Version : **2021.01**

Dernière mise-à-jour : 2021/02/03 14:30

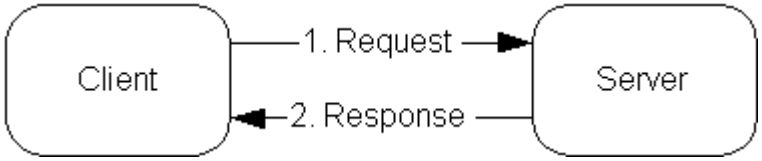
SER702 - Configuration d'un serveur OpenLDAP

Contenu du Module

Présentation

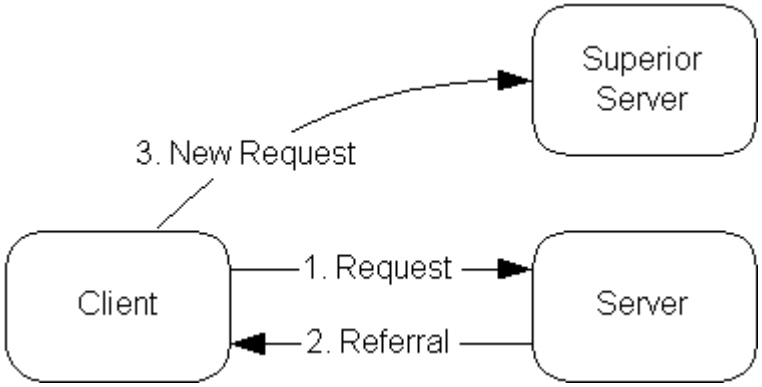
Le choix de la configuration de l'annuaire se fait en fonction de l'organisation de l'entité dont il détient l'information. Plusieurs configurations sont possible.

L'annuaire Local



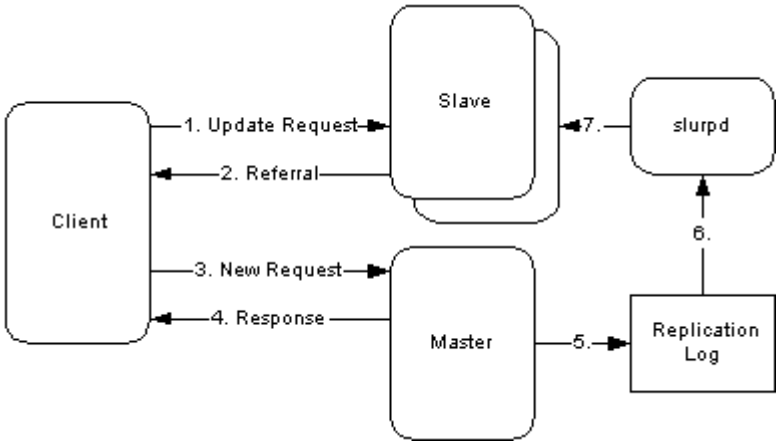
Dans ce cas, le service d'annuaire ne concerne que le domaine local. Il n'y a aucune interaction avec d'autres annuaires.

L''annuaire Local avec des Referrals



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

L'annuaire local avec réplication



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

Configuration des Versions Antérieures à la 2.3

La configuration d'OpenLDAP ést 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_ssf=112 simple_bind=64

# Sample access control policy:
#   Root DSE: allow anyone to read it
#   Subschema (sub)entry DSE: allow anyone to read it
#   Other DSEs:
#       Allow self write access
#       Allow authenticated users read access
```

```
#       Allow anonymous users to authenticate
#   Directives needed to implement policy:
# access to dn.base="" by * read
# access to dn.base="cn=Subschema" by * read
# access to *
#   by self write
#   by users read
#   by anonymous auth
#
# if no access controls are present, the default policy
# allows anyone and everyone to read anything but restricts
# updates to rootdn.  (e.g., "access to * by * read")
#
# rootdn can always read and write EVERYTHING!

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

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

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

database    bdb
suffix      "dc=my-domain,dc=com"
```

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

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

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

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

Les directives actives sont :

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

```
include     /etc/openldap/schema/java.schema
include     /etc/openldap/schema/misc.schema
include     /etc/openldap/schema/nis.schema
include     /etc/openldap/schema/openldap.schema
include     /etc/openldap/schema/ppolicy.schema
include     /etc/openldap/schema/collective.schema
allow bind_v2
pidfile     /var/run/openldap/slapd.pid
argsfile    /var/run/openldap/slapd.args
TLSCACertificatePath /etc/openldap/certs
TLSCertificateFile "\"OpenLDAP Server\""
TLSCertificateKeyFile /etc/openldap/certs/password
database config
access to *
    by dn.exact="gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth" manage
    by * none
database monitor
access to *
    by dn.exact="gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth" read
        by dn.exact="cn=Manager,dc=my-domain,dc=com" read
        by * none
database    bdb
suffix      "dc=my-domain,dc=com"
checkpoint  1024 15
rootdn      "cn=Manager,dc=my-domain,dc=com"
directory   /var/lib/ldap
index objectClass                       eq,pres
index ou,cn,mail,surname,givenname      eq,pres,sub
index uidNumber,gidNumber,loginShell    eq,pres
index uid,memberUid                     eq,pres,sub
index nisMapName,nisMapEntry            eq,pres,sub
```

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 sssvlv-2.4.so.2 -> sssvlv-2.4.so.2.10.7
-rwxr-xr-x. 1 root root  28128 Jan 29  2019 sssvlv-2.4.so.2.10.7
-rwxr-xr-x. 1 root root   1082 Jan 29  2019 sssvlv.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 -> valsort-2.4.so.2.10.7
-rwxr-xr-x. 1 root root  19808 Jan 29  2019 valsort-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 valsort.la
```

TLSCACertificateFile, TLSCertificateFile & TLSCertificateKeyFile

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

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

security

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

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

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

access to

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

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

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

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	Intérrogation d'un serveur DNS en utilisant les champs SRV des enrigistrements DNS
ldap	Transmission des reqûetes en tant que proxy vers un autre serveur LDAP
meta	Transmission des reqûetes en tant que proxy avec méchanisme de ré-écriture des noms des objets
monitor	Pseudo backend pour accéder aux informations du serveur
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	Affichange du traitement des paquets
4	Args	Affichage détaillé des appels de fonctions
8	Conns	Affichage des connexions
16	BER	Affichage des paquets reçus et émis
32	Filter	Affichage du traitement d'un filtre
64	Config	Affichage du traitement du fichier de configuration
128	ACL	Affichage du traitement des permissions de chaque opération
256	Stats	Affichage du résultat des opérations
512	Stats2	Affichage des statistiques
1024	Shell	Affichage des communications avec des backends de type shell
2048	Parse	Affichage du traitement des entrées
4096	Cache	Affichage des opérations de gestion du cache des bases de données
8192	Index	Affichage des opérations d'indexation des bases de données
16384	Sync	Affichage des opérations syncrepl

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 **ldappassword** :

- {SSHA} (**Salted** **S**ecure **H**ash **A**lgorithm - 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 #1 - 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.

1.1 - Le format LDIF

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

Le fichier LDIF est un fichier texte qui peut comprendre :

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

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

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

1.2 - /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: valsort.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,c
 n=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,c
 n=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
conn_max_auth	olcConnMaxPendingAuth
defaultaccess	Non supporté
defaultsearchbase	olcDefaultSearchBase
disallow	olcDisallows
gentlehup	olcGentleHUP
idletimeout	olcIdleTimeout
include	Non supporté
index	olcDbIndex
logfile	olcLogFile
loglevel	olcLogLevel
moduleload	olcModuleLoad
modulepath	olcModulePath
objectclass	olcObjectClasses

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

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

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}HPtjJrdK0QlLvpfT2GHiQhMrMUt5l5vb**. 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,c
 n=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
```

1.3 - 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
```

1.4 -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 ~]# slaptest -u
config file testing succeeded
```

LAB #2 - Démarrer le 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/slapd -u ldap -h ldapi:/// ldap:///
```

2.1 - Options de la ligne de commande de slapd

La commande slapd peut prendre plusieurs options :

```
[root@centos7 ~]# slapd --help
slapd: invalid option -- '-'
usage: slapd options
    -4        IPv4 only
    -6        IPv6 only
    -T {acl|add|auth|cat|dn|index|passwd|test}
            Run in Tool mode
    -c cookie    Sync cookie of consumer
    -d level    Debug level
```

```
    -f filename    Configuration file
    -F dir    Configuration directory
    -g group    Group (id or name) to run as
    -h URLs        List of URLs to serve
    -l facility    Syslog facility (default: LOCAL4)
    -n serverName    Service name
    -o <opt>[=val] generic means to specify options; supported options:
        slp[={on|off|(attrs)}] enable/disable SLP using (attrs)
    -r directory    Sandbox directory to chroot to
    -s level    Syslog level
    -u user        User (id or name) to run as
    -V        print version info (-VV exit afterwards, -VVV print
            info about static overlays and backends)
```

<html>

</html>