INFORMATIQUE
TECHNIQUE

Expert

LDAP

Planification et mise en œuvre d'un annuaire OpenLDAP

Stéphane ROPARS

eni

Table des matières

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

Chapitre 4
Installation/configuration d'un serveur OpenLDAP

Chapitre 5
Installer et configurer un navigateur LDAP

Chapitre 6
Démarrage du serveur OpenLDAP

Chapitre 7
Les schémas

Chapitre 8
Préparation des données de l'annuaire

Chapitre 9
Provisionner l'annuaire LDAP

Chapitre 10
Sécuriser un annuaire OpenLDAP

Chapitre 11
Protection des données de l'annuaire

Chapitre 12
Ajout de fonctionnalités appelées "overlay"

Chapitre 13
Configuration de clients LDAP

Chapitre 14
Sauvegarder/restaurer un annuaire OpenLDAP

Chapitre 15
La réplication

Chapitre 16
Surveillance d'un annuaire OpenLDAP

Chapitre 17
Amélioration des performances

Chapitre 18
Dépannage

Chapitre 19
L'autogestion des comptes utilisateurs

Annexe

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 :
"ldap://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 slap
ldap      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 slap

[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>
```