第 3 章

用户和组管理

由于 Linux 支持多用户使用，当多个用户登录使用同一个 Linux 系统时，需要对各个用户进行管理，以保证用户文件的安全存取。

本章主要介绍如何对 Linux 中的用户和用户组进行管理，包括用户和组的重要配置文件、使用命令行方式和使用用户管理器 3 种方法进行用户和用户组的管理。

教学目标

- 了解用户和组群配置文件。
- 熟练掌握 Linux 下用户和组的创建与维护管理。
- 熟悉用户账户管理器的使用方法。

3.1 什么是用户

在 Linux 系统中，每个用户都拥有一个唯一的标识符，称为用户 ID(UID)。Linux 系统中的用户至少属于一个组，称为用户分组。用户分组是由系统管理员建立的，一个用户分组内包含若干个用户，一个用户也可以归属于不同的分组。用户分组也有一个唯一的标识符，称为分组 ID(GID)。对某个文件的访问都是以文件的用户 ID 和分组 ID 为基础的。同时根据用户和分组信息可以控制如何授权用户访问系统，以及允许访问后用户可以进行的操作权限。

用户的权限可以被定义为普通用户或超级用户，超级用户也被称为 root 用户。普通用户只能访问自己的文件和其他有权限访问的文件，而超级用户权限最大，可以访问系统的全部文件并执行任何操作。一般系统管理员使用的是超级用户 root，有了这个账号，管理员可以突破系统的一切限制，方便地维护系统。普通用户也可以用 su 命令使自己转变为超级用户。

系统的这种安全机制有效地防止了普通用户对系统的破坏。例如，存放于/dev 目录下的设备文件分别对应于硬盘驱动器、打印机、光盘驱动器等硬件设备，系统通过对这些文件设置用户访问权限，使普通用户无法通过覆盖硬盘面破坏整个系统，从而保护了系统。

在 Linux 中可以利用用户配置文件以及用户查询和管理的控制工具来进行用户管理，用户管理主要通过修改用户配置文件完成。用户管理控制工具最终也是为了修改用户配置文件，所以在进行用户管理时，直接修改用户配置文件一样可以达到用户管理的目的。

与用户相关的系统配置文件主要有/etc/passwd 和/etc/shadow，其中/etc/shadow 是用户信息的加密文件，比如用户的密码、口令的加密保存等；/etc/passwd 和/etc/shadow 文件是互补的，下面对这两个文件进行介绍。

3.1.1　用户账号文件/etc/passwd

/etc/passwd 是系统识别用户的一个文件，用来保存用户的账号数据等信息，又被称为密码文件或口令文件。系统所有用户都在此文件中有记载。例如，当用户以 student 这个账号登录时，系统首先会查阅/etc/passwd 文件，看是否有 student 这个账号，然后确定 student 的 UID，通过 UID 来确认用户和身份。如果存在，则读取 /etc/shadow 影子文件中所对应的 student 的密码；如果密码核实无误，则登录系统，读取用户的配置文件。

用户登录进入系统后都有一个属于自己的操作环境，可以执行 cat 命令查看完整的系统账号文件。假设当前用户以超级用户身份登录，执行下列命令：

```
[root@localhost ~]# cat /etc/passwd
```

可得到/etc/passwd 文件的内容，如图 3-1 所示。

图 3-1　查看/etc/passwd 文件

在/etc/passwd 中，每一行表示的是一个用户的信息，一行有 7 个域，每个域用冒号(:)分隔。下面是一个实际用户的例子。

```
student:x:1000:1000:student:/home/student:/bin/bash
```

该用户各项基本信息的含义如下。

第 1 字段：用户名(也被称为登录名)。在上面的例子中,用户的用户名是 student。

第 2 字段：口令。在例子中看到的是一个 x,密码已被映射到/etc/shadow 文件中。

第 3 字段：UID。用户的 ID。0 是 root 用户,1～999 为系统用户,1000＋为普通用户。

第 4 字段：GID。用户所属组 ID 为 1000 的组的名字。

第 5 字段：用户名全称。这是可选的,可以不设置,在此用户中,用户的全称是 student。

第 6 字段：用户的登录目录所在位置。student 这个用户是/home/student。

第 7 字段：用户所用 Shell 的类型。此例为/bin/bash。如果是系统用户不允许登录,需要设置 Shell 为/sbin/nologin。

在以上字段中,用户的登录名是用户自己选定的,主要是方便记忆,可以由一串具有特定含义的字符串组成。

用户的口令在此文件不会显示,因为用户的口令是加密存放的,一般采用的是不可逆加密算法。当用户登录输入口令后,系统会对用户输入的口令进行加密,再把加密的口令与机器中存放的用户口令进行比对。如果这两个加密数据匹配,则允许用户进入系统。

在/etc/passwd 文件中,UID 字段信息也非常重要。UID 是用户的 ID 值,在系统中每个用户的 UID 的值是唯一的,更确切地说,每个用户都要对应一个唯一的 UID,系统管理员应该确保这一规则。系统用户的 UID 值从 0 开始,是一个正整数。UID 的最大值可以在文件/etc/login.defs 中查到,RHEL7 规定为 60000。在 Linux 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,用户登录系统所处的角色是通过 UID 来实现的,而非用户名。让几个用户共用一个 UID 是危险的,比如把普通用户的 UID 改为 0,和 root 共用一个 UID,这就造成了系统管理权限的混乱。Linux 预留了一定的 UID 和 GID 给系统虚拟用户占用,虚拟用户一般是系统安装时就有的,是为了完成系统任务所必需的用户,但虚拟用户是不能登录系统的,比如 ftp、nobody、adm、rpm、bin、shutdown 等。

每一个用户都需要保存自己的配置文件,保存的位置即用户登录子目录,在这个子目录中,用户不仅可以保存自己的配置文件,还可以保存自己日常工作中的各种文件。出于一致性考虑,一般都把用户登录子目录安排在/home 下,名称为用户登录使用的用户名。用户可以在账号文件中更改用户登录子目录。

3.1.2 用户影子文件/etc/shadow

Linux 使用了不可逆算法来加密登录口令,所以黑客从密文得不到明文。但由于/etc/passwd 文件是任何用户都有权限读取的,所以用户口令很容易被黑客盗取。针对这种安全问题,Linux 使用影子文件/etc/shadow 来提高口令的安全性。

使用影子文件是将用户的加密口令从/etc/passwd 中移出,保存在只有超级用户 root 才有权限读取的/etc/shadow 中,/etc/passwd 中的口令域显示一个“x”。

/etc/shadow 文件是/etc/passwd 的影子文件,这个文件并不是由/etc/passwd 产生的,这两个文件是对应互补的。/etc/shadow 文件的内容包括用户、被加密的密码,以及其他/etc/passwd 不能包括的信息,比如用户的有效期限等,如图 3-2 所示。

图 3-2　查看/etc/shadow 文件

/etc/shadow 文件的内容包括 9 个字段。

①name ②password ③lastchange ④minage ⑤maxage ⑥warning ⑦inactive ⑧expire ⑨blank

说明如下。

① name：登录名称。

② password：已被加密的用户口令，密码字段开头为感叹号时，表示该密码锁定。

③ lastchange：最近一次修改口令的时间。以距离 1970 年 01 月 01 日的天数表示。

④ minage：两次修改口令间隔最少的天数。如果设置为 0，表示无最短期限要求。

⑤ maxage：必须更改密码的最多天数。

⑥ warning：密码到期警告。以天数表示，0 表示不警告。

⑦ inactive：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，也就是说系统不能再让此用户登录，也不会提示用户过期，是完全禁用。

⑧ expire：用户过期日期。从 1970 年 1 月 1 日开始的天数，字段为空，则账号永久可用。

⑨ blank：保留字段。未使用。

3.1.3　组账号文件/etc/group

具有某种共同特征的用户集合起来就是用户组(Group)。用户组的设置主要是为了方便检查，设置文件或目录的访问权限。每个用户组都有唯一的用户组号 GID。

/etc/group 文件是用户组的配置文件，内容包括用户和用户组，并且能显示出用户归属哪个用户组或哪几个用户组。同一用户组的用户之间具有相似的特征，比如，把某一用户加入到 info 用户组，那么这个用户就可以浏览 info 用户登录目录的文件。如果 info 用户把某个文件的读/写执行权限开放，info 用户组的所有用户都可以修改此文件，如果是可执行的文件(比如脚本)，info 用户组的用户也是可以执行的。

/etc/group 的内容包括用户组名、用户组口令、GID 及该用户组所包含的用户，每个用

户组一条记录。格式如下：

```
Group_ name:passwd:GID:user_list
```

在/etc/group 中的每条记录分 4 个字段。第 1 字段：用户组名称；第 2 字段：用户组密码；第 3 字段：GID；第 4 字段：用户列表，每个用户之间用逗号“,”分隔，本字段可以为空，如果字段为空，表示用户组为 GID 的全部用户。

通过执行 cat/etc/group 命令，可以得到/etc/group 文件的内容，如图 3-3 所示。

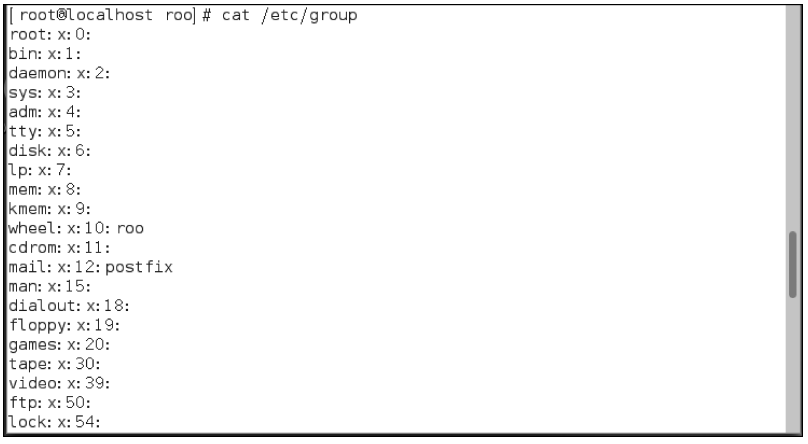

图 3-3　查看/etc/group 文件

下面举例说明/etc/group 的内容。

root:x:0:root 表示用户组名为 root；x 是已加密的密码段；GID 是 0；root 用户组下包括 root 用户。

GID 和 UID 类似，是一个从 0 开始的正整数。root 用户组的 GID 为 0，系统会预留一些较靠前的 GID 给系统虚拟用户使用。

对照/etc/passwd 和/etc/group 两个文件，会发现在/etc/passwd 中的每条用户记录有用户默认的 GID。在/etc/group 中，也会发现每个用户组下有多少个用户。在创建目录和文件时，会使用默认的用户组。

需要注意的是，判断用户的访问权限时，默认的 GID 并不是最重要的，只要一个目录让同组用户具有可以访问的权限，那么同组用户就可以拥有该目录的访问权。

3.1.4　用户组影子文件/etc/gshadow

与/etc/shadow 文件一样，考虑到组信息文件中口令的安全性，引入相应的组口令影子文件/etc/gshadow。

/etc/gshadow 是/etc/group 的加密文件，比如用户组管理密码就存放在这个文件中。/etc/gshadow 和/etc/group 是互补的两个文件。对于大型服务器，针对很多用户和组，定制一些关系结构比较复杂的权限模型，设置用户组密码是极有必要的。例如，如果不想让一些非用户组成员永久拥有用户组的权限和特性，可以通过密码验证的方式让某些用户临时拥有一些用户组特性，这时就要用到用户组密码。

/etc/gshadow 格式如下，每个用户组独占一行。

```
groupname:password:admin,admin,...:member,member,...
```

第 1 字段：用户组；第 2 字段：用户组密码，这个字段可以是空的或“!”，如果是空的或有“!”，表示没有密码；第 3 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，用逗号“,”分隔；第 4 字段：组成员，如果有多个成员，用逗号“,”分隔。

执行 cat /etc/gshadow 命令，可以查看用户组影子文件的内容，如图 3-4 所示。

图 3-4　查看/etc/gshadow 文件

下面举例说明/etc/gshadow 的内容。

例如，student:!:::，其用户组名为 student，没有设置密码，该用户没有用户组管理者，没有组成员。

3.2　用户管理

Linux 提供了 useradd、passwd、userdel 和 usermod 等 Shell 命令来管理用户，下面分别进行介绍。

3.2.1　添加用户

1. useradd 命令

格式：

```
useradd [选项] 用户名
```

功能：添加用户账号或更新创建用户的默认信息。

常用选项说明：

-n　用于禁止系统建立与用户名同名的用户组。

-s　设置用户的登录 Shell,默认为/bin/bash。

-g 组群名　定义用户默认的组名或组号码(初始组),该组在指定前必须存在。

-G 组群列表　设置新用户到其他组中(附属组),该组在指定前必须存在。

-u UID　指定用户 ID,不使用系统默认的设置方式。

-d 路径　用于取代默认的/home/username 主目录。

-e 日期　禁用账号的日期,格式为 YYYY-MM-DD。

-f 天数　口令过期后,账号禁用前的天数,若指定为 1,则口令过期后,账号将不会禁用。

2. passwd 命令

格式:

```
passwd[选项][用户名]
```

功能:设置或修改用户的口令,以及口令的属性。

常用选项说明:

-d 用户名　删除用户的口令,则该用户账号无需口令就可以登录系统。

-l 用户名　暂时锁定指定的用户账号。

-u 用户名　解除指定用户账号的锁定。

-S 用户名　显示指定用户账号的状态。

3.2.2　删除用户

格式:

```
userdel[选项]用户名
```

功能:删除指定的用户账号,只有超级用户才可以使用该命令。

常用选项说明:

-r　删除用户时删除用户的主目录及其中的所有内容,如果不加此选项,则仅删除此用户账号。

一般情况下,用户只有对自己主目录有写权限,主目录被删除后,其相关的文件也被删除。但有时系统对用户开放了其他目录的写权限,删除用户时非用户主目录下的用户文件并不会被删除,这时必须使用 find 命令来搜索删除这些文件。

利用 find 命令中的-user 和-uid 选项可以很方便地找到属于某个用户的文件。命令如下:

```
[root@localhost ~]# find / -user user1
```

或

```
[root@localhost ~]#find / -uid user1
```

上述命令是从根目录开始查找系统中所有属于用户 user1 的文件。

3.2.3　修改用户信息

格式：

```
usermod[选项]用户名
```

功能：修改用户账号信息。可以修改的信息与 useradd 命令所添加的信息一致，包括用户主目录、私有组、登录 Shell 等内容。只有超级用户才可以使用该命令。

该命令使用的参数和 useradd 命令使用的参数一致，这里不再一一描述。下面举例说明 usermod 命令的使用。

3.3　组管理

3.3.1　创建用户组

格式：

```
groupadd[选项]组群名
```

功能：创建用户组群，只有超级用户才可以使用该命令。

常用选项说明：

-g GID　组 ID 值。除非使用-o 参数，否则该值必须唯一，预设为不小于 1000 的正整数，而且逐次增加。数值 0～999 是保留给系统账号使用的。

-o　配合-g 选项使用，可以设定不唯一的组 ID 值。

-r　此参数用来建立系统账号。

-f　新增加一个已经存在的组账号时，系统会出现错误信息然后结束命令。如果新增组的 GID 已经存在，可以结合使用-o 选项成功创建。

用户组的密码可以通过 passwd 命令来实现。passwd 的用法如下：

```
passwd用户组名
```

例如，执行下列命令：

```
[root@localhost ～]# gpasswd mylinux
```

按下 Enter 键后，根据提示输入两次密码即可。

3.3.2　删除用户组

格式：

```
groupdel组群名
```

功能：删除指定的组群，只有超级用户才可以使用该命令。

使用 groupdel 命令时，首先要确认被删除的用户组存在。另外，如果有一个属于待删除组的用户正在使用系统，则不能删除该组，必须先删除其中的用户后再执行组的删除操作。

3.3.3 修改用户组信息

格式：

```
groupmod[选项]组群名
```

功能：修改指定组群的属性，只有超级用户才可以使用该命令。

常用选项说明：

-g GID　组 ID 值。该值必须唯一，除非使用-o 参数。

-o　配合-g 选项使用，可以设定不唯一的组 ID 值。

-n 组群名　更改组名。

3.4 使用用户管理器管理用户和组

在 Linux 中除了可以利用命令行对用户和组进行管理外，还可以使用具有图形用户界面的用户管理器来查看、修改、添加和删除用户和组。与命令行管理方式相比，图形界面具有简单、直观的特点。下面介绍 Linux 的用户管理器。

3.4.1 启动用户管理器

要使用用户管理器，必须安装 system-config-users-1.3.5-2.el7.noarch rpm 软件包。执行下列命令即可安装，如图 3-5 所示。

```
[root@localhost ~]#yum install -y system-config-users-1.3.5-2.el7.noarch rpm
```

```
[root@localhost ~]# yum install -y system-config-users-1.3.5-2.el7.noarch rpm
已加载插件：fastestmirror, langpacks
dvd                                                      | 3.6 kB     00:00
Loading mirror speeds from cached hostfile
软件包 rpm-4.11.1-16.el7.x86_64 已安装并且是最新版本
正在解决依赖关系
--> 正在检查事务
---> 软件包 system-config-users.noarch.0.1.3.5-2.el7 将被 安装
--> 正在处理依赖关系 system-config-users-docs，它被软件包 system-config-users-1.
3.5-2.el7.noarch 需要
--> 正在检查事务
---> 软件包 system-config-users-docs.noarch.0.1.0.9-6.el7 将被 安装
--> 正在处理依赖关系 rarian-compat，它被软件包 system-config-users-docs-1.0.9-6.
el7.noarch 需要
--> 正在检查事务
---> 软件包 rarian-compat.x86_64.0.0.8.1-11.el7 将被 安装
--> 正在处理依赖关系 rarian = 0.8.1-11.el7，它被软件包 rarian-compat-0.8.1-11.el
7.x86_64 需要
--> 正在处理依赖关系 rarian，它被软件包 rarian-compat-0.8.1-11.el7.x86_64 需要
--> 正在处理依赖关系 librarian.so.0()(64bit)，它被软件包 rarian-compat-0.8.1-11.
el7.x86_64 需要
--> 正在检查事务
---> 软件包 rarian.x86_64.0.0.8.1-11.el7 将被 安装
--> 解决依赖关系完成
```

图 3-5　安装界面

```
依赖关系解决

================================================================================
 Package                  架构          版本                源          大小
================================================================================
正在安装:
 system-config-users      noarch        1.3.5-2.el7         dvd        337 k
为依赖而安装:
 rarian                   x86_64        0.8.1-11.el7        dvd         98 k
 rarian-compat            x86_64        0.8.1-11.el7        dvd         66 k
 system-config-users-docs noarch        1.0.9-6.el7         dvd        308 k

事务概要
================================================================================
安装  1 软件包 (+3 依赖软件包)

总下载量：809 k
安装大小：3.9 M
Downloading packages:
--------------------------------------------------------------------------------
总计                                              510 kB/s | 809 kB  00:01
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  正在安装     : rarian-0.8.1-11.el7.x86_64                                 1/4
  正在安装     : rarian-compat-0.8.1-11.el7.x86_64                          2/4
  正在安装     : system-config-users-1.3.5-2.el7.noarch                     3/4
  正在安装     : system-config-users-docs-1.0.9-6.el7.noarch                4/4
  验证中       : rarian-compat-0.8.1-11.el7.x86_64                          1/4
  验证中       : system-config-users-1.3.5-2.el7.noarch                     2/4
  验证中       : rarian-0.8.1-11.el7.x86_64                                 3/4
  验证中       : system-config-users-docs-1.0.9-6.el7.noarch                4/4

已安装:
  system-config-users.noarch 0:1.3.5-2.el7

作为依赖被安装:
  rarian.x86_64 0:0.8.1-11.el7
  rarian-compat.x86_64 0:0.8.1-11.el7
  system-config-users-docs.noarch 0:1.0.9-6.el7

完毕！
```

图　3-5(续)

有两种方法可以启动用户管理器。一种方法是在桌面环境下选择“应用程序”→“杂项”→“用户和组群”菜单命令来显示用户管理器界面，如图 3-6 所示。另一种方法是以超级用户 root 登录，执行以下命令：

```
[root@localhost ~]# system-config-users
```

图 3-6　启动用户管理器