**权限和归属、使用LDAP认证、家目录漫游**

**真机：设置永久的别名**

**[root@room9pc14 桌面]# head -3 /root/.bashrc**

**# .bashrc**

alias s='ssh -X root@172.25.0.11'

alias d='ssh -X root@172.25.0.10'

/root/.bashrc : 每开启一个终端,专用于root用户初始化的配置文件

在开一个新的终端

[root@room9pc14 桌面]# s

[root@room9pc14 桌面]# d

###############################################**基本权限的类别**

**• 访问方式(权限)**

**– 读取:允许查看内容-read**

**– 写入:允许修改内容-write**

**– 可执行:允许运行和切换-execute**

**• 权限适用对象(归属)**

**– 所有者:拥有此文件/目录的用户-user**

**– 所属组:拥有此文件/目录的组-group**

**– 其他用户:除所有者、所属组以外的用户-other**

**• 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**

基本权限对于文本文件作用：

**r: 读取内容 cat head less tail**

**w: 修改内容 vim**

**x: 执行该文本文件**

###############################################**设置基本权限**

**• 使用 chmod 命令**

**– chmod [-R] 归属关系+-=权限类别 文档...**

[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=rx,o=rx /nsd01

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

############################################### **Linux判断权限：**

**1.用户的身份，属于哪一个归属关系 所有者>所属组>其他人 匹配即停止**

**2.相应权限位置的权限**

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zhangsan能够在此目录下创建子目录 切换用户 su - zhangsan

chmod o+w /nsddir/

2）使用户zhangsan不能够在此目录下创建子目录

chmod o-w /nsddir/

3）使用户zhangsan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/

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

**• 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

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

[root@server0 /]# groupadd stugrp

[root@server0 /]# chown zhangsan:stugrp /nsd03/

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

[root@server0 /]# chown lisi /nsd03/

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

[root@server0 /]# chown :root /nsd03

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

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

**附加权限**

**• 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(继承)**

[root@server0 /]# mkdir /nsd12

[root@server0 /]# chown :stugrp /nsd12

[root@server0 /]# ls -ld /nsd12

[root@server0 /]# mkdir /nsd12/test01

[root@server0 /]# ls -ld /nsd12/test01

[root@server0 /]# chmod g+s /nsd12 **#设置附加权限SetGID**

[root@server0 /]# ls -ld /nsd12

[root@server0 /]# mkdir /nsd12/test02

[root@server0 /]# ls -l /nsd12/

**Sticky Bit**

**• 附加在其他人的 x 位上**

**– 其他人的权限标识会变为 t**

**– 适用于开放 w 权限的目录,可以阻止用户滥用 w 写入权限(禁止操作别人的文档)**

[root@server0 /]# mkdir /public

[root@server0 /]# chmod u=rwx,g=rwx,o=rwx /public

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

[root@server0 /]# chmod o+t /public/

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

drwxrwxrwt. 2 root root 6 12月 20 14:29 /public/

###############################################**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文件系统默认已支持

**设置ACL权限 : setfacl -m u:用户:权限 文件路径**

[root@server0 /]# mkdir /nsd20

[root@server0 /]# ls -ld /nsd20

[root@server0 /]# chmod o=--- /nsd20

[root@server0 /]# su - zhangsan

[zhangsan@server0 ~]$ cd /nsd20

-bash: cd: /nsd20: Permission denied

[zhangsan@server0 ~]$ exit

[root@server0 /]# setfacl -m u:zhangsan:rx /nsd20

[root@server0 /]# ls -ld /nsd20

[root@server0 /]# su - zhangsan

[zhangsan@server0 ~]$ cd /nsd20

[zhangsan@server0 nsd20]$ pwd

[zhangsan@server0 nsd20]$ exit

[root@server0 /]#

###############################################**• 使用 getfacl、setfacl 命令**

**– getfacl 文档...**

**– setfacl [-R] -m u:用户名:权限类别 文档...**

**– setfacl [-R] -m g:组名:权限类别 文档...**

**– setfacl -x u:用户名 文档... #删除指定用户的ACL权限**

**– setfacl [-R] -b 文档...**

[root@server0 /]# mkdir /nsd30

[root@server0 /]# ls -ld /nsd30

[root@server0 /]# setfacl -m u:zhangsan:rx /nsd30

[root@server0 /]# setfacl -m u:lisi:rwx /nsd30

[root@server0 /]# setfacl -m u:dc:rx /nsd30

[root@server0 /]# getfacl /nsd30

[root@server0 /]# setfacl -x u:lisi /nsd30 #删除指定的ACL

[root@server0 /]# getfacl /nsd30

[root@server0 /]# setfacl -b /nsd30 #删除所有的ACL

[root@server0 /]# getfacl /nsd30

############################################### **使用LDAP认证 : 实现网络用户验证的服务器**

典型的LDAP工作模式

• 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

**一、 搭建服务器 LDAP 服务端 classroom.example.com**

**二、 客户端 server0.example.com**

1.安装客户端软件 sssd 专用于与 LDAP 服务端沟通的软件

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

2.安装图形软件 authconfig-gtk 专用于配置sssd工具

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

3.利用 authconfig-gtk 配置sssd程序

[root@server0 /]# authconfig-gtk

选择LDAP

dc=example,dc=com

classroom.example.com

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

选择LDAP密码

**4.重起sssd 服务**

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

**[root@server0 /]# systemctl enable sssd : #设置服务随机自启动**

**5.LDAP服务器上的用户可以在本地识别**

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

**[root@server0 ~]# id ldapuser0**

**三、能够在客户端本地访问网络用户的家目录**

• 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

**1.客户端查看NFS资源**

**– showmount -e [服务器地址]**

**[root@server0 ~]# showmount -e 172.25.254.254**

Export list for classroom:

/home/guests 172.25.0.0/255.255.0.0

**2.挂载指定的家目录位置**

**[root@server0 ~]# su - ldapuser0**

上一次登录：三 12月 20 17:04:27 CST 2017pts/0 上

su: 警告：无法更改到 /home/guests/ldapuser0 目录: 没有那个文件或目录

mkdir: cannot create directory '/home/guests': Permission denied

-bash-4.2$ exit

**[root@server0 ~]# mkdir /home/guests**

**[root@server0 ~]# ls /home/guests**

**# mount 172.25.254.254:/home/guests/ /home/guests**

**[root@server0 ~]# ls /home/guests**

**[root@server0 ~]# su - ldapuser0**