

# 第三部分：用户与权限管理

## 一、Linux 用户与组基础概念

### 1.1 用户类型

- 超级用户（root）：系统管理员，拥有所有权限；
- 普通用户：仅能访问自己授权的资源；
- 系统用户：用于运行系统服务（如 `www-data`，`syslog`）。

### 1.2 用户组（Group）

- 每个用户属于一个主组，也可以属于多个附加组；
- 权限可以授予组而不是个人用户。

### 1.3 用户信息文件

文件路径	说明
<code>/etc/passwd</code>	存储用户账户基本信息
<code>/etc/shadow</code>	存储加密后的用户密码
<code>/etc/group</code>	存储组信息
<code>/etc/login.defs</code>	登录策略配置

## 二、用户与组管理命令

### 2.1 用户相关命令

命令	说明
<code>useradd 用户名</code>	添加新用户
<code>passwd 用户名</code>	设置或修改密码
<code>usermod -aG 组名 用户名</code>	把用户加入附加组
<code>deluser 用户名</code>	删除用户（保留文件）

<code>userdel -r 用户名</code>	删除用户及其主目录
-----------------------------	-----------

示例：

```
sudo useradd -m alice      # 创建用户并自动创建主目录
sudo passwd alice          # 设置密码
sudo usermod -aG sudo alice # 将 alice 加入 sudo 组（允许提权）
```

## 2.2 组管理命令

命令	说明
<code>groupadd 组名</code>	添加新组
<code>groupdel 组名</code>	删除组
<code>groups 用户名</code>	查看用户所属组
<code>id 用户名</code>	查看用户UID/GID和组信息

示例：

```
sudo groupadd devgroup
sudo usermod -aG devgroup alice
groups alice
```

## 三、用户切换与权限提升

### 3.1 切换用户

```
su 用户名      # 切换到指定用户（需输入密码）
exit           # 返回上一个用户
```

### 3.2 sudo 提权

- 普通用户默认不能执行系统管理命令；
- 加入 `sudo` 组的用户可使用 `sudo` 提权运行命令：

```
sudo apt update
```

- 若输入命令错误、权限不足，系统会提示类似：

```
Permission denied
```

### 3.3 编辑 sudo 权限（了解）

```
sudo visudo
```

修改错误可能会锁死系统权限，初学者应谨慎操作。

## 四、文件权限与属主

### 4.1 权限基础（rwx）

每个文件/目录都有三种访问权限：

权限	英文	含义
r	read	读取权限
w	write	写入权限
x	execute	执行/访问权限（目录时表示“可进入”）

三组权限对象：

对象	说明
所有者（user）	创建文件的用户
所属组（group）	文件所属的组
其他人（others）	任何非属主也非组成员的用户

查看权限示例：

```
ls -l
```

输出示例：

```
-rw-r--r-- 1 alice staff 1234 Jul 10 10:00 example.txt
```

解释：

- `-rw-r--r--`：用户可读写，组和其他用户只读；
- 文件属主是 `alice`，属组是 `staff`。

## 4.2 修改权限命令

命令	功能
<code>chmod</code>	修改权限
<code>chown</code>	修改属主
<code>chgrp</code>	修改属组

示例：

```
chmod 755 script.sh      # 设置权限：rwxr-xr-x
chown bob:devgroup file.txt # 设置属主为 bob，属组为 devgroup
```

## 4.3 权限数字表示法（八进制）

权限	数值
<code>rwx</code>	7
<code>rw-</code>	6
<code>r--</code>	4
<code>---</code>	0

例如：

```
1  chmod 644 a.txt      # 所有者读写，其他只读
2  chmod 700 script.sh # 只有属主能读写执行
```

# 本章练习任务

## ✅ 练习1：用户与组管理

```
sudo useradd -m student1
sudo passwd student1
sudo groupadd students
sudo usermod -aG students student1
id student1
groups student1
```

## ✅ 练习2：切换用户体验

```
su student1      # 切换用户
whoami           # 查看当前用户
cd ~             # 回当前用户的主目录（也可以直接执行 cd ）
exit            # 回到原用户
```

## ✅ 练习3：文件权限操作

```
touch testfile
ls -l testfile
chmod 600 testfile
ls -l testfile
chmod u+x testfile
```

## ✅ 练习4：修改属主和属组

```
sudo chown student1 testfile
sudo chgrp students testfile
ls -l testfile
```

## 📦 课后拓展任务

1. 使用 `chmod +x` 给自己写的小脚本添加执行权限；
2. 尝试创建一个只能自己访问的目录，并验证其他用户无法进入；
3. 研究 `/etc/sudoers` 文件结构，但不要直接手动编辑（使用 `visudo`）；
4. 阅读 `man chown`，`man chmod`，`man useradd`。