7ocCuv18GIWX2F8bHuUH0oNZC.:1549
3:2:10:1:10::
```

【例8.57】 设置用户**shanghai**账户过期时间为**2018-10-10**。

```
[root@PC-LINUX ~]# chage -E 2018-10-10 shanghai
[root@PC-LINUX ~]# cat /etc/shadow|grep shanghai
shanghai:$6$4BPUKYr9$VFFar9mJgn10Uim3BX1sjfauL2duGa36mdI4B
oowWM63wtk.q9CbGXGbJhUA7ocCuv18GIWX2F8bHuUH0oNZC.:1549
3:2:10:1:10:17814:
```

【例**8.58**】显示用户**shanghai**当前口令失效的信息。

```
[root@PC-LINUX ~]# chage -l shanghai
Last password change                    : Jun 02, 2012
Password expires                        : Jun 12, 2012
Password inactive                       : Jun 22, 2012
Account expires                         : Oct 10, 2018
Minimum number of days between password change          : 2
Maximum number of days between password change          : 10
Number of days of warning before password expires       : 1
```

【例**8.59**】用交互式的方式设置用户**beijing**的口令时效。

```
[root@PC-LINUX ~]# chage beijing
Changing the aging information for beijing
Enter the new value, or press ENTER for the default

Minimum Password Age [0]: 2
Maximum Password Age [99999]: 10
Last Password Change (YYYY-MM-DD) [2012-06-02]: 2018-02-04
Password Expiration Warning [7]: 1
Password Inactive [-1]: 10
Account Expiration Date (YYYY-MM-DD) [1969-12-31]: 2018-10-10
```

小　　结

用户在Linux系统中是分角色的，由于角色不同，每个用户的权限和所能完成的操作任务也不同。而在实际的管理工作中，用户的角色是通过UID（用户ID号）来标识的，每个用户的UID都是不同的。用户管理主要是通过修改用户配置文件/etc/passwd和/etc/shadow完成的，使用用户管理控制工具的最终目的也是为了修改用户配置文件。

小　　结

在Linux系统图形界面下管理员可以通过“用户管理者”创建、修改和删除用户账户。而在Linux系统字符界面下创建、修改以及删除用户账户主要使用useradd，usermod和userdel这3个命令，其结果与使用“用户管理者”工具一样。

小　　结

用户组群是指具有某种共同特征的用户集合，用户组群配置文件主有/etc/group和/etc/gshadow，其中/etc/gshadow文件是/etc/group文件的加密信息文件。

小　　结

在Linux系统图形界面下管理员可以通过“用户管理者”创建、修改和删除组群账户。而在Linux系统字符界面下创建、修改以及删除组群账户主要使用groupadd、groupmod和groupdel这3个命令，其结果与使用“用户管理者”工具一样。

小　　结

在创建、修改和删除账户时，涉及到众多的相关文件和目录。/etc/skel目录是存放用户启动文件的目录，这个目录由root用户管理，当管理员创建新用户时，这个目录下的文件会自动复制到新创建的用户的主目录下。/etc/login.defs文件规定了创建新用户时的一些默认设置，比如创建用户时是否需要主目录、UID和GID的范围、用户账户口令的期限等。/etc/default/useradd文件是在使用useradd命令创建用户账户时的规则文件。

小　　结

在平时的工作中对账户进行维护主要用到passwd，gpasswd，chfn，chsh，su，pwck以及newgrp等众多命令。要显示账户的信息主要用到finger，groups，id，w以及who等众多命令。

在Linux系统中可以使用chage命令管理用户口令的时效，防止用户口令由于长时间使用而导致泄漏，或是被黑客破解口令而受到攻击。