

实验 08 用户和权限管理

班级：20 级数据科学与大数据技术 2 班

学号：202026203039

姓名：赖丽婷

用户名：llt

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，比如修改了哪些文件、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(除密码外)

```
llt:x:1000:1000:llt,,,:/home/llt:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:./usr/sbin/
sshd:x:126:65534:./run/sshd:usr/sbin/nologin
llt-myuser:X:2001:2001:./home/llt-myuser:/bin/bash
"/etc/passwd" 481 28206

llt@llt-virtual-machine:~/桌面$ perl -e 'print crypt("123", "\$6\$sdfhkfjh\$") . "\n"'
$6$sdfhkfjh$P11naAAeRxLEkP1XUZndZo8cBXpTUj0H1i7FYuG4Rr/YtpSdtp.S5Gq19y3fCL/9Jiq
YIzDPbL.98NOhgRqC0.
llt@llt-virtual-machine:~/桌面$

sshd:*:19245:0:99999:7:::
llt-myuser:$6$sdfhkfjh$P11naAAeRxLEkP1XUZndZo8cBXpTUj0H1i7FYuG4Rr/YtpSdtp.S5Gq1
9y3fCL/9JiqYIzDPbL.98NOhgRqC0.:19246:0:99999:7:::
插入 48 129 底端
```

(2) 请测试以手工创建的新用户登录，并截图。

```

root@llt-virtual-machine:/home/llt/桌面# mkdir /home/llt-myuser
root@llt-virtual-machine:/home/llt/桌面# cp /etc/skel/.bash* /home/llt-myuser/
cp: 无法获取 '/etc/skel/.bash*' 的文件状态(stat): 没有那个文件或目录
root@llt-virtual-machine:/home/llt/桌面# cp /etc/skel/.bash* /home/llt-myuser/
root@llt-virtual-machine:/home/llt/桌面# chown -R llt-myuser:llt-myuser /home/m
yuser/
chown: 无法访问 '/home/myuser/': 没有那个文件或目录
root@llt-virtual-machine:/home/llt/桌面# chown -R llt-myuser:llt-myuser /home/l
lt-myuser/
root@llt-virtual-machine:/home/llt/桌面# su llt-myuser
llt-myuser@llt-virtual-machine:/home/llt/桌面$ cd
bash: cd: /home/llt-myuser: 没有那个文件或目录
llt-myuser@llt-virtual-machine:/home/llt/桌面$ cd
bash: cd: /home/llt-myuser: 没有那个文件或目录
llt-myuser@llt-virtual-machine:/home/llt/桌面$ pwd
/home/llt/桌面
llt-myuser@llt-virtual-machine:/home/llt/桌面$ id
uid=2001(llt-myuser) gid=2001(llt-myuser) 组=2001(llt-myuser)
llt-myuser@llt-virtual-machine:/home/llt/桌面$

```

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。

使用 **root** 用户批量创建用户

```
root@llt-virtual-machine:/home/llt/8# newusers user.txt
```

设置各个部门管理员，建立经理组并添加经理

```

root@llt-virtual-machine:~# gpasswd -A llt-tech llt-tech
root@llt-virtual-machine:~# gpasswd -A llt-market llt-market
root@llt-virtual-machine:~# gpasswd -A llt-service llt-service
root@llt-virtual-machine:~# gpasswd -A llt-finance llt-finance
root@llt-virtual-machine:~# groupadd llt-managers
root@llt-virtual-machine:~# gpasswd -M llt-tony,ltt-service,ltt-market,ltt-fran
k llt-managers

```

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**)


```
llt-tech@llt-virtual-machine:~$ gpasswd -a llt-tyon llt-tech
正在将用户“llt-tyon”加入到“llt-tech”组中
llt-tech@llt-virtual-machine:~$ gpasswd -a llt-t1 llt-tech
正在将用户“llt-t1”加入到“llt-tech”组中
llt-tech@llt-virtual-machine:~$ gpasswd -a llt-t2 llt-tech
正在将用户“llt-t2”加入到“llt-tech”组中
llt-tech@llt-virtual-machine:~$ gpasswd -a llt-t3 llt-tech
正在将用户“llt-t3”加入到“llt-tech”组中
llt-tech@llt-virtual-machine:~$ gpasswd -a llt-t4 llt-tech
正在将用户“llt-t4”加入到“llt-tech”组中
llt-tech@llt-virtual-machine:~$
```

市场部(market)

```
root@llt-virtual-machine:/home/llt-tech# su llt-market
llt-market@llt-virtual-machine:/home/llt-tech$ cd
llt-market@llt-virtual-machine:~$ gpasswd -a llt-mary llt-market
正在将用户“llt-mary”加入到“llt-market”组中
llt-market@llt-virtual-machine:~$ gpasswd -a llt-m1 llt-market
正在将用户“llt-m1”加入到“llt-market”组中
llt-market@llt-virtual-machine:~$ gpasswd -a llt-m2 llt-market
正在将用户“llt-m2”加入到“llt-market”组中
llt-market@llt-virtual-machine:~$ gpasswd -a llt-m3 llt-market
正在将用户“llt-m3”加入到“llt-market”组中
llt-market@llt-virtual-machine:~$ gpasswd -a llt-m4 llt-market
正在将用户“llt-m4”加入到“llt-market”组中
llt-market@llt-virtual-machine:~$
```

服务部(service)

```
root@llt-virtual-machine:/home/llt-market# su llt-service
llt-service@llt-virtual-machine:/home/llt-market$ cd
llt-service@llt-virtual-machine:~$ gpasswd -a llt-sandy llt-service
正在将用户“llt-sandy”加入到“llt-service”组中
llt-service@llt-virtual-machine:~$ gpasswd -a llt-s1 llt-service
正在将用户“llt-s1”加入到“llt-service”组中
llt-service@llt-virtual-machine:~$ gpasswd -a llt-s2 llt-service
正在将用户“llt-s2”加入到“llt-service”组中
llt-service@llt-virtual-machine:~$ gpasswd -a llt-s3 llt-service
正在将用户“llt-s3”加入到“llt-service”组中
llt-service@llt-virtual-machine:~$ gpasswd -a llt-s4 llt-service
正在将用户“llt-s4”加入到“llt-service”组中
llt-service@llt-virtual-machine:~$
```

财务部(finance)

```
root@llt-virtual-machine:/home/llt-service# su llt-finance
llt-finance@llt-virtual-machine:/home/llt-service$ cd
llt-finance@llt-virtual-machine:~$ gpasswd -a llt-frank llt-finance
正在将用户“llt-frank”加入到“llt-finance”组中
llt-finance@llt-virtual-machine:~$ gpasswd -a llt-f1 llt-finance
正在将用户“llt-f1”加入到“llt-finance”组中
llt-finance@llt-virtual-machine:~$ gpasswd -a llt-f2 llt-finance
正在将用户“llt-f2”加入到“llt-finance”组中
llt-finance@llt-virtual-machine:~$ gpasswd -a llt-f3 llt-finance
正在将用户“llt-f3”加入到“llt-finance”组中
llt-finance@llt-virtual-machine:~$ gpasswd -a llt-f4 llt-finance
正在将用户“llt-f4”加入到“llt-finance”组中
llt-finance@llt-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。

建立项目组 group1, 设置管理员和成员

```
root@llt-virtual-machine:/home/llt-finance# groupadd group01
root@llt-virtual-machine:/home/llt-finance# gpasswd -A llt-t2 group01
root@llt-virtual-machine:/home/llt-finance# gpasswd -M llt-t1,llt-s1,llt-m1,llt-f1 group01
root@llt-virtual-machine:/home/llt-finance#
```

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

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@llt-virtual-machine:~# cd Prj01
root@llt-virtual-machine:~/Prj01# touch contract01
root@llt-virtual-machine:~/Prj01# chattr +i contract01
root@llt-virtual-machine:~/Prj01# lsattr contract01
----i-----e----- contract01
root@llt-virtual-machine:~/Prj01# echo "11">contract01
bash: contract01: 不允许的操作
root@llt-virtual-machine:~/Prj01#

```

创建 prj01.log 文件，设置只能从尾部添加

```

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

```

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@llt-virtual-machine:~# setfacl -m g:llt-managers:x Prj01
root@llt-virtual-machine:~# setfacl -m u:llt-carl:x Prj01
root@llt-virtual-machine:~# setfacl -m d:u:llt-carl:rw Prj01
root@llt-virtual-machine:~# setfacl -m d:u:llt-managers:r Prj01
setfacl: 选项 -m: 无效的参数 靠近字符 s
root@llt-virtual-machine:~# setfacl -m d:g:llt-managers:r Prj01

```

新建测试文件 project.txt

公司总裁可读写

```

root@llt-virtual-machine:~/Prj01# su llt-carl
llt-carl@llt-virtual-machine:/root/Prj01$ cat project.txt
test
llt-carl@llt-virtual-machine:/root/Prj01$ echo 'carl'>project.txt

```

部门经理只可读

```

root@llt-virtual-machine:~/Prj01# su llt-tony
llt-tony@llt-virtual-machine:/root/Prj01$ cat project.txt
test
llt-tony@llt-virtual-machine:/root/Prj01$ echo 'carl' > project.txt
bash: project.txt: 权限不够
llt-tony@llt-virtual-machine:/root/Prj01$

```

其他员工不可读不可写

```

root@llt-virtual-machine:~/Prj01# su llt-f3
llt-f3@llt-virtual-machine:/root/Prj01$ cat project.txt
cat: project.txt: 权限不够
llt-f3@llt-virtual-machine:/root/Prj01$ echo 'carl' > project.txt
bash: project.txt: 权限不够
llt-f3@llt-virtual-machine:/root/Prj01$

```