项目 3　管理信息中心的用户与组

学习目标

（1）掌握 openEuler 操作系统中用户与组的概念及应用。

（2）掌握 openEuler 操作系统中用户与组的常用命令。

（3）掌握用户与组权限的继承性概念及应用。

（4）掌握企业组织架构下用户与组的部署业务实施流程。

项目描述

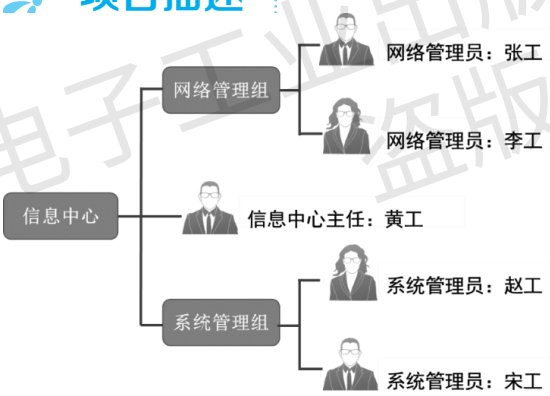

图 3-1　Jan16 公司信息中心的组织架构

Jan16 公司信息中心的组织架构如图 3-1 所示。

Jan16 公司信息中心在一台服务器上安装了 openEuler 操作系统用于部署公司网络服务，信息中心的所有员工均需要使用该服务器。系统管理员根据员工的岗位职责，为每个员工规划相应的权限。信息中心员工的用户账号信息如表 3-1 所示。

表 3-1　信息中心员工的用户账号信息

姓　名	用 户 账 号	隶属自定义组	权　限	备　注
黄工	Huang	Sysadmins	系统管理	信息中心主任
张工	Zhang	Netadmins	网络管理 虚拟化管理	网络管理组
李工	Li			
赵工	Zhao	Sysadmins	系统管理	系统管理组
宋工	Song			

项目分析

Linux 操作系统是多用户多任务系统，系统中的用户对应的用户账号可以是真实物理用户的账号，也可以是特定应用程序使用的身份账号。Linux 操作系统通过定义不同的用户来控制用户在系统中的权限。系统中的每个文件都设计为属于相应的用户与组，定义不同的用户决定了其可以访问、写入或执行系统内的哪些文件。

因此，本项目需要运维工程师熟悉 openEuler 操作系统中的用户与组管理，具体包括以下几个工作任务。

（1）管理信息中心的用户账号。

（2）管理信息中心的组账号。

相关知识

Linux 操作系统是多用户多任务系统，允许多个用户同时登录系统使用系统资源。用户账号是用户的身份标识，用户通过用户账号可以登录系统，并且访问已经被授权的资源。系统依据用户账号来区分属于每个用户的文件、进程、任务，并为每个用户提供特定的工作环境，使每个用户都不能不受干扰地独立工作。

3.1　用户类型

在 Linux 操作系统中，主要有以下 3 种用户类型。

（1）root 用户：在 Linux 操作系统中，root 用户的 UID 为 0，该用户对所有的命令和文件具有访问、修改、执行的权限，一旦操作失误很容易对系统造成损坏，因此在生产环境中，不建议使用 root 用户直接登录系统。

（2）普通用户：系统中的大多数用户为普通用户，需要管理员用户进行创建，该类用户拥有的权限受到一定的限制，一般其仅在自己的主目录下拥有完全控制权限，提升权限需要使用“sudo”命令。

（3）系统用户：系统用户通常用于守护进程或软件，该类用户在安装系统或服务后默认存在，并且在默认情况下，通常不允许通过交互式 Shell 登录系统，但是该类用户方便进行系统管理，对于系统的正常运行是不可或缺的。

3.2 用户配置

Linux 操作系统中用于用户配置的文件主要有 /etc/passwd 和 /etc/shadow。前者用于保存用户的基本信息，后者用于保存用户密码的加密信息及其他相关安全信息，这两个文件是互补的。

/etc/passwd 文件是文本文件，其中包含用户登录的相关信息，每行代表一个用户的信息，该文件对所有用户可读。/etc/passwd 文件的部分输出如下：

```
[root@EulerOS ~]# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
```

上述 /etc/passwd 文件的部分输出对应的完整格式如下：

```
< 用户名 >:< 口令 >:< 用户标识号 >:< 组标识号 >:< 注释 >:< 主目录 >:< 默认 shell>
```

（1）用户名：代表用户账号的字符串。

（2）口令：存储加密后的用户密码，由于 /etc/passwd 文件对所有用户可读，因此基于安全性考虑，将用户密码的加密信息存储在 /etc/shadow 文件中。

（3）用户标识号：每个用户都有唯一的 UID，0 是超级用户 root 的用户标识号，用户的类型和权限定义都是通过 UID 实现的。

（4）组标识号：组的 GID，该字段记录了用户所属的组，对应 /etc/group 文件中的一条记录。

（5）注释：用户的注释信息，可填写与用户相关的信息，该字段可选。

（6）主目录：用户登录系统后默认所在的目录。

（7）默认 shell：用户登录所用的 Shell 类型，默认为 /bin/bash。

/etc/shadow 中文件包含用户密码的加密信息及其他相关安全信息。基于安全性考虑，只有 root 用户才有权限读取 /etc/shadow 文件中的内容，普通用户没有权限查看。/etc/shadow 文件的部分输出如下：

```
[root@EulerOS ~]# cat /etc/shadow
root:$6$6SCTc3Uz3kXN7tQL$a9I6hiw6zMygSGgZvSbCaQUiaZdJEFwYMFQq9ixzcLrNINRDPr-
VI.iFNIyWu.qCgariKDbu6iTl.gxMTxv1x5.::0:99999:7:::
```

上述 /etc/shadow 文件的部分输出对应的完整格式如下：

```
< 用户名 >:< 加密口令 >:< 最后一次修改时间 >:< 最小时间间隔 >:< 最大时间间隔 >:< 警告时间 >:<
密码禁用期 >:< 失效时间 >:< 保留字段 >
```

（1）用户名：代表用户账号的字符串。

（2）加密口令：$ 为分隔符，首先是使用的加密算法，其次是随机数，最后是加密的密码。若该字段是“*”“！”“x”等字符，则对应的用户不能登录系统。

（3）最后一次修改时间：从 1970 年 1 月 1 日算起，到最近一次密码被修改的天数。

（4）最小时间间隔：表示密码最近一次被修改的日期到下次允许被修改的日期之间的最小天数。

（5）最大时间间隔：表示密码最近一次被修改的日期到下次允许被修改的日期之间的最大天数。

（6）警告时间：表示从系统开始警告用户到密码正式失效之间的天数。

（7）密码禁用期：表示密码失效后自动禁用账号的天数。若密码禁用期设置为 -1，则代表账号永不禁用。

（8）失效时间：表示账号的生存期。若失效时间设置为 -1，则表示该账号为启用状态。

（9）保留字段：保留域，用于未来的功能拓展。

3.3　用户组

在 Linux 操作系统中，为了方便运维工程师管理用户，产生了用户组的概念。用户组就是具有相同特征的用户集合体，使用用户组有利于运维工程师按照用户的特性来组织和管理用户，提高工作效率。为用户设置用户组，在进行资源授权时可以把权限赋予某个用户组，用户组中的成员即可获得对应的权限，而且方便运维工程师检查，用户组可以更高效地管理用户权限。

用于保存主账号基本信息的文件是 /etc/group，保存格式为 group_name:password:GID:user_list，每行信息包括 4 个字段。

/etc/group 文件的部分输出如下：

```
[root@localhost ~]# cat /etc/group
root:x:0:
```

上述 /etc/group 文件的部分输出对应的完整格式如下：

```
< 组名 >:< 组口令 >:<GID>:< 用户列表 >
```

（1）组名：用户组的名称。

（2）组口令：用占位符 x 表示，加密后的密码保存在 /etc/gshadow 文件中。

（3）GID：用户组的 ID，Linux 操作系统通过 GID 区分用户组。

（4）用户列表 ：每个用户组包含的所有用户，这里列出的是以该用户组为附加组的用户，并没有列出以此用户组为主组的用户。

/etc/gshadow 是 /etc/group 的加密文件，两个文件为互补的关系。对于大型的生产环境，设置明确的用户与组，定制关系结构比较复杂的权限模型，设置用户组密码很有必要。/etc/gshadow 文件中的每行信息包括 4 个字段，字段之间用冒号隔开。

/etc/gshadow 文件的部分输出如下：

```
[root@EulerOS ~]# cat /etc/gshadow
root:::
```

上述 /etc/gshadow 文件的部分输出对应的完整格式如下：

```
< 用户组名 >:< 用户组密码 >:< 用户组管理员名称 >:< 用户组成员列表 >
```

（1）用户组名：用户组的名称。

（2）用户组密码：大部分用户通常不设置组密码，因此该字段常为空。若该字段中出现“！”字符，则代表用户组没有密码，也不设置用户组管理员。

（3）用户组管理员名称：该字段可为空，也可设置多个用户组管理员名称。

（4）用户组成员列表：该字段显示用户组中有哪些附加用户，与 /etc/group 文件中的附加值显示内容相同。

用户和用户组的对应关系：一对一、一对多、多对一和多对多。这 4 种对应关系的解析如下。

（1）一对一：一个用户可以存在于一个组中，也可以是组中的唯一成员。

（2）一对多：一个用户可以存在于多个组中，此用户具有多个组的共同权限。

（3）多对一：多个用户可以存在于一个组中，这些用户具有与组相同的权限。

（4）多对多：多个用户可以存在于多个组中，这种对应关系就是上面 3 种对应关系的拓展。

在 Linux 操作系统的设计中，每个用户都有一个对应的组，组是多个（含一个）用户为达到同一目的而组成的组织，组内的成员对属于该组的文件具有相同的权限。在默认情况下，Linux 操作系统拥有用户私人组（User Private Group，UPG），创建一个新用户的同时会创建一个和用户名相同的用户私人组。

项目实施

任务 3-1　管理信息中心的用户账号

任务规划

为满足 Jan16 公司信息中心员工对安装了 openEuler 操作系统的服务器的访问需求，运维工程师需要根据表 3-1 中的内容为每个员工创建用户账号。运维工程师可通过向导式菜单为员工创建

扫一扫

微课：管理信息中心的用户账户

用户账号，并在用户属性管理界面中修改用户账号的相关信息。当用户使用新账号登录系统时，可以自行修改登录密码。

在 openEuler 操作系统终端上为信息中心员工创建用户账号，可通过以下操作步骤实现。

（1）通过“useradd”命令创建用户账号。

（2）通过不同的参数修改用户账号的属性。

（3）在任务验证中，使用新用户账号登录系统，测试新用户账号第一次登录系统是否需要更改密码。

任务实施

（1）运维工程师以用户账号 root 登录服务器，打开 openEuler 操作系统终端，创建用户账号 Huang，备注为“信息中心主任”，代码如下：

```
[root@EulerOS ~]# useradd -c "信息中心主任" Huang
[root@EulerOS ~]# echo “1qaz@WSX” | passwd --stdin Huang
```

在创建用户账号时，参数 -c 代表加上备注文字，备注文字保存在 /etc/passwd 文件对应的用户备注栏中。

（2）查看用户账号 Huang 是否创建成功，代码如下：

```
[root@EulerOS ~]# cat /etc/passwd
Huang:x:1001:1001:信息中心主任:/home/Huang:/bin/bash
```

（3）限制用户账号 Huang 在第一次登录系统时必须修改密码，代码如下：

```
[root@EulerOS ~]# chage -d0 Huang
```

在上述代码中，“-d <N>”选项应该被设置为密码的“有效期”（自密码上一次被修改的时间 1970 年 1 月 1 日以来的天数），所以“-d0”表明该密码是在 1970 年 1 月 1 日被修改的，这实际上会让当前密码到期失效，从而让密码在下一次登录时必须进行修改。

（4）切换用户账号，查看是否能够成功限制用户账号 Huang 登录，需要注意的是，不能使用 root 用户进行切换，因为 root 用户切换时不需要输入密码。使用 SSH 远程登录的方式对用户账号 Huang 进行测试，用户在认证界面中输入正确密码后，系统强制要求管理员更改用户账号 Huang 的密码，输入当前密码后，提示输入新密码，测试完成。代码如下：

```
[root@EulerOS ~]$ ssh Huang@localhost
Huang@localhost's password:
You are required to change your password immediately (administrator en-
forced).

WARNING: Your password has expired.
You must change your password now and login again!
```

```
Changing password for user Huang.
Changing password for Huang.
Current password:New password:
Retype new password:
passwd: all authentication tokens updated successfully.
```

（5）使用“useradd”命令创建 Zhang、Li、Zhao、Song 四个用户账号，代码如下：

```
[root@EulerOS ~]# useradd -c "网络管理组" Zhang
[root@EulerOS ~]# useradd -c "网络管理组" Li
[root@EulerOS ~]# useradd -c "系统管理组" Zhao
[root@EulerOS ~]# useradd -c "系统管理组" Song
```

（6）查看用户账号创建的情况，代码如下：

```
[root@EulerOS ~]# cat /etc/passwd
Huang:x:1001:1001:信息中心主任:/home/Huang:/bin/bash
Zhang:x:1003:1003:网络管理组:/home/Zhang:/bin/bash
Li:x:1004:1004:网络管理组:/home/Li:/bin/bash
Zhao:x:1005:1005:系统管理组:/home/Zhao:/bin/bash
Song:x:1006:1006:系统管理组:/home/Song:/bin/bash
```

任务验证

（1）创建用户账号后，注销用户账号 root，在 openEuler 操作系统登录界面中使用用户账号 Huang 登录，系统会出现如图 3-2 所示的“You are required to change your password immediately (administrator enforced)”（管理员强制要求您立即更改密码）提示信息。

```
Authorized users only. All activities may be monitored and reported.
EulerOS login: Huang
Password:
You are required to change your password immediately (administrator enforced).
Changing password for Huang.
Current password:
```

图 3-2　提示更改用户账号 Huang 的密码

（2）根据要求更改用户账号 Huang 的密码，如图 3-3 所示。

```
Authorized users only. All activities may be monitored and reported.
EulerOS login: Huang
Password:
You are required to change your password immediately (administrator enforced).
Changing password for Huang.
Current password:
New password:
Retype new password:
Last login: Wed Dec 22 15:29:43 from 192.168.79.1
```

图 3-3　更改用户账号 Huang 的密码

（3）更改密码后，openEuler 操作系统将以用户账号 Huang 登录，如图 3-4 所示。

图 3-4　以用户账号 Huang 登录

任务 3-2　管理信息中心的组账号

任务规划

扫一扫

微课：管理信息中心的组账户

Jan16 公司信息中心网络管理组的员工试用安装了 openEuler 操作系统的服务器一段时间后，决定在服务器上部署业务系统进行系统测试，确定该系统能稳定支撑公司业务后再进行业务系统迁移，并在这台服务器上创建共享，同时将系统测试文档统一保存在网络共享文件夹中。

Jan16 公司业务系统的管理涉及信息中心网络管理组和系统管理组的所有员工，因此 Jan16 公司信息中心需要为每位员工的用户账号授予管理权限。

根据图 3-1、表 3-1 和 openEuler 操作系统的权限情况，运维工程师对用户隶属的组账号进行如下分析。

（1）Jan16 公司信息中心的黄工是信息中心主任，对系统具有完全控制权限，并且可

以向其他用户账号分配用户权限和访问控制权限，还具有服务器管理的最高权限，即用户账号 root，该用户账号应隶属于 root 组。

（2）网络管理组由张工和李工两位工程师组成，他们需要对该服务器的网络服务进行相关配置和管理，具有服务器的网络管理权限。网络管理组的工程师可以更改网卡配置方面的文件，并更新和发布 TCP/IP 地址，但是两位工程师没有修改其他用户密码和终止其他用户进程的权限，Zhang 和 Li 两个用户账号应隶属于 Netadmins 组。

（3）系统管理组由赵工和宋工两位工程师组成，他们需要对系统进行修改、管理和维护。系统管理组的工程师需要对系统具有完全控制权限，Zhao 和 Song 两个用户账号应隶属于自定义组。

（4）从信息中心的组织架构和后续权限管理需求出发，需要分别为网络管理组和系统管理组创建组账号 Netadmins 和 Sysadmins，并将组成员分别添加至各自隶属的自定义组中。

综上所述，运维工程师对信息中心所有员工的用户账号的操作权限和系统内置组做了映射。服务器系统自定义组规划如表 3-2 所示。

表 3-2　服务器系统自定义组规划

用 户 账 号	隶属自定义组	权　　限
Zhao	Netadmins	网络管理 虚拟化管理
Song		
Huang	Sysadmins	系统管理
Zhang		
Li		

任务实施

1. 创建本地组账号并配置其隶属的系统内置组

（1）使用用户账号 root 在终端界面中分别创建组账号 Netadmins 和 Sysadmin，代码如下：

```
[root@EulerOS ~]# groupadd Netadmins
[root@OpenEuler ~]# groupadd Sysadmins
```

（2）组账号创建完成后，查看配置文件，验证两个组账号是否创建成功，代码如下：

```
[root@EulerOS ~]# cat /etc/group
Netadmins:x:1007:
Sysadmins:x:1008:
```

2. 设置用户账号的隶属组账号

（1）将用户账号 Zhao 和 Song 加入 Netadmins 组，并查看用户组的 ID 是否变更，代码如下：

```
[root@EulerOS ~]# usermod -g Netadmins Zhao
[root@EulerOS ~]# usermod -g Netadmins Song
[root@EulerOS ~]# cat /etc/passwd
Zhao:x:1004:1007:系统管理组:/home/Zhao:/bin/bash
Song:x:1005:1007:系统管理组:/home/Song:/bin/bash
```

（2）使用同样的方法将用户账号 Huang、Zhang 和 Li 加入 Sysadmins 组，并查看用户账号的组 ID 是否变更，代码如下：

```
[root@EulerOS ~]# usermod -g Sysadmins Huang
[root@EulerOS ~]# usermod -g Sysadmins Zhang
[root@EulerOS ~]# usermod -g Sysadmins Li
[root@EulerOS ~]# cat /etc/passwd
Huang:x:1001:1008:信息中心主任:/home/Huang:/bin/bash
Zhang:x:1003:1008:网络管理组:/home/Zhang:/bin/bash
Li:x:1004:1008:网络管理组:/home/Li:/bin/bash
```

（3）将用户账号 Huang 加入 root 组，并为用户账号 Huang 提升权限为系统管理，使得该用户拥有对系统的完全控制权限，代码如下：

```
[root@EulerOS ~]# usermod -g root Huang
[root@EulerOS ~]# cat /etc/passwd
Huang:x:1001:0:信息中心主任:/home/Huang:/bin/bash
```

（4）修改配置文件，授予用户账号 Huang 系统管理的权限，使用用户账号 root 修改 /etc/sudoers 文件，添加对应的红色字体的权限，并使用“wq!”命令强制保存后退出，此时用户账号 Huang 已经获取用户 root 的权限，切换到用户账号 Huang 可以使用“sudo -i”命令获取权限，执行需要系统管理员身份才能执行的操作，如查看 /etc/sudoers 文件。代码如下：

```
[root@EulerOS ~]# visudo /etc/sudoers
## Allow root to run any commands anywhere
root    ALL=(ALL)     ALL
Huang   ALL=(ALL)     ALL
[root@EulerOS ~]# su Huang
[Huang@EulerOS root]$ sudo -i

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for Huang:
[root@EulerOS ~]# tail -4 /etc/sudoers
# %users  localhost=/sbin/shutdown -h now

## Read drop-in files from /etc/sudoers.d (the # here does not mean a
```

```
comment)
#includedir /etc/sudoers.d
```

（5）没有配置的用户账号无法使用“sudo -i”命令获取系统管理权限，代码如下：

```
[Huang@EulerOS ~]$ su - Li
Password:
[Li@EulerOS ~]$ sudo -i
[sudo] password for Li:
Li is not in the sudoers file.  This incident will be reported.
```

（6）对用户账号 Zhang 和 Li 进行限制，用户账号 Zhang 可以使用 /usr/bin 和 /bin 目录下的所有命令，但是为了保障系统的安全性，用户账号 Zhang 不可以修改其他用户的密码和终止（kill）其他用户的进程；用户账号 Li 可以使用 /bin 目录下的所有命令，但是不能修改其他用户的密码和终止其他用户的进程，也不能使用“nmcli”命令。在 /etc/sudoers.d 目录下使用“visudo”命令创建名称与用户名相同的策略文件并写入以下配置，代码如下：

```
[root@EulerOS ~]# visudo -s /etc/sudoers.d/Zhang
Zhang ALL=/usr/bin/,/bin/,!/usr/bin/passwd,!/bin/kill
[root@EulerOS ~]# visudo -s /etc/sudoers.d/Li
Li ALL=/bin/,!/usr/bin/passwd,!/bin/kill
```

“visudo”命令用于安全地编辑 /etc/sudoers 文件，该命令具有如下特点。

① 需要超级用户权限。

② 默认使用“vi”命令编辑 /etc/sudoers 文件。

③ /etc/sudoers 文件的默认权限是 440，即默认无法修改。

④“visudo”命令可以在不更改 /etc/sudoers 文件权限的情况下直接修改此文件。

⑤“visudo”命令在退出并保存时会检查内部语法，避免用户输入错误信息。

⑥“-s”“--strict”选项可对文件进行严格的语法检查。

（7）将用户账号 Song 和 Zhao 加入 root 组，代码如下：

```
[root@EulerOS ~]# usermod -g root Zhao
[root@EulerOS ~]# usermod -g root Song
[root@EulerOS ~]# cat /etc/passwd
Zhao:x:1005:0: 系统管理组 :/home/Zhao:/bin/bash
Song:x:1006:0: 系统管理组 :/home/Song:/bin/bash
```

任务验证

（1）用户账号 Zhang 隶属于 Netadmins 组，该用户账号并不具有系统管理权限，但是该用户账号的权限支持该用户使用 /usr/bin、/bin 目录下的所有命令，而不能使用“passwd”命令去修改其他用户的密码，也不能使用“kill”命令去终止其他用户的进程，代码如下：

```
[Zhang@EulerOS ~]$ sudo cd
[sudo] password for Zhang:
```

```
[Zhang@EulerOS ~]$
[Zhang@EulerOS ~]$ pwd
/home/Zhang
[Zhang@EulerOS ~]$ sudo kill
Sorry, user Zhang is not allowed to execute '/usr/bin/kill' as root on
EulerOS.jan16.cn.（抱歉，用户账号 Zhang 不能在 EulerOS.jan16.cn 机器上作为 root 用户执
行‘/usr/bin/kill’命令）
[Zhang@EulerOS ~]$ sudo passwd
Sorry, user Zhang is not allowed to execute '/usr/bin/passwd' as root on
EulerOS.jan16.cn.
```

（2）用户账号 Li 隶属于 Netadmins 组，该用户账号并不具有系统管理权限，但是该用户账号可以使用 /bin 目录下的所有命令，而不能使用“passwd”命令去修改其他用户的密码，也不能使用“kill”命令去终止其他用户的进程，代码如下：

```
[root@EulerOS ~]$ su - Li
[Li@EulerOS ~]$ sudo kill
Sorry, user Li is not allowed to execute '/usr/bin/kill' as root on EulerOS.
jan16.cn.
 [Li@EulerOS ~]$ sudo passwd
Sorry, user Li is not allowed to execute '/usr/bin/passwd' as root on EulerOS.
jan16.cn.
[Li@EulerOS ~]$ sudo nmcli
ens33: connected to ens33
        "Intel 82545EM"
        ethernet (e1000), 00:0C:29:A1:19:D8, hw, mtu 1500
        ip4 default
        inet4 192.168.47.128/24
        route4 0.0.0.0/0
        route4 192.168.47.0/24
        inet6 fe80::8fbe:52f4:8ed2:3a2b/64
        route6 fe80::/64
        route6 ff00::/8
[Li@EulerOS ~]$ sudo date
Mon Jul 27 02:41:47 EDT 2020
```


练习与实践

一、理论习题

选择题

1．openEuler 操作系统中默认的管理员账号是（　　）。

A．admin　　B．root　　C．supervisor　　D．administrator

2．当需要展示 Linux 操作系统中的某目录结构时，可以使用的命令是（　　）。

A．tree　　B．cd　　C．mkdir　　D．cat

3．需要创建一个名为 /jan16/test 的目录，可以使用的命令是（　　）。

A．mkdir -pv /jan16/test　　B．touch / jan16/test

C．rm -rf / jan16/test　　D．mount / jan16/test

4．若新建的磁盘需要永久挂载，则需要修改的配置文件是（　　）。

A．/etc/fstab　　B．/etc/sysconfig

C．/usr/local　　D．/dev/cdrom

5．临时修改 selinux 权限为允许，需要执行的命令为（　　）。

A．systemctl stop firewalld　　B．setneforce 0

C．getenforce　　D．nmcli connection show

二、项目实训题

实训一

1．在 openEuler 操作系统中使用命令创建 STUs 组和用户账号 st1、st2、st3，并将这三个用户账号加入 STUs 组。

2．设置用户账号 st1 下次登录时必须修改密码，设置用户账号 st2 不能更改密码且密码永不过期，停用用户账号 st3。

3．用 root 用户账号登录计算机，在计算机用户与组管理界面中完成如下操作。

（1）创建用户账号 test，使 test 用户账号隶属于 root 组。

（2）注销后用 test 用户账号登录，通过 /etc/passwd 文件查看自己的安全标识符。

（3）在用户家目录下创建一个文本文件，命名为 test.txt。

（4）思考：注销后重新用 root 用户账号登录，这时是否可以在桌面上看到刚才创建的文本文件？如果看不到，那么应该在哪里找到它？

（5）思考：删除 test 用户账号，重新创建一个 test 用户账号，注销后用 test 用户账号登录，此时是否还可以在桌面上看到刚刚创建的文本文件？这个新的 test 用户账号的安全标识符是否和原先删除的 test 用户账号的安全标识符一样？

实训二

1．项目描述

Jan16 公司研发部由研发部主任赵工、软件开发组钱工和孙工、软件测试组李工和简工 5 位工程师组成。研发部的组织架构如图 3-5 所示。

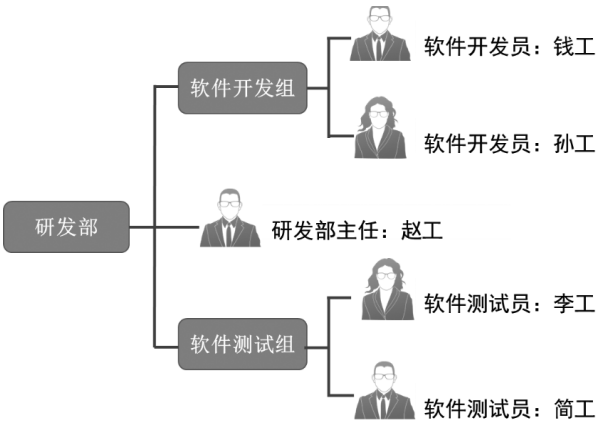

图 3-5　研发部的组织架构

研发部为满足新开发软件产品的部署需要，采购了一台安装了 openEuler 操作系统的服务器用于软件部署和测试。研发部根据员工的岗位需要，为每个员工规划了相应权限。研发部员工账号信息如表 3-3 所示。

表 3-3　研发部员工账号信息

姓　名	用 户 账 号	权　限	备　注
赵工	Zhao	系统管理	研发部主任
钱工	Qian	系统管理	软件开发组
孙工	Sun		
李工	Li	网络管理 系统备份 打印管理	软件测试组
简工	Jian		

2．项目要求

1）根据项目背景规划、研发部员工用户账号权限、自定义组信息和用户隶属组关系，填写表 3-4。

表 3-4　研发部用户与组账号权限规划

自定义组名称	组　成　员	权　限

2）在研发部的服务器上完成用户与组的创建，同时要求所有用户第一次登录系统时需要修改密码，并截取以下图片。

（1）截取 /etc/passwd 文件界面，查看用户账号所隶属的组。

（2）截取 /etc/group 文件界面。