网上有很多Openldap安装部署的文章，往往这些文章都浓墨重彩的描述服务端（Server）的安装和部署，以及排错等过程及说明，但是作为一个C/S架构的软件，可能很多技术牛人认为客户端（Client）的安装就不过如此而已了（虽然有的博客贴出了在桌面环境下设置，不过我觉得生产服务器大部分都是没有桌面环境的），所以大多都寥寥几笔带过，于是就导致配置一个服务端可能有各种教程，反正轻易的就能完成，即使出错也有章可循，而客户端则恰恰相反。然而，配置Openldap的初衷就是用来管理客户端和用户、用户组，既然服务器端已经OK了，那么后续肯定要将众多的Linux服务器加入这个ldap域中来，从而实现统一身份认证，所以别的不多说，以CentOS 6.5为例配置Openldap的客户端。

1、准备工作

#停止iptables，并查看iptables状态

/etc/init.d/iptables stop

iptables -L -n

#禁用SELinux,并查看SELinux状态

setenforce 0

getenforce

#编辑/etc/hosts，添加openldap server的记录

echo "192.168.30.217 ldap.unifgroup.com" >>/etc/hosts

#添加成功后，最好ping一下，看是否能解析正常

2、安装openldap客户端软件包

yum -y install nss-pam-ldapd pam\_ldap openldap-clients

3、配置/etc/sysconfig/authconfig

/etc/sysconfig/authconfig 文件由authconfig-5.3.21-3.e15RPM包生成系统默认安装。配置该文件用来跟踪LDAP身份认证机制是否正确启用。

cp /etc/sysconfig/authconfig /etc/sysconfig/authconfig.bak$(date +%F)

sed -i '/USESYSNETAUTH/s/no/yes/' /etc/sysconfig/authconfig

sed -i '/USELDAPAUTH/s/no/yes/' /etc/sysconfig/authconfig

sed -i '/USEMKHOMEDIR/s/no/yes/' /etc/sysconfig/authconfig

sed -i '/PASSWDALGORITHM/s/md5/yes/' /etc/sysconfig/authconfig

sed -i '/USELDAP/s/no/yes/' /etc/sysconfig/authconfig

[root@ldapclient ~]# diff /etc/sysconfig/authconfig.bak2016-09-11 /etc/sysconfig/authconfig

2c2

< USEMKHOMEDIR=no

---

> USEMKHOMEDIR=yes

12,13c12,13

< PASSWDALGORITHM=md5

< USELDAPAUTH=no

---

> PASSWDALGORITHM=yes

> USELDAPAUTH=yes

21c21

< USELDAP=no

---

> USELDAP=yes

24c24

< USESYSNETAUTH=no

---

> USESYSNETAUTH=yes

补充一点，也可以用authconfig-tui命令打开一个图形化的界面来配置，但是不推荐使用，因为字符或语言的关系，你可能看到的是乱码的界面，当然字符和语言都能调整，问题是耗费了事假；另外就是，如果你自己已经配置过/etc/openldap/ldap.conf，再通过authconfig-tui图形界面配置ldapserver信息后，可能会造成你的/etc/openldap/ldap.conf文件多出一些字符，就是因为图形界面的一些空格或者其他看不到的字符造成的更改。

4、配置/etc/nsswith.conf

/etc/nsswith.conf文件由glibc-2.5-24生成，CentOS5.2中缺省安装。该文件用于名称转换服务。通常LINUX系统身份验证读取本地文件，要使身份验证查询通过LDAP服务器必须在该文件中找到passwd;shadow;group;三行在files后空格添加“ldap”4

cp /etc/nsswitch.conf /etc/nsswitch.conf.bak$(date +%F)

sed -i '/^passwd:/s/files/files ldap/' /etc/nsswitch.conf

sed -i '/^shadow:/s/files/files ldap/' /etc/nsswitch.conf

sed -i '/^group:/s/files/files ldap/' /etc/nsswitch.conf

[root@ldapclient ~]# egrep "^passwd|^shadow|^group" /etc/nsswitch.conf

passwd: files ldap

shadow: files ldap

group: files ldap

5、配置/etc/pam.d/system-auth

身份验证服务是实际向LDAP验证用户身份的服务。可插入身份验证模块（PAM）提供了本地Linux身份验证服务。pam\_unix.so模块是通用模块，使PAM机制对本地的/etc/passwd文件检查用户帐号。PAMLDAP模块可以用来将身份验证重定向到LDAP目录上。身份验证本身是由PAM程序执行的，它从身份验证候选机制中获取用户名，将其绑定到openLDAP 服务器上。如果绑定成功，PAM会报告说这个用户已经成功通过了pam\_ldap.so提供的身份验证测试。根据PAM的配置不同，在用户看到命令提示符之前可能会执行其它测试。

/etc/pam.d/system-auth文件是CentOS的系统认证PAM文件。在该文件的auth,account,password,session四段中pam\_unix.so模块后添加pam\_ldap.so模块使身份验证先对本地的/etc/passwd文件检查用户帐号，然后再对LDAP服务器进行检查。同时因为是LDAP认证需要为用户创建根目录，所以还必须在会话（SESSION）阶段增加pam\_mkhomedir.so模块，为用户登录自动创建宿主目录。

[root@ldapclient sysconfig]# cat /etc/pam.d/system-auth

#%PAM-1.0

# This file is auto-generated.

# User changes will be destroyed the next time authconfig is run.

auth required pam\_env.so

auth sufficient pam\_fprintd.so

auth sufficient pam\_unix.so nullok try\_first\_pass

auth requisite pam\_succeed\_if.so uid >= 500 quiet

auth sufficient pam\_ldap.so use\_first\_pass

auth required pam\_deny.so

account required pam\_unix.so

account sufficient pam\_localuser.so

account sufficient pam\_succeed\_if.so uid < 500 quiet

account [default=bad success=ok user\_unknown=ignore] pam\_ldap.so

account required pam\_permit.so

password requisite pam\_cracklib.so try\_first\_pass retry=3 type=

password sufficient pam\_unix.so md5 shadow nullok try\_first\_pass use\_authtok

password sufficient pam\_ldap.so use\_authtok

password required pam\_deny.so

session optional pam\_keyinit.so revoke

session required pam\_limits.so

session [success=1 default=ignore] pam\_succeed\_if.so service in crond quiet use\_uid

session required pam\_unix.so

session required pam\_mkhomedir.so skel=/etc/skel/ umask=0077

session optional pam\_ldap.so

#蓝色部分为添加的配置

6、配置/etc/openldap/ldap.conf

cp /etc/openldap/ldap.conf /etc/openldap/ldap.conf.bak$(date +%F)

echo "BASE dc=contoso,dc=com" >>/etc/openldap/ldap.conf

echo "URI ldap://ldapsrv01.contoso.com" >>/etc/openldap/ldap

[root@ldapclient ~]# tail -2 /etc/openldap/ldap.conf

BASE dc=contoso,dc=com

URI ldap://ldapsrv01.contoso.com

7、使用ldapsearch命令测试能否读取openldap server中的数据

[root@ldapclient ~]# ldapsearch -x -b "dc=unifgroup,dc=com"

这里成功读取了ldap中的数据，网上给出的大部分教程，到此之后就直接#service nslcd restart，然后就可以使用getent测试获取ldap中的用户信息，我分别在CentOS 5.5和CentOS 6.5上做了测试，都无法获取，而且也无法使用id user这个命令查询ldap上用户的信息，所以该方法不可取，至少在CentOS 6上是不行的。

补充：如果出现“ldap\_sasl\_bind(SIMPLE): Can't contact LDAP server (-1)”，那么解决该问题的方法是：

1)检查/etc/hosts文件，是否有ldapserver的记录，最好能ping一下，看能否解析成功

2)到openldap server上检查slapd服务是否正在运行，如果没有，启动slapd服务

3)检查/etc/openldap/ldap.conf文件，查看里面的BASE和URI是否正确，很有可能是在图形界面中的设置，导致配置文件多了一些字符，从而出错

8、使用authconfig命令启动nslcd

authconfig --enableldap --enableldapauth --ldapserver=ldap.unifgroup.com --ldapbasedn="dc=contoso,dc=com" --enablemkhomedir --update

#该命令要包含ldapserver和basedn的信息

9、测试ldap用户登录

[root@ldapclient ~]# getent passwd|grep elasearch

elasearch:x:500:500:elasearch:/home/elasearch:/bin/bashlv:/home/charleslv:/bin/bash

[root@ldapclient ~]# id elasearch

uid=500(elasearch) gid=500 组=500 [root@ldapclient ~]# id zhangs

[root@ldapclient ~]# su - elasearch

[elasearch@localhost ~]$ pwd

/home/elasearch

[elasearch@localhost ~]$ ll

总用量 0

[elasearch@localhost ~]$

到此，CentOS 6.5配置openldap客户端成功