# 用户/组基本概念

用户和组

- 系统上的每个进程(运行的程序)都是作为特定用户运行
- 每个文件是由一个特定的用户拥有
- 访问文件和目录受到用户的限制
- 与正在运行的进程相关联的用户确定该进程可访问的文件和目录

查看当前登录的用户信息

```
[root@xwz ~]# id
uid=0(root) gid=0(root) 组=0(root) 环境
=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[root@xwz ~]# id centos
uid=1000(centos) gid=1000(centos) 组=1000(centos),10(wheel)
```

查看文件owner

```
[root@xwz ~]# ll /home
总用量 4
drwx------. 15 centos centos 4096 8月  25 11:05 centos
```

查看运行进程的username

```
[root@xwz ~]# ps aux |less
USER        PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root          2  0.0  0.0      0     0 ?        S    15:01   0:00 [kthreadd]
root          3  0.0  0.0      0     0 ?        S    15:01   0:00
[ksoftirqd/0]
root          5  0.0  0.0      0     0 ?        S<   15:01   0:00
[kworker/0:0H]
root          7  0.0  0.0      0     0 ?        S    15:01   0:00
[migration/0]
root          8  0.0  0.0      0     0 ?        S    15:01   0:00 [rcu_bh]
```

```
[root@xwz ~]# yum -y install httpd
[root@xwz ~]# systemctl start httpd
[root@xwz ~]# ps aux |grep httpd
root      13655  0.1  0.2 230408  5196 ?        Ss   16:17   0:00
/usr/sbin/httpd -DFOREGROUND
apache    13678  0.0  0.1 232492  3164 ?        S    16:17   0:00
/usr/sbin/httpd -DFOREGROUND
apache    13679  0.0  0.1 232492  3164 ?        S    16:17   0:00
/usr/sbin/httpd -DFOREGROUND
apache    13680  0.0  0.1 232492  3164 ?        S    16:17   0:00
/usr/sbin/httpd -DFOREGROUND
apache    13681  0.0  0.1 232492  3164 ?        S    16:17   0:00
/usr/sbin/httpd -DFOREGROUND
apache    13682  0.0  0.1 232492  3164 ?        S    16:17   0:00
/usr/sbin/httpd -DFOREGROUND
root      13714  0.0  0.0 112724   988 pts/1    S+   16:18   0:00 grep --
color=auto httpd
```

和用户组相关的一些文件

```
/etc/passwd     root:x:0:0:root:/root:/bin/bash
# 用户名:x:uid:gid:描述:HOME:shell   x密码占位符
/etc/shadow
root:$6$j3YZCHCXpIiDho7x$v4/j6bOzGgyTcfP6jOa1ZY.q.sHvqQp/nsmEowjrtmo/iFKdo4X
piWZm5OpDKqhZEw8OSXTpdAM2JyIgBI.MzO::0:99999:7:::
                    $id$salt$encrypted
# 密码信息
/etc/group      root:x:0:               # 组的信息

[root@xwz ~]# man 5 passwd
[root@xwz ~]# man 5 shadow
[root@xwz ~]# man 5 group
[root@xwz ~]# man 3 crypt
```

加密算法$id

```
$1      MD5
$5      SHA-256
$6      SHA-512
```

系统约定

```
uid:0       特权用户
uid:1~999   系统用户
uid:1000+   普通用户
```

root用户

- uid是0
- 所有权力
- 该用户有权力覆盖文件系统上的普通权限
- 安装或删除软件并管理系统文件和目录
- 大多数设备只能由root控制

# 用户管理

groupadd,groupdel

useradd,usermod,userdel

passwd,chage

## 用户组

```
[root@xwz ~]# groupadd hr
[root@xwz ~]# groupadd sale
[root@xwz ~]# groupadd it
[root@xwz ~]# groupadd fd
[root@xwz ~]# groupadd market
[root@xwz ~]# groupadd net01 -g 2000
[root@xwz ~]# grep 'net01' /etc/group
net01:x:2000:
[root@xwz ~]# groupdel net01
```

## 用户

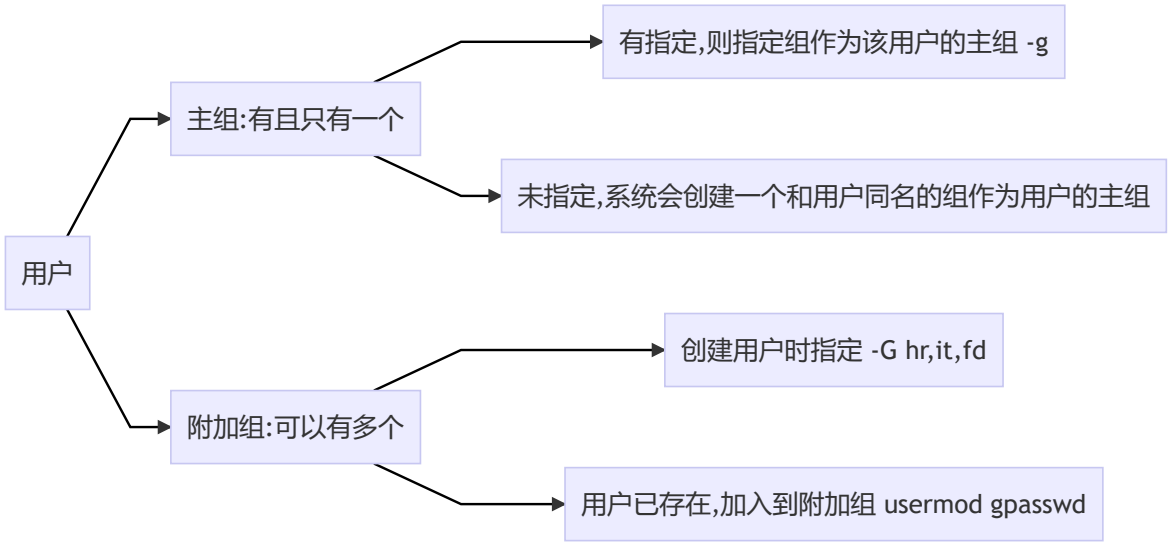
- 添加用户
- useradd常用参数

```
常用选项：
-u：指定uid
-g：指定gid
-c：用户注释信息
-d：家目录
-s：指定shell（/etc/shells）
-G：附加组
-r：创建系统用户
```

```
[root@xwz ~]# useradd user01
# 未指定该用户的主组
# 未指定该用户的附加组
# 未指定用户的HOME
# 未指定用户的SHELL
# 未指定用户的UID...
[root@xwz ~]# grep 'user01' /etc/passwd /etc/shadow /etc/group
/etc/passwd:user01:x:1001:1006::/home/user01:/bin/bash
/etc/shadow:user01:!!:18140:0:99999:7:::
/etc/group:user01:x:1006:
[root@xwz ~]# id user01
uid=1001(user01) gid=1006(user01) 组=1006(user01)
[root@xwz ~]# ls /var/spool/mail/user01
/var/spool/mail/user01
[root@xwz ~]# ls /home
```

如果创建一个用户时，未指定任何选项，系统会创建一个和用户名相同的组作为用户的`Primary Group`

```
[root@xwz ~]# useradd user02 -u 503                    # 创建用户user02,指定uid
[root@xwz ~]# useradd user03 -d /user033               # 创建用户user03,指定家目录
[root@xwz ~]# useradd user04 -s /sbin/nologin          # 创建用户并指定shell
[root@xwz ~]# useradd user05 -G hr,it,fd               # 创建用户，指定附加组
[root@xwz ~]# useradd user06 -u 4000 -s /sbin/nologin
```




注意:

- -g -G 仅适用useradd创建用户时使用
- -g -G 指定的组必须事先存在

```
[root@xwz ~]# userdel user06    # 删除用户user06，但是不删除用户的home和mail
[root@xwz ~]# ll -d /home/user06
drwx------. 3 4000 4000 78 9月   1 10:34 /home/user06
[root@xwz ~]# ll /var/spool/mail/user06
-rw-rw----. 1 4000 mail 0 9月   1 10:34 /var/spool/mail/user06
[root@xwz ~]# userdel -r user02 # 删除用户user02,并且同时删除用户的home和mail
```

- 给用户修改密码

```
[root@xwz ~]# passwd user05
# root用户可以直接设置普通用户密码
# 普通用户必须要提供原密码，才可以修改自己密码
常用选项：
-n mindays：指定最短使用期限
-x maxdays：最大使用期限
-w warndays：提前多少天开始警告
-i inactivedays：非活动期限
--stdin：从标准输入接收用户密码
echo "PASSWD" | passwd --stdin username
```

- 修改用户组

```
[root@xwz ~]# usermod -G hr user05      # 覆盖原有的附加组
[root@xwz ~]# usermod -G fd,it user05
[root@xwz ~]# usermod -aG sale user05   # 增加新的附加组
```

```
[root@xwz ~]# grep 'user03' /etc/group
user03:x:1008:
[root@xwz ~]# gpasswd -a user03 hr
正在将用户“user03”加入到“hr”组中
[root@xwz ~]# grep 'user03' /etc/group
hr:x:1001:user03
user03:x:1008:
```

```
[root@xwz ~]# gpasswd -M user03,user04 fd
[root@xwz ~]# id user03
uid=1002(user03) gid=1008(user03) 组=1008(user03),1001(hr),1004(fd)
[root@xwz ~]# id user04
uid=1003(user04) gid=1009(user04) 组=1009(user04),1004(fd)
```

```
[root@xwz ~]# gpasswd -d user03 hr
正在将用户“user03”从“hr”组中删除
[root@xwz ~]# id user03
uid=1002(user03) gid=1008(user03) 组=1008(user03),1004(fd)
```

```
[root@xwz ~]# usermod -s /sbin/nologin user03
# 修改用户的shell
```

- 用户删除

```
userdel
-r：连同家目录一起删除
```

# no shell

shell 是用户登录后运行的第一个程序

/sbin/nologin　用户无法登录系统，实现管理。仅作为运行进程的用户，访问FTP的用户。安全的用户

/bin/bash　　登录系统，实现管理

图形化登录

命令行登录

切换用户

如果设置为/usr/sbin/poweroff，那么一登录就会关机(setenforce 0)

`grep 'bash$' /etc/passwd` 查看允许登录的所有用户

# login.defs

useradd参照文件

创建用户时对用户的一些限制，对root用户无效

```
[root@xwz ~]# vim /etc/login.defs
MAIL_DIR        /var/spool/mail
PASS_MAX_DAYS   99999
PASS_MIN_DAYS   0
PASS_MIN_LEN    5
PASS_WARN_AGE   7
CREATE_HOME     yes
ENCRYPT_METHOD SHA512
[root@xwz ~]# vim /etc/default/useradd
SHELL=/bin/bash
```

```
[root@xwz ~]# chage -m 0 -M 90 -W 7 -I 14 user01
[root@xwz ~]# chage -h
用法：chage [选项] 登录

选项：
  -d, --lastday 最近日期          将最近一次密码设置时间设为“最近日期”
  -E, --expiredate 过期日期       将帐户过期时间设为“过期日期”
  -h, --help                      显示此帮助信息并推出
  -I, --inactive INACITVE         过期 INACTIVE 天数后，设定密码为失效状态
  -l, --list                      显示帐户年龄信息
  -m, --mindays 最小天数          将两次改变密码之间相距的最小天数设为“最小天数”
  -M, --maxdays 最大天数          将两次改变密码之间相距的最大天数设为“最大天数”
  -R, --root CHROOT_DIR           chroot 到的目录
  -W, --warndays 警告天数         将过期警告天数设为“警告天数”
```

```
[root@xwz ~]# useradd user01
[root@xwz ~]# echo 123456 |passwd --stdin user01
更改用户 user01 的密码 。
passwd：所有的身份验证令牌已经成功更新。
[root@xwz ~]# chage -d 0 user01      # 强制用户在下次登录的时候换密码
```

新建用户`home`目录下的`bash`开头的文件是从`/etc/skel/`中复制过去的

# sudo提权

切换到root用户

```
[centos@xwz ~]$ useradd u1
-bash: /usr/sbin/useradd: 权限不够
[centos@xwz ~]$ su - root
密码：
[root@xwz ~]# useradd u1
```

以root身份授权普通用户

```
[root@xwz ~]# vim /etc/sudoers
%wheel        ALL=(ALL)       NOPASSWD: ALL
[root@xwz ~]# gpasswd -a centos wheel
[root@xwz ~]# su - centos
[centos@xwz ~]$ useradd u2
-bash: /usr/sbin/useradd: 权限不够
[centos@xwz ~]$ sudo useradd u2
[sudo] centos 的密码：
[centos@xwz ~]$ id u2
uid=1006(u2) gid=1012(u2) 组=1012(u2)
```