Linux用户和组

Linux用户和组
- 课堂作业
- 用户和组的相关文件
  - /etc/passwd
  - /etc/shadow
  - /etc/group
  - /etc/gshadow
  - /etc/default/useradd
  - /etc/skel/
  - /etc/login.defs
  - /etc/shells
- 用户和组的相关命令
  - 新建用户和组
    - groupadd
    - useradd
    - passwd
  - 修改用户和组属性
    - groupmod
    - usermod
    - chage
    - chsh
  - 删除用户和组
    - groupdel
    - userdel
  - 查看用户和组信息
    - id
    - groups
- 用户身份切换 sudo / su
  - su
  - sudo
    - sudo 执行流程
    - 添加用户 sudo 执行权限的方法
- Linux用户和组课后作业

课堂作业

1. 添加2个组，一个组名为justice，另外一个组名为ninja。
2. 添加4个新用户，分别为 superman、batman、wonderwoman、greenlantern，密码均为uplooking；其附加组为justice。
3. 添加4个新用户，分别为 leo、raph、mikey、don ，密码均为uplooking，其附加组为ninja。
4. mikey用户总是在系统里搞破坏，root决定封他的号，让他不能登陆。过了几天，再解封。
5. leo想加入justice，root同意了，将justice作为附加组添加给leo。
6. don整天搞创造，root要求他的密码要更安全，所以将他的密码设置成7天之后要换密码，并且密码过期前3天要提醒他，如果密码过期后2天还没有设置新密码，那么就封锁don账户。
7. batman总是喜欢修改密码，没事就在修改密码，而使用该batman账户的人有好几个，比如蝙蝠侠，蝙蝠侠的

管家，蝙蝠侠的助手罗宾等等。所以root决定将batman账户的密码的最小存活期改为10天。也就是说10天之内batman账户不能修改密码。

8. leo想退出justice,root帮他设置一下。
9. superman想把密码改为uplooking123，让他自己改。发现改不了，密码太简单了，自己去想一个复杂的密码。
10. 让superman能够修改root用户的密码。

用户和组的相关文件

文件名	作用
/etc/passwd	系统中的账号信息
etc/shadow	存放密码及其策略相关信息
/etc/group	存放用户组的信息
/etc/gshadow	存放用户组的密码及其策略相关信息
/etc/default/useradd	创建新用户时默认的配置信息
/etc/skel/*	Directory containing default files.
/etc/login.defs	用户和组默认的配置信息
/etc/shells	该文件记录着合法的 shell 版本

/etc/passwd

每一行都代表一个账号，有几行就代表有几个账号在你的系统中

系统统账号: bin, daemon, adm, nobody

以“：”作为分隔符,七个字段

`root:x:0:0:root:/root:/bin/bash`

1. 账号名称 :root
2. 密码 :X
3. UID: 使用者标识符
   rhel6 root_uid=0 sys_uid=1-499 user_uid=500-65535 (2^32-1)
   rhel7 root_uid=0 sys_uid=201-999 user_uid=1000-65535
4. GID: 用户组标识符 root_guid=0
5. 用户信息说明栏
6. 家目录 : 用户的家目录 root 的家目录在 /root, 默认用户的家目录在 /home/yourname
7. Shell: 命令解释器
   - 系统默认为 /bin/bash

- /sbin/nologin 不可通过终端登录系统

/etc/shadow

存放密码及其策略相关信息

以“：”作为分隔符九个字段

`root:$1$/30QpE5e$y9N/D0bh6rAACBEz.hqo00:14126:0:99999:7:::`

1. 账号名称 :root
2. 密码 : 加密后的字符串，以N 开头
3. 最近变更密码的日期 : 天数,以 1970 年 1 月 1 日作为 1 而累加的日期
   echo (((date --date="2008/09/04" +%s)/86400+1))
   14126
4. 密码不可被更改的天数 :0 : 表示密码随时可以更改， 20 :表示 距最近一次修改密码20 天之内都不能修改密码
5. 密码需要重新变更的天数 :99999 (计算为 273 年) 表示密码的变更没有强制性。
6. 密码需要变更期限前的警告天数 : 在密码到期之前几天提醒
7. 密码过期后的账号宽限时间 (密码失效日): 密码过期特性。
8. 账号失效日期 : 天数，以 1970 年 1 月 1 日作为 1 而累加的日期
9. 保留 : 保留段

/etc/group

存放用户组的信息

每一行代表一个群组以“：”作为分隔符四个字段

`root:x:0:root`

1. 组名 :root
2. 群组密码 :x 一般不设定,通常是给『群组管理员』使用
3. GID: 群组的 ID
4. 此群组支持的账号名称 : 一个账号可以加入多个群组

例如,将 dabao 加入 root 群组后 :

```
root:x:0:root,dmtsai
```

/etc/gshadow

存放用户组的密码及其策略相关信息

每一行代表一个群组 “: ” 作为分隔符四个字段

`newgroup:!::redhat`

1. 组名 :newgroup
2. 密码栏 : 开头为 ! 表示无合法密码 , 所以无群组管理员
3. 群组管理员的账号
4. 此群组支持的账号名称 : 与 /etc/group 相同

/etc/default/useradd

创建新用户时默认的配置信息

```
GROUP=100 <== 预设的群组，现已不生效，如果创建用户时不指定群组，则使用与用户同名的群组
HOME=/home <== 默认的家目录所在目录
INACTIVE=-1 <== 密码失效日 , 在 shadow 第 7 栏
EXPIRE= <== 账号失效日 , 在 shadow 第 8 栏
SHELL=/bin/bash <== 预设的 shell /sbin/nologin 将无法登陆
SKEL=/etc/skel<== 用户家目录的内容数据参考目录
CREATE_MAIL_SPOOL=yes <== 是否主动帮助使用者建立邮件信箱 (mailbox)
```

/etc/skel/

Directory containing default files.

.bash_logout .bash_profile .bashrc .gnome2 .mozilla

```
[root@rhel7 skel]# ll -a /etc/skel
total 40
drwxr-xr-x. 4 root root 4096 Jan 2 01:58 .
drwxr-xr-x. 125 root root 12288 Mar 21 03:09 ..
-rw-r--r--. 1 root root 18 Jul 9 2013 .bash_logout
-rw-r--r--. 1 root root 176 Jul 9 2013 .bash_profile
-rw-r--r--. 1 root root 124 Jul 9 2013 .bashrc
-rw-r--r--. 1 root root 500 May 7 2013 .emacs
drwxr-xr-x. 2 root root 4096 Jul 14 2010 .gnome2
drwxr-xr-x. 4 root root 4096 Jan 2 01:52 .mozilla
```

/etc/login.defs

默认的配置信息 rhel6 下的信息

```
MAIL_DIR          /var/spool/mail 用户默认邮件信箱放置目录
PASS_MAX_DAYS     99999 /etc/shadow 第 5 栏 , 密码需要重新变更的天数
PASS_MIN_DAYS     0 /etc/shadow 第 4 栏 , 密码不可被更动的天数
PASS_MIN_LEN      5 密码最短的字符长度 , 已被 pam 模块取代 , 失去效用 !
PASS_WARN_AGE     7 /etc/shadow 第 6 栏 , 过期前会警告天数
UID_MIN           500 使用者最小的 UID 不能 <500
UID_MAX           60000  使用者最大的 UID 不能 >60000
GID_MIN           500  自定义组最小的 UID 不能 <500
GID_MAX           60000  自定义组最大的 UID 不能 >60000
CREATE_HOME     yes  在 username 命令不加 -M 及 -m 时 , 是否主动建立用户家目录
UMASK        077  用户家目录建立的 umask , 因此权限会是 700 『 drwx------ 』
USERGROUPS_ENAB  yes  使用 userdel 时 , 是否会删除初始群组(如果使用 userdel 去删除一个账号时 , 该账
号所属的初始群组已经没有人隶属于该群组了 , 那举就删掉该群组)
ENCRYPT_METHOD    SHA512  经过 SHA512 进行加密处理
```

/etc/shells

该文件记录着合法的 shell 版本

```
[root@rhel7 skel]# cat /etc/shells
/bin/sh
/bin/bash
/sbin/nologin
/bin/dash
/bin/tcsh
/bin/csh
```

用户和组的相关命令

用户和组	
新建组	groupadd
新建用户	useradd
修改密码	passwd 密码 >8 位字符、小写 / 大写 / 数字 / 特殊符号之间任选 3 位
修改用户属性	usermod
修改组属性	groupmod
修改密码属性	chage
修改 shell	chsh
删除用户	userdel
删除组	groupdel
查看已存在用户的基本信息	id
查看当前用户支持的群组信息	groups

通过文件查看

```
/etc/passwd
/etc/shadow
/etc/group
/etc/gshadow
```

新建用户和组

groupadd

```
groupadd 创建组
-g, --gid GID
-r, --system  Create a system group

 新建组 test 制定 gid 为 888
[root@rhel7 ~]# groupadd -g 888 test
 新建一个系统组 baby
[root@rhel7 ~]# groupadd -r baby
 查看一下刚刚新建的组的信息
[root@rhel7 ~]# tail -n 2 /etc/group
test:x:888:
baby:x:490:
```

useradd

```
创建新用户
useradd [-u UID] [-g 初始群组 ] [-G 次要群组 ] [-mM] [-c 说明栏 ] [-d 家目录绝对路径 ] [-s shell]
账号名
拓展: -e : 接日期『 YYYY-MM-DD 』 shadow 第八字段账号失效日期
    -f : 接天数 shadow 第七字段密码失效日 0 :立刻失效 -1 :永不失效
        失效后可登陆,但是会强制你重新设置密码
[root@rhel7 ~]# useradd -u 888 -g 888 -f 0 -e 2016-03-21 t1
[root@rhel7 ~]# id t1
uid=888(t1) gid=888(test) groups=888(test)
[root@rhel7 ~]# tail -n 1 /etc/passwd
t1:x:888:888::/home/t1:/bin/bash
[root@rhel7 ~]# tail -n 1 /etc/shadow
t1:!!:16880:0:99999:7:0:16881:
```

passwd

```
给用户设置密码
passwd [--sdtin] <== 所有人均可使用更改自己的密码
passwd [-l] [-u] [--sdtin] [-S] [-n 日数 ] [-x 日数 ] [-w 日数 ] [-i 日期 ] 账号 <==root 功能
选项与参数 :
--stdin : 可以透过来自前一个管线的数据 , 作为密码输入 echo 123 | passwd --stdin dabao
-l : 是 Lock 的缩写 , 会将 /etc/shadow 第二栏最前面加上 ! 使密码失效
-u : 与 -l 相对 , 是 Unlock 的缩写
-S : 列出密码相关参数 shadow 大部分信息。
-n : 后面接天数 ,shadow 第 4 字段 , 密码不可被更动的天数
-x : 后面接天数 ,shadow 第 5 字段 , 密码需要重新变更的天数
-w : 后面接天数 ,shadow 第 6 字段 , 密码需要变更期限前的警告天数
-i : 后面接天数 ,shadow 第 7 字段 , 密码失效日期
```

```
[root@rhel7 ~]# passwd t1
Changing password for user t1.
New password:
BAD PASSWORD: it is based on a dictionary word
Retype new password:
passwd: all authentication tokens updated successfully.

 设置密码失效日期为 7 天
[root@rhel7 ~]# passwd -i 7 t1
Adjusting aging data for user t1.
passwd: Success

 查看记录用户密码属性的文件 /etc/shadow ,截取 t1 用户的那一行
[root@rhel7 ~]# sed -n '/t1/p' /etc/shadow
t1:$6$TDnycU/C$0AmM5AoZmoHZQMex.dQCoroH2JxdSnDhLnBMorcUPlWgshYrlstZJmH.Q.fT
OTV.pECGEuqFqugj8YccRqcdD/:16880:0:99999:7:7:16881:

 截取 t1 用户密码属性,以 : 为分割的第 7 字段
[root@rhel7 ~]# sed -n '/t1/p' /etc/shadow|cut -d":" -f 7
7
[root@rhel7 ~]# sed -n '/t1/p' /etc/shadow|awk -F: '{print 7}'
7
```

修改用户和组属性

groupmod

修改组属性

```
groupmod -g gid [gname] 修改 gid
groupmod -n new_gname [gname] 修改组的名字
[root@rhel7 ~]# groupmod -g 999 test
[root@rhel7 ~]# grep test /etc/group
test:x:999:
[root@rhel7 ~]# groupmod -n test1 test
[root@rhel7 ~]# grep test /etc/group
test1:x:999:
```

usermod

修改用户属性

```
usermod [-cdegGlsuLU] username
选项不参数 :
-c : 后面接账号的说明 修改 /etc/passwd 第 5 字段
-d : 后面接账号的家目录 修改 /etc/passwd 第 6 字段
-e : 后面接日期 , 格式是 YYYY-MM-DD 修改 shadow 第 8 字段 ( 账号失效日 )
-f : 后面接天数 修改 shadow 第 7 字段 ( 密码失效日期 )
-g : 后面接初始群组 修改 /etc/passwd 第 4 字段 GID
-G : 后面接次要群组 , 修改这个使用者能够支持的群组 修改 /etc/group
-aG : 『增加次要群组的支持』而非『设定』
-l : 后面接账号名称 修改账号名称 修改 /etc/passwd 第 1 字段
-s : 后面接 Shell 的实际档案 , 例如 /bin/bash /bin/csh 等等
-u : 后面接 UID 数字啦 ! 即 /etc/passwd 第三栏的资料 ;
-L : 暂时将用户的密码冻结 , 让他无法登入。修改 /etc/shadow 密码栏
-U : 将 /etc/shadow 密码栏的 ! 拿掉 , 解冻
```

```
[root@rhel7 ~]# usermod -g test2 -G test3 t1
[root@rhel7 ~]# id t1
uid=888(t1) gid=1000(test2) groups=1000(test2),1001(test3)
[root@rhel7 ~]# usermod -s /sbin/nologin t1
[root@rhel7 ~]# grep t1 /etc/passwd
t1:x:888:1000::/home/t1:/sbin/nologin
[root@rhel7 ~]# su - t1
This account is currently not available.
```

chage

修改用户密码属性

```
chage [-ldEImMW] 账号名
选项与参数 :
-l : 列出该账号的详细密码参数 ;
-d : 后面接日期 , 修改 shadow 第 3 字段 ( 最近一次更改密码的日期 ), 格式 YYYY-MM-DD
-m : 后面接天数 , 修改 shadow 第 4 字段 ( 密码不可被更动的天数 )
-M : 后面接天数 , 修改 shadow 第 5 字段 ( 密码需要重新变更的天数 )
-W : 后面接天数 , 修改 shadow 第 6 字段 ( 密码需要变更期限前的警告天数 )
-I : 后面接天数 , 修改 shadow 第 7 字段 ( 密码失效日期 )
-E : 后面接日期 , 修改 shadow 第 8 字段 ( 账号失效日 ), 格式 YYYY-MM-DD
```

```
[root@rhel7 ~]# chage t1
Changing the aging information for t1
Enter the new value, or press ENTER for the default
Minimum Password Age [0]:
Maximum Password Age [99999]:
Last Password Change (YYYY-MM-DD) [2016-03-20]:
Password Expiration Warning [7]:
Password Inactive [7]:
Account Expiration Date (YYYY-MM-DD) [2016-03-21]:
```

chsh

change shell 的简写

```
chsh [-ls]
选项与参数 :
-l : 列出目前系统上面可用的 shell /etc/shells 里内容
-s : 修改自己的 Shell
[root@rhel7 ~]# chsh -s /bin/bash t1
Changing shell for t1.
Shell changed.
[root@rhel7 ~]# grep t1 /etc/passwd
t1:x:888:1000::/home/t1:/bin/bash
```

删除用户和组

groupdel

删除组

groupdel groupname

userdel

删除用户

```
userdel [-r] username
选项不参数 :
-r 没有这个选项删除会不彻底,关于用户的目录、文档全部删除

[root@rhel7 ~]# tail -3 /etc/group
test:x:999:
test2:x:1000:
test3:x:1001:t1
[root@rhel7 ~]# groupdel test3
[root@rhel7 ~]# tail -3 /etc/group
baby:x:490:
test:x:999:
test2:x:1000:
[root@rhel7 ~]# userdel -r t1
[root@rhel7 ~]# ll /home
total 12
drwx------. 27 cong cong 4096 Jan 1 18:40 cong
drwx------. 4 g2
888 4096 Mar 21 03:56 g2
drwx------. 12 tom tom 4096 Mar 21 02:14 tom
```

查看用户和组信息

id

查看已存在用户的基本信息

```
[root@rhel7 ~]# id root
uid=0(root) gid=0(root) groups=0(root)
[root@rhel7 ~]# id -g root
0
[root@rhel7 ~]# id -u root
0
```

groups

查看当前用户支持的群组信息

```
[root@rhel7 ~]# groups
root
```

思考题: root 和普通用户都可以修改 /etc/passwd 文档,那么这个文档的权限是什么呢?
SUID

用户身份切换 sudo / su

su

```
su [-lm] [-c 指令 ] [username]
选项与参数 :
- : 单纯使用 - 如『 su - 』 以 login-shell 变量档案读取方式登入系统 ; 默认切换为 root
-l : 与 - 类似 login-shell
-m :-m 与 -p 一样 , 表示『使用目前的环境设定 , 而不读取新使用者的配置文件』
-c : 接指令
```

总结:

1. su - username 或 su -l username
   完整切换成新使用者的环境 用 env 查看环境变量
   PATH/USER/MAIL
2. su - -c " 指令 "
   仅想要执行一次 root 的指令
3. 使用 root 切换成为任何使用者时 , 不需要输入新用户密码
4. 缺点:当主机多人管理时, su 切换成 root ,那每个人都需要知道 root 密码,不安全。

sudo

sudo [-u user name | #uid][command]

sudo 执行流程

1. 在 /etc/sudoers 档案中查看 user 是否有 sudo 执行权限
2. 若有 sudo 执行权限 , 『输入用户的密码』
3. 密码正确 , 开始执行 sudo 后续接的指令
4. root 无需密码,自己切换自己也无需密码

添加用户 sudo 执行权限的方法

(如何让用户可以使用 sudo ?)

1. visudo 可以让系统检验 /etc/sudoers 的语法是否正确
2. 修改 /etc/sudoers 中的语法

1)单一用户可使用 root 所有指令或某些指令

```
root        ALL=(ALL)   ALL <== 找到这一行 ,rh6 在 98 行
username    ALL=(ALL)   ALL <== 新增这一行
username    ALL=(root)  /bin/touch<== 新增这一行
```

语法解释:

使用者账号 登入者的来源主机名 =(可切换的身份)　　可下达的指令

root　　ALL=(ALL)　　ALL <== 这是默认值

1. 使用者帐号:系统哪个帐号可以使用 sudo
2. 登入者的来源主机名:信任用户 默认 root 可来自任何一部网络主机
3. 可切换的身份:该账号可以切换成谁来下命令 , 末日 root 可以切换成任何人
4. 可下达的指令:可用该身份下达什么指令。必需使用绝对路径 (可通过 which\whereis 查询)
5. ALL : 是特殊关键词 , 代表任何身份、任何主机、任何命令

2)群组和免密码的功能处理

```
%wheel ALL=(ALL) ALL<== 找到这一行 ,rh6 在 105 行
%wheel ALL=(ALL) NOPASSWD: ALL<== 找到这一行 ,rh6 在 108 行
```

语法解释:

1. % 接群组
2. wheel 群组内的用户有使用 sudo 的权限,并可以切换成任何人,执行切换后身份的任何命令
3. wheel 群组内的用户切换用户时不需要输入自己的密码

3）有限的权限操作

```
dabao ALL=(root) /usr/bin/passwd <== 有 bug , dabao 能修改 root 密码
dabao ALL=(root) !/usr/bin/passwd, /usr/bin/passwd [A-Za-z]*,!/usr/bin/passwd root<== 可以执
行『 passwd 任意字符』 , 但是『 passwd 』和『 passwd root 』这两个命令不可执行
```

4)别名设置 visudo

```
User_Alias DABAO=dabao,jerry,tom,g1,g2,g3
Cmnd_Alias DABAOCOM = !/usr/bin/passwd,/usr/bin/passwd [A-Za-z]*,!/usr/bin/passwd root
DABAO ALL=(root) DABAOCOM
```

5) sudo 搭配 su 使用

```
username ALL=(root) /bin/su -
sudo su - <==sudo -u root su -l root
```

可以直接切换成 root 用户,而且不需要输入 root 密码

6) 5 分钟内可以不用再输入密码。

Linux用户和组课后作业

1. 新建一个用户名为 redhat。密码为 password ， 配置以下信息,以达到要求:

- 密码的最小存活期为:1 天
- 密码的最大存活期为:10 天
- 密码过期前 5 天提醒
- 密码过期后如 15 天仍未设置新密码,则封锁该帐户。

1. 创建一个新组 newgroup、将 redhat 以附加组成员的身份加入 到 newgroup 中。
2. 添加 3 个用户,用户 harry,natasha,tom,和一个组 ,组名为 admin 组 ，
   要求 ：

- harry,natasha 用户的附加组为 admin 组；
- tom 用户的登陆 shell 为非交互式 shell；
- 用户密码都为 uplooking

1. 使用 harry 用户登陆系统,尝试修改自己的密码,密码自己设 定。
2. 创建一个叫做 alex 用户,用户 uid 为 1234,不能登陆系统。
3. 以 root 用户身份给 natasha 用户修改密码,密码修改为 abc12345。
4. 给 tom 用户追加附加组,追加的附加组为 alex,同时给 tom 用户修改 uid,修改为 2222。