

COMPTE RENDU TP1

Lightweight Directory Access Protocol (LDAP)

Matière Service d'annuaire

LDAP

Lightweight Directory
Access Protocol

Réalisé par :

Mme Kardiatou TOURE &
M. Mohamed Amine MZOUGH

Encadré par :

M. BONDJE Gaetan

BUT2 Réseaux et Télécommunications parcours Cybersécurité

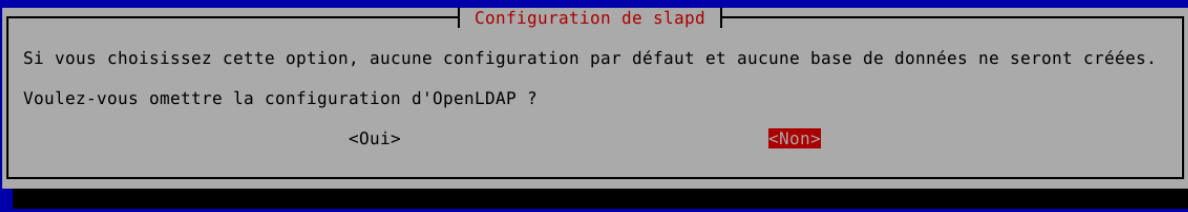
GROUPE 1

Lundi 14 Novembre 2022

Pour créer un squelette de configuration de slapd, nous allons utiliser la commande `apt-get install slapd` comme suit pour installer slapd:

```
q20309: root /home/mzmz# apt-get install slapd
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances
Lecture des informations d'état... Fait
slapd is already the newest version (2.4.44+dfsg-5+deb9u9).
Les paquets suivants ont été installés automatiquement et ne sont plus nécessaires :
  libdirectfb-1.2-9 libgles1-mesa libiso9660-8 libonig2 libqdbm14 libvcdinfo0 libvlccore8
Veuillez utiliser « sudo apt autoremove » pour les supprimer.
0 mis à jour, 0 nouvellement installés, 0 à enlever et 398 non mis à jour.
q20309: root /home/mzmz#
```

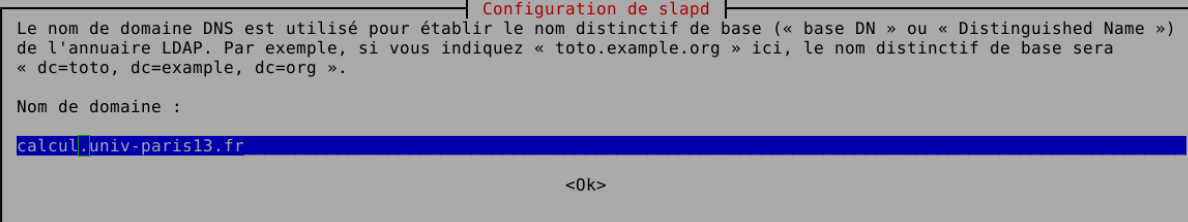
À l'invocation de cette commande, une suite de menus en ncurses va se succéder pour configurer le paquet slapd. Il faut utiliser la tabulation pour se déplacer dans ces menus et la touche Entrée pour valider. Deux captures suivent pour vous présenter l'aspect des menus . Le premier menu nous demande si on veut omettre la configuration de slapd, il faut évidemment répondre non



CONFIGURATION SLAPD - ETAPE 1

Après la configuration, on a choisi le mot de passe

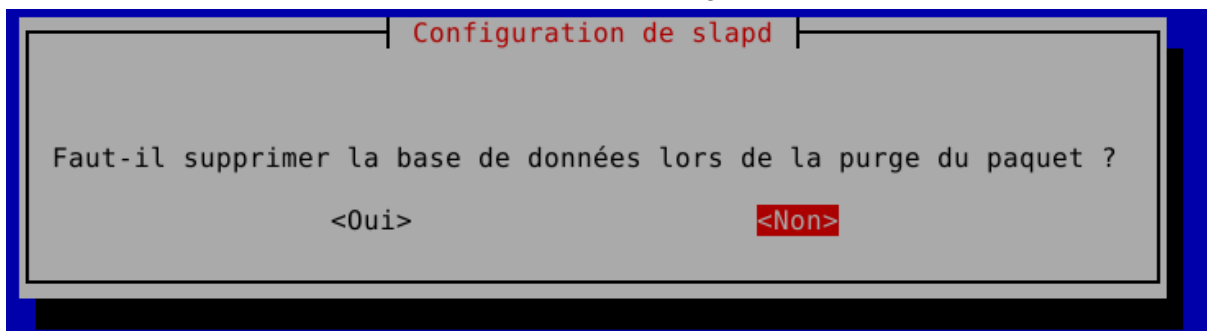
La question suivante sert à fixer la racine de l'annuaire LDAP. Comme vu dans la partie 1, cette racine va correspondre au domaine DNS. Nous entrons donc `calcul.univ-paris13.fr` comme notre nom de domaine.



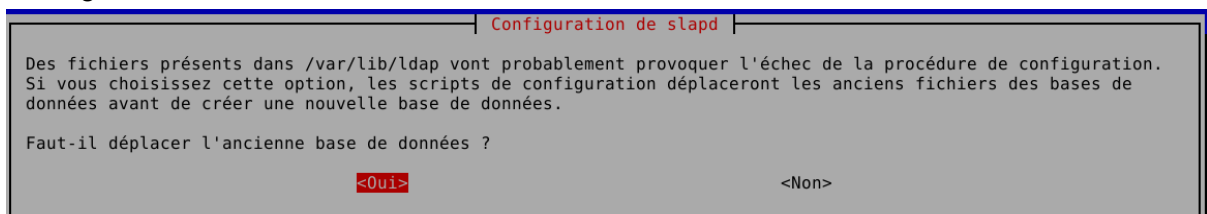
À l'issue de cette étape, la racine `dc=calcul,dc=univ-paris13,dc=fr` est créée. Ensuite, on fixe le moteur de base de données de l'annuaire. Nous choisirons MDB qui est le standard actuel.



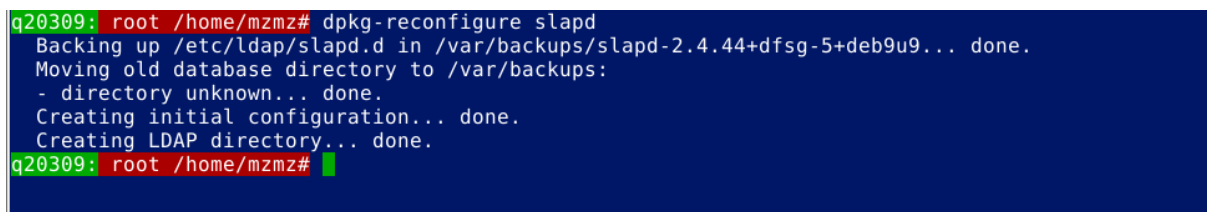
Après cela, nous devons choisir l'option en cas de purge, soit NON



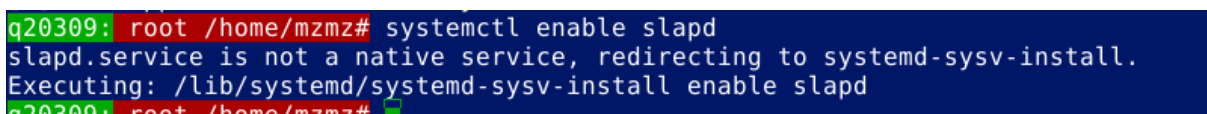
Enfin, dpkg-reconfigure demande s'il doit bouger la base de données actuelle pour la sauvegarder, le choix est évidemment oui.



Nous constatons que notre « slapd » est opérationnel



CONFIGURATION SLAPD - ETAPE 2



4. Tests fonctionnels

Les deux premières choses à faire sont respectivement d'activer slapd au démarrage et de le lancer. Ces actions se font avec systemctl :

Commençons par configurer les deux fichiers suivants : etc/hosts

```
Terminal - mzmz@q20309: ~
Fichier  Édition  Affichage  Terminal  Onglets  Aide
GNU nano 2.7.4                                Fichier : /etc/hosts

127.0.0.1    localhost
127.0.1.1    serveur.calcul.univ-paris13.fr  q20309

# The following lines are desirable for IPv6 capable hosts
::1         localhost ip6-localhost ip6-loopback
ff02::1     ip6-allnodes
ff02::2     ip6-allrouters
```

et ldap.conf

```
q20309: root /home/mzmz# gedit ldap.conf
```

5.

```
*ldap.conf
/home/mzmz

Ouvrir  [Icon]

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

BASE    dc=calcul,dc=univ-paris13.fr,dc=fr'
URI      ldap://serveur.calcul.univ-paris13.fr
#SIZELIMIT    12
#TIMELIMIT    15
#DEREF        never

#TLS certificates (needed for CNUtls)
TLS_CACERT    /etc/ssl/certes/ca-certificates.crt
```

On veut sur quel port réseau écoute slapd pour cela nous utilisons la commande netstat -laptun | grep slapd

```
q20309: root /home/mzmz# netstat -laptun|grep slapd
tcp        0      0 0.0.0.0:389          0.0.0.0:*           LISTEN      4605/slapd
tcp6       0      0 :::389             :::*                LISTEN      4605/slapd
q20309: root /home/mzmz#
```

Regardons avec quels arguments s'exécute le service :

```
q20309: root /home/mzmz# cat /var/run/slapd/slapd.args
/usr/sbin/slapd -h ldap:/// ldapi:/// -g openldap -u openldap -F /etc/ldap/slapd.d
```

On installe un outil pour un affichage ultime

```

q20309: root /home/mzmz# apt-get install ldap-utils
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances
Lecture des informations d'état... Fait
Les paquets suivants ont été installés automatiquement et ne sont plus nécessaires :
  libdirectfb-1.2-9 libgles1-mesa libiso9660-8 libonig2 libqdbm14 libvcdinfo0 libvllcore8
Veuillez utiliser « sudo apt autoremove » pour les supprimer.
Paquets suggérés :
  libsasl2-modules-gssapi-mit | libsasl2-modules-gssapi-heimdal
Les NOUVEAUX paquets suivants seront installés :
  ldap-utils
0 mis à jour, 1 nouvellement installés, 0 à enlever et 398 non mis à jour.
Il est nécessaire de prendre 193 ko dans les archives.
Après cette opération, 686 ko d'espace disque supplémentaires seront utilisés.
Réception de:1 http://security.debian.org stretch/updates/main amd64 ldap-utils amd64 2.4.44+dfsg-5+deb9u9 [193 kB]
193 ko réceptionnés en 0s (10,7 Mo/s)
Sélection du paquet ldap-utils précédemment désélectionné.
(Lecture de la base de données... 139289 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de .../ldap-utils_2.4.44+dfsg-5+deb9u9_amd64.deb ...
Dépaquetage de ldap-utils (2.4.44+dfsg-5+deb9u9) ...
Paramétrage de ldap-utils (2.4.44+dfsg-5+deb9u9) ...
Traitement des actions différées (« triggers ») pour man-db (2.7.6.1-2) ...
localepurge: Disk space freed in /usr/share/locale: 0 KiB
localepurge: Disk space freed in /usr/share/man: 0 KiB
localepurge: Disk space freed in /usr/share/gnome/help: 0 KiB
localepurge: Disk space freed in /usr/share/omf: 0 KiB

Total disk space freed by localepurge: 0 KiB

```

```

q20309: root /home/mzmz# ldapsearch -x -H ldap://serveur.calcul.univ-paris13.fr -b'dc=calcul,dc=univ-paris13,dc=fr'
# extended LDIF
#
# LDAPv3
# base <dc=calcul,dc=univ-paris13,dc=fr> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#
# calcul.univ-paris13.fr
dn: dc=calcul,dc=univ-paris13,dc=fr
objectClass: top
objectClass: dcObject
objectClass: organization
o: iutv.univ-paris13.fr
dc: calcul
# admin, calcul.univ-paris13.fr
dn: cn=admin,dc=calcul,dc=univ-paris13,dc=fr
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator
# search result
search: 2
result: 0 Success

# numResponses: 3
# numEntries: 2
q20309: root /home/mzmz# █

```

6. Peuplement de l'annuaire

Nous allons peupler l'annuaire en créant les deux OU puis un compte système avec son groupe primaire. Dans le monde LDAP, les données à ajouter à l'annuaire peuvent être inscrites dans un fichier rédigé au format LDIF (LDAP Data Interchange Format). Ce format présente les objets à manipuler dans l'annuaire accompagnés de leurs attributs. Par exemple, pour nos deux OU le fichier se présente de la façon suivante :

```
Fichier  Édition  Affichage  Terminal  Onglets  Aide
GNU nano 2.7.4                                Fichier : ou.ldif
dn:ou=posixaccounts,dc=calcul,dc=univ-paris13,dc=fr
objectclass: OrganizationalUnit
dn:ou=posixgroups,dc=calcul,dc=univ-paris13,dc=fr
objectclass: OrganizationalUnit
```

Pour créer l'empreinte du mot de passe userPassword, il est possible d'utiliser la commande slappasswd comme suit :

```
q20309: root /home/mzmz# slappasswd
New password:
Re-enter new password:
{SSHA}mzV0hfqzP8ERDa8YrjW3q7DExn1W138c
q20309: root /home/mzmz#
```

7. Sécurisation avec SSL

7.1 Création des certificats

Le plus simple est de créer un sous-répertoire ssl où mettre le certificat et de se placer dedans :

```
q20309: root /home/mzmz# /etc/ldap/ssl # mkdir/etc/ldap/ssl&&cd/etc/ldap/ssl
```

on veut générer un certificat autosigné en utilisant openssl

```
q20309: root /home/mzmz# openssl
OpenSSL>
req: Unknown digest <NULL>
req: Use -help for summary.
error in req
OpenSSL>
OpenSSL>
```

La clé privée ne doit être accessible que par root :

```
[1]+  Stoppé                                openssl
q20309: root /home/mzmz# ~/config/slapd# chmod 400 /etc/ldap/ssl/key.pem
```

7.2 Configuration de slapd

Le fichier à utiliser

```
q20309: root /home/mzmz# cat cert.ldif
```

commencer l'authentification

Verification:

```
q20309: root /home/mzmz# ldapmodify -Y EXTERNAL -H ldapi:/// -f cert.ldif
```

```
q20309: root /home/mzmz# vim.tiny /etc/defaults/slapd
```

```
[4]+  Stoppé vim.tiny /etc/defaults/slapd
```

```
q20309: root /home/mzmz#
```