第6章 Linux系统用户与用户组管理（上）

阿铭linux
2023年10月23日 10:18

关于这部分内容，阿铭在Linux系统日常管理工作中用得并不多，但并不代表这部分内容不重要。毕竟Linux系统是一个多用户系统，每个账号用来干什么，我们必须了如指掌，因为这涉及安全问题。

安装完系统后，我们就一直使用root账号来操作，其实这并不安全。因为root账号权限太高，容易误操作。阿铭建议你以后在工作中尽量避免直接使用root账号登录系统，使用普通用户也可以完成大部分工作。

6.1 认识用户配置文件

接下来要讲的这两个配置文件可以说是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了问题，则无法正常登录系统。下面咱们先来看看第一个文件，示例命令如下：

```
[root@aminglinux01 ~]# 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
operator:x:11:0:operator:/root:/sbin/nologin
```

看到上面那条命令，你是不是有点不知所以呢？其实，head前面的符号|，我们称为管道符，它的作用是把前面的命令的输出再输入给后面的命令。管道符在第11章中还会介绍，阿铭用得也是蛮多的，请掌握它的用法。

6.1.1 配置文件解说

可以是大小写字母、数字、减号（不能出现在首位）、点或下划线，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。另外，减号也不建议使用，容易造成混淆。

- 第2个字段存放的是该账号的口令。这里为什么是x呢？早期的Unix系统口令确实存放在这里，但基于安全因素，后来就将其存放到/etc/shadow中了，这里只用一个x代替。
- 第3个字段为一个数字，这个数字代表用户标识号，也称为uid。系统就是通过这个数字识别用户身份的。这里的0就是root，也就是说我们可以修改test用户的uid为0，那么系统会认为root和test为同一个账户。uid的取值范围是0~655 35（但实际上已经可以支持到429 496 729 4），0是超级用户（root）的标识号，Rocky 8的普通用户标识号从1000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1000的。
- 第4个字段也是数字，表示组标识号，也称为gid。这个字段对应着/etc/group中的一条记录，其实/etc/group和/etc/passwd基本类似。
- 第5个字段为注释说明，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。我们可以使用chfn命令来更改这些信息，这在稍后会介绍。
- 第6个字段为用户的家目录，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，用户家目录是可以自定义的。比如，建立一个普通用户test1，要想让test1的家目录在/data目录下，只要将/etc/passwd文件中对应该用户那行中的本字段修改为/data即可。
- 最后一个字段为用户的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sh、csh、ksh、tcsh、bash等多种，而RHEL/Rocky的shell就是bash。查看/etc/passwd文件，该字段中除了/bin/bash，还有很多/sbin/nologin，它表示不允许该账号登录。如果想建立一个不允许登录的账号，可以把该字段改成/sbin/nologin，默认是/bin/bash。

6.1.2 /etc/shadow解说

/etc/shadow和/etc/passwd类似，由：分割成9个字段，示例命令如下：

```
[root@aminglinux01 ~]# cat /etc/shadow |head -n 3
root:$6$by/DDoSKRcnPViAW$Xl18y12843bSwfdWBYYMj9ZuLjECSEIcq1EXhrxe0UbKsfY19NbXf1GLtLFn87RwRWyS1zk4Q01YsFJF5JR0h.::0:99999:7:::
bin:*:18700:0:99999:7:::
daemon:*:18700:0:99999:7:::
```

每个字段的含义如下所示：

- 第1个字段为用户名，与上个配置文件对应。
- 第2个字段为用户密码，是该账号的真正密码。这个密码已经加密，但是有些黑客还是能够解密的。所以，将该文件属性设置为000，但root账户是可以访问或更改的。使用命令ls -l查看该文件的权限，示例命令如下：

 # ls -l /etc/shadow

---------- 1 root 689 12月 30 07:46 /etc/shadow

- 第3个字段为上次更改密码的日期，这个数字以1970年1月1日和上次更改密码的日期为基准计算而来。例如，上次更改密码的日期为2020年1月1日，则这个值就是365* (2020-1970)+(2020-1970)/4+1=18263。如果是闰年，则有366天。
- 第4个字段为要过多少天才可以更改密码，默认是0，即不受限制。
- 第5个字段为密码多少天后到期，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。
- 第6个字段为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，提醒用户他的密码将在7天后到期。
- 第7个字段为账号失效期限。如果这个值设置为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，这个账号便失效，即锁定。
- 第8个字段为账号的生命周期。跟第3个字段一样，这个周期是按距离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，到期后账号将作废。
- 最后一个字段作为保留用的，没有什么意义。

上面关于密码文件字段的介绍内容偏多并不太容易记住，在这里阿铭提醒你，这部分内容无需记住，只需要了解即可，因为在工作中我们几乎用不到这些知识点。

6.2 用户和用户组管理

6.2.1 新增组的命令groupadd

命令groupadd的格式为 groupadd [-g GID] groupname，示例命令如下：

 # groupadd grptest1

 # tail -n1 /etc/group

grptest1:x:1002:

如果不加-g选项，则按照系统默认的gid创建组。跟uid一样，gid也是从1000开始的。我们也可以按如下操作自定义gid：

 # groupadd -g 1008 grptest2

 # tail -n2 /etc/group

grptest1:x:1002:

grptest2:x:1008:

6.2.2 删除组的命令groupdel

有时，我们会有删除组的需求，此时可进行如下操作：

 # groupdel grptest2

 # tail -n2 /etc/group

slocate:x:21:

grptest1:x:1002:

命令groupdel没有特殊选项，但有一种情况不能删除组，如下所示：

 # groupdel user1

groupdel：不能移除用户“user1”的主组

上例中，user1组中包含user1账户，只有删除user1账户后才可以删除该组。

6.2.3 增加用户的命令useradd

从字面意思上来看，useradd就是增加用户，该命令的格式为useradd [-u UID] [-g GID] [-d HOME] [-M] [-s]，其中各个选项的具体含义如下。

- **-u**：表示自定义UID。
- **-g**：表示使新增用户属于已经存在的某个组，后面可以跟组id，也可以跟组名。
- **-d**：表示自定义用户的家目录。
- **-M**：表示不建立家目录。
- **-s**：表示自定义shell。

下面我们先来新建一个用户test10，示例命令如下：

 # useradd test10

 # tail -n1 /etc/passwd

test10:x:1001:1001::/home/test10:/bin/bash

 # tail -n1 /etc/group

test10:x:1001:

如果useradd不加任何选项，直接跟用户名，则会创建一个跟用户名同名的组。当然，很多时候需要我们自己去定义uid、gid或者所属的组，示例命令如下：

 # useradd -u1005 -g 1006 -M -s /sbin/nologin user11

 # useradd -u1006 -g grptest1 user12

 # tail -n2 /etc/passwd

user11:x:1005:1001::/home/user11:/sbin/nologin

user12:x:1006:1002::/home/user12:/bin/bash

 # tail -n2 /etc/group

user1:x:1003:

test10:x:1001:

如果-g选项后面跟一个不存在的gid，则会报错，提示该组不存在。刚刚上面说过，加上-M选项后，则不建立用户家目录，但在第一个配置文件中仍然有这个字段。如果你使用命令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。下面我们来查看user11的家目录，会提示我们目录不存在，示例命令如下：

 # ls /home/user11

ls: 无法访问/home/user11: 没有那个文件或目录

6.2.4 删除账户的命令userdel

命令userdel的格式为userdel [-r] username，其中-r选项的作用是，当删除用户时，一并删除该用户的家目录。下面我们先来看看user12的家目录，示例命令如下：

 # ls -ld /home/user12

drwx------ *2 user12 grptest1 62 1月 2 06:47 /home/user12*

如果不加-r选项，则会直接删除用户user12，但保留其家目录，如下所示：

 # userdel user12

 # ls -ld /home/user12

drwx------ *2 user12 grptest1 62 1月 2 06:47 /home/user12*

此时user12的家目录还在，那么我们再加上-r选项删除user1用户，如下所示：

 # ls -ld /home/user1

drwx------ 2 user1 test10 62 12月 30

07:46 /home/user1

 # userdel -r user1

 # ls -ld /home/usre1

ls: 无法访问/home/user1: 没有那个文件或目录

此时user1的家目录已经不复存在。

置顶 请点“+关注”，并点赞、投币，然后看你的私信，我会送你一份价值千元的运维笔记。
2023-10-23 10:19 回复

月影薄纱悟空 LV2
都是干货
2023-10-23 17:49 回复

月影薄纱悟空 LV2
加油
2023-10-23 17:47 回复

9
1
2
0
3

回到
旧版