

文件权限管理 - POSIXACL PDF转换可能丢失图片或格式，
建议阅读原文

https://www.100test.com/kao_ti2020/253/2021_2022__E6_96_87_E4_BB_B6_E6_9D_83_E9_c103_253023.htm 在 Unix/Linux 系统上沿用了多年的权限机制，由于欠缺灵活性，在现今的信息系统上显得落后和不敷应用。然而一个新的权限机制标准已经诞生出来，本文将为大家介绍这个新机制在 Linux 上的操作方式。传统上，在 Linux 系统中每个档案和目录都设有权限 (permission) 来决定那些人能够使用这个档案。权限分为三组，分别为：拥有者 (file owner)，群组 (group)，及其它 (other)。每组中再设有其属性。属性亦分为三种，分别为：读取 (read)，写入 (write)，及执行 (executable)。我们可以用 "ls -l" 来检视档案的权限：
-rwxrw-r-- 1 adam mis 272401 May 10 2003 report.doc
在上面的例子，档案 report.doc 的拥有者为 "adam" 而 adam 可以读取，写入和执行这个档案，另外 report.doc 的群组为 "mis"，在系统中所有属于 mis 群组的使用者皆可读取和写入这个档案，而其它的使用者只能够读取这个档案。如果我们想 report.doc 的内容只能给 mis 群组的使用者读取，我们可以用 "chmod 640 report.doc" 这个指令更改其权限。
-rw-r----- 1 adam mis 272401 May 10 2003 report.doc
要是 report.doc 这个档案同时要给 mis 和 hr 两个群组的使用者读取，现有的权限机制已不能够让我们简易地设定。我们得要劳烦系统管理员为我们加入一个新的群组 (i.e. mishr)，并把所有 mis 和 hr 中的使用者加进 mishr 群组中。然后我们要用 "chgrp mishr report.doc" 把群组设为 mishr。
-rw-r----- 1 adam mishr 272401 May 10 2003 report.doc
假若，我们的要求再复杂一点：

要让使用者 adam 和 eva 能读取和写入，群组 mis 和 hr 只能读取。那么，任我们再多加新的群组亦没办法得到这样的权限设定。要得到以上的权限设定，我们须要一个新的权限机制。而这个机制名为存取控制清单 (Access Control List，简称 ACL)。ACL 实为现有权限机制的延伸，在三个基本设定 (拥有者，群组及其它) 外，允许我们加入对某指定使用者或群组的存取权限设定。为针对 Unix 系统先天的不足，一个名为 POSIX ACL 的权限机制标准便诞生出来。其目的是为各 Unix 系统之间制定一个兼容的 ACL 标准，使各用家能在各系统之间使用统一的接口。这个 POSIX ACL 的功能在 Linux kernel 2.6 上被正式支持，之后又被 back-port 到 2.4 kernel 上。大家常用的档案系统，如：ext3，xfs，jfs，和 ReiserFS，都能使用 ACL。当然，大家须要在编译 kernel 时启动 ACL。相关的 kernel option：

`CONFIG_FS_POSIX_ACL`
`CONFIG_EXT3_FS_POSIX_ACL`

`CONFIG_EXT2_FS_POSIX_ACL` 挂上档案系统虽然在 kernel 中已加进了 POSIX ACL 的支持，但是并不会自动启用的。我们必须在挂上档案系统时指明要使用 ACL。例如：`mount -t ext3 -o acl /dev/sda1 /home` 当中 “`-o acl`” 便是在 `/dev/sda1` 上启用 ACL 的选项。我们亦可以在 `/etc/fstab` 中加入选项：

`/dev/sda1 /home ext3 acl 1 2` 检视 ACL 要检视一个档案或目录的 ACL，便要使用 “`getfacl`” 指令：`[adam@www adam]$ getfacl report.doc` # file: report.doc # owner: adam # group: mis

`user::rwgroup::rwother::r--` 以上的例子列出了一个基本的 ACL (Minimum ACL)。头三行为档案数据，当中包括了档案的拥有者和所属群组。之后的便是 ACL 中的每一条的规则。在这

个基本的 ACL 中： user::rw- 拥有者 adam 能读取和写入
group::rw- 属于 mis 群组的使用者能读取和写入 other::r-- 其它
的使用者只能读取 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