第5章 Linux文件(目录)访问权限

5.1 实验目的

(1) 理解Linux系统中文件、目录、文件系统的概念和特点。
(2) 掌握Linux系统中常用文件的操作命令的使用方法。
(3) 掌握Linux文件和目录的访问权限设置的方法。

5.2 实验环境

一台已安装好VMware软件的主机,虚拟机系统为CentOS 7。

5.3 预备知识

5.3.1 Linux文件系统

Linux文件系统采用带链接的树形结构,即只有一个根目录(通常用"/"表示),根目录中含有下级子目录或文件的信息;子目录中又可含有下级的子目录或文件的信息,……这样一层一层地延伸下去,构成一棵倒置的树,如图5-1所示。

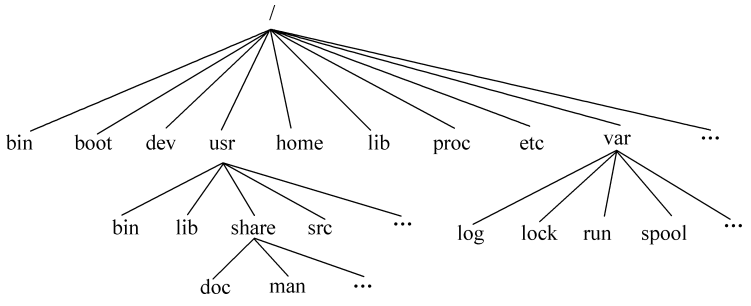

图5-1 Linux的目录树结构示意

在Linux系统中,在用ls命令查看文件时,文件名颜色不同,代表文件类型也不一样,如图5-2所示。可以用"dircolors -p"命令查看默认的颜色设置,包括各种颜色、粗体、下画线和闪烁等的定义(配置文件为/etc/DIR_COLORS)。通常,蓝色表示目录;绿色表示可执

行文件；红色表示压缩文件；浅蓝色表示超链接文件；灰色表示其他文件；红色闪烁表示链接的文件有问题。

```
filesystems             nsswitch.conf.bak          sysctl.conf
firewalld               oci-register-machine.conf  sysctl.d
fstab                   oci-umount                 systemd
fuse.conf               oci-umount.conf            system-release
gcrypt                  openldap                   system-release-cpe
gdbinit                 opt                        tcsd.conf
gdbinit.d               os-release                 terminfo
GeoIP.conf              pam.d                      tmpfiles.d
GeoIP.conf.default      passwd                     tuned
gnupg                   passwd-                    udev
GREP_COLORS             pkcs11                     vconsole.conf
groff                   pki                        vimrc
group                   plymouth                   virc
group-                  pm                         vmware-tools
grub2.cfg               polkit-1                   wpa_supplicant
grub.d                  popt.d                     X11
gshadow                 postfix                    xdg
gshadow-                ppp                        xinetd.d
gss                     prelink.conf.d             yum
host.conf               printcap                   yum.conf
hostname                profile                    yum.repos.d
hosts                   profile.d
hosts.allow             protocols
```

图 5-2　文件查看显示示意

5.3.2　Linux 文件属性

在文件管理中，操作系统会给文件设置各种属性信息，因为在 Linux 系统内部，文件系统对文件的管理是通过对文件的属性信息的管理来完成的。使用命令 ls -l 可以查看文件属性信息，如图 5-3 所示。

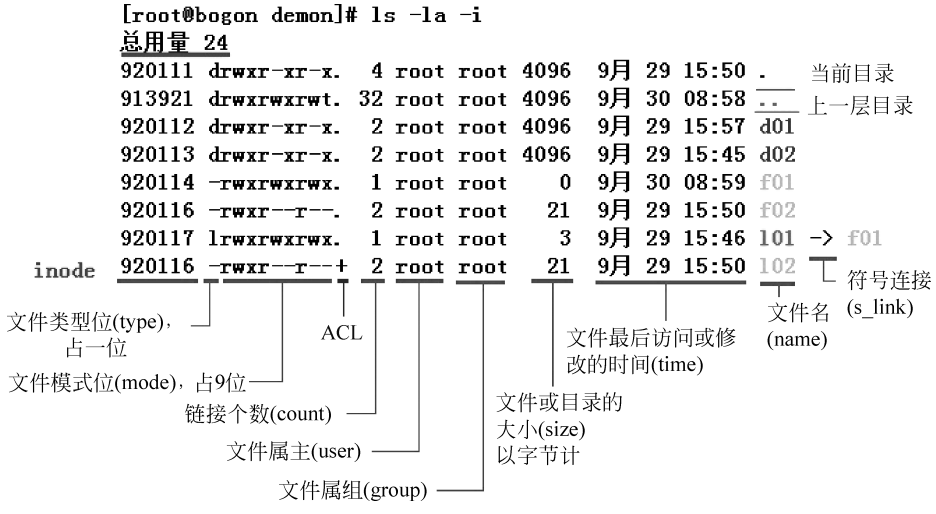

图 5-3　文件属性查看示意

1. 文件命名规则

在 Linux 系统中，每一个文件或目录的文件名最长可以达到 255 个字符(127 个中文字符)，若加上完整路径时，则最长可达到 4096 个字符。命名有如下规则：

(1) 大小写敏感。

(2) 通常文件名使用的字符包括：字母、数字、“.”(点)、“_”(下画线)和“-”(连字符)。

(3) 除了“/”之外，所有的字符都合法。

(4) 避免使用加号、减号或者点“.”作为普通文件的第一个字符。文件名开头为点时，表示该文件为隐藏文件。

(5) 避免使用 * ? > < ; & ! [ ] | \ ' " ` ( ) { } 等符号，因其在文件处理时具有特殊的意义，如：

① * 表示匹配 0 个或多个任意字符。

② ? 表示匹配任意一个字符。

③ [ ]表示匹配任何包含在括号里的单个字符，如 file1.txt、file2.txt。若要删除 file1 和 file2，则可以写为 rm file[12].txt。

2. Linux 常用文件类型

Linux 的常用文件类型如表 5-1 所示。

表 5-1 Linux 的常用文件类型

文件类型	标志	说明
普通文件	—	纯文本文档(ASCII 码)、二进制文件(binary)、数据格式文件(data)
目录文件	d	在 Linux 中目录是一个比较特殊的文件
符号链接文件	l	符号链接(软链接)，可以创建跨不同文件系统的链接
硬链接文件	—	只能面向同一文件系统的链接文件

除了以上几种类型文件外，还有字符设备文件(c)、块设备文件(b)、套接字文件(s)和命名管道文件(p)。

3. 文件的保护属性

Linux 采用存取控制表(Access Control Lists，ACL)机制，可把用户和文件的关系定为以下 3 类。

(1) 第一类是文件所有者(文件主)，即创建文件的人。

(2) 第二类是同组用户，即几个有某些共同关系的用户组成的集合。

(3) 第三类是其他用户。

Linux 把文件权限也分为以下 3 类。

(1) 第一类是可读，用 r 表示。

(2) 第二类是可写，用 w 表示。

(3) 第三类是可执行，用 x 表示。

用户和文件权限的方式如图 5-4 所示。图 5-4 所示的详细解释描述如表 5-2 所示。

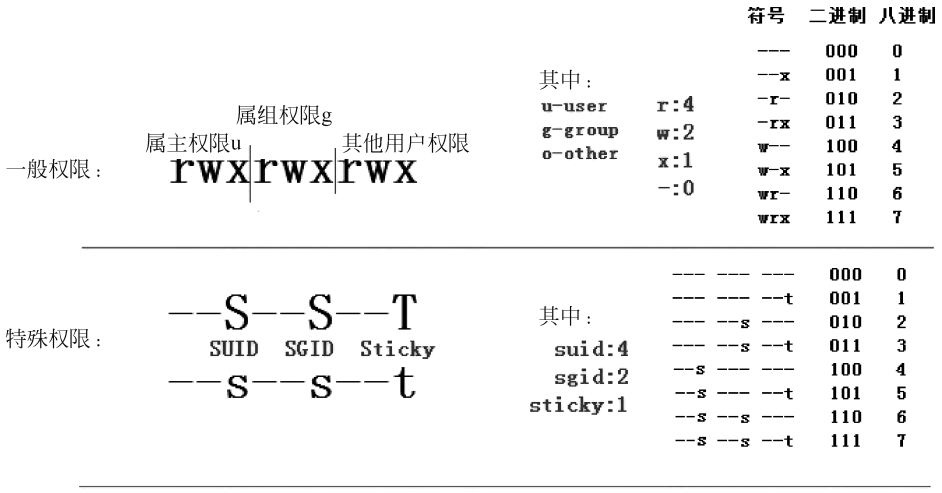

图 5-4　用户和文件权限示意

表 5-2　文件权限描述信息表

类型	权　　限	说　　明
一般权限	r(Read,读取)	对文件而言,具有读取文件内容的权限；对目录来说,具有浏览目录的权限
	w(Write,写入)	对文件而言,具有新增、修改文件内容的权限；对目录来说,具有删除、移动目录内文件的权限
	x(eXecute,执行)	对文件而言,具有执行文件的权限；对目录来说,具有进入目录的权限
特殊权限	s 或 S(SUID,Set UID)	用于可执行文件的设置。任何用户在执行该文件时,将获得该文件属组的身份
	s 或 S(SGID,Set GID)	用于可执行文件的设置。任何用户在执行该文件时,将获得该文件属组的身份
	t 或 T(Sticky,粘贴位)	通常对目录权限设置而言,一个目录开启了粘着位,在其目录下用户只能管理自己的目录/文件,而不能删除其他用户的文件
ACL	访问控制列表	是 Linux 系统权限额外支持的一项功能,需要文件系统的支持(查看命令 # mount)。主要是针对单一用户、单一文件或目录进行 rwx 权限的额外设定

5.3.3　常用文件操作命令

表 5-3 所示的是文件或者目录操作中常用的一些命令及其说明,希望读者能够熟记并掌握其使用。

表 5-3　常用文件操作命令一览表

命令	说　明
ls 或 dir	ls 和 dir 使用相同，只是 dir 显示的信息没有颜色区分。列举目录下所有的文件及其详情
cd	change directory：cd [目的目录]，如：＃cd /tmp/demon 进入目录/tmp/demon
touch	touch[-acm][文件名]，改变文件的时间戳，或者新建一个不存在的文件
pwd	print working directory，直接输入命令查看工作目录的绝对路径
mkdir	mkdir [-p][-m <目录属性>][目录名称]，创建一个或多个目录
rm	rm[-dfirv][文件或目录…]，删除文件或目录
rmdir	rmdir[-p][目录...]，删除一个或多个空目录
vi	vi 文本编辑器
echo	echo[-ne][字符串]，在终端显示信息
cp	cp[选项][源文件][目标文件]，复制文件
mv	mv[选项][源文件][目标文件]，移动文件
find	find path expression，根据文件的属性进行查找，如文件名、文件大小、所有者、所属组、是否为空、访问时间、修改时间等。如＃find / -name ‘f00＊’，在根目录下查找出文件开头名为 f00 的所有文件
ln	ln[选项][源文件][目标文件]，为源文件创建一个链接
cat	cat[选项列表][文件列表]…，连接文件并在标准输出上输出
more	more[选项][文件]，类似 cat，但可以进行前、后翻页显示，查找字符，如按空白键(space)就往下一页显示，按 b 键就会往上一页显示，输入“/”和字符在文中搜寻
less	less[选项][文件]，和 more 相似，但可以前后自由地移动阅读
chmod	chmod[选项][权限设置]文件或目录，改变文件的访问权限。 如：＃chmod u＝rwx，g＝rx，o＝r t001.txt 等同于＃chmod 754 t001.txt 设置文件权限为属组可以读写执行，属组用户可以读执行，而其他用户只能读。 ＃chmod 1754 t001.txt 设置文件粘贴位
chown	chown[参数][属主]：[组]文件或目录，修改文件所有者和组别。 如：＃chown testor t001.txt，只改变文件的属主；＃chown：test t001.txt，只改变属组 ＃chown testor：test t001.txt，同时改变属主与属组
chgrp	chgrp[参数][属组][文件或目录…]，改变文件的组所有权。 如：＃chgrp test t001.txt，改变文件的属组
umask	umask[-p][-S][mode]，将用户创建文件的掩码设置为 mode。如果 mode 以数字开始，它被解释为一个八进制数；否则被解释为类似于 chmod 中接收的符号形式的模式掩码。如果忽略了 mode，那么将打印当前掩码值。选项-S 使得掩码以符号形式打印；默认输出是八进制数。如果给出了-p 选项，并且忽略了 mode，那么输出将是一种可以重用为输入的形式
getfacl	getfacl　[选项]文件或目录，得到文件的访问控制列表(ACL)
setfacl	setfacl[选项][权限]文件或目录，设置或删除 ACL 权限。如： ＃setfacl -m u：testor02：rw t001.txt，赋予用户 testor02 读写的权限； ＃setfacl -m g：test：rw t001.txt，赋予用户组 test 读写的权限； ＃setfacl -x u：testor02 t001.txt，删除用户 testor02 的 ACL 权限； ＃setfacl -b t001.txt，删除所有设定的 ACL 权限

5.4 实验步骤

5.4.1 查看和修改文件的权限

在/root目录下,有一个文件anaconda-ks.cfg(如果没有,可以自己创建),使用ls的长格式命令可以查看其权限,使用chmod命令可以修改其权限。如表5-4所示为文件权限查看与修改操作命令,并完成表中空格的内容。

表5-4 文件权限查看与修改操作命令

操作目的	文件拥有者	文件所属组	其他用户	操作命令
查看anaconda-ks.cfg的权限				
使用字符修改法将文件拥有者、文件所属组、其他用户均设置为可读、可写、可执行	rwx	rwx	rwx	
使用字符修改法将文件所属组去掉执行权限、其他用户去掉可写、可执行权限	rwx	rw-	r--	
使用数字的方式将文件拥有者设置为可读、可写、可执行,文件所属组、其他用户均无权限	rwx	---	---	
使用数字的方式将文件拥有者设置为可读、可写,文件所属组、其他用户均为可读	rw-	r--	r--	

5.4.2 用户和用户组权限设置测试

系统中有group1和group2两个组。其中,group1中有普通用户user1和user2;group2组中有普通用户user3;用户user1在自己的家目录中创建文件a.txt。用户组、用户和文件之间的关系如表5-5所示。

表5-5 用户、用户组及文件关系表

用户组	权限用户	文件
group1	user1,user2	/home/user1/a.txt,由用户user1创建
group2	user3	

操作步骤如下:

(1) 创建用户组group1,group2。

参考命令:groupadd。

(2) 创建用户并将用户加入组中。

参考命令:useradd、passwd。

(3) 使用账户user1登录系统,在家目录/home/user1中新建文件a.txt,并编辑文件的内容(具体内容自定)。

参考命令:cd,ls,touch或vi。

(4) 修改用户家目录/home/user1的权限,增加同组和其他人都可以读和执行的权限。

参考命令:chmod。

(5) 用账号 user2、user3 分别登录系统，测试文件 a.txt 是否可读、可写。

参考命令：su，vi，cat。

(6) 切换到账户 user1，改变文件 a.txt 权限，使用户 user2、user3 对文件 a.txt 有读写权限。

参考命令：chmod。

(7) 用账号 user2，user3 分别登录系统，测试文件 a.txt 是否可读、可写。

参考命令：su，vi，cat。

(8) 切换到 root 用户，修改文件 a.txt 的属主为 user2。

参考命令：chown。

5.5 思考与练习

Linux 系统中使用 chmod 命令改变指定文件访问权限的方式有哪些？