## 一、Linux系统用户账号的管理

添加用户账号就是在系统中创建一个新账号，然后为新账号分配用户号、用户组、主目录和登录Shell等资源。刚添加的账号是被锁定的，无法使用。

### **1、添加新的用户账号使用useradd命令，其语法如下：**

useradd 选项 用户名

参数说明：

选项:

-c comment 指定一段注释性描述。

-d 目录 指定用户主目录，如果此目录不存在，则同时使用-m选项，可以创建主目录。

-g 用户组 指定用户所属的用户组。

-G 用户组，用户组 指定用户所属的附加组。

-s Shell文件 指定用户的登录Shell。

-u 用户号 指定用户的用户号，如果同时有-o选项，则可以重复使用其他用户的标识号。

用户名:

指定新账号的登录名。

#### 实例1

# useradd –d /home/sam -m sam

此命令创建了一个用户sam，其中-d和-m选项用来为登录名sam产生一个主目录 /home/sam（/home为默认的用户主目录所在的父目录）。

#### 实例2

# useradd -s /bin/sh -g group –G adm,root gem

此命令新建了一个用户gem，该用户的登录Shell是 /bin/sh，它属于group用户组，同时又属于adm和root用户组，其中group用户组是其主组。

增加用户账号就是在/etc/passwd文件中为新用户增加一条记录，同时更新其他系统文件如/etc/shadow, /etc/group等。

### **2、删除帐号**

删除用户账号就是要将/etc/passwd等系统文件中的该用户记录删除，必要时还删除用户的主目录。

删除一个已有的用户账号使用userdel命令，其格式如下：

userdel 选项 用户名

常用的选项是 **-r**，它的作用是把用户的主目录一起删除。

例如：

# userdel -r sam

此命令删除用户sam在系统文件中（主要是/etc/passwd, /etc/shadow, /etc/group等）的记录，同时删除用户的主目录。

### **3、修改帐号**

修改已有用户的信息使用usermod命令，其格式如下：

usermod 选项 用户名

常用的选项包括-c, -d, -m, -g, -G, -s, -u以及-o等，这些选项的意义与useradd命令中的选项一样，可以为用户指定新的资源值。

另外，有些系统可以使用选项：-l 新用户名

这个选项指定一个新的账号，即将原来的用户名改为新的用户名。

例如：

# usermod -s /bin/ksh -d /home/z –g developer sam

此命令将用户sam的登录Shell修改为ksh，主目录改为/home/z，用户组改为developer。

### **4、用户口令的管理**

用户管理的一项重要内容是用户口令的管理。用户账号刚创建时没有口令，但是被系统锁定，无法使用，必须为其指定口令后才可以使用，即使是指定空口令。

指定和修改用户口令的Shell命令是passwd。超级用户可以为自己和其他用户指定口令，普通用户只能用它修改自己的口令。命令的格式为：

passwd 选项 用户名

可使用的选项：

* -l 锁定口令，即禁用账号。
* -u 口令解锁。
* -d 使账号无口令。
* -f 强迫用户下次登录时修改口令。

如果默认用户名，则修改当前用户的口令。

例如，假设当前用户是sam，则下面的命令修改该用户自己的口令：

$ passwd

Old password:\*\*\*\*\*\*

New password:\*\*\*\*\*\*\*

Re-enter new password:\*\*\*\*\*\*\*

如果是超级用户，可以用下列形式指定任何用户的口令：

# passwd sam

New password:\*\*\*\*\*\*\*

Re-enter new password:\*\*\*\*\*\*\*

为用户指定空口令时，执行下列形式的命令：

# passwd -d sam

此命令将用户 sam 的口令删除，这样用户 sam 下一次登录时，系统就不再允许该用户登录了。

passwd 命令还可以用 -l(lock) 选项锁定某一用户，使其不能登录，例如：

# passwd -l sam

## 二、Linux系统用户组的管理

每个用户都有一个用户组，系统可以对一个用户组中的所有用户进行集中管理。

用户组的管理涉及用户组的添加、删除和修改。组的增加、删除和修改实际上就是对/etc/group文件的更新。

### **1、增加一个新的用户组使用groupadd命令。其格式如下：**

groupadd 选项 用户组

可以使用的选项有：

-g GID 指定新用户组的组标识号（GID）。

-o 一般与-g选项同时使用，表示新用户组的GID可以与系统已有用户组的GID相同。

#### 实例1：

# groupadd group1

此命令向系统中增加了一个新组group1，新组的组标识号是在当前已有的最大组标识号的基础上加1。

#### 实例2：

# groupadd -g 101 group2

此命令向系统中增加了一个新组group2，同时指定新组的组标识号是101。

### **2、如果要删除一个已有的用户组，使用groupdel命令，其格式如下：**

groupdel 用户组

#### 例如：

# groupdel group1

此命令从系统中删除组group1。

### **3、修改用户组的属性使用groupmod命令。其语法如下：**

groupmod 选项 用户组

常用的选项有：

-g GID 为用户组指定新的组标识号。

-o 与-g选项同时使用，用户组的新GID可以与系统已有用户组的GID相同。

-n新用户组 将用户组的名字改为新名字

#### 实例1：

# groupmod -g 102 group2

此命令将组group2的组标识号修改为102。

#### 实例2：

# groupmod –g 10000 -n group3 group2

此命令将组group2的标识号改为10000，组名修改为group3。

### **4、如果一个用户同时属于多个用户组，那么用户可以在用户组之间切换，以便具有其他用户组的权限。**

用户可以在登录后，使用命令newgrp切换到其他用户组，这个命令的参数就是目的用户组。例如：

$ newgrp root

这条命令将当前用户切换到root用户组，前提条件是root用户组确实是该用户的主组或附加组。

## 三、与用户账号有关的系统文件

完成用户管理的工作有许多种方法，但是每一种方法实际上都是对有关的系统文件进行修改。

与用户和用户组相关的信息都存放在一些系统文件中，这些文件包括/etc/passwd, /etc/shadow, /etc/group等。

下面分别介绍这些文件的内容。

### **1、/etc/passwd文件是用户管理工作涉及的最重要的一个文件。**

Linux系统中的每个用户都在/etc/passwd文件中有一个对应的记录行，它记录了这个用户的一些基本属性。

这个文件对所有用户都是可读的。它的内容类似下面的例子：

＃ cat /etc/passwd

root:x:0:0:Superuser:/:

daemon:x:1:1:System daemons:/etc:

bin:x:2:2:Owner of system commands:/bin:

sys:x:3:3:Owner of system files:/usr/sys:

adm:x:4:4:System accounting:/usr/adm:

uucp:x:5:5:UUCP administrator:/usr/lib/uucp:

auth:x:7:21:Authentication administrator:/tcb/files/auth:

cron:x:9:16:Cron daemon:/usr/spool/cron:

listen:x:37:4:Network daemon:/usr/net/nls:

lp:x:71:18:Printer administrator:/usr/spool/lp:

sam:x:200:50:Sam san:/home/sam:/bin/sh

从上面的例子我们可以看到，/etc/passwd中一行记录对应着一个用户，每行记录又被冒号(:)分隔为7个字段，其格式和具体含义如下：

用户名:口令:用户标识号:组标识号:注释性描述:主目录:登录Shell

### **1）"用户名"是代表用户账号的字符串。**

为了兼容起见，登录名中最好不要包含点字符(.)，并且不使用连字符(-)和加号(+)打头。

### **2）“口令”一些系统中，存放着加密后的用户口令字。**

现在许多Linux 系统（如SVR4）都使用了shadow技术，把真正的加密后的用户口令字存放到/etc/shadow文件中，而在/etc/passwd文件的口令字段中只存放一个特殊的字符，例如“x”或者“\*”。

### **3）“用户标识号”是一个整数，系统内部用它来标识用户。**

通常用户标识号的取值范围是0～65 535。0是超级用户root的标识号，1～99由系统保留，作为管理账号，普通用户的标识号从100开始。在Linux系统中，这个界限是500。

### **4）“组标识号”字段记录的是用户所属的用户组。**

它对应着/etc/group文件中的一条记录。

### **5)“注释性描述”字段记录着用户的一些个人情况。**

例如用户的真实姓名、电话、地址等，这个字段并没有什么实际的用途。

### **6)“主目录”，也就是用户的起始工作目录。**

它是用户在登录到系统之后所处的目录。各用户对自己的主目录有读、写、执行（搜索）权限，其他用户对此目录的访问权限则根据具体情况设置。

### **7)用户登录后，要启动一个进程，负责将用户的操作传给内核，这个进程是用户登录到系统后运行的命令解释器或某个特定的程序，即Shell。**

Shell是用户与Linux系统之间的接口。Linux的Shell有许多种，每种都有不同的特点。常用的有sh(Bourne Shell), csh(C Shell), ksh(Korn Shell), tcsh(TENEX/TOPS-20 type C Shell), bash(Bourne Again Shell)等。

系统管理员可以根据系统情况和用户习惯为用户指定某个Shell。如果不指定Shell，那么系统使用sh为默认的登录Shell，即这个字段的值为/bin/sh。

用户的登录Shell也可以指定为某个特定的程序（此程序不是一个命令解释器）。

利用这一特点，我们可以限制用户只能运行指定的应用程序，在该应用程序运行结束后，用户就自动退出了系统。有些Linux 系统要求只有那些在系统中登记了的程序才能出现在这个字段中。

### **8)系统中有一类用户称为伪用户（pseudo users）。**

这些用户在/etc/passwd文件中也占有一条记录，但是不能登录，因为它们的登录Shell为空。它们的存在主要是方便系统管理，满足相应的系统进程对文件属主的要求。

常见的伪用户如下所示：

伪 用 户 含 义

bin 拥有可执行的用户命令文件

sys 拥有系统文件

adm 拥有帐户文件

uucp UUCP使用

lp lp或lpd子系统使用

nobody NFS使用

## 拥有帐户文件

**1、除了上面列出的伪用户外，还有许多标准的伪用户，例如：audit, cron, mail, usenet等，它们也都各自为相关的进程和文件所需要。**

**2、/etc/shadow中的记录行与/etc/passwd中的一一对应，它由pwconv命令根据/etc/passwd中的数据自动产生**

它的文件格式与/etc/passwd类似，由若干个字段组成，字段之间用":"隔开。这些字段是：

登录名:加密口令:最后一次修改时间:最小时间间隔:最大时间间隔:警告时间:不活动时间:失效时间:标志

1. "登录名"是与/etc/passwd文件中的登录名相一致的用户账号
2. "口令"字段存放的是加密后的用户口令字，长度为13个字符。如果为空，则对应用户没有口令，登录时不需要口令；如果含有不属于集合 { ./0-9A-Za-z }中的字符，则对应的用户不能登录。
3. "最后一次修改时间"表示的是从某个时刻起，到用户最后一次修改口令时的天数。时间起点对不同的系统可能不一样。例如在SCO Linux 中，这个时间起点是1970年1月1日。
4. "最小时间间隔"指的是两次修改口令之间所需的最小天数。
5. "最大时间间隔"指的是口令保持有效的最大天数。
6. "警告时间"字段表示的是从系统开始警告用户到用户密码正式失效之间的天数。
7. "不活动时间"表示的是用户没有登录活动但账号仍能保持有效的最大天数。
8. "失效时间"字段给出的是一个绝对的天数，如果使用了这个字段，那么就给出相应账号的生存期。期满后，该账号就不再是一个合法的账号，也就不能再用来登录了。

下面是/etc/shadow的一个例子：

＃ cat /etc/shadow

root:Dnakfw28zf38w:8764:0:168:7:::

daemon:\*::0:0::::

bin:\*::0:0::::

sys:\*::0:0::::

adm:\*::0:0::::

uucp:\*::0:0::::

nuucp:\*::0:0::::

auth:\*::0:0::::

cron:\*::0:0::::

listen:\*::0:0::::

lp:\*::0:0::::

sam:EkdiSECLWPdSa:9740:0:0::::

### **3、用户组的所有信息都存放在/etc/group文件中。**

用户组的所有信息都存放在/etc/group文件中。此文件的格式也类似于/etc/passwd文件，由冒号(:)隔开若干个字段，这些字段有：

组名:口令:组标识号:组内用户列表

1. "组名"是用户组的名称，由字母或数字构成。与/etc/passwd中的登录名一样，组名不应重复。
2. "口令"字段存放的是用户组加密后的口令字。一般Linux 系统的用户组都没有口令，即这个字段一般为空，或者是\*。
3. "组标识号"与用户标识号类似，也是一个整数，被系统内部用来标识组。
4. "组内用户列表"是属于这个组的所有用户的列表/b]，不同用户之间用逗号(,)分隔。这个用户组可能是用户的主组，也可能是附加组。

/etc/group文件的一个例子如下：

root::0:root

bin::2:root,bin

sys::3:root,uucp

adm::4:root,adm

daemon::5:root,daemon

lp::7:root,lp

users::20:root,sam

### **四、添加批量用户**

Linux系统提供了创建大量用户的工具，可以让您立即创建大量用户，方法如下：

### **（1）先编辑一个文本用户文件。**

每一列按照/etc/passwd密码文件的格式书写，要注意每个用户的用户名、UID、宿主目录都不可以相同，其中密码栏可以留做空白或输入x号。一个范例文件user.txt内容如下：

user001::600:100:user:/home/user001:/bin/bash

user002::601:100:user:/home/user002:/bin/bash

user003::602:100:user:/home/user003:/bin/bash

user004::603:100:user:/home/user004:/bin/bash

user005::604:100:user:/home/user005:/bin/bash

user006::605:100:user:/home/user006:/bin/bash

### **（2）以root身份执行命令 /usr/sbin/newusers，从刚创建的用户文件user.txt中导入数据，创建用户：**

# newusers < user.txt

然后可以执行命令 vipw 或 vi /etc/passwd 检查 /etc/passwd 文件是否已经出现这些用户的数据，并且用户的宿主目录是否已经创建。

### **（3）执行命令/usr/sbin/pwunconv。**

将 /etc/shadow 产生的 shadow 密码解码，然后回写到 /etc/passwd 中，并将/etc/shadow的shadow密码栏删掉。这是为了方便下一步的密码转换工作，即先取消 shadow password 功能。

# pwunconv

### **（4）编辑每个用户的密码对照文件。**

范例文件 passwd.txt 内容如下：

user001:密码

user002:密码

user003:密码

user004:密码

user005:密码

user006:密码

### **（5）以root身份执行命令 /usr/sbin/chpasswd。**

创建用户密码，chpasswd 会将经过 /usr/bin/passwd 命令编码过的密码写入 /etc/passwd 的密码栏。

# chpasswd < passwd.txt

### **（6）确定密码经编码写入/etc/passwd的密码栏后。**

执行命令 /usr/sbin/pwconv 将密码编码为 shadow password，并将结果写入 /etc/shadow。

# pwconv

这样就完成了大量用户的创建了，之后您可以到/home下检查这些用户宿主目录的权限设置是否都正确，并登录验证用户密码是否正确。