权限

我们已经知道了，文件的权限分为 r （可读）、 w （可写）、 x （可执行）三种类型，而一个文件可以针对归属用户，归属群组，其它用户或群组分别设定权限。

这种权限管理的方式灵活、简单、严密、明晰。尽管如此，在最初的阶段，可能会有一点小小的不适。因为它无所不在，而您习惯了的 Windows 的权限管理却不是这样（非常混乱，大多数时间形同虚设，偶尔用到却让人伤透脑筋）。

使用 chmod 命令更改文件的权限，使用 chown 来更改文件的归属。例如：

```
chmod 755 xxxchmod a+x xxxchown user:group xxx  #用来更改文件的归属用户，也可以同时更改其归属群组chgrp   gro
```

上面命令中的 755 和 a+x 是两种类型的表达式

我们将在"权限管理"一节中详细介绍

执行命令的权限

有一些命令，普通用户也可以执行，但是只有 root用户 才能执行成功，这是为什么呢？

例如在系统中增加一个新用户 useradd，我们看看这个命令的程序文件

```
ls -l /usr/sbin/useradd     -rwxr-xr-x 1 root root 56156 2006-04-03 21:37 /usr/sbin/useradd
```

所有的用户都可以执行？

这是因为， useradd 命令是修改 /etc/passwd 文件的一个工具，来看看这个文件：

```
ls -l /etc/passwd-rw-r--r-- 1 root root 1835 2006-06-24 17:58 /etc/passwd
```

原来只有 root用户 才能写入修改结果，非 root用户 执行 useradd 命令当然不会有结果。