istic

UNIVERSITÉ DE RENNES 1

Master 2 RSH

TP7 ADMI

ANNUAIRE LDAP

Encadré par:
Ahmad FADEL

Réalisé par:
Fanny PRIEUR / **Lorenzo MAZZOCCHI**

Année 2018/2019

Table des matières

I-Introduction et but du TP7

Le but du TP7 est de nous familiariser avec l'utilisation des annuaires LDAP (Lightweight Directory Access Protocol) comme base d'authentification d'utilisateurs de système Unix, ou pour d'autres types d'application tel que : Apache, Samba, Postfix etc.. Pour cela, nous nous baserons sur le serveur open source OpenLDAP.

Les annuaires LDAP (Lightweight Directory Access Protocol) se situent au cœur des fonctions de communication et de collaboration de l'entreprise à travers son Intranet car ils en simplifient la gestion et l'administration. La mise en œuvre d'un annuaire LDAP au sein d'un Intranet apporte donc une gestion optimale des utilisateurs et de leurs profils, des ressources, et la possibilité de partager ce référentiel avec l'ensemble.

LDAP est un standard destiné à normaliser l'interface d'accès aux annuaires.

LDAP simplifie la gestion des profils de personnes et de ressources, favorise l'interopérabilité des systèmes d'informations à travers le partage de ces profils, et améliore la sécurité d'accès aux applications.

Ce standard se représente par 3 notions importantes :

- Le protocole d'échange d'informations ; TCP/IP
- La nature des données : 4 modèles
- Les interfaces : LDIF

LDIF : LDAP Data Interchange Format (LDIF) permet de représenter les données LDAP sous format texte standardisé, il est utilisé pour afficher ou modifier les données de la base. Il a vocation à donner une lisibilité des données pour le commun des mortels.
LDIF est utilisé dans deux optiques :

- Faire des imports/exports de base
- Faire des modifications sur des entrées.

II-Service d'annuaire LDAP

Un service d'annuaire est une base de données spécialement optimisée pour la recherche, le survol et la lecture rapide d'informations. Elle stocke des données légèrement typées, organisées selon des classes particulières et présentées dans un arbre. L'exemple le plus commun dont il tire son nom est l'annuaire de personnes. Mais il peut stocker bien d'autres choses : des comptes Unix, des données personnelles (carnet d'adresses, photos, numéros de téléphone etc..), un parc matériels (imprimantes, pc etc..). Pour cela LDAP dispose de plusieurs schémas (Exemple: nis.schema pour l'authentification unix) en plus des schémas standard (core.schema).

III-Configuration d'OpenLDAP

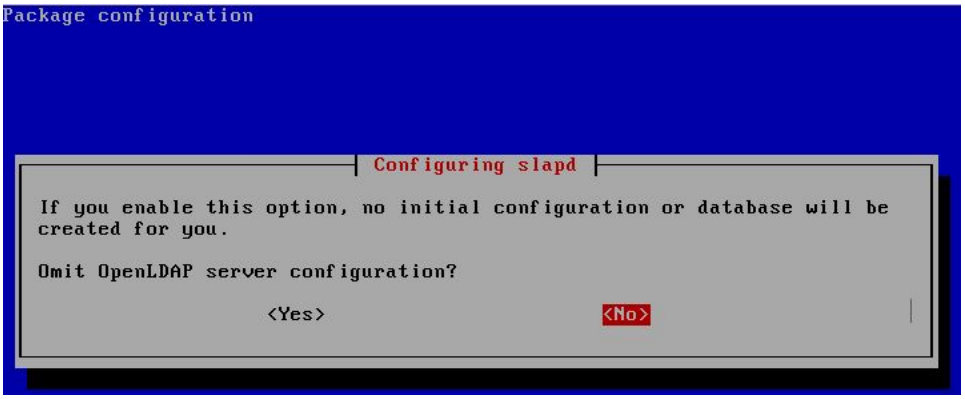
OpenLDAP est un annuaire libre mettant en oeuvre le protocole LDAP, sous une licence qui est équivalente à la license BSD révisée. Il est dérivé du serveur LDAP de l'Université du Michigan, et a largement évolué depuis. Historiquement, la configuration de LDAP reposait uniquement sur le fichier **slapd.conf.** A partir de la version 2.23, ce fichier a été éclaté en sous fichiers disponibles dans le répertoire **/usr/share/slapd**. Pour plus de détails voir le lien suivant http://www.openldap.org/doc/admin24/slapdconf2.html

Nous allons installer les paquets **slapd** et **ldap-utils** ainsi que toute les dépendances. lors de l'installation, **slapd** peut nous demander un mot de passe, dans ce cas entrer **"secret"**.

Durant le TP nous avons la responsabilité du domaine m0X.i207 (X le numéro de notre machine). Pour reconfigurer LDAP, on utilisera l'outil disponible avec Debian pour la reconfiguration des packages. Nous entrons alors la commande :

```
$dpkg-reconfigure slapd
```

Nous obtenons une interface graphique sur laquelle nous pourrons configurer les paramètres qui vont suivre.



Interface graphique de la configuration du service slapd

A partir d'ici, nous entrons les paramètres suivant à chaque nouvelle fenêtre de l'interface graphique de configuration de slapd:

- Omit LDAP server configuration : non
- Domain DNS : m0X.i207
- Organization : m2pro
- Mot de passe de l'admin : secret
- Type de base de données : HDB
- Do you want the database to be removed when slapd is purged : non
- Purger la vieille BD : non
- Utiliser le protocole LDAPv2 : non

Nous pouvons à présent lancer le service slapd en utilisant la commande :

```
$/etc/init.d/slapd start
```

1. Pour obtenir le port TCP utilisé par notre serveur LDAP nous entrons la commande suivante :

```
$netstat -antp
```

```
root@localhost:~# /etc/init.d/slapd start
[ ok ] Starting slapd (via systemctl): slapd.service.
root@localhost:~# netstat -antp
Connexions Internet actives (serveurs et établies)
Proto Recv-Q Send-Q Adresse locale          Adresse distante        Etat        PID/Program name
tcp        0      0 0.0.0.0:389             0.0.0.0:*               LISTEN      10238/slapd
tcp        0      0 0.0.0.0:902             0.0.0.0:*               LISTEN      1071/vmware-authdla
```

Démarrage du service slapd et affichage du port TCP pour slapd ainsi que preuve qu'il est bien en LISTEN

Il existe d'autres moyen d'obtenir cette information mais nous avons choisi cette commande car nous l'avons utilisé lors des TPs précédent.

Nous remarquons que le port TCP utilisé par le serveur LDAP est le **port 389** que cela soit sur IPv4 ou IPv6.

2. A l'aide de la commande netstat nous vérifions que le serveur est bien en écoute sur le port TCP numéro 389.

```
$netstat -antp
```

Nous pouvions aussi utiliser la commande qui suit pour plus de précision:

```
$netstat -ant | grep LISTEN
```

```
root@localhost:~# /etc/init.d/slapd start
[ ok ] Starting slapd (via systemctl): slapd.service.
root@localhost:~# netstat -antp
Connexions Internet actives (serveurs et établies)
Proto Recv-Q Send-Q Adresse locale          Adresse distante        Etat        PID/Program name
tcp        0      0 0.0.0.0:389             0.0.0.0:*               LISTEN      10238/slapd
tcp        0      0 0.0.0.0:902             0.0.0.0:*               LISTEN      1071/vmware-authdla
tcp        0      0 0.0.0.0:111             0.0.0.0:*               LISTEN      571/rpcbind
tcp        0      0 0.0.0.0:38483           0.0.0.0:*               LISTEN      580/rpc.statd
tcp        0      0 148.60.12.3:53          0.0.0.0:*               LISTEN      603/named
tcp        0      0 127.0.0.1:53            0.0.0.0:*               LISTEN      603/named
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      718/sshd
tcp        0      0 127.0.0.1:25            0.0.0.0:*               LISTEN      1017/exim4
tcp        0      0 127.0.0.1:953           0.0.0.0:*               LISTEN      603/named
tcp        0      0 148.60.12.3:50317       64.233.166.189:443      TIME_WAIT   -
tcp        0      0 148.60.12.3:59511       172.217.21.67:443       ESTABLISHED 2332/x-www-browser
tcp        0      0 148.60.12.3:50316       64.233.166.189:443      ESTABLISHED 2332/x-www-browser
tcp        0      0 148.60.12.3:40491       172.217.21.78:443       ESTABLISHED 2332/x-www-browser
tcp6       0      0 :::389                  :::*                    LISTEN      10238/slapd
tcp6       0      0 :::902                  :::*                    LISTEN      1071/vmware-authdla
tcp6       0      0 :::111                  :::*                    LISTEN      571/rpcbind
tcp6       0      0 :::53                   :::*                    LISTEN      603/named
tcp6       0      0 :::22                   :::*                    LISTEN      718/sshd
tcp6       0      0 :::56759                :::*                    LISTEN      580/rpc.statd
tcp6       0      0 ::1:25                  :::*                    LISTEN      1017/exim4
tcp6       0      0 ::1:953                 :::*                    LISTEN      603/named
```

Démarrage du service slapd et affichage du port TCP pour slapd ainsi que preuve qu'il est bien en LISTEN

3. Afin de vérifier que le serveur est bien démarré, on l'interroge en utilisant la commande ldapsearch. Mais avant, renseignons nous sur la commande ldapsearch.

```
$man ldapsearch
```

```
LDAPSEARCH(1)                                General Commands Manual                                LDAPSEARCH(1)

NAME
       ldapsearch - LDAP search tool

SYNOPSIS
       ldapsearch [-V[V]] [-d debuglevel] [-n] [-v] [-c] [-u] [-t[t]] [-T path] [-F prefix] [-A] [-L[L[L]]] [-S attribute]
       [-b searchbase]    [-s {base|one|sub|children}]    [-a {never|always|search|find}]    [-l timelimit]    [-z sizelimit]
       [-f file]  [-M[M]]  [-x]  [-D binddn]  [-W]  [-w passwd]  [-y passwdfile]  [-H ldapuri] [-h ldaphost] [-p ldapport]
       [-P {2|3}] [-e [!]ext[=extparam]] [-E [!]ext[=extparam]]  [-o opt[=optparam]]  [-O security-properties]  [-I]  [-Q]
       [-N] [-U authcid] [-R realm] [-X authzid] [-Y mech] [-Z[Z]] filter [attrs...]

DESCRIPTION
       ldapsearch is a shell-accessible interface to the ldap_search_ext(3) library call.

       ldapsearch  opens  a  connection  to an LDAP server, binds, and performs a search using specified parameters.   The
       filter should conform to the string representation for search filters as defined in RFC 4515.  If not provided, the
       default filter, (objectClass=*), is used.

       If  ldapsearch finds one or more entries, the attributes specified by attrs are returned.  If * is listed, all user
       attributes are returned.  If + is listed, all operational attributes are returned.  If no  attrs  are  listed,  all
       user attributes are returned.  If only 1.1 is listed, no attributes will be returned.

       The search results are displayed using an extended version of LDIF.  Option -L controls the format of the output.
```

```
-b searchbase
       Use searchbase as the starting point for the search instead of the default.

-s {base|one|sub|children}
       Specify the scope of the search to be one of base, one, sub, or children to specify a base object, one-
       level, subtree, or children search. The default is sub. Note: children scope requires LDAPv3 subordinate
       feature extension.

-a {never|always|search|find}
       Specify how aliases dereferencing is done. Should be one of never, always, search, or find to specify that
       aliases are never dereferenced, always dereferenced, dereferenced when searching, or dereferenced only when
       locating the base object for the search. The default is to never dereference aliases.

-l timelimit
       wait at most timelimit seconds for a search to complete. A timelimit of 0 (zero) or none means no limit. A
       timelimit of max means the maximum integer allowable by the protocol. A server may impose a maximal time-
       limit which only the root user may override.

-z sizelimit
       retrieve at most sizelimit entries for a search. A sizelimit of 0 (zero) or none means no limit. A size-
       limit of max means the maximum integer allowable by the protocol. A server may impose a maximal sizelimit
       which only the root user may override.

-f file
       Read a series of lines from file, performing one LDAP search for each line. In this case, the filter given
       on the command line is treated as a pattern where the first and only occurrence of %s is replaced with a
       line from file. Any other occurrence of the the % character in the pattern will be regarded as an error.
       Where it is desired that the search filter include a % character, the character should be encoded as \25
       (see RFC 4515). If file is a single - character, then the lines are read from standard input. ldapsearch
       will exit when the first non-successful search result is returned, unless -c is used.

-M[M]  Enable manage DSA IT control. -MM makes control critical.

-x     Use simple authentication instead of SASL.
```

Affichage de la commande man ldapsearch

Une fois renseigné sur la commande, nous envoyons une requête ldapsearch comme suit :

```
$ldapsearch -x -b "dc=m03,dc=i207"
```

```
root@localhost:~# ldapsearch -x -b "dc=m03,dc=i207"
# extended LDIF
#
# LDAPv3
# base <dc=m03,dc=i207> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# m03.i207
dn: dc=m03,dc=i207
objectClass: top
objectClass: dcObject
objectClass: organization
o: m2pro
dc: m03

# admin, m03.i207
dn: cn=admin,dc=m03,dc=i207
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator

# search result
search: 2
result: 0 Success

# numResponses: 3
# numEntries: 2
```

Résultat de la commande ldapsearch

4. Le résultat de la commande ldapsearch est le suivant :
   -x : pour utiliser une authentification simple.
   -b : pour préciser la branche dans laquelle effectuer la recherche.

5. Nous allons maintenant créer une entrée dans l'annuaire. Cette entrée concernera la personne qui est par exemple, le responsable de l'organisation. Pour cela, nous créerons le fichier **base.ldif** sous l'arborescence **/usr/share/slapd/base.ldif**. Attention, toutes les entrées à rajouter à l'annuaire doivent passer par un fichier .ldif. Notre fichier sera donc structuré comme tel:

```
#Déclaration du responsable
dn: cn=nom, dc=m03, dc=i207
objectClass: top
objectClass: person
userPassword: secret
cn: nom
sn: person
```

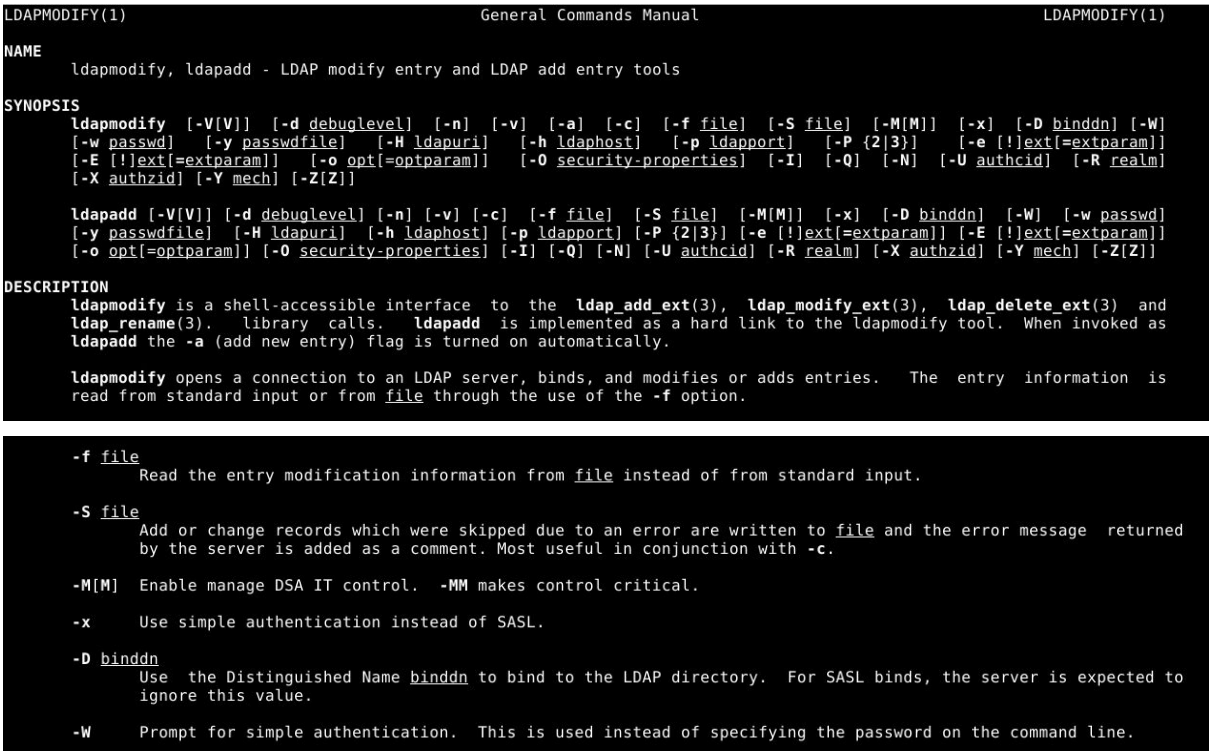
6. L'utilitaire pour l'ajout dans l'annuaire est **ldapadd** (**man ldapadd** pour plus de précisions). Pour ajouter les deux enregistrements nous entrons la commande :

```
$ldapadd -f base.ldif -x -D "cn=admin,dc=m03,dc=i207" -W
```

```
root@localhost:/usr/share/slapd# ldapadd -f base.ldif -x -D "cn=admin,dc=m03,dc=i207" -W
Enter LDAP Password:
adding new entry "cn=nom, dc=m03, dc=i207"
```

Résultat de la commande ldapadd

7. Détaillons les paramètres utilisés avec la commande vu en **question 6**, **ldapadd**:



```
LDAPMODIFY(1)                                General Commands Manual                                LDAPMODIFY(1)

NAME
       ldapmodify, ldapadd - LDAP modify entry and LDAP add entry tools

SYNOPSIS
       ldapmodify  [-V[V]]  [-d debuglevel]  [-n]  [-v]  [-a]  [-c]  [-f file]  [-S file]  [-M[M]]  [-x]  [-D binddn] [-W]
       [-w passwd]   [-y passwdfile]   [-H ldapuri]   [-h ldaphost]   [-p ldapport]   [-P {2|3}]   [-e [!]ext[=extparam]]
       [-E [!]ext[=extparam]]   [-o opt[=optparam]]   [-O security-properties]  [-I]  [-Q]  [-N]  [-U authcid]  [-R realm]
       [-X authzid] [-Y mech] [-Z[Z]]

       ldapadd [-V[V]] [-d debuglevel] [-n] [-v] [-c]  [-f file]  [-S file]  [-M[M]]  [-x]  [-D binddn]  [-W]  [-w passwd]
       [-y passwdfile]  [-H ldapuri]  [-h ldaphost] [-p ldapport] [-P {2|3}] [-e [!]ext[=extparam]] [-E [!]ext[=extparam]]
       [-o opt[=optparam]] [-O security-properties] [-I] [-Q] [-N] [-U authcid] [-R realm] [-X authzid] [-Y mech] [-Z[Z]]

DESCRIPTION
       ldapmodify is a shell-accessible interface  to  the  ldap_add_ext(3),  ldap_modify_ext(3),  ldap_delete_ext(3)  and
       ldap_rename(3).   library  calls.   ldapadd  is implemented as a hard link to the ldapmodify tool.  When invoked as
       ldapadd the -a (add new entry) flag is turned on automatically.

       ldapmodify opens a connection to an LDAP server, binds, and modifies or adds entries.   The  entry  information  is
       read from standard input or from file through the use of the -f option.
```

```
       -f file
              Read the entry modification information from file instead of from standard input.

       -S file
              Add or change records which were skipped due to an error are written to file and the error message  returned
              by the server is added as a comment. Most useful in conjunction with -c.

       -M[M]  Enable manage DSA IT control.  -MM makes control critical.

       -x     Use simple authentication instead of SASL.

       -D binddn
              Use  the Distinguished Name binddn to bind to the LDAP directory.  For SASL binds, the server is expected to
              ignore this value.

       -W     Prompt for simple authentication.  This is used instead of specifying the password on the command line.
```

Résultat de la commande ldapmodify

- **ldapadd** : Ajoute un objet dans la base de données LDAP.
- **-f** : Lis les entrées du fichier spécifié. C'est une autre manière de faire que de faire les entrées en une seule ligne de commande.
- **-x** : pour utiliser une authentification simple. (On ne passe pas par SASL)
- **-D** : pour indiquer le compte administrateur du LDAP et ainsi accéder à davantage d'attributs des entrées.
- **-W** : pour se voir demander le mot de passe du compte administrateur du LDAP.

8. Pour modifier un enregistrement on utilise **ldapmodify**. Comme pour ldapadd, nous éditerons un fichier nommé **modif.ldif** contenant :

```
dn: dc=m03,dc=i207
changtype: modify
add: telephoneNumber
telephoneNumber: 01 23 45 67 89
```

9. Ces lignes correspondent à :

- **dn : dc=m03,dc=i207** : La catégorie sélectionnée pour les éventuelles actions suivantes.
- **changtype: modify** : Spécifie l'action qui devra être faite sur le dn choisit. Ici, nous souhaitons modifier cette catégorie.
- **add: telephoneNumber** : Ajoute le nom champ ***telephoneNumber*** à la catégorie sélectionnée dans dn.

- **telephoneNumber: 01 23 45 67 89** : Spécifie les valeurs souhaitées pour les inclures dans le champ susmentionné.

Nous utilisons la commande **ldapmodify** pour mettre à jour cette entrée comme tel :

```
$ldapmodify -f modif.ldif -D "cn=admin ,dc=m03,dc=i207" -w secret
```

```
root@localhost:/usr/share/slapd# ldapmodify -f modif.ldif -D "cn=admin,dc=m03,dc=i207" -w secret
modifying entry "dc=m03,dc=i207"
```

Résultat de la commande ldapmodify

10. Nous utilisons à présent la commande **ldapsearch** pour rechercher l'ensemble des enregistrements rajoutés à la racine dc=m03,i207. Nous entrons alors la commande:

```
$ldapsearch -x -b 'dc=m03,dc=i207' '(objectclass=*)'
```

```
root@localhost:/usr/share/slapd# ldapsearch -x -b 'dc=m03,dc=i207' '(objectclass=*)'
# extended LDIF
#
# LDAPv3
# base <dc=m03,dc=i207> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# m03.i207
dn: dc=m03,dc=i207
objectClass: top
objectClass: dcObject
objectClass: organization
o: m2pro
dc: m03

# admin, m03.i207
dn: cn=admin,dc=m03,dc=i207
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator

# nom, m03.i207
dn: cn=nom,dc=m03,dc=i207
objectClass: top
objectClass: person
cn: nom
sn: responsable

# search result
search: 2
result: 0 Success

# numResponses: 4
# numEntries: 3
```

*Résultat de la commande ldapsearch pour **

11. Nous affinons la recherche pour ne récupérer que les **objects de type person.** Puis, nous trouvons le numéro de téléphone de **l'organisation m2pro**/.

```
root@localhost:/usr/share/slapd# ldapsearch -x -b 'dc=m03,dc=i207' '(objectClass=person)'
# extended LDIF
#
# LDAPv3
# base <dc=m03,dc=i207> with scope subtree
# filter: (objectClass=person)
# requesting: ALL
#

# nom, m03.i207
dn: cn=nom,dc=m03,dc=i207
objectClass: top
objectClass: person
cn: nom
sn: responsable

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
```

Résultat de la commande ldapsearch pour person

```
root@localhost:/usr/share/slapd# ldapsearch -x -b 'dc=m03,dc=i207' '(objectClass=organization)' 'telephoneNumber'
# extended LDIF
#
# LDAPv3
# base <dc=m03,dc=i207> with scope subtree
# filter: (objectClass=organization)
# requesting: telephoneNumber
#

# m03.i207
dn: dc=m03,dc=i207
telephoneNumber: 01 23 45 67 89

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
```

Résultat de la commande ldapsearch pour le telephoneNumber

IV-Authentification basée sur LDAP

A présent nous allons utiliser le serveur LDAP pour pour faire de l'authentification d'utilisateurs au lieu des fichiers **/etc/group** et **/etc/passwd**. Il faudrait passer passer par les deux étapes:

1. Ajouter les utilisateurs et les groupes dans l'annuaire:
2. Dire à la machine d'utiliser un serveur LDAP pour authentifier les utilisateurs.

IV.1-Ajout des utilisateurs et des groupes dans l'annuaire.

Pour faire la différence avec les utilisateurs installés sur la machine, on va créer un nouveau compte utilisateur qui n'est pas déclaré dans le fichier **/etc/passwd**.

On va commencer par déclarer les groupes et les utilisateurs comme une **organizationalUnit** de **m0X.i207**.

1. Editez un fichier que vous nommerez **o_unit.ldif**.

Afin de répondre à la question suivante, nous avons configuré le fichier **o_unit.ldif** de la manière suivante :

```
dn: ou=People,dc=m03,dc=i207
objectClass: organizationalUnit
ou: People
description: People

dn: ou=Group,dc=m03,dc=i207
objectClass: organizationalUnit
ou: Group
description: Groupes
```

2. Utilisez **ldapadd** pour ajouter ces deux enregistrements.

   Nous utilisons la commande ldapadd de cette façon:

```
$ldapadd -f o_unit.ldif -D "cn=admin,dc=m03,dc=i207" -w secret
```

```
root@localhost:/usr/share/slapd# ldapadd -f o_unit.ldif -D "cn=admin,dc=m03,dc=i207" -w secret
adding new entry "ou=People,dc=m03,dc=i207"

adding new entry "ou=Group,dc=m03,dc=i207"
```

Résultat de la commande ldapadd du fichier o_unit.ldif

3. Nous allons à présent créer un groupe pour les utilisateurs. Pour celà, nous éditons un fichier qui se nommera **group.ldif.** Ce fichier doit contenir les lignes suivantes:

```
dn: cn=utils,ou=Group,dc=m03,dc=i207
cn:utils
objectClass: posixGroup
objectClass: top
gidNumber: 9000
description: utilisateurs sans droits
```

4. Nous ajoutons ce fichier dans l'annuaire en utilisant la commande ldapadd comme tel:

```
$ldapadd -x -f group.ldif -D "cn=admin,dc=m03,dc=i207" -w secret
```

   Le résultat doit être un message d'ajout d'une nouvelle entrée.

5. Une fois le fichier group.ldif ajouté dans l'annuaire, nous céerons un fichier **utils.ldif** qui contiendra :

```
dn: cn=tot,ou=People,dc=m03,dc=i207
```

```
cn: toto
objectClass: account
objectClass: posixAccount
objectClass: shadowAccount
objectClass: top
uid: toto
uidNumber: 1025
gidNumber: 9000
homeDirectory: /home/toto
loginshell: /bin/sh
userpassord: Xr4ilOzQ4PCOq3aQ0qbuaQ== # Chiffré avec MD5
```

La commande pour avoir le chiffré du mot de passe de l'utilisateur toto avec la commande slappasswd est la suivante:

```
/usr/sbin/slappasswd -h '{MD5}' -s secret -v
```

La commande nous renverra un résultat du mot de passe en chiffré **{MD5}Xr4ilOzQ4PCOq3aQ0qbuaQ==**

Il ne reste plus qu'à mettre cette valeur dans le champ **userpassword** du fichier **utils.ldif**.

6. Pour ajouter le fichier **utils.ldif** à l'annuaire nous entrons la commande :

```
$ldapadd -x -f utils.ldif -D "cn=admin,dc=m03,dc=i207" -w secret
```

Le résultat doit être un message d'ajout d'une nouvelle entrée.

7. Les différents champs des fichiers group.ldif et utils.ldif sont :

group.ldif	utils.ldif
dn: cn=utils,ou=Group,dc=m03,dc=i207 : Correspond à l'état du DN (Distinguished Name) des entrées que le processus capture.	**dn : cn=toto,ou=People,dc=m03,dc=i207 :** Correspond à l'état du DN (Distinguished Name) des entrées que le processus capture.
cn: utils : Correspond à la déclaration de CN (Common Name) de l'entrée que le processus capture.	**cn:toto :** Correspond à la déclaration de CN (Common Name) de l'entrée que le processus capture.
objectClass: posixGroup : Spécifie le type du groupe.	**objectClass: account** : Spécifie que nous allons créer un compte utilisateur ci-après.
objectClass: top : Indique que utils est un object du plus haut level dans la classe.	**objectClass: posixAccount** : Le type du compte.
gidNumber: 9000 : Définition du Group ID.	**objectClass: shadowAccount** : Le sous-type du

	compte. Permet de définir des attributs additionnel.
description :Utilisateurs sans droits : Est une description succincte de l'utilisateur appartenant au groupe, ici il n'a aucun droits.	**objectClass: top :** Indique que utils est un object du plus haut level dans la classe.
	uid : toto : L'identifiant de l'utilisateur, ici toto.
	uidNumber: 1025 : Définit le User ID.
	gidNumber: 9000 : Définition du Group ID.
	homeDirectory : /home/toto : Le répertoire ou se trouve répertoire de l'utilisateur toto.
	loginshell: /bin/sh : Le terminal a utilisé quand l'utilisateur se connecte.
	userpassword: Xr4ilOzQ4PCOq3aQ0qbuaQ : Spécification du mot de passe du compte. Ici, le mot de passe est chiffré en MD5 (Il peut être mis en clair).

Les différents champs qui sont en relations avec l'authentification Unix sont :

- Pour le fichier utils.ldif:
  - uid
  - uidNumber
  - gidNumber
  - homeDirectory
  - loginShell
  - userpassword

- Pour le fichier group.ldif:
  - gidNumber

8. Il faut maintenant lancer une recherche pour afficher les informations concernant toto. nous lançons la recherche de cette façon:

```
$ldapsearch -x -b 'dc=m03,dc=i207' '(cn=toto)'
```

IV.2-Configuration du PC en client LDAP.

La dernière opération consiste à configurer le PC en client LDAP pour permettre l'authentification des utilisateurs. Pour cela, modifier le fichier **/etc/ldap/ldap.conf** (référence pour le client LDAP).

1. Dans ce fichier nous avons dû mettre les deux lignes suivantes :

```
BASE dc=m03,dc=i207
URI ldap://127.0.0.1/
```

2. Nous installons les packages libnss-ldap, lippam-ldap et nscd de la façon suivante :

```
$sudo apt-get install libnss-ldap libpam-ldap nscd
```

3. Répondre aux questions comme suit:

```
URI: ldap://127.0.0.1/
Distinguish name : dc=m03,dc=i207
Ldap version : 3
LDAP account for root : cn=admin,dc=m03,dc=i207
Root passwd: secret
Allow root local admin : yes
LDAP database requires login : no
LDAP account for root: cn=admin,dc=m03,dc=i207
Root passwd : secret
```

4. Par la suite, nous avons modifié le fichier **/etc/nsswitch.conf** comme suit :

```
passwd:         compat ldap
group:          compat ldap
shadow:         compat ldap
```

La machine peut s'authentifier sur le compte LDAP. L'authentification se fait d'abord en regardant les fichiers en local voir si ils existent, s'ils n'existent pas, on regarde si ils se trouvent dans le répertoire LDAP.

5. Ensuite, nous avons copié le fichier **/usr/share/doc/libpam_ldap/example/pam.d/ssh** à l'emplacement **/etc/pam.d/sshd** comme suivant :

```
$cp /usr/share/doc/libpam_ldap/example/pam.d/ssh /etc/pam.d/sshd
```

6. Ensuite, nous avons arrêté le service **nscd** avec la commande:

```
$/etc/init.d/nscd stop
```

Puis nous redemarrons le service LDAP avec la commande :

```
$/etc/init.d/slapd restart
```

7. L'utilisateur toto n'a pas de compte de système. Il n'existe que dans l'annuaire LDAP. Afin de voir si **toto est visible**, nous effectuons la commande :

```
$getent passwd
```

L'utilisateur toto n'est pas présent dans passwd mais c'est quand même un utilisateur du répertoire LDAP.

8. Avec les résultats précédents, il nous a été demandé de lui créer un répertoire. Nous avons procédé comme suit :

```
$mkdir /home/toto && chown toto /home/toto
```

La commande **mkdir /home/toto** va créer une répertoire dans le **dossier /home** puis la commande **chown toto/home/toto** va changer le propriétaire actuel du dossier par toto.

9. Afin de nous connecter avec le compte de toto, nous effectuons la commande suivante :

```
$su toto
```

Localement nous nous sommes connecté avec succès.
Maintenant, nous nous sommes essayé à une connexion SSH avec la compte toto comme suivant :

```
$ssh toto@127.0.0.1 -p 22
```

Nous nous sommes connecté avec succès.

V - Remise en état du matériel

- Penser à la remise en état du routeur **Cisco** et **Switch**:
    - Si la startup-configuration n'a pas été modifier, **éteindre le routeur**.
    - Sinon, se connecter dessus avec **minicom**, passer en mode **enable** et lancer la commande **reload**.
    - Pour le Switch idem en lançant **reload**.

- Penser à la remise en état du PC **Linux**:
    - Vérifiez que l'interface **eth0** est bien **up**.
    - Lancez les scripts **/script/init_machine.sh** et **/script/init_reseau.sh**.

- Penser à remettre le **câblage** en état:
    - Tous les câbles doivent être débranchés de leur interface, **sauf eth0** qui ne doit pas l'être.

VI - Conclusion

Le but de ce TP était de nous familiariser avec le LDAP (Lightweight Directory Access Protocol).

Nous avons vu qu'un service d'annuaire, LDAP, est une base de données spécialement conçue et optimisée pour la recherche rapide d'informations. De plus, il est capable de faire bien plus comme gérer de simples comptes jusqu'à un parc informatique entier en se basant sur des schémas bien précis.

Nous avons pu au travers de ce TP survoler les différents types de fichiers pouvant être créés pour définir nos données pour que le service LDAP les gèrent.

Ce n'était qu'une initiation mais nous avons pu voir qu'il est difficile de mettre en place ce genre de fichiers de par leur longueur (Ici, les fichiers étaient petits mais certains peuvent être immenses) mais après quoi, la gestion d'informations et les modifications sur l'annuaire deviennent faciles.