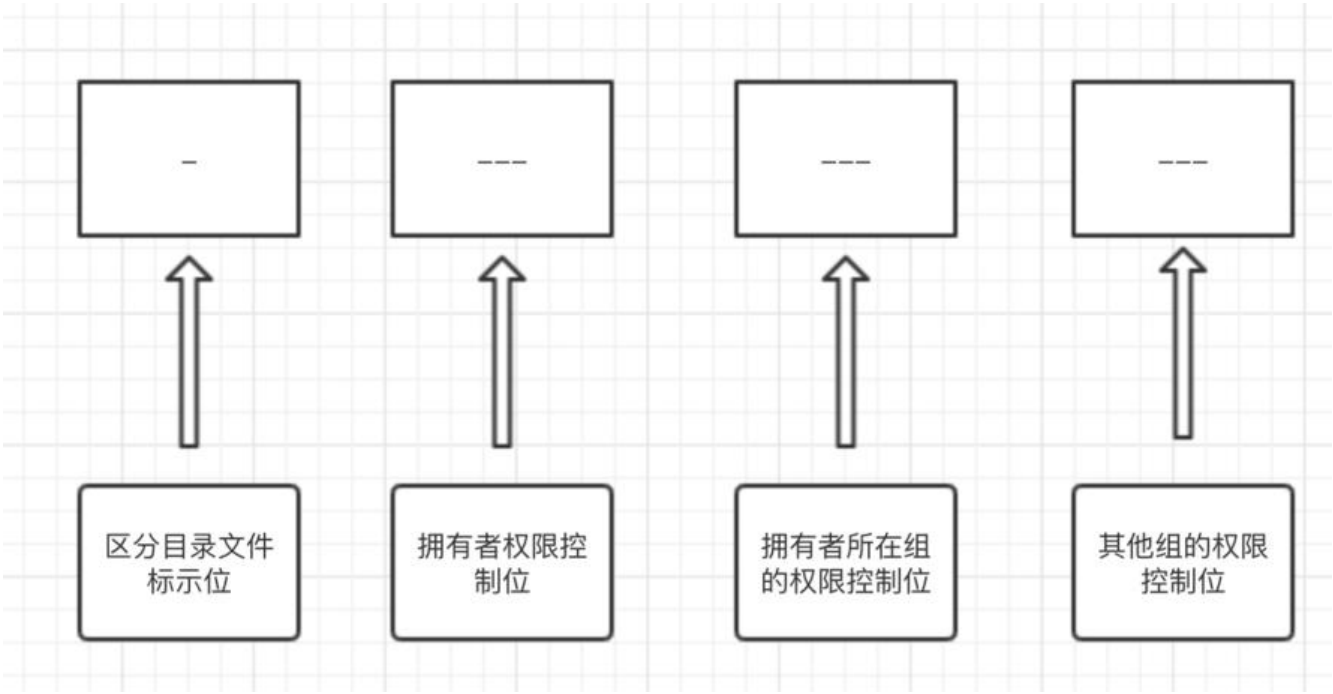
戏说 linux 文件权限

作者：yuanhenglizhen
原文链接：https://ld246.com/article/1574930558697
来源网站：链滴

很尴尬的一件事，之前一直没有去了解权限这部分的知识。一直在裸奔的边缘试探，偶然的机会看了《inux系统安全》这边书，顺便把这部分知识补上了。

linux的权限分为 10个标志位： ----------



文件标示位：

-

d标示此物体是个目录

-标示此物体是个文件

其他三个权限控制位：

- r=4 #读
- w=2 #写
- x=1 #执行

举个栗子：

一个权限为0755的文件显示如下

-rwxr-xr-x

有些人好奇这个0是什么意思，这是表示suid和guid的东西

- suid意味着如果某个用户对属于自己的shell脚本设置了这种权限，那么其他用户在执行这一脚本时会具有其属主的相应权限。
- guid则表示执行相应脚本的用户将具有该文件所属用户组中用户的权限

上诉例子设置了suid，那么其他任何用户的权限都是7

如果设置了guid，那么任何用户的权限都是5

如何设置suid和guid：

设置suid就是把0变为4

设置guid就把0变为2，如果都设置那就是6

一旦设置了这一位，一个s将出现在x位上。记住:在设置suid和guid的同时，相应的执行权限位必须要设置

chmod 4777 xxx.sh 设置了suid
chmod 2777 xxx.sh 设置了guid
chmod 6777 xxx.sh 同时设置了suid和guid
chmod 0777 xxx.sh 常规

附上一个对于rwx的说明图

表1-7 设置suid/guid

命 令	结 果	含 义
chmod 4755	rws r-x r-x	文件被设置了suid，文件属主具有读、写和执行的权限，所有其他用户具有读和执行的权限
chmod 6711	rws --s --s	文件被设置了suid和guid，文件属主具有读、写和执行的权限，所有其他用户具有执行的权限
chmod 4764	rws rw- r--	文件被设置了suid，文件属主具有读、写和执行的权限，同组用户具有读和执行的权限，其他用户具有读权限

最后理解起来也不是那么难，只是没有去做那件事情罢，和生活中的很多事情一样，你做和不做的结肯定是不一样的，而且你去做了这件事肯定有收获。

补充：

其实权限还有一位，少说了。因为我都是把selinux关掉了的。

直到测试ACL的时候才发现，**这个点表示的是存在“SELinux的安全标签”！**，如下图所示

```
[u1@ansible2 u1]$ mkdir 1
[u1@ansible2 u1]$ ll
总用量 0
drwxrwxr-x. 2 u1 u1  6 12月  3 23:01 1
drwxrwx---+ 3 u1 u1 17 12月  3 22:58 accounts
```