République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université A/Mira de Béjaïa
Faculté des Sciences Exactes
Département d'Informatique

Mémoire de fin de cycle
en vue d'obtention du diplôme de master professionnel en informatique
spécialité : Administration et Sécurité des Réseaux

Thème

La mise en oeuvre et l'administration d'un serveur de messagerie.

Présenté par :

M^elle^ ***BENBARA*** **Kahina**

M^elle^ ***RABHI*** **Meriem**

Président	M^r^ ***BADACHE*** **A**
Examinateur	M^r^ ***SAADI*** **M**
Examinateur	M^r^ ***AISSANI*** **S**
Encadreur	M^r^ **HAMMOUMA M**

Promotion 2012/2013

Remerceiments

Nous tenons à adresser nos remerciements à toutes personnes qui nous ont apporté de laide afin que ce mémoire soit réalisé.

En premier, nous remercions notre encadreur Mr HAMMOUMA Moumene, pour ses suggestions et ses propositions qui nous ont été d'une grande utilité.

Ensuite, nos remercîments vont aux personnes de la D.O.T de Bejaia, en particulier, Mr LAKHDER CHAOUCHE Mohamed chef de département commercial et Mme MEZOUARI, sans oublier Mr. ZOUGAR.A et Mr. MAOUDA.T, de Data Center et Djaweb d'Alger, pour toutes les informations qu'ils nous ont fournies et pour le temps qu'ils nous ont consacré. Merci.

Nous remerciement sadresse aussi à notre professeur de sécurité Mr AKILAL pour le temps quil nous a consacré, pour ses suggestions, pour ses orientations ainsi que ses encouragements.

En dernier, nous remercions nos très chères familles, pour leurs soutiens, leurs encouragements et leur patience.

Dédicace

Je dédie ce modeste travail à mes plus chers êtres au monde, mes parents qui, par leurs aides et leur amour, m'ont appris à m'épanouir.

A ma soeur, mes frères et mes belles-soeurs qui, m'ont beaucoup aidé, encouragé et mont trop supporté.

A mes quatre neveux, Nahil, Wassim, Badis et Nazim que j'adore.

A ma grande famille, qui m'en soutenu.

A Meriem, avec qui j'ai passé des bons moments et parfois difficile, ensemble on a su tous surmonter.

A mes amis, qui sont autour de moi tout le temps et qui nont jamais cessé de m'encourager.

Et à tous ceux qui ont contribué à la réussite de ce projet.

Kahina

Dédicace

Je dédie ce travail, à ma famille, à mes très chers parents,
auxquels je souhaite, une longue vie et une bonne santé ; à mes quatre soeurs, Houda,
Sihem, Yasmine et Yakout Malek (kouka) ; à mes deux familles paternelle et maternelle,
dont je suis fière de porter le sang dans les vignes.
Une dédicace à tous mes amis, avec qui j'ai passé d'agréables moments pendant mon
parcours universitaire.
Une dédicace spéciale à mes deux amies, Leila et Lydia, avec lesquelles je partage des
bons souvenirs que je n'oublierai jamais.
A Kahina, avec qui j'ai eu le plaisir de réaliser ce projet, nous avons
Passé des périodes riche d'émoussions. Le plus important, est que nous avons pu
réussir à faire notre projet ensemble, un travail d'équipe.
Une pensée à une personne qui m'est très cher, malheureusement elle n'est plus parmi
nous, j'aurais tant aimé qu'elle soit avec moi en ce moment, mais
la vie est faite ainsi, à ma grand-mère qui me manque tant,
TAYAKOUT « Yema Kouka ».

Meriem

Résumé

La messagerie électronique est un service très répondu et indispensable dans le domaine professionnel et dans la vie quotidienne. Ce service rend la communication plus facile et plus simple grâce au gain du temps et de qualité de réponse. En revanche, il peut être une menace pour la sécurité, d'où vient l'obligation de le sécurisé et de maintenir sa sécurité.

Notre travail consiste à mettre en œuvre et administrer un serveur de messagerie pour la DOT de Bejaia pour répondre à leurs besoins.

Nous avons commencé, par expliquer quelques notions de base de la messagerie électronique et détailler son fonctionnement, les outils utilisés avant de passer à sa réalisation, et nous avons finis par le sécurisé.

La réalisation est faite en utilisant le serveur de messagerie postfix et squirrelmail comme client pour la gestion des mails.

Mots-clés : MUA, MTA, MDA, SMTP, IMAP, POP,postfix, Squirrelmail.

Abstract

Email is a very essential service and answered in the professional field and in everyday life. This service makes communication easier and easier thanks to gain time and quality of response. However, it may be a security threat, which has an obligation to secure and maintain its security.

Our job is to implement and administer a mail server for the DOT Bejaia to meet their needs.

We started by explaining some basics of e-mail and detail its operation, the tools used before moving to its realization, and we finally secure it.

The implementation is done using the postfix mail server and squirrelmail as a client for managing email.

Keywords :MUA, MTA, MDA, SMTP, IMAP, POP, postfix, Squirrelmail.

LISTE DES ABRÉVIATIONS

LAN : Local Area Network
MAN : Metropolitan Area Network
WAN : Wide Area Network
OSI : Open System Interconnection
TCP/IP : Transmission Control Protocol / Internet Protocol
MTU : Maximum Transmission Unit
MUA : Mail User Agent
MTA : Mail Transfert Agent
MDA : Mail Delivery Agent
SMTP : Simple Mail Transfer Protocol
POP3 : Post Office Protocol version 3
IMAP : Interactive Mail Access Protocol
DNS : Domain Name Server
MX : Mail eXchanger
NAT : Natwork Address Translation
DMZ : DeMilitarized Zone
VPN : Virtual Private Network
PPTP : Point to Point Tunneling Protocol
L2TP : Layer 2 Tunneling Protocol
DOT : Directions Opérationnelles des Télécommunication
D.R.T : Délégations Régionales des Télécommunications
DG : La Direction Générale de lentreprise
RMS : Réseau multimédia et sécurité
PHP :Hypertext Preprocessor
S/MIME : Secure/Multipuprose Internet Mail Extension

SSL : Secure Socket Layer

SSH : Secure SHell

LAMP : Linux Apache2 Mysql Php

TABLE DES MATIÈRES

LISTE DES TABLEAUX

TABLE DES FIGURES

INTRODUCTION GÉNÉRALE

Dans le cadre de préparation, de notre projet fin d'étude, spécialité Informatique, option, Administration et Sécurité des Réseaux, nous avons opté pour le thème, mise en uvre et administration d'un serveur messagerie.

Ce thème, nous l'avons choisi afin de remédier aux problèmes de l'échange d'informations, au sein de notre organisme d'accueil, la Direction Opérationnelle des Télécommunication de Bejaia, où nous avons effectué notre stage. Ces problèmes seront cités dans le cahier de charge. Dans le but de faciliter leurs taches nous leurs avons suggérer des solutions.

La messagerie électronique est parmi les services les plus utilisé et plus répondu pour les entreprises et les individus dans la technologie de l'information et la communication, car, il optimise la communication, facile à utiliser, c'est un service gratuit et assez développé, ce qui le rend indispensable. En revanche, ce service est la cible des attaques, à cause de nombres d'informations qui sont échangé et l'importance qu'ils peuvent avoir. C'est la raison pour laquelle il faut le sécuriser. Pour assurer la sécurité, il existe plusieurs mécanismes qui nous la garantie. Dans notre mémoire, nous essayerons de traiter les différents points en relation avec la messagerie électronique, dans le but de mieux comprendre le fonctionnement de ce système.

Nous allons exposer le plan du mémoire qui se subdivise en quatre principaux chapitres :

- Le premier chapitre comporte des généralités sur les réseaux informatiques, le rôle indispensable de DNS (Domain Name Server) et la sécurité des réseaux locaux.
- Dans le second, nous avons présenté l'organisme d'accueil et le cahier de charge.
- Le troisième est consacrer à la messagerie : les adresses électroniques, les serveurs, moyens d'envoie des courriers électroniques et les protocoles utiliséspour cela, son système de fonctionnement et les techniques utilisées pour sa sécurité.
- En dernier,dans le quatrième chapitre, nous illustrons les différentes étapes que nous avons suivies, pour la mise en uvre et l'administration de notre serveur de messagerie.

CHAPITRE 1

GÉNÉRALITÉS

1.1 Introduction

Afin de mieux comprendre notre thème et savoir le traiter avec indulgence, il faudrait bien connaitre certains termes de base, et c'est le but de ce chapitre. Dans ce qui suit nous allons élaborer des notions qu'on aura certainement besoin dans les chapitres qui suivront. Ces notions sont en relation avec les réseaux informatiques (topologie d'un réseau, architecture, le routage,...), la manière avec laquelle ces réseaux se communiquent et de quoi un réseau interne a besoin pour qu'il soit sécuriser.

1.2 Généralités sur les réseaux

Un réseau informatique est un ensemble de machines qui sont connectées les unes aux autres dans le but de se communiquer, d'échanger les informations, partage de ressources, ..etc.

Les réseaux ont pour fonction de transférer des données d'une machine terminale vers une autre. Pour ce faire, une série d'équipements et de processus sont nécessaires, allant de l'environnement matériel utilisant des câbles terrestres ou des ondes radio jusqu'à l'environnement logiciel, constitué de protocoles, c'est-à-dire de règles permettant de décider de la façon de traiter les données transportées[1]. Dans ce qui suit nous allons définir les termes qui figurent dans l'organisme d'accueil.

1.2.1 Réseaux locaux LAN

Réseau local ou LAN (Local Area Network) est un réseau qu'est propre à une entreprise où ils partagent leur informations confidentiels, et spécifient les règles de partage. Les LAN se

distinguent (des MAN et des WAN) par leur taille, leur technologie de transmission, leur vitesse de transmission et leur topologie. Un LAN en général offre une bande passante de 4Mbits/s jusqu'à 100Mbits/s.[2]

1.2.1.1 Moyens de transmission

Les réseaux locaux emploient des supports à propagation guidée ou des supports à propagation libre. Les supports à propagation guidée utilisent des câbles. Le signal transmis peut être électrique ou optique. Les supports électriques utilisés par les réseaux locaux sont la paire torsadée et le câble coaxial. La fibre optique est utilisée pour acheminer les ondes lumineuses.[3]

1.2.2 Intranet

L'intranet est un réseau informatique interne utilisé au sein d'un organisme et utilisant les services et caractéristiques de l'internet[4]

1.2.3 Internet

L'interconnexion des réseaux permet de relier les différents réseaux qui facilitent le partage d'informations d'une manière fiable en utilisant des protocoles tel que les protocoles de routage et de contrôle. Internet permet d'atteindre plusieurs services dont on cite : le World Wide Web, le courrier électronique, la messagerie instantanée, la téléphonie sur IP ...[5]

1.2.4 Topologie du réseau

Un réseau est représenté par une topologie. Une topologie peut être vue de deux façons, physique qu'est la manière dont est câblé ce réseau et dépend de l'environnent et les besoins techniques, logique qu'est déterminée selon le parcoure de l'information entre les différents matériels[2].

1.3 Architecture réseau

Il existe deux types d'architecture réseaux : l'architecture client/serveur et l'architecture peer to peer ou poste à poste.

1.3.1 Client/serveur

L'architecture client/serveur s'articule en général autour d'un réseau. Deux types d'ordinateurs sont interconnectés au réseau. Le serveur assure la gestion des données partagées entre les

utilisateurs. Le client gère l'interface graphique de la station de travail personnelle d'un utilisateur[6]. Cette architecture, est réalisable sur une même machine en dégageant deux processus, un client et un serveur.

- **Fonctionnement :**
  Le modèle client/serveur, est un modèle d'architecture applicative où les programmes sont répartis entre processus clients et serveurs communiquants par des requêtes avec réponses. [6]
  Le client, envoie des requêtes au serveur, ce dernier les traite et revoie des réponses au client[6].
- **L'architecture client/serveur à deux niveaux**
  Elle caractérise les systèmes clients/serveurs pour lesquels le client demande une ressource et le serveur la lui fournit directement, en utilisant ses propres ressources[7].

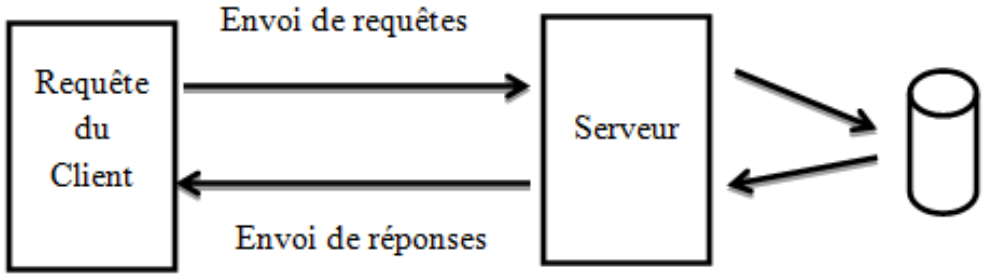


FIGURE 1.1 – Architecture à deux niveaux.

- **L'architecture client/serveur à trois niveaux**
  Dans cette architecture un niveau intermédiaire se fait place entre les deux niveaux de l'architecture précédente :
  - Le client (niveau 1) : demandeur de ressource.
  - Le serveur d'application (niveau 2) : est chargé de fournir la ressource mais qui fait appel à un autre serveur pour certaines demandes de ressources. Le niveau 2 lui-même est le client d'un serveur de base de données.
  - Le serveur de base de données (niveau3) : fournit les ressources au premier serveur [7].

1.3.2 Architecture Peer to Peer (poste à poste)

Cette architecture est en fait un réseau sans serveur constitué de deux ou plusieurs ordinateurs. Ainsi chaque ordinateur joue à la fois le rôle de serveur et de client, cela signifie que chacun des ordinateurs du réseau est libre de partager ses ressources [7].

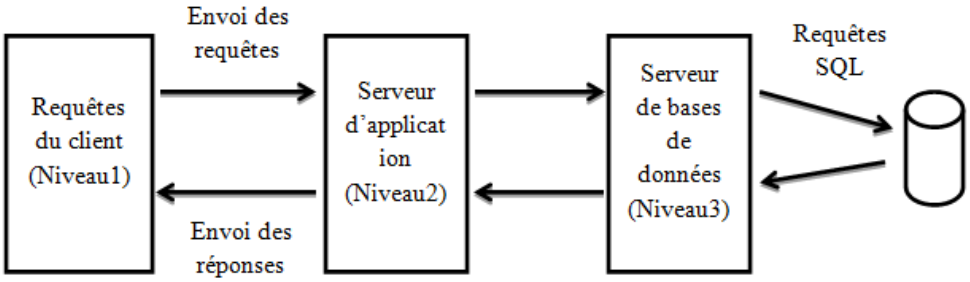


FIGURE 1.2 – Architecture à trois niveaux.

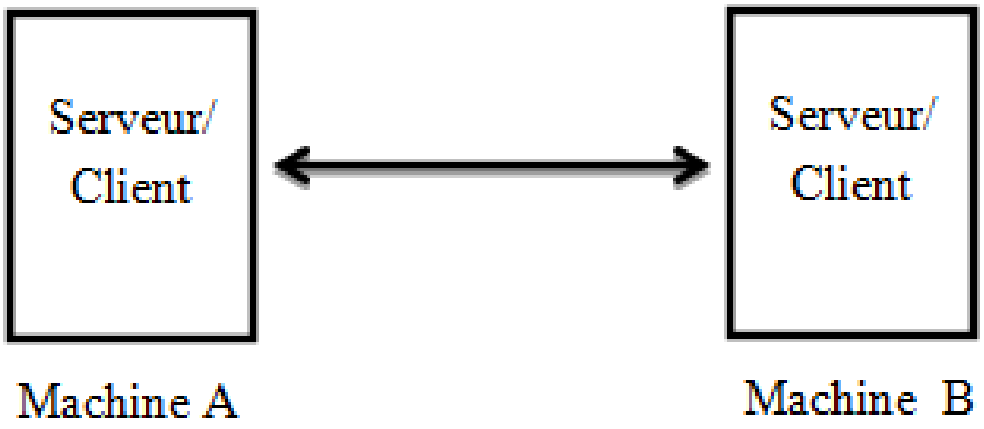


FIGURE 1.3 – Architecture poste à poste.

1.4 Les modèles de communication réseau

Les modèles de communication entre utilisateurs réseau les plus répondus sont : le modèle TCP/IP (Transmission Control Protocol / Internet Protocol), qui est un modèle de quatre couches et le modèle OSI (Open System Interconnection), qui est un modèle de sept couches. Les deux modèles OSI et TCP/IP sont présentés comme suit :

7	Application			Applications
6	Présentation		4	Services
5	Session			Internet
4	Transport		3	Transport (TCP)
3	Réseau		2	Internet (IP)
2	Liaison		1	Accès au réseau
1	Physique			

Notions

– *Transfert de bout en bout* : assurer le transfert de données utilisateur d'une extrémité à une autre par le service réseau (les couches 5, 6 et 7 du modèle OSI travaillent de bout

FIGURE 1.4 – Le modèle OSI et le modèle TCP/IP

en bout) [8].

- *Transfert de nœud à nœud* : le transfert des paquets d'une extrémité à une autre en passant par des nœuds intermédiaires (les couches 1, 2, 3 et 4 du modèle OSI travaillent de nœud à nœud) [8].
- *Encapsulation* : elle consiste à envelopper les données à chaque couche du modèle OSI [9].
- *Fragmentation* : en réseau la fragmentation est le découpage d'un paquet de données en plusieurs petits pour passer à travers un lieu plus faible MTU (Maximum Transmission Unit : la taille en octet de la plus grande trame (paquet), qui peut être transmise par l'interface sans fragmentation) [10,11].

1.5 Le routage

Le routage est le processus par lequel un élément (courrier, appels téléphoniques, paquets IP,...) va être acheminé d'un endroit à un autre [12]. Le routage définit le chemin emprunté par les paquets entre son point de départ et son point d'arrivée

1.5.1 Le routage dans le réseau

Le routage dans un réseau (*ou le routage IP*) est basé sur l'adresse du destinataire. Il se fait suivant deux opérations : la sélection de la meilleure voie et la commutation du paquet sur l'interface appropriée. Les informations de routage sont mémorisées dans la table de routage des équipements (routeurs)[12].

1.6 Les protocoles

Un protocole définit un ensemble de règles suivies par les équipements lors de l'échange d'informations dans un réseau. En informatique les protocoles sont associés aux services, à l'acheminement des données et à l'établissement d'une connexion entre les systèmes [13].

1.6.1 Protocoles de routage

Un protocole de routage est programme qui défini l'ensemble des chemins que peuvent empreinter les informations transférées dans un réseau depuis la station émettrice jusqu'à destination. Le résultat de cette opération est une table de routage dans la quelle sont stockées les informations relatives à la structure du réseau.

1.7 Les serveurs

Un serveur a comme rôle de rendre des services et répondre aux requêtes des clients. En d'autres termes, c'est un serveur de données ou d'informations. Dans les réseaux, les serveurs se communiquent entre eux . Il existe plusieurs types de serveurs, il y'a des serveurs racine qui ont comme fonction d'avoir toutes les informations qui circulent sur le réseau, ils nécessitent une sécurité solide et performante. Il existe d'autres, offrant des services internet, ceux-ci possèdent des numéros de ports propres à eux, citant à titre d'exemple :

1. Le port 21 (service ftp).
2. Le port 22 (service ssh).
3. Le port 23 (le service telnet).
4. Le port 25 (service smtp).
5. Le port 80 (service http).

Il existe d'autres serveurs qu'on appelle serveurs locaux, ils sauvegardent les informations internes à l'entreprise et offrent des services aux utilisateurs de cette dernière.

1.7.1 Serveur Messagerie

L'échange de messages et des fichiers peut être fait grace à un serveur de messagerie. Ce dernier nécessite :

- Un client de messagerie et un logiciel client MUA (Mail User Agent, ex. : Outlook) pour l'expéditeur et le destinataire.
- Un serveur de messagerie expéditeur et un logiciel pour le transfert MTA (Mail Transfert Agent, ex. : Sendmail).
- Un agent de messagerie destinataire intégrant une boite aux lettres (BAL) à chaque client, un MTA pour le transfert entre serveurs et un logiciel serveur pour la délivrance des messages MDA (Mail Delivery Agent, ex. : Sendmail).
- Des protocoles d'échange (SMTP, POP3, IMAP,...)[13]. Cette partie sera plus détaillée dans le chapitre trois.

1.7.1.1 Le routage des courriers

L'adresse d'un destinataire est constituée d'un nom d'utilisateur et d'un nom de domaine ; lorsqu'un courrier doit être délivré à un certain domaine, il est nécessaire de savoir quelle machine est capable de gérer l'arrivée du mail. Afin d'effectuer ce travail il faut faire appel au DNS. Les fichiers de configuration des serveurs DNS ont un enregistrement MX (Mail eXchanger) [11]. Les enregistrements MX désignent un hôte appelé échangeur de messages qui traite le courrier et le transmet [11].

1. Le traitement du courrier consiste à sa livraison à l'adresse indiquée.
2. La retransmission concerne son envoie vers sa destination finale ou vers un autre échangeur de messages proche de la destination.[11]

1.7.2 Serveur DNS (Domain Name Server)

DNS est le service de résolution de nom d'hôte, il permet d'adresser une machine par un nom plutôt que de l'adresser par une adresse IP. La structure d'un nom d'hôte est comme suit :

Nom de machine	Nom de machine

Notions

1. *Domaine* : le nom de domaine identifie une organisation dans l'internet. Un domaine est un sous arbre de l'espace de nommage. Un domaine peut être organisé en sous domaines, .univ.org est un sous domaine du domaine .org [10].
2. *Zone* : est une organisation logique (administrative) des domaines. Son rôle est de simplifier l'administration des domaines. Le domaine .com peut être découpé en plusieurs zones, z1.com, z2.com..etc [10].
3. *Délégation* : consiste à déléguer l'administration d'une zone ou une sous zone aux administrateurs de cette zone [10].

la résolution d'un nom de domaine est comme suit : le serveur primaire (c'est le serveur local avec lequel le client communique) transmet à un serveur distant ayant autorité sur le domaine de premier niveau ; le serveur choisi, qui a la connaissance complète des adresses des machines de sa zone relaie la requête vers le serveur DNS de deuxième niveau. La requête est ensuite relayée jusqu'à atteindre le serveur DNS ayant autorité sur la zone demandée [13].

La résolution s'établit en deux méthodes : résolution itérative et résolution récursive.

1. *La résolution récursive* : le serveur primaire contacte le serveur racine et c'est à ce dernier de contacter le serveur ayant autorité sur le domaine demandé, et remis à son tour la réponse au serveur racine qui la transmit au serveur primaire [13].

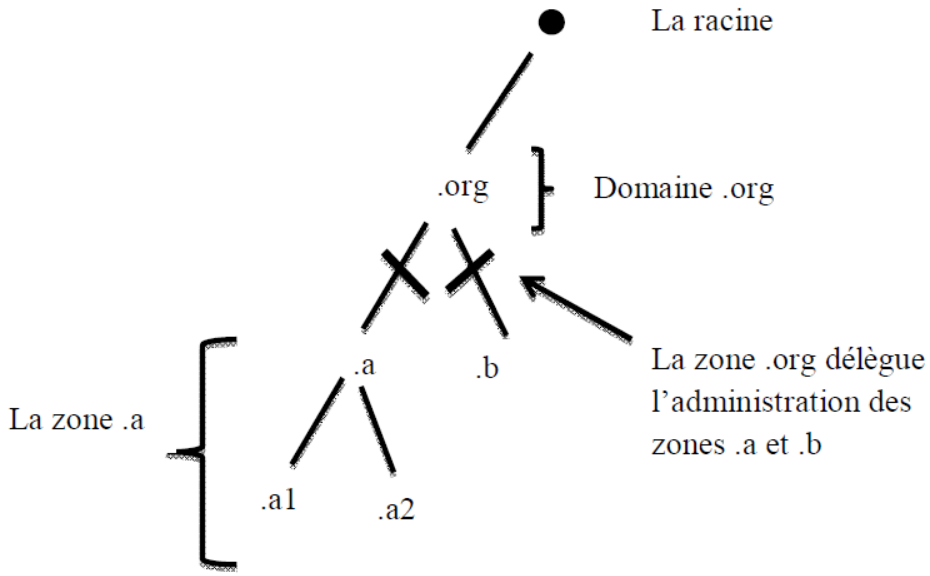


FIGURE 1.5 – Le domaine, la zone et la délégation

2. *La résolution itérative* : le serveur primaire contacte le serveur racine qui lui renvoie l'adresse du serveur du premier domaine auquel le serveur primaire renvoie la requête [13].

Remarque1 : si le nom recherché est local ou qu'il est déjà mémorisé dans la mémoire cache (liste des serveurs de noms de niveau supérieur) du serveur primaire dans ce cas la réponse est renvoyée directement au client [10,13].
Remarque2 : la résolution de noms s'établit inversement, c'est-à-dire qu'elle se fait de droite en gauche, soit l'ex. www.google.fr. , la résolution se fait comme suit [10] :

1. (.) (serveur racine).
2. .fr (serveur de domaine .fr).
3. google.fr (serveur de domaine google.fr).

Propriétés propres au DNS

– Numéro de port : 53.
– Type d'enregistrement : les principaux types d'enregistrement DNS sont :

1.8 Sécurité informatique

La sécurité est l'objectif principal de toutes les entreprises ; elles posent tout le temps des questions concernant la sécurité de leur système d'information. Dans le but de protéger leur réseau et de garder leurs informations en sécurité de tout intrus, il y'a des objectifs à assurer et des étapes à suivre.

OA (Start Of Authority)	Indique l'autorité sur la zone. Ces enregistrements contiennent toutes les informations sur le domaine
NS (Name Server)	Ces enregistrements donnent les adresses des serveurs de noms pour le domaine.
A (Adresse)	Ces enregistrements permettent de définir les nœuds fixes du réseau (ceux qui ont des adresses IP statiques)
MX (Mail eXchanger)	C'est un enregistrement qui sert pour déclarer les serveurs de messagerie. Chaque enregistrement MX possède une valeur de référence codé sur 16 bits. Cette valeur indique au routeur l'ordre de priorité à utiliser lors du choix d'un échangeur de messages.
CNAME (Canonical Name)	Il permet de définir des alias sur des nœuds existants
PTR (Pointeur)	Il permet la résolution de noms inverse dans le domaine in-addr.arpa

TABLE 1.1 – les principaux types d'enregistrement DNS

- **Les objectifs de la sécurité à assurer**
  1. La confidentialité : seuls les entités autorisées peuvent accéder à l'information. En autre terme, en cas de transmission de l'information, garantir qu'elle ne soit compréhensible que par les destinataires.
  2. L'intégrité : d'une part l'information ne peut être modifiée ou détruite, d'une autre part il faut assurer la non répudiation (en cas d'échange d'informations entre entités aucune d'elles ne peut nier cet échange) et l'authenticité (les informations reçues sont bien de la part des entités qu'elles prétendent être (source de confiance)).
  3. Disponibilité : assurer l'accessibilité des entités authentifiées du système d'information aux ressources de ce système [14].
- **Pour sécuriser l'information il faut sécuriser aussi [14] :**
  - Le matériel (là où elle se trouve).
  - Les applications (qui traitent l'information).
  - Les supports (moyen de son transport), de l'information.
- **Notions**[15]
  - *Cryptographie* : l'art et la science de garder le secret des messages elle est pratiquée par les cryptographes.
  - *Cryptanalyse* : consiste à trouver le message en clair sans connaitre les clés et l'algorithme de déchiffrement, en possédant un ou plusieurs chiffrés.

- *Chiffrement (Cryptage)* : la transformation d'un message de telle manière à le rendre incompréhensible.
- *Cryptage symétrique* : il est basé sur l'utilisation d'une clé privée partagée entre deux parties communicantes[13].
- *Cryptage asymétrique* : il utilise deux clé différentes pour chaque utilisateur, une est privée et n'est pas connue que de l'utilisateur qui a généré les clés ; l'autre est publique et peut être transmise sur internet[13].
- *Crypto système* : l'algorithme cryptographique, toutes les clés possibles et tous les protocoles qui le font fonctionner .
- *Sureté* : protection contre les actions non intentionnelles.
- *Menace* : évènement d'origine accidentel ou délibéré, capable s'il se réalise de causer un dommage à un système donné.
- *Vulnérabilité* : une faiblesse dans le système qui peut être exploité par une menace.
- *Risque* : association d'une menace à une vulnérabilité qui menace sa réalisation.
- *Signature* : le moyen de lier l'information à une entité.
- *Certificat* : il est délivré par une tiers partie de confiance qui est garantie par une signature, le certificat réalise l'association d'une clé publique à une entité afin d'assurer la validité[13].

Pour appliquer une bonne stratégie de sécurité pour un système d'information, le coté organisationnel et gérance des ressources de l'entreprise doivent etre pris en considération. En premier lieu les ressources humaines afin de minimiser les dépenses en terme protection[14].

1.8.1 Les attaque

Une attaque représente les moyens d'exploiter une vulnérabilité dans le système. Une attaque peut être :

1. *Passive* : l'intrus a une vision sur l'information, mais ne peut ni la changer ni la supprimer[14].
2. *Active* : dans ce type d'attaque l'intrus peut changer le message ou fabriquer un, il en existe trois types : interruption (l'intrus altère le message entre deux entités), modification (l'intrus modifie le message venant d'une entité et l'envoie en se faisant passé par cette dernière) et fabrication (l'intrus fabrique un message et l'envoie en se faisant passé par une entité de confiance)[14].

1.9 Sécuriser un LAN

La sécurité d'un réseau local nous oblige à connaitre les éléments suivant, qui sont d'une grande importance et qui participent à assurer le secret de l'information.

1.9.1 Le firewall

Le firewall ou le pare-feu est chargé de filtrer les accès entre le réseau local et le réseau externe[13].

1.9.2 Le NAT (NatworkAddress Translation)

Le NAT, ou translation d'adresse permet à une machine d'un réseau interne de se connecter à un réseau externe, internet. On distingue deux types de NAT, le NAT statique et le NAT dynamique[16].

1.9.3 Le DMZ(DeMilitarized Zone)

Une zone démilitarisée, est une zone de réseau privé. DMZ permet de regrouper des ressources nécessitant un niveau de protection intermédiaire. Comme un réseau privé, DMZ est isolé par un firewall[13].

1.9.4 Serveur Proxy

Le proxy est un autre moyen de sécurité, utilisé comme une passerelle entre le réseau privé et le réseau publique ; il est généralement utilisé dans les systèmes institutionnels ou d'entreprise. Le proxy a trois fonctions principales :

1. *Caching* : stocke les pages demandés par les clients et les redistribuées en cas de demande.
2. *Traking* : création des journaux de connexion où se trouvent les informations du client.
3. *Filtring* : filtrage des requêtes et réponses[16].

1.9.5 VPN (Virtual Private Network)

Le réseau privé virtuel est constitué d'un ensemble de LAN, reliés à travers un tunnel sécurisé dans lequel les données sont cryptées. Les postes distants faisant partie du même VPN communiquent d'une manière sécurisée, cette communication se fait virtuellement. Les informations circulent dans le tunnel en toute sécurité, cela est garce à des protocoles

de sécurité VPN : PPTP (Point to Point Tunneling Protocol), L2TP (Layer 2 Tunneling Protocol), IPSec et niveau supérieur on retrouve SSL/TLS et SSH[13]. Près de ces cinq éléments, on retrouve le serveur antivirus qui est responsable de l'analyse du courrier entrant et sortant ; en cas de virus ille signale.

1.10 Conclusion

Dans ce chapitre, nous avons pris en charge de présenter les différents termes qui sont en relation avec notre thème. Une brève définition sur les réseaux, les moyens de transmission dans un réseau, leur topologie, leurs architectures, leurs modèles de transmission ainsi que le routage et le routage du courrier électronique, qui est en relation avec notre thème sont illustrés.

Nous avons cité le rôle indispensable du serveur DNS, où nous avons mentionné ses différentes fonctions, ses types d'enregistrement et la résolution DNS, le problème majeur de la sécurité et comment sécuriser notre réseau interne. Enfin, nous avons illustré les principaux composants qui participent à la sécurité d'un réseau interne.

Ce chapitre, englobe toutes les généralités que aurons besoin. Dans le chapitre suivant, nous présenterons, Algérie Télécom, notre organisme d'accueil.

CHAPITRE 2

ORGANISME D'ACCEUIL

2.1 Introduction

Dans ce chapitre nous allons présenter notre organisme d'accueil : Algérie Télécom, son historique, ses ambition ainsi que son organisation. Nous nous intéresserons en particulier à la direction opérationnelle des télécommunicationsde Bejaia, à ses différents départements, services, applications, la gestion de son système d'information, leur méthode de sécurité ainsi que d'autres caractéristiques que nous citrons dans la suite de ce chapitre. Ces informations nous ont été attribuées par les différents services de la DOT(Direction Opérationnelle des Télécommunications) de Bejaia ; où nous avons fait un stage de quarante-cinq jours, dont une semaine à Data Centre et Djaweb d'Alger.

2.2 Présentation générale d'organisme d'accueil

Algérie Télécomale statut d'une entreprise publique économique, la naissance de cette entreprise a été consacrée par la loi 2000/03 du 5 août 2000. Elle est entrée officiellement en activité à partir du 1er janvier 2003. Elle a pour objectifs :

1. La rentabilité.
2. L'efficacité et la qualité de service.

Ses ambitions, sont, d'avoir un niveau élevé de performance technique, économique, et sociale pour se maintenir durablement leader dans son domaine, dans un environnement devenu concurrentiel. Son souciconsiste, à préserver et développer sa dimension internationale et participer à la promotion de la société de l'information en Algérie.

2.3 Organisation d'Algérie Télécom

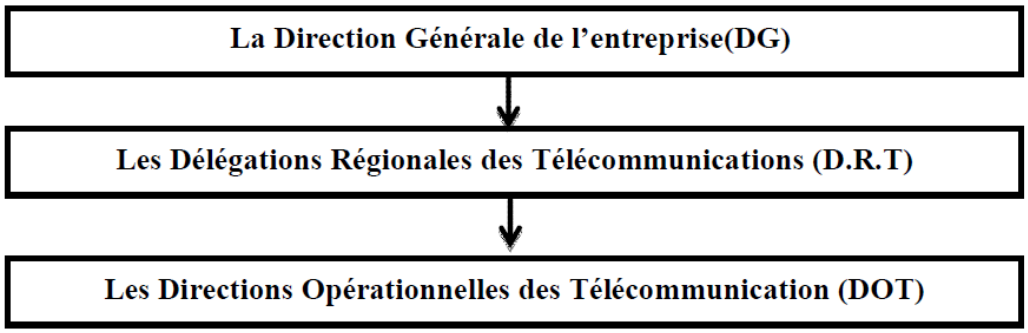


FIGURE 2.1 – Les niveaux organisationnels de l'entreprise

L'organisation générale d'Algérie Télécom s'articule autour de trois niveaux, comme le montre la figure précédente.

Niveau1 : **La Direction Générale de l'entreprise(DG)**
L'entreprise est organisée en structures centrales (opérationnelles et fonctionnelles) ou centres nationaux, elle est constituée de :

1. Cinq directions centrales.
2. Deux divisions centrales.
3. Trois directions projet et une structure de staff.

Niveau2 : **Les Délégations Régionales des Télécommunications (D.R.T)**
Elles sont Constituées de : Structures générales ou centres régionaux (Il existe huit D.R.T à travers le territoire national)

- Plusieurs D.O.T.
- Un staff composé de cinq sous directions (gestion commercial, gestion technique de réseaux et travaux neufs, sous directions réseaux d'entreprises, budget et comptabilité, gestion de personnel et la logistique).
- Une sous directions internationale de la D.R.T d'Alger.
- Une inspection régionale.

Niveau3 : **Les Directions Opérationnelles des Télécommunications (DOT)**
La Direction opérationnelle des Télécommunications est une entité opérationnelle dotée de l'autonomie budgétaire et financière. Elle gère les entités techniques et commerciales qui lui sont rattachées.

2.4 Directions Opérationnelles des Télécommunication (DOT) de Bejaia

La Direction Opérationnelle des Télécom de Bejaia est placée sous l'autorité directe de la DRT de Sétif, son siège se situe au chef-lieu de wilaya de Bejaia, dirigé par un Directeur. Le Directeur de la D.O.T est assisté pour le management des ACTEL, CPT et centres des télécommunications. La D.O.T de Bejaia est composéede, quatre départements assurant des services, des cellules et des services extérieurs. Le diagramme suivant,illustre ces différents composants.

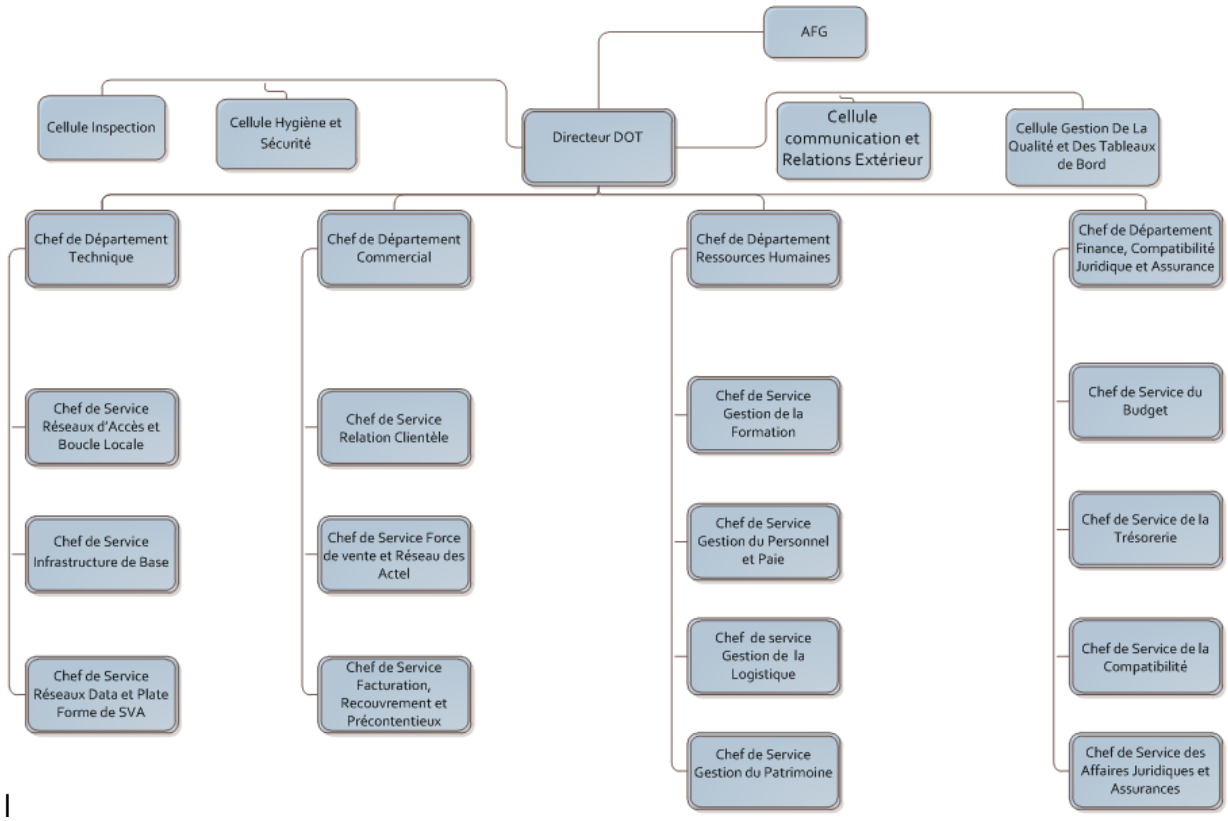


FIGURE 2.2 – Organigramme DOT Bejaia

1. **Département technique**
   - Service réseaux d'accès et boucle locale.
   - Service infrastructure de base.
   - Service réseaux DATA et plateforme de SVA.
2. **Le Département Commercial**
   - Service relation clientèle.
   - Service force de vente et réseaux des ACTEL.
3. **Département ressources humaines et moyens**

   - Service gestion de la formation.
   - Service gestion du personnels et paie.
   - Service de gestion du patrimoine.
4. **Département finance, comptabilité, juridique et assurances**
   - Service du budget.
   - Service de la comptabilité.
   - Services des affaires juridiques et assurances.

- **Les cellulesde la D.O.T**
  - Cellule hygiène et sécurité.
  - Cellule communication et relations extérieures.
  - Cellule gestion de la qualité et des tableaux de bords.
- **Les services extérieurs de la D.O.T**
  - Centre d'amplification(CA).
  - Centre de Commutation Locale et de Transit(CCLT).
  - Centre d'Entretien et de Construction des Lignes(CECLI).
  - Agence Commerciale des Télécommunications(ACTEL).

2.5 Les applications et matériaux utilisés à la D.O.T de Bejaia

1. HR ACCESS : c'est un logiciel destiné pour la gestiondes ressources humaines et le suivi du personnel, à savoir les paies, les absences, les maladies,...
2. GAIA : c'est le système d'informations d'Algérie Télécom, il a pour taches :
   - La gestion des parcs téléphoniques.
   - La résiliation.
   - La suppression.
   - Les factures.
3. Oracle finance.
4. Système de supervision : qui se trouve au centre d'amplification, pour la gestion des ADSL.
5. Beling ADSL
6. Application ADSL : qui sont accessibles via GAIA.

Concernant le matériel on y trouve :

Equipements	**Marque**
Switch	NETGEAR 24 port 1GBPS avec modules Fibre optique
– Serveur AD + DNS + Messagerie. – Serveur de fichier. – Serveur BDD SQL 2000. – Serveur Kespersky. – Serveur BDD SQL 7.0. – Windows 2003 server. – SQL 2003 server.	– Pentium 4 – PC dual core 1.8 – Pentium 4 – Pentium 4 – Pentium 4 – Pentium 4
PC utilisateur	– AMD Athlon 500 mhz – PC dual core 1.8 – PC P4 3.06 GHZ
Câble et moyens de transmission	– RJ 45 catégorie 6 – RJ 45 catégorie 5 – RJ 11 – G703 (Mic de 2M) – Fibre Optique – Paire torsadé – Ondes hertziennes
– Armoire de brassage équipé de tiroir Optique 19Unités. – Armoire de brassage équipé de tiroir Optique24 Unités. – Armoire de brassage équipé de tiroir Optique 09 Unités.	

Imprimantes	CANON LBP-1120c
Scanner	Photo Epson perfection 1670
Pare-feu	Fortigate 80C
Modem Wi Max	D-LINK et Djaweb
Des serveurs (au niveau du WLL)	
Des MSAN	
Des multiplexeurs et démultiplexeurs	

Topologie

La topologie réseau utilisé au sein de l'entreprise, est la topologie en Etoile.

Communication

Coté communication Algérie télécom a opté pour le protocole X25. L'utilisation d'un réseau opérateur.

Sécurité

Pour la sécurité ils utilisent le système en boucle etle RMS (Réseau multimédia et sécurité). Algérie Télécom possède un intranet, où circulent leurs informations.

Authentification

Algérie Télécom, utilise les adresses IP pour l'authentification. Par exemple, si on prend la D.O.T de Bejaia, qui est une D.O.T de la D.R.T de Sétif, leurs adresses sont sous la forme :

Partie réseau	Code wilaya de Sétif	Code wilaya de Bejaia	Chiffres
10	19	06	x

Remarque :

1. La configuration des matériaux se fait au niveau de Sétif et même pour leur système d'information.
2. La plage d'adressage de LAN de la D.O.T de Bejaia est attribuée par la D.R.T de Sétif.
3. La D.R.T de Sétif s'occupe de l'installation des nouveaux matériaux, de leur configuration et assure que la D.O.T de Bejaia s'intègre à la nouvelle technologie.

2.6 Cahier de charge

Présentation du sujet

Avec les nombreuses informations, fichiers, documents à échanger entre le personnel de la DOT et ses services extérieur, cette dernière souhaite faciliter cet échange. C'est dans ce cadre, que nous souhaitons améliorer leurs système d'échange, en leurs installant un serveur de messagerie.

Problématique

Lors de notre passage dans la DOT de Bejaia, certain problèmes ont été soulevé :

- Fusion des messages reçues/envoyer au niveau national et locale.
- Pour l'échange d'informations, ils utilisent le fax, ce qui est une perte de temps.
- La procédure d'obtention d'une adresse électronique est très lente.
- Dans le cas de perte de mot de passe ou d'inactivation du compte messagerie, on est obligé d'écrire une autre demande.

Suggestion

Afin de résoudre les problèmes soulevés ci-dessus, nous proposons les solutions suivantes :

- Mise d'un serveur de messagerieavec l'interface SquirrelMail, qui sera propre à la DOT de Bejaia pour une gestion meilleure.
- Création, d'une boite électronique commune, qui sera utilisée par les abonnées dans le cas où leur propre boite est inactive ou avoir un nouveau compte utilisateur.
- Sécuriser le serveur, par les deux protocoles SSL et SSH.
- Faciliter l'administration du serveur messagerie.

Objectifs

- Rédaction et envoi très rapide pour un ou plusieurs destinataires à la fois.
- Le message électronique peut être archivé et imprimé.
- Le courrier électronique est peu couteux.
- Permettre à l'administrateur de :
  - Créer, détruire des comptes utilisateurs (boîtes aux lettres).
  - Créer, modifier des listes de diffusion (ensembles de destinataires réunis sous une même dénomination).
  - Démarrer / Stopper un Service (Service SMTP ou POP).
- Permettre à l'utilisateur de :
  - Rédiger et expédier un message et consulter les messages qui lui sont destiné.
  - Classer les messages dans des dossiers.
  - Répondre à un message sans avoir à retaper l'entête.
  - Utiliser des fonctions de recherche (retrouver les messages répondant à des critères spécifiques, tel que : la date, le nom de l'expéditeur, le sujet).
  - Créer un annuaire personnel.

2.7 Conclusion

Dans ce chapitre nous avons présenté l'organisme d'accueil, où nous avons élaboré ses différents services et spécifié leur besoins dans le cahier de charge ; ce qui engendre la nécessité de mettre en œuvre un serveur de messagerie électronique dont les caractéristiques seront développées dans le chapitre qui suit.

CHAPITRE 3

SYSTÉME DE MESSAGERIE ET SA SÉCURITÉ

3.1 Introduction

Dans le chapitre précédent, nous avons présenté l'organisme d'accueil, où nous avons traité la problématique, concernant la messagerie. Dans ce qui suit, nous nous consacrerons sur les éléments à apporter et ce qu'il faut connaitre, afin d'installer et mettre en uvre un serveur de messagerie.

3.2 Serveur de messagerie

Un serveur de messagerie a pour vocation de recevoir et d'envoyer le courrier électronique à travers le réseau. Un utilisateur n'est jamais en contact direct avec ce serveur, il utilise soit logiciels de messagerie, soit un webmail, qui se charge de contacter le serveur pour envoyer ou recevoir les messages via l'internet.

3.3 L'adresse électronique

L'adresse électronique est un service permettant à des utilisateurs d'échanger des messages via un réseau informatique. En ce sens, elle doit permettre d'identifier une boite aux lettres de façon unique. Habituellement, cette adresse comprend trois composantes : la première partie identifie le destinataire, puis le signe "@", et une partie qui identifie le nom de domaine auquel le message est envoyé. Ces adresses prennent toujours la forme suivante : identifiant@nom_de_domaine.

– **Les adresses nominatives** : l'adresse électronique peut être par exemple "prénom.nom@algerietelecome.dz" . On appelle cette adresse, l'adresse nominative ou per-

sonnelle.

- **Les adresses fonctionnelles** : pour une administration plus facile à gérer, de préférable opter les adresses fonctionnelles ex.chef-departement@algerietelecome.dz.
- **Les alias** : à côté de ces adresses électroniques, il existe des " alias ". Un alias est un nom de substitution qui peut être associé à une ou plusieurs boîtes aux lettres. Les alias sont utiles lorsqu'on s'adresse régulièrement à un correspondant dont l'adresse électronique est longue ou bien à un groupe d'individu.

Procédure d'attribution d'une adresse électronique

Pour avoir un compte, l'utilisateur se trouve dans l'obligation de rédiger une demande et l'envoyé à l'administrateur, ce dernier lui attribue un, plus un mot de passe qui pourra modifier.

3.4 Les règles d'écriture à suivre dans la formulation d'une adresse électronique

Qu'il s'agisse d'adresses fonctionnelles ou nominatives, ou d'alias, le choix du libellé doit répondre à un besoin de :

- **Lisibilité** : par lisibilité, on entend la bonne compréhension de l'adresse e-mail. Pour cela l'adresse ne doit pas s'inspirer d'abréviations utilisées à l'intérieure de l'organisme, ni faire référence à une terminologie vague.
- **Homogénéité** : le choix du terme identifiant un service doit s'inscrire dans une logique organisationnelle précise.
- **Réglementation** : Attribuer les adresses selon la nécessité et le besoin d'utilisation pour le bon usage des adresses.

3.5 Le message électronique

La structure d'un message est composée de, corps du message et données d'administration. Les données d'administration peuvent être partagées en deux catégories, enveloppe et en-tête du message.

3.5.1 Les champs des en-têtes

1. From : contient l'adresse mail de l'expéditeur.
2. To : une partie de l'en-tête qui contient les adresses de tous les destinataires.

3. CC (Carbon Copies) : détermine la liste des destinataires qui recevront une copie du message.
4. Subject : permet de décrire l'objet du sujet (c'est un champ qu'on trouve dans tous les messages).
5. Date : se trouve la date d'envoi.
6. Replay-To : pour spécifier l'adresse à laquelle les réponses doivent être expédiées.
7. Message-ID : une valeur qu'est générée par le programme du transport du système du départ permettant d'identifier le message de manière univoque.
8. Received : ce champ permet de retracer le chemin emprunté par le message, car, tous les hôtes par lesquels le message transite ajoute ce champ à l'en-tête ; sur ce dernier on trouve les caractères suivants : l'identifiant du site, un identificateur du message, le moment de la réception du message, le site su provenance du message ainsi que le nom du logiciel du transport utilisé.

3.6 Stockage et archivage des messages

L'archivage consiste à maintenir dans le temps un document en état, et ainsi à le préserver contre toute altération, modification ou destruction. L'archivage remplit trois fonctions principales qui justifient son utilisation, à savoir : la preuve, la mémorisation et la compréhension. Pour l'organisation de l'archivage la norme ISO 15489-1 définit les étapes suivantes [18] :

1. Sélection des documents à archiver
2. Définition des durées de conservation
3. Intégration des documents au système d'archivage
4. Plan de classement des activités
5. Stockage et conditionnement sur des supports
6. définition des droits d'accès
7. Traçabilité
8. destruction physique ou versement à un service d'archives historiques.
9. Rédaction d'une Charte d'archivage
10. contrôle régulier de conformité à la norme.
11. Formation.

3.7 Les moyens d'envoyer un courrier électronique

a) **Le logiciel de messagerie** est un logiciel installé sur l'ordinateur de l'utilisateur qui permet d'envoyer et de recevoir des messages. Les logiciels de messagerie les plus connus sont " Outlook Express " et " Eudora ", ... Ils sont appelés " Mail User Agent " (MUA) ou " Agents de messagerie. Tel un facteur, ce logiciel va se charger d'aller relever, sur le serveur, le courrier électronique arrivé dans la boîte aux lettres de l'utilisateur.

b) **Webmail** : est un client de messagerie utilisant une interface Web au lieu d'utiliser un logiciel de messagerie.L'avantage est que pour utiliser le webmail, un navigateur suffit. Il n'est donc pas besoin d'avoir un logiciel de messagerie installer sur son ordinateur, donc moins de pannes. Les Webmail les plus connus sont :

- ***IBM Lotus Domino***

  IBM Notes/LotusDomino est la plate-forme de travail collaboratif propriétaire d'IBM, destinée explicitement à faciliter la coordination entre membres d'un groupe de travail fermé ou ouvert avec comme points forts : la facilité et rapidité de développement, la réplication et la sécurité. Lotus Notes représente le client lourd d'IBM pour cette plate-forme tandis que Domino représente le serveur. Cet outil comporte une gestion de messagerie, un annuaire intégré, un agenda collectif, un gestionnaire de documents organisé en base (base documentaire). La structure de ces bases de données non relationnelles et les événements interactifs qui lui sont associés sont programmables en langage LotusScript, en langage de formules Lotus, en JavaScript ou enJava. IBM Notes/Lotus Domino est le serveur de messagerie utilisé au niveau de la direction générale d'Algérie télécom.

- ***Microsoft Exchange Server***

  Exchange server est le serveur de messagerie crée par Microsoft, sa première apparition était en 1996 sous le nom Exchanger 4.0, et le dernier est Exchange Server 2013. Conçu pour rivaliser le produit de IBM, Lotus Domino, Exchange Server, est le serveur de messagerie le plus utilisé dans les entreprises professionnelles.

- ***RoundCube***

  RoundCube est le projet le plus récent et dont l'objectif est de réaliser un Webmail utilisant les technologies XHTML et CSS 2 pour offrir a l'utilisateur une ergonomie la plus proche possible de celle d'un logiciel de messagerie classique installé sur son PC. RoundCube est un webmail gratuit et open source, facile à installer et à configurer. Il comprend d'autres bibliothèques open-source sophistiqués tels que PEAR, une bibliothèque IMAP dérivé de IlohaMail l'éditeur de texte riche

TinyMCE, bibliothèque Googiespell pour laé correction orthographique ou le désinfectant WasHTML par Frédéric Motte.

- ***Zimbra***
  Zimbra est un logiciel serveur collaboratif qui permet à ses utilisateurs de stocker, organiser et partager rendez-vous, contacts, courriels, liens, documents et plus. Il logiciel développé sur un mode "Web service" : Son interface entièrement en AJAX est chargée à la première connexion, puis les interactions et ajouts/modifications d'informations sont envoyés auserveur par le protocole SOAP. Zimbra propose aussi un logiciel client utilisable en mode déconnecté : le Yahoo ! Zimbra Desktop (YZD).

  En dernier nous parlons du webmail que nous avions choisi comme client pour notre système de messagerie

- ***Squirrelmail***
  Le projet squirrelmail a été lancé en 1999 par deux frères : Luke et Nathan Ehresman. L'objectif de ce projet est de mettre à disposition un Webmail simple et léger pour le serveur et ne demandant pas de bibliothèque de codes additionnelles. WebmailSquirrelMail a été traduit en plus de 50 langues, dont l'arabe, le chinois, le français, l'allemand et l'espagnol. SquirrelMail a été mis en uvre le système de messagerie officielle du Bureau du Premier Ministre de la République de l'Inde pour ses avantages de sécurité sur Microsoft Outlook Express, ainsi que d'autres universités, comme Carnegie Mellon University, Université de Californie, Berkeley...

  Squirrelmail est un MUA, écrit en PHP, il assure une grande compatibilité avec de nombreux navigateurs.SquirrelMail est un projet Open Source qui offre à la fois une application de messagerie basé sur le Web et un serveur proxy IMAP. Il peut être installé sur presque tous les serveurs Web aussi longtemps que PHP est présent et que le serveur web a accès à un serveur IMAP et SMTP.
  Squirrelmail est un produit stable, facile à installer et à administrer. Sa fonction principale est d'accéder aux mails fournis par un serveur IMAP, il propose également un grand nombre de modules supplémentaires qu'on appelle plug-in (un plug-in ou greffon, est un ensemble de composants logiciels qui ajoute des capacités spécifiques à une application, lui permettant ainsi de personnaliser ses fonctionnalités qui permettent d'enrichir les fonctionnalités de base. 224 modules sont proposés au total, parmi lesquels on peut trouver :
  – Calendrier partagé.

- Carnet d'adresses.
- Gestion des réponses automatiques (vacation).
- Gestion des spams.

SquirrelMail est disponible pour toute plate-forme supportant PHP. Plates-formes les plus couramment utilisés sont Linux, FreeBSD, Mac OS X et les variantes de serveur de Microsoft Windows.
Pour le transfert, l'envoie et la récupération du courrier électronique il existe des protocoles qui les permettent.

3.8 Les protocoles de messagerie

1. ***SMTP*** (Simple Mail Transfer Protocol) : ce protocole est responsable de transférer le courrier électronique.
2. ***POP***(Post Office Protocol, Protocole de bureau de poste) : ce protocole est responsable de la récupération du courrier électronique à partir du MDA.L'inconvénient de ce protocole est qu'il n'est pas sécurisé ; les messages sont stockés en clair sur le serveur de courrier.
3. ***IMAP*** (Interactive Mail Access Protocol) : c'est un protocole plus récent, une alternatif au protocole POP. Il est plus puissant et plus complexe. IMAP est un protocole de récupération du courrier électronique.Il permet la gestion des mails sur le serveur même, en linge car les mails restent sur le serveur et sont manipulés à distance par le client de messagerie. Cela permet
   - La lecture des objets des messages seulement (sans le corps).
   - La lecture des messages en les laissant sur le serveur.
   - La suppression des messages sans les avoir lus.
   - Marquer les messages sur le serveur (non lus, récent).
   - Création de dossier sur le serveur.
   - Déplacement du message sur le serveur d'un dossier à un autre.

3.9 Principe de livraison des mails par le protocole SMTP

Avant d'expliquer le principe de livraison, il y a des éléments qu'il faut connaitre :

1. MUA ou UA (Mail User Agent) : est le programme utilisé par le client pour composer, envoyer et recevoir les messages.

2. MTA (Mail Transfert Agent) : est l'agent responsable de transfert des messages et pour cela il utilise le protocole de transfert SMTP.
3. MDA (Mail Delivred Agent) : l'agent de remise de message reçoit tous les messages entrant de MTA et les place dans la boite aux lettres des utilisateurs appropriés.

Un mail utilise des programmes tel que, Outlook ouThunderbird, ces programmes sont appelés des MUA (Mail User Agent). Lorsque un serveur expédié un mail en utilisant l'interface d'un MUA, le message est transmis à un MTA qu'est chargé de l'expédition. MTA est responsable de l'acheminement des mails locaux et distants.
Les MTA peuvent traiter des alias ainsi que faire suivre un message à un destinataire, ou sa retransmission (le forwarding). Si le destinataire existe, l'e-mail est transféré au MDA dans l'attente que son destinataire vienne le récupérer. La récupération est assurée par le MUA ; si non, le MTA retourne un message d'erreur.

Remarque :

Si le message est adressé à un utilisateur dont la boîte aux lettres réside sur le serveur local, le message est transmis à l'agent de remise des messages (MDA). Si le message est adressé à un utilisateur ne se situant pas sur le serveur local, l'agent de transfert des messages l'achemine vers l'agent de transfert des messages du serveur approprié.

3.10 Exemples de serveur de messagerie

Serveur de messagerie	Description	Avantages	Inconvénients
Sendmail	Sendmail est un serveur de messagerie dont le code source est ouvert. Descendant du logiciel ARPANETDelivermail.	Sendmail est très puissant et résiste à la grande charge. Une très bonne sécurité.	Sendmail est très critiqué car il est lent, difficile à configurer à cause de son architecture, elle est vieille et sa maintenance est difficile en la comparant avec d'autres (MTA) tels que,Qmail et Postfix.
Qmail	serveurs messagerie les plus performant, les plus surs et les plus stables, probablement supérieur à postfix dans le cas de traitement de très gros flux de messages	Qmail présente un haut niveau de sécurité grâce à sa structure " éclatée " et de très bonnes performances grâce à une gestion de queue très rapide.	c'est un outil plutôt difficile à installer et à maîtriser
Postfix(Le serveur que nous avons choisi)	Postfix est un MTA avec codes sources libres.Postfix est écrit dans l'idée de remplacer sendmail. Il est composé d'une dizaine de processus assurant chacun une tâche et communiquant entre eux par socket ou queues.	Il est adapter pour des gros besoins, facile à installer et à configurer, sa maintenance est aisée, il permet d'éviter de nombreux spams sans devoir scanner les contenus de message et il est multi plate-forme de type UNIX (MAC OS, GNU/LINUX).	

Architecture de Postfix

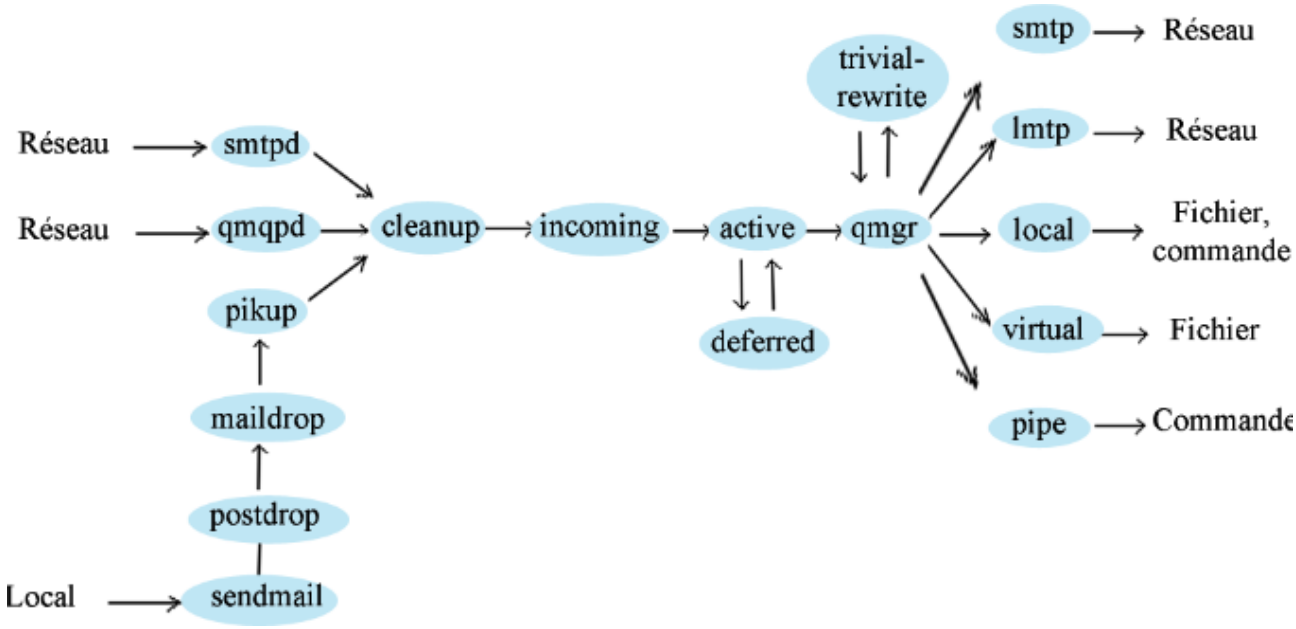


FIGURE 3.1 – Architecture Postfix

•Processus d'envoi des messages

1. **Dans le cas où le Message est posté localement**
   Le message local reçu par le programme postfix "sendmail " est déposer dans la file d'attente "maildrop " par la commande privilégiée "postdrop". Le message est après retirer par le service " pickup", il effectue des contrôles dans le but de protéger le reste du système Postfix et le passe au service " cleanup".

2. **Dans le cas où le message vient du réseau**
   Le serveur " smtpd" ou " qmqpd" reçoit le message, retire les enveloppes protocolaires, effectue quelques contrôles de sécurité pour protéger Postfix et donnent l'expéditeur, les destinataires et le contenu du message au service " cleanup".

•Processus de traitement des messages

1. **Le message n'est pas livrable**
   Un e-mail est généré automatiquement par le serveur " bounds" dans le but de renvoyer ce message à son expéditeur, également dans le but de prévenir le responsable de la messagerie en cas de problème.

2. **Le message est livrable**
   " cleanup " implémente le dernier traitement du message. Il ajoute le champ "

From : " manquant et d'autres en-têtes dans le message et arranges les adresses dans le format " user@fully.qualified.domain " puis insère le résultat dans un fichier dans la file " incoming " et notifie le "gestionnaire de file d'attente " qmgr " l'arrivée d'un nouveau message. Le daemon " trivial-rewrite " réécrit les adresses dans le format standard "utilisateur@domaine.qualifié".

•**Processus de livraison des messages** L'étape de livraison commence à l'arrivé d'un message à " incoming". Le gestionnaire de files maintient deux files d'attente :

- '***deferred***' : séparée, pour les messages qui n'ont pas pu être livré.
- '***active***' : aussi petite que possible avec juste quelques messages prêts pour la livraison.

Les messages sortant de " deferred ", passent au gestionnaire des files d'attente " qmgr", les dépile et les remet à un agent de livraison "smtp", "lmtp", "local", " virtual ", "pipe " en fonction de l'adresse de destination. " trivial-rewrite " résout chaque adresse de destination en distinguant entre les destinations locales où distantes. Des informations de routage additionnelles peuvent être spécifiées dans la table " transport ". Il interroge éventuellement la table " relocated " pour connaître les destinataires dont l'adresse a changé ; le courrier de ces destinataires est retourné à l'expéditeur avec une explication.

3.11 Les risques d'un serveur de messagerie

Un serveur de messagerie pourrait avoir des risques menaçant sa sécurité, parmi ces risques on cite :

- Perte de messages : ex. résister à la charge à des attaques en déni de service qui conduiraient à des pertes de messages.
- Indisponibilité du serveur de messagerie : Si le serveur de messagerie est la cible d'attaques en déni de service, il peut être indisponible pendant une longue durée.
- Possibilité d'une attaque interne.

3.12 Sécurité de la messagerie

Comme le protocole SMTP n'est pas sécurisé, alors les hackers profitent de cette faiblesse afin de pénétrer dans le réseau interne d'une entreprise. Parmi les attaques d'un hacker, on nomme :

Afin de remédier aux risques de la messagerie, il faut prendre certaines précautions. Le protocole responsable du transfert du courrier électronique SMTP, transmet les messages en claire sans les chiffrés, ce qui engendre un problème de sécurité, pour cela il faut sécuriser notre serveur de messagerie. Les mécanismes de sécurité qu'il faut suivre sont :

▷Identifier les deux flux à sécuriser sur le serveur ; le flux de transfert qui utilise SMTP et le flux de récupération des courriers qui utilise POP3 ou IMAP.

Le protocole SMTP dispose d'une extension STARTTLS définie par la RFC 2487. Cette extension permet :

- l'authentification forte des serveurs SMTP (via un certificat),
- l'établissement d'une session TLS (chiffrée) entre 2 serveurs (MTA-MTA),
- l'authentification forte des clients SMTP (via un certificat),
- l'établissement d'une session TLS (chiffrée) entre le client et le serveur (UA-MTA),

Les protocoles POP3 et IMAP, ont l'inconvénient de transmetre l'authentification (username/password) en claire. La RFC 2595 répond à ce problème en introduisant l'extension STARTTLS (STLS est son nom pour POP3). Tout comme pour SMTP, cette commande permet de passer en mode TLS une fois la connexion établie. Elle permet également, comme pour SMTP, d'authentifier de façon forte le client et de remplacer le couple username/password par un certificat client.

Cette sécurité est au niveau du serveur, il faut également sécuriser le coté client.
▷La sécurité coté clients repose sur l'usage du protocole S/MIME. Ce protocole permet de signer et de chiffrer le contenu des courriers électroniques.

3.13 Les protocoles de sécurité

3.13.1 Le protocole SSL (Secure Socket Layer)

SSL a été développé par Netscape pour offrir un accès sécurisé à des serveurs web, et il permet de sécuriser n'importe quel service basé sur TCP (https, pop3s, telnets, ftps, esmatp,...). Les propriétés de SSL peuvent être résumées comme suit :

- Confidentialité via le chiffrement (symétrique et asymétrique).
- Intégrité via des fonctions de hachage MAC.
- Authentification via des certificats X.509 (serveur et client).
- Rapidité via des clés symétriques de sessions.
- Interopérabilité via la négociation des algorithmes de chiffrement et des fonctions de hachage.

3.13.1.1 Architecture SSL

SSL a été conçu pour fournir une utilisation de service de bout en bout, à base du protocole TCP sécurisé. SSL est la combinaison de deux couches protocolaire :

- SSL Record Protocol : cette couche fournie les mécanismes de sécurité de base pour la couche supérieure.

SSL handshake Protocol	SSL change CipherSpec Protocol	SSL Alert Protocol	http
SSL Record Protocol			
TCP			
IP			

TABLE 3.1 – Architecture SSL

- SSL Handshake Protocol : permet l'authentification des entités impliquées par e protocole et la négocation des paramètres de chiffrement.
- SSL Record Protocol : met en uvre les paramètres de chiffrement négociés, ainsi que la fragmentation des données et leur compression.
- SSL Change CipherSpec Protocol : signale à la couche SSL Record Protocol tout changement dans la spécification des paramètres de sécurité.
- SSL Alert Protocol : signale à l'application, les erreurs rencontrées lors de vérification des messages, les problèmes de compatibilité entre les systèmes cryptographiques qui peuvent survenir lors de Handshake.

3.13.2 Le protocole SSH (Secure SHell)

SSH est un protocole qui assure la sécurité de communication au sein d'un réseau, il est conçu pour être simple d'implémentation et pas couteux. Au début il se destinait à assurer un login distant, et remplacer telnet. SSH offre des possibilités client/serveur, pour les services réseau et peut être utilisé pour le transfert des fichiers ou des mails.

3.14 conclusion

Le chapitre trois, comprend les principaux facteurs de la messagerie électronique ; par lequel, on conclut les éléments nécessaires à installer, afin de mettre en œuvre notre serveur de messagerie. Ce chapitre, est un amont pour le chapitre suivant qui consiste à mettre en pratique notre système de messagerie.

CHAPITRE 4

RÉALISATION ET ADMINISTRATION

Dans les chapitres précédents, nous avons parlé de notre projet d'une façon théorique. Ce chapitre est la partie pratique de la réalisation de notre objectif. Dans ce qui suit nous citerons, d'une manière explicite les étapes, d'installation et configuration de notre système de messagerie..etc.

4.1 Installation et configuration des composants de la messagerie

Les étapes suivantes, expliquent les différents éléments à installer afin de mettre en uvre notre système de messagerie.

1. Installation et configuration d'un serveur DNS.
2. Installation et configuration de lamp-server.
3. Installation et configuration du serveur messageriepostfix (MTA).
4. Installation et configuration du dovecot pop et du dovecotimap (MDA).
5. Installation et configuration du webmail Squirrelmail (MUA).

Remarque : dans ce qui suit nous travaillerons en super utilisateur (en mode root), pour cela il faut taper la commande suivante :

```
sudo su
```

Première étape : installation et configuration d'un serveur DNS primaire (secondaire). Pour le serveur DNS, nous avons choisi d'installer " *bind9* " :

```
root@meriem-Satellite-L350: ♯ifconfig wlan0:0 192.168.56.1 up
```

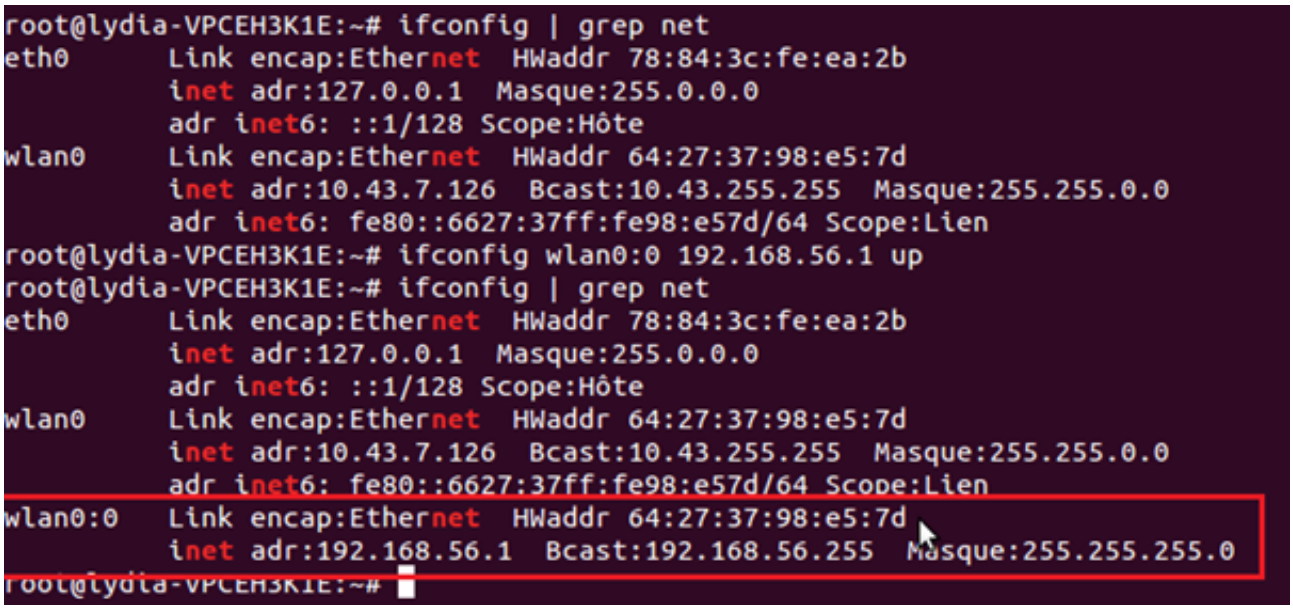


FIGURE 4.1 – Ajout du wlan 192.168.56.1

Pour le serveur DNS, nous avons choisi d'installer " bind9 " :

`root@meriem-Satellite-L350: ♯apt-get install bind9 dnsutils`

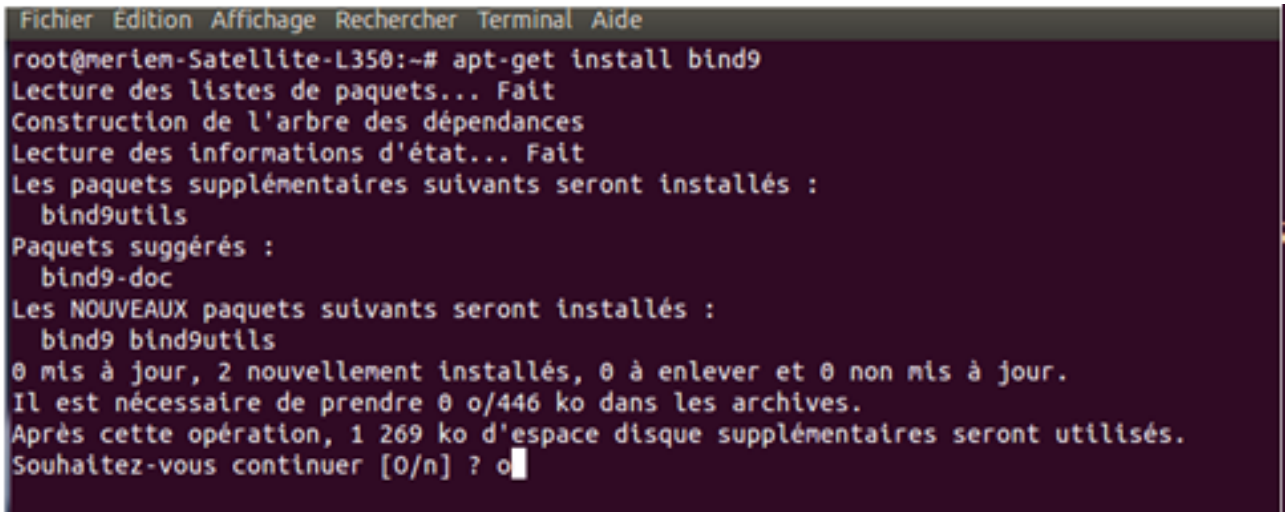


FIGURE 4.2 – Confirmation de continuer installation de bind9

Après avoir confirmé l'installation de notre serveur, on aura le résultat suivant (figure 4.4) :

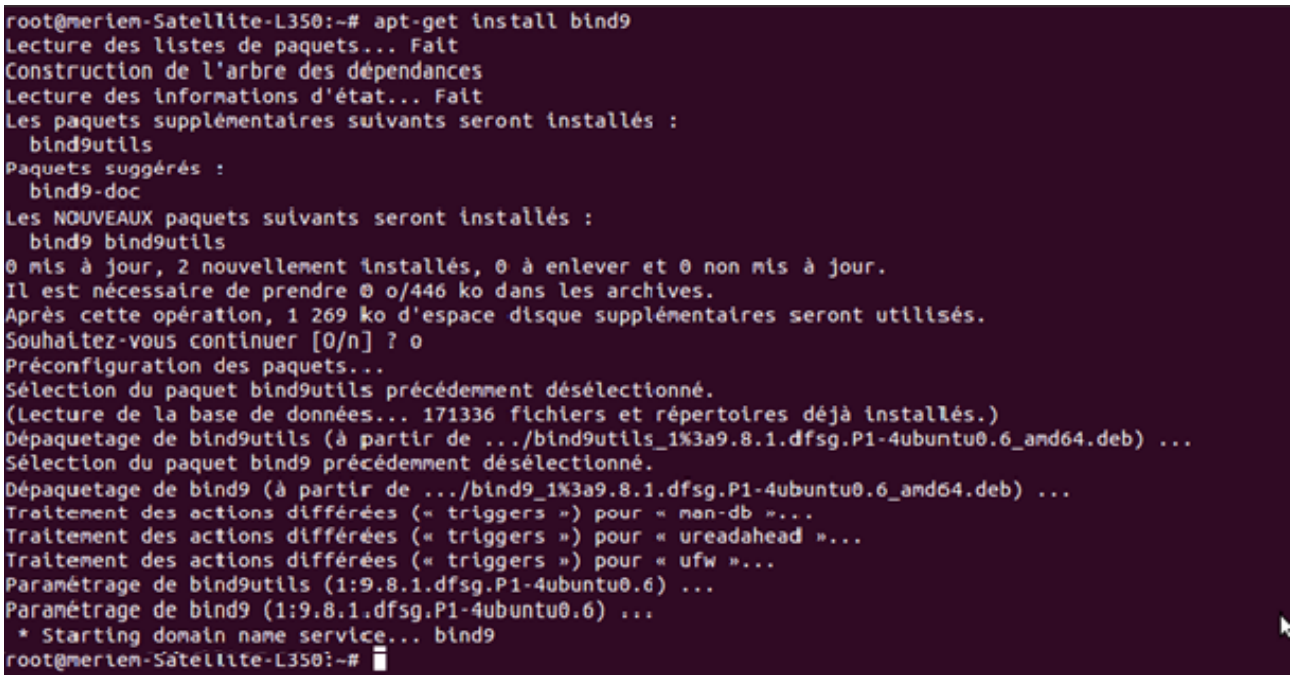


FIGURE 4.3 – Installation de bind9

Une fois que bind9 est installé, on le configure. Pour la configuration on a besoin de créer trois fichiers :

1. Le fichier named.conf.local.
2. Le fichier PFEM2.dz.db.
3. Le fichier inv. 56.168.192.in-addr.arpa .zone.

Ces fichiers, seront configurés afin de donner à notre serveur une adresse statique et lui indiquer le nom de domaine avec lequel il fera la résolution. Ils seront créés dans le répertoire bind :

`root@meriem-Satellite-L350: ♯cd /etc/bind/`

– Le premier fichier à créer, est le fichier " named.conf.local. " : `root@meriem-Satellite-L350:/etc/bind mkdirnamed.conf.local`

Une fois que le fichier est créé, on l'édite par la commande " nano " (il existe d'autres commandes pour cela, tel que : vi et gedit), afin de le configuré. Dans ce fichier, seront créées les zones (PFEM2.dz et 56.168.192.in-addr.arpa) de notre serveur DNS.

Remarque : concernant un fichier "nano" :

- CTRL+o+ENTRER : permet de sauvegarder le ficher.
- permet de quitter le fichier et der evenir sur le shell.
- permet de faire la recherche sur le fichier.

La figure qui suit, illustre le fichier " named.conf.local ", que nous avons créé et configuré :

`root@meriem-Satellite-L350:/etc/bind ♯ nanonamed.conf.local`

```
 GNU nano 2.2.6                          Fichier : named.conf.local

// // Do any local configuration here //

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";

zone "PFEM2.dz"  {
        type master;
        file "/etc/bind/PFEM2.dz.db";
};


zone "56.168.192.in-addr.arpa"  {
        type master;
        file "/etc/bind/inv.56.168.192.in-addr.arpa.zone";
};
```

FIGURE 4.4 – Configuration du fichier " named.conf.local "

Création de la zone, PFEM2.dz :

zone "PFEM2.dz" {
type master ;
file "/etc/bind/PFEM2.dz.db " ; } ;

Création de la zone,56.168.192.in-addr.arpa :

zone "56.168.192.in-addr.arpa " {
type master ;
file "/etc/bind/inv.56.168.192.in-addr.arpa .zone " ;
} ;

– Le deuxième fichier à créer est le ficher " PFEM2.dz.db ", dont le contenu est le même que le fichier, " db.local " :

`root@meriem-Satellite-L350:/etc/bind ♯ cpdb.local PFEM2.dz.db`

Configuration du fichier, " PFEM2.dz.db " :

`root@meriem-Satellite-L350:/etc/bind♯nano PFEM2.dz.db`

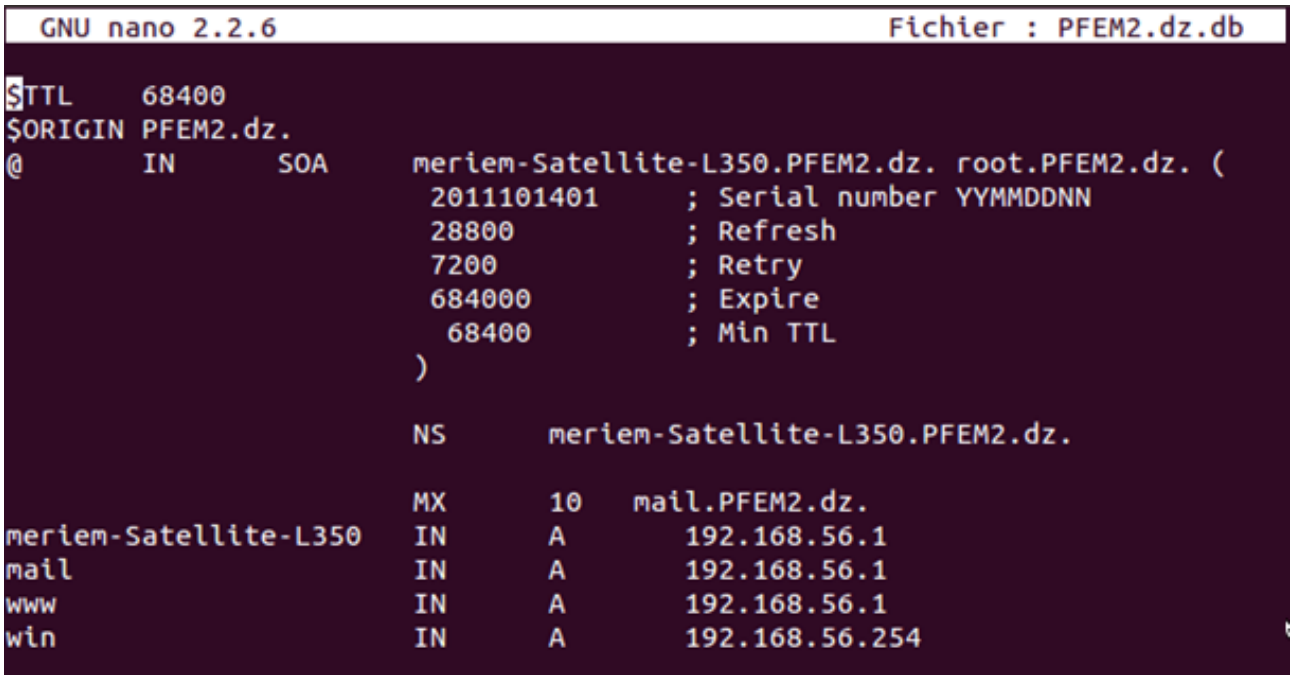


FIGURE 4.5 – Configuration du fichier " PFEM2.dz.zone "

Remarque : pour savoir le nom de notre machine, il suffit d'écrire la commande suivante :

```
meriem@meriem-Satellite-L350: hostname
```

(meriem-Stellite-L350, est le nom de la machine, sur laquelle nous avons configuré)

Concernant le code, qui se trouve dans le fichier PFEM2.dz.zone, la première partie consiste à synchroniser notre serveur DNS.

La deuxième partie, indique :

- Le nom de serveur par l'enregistrement NS.
- Les adresses, qui correspondent aux machines.

Créationet configuration du fichier " inv. 56.168.192.in-addr.arpa .zone " :

root@meriem-Satellite-L350 :/etc/bindc nano inv. 56.168.192.in-addr.arpa .zone

Une fois, les trois fichiers sont configurer, nous établirons un test, pour voir si notre configuration est correcte :

La première verification,*named-checkconf -z named.conf.local*

Les tests ne retournent aucune erreur, alors nous entamons la configuration du fichier, " resolv.conf ", ce fichier permet d'indiquer le domaine de recherche ainsi que l'adresse du serveur DNS.

root@meriem-Satellite-L350 :/etc/bind♯nano /etc/resolv.conf

Une fois que nous avons établi, toute la configuration nécessaire. Nous redémarrons, le service bind9 :

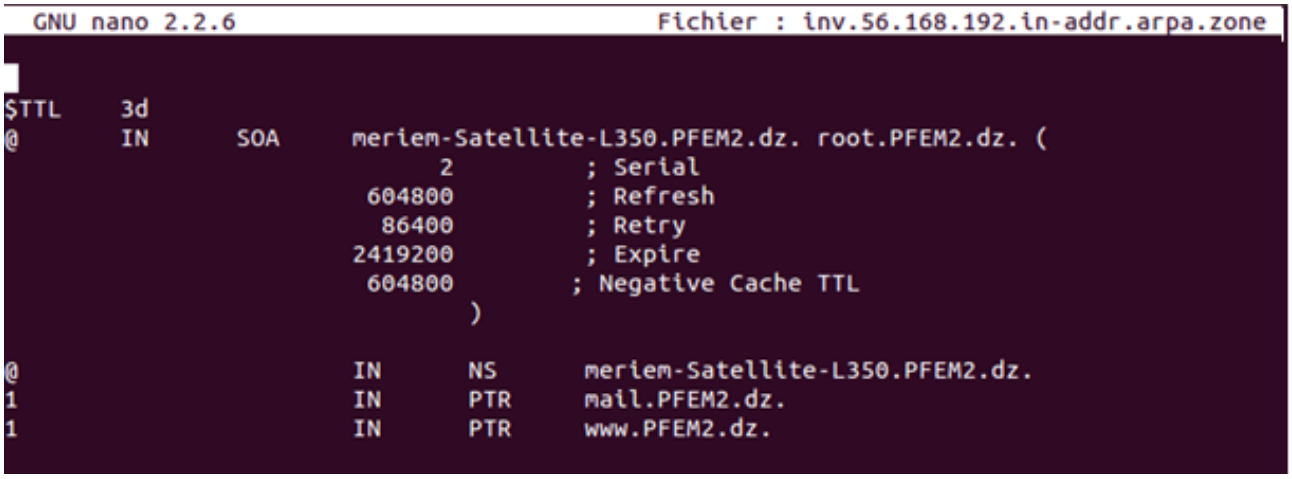


FIGURE 4.6 – Configuration du fichier " inv. 56.168.192.in-addr.arpa .zone"

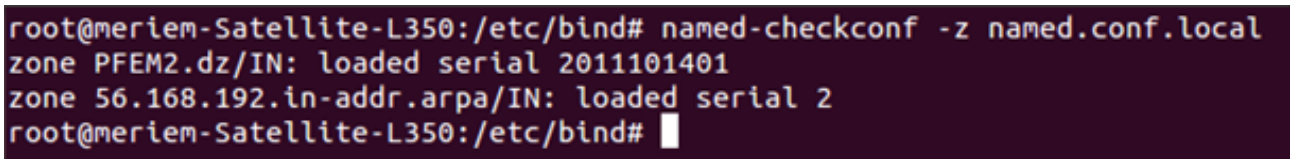


FIGURE 4.7 – Vérification de la configuration des zones

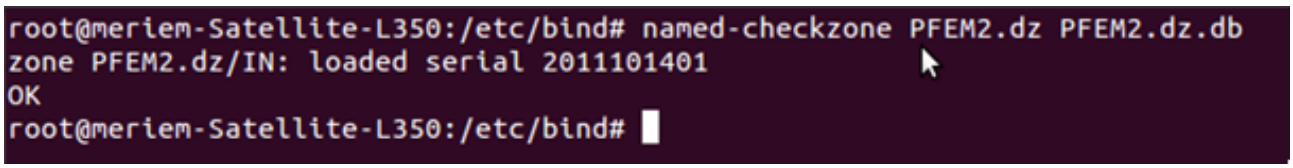


FIGURE 4.8 – Configuration du fichier resolv.conf

root@meriem-Satellite-L350 :/etc/bind♯ service bind9 restart

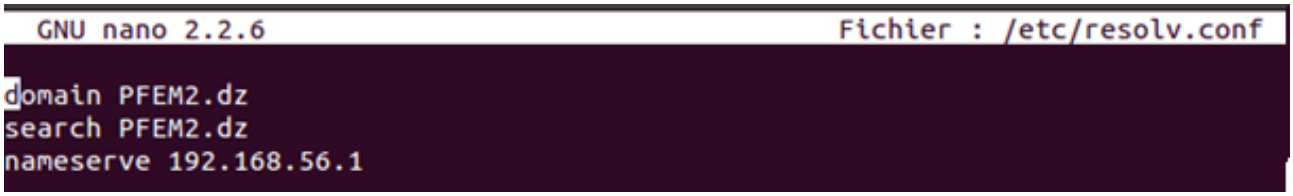


FIGURE 4.9 – Redémarrage du service bind9

Test de bind9, par la commandenslookup :

root@meriem-Satellite-L350 :/etc/bindnslookup

FIGURE 4.10 – Test DNS, par la commande nslookup

```
root@meriem-Satellite-L350:/etc/bind# nslookup
> 192.168.56.1
Server:         192.168.56.1
Address:        192.168.56.1#53

1.56.168.192.in-addr.arpa       name = www.PFEM2.dz.
1.56.168.192.in-addr.arpa       name = mail.PFEM2.dz.
> mail
Server:         192.168.56.1
Address:        192.168.56.1#53

Name:   mail.PFEM2.dz
Address: 192.168.56.1
> www
Server:         192.168.56.1
Address:        192.168.56.1#53

Name:   www.PFEM2.dz
Address: 192.168.56.1
> meriem-Satellite-L350
Server:         192.168.56.1
Address:        192.168.56.1#53

Name:   meriem-Satellite-L350.PFEM2.dz
Address: 192.168.56.1
```

FIGURE 4.11 – root@meriem-Satellite-L350 :/etc/bind ♯ nslookup

Sur la figure précédente, nous remarquant, quand nous écrivons l'adresse de notre serveur (>192.168.56.1), il nous retourne le nom de notre machine (name = meriem-Satellite-L350).

Quand nous écrivons, le nom de notre machine (name = meriem-Satellite-L350), il nous retourne l'adresse de notre serveur (Address : 192.168.56.1)
D'où, notre serveur DNS fonctionne, c'est-à-dire qu'il peut faire la résolution.

Deuxième étape : installation de lamp-server
LAMP (Linux ApacheMysqlPhp), donc nous installerons :

1. Apache2.
2. Mysqlserver.
3. Php5.

Concernant linux, nous l'avons déjà comme système sur notre machine (Ubuntu 12.4LTS), il nous reste donc à installer, Apach2, Mysql et Php.

– Installation de Apache2 :
root@meriem-Satellite-L350 : ♯sudo apt-get install apache2
Une fois que apache2 est installé. Vérification de son installation, pour cela il suffit d'écrire le lien suivant sur notre navigateur " http ://localhost/ ".

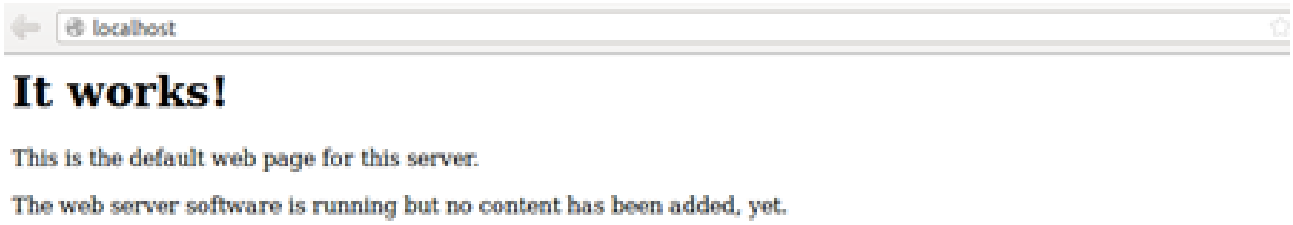


FIGURE 4.12 – Vérification de l'installation apche2.

– Installation de Mysql-server :
root@ubuntu :/home/kah♯ apt-get installmysql-server

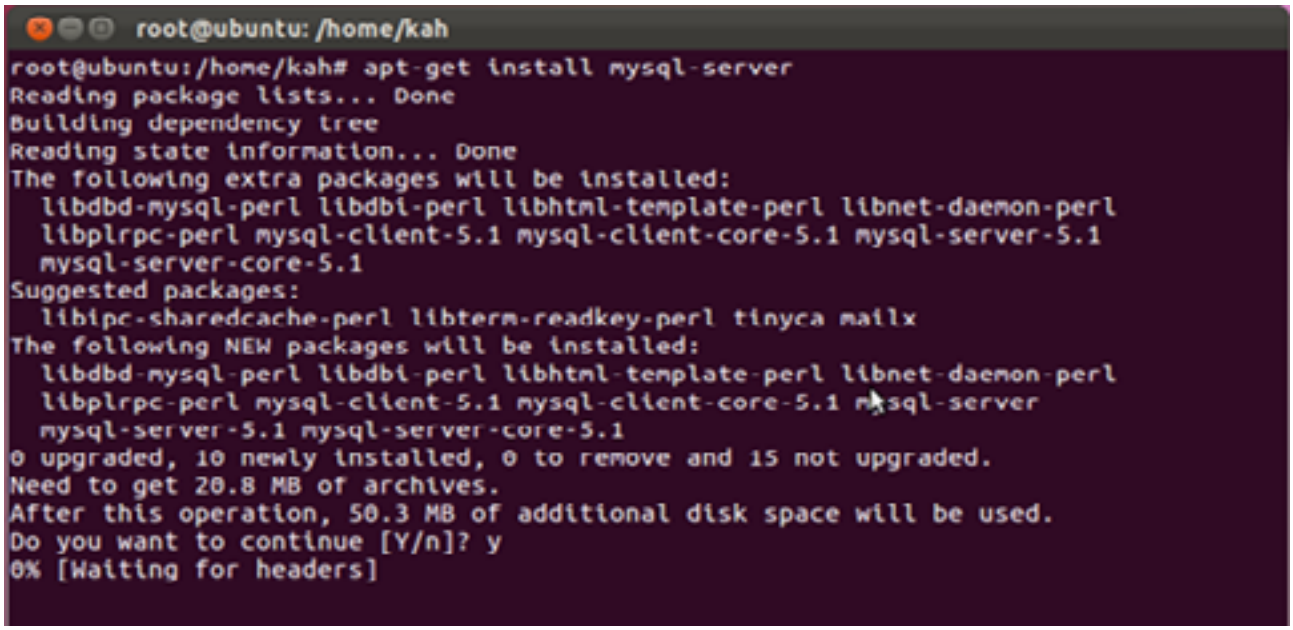


FIGURE 4.13 – Confirmation d'installation de mysql-server

Le serveur Mysql, nous permettra de créer la base de données postfix, qui sera liée au serveur postfix.
Pendant l'installation demysql-server, une fenêtre de configuration apparait, pour faire entrer un mot de passe.Cette étape est obligatoire, sinon le mot de passé sera crééaléatoirement.

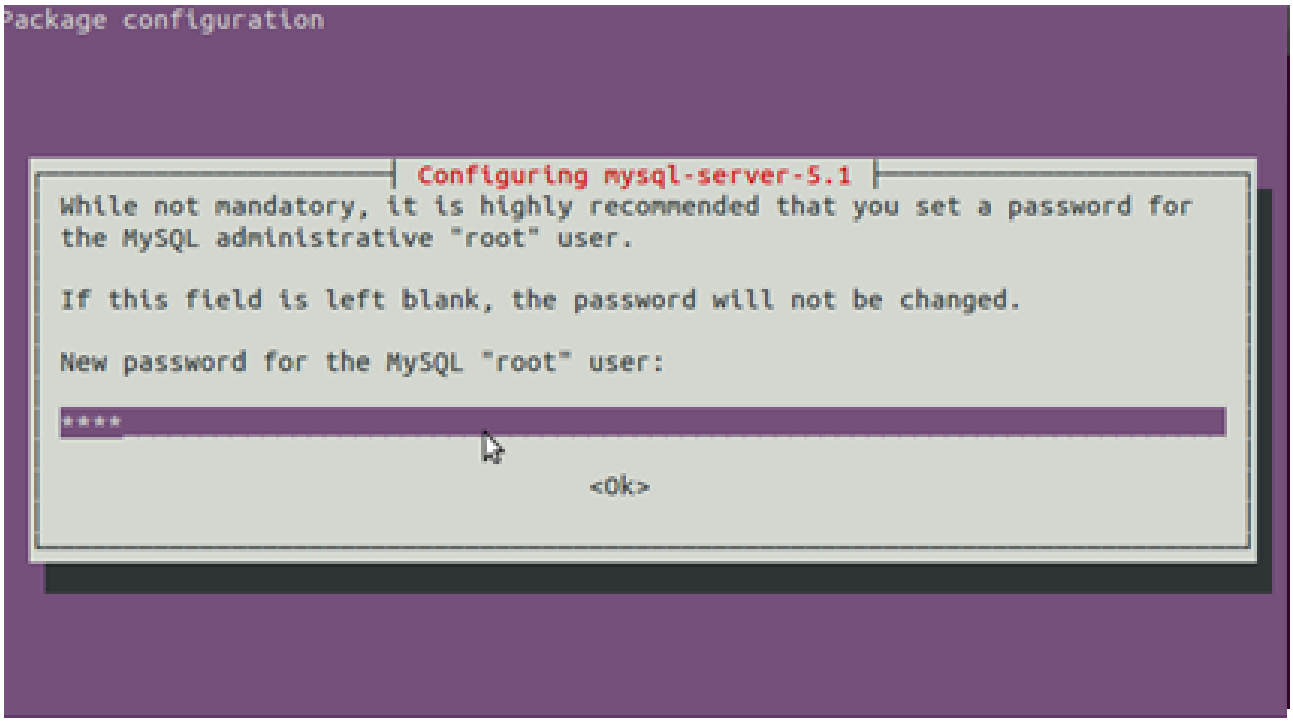


FIGURE 4.14 – Attribution d'un mot de passe au serveur mysql

Après cette étape, mysql-server, s'installera

– Installation de php5 :

root@meriem-Satellite-L350 : ♯apt-get install php5

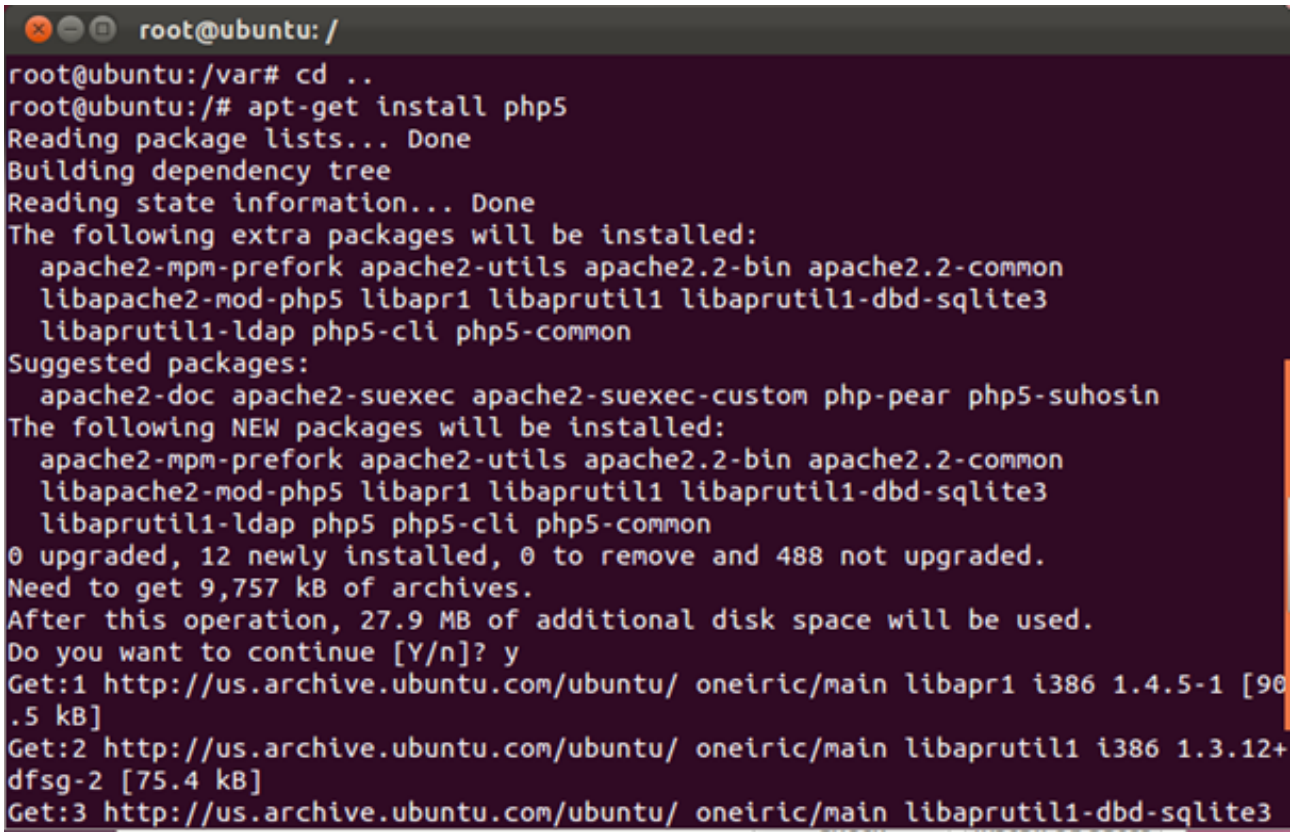


FIGURE 4.15 – Installation de php5

Maintenant il faut redémarrer apache2, pour qu'il soit compatible avec php5 :

root@meriem-Satellite-L350 : c /etc/init.d/apache2 restart

pour tester le bon fonctionnement de php5, nous éditons le fichier testphp.php et écrire : *< ?phpphpinfo() ; ?>*.

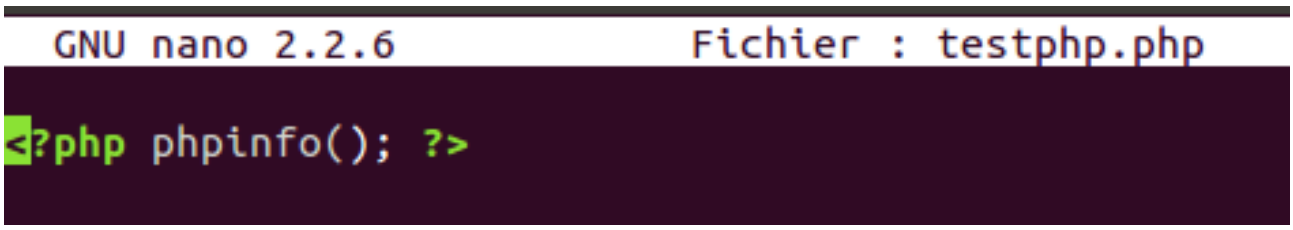
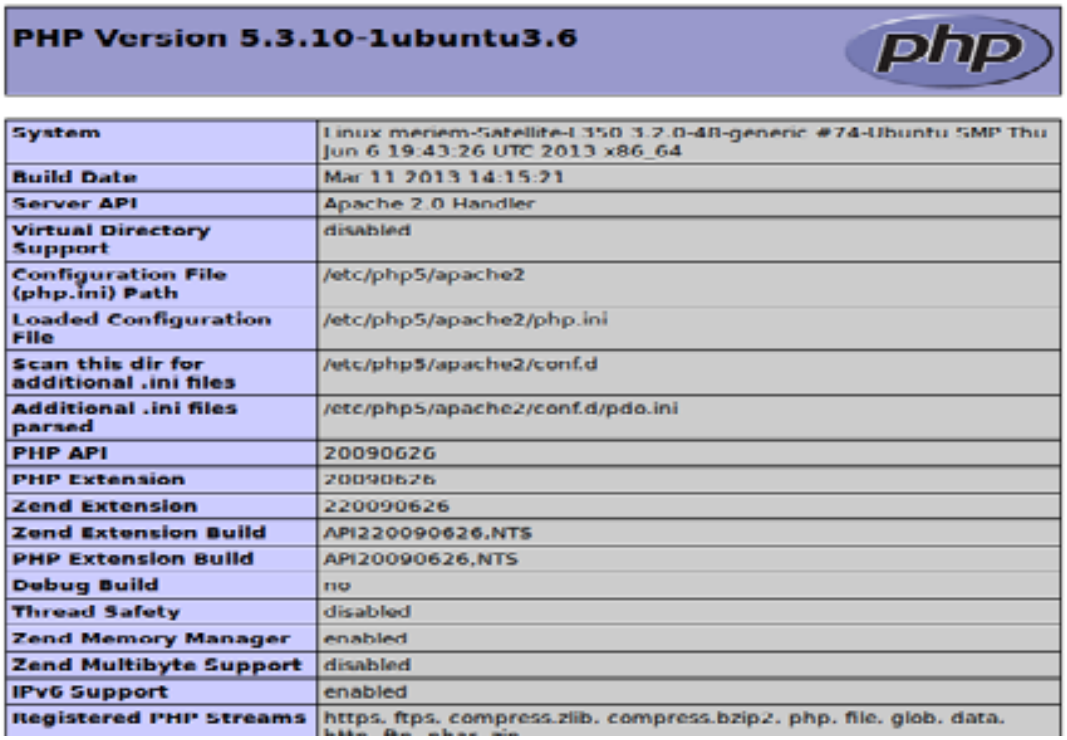


FIGURE 4.16 – le fichier testphp.php

Ensuite, sur le navigateur, par le lien : http ://localhost/testphp.php , c'est cette page qui doit apparaitre :



PHP Version 5.3.10-1ubuntu3.6

System	Linux meriem-Satellite-L350 3.2.0-48-generic #74-Ubuntu SMP Thu Jun 6 19:43:26 UTC 2013 x86_64
Build Date	Mar 11 2013 14:15:21
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php5/apache2
Loaded Configuration File	/etc/php5/apache2/php.ini
Scan this dir for additional .ini files	/etc/php5/apache2/conf.d
Additional .ini files parsed	/etc/php5/apache2/conf.d/pdo.ini
PHP API	20090626
PHP Extension	20090626
Zend Extension	220090626
Zend Extension Build	API220090626,NTS
PHP Extension Build	API20090626,NTS
Debug Build	no
Thread Safety	disabled
Zend Memory Manager	enabled
Zend Multibyte Support	disabled
IPv6 Support	enabled
Registered PHP Streams	https, ftps, compress.zlib, compress.bzip2, php, file, glob, data,

FIGURE 4.17 – Vérification d'installation de php5

Troisième étape :installation et configuration de phpmyadmin

root@meriem-Satellite-L350 : ♯-get installphpmyadmin

A la fin d'installation de phpmyadmin, nous ajoutrons la ligne " Include /etc/phpmyadmin/apache.conf ", au fichier " apache2.conf ", pour que phpmyadmin puis se fonctionner.

Une fois phpmyadmin est installé, nous accédons à son interface, sur le navigateur par : 192.168.56.1/phpmyadmin.

FIGURE 4.18 – l'interface phpmyadmin

Quatrième étape :installation et configuration du serveur messagerie (MTA), Postfix
En ouvrant un nouveau terminal, nous installons postfix, par la commande :
root@meriem-Satellite-L350 : ♯apt-get install postfix-mysql
Une fois postfix est installé, nous entamons sa configuration. Pour cela, il faut être dans le répertoirepostfix.
root@meriem-Satellite-L350 : ♯cd /etc/postfix/
Une fois dans le répertoire, nous écrivons la commande suivante pour voir les différents fichiers de postfix,
root@meriem-Satellite-L350 :/etc/postfix♯ ls

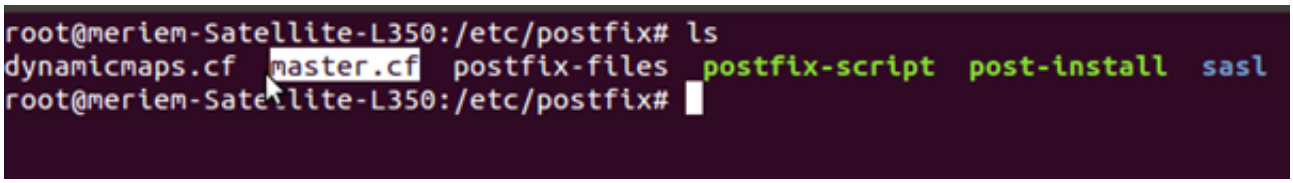


FIGURE 4.19 – Les fichiers de postfix

Le fichier qui nous intéresse le plus, est le fichier : master.cf ; nous l'éditons avec cette commande : *root@meriem-Satellite-L350 :/etc/postfix♯* nano master.cf ; dans ce fichier nous vérifions la ligne *smtp* qui correspond à la colonne *chroot*, qu'elle contient un tiret et non pas autre chose.

```
  GNU nano 2.2.6                                  Fichier : master.cf

#
# Postfix master process configuration file.  For details on the format
# of the file, see the master(5) manual page (command: "man 5 master").
#
# Do not forget to execute "postfix reload" after editing this file.
#
# ==========================================================================
# service type  private unpriv  chroot  wakeup  maxproc command + args
#               (yes)   (yes)   (yes)   (never) (100)
# ==========================================================================
smtp      inet  n       -       -       -       -       smtpd
#smtp      inet  n       -       -       -       1       postscreen
#smtpd     pass  -       -       -       -       -       smtpd
#dnsblog   unix  -       -       -       -       0       dnsblog
#tlsproxy  unix  -       -       -       -       0       tlsproxy
#submission inet n       -       -       -       -       smtpd
#  -o syslog_name=postfix/submission
#  -o smtpd_tls_security_level=encrypt
#  -o smtpd_sasl_auth_enable=yes
#  -o smtpd_client_restrictions=permit_sasl_authenticated,reject
#  -o milter_macro_daemon_name=ORIGINATING
#smtps     inet  n       -       -       -       -       smtpd
#  -o syslog_name=postfix/smtps
#  -o smtpd_tls_wrappermode=yes
#  -o smtpd_sasl_auth_enable=yes
#  -o smtpd_client_restrictions=permit_sasl_authenticated,reject
#  -o milter_macro_daemon_name=ORIGINATING
#628       inet  n       -       -       -       -       qmqpd
pickup    fifo  n       -       -       60      1       pickup
cleanup   unix  n       -       -       -       0       cleanup
qmgr      fifo  n       -       n       300     1       qmgr
#qmgr     fifo  n       -       n       300     1       oqmgr
tlsmgr    unix  -       -       -       1000?   1       tlsmgr
rewrite   unix  -       -       -       -       -       trivial-rewrite
```

FIGURE 4.20 – configuration du fichier master.cf

Une fois que nous avons vérifié le fichier master.cf, nous allons créer, la base de données postfix, en utilisant l'interface phpmyadmin :

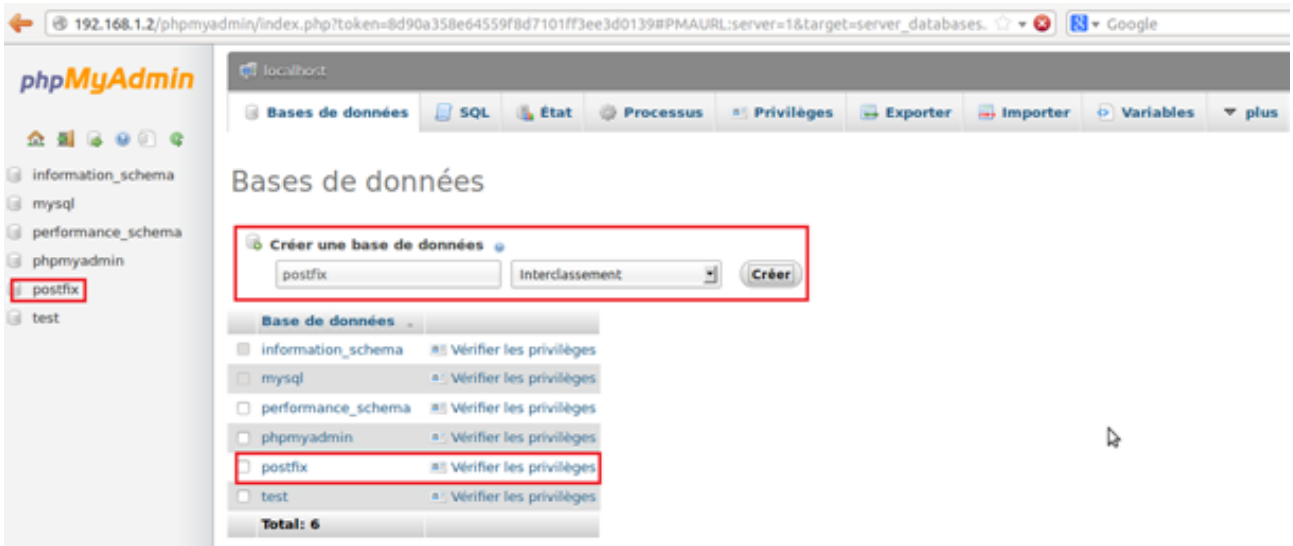


FIGURE 4.21 – Création de la base de données Postfix

Maintenant que la base de données est créée, il faut ajouter un nouvel utilisateur postfix, et lui donner tous les privilèges sur la base de données postfix ; de cette manière si un intrusaccède à cette base il ne pourra pas accéder aux autres bases. Pour établir cette action il faut être sur la base de données potfix.

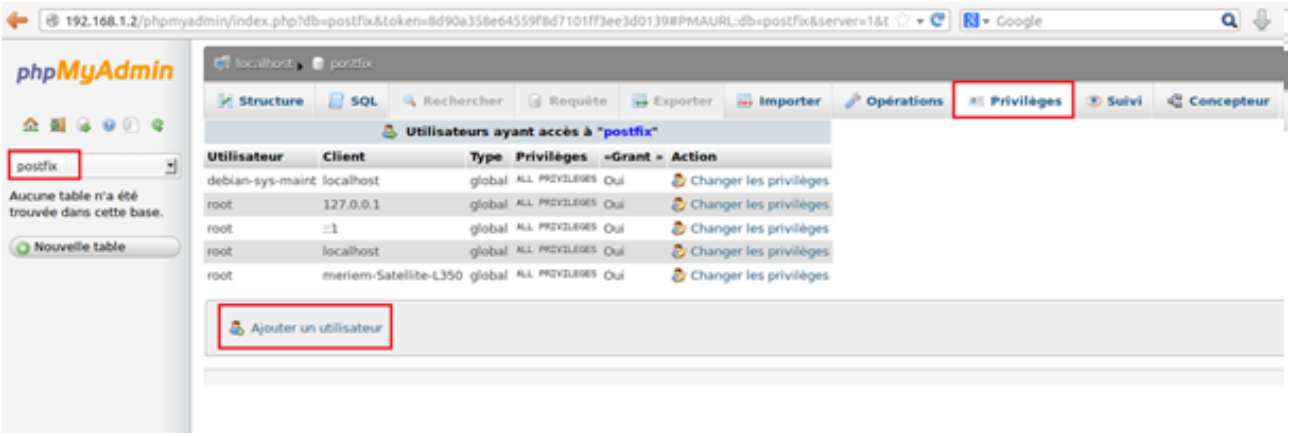


FIGURE 4.22 – Création du nouvel utilisateur Postfix

Dans notre cas, nous avons besoins de créer trois tables, dans la base de données postfix. Ces trois tables sont :

1. Table domaines : contiendra tous les domaines de notre serveur.
2. Table comptes : contiendrales comptes des domaines qu'on va créer.
3. Table alias : contiendra tous les alias des e-mail.

Pour la création de ces tables, il faut aller sur la base postfix >SQL et écrire le code suivant :

```
USE postfix;
CREATE TABLE `domaines` (
  `domaine` varchar(255) NOT NULL default '',
  `etat` tinyint(1) NOT NULL default '1',
  PRIMARY KEY  (`domaine`)
) ENGINE=MyISAM;


CREATE TABLE `comptes` (
  `email` varchar(255) NOT NULL default '',
  `password` varchar(255) NOT NULL default '',
  `quota` int(10) NOT NULL default '0',
  `etat` tinyint(1) NOT NULL default '1',
  `imap` tinyint(1) NOT NULL default '1',
  `pop3` tinyint(1) NOT NULL default '1',
  PRIMARY KEY  (`email`)
) ENGINE=MyISAM;


CREATE TABLE `alias` (
  `source` varchar(255) NOT NULL default '',
  `destination` text NOT NULL,
  `etat` tinyint(1) NOT NULL default '1',
  PRIMARY KEY  (`source`)
) ENGINE=MyISAM;
```

Ce code nous permettra la création des trois tables : domaines, comptes et alias.

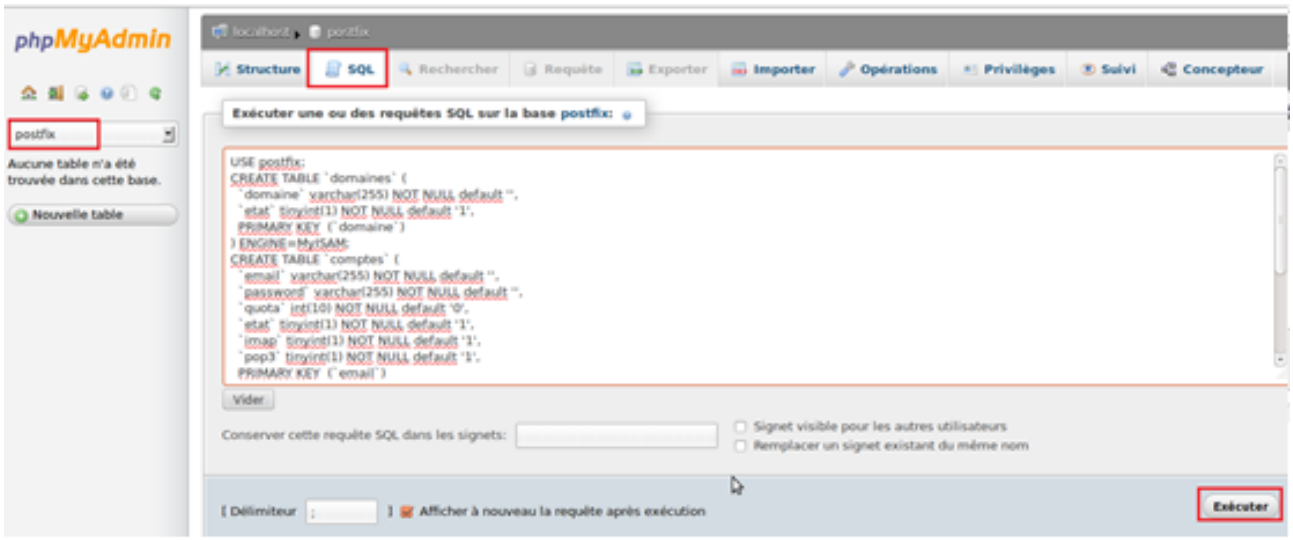


FIGURE 4.23 – Le code SQL, pour la création des trois tables dans la base de données postfix.

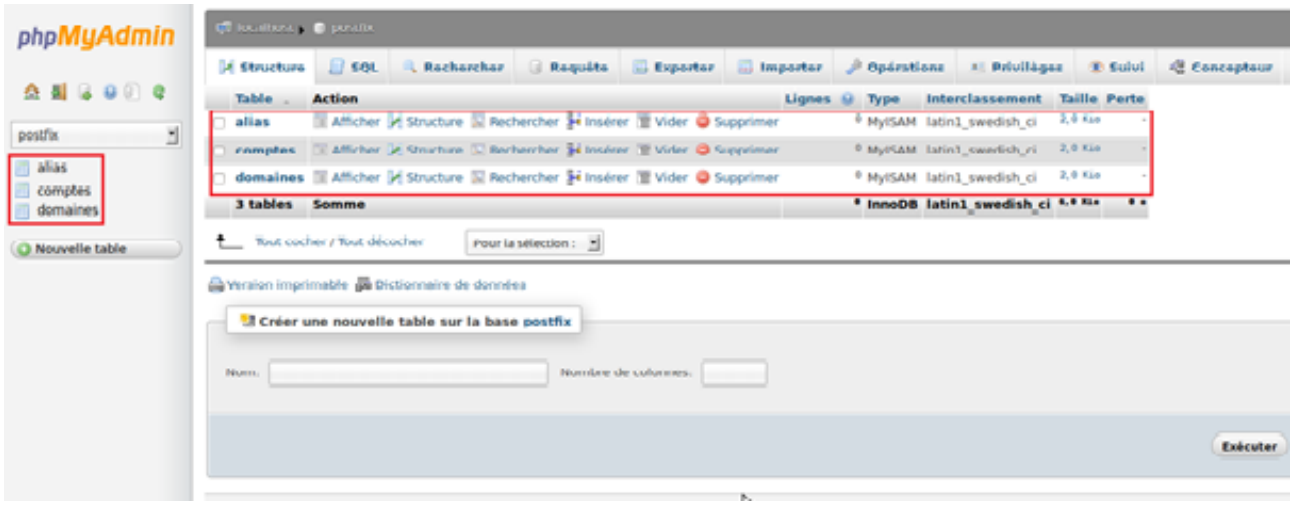


FIGURE 4.24 – Création des tables.

Une fois la base de données postfix, l'utilisateur postfix et les trois tables, sont créés, nous revenons à la configuration du serveur postfix. Pour la configuration, on a besoin de créer cinq, fichiers :

1. Le fichier mysql-virtual-comptes.cf.
2. Le fichiermysql-virtual-aliases.cf.
3. Le fichier mysql-virtual-alises-comptes.cf.
4. Le fichier mysql-virtual-domaines.cf.
5. Le fichier mysql-virtual-quotas.cf.

Ces fichiers, indiqueront au serveur postfix, la base de donnéesposfix, l'utilisateur postfix, les tables de postfix ainsi que les quotas d'un compte d'un nom de domaine.

– Creation du fichiermysql-virtual-domaines.cf

root@meriem-Satellite-L350 :/etc/postfix♯nano mysql-virtual-domaines.cf

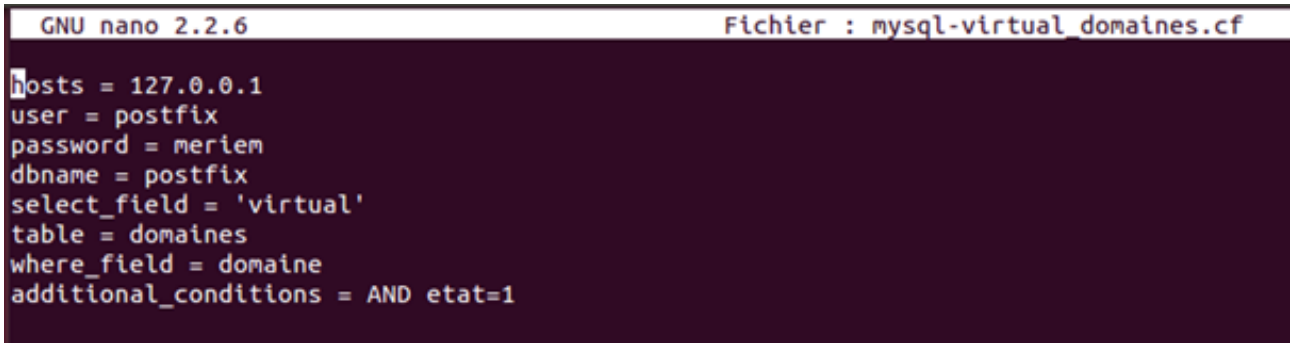


FIGURE 4.25 – Le fichier mysql-virtual-domaines.cf.

Comme le montre la figure précédente, le fichier mysql-virtual-domaines.cf, contient huit lignes, les quatre premières lignes sont les mêmes, pour tous les autres fichiers, il n'y aura que les quatre dernières qui seront changer.

```
hosts = 127.0.0.1          //la base est hibergée sur le serveur host
user = postfix             //l'utilisateur c'est postfix
password = meriem          //le mot de passe postfix
dbname = postfix           //la table est dans la base de données postfix
select_field = 'virtual'   //le champs sélectionné est virtual
table = domaines           //la table sélectionnée est la table domaine
where_field = domaine      //la condition choisie est domaine dans la table domaines
additional_conditions = AND etat=1   //le champs de condition est etat=1 sur la table domaine
```

FIGURE 4.26 –

– Creation du fichier mysql-virtual-comptes.cf

Pour ne pas perdre le temps à réécrire les lignes une deuxième fois, il suffit de copier le contenu du fichier mysql-virtual-domaines.cf dans le fichier mysql-virtual-comptes.cf, en utilisant la commande "cp" :

root@meriem-Satellite-L350 :/etc/postfix♯ cp mysql-virtual-domaines.cfmysql-virtual-comptes.cf

root@meriem-Satellite-L350 :/etc/postfix♯ nano mysql-virtual-comptes.cf

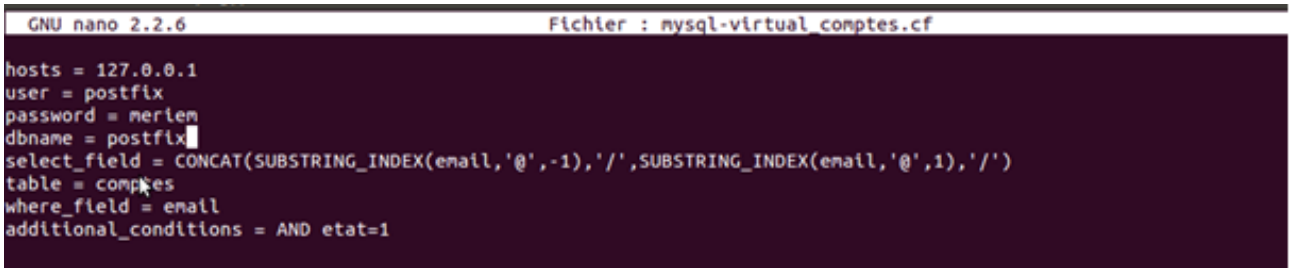


FIGURE 4.27 – Le fichier mysql-virtual-comptes.cf.

Comme le montre la figure précédente, les quatre premières lignes sont les même que celle du fichier précèdent et elles ont le même rôle. Concernant les autres lignes :

```
table = comptes              //la table sélectionnée est la table comptes
select_field = CONCAT(SUBSTRING_INDEX(email,'@',-1),'/',SUBSTRING_INDEX(email,'@',1),'/')
//le champs que allons récupérer
where_field = email    //correspond au champ email sur la table comptes
additional_conditions = AND etat=1      //le champs de condition est etat=1 sur la table comptes
```

– Creation du fichier mysql-virtual-aliases.cf.

Nous allons faire, la même chose avec le fichier précédent :
root@meriem-Satellite-L350 :/etc/postfix♯cp mysql-virtual-domaines.cf mysql-virtual-aliases.cf

root@meriem-Satellite-L350 :/etc/postfix♯nano mysql-virtual-aliases.cf

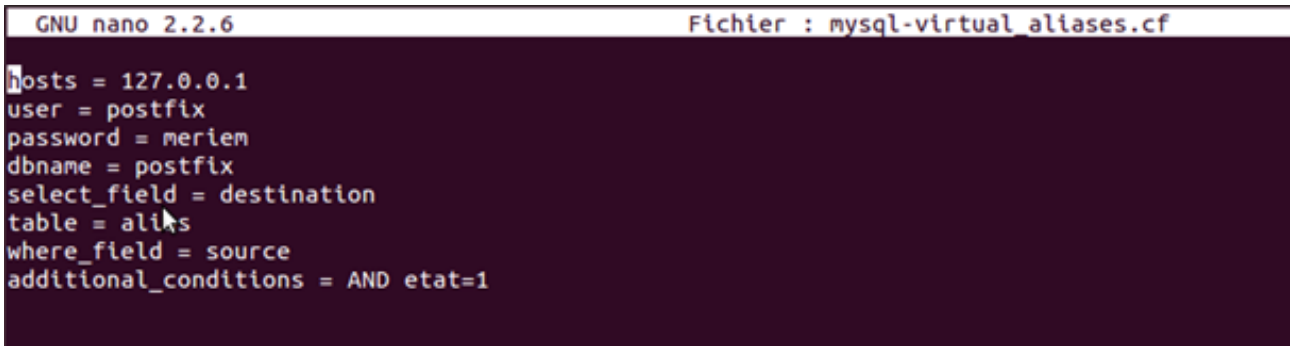


FIGURE 4.28 – Le fichier mysql-virtual-aliases.cf.

```
table = alias          //la table sélectionnée est la table alias
select_field = destination       //le champs sélectionné est destination
where_field = source      // correspond au champ email sur la table alias
additional_conditions = AND etat=1     //le champs de condition est etat=1 sur la table alias
```

– Creation du fichier mysql-virtual-aliases-comptes.cf :
root@meriem-Satellite-L350 :/etc/postfix♯ cp mysql-virtual-domaines.cf mysql-virtual-alises-comptes.cf.

root@meriem-Satellite-L350 :/etc/postfix♯nano mysql-virtual-alises-comptes.cf

```
 GNU nano 2.2.6                    Fichier : mysql-virtual_aliases_comptes.cf

hosts = 127.0.0.1
user = postfix
password = meriem
dbname = postfix
select_field = email
table = comptes
where_field = email
additional_conditions = AND etat=1
```

FIGURE 4.29 – Le fichier mysql-virtual-aliases-comptes.cf.

– Création du fichier mysql-virtual-quotas.cf :
root@meriem-Satellite-L350 :/etc/postfix♯ cp mysql-virtual-domaines.cfmysql-virtual-quotas.cf.

root@meriem-Satellite-L350 :/etc/postfix♯ nano mysql-virtual-quotas.cf

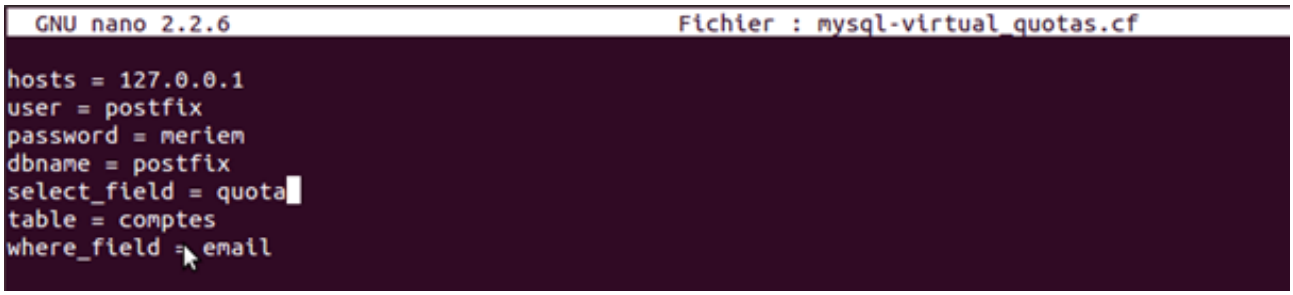


FIGURE 4.30 – Le fichier mysql-virtual-quotass.cf.

Dans ce fichier, ne figure pas la dernière ligne des fichiers précédents, car ce fichier concerne le champ quotas de la table comptes, donc la dernière ligne n'est pas obligatoire.

Une fois que les fichiers sont créés, on leur attribuera des droits, comme suit : *root@meriem-Satellite-L350 :/etc/postfix♯chmod u=rw,g=r,o= /etc/postfix/mysql-virtual*.*cf

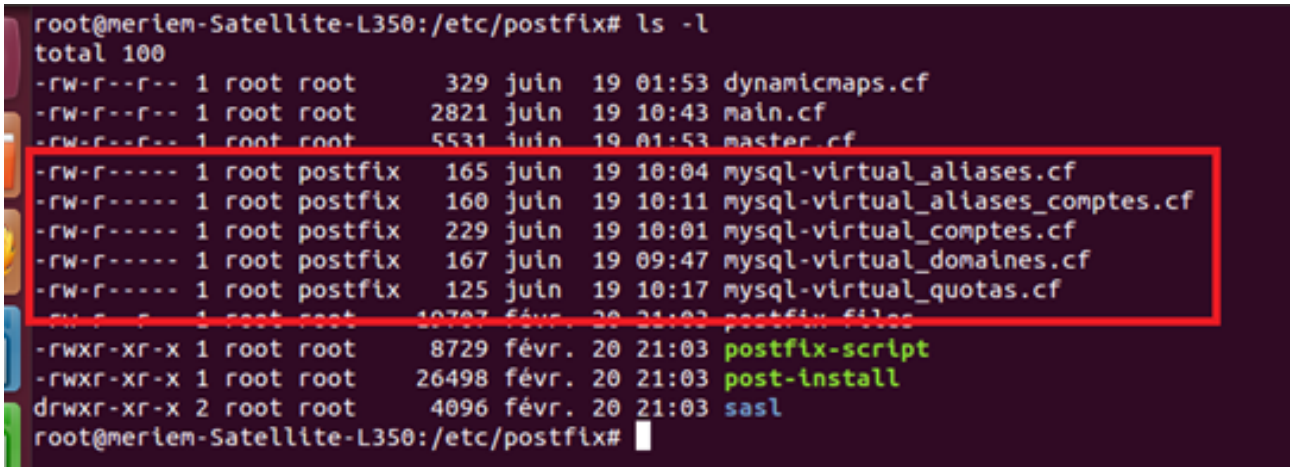


FIGURE 4.31 – Attribution des droits aux fichiers mysql-virtual-∗

Après avoir attribué les droits, aux fichiers, nous allons leur changer de groupe, pour plus de sécurité :

Ajouter un groupe g dans le répertopoirvmail, avec 5000 comme identifiant :
root@meriem-Satellite-L350 :/etc/postfix♯groupadd-g 5000 vmail
Ajouter un utilisateur u au groupe g, dans le répertoire vmail :
root@meriem-Satellite-L350 :/etc/postfix♯ useradd -g vmail -u 5000 vmail -d /var/spool/vmail-m*root@meriem-Satellite-L350 :/etc/postfixchgrppostfix /etc/postfix/mysql-virtual-∗.cf*

Ajouter un groupe g dans le répertopoirvmail, avec 5000 comme identifiant :
root@meriem-Satellite-L350 :/etc/postfix♯groupadd-g 5000 vmail
Ajouter un utilisateur u au groupe g, dans le répertoire vmail :
root@meriem-Satellite-L350 :/etc/postfix♯ useradd -g vmail -u 5000 vmail -d /var/spool/vmail-m

Une fois, les cinq fichiers, sont créés, nous configurons, le fichier main.cf, qui contiendra le code suivant :

```
GNU nano 2.2.6                                  Fichier : main.cf

# Bannière afficher lorsqu'on se connecte en SMTP sur le port 25
smtpd_banner = $myhostname ESMTP $mail_name (Debian/GNU)

# Service qui envoie des notifications "nouveau message"
biff = no

# Desactive la commande SMTP VRFY. Arrête certaine technique pour avoir des adresses email
disable_vrfy_command = yes

# Impose au client SMTP de démarrer la session SMTP par une commande Helo (ou ehlo)
smtpd_helo_required = yes

# Avec le courier local ça ajoute .NDD aux adresses incomplètes (seulement le nom d'hote)
append_dot_mydomain = no

# Le nom de la machine du systène de messagerie
# Par défaut c'est host.domain.tld mais on peut mettre un reverse dns
myhostname = 2.1.168.192.in-addr.arpa

# Le domaine utilisé par defaut pour poster les message local
myorigin = 2.1.168.192.in-addr.arpa

# Liste des domaines pour lequel le serveur doit accepter le courrier
mydestination = 2.1.168.192.in-addr.arpa, localhost.localdomain, localhost

# Pour effectuer des livraisons de courrier avec un relay (ici non)
relayhost =

# Liste des réseaux locaux autorisés
mynetworks = 127.0.0.0/8, 192.168.1.2
```

FIGURE 4.32 – Le fichier main.cf

Cinquième étape : Installation et configuration dedovecot pop3 et du dovecoptimap
root@meriem-Satellite-L350 :/etc/postfix♯ apt-get installdovecot pop3 dovecot imap
Sixième étape : installation et cofiguration de Squirellmail :
root@meriem-Satellite-L350 :/etc/postfix♯ apt-get installsquirrelmail
Une fois notre MUA est installé, on ajoute la ligne *" Include /etc/squirrelmail "*, au fichier " apache2.conf ", pour qu'il sera compatible avec apache2. Pour accéder à squirrelmail, il suffit d'écrire *" www.PFEM2.dz/squirrelmail "*, sur le navigateur ; l'interface

du webmail, apparaîtra.

FIGURE 4.33 – L'interface de squirrelmail

En entrant le nom d'utilisateur, avec le mot de passe, nous aurons la page principale, suivante :

FIGURE 4.34 – La page principale de squirrelmail

Cette page comporte trois parties principales :

1. Liste des dossiers et le quota utilisé(partie haute).
2. Menus (partie haute).
3. Liste des messages d'un dossier (partie centrale).

– Liste des dossiers et le quota utilisé (partie gauche)

On y trouve quatre dossiers destinés au rangement des messages :

- Boite de réception, dans lequel les messages reçus sont stockés par défaut.
- Brouillons,permet de stocker temporairement des messages en cours de rédaction pour un envoi ultérieur.
- Envoyer, contient une copie de chaque message que nous envoyons.
- Corbeille,contient les messages supprimés.

– Menus (partie haute)

Se trouve au sommet de la page permettant plusieurs actions :

- Composer, pour rédiger un message.
- Adresses, pour créer et utiliser le carnet d'adresses,
- Dossier, pour gérer les dossiers par défaut et en créant de nouveaux,
- Options, permet la personnalisation de l'environnement (modifier les informations personnelles, changer de mot de passe,).
- Rechercher, nous aide à rechercher un ou plusieurs messages dans nos dossiers,
- Aide, pour un aide en ligne du webmailsquirrelmail,
- Filtres, pour la création des règles de partage,
- Fermer la session,permet de se déconnecter du webmail et retour à la page d'accueil.

– Liste des messages d'un dossier (partie centrale)

La partie où sont affichés les messages du dossier sélectionné dans la partie gauche de la fenêtre. Organisé selon Une barre de menu avec trois champs (De, Date et Objet) est située juste en dessous. Les messages non lus apparaissent en gras. Pour lire un message il suffit simplement de cliquer sur le sujet (objet) du message.

Une ligne se trouve sous le menu, nous informe, de nombre de mail contenu dans ce dossier.

Juste en dessous est placé une barre contenant des boutons :

- Déplacer, qui va déplacer les messages sélectionner vers le dossier choisi à gauche de ce bouton.
- Supprimer et Purger, pour effacer les messages sélectionnés.
- Dossier, pour gérer les dossiers par défaut et en créant de nouveaux,
- Options, permet la personnalisation de l'environnement (modifier les informations personnelles, changer de mot de passe,).
- D'autres pour marquer le message comme lu ou non lu et l'autre pour faire suivre.

Actions du menu Nous allons donner quelques actions du menu :

- Compose

  La fenêtre suivante permet de composer un message :

  En cliquant sur le lien " composer ", une nouvelle page s'ouvre nous permettons de rédiger notre message. Elle comporte les informations et options classiques de la composition d'un message électronique :

  - Le champ To : ce champs comprendra l'adresse du ou des destinataire(s) de notre message.
  - Supprimer et Purger, pour effacer les messages sélectionnés.
  - Le champCc : comprendra l'adresse d'une tierce personne, si nous voulons envoyer une copie du message.

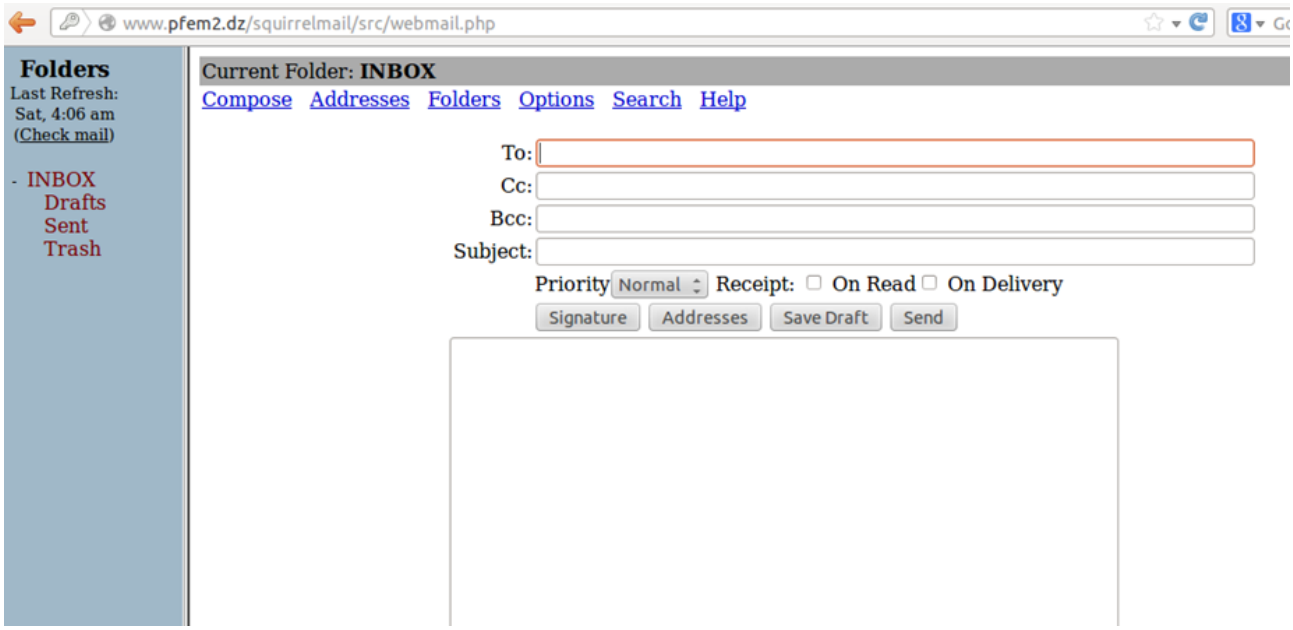


FIGURE 4.35 – Ecrire un message

- Le champ Bcc : comprendra l'adresse du destinataire à qui envoyer une copie d'un message sans que les destinataires des champs To ou Cc n'en soient informés.
- Le champ subject : indique le sujet du message.

Sur cette pages plusieurs options sont possibles (donner l'ordre de priorité, le signer, l'enregistrer comme brouillon, joindre une pièce).

Une fois le message est composé, il peut être envoyé en cliquant sur le bouton Send.

- Gestion du carnet d'adresses

  Le répertoire nous permet un gain de temps appréciable. Il permet d'enregistrer les adresses électroniques des utilisateurs courants.

  En cliquant sur le lien Adresses dans la barre de menus, nous aurons une page qui permet de saisir les données de notre carnet d'adresses (5 champs maximum : surnom (alias), prénom, nom, adresse électronique, informations complémentaires). Pour utiliser ensuite le carnet d'adresses, cliquons sur le bouton Adresses dans la fenêtre de composition d'un message.

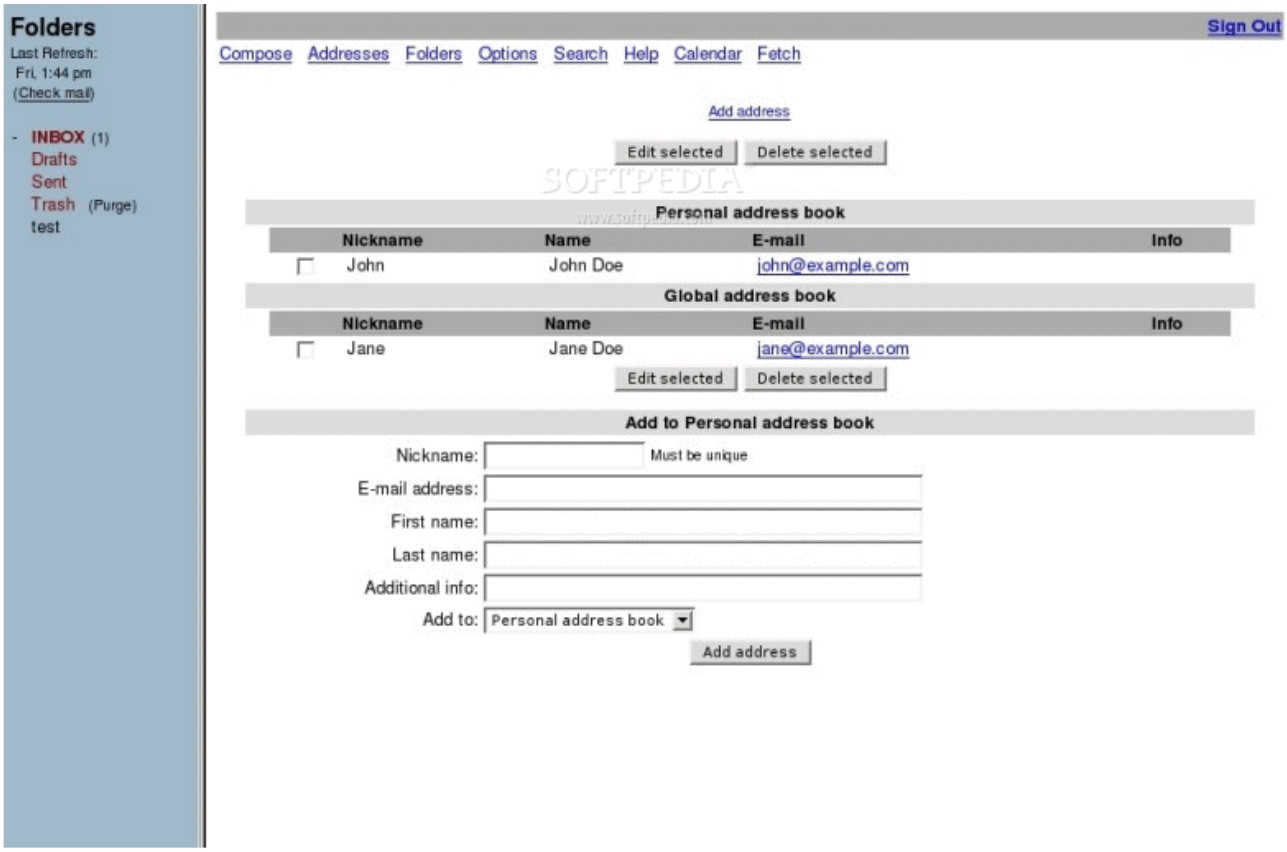


FIGURE 4.36 – Carnet d'adresse

- Options

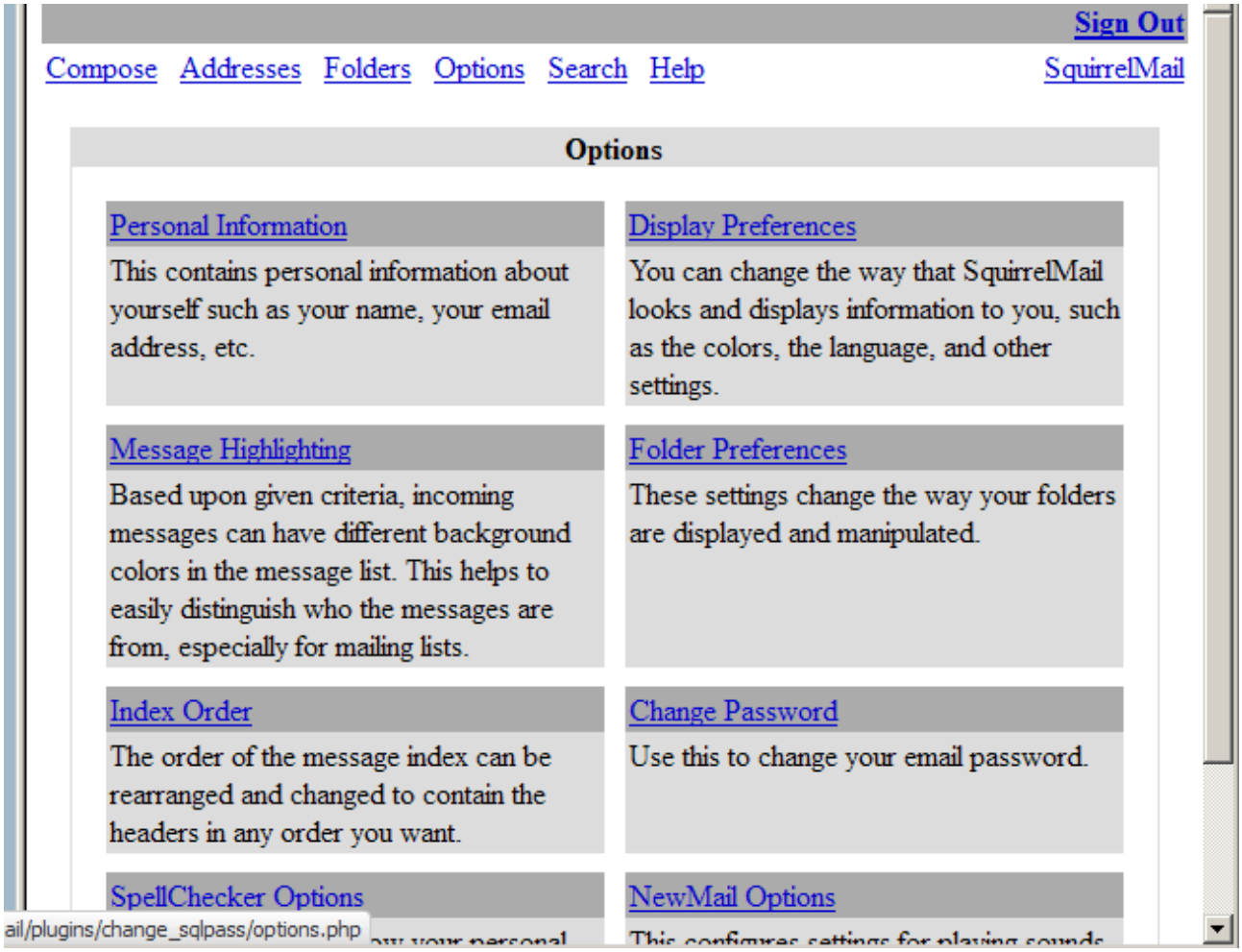


FIGURE 4.37 – Les options

Si nous choisissons par exemple l'option " changer le mot de passe", nous aurons la page suivante, où il faut écrire l'ancien mot de passe et deux fois le nouveau :
L'option " Préférence de fichier", ces paramètre modifient la façon dont nos dossiers sont affichés et manipulés.

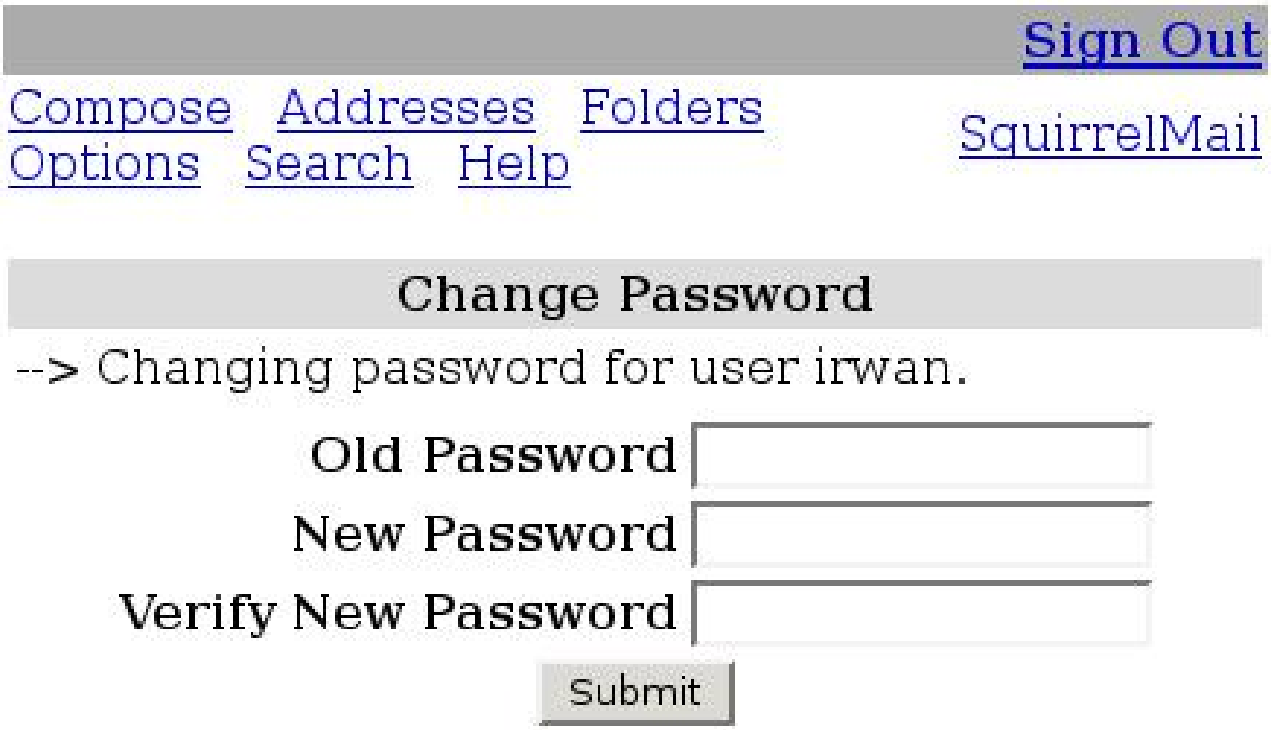


FIGURE 4.38 – Changer le mot de passe

- Filtres La définition des nouvelles règles de filtrage pour la gestion automatiques des messages, nous cliquant sur *Ajouter une nouvelle règle.*
  La page suivante s'affichera :

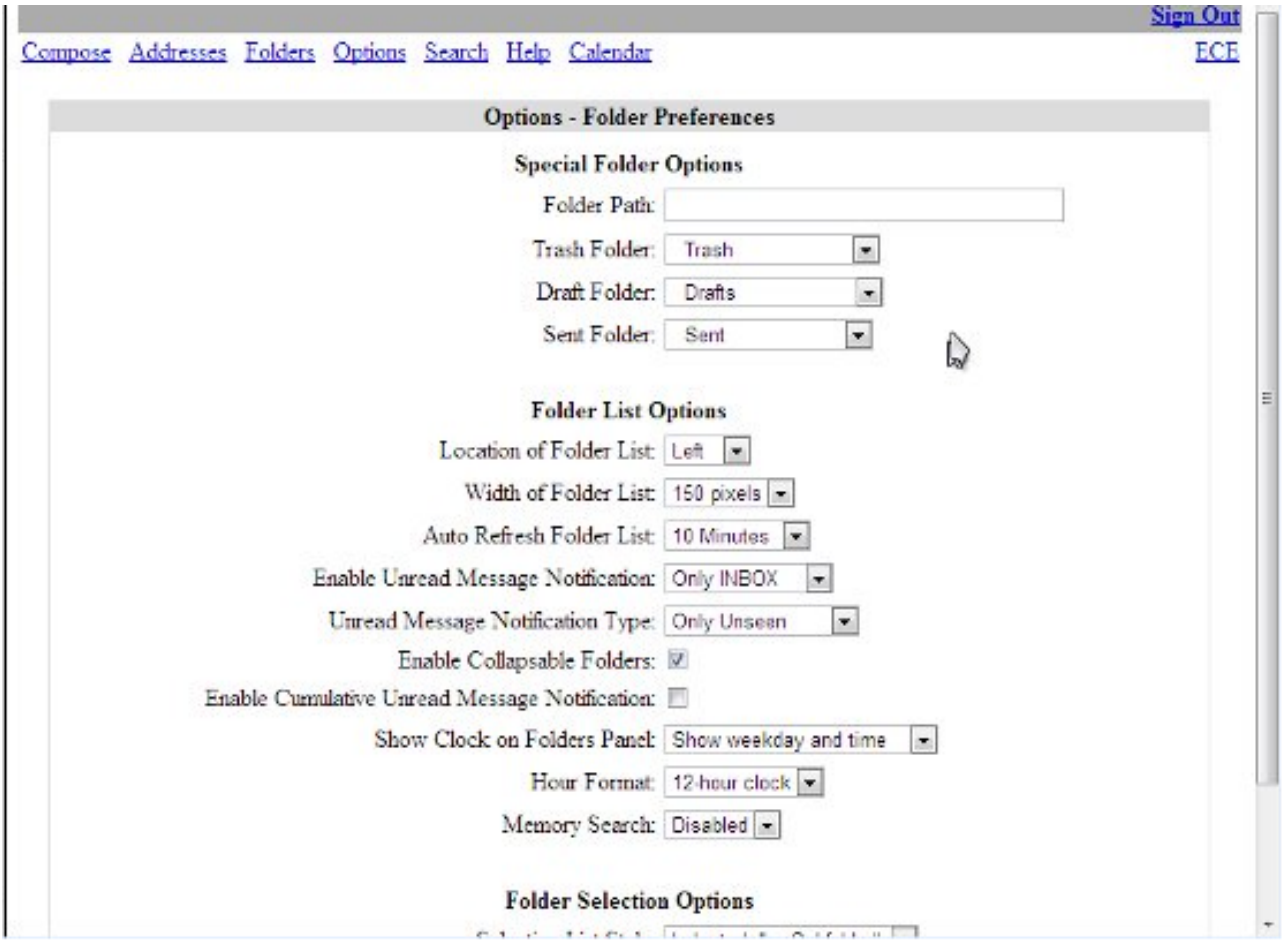


FIGURE 4.39 – Préférence de fichier

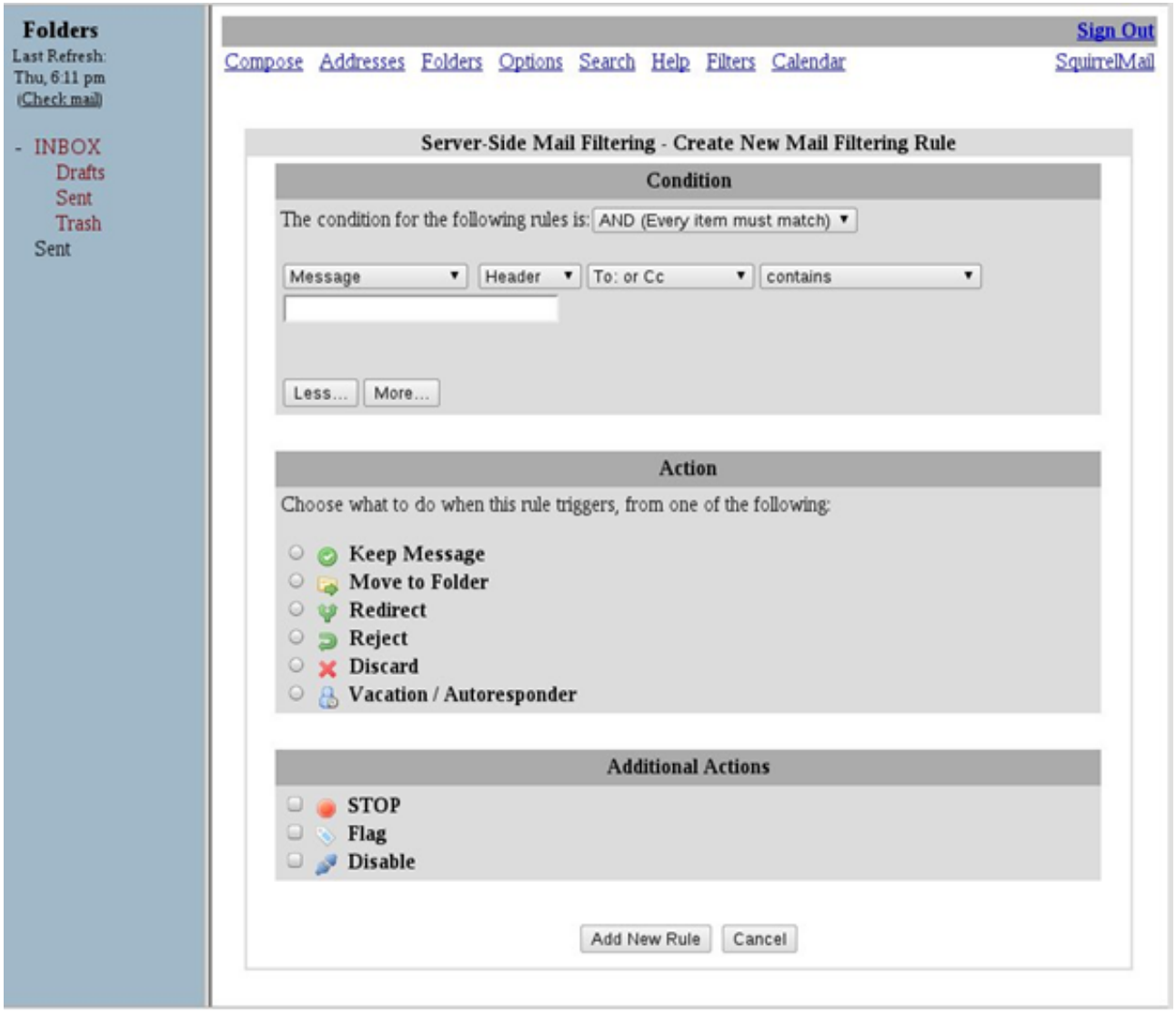


FIGURE 4.40 – Ajouter une règle

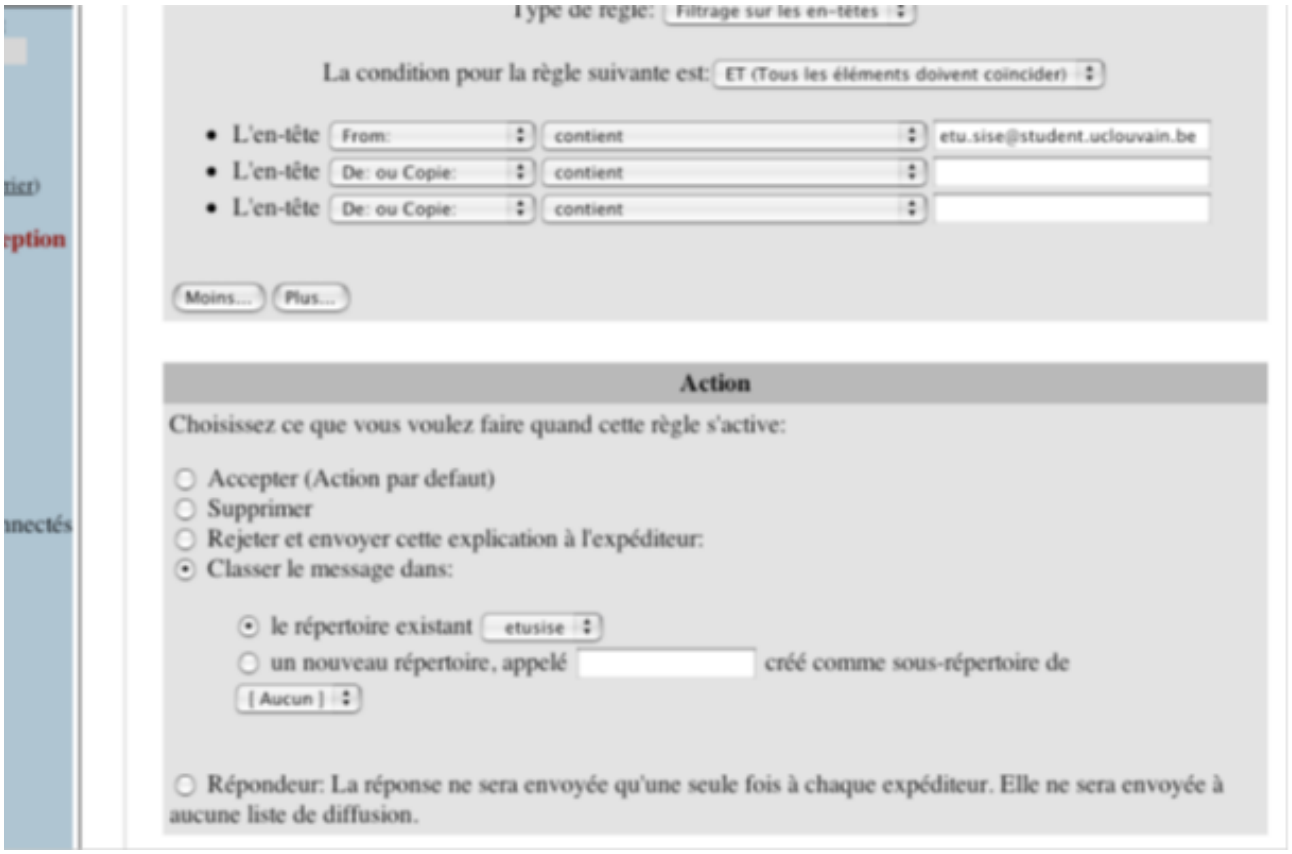


FIGURE 4.41 – Classer un message

L'option filtres nous permet aussi de créer des réponses automatiques aux messages envoyés (Exemple de message d'absence).

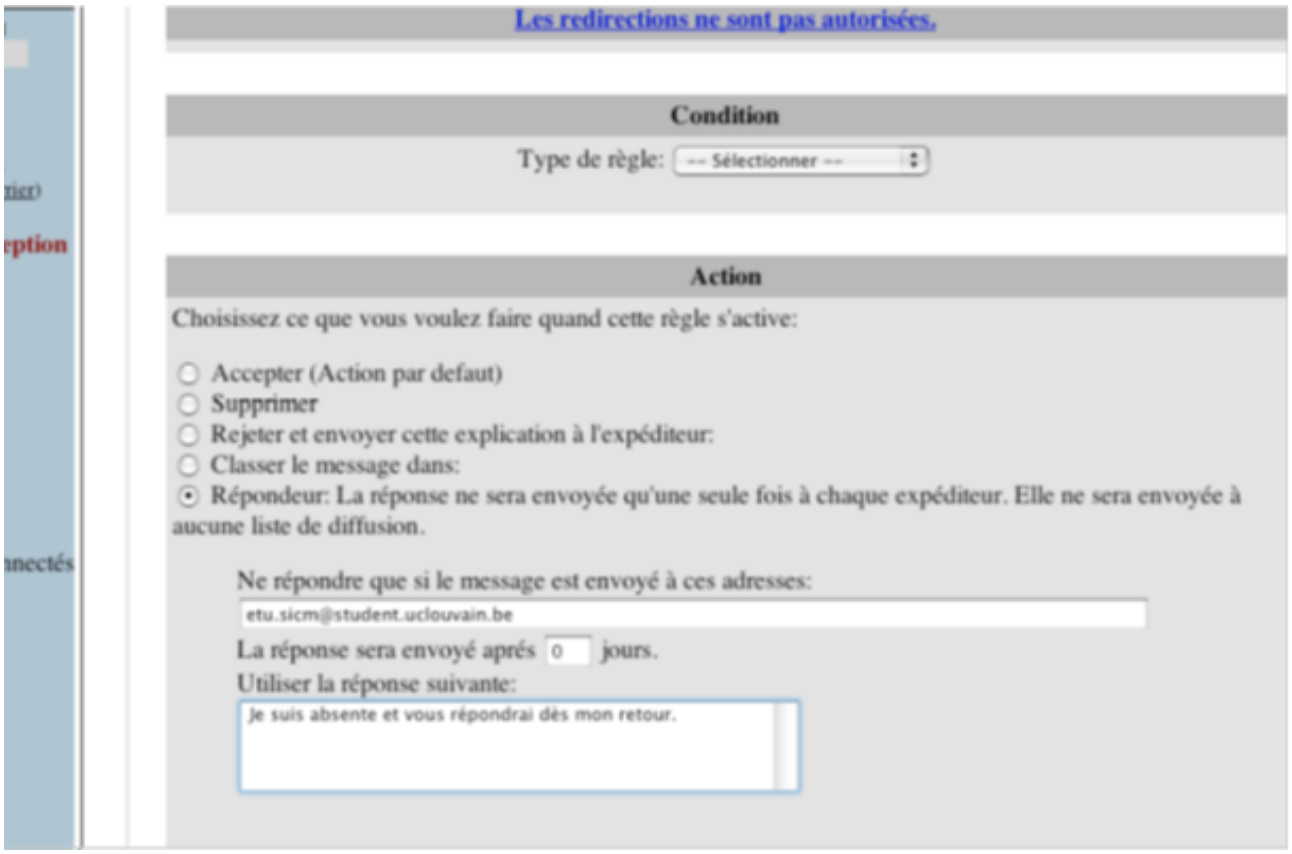


FIGURE 4.42 – Message de réponse automatique

– Gestion du quota

  Nous pouvons voir l'état de notre quota sur la barre de remplissage qui indique le niveau de son utilisation (Cette barre est, verte entre 0 et 70

  Lorsqu'un message est mis à la corbeille, il n'est pas réellement supprimé du serveur, squirrelmail ne fait que le déplacer vers le dossier corbeille et donc l'espace occupé par notre messagerie sur le serveur reste le même.

  Pour la meilleure gestion il faut :

  - Purger régulièrement la poubelle.
  - Compresser les fichiers attachés.
  - Utiliser à bon escient le dossier des messages envoyés.
  - Utiliser à bon escient le dossier des messages envoyés.

4.2 conclusion

Ce chapitre comprend les étapes que nous avons suivies, ces étapes, montrent l'installation et la configuration des différents composants de notre système. Ce moyen de communication est extrêmement facile et pratique. Par contre, il ne faut pas négliger la sécurité.

CONCLUSION GÉNÉRALE

C'est dans le but de mettre en œuvre notre proposition ou suggestion, à la D.O.T de Bejaia, qui est l'administration et la mise en uvre d'un serveur messagerie, que nous avons réalisé ce projet, qui le thème de notre projet fin d'études.

Après avoir étudié les différents facteurs d'un système de messagerie, nous avons opté pour :

- Postfix, comme MTA.
- Squirrelmail, comme MUA.
- Courrier IMAP et courrier POP, comme MDA.
- SSH et SSL, pour la sécurité du serveur.

Ces composants, nous les avons installés et configurés. Les étapes que nous avons suivies, sont citées explicitement dans le chapitre quatre. Ce projet a été une expérience, pour exploiter nos connaissances, nos capacités et d'affronter le domaine professionnel.

En revanche, la sécurité d'un système de messagerie reste un problème majeur ; ce qui nous oblige à être à jour afin de maintenir sa sécurité. Enfin, nous espérons que notre travail saurait satisfaire Algérie Télécom (la D.O.T de Bejaia) et qu'il leur serait d'un bénéfice.

Perspectives :

- Installation de LDAP, pour enregistrer tous les utilisateurs.
- Implémentation de notre système, à la D.O.T de Bejaia.
- Utilisation de TO-IP.

BIBLIOGRAPHIE

[1] ANTIPOLIS.S. Les Réseaux Informatiques, Université de Nice, 2003.

[2] Cours réseaux 3ème année Licence.

[3] Nates-Wireless et Angers- Wireless. 802.11 Les Réseaux sans Fils. INFRACOM.2003.

[4] CAUBERE.B, CONVERSIN.P, COPITET.M, GONEL. JF, HUTIN.T, PAPA-VOINE.F, PEJASACHOWICZ.L, RICHY.P, SALAH.M et SCHAUER.H. Sécurité intranet. Le CLUSIF (Club de la sécurité des Systèmes dInformation Français), 1998.

[5] TRIQUENAUX-MARTIN.V, Sciences et Techniques de lInformation, INTD (Institut National des Techniques de la Documentation), 2005.

[6] GARDRIN .G et GARDRIN. O. Le Client-Serveur. EYROLLES. Paris, 2000.

[7] Pujolle.G, Les réseaux. 6ème édition. EYROLLES. Paris, 2007.

[8] Guy Pujolle, Olivier Salvaton et Jack Nozick. Les Réseaux. 5ème édition. Eyrolles. Paris, 2004.

[9] principe-d-encapsulation-1.html

[10] http : //www.linux−france.org/prj/edu/archinet/systeme/index$_{m}$onopage.html

[11] CHALLE.JF. Administration et Sécurité des Réseaux. HEPCUT-ISIPH. Province de Hainaut.

[12] HOUNTOMEY.JR, Le Routage Statique. NAIROB I. Kenya, 2006.

[13] LOHIER.S et QUIDELLEUR.A. Le Réseau Internet. DUNOD. Paris, 2010.

[14] Cours de sécurité M2

[15] Cours de sécurité, 1ère année Master Informatique.

[16] Cours Réseaux informatiques université de Franche compté

[17]

[18] NAVARRE.F et VEREECKEN.I, Cellule Wall On Line. FUNDP, 2005.

[19] www2.afnor.org/espace-normalisation/structure.aspx ?commid=3175long=french

[20] www.postfix.org