一、环境准备

开启CentOS7虚拟机

二、基本权限和归属

•基本权限访问权限

–读取：允许查看内容-read 利用字母r表示

–写入：允许修改内容-write 利用字母w表示

–可执行：允许运行和切换-excute 利用字母x表示

针对文本文件：

r：cat less head tail

w：vim > >>

x: 学习Shell脚本

•归属关系

–所有者：拥有此文件/目录的用户-user u

–所属组：拥有此文件/目录的组-group g

–其他用户：除所有者、所属组以外的用户-other o

zhangsan zhangsan组 1.txt

•查看权限：执行 ls  -l .. .. 命令查看

[root@localhost ~]# ls -l /etc/passwd

-rw-r--r--. 1 root root 3446 6月 5 17:14 /etc/passwd

权限位   硬连接数   属主   属组   大小   最后修改时间   文件/目录名称

以-开头：文本文件

以d开头：目录

以l开头：快捷方式

在根目录下，默认情况/tmp目录具备特殊权限

[root@localhost ~]# ls -l /etc/passwd

[root@localhost ~]# ls -l /etc/shadow

[root@localhost ~]# ls -ld /etc

[root@localhost ~]# ls -ld /root

[root@localhost ~]# ls -ld /tmp

[root@localhost ~]# ls -ld /home/lisi

三、修改权限

•chmod命令

–格式：chmod  [ugoa][+-=][rwx]  文件...

•常用命令选项

– -R：递归修改权限

[root@localhost ~]# mkdir /nsd02

[root@localhost ~]# ls -ld /nsd02

[root@localhost ~]# chmod u-w /nsd02

[root@localhost ~]# ls -ld /nsd02

[root@localhost ~]# chmod u+w /nsd02

[root@localhost ~]# ls -ld /nsd02

[root@localhost ~]# chmod g=rwx /nsd02

[root@localhost ~]# ls -ld /nsd02

[root@localhost ~]# chmod u=rwx,g=rx,o=--- /nsd02

[root@localhost ~]# ls -ld /nsd02

[root@localhost ~]# chmod a=rwx /nsd02

[root@localhost ~]# ls -ld /nsd02

[root@localhost ~]# mkdir -p /opt/aa/bb/cc/dd

[root@localhost ~]# chmod -R o=--- /opt/aa #递归设置权限

[root@localhost ~]# ls -ld /opt/aa

[root@localhost ~]# ls -ld /opt/aa/bb

[root@localhost ~]# ls -ld /opt/aa/bb/cc

[root@localhost ~]# ls -ld /opt/aa/bb/cc/dd

Linux系统的权限判定：

1.判断用户对于该数据所处的身份

2.查看相应身份权限位

针对目录：

r：查看目录内容

w：可以新建/删除/改名,该目录的内容（对目录本身无法进行修改）

x：切换到此目录（进入此目录）

**案例1：设置基本权限**

以root身份新建/nsddir1/目录，在此目录下新建readme.txt文件

[root@localhost ~]# mkdir /nsddir1

[root@localhost ~]# echo 123456 > /nsddir1/readme.txt

[root@localhost ~]# cat /nsddir1/readme.txt

1）使用户zhangsan能够在此目录下创建/删除子目录

[root@localhost ~]# chmod o+w /nsddir1/

[root@localhost ~]# ls -ld /nsddir1/

2）使用户zhangsan能够修改readme.txt文件

[root@localhost ~]# chmod o+w /nsddir1/readme.txt

3）调整此目录的权限，使任何用户都不能进入，然后测试用户zhangsan是否还能修改readme.txt

[root@localhost ~]# chmod a-x /nsddir1/

4）为此目录及其下所有文档设置权限 rwxr-x---

[root@localhost ~]# chmod -R u=rwx,g=rx,o=--- /nsddir1/

•权限位的8进制数表示

–r、w、x分别对应4、2、1，后3组分别求和

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **分组** | User权限 | | | Group权限 | | | Other权限 | | |
| **字符** | r | w | x | r | - | x | r | - | x |
| **数字** | 4 | 2 | 1 | 4 | 0 | 1 | 4 | 0 | 1 |
| **求和** | **7** | | | **5** | | | **5** | | |

[root@localhost ~]# mkdir /nsd04

[root@localhost ~]# ls -ld /nsd04

[root@localhost ~]# chmod 750 /nsd04

[root@localhost ~]# ls -ld /nsd04

[root@localhost ~]# chmod 770 /nsd04

[root@localhost ~]# ls -ld /nsd04

[root@localhost ~]# chmod 007 /nsd04

[root@localhost ~]# ls -ld /nsd04

•新建文件/目录的默认权限

–一般文件默认均不给 x 执行权限

–其他取决于 umask值 设置

[root@localhost ~]# umask 022

[root@localhost ~]# umask -S

u=rwx,g=rx,o=rx

[root@localhost ~]#

四、修改归属关系

•chown命令

–chown   属主  文件...

–chown  属主:属组   文件...

–chown  :属组  文件...

•常用命令选项

–-R：递归修改归属关系

[root@localhost ~]# mkdir /nsd11

[root@localhost ~]# ls -ld /nsd11

[root@localhost ~]# groupadd tmooc

[root@localhost ~]# chown zhangsan:tmooc /nsd11

[root@localhost ~]# ls -ld /nsd11

[root@localhost ~]# chown root /nsd11 #只修改所有者

[root@localhost ~]# ls -ld /nsd11

[root@localhost ~]# groupadd sg

[root@localhost ~]# chown :sg /nsd11 #只修改所属组

[root@localhost ~]# ls -ld /nsd11

Linux系统的权限判定：

1.判断用户对于该数据所处的身份 所有者>所属组>其他人（匹配及停止）

2.查看相应身份权限位

root的身份新建/tarena目录，并进一步完成下列操作

[root@localhost ~]# mkdir /tarena

[root@localhost ~]# echo haha > /tarena/a.txt

1）将属主设为gelin01，属组设为tmooc组

[root@localhost ~]# useradd gelin01

[root@localhost ~]# groupadd tmooc

[root@localhost ~]# chown gelin01:tmooc /tarena

[root@localhost ~]# ls -ld /tarena

2）使用户gelin01对此目录具有rwx权限，除去所有者与所属组之外的用户对此目录无任何权限

[root@localhost ~]# chmod o=--- /tarena

3）使用户gelin02能进入、查看此目录

[root@localhost ~]# useradd gelin02

[root@localhost ~]# gpasswd -a gelin02 tmooc

4）将gelin01加入tmooc组，将tarena目录的权限设为450，再测试gelin01用户能否进入此目录

[root@localhost ~]# gpasswd -a gelin01 tmooc

[root@localhost ~]# chmod 450 /tarena

五、附加权限（特殊权限）

•Set GID权限

–占用属组（Group）的 x 位

–显示为 s 或 S，取决于属组是否有 x 权限

–对目录有效

–在一个具有SGID权限的目录下，新建的文档会自动继承此目录的属组身份

[root@localhost /]# mkdir /nsd15

[root@localhost /]# chown :tmooc /nsd15 #修改所属组

[root@localhost /]# ls -ld /nsd15

[root@localhost /]# mkdir /nsd15/test01

[root@localhost /]# ls -ld /nsd15/test01

[root@localhost /]# chmod g+s /nsd15 #设置Set Gid权限

[root@localhost /]# ls -ld /nsd15

[root@localhost /]# mkdir /nsd15/test02

[root@localhost /]# ls -ld /nsd15/test02 #查看所属组信息

[root@localhost /]# touch /nsd15/1.txt

[root@localhost /]# ls -l /nsd15/1.txt

•粘滞位，Sticky Bit 权限（t权限）

–占用其他人（Other）的 x 位

–显示为 t 或 T，取决于其他人是否有 x 权限

–适用于目录，用来限制用户滥用写入权

–在设置了粘滞位的文件夹下，即使用户有写入权限，也不能删除或改名其他用户文档

[root@localhost /]# mkdir /nsd16

[root@localhost /]# ls -ld /nsd16

[root@localhost /]# chmod 777 /nsd16

[root@localhost /]# ls -ld /nsd16

[root@localhost /]# chmod o+t /nsd16 #赋予t权限

[root@localhost /]# ls -ld /nsd16

六、ACL策略管理

•文档归属的局限性

任何人只属于三种角色：属主、属组、其他人

无法实现更精细的控制

•acl访问策略

**能够对个别用户、个别组设置独立的权限**

大多数挂载的EXT3/4、XFS文件系统默认已支持

[root@localhost /]# mkdir /nsd17

[root@localhost /]# chmod 770 /nsd17

[root@localhost /]# ls -ld /nsd17

[root@localhost /]# su - dc

[dc@localhost ~]$ cd /nsd17

-bash: cd: /nsd17: 权限不够

[dc@localhost ~]$ exit

[root@localhost /]# setfacl -m u:dc:rx /nsd17 #设置ACL策略

[root@localhost /]# getfacl /nsd17 #查看ACL策略

[root@localhost /]# su - dc

[dc@localhost ~]$ cd /nsd17

[dc@localhost nsd17]$ pwd

[dc@localhost nsd17]$ exit

登出

[root@localhost /]#

•setfacl命令

–格式： setfacl [选项] u:用户名:权限  文件...

        setfacl [选项] g:组名:权限  文件...

•常用命令选项

–-m：定义一条ACL策略

–-x：清除指定的ACL策略

–-b：清除所有已设置的ACL策略

–-R：递归设置ACL策略

[root@localhost /]# mkdir /nsd18

[root@localhost /]# setfacl -m u:dc:rx /nsd18

[root@localhost /]# setfacl -m u:zhangsan:rwx /nsd18

[root@localhost /]# setfacl -m u:lisi:rx /nsd18

[root@localhost /]# setfacl -m u:harry:rx /nsd18

[root@localhost /]# getfacl /nsd18

[root@localhost /]# setfacl -x u:zhangsan /nsd18 #删除指定用户的ACL

[root@localhost /]# getfacl /nsd18

[root@localhost /]# setfacl -x u:dc /nsd18 #删除指定用户的ACL

[root@localhost /]# getfacl /nsd18

[root@localhost /]# setfacl -b /nsd18 #清除所有用户的ACL

[root@localhost /]# getfacl /nsd18

–-R：递归设置ACL策略

[root@localhost /]# mkdir -p /nsd19/test

[root@localhost /]# setfacl -Rm u:dc:rx /nsd19 #选项Rm顺序不可颠倒

[root@localhost /]# getfacl /nsd19

[root@localhost /]# getfacl /nsd19/test/

•单独拒绝一个人

[root@localhost /]# mkdir /public

[root@localhost /]# chmod 777 /public

[root@localhost /]# setfacl -m u:lisi:--- /public/

[root@localhost /]# getfacl /public/

•附加权限Set UID（了解内容）

–占用属主（User）的 x 位

–显示为 s 或 S，取决于属主是否有 x 权限

–仅对可执行的程序有意义

–当其他用户执行带SUID标记的程序时，具有此程序属主的身份和相应权限



[root@localhost ~]# which mkdir

/usr/bin/mkdir

[root@localhost ~]# /usr/bin/mkdir /opt/haha

[root@localhost ~]# ls /opt/

[root@localhost ~]# cp /usr/bin/mkdir /usr/bin/hahadir

[root@localhost ~]# ls -l /usr/bin/hahadir

[root@localhost ~]# ls -l /usr/bin/mkdir

[root@localhost ~]# chmod u+s /usr/bin/hahadir #赋予Set UID权限

[root@localhost ~]# ls -l /usr/bin/hahadir

[root@localhost ~]# su - zhangsan

[zhangsan@localhost ~]$ /usr/bin/mkdir test01

[zhangsan@localhost ~]$ ls -l

[zhangsan@localhost ~]$ /usr/bin/hahadir test02

[zhangsan@localhost ~]$ ls -l

课后习题：

例1：chmod权限设置

1）以root用户新建/nsddir/目录，在该目录下新建文件readme.txt

2）使用户zhangsan能够在/nsddir/目录下创建/删除子目录

3）使用户zhangsan能够修改/nsddir/readme.txt文件的内容

案例2：chown归属设置

1）新建/tarena1目录

a）将属主设为gelin01，属组设为tarena组

b）使用户gelin01对此目录具有rwx权限，其他人对此目录无任何权限

2）使用户gelin02能进入、查看/tarena1文件夹（提示：将gelin02加入所属组）

3）新建/tarena2目录

a）将属组设为tarena

b）使tarena组的任何用户都能在此目录下创建、删除文件

4）新建/tarena/public目录

a）使任何用户对此目录都有rwx权限

b）拒绝zhangsan进入此目录，对此目录无任何权限（提示：ACL单独拒绝）

案例3:权限设置

1、创建文件夹/data/test,设置目录的访问权限，使所有者和所属组具备读写执行的权限；其他人无任何权限。

2、递归修改文件夹/data/test的归属使所有者为zhangsan，所属组为tarena。

3、请实现在test目录下，新建的所有子文件或目录的所属组都会是tarena。

4、为lisi创建ACL访问权限，使得lisi可以查看/etc/shadow文件

案例4:虚拟机上操作

将文件 /etc/fstab 拷贝为 /var/tmp/fstab，并调整文件 /var/tmp/fstab权限

满足以下要求：

– 此文件的拥有者是 root

– 此文件对任何人都不可执行

– 用户 natasha 能够对此文件具备读和写操作

– 用户 harry 对此文件既不能读，也不能写

案例5:虚拟机上操作

创建一个共用目录 /home/admins，要求如下：

– 此目录的所属组是 adminuser

– adminuser 组的成员对此目录有读写和执行的权限，并且其他用户没有任何权限

– 在此目录中创建的文件，其所属组会自动设置为 属于 adminuser 组