权限和归属

基本权限

访问方式(权限)

– 读取:允许查看内容-read r

– 写入:允许修改内容-write w

– 可执行:允许运行和切换-execute x

文本文件：

r: cat head less 读

w： vim > 写

x: 脚本文件 执行

• 权限适用对象(归属)

– 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

查看权限

• 使用 ls -l 命令

– ls -ld 文件或目录...

以 - 开头：文本文件

以 d 开头：目录

以 l 开头：快捷方式

[root@server0 ~]# ls -l /etc/passwd

[root@server0 ~]# ls -ld /etc/

[root@server0 ~]# ls -ld /root

[root@server0 ~]# ls -ld /boot

[root@server0 ~]# ls -l /etc/shadow

################################################

设置基本权限

• 使用 chmod 命令

– chmod [-R] 归属关系+-=权限类别 文档...

-R :递归设置

[root@server0 ~]# mkdir /nsd01

[root@server0 ~]# ls -ld /nsd01

[root@server0 ~]# chmod u-w /nsd01

[root@server0 ~]# ls -ld /nsd01

[root@server0 ~]# chmod g+w /nsd01

[root@server0 ~]# ls -ld /nsd01

[root@server0 ~]# chmod o=--- /nsd01

[root@server0 ~]# ls -ld /nsd01

[root@server0 ~]# chmod u=rwx,g=rwx,o=rx /nsd01

[root@server0 ~]# ls -ld /nsd01

[root@server0 ~]# chmod ugo=rwx /nsd01

[root@server0 ~]# ls -ld /nsd01

#####################################################

判别用户的权限：

1.判别用户的归属关系（角色） 所有者>所属组>其他人 匹配及停止

u g o

2.查看相应归属角色的权限位

#####################################################

Permission denied :权限不足

####################################################

目录的 r 权限:能够 ls 浏览此目录内容

目录的 w 权限:能够执行 rm/mv/cp/mkdir/touch/ 等更改目录内容的操作

目录的 x 权限:能够 cd 切换到此目录

以root用户新建/nsddir/目录，在此目录下新建readme.txt文件，并进一步完成下列操作

1）使用户lisi能够在此目录下创建子目录 切换用户 su - lisi

chmod o+w /nsddir/

2）使用户lisi不能够在此目录下创建子目录

chmod o-w /nsddir/

3）使用户lisi能够修改readme.txt文件

chmod o+w /nsddir/readme.txt

4）调整此目录的权限，使所有用户都不能cd进入此目录

chmod u-x,g-x,o-x /nsddir/

5）为此目录及其下所有文档设置权限 rwxr-x---

chmod -R u=rwx,g=rx,o=--- /nsddir/

######################################################

设置文档归属

• 使用 chown 命令

– chown [-R] 属主 文档...

– chown [-R] :属组 文档...

– chown [-R] 属主:属组 文档...

[root@server0 ~]# mkdir /nsd03

文档

[root@server0 ~]# ls -ld /nsd03

查看文档 所有者 所属组 所有用户

[root@server0 ~]# groupadd kaka

创建组 卡卡

[root@server0 ~]# chown lisi:kaka /nsd03

将lisi加入卡卡组

[root@server0 ~]# ls -ld /nsd03

[root@server0 ~]# useradd zhangsan

[root@server0 ~]# chown zhangsan /nsd03 #修改所有者

[root@server0 ~]# ls -ld /nsd03/

[root@server0 ~]# chown :root /nsd03 #修改所属组

[root@server0 ~]# ls -ld /nsd03/

#######################################################

利用root用户新建/nsd06目录，并进一步完成下列操作

1）将属主设为gelin01，属组设为tarena组

[root@server0 /]# useradd gelin01

[root@server0 /]# groupadd tarena

[root@server0 /]# chown gelin01:tarena /nsd06

2）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

[root@server0 /]# chmod o=--- /nsd06

3）使用户gelin02能进入、查看此目录

[root@server0 /]# gpasswd -a gelin02 tarena

4）将gelin01加入tarena组, 将nsd06目录的权限设为rw-r-x---

再测试gelin01用户能否进入此目录

[root@server0 /]# chmod u=rw,g=rx /nsd06

#######################################################

特殊权限(附加权限)

Set GID

• 附加在属组的 x 位上

– 属组的权限标识会变为 s

– 适用于目录,Set GID可以使目录下新增的文档自动设

置与父目录相同的属组

– 让新增子文档继承父目录的属组

[root@server0 ~]# mkdir /nsd08

[root@server0 ~]# chown :tarena /nsd08

[root@server0 ~]# ls -ld /nsd08

[root@server0 ~]# mkdir /nsd08/test01

[root@server0 ~]# ls -ld /nsd08/test01

[root@server0 ~]# chmod g+s /nsd08 #设置Set GID权限

[root@server0 ~]# ls -ld /nsd08

[root@server0 ~]# mkdir /nsd08/test02

[root@server0 ~]# ls -ld /nsd08/test02

[root@server0 ~]# ls -ld /nsd08/test01

[root@server0 ~]# touch /nsd08/1.txt

[root@server0 ~]# ls -l /nsd08/1.txt

######################################################

acl访问控制列表

acl策略的作用

• 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

[root@server0 ~]# mkdir /nsd09

[root@server0 ~]# chmod o=--- /nsd09

[root@server0 ~]# su - lisi

[lisi@server0 ~]$ cd /nsd09

-bash: cd: /nsd09: Permission denied

[lisi@server0 ~]$ exit

[root@server0 ~]# setfacl -m u:lisi:rx /nsd09 #设置ACL策略

[root@server0 ~]# getfacl /nsd09 #显示ACL策略

[root@server0 ~]# su - lisi

[lisi@server0 ~]$ cd /nsd09

[lisi@server0 nsd09]$ pwd

[lisi@server0 nsd09]$ exit

[root@server0 ~]#

######################################################

使用 getfacl、setfacl 命令 ACL策略

– getfacl 文档...

– setfacl -m u:用户名:权限类别 文档...

– setfacl -m g:组名:权限类别 文档...

– setfacl -x u:用户名 文档... #删除指定的ACL

– setfacl -b 文档... #删除所有ACL

-R: 递归设置

[root@server0 ~]# mkdir /nsd10

[root@server0 ~]# setfacl -m u:lisi:rx /nsd10

[root@server0 ~]# setfacl -m u:gelin01:rwx /nsd10

[root@server0 ~]# setfacl -m u:zhangsan:rx /nsd10

[root@server0 ~]# getfacl /nsd10 #查看ACL权限

[root@server0 ~]# setfacl -x u:gelin01 /nsd10 #删除指定ACL

[root@server0 ~]# getfacl /nsd10

[root@server0 ~]# setfacl -b /nsd10 #删除所有的ACL

[root@server0 ~]# getfacl /nsd10

###################################################

[root@server0 ~]# mkdir /public

[root@server0 ~]# chmod ugo=rwx /public

[root@server0 ~]# ls -ld /public

[root@server0 ~]# setfacl -m u:lisi:--- /public/

[root@server0 ~]# getfacl /public/

##################################################

使用LDAP认证,网络用户

网络用户:LDAP服务器存储

本地用户:/etc/passwd

什么是LDAP?

• 轻量级目录访问协议

• 为一组客户机集中提供可登录的用户账号

– 网络用户:用户名、密码信息存储在 LDAP 服务端

– 这些客户机都加入同一个 LDAP 域

服务端:LDAP服务器classroom.example.com

客户端:虚拟机Server0

1.安装一个sssd软件,与LDAP服务器沟通

[root@server0 ~]# yum -y install sssd

2.安装图形的工具authconfig-gtk,图形配置sssd

[root@server0 ~]# yum -y install authconfig-gtk

3.运行图形的工具进行配置

[root@server0 ~]# authconfig-gtk

选择LDAP

dc=example,dc=com #指定服务端域名

classroom.example.com #指定服务端主机名

勾选TLS加密

使用证书加密: http://classroom.example.com/pub/example-ca.crt

选择LDAP密码

4.重起服务

[root@server0 ~]# systemctl restart sssd #重起服务

[root@server0 ~]# systemctl enable sssd #设置开机自启动

5.验证:

[root@server0 ~]# grep ldapuser0 /etc/passwd

[root@server0 ~]# id ldapuser0

#######################################################

家目录的实现

共享: 本地数据传递给网络中其他主机

• Network File System,网络文件系统

– 由NFS服务器将指定的文件夹共享给客户机

– 客户机将此共享目录 mount 到本地目录,访问此共享

资源就像访问本地目录一样方便

– 类似于 EXT4、XFS等类型,只不过资源在网上

服务端:classroom.example.com NFS服务器共享所有用户的家目录

客户端:虚拟机Server0

• 查看NFS资源

# showmount -e classroom.example.com

• 挂载NFS资源

# mkdir /nfs

# mount classroom.example.com:/home/guests /nfs

# ls /nfs

# umount /nfs

# mkdir /home/guests

# mount classroom.example.com:/home/guests /home/guests

# ls /home/guests

# su - ldapuser0

########################################################