**NSD admin DAY6**

**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 执行权限

对文本文件:

r:cat less tail head 查看内容

w:vim > >> 可以保存并退出

x:shell脚本

权限适用对象

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 查看文件/目录

以 - 开头:文本文件

以 d 开头:目录

以 l 开头:快捷方式

-rwxr-----. 1 root root 3 12月 6 11:12 /nsddir/readme.txt

9个

**设置基本权限**

权限

chmod 命令

格式:chmod 基本权限 参数 文件源

**chmod [-R] 归属关系+-(=权限类别) 文档.**..

[-R] 递归权限修改

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

[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

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

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

**Linux判断用户对于文档,属于什么身份**

1. 判断用户对于文档 **所有者>所属组>其他人 匹配即停止**
2. 查看文档,相应角色的权限

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  **(更改子目录内容)**

**目录的x权限**:能够cd切换到此目录

**设置文档归属**

**使用chown命令**

chown [-R] 所有者 文件

[root@server0 ~]# mkdir /nsd03

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

[root@server0 ~]# groupadd tarena

[root@server0 ~]# chown lisi:tarena /nsd03 #**修改所有者和所属组**

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

[root@server0 ~]# useradd zhangsan

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

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

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

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

**附加权限(特殊权限)**

set GID

附加在属组的x位上

属组的权限标识会变为s  **-s包含x S不包含x**

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

传递所属组身份(让子文档自动继承父目录的所属组身份)

[root@server0 ~]# mkdir /nsd07

[root@server0 ~]# chown :tarena /nsd07 #**修改所属组身份**

[root@server0 ~]# ls -ld /nsd07

[root@server0 ~]# mkdir /nsd07/abc01

[root@server0 ~]# ls -ld /nsd07/abc01/

[root@server0 ~]# chmod g+s /nsd07 #**设置set GID**

[root@server0 ~]# ls -ld /nsd07

[root@server0 ~]# mkdir /nsd07/abc02

[root@server0 ~]# ls -ld /nsd07/abc02

[root@server0 ~]# mkdir /nsd07/abc02/test

[root@server0 ~]# ls -ld /nsd07/abc02/test

**acl访问控制列表**

acl策略的作用

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文件的系统默认已支持

setfacl -m u:用户名/g:组名:基本权限 /文档  **u:代表用户 g:代表组**

gerfacl /文档

[root@server0 ~]# mkdir /nsd10

[root@server0 ~]# chmod o=--- /nsd10

[root@server0 ~]# ls -ld /nsd10

[root@server0 ~]# su - lisi

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

[root@server0 ~]# getfacl /nsd10 #查看

使用 getfacl setfacl 命令

acl设置黑名单

使用LDAP认证

什么是LDAP

轻量级目录访问协议

用户的集中管理

LDAP用户:网络用户.由网络中LDAP服务器统一提供用户信息

LADP服务器:虚拟机classroom

LADP客户端:虚拟机server

1. 安装软件sssd,客户端与LDAP服务器沟通

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

[root@server0 ~]# rpm -q sssd

1. 图形工具authconfig-gtk进行配置

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

[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

1. 重启sssd服务

[root@server0 ~]# systemctl restart sssd #重启服务

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

4.验证

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

[root@server0 ~]# id ldapuser0

家目录漫游

NFS共享

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,只不过放在网上

NFS服务器:虚拟机classroom

客户端虚拟机server:访问共享

查看NFS共享

showmount -e 服务器地址

挂载NFS共享目录

mount 服务器地址:目录路径 本地挂载点

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

[root@server0 ~]# mount classroom.example.com:/home/guests/ /home/guests

[root@server0 ~]# su - ldapuser0