1,用户和用户组文件

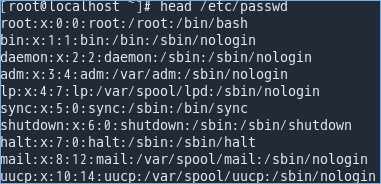
  在linux中，用户帐号，用户密码，用户组信息和用户组密码均是存放在不同的配置文件中的。

  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zhangjie的用户，并作为student用户组的成员，则操作命令为：

[root@localhost ～]# useradd -g student zhangjie

[root@localhost ～]# tail -1 /etc/passwd

zhangjie:x:501:501::/home/zhangjie:/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lijie的账户，但不指定用户组，其操作结果为：

[root@localhost ~]# useradd lijie

[root@localhost ~]# tail -1 /etc/passwd

lijie:x:502:502::/home/lijie:/bin/bash

[root@localhost ~]# tail -2 /etc/group

student:x:501:

lijie:x:502:          #系统自动创建了名为lijie的用户组，ID号为502

  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 ~]# tail -1 /etc/passwd

vodup:x:503:503::/var/vodup:/sbin/nologin

[root@localhost ~]# tail -1 /etc/group

vodup:x:503:

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lijie更名为lijunjie，则操作命令为：

[root@localhost ~]# usermod -l lijunjie lijie

[root@localhost ~]# tail -1 /etc/passwd

lijunjie:x:502:502::/home/lijie:/bin/bash

从输出结果可见，用户名已更改为lijunjie。主目录仍为原来的/home/lijie，若也要更改为/home/lijunjie，则可通过执行以下命令来实现

[root@localhost ~]# usermod -d /home/lijunjie lijunjie

[root@localhost ~]# tail -1 /etc/passwd

lijunjie:x:502:502::/home/lijunjie:/bin/bash

[root@localhost ~]# mv /home/lijie /home/lijunjie

（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。

（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

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。

  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lijunjie账户的登陆密码，则操作命令为：

[root@localhost ～]# passwd lijunjie

更改用户 lijunjie 的密码 。

新的 密码：

重新输入新的 密码：

passwd： 所有的身份验证令牌已经成功更新。

  账户登录密码设置后，该账户就可以登录系统了。按ctrl+alt+F2键，选择第2号虚拟控制台（tty2），然后利用lijunjie账户登录，以检验能否登录。

8，锁定/解锁账户密码

  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菜蔬的passwd命令，其用法为：

 passwd -l 帐户名

 passwd -u 帐户名    #解锁账户密码

9，查询密码状态

  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 etc]# passwd -S lijunjie

lijunjie LK 2011-03-25 0 99999 7 -1 (密码已被锁定。)

[root@localhost etc]# passwd -u lijunjie

解锁用户 lijunjie 的密码 。

passwd: 操作成功

[root@localhost etc]# passwd -S lijunjie

lijunjie PS 2011-03-25 0 99999 7 -1 (密码已设置，使用 SHA512 加密。)

10，删除账户密码

  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。

11，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.

12，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 ~]# tail -3 /etc/group

    student:x:501:

    lijie:x:502:

    vodup:x:503:

    [root@localhost ~]# groupmod -n teacher student

    [root@localhost ~]# tail -3 /etc/group

    lijie:x:502:

    vodup:x:503:

    teacher:x:501:

（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504，则操作命令为：

[root@localhost ~]# tail -3 /etc/group

lijie:x:502:

vodup:x:503:

teacher:x:501:

[root@localhost ~]# groupmod -g 504 teacher

[root@localhost ~]# tail -3 /etc/group

lijie:x:502:

vodup:x:503:

teacher:x:504:

13，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 ~]# groupdel teacher

groupdel: cannot remove the primary group of user 'zhangjie'

[root@localhost ~]# userdel -r zhangjie

[root@localhost ~]# 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

14，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，现在将上面创建的lijunjie用户添加到vodup用户组中

[root@localhost ~]# groups lijunjie

lijunjie : lijie

[root@localhost ~]# gpasswd -a lijunjie vodup  #添加用户到指定的用户组

Adding user lijunjie to group vodup

[root@localhost ~]# groups lijunjie

lijunjie : lijie vodup

[root@localhost ~]# gpasswd -d lijunjie vodup  #从指定的用户组中移除用户

Removing user lijunjie from group vodup

[root@localhost ~]# groups lijunjie   #查看用户所属的组

lijunjie : lijie

15，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 ~]# gpasswd -A lijunjie vodup

[root@localhost ~]# useradd fen

[lijunjie@localhost ~]# gpasswd -a fen vodup

Adding user fen to group vodup

[lijunjie@localhost ~]# groups fen

fen : fen vodup

[lijunjie@localhost ~]# gpasswd -d fen vodup

Removing user fen from group vodup

[lijunjie@localhost root]$ gpasswd -d fen fen  #试图将fen用户从fen用户组中移除

gpasswd: Permission denied.     #操作被拒绝，说明无权对其他用户组进行管理

  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。