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: System Security Services Daemon

```
[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
le-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 ~]$
```