

République Algérienne Démocratique et Populaire  
Université Abou Bakr Belkaid– Tlemcen  
Faculté des Sciences  
Département d'Informatique

Mémoire de fin d'études

Pour l'obtention du diplôme de Licence en Informatique

*Thème*

**Configuration et administration d'un annuaire  
LDAP avec un serveur de messagerie électronique  
en utilisant l'outil phpLDAPadmin**

**Réalisé par :**

- Latti Fatima
- Hammadi Nadjjet

*Présenté le 08 Juin 2014 devant la commission d'examination composée de MM.*

- *Benaissa Mohammed Samir* (Encadreur)
- *Brikci Amine* (Examineur)
- *Chaouche Lamia* (Examineur)

## *Remerciements*

En préambule à ce mémoire nous remerciant ALLAH qui nous aide et nous donne la patience et le courage durant ces longues années d'étude. Nous souhaitant adresser nos remerciements les plus sincères aux personnes qui nous ont apporté leur aide et qui ont contribué à l'élaboration de ce mémoire ainsi qu'à la réussite de cette formidable année universitaire. Ces remerciements vont tout d'abord au corps professoral et administratif de la Faculté science Dep informatique, pour la richesse et la qualité de leur enseignement et qui déploient de grands efforts pour assurer leurs étudiants une formation actualisée.

Nous tenant à remercier sincèrement Monsieur, Benissa mohammed Samir, qui, en tant que Directeurs de mémoire, est toujours montrés à l'écoute et très disponible tout au long de la réalisation de ce mémoire, ainsi pour l'inspiration, l'aide et le temps qu'il est bien voulu nous consacrer et sans qui ce mémoire n'aurait jamais vu le jour. On n'oublie pas nos parents pour leur contribution, leur soutien et leur patience.

Enfin, nous adressons nos plus sincères remerciements à tous nos proches et amis, qui nous ont toujours encouragée au cours de la réalisation de ce mémoire.

À tous ces intervenants, je présente mes remerciements, mon respect et ma gratitude



Merci

# DEDICACES

## Je dédie cette thèse à ...

Merci Allah (mon dieu) de m'avoir donné la capacité d'écrire et de réfléchir, la force d'y croire, la patience d'aller jusqu'au bout du rêve et le bonheur de lever mes mains vers le ciel et de dire " Ya Kayoum "

Je dédie ce modeste travail à celle qui m'a donné la vie, le symbole de

tendresse, qui s'est sacrifiée pour mon bonheur et ma réussite, à ma mère

Aicha...A mon père Mohammed, école de mon enfance, qui a été mon ombre

durant toutes les années des études, et qui a veillé tout au long de ma vie

à m'encourager, à me donner l'aide et à me protéger. Que dieu les garde et les

protège. A mes adorables sœurs Sara Asmaa Nadjat et la petite Nis Nada-Bissane.....

A mon frère Othmane.....A mes amies. A tous ceux qui me sont chères.

A tous ceux qui m'aiment. A tous ceux que j'aime.

*Latti Fatima*

Je dédie ce modeste travail à celle qui m'a donné la vie, le symbole de

tendresse, qui s'est sacrifiée pour mon bonheur et ma réussite, à ma mère

Farida...A mon père Ghaouti, école de mon enfance, qui a été mon ombre

durant toutes les années des études, et qui a veillé tout au long de ma vie

à m'encourager, à me donner l'aide et à me protéger. Que dieu les garde et les

protège. A adorable sœur Hanane ,

A mon frère Abdelatif.....A mes amies. A tous ceux qui me sont chères.

A tous ceux qui m'aiment. A tous ceux que j'aime.

*Hammadi Nadjat*

# Table de matière

<b>Introduction générale.....</b>	<b>1</b>
<b>Chapitre I : Généralités sur les annuaires</b>	
1.1.Introduction .....	2
1.2 .Définition d'un annuaire.....	3
1.3.Différences avec une base de données .....	4
1.4.L'annuaire LDAP .....	5
1.4.1.Les modèles LDAP.....	5
1.4.1.1.Le modèle d'information .....	6
1.4.1.2.Le modèle de nommage .....	8
1.4.1.3.Le modèle de fonctionnement .....	9
1.4.1.4. Le modèle de sécurité .....	9
1.4.1.5. Le modèle de duplication.....	9
1.4.2. Schéma.....	10
1.5.Organisation client/serveur .....	11
1.6.Quelques outils basés sur LDAP .....	11
1.7.Conclusion.....	12
<b>Chapitre II: configuration LDAP par phpLDAPadmin</b>	
2.1. Introduction.....	13
2.2.Open-LDAP.....	14
2.2.1. Composants d'OpenLDAP .....	14
2.2.2. Installation open-ldap .....	15
2.3. phpLDAPadmin.....	16
2.3.1. création d'un schéma de l'annuaire .....	18
2.3.2.création du carnet d'adresses.....	19
2.4.Conclusion.....	23

## **Chapitre III :relation entre service messagerie et annuaire**

### **LDA**

<b>3.1.Introduction</b> .....	<b>24</b>
<b>3.2. Logiciel de virtualisation : Virtualbox</b> .....	<b>25</b>
<b>3.2.1</b> Configuration réseau de virtualbox.....	<b>25</b>
<b>3.3. Messagerie électronique (serveur mail postfix)</b> .....	<b>26</b>
<b>3.3.1.</b> Description de l'architecture de fonctionnement d'un service de messagerie électronique .....	<b>26</b>
<b>3.3.2.</b> Configurer un serveur de mail avec postfix.....	<b>27</b>
<b>3.3.3.</b> Installation du serveur Postfix.....	<b>28</b>
<b>3.3.4.</b> Installation d'un client messagerie (MUA) mail useragent.....	<b>31</b>
<b>3.3.5.</b> Installation client messagerie Thunderbird sous linux (MUA).....	<b>32</b>
<b>3.4. Relation entre annuaire LDAP et serveur de messagerie électronique</b> .....	<b>35</b>
<b>3.4.1.</b> Configuration postfix-ldap.....	<b>36</b>
<b>3.4.2.</b> Configuration et schémas.....	<b>37</b>
<b>3.5.Conclusion</b> .....	<b>41</b>
<b>Conclusion générale</b> .....	<b>42</b>

# Liste des Figures

## Chapitre I :

<b>Figure 1.1</b> : une entrer d'un annuaire .....	<b>6</b>
<b>Figure 1.2</b> : attributs d'un annuaire .....	<b>7</b>
<b>Figure 1.3</b> : schéma d'un annuaire .....	<b>7</b>
<b>Figure 1.4</b> : système de nommage d'un annuaire .....	<b>8</b>
<b>Figure 1.5</b> : exemple de système de nommage .....	<b>8</b>
<b>Figure 1.6</b> : communication client/serveur .....	<b>11</b>

## Chapitre II :

<b>Figure 2.1</b> : interface phpLDAPadmin .....	<b>16</b>
<b>Figure 2.2</b> : connexion au serveur LDAP .....	<b>16</b>
<b>Figure 2.3</b> : serveur LDAP .....	<b>17</b>
<b>Figure 2.4</b> : les entrées d'un annuaire .....	<b>17</b>
<b>Figure 2.5</b> : option importer un schéma LDAP .....	<b>18</b>
<b>Figure 2.6</b> : création d'un schéma LDAP .....	<b>18</b>
<b>Figure 2.7</b> : création d'une sous entrée LDAP .....	<b>19</b>
<b>Figure 2.8</b> : les objets d'un annuaire .....	<b>20</b>
<b>Figure 2.9</b> : création d'une entrée .....	<b>20</b>
<b>Figure 2.10</b> : create object .....	<b>21</b>
<b>Figure 2.11</b> : exemple d'une entrée LDAP .....	<b>22</b>
<b>Figure 2.12</b> : arborescence annuaire LDAP .....	<b>22</b>

## Chapitre III :

<b>Figure 3.1</b> : Virtualbox .....	<b>25</b>
<b>Figure 3.2</b> : schéma courrier électronique .....	<b>27</b>
<b>Figure 3.3</b> : service mail Postfix .....	<b>27</b>
<b>Figure 3.4</b> : client messagerie mutt .....	<b>31</b>
<b>Figure 3.5</b> : client messagerie Thinderbird .....	<b>32</b>
<b>Figure 3.6</b> : adresse serveur mail Postfix .....	<b>33</b>
<b>Figure 3.7</b> : nom utilisateur .....	<b>34</b>
<b>Figure 3.8</b> : compte mail Thinderbird .....	<b>34</b>
<b>Figure 3.9</b> : relation service mail et annuaire LDAP .....	<b>35</b>
<b>Figure 3.10</b> : carnet d'adressage LDAP et Postfix ...	<b>40</b>

# INTRODUCTION GENERALE

Les particuliers et les entreprises ont de plus en plus recours aux réseaux pour accéder à des applications distribuées et à des ressources partagées (sites web, serveurs d'applications, serveurs de fichiers, etc.).

Ces applications et ces ressources doivent interagir avec des ordinateurs situés dans le même réseau local, à travers l'intranet de l'entreprise, ou plus généralement au travers de l'Internet. Cela nécessite a priori la connaissance des adresses de ces différentes machines. Or, dans la très grande majorité des cas, on n'utilise jamais les adresses réelles des machines ; on utilise des noms.

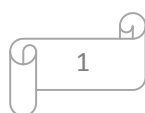
De nombreux outils d'annuaires ont donc vu le jour au fil des années, offrant des services divers et variés ; certains ont périclité, d'autres sont devenus immédiatement des standards incontournables, tel DNS (Domain Name System). Depuis quelques années maintenant, est apparu un nouveau standard, lui-même en passe de devenir absolument indispensable connu sous le sigle LDAP (Lightweight Directory Access Protocol). Ce standard ne remplacera pas DNS, ce n'est pas sa vocation, mais il permet d'unifier certains besoins tels que ceux d'annuaires de type pages blanches, d'annuaires de type NIS (Network Information Service ; « yellow pages »), d'authentification, etc.

L'étude de LDAP va être découpée de la manière décrite ci-après.

Le premier chapitre présentera les grandes généralités liées à un annuaire.

Dans Le deuxième, nous attaquerons le cœur du problème, autrement dit les concepts théoriques nécessaire à une bonne connaissance de ce type d'annuaire en basons sur les différentes étapes de configuration d'un serveur ldap par l'outil phpldapadmin.

Dans Le troisième chapitre, nous présentons les performances d'un serveur ldap pour définir les différents adresses mails qui seront utilisées par le service de messagerie électronique postfix,



# Chapitre I

## **Généralités sur les annuaires**



## 1.1. Introduction

En informatique, un **serveur** est un ordinateur, dont le rôle est de répondre de manière automatique à des demandes envoyées par des clients (ordinateur et logiciel), via un réseau (local ou externe).

Il nous semble importante de bien comprendre ce qu'est un annuaire et ce à quoi il sert, avant de décrire le standard LDAP lui-même.

En effet, le standard LDAP et un annuaire sont deux choses différentes : le premier définit l'interface d'accès à un annuaire et le deuxième est une sorte de base de données permettant de retrouver facilement des personnes ou des ressources comme imprimante, des ordinateurs et des applications.

L'accès aux annuaires nécessite de définir un standard en raison de certains besoin caractéristiques de ces derniers. Les annuaires ne sont pas que des bases de données, ils doivent également offrir des services particuliers comme la sécurité d'accès aux données, la recherche, le classement ou l'organisation des formations.

Nous aboutirons ainsi à l'identification des caractéristiques d'un annuaire et à la nécessité d'établir un standard, décrivant l'interface d'accès à celui-ci.

C'est ce rôle que joue LDAP. Par ailleurs, comme nous l'avons souligné dans l'introduction, les annuaires ne sont qu'une brique de la gestion des identités.

## 1.2. Définition d'un annuaire

Un annuaire électronique peut être vu comme une base de données spécialisée, dont la fonction première est de retourner un ou plusieurs attributs d'un objet grâce à des fonctions de recherche multicritères. Les objets peuvent être de nature très diverse. Par exemple, un objet de l'annuaire peut représenter une personne et les attributs de cet objet seront alors son nom, son prénom, son numéro de téléphone, etc. par exemple, un objet représentera une imprimante et les attributs de l'objet seront alors les différents noms de cette imprimante, son adresse réseau, sa situation géographique, etc.

Un annuaire électronique va centraliser des informations et les rendre disponibles, via le réseau, à des applications, des systèmes d'exploitation ou des utilisateurs. Il va généralement s'appuyer sur les éléments suivants :

- Un protocole : échange des données proprement dit et indication des opérations à effectuer sur ces dernières.
- Un modèle fonctionnel : description de la nature des opérations que l'on peut effectuer, comme par exemple une recherche, ou une modification.
- Un modèle de nommage : identification des données ; organisation des différentes entrées de l'annuaire.
- Un modèle d'information : nature des données pouvant être enregistrées (des chaînes de caractères, des nombres, des numéros de téléphone...).
- Un modèle de sécurité : description des services de sécurité permettant d'assurer par exemple le chiffrement des données transférées ou bien l'authentification du client vis-à-vis du serveur.
- Un modèle de distribution : création et gestion de serveurs secondaires dans un but de sauvegarde ou de répartition de charge, création et gestion de liens spéciaux pointant vers des annuaires responsables d'une partie des données de l'entreprise ou vers des annuaires complètement différents.[1]

### 1.3. Différences avec une base de données

Bien qu'un annuaire soit comparable à une base de données pour un grand nombre de fonctionnalités, il en diffère en de nombreux points.

1. Un annuaire est très performant en consultation (c'est-à-dire en lecture ou en recherche ; la lecture n'étant qu'une recherche particulière). Par contre, un annuaire n'est pas très adapté pour des mises à jour fréquentes (autrement dit en écriture). Les données contenues dans un annuaire sont en effet beaucoup plus pérennes, et il est donc totalement inutile d'optimiser les fonctions de mise à jour.

Un annuaire doit, à l'opposé, supporter un nombre important de consultations simultanées. L'exemple le plus évident est l'annuaire électronique téléphonique. L'optimisation de la fonction « lecture » est donc à privilégier dans ce contexte.

2. Une base de données doit, par contre, généralement supporter des applications qui la remettent constamment à jour. Cela signifie que la fonctionnalité « écriture » dans une base de données est importante et doit par conséquent être optimisée. Parmi les exemples les plus classiques de bases de données, on trouve :
  - un système de réservation de billets d'avion ;
  - un système de gestion des stocks d'une grande surface de distribution ;
  - un gestionnaire de comptes bancaires.
3. Dans le cas d'un annuaire, par contre, l'accès en écriture est généralement réservé aux administrateurs de l'annuaire ou bien aux propriétaires des informations. Il n'est donc pas nécessaire que la fonction « écriture » soit optimisée ; ce type d'opération sera beaucoup plus épisodique que la lecture.

Ceci étant posé, il est évident que pour des raisons de facilité de mise en œuvre, les différents produits existant sur le marché vont le plus souvent faire appel à des outils de base de données pour matérialiser la base de l'annuaire proprement dit, plutôt que de mettre en œuvre un outil spécifique pour gérer cette dernière.

## 1.4. L'annuaire LDAP

**Lightweight Directory Access Protocol (LDAP)** est à l'origine un protocole permettant l'interrogation et la modification des services d'annuaire. Ce protocole repose sur TCP/IP. Il a cependant évolué pour représenter une norme pour les systèmes d'annuaires, incluant un modèle de données, un modèle de nommage, un modèle fonctionnel basé sur le protocole LDAP, un modèle de sécurité et un modèle de réplication. Un annuaire LDAP respecte généralement le modèle X.500. C'est une structure arborescente dont chacun des nœuds est constitué d'attributs associés à leurs valeurs.

Le nommage des éléments constituant l'arbre (racine, branches, feuilles) reflète souvent le modèle politique, géographique ou d'organisation de la structure représentée. La tendance actuelle est d'utiliser le nommage DNS pour les éléments de base de l'annuaire (racine et premières branches, *domain components* ou **dc=...**). Les branches plus profondes de l'annuaire peuvent représenter des unités d'organisation ou des groupes (*organizationalunits* ou **ou=...**), des personnes (*commonname* ou **cn=...** voire *user identifieruid=...*), ... L'assemblage de tous les composants (du plus précis au plus général) d'un nom forme son *distinguishedname*

### 1.4.1. Les modèles LDAP

Le protocole LDAP met en jeu 5 modèles qui définissent son fonctionnement à différents niveaux. Ces 5 modèles sont :

- un modèle d'information: pour définir le type de données de l'annuaire
- un modèle de nommage: pour indiquer comment les données sont organisées
- un modèle fonctionnel: pour indiquer comment accéder aux données
- un modèle de sécurité: pour indiquer comment protéger l'accès aux données
- un modèle de duplication: pour indiquer comment répartir les données entre serveur.

Dans la suite, nous présenterons l'ensemble de ces modèles.

#### 1.4.1.1. Le modèle d'information

LDAP permet de gérer des données. Ces données utilisent un modèle particulier pour être stockées. Dans ce modèle, l'élément de base est appelé "Entry".

Une entrée (entry) est un élément de base de l'annuaire. C'est lui qui contient les données. C'est l'équivalent en programmation orientée objet d'une "classe d'objet". Une entrée regroupe un ensemble d'attribut contenant les différentes informations relatives à l'entrée.

Client	
Type d'attribut	Valeur d'attribut
cn:	Ziggy NIGHT
uid	Znight
telnumber	0388123456
mail	Ziggy.night@gmail.co
solde	1000000

**Figure 1.1** : une entréer d'un annuaire

Sur l'exemple ci-dessus, on a une entrée de type "Client" qui contient plusieurs arguments avec les différentes informations sur le client.

Un attribut est caractérisé par:

- un nom
- un type
- une méthode de comparaison
- un « Object Identifier » (IOD)
- une valeur

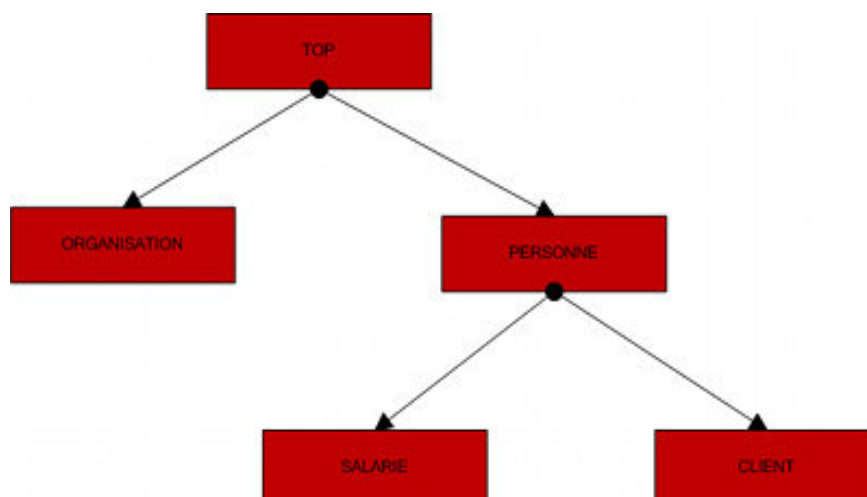
Par exemple, une entréer de type "Fournisseur" peut avoir le meme attribut "cn" (commonname) qu'une entrée de type "Client".

Voici une liste des attributs classiques que l'on retrouve sur les entrées d'un service LDAP:

attribu	description
cn	« common name » ou nom commun
o	« organization name » ou nom de l'organisation
gn	« given name » ou le surnom
l	« locality name » ou nom de la localité
st	« state name » ou nom de l'état
ou	« organisational unit » ou unité d'organisation
dc	« domain component » ou nom de domaine

**Figure 1.2** : attributs d'un annuaire

D'une manière générale, tous les types d'entrées (Client, Fournisseur, ...) et leurs attributs (cn, ou, ...) sont définis dans un schéma. Le schéma définit l'ensemble des types d'entrées par le service LDAP. Chaque entrée de l'annuaire fait obligatoirement référence à une classe d'objet du schéma. Les types d'entrées sont organisés de manière hiérarchique. Le sommet de cette organisation hiérarchique est toujours occupé par le type "Top". Et cette organisation met en place un système d'héritage où chaque type hérite des attributs de son type parent.



**Figure 1.3** : schéma d'un annuaire

1.4.1.2. Le modèle de nommage

Une fois le modèle d'information définit, il faut pouvoir définir la manière dont sont référencées les différentes informations gérées par les services LDAP. C'est le rôle du modèle de nommage. Il définit comment sont organisées les entrées de l'annuaire et comment elles sont référencées.

Cette organisation est représentée par le Directory Information Tree (DIT). C'est une classification comparable au système de fichier UNIX.

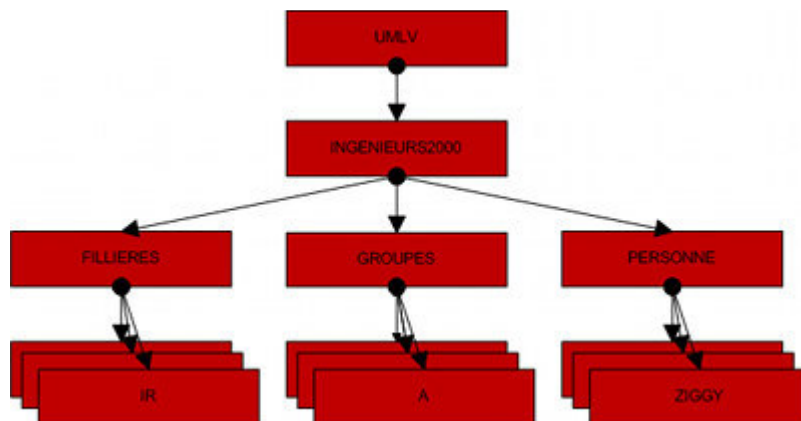


Figure 1.4 système de nommage d'un annuaire

Chaque noeud du DIT correspond à une entrée de l'annuaire. Au sommet se trouve l'entrée "Suffix" ou "Root Entry". Cette dernière correspond à l'espace de nommage

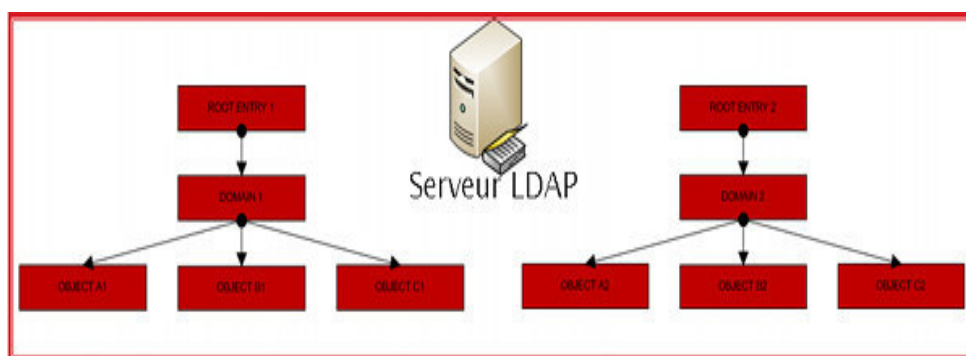


Figure 1.5 : exemple de système de nommage

Il est important de s'assurer que 2 entrées d'un même DIT n'aient pas le même DN. Pour cela, il faut s'assurer que la sélection des attributs composant le DN donne un résultat unique.

**1.4.1.3. Le modèle de fonctionnement**

Une fois les données stockées et référencées, il faut permettre d'utiliser ces données. Pour cela, LDAP définit un modèle de fonctionnement. Ainsi, ce modèle définit les opérations possibles sur les données. On recense 4 types d'opérations:

- opérations d'interrogation: requête pour accéder aux données
- opérations de comparaison: renvoie vrai ou faux si égal
- opérations de mise à jour: add, delete, rename, modify
- opérations d'authentification et de contrôle: bind, unbind, abandon

**1.4.1.4. Le modèle de sécurité**

Le modèle de sécurité permet de protéger l'accès aux données de l'annuaire. La sécurité se fait à plusieurs niveaux. Au niveau de l'authentification pour se connecter au service, par des règles d'accès aux données et par le chiffrement des communications.

Pour l'authentification, LDAPv3 propose plusieurs choix:

- Anonymes authentication: accès sans authentification
- Root DN authentication: accès administrateur
- Mot de passe + SSL ou TLS: accès chiffré
- Certificats sur SSL: échange clé publique/privée

Pour le contrôle d'accès, c'est un fonctionnement similaire à la gestion des droits des systèmes UNIX. Un utilisateur peut avoir des droits d'accès en lecture, écriture, recherche, comparaison). Et pour le chiffrement des communications, il est possible d'utiliser des algorithmes de cryptage.

**1.4.1.5. Le modèle de duplication**

Le protocole LDAP offre des facilités pour dupliquer ou synchroniser les données entre plusieurs serveurs LDAP. Pour réaliser cela, il définit un modèle de duplication. Ce dernier définit comment échanger les informations d'un serveur à l'autre.



L'intérêt de dupliquer un serveur est par exemple de pallier une panne de l'un des serveurs, ou d'une coupure réseaux. Mais aussi pour répartir la charge du service et garantir une qualité de service.

### 1.4.2. Schéma

Un serveur LDAP va gérer plusieurs entrées, chacune comportant une ou plusieurs classes d'objet, comprenant plusieurs attributs, eux-mêmes soumis à des règles syntaxiques, des règles de comparaisons, etc.

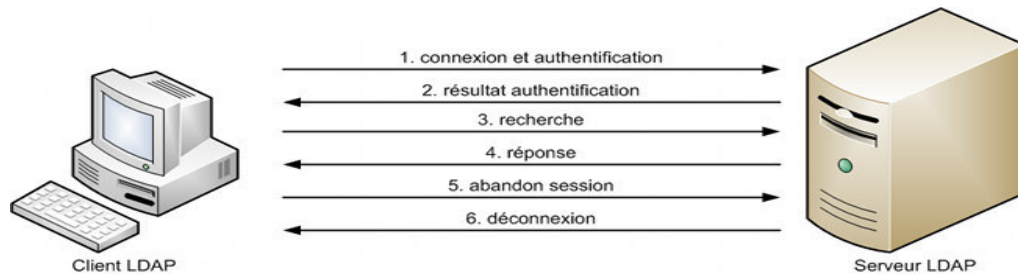
L'ensemble des définitions relatives à tous ces objets que sait gérer un serveur LDAP s'appelle le schéma. Le schéma décrit par conséquent les classes d'objets, les types d'attributs et leur syntaxe, ainsi que les règles de comparaison d'attributs connus du serveur.

Le protocole LDAP version 3 exige que le schéma soit publié par un serveur. Celui-ci est enregistré dans des attributs opérationnels.

La publication du schéma est fondamentale. En effet, si n'importe quelle application cliente est capable de reconnaître l'attribut « cn » ou « gn », ou bien la classe « inetOrgPerson », autrement dit les attributs et les classes de bases, il n'en est pas de même pour les attributs et classes définis spécifiquement pour un serveur particulier. La publication du schéma va permettre à ces applications clientes, dans une certaine mesure, de connaître ces nouveaux attributs et ces nouvelles classes. La publication garantit ainsi un plus grand niveau d'interopérabilité.

### 1.5. Organisation client/serveur

Une communication de type client/serveur pour permettre au client d'accéder aux informations contenues sur le serveur.



**Figure 1.6** : communication client/serveur

Les échanges avec le protocole LDAP se font au format ASCII comme pour HTTP ou SMTP. En plus des opérations présentées sur l'exemple de communication client/serveur ci-dessus, les opérations de base définies par le protocole LDAP sont :

- interrogation: search, compare
- mise à jour: add, delete, modify
- connexion: bind, unbind, abandon

Etant donné que ces échanges sont réalisés au format ASCII, des mécanismes d'authentification et de chiffrement sont mis en place pour sécuriser le service.

### 1.6. Quelques outils basés sur LDAP

Bien que les exemples donnés tout au long de ce chapitre font référence à l'outil proposé par le projet OpenLDAP, ce n'est pas le seul existant sur le marché. Il existe en effet de nombreux autres outils dont le cœur est construit autour de LDAP. En voici une liste non exhaustive :

- Active Directory ; nom du service d'annuaire de Microsoft®. Particularité : le moins « compatible » des serveurs LDAP.
- Sun Java System Directory Server Enterprise Edition ; comme son nom l'indique, est le serveur d'annuaire de Sun Microsystems®.
- Fedora Directory Server (libre) ; serveur LDAP de RedHat issu du serveur de Netscape®.

- Oracle Internet Directory ; serveur d'annuaire proposé par la société Oracle®.

Si l'outil proposé par OpenLDAP est un des plus répandus parmi les outils libres, son inconvénient majeur en comparaison de ses concurrents est d'être assez limité dans ses possibilités d'interface avec l'utilisateur, en particulier si l'utilisateur doit jouer le rôle de l'administrateur de l'annuaire. Par contre, l'outil a un avantage indéniable par rapport à ses concurrents : son prix. L'outil est non seulement libre, mais il est également gratuit. Côté client, de nombreux outils intègrent le protocole LDAP. Ce sont souvent des outils de messagerie électroniques comme par exemple « Outlook Express » ou bien « Netscape Messenger » ou encore « Thunderbird ». Il existe également des outils orientés PHP permettant d'accéder à un serveur LDAP, comme par exemple PhPLDAPAdmin. Tous ces logiciels sont bien entendu accessibles via Internet.

## 1.7. Conclusion

Il est de plus en plus courant de trouver dans la littérature, comme dans des pages web, de nombreuses références à LDAP. Et il semble bien évident que ce phénomène s'accroisse de plus en plus. En effet, il est de plus en plus difficile d'imaginer un monde sans annuaires partagés et en particulier sans annuaires basés sur LDAP. Ce protocole semble s'être imposé naturellement comme le standard du domaine. Les usages de LDAP couvrent de nombreux aspects de la vie de l'entreprise, et ce, quelle que soit sa taille. LDAP est en effet utilisé pour la diffusion d'annuaires de type « pages blanches », commence à remplacer de plus en plus souvent les serveurs NIS, permet de jouer le rôle de serveur de distribution de certificats, permet l'authentification des utilisateurs, etc.

Ce chapitre présente en particulier les concepts de base d'un annuaire LDAP : qu'est-ce qu'une entrée, un attribut ? Comment sont identifiées les données au sein de l'annuaire ? qu'est-ce que le schéma ? Etc. Il décrit ensuite la manière d'accéder à un serveur LDAP. Il expose enfin la façon dont sont échangées les données entre un client et un serveur d'annuaire.[5]

Comme cela a été dit plus haut, les annuaires LDAP jouent souvent un rôle non négligeable dans la sécurité d'une entreprise (publication de certificats, authentification des utilisateurs). Dans le chapitre suivant, nous détaillons la configuration et l'administration ldap par phpldapadmin.

# Chapitre II

## **Configuration LDAP par phpldapadmin**

## 2.1. Introduction

Après avoir étudié les nombreux concepts liés aux annuaires LDAP, passons à la pratique et nous étudions l'implémentation libre la plus utilisée OpenLDAP.

OpenLDAP est un projet libre diffusé sous licence "OpenLDAP Public. Nous verrons une utilisation avancée d'OpenLDAP, avec l'écriture de schéma et la mise en haute disponibilité via la réplication. Ensuite, un des contextes dans lequel l'utilisation d'un annuaire est intéressante est la centralisation des comptes utilisateurs Unix/Linux.

Par suite il n'est pas toujours simple d'administrer une base OpenLDAP, surtout quand on ne connaît pas par cœur tous les champs (en même temps, il y en a tellement). Voici donc une interface assez simple d'utilisation phpLDAPAdmin qu' est une interface écrite en PHP qui permet de modifier facilement et via une interface conviviale un annuaire LDAP (OpenLDAP principalement), sur le même principe que phpMyAdmin pour les bases de données MySQL. Il permet de gérer plusieurs annuaires LDAP et implémente plusieurs modes d'authentification. Il est présent sous forme de paquets dans la plupart des distributions récentes. [2]

Pour cela phpLDAPAdmin est un Mise en place d'une solution de management graphique pour OpenLDAP.

## 2.2. Open-LDAP



Pour réaliser le déploiement d'un service LDAP, nous allons utiliser OpenLDAP.

OpenLDAP est un serveur LDAP open-source permettant de mettre en place un service LDAP. Dans les parties suivantes, nous décrirons les principales tâches à réaliser pour déployer un service LDAP.

OpenLDAP est un annuaire informatique qui fonctionne sur le modèle client/serveur. Il contient des informations de n'importe quelle nature qui sont rangées de manière hiérarchique. Pour bien comprendre le concept, il est souvent comparé aux Pages Jaunes (Yellowpages), où le lecteur recherche un numéro de téléphone particulier: il va d'abord sélectionner la profession, puis la ville, puis le nom de l'entrée pour trouver au final le numéro de téléphone. En pratique, il est utilisé pour enregistrer une grande quantité d'utilisateurs ou de services (parfois des centaines de milliers) dans un réseau informatique. Il permet d'organiser hiérarchiquement les utilisateurs par département, par lieu géographique ou par n'importe quel autre critère. C'est une alternative libre à Microsoft Active Directory.[8]

### 2.2.1. Composants d'OpenLDAP

OpenLDAP est constitué de 3 éléments principaux :

- **slapd** (Stand-alone LDAP Daemon): démon LDAP autonome. Il écoute les connexions LDAP sur n'importe quel port(389 par défaut) et répond aux opérations LDAP qu'il reçoit via ces connexions. Typiquement, slapd est appelé au moment du boot.
- des **bibliothèques** implémentant le protocole LDAP.
- des **utilitaires**, des outils et des exemples de clients.

### 2.2.2. Installation open-ldap

Tout d'abord, installer le daemon serveur **slapd** de OpenLDAP et le paquet **ldap-utils**, un paquet contenant des utilitaires de gestion de LDAP:

```
sudo apt-get install slapd ldap-utils
```

Par défaut **slapd** est configuré avec des options minimales nécessaires pour exécuter le démon **slapd**.

#### La syntaxe LDIF

Le format LDIF a été développé par l'Université du Michigan, dans ses implémentations d'annuaire LDAP. La première utilisation a été celle de fichiers descriptifs, puis le format a évolué pour pouvoir décrire des modifications apportées à un annuaire.

LDIF est un format de fichier. Les fichiers de type LDIF sont utilisés d'une part pour décrire des objets d'un annuaire LDAP, et d'autre part pour décrire un ensemble d'opérations à effectuer sur le contenu d'un annuaire. L'utilisation descriptive permet, par exemple, de créer les premières entrées d'un annuaire, ou bien d'avoir une sauvegarde d'un annuaire sous la forme d'un fichier.[9]

La syntaxe d'une entrée dans un fichier LDIF est la suivante :

```
dn: <distinguished name>
<attrdesc>: <attrvalue>
<attrdesc>: <attrvalue>
<attrdesc>:: <base64-encoded-value>
<attrdesc>:<<URL>
```

### 2.3. phpLDAPAdmin

Pour vous connecter à phpLDAPAdmin, accédez à <http://localhost/phpLDAPAdmin>



Figure 2.1 interface phpldapadmin



Figure 2.2 : connexion au serveur ldap

- **Login DN:** - *cn=admin, dc=example, dc=com*
- **Password:** - le mot de passe pour la connexion a l'annuaire phpLDAPAdmin



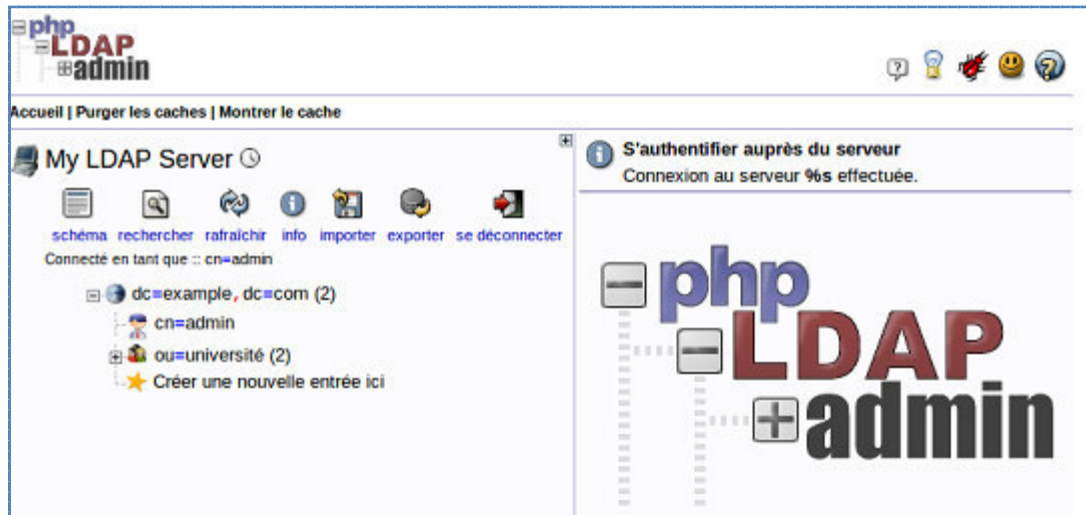


Figure 2.3 : serveur LDAP

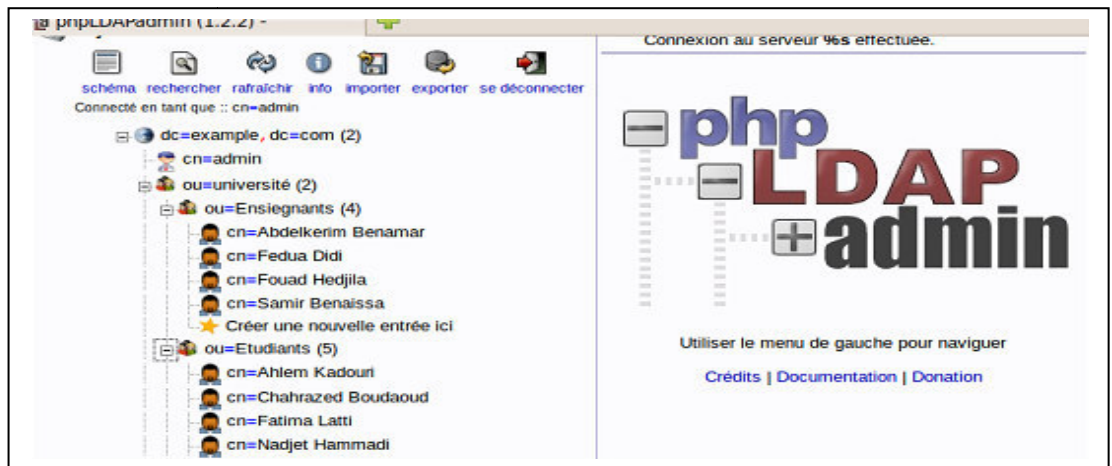


Figure 2.4 : les entrées d'un annuaire

### 2.3.1. Création d'un schéma de l'annuaire

Une fois que vous êtes connecté à phpLDAPAdmin, vous pouvez installer un schéma d'annuaire. Il s'agit juste d'un schéma très simple qui met en place un carnet d'adresses partagé, et ne représente qu'une fraction de ce qui peut être fait avec OpenLDAP. [7]

Dans la section Mon serveur LDAP de l'écran principal de phpLDAPAdmin, Cliquez sur le lien pour l'importation, Ceci nous amène à l'écran d'importation.



Figure 2.5 :option importer un schéma LDAP

Copiez et collez le texte suivant dans la ou collez votre LDIF ici partie de l'écran.

```
dn: ou=people, dc=example, dc=com
```

```
objectClass: top
```

```
objectClass: organizationalUnit
```

```
ou: people
```

Cliquez sur Continuer pour créer le schéma de carnet d'adresses.

Vous devriez voir le message sur l'écran:

**Adding ou=people,dc=example,dc=com Success**

The screenshot shows the 'Importer' screen with the following content:

Sélectionner un fichier LDIF :

Taille maximale du fichier : 2M

ou collez votre LDIF ici

```
# Create top-level object in domain
dn: dc=example,dc=com
objectClass: top
objectClass: dcObject
objectClass: organization
o: Example Organization
dc: Example
description: LDAP Example

# Admin user.
```

Figure 2.6 : création d'un schéma ldap

### 2.3.2. Création du carnet d'adresses

Sur le volet de navigation à gauche de l'écran phpLDAPAdmin, cliquez sur le signe [+] à côté de la dc = example, dc = entrée de com pour le développer. Cela montre université entrée et l'entrée des personnes nouvellement ajouté.

Cliquez sur l'entrée de ou =Enseignants. Vous pouvez obtenir quelques erreurs la première fois que vous sélectionnez cette entrée, similaire à supprimé automatiquement objet. Ceux-ci peuvent être ignorés, et ne seront pas montrer de nouveau lorsque vous cliquez sur l'entrée ou = Enseignants.

Dans l'écran suivant, sélectionnez **créer une sous- entrée**



Figure 2.7 : création d'une sous entrée LDAP

Dans la liste Sélectionnez un modèle pour modifier l'écran de saisie qui apparaît sur le côté droit de l'écran principal de phpLDAPAdmin, sélectionnez le E-Mail : compte modèle entrée de carnet.

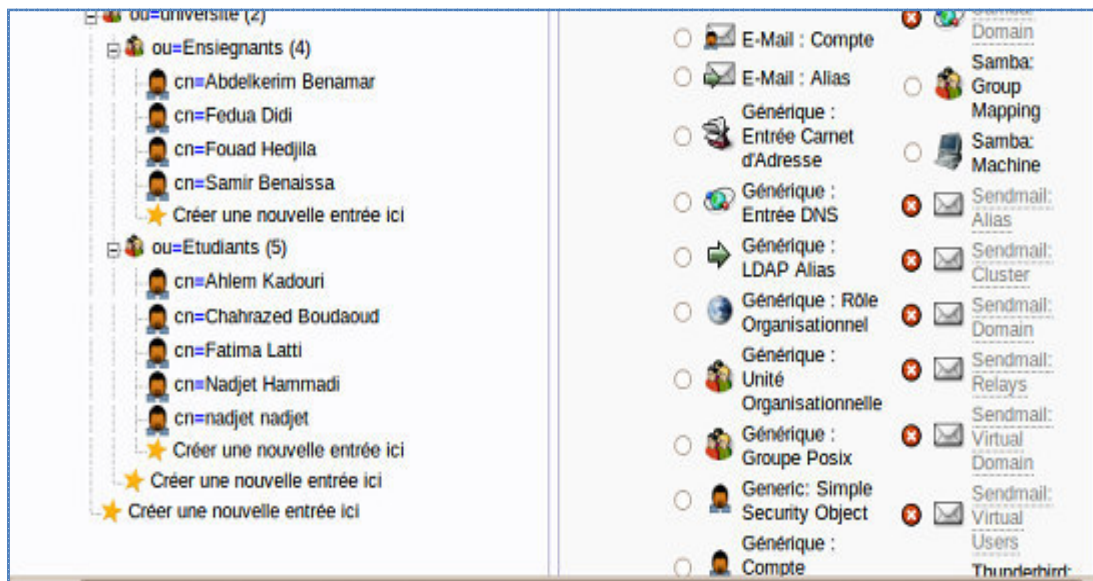


Figure 2.8 : les objets d'un annuaire

L'écran suivant affiche toutes les valeurs que vous pouvez utiliser pour créer la nouvelle entrée de carnet d'adresses. La seule valeur requise est Nom. Vous pouvez également revenir en arrière et modifier l'entrée à tout moment.

The screenshot shows the 'Créer un objet' (Create an object) form. At the top, it displays the server information: 'Serveur: My LDAP Server' and 'Conteneur: ou=Enseignants,ou=université,dc=example,dc=com'. Below this, it specifies the model: 'Modèle: Courier Mail: Account (courierMailAccount)'. The main heading is 'New Courier Mail Account (Étape 1 sur 1)'. The form has three sections: 'Nom Commun' (Common Name) with the value 'mohamed chouiti' and a note 'alias, requis, rdn'; 'Courriel' (Email) with the value 'chouiti@example.com' and a note 'alias'; and 'Given Name' (empty) with a note 'alias'.

Figure 2.9 : création d'une entrée

Lorsque vous avez entré les informations pour l'entrée du carnet d'adresses, cliquez sur Create Object

Figure 2.10 : createobject

Dans l'écran suivant, cliquez sur valider pour créer l'entrée LDAP

Attribut	Nouvelle valeur	Passer
<b>cn= chouiti,ou=Enseignants,ou=université,dc=example,dc=com</b>		
Common Name	chouiti	<input type="checkbox"/>
Last name	chouiti	<input type="checkbox"/>
objectClass	inetOrgPerson	<input type="checkbox"/>
Password	*****	<input type="checkbox"/>
User ID	101	<input type="checkbox"/>

Figure 2.11 : exemple d'une entrée LDAP

Vous verrez la nouvelle entrée, et vous devriez voir un message semblable à: Creation successful! DN: cn=chouiti ,ou=université ,dc=example ,dc=com a été créé. Or, dans le volet de navigation de gauche, il y aura un signe [+] à côté de ou = personnes. Cliquez sur cela pour développer, et la nouvelle entrée sera disponible.



Figure 2.12 : arborescence annuaire LDAP

Pour ajouter des entrées supplémentaires, cliquez sur ou = Etudiant, puis sur Créer une entrée d'étudiant, et suivre les mêmes étapes.

Vous pouvez configurer votre client e-mail à utiliser ce carnet d'adresses. Parce que le carnet d'adresses est stocké sur la machine virtuelle, vous pouvez la partager avec plusieurs utilisateurs. De cette façon, vous pouvez créer un carnet d'adresses pour une entreprise ou une organisation qui a été partagé entre tous les employés ou les membres.[3]

## 2.4. Conclusion

OpenLDAP offre donc une implémentation complète et robuste de ce standard en proposant un serveur et des outils clients.

Suite à ce chapitre vous serez en mesure de comprendre le protocole LDAP, administrer un serveur ainsi que connaître les principes de fonctionnement de cet annuaire.[12]

Nous devons maintenant avoir un serveur LDAP de base mis en place avec quelques utilisateurs et groupes. dans le chapitre suivant ne présentons la relation qui existe entre un serveur ldap et le service de courrier électroniques

# chapitre III

## **Relation entre service messagerie & Annuaire LDAP**



## Chapitre III relation entre service messagerie et annuaire LDAP

---

### 3.1. Introduction

Le courrier électronique est le service le plus utilisé aujourd'hui dans un Intranet ou sur Internet. Il permet aux utilisateurs qui possèdent une boîte aux lettres d'envoyer ou de recevoir des messages. La boîte aux lettres est identifiée par son adresse e-mail. Il est plus rapide et moins onéreuse que la plupart des autres moyens de communication (télécopie, téléphone, courrier postal, coursier).

Dans ce chapitre, nous présentons les étapes d'installation et configuration d'un serveur messagerie électronique Postfix. Puis nous montrons la relation qui existe entre le serveur de courrier électronique et l'annuaire LDAP.

Nous utilisons l'outil Thunderbird pour l'envoi et la réception des messages électroniques. Cet outil est très performant et qui possède une interface graphique.

### 3.2. Logiciel de virtualisation : Virtualbox

Nous sommes intéressés dans notre projet par l'application de la virtualisation virtualbox. C'est un logiciel formidable et techniquement avancé, Virtualbox, qui vous permettra de faire tourner un système dans un autre, tout cela de manière « virtuelle ». Découvrons d'abord ensemble ce qu'est VirtualBox avant de nous intéresser à son installation et à son fonctionnement. Un logiciel qui permet au débutant et à l'utilisateur expérimenté, de découvrir une distribution.

Bien entendu, seul le système hôte pourra interagir réellement avec les périphériques. Pour pouvoir faire tourner VirtualBox sur une machine, il faudra que celle-ci soit assez solide avec un processeur pas trop lent, suffisamment de Ram et de l'espace libre (de la place sera prise sur le disque dur physique pour créer l'espace virtuel). En gros, on pourra dire qu'il vous faudra en moyenne un processeur tournant entre 1 Ghz et 2 Ghz minimum, 1 Go de mémoire vive et un espace disque d'environ 10 Go pour une utilisation confortable.

Sous VirtualBox, la manipulation des machines virtuelles nécessite plusieurs étapes :

## Chapitre III relation entre service messagerie et annuaire LDAP

- ✓ **création d'un disque dur virtuel (VDI).** Nous pouvons soit créer un disque virtuel de taille fixe, soit utiliser un live-cd. Cette deuxième solution permet d'obtenir un disque virtuel n'occupant que peu de place ;
- ✓ **créer une nouvelle machine virtuelle.** Un fichier de description de la machine, comportant des différents paramètres de configuration, est créé ;
- ✓ **rattacher le disque VDI et l'image ISO** du système d'exploitation invité à la machine virtuelle ;
- ✓ **configurer le réseau** de la machine virtuelle
- ✓ **Lancer la machine virtuelle.**

### 3.2.1. Configuration réseau de virtualbox

Virtualbox possède 3 modes de fonctionnement réseau :

**Réseau interne** : les machines virtuelles sont confinées entre elles dans un réseau virtuel.

**NAT** : Les machines virtuelles peuvent accéder à internet via une connexion NAT.

**Adaptateur réseau hôte** : Les machines virtuelles utilisent une interface de l'ordinateur hôte pour accéder au réseau.

Dans notre cas, nous avons créés deux machine virtuelles a l aide de virtualbox.

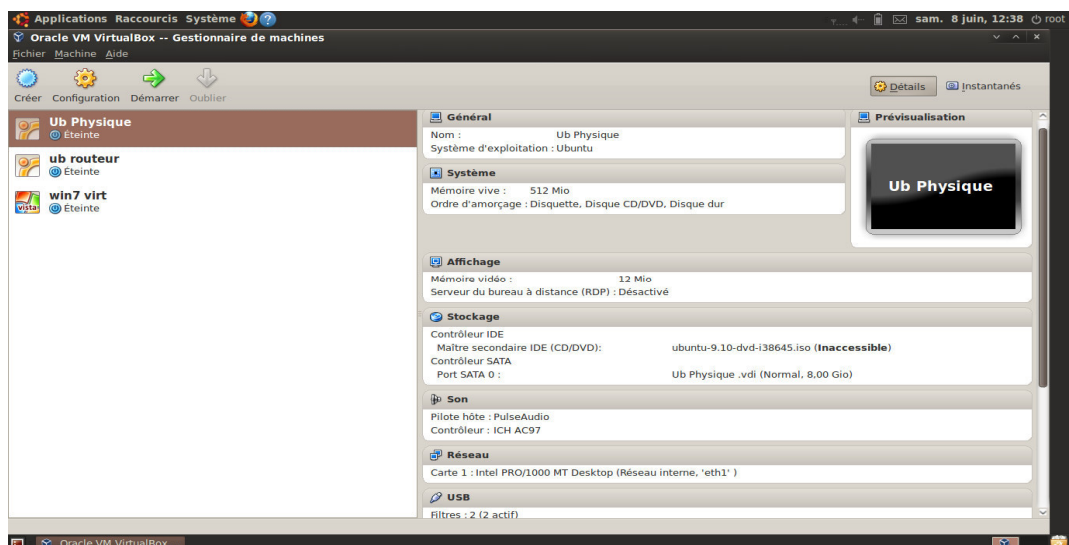


Figure 3.1 :Virtualbox

### 3.3. Messagerie électronique (serveur mail postfix)

Un système de messagerie électronique est l'ensemble des éléments contribuant à transmettre un courriel (courrier électronique : message transmis via un réseau informatique) de l'émetteur au récepteur.[4] Il y a trois éléments fondamentaux. Ce sont:

- le Mail Transfert Agent ou **MTA**
- le Mail Delivery Agent ou **MDA**
- le Mail User Agent ou **MUA**

#### **MUA (Mail User Agent) : client messagerie**

L'agent utilisateur (MUA) est le programme dont vous vous servez pour communiquer avec le système de courrier électronique (client de courrier électronique). Sous Linux l'agent utilisateur le plus simple se nomme mail, mutt et pine.

#### **MTA (Mail Transfert Agent)**

Un agent de transport (MTA, Mail Transport Agent), aussi appelé serveur de messagerie, comme postfix et sendmail. Il est utilisé pour l'envoi des courriers électroniques en utilisant le protocole SMTP (Simple Mail Transport Protocol : Port 25)

#### **MDA : Mail Delevred Agent**

Protocole de récupération des courriers électroniques, utilise le POP3

#### **3.3.1. Description de l'architecture de fonctionnement d'un service de messagerie électronique**

Les différents éléments du système de messagerie sont agencés selon une architecture logique, pour en assurer le fonctionnement.

## Chapitre III relation entre service messagerie et annuaire LDAP

Nous représentons cette architecture par le schéma suivant:

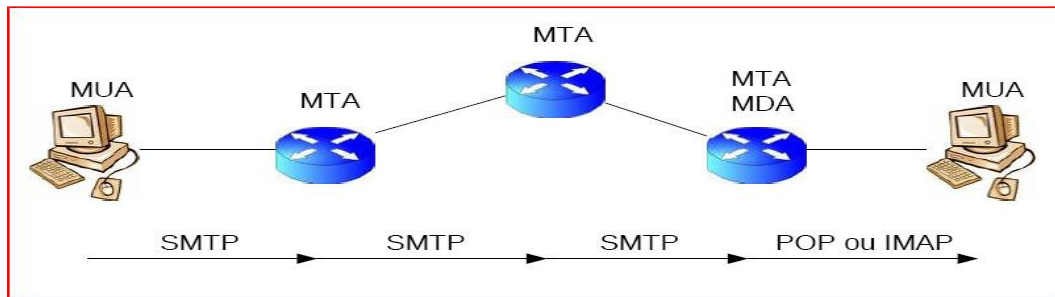


Figure 3.2 : schéma courrier électronique

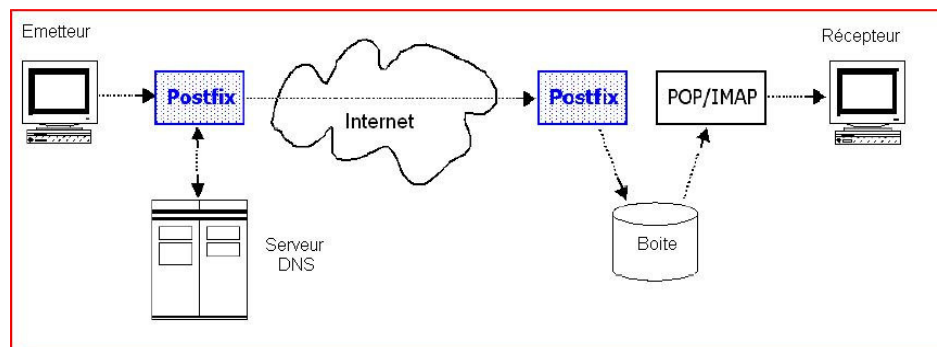


Figure 3.3 : service mail Postfix

### 3.3.2. Configurer un serveur de mail avec postfix

#### Le Mail Transfer Agent Postfix

Un Mail Transfer Agent (MTA), ou SMTP daemon, permet de transmettre des messages (mail) d'un ordinateur à un autre.

Pour envoyer un mail, on se connecte au serveur SMTP en s'authentifiant en utilisant un client de mail (outlook, thunderbird, mutt ...), qui transmet le message.

Le serveur SMTP applique des filtres (souvent antispam) sur le mail. Le MTA postfix a aussi des fonctionnalités de Mail Delivery Agent (MDA) qui lui permettent de livrer le courrier dans une mailbox (mbox ou Maildir).

Les clients utilisateur utilisent ensuite un serveur POP (Pop : serveur de récupération des courriers électroniques - MDA Mail Delivery Agent) pour aller chercher le mail dans la mailbox qui se trouve sur le serveur.[29]

## Chapitre III relation entre service messagerie et annuaire LDAP

---

La configuration de base de Postfix se fait dans le fichier `/etc/postfix/main.cf`. On y spécifie essentiellement les filtres à appliquer au mail pour éviter que les utilisateurs ne reçoivent trop de spams, mais aussi pour éviter que le MTA ne soit utilisé comme relai par des spammeurs.

Postfix est un serveur qui peut seulement envoyer du courrier électronique

Les adresses email seront du style: `nom_de_la_personne@nom_de_votre_domaine`. Il y aura deux serveurs pour la réception des messages, un **POP** et un **Imap**

Le **Pop** permet de récupérer tous les courriers du serveur vers le client, tandis que l'**Imap** se synchronise avec le serveur, donc tous les mails restent sur le serveur pour ce dernier

### 3.3.3. Installation du serveur Postfix

Commençons par taper la commande suivante pour installer Postfix







**apt-getinstallpostfix**

Pendant l'installation de Postfix, vous allez voir apparaître des fenêtres pour la configuration du serveur de mail, suivez ci-dessous le paramétrage de votre serveur.[21]

1- Choisissez l'option "**Site Internet**"

2- Indiquez le nom des domaines autorisé, exemple **licence-pfe.dz**

Voilà l'installation est terminée, allez voir dans le dossier: `/etc/postfix/`, si vous avez

 <code>dynamicmaps.cf</code>	318 octets Texte simple
 <code>main.cf</code>	589 octets Texte simple
 <code>master.cf</code>	6,4 ko Texte simple
 <code>postfix-files</code>	15,7 ko Texte simple
 <code>postfix-script</code>	5,7 ko Script shell
 <code>post-install</code>	20,7 ko Script shell

## Chapitre III relation entre service messagerie et annuaire LDAP

---

les fichiers suivants:

Le fichier principale se nome **main.cf**, c'est le fichier principale de configuration du serveur de mail. Il est déjà rempli avec les options définies lors de l'installation

Avec les paramètres par défaut votre serveur de mail peut fonctionner en local. Donc que sur la machine ou il a été installé.

### Configuration du serveur

#### Le fichier de configuration main.cf

1- Ici regroupe les **paramètres de fonctionnement** de postfix. Ne pas modifier cette partie au risque de faire planter le serveur.

```
command_directory = /usr/sbin
daemon_directory = /usr/lib/postfix
program_directory = /usr/lib/postfix
smtpd_banner = $myhostname ESMTP $mail_name
setgid_group = postdrop
biff = no
```

2- Maintenant on définit le domaine. Remplacer par le votre, exemple de nom de domaine : **Example.com**

```
mydomain = Example.com
```

3- Ensuite en met le nom d'hôte du serveur de mail. Remplacer "**nadjet**", par le nom de votre serveur : nadjet.licence-pfe.dz

```
myhostname = nadjet.$mydomain
```

4- L'extension pour les mails envoyés depuis la machine. Remplacer "**Example.com**", par l'extension que vous désirez.

```
myorigin = Example.com
```

## Chapitre III relation entre service messagerie et annuaire LDAP

---

5- Puis il faut indiquer la liste de domaine autorisé par Postfix.

```
mydestination = nadjat.Example.com, localhost.$mydomain
```

6- Puis si vous voulez envoyer du mail sur l'internet depuis votre réseau local, indiquer le serveur **smtp** de votre FAI.

```
relayhost = smtp.fawri.dz
```

7- Ensuite on indique à Postfix dans quels réseaux il doit travailler. La remplacer "**192.168.1.1**", par votre réseau.

```
mynetworks = 127.0.0.0/8, 192.168.1.1
```

8- Vous pouvez utiliser un quota pour la taille des boîtes aux lettres. A noter que si la valeur est de zéro, alors la boîte est illimitée.

```
mailbox_size_limit = 0
```

9- Indiquer le type de réseau utilise : réseau local :

```
mynetworks_style = subnet
```

10- le répertoire de stockage des courriers électroniques reçues

```
mail_spool_directory = /var/mail
```

### Installation d'un Serveur Pop (MDA) de récupération des courriers électroniques

Nous allons installer **Qpop** comme serveur (*Taille: 602 Ko*). Pour cela taper dans la console la commande suivante.

## apt-getinstallqpopper

### 3.3.4. Installation d'un client messagerie (MUA) mail user agent

#### Installation d'un client messagerie mutt( MUA)

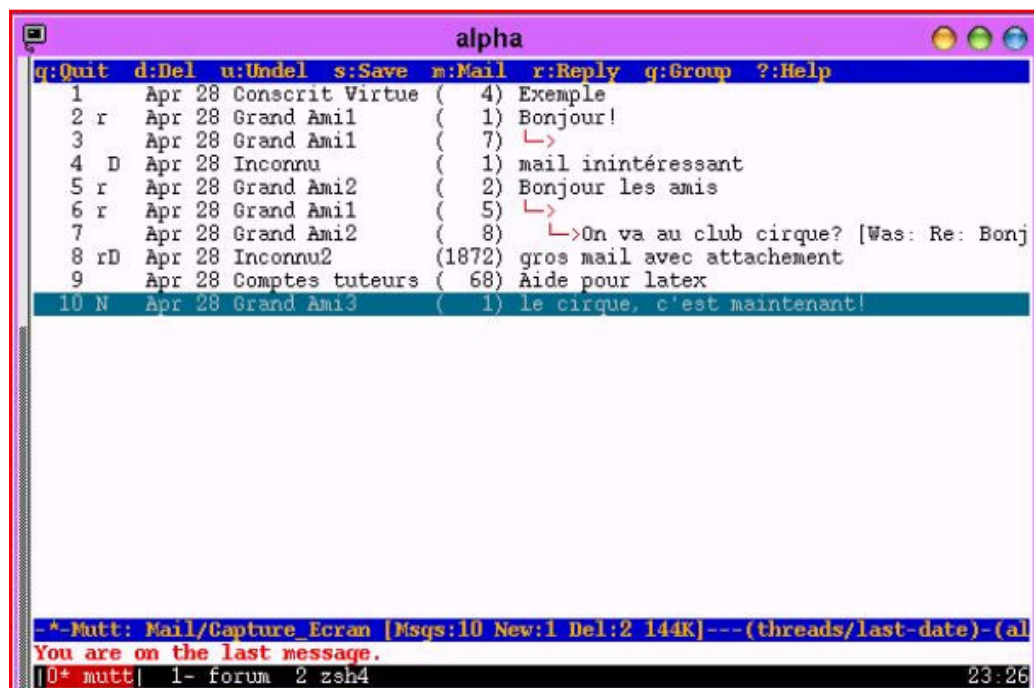
Mutt permet de gérer une messagerie électronique sous UNIX. Il permet donc d'envoyer et de recevoir des messages, de gérer des boîtes aux lettres, d'utiliser des alias.

#### Installer le paquet mutt

#### apt-getinstallmutt

Tapez la commande mutt sur le shell pour lancer le client messagerie mutt

Vous avez l'écran suivant :



```
alpha
q:Quit d:Del u:Undel s:Save m:Mail r:Reply q:Group ?:Help
1 Apr 28 Conscrit Virtue ( 4) Exemple
2 r Apr 28 Grand Amil ( 1) Bonjour!
3 Apr 28 Grand Amil ( 7) ↳
4 D Apr 28 Inconnu ( 1) mail inintéressant
5 r Apr 28 Grand Ami2 ( 2) Bonjour les amis
6 r Apr 28 Grand Amil ( 5) ↳
7 Apr 28 Grand Ami2 ( 8) ↳On va au club cirque? [Was: Re: Bonj
8 rD Apr 28 Inconnu2 (1872) gros mail avec attachement
9 Apr 28 Comptes tuteurs ( 68) Aide pour latex
10 N Apr 28 Grand Ami3 ( 1) le cirque, c'est maintenant!

--*.Mutt: Mail/Capture Ecran [Msgs:10 New:1 Del:2 144K]---(threads/last-date)-(al
You are on the last message.
|0+ mutt| 1- forum 2 zsh4 23.26
```

Figure 3.4 : client messagerie mutt



# Chapitre III relation entre service messagerie et annuaire LDAP

## 3.3.5. Installation client messagerie Thunderbird sous linux (MUA)

Installer le client Mozilla Thunderbird qui se trouve sur dépôt de système linux ubuntu

### Configuration

Lors du 1er lancement de Thunderbird, vous est proposé de créer le premier compte, suivez l'installation[15] :

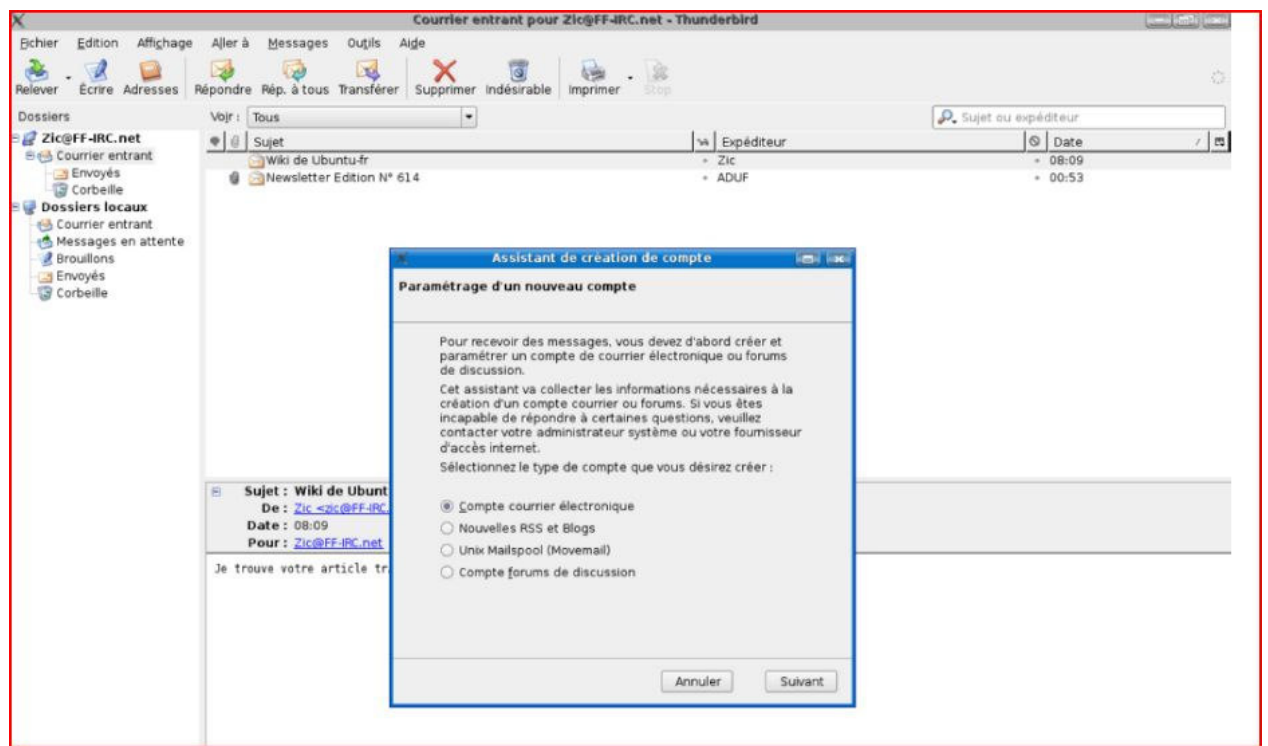


Figure 3.5 : client messagerie Thinderbird

# Chapitre III relation entre service messagerie et annuaire LDAP

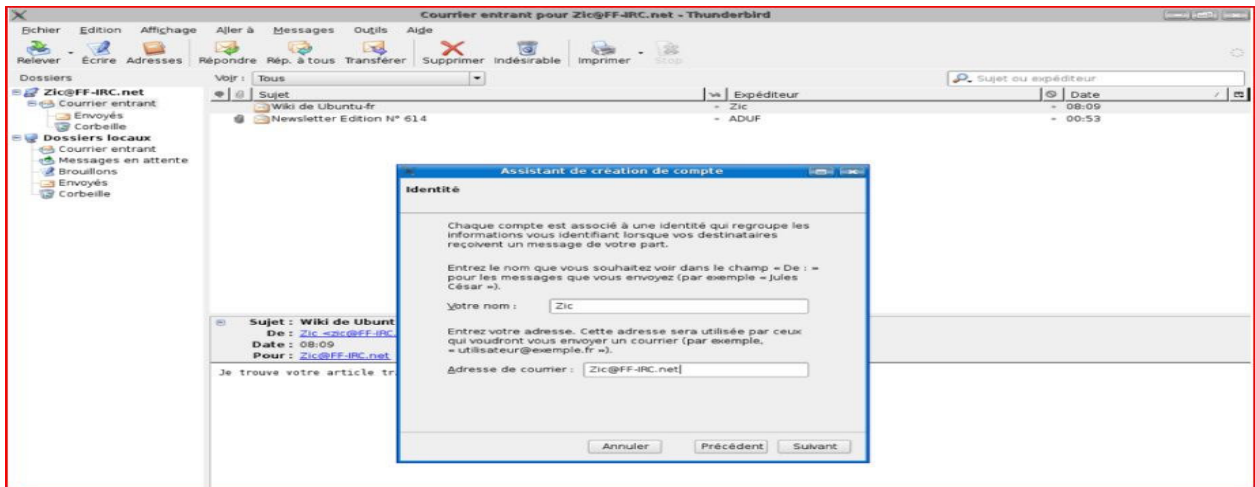


Figure 3.6 : adresse serveur mail postfix

Entrer adresse IP de serveur mail (MTA : protocole SMTP : postfix) et serveur de réception de courrier électronique (MDA : protocole pop3 : qpopper))

Cochez **pop** au lieu **ima** **Figure 3.6** : adresse serveur mail Postfix **serveur de mail** est situé dans mon réseau, donc l'adresse est 192.168.0.2, et l'utilisateur,

Entrez le nom de l'utilisateur : login

# Chapitre III relation entre service messagerie et annuaire LDAP

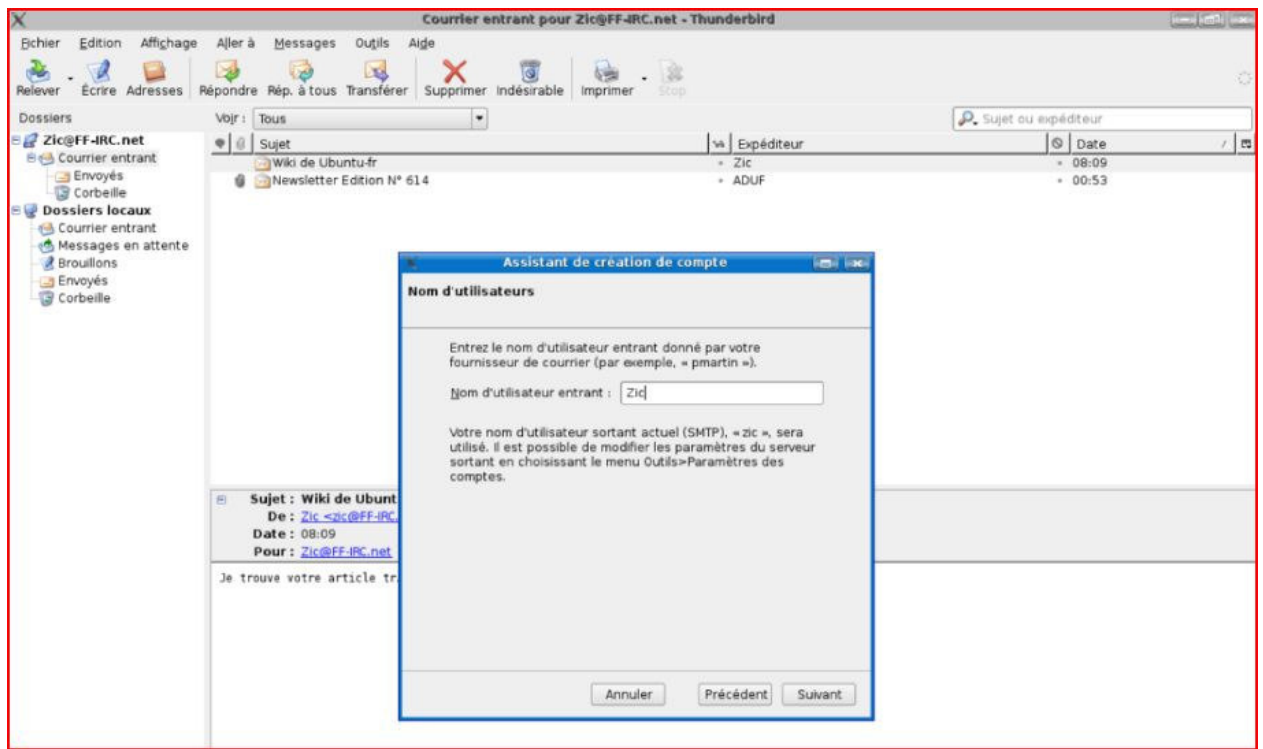


Figure 3.7 : nom utilisateur

Entrez l'adresse électronique de courrier mail

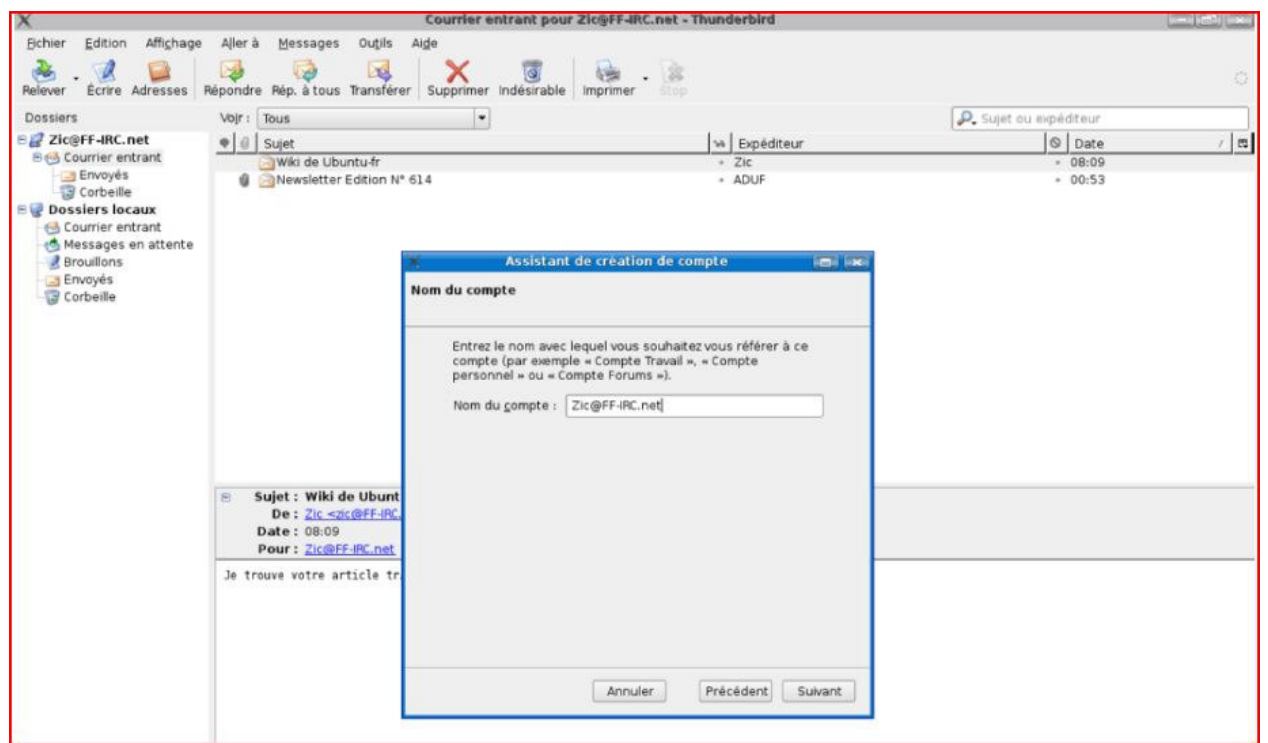


Figure 3.8 : compte mail Thunderbird

## 3.4. Relation entre annuaire LDAP et serveur de messagerie électronique

Le serveur Postfix accepte tous les mails à destination d'un domaine particulier mais, n'ayant pas connaissance des comptes existant sur ce domaine, il ne peut filtrer plus précisément les mails entrants. La solution est de relier postfix à l'outil de gestion des utilisateurs, ici LDAP. Pour cela, il faut tout d'abord avoir un système LDAP fonctionnel.[26]

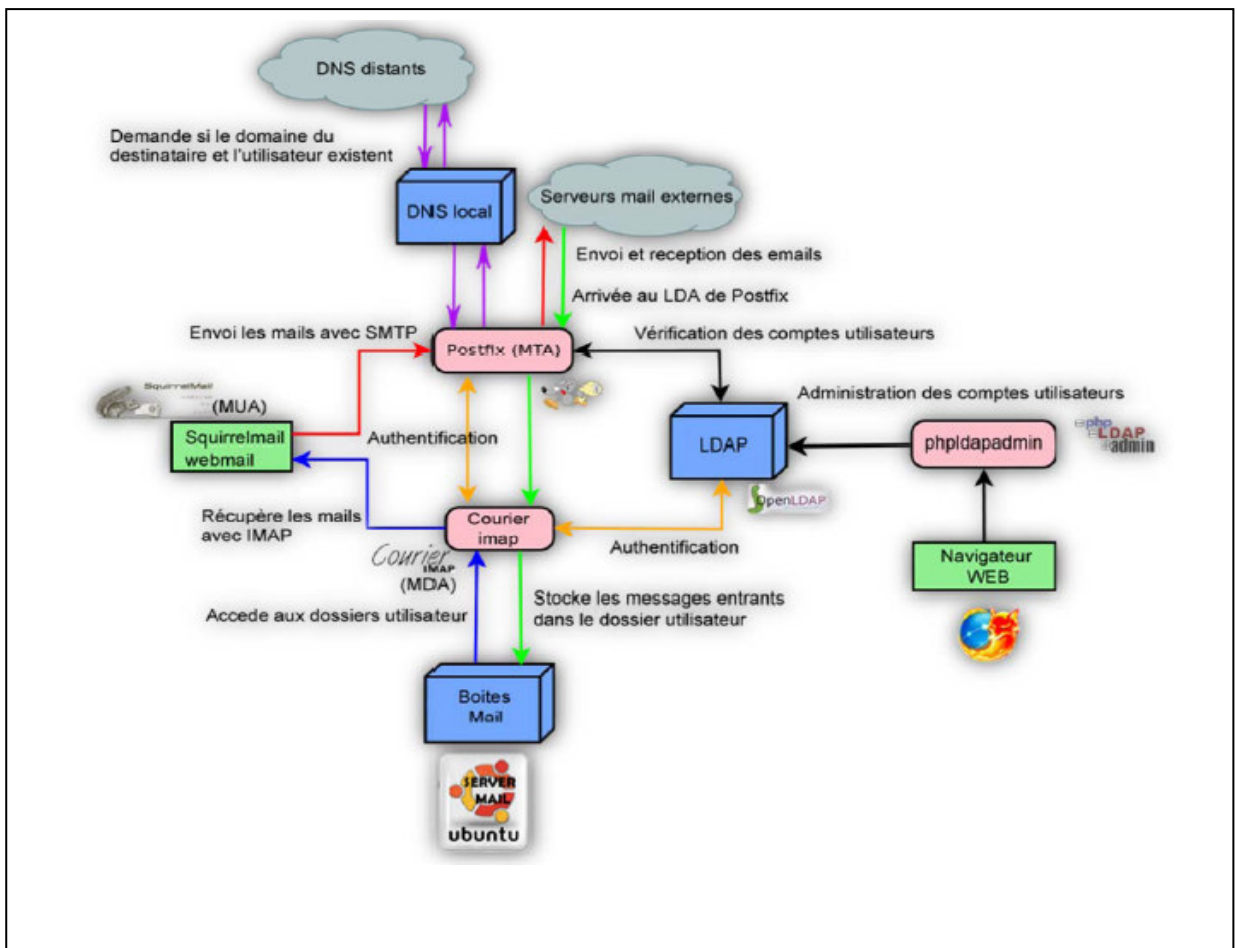


Figure 3.9 : relation service mail et annuaire LDAP

## Chapitre III relation entre service messagerie et annuaire LDAP

---

-**LDAP** est le logiciel permettant de gérer les utilisateurs et les groupes pour des clients systèmes (droits utilisateurs systèmes dans un domaine AD) ou pour des logiciels.

- **Courier** est un logiciel permettant de proposer le service IMAP ou POP3 pour la livraison des mails aux utilisateurs de la base de données.

-**Postfix**, quant à lui, est un logiciel permettant de proposer le service SMTP pour l'envoi des mails par les utilisateurs de la base de données.

- **Squirrelmail** ou **Thunderbird** permet de fournir aux utilisateurs une interface WEB conviviale pour gérer leur messagerie.

Il sera possible, par la suite de paramétrer des clients de messagerie locaux pour les comptes créés dans LDAP

### 3.4.1. Configuration postfix-ldap

Quand il reçoit un mail, postfix check la table des alias dans `/etc/aliases` (par défaut) pour voir si le mail doit être forwarder autre part. Il est possible de rajouter une directive dans le `'main.cf'` pour que postfix requête LDAP avant ou après avoir checké cette table. Bien entendu, la première chose à faire est d'installer, toujours avec `apt-get`, le package `postfix-ldap` :

```
apt-get install postfix-ldap
```

Ensuite, à directive à ajouter est :

```
local_recipient_maps = ldap:/etc/postfix/ldap_local_recipient.cf, $alias_maps
```

Sachant que `alias_maps` est habituellement placé sur la valeur

## Chapitre III relation entre service messagerie et annuaire LDAP

```
alias_maps = hash:/etc/aliases
```

Mais ce qui nous intéresse ici, c'est `ldap_local_recipient.cf`. Ce fichier doit contenir la méthode à utiliser pour interroger LDAP. Vous pouvez utiliser le modèle ci-dessous :

```
server_host = 127.0.0.1
server_port = 389
search_base = dc=licence-pfe,dc=dz
# le %s signifie "adresse du destinataire telle que fourni par la commande "RCPT
TO:"
query_filter = (mail=%s)
result_attribute = mail
```

Il ne reste plus qu'à recharger Postfix et à tester. La commande `postmap` nous permet de vérifier que cela fonctionne :

```
nadjet:##postmap -q samir@licence-pfe.dz ldap://etc/postfix/ldap_local_recipient.cf
samir@licence-pfe.dz
nadjet:##postmap -q hamadi@licence-pfe.dz ldap://etc/postfix/ldap_local_recipient.cf
nadjet:##
```

Dans le premier cas, `postmap` renvoie une réponse positive à la requête. Notez bien que vous devez requêter sous la forme `user@domain` et pas autrement. Dans le second cas, `postmap` ne renvoie rien, l'entrée n'a pas été trouvée.

### 3.4.2. Configuration et schémas

Le fichier `slapd.conf` permet de configurer le serveur, de définir les schémas utilisés et le mot de passe de l'administrateur du serveur LDAP.

Les schémas LDAP sont une collection d'objets répondant aux normes de l'OMG (Object Management Group) et dont chaque composant est attribué d'un OID (Object ID). Ces différents schémas permettent ainsi d'implémenter l'utilisation des comptes Postfix. La déclaration de leur utilisation se fait dans le fichier `slapd.conf`.

## Chapitre III relation entre service messagerie et annuaire LDAP

---

Une fois l'installation d'OpenLDAP réalisée et les schémas choisis, il faut déterminer l'architecture de l'arbre et des données à insérer. Ce paramétrage n'est pas définitif et il est possible à posteriori de procéder à une extension des schémas et donc d'en utiliser de nouveaux.

Extrait du fichier slapd.conf :

```
# Schema and objectClass definitions
include /usr/local/ldap/etc/openldap/schema/core.schema
include /usr/local/ldap/etc/openldap/schema/cosine.schema
include /usr/local/ldap/etc/openldap/schema/nis.schema
include /usr/local/ldap/etc/openldap/schema/misc.schema
include /usr/local/ldap/etc/openldap/schema/inetorgperson.schema
include /usr/local/ldap/etc/openldap/schema/openldap.schema
include /usr/local/ldap/etc/openldap/schema/samba.schema
include /usr/local/ldap/etc/openldap/schema/postfix.schema
```

Ces schémas sont fournis avec les sources des logiciels des logiciels concernés, ici Samba et Postfix

### Choix de la structure de l'arbre

#### Organisation des données dans un annuaire

Les données dans un annuaire LDAP sont organisées dans une structure modélisée par un arbre où nous pouvons distinguer deux catégories d'objets :

- les conteneurs qui peuvent-être considérés comme le départ d'une nouvelle branche,
- les feuilles qui sont les terminaisons des branches.

Un conteneur peut contenir les deux catégories d'objet, soit des conteneurs, soit des feuilles.

## Chapitre III relation entre service messagerie et annuaire LDAP

---

### Organisation des conteneurs et des feuilles

Concrètement les conteneurs correspondront aux centres et unités de recherches et les objets feuilles correspondront aux utilisateurs et machines.

Il est également possible d'utiliser des objets conteneurs à des fins de rangements. Ainsi les conteneurs USER, GROUP et COMPUTER, stockent respectivement les comptes utilisateurs, les groupes Posix et les comptes machines. Ils n'ont pas d'autre utilité que de faciliter la lecture des données lors de la navigation.

### Choix des Objets

#### Centre et Unités de recherches

Il s'agit des objets conteneurs qui forme la base de la structure de notre arbre. L'objet LDAP classique est l'OU ou OrganizationalUnit. C'est l'objet conteneur le plus classiquement utilisé dans ce rôle et que l'on retrouve d'ailleurs dans Active Directory. Dans certains cas ces conteneurs ont été associés à des objets PosixAccount afin de pouvoir gérer des droits.

#### Centre et Unités de recherches

Il s'agit des objets conteneurs qui forme la base de la structure de notre arbre. L'objet LDAP classique est l'OU ou OrganizationalUnit. C'est l'objet conteneur le plus classiquement utilisé dans ce rôle et que l'on retrouve d'ailleurs dans Active Directory. Dans certains cas ces conteneurs ont été associés à des objets PosixAccount afin de pouvoir gérer des droits.

#### Les comptes utilisateurs

L'un des principaux objectifs de l'utilisation de LDAP est la gestion des comptes de tous les utilisateurs. Un objet utilisateur tel que nous l'entendons n'existe pas dans LDAP et il est nécessaire de le définir en fonction des données administrative (mail, téléphone, photo ...) et système dont nous avons besoin.[24]

#### Les groupes

Il s'agit de gérer les groupes de travail et les équipes de recherche



## Chapitre III relation entre service messagerie et annuaire LDAP

### Utilisation et exploitation de l'annuaire LDAP par la messagerie électronique

Postfix est livré avec un schéma pour LDAP qui permet de gérer tous les paramètres d'un compte mail-Postfix via l'objet LDAP PostfixUser dans phpldapadmin

Voilà des exemples réalisés par client MUA thunderbird pour la recherche directe des comptes mail dans l'annuaire LDAP.

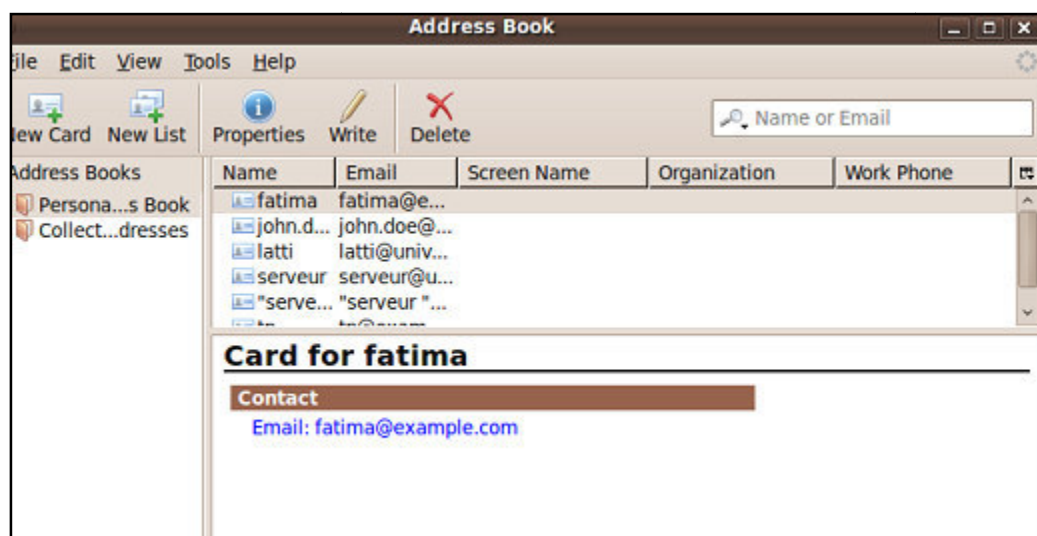


Figure 3.10 :carnet d'adressage LDAP et Postfix

### 3.5. Conclusion

LDAP permet de gérer toutes les informations nécessaires comme compte utilisateur avec une très grande facilité. Son fonctionnement en réseau et son déploiement, sont relativement aisés et rapides à mettre en œuvre. Sa compatibilité avec de nombreux logiciels en font dorénavant un outil incontournable pour une administration de plusieurs services réseaux comme dans notre cas le serveur de messagerie électronique postfix.

Dans ce chapitre, nous avons montrés l'efficacité et les performances de l'annuaire LDAP dans la gestion et la centralisation de tous les informations sur un utilisateur qui inscrit dans un serveur de messagerie électronique.

## Conclusion générale

L'administration des comptes utilisateurs en réseau, sur plusieurs serveurs Linux simultanément peut être relativement compliquée

Notre objectif était de mettre en place un outil d'administration, centralisé, unique, nous permettant de gérer à la fois les comptes utilisateur avec leurs adresses mail.

LDAP permet de gérer toutes les informations nécessaires à la mise en place d'une telle structure, avec une très grande facilité, pour peu que l'on ait quelques notions sur les annuaires. Son fonctionnement en réseau et son déploiement, sont relativement aisés et rapides à mettre en œuvre. Sa compatibilité avec de nombreux logiciels en font dorénavant un outil incontournable pour un administrateur réseau.

L'objectif de notre projet de fin d'étude n'est pas de donner un cours théorique sur LDAP mais de présenter une utilisation concrète des fonctionnalités de LDAP au travers du logiciel OpenLDAP associé avec un service de messagerie électronique Postfix.

L'administration d'un serveur de messagerie électronique devient très souple et très simple. Le point capital est d'appréhender le fonctionnement d'un annuaire LDAP et la façon d'organiser les données.

Si le point de départ de notre implémentation d'OpenLDAP était de faciliter l'administration des comptes mail d'un serveur de courrier électronique, très vite, nous avons organisé les informations contenues dans l'annuaire afin de l'utiliser comme base de données. C'est un outil qui offre des perspectives et des fonctionnalités très complètes sur le plan de l'administration système et réseau

Un point faible, cependant, il n'existe pas encore d'outil permettant à la fois de gérer le contenu de l'annuaire et les droits d'accès à ce même annuaire.

## **Résumé**

L'administration des comptes utilisateurs en réseau, sur plusieurs serveurs Linux simultanément peut être relativement compliquée.

Notre objectif était de mettre en place un outil d'administration, centralisé, unique, nous permettant de gérer à la fois les comptes utilisateur avec leurs adresses mail.

L'utilisation de LDAP et en particulier d'OpenLDAP nous a permis de nous doter d'un outil d'administration réseau très performant.

L'annuaire OpenLDAP, nous permet de gérer les comptes utilisateurs et leur groupes. L'association OpenLDAP avec la messagerie électronique nous permet aussi d'utiliser des mails des utilisateurs d'une façon centralisée.

Il s'agit là d'un formidable outil d'administration à tout point de vue, pour la gestion centralisée des comptes aussi bien que pour le suivi du parc informatique et la gestion de la sécurité.

## **Abstract**

The administration of network users accounts on several Linux servers simultaneously can be quite complicated.

Our goal was to establish a single administrative tool, centralized, allowing us to manage both user accounts with their email addresses.

The use of LDAP and OpenLDAP in particular has allowed us to provide us with a very efficient network administration tool.

The OpenLDAP directory, allows us to manage user accounts and groups. The OpenLDAP association with email also allows us to use mail users in a centralized manner.

This is a great management tool at any point of view, for centralized account management as well as to monitor the IT infrastructure and security management.