账户管理概述

内容提要

1. 理解用户和组的概念
2. 熟悉Linux环境下的账户系统文件的格式

账户实质

Linux操作系统是多用户的操作系统，它允许多个用户同时登录到系统上，使用系统资源。当多个用户能同时使用系统时，为了使所有用户的工作都能顺利进行，保护每个用户的文件和进程，也为了系统自身的安全和稳定，必须建立起一种秩序，使每个用户的权限都能得到规范。为此，首先就需要区分不同的用户，这就产生了用户账户。 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。

用户和组

广义上讲，Linux的账户包括用户账户和组账户两种。

Linux系统下的用户账户（简称用户）有两种，普通用户账户和超级用户账户（或管理员账户）。普通用户在系统上的任务是进行普通工作，管理员在系统上的任务是对普通用户和整个系统进行管理。管理员账户对系统具有绝对的控制权，能够对系统进行一切操作，如操作不当很容易对系统造成损坏。因此即使系统只有一个用户使用，也应该在管理员账户之外建立一个普通用户账户，在用户进行普通工作的时候以普通用户账户登录系统。

除了用户账户之外，在Linux下还存在组账户（简称组）。组是用户的集合。在 Linux中组有两种类型：私有组和标准组。当创建一个新用户时，若没有指定他所属于的组，Linux就建立一个和该用户同名的私有组。此私有组中只包含这个用户自己。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。

从另一方面讲，同一个用户可以同属于多个组，例如某单位有领导组和技术组等，Tom是该单位的技术主管，所以他既应该属于领导组又应该属于技术组。当一个用户属于多个组时，其登录后所属的组称为主组，其他的组称为附加组。

Linux环境下的账户系统文件

Linux下的账户系统文件主要有 /etc/passwd、/etc/shadow、/etc/group 和 /etc/gshadow 四个文件。

/etc/passwd

/etc/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账号的不同属性，各字段间用":"分隔。例如：

```
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:
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
rpm:x:37:37::/var/lib/rpm:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
apache:x:48:48:Apache:/var/www:/sbin/nologin
avahi:x:70:70:Avahi daemon:/:/sbin/nologin
mailnull:x:47:47::/var/spool/mqueue:/sbin/nologin
smmsp:x:51:51::/var/spool/mqueue:/sbin/nologin
distcache:x:94:94:Distcache:/:/sbin/nologin
nscd:x:28:28:NSCD Daemon:/:/sbin/nologin
vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin
rpc:x:32:32:Portmapper RPC user:/:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin
named:x:25:25:Named:/var/named:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
dovecot:x:97:97:dovecot:/usr/libexec/dovecot:/sbin/nologin
webalizer:x:67:67:Webalizer:/var/www/usage:/sbin/nologin
squid:x:23:23::/var/spool/squid:/sbin/nologin
pcap:x:77:77::/var/arpwatch:/sbin/nologin
haldaemon:x:68:68:HAL daemon:/:/sbin/nologin
osmond:x:500:500::/home/osmond:/bin/bash
crq:x:501:501::/home/crq:/bin/bash
jason:x:502:502::/home/jason:/bin/bash
qu10m:x:503:503::/home/qu10m:/bin/bash
```

下表描述了这些字段的意义。

字段	说明
用户名	这是用户登录系统时使用的用户名，它在系统中是唯一的。
口令	此字段存放加密的口令。在此文件中的口令是X，这表示用户的口令是被/etc/shadow文件保护的，所有加密的口令以及和口令有关的设置都保存在/etc/shadow中。
用户标识号	是一个整数，系统内部用它来标识用户。每个用户的UID都是唯一的。root用户的UID是0，从1到999是系统的标准账户。普通用户的UID从1000开始。
组标识号	是一个整数，系统内部用它来标识用户所属的组。每个用户账户在建立好后都会有一个主组。主组相同的账户其GID相同。
注释性描述	例如存放用户全名等信息。
自家目录	用户登录系统后所进入的目录。
命令解释器	指示该用户使用的Shell，Linux默认为bash。

/etc/shadow

/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。/etc/shadow只对root用户可读。在安装系统时，会询问用户是否启用shadow passwords功能。在安装好系统后也可以用pwconv命令和pwunconv命令来启动或取消shadow passwords的保护。

CentOS 默认使用shadow passwords保护。经过shadow passwords保护的账户口令和相关设置信息保存在/etc/shadow文件里。shadow文件的内容形式如下：

```
root:$1$UMHcnkVs$WbsUEcstZXKtYvixx34Qi0:13855:0:99999:7:::
bin:*:13855:0:99999:7:::
daemon:*:13855:0:99999:7:::
adm:*:13855:0:99999:7:::
lp:*:13855:0:99999:7:::
sync:*:13855:0:99999:7:::
```

```
shutdown:*:13855:0:99999:7:::
halt:*:13855:0:99999:7:::
mail:*:13855:0:99999:7:::
news:*:13855:0:99999:7:::
uucp:*:13855:0:99999:7:::
operator:*:13855:0:99999:7:::
games:*:13855:0:99999:7:::
gopher:*:13855:0:99999:7:::
ftp:*:13855:0:99999:7:::
nobody:*:13855:0:99999:7:::
rpm:!!:13855:0:99999:7:::
dbus:!!:13855:0:99999:7:::
apache:!!:13855:0:99999:7:::
avahi:!!:13855:0:99999:7:::
mailnull:!!:13855:0:99999:7:::
smmsp:!!:13855:0:99999:7:::
distcache:!!:13855:0:99999:7:::
nscd:!!:13855:0:99999:7:::
vcsa:!!:13855:0:99999:7:::
rpc:!!:13855:0:99999:7:::
rpcuser:!!:13855:0:99999:7:::
nfsnobody:!!:13855:0:99999:7:::
named:!!:13855:0:99999:7:::
sshd:!!:13855:0:99999:7:::
dovecot:!!:13855:0:99999:7:::
webalizer:!!:13855:0:99999:7:::
squid:!!:13855:0:99999:7:::
pcap:!!:13855:0:99999:7:::
haldaemon:!!:13855:0:99999:7:::
osmond:$1$DEXUnuYT$LDqcRsYSKu5Pd5CYxbU.v/:13855:0:99999:7:::
crq::13857:0:99999:7:::
jason:!!:13861:0:99999:7:::
qu10m:!!:13862:0:99999:7:::
```

其中各字段的意义如表所示。

字段	说明
用户名	用户的账户名
口令	用户的口令，是加密过的
最后一次修改的时间	从1970年1月1日起，到用户最后一次更改口令的天数
最小时间间隔	从1970年1月1日起，到用户可以更改口令的天数
最大时间间隔	从1970年1月1日起，到用户必须更改口令的天数
警告时间	在用户口令过期之前多少天提醒用户更新
不活动时间	在用户口令过期之后到禁用账户的天数
失效时间	从1970年1月1日起，到账户被禁用的天数
标志	保留位

/etc/group

将用户分组是Linux中对用户进行管理及控制访问权限的一种手段。每个用户都属于某一个组；一个组中可以有多个用户，一个用户也可以属于不同的组。当一个用户同时是多个组的成员时，在/etc/passwd文件中记录的是用户所属的主组，也就是登录时所属的默认组，而其他组称为附加组。用户要访问附加组的文件时，必须首先使用newgrp命令使自己成为所要访问的组的成员。组的所有属性都存放在/etc/group文件中。/etc/group文件对任何用户均可读。下面是一个/etc/group文件的例子：

```
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
mem:x:8:
kmem:x:9:
wheel:x:10:root
mail:x:12:mail
news:x:13:news
uucp:x:14:uucp
man:x:15:
games:x:20:
gopher:x:30:
dip:x:40:
ftp:x:50:
lock:x:54:
nobody:x:99:
users:x:100:
rpm:x:37:
dbus:x:81:
utmp:x:22:
apache:x:48:
avahi:x:70:
mailnull:x:47:
smmsp:x:51:
distcache:x:94:
nscd:x:28:
utempter:x:35:
floppy:x:19:
vcsa:x:69:
rpc:x:32:
rpcuser:x:29:
nfsnobody:x:65534:
named:x:25:
sshd:x:74:
dovecot:x:97:
webalizer:x:67:
squid:x:23:
pcap:x:77:
slocate:x:21:
haldaemon:x:68:
osmond:x:500:
crq:x:501:
jason:x:502:
fuse:x:101:
qul0m:x:503:
```

和/etc/passwd文件类似，其中每一行记录了一个组的信息。每行包括四个字段，不同字段之间用冒号隔开。其中各字段的内容说明见下表。

字段	说明
组名	该组的名称
组口令	用户组口令，由于安全性原因，已不使用该字段保存口令，用"x"占位
GID	组的识别号，和UID类似，每个组都有自己独有的识别号，不同组的GID不会相同
组成员	属于这个组的成员

/etc/gshadow

/etc/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。下面是一个/etc/gshadow文件的例子：

```
root:::root
bin:::root,bin,daemon
daemon:::root,bin,daemon
sys:::root,bin,adm
adm:::root,adm,daemon
tty:::
```

```
disk:::root
lp:::daemon,lp
mem:::
kmem:::
wheel:::root
mail:::mail
news:::news
uucp:::uucp
man:::
games:::
gopher:::
dip:::
ftp:::
lock:::
nobody:::
users:::
rpm:x::
dbus:x::
utmp:x::
apache:x::
avahi:x::
mailnull:x::
smmsp:x::
distcache:x::
nscd:x::
utempter:x::
floppy:x::
vcsa:x::
rpc:x::
rpcuser:x::
nfsnobody:x::
named:x::
sshd:x::
dovecot:x::
webalizer:x::
squid:x::
pcap:x::
slocate:x::
haldaemon:x::
osmond:!::
crq:!::
jason:!::
fuse:!::
qul0m:!::
```

和/etc/group文件类似，其中每一行记录了一个组的信息。每行包括四个字段，不同字段之间用冒号隔开。其中各字段的内容说明见下表。

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

- 显示源文件
- 登录