

实验 07 用户和权限管理

班级：数据科学与大数据一班

学号：202026203005

姓名：张华

用户名：s13

一、实验目的

1. 练习用户和组管理
2. 练习权限管理

二、实验要求

1. 填写实验报告，请将关键命令及其结果进行截图(请确保截图中的文字清晰可见)
2. 导出为 pdf 文件，文件名为用户名-姓名-lab06.pdf，在规定截止时间之前上传作业)
3. 以下步骤中所有 s01 请换成你自己的用户名，01 请换成你自己用户名中的序号。

三、实验步骤

1. 不通过 `useradd` 命令，而是手工创建用户 s01-myuser，设定其 UID 和 GID 均为 2001
(提示: 请事先仔细调查清楚 `useradd` 命令幕后到底做了哪些事情, 比如修改了那些文件、设置了哪些权限、复制了哪些文件等)

(1) 请给出你的具体步骤及其截图。

(提示: 可以用命令 `perl -e 'print crypt("password", "\$6\$salt\$") . "\n"'` 命令手工生成加密的登录密码, 其中 `password` 可自选选择, `salt` 请选择 8 位随机字符串)

1、修改/etc/passwd 文件，添加一条用户信息

```
nscd:x:28:28:Nscd Daemon:/usr/sbin/nologin
admin:x:1000:1000::/home/admin:/bin/bash
s13:x:1001:1001::/home/s13:/bin/bash
mike:x:1002:1002::/home/mike:/bin/bash
s13-myuser:x:2001:2001::/home/s13-myuser:/bin/bash
```

2、修改 /etc/shadow 文件，加入用户信息

```
[root@iZuf6ixnt8107e8ns3k4tuZ ~]# perl -e 'print crypt("123", "\$6\$asdfghjk\$") . "\n"'
$6$asdfghjk$0zY6eoGr0ypF/6mnuEF1CtPgZDvTwYU0VDyhoHwgBh.PkV1tv/LDDFdFZRhe1VzRrLHm7R4vrx0ZFLAXUuv5d1
```

```
admin:!:19177:0:99999:7:::
s13:!:19239:0:99999:7:::
mike:!:19288:0:99999:7:::
s13-myuser:$6$asdfghjk$0zY6eoGr0ypF/6mnuEF1CtPgZDvTwYU0VDyhoHwgBh.PkV1tv/LDDFdFZRhe1VzRrLHm7R4vrx0ZFLAXUuv5d1:19288:0:99999:7:::
~
```

3、修改 /etc/group 文件，添加一条组信息

```
s13:x:1001:
mike:x:1002:
s13-myuser:x:2001:
```

4、建立用户主目录，添加环境变量，给与权限

```
[root@iZuf6ixnt8107e8ns3k4tuZ ~]# mkdir /home/s13-myuser
[root@iZuf6ixnt8107e8ns3k4tuZ ~]# cp /etc/skel/.bash* /home/s13-myuser/
[root@iZuf6ixnt8107e8ns3k4tuZ ~]# chown -R s13-myuser:s13-myuser /home/s13-myuser/
[root@iZuf6ixnt8107e8ns3k4tuZ ~]#
```

(2) 请测试以手工创建的新用户登录，并截图。

```
[root@iZuf6ixnt8107e8ns3k4tuZ ~]# su s13-myuser
[s13-myuser@iZuf6ixnt8107e8ns3k4tuZ root]$ cd
[s13-myuser@iZuf6ixnt8107e8ns3k4tuZ ~]$ pwd
/home/s13-myuser
[s13-myuser@iZuf6ixnt8107e8ns3k4tuZ ~]$ id
uid=2001(s13-myuser) gid=2001(s13-myuser) groups=2001(s13-myuser)
[s13-myuser@iZuf6ixnt8107e8ns3k4tuZ ~]$
```

2. 假设 A 公司的总经理兼总裁为 **s01-carl**，公司下设 4 个部门：

(1) 技术部(**tech**)：部门经理为 **s01-tony**，部门员工包括 **s01-t1**、**s01-t2**，**s01-t3**、**s01-t4**，他们都属于组 **s01-tech**，组管理员为 **s01-tech**。

(2) 市场部(**marcket**)：部门经理为 **s01-mary**，部门员工包括 **s01-m1**、**s01-m2**，**s01-m3**、**s01-m4**，他们都属于组 **s01-market**，组管理员为 **s01-marcket**。

(3) 服务部(**service**)：部门经理为 **s01-sandy**，部门员工包括 **s01-s1**、**s01-s2**，**s01-s3**、**s01-s4**，他们都属于组 **s01-service**，组管理员为 **s01-service**。

(4) 财务部(**finance**)：部门经理为 **s01-frank**，部门员工包括 **s01-f1**、**s01-f2**，**s01-f3**、**s01-f4**，他们都属于组 **s01-finance**，组管理员为 **s01-finance**。

(5) 各部门经理均属于 **s01-managers** 组

假设公司新承接了一个项目，项目编号为 **prj01**，需要为该项目成立一个新项目组 **group01**，假设该项目组从各部门抽调如下员工参与该项目并加入组 **group01**：

技术部：**s01-t1**、**s01-t2**

市场部：**s01-m1**

服务部：**s01-s1**

财务部：**s01-f1**

现在指派 **s01-t2** 为 **prj01** 的项目负责人兼 **group01** 组的组管理员，由他负责该组的管理。指定目录/**Prj01** 专门用于存放 **prj01** 项目的相关资料，该目录属于 **root** 用户和 **group01** 组，权限为 **770**，并要求所有在该目录中创建的文件和目录自动属于 **group01** 组，目录中创建一个项目合同文件 **contract01**，要求任何人不得更改、删除、移动该文件，还要创建一个 **prj01.log** 文件用于记录项目日志，要求该文件只能从尾部添加内容。另外要求允许总裁 **s01-carl** 对该目录中的文件具有读写权限，而属于 **s01-managers** 组的各部门经理均对该目录中的文件具有只读权限。

(1) 请根据以上描述，以适当身份合理添加用户、组、目录、文件并设置相应的权限，请把设置过程截图。

1、使用 **root** 用户批量创建公司用户

```

CREATE_MAIL_SPOOL=no
root@s13-virtual-machine:~# vim userfile.txt
root@s13-virtual-machine:~# cat userfile.txt
s13-carl:x:2002:2002::/home/s13-carl:/bin/bash
s13-tech:x:2003:2003::/home/s13-tech:/bin/bash
s13-tony:x:2004:2004::/home/s13-tony:/bin/bash
s13-t1:x:2005:2005::/home/s13-t1:/bin/bash
s13-t2:x:2006:2006::/home/s13-t2:/bin/bash
s13-t3:x:2007:2007::/home/s13-t3:/bin/bash
s13-t4:x:2008:2008::/home/s13-t4:/bin/bash
s13-market:x:2009:2009::/home/s13-market:/bin/bash
s13-mary:x:2010:2010::/home/s13-mary:/bin/bash
s13-m1:x:2011:2011::/home/s13-m1:/bin/bash
s13-m2:x:2012:2012::/home/s13-m2:/bin/bash
s13-m3:x:2013:2013::/home/s13-m3:/bin/bash
s13-m4:x:2014:2014::/home/s13-m4:/bin/bash
s13-service:x:2015:2015::/home/s13-service:/bin/bash
s13-sandy:x:2016:2016::/home/s13-sandy:/bin/bash
s13-s1:x:2017:2017::/home/s13-s1:/bin/bash
s13-s2:x:2018:2018::/home/s13-s2:/bin/bash
s13-s3:x:2019:2019::/home/s13-s3:/bin/bash
s13-s4:x:2020:2020::/home/s13-s4:/bin/bash
s13-finance:x:2021:2021::/home/s13-finance:/bin/bash
s13-f1:x:2022:2022::/home/s13-f1:/bin/bash
s13-f2:x:2023:2023::/home/s13-f2:/bin/bash
s13-f3:x:2024:2024::/home/s13-f3:/bin/bash
s13-f4:x:2025:2025::/home/s13-f4:/bin/bash
s13-frank:x:2026:2026::/home/s13-frank:/bin/bash
root@s13-virtual-machine:~#

```

```

s13-frank:x:2026:2026::/home/s13-frank:/bin/bash
root@s13-virtual-machine:~# newusers userfile.txt
root@s13-virtual-machine:~#

```

2、设置各个部门管理员，建立经理组并添加经理

```

root@s13-virtual-machine:/home/s13-tech# cd
root@s13-virtual-machine:~# gpasswd -A s13-tech s13-tech
root@s13-virtual-machine:~# gpasswd -A s13-market s13-market
root@s13-virtual-machine:~# gpasswd -A s13-service s13-service
root@s13-virtual-machine:~# gpasswd -A s13-finance s13-finance
root@s13-virtual-machine:~#

```

```

zhong...
root@s13-virtual-machine:~# groupadd s13-managers
root@s13-virtual-machine:~# gpasswd -M s13-tony,s13-service,s13-market,s13-frank s13-managers
root@s13-virtual-machine:~#

```

3、切换到各部门管理员用户并将组成员和经理添加至部门

技术部(tech)

```

root@s13-virtual-machine:~# su s13-tech
s13-tech@s13-virtual-machine:/root$ cd
s13-tech@s13-virtual-machine:~$ gpasswd -a s13-tony s13-tech
正在将用户"s13-tony"加入到"s13-tech"组中
s13-tech@s13-virtual-machine:~$ gpasswd -a s13-t1 s13-tech
正在将用户"s13-t1"加入到"s13-tech"组中
s13-tech@s13-virtual-machine:~$ gpasswd -a s13-t2 s13-tech
正在将用户"s13-t2"加入到"s13-tech"组中
s13-tech@s13-virtual-machine:~$ gpasswd -a s13-t3 s13-tech
正在将用户"s13-t3"加入到"s13-tech"组中
s13-tech@s13-virtual-machine:~$ gpasswd -a s13-t4 s13-tech
正在将用户"s13-t4"加入到"s13-tech"组中

```

市场部(market)

```
s13-tech@s13-virtual-machine:~$ su s13-market
密码:
s13-market@s13-virtual-machine:/home/s13-tech$ cd
s13-market@s13-virtual-machine:~$ gpasswd -a s13-mary s13-market
正在将用户"s13-mary"加入到"s13-market"组中
s13-market@s13-virtual-machine:~$ gpasswd -a s13-m1 s13-market
正在将用户"s13-m1"加入到"s13-market"组中
s13-market@s13-virtual-machine:~$ gpasswd -a s13-m2 s13-market
正在将用户"s13-m2"加入到"s13-market"组中
s13-market@s13-virtual-machine:~$ gpasswd -a s13-m3 s13-market
正在将用户"s13-m3"加入到"s13-market"组中
s13-market@s13-virtual-machine:~$ gpasswd -a s13-m4 s13-market
正在将用户"s13-m4"加入到"s13-market"组中
s13-market@s13-virtual-machine:~$
```

服务部(service)

```
s13-market@s13-virtual-machine:~$ su s13-service
密码:
s13-service@s13-virtual-machine:/home/s13-market$ cd
s13-service@s13-virtual-machine:~$ gpasswd -a s13-sandy s13-service
正在将用户"s13-sandy"加入到"s13-service"组中
s13-service@s13-virtual-machine:~$ gpasswd -a s13-s1 s13-service
正在将用户"s13-s1"加入到"s13-service"组中
s13-service@s13-virtual-machine:~$ gpasswd -a s13-s2 s13-service
正在将用户"s13-s2"加入到"s13-service"组中
s13-service@s13-virtual-machine:~$ gpasswd -a s13-s3 s13-service
正在将用户"s13-s3"加入到"s13-service"组中
s13-service@s13-virtual-machine:~$ gpasswd -a s13-s4 s13-service
正在将用户"s13-s4"加入到"s13-service"组中
s13-service@s13-virtual-machine:~$
```

财务部(finance)

```
s13-service@s13-virtual-machine:~$ su s13-finance
密码:
s13-finance@s13-virtual-machine:/home/s13-service$ cd
s13-finance@s13-virtual-machine:~$ gpasswd -a s13-frank s13-finance
正在将用户"s13-frank"加入到"s13-finance"组中
s13-finance@s13-virtual-machine:~$ gpasswd -a s13-f1 s13-finance
正在将用户"s13-f1"加入到"s13-finance"组中
s13-finance@s13-virtual-machine:~$ gpasswd -a s13-f2 s13-finance
正在将用户"s13-f2"加入到"s13-finance"组中
s13-finance@s13-virtual-machine:~$ gpasswd -a s13-f3 s13-finance
正在将用户"s13-f3"加入到"s13-finance"组中
s13-finance@s13-virtual-machine:~$ gpasswd -a s13-f4 s13-finance
正在将用户"s13-f4"加入到"s13-finance"组中
s13-finance@s13-virtual-machine:~$
```

4、建立项目组 group1，设置管理员和成员

```
root@s13-virtual-machine:~# groupadd group01
root@s13-virtual-machine:~# gpasswd -M s13-t1,s13-s1,s13-m1,s13-f1 group01
root@s13-virtual-machine:~# gpasswd -A s13-t2 group01
root@s13-virtual-machine:~#
```

5、建立 prj01 目录，设置目录所有者和属组以及 770 权限，为该目录设置特殊权限 sgid

```
root@s13-virtual-machine:~# mkdir Prj01
root@s13-virtual-machine:~# chown root:group01 Prj01
root@s13-virtual-machine:~# chmod 770 Prj01
root@s13-virtual-machine:~# chmod g+s Prj01
root@s13-virtual-machine:~#
```

6、创建 contract01 文件，给文件增加保护（任何人不得更改、删除、移动该文件）

```

root@s13-virtual-machine:~/Prj01# touch contract01
root@s13-virtual-machine:~/Prj01# chatter +i contract01
root@s13-virtual-machine:~/Prj01# lsattr contract01
----i-----e----- contract01
root@s13-virtual-machine:~/Prj01# echo "222222">contract01
bash: contract01: 不允许的操作
root@s13-virtual-machine:~/Prj01#

```

7、创建 prj01.log 文件，设置只能从尾部添加

```

root@s13-virtual-machine:~/Prj01# touch prj01.log
root@s13-virtual-machine:~/Prj01# chatter +a prj01.log
root@s13-virtual-machine:~/Prj01# lsattr prj01.log
-----a-----e----- prj01.log
root@s13-virtual-machine:~/Prj01#

```

8、总裁 s01-carl 对该目录中的文件具有读写权限，而属于 s01-managers 组的各部门经理均对该目录中的文件具有只读权限

```

root@s13-virtual-machine:~# setfacl -m g:s13-managers:x Prj01
root@s13-virtual-machine:~# setfacl -m u:s13-carl:x Prj01
root@s13-virtual-machine:~#

root@s13-virtual-machine:~# setfacl -m d:g:s13-managers:rw Prj01
root@s13-virtual-machine:~# setfacl -m d:u:s13-carl:rw Prj01
root@s13-virtual-machine:~# setfacl -m d:g:s13-managers:r Prj01
root@s13-virtual-machine:~#

```

(2) 请分别以项目组成员、公司总裁、部门经理、其他员工身份进行访问测试并截图。

新建测试文件 text.txt

1、项目中成员用户可读写

```

s13-t1@s13-virtual-machine:~$ cat /root/Prj01/text.txt
add
s13-t1@s13-virtual-machine:~$ echo "update"> /root/Prj01/text.txt
s13-t1@s13-virtual-machine:~$ cat /root/Prj01/text.txt
update
s13-t1@s13-virtual-machine:~$

```

2、公司总裁可读写

```

s13-carl@s13-virtual-machine:~$ cat /root/Prj01/text.txt
update
s13-carl@s13-virtual-machine:~$ echo carl1 >>/root/Prj01/text.txt
s13-carl@s13-virtual-machine:~$ cat /root/Prj01/text.txt
update
carl1
s13-carl@s13-virtual-machine:~$

```

3、部门经理只可读


```
s13-tony@s13-virtual-machine:~/none/s13-carl$ cd /root/Prj01/
s13-tony@s13-virtual-machine:~$ cat /root/Prj01/text.txt
update
carl1
s13-tony@s13-virtual-machine:~$ echo tony >> /root/Prj01/text.txt
bash: /root/Prj01/text.txt: 权限不够
s13-tony@s13-virtual-machine:~$
```

4、其他员工不可读不可写

```
s13-t3@s13-virtual-machine:~$ cat /root/Prj01/text.txt
cat: /root/Prj01/text.txt: 权限不够
s13-t3@s13-virtual-machine:~$ echo other >> /root/Prj01/text.txt
bash: /root/Prj01/text.txt: 权限不够
s13-t3@s13-virtual-machine:~$
```