Linux用户及权限管理

一、实验介绍

1.内容描述

本实验主要介绍了Ubuntu操作系统的文件和权限管理。

2.实验目的

- 掌握用户和组的管理；
- 掌握文件权限的管理；
- 掌握文件访问控制。

二、用户和用户组的管理

步骤1 who命令是显示目前登录系统的用户信息。

```
[root@localhost ~]# who
root     tty1         2020-07-08 11:23
root     pts/0        2020-07-08 14:06 (172.19.130.137)
```

步骤2 id命令用于显示用户的 ID，以及所属群组的 ID

```
[root@localhost ~]# id
uid=0(root) gid=0(root) groups=0(root)
context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
```

步骤3 以 root用户登录到系统，创建用户 tom、bob、jack，且创建 jack用户时指定其UID为 1024。

```
[root@localhost ~]# useradd tom
[root@localhost ~]# useradd bob
[root@localhost ~]# useradd -u 1024 jack
[root@localhost ~]# tail -3 /etc/passwd
tom:x:1001:1001::/home/tom:/bin/bash
bob:x:1002:1002::/home/bob:/bin/bash
jack:x:1024:1024::/home/jack:/bin/bash
[root@localhost ~]# useradd -d /home/myd bob1      #为新添加的用户指定home目录
Creating mailbox file: File exists
[root@localhost ~]# useradd -d /usr/local/apache -g apache -s /bin/false bob2
#添加一个不能登录的用户；添加一个bob2用户，登录目录为/usr/local/apache，用户组为apache，指定shell为/bin/false；将用户shell设置为/usr/sbin/nologin或者/bin/false，表示拒绝系统用户登录
```

步骤4 将用户 tom的用户名改为 tony，以及将其家目录改为/home/tony。

```
[root@localhost ~]# usermod -l tony tom
[root@localhost ~]# cp -r /home/tom/ /home/tony/
[root@localhost ~]# cd /home/tony/
[root@localhost tony]# cd ~
[root@localhost ~]# usermod -d /home/tony/ tony
[root@localhost ~]# tail -3 /etc/passwd
bob:x:1002:1002::/home/bob:/bin/bash
jack:x:1024:1024::/home/jack:/bin/bash
tony:x:1001:1001::/home/tony/:/bin/bash
```

修改原tom用户的私有组名tom改为tony

```
[root@localhost ~]# groupmod -n tony tom
[root@localhost ~]# tail -1 /etc/group
tony:x:1001:
```

步骤5 将用户 bob及家目录一并给删除掉。

```
[root@localhost ~]# userdel -r bob
[root@localhost ~]# tail -2 /etc/passwd
jack:x:1024:1024::/home/jack:/bin/bash
tony:x:1001:1001::/home/tony/:/bin/bash
```

注意：上图是显示用户配置文件的末尾 2行，可以看到这里没有 bob用户了在家目录中也没有了 bob目录。

```
[root@localhost ~]# ls /home/
jack  openeuler  tom  tony
```

步骤6 sudo切换用户。

我们在终端上从当前 root用户切换的到 jack用户

```
[root@localhost ~]# su jack
[jack@localhost root]$ pwd
/root
[jack@localhost root]$ exit
exit
[root@localhost ~]# su - jack
[jack@localhost ~]$ pwd
/home/jack
[jack@localhost ~]$ exit
```

三、用户账号的锁定操作

步骤1 首先分别给 tony账号和 jack账号设置密码，密码设置为 Huawei@123，此处输入密码不会有显示。

```
[root@localhost ~]# passwd tony
Changing password for user tony.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
```

```
[root@localhost ~]# passwd jack
Changing password for user jack.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
```

步骤2 然后将 jack账号锁定，测试效果后再解锁。查看 jack 账号当前的状态。

```
[root@localhost ~]# passwd -S jack
jack PS 2020-07-08 0 99999 7 -1 (Password set, SHA512 crypt.)
[root@localhost ~]# passwd -l jack
Locking password for user jack.
passwd: Success
[root@localhost ~]#
[root@localhost ~]# passwd -S jack
jack LK 2020-07-08 0 99999 7 -1 (Password locked.)
[root@localhost ~]# passwd -uf jack      →      //openEuler 在这里做了安全加强，必须加上-f 强制解锁。
Unlocking password for user jack.
passwd: Success
[root@localhost ~]# passwd -S jack
jack PS 2020-07-08 0 99999 7 -1 (Password set, SHA512 crypt.)
```

步骤3 chage命令查看编辑密码过期时间。

查看用户密码过期时间。

```
[root@localhost ~]# chage -l jack
Last password change                                    : Jul 08, 2020
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
```

编辑用户密码过期时间，其它参数说明：

- -m密码可更改的最小天数。为零时代表任何时候都可以更改密码。
- -M密码保持有效的最大天数。
- -W用户密码到期前，提前收到警告信息的天数。
- -E帐号到期的日期。过了这天，此帐号将不可用。
- -d上一次更改的日期
- -I停滞时期。如果一个密码已过期这些天，那么此帐号将不可用。
- -l例出当前的设置。由非特权用户来确定他们的密码或帐号何时过期。
  -

四、用户组管理

步骤1 创建hatest组，且将用户tony、jack加到hatest组里面。

```
[root@localhost ~]# groupadd hatest
```

```
[root@localhost ~]# gpasswd -M tony,jack hatest
[root@localhost ~]# tail -1 /etc/group      #查看用户组是否创建成功
hatest:x:1025:tony,jack
```

步骤2 删除，修改用户组。

```
[root@localhost ~]# groupadd group1
[root@localhost ~]# groupadd -g 101 group2
[root@localhost ~]# groupdel group1      #删除用户组
[root@localhost ~]# groupmod -g 102 group2 #更改用户组 ID
[root@localhost ~]# cat /etc/group         #查看用户组
root:x:0:
bin:x:1:
daemon:x:2:
```

五、手工及批量创建账号

步骤 1 编辑一个文本用户文件，每一列按照/etc/passwd密码文件的格式书写，要注意每个用户的用户名、UID、宿主目录都不可以相同，其中密码栏可以留做空白或输入x 号。

```
[root@localhost ~]# vim users.txt
user1:x:1200:1200:user001:/home/user1:/bin/bash
user2:x:1201:1201:user002:/home/user2:/bin/bash
user3:x:1202:1202:user003:/home/user3:/bin/bash
```

步骤 2 以 root身份执行命令 newusers，从刚创建的用户文件 user.txt中导入数据，创建用户。

```
[root@localhost ~]# newusers < users.txt
[root@localhost ~]# tail -3 /etc/passwd
user1:x:1200:1200:user001:/home/user1:/bin/bash
user2:x:1201:1201:user002:/home/user2:/bin/bash
user3:x:1202:1202:user003:/home/user3:/bin/bash
```

六、查看常见用户关联文件

步骤1 查看用户账号信息文件：/etc/passwd。

```
[root@localhost ~]# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
...
```

步骤2 查看用户账号信息加密文件/etc/shadow。

```
[root@localhost ~]# cat /etc/shadow
root:$6$4KT4vnGt0.9B/FQS$IcrlSwJmvkyFjrhPrgOCtg.b2FbTdQx4XWqTBiuRzUN7EoRCgDkkepeLq3KXdesc
uFnHNCf.zPVt6L4..N7Mw.:18451:0:99999:7:::
bin:*:18344:0:99999:7:::
...
```

步骤3 查看组信息文件/etc/group。

```
[root@localhost ~]# cat /etc/group
root:x:0:
bin:x:1:
daemon:x:2:
...
```

步骤4 查看组信息加密文件/etc/gshadow。

```
[root@localhost ~]# cat /etc/gshadow
root:::
bin:::
daemon:::
...
```

七、设置文件及目录的权限及归属

步骤1 使用 root用户创建目录/test以及在其下创建文件 file1、文件 file2，并查看其默认的权限及归属。

```
[root@localhost ~]# mkdir test
[root@localhost ~]# cd /test
[root@localhost test]# touch file1
[root@localhost test]# touch file2
[root@localhost  test]#  ls -l
total 0
-rwxr-xr-x. 1 root root 0 Jul  8 15:48 file1
-rwxr-xr-x. 1 root root 0 Jul  8 15:48 file2
[root@localhost test]# ls -l / | grep test
drwxrwxrwt.    2 root root  4096 Jul  8 15:41 test
```

步骤2 将/test目录修改为公共共享目录即给其设置 t位权限位。

```
[root@localhost test]# cd
[root@localhost ~]# chmod 1777 /test/
[root@localhost ~]# ls -l / | grep test
drwxrwxrwt.    2 root root  4096 Jul  8 15:41 test
```

将文件 file1和 file2设置权限为 755。

```
[root@localhost ~]# chmod 755 /test/file1 /test/file2
[root@localhost ~]# ls -l /test/
total 0
-rwxr-xr-x. 1 root root 0 Jul  8 15:41 file1
-rwxr-xr-x. 1 root root 0 Jul  8 15:41 file2
```

步骤3 将文件 file1设为所有人皆可读取。

```
[root@localhost test]# chmod ugo+r file1
```

步骤4 将文件 file1设为所有人皆可读取。

```
[root@localhost test]# chmod a+r file1
```

步骤5 将文件 file1与 file2设为该文件拥有者，与其所属同一个群体者可写入，但其他以外的人则不可写入。

```
[root@localhost test]# chmod ug+w,o-w file1 file2
```

步骤6 将目前目录下的所有文件与子目录皆设为任何人可读取。

```
[root@localhost test]# chmod -R a+r *
```

步骤7 将文件 file1的所属用户改为 jack，所属用户组改为 hatest组。

```
[root@localhost ~]# chown jack:hatest /test/file1
[root@localhost ~]# ls -l /test/
total 0
-rwxr-xr-x. 1 root root 0 Jul  8 15:41 file1
-rwxr-xr-x. 1 root root 0 Jul  8 15:41 file2
```

步骤8 修改文件群组属性。

```
[root@localhost test]# chgrp -v bin file1
changed group of 'file1' from root to bin
[root@localhost test]# ll
total 4.0K
-rwxrwxr-x+ 1 root bin  0 Jul  8 15:48 file1
-rwxrwxr-x. 1 root root 0 Jul  8 15:48 file2
```

步骤9 通过 umask来查看为修改权限掩码前 umask值。

```
[root@localhost test]# umask
0077
```

步骤10 使用 umask命令进行权限的修改。

```
[root@localhost test]# umask 022
[root@localhost test]# umask
0022
```

八、ACL的设置

步骤1 先使得文件 file1的所属组对其有写入权限。

```
[root@localhost ~]# chmod 775 /test/file1
[root@localhost ~]# ls -l /test | grep file1
-rwxrwxr-x. 1 root root 0 Jul  8 15:48 file1
```

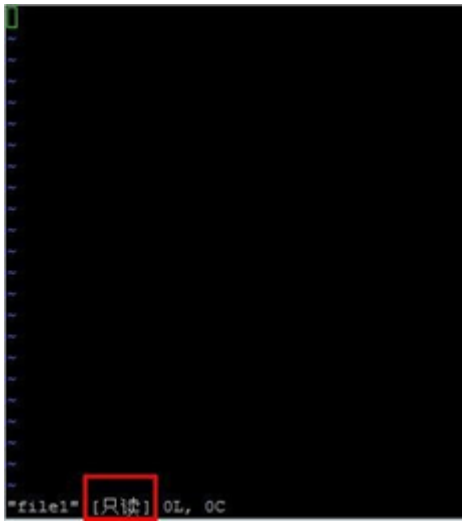
步骤2 配置文件 ACL使得 hatest组中 tony用户对文件 file1只有只读权限。

```
[root@localhost ~]# getfacl /test/file1
getfacl: Removing leading '/' from absolute path names
# file: test/file1
# owner: jack
# group: hatest
user::rwx
group::rwx
other::r-x
```

```
[root@localhost ~]# setfacl -m u:tony:r /test/file1
[root@localhost ~]# getfacl /test/file1
getfacl: Removing leading '/' from absolute path names
# file: test/file1
# owner: jack
# group: hatest
user::rwx
user:tony:r--
group::rwx
mask::rwx
other::r-x
```

步骤3 切换到 tony用户下测试是否能写入 file1文件。注意：这里为了测试起冲突，取消掉/test目录的 t 位。

```
[root@localhost ~]# chmod 777 /test/
[root@localhost ~]# ls -l / | grep test
drwxrwxrwx.    2 root root  4096 Jul  8 15:41 test
[root@localhost ~]# su - tony
[tony@localhost root]$ cd /test/
[tony@localhost test]$ vim file1
```



发现文件是只读的，无法写入。

步骤4 清除文件名为 file1的文件上的 ACL设置。

```
[root@localhost test]# getfacl -e file1
# file: file1
# owner: root
```

```
# group: bin
user::rwx
user:tony:r--                   #effective:r--
group::rwx                      #effective:rwx
mask::rwx
other::r-x

[root@localhost test]# chacl -B file1
[root@localhost test]# getfacl -e file1
# file: file1
# owner: root
# group: bin
user::rwx
group::rwx
other::r-x
```

九、练习题

- 创建一个目录 /data；
- 创建 user1,user2,user3三个用户要求如下：
  user1家目录在/data目录下，该用户的描述为 testuser；

  user2用户的 uid应当为 2000；

  user3用户应当使用 /bin/tcsh这个登录 shell。
- 将以上三个用户加入到一个 GID为 3000，名为 it的组中；
- 创建/it；
- 要求 it 组内的所有成员都可以在/it目录下创建文件，删除文件；
- 给 it组更名为 cloud。
- 设置 user1用户密码过期时间为 15天，过期前 3天提醒；
- 设置 user2不允许登录
- 创建一个目录/test，设置该目录 ACL，仅允许 user1具有读写权限，user3具有读权限，其他人无权限。