linux rwt rwT rws rwS 特殊权限

2010-11-25 17:46:01

标签：rwS rwT rws linux rwt

众所周知，Linux的文件权限如: 777；666等，其实只要在相应的文件上加上UID的权限，就可以用到加权限人的身份去运行这个文件。所以我们只需要将bash复制出来到另一个地方，然后用root加上UID权限,只要用户运行此Shell就可以用用root的身份来执行任何文件了

一个文件都有一个所有者, 表示该文件是谁创建的. 同时, 该文件还有一个组编号, 表示该文件所属的组, 一般为文件所有者所属的组.

如果是一个可执行文件, 那么在执行时, 一般该文件只拥有调用该文件的用户具有的权限. 而setuid, setgid 可以来改变这种设置.

setuid: 设置使文件在执行阶段具有文件所有者的权限. 典型的文件是 /usr/bin/passwd. 如果一般用户执行该文件, 则在执行过程中, 该文件可以获得root权限, 从而可以更改用户的密码.

setgid: 该权限只对目录有效. 目录被设置该位后, 任何用户在此目录下创建的文件都具有和该目录所属的组相同的组.

sticky bit: 该位可以理解为防删除位. 一个文件是否可以被某用户删除, 主要取决于该文件所属的组是否对该用户具有写权限. 如果没有写权限, 则这个目录下的所有文件都不能被删除, 同时也不能添加新的文件. 如果希望用户能够添加文件但同时不能删除文件, 则可以对文件使用sticky bit位. 设置该位后, 就算用户对目录具有写权限, 也不能删除该文件.

下面说一下如何操作这些标志:

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) chmod u+s temp -- 为temp文件加上setuid标志. (setuid 只对文件有效)

chmod g+s tempdir -- 为tempdir目录加上setgid标志 (setgid 只对目录有效)

chmod o+t temp -- 为temp文件加上sticky标志 (sticky只对文件有效)

2) 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

a - setuid位, 如果该位为1, 则表示设置setuid

b - setgid位, 如果该位为1, 则表示设置setgid

c - sticky位, 如果该位为1, 则表示设置sticky

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

rwsrw-r-- 表示有setuid标志

rwxrwsrw- 表示有setgid标志

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)