一、Linux下用户管理

㈠ 用户概念及作用(了解)

用户：指的是==Linux操作系统中==用于管理系统或者服务的==人==

一问：管理系统到底在**管理什么**?

答：Linux下一切皆**文件**，所以用户管理的是相应的==文件==

二问：**如何管理**文件呢?

答：

1. 文件==基本管理==，比如文件的创建、删除、复制、查找、打包压缩等；文件的权限增加、减少等；
2. 文件==高级管理==，比如**程序文件**的安装、卸载、配置等。终极目的是对外提供稳定的服务。

㈡ ==用户的分类==

1、超级用户

- 超级用户，也叫管理员，**==root==**。该用户(root)具有==所有权限==，==UID=0==并且绝对只能是0。

2、系统用户

- 系统用户，也叫程序用户。一般都是由程序创建，用于程序或者服务运行时候的身份。
- 默认==不允许登录系统==。==1<=UID<=499==
- 比如后面要学的web服务的管理用户apache，文件共享ftp服务的管理用户ftp等

  注意：Centos7/RHEL7中，系统用户UID范围：==1<=UID<=999==

3、普通用户

- 普通用户，一般都是由==管理员创建==，用于==对系统进行有限的管理维护操作==。
- 默认==可以登录系统==。==500<=UID<=60000==

  注意：Centos7/RHEL7中，普通用户UID范围：==1000<=UID<=60000==

==特别说明==：

1. 用户指的是操作系统上==管理系统或服务==的==人==，是人，就有相关的==属性信息==
2. 用户的属性信息包括但不限于，如：==家目录、唯一身份标识(UID)、所属组(GID)==等
3. 今天我们讨论的用户指的是==普通用户==，即由管理员创建的用户

㈢ ==用户的基本管理(掌握)==

1、创建用户(useradd)

(1) 基本语法和选项

```
useradd [选项] 用户名
常用选项：
-u  指定用户uid，唯一标识，必须唯一
-g  指定用户的默认组(主组)
-G  指定用户附加组(一个用户可以加入多个组，但是默认组只有一个)
-d  指定用户家目录(每个用户都有一个自己的家，并且默认在/home/xxx)
-s  指定用户默认shell

查看系统支持的shell(命令解释器)
[root@localhost Desktop]# cat /etc/shells
/bin/sh              系统默认解释器bash的软链接
/bin/bash            系统默认的解释器
/sbin/nologin        不能登录操作系统，也叫非交互式shell
/bin/dash            兼容shell脚本不好，Ubuntu 6.10默认是Dash Shell
/bin/tcsh            其他shell
/bin/csh                 其他shell
```

(2) 举例说明

① 创建默认用户

```
创建一个用户stu1
[root@localhost Desktop]# useradd stu1
查看用户信息
[root@localhost Desktop]# id stu1
uid=501(stu1) gid=501(stu1) groups=501(stu1)

注意：当创建一个默认用户时，系统会给该用户以下东西，以stu1为例说明

1）用户的UID(唯一标识)       501（系统自动分配）
2）用户的默认组(主组)       stu1组，默认跟该用户的用户名一致；组ID(501),默认和用户UID一致
3）用户的家目录                 /home/stu1
4）拷贝相应的文件到用户的家里
[root@localhost Desktop]# su - stu1
[stu1@localhost ~]$ ls -a
.  ..  .bash_logout  .bash_profile  .bashrc  .gnome2  .mozilla
```

② 根据需求创建用户

```
1. 创建用户stu2，但是不能登录操作系统
注意：-s   指定用户的默认shell，/sbin/nologin表示不能登录系统，也叫非交互
[root@localhost Desktop]# useradd -s /sbin/nologin stu2
验证：
[root@localhost Desktop]# id stu2
uid=502(stu2) gid=502(stu2) groups=502(stu2)
切换用户失败，说明该用户不能登录系统
[root@localhost Desktop]# su - stu2
This account is currently not available.

2. 创建用户stu2，同时指定该用户的家目录为/rhome/stu2
注意：-d   指定用户的家目录，前提该用户家目录的上一级目录/rhome必须存在

[root@localhost Desktop]# mkdir /rhome
```

```
[root@localhost Desktop]# useradd -d /rhome/stu2 stu2
[root@localhost Desktop]# id stu2
uid=502(stu2) gid=502(stu2) groups=502(stu2)
说明：指定stu2家目录/rhome/stu2时，只需要/rhome存在即可，系统会默认在/rhome下创建stu2目录
```

③ 保存用户信息的文件

```
1. 用户信息保存文件/etc/passwd
了解相关配置文件内容，可以通过求man文档解决，即 man 5 passwd

以冒号:分割为7列，如下：
account  -->  stu1  用户名称
password -->  x     密码,将密码单独存放在另外一个文件中
UID      --> 501    用户ID
GID      --> 501    组ID
GECOS    -->            用户自定义,描述说明
directory -->           /home/stu1  用户的家目录
shell    -->        /bin/bash用户的默认shell,其中/sbin/nologin表示非交互，不能登录系统

2. 用户密码信息保存文件/etc/shadow
了解相关配置文件内容，可以通过求man文档解决，即 man 5 shadow

以冒号:分隔为9列，如下：
login name
登录的用户名
encrypted password
加密后的密码;!!表示空密码，没有设置密码
date of last password change
最后一次更改密码的天数（距离1970年的1月1日到现在的天数）
minimum password age
密码的最小生存周期;0表示可以立刻修改密码；如果是3，则表示3天后才能更改密码
maximum password age
密码的最大生存周期;如果30表示每隔30天需要更新一次密码
password warning period      密码过期前几天发出警告；7表示过期前7天开始警告
password inactivity period
密码的宽限期；如果3表示允许密码过期3天,3天内还能登录系统，但是要求修改密码。3天后（密码过期3天后账户被封锁，需要联系管理员）
account expiration date
账户过期的时间，账户过期的用户不能登录；密码过期用户不能用原来的密码登录。以1970年1月1日算起。
reserved field
保留
```

④ 更改用户的账号信息(chage)[==扩展==]

```
chage  --help
-l：列出用户的详细密码状态;
-d 日期：修改 /etc/shadow 文件中指定用户密码信息的第3个字段，也就是最后一次修改密码的日期，格式为 YYYY-MM-DD;
-m 天数：修改密码最短保留的天数，也就是 /etc/shadow 文件中的第4个字段;
注：几天后才能修改一次密码
-M 天数：修改密码的有效期，也就是 /etc/shadow 文件中的第5个字段;
注：每隔多少天更新一次密码
-W 天数：修改密码到期前的警告天数，也就是 /etc/shadow 文件中的第6个字段;
-i 天数：修改密码过期后的宽限天数，也就是 /etc/shadow 文件中的第7个字段;
注：过期后还可以使用的天数，达到这个天数后，账号失效

-E 日期：修改账号失效日期，格式为 YYYY-MM-DD，也就是 /etc/shadow 文件中的第8个字段;
```

```
举例说明：
查看用户账号的相关信息命令：chage -l stu1
[root@localhost Desktop]# chage -l stu1
Last password change                    : Mar 04, 2019
Password expires                        : never
Password inactive                       : never
Account expires                         : never
Minimum number of days between password change      : 0
Maximum number of days between password change      : 99999
Number of days of warning before password expires   : 7

修改用户账号的过期时间：2019-03-10过期
[root@localhost Desktop]# chage -E '2019-03-10' stu1
[root@localhost Desktop]# chage -l stu1
Last password change                    : Mar 04, 2019
Password expires                        : never
Password inactive                       : never
Account expires                      : Mar 10, 2019
Minimum number of days between password change      : 0
Maximum number of days between password change      : 99999
Number of days of warning before password expires   : 7
修改用户账号的过期时间为10天以后：
[root@localhost Desktop]# chage -E $(date +%F -d '+10days') stu1
```

案例：设置mysql用户60天后密码过期，至少7天后才能修改密码，密码过期前7天开始收到告警信息

```
# chage -M 60 -m 7 -w 7 mysql
```

案例：强制新建用户test第一次登陆时修改密码

```
# chage -d 0 test
```

案例：设置mysql用户60天后密码过期，至少7天后才能修改密码，密码过期前7天开始收到告警信息

```
# chage
```

2、用户密码设置(passwd)

```
passwd 用户名        表示给指定用户修改密码
passwd 直接回车       表示给当前用户修改密码

[root@localhost Desktop]# passwd stu1
Changing password for user stu1.
New password: 密码不显示
BAD PASSWORD: it is WAY too short
BAD PASSWORD: is too simple
Retype new password: 密码不显示
passwd: all authentication tokens updated successfully.
说明：
1.管理员root可以给任何用户修改密码
2.普通用户可以自己给自己修改密码，但是密码复杂度要符合规范
```

3、修改用户信息(usermod)

① 基本语法选项

```
usermod [选项] 用户名
常用选项：
-u  指定用户uid，唯一标识，必须唯一
-g  指定用户的默认组(主组)
-G  指定用户附加组(一个用户可以加入多个组，但是默认组只有一个)
-d  指定用户家目录(每个用户都有一个自己的家，并且默认在/home/xxx)
-s  指定用户默认shell
```

② 举例说明

```
1. 修改用户stu1的uid为505
[root@localhost tmp]# id stu1
uid=501(stu1) gid=501(stu1) groups=501(stu1)
[root@localhost tmp]# usermod -u 505 stu1
[root@localhost tmp]# id stu1
uid=505(stu1) gid=501(stu1) groups=501(stu1)

2. 修改stu1用户的家目录为/rhome/redhat/stu1,默认为/home/stu1
[root@localhost tmp]# su - stu1
[stu1@localhost ~]$ pwd
/home/stu1
1) 创建新的家目录/rhome/redhat/stu1
[root@localhost tmp]# mkdir /rhome/redhat/stu1 -p
注意：新的家目录必须全部存在！！！
2) 修改stu1的家为新家/rhome/redhat/stu1
[root@localhost tmp]# usermod -d /rhome/redhat/stu1 stu1
[root@localhost tmp]# su - stu1
-bash-4.1$ pwd
/rhome/redhat/stu1
3) 拷贝家具(相关的配置文件)到新家里
[root@localhost tmp]# cp -a /etc/skel/. /rhome/redhat/stu1/
4) 再次查看
[root@localhost tmp]# su - stu1
[stu1@localhost ~]$

思考：是否可以直接在修改家目录时将原来家目录里的文件一起拷贝过去呢？
```

4、删除用户(userdel)

① 基本语法选项

```
userdel [选项] 用户名
常用选项:
-r  删除用户并且移除其家目录和邮箱
-f  强制删除正在登录的用户
```

② 举例说明

```
说明:
创建完用户后，家目录默认在/home/用户名下；用户的邮箱在/var/spool/mail/用户名
1. 删除user01用户以及家目录
[root@localhost tmp]# userdel -r user01
[root@localhost tmp]# id user01
id: user01: No such user

2.强制删除一个正在登录的用户
[root@localhost tmp]# userdel stu1
userdel: user stu1 is currently used by process 6052     说明该用户正在登录
[root@localhost tmp]# userdel -f stu1    强制删除

3. 只删除用户user02，不删除其家目录
[root@localhost tmp]# userdel user02
```

㈣ 课堂练习

- 创建3个普通用户stu1~stu3,要求如下:
    1. stu1默认创建，密码为123
    2. stu2的家目录为/rhome/redhat/stu2,密码为123
    3. stu3用户不能登录操作系统，密码为123

```
useradd stu1
echo 123|passwd --stdin stu1

mkdir /rhome/redhat -p
useradd -d /rhome/redhat/stu2 stu2
echo 123|passwd --stdin stu2

useradd -s /sbin/nologin stu3
echo 123|passwd --stdin stu3
```

- 修改stu2用户的家目录为/home/stu2

```
usermod -md /home/stu2 stu2
```

- 修改stu3用户信息，让其可以登录操作系统

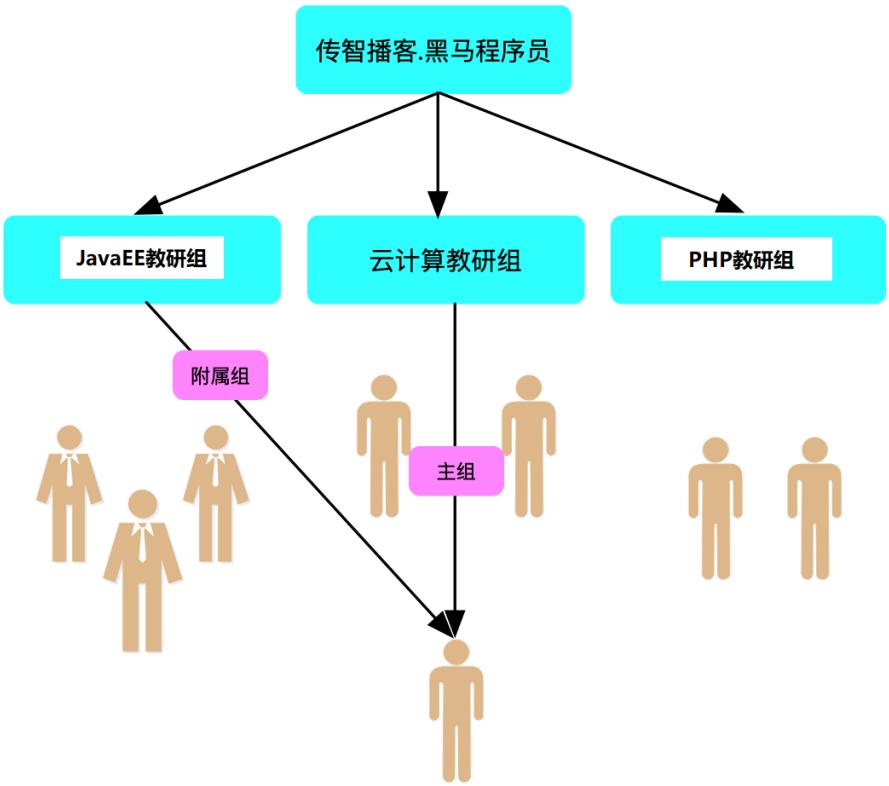
```
usermod -s /bin/bash stu3
```

- 删除stu1~stu3三个用户以及其家目录

```
userdel -r stu1
...
```

二、Linux下组管理

(一) 组和用户的关系(理解)



核心：==组的目的是为了方便管理用户==

- 用户是操作系统上管理维护系统或服务的人
- 组是用户的一个==属性信息==
- 任何一个用户==默认都会有==一个==主组==(默认组)
- 一个用户除了主组也==可以有多个其他组==(**附加组**)

一问：用户的主组和附加组到底有啥关系呢?

答：用户的主组和附加组==半毛钱关系都木有==

二问：那要这个主组或者附加组有啥用呢?

答：肯定是**有用**的，组的目的是方便管理用户，用户的目的是管理==操作文件==，文件就有==权限==这个属性。

1. 用户要操作一些文件，文件是由用户创建，不同用户创建的文件的==属性信息==也就不一样
2. 文件的属性都有啥呢？比如，文件的==创建者==，文件==属于哪个组==，文件大小，文件时间等
3. 其中，不同用户所创建的==文件的属组==就是==该用户的主组==(默认组)
4. A用户附加组也有可能是其他用户的主组，道理同上（权限章节再细细体会组的作用）

(二) ==组的管理(掌握)==

1、创建组(groupadd)

① 基本语法

```
groupadd [选项] 组名
常用选项：
-g  指定组的GID(编号)，默认唯一
```

② 举例说明

```
1.创建一个组admin
[root@localhost Desktop]# groupadd admin
2.查看组信息
[root@localhost Desktop]# tail -1 /etc/group
admin:x:506:
说明：关于/etc/group配置文件说明，可以man 5 group找帮助

3.创建一个组sysadmin，指定组的GID为1001
[root@localhost Desktop]# groupadd -g 1001 sysadmin
[root@localhost Desktop]# tail -1 /etc/group
admin:x:506:
sysadmin:x:1001
```

2、删除组(groupdel)

① 基本语法

```
groupdel 组名
```

② 举例说明

```
[root@localhost Desktop]# groupdel admin
[root@localhost Desktop]# groupdel stu2
groupdel: cannot remove the primary group of user 'stu2'
注意：以上信息说明不能删除属于其他用户的主组
```

3、组成员管理(gpasswd)

① 基本语法

```
gpasswd [选项] 组名
常见选项：
-a      添加用户到组
-d      从组中删除成员
-A      指定管理员
-M      指定组成员，可以批量添加用户到组中
-r      删除密码

gpasswd 组名       给组设置密码
```

② 举例说明

- 添加用户到组里

```
1. 创建3个用户user01~user03
2. 将user01添加到sysadmin组里
方法:1：指定user01用户的附加组为sysadmin（站在用户角度）
# usermod -G sysadmin user01
方法2：使用gpasswd命令添加用户到组里
# gpasswd -a user01 sysadmin
-a选项：表示往组里追加用户
# gpasswd -M user02,user03 sysadmin      设置sysadmin组成员为user02,user03
-M选项：表示覆盖设置组成员（会覆盖原来的成员列表）
```

- 删除组成员

```
将user03用户从组sysadmin里移除
# gpasswd -d user03 sysadmin
```

##㈢ 课堂练习

1. 创建一个admin组，组id为900

```
groupadd -g 900 admin
```

2. 创建一个用户tom,并且admin组作为tom用户的附加组（要求在建立用户的时候就完成）,密码为123

```
useradd tom -G admin
echo 123|passwd --stdin tom
```

3. 创建一个用户jack,要求在建立用户之后使用gpasswd把jack加入到admin组，密码为123

```
useradd jack
gpasswd -a jack admin
```

4. 给admin组设定一个默认密码为123 （gpasswd命令）

```
gpasswd admin
```

5. 把tom用户设定为admin组的组管理员（gpasswd命令）

```
gpasswd -A tom admin
验证：
su - tom
gpasswd -a xxx admin

tail -5 /etc/gshadow
```

三、综合实战

作业1

1. 创建一个公司itcast，3个部门财务(cw)，人事(rs)，市场(sc)

   说明：==实际是创建4个组==，分别为itcast、cw、rs、sc，没有包含的关系

2. 每个部门创建2个用户，如 cw01 cw02，rs01，rs02，sc01，sc02；boss01管理公司所有部门；

   说明：boss01管理所有部门说明，boss01的附加组为财务、人事和市场部门

3. 所有用户账号有效期3个月<90天>，第一次登录强制修改密码，每隔15天更新一次密码；默认密码为123456

```
groupadd itcast
groupadd cw
groupadd rs
groupadd sc

useradd cw01 -g cw -G itcast
useradd sc01 -g sc -G itcast
useradd rs01 -g rs -G itcast
useradd boss01 -g itcast -G cw,sc,rs

[root@node1 ~]# chage --help
Usage: chage [options] LOGIN

Options:
  -d, 设置最后一次更改密码的日期，0表示下次登录强制更改密码
  -E, 设置账号的过期日期
  -h, --help                    display this help message and exit
  -I, 设置的密码的宽限期
  -l, 查看列出账号的信息

chage -d 0 -E '+90days' -M 15 cw01
```

作业2

1. 添加3个用户，用户harry，natasha，sarsh，要求harry，natasha用户的附加组为admin组，sarsh用户的登录shell为非交互式shell。密码均为redhat
2. 修改harry用户的家目录为/home/heima/redhat/harry
3. 修改natasha，sarsh用户的主组为heima，并且可以登录系统

```
groupadd admin
useradd harry -G admin
useradd natasha -G admin
useradd sarsh -s /sbin/nologin
echo redhat|passwd --stdin harry

mkdir -p /home/heima/redhat
usermod -md /home/heima/redhat/harry harry

groupadd heima
usermod -g heima natasha
usermod -g heima -s /bin/bash sarsh
```

w