项 目 5

Linux 用户管理

Linux 操作系统的典型特点之一是安全，对用户和用户组的严格管理对于合理分配系统资源、提升系统服务、保障系统安全都是至关重要的。

在本项目中，将通过完成两个具体任务：用户管理、用户组管理，来系统学习 Linux 中的用户和用户组的管理，包含用户和组的基础知识，配置文件，添加修改删除用户，设置用户密码，添加、修改、删除用户组，用户身份切换等。通过任务的实践，读者将能够全面而综合地使用 Linux 中用户和用户组的管理命令。

【学习目标】

知识目标

1. 掌握用户 ID(UID)和组 ID(GID)的概念及其作用。
2. 掌握用户文件/etc/passwd 和用户影子文件/etc/shadow 的结构和内容。
3. 掌握主组和附加组的作用和区别。
4. 掌握用户组管理文件/etc/group 的结构和内容。
5. 掌握 sudo 命令的作用及其配置文件/etc/sudoers 的使用方法。

能力目标

1. 使用 useradd 命令创建新用户账号，并为其设置属性。
2. 使用 passwd 命令管理用户密码等信息。
3. 使用 usermod 命令修改用户账号的属性。
4. 使用 userdel 命令删除用户账号。
5. 使用 groupadd 命令创建新用户组，并为其设置属性。
6. 使用 groupmod 命令修改用户组的属性。
7. 使用 groupdel 命令删除用户组。
8. 使用 sudo 命令以超级用户身份执行命令。

素质目标

1. 培养系统管理中的安全意识。
2. 了解并遵守行业相关的安全政策和合规性要求。
3. 培养保护和尊重隐私的意识。

【建议学时】

4 学时。

任务 1　用 户 管 理

【任务提出】

Linux 在运维过程中需要用户才可以登录使用，现需要新增一个临时用户 ceshi，设置密码允许其登录系统进行代码测试，测试完成后再将 ceshi 用户删除。

【任务分析】

首先，根据需求中用户的属性新增用户，也可以重新修改用户的属性；其次，设置新增用户的密码；再次，可以退出系统使用新增用户和密码登录系统，也可以基于当前用户切换到新增用户，完成代码测试工作；最后，将新增用户删除，并检查是否删除完成。具体的任务实施分析如下。

1. 新增用户。
2. 设置新增用户的密码。
3. 使用新增用户登录系统。
4. 删除新增用户。

【知识准备】

5.1　用户基础知识

5.1.1　用户分类

Linux 是多用户多任务的分时操作系统，允许不同的用户从本地或远程登录，并同时访问文件。每个用户都拥有唯一的用户名和密码。输入正确的用户名和密码后，才能登录系统，如图 5.1 所示。

Linux 的用户分为 3 类：超级用户、系统用户和普通用户。

- 超级用户：用户名为 root，具有一切权限，但是只在系统维护（如创建账号）或其他必要情况下才使用超级用户登录，以避免系统出现安全问题。
- 系统用户：是 Linux 系统正常工作所必需的内建用户，主要是为了满足相应的系统进程对文件属性的要求而建立的，系统用户不能用来登录，如 bin、daemon、adm、lp

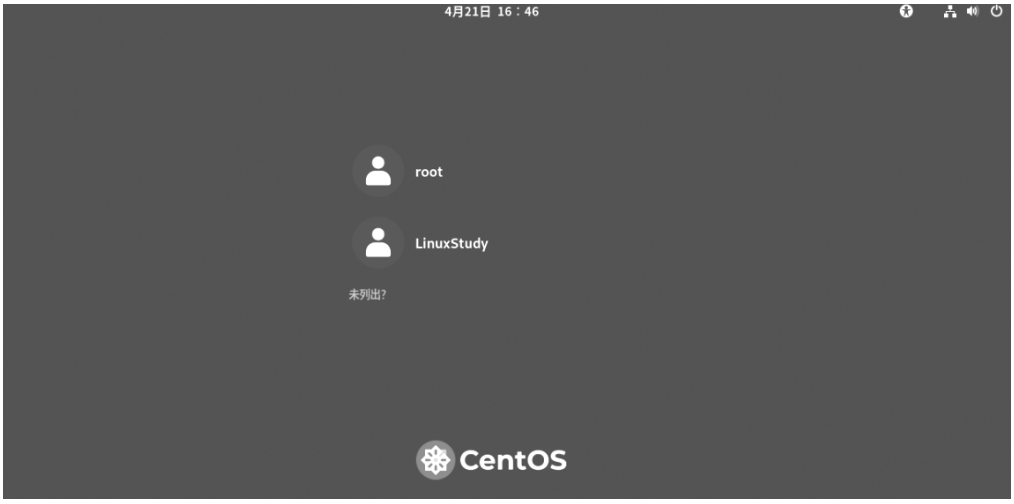

图 5.1 用户登录界面

等用户。

- 普通用户：用于登录管理和应用的用户，使用命令创建的用户均属于普通用户。

5.1.2 UID 和 GID

每个用户都有一个唯一标识码，称为 UID。在 CentOS Stream 9 中，超级用户 root 的 UID 为 0；系统用户的 UID 一般为 1～999；普通用户的 UID 为 1000～60000。

一般情况下，创建用户的同时也会创建一个与用户同名的组，该组是用户的主组。组的唯一标识码称为 GID，默认值为 1000～60000。使用 id 命令可以查看用户有关的 ID 信息。

命令名称：id

使用方式：id [选项] [--help] [--version] [用户名]

说明： 用于显示用户的 ID，以及所属群组的 ID。

参数：

-Z：只输出当前用户的安全上下文。

-g，--group：显示用户所属的组 ID。

-G，--groups：显示用户所属附加组的 ID。

-n，--name：显示用户、组的名称。

-r，--real：显示真实 ID 而不是有效 ID。

-u，--user：显示有效 ID。

--help：显示帮助信息。

--version：显示版本信息。

例 5.1 查看当前用户的 id 信息

```
[linuxstudy@LinuxServer ~]$id
用户 id=1000(linuxstudy) 组 id=1000(linuxstudy) 组=1000(linuxstudy) 上下文=
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[linuxstudy@LinuxServer ~]$su root
```

```
密码：
[root@LinuxServer linuxstudy]#id
用户 id=0(root) 组 id=0(root) 组=0(root) 上下文=unconfined_u:unconfined_r:
unconfined_t:s0-s0:c0.c1023
```

说明：上述结果中，uid 就是用户名对应的 ID，gid 就是用户所属组对应的 ID。su 命令用来切换用户，实验证明，切换账号后 UID 和 GID 发生了改变。root 的 UID 和 GID 都是 0。

每个文件都有一个所有者，表示该文件是谁创建的，所有者使用 UID 表示，同时还有一个组编号 GID，表示该文件所属的组，一般为文件所有者所属的组。除了 id 命令以外，还可以通过查找配置文件的方式查看某账户的 UID 与 GID。

例 5.2 查看/etc/passwd 文件中 linuxstudy 用户的信息。

```
[root@LinuxServer /]    #grep 'linuxstudy' /etc/passwd
linuxstudy:x:1000:1000:LinuxStudy:/home/linuxstudy:/bin/bash
```

说明：/etc/passwd 文件中的第 3 列是 UID，第 4 列是 GID，该文件将在 5.2 节详细介绍。

5.2 配置文件

用户(User)和用户组(Group)的配置文件是系统管理员应该掌握的基础文件之一，合格的系统管理员应该对用户和用户组配置文件有比较透彻的了解。

用户和组相关的 4 个配置文件是：①用户信息文件/etc/passwd；②用户密码信息文件/etc/shadow；③用户组信息文件/etc/group；④用户组加密信息文件。用户与组的创建、删除、修改等操作就是针对这几个配置文件的操作。下面详细讲解这四个配置文件。

5.2.1 /etc/passwd

/etc/passwd 文件存储用户相关信息，每个用户都在/etc/passwd 文件中有一个与之相对应的记录行。/etc/passwd 文件对任何用户都是可读的，但只有 root 拥有其写权限。

例 5.3 使用 root 用户查看/etc/passwd 文件的前 3 行。

```
[root@LinuxServer ~]    #head -3 /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
```

说明：在/etc/passwd 中，每行有 7 个字段；各字段之间用“：”分隔。

1) 第一字段：用户名

在不包括路径的情况下，Linux 中用户名一般不超过 32 个字符，由大写字母、小写字母或数字组成，用户名中不能包含特殊字符。

2) 第二字段：口令占位符

x 表示口令占位符，代表算法加密，Linux 中使用最广泛的加密方式是 MD5，口令存放

在/etc/shadow 中。

3）第三字段：UID

UID 是唯一表示某用户的数字标识。如果多个用户名对应同一个 UID，则 Linux 内核会将其解析成同一个账号，但它们可以拥有不同的口令，登录之后使用不同的主目录和登录不同的 Shell。用户名是给计算机使用者看的，Linux 内核真正识别的是 UID。

4）第四字段：GID

记录用户所属组的 ID 简称为 GID，GID 对应/etc/group 中的一条记录。

5）第五字段：用户名全称

用于解释用户名，此项配置是可选的。该字段没有实际意义，旨在对用户名进行解释与标注，除了用户名全称以外，还可以存储姓名、地址、电话号码等信息，finger 命令用于修改用户信息并保存到该字段。

6）第六字段：主目录

用户主目录所在位置，root 的主目录是/root，所以当 root 登录之后会立刻登录到/root 目录。用户可根据需要修改该字段，将账号的主目录移动到硬盘的其他位置。linuxstudy 用户的主目录是/home/linuxstudy，在创建普通账户时，默认在/home 目录下创建同名主目录。

7）第七字段：用户所用 Shell

用户登录后需要启动一个进程，负责将用户的操作传递给内核，这个进程就是用户登录到系统后的命令解释器或命令翻译程序，称为 Shell，Shell 是用户与 Linux 系统之间交互的接口，默认是/bin/bash，系统用户的 Shell 默认是/sbin/nologin。

5.2.2 /etc/shadow

/etc/shadow 文件是/etc/passwd 的影子文件，二者之中的记录行一一对应。该文件不是由/etc/passwd 生成的，而是由 pwconv 命令根据/etc/passwd 文件中的数据字段生成的，两个文件是对应互补的。shadow 文件的内容包括被加密的密码以及其他/etc/passwd 不能包括的信息，如用户的有效期限等。

/etc/shadow 文件只有 root 用户可以操作，其他用户没有权限操作，这样就保证了用户密码的安全。普通用户查看该文件将会被提示权限不够。

例 5.4 使用 linuxstudy 用户查看/etc/shadow 文件。

```
[linuxstudy@LinuxServer ~]$ls -l /etc/shadow
----------. 1 root root 1246 5月  15 17:38 /etc/shadow
[linuxstudy@LinuxServer ~]$cat /etc/shadow
cat: /etc/shadow: 权限不够
```

说明：使用 ls -l /etc/shadow 查看该文件，权限为空，代表除了文件的拥有者 root 之外，其他人不能进行读、写、执行等操作，所以在 linuxstudy 用户查看文件时会提示权限不够。

例 5.5 使用 root 用户查看/etc/shadow 文件的前 3 行。

```
[root@LinuxServer ~]    #head -3 /etc/shadow
root: $6 $Vq27uyT1 $2h705diNumv0qRI. pWfb8wyzgWPhhg4CNU. 3eT0TlRjoVV9E81g.
prR01L0E2YzvZs.9Hm5fc/0N7.3U23Lt/0:20195:0:99999:7:::
bin:*:19760:0:99999:7:::
daemon:*:19760:0:99999:7:::
```

说明：在/etc/group 中，每行有 9 个字段；各字段之间用“：”分隔。

1）第 1 字段：用户名

在/etc/shadow 中，用户名和/etc/passwd 是相同的，这样就把 passwd 和 shadow 中使用的用户记录联系在了一起；该字段是非空的，必须保证与/etc/passwd 完全相同。

2）第 2 字段：密码（已被加密）

加密后的用户口令，其中“*”表示非登录用户，“!!”表示没有设置密码。

3）第 3 字段：上次修改口令的时间

该字段是从 1970 年 1 月 1 日起到用户最近一次修改口令的天数。

4）第 4 字段：最小使用期限

该字段是自上次更改密码以来用户可以再次更改密码的天数，如果为 0，则表示没有限制，随时可修改；如果为 100，则表示这次修改后 100 天内不可再修改。该字段的默认值读取/etc/login.defs 文件的 PASS_MIN_DAYS 字段值。

5）第 5 字段：最大使用期限

该字段是指相对于第 3 个字段强制多长时间内必须修改密码，如果设置为 99999，则表示没有限制。该字段的默认值读取/etc/login.defs 文件的 PASS_MAX_DAYS 字段值。

6）第 6 字段：密码更改前的警告天数

该字段是指相对于第 5 个字段到期前的警告。当密码接近过期时，系统会提前通知用户更改密码。该字段的默认值读取/etc/login.defs 文件的 PASS_WARN_AGE 字段值。

7）第 7 字段：密码过期后的账号宽限天数

该字段是指相对于第 5 个字段在密码过期之后多少天禁用此用户。此字段表示用户密码到期后宽限多少天，在宽限的时间内允许修改密码，若仍未修改，则完全禁用该账户。

8）第 8 字段：账户失效日期

相对第 3 个字段，用户作废的天数。如果该字段为空，则表示账户永久可用，否则该账户在此字段规定的日期之后将无法使用。

9）第 9 字段：保留字段

该字段目前为空，以备将来 Linux 发展使用。

例 5.6 查看 linuxstudy 账户的密码情况。

```
[root@LinuxServer ~]    #cat /etc/shadow | grep linuxstudy
linuxstudy:$6$JhfctPuiM2HYi6vN$lcPlKWo5TmCvuABNQIgobXHrTlUYtRd7gW0cjawtFuTRUjCu
AbITJGeAPT8jNunMWObj4PaHP8Na49mFFEuFY/::0:99999:7:::
```

说明：“|”是管道符，代表将 cat 命令的结果作为 grep 命令的输入，即先查看 shadow 文件内容，再在里面查找 linuxstudy 关键字。linuxstudy 用户密码已加密，密码未被修改。密码使用没有最小使用限制和最大使用限制，密码过期前 7 天通知用户，没有失效日期。

5.2.3 /etc/group

具有某种共同特征的用户集合起来就是用户组(Group),用户组配置文件主要有/etc/group 和/etc/gshadow,其中/etc/gshadow 是与/etc/group 对应的加密信息文件。

/etc/group 是用户组的信息文件,一个组可以包含 n 个用户,一个用户也可以属于多个组,但必须有一个主组,即/etc/passwd 文件中记录的第 4 个字段。/etc/group 文件的内容允许所有用户查看。

例 5.7 使用 linuxstudy 用户查看/etc/shadow 文件属性和前 3 行内容。

```
[root@LinuxServer ~]      #ls -l /etc/group
-rw-r--r--. 1 root root 1190 6月  19 09:31 /etc/group
[root@LinuxServer ~]      #head -3 /etc/group
root:x:0:
bin:x:1:
daemon:x:2:
```

/etc/group 文件的内容共有 4 个字段,包括用户组、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,文件内容以“:”分隔。

1) 第 1 字段:用户组名称

用户组的名称,其命名规则与/etc/passwd 中的用户名相同。

2) 第 2 字段:用户组密码

x 表示密码已经迁移,其迁移文件为/etc/gshadow,用户组的密码主要用于指定组管理员。

3) 第 3 字段:GID

用户组的唯一标志,称为 GID。GID 也是一组整数,被系统内部用来标志组,/etc/passwd 中的 GID 就来源于/etc/group。

说明: GID 和 UID 类似,是一串整数,GID 从 0 开始,GID 为 0 的组是 root 用户组;系统会预留一些较靠前的 GID 给系统虚拟用户组;每个系统预留的 GID 都有所不同,例如 CentOS 7 预留了 1000 个,用户添加新用户组时,GID 从 1000 开始。若要查看系统添加用户组默认的 GID 范围,则应该查看/etc/login.defs 中的 GID_MIN 和 GID_MAX 值。

4) 第 4 字段:组中的用户

每个用户之间用“,”分隔,本字段可以为空,一个用户可以加入多个组,加入组其实就是将其用户名写入该字段。

5.2.4 /etc/gshadow

/etc/gshadow 文件用于存放用户组的加密口令、组管理员等信息,该文件只有 root 用户可以读取。每个用户组一条记录,依然是用“;”分隔的,共有 4 个字段。

1) 第 1 字段:用户组

用户组的名称,同/etc/group 文件中的组名相对应。

2) 第 2 字段:用户组密码

这个字段通常为空,表示不设置密码;有时该字段为“!”,表示没有密码,也不设置管

理员。

3）第 3 字段：用户组管理者

这个字段最大的功能就是创建组管理员，如果有多个管理员，则用“,”分隔。

4）第 4 字段：组织成员

该字段显示这个用户组中有哪些附加用户，和/etc/group 文件中附加组的显示内容相同。

5.3 管理用户账户

用户账户管理包括新建用户、修改用户信息、删除用户。

5.3.1 添加用户

添加用户账号就是在系统中创建一个新用户，然后为新用户分配 UID、用户组、主目录和登录 Shell 等资源。

命令名称：useradd

使用方式：useradd ［选项参数］［用户名］

说明：只有 root 用户具有执行 useradd 命令的权限。

参数：

-c：设置用户的注释性信息，写到/etc/passwd 的第 5 栏。

-u，--uid UID：设置用户的 UID，它必须唯一，且大于 999。

-d，--home-dir HOME_DIR：设置用户的主目录。

-g，--gid GROUP：设置用户所属主组的组名称或 GID。

-G，--groups GROUPS：设置用户所属附加组的组列表，多个组之间用逗号分隔。

-m，--create-home：若用户主目录不存在，则创建主目录。

-M，--no-create-home：不创建用户的主目录。

-r，--system：创建一个系统用户。

-s，--shell SHELL：设置用户的登录 Shell，默认为/bin/bash。

-D：查看用户的初始属性。

例 5.8 以默认参数增加一个账户，名称为 test1。

```
[linuxstudy@LinuxServer root]$ useradd test1
useradd: Permission denied.
useradd: 无法锁定 /etc/passwd,请稍后再试
[linuxstudy@LinuxServer root]$su root
密码:
[root@LinuxServer ~]      #useradd test1
[root@LinuxServer ~]      #grep test1 /etc/passwd /etc/shadow /etc/group
/etc/passwd:test1:x:1001:1001::/home/test1:/bin/bash
/etc/shadow:test1:!!:20199:0:99999:7:::
/etc/group:test1:x:1001:
[root@LinuxServer ~]      #ls -ld /home/test1
drwx------. 3 test1 test1 78 8月  28 17:07 /home/test1
```

说明 1：普通用户不能使用 useradd 命令。

说明 2：grep 命令可以在多个文件中按照关键词查看内容。

说明 3：使用 useradd 命令创建后，/etc/passwd、/etc/shadow、/etc/group 三个文件全都增加了一条数据，其新建的用户 UID 和 GID 都为 1001。

说明 4：新用户的主目录的权限为 rwx------，即只有用户自己能够操作该目录，其他用户没有权限。

例 5.9 使用 test1 为用户主组，1111 为 UID，创建用户 test2。

```
[root@LinuxServer ~]        #useradd -u 1111 -g test1 test2
[root@LinuxServer ~]        #grep test2 /etc/passwd /etc/shadow /etc/group
/etc/passwd:test2:x:1111:1001::/home/test2:/bin/bash
/etc/shadow:test2:!!:20199:0:99999:7:::
```

说明： -g 参数指定主组 test1 时，要确保主组 test1 已创建，且不会再创建同名的组 test2。

例 5.10 创建用户 test3，将其加入组 test1，并设置登录 Shell 为/sbin/nologin 不作为用户的主组。

```
[root@LinuxServer ~]      #useradd -G test1 -s /sbin/nologin test3
[root@LinuxServer ~]      #grep test3 /etc/passwd /etc/shadow /etc/group
/etc/passwd:test3:x:1112:1112::/home/test3:/sbin/nologin
/etc/shadow:test3:!!:20199:0:99999:7:::
/etc/group:test1:x:1001:test3
/etc/group:test3:x:1112:
```

说明 1：-G 参数指定附加组，创建用户 test3 时依旧会创建主组 test3，且在组文件/etc/group 中将 test3 用户列到 test1 组中。

说明 2：登录 Shell 设置为/sbin/nologin 代表该用户无法正常登录系统。

例 5.11 查看用户的初始属性。

```
[root@LinuxServer ~]      #useradd -D
GROUP=100
HOME=/home
INACTIVE=-1
EXPIRE=
SHELL=/bin/bash
SKEL=/etc/skel
CREATE_MAIL_SPOOL=yes
```

说明：

（1）GROUP＝100 表示设置默认创建的用户都属于 GID 为 100 的组，也就是 users 组。

（2）HOME＝/home 表示默认的用户主目录，用户的主目录通常与账号名名称相同，这个目录会放在/home/下面。

（3）INACTIVE＝-1 表示密码的失效日，即 shadow 文件的第 7 列，如果为 0 则代表立即失效，如果为-1 则代表永久有效。

(4) EXPIRE=账号失效日,即 shadow 文件的第 8 列。

(5) SHELL=/bin/bash 指默认的 Shell。

(6) SKEL=/etc/skel 表示用户文件夹的内容数据参考目录,新增用户主目录的各项数据是从该文件中复制过去的。

(7) CREATE_MAIL_SPOOL=yes 表示是否主动帮助用户创建邮件信箱,yes 表示创建。

除了 useradd -D 查看的这些基本设置外,/etc/login.defs 中还详细描述了关于用户的各项设置。

```
[root@LinuxServer ~]    #grep -Ev "^#|^$" /etc/login.defs
MAIL_DIR            /var/spool/mail          //用户邮箱的默认存放目录
UMASK               022                      //创建用户主目录的 umask 值
HOME_MODE           0700                     //用户主目录的默认权限为 drwx------
PASS_MAX_DAYS       99999                 //密码有效期(天),即/etc/shadow 中的第 5 列
PASS_MIN_DAYS       0     //允许用户修改密码的最小间隔天数,即/etc/shadow 中的第 4 列
PASS_WARN_AGE       7         //密码过期前提前几天警告用户,即/etc/shadow 中的第 6 列
UID_MIN             1000                     //普通用户使用的最小 UID 值
UID_MAX             60000                    //普通用户使用的最大 UID 值
SYS_UID_MIN         201                      //系统用户使用的最小 UID 值
SYS_UID_MAX         999                      //系统用户使用的最大 UID 值
SUB_UID_MIN         100000                   //子用户使用的最小 UID 值
SUB_UID_MAX         600100000                //子用户使用的最大 UID 值
SUB_UID_COUNT       65536                    //每个主用户可分配的子 ID 数量
GID_MIN             1000                     //普通用户组使用的最小 GID 值
GID_MAX             60000                    //普通用户组使用的最大 GID 值
SYS_GID_MIN         201                      //系统用户组使用的最小 GID 值
SYS_GID_MAX         999                      //系统用户组使用的最大 GID 值
SUB_GID_MIN         100000                   //子组使用的最小 GID 值
SUB_GID_MAX         600100000                //子组使用的最大 GID 值
SUB_GID_COUNT       65536                    //每个主组可分配的子 ID 数量
ENCRYPT_METHOD SHA512                        //用户密码的加密算法
SHA_CRYPT_MAX_ROUNDS 100000                  //SHA512 算法的迭代次数
USERGROUPS_ENAB yes                 //删除用户时,若其初始组无其他成员,则自动删除该组
CREATE_HOMEyes                               //创建用户时自动创建主目录
HMAC_CRYPTO_ALGO SHA512                      //HMAC(密钥哈希消息认证码)使用的算法
```

5.3.2 修改用户

修改用户信息可以通过修改/etc/passwd 和/etc/shadow 文件实现,也可以使用 usermod 命令实现。

命令名称:usermod

使用方式:usermod [参数] [用户名]

说明:修改用户信息只有 root 用户才可以执行。

参数:

-a, --append:将用户添加到附加组,只能和-G 选项一起使用。