

# 文件和目录权限管理——默认权限、隐藏属性、特殊权限

## 1. 默认权限

### umask命令

格式：umask [mask]

功能：设置文件或目录的默认权限

当用户创建文件或目录后，系统将设置一个默认权限，可通过命令umask查看或设置系统默认的权限。umask用一个3位2进制数来指定，由命令的mask可看出这是要屏蔽部分权限。当创建文件时，文件的权限就设置为创建程序请求的任何权限去掉umask屏蔽的权限。

由于系统默认屏蔽的权限为022，因此新创建的目录权限就为 $777-022=755$ ，即新创建的目录的权限为755（用字符表示就是rwxr-xr-x），表示所有者具有所有权限，同组用户和其他用户具有读和执行权限，没有写的权限。新创建的普通文件权限为 $666-022=644$ ，即rw-r--r--。

## 2. 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。

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???)
```

### 3. 文件特殊权限

文件特殊权限有以下三种:

**SUID, SGID, SBIT**

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

例如: `ls -l /usr/bin/passwd`

注意: 当用户执行passwd命令的时候, 需要修改/etc/shadow文件。

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, 因此, /usr/bin/passwd的权限为4755。

2) **SGID: Set GID**

例如: `ls -l /usr/bin/locate`

注意: 当用户执行locate命令的时候, 需要读取/var/lib/mlocate/mlocate.db文件。

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, 因此, /usr/bin/locate的权限为2711。

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）

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，因此，/tmp的权限为1777。

#### 4. 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