slapd.conf

Fichier de configuration de slapd (ancien format)

Le fichier de configuration (slapd.conf) consiste de 3 types d'information de configuration : **global**, **backend** et **database**. Les informations globales sont spécifiées en premier, suivis par les informations associées avec un type de backend particulier, puis les informations associées avec un type particulier de base. Les directives globales peuvent être écrasées par des directives de base ou de backend, et les directives backend peuvent être écrasées par les directives de base de données.

Les lignes blanches et les lignes de commentaire commençant par un # et sont ignorées. Si une ligne commence par un espace blanc, il est considéré comme la suite de la ligne précédente (même si la précédente ligne est un commentaire).

Format général

```
# Directives de configuration globale:
<global config directives>

# backend definition
backend <typeA>
<backend-specific directives>

# first database definition & config directives
database <typeA>
<database-specific directives>

# second database definition & config directives
database <typeB>
<database-specific directives>

# second database definition & config directives
database <typeA>
<database-specific directives>

# subsequent backend & database definitions & config directives
...
```

Directives Global

Les directives décrites dans cette section s'appliquent à tous les backend et bases.

access to <what> [by <who> [<accesslevel>] [<control>]]+ Cette directive donne accès spécifié par accesslevel à un set d'entrée et/ou d'attributs spécifiés par what, par un ou plusieurs utilisateurs spécifiés par who. **note** : si aucune directive access n'est spécifié, la politique est access to * by * read.

attributetype <rfc4512 Attribute Type Description> cette directive définit un type d'attribut.

idletimeout <integer> Spécifie le nombre de secondes à attendre avant de forcer la fermeture de la connexion d'un client. à 0, désactive la fonction.

include <filename> Spécifie une fichier à lire, contenant d'autres informations de configuration. Généralement utilisé pour inclure les spécification de schéma.

loglevel <integer> Cette directive spécifie le niveau de log (actuellement placé dans syslogd LOG_LOCAL4). Le loglevel peut être spécifié sous forme d'entier ou par mot clé.

level	keyword	Description
-1	any	enable all debugging
0		no debugging
1	(0x1 trace)	trace function calls
2	(0x2 packets)	debug packet handling
4	(0x4 args)	heavy trace debugging
8	(0x8 conns)	connection management
16	(0x10 BER)	print out packets sent and received
32	(0x20 filter)	search filter processing
64	(0x40 config)	configuration processing
128	(0x80 ACL)	access control list processing
256	(0x100 stats)	stats log connections/operations/results
512	(0x200 stats2)	stats log entries sent
1024	(0x400 shell)	print communication with shell backends
2048	(0x800 parse)	print entry parsing debugging
16384	(0x4000 sync)	syncrepl consumer processing
32	(0x8000 none)	only messages that get logged whatever log level is set

on peut additionner les valeurs :
loglevel 129
loglevel 0x81
loglevel 128 1
sont équivalent :
loglevel 0x80 0x1
et
loglevel acl trace

objectclass <rfc4512 Object Class Description> Cette directive définit une classe objet

referral <URI> Cette directive spécifie le référant quand slapd ne peut trouver une base locale pour manipuler les requêtes.

sizelimit <integer> Cette directive spécifie le nombre maximum d'entrée à retourner pour une opération de recherche. défaut : sizelimit 500

timelimit <integer> Cette directive spécifie le nombre maximum de seconde que slapd va passer à répondre à une requete. Au delà, il envoie un exceeded timelimit. defaut : timelimit 3600

Directives Backend

Les directives dans cette section s'appliquent uniquement au backend dans lequel elles sont définies. Elles sont supportées par tous les types de backend. Les directives d'un backend s'appliquent à toutes les instances de base du même type.

backend <type> Cette directive marque le début d'une déclaration backend. <type> peut être un des types supportés :

Types	Description
bdb	Berkeley DB transactional backend
dnssrv	DNS SRV backend
hdb	Hierarchical variant of bdb backend
ldap	Lightweight Directory Access Protocol (Proxy) backend
meta	Meta Directory backend
monitor	Monitor backend
passwd	Provides read-only access to passwd(5)
perl	Perl Programmable backend
shell	Shell (extern program) backend

Directives générales de bases de données

Les directives dans cette section s'appliquent uniquement à la base dans laquelle elles sont définies

database <type> Cette directive marque le début d'une déclaration d'instance de base. <type> doit être un des type de backend supporté.

limits <who><limit> [<limit> [...]] spécifie les limites de temps et de taille sur qui initie une opération

readonly on|off Cette directive place la base en lecture seule

rootdn <DN> Cette directive spécifie le DN qui n'est pas sujet aux restriction de limites administratives et de contrôle d'accès pour les opérations sur cette base. le DN doit référer à une entrée dans l'annuaire. Le DN peut référer à une identité SASL. (ex : rootdn "cn=Manager,dc=example,dc=com", avec sasl : rootdn "uid=root,cn=example.com,cn=digest-md5,cn=auth")

rootpwd <password> Cette directive spécifie le mot de passe pour le rootdn. Il est possible d'utiliser slappasswd -s pour générer un hash.

suffix <dn suffix> Cette directive spécifie le suffixe DN des requêtes qui seront passé à cette base. Plusieurs lignes peuvent être spécifiées, et au moins une est requise pour chaque définition de base.(ex : suffix "dc=example,dc=com" # les requêtes avec un DN se terminant avec "dc=Example,dc=com" seront passées à ce backend)

syncrepl

syncrepl rid=<replica ID>

provider=ldap[s] ://<hostname>[:port]

type=refreshOnly

[interval=dd :hh :mm :ss]

[retry= [<retry interval> <# of retries>] +]

searchbase=<base DN>

[filter=<filter str>]

[scope=sub|one|base]

[attrs=<attr list>]

[attrsonly]

[sizelimit=<limit>]

[timelimit=<limit>]

schemachecking=on

bindmethod=simple

[binddn=<DN>]

[saslmech=<mech>]

[authcid=<identity>]

[authzid=<identity>]

[credentials=<passwd>]

[realm=<realm>]

[secprops=<properties>]

starttls=yes

[tls_cert=<file>]

[tls_key=<file>]

[tls_cacert=<file>]

[tls_cacertdir=<path>]

[tls_reqcert=never|allow|try|demand]

[tls_ciphersuite=<ciphers>]

[tls_crlcheck=none|peer|all]

[logbase=<base DN>]

[logfilter=<filter str>]

[syncdata=default|accesslog|changelog] Cette directive spécifie la base courante comme réplique du contenu d'un master en utilisant le moteur de réplication syncrepl.

provider indique le master. spécifie un schéma, un hôte et un port

rid est utilisé pour l'identification de la directive syncrepl courante dans le serveur de réplication.

searchbase n'a pas de valeur par défaut et doit toujours être spécifié.

scope est à sub par défaut

filter est à (objectclass=*) par défaut

attrs à "*,+" par défaut pour répliquer tous les utilisateurs et tous les attributs optionnels

attrsonly est désactivé par défaut

sizelimit est à unlimited par défaut

timelimit est à unlimited par défaut

Le protocole de synchronisation de contenu LDAP à 2 types d'opérations : **refreshOnly** et **refreshResultEntry**. Avec **RefreshOnly**, la synchronisation est périodique. l'interval est spécifié par le paramètre interval. Par défaut il est à 1 jour. Avec **refreshAndPersist**, la synchronisation est persistante.

Si une erreur se produit durant la réplication, le réplicateur tente de se reconnecter en accord avec le paramètre **retry**, qui est une liste de paire de paramètres **<retry interval>** et **<# of retries>**. Par exemple, **retry "60 10 300 3"** tente de se reconnecter toutes les 60 secondes, 10 fois, puis retente toutes les 300 secondes, 3 fois, avant de stopper la tentative de reconnexion.

La vérification de schéma peut être renforcée avec le paramètre **schemachecking**. Activé, toute entrée répliquée sera vérifié pour ce schéma avant de le stocker. Le paramètre **binddn** donne le DN à lier pour la recherche syncrepl. Il doit être un DN qui a les droits d'accès en lecture.

bindmethod est simple ou sasl, en fonction si l'authentification par mot de passe est simple pour sasl. L'authentification simple ne devrait pas être utilisé a moins que l'intégrité des données des protections de confidentialité soient en place (par exemple : TLS ou IPsec) L'authentification simple requière les paramètres **binddn** et **credentials**. L'authentification SASL requière la spécification d'un mécanisme utilisant le paramètre **saslmech**. **authcid** et **credential** peuvent être spécifiés pour l'identité d'authentification et le credential. authzid peut être utilisé pour spécifier l'identité d'autorisation.

le paramètre **realm** spécifie un domaine. le paramètre **secprops** spécifie les propriétés de sécurité Cyrus SASL.

starttls spécifie l'utilisation de TLS. Si l'argument critical est spécifié, la session sera abordée si la requête StartTLS échoue. Sinon la session SyncRepl continu sans TLS.

Au lieu de répliquer toutes les entrées, le réplicateur peut chercher les logs de modification de données. Ce mode d'opération s'appel delta syncrepl. En plus des paramètres ci-dessus, les paramètres logbase et logfilter doivent être spécifiés pour les logs à utiliser. Le paramètre syncdata doit être soit à "accesslog" si le log est conforme au format slapo-accesslog ou "changelog". Si le paramètre syncdata est omis ou à "default", les paramètres de log seront ignorés. La réplication syncrepl est supportées par bdb et hdb.

updateref <URL> Cette directive est seulement applicable dans un slave. Il spécifie l'URL à retourner aux clients qui envoient des requêtes de mise à jours sur la réplique. Peut être spécifié plusieurs fois.

directives de base BDB et HDB Ces directives s'appliquent uniquement aux bases BDB et HDB.

directory <directory> Cette directive spécifie le dossier où les fichiers contenant la base et indices associés sont stockés.

Exemple de fichier de configuration

L'exemple suivant définit 2 bases pour manipuler différentes parties d'un arbre x500. Les 2 bases sont des instances BDB.

```
# example config file - global configuration section
include /usr/local/etc/schema/core.schema # inclue un fichier de définition de schéma
referral ldap ://root.openldap.org # les requêtes non local sur une des bases définies vont référer au server
LDAP à l'hôte root.openldap.org
access to * by * read # Contrôle d'accès global.

# BDB definition for the example.com
database bdb
suffix "dc=example,dc=com" # suffix DN pour cette base
directory /usr/local/var/openldap-data # dossier où se trouve les fichiers de cette base.
rootdn "cn=Manager,dc=example,dc=com" # rootdn pour cette base
rootpw secret # mdp du rootdn
# indexed attribute definitions
index uid pres,eq # indique les indices pour maintenir divers attributs
index cn,sn,uid pres,eq,approx,sub
index objectClass eq
# database access control definitions
access to attrs=userPassword # Spécifier le controle d'accès pour les entrées dans cette base.
by self write
by anonymous auth
by dn.base="cn=Admin,dc=example,dc=com" write
by * none
access to *
by self write
by dn.base="cn=Admin,dc=example,dc=com" write
by * read

# BDB definition for example.net
database bdb
suffix "dc=example,dc=net"
directory /usr/local/var/openldap-data-net
rootdn "cn=Manager,dc=example,dc=com"
index objectClass eq
access to * by users read
```