slapd-config

Backend de configuration de slapd

Options de configuration globale

Ces options sont spécifiées dans l'entrée cn=config. Elle doit avoir un objectClass olcGlobal.

cn =config

olcAllows Spécifie un jeu de fonctionnalités à autoriser. **bind_anon_cred** permet un bind anonyme quand les crédentials ne sont pas vide, **bind_anon_dn** permet un bind non-authentifié quand le DN n'est pas vide et **proxy_authz_anon** permet un contrôle d'autorisation proxy non-authentifié

olcArgsFile Chemin d'un fichier qui maintient la ligne de commande du serveur slapd

olcAttributeOptions Définis le tagging d'options d'attributs ou des préfixes tag/range. un préfixe se termine par '-'.

olcAuthIDRewrite Utilisé par le framework d'authentification pour convertir un simple nom en DN utilisé pour l'autorisation. Son but est analogue à olcAuthzRegexp. Ce jeu de règle est analogue à ceux décrit dans slapo-rwm

olcAuthzPolicy Spécifie quelles règles utiliser pour l'autorisation proxy. **none** désactive, **from** utilise les règles dans authzFrom, **to** utilise celles dans authzTo, **any**, et **all** (toutes les autorisations doivent réussir)

olcAuthzRegexp Utilisé par le framework d'authentification pour convertir un simple nom en DN utilisé pour l'autorisation.

olcConcurrency Spécifie un niveau de concurrence.

olcConnMaxPending Nombre maximum de requêtes en attente pour une session anonyme

olcConnMaxPendingAuth Spécifie le nombre maximum de requêtes en attente pour une session authentifiée.

olcDisallows Spécifie un jeu de fonctionnalités à désactiver. **bind_anon** n'accèpte plus les requêtes bind anonymes. **bind_simple** désactive le simple bind. **tls_2_anon** désactive les sessions forcées en status anonyme une fois l'opération StartTLS reçue. **tls_authc** désactive es opérations StartTLS si authentifié.

olcGentleHUP a TRUE, SIGHUP ne fait qu'une tentative d'arrêt. slapd n'accèpte plus les nouvelle connexions, mais attend que les connexions en cours se terminent.

olcIdleTimeout Nombre de secondes avant de fermer une session client non active. (0 désactive)

olcIndexIntLen Longueur de clé pour les indices entier ordonnés. Le MSB d'un binaire entier sera utilisé pour indexer les clés.

olcIndexSubstrIfMaxLen Longueur max des indices subinitial et subfinal.

olcIndexSubstrIfMinLen Longueur mini des indices subinitial et subfinal. Une valeur d'attribut doit avoir au moins cette longueur pour être traitée

olcIndexSubstrAnyLen Longueur utilisée pour les indices subany. Une valeur d'attribut doit avoir au moins cette longueur pour être traitée. est utilisé pour les indices subinitial et subfinal quand le filtre est supérieur à olcIndexSubstrIfMaxlen

olcIndexSubstrAnyStep Spécifie les étapes utilisée dans les recherchée d'index subany. définis l'offset pour les segments d'une chaîne de recherche

olcListenerThreads Spécifie le nombre de threads à utiliser pour le gestionnaire de connexion

olcLocalSSF Spécifie le Security Strength Factor (SSF) pour les sessions LDAP locales.

olcLogFile Fichier où enregistrer les logs

olcLogLevel Niveau de log

olcPasswordCryptSaltFormat Spécifie le format du salt passé à crypt(3) en générant les mots de passe {CRYPT}. Doit être au format sprintf(3) et peut inclure une conversion %s

olcPidFile Chemin absolu du fichier PID

olcPluginLogFile Chemin absolu d'un fichier contenant les logs pour le plugin SLAPI

olcReferral Spécifie les referrals à passer quand slapd ne peut pas trouver une base à utiliser pour une requête

olcReverseLookup Active/désactive la recherche inversée d'un nom de client

olcRootDSE Nom d'un fichier ldif contenant les attributs utilisateur pour le root DSE

olcSaslAuxprops Spécifie quels plugins auxprop utiliser pour les recherches d'authentification.

olcSaslHost fqdn utilisé pour le traitement SASL

olcSaslRealm Royaume SASL

olcSaslSecProps Spécifie les propriétés de sécurité pour cyrus SASL. none efface les flags "**noanonymous,noplain**". **noplain** désactive les mécanismes sujets à attaques passives. **noactive** désactive les mécanismes sujet à attaques actives. **nodict** désactive les mécanismes sujets à attaque passive par dictionnaire. **noanonymous** désactive le support des login anonymes. **forwardsec** nécessite un renvoie de secret entre les sessions. **passcred** nécessite un mécanisme qui passe les crédentials clients. **minssf=<factor>** spécifie le SSF minimum acceptable. **maxssf=<factor>** spécifie le SSF maximum acceptable. **maxbufsize=<size>** spécifie la taille de tampon max.

olcServerID Spécifie un ID de 0 à 4096 pour ce serveur.

olcSockbufMaxIncoming Taille de PDU LDAP maximum entrante pour les sessions anonymes.

olcSockbufMaxIncomingAuth Taille de PDU LDAP maximum entrante pour les sessions authentifiées.

olcTCPBuffer Taille du tampon TCP. Une valeur globale est définie, et des valeur pour la lecture et l'écriture peuvent être spécifiés

olcThreads Taille maximum du pool de thread primaire.

olcToolThreads Nombre de thread maximum à utiliser en mode tool. ne devrait pas être supérieur au nombre de CPU.

olcWriteTimeout Nombre de secondes à attendre avant de fermer une connexion avec une écriture en cours. permet une récupération face à divers problèmes réseau

Options TLS

olcTLSCipherSuite Permet de configurer les chiffrement acceptés et l'ordre de préférence.

olcTLSCACertificateFile Fichier contenant les certificats pour toutes les CA que slapd reconnaît

olcTLSCACertificatePath Chemin d'un répertoire contenant les certificats CA

olcTLSCertificateFile Fichier contenant le certificat du server ldap

olcTLSCertificateKeyFile Fichier contenant la clé privée du serveur ldap

olcTLSDHParamFile Spécifie le fichier contenant les paramètres pour les échanges de clé Diffie-Hellman. " !AH" devrait être ajouté à la suite de chiffrements si des chiffrements sont spécifiés et utilisent les échanges de clé DH anonymes.

olcTLSRandFile Fichier pour obtenir des données aléatoires quand /dev/urandom n'est pas disponible

olcTLSVerifyClient Spécifie quelle vérification exécuter sur les certificats clients. **never** ne demande pas de certificat, **allow** nécessite un certificat. **try** le certificat est demandé, mais non obligatoire. **demand|hard|true** sont équivalent

olcTLSCRLCheck Spécifie si la CRL doit être utilisée pour vérifier les certificats clients. **none** ne vérifie pas la CRL. **peer** vérifie dans la CRL. **all** vérifie toute la chaîne dans le CRL.

olcTLSCRLFile Spécifie le fichier contenant la CRL à vérifier

Options de modules dynamique

Chaque module a une entrée nommée cn=module{x},cn=config

olcModuleLoad Spécifie le nom d'un module dynamique

olcModulePath Spécifie une liste de répertoires où chercher les modules.

Options de schéma

Les définitions de schéma sont créées en tant qu'entrée dans cn=schema,cn=config

olcAttributeTypes Spécifie une type d'attribut utilisant la syntaxe LDAPv3

olcDitContentRules Spécifie un DIT Content Rule utilisant la syntaxe LDAPv3

olcObjectClasses Spécifie une classe d'objet en utilisant la syntaxe LDAPv3

olcObjectIdentifier Définis une nom équivalent à l'OID donné

Options général de backend

Chaque backend est définies dans une entrée nommée : olcBackend=<databasetype>,cn=config

Options de base de données

Les options de base de données sont définies dans des entrées nommées olcDatabase={x}<databasetype>,cn=config. La base frontend spéciale est toujours numérotée {-1} et la base de configuration est toujours numérotée {0}

Ces options peuvent être définies dans le frontend et doivent avoir l'objet olcFrontEndConfig

olcAccess Définis l'accès à une base de données

olcDefaultSearchBase Spécifie le dn de bas de recherche par défaut à utiliser quand les clients ne spécifient pas de base de recherche

olcExtraAttrs Liste les attributs devant être ajoutés aux requêtes de recherche. Les backend locaux retournent toute l'entrée, le frontend ne retourne que celles autorisées par les ACL.

olcPasswordHash Configure les hash à utiliser lors de la génération de mots de passe dans l'attribut userPassword. {SSHA}, {SHA}, {MD5}, {SMD5}, {CRYPT}, {CLEARTEXT}

olcReadOnly Place la base de donnée en lecture seule

olcRequires Spécifie un jeu de conditions requis. Peut être spécifié globalement et/ou par base de données (additive). **authc** nécessite une authentification avant toute opération, **SASL** nécessite une authentification SASL, **strong** nécessite une authentification forte. **none** ne spécifie aucune condition

olcRestrict Spécifie une liste d'opérations interdites. Peut être spécifié globalement et/ou par base de données (superseed). add, bind, compare, delete, extended[=<OID>], modify, rename, search, read, write

olcSchemaDN Spécifie le DN de la sous-entrée du sous-schéma qui contrôle les entrées sur ce serveur.

olcSecurity Spécifie un jeu de SSF. Peut être spécifié globalement et/ou par base de données. **ssf=<n>** Spécifie le SSF général. **transport=<cn>** spécifie le transport SSF. **tls=<n>** spécifie le TLS SSF. **update_ssf=<n>** spécifie le SSF général pour les updates. **update_transport=<n>** spécifie le transport SSF pour les updates. **update_tls=<n>** spécifie les TSL SSF pour les updates. **update_sasl=<n>** spécifie le SASL SSF pour les updates. **simple_bind=<n>** requière une authentification simple

olcSizeLimit Spécifie le nombre maximum d'entrées à retourner lors d'une recherche.

olcSortVals Spécifie une liste d'attributs multi-valués qui seront toujours maintenus en ordre trié. Permet aux opération modify, compare et aux filtres d'évaluation d'être traités plus efficacement. frontend only.

olcTimeLimit Spécifie le temps maximum en secondes pour une réponse à une recherche

Options de base de données générales

olcAddContentAcl Contrôle si les opérations Add vont effectuer une vérification d'ACL sur le contenu de l'entrée ajoutée.

olcHidden Contrôle si la base sera utilisée pour répondre aux requêtes

olcLastMod Contrôle si slapd maintient automatiquement les attributs modifiersName, modifyTimestamp, creatorsName, et createTimestamp pour les entrées. Contrôle aussi entryCSN et entryUUID

olcLimits Spécifie les limites de temps et de taille basé sur l'initiateur de l'opération ou base DN.

olcMaxDerefDepth Nombre maximum d'aliase à déréférencer en essayant de résoudre une entrée.

olcMirrorMode à TRUE, place un réplica de base en mode mirroir. les updates sont accèptées par tout utilisateur. La base doit être en syncrepl

olcPlugin Configure le plugin SLAPI

olcRootDN Spécifie le DN qui n'est pas sujet à contrôle d'accès ou restrictions administratives

olcRootPW Mot de pas du RootDN

olcSubordinate Spécifie que le backend est subordonné à un autre backend. une base subordonnée peut avoir une seul suffix. Utile pour accoler plusieurs suffix dans un simple contexte de nommage. TRUE, FALSE, advertise (si spécifié, le contexte de nommage de cette base est indiquée dans le rootDSE)

olcSuffix Spécifie le suffix DN des requêtes passée au backend

olcSyncUseSubentry Stocke le contextCSN syncrepl dans une sous-entrée au lieu de l'entrée context de la base

olcSyncrepl Spécifie la base courante comme réplica d'un contenu master

olcUpdateDN applicable uniquement pour les base esclaves. Spécifie le DN autorisé à updater la base

olcUpdateRef Spécifie les référants à passer quand slapd reçoit le demande de modifier une base local répliquée.

Overlays

Un overlay est une code qui intercepte les opérations de la base dans le but de les étendre ou les changer. Les overlays doivent être configurés comme entrées enfant d'une base spécifique le RDN de l'entrée doit avoir l'objectClass olcOverlayConfig

Exemple

L'exemple suivant, s'il est copié dans le fichier config.ldif, la commande suivante va initialiser la configuration :
slapadd -F /usr/local/etc/openldap/slapd.d -n 0 -l config.ldif

```
dn: cn=config
objectClass: olcGlobal
cn: config
olcPidFile: /usr/local/var/run/slapd.pid
olcAttributeOptions: x-hidden lang-

dn: cn=schema,cn=config
objectClass: olcSchemaConfig
cn: schema

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

dn: olcDatabase=frontend,cn=config
objectClass: olcDatabaseConfig
objectClass: olcFrontendConfig
olcDatabase: frontend
# Subtypes of "name" (e.g. "cn" and "ou") with the
# option ";x-hidden" can be searched for/compared,
# but are not shown. See slapd.access(5).
olcAccess: to attrs=name;x-hidden by * =cs
# Protect passwords. See slapd.access(5).
olcAccess: to attrs=userPassword by * auth
```

```
# Read access to other attributes and entries.
olcAccess: to * by * read

# set a rootpw for the config database so we can bind.
# deny access to everyone else.
dn: olcDatabase=config,cn=config
objectClass: olcDatabaseConfig
olcDatabase: config
olcRootPW: {SSHA}XKYnrjvGT3wZFQrDD5040US592LxsdLy
olcAccess: to * by * none

dn: olcDatabase=bdb,cn=config
objectClass: olcDatabaseConfig
objectClass: olcBdbConfig
olcDatabase: bdb
olcSuffix: "dc=our-domain,dc=com"
# The database directory MUST exist prior to
# running slapd AND should only be accessible
# by the slapd/tools. Mode 0700 recommended.
olcDbDirectory: /usr/local/var/openldap-data
# Indices to maintain
olcDbIndex: objectClass eq
olcDbIndex: cn,sn,mail pres,eq,approx,sub

# We serve small clients that do not handle referrals,
# so handle remote lookups on their behalf.
dn: olcDatabase=ldap,cn=config
objectClass: olcDatabaseConfig
objectClass: olcLdapConfig
olcDatabase: ldap
olcSuffix: ""
olcDbUri: ldap://ldap.some-server.com/
```

Limite de taille et de temps

```
olcLimits: <selector> <limit> [<limit> [...]]
selector: anonymous|users|[<dnspec>=]<pattern>|group[/oc[/at]]=<pattern>
<dnspec> ::= dn[.<type>][.<style>]
<type> ::= self | this
<style> ::= exact | base | onelevel | subtree | children | regex | anonymous
```

unchecked définie une limite sur le nombre de candidats qu'une recherche est autorisé à examiner
size[.{soft|hard|unchecked}]=<integer>
Contrôle pageResult total permis de retourner :
size.prtotal={<integer>|unlimited|disabled}
contrôle pageResult :
size.pr={<integer>|noEstimate|unlimited}

integer Taille de page maximum si aucune limite explicite n'est définies.

noEstimate ne retourne pas d'estimation du nombre d'entrée qui peuvent être retournées

olcSyncrepl

olcSyncrepl : rid=<replicaID> provider=ldap[s] ://<hostname>[:port] searchbase=<baseDN> [type=refreshOnly|refreshAndPersist] [interval=dd :hh :mm :ss] [retry=[<retry interval> <# of retries>]+] [filter=<filterstr>] [scope=sub|one|base|subord] [attrs=<attrlist>] [exattrs=<attrlist>] [attrsonly] [sizelimit=<limit>] [timelimit=<limit>] [schemachecking=on|off] [network-timeout=<seconds>] [timeout=<seconds>] [bindmethod=simple|sasl] [binddn=<dn>] [saslmech=<mech>] [authcid=<identity>] [authzid=<identity>] [credentials=<passwd>] [realm=<realm>] [secprops=<properties>] [keepalive=<idle> :<probes> :<interval>] [starttls=yes|critical] [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] [suffixmassage=<real DN>] [logbase=<base DN>] [logfilter=<filterstr>] [syncdata=default|accesslog|changelog]

rid ID qui identifie la directive syncrepl dans le site de réplication.

provider Spécifie le fournisseur de réplication contenant le contenu master

searchbase, scope, filter, attrs, attrsonly, sizelimit, timelimit servent de spécification pour filtrer le contenu du réplica

refreshOnly la prochaine opération de recherche de synchronisation est re-planifiée à intervalle définis par interval.

refreshAndPersist la synchronisation est persistante

retry Si la connexion est perdue, retente avec des pair de valeur <retry inval> et <# of retries>. ex : retry"60 10 300 3". + vaut indéfinis

schemachecking Force la vérification du schéma.

network-timeout Définis le temps d'établissement d'une connexion réseau avec le fournisseur

timeout Détermine le temps que le client attend que la requête Bind initiale soit complétée

bindmethod simple, sasl

binddn DN pour un simple bind

saslmech requis pour SASL

authcid Identité et/ou crédentials pour l'authentification sasl

authzid identité d'authorisation

credentials Crédentials pour le bind

realm Royaume SASL

secprops Définis les propriétés de sécurité spécifiques

keepalive Définis les valeurs de idle (temps avant un TCP keepalive), probes (nombre max de keepalive avant de fermer la connexion) et intervalles (temps entre les keepalive)

starttls Spécifie l'utilisation de l'opération étendue StartTLS pour établir une session TLS.

tls_cert Certificat pour la connexion TLS

tls_key Clé privée

tls_cacert Fichier contenant les certificats CA

tls_cacertdir Répertoire contenant les certificats CA

tls_reqcert Spécifie si le certificat est requis

tls_ciphersuite Spécifie la suite de chiffrement et l'ordre à utiliser

tls_crlcheck Vérifie les certificat dans la CRL

suffixmassage Permet au client de pousser des entrée depuis un annuaire distant dont le suffixe DN diffère de l'annuaire local Les entrée qui matche le searchbase seront remplacé avec ce DN

logbase Fichier où écrire les logs

logfilter Filtre pour les logs

syncdata accesslog, les logs sont conforme à slapo-accesslog. changelog les logs sont conforme au format changelog (obsolète). default, les paramètres de logs sont ignorés