第8章　用户账号x的管理

本章将解释如何建立新的用户账号，如何修改用户账号的属性，以及如何删除账号。不同版本的Linux，将采用不同的工具来对这一切进行管理。

8.1　何谓账号

当一台计算机供多名用户使用时，通常有必要区分各个用户，以便他们的私人文件只供他们私人使用。即使该计算机一次只供一名用户使用时，也同等重要（如果不这样的话，某某人可以看到我的情书，多难为情）。因此，每名用户都将被指定一个独一无二的用户名，这个用户名供他们登录时使用。

但是，对用户来说，还有更重要的。那就是账号。所谓账号，就是属于某个用户的所有文件、资源和信息。在银行和商业系统中，账号通常和钱有关。根据用户的使用程度，账号上的钱以不同的速度减少至零。举个例子来说，用户在磁盘空间上的消费就比较缓慢，但是处理器时间就显得要“宝贵”得多。

8.2　创建用户

Linux内核本身把用户当作数字对待。每个用户都是用一个独一无二的整数来标识的，它就是用户ID或称uid，因为对计算机来说，与处理文字化的用户名相比，对数字的处理要快得多，而且容易得多。

内核外部的一个独立的数据库负责为每个用户 ID分配一个文字化的名称，也就是用户名。这个数据库中也包含额外的一些信息。

为了创建用户，你需要把与之相关的用户信息添加到用户数据库内，并为准备创建的用户创建一个根目录。同时，还必须训练这个新用户，为它设置一个合适的初始化环境。

许多Linux版本都带有用于创建账号的程序。有几个此类的程序是可以采用的。这里，有两个命令行供你选择，它们是 adduser和useradd；另外，可能还有一个 GUI工具。不管采用什么程序，如果采用手工操作的话，其结果都将收效甚微。即使其细节翔实而复杂，这些程序仍使创建用户的操作变得琐碎平常。随后的“手工创建用户”中，将为大家介绍如何手工创建用户。

8.2.1　/etc/passwd和其他的信息性文件

Unix系统中，基本的用户数据库是一个文本文件，名为 /etc/passwd（也称为密码文件），它列出了所有有效用户名及其相关信息。该文件内，每个用户名都有一行，它被分为 7个字段，中间用冒号定界：

- 用户名。
- 密码，采用加密形式。
- 数字式的用户ID。

- 数字式的组ID。
- 账号的全名或其他说明。
- 根目录。
- 登录外壳。

有关其格式的详情，可参考passwd手册页。

系统上的任何一名用户都可能读取这个密码文件，所以他们能够从中得知另一个用户的用户名。这意味着人人都能看见密码（第二个字段）。密码文件对密码进行了加密，所以从理论上讲，以加密形式保存的密码是可靠的。但是，加密也是很容易被解密的，特别是密码比较薄弱的时候（也就是说，如果它很短，或很容易猜测得到的话）。因此，把密码放在密码文件内通常不是个好主意。

许多Linux系统都有影子密码。这是另一种保存密码的方案：加密的密码被保存在一个独立的文件内，该文件名为 /etc/shadow，只有root才能读取这个文件。 /etc/passed文件只在第二个字段内包含一个特殊的标记。任何需要验证用户是 setuid的程序，都可因此而访问影子密码文件。以只能使用密码文件内其他字段的普通程序来说，它们是不能看到这个影子密码文件的（对，这意味着密码文件中有关于用户的所有信息，但密码除外）。

8.2.2 如何选择数字式用户和组ID

大多数系统上，对数字式用户和组 ID没有具体的标准，但是在使用 NFS（网络文件系统）时，所有的系统上都必须采用同一个 uid和gid。这是因为NFS也要利用数字式uid来识别用户。如果你没有用NFS，大可让你的账号创建工具自动选择 ID。

在使用NFS时，将必须发明一种机制，用于同步更新账号信息。有个方案是 NIS系统（详情参考本书的第一部分“ 网络管理员指南 ”）。

但是，你应该尽量避免重复使用数字式 uid（和文字化的用户名），因为uid（或用户名）的新拥有者可能访问旧拥有者的文件（以及邮件等）。

8.2.3 初始化环境：/etc/skel

新用户的根目录建立时，要通过 /etc/skel目录下的文件，对它进行初始化。系统管理员可创建/etc/skel内的文件，使其为用户提供一个好的默认环境。举个例子来说，他可创建一个 /etc/skel/.profile文件，该文件把EDITOR环境参数设置为某个编辑器，对新用户来说，这个编辑器是非常友好的。

但是，通常情况下，最好尽量让 etc/skel尽可能的小，因为要更新现成用户的文件几乎是不可能的。例如，如果友好编辑器的名称发生了变化，全部现成用户都将不得不编辑自己的.profile。系统管理员可试着利用一个脚本自动处理，但毫无疑问，这样做肯定会损毁有些用户的文件。

可能的情况下，最好把全局配置放入诸如 /etc/profile之类的全局文件内。从而可能在不损毁用户本人设置的前提下，更新所有现成用户的文件。

8.2.4 手工创建一个用户

要手工创建一个用户，需遵循下面的步骤：

1) 利用vipw退出/etc/passwd，为新账号增加一个新行。注意语法。千万不能直接用编辑器编辑！vipw锁住了文件，所以其他命令不会同时对该文件进行更新。你应该令密码字段为“*”，以便用户不可能进行登录。

2) 如果你还需要创建一个新组的话，采用类似的做法，利用 vigr编辑/etc/group。

3) 利用mkdir创建用户根目录。

4) 把文件从/etc/skel复制到新建的根目录。

5) 利用chown和chmod，确定拥有权和访问许可。 -R选项是最有用的。对不同站点的访问许可同中存异，但通常都会采用下面的命令：

```
cd /home/newusername
chown -R username.group .
chmod -R go=u,go-w .
chmod go= .
```

最后，利用passwd设置密码。

设置密码之后，账号就开始发挥作用了。注意，在别的操作没有完成之前，一定不要设置密码，如若不然，用户就可能在你正忙于复制文件时，一不小心登录进来。

有时，创建无人使用的伪账号是很有必要的。例如，为了设置一个匿名 FTP服务器（以便任何人无须先获得账号，就可从这里下载文件），你需要建立一个名为ftp的账号。碰到此类情况时，通常没必要设置密码（即上面的最后一步）。实际上，最好不要设置，因为没有人能够用那个账号，除非先拥有root的身份，因为root可以成为任何一个用户。

8.3 更改用户属性

下面有几条命令，是用于更改账号属性（也就是 /etc/passwd内的相关字段）的：

- chfn —— 更改完整用户名字段。
- chsh —— 更改login外壳。
- passwd —— 更改密码。

超级用户可能用这些命令来更改任何一个账号的属性。普通用户只能更改他们自己账号的属性。对普通用户来说，有时可能还必需禁用这些命令（利用 chmod来实现），比如在有许多新用户的环境中。

其他的事情需要手工完成。比方说，要更改用户名，你需要直接编辑 /etc/passwd（记住用vipw）。类似地，要增加或删除用户，需要编辑 /etc/group（用vigr）。但是，这类任务较少执行，而且执行过程中应该谨慎：举个例子来说，如果你更改了用户名，电子邮件再也不能抵达这个用户的手中，除非你另外还建立了一个邮件别名（用户的名字可能会因为结婚而发生变化，而且他希望有一个用户名来体现自己的新名）。

8.4 删除用户

要删除一个用户，必须先删除他的所有文件、邮件别名、打印作业、 cron和at作业，以及其他对该用户的所有引用。然后，才能从 /etc/passwd和/etc/group内删除相关的行（记住，从已经添加该用户名的所有组中，删除这个用户名）。较好的做法是在开始删除用户名之前，先取消其账号（如下所示），以防止该用户在删除期间，仍然使用这个账号。

记住，用户在其根目录外面可能还有文件。利用 find命令可以找出它们：

```
find / -user username
```

但是注意，如果你的硬盘很大的话，上面的命令会花很长的一段时间。如果你装入网络磁盘，就一定要小心行事，以便自己不会丢弃网络或服务器。

有些Linux版本附带某些特殊的命令来执行这项任务；查找 deluser和userdel。然而，用手工执行一样容易，毕竟命令不是万能的。

8.5 临时禁用用户

有时，必须在不删除账号的情况下，临时禁用它。举个例子来说，用户可能没有按时交费或系统管理员怀疑有人盗用账号等。

要禁用账号，最好的方法是将其外壳改为一个特殊的程序，这个程序只打印一条消息。通过这种方式，任何想采用这个账号登录的人都会失败，而且将知道失败的原因。这条消息能够要求用户和系统管理员取得联系，以便解决存在的问题。

另外，把用户名或密码更改为别的东西也是有可能的，但那样的话，用户就不能知道到底发生了什么事。

要创建这样的特殊程序，较简单的方法是编写“ tail脚本 ”，如下所示：

```
#!/usr/bin/tail +2
This account has been closed due to a security breach.
Please call 555-1234 and wait for the men in black to arrive.
```

前两个字符“ #! ”告诉内核该行中的其他部分是一条命令，该命令需要得以运行，以便翻译这个文件。这里的tail命令将在标准输出内输出除了第一行以外的所有消息。

如果用户billg被怀疑违反了安全规则，系统管理员就会像这样：

```
# chsh -s /usr/local/lib/no-login/security billg
# su - tester
This account has been closed due to a security breach.
Please call 555-1234 and wait for the men in black to arrive.
#
```

当然，su的目的是测试改动是否见效。

tail脚本应该保存在一个单独的目录下，以便其命令不和普通用户命令发生冲突。