Linux认证辅导:Linux特殊文件权限Linux认证考试 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/644/2021_2022_Linux_E8_AE_A4_E8_AF_c103_644855.htm 一般来说，使用过Linux的同学都知道，Linux文件的权限有rwx，所有者、所有组、其它用户的rwx权限是彼此独立的。为此，经常会听到如果某个web文件需要被修改的话，需要加上777的权限，这就是让所有用户可写。 但仔细一想，这样的权限未免有些想得比较天真，没有考滤特殊情况。例如/tmp目录默认权限是777，而且有些文件也是允许所有用户访问修改的，那么是不是任何一个用户都可以将这些删除呢？再如/etc/shadow保存的是用户密码文件，默认情况下它的权限是640，那么只有shadow的owner(root)才能修改它，按照常规理解，这是不可理解的，因为每个用户都可能修改密码，也就是会修改这个文件。 为了把这些情况解释清楚，需要引入Linux特殊文件权限的概念。Linux特殊文件权限有三个玩意：sticky bit、SGID、SUID，以下一一道来。 sticky bit sticky bit只对目录有效，使目录下的文件，只有文件拥有者才能删除（如果他不属于owner，仅属于group或者other，就算他有w权限，也不能删除文件）。 加sticky bit的方法： chmod o t /tmp或者 chmod 1777 /tmp 查看是否加了sticky bit，用ls -l，可以看到有类似这样的权限：“ -rwxrwxrwt ”，t就代表已经加上了sticky bit，而且生效了，如果显示的是“ -rwxrwxrwT ”，说明也已经加上了sticky bit，但没有生效（因为本来other就没有写的权限）。 看看/tmp目录的权限，就是drwxrwxrwt吧 SGID(The Set GroupID ) 加上SGID的文件，表示运行这个程序时，是临时以这个文件的

拥有组的身份运行的；加上SGID的文件夹，表示在这个目录下创建的文件属于目录所有的组，而不是创建人所在的组，在这个目录下创建的目录继承本目录的SGID。 加SGID的方法： chmod g s /tmp或 chmod 2777 /tmp 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com