

第6章 用户和进程管理

1 用户概述

- 账户实质
- 账户实质上就是一个用户在系统上的标识，系统依据账户来区分每个用户的文件、进程、任务，给每个用户提供特定的工作环境（如用户的工作目录、**shell**版本、以及**X-Windows**环境的配置等），使每个用户的工作都能独立不受干扰地进行。

Linux中的账户

■ 用户账户

- 超级用户：UID=0，GID=0
- 普通用户：UID>=500
- 伪用户：0<UID<500

■ 组账户

- 标准组：标准组可以容纳多个用户，若使用标准组，在创建一个新的用户时就应该指定他所属于的组。
- 私有组：私有组中只有用户自己。当在创建一个新用户**user**时，若没有指定他所属于的组，**Red Hat** 就建立一个和该用户同名的私有组。

用户和组的关系

- 组是用户的集合。一个标准组可以容纳多个用户。
- 同一个用户可以同属于多个组，这些组可以是私有组，也可以是标准组。
- 当一个用户同属于多个组时，将这些组分为：
 - 主组：用户登录系统时的组。
 - 附加组：可切换的其他组。

系统账户文件

- 用户口令文件/etc/passwd
 - 文件权限: (-rw-r--r--)
- 用户影子口令文件/etc/shadow
 - 文件权限: (-r-----)
- 组账号文件/etc/group
 - 文件权限: (-rw-r--r--)
- 组口令文件/etc/gshadow
 - 文件权限: (-r-----)

账户管理的特性

- 默认启用shadow passwords功能。 /etc/passwd文件对任何用户均可读， 为了增加系统的安全性， 用户的口令通常用shadow passwords保护。
- 经过shadow passwords保护的账户密码和相关设置信息保存在/etc/shadow文件里。 /etc/shadow只对root用户可读。
- 默认使用MD5算法的用户口令。
- 一般不设置组口令。因为绝大多数应用程序不使用组口令。
- 建议尽量使用私有组来提高系统安全性。

账户管理的特性

- 不建议管理员直接编辑修改系统账户文件来维护账户。若用户直接编辑了账户文件， 建议使用账号文件的一致性检测命令。
 - **pwck**命令：检测文件“/etc/passwd”和“/etc/shadow” 的每行中字段的格式和值是否正确。
 - **grpck**命令：检测文件“/etc/group”和“/etc/gshadow”的每行中字段的格式和值是否正确。

2 用户和工作组管理

- 用户管理的日常任务包括创建用户、管理用户和删除用户。
- **Linux2.0**以上的版本将用户基本信息存于**/etc/passwd**文件，用户密码存放在**/etc/shadow**文件，从而提高了系统的安全性。
- 系统创建一个用户要完成**3**个任务。
 - 1) 在**/etc/passwd**文件中添加用户的相关信息
 - 2) 在**/etc/shadow**文件中添加用户的密码和相关信息
 - 3) 创建用户的登陆目录，默认状态下是在**/home**目录下面为用户创建登陆目录

2.1 用户相关文件

- 1. 用户账号文件——**passwd**
- **Passwd** 是一个文本文件，用于定义系统的用户账号，该文件位于“**/etc**”目录下。它包含了一个系统账户列表，给出每个账户一些有用的信息，例如，用户 **ID**、组 **ID**、主目录、**shell**等等。由于所有用户都对**passwd**有读权限，所以该文件中只定义用户账号，而不保存口令。
- **passwd**文件中每行定义一个用户账号，一行中又划分为多个字段定义用户的账号的不同属性，各字段用“:”隔开，格式如下：
- **username:passwd:UID:GID:full name:home directory:login shell**
- 图3-1中显示了**passwd**文件的前10行内容。在图中显示出了文件显示各用户的每一个字段，各字段的说明如表3-1所示。

passwd文件的属性及部分内容

- `root:x:0:0:root:/root:/bin/bash`
- `bin:x:1:1:bin:/bin:/sbin/nologin`
- `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`
- `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`
- `news:x:9:13:news:/etc/news:`

表3-1 passwd文件各字段说明

字 段	说 明
Account	使用者在系统中的名字，它不能包含大写字母。
Password 保存口令， shadow文件。	用户口令，出于安全考虑，现在不使用该字段而用字母“x”来填充该字段，真正的密码保存在shadow文件。
UID	用户 ID 号，惟一表示某用户的数字。
GID	用户所属的私有组号，该数字对应group文件中的GID。
GECOS	这字段是可选的，通常用于保存用户命名的信息。
Directory	用户的主目录，用户成功登录后的默认目录。
shell	用户所使用的shell，如该字段为空则使用“/bin/sh”。

2. 用户口令文件——shadow

在shadow文件中，每行定义了一个用户信息，行中各字段各字段用“:”隔开。为进一步提高安全性，shadow文件中保存的是已加密的口令。图3-2中显示了shadow文件的前10行内容。

2. 用户口令文件——shadow

- 在shadow文件中，每行定义了一个用户信息，行中各字段各字段用“:”隔开。为进一步提高安全性，shadow文件中保存的是已加密的口令。图3-2中显示了shadow文件的前10行内容。
- root:\$1\$w3i0i42Q\$2ogWYbuUKdm4CfJ3z3sJl1:15429:0:99999:7:::
- bin:*:15429:0:99999:7:::
- daemon:*:15429:0:99999:7:::
- adm:*:15429:0:99999:7:::
- lp:*:15429:0:99999:7:::
- sync:*:15429:0:99999:7:::
- shutdown:*:15429:0:99999:7:::
- halt:*:15429:0:99999:7:::
- mail:*:15429:0:99999:7:::
- news:*:15429:0:99999:7:::

从图3-2中可以看出，“/etc/shadow”文件中的每个记录用“:”隔开为9个域，每个域的含义分别为：

- Ø 登录名
- Ø 加密口令
- Ø 口令上次更改时距1970年1月1日的天数
- Ø 口令更改后不可以更改的天数
- Ø 口令更改后必须再更改的天数(有效期)
- Ø 口令失效前警告用户的天数
- Ø 口令失效后距账号被查封的天数
- Ø 账号被封时距1970年1月1日的天数
- Ø 保留未用

3. 用户组账号文件——group

用户组是逻辑地组织用户账号集合的方便途径，它允许用户在组内共享文件。系统上的每一个文件都有一个用户和一个组的属主。使用“ls -l”命令可以看到每一个文件的属主和组。

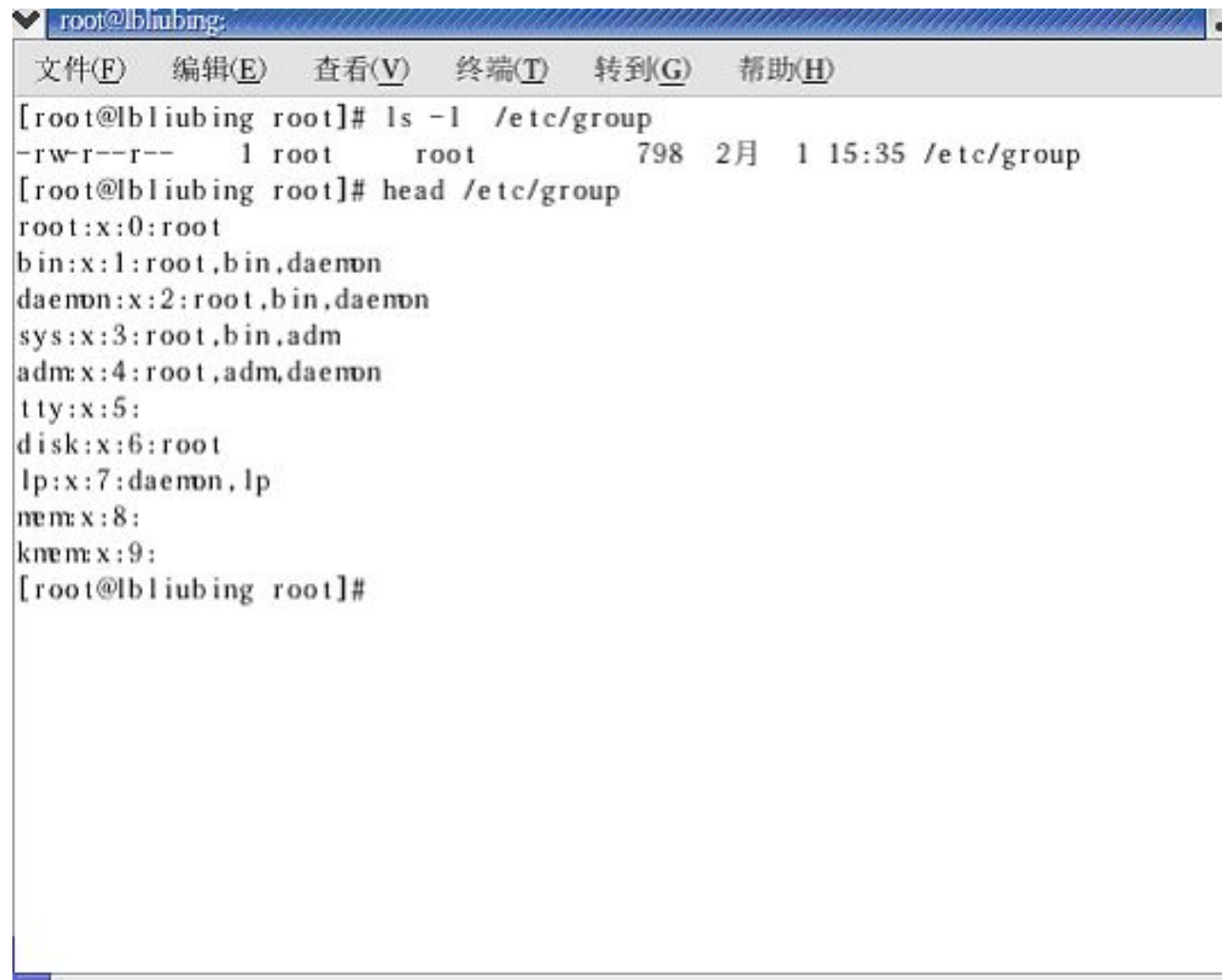
于系统上的每个组，在/etc/group文件中有一行记录，记录的格式为：

```
groupname : passwd : GID : userlist
```

表3-2 group文件字段说明

字 段	说 明
Groupname	是组的名字
Passwd	是组的加密口令
GID	是系统区分不同组的ID，在/etc/passwd域中的GID域是用这个数来指定用户的缺省组。
Userlist	是用“，”分开的用户名，列出的是这个组的成员。

图3-3中显示了shadow文件的前10行内容。



```
root@bliubing:
文件(F)  编辑(E)  查看(V)  终端(T)  转到(G)  帮助(H)
[root@bliubing root]# ls -l /etc/group
-rw-r--r--  1 root    root      798  2月  1 15:35 /etc/group
[root@bliubing root]# head /etc/group
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
tty:x:5:
disk:x:6:root
lp:x:7:daemon,lp
nem:x:8:
knem:x:9:
[root@bliubing root]#
```


- 第1行得**root**是一个特殊的系统组，是为超级用户保留的
- 第2行的**bin**是应用程序或进程使用的组，**root,bin,daemon**都是该组成员。
- 第3行的**daemon**是系统进程组，**root,bin,daemon**都是该组成
- 员
- 第4行的**adm**是系统管理使用的组，**root,adm,daemon**都是
- 该组成员。
- **User**是常规用户组

4. 用户组口令文件——gshadow

gshadow文件用于定义用户组口令、组管理员等信息，该文件只有root用户可以读取。Gshadow文件中每行定义一个用户组信息，行中各字段间用“:”分隔，每行记录的格式为：

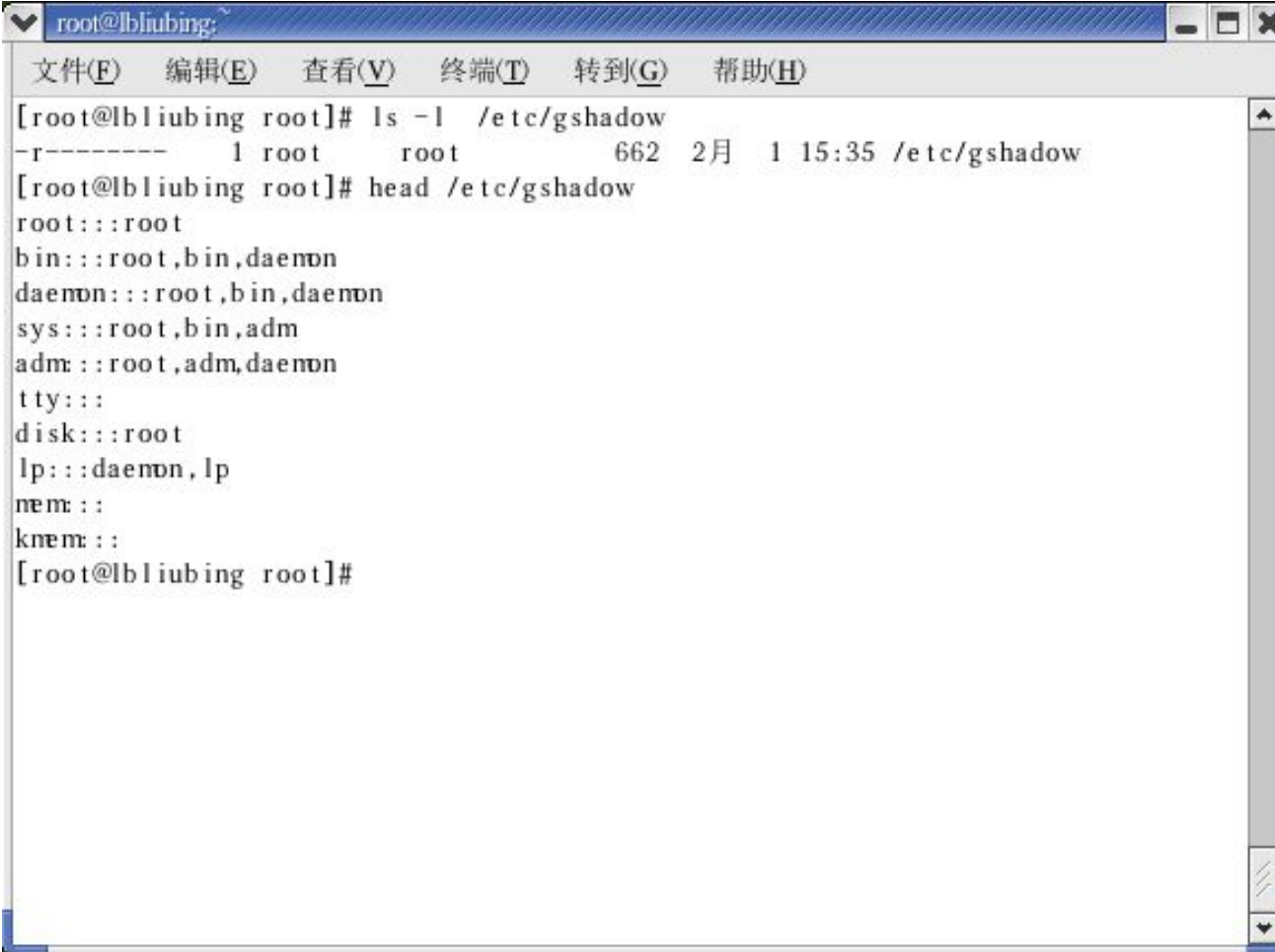
```
groupname : Encrypted password: Group administrators: Group members
```

各字段的含义如表3-3所示。在图3-4中给出了该文件的属性及文件的部分内容。

表3-3 group文件字段说明

字 段	说 明
Groupname	用户组名称，该字段与group文件中的组名称对应。
Encrypted password	用户组口令，该字段用于保存已加密的口令
Group administrators	组的管理员账号，管理员有权对该组添加删除账号。
Group members	属于该组的用户成员列表，列表中多个用户间用“，”分隔。

图3-4 group文件的属性及部分内容



```
root@bliubing:~  
文件(F) 编辑(E) 查看(V) 终端(T) 转到(G) 帮助(H)  
[root@bliubing root]# ls -l /etc/gshadow  
-r----- 1 root root 662 2月 1 15:35 /etc/gshadow  
[root@bliubing root]# head /etc/gshadow  
root:::root  
bin:::root,bin,daemon  
daemon:::root,bin,daemon  
sys:::root,bin,adm  
adm:::root,adm,daemon  
tty:::  
disk:::root  
lp:::daemon,lp  
nem:::  
knem:::  
[root@bliubing root]#
```

2.2 用户和组账户的维护命令

1. 增加用户帐号

在命令行下使用 `useradd` 命令：

```
useradd 用户名
```

该命令做了下面几件事：

- 1) 在 `/etc/passwd` 文件中增添了一行记录；
- 2) 在 `/home` 目录下创建新用户的主目录，并将 `/etc/skel` 目录中的文件拷贝到该目录中去；但是使用了该命令后，新建的用户暂时还无法登录，因为还没有为该用户设置口令，需要再用 `passwd` 命令为其设置口令后，才能登录。用户的 UID 和 GID 是 `useradd` 自动选取的，它是将 `/etc/passwd` 文件中的 UID 加 1，将 `etc/group` 文件中的 GID 加 1。

增加新用户时，系统将为用户创建一个与用户名相同的组，称为私有组。这一方法是为了能让新用户与其他用户隔离，确保安全性的措施

下面通过增加一个用户“**xuan**”，以及查看其相关信息，来帮助用户理解该命令所执行的操作。其在终端上的操作命令及响应如图3--5所示。

```
#useradd xuan
```

```
//建立用户账号
```

```
#tail -l /etc/passwd  
用户
```

```
//查看password文件中添加的  
账号信息
```

```
#tail -l /etc/shadow
```

```
# ls /home
```

```
//查看所建立账号的主目录
```

图3-5 增加用户及相关操作

选项

功能描述

-g

用于添加用户账号时指定该用户的私有组。如不指定“-g”参数，**useradd**命令将自动建立与用户账号同名的组作为该账号的私有组。

-D

用于显示或设置**useradd**命令所使用的默认值

Ø 在“-g”选项时，其语法格式如下：

```
useradd -g 组名 用户名
```

Ø在“-D”选项中，如果是用来修改**useradd**命令所使用的默认值，那么该命令使用的语法格式如下：

```
useradd -D [-g group][-b base][-s shell][-f inactive][-e expire]
```

2. 修改用户账号——usermod

usermod命令可用来修改用户帐号的各种属性，包括用户主目录、私有组、登录、shell等内容。Usermod的命令格式如下：

```
usermod [-LU][-c <备注>][-d <登入目录>][-e <有效期限>][-f <缓冲天数>][-g <群组>]  
        [-G <群组>][-l <帐号名称>][-s ][-u ][用户帐号]
```

该命令的各个参数说明如下：

- c<备注>： 修改用户帐号的备注文字。
- d<登入目录>： 修改用户登入时的目录。
- e<有效期限>： 修改帐号的有效期限。
- f<缓冲天数>： 修改在密码过期后多少天即关闭该帐号。
- g<群组>： 修改用户所属的群组。

下面举例说明该命令的使用方法：

（1）修改用户名，把用户名“xuan”改名为“xjh”，使用的命令是：

```
# usermod -l xjh xuan
```

（2）锁定“xjh”用户，使其不能登录。命令如下：

```
# usermod -L xjh
```

（3）解锁“xjh”用户账号，使其可以登录。命令如下：

```
# usermod -U xjh
```


3. 删除用户——userdel

userdel命令用于删除指定的用户账号。其使用的语法格式为：

userdel [-r][用户账号]

需要补充说明的是userdel命令可删除用户账号与相关的文件。若不加参数，则仅删除用户账号，而不删除相关文件。

其中参数“-r”是用来删除用户登入目录以及目录中所有文件。

下面举例说明该命令的使用方法：

```
#grep xjh /etc/passwd          //查询用户账号
                                是否存在
#userdel xjh                    //删除账号
#grep xjh /etc/passwd          //再次查询用户账号
                                号lyd是否存在
#ll -d /home                    //查询用户的主目录是否还存在
#userdel -r xjh                //删除用户的同时删除其工作主目录
```

4. 组增加命令——groupadd

groupadd命令可指定群组名称来建立新的群组账号。该组账号的ID值必须是惟一的，且数值不可为负。预设的最小值不得小于500，且每增加一个组账号ID值逐次增加。ID值0~499是保留给系统账号使用。该指令使用的语法格式为：

```
groupadd [-r] group
```

其中“-r”参数是用来建立系统账号。系统账号的ID值不能大于500。下面举例说明该命令的使用方法：

```
# groupadd lbgroup           //建立组账号lbgroup
# grep lbgroup /etc/group     //查询group文件中lbgroup组是否建立
#groupadd -r syslbgroup       //建立系统组账号
# grep lbgroup /etc/group     //查询group文件中
                             syslbgroup组是否建立
```

5. 组账号修改

groupmod命令用来更改群组识别码或名称。该命令的语法格式为：

```
groupmod [-g <群组识别码> <-o>][-n <新  
群组名称>][群组名称]
```

命令中所使用的参数说明如下：

- Ø -g <群组识别码> 设置欲使用的群组识别码。
- Ø -o 重复使用群组识别码。
- Ø -n <新群组名称> 设置欲使用的群组名称。

下面举例说明该命令的使用方法:

# grep lbgroup /etc/group	// 查询 group 文件中 lbgroup 组属性
# groupmod -g 503 lbgroup	// 改变 lbgroup 组的 GID 为 503
# grep lbgroup /etc/group	// 查询操作结果是否正确
# groupmod -n ydgroup lbgroup	// 改变 lbgroup 组名为 ydgroup
# grep 503 /etc/group	// 查询操作结果是否正确

6. 删除组账号

groupdel命令用于删除指定的组账号，若该群组中仍包括某些用户，则必须先删除这些用户后，方能删除群组。该命令的语法格式为：

```
groupdel [群组名称]
```

7. 口令维护命令

出于系统安全考虑，Linux系统中的每一个用户除了有其用户名外，还有其对应的用户口令。因此使用useradd命令增加时，还需使用passwd命令为每一位新增加的用户设置口令；用户以后还可以随时用passwd命令改变自己的口令。该命令的一般格式为：

```
passwd [用户名]
```

其中用户名为需要修改口令的用户名。只有超级用户可以使用“passwd 用户名”修改其他用户的口令，普通用户只能不带参数的passwd命令修改自己的口令。

另外，passwd命令还可以使用一些参数选项，这些参数选项可对账号的口令进行不同的操作，但这些带参数的passwd命令只有root用户可以使用。这些参数选择包括：

Ø -S：用于查询指定用户账号的状态。

Ø -l：用于锁定账号的口令。

Ø -u：解除锁定账号的口令。

Ø -d：删除指定账号的口令。

8. 组中用户成员的维护

gpsswd命令可用于把一个账户添加到组、把一个账户从组中删除、把一个账户设为组管理员。

(1) 添加用户到使用的命令格式为:

```
gpsswd -a 用户账号名 组账号名
```

(2) 从组中删除用户的命令格式为:

```
gpsswd -d 用户账号名 组账号名
```

(3) 设置用户为组管理员的命令格式为:

```
gpsswd -A 组管理员用户列表 用户组
```

2.3 用户和组的状态命令

1. id命令

id命令用于显示用户当前的UID，gid以及所属群组的组列表该指令的语法格式为：

id [选项] [用户名称]

该命令所使用的选项参数说明如下：

- Ø -g: 显示用户所属群组的ID。
- Ø -G: 显示用户所属附加群组的ID。
- Ø -n: 显示用户，所属群组或附加群组的名称。
- Ø -r: 显示实际ID。
- Ø -u: 显示用户ID。

2. whoami命令

whoami命令用于显示登录者自身的用户名称，本指令相当于执行“id -un”指令。

3. su命令

su命令是用来将当前用户转换为其他用户身份。其命令的语法格式为：

```
su [-flmp] [-][ -c <指令> ][ -s ] [用户帐号]
```

需要指出的是su命令可让用户暂时变更登入的身份。变更时须输入所要变更的用户账号与密码。该命令中的选项参数说明如下：

- Ø -c<指令>: 执行完指定的指令后, 即恢复原来的身份。
- Ø -f: 适用于csh与tsch, 使shell不用去读取启动文件。
- Ø -: 改变身份时, 也同时变更工作目录, 以及HOME, SHELL, USER, LOGNAME。此外, 也会变更PATH变量。
- Ø -m, -p: 变更身份时, 不要变更环境变量。
- Ø -s: 指定要执行的shell。

[用户帐号]: 指定要变更的用户。若不指定此参数, 则预设变更为root。

4. groups命令

groups命令用于显示指定用户所属的组, 如未指定用户则显示当前用户所属的组。该命令的语法格式为:

```
groups 用户名
```

3 图形用户管理工具

- 用户和组群概述
- 添加新用户
- 修改用户属性
- 添加新组群
- 修改组群属性

用户和组群概述

- 用户和组群 允许你查看、修改、添加和删除本地用户和组群。
- 要使用 用户和组群，你必须运行 X 窗口系统，具备根特权，并且安装了 **system-config-users RPM** 软件包。要从桌面启动 用户管理器，点击面板上的「系统」 => 「用户和组群」，或在 **shell** 提示（如 **XTerm** 或 **GNOME 终端**）下键入 **system-config-users** 命令。

用户和组群窗口



添加新用户

用户名:	<input type="text" value="zhangsan"/>
全称:	<input type="text" value="Zhang San"/>
口令:	<input type="password" value="*****"/>
确认口令:	<input type="password" value="*****"/>
登录 Shell:	<input type="text" value="/bin/bash"/> 
<input checked="" type="checkbox"/> 创建主目录	
主目录:	<input type="text" value="/home/zhangsan"/>
<input checked="" type="checkbox"/> 为该用户创建私人组群	
<input type="checkbox"/> 手工指定用户 ID	
UID:	<input type="text" value="500"/>  
<div> 取消(C)</div> <div> 确定(O)</div>	

修改用户属性

用户数据(U)	帐号信息(A)	口令信息(P)	组群(G)
用户名:	<input type="text" value="zhangsan"/>		
全称:	<input type="text" value="Zhang San"/>		
口令:	<input type="password" value="*****"/>		
确认口令:	<input type="password" value="*****"/>		
主目录:	<input type="text" value="/home/zhangsan"/>		
登录 Shell:	<input type="text" value="/bin/bash"/> 		
<div> 取消(C)  确定(O)</div>			

用户属性窗口

- 用户数据 — 显示在你添加用户时配置的基本用户信息。使用这个标签来改变用户的全称、口令、主目录或登录 **shell**。
- 账号信息 — 如果你想让账号到达某一固定日期时过期，选择「启用账号过期」。在提供的字段内输入日期。选择「用户账号已被锁」来锁住用户账号，从而使用户无法在系统登录。
- 口令信息 — 这个标签显示了用户口令最后一次被改变的日期。要强制用户在一定天数之后改变口令，选择「启用口令过期」。你还可以设置允许用户改变口令之前要经过的天数，用户被警告去改变口令之前要经过的天数，以及账号变为不活跃之前要经过的天数。
- 组群 — 选择你想让用户加入的组群以及用户的主要组群。

添加新组群

文件(E) 首选项(P) 帮助(H)

 添加用户(U)

 添加组群(G)

 属性(T)

 删除(D)

 帮助(H)

 刷新(R)

搜索过滤器: 应用过滤器

用户 组群


用户名	用户 ID ▼	主要组群	全称	登录 Shell	主目录
zhangsan	500	zhangsan	Zhang San	/bin/bash	/home/zhangsan

组群名:

☐ 手工指定组群 ID

GID:

 取消(C)

 确定(O)

修改 组群 属性

组群数据(D)

组群用户(U)

组群名:

 取消(C)

 确定(O)

本章思考题

- **Linux**系统是如何标识用户和组的？
- 什么是标准组？什么是私有组？**Red Hat**为什么使用了私有组？
- 简述**Linux**的四个账户系统文件及其各个字段的含义？
- 举例说明如何创建一个用户账号？
- 举例说明如何将一个用户账号添加到一个当前还不存在的组中？
- 如何设置用户口令？如何锁定用户账号？
- **Linux**文件系统的三种基本权限为何？
- **Linux**文件系统的三种特殊权限为何？何时使用它们？
- 如何更改文件或目录的属主和/或同组人？
- 简述三种特殊权限及其设置方法？

进程的定义

- **Linux**系统上所有运行的程序都可以称之为一个进程。
- **Linux**用分时管理方法使所有的任务共同分享系统资源。
- 和程序的区别？

进程状态

- **ps (Process Status)**
- 功能
 - 进程执行的状态
 - 进程是否结束、进程有没有僵死
 - 哪些进程占用了过多的系统资源等

ps格式

- **-e (或者-A)**
 - **all processes**
- **-a**
 - **all w/ tty except session leaders**
- **a**
 - **all w/ tty, including other users**
- **-u**
 - **by effective user ID (supports names)**
- **X**
 - **processes w/o controlling ttys**

ps例子

- **ps**
- **ps -e**
- **ps aux**
- **ps | grep vi**
- **pstree**

结束进程

- why?
 - 进程占用的**CPU**时间过多
 - 进程已经挂死
- 中断一个前台进程
 - **<Ctrl+c>**
- 通用命令: **kill**
 - **kill -9 pid**
 - **killall -9 process_name**

前台和后台进程

- 前台

- 指一个程序控制着标准输出和标准输入。

- 后台

- 指一个程序不从标准输入接受输入，一般也不将结果输出到标准输出上。

后台

- **&**
 - Ctrl+Z、Ctrl+D、Ctrl+C、bg、fg、jobs
- **nohup (No-Hang-Up不挂起) :**
 - nohup 命令 [参数] 输出文件 &
- **at**
 - 在指定时间候执行命令
- **cron**
 - 安排周期性任务

查看登录用户及日志文件信息

识别Linux中的用户

1. 查看用户的操作

系统管理员在任一时刻都可查看用户的行为，在终端的提示符下输入w命令即可

命令响应中所示的信息分别说明如下：

第一行显示系统的汇总信息，字段分别表示系统当前时间、系统运行时间、登录用户总数及系统平均负载信息。对于该行显示的几个数据意义是：

Ø 4:50pm 表示执行w的时间是在下午4:50。

Ø 0days, 11:18 表示系统运行0天11小时18分。

Ø 4users 表示当前系统登录用户总数为4

Ø load average 与后面的数字一起表示系统在过去1、5、10分钟内的负载程度，数值越小，系统负载越轻。

查看日志文件系统

日志文件（Log files）是包含关于系统消息的文件，包括内核、服务、在系统上运行的应用程序等。不同的日志文件记载不同的信息。

1. 定位日志文件

多数日志文件位于 `/var/log` 目录中。某些程序如 `httpd` 和 `samba` 在 `/var/log` 中有单独的存放日志文件的目录。

2. 日志文件被循环使用

本章思考题

- 什么是进程？它与程序有何关系？
- 简述进程的类型和进程的启动方式？
- 如何查看进程？如何删除进程？