**权限和归属（匹配原则所有者>所属组>其他人）**

基本权限

基本权限类别

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

文件的r权限：能够查看文件的内容cat head tail less

文件的w权限：可以编辑文件内容vim

文件的x权限：可以运行该文件

目录的r权限：能够ls浏览次目录内容

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

权限适用对象（归属）

所有者（属主）：拥有此文件/目录的用户-user u

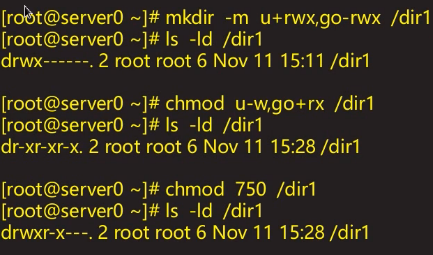
所属组（属组）：拥有此文件/目录的组-group g

其他用户：除所有者、所属组以外的用户-other o

设置基本权限

适用chmod命令

chmod -R 归属关系+-=权限类别 文档...



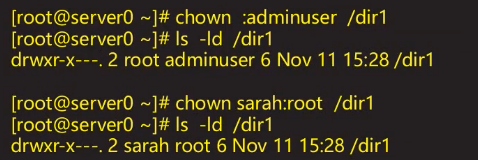
设置文档归属

使用chown命令

chown -R 属组 文档...

chown -R :属组 文档...

chown -R 属主:属组 文档...



附加权限（特殊权限）

set gid

属组的权限标识会变为s（大写原来没有执行，小写原来有执行）

适用于目录，set gid可以使目录下新增的文档自动设置域父目录相同的属组（继承父目录的所属组身份）

设置附加权限

chmod g+s 文档...

acl访问控制列表（acl策略）

文件归档的局限性

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ext3/4、xfs文件系统默认已支持

设置acl访问控制策略

使用getfacl、setfacl命令

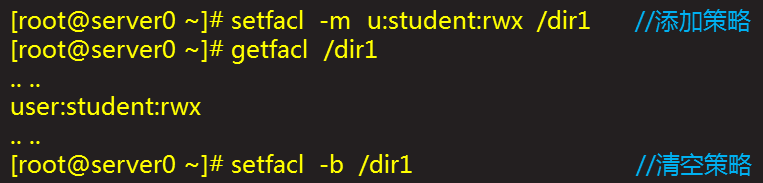
getfacl 文档...

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 -R -b 文档... 清除所有的ACL

setfacl -x u:用户名 文档... 删除指定的acl



**使用LDAP（服务器）认证**

作用：集中管理维护网络中的用户

LDAP目录服务

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。

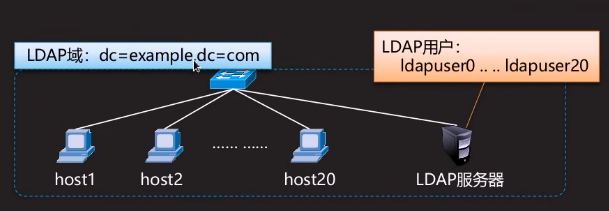
提供的信息包括：用户名、密码、通信录、主机映射记录......

典型的LDAP工作模式

为一组客户机集中提供可登录的用户帐号

网络用户：用户名、密码信息存放在LDAP服务端

这些客户机都加入同一个LDAP域



如何加入LDAP域

加入LDAP需要的条件

服务端提供：

LDAP服务器地址、基本DN（域名）名称

加密用的证书（若需要）

客户端准备：

修改用户登录的验证方式，启用LDAP

正确配置LDAP服务端参数

软件包：sssd、authconfig-gtk



使用系统classroom.example.com提供的LDAP服务

验证服务基本DN是：dc=example,dc=com

账户信息和安装信息都是由LDAP提供的

连接要使用证书加密，证书可以在下面的链接下载

<http://classroom.example.com/pub/example-ca.crt>

当正确配置完成后，用户ldapuser0应该能登录到系统，暂时没有主目录，密码是password

步骤1：安装sssd客户端软件，与服务端LDAP服务器沟通

yum -y install sssd

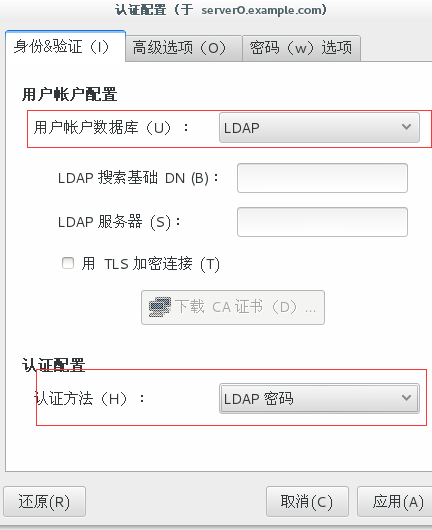
步骤2：安装图形工具配置ssd软件

yum -y install authconfig-gtk

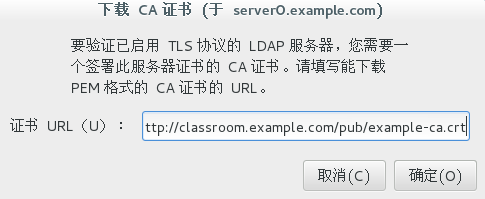
步骤3：运行authconfig-gtk配置ssd软件

[root@server0 ~]#authconfig-gtk







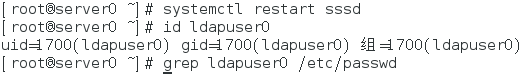


步骤4：验证（重新启动sssd服务）

systemctl restart sssd

id ldapuser0

grep ldapuser0 /etc/passwd



**家目录漫游**

访问NFS（网络文件系统）共享

什么是NFS共享

由NFS服务器将指定的文件夹共享给客户机

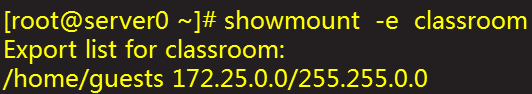
客户机将此共享目录mount到本地目录，访问此共享资源就像访问本地目录一样方便

类似于EXT4、XFS等类型，只不过资源在网上

如何访问NFS共享目录

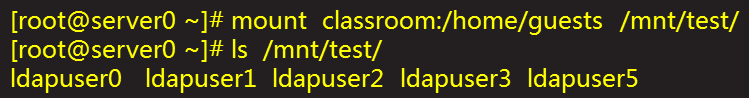
查看NFS资源

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



挂载LDAP家目录



