**1\_Admin08管理LDAP**

**一 功能**

使用LDAP认证,实现网络用户认证,达到用户的集中管理

网络用户:用户信息会放在网络中LDAP服务器

本地用户:用户信息会放在/etc/passwd

**正确: 只要在/etc/passwd文件内容有的用户信息,本地都能识别**

**错误: 本地都能识别的用户,信息都在/etc/passwd**

**二 搭建LDAP**

LDAP服务器:虚拟机classroom

客户端:虚拟机server

2.1 安装**sssd**软件,与LDAP服务器沟通

**SSSD:** **S**ystem **S**ecurity **S**ervices **D**aemon

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

[root@server0 /]# rpm -q sssd

2.2 安装**authconfig-tui**图形的工具,并配置

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

[root@server0 /]# authconfig-tui

完全合格的主机名 www.baidu.com　www.qq.com

勾选使用LDAP->勾选使用LDAP认证->下一步

勾选使用TLS->下一步

服务器: classroom.example.com

基础DN: dc=example,dc=com->确认

警告 要连接到启用TLS的LDAP..... 不要退出,另开终端下载证书

~]# cd /etc/openldap/cacerts/

cacerts]# wget [http://classroom.example.com/pub/examp](http://classroom.example.com/pub/example-ca.crt)

[le-ca.crt](http://classroom.example.com/pub/example-ca.crt)

返回警告终端,点击确定

**2.3 重起服务**

~]# systemctl restart sssd #重起服务

~]# systemctl enable sssd #设置开机自启动

~]# grep ldapuser0 /etc/passwd

~]# id ldapuser0 #验证LDAP用户信息

**2.4 家目录漫游**

在LDAP服务器搭建共享,共享所有普通用户的家目录

LDAP服务器:虚拟机classroom

虚拟机classroom已经完成共享所有操作

虚拟机server:访问共享数据

~]# mkdir /haha

~]# ls /haha

~]# **showmount -e** classroom.example.com

#查看classroom共享的档

Export list for classroom.example.com:

/home/guests 172.25.0.0/255.255.0.0

~]# mount classroom.example.com:/home/guests /haha

#将classroom共享的网络用户家目录挂载到本地/haha/下

~]# df -h #查看挂载信息

~]# mkdir /home/guests #创建本地存放LDAP网络用户的家目录

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

#将classroom共享的网络用户家目录挂载到本地创建的网络用户家目录

~]# ls /home/guests #查看挂载后的信息

~]# su - ldapuser0 #测试,切换到网络用户ldapuser0

上一次登录：三 4月 10 19:21:04 CST 2019pts/0 上 #测试成功

[ldapuser0@server0 ~]$