**用户和用户组的管理**

1. **用户的概述**
2. 用户概述
3. 用户分类

3类用户：

1. 管理员 root,UID为0，有最高权限
2. 系统用户 UID 1-999
3. 自定义用户 UID 1000-6000
4. 用户的配置文件
5. 用户基本信息文件 /etc/passwd

文件拥有者：root

文件权限：rw-r--r-- (只有管理员才可以写文件)

文件的格式：

用户名：密码：UID：GID：用户描述：用户主目录：用户登录Shell

1. 密码等相关安全信息文件 /etc/shadow

文件拥有者：root

文件权限：--------- (只有管理员才可以读写该文件，其他用户没有任何操作权限)

文件的格式：

用户名:密码:上次改动密码的日期 :密码不可被改动的天数 :密码需要重新变更的天数 :密码需要变更期限前的警告期限 :账号失效期限 :账号过期的期限 :保留

1. **用户组的概述**
2. 用户组概述
3. 用户组配置文件
4. 组的基本信息文件 /etc/group

文件拥有者：root

文件权限：rw-r--r-- (只有管理员才可以写文件)

文件格式：

组名称:群组密码 :群组 ID :组里面的用户成员

1. 组的密码信息文件 /etc/gshadow

文件拥有者：root

文件权限：--------- (只有管理员才可以读写该文件，其他用户没有任何操作权限)

文件格式：

用户组名:用户组密码:用户组管理员的名称:成员列表

1. **用户的管理**
2. useradd 添加用户

语法格式：useradd 选项 用户名

常用选项：

例如：

1. 添加一个名为user1的用户

useradd user1

1. 添加一个名为user2的用户,其用户ID为1010，主属组ID为1030，主目录为/home/user2\_test，登录时的shell为/bin/nologin，备注信息为“New user”

useradd -u 1010 -g 1030 -d /home/user2\_test -s /bin/nologin -c "New user" user2

1. 添加一个名为user3的用户，不创建主目录，账户过期时间为2020/04/14

useradd -M -e 2020/04/14 user3

（2）usermod 修改用户信息

语法格式：usermod 选项 用户名

常用选项：

例如：

1. 修改user2用户的信息，修改登录时所使用的shell为/bin/bash，修改其主目录为/home/user2（将以前主目录中的文件移动到新的主目录），并且将用户名修改为user\_2

usermod -s /bin/bash -d /home/user2 -m -l user\_2 user2

1. 锁定user\_2用户的密码

usermod -L user\_2

1. 解锁user\_2用户的密码

usermod -U user\_2

（3）passwd 修改用户密码信息

语法格式：passwd 选项 用户名

常用选项：

1. 修改user1用户的密码

passwd user1

2）修改user1用户的信息，修改密码最大有效天数为88888，修改密码不能被更改的天数为2天，修改提示天数为5天，账号禁用天数为3天

passwd -x 88888 -n 2 -w 5 -i 3 user1

3）删除user1用户的密码

passwd -d user1

（4）userdel 删除用户

语法格式：userdel 选项 用户名

常用选项：

-r

例如：

删除用户user2及主目录

userdel -r user2

1. **用户组的管理**
2. groupadd 添加用户组

语法：groupadd [选项] 组名

常用选项：

-g 组ID 设置用户组ID

-p 组的密码 设置用户组密码

例如：

1. 添加一个名为group1的用户组

groupadd group1

1. 添加一个名为group2的用户组，组ID为1010，组密码为“123456”

groupadd -g 1010 -p 123456 group2

1. groupdel 删除用户组

语法：groupdel [选项] 组名

常用选项：

例如：

1. 删除group2用户组

groupdel group2

如果某个用户组是其他用户的主属组，这个组不能直接删除

1. groupmod 修改用户组信息

语法：groupmod [选项] 组名

常用选项：

例如：

1. 修改group1组的信息，GID设置为1001（允许其重复），密码设置为“654321”，组名设置为group

groupmod -g 1001 -o -p 654321 -n group group1

1. gpasswd 设置群组密码

语法：gpasswd [选项] 组名

常用选项：

例如：

1. 将user1、user2、user3用户添加到group组中

第一种方法：

gpasswd -a user1 group (-a不覆盖之前的用户)

gpasswd -a user2 group

gpasswd -a user3 group

第二种方法：

gpasswd -M user1,user2,user3 group（-M覆盖之前的用户）

添加用户到组或设置组的成员，这个组指的是附属组

1. 将user1、user2、user3用户从group组中删除

gpasswd -d user1 group

gpasswd -d user2 group

gpasswd -d user3 group

1. 删除group组的密码

gpasswd -r group

1. 设置group组的管理员为user1

gpasswd -A user1 group

1. groups 查看用户属组

groups Admin 列出Admin用户的所有属组

groups 只列出当前用户的所有属组

1. newgrp 切换用户组

语法：newgrp 组名 （把当前用户切换到指定的用户组）

例如：

1. /home/user2/file1文件的拥有者为root,属组group1,而Admin用户是group1组的成员，请问如何让Admin用户访问/home/user2/file1文件

第一步：Admin用户要能够访问/home/user2目录

1. 查看Admin对/home/user2目录的访问权限

ls -l /home

drwx------. 3 user2 user2 91 4月 20 08:40 user2

根据该目录的文件拥有者和属组可以看出Admin用户属于其他用户

其他用户的权限为：---（没有任何权限）

2）修改/home/user2目录的权限，让Admin用户可以访问

chmod o+rwx /home/user2（管理员来修改）

修改后查看Admin是否可以访问该目录：ls -l /home

drwx---rwx. 3 user2 user2 91 4月 20 08:52 user2

第二步：Admin用户对该目录下的file1文件要有读的权限才可以

1. 查看file1文件的权限

ls -l /home/user2/file1

1. 如果Admin用户对file1文件没有读的权限，则为其添加读的权限

chmod g+r /home/user1/file1（管理员来修改）

1. 把Admin用户切换到group1组

newgrp group1 （Admin用户来执行）

1. 查看Admin用户的当前工作组

id （Admin用户来执行）

1. Admin用户访问file1文件

cat /home/user2/file1

注意事项：

1. 默认情况，当前用户是在主属组工作
2. 如果当前用户要使用附属组的资源，必须要切换到附属组
3. 切换到附属组是临时有效，一旦退出就是失效
4. id 查看用户ID以及组ID

语法：id [选项] 用户名

选项：

例如：

1. 查看Admin用户的用户和组信息

id Admin