

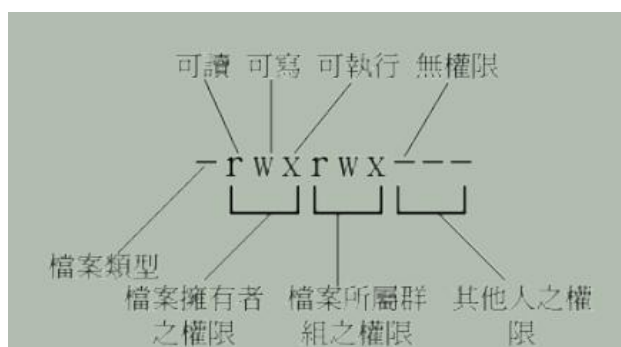
要从普通用户切换到 root 用户，只需要输入指令 su，回车，然后输入 root 账号的密码即可。输入指令 exit 即可回到普通用户登录

在 Linux 里面，任何一个档案都具有『User, Group 及 Others』三种身份的个别权限

ls 是『list』的意思，重点在显示档案的文件名的相关属性。而选项『-al』则表示列出所有的档案详细的权限和属性 (包括隐藏文件，就是文件名第一个字符为『.』的档案)。

```
drwxr-xr-x. 2 root root 4096 Mar  8 19:57 Desktop
drwxr-xr-x. 2 root root 4096 Mar  8 19:57 Documents
drwxr-xr-x. 2 root root 4096 Mar  8 19:57 Downloads
-rw-r--r-- 1 root root 16 Mar  8 19:57 esd_auth
```

1、第一栏代表这个档案的类型和权限(permission): drwxr-xr-x



第一个是 d，说明这是一个目录

如果是-，则说明是一个文件

*若是[l]则表示为连结档(link file);

若是[b]则表示为装置文件里面的可供储存的接口设备(可随机存取装置);

若是[c]则表示为装置文件里面的串行端口设备，例如键盘、鼠标(一次性读取装置)。

接下来有 9 个字符，以三个为一组，均为『rwx』的三个参数的组合。其中，[r]代表可读(read)、[w]代表可写(write)、[x]代表可执行(execute)（即可以进入该目录工作）。如果没有权限，就会出现减号[-]。

取上面的 Destop 为例

```
drwxr-xr-x. 2 root root 4096 Mar  8 19:57 Desktop
```

它是一个目录，

对于 User（拥有者）而言，它可读、可写、可执行；

对于 Group（同群组用户）而言，它可读、不可写、可执行；

对于 Others（其他用户）而言，它可读、不可写、可执行。

2、第二栏表示有多少档名连接到该节点（i-node）：2

*不是很懂

3、第三栏表示这个文件/目录的拥有者账号：root

- 4、第四栏表示这个文件的所属群组：root
- 5、第五栏表示这个文件的容量大小(bytes)：4096
- 6、第六栏表示建立日期或最近修改日期：Mar 8 19:57
- 7、第七栏表示文件名，如果文件名前有一个.，则说明这是一个隐藏文件

哇，很烦，这个虚拟机开的 CentOS，不能复制粘贴，甚至不能鼠标滑轮上下移动。于是换用 XShell 远程连接：

<https://jingyan.baidu.com/article/36d6ed1f7520991bcf4883e6.html>

根目录下的 ls 是这样的：

```
[root@localhost /]# ls
bin  dev  home  lib64  media  opt  root  sbin  sys  usr
boot  etc  lib  lost+found  mnt  proc  run  srv  tmp  var
```

而之前我们一直都在 root 文件夹里，

```
[root@localhost ~]# ls
anaconda-ks.cfg  Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos
```

而如果是 Ray 账户登录的，则根目录的 ls 是这样的：

```
[Ray@localhost ~]# ls
linuxide  lost+found  Ray
```

如何改变文件属性和权限

- 1、改变所属群组：chgrp (change group)

但是要改变的组名，要在/etc/group 里存在，否则错误提示找不到这个群组

```
[root@localhost ~]# vi haha.txt
[root@localhost ~]# chgrp users haha.txt
[root@localhost ~]# chgrp testgroup haha.txt
chgrp: 无效的组: "testgroup"
```

创建一个 txt 文件，改变其群组为 users，成功，改变其群组为 testgroup，失败，因为没有这个群组。

```
-rw-r--r--. 1 root users 9 3月 11 22:42 haha.txt
```

同样方法，又改回来：

```
-rw-r--r--. 1 root root 9 3月 11 22:42 haha.txt
```

- 2、改变文件拥有者：chown (change owner)

比如上面的 haha.txt 本来的拥有者是 root

现在 [root@localhost ~]# chown Ray haha.txt

```
-rw-r--r--. 1 Ray root 9 3月 11 22:42 haha.txt
```

确实有时候需要变更文件拥有者，比如复制文件给其他人时，使用 cp 指令：

cp 来源档案 目标文件

```
[root@localhost ~]# cp haha.txt haha_copy.txt
```

```
-rw-r--r--. 1 root root 9 3月 11 22:56 haha_copy.txt
-rw-r--r--. 1 root root 9 3月 11 22:42 haha.txt
```

所有属性权限都复制了原有文件的，这样就算交给其他用户他也无法读写文件，于是就需要 `chown` 和 `chgrp` 了

比如我把这个文件复制到 Ray 用户的文件夹下(Ray 用户登录时没权限进入 root 文件夹，所以直接把 root 文件夹下的这个文件复制过去测试)

```
[root@localhost ~]# cp haha_copy.txt /home/Ray
[root@localhost ~]# cd /home/Ray
[root@localhost Ray]# ls
Desktop Documents Downloads haha_copy.txt Music Pi
```

然后在虚拟机上用 Ray 账号登录，尝试打开这个文件

```
-- INSERT -- W10: Warning: Changing a readonly file
```

打开成功，但是提示只能读不能写

然后又回到 root 模式，使用 `chown`:

```
[root@localhost Ray]# chown Ray haha_copy.txt
```

```
-rw-r--r--. 1 Ray root 9 3月 11 23:00 haha_copy.txt
```

再次打开，已经没有 warning 了

```
"haha_copy.txt" 1L, 9C
```

3、改变权限: `chmod`

各权限的分数对照表如下: `r:4 w:2 x:1`

每种身份(owner/group/others)各自的三个权限(r/w/x)分数是需要累加的，例如当权限为:

`[-rwxrwx---]` 分数则是:

`owner = rwx = 4+2+1 = 7`

`group = rwx = 4+2+1 = 7`

`others= --- = 0+0+0 = 0`

那如果要将权限变成『 `-rwxr-xr--` 』呢? 那改权限的分数就成为

`[4+2+1][4+0+1][4+0+0]=754` 啰! 所以你需要下达『 `chmod 754 filename` 』

如果有些文件你不希望被其他人看到，那举应该将档案的权限设定为例如:『 `-rwxr-----` 』，那就下达『 `chmod 740 filename` 』吧!

比如将一个文件的全部权限都开启:

```
[root@localhost ~]# chmod 777 haha_copy.txt
```

```
-rwxrwxrwx. 1 root root 9 3月 11 22:56 haha_copy.txt
```

则所有用户都能读写和执行

```
[root@localhost ~]# chmod 740 haha_copy.txt
```

```
-rwxr-----. 1 root root 9 3月 11 22:56 haha_copy.txt
```

另外的方法，我倒是觉得这个更好：

假如是『 -rwxr-xr-- 』这样的权限呢？可以使用『 `chmod u=rwx,g=rx,o=r filename` 』

```
[root@localhost ~]# chmod u=rwx,g=rx,o=x haha.txt
```

```
-rwxr-x--x. 1 root root 9 3月 11 22:42 haha.txt
```

chmod	u	+(加入)	r	档案或目录
	g	-(除去)	w	
	o	=(设定)	x	
	a			

比如说在上面权限的基础上，全部去掉 x（执行）权限：

```
[root@localhost ~]# chmod a-x haha.txt
```

```
-rw-r-----. 1 root root 9 3月 11 22:42 haha.txt
```

又或者全部加上 w 权限：

```
[root@localhost ~]# chmod a+w haha.txt
```

```
-rw-rw--w-. 1 root root 9 3月 11 22:42 haha.txt
```

又或者单独去掉 others 的 w 权限：

```
[root@localhost ~]# chmod o-w haha.txt
```

```
-rw-rw----. 1 root root 9 3月 11 22:42 haha.txt
```

目录和文件的权限意义

对于文件：

r (Read): 可读取此一档案的实际内容，如读取文本文件的文字内容等；

w (Write): 可以编辑、新增或者是修改该档案的内容(但不含删除该档案)；

x (eXecute): 该档案具有可以被系统执行的权限

Windows 底下一个文件是否具有执行的能力是藉由『 扩展名 』来判断的，例如：.exe, .bat, .com 等能执行；

但是在 Linux 底下，我们的文件是否能被执行，则是藉由是否具有『x』这个权限来决定的！跟文件名没有绝对的关系

对于目录：

r (read contents in directory): 当你具有读取(r)一个目录的权限时，表示你可以查询该目录下的文件名数据，所以你就可以利用 `ls` 这个指令将该目录的内容列表显示出来！

w (modify contents of directory): 代表拥有以下这些权限：

- 1、建立新的文件和目录；
- 2、删除已经存在的文件和目录(无论该文件有什么权限)
- 3、重命名文件或目录

4、搬移该目录内的文件、目录位置。

x (access directory):

目录不可以被执行，目录的 **x** 代表的是用户能否进入该目录工作！所谓的工作目录 (work directory) 就是你目前所在的目录啦！比如，当你登入 Linux 时，你所在的家目录就是你当下的工作目录。而变换目录的指令是『cd』 (change directory) 啰！

比如说，root 这个文件夹的权限如下

```
drwx-----. 2 root root 16384 Mar 7 20:00 lost+found
```

则只有在 root 账号登录的情况下才能进入该目录

如果你在某目录下不具有 **x** 的权限，那么久无法切换到该目录下，也无法执行该目录下的任何指令，即使具有该目录的 **r** 权限。

架设网站时，有的人开放目录数据给网上的任何人浏览，但却只开放 **r** 的权限，结果导致网站服务器软件无法到该目录下读取文件（最多只能看到文件名）。因此，如果要开放目录给任何人浏览，至少基于 **r**、**x** 权限，而 **w** 权限不能随便给。

我们用 root 的身份在所有人都是可以工作的/tmp 目录中建立一个名为 testing 的目录，该目录的权限为 744 且目录拥有者为 root。另外，在 testing 目录下在建立一个空的文件，文件名亦为 testing。建立目录可用 mkdir(make directory)

```
[root@localhost tmp]# mkdir testing
```

```
drwxr-xr-x. 2 root root 4096 3月 12 23:47 testing
```

```
[root@localhost testing]# touch testing/testing
```

```
[root@localhost tmp]# ls -al testing
总用量 8
drwxr-xr-x. 2 root root 4096 3月 12 23:51 .
drwxrwxrwt. 25 root root 4096 3月 12 23:47 ..
-rw-r--r--. 1 root root 0 3月 12 23:51 testing
[root@localhost tmp]# chmod g-r,o-r testing/testing
[root@localhost tmp]# ls -al testing
总用量 8
drwxr-xr-x. 2 root root 4096 3月 12 23:51 .
drwxrwxrwt. 25 root root 4096 3月 12 23:47 ..
-rw-----. 1 root root 0 3月 12 23:51 testing
[root@localhost tmp]#
```

```
[root@localhost tmp]# chmod g-x,o-x testing/testing
```

```
drwxr--r--. 2 root root 4096 3月 12 23:51 testing
```



```
[root@www tmp]# ls -ald testing/testing
drwxr--r-- 2 root root 4096 Sep 19 16:01 testing
-rw----- 1 root root  0 Sep 19 16:01 testing/testing
# 仔细看一下，目录的权限是 744，且所属群组与使用者均是 root 喔！
# 那么在这样的情况下，一般身份用户对这个目录/档案的权限为何？
```

然后用一般用户登录

```
[Ray@localhost ~]$ cd /tmp
[Ray@localhost tmp]$ ls -l testing
ls: 无法访问testing/testing: 权限不够
总用量 0
-???????? ? ? ? ? ? testing
```

因为具有 r 的权限可以查询 testing 目录下的文件名。不过权限不足(没有 x)，所以会有一堆问号。

```
[Ray@localhost tmp]$ cd testing
-bash: cd: testing: 权限不够
```

因为没有 x 权限，因此进不去

也就是说，目录的 r 权限能让用户读取目录的文件名列表，但详细信息读不到，同时也不能将此目录变为工作目录（不能 cd 进入）

尝试将 testing 目录拥有者变为 Ray，看 Ray 能不能在此目录下删除文件（按道理是可以的）

```
[root@localhost tmp]# chown Ray testing

drwxr--r--. 2 Ray root 4096 3月 12 23:51 testing
```

```
[root@localhost tmp]# su Ray
[Ray@localhost tmp]$ cd testing
[Ray@localhost testing]$
```

能够进入该目录了

```
[Ray@localhost testing]$ ls -l
总用量 0
-rw----- 1 root root 0 3月 12 23:51 testing
```

也能看到该目录下的文件名

```
[Ray@localhost testing]$ rm testing
rm: 是否删除有写保护的普通空文件 "testing"?
[Ray@localhost testing]$ ls -l
总用量 0
```

也能删除掉该文件

Linux 文件种类和扩展名：

任何装置在 Linux 底下都是文件

除了前面提到的一般文件(-)和目录文件(d)之外，还有哪些种类的文件呢？

正规文件(regular file): 就是 ls -al 显示出来的第一个属性为-

目录(directory): 第一个属性为 d

连接档(link): 第一个属性为 l, 相当于快捷方式

设备与装置文件(device):

与系统周边及存储等相关的一些文件, 通常都在/dev 目录下, 有以下两种:

1、区块(block)设备文件: 软盘、硬盘等, 一些存储数据, 以提供系统随机存取的接口设备。/dev/sda 第一个属性为 b:

```
brw-rw----. 1 root disk      8,  0 3月 13 12:13 sda
brw-rw----. 1 root disk      8,  1 3月 13 12:13 sda1
```

2、字符(character)设备文件: 一些串行端口的接口设备, 如键盘、鼠标等, 这些设备特点是“一次性读取”, 不能截断输出。

数据接口文件(socket): 用于网络上的数据承接。我们可以启动一个程序来监听客户端的请求(当前的这部 linux 机是服务器), 然后通过这个 socket 来进行数据的沟通。第一个属性为 s, 在/var/run 目录下

数据输送文件(FIFO): 用以解决多个程序同时存取同一个文件造成的错误问题。

在 Linux 底下, 只要你的权限当中具有 x 的话, 例如[-rwx-r-xr-x] 即代表这个文件可以被执行。x 代表这文件具有可执行的能力, 但是能不能执行成功, 当然就得要看该文件的内容。

而扩展名虽然不能决定能否被执行, 但仍可以通过扩展名知道这文件是什么东西。

.sh 脚本或批处理文件(scripts)

.Z .tar .tar.gz .zip .tgz 压缩文件

.html .php 网页相关文件

在 Linux 底下, 使用预设的 Ext2/Ext3 文件系统时, 针对文件的文件名长度限制为:

单一文件或目录的最大容许文件名为 255 个字符;

包含完整路径名称及目录 (/) 的完整文件名为 4096 个字符

Linux 目录配置的依据--FHS

FHS 的重点在于规范每个特定的目录下应该要放置什么样子的数据

	可分享的(shareable)	不可分享的(unshareable)
不变的(static)	/usr (软件放置处)	/etc (配置文件)
	/opt (第三方协力软件)	/boot (开机与核心档)
可变动的(variable)	/var/mail (使用者邮件信箱)	/var/run (程序相关)
	/var/spool/news (新闻组)	/var/lock (程序相关)

事实上, FHS 针对目录树架构仅定义出三层目录底下应该放置什么数据而已, 分别是底下这三个目录的

定义:

/ (root, 根目录): 与开机系统有关;

/usr (unix software resource): 与软件安装/执行有关;

/var (variable): 与系统运作过程有关。

根目录 (/) 的意义:

最重要的目录, 所有目录都由根目录衍生而来, 根目录还与 (开机/还原/系统修复) 等有关。FHS 要求根目录所在分隔槽越小越好, 且应用程序安装的软件不要与根目录放同一个分隔槽。因为分隔槽里数据越多, 可能发生的错误就越多。

根目录下的次目录:

/bin 放置的指令恶意被 root 和一般用户使用

/boot 放置开机会用到的文件

/dev 任何装置和接口设备都以文件形态存在于此

/etc 系统主要的配置文件 (账号密码文件、服务启动文件等等, 这些文件一般可以让一般用户查阅, 但只有 root 能修改)

/home 系统默认的用户家目录, 每次新增一般用户, 其默认用户家目录都在这里

/lib 开机时用到的函式库

/media 可移除的装置如软盘、光盘等

/opt 给第三方协力软件放置的目录

/root 系统管理员 (root) 的家目录, root 的家目录和根目录放置在同一个分割槽中

/sbin 开机过程所需要的, 包括了开机、修复、还原系统等指令

/srv 一些网络服务启动后, 这些服务所需要取用的数据目录, 比如 WWW 服务器所需的网页资料就放在/srv/www/里面

/tmp 让一般用户或者正在执行的程序暂时放置文件的地方, 这个目录是任何人都能存取的, FHS 建议开机时将/tmp 目录下的数据都删除

/lost+found 文件系统发生错误时, 将遗失的片段放在此目录下

/proc 这个目录是一个“虚拟文件系统”, 他放置的数据都在内存当中

/sys 也是虚拟文件系统, 主要也是记录与核心相关的信息。

根目录与开机有关, 开机过程中仅有根目录会被挂载, 其他分隔槽会在开机完成后才挂载。即与开机过程有关的目录和文件必须放在根目录下, 这些目录有:

/etc 配置文件

/bin 重要执行文件

/dev 装置文件

/lib 执行文件所需的函式库和核心所需的模块

/sbin 重要的系统执行文件

以上这些目录必须放置在根目录下

/usr: 里面放置的数据属于可分享的、不可变动的, /usr 可以分享给局域网内的其他主机使用。

/usr 是 Unix Software Resource(Unix 操作系统软件资源)的缩写, 所有系统默认的软件都会放置在/usr 下, 因此类似于 Windows 系统的“C:\Program files 和 C:\Windows\”。

/usr/local/ 系统管理员在本机自行安装自己下载的软件时一般安装到这个目录下。

/var:

对比于/usr 是安装时占用较大硬盘容量的目录，/var 是系统运作后才组件占用硬盘容量的目录，因为此目录下主要有常态性变动的文件（cache、log file 等）

根据 FHS，最好将/var 独立出来，因为当/var 死掉时根目录还可以工作，能进入救援模式

你目前在/home 这个目录下，如果想要进入 /var/log 这个目录时（/home 和/var 是同一级的目录），可以这样写：

1. cd /var/log (absolute)
2. cd ../var/log (relative)

如何先进入/var/spool/mail/目录，再进入到/var/spool/cron/目录内？

答：由于/var/spool/mail 和/var/spool/cron 是同样在/var/spool/目录中，因此最简单的指令下达方法为：

1. cd /var/spool/mail
2. cd ../cron

『./』代表『本目录』的意思，所以『./run.sh』代表『执行本目录下，名为 run.sh 的文件』