

ROYAUME DU MAROC

مكتب التكوين المهني وإنعاش الشغل

Office de la Formation Professionnelle et de la Promotion du Travail

Installation LDAP sous Gnu/Linux

www.ofppt.info



OFPPT

DIRECTION RECHERCHE ET INGENIERIE DE FORMATION
SECTEUR NTIC

Sommaire

1.1.	Introduction	2
1.2.	Présentation de LDAP	3
1.2.1.	Le protocole	3
1.2.2.	Le modèle de données	3
1.2.3.	Les méthodes d'accès	7
1.2.4.	Le langage de commande.....	9
1.3.	Concevoir un annuaire	9
1.3.1.	Déterminer les besoins, les données, le schéma.....	9
1.4.	Créer une base de données	10
1.5.	Installer, configurer et Administrer LDAP.....	10
1.5.1.	Installer les packages sur le serveur.....	10
1.5.2.	Les fichiers de configuration du serveur	11
2.	Authentification système LDAP sur un système GNU/Linux	12
2.1.1.	Configuration de l'environnement pour l'authentification système.	13
2.1.2.	Premiers tests de l'annuaire	13
2.1.3.	Vérification du fonctionnement de l'annuaire.	13
2.1.4.	Mise en place de l'authentification	14

Résumé

Un annuaire électronique est une solution permettant la création d'une collection d'objets. Dans les réseaux, les annuaires permettent à l'échelle d'une entreprise de déclarer tous les objets (utilisateurs, applications, équipements matériels...), et pour chaque objet de définir ses propriétés (attributs).

Cela permet d'avoir un recensement de tous les objets dans une base de données. Cette base étant, le plus souvent répartie. Novell, Microsoft utilisent des bases de données d'annuaires (respectivement les NDS Netware Directory Services et AD Active Directory) pour la manipulation des ressources sur leurs réseaux.

Les annuaires sont ensuite accessibles à partir de tous types d'applications (outlook, mozilla, konqueror...), mais aussi par les processus d'identification/authentification, les processus systèmes...

1.1. Introduction

LDAP (Light Directory Access Protocol) est un service d'annuaire dérivé de la norme X.500. La norme X.500 est très lourde, LDAP en est une version allégée ("light") dans un sens absolument pas péjoratif.

Vous trouverez de bien meilleures descriptions du principe, concept et du protocole LDAP en suivant les références indiquées à la fin de ce document.

Un serveur LDAP permet de centraliser des informations très diverses. Il offre de nombreux avantages :

- un serveur d'annuaire (recensement de tous les objets d'un système) : c'est la fonction la plus connue, on peut trouver des serveurs LDAP chez bigfoot, netscape (netcenter), infoseek et bien d'autres ;
- Information sur les utilisateurs (nom, prénom...), et données d'authentification pour les utilisateurs : cela permet aussi la définition de droits.
- Information pour les applications clientes et fonctions de serveur d'accès itinérant : cela permet de stocker ses informations personnelles sur un serveur et de les récupérer lors de la connexion;
- bien d'autres choses...

LDAP supporte le chiffrement SSL et cohabite parfaitement avec les applications Samba, DNS, NFS... ce qui permet son utilisation pour des applications comme les serveurs de liste de diffusion(sympa par exemple).

L'objet de cette séquence sera de voir comment installer, configurer puis administrer un serveur LDAP. Nous utiliserons la distribution OpenLDAP disponible sur les distributions Linux

www.ofppt.info	Document	Millésime	Page
	Installation LDAP sous Gnu/Linux	août 14	2 - 15

1.2. Présentation de LDAP

LDAP fournit un ensemble d'outils.

1. un protocole permettant d'accéder à l'information contenue dans l'annuaire,
2. un modèle d'information définissant l'organisation et le type des données contenues dans l'annuaire,
3. un modèle de nommage définissant comment l'information est organisée et référencée
4. un modèle fonctionnel qui définit comment accéder à l'information,
5. un modèle de sécurité qui définit comment accéder aux données et comment celles-ci sont protégées. OpenLDAP est souvent configuré avec SASL (Simple Authentication and Security Layer), qui permet les transactions cryptées avec les protocoles fonctionnant en mode connecté.
6. un modèle de duplication qui définit comment la base est répartie entre serveurs,
7. des APIs pour développer des applications clientes,
8. LDIF, (Ldap Data Interchange Format) un format d'échange de données.

1.2.1. Le protocole

Un protocole d'accès aux données, qui décrit comment ajouter, modifier, supprimer des données dans la base de donnée, quels protocoles de chiffrement (kerberos, ssl...), et quels mécanismes d'authentification sont utilisés. Ce protocole est utilisé dans la relation client/serveur, mais également entre serveurs (serveur/serveur) car une base de données LDAP peut être répartie.

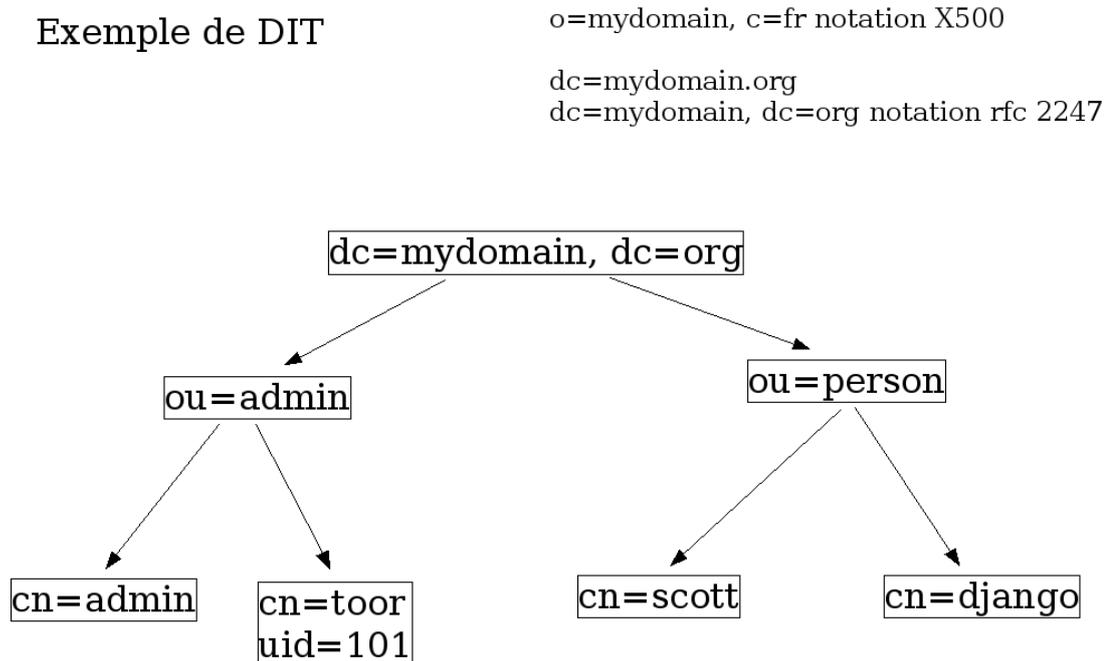
1.2.2. Le modèle de données

Le Directory Information Tree

LDAP fournit un modèle d'organisation des données. Ces données sont organisées sous forme hiérarchique. L'arbre est nommé Directory Information Tree (DIT). Le sommet (racine), contient le "suffixe". Chaque noeud représente une "entrée" ou "Directory Entry Service" (DSE). Les données sont stockées sur un format de base de données hiérarchique de type "dbm". Ce format est différent des bases de données relationnelles, conçues pour supporter de multiples mises à jour. DBM est conçu pour supporter peu de mises à jour, mais de nombreuses consultations.

www.ofppt.info	Document	Millésime	Page
	Installation LDAP sous Gnu/Linux	août 14	3 - 15

Figure 1. LDAP : le DIT Directory Information Tree



Classes d'objets, objets, attributs et schéma

Une entrée (DSE) dans le DIT correspond à un objet abstrait (organisation, ressource) ou concret (personne, équipement...). Les objets possèdent une description dans une "classe d'objet". Une classe d'objet donne une représentation modélisée des objets qu'elle représente en caractérisant tous les attributs des objets.

Certaines classes d'objet ont fait l'objet d'une normalisation et sont réutilisables. Elles sont définies par un nom, un OID (Object Identifier), la liste des attributs (facultatifs ou obligatoires), et, pour chaque attribut, un type. Le type est lié à la nature (essentiellement texte ou binaire) des attributs utilisés.

Une classe d'objet est définie par un nom, un OID (Object Identifier), la liste des attributs (facultatifs et obligatoires), un type. Le type est lié à la nature des attributs utilisés.

Chaque objet est composé d'attributs en fonction des types d'attributs décrits dans les classes d'objets. Un attribut est généralement un couple clé/valeur, mais peut être caractérisé par un nom, un OID, s'il est mono ou multi-évalué, un indicateur d'usage (facultatif/obligatoire), un format (voir par exemple pour les images).

Les OID sont normalisés par la RFC2256 et sont issus d'un schéma X500. Les OID sont tenus à jour par l'IANA Internet Assigned Numbers Authority. Un OID est une séquence de chiffres séparés par un "." point (Exemple 1.2.3.4) qui permet d'identifier de façon unique un élément du schéma LDAP.

Installation LDAP sous Gnu/Linux

Exemple de la la classe inetOrgPerson (dépend de organizationalPerson)

```
# The inetOrgPerson represents people who are associated with an
# organization in some way. It is a structural class and is derived
# from the organizationalPerson which is defined in X.521 [X521].
Objectclass ( 2.16.840.1.113730.3.2.2 <----- OID
  NAME 'inetOrgPerson'
  DESC 'RFC2798: Internet Organizational Person'
  SUP organizationalPerson
  STRUCTURAL
  MAY (
    audio $ businessCategory $ carLicense $ departmentNumber $
    displayName $ employeeNumber $ employeeType $ givenName $
    homePhone $ homePostalAddress $ initials $ jpegPhoto $
    labeledURI $ mail $ manager $ mobile $ o $ pager $
    photo $ roomNumber $ secretary $ uid $ userCertificate $
    x500uniqueIdentifier $ preferredLanguage $
    userSMIMECertificate $ userPKCS12 )
)

et l'attribut employeeType
# employeeType
# Used to identify the employer to employee relationship. Typical values
# used will be "Contractor", "Employee", "Intern", "Temp", "External", and
# "Unknown" but any value may be used.
Attributetype ( 2.16.840.1.113730.3.1.4
  NAME 'employeeType'
  DESC 'RFC2798: type of employment for a person'
  EQUALITY caseIgnoreMatch
  SUBSTR caseIgnoreSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )
Signification des mots réservés :

DESC : Description
SUP :      Objet parent
MUST : Attributs requis
MAY :   Attributs possibles
```

Chaque objet de l'annuaire qui correspond à une classe d'objet est décrit par des valeurs en fonction des attributs qui décrivent la classe d'objets. Un attribut est généralement un couple clé/valeur, mais peut être caractérisé par un nom, un OID, indique s'il est mono ou multi-évalué, donne un indicateur d'usage (facultatif/obligatoire), impose un format (par exemple base64 pour les images, utf-8 pour les données).

Les objets sont rattachés obligatoirement à au moins une classe d'objet. Une classe d'objet caractérise ou modélise les objets qui lui seront rattachés. On en déduit qu'un objet ne pourra pas avoir d'attribut non déclaré dans la classe d'objet. Par contre dans la classe d'objet, un attribut pourra être soit optionnel, soit obligatoire. L'administrateur a déjà des classes d'objets prédéfinies, il a la possibilité d'en définir d'autres.

Chaque objet hérite des attributs des objets dont il hérite. Quand on décrit un objet "fils", on doit décrire tous les liens de parenté avec l'attribut "ObjetClass". Les objets forment une hiérarchie, avec, au sommet, l'objet "top". Exemple pour enrichir l'objet "person" des attributs "technicalPerson".

objectClass: top

www.ofppt.info	Document	Millésime	Page
	Installation LDAP sous Gnu/Linux	août 14	5 - 15

Installation LDAP sous Gnu/Linux

```
objectClass: myOrganization
objectClass: person
objectClass: technicalPerson
```

L'ensemble de la description des classes d'objet et des types d'attributs définissent le "schéma".

Une entrée peut appartenir à plusieurs classes d'objets. Les attributs de l'objets sont la réunion des attributs de toutes les classes d'objets :

Entry Type	Required Attributes	Optional Attributes
person	commonName (cn) surName (sn) objectClass	mail mobile ...
OrganizationUnit	ou objectClass	description localisation ...
Organization	o objectClass	description ...

Les OID sont normalisés par la RFC2256 et sont issus d'un schéma X55. Les OID sont tenus à jour par l'IANA Internet Assigned Numbers Authority. Un OID est une séquence de chiffres séparés par un "." point. Exemple 1.2.3.4

Le "dn", ou Distinguished Name, est le chemin absolu de l'entrée dans le DIT à partir de la racine. Par exemple :

```
dc=org, dc=mydomaine, ou=person, uid=toor
```

On peut utiliser aussi un nommage "relatif" par rapport à une position courante. Dans ce cas on utilise le RDN (Relative Distinguished Name).

Le format d'échange de donnée LDIF

Le format d'échange permet l'import/export de données des bases, mais sert également pour l'ajout ou la modification. Les données sont en ASCII codées en UTF-8, sauf pour le binaire qui est codé en base64 (images par exemple).

Les fichiers au format LDIF respectent une structure de description des objets et des commandes :

```
Syntaxe générale :
dn: <distinguished name>
objectClass: <object class>
objectClass: <object class>
...
<attribute type>:<attribute value>
<attribute type>:<attribute value>
...
```

Exemple :

```
dn: cn= Manon Des Sources, ou= compta, dc=mydomain, dc=org
objectClass: person
objectClass: organization
```

www.ofppt.info	Document	Millésime	Page
	Installation LDAP sous Gnu/Linux	août 14	6 - 15

Installation LDAP sous Gnu/Linux

```
cn: AN GROSSI
sn: GROSSI
givenName: AM
userPassword: {sha}KDIE3AL9DK
uid: amg
```

Les fichiers supportent également des commandes pour ajouter, modifier ou supprimer une entrée.

```
dn: distinguished name
changetype <identifiant
change operation identifier
list of attributes...
...
-
change operation identifier
list of attributes
...
<identifiant :
    add (ajouter une entrée,
    delete (suppression),
    modrdn (modification du RDN),
    modify (modification : add, replace, delete d'un attribut)
```

On utilise le caractère "-" pour séparer 2 instructions. Par exemple :

```
dn: cn= Morina Fuentes, ou=admin, dc=mydomain, dc=org
changetype: modify
add: telephonenumber
telephonenumber: 05 55 55 55 55
-
add: manager
manager: cn= toor root, ou=admin, dc=mydomain, dc=org
```

1.2.3. Les méthodes d'accès

Les opérations de base sont résumées ici :

Opération	
Search	recherche dans l'annuaire d'objets
Compare	comparaison du contenu de deux objets
Add	ajout d'une entrée
Modify	modification du contenu d'une entrée
Delete	suppression d'un objet
Rename (Modify DN)	modification du DN d'une entrée
Bind	connexion au serveur
Unbind	deconnexion

Les requêtes de type "search" ou "compare" reçoivent des paramètres.

Paramètre	
base object	l'endroit de l'arbre où doit commencer la recherche
scope	la profondeur de la recherche
size limit	nombre de réponses limite
time limit	temps maxi alloué pour la recherche
attrOnly	renvoie ou pas la valeur des attributs en plus de leur type

www.ofppt.info	Document	Millésime	Page
	Installation LDAP sous Gnu/Linux	août 14	7 - 15

Installation LDAP sous Gnu/Linux

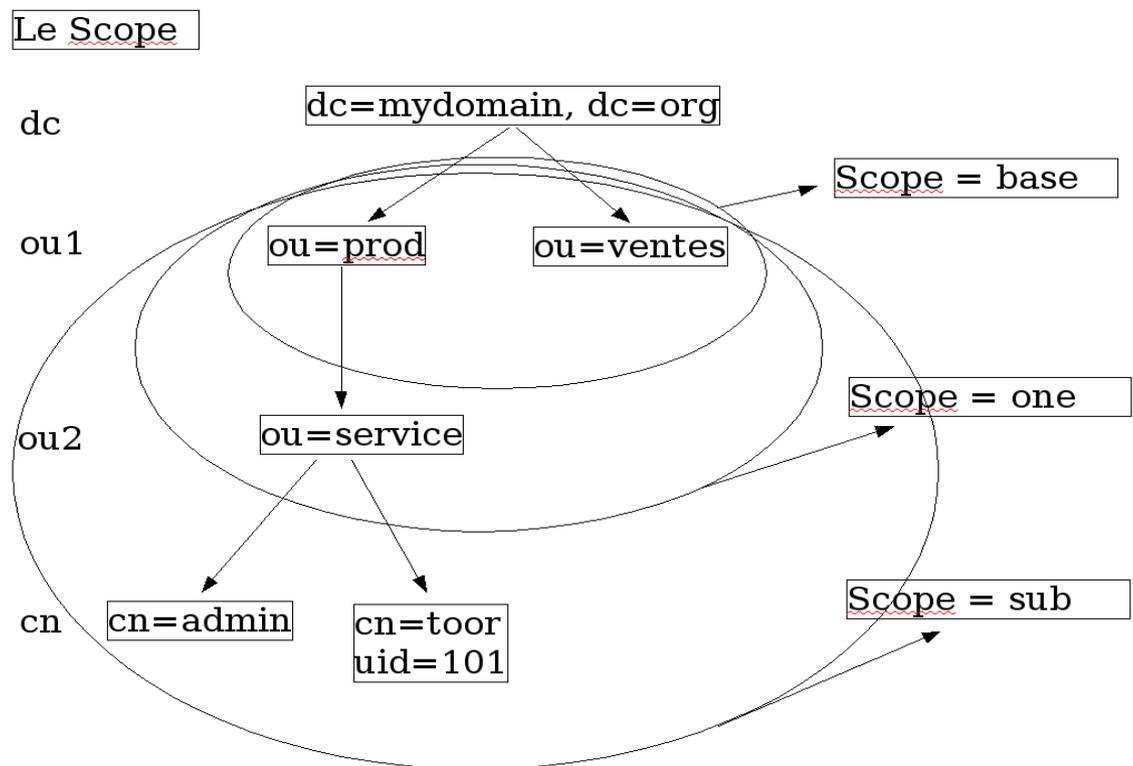
search filter le filtre de recherche
list of attributes la liste des attributs que l'on souhaite connaître

Le scope (Profondeur de recherche)

Le scope définit la profondeur de la recherche dans l'arbre des données. La figure montre la portée d'une recherche ou d'une comparaison en fonction du paramètre scope.

search scope=base recherche uniquement dans l'entrée définie
search scope=one recherche dans l'entrée définie et le premier sous-niveau
search scope = subtree, cherche dans toute la sous-arborescence.

Figure 1.2. LDAP : ls scope



search scope=base recherche uniquement dans l'entrée définie

search scope=onelevel search, cherche dans tous les noeuds fils rattachés directement au noeud courant

search scope = subtree, cherche dans toute la sous-arborescence.

Les URL LDAP offrent aux client web un accès aux bases de données :

```
ldap[s]://<hostname>:<port>/<base_dn>?\
<attributes>?<scope>?<filter>
```

<base_dn> : DN de l'entrée qui est le point de départ de la recherche

www.ofppt.info	Document	Millésime	Page
	Installation LDAP sous Gnu/Linux	août 14	8 - 15

Installation LDAP sous Gnu/Linux

```
<attributes>: les attributs que l'on veut consulter
<scope>      : la profondeur de recherche dans le
               DIT à partir du
<base_dn>    : "base" | "one" | "sub"
<filter>     : filtre de recherche,
               par défaut (objectClass=*)
```

Exemples :

```
ldap://ldap.netscape.com/ou=Sales,o=Netscape,c=US?cn,\
tel,mail?scope=sub?(objectclass=person)
ldap://ldap.point-libre.org/cn=Manon,ou=Contact,o=point-libre.org
```

1.2.4. Le langage de commande

1. - slapadd, slapcat, slapindex, slappasswd, fournis avec les serveurs LDAP (utilisables sous le compte root).
2. - ldapadd, ldapdelete, ldapmodify, ldapmodrdn, ldappasswd, ldapsearch, fournis avec les utilitaires ldap (utilisable par les utilisateurs et les applications). Ils sont fournis par le paquet (ldap-utils)

Exemple :

```
ldapsearch -x -h localhost -b "dc=mydomain,dc=fr" "objectclass=*"
```

Recherche de tous les objets sur l'annuaire de la machine locale, à partir de la racine. (-b indique à partir de quel niveau la recherche doit être exécutée). L'option « -x » indique de ne pas utiliser la méthode d'authentification SASL si elle n'est pas activée.

```
ldapdelete 'cn=Jean Colombani,cn=mydomain,cn=fr'
```

Suppression d'une entrée dans l'annuaire

```
ldapadd -f /tmp/unFichierAuFormatLDIF
```

Ajout dans l'annuaire à partir d'un fichier contenant des données au format LDIF.

Note: Pour éviter d'avoir à préciser à chaque fois certains paramètres (machine, port, annuaire...) il est possible de configurer le fichier de configuration « ldap.conf » qui sera utilisé par les applications clientes.

1.3. Concevoir un annuaire

1.3.1. Déterminer les besoins, les données, le schéma

La première opération est une phase d'analyse qui va permettre de déterminer l'organisation du système. Le résultat sera souvent représentable sous une forme arborescente. Cette étape permet de déterminer quel "schéma" sera nécessaire pour le contexte.

LDAP fournit par défaut une hiérarchie de classe déjà complète. Ces classes font l'objet d'une normalisation. Il sera nécessaire d'en prendre connaissance, puis, ensuite de procéder aux extensions

www.ofppt.info	Document	Millésime	Page
	Installation LDAP sous Gnu/Linux	août 14	9 - 15

nécessaires pour l'étude en cours.

1.4. Créer une base de données

Créer une base de données LDAP, va consister donc d'abord à créer

- une country (c)
- une ou plusieurs organisation (o) à 1 ou plusieurs niveaux
- définir les objets (feuilles de l'arbre)

Il est possible d'importer les informations à partir d'un fichier texte dans la base de données grâce à un format d'échange de données, le format LDIF (Lightweight Data Interchange Format).

1.5. Installer, configurer et Administrer LDAP

Vous allez avoir schématiquement 4 étapes :

1. Installer les packages nécessaires
2. configurer les fichiers de configuration
3. initialiser la base de données
4. configurer un client et tester le ou les services à partir d'un client
5. passer à l'administration

1.5.1. Installer les packages sur le serveur

Il va falloir installer les packages OpenLDAP. La procédure est standard à partir de paquets (debian ou rpm), sinon à partir des sources.

```
tar xzvf openldap-x.y.z.tgz
cd openldap.x.y.z
./configure
make
make depend
make test
make install
```

Installez également les packages perl, php et "dévelop" pour l'administration.

```
ii  slapd                2.1.30-2          OpenLDAP server (slapd)
ii  ldap-utils           2.1.30-2          OpenLDAP utilities
ii  libldap2             2.1.30-2          OpenLDAP libraries
ii  php4-ldap            4.3.8-1           LDAP module for php4
```

Il est intéressant de prévoir aussi les bibliothèques de développement.

1.5.2. Les fichiers de configuration du serveur

Il faut bien identifier les objets à référencer et les objectifs de l'annuaire. Les fichiers sont dans "/etc/openldap".

Le premier fichier est "sldapd.conf" qui décrit les principaux paramètres de votre annuaire :

```
# $OpenLDAP: pkg/ldap/servers/slapd/slapd.conf,v 1.8.8.6 2001/04/20 23:32:43
kurt Exp $
#
# See slapd.conf(5) for details on configuration options.
# This file should NOT be world readable.
#
# Inclusion des schémas nécessaires
include      /etc/openldap/schema/core.schema
include      /etc/openldap/schema/cosine.schema
include      /etc/openldap/schema/inetorgperson.schema
include      /etc/openldap/schema/nis.schema

# Options que vous pouvez modifier
#pidfile     //var/run/slapd.pid
#argsfile    //var/run/slapd.args

#####
# ldbm database definitions
#####
# Choix du format de base de données pour le stockage des informations.
database     ldbm

# Configurer le suffixe (racine) de l'annuaire
# en fonction du domaine DNS
suffix       "dc=my-domain,dc=com"
# ou d'une autre organisation
#suffix      "o=My Organization Name,c=US"

# L'administrateur de l'annuaire
rootdn       "cn=Manager,dc=my-domain,dc=com"

# Le mot de passe de l'administrateur, préférer une option cryptée
# La commande htpasswd peut très bien faire l'affaire pour encrypter

# rootpw          secret
# rootpw          {crypt}ijFYncSNctBYg

# Emplacement de la base de données
directory    /var/lib/ldap

# Création des index.
# Comme pour une base de données, indexer les rubriques
# les plus utilisées.

index        objectClass,uid,uidNumber,gidNumber,memberUid    eq
index        cn,mail,surname,givenname                        eq,subinitial

# La répllication ne sera pas utilisée ici
```

www.ofppt.info	Document	Millésime	Page
	Installation LDAP sous Gnu/Linux	août 14	11 - 15

Installation LDAP sous Gnu/Linux

```
# Vous pouvez répliquer tout ou partie d'un arbre
# activée par le daemon slurpd

# Directives de replication
# sinon les mettre dans un fichier à part et utiliser
# relogfile /chemincomplet/du/fichier

# Indiquer quels sont les serveurs répliqués
# et la méthode d'authentification
# Ici le serveur local, se répliquera sur ldap1

#replica host:ldap-1.example.com:389
#       bindmethod=simple
#       binddn="cn=replicat_slave1, dc=mydomain, dc=fr"
#       credential=UnMotDePasse

# Accès par défaut sur la base
defaultaccess read
```

Protéger ensuite le fichier avec un "chmod 600 /etc/openldap/slapd.conf".

Les autorisations d'accès nécessitent une remarque.

Ici l'accès par défaut est "read", mais il est possible d'affiner. Par exemple avec des règles d'écriture comme:

```
access to <what> [ by <who> <none | compare | search | read | write>]
# Donne un accès en écriture pour le manager du domaine
access to * by dn="cn=Manager,dc=mydomain,dc=fr" write
# Donne un accès en lecture à tout le monde sur la base
access to * by * read
# Donne un accès en écriture sur un attribut pour le manager
#           en lecture pour les autres.
access to attr=uid
           by dn="manager,dc=mydomain,dc=fr" write
           by * none
```

Le nombre d'options est très important, utilisez la commande "man slapd.conf".

2. Authentification système LDAP sur un système GNU/Linux

Faites une sauvegarde de vos fichiers de configuration.

```
root@uranus:/etc/ldap# cp ldap.conf ldap.conf.orig
root@uranus:/etc/ldap# cp slapd.conf slapd.conf.orig
root@uranus:/etc# cp nsswitch.conf nsswitch.conf.orig
root@uranus:/etc# cp libnss-ldap.conf libnss-ldap.conf.orig
```

Vérifier que votre serveur LDAP fonctionne.

Vérifier que votre serveur Annuaire est opérationnel.

www.ofppt.info	Document	Millésime	Page
	Installation LDAP sous Gnu/Linux	août 14	12 - 15

2.1.1. Configuration de l'environnement pour l'authentification système

Les fichiers `/etc/libnss-ldap.conf` et `/etc/pam_ldap.conf` sont normalement configurés. Sinon vous pouvez utiliser les commandes :

```
dpkg-reconfigure libnss-ldap
dpkg-reconfigure libpam-ldap
```

Prenez les options par défaut en prenant soin de tenir compte de la structure de votre annuaire. Pour nous :

```
dc=point-libre,dc=org
```

Vous devez également modifier le fichier `/etc/nsswitch.conf` afin que les applications utilisent aussi bien les fichiers standards (`passwd`, `shadow`) que l'annuaire ldap. :

```
passwd:      files ldap
group:       files ldap
shadow:      files ldap
```

2.1.2. Premiers tests de l'annuaire

La commande `getent passwd` doit vous permettre de récupérer à la fois les comptes du fichier `/etc/passwd`, mais également les compte de l'annuaire ldap qui n'existent pas dans la base `passwd`.

```
# getent passwd
[...]
mlx:2/yajBmqc3tYw:1005:1005:BOURG Jean:/home/mlx:/bin/bash
mly:2/yajBmqc3tYw:1006:1006:BOURG Marine:/home/mly:/bin/bash
```

Ces deux comptes proviennent bien de l'annuaire ldap.

2.1.3. Vérification du fonctionnement de l'annuaire.

L'utilisateur `mly` n'a pas de compte système. Il n'existe que dans l'annuaire ldap. Créez un répertoire et affectez-le au compte.

```
# mkdir /home/mly
# chown 1006:100 /home/mly
# ls -al /home/mly
drwxr-sr-x  2 mly      users          4096 2003-06-09 13:50 .
# Ici le serveur fonctionne car il substitue bien l'UID à l'uidNumber

# ls -al /home/mly
# Ici le serveur LDAP n'a pas été trouvé ou il ne fonctionne pas.
drwxr-sr-x  2 1006    users          4096 2003-06-09 13:50 .
```

www.ofppt.info	Document	Millésime	Page
	Installation LDAP sous Gnu/Linux	août 14	13 - 15

2.1.4. Mise en place de l'authentification

On va mettre en place maintenant l'authentification ldap. Il faut modifier les fichiers de configuration qui assurent l'authentification. Mettez en début de fichier :

```
#/etc/pam.d/login
auth    sufficient pam_ldap.so
account sufficient pam_ldap.so
password          required          pam_ldap.so

#/etc/pam.d/passwd
auth    sufficient pam_ldap.so
account sufficient pam_ldap.so
password          sufficient        pam_ldap.so
```

Vérification de l'authentification :

```
mlx@uranus:~$ su mly
Password: #ici taper toto
mly@uranus:~$ cd
mly@uranus:~$ pwd
/home/mly
```