用户和组管理

# 基本概念

## 用户类型

### 超级用户

超级用户：root，UID（唯一标识用户）为0。拥有最高的权限，用户的主目录是/root。把普通用户改成超级用户：只需要把/etc/passwd把用户的uid改成0。

### 普通用户

普通用户：UID为500-60000。通常只能在自己的目录进行写操作；主目录通常在/home下，其中包含用户的配置信息。每个linux服务器有个mail客户端可以收发邮件，/var/spool/mail/用户名/。

### 伪用户

* 伪用户：UID为1-499
* 伪用户与系统和程序服务相关
* bin、daemon、shutdown、halt等，任何Linux系统默认都有这些伪用户
* mail、news、games、apache、ftp、mysql及sshd 等，与Linux 系统的进程相关
* 伪用户通常不需要或无法登录系统
* 可以没有宿主目录

## 用户组

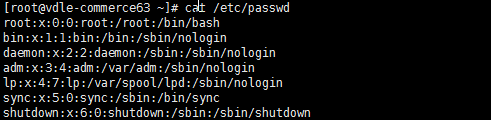
每个用户都至少属于一个用户组，只有一个初始组初始组一般和用户名一样 。每个用户组可以包括多个用户，只要在用户组文件/etc/group/后添加用户。同一用户组的用户享有该组共有的权限。

# 用户和组管理配置文件

## 用户信息文件：/etc/passwd

文件格式：用户名：密码：UID：GID：注释描述：宿主目录：用户shell

例如：root:x:0:0:root:/root:/bin/bash



## 密码文件：/etc/shadow

文件格式：

用户名：密码（MD5加密过）：最后一次修改时间（天数）：密码修改最小间隔时间：密码最大有效时间：警告时间：账号闲置时间：失效时间（天）：标志（一般不使用）。例如：root:$1$NV0hQ/3m$nKludCy6gZOJ8WX/zADeU1:15321:0:99999:7:::

注意：/etc/shadow权限000，加密字段"!!","\*"表示没有密码，所以不能登陆。可以在密码前面加上!!让密码失效(锁定用户)

## 用户组文件：/etc/group

文件格式：组名：组密码（一般不使用）：GID：组内用户列表

例子：user：x：1005：user

## 其它配置文件

### 用户组密码文件

/etc/gshadow

### 用户配置文件

/etc/login.defs ,/etc/default/useradd

|  |
| --- |
| # useradd defaults file  GROUP=100 #用户默认组  HOME=/home #用户家目录  INACTIVE=-1 #密码过期宽限天数（shadow文件的第七个字段）  EXPIRE= #密码失效天数（shadow文件的第八个字段）  SHELL=/bin/bash #默认shell  SKEL=/etc/skel #模板目录  CREATE\_MAIL\_SPOOL=yes #是否建立邮箱 |

/etc/login.defs定义密码规则

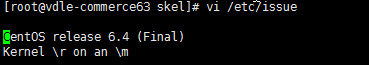
### 用户模板信息：/etc/ske1/\*

用户创建的同时会把，/etc/skel/\*拷贝到/home/用户名/下）,里面包含文件有：

.bash\_logout，.bash\_profile，.bashrc

### 登录信息

/etc/motd ，/etc/issue



# 用户管理命令

## useradd命令

useradd 设置选项 用户名

* -D 查看缺省参数
* u：UID
* g：缺省所属用户组GID（初始组）
* G：指定用户所属多个组（附加组）
* d：宿主目录（默认/home/用户名（700） /root（550））
* s：命令解释器Shell
* c：描述信息
* e：指定用户失效时间

例如：useradd –d /home/student student

操作实质，分别修改一下文件：

* /etc/passwd
* /etc/shadow
* /etc/group
* /etc/gshadow
* /var/spool/mail/用户/
* /home/用户/

## passwd命令

命令格式：passwd 选项 用户名

|  |
| --- |
| #锁定指定用户账号  passwd -l username  #解除指定用户账号的锁定  passwd -u username  删除用户密码，登录无需口令  passwd -d username  #查看用户密码状态  passwd -S  #修改用户的密码  passwd username |

## chage命令设定密码

-l 查看用户密码设置

-m 密码修改最小天数

-M 密码修改最大天数

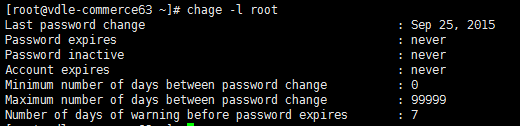
-d 密码最后修改的日期

-I 密码过期后，锁定账户的天数

-E 设置密码的过期日期，如果为0，代表密码立即过期；如果为-1，代表密码永不过期

-W 设置密码过期前，开始警告的天数

例如：chage -d 7/6/15 kobe



## usermod命令

命令格式：usermod 选项 用户名

选项：

* 选项和useradd一样的，
* -l：改变用户的登录名称
* -g：用户加入的组

|  |
| --- |
| #将用户samlee添加到softgroup用户组中  usermod -G softgroup samlee  #将用户liming的登录名改为samlee，加入到lampbrother组中，用户目录改为#/home/samlee  usermod -l samlee -d /home/samlee -g lampbrother liming |

## userdel命令

命令格式：userdel -r 用户名

-r：删除用户目录

## su命令

su – 用户名 #切换到其他用户（当前目录为用户名主目录）

su - root -c "ls -lih /root" #切换用户root执行一次命令

## pwck命令

此命令检查 /etc/passwd 这个账号配置文件内的信息，与实际的主文件夹是否存在等信息，还可以比较 /etc/passwd /etc/shadow的信息是否一致等。一般来说，我们利用这个工具检查我们的输入是否正确。

## vipw 命令

编辑/etc/passwd文件

## pwconv命令

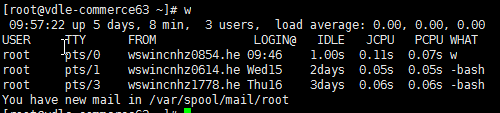
这个命令主要目的是将 /etc/passwd 内的账号与密码移动到 /etc/shadow 当中。使用这个命令以后：

1. 比较/etc/passwd 及 /etc/shadow,若/etc/passwd内的账号并没有对应的 /etc/shadow 密码，则pwconv会去/etc/login.defs取用相关的密码数据，并新建该账号的/etc/shadow数据。
2. 若/etc/passwd内存在加密数据时，则会将密码转移到/etc/shadow内，并将/etc/passwd内的密码位置设为 x 。
3. 新建账号时一般不会有问题，但是手动新建账号时可能就会有问题，此时再用这个命令。

## pwunconv命令

相对于pwconv,pwunconv则是将/etc/shadow内的密码列数据写回 /etc/passwd，并删除/etc/shadow.最好不要用这个命令，因为他会将/etc/shadow 文件删除，如果你不备份，后果很严重。

## who、w查看当前登录用户信息



# 组管理命令

## 添加用户组groupadd

groupadd -g 888 webadmin

创建用户组webadmin，其GID为888

## 删除用户组：groupdel 组名

注意：初始组对应有用户，不能直接groupdel（要先删除对应用户）

## 修改用户组信息groupmod

groupmod -n apache webadmin

修改webadmin组名为apache

## gpasswd 设置组密码及管理组内成员

-a 添加用户到用户组

-d 从用户组中删除用户

-A 设置用户组管理员

-r 删除用户组密码

-R 禁止用户切换为该组

例如：gpasswd -a mary softadm

gpasswd 组名 #设置组密码

## grpconv（作用同pwconv）

## newgrp命令

格式：newgrp 组名

一个用户同时隶属于两个或两个以上分组，需要切换到其它用户组来执行一些操作，就用到了newgrp命令切换当前登陆所在组。

## id命令

查看用户id和组信息

## groups命令

命令格式：groups 用户

作用：查看用户所属组

## grpck命令(检测用户组配置文件)

## vigr命令（编辑/etc/group）

# 用户授权

## 限制用户

|  |
| --- |
| #su(4755)为root  groupadd sugroup  chmod 4750 /bin/su  chgrp sugroup /bin/su  ls -l /bin/su  #-r-sr-x--- 1 root sugroup 18360 Jan 15 2010 /bin/su |

## 用sudo代替su

使用su – root需要使用者知道root的密码，这样很不安全。故使用sudo

### Sudo介绍

sudo是linux下常用的允许普通用户使用超级用户权限的工具，允许系统管理员让普通用户执行一些或者全部的root命令，如halt，reboot，su等等。这样不仅减少了root用户的登陆 和管理时间，同样也提高了安全性。Sudo不是对shell的一个代替，它是面向每个命令的。它的特性主要有这样几点：

* sudo能够限制用户只在某台主机上运行某些命令。
* sudo提供了丰富的日志，详细地记录了每个用户干了什么。它能够将日志传到中心主机或者日志服务器。
* sudo使用时间戳文件来执行类似的“检票”系统。当用户调用sudo并且输入它的密码时，用户获得了一张存活期为5分钟的票（这个值可以在编译的时候改变）。
* sudo的配置文件是sudoers文件，它允许系统管理员集中的管理用户的使用权限和使用的主机。它所存放的位置默认是在/etc/sudoers，属性必须为0411。

注意：root把本来只能超级用户执行的命令赋予给普通用户执行，sudo操作的对象是系统命令。

### 常用sudo命令的使用方法

|  |
| --- |
| sudo -V ：显示版本编号 sudo -h ：会显示版本编号及指令的使用方式说明 sudo -l ：显示出自己（执行 sudo 的使用者）的权限 sudo -v ：因为 sudo 在第一次执行时或是在 N 分钟内没有执行会问密码  sudo -k ：将会强迫使用者在下一次执行 sudo 时问密码 sudo -s ：执行环境变数中的 SHELL 所指定的 shell sudo -H ：将环境变数中的 HOME （家目录）指定为要变更身份的使用者家目录（如不加 -u 参数就是系统管理者 root ）  sudo command ：要以系统管理者身份（以-u 更改为其他人）执行的指令 |

### sudo配置文件的配置

配置文件：/etc/sudoers，编辑配置文件命令visudo，普通用户使用命令sudo。格式：用户名（组名） 主机地址=(指定用户) [NOPASSWD:]命令(ALL)

|  |
| --- |
| #允许john用户从任何地方登陆后执行任何人的任何命令  John ALL=(ALL) NOPASSWD:ALL  #允许用户组john  %john ALL=(ALL) NOPASSWD:/sbin/shutdown,/usr/bin/reboot |

注意：用户命令必须使用绝对路径。配置的含义指定主机的指定用户具有访问指定命令的权限。

# 常见应用

## 授权用户jack和mary对目录/software有写权限

|  |
| --- |
| groupadd softadm  usermod -G softadm jack  gpasswd -a mary softadm  chgrp softadm /software  chmod g+w /software |

## 手动添加一个用户

第一步：修改/etc/passwd，添加用户记录（不能有重复的UID）例如：user2:x:1004:1004::/home/user2:/bin/bash。然后执行pwconv,让/etc/passwd和/etc/shadow同步

第二步：修改/etc/group,添加记录user2:x:1004: ，然后执行grpconv来同步、etc/gshadow内容。

第三步：创建用户的主目录，把用户启动的文件也复制进，然后改变目录用户所属：

|  |
| --- |
| mkdir –p /home/user2  cp /etc/skel/.\* /home/hello  chown -R user2:user2 /home/user2 |

第四步：设置用户密码：passwd

第五步：使用su测试用户

## 批量添加用户

|  |
| --- |
| #手动添加密码  echo "123" | passwd --stdin user  #用户密码1970年1月1日创建，要求用户登录必须修改密码（其他选项可以通过#修改/etc/shadow来达到相同的效果）  chage -d 0 lamp |

批量添加用户脚本

|  |
| --- |
| #!/bin/bash  . /etc/profile  user\_info=/home/k12/adduser.txt  for userinfo in $(cat ${user\_info})  do  username=$(echo $userinfo | cut -f1 -d ":")  password=$(echo $userinfo | cut -f2 -d ":")  useradd $username  if [ $? -ne 0 ]; then  echo "$username exists,skip set password"  else  echo $password | passwd --stdin $username  chage -d 0 $username  fi  done |