Dernière mise-à-jour : 2020/01/30 03:27

Topic 210 - Gestion du Client et du Serveur OpenLDAP (6/60)

210.3 - LDAP client usage

Weight: 2 Description: Candidates should be able to perform queries and updates to an LDAP server. Also included is importing and adding items, as well as adding and managing users.

Key Knowledge Areas:

- LDAP utilities for data management and queries
- Change user passwords
- Querying the LDAP directory

Terms and Utilities:

- ldapsearch
- ldappasswd
- ldapadd
- ldapdelete

210.4 - Configuring an OpenLDAP server

Weight: 4

Description: Candidates should be able to configure a basic OpenLDAP server including knowledge of LDIF format and essential access controls.

Key Knowledge Areas:

- OpenLDAP
- Directory based configuration
- Access Control
- Distinguished Names
- Changetype Operations
- Schemas and Whitepages
- Directories
- Object IDs, Attributes and Classes

Terms and Utilities:

- slapd
- slapd-config
- LDIF
- slapadd
- slapcat
- slapindex
- /var/lib/ldap/
- loglevel

Présentation

Qu’est-ce que LDAP ?

LDAP est une abréviation de **L**ighweight **D**irectory **A**ccess **P**rotocol. Comme son nom indique, LDAP est un service d'**annuaire**.

Un service d'annuaire est une base de données spécialisée optimisée pour la consultation. Certains services d'annuaire peuvent être locaux tandis que d'autres sont appellés **distribués**. Un bon exemple d'une service d'annuaire distribué est le **DNS**.

Plusieurs points sont à retenir :

- LDAP est un adaptation TCP/IP du protocole **DAP** (**D**irectory **A**ccess **P**rotocol),
- LDAP et DAP sont des protocoles d'interrogation des annuaires au format **X.500**,

- LDAP utilise TCP/IP au lieu de parcourir les sept couches du modèle OSI, d'où la notion de **Lighweight**,
- LDAP emploie une approche client/serveur en mode connecté sur le port **389/tcp**,
- LDAPS emploie une approche client/serveur sécurisée via SSL en mode connecté sur le port **636/tcp**. Il utilise aussi **TLS** et **SASL**,
- LDAP utilise le codage **B**asic **E**ncoding **R**ule au lieu d'ASCII. Cette approche consiste en un codage en hexadécimal d'un code en décimal correspondant à une action spécifique. Par exemple, l'opération **Search Request** correspond au code **63**,
- LDAP prévoit la **réplication** des données :
  - La réplication **Maître > Esclave** appelée **push-based** ou encore **SIR** (**S**erver **I**nitiated **R**eplication),
  - La réplication **Esclave > Maître** appelée **pull-based** ou encore **CIR** (**C**onsumer **I**nitiated **R**eplication),

Le Protocole X.500

X.500 est un ensemble de normes qui s'appuie sur le modèle **OSI** :

- **X.509** - mécanismes d'authentification par clefs publiques,
- **X.511** - services offerts par X.500 tels les recherches et les modifications,
- **X.519** - protocoles de communication, y compris le **DAP**, entre deux serveurs X.500 et entre un client et serveur X.500.

LDAP v3

LDAP est actuellement à la version **3**. Cette version est notamment définie par :

- **RFC 4510** - LDAP: Technical Specification Road Map qui remplace le **RFC3377**,
- **RFC 4511** - LDAP: Authentification Methods and Security Mechanisms qui remplace les RFC **RFC 2829** et **RFC 2830**,

Comment fonctionne LDAP ?

Le protocole LDAP définit neuf opérations divisées en trois catégories :

- **Accès à l'annuaire** - bind, unbind, abandon,
- **Interrogation** - search, compare,
- **Mise à jour** - add, delete, modify, modifyDN.

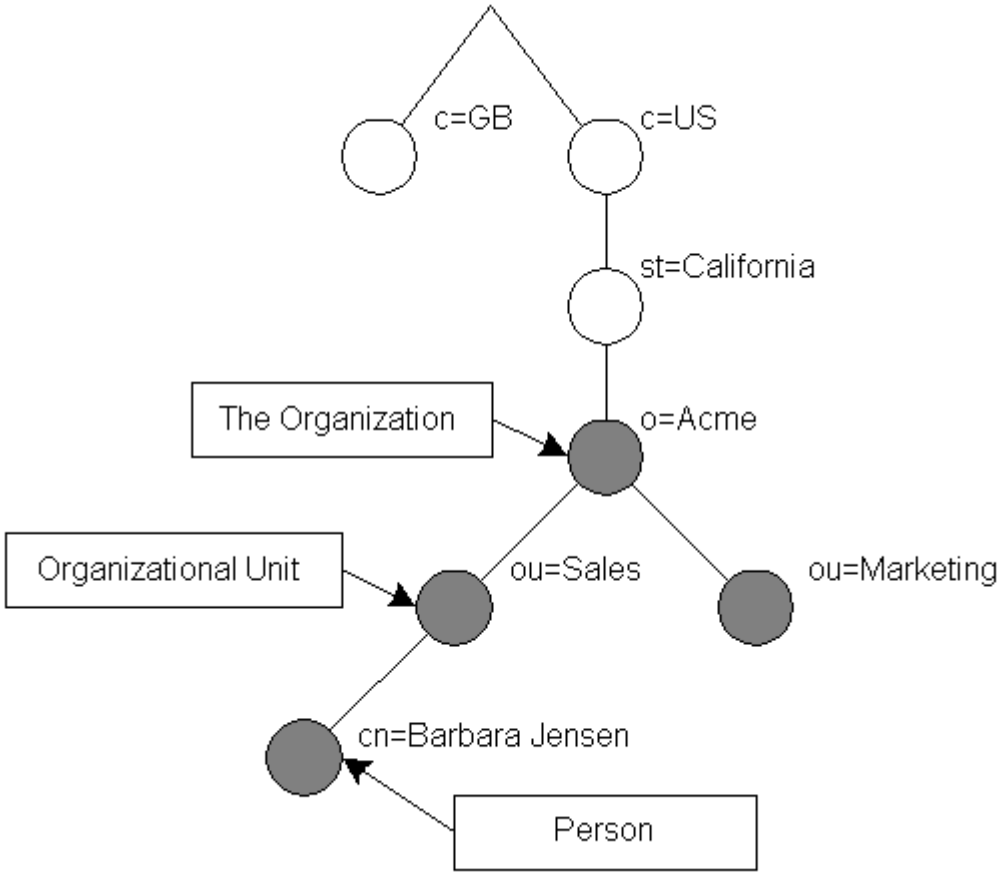
Le Modèle d'Information de LDAP

Le modèle d'information de LDAP est basé sur des **entrées** :

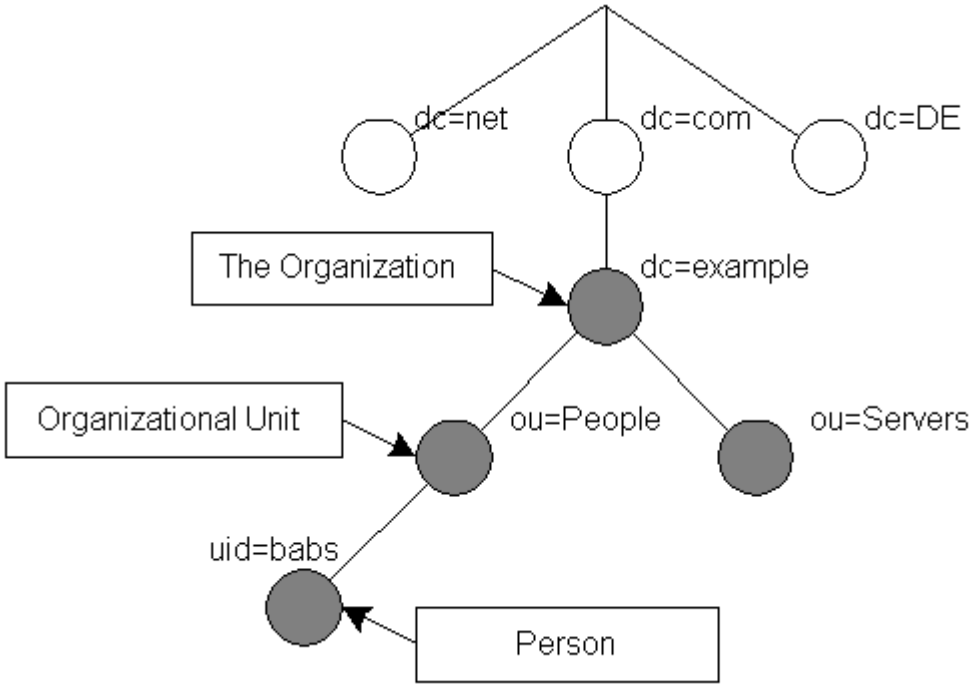
- L'ensemble des entrées est contenu dans un **DIT** (**D**irectory **I**nformation **T**ree),
- Chaque entrée représente une instance d'une **classe** d'objets contenant une collection d'**attributs** qui possède un nom unique appelé le **D**istinguished **N**ame et un nom relatif appelé le **R**elative **D**istinguished **N**ame.

Deux structures classiques des entrées sont :

- l'organisation géographique



- l'organisation Internet



Les DN et les RDN

Un DN est l'ensemble des RDN des noeuds supérieurs :

- cn=hugh norris, ou=formation, dc=hugh-norris, dc=info

Un RDN est un couple composé d'un attribut et un valeur, par exemple :

- mail=info@hugh-norris.info

Dans le cas de plusieurs couples, ceux-ci sont séparés par le caractère **+** :

- mail=info@hugh-norris.info+cn=info

Le format des valeurs de attributs ne doit **pas** contenir :

- Le caractère **#** ou un espace au début de la chaîne,
- Un espace à la fin de la chaîne.

En plus des ces restrictions, les caractères suivants doivent être protégés par le caractère **** :

- ,
- +
- “
- \
- <
- >
- ;

La Structure d’un annuaire LDAP

Les Attributs

Un attribut est défini par un ensemble d'informations :

- Un ou plusieurs noms,
- Des règles de comparaison telles EQUALITY, ORDERING, SUBSTR,
- Une syntaxe définie par un OID,
- Un indicateur de multivaluation tel SINGLE-VALUE,
- Un indicateur de modification par l'utilisateur tel NO-USER-MODIFICATION,
- Un indicateur d'usage USAGE qui indique le type de l'attribut soit utilisateur ou opérationnel.

Les Attributs Utilisateur

Ce sont des attributs pouvant être modifiés par des utilisateurs ayant le droit d'écriture.

Les Attributs Opérationnels

Ce sont de attributs stockant les information sur le statut de l'annuaire.

Les Classes d'Objets

Une classe d'objets est définie par :

- Un OID,
- Un nom,
- Une hiérarchie de classes supérieurs,
- Un type, soit Abstract, Structural ou Auxiliary,
- Une liste d'attributs obligatoires,
- Une liste d'attributs facultatifs.

Les Types de Classe d'Objets

Le type de classe d'objets peut être :

- **Abstract** - une classe abstraite dont d'autres classes vont pouvoir hériter,
- **Structural** - un objet **réel**. Chaque entrée de l'annuaire n'a qu'une seule classe d'objets structurelle,
- **Auxiliary** - une classe d'objets auxiliaire qui sert à compléter un objet structurel :
  - **extensibleObject** - ne contenant aucun attribut obligatoire, elle contient en tant qu'attributs facultatifs tous les attributs définis dans le schéma de l'annuaire,
  - **subschema** - ne contenant aucun attribut obligatoire, elle contient l'ensemble des classes d'objets de l'annuaire, les règles de comparaison, les attributs et les syntaxes.

Les OID

Chaque attribut et chaque classe d'objets est décrit par un OID (**O**ject **ID**entifier) :

- Les OID sont attibués par IANA (**I**nternet **A**ssigned **N**umbers **A**uthority),
- LDAP contient les OID suivants :
  - 2.5.4 - attributs utilisateurs,
  - 2.5.18 - attributs opérationnels,
  - 1.3.6.1.4.1.1466.115.121.1 - syntaxe des attributs,
  - 2.5.6 - classes d'objets.

Les Schémas de l'Annuaire

Un **schéma** regroupe les informations suivantes :

- Les classes d'objets,
- Les attributs,
- La syntaxe des attributs,
- Les règles de comparaison.

Un schéma **doit** contenir au moins une classe d'objets.

Les schémas les plus utilisés sont :

Schéma	**Description**
core.schema	**Obligatoire**. Permet de stocker dans l'annuaire les Common Attribute Object Classes. C'est le noyau OpenLDAP.
cosine.schema	**Utile** - Permet le support des annuaires **cosine** et X.500.
inetorgperson.schema	**Utile** - Permet de stocker dans l'annuaire les informations concernant les personnes.
bind.schema	Permet de stocker dans l'annuaire des objets DNS.
dhcp.schema	Permet de stocker dans l'annuaire des objets DHCP.
nis.scema	Permet de stocker dans l'annuaire les utilisateurs UNIX et les paramètres associés.
samba3.schema	Permet l'intégration de samba et LDAP.
cobra.schema	Permet de stocker dans l'annuaire des objets **COBRA** (**C**ommon **O**bject **B**roker **R**equest **A**rchitecture).
openldap.schema	**Expérimental**. Concerne le projet OpenLDAP Project.
dyngroup.schema	**Expérimental**. Dynamic Group - utilisé avec le Netscape Enterprise Server.
collective.schema	**Expérimental**. Permet de stocker dans l'annuaire des objets collectifs.

Schéma	Description
java.schema	**Expérimental**. Permet de stocker dans l'annuaire des objets java.
misc.schema	**Expérimental**. Permet le routage des messages électroniques (emails).
ppolicy.schema	**Expérimental**. Schéma de stratégie de mots de passe.

Installation du serveur LDAP

Pour installer le serveur OpenLDAP sous GNU/Linux ou Unix vous pouvez soit utiliser la version binaire fournie par les dépôts de paquets de votre distribution GNU/Linux ou Unix soit télécharger la dernière version à compiler du site d'OpenLDAP.

Dans notre cas, nous allons installer OpenLDAP à partir des dépôts sur un système RHEL / CentOS. Commencez par mettre à jour le système :

```
[root@centos6 ~]# yum update --skip-broken
```

Puis installez OpenLDAP :

```
[root@centos6 ~]# yum install openldap-servers openldap-clients openldap
Loaded plugins: fastestmirror, refresh-packagekit, security
Loading mirror speeds from cached hostfile
 * atomic: mir01.syntis.net
 * base: centos.quelquesmots.fr
 * epel: mirror.1000mbps.com
 * extras: centos.quelquesmots.fr
 * rpmforge: mirror.ate.info
 * updates: centos.quelquesmots.fr
Setting up Install Process
Resolving Dependencies
--> Running transaction check
---> Package openldap.i686 0:2.4.23-32.el6_4.1 will be updated
---> Package openldap.i686 0:2.4.23-34.el6_5.1 will be an update
---> Package openldap-clients.i686 0:2.4.23-34.el6_5.1 will be installed
---> Package openldap-servers.i686 0:2.4.23-34.el6_5.1 will be installed
```

```
--> Processing Dependency: libcrypto.so.10(libcrypto.so.10) for package: openldap-servers-2.4.23-34.el6_5.1.i686
--> Running transaction check
---> Package openssl.i686 0:1.0.0-27.el6_4.2 will be updated
---> Package openssl.i686 0:1.0.1e-16.el6_5.7 will be an update
--> Finished Dependency Resolution

Dependencies Resolved

================================================================================================================
================================================================
 Package                                        Arch                                Version
Repository                                Size
================================================================================================================
================================================================
Installing:
 openldap-clients                               i686                                2.4.23-34.el6_5.1
updates                                   160 k
 openldap-servers                               i686                                2.4.23-34.el6_5.1
updates                                   2.0 M
Updating:
 openldap                                       i686                                2.4.23-34.el6_5.1
updates                                   267 k
Updating for dependencies:
 openssl                                        i686                                1.0.1e-16.el6_5.7
updates                                   1.5 M

Transaction Summary
================================================================================================================
================================================================
Install       2 Package(s)
Upgrade       2 Package(s)

Total download size: 3.9 M
Is this ok [y/N]: y
```

Configuration de Démarrage du serveur LDAP

Sous RHEL / CentOS le service OpenLDAP s'appelle **slapd**. Une vérification de son état démontre qi'il n'est démarré dans aucun niveau d'exécution :

```
[root@centos6 ~]# chkconfig --list slapd
slapd           0:arrêt    1:arrêt    2:arrêt    3:arrêt    4:arrêt    5:arrêt    6:arrêt
```

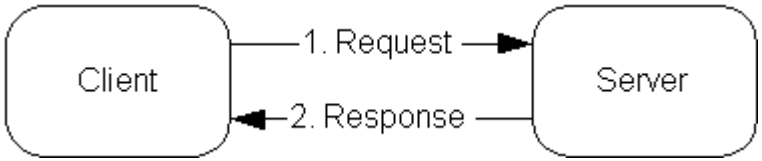
Il convient donc d'activer le service :

```
[root@centos6 ~]# chkconfig slapd on
[root@centos6 ~]# chkconfig --list slapd
slapd           0:arrêt    1:arrêt    2:marche    3:marche    4:marche    5:marche    6:arrêt
```

Configuration du serveur LDAP

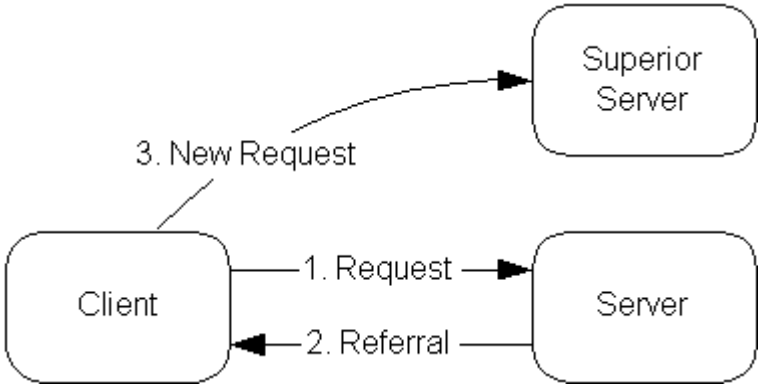
Le choix de la configuration de l'annuaire se fait en fonction de l'organisation de l'entité dont il détient l'information. Plusieurs configurations sont possible.

L'annuaire Local



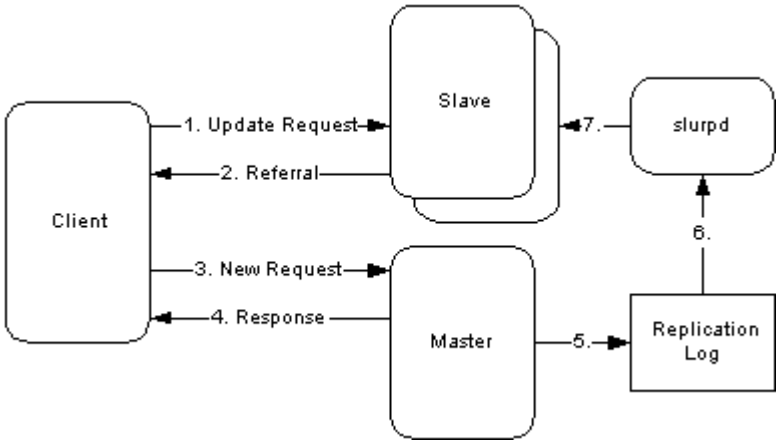
Dans ce cas, le service d'annuaire ne concerne que le domaine local. Il n'y a aucune interaction avec d'autres annuaires.

L''annuaire Local avec des Referrals



Dans ce cas, le service d'annuaire concerne le domaine local. Toute requête concernant quelquechose en dehors du domaine local est retournée au client en lui indiquant un service d'annuaire supérieur où il faut que le client s'adresse.

L'annuaire local avec réplication



Dans ce cas, le service d'annuaire concerne le domaine local. Il existe un annuaire **maître** et un annuaire **esclave**. Le démon **slurpd** effectue les mise à jour de l’esclave.

Fichier(s) de Configuration

Le Fichier slapd.conf

Antérieure à la version 2.3 d'OpenLDAP, la configuration d'OpenLDAP était effectuée en éditant le fichier **/etc/openldap/slapd.conf**. Un exemple de ce fichier est fourni dans le répertoire **/usr/share/openldap-servers/** :

```
[root@centos6 ~]# cat /usr/share/openldap-servers/slapd.conf.obsolete
#
# See slapd.conf(5) for details on configuration options.
# This file should NOT be world readable.
#

include     /etc/openldap/schema/corba.schema
include     /etc/openldap/schema/core.schema
include     /etc/openldap/schema/cosine.schema
include     /etc/openldap/schema/duaconf.schema
include     /etc/openldap/schema/dyngroup.schema
include     /etc/openldap/schema/inetorgperson.schema
include     /etc/openldap/schema/java.schema
include     /etc/openldap/schema/misc.schema
include     /etc/openldap/schema/nis.schema
include     /etc/openldap/schema/openldap.schema
include     /etc/openldap/schema/ppolicy.schema
include     /etc/openldap/schema/collective.schema

# Allow LDAPv2 client connections.  This is NOT the default.
allow bind_v2

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

```
pidfile     /var/run/openldap/slapd.pid
argsfile    /var/run/openldap/slapd.args

# Load dynamic backend modules
# - modulepath is architecture dependent value (32/64-bit system)
# - back_sql.la overlay requires openldap-server-sql package
# - dyngroup.la and dynlist.la cannot be used at the same time

# modulepath /usr/lib/openldap
# modulepath /usr/lib64/openldap

# moduleload accesslog.la
# moduleload auditlog.la
# moduleload back_sql.la
# moduleload chain.la
# moduleload collect.la
# moduleload constraint.la
# moduleload dds.la
# moduleload deref.la
# moduleload dyngroup.la
# moduleload dynlist.la
# moduleload memberof.la
# moduleload pbind.la
# moduleload pcache.la
# moduleload ppolicy.la
# moduleload refint.la
# moduleload retcode.la
# moduleload rwm.la
# moduleload seqmod.la
# moduleload smbk5pwd.la
# moduleload sssvlv.la
# moduleload syncprov.la
# moduleload translucent.la
# moduleload unique.la
```

```
# moduleload valsort.la

# The next three lines allow use of TLS for encrypting connections using a
# dummy test certificate which you can generate by running
# /usr/libexec/openldap/generate-server-cert.sh. Your client software may balk
# at self-signed certificates, however.
TLSCACertificatePath /etc/openldap/certs
TLSCertificateFile "\"OpenLDAP Server\""
TLSCertificateKeyFile /etc/openldap/certs/password

# 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!

# enable on-the-fly configuration (cn=config)
database config
access to *
    by dn.exact="gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth" manage
    by * none

# enable server status monitoring (cn=monitor)
database monitor
access to *
    by dn.exact="gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth" read
        by dn.exact="cn=Manager,dc=my-domain,dc=com" read
        by * none

#######################################################################
# database definitions
#######################################################################

database    bdb
suffix      "dc=my-domain,dc=com"
checkpoint  1024 15
rootdn      "cn=Manager,dc=my-domain,dc=com"
# Cleartext passwords, especially for the rootdn, should
# be avoided.  See slappasswd(8) and slapd.conf(5) for details.
# Use of strong authentication encouraged.
# rootpw        secret
# rootpw        {crypt}ijFYNcSNctBYg

# The database directory MUST exist prior to running slapd AND
# should only be accessible by the slapd and slap tools.
# Mode 700 recommended.
directory   /var/lib/ldap
```

```
# Indices to maintain for this database
index objectClass                       eq,pres
index ou,cn,mail,surname,givenname      eq,pres,sub
index uidNumber,gidNumber,loginShell    eq,pres
index uid,memberUid                     eq,pres,sub
index nisMapName,nisMapEntry            eq,pres,sub

# Replicas of this database
#replogfile /var/lib/ldap/openldap-master-replog
#replica host=ldap-1.example.com:389 starttls=critical
#     bindmethod=sasl saslmech=GSSAPI
#     authcId=host/ldap-master.example.com@EXAMPLE.COM
```

Les directives actives sont :

```
include     /etc/openldap/schema/corba.schema
include     /etc/openldap/schema/core.schema
include     /etc/openldap/schema/cosine.schema
include     /etc/openldap/schema/duaconf.schema
include     /etc/openldap/schema/dyngroup.schema
include     /etc/openldap/schema/inetorgperson.schema
include     /etc/openldap/schema/java.schema
include     /etc/openldap/schema/misc.schema
include     /etc/openldap/schema/nis.schema
include     /etc/openldap/schema/openldap.schema
include     /etc/openldap/schema/ppolicy.schema
include     /etc/openldap/schema/collective.schema
allow bind_v2
pidfile     /var/run/openldap/slapd.pid
argsfile    /var/run/openldap/slapd.args
TLSCACertificatePath /etc/openldap/certs
TLSCertificateFile "\"OpenLDAP Server\""
TLSCertificateKeyFile /etc/openldap/certs/password
database config
```

```
access to *
    by dn.exact="gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth" manage
    by * none
database monitor
access to *
    by dn.exact="gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth" read
        by dn.exact="cn=Manager,dc=my-domain,dc=com" read
        by * none
database    bdb
suffix      "dc=my-domain,dc=com"
checkpoint  1024 15
rootdn      "cn=Manager,dc=my-domain,dc=com"
directory   /var/lib/ldap
index objectClass                       eq,pres
index ou,cn,mail,surname,givenname      eq,pres,sub
index uidNumber,gidNumber,loginShell    eq,pres
index uid,memberUid                     eq,pres,sub
index nisMapName,nisMapEntry            eq,pres,sub
```

Les Directives du Fichier slapd.conf

include

Ces directives chargent les schémas :

```
include     /etc/openldap/schema/corba.schema
include     /etc/openldap/schema/core.schema
include     /etc/openldap/schema/cosine.schema
include     /etc/openldap/schema/duaconf.schema
include     /etc/openldap/schema/dyngroup.schema
include     /etc/openldap/schema/inetorgperson.schema
include     /etc/openldap/schema/java.schema
```

```
include     /etc/openldap/schema/misc.schema
include     /etc/openldap/schema/nis.schema
include     /etc/openldap/schema/openldap.schema
include     /etc/openldap/schema/ppolicy.schema
include     /etc/openldap/schema/collective.schema
```

allow

Cette directive permet l'utilisation du protocole LDAPv2 pour la connexion :

```
allow bind_v2
```

referral

Cette directive spécifie l'url de referral pour la base LDAP locale.

```
#referral       ldap://root.openldap.org
```

pidfile

Cette directive spécifie l'emplacement du fichier contenant le PID de slapd.

```
pidfile     /var/run/openldap/slapd.pid
```

argsfile

Cette directive contient la ligne de commande du lancement de slapd.

```
argsfile    /var/run/openldap/slapd.args
```

modulepath

Depuis la version 2.0 d'OpenLDAP, slapd peut être compilé pour utiliser des modules dynamiques, appelés **overlays** qui sont des bibliothèques partagés. Ces directives indiquent donc les endroits où sont stockés les modules dynamiques :

```
# modulepath /usr/lib/openldap
# modulepath /usr/lib64/openldap
```

```
[root@centos6 ~]# ls -l /usr/lib/openldap
total 688
lrwxrwxrwx. 1 root root    22 10 avril 15:18 accesslog-2.4.so.2 -> accesslog-2.4.so.2.5.6
-rwxr-xr-x. 1 root root 39264  3 févr. 20:09 accesslog-2.4.so.2.5.6
-rwxr-xr-x. 1 root root   939  3 févr. 20:08 accesslog.la
lrwxrwxrwx. 1 root root    21 10 avril 15:18 auditlog-2.4.so.2 -> auditlog-2.4.so.2.5.6
-rwxr-xr-x. 1 root root  9780  3 févr. 20:09 auditlog-2.4.so.2.5.6
-rwxr-xr-x. 1 root root   933  3 févr. 20:08 auditlog.la
lrwxrwxrwx. 1 root root    20 10 avril 15:18 collect-2.4.so.2 -> collect-2.4.so.2.5.6
-rwxr-xr-x. 1 root root  9812  3 févr. 20:09 collect-2.4.so.2.5.6
-rwxr-xr-x. 1 root root   927  3 févr. 20:08 collect.la
lrwxrwxrwx. 1 root root    23 10 avril 15:18 constraint-2.4.so.2 -> constraint-2.4.so.2.5.6
-rwxr-xr-x. 1 root root 22200  3 févr. 20:09 constraint-2.4.so.2.5.6
-rwxr-xr-x. 1 root root   945  3 févr. 20:08 constraint.la
lrwxrwxrwx. 1 root root    16 10 avril 15:18 dds-2.4.so.2 -> dds-2.4.so.2.5.6
-rwxr-xr-x. 1 root root 34816  3 févr. 20:09 dds-2.4.so.2.5.6
-rwxr-xr-x. 1 root root   903  3 févr. 20:08 dds.la
lrwxrwxrwx. 1 root root    18 10 avril 15:18 deref-2.4.so.2 -> deref-2.4.so.2.5.6
-rwxr-xr-x. 1 root root 13692  3 févr. 20:09 deref-2.4.so.2.5.6
-rwxr-xr-x. 1 root root   915  3 févr. 20:08 deref.la
lrwxrwxrwx. 1 root root    21 10 avril 15:18 dyngroup-2.4.so.2 -> dyngroup-2.4.so.2.5.6
-rwxr-xr-x. 1 root root  9748  3 févr. 20:09 dyngroup-2.4.so.2.5.6
```

```
-rwxr-xr-x. 1 root root   933  3 févr. 20:08 dyngroup.la
lrwxrwxrwx. 1 root root    20 10 avril 15:18 dynlist-2.4.so.2 -> dynlist-2.4.so.2.5.6
-rwxr-xr-x. 1 root root 26404  3 févr. 20:09 dynlist-2.4.so.2.5.6
-rwxr-xr-x. 1 root root   927  3 févr. 20:08 dynlist.la
lrwxrwxrwx. 1 root root    21 10 avril 15:18 memberof-2.4.so.2 -> memberof-2.4.so.2.5.6
-rwxr-xr-x. 1 root root 30612  3 févr. 20:09 memberof-2.4.so.2.5.6
-rwxr-xr-x. 1 root root   933  3 févr. 20:08 memberof.la
lrwxrwxrwx. 1 root root    19 10 avril 15:18 pcache-2.4.so.2 -> pcache-2.4.so.2.5.6
-rwxr-xr-x. 1 root root 72312  3 févr. 20:09 pcache-2.4.so.2.5.6
-rwxr-xr-x. 1 root root   921  3 févr. 20:08 pcache.la
lrwxrwxrwx. 1 root root    20 10 avril 15:18 ppolicy-2.4.so.2 -> ppolicy-2.4.so.2.5.6
-rwxr-xr-x. 1 root root 38764  3 févr. 20:09 ppolicy-2.4.so.2.5.6
-rwxr-xr-x. 1 root root   934  3 févr. 20:08 ppolicy.la
lrwxrwxrwx. 1 root root    19 10 avril 15:18 refint-2.4.so.2 -> refint-2.4.so.2.5.6
-rwxr-xr-x. 1 root root 18132  3 févr. 20:09 refint-2.4.so.2.5.6
-rwxr-xr-x. 1 root root   921  3 févr. 20:08 refint.la
lrwxrwxrwx. 1 root root    20 10 avril 15:18 retcode-2.4.so.2 -> retcode-2.4.so.2.5.6
-rwxr-xr-x. 1 root root 26444  3 févr. 20:09 retcode-2.4.so.2.5.6
-rwxr-xr-x. 1 root root   927  3 févr. 20:08 retcode.la
lrwxrwxrwx. 1 root root    16 10 avril 15:18 rwm-2.4.so.2 -> rwm-2.4.so.2.5.6
-rwxr-xr-x. 1 root root 59552  3 févr. 20:09 rwm-2.4.so.2.5.6
-rwxr-xr-x. 1 root root   903  3 févr. 20:08 rwm.la
lrwxrwxrwx. 1 root root    19 10 avril 15:18 seqmod-2.4.so.2 -> seqmod-2.4.so.2.5.6
-rwxr-xr-x. 1 root root  5456  3 févr. 20:09 seqmod-2.4.so.2.5.6
-rwxr-xr-x. 1 root root   921  3 févr. 20:08 seqmod.la
lrwxrwxrwx. 1 root root    21 10 avril 15:18 smbk5pwd-2.4.so.2 -> smbk5pwd-2.4.so.2.5.6
-rwxr-xr-x. 1 root root 14024  3 févr. 20:09 smbk5pwd-2.4.so.2.5.6
-rwxr-xr-x. 1 root root  1166  3 févr. 20:08 smbk5pwd.la
lrwxrwxrwx. 1 root root    19 10 avril 15:18 sssvlv-2.4.so.2 -> sssvlv-2.4.so.2.5.6
-rwxr-xr-x. 1 root root 22204  3 févr. 20:09 sssvlv-2.4.so.2.5.6
-rwxr-xr-x. 1 root root   921  3 févr. 20:08 sssvlv.la
lrwxrwxrwx. 1 root root    21 10 avril 15:18 syncprov-2.4.so.2 -> syncprov-2.4.so.2.5.6
-rwxr-xr-x. 1 root root 51148  3 févr. 20:09 syncprov-2.4.so.2.5.6
-rwxr-xr-x. 1 root root   933  3 févr. 20:08 syncprov.la
```

```
lrwxrwxrwx. 1 root root    24 10 avril 15:18 translucent-2.4.so.2 -> translucent-2.4.so.2.5.6
-rwxr-xr-x. 1 root root 26552  3 févr. 20:09 translucent-2.4.so.2.5.6
-rwxr-xr-x. 1 root root   951  3 févr. 20:08 translucent.la
lrwxrwxrwx. 1 root root    19 10 avril 15:18 unique-2.4.so.2 -> unique-2.4.so.2.5.6
-rwxr-xr-x. 1 root root 26388  3 févr. 20:09 unique-2.4.so.2.5.6
-rwxr-xr-x. 1 root root   921  3 févr. 20:08 unique.la
lrwxrwxrwx. 1 root root    20 10 avril 15:18 valsort-2.4.so.2 -> valsort-2.4.so.2.5.6
-rwxr-xr-x. 1 root root 14028  3 févr. 20:09 valsort-2.4.so.2.5.6
-rwxr-xr-x. 1 root root   927  3 févr. 20:08 valsort.la
```

moduleload

Ces directives chargent un module dynamique pour un **backend** spécifique.

```
# moduleload accesslog.la
# moduleload auditlog.la
# moduleload back_sql.la
# moduleload chain.la
# moduleload collect.la
# moduleload constraint.la
# moduleload dds.la
# moduleload deref.la
# moduleload dyngroup.la
# moduleload dynlist.la
# moduleload memberof.la
# moduleload pbind.la
# moduleload pcache.la
# moduleload ppolicy.la
# moduleload refint.la
# moduleload retcode.la
# moduleload rwm.la
# moduleload seqmod.la
# moduleload smbk5pwd.la
```

```
# moduleload sssvlv.la
# moduleload syncprov.la
# moduleload translucent.la
# moduleload unique.la
# moduleload valsort.la
```

TLSCACertificateFile, TLSCertificateFile & TLSCertificateKeyFile

Ces directives permettent l'utilisation de connexions crypées en utilisant TLS.

```
TLSCACertificatePath /etc/openldap/certs
TLSCertificateFile "\"OpenLDAP Server\""
TLSCertificateKeyFile /etc/openldap/certs/password
```

security

Le serveur utilise des **SSF** (Security Strength Factors) pour fixer le niveau de sécurité. Une valeur de SSF=0 indique qu'aucune protection n'est en place :

```
# security ssf=1 update_ssf=112 simple_bind=64
```

- ssf1 = La vérification de l'intégrité des données est requise,
- update_ssf = Un cryptage de 112 bit ou mieux (3DES ou mieux) est requis pour les opérations de mises-à-jour,
- simple_bind = Un cryptage de 64 bit est requis pour se connecter à l'annuaire en mode :
  - anonyme,
  - non-authentifié,
  - authentifié en utilisant un couple utilisateur/mot de passe.

access to

OpenLDAP utilise des ACL (**A**ccess **C**ontrol **L**ists) pour sécuriser l'accès aux données. Sans ACL définis, la valeur par défaut est :

```
access to * by * READ
```

> Le rootdn peut toujours tout lire et tout écrire.

Le format de cette ligne est :

```
access to OBJET by SUJET AUTORISATION CONTROLE
```

où :

- **OBJET** désigne une entrée ou un attribut
- **SUJET** désigne le(s) DN à qui la directive donne accès
- **AUTORISATION** définit l'autorisation donnée
- **CONTROLE** définit le comportement du serveur après l'accès.

L'exemple suivant :

```
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
```

indique donc :

- **access to dn.base=”“ by * read** - tout le monde peut lire le Root DSE (**R**oot **D**irectory **S**pecific **E**ntry),
- **access to dn.base=“cn=Subschema” by * read** - tout le monde peut lire le Subschema (sub)entry DSE,
- **access to** * - pour les autres DSE :

- **Allow self write access** - l'utilisateur concerné par l'entrée peut le modifier,
- **Allow authenticated users read access** - tout utilisateur authentifié peut lire les entrées,
- **Allow anonymous users to authenticate** - les utilisateurs anonymes peuvent se connecter.

Pour plus d'information concernant les ACL, consultez **cette page**.

database config

Cette directive permet l'utilisation de cn=config :

```
# enable on-the-fly configuration (cn=config)
database config
access to *
    by dn.exact="gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth" manage
    by * none
```

backend

Cette directive stipule le type de **backend** autrement dit le moteur de base de données :

Moteur	Description
bdb	Base de données transactionnelle Berkeley
hdb	Base de données transactionnelle Berkeley hiérarchisée
ldbm	Base de données avec des fichiers au format dbm ou gdbm
dnssrv	Intérrogation d'un serveur DNS en utilisant les champs SRV des enrigistrements DNS
ldap	Transmission des reqûetes en tant que proxy vers un autre serveur LDAP
meta	Transmission des reqûetes en tant que proxy avec méchanisme de ré-écriture des noms des objets
monitor	Pseudo backend pour accéder aux informations du serveur

Moteur	Description
passwd	Base de données transactionnelle Berkeley
perl	Transmission des commandes LDAP vers un interpréteur perl
shell	Transmission des commandes LDAP vers un interpréteur shell
sql	Utilisation d'une base de données

suffix DN

Cette directive indique le noeud que la base de données va gérer :

```
suffix          "dc=domain,dc=com"
```

checkpoint

Cette directive indique la fréquence, en KO et en minutes, des checkpoints. Un checkpoint déclenche l'écriture des données dans les buffers vers le disque et l'insertion d'un enregistrement de type checkpoint dans le fichier de journalisation BDB. Les checkpoints font partie intégrale du fonctionnement des bases de données au format BDB et HDB. Pour plus d'informations voir **man slapd-bdb** :

```
checkpoint  1024 15
```

rootdn <DN>

Cette directive identifie l'utilisateur dont les accès ne seront pas soumis aux clauses d'accès :

```
rootdn      "cn=Manager,dc=my-domain,dc=com"
```

rootpw <mot de passe>

Cette directive indique le mot de passe de l'utilisateur rootdn :

```
# rootpw        {crypt}ijFYNcSNctBYg
```

directory

Cette directive indique l'emplacement des bases de données et les indexes :

```
directory       /var/lib/ldap
```

> Dans le cas d'une compilation des sources, la valeur par défaut est **/usr/local/var/open-ldap**.

index

Cette directive indique les index à créer et à maintenir pour la base de données.

Dans l'exemple qui suit les index :

- **égalité** et **présence** sont créés pour les attributs **objectClass**, **uidNumber**, **gidNumber** et **loginShell**,
- **égalité**, **présence** et **sous-chaîne** sont créés pour les attributs **ou**, **cn**, **mail**, **surname**, **givenname**, **uid**, **memberUid**, **nisMapName** et **nisMapEntry**.

```
index objectClass                       eq,pres
index ou,cn,mail,surname,givenname      eq,pres,sub
index uidNumber,gidNumber,loginShell    eq,pres
index uid,memberUid                     eq,pres,sub
index nisMapName,nisMapEntry            eq,pres,sub
```

La commande **slapindex** crée et met à jour les index spécifiés dans le fichier slapd.conf.

replogfile <filename>

Cette directive indique le nom et l'emplacement du fichier de journalisation de la replication.

```
#replogfile /var/lib/ldap/openldap-master-replog
```

replica host <hostname>[:<port>] [bindmethod={ simple | kerberos | sasl }]

Cette directive détaille l'esclave pour la replication.

```
#replica host=ldap-1.example.com:389 starttls=critical
#     bindmethod=sasl saslmech=GSSAPI
#     authcId=host/ldap-master.example.com@EXAMPLE.COM
```

Autres Directives Utiles

loglevel

Cette directive stipule le niveau de verbosité des journaux selon les valeurs dans le tableau suivant :

Niveau	Mot clé	Description
-1	Any	Affichage de toutes les informations
0		Aucune information
1	Trace	Liste des appels de fonctions
2	Packets	Affichange du traitement des paquets
4	Args	Affichage détaillé des appels de fonctions
8	Conns	Affichage des connexions
16	BER	Affichage des paquets reçus et émis
32	Filter	Affichage du traitement d'un filtre

Niveau	Mot clé	Description
64	Config	Affichage du traitement du fichier de configuration
128	ACL	Affichage du traitement des permissions de chaque opération
256	Stats	Affichage du résultat des opérations
512	Stats2	Affichage des statistiques
1024	Shell	Affichage des communications avec des backends de type shell
2048	Parse	Affichage du traitement des entrées
4096	Cache	Affichage des opérations de gestion du cache des bases de données
8192	Index	Affichage des opérations d'indexation des bases de données
16384	Sync	Affichage des opérations syncrepl

Pour activer à la fois la journalisation du traitement des permissions et des connexions, la directive peut être écrite de deux façons différentes : **loglevel 128 1** ou **loglevel 129**.

password-hash

Cette directive spécifie le type de cryptage utilisé par la commande **ldappassword** :

- {SSHA} (**Salted** **S**ecure **H**ash **A**lgorithm - une amélioration de SHA)
- {SHA}
- {SMD5}
- {MD5},
- {CRYPT}

La valeur pas défaut est **{SSHA}**.

schemacheck

Cette directive permet de stipuler si oui ou non le serveur vérifie le respect du schéma lors d'une modification de l'annuaire.

La valeur pas défaut est **on**.

idletimeout

Cette directive spécifie le nombre de secondes à attendre avant de fermer la connexion d'un client inactif.

La valeur par défaut est **0** qui désactive cette option.

sizelimit

Cette directive indique le nombre maximal d'entrées à retourner lors d'une requête.

La valeur par défaut est **500**.

timelimit

Cette directive indique le nombre de seconds maximum alloué par le serveur à chaque requête de recherche. Une valeur d'**unlimited** désactive cette option.

La valeur par défaut est **3600**.

readonly <on | off>

Cette directive met la base en lecture seule.

La valeur par défaut est **off**.

lastmod <on | off>

Cette directive définit si les attributs opérationnels tels modifiersName et modifyTimestamp des entrées seront stockés ou pas.

La valeur par défaut est **on**.

Le Fichier /etc/openldap/ldap.conf

Nous avons déjà établi que le fichier de configuration de slapd est /etc/openldap/slapd.conf.

Il existe aussi un autre fichier de configuration : **/etc/openldap/ldap.conf**.

Le fichier de configuration ldap.conf est utilisé pour configurer les commandes clients. Il est aussi possible de mettre en place des configurations spécifiques à un utilisateur en créant un fichier **.ldaprc** dans son répertoire de connexion, voire de créer un fichier de configuration **ldaprc** propre à un utilisateur et le placer dans le répertoire courant.

cn=config

Depuis la version 2.3 d'OpenLDAP, les fichiers de configuration sont stockés dans le répertoire **/usr/local/etc/openldap/slapd.d** (dans le cas d'une installation depuis des sources) ou **/etc/openldap/slapd.d** (dans le cas d'une installation à partir des dépôts).

> Pour pouvoir utiliser le fichier **slapd.conf**, il convient de le copier dans le répertoire **/usr/local/etc/openldap** ou **/etc/openldap/slapd.d** puis de **supprimer** le répertoire **/usr/local/etc/openldap/slapd.d** ou **/etc/openldap/slapd.d**.

La configuration est stockée dans un annuaire spécifique, dont la structure de base est :

Ce qui se traduit par l'arborescence suivante :

```
/etc/openldap/slapd.d
/etc/openldap/slapd.d/cn=config
/etc/openldap/slapd.d/cn=config.ldif
/etc/openldap/slapd.d/cn=config/cn=schema
/etc/openldap/slapd.d/cn=config/cn=schema.ldif
/etc/openldap/slapd.d/cn=config/olcDatabase={-1}frontend.ldif
/etc/openldap/slapd.d/cn=config/olcDatabase={0}config.ldif
/etc/openldap/slapd.d/cn=config/olcDatabase={1}monitor.ldif
/etc/openldap/slapd.d/cn=config/olcDatabase={2}bdb.ldif
/etc/openldap/slapd.d/cn=config/cn=schema/cn={0}corba.ldif
/etc/openldap/slapd.d/cn=config/cn=schema/cn={10}ppolicy.ldif
/etc/openldap/slapd.d/cn=config/cn=schema/cn={11}collective.ldif
/etc/openldap/slapd.d/cn=config/cn=schema/cn={1}core.ldif
/etc/openldap/slapd.d/cn=config/cn=schema/cn={2}cosine.ldif
/etc/openldap/slapd.d/cn=config/cn=schema/cn={3}duaconf.ldif
/etc/openldap/slapd.d/cn=config/cn=schema/cn={4}dyngroup.ldif
/etc/openldap/slapd.d/cn=config/cn=schema/cn={5}inetorgperson.ldif
```

```
/etc/openldap/slapd.d/cn=config/cn=schema/cn={6}java.ldif
/etc/openldap/slapd.d/cn=config/cn=schema/cn={7}misc.ldif
/etc/openldap/slapd.d/cn=config/cn=schema/cn={8}nis.ldif
/etc/openldap/slapd.d/cn=config/cn=schema/cn={9}openldap.ldif
```

Les numéros {X} indiquent l'ordre dans lequel slapd va traiter les fichiers.

Les attributs de cette nouvelle configuration ont une correspondance avec les directives du fichier slapd.conf :

Directive slapd.conf	**Attribut cn=config**
access to	olcAccess
allow	olcAllows
argsfile	olcArgsFile
attributetype	olcAttributeTypes
concurrency	olcConcurrency
conn_max_pending	olcConnMaxPending
conn_max_auth	olcConnMaxPendingAuth
defaultaccess	Non supporté
defaultsearchbase	olcDefaultSearchBase
disallow	olcDisallows
gentlehup	olcGentleHUP
idletimeout	olcIdleTimeout
include	Non supporté
index	olcDbIndex
logfile	olcLogFile
loglevel	olcLogLevel
moduleload	olcModuleLoad
modulepath	olcModulePath
objectclass	olcObjectClasses

Directive slapd.conf	Attribut cn=config
password-hash	olcPasswordHash
pidfile	olcPidFile
referral	olcReferral
replicationinterval	Non supporté
require	olcRequires
reverse-lookup	olcReverseLookup
rootDSE	olcRootDSE
schemadn	olcSchemaDN
security	olcSecurity
ServerID	olcServerID
sizelimit	olcSizeLimit
sockbuf_max_incoming	olcSockBufMaxIncoming
sockbuf_max_incoming_auth	olcSockBufMaxIncomingAuth
threads	olcThreads
timelimit	olcTimeLimit
TLSCACertificateFile	olcTLSCACertificateFile
TLSCertificateFile	olcTLSCertificateFile
TLSCertificateKeyFile	olcTLSCertificateKeyFile
TLSCipherSuite	olcTLSCipherSuite
TLSRandFile	olcTLSRandFile
TLSEphemeralDHParamFile	olcTLSDHParamFile
TLSVerifyClient	olcTLSVerifyClient
backend	olcBackend
access to	olcAccess
database	olcDatabase
index	olcDbIndex
mirrormode	olcMirrorMode
overlay	olcOverlay
readonly	olcReadOnly
replica	olcReplica

Directive slapd.conf	Attribut cn=config
replogfile	olcReplogFile
require	olcRequires
rootdn	olcRootDN
rootpw	olcRootPW
suffix	olcSuffix
syncrepl	olcSyncrepl
updatedn	olcUpdateDN
updateref	olcUpdateref

Sécuriser l'Annuaire

Créer le Mot de Passe de l'Administrateur

La première tâche à accomplir est de générer un mot de passe pour l'administrateur d'OpenLDAP :

```
[root@centos6 ~]# slappasswd
New password:
Re-enter new password:
{SSHA}/0IpH1CvbXjX0HBLjwjzKfYyhtwCX524
```

La commande slappasswd prend les options suivantes :

```
Usage: slappasswd [options]
  -h hash       password scheme
  -s secret     new password
  -c format     crypt(3) salt format
  -u            generate RFC2307 values (default)
  -v            increase verbosity
  -T file       read file for new password
```

Il convient ensuite de modifier le fichier **/etc/openldap/slapd.d/cn\=config/olcDatabase\=\{2\}bdb.ldif** en y ajoutant la ligne **olcRootPW:**

{SSHA}/0IpH1CvbXjX0HBLjwjzKfYyhtwCX524 :

```
dn: olcDatabase={2}bdb
objectClass: olcDatabaseConfig
objectClass: olcBdbConfig
olcDatabase: {2}bdb
olcSuffix: dc=my-domain,dc=com
olcAddContentAcl: FALSE
olcLastMod: TRUE
olcMaxDerefDepth: 15
olcReadOnly: FALSE
olcRootDN: cn=Manager,dc=my-domain,dc=com
olcRootPW: {SSHA}/0IpH1CvbXjX0HBLjwjzKfYyhtwCX524
olcSyncUseSubentry: FALSE
olcMonitoring: TRUE
olcDbDirectory: /var/lib/ldap
olcDbCacheSize: 1000
olcDbCheckpoint: 1024 15
olcDbNoSync: FALSE
olcDbDirtyRead: FALSE
olcDbIDLcacheSize: 0
olcDbIndex: objectClass pres,eq
olcDbIndex: cn pres,eq,sub
olcDbIndex: uid pres,eq,sub
olcDbIndex: uidNumber pres,eq
olcDbIndex: gidNumber pres,eq
olcDbIndex: ou pres,eq,sub
olcDbIndex: loginShell pres,eq
olcDbIndex: mail pres,eq,sub
olcDbIndex: sn pres,eq,sub
olcDbIndex: givenName pres,eq,sub
olcDbIndex: memberUid pres,eq,sub
olcDbIndex: nisMapName pres,eq,sub
olcDbIndex: nisMapEntry pres,eq,sub
```

```
olcDbLinearIndex: FALSE
olcDbMode: 0600
olcDbSearchStack: 16
olcDbShmKey: 0
olcDbCacheFree: 1
olcDbDNcacheSize: 0
structuralObjectClass: olcBdbConfig
entryUUID: 4dddce5c-54fe-1033-8153-dbe2595ccd66
creatorsName: cn=config
createTimestamp: 20140410131809Z
entryCSN: 20140410131809.201468Z#000000#000#000000
modifiersName: cn=config
modifyTimestamp: 20140410131809Z
```

Les directives **olcSuffix: dc=my-domain,dc=com** et **olcRootDN: cn=Manager,dc=my-domain,dc=com** doivent être modifiées pour votre système ainsi :

```
...
olcSuffix: dc=fenestros,dc=com
olcRootDN: cn=Manager,dc=fenestros,dc=com
...
```

La directive **olcSuffix** indique la racine de l'arbre qui est détenu dans la base de données. La directive **olcRootDN** indique les coordonnées de connexion de l'administrateur de cet arbre. N'utilisez pas cn=**root**.

Sécuriser avec SSL

Ajoutez les deux directives suivantes pour les connexions **ssl** au fichier **/etc/openldap/slapd.d/cn\=config/olcDatabase\=\{2\}bdb.ldif**:

```
...
```

```
olcTLSCertificateFile: /etc/pki/tls/certs/ldapcert.pem
olcTLSCertificateKeyFile: /etc/pki/tls/certs/ldapkey.pem
```

Votre fichier devient donc :

bdb.ldif

```
dn: olcDatabase={2}bdb
objectClass: olcDatabaseConfig
objectClass: olcBdbConfig
olcDatabase: {2}bdb
olcSuffix: dc=fenestros,dc=com
olcAddContentAcl: FALSE
olcLastMod: TRUE
olcMaxDerefDepth: 15
olcReadOnly: FALSE
olcRootDN: cn=Manager,dc=fenestros,dc=com
olcRootPW: {SSHA}IlHgBODYC3npHKLPGounjqTtLgxRJEmU
olcSyncUseSubentry: FALSE
olcMonitoring: TRUE
olcDbDirectory: /var/lib/ldap
olcDbCacheSize: 1000
olcDbCheckpoint: 1024 15
olcDbNoSync: FALSE
olcDbDirtyRead: FALSE
olcDbIDLcacheSize: 0
olcDbIndex: objectClass pres,eq
olcDbIndex: cn pres,eq,sub
olcDbIndex: uid pres,eq,sub
olcDbIndex: uidNumber pres,eq
olcDbIndex: gidNumber pres,eq
olcDbIndex: ou pres,eq,sub
olcDbIndex: loginShell pres,eq
olcDbIndex: mail pres,eq,sub
```

```
olcDbIndex: sn pres,eq,sub
olcDbIndex: givenName pres,eq,sub
olcDbIndex: memberUid pres,eq,sub
olcDbIndex: nisMapName pres,eq,sub
olcDbIndex: nisMapEntry pres,eq,sub
olcDbLinearIndex: FALSE
olcDbMode: 0600
olcDbSearchStack: 16
olcDbShmKey: 0
olcDbCacheFree: 1
olcDbDNcacheSize: 0
structuralObjectClass: olcBdbConfig
entryUUID: d34566ca-44d6-1031-9e81-6756bfd20624
creatorsName: cn=config
createTimestamp: 20120607102519Z
entryCSN: 20120607102519.200524Z#000000#000#000000
modifiersName: cn=config
modifyTimestamp: 20120607102519Z
olcTLSCertificateFile: /etc/pki/tls/certs/ldapcert.pem
olcTLSCertificateKeyFile: /etc/pki/tls/certs/ldapkey.pem
```

Activez ssl dans le fichier **/etc/sysconfig/ldap** en modifiant la directive **SLAPD_LDAPS** :

/etc/sysconfig/ldap

```
# Options of slapd (see man slapd)
#SLAPD_OPTIONS=

# At least one of SLAPD_LDAP, SLAPD_LDAPI and SLAPD_LDAPS must be set to 'yes'!
#
# Run slapd with -h "... ldap:/// ..."
#   yes/no, default: yes
SLAPD_LDAP=yes
```

```
# Run slapd with -h "... ldapi:/// ..."
#   yes/no, default: yes
SLAPD_LDAPI=yes

# Run slapd with -h "... ldaps:/// ..."
#   yes/no, default: no
SLAPD_LDAPS=yes

# Run slapd with -h "... $SLAPD_URLS ..."
# This option could be used instead of previous three ones, but:
# - it doesn't overwrite settings of $SLAPD_LDAP, $SLAPD_LDAPS and $SLAPD_LDAPI options
# - it isn't overwritten by settings of $SLAPD_LDAP, $SLAPD_LDAPS and $SLAPD_LDAPI options
# example: SLAPD_URLS="ldapi:///var/lib/ldap_root/ldapi ldapi:/// ldaps:///"
# default: empty
#SLAPD_URLS=""

# Maximum allowed time to wait for slapd shutdown on 'service ldap stop' (in seconds)
#SLAPD_SHUTDOWN_TIMEOUT=3

# Parameters to ulimit, use to change system limits for slapd
#SLAPD_ULIMIT_SETTINGS=""
```

Générez ensuite votre certificat :

```
[root@centos6 ~]# openssl req -new -x509 -nodes -out /etc/pki/tls/certs/ldapcert.pem -keyout
/etc/pki/tls/certs/ldapkey.pem -days 365
Generating a 2048 bit RSA private key
.......+++
.....................................................................................+++
writing new private key to '/etc/pki/tls/certs/ldapkey.pem'
-----
You are about to be asked to enter information that will be incorporated
```

```
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:FR
State or Province Name (full name) []:VAR
Locality Name (eg, city) [Default City]:Toulon
Organization Name (eg, company) [Default Company Ltd]:Linux E-Learning
Organizational Unit Name (eg, section) []:Formation
Common Name (eg, your name or your server's hostname) []:centos.fenestros.com
Email Address []:root@localhost
```

Modifiez le groupe et les permissions :

```
[root@centos6 ~]# chown -Rf root:ldap /etc/pki/tls/certs/ldapcert.pem
[root@centos6 ~]# chmod -Rf 750 /etc/pki/tls/certs/ldapkey.pem
```

La présence du fichier **DB_CONFIG** est primordiale pour le bon fonctionnement d'OpenLDAP.

Un exemple de fichier se trouve dans le répertoire **/usr/share/openldap-servers/** :

```
[root@centos6 ~]# ls -l /usr/share/openldap-servers/DB*
-rw-r--r--. 1 root root 921  7 déc.   2011 /usr/share/openldap-servers/DB_CONFIG.example
```

Le fichier de configuration DB_CONFIG permet aux administrateurs de personnaliser l'environnement de la base de données indépendamment des applications qui l'utilise. Par exemple l'administrateur pourrait déplacer l'emplacement des bases de données et les fichiers de journalisation sans avoir à recompiler les applications qui les utilisent. Le fichier DB_CONFIG est lu au moment du chargement de l'environnement de la base de données. Ceci implique que les valeurs dans ce fichier surchargent celles dans les fichiers de configuration.

DB_CONFIG.example

```
# $OpenLDAP: pkg/ldap/servers/slapd/DB_CONFIG,v 1.3.2.4 2007/12/18 11:53:27 ghenry Exp $
```

```
# Example DB_CONFIG file for use with slapd(8) BDB/HDB databases.
#
# See the Oracle Berkeley DB documentation
#   <http://www.oracle.com/technology/documentation/berkeley-db/db/ref/env/db_config.html>
# for detail description of DB_CONFIG syntax and semantics.
#
# Hints can also be found in the OpenLDAP Software FAQ
#   <http://www.openldap.org/faq/index.cgi?file=2>
# in particular:
#   <http://www.openldap.org/faq/index.cgi?file=1075>

# Note: most DB_CONFIG settings will take effect only upon rebuilding
# the DB environment.

# one 0.25 GB cache
set_cachesize 0 268435456 1

# Data Directory
#set_data_dir db

# Transaction Log settings
set_lg_regionmax 262144
set_lg_bsize 2097152
#set_lg_dir logs

# Note: special DB_CONFIG flags are no longer needed for "quick"
# slapadd(8) or slapindex(8) access (see their -q option).
```

Il convient donc de copier ce fichier vers **/var/lib/ldap/DB_CONFIG** :

```
[root@centos6 ~]# cp /usr/share/openldap-servers/DB_CONFIG.example /var/lib/ldap/DB_CONFIG
```

Puis de modifier le propriétaire et le groupe :

```
[root@centos6 ~]# chown -R ldap:ldap /var/lib/ldap/
```

A titre d'exemple d'une modification du fichier DB_CONFIG, ajoutons une directive qui permettra de nettoyer automatiquement les fichiers logs **set_flags DB_LOG_AUTOREMOVE** :

```
...
# Note: most DB_CONFIG settings will take effect only upon rebuilding
# the DB environment.

set_flags DB_LOG_AUTOREMOVE

# one 0.25 GB cache
set_cachesize 0 268435456 1
...
```

Les directives admises du fichier DB_CONFIG peuvent être consultées dans **la documentation de Berkeley-db**

Éditez maintenant le fichier **/etc/openldap/slapd.d/cn\=config/olcDatabase\={1}monitor.ldif** et modifiez la directive **olcAccess** :

```
dn: olcDatabase={1}monitor
objectClass: olcDatabaseConfig
olcDatabase: {1}monitor
olcAccess: {0}to *  by dn.base="gidNumber=0+uidNumber=0,cn=peercred,cn=externa
 l,cn=auth" read  by dn.base="cn=Manager,dc=fenestros,dc=com" read  by * none
olcAddContentAcl: FALSE
olcLastMod: TRUE
olcMaxDerefDepth: 15
olcReadOnly: FALSE
olcSyncUseSubentry: FALSE
olcMonitoring: FALSE
structuralObjectClass: olcDatabaseConfig
```

```
entryUUID: d34561de-44d6-1031-9e80-6756bfd20624
creatorsName: cn=config
createTimestamp: 20120607102519Z
entryCSN: 20120607102519.200524Z#000000#000#000000
modifiersName: cn=config
modifyTimestamp: 20120607102519Z
```

Vous pouvez maintenant tester votre configuration :

```
[root@centos6 ~]# slaptest -u
config file testing succeeded
```

Ensuite vous pouvez démarrer le serveur slapd :

```
[root@centos6 ~]# service slapd start
Démarrage de slapd :                                       [  OK  ]
```

Constatez le processus en cours :

```
[root@centos6 ~]# ps aux | grep slapd
ldap      2546  0.0  0.3  24176  4016 ?        Ssl  19:07   0:00 /usr/sbin/slapd -h  ldap:/// ldaps:/// ldapi:///
-u ldap
root      2552  0.0  0.0   4376   800 pts/0    S+   19:07   0:00 grep slapd
```

On note la présence d'arguments. Ceux-ci sont détaillés dans le fichier **/var/run/openldap/slapd.args** :

```
[root@centos6 ~]# cat /var/run/openldap/slapd.args
/usr/sbin/slapd -h  ldap:/// ldaps:/// ldapi:/// -u ldap
```

Options de la ligne de commande de slapd

La commande slapd peut prendre plusieurs options :

```
[root@centos6 ~]# slapd --help
slapd: invalid option -- '-'
usage: slapd options
    -4        IPv4 only
    -6        IPv6 only
    -T {acl|add|auth|cat|dn|index|passwd|test}
            Run in Tool mode
    -c cookie    Sync cookie of consumer
    -d level    Debug level
    -f filename    Configuration file
    -F dir    Configuration directory
    -g group    Group (id or name) to run as
    -h URLs        List of URLs to serve
    -l facility    Syslog facility (default: LOCAL4)
    -n serverName    Service name
    -o <opt>[=val] generic means to specify options; supported options:
        slp[={on|off|(attrs)}] enable/disable SLP using (attrs)
    -r directory    Sandbox directory to chroot to
    -s level    Syslog level
    -u user        User (id or name) to run as
    -V        print version info (-VV only)
```

Création et maintenance de la base de données

Le format LDIF

Les fichiers au format LDIF (**LD**AP **I**nterchange **F**ormat) sont utilisés lors de modifications de masse sur une base LDAP. Les fichiers LDIF sont traités dans un ordre séquentielle.

Le fichier LDIF est un fichier texte qui peut comprendre :

- des descriptions d'entrées de l'annuaire,

- des valeurs d'attribut pour les entrées de l'annuaire,
- des instructions de traitements pour le serveur.

Un fichier LDIF commence avec un **numéro de version** et peut comporter des commentaires à l'aide du caractère **#**. Chaque enregistrement doit être séparé du précédent par une ligne blanche et il ne peut pas avoir deux lignes blanches consécutives.

Les attributs peuvent être sur plusieurs lignes. Dans ce cas les lignes supplémentaires commencent par un blanc.

Un fichier LDIF pour créer l'arbre de l'annuaire ressemble à cet exemple :

```
version: 1
dn: ou=France,dc=fenestros,dc=com
objectClass: organizationalUnit
objectClass: top
ou: France

dn: ou=Commercial,ou=France,dc=fenestros,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Commercial

dn: ou=Recherche,ou=France,dc=fenestros,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Recherche

dn: ou=Production,ou=France,dc=fenestros,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Production

dn: ou=Suisse,dc=fenestros,dc=com
objectClass: organizationalUnit
objectClass: top
```

```
ou: Suisse

dn: ou=Commercial,ou=Suisse,dc=fenestros,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Commercial

dn: ou=USA,dc=fenestros,dc=com
objectClass: organizationalUnit
objectClass: top
ou: USA

dn: ou=Commercial,ou=USA,dc=fenestros,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Commercial

dn: ou=Recherche,ou=USA,dc=fenestros,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Recherche
```

Création d’une base de données en ligne

La commande ldapadd

Afin de pouvoir utiliser notre fichier LDIF, il est nécessaire de faire appel au client **ldapadd**. Cet utilitaire prend un ou plusieurs options :

```
[root@centos6 tmp]# ldapadd --help
ldapadd: invalid option -- '-'
ldapadd: unrecognized option --
Add or modify entries from an LDAP server
```

```
usage: ldapadd [options]
    The list of desired operations are read from stdin or from the file
    specified by "-f file".
Add or modify options:
  -a         add values (default)
  -c         continuous operation mode (do not stop on errors)
  -E [!]ext=extparam    modify extensions (! indicate s criticality)
  -f file    read operations from `file'
  -M         enable Manage DSA IT control (-MM to make critical)
  -P version protocol version (default: 3)
  -S file    write skipped modifications to `file'
Common options:
  -d level   set LDAP debugging level to `level'
  -D binddn  bind DN
  -e [!]<ext>[=<extparam>] general extensions (! indicates criticality)
             [!]assert=<filter>     (RFC 4528; a RFC 4515 Filter string)
             [!]authzid=<authzid>   (RFC 4370; "dn:<dn>" or "u:<user>")
             [!]chaining[=<resolveBehavior>[/<continuationBehavior>]]
                    one of "chainingPreferred", "chainingRequired",
                    "referralsPreferred", "referralsRequired"
             [!]manageDSAit         (RFC 3296)
             [!]noop
             ppolicy
             [!]postread[=<attrs>]  (RFC 4527; comma-separated attr list)
             [!]preread[=<attrs>]   (RFC 4527; comma-separated attr list)
             [!]relax
             abandon, cancel, ignore (SIGINT sends abandon/cancel,
             or ignores response; if critical, doesn't wait for SIGINT.
             not really controls)
  -h host    LDAP server
  -H URI     LDAP Uniform Resource Identifier(s)
  -I         use SASL Interactive mode
  -n         show what would be done but don't actually do it
  -N         do not use reverse DNS to canonicalize SASL host name
```

```
  -O props   SASL security properties
  -o <opt>[=<optparam] general options
             nettimeout=<timeout> (in seconds, or "none" or "max")
  -p port    port on LDAP server
  -Q         use SASL Quiet mode
  -R realm   SASL realm
  -U authcid SASL authentication identity
  -v         run in verbose mode (diagnostics to standard output)
  -V         print version info (-VV only)
  -w passwd  bind password (for simple authentication)
  -W         prompt for bind password
  -x         Simple authentication
  -X authzid SASL authorization identity ("dn:<dn>" or "u:<user>")
  -y file    Read password from file
  -Y mech    SASL mechanism
  -Z         Start TLS request (-ZZ to require successful response)
```

Créons maintenant notre fichier LDIF dans le répertoire /tmp :

```
[root@centos6 ~]# cd /tmp; vi setup.ldif
```

Editez ensuite **setup.ldif** de la façon suivante :

setup.ldif

```
# Organisation fenestros
dn: dc=fenestros,dc=com
objectClass: dcObject
objectClass: organization
dc: fenestros
o: fenestros.com
description: Exemple

# Gestionnaire de l'arbre
```

```
dn: cn=Manager,dc=fenestros,dc=com
objectClass: organizationalRole
cn: Manager
description: Gestionnaire
```

Il convient maintenant d'utiliser la commande ldapadd afin d'injecter le contenu du fichier setup.ldif dans notre base :

```
[root@centos6 ~]# ldapadd -f /tmp/setup.ldif -x -D "cn=Manager,dc=fenestros,dc=com" -w fenestros
adding new entry "dc=fenestros,dc=com"

adding new entry "cn=Manager,dc=fenestros,dc=com"
```

Nous procédons maintenant de la même façon pour les autres données. Créez le fichier **/tmp/import.ldif** :

import.ldif

```
version: 1
dn: ou=France,dc=fenestros,dc=com
objectClass: organizationalUnit
objectClass: top
ou: France

dn: ou=Commercial,ou=France,dc=fenestros,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Commercial

dn: ou=Recherche,ou=France,dc=fenestros,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Recherche

dn: ou=Production,ou=France,dc=fenestros,dc=com
```

```
objectClass: organizationalUnit
objectClass: top
ou: Production

dn: ou=Suisse,dc=fenestros,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Suisse

dn: ou=Commercial,ou=Suisse,dc=fenestros,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Commercial

dn: ou=USA,dc=fenestros,dc=com
objectClass: organizationalUnit
objectClass: top
ou: USA

dn: ou=Commercial,ou=USA,dc=fenestros,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Commercial

dn: ou=Recherche,ou=USA,dc=fenestros,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Recherche
```

Il convient maintenant d'utiliser de nouveau la commande ldapadd afin d'injecter le contenu du fichier import.ldif dans notre base :

```
[root@centos6 ~]# ldapadd -f /tmp/import.ldif -x -D "cn=Manager,dc=fenestros,dc=com" -w fenestros
adding new entry "ou=France,dc=fenestros,dc=com"
```

```
adding new entry "ou=Commercial,ou=France,dc=fenestros,dc=com"

adding new entry "ou=Recherche,ou=France,dc=fenestros,dc=com"

adding new entry "ou=Production,ou=France,dc=fenestros,dc=com"

adding new entry "ou=Suisse,dc=fenestros,dc=com"

adding new entry "ou=Commercial,ou=Suisse,dc=fenestros,dc=com"

adding new entry "ou=USA,dc=fenestros,dc=com"

adding new entry "ou=Commercial,ou=USA,dc=fenestros,dc=com"

adding new entry "ou=Recherche,ou=USA,dc=fenestros,dc=com"
```

Utilisation du client graphique luma

Téléchargez le client **luma**, **PyQt** et **python-smbpasswd** à partir de ce lien :
http://downloads.naulinux.ru/pub/NauLinux/6.2/i386/sites/School/RPMS/ :

```
[root@centos6 tmp]# wget
http://downloads.naulinux.ru/pub/NauLinux/6.2/i386/sites/School/RPMS/luma-2.4-9.el6.noarch.rpm
--2014-05-10 19:14:46--
http://downloads.naulinux.ru/pub/NauLinux/6.2/i386/sites/School/RPMS/luma-2.4-9.el6.noarch.rpm
Résolution de downloads.naulinux.ru... 91.151.181.162
Connexion vers downloads.naulinux.ru|91.151.181.162|:80...connecté.
requête HTTP transmise, en attente de la réponse...200 OK
Longueur: 970868 (948K) [application/x-rpm]
Sauvegarde en : «luma-2.4-9.el6.noarch.rpm»

100%[==========================================================================================
==================>] 970 868      118K/s   ds 7,9s
```

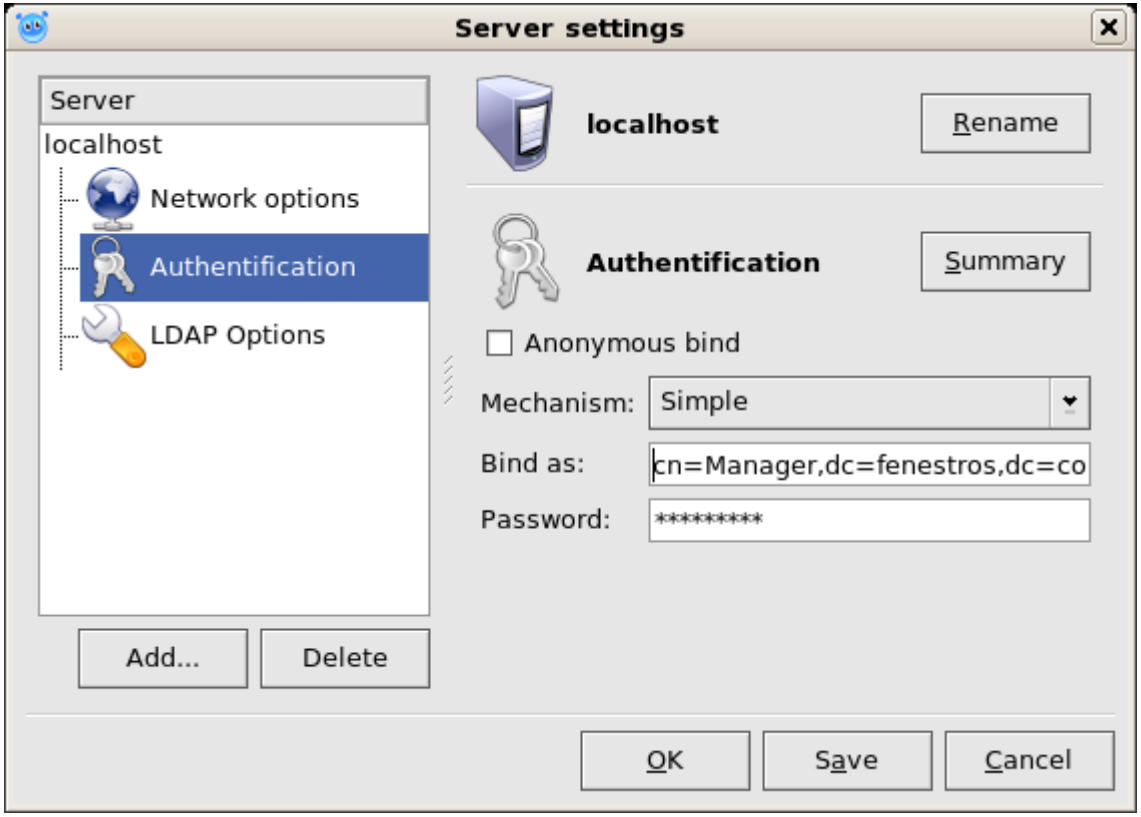
```
2014-05-10 19:15:00 (121 KB/s) - «luma-2.4-9.el6.noarch.rpm» sauvegardé [970868/970868]

[root@centos6 tmp]# wget
http://downloads.naulinux.ru/pub/NauLinux/6.2/i386/sites/School/RPMS/PyQt-3.18.1-6.el6.i686.rpm
--2014-05-10 19:15:28--
http://downloads.naulinux.ru/pub/NauLinux/6.2/i386/sites/School/RPMS/PyQt-3.18.1-6.el6.i686.rpm
Résolution de downloads.naulinux.ru... 91.151.181.162
Connexion vers downloads.naulinux.ru|91.151.181.162|:80...connecté.
requête HTTP transmise, en attente de la réponse...200 OK
Longueur: 1410428 (1,3M) [application/x-rpm]
Sauvegarde en : «PyQt-3.18.1-6.el6.i686.rpm»

100%[==========================================================================================
==================>] 1 410 428    118K/s   ds 11s

2014-05-10 19:15:45 (120 KB/s) - «PyQt-3.18.1-6.el6.i686.rpm» sauvegardé [1410428/1410428]

[root@centos6 tmp]# wget
http://downloads.naulinux.ru/pub/NauLinux/6.2/i386/sites/School/RPMS/python-smbpasswd-1.0.1-17.el6.i686.rpm
--2014-05-10 19:16:12--
http://downloads.naulinux.ru/pub/NauLinux/6.2/i386/sites/School/RPMS/python-smbpasswd-1.0.1-17.el6.i686.rpm
Résolution de downloads.naulinux.ru... 91.151.181.162
Connexion vers downloads.naulinux.ru|91.151.181.162|:80...connecté.
requête HTTP transmise, en attente de la réponse...200 OK
Longueur: 17824 (17K) [application/x-rpm]
Sauvegarde en : «python-smbpasswd-1.0.1-17.el6.i686.rpm»

100%[==========================================================================================
==================>] 17 824      56,7K/s   ds 0,3s

2014-05-10 19:16:17 (56,7 KB/s) - «python-smbpasswd-1.0.1-17.el6.i686.rpm» sauvegardé [17824/17824]
```

Installez-les :

```
[root@centos6 tmp]# yum localinstall luma-2.4-9.el6.noarch.rpm PyQt-3.18.1-6.el6.i686.rpm python-
smbpasswd-1.0.1-17.el6.i686.rpm --nogpgcheck
Loaded plugins: fastestmirror, refresh-packagekit, security
Setting up Local Package Process
Examining luma-2.4-9.el6.noarch.rpm: luma-2.4-9.el6.noarch
Marking luma-2.4-9.el6.noarch.rpm to be installed
Loading mirror speeds from cached hostfile
 * atomic: mir01.syntis.net
 * base: mirrors.prometeus.net
 * epel: mir01.syntis.net
 * extras: mirrors.prometeus.net
 * rpmforge: mir01.syntis.net
 * updates: mirrors.prometeus.net
Examining PyQt-3.18.1-6.el6.i686.rpm: PyQt-3.18.1-6.el6.i686
Marking PyQt-3.18.1-6.el6.i686.rpm to be installed
Examining python-smbpasswd-1.0.1-17.el6.i686.rpm: python-smbpasswd-1.0.1-17.el6.i686
Marking python-smbpasswd-1.0.1-17.el6.i686.rpm to be installed
Resolving Dependencies
--> Running transaction check
---> Package PyQt.i686 0:3.18.1-6.el6 will be installed
--> Processing Dependency: sip-api(6) >= 6.0 for package: PyQt-3.18.1-6.el6.i686
---> Package luma.noarch 0:2.4-9.el6 will be installed
---> Package python-smbpasswd.i686 0:1.0.1-17.el6 will be installed
--> Running transaction check
---> Package sip.i686 0:4.9.3-1.el6 will be installed
--> Finished Dependency Resolution

Dependencies Resolved

================================================================================================================
================================================
 Package                                  Arch                          Version
Repository                                                        Size
================================================================================================================
```

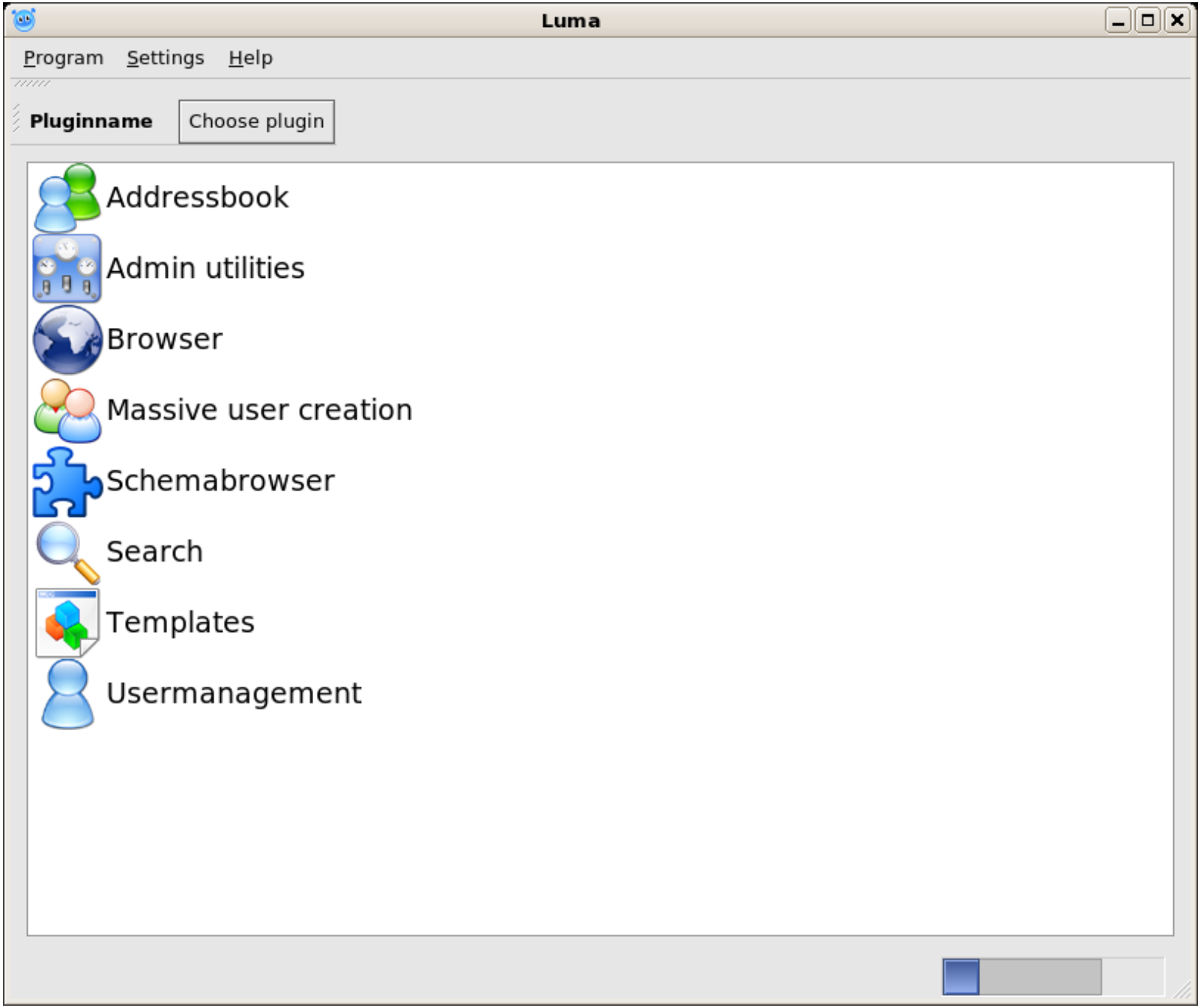
```
================================================================
Installing:
 PyQt                                i686                        3.18.1-6.el6
/PyQt-3.18.1-6.el6.i686                                  8.9 M
 luma                                noarch                      2.4-9.el6
/luma-2.4-9.el6.noarch                                   4.0 M
 python-smbpasswd                    i686                        1.0.1-17.el6                    /python-
smbpasswd-1.0.1-17.el6.i686                        31 k
Installing for dependencies:
 sip                                 i686                        4.9.3-1.el6                     base
146 k

Transaction Summary
================================================================================================================
================================================================
Install       4 Package(s)

Total size: 13 M
Total download size: 146 k
Installed size: 13 M
Is this ok [y/N]: y
```

Connectez-vous à votre serveur LDAP en utilisant luma. Cliquez sur le menu **Paramètres/Editer la Liste de Serveurs**. Cliquez sur **Add** puis renseignez le nom localhost. Sélectionnez **localhost/Athentification**, décochez **Anonymous bind** et remplissez les champs pour une connexion **simple** :

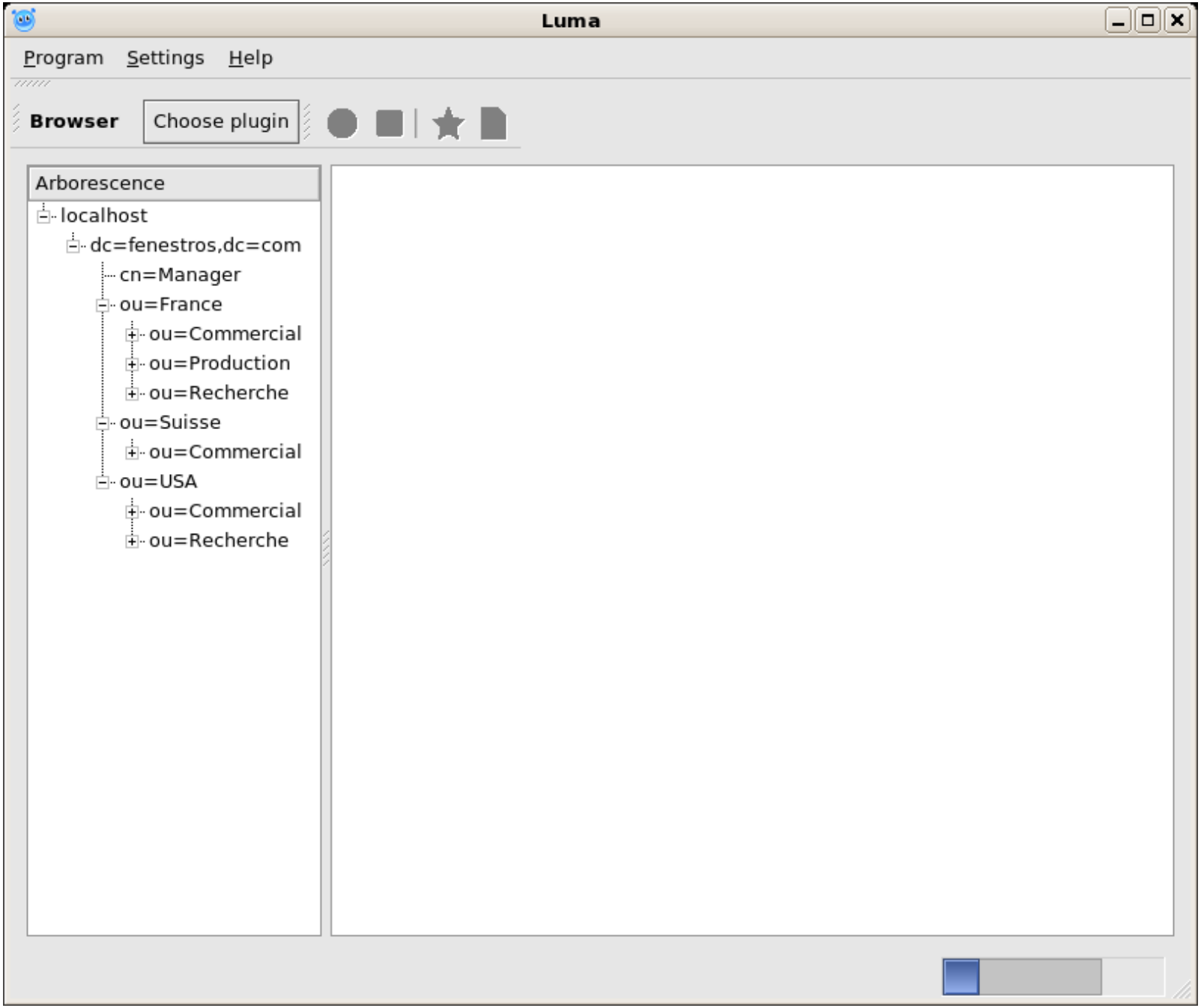


Cliquez sur le bouton **OK**.

Vous obtiendrez un résultat similaire à celui-ci :


Luma
Program
Settings
Help
Pluginname
Choose plugin
Addressbook
Admin utilities
Browser
Massive user creation
Schemabrowser
Search
Templates
Usermanagement

Cliquez sur **Browser** puis sur **localhost**. Vous obtiendrez un résultat similaire à celui-ci :


Luma
Program
Settings
Help
Browser
Choose plugin
Arborescence
localhost
dc=fenestros,dc=com
cn=Manager
ou=France
ou=Commercial
ou=Production
ou=Recherche
ou=Suisse
ou=Commercial
ou=USA
ou=Commercial
ou=Recherche

Le Directory Information Tree

Ce que vous pouvez constater avec ces deux outils est la présence du DIT (**D**irectory **I**nformation **T**ree). Ce DIT contient des **entrées** ayant des attributs dont les principaux types sont :

Noeud	Nom	Description
dc	domain component	domaine internet
c	country	pays
o	organization	organisation
ou	organizational unit	unité d'organisation
cn	common name	nom

Il est possible de faire référence à un entrée en utilisant un de deux noms :

Nom	Abréviation	Exemple
Distinguished Name	DN	ou=Commercial,ou=Suisse,dc=fenestros,dc=com
Relative Distinguished Name	RDN	ou=Commercial

Vous noterez qu'il existe trois entrées ayant le même **RDN** :

RDN	DN
ou=Commercial	ou=Commercial,ou=France,dc=fenestros,dc=com
ou=Commercial	ou=Commercial,ou=Suisse,dc=fenestros,dc=com
ou=Commercial	ou=Commercial,ou=USA,dc=fenestros,dc=com

Comme démontre cet exemple, il n'y a pas de contraintes au niveau des noms *à l'excéption de l'unicité* du DN.

Les noms des entités sont codés en UTF-8. Ceci implique que les noms peuvent contenir n'importe quelle combinaison de caractères y compris des éspaces.

Les alias

Le DIT peut également comporter des **alias** - des noeuds qui pointent vers une autre entrée du DIT.

Pour illustrer ce point, créez le fichier LDIF **/tmp/alias.ldif** et éditez-le ainsi :

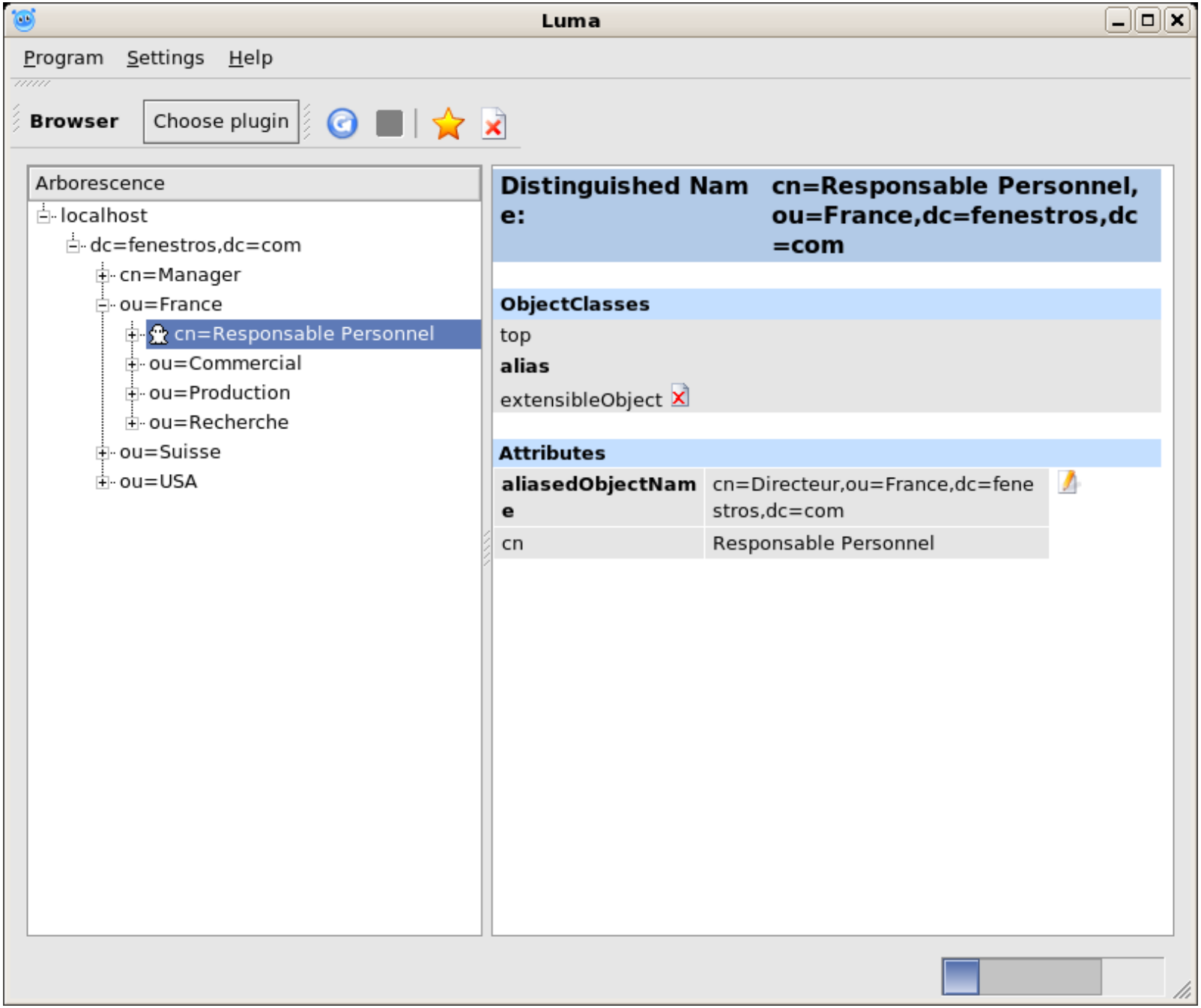
alias.ldif

```
version: 1
dn: cn=Responsable Personnel,ou=France,dc=fenestros,dc=com
cn: Responsable Personnel
aliasedObjectName: cn=Directeur,ou=France,dc=fenestros,dc=com
objectClass: top
objectClass: alias
objectClass: extensibleObject
```

Importez maintenant le fichier LDIF dans le DIT :

```
[root@centos6 ~]# ldapadd -f /tmp/alias.ldif -x -D "cn=Manager,dc=fenestros,dc=com" -w fenestros
adding new entry "cn=Responsable Personnel,ou=France,dc=fenestros,dc=com"
```

Constatez maintenant le résultat :


Luma
Program
Settings
Help
Browser
Choose plugin
Arborescence
localhost
dc=fenestros,dc=com
cn=Manager
ou=France
cn=Responsable Personnel
ou=Commercial
ou=Production
ou=Recherche
ou=Suisse
ou=USA
Distinguished Name:
cn=Responsable Personnel, ou=France,dc=fenestros,dc=com
ObjectClasses
top
alias
extensibleObject
Attributes
aliasedObjectName
cn=Directeur,ou=France,dc=fenestros,dc=com
cn
Responsable Personnel

Notez que le noeud vers lequel pointe l'alias n'existe pas.

Créez le fichier LDIF **/tmp/directeur.ldif** et éditez-le ainsi :

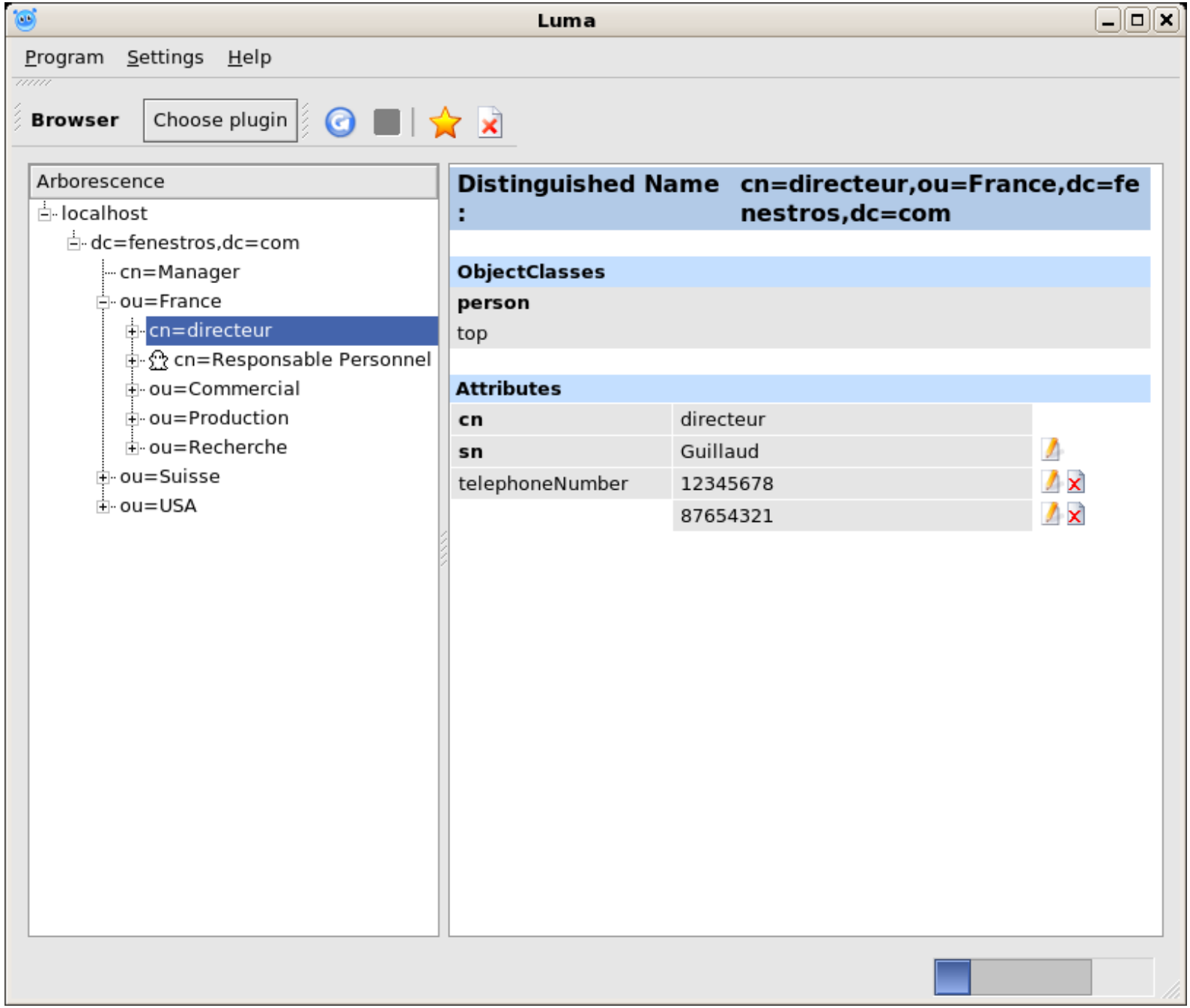
directeur.ldif

```
version: 1
dn: cn=directeur,ou=France,dc=fenestros,dc=com
objectClass: person
objectClass: top
cn: directeur
sn: Guillaud
telephoneNumber: 12345678
telephoneNumber: 87654321
```

Créez donc l'entrée **directeur** en utilisant le fichier **/tmp/directeur.ldif** :

```
[root@centos6 ~]# ldapadd -f /tmp/directeur.ldif -x -D "cn=Manager,dc=fenestros,dc=com" -w fenestros
adding new entry "cn=directeur,ou=France,dc=fenestros,dc=com"
```

Revenez à Luma. Vous obtiendrez une fenêtre similaire à celle-ci :


Luma
Program
Settings
Help
Browser
Choose plugin
Arborescence
localhost
dc=fenestros,dc=com
cn=Manager
ou=France
cn=directeur
cn=Responsable Personnel
ou=Commercial
ou=Production
ou=Recherche
ou=Suisse
ou=USA
Distinguished Name :
cn=directeur,ou=France,dc=fenestros,dc=com
ObjectClasses
person
top
Attributes
cn
directeur
sn
Guillaud
telephoneNumber
12345678
87654321

Créez le maintenant fichier LDIF **/tmp/plus.ldif** et éditez-le ainsi :

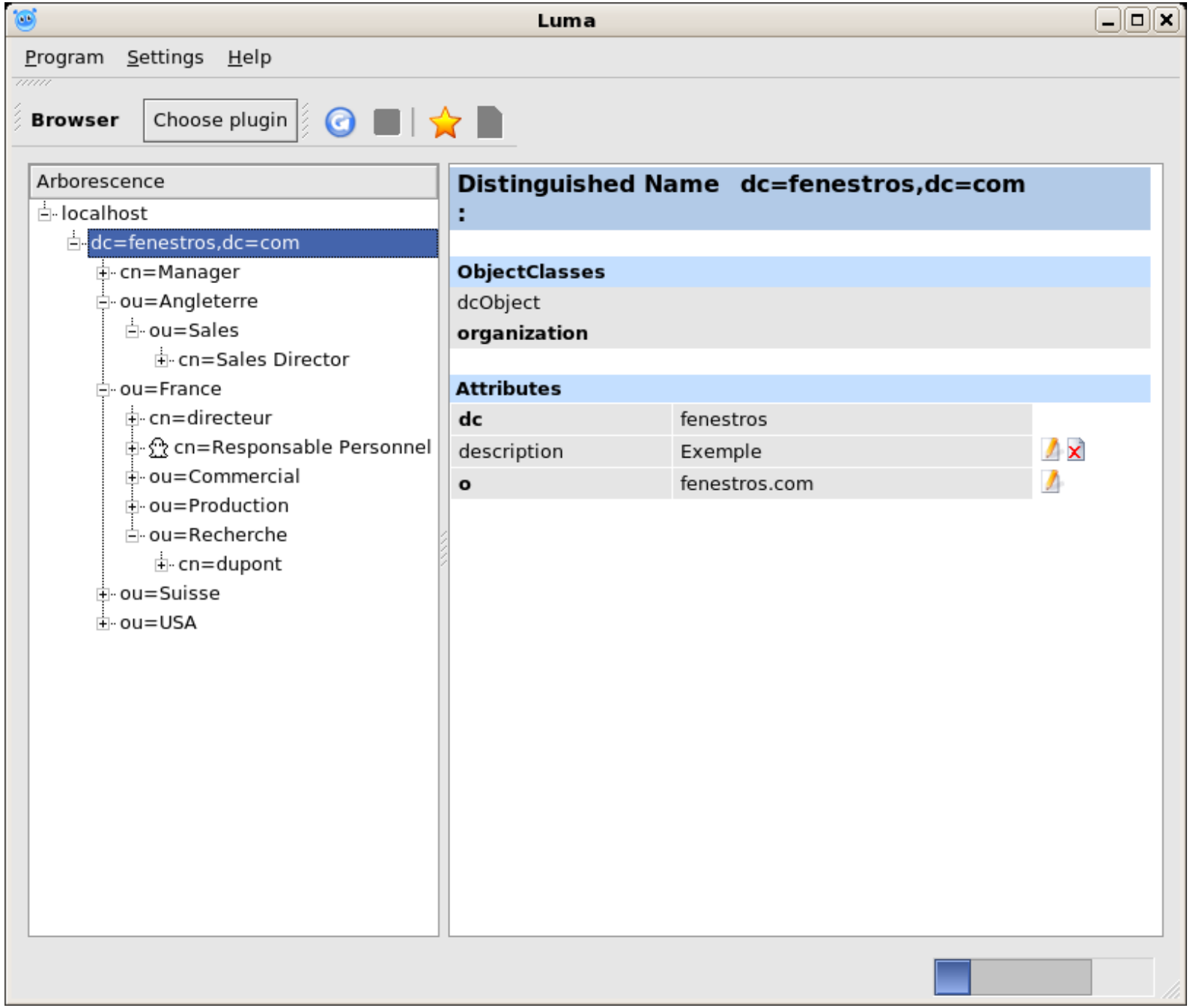
plus.ldif

```
version: 1
dn: ou=Angleterre,dc=fenestros,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Angleterre

dn: ou=Sales,ou=Angleterre,dc=fenestros,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Sales

dn: cn=Sales Director,ou=Sales,ou=Angleterre,dc=fenestros,dc=com
objectClass: person
objectClass: top
cn: Sales Director
sn: Smith

dn: cn=Sales Manager,cn=Sales Director,ou=Sales,ou=Angleterre,dc=fenestros,dc=com
objectClass: person
objectClass: top
cn: Sales Manager
sn: Brown

dn: cn=dupont,ou=Recherche,ou=France,dc=fenestros,dc=com
objectClass: person
objectClass: top
cn: dupont
sn: dupont
```

Créez donc les entrées en utilisant le fichier **/tmp/plus.ldif** :

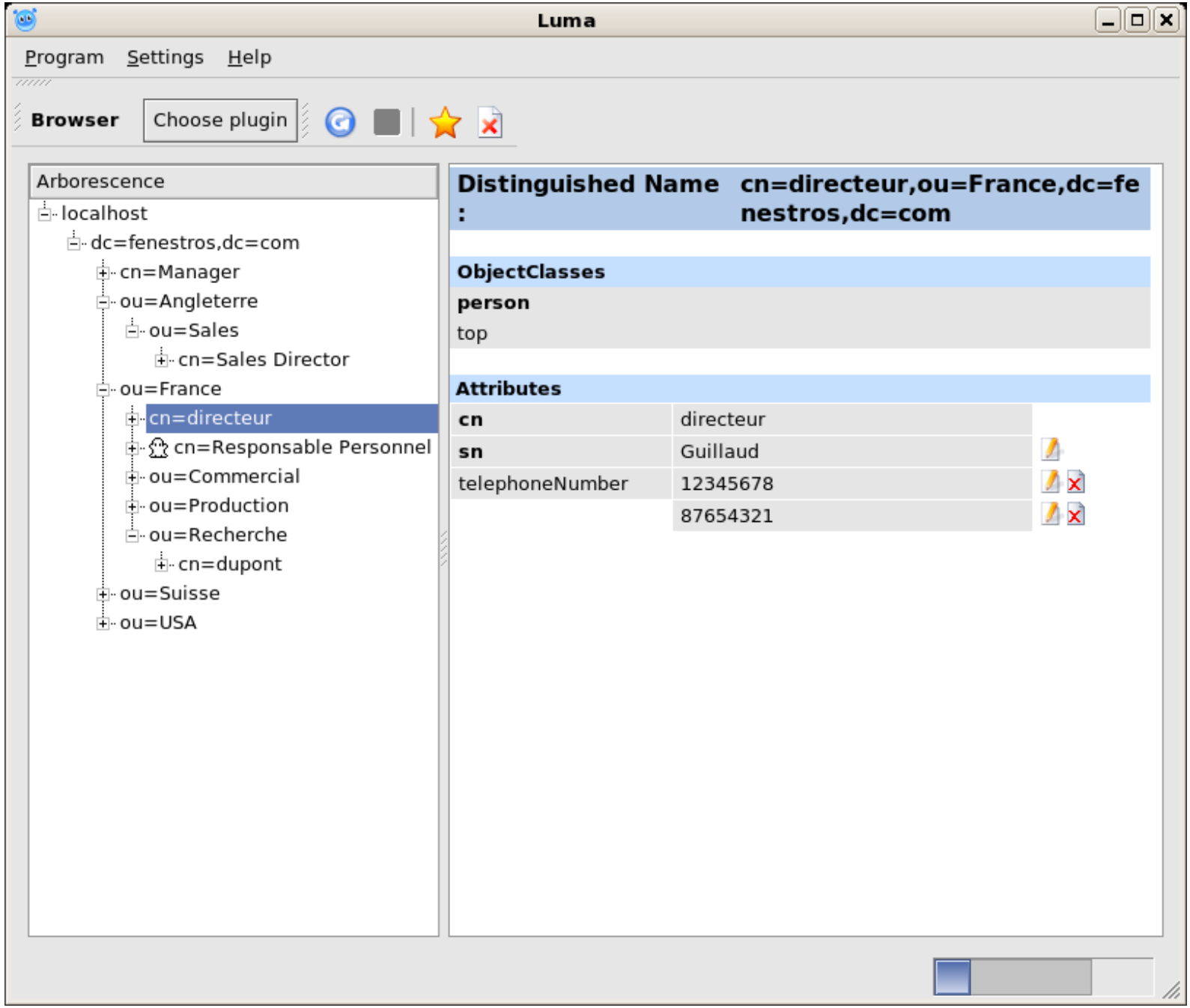
```
[root@centos6 ~]# ldapadd -f /tmp/plus.ldif -x -D "cn=Manager,dc=fenestros,dc=com" -w fenestros
adding new entry "ou=Angleterre,dc=fenestros,dc=com"

adding new entry "ou=Sales,ou=Angleterre,dc=fenestros,dc=com"

adding new entry "cn=Sales Director,ou=Sales,ou=Angleterre,dc=fenestros,dc=com"

adding new entry "cn=Sales Manager,cn=Sales Director,ou=Sales,ou=Angleterre,dc=fenestros,dc=com"

adding new entry "cn=dupont,ou=Recherche,ou=France,dc=fenestros,dc=com"
```

Revenez à Luma.Vous obtiendrez une fenêtre similaire à celle-ci :


Luma
Program
Settings
Help
Browser
Choose plugin
Arborescence
localhost
dc=fenestros,dc=com
cn=Manager
ou=Angleterre
ou=Sales
cn=Sales Director
ou=France
cn=directeur
cn=Responsable Personnel
ou=Commercial
ou=Production
ou=Recherche
cn=dupont
ou=Suisse
ou=USA
Distinguished Name : dc=fenestros,dc=com
ObjectClasses
dcObject
organization
Attributes
dc
fenestros
description
Exemple
o
fenestros.com

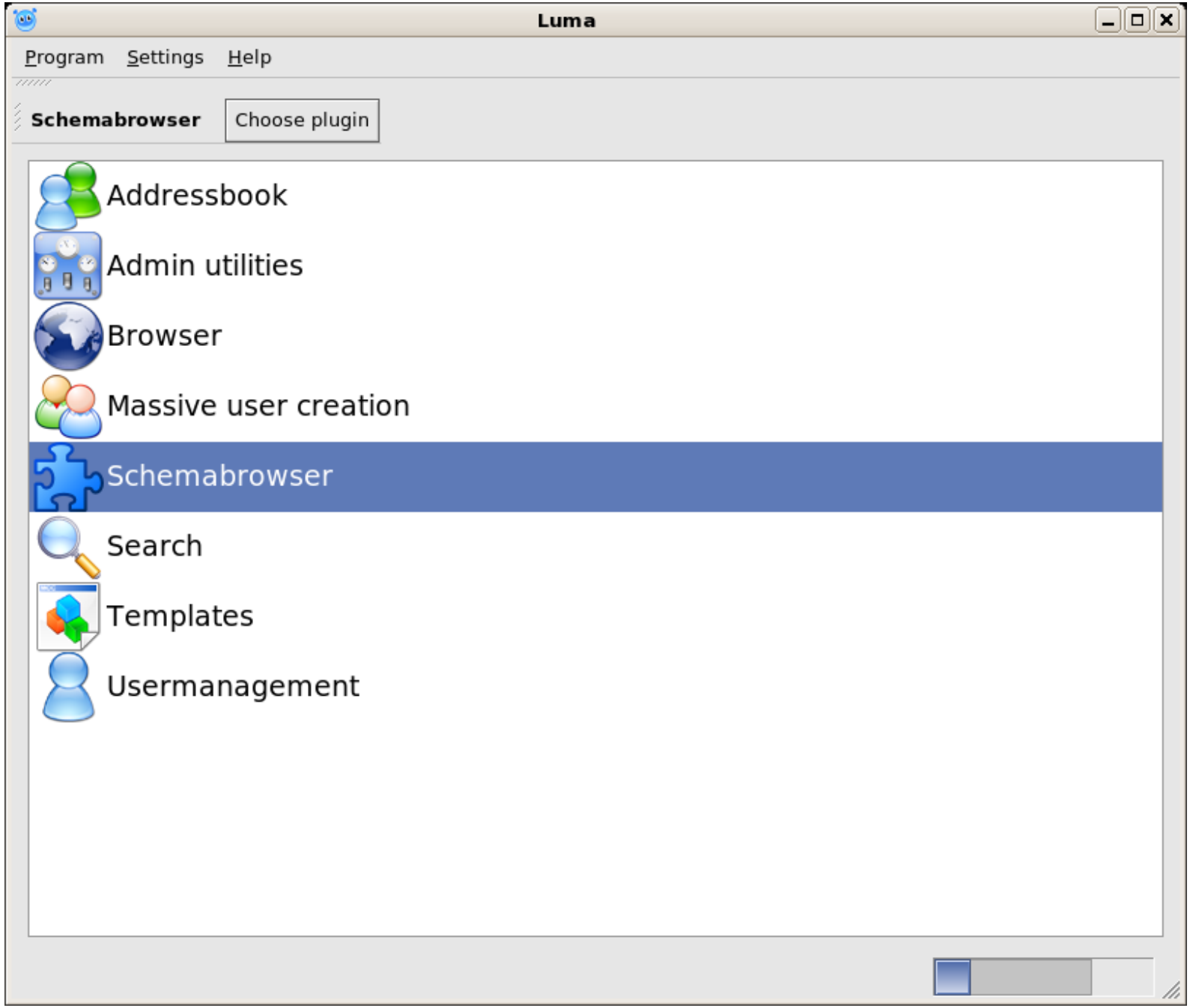
Les attributs

Regardons maintenant l'entrée du **directeur** en France et plus spécifiquement les **attributs** :

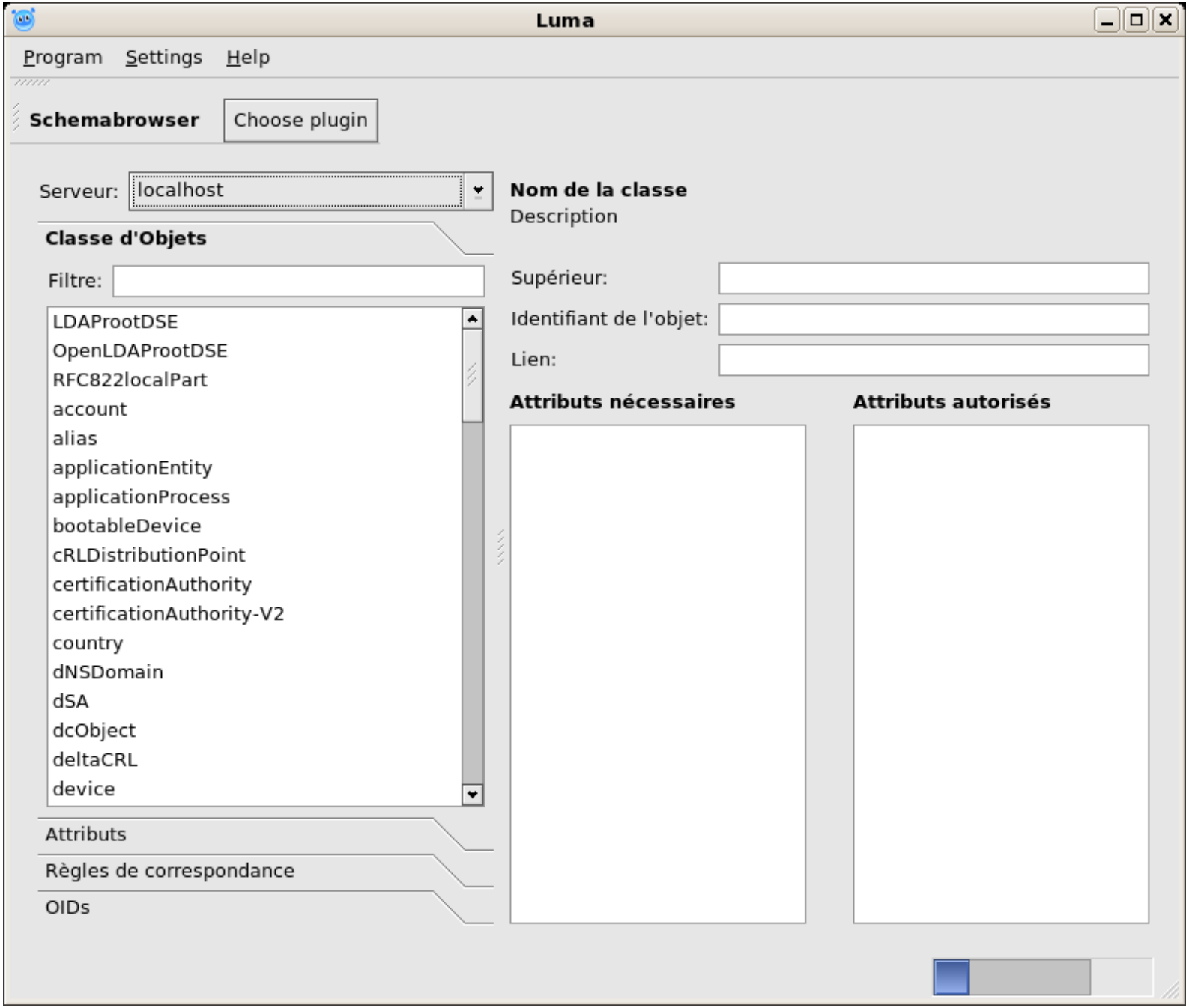

Luma
Program
Settings
Help
Browser
Choose plugin
Arborescence
localhost
dc=fenestros,dc=com
cn=Manager
ou=Angleterre
ou=Sales
cn=Sales Director
ou=France
cn=directeur
cn=Responsable Personnel
ou=Commercial
ou=Production
ou=Recherche
cn=dupont
ou=Suisse
ou=USA
Distinguished Name : cn=directeur,ou=France,dc=fenestros,dc=com
ObjectClasses
person
top
Attributes
cn directeur
sn Guillaud
telephoneNumber 12345678
87654321

On peut constater la présence de trois attributs, certains apparaissent en plusieurs exemples.

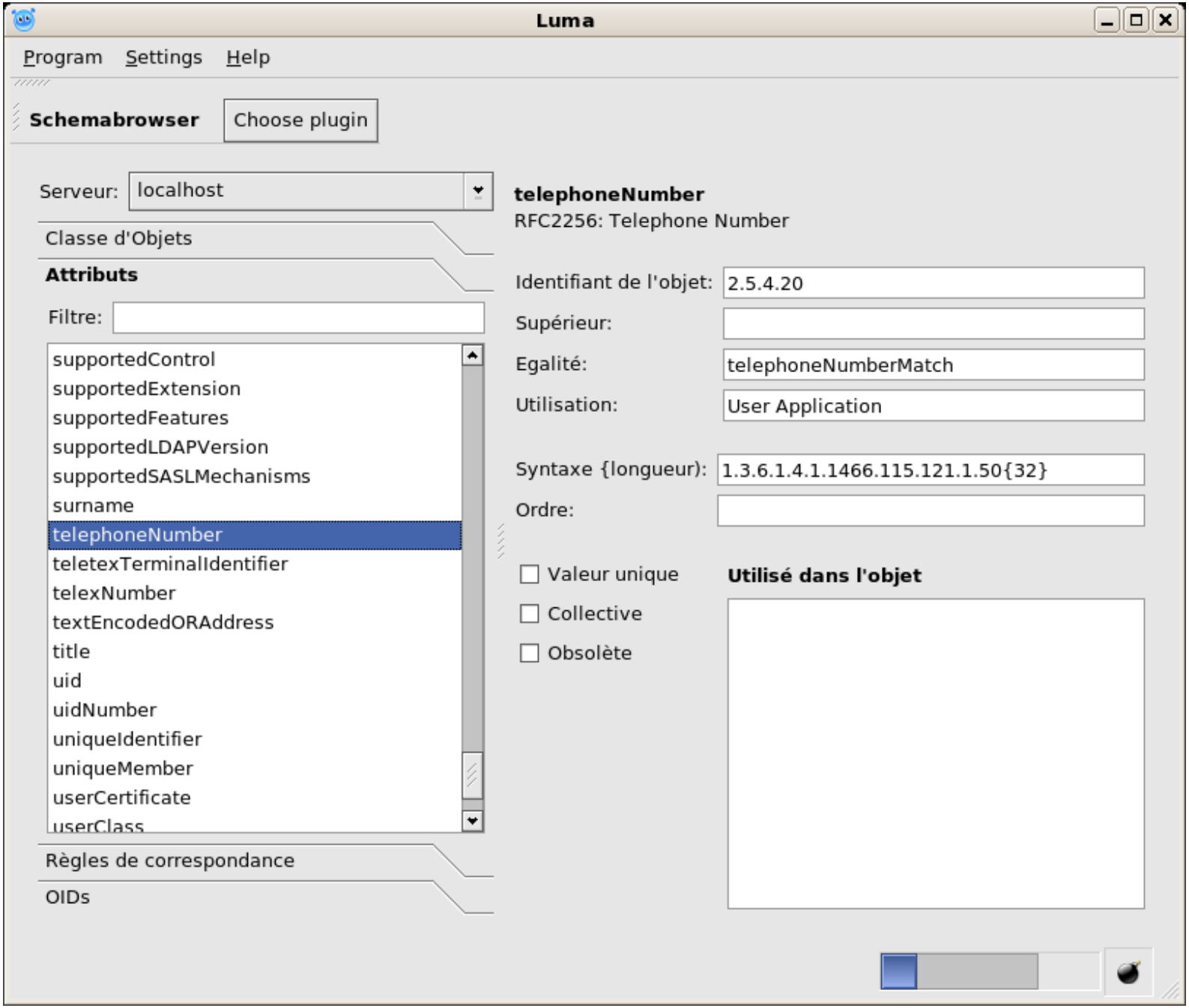
Choisissez maintenant le plugin **Schemabrowser** :


Luma
Program
Settings
Help
Schemabrowser
Choose plugin
Addressbook
Admin utilities
Browser
Massive user creation
Schemabrowser
Search
Templates
Usermanagement

Vous obtiendrez une fenêtre comme celle-ci :


Luma
Program
Settings
Help
Schemabrowser
Choose plugin
Serveur:
localhost
Nom de la classe
Description
Classe d'Objets
Filtre:
LDAProotDSE
OpenLDAProotDSE
RFC822localPart
account
alias
applicationEntity
applicationProcess
bootableDevice
cRLDistributionPoint
certificationAuthority
certificationAuthority-V2
country
dNSDomain
dSA
dcObject
deltaCRL
device
Supérieur:
Identifiant de l'objet:
Lien:
Attributs nécessaires
Attributs autorisés
Attributs
Règles de correspondance
OIDs

Dans le panneau de gauche, choisissez **Attributs** et trouvez l'entrée **telephoneNumber** :

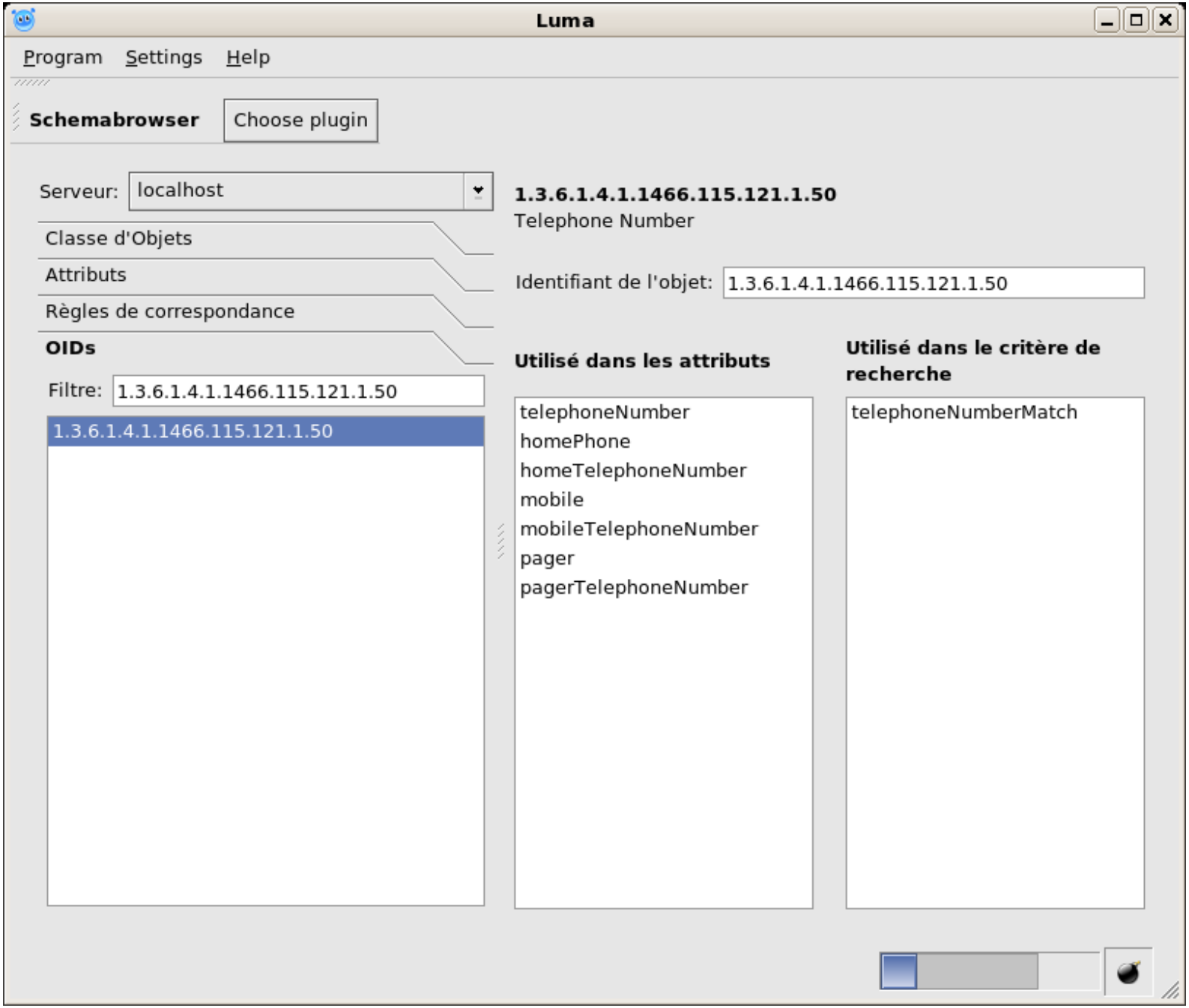

Luma
Program
Settings
Help
Schemabrowser
Choose plugin
Serveur:
localhost
Classe d'Objets
Attributs
Filtre:
supportedControl
supportedExtension
supportedFeatures
supportedLDAPVersion
supportedSASLMechanisms
surname
telephoneNumber
teletexTerminalIdentifier
telexNumber
textEncodedORAddress
title
uid
uidNumber
uniqueIdentifier
uniqueMember
userCertificate
userClass
Règles de correspondance
OIDs
telephoneNumber
RFC2256: Telephone Number
Identifiant de l'objet:
2.5.4.20
Supérieur:
Egalité:
telephoneNumberMatch
Utilisation:
User Application
Syntaxe {longueur):
1.3.6.1.4.1.1466.115.121.1.50{32}
Ordre:
Valeur unique
Collective
Obsolète
Utilisé dans l'objet

Chaque attribut est défini par plusieurs *types*. Dans le cas du **telephoneNumber**, nous trouvons :

Type	**Nom français**	**Description**
EQUALITY	Egalité	Règles d'égalités
OID	Identifiant de l'objet	Object Identifier
SYNTAX	Syntaxe	OID de ce que peut contenir l'attribut

Les **OID** sont standardisés. Vous pouvez chercher un OID sur le site Internet http://www.oid-info.com/.

Vous pouvez également voir l'OID dans Luma grâce à l'onglet **OIDs** :


Luma
Program
Settings
Help
Schemabrowser
Choose plugin
Serveur:
localhost
Classe d'Objets
Attributs
Règles de correspondance
OIDs
Filtre:
1.3.6.1.4.1.1466.115.121.1.50
1.3.6.1.4.1.1466.115.121.1.50
Telephone Number
Identifiant de l'objet:
1.3.6.1.4.1.1466.115.121.1.50
Utilisé dans les attributs
telephoneNumber
homePhone
homeTelephoneNumber
mobile
mobileTelephoneNumber
pager
pagerTelephoneNumber
Utilisé dans le critère de recherche
telephoneNumberMatch

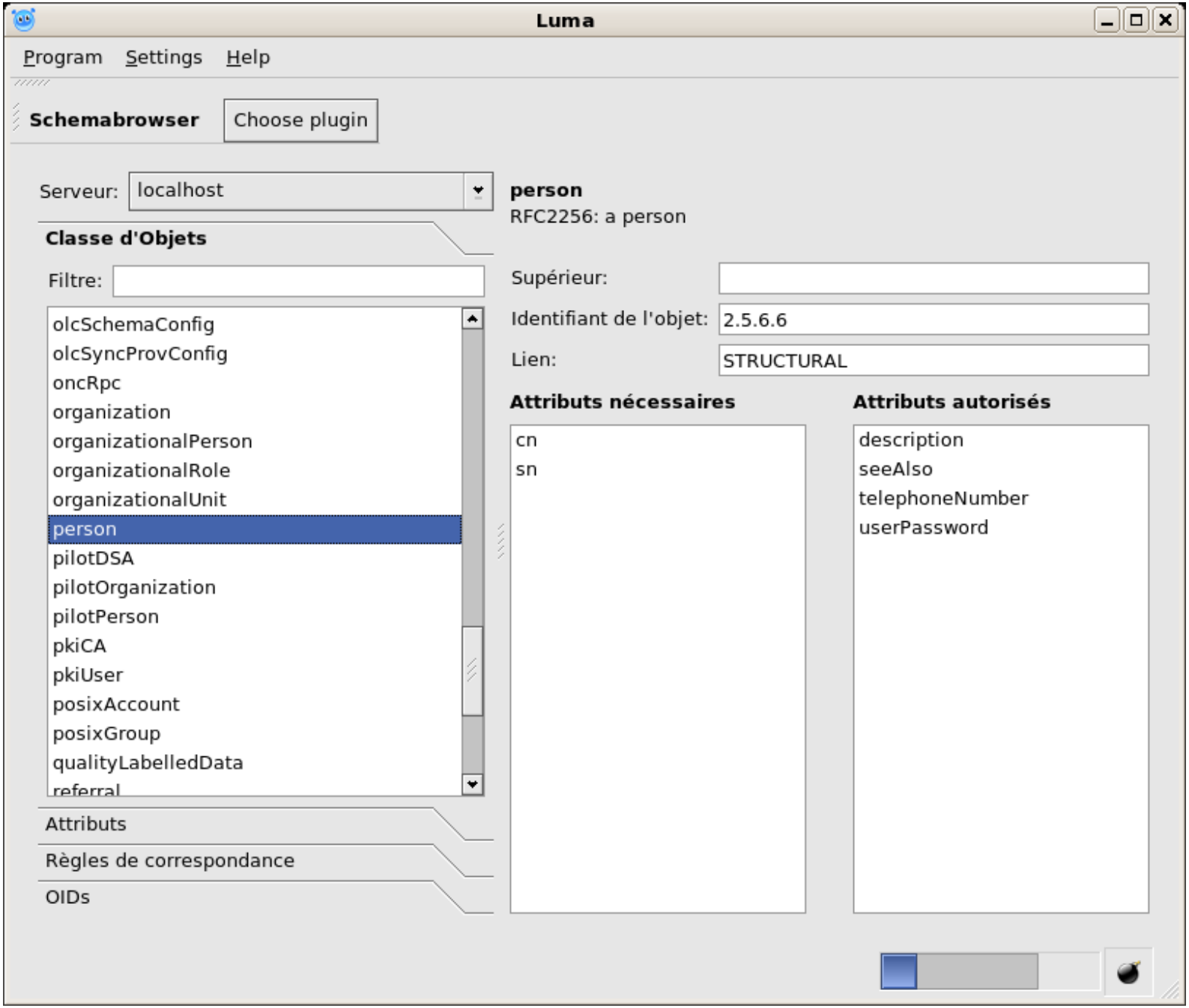
Un attribut peut dériver d'un autre attribut. Cet héritage implique le respect des caractériqtiques de l'attribut parent. Dans ce cas l'héritage est défini par l'attribut **SUP** dont la valeur est le nom de l'attribut parent.

Le serveur gère certains attributs automatiquement. Ces attributs sont appelés **attributs opérationnels**, par exemple :

Attributs Opérationnel	**Exemple**
createTimestamp	20080606075042Z
modifyTimestamp	20080606075042Z
creatorsName	cn=Manager,dc=fenestros,dc=com
modifiersName	cn=Manager,dc=fenestros,dc=com

Les classes

Chaque entrée dans le DIT **doit** comporter au moins **un** attribut **objectClass**. La classe d'objet du directeur est **person**. Dans le panneau de gauche, cliquez sur l'onglet **Classe d'objets** et trouvez la classe **Person** :


Luma
Program
Settings
Help
Schemabrowser
Choose plugin
Serveur:
localhost
person
RFC2256: a person
Classe d'Objets
Filtre:
olcSchemaConfig
olcSyncProvConfig
oncRpc
organization
organizationalPerson
organizationalRole
organizationalUnit
person
pilotDSA
pilotOrganization
pilotPerson
pkiCA
pkiUser
posixAccount
posixGroup
qualityLabelledData
referral
Supérieur:
Identifiant de l'objet:
2.5.6.6
Lien:
STRUCTURAL
Attributs nécessaires
cn
sn
Attributs autorisés
description
seeAlso
telephoneNumber
userPassword
Attributs
Règles de correspondance
OIDs

Dans cette fenêtre vous pouvez constater des Attributs nécessaires et des Attributs autorisés. En anglais ces deux termes correspondent à :

Elément	**Description**
MAY	Attributs autorisés
MUST	Attributs nécessaires

Notez aussi que cette classe est dite **STRUCTURAL**. Une entrée dans le DIT ne peut pas avoir plus d'une classe STRUCTURAL.

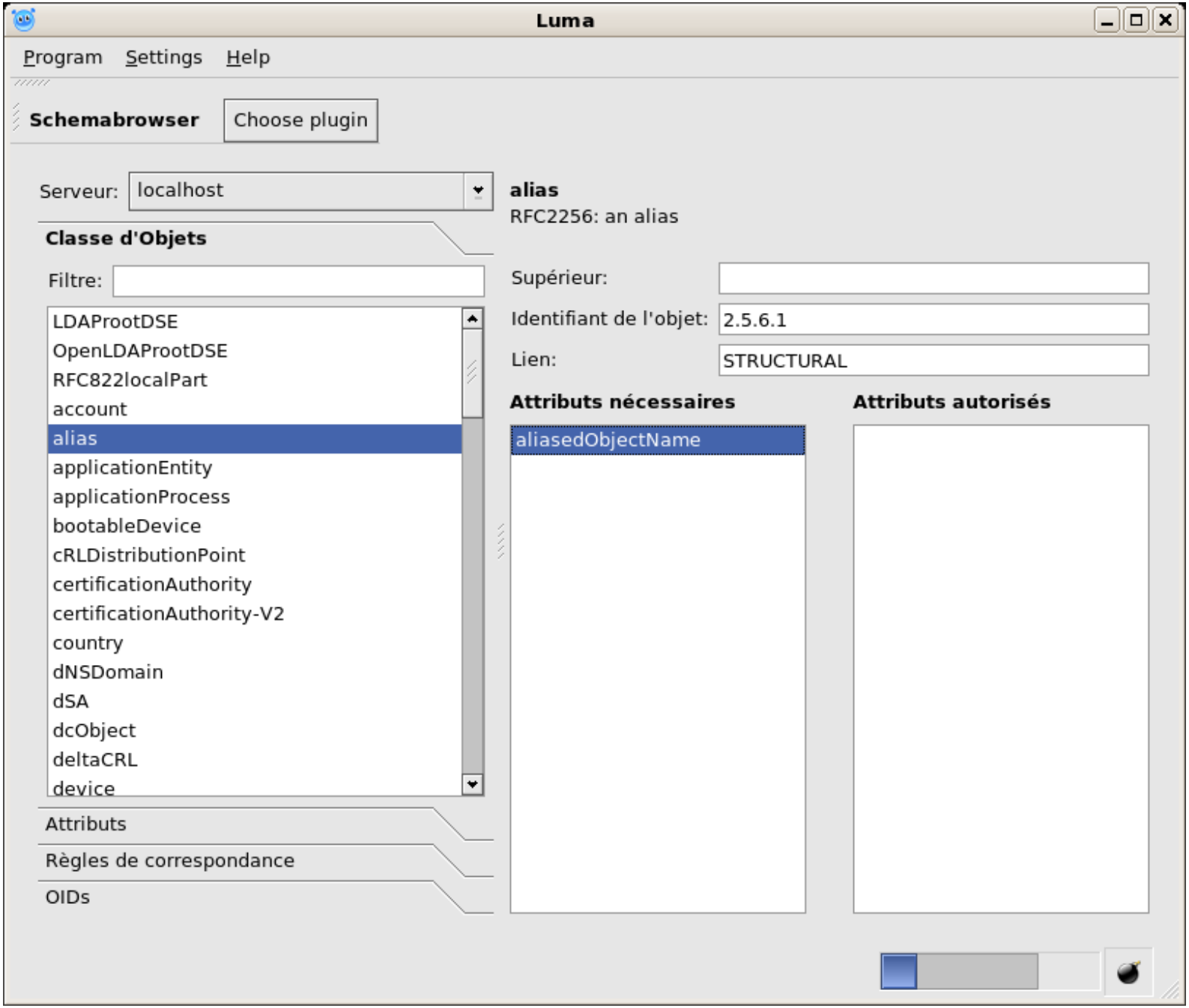
Le serveur OpenLDAP s'appuie sur trois types de classes d'objets :

- STRUCTURAL (STRUCTUREL)
- AUXILIARY (AUXILIAIRE)
- ABSTRACT (ABSTRAIT)

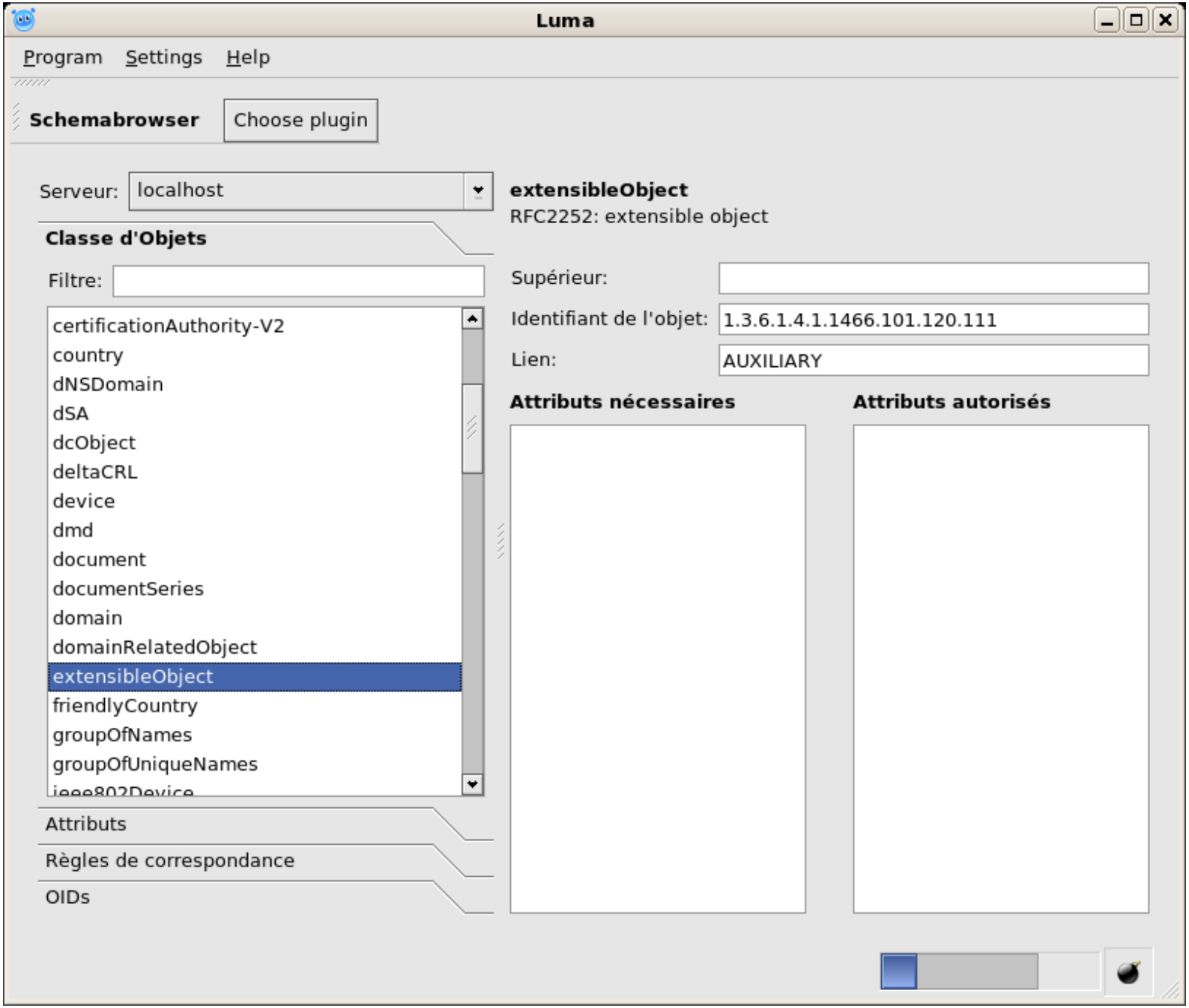
Prenons la cas de notre fichier LDIF **/tmp/alias.ldif**. Notons que dans ce fichier, nous avions utilisé un objectClass: alias :

```
version: 1
dn: cn=Responsable Personnel,ou=France,dc=fenestros,dc=com
cn: Responsable Personnel
aliasedObjectName: cn=Directeur,ou=France,dc=fenestros,dc=com
objectClass: top
objectClass: alias
objectClass: extensibleObject
```

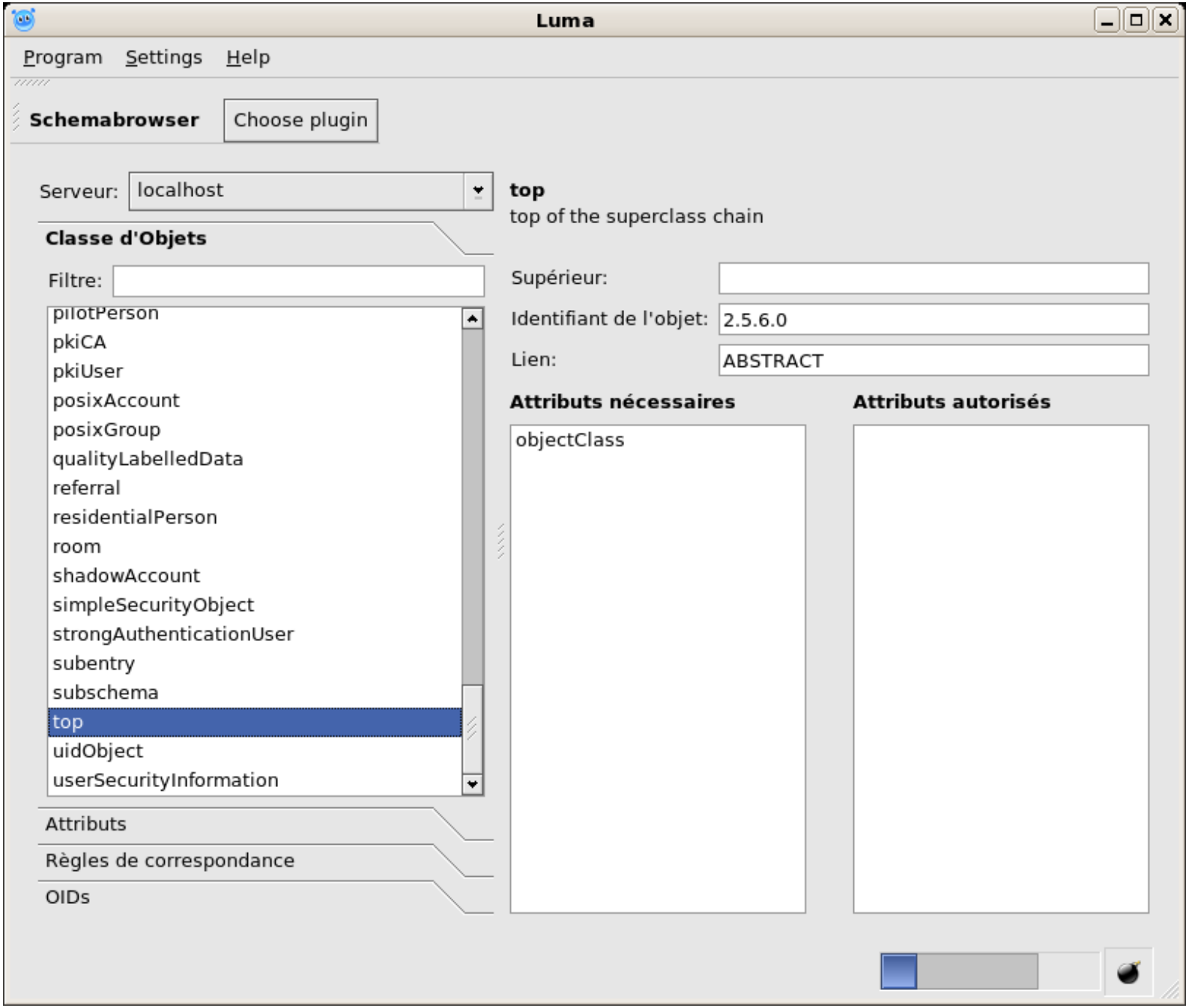
Si nous cherchons la définition de la classe alias, nous constatons que cette classe ne comprends pas d'attribut **cn** :


Luma
Program
Settings
Help
Schemabrowser
Choose plugin
Serveur:
localhost
alias
RFC2256: an alias
Classe d'Objets
Filtre:
Supérieur:
Identifiant de l'objet:
2.5.6.1
Lien:
STRUCTURAL
Attributs nécessaires
Attributs autorisés
aliasedObjectName
LDAProotDSE
OpenLDAProotDSE
RFC822localPart
account
alias
applicationEntity
applicationProcess
bootableDevice
cRLDistributionPoint
certificationAuthority
certificationAuthority-V2
country
dNSDomain
dSA
dcObject
deltaCRL
device
Attributs
Règles de correspondance
OIDs

L'utilisation de la classe auxiliaire **extensibleObject** a permis de créer l'attribut cn non défini dans la classe alias :


Luma
Program
Settings
Help
Schemabrowser
Choose plugin
Serveur:
localhost
extensibleObject
RFC2252: extensible object
Classe d'Objets
Filtre:
Supérieur:
Identifiant de l'objet:
1.3.6.1.4.1.1466.101.120.111
Lien:
AUXILIARY
Attributs nécessaires
Attributs autorisés
certificationAuthority-V2
country
dNSDomain
dSA
dcObject
deltaCRL
device
dmd
document
documentSeries
domain
domainRelatedObject
extensibleObject
friendlyCountry
groupOfNames
groupOfUniqueNames
Attributs
Règles de correspondance
OIDs

Le dernier type de classe est **ABSTRACT**. La classe **top** est une classe ABSTRACT et chaque entrée de l'annuaire doit comporté une classe top :


Luma
Program
Settings
Help
Schemabrowser
Choose plugin
Serveur:
localhost
top
top of the superclass chain
Classe d'Objets
Filtre:
pilotPerson
pkiCA
pkiUser
posixAccount
posixGroup
qualityLabelledData
referral
residentialPerson
room
shadowAccount
simpleSecurityObject
strongAuthenticationUser
subentry
subschema
top
uidObject
userSecurityInformation
Supérieur:
Identifiant de l'objet:
2.5.6.0
Lien:
ABSTRACT
Attributs nécessaires
objectClass
Attributs autorisés
Attributs
Règles de correspondance
OIDs

Les schémas

L'ensemble des attributs et des classes d'un annuaire porte le nom de **schéma**. Les schémas sont normalisés. Les fichiers de schémas sont stockés dans le répertoire **/etc/openldap/schema/** :

```
[root@centos6 ~]# ls /etc/openldap/schema/
collective.schema  cosine.schema       inetorgperson.schema  openldap.ldif
corba.schema       dhcp.schema         java.schema           openldap.schema
core.ldif          duaconf.schema      misc.schema           pmi.schema
core.schema        dyngroup.schema     nis.ldif              ppolicy.schema
cosine.ldif        inetorgperson.ldif  nis.schema
```

Le schema de base est **core.schema**. D'autres schémas utiles sont notamment :

- inetorgperson.schema
- cosine.schema

Le chargement de ces deux fichiers de schémas nous permet de créer un objet pour une adresse email.

Créez le fichier LDIF **/tmp/mail.ldif** et éditez-le ainsi :

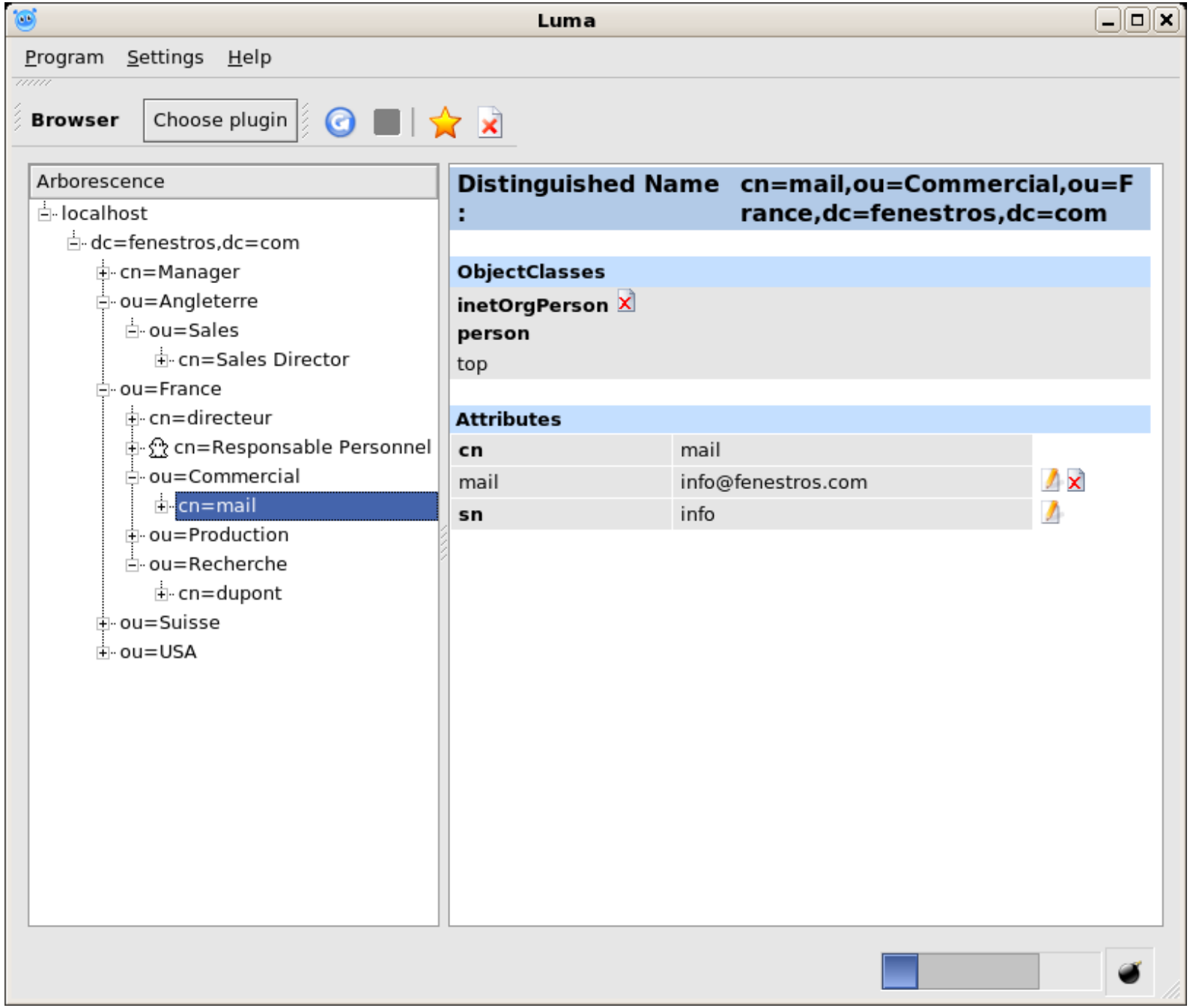
mail.ldif

```
version: 1
dn: cn=mail,ou=Commercial,ou=France,dc=fenestros,dc=com
objectClass: inetOrgPerson
objectClass: person
objectClass: top
cn: mail
mail: info@fenestros.com
sn: info
```

Créez donc l'entrée **mail** en utilisant le fichier **/tmp/mail.ldif** :

```
[root@localhost tmp]# ldapadd -f /tmp/mail.ldif -x -D "cn=Manager,dc=fenestros,dc=com" -w fenestros
adding new entry "cn=mail,ou=Commercial,ou=France,dc=fenestros,dc=com"
```

Constatez maintenant le résultat avec Luma :


Luma
Program
Settings
Help
Browser
Choose plugin
Arborescence
localhost
dc=fenestros,dc=com
cn=Manager
ou=Angleterre
ou=Sales
cn=Sales Director
ou=France
cn=directeur
cn=Responsable Personnel
ou=Commercial
cn=mail
ou=Production
ou=Recherche
cn=dupont
ou=Suisse
ou=USA
Distinguished Name :
cn=mail,ou=Commercial,ou=France,dc=fenestros,dc=com
ObjectClasses
inetOrgPerson
person
top
Attributes
cn
mail
mail
info@fenestros.com
sn
info

Les referrals

Il existe une autre entrée spéciale qui s'appelle un **referral**. Un referral est un pointeur vers une entrée vers un autre serveur LDAP. Pour illustrer ce point, créez le fichier LDIF **/tmp/referral.ldif** et éditez-le ainsi :

referral.ldif

```
version: 1
dn: ou=Informatique,dc=fenestros,dc=com
objectClass: referral
objectClass: extensibleObject
objectClass: top
ref: ldap://ldap.fenestros.net/ou=fenestros.com,dc=fenestros,dc=net
ou: Informatique
```

Utilisez la commande ldapadd pour ajouter l'entrée au DIT :

```
[root@centos6 tmp]# ldapadd -f /tmp/referral.ldif -x -D "cn=Manager,dc=fenestros,dc=com" -w fenestros
adding new entry "ou=Informatique,dc=fenestros,dc=com"
```

Constatez le résultat avec Luma. Expliquez ce que vous voyez.

La commande ldapsearch

Chaque annuaire contient une entrée **RootDSE**. Cette entrée est particulière puisque son DN est vide. Son rôle est de contenir les attributs opérationnels du serveur qui comportent des **extensions de contrôle** et **opérations** disponibles sur le serveur. Cette information est utilisée par le client LDAP lors de sa connexion afin de connaître ce que peut et ce que ne peut pas faire le serveur.

Afin de connaître le contenu du **RootDSE**, il convient d'utiliser la commande **ldapsearch**. Cette commande prend les options suivantes :

```
[root@centos6 tmp]# ldapsearch  --help
ldapsearch: invalid option -- '-'
ldapsearch: unrecognized option --
usage: ldapsearch [options] [filter [attributes...]]
where:
  filter    RFC 4515 compliant LDAP search filter
  attributes    whitespace-separated list of attribute descriptions
    which may include:
      1.1   no attributes
      *     all user attributes
      +     all operational attributes
Search options:
  -a deref   one of never (default), always, search, or find
  -A         retrieve attribute names only (no values)
  -b basedn  base dn for search
  -c         continuous operation mode (do not stop on errors)
  -E [!]<ext>[=<extparam>] search extensions (! indicates criticality)
             [!]domainScope              (domain scope)
             !dontUseCopy                (Don't Use Copy)
             [!]mv=<filter>              (RFC 3876 matched values filter)
             [!]pr=<size>[/prompt|noprompt] (RFC 2696 paged results/prompt)
             [!]sss=[-]<attr[:OID]>[/[-]<attr[:OID]>...]
                                         (RFC 2891 server side sorting)
             [!]subentries[=true|false]  (RFC 3672 subentries)
             [!]sync=ro[/<cookie>]       (RFC 4533 LDAP Sync refreshOnly)
                     rp[/<cookie>][/<slimit>] (refreshAndPersist)
             [!]vlv=<before>/<after>(/<offset>/<count>|:<value>)
                                         (ldapv3-vlv-09 virtual list views)
             [!]deref=derefAttr:attr[,...][;derefAttr:attr[,...][;...]]
             [!]<oid>=:<value>           (generic control; no response handling)
  -f file    read operations from `file'
  -F prefix  URL prefix for files (default: file:///tmp/)
```

```
  -l limit   time limit (in seconds, or "none" or "max") for search
  -L         print responses in LDIFv1 format
  -LL        print responses in LDIF format without comments
  -LLL       print responses in LDIF format without comments
             and version
  -M         enable Manage DSA IT control (-MM to make critical)
  -P version protocol version (default: 3)
  -s scope   one of base, one, sub or children (search scope)
  -S attr    sort the results by attribute `attr'
  -t         write binary values to files in temporary directory
  -tt        write all values to files in temporary directory
  -T path    write files to directory specified by path (default: /tmp)
  -u         include User Friendly entry names in the output
  -z limit   size limit (in entries, or "none" or "max") for search
Common options:
  -d level   set LDAP debugging level to `level'
  -D binddn  bind DN
  -e [!]<ext>[=<extparam>] general extensions (! indicates criticality)
             [!]assert=<filter>     (RFC 4528; a RFC 4515 Filter string)
             [!]authzid=<authzid>   (RFC 4370; "dn:<dn>" or "u:<user>")
             [!]chaining[=<resolveBehavior>[/<continuationBehavior>]]
                    one of "chainingPreferred", "chainingRequired",
                    "referralsPreferred", "referralsRequired"
             [!]manageDSAit         (RFC 3296)
             [!]noop
             ppolicy
             [!]postread[=<attrs>]  (RFC 4527; comma-separated attr list)
             [!]preread[=<attrs>]   (RFC 4527; comma-separated attr list)
             [!]relax
             abandon, cancel, ignore (SIGINT sends abandon/cancel,
             or ignores response; if critical, doesn't wait for SIGINT.
             not really controls)
  -h host    LDAP server
  -H URI     LDAP Uniform Resource Identifier(s)
```

```
  -I         use SASL Interactive mode
  -n         show what would be done but don't actually do it
  -N         do not use reverse DNS to canonicalize SASL host name
  -O props   SASL security properties
  -o <opt>[=<optparam] general options
             nettimeout=<timeout> (in seconds, or "none" or "max")
  -p port    port on LDAP server
  -Q         use SASL Quiet mode
  -R realm   SASL realm
  -U authcid SASL authentication identity
  -v         run in verbose mode (diagnostics to standard output)
  -V         print version info (-VV only)
  -w passwd  bind password (for simple authentication)
  -W         prompt for bind password
  -x         Simple authentication
  -X authzid SASL authorization identity ("dn:<dn>" or "u:<user>")
  -y file    Read password from file
  -Y mech    SASL mechanism
  -Z         Start TLS request (-ZZ to require successful response)
```

La syntaxe de la recherche du **RootDSE** est :

```
ldapsearch -x -s base -b "" "(objectclass=*)" +
```

Dans cette commande on peut constater des options :

Option	**Description**
-s base	Définit la portée de la recherche
-b ”“	Définit un dn vide pour la recherche
”(objectclass=*)“	Définit ce que l'on recherche
+	Définit tous les attributs opérationnels

Le résultat obtenu est :

```
[root@centos6 tmp]# ldapsearch -x -s base -b "" "(objectclass=*)" +
# extended LDIF
#
# LDAPv3
# base <> with scope baseObject
# filter: (objectclass=*)
# requesting: +
#

#
dn:
structuralObjectClass: OpenLDAProotDSE
configContext: cn=config
monitorContext: cn=Monitor
namingContexts: dc=fenestros,dc=com
supportedControl: 2.16.840.1.113730.3.4.18
supportedControl: 2.16.840.1.113730.3.4.2
supportedControl: 1.3.6.1.4.1.4203.1.10.1
supportedControl: 1.2.840.113556.1.4.319
supportedControl: 1.2.826.0.1.3344810.2.3
supportedControl: 1.3.6.1.1.13.2
supportedControl: 1.3.6.1.1.13.1
supportedControl: 1.3.6.1.1.12
supportedExtension: 1.3.6.1.4.1.1466.20037
supportedExtension: 1.3.6.1.4.1.4203.1.11.1
supportedExtension: 1.3.6.1.4.1.4203.1.11.3
supportedExtension: 1.3.6.1.1.8
supportedFeatures: 1.3.6.1.1.14
supportedFeatures: 1.3.6.1.4.1.4203.1.5.1
supportedFeatures: 1.3.6.1.4.1.4203.1.5.2
supportedFeatures: 1.3.6.1.4.1.4203.1.5.3
supportedFeatures: 1.3.6.1.4.1.4203.1.5.4
supportedFeatures: 1.3.6.1.4.1.4203.1.5.5
supportedLDAPVersion: 3
```

```
supportedSASLMechanisms: GSSAPI
entryDN:
subschemaSubentry: cn=Subschema

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
```

Utilisez le site web http://www.oid-info.com pour rechercher les **supportedFeatures**.

La commande ldapsearch utilisée ci-dessus a précisé une **portée** de base grâce à l'option **-s base**.

L'intérrogation de l'annuaire se fait avec une reqûete composée de 4 éléments :

Elément	**Description**
Base	Le point de départ de la reqûete
Attributs	La liste des attributs à retourner. Si vide ou *, tous les attributs sont retournés
Portée	Indique la portée de la reqûete. Elle peut être **Base**, **One** ou **Sub**
Filtre	Spécifie des critères a appliquer au attributs

La notion de la portée est la suivante :

- Base
  - Seul l'objet de base est fourni,
- One
  - Seuls les objets au premier niveau en dessous de l'objet de base sont fournis,
- Sub
  - Tous les objets en dessous de l'objet de base sont fournis.

La forme d'un filtre est :

- attribut, opérateur, valeur

L'opérateur est un des éléments suivants :

Opérateur	**Description**
=	égalité stricte
~=	égalité approximative
<=	inférieur ou égal
>=	supérieur ou égal
&	et logique
|	ou logique
!	non logique

La valeur peut être :

- une valeur exacte,
- une expression contenant le joker *.

Quand on veut trouver un caractère spécial, il convient de le remplacer avec une séquence spécifique :

Caractère	**Séquence**
*	\2A
(	\28
)	\29
\	\5C
Nul	\00

L'utilisation de ldapsearch peut être illustrée avec quelques exemples.

Dans cet exemple, nous cherchons les entrées du type **ou** à partir de **ou=France,dc=fenestros,dc=com** :

```
[root@centos6 tmp]# ldapsearch -x -b "ou=France,dc=fenestros,dc=com" "(objectClass=organizationalUnit)"
```

```
# extended LDIF
#
# LDAPv3
# base <ou=France,dc=fenestros,dc=com> with scope subtree
# filter: (objectClass=organizationalUnit)
# requesting: ALL
#

# France, fenestros.com
dn: ou=France,dc=fenestros,dc=com
objectClass: organizationalUnit
objectClass: top
ou: France

# Commercial, France, fenestros.com
dn: ou=Commercial,ou=France,dc=fenestros,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Commercial

# Recherche, France, fenestros.com
dn: ou=Recherche,ou=France,dc=fenestros,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Recherche

# Production, France, fenestros.com
dn: ou=Production,ou=France,dc=fenestros,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Production

# search result
search: 2
```

```
result: 0 Success

# numResponses: 5
# numEntries: 4
```

Dans cet exemple, nous cherchons les entrées **enfants** du type **ou** à partir de **ou=France,dc=fenestros,dc=com** sans commentaires :

```
[root@centos6 tmp]# ldapsearch -x -LLL -s children -b "ou=France,dc=fenestros,dc=com"
"(objectClass=organizationalUnit)"
dn: ou=Commercial,ou=France,dc=fenestros,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Commercial

dn: ou=Recherche,ou=France,dc=fenestros,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Recherche

dn: ou=Production,ou=France,dc=fenestros,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Production
```

Dans cet exemple, nous cherchons les entrées **enfants** du type **ou** à partir de **ou=France,dc=fenestros,dc=com** sans commentaires et avec un tri sur la valeur de l'ou :

```
[root@centos6 tmp]# ldapsearch -x -LLL -S ou -s children -b "ou=France,dc=fenestros,dc=com"
dn: cn=Responsable Personnel,ou=France,dc=fenestros,dc=com
cn: Responsable Personnel
aliasedObjectName: cn=Directeur,ou=France,dc=fenestros,dc=com
objectClass: top
objectClass: alias
objectClass: extensibleObject
```

```
dn: cn=directeur,ou=France,dc=fenestros,dc=com
objectClass: person
objectClass: top
cn: directeur
sn: Guillaud
telephoneNumber: 12345678
telephoneNumber: 87654321

dn: cn=dupont,ou=Recherche,ou=France,dc=fenestros,dc=com
objectClass: person
objectClass: top
cn: dupont
sn: dupont

dn: cn=mail,ou=Commercial,ou=France,dc=fenestros,dc=com
objectClass: inetOrgPerson
objectClass: person
objectClass: top
cn: mail
mail: info@fenestros.com
sn: info

dn: ou=Commercial,ou=France,dc=fenestros,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Commercial

dn: ou=Production,ou=France,dc=fenestros,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Production

dn: ou=Recherche,ou=France,dc=fenestros,dc=com
objectClass: organizationalUnit
```

```
objectClass: top
ou: Recherche
```

Dans cet exemple, nous cherchons les entrées **enfants** du type **ou** à partir de **ou=France,dc=fenestros,dc=com** sans commentaires, avec un tri sur la valeur de l'ou et en demandant une affichage plus lisible :

```
[root@centos6 ~]# ldapsearch -x -LLL -S ou -s children -u -b "ou=France,dc=fenestros,dc=com"
dn: cn=Responsable Personnel,ou=France,dc=fenestros,dc=com
ufn: Responsable Personnel, France, fenestros.com
cn: Responsable Personnel
aliasedObjectName: cn=Directeur,ou=France,dc=fenestros,dc=com
objectClass: top
objectClass: alias
objectClass: extensibleObject

dn: cn=directeur,ou=France,dc=fenestros,dc=com
ufn: directeur, France, fenestros.com
objectClass: person
objectClass: top
cn: directeur
sn: Guillaud
telephoneNumber: 12345678
telephoneNumber: 87654321

dn: cn=dupont,ou=Recherche,ou=France,dc=fenestros,dc=com
ufn: dupont, Recherche, France, fenestros.com
objectClass: person
objectClass: top
cn: dupont
sn: dupont

dn: ou=Commercial,ou=France,dc=fenestros,dc=com
ufn: Commercial, France, fenestros.com
objectClass: organizationalUnit
```

```
objectClass: top
ou: Commercial

dn: ou=Production,ou=France,dc=fenestros,dc=com
ufn: Production, France, fenestros.com
objectClass: organizationalUnit
objectClass: top
ou: Production

dn: ou=Recherche,ou=France,dc=fenestros,dc=com
ufn: Recherche, France, fenestros.com
objectClass: organizationalUnit
objectClass: top
ou: Recherche
```

Dans cet exemple, nous cherchons les entrées du type **ou** et **cn** à partir de **ou=France,dc=fenestros,dc=com** en utilisant un fichier de filtre. Le fichier de filtre est **/tmp/filtre** et contient **trois** lignes :

```
organizationalUnit
inetOrgPerson
```

Ce fichier filtre DOIT comporter une ligne vide à la fin.

La commande est :

```
[root@centos6 tmp]# ldapsearch -x -b "ou=France,dc=fenestros,dc=com" -f /tmp/filtre "(objectClass=%s)" ou cn
# extended LDIF
#
# LDAPv3
# base <ou=France,dc=fenestros,dc=com> with scope subtree
# filter pattern: (objectClass=%s)
```

```
# requesting: ou cn
#

#
# filter: (objectClass=organizationalUnit)
#
# France, fenestros.com
dn: ou=France,dc=fenestros,dc=com
ou: France

# Commercial, France, fenestros.com
dn: ou=Commercial,ou=France,dc=fenestros,dc=com
ou: Commercial

# Recherche, France, fenestros.com
dn: ou=Recherche,ou=France,dc=fenestros,dc=com
ou: Recherche

# Production, France, fenestros.com
dn: ou=Production,ou=France,dc=fenestros,dc=com
ou: Production

# search result
search: 2
result: 0 Success

# numResponses: 5
# numEntries: 4

#
# filter: (objectClass=inetOrgPerson)
#
# mail, Commercial, France, fenestros.com
dn: cn=mail,ou=Commercial,ou=France,dc=fenestros,dc=com
```

```
cn: mail

# search result
search: 3
result: 0 Success

# numResponses: 2
# numEntries: 1

#
# filter: (objectClass=)
#
# search result
search: 4
result: 0 Success

# numResponses: 1
```

Saisissez les commandes ci-dessus et vérifiez que vous obtenez les mêmes résultats. Identifiez les options de la commande responsables pour chaque résultat spécifique.

La commande ldapmodify

Afin d'illustrer l'utilisation de la commande **ldapmodify**, créez une fichier **/tmp/prepa_modify.ldif** et éditez-le ainsi :

prepa_modify.ldif

```
dn: cn=dupond,ou=Recherche,ou=France,dc=fenestros,dc=com
objectClass: inetOrgPerson
objectClass: top
```

```
cn: dupond
sn: dupond
```

Saisissez ensuite la commande suivante :

```
[root@centos6 tmp]# ldapadd -f /tmp/prepa_modify.ldif -x -D "cn=Manager,dc=fenestros,dc=com" -W
Enter LDAP Password:
adding new entry "cn=dupond,ou=Recherche,ou=France,dc=fenestros,dc=com"
```

Notez l'utilisation de l'option **-W** qui permet de demander au serveur un prompt pour le mot de passe au lieu de l'écrire en clair dans la commande elle-même.

Visualisez votre DIT avec Luma. Vous constaterez un résultat similaire à celui-ci :

```
{{redhat:lx08:luma18.png|}}
```

La commande ldapmodify prend les options suivantes :

```
[root@centos6 ~]# ldapmodify --help
ldapmodify: invalid option -- '-'
ldapmodify: unrecognized option --
Add or modify entries from an LDAP server

usage: ldapmodify [options]
    The list of desired operations are read from stdin or from the file
    specified by "-f file".
Add or modify options:
  -a         add values (default is to replace)
  -c         continuous operation mode (do not stop on errors)
  -E [!]ext=extparam    modify extensions (! indicate s criticality)
```

```
  -f file    read operations from `file'
  -M         enable Manage DSA IT control (-MM to make critical)
  -P version protocol version (default: 3)
  -S file    write skipped modifications to `file'
Common options:
  -d level   set LDAP debugging level to `level'
  -D binddn  bind DN
  -e [!]<ext>[=<extparam>] general extensions (! indicates criticality)
             [!]assert=<filter>     (RFC 4528; a RFC 4515 Filter string)
             [!]authzid=<authzid>   (RFC 4370; "dn:<dn>" or "u:<user>")
             [!]chaining[=<resolveBehavior>[/<continuationBehavior>]]
                     one of "chainingPreferred", "chainingRequired",
                     "referralsPreferred", "referralsRequired"
             [!]manageDSAit         (RFC 3296)
             [!]noop
             ppolicy
             [!]postread[=<attrs>]  (RFC 4527; comma-separated attr list)
             [!]preread[=<attrs>]   (RFC 4527; comma-separated attr list)
             [!]relax
             abandon, cancel, ignore (SIGINT sends abandon/cancel,
             or ignores response; if critical, doesn't wait for SIGINT.
             not really controls)
  -h host    LDAP server
  -H URI     LDAP Uniform Resource Identifier(s)
  -I         use SASL Interactive mode
  -n         show what would be done but don't actually do it
  -N         do not use reverse DNS to canonicalize SASL host name
  -O props   SASL security properties
  -o <opt>[=<optparam] general options
             nettimeout=<timeout> (in seconds, or "none" or "max")
  -p port    port on LDAP server
  -Q         use SASL Quiet mode
  -R realm   SASL realm
  -U authcid SASL authentication identity
```

```
  -v         run in verbose mode (diagnostics to standard output)
  -V         print version info (-VV only)
  -w passwd  bind password (for simple authentication)
  -W         prompt for bind password
  -x         Simple authentication
  -X authzid SASL authorization identity ("dn:<dn>" or "u:<user>")
  -y file    Read password from file
  -Y mech    SASL mechanism
  -Z         Start TLS request (-ZZ to require successful response)
```

Nous allons maintenant utiliser la commande ldapmodify pour ajouter une adresse email à l'entrée **Dupond**. Créez donc le fichier **/tmp/modify.ldif** et éditez-le ainsi :

modify.ldif

```
dn: cn=dupond,ou=Recherche,ou=France,dc=fenestros,dc=com
changetype: modify
add: mail
mail: dupond@fenestros.com
```

Saisissez maintenant la commande suivante :

```
[root@centos6 tmp]# ldapmodify -f /tmp/modify.ldif -x -D "cn=Manager,dc=fenestros,dc=com" -W
Enter LDAP Password:
modifying entry "cn=dupond,ou=Recherche,ou=France,dc=fenestros,dc=com"
```

Visualisez votre DIT avec Luma. Vous constaterez un résultat similaire à celui-ci :

```
{{redhat:lx08:luma19.png|}}
```

La commande ldapdelete

Comme vous pouvez constater, vous avez deux entrées dans **ou=Recherche,ou=France,dc=fenestros,dc=com** :

- dupond
- dupont

Nous souhaitons maintenant supprimer l'entrée **dupont** en utilisant la commande **ldapdelete**. Les options de ldapdelete sont :

```
[root@centos6 ~]# ldapdelete --help
ldapdelete: invalid option -- '-'
ldapdelete: unrecognized option --
Delete entries from an LDAP server

usage: ldapdelete [options] [dn]...
    dn: list of DNs to delete. If not given, it will be readed from stdin
        or from the file specified with "-f file".
Delete Options:
  -c         continuous operation mode (do not stop on errors)
  -f file    read operations from `file'
  -M         enable Manage DSA IT control (-MM to make critical)
  -P version protocol version (default: 3)
  -r         delete recursively
Common options:
  -d level   set LDAP debugging level to `level'
  -D binddn  bind DN
  -e [!]<ext>[=<extparam>] general extensions (! indicates criticality)
             [!]assert=<filter>     (RFC 4528; a RFC 4515 Filter string)
             [!]authzid=<authzid>   (RFC 4370; "dn:<dn>" or "u:<user>")
             [!]chaining[=<resolveBehavior>[/<continuationBehavior>]]
                    one of "chainingPreferred", "chainingRequired",
                    "referralsPreferred", "referralsRequired"
             [!]manageDSAit         (RFC 3296)
             [!]noop
```

```
            ppolicy
            [!]postread[=<attrs>]  (RFC 4527; comma-separated attr list)
            [!]preread[=<attrs>]   (RFC 4527; comma-separated attr list)
            [!]relax
            abandon, cancel, ignore (SIGINT sends abandon/cancel,
            or ignores response; if critical, doesn't wait for SIGINT.
            not really controls)
  -h host    LDAP server
  -H URI     LDAP Uniform Resource Identifier(s)
  -I         use SASL Interactive mode
  -n         show what would be done but don't actually do it
  -N         do not use reverse DNS to canonicalize SASL host name
  -O props   SASL security properties
  -o <opt>[=<optparam] general options
            nettimeout=<timeout> (in seconds, or "none" or "max")
  -p port    port on LDAP server
  -Q         use SASL Quiet mode
  -R realm   SASL realm
  -U authcid SASL authentication identity
  -v         run in verbose mode (diagnostics to standard output)
  -V         print version info (-VV only)
  -w passwd  bind password (for simple authentication)
  -W         prompt for bind password
  -x         Simple authentication
  -X authzid SASL authorization identity ("dn:<dn>" or "u:<user>")
  -y file    Read password from file
  -Y mech    SASL mechanism
  -Z         Start TLS request (-ZZ to require successful response)
```

Saisissez donc la commande suivante :

```
[root@centos6 tmp]# ldapdelete -x -D "cn=Manager,dc=fenestros,dc=com" -W
"cn=dupont,ou=Recherche,ou=France,dc=fenestros,dc=com"
```

```
Enter LDAP Password:
```

Notez l'absence d'une confirmation de la suppression.

Déconnectez-vous et reconnectez-vous avec Luma. Vous constaterez un résultat similaire à celui-ci :

```
{{redhat:lx08:luma20.png|}}
```

Supprimer maintenant le referral mis en place tout à l'heure :

```
[root@centos6 tmp]# ldapdelete -x -M -D "cn=Manager,dc=fenestros,dc=com" -W "ou=Informatique,dc=fenestros,dc=com"
Enter LDAP Password:
```

A quoi sert l'option **-M** ?

Création d'une base de données hors ligne

La commande slapadd

Jusqu'à maintenant nous avons apporter des modifications à la base LDAP **en ligne**, autrement dit pendant que le serveur était en cours de fonctionnement. Il est aussi possible d'apporter des modifications quand le serveur est arrêté. Pour faire ceci, on dispose de la commande **slapadd**. Les options de la commande slapadd sont :

```
[root@centos6 ~]# slapadd --help
slapadd: invalid option -- '-'
usage: slapadd [-v] [-d debuglevel] [-f configfile] [-F configdir] [-o <name>[=<value>]] [-c]
```

```
    [-g] [-n databasenumber | -b suffix]
    [-l ldiffile] [-j linenumber] [-q] [-u] [-s] [-w]
```

Créez d'abord le fichier LDIF **/tmp/slapadd.ldif** et éditez-le ainsi :

```
dn: cn=dupois,ou=Production,ou=France,dc=fenestros,dc=com
objectClass: inetOrgPerson
objectClass: top
cn: dupois
sn: dupois
```

Arrêtez maintenant le service slapd :

```
[root@centos6 tmp]# service slapd stop
Arrêt de slapd :                                           [  OK  ]
```

Saisissez maintenant la commande suivante :

```
[root@centos6 tmp]# slapadd -b "dc=fenestros,dc=com" -l /tmp/slapadd.ldif
_################### 100.00% eta   none elapsed            none fast!
Closing DB...
```

Démarrez le service slapd :

```
[root@centos6 openldap]# service slapd start
Démarrage de slapd :                                       [  OK  ]
```

Reconnectez-vous avec Luma. Vous constaterez un résultat similaire à celui-ci :

```
{{redhat:lx08:luma21.png|}}
```

Maintenance d’une base de données LDAP

La commande slapcat

La commande **slapcat** produit un fichier LDIF à partir d'une base de données slapd.

L'exportation ne produit **pas** un fichier hiérarchique. Pour cette raison, le fichier peut être utilisé par la commande **slapadd** mais ne peut **pas** être utilisé par la commande **ldapadd**.

Les options de cette commande sont :

```
usage: slapcat [-v] [-d debuglevel] [-f configfile] [-F configdir] [-c]
        [-g] [-n databasenumber | -b suffix] [-l ldiffile] [-a filter]
```

Saisissez donc les commandes suivantes :

```
[root@centos6 tmp]# service slapd stop
Arrêt de slapd :                                           [  OK  ]
[root@centos6 tmp]# slapcat -b "dc=fenestros,dc=com" -l /tmp/backup.ldif
[root@centos6 tmp]# cat /tmp/backup.ldif
dn: dc=fenestros,dc=com
objectClass: dcObject
objectClass: organization
dc: fenestros
o: fenestros.com
description: Exemple
structuralObjectClass: organization
entryUUID: b5efc0fc-6cb1-1033-9919-a55157702d31
creatorsName: cn=Manager,dc=fenestros,dc=com
createTimestamp: 20140510171020Z
entryCSN: 20140510171020.464320Z#000000#000#000000
modifiersName: cn=Manager,dc=fenestros,dc=com
modifyTimestamp: 20140510171020Z
```

```
dn: cn=Manager,dc=fenestros,dc=com
objectClass: organizationalRole
cn: Manager
description: Gestionnaire
structuralObjectClass: organizationalRole
entryUUID: b5f1ed32-6cb1-1033-991a-a55157702d31
creatorsName: cn=Manager,dc=fenestros,dc=com
createTimestamp: 20140510171020Z
entryCSN: 20140510171020.478560Z#000000#000#000000
modifiersName: cn=Manager,dc=fenestros,dc=com
modifyTimestamp: 20140510171020Z

dn: ou=France,dc=fenestros,dc=com
objectClass: organizationalUnit
objectClass: top
ou: France
structuralObjectClass: organizationalUnit
entryUUID: da8700c4-6cb1-1033-991b-a55157702d31
creatorsName: cn=Manager,dc=fenestros,dc=com
createTimestamp: 20140510171121Z
entryCSN: 20140510171121.853517Z#000000#000#000000
modifiersName: cn=Manager,dc=fenestros,dc=com
modifyTimestamp: 20140510171121Z

dn: ou=Commercial,ou=France,dc=fenestros,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Commercial
structuralObjectClass: organizationalUnit
entryUUID: da8922c8-6cb1-1033-991c-a55157702d31
creatorsName: cn=Manager,dc=fenestros,dc=com
createTimestamp: 20140510171121Z
entryCSN: 20140510171121.867502Z#000000#000#000000
modifiersName: cn=Manager,dc=fenestros,dc=com
```

```
modifyTimestamp: 20140510171121Z

dn: ou=Recherche,ou=France,dc=fenestros,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Recherche
structuralObjectClass: organizationalUnit
entryUUID: da8a274a-6cb1-1033-991d-a55157702d31
creatorsName: cn=Manager,dc=fenestros,dc=com
createTimestamp: 20140510171121Z
entryCSN: 20140510171121.874173Z#000000#000#000000
modifiersName: cn=Manager,dc=fenestros,dc=com
modifyTimestamp: 20140510171121Z

dn: ou=Production,ou=France,dc=fenestros,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Production
structuralObjectClass: organizationalUnit
entryUUID: da8a8c4e-6cb1-1033-991e-a55157702d31
creatorsName: cn=Manager,dc=fenestros,dc=com
createTimestamp: 20140510171121Z
entryCSN: 20140510171121.876759Z#000000#000#000000
modifiersName: cn=Manager,dc=fenestros,dc=com
modifyTimestamp: 20140510171121Z

dn: ou=Suisse,dc=fenestros,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Suisse
structuralObjectClass: organizationalUnit
entryUUID: da8aea5e-6cb1-1033-991f-a55157702d31
creatorsName: cn=Manager,dc=fenestros,dc=com
createTimestamp: 20140510171121Z
```

```
entryCSN: 20140510171121.879166Z#000000#000#000000
modifiersName: cn=Manager,dc=fenestros,dc=com
modifyTimestamp: 20140510171121Z

dn: ou=Commercial,ou=Suisse,dc=fenestros,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Commercial
structuralObjectClass: organizationalUnit
entryUUID: da8bf9e4-6cb1-1033-9920-a55157702d31
creatorsName: cn=Manager,dc=fenestros,dc=com
createTimestamp: 20140510171121Z
entryCSN: 20140510171121.886122Z#000000#000#000000
modifiersName: cn=Manager,dc=fenestros,dc=com
modifyTimestamp: 20140510171121Z

dn: ou=USA,dc=fenestros,dc=com
objectClass: organizationalUnit
objectClass: top
ou: USA
structuralObjectClass: organizationalUnit
entryUUID: da8c8a62-6cb1-1033-9921-a55157702d31
creatorsName: cn=Manager,dc=fenestros,dc=com
createTimestamp: 20140510171121Z
entryCSN: 20140510171121.889815Z#000000#000#000000
modifiersName: cn=Manager,dc=fenestros,dc=com
modifyTimestamp: 20140510171121Z

dn: ou=Commercial,ou=USA,dc=fenestros,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Commercial
structuralObjectClass: organizationalUnit
entryUUID: da8cb4d8-6cb1-1033-9922-a55157702d31
```

```
creatorsName: cn=Manager,dc=fenestros,dc=com
createTimestamp: 20140510171121Z
entryCSN: 20140510171121.890904Z#000000#000#000000
modifiersName: cn=Manager,dc=fenestros,dc=com
modifyTimestamp: 20140510171121Z

dn: ou=Recherche,ou=USA,dc=fenestros,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Recherche
structuralObjectClass: organizationalUnit
entryUUID: da8d09d8-6cb1-1033-9923-a55157702d31
creatorsName: cn=Manager,dc=fenestros,dc=com
createTimestamp: 20140510171121Z
entryCSN: 20140510171121.893079Z#000000#000#000000
modifiersName: cn=Manager,dc=fenestros,dc=com
modifyTimestamp: 20140510171121Z

dn: cn=Responsable Personnel,ou=France,dc=fenestros,dc=com
cn: Responsable Personnel
aliasedObjectName: cn=Directeur,ou=France,dc=fenestros,dc=com
objectClass: top
objectClass: alias
objectClass: extensibleObject
structuralObjectClass: alias
entryUUID: f1819abc-6cb3-1033-9f7e-57ef2f3fd768
creatorsName: cn=Manager,dc=fenestros,dc=com
createTimestamp: 20140510172619Z
entryCSN: 20140510172619.399206Z#000000#000#000000
modifiersName: cn=Manager,dc=fenestros,dc=com
modifyTimestamp: 20140510172619Z

dn: cn=directeur,ou=France,dc=fenestros,dc=com
objectClass: person
```

```
objectClass: top
cn: directeur
sn: Guillaud
telephoneNumber: 12345678
telephoneNumber: 87654321
structuralObjectClass: person
entryUUID: 281f1928-6cb4-1033-9f7f-57ef2f3fd768
creatorsName: cn=Manager,dc=fenestros,dc=com
createTimestamp: 20140510172751Z
entryCSN: 20140510172751.028311Z#000000#000#000000
modifiersName: cn=Manager,dc=fenestros,dc=com
modifyTimestamp: 20140510172751Z

dn: ou=Angleterre,dc=fenestros,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Angleterre
structuralObjectClass: organizationalUnit
entryUUID: 5451fd26-6cb4-1033-9f80-57ef2f3fd768
creatorsName: cn=Manager,dc=fenestros,dc=com
createTimestamp: 20140510172905Z
entryCSN: 20140510172905.181577Z#000000#000#000000
modifiersName: cn=Manager,dc=fenestros,dc=com
modifyTimestamp: 20140510172905Z

dn: ou=Sales,ou=Angleterre,dc=fenestros,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Sales
structuralObjectClass: organizationalUnit
entryUUID: 5452e1aa-6cb4-1033-9f81-57ef2f3fd768
creatorsName: cn=Manager,dc=fenestros,dc=com
createTimestamp: 20140510172905Z
entryCSN: 20140510172905.187435Z#000000#000#000000
```

```
modifiersName: cn=Manager,dc=fenestros,dc=com
modifyTimestamp: 20140510172905Z

dn: cn=Sales Director,ou=Sales,ou=Angleterre,dc=fenestros,dc=com
objectClass: person
objectClass: top
cn: Sales Director
sn: Smith
structuralObjectClass: person
entryUUID: 545637b0-6cb4-1033-9f82-57ef2f3fd768
creatorsName: cn=Manager,dc=fenestros,dc=com
createTimestamp: 20140510172905Z
entryCSN: 20140510172905.209285Z#000000#000#000000
modifiersName: cn=Manager,dc=fenestros,dc=com
modifyTimestamp: 20140510172905Z

dn: cn=Sales Manager,cn=Sales Director,ou=Sales,ou=Angleterre,dc=fenestros,dc=
 loc
objectClass: person
objectClass: top
cn: Sales Manager
sn: Brown
structuralObjectClass: person
entryUUID: 5457078a-6cb4-1033-9f83-57ef2f3fd768
creatorsName: cn=Manager,dc=fenestros,dc=com
createTimestamp: 20140510172905Z
entryCSN: 20140510172905.214614Z#000000#000#000000
modifiersName: cn=Manager,dc=fenestros,dc=com
modifyTimestamp: 20140510172905Z

dn: cn=mail,ou=Commercial,ou=France,dc=fenestros,dc=com
objectClass: inetOrgPerson
objectClass: person
objectClass: top
```

```
cn: mail
mail: info@fenestros.com
sn: info
structuralObjectClass: inetOrgPerson
entryUUID: 9da96d6e-6cb5-1033-9f85-57ef2f3fd768
creatorsName: cn=Manager,dc=fenestros,dc=com
createTimestamp: 20140510173817Z
entryCSN: 20140510173817.725029Z#000000#000#000000
modifiersName: cn=Manager,dc=fenestros,dc=com
modifyTimestamp: 20140510173817Z

dn: cn=dupond,ou=Recherche,ou=France,dc=fenestros,dc=com
objectClass: inetOrgPerson
objectClass: top
cn: dupond
sn: dupond
structuralObjectClass: inetOrgPerson
entryUUID: 6d6481be-6cb7-1033-9f87-57ef2f3fd768
creatorsName: cn=Manager,dc=fenestros,dc=com
createTimestamp: 20140510175115Z
mail: dupond@fenestros.com
entryCSN: 20140510175239.535515Z#000000#000#000000
modifiersName: cn=Manager,dc=fenestros,dc=com
modifyTimestamp: 20140510175239Z

dn: cn=dupois,ou=Production,ou=France,dc=fenestros,dc=com
objectClass: inetOrgPerson
objectClass: top
cn: dupois
sn: dupois
structuralObjectClass: inetOrgPerson
entryUUID: fb863992-6cb7-1033-9885-d3c28e994865
creatorsName: cn=Manager,dc=fenestros,dc=com
createTimestamp: 20140510175514Z
```

```
entryCSN: 20140510175514.193596Z#000000#000#000000
modifiersName: cn=Manager,dc=fenestros,dc=com
modifyTimestamp: 20140510175514Z
```

La commande slapindex

La commande **slapindex** crée ou met à jour les index définis pour une base de données slapd.

Les options de cette commande sont :

```
usage: slapindex [-v] [-d debuglevel] [-f configfile] [-F configdir] [-c]
        [-g] [-n databasenumber | -b suffix] [-q]
```

Saisissez donc la commande suivante :

```
[root@centos6 tmp]# slapindex -b "dc=fenestros,dc=com" -v
indexing id=00000001
indexing id=00000002
indexing id=00000003
indexing id=00000004
indexing id=00000005
indexing id=00000006
indexing id=00000007
indexing id=00000008
indexing id=00000009
indexing id=0000000a
indexing id=0000000b
indexing id=0000000c
indexing id=0000000d
indexing id=0000000e
indexing id=0000000f
indexing id=00000010
indexing id=00000011
```

```
indexing id=00000013
indexing id=00000015
indexing id=00000016
```

La commande slapdn

La commande **slapdn** vérifie la cohérence d'une entrée spécifiée par rapport au(x) schéma(s) défini(s) pour slapd.

Les options de cette commande sont :

```
usage: slapdn [-v] [-d debuglevel] [-f configfile] [-F configdir]
        [-N | -P] DN [...]
```

Saisissez donc la commande suivante :

```
[root@centos6 tmp]# slapdn cn=smith,dc=fenestros,dc=com
DN: <cn=smith,dc=fenestros,dc=com> check succeeded
normalized: <cn=smith,dc=fenestros,dc=com>
pretty:     <cn=smith,dc=fenestros,dc=com>
```

Saisissez maintenant la commande suivante :

```
[root@centos6 tmp]# slapdn nom=smith,dc=fenestros,dc=com
DN: <nom=smith,dc=fenestros,dc=com> check failed 21 (Invalid syntax)
```

La commande slaptest

La commande **slaptest** vérifie la syntaxe des fichiers de configuration de slapd.

Les options de cette commande sont :

```
usage: slaptest [-v] [-d debuglevel] [-f configfile] [-F configdir] [-u]
```

Saisissez donc la commande suivante :

```
[root@centos6 tmp]# slaptest -u
config file testing succeeded
```

La commande slapauth

La commande **slapauth** vérifie la correspondance entre les ID et les DN en fonction des directives **authz** et **authc** du fichier de configuration slapd.conf.

Les options de cette commande sont :

```
usage: slapauth [-v] [-d debuglevel] [-f configfile] [-F configdir]
        [-U authcID] [-X authzID] [-R realm] [-M mech] ID [...]
```

Saisissez donc la commande suivante :

```
[root@centos6 tmp]# slapauth -v U smith X u :smith
ID: <U> check succeeded
authcID:     <uid=u,cn=auth>
ID: <smith> check succeeded
authcID:     <uid=smith,cn=auth>
ID: <X> check succeeded
authcID:     <uid=x,cn=auth>
ID: <u> check succeeded
authcID:     <uid=u,cn=auth>
ID: <:smith> check succeeded
authcID:     <uid=:smith,cn=auth>
```

Démarrez slapd :

```
[root@centos6 tmp]# service slapd start
Démarrage de slapd :                                       [  OK  ]
```

LAB #1 - Replication de Serveurs OpenLDAP

Afin d'assurer la répartition de la charge sur plusieurs serveurs, OpenLDAP est capable de mettre en œuvre de ce que l'on appelle la réplication.

Préparation

Créez deux clônes à partir de votre machine virtuelle.

La première doit s'appeler **ldap1.fenestros.com** et la deuxième **ldap2.fenestros.com**.

Chaque VM doit avoir une adresse IP fixe. Par exemple :

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=none
NETMASK=255.255.255.0
IPADDR=10.0.2.15
USERCTL=no
PEERDNS=yes
GATEWAY=10.0.2.2
TYPE=Ethernet
IPV6INIT=no
```

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=none
NETMASK=255.255.255.0
IPADDR=10.0.2.16
```

```
USERCTL=no
PEERDNS=yes
GATEWAY=10.0.2.2
TYPE=Ethernet
IPV6INIT=no
```

Dans le fichier **/etc/hosts** de **chaque** VM ajoutez les adresses IP et noms de machines :

```
10.0.2.15      ldap1.fenestros.com
10.0.2.16      ldap2.fenestros.com
```

Replication

Le mécanisme de réplication **syncrepl** est basé sur l'architecture de **serveurs homologues**. Le serveur dit *consommateur* lance le démon **syncrepl** dans un thread. Ce dernier contact le serveur fournisseur et charge une première version de l'annuaire. Ensuite il se maintient à jour.

Configuration du serveur fournisseur

La configuration du serveur fournisseur se fait dans le fichier slapd.conf. L'exemple suivant démontre l'essentiel des directives à utiliser :

```
moduleload syncprov.la
overlay syncprov
syncprov-checkpoint 100 10
```

Directive	**Description**
moduleload	Sert à charger le module syncprov.
overlay	Appel du module syncprov.
syncprov-checkpoint	Un checkpoint est créé après chaque 100 modifications ou 10 minutes.

Configuration du serveur consommateur

La configuration du serveur consommateur se fait dans le fichier slapd.conf. L'exemple suivant démontre les directives à utiliser :

```
syncrepl rid=123
    provider=ldap://10.0.2.15:389
    type=refreshAndPersist
    interval=00:00:00:10
    retry="5 10 60 +"
    searchbase="dc=fenestros,dc=com"
    bindmethod=simple
    binddn="cn=Manager,dc=fenestros,dc=com"
    credentials=fenestros
updateref ldap://10.0.2.15
```

Directive	Description
rid	L'identifiant unique du consommateur.
provider	Le serveur à répliquer.
type	Deux modes sont possibles : le mode “refreshOnly” ou le consommateur initie une connexion à intervalle régulier avec le fournisseur. Toutes les modifications survenues depuis la dernière connexion sont répliquées sur le serveur consommateur. Le mode “refreshAndPersist” ou le consommateur initie une connexion avec le fournisseur pour la première synchronisation, puis garde la connexion ouverte de sorte que toute modification intervenant sur le fournisseur soit immédiatement répliquée sur le consommateur.
interval	Définition de l’interval de réplication au format “jj:hh:mm:ss”
retry	Définition du comportement à adopter en cas d’erreur de synchronisation. Ici, l’esclave tentera de ce reconnecter au maitre toutes les 5 secondes les 10 premières tentatives, ensuite il ré essayera toutes les 60 secondes indéfiniment (“+”). En remplacent le “+” par une valeur “N”, le consumer effectuera “N” tentative espacées de 60 secondes.
searchbase	Définition de la branche à répliquer.
bindmethod	Type d’authentification (simple ou sasl).
binddn	Définition de l’utilisateur effectuant la réplication.
credentials	Mot de passe associé avec le binddn.

Mise en place

La mise en place comporte plusieurs phases :

- Relancez slapd sur le fournisseur,
- Démarrage slapd sur le consommateur,
- Modification d'une donnée,
- Vérification de la réplication.

LAB #2 - Authentification Apache en utilisant OpenLDAP

Arrêtez le serveur slapd :

```
[root@centos6 ~]# service slapd stop
Arrêt de slapd :                                           [  OK  ]
```

Créez le répertoire **/var/lib/ldap/fenestros** pour contenir un nouveau base de données :

```
[root@centos6 ~]# mkdir /var/lib/ldap/fenestros
```

Nettoyez les anciens fichiers de configuration et fichiers de données :

```
[root@centos6 ~]# rm -Rf /etc/openldap/slapd.d/*
[root@centos6 ~]# rm -f /var/lib/ldap/alock
[root@centos6 ~]# rm -f /var/lib/ldap/__db.00?
```

Créez le fichier **/etc/openldap/slapd.conf** :

```
[root@centos6 ~]# touch /etc/openldap/slapd.conf
```

Editez le fichier **/etc/openldap/slapd.conf** ainsi :

/etc/openldap/slapd.conf

```
include     /etc/openldap/schema/corba.schema
include     /etc/openldap/schema/core.schema
include     /etc/openldap/schema/cosine.schema
include     /etc/openldap/schema/duaconf.schema
include     /etc/openldap/schema/dyngroup.schema
include     /etc/openldap/schema/inetorgperson.schema
include     /etc/openldap/schema/java.schema
include     /etc/openldap/schema/misc.schema
include     /etc/openldap/schema/nis.schema
include     /etc/openldap/schema/openldap.schema
include     /etc/openldap/schema/ppolicy.schema
include     /etc/openldap/schema/collective.schema

allow bind_v2

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

TLSCACertificatePath /etc/openldap/certs
TLSCertificateFile "\"OpenLDAP Server\""
TLSCertificateKeyFile /etc/openldap/certs/password

database config
access to *
    by dn.exact="gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth" manage
    by * none

database monitor
access to *
    by dn.exact="gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth" read
        by dn.exact="cn=Admin,o=fenestros" read
        by * none
```

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

database    bdb
suffix      "o=fenestros"
checkpoint      1024 15
rootdn      "cn=Admin,o=fenestros"
rootpw
directory   /var/lib/ldap/fenestros
lastmod         on
index           cn,sn,st        eq,pres,sub
```

Créez un mot de passe crypté pour l'admistrateur LDAP :

```
[root@centos6 ~]# slappasswd -s fenestros
{SSHA}C7ieZyzD/uvgaIOca3iukkwYUfl3TRB2
```

Editez ensuite la section **database** du fichier **/etc/openldap/slapd.conf** :

```
...
database        bdb
suffix          "o=fenestros"
checkpoint      1024 15
rootdn          "cn=Admin,o=fenestros"
rootpw          {SSHA}C7ieZyzD/uvgaIOca3iukkwYUfl3TRB2
directory       /var/lib/ldap/fenestros
lastmod         on
index           cn,sn,st                eq,pres,sub
```

Initialisez la première base de données :

```
[root@centos6 ~]# echo “” | slapadd -f /etc/openldap/slapd.conf
The first database does not allow slapadd; using the first available one (2)
```

```
str2entry: entry -1 has no dn
slapadd: could not parse entry (line=1)
```

Initialisez ensuite l'arborescence dans **/etc/openldap/slapd.d** :

```
[root@centos6 ~]# slaptest -f /etc/openldap/slapd.conf -F /etc/openldap/slapd.d
config file testing succeeded
```

Vérifiez que l'arborescence initiale soit créée :

```
[root@centos6 ~]# ls -l /etc/openldap/slapd.d
total 8
drwxr-x---. 3 root root 4096  8 sept. 18:25 cn=config
-rw-------. 1 root root 1127  8 sept. 18:25 cn=config.ldif
```

Modifiez le propriétaire, le groupe ainsi que le droits du répertoire **/etc/openldap/slapd.d** :

```
[root@centos6 ~]# chown -R ldap:ldap /etc/openldap/slapd.d
[root@centos6 ~]# chmod -R u+rwX /etc/openldap/slapd.d
```

Modifiez le propriétaire et le groupe répertoire **/var/lib/ldap/fenestros** ainsi que le fichier **/etc/openldap/slapd.conf** :

```
[root@centos6 ~]# chown -R ldap:ldap /var/lib/ldap/fenestros /etc/openldap/slapd.conf
```

Copiez le fichier /usr/share/openldap-servers/DB_CONFIG.example vers **/var/lib/ldap/DB_CONFIG** :

```
[root@centos6 ~]# cp /usr/share/openldap-servers/DB_CONFIG.example /var/lib/ldap/fenestros/DB_CONFIG
```

Démarrez ensuite le service slapd :

```
[root@centos6 ~]# service slapd start
Démarrage de slapd :                                       [  OK  ]
```

Créez le fichier **fenestros.ldif** :

```
dn: o=fenestros
objectClass: top
objectClass: organization
o: fenestros
description: LDAP Authentification

dn: cn=Admin,o=fenestros
objectClass: organizationalRole
cn: Admin
description: Administrateur LDAP

dn: ou=GroupA,o=fenestros
ou: GroupA
objectClass: top
objectClass: organizationalUnit
description: Membres de GroupA

dn: ou=GroupB,o=fenestros
ou: GroupB
objectClass: top
objectClass: organizationalUnit
description: Membres de GroupB

dn: ou=group,o=fenestros
ou: group
objectclass: organizationalUnit
objectclass: domainRelatedObject
associatedDomain: fenestros

dn: cn=users,ou=group,o=fenestros
cn: users
objectClass: top
```

```
objectClass: posixGroup
gidNumber: 100
memberUid: jean
memberUid: jacques

dn: cn=Jean Legrand,ou=GroupA,o=fenestros
ou: GroupA
o: fenestros
cn: Jean Legrand
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
objectClass: top
mail: jean.legrand@fenestros.com
givenname: Jean
sn: Legrand
uid: jean
uidNumber: 1001
gidNumber: 100
gecos: Jean Legrand
loginShell: /bin/bash
homeDirectory: /home/jean
shadowLastChange: 14368
shadowMin: 0
shadowMax: 999999
shadowWarning: 7
userPassword: secret1
homePostalAddress: 99 avenue de Linux, 75000 Paris
postalAddress: 99 avenue de Linux.
l: Paris
st: 75
postalcode: 75000
```

```
telephoneNumber: 01.10.20.30.40
homePhone: 01.50.60.70.80
facsimileTelephoneNumber: 01.99.99.99.99
title: Ingénieur

dn: cn=Jacques Lebeau,ou=GroupA,o=fenestros
ou: GroupA
o: fenestros
cn: Jacques Lebeau
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
objectClass: top
mail: jacques.lebeau@fenestros.com
givenname: Jacques
sn: Lebeau
uid: jacques
uidNumber: 1002
gidNumber: 100
gecos: Jacques Lebeau
loginShell: /bin/bash
homeDirectory: /home/jacques
shadowLastChange: 14365
shadowMin: 0
shadowMax: 999999
shadowWarning: 7
userPassword: secret2
initials: JL
homePostalAddress: 99 route d'Unix, 75000 Paris
postalAddress: 99 route d'Unix.
l: Paris
st: 75
```

```
postalcode: 75000
pager: 01.04.04.04.04
homePhone: 01.05.05.05.05
telephoneNumber: 01.06.06.06.06
mobile: 06.01.02.03.04
title: Technicienne
facsimileTelephoneNumber: 01.04.09.09.09
manager: cn=Jean Legrand,ou=GroupA,o=fenestros
```

Injectez le fichier fenestros.ldif dans OpenLDAP :

```
[root@centos6 ~]# ldapadd -f fenestros.ldif -xv -D "cn=Admin,o=fenestros" -h 127.0.0.1 -w fenestros
ldap_initialize( ldap://127.0.0.1 )
add objectClass:
    top
    organization
add o:
    fenestros
add description:
    LDAP Authentification
adding new entry "o=fenestros"
modify complete

add objectClass:
    organizationalRole
add cn:
    Admin
add description:
    Administrateur LDAP
adding new entry "cn=Admin,o=fenestros"
modify complete

add ou:
    GroupA
```

```
add objectClass:
    top
    organizationalUnit
add description:
    Membres de GroupA
adding new entry "ou=GroupA,o=fenestros"
modify complete

add ou:
    GroupB
add objectClass:
    top
    organizationalUnit
add description:
    Membres de GroupB
adding new entry "ou=GroupB,o=fenestros"
modify complete

add ou:
    group
add objectclass:
    organizationalUnit
    domainRelatedObject
add associatedDomain:
    fenestros
adding new entry "ou=group,o=fenestros"
modify complete

add cn:
    users
add objectClass:
    top
    posixGroup
add gidNumber:
```

```
    100
add memberUid:
    jean
    jacques
adding new entry "cn=users,ou=group,o=fenestros"
modify complete

add ou:
    GroupA
add o:
    fenestros
add cn:
    Jean Legrand
add objectClass:
    person
    organizationalPerson
    inetOrgPerson
    posixAccount
    shadowAccount
    top
add mail:
    jean.legrand@fenestros.com
add givenname:
    Jean
add sn:
    Legrand
add uid:
    jean
add uidNumber:
    1001
add gidNumber:
    100
add gecos:
    Jean Legrand
```

```
add loginShell:
    /bin/bash
add homeDirectory:
    /home/jean
add shadowLastChange:
    14368
add shadowMin:
    0
add shadowMax:
    999999
add shadowWarning:
    7
add userPassword:
    secret1
add homePostalAddress:
    99 avenue de Linux, 75000 Paris
add postalAddress:
    99 avenue de Linux.
add l:
    Paris
add st:
    75
add postalcode:
    75000
add telephoneNumber:
    01.10.20.30.40
add homePhone:
    01.50.60.70.80
add facsimileTelephoneNumber:
    01.99.99.99.99
add title:
    NOT ASCII (10 bytes)
adding new entry "cn=Jean Legrand,ou=GroupA,o=fenestros"
modify complete
```

```
add ou:
    GroupA
add o:
    fenestros
add cn:
    Jacques Lebeau
add objectClass:
    person
    organizationalPerson
    inetOrgPerson
    posixAccount
    shadowAccount
    top
add mail:
    jacques.lebeau@fenestros.com
add givenname:
    Jacques
add sn:
    Lebeau
add uid:
    jacques
add uidNumber:
    1002
add gidNumber:
    100
add gecos:
    Jacques Lebeau
add loginShell:
    /bin/bash
add homeDirectory:
    /home/jacques
add shadowLastChange:
    14365
add shadowMin:
```

```
    0
add shadowMax:
    999999
add shadowWarning:
    7
add userPassword:
    secret2
add initials:
    JL
add homePostalAddress:
    99 route d'Unix, 75000 Paris
add postalAddress:
    99 route d'Unix.
add l:
    Paris
add st:
    75
add postalcode:
    75000
add pager:
    01.04.04.04.04
add homePhone:
    01.05.05.05.05
add telephoneNumber:
    01.06.06.06.06
add mobile:
    06.01.02.03.04
add title:
    Technicienne
add facsimileTelephoneNumber:
    01.04.09.09.09
add manager:
    cn=Jean Legrand,ou=GroupA,o=fenestros
adding new entry "cn=Jacques Lebeau,ou=GroupA,o=fenestros"
```

```
modify complete
```

Arrêtez le serveur Apache :

```
[root@centos6 ~]# service httpd stop
Arrêt de httpd :                                           [  OK  ]
```

Editez la section **<Directory ”/var/www/html“>** du fichier **/etc/httpd/conf/httpd.conf** :

```
...
<Directory "/var/www/html">
   AuthType Basic
   AuthName "Bienvenue : Connectez-vous avec votre nom d'utilisateur"
   AuthBasicProvider ldap
   AuthzLDAPAuthoritative on
   AuthLDAPURL ldap://localhost:389/o=fenestros?uid?sub
   AuthLDAPBindDN "cn=Admin,o=fenestros"
   AuthLDAPBindPassword fenestros
   require ldap-user jean jacques
   AllowOverride None
   Options Indexes FollowSymLinks
</Directory>
...
```

Démarrez le serveur apache :

```
[root@centos6 ~]# service httpd start
Démarrage de httpd :                                       [  OK  ]
```

Connectez-vous à http://localhost en utilisant le compte de jean puis le compte de jacques.

<html>

</html>