Linux文件系统ACLs权限控制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_E6_96_87_E4_BB_c103_644803.htm Linux文件系统给所有者（owner）、所有组（owning group）、其它（other）每一类用户分别定义了的rwx权限，且是彼此独立的。虽然Linux有也Linux特殊文件权限的功能支持，但要像在Windows下把权限控制可以精确到用户和组（如允许某个文件允许某一特殊用户修改，允许某一组的用户可以查看等）一样灵活，这些显然还不够。令人欣慰的是，Linux 也有ACLs权限控制的支持，在Linux中ACLs在ReiserFS,Ext2,Ext3,JFS,XFS等文件系统中受到支持。 修改文件ACL：setfacl -m u:tux:rw file 允许用户tux读写file文件 查看文件ACL：getfacl file 使用了ACL的文件，通过ls -l命令来查看权限时，后面会有一个“ ”号，group的权限会有变化（使用了ACL mask权限）。 文件使用ACL后，权限角色有如下几种类型： 最小化ACL： owning user owning group other 扩展ACL： 可以包含若干个对象：named user（设置单独用户的访问权限）、named group（设置单独群组的访问权限） 包含一个mask（限制named users 和 named groups的权限） 举例说明如下： owner user::rwx named user user:name:rwx owning group group ::rwx named group group :name:rwx mask mask::rwx other other::rwx 定义在owner、other里的权限一直都是有效的，其它权限可能用效或者被隐蔽。 named user与named group的值是否生效，还要看其值与mask的“ 与 ”值，即mask也要有该权限，才能生效。 mask的值一般是与owning group一致的，可以通过修改owning group的值

来修改mask。 举例说明如下：
linux-canbeing:/home/canbeing/temp # getfacl my # file: my # owner: canbeing # group: users user::rw- user:canbeing:rwx #effective:r-x w没有生效 group::r-- mask::r-x other::r-- 子目录会继承父目录的ACL。 如果父目录有ACL，则创建新文件或者文件夹时，默认权限不会根据umask来计算，而是继承或者根据命令参数。 使用setfacl -d -m u:canbeing:rw /tmp/acl_test/ 则此权限会得到子目录及文件的继承（权限以default开头）
linux-canbeing:/tmp/acl_test # getfacl /tmp/acl_test/ getfacl: Removing leading / from absolute path names # file: tmp/acl_test/ # owner: root # group: root user::rwx user:canbeing:rwx group::--- mask::rwx other::--- default:user::rwx default:user:canbeing:rw- default:group::--- default:mask::rw- default:other::--- 编辑特别推荐: Linux系统通过手机GPRS上网设置简介 提高Apache服务器性能的四个建议 Linux认证能帮助你找到一份好工作吗 linux面试题参考答案 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