Linux 用户与用户组关系

1、用户和用户组文件

在 linux 中，用户帐号，用户密码，用户组信息和用户组密码均是存放在不同的配置文件中的。

在 linux 系统中，所创建的用户帐号和其相关信息 (密码除外) 均是存放在 / etc/passwd 配置文件中。由于所有用户对 passwd 文件均有读取的权限，因此密码信息并未保存在该文件中，而是保存在了 / etc/shadow 的配置文件中。

在 passwd 文件中，一行定义一个用户帐号，每行均由多个不同的字段构成，各字段值间用 ":" 分隔，每个字段均代表该帐号某方面的信息。

在刚安装完成的 linux 系统中，passwd 配置文件已有很多帐号信息了，这些帐号是由系统自动创建的，他们是 linux 进程或部分服务程序正常工作所需要使用的账户，这些账户的最后一个字段的值一般为 / sbin/nologin，表示该帐号不能用来登录 linux 系统。

在 passwd 配置文件中，从左至右各字段的对应关系及其含义：

用户帐号	用户密码	用户 ID	用户组 ID	用户名全称	用户主目录	用户所使用的 shell
root	x	0	0	root	/root	/bin/bash

由于 passwd 不再保存密码信息，所以用 x 占位代表。

若要使某个用户账户不能登录 linux，只需设置该用户所使用的 shell 为 / sbin/nologin 即可。比如，对于 FTP 账户，一般只允许登录和访问 FTP 服务器，不允许登录 linux 操作系统。若要让某用户没有 telnet 权限，即不允许该用户利用 telnet 远程登录和访问 linux 操作系统，则设置该用户所使用的 shell 为 / bin/true 即可。若要让用户没有 telnet 和 ftp 登录权限，则可设置该用户的 shell 为 / bin/false。

在 / etc/shells 文件中，若没有 / bin/true 或 / bin/false，则需要手动添加：

```
[root@localhost ~]# echo "/bin/false">>/etc/shells
[root@localhost ~]# echo "/bin/true">>/etc/shells
```

2、用户密码文件

为安全起见，用户真实的密码采用 MD5 加密算法加密后，保存在 / etc/shadow 配置文件中，该文件只有 root 用户可以读取。

与 passwd 文件类似，shadow 文件也是每行定义和保存一个账户的相关信息。第一个字段为用户帐户名，第二个字段为账户的密码。

3、用户组帐号文件

用户组帐号信息保存在 / etc/group 配置文件中，任何用户均可以读取。用户组的真实密码保存在 / etc/gshadow 配置文件中。

在 group 中，第一个字段代表用户组的名称，第二个字段为 x，第三个为用户组的 ID 号，第四个为该用户组的用户成员列表，各用户名间用逗号分隔。

4、添加用户

创建或添加新用户使用 useradd 命令来实现，其命令用法为：

useradd [option] username

该命令的 option 选项较多，常用的主要有：
-c 注释　　用户设置对账户的注释说明文字
-d 主目录　　指定用来取代默认的 / home/username 的主目录
-m　　若主目录不存在，则创建它。-r 与 - m 相结合，可为系统账户创建主目录
-M　　不创建主目录
-e date　　指定账户过期的日期。日期格式为 MM/DD/YY
-f days　　帐号过期几日后永久停权。若指定为 -，则立即被停权，若为 - 1，则关闭此功能
-g 用户组　　指定将用户加入到哪个用户组，该用户组必须存在
-G 用户组列表 指定用户同时加入的用户组列表，各组用逗分隔
-n　　不为用户创建私有用户组
-s shell　　指定用户登录时使用的 shell，默认为 / bin/bash
-r　　创建一个用户 ID 小于 500 的系统账户，默认不创建对应的主目录
-u 用户 ID　　手动指定新用户的 ID 值，该值必须唯一，且大于 499
-p password 为新建用户指定登录密码。此处的 password 是对应登录密码经 MD5 加密后所得到的密码值，不实真实密码原文，因此在实际应用中，该参数选项使用较少，通常单独使用 passwd 命令来为用户设置登录密码。

示例：

若要创建一个名为 nisj 的用户，并作为 babyfish 用户组的成员，则操作命令为：

```
[root@localhost ~]# useradd -g babyfish nisj
[root@localhost ~]# id nisj
uid=502(nisj) gid=500(babyfish) groups=500(babyfish)
[root@localhost ~]# tail -1 /etc/passwd
nisj:x:502:500::/home/nisj:/bin/bash
```

添加用户时，若未用 - g 参数指定用户组，则系统默认会自动创建一个与用户帐号同名的私有用户组。若不需要创建该私有用户组，则可选用 - n 参数。
比如，添加一个名为 nsj820 的账户，但不指定用户组，其操作结果为：

```
[root@localhost ~]# useradd nsj820
[root@localhost ~]# id nsj820
```

uid=503(nsj820) gid=503(nsj820) groups=503(nsj820)
[root@localhost ~]# tail -1 /etc/passwd
nsj820:x:503:503::/home/nsj820:/bin/bash
[root@localhost ~]# tail -2 /etc/passwd
nisj:x:502:500::/home/nisj:/bin/bash
nsj820:x:503:503::/home/nsj820:/bin/bash #系统自动创建了名为 nsj820 的用户组，ID 号为 503

创建用户账户时，系统会自动创建该用户对应的主目录，该目录默认放在 / home 目录下，若要改变位置，可以利用 - d 参数指定；对于用户登录时使用的 shell，默认为 / bin/bash，若要更改，则使用 - s 参数指定

例如，若要创建一个名为 vodup 的账户，主目录放在 / var 目录下，并指定登录 shell 为 / sbin/nologin，则操作命令为：

[root@localhost ~]# useradd -d /var/vodup -s /sbin/nologin vodup
[root@localhost ~]# id vodup
uid=504(vodup) gid=504(vodup) groups=504(vodup)
[root@localhost ~]# tail -1 /etc/passwd
vodup:x:504:504::/var/vodup:/sbin/nologin
[root@localhost ~]# tail -1 /etc/group
vodup:x:504:

5、设置帐号属性

对于已创建好的用户，可使用 usermod 命令来修改和设置账户的各项属性，包括登录名，主目录，用户组，登录 shell 等，该命令用法为：

usermod [option] username
部分 option 选项

（1）改变用户帐户名

使用 - l 参数来实现，命令用法为：
usermod -l 新用户名 原用户名

例如，若要将用户 nsj820 更名为 nsj0820，则操作命令为：
[root@localhost ~]# usermod -l nsj0820 nsj820
[root@localhost ~]# id nsj0820
uid=503(nsj0820) gid=503(nsj820) groups=503(nsj820)
[root@localhost ~]# tail -1 /etc/passwd
nsj0820:x:503:503::/home/nsj820:/bin/bash
从输出结果可见，用户名已更改为 nsj0820。主目录仍为原来的 / home/nsj820，若也要更

改为 / home/nsj0820，则可通过执行以下命令来实现
[root@localhost ~]# usermod -d /home/nsj0820 nsj0820
[root@localhost ~]# id nsj0820
uid=503(nsj0820) gid=503(nsj820) groups=503(nsj820)
[root@localhost ~]# tail -1 /etc/passwd
nsj0820:x:503:503::/home/nsj0820:/bin/bash
[root@localhost home]# mv /home/nsj820 /home/nsj0820

（2）锁定账户

若要临时禁止用户登录，可将该用户账户锁定。锁定账户可利用 - L 参数来实现，其命令用法为：

usermod -L 要锁定的账户

linux 锁定用户，是通过在密码文件 shadow 的密码字段前加“！”来标识该用户被锁定。

[root@localhost home]# usermod -L nsj0820
[root@localhost home]# tail -1 /etc/shadow
nsj0820:!1JEW25RtU$X9kIdwJi/HPzSKMVe3EK30:16910:0:99999:7:::

但通过 root 用户进去，然后 su 到被锁定的用户，是可以进去的。

（3）解锁账户

要解锁账户，可以使用带 **-U** 参数的 usermod 命令来实现。

[root@localhost ~]# usermod -U nsj0820
[root@localhost ~]# tail -1 /etc/shadow
nsj0820:1JEW25RtU$X9kIdwJi/HPzSKMVe3EK30:16910:0:99999:7:::

6、删除账户

要删除账户，可以使用 userdel 命令来实现，其用法为：
userdel [-r] 帐户名

-r 为可选项，若带上该参数，则在删除该账户的同时，一并删除该账户对应的主目录。

[root@localhost ~]# userdel -r nsj0820

若要设置所有用户账户密码过期的时间，则可通过修改 / etc/login.defs 配置文件中的 PASS_MAX_DAYS 配置项的值来实现，其默认值为 99999，代表用户账户密码永不过期。其中 PASS_MIN_LEN 配置项用于指定账户密码的最小长度，默认为 5 个字符。

7、设置用户登录密码

使用 passwd 命令来设置，其命令用法为：

passwd [帐户名]

若指定了帐户名称，则设置指定账户的登录密码，原密码自动被覆盖。**只有 root 用户才有权设置指定账户的密码。一般用户只能设置或修改自己账户的密码（不带参数）。**

例如，若要设置 nisj 账户的登陆密码，则操作命令为：

```
[root@localhost home]# passwd nisj
Changing password for user nisj.
New password:
BAD PASSWORD: it is too short
BAD PASSWORD: is too simple
Retype new password:
passwd: all authentication tokens updated successfully.
```

账户登录密码设置后，该账户就可以登录系统了。

8、锁定 / 解锁账户密码及查询密码状态、删除账户密码

在 linux 中，除了用户账户可被锁定外，账户密码也可被锁定，任何一方被锁定后，都将无法登录系统。只有 root 用户才有权执行该命令，锁定账户密码使用带 -l 选项的 passwd 命令，其用法为：

passwd -l 帐户名

passwd -u 帐户名 #解锁账户密码

```
[root@localhost home]# passwd -l nisj
Locking password for user nisj.
passwd: Success
[root@localhost home]# passwd -u nisj
Unlocking password for user nisj.
passwd: Success
```

要查询当前账户的密码是否被锁定，可以使用带 -S 参数的 passwd 命令来实现，其用法为：

passwd -S 账户名

例如

```
[root@localhost home]# passwd -S nisj
nisj PS 2016-04-18 0 99999 7 -1 (Password set, MD5 crypt.)
```

如要删除账户的密码，使用带 -d 参数的 passwd 命令来实现，该命令也只有 root 用户才有权执行，其用法为：

passwd -d 帐户名

帐户密码被删除后，将不能登录系统，除非重新设置密码。

9、创建用户组

用户和用户组属于多对多关系，一个用户可以同时属于多个用户组，一个用户组可以包含多个不同的用户。

创建用户组使用 groupadd 命令，其命令用法为：
groupadd [-r] 用户组名称

若命令带有 -r 参数，则创建系统用户组，该类用户组的 GID 值小于 500；若没有 -r 参数，则创建普通用户组，其 GID 值大于或等于 500.

10、修改用户组属性

用户组创建后，根据需要可对用户组的相关属性进行修改。对用户组属性的修改，主要是修改用户组的名称和用户组的 GID 值。

（1）改变用户组的名称

若要对用户组进行重命名，可使用带 -n 参数的 groupmod 命令来实现，其用法为：
groupmod -n 新用户组名 原用户组名

对于用户组改名，不会改变其 GID 的值

比如，若要将 student 用户组更名为 teacher 用户组，则操作命令为：

```
[root@localhost home]# groupadd student
[root@localhost home]# tail -1 /etc/group
student:x:505:
[root@localhost home]# groupmod -n teacher student
[root@localhost home]# tail -1 /etc/group
teacher:x:505:
```

（2）重设用户组的 GID

用户组的 GID 值可以重新进行设置修改，但不能与已有用户组的 GID 值重复。对 GID 进行修改，不会改变用户名的名称。

要修改用户组的 GID，可使用带 -g 参数的 groupmod 命令，其用法为：
groupmod -g new_GID 用户组名称

例如，若要将 teacher 组的 GID 更改为 506，则操作命令为：

```
[root@localhost home]#  groupmod -g 506 teacher
[root@localhost home]# tail -1 /etc/group
teacher:x:506:
```

11、删除用户组

删除用户组使用 groupdel 命令来实现，其用法为：
groupdel 用户组名

在删除用户组时，被删除的用户组不能是某个账户的私有用户组，否则将无法删除，若要删除，则应先删除引用该私有用户组的账户，然后再删除用户组。

[root@localhost home]# groupdel teacher
[root@localhost ~]# grep teacher /etc/group　#没有输出，说明 teacher 用户组以不存在，删除成功

12、添加用户到指定的组 / 从指定的组中移除用户

可以将用户添加到指定的组，使其成为该组的成员。其实现命令为：

gpasswd -a 用户账户　用户组名

若要从用户组中移除某用户，其实现命令为：

gpasswd -d 用户账户　用户组名

例如:

[root@localhost home]# groupadd student
[root@localhost home]# gpasswd -a nisj student
Adding user nisj to group student
[root@localhost home]# id nisj
uid=502(nisj) gid=500(babyfish) groups=500(babyfish),505(student)
[root@localhost home]# gpasswd -d nisj student
Removing user nisj from group student
[root@localhost home]# id nisj
uid=502(nisj) gid=500(babyfish) groups=500(babyfish)
[root@localhost home]# groups nisj
nisj : babyfish

13、设置用户组管理员

添加用户到组和从组中移除某用户，除了 root 用户可以执行该操作外，用户组管理员也可以执行该操作。

要将某用户指派为某个用户组的管理员，可使用以下命令来实现；

gpasswd -A 用户账户 要管理的用户组

命令功能：**将指定的用户设置为指定用户组的用户管理员。用户管理员只能对授权的用户组进行用户管理 (添加用户到组或从组中删除用户)，无权对其他用户组进行管理。**

[root@localhost home]# gpasswd -a nisj student
Adding user nisj to group student
[root@localhost home]# gpasswd -A nisj student
[root@localhost home]# useradd stu
[root@localhost home]# gpasswd -a stu student
Adding user stu to group student
[root@localhost home]# groups stu

stu : stu student
[root@localhost home]# su - nisj
[nisj@localhost ~]$ gpasswd -d stu student
Removing user stu from group student
[nisj@localhost ~]$ gpasswd -d stu stu
gpasswd: Permission denied.

14、用户其他相关

另外，linux 还提供了 id，whoami 和 groups 等命令，用来查看用户和组的状态。**id 命令用于显示当前用户的 uid，gid 和所属的用户组的列表；whoami 用于查询当前用户的名称；groups 用于产看指定用户所隶属的用户组。**

同时，我们可以使用图形界面来管理用户和用户组，**系统 ---> 管理 ---> 用户和组群可以打开相应的配置界面。**

附：将用户添加到组中，也可以如下操作
将一个用户添加到用户组中，千万不能直接用：
usermod -G groupA
这样做会使你离开其他用户组，仅仅做为这个用户组 groupA 的成员。
应该用 加上 -a 选项：
usermod -a -G groupA user
(FC4: usermod -G groupA,groupB,groupC user)
-a 代表 append， 也就是 将自己添加到 用户组 groupA 中，而不必离开其他用户组。