Installation OpenLDAP version LTB project

OpenLDAP, LDAP Toolbox Project

Nous installons les paquets pré requis

```
sudo aptitude install apt-transport-https gnupg2
```

Nous créons le fichier du dépôt LTB

```
sudo vi /etc/apt/sources.list.d/ltb-project.list
```

et ajoutons ces lignes

```
##
# LTB project repository
# version: Buster
##

deb [arch=amd64] https://ltb-project.org/debian/buster buster main
```

Nous importons la clé GPG du dépôt

```
wget -qO - https://ltb-project.org/lib/RPM-GPG-KEY-LTB-project | sudo apt-
key add -
```

Nous installons le paquet

```
sudo aptitude update && sudo aptitude install openldap-ltb
```

Configuration

Par défaut, OpenLDAP LTB utilise le fichier slapd.conf. Nous allons plutôt utiliser la méthode cn=config pour stocker la configuration

Nous stoppons le service

```
sudo service slapd stop
```

Nous “salons” notre mot de passe Manager

```
sudo /usr/local/openldap/sbin/slappasswd
```

Il vous est demandé de saisir deux fois votre mot de passe, et le mot de passe “salé” sera généré (exemple avec le mot de passe “secret”

```
New password:
```

```
Re-enter new password:
{SSHA}OZTmkv3eYx3uZHnrG7PtnVyk+AkZh3OS
```

Nous adaptons le fichier slapd.conf

```
sudo vi /usr/local/openldap/etc/openldap/slapd.conf
```

```
#
# See slapd.conf(5) for details on configuration options.
# This file should NOT be world readable.
#
include     /usr/local/openldap/etc/openldap/schema/core.schema
include     /usr/local/openldap/etc/openldap/schema/cosine.schema
include     /usr/local/openldap/etc/openldap/schema/nis.schema
include     /usr/local/openldap/etc/openldap/schema/inetorgperson.schema

# Define global ACLs to disable default read access.

# Do not enable referrals until AFTER you have a working directory
# service AND an understanding of referrals.
#referral   ldap://root.openldap.org

pidfile     /usr/local/openldap/var/run/slapd.pid
argsfile    /usr/local/openldap/var/run/slapd.args

# Load dynamic backend modules:
# modulepath    /usr/local/openldap/libexec/openldap
# moduleload    back_mdb.la
# moduleload    back_ldap.la

# Sample security restrictions
#   Require integrity protection (prevent hijacking)
#   Require 112-bit (3DES or better) encryption for updates
#   Require 63-bit encryption for simple bind
# security ssf=1 update_ssf=112 simple_bind=64

# Sample access control policy:
#   Root DSE: allow anyone to read it
#   Subschema (sub)entry DSE: allow anyone to read it
#   Other DSEs:
#       Allow self write access
#       Allow authenticated users read access
#       Allow anonymous users to authenticate
#   Directives needed to implement policy:
# access to dn.base="" by * read
# access to dn.base="cn=Subschema" by * read
access to *
    by self write
    by users read
```

```
    by anonymous auth
#
# if no access controls are present, the default policy
# allows anyone and everyone to read anything but restricts
# updates to rootdn.  (e.g., "access to * by * read")
#
# rootdn can always read and write EVERYTHING!

#######################################################################
# MDB database definitions
#######################################################################

database    mdb
maxsize     1073741824
suffix      "dc=domain,dc=tld"
rootdn      "cn=Manager,dc=domain,dc=tld"
# Cleartext passwords, especially for the rootdn, should
# be avoid.  See slappasswd(8) and slapd.conf(5) for details.
# Use of strong authentication encouraged.
rootpw      {SSHA}OZTmkv3eYx3uZHnrG7PtnVyk+AkZh3OS
# The database directory MUST exist prior to running slapd AND
# should only be accessible by the slapd and slap tools.
# Mode 700 recommended.
directory   "/usr/local/openldap/var/openldap-data"
# Indices to maintain
index   objectClass    eq
```

Nous créons le répertoire qui accueillera la configuration

```
sudo mkdir -v /usr/local/openldap/etc/openldap/slapd.d/
```

Nous copions la configuration

```
sudo /usr/local/openldap/sbin/slaptest -f
/usr/local/openldap/etc/openldap/slapd.conf -F
/usr/local/openldap/etc/openldap/slapd.d -d 256
```

Nous mettons les droits sur le répertoire

```
sudo chown -R ldap.ldap /usr/local/openldap/etc/openldap/slapd.d
```

Nous adaptons le paramètre “SLAPD_CONF_DIR” dans le fichier /usr/local/openldap/etc/openldap/slapd-cli.conf

```
SLAPD_CONF_DIR="$SLAPD_PATH/etc/openldap/slapd.d"
```

Nous démarrons le service

```
sudo service slapd start
```

Peuplement de l'annuaire

Nous créons un fichier base.ldif

```
cd ~
vi base.ldif
```

Nous y ajoutons les éléments

```
dn: dc=domain,dc=tld
objectClass: top
objectClass: dcObject
objectClass: organization
o: domain.tld
dc: domain

dn: ou=users,dc=domain,dc=tld
ou: users
objectClass: organizationalUnit
objectClass: top

dn: ou=groups,dc=domain,dc=tld
ou: groups
objectClass: organizationalUnit
objectClass: top
```

Nous ajoutons ces infos à l'annuaire

```
sudo /usr/local/openldap/bin/ldapadd -x -D "cn=Manager,dc=domain,dc=tld" -W
-f base.ldif
```

Nous listons le contenu de notre annuaire

```
sudo ldapsearch -x -H ldap://localhost -D cn=Manager,dc=domain,dc=tld -W -b
dc=domain,dc=tld -LLL
```

Liens

- téléchargement depuis dépôt APT du projet
- documentation