项 目 3

掌握账户与权限管理

Linux是多用户、多任务的网络操作系统，对用户和权限的管理是系统管理员应掌握的基本内容，对文件的属性进行设置，根据用户需求进行分组，是实现资源共享和保障系统安全的关键。

【知识能力培养目标】

（1）了解用户和组的配置文件。

（2）掌握用户和组的操作管理方法。

（3）掌握文件和目录的权限管理。

【课程思政培养目标】

课程思政培养目标如表3-1所示。

表3-1 课程思政培养目标

教学内容	思政元素切入点	育人目标
管理账户与文件属性操作、权限管理	讲述网络管理员在工作中对账户的管理与权限分配的重要性，权责分明，各司其职	增强工作中的规范意识，明确职业技术岗位所需的职业规范和精神，树立社会主义核心价值观
访问控制列表	访问控制列表的功能是对到访的数据包进行访问控制。只允许符合访问条件的数据包进行访问，达到网络安全的目的。在人类社会生活中，做任何事都要遵守规则	培养学生树立法律意识，遵守校规，做一个遵纪守法的好学生

任务1 掌握用户和组管理

Linux是多用户、多任务的网络操作系统，用户和组的管理对系统安全尤为重要。

学习情境 1　了解 Linux 账户类型

Linux 是多用户、多任务的操作系统，可以同一时间多个用户登录同一个系统，执行多个不同任务且互相不受影响，为实现多用户共享和保障资源的安全，要对用户进行不同权限的分配，权限不同所完成的任务也不同，用户组则在很大程度上提高了管理效率。

(1) 超级用户：管理员，默认是 root 用户，拥有对系统最高的管理权限，对所有文件具有访问、修改和执行权限。

(2) 普通用户：由管理员创建，拥有的权限具有局限性，只能对自己主目录下的文件进行访问、修改和执行。

(3) 程序用户：主要用于让服务类进程或后台进程以非管理员身份运行，该类用户不能登录系统，多为安装系统或应用程序时自动添加，一般权限较低。

在日常工作中，若以 root 用户登录对系统进行操作，如果出现误操作，将对操作系统造成不可逆的损伤，通常创建一个普通用户对系统进行常规操作，而不使用 root 用户直接登录访问系统。

当多个用户具有相同的权限，则组成一个用户组。

学习情境 2　了解用户管理

在 Linux 系统中，用户管理主要包括创建新用户、修改用户属性、密码管理以及删除用户等操作。

1. 创建用户

使用 useradd 命令创建新用户，基本命令格式为：

```
useradd  [选项] [用户名]
```

常用选项及说明如表 3-2 所示。

表 3-2　创建用户命令常用选项列表

选项	说　明	选项	说　明
-d	指定用户主目录	-u	手动指定用户的 UID
-g	指定用户组	-s	指定用户登录 Shell
-c	设置对该账号的注释说明	-M	不创建用户家目录

【例 3-1】 创建名为 Jack 的用户。

```
[root@localhost ~]# useradd Jack
```

当用户创建成功，在系统文件/etc/passwd 和/etc/shadow/中增加该用户的记录。如果在创建用户时没有指明用户的家目录和用户组，则会在/home 目录下自动创建与用户同名的家目录，同时会自动创建与该用户同名的用户组，组账号的记录信息则保存在/etc/group 和/etc/gshadow 中。

【例 3-2】 创建新用户 Ryan，并将其家目录指定为/test。

```
[root@localhost ~]# useradd -d /test Ryan
```

创建新用户 Ryan 的同时，在根目录下创建了 Ryan 用户的家目录/test。

【例 3-3】 创建新用户 Sean，并将其 UID 指定为 1007。

```
[root@localhost ~]# useradd -u 1007 Sean
[root@localhost ~]# tail -1 /etc/passwd
Sean:x:1007:1007::/home/Sean:/bin/bash
```

普通用户的 UID 从 1000 开始递增，使用“-u”选项，则可以给新建用户账号指定 UID。

【例 3-4】 创建新用户 Kaka，指定为组 student 的成员。

```
[root@localhost ~]# useradd -g student Kaka
[root@localhost ~]# id Kaka
uid=1008(Kaka) gid=1000(student) 组=1000(student)
```

在创建新用户时为其指定基本组，必须保证指定用户组已经存在，系统将不再创建与用户名同名的用户组。

【例 3-5】 创建新用户 Messi，设置家目录为/milan，加入 root 组，加注释 university，指定登录 Shell 为/bin/sh。

```
[root@localhost ~]# useradd -d /milan -g root -c university -s /bin/sh Messi
[root@localhost ~]# tail -1 /etc/passwd
Messi:x:1009:0:university:/milan:/bin/sh
[root@localhost ~]# id Messi
uid=1009(Messi) gid=0(root) 组=0(root)
```

useradd 命令的选项也可联合起来同时使用。

2. 修改用户属性

对于已经创建好的用户，如果要修改其属性信息，可以编辑/etc/passwd 文件中的相关参数，或者使用 usermod 命令修改和设置账号的各项属性。基本命令格式为：

```
usermod [选项] [用户名]
```

修改用户账号属性使用 usermod 命令，常用选项及说明如表 3-3 所示。

表 3-3　修改用户属性命令常用选项列表

选项	说　明	选项	说　明
-l	修改用户名	-s	修改用户登录后使用的 Shell
-d	修改用户主目录	-u	修改用户 UID
-c	修改用户注释信息	-L	锁定账号，临时禁止用户登录
-g	修改用户所属基本组	-U	解锁账号
-G	修改用户所属附加组		

【例 3-6】 将用户的名称 Jack 修改为 Monica。

```
[root@localhost ~]# usermod -l Monica Jack
```

【例 3-7】 将用户 Ryan 的主目录 Ryan 修改为/var/rui。

```
[root@localhost ~]# mkdir /var/rui
[root@localhost ~]# usermod -d /var/rui Ryan
```

【例 3-8】 将用户 Sean 的基本组修改为 root。

```
[root@localhost ~]# id Sean
uid=1007(Sean) gid=1007(Sean) 组=1007(Sean)
[root@localhost ~]# usermod -g root Sean
[root@localhost ~]# id Sean
uid=1007(Sean) gid=0(root) 组=0(root)
```

3. 密码管理

新用户需要创建密码之后才能登录系统,使用 passwd 命令对用户密码进行管理,可对当前用户设置或更改密码。基本命令格式为:

```
passwd [选项] [用户名]
```

用户账号密码管理使用 passwd 命令,常用选项及说明如表 3-4 所示。

表 3-4 密码管理命令常用选项列表

选项	说 明	选项	说 明
-S	查看用户密码状态	-u	解锁用户密码
-l	锁定用户密码	-d	删除用户密码

【例 3-9】 为用户 Jack 设置系统登录密码。

```
[root@localhost ~]# passwd Jack
```

passwd 命令除了设置用户密码外,还用来管理用户的密码。

4. 删除用户

删除一个已存在的账号使用 userdel 命令。基本命令格式为:

```
userdel [选项] [用户名]
```

【例 3-10】 删除用户 Jack 及其主目录。

```
[root@localhost ~]# userdel -r Jack
```

学习情境 3 管理用户组

1. 创建用户组

使用 groupadd 命令创建用户组。基本命令格式为:

```
groupadd [选项] [用户组名]
```

【例 3-11】 创建用户组 manage。

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

2. 修改用户组属性

对于已创建好的用户组,使用 groupmod 命令修改其属性。基本命令格式为:

```
groupmod [选项] [用户组名]
```

【例 3-12】　修改用户组 teacher 为 engineer。

```
[root@localhost ~]# groupmod -n teacher engineer
```

3. 维护用户组

gpasswd 命令用于给群组设置一个群组管理员，进行将用户加入或移出群组的操作。基本命令格式为：

```
gpasswd [选项] [用户名] [用户组名]
```

【例 3-13】　添加用户 Jack 到用户组 sales。

```
[root@localhost ~]# gpasswd -a Jack sales
```

4. 删除用户组

使用 groupdel 命令删除用户组。基本命令格式为：

```
groupdel [用户组名]
```

【例 3-14】　删除用户组 sales。

```
[root@localhost ~]# groupdel sales
```

学习情境 4　熟知相关系统的配置文件

1. 用户信息配置文件/etc/passwd

在 Linux 系统中，/etc/passwd 文件包含系统里用户的基本信息，每个用户对应文件里的一行记录，每行记录由 7 个字段构成，内容通过“:”分隔开来，每个字段分别表示该用户的属性信息。所有用户对该文件都有访问权限。

```
[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
…
```

以文件的第一行 root 的信息为例，介绍字段的含义。

第 1 个字段 root：用户名。

第 2 个字段 x：密码占位符。出于安全性的考虑，使用占位符表示这是一个密码字段，真正的密码并不存放于此，而是存放在权限受到严格限制的/etc/shadow 中。

第 3 个字段 0：用户的 UID，root 的 UID 默认为 0。普通用户的 UID 默认值为 1000～60000。

第 4 个字段 0：用户所属组的 GID。普通用户组的 GID 默认值为 1000～60000。

第 5 个字段 root：用户的注释信息。

第 6 个字段/root：用户主目录。

第 7 个字段/bin/bash：用户所用的 Shell 类型。如果指定 Shell 为/sbin/nologin，表示该用户为虚拟用户，无法登录系统。

2. 用户密码配置文件/etc/shadow

/etc/shadow 是 Linux 操作系统的密码管理文件，包含用户密码的加密信息及其他相关安全信息，文件中每一行对应一个用户的密码信息，每行内容由 9 个字段组成，通过“:”分隔开来。只有 root 用户有读取文件内容的权限，普通用户无法访问。

```
[root@localhost ~]# cat /etc/shadow
root: $6 $a/yX9o4du6MNs6P. $5Tdd4. KpGAfgL5DuoV//d/GwnPMxtLcVURF6cdulXvijFdmq0R8E8oSlOZZIK4Df/
Y0Q30sABpoyITK56mO8y0::0:99999:7:::
bin: * :17110:0:99999:7:::
daemon: * :17110:0:99999:7:::
…
```

以文件的第一行 root 的密码信息为例，介绍字段的含义。

第 1 个字段：用户名。

第 2 个字段：用户的加密密码。密码由三部分组成，用“$”分隔开来，第一部分表示所用的加密算法，$6 对应 SHA512 加密算法；第二部分是在密码中加入随机数来增强密码安全性；第三部分是用户密码加密后的密文。

第 3 个字段：最后一次修改时间。

第 4 个字段：用户可以更改密码的天数。0 表示随时可进行变更。

第 5 个字段：到期更改密码的天数。99999 表示永不过期。

第 6 个字段：密码过期警告时间。默认值是 7 天。

后三个字段分别为用户密码过期后禁用账号天数、失效时间和保留位。

3. 用户组配置文件/etc/group

对用户进行分组管理是 Linux 系统一种非常有效的管理方式，/etc/group 用于保存用户组的基本信息。文件中每行记录对应一个用户组的信息，每行由 4 个字段组成，通过“:”分隔开来。

```
[root@localhost ~]# cat /etc/group
root:x:0:
bin:x:1:
daemon:x:2:
sys:x:3:
adm:x:4:
tty:x:5:
…
```

以文件的第一行 root 组的信息为例，介绍字段的含义。

第 1 个字段 root：组的名称。

第 2 个字段 x：密码占位符。

第 3 个字段 0：组的 GID。

第 4 个字段：该组成员。

4. 用户组密码配置文件/etc/shadow

文件包含组密码和加密信息，该文件 root 用户可访问。

```
[root@localhost ~]# cat /etc/gshadow
```

```
root:::
bin:::
daemon:::
…
```

文件中四个字段的含义分别如下。

第 1 个字段：组的名称。

第 2 个字段：用户组的口令。

第 3 个字段：组的管理员账号。

第 4 个字段：该组成员。

任务 2　熟知权限管理

学习情境 1　了解查看文件和目录权限

在 Linux 操作系统中，文件和目录是信息存储的基本机构，每一个文件或目录包含了相应的访问权限，根据赋予权限的不同，不同用户对同一文件或目录的操作也不尽相同。

1. 权限和归属的概念

(1) Linux 系统文件的权限分为以下三种类型。

① 读取：对文件而言是读取文件的内容；对目录而言是浏览目录的内容。

② 写入：对文件而言是修改文件的内容；对目录而言是删除和修改目录内的文件。

③ 执行：对文件而言是执行文件；对目录而言是用户可进入目录。

(2) 文件的归属包括所有者和所属组。

① 所有者：拥有该文件或目录的用户账号。

② 所属组：拥有该文件或目录的组账号。

2. 查看权限和归属

使用“ls -l[文件名]”命令可以查看文件的详细信息，详细信息包含了文件的类型、访问权限、所有者(属主)、所属组(属组)、占用的磁盘大小、修改时间和文件名称等信息，例如：

```
[root@localhost ~]# ls -l initial-setup-ks.cfg
-rw-r--r--. 1 root root 2020 8月  23 2019 initial-setup-ks.cfg
```

在显示的文件详细信息中，第一个符号用来表示文件的类型，在 Linux 系统中，使用不同符号表示不同的文件，如表 3-5 所示。

表 3-5　符号列表

符号	文件类型	符号	文件类型
-	普通文件	b	块设备文件
d	目录	c	字符设备文件
l	链接文件	p	管道文件

在文件类型符号之后的字段表示文件的权限，权限字段分为三个部分：第一部分表示文件所有者对文件的权限；第二部分表示文件所属组成员用户对文件的权限；第三部分表

示其他用户对文件的权限。文件权限类型如图 3-1 所示。

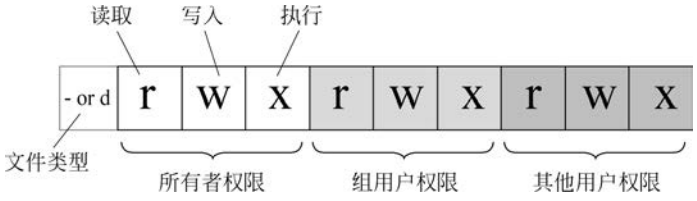

图 3-1　文件权限类型

文件的权限使用三个字符对应表示，文件的读取用 r(Read)表示，写入用 w(Write)表示，执行用 x(eXecute)表示，倘若没有某个权限，则在对应权限处用“-”代替，表示无此权限。

学习情境 2　设置文件和目录权限

1. chmod 命令设置权限

使用 chmod 命令可以设置和修改文件或目录的权限，root 用户和文件所有者可以通过数字权限法和字符权限法改变文件或目录的访问权限。

1) 数字形式的 chmod 命令

```
chmod [可选项] < mode > < file...>
```

数字形式表示权限就是将 r、w、x 权限字符分别用数字 4、2、1 表示，没有权限的位置上的“-”则用 0 表示。一个权限组合即为 3 个数字的相加，得到一个 0～7 的数字，来实现对文件或目录的权限表示，数字表示法也称为绝对权限表示法，如表 3-6 所示。

表 3-6　权限操作表

权　　限	字母表示	数字表示
读＋写＋执行	rwx	7
读＋写	rw-	6
读＋执行	r-x	5
只读	r--	4
写＋执行	-wx	3
只写	-w-	2
只执行	--x	1
无	---	0

【例 3-15】 rwx 采用数字表示形式为数字 7，r-x-采用数字表示形式为 5，一个文件的权限是 rwxr-xr--，转换过来就是 754，意味着所有者的权限是 rwx，也就是 4＋2＋1＝7，用户组的权限是 r-x，也就是 4＋0＋1＝5，其他用户的权限是 r--，也就是 4＋0＋0＝4。

chmod 命令格式为：

```
chmod [选项] [文件名]
```

【例 3-16】 修改文件权限，使所有用户对 test 文件有读、写和执行权限。

```
[root@localhost ～]# chmod 777 test
```

2）字符形式的 chmod 命令

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组，o 表示其他用户，a 表示三者的集合。字符形式命令选项如表 3-7 所示。

表 3-7　字符形式命令选项

用户代号	用户类型	说　明
u	user	文件所有者
g	group	文件所有者所在组
o	others	所有其他用户
a	all	所用用户

在用户代号的后面通过运算符和权限组合对文件权限进行设置，如表 3-8 所示。

表 3-8　组合符号

运算符	说　明
＋	为指定的用户类型增加权限
－	去除指定用户类型的权限
＝	设置指定用户权限

【例 3-17】 修改文件权限，使组用户对 test 文件添加写权限。

```
[root@localhost ~]# chmod g+w test
```

【例 3-18】 修改文件权限，取消其他用户对 test 文件的读权限。

```
[root@localhost ~]# chmod o-r test
```

2. chown 设置归属

一般来说，文件或目录的所有者有着对文件最高的权限，根据需求也可将文件或目录的拥有权转给其他用户，我们可以通过 chown 命令修改文件或目录的所有者和所属组，要注意的是，需要 root 用户的权限才能执行该命令，而且文件所有者只能将所属组更改为当前用户所在的组。

命令格式：

```
chown [选项] [新用户：新用户组] [文件名或目录名]
```

常用的选项如下。

user：新的文件拥有者的使用者 ID。

group：新的文件拥有者的使用者群体(group)。

-c：若该文件拥有者确实已经更改，才显示其更改动作。

-f：若该文件拥有者无法被更改也不要显示错误信息。

-v：显示拥有者变更的详细资料。

-R：递归处理指定目录以及其子目录下的所有文件。

【例 3-19】 将 test.txt 的所有者修改成 ryan，所属组设置为 teacher 组。

```
[root@localhost ~]# chown ryan:teacher test.txt
```

【例 3-20】 将目录 dir1 的所有文件和子目录的所有者设置为 ryan，所属组设置为 teacher。

```
[root@localhost ~]# chown -R ryan:teacher dir1
```

【例 3-21】 将 test.txt 的所属组设置为 teacher。

```
[root@localhost ~]# chown :teacher test.txt
```

任务 3 特 殊 权 限

Linux 系统中常见的权限设置读、写和执行在某些特殊应用环境中无法满足系统用户的要求。因此，Linux 系统提供了几种特殊权限来扩展用户对文件或目录的控制方式。特殊权限包括 SET 位权限和粘滞位权限。

学习情境 1 设置 SET 位权限

SET 位权限一般对可执行的文件或者目录进行设置，权限字符为 s，根据设置的权限对象不同，分为 SUID 和 SGID。

1. SUID

SUID 是一种对二进制程序进行设置的特殊权限，设置了 SUID 的程序文件，在用户执行该程序文件时，用户暂时获得该程序文件所有者的权限。例如，程序文件的所有者是 root，那么执行该程序的用户就将临时获得 root 账户的权限。

【例 3-22】 用来修改账户密码的 passwd 命令，查看其对应程序文件的属性信息。

```
[root@localhost ~]# ll /usr/bin/passwd
-rwsr-xr-x. 1 root root 27832 1月  30 2014 /usr/bin/passwd
```

该程序文件的所有者为 root，对应的权限为 rws，表示对所有者 root 进行了 SET 位权限设置，当其他用户执行 passwd 命令时，会自动以文件所有者 root 的身份去执行。当用户使用 passwd 命令进行密码设置时，这个操作将会编辑一些配置文件，如/etc/passwd，/etc/shadow，当查看这些文件的属性信息会发现，这些文档只能通过 root 用户拥有权限打开或者浏览。

```
[root@localhost ~]# ll /etc/passwd
-rw-r--r--. 1 root root 3448 6月  22 2020 /etc/passwd
[root@localhost ~]# ll /etc/shadow
----------.  1 root root 1672 6月  22 2020 /etc/shadow
```

也就是说当一个普通用户在执行 passwd 命令试图修改密码时，将会遇到权限不够被拒绝的情形，这就需要临时为该用户赋予 root 用户的权限，在执行过程中，普通用户暂时获得该文件的所有者权限，使其可以更新/etc/shadow 和其他文件。

如果文件的所有者权限由 rwx 变成了 rws，其中 x 变为 s，这就意味着该文件被赋予了 SUID 权限。