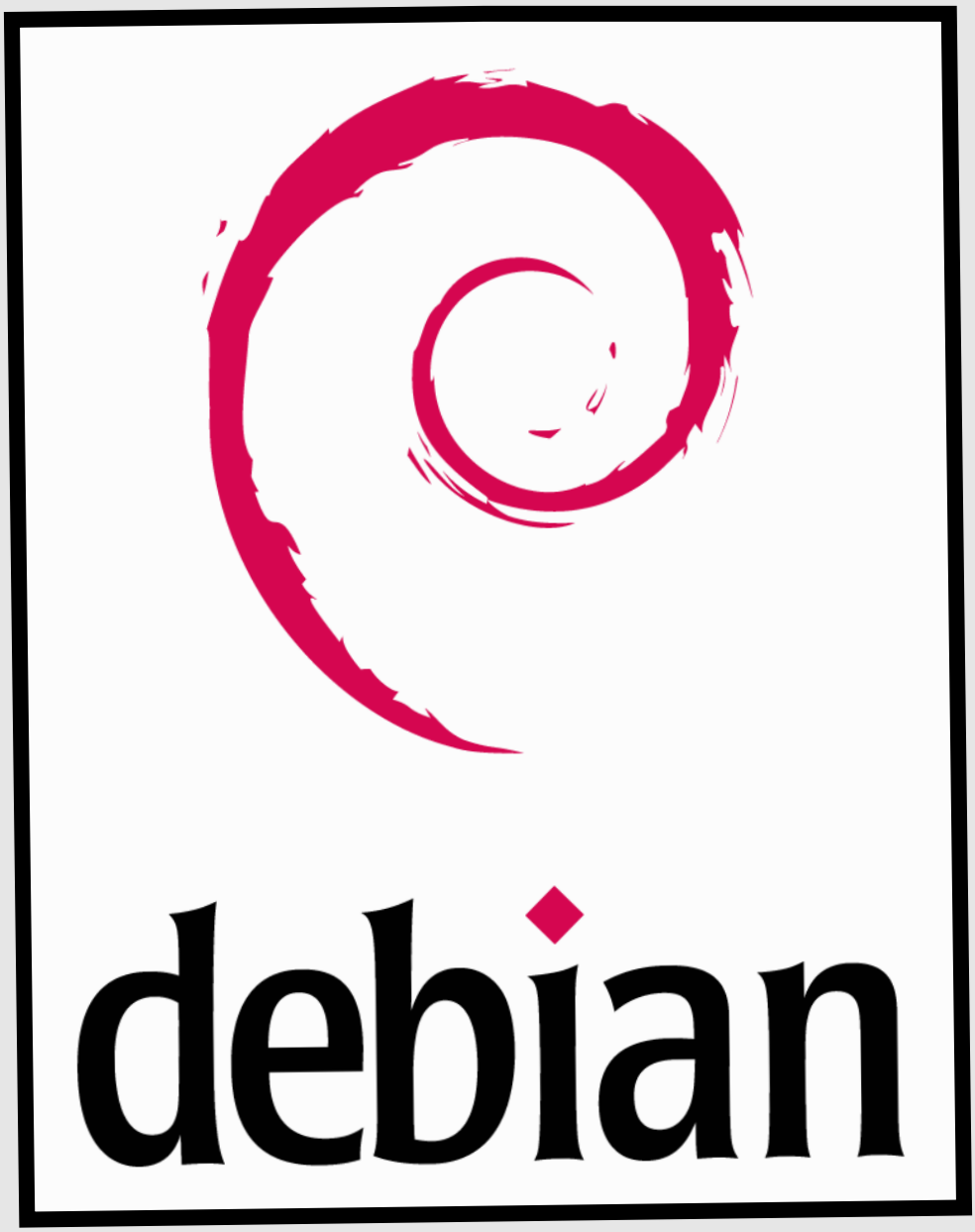
Enzo Lefrançois

version 1.0



Installation Configuration

Serveur LDAP

Debian 7.2

OpenLDAP 2.4.39

Objectif : Mettre en place une base d'annuaire sous debian qui permettra de gérer des utilisateurs au sein d'un domaine.

LDAP (Light Directory Access Protocol) est un service d'annuaire dérivé de la norme X.500. La norme X.500 est très lourde, LDAP en est une version allégée ("light") dans un sens absolument pas péjoratif.

Vous trouverez de bien meilleures descriptions du principe, concept et du protocole LDAP en suivant les références indiquées à la fin de ce document.

Un serveur LDAP permet de centraliser des informations très diverses. Il offre de nombreux avantages :

- un serveur d'annuaire (recensement de tous les objets d'un système) : c'est la fonction la plus connue, on peut trouver des serveurs LDAP chez bigfoot, netscape (netcentrer), infoseek et bien d'autres ;

- Information sur les utilisateurs (nom, prénom...), et données d'authentification pour les utilisateurs : cela permet aussi la définition de droits.

- Information pour les applications clientes et fonctions de serveur d'accès itinérant : cela permet de stocker ses informations personnelles sur un serveur et de les récupérer lors de la connexion;

Installation du serveur LDAP :

En premier , il faut aller rechercher l'archive à l'adresse ftp dans les serveurs de debian :

```
root@debian:~# wget ftp://ftp.openldap.org/pub/OpenLDAP/openldap-release/openlda
p-2.4.39.tgz_
```

Puis, on installe libtool :

```
root@debian:~# apt-get install libtool libltdl-dev libssl-dev libdb5.1-dev libsa
asl2-dev_
```

Ensuite, on extrait dans le même répertoire le fichier openldap téléchargé précédemment :

```
root@debian:~# tar xzvf openldap-2.4.39.tgz_
```

Puis, on se place dans le dossier créé afin de taper diverses commandes pour procéder à l'installation :

```
root@debian:~# cd openldap-2.4.39_
```

En premier, la commande **./configure**, suivi de tous ses arguments afin de spécifier tous les champs :

```
root@debian:~/openldap-2.4.39# ./configure -enable-crypt=yes -enable-lmpasswd=ye
s -enable-spasswd=yes -enable-modules=yes -enable-overlays=yes_
```

Puis, on crée les dépendances :

```
root@debian:~/openldap-2.4.39# make depend_
```

Avant on créer le fichier pour ensuite faire l'installation :

```
root@debian:~/openldap-2.4.39# make_
```

Ensuite, on lance l'installation avec la commande **make install** :

```
root@debian:~/openldap-2.4.39# make install_
```

Configuration du serveur LDAP:

En premier, on ajoute un utilisateur afin d'éviter d'utiliser le root. On crée un utilisateur sans shell :

```
root@debian:~/openldap-2.4.39# useradd -s /bin/false -d /usr/local/var/openldap-
data openldap
```

Puis, on se place dans le répertoire du fichier de configuration **slapd.conf** et on l'ouvre :

```
root@debian:~# cd /usr/local/etc/openldap
root@debian:/usr/local/etc/openldap# ls
DB_CONFIG.example  ldap.conf.default  slapd.conf          slapd.ldif
ldap.conf          schema             slapd.conf.default  slapd.ldif.default
root@debian:/usr/local/etc/openldap# _
```

On modifie les lignes suivantes en les décommentant sur le fichier :

```
  GNU nano 2.2.6                Fichier : slapd.conf

#       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
#
```

Puis, on crée un utilisateur manager avec mot de passe password :

```
root@debian:~# adduser manager
Ajout de l'utilisateur « manager » ...
Ajout du nouveau groupe « manager » (1010) ...
Ajout du nouvel utilisateur « manager » (1010) avec le groupe « manager » ...
Création du répertoire personnel « /home/manager »...
Copie des fichiers depuis « /etc/skel »...
Entrez le nouveau mot de passe UNIX :
Retapez le nouveau mot de passe UNIX :
passwd : le mot de passe a été mis à jour avec succès
Modification des informations relatives à l'utilisateur manager
Entrez la nouvelle valeur ou « Entrée » pour conserver la valeur proposée
        Nom complet []: nom
        N° de bureau []: bureau
        Téléphone professionnel []: téléphone
        Téléphone personnel []: jesaisplus
        Autre []: ben, j'en sais rien moi
chfn : téléphone professionnel non valable : « téléphone »
adduser : « /usr/bin/chfn manager » a retourné le code d'erreur 1. Abandon.
root@debian:~# adduser manager
adduser : L'utilisateur « manager » existe déjà.
root@debian:~#
root@debian:~# _
```

Si l'on veut supprimer un utilisateur, il faut utiliser la commande **userdel** :

```
root@debian:~# userdel -r manager
userdel : l'emplacement de boîte aux lettres de manager (/var/mail/manager) n'a
pas été trouvé
userdel : le répertoire personnel de manager (/home/manager) n'a pas été trouvé
root@debian:~# _
```

Ensuite on crée un répertoire pour ldap :

```
root@debian:~# mkdir /usr/local/etc/openldap/slapd.d
root@debian:~# _
```

Ensuite, on se déplace dans le dossier :

```
root@debian:~# cd /usr/local/etc/openldap
root@debian:/usr/local/etc/openldap# _
```

Puis on fait un test avec la commande **slaptest** qui nous renverra un message négatif :

```
root@debian:/usr/local/etc/openldap# slaptest -f slapd.conf -F slapd.d_
```

Ensuite, on change les droits avec la commande **chown** :

```
root@debian:/usr/local/etc/openldap# chown -R openldap.openldap /usr/local/etc/o
penldap_
```

Puis on va dans le répertoire openldap-data et on crée le fichier **db-config** :

```
root@debian:~# cd /usr/local/var/openldap-data
root@debian:/usr/local/var/openldap-data# ls
alock      __db.002  __db.004  __db.006
__db.001   __db.003  __db.005  DB_CONFIG.example
root@debian:/usr/local/var/openldap-data# _
```

```
root@debian:/usr/local/var/openldap-data# touch DB_CONFIG
root@debian:/usr/local/var/openldap-data# _
```

Ensuite on déplace les fichiers de configuration avec cette commande :

```
root@debian:~# mv /usr/local/var/openldap-data/DB_CONFIG.example /usr/local/var/
openldap-data/DB_CONFIG_
```

Ensuite, on retape la commande **chown** pour modifier les droits :

```
root@debian:~# chown -R openldap.openldap /usr/local/var/openldap-data_
```

Puis, la commande **slapd avec les attributs u , g et h** :
u et g signifient sous quel utilisateur et groupe le serveur doit tourner. l'argument h indique le type de connexion supporté (ici, connexion simple).

```
root@debian:~# /usr/local/libexec/slapd -u openldap -g openldap -h 'ldap:///'
root@debian:~# _
```

Ensuite, si l'on à oublié de modifier tout le fichier de configuration, on fait la commande suivant: on copie de fichier db config pour le réinjecter plus tard :

```
root@debian:/usr/local/etc/openldap# cp /usr/local/var/openldap-data/DB_CONFIG /
root/
root@debian:/usr/local/etc/openldap# _
```

Puis on supprime toutes les données utilisateurs :

```
root@debian:~# rm -rf /usr/local/etc/openldap/slapd.d/*
root@debian:~#
root@debian:~# rm -rf /usr/local/var/openldap-data/*
root@debian:~# _
```

Puis, on remets le fichier configuration dans le répertoire précédent :

```
root@debian:~# cp /root/DB_CONFIG /usr/local/var/openldap-data/
root@debian:~# _
```

Ensuite, voila le fichier de configuration totalement rempli :

```
  GNU nano 2.2.6              Fichier : slapd.conf                        Modifié

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

# Load dynamic backend modules:
```

```
# Load dynamic backend modules:
# modulepath    /usr/local/libexec/openldap
# moduleload    back_bdb.la
# moduleload    back_hdb.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 *
```

```
 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!

#######################################################################
```

```
#######################################################################
# BDB database definitions
#######################################################################
database config
rootdn          "cn=manager,cn=config"
rootpw          password


database        bdb
suffix          "dc=rezo,dc=com"
rootdn          "cn=admin,dc=rezo,dc=com"
# Cleartext passwords, especially for the rootdn, should
```

```
database        bdb
suffix          "dc=rezo,dc=com"
rootdn          "cn=admin,dc=rezo,dc=com"
# Cleartext passwords, especially for the rootdn, should
# be avoid.  See slappasswd(8) and slapd.conf(5) for details.
# Use of strong authentication encouraged.
rootpw          password
# 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/var/openldap-data
# Indices to maintain
index   objectClass     eq
index   uid     eq
index   cn,gn,mail      eq,sub
```

```
rootpw          password
# 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/var/openldap-data
# Indices to maintain
index   objectClass     eq
index   uid     eq
index   cn,gn,mail      eq,sub
index   ou      eq
index   default eq,sub
```

Ensuite, on lance la commande **/usr/local/libexec/slapd -d 3**. Puis, on ouvre une nouvelle session avec la commande **ctrl+alt+f1 à f6** en fonction de la session que l'on veut ouvrir.

Ensuite, dans la session 2, on tape la commande suivante :

```
root@debian:~# slapcat -s cn=config | less_
```

Puis, on ouvre une 3e session et on tape la commande suivante :

```
root@debian:~# ldapsearch -b cn=config -D "cn=manager,cn=config" -w password
```

Ensuite, il faut créer un fichier **init.ldif** :

```
root@debian:~# nano /usr/local/etc/openldap/init.ldif_
```

Dans ce fichier, on insert les lignes suivantes:

```
dn:     dc=rezo,dc=com
objectclass:    dcObject
objectclass:    organization
o:      Linux
dc:     rezo

dn:     cn=admin,dc=rezo,dc=com
objectclass:    organizationalRole
cn:     admin_
```

Puis, on lance la commande suivante, afin d'ajouter de nouvelles entrées:

```
root@debian:~# ldapadd -x -D"cn=admin,dc=rezo,dc=com" -w password -f /usr/local/
etc/openldap/init.ldif
adding new entry "dc=rezo,dc=com"

adding new entry "cn=admin,dc=rezo,dc=com"

root@debian:~# _
```

Ensuite, on effectue la commande suivante:

```
root@debian:~# ldapsearch -LLL -x -D "cn=admin,dc=rezo,dc=com" -w password -b 'd
c=rezo,dc=com' '(objectclass=*)'
dn: dc=rezo,dc=com
objectClass: dcObject
objectClass: organization
o: Linux
dc: rezo

dn: cn=admin,dc=rezo,dc=com
objectClass: organizationalRole
cn: admin

root@debian:~# _
```

Puis, on crée le fichier **ou.ldif** :

```
root@debian:~# nano /usr/local/etc/openldap/ou.ldif_
```

Dans ce fichier, on rentre les paramètres suivants :

```
dn:     ou=people,dc=rezo,dc=com
objectclass:    organizationalUnit
ou:     people

dn:     ou=groups,dc=rezo,dc=com
objectclass:    organizationalUnit
ou:     groups
```

Puis, on ajoute les entrées du fichier :

```
root@debian:/usr/local/etc/openldap# ldapadd -x -D"cn=admin,dc=rezo,dc=com" -w p
assword -f ou.ldif
adding new entry "ou=people,dc=rezo,dc=com"
ldap_add: Already exists (68)

root@debian:/usr/local/etc/openldap# _
```

Ensuite, on crée le fichier **users.ldif** :

```
root@debian:/usr/local/etc/openldap# nano users.ldif_
```

Et, on ajoute les lignes suivantes dans le fichier :

```
  GNU nano 2.2.6                Fichier : users.ldif

dn:     cn=sfonfec,ou=people,dc=rezo,dc=com
objectclass:    top
objectclass:    account
objectclass:    posixAccount
objectclass:    shadowAccount
uid:    sfonfec
uidnumber:      1500
gidnumber:      10000
userpassword:   password
gecos:  sophie  Fonfec
loginshell:     /bin/bash
homedirectory:  /home/sfonfec
shadowwarning:  7
shadowmin:      8
shadowmax:      9999
shadowlastchange:       10877_
```

Puis, on crée le fichier **groups.ldif** et on ajoute les lignes suivantes :

```
root@debian:/usr/local/etc/openldap# nano groups.ldif_
```

```
  GNU nano 2.2.6                Fichier : groups.ldif

dn:     cn=ldap,ou=groups,dc=rezo,dc=com
objectclass:    top
objectclass:    posixGroup
cn:     ldap
gidNumber:      10000_
```

Puis, on mets les entrées du fichier a jour:

```
root@debian:/usr/local/etc/openldap# ldapadd -x -D"cn=admin,dc=rezo,dc=com" -w p
assword -f users.ldif
adding new entry "cn=sfonfec,ou=people,dc=rezo,dc=com"

root@debian:/usr/local/etc/openldap# _
```

```
root@debian:/usr/local/etc/openldap# ldapadd -x -D"cn=admin,dc=rezo,dc=com" -w p
assword -f groups.ldif
adding new entry "cn=ldap,ou=groups,dc=rezo,dc=com"
ldap_add: No such object (32)
        matched DN: dc=rezo,dc=com

root@debian:/usr/local/etc/openldap# _
```

Puis, on tape cette commande :

```
root@debian:/usr/local/etc/openldap# ldapsearch -x -D 'cn=sfonfec,ou=people,dc=r
ezo,dc=com' -w password -b 'ou=people,dc=rezo,dc=com' _
```

Ensuite, on se connecte avec l'utilisateur créé dans les fichiers afin de valider la configuration :

```
objectClass: top
objectClass: account
objectClass: posixAccount
objectClass: shadowAccount
uid: sfonfec
uidNumber: 1500
gidNumber: 10000
userPassword:: cGFzc3dvcmQ=
gecos:: c29waGllCUZvbmZlYw==
loginShell: /bin/bash
homeDirectory: /home/sfonfec
shadowWarning: 7
shadowMin: 8
shadowMax: 9999
shadowLastChange: 10877
cn: sfonfec

# search result
search: 2
result: 0 Success

# numResponses: 3
# numEntries: 2
root@debian:/usr/local/etc/openldap# _
```

Installation et configuration de Samba :

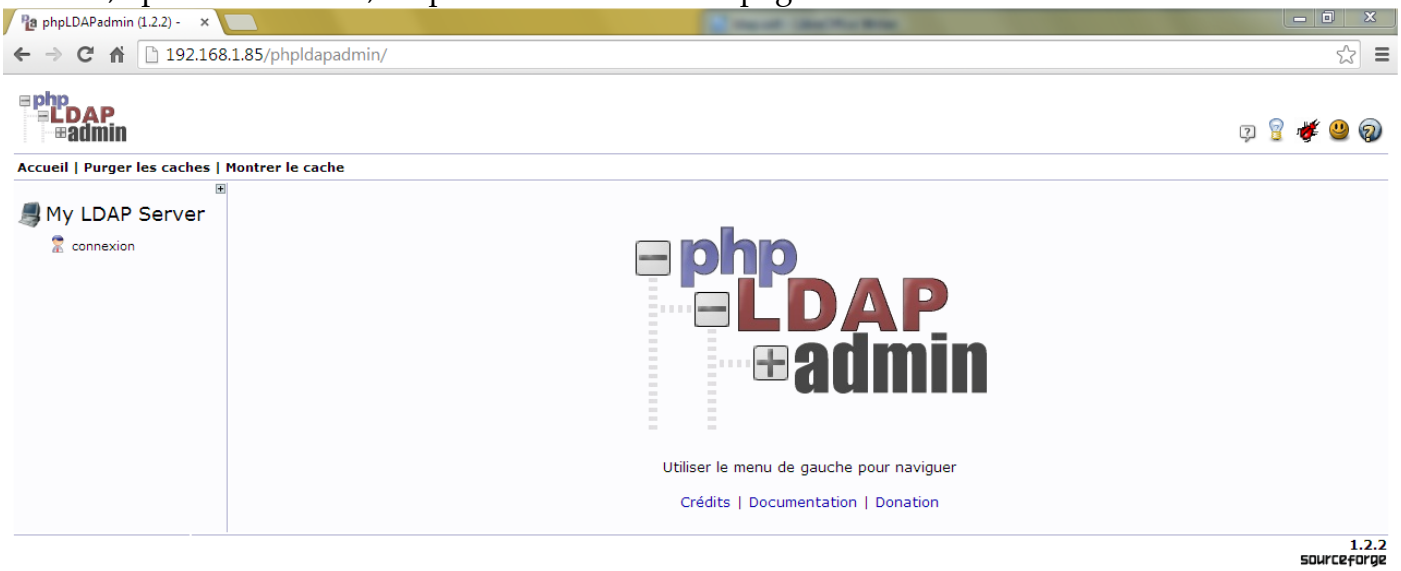
En premier, installer php5 :

```
root@debian:~# apt-get install php5
```

Puis, installer phpldapadmin :

```
root@debian:~# apt-get install phpldapadmin
```

Ensuite, après installation, on peut se connecter à la page internet de notre serveur:



Ensuite, il faut modifier les droits d'accès aux fichiers :

```
root@debian:~# chown -R www-data:www-data /etc/phpldapadmin
```

```
root@debian:~# cd /etc/phpldapadmin/
root@debian:/etc/phpldapadmin# ls
apache.conf  config.php  templates
root@debian:/etc/phpldapadmin# chmod 640 config.php
root@debian:/etc/phpldapadmin# _
```

```
root@debian:/etc/phpldapadmin# chown -R www-data:www-data /usr/share/phpldapadmi
n
root@debian:/etc/phpldapadmin# _
```

En premier, on va dans php my admin et on modifie le fichier **config.php** :

```
root@debian:~# cd /etc/phpldapadmin/
root@debian:/etc/phpldapadmin# ls
apache.conf  config.php  templates
root@debian:/etc/phpldapadmin# nano config.php _
```

Dans le fichier, modifier les paramètres suivants :

```
$servers = new Datastore();

/* $servers->NewServer('ldap_pla') must be called before each new LDAP server
   declaration. */
$servers->newServer('ldap_pla');

/* A convenient name that will appear in the tree viewer and throughout
   phpLDAPadmin to identify this LDAP server to users. */
$servers->setValue('server','name','thibi');
```

```
/* Array of base DNs of your LDAP server. Leave this blank to have phpLDAPadmin
   auto-detect it for you. */
$servers->setValue('server','base',array('dc=rezo,dc=com'));
```

```
   binds. */
$servers->setValue('login','bind_id','cn=admin,dc=rezo,dc=com');
#  $servers->setValue('login','bind_id','cn=Manager,dc=example,dc=com');
```

En premier, il faut copier le fichier d'archive samba dans le répertoire openldap:

```
root@debian:~# cp /usr/share/doc/samba-doc/examples/LDAP/samba.ldif.gz /usr/loca
l/etc/openldap/
root@debian:~# _
```

Puis, il faut dézipper le fichier avec la commande **gunzip** :

```
root@debian:/usr/local/etc/openldap# gunzip samba.ldif.gz
root@debian:/usr/local/etc/openldap# ls
DB_CONFIG.example  ldap.conf.default  slapd.conf          slapd.ldif.default
groups.ldif        ou.ldif            slapd.conf.default  users.ldif
init.ldif          samba.ldif         slapd.d
ldap.conf          schema             slapd.ldif
root@debian:/usr/local/etc/openldap# _
```

Ensuite, il faut ajouter dynamiquement le serveur :

```
root@debian:/usr/local/etc/openldap# ldapadd -x -w password -D 'cn=manager,cn=co
nfig' -f samba.ldif
adding new entry "cn=samba,cn=schema,cn=config"

root@debian:/usr/local/etc/openldap# _
```

Puis, il faut créer le fichier **sambaou.ldif** et implémenter les lignes suivantes :

```
root@debian:/usr/local/etc/openldap# nano sambaou.ldif_
```

```
  GNU nano 2.2.6                Fichier : sambaou.ldif

dn:     ou=Computers,dc=rezo,dc=com
objectclass:    organizationalUnit
ou:     Computers
```

En dernier, il faut injecter ce fichier crée :

```
root@debian:/usr/local/etc/openldap# ldapadd -x -D"cn=admin,dc=rezo,dc=com" -w p
assword -f sambaou.ldif
adding new entry "ou=Computers,dc=rezo,dc=com"

root@debian:/usr/local/etc/openldap# _
```

Puis, il faut aller dans le fichier **smb.conf** et ajouter les lignes suivantes :

```
# If you are using encrypted passwords, Samba will need to know what
# password database type you are using.
   passdb backend = ldapsam:ldap://192.168.1.85.rezo.com:389
ldap admin dn="cn=admin,dc=rezo,dc=com"
ldap suffix=dc=rezo,dc=com
ldap delete dn=no
ldap password sync=yes
ldap user suffix=ou=people
ldap group suffix=ou=groups
ldap machine suffix=ou=Computers
ldap ssl=off
```

Puis, il faut faire la commande suivante :

```
root@debian:~# smbpasswd -w password
Setting stored password for "cn=admin,dc=rezo,dc=com" in secrets.tdb
root@debian:~#
```

Puis, il faut ensuite créer l'utilisateur titi :

```
root@debian:~# adduser titi
Ajout de l'utilisateur « titi » ...
Ajout du nouveau groupe « titi » (1011) ...
Ajout du nouvel utilisateur « titi » (1011) avec le groupe « titi » ...
Création du répertoire personnel « /home/titi »...
Copie des fichiers depuis « /etc/skel »...
Entrez le nouveau mot de passe UNIX :
Retapez le nouveau mot de passe UNIX :
passwd : le mot de passe a été mis à jour avec succès
Modification des informations relatives à l'utilisateur titi
Entrez la nouvelle valeur ou « Entrée » pour conserver la valeur proposée
        Nom complet []: titi
        N° de bureau []: titi
        Téléphone professionnel []: titi
        Téléphone personnel []: titi
        Autre []: titi
Cette information est-elle correcte ? [O/n]o
```