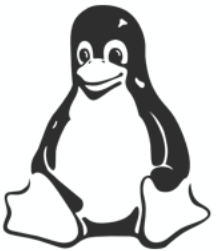


Linux系统管理

南通师范高等专科学校 朱亚林

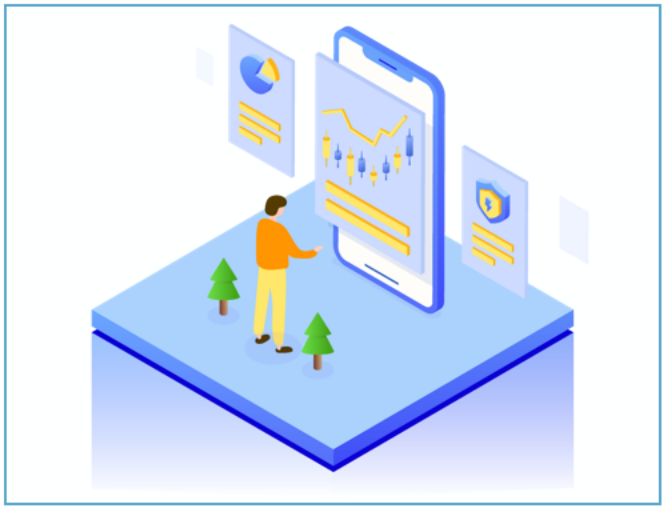
本章导言

- Linux操作系统以高安全性著称。其中有一个显著特点就是：Linux操作系统通过对用户的分类很好地限制了“root”权限，对各类文件加上权限很好地保护了文件的安全。从而让别人不可能随意动得了你的“奶酪”。Linux操作系统的众多用户犹如微信中的用户，每位用户都可以根据实际情况为自己定制一个开放共享的准则，或是朋友圈或是工作群，而这个准则就是权限。
- 本章内容，就将详细介绍Linux操作系统中用户的管理和文件权限的管理。

第5章

朋友圈：用户、群组和权限

5.1 用户



Linux将用户分为以下几类：

- 系统管理员（root）
- 系统用户
- 普通用户

其中系统管理员和普通用户是可以登录的，而系统用户只是具有一些特殊的意义，不具备登录权限。一般而言，普通用户的账户包括了用户名、密码、所属用户组、主目录等信息。

5.1 用户

- 在Linux中，管理员（具备管理员权限的用户）可以添加用户、修改用户设置、删除用户、添加用户组以及删除用户组。修改用户设置又包括了修改用户的组信息、附加组、用户的shell类型、用户的密码等信息。
- 对于系统中已经存在的用户，可以查看/etc/passwd文档。

5.1 用户

- 案例：查看系统中的用户情况

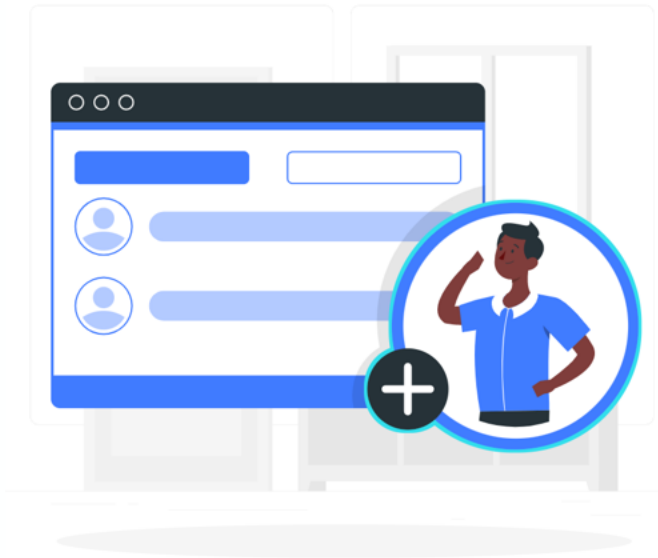
```
zz@zz-lab:~$ cat /etc/passwd | tail -5
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
zz:x:1000:1000:zz,,,:/home/zz:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
```

- 红框内显示的就是当前用户的相关信息。这一条记录包含了7个组成部分，用6个“:”分隔开来。
- 其中第1段表示用户名，第2段表示密码，第3段表示uid（用户编号），第4段表示gid（群组编号），第5段表示描述信息，第6段表示用户的主目录，第7段表示登录时使用的shell。

5.1.1 添加用户

- Linux中提供了useradd命令来为系统增加新的用户
- useradd命令的一般格式如下：

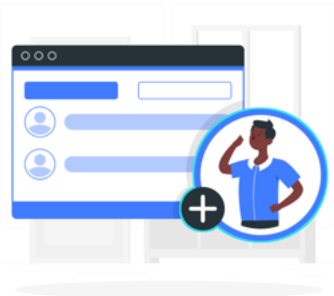
```
useradd [选项] 用户名
```



5.1.1 添加用户

- useradd的常用选项如下表所示

选项	作用
-c comment	用户password文件的说明，可任意设置
-d home_dir	设置用户每次登入系统时所使用的主目录，默认为/home/用户名
-e expire_date	设置用户账号的过期日期。格式为MM/DD/YY
-f inactive_days	设置用户账号过期几日后永久停用
-g inital_group	设置用户的初始组。一般以和用户名相同的组作为用户的初始组，在创建用户时会默认建立初始组。一旦手动指定，则系统将不会在创建此默认的初始组目录。
-G group	指定用户的附加组,当把用户加入其他组，一般都使用附加组
-m	如果用户目录不存在，则自动创建
-M	不创建用户目录
-r	创建供系统程序使用的用户（UID 在 1~499 之间），由于系统用户主要用于运行系统所需服务的权限配置，因此系统用户的创建默认不会创建主目录。
-s	指定用户账户登录时使用的shell解释器



5.1.1 添加用户

案例：新建用户newbie

1. 创建用户

2. 设置密码

```
zz@zz-lab:~$ sudo useradd newbie
[sudo] password for zz:
zz@zz-lab:~$ id newbie
uid=1001(newbie) gid=1001(newbie) groups=1001(newbie)
zz@zz-lab:~$ sudo passwd newbie
New password:
Retype new password:
passwd: password updated successfully
```

5.1.1 添加用户

案例：

新建用户newuser，使其组名为newbie，主目录为/home/n-user，同时新用户也是root和bin的成员，shell使用zsh

```
zz@zz-lab:~$ sudo useradd -g newbie -d /home/n-user -G root,bin -s /bin/zsh newuser
```

```
zz@zz-lab:~$ sudo cat /etc/group
root:x:0:newuser
daemon:x:1:
bin:x:2:newuser
```

5.1.1 添加用户

案例：

创建一个普通用户test，设置用户账户过期时间为当前日期的三个月后

```
zz@zz-lab:~$ date
Mon 28 Mar 2022 08:59:24 AM CST
zz@zz-lab:~$ sudo useradd -e 06/28/2022 test
```

5.1.1 添加用户

- 另一个添加用户的脚本命令：adduser

5.1.2 密码管理

- 在Linux中，密码是系统安全的第一道大门。管理员拥有对所有用户密码管理的权限，普通用户一般可以对自己的密码进行管理。
- Linux中密码管理的命令是passwd，其基本格式如下：

```
passwd [选项] [用户名]
```

5.1.2 密码管理

- passwd常用选项如下表所示

选项	作用
-d	删除密码
-f	强制用户下次登录时必须修改密码
-w	口令到期前的警告天数
-l	锁定账户，禁止登录
-S	显示密码信息（是否被锁定，加密算法等）
-u	启用被停止的账户

5.1.2 密码管理

案例：使用passwd对用户newuser进行操作

- 修改newuser登录密码
- 查看账户密码信息
- 查看登录情况
- 尝试锁定账户后再次登录
- 解锁账户后再次登录

```
zz@zz-lab:~$ sudo passwd newuser
New password:
Retype new password:
passwd: password updated successfully
zz@zz-lab:~$ sudo passwd -S newuser
newuser P 03/28/2022 0 99999 7 -1
zz@zz-lab:~$ sudo passwd -l newuser
passwd: password expiry information changed.
zz@zz-lab:~$ sudo passwd -u newuser
passwd: password expiry information changed.
```

5.1.3 修改用户账户

- usermod命令根据命令选项修改系统中指定用户账号文件里的信息。
- usermod命令的一般格式如下：

```
usermod [选项] 用户名
```

5.1.3 修改用户账户

- usermod常用选项如下表所示

选项	作用
-m，-d	参数-m与-d连用，可重新指定用户的主目录，并将其中数据进行整体转移
-e	修改账户过期日期，格式为MM/DD/YY或YYYY-MM-DD
-g	修改账户的主组群
-G	修改账户所属的附属组群，多个组群以逗号分隔
-l n_name	将用户账号修改为n_name，主目录也会修改。其他属性不变。
-L	锁定用户，禁止登录
-U	解锁用户，允许登录
-s	修改用户使用的shell解释器
-u	修改账户的UID

5.1.3 修改用户账户

案例：用户信息的修改

- 将newbie用户的shell修改成了zsh
- 将newbie用户的主目录修改为/home/newbie-home，同时将主目录所有的内容都进行了迁移
- 修改newuser的用户名为newuser001

```
zz@zz-lab:~$ sudo usermod -s /bin/zsh newbie
zz@zz-lab:~$ sudo usermod -d /home/newbie-home -m newbie
```

5.1.4 删除用户账户

- 可以使用userdel命令删除现有用户。此项操作一定要谨慎，一旦删除一般情况下无法恢复。
- userdel命令的一般格式是：

```
userdel [选项] [用户账号]
```

5.1.4 删除用户账户

- userdel常用选项如下表所示

选项	作用
-r	在删除账号的同时，将该用户主目录中的文件一同删除
-f	即使用户账号处于登录状态，也要强制删除

5.1.4 删除用户账户

- 案例：删除newuser账号及主目录中文件

```
zz@zz-lab:~$ sudo userdel -r newuser
userdel: newuser mail spool (/var/mail/newuser) not found
userdel: newuser home directory (/home/n-user) not found
```

5.2 群组

- Linux系统中，每个用户都一定隶属于至少一个群组。
- 系统可以对一个用户组中的所有用户进行集中管理。
- 当一个新用户被创建时，系统中自动为该用户创建一个同名的群组。
- 每一个群组都有一个group 标识符（号码），即gid。
- 所有的群组信息都存放在/etc/group 文件中。

5.2 群组

案例：查看群组信息

```
zz@zz-lab:~$ tail -5 /etc/group
messagebus:x:110:
ssh:x:111:
newbie:x:1001:
nu:x:1003:
test:x:1004:
```

以屏幕输出newbie:x:1001: 这行为例，用户群组信息由4个部分组成。第一部分是群组名，第二部分是群组密码，第三部分是群组编号，第四部分是当前群组的其他成员。作一个解读即是当前群组名为是newbie，密码不可见，群组编号（gid）是1001，这个群组中暂无其他用户。

5.2.1 添加用户群组

- 添加用户群组的命令是groupadd，它的基本格式如下

```
groupadd [选项] 用户群组名
```

选项	作用
-g	指定新建工作组的 id；
-r	创建系统工作组，系统工作组的组ID小于 500；

5.2.1 添加用户群组

案例：使用groupadd添加新的用户群组

1. 用默认的方式添加群组test1
2. 创建新的群组test2，指定gid为1020
3. 将用户newbie加入群组test1
4. 查看新创建的群组情况

```
zz@zz-lab:~$ sudo groupadd test1
[sudo] password for zz:
zz@zz-lab:~$ sudo groupadd -g 1020 test2
zz@zz-lab:~$ sudo usermod -G test1 newbie
zz@zz-lab:~$ tail -2 /etc/group
test1:x:1005:newbie
test2:x:1020:
```

5.2.2 修改群组属性

- groupmod命令用于更改群组编号或者名称。
- groudmod命令的格式如下:

```
groupmod [选项] 群组名
```

选项	作用
-g	修改用户群组的gid号
-n	修改用户群组的组名

5.2.2 修改群组属性

案例：使用groupmod修改群组信息

1. 修改test2群组的gid为1089

2. 修改test1群组名称为test3

```
zz@zz-lab:~$ sudo groupmod -g 1089 test2
zz@zz-lab:~$ sudo groupmod -n test3 test1
```

5.2.3 删除用户群组

- groupdel命令用于删除群组。如果需要被删除的群组中仍包括某些用户，则必须先删除这些用户后，方能删除群组。
- groupdel命令的格式如下：

```
groupdel  群组名
```

5.2.3 删除用户群组

案例：使用groupdel删除群组test3

```
zz@zz-lab:~$ sudo groupdel test3
zz@zz-lab:~$
```

5.2.4 进群与出群

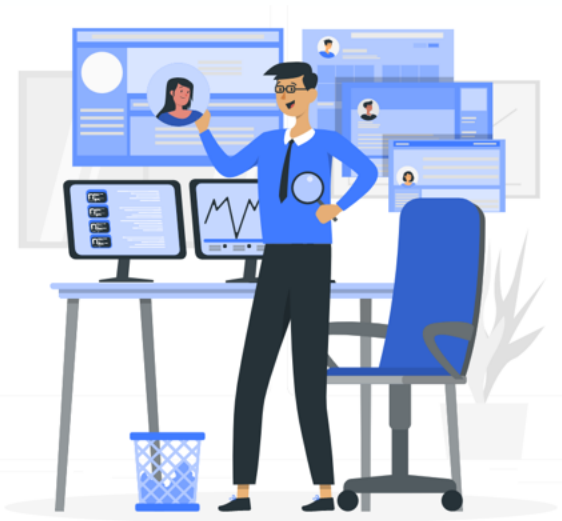
- Linux中用户与群组之间的关系有点类似微信群。一个用户可以在一个群，也可以在多个群，不同的群有着不同的功能。那么，在Linux系统中如何设置“群管理员”，以及“拉用户进群”或者“踢用户出群”呢?
- gpasswd命令是Linux系统中群组设置文件/etc/group和/etc/gshadow的管理工具，专门用于管理用户群组。

```
gpasswd [选项] 组名
```

5.2.4 进群与出群

- gpasswd常用选项如下表所示

选项	作用
-a	添加用户到组；
-d	从组删除用户；
-A	指定管理员；
-M	指定组成员和-A的用途差不多；
-r	删除密码；
-R	限制用户登入组，只有组中的成员才可以用newgrp加入该组。



5.2.4 进群与出群

案例：使用gpasswd进行群组管理

1. 创建一个新的群组linuxStudy
2. 将用户newbie加入linuxStudy群组
3. 将用户newbie设置成linuxStudy群组的管理员
4. 将用户newbie从linuxStudy群组中移除

```
zz@zz-lab:~$ sudo groupadd linuxStudy
[sudo] password for zz:
zz@zz-lab:~$ sudo gpasswd -a newbie linuxStudy
Adding user newbie to group linuxStudy
zz@zz-lab:~$ sudo gpasswd -A newbie linuxStudy
zz@zz-lab:~$ sudo gpasswd -d newbie linuxStudy
Removing user newbie from group linuxStudy
zz@zz-lab:~$
```

5.3 权限

- 在微信的朋友圈中，可以为不同的好友设置不同的访问权限。有的仅限聊天，有的不看对方日常，有的不让对方看日常，有的可以互相看日常。在Linux操作系统中，各个文件也都有着相似的权限。有的文件只能自己编辑访问，有的文件别人可以看但不能编辑，有的文件别人可看可编辑……

5.3.1 认识权限

- 当使用ls命令加上-l选项时，被查询目录中所有的对象都会以列表的形式进行陈列，在每一项文件或者目录最前面，会有一串10个字符组成的字符串。如下图所示

```
zz@debian:~$ ls -l
total 20
drwxr-xr-x 2 zz zz 4096 Jan 17 21:25 Documents
drwxr-xr-x 2 zz zz 4096 Jan 17 21:29 Downloads
drwxr-xr-x 2 zz zz 4096 Jan 17 21:05 LinuxStudy
drwxr-xr-x 2 zz zz 4096 Jan 17 21:29 Music
-rw-r--r-- 1 zz zz    0 Jan 19 09:31 run.sh
drwxr-xr-x 2 zz zz 4096 Jan 17 21:30 Videos
```

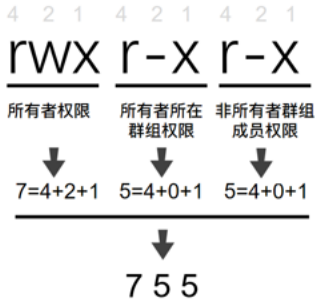
5.3.1 认识权限

案例：用户权限的演示

1. 通过终端登录当前系统中已有的两个用户（zz和newbie）
2. 使用zz账户查看其主目录下各文件、目录的权限
3. 使用newbie账户进入到/home目录中，并查看该目录下相关文件及目录的权限
4. 使用newbie账户进入到zz目录中，查看目录内容情况，并尝试在该目录下建立一个空文件“Test”

5.3.2 权限的数字表示法

- Linux操作系统通过对文件赋予权限增强了其安全性。文件权限的表示方法除了上节中提到了“rwx”表示方法之外，还有一种数字表示法。
- 在数字表示法中，“r”对应着数值4，“w”对应着数值2，“x”对应着数值1。权限可用，则对应相应数字，不然就对应0。



5.3.3 权限的修改

系统会在文件和目录的创建之初赋予它们初始权限，但这些权限并不是一尘不变的。很多时候，同一台服务器上的用户间也需要进行文件共享的授权。此时，就可以有两种思路来进行设置。

1. 目录的所有者（或者管理员）对Share这个目录进行授权，将目录权限“rwxr-xr-x”（755）设置成同一组的其他人甚至所有人可读可写可执行，即“rwxrwxrwx”（777）。
2. 作为Share目录的所有者（或者管理员）将Share目录的归属权（所有者或者所属于群组）进行转让，让指定对象和群组获得权限，当然此时自己就有可能失去权限。

5.3.3 权限的修改

修改权限——chmod

使用字母表示权限

chmod [选项] 模式 文件

对象	赋予/取消	权限
[ugoa]	[+-=]	[rwx]

模式中包含着表示权限设置的字符串，一般由以下部分组成：

1. 这里的u表示该文件的拥有者，g表示与该文件的拥有者属于同一个群体(group)者，o表示其他以外（other）的人，a 表示这三者皆是（all）；
2. +表示增加权限，-表示取消权限，=表示唯一设定权限；
3. r表示可读取，w表示可写入，x表示可执行。

5.3.3 权限的修改

修改权限——chmod

使用数字表示权限

```
chmod [选项] 数值 文件
```

这种方式相对简单，只需要将所有者、群组、其他人分别对应权限的数值放在一起就可以了，如777、755、744等等

5.3.3 权限的修改

- chmod的常用选项如下表所示

选项	作用
-c	若该文件权限确实已经更改，才显示其更改动作
-f	若该文件权限无法被更改也不要显示错误讯息
-v	显示权限变更的详细信息
-R	对目前目录下的所有文件与子目录进行相同的权限变更(即以递归的方式逐个变更)

5.3.3 权限的修改

案例：将zz主目录LinuxStudy/chapter-5/Share-1目录设置为newbie可读可写可执行

1. 通过zz登录，检查zz指定目录下是否有Share-1目录，如无则创建
2. 检查newbie账户基本信息
3. 为刚刚建立的Share-1设置相关权限
4. 通过newbie账户进入/home/zz/LinuxStudy/chapter-5/Share-1中尝试建立目录

```
zz@zz-lab:~$ ls LinuxStudy/chapter-5/Sha*
ls: cannot access 'LinuxStudy/chapter-5/Sha*': No such file or directory
zz@zz-lab:~$ id newbie
uid=1001(newbie) gid=1001(newbie) groups=1001(newbie)
zz@zz-lab:~$ mkdir -p LinuxStudy/chapter-5/Share-1
zz@zz-lab:~$ chmod -R  o=rwx  LinuxStudy/chapter-5/Share-1/
zz@zz-lab:~$
```

```
zz-lab% pwd
/home/newbie-home
zz-lab% cd /home/zz/LinuxStudy/chapter-5/Share-1
zz-lab% pwd
/home/zz/LinuxStudy/chapter-5/Share-1
zz-lab% mkdir hello
zz-lab% ls
hello
```

```
zz@zz-lab:~/LinuxStudy/chapter-5/Share-1$ ls -al
total 12
drwxr-xrwx 3 zz     zz     4096 Mar 28 14:53 .
drwxr-xr-x 3 zz     zz     4096 Mar 28 14:47 ..
drwxr-xr-x 2 newbie newbie 4096 Mar 28 14:53 hello
```

5.3.3 权限的修改

修改归属——chown、chgrp

- 所谓修改归属，就是将文件的所有者，或者所归属的相关群组进行调整。
- 同样还是在zz的LinuxStudy/chapter-5目录中建立一个目录Share-2，目标是通过修改归属让newbie可以对该目录拥有可读可写可执行的权限。

5.3.3 权限的修改

修改文件所有者

修改文件所有者的命令是chown。chown命令的一般格式是：

```
chown [选项] 用户名:[群组名] 文件/目录
```

在进行文件归属权限修改时，新的用户名必须存在，新的用户群组名为可选。

chown命令常用的选项如下表所示：

选项	作用
-c	显示更改的部分的信息
-f	忽略错误信息
-v	显示权限变更的详细信息
-R	对目前目录下的所有文件与子目录进行相同的权限变更(即以递归的方式逐个变更)

5.3.3 权限的修改

案例：修改zz主目录LinuxStudy/chapter-5/Share-2目录权限为newbie所有，归属群组一同修改

1. 通过zz登录，检查指定主目录下是否有Share-2目录，如无则创建
2. 检查newbie账户基本信息
3. 设置Share-2的归属
4. 通过newbie账户进入/home/zz/LinuxStudy/chapter-5/Share-2中尝试建立目录

```
zz@zz-lab:~$ ls LinuxStudy/chapter-5/
Share-1
zz@zz-lab:~$ mkdir -p LinuxStudy/chapter-5/Share-2
zz@zz-lab:~$ id newbie
uid=1001(newbie) gid=1001(newbie) groups=1001(newbie)
zz@zz-lab:~$ sudo chown -R newbie:newbie LinuxStudy/chapter-5/Share-2
zz@zz-lab:~$
```

```
zz-lab% cd /home/zz/LinuxStudy/chapter-5/Share-2
zz-lab% mkdir test
zz-lab% ls -l
total 4
drwxr-xr-x 2 newbie newbie 4096 Mar 28 15:44 test
zz-lab% cd ..
zz-lab% ls -l
total 8
drwxr-xrwx 3 zz     zz     4096 Mar 28 14:53 Share-1
drwxr-xr-x 3 newbie newbie 4096 Mar 28 15:44 Share-2
```

5.3.3 权限的修改

修改文件归属群组

- 当zz建立了一个目录，不想更改他对目录的所有权，但是又想让不在同一群组的newbie及newbie同组人员拥有一定的权限，而其他人无权访问，那该如何设置呢？此时，就要考虑使用修改文件归属群组的属性了，可以使用chgrp命令。
- chgrp命令的一般格式如下：

```
chgrp [选项] 群组名 文件/目录
```

5.3.3 权限的修改

修改文件归属群组

- chgrp命令的常用选项如下表所示

选项	作用
-c	显示更改的部分的信息
-f	忽略错误信息
-v	显示权限变更的详细信息
-R	对目前目录下的所有文件与子目录进行相同的权限变更(即以递归的方式逐个变更)

5.3.3 权限的修改

案例：修改zz主目录LinuxStudy/chapter-5/Share-3的归属权限为newbie群组所有，除zz及newbie群组之外，其他人员无限访问

1. 通过zz登录，检查指定目录下是否有Share-3目录，如无则创建
2. 检查newbie账户基本信息
3. 设置Share-3的归属
4. 设置Share-3的权限

```
zz@zz-lab:~$ ls LinuxStudy/chapter-5/
Share-1  Share-2
zz@zz-lab:~$ mkdir -p LinuxStudy/chapter-5/Share-3
zz@zz-lab:~$ id newbie
uid=1001(newbie) gid=1001(newbie) groups=1001(newbie)
zz@zz-lab:~$ sudo chgrp newbie LinuxStudy/chapter-5/Share-3
[sudo] password for zz:
zz@zz-lab:~$ chmod 770 -R LinuxStudy/chapter-5/Share-3
```

```
zz-lab% cd /home/zz/LinuxStudy/chapter-5
zz-lab% ls -l
total 12
drwxr-xrwx 3 zz     zz     4096 Mar 28 14:53 Share-1
drwxr-xr-x 3 newbie newbie 4096 Mar 28 15:44 Share-2
drwxrwx--- 2 zz     newbie 4096 Mar 28 15:56 Share-3
```

本课习题

- 见教学网站