《Linux 操作系统》第四讲：

用户管理

学时计划：4 学时 理论，2 学时 实验

（实验四：用户管理）

教学大纲：

1、用户管理的基本概念

2、Linux 的用户与用户组

3、与用户管理有关的配置文件

4、用户管理

5、用户组管理

6、讨论与思考

Linux 操作系统是一个多用户多任务的操作系统，在用户管理方面，拥有用户添加、用户管理、用户组管理、用户切换等多种工具。

本讲介绍 Linux 操作系统下的用户管理的一些基本概念，并详细讲解用户和用户组管理的工具的使用。

一、用户管理的基本概念

1.1 单用户多任务和多用户多任务

Linux 是一个多用户、多任务的操作系统。操作系统可以分为单用户多任务和多用户多任务操作系统。

（1）单用户多任务

单用户多任务操作系统要求系统在单一时间内为单个用户服务，但它允许用户一次提交多项任务。例如，用户可以在运行程序的同时开始另一文档的编辑工作。

举例来说，用户 zhaodongfeng 登录 Linux 系统，进入系统后，首先打开 Netbeans 撰写程序，但在写程序的过程中，又打开 xmms 欣赏音乐，同时打开 QQ 软件和朋友保持联系。这样，用户同时打开了 3 个应用软件，这样的系统就是单用户多任务操作系统。

（2）多用户多任务

多用户多任务操作系统允许多个用户共享使用同一台计算机的资源，即在一台计算机上联接几台甚至几十台终端机，终端机可以没有自己的CPU与内存，只有键盘与显示器，每个用户都通过各自的终端机使用这台计算机的资源，计算机按固定的时间片轮流为各个终端服务。由于计算机的处理速度很快，用户感觉不到等待时间，似乎这台计算机专为自己服务一样。

当然，多用户多任务并不是必须许多用户同时通过多个终端设备来使用同一台计算机，多用户也可以通过远程登录的方式来进行。

举例来讲，一台Ubuntu Server服务器，服务器上开设有FTP用户、系统管理员、Web管理用户等，在同一时刻，这些用户可以在同一时刻访问服务器，并执行不同的任务。

1.2 用户角色识别

用户在操作系统中是分角色的，角色不同，权限和所能够完成的任务也不同。

在Linux操作系统中，用户角色是通过UID和用户名进行识别的，并且主要使用UID进行识别。

二、Linux的用户和用户组

2.1 用户（User）

用户是能够获取系统资源的权限的集合。Linux操作系统中，主要有三类用户，分别如下所示。

root用户：系统唯一的一个拥有最高权限的账户。

虚拟用户：也被称之为伪用户或假用户，与真实用户区分开来，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，主要用户FTP服务、NFS服务等公共服务的启动账户，这类用户通常都是系统自身拥有的，而非管理员自行添加的。

普通用户：是系统真实账户。这类用户能够登录操作系统，但只能操作个人目录下的内容。普通用户通常都是由系统管理员自行添加的并指定权限。

Linux 操作系统中，与用户有关的信息保存在/etc/passwd 和/etc/shadow这两个文件中。

2.2 用户组（Group）

用户组（group）就是具有相同特征的用户（user）的集合体，用户组是权限的容器。在 Linux 操作系统中，主要有三类用户组，分别如下所示。

普通用户组:通常是由系统管理员创建的，可以指定加入多个用户，加入的用户将继承用户组的权限。

系统用户组:该组内一般存放系统管理用户。

私有组：也称基本组。当创建用户时，如果没有为其指明所属用户组，则就为其定义一个私有的用户组，私有用户组得名称和用户名相同。私有组可以转变成普通用户组，当把其他用户加入到一个私有组中，私有组就转变成了普通用户组。

Linux 操作系统中，与用户组有关的信息保存在/etc/group 和/etc/gshadow 这两个文件中。

三、与用户管理有关的配置文件

Linux 操作系统中，与用户有关的信息保存在/etc/passwd 和/etc/shadow 这两个文件中，与用户组有关的信息保存在/etc/group 和/etc/gshadow 这两个文件中。

3.1/etc/passwd

（1）关于/etc/passwd

/etc/passwd 是系统识别用户的一个文件。不准确的讲，/etc/passwd 操作系统的花名册，系统所有的用户都在这里有记载。

当以 zhaodongfeng 账号登录时，系统首先查阅/etc/passwd 文件，判断是否有 zhaodongfeng 账号，然后确定帐号的 UID，之后通过 UID 来确认用户和身份。系统中如果存在 zhaodongfeng 账号，则读取/etc/shadow 文件中所对应的 zhaodongfeng 帐号的密码。如果密码核实无误则登录系统成功，并开始读取用户的配置文件。

（2）/etc/passwd 的详细说明

在/etc/passwd 中，每一行都表示的是一个用户的信息。每一行有 7 个段位，每个段位用:号分割。

查看系统的/etc/passwd 的文件内容，具体如下。

```
zhaodongfeng@TeachServer:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
syslog:x:101:103::/home/syslog:/bin/false
mysql:x:102:105:MySQL Server,,,:/nonexistent:/bin/false
sshd:x:103:65534::/var/run/sshd:/usr/sbin/nologin
zhaodongfeng:x:1000:1000:zhaodongfeng,,,:/home/zhaodongfeng:/bin/bash
ftp:x:104:112:ftp daemon,,,:/srv/ftp:/bin/false
snmp:x:105:114::/var/lib/snmp:/bin/false
zhaodongfeng@TeachServer:~$
```

说明如下：

第一字段：用户名（也被称为登录名）

第二字段：口令，具体内容是一个字母 x，其密码已被映射到/etc/shadow 文件中。

第三字段：UID。

第四字段：GID。

第五字段：用户名全称，这是可选的，可以不设置。

第六字段：用户个人目录所在位置。

第七字段：用户所用 SHELL 的类型。

（3）关于 UID

UID 是用户的 ID 值,在操作系统中每个用户的 UID 值是唯一的。确切的说每个用户都要对应一个唯一的 UID，UID 的唯一性关系到系

统的安全。系统管理员应该确保这一规则。

系统用户的UID的值从0开始，是一个正整数，至于最大值可以在/etc/login.defs可以查到，一般Linux发行版约定为60000。在Linux操作系统中，root的UID是0，拥有系统最高权限。

UID是确认用户权限的标识，用户登录系统所属的角色是通过UID来实现的,而非用户名,因此把几个用户共用一个UID是危险的。

UID的唯一性是需要管理员人为保障的，因为管理员可以通过修改/etc/passwd文件来修改任何用户的UID的值。通常情况下，Linux发行版都会预留一定的UID和GID给系统虚拟用户占用。例如,Fedora系统会把前499个UID和GID 预留,管理员自行添加新用户时的UID和GID从500开始。在Linux操作系统中,系统通过/etc/login.defs文件的UID_MIN选项指定UID和GID的最小值。

3.2/etc/shadow

（1）关于/etc/shadow

/etc/shadow文件是/etc/passwd 的影子文件，这个文件不是由/etc/passwd产生的。/etc/shadow和/etc/passwd是对应互补的。

/etc/shadow文件内容包括了用户名及被加密的密码以及其它在/etc/passwd中没有包括的用户信息。比如用户的有效期限、密码过期时间等。/etc/shadow文件的读取和修改需要root权限。

（2）/etc/shadow的详细说明

/etc/shadow 文件的内容包括9个段位，每个段位之间用:号分割。

查看系统的/etc/shadow的文件内容，具体如下。

```
zhaodongfeng@TeachServer:~$ sudo cat /etc/shadow
[sudo] password for zhaodongfeng:
root:!:15023:0:99999:7:::
daemon:*:15023:0:99999:7:::
bin:*:15023:0:99999:7:::
sys:*:15023:0:99999:7:::
sync:*:15023:0:99999:7:::
games:*:15023:0:99999:7:::
man:*:15023:0:99999:7:::
lp:*:15023:0:99999:7:::
mail:*:15023:0:99999:7:::
```

```
news:*:15023:0:99999:7:::
uucp:*:15023:0:99999:7:::
proxy:*:15023:0:99999:7:::
www-data:*:15023:0:99999:7:::
backup:*:15023:0:99999:7:::
list:*:15023:0:99999:7:::
irc:*:15023:0:99999:7:::
gnats:*:15023:0:99999:7:::
nobody:*:15023:0:99999:7:::
libuuid:!:15023:0:99999:7:::
syslog:*:15023:0:99999:7:::
mysql:!:15023:0:99999:7:::
sshd:*:15023:0:99999:7:::
zhaodongfeng:$6$UU0Eeci2$jOM4Ob76bGjbezGf7zqDSyAoFN68GCvjRUtcB9
wUUz7.wkPQo12NN8yubeh0Qhv4spkjKp2JIrHCRjXsj0AkZ0:15023:0:99999:7:::
ftp:*:15031:0:99999:7:::
snmp:*:15245:0:99999:7:::
zhaodongfeng@TeachServer:~$
```

说明如下。

第一字段：用户名（也被称为登录名），在/etc/shadow 中，用户名和/etc/passwd 是相同的，这样就把 passwd 和 shadow 中用的用户记录联系在一起，这个字段是非空的。

第二字段：密码（已被加密），如果是有些用户在这段是 x，表示这个用户不能登录到系统，这个字段是非空的。

第三字段：上次修改口令的时间。这个时间是从 1970 年 01 月 01 日算起到最近一次修改口令的时间间隔（天数）。

第四字段：两次修改口令间隔最少的天数，如果设置为 0，则表示禁用此功能。此项功能对于提高系统的安全性有重要的意义。其默认值是通过/etc/login.defs 文件的 PASS_MIN_DAYS 选项进行定义。

第五字段：两次修改口令间隔最多的天数，也就是所谓的口令有效期。此功能增强了操作系统用户管理口令的时效性，对于提高系统的安全性有重要的意义。其默认值是通过/etc/login.defs 文件的 PASS_MAX_DAYS 选项进行定义。

第六字段：提前多少天警告用户口令将过期。当用户登录系统后，系统登录程序提醒用户口令将要在多少天内作废。其默认值是通过/etc/login.defs 文件的 PASS_WARN_AGE 选项进行定义。

第七字段：在口令过期之后多少天禁用此用户。此字段表示用户口令作废多少天后，系统会禁用此用户。用户禁用后，将无法登陆系统且无法进行口令修改。

第八字段：用户过期日期。此字段指定了用户过期的天数（从1970 年的 1 月 1 日开始的天数），如果这个字段的值为空，帐号永远不过期；

第九字段：保留字段，目前为空，以备将来 Linux 发展之用。

可以使用 man shadow 命令来查看帮助，从而获得更为详尽的资料。

3.3/etc/group

（1）关于/etc/group

/etc/group 文件是用户组的配置文件，内容包括用户和用户组，并且能显示出用户是归属哪个用户组或哪几个用户组。一个用户可以归属一个或多个不同的用户组，同一用户组的用户之间具有相似的特征。

用户组在系统管理中为系统管理员提供了极大的方便，但安全性方面也存在一定的问题。如某个用户对系统管理有重要的权限，那就最好让用户拥有独立的用户组，或者是把用户下的文件的权限设置为完全私有，从而确保不会因为用户组的权限继承特性造成其他用户也越权得到管理权限。特别需要说明的是，root 用户组通常不要把普通用户加入进去，以防止普通用户拥有 root 权限。

（2）/etc/group 的详细说明

/etc/group 内容包括用户组（Group）、用户组口令、GID 及该用户组所包含的用户（User），每个用户组一条记录。

查看系统/etc/group 的文件内容，具体如下。

```
zhaodongfeng@TeachServer:~$ cat /etc/group
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:zhaodongfeng
tty:x:5:
disk:x:6:
```

```
lp:x:7:
mail:x:8:
news:x:9:
uucp:x:10:
man:x:12:
proxy:x:13:
kmem:x:15:
dialout:x:20:zhaodongfeng
fax:x:21:
voice:x:22:
cdrom:x:24:zhaodongfeng
floppy:x:25:
tape:x:26:
sudo:x:27:
audio:x:29:
dip:x:30:
www-data:x:33:
backup:x:34:
operator:x:37:
list:x:38:
irc:x:39:
src:x:40:
gnats:x:41:
shadow:x:42:
utmp:x:43:
video:x:44:
sasl:x:45:
plugdev:x:46:zhaodongfeng
staff:x:50:
games:x:60:
users:x:100:
nogroup:x:65534:
libuuid:x:101:
crontab:x:102:
syslog:x:103:
fuse:x:104:
mysql:x:105:
mlocate:x:106:
ssh:x:107:
ssl-cert:x:108:
zhaodongfeng:x:1000:
lpadmin:x:109:zhaodongfeng
sambashare:x:110:zhaodongfeng
admin:x:111:zhaodongfeng
utempter:x:113:
ftp:x:112:ftp
```

```
snmp:x:114:
zhaodongfeng@TeachServer:~$
```

说明如下。

第一字段：用户组名称。

第二字段：用户组密码。

第三字段：GID。

第四字段：用户列表，每个用户之间用，号分割。该字段可以为空，如果字段为空表示用户组为 GID 的用户名

（3）关于 GID

GID 和 UID 类似，是一个正整数或 0。GID 从 0 开始，GID 为 0 的组让系统赋予给 root 用户组。

Linux 系统会预留一些较靠前的 GID 给系统虚拟用户使用，每个系统预留的 GID 都有所不同。系统添加用户组默认的 GID 范围在/etc/login.defs 文件中通过 GID_MIN 和 GID_MAX 两个选项进行定义。

3.4/etc/gshadow

（1）关于/etc/gshadow

/etc/gshado 是/etc/group 的加密文件，用户组（Group）管理的密码就是存放在这个文件中。/etc/gshadow 和/etc/group 是互补的两个文件。

（2）/etc/gshadow 的详细说明

查看系统/etc/gshodow 的文件内容，具体如下。

```
zhaodongfeng@TeachServer:~$ sudo    cat /etc/gshadow
[sudo] password for zhaodongfeng:
root:*::
daemon:*::
bin:*::
sys:*::
adm:*::zhaodongfeng
tty:*::
disk:*::
lp:*::
mail:*::
news:*::
uucp:*::
```

```
man:*::
proxy:*::
kmem:*::
dialout:*::zhaodongfeng
fax:*::
voice:*::
cdrom:*::zhaodongfeng
floppy:*::
tape:*::
sudo:*::
audio:*::
dip:*::
www-data:*::
backup:*::
operator:*::
list:*::
irc:*::
src:*::
gnats:*::
shadow:*::
utmp:*::
video:*::
sasl:*::
plugdev:*::zhaodongfeng
staff:*::
games:*::
users:*::
nogroup:*::
libuuid:!::
crontab:!::
syslog:!::
fuse:!::
mysql:!::
mlocate:!::
ssh:!::
ssl-cert:!::
zhaodongfeng:!::
lpadmin:!::zhaodongfeng
sambashare:!::zhaodongfeng
admin:!::zhaodongfeng
utempter:!::
ftp:!::ftp
snmp:!::
zhaodongfeng@TeachServer:~$
```

具体说明。

第一字段：用户组。

第二字段：用户组密码。这个段可以是空的或!，如果是空的或有!，表示没有密码。

第三字段：用户组管理者。这个字段也可为空，如果有多个用户组管理者，用，号分割。

第四字段：组成员。如果有多个成员，用，号分割。

3.5 /etc/login.defs

/etc/login.defs 文件是当创建用户时的一些默认规划。对此文件的修改需要 root 权限。

查看/etc/login.defs 文件的内容，具体如下。

```
# *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  注：创建用户时，要在目录/var/spool/mail 中创建一个用户 mail 文件；
#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   注：用户的密码不过期最多的天数；
PASS_MIN_DAYS   0       注：密码修改之间最小的天数；
PASS_MIN_LEN    5       注：密码最小长度；
PASS_WARN_AGE   7       注：
#
# Min/max values for automatic uid selection in useradd
#
UID_MIN  500  注：最小 UID 为 500 ，也就是说添加用户时，UID 是从 500 开始的；
UID_MAX  60000   注：最大 UID 为 60000；
```

```
#
# Min/max values for automatic gid selection in groupadd
#
GID_MIN   500     注：GID 是从 500 开始；
GID_MAX   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 ORed with the -m flag on
# useradd command line.
#
CREATE_HOME       yes     注：是否创用户家目录，要求创建；
```

3.6 /etc/default/useradd

/etc/default/useradd 定义了通过 useradd 命令添加用户时的规则。

查看系统/etc/default/useradd 文件的内容，具体如下。

```
# useradd defaults file
GROUP=100
HOME=/home    注：把用户的家目录建在/home 中。
INACTIVE=-1    注：是否启用帐号过期停权，-1 表示不启用。
EXPIRE=        注：帐号终止日期，不设置表示不启用。
SHELL=/bin/bash     注：所用 SHELL 的类型。
SKEL=/etc/skel        注：  默认添加用户的目录默认文件存放位置。当用
adduser 添加用户时，用户个人目录下的文件，都是从这个目录中复制过去。
```

四、用户管理

4.1 管理用户的常用命令

在 Linux 操作系统中，提供了一系列用于用户管理的命令，具体如下表所示。

表 4-1 用户管理命令一览表

序号	命令	说明
1	useradd	添加用户。

2	adduser	添加用户。
3	passwd	设置用户的密码。
4	usermod	修改用户的配置参数。例如登录名、用户的个人目录等。
5	pwconv	可以开启用户的投影密码。将用户密码从/etc/passwd 同步到/etc/shadow。
6	pwck	校验用户配置文件/etc/passwd 和/etc/shadow 文件内容是否合法或完整。
7	pwunconv	执行 pwunconv 指令可以关闭用户投影密码，它会把密码从 shadow 文件内，重回存到 passwd 文件里。
8	finger	查看用户信息工具。
9	id	查看用户的 UID、GID 及所归属的用户组。
10	chfn	更改用户信息。
11	su	用户切换工具。
12	sudo	sudo 是通过另一个用户来执行命令（execute a command as another user），su 用来切换用户，然后通过切换到的用户来完成相应的任务。
13	visudo	visodo 是编辑/etc/sudoers 的命令，相当于直接编辑/etc/sudoers。
14	sudoedit	

4.2 查看用户信息

4.2.1 使用 id 查看用户信息

命令：

```
shell>id [参数] [用户名]
```

命令参数：

```
-g 或--group     显示用户所属群组的 ID。
-G 或--groups    显示用户所属附加群组的 ID。
-n 或--name      显示用户，所属群组或附加群组的名称。
-r 或--real      显示实际 ID。
-u 或--user      显示用户 ID。
--help      显示帮助。
--version      显示版本信息
```

命令说明：

（1）id 命令用于查看用户信息和用户组信息。

（2）指定用户名时查看指定用户的信息，不指定用户名时查看当前用户的信息。不指定参数时，显示所有信息。

4.2.2 查看登陆到系统的用户

命令：

```
shell>w
shell>who
shell>users
```

命令说明：

（1）w、who 和 users 命令可以查询已登录当前主机的用户。

（2）w、who 和 users 命令的作用相同，展示数据的方式不同。

4.3 使用 useradd 添加新用户

命令：

```
shell>useradd [-u uid [-o]] [-g group] [-G group,...]
                    [-d home] [-s shell] [-c comment] [-m [-k template]]
                    [-f inactive] [-e expire ] [-p passwd] name
shell>useradd -D [-g group] [-b base] [-s shell]
                    [-f inactive] [-e expire ]
```

命令参数：

```
-c：加上备注文字，备注文字保存在 password 的备注栏中。
-d：指定用户登入时的启始目录。
-D：变更预设值。
-e：指定账号的有效期限，缺省表示永久有效。
-f：指定在密码过期后多少天即关闭该账号。
-g：指定用户所属的群组。
-G：指定用户所属的附加群组。
-m：自动建立用户的登入目录。
-M：不要自动建立用户的登入目录。
-n：取消建立以用户名称为名的群组。
-r：建立系统账号。
-s：指定用户登入后所使用的 shell。
-u：指定用户 ID 号。
```

命令说明：

（1）useradd 后面直接跟用户名，不加任何参数，表示添加用户时按事先/etc/default/adduser 和/etc/login.defs 添加新用户的配置文件的规则来添加用户。

useradd 不加参数选项，后面直接跟所添加的用户名进行执行时

的过程是：

第一步：读取添加用户配置文件/etc/login.defs 和/etc/default/useradd 中所定义的规则。

第二步：依据规则添加用户。

第三步：向/etc/passwd 和/etc/groups 文件添加用户和用户组记录。

第四步：在/etc/shadow 和/etc/gshadow 加密资讯文件中同步生成记录。

第四步：在/etc/default/useradd 中所指定的用户默认文件存储的目录中建立用户个人目录。

第五步：复制/etc/skel 中的文件所有文件（包括隐藏文件）到新创建的用户个人目录。

（2）useradd 加-D 参数，可以修改配置文件中的默认参数。后面不添加任何内容直接执行 useradd -D 命令，显示配置文件信息。

（3）useradd 命令在创建用户时，没有指定用户密码，在用户创建完成后，使用 passwd 命令设置用户密码。

4.4 使用 passwd 修改用户口令

命令：

```
shell>passwd [-dklS][-u <-f>][用户名称]
```

命令参数：

-k, --keep-tokens：保留即将过期的用户在期满后能仍能使用。
-d, --delete：删除用户密码，仅能以 root 权限操作。
-l, --lock：锁住用户无权更改其密码，仅能通过 root 权限操作。
-u, --unlock：解除锁定。
-f, --force：强制操作；仅 root 权限才能操作。
-x, --maximum=DAYS：两次密码修正的最大天数，后面接数字；仅能 root 权限操作。
-n, --minimum=DAYS：两次密码修改的最小天数，后面接数字，仅能 root 权限操作。
-w, --warning=DAYS：在距多少天提醒用户修改密码；仅能 root 权限操作。
-i, --inactive=DAYS：在密码过期后多少天，用户被禁掉，仅能以 root 操作。
-S, --status：查询用户的密码状态，仅能 root 用户操作。

命令说明：

（1）passwd 的执行权限为普通用户和超级权限用户。普通用户只能更改自己的用户密码，但前提是没有被 root 用户锁定。root 用户可以设置或修改任何用户的密码。

（2）passwd 命令后面不接任何参数或用户名，则表示修改当前用户的密码。

（3）使用 useradd 命令创建新用户后，新创建的用户是没有密码的，需要及时通过 passwd 命令为其创建密码。

（4）如果需要指定某个用户不能修改密码，passwd -l 锁定用户的密码修改权限。

4.5 使用 usermod 修改用户信息

命令：

```
shell>usermod [-u uid [-o]] [-g group] [-G group,...]
                [-d 主目录 [-m]] [-s shell] [-c 注释] [-l 新名称]
                [-f 失效日] [-e 过期日] [-p 密码] [-L|-U] 用户名
```

命令参数：

-c comment：更新用户 password 档中的注解内容。
-d home_dir：更新用户的登入目录。如果给定-m 选项，用户旧目录会搬到新的目录去，如旧目录不存在则建新的目录。
-e expire_date：设置用户帐号过期的日期，日期格式为 MM/DD/YY。
-f inactive_days：帐号过期几日后永久停权。当值为 0 时帐号则立刻被停权。而当值为-1 时则关闭此功能。预设值为-1。
-g initial_group：更新用户新的起始登入用户组。用户组名须已存在。用户组 ID 必须参照既有的的用户组。用户组 ID 预设值为 1。
-G group [...]：定义用户为多个用户组成员。每个用户组使用","隔开，不可以夹杂空白内容。用户组名同-g 选项的限制。如果用户已经所属的用户组不在此列，则将用户从不在此列的用户组中移除。
-l login_name：变更用户 login 时的名称为 login_name。用户目录名也会同步更动为新的登入名。
-s shell：指定用户使用的 shell。如此栏留白，将选用系统预设 shell。
-u uid：修改用户 ID 值。为用户指定的 ID 值必须为唯一 ID 值，除非用-o 选项。数字不可为负值。UID 值不得小于/etc/login.defs 中定义的 UID_MIN 值。用户目录树下所有的档案目录其 userID 会自动改变。放在用户目录外的档案则要不会自动更新，需要手动更新。

命令说明：

（1）usermod 能够修改用户的各种信息与配置，例如修改用户的 SHELL 类型、所归属用户组、用户密码有效期以及登录名等信息。

（2）usermod 不允许修改当前活动用户的信息。当 usermod 修改用户信息时，首先确认被修改用户的 UID 没有执行任何程序。

（3）usermod 和 useradd 名的参数信息基本一致，useradd 用于创建用户，而 usermod 用于修改用户信息。

4.6 使用 userdel 删除用户

命令：

```
shell>userdel [-r][用户帐号]
```

命令说明：

（1）userdel 删除指定用户信息。

（2）使用-r 参数，可以在删除用户信息的同时，删除用户的个人目录的全部数据。

4.7 案例

案例 1：用户管理

（1）查看系统中所有的用户信息。

（2）查看当前用户的基本信息。

（3）查看当前登录系统的用户信息。

（4）创建用户 demouser1、demouser2、demouser3，并设置用户的口令为 user1pwd、user2pwd、user3pwd。

（5）用创建的用户登录，验证用户的信息是否正确。

（6）删除用户 demouser3，并验证是否删除成功。

五、用户组管理

5.1 管理用户组的常用命令

在 Linux 操作系统中，提供了一系列用于用户组管理的命令，具体如下表所示。

表 4-2 用户组管理命令一览表

序号	命令	说明
1	groupadd	添加用户组。
2	groupdel	删除用户组。
3	groupmod	修改用户组信息。
4	groups	显示用户所属的用户组信息。
5	grpck	检查用户组及密码文件的完整性（etc/group 和/etc/gshadow）
6	grpconv	开启用户组的投影密码。将用户组密码从/etc/group 同步到/etc/gshadow。如果/etc/gshadow 不存在则创建。
7	grpunconv	执行 grpunconv 指令可以关闭用户组投影密码，它会把密码从 gshadow 文件内，重回存到 group 文件里，并删除 gshadow 文件。

5.2 使用 groupadd 创建用户组

命令：

```
shell>groupadd [-g gid [-o]] [-r] [-f]  用户组名
```

命令参数：

-g gid：除非使用-o 参数，否则该值必须是唯一的。数值不可为负。
-o：允许设置相同组 id 的群组。
-r：建立系统组。
-f：强制执行，默认是不允许创建相同 id 的组的，使用此参数就可以，而且不用-o 选项。

命令说明：

（1）groupadd 可指定用户组名称来建立新的用户组帐号，需要时可从系统中取得新用户组值。

（2)建议创建用户组是尽量简单,直接指定用户组名称就可以。

5.3 使用 groupdel 删除用户组

命令：

```
shell>groupdel  用户组名称
```

命令说明：

（1）groupdel 用于删除指定的用户组。

（2）删除用户组时，用户组必须存在，如果被删除用户组中的任一用户在使用，则不能删除该用户组。

5.4 使用 groupmod 修改用户组信息

命令：

```
shell>groupmod [-g gid [-o]] [-n NewGroupName] 用户组名
```

命令参数：

```
-g gid：指定 GID。
-o：与 groupadd 命令中相同的作用。
-n NewGroupName：修改用户组名为 NewGroupName。
```

命令说明：

（1）groupmod 命令用于修改用户组的基本信息。

（2）指定的 GID 必须在系统中唯一，指定的 NewGroupName 必须在系统中唯一。

5.5 查询用户所属用户组信息

命令：

```
shell>groups [用户名]
```

命令说明：

（1）groups 用于查询指定用户所归属的用户组信息。

（2）如果不指定用户名，groups 查询当前用户的用户组信息。

5.6 案例

案例 2：用户组管理

（1）查看系统内所有的用户组信息。

（2）创建用户组 student。

（3）将 demouser1、demouser2 用户归于此用户组。

（4）查看 demouser1、demouser2 的用户信息，查看用户组变更操作是否成功。

六、讨论与思考

6.1 用户和用户组管理的方式

（1）除了使用用户和用户组管理的命令可以进行用户管理外，有哪些进行用户管理的图形工具？

（2）是否可以通过直接编辑/etc/passwd、/etc/shadow、/etc/group、/etc/gshadow 文件的方式进行用户和用户组管理？

6.2UID 和 GID

（1）在 Linux 中，root 用户的 UID 为 0，当前系统有普通用户 zhaodongfeng，其 UID 为 502。通过直接修改/etc/passwd 文件将 zhaodongfeng 用户的 UID 变更为 0 后，系统会发生什么？

（2）在 Linux 中，root 用户组的 GID 为 0，当前系统有普通用户组 student，其 GID 为 509。通过直接修改/etc/group 文件将 student 用户组的 GID 变更为 0 后，系统会发生什么？

6.3 通过数据库技术管理用户和用户组信息

（1）用户和用户组管理是操作系统的基本功能，如果一个服务器需要开放大量的用户信息，并且这些用户信息需要经常变更，可以有哪些方便的管理方式？

（2）Linux 操作系统中，用户和用户组信息存放在文件中，是否可以将用户和用户组信息存放到数据库中，以便于管理？