第8章 Linux系统用户及用户组管理

学习Linux请加QQ群： 群1(163262181) 群2(148412746) 群3(246401509) 群4(173884211)

跟阿铭学Linux邀请函 (http://www.aminglinux.com)，**猿课已上线，请加微信aminglinux84索要配套视频教程。**

关于这部分内容，阿铭在日常的linux系统管理工作中用到的并不多，但这并不代表该内容不重要。毕竟linux系统是一个多用户的系统，每个账号都干什么用，你必须了如指掌。因为这涉及到一个安全的问题。

认识/etc/passwd和/etc/shadow

这两个文件可以说是linux系统中最重要的文件之一。如果没有这两个文件或者这两个文件出问题，则你是无法正常登录linux系统的。

```
[root@localhost ~]# cat /etc/passwd | head
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
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
```

你是不是对上面的命令有点不知所以，”head” 前面的 “|” 我们叫做管道符，它的作用是把前面的命令的输出再输入给后面的命令。管道符会在后面章节中提及，这个符号用的也是蛮多的，请掌握它的用法。

‘/etc/passwd’ 由 ‘:’ 分割成7个字段，每个字段的具体含义是:

1）用户名（如第一行中的root就是用户名），代表用户账号的字符串。用户名字符可以是大小写字母、数字、减号（不能出现在首位）、点以及下划线，其他字符不合法。虽然用户名中可以出现点，但不建议使用，尤其是首位为点时，另外减号也不建议使用，因为容易造成混淆。

2）存放的就是该账号的口令，为什么是 ‘x’ 呢？早期的unix系统口令确实是存放在这里，但基于安全因素，后来就将其存放到 ‘/etc/shadow’ 中了，在这里只用一个 ‘x’ 代替。

3）这个数字代表用户标识号，也叫做uid。系统识别用户身份就是通过这个数字来的，0就是root，也就是说你可以修改test用户的uid为0，那么系统会认为root和test为同一个账户。通常uid的取值范围是0~65535(但实际上已经可以支持到4294967294)，0是超级用户（root）的标识号，1~499由系统保留，作为管理账号，普通用户的标识号从500开始，如果我们自定义建立一个普通用户，你会看到该账户的标识号是大于或等于500的。

4）表示组标识号，也叫做gid。这个字段对应着/etc/group 中的一条记录，其实/etc/group和/etc/passwd基本上类似。

5）注释说明，该字段没有实际意义，通常记录该用户的一些属性，例如姓名、电话、地址等等。不过，当你使用finger的功能时就会显示这些信息的（稍后做介绍）。

6）用户的家目录，当用户登录时就处在这个目录下。root的家目录是/root，普通用户的家目录则为/home/username，这个字段是可以自定义的，比如你建立一个普通用户test1，要想让test1的家目录在/data目录下，只要修改/etc/passwd文件中test1那行中的该字段为/data即可。

7）shell，用户登录后要启动一个进程，用来将用户下达的指令传给内核，这就是shell。Linux的shell有很多种sh，csh，ksh，tcsh，bash等，而Redhat/CentOS的shell就是bash。查看/etc/passwd文件，该字段中除了/bin/bash外还有/sbin/nologin比较多，它表示不允许该账号登录。如果你想建立一个账号不让他登录，那么就可以把该字段改成/sbin/nologin，默认是/bin/bash.

再来看看/etc/shadow这个文件，和/etc/passwd类似，用 ‘:’ 分割成9个字段。

```
[root@localhost ~]# cat /etc/shadow |head -n 3
root:$6$Wo0kPkgm$OAp0Wl2AsaE4ei4YVbxo3DIU5OBSYxn1y7qxB5Jns70Yk91AvzElsR5GmoGCC8DUXkKzK7vyiV8wXNeaWNm861:
bin:*:15628:0:99999:7:::
daemon:*:15628:0:99999:7:::
```

每个字段的含义是:

1）用户名，跟/etc/passwd对应。

2）用户密码，这个才是该账号的真正的密码，不过这个密码已经加密过了，但是有些黑客还是能够解密的。所以，该文件属性设置为000，但是root账户是可以访问或更改的。

```
[root@localhost ~]# ls -l /etc/shadow
---------- 1 root root 719 5月  10 09:02 /etc/shadow
```

目录列表

3）上次更改密码的日期，这个数字是这样计算得来的，距离1970年1月1日到上次更改密码的日期，例如上次更改密码的日期为2012年1月1日，则这个值就是‘365 x (2012-1970) + (2012-1970)/4 + 1 = 15341’. 因为如果是闰年，则有366天。

4）要过多少天才可以更改密码，默认是0，即不限制。

5）密码多少天后到期。即在多少天内必须更改密码，例如这里设置成30，则30天内必须更改一次密码，否则将不能登录系统，默认是99999，可以理解为永远不需要改。

6）密码到期前的警告期限，若这个值设置成7，则表示当7天后密码过期时，系统就发出警告告诉用户，提醒用户他的密码将在7天后到期。

7）账号失效期限。你可以这样理解，如果设置这个值为3，则表示：密码已经到期，然而用户并没有在到期前修改密码，那么再过3天，则这个账号就失效了，即锁定了。

8）账号的生命周期，跟第三段一样，是按距离1970年1月1日多少天算的。它表示的含义是，账号在这个日期前可以使用，到期后账号作废。

9）作为保留用的，没有什么意义。

新增/删除用户和用户组

1. 新增一个组

命令：groupadd

语法：`groupadd [-g GID] groupname`

```
[root@localhost ~]# groupadd grptest1
[root@localhost ~]# tail -n1 /etc/group
grptest1:x:502:
```

不加“-g”选项则按照系统默认的gid创建组，跟用户一样，gid也是从500开始的。

```
[root@localhost ~]# groupadd -g 511 grptest2
[root@localhost ~]# tail -n2 /etc/group
grptest1:x:502:
grptest2:x:511:
```

“-g”选项可以自定义gid.

2. 删除组

命令：groupdel

```
[root@localhost ~]# groupdel grptest2
[root@localhost ~]# tail -n3 /etc/group
testgroup:x:500:
user1:x:501:
grptest1:x:502:
```

该命令没有特殊选项，但有一种情况不能删除组：

```
[root@localhost ~]# groupdel user1
groupdel: cannot remove the primary group of user 'user1'
```

这是因为user1组中包含user1账户，只有删除user1账户后才可以删除该组。

3. 增加账户

命令：useradd

语法：`useradd [-u UID] [-g GID] [-d HOME] [-M] [-s]`

‘-u’ 自定义UID

‘-g’ 使其属于已经存在的某个组，后面可以跟组id, 也可以跟组名

‘-d’ 自定义用户的家目录

‘-M’ 不建立家目录

‘-s’ 自定义shell

```
[root@localhost ~]# useradd test10
[root@localhost ~]# tail -n1 /etc/passwd
test10:x:500:503::/home/test10:/bin/bash
[root@localhost ~]# tail -n1 /etc/group
test10:x:503:
```

‘useradd’ 不加任何选项直接跟用户名，则会创建一个跟用户名同样名字的组。

```
[root@localhost ~]# useradd -u510 -g 513 -M -s /sbin/nologin user11
```

```
useradd: group '513' does not exist
[root@localhost ~]# useradd -u510 -g 502 -M -s /sbin/nologin user11
[root@localhost ~]# useradd -u511 -g grptest1 user12
[root@localhost ~]# tail -n2 /etc/passwd
user11:x:510:502::/home/user11:/sbin/nologin
user12:x:511:502::/home/user12:/bin/bash
[root@localhost ~]# tail -n2 /etc/group
grptest1:x:502:
test10:x:503:
```

‘-g’ 选项后面跟一个不存在的gid会报错，提示该组不存在。刚刚上面说过 ‘-M’ 选项加上后则不建立用户家目录，但是在/etc/passwd文件中仍然有这个字段。但是你使用 `ls /home/user11` 查看一下会提示该目录不存在。所以 ‘-M’ 选项的作用只是不创建那个目录。

```
[root@localhost ~]# ls /home/user11
ls: 无法访问/home/user11: 没有那个文件或目录
```

4. 删除账户

命令：userdel

语法：`userdel [-r] username`

```
[root@localhost ~]# ls -ld /home/user12
drwx------ 3 user12 grptest1 4096 5月  11 07:12 /home/user12
[root@localhost ~]# userdel user12
[root@localhost ~]# ls -ld /home/user12
drwx------ 3 511 grptest1 4096 5月  11 07:12 /home/user12
[root@localhost ~]# ls -ld /home/test10/
drwx------ 3 test10 test10 4096 5月  11 07:09 /home/test10/
[root@localhost ~]# userdel  -r test10
[root@localhost ~]# ls -ld /home/test10/
ls: 无法访问/home/test10/: 没有那个文件或目录
```

‘-r’ 选项的作用只有一个，就是删除账户的时候连带账户的家目录一起删除。

chfn 更改用户的finger （不常用）

阿铭几乎没有用过这个功能，只简单介绍一下即可，而你也许了解一下即可。前面内容中提到了findger，即在/etc/passwd文件中的第5个字段中所显示的信息，那么如何去设定这个信息呢？

```
[root@localhost ~]# chfn user11
Changing finger information for user11.
Name []: user11
Office []: user11's office
Office Phone []: 12345678
Home Phone []: 123456789

Finger information changed.
[root@localhost ~]# grep 'user11' /etc/passwd
user11:x:510:502:user11,user11's office,12345678,123456789:/home/user11:/sbin/nologin
```

‘chfn’ 命令可以修改用户的findger信息，比如name, office, office phone 以及 Home phone.修改完后，就会在/etc/passwd文件中的user11的那一行第五个字段中看到相关信息了，默认是空的。 在本例中，阿铭使用了 “grep” 命令，它是用来过滤指定关键词的行，阿铭会在以后的章节中详细介绍它的用法。

创建/修改一个用户的密码

命令：passwd

语法：`passwd [username]`

等创建完账户后，默认是没有设置密码的，虽然没有密码，但该账户同样登录不了系统。只有设置好密码后方可登录系统。为用户创建密码时，为了安全起见，请尽量设置复杂一些。你可以按照这样的规则来设置密码：

1. 长度大于10个字符；
2. 密码中包含大小写字母数字以及特殊字符 ‘*’, ‘&’, ‘%’ 等；
3. 不规则性（不要出现root, happy, love, linux, 7758520, 111111等等单词或者数字）；
4. 不要带有自己名字、公司名字、自己电话、自己生日等。

```
[root@localhost ~]# passwd
更改用户 root 的密码 。
新的 密码：
重新输入新的 密码：
passwd： 所有的身份验证令牌已经成功更新。
```

“passwd” 后面不加username则是修改当前账户的密码。如果你登陆的是root账户，后面可以跟普通账户的名字，意思是修改指定账户的密码。

```
[root@localhost ~]# passwd user11
更改用户 user11 的密码 。
新的 密码：
重新输入新的 密码：
passwd： 所有的身份验证令牌已经成功更新。
```

只有root才可以修该其他账户的密码，普通账户只能修改自己的密码，其他账户的密码是不可以修改的。

命令：mkpasswd

这个命令阿铭经常用来生成密码，省的自己去想。默认你的Linux是没有这个命令的，需要安装一个包“expect”，如果你的CentOS可以上网，请使用命令 `yum install -y expect` 即可完成安装。安装好后，输入命令：

```
[root@localhost ~]# mkpasswd
HXut8oy*8
```

生成的随机字符串就可以作为一个密码，只不过这个密码不容易记忆，没有关系，阿铭等会介绍一个小工具来帮你记录密码，而且很安全。

用户身份切换

Linux系统中，有时候普通用户有些事情是不能做的，除非是root用户才能做到。这时就需要临时切换到root身份来做事了。下面阿铭带你做一个小实验，创建“test”账户，并修改其密码，这样我们就可以使用test账户登陆Linux了。

```
[root@localhost ~]# useradd test
[root@localhost ~]# passwd test
更改用户 test 的密码 。
新的 密码：
重新输入新的 密码：
passwd： 所有的身份验证令牌已经成功更新。
```

然后用test账户登陆Linux.

```
login as: test
test@10.72.137.78's password:
[test@localhost ~]$ whoami
test
```

登陆后，使用“whoami”命令可以查看当前用户是谁。

命令su

语法：`su [-] username`

后面可以跟 ‘-’ 也可以不跟，普通用户su不加username时就是切换到root用户，当然root用户同样可以su到普通用户。 ‘-’ 这个字符的作用是，加上后会初始化当前用户的各种环境变量，关于环境变量这部分内容阿铭放在后面的章节中讲解。 下面阿铭做个简单的实验来说明加与不加 ‘-’ 的区别：

```
[test@localhost ~]$ pwd
/home/test
[test@localhost ~]$ su
密码：
[root@localhost test]# pwd
/home/test
[root@localhost test]# exit
exit
[test@localhost ~]$ su -
密码：
[root@localhost ~]# pwd
/root
```

如果不加 ‘-’ 切换到root账户下时，当前目录没有变化，而加上 ‘-’ 切换到root账户后，当前目录为root账户的家目录，这跟直接登陆root账户是一样的。当用root切换普通用户时，是不需要输入密码的。这也体现了root用户至高无上的权利。

命令：sudo

用su是可以切换用户身份，如果每个普通用户都能切换到root身份，如果某个用户不小心泄漏了root的密码，那岂不是系统非常的不安全？没有错，为了改进这个问题，产生了sudo这个命令。使用sudo执行一个root才能执行的命令是可以办到的，但是需要输入密码，这个密码并不是root的密码而是用户自己的密码。默认只有root用户能使用sudo命令，普通用户想要使用sudo，是需要root预先设定的，即，使用 `visudo` 命令去编辑相关的配置文件/etc/sudoers. 如果没有visudo这个命令，请使用 `yum install -y sudo` 安装。

默认root能够sudo是因为这个文件中有一行 “root ALL=(ALL) ALL” 在该行下面加入 “test ALL=(ALL) ALL” 就可以让test用户拥有了sudo的权利。使用 “visudo” 命令编辑/etc/sudoers配置文件，其实它的操

作方法和前面阿铭介绍的“vi”命令使用方法是一样的，按‘i’进入编辑模式，编辑完成后，按“Esc”，再输入”:wq”完成保存。

```
## Allow root to run any commands anywhere
root    ALL=(ALL)       ALL
test    ALL=(ALL)       ALL
```

此时可以验证一下test账户的权限了。

```
[root@localhost ~]# su test
[test@localhost root]$ ls
ls: 无法打开目录.: 权限不够
[test@localhost root]$ sudo ls

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for test:
123  456  789  anaconda-ks.cfg  dirb  install.log  install.log.syslog  test  test1  test2  test3
```

由于切换到test账户后的当前目录依旧是在/root 下，test账户没有任何权限，所以‘ls’的时候提示说权限不够，然而使用 `sudo ls` 输入test账户自身的密码后就有权限了。初次使用sudo 时会有上面的一大段提示，而后再次使用sudo 命令则不再提示。

如果每增加一用户就设置一行，这样太麻>烦了。所以你可以这样设置。把“# %wheel ALL=(ALL) ALL”前面的‘# ’去掉，让这一行生效。它的意思是，wheel这个组的所有用户都拥有了sudo的权利。接下来就需要你把想让有sudo权利的所有用户加入到wheel这个组中即可。

```
## Allows people in group wheel to run all commands
%wheel  ALL=(ALL)       ALL
```

配置文件/etc/sudoers包含了诸多配置项，可以使用命令 `man sudoers` 来获得帮助信息。下面阿铭介绍一个很实用的案例，我们的需求是把Linux服务器设置成这个样子：只允许使用普通账户登陆，而普通账户登录后，可以不输入密码就能sudo切换到root账户。下面但是阿铭的配置：

```
[root@localhost ~]# visudo
```

然后在文件的最后面加入三行：

```
User_Alias USER_SU = test, test1, aming
Cmnd_Alias SU = /bin/su
USER_SU ALL=(ALL) NOPASSWD: SU
```

保存配置文件后，使用test, test1, aming 三个账户登陆Linux后，执行命令 `sudo su -` 切换到root账户，获取root账户的所有权利。

```
[root@localhost ~]# su - test
[test@localhost ~]$ sudo su -
[root@localhost ~]# whoami
root
```

而不让root直接登陆，这个简单，设置一个非常复杂连自己都记不住的密码。不过这样也有一个问题，就是普通用户可以su到root，然后他再自己修改简单的密码就能直接root登陆了不是嘛？的确有这个问题，其实阿铭还有一个更好的办法，会在后面的扩展学习章节中介绍。

使用密码记录工具keepass来保存密码

在第3章，阿铭曾经给过你建议，密码不要保存在文档中，那样不安全，如果密码很多而且又很复杂，人的大脑是不可能很容易记住的，只能记录下来，如果不能记在文档中那记在哪里呢？阿铭介绍给你一款记录密码的软件，是在windows上用的哦！它就是keepass.

Keepass官网地址是：http://www.keepass.info 在官网keepass是这样被形容的：The free, open source, light-weight and easy-to-use password manager. 没错，这款软件是免费的、开源的、容易使用轻量级的密码管理工具。

我们下载最新版本的keepass，当前最新的发行版本为2.22,下载地址：http://downloads.sourceforge.net/keepass/KeePass-2.22-Setup.exe 下载后安装它。安装过程没有什么可说的，直接next一直到安装完成。

1. 安装好后，运行keepass，首先创建一个新的密码库文件。

点菜单栏“file”然后选择“new”，为密码库文件找一个安全的地方存放。接下来，为我们的密码文件创建一个“master password”，这个密码以后每次我们查看密码的时候都需要输入，输入正确后才可以查看，这样的设计也是为了安全。设置好密码后连续点两个“ok”完成创建密码库文件。

2. 增加一个group

鼠标选中左侧的 “NewDatebase”, 点右键选择 “Add Group”, 单击后创建新组，然后更改组名，比说叫做 “test”. 当然组下面还可以创建组，方法一样的。

3. 创建一个Entry

鼠标左键先点一下刚才创建的组 “test” ， 然后在右侧空白处右键单击，选择 “Add Entry”. 弹出一个会话窗口，Title 自定义，方便我们以后查找; User name 用来记录密码的用户是谁; Password 这个默认就存在了，也可以更改，点一下后面的 ”...” 图标可以查看密码的内容，再点一下变为不可见状态; URL 用来记录网址，方便我们跳转，比如这个密码为某个网站的某个会员的密码，那如果在这里填写了该网址地址，则可以直接跳转到那个网站，可以留空; Notes 用来写一些与这个密码相关的信息，方便我们记忆，可以留空。

4. 修改Entry信息

在右侧窗口，选中要修改的Entry那行，鼠标移动到Title区域，双击则会跳出一个会话窗口，我们可以更改Entry的各项信息。

5. 获取Entry密码

同样是在右侧窗口，选中要获取的密码那行，鼠标移动到Password区域，直接双击，就把密码复制到剪切板了，密码会在剪切板中保存12s，过期会失效，所以你应该在12s内把密码粘贴。

阿铭建议你最好再扩展学习一下: http://www.aminglinux.com/bbs/thread-5409-1-1.html

教程答疑: 请移步这里.

欢迎你加入 阿铭学院 和阿铭一起学习Linux，让阿铭成为你Linux生涯中永远的朋友吧！