Day 06 权限和归属 使用LDAP认证 家目录漫游

1. 权限和归属
2. 基本权限

a) 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

· 对于文本文件：

r:cat less head tail

w:vim 能够保存

x:Shell脚本

b) 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

1. 查看权限
2. 命令ls -l
3. 开头含义：

· 以 - 开头：文本文件

· 以d开头：目录

· 以l开头：快捷方式（链接）

c) 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

d) 如何判断Linux中用户的权限

· 查看用户对于该文档 所属的身份 匹配即停止

· 查看相应身份的权限

常见的提示信息：权限不足

Permission denied

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

e) 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...

1. 附加权限（特殊权限）

a) Set GID

· 附加在属组的x位上

- 属组的权限标识会变为s（s覆盖执行权限x，分大小写区别原执行权限）

- 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

- 继承父目录所属组身份

b) 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（禁止操作别人文档）

c) Set UID

· 附加再属主的x位上

- 属主的执行标识会变成s

- 适用于可执行文件，Set UID可以让使用者具有为鄂东南角爱你属主的身份及部分权限

1. acl访问控制列表
2. 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

b) 命令设置：

· 使用getfacl、setfacl

- setfacl [-R] -m u:用户名:权限类别 文档... #添加策略

- setfacl [-R] -m g:组名:权限类别 文档...

- setfacl [-R] -x u:用户名 文档... #删除指定策略

- setfacl [-R] -b 文档... #清空策略

1. 使用LDAP认证
2. 什么是LDAP？

· 轻量级目录访问协议

- 由服务器来集中存储并向客户端提供的信息，存储方式类似于DNS分层结构

- 提供的信息包括：用户名、密码、通信录、主机名映射记录、……

· 为一组客户机提供可登陆的用户帐号

- 本地用户：/etc/passwd /etc/shadow

- 网络用户：用户名、密码信息存储在LDAP服务端

服务端：classroom.example.com

客户端：指定LDAP服务端位置（域名）

1. 安装一个客户端sssd软件

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

b) authconfig-gtk图形的配置

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

c) authconfig-gtk 启动

选择LPAD

dc=example,dc=com

classroom.example.com

TLS加密，证书加密

systemctl restart sssd

systemctl enable sssd

1. 家目录漫游
2. 共享服务

· NFS共享：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

· 客户端：server0.example.com

1. 查看共享classroom.example.com

[root@server0 ~]# showmount -e classroom.example.com

Export list for classroom.example.com:

/home/guests 172.25.0.0/255.255.0.0

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

[root@server0 ~]# mount 172.25.254.254:/home/guests /home/guests

[root@server0 ~]# su - ldapuser0

1. autofs工具配置
2. 装包

yum -y install autofs

1. 修改主配置文件

vim /etc/auto.master

/home/guests /etc/auto.guests

:wq

1. 修改次级配置

\* -rw classroom.example.com:/home/guests/& (&:和前一个\*相同)

:wq

1. 重启服务

systemctl restart autofs

systemctl enable autofs