

Dernière mise-à-jour : 2020/02/21 07:36

SER701 - Gestion du Serveur OpenLDAP sous CentOS 7

Présentation

Qu'est-ce que LDAP ?

LDAP est une abréviation de **Lightweight Directory Access Protocol**. 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'un service d'annuaire distribué est le **DNS**.

Plusieurs points sont à retenir :

- LDAP est un adaptation TCP/IP du protocole **DAP (Directory Access Protocol)**,
- 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 **Lightweight**,
- 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 **Basic Encoding Rule** 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 (Server Initiated Replication)**,
 - La réPLICATION **Esclave > Maître** appelée **pull-based** ou encore **CIR (Consumer Initiated Replication)**,

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: Authentication 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.

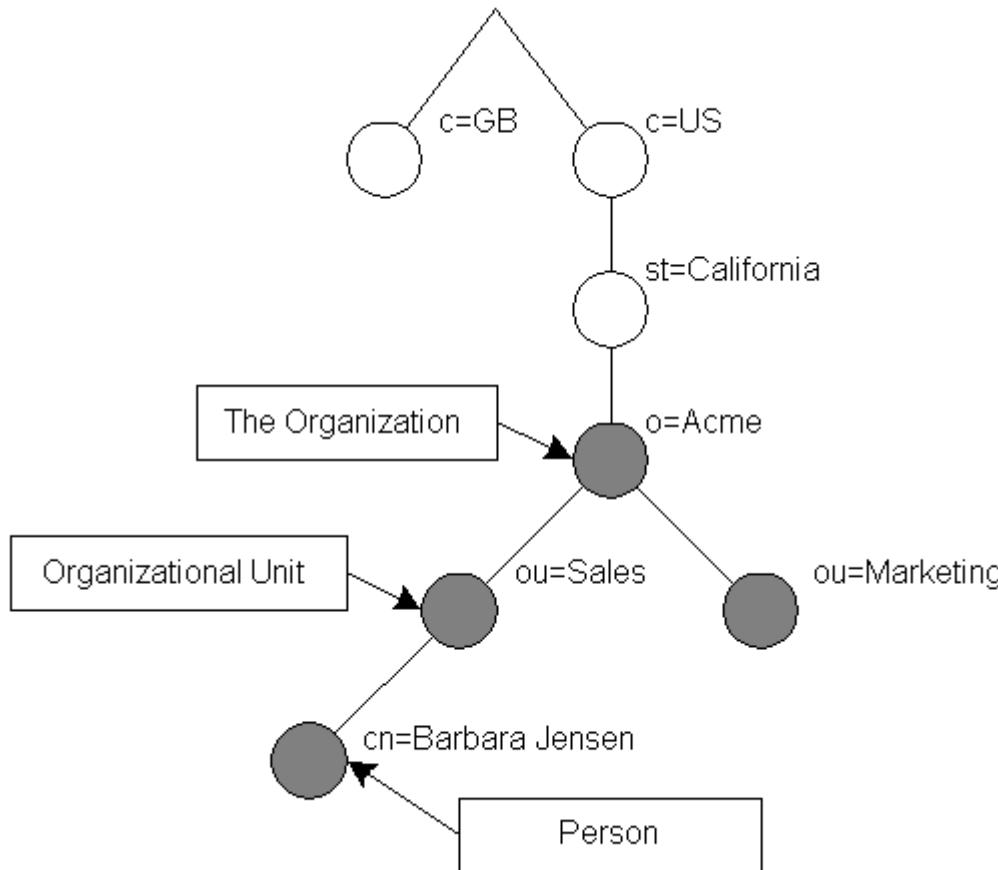
Le Modèle d'Information de LDAP

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

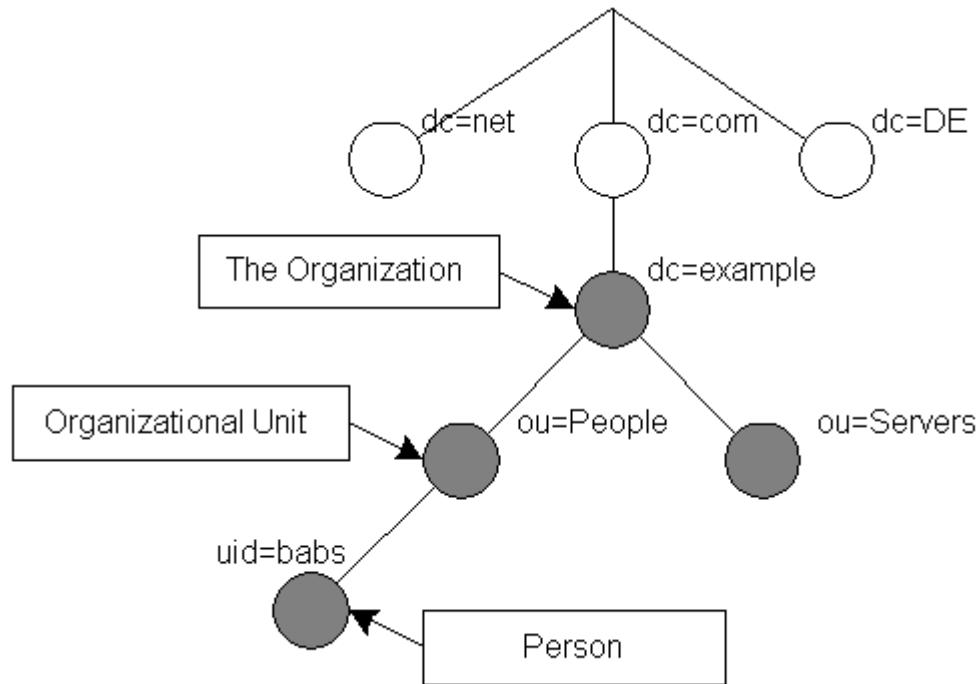
- L'ensemble des entrées est contenu dans un **DIT (Directory Information Tree)**,
- Chaque entrée représente une instance d'une **classe** d'objets contenant une collection d'**attributs** qui possède un nom unique appelé le **Distinguished Name** et un nom relatif appelé le **Relative Distinguished Name**.

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=i2tch,dc=com

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

- mail=info@i2tch.com

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

- mail=info@i2tch.com+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**bject **I**Dentifier) :

- Les OID sont attribués 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.schema	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 Broker Request Architecture).
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.

LAB #1 - Installation et Activation du serveur OpenLDAP sous CentOS 7

Avant d'installer OpenLDAP, passez SELinux en mode permissif :

```
[root@centos7 ~]# setenforce permissive
[root@centos7 ~]# vi /etc/sysconfig/selinux
[root@centos7 ~]# cat /etc/sysconfig/selinux

# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#       enforcing - SELinux security policy is enforced.
#       permissive - SELinux prints warnings instead of enforcing.
#       disabled - No SELinux policy is loaded.
SELINUX=permissive
# SELINUXTYPE= can take one of three two values:
#       targeted - Targeted processes are protected,
#       minimum - Modification of targeted policy. Only selected processes are protected.
#       mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

Ensuite désactivez le pare feu firewalld :

```
[root@centos7 ~]# systemctl stop firewalld
[root@centos7 ~]# systemctl disable firewalld
Removed symlink /etc/systemd/system/dbus-org.fedoraproject.FirewallD1.service.
Removed symlink /etc/systemd/system/basic.target.wants/firewalld.service.
[root@centos7 ~]# systemctl status firewalld
```

```
● firewalld.service - firewalld - dynamic firewall daemon
  Loaded: loaded (/usr/lib/systemd/system/firewalld.service; disabled; vendor preset: enabled)
  Active: inactive (dead)
    Docs: man:firewalld(1)
```

```
Jan 10 08:25:43 centos7.fenestros.loc systemd[1]: Starting firewalld - dynamic firewall daemon...
Jan 10 08:25:44 centos7.fenestros.loc systemd[1]: Started firewalld - dynamic firewall daemon.
Jan 10 12:15:48 centos7.fenestros.loc systemd[1]: Stopping firewalld - dynamic firewall daemon...
Jan 10 12:15:48 centos7.fenestros.loc systemd[1]: Stopped firewalld - dynamic firewall daemon.
```

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 :

```
[trainee@centos7 ~]$ su -
Mot de passe : fenestros
[root@centos7 ~]# yum update
...
[root@centos7 ~]# reboot
```

Puis installez OpenLDAP :

```
[root@centos7 ~]# yum install openldap-servers openldap-clients openldap
```

Sous RHEL / CentOS le service OpenLDAP s'appelle **slapd**. Une vérification de son état démontre qu'il n'est pas activé :

```
[root@centos7 ~]# systemctl status slapd
● slapd.service - OpenLDAP Server Daemon
  Loaded: loaded (/usr/lib/systemd/system/slapd.service; disabled; vendor preset: disabled)
  Active: inactive (dead)
    Docs: man:slapd
          man:slapd-config
          man:slapd-hdb
```

```
man:slapd-mdb  
file:///usr/share/doc/openldap-servers/guide.html
```

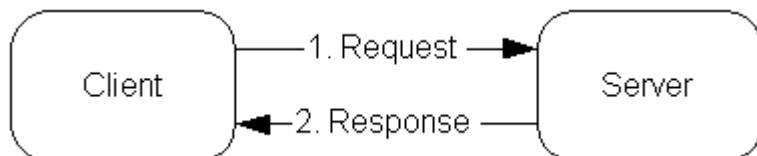
Il convient donc d'activer le service **sans** le démarrer :

```
[root@centos7 ~]# systemctl enable slapd  
Created symlink from /etc/systemd/system/multi-user.target.wants/slapd.service to  
/usr/lib/systemd/system/slapd.service.  
[root@centos7 ~]# systemctl status slapd  
● slapd.service - OpenLDAP Server Daemon  
  Loaded: loaded (/usr/lib/systemd/system/slapd.service; enabled; vendor preset: disabled)  
  Active: inactive (dead)  
    Docs: man:slapd  
          man:slapd-config  
          man:slapd-hdb  
          man:slapd-mdb  
          file:///usr/share/doc/openldap-servers/guide.html
```

Configuration d'un serveur OpenLDAP

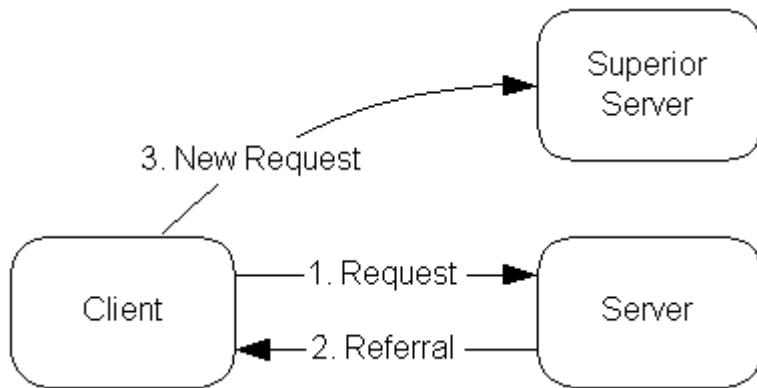
Le choix de la configuration de l'annuaire se fait en fonction de l'organisation de l'entité dont il détient l'information. Plusieurs configurations sont possibles.

L'annuaire Local



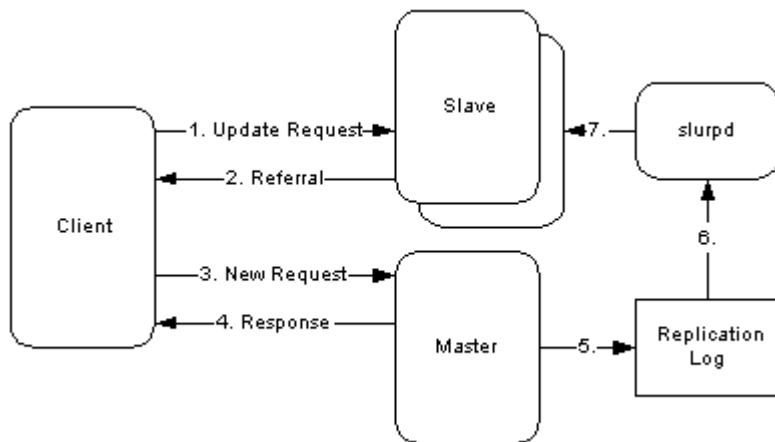
Dans ce cas, le service d'annuaire ne concerne que le domaine local. Il n'y a aucune interaction avec d'autres annuaires.

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.

Configuration des Versions Antérieures à la 2.3

La configuration d'OpenLDAP est effectuée en éditant le fichier **/etc/openldap/slapd.conf**. Un exemple de ce fichier est :

```
#  
# 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_ssfc=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
```

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@centos7 ~]# ls -l /usr/lib64/openldap
total 1320
lrwxrwxrwx. 1 root root    23 Jan  9 14:42 accesslog-2.4.so.2 -> accesslog-2.4.so.2.10.7
-rwxr-xr-x. 1 root root 49600 Jan 29 2019 accesslog-2.4.so.2.10.7
-rwxr-xr-x. 1 root root   1100 Jan 29 2019 accesslog.la
lrwxrwxrwx. 1 root root    19 Jan  9 14:42 allop-2.4.so.2 -> allop-2.4.so.2.10.7
-rwxr-xr-x. 1 root root 11056 Jan 29 2019 allop-2.4.so.2.10.7
-rwxr-xr-x. 1 root root   1076 Jan 29 2019 allop.la
lrwxrwxrwx. 1 root root    22 Jan  9 14:42 auditlog-2.4.so.2 -> auditlog-2.4.so.2.10.7
-rwxr-xr-x. 1 root root 11392 Jan 29 2019 auditlog-2.4.so.2.10.7
-rwxr-xr-x. 1 root root   1094 Jan 29 2019 auditlog.la
lrwxrwxrwx. 1 root root    25 Jan  9 14:42 back_dnssrv-2.4.so.2 -> back_dnssrv-2.4.so.2.10.7
-rwxr-xr-x. 1 root root 15256 Jan 29 2019 back_dnssrv-2.4.so.2.10.7
-rwxr-xr-x. 1 root root   1112 Jan 29 2019 back_dnssrv.la
lrwxrwxrwx. 1 root root    23 Jan  9 14:42 back_ldap-2.4.so.2 -> back_ldap-2.4.so.2.10.7
-rwxr-xr-x. 1 root root 161392 Jan 29 2019 back_ldap-2.4.so.2.10.7
-rwxr-xr-x. 1 root root   1100 Jan 29 2019 back_ldap.la
lrwxrwxrwx. 1 root root    23 Jan  9 14:42 back_meta-2.4.so.2 -> back_meta-2.4.so.2.10.7
-rwxr-xr-x. 1 root root 151016 Jan 29 2019 back_meta-2.4.so.2.10.7
-rwxr-xr-x. 1 root root   1100 Jan 29 2019 back_meta.la
lrwxrwxrwx. 1 root root    23 Jan  9 14:42 back_null-2.4.so.2 -> back_null-2.4.so.2.10.7
-rwxr-xr-x. 1 root root 15792 Jan 29 2019 back_null-2.4.so.2.10.7
-rwxr-xr-x. 1 root root   1100 Jan 29 2019 back_null.la
lrwxrwxrwx. 1 root root    25 Jan  9 14:42 back_passwd-2.4.so.2 -> back_passwd-2.4.so.2.10.7
-rwxr-xr-x. 1 root root 15528 Jan 29 2019 back_passwd-2.4.so.2.10.7
-rwxr-xr-x. 1 root root   1112 Jan 29 2019 back_passwd.la
lrwxrwxrwx. 1 root root    23 Jan  9 14:42 back_perl-2.4.so.2 -> back_perl-2.4.so.2.10.7
-rwxr-xr-x. 1 root root 28104 Jan 29 2019 back_perl-2.4.so.2.10.7
-rwxr-xr-x. 1 root root   1156 Jan 29 2019 back_perl.la
lrwxrwxrwx. 1 root root    24 Jan  9 14:42 back_relay-2.4.so.2 -> back_relay-2.4.so.2.10.7
-rwxr-xr-x. 1 root root 15568 Jan 29 2019 back_relay-2.4.so.2.10.7
```

```
-rwxr-xr-x. 1 root root 1106 Jan 29 2019 back_relay.la
lrwxrwxrwx. 1 root root 24 Jan 9 14:42 back_shell-2.4.so.2 -> back_shell-2.4.so.2.10.7
-rwxr-xr-x. 1 root root 24256 Jan 29 2019 back_shell-2.4.so.2.10.7
-rwxr-xr-x. 1 root root 1106 Jan 29 2019 back_shell.la
lrwxrwxrwx. 1 root root 23 Jan 9 14:42 back_sock-2.4.so.2 -> back_sock-2.4.so.2.10.7
-rwxr-xr-x. 1 root root 28736 Jan 29 2019 back_sock-2.4.so.2.10.7
-rwxr-xr-x. 1 root root 1100 Jan 29 2019 back_sock.la
lrwxrwxrwx. 1 root root 21 Jan 9 14:42 check_password.so -> check_password.so.1.1
-rwxr-xr-x. 1 root root 15752 Jan 29 2019 check_password.so.1.1
lrwxrwxrwx. 1 root root 21 Jan 9 14:42 collect-2.4.so.2 -> collect-2.4.so.2.10.7
-rwxr-xr-x. 1 root root 15504 Jan 29 2019 collect-2.4.so.2.10.7
-rwxr-xr-x. 1 root root 1088 Jan 29 2019 collect.la
lrwxrwxrwx. 1 root root 24 Jan 9 14:42 constraint-2.4.so.2 -> constraint-2.4.so.2.10.7
-rwxr-xr-x. 1 root root 27880 Jan 29 2019 constraint-2.4.so.2.10.7
-rwxr-xr-x. 1 root root 1106 Jan 29 2019 constraint.la
lrwxrwxrwx. 1 root root 17 Jan 9 14:42 dds-2.4.so.2 -> dds-2.4.so.2.10.7
-rwxr-xr-x. 1 root root 36560 Jan 29 2019 dds-2.4.so.2.10.7
-rwxr-xr-x. 1 root root 1064 Jan 29 2019 dds.la
lrwxrwxrwx. 1 root root 19 Jan 9 14:42 deref-2.4.so.2 -> deref-2.4.so.2.10.7
-rwxr-xr-x. 1 root root 15208 Jan 29 2019 deref-2.4.so.2.10.7
-rwxr-xr-x. 1 root root 1076 Jan 29 2019 deref.la
lrwxrwxrwx. 1 root root 22 Jan 9 14:42 dyngroup-2.4.so.2 -> dyngroup-2.4.so.2.10.7
-rwxr-xr-x. 1 root root 11392 Jan 29 2019 dyngroup-2.4.so.2.10.7
-rwxr-xr-x. 1 root root 1094 Jan 29 2019 dyngroup.la
lrwxrwxrwx. 1 root root 21 Jan 9 14:42 dynlist-2.4.so.2 -> dynlist-2.4.so.2.10.7
-rwxr-xr-x. 1 root root 32112 Jan 29 2019 dynlist-2.4.so.2.10.7
-rwxr-xr-x. 1 root root 1088 Jan 29 2019 dynlist.la
lrwxrwxrwx. 1 root root 22 Jan 9 14:42 memberof-2.4.so.2 -> memberof-2.4.so.2.10.7
-rwxr-xr-x. 1 root root 36640 Jan 29 2019 memberof-2.4.so.2.10.7
-rwxr-xr-x. 1 root root 1094 Jan 29 2019 memberof.la
lrwxrwxrwx. 1 root root 20 Jan 9 14:42 pcache-2.4.so.2 -> pcache-2.4.so.2.10.7
-rwxr-xr-x. 1 root root 78664 Jan 29 2019 pcache-2.4.so.2.10.7
-rwxr-xr-x. 1 root root 1082 Jan 29 2019 pcache.la
lrwxrwxrwx. 1 root root 21 Jan 9 14:42 ppolicy-2.4.so.2 -> ppolicy-2.4.so.2.10.7
```

```
-rwxr-xr-x. 1 root root 44752 Jan 29 2019 ppolicy-2.4.so.2.10.7
-rwxr-xr-x. 1 root root 1095 Jan 29 2019 ppolicy.la
lrwxrwxrwx. 1 root root 21 Jan 9 14:42 pw-sha2-2.4.so.2 -> pw-sha2-2.4.so.2.10.7
-rwxr-xr-x. 1 root root 23592 Jan 29 2019 pw-sha2-2.4.so.2.10.7
-rwxr-xr-x. 1 root root 1088 Jan 29 2019 pw-sha2.la
lrwxrwxrwx. 1 root root 20 Jan 9 14:42 refint-2.4.so.2 -> refint-2.4.so.2.10.7
-rwxr-xr-x. 1 root root 23928 Jan 29 2019 refint-2.4.so.2.10.7
-rwxr-xr-x. 1 root root 1082 Jan 29 2019 refint.la
lrwxrwxrwx. 1 root root 21 Jan 9 14:42 retcode-2.4.so.2 -> retcode-2.4.so.2.10.7
-rwxr-xr-x. 1 root root 32200 Jan 29 2019 retcode-2.4.so.2.10.7
-rwxr-xr-x. 1 root root 1088 Jan 29 2019 retcode.la
lrwxrwxrwx. 1 root root 17 Jan 9 14:42 rwm-2.4.so.2 -> rwm-2.4.so.2.10.7
-rwxr-xr-x. 1 root root 65776 Jan 29 2019 rwm-2.4.so.2.10.7
-rwxr-xr-x. 1 root root 1064 Jan 29 2019 rwm.la
lrwxrwxrwx. 1 root root 20 Jan 9 14:42 seqmod-2.4.so.2 -> seqmod-2.4.so.2.10.7
-rwxr-xr-x. 1 root root 11088 Jan 29 2019 seqmod-2.4.so.2.10.7
-rwxr-xr-x. 1 root root 1082 Jan 29 2019 seqmod.la
lrwxrwxrwx. 1 root root 22 Jan 9 14:42 smbk5pwd-2.4.so.2 -> smbk5pwd-2.4.so.2.10.7
-rwxr-xr-x. 1 root root 15792 Jan 29 2019 smbk5pwd-2.4.so.2.10.7
-rwxr-xr-x. 1 root root 1094 Jan 29 2019 smbk5pwd.la
lrwxrwxrwx. 1 root root 20 Jan 9 14:42 sssv lv-2.4.so.2 -> sssv lv-2.4.so.2.10.7
-rwxr-xr-x. 1 root root 28128 Jan 29 2019 sssv lv-2.4.so.2.10.7
-rwxr-xr-x. 1 root root 1082 Jan 29 2019 sssv lv.la
lrwxrwxrwx. 1 root root 22 Jan 9 14:42 syncprov-2.4.so.2 -> syncprov-2.4.so.2.10.7
-rwxr-xr-x. 1 root root 57128 Jan 29 2019 syncprov-2.4.so.2.10.7
-rwxr-xr-x. 1 root root 1094 Jan 29 2019 syncprov.la
lrwxrwxrwx. 1 root root 25 Jan 9 14:42 translucent-2.4.so.2 -> translucent-2.4.so.2.10.7
-rwxr-xr-x. 1 root root 32576 Jan 29 2019 translucent-2.4.so.2.10.7
-rwxr-xr-x. 1 root root 1112 Jan 29 2019 translucent.la
lrwxrwxrwx. 1 root root 20 Jan 9 14:42 unique-2.4.so.2 -> unique-2.4.so.2.10.7
-rwxr-xr-x. 1 root root 32312 Jan 29 2019 unique-2.4.so.2.10.7
-rwxr-xr-x. 1 root root 1082 Jan 29 2019 unique.la
lrwxrwxrwx. 1 root root 21 Jan 9 14:42 valsort-2.4.so.2 -> vals sort-2.4.so.2.10.7
-rwxr-xr-x. 1 root root 19808 Jan 29 2019 vals sort-2.4.so.2.10.7
```

```
-rwxr-xr-x. 1 root root 1088 Jan 29 2019 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 valsrt.la
```

TLSCACertificateFile, TLSCertificateFile & TLSCertificateKeyFile

Ces directives permettent l'utilisation de connexions cryptées 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_ss=112 simple_bind=64
```

- **ssf1** = La vérification de l'intégrité des données est requise,
- **update_ss** = 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 (**Access Control Lists**) pour sécuriser l'accès aux données. Sans ACL définis, la valeur par défaut est :

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

Important - 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 la modifier,
 - **Allow authenticated users read access** - tout utilisateur authentifié peut lire les entrées,
 - **Allow anonymous users to authenticate** - les utilisateurs anonymes peuvent se connecter.

Important - 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	Intérogation d'un serveur DNS en utilisant les champs SRV des enregistrements DNS
ldap	Transmission des requêtes en tant que proxy vers un autre serveur LDAP
meta	Transmission des requêtes en tant que proxy avec mécanisme de ré-écriture des noms des objets
monitor	Pseudo backend pour accéder aux informations du serveur
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
```

Important - 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	Affichage 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
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

Niveau	Mot clé	Description
8192	Index	Affichage des opérations d'indexation des bases de données
16384	Sync	Affichage des opérations syncrepl

Important - 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 **Idappassword** :

- {SSHA} (**Salted** **Secure Hash Algorithm** - une amélioration de SHA)
- {SHA}
- {SMD5}
- {MD5},
- {CRYPT}

Important - 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.

Important - 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.

Important - 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.

Important - 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.

Important - 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**.

LAB #2 - Configuration des Versions 2.3 et Supérieures

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).

Important - Pour pouvoir utiliser le fichier **slapd.conf**, il convient de le copier dans le répertoire **/usr/local/etc/openldap** ou **/etc/openldap** 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 :

```
[root@centos7 ~]# ls -lR /etc/openldap/slapd.d
```



```
/etc/openldap/slapd.d:  
total 8  
drwxr-x---. 3 ldap ldap 4096 Jan  9 14:42 cn=config  
-rw-----. 1 ldap ldap  589 Jan  9 14:42 cn=config.ldif  
  
/etc/openldap/slapd.d/cn=config:  
total 20  
drwxr-x---. 2 ldap ldap  28 Jan  9 14:42 cn=schema  
-rw-----. 1 ldap ldap 378 Jan  9 14:42 cn=schema.ldif  
-rw-----. 1 ldap ldap 513 Jan  9 14:42 olcDatabase={0}config.ldif  
-rw-----. 1 ldap ldap 443 Jan  9 14:42 olcDatabase={-1}frontend.ldif  
-rw-----. 1 ldap ldap 562 Jan  9 14:42 olcDatabase={1}monitor.ldif  
-rw-----. 1 ldap ldap 609 Jan  9 14:42 olcDatabase={2}hdb.ldif  
  
/etc/openldap/slapd.d/cn=config/cn=schema:  
total 16  
-rw-----. 1 ldap ldap 15578 Jan  9 14:42 cn={0}core.ldif
```

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

Le format LDIF

Les fichiers au format LDIF (**L**DAP **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.

/usr/share/openldap-servers/slapd.ldif

La configuration d'OpenLDAP se trouve dans le fichier **/usr/share/openldap-servers/slapd.ldif** :

```
[root@centos7 ~]# cat /usr/share/openldap-servers/slapd.ldif
#
# See slapd-config(5) for details on configuration options.
# This file should NOT be world readable.
#
dn: cn=config
objectClass: olcGlobal
cn: config
olcArgsFile: /var/run/openldap/slapd.args
olcPidFile: /var/run/openldap/slapd.pid
#
# TLS settings
#
olcTLSCACertificatePath: /etc/openldap/certs
olcTLSCertificateFile: "OpenLDAP Server"
olcTLSCertificateKeyFile: /etc/openldap/certs/password
#
# Do not enable referrals until AFTER you have a working directory
# service AND an understanding of referrals.
#
#olcReferral: ldap://root.openldap.org
#
# Sample security restrictions
```

```
# Require integrity protection (prevent hijacking)
# Require 112-bit (3DES or better) encryption for updates
# Require 64-bit encryption for simple bind
#
#olcSecurity: ssf=1 update_ssf=112 simple_bind=64

#
# Load dynamic backend modules:
# - modulepath is architecture dependent value (32/64-bit system)
# - back_sql.la backend requires openldap-servers-sql package
# - dyngroup.la and dynlist.la cannot be used at the same time
#
#dn: cn=module,cn=config
#objectClass: olcModuleList
#cn: module
#olcModulepath: /usr/lib/openldap
#olcModulepath: /usr/lib64/openldap
#olcModuleload: accesslog.la
#olcModuleload: auditlog.la
#olcModuleload: back_dnssrv.la
#olcModuleload: back_ldap.la
#olcModuleload: back_mdb.la
#olcModuleload: back_meta.la
#olcModuleload: back_null.la
#olcModuleload: back_passwd.la
#olcModuleload: back_relay.la
#olcModuleload: back_shell.la
#olcModuleload: back_sock.la
#olcModuleload: collect.la
#olcModuleload: constraint.la
#olcModuleload: dds.la
#olcModuleload: deref.la
```

```
#olcModuleload: dyngroup.la
#olcModuleload: dynlist.la
#olcModuleload: memberof.la
#olcModuleload: pcache.la
#olcModuleload: ppolicy.la
#olcModuleload: refint.la
#olcModuleload: retcode.la
#olcModuleload: rwm.la
#olcModuleload: seqmod.la
#olcModuleload: smbk5pwd.la
#olcModuleload: sssvlv.la
#olcModuleload: syncprov.la
#olcModuleload: translucent.la
#olcModuleload: unique.la
#olcModuleload: valsrt.la

#
# Schema settings
#
dn: cn=schema,cn=config
objectClass: olcSchemaConfig
cn: schema

include: file:///etc/openldap/schema/core.ldif

#
# Frontend settings
#
dn: olcDatabase=frontend,cn=config
objectClass: olcDatabaseConfig
objectClass: olcFrontendConfig
```

```
olcDatabase: frontend
#
# Sample global 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
#
#olcAccess: to dn.base="" by * read
#olcAccess: to dn.base="cn=Subschema" by * read
#olcAccess: 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!
#
#
# Configuration database
#
dn: olcDatabase=config,cn=config
objectClass: olcDatabaseConfig
olcDatabase: config
olcAccess: to * by dn.base="gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth" manage by * none
```

```

#
# Server status monitoring
#
dn: olcDatabase=monitor,cn=config
objectClass: olcDatabaseConfig
olcDatabase: monitor
olcAccess: to * by dn.base="gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth" read by dn.base="cn=Manager,dc=my-domain,dc=com" read by * none

#
# Backend database definitions
#
dn: olcDatabase=hdb,cn=config
objectClass: olcDatabaseConfig
objectClass: olcHdbConfig
olcDatabase: hdb
olcSuffix: dc=my-domain,dc=com
olcRootDN: cn=Manager,dc=my-domain,dc=com
olcDbDirectory: /var/lib/ldap
olcDbIndex: objectClass eq,pres
olcDbIndex: ou,cn,mail,surname,givenname eq,pres,sub

```

Les attributs 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

Directive slapd.conf	Attribut cn=config
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
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

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

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

```
[root@centos7 ~]# slappasswd
New password: fenestros
Re-enter new password: fenestros
{SSHA}HPtjJrdK0QlLvpfT2GHiQhMrMUT5l5vb
```

La commande slappasswd prend les options suivantes :

```
[root@centos7 ~]# slappasswd --help
slappasswd: invalid option -- '-'
Usage: slappasswd [options]
  -c format crypt(3) salt format
  -g      generate random password
  -h hash  password scheme
  -n      omit trailing newline
  -o <opt>[=val] specify an option with a(n optional) value
    module-path=<pathspec>
    module-load=<filename>
  -s secret new password
  -u      generate RFC2307 values (default)
  -v      increase verbosity
  -T file  read file for new password
```

Il convient ensuite de modifier le fichier **/usr/share/openldap-servers/slapd.ldif** en y ajoutant la ligne **olcRootPW: {SSHA}HPtjJrdK0QILvpfT2GHiQhMrMUt5I5vb**. 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=i2tch,dc=com
olcRootDN: cn=Manager,dc=i2tch,dc=com
...
```

Vous obtiendrez :

```
[root@centos7 ~]# cp /usr/share/openldap-servers/slapd.ldif /root
[root@centos7 ~]# vi slapd.ldif
[root@centos7 ~]# tail slapd.ldif
dn: olcDatabase=hdb,cn=config
objectClass: olcDatabaseConfig
objectClass: olcHdbConfig
olcDatabase: hdb
olcSuffix: dc=i2tch,dc=com
```

```
olcRootDN: cn=Manager,dc=i2tch,dc=com
olcRootPW: {SSHA}HPTjJrdK0QlLvpfT2GHiQhMrMUT5l5vb
olcDbDirectory: /var/lib/ldap
olcDbIndex: objectClass eq,pres
olcDbIndex: ou,cn,mail,surname,givenname eq,pres,sub
```

Important - 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**.

Modifiez la directive **olcAccess** dans la section **Server status monitoring** :

```
...
#
# Server status monitoring
#
dn: olcDatabase=monitor,cn=config
objectClass: olcDatabaseConfig
olcDatabase: monitor
olcAccess: to * by dn.base="gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth" read by dn.base="cn=Manager,dc=i2tch,dc=com" read by * none
#
# Backend database definitions
#
dn: olcDatabase=hdb,cn=config
objectClass: olcDatabaseConfig
objectClass: olcHdbConfig
olcDatabase: hdb
```

```
olcSuffix: dc=i2tch,dc=com
olcRootDN: cn=Manager,dc=i2tch,dc=com
olcRootPW: {SSHA}c8ex7wY3bqGmiknRM8P1rKBzz9zCIo+I
olcDbDirectory: /var/lib/ldap
olcDbIndex: objectClass eq,pres
olcDbIndex: ou,cn,mail,surname,givenname eq,pres,sub
```

Le Fichier DB-CONFIG

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@centos7 ~]# ls -l /usr/share/openldap-servers/DB*
-rw-r--r--. 1 root root 845 Jan 29 2019 /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.

```
[root@centos7 ~]# cat /usr/share/openldap-servers/DB_CONFIG.example
# $OpenLDAP$
# 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@centos7 ~]# cp /usr/share/openldap-servers/DB_CONFIG.example /var/lib/ldap/DB_CONFIG
```

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 :

```
[root@centos7 ~]# vi /var/lib/ldap/DB_CONFIG
[root@centos7 ~]# cat /var/lib/ldap/DB_CONFIG
# $OpenLDAP$
# 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.
set_flags DB_LOG_AUTOREMOVE

# 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).
```

Dernièrement, créez la base de données de configuration :

```
[root@centos7 ~]# rm -rf /etc/openldap/slapd.d/*
[root@centos7 ~]# ls /etc/openldap/slapd.d
[root@centos7 ~]# slapadd -F /etc/openldap/slapd.d -n 0 -l slapd.ldif
#####
100.00% eta    none elapsed          none fast!
Closing DB...
[root@centos7 ~]# chown -R ldap:ldap /etc/openldap/slapd.d
[root@centos7 ~]# ls -l /etc/openldap/slapd.d
total 8
drwxr-x---. 3 ldap ldap 4096 Jan  9 16:32 cn=config
```

```
- rw-----. 1 ldap ldap 604 Jan 9 16:32 cn=config.ldif
```

LAB #3 -Le Fichier /etc/openldap/ldap.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.

```
[root@centos7 ~]# cat /etc/openldap/ldap.conf
#
# LDAP Defaults
#
# See ldap.conf(5) for details
# This file should be world readable but not world writable.

#BASE    dc=example,dc=com
#URI     ldap://ldap.example.com ldap://ldap-master.example.com:666

#SIZELIMIT 12
#TIMELIMIT 15
#DEREF    never

TLS_CACERTDIR /etc/openldap/cacerts

# Turning this off breaks GSSAPI used with krb5 when rdns = false
SASL_NOCANON    on
```

Modifiez ce fichier ainsi :

```
[root@centos7 ~]# cat /etc/openldap/ldap.conf
#
# LDAP Defaults
#
# See ldap.conf(5) for details
# This file should be world readable but not world writable.

BASE    dc=i2tch,dc=com
URI     ldap://10.0.2.15

#SIZELIMIT 12
#TIMELIMIT 15
#DEREF    never

TLS_CACERTDIR /etc/openldap/cacerts

# Turning this off breaks GSSAPI used with krb5 when rdns = false
SASL_NOCANON    on
```

Vous pouvez maintenant tester votre configuration :

```
[root@centos7 ~]# slapttest -u
config file testing succeeded
```

LAB #4 - Démarrer les Serveur OpenLDAP

Ensuite vous pouvez démarrer le serveur slapd :

```
[root@centos7 ~]# systemctl start slapd
[root@centos7 ~]# systemctl status slapd
● slapd.service - OpenLDAP Server Daemon
```

```

Loaded: loaded (/usr/lib/systemd/system/slapd.service; enabled; vendor preset: disabled)
Active: active (running) since Thu 2020-01-09 16:15:42 CET; 6s ago
  Docs: man:slapd
        man:slapd-config
        man:slapd-hdb
        man:slapd-mdb
        file:///usr/share/doc/openldap-servers/guide.html
 Process: 26442 ExecStart=/usr/sbin/slapd -u ldap -h ${SLAPD_URLS} $SLAPD_OPTIONS (code=exited,
status=0/SUCCESS)
 Process: 26428 ExecStartPre=/usr/libexec/openldap/check-config.sh (code=exited, status=0/SUCCESS)
Main PID: 26456 (slapd)
 CGroup: /system.slice/slapd.service
         └─26456 /usr/sbin/slapd -u ldap -h ldapi:/// ldap:///

```

Jan 09 16:15:41 centos7.fenestros.loc systemd[1]: Starting OpenLDAP Server Daemon...
 Jan 09 16:15:41 centos7.fenestros.loc runuser[26431]: pam_unix(runuser:session): session opened for user ldap by (uid=0)
 Jan 09 16:15:41 centos7.fenestros.loc slapd[26442]: @(#) \$OpenLDAP: slapd 2.4.44 (Jan 29 2019 17:42:45) \$mockbuild@x86-01.bsys.centos.org:/builddir/build/BUILD/openldap-2.4.44/openldap-2.4.44/servers/slapd
 Jan 09 16:15:41 centos7.fenestros.loc slapd[26442]: tlsmc_get_pin: INFO: Please note the extracted key file will not be protected with a PIN any more, howeve...missions.
 Jan 09 16:15:42 centos7.fenestros.loc slapd[26456]: slapd starting
 Jan 09 16:15:42 centos7.fenestros.loc systemd[1]: Started OpenLDAP Server Daemon.
 Hint: Some lines were ellipsized, use -l to show in full.

Constatez le processus en cours :

```
[root@centos7 ~]# ps aux | grep slapd
ldap    26456  0.0  6.2 494476 31356 ?        Ssl   16:15   0:00 /usr/sbin/slapd -u ldap -h ldapi:/// ldap:///
root    26857  0.0  0.1 112712   960 pts/0      S+   16:16   0:00 grep --color=auto slapd
```

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

```
[root@centos7 ~]# cat /var/run/openldap/slapd.args
```

```
/usr/sbin/slappd -u ldap -h ldapi:/// ldap:///
```

Options de la ligne de commande de slappd

La commande slappd peut prendre plusieurs options :

```
[root@centos7 ~]# slappd --help
slappd: invalid option -- '-'
usage: slappd 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 exit afterwards, -VVV print
              info about static overlays and backends)
```

LAB #5 - La Commande **ldapadd**

Les commandes **ldap*** sont utilisées quand le serveur OpenLDAP fonctionne.

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

```
[root@centos7 ~]# 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
[!]sessiontracking
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")
            ldif-wrap=<width> (in columns, or "no" for no wrapping)
-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)
```

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

```
[root@centos7 ~]# vi setup.ldif
```

```
[root@centos7 ~]# cat setup.ldif
# Organisation i2tch
dn: dc=i2tch,dc=com
objectClass: dcObject
objectClass: organization
dc: i2tch
o: i2tch.com
description: Exemple

# Gestionnaire de l'arbre
dn: cn=Manager,dc=i2tch,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@centos7 ~]# ldapadd -f setup.ldif -x -D "cn=Manager,dc=i2tch,dc=com" -w fenestros
adding new entry "dc=i2tch,dc=com"

adding new entry "cn=Manager,dc=i2tch,dc=com"
```

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

```
[root@centos7 ~]# vi import.ldif
[root@centos7 ~]# cat import.ldif
version: 1
dn: ou=France,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: France

dn: ou=Commercial,ou=France,dc=i2tch,dc=com
objectClass: organizationalUnit
```

```
objectClass: top
ou: Commercial

dn: ou=Recherche,ou=France,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Recherche

dn: ou=Production,ou=France,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Production

dn: ou=Suisse,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Suisse

dn: ou=Commercial,ou=Suisse,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Commercial

dn: ou=USA,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: USA

dn: ou=Commercial,ou=USA,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Commercial

dn: ou=Recherche,ou=USA,dc=i2tch,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@centos7 ~]# ldapadd -f import.ldif -x -D "cn=Manager,dc=i2tch,dc=com" -w fenestros  
adding new entry "ou=France,dc=i2tch,dc=com"  
  
adding new entry "ou=Commercial,ou=France,dc=i2tch,dc=com"  
  
adding new entry "ou=Recherche,ou=France,dc=i2tch,dc=com"  
  
adding new entry "ou=Production,ou=France,dc=i2tch,dc=com"  
  
adding new entry "ou=Suisse,dc=i2tch,dc=com"  
  
adding new entry "ou=Commercial,ou=Suisse,dc=i2tch,dc=com"  
  
adding new entry "ou=USA,dc=i2tch,dc=com"  
  
adding new entry "ou=Commercial,ou=USA,dc=i2tch,dc=com"  
  
adding new entry "ou=Recherche,ou=USA,dc=i2tch,dc=com"
```

LAB #6 - Installation et Utilisation du client graphique luma

Configurez votre machine virtuelle pour démarrer en mode graphique :

```
[root@centos7 ~]# ls -l /etc/systemd/system/default.target  
lrwxrwxrwx. 1 root root 37 Apr 30 2016 /etc/systemd/system/default.target -> /lib/systemd/system/multi-  
user.target
```

```
[root@centos7 ~]# rm -rf /etc/systemd/system/default.target
[root@centos7 ~]# ln -s /lib/systemd/system/graphical.target /etc/systemd/system/default.target
[root@centos7 ~]# ls -l /etc/systemd/system/default.target
lrwxrwxrwx. 1 root root 36 Jan  9 18:09 /etc/systemd/system/default.target ->
/lib/systemd/system/graphical.target
```

Arrêtez votre machine virtuelle et augmentez sa mémoire à 2Go. Démarrer ensuite la VM.

Ouvrez un navigateur web **dans la VM** et visitez votre plateforme de cours. Dans la section Liens du module d'OpenLDAP cliquez sur le lien **luma-master.zip** pour télécharger Luma : <https://drive.google.com/file/d/17rt40mgjlq-YHCn7Tzz9UodpyRAIQtdf/view?usp=sharing>

Ouvrez une session via putty ou un terminal sur votre machine hôte puis installez le paquet **PyQt4** :

```
[trainee@centos7 ~]$ su -
Mot de passe : fenestros
[root@centos7 ~]# yum install PyQt4
```

Déplacez le fichier **luma-master.zip** vers /root :

```
[root@centos7 ~]# mv /home/trainee/Downloads/luma-master.zip .
```

Décompressez l'archive :

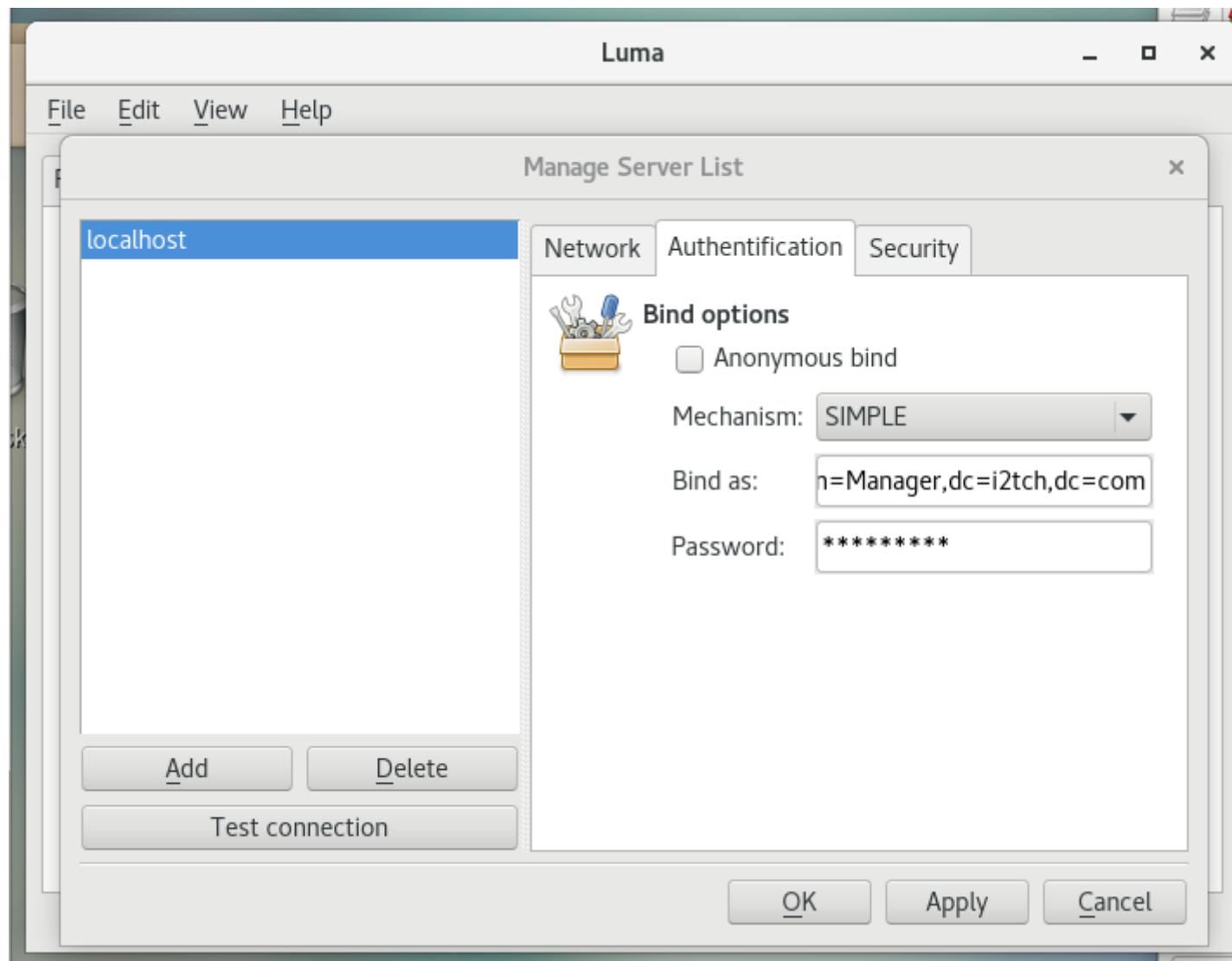
```
[root@centos7 ~]# unzip luma-master.zip
```

Installez luma :

```
[root@centos7 ~]# cd luma-master/
[root@centos7 luma-master]# ls
AUTHORS bumpversion.sh contrib data HACKING luma      luma.qrc  MANIFEST.in resources setup.py tools
bin      ChangeLog          COPYING doc    INSTALL luma.pro  Makefile README      setup      TODO
[root@centos7 luma-master]# python setup.py install
```

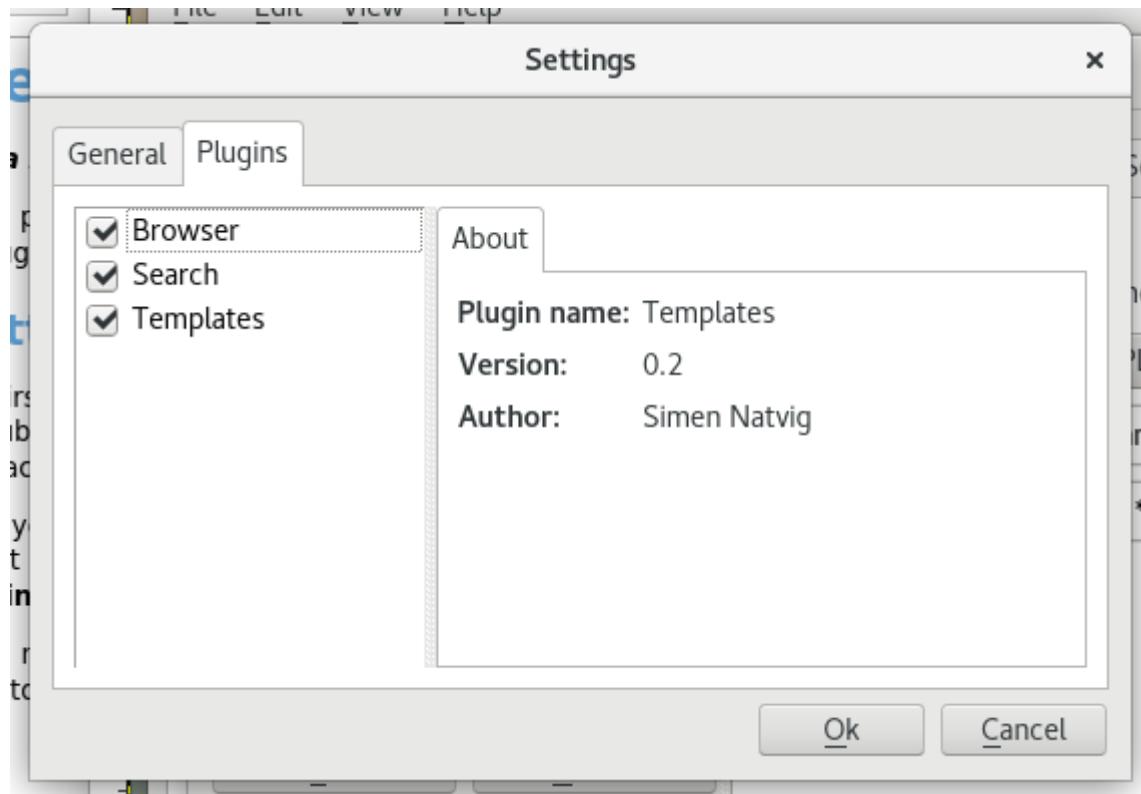
Retournez à votre VM et lancez luma via les menus **Applications > System Tools > Luma LDAP Browser**.

Connectez-vous à votre serveur LDAP en utilisant luma. Cliquez sur le menu **Edit > Server List**. Cliquez sur **Add** puis renseignez le nom localhost. Sélectionnez **Authentification**, décochez **Anonymous bind** et remplissez les champs pour une connexion **simple** :

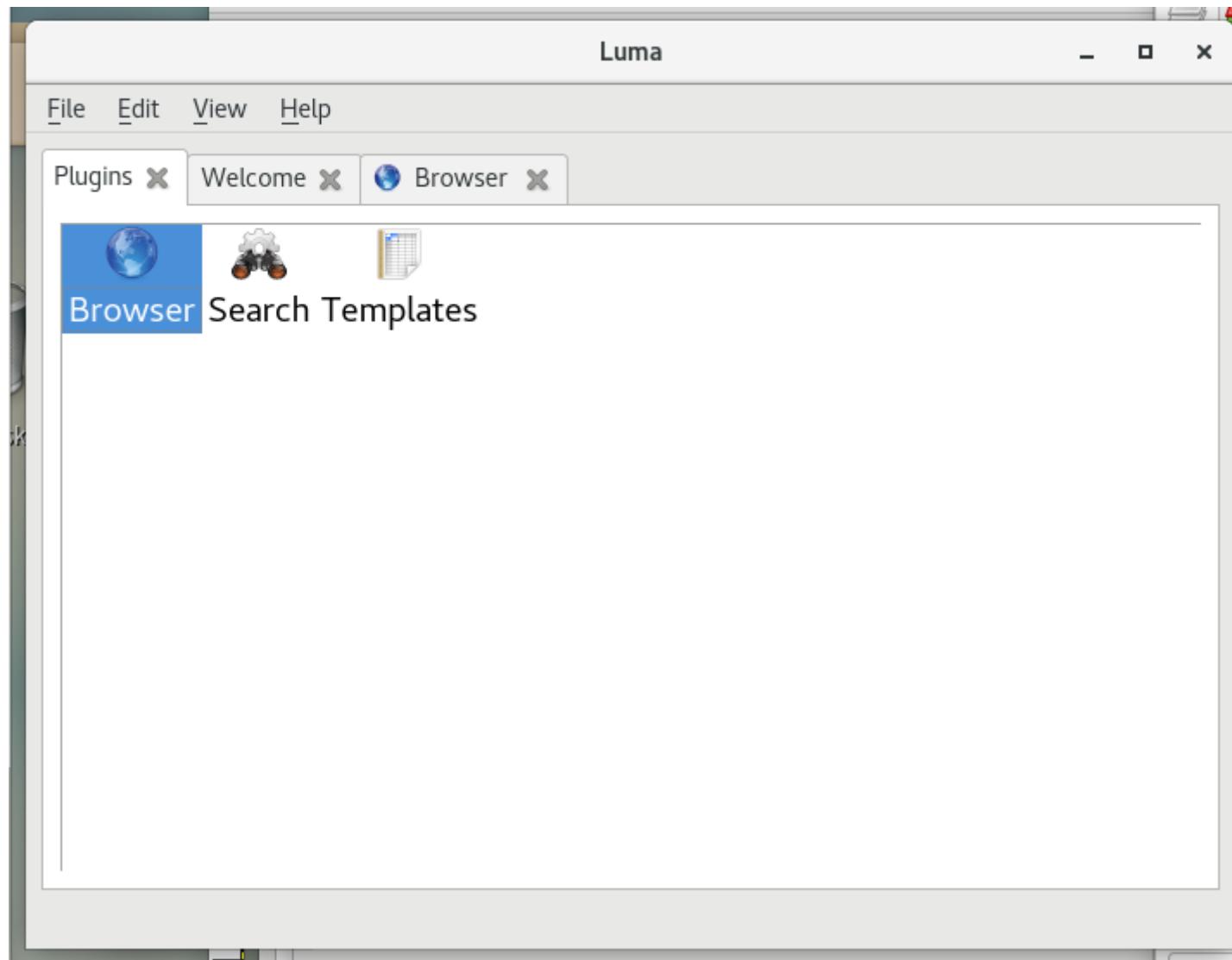


Cliquez sur le bouton **Apply** puis sur le bouton **Ok**.

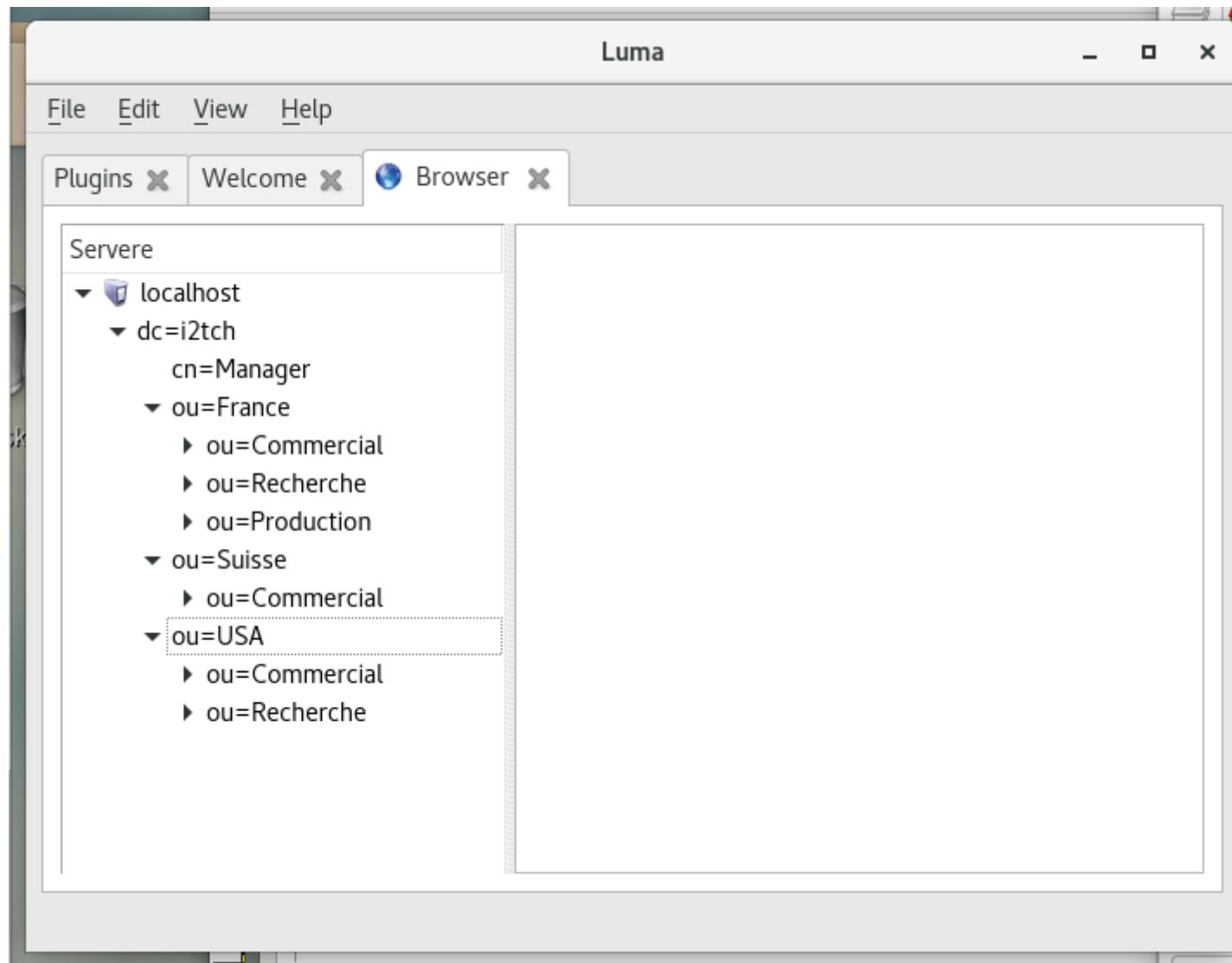
Cliquez sur l'onglet **Plugins** et cochez tout. Cliquez ensuite sur le bouton **Ok** :



Double-cliquez sur **Browser** :



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



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'*exception 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 espaces.

Les alias

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

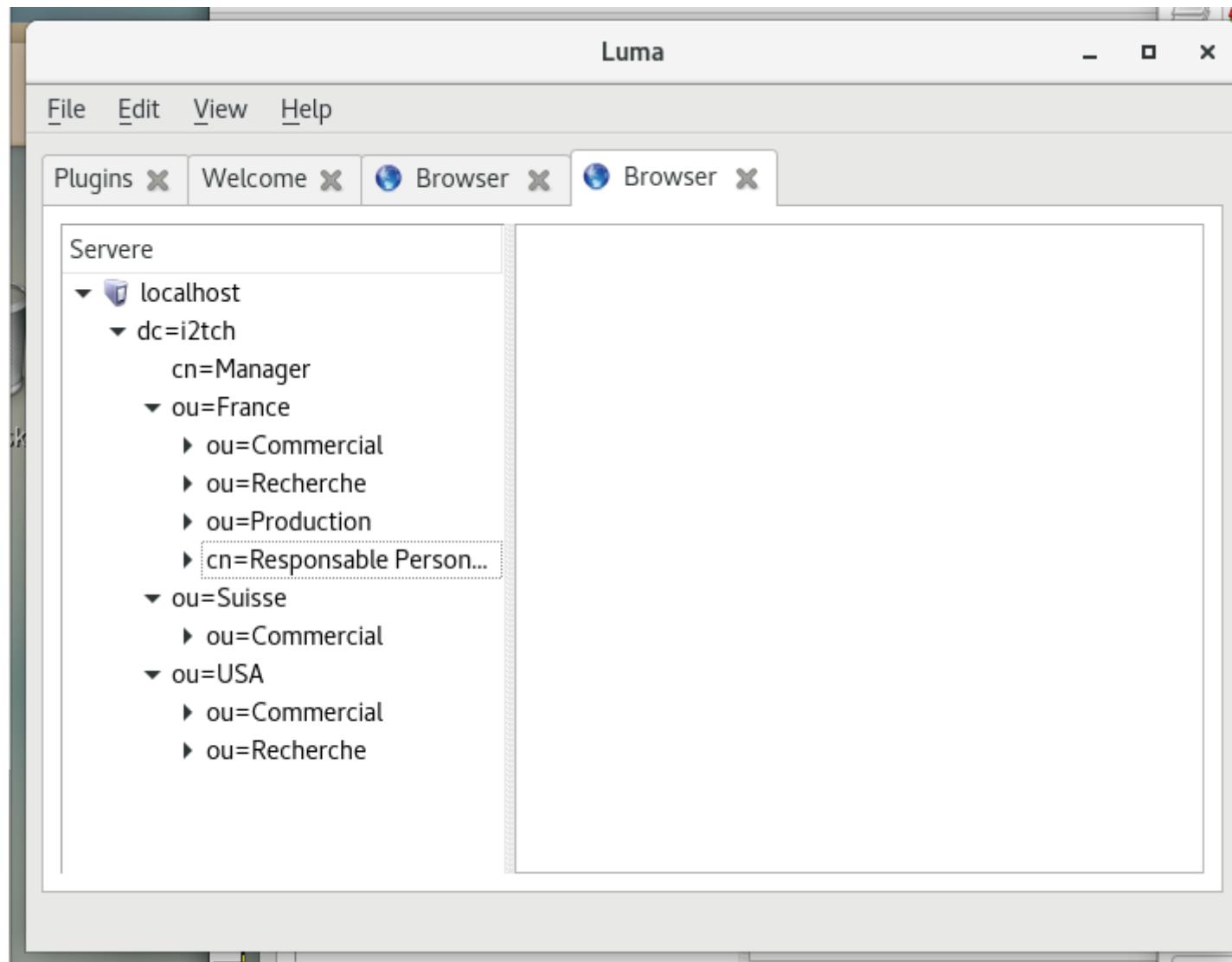
Pour illustrer ce point, créez le fichier LDIF **alias.ldif** et éditez-le ainsi :

```
[root@centos7 luma-master]# cd ~
[root@centos7 ~]# vi alias.ldif
[root@centos7 ~]# cat alias.ldif
version: 1
dn: cn=Responsable Personnel,ou=France,dc=i2tch,dc=com
cn: Responsable Personnel
aliasedObjectName: cn=Directeur,ou=France,dc=i2tch,dc=com
objectClass: top
objectClass: alias
objectClass: extensibleObject
```

Importez maintenant le fichier LDIF dans le DIT :

```
[root@centos7 ~]# ldapadd -f alias.ldif -x -D "cn=Manager,dc=i2tch,dc=com" -w fenestros
adding new entry "cn=Responsable Personnel,ou=France,dc=i2tch,dc=com"
```

Constatez maintenant le résultat :



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

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

```
[root@centos7 ~]# vi directeur.ldif
```

```
[root@centos7 ~]# cat directeur.ldif
version: 1
dn: cn=directeur,ou=France,dc=i2tch,dc=com
objectClass: person
objectClass: top
cn: directeur
sn: Guillaud
telephoneNumber: 12345678
telephoneNumber: 87654321
```

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

```
[root@centos7 ~]# ldapadd -f directeur.ldif -x -D "cn=Manager,dc=i2tch,dc=com" -w fenestros
adding new entry "cn=directeur,ou=France,dc=i2tch,dc=com"
ldap_add: Server is unwilling to perform (53)
        additional info: no global superior knowledge
```

Important - Cette erreur indique que OpenLDAP ne sait pas où mettre les données. Ceci est causé par le fait que le schéma adéquat n'a pas été chargé.

Modifiez donc votre fichier slapd.ldif en ajoutant les lignes suivantes :

```
[root@centos7 ~]# vi slapd.ldif
[root@centos7 ~]# cat slapd.ldif
...
include: file:///etc/openldap/schema/core.ldif
include: file:///etc/openldap/schema/corba.ldif
include: file:///etc/openldap/schema/cosine.ldif
include: file:///etc/openldap/schema/duaconf.ldif
include: file:///etc/openldap/schema/dyngroup.ldif
include: file:///etc/openldap/schema/inetorgperson.ldif
```

```
include: file:///etc/openldap/schema/java.ldif
include: file:///etc/openldap/schema/misc.ldif
include: file:///etc/openldap/schema/nis.ldif
include: file:///etc/openldap/schema/openldap.ldif
include: file:///etc/openldap/schema/ppolicy.ldif
include: file:///etc/openldap/schema/collective.ldif
...
```

Arrêtez le serveur slapd :

```
[root@centos7 ~]# systemctl stop slapd
```

Re-créez la base de données de la configuration :

```
[root@centos7 ~]# rm -rf /etc/openldap/slapd.d/*
[root@centos7 ~]# ls /etc/openldap/slapd.d
[root@centos7 ~]# slapadd -F /etc/openldap/slapd.d -n 0 -l slapd.ldif
#####
100.00% eta    none elapsed           none fast!
Closing DB...
[root@centos7 ~]# chown -R ldap:ldap /etc/openldap/slapd.d
[root@centos7 ~]# ls -lR /etc/openldap/slapd.d
/etc/openldap/slapd.d:
total 8
drwxr-x---. 3 ldap ldap 4096 Jan 10 10:46 cn=config
-rw-----. 1 ldap ldap  627 Jan 10 10:46 cn=config.ldif

/etc/openldap/slapd.d/cn=config:
total 24
drwxr-x---. 2 ldap ldap 4096 Jan 10 10:46 cn=schema
-rw-----. 1 ldap ldap  378 Jan 10 10:46 cn=schema.ldif
-rw-----. 1 ldap ldap  513 Jan 10 10:46 olcDatabase={0}config.ldif
-rw-----. 1 ldap ldap  443 Jan 10 10:46 olcDatabase={-1}frontend.ldif
-rw-----. 1 ldap ldap  558 Jan 10 10:46 olcDatabase={1}monitor.ldif
-rw-----. 1 ldap ldap  666 Jan 10 10:46 olcDatabase={2}hdb.ldif
```

```
/etc/openldap/slapd.d/cn=config/cn=schema:  
total 76  
-rw----- . 1 ldap ldap 15578 Jan 10 10:46 cn={0}core.ldif  
-rw----- . 1 ldap ldap 3845 Jan 10 10:46 cn={10}ppolicy.ldif  
-rw----- . 1 ldap ldap 1523 Jan 10 10:46 cn={11}collective.ldif  
-rw----- . 1 ldap ldap 1283 Jan 10 10:46 cn={1}corba.ldif  
-rw----- . 1 ldap ldap 11363 Jan 10 10:46 cn={2}cosine.ldif  
-rw----- . 1 ldap ldap 4489 Jan 10 10:46 cn={3}duaconf.ldif  
-rw----- . 1 ldap ldap 1693 Jan 10 10:46 cn={4}dyngroup.ldif  
-rw----- . 1 ldap ldap 2857 Jan 10 10:46 cn={5}inetorgperson.ldif  
-rw----- . 1 ldap ldap 2589 Jan 10 10:46 cn={6}java.ldif  
-rw----- . 1 ldap ldap 1519 Jan 10 10:46 cn={7}misc.ldif  
-rw----- . 1 ldap ldap 6495 Jan 10 10:46 cn={8}nis.ldif  
-rw----- . 1 ldap ldap 1290 Jan 10 10:46 cn={9}openldap.ldif
```

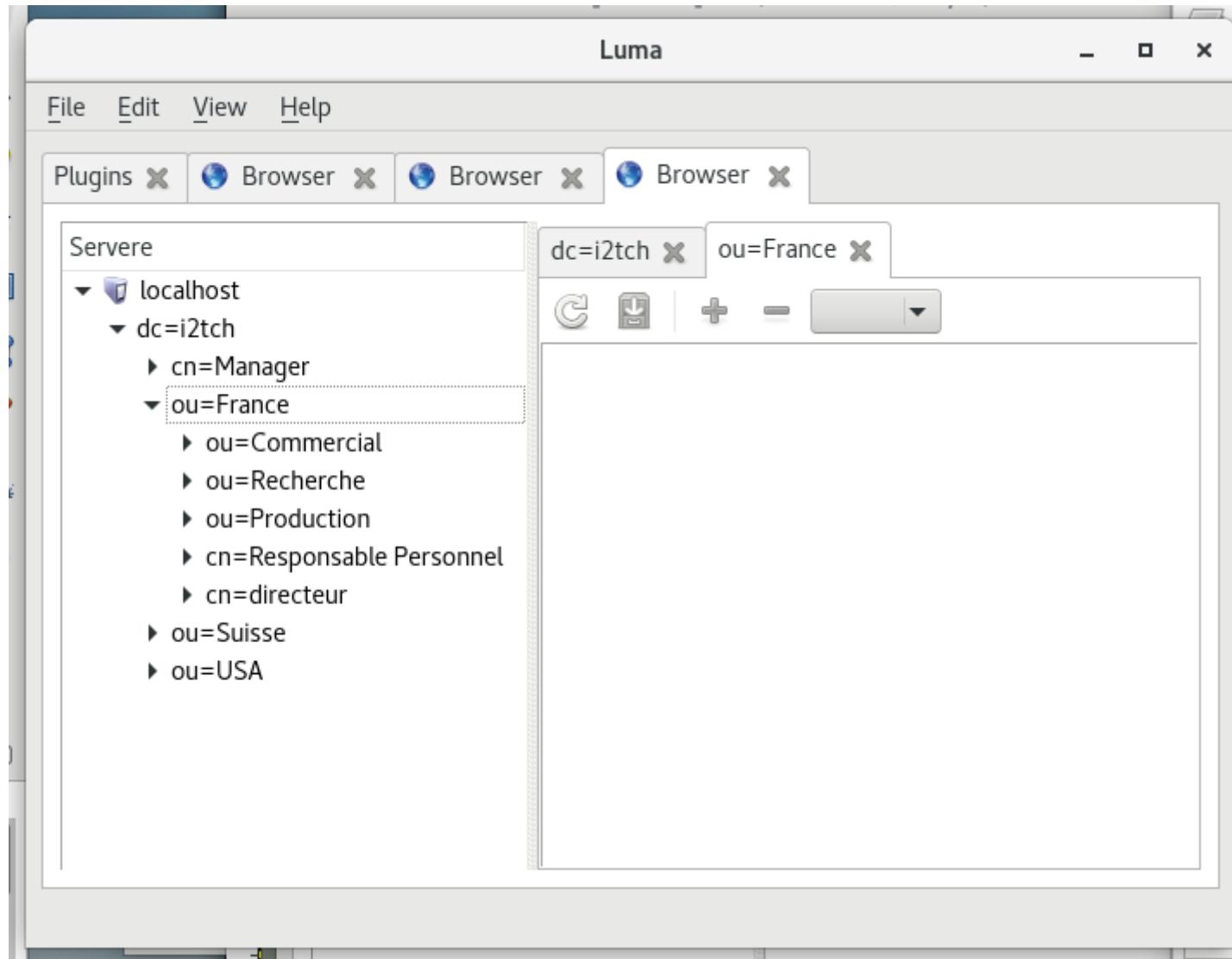
```
[root@centos7 ~]# slapttest -u  
config file testing succeeded
```

```
[root@centos7 ~]# systemctl start slapd
```

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

```
[root@centos7 ~]# ldapadd -f directeur.ldif -x -D "cn=Manager,dc=i2tch,dc=com" -w fenestros  
adding new entry "cn=directeur,ou=France,dc=i2tch,dc=com"
```

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



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

```
[root@centos7 ~]# vi plus.ldif
[root@centos7 ~]# cat plus.ldif
version: 1
```

```
dn: ou=Angleterre,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Angleterre

dn: ou=Sales,ou=Angleterre,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Sales

dn: cn=Sales Director,ou=Sales,ou=Angleterre,dc=i2tch,dc=com
objectClass: person
objectClass: top
cn: Sales Director
sn: Smith

dn: cn=Sales Manager,cn=Sales Director,ou=Sales,ou=Angleterre,dc=i2tch,dc=com
objectClass: person
objectClass: top
cn: Sales Manager
sn: Brown

dn: cn=dupont,ou=Recherche,ou=France,dc=i2tch,dc=com
objectClass: person
objectClass: top
cn: dupont
sn: dupont
```

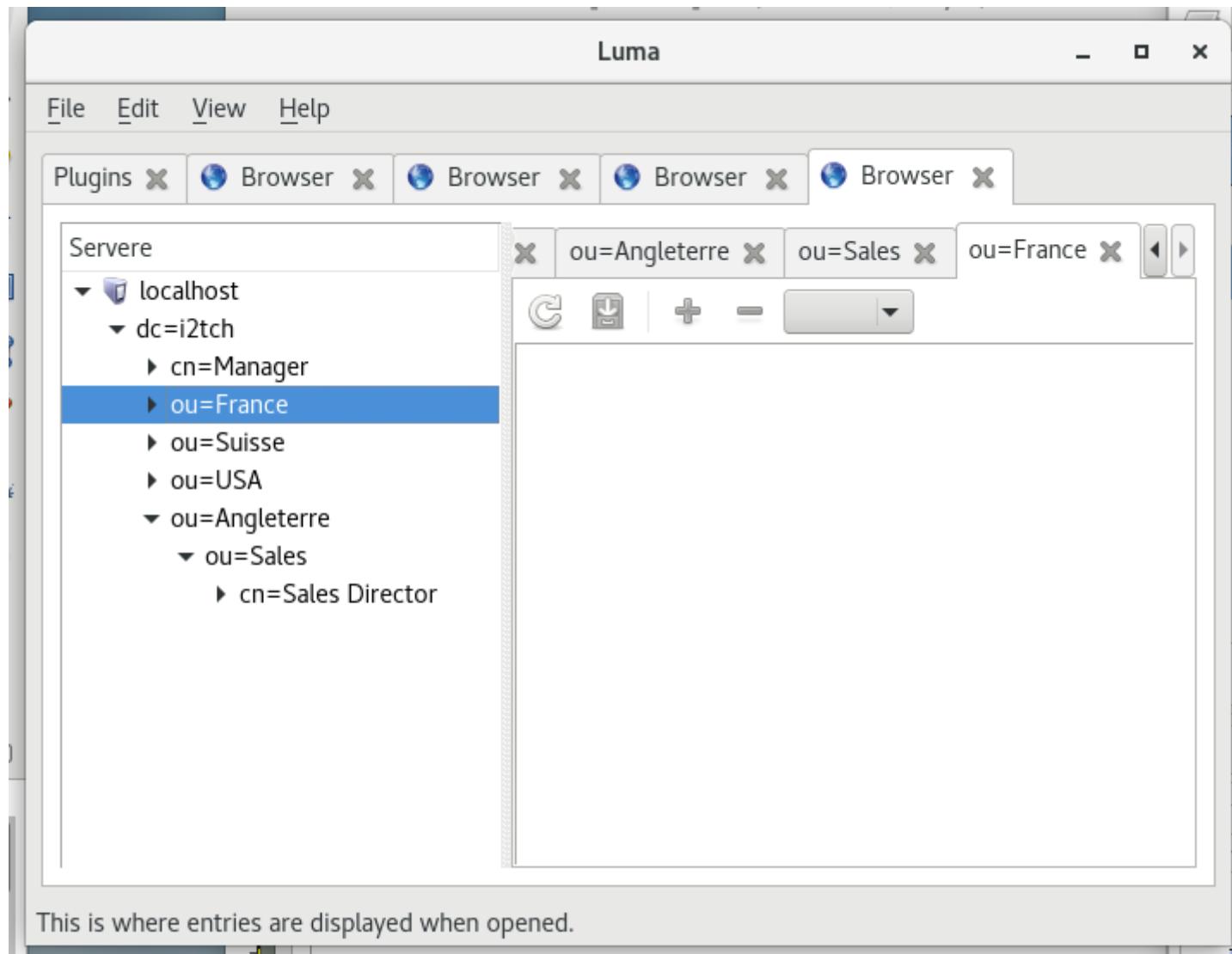
Créez donc les entrées en utilisant le fichier **plus.ldif** :

```
[root@centos7 ~]# ldapadd -f plus.ldif -x -D "cn=Manager,dc=i2tch,dc=com" -w fenestros
adding new entry "ou=Angleterre,dc=i2tch,dc=com"

adding new entry "ou=Sales,ou=Angleterre,dc=i2tch,dc=com"
```

```
adding new entry "cn=Sales Director,ou=Sales,ou=Angleterre,dc=i2tch,dc=com"
adding new entry "cn=Sales Manager,cn=Sales Director,ou=Sales,ou=Angleterre,dc=i2tch,dc=com"
adding new entry "cn=dupont,ou=Recherche,ou=France,dc=i2tch,dc=com"
```

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



LAB #7 - Installation et Utilisation du Client HTML phpLDAPadmin

Commencez par installer phpLDAPadmin :

```
[root@centos7 ~]# yum -y install httpd
[root@centos7 ~]# systemctl status httpd
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; vendor preset: disabled)
   Active: inactive (dead)
     Docs: man:httpd(8)
           man:apachectl(8)
[root@centos7 ~]# systemctl enable httpd
Created symlink from /etc/systemd/system/multi-user.target.wants/httpd.service to
/usr/lib/systemd/system/httpd.service.
[root@centos7 ~]# systemctl start httpd
[root@centos7 ~]# yum -y install php php-mbstring php-pear php-ldap
[root@centos7 ~]# yum -y install epel-release
[root@centos7 ~]# systemctl restart httpd
```

Modifiez les lignes **332, 388, 397 et 398** du fichier **/etc/phpldapadmin/config.php** :

```
[root@centos7 ~]# vi /etc/phpldapadmin/config.php
[root@centos7 ~]# cat /etc/phpldapadmin/config.php
...
332 $servers->setValue('login','bind_id','cn=Manager,dc=i2tch,dc=com');
...
388 $servers->setValue('appearance','password_hash','ssha');

397 $servers->setValue('login','attr','dn');
398 // $servers->setValue('login','attr','uid');
...
```

Les attributs

Dans le navigateur web de la **machine virtuelle** rendez-vous à l'URL <http://localhost/ldapadmin> et connectez-vous :



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



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

Cliquez sur l'icone **schema** :



Dans le panneau de droite, cliquez sur le lien **Attribute Types** :



Dans la liste déroulante, choisissez l'attribut **telephoneNumber** :



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/>.

Un attribut peut dériver d'un autre attribut. Cet héritage implique le respect des caractéristiques 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=i2tch,dc=com
modifiersName	cn=Manager,dc=i2tch,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 droite, cliquez sur le lien **ObjectClasses** et trouvez la classe **Person** dans la liste déroulante :



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 le cas de notre fichier LDIF **alias.ldif**. Notons que dans ce fichier, nous avons utilisé un objectClass **alias** :

```
version: 1
dn: cn=Responsable Personnel,ou=France,dc=i2tch,dc=com
cn: Responsable Personnel
aliasedObjectName: cn=Directeur,ou=France,dc=i2tch,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** :



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



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 :



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@centos7 ~]# ls /etc/openldap/schema/
collective.ldif    corba.schema   cosine.ldif      duacnf.schema    inetorgperson.ldif    java.schema    nis.ldif
openldap.schema    ppolicy.ldif
collective.schema   core.ldif     cosine.schema   dyngroup.ldif   inetorgperson.schema  misc.ldif     nis.schema
ppmi.ldif          ppolicy.schema
corba.ldif         core.schema   duacnf.ldif    dyngroup.schema  java.ldif           misc.schema  openldap.ldif
pmi.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 **mail.ldif** et éditez-le ainsi :

```
[root@centos7 ~]# vi mail.ldif
[root@centos7 ~]# cat mail.ldif
version: 1
dn: cn=mail,ou=Commercial,ou=France,dc=i2tch,dc=com
objectClass: inetOrgPerson
objectClass: person
objectClass: top
cn: mail
mail: info@i2tch.com
sn: info
```

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

```
[root@centos7 ~]# ldapadd -f mail.ldif -x -D "cn=Manager,dc=i2tch,dc=com" -w fenestros
adding new entry "cn=mail,ou=Commercial,ou=France,dc=i2tch,dc=com"
```

Constatez maintenant le résultat avec phpLDAPAdmin en cliquant sur l'icone **refresh** dans le panneau de gauche :



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 **referal.ldif** et éditez-le ainsi :

```
[root@centos7 ~]# vi referal.ldif
[root@centos7 ~]# cat referal.ldif
```

```
version: 1
dn: ou=Informatique,dc=i2tch,dc=com
objectClass: referral
objectClass: extensibleObject
objectClass: top
ref: ldap://ldap.i2tch.net/ou=i2tch.com,dc=i2tch,dc=net
ou: Informatique
```

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

```
[root@centos7 ~]# ldapadd -f referal.ldif -x -D "cn=Manager,dc=i2tch,dc=com" -w fenestros
adding new entry "ou=Informatique,dc=i2tch,dc=com"
```

Constatez maintenant le résultat avec `phpLDAPAdmin` en cliquant sur l'icone **refresh** dans le panneau de gauche :



LAB #8 - 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@centos7 ~]# 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>[=:<b64value>] (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
        [!]sessiontracking
                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")
        ldif-wrap=<width> (in columns, or "no" for no wrapping)
-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@centos7 ~]# 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=i2tch,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: 1.3.6.1.1.22  
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: SCRAM-SHA-1  
supportedSASLMechanisms: GSS-SPNEGO  
supportedSASLMechanisms: GSSAPI  
supportedSASLMechanisms: DIGEST-MD5  
supportedSASLMechanisms: CRAM-MD5  
ref: ldap://root.openldap.org
```

```
entryDN:  
subschemaSubentry: cn=Subschema
```

```
# search result  
search: 2  
result: 0 Success
```

```
# numResponses: 2  
# numEntries: 1
```

A Faire - 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'intérogation de l'annuaire se fait avec une requête composée de 4 éléments :

Elément	Description
Base	Le point de départ de la requête
Attributs	La liste des attributs à retourner. Si vide ou *, tous les attributs sont retournés
Portée	Indique la portée de la requête. Elle peut être Base , One ou Sub
Filtre	Spécifie des critères à appliquer aux 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 l'exemple suivant, nous cherchons les entrées du type **ou** à partir de **ou=France,dc=i2tch,dc=com** :

```
[root@centos7 ~]# ldapsearch -x -b "ou=France,dc=i2tch,dc=com" "(objectClass=organizationalUnit)"
```

```
# extended LDIF
#
# LDAPv3
# base <ou=France,dc=i2tch,dc=com> with scope subtree
# filter: (objectClass=organizationalUnit)
# requesting: ALL
#
# France, i2tch.com
dn: ou=France,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: France

# Commercial, France, i2tch.com
dn: ou=Commercial,ou=France,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Commercial

# Recherche, France, i2tch.com
dn: ou=Recherche,ou=France,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Recherche

# Production, France, i2tch.com
dn: ou=Production,ou=France,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Production

# search result
search: 2
```

```
result: 0 Success  
  
# numResponses: 5  
# numEntries: 4
```

Dans l'exemple suivant, nous cherchons les entrées **enfants** du type **ou** à partir de **ou=France,dc=i2tch,dc=com** sans commentaires :

```
[root@centos7 ~]# ldapsearch -x -LLL -s children -b "ou=France,dc=i2tch,dc=com"  
"(objectClass=organizationalUnit)"  
dn: ou=Commercial,ou=France,dc=i2tch,dc=com  
objectClass: organizationalUnit  
objectClass: top  
ou: Commercial  
  
dn: ou=Recherche,ou=France,dc=i2tch,dc=com  
objectClass: organizationalUnit  
objectClass: top  
ou: Recherche  
  
dn: ou=Production,ou=France,dc=i2tch,dc=com  
objectClass: organizationalUnit  
objectClass: top  
ou: Production
```

Dans l'exemple suivant, nous cherchons les entrées **enfants** du type **ou** à partir de **ou=France,dc=i2tch,dc=com** sans commentaires et avec un tri sur la valeur de l'ou :

```
[root@centos7 ~]# ldapsearch -x -LLL -S ou -s children -b "ou=France,dc=i2tch,dc=com"  
dn: cn=Responsable Personnel,ou=France,dc=i2tch,dc=com  
cn: Responsable Personnel  
aliasedObjectName: cn=Directeur,ou=France,dc=i2tch,dc=com  
objectClass: top  
objectClass: alias  
objectClass: extensibleObject
```

```
dn: cn=directeur,ou=France,dc=i2tch,dc=com
objectClass: person
objectClass: top
cn: directeur
sn: Guillaud
telephoneNumber: 12345678
telephoneNumber: 87654321
```

```
dn: cn=dupont,ou=Recherche,ou=France,dc=i2tch,dc=com
objectClass: person
objectClass: top
cn: dupont
sn: dupont
```

```
dn: cn=mail,ou=Commercial,ou=France,dc=i2tch,dc=com
objectClass: inetOrgPerson
objectClass: person
objectClass: top
cn: mail
mail: info@i2tch.com
sn: info
```

```
dn: ou=Commercial,ou=France,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Commercial
```

```
dn: ou=Production,ou=France,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Production
```

```
dn: ou=Recherche,ou=France,dc=i2tch,dc=com
objectClass: organizationalUnit
```

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

Dans l'exemple suivant, nous cherchons les entrées **enfants** du type **ou** à partir de **ou=France,dc=i2tch,dc=com** sans commentaires, avec un tri sur la valeur de l'ou et en demandant une affichage plus lisible :

```
[root@centos7 ~]# ldapsearch -x -LLL -S ou -s children -u -b "ou=France,dc=i2tch,dc=com"
dn: cn=Responsable Personnel,ou=France,dc=i2tch,dc=com
ufn: Responsable Personnel, France, i2tch.com
cn: Responsable Personnel
aliasedObjectName: cn=Directeur,ou=France,dc=i2tch,dc=com
objectClass: top
objectClass: alias
objectClass: extensibleObject

dn: cn=directeur,ou=France,dc=i2tch,dc=com
ufn: directeur, France, i2tch.com
objectClass: person
objectClass: top
cn: directeur
sn: Guillaud
telephoneNumber: 12345678
telephoneNumber: 87654321

dn: cn=dupont,ou=Recherche,ou=France,dc=i2tch,dc=com
ufn: dupont, Recherche, France, i2tch.com
objectClass: person
objectClass: top
cn: dupont
sn: dupont

dn: cn=mail,ou=Commercial,ou=France,dc=i2tch,dc=com
ufn: mail, Commercial, France, i2tch.com
objectClass: inetOrgPerson
```

```
objectClass: person
objectClass: top
cn: mail
mail: info@i2tch.com
sn: info

dn: ou=Commercial,ou=France,dc=i2tch,dc=com
ufn: Commercial, France, i2tch.com
objectClass: organizationalUnit
objectClass: top
ou: Commercial

dn: ou=Production,ou=France,dc=i2tch,dc=com
ufn: Production, France, i2tch.com
objectClass: organizationalUnit
objectClass: top
ou: Production

dn: ou=Recherche,ou=France,dc=i2tch,dc=com
ufn: Recherche, France, i2tch.com
objectClass: organizationalUnit
objectClass: top
ou: Recherche
```

Dans l'exemple suivant, nous cherchons les entrées du type **ou** et **cn** à partir de **ou=France,dc=i2tch,dc=com** en utilisant un fichier de filtre. Le fichier de filtre est **filtre** et contient **trois** lignes :

```
[root@centos7 ~]# vi filtre
[root@centos7 ~]# cat filtre
organizationalUnit
inetOrgPerson
```

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

La commande est :

```
[root@centos7 ~]# ldapsearch -x -b "ou=France,dc=i2tch,dc=com" -f filtre "(objectClass=%s)" ou cn
# extended LDIF
#
# LDAPv3
# base <ou=France,dc=i2tch,dc=com> with scope subtree
# filter pattern: (objectClass=%s)
# requesting: ou cn
#
#
# filter: (objectClass=organizationalUnit)
#
# France, i2tch.com
dn: ou=France,dc=i2tch,dc=com
ou: France

# Commercial, France, i2tch.com
dn: ou=Commercial,ou=France,dc=i2tch,dc=com
ou: Commercial

# Recherche, France, i2tch.com
dn: ou=Recherche,ou=France,dc=i2tch,dc=com
ou: Recherche

# Production, France, i2tch.com
dn: ou=Production,ou=France,dc=i2tch,dc=com
ou: Production

# search result
```

```
search: 2
result: 0 Success

# numResponses: 5
# numEntries: 4

#
# filter: (objectClass=inetOrgPerson)
#
# mail, Commercial, France, i2tch.com
dn: cn=mail,ou=Commercial,ou=France,dc=i2tch,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
```

LAB #9 - La Commande ldapmodify

La commande `ldapmodify` prend les options suivantes :

```
[root@centos7 ~]# 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
        [!]sessiontracking
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")
             ldif-wrap=<width> (in columns, or "no" for no wrapping)
-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)
```

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

```
[root@centos7 ~]# vi prepa_modify.ldif
[root@centos7 ~]# cat prepa_modify.ldif
dn: cn=dupond,ou=Recherche,ou=France,dc=i2tch,dc=com
objectClass: inetOrgPerson
objectClass: top
cn: dupond
sn: dupond
```

Saisissez ensuite la commande suivante :

```
[root@centos7 ~]# ldapadd -f prep_modif.ldif -x -D "cn=Manager,dc=i2tch,dc=com" -W  
Enter LDAP Password: fenestros  
adding new entry "cn=dupond,ou=Recherche,ou=France,dc=i2tch,dc=com"
```

Important - 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. Notez donc que le mot de passe saisi ne sera **pas** en clair.

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



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

```
[root@centos7 ~]# vi modify.ldif  
[root@centos7 ~]# cat modify.ldif  
dn: cn=dupond,ou=Recherche,ou=France,dc=i2tch,dc=com  
changetype: modify  
add: mail  
mail: dupond@i2tch.com
```

Saisissez maintenant la commande suivante :

```
[root@centos7 ~]# ldapmodify -f modify.ldif -x -D "cn=Manager,dc=i2tch,dc=com" -W  
Enter LDAP Password: fenestros  
modifying entry "cn=dupond,ou=Recherche,ou=France,dc=i2tch,dc=com"
```

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



LAB #10 - La Commande **ldapdelete**

Comme vous pouvez constater, vous avez deux entrées dans **ou=Recherche,ou=France,dc=i2tch,dc=com** :

- dupond
- dupont

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

```
[root@centos7 ~]# 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
[!]sessiontracking
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")
            ldif-wrap=<width> (in columns, or "no" for no wrapping)
-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@centos7 ~]# ldapdelete -x -D "cn=Manager,dc=i2tch,dc=com" -W  
"cn=dupont,ou=Recherche,ou=France,dc=i2tch,dc=com"  
Enter LDAP Password: fenestros
```

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

Rafraîchissez phpLDAPadmin. Vous constaterez un résultat similaire à celui-ci :



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

```
[root@centos7 ~]# ldapdelete -x -M -D "cn=Manager,dc=i2tch,dc=com" -W "ou=Informatique,dc=i2tch,dc=com"  
Enter LDAP Password: fenestros
```

LAB #11 - 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@centos7 ~]# 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 **slapadd.ldif** et éditez-le ainsi :

```
[root@centos7 ~]# vi slapadd.ldif
[root@centos7 ~]# cat slapadd.ldif
dn: cn=dupois,ou=Production,ou=France,dc=i2tch,dc=com
objectClass: inetOrgPerson
objectClass: top
cn: dupois
sn: dupois
```

Arrêtez maintenant le service slapd :

```
[root@centos7 ~]# systemctl stop slapd
[root@centos7 ~]# systemctl status slapd
● slapd.service - OpenLDAP Server Daemon
  Loaded: loaded (/usr/lib/systemd/system/slapd.service; enabled; vendor preset: disabled)
  Active: inactive (dead) since Sun 2020-01-12 15:31:13 CET; 5s ago
    Docs: man:slapd
          man:slapd-config
          man:slapd-hdb
          man:slapd-mdb
          file:///usr/share/doc/openldap-servers/guide.html
   Process: 1061 ExecStart=/usr/sbin/slapd -u ldap -h ${SLAPD_URLS} $SLAPD_OPTIONS (code=exited, status=0/SUCCESS)
   Process: 923 ExecStartPre=/usr/libexec/openldap/check-config.sh (code=exited, status=0/SUCCESS)
 Main PID: 1077 (code=exited, status=0/SUCCESS)

Jan 12 15:27:38 centos7.fenestros.loc slapd[1077]: conn=1008 op=0 BIND dn="cn...
Jan 12 15:27:38 centos7.fenestros.loc slapd[1077]: conn=1008 op=0 RESULT tag=...
Jan 12 15:27:38 centos7.fenestros.loc slapd[1077]: conn=1008 op=1 DEL dn="ou=...
Jan 12 15:27:38 centos7.fenestros.loc slapd[1077]: conn=1008 op=1 RESULT tag=...
Jan 12 15:27:38 centos7.fenestros.loc slapd[1077]: conn=1008 op=2 UNBIND
Jan 12 15:27:38 centos7.fenestros.loc slapd[1077]: conn=1008 fd=11 closed
Jan 12 15:31:13 centos7.fenestros.loc slapd[1077]: daemon: shutdown requested...
Jan 12 15:31:13 centos7.fenestros.loc systemd[1]: Stopping OpenLDAP Server Da...
```

```
Jan 12 15:31:13 centos7.fenestros.loc slapd[1077]: slapd shutdown: waiting fo...
Jan 12 15:31:13 centos7.fenestros.loc systemd[1]: Stopped OpenLDAP Server Dae...
Hint: Some lines were ellipsized, use -l to show in full.
```

Saisissez maintenant la commande suivante :

```
[root@centos7 ~]# slapadd -b "dc=i2tch,dc=com" -l slapadd.ldif
#####
100.00% eta    none elapsed           none fast!
Closing DB...
```

Démarrez le service slapd :

```
[root@centos7 ~]# systemctl start slapd
[root@centos7 ~]# systemctl status slapd
● slapd.service - OpenLDAP Server Daemon
  Loaded: loaded (/usr/lib/systemd/system/slapd.service; enabled; vendor preset: disabled)
  Active: active (running) since Sun 2020-01-12 15:33:21 CET; 3s ago
    Docs: man:slapd
          man:slapd-config
          man:slapd-hdb
          man:slapd-mdb
          file:///usr/share/doc/openldap-servers/guide.html
   Process: 6693 ExecStart=/usr/sbin/slapd -u ldap -h ${SLAPD_URLS} $SLAPD_OPTIONS (code=exited, status=0/SUCCESS)
   Process: 6651 ExecStartPre=/usr/libexec/openldap/check-config.sh (code=exited, status=0/SUCCESS)
 Main PID: 6695 (slapd)
    CGroup: /system.slice/slapd.service
             └─6695 /usr/sbin/slapd -u ldap -h ldapi:/// ldap:///

Jan 12 15:33:21 centos7.fenestros.loc runuser[6679]: pam_unix(runuser:session...]
```

```
Jan 12 15:33:21 centos7.fenestros.loc runuser[6681]: pam_unix(runuser:session...]
Jan 12 15:33:21 centos7.fenestros.loc runuser[6683]: pam_unix(runuser:session...]
Jan 12 15:33:21 centos7.fenestros.loc runuser[6685]: pam_unix(runuser:session...]
Jan 12 15:33:21 centos7.fenestros.loc runuser[6687]: pam_unix(runuser:session...]
Jan 12 15:33:21 centos7.fenestros.loc runuser[6689]: pam_unix(runuser:session...]
```

```
Jan 12 15:33:21 centos7.fenestros.loc runuser[6691]: pam_unix(runuser:session...
Jan 12 15:33:21 centos7.fenestros.loc slapd[6693]: @(#) $OpenLDAP: slapd 2.4....
                                         mockbuild@x86-01.b...
Jan 12 15:33:21 centos7.fenestros.loc slapd[6695]: slapd starting
Jan 12 15:33:21 centos7.fenestros.loc systemd[1]: Started OpenLDAP Server Dae...
Hint: Some lines were ellipsized, use -l to show in full.
```

Rafraîchissez phpLDAPAdmin. Vous constaterez un résultat similaire à celui-ci :



LAB #12 - 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 :

```
[root@centos7 ~]# slapcat --help
slapcat: invalid option -- '-'
usage: slapcat [-v] [-d debuglevel] [-f configfile] [-F configdir] [-o <name>[=<value>]] [-c]
               [-g] [-n databasenumber | -b suffix] [-l ldiffile] [-a filter] [-s subtree] [-H url]
```

Saisissez donc les commandes suivantes :

```
[root@centos7 ~]# systemctl stop slapd
[root@centos7 ~]# slapcat -b "dc=i2tch,dc=com" -l backup.ldif
```

Consultez maintenant le contenu du fichier **bakcup.ldif** :

```
[root@centos7 ~]# cat backup.ldif
dn: dc=i2tch,dc=com
objectClass: dcObject
objectClass: organization
dc: i2tch
o: i2tch.com
description: Exemple
structuralObjectClass: organization
entryUUID: 7f60340c-c739-1039-9642-efd3014890db
creatorsName: cn=Manager,dc=i2tch,dc=com
createTimestamp: 20200109143851Z
entryCSN: 20200109143851.158182Z#000000#000#000000
modifiersName: cn=Manager,dc=i2tch,dc=com
modifyTimestamp: 20200109143851Z

dn: cn=Manager,dc=i2tch,dc=com
objectClass: organizationalRole
cn: Manager
description: Gestionnaire
structuralObjectClass: organizationalRole
entryUUID: 7f611b60-c739-1039-9643-efd3014890db
creatorsName: cn=Manager,dc=i2tch,dc=com
createTimestamp: 20200109143851Z
entryCSN: 20200109143851.164106Z#000000#000#000000
modifiersName: cn=Manager,dc=i2tch,dc=com
modifyTimestamp: 20200109143851Z

dn: ou=France,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: France
structuralObjectClass: organizationalUnit
```

```
entryUUID: a622df86-c739-1039-9644-efd3014890db
creatorsName: cn=Manager,dc=i2tch,dc=com
createTimestamp: 20200109143956Z
entryCSN: 20200109143956.187387Z#000000#000#000000
modifiersName: cn=Manager,dc=i2tch,dc=com
modifyTimestamp: 20200109143956Z
```

```
dn: ou=Commercial,ou=France,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Commercial
structuralObjectClass: organizationalUnit
entryUUID: a624e218-c739-1039-9645-efd3014890db
creatorsName: cn=Manager,dc=i2tch,dc=com
createTimestamp: 20200109143956Z
entryCSN: 20200109143956.200565Z#000000#000#000000
modifiersName: cn=Manager,dc=i2tch,dc=com
modifyTimestamp: 20200109143956Z
```

```
dn: ou=Recherche,ou=France,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Recherche
structuralObjectClass: organizationalUnit
entryUUID: a6253092-c739-1039-9646-efd3014890db
creatorsName: cn=Manager,dc=i2tch,dc=com
createTimestamp: 20200109143956Z
entryCSN: 20200109143956.202576Z#000000#000#000000
modifiersName: cn=Manager,dc=i2tch,dc=com
modifyTimestamp: 20200109143956Z
```

```
dn: ou=Production,ou=France,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
```

```
ou: Production
structuralObjectClass: organizationalUnit
entryUUID: a625d74a-c739-1039-9647-efd3014890db
creatorsName: cn=Manager,dc=i2tch,dc=com
createTimestamp: 20200109143956Z
entryCSN: 20200109143956.206843Z#000000#000#000000
modifiersName: cn=Manager,dc=i2tch,dc=com
modifyTimestamp: 20200109143956Z
```

```
dn: ou=Suisse,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Suisse
structuralObjectClass: organizationalUnit
entryUUID: a6261b24-c739-1039-9648-efd3014890db
creatorsName: cn=Manager,dc=i2tch,dc=com
createTimestamp: 20200109143956Z
entryCSN: 20200109143956.208581Z#000000#000#000000
modifiersName: cn=Manager,dc=i2tch,dc=com
modifyTimestamp: 20200109143956Z
```

```
dn: ou=Commercial,ou=Suisse,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Commercial
structuralObjectClass: organizationalUnit
entryUUID: a62660e8-c739-1039-9649-efd3014890db
creatorsName: cn=Manager,dc=i2tch,dc=com
createTimestamp: 20200109143956Z
entryCSN: 20200109143956.210367Z#000000#000#000000
modifiersName: cn=Manager,dc=i2tch,dc=com
modifyTimestamp: 20200109143956Z
```

```
dn: ou=USA,dc=i2tch,dc=com
```

```
objectClass: organizationalUnit
objectClass: top
ou: USA
structuralObjectClass: organizationalUnit
entryUUID: a626bca0-c739-1039-964a-efd3014890db
creatorsName: cn=Manager,dc=i2tch,dc=com
createTimestamp: 20200109143956Z
entryCSN: 20200109143956.212715Z#000000#000#000000
modifiersName: cn=Manager,dc=i2tch,dc=com
modifyTimestamp: 20200109143956Z
```

```
dn: ou=Commercial,ou=USA,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Commercial
structuralObjectClass: organizationalUnit
entryUUID: a626fc4c-c739-1039-964b-efd3014890db
creatorsName: cn=Manager,dc=i2tch,dc=com
createTimestamp: 20200109143956Z
entryCSN: 20200109143956.214345Z#000000#000#000000
modifiersName: cn=Manager,dc=i2tch,dc=com
modifyTimestamp: 20200109143956Z
```

```
dn: ou=Recherche,ou=USA,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Recherche
structuralObjectClass: organizationalUnit
entryUUID: a6274a12-c739-1039-964c-efd3014890db
creatorsName: cn=Manager,dc=i2tch,dc=com
createTimestamp: 20200109143956Z
entryCSN: 20200109143956.216336Z#000000#000#000000
modifiersName: cn=Manager,dc=i2tch,dc=com
modifyTimestamp: 20200109143956Z
```

```
dn: cn=Responsable Personnel,ou=France,dc=i2tch,dc=com
cn: Responsable Personnel
aliasedObjectName: cn=Directeur,ou=France,dc=i2tch,dc=com
objectClass: top
objectClass: alias
objectClass: extensibleObject
structuralObjectClass: alias
entryUUID: bbb6f964-c7d3-1039-905e-0bb7ee6decc3
creatorsName: cn=Manager,dc=i2tch,dc=com
createTimestamp: 20200110090254Z
entryCSN: 20200110090254.886500Z#000000#000#000000
modifiersName: cn=Manager,dc=i2tch,dc=com
modifyTimestamp: 20200110090254Z
```

```
dn: cn=directeur,ou=France,dc=i2tch,dc=com
objectClass: person
objectClass: top
cn: directeur
sn: Guillaud
telephoneNumber: 12345678
telephoneNumber: 87654321
structuralObjectClass: person
entryUUID: c0bba43a-c7da-1039-9f6f-31eb8911c0ef
creatorsName: cn=Manager,dc=i2tch,dc=com
createTimestamp: 20200110095309Z
entryCSN: 20200110095309.782800Z#000000#000#000000
modifiersName: cn=Manager,dc=i2tch,dc=com
modifyTimestamp: 20200110095309Z
```

```
dn: ou=Angleterre,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Angleterre
structuralObjectClass: organizationalUnit
```

```
entryUUID: 95e2dba6-c7e0-1039-9f70-31eb8911c0ef
creatorsName: cn=Manager,dc=i2tch,dc=com
createTimestamp: 20200110103454Z
entryCSN: 20200110103454.878156Z#000000#000#000000
modifiersName: cn=Manager,dc=i2tch,dc=com
modifyTimestamp: 20200110103454Z

dn: ou=Sales,ou=Angleterre,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Sales
structuralObjectClass: organizationalUnit
entryUUID: 95e965d4-c7e0-1039-9f71-31eb8911c0ef
creatorsName: cn=Manager,dc=i2tch,dc=com
createTimestamp: 20200110103454Z
entryCSN: 20200110103454.921008Z#000000#000#000000
modifiersName: cn=Manager,dc=i2tch,dc=com
modifyTimestamp: 20200110103454Z

dn: cn=Sales Director,ou=Sales,ou=Angleterre,dc=i2tch,dc=com
objectClass: person
objectClass: top
cn: Sales Director
sn: Smith
structuralObjectClass: person
entryUUID: 95f02de2-c7e0-1039-9f72-31eb8911c0ef
creatorsName: cn=Manager,dc=i2tch,dc=com
createTimestamp: 20200110103454Z
entryCSN: 20200110103454.965453Z#000000#000#000000
modifiersName: cn=Manager,dc=i2tch,dc=com
modifyTimestamp: 20200110103454Z

dn: cn=Sales Manager,cn=Sales Director,ou=Sales,ou=Angleterre,dc=i2tch,dc=co
m
```

```
objectClass: person
objectClass: top
cn: Sales Manager
sn: Brown
structuralObjectClass: person
entryUUID: 95f62710-c7e0-1039-9f73-31eb8911c0ef
creatorsName: cn=Manager,dc=i2tch,dc=com
createTimestamp: 20200110103455Z
entryCSN: 20200110103455.004608Z#000000#000#000000
modifiersName: cn=Manager,dc=i2tch,dc=com
modifyTimestamp: 20200110103455Z
```

```
dn: cn=mail,ou=Commercial,ou=France,dc=i2tch,dc=com
objectClass: inetOrgPerson
objectClass: person
objectClass: top
cn: mail
mail: info@i2tch.com
sn: info
structuralObjectClass: inetOrgPerson
entryUUID: aa1bfccb0-c808-1039-900b-092b75c3c5a4
creatorsName: cn=Manager,dc=i2tch,dc=com
createTimestamp: 20200110152148Z
entryCSN: 20200110152148.676173Z#000000#000#000000
modifiersName: cn=Manager,dc=i2tch,dc=com
modifyTimestamp: 20200110152148Z
```

```
dn: cn=dupond,ou=Recherche,ou=France,dc=i2tch,dc=com
objectClass: inetOrgPerson
objectClass: top
cn: dupond
sn: dupond
structuralObjectClass: inetOrgPerson
entryUUID: 96de82d0-c97f-1039-92ab-977e121b768c
```

```
creatorsName: cn=Manager,dc=i2tch,dc=com
createTimestamp: 20200112120537Z
mail: dupond@i2tch.com
entryCSN: 20200112121812.106114Z#000000#000#000000
modifiersName: cn=Manager,dc=i2tch,dc=com
modifyTimestamp: 20200112121812Z

dn: cn=dupois,ou=Production,ou=France,dc=i2tch,dc=com
objectClass: inetOrgPerson
objectClass: top
cn: dupois
sn: dupois
structuralObjectClass: inetOrgPerson
entryUUID: 066ceaf6-c994-1039-8f6f-ab1664534830
creatorsName: cn=Manager,dc=i2tch,dc=com
createTimestamp: 20200112143154Z
entryCSN: 20200112143154.765140Z#000000#000#000000
modifiersName: cn=Manager,dc=i2tch,dc=com
modifyTimestamp: 20200112143154Z
```

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 :

```
[root@centos7 ~]# slapindex --help
slapindex: invalid option -- '-'
usage: slapindex [-v] [-d debuglevel] [-f configfile] [-F configdir] [-o <name>[=<value>]] [-c]
                 [-g] [-n databasenumber | -b suffix] [attr ...] [-q] [-t]
```

Saisissez donc la commande suivante :

```
[root@centos7 ~]# slapindex -b "dc=i2tch,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 :

```
[root@centos7 ~]# slapdn --help
slapdn: invalid option -- '-'
usage: slapdn [-v] [-d debuglevel] [-f configfile] [-F configdir] [-o <name>[=<value>]]
              [-N | -P] DN [...]
```

Saisissez donc la commande suivante :

```
[root@centos7 ~]# slapdn cn=smith,dc=i2tch,dc=com
DN: <cn=smith,dc=i2tch,dc=com> check succeeded
normalized: <cn=smith,dc=i2tch,dc=com>
pretty:      <cn=smith,dc=i2tch,dc=com>
```

La commande **slaptest**

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

Les options de cette commande sont :

```
[root@centos7 ~]# slaptest --help
slaptest: invalid option -- '-'
usage: slaptest [-v] [-d debuglevel] [-f configfile] [-F configdir] [-o <name>[=<value>]] [-n databasenumber] [-u] [-Q]
```

Saisissez donc la commande suivante :

```
[root@centos7 ~]# slaptest -u
config file testing succeeded
```

La commande **slapauth**

La commande **slapauth** vérifie la correspondance entre les ID et les DN.

Les options de cette commande sont :

```
root@centos7 ~]# slapauth --help
slapauth: invalid option -- '-'
```

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

Saisissez donc la commande suivante :

```
[root@centos7 ~]# 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@centos7 ~]# systemctl start slapd  
[root@centos7 ~]# systemctl status slapd  
● slapd.service - OpenLDAP Server Daemon  
  Loaded: loaded (/usr/lib/systemd/system/slapd.service; enabled; vendor preset: disabled)  
  Active: active (running) since Sun 2020-01-12 15:50:26 CET; 5s ago  
    Docs: man:slapd  
          man:slapd-config  
          man:slapd-hdb  
          man:slapd-mdb  
          file:///usr/share/doc/openldap-servers/guide.html  
  Process: 11958 ExecStart=/usr/sbin/slappd -u ldap -h ${SLAPD_URLS} $SLAPD_OPTIONS (code=exited,  
  status=0/SUCCESS)  
  Process: 11915 ExecStartPre=/usr/libexec/openldap/check-config.sh (code=exited, status=0/SUCCESS)  
 Main PID: 11966 (slapd)  
 CGroup: /system.slice/slappd.service
```

```
└─11966 /usr/sbin/slapd -u ldap -h ldapi:/// ldap:///  
  
Jan 12 15:50:26 centos7.fenestros.loc runuser[11943]: pam_unix(runuser:session): session opened for user runuser by (uid=0)  
Jan 12 15:50:26 centos7.fenestros.loc runuser[11945]: pam_unix(runuser:session): session opened for user runuser by (uid=0)  
Jan 12 15:50:26 centos7.fenestros.loc runuser[11947]: pam_unix(runuser:session): session opened for user runuser by (uid=0)  
Jan 12 15:50:26 centos7.fenestros.loc runuser[11949]: pam_unix(runuser:session): session opened for user runuser by (uid=0)  
Jan 12 15:50:26 centos7.fenestros.loc runuser[11951]: pam_unix(runuser:session): session opened for user runuser by (uid=0)  
Jan 12 15:50:26 centos7.fenestros.loc runuser[11953]: pam_unix(runuser:session): session opened for user runuser by (uid=0)  
Jan 12 15:50:26 centos7.fenestros.loc runuser[11955]: pam_unix(runuser:session): session opened for user runuser by (uid=0)  
Jan 12 15:50:26 centos7.fenestros.loc slapd[11958]: @(#) $OpenLDAP: slapd 2.4...  
                                              mockbuild@x86-01....  
Jan 12 15:50:26 centos7.fenestros.loc slapd[11966]: slapd starting  
Jan 12 15:50:26 centos7.fenestros.loc systemd[1]: Started OpenLDAP Server Dae...  
Hint: Some lines were ellipsized, use -l to show in full.
```

LAB #13 - Importer les Machines Virtuelles pour la Replication

Importez les machines virtuelles **ldapmaster** et **ldapslave**.

Ces deux machines doivent être mises dans le réseau NAT **NatNetwork**.

Dans la fenêtre de VirtualBox, créez le réseau NAT **NatNetwork** :

Fichier > Paramètres > Réseau > bouton + > OK

Configurez les cartes réseaux pour les machines virtuelles **CentOS_7** et **Debian_10** en “NatNetwork”.

Machine > Configuration > Réseau > Mode d'accès réseau > NatNetwork

Créez les redirections de ports dans le réseau NAT **NatNetwork** de VirtualBox :

Fichier > Paramètres > Réseau > NatNetwork > Redirection de ports

Nom	Protocole	IP hôte	Port hôte	IP invité	Port invité
master	TCP	127.0.0.1	3022	10.0.2.15	22
slave	TCP	127.0.0.1	4022	10.0.2.16	22

Démarrez les deux machines virtuelles.

Connectez-vous à chaque machine virtuelle en SSH :

Machine	IP	Port
master	127.0.0.1	3022
slave	127.0.0.1	4022

Vérifiez votre configuration dans les deux machines **ldapmaster** et **ldapslave** :

```
[root@master ~]# ldapsearch -xLLL
dn: dc=i2tch,dc=com
objectClass: dcObject
objectClass: organization
dc: i2tch
o: i2tch.com
description: Exemple

dn: cn=Manager,dc=i2tch,dc=com
objectClass: organizationalRole
cn: Manager
description: Gestionnaire

dn: ou=France,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: France

dn: ou=Commercial,ou=France,dc=i2tch,dc=com
objectClass: organizationalUnit
```

```
objectClass: top
ou: Commercial

dn: ou=Recherche,ou=France,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Recherche

dn: ou=Production,ou=France,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Production

dn: ou=Suisse,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Suisse

dn: ou=Commercial,ou=Suisse,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Commercial

dn: ou=USA,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: USA

dn: ou=Commercial,ou=USA,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Commercial

dn: ou=Recherche,ou=USA,dc=i2tch,dc=com
```

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

dn: cn=Responsable Personnel,ou=France,dc=i2tch,dc=com
cn: Responsable Personnel
aliasedObjectName: cn=Directeur,ou=France,dc=i2tch,dc=com
objectClass: top
objectClass: alias
objectClass: extensibleObject

dn: cn=directeur,ou=France,dc=i2tch,dc=com
objectClass: person
objectClass: top
cn: directeur
sn: Guillaud
telephoneNumber: 12345678
telephoneNumber: 87654321

dn: ou=Angleterre,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Angleterre

dn: ou=Sales,ou=Angleterre,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Sales

dn: cn=Sales Director,ou=Sales,ou=Angleterre,dc=i2tch,dc=com
objectClass: person
objectClass: top
cn: Sales Director
sn: Smith
```

```
dn: cn=Sales Manager,cn=Sales Director,ou=Sales,ou=Angleterre,dc=i2tch,dc=com
objectClass: person
objectClass: top
cn: Sales Manager
sn: Brown
```

```
dn: cn=mail,ou=Commercial,ou=France,dc=i2tch,dc=com
objectClass: inetOrgPerson
objectClass: person
objectClass: top
cn: mail
mail: info@i2tch.com
sn: info
```

```
dn: cn=dupond,ou=Recherche,ou=France,dc=i2tch,dc=com
objectClass: inetOrgPerson
objectClass: top
cn: dupond
sn: dupond
mail: dupond@i2tch.com
```

```
dn: cn=dupois,ou=Production,ou=France,dc=i2tch,dc=com
objectClass: inetOrgPerson
objectClass: top
cn: dupois
sn: dupois
```

```
[root@slave ~]# ldapsearch -xLLL
dn: dc=i2tch,dc=com
objectClass: dcObject
objectClass: organization
dc: i2tch
o: i2tch.com
description: Exemple
```

```
dn: cn=Manager,dc=i2tch,dc=com
objectClass: organizationalRole
cn: Manager
description: Gestionnaire

dn: ou=France,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: France

dn: ou=Commercial,ou=France,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Commercial

dn: ou=Recherche,ou=France,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Recherche

dn: ou=Production,ou=France,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Production

dn: ou=Suisse,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Suisse

dn: ou=Commercial,ou=Suisse,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Commercial
```

```
dn: ou=USA,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: USA

dn: ou=Commercial,ou=USA,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Commercial

dn: ou=Recherche,ou=USA,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Recherche

dn: cn=Responsable Personnel,ou=France,dc=i2tch,dc=com
cn: Responsable Personnel
aliasedObjectName: cn=Directeur,ou=France,dc=i2tch,dc=com
objectClass: top
objectClass: alias
objectClass: extensibleObject

dn: cn=directeur,ou=France,dc=i2tch,dc=com
objectClass: person
objectClass: top
cn: directeur
sn: Guillaud
telephoneNumber: 12345678
telephoneNumber: 87654321

dn: ou=Angleterre,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Angleterre
```

```
dn: ou=Sales,ou=Angleterre,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Sales
```

```
dn: cn=Sales Director,ou=Sales,ou=Angleterre,dc=i2tch,dc=com
objectClass: person
objectClass: top
cn: Sales Director
sn: Smith
```

```
dn: cn=Sales Manager,cn=Sales Director,ou=Sales,ou=Angleterre,dc=i2tch,dc=com
objectClass: person
objectClass: top
cn: Sales Manager
sn: Brown
```

```
dn: cn=mail,ou=Commercial,ou=France,dc=i2tch,dc=com
objectClass: inetOrgPerson
objectClass: person
objectClass: top
cn: mail
mail: info@i2tch.com
sn: info
```

```
dn: cn=dupond,ou=Recherche,ou=France,dc=i2tch,dc=com
objectClass: inetOrgPerson
objectClass: top
cn: dupond
sn: dupond
mail: dupond@i2tch.com
```

```
dn: cn=dupois,ou=Production,ou=France,dc=i2tch,dc=com
objectClass: inetOrgPerson
```

```
objectClass: top
cn: dupois
sn: dupois
```

Important - Dans ce cas les deux machines possèdent un DIT identique.

LAB #14 - Sauvegarde et Restauration

Dans le cas où les deux machines ne contiennent pas de DIT identique, il convient de dupliquer le DIT du master dans l'esclave.

Retournez à la machine virtuelle **Idapmaster**.

Sauvegardez les données de la configuration :

```
[root@master ~]# slapcat -b cn=config > save_config.ldif
```

Sauvegardez les données de la configuration :

```
[root@master ~]# slapcat -b dc=i2tch,dc=com > save_data.ldif
```

Transférez les deux fichiers à la machine virtuelle **Idapslave** :

```
[root@master ~]# scp save_*.ldif trainee@10.0.2.16:/tmp
The authenticity of host '10.0.2.16 (10.0.2.16)' can't be established.
ECDSA key fingerprint is SHA256:Rg0sp/XI7JHNq+oIfHKw+jkHdtTnBIh+Dd7kVmHRxtU.
ECDSA key fingerprint is MD5:19:cd:05:58:af:2c:10:82:52:ba:e3:31:df:bd:72:54.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.0.2.16' (ECDSA) to the list of known hosts.
trainee@10.0.2.16's password:
```

```
save_config.ldif
100% 55KB 10.9MB/s 00:00
save_data.ldif
100% 8118 2.8MB/s 00:00
```

Retournez à la machine virtuelle **Idapslave** et arrêtez le service **slapd** :

```
[root@slave ~]# systemctl stop slapd
```

Supprimez la configuration existante :

```
[root@slave ~]# rm -rf /etc/openldap/slapd.d/*
```

Injectez la sauvegarde de la configuration en provenance de la machine virtuelle **master** :

```
[root@slave ~]# slapadd -F /etc/openldap/slapd.d -b cn=config -l /tmp/save_config.ldif
#####
# 100.00% eta    none elapsed          none fast!
Closing DB...
```

Modifiez le propriétaire et le groupe :

```
root@debian10:~# chown -R ldap:ldap /etc/openldap/slapd.d/
```

Supprimez maintenant les données existantes :

```
[root@slave ~]# rm -rf /var/lib/ldap/*
```

Injectez la sauvegarde des données en provenance de la machine virtuelle **master** :

```
[root@slave ~]# slapadd -b dc=i2tch,dc=com -l /tmp/save_data.ldif
5e1c9ee9 hdb_db_open: warning - no DB_CONFIG file found in directory /var/lib/ldap: (2).
Expect poor performance for suffix "dc=i2tch,dc=com".
#####
# 100.00% eta    none elapsed          none fast!
```

Closing DB...

Important - Notez l'avertissement concernant le fichier DB_CONFIG.

Remettez en place donc ce fichier :

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

Modifiez le propriétaire et le groupe :

```
root@debian10:~# chown -R ldap:ldap /var/lib/ldap/
```

Ré-indexez la base de données :

```
[root@slave ~]# slapindex  
5e1ca06f The first database does not allow slapindex; using the first available one (2)
```

Démarrez le serveur OpenLDAP :

```
[root@slave ~]# systemctl start slapd
```

Vérifiez les restaurations :

```
[root@slave ~]# ldapsearch -xLLL | more  
dn: dc=i2tch,dc=com  
objectClass: dcObject  
objectClass: organization  
dc: i2tch  
o: i2tch.com  
description: Exemple
```

```
dn: cn=Manager,dc=i2tch,dc=com
objectClass: organizationalRole
cn: Manager
description: Gestionnaire

dn: ou=France,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: France

dn: ou=Commercial,ou=France,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Commercial

dn: ou=Recherche,ou=France,dc=i2tch,dc=com
--More--
```

LAB #15 - 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. La fonctionnalité **syncrepl** fournit la réPLICATION :

- maître - esclave,
- maître - maître.

Le **consommateur** initie la réPLICATION soit en prenant les mises à jour du fournisseur, processus appelé **refreshOnly**, soit en demandant au fournisseur de fournir les mises à jour d'une manière périodique, processus appelé **refreshAndPersist**.

Pour que **syncrepl** fonctionne, il faut que l'Overlay **syncprov** soit chargé dans les deux serveurs.

Activation de l'Overlay Syncprov

Créez le fichier **syncrepl.ldif** suivant dans les machines virtuelles **ldapmaster** et **ldapslave** :

```
[root@master ~]# vi syncrepl.ldif
[root@master ~]# cat syncrepl.ldif
dn: cn=module,cn=config
cn: module
objectclass: olcModuleList
objectclass: top
olcmoduleload: syncprov.la
olcmodulepath: /usr/lib/ldap
```

```
[root@slave ~]# vi syncrepl.ldif
[root@slave ~]# cat syncrepl.ldif
dn: cn=module,cn=config
cn: module
objectclass: olcModuleList
objectclass: top
olcmoduleload: syncprov.la
olcmodulepath: /usr/lib/ldap
```

Injectez la configuration dans chaque machine :

```
[root@slave ~]# ldapadd -Y EXTERNAL -H ldapi:/// -f syncrepl.ldif
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
adding new entry "cn=module,cn=config"
```

```
[root@slave ~]# ldapadd -Y EXTERNAL -H ldapi:/// -f syncrepl.ldif
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
```

```
SASL SSF: 0
adding new entry "cn=module,cn=config"
```

Vérifiez la mise en place de la configuration :

```
[root@master ~]# ldapsearch -LLL external -H ldapi:/// -b "cn=config" "objectClass=olcModuleList"
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
dn: cn=module{0},cn=config
objectClass: olcModuleList
objectClass: top
cn: module{0}
olcModulePath: /usr/lib64/openldap
olcModuleLoad: {0}syncprov.la
```

```
[root@slave ~]# ldapsearch -LLL external -H ldapi:/// -b "cn=config" "objectClass=olcModuleList"
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
dn: cn=module{0},cn=config
objectClass: olcModuleList
objectClass: top
cn: module{0}
olcModulePath: /usr/lib64/openldap
olcModuleLoad: {0}syncprov.la
```

Modification du ServerID

Chaque serveur homologue doit être identifié par une entrée **olcServerID** différente. Créez donc les fichiers **serverid.Idif** suivants dans **Idapmaster** et **Idapslave** respectivement :

```
[root@master ~]# vi serverid.ldif
[root@master ~]# cat serverid.ldif
dn: cn=config
changetype: modify
add: olcServerID
olcServerID: 1
```

```
[root@slave ~]# vi serverid.ldif
[root@slave ~]# cat serverid.ldif
dn: cn=config
changetype: modify
add: olcServerID
olcServerID: 2
```

Injectez la configuration dans chaque machine :

```
[root@master ~]# ldapadd -Y EXTERNAL -H ldapi:/// -f serverid.ldif
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
modifying entry "cn=config"
```

```
[root@slave ~]# ldapadd -Y EXTERNAL -H ldapi:/// -f serverid.ldif
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
modifying entry "cn=config"
```

Vérifiez la mise en place de la configuration :

```
[root@master ~]# ldapsearch -LLL external -H ldapi:/// -b "cn=config" "objectClass=olcGlobal" olcServerID
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
```

```
SASL SSF: 0
dn: cn=config
olcServerID: 1
```

```
[root@slave ~]# ldapsearch -LLL external -H ldapi:/// -b "cn=config" "objectClass=olcGlobal" olcServerID
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
dn: cn=config
olcServerID: 2
```

Création d'un Fichier de Mot de Passe de l'Administrateur

Afin d'éviter de passer le mot de passe de l'administrateur d'OpenLDAP sur la ligne de commande, créez le fichier **/root/passwdldap** dans chaque machine virtuelle :

```
[root@master ~]# echo -n "fenestros" > /root/passwdldap
[root@master ~]# chmod 600 /root/passwdldap
```

```
[root@slave ~]# echo -n "fenestros" > /root/passwdldap
[root@slave ~]# chmod 600 /root/passwdldap
```

Création d'un Utilisateur pour la RéPLICATION

Créez le fichier **repuser.ldif** suivant dans les machines virtuelles **ldapmaster** et **ldapslave** :

```
[root@master ~]# vi repuser.ldif
[root@master ~]# cat repuser.ldif
dn: ou=system,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
```

```
ou: system
```

```
dn: cn=replicant,ou=system,dc=i2tch,dc=com
userPassword: password
cn: replicant
objectclass: top
objectclass: person
sn: replicant
```

```
[root@slave ~]# vi repuser.ldif
[root@slave ~]# cat repuser.ldif
dn: ou=system,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: system

dn: cn=replicant,ou=system,dc=i2tch,dc=com
userPassword: password
cn: replicant
objectclass: top
objectclass: person
sn: replicant
```

Injectez la configuration dans chaque machine :

```
[root@master ~]# ldapadd -x -H ldap://localhost -D cn=Manager,dc=i2tch,dc=com -y /root/passwdldap -f repuser.ldif
adding new entry "ou=system,dc=i2tch,dc=com"

adding new entry "cn=replicant,ou=system,dc=i2tch,dc=com"
```

```
[root@slave ~]# ldapadd -x -H ldap://localhost -D cn=Manager,dc=i2tch,dc=com -y /root/passwdldap -f repuser.ldif
adding new entry "ou=system,dc=i2tch,dc=com"
```

```
adding new entry "cn=replicant,ou=system,dc=i2tch,dc=com"
```

Authorisation des Modifications de la Configuration d'OpenLDAP

Il est maintenant nécessaire d'autoriser des modifications de la configuration d'OpenLDAP par l'utilisateur **cn=replicant,ou=system,dc=i2tch,dc=com**.

ACLs

Créez le fichier **acls.ldif** dans les machines virtuelles **ldapmaster** et **ldapslave** :

```
[root@master ~]# vi acls.ldif
[root@master ~]# cat acls.ldif
dn: olcDatabase={0}config,cn=config
changeType: modify
add: olcAccess
olcAccess: to * by dn.exact=cn=replicant,ou=system,dc=i2tch,dc=com manage by * break
```

```
[root@slave ~]# vi acls.ldif
[root@slave ~]# cat acls.ldif
dn: olcDatabase={0}config,cn=config
changeType: modify
add: olcAccess
olcAccess: to * by dn.exact=cn=replicant,ou=system,dc=i2tch,dc=com manage by * break
```

Injectez la configuration dans chaque machine :

```
[root@master ~]# ldapmodify -Y EXTERNAL -H ldapi:/// -f acls.ldif
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
```

```
modifying entry "olcDatabase={0}config,cn=config"

[root@slave ~]# ldapmodify -Y EXTERNAL -H ldapi:/// -f acls.ldif
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
modifying entry "olcDatabase={0}config,cn=config"
```

Configuration

Créez le fichier **configuration.ldif** dans les machines virtuelles **ldapmaster** et **ldapslave** :

```
[root@master ~]# vi configuration.ldif
[root@master ~]# cat configuration.ldif
dn: olcOverlay=syncprov,olcDatabase={0}config,cn=config
changetype: add
objectClass: olcOverlayConfig
objectClass: olcSyncProvConfig
olcOverlay: syncprov
```

```
[root@master ~]# vi configuration.ldif
[root@master ~]# cat configuration.ldif
dn: olcOverlay=syncprov,olcDatabase={0}config,cn=config
changetype: add
objectClass: olcOverlayConfig
objectClass: olcSyncProvConfig
olcOverlay: syncprov
```

Injectez la configuration dans chaque machine :

```
[root@master ~]# ldapmodify -Y EXTERNAL -H ldapi:/// -f configuration.ldif
SASL/EXTERNAL authentication started
```

```
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
adding new entry "olcOverlay=syncprov,olcDatabase={0}config,cn=config"
```

```
[root@slave ~]# ldapmodify -Y EXTERNAL -H ldapi:/// -f configuration.ldif
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
adding new entry "olcOverlay=syncprov,olcDatabase={0}config,cn=config"
```

Paramétrage

Créez le fichier **settings.ldif** dans les machines virtuelles **ldapmaster** et **ldapslave** :

```
[root@master ~]# vi settings.ldif
[root@master ~]# cat settings.ldif
dn: olcDatabase={0}config,cn=config
changetype: modify
add: olcSyncRepl
olcSyncRepl: rid=01 provider=ldap://10.0.2.15
  binddn="cn=replicant,ou=system,dc=i2tch,dc=com" bindmethod=simple
  credentials=password searchbase="cn=config"
  type=refreshAndPersist retry="5 5 300 5" timeout=1
olcSyncRepl: rid=02 provider=ldap://10.0.2.16
  binddn="cn=replicant,ou=system,dc=i2tch,dc=com" bindmethod=simple
  credentials=password searchbase="cn=config"
  type=refreshAndPersist retry="5 5 300 5" timeout=1
-
add: olcMirrorMode
olcMirrorMode: TRUE
```

```
[root@slave ~]# vi settings.ldif
```

```
[root@slave ~]# cat settings.ldif
dn: olcDatabase={0}config,cn=config
changetype: modify
add: olcSyncRepl
olcSyncRepl: rid=01 provider=ldap://10.0.2.15
  binddn="cn=replicant,ou=system,dc=i2tch,dc=com" bindmethod=simple
  credentials=password searchbase="cn=config"
  type=refreshAndPersist retry="5 5 300 5" timeout=1
olcSyncRepl: rid=02 provider=ldap://10.0.2.16
  binddn="cn=replicant,ou=system,dc=i2tch,dc=com" bindmethod=simple
  credentials=password searchbase="cn=config"
  type=refreshAndPersist retry="5 5 300 5" timeout=1
-
add: olcMirrorMode
olcMirrorMode: TRUE
```

Injectez la configuration dans chaque machine :

```
[root@master ~]# ldapmodify -Y EXTERNAL -H ldapi:/// -f settings.ldif
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
modifying entry "olcDatabase={0}config,cn=config"
```

```
[root@slave ~]# ldapmodify -Y EXTERNAL -H ldapi:/// -f settings.ldif
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
modifying entry "olcDatabase={0}config,cn=config"
```

Vérification du Fonctionnement de la RéPLICATION

Vérifiez la configuration :

```
[root@master ~]# ldapsearch -QLLY external -H ldapi:/// -b "cn=config" "olcDatabase={0}config" olcSyncRepl
dn: olcDatabase={0}config,cn=config
olcSyncrepl: {0}rid=01 provider=ldap://10.0.2.15 binddn="cn=replicant,ou=syste
m,dc=i2tch,dc=com" bindmethod=simple credentials=password searchbase="cn=conf
ig" type=refreshAndPersist retry="5 5 300 5" timeout=1
olcSyncrepl: {1}rid=02 provider=ldap://10.0.2.16 binddn="cn=replicant,ou=syste
m,dc=i2tch,dc=com" bindmethod=simple credentials=password searchbase="cn=conf
ig" type=refreshAndPersist retry="5 5 300 5" timeout=1
```

```
[root@slave ~]# ldapsearch -QLLY external -H ldapi:/// -b "cn=config" "olcDatabase={0}config" olcSyncRepl
dn: olcDatabase={0}config,cn=config
olcSyncrepl: {0}rid=01 provider=ldap://10.0.2.15 binddn="cn=replicant,ou=syste
m,dc=i2tch,dc=com" bindmethod=simple credentials=password searchbase="cn=conf
ig" type=refreshAndPersist retry="5 5 300 5" timeout=1
olcSyncrepl: {1}rid=02 provider=ldap://10.0.2.16 binddn="cn=replicant,ou=syste
m,dc=i2tch,dc=com" bindmethod=simple credentials=password searchbase="cn=conf
ig" type=refreshAndPersist retry="5 5 300 5" timeout=1
```

Créez le fichier LDIF **director.ldif** et éditez-le ainsi :

```
[root@master ~]# vi director.ldif
[root@master ~]# cat director.ldif
version: 1
dn: cn=director,ou=Angleterre,dc=i2tch,dc=com
objectClass: person
objectClass: top
cn: director
sn: Smith
telephoneNumber: 11111111
telephoneNumber: 99999999
```

Injectez la configuration dans la machine **Idapmaster** :

```
[root@master ~]# ldapadd -x -H ldap://localhost -D cn=Manager,dc=i2tch,dc=com -y /root/passwdldap -f director.ldif
adding new entry "cn=director,ou=Angleterre,dc=i2tch,dc=com"
```

Vérifiez que l'ajout de l'utilisateur s'est déroulé correctement dans la machine **ldapmaster** :

```
[root@master log]# ldapsearch -x -LLL -S ou -s children -u -b "ou=Angleterre,dc=i2tch,dc=com"
dn: cn=Sales Director,ou=Sales,ou=Angleterre,dc=i2tch,dc=com
ufn: Sales Director, Sales, Angleterre, i2tch.com
objectClass: person
objectClass: top
cn: Sales Director
sn: Smith

dn: cn=Sales Manager,cn=Sales Director,ou=Sales,ou=Angleterre,dc=i2tch,dc=com
ufn: Sales Manager, Sales Director, Sales, Angleterre, i2tch.com
objectClass: person
objectClass: top
cn: Sales Manager
sn: Brown

dn: cn=director,ou=Angleterre,dc=i2tch,dc=com
ufn: director, Angleterre, i2tch.com
objectClass: person
objectClass: top
cn: director
sn: Smith
telephoneNumber: 11111111
telephoneNumber: 99999999

dn: ou=Sales,ou=Angleterre,dc=i2tch,dc=com
ufn: Sales, Angleterre, i2tch.com
objectClass: organizationalUnit
objectClass: top
```

ou: Sales

Dernièrement, vérifiez que la réPLICATION fonctionne :

```
[root@slave ~]# ldapsearch -x -LLL -S ou -s children -u -b "ou=Angleterre,dc=i2tch,dc=com"
dn: cn=Sales Director,ou=Sales,ou=Angleterre,dc=i2tch,dc=com
ufn: Sales Director, Sales, Angleterre, i2tch.com
objectClass: person
objectClass: top
cn: Sales Director
sn: Smith

dn: cn=Sales Manager,cn=Sales Director,ou=Sales,ou=Angleterre,dc=i2tch,dc=com
ufn: Sales Manager, Sales Director, Sales, Angleterre, i2tch.com
objectClass: person
objectClass: top
cn: Sales Manager
sn: Brown

dn: cn=director,ou=Angleterre,dc=i2tch,dc=com
ufn: director, Angleterre, i2tch.com
objectClass: person
objectClass: top
cn: director
sn: Smith
telephoneNumber: 11111111
telephoneNumber: 99999999

dn: ou=Sales,ou=Angleterre,dc=i2tch,dc=com
ufn: Sales, Angleterre, i2tch.com
objectClass: organizationalUnit
objectClass: top
ou: Sales
```

<html>

Copyright © 2020 Hugh Norris.

</html>