



Expert

LDAP

Planification et mise en œuvre
d'un annuaire **OpenLDAP**

Stéphane ROPARS

Avant-propos

Chapitre 1

Un annuaire, un choix évident

1. Le casse-tête de la gestion des identifiants électroniques en entreprise. 15
2. La centralisation des identités électroniques 16
3. Les annuaires. 17
4. Annuaires vs mécanismes d'authentification 18
5. Annuaire vs base de données 18

Chapitre 2

Les concepts de base LDAP

1. Introduction 21
2. LDAP : Protocole ou normalisation des systèmes d'annuaires informatiques 21
3. Modèle de stockage des informations 25
 - 3.1 Les attributs 26
 - 3.2 Les classes d'objets et les schémas 29
4. Modèle d'organisation des informations 35
 - 4.1 La structure arborescente (DIT) 35
 - 4.2 Le format LDIF 38
5. Modèle fonctionnel 39
 - 5.1 Les opérations de type requête 40
 - 5.2 La syntaxe du filtre de recherche 42
 - 5.3 Comparaison. 44
 - 5.4 Les opérations de mise à jour 44
 - 5.5 Les opérations d'authentification 44
6. Modèle de sécurisation et de confidentialité des informations 45

Chapitre 3**Planification de l'intégration d'un annuaire LDAP**

1. Introduction	47
2. Source et contenu de l'annuaire	49
2.1 Utilisation principale de l'annuaire	49
2.2 Recensement des différents systèmes d'information utilisés dans votre entreprise	49
2.3 Vérifier la compatibilité avec le protocole LDAP	50
3. Modélisation et définition du contenu de l'annuaire	52
3.1 Connaissance des schémas utilisés par les clients LDAP	52
3.2 Modélisation	53
4. Stockage physique des données	55
4.1 Disques locaux ou architecture de stockage de données	55
4.2 Base de données, moteurs de stockage (backend)	57
4.3 Le format LDIF	57
5. Sécurisation de l'annuaire	58
5.1 Objectif	58
5.2 Étude de l'authentification à l'annuaire	59
5.3 Étude de l'autorisation au contenu de l'annuaire	61
6. Conception de l'infrastructure du service d'annuaire	62
6.1 Les différentes topologies	62
6.1.1 Un service d'annuaire local	63
6.1.2 Un service d'annuaire local avec référent(s)	63
6.1.3 Un service d'annuaire local et répliqué	65
6.1.4 Un service d'annuaire distribué et répliqué	66
6.1.5 Un service d'annuaire distribué et répliqué avec référents	67
6.2 La haute disponibilité des annuaires	68
6.2.1 Configuration de multiples serveurs LDAP	69
6.2.2 Configuration de la mise en cache LDAP	70

- 6.2.3 Ajout d'un équipement matériel ou applicatif de type commutateur IP avec ou sans équilibrage de charge en "Front-end" 72
- 6.3 Présentation d'un cluster de répartition de charge (load-balancing cluster) 73
 - 6.3.1 Fonction de haute disponibilité en mode "actif/passif" (clustering) 74
 - 6.3.2 Fonction de répartition de charge (load-balancing) 77
 - 6.3.3 Méthode de réponse du "load-balancer" 78
 - 6.3.4 Exemple de configuration pour la fonction cluster à répartition de charge en mode dispatcher (sous AIX) . . 81
- 6.4 Un service d'annuaire local avec délégation d'authentification (PTA) 85

Chapitre 4

Installation/configuration d'un serveur OpenLDAP

- 1. Introduction 87
- 2. Présentation de l'architecture LDAP à intégrer 87
- 3. Installation du serveur OpenLDAP 90
 - 3.1 Les prérequis applicatifs 90
 - 3.2 À partir de packages RPM (exemple de la distribution Red Hat) 90
 - 3.3 Depuis les sources du code 93
- 4. Configuration du serveur OpenLDAP 95
 - 4.1 Organisation des fichiers de configuration 96
 - 4.2 Présentation des entrées de configuration 98
 - 4.2.1 "dn: cn=config" 99
 - 4.2.2 "dn: cn=module, cn=config" 100
 - 4.2.3 "dn: cn=schema, cn=config" 101
 - 4.2.4 "dn: olcBackend=<type>, cn=config" 101
 - 4.2.5 "dn: Database={x}<type>, cn=config" 102

4.3	Présentation des backend disponibles	103
4.3.1	Les backend locaux	103
4.3.2	Les proxy backend	104
4.3.3	Les backend dynamiques	104
4.4	Configuration initiale par le fichier "slapd.conf"	104
4.4.1	Création du fichier "/etc/openldap/slapd.conf"	105
4.4.2	Conversion de l'ancien (slapd.conf) au nouveau format de configuration (olc, cn=config)	108

Chapitre 5

Installer et configurer un navigateur LDAP

1.	Introduction	111
2.	Présentation de Apache Directory Studio	111
3.	Installation sous Linux	112
4.	Configuration d'une connexion à un annuaire	113
5.	Quelques exemples d'utilisation	118
6.	Première connexion au DIT de configuration	125

Chapitre 6

Démarrage du serveur OpenLDAP

1.	Introduction	129
2.	Le service "slapd"	129
3.	Présentation des options de démarrage du processus "slapd"	130
4.	Vérification du démarrage automatique du service "slapd"	133
5.	Démarrage et arrêt du processus "slapd" en ligne de commande	133

Chapitre 7
Les schémas

- 1. Introduction 135
- 2. Les schémas contenus dans OpenLDAP 135
- 3. Extension de schéma 138
- 4. Ajout du schéma "sudo" 140
- 5. Suppression d'un schéma 142

Chapitre 8
Préparation des données de l'annuaire

- 1. Introduction 145
- 2. Choix du suffixe 145
- 3. Structure et nommage des entrées 145
- 4. Configuration de la structure LDAP au format LDIF 148

Chapitre 9
Provisionner l'annuaire LDAP

- 1. Introduction 151
- 2. Les méthodes de chargement de l'annuaire 151
 - 2.1 Chargement des données en ligne 152
 - 2.2 Chargement des données hors ligne 153
- 3. Présentation des commandes LDAP 155
 - 3.1 La commande ldapsearch 156
 - 3.2 La commande ldapdelete 160
 - 3.3 La commande "ldapadd" 161
 - 3.4 La commande ldapmodify 162
 - 3.5 Les commandes ldapmodrdn, slapasswd, ldapwhoami, ldapurl 164
 - 3.6 Configuration des commandes LDAP 164

Chapitre 10**Sécuriser un annuaire OpenLDAP**

1. Introduction	167
2. Authentification (ou ouverture de session LDAP)	168
2.1 L'authentification de base ou simple	169
2.2 L'authentification SASL	170
2.3 Consulter les mécanismes SASL disponibles sur OpenLDAP .	173
3. La politique de mot de passe	175
4. Le stockage des mots de passe	175
4.1 Rappel sur les algorithmes de cryptage de type condensé . . .	176
4.2 Revue des fonctions de hachage supportées par OpenLDAP .	178
4.2.1 CRYPT	178
4.2.2 MD5	179
4.2.3 SMD5	179
4.2.4 SHA "Secure Hash Algorithm"	179
4.2.5 SSHA	180
4.2.6 PTA	181
4.3 Configuration du service PTA	182
4.3.1 Configuration du service saslauthd	184
5. La configuration réseau	192
5.1 Sélectionner son (ou ses) interface(s) réseau et son (ou ses) port(s) d'écoute(s)	192
5.2 Sélectionner les réseaux autorisés	193
6. Fixer des limites aux opérations LDAP	194
6.1 Le type de limites	194
6.2 Les limites hard ou soft	194
6.3 La portée des limites	195
6.3.1 Les limites globales	195
6.3.2 Les limites par base de données	196

- 7. Confidentialité et intégrité des communications. 197
 - 7.1 Présentation de SSL et TLS 197
 - 7.1.1 Son fonctionnement. 198
 - 7.2 StartTLS 201
 - 7.3 Présentation du programme OpenSSL 202
 - 7.3.1 Commande de création de certificats 203
 - 7.3.2 Commande de contrôle des certificats 204
 - 7.3.3 Recherche de pannes 204
 - 7.3.4 Commandes de conversion de certificats 205
- 8. Configuration du LDAPS avec SSL/TLS 206

Chapitre 11
Protection des données de l'annuaire

- 1. Compréhension de la sécurité d'un annuaire 215
- 2. Configuration générale des ACL 216
 - 2.1 Les entrées ciblées (à quoi ?) 216
 - 2.2 Les entrées accréditées (qui a accès ?) 219
 - 2.3 Les droits accordés (pour faire quoi ?) 220
 - 2.4 Évaluation des droits 221
 - 2.5 Exemples de configuration d'ACL 222
- 3. Configuration des ACL dans l'annuaire de démonstration 225
 - 3.1 Configuration des ACL standard. 226
 - 3.2 Cloisonnement de l'annuaire par client 227
 - 3.3 Pour aller plus loin dans le cloisonnement 229

Chapitre 12**Ajout de fonctionnalités appelées "overlay"**

1. Introduction	235
2. Ajouter un overlay	236
2.1 Vérification de son existence dans l'annuaire	236
2.2 Charger le module de l'overlay dans l'annuaire	237
2.3 Créer un overlay pour la base de données désirée	237
3. AccessLog	238
3.1 Présentation	238
3.2 Exemple de configuration	239
4. Audit logging	241
4.1 Présentation	241
4.2 Exemple de configuration	241
5. Constraint	242
5.1 Présentation	242
5.2 Exemple de configuration	242
6. Dynamic Lists	243
6.1 Présentation	243
6.2 Exemple de configuration	244
7. Password Policy	246
7.1 Présentation	246
7.2 Exemple de configuration	247
8. L'intégrité référentielle	253
8.1 Présentation	253
8.2 Exemple de configuration	255
9. Sync Provider	256
9.1 Présentation	256
9.2 Exemple de configuration	256
10. Attribute Uniqueness	257
10.1 Présentation	257
10.2 Exemple de configuration	258

- 11. Reverse Group Membership Maintenance 259
 - 11.1 Présentation 259
 - 11.2 Exemple de configuration 259

Chapitre 13
Configuration de clients LDAP

- 1. Introduction 261
- 2. Prérequis 261
- 3. Les systèmes d'exploitation 262
 - 3.1 Les serveurs Linux Red Hat (cas d'un RHEL6) 262
 - 3.1.1 Installation des packages 262
 - 3.1.2 Configuration du service "sssd" 264
 - 3.1.3 Ajout du certificat de l'autorité de certification 265
 - 3.1.4 Mise à jour du fichier /etc/hosts 266
 - 3.1.5 Dissimulation du mot de passe du Bind user 266
 - 3.1.6 Redémarrage du service "sssd" 266
 - 3.1.7 Vérifier le bon fonctionnement de la configuration 267
 - 3.1.8 Observation du mécanisme PAM 268
 - 3.2 Les serveurs IBM AIX 270
 - 3.2.1 Prérequis 270
 - 3.2.2 Installation et configuration des paquetages de cryptographie (gsk) 271
 - 3.2.3 Installation et configuration des paquetages du client LDAP 272
 - 3.2.4 Paramétrage système 272
 - 3.2.5 Vérification de l'installation du client LDAP 272
- 4. Les équipements Hardwares 274
 - 4.1 Cas d'une interface HP iLO 274
 - 4.1.1 Configuration 275
 - 4.2 Cas d'un Routeur (Cisco ASA) 278
 - 4.2.1 Les méthodes d'authentification à l'annuaire LDAP 279
 - 4.2.2 Les informations à rechercher 280

4.2.3	La configuration	280
5.	Les applications et utilitaires	284
5.1	Cas de l'application de monitoring OP5	284
5.2	Cas du programme sudo	289

Chapitre 14

Sauvegarder/restaurer un annuaire OpenLDAP

1.	Les données de l'annuaire.	293
2.	Les stratégies de sauvegarde.	294
3.	Méthode de sauvegarde des données de l'annuaire.	296
3.1	Sauvegarde hors-ligne au niveau des répertoires du système de fichiers	296
3.2	Sauvegarde hors-ligne au niveau de la base de données.	296
3.3	Sauvegarde en ligne au format LDIF	299
4.	Restauration de l'annuaire	300
4.1	Restauration totale.	300
4.2	Restauration partielle.	302
4.2.1	Restauration en ligne de type "import/export"	302
4.2.2	Restauration hors-ligne	303
5.	Exemple de script de sauvegarde	304
6.	Migration d'annuaire OpenLDAP	306

Chapitre 15

La réplication

1.	Introduction	307
2.	Fonctionnement du protocole de réplication "LDAP Sync".	308
2.1	Réplication en mode "refreshOnly" ou "Pull-based"	309
2.2	Réplication en mode "refreshAndPersist" ou "Push-based"	311

- 3. Configuration du "Syncrepl" en utilisant OLC 312
 - 3.1 Configuration du provider 312
 - 3.2 Configuration du consumer 313
- 4. Les problèmes liés à la réplication LDAP Sync 314
 - 4.1 SessionLog 315
 - 4.2 Delta-syncrepl ou AccessLog 316
 - 4.2.1 Exemple de configuration 317
- 5. Les différentes architectures de réplication 320
 - 5.1 Architecture de réplication simple "provider/consumer" 320
 - 5.2 Architecture de réplication "Peer to peer" ou "multi-Peer" 321
 - 5.2.1 Exemple de configuration 322
 - 5.3 Architecture de réplication "miroir" 325
 - 5.4 Architecture avec un proxy de réplication 327
 - 5.5 Configuration du NTP 328
 - 5.6 Réaliser la première synchronisation 329

Chapitre 16
Surveillance d'un annuaire OpenLDAP

- 1. Surveiller le service LDAP 331
 - 1.1 Le processus "slapd" 331
 - 1.2 Les systèmes de fichiers 331
- 2. Surveiller la réplication 332
- 3. Surveiller les connexions au serveur LDAP 334
- 4. Surveiller les modifications du contenu de l'annuaire 336

Chapitre 17**Amélioration des performances**

1. Considérations matérielles 339
 - 1.1 La mémoire ou RAM 339
 - 1.2 Le stockage 340
 - 1.3 Le réseau 341
2. Au niveau du processus "slapd" 341
 - 2.1 Paramétrage des threads. 341
3. Au niveau du backend 342
 - 3.1 Paramétrage du cache (ou la zone tampon) 342
 - 3.2 Paramétrage des index 346
 - 3.2.1 Syntaxe 347
 - 3.2.2 Exemples de configuration. 348
 - 3.2.3 Application 349
4. Changer de backend 349

Chapitre 18**Dépannage**

1. Liste de contrôle (checklist) 353
2. Activer le mode "debug" 355
3. Activer et modifier la verbosité des logs 356

Chapitre 19**L'autogestion des comptes utilisateurs**

1. Problématique. 361
2. Infrastructure de gestion des identités 362
 - 2.1 Fonctionnement général 362
 - 2.2 Création/modification de compte. 364
 - 2.3 Suppression de compte. 365

- 3. Présentation ITIM 366
 - 3.1 Bannière de connexion 368
 - 3.2 Espace de gestion des comptes de l'utilisateur 368
 - 3.3 Workflow 370
 - 3.4 Approbation 371
- 4. Intégration du serveur OpenLDAP dans ITIM. 373

Annexe

- 1. Le schéma "sudo" pour OpenLDAP 375
- 2. Quelques problèmes rencontrés. 377
 - 2.1 Cas 1 377
 - 2.2 Cas 2 378
 - 2.3 Cas 3 : reconfigurer le "checksum"
dans les fichiers de configuration 378
- 3. Déverrouiller les comptes. 379

- Index 383

Chapitre 6

△ Démarrage du serveur OpenLDAP

1. Introduction

Ce chapitre abordera les méthodes de démarrage et d'arrêt du service LDAP, ainsi que de ses différents paramètres de configuration.

2. Le service "slapd"

Le processus serveur d'OpenLDAP se nomme "slapd" et est géré sous Red Hat par le service du même nom. Celui-ci est fourni lors de l'installation du package `openldap-servers` par le script `/etc/rc.d/init.d/slapd` :

```
[root@ldap02 init.d]# rpm -ql openldap-servers-2.4.39
-8.el6.x86_64 | grep slapd
/etc/rc.d/init.d/slapd
...
```

Ce script agit donc sur le daemon "slapd" (`/usr/sbin/slapd`) en lui fournissant des paramètres issus du fichier de configuration : `/etc/sysconfig/ldap`, ce qui rend primordial son usage quand il s'agit de stopper ou de redémarrer le processus.

Les actions ainsi disponibles sont :

```
root@ldap02 sysconfig]# service slapd
Usage: /etc/init.d/slapd {start|stop|restart|force-
reload|status|condrestart|try-restart|configtest|usage}
[root@ldap02 sysconfig]#
```

Pour démarrer le service, il suffira de saisir par exemple :

```
service slapd start
```

Pour le stopper :

```
service slapd stop
```

Ou bien pour réaliser un redémarrage :

```
service slapd restart
```

3. Présentation des options de démarrage du processus "slapd"

Le processus (ou démon) "slapd" accepte des paramètres de configuration provenant du fichier : /etc/sysconfig/ldap.

Ces paramètres agissent essentiellement sur les adresses et les ports d'écoute du démon "slapd".

Exemple

```
[root@ldap02 sysconfig]# cat /etc/sysconfig/ldap
# Options of slapd (see man slapd)
#SLAPD_OPTIONS=

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

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

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

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

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

# Parameters to ulimit, use to change system limits for slapd
#SLAPD_ULIMIT_SETTINGS=""
[root@ldap02 sysconfig]#
```

Par exemple, dans le fichier ci-dessus, les paramètres `SLAPD_LDAP=yes` et `SLAPD_LDAPS=yes` indiquent au service LDAP d'écouter sur toutes ses interfaces réseau IP et sur les ports standards '389/TCP' pour les communications non sécurisées et '636/TCP' pour les communications sécurisées.

Un autre exemple serait d'utiliser le paramètre `SLAPD_URLS` et de lui donner les valeurs suivantes :

```
"ldaps://127.0.0.1:9009/ ldaps://10.10.110.41:636/ ldapi:///"
```

Cela configurerait le serveur LDAP à établir des communications non sécurisées en local seulement (loopback) et sur le port 9009/TCP, des communications sécurisées par SSL sur son interface configurée en 10.10.110.41 et sur le port standard 636/TCP, et enfin d'accepter des communications LDAP en IPC (*Unix domain sockets*).

D'autres paramètres de configuration du daemon "slapd" existent. La commande `man slapd` permet de les consulter. On y découvre par exemple, que le démon "slapd" va par défaut chercher le fichier de configuration du serveur LDAP à l'aide des paramètres `-f slapd-config-file` (valeur par défaut : `/etc/openldap/slapd.conf`) et `-F slapd-config-directory` (valeur par défaut : `/etc/openldap/slapd.d`).

Si les deux paramètres sont configurés, le démon "slapd" va convertir le 'slapd-config-file' pour le mettre dans le répertoire spécifié par le paramètre slapd-config-directory.

Si aucun des paramètres n'est spécifié, alors le démon "slapd" va lire en premier la configuration dans le répertoire : /etc/openldap/slapd.d ...s'il trouve une configuration valide, il ignore le fichier : /etc/openldap/slapd.conf et dans le cas contraire, il le consulte.

Le paramètre concernant le mode debug peut s'avérer également intéressant dans le cadre de recherche de pannes. Il suffira alors de se servir de la variable SLAPD_OPTIONS du fichier /etc/sysconfig/ldap et de mettre la valeur : -dX.

Exemple

```
# Options of slapd (see man slapd)
SLAPD_OPTIONS=-d1
```

Les différentes valeurs (X) peuvent se trouver en effectuant la commande suivante :

```
[root@ldap01]# slapd -d ?
Installed log subsystems:

....Any                (-1, 0xffffffff)
....Trace              (1, 0x1)
....Packets            (2, 0x2)
....Args               (4, 0x4)
....Conns              (8, 0x8)
....BER                (16, 0x10)
....Filter             (32, 0x20)
....Config             (64, 0x40)
....ACL                (128, 0x80)
....Stats              (256, 0x100)
....Stats2             (512, 0x200)
....Shell              (1024, 0x400)
....Parse              (2048, 0x800)
....Sync               (16384, 0x4000)
....None               (32768, 0x8000)
```

NOTE: custom log subsystems may be later installed by specific code

```
[root@ldap01]#
```

4. Vérification du démarrage automatique du service "slapd"

Nous pouvons ensuite vérifier que le processus "slapd" est bien démarré à l'aide d'une commande `ps -aef`, et qu'il s'est placé en écoute sur les ports prévus.

Pour cela; taper les commandes ci-dessous :

```
[root@ldap01 certs]# ps -ef | grep slapd
ldapd      5224      1  0 Jul01 ?        00:00:44 /usr/sbin/slapd
-h ldap:/// ldaps:/// ldapi:/// -u ldap
root      14572 14496  0 15:28 pts/0    00:00:00 grep slapd
```

```
[root@ldap01 Desktop]# netstat -atunp | grep -i slapd
tcp        0      0 0.0.0.0:389          0.0.0.0:*           LISTEN      2996/slapd
tcp        0      0 :::389             :::*                 LISTEN      2996/slapd
tcp        0      0 0.0.0.0:636        0.0.0.0:*           LISTEN      2996/slapd
tcp        0      0 :::636             :::*                 LISTEN      2996/slapd
```

Pour s'assurer du démarrage automatique du process "slapd", on peut sur une distribution Red Hat vérifier avec la commande `chkconfig` l'état d'activation pour chacun des niveaux d'exécution comme suit :

```
[root@ldap01 Desktop]# chkconfig --list | grep slapd
slapd      0:off  1:off  2:off  3:off  4:off  5:off  6:off
[root@ldap01 Desktop]# chkconfig --levels 2345 slapd on
[root@ldap01 Desktop]# chkconfig --list | grep slapd
slapd      0:off  1:off  2:on   3:on   4:on   5:on   6:off
[root@ldap01 Desktop]#
```

5. Démarrage et arrêt du processus "slapd" en ligne de commande

Il est aussi possible de démarrer le processus "slapd" sans l'aide d'un service, directement en lançant le fichier binaire et en spécifiant des paramètres comme vu précédemment :

```
/usr/sbin/slapd [<option>]
```

ou

```
/usr/local/libexec/slapd [<option>]
```

Exemple

```
[root@ldap01 libexec]# /usr/sbin/slapd -h ldap:///
[root@ldap01 libexec]# ps -aef | grep -i slapd
root      24634      1  0 22:37 ?          00:00:00 /usr/sbin/slapd
-h ldap:///
root      24642  2645  0 22:38 pts/0    00:00:00 grep -i slapd
[root@ldap01 libexec]#
```

Pour l'arrêt de ce processus, après s'être procuré le PID, il faudra utiliser la commande `kill` avec le signal `INT`.

Exemple

```
kill -INT <pid_slapd>
```