



# 文件和目录权限管理

计算机学院 盛剑会

# 文件和目录权限管理

---

## 文件的访问权限

**读(r)**: 允许读文件的内容

**写(w)**: 允许向文件中写入数据

**执行(x)**: 允许将文件作为程序执行

---

# 文件和目录权限管理

---

## 目录的访问权限

**读(r)**: 允许查看目录中有哪些文件和目录

**写(w)**: 允许**该在目录下**创建（或删除）文件、目录，修改  
文件名字或者目录名字

**执行(x)**: 允许访问目录(用 **cd 命令进入该目录**，并查看目  
录中可读文件的内容)

---

# 文件和目录权限管理

---

## 用户分类

**文件所有者** (owner) : 建立文件、目录的用户。

**同组用户**(group): 属于同一组群的用户对属于该组群的文件有相同的访问权限。

**其他用户**(other): 除了文件所有者、同组用户的其他用户。

---

# 文件和目录权限管理

在Linux中，将文件访问权限分为**3类用户**进行设置：

**文件所有者 (u)**、**和文件所有者同组的用户 (g)** 和**其他用户 (o)**。对于每一类用户，又可以设置读 (r)、写 (w) 和执行 (x) 3种权限。

这样Linux下对于任何文件或者目录的访问权限都有**3组**。

drwxrwxrwx

文件类型

所有者权限

同组用户权限

其他用户权限

# 文件和目录权限管理

## 访问权限的表示

(1) 字母表示法 (如: `rwxr-xr-x`)

(2) 数字表示法 (如: `755`)

权限	二进制	八进制	权限	二进制	八进制
---	000	0	r--	100	4
--x	001	1	r-x	101	5
-w-	010	2	rw-	110	6
-wx	011	3	rwX	111	7

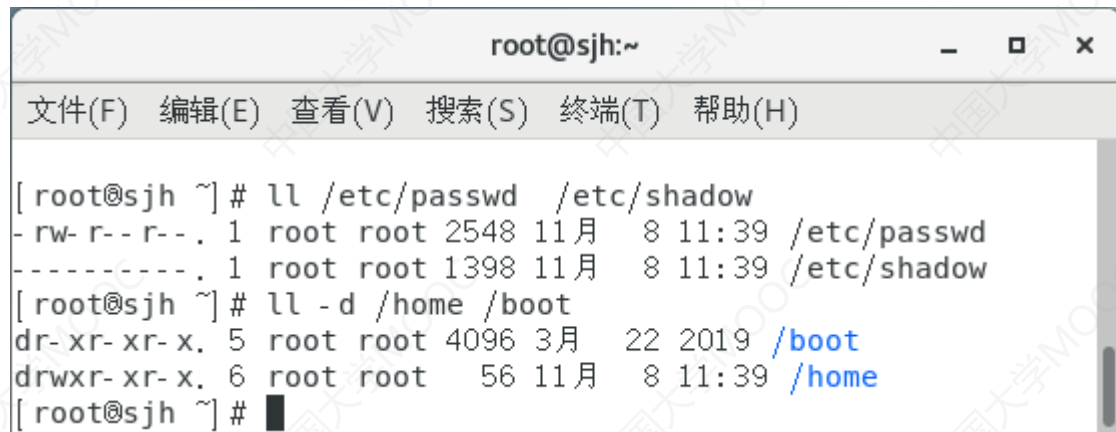
使用数字进行文件权限的划分, 其中 $r=4$ 、 $w=2$ 、 $x=1$ 、 $-=0$ , 这样`rwX`这组权限就是 $4+2+1=7$ , `r-x`这组权限就是5。

# 文件和目录权限管理

## 访问权限举例

要求用**数字表示法**表示

右图中所列文件和文件夹的  
权限。



```
root@sjh:~  
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)  
[ root@sjh ~] # ll /etc/passwd /etc/shadow  
-rw-r--r--. 1 root root 2548 11月  8 11:39 /etc/passwd  
-----. 1 root root 1398 11月  8 11:39 /etc/shadow  
[ root@sjh ~] # ll -d /home /boot  
dr-xr-xr-x. 5 root root 4096 3月  22 2019 /boot  
drwxr-xr-x. 6 root root  56 11月  8 11:39 /home  
[ root@sjh ~] #
```

# 文件和目录权限管理

---

## 修改权限的命令: **chmod**

1) 命令格式1:

**chmod n1n2n3 <文件|目录>**

功能: 为指定文件或目录修改给定的数值访问权限。其中n1代表所有者的权限, n2代表同组用户的权限, n3代表其他用户的权限。

选项: **n1n2n3**三位数字表示的文件访问权限。

---



# 文件和目录权限管理

---

## 修改权限的命令: **chmod**

2) 命令格式2:

**chmod [ugoa][+ -=][rwxugo] <文件名或目录名>**

功能: 修改文件或目录的访问权限。

选项:

- (1) 用户标识: 所有者 (u)、同组 (g)、其他人 (o)、所有的人员 (a)
  - (2) 设定方法: + 增加权限、- 删除权限、= 分配权限, 同时删除旧的权限
  - (3) 权限字符: r (读)、w (写)、x (执行)、u (和所有者的权限相同)、g (和同组用户的权限相同)、o (和其他用户的权限相同)
-

# 文件和目录权限管理

---

## 修改文件权限举例

要求：新建a.txt文件并将该文件设置为所有者拥有全部权限，其他人拥有执行权限。

修改方法：

①字母表示法：**chmod u=rwx, go=x a.txt**

②数字表示法：**chmod 711 a.txt**

这两条命令的效果是一样的。

---

# 文件和目录权限管理

---

## 修改文件所有者的命令：chown

格式：chown [-R] <用户[: 组]> <文件或目录>

功能：更改属主和组。

选项：

-R：对目录及其子目录进行递归设置。

例如：chown sjh: sjh result.txt

---

# 文件和目录权限管理

---

## 修改文件所属组群的命令: **chgrp**

格式: **chgrp group file**

其中group: 组名或组代号

功能: 改变文件或目录组群

例如: **chgrp user result.txt**

---

# 文件和目录权限管理

## 桌面环境下修改文件权限

桌面环境下选中需要修改文件权限的文件、文件夹（目录），**右击**弹出快捷菜单，选中文件“**属性**”对话框。在“基本”选项卡中修改文件名，并可修改文件图标。在“**权限**”选项卡，可以修改文件的权限。



# 文件和目录权限管理

---

## 修改默认权限的命令：umask

格式：umask [mask]

功能：设置文件或目录的默认权限

注意：系统默认屏蔽的权限为022（umask的默认值为0022），因此新

创建的目录权限就为 $777-022=755$ ，用字符表示就是rwxr-xr-x，新创

建的普通文件权限为 $666-022=644$ ，即rw-r--r--。

---

# 文件和目录权限管理

---

## 文件隐藏属性

1) 查看文件隐藏属性: **lsattr**

2) 修改文件隐藏属性: **chattr**

**chattr** [+ -=] [ ai] 文件或目录名称

a: 当设置a之后, 这个文件将只能增加数据, 而不能删除也不能修改数据, 必须要为root才能设置这个属性。

i: 不能删除, 不能修改, 不能改名。必须要为root才能设置这个属性。

---

# 文件和目录权限管理

---

## 文件隐藏属性举例：

举例：**touch attrtest** （此时，文件attrtest能改名，能删除，能修改）

**lsattr attrtest**

**chattr +a attrtest** （此时，文件attrtest不能改名，不能删除，不能修改，只能在文件尾追加内容）

**cat >>attrtest**

**chattr +i attrtest**

**cat >>attrtest** （此时还能不能追加数据？ ？ ？ ）

---



# 文件和目录权限管理

---

## 文件特殊权限

文件特殊权限有以下**三种**：

- 1) **SUID: Set UID**
  - 2) **SGID: Set GID**
  - 3) **SBIT: Sticky Bit**
-

# 文件和目录权限管理

## 文件特殊权限-SUID

**1) SUID: Set UID** (只对二进制程序有效, 对shell script无效)

例如: `ll /usr/bin/passwd`

注意: 当用户执行passwd命令的时候, 需要修改/etc/shadow文件, 而该文件普通用户并没有任何权限。



```
root@sjh:~  
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)  
[root@sjh ~]# ll /usr/bin/passwd  
-rwsr-xr-x. 1 root root 27832 6月 10 2014 /usr/bin/passwd  
[root@sjh ~]# ll /etc/shadow  
----- . 1 root root 1398 11月 8 11:39 /etc/shadow  
[root@sjh ~]#
```

# 文件和目录权限管理

---

## 文件特殊权限-SGID

### 2) SGID: Set GID

例如：ll /usr/bin/locate

```
[root@sjh ~]# ll /usr/bin/locate
-rwx--s--x. 1 root slocate 40520 4月 11 2018 /usr/bin/locate
[root@sjh ~]# ll /var/lib/mlocate/mlocate.db
-rw-r----- 1 root slocate 3073396 11月 11 11:15 /var/lib/mlocate/mlocate.db
```

注意：当用户执行locate命令的时候，需要读取

/var/lib/mlocate/mlocate.db文件。

---

# 文件和目录权限管理

## 文件特殊权限-SBIT

### 3) SBIT: Sticky Bit (只对目录有效)

例如：ls -dl /tmp (当用户在该目录下创建文件或目录时，仅有自己与root才有权利删除该文件)



```
root@sjh:~  
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)  
[ root@sjh ~] # ll -d /tmp  
drwxrwxrwt. 11 root root 4096 11月 19 11:49 /tmp  
[ root@sjh ~] #
```

# 文件和目录权限管理

## 文件特殊权限的数字表示法

当文件具有特殊权限SUID时，其权限的数字表示法需要在原来的三位数字前面加上4；

```
-rwsr-xr-x. 1 root root 27856 Apr 1 2020 /bin/passwd 4755
```

当文件具有特殊权限SGID时，其权限的数字表示法需要在原来的三位数字前面加上2；

```
-rwx--s--x. 1 root slocate 40520 Apr 11 2018 /bin/locate 2711
```

当文件具有特殊权限SBIT时，其权限的数字表示法需要在原来的三位数字前面加上1。

```
drwxrwxrwt. 32 root root 4096 Jun 4 16:00 /tmp 1777
```

# 文件和目录权限管理

---

## 查找具有特殊权限的文件

- 1) `find / -perm 2711` //查找权限等于2711的文件
- 2) `find / -perm -6000` //查找既具有SUID又具有SGID的文件
- 3) `find / -perm /6000` //查找或者具有SUID或者具有SGID或者

两者都有的文件

---