简介：

　　LDAP(轻量级目录服务访问协议，Lightweight Directory Access Protocol)基于X.500标准，支持TCP/IP，使用简单方便。现在越来越多的网络应用系统都支持LDAP。

　　目录是一个为查询、浏览和搜索而优化的专业分布式数据库，它成树状结构组织数据，就好象Linux/Unix系统中的文件目录一样。目录数据库和关系数据库不同，它有优异的读性能，但写性能差，并且没有事务处理、回滚等复杂功能，不适于存储修改频繁的数据。所以目录天生是用来查询的，就好象它的名字一样。目录服务是由目录数据库和一套访问协议组成的系统。类似以下的信息适合储存在目录中： 企业员工和企业客户之类人员信息；公用证书和安全密钥；邮件地址、网址、IP等电脑信息；电脑配置信息。

　　而且在我们的日常生活中，很多的应用都是基于LDAP的，比如Microsoft服务器的AD管理以及IBM的邮件Lotus都是基于LDAP的，并且Linux下的Postfix也可以设计成支持LDAP的形式，这篇文单权当是入门之用吧．以前有试过做基于Mysql的Postfix邮件系统（ [url]http://waringid.blog.51cto.com/65148/58580[/url]），也打算用LDAP来实现，我会把我的安装经历整理出来的．

支持软件：

　　安装OpenLDAP的相关支持软件是Berkeley DB，有了它就可以进行了，当然，如果你要求Sasl的支持的话那cyrus-sasl这个支持包也是少不了的．不过这个软件包一般系统中会自带，而且OpenLDAP在编译时默认会加入此功能支持．这些软件的下载地址可以参考我以前写过的一篇文章（ [url]http://waringid.blog.51cto.com/65148/58144[/url]），其中有列出下载地址．而OpenLDAP的下载地址则是： [url][ftp://ftp.openldap.org/pub/OpenLDAP/openldap-release[/url](ftp://ftp.openldap.org/pub/OpenLDAP/openldap-release%5b/url)]．

查询并卸载系统中原有的相关软件：

rpm -qa |grep ldap

rpm -e --nodeps

安装BerkeleyDB：

tar zxvf db-4.5.20.tar.gz

cd db-4.5.20/build\_unix

../dist/configure --prefix=/usr/local/BerkeleyDB

make

make install

echo "/usr/local/BerkeleyDB/lib" >> /etc/ld.so.conf

ldconfig -v 必须

安装Cyrus-Sasl：

tar zxvf cyrus-sasl-2.1.21.tar.gz

cd cyrus-sasl-2.1.21

./configure --prefix=/usr/local/sasl --enable-cram --enable-plain \

--enable-digest --disable-anon --enable-krb4 --enable-ntlm

make

make install

echo "/usr/local/sasl/lib/" >> /etc/ld.so.conf

ldconfig -v

ln -sv /usr/local/sasl/include/sasl/\* /usr/local/include/

ln -sv /usr/local/sasl/lib/\* /usr/local/lib/

ln -sv /usr/local/sasl/lib/sasl2/\* /usr/local/lib/

安装OpenLDAP：

gunzip -c openldap-2.4.9.tgz | tar xvfB -

cd openldap-2.4.9

env CPPFLAGS="-I/usr/local/BerkeleyDB/include" LDFLAGS="-L/usr/local/BerkeleyDB/lib" \

./configure --prefix=/usr/local/openldap --sysconfdir=/etc --enable-ldbm \

--enable-lmpasswd --enable-spasswd --enable-bdb --enable-ldap

make depend

make

make install

echo /usr/local/openldap/lib >> /etc/ld.so.conf

ldconfig -v

配置LADP：

　　LDAP的配置中，我们要实现的功能如图所示．需要增加一个用户＂Ben＂．

生成LDAP管理密码：

/usr/local/openldap/sbin/slappasswd -h {md5}

{MD5}X03MO1qnZdYdgyfeuILPmQ==##此密码是LDAP管理密码,和系统密码无关

增加相关查询记录：

echo "127.0.0.1 ldap.test.com" >> /etc/hosts

echo "127.0.0.1 ldap-master.test.com" >> /etc/hosts

设置slapd.conf文件：

vi /etc/openldap/slapd.conf

include /etc/openldap/schema/core.schema

include /etc/openldap/schema/cosine.schema

include /etc/openldap/schema/inetorgperson.schema

include /etc/openldap/schema/nis.schema

pidfile /var/run/openldap/slapd.pid

argsfile /var/run/openldap/slapd.args

database bdb

suffix "dc=test,dc=com"

rootdn "cn=Manager,dc=test,dc=com"

rootpw {MD5}X03MO1qnZdYdgyfeuILPmQ==

directory /var/lib/ldap

设置ldap.conf文件：

vi /etc/openldap/ldap.conf

HOST 127.0.0.1

BASE dc=test,dc=com

URI ldap://ldap.test.com ldap://ldap-master.test.com:389

SIZELIMIT 12

TIMELIMIT 15

DEREF nerver

启动LDAP：

/usr/local/openldap/libexec/slapd

增加用户资料：

系统上存在的用户（存储在/etc/passwd和/etc/shadow上），并没有在LDAP数据库里，所以要把这些用户导入到LDAP里面去。但LDAP只能识别特定格式的文件 即后缀为ldif的文件（也是文本文件），所以不能直接使用/etc/passwd和/etc/shadow。 需要migrationtools这个工具把这两个文件转变成LDAP能识别的文件。

安装配置migrationtools:

# yum install migrationtools -y

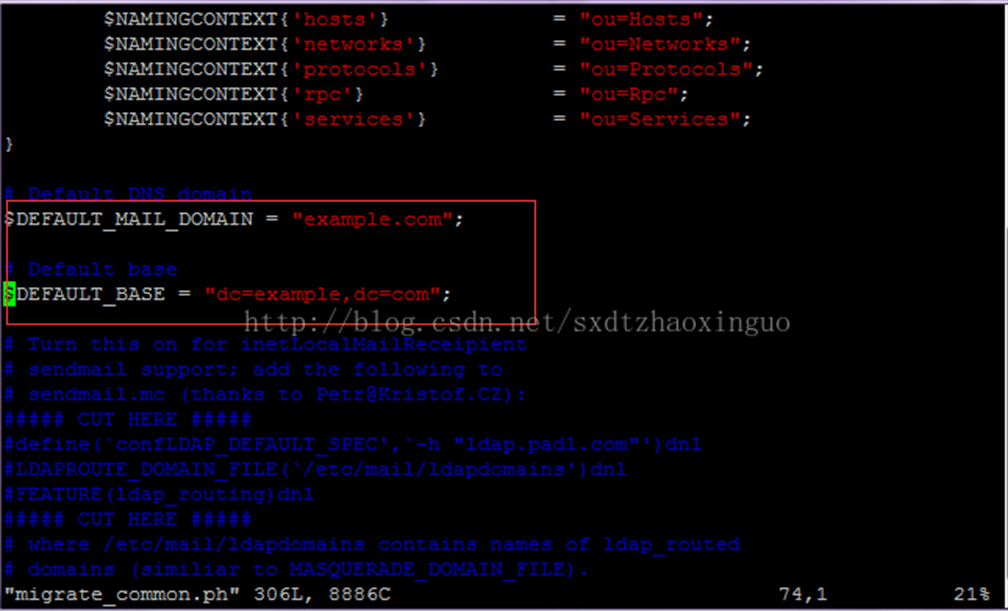
进入migrationtool配置目录:

# cd /usr/share/migrationtools/

首先编辑migrate\_common.ph:

# vi  migrate\_common.ph

找到如下内容（大概在70行):



修改完后，保存并退出。

下面利用pl脚本将/etc/passwd 和/etc/shadow生成LDAP能读懂的文件格式，保存在/tmp/下:

# ./migrate\_base.pl > /tmp/base.ldif

# ./migrate\_passwd.pl  /etc/passwd > /tmp/passwd.ldif

# ./migrate\_group.pl  /etc/group > /tmp/group.ldif

下面就要把这三个文件导入到LDAP，这样LDAP的数据库里就有了我们想要的用户:

# ldapadd -x -D "cn=admin,dc=example,dc=com" -W -f /tmp/base.ldif

# ldapadd -x -D "cn=admin,dc=example,dc=com" -W -f /tmp/passwd.ldif

# ldapadd -x -D "cn=admin,dc=example,dc=com" -W -f /tmp/group.ldif

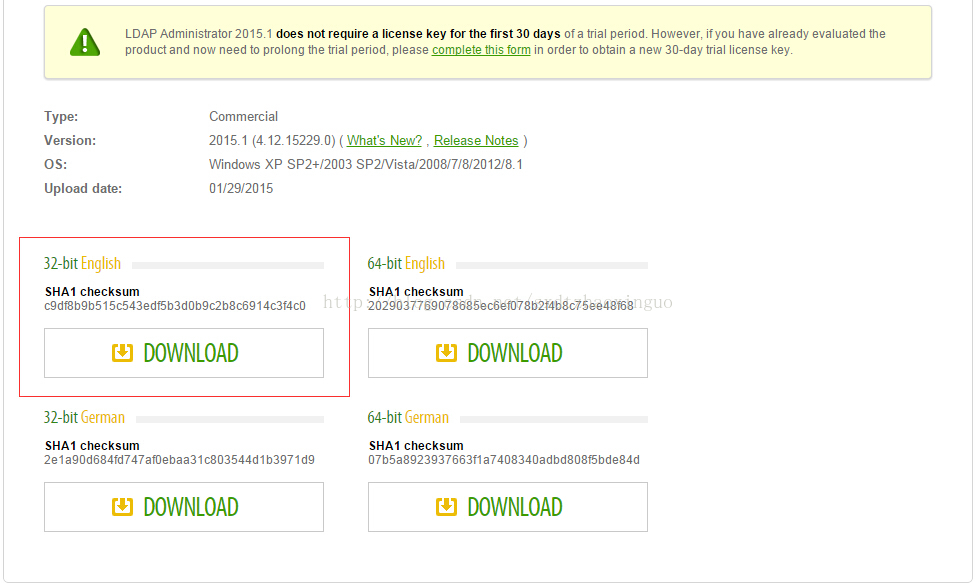
这里导入的时候提示输入LDAP的密码

过程若无报错，则LDAP服务端配置完毕，重启slapd完成配置:

# service slapd restart

通过Softerra LDAP Administrator 2015.1管理工具连接OpenLdap数据库：

(1).首先下载和你本机对应版本的客户端软件，我这里下载的64位的，下载地址：<http://www.ldapadministrator.com/download.htm>，如下图：



(2).下载安装好就可以连接了，连接步骤如下：

