OpenLDAP 安装指南

本手册仅用于配置 Ubuntu9.10 中的 OpenLDAP，其他版本的 OpenLDAP 可能有所不同。

首先，安装 OpenLDAP:

代码:

```
apt-get -y install slapd ldap-utils
```

步骤 1

运行如下命令，将 slapd 包中带的 LDAP schema 全部添加到 cn=config 中（默认只有 core schema 被添加）:

代码:

```
ls /etc/ldap/schema/*.ldif | xargs -I {} sudo ldapadd -Y EXTERNAL -H
ldapi:/// -f {}
```

步骤 2

创建一个 db.ldif 文件，其内容如下所示，此步骤将为域 dc=home,dc=local（即 home.local）安装配置一个 database。并且，只有 cn=admin,dc=hoome,dc=local 可以管理这个数据库（密码：admin）。

代码:

```
# Load modules for database type
dn: cn=module,cn=config
objectclass: olcModuleList
cn: module
olcModuleLoad: back_bdb.la

# Create directory database
dn: olcDatabase=bdb,cn=config
objectClass: olcDatabaseConfig
objectClass: olcBdbConfig
olcDatabase: bdb
# Domain name (e.g. home.local)
olcSuffix: dc=home,dc=local
# Location on system where database is stored
olcDbDirectory: /var/lib/ldap
# Manager of the database
olcRootDN: cn=admin,dc=home,dc=local
olcRootPW: admin
# Indices in database to speed up searches
olcDbIndex: uid pres,eq
olcDbIndex: cn,sn,mail pres,eq,approx,sub
olcDbIndex: objectClass eq
# Allow users to change their own password
```

```
# Allow anonymous to authenciate against the password
# Allow admin to change anyone's password
olcAccess: to attrs=userPassword
 by self write
 by anonymous auth
 by dn.base="cn=admin,dc=home,dc=local" write
 by * none
# Allow users to change their own record
# Allow anyone to read directory
olcAccess: to *
 by self write
 by dn.base="cn=admin,dc=home,dc=local" write
 by * read
```

对上述文件，使用如下命令将数据库添加到 LDAP server 上. 需要知道的是 Karmic 使用 EXTERNAL SASL 和 LDAP server 通信. 这里没有 admin user 或者 password:

代码:

```
sudo ldapadd -Y EXTERNAL -H ldapi:/// -f db.ldif
```

步骤 3

创建另一个文件，该文件包含所有你想要添加的用户，这里以 people.ldif 命名之。

代码:

```
# Create top-level object in domain
dn: dc=home,dc=local
objectClass: top
objectClass: dcObject
objectclass: organization
o: home.local
dc: home
description: Home network

dn: ou=people,dc=home,dc=local
objectClass: organizationalUnit
ou: people

dn: ou=groups,dc=home,dc=local
objectClass: organizationalUnit
ou: groups

dn: uid=john,ou=people,dc=home,dc=local
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: john
sn: Doe
givenName: John
cn: John Doe
displayName: John Doe
```

```
uidNumber: 1000
gidNumber: 10000
userPassword: password
gecos: John Doe
loginShell: /bin/bash
homeDirectory: /home/john
shadowExpire: -1
shadowFlag: 0
shadowWarning: 7
shadowMin: 8
shadowMax: 999999
shadowLastChange: 10877
mail: john.doe@example.com
postalCode: 31000
l: Toulouse
o: Example
mobile: +33 (0)6 xx xx xx xx
homePhone: +33 (0)5 xx xx xx xx
title: System Administrator
postalAddress:
initials: JD

dn: cn=example,ou=groups,dc=home,dc=local
objectClass: posixGroup
cn: example
gidNumber: 10000
```

因为我们已经为 dc=home,dc=local 数据库创建了自己的访问控制，我们必须改变连接方式（例如，使用 admin 用户和其密码来认证）。通过如下命令为目录添加数据：

代码:

```
sudo ldapadd -x -D cn=admin,dc=home,dc=local -w admin -f people.ldif
```

步骤 4

从客户端，你现在就可以用检查你是否可以读取数据库了：

代码:

```
ldapsearch -x -H ldap://dustball.home.local -b dc=home,dc=local
```

故障处理

ldap_add: Other (e.g., implementation specific) error (80)
additional info: <olcModuleLoad> handler exited with 1

该问题的原因在于你试图加载同一个 module 两次，譬如：你已经将 db.ldif 添加了，但是你现在又运行 ldapadd 试图添加它。

ldap_add: Invalid syntax (21)
additional info: olcSuffix: value #0 invalid per syntax

你载 olcSuffice 的值上使用了双引号，譬如： olcSuffix："dn=home,dn=local"。无论你在文档中看到的是什么样子，双引号是不需要的。

ldap_add: Server is unwilling to perform (53)
additional info: no global superior knowledge

你试图往一个不存在的域上添加一些东西。譬如：你想望 dn=home,dn=local 上添加一个 Tom Green，但是 dn=home,dn=local 根本不存在。