Linux文件权限的设置技巧 PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/143/2021_2022_Linux_E6_96_87_E4_BB_c103_143859.htm Windows系统其实和Linux系统有相似的地方，Windows系统文件、目录的属性有只读、隐藏，而Linux也一样。 Linux中，每一个文件都具有特定的属性。主要包括文件类型和文件权限两个方面。可以分为5种不同的类型：普通文件、目录文件、链接文件、设备文件和管道文件。 所谓的文件权限，是指对文件的访问权限，包括对文件的读、写、删除、执行。Linux 是一个多用户操作系统，它允许多个用户同时登录和工作。因此 Linux 将一个文件或目录与一个用户或组联系起来。访问控制列表(ACL：Access Control List)为计算机提供更好的访问控制，它的作用是限制包括root用户在内的所有用户对文件、资源或者套接字的访问。下面就来教大家简单的设置方法。 步骤1 检查系统核心 首先检查你的Linux系统的核心是否有支持ACL的功能。因为Linux系统并不是每一个版本的核心都有支持ACL的功能，而最简单的方法就是检查系统目前的核心能否支持：
[root@mail /]# cat /boot/config-kernel-version | grep -i ext3
CONFIG_EXT3_FS=m CONFIG_EXT3_IDEX=y
CONFIG_EXT3_FS_XATTR_SHARING=y
CONFIG_EXT3_FS_XATTR_USER=y
CONFIG_EXT3_FS_XATTR_TRUSTED=y
CONFIG_EXT3_FS_ACL=y 此时如果能看到上面的几项则表示已经编译到核心中,ext3文件系统已支持ACL功能，这些功能在编译核心选项中都可以找到。如果编译时找不到，可以

到ACL的官方网站来安装Kernel(acl.bestbits.at/)。 步骤2 挂载分区 你可以用下列的方式挂载分区并启用ACL： #mount -t ext3 -o acl /dev/sda1 /fs1 你也可以直接写在/etc/fstab文件中,这样就可以在开机后支持ACL功能： #vi /etc/fstab 步骤3 设置ACL权限 ACL常常针对个别用户来进行设置，下面是多个不同的例子： 例如需要创建test1、test2、test3三个用户，可以先用root身份登录系统，然后执行以下命令分别创建三个用户名和密码： [root@mail root]#adduser test1 [root@mail root]#adduser test2 [root@mail root]#adduser test3 [root@mail root]#passwd test1 [root@mail root]#passwd test2 [root@mail root]#passwd test3 然后mount一个ext3文件到目录/fs1： [root@mail root]#mount -t ext3 -o acl /dev/sda1 /fs1 再将test1 建立的文件设置读写的权限给test2 ： [root@mail root]#chmod -R 777 /fs1 让所有的用户都能增加文件到目录的权限： 先用test1登录系统，执行命令： [test1@mail test1]# cd /fs1 [test1@mail fs1]# echo "Create by test1" > test1.txt [test1@mail fs1]# chmod go-r test1.txt [test1@mail fs1]# ll test1.txt -rw------- 1 test1 test1 17 Jul 14 22:11 test1.txt 而如下操作则可以让除了test1有读写的权限外其他人没有读写test1.txt的权限（root除外），先用test2 登录系统后执行以下命令： [test2@mail test2]# cd /fs1 [test2@mail fs1]# cat test1.txt cat : test1.txt Permission denied 接着用test1登录系统，执行如下命令： [test1@mail fs1]# setfacl -m u:test2:rw test1.txt 这样就修改权限允许test2 有这个文件的读写权限。再看一下它的文件属性的变化： [test1@mail fs1]# ll -rw-rw-r-- 1 test1 test1 10 Feb 16 13:52 test1.txt 会看到后面多了一个“ ”，表示这个文件使用ACL的属性设置，再用命令getfacl来看ACL的文件属性设置：

[test1@mail fs1]# getfacl test1.txt # file: test1.txt # owner: test1 # group: test1 user::rw- user:test2:rw- group::rw- mask::rw- other::r-- 可以看到 test2 有权限读写这个文件。 我们再用test2登录系统执行以下命令，看看发生了什么？ [test2@mail test2]# cd /fs1 [test2@mail fs1]# cat test1.txt Create by test1 原来test2可以读取test1.txt文件了。 [test2@mail fs1]# echo "Modify by test2" >> test1.txt [test2@mail fs1]# cat test1.txt Create by test1 Modify by test2 现在test2也可以修改test1.txt文件了。 接着用test3 登录系统： [test3@mail test3]# cd /fs1 [test3@mail fs1]# cat test1.txt cat : test1.txt Permission denied 嘿嘿，除了test1、test2外没有其他用户有读写test1.txt的权限（root 除外）。 看着虽然有点晕，其实命令就是这么一两条，主要是把各种情况给大家讲清楚，这样，大家在使用Linux中才会发现，比起脆弱的Windows的权限防护，Linux实在是做得相当不错！ 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