**[linux特殊权限SUID、SGID、SBIT](http://www.cnblogs.com/javaee6/p/4026108.html)**

对于linux中文件或目录的权限，应该都知道普通的rwx权限（关于linux中rwx权限的看我的这篇博文[http://www.cnblogs.com/javaee6/p/3994750.html](http://www.cnblogs.com/javaee6/p/3994750.html" \o "http://www.cnblogs.com/javaee6/p/3994750.html" \t "_blank)）。我们先看看下面两个的权限是什么

image

image

非常奇怪，/tmp目录和 passwd文件的权限怎么怪怪的，怎么有s和t权限呢。看了下面的内容你就明白了。

**1 SUID**

当s出现在文件拥有者的x权限上时,如我们上面看到的/usr/bin/passwd这个文件的权限时-rwsr-xr-x,此时就被称为SET UID简称SUID.SUID对于一个文件有什么限制和功能呢？

1. **SUID权限仅对二进制可执行文件有效**
2. 执行者对于该文件具有x的权限
3. 本权限仅在执行该文件的过程中有效
4. 执行者将具有该文件拥有者的权限

例如普通用户用passwd修改自己的命令，实际上最终更改的是/etc/passwd文件. 此文件时用户管理配置文件,只有root权限才能更改。

image

既然是root用户才拥有此权限，为什么我们可以通过passwd命令来修改密码呢，那这就要归功于passwd设置了suid权限位了。

image

此时普通用户通过执行passwd命令，临时拥有root权限，间接的修改/etc/passwd，以达到修改自己密码的权限。

**2 SGID**

当s出现在目录或文件所属群的x权限上时，此时就称为SET GID简称SGID,那SGID对文件和目录分部有哪些功能呢？

**2.1 SGID对目录**

1. 使用者若对于此目录具有 r 与 x 的权限时，该使用者能够进入此目录
2. 使用者在此目录下的群组将会变成该目录的群组
3. 若使用者在此目录下具有 w 的权限(可以新建文件)，则使用者所创建的新文件，该新文件的群组与此目录的群组相同

**2.2 SGID对文件**

1. SGID 对二进制可执行文件有效
2. 程式执行者对于该文件来说，需具备 x 的权限
3. 执行者在执行的过程中将会获得该文件群组的支援（用于改文件群组的权限）

**3 SBIT**

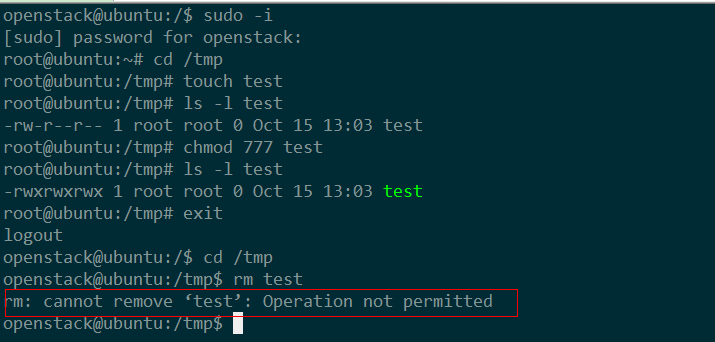
当s出现在目录其他用户的x权限上时，此时就称为Sticky Bit简称SBIT,那SBIT有哪些限制和作用呢?

1. 仅对目录有效，对文件无效
2. 当使用者在该目录下建立文件或目录时(有权限的情况下)，**仅自己与 root 才有权力删除新建的目录或文件**

我们知道/tmp目录是这样的权限。

image

现在我们来验证下，先用root账号在tmp文件中创建一个文件test,然后用openstack(其他账号)进入该目录,删除test文件，看看发生什么情况



我们看到这样是不能删除文件的。因为/temp目录有SBIT权限。

**4 怎么操作SUID、SBID、SBIT**

操作这些标志与操作文件权限的命令是一样的, 都是 **chmod**. 有两种方法来操作,

**(1)符号类型改变权限**

1. chmod u+s testbin-- 为testbin文件加上setuid标志.
2. chmod g+s testdir-- 为testdir目录加上setgid标志
3. chmod o+t testdir-- 为testdir目录加上sticky标志

**(2) 数字类型改变档案权限**

采用八进制方式. 对一般文件通过三组八进制数字来置标志, 如 666, 777, 644等. 如果设置这些特殊标志, 则在这组数字之外外加一组八进制数字. 如 4666, 2777等. 这一组八进制数字三位的意义如下,

**abc**

1. a - setuid位, 如果该位为1, 则表示设置setuid 4---
2. b - setgid位, 如果该位为1, 则表示设置setgid 2---
3. c - sticky位, 如果该位为1, 则表示设置sticky 1---

设置完这些标志后, 可以用 ls -l 来查看. 如果有这些标志, 则会在原来的执行标志位置上显示. 如

1. rwsrw-r-- 表示有setuid标志
2. rwxrwsrw- 表示有setgid标志
3. rwxrw-rwt 表示有sticky标志

**那么原来的执行标志x到哪里去了呢? 系统是这样规定的, 如果本来在该位上有x, 则这些特殊标志显示为小写字母 (s, s, t). 否则, 显示为大写字母 (S, S, T)**