Wang Peng Chao
Brahimi Ayman

TP LDAP

Introduction

Le but de ce TP est d'installer LDAP afin de créer notre propre accès aux services d'annuaire et gestion.

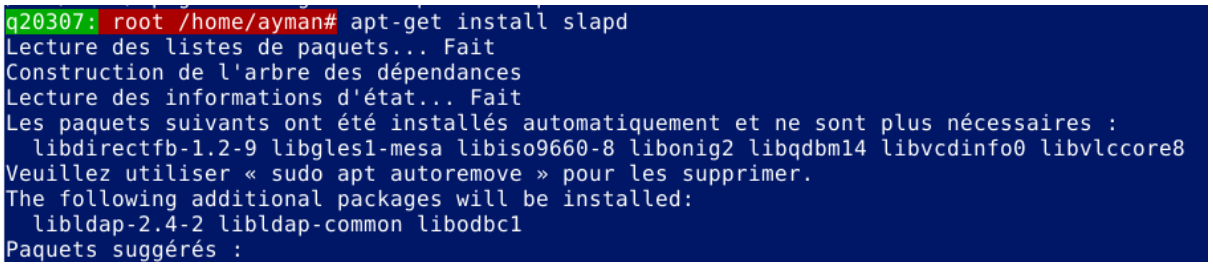
Dans un premier temps, on doit configurer sur le serveur le squelette de configuration de slapd.
Puis, dans un deuxième temps, on doit tester le fonctionnement.
Ensuite, dans un troisième temps, on doit peupler l'annuaire pour initialiser les listes des auteurs à partir d'une recherche sur une annuelle LDAP.
A la fin , on doit créer des certificats pour sécuriser l'annuaire.

Le serveur:

1)Création d'un squelette de configuration de slapd :

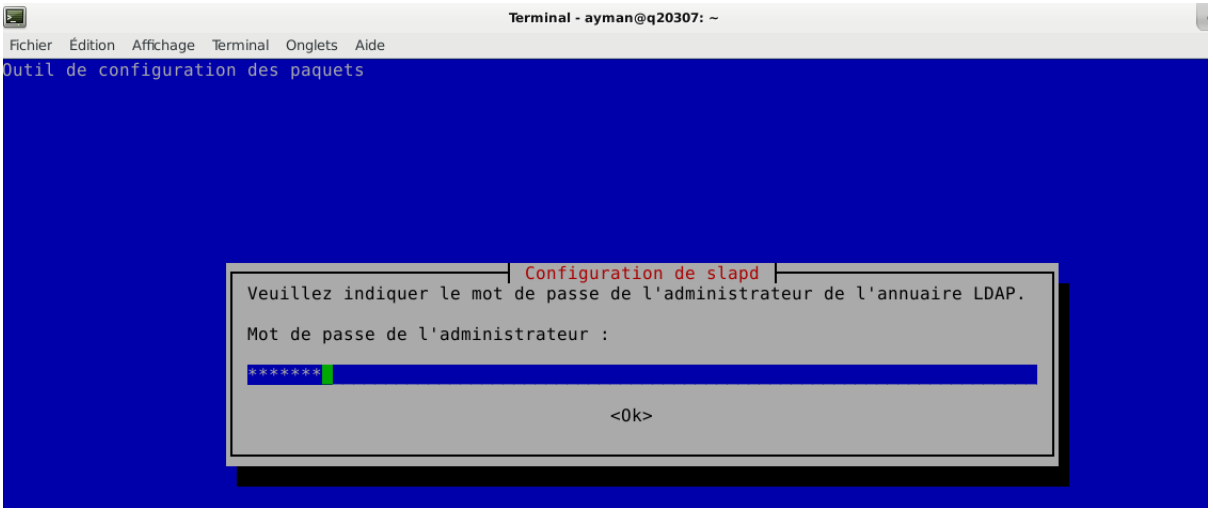
Tout d'abord , on utilise la commande "sudo su" pour pouvoir se connecter en Admin. Puis,on utilise la commande "apt-get update" pour avoir les dernières versions de debian afin d'installer les paquets sldap.

On utilise la commande "apt-get install slapd" pour l'installation de LDAP.

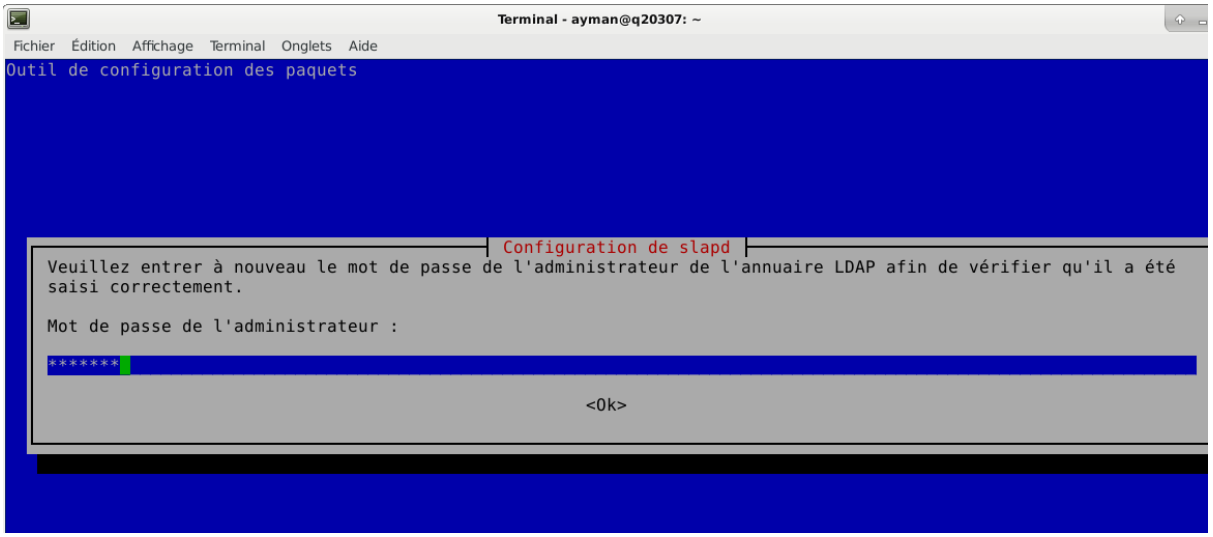


2) Configuration slapd étape 1 :

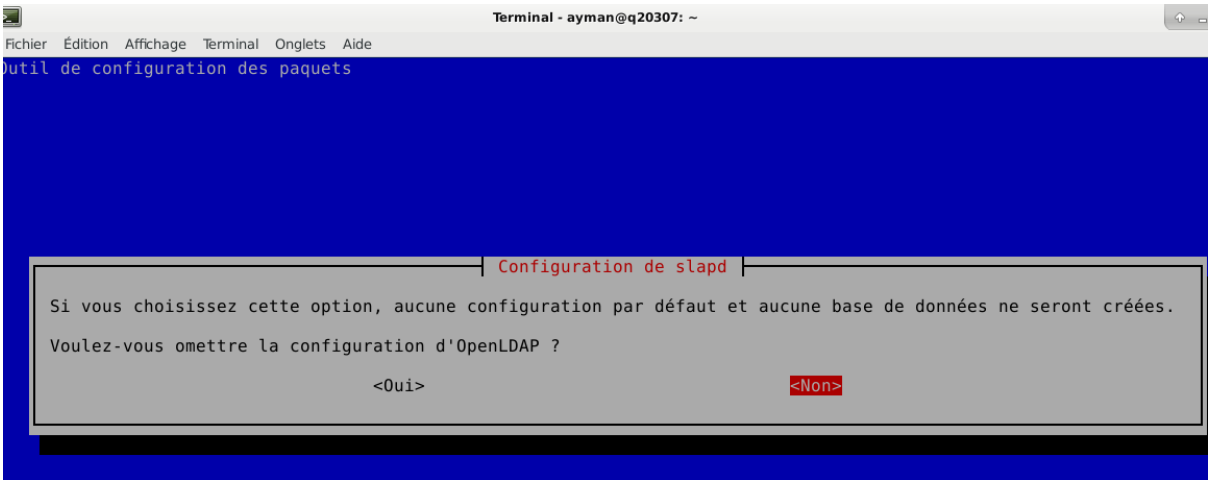
On utilise la commande dpkg-reconfigure slapd pour faire la configuration de slapd

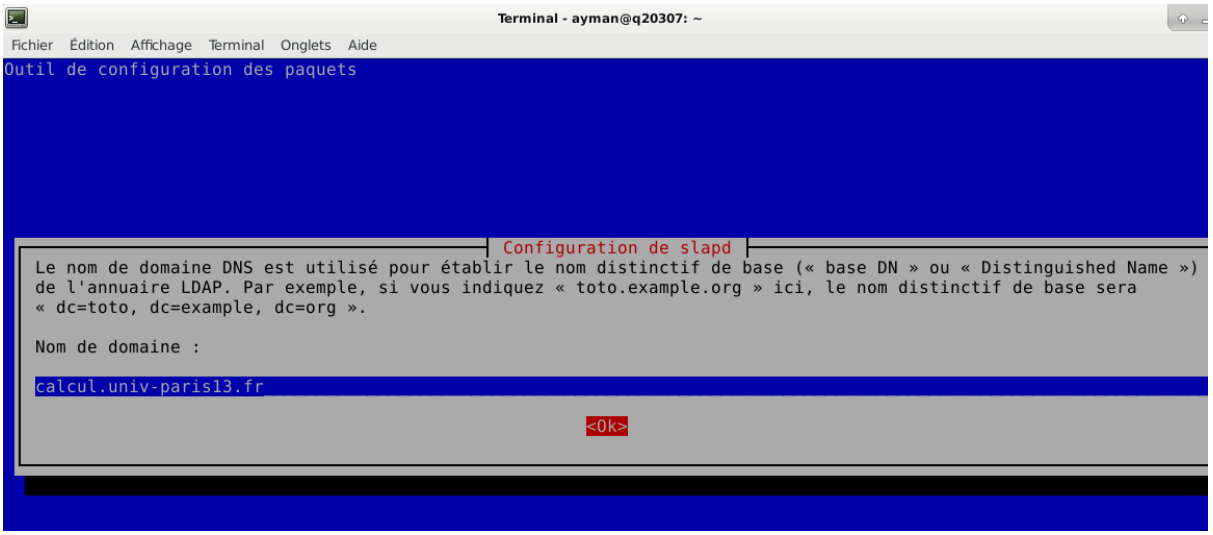


On crée un mot de passe de l'administration

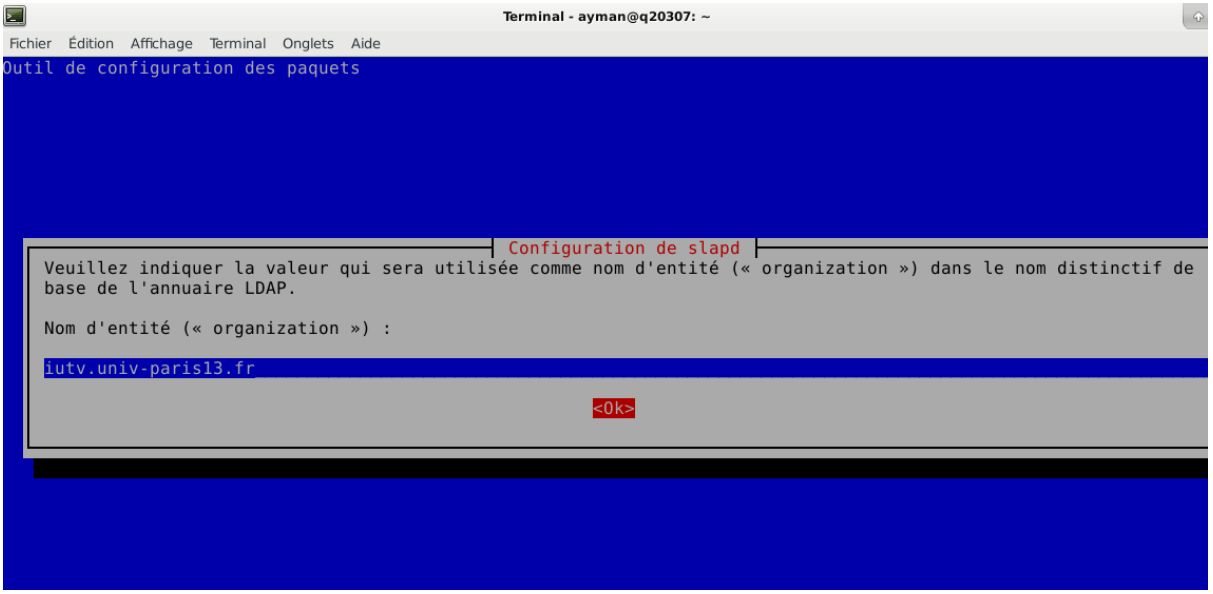


Dans cette partie, nous allons fixer la racine de l’annuaire LDAP, cette racine va correspondre au domaine DNS.
On entre le nom de domaine “calcul.univ-paris13.fr”

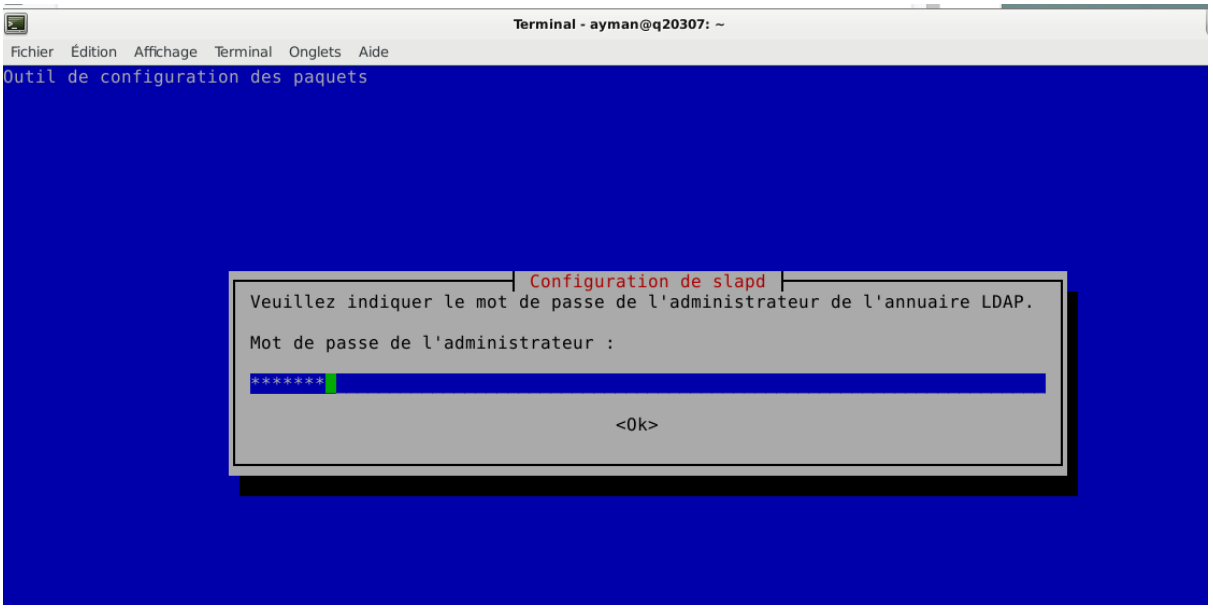




Pour le choix du Nom d'entité, on a choisit "iutv.univ-paris13.fr"



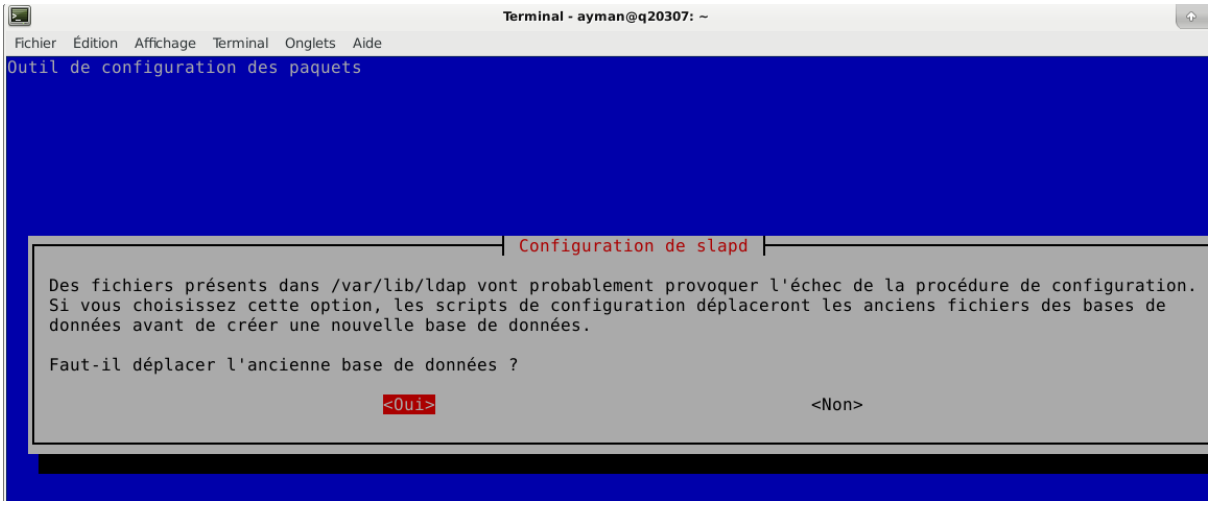
Puis, on crée un mot de passe de l'administration



On remarque que la racine dc=calcul, dc=univ-paris13,dc=fr est crée. On doit fixer le moteur de base de données de l'annuaire, on choisit "MDP" qui est le standard actuel.

Ensuite, on choisit l'option "NON" en cas de purge. Le purge intervient lorsque l'on utilise l'option –purge à la suppression d'un paquet avec apt-get.

Cette configuration nous demande de bouger la base de données actuelle pour la sauvegarde, on choisit “Oui”.



Avec la commande “systemctl enable slapd” , on remarque que “slapd” est opérationnel

```
q20307: root /home/ayman# dpkg-reconfigure slapd
  Backing up /etc/ldap/slapd.d in /var/backups/slapd-2.4.44+dfsg-5+deb9u9... done.
  Moving old database directory to /var/backups:
  - directory unknown... done.
  Creating initial configuration... done.
  Creating LDAP directory... done.
q20307: root /home/ayman#
```

```
q20307: root /home/ayman# systemctl enable slapd
slapd.service is not a native service, redirecting to systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable slapd
q20307: root /home/ayman#
```

```
q20307: root /home/ayman# /lib/systemd/systemd-sysv-install enable slapd
q20307: root /home/ayman#
```

4) Test fonctionnels:

On procède au test de fonctionnement de slapd, pour pouvoir activer slapd au démarrage et de le lancer, on utilise le systemctl :

```
q20307: root /home/ayman# systemctl enable slapd
slapd.service is not a native service, redirecting to systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable slapd
q20307: root /home/ayman#
```

```
q20307: root /home/ayman# /lib/systemd/systemd-sysv-install enable slapd
q20307: root /home/ayman# systemctl start slapd
q20307: root /home/ayman#
```

Voici la configuration de /etc/hosts

Ouvrir | *hosts /etc | Enregistrer

```
127.0.0.1       localhost
127.0.1.1       serveur.calcul.univ-paris13.fr  q20307

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

Voici la configuration de ldap.conf

Ouvrir

ldap.conf
/home/ayman

```
# See ldap.conf(5) for details
# This file should be word 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 GnuTLS)
TLS_CACERT      /etc/ssl/certs/ca-certificates.crt
```

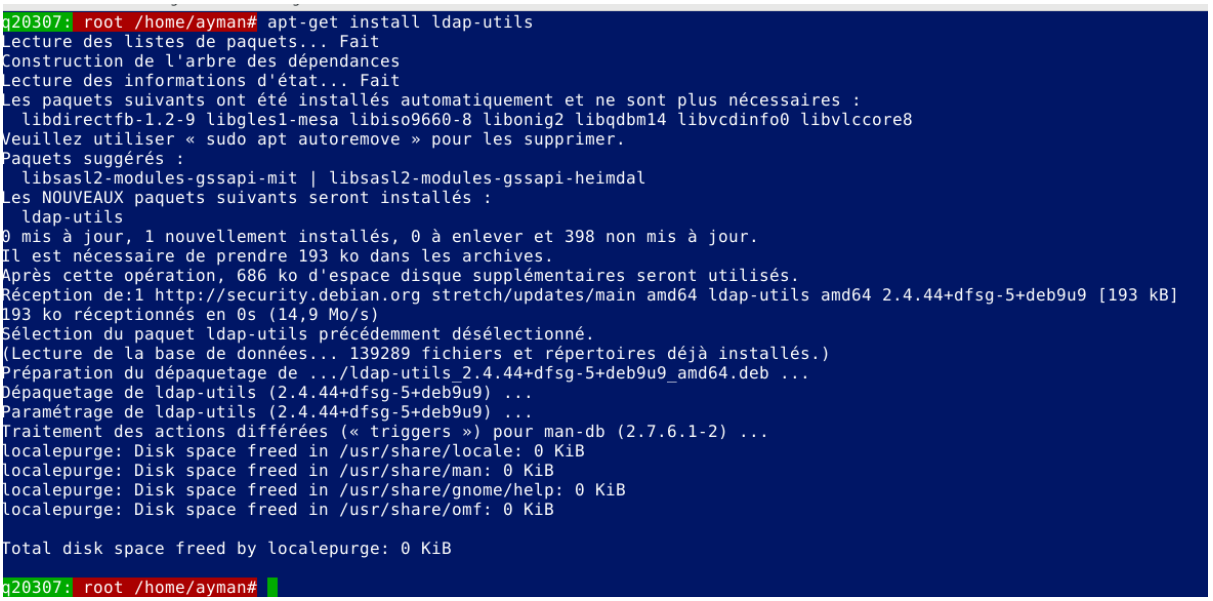
On utilise la commande “systemctl start slapd” pour pouvoir activer slapd
On utilise la commande netstat -laputn | grep slapd pour écouter les ports et les connexions internet actives (serveurs établies).
On voit que slapd attend les requêtes LDAP sur le port TCP 389.

```
q20307: root /home/ayman# systemctl start slapd
q20307: root /home/ayman# netstat -laputn |grep dlapd
q20307: root /home/ayman# netstat -laputn |grep slapd
tcp        0      0 0.0.0.0:389             0.0.0.0:*               LISTEN      4673/slapd
tcp6       0      0 :::389                  :::*                    LISTEN      4673/slapd
q20307: root /home/ayman#
```

On utilise la commande cat /var/run/slapd.args pour exécuter le service

```
q20307: root /home/ayman# cat /var/run/slapd/slapd.args
/usr/sbin/slapd -h ldap:/// ldapi:/// -g openldap -u openldap -F /etc/ldap/slapd.d
q20307: root /home/ayman#
```

On utilise la commande “apt-get install ldap-utils” pour installer ldap-utils afin d’afficher des données de l’annuaire.



On utilise la commande ldapsearch -x -H ldap://serveur.calcul.univ-paris13.fr -b’dc=calcul,dc=univ-paris13,dc=fr’ pour afficher les données de l’annuaire.

```
q20307: root /home/ayman# 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
q20307: root /home/ayman#
```

6)Peuplement de l'annuaire:

Dans cette partie, il faut peupler l'annuaire en créant les deux OU puis un compte système avec son groupe primaire.

On utilise la commande "cat ou.ldif" pour afficher le fichier de l'annuaire.

```
q20307: root /home/ayman# cat 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
q20307: root /home/ayman#
```

On utilise la commande "cat userandupg.ldif" pour lire le fichier userandupg.ldif

Dans ce fichier , on voit deux comptes qu'il contient deux objets le compte:
système'uid=nicolas.greneche,ou=posixaccounts,dc=calcul,dc=univ-paris13,dc=fr'
(objectclass posixAccount) et le groupe primaire associé
'cn=nicolas.greneche,ou=posixgroups,dc=calcul,dc=univ-paris13,dc=fr'
(objectclass posixGroup),

```
q20307: root /home/ayman# cat userandupg.ldif

dn: uid=nicolas.greneche,ou=posixaccounts,dc=calcul,dc=univ-paris13,dc=fr
uid: nicolas.greneche
sn: nicolas.greneche
homeDirectory: /home/nicolas.greneche
cn: nicolas.greneche
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: top
loginShell: /bin/bash
uidNumber: 6001
gidNumber: 6001
gecos: nico
mail: nicolas.greneche@univ-paris13.fr
userPassword: {SSHA}XXXXXXXXXXXXXXXXXXXXXXX
dn: cn=nicolas.greneche,ou=posixgroups,dc=calcul,dc=univ-paris13,dc=fr
objectClass: posixGroup
objectClass: top
gidNumber: 6001
q20307: root /home/ayman#
```

Pour créer l'empreinte du mot de passe userPassword , on utilise la commande "slappasswd"

```
q20307: root /home/ayman# slappasswd
New password:
Re-enter new password:
{SSHA}kTd8U7U+Et6+otlIJ3g4gZWjgTOXhrtQ
q20307: root /home/ayman#
```

7)Sécurisation avec SSL:

SSL (Secure Socket Layer) est une couche additionnelle à TCP ajoutant une propriété de confidentialité à la connexion en chiffrant les échanges lors de son établissement. La sécurisation de notre serveur LDAP va se résumer à activer l'accès en ldaps (en plus du ldap
et ldapi mentionnés ci-dessus). Pour autoriser l'accès en ldaps, il faut modifier les paramètres de lancement du service ldap pour ajouter ldaps à ldap et ldapi et générer un certificat.
Commençons par le certificat.

On utilise la commande mkdir pour crée le répertoir /etc/ldap/ssl

On va utiliser la commande openssl, qui nous permettra de générer un certificat auto signé.