INSTALLATION ET CONFIGURATION DE OPENLDAP

Ce document a pour intérêt de décrire les étapes de l'installation et de la configuration de l'outil OpenLDAP sous l'OS FreeBSD 4.8

TABLE DES MATIERES

Etape 1 : Installation et Configuration de FreeBSD

Cette étape n'étant pas le sujet de ce document, nous ne détaillerons pas les parties de l'installation et de la configuration du système d'exploitation FreeBSD.

Il est juste nécessaire de spécifier que l'installation et la configuration de OpenLDAP ont été réalisés à partir de la version 4.8

Etape 2 : Installation de OpenLDAP

Cette installation nécessite la récupération des fichiers sources disponibles à partir du site www.openldap.org. Les sources utilisés pour ces tests sont ceux de la version OpenLDAP 2.1.17, compatible avec FreeBSD 4.8

1) Installation des sources de OpenLDAP

Une fois les sources de OpenLDAP récupérées, il faut les placer dans /usr/ports/distfiles.

Afin de gagner du temps, à l'appel du premier **make** pour compiler OpenLDAP, il va demander des dépendances qu'il faudra mettre dans */usr/ports/distfiles/bdb*. *Si le* ***make.conf*** n'a pas été changé voici les fichiers qu'il faudra récupérer :

db-4.1.25.tar.gz
patch.4.1.25.1

Ensuite pour compiler les sources, il faut se placer dans usr/ports/net/openldap21 puis **make** et ensuite **make install.**

L'installation de OpenLDAP se fait dans /usr/local/etc/openLDAP.

2) Démarrage/Arrêt du serveur LDAP

Pour lancer le démon slapd il est impératif que la database existe et qu'elle soit accessible.

Démarrage et arrêt du démon ldap :

- Pour le démarrer : **/usr/local/libexec/slapd**
- Pour l'arrêter : **kill –INT `cat /var/run/slapd.pid`**

3) Installation du module JAVA

L'installation de JAVA sera nécessaire dans l'optique de l'installation et de l'utilisation d'un client LDAP qui permettra par la suite de gérer la base Annuaire.

FreeBSD 4.8 possède dans les ports le package java1.4

Afin de compiler les sources java, il faut récupérer les sources sur Internet et les placer dans le répertoire */usr/ports/distfiles* :

bsd-jdk14-patches-3.tar.gz
j2sdk-1_4_1_02-linux-i586.bin
j2sdk-1_4_1-src-scsl.zip

Dans /usr/ports/java/jdk14 → make → make install

RMQ : Ne pas oublier le path pour utiliser JAVA

Etape 3 : Configuration de OpenLDAP

La configuration d'un serveur LDAP est la phase préliminaire à tout mise en œuvre de celui-ci. Elle est bien entendu spécifique à l'outil que vous utilisez. Dans le cas de OpenLDAP, cela consiste à éditer un fichier : slapd.conf

Le fichier slapd.conf est constitué de trois types d'informations de configuration : global, spécifique au backend, et spécifique à la base de données. L'information globale est spécifiée en premier, suivie par l'information associée à un type de backend particulier, qui est elle même suivie par l'information associée avec une instance de base de données particulière.

Les lignes blanches et les commentaires commençant par le caractère « # » sont ignorés. Si une ligne commence avec un espace, elle est considérée comme la continuation de la ligne précédente.

1) Gestion des schémas

Rappelons qu'un objet LDAP est décrit par des attributs et des classes d'objets. Un schéma regroupe les attributs et les classes d'objet que pourront posséder les objets de l'annuaire. Il précise pour chaque attribut et chaque classe les contraintes, les héritages, les syntaxes, les règles de comparaison,…

Dans le cas de l'outil OpenLDAP, les schémas sont des fichiers textes. Les schémas nécessaires au bon fonctionnement du serveur sont inclus dans le fichier slapd.conf

La ligne suivante :

include /usr/local/etc/openldap/schema/core.schema

va permettre de spécifier quel schéma l'annuaire doit mettre en œuvre. Ici ce fichier décrit le schéma de base de tous les annuaires LDAP. Il contient les définitions des attributs et classes d'objets standards. Ce schéma est obligatoire ; c'est le minimum attendu par un serveur LDAP.

Voici un extrait du fichier **core.schema** avec la classe 'person'

```
ObjectClass (2.5.6.6 NAME 'person'
        DESC 'RFC2256 : a person'
        SUP top structural
        MUST (sn, $ cn )
        MAY ( userPasswd $ telephoneNumber $ description $ seeAlso ))
```

Légende:

MUST correspond aux attributs obligatoires et MAY à ceux facultatifs
ObjectClass est le nom de la classe qui descend elle même de la classe top
sn correspond à nom
cn correspond à prénom + nom

Pour créer un annuaire contenant des fiches de personnes, il sera nécessaire de rajouter plusieurs schémas complémentaires tels que :

include /usr/local/etc/openldap/schema/inetorgperson.schema
include /usr/local/etc/openldap/schema/cosine.schema

Ces schémas permettent d'avoir une description plus intéressante des objets de l'annuaire.

2) Gestion du serveur

Le serveur, lors de son démarrage, essaye d'écrire dans deux fichiers particuliers ; s'il échoue dans l'écriture, ceci n'empêche pas son fonctionnement. Mais il vaut mieux que ces fichiers soient présents en cas de problèmes ultérieurs.

Les lignes suivantes :

pidfile /var/run/slapd.pid
argsfile /var/run/slapd.args

Le fichier slapd.pid contient le numéro du premier processus UNIX sous lequel le serveur tourne.
Le fichier slapd.args contient la liste des arguments avec lesquels a été lancé le serveur

3) Gestion de la base de donnée

La gestion de la base de donnée va permettre de préciser plusieurs choses :

- Le nom (suffixe) de la base de données
- L'identité (DN) du gestionnaire de la base
- L'endroit où seront stockés les différents fichiers représentant les données de l'annuaire

a) Le suffixe de la base

C'est en quelque sorte l'identifiant général de la base de données. Toutes les entrées de la base contiendront ce suffixe.

Il est définit ainsi : **dc=annucentre ,dc=fr**

b) Le gestionnaire de la base

C'est une entrée spéciale de la base. Elle peut être virtuelle. Elle est gérée par la ligne **rootdn**. La solution la plus simple consiste à utiliser une forme en fonction du choix du suffixe.

rootdn « cn=Manager, dc=annucentre , dc=fr »

Le gestionnaire de la base doit se connecter à l'aide d'un mot de passe ; celui-ci est décrit par la ligne suivante

rootpw secret

Le répertoire de stockage des données de l'annuaire est indiqué par la line suivante :

directory /var/db/openldap-data

4) Gestion des contrôles d'accès

L'accès aux entrées et attributs slapd est contrôlé par la directive de configuration d'accès. La forme générale d'une ligne d'accès est la suivante :

```
<access directive ::= access to <what>
        [by <who> <access><control>]
<what> ::=* | [dn.<target style>]=<regex>]
        [filter=<ldapfilter>] [attrs=<attrlist>]
<who> ::= [* | anonymous | users | self | [dn.<subject style>]
```

Où le <what> définit les entrées et/ou les attributs sur lesquelles les règles s'appliquent, le <who> définit quelles identités ont accès, et le <acces> définit le type d'accès.

Exemples :

 # Autorise la visualisation d'une entrée comprenant l'attribut organizationalStatus avec comme valeur parti uniquement à l'admin de l'annuaire et personne d'autre
access to attr=entry filter=(organizationalStatus=*parti)*
by dn="cn=Manager,dc=annucentre.fr" read
by dn="cn=Manager,dc=annucentre.fr" write
by * none

 # Autorise la consultation de toutes les entrées à tout le monde
*access to * by * read*

Extrait du fichier slapd.conf

```
# $OpenLDAP: pkg/ldap/servers/slapd/slapd.conf,v 1.23.2.7 2003/03/24 03:54:12 kurt Exp $
#
# See slapd.conf(5) for details on configuration options.
# This file should NOT be world readable.
#
include         /usr/local/etc/openldap/schema/core.schema
include         /usr/local/etc/openldap/schema/inetorgperson.schema
include         /usr/local/etc/openldap/schema/cosine.schema
include         /usr/local/etc/openldap/schema/nis.schema

pidfile         /var/run/slapd.pid
argsfile        /var/run/slapd.args

access to attr=entry filter=(organizationalStatus=parti)
        by dn="cn=Manager,dc=annucentre.fr" read
        by dn="cn=Manager,dc=annucentre.fr" write
        by * none

access to * by * read

 rootdn can always write!

database        bdb
suffix                  "dc=annucentre ,dc=fr"
rootdn                  "cn=Manager, dc=annucentre, dc=fr"

rootpw                  secret

directory       /var/db/openldap-data

index           default pres,eq
indexobjectClass
indexcn, s ,mail eq, sub, approx
```

Le fichier **ldap.conf** va permettre de définir l'URL vers laquelle on peut accéder au serveur LDAP. Il est important d'y spécifier également l'adresse IP de la machine ainsi que le DN de l'annuaire et le port de connexion.

Extrait du fichier ldap.conf

```
# $OpenLDAP: pkg/ldap/libraries/libldap/ldap.conf ,v 1.9 2000/09/04 19:57:01 kurt Exp $
#
# LDAP Defaults
#

# See ldap.conf(5) for details
# This file should be world readable but not world writable.

BASE            dc=annucentre, dc=fr
URI  ldap://xxx.xxx.xxx.xxx/dc=annucentre, dc=fr ldap://localhost:389

#SIZELIMIT 12
#TIMELIMIT          15
#DEREF              never
```

Etape 4 : Utilisation de OpenLDAP

Il existe différents moyens de manipuler des données de l'annuaire :

- En ligne de commande
- A l'aide du client LDAP Browser (cf. doc. LDAP Browser)

La seconde méthode étant détaillé dans un autre document, nous allons détailler la manipulation des données de l'annuaire en ligne de commande.

Les commandes LDAP existantes sont les suivantes :

- ldapadd,
- ldapcompare
- ldapmodrdn
- ldapdelete
- ldapmodify
- ldapsearch
- ldappasswd

1) Ajouter un enregistrement

Pour ajouter des données au serveur LDAP il faut fournir un fichier au format LDIF, le format est un format texte facilement lisible au contraire du format interne de l'annuaire.

Le format d'un fichier .ldif est le suivant :

Dn : description du distinguished name
ObjectClass : classe d'objet d'origine
…
objectClass : classe d'objet d'arrivée
type attribut : valeur

Exemple :

dn: dc=annucentre, dc=fr
objectClass: dcObject
objectClass: organization
dc: annucentre
o: sagem

Création du rootdn avec la syntaxe suivante dc=annucentre , dc=fr représentant l'organisation sagem (o)

dn: ou=SITES, dc=annucentre, dc=fr
objectClass: organizationalUnit
ou: SITES

Création de l'objet SITES qui est de type OrganizationalUnit. *Cette entité appartient à l'organisation* ***sagem****.*

dn: cn=Steve HERVE, ou=ERAGNY ,ou=SITES, dc=annucentre, dc=fr
cn: Steve HERVE
objectClass: person
objectClass: inetOrgPerson
sn: herve
mail: steve.herve@sagem.com
telephoneNumber:0134305911

Création de la fiche d'une personne qui appartient au ***SITES****, ce même service appartenant à l'organisation* ***sagem***

RMQ : Chaque enregistrement dans le fichier est séparé du précédent et du suivant par une ligne vierge. Les espaces sont pris en compte.
ATTENTION : Il est important qu'il n'y ait aucun espace en fin de ligne.

Pour ajouter l'enregistrement on utilisera la syntaxe suivante :

ldapadd –D « <description du DN de l'administrateurs> » -w –f <nom du fichier>.ldif

Exemple : On souhaite rajouter le fichier test.ldif crée ci-dessus

ldapadd –D « cn=Manager, dc=annucentre, dc=fr » -w –f test.ldif
Enter LDAP password : secret

Adding new entry « dc=annucentre ,dc=fr ».

Adding new entry « ou=SITES ,dc=annucentre, dc=fr ».

Adding new entry « cn=Steve HERVE, ou=SITES, dc=annucentre ,dc=fr ».

RMQ : Attention l'ajout d'un fichier .ldif ne fonctionne qu'une seule fois (ceci est du qu'au second lancement du fichier, il va percevoir une redondance des objets crées et va annuler l'ajout même si le fichier comporte de nouvelles informations). Pour le réutiliser, il faudra vider la base auparavant, sinon utiliser un autre fichier .ldif pour accroître l'annuaire

2) Rechercher un enregistrement

On utilisera la fonction ldapsearch. Pour visualiser tout l'annuaire on peut taper :

ldapsearch –b « dc=annucentre, dc=fr » '(objectClass=)'*

3) Modifier un enregistrement

a) Rajouter un attribut à un enregistrement

Pour rajouter l'attribut facultatif location (**l**) à l'enregistrement **Steve HERVE.** On va créer un fichier *modif.ldif contenant :*

dn: cn=Steve HERVE, ou=ERAGNY ,ou=SITES, dc=annucentre, dc=fr
add : l
title : extensionDOC

On tape ensuite :

ldapmodify –D "cn=Manager, dc=annucentre, dc=fr » -w –f modif.ldif
Enter LDAP password : secret
Modifying entry « cn=Steve HERVE, ou=SITES, dc=annucentre ,dc=fr ».

b) Modifier un attribut

On va modifier l'attribut titre (**title**) à l'enregistrement **Steve HERVE.** On va créer un fichier modif.ldif contenant :

dn: cn=Steve HERVE, ou=ERAGNY ,ou=SITES, dc=annucentre, dc=fr
changetype: modify

replace: telephoneNumber
telephoneNumber: 5911

On tape ensuite :

ldapmodify –D "cn=Manager, dc=annucentre, dc=fr » -w –f modif.ldif
Enter LDAP password : secret
Modifying entry « cn=Steve HERVE, ou=SITES, dc=annucentre ,dc=fr ».

c) Supprimer un attribut

On veut supprimer l'attribut location (**l**) à l'enregistrement **Steve HERVE.** On va créer un fichier *modif.ldif* contenant :

dn: cn=Steve HERVE, ou=ERAGNY ,ou=SITES, dc=annucentre, dc=fr
delete : l

On tape ensuite :

ldapmodify –D "cn=Manager, dc=annucentre, dc=fr » -w –f modif.ldif
Enter LDAP password : secret
Modifying entry « cn=Steve HERVE, ou=SITES, dc=annucentre ,dc=fr ».

4) Supprimer un enregistrement

On veut supprimer l'entrée Steve HERVE :

ldapdelete –v –D « cn=Manager,dc=annucentre.fr » -w « cn=Steve HERVE,dc=annucentre.fr »