第3章 Linux的权限用户(组)管理基本操作

3.1 实验目的

掌握使用命令创建和修改权限用户(组)属性信息的方法。

3.2 实验环境

一台已安装好VMware软件的主机,虚拟机系统为CentOS 7。

3.3 预备知识

3.3.1 与权限用户(组)管理相关的文件

与权限用户(组)管理相关的文件有/etc/passwd、/etc/shadow、/etc/group、/etc/gshadow、/etc/login.defs、/etc/default/useradd等,用于对权限用户设置和登录项目进行控制。

(1) /etc/passwd是一个文本文件,它包含一个系统账户列表,给出每个账户一些有用的信息,例如用户ID、组ID、家目录、shell等,每一行包含一条记录。

(2) /etc/shadow是影子化了的密码文件,它包含系统账户的密码信息和可选的年龄信息。此文件的每行包括9个字段,使用半角冒号(“:”)分隔。此文件的组成信息及顺序如下:

登录名:加密了的密码:最后一次更改密码的日期:密码的最小年龄:最大密码年龄:密码警告时间段:密码禁用期:账户过期日期:保留字段。

(3) /etc/group是一个ASCII码的文件,它定义了权限用户所属的组。文件中每行包括一条记录。其格式如下:

```
group_name:passwd:GID:user_list
```

其中,passwd为(加密的)组密码,若该字段为空,则不需要密码。组内所有成员的用户名,以半角逗号分隔。

(4) /etc/gshadow是影子化了的组文件,包含组账户信息,类似于shadow文件。

(5) /etc/login.defs是针对影子密码的配置文件(与影子密码配套使用)。

(6) /etc/default/useradd 是 useradd 命令默认参数的配置文件。

上述文件不建议手动修改,可以通过使用下面的命令达到修改相应文件的目的,以实现账户的管理。

3.3.2 权限用户管理命令

权限用户管理的命令主要有 useradd、userdel 和 usermod 3 个。它们分别用于权限用户的建立、权限用户的删除和权限用户属性的修改。另外,还有一个命令 su 用于运行替换权限用户和组标识、替换 shell 等操作。

1. useradd

功能:创建一个新权限用户或更新默认新权限用户信息。

语法:useradd [选项] 登录
useradd -D
useradd -D [选项]

useradd 的常用选项及说明如表 3-1 所示。

表 3-1 useradd 的常用选项及说明

常用选项	选项说明
-b,--base-dir BASE_DIR	新账户的主目录的基目录
-d,--home-dir HOME_DIR	新账户的主目录
-D,--defaults	显示或更改默认的 useradd 配置
-e,--expiredate EXPIRE_DATE	新账户的过期日期
-f,--inactive INACTIVE	新账户的密码不活动期
-g,--gid GROUP	新账户主组的名称或 ID
-G,--groups GROUPS	新账户的附加组列表
-o,--non-unique	允许使用重复的 UID 创建权限用户
-s,--shell SHELL	新账户的登录 shell
-u,--uid UID	新账户的用户 ID
-U,--user-group	创建与权限用户同名的组

注意,用户名不能超过 32 个字符长。

2. userdel

功能:删除权限用户账户和相关文件。

语法:userdel [选项] 登录

userdel 的常用选项及说明如表 3-2 所示。

表 3-2 userdel 的常用选项及说明

常用选项	选项说明
-f,--force	强制删除权限用户账户,甚至权限用户仍然在登录状态。注意:此选项危险,可能会破坏系统的稳定性
-r,--remove	删除主目录和邮件池

3. usermod

功能:修改一个权限用户账户信息。

语法：usermod [选项] 登录

usermod 的常用选项及说明如表 3-3 所示。

表 3-3　usermod 的常用选项及说明

常 用 选 项	说　　明
-d,--home HOME_DIR	权限用户的新主目录
-e,--expiredate EXPIRE_DATE	设定账户过期的日期为 EXPIRE_DATE
-f,--inactive INACTIVE	过期 INACTIVE 天数后，设定密码为失效状态
-g,--gid GROUP	强制使用 GROUP 为新主组
-G,--groups GROUPS	新的附加组列表 GROUPS
-a,--append GROUP	将权限用户追加至上边-G 中提到的附加组中，并不从其他组中删除此权限用户
-l,--login LOGIN	新的登录名称
-L,--lock	锁定权限用户账号
-m,--move-home	将目录内容移至新位置(仅与-d 一起使用)
-o,--non-unique	允许使用重复的(非唯一的)UID
-p,--password PASSWORD	将加密过的密码(PASSWORD)设为新密码
-s,--shell SHELL	该权限用户账号的新登录 shell
-u,--uid UID	权限用户账号的新 UID
-U,--unlock	解锁权限用户账号

注意，如果要更改权限用户的 ID、用户名或主目录，需要确保在执行命令时，权限用户没有运行任何进程。

4. su

功能：用于将当前权限用户修改为有效权限用户的标识(即实现用户切换的功能)。

语法：su [OPTION]... [-] [USER [ARG]...]

su 的常用选项及说明如表 3-4 所示。

表 3-4　su 的常用选项及说明

常 用 选 项	选 项 说 明
单个-视为-l	如果未指定 USER，将假定为 root
-m, -p,--preserve-environment	不重置环境变量
-g,--group <组>	指定主组
-G,--supp-group <组>	指定一个辅助组
-c,--command <命令>	使用-c 向 shell 传递一条命令
-s,--shell < shell >	若/etc/shells 允许，则运行 shell

3.3.3　权限用户组管理命令

权限用户组管理命令主要有 groupadd、groupdel 和 groupmod 等，分别用于组的创建、组的删除和组的属性修改。

1. groupadd

功能：创建一个新组。

语法：groupadd [选项] 组

groupadd 的常用选项及说明如表 3-5 所示。

表 3-5　groupadd 的常用选项及说明

常 用 选 项	选 项 说 明
-f,--force	如果组已经存在则退出，如果 GID 已经存在则取消-g
-g,--gid GID	为新组使用 GID
-K,--key KEY＝VALUE	不使用/etc/login. defs 中的默认值
-o,--non-unique	允许创建有重复 GID 的组

组名最长为 32 个字符。

2. groupdel

功能：删除一个组。

语法：groupdel [选项] GROUP

注意，在使用此选项删除一个组时，不能移除现有权限用户的主组。在移除此组之前，必须先移除此用户，再手动检查所有文件系统，以确保没有遗留的属于此组的文件。

3. groupmod

功能：修改组的属性信息。

语法：groupmod [选项] 组

groupmod 的常用选项及说明如表 3-6 所示。

表 3-6　groupmod 的常用选项及说明

常 用 选 项	选 项 说 明
-g,--gid GID	将组 ID 改为 GID
-n,--new-name NEW_GROUP	改名为 NEW_GROUP
-o,--non-unique	允许使用重复的 GID

3.3.4　密码管理命令

密码管理的命令包括 passwd 和 chage 两个。其中，passwd 用于修改权限用户的密码；chage 用于更改权限用户密码过期的信息(使用的天数)。

1. passwd

功能：更新权限用户的口令。

语法：passwd [选项...] <账号名称>

passwd 的常用选项及说明如表 3-7 所示。

表 3-7　passwd 的常用选项及说明

常 用 选 项	选 项 说 明
-k,--keep-tokens	保持身份验证令牌不过期
-d,--delete	删除已命名账号的密码(仅限 root 用户)
-l,--lock	锁定指名账户的密码(仅限 root 用户)
-u,--unlock	解锁指名账户的密码(仅限 root 用户)

续表

常用选项	选项说明
-e,--expire	终止指名账户的密码(仅限 root 用户)
-f,--force	强制执行操作
-x,--maximum=DAYS	密码的最长有效时限(仅限 root 用户)
-n,--minimum=DAYS	密码的最短有效时限(仅限 root 用户)
-w,--warning=DAYS	在密码过期前多少天开始提醒用户(仅限 root 用户)
-i,--inactive=DAYS	当密码过期后经过多少天该账号会被禁用(仅限 root 用户)
-S,--status	报告已命名账号的密码状态(仅限 root 用户)
--stdin	从标准输入读取令牌(仅限 root 用户)

2. chage

功能：更改权限用户密码过期的信息。

语法：chage [选项] 登录

chage 的主要选项如表 3-8 所示。

表 3-8 chage 的主要选项及说明

主要选项	选项说明
-d,--lastday 最近日期	将最近一次密码设置时间设为“最近日期”
-E,--expiredate 过期日期	将账户过期时间设为“过期日期”
-I,--inactive INACITVE	过期 INACTIVE 天数后,设定密码为失效状态
-l,--list	显示账户年龄信息
-m,--mindays 最小天数	将两次改变密码之间相距的最小天数设为“最小天数”
-M,--maxdays 最大天数	将两次改变密码之间相距的最大天数设为“最大天数”
-W,--warndays 警告天数	将过期警告天数设为“警告天数”

注意,如果没有选择任何选项,chage 会进入交互模式,并以所有字段的当前值提示用户。输入一个新值可以更改这些字段,或者留空使用当前值(当前值出现在[ ]标记对中)。只有 root 才可以使用 chage。-l 选项是一个特殊情况,它用来让非特权用户知道自己的密码或账户何时过期。

3.4 实验步骤

3.4.1 权限用户创建和管理

(1) 在控制台上用 root 用户登录系统,并切换到字符界面(如果已经是字符界面,就可忽略本操作)。命令如下:

```
[root@localhost ~]# systemctl isolate multi-user.target,
```

或

```
[root@localhost ~]# init 3
```

(2) 创建用户组 wlx:新建两个普通用户 st01、st02,并加入用户组 wlx;使用命令

passwd 给新用户 st01 和 st02 设置密码。

输入如下命令新建用户组：

```
# groupadd wlx
```

输入如下命令新建一个用户 st01，将用户加入到用户组 wlx：

```
# useradd -g wlx st01
```

输入如下命令给 st01 设置密码：

```
#passwd st01
```

按照创建 st01 的方法创建另一个用户 st02。

输入命令 exit 或 logout 退出登录。

(3) 在虚拟控制台 tty1 上用 st01 登录，练习命令 pwd、whoami、who。

(4) 在虚拟控制台 tty2 上用 st02 登录，练习命令 pwd、whoami、who。

说明：切换虚拟控制台的方法：同时按 Alt+F[1～6]组合键，如切换到虚拟控制台 tty1，则按 Alt+F1 组合键；切换到虚拟控制台 tty2，则按 Alt+F2 组合键，以此类推，等等。

3.4.2 练习完成以下操作

(1) 练习以下命令 man、clear、cal、date 的使用。

① 查看 man 手册页的使用方法。

② 将当前屏幕清屏。

③ 打印今年的日历。

④ 显示系统时间，如果和当前时间不一致，请修改时间。

(2) 通过查看文件/root/anaconda-ks.cfg，练习 more、less、wc 命令的使用。

(3) 查看以下文件的内容，找出在本章 3.4.1 小节中添加的账户信息。

```
/etc/passwd
/etc/shadow
/etc/group
```

3.5 思考与练习

more、less、cat、wc 命令有什么区别？