第5章 Linux系统用户管理

本章学习目标

- 了解 Linux 的用户和组的管理。
- 掌握用户管理的相关命令。
- 熟悉组管理的相关命令。

在 Linux 系统中，任何文件都属于某一特定用户，而任何用户都至少隶属于一个用户组。用户是否有权限对某文件进行访问、读写以及执行，受到用户与用户组管理系统的严格约束。本章将对 Linux 系统中重要的用户和用户组管理文件进行介绍，并且介绍如何进行管理。

5.1 Linux 用户介绍

5.1.1 用户和用户组

登录 Linux 系统时，用户通过特定的用户名(Username)来标识自己，用户的用户名就代表用户自己。用户所做的任何事情都与用户的用户名有关：系统上运行的每个进程都有一个相关的用户名。用户的用户名与用户所保存的内容有关：系统上每个文件被表明由某个特定用户所拥有。用户的用户名与用户使用的内容有关：用户所使用的磁盘空间总量或者用户使用的处理器时间总量都可以通过用户名追踪到。

系统上每个用户不仅有唯一的用户名，也有唯一的用户 ID，用户 ID 缩写为 UID。Linux 系统分配的 UID 是一个 32 位整数，这意味着最多可以有 2^{32} 个不同的用户。人们喜欢用文字来思考，而对 Linux 内核而言使用数字更简单。当内核记录谁拥有进程或者谁拥有文件时，它记下的是用户 ID 而不是用户名。

系统有一个数据库，存放着用户名与 UID 的对应关系，这个数据库被保存在配置文件/etc/passwd 中。Linux 像 UNIX 一样有一个优良的传统，那便是系统配置文件也是可读格式的文本，从而可以方便地用文本编辑器来编辑修改。用户和管理员可以用处理文本的小工具，如分页查看程序来检查这个数据库。系统中的大多数用户都有权限读取这个文件，但是不能进行修改。

由于每个文件必须有一个组所有者，因此必须有一个与每个用户相关的默认组。这个默认组成为新建文件的组所有者，被称作用户的主要组。除了主要组以外，用户也可以根据需要隶属于其他组，这些组被称作次要组。

5.1.2 用户分类

在 Linux 系统中，将用户分成 3 类：普通用户、超级用户和系统用户。

1. 普通用户

普通用户是使用系统的多数用户人群。普通用户通常通过/bin/bash 登录 Shell，把/home 作为用户主目录。一般情况下，普通用户只在自己的主目录和系统范围内的临时目录中创建文件。

2. 超级用户

超级用户的 UID 为 0。超级用户在系统上有完全权限：可以修改和删除任何文件；可以运行任何命令；可以取消任何进程。超级用户负责增加和保留其他用户，配置添加系统软硬件。超级用户通常使用/root 作为主目录。

3. 系统用户

大多数 Linux 系统会将一些低 UID 保留给系统用户。系统用户不代表人，而代表系统的组成部分。例如，处理电子邮件的进程经常以用户名 mail 来运行；运行 Apache 网络服务器的进程经常作为用户 apache 来运行。系统用户通常没有登录 Shell，因为它们不代表实际登录的用户。同样地，系统用户的主目录很少在/home 中，而通常在属于相关应用的系统目录中。例如，用户 apache 的目录/var/www。

用户类型及其 ID 范围如表 5.1 所示。

表 5.1 Linux 用户类型及 ID 范围

用户 ID 范围	用户类型
0	根用户
1～499	系统用户
500＋	普通用户

5.2 相关文件

Linux 操作系统在存储用户信息时，继承了 UNIX 的传统，把全部用户信息保存为普通的文本文件。它们分别是 passwd 文件、shadow 文件、group 文件、gshadow 文件。这些文件通过文本编辑器就可以查看。

5.2.1 passwd 文件

在 Linux 操作系统中，用户的关键信息被存放在系统的/etc/passwd 文件中，系统的每一个合法用户账号对应于该文件中的一行记录。这行记录定义了每个用户账号的属性。用户数据按字段以冒号分隔，格式如下。

```
username:password:uid:gid:userinfo:home:shell
```

其中，各个字段的含义如表 5.2 所示。

表 5.2 /etc/passwd 字段说明

字 段 名	编 号	说 明
username	1	给一个用户可读的用户名称
password	2	加密的用户密码
uid	3	用户 ID,Linux 内核用这个整数来识别用户
gid	4	用户组 ID,Linux 内核用这个整数识别用户组
userinfo	5	用来保存帮助识别用户的简单文本
home	6	当用户登录时,分配给用户的主目录
shell	7	登录 Shell 是用户登录时的默认 Shell,通常是/bin/bash

范例：解释图 5.1 中第一个用户 root 的基本信息。

图 5.1 passwd 文件

root 用户的基本信息如表 5.3 所示。

表 5.3 root 用户的基本信息

字 段 名	编 号	说 明
username	1	root
password	2	x
uid	3	0
gid	4	0
userinfo	5	root
home	6	/root
shell	7	/bin/bash

5.2.2 shadow 文件

用户的加密密码通常被保存在/etc/passwd 文件的第二个字段中。由于/etc/passwd 文件所包含的信息远远多于单纯的密码,每个人都必须能够读取它,因此,随着计算机性能的飞速发展,即使是暴露密码的加密形式也是非常危险的。高性能计算机可以通过穷举,在很短的时间破解密码,这就是“暴力”破解。

因此,在 Linux 和 UNIX 系统中,采用一种更新的叫作“影子密码”的技术来保存密码,用户的密码被保存在专门的/etc/shadow 文件中。由于该文件包含的是只与密码有关的信息,所以其权限不允许普通用户查看内容。查看这个文件需要超级管理员 root 的权限。

和/etc/passwd 文件类似,/etc/shadow 文件中的每行记录一个合法用户账号的数据,文件中的每一行的数据也是用冒号分隔,格式如下。

```
username: password:lastchg:min:max:warn:inactive:expire:flag
```

其中,各个字段的含义如表 5.4 所示。

表 5.4 /etc/shadow 字段说明

字 段 名	编 号	说 明
username	1	用户的登录名
password	2	加密的用户密码
lastchg	3	自 1970 年 1 月 1 日起到上次修改口令所经过的天数
min	4	两次修改口令之间至少经过的天数
max	5	口令还会有效的最大天数
warn	6	口令失效前多少天内向用户发出警告
inactive	7	禁止登录前用户还有效的天数
expire	8	用户被禁止登录的时间
flag	9	保留

范例:解释图 5.2 中第一个用户 root 的 shadow 信息。

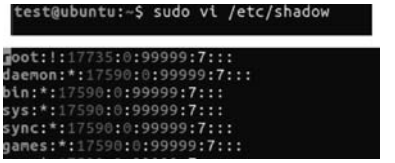

图 5.2 shadow 文件

对 root 用户的信息进行解释,该信息含义如表 5.5 所示。

表 5.5 root 用户的 shadow 文件信息

字 段 名	编 号	说 明
username	1	root
password	2	加密口令:6zAkvHVUq$Rg0ruC1MW8Iw.2 NiJMR/FDqt6/0q8vtGuLqaiXzED.YchzObeweCp3hvagWBOzl4rrNWnRqshEAuNPZsHvbH1
lastchg	3	自 1970 年 1 月 1 日起到上次修改口令所经过的天数:0
min	4	需几天可以修改口令:0 天
max	5	口令还会有效的最大天数:99999 天,即永不过期
warn	6	口令失效前 7 天内向用户发出警告
inactive	7	禁止登录前用户还有效的天数未定义,以“:”表示
expire	8	用户被禁止登录的时间未定义,以“:”表示
flag	9	保留未使用,以“:”表示

5.2.3 group 文件

Linux 内核用 32 位整数来标识用户组。/etc/group 文件把组名与组 ID 联系在一起,并且定义了用户属于哪些组。/etc/group 文件对组的作用相当于/etc/passwd 文件对用户的作用,有着类似的结构和更合理的名称。这也是一个以行为单位的配置文件,每行含有被

冒号隔开的字段，格式如下。

```
group_name:group_password:group_id:group_members
```

其中，各个字段的含义如表 5.6 所示。

表 5.6　/etc/group 字段说明

字　段　名	编　　号	说　　明
group_name	1	用户组名
group_password	2	加密后的用户组密码
group_id	3	用户组 ID
group_members	4	逗号分隔开的组成员

范例：解释图 5.3 中第一个组 root 的组信息。

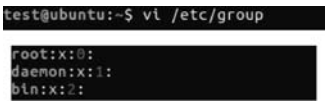

图 5.3　group 文件

root 用户组的信息如表 5.7 所示。

表 5.7　root 用户组的信息

字　段　名	编　　号	说　　明
group_name	1	root
group_password	2	加密后的用户组密码：x
group_id	3	0
group_members	4	group_members4 没有组成员

5.2.4　gshadow 文件

和用户账号文件 passwd 一样，为了防止暴力破解，用户组文件也采用将组口令与组的其他信息分离的安全机制，即使用/etc/gshadow 文件存储加密的组口令。查看这个文件需要 root 权限。gshadow 文件也是一个以行为单位的配置文件，每行含有被冒号隔开的字段，gshadow 文件的格式如下。

```
group_name:group_password:group_id:group_members
```

其中，各个字段的含义如表 5.8 所示。

表 5.8　/etc/gshadow 字段说明

字　段　名	编　　号	说　　明
group_name	1	用户组名
group_password	2	加密后的用户组密码：
group_id	3	用户组 ID(可以为空)
group_members	4	逗号分隔开的组成员(可以为空)

范例：解释图 5.4 中 root 组的信息。

图 5.4　gshadow 文件

root 用户组的信息如表 5.9 所示。

表 5.9　root 用户组的信息

字　段　名	编　　号	说　　明
group_name	1	root
group_password	2	加密后的用户组密码：*
group_id	3	空
group_members	4	空

5.3　用户管理命令

5.3.1　useradd 命令

功能描述：在 Linux 系统中创建新用户。

语法：

useradd [选项] 用户名

选项：useradd 命令中的常用选项如表 5.10 所示。

表 5.10　useradd 命令选项

选　　项	作　　用
-d	指定用户主目录
-g	指定 gid
-u	指定 uid
-l	不要把用户添加到 lastlog 和 failog 中，这个用户的登录记录不需要记载
-m	自动创建用户主目录
-p	指定新用户的密码
-r	建立一个系统账号
-s	指定 Shell

范例：

使用 useradd 命令创建一个 test 用户。用户组为 test，登录 Shell 为/bin/bash，用户主目录为/home/Mym，命令的执行过程和结果如图 5.5 所示。

使用 useradd 命令创建一个 test2 用户。创建时 useradd 后面不添加任何参数选项，命

图 5.5　使用 useradd 命令创建用户

令的执行过程和结果如图 5.6 所示。

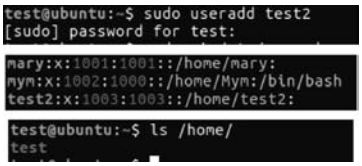

图 5.6　使用 useradd 命令创建三无用户

使用 useradd 命令时，如果后面不添加任何参数选项，创建出来的用户将是默认的“三无”用户：一无主目录，二无密码，三无系统 Shell。

在 Ubuntu 系统中，还有一个可以创建用户的命令：adduser。使用 adduser 命令时，创建用户的过程更像是一种人机对话过程，系统会提示用户输入各种信息，然后会根据这些信息创建新用户。

范例：使用 adduser 命令创建一个 test1 用户命令的执行过程和结果如图 5.7 所示。

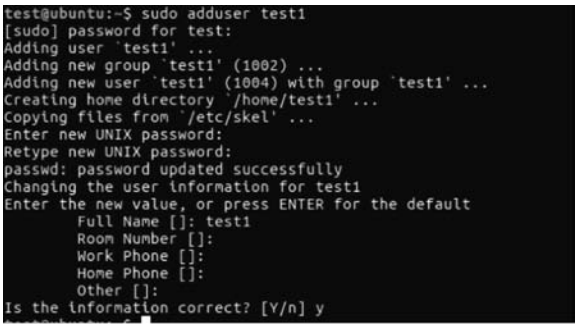

图 5.7　使用 adduser 命令创建用户

adduser 命令简单，适合初级使用者，因为不用去记那些烦琐的参数选项，只要跟着系统的提示一步一步去做即可完成。而 useradd 命令适合有经验的使用者，往往一行命令加参数就能解决很多问题，所以创建起来十分方便。

5.3.2　passwd 命令

功能描述：为新增加的用户设置口令，也可以更改原有用户的口令，管理员还可以使用 passwd 命令锁定某个用户账户。

语法：

```
passwd[选项]用户名
```

选项：passwd 命令中的常用选项如表 5.11 所示。

表 5.11　passwd 命令选项

选　项	作　用
-l	管理员锁定已经命名的账户名称
-u	管理员解开账户锁定状态
-x	管理员设置最大密码使用时间(天)
-n	管理员设置最小密码使用时间(天)
-d	管理员用来删除用户的密码

范例：为新建用户 testl 设定密码。命令的执行过程如图 5.8 所示。

```
test@ubuntu:~$ sudo passwd test1
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
```

图 5.8　为 test 设定密码

5.3.3　usermod 命令

功能描述：修改用户账户的信息。

语法：

usermod [选项]用户名

选项：命令中的常用选项如表 5.12 所示。

表 5.12　usermode 命令选项

选　项	作　用
-d	修改用户主目录
-e	修改账号的有效期限
-f	修改在密码过期后多少天即关闭该账号
-g	修改用户所属的组
-G	修改用户所属的附加组
-l	修改用户账号名称
-L	锁定用户密码,使密码无效
-s	修改用户登录后所使用的 Shell
-u	修改用户 ID
-U	解除密码锁定

范例：

将 test1 用户添加到组 users 中,命令的执行过程如图 5.9 所示。

```
test@ubuntu:~$ sudo usermod -G users test1
test@ubuntu:~$ vi /etc/gr
staff:x:50:
games:x:60:
users:x:100:test1
```

图 5.9　修改用户附加组

修改 Mym 的用户名为 Myx。命令的执行过程如图 5.10 所示。

锁定账号 Myhx,锁定账号后,使用文本编辑器查看/etc/shadow,用户的密码项的开始

处插入一个感叹号表示用户被锁定。命令的执行过程如图 5.11 所示。

```
test@ubuntu:~$ sudo usermod -l myx mym
test@ubuntu:~$ vi /etc/passwd
```

图 5.10　修改用户名

```
test@ubuntu:~$ sudo usermod -l mym myx
test@ubuntu:~$ sudo usermod -L mym
test@ubuntu:~$ sudo vi /etc/shadow
```

图 5.11　锁定用户

解除对 Myx 的锁定，使用文本编辑器查看/etc/shadow，用户的密码项的开始处的感叹号消失，表示用户的锁定被解除。命令的执行过程如图 5.12 所示。

```
test@ubuntu:~$ sudo usermod -U myx
[sudo] password for test:
test@ubuntu:~$ sudo vi /etc/shadow
```

图 5.12　解除锁定

5.3.4　userdel 命令

功能描述：userdel 命令用来删除系统中的用户。

语法：

```
userdel [选项] 用户名
```

选项：userdel 命令中的常用选项如表 5.13 所示。

表 5.13　userdel 命令选项

选　　项	作　　用
-r	删除账户时，连同用户主目录一起删除

范例：

删除 test1 账户，不删除用户主目录。命令的执行过程和结果如图 5.13 所示。

```
test@ubuntu:~$ ls /home/
test  test1
test@ubuntu:~$ sudo userdel test1
[sudo] password for test:
test@ubuntu:~$ ls /home/
test  test1
```

图 5.13　不删除用户主目录

删除 test1 账户，并将用户主目录一同删除。命令的执行过程和结果如图 5.14 所示。

```
test@ubuntu:~$ ls /home
test
test@ubuntu:~$ sudo userdel -r test1
test@ubuntu:~$ ls /home/
test  test1
```

图 5.14　删除用户主目录

5.4 用户组管理命令

5.4.1 groupadd 命令

功能描述：groupadd 命令可指定组名称来建立新的组账号。

语法：

```
groupadd [选项]组名
```

选项：groupadd 命令中的常用选项如表 5.14 所示。

表 5.14 groupadd 命令选项

选　项	作　用
-g	组 ID，除非使用-o 选项，否则该值必须唯一
-o	允许设置相同组 ID 的群组
-r	建立系统组
-f	强制执行，创建相同 ID 的组

范例：新建组 helo，指定 gid 为 400。命令的执行过程和结果如图 5.15 所示。

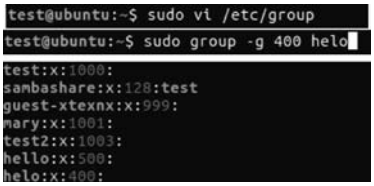

图 5.15 新建组

5.4.2 groupmod 命令

功能描述：groupmod 命令用来修改用户组属性。

语法：

```
groupmod [选项] 组名
```

groupmod 命令中的常用选项如表 5.15 所示。

表 5.15 groupmod 命令选项

选　项	作　用
-g	指定组 ID
-o	与 groupadd 相同
-n	修改用户组名

范例：修改组 helo 的组名为 ehlo，gid 为 6000。命令的执行过程和结果如图 5.16 所示。

图 5.16　修改组

5.4.3　groupdel 命令

功能描述：groupdel 命令可以从系统上删除组。如果该组中仍包含某些用户，则必须先删除这些用户后，方能删除组。

语法：

```
groupdel 组名
```

范例：为组 ehlo 添加新用户 wangli，然后删除组 ehlo。命令的执行过程和结果如图 5.17 所示。

图 5.17　删除组

5.4.4　gpasswd 命令

功能描述：gpasswd 命令用来管理组。使用 gpasswd 命令为组设定密码，让知道该组密码的用户可以暂时切换具备该组功能。

语法：

```
gpasswd [选项]组名
```

gpasswd 命令中的常用选项如表 5.16 所示。

表 5.16　gpasswd 命令选项

选　项	作　用
-a	指定组 ID
-d	从组删除用户
-A	指定管理员
-M	指定组成员
-r	删除密码
-R	限制用户登录组，只有组中的成员才可以用 newgrp 加入该组

范例：系统中有个 test 账户，该账户本身不是 users 群组的成员，就不能为该组添加成员。通过 gpasswd 命令将 test 用户设置为 users 群组的管理员，之后 test 就可以为 users 组添加成员了。命令的执行过程如图 5.18 和图 5.19 所示。

```
usbmux:x:120:46:usbmux daemon,,,:/var/lib/usbmux:/bin/false
test:x:1000:1000:test,,,:/home/test:/bin/bash
sshd:x:121:65534::/var/run/sshd:/usr/sbin/nologin
```

图 5.18　查看 test 账户信息

```
test@ubuntu:~$ gpasswd -a mary users
gpasswd: Permission denied.
test@ubuntu:~$ sudo gpasswd -A test users
test@ubuntu:~$ gpasswd -a mary users
Adding user mary to group users
```

图 5.19　gpasswd 命令应用

5.5　su 和 sudo 命令

5.5.1　su 命令

功能描述：su 命令的作用是切换用户，超级权限用户 root 向普通或虚拟用户切换不需要密码，而普通用户切换到其他任何用户都需要密码验证。

语法：

su [选项] 用户名

su 命令中的常用选项如表 5.17 所示。

表 5.17　su 命令选项

选　项	作　用
-l	切换用户时，如同重新登录，如果没有指定用户名，默认为 root
-p	切换当前用户时，不切换用户工作环境，此为默认值
-c	以指定用户身份执行命令
-	切换当前用户时，切换用户工作环境

范例：切换用户名

不切换用户工作环境，命令的执行过程如图 5.20 所示。

```
test@ubuntu:~$ ls
aaa       directory.out  examples.desktop  More       Public
cat.txt   Documents      file              Music      Templates
Desktop   Downloads      hosts.bak         Pictures   Videos
test@ubuntu:~$ su root
Password:
root@ubuntu:/home/test# ls
aaa       directory.out  examples.desktop  More       Public
cat.txt   Documents      file              Music      Templates
Desktop   Downloads      hosts.bak         Pictures   Videos
```

图 5.20　不切换用户工作环境

范例：切换用户名，并切换用户工作环境，命令的执行过程如图 5.21 所示。

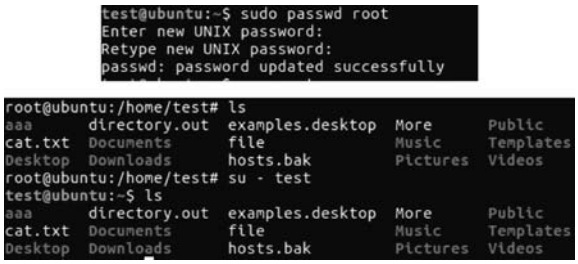

图 5.21　切换用户工作环境

5.5.2　sudo 命令

使用 su 命令切换到超级权限用户 root 后，权限是无限制的。但是当服务器的管理有多人参与时，有时不能明确哪些工作是由哪个用户切换到超级权限用户进行的操作。这对于服务器系统来说是不安全的。所以最好是针对每个管理员的技术特长和管理范围，有针对性地下放权限，并且约定其使用哪些工具来完成与其相关的工作，这时就有必要用到 sudo 命令了。在 Ubuntu 系统中，默认会将 root 用户关闭，使用 sudo 命令来获得 root 权限。

功能描述：允许超级权限用户 root 为其他用户委派权利，使之能运行部分或全部由 root 用户执行的命令。

语法：

sudo [选项]命令

sudo 命令中的常用选项如表 5.18 所示。

表 5.18　sudo 命令选项

选　项	作　用
-h	列出帮助信息
-V	列出版本信息
-l	列出当前用户可以执行的命令
-u	以指定用户的身份执行命令
-k	清除 timestamp 文件，下次使用 sudo 时需要再输入密码
-b	在后台执行指定的命令
-p	更改询问密码的提示语
-	不是执行命令，而是修改文件，相当于命令 sudoedit

范例：test 用户环境

查看/root 目录的内容，命令的执行过程如图 5.22 所示。

图 5.22　sudo 命令范例 1

test 用户为 test2 用户设置密码，命令的执行过程如图 5.23 所示。

```
test@ubuntu:~$ passwd test2
passwd: You may not view or modify password information for test2.
test@ubuntu:~$ sudo /usr/bin/passwd test2
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
```

图 5.23　sudo 命令范例 2

范例：清除 timestamp 文件，下次使用 sudo 命令时需要再输入密码，命令的执行过程如图 5.24 所示。

```
test@ubuntu:~$ sudo ls /root/
test@ubuntu:~$ sudo -k
test@ubuntu:~$ sudo ls /root/
[sudo] password for test:
```

图 5.24　sudo 命令范例 3

sudo 命令的执行流程是当前用户切换到 root(或其他指定切换到的用户)，然后以 root(或其他指定的切换到的用户)身份执行命令，执行完成后，直接退回到当前用户；而这些前提是要通过 sudo 的配置文件/etc/sudoers 来进行授权。

通过 sudo 命令，能有针对性地下放某些超级权限，并且不需要普通用户知道 root 密码，所以 sudo 命令相对于权限无限制性的 su 命令来说，还是比较安全的，sudo 也被称为受限制的 su。另外，sudo 是需要授权许可的，所以也被称为授权许可的 su。

小　　结

本章主要介绍了 Linux 系统中用户和组的管理，包括一些重要的文件的使用，以及管理用户和组的相关命令的使用方法。这一章介绍的内容对于系统的管理是很重要的一部分内容。

习　　题

1. 下面关于 passwd 命令说法不正确的是(　　)。

A. 普通用户可以利用 passwd 命令修改自己的密码

B. 超级用户可以利用 passwd 命令修改自己和其他用户的密码

C. 普通用户不可以利用 passwd 命令修改其他用户的密码

D. 普通用户可以利用 passwd 命令修改自己和其他用户的密码

2. 文件 exer 的访问权限为 rw-r--r--，现要增加所有用户的执行权限和同组用户的写权限，下列命令正确的是(　　)。

A. chmod a+x g+w exer　　B. chmod 765 exer

C. chmod o+x exer　　D. chmod g+w exer

3. 为了保证系统的安全，目前的 Linux 一般是将用户账号的口令信息加密后存储于(　　)文件中。

A. /etc/passwd　　B. /etc/shadow

C. /var/passwd　　D. /var/shadow

4. passwd 文件各字段说明中，表示使用者在系统中的名字是(　　)。

A. account　　B. password　　C. UID　　D. GID

5. 把用户名“liuyidan”改为“lyd”，使用的命令是(　　)。

A. ＃usermod -l lyd liuyidan　　B. ＃usermod -L lyd liuyidan

C. ＃useradd -L lyd liuyidan　　D. ＃useradd -l lyd liuyidan

6. 在终端提示符后使用 useradd 命令，该命令没做下面(　　)操作。

A. 在/etc/passwd 文件中增添了一行记录

B. 在/home 目录下创建新用户的主目录

C. 将/etc/skel 目录中的文件复制到新用户的主目录中去

D. 建立新的用户并且登录

7. 新建用户时指定该账户在 30 天后过期，现在想改变这个过期时间，使用(　　)命令。

A. usermod -a　　B. usermod -d

C. usermod -x　　D. usermod -e

8. Linux 使用哪个文件存储用户账号、密码和组名称？

9. 如何为新增用户指定用户主目录？

10. 使用什么命令可以从普通用户变为超级用户？

11. 简述 su 和 sudo 命令的作用与区别。

12. 如何让一个用户具有 sudu 的权限？

13. 上机练习：对 Linux 用户、组管理相关的命令进行练习，掌握 Linux 系统中用户的创建及管理。

实验 5-1　用户和组的管理

1. 实验目的

熟悉命令行中用户和组的管理方法。

2. 实验内容

(1) 新增一个名为 erdi 的用户，将这个用户分配到一个新组 some 中。

(2) 切换到 root 用户，修改 erdi 的密码。

(3) 添加一个用户名为 student，组名为 students，初始密码为 123456。

(4) 给 student 用户修改密码为 123123。

(5) 删除 student 用户。

(6) 从普通用户切换到 su 用户。

(7) 比较 su 用户与 sudo 用户的区别。