

الجمهورية الجزائرية الديمقراطية الشعبية  
République Algérienne démocratique et populaire

وزارة التعليم العالي والبحث العلمي  
Ministère de l'enseignement supérieur et de la recherche scientifique

جامعة سعد دحلب بليلة  
Université SAAD DAHLAB de BLIDA

كلية التكنولوجيا  
Faculté de Technologie

قسم الإلكترونيك  
Département d'Électronique



# Mémoire de Master

Mention Électronique

Réseaux et Télécommunications (RT)

Présenté par

Berkane Selma

&

Chettah Hanane

---

# Mise en place d'un système de messagerie sous Linux

---

Proposé par : Dr. ANOU Abderrahmane

Année Universitaire 2019-2020.

---

## ملخص:

يعد البريد الإلكتروني أحد أكثر الأدوات شيوعاً على الإنترنت للشركات والأفراد. إنها أداة أساسية وطريقة الاتصال الأكثر استخداماً في الدوائر المهنية. لقد تم تطويره بشكل أكبر في المنظمات خلال العقد الماضي، وذلك بفضل سهولة استخدامه وفائدته المتصورة  
مشروعنا هو بناء نظام مراسلة لجامعة سعد دحلب البلدية لتلبية احتياجاتهم  
بدأنا بشرح بعض المفاهيم الأساسية للرسائل الإلكترونية وتفصيل كيفية عملها والأدوات المستخدمة قبل الانتقال إلى تحقيقها  
كعميل وخادم "Zimbra Collaboration Suite Open Source Edition" يتم الإدراك باستخدام خادم البريد لإدارة البريد

**الكلمات الجوهرية:** الرسائل الإلكترونية، الاتصالات، Zimbra CS، والبريد الإلكتروني.

---

## Résumé :

La messagerie électronique est l'un des outils les plus répandus dans l'Internet des entreprises ou des particuliers. Cet outil indispensable et le mode de communication le plus utilisé dans les milieux professionnels. Elle est beaucoup plus développée dans les organisations aux cours de ces dix dernières années, grâce à sa facilité d'utilisation et son utilité perçue.

Notre projet consiste à réaliser un système de messagerie pour l'université Saad Dahlab Blida 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.

La réalisation est faite en utilisant le serveur de messagerie « Zimbra Collaboration Suite Open Source Edition » comme client et serveur pour la gestion des mails.

**Mots clés :** Messagerie électronique, communication, Zimbra CS, mails.

---

## Abstract:

Email is one of the most common tools in the Internet for businesses or individuals. It is an indispensable tool and the mode of communication most used in professional circles. It is much more developed in organizations over the last ten years, thanks to its ease of use and perceived usefulness.. Our project is to build a messaging system for Saad Dahlab Blida University to meet their needs.. We started by explaining some basic notions of electronic messaging and detailing its operation, the tools used before moving to its realization.

The realization is made using the mail server «Zimbra Collaboration Suite Open Source Edition» as client and server for mail management.

**Keywords:** Email, communication, Zimbra CS, emails.

---

# *Dédicace*

✿ *Je dédie ce mémoire* ✍

*A mes chers parents, pour tous leurs sacrifices, leur amour, leur tendresse, leur soutien et leur prière tout au long mes études,*

*A mes chères sœurs AMINA et RITADJ pour leurs encouragements permanents, et leur soutien moral*

*A mes chers frères, AMINE et KHEIR EDDINE, pour leur appui et leur encouragement, A toute ma famille pour leur soutien tout au long de mon parcours universitaire,*

*Que ce travail soit l'accomplissement de vos vœux tant allégués, et le fruit de votre soutien infailible,*

*A mes chères amies Sarah Hammadouch et Hocine Dounia*

*A ma très chère amie Selma*

*Tu va trouver ici le témoignage d'une fidélité et d'une amétier infinie, tu es et tu resteras toujours dans mon cœur .Merci d'être toujours là pour moi.*



*CHETTAN Hanane*

# *Dédicace*

*Je tiens à dédier vivement ce modeste travail à mes très chers parents auxquels je dois ma réussite et auxquels je ne rendrai jamais assez. Je leurs souhaite une longue vie.*

*A mon frère Rochdi et sa femme Abir*

*A mes sœurs Racha , Ahlem et son marie Kamel*

*A ma chère grande-mère et toute ma famille.*

*A toutes mes amies et leurs familles.*

*A ma binôme Hanane et toute sa famille.*

*A ceux qui m'ont poussé à aller toujours de l'avant.*

*BERKANE Selma*



## *Remerciement*

*Avant de commencer le développement de cette expérience professionnelle, il nous paraît tout naturel de commencer par remercier les personnes qui nous ont permis d'effectuer ce travail ainsi que ceux qui nous ont permis d'en faire un moment agréable et profitable.*

*Nous remercions donc Mr Abderrahmane Anou et Mr Mehdi Meroune, de nous offrir la chance de vivre cette expérience professionnelle et de nous former avec rigueur et patience, Ainsi pour les conseils qu'ils nous ont continuellement prodigués. Et, pour conclure, nous aimons bien remercier Mme Asma et l'ensemble des employés pour l'attention et l'aide qu'ils nous ont apportées au cours de cette expérience.*



# Table des matières

Introduction Générale.....	1
CHAPITRE 1 : Généralité sur les réseaux .....	2
1.1 Introduction .....	2
1.2 Réseaux informatiques .....	2
1.2.1 Définition d'un réseau informatique .....	2
1.2.2 Intérêt d'un réseau .....	2
1.2.3 Classification des réseaux.....	3
1.2.4 Réseau Internet .....	6
1.2.5 L'architecture Client/serveur.....	8
1.3 Les modèles de communication réseau .....	10
1.4 Le routage.....	12
1.4.1 Le routage dans les réseaux.....	12
1.5 Les protocoles .....	13
1.5.1 Protocoles de routage .....	13
1.6 Les serveurs.....	13
1.6.1 Serveur Messagerie .....	14
1.6.2 Serveur DNS (Domain Name Server) .....	14
1.7 Sécurité informatique .....	15
1.7.1 Les objectifs de la sécurité .....	15
1.7.2 Les attaques .....	16
1.8 Sécuriser un LAN.....	16
1.8.1 Le firewall.....	16
1.8.2 Le NAT (NatworkAddress Translation).....	16
1.8.3 Le DMZ (DeMilitarized Zone).....	16
1.8.4 Serveur Proxy .....	17
1.8.5 Le VPN (Virtual Private Network).....	17
1.9 Conclusion.....	17
Chapitre 2 : Serveur de messagerie .....	18
2.1 Introduction .....	18
2.2 Système de messagerie électronique .....	18
2.3 Les agents de la messagerie.....	18
2.3.1 Le Mail Transfert Agent (MTA) .....	18
2.3.2 Le Mail User Agent (MUA) .....	18
2.3.3 Le Mail Access Agent (MAA) .....	19
2.3.4 Le Mail Delivery Agent (MDA).....	19

2.4 Les protocoles de la messagerie .....	20
2.5 Serveur de messagerie .....	23
2.6 Client de messagerie.....	24
2.6.1 Les clients lourds.....	25
2.6.2 Les clients légers .....	25
2.7 Client lourd VS Client léger.....	26
2.8 L'adresse électronique.....	27
2.9 Le message électronique .....	27
2.9.1 Structure d'un message électronique .....	27
2.9.2 Les formats standards d'un message .....	28
2.10 Principaux risques de la messagerie .....	29
2.10.1 Réception/Envoi de virus .....	29
2.10.2 Réception/Envoi messages falsifiés .....	29
2.10.3 Lecture de messages par de tierces personnes.....	29
2.10.4 Perte de message .....	29
2.10.5 Indisponibilité du serveur de messagerie .....	29
2.10.6 Rebond possible pour une attaque en interne .....	29
2.11 Sécurité de la messagerie .....	30
2.12 Les protocoles de sécurité .....	30
2.12.1 Le protocole SSL (Secure Socket Layer) .....	30
2.12.2 Le protocole SSH (Secure Shell).....	31
2.13 Conclusion.....	32
Chapitre 3 : Réalisation .....	34
3.1 Introduction .....	34
3.2 Définitions du serveur de messagerie Zimbra.....	34
3.2.1 Environnement du travail .....	35
3.3 Installation et configuration des composants de la messagerie .....	35
3.3.1 Installation CentOS 7 64 bits version minimale.....	35
3.3.2 Installation de Zimbra .....	39
3.4 Administration de serveur de messagerie.....	46
3.5 Client de messagerie Zimbra.....	52
3.6 Conclusion.....	67
Conclusion générale .....	68
Bibliographie .....	69
Bibliographie .....	70

## Liste des figures

Figure 1. 1 : Classification des réseaux selon l'étendue géographique.....	3
Figure 1. 2: Topologie en bus.....	4
Figure 1. 3: Topologie en anneau.....	5
Figure 1. 4: Topologie en étoile.....	5
Figure 1. 5: Topologie maillée.....	6
Figure 1. 6: Architecture à deux niveaux.....	8
Figure 1. 7: Architecture à trois niveaux.....	9
Figure 1. 8: Architecture multi niveau.....	9
Figure 2. 1: Architecture modulaire d'un système de messagerie Internet.....	19
Figure 2. 2:Principe d'envoi via SMTP.....	20
Figure 2. 3: Principe d'envoi via POP3.....	21
Figure 2. 4: Principe d'envoi via IMAP.....	22
Figure 2. 5: Les quatre principales étapes du trajet d'un courrier électronique.....	22
Figure 3. 1: Installation de CentOS 7.....	35
Figure 3. 2: Configuration des paramètres.....	36
Figure 3. 3: Choix de langue.....	36
Figure 3. 4: Configuration de la carte réseau.....	37
Figure 3. 5: Configuration d'un mot passe.....	37
Figure 3. 6: Redémarrage du système.....	38
Figure 3. 7: Interface de bureau.....	39
Figure 3. 8: Définition d'un nom de la machine.....	39
Figure 3. 9: Définition du nom de domaine de la messagerie.....	40
Figure 3. 10: Configuration de A.....	40
Figure 3. 11: Configuration de MX.....	41
Figure 3. 12: Installations des paquets manquant.....	41
Figure 3. 13: Téléchargement de Zimbra.....	42
Figure 3. 14: Décompression du package Zimbra.....	42
Figure 3. 15: Accéder au dossier décompressé.....	42
Figure 3. 16: Lancement du scripte d'installation du Zimbra.....	43
Figure 3. 17: Exécution de l'installation.....	43
Figure 3. 18: Installations des modules de Zimbra.....	44
Figure 3. 19: Menu des paquets a installé.....	44
Figure 3. 20: Listes des modules de Zimbra installé.....	44
Figure 3. 21: Fin de l'exécution de scripte d'installation.....	45
Figure 3. 22: Création d'un mot de passe pour l'administrateur.....	45
Figure 3. 23: Fin d'installation.....	46
Figure 3. 24: Ouverture de port mail.....	46
Figure 3. 25: Accès l'interface administrateur.....	48
Figure 3. 26: Interface web administrateur.....	48
Figure 3. 27: Page d'accueil d'administrateur.....	48
Figure 3. 28: Vérification de l'état du serveur.....	49
Figure 3. 29: Création d'un compte utilisateur.....	49
Figure 3. 30: Listes des comptes créés.....	50
Figure 3. 31: Les informations de compte.....	50

Figure 3. 32: Quota d'utilisateur.....	51
Figure 3. 33: Le fichier LOGO.....	51
Figure 3. 34: Interface web de l'administrateur.....	52
Figure 3. 35: Accéder au console utilisateur.....	53
Figure 3. 36: Modification d'un mot passe par l'utilisateur.....	53
Figure 3. 37: Page d'accueil d'utilisateur.....	54
Figure 3. 38: L'envois d'un email.....	54
Figure 3. 39: Réception d'email.....	55
Figure 3. 40: Réception d'un mail par un utilisateur.....	55
Figure 3. 41: Ajoute un contact.....	55
Figure 3. 42: Création un groupe de contact.....	56
Figure 3. 43: Stocker un document.....	56
Figure 3. 44: L'envoi d'un document stocké.....	57
Figure 3. 45: Réception d'un document.....	57
Figure 3. 46: Création d'un rendez-vous simple.....	57
Figure 3. 47: Création d'un rendez-vous détaillé.....	58
Figure 3. 48: Réception d'un rendez- vous.....	58
Figure 3. 49: Divers calendrier.....	59
Figure 3. 50: Création d'une tache.....	59
Figure 3. 51: L'envoi d'une tache.....	60
Figure 3. 52: Création une liste de tâche.....	60
Figure 3. 53 : Menu Zimlets.....	60
Figure 3. 54 : Fenêtre chat.....	61
Figure 3. 55: Création dossier spam.....	62
Figure 3. 56: Création filtre.....	62
Figure 3. 57: Réception d'un message spam.....	63
Figure 3. 58 : Affichage fenêtre de filtre.....	63
Figure 3. 59: Création de tag d'un mail.....	64
Figure 3. 60: Création de tag d'un contact.....	64
Figure 3. 61: Gestion des comptes.....	65
Figure 3. 62 : Création d'une réunion.....	65
Figure 3. 63 : Réunion rapide.....	66
Figure 3. 64 : Page d'accueil de client.....	66
Figure 3. 65 : Page d'accueil d'administrateur.....	34

## Liste des tableaux

Tableau 1. 1: Les modèles de couches réseaux.....	10
Tableau 1. 2: les principaux types d'enregistrement DNS.....	15
Tableau 3. 1: Commandes de bas du linux.....	38

## Listes des acronymes et abréviations

COS	Class Of Service
DMZ	DeMilitarized Zone
DNS	Domain Name Server
GAL	List global d'adresse
IMAP	Interactive Mail Access Protocol
LAN	Local Area Network
MAN	Metropolitan Area Network
MDA	Mail Delivery Agent
MIME	Multipurpose Internet Mail Extension
MTA	Mail Transfert Agent
MTU	Maximum Transmission Unit
MUA	Mail User Agent
MX	Mail eXchanger
NAT	Network Address Translation
OSI	Open System Interconnection
POP3	Post Office Protocol version 3
SMTP	Simple Mail Transfer Protocol
SSH	Secure SHell
SSL	Secure Socket Layer
TCP/IP	Transmission Control Protocol / Internet Protocol
VPN	Virtual Private Network
WAN	Wide Area Network

# Introduction Générale

## Introduction Générale

Depuis les origines, l'homme a eu besoin de communiquer. Pour cela, il a mis au point des codes, des alphabets et des langages (Parole, gestes de la main, tam-tam, document écrit...etc.) pour véhiculer le message. La communication n'a pas cessé de se développer, devenant ainsi de plus en plus technique. Il s'agit d'une notion moderne, qui n'a fait qu'évoluer jusqu'à devenir aujourd'hui un élément fondamental de la stratégie d'entreprise.

Pour cette raison les technologies de l'Information et de la Communication (TIC) ont bouleversé les modes traditionnels de circulation de l'information en apportant de nouvelles formes de circulation de l'information, un partage plus facile, une diffusion plus rapide qui est la messagerie électronique.

Ce mémoire présente le fruit d'un travail de quatre mois portant sur la réalisation d'un serveur de messagerie consiste à le mettre en exploitation pour l'administration de l'université Saad Dahlab (Blida1) actuel.

Nous allons essayer de présenter dans ce rapport les objectifs de notre développement, ainsi que la méthodologie de travail employée pour arriver aux résultats voulus.

Pour cela nous avons proposé :

La solution Zimbra est un logiciel serveur collaboratif qui permet à ses utilisateurs de stocker, organiser et partager rendez-vous, contacts, courriels, liens, documents et plus, est un logiciel développé sur un mode "Web service" : Son interface entièrement en AJAX est chargée à la première connexion, puis les interactions et ajouts/modification d'informations sont envoyés au serveur par le protocole SOAP.

Notre travail est décomposé en deux grandes parties : la première consiste à étudier théoriquement la spécification des besoins et la seconde consiste en la phase pratique de l'application.

Nous allons exposer le plan du mémoire qui se subdivise en trois 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 élaborons une présentation d'une manière théorique des éléments important au déroulement et fonctionnement de la messagerie électronique.

En dernier, dans le troisième chapitre, nous illustrons les différentes étapes que nous avons suivies, pour la mise en œuvre et l'administration de notre serveur de messagerie.

# CHAPITRE 1

# CHAPITRE 1 : Généralité sur les réseaux

## 1.1 Introduction

Historiquement l'informatique s'est développée autour de la saisie, du traitement et de la mise à disposition de données structurées. Mais avec l'évolution de l'intranet et des technologies de l'information et de la communication, il ne s'agit plus de traiter des données : les ordinateurs sont utilisés pour envoyer du courrier (messagerie), partager les agendas, diffuser la documentation, etc. La messagerie électronique constitue alors un moyen de communication, utilisés dans différents environnements professionnels : entreprises privées et publiques, collectivités locales, administrations, institutions et ministères. Avant d'entamer ce concept, dans ce chapitre nous allons voir quelques généralités sur les réseaux, en particulier le réseau Internet ainsi que ses services ensuite nous allons expliquer le routage dans les réseaux, après on va définir le DNS, et enfin nous définissons la sécurité informatique et nous expliquerons les différentes manières pour sécuriser un réseau local.

## 1.2 Réseaux informatiques

### 1.2.1 Définition d'un réseau informatique

C'est un ensemble d'objets (ordinateurs, stations de travail, cartes réseau, imprimantes...) reliés entre eux. La connexion entre ces éléments peut se faire de manière physique (connexion filaire avec prise Ethernet), ou via des ondes radio (connexion sans fil, wifi).

Le but des réseaux informatiques est d'assurer le partage des différentes ressources matériels et logiciels (fichiers, applications, imprimantes...) et la communication par l'échange des informations d'une manière simple, rapide et efficace entre les stations.

### 1.2.2 Intérêt d'un réseau

Un réseau informatique peut servir plusieurs buts distincts :

- Partage et centralisation des informations (fichiers, ressources, applications).
- Economie du matériel (grâce au partage des périphériques : imprimantes, scanners, etc.).
- La communication entre processus (entre des ordinateurs industriels par exemple).
- La garantie de l'unicité et de l'universalité de l'accès à l'information (bases de données en réseau).
- Le jeu vidéo multijoueur.

### 1.2.2.1 Les inconvénients majeurs des réseaux informatiques sont [1]:

- Problèmes de sécurité.
- La propagation rapide de virus informatiques.

### 1.2.3 Classification des réseaux

On peut distinguer plusieurs types de réseaux pouvant être classés selon plusieurs critères, dont les principales sont : l'étendue géographique et la topologie [2].

#### 1.2.3.1 Classification selon l'étendue géographique

En fonction de localisation, la distance et le débit, les réseaux sont classés en quatre types [3] : PAN, LAN, MAN, WAN.

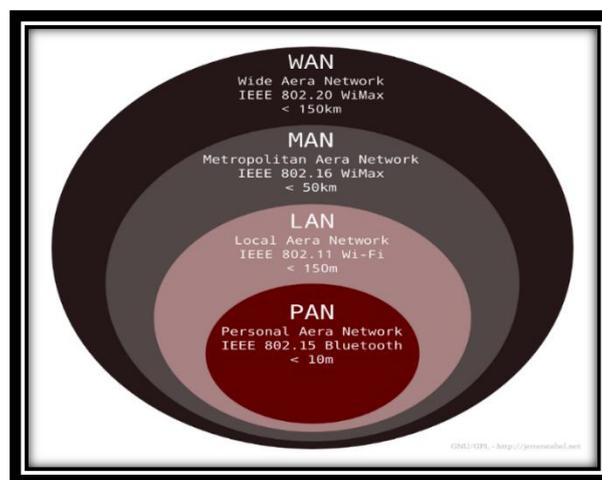


Figure 1. 1 : Classification des réseaux selon l'étendue géographique.

#### A. PAN (Personal Area Network)

Réseau personnel, généralement mis en œuvre dans un espace d'une dizaine de mètres reliant ainsi des périphérique (imprimantes, téléphones portables, etc.) à un ordinateur personnel avec une liaison câblée ou sans fil (ex : par Bluetooth).

#### B. LAN (Local Area Network)

Réseau local d'entreprise, représentant un ensemble d'ordinateurs interconnectés dans une petite aire géographique, de manière relativement simple pour l'échange de données et le partage de ressources.

#### C. MAN (Métropolitan Area Network)

Réseau métropolitain, qui correspond à la réunion de plusieurs réseaux locaux "LAN" à l'échelle d'une ville.

## D. WAN (Wide Area Network)

Réseau informatique étendu, couvrant une grande zone géographique, typiquement à l'échelle d'un pays, d'un continent, le plus grand WAN est le réseau internet.

### 1.2.3.2 Classification selon la topologie

La topologie représente l'arrangement physique des différents matériels constituant le réseau. Les principales topologies sont les suivantes [4]:

#### A. Topologie en bus

Les ordinateurs sont reliés à une même ligne de transmission par l'intermédiaire de câbles, généralement coaxial, débutés et terminés par des terminateurs (bouchons). Le principe de cette topologie consiste à ce qu'un message véhiculé par le canal peut être reçu par toutes les stations, ce qui va causer des problèmes de sécurité. Ce type de montage est facile à mettre en œuvre et peu coûteux, mais s'il y avait une rupture du câble, tout le réseau tomberait en panne.

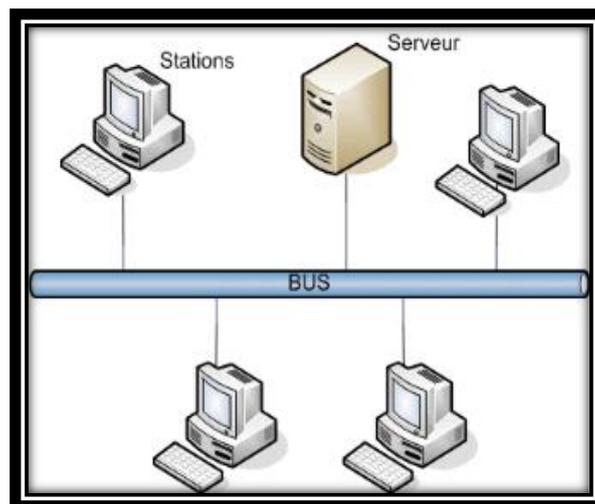


Figure 1. 2: Topologie en bus.

#### B. Topologie en anneau

Les ordinateurs sont situés sur une boucle et communiquent chacun à leur tour. Une machine connectée au réseau possède un jeton virtuel (autorisation de Communiquer). Une fois que la machine a transmis ce qu'elle voulait, elle passe le jeton à la machine suivante, et ainsi de suite. Si le détenteur du jeton n'a rien à dire, il le passe au suivant. Cette topologie permet un accès égal pour tous les ordinateurs, mais la panne d'un ordinateur peut infecter le reste du réseau.

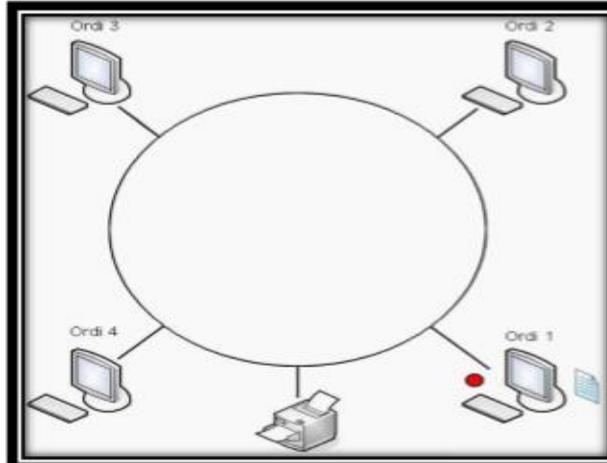


Figure 1. 3: Topologie en anneau.

### C. Topologie en étoile

La figure ci-dessous représente l'architecture d'un réseau étoile. Dans cette topologie, tous les équipements sont reliés à un point central (concentrateur, commutateur, routeur...) qui a pour rôle d'assurer la communication entre les différentes machines. L'avantage de cette topologie est que La panne d'une station ne perturbe pas le fonctionnement du réseau et il est facile d'ajouter des stations ou de procéder à des modifications. L'inconvénients est que si le point central tombe en panne le réseau devient inutilisable.

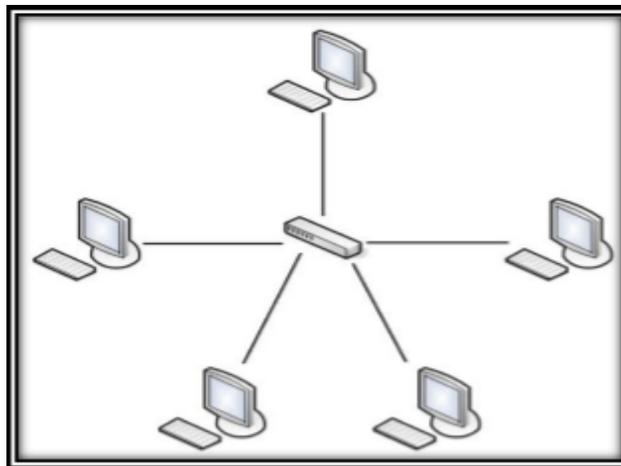


Figure 1. 4: Topologie en étoile.

### D. Topologie maillée

La topologie maillée est une évolution de la topologie en étoile. Elle utilise plusieurs chemins de transferts entre les différents nœuds (Exemple : internet). En cas de rupture d'un lien, l'information peut quand même être acheminée, mais cette topologie nécessite beaucoup de câble.

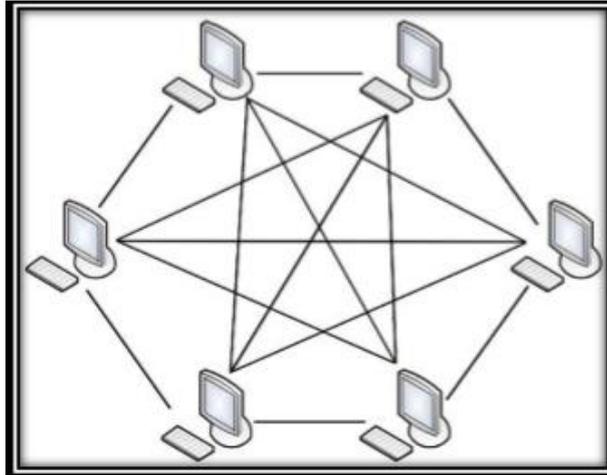


Figure 1. 5: Topologie maillée.

## 1.2.4 Réseau Internet

### 1.2.4.1 Définition

L'Internet est un système d'interconnexion de machines qui constitue un réseau informatique mondial, utilisant un ensemble standardisé par un protocole de transfert de données (TCP/IP : Transfert Control Protocol / Internet Protocol). Ce modèle peut être considéré comme un langage commun par des ordinateurs aux architectures diverses pour échanger des informations sur un réseau.

L'Internet n'est pas en lui-même un réseau primitif d'ordinateurs mais représente plutôt une multitude des réseaux reliés entre eux au fil du temps pour constituer un réseau des réseaux (Interconnected Networks) [5].

#### ➤ **Internet aujourd'hui :**

Actuellement c'est la version 4 (IPV 4) du protocole IP qui est utilisée permettre aux machines de dialoguer entre elles. Ce qui ne va pas sans poser de multiples problèmes [6] :

- Manque d'adresse IP
- Vitesse de transmission trop faibles devant des fichiers de plus en plus gros (vidéo)
- Manque de sécurité (spam, virus...)

#### ➤ **Internet de demain :**

Actuellement un réseau IPV6 et tester aux États-Unis.

Ce réseau s'appelle internet 2. Il a pour but de permettre aux Instituts stratégiques (armée, universités, très grosse entreprises) de pouvoir communiquer efficacement maintenant que

Internet est saturé par les particuliers qui ne cessent de s'envoyer photos, musiques et films... Le problème majeur est que IPv6 n'est pas compatible avec IPv4 on prévoit donc un basculement vers IPv6 sans doute en commençant par tous les gros Instituts dans le monde.

Le système d'exploitation (Unix, Linux, MacOS X, Windows...) sont déjà en général capables de comprendre IPV6.

Le basculement se fera par la mise à jour des applications (comme le navigateur et le logiciel de messagerie) un peu comme l'arrivée du premier navigateur avait changé notre mode de fonctionnement [6].

#### **1.2.4.2 Les services de l'Internet**

L'Internet est un outil capable de nous rendre un certain nombre de services. Voici une liste des différents services les plus utilisés sur Internet, les plus importants seront détaillés dans la suite du rapport [7] :

➤ **Le courrier électronique (e-mail) :**

Permet aux internautes qui possèdent une adresse e-mail de s'expédier mutuellement des messages dans le monde entier. Les messages sont expédiés et reçus grâce à deux protocoles (SMTP et POP).

➤ **FTP (File Transfer Protocol) :**

Le FTP est un protocole de transfert de fichiers. Ce transfert s'effectue en établissant une connexion entre un serveur FTP et un client FTP situé sur votre ordinateur. Les fichiers échangés sont des fichiers informatiques de tous types (texte, images, sons, logiciels, ...)

News : ce sont des espaces de discussions où des groupes discutent en temps différé. Les news sont regroupés par thèmes d'intérêt, appelés newsgroups ou forums.

➤ **Telnet et SSH :**

Ces services permettent à un internaute de se connecter et donc d'utiliser à distance une machine comme s'il se trouvait face à elle. Cela ouvre par exemple des possibilités pour le travail à domicile, puisqu'il devient possible d'utiliser les machines se trouvant sur son lieu de travail depuis chez soi [8].

➤ **Le World Wide Web (WWW) :**

Ce service permet d'accéder à des pages, appelées pages Webs. Une page Web est écrite en langage HTML et peut contenir du texte, des images, des séquences vidéo, du son et des liens. Ces liens permettent de passer d'une page Web à une autre. Le protocole utilisé est http (HyperText Transfer Protocol) [9].

Le système fonctionne selon une architecture client/serveur, qui désigne le mode de communication entre plusieurs composants.

## 1.2.5 L'architecture Client/serveur

### 1.2.5.1 Définition

L'architecture client-serveur est un modèle de fonctionnement logiciel qui se réalise sur tout type d'architecture matérielle (petites à grosses machines), à partir du moment où ces architectures peuvent être interconnectées.

On parle de fonctionnement logiciel dans la mesure où cette architecture est basée sur l'utilisation de deux types de logiciels, à savoir un logiciel serveur et un logiciel client s'exécutant normalement sur 2 machines différentes [10].

### 1.2.5.2 Les types de l'architecture client/serveur

Les différents types de l'architecture client/serveur sont exposés ci-après [11] :

#### A. Architecture à deux niveaux

L'architecture à deux niveaux caractérise les systèmes clients/serveurs pour lesquels le client demande une ressource et le serveur la lui fournit directement, en utilisant ses propres ressources. Cela signifie que le serveur ne fait pas appel à une autre application afin de fournir une partie du service (sans passer par un service intermédiaire) [12].

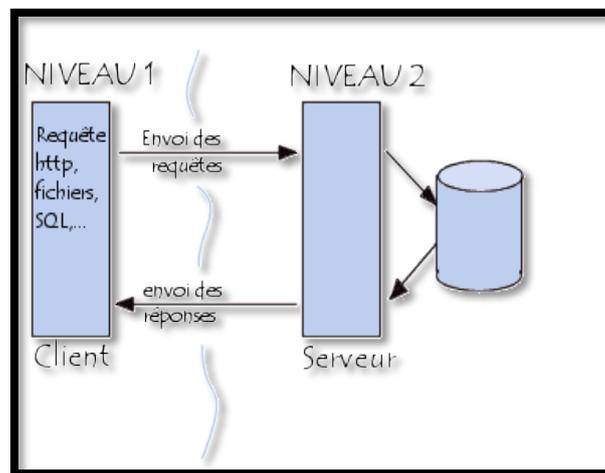


Figure 1. 6: Architecture à deux niveaux.

#### B. Architecture à trois niveaux

Dans l'architecture à 3 niveaux, il existe un niveau intermédiaire, c'est-à-dire que l'on a généralement une architecture partagée entre :

1. Un client, c'est-à-dire l'ordinateur demandeur de ressources, équipée d'une interface utilisateur (généralement un navigateur web) chargée de la présentation.
2. Le serveur d'application (appelé également middleware), chargé de fournir la ressource mais faisant appel à un autre serveur.
3. Le serveur de données, fournissant au serveur d'application les données dont il a besoin.

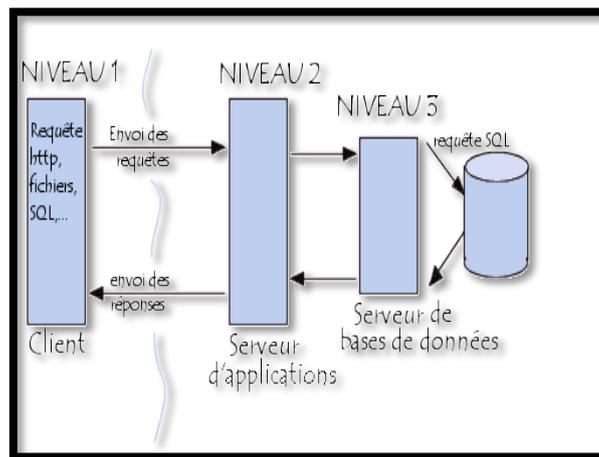


Figure 1. 7: Architecture à trois niveaux.

### C. Architecture multi-niveau

Dans l'architecture à N niveaux, chaque serveur (niveaux 2 et 3) exécute une tâche (un service) spécifique. Un serveur peut donc utiliser les services d'un ou plusieurs autres serveurs afin de fournir son propre service.

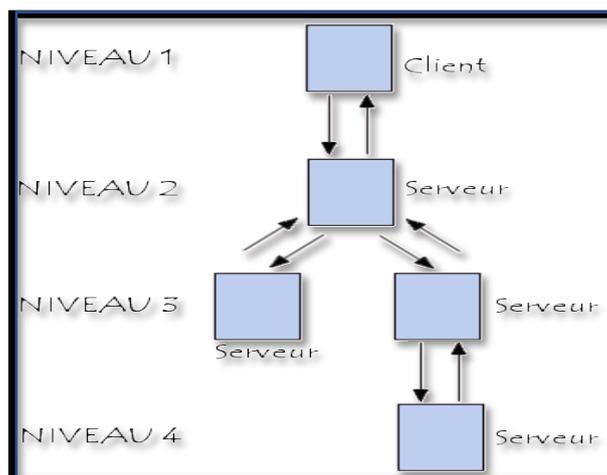


Figure 1. 8: Architecture multi niveau.

### 1.3 Les modèles de communication réseau

Les modèles de communication entre utilisateurs réseau les plus répandus 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.

Le modèle **TCP / IP** a été développé avant le modèle **OSI** et, par conséquent, les couches diffèrent. En ce qui concerne l'image ci-dessous, il est clairement vu que le modèle **TCP / IP** a quatre couches : Réseau, Internet, Transport et Application. La couche Application de **TCP / IP** est une combinaison des couches Session, Présentation et Application du modèle **OSI**.

Les deux modèles OSI et TCP/IP sont présentés comme suit (sur le tableau 1.1) :

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

Tableau 1. 1: Les modèles de couches réseaux.

Nous décrivons brièvement chacune des 7 couches du modèle OSI [13] :

- Application : Transfert des fichiers des applications s'exécutant sur l'ordinateur.
- Présentation : Codage des données selon un mode approprié.
- Session : Gestion des connexions entre les ordinateurs.
- Transport : Gestion du transfert des données vers le destinataire.
- Réseau : Schéma général d'interconnexion (adressage) afin d'assurer le repérage physique du destinataire.
- Liaison : Règles permettant d'effectuer le réassemblage et l'acheminement des données vers le matériel physique de la couche 1.
- Physique : Description physique du transport des données à travers des câbles, des hubs...

Le protocole TCP permet de :

- ✓ Gérer les ports.
- ✓ Vérifier l'état du destinataire pour assurer la réception des paquets.

- ✓ Gérer les paquets IP :
  - Découpe des paquets.
  - Vérification de la réception de tous les paquets.
  - Redemande des paquets manquants.
- ✓ Assemblage des paquets arrivés.

Plusieurs protocoles plus généraux sont fondés sur TCP/IP : DNS, SMTP, FTP, POP3, HTTP tel que :

**DNS** : est un protocole permettant de convertir un nom de domaine Internet en une adresse IP

**SMTP** : est un protocole d'envoi de messages électroniques (mails) vers un destinataire hébergeant la boîte aux lettres.

**POP3** : est un protocole permettant de rapatrier sur votre machine personnelle le courrier qui a été déposé dans la boîte aux lettres de l'hébergeur.

**FTP** : est un protocole permettant de rapatrier sur votre machine ou d'expédier à partir de votre machine des fichiers binaires quelconques.

**HTTP** : est un protocole permettant d'envoyer et de recevoir sur votre machine des fichiers HTML au format ASCII.

Attention : Protocoles de transfert non sûrs, c'est-à-dire que les données circulent en clair sur le réseau.

### 1.3.1 Différences clés entre TCP / IP et le modèle OSI

Dans ce paragraphe on va exposer les différences clés entre TCP/IP et le modèle OSI [6] :

- ✓ **TCP / IP** est un modèle client-serveur, c'est-à-dire lorsque le client demande un service, il est fourni par le serveur. Tandis que, le modèle **OSI** est un modèle conceptuel.
- ✓ **TCP / IP** est un protocole standard utilisé pour tous les réseaux, y compris Internet, tandis que **OSI** n'est pas un protocole mais un modèle de référence utilisé pour comprendre et concevoir l'architecture du système.
- ✓ **TCP / IP** est un modèle à quatre couches, tandis que **OSI** a sept couches.
- ✓ **TCP / IP** suit l'approche verticale. Alors, le modèle **OSI** prend en charge l'approche horizontale.
- ✓ **TCP / IP** est réel, par contre **OSI** est conceptuel.
- ✓ **TCP / IP** suit une approche de haut en bas, tandis que le modèle **OSI** suit une approche ascendante.

### 1.3.2 La messagerie électronique

Le courrier électronique est considéré avec le web comme étant le service le plus utilisé sur l'internet. Ainsi la suite de protocole TCP /IP offre une panoplie de protocole permettant de gérer facilement routage du courrier sur le réseau. Cette partie sera plus détaillée dans le chapitre deux [14].

## 1.4 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.

Le routage définit le chemin emprunté par les paquets entre son point de départ et son point d'arrivée [15].

### 1.4.1 Le routage dans les réseaux

L'internet n'est rien d'autre qu'un immense réseau de lien et d'interconnexion entre plusieurs réseaux. Il faut qu'un protocole de routage ait été mis en place. Le but du routage est de définir une route ou un chemin a un paquet quand celui-ci arrive sur un routeur. Le but du routage est donc d'assurer qu'il existe toujours un chemin pour aller d'un réseau a un autre .il existe deux modes de routages bien distincts lorsque nous souhaitons aborder la mise en place d'un protocole de routage [16].

#### A. Routage Statique :

Les informations sont mises à jour manuellement à chaque modification topologique de l'inter réseau par l'administrateur du réseau, conçu pour des petits réseaux de quelques routeurs.

**Avantages :** économie de bande passante, sécurité, connaissance du chemin à l'avance.

#### B. Routage Dynamique :

Les informations relatives à la route sont mises à jour automatiquement entre les routeurs. Sans intervention manuelle de l'administrateur du réseau. Conçu pour des réseaux a forte évolution ou pour les réseaux de grande taille.

**Avantages :** une maintenance réduite, une modularité et une flexibilité accrue, et sa mise en place ne dépendent pas de la taille du réseau.

### 1.4.2 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). Les enregistrements MX désignent un hôte appelé échangeur de messages qui traite le courrier et le transmet : [17].

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

## **1.5 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 [18].

### **1.5.1 Protocoles de routage**

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

## **1.6 Les serveurs**

Un serveur est un ordinateur dont la fonction est d'assurer l'adressage de logiciels ou de données aux ordinateurs connectés, nommés ordinateurs clients.

Dans un réseau informatique, le ou les serveur(s) sont la clé de voûte du système : ils adressent les fichiers aux postes clients qui en font la demande. 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.

### **1.6.1 Serveur Messagerie**

Un serveur de messagerie électronique est un logiciel qui, connecté à Internet, permet à ses utilisateurs d'envoyer et de recevoir des courriers électroniques

L'échange de messages et des fichiers peut être fait grâce 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 boîte 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...) [18].

Cette partie sera plus détaillée dans le chapitre deux.

### **1.6.2 Serveur DNS (Domain Name Server)**

#### **1.6.2.1 Définition de serveur DNS**

Le serveur DNS (Domain Name System. Ou système de nom de domaine français) est un service dont la principale fonction est de traduire un nom de domaine en adresse IP. Pour simplifier le serveur DNS est un peu l'annuaire que consulte un ordinateur au moment d'accéder à un autre ordinateur via un réseau. Autrement dit, le serveur DNS est ce service qui permet à site web (ou un ordinateur connecté ou un serveur) une adresse IP [19].

#### **1.6.2.2 La résolution des noms**

Le Domain Name System a donc été mis en place pour identifier de manière plus simple les différents sites Web : il s'agit d'un système de "traduction" des adresses IP, adresses attribuées de manière unique à chaque machine connectée à l'Internet (les adresses IP sont en quelque sorte l'analogie des numéros de téléphone). L'opération de traduction est appelée la "résolution du nom (de domaine)" et doit être parfaitement maîtrisée (de même qu'un numéro de téléphone doit bien aboutir à l'établissement de la bonne communication). C'est le rôle de l'ICANN que d'assurer le bon déroulement de la résolution des noms [19].

## 1.7 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 qui sont résumé dans le tableau suivant [20] :

Enregistrement	Signification
• 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 inaddr.arpa.

Tableau 1. 2: les principaux types d'enregistrement DNS.

### 1.7.1 Les objectifs de la sécurité

On doit assurer :

#### 1. La confidentialité

Seules 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

C'est pour assurer l'accessibilité des entités authentifiées du système d'information aux ressources de ce système et pour sécuriser l'information il faut aussi :

- Le matériel (là où elle se trouve).
- Les applications (qui traitent l'information).
- Les supports (moyen de son transport), de l'information.

#### 1.7.2 Les attaques

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.
2. **Active** : dans ce type d'attaque l'intrus peut changer le message ou fabriquer, 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) [20].

### 1.8 Sécuriser un LAN

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

#### 1.8.1 Le firewall

Le firewall ou le pare-feu est chargé de filtrer les accès entre le réseau local et le réseau externe [18].

#### 1.8.2 Le NAT (NetworkAddress 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 [14].

#### 1.8.3 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 [18].

### 1.8.4 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 [14] :

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.

### 1.8.5 Le 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. 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 [18].

## 1.9 Conclusion

Dans ce chapitre, nous avons pris en charge de présenter les déférents termes qui sont en relation avec notre thème. Une brève définition sur les réseaux informatiques, 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 qu'aurons besoin. Dans le chapitre suivant, nous expliquons le serveur de messagerie.

# CHAPITRE 2

## **Chapitre 2 : Serveur de messagerie**

### **2.1 Introduction**

La messagerie électronique est l'une des applications d'Internet les plus anciennes premières messageries électroniques datent des années 60 et le premier protocole de messagerie sur ARPANET a été créé en 1972. Aujourd'hui, l'e-mail est l'application d'Internet la plus populaire et la plus répandue au monde. Le courrier électronique deviendra très vite la première application d'Arpanet utilisée par les chercheurs universitaires (alors seuls utilisateurs de réseau), alors que le réseau avait été conçu pour le partage des ressources informatiques...

Dans ce chapitre, nous nous consacrerons sur les éléments à apporter et ce qu'il faut connaître, afin d'installer et mettre en œuvre un serveur de messagerie [21].

### **2.2 Système de messagerie électronique**

Un système de messagerie électronique est l'ensemble des éléments contribuant à transmettre un courriel (courrier électronique : message transmis via un réseau informatique) de l'émetteur au récepteur.

### **2.3 Les agents de la messagerie**

Il y a quatre éléments fondamentaux pour assurer les échanges de courriers : le Mail Transfert Agent (MTA), le Mail Delivery Agent (MDA) et le Mail User Agent (MUA). Le Mail Access Agent (MAA)

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

Le MTA est un programme qui permet d'envoyer le message d'un serveur à un autre. Ce logiciel est situé sur chaque serveur de messagerie. Il est composé d'un agent de routage et d'un agent de transmission. Il envoie le message via un protocole sortant. Notons que les protocoles sortants permettent de gérer la transmission du courrier entre les systèmes de messagerie [22].

#### **2.3.2 Le Mail User Agent (MUA)**

Sert pour l'expéditeur et le destinataire, est un logiciel client pour le MTA. Il formate les messages en partance afin de les donner au MTA, est un client pour le MDA il formate les messages de la boîte aux lettres afin de les afficher sur écran [22].

### 2.3.3 Le Mail Access Agent (MAA)

Agent d'accès aux messages son rôle est de Permettre à un MUA d'accéder à une boîte à lettre. Versions protocole propriétaire et surtout version POP ou IMAP. Quelques versions : qpopper (protocole POP3), courrier\_imap (POP et IMAP).

### 2.3.4 Le Mail Delivery Agent (MDA)

Le MDA est un agent qui est en charge de la gestion des boîtes aux lettres. Il prélève le courrier dans les files d'attente du MTA et le dépose dans le répertoire de boîtes aux lettres de l'utilisateur. Pour cela il est souvent considéré comme le point final d'un système de messagerie. Il est possible de placer des fonctions de sécurité à ce niveau : appels antivirus et ou anti-spam [22].

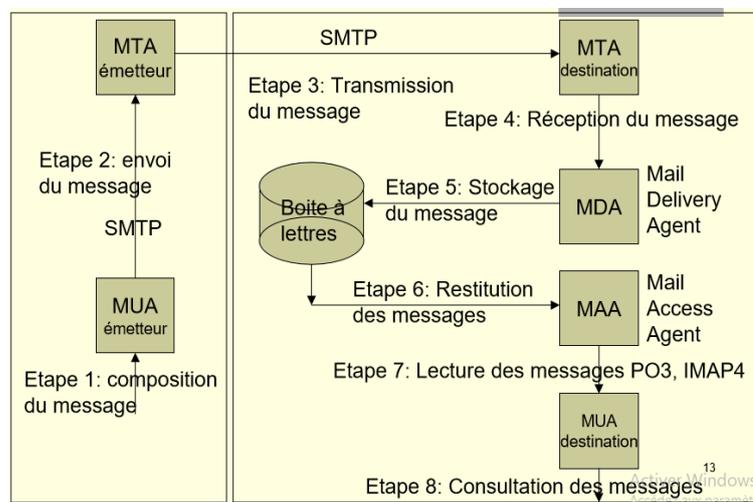


Figure 2. 1: Architecture modulaire d'un système de messagerie Internet.

#### Détail des étapes (1) [23]

Etape 1 : Un usager compose, avec l'aide de son client de messagerie (MUA) un message.

Etape 2 : Le message est transmis au MTA de l'usager (son serveur de messagerie en SMTP).

Etape 3 : Le message est transmis au serveur de messagerie du destinataire (SMTP).

Etape 4 : Le serveur transmet le message à un agent : notion d'agent MDA 'Mail Delivery Agent'.

Etape 5 : Le MDA stocke le courrier dans la boîte à lettres du destinataire. "

Etape 6 : Sur requête du destinataire dans le cadre d'un protocole de relève POP ou IMAP les messages sont extraits de la boîte à lettre par un agent : MAA ('Mail Access Agent'). "

Etape 7 : Les messages sont transmis au client de messagerie utilisateur (protocoles POP ou IMAP). Ils sont stockés dans des boîtes à lettre client. "

Etape 8 : Le destinataire consulte ses messages en utilisant son client de messagerie (MUA).

## 2.4 Les protocoles de la messagerie

Le fonctionnement du courrier électronique repose sur une série de protocoles de communication destinés à envoyer ses messages, de serveur à serveur, à travers l'Internet. Les principaux protocoles sont les suivants : SMTP, POP3 ou encore IMAP, chacun jouant un rôle bien précis.

### 1. Le SMTP

Le Simple Mail Transfer Protocol traduit en Protocole Simple de Transfert de Courrier sert à l'envoi des messages électroniques, il gère les courriers sortant sur internet. En d'autres mots, il est le protocole qui gère le transfert de mails d'un serveur à un autre. Il est commencé fortement à être utilisé dans les années 1980 et le premier serveur de messagerie électronique à utiliser le SMTP est le logiciel Sendmail créé en 1983. De nos jours, la plupart des serveurs, clients messagerie ou webmail utilise le SMTP pour envoyer des mails. Le port 25 est celui généralement utilisé par le serveur pour recevoir une connexion. Le gros défaut du protocole SMTP, c'est que les messages ne sont pas protégés une fois envoyés sur le réseau. Il est donc tout à fait possible de s'emparer de trames, de lire des données non cryptées. Pour parer à cette erreur, certaines personnes ont recours à une méthode de codage de leurs mails importants. Il y a bien sûr d'autres anomalies comme par exemple : si quelqu'un si connaît bien en SMTP, il peut à partir des commandes disponibles modifier l'adresse d'envoi du mail et donc se faire passer pour n'importe qui. Il faut aussi bien faire attention aux serveurs SMTP qui sont mal configurés ou mal sécurisés, les spammeurs peuvent facilement s'introduire pour se servir de votre serveur comme relai pour envoyer des spam et des pourriels difficilement repérables [24].

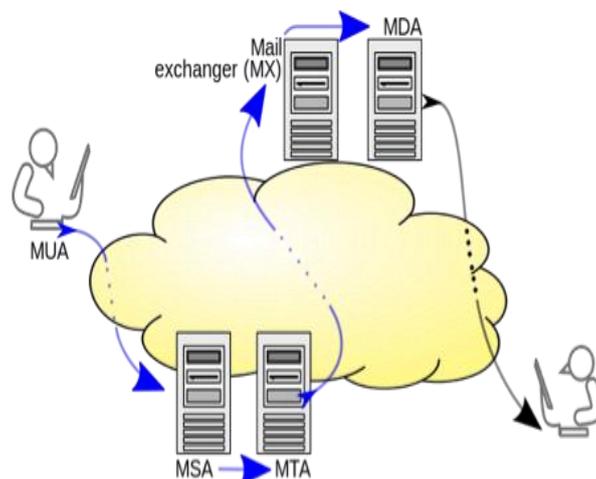


Figure 2. 2:Principe d'envoi via SMTP.

## 2. Le POP3

Le « Post Office Protocole » plus communément appelé POP3 est l'un des types de protocoles les plus couramment proposés sur un serveur mail. C'était le protocole le plus utilisé dans les débuts d'Internet car c'était la façon la plus efficace de recevoir rapidement ses mails (le modem étant relié à la ligne téléphonique à cette époque). La version 3 est la plus récente, succédant au POP 1 et POP 2, celle-ci est standardisée dans le monde et utilisée par un grand nombre de personnes, surtout dans le domaine familial. Ce serveur pop utilise le port 110 de la machine. Le port permettant la communication entre la machine et le serveur. C'est donc la couche de transport du modèle OSI qui lui est attribué, différents ports s'envoient des informations dans un ordre précis, donné par des chiffres.

Les avantages du POP 3 sont : La conservation de l'e-mail de façon temporaire sur un serveur externe à notre machine. Le mail est conservé sur un serveur directement après l'envoi et ce jusqu'à réception par le destinataire. Efficace dans certains cas, il peut aussi se trouver gênant quand on souhaite garder une trace de certains mails importants. Le protocole POP 3 est donc d'avantage conseillé pour une gestion simple des mails, via un post unique (un seul ordinateur) et pour une personne souhaitant recevoir tous ses mails sans tri tout en souhaitant (si elle le désire) lire ses mails en mode hors-ligne, c'est-à-dire sans connexion au serveur, les mails étant directement rapatriés sur notre machine [24].

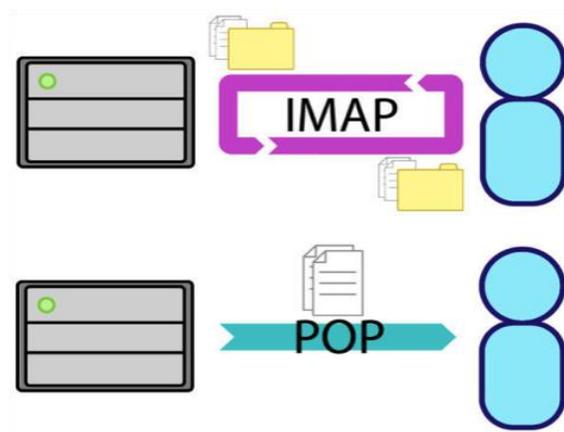


Figure 2. 3: Principe d'envoi via POP3.

## 3. Le IMAP

Le protocole IMAP (Interactive Mail Access Protocol) est le successeur du protocole POP3. Il est plus pratique et efficace par rapport au protocole POP3. Sa particularité est le transfert et la synchronisation (messages reçus, envoyés, archives, brouillons,..) de la boîte de réception sur l'ordinateur tout en effaçant le serveur. Notre messagerie reste quand même stockée dans son intégralité sur le serveur. L'IMAP a des fonctionnalités plus avancées tel que : créer, renommer

ou supprimer des répertoires de messagerie sur le serveur dans le but de mieux organiser et stocker les courriers électroniques. On peut y accéder par différents terminaux. On a droit à accéder aux mêmes données. Lorsque on effectue une action depuis un terminal, celle-ci est actionnée automatiquement et reportée sur le serveur [24].

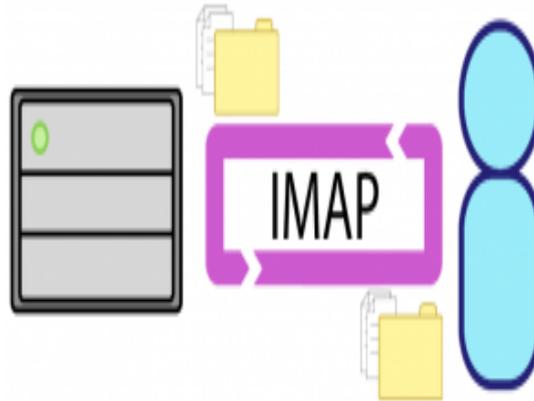


Figure 2. 4: Principe d'envoi via IMAP.

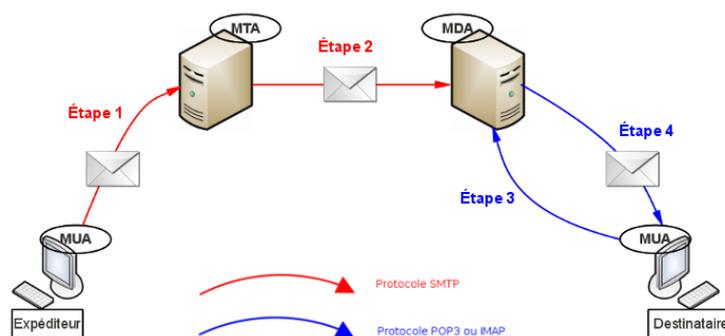


Figure 2. 5: Les quatre principales étapes du trajet d'un courrier électronique.

## ÉTAPE 1

Grâce à son **MUA** (client de messagerie ou webmail), l'expéditeur rédige un e-mail, puis clique ensuite sur le bouton "envoyer". Via le protocole **SMTP**, l'e-mail est alors confié à un **MTA** (serveur SMTP de l'expéditeur).

## ÉTAPE 2

L'e-mail va alors subir un long voyage à travers l'internet. En effet, toujours via le protocole **SMTP**, c'est tout un tas de **MTA** qui vont le relayer jusqu'à ce qu'il arrive à bon port, à savoir un **MDA** (le serveur **POP3** ou **IMAP** du destinataire).

### ÉTAPE 3

Le destinataire clique alors sur le bouton "relever" de son **MUA** préféré (client de messagerie ou webmail). Une demande est alors faite auprès de son **MDA** afin de savoir s'il a reçu du courrier ou non. Cette demande se fait via le protocole **POP3** ou **IMAP** suivant la configuration du **MUA**.

### ÉTAPE 4

Dans le cas où un e-mail est sur le **MDA**, le serveur le transmet au **MUA** du destinataire afin que ce dernier puisse lire son e-mail. Cette dernière étape est une étape de réception, c'est pourquoi elle se fait via le protocole **POP3** ou **IMAP** suivant la configuration du **MUA** du destinataire.

## 2.5 Serveur de messagerie

Un serveur de messagerie électronique est un logiciel serveur, matériel ou logiciel informatique qui offre des services, de courrier électronique aussi appelé courriel. Son but est de transférer les messages électroniques d'un serveur à un autre. L'utilisateur ne sera jamais en contact direct avec son serveur, il doit utiliser soit un courriel web, appelé aussi webmail c'est une interface web qui sert à l'envoi, la consultation, la manipulation de courriers électronique directement sur le web depuis un navigateur, ou un client de messagerie, logiciel pour lire et envoyer des courriers électroniques. Le webmail ou le client de messagerie se chargent donc d'appréhender le serveur de messagerie pour envoyer ou recevoir un mail. Les serveurs de messageries électroniques servent aussi à l'élimination de spam ou de mail contenant des virus informatiques [24].

Des exemples sur les serveurs de messagerie [25]:

1. **Sendmail** : Est un serveur de messagerie dont le code source est ouvert. Il se charge de la livraison des messages électroniques et possède les atouts suivants :
  - Très puissant et résiste beaucoup à la grande charge.
  - Une très bonne sécurité.
  - Code source libre.
2. **Postfix** : est un MTA avec codes sources libres. Il 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 a les caractéristiques suivantes :

- Il est adapté aux gros besoins.

- Facile à installer et à configurer.
  - Maintenance aisée.
  - Sécurisé avec anti-Spam.
  - Codes sources libres.
  - Multi plate-forme de type UNIX (MAC OS, GNU/LINUX).
  - Gratuit.
  - Accessible en mobilité. Inconvénients : Pas d'inconvénients majeurs.
3. **MS Exchange** : Microsoft Exchange est un logiciel de messagerie qui permet de gérer les Mails, les Calendriers et les Contacts. Il a les caractéristiques suivantes :
- Accès en mobilité, c'est-à-dire vous avez accès à vos mails, vos calendriers ou vos contacts via votre ordinateur portable, votre téléphone portable et ce depuis tout endroit connecté à Internet.
  - Une bonne sécurité anti-spam qui sauvegarde et archive vos données critiques.
  - Une bonne efficacité permettant de partager votre agenda et contact professionnel avec vos collègues ou collaborateurs.
  - Les codes sources ne sont pas libres.
  - Uni plate-forme (MS Windows).
4. **Zimbra**
- Il a les caractéristiques suivantes [16] :
- Open source.
  - Déploiement ont permise possible.
  - Fonction de recherche/filtrage.
  - Interface utilisateur.
  - Customisation possible des interfaces.
  - SDK mobile
  - Pas de service cloud manage par l'éditeur

## 2.6 Client de messagerie

Un client de messagerie est un logiciel de lecture des emails qui est installé sur le poste de l'utilisateur et qui permet de rapatrier et stocker les emails reçus sur le disque de l'utilisateur. Ce sont en général des clients lourds mais il existe aussi des applications Web (les webmails) qui offrent les mêmes fonctionnalités.

### 2.6.1 Les clients lourds

C'est un logiciel installé sur les ordinateurs des utilisateurs. Le traitement métier des données se fait au niveau de la machine de l'utilisateur qui prend en charge la communication avec la base de données. Les clients lourds ont l'avantage de récupérer nos messages et de les copier sur nos postes locaux, en mode connecté au serveur. Ainsi en mode hors connexion, nous avons accès à nos messages [26].

#### 1. Thunderbird de Mozilla :

IL se caractérise par [25] :

- Très léger.
- Multi plate-forme (Windows, Mac OS, Linux).
- Rapide.
- Extensible (peut recevoir de nouvelles fonctionnalités).
- Les codes sources sont libres d'accès.
- Installation et configuration simples.
- Transfert de messages avec pièces jointes.

#### 2. Zimbra Desktop :

IL se caractérise par [27]:

- Multi plateforme (Windows, Mac OS, Linux).
- Codes sources libres.
- Regroupe tous les comptes dans un seul répertoire.
- Installation et configuration rapide et facile.
- Transfert des messages avec des pièces jointes.
- Extensible.

### 2.6.2 Les clients légers

C'est une application installée sur un serveur Web et les utilisateurs n'ont besoin que d'un navigateur internet pour pouvoir accéder à l'ensemble des services. Le traitement métier des données est donc centralisé. Il se fait au niveau du serveur web qui prendra en charge la communication avec la base de données pour répondre aux besoins de tous les utilisateurs [26].

#### 1.Outlook Web Access :

Outlook Web App est basée sur le Web du client de messagerie de Microsoft Exchange Server 2010. Anciennement connu sous Outlook Web Access dans les itérations précédentes de

Exchange Server, Outlook Web App permet aux utilisateurs une expérience similaire à Microsoft Outlook sans nécessiter la présence du client de messagerie complète.

Il se caractérise par [28] :

- Installation rapide et facile.
- Très léger.
- Codes sources non libres.

## **2.Web Mail Ajax de Zimbra:**

Zimbra Collaboration Suite (ZCS) est une suite de logiciels de collaboration, qui comprend un serveur de messagerie et un client Web, actuellement détenue et développée par Zimbra, il se caractérise par [27] :

- Multi plate-forme (MS Windows, Mac OS, Linux, etc.).
- Elle est Gratuite.
- Codes sources libres.
- Transfère les messages avec pièces jointes.
- Permet les messages instantanés.

## **2.7 Client lourd VS Client léger**

Un client léger communique avec un serveur central de traitement. Du coup, l'utilisateur final n'a besoin que d'un navigateur internet pour accéder aux services de son application. Cela permet aux systèmes des utilisateurs finaux d'être gérées de manière centralisée et avec des logiciels déployés sur un seul serveur central, par opposition au client lourd qui nécessite l'installation du logiciel sur chaque poste utilisateur. Les clients légers sont vraiment mieux adaptés aux environnements dans lesquels les mêmes informations vont être accessibles par les clients, ce qui présente en fait une meilleure solution pour les environnements publics. Pour cette raison, les clients légers sont souvent déployés dans des établissements comme les hôtels et les aéroports, où l'installation de logiciels est centralisée. Cela facilite le déploiement et la maintenance. En revanche, un client lourd fournit aux utilisateurs finaux plus de fonctionnalités, des graphiques et des choix qui rendent les applications plus personnalisables. Contrairement à des clients légers, les clients lourds ne reposent pas sur un serveur central de traitement parce que le traitement est effectué localement sur le système de l'utilisateur et le serveur est accessible principalement à des fins de stockage. Pour cette raison, les clients lourds ne sont souvent pas bien adaptés pour les environnements publics. Pour maintenir un client lourd, il est nécessaire de maintenir tous les postes utilisateurs pour le déploiement et les mises à niveau des logiciels, plutôt que de

simplement maintenir les applications une seule fois sur un seul serveur centrale. En outre, les clients lourds nécessitent souvent l'exploitation des applications spécifiques, encore une fois imposant plus de travail et de limitations pour le déploiement [26].

## 2.8 L'adresse électronique

Une adresse électronique, adresse courriel ou adresse e-mail (de l'anglais ['i:meil]) est une chaîne de caractères permettant d'acheminer du courrier électronique dans une boîte aux lettres informatique. Une adresse électronique valide est une adresse composée de deux parties, un nom d'utilisateur et un nom de domaine, qui se présente sous la forme suivante :

"nomd'utilisateur@nomdedomaine.extension"

- **Le nom d'utilisateur** est l'identifiant que vous avez choisi aux fins du courrier électronique et que vous avez communiqué au serveur de messagerie pour créer votre compte de messagerie.
- **Le nom de domaine** est la désignation Internet du serveur de messagerie, qui peut être un site privé, une entreprise, une organisation ou une entité gouvernementale.
- **L'extension** peut prendre des formes très diverses telles que .com, .org, .fr (code pays), .biz, .info, .gov, .int, etc.

## 2.9 Le message électronique

Document informatisé qu'un utilisateur saisit, envoie ou consulte en différé par l'intermédiaire d'un réseau.

### 2.9.1 Structure d'un message électronique

La structure d'un message est composée fondamentalement trois parties ; corps du message et données d'administration. Les données d'administration peuvent être partagées en deux catégories, enveloppe et en-tête du message [29] :

- **L'enveloppe** est un ensemble de lignes contenant les informations de transport telles que l'adresse de l'expéditeur, l'adresse du destinataire ou encore l'horodatage du traitement du courrier par les serveurs intermédiaires nécessaires aux serveurs de transports (MTA) faisant office de bureaux de tri postal. L'enveloppe commence par une ligne *From* et est modifié par chaque serveur intermédiaire. Ainsi, grâce à l'enveloppe, il est possible de connaître le chemin parcouru par le courrier et le temps de traitement par chaque serveur.
- **Le message** à proprement parler, composé des deux éléments suivants :

➤ **Les champs d'en-tête** (en anglais *header fields*), un ensemble de lignes décrivant les paramètres du message, tels que l'expéditeur, le destinataire, la date, etc. Chaque entête possède la forme suivante :

- **From** : adresse électronique de l'expéditeur
- **To** : adresse électronique du destinataire
- **Date** : date de création du courrier

Il peut contenir les en-têtes facultatifs suivants :

- **Received** : diverses informations sur les serveurs intermédiaires et la date de traitement du message associée.
- **Reply-To** : Une adresse pour la réponse.
- **Subject** : Le sujet du message.
- **Message-ID** : un identifiant unique du message.

➤ **Le corps du message**, contenant le message, séparé de l'en-tête par une ligne vide.

### 2.9.2 Les formats standards d'un message

MIME propose de décrire, grâce à des en-têtes, le type de contenu du message et le codage utilisé. MIME apporte à la messagerie les fonctionnalités suivantes [30] :

- Possibilité d'avoir plusieurs objets (pièces jointes) dans un même message ;
- Une longueur de message illimitée ;
- L'utilisation de jeux de caractères (alphabets) autres que le code ASCII ;
- L'utilisation de texte enrichi (mise en forme des messages, polices de caractères, couleurs, etc.) ;
- Des pièces jointes binaires (exécutables, images, fichiers audio ou vidéo, etc.), comportant éventuellement plusieurs parties ;

MIME utilise des directives d'entête spécifiques pour décrire le format utilisé dans le corps d'un message, afin de permettre au client de messagerie de pouvoir l'interpréter correctement :

- **MIME-Version** : Il s'agit de version du standard MIME utilisée dans le message. Actuellement seule la version 1.0 existe.
- **Content-type** : Décrit le type et les sous-types des données. Il peut posséder un paramètre « charset », séparé par un point-virtule, définissant le jeu de caractères utilisé.
- **Content-Transfer-Encoding** : Définit l'encodage utilisé dans le corps du message.
- **Content-ID** : Représente un identificateur unique de partie de message.
- **Content-Description** : Donne des informations complémentaires sur le contenu du message.

- **Content-Disposition** : Définit les paramètres de la pièce jointe, notamment le nom associé au fichier grâce à l'attribut *filename*.

## 2.10 Principaux risques de la messagerie

### 2.10.1 Réception/Envoi de virus

La messagerie électronique permet de véhiculer tous les types de fichiers, en particulier les scripts et les fichiers exécutables. Si ces programmes sont exécutés sur la machine qui a reçu le courrier, un virus est susceptible d'infecter la machine[20].

### 2.10.2 Réception/Envoi messages falsifiés

Le protocole standard le plus utilisé pour la messagerie électronique est SMTP. Cependant ce protocole ne présente, dans sa fonction de base, aucune garantie contre la falsification des messages électroniques. Il n'y a aucun contrôle effectué sur l'expéditeur du message, et par conséquent n'importe qui sur le même réseau peut se faire passer quelqu'un autre[20].

### 2.10.3 Lecture de messages par de tierces personnes

Une autre faiblesse du protocole SMTP réside dans le fait que les messages envoyés ou reçus par ce biais sont transmis en clair sur le réseau, c'est-à-dire qu'ils ne sont pas chiffrés. Ainsi, toutes personnes écoutant sur le réseau à la possibilité de voir le contenu de message.

### 2.10.4 Perte de message

Un serveur de messagerie, que ce soit en relais ou en serveur interne, doit être bien dimensionné et bien sécurisé pour résister à la charge et à attaques en déni de service qui conduiraient à des pertes des messages. Ce risque doit être pris en considération, car une perte de message électronique est très difficilement acceptée par les utilisateurs[20].

### 2.10.5 Indisponibilité du serveur de messagerie

Si le serveur de messagerie est la cible d'attaque en déni de service, il peut être indisponible pendant une longue durée. L'indisponibilité peut être due par exemple à une saturation du serveur par un grand nombre de messages envoyés volontairement (attaque ciblée d'un pirate), par un ou plusieurs messages envoyés à un nombre de destinataires élevé. L'attaque peut également provenir par exemple de l'envoi de messages infectés.

### 2.10.6 Rebond possible pour une attaque en interne

Un serveur de messagerie peut être situé en zone protégées (dans une DMZ ou sur le réseau interne). Il est ainsi possible qu'il dispose de privilèges supplémentaires par rapport à un

attaquant situé dans une zone non protégées (Internet par exemple). Si ce serveur de messagerie est compromis, il pourra potentiellement servir de rebond pour une attaque à destination d'une machine dans un réseau sécurisé qui n'aurait pu être réalisées autrement.

## **2.11 Sécurité de la messagerie**

Aujourd'hui environ 75% des e-mails seraient des spam et 90% des infections par des vers où des vers sont véhiculés par la messagerie électronique. Cependant, le courrier électronique est le plus populaire des services sur l'internet d'où, sa sécurisation dans sa mise en place doit être de rigueur. Au niveau de l'utilisateur, il présente toutes les caractéristiques du courrier classique : envoi par dépôt au poste client, centre de tri, acheminement, boîte aux lettres, distribution. Toutefois, le protocole SMTP (Simple Mail Transfer Protocol), lors de sa conception n'a pas tenu compte des préoccupations de sécurité actuelles. C'est ce qui explique la prolifération des menaces techniques qui pèsent aujourd'hui sur la messagerie : virus, hoax, attaque déni de service, usurpation d'adresses, piratage d'adresses et du contenu du mail, etc.

De plus, parce que c'est un outil simple, rapide et expansif, des dérives comportementales et légales peuvent en résulter et doivent être contrôlées dans le monde des entreprises : fuite d'informations, manque de confidentialité, contenus illicites et saturation des ressources informatiques. Le Directeur informatique ou Manager trouvera sans doute des éléments à prendre en compte pour la sécurisation de la messagerie électronique. Les menaces sont en perpétuelle évolution alors que la messagerie est l'application la plus utilisée dans nos entreprises d'où, sa sécurisation doit être au centre des préoccupations de ces dernières, la politique de sa conception doit être cohérente et intégrée

## **2.12 Les protocoles de sécurité**

### **2.12.1 Le protocole SSL (Secure Socket Layer)**

SSL (Secure Sockets Layer), devenu TLS (Transport Layer Security), est un protocole de sécurisation des échanges sur Internet. Cette norme de sécurité de transfert permet à la fois de chiffrer les données échangées, d'authentifier le serveur et de contrôler l'intégrité du message.

Il s'agit d'un protocole de communication sécurisé, principalement utilisé par les webmarchands qui effectuent des transactions bancaires en ligne. Doté de plusieurs services de sécurité, SSL est généralement employé par les systèmes de paiement et de transactions en ligne relevant du protocole HTTP pour le web et du protocole TCP/IP. SSL remplit les objectifs de sécurité suivants [31] :

- La confidentialité des données via leur cryptage
- L'authentification du serveur pour le client
- L'intégrité des messages échangés.

En option, il peut également authentifier le client avec l'utilisation d'un certificat numérique.

### **2.12.1.1 Fonctionnalités de SSL**

SSL est localisé entre la couche application et la couche transport TCP dans la pile de protocole TCP/IP, même si son utilisation la plus courante se situe en dessous de HTTP. SSL est implémenté par la couche session de la pile. Les conséquences sont de deux ordres :

- Une application qui utilise SSL peut exister pour toutes les applications existantes qui utilisent TCP. C'est le cas notamment pour l'application HTTPS qui correspond à HTTP au-dessus de SSL ;
- Une application SSL peut se voir attribuer un autre numéro de port par l'IANA, à l'image de HTTPS qui est associé au port 443.

### **2.12.2 Le protocole SSH (Secure Shell)**

SSH (ou *Secure SHell*) est un protocole qui facilite les connexions sécurisées entre deux systèmes à l'aide d'une architecture client/serveur et permet aux utilisateurs de se connecter à distance à des systèmes hôte de serveurs. Toutefois, contrairement à d'autres protocoles de communication à distance, tels que FTP ou Telnet, SSH crypte la session de connexion et empêche ainsi tout agresseur de recueillir des mots de passe non-cryptés [32].

#### **2.12.2.1 Fonctionnalités de SSH**

SSH offre les précautions suivantes au niveau de la sécurité :

- Après avoir effectué une connexion initiale, le client peut s'assurer que sa connexion est établie avec le même serveur que lors de sa session précédente.
- Le client transmet ses données d'authentification au serveur au moyen d'un cryptage solide 128 bits.
- Toutes les données envoyées et reçues lors d'une session sont transférées au moyen d'un cryptage 128 bits, rendant ainsi le décryptage et la lecture de toute transmission interceptée extrêmement difficile.
- Le client peut retransmettre des applications X11 depuis le serveur. Cette technique appelée *retransmission X11*, fournit un moyen d'utiliser en toute sécurité des applications graphiques sur un réseau. (X11 fait référence au système d'affichage de fenêtres

X11R6.7, généralement appelé X Window System ou X. Red Hat Enterprise Linux inclut XFree86, un système X Window System Open Source).

## **2.13 Conclusion**

Le chapitre deux, 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 3

## Chapitre 3 : Réalisation

### 3.1 Introduction

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 de configuration de notre système de messagerie.

### 3.2 Définitions du serveur de messagerie Zimbra

Zimbra est une plate-forme complète de messagerie et de travail collaboratif, développée autour des nouvelles technologies Web Ajax, et basée sur des logiciels libres (Jetty, Postfix, openLDAP, mysql et d'autres).

Il Comprend aussi la fonction de serveur de messagerie, de calendriers partagés, de carnets d'adresses partagés, de gestionnaire de fichiers, de gestionnaire de tâches, messagerie instantanée.

Parmi les avantages de Zimbra, on retrouve :

- **Le partage** : Zimbra permet de transmettre et de partager l'information aisément. Ce qui permet de mutualiser les efforts afin de travailler plus efficacement, en effectuant un partage de documents, d'agenda et de contact.
- **L'accessibilité** : Grâce à un accès web, on peut se connecter à Zimbra depuis n'importe quels supports dotés d'une connexion internet et quel que soit son emplacement (téléphone, tablette, ordinateur ou tout autre équipement connecté)
- **La stabilité** : L'open-source est reconnue pour être très fiable. Le code source de ses logiciels est mis à jour régulièrement.
- **L'organisation** : Cette messagerie permet de classer efficacement ces mails, grâce au « tags » permettant ainsi de créer des catégories. Il est aussi possible de créer des filtres, qui **archivent** et rangent les mails dans des groupes prédéfinis, dès leur réception.
- **Les ajouts** : Zimbra est modulable, grâce aux « Zimlets » qui permettent d'y intégrer des outils utilisables quotidiennement. Tel que : Facebook, Twitter, Google maps...La messagerie devient alors un point névralgique du système d'information.

### 3.2.1 Environnement du travail

Pour la réalisation de notre application, nous avons eu recours à des moyens matériels et logiciels.

#### 3.2.1.1 Matériel de base

Nous disposant d'un PC de bureau (Condor) dont les caractéristiques sont :

- Processeur Intel Core i3-3220 CPU de fréquence d'horloge 3.30GHz.
- 8 Go de mémoire vive.
- Disque dur de 500 Go.

#### 3.2.1.2 Logiciel de base

- Système d'exploitation linux (centOS 7).
- Serveur du messagerie Zimbra 8.7.1.

### 3.3 Installation et configuration des composants de la messagerie

Dans cette partie nous allons réaliser l'installation du CentOS 7 dans ces deux versions, minimale et finale.

#### 3.3.1 Installation CentOS 7 64 bits version minimale

On procède ici à l'installation de la version minimale. Dis la mise en marche de notre machine on obtient l'affichage de la (figure 3.1), qui nous invite à installer CentOS 7.

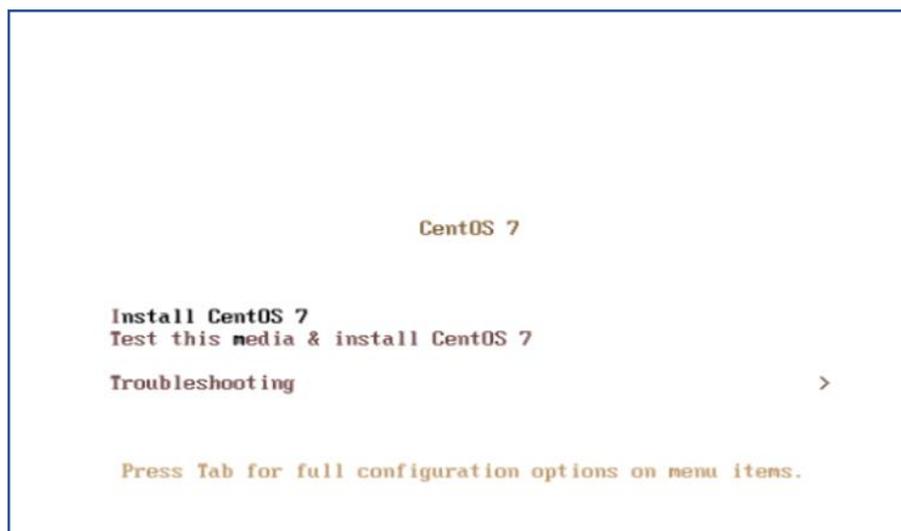


Figure 3. 1: Installation de CentOS 7.

Après validation de l'installation, un nouveau menu s'affiche (figure 3.2) qui nous invite à choisir une configuration de :

- La date
- L'emplacement
- La langue
- La carte réseau
- Mot de passe en mode root

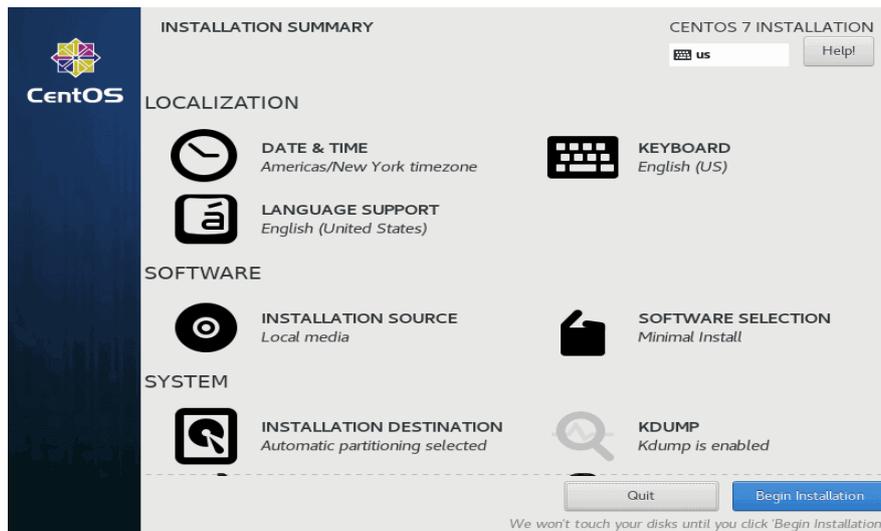


Figure 3. 2: Configuration des paramètres.

### Etape 1 : Modification de la langue



Figure 3. 3: Choix de langue.

## **Etape 2 : Configuration de la carte réseau**

Maintenant notre système est destiné à être un serveur, il est préférable de configurer le réseau statique sur Ethernet en cliquant sur le bouton Configurer et en ajoutant tous les paramètres d'interface statiques comme sur la figure ci-dessous.

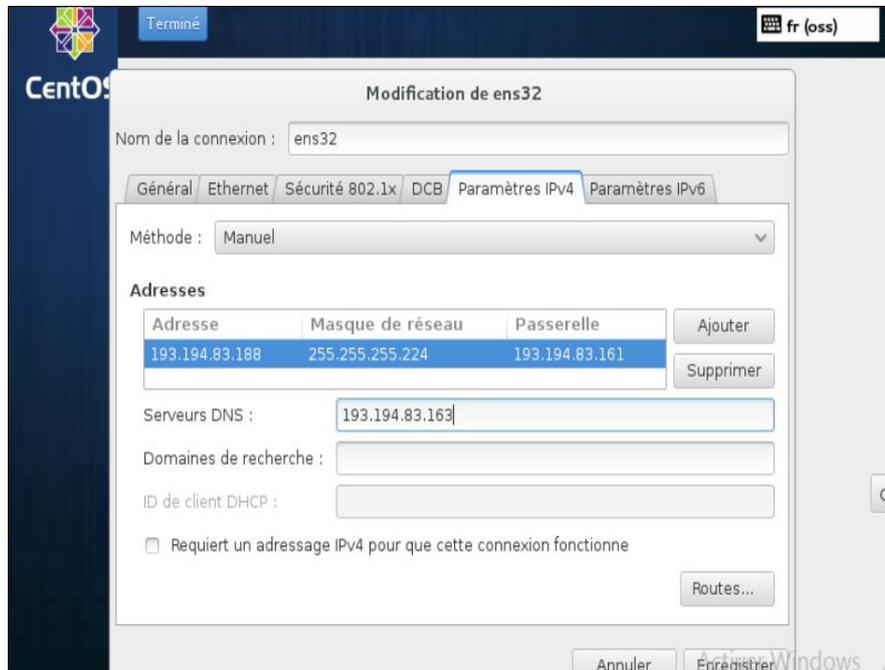


Figure 3. 4: Configuration de la carte réseau.

## **Etape 3 : Configurer un mot de passe pour le compte root « super-utilisateur »**

Il est important de protéger la configuration de notre système d'exploitation par un mot de passe.

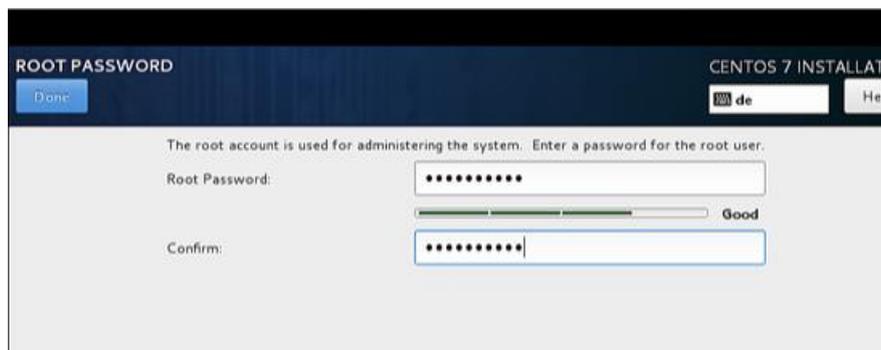


Figure 3. 5: Configuration d'un mot passe.

Une fois l'installation terminée, le serveur redémarre et demandera ensuite notre nom d'utilisateur (en mode root) et notre mot de passe (figure 3.6).

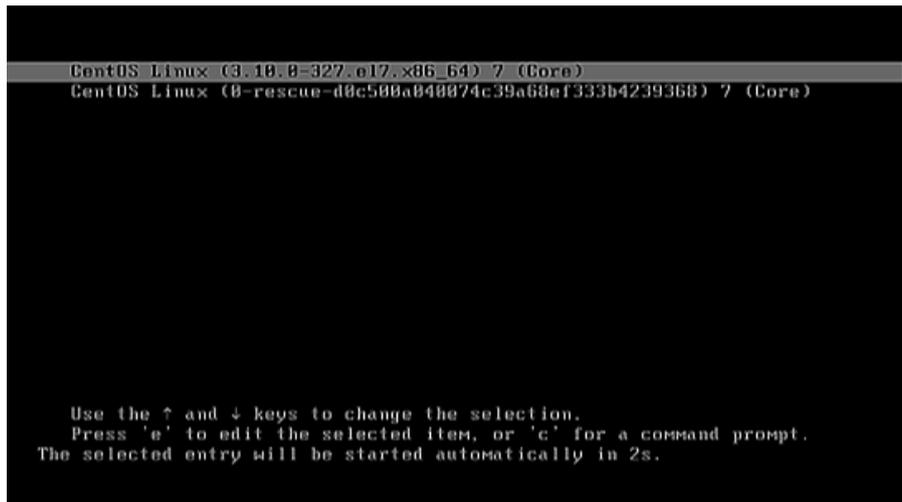


Figure 3. 6: Redémarrage du système.

En tant qu'administrateur système on aura tous les droits sur l'appareil et on pourra modifier tous les éléments de l'OS y compris les fichiers sensibles.

Lors de l'installation de CentOS 7 dans la version minimale, un écran s'affiche en mode Ligne de commande.

Afin de pouvoir effectuer certaines étapes d'installation on utilise les commandes qui sont résumé dans le tableau suivant :

Commandes	Fonctionnalités
<b>Yum</b>	Il permet de gérer l'installation et la mise à jour des logiciels installés sur le système d'exploitation.
<b>Update</b> "Mettre à jour"	L' <b>update</b> concerne donc les mises à jour ( <i>logiciels, systèmes...</i> ). Elle va remettre votre version au dernier niveau en vigueur.
<b>Upgrade</b> "Améliorer"	L' <b>upgrade</b> correspond, elle, à la mise à jour vers une nouvelle version. Cette nouvelle version va contenir des nouveautés dites « majeures ».
<b>GNOME Desktop</b>	Tous les composants et dépendances nécessaires sont installés par le groupe de packages GNOME Desktop.
<b>Startx</b>	Si GNOME est le seul environnement de bureau installé, il sera exécuté par défaut lorsque nous lancerons X avec startx.

Tableau 3. 1: Commandes de bas du linux

Après l'installation des deux versions une interface de bureau s'affiche (figure 3.7).



Figure 3. 7: Interface de bureau.

### 3.3.2 Installation de Zimbra

Pour installer Zimbra on doit suivre les étapes suivantes :

#### **Etape 1** : Définition du nom de la machine

On doit définir le nom d'hôte de notre serveur (figure 3.8).

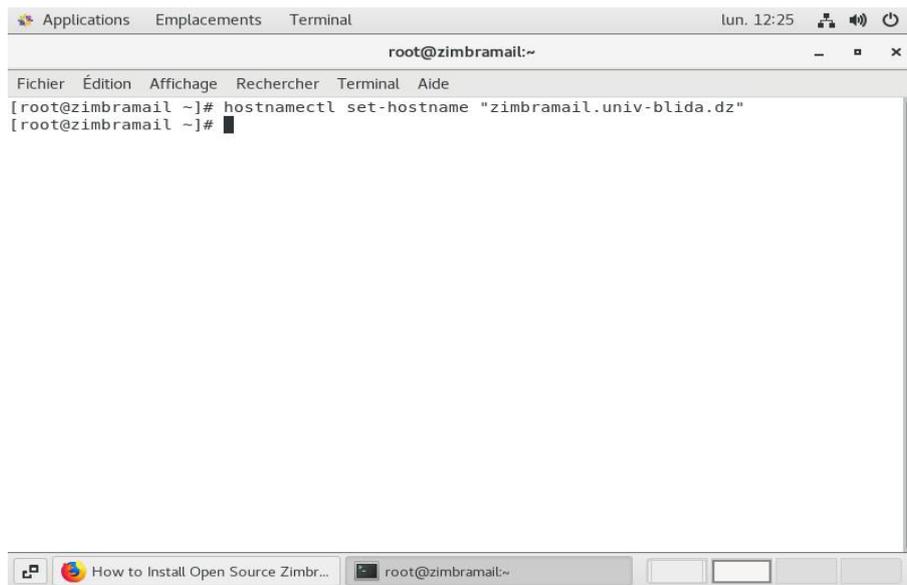


Figure 3. 8: Définition d'un nom de la machine.



```

[root@zimbramail ~]# dig -t MX univ-blida.dz

; <<>> DiG 9.11.4-P2-RedHat-9.11.4-16.P2.el7_8.6 <<>> -t MX univ-blida.dz
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 49615
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;univ-blida.dz.                IN      MX

;; ANSWER SECTION:
univ-blida.dz.                3600   IN      MX      10 mail.univ-blida.dz.

;; ADDITIONAL SECTION:
mail.univ-blida.dz.          3600   IN      A       193.194.83.172

;; Query time: 3 msec
;; SERVER: 193.194.83.163#53(193.194.83.163)
;; WHEN: lun. août 31 12:30:44 CEST 2020
;; MSG SIZE rcvd: 79

[root@zimbramail ~]# █

```

Figure 3. 11: Configuration de MX.

#### **Etape 4** : préparation de l'installations de Zimbra

Installations des packages nécessaires pour la préparation de l'installations de Zimbra collaboration suite 8.7.1 (figure 3.12) :

```

[root@zimbramail ~]# yum install unzip net-tools sysstat openssh-clients perl-core liba
io nmap-ncat libstdc++.so.6 wget -y
Modules complémentaires chargés : fastestmirror, langpacks
Loading mirror speeds from cached hostfile
 * base: ftp.rediris.es
 * extras: ftp.rediris.es
 * updates: ftp.rediris.es
base                               | 3.6 kB  00:00:00
extras                             | 2.9 kB  00:00:00
updates                             | 2.9 kB  00:00:00
Le paquet unzip-6.0-21.el7.x86_64 est déjà installé dans sa dernière version
Le paquet net-tools-2.0-0.25.20131004git.el7.x86_64 est déjà installé dans sa dernière
version
Le paquet sysstat-10.1.5-19.el7.x86_64 est déjà installé dans sa dernière version
Le paquet openssh-clients-7.4p1-21.el7.x86_64 est déjà installé dans sa dernière versio
n
Le paquet libaio-0.3.109-13.el7.x86_64 est déjà installé dans sa dernière version
Le paquet 2:nmap-ncat-6.40-19.el7.x86_64 est déjà installé dans sa dernière version
Le paquet libstdc++-4.8.5-39.el7.i686 est déjà installé dans sa dernière version
Le paquet wget-1.14-18.el7_6.1.x86_64 est déjà installé dans sa dernière version
Résolution des dépendances
--> Lancement de la transaction de test
-->> Le paquet perl-core x86_64 4.5.16-3.295.el7 sera installé

```

Figure 3. 12: Installations des paquets manquant.

**Etape 5** : Téléchargement le lien de Zimbra CS 8.7.1 :

La commande « mkdir » nous a permis de créer le dossier zimbra, et pour accéder à ce dernier on utilise la commande « cd » puis on télécharge le lien de zimbra cs grâce à la commande « wget » (figure 3.13).

```
[root@zimbra@mail ~]# mkdir zimbra && cd zimbra
[root@zimbra@mail zimbra]# wget https://files.zimbra.com/downloads/8.7.1_GA/zcs-8.7.1_GA_1670.RHEL7_64.20161025045328.tgz
--2020-08-31 12:42:12-- https://files.zimbra.com/downloads/8.7.1_GA/zcs-8.7.1_GA_1670.RHEL7_64.20161025045328.tgz
Résolution de files.zimbra.com (files.zimbra.com)... 54.230.107.78
Connexion vers files.zimbra.com (files.zimbra.com)|54.230.107.78|:443...connecté.
requête HTTP transmise, en attente de la réponse...200 OK
Longueur: 304471419 (290M) [binary/octet-stream]
Sauvegarde en : «zcs-8.7.1_GA_1670.RHEL7_64.20161025045328.tgz»

12% [====>] 38 835 852 346KB/s eta 22m 49s
```

Figure 3. 13: Téléchargement de Zimbra.

**Etape 6** : Décompression du package Zimbra CS 8.7.1 :

On va Extraire le fichier tgz téléchargé de ZCS 8.7.1 (figure 3.14).

```
[root@zimbra@mail ~] #tar xzf zcs-8.7.1_GA_1670.RHEL7_64.20161025045328.tgz
```

Figure 3. 14: Décompression du package Zimbra.

**Etape 7** : Accès dans le dossier décompressé

On accède au dossier extrait précédemment et on exécute le script d'installation (figure 3.15).

```
[root@zimbra@mail ~]# cd zimbra
[root@zimbra@mail zimbra]# cd zcs-8.7.1_GA_1670.RHEL7_64.20161025045328.tgz
bash: cd: zcs-8.7.1_GA_1670.RHEL7_64.20161025045328.tgz: N'est pas un dossier
[root@zimbra@mail zimbra]# cd zcs-8.7.1_GA_1670.RHEL7_64.20161025045328
[root@zimbra@mail zcs-8.7.1_GA_1670.RHEL7_64.20161025045328]# ./install.sh
```

Figure 3. 15: Accéder au dossier décompressé.

**Etape 8** : Installation du Zimbra CS 8.7.1

La commande « install.sh » nous a permis d'installer zimbra cs (figure 3.16 et figure 3.17).

```
[root@zimbra1 zcs-8.7.1_GA_1670.RHEL7_64.20161025045328]# ./install.sh

Operations logged to /tmp/install.log.vDNDst9z
Checking for existing installation...
  zimbra-ldap...NOT FOUND
  zimbra-logger...NOT FOUND
  zimbra-mta...NOT FOUND
  zimbra-dnscache...NOT FOUND
  zimbra-snmp...NOT FOUND
  zimbra-store...NOT FOUND
  zimbra-apache...NOT FOUND
  zimbra-spell...NOT FOUND
  zimbra-convertd...NOT FOUND
  zimbra-memcached...NOT FOUND
  zimbra-proxy...NOT FOUND
  zimbra-archiving...NOT FOUND
  zimbra-core...NOT FOUND
```

Figure 3. 16: Lancement du scripte d'installation du Zimbra.

```
Operations logged to /tmp/install.log.v6G169iH
Checking for existing installation..
  zimbra-chat...NOT FOUND
  zimbra-drive...NOT FOUND
  zimbra-ldap...NOT FOUND
  zimbra-logger...NOT FOUND
  zimbra-mta...NOT FOUND
  zimbra-dnscache...NOT FOUND
  zimbra-snmp...NOT FOUND
  zimbra-store...NOT FOUND
  zimbra-apache...NOT FOUND
  zimbra-spell...NOT FOUND
  zimbra-convertd...NOT FOUND
  zimbra-memcached...NOT FOUND
  zimbra-proxy...NOT FOUND
  zimbra-archiving...NOT FOUND
  zimbra-core...NOT FOUND

-----
PLEASE READ THIS AGREEMENT CAREFULLY BEFORE USING THE SOFTWARE.
SYNACOR, INC. ("SYNACOR") WILL ONLY LICENSE THIS SOFTWARE TO YOU IF YOU
FIRST ACCEPT THE TERMS OF THIS AGREEMENT. BY DOWNLOADING OR INSTALLING
THE SOFTWARE, OR USING THE PRODUCT, YOU ARE CONSENTING TO BE BOUND BY
THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS
AGREEMENT, THEN DO NOT DOWNLOAD, INSTALL OR USE THE PRODUCT.

License Terms for this Zimbra Collaboration Suite Software:
https://www.zimbra.com/license/zimbra-public-eula-2-6.html
-----

Do you agree with the terms of the software license agreement? [N] y
```

Figure 3. 17: Exécution de l'installation.

### **Etape 9** : Sélection de composant à installer

Nous allons maintenant configurer le référentiel de paquets Zimbra et sélectionner tous les composants Zimbra à installer (figure 3.18 à figure 3.21).

```
Use zimbra's package repository [Y]
Importing Zimbra GPG key
Configuring package repository
Checking for installable packages

Found zimbra-core (local)
Found zimbra-ldap (local)
Found zimbra-logger (local)
Found zimbra-mta (local)
Found zimbra-dnscache (local)
Found zimbra-snmp (local)
Found zimbra-store (local)
Found zimbra-apache (local)
Found zimbra-spell (local)
Found zimbra-memcached (repo)
Found zimbra-proxy (local)
Found zimbra-chat (repo)
Found zimbra-drive (repo)
```

Figure 3. 18: Installations des modules de Zimbra.

```
Select the packages to install
Install zimbra-ldap [Y] y
Install zimbra-logger [Y] y
Install zimbra-mta [Y] y
Install zimbra-dnscache [Y] y
Install zimbra-snmp [Y] y
Install zimbra-store [Y] y
Install zimbra-apache [Y] y
Install zimbra-spell [Y] y
Install zimbra-memcached [Y] y
Install zimbra-proxy [Y] y
Install zimbra-chat [Y]
Install zimbra-drive [Y] █
```

Figure 3. 19: Menu des paquets a installé.

```
root@zimbra@mail:~/zimbra/zcs-8.7.1_GA_I670.RHEL7_64.20161025045328
Fichier  Édition  Affichage  Rechercher  Terminal  Aide
zimbra-mta
zimbra-dnscache
zimbra-snmp
zimbra-store
zimbra-apache
zimbra-spell
zimbra-memcached
zimbra-proxy
```

Figure 3. 20: Listes des modules de Zimbra installé.

```

The system will be modified. Continue? [N] y
Installing packages

zimbra-core will be downloaded.
zimbra-ldap will be downloaded.
zimbra-logger will be downloaded.
zimbra-mta will be downloaded.
zimbra-dnscache will be downloaded.
zimbra-snmp will be downloaded.
zimbra-store will be downloaded.
zimbra-apache will be downloaded.
zimbra-spell will be downloaded.
zimbra-memcached will be downloaded.
zimbra-proxy will be downloaded.
Downloading packages. This will not modify the system. This may take some time.

```

Figure 3. 21: Fin de l'exécution de scripte d'installation.

### **Etape 10** : Création d'un mot de passe pour l'administrateur :

Une fois que tous les packages Zimbra sont installés dans le backend, on va définir le mot de passe de l'administrateur (figure 3.22).

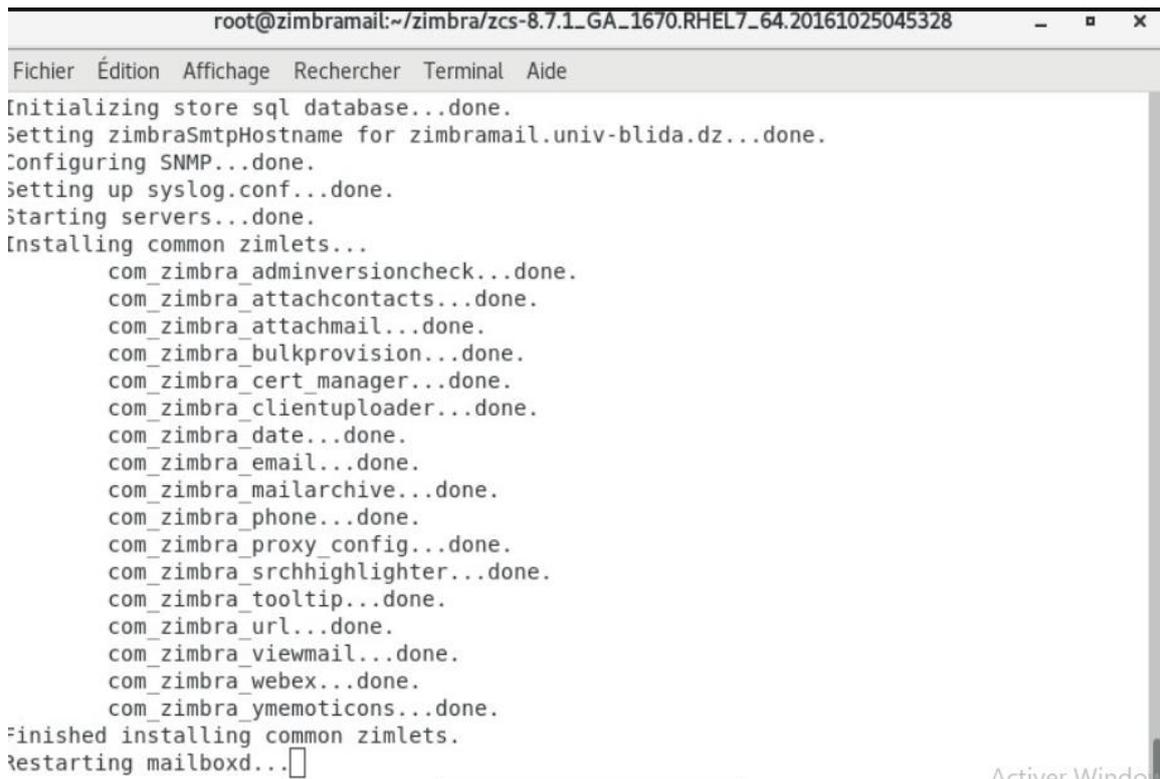
```

root@zimbramail:~/zimbra/zcs-8.7.1_GA_1670.RHEL7_64.20161025045328
Fichier  Édition  Affichage  Rechercher  Terminal  Aide
4) Admin Password: set
5) Anti-virus quarantine user: virus-quarantine.aofj5d7ny@zimbramail.univ-blida.dz
6) Enable automated spam training: yes
7) Spam training user: spam.jzjvy54o@zimbramail.univ-blida.dz
8) Non-spam(Ham) training user: ham.8958ygljx@zimbramail.univ-blida.dz
9) SMTP host: zimbramail.univ-blida.dz
10) Web server HTTP port: 8080
11) Web server HTTPS port: 8443
12) Web server mode: https
13) IMAP server port: 7143
14) IMAP server SSL port: 7993
15) POP server port: 7110
16) POP server SSL port: 7995
17) Use spell check server: yes
18) Spell server URL: http://zimbramail.univ-blida.dz:7780/asp
19) Enable version update checks: TRUE
20) Enable version update notifications: TRUE
21) Version update notification email: admin@zimbramail.univ-blida.dz
22) Version update source email: admin@zimbramail.univ-blida.dz
23) Install mailstore (service webapp): yes
24) Install UI (zimbra,zimbraAdmin webapps): yes

```

Figure 3. 22: Création d'un mot de passe pour l'administrateur.

Une fois que nous avons appliqué toutes les modifications et démarré les services liés à Zimbra, nous obtiendrons le résultat comme suit (figure 3.23).

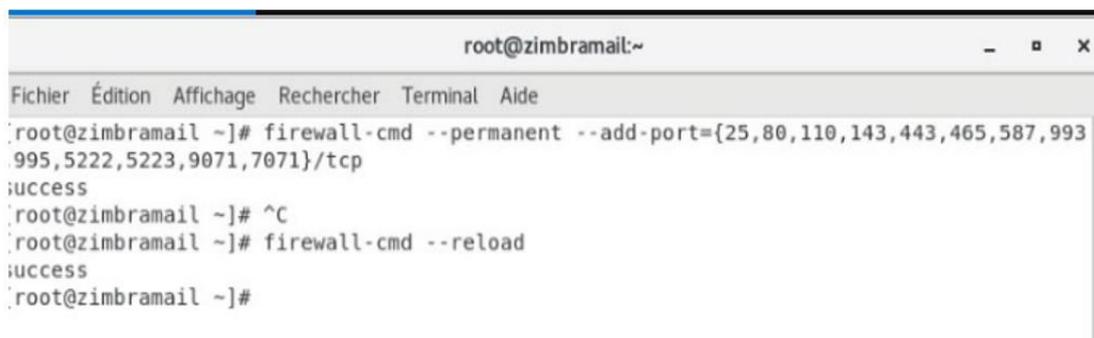


```
root@zimbramail:~/zimbra/zcs-8.7.1_GA_1670.RHEL7_64.20161025045328
Fichier Édition Affichage Rechercher Terminal Aide
Initializing store sql database...done.
Setting zimbrasMtpHostname for zimbramail.univ-blida.dz...done.
Configuring SNMP...done.
Setting up syslog.conf...done.
Starting servers...done.
Installing common zimlets...
  com_zimbra_adminversioncheck...done.
  com_zimbra_attachcontacts...done.
  com_zimbra_attachmail...done.
  com_zimbra_bulkprovision...done.
  com_zimbra_cert_manager...done.
  com_zimbra_clientuploader...done.
  com_zimbra_date...done.
  com_zimbra_email...done.
  com_zimbra_mailarchive...done.
  com_zimbra_phone...done.
  com_zimbra_proxy_config...done.
  com_zimbra_srchhighlighter...done.
  com_zimbra_tooltip...done.
  com_zimbra_url...done.
  com_zimbra_viewmail...done.
  com_zimbra_webex...done.
  com_zimbra_ymemoticons...done.
Finished installing common zimlets.
Restarting mailboxd...□
```

Figure 3. 23: Fin d'installation

### **Etape 11** : Configuration du firewall logiciel

Nous ouvrirons les ports dans le pare-feu si le pare-feu du système d'exploitation est activé sur notre serveur (figure 3.24).



```
root@zimbramail:~
Fichier Édition Affichage Rechercher Terminal Aide
root@zimbramail ~]# firewall-cmd --permanent --add-port={25,80,110,143,443,465,587,993,995,5222,5223,9071,7071}/tcp
success
root@zimbramail ~]# ^C
root@zimbramail ~]# firewall-cmd --reload
success
root@zimbramail ~]#
```

Figure 3. 24: Ouverture de port mail.

## **3.4 Administration de serveur de messagerie**

Il existe Deux types d'administrateurs peuvent être créés : Administrateur global et Administrateurs délégués

### 3.4.1 Administrateur global

Les tâches d'administration globale sont effectuées soit à partir de la console d'administration, soit à l'aide des outils d'interface de ligne de commande Zimbra.

Les principales responsabilités des administrateurs globaux incluent la configuration des éléments suivants :

- Paramètres globaux qui définissent les valeurs globales par défaut pour les serveurs, comptes, COS et domaines.
- Paramètres de domaines, paramètres GAL et paramètres d'authentification.
- Services serveur, MTA, IMAP et POP
- Comptes d'utilisateurs, alias et listes de distribution, attribuant un COS à un compte ou configurant les fonctionnalités et les préférences d'un compte individuel.
- Planifications de sauvegarde afin qu'en cas de panne du système, les serveurs de messagerie Zimbra puissent être restaurés.
- Maintenance générale et surveillance du système de messagerie.

En outre, l'administrateur général peut télécharger et exécuter l'assistant de migration pour importer des comptes de messagerie sur le serveur Zimbra.

L'administrateur général peut déléguer un utilisateur en tant qu'administrateur de domaine et attribuer un COS spécifique à un domaine.

### 3.4.2 Administrateurs délégués

L'un des rôles d'administrateur délégué préconfigurés est la liste de distribution des administrateurs de groupe d'administrateurs de domaine. Pour tous les droits associés au rôle d'administrateur de domaine, un compte d'administrateur est attribué au groupe zimbradomainadmins.

L'administrateur de domaine peut créer des comptes uniquement pour son domaine et toutes les tâches sont effectuées à partir de la console d'administration.

Le groupe « DL zimbradomainadmins » a reçu les droits qui permettent aux administrateurs de domaine de gérer les tâches suivantes sur leur domaine :

- Modifier les informations du compte.
- Changer les mots de passe.
- Changer le statut d'un compte.
- Créer, supprimer et déplacer des alias.

- Créer, modifier et supprimer des listes de distribution.
- Attribuer d'autres utilisateurs en tant qu'administrateurs.
- Téléchargez et exécutez les outils d'importation et de migration.
- Afficher les quotas de boîte aux lettres.

Pour prendre en main l'interface web d'administrateur il faut se rendre sur l'interface web en https sur le port 7071 : <https://zimbramail.univ-blida.dz:7071/zimbraAdmin/> :

1. On va accéder au Console d'utilisateur AJAX de type navigateur. Avec L'URL suivant (figure 3.25) :



Figure 3. 25: Accès l'interface administrateur.

2. Afin d'accéder à notre espace d'administration, on va entrer le nom d'utilisateur et le mot de passe déjà attribuer au cours de l'installation précédente (figure 3.26 et figure 3.27).



Figure 3. 26: Interface web administrateur.



Figure 3. 27: Page d'accueil d'administrateur.

### 3. Vérification de l'état du serveur :

Service	Heure
✓ logger	25 Aou 20 11:28
✓ antivirus	25 Aou 20 11:28
✓ ldap	25 Aou 20 11:28
✓ proxy	25 Aou 20 11:28
✓ stats	25 Aou 20 11:28
✓ mta	25 Aou 20 11:28
✓ memcached	25 Aou 20 11:28
✓ antispam	25 Aou 20 11:28
✓ amavis	25 Aou 20 11:28
✓ service	25 Aou 20 11:28
✓ opendkim	25 Aou 20 11:28
✓ zimbraAdmin	25 Aou 20 11:28
✓ zmconfigd	25 Aou 20 11:28
✓ snmp	25 Aou 20 11:28
✓ spell	25 Aou 20 11:28
✓ mailbox	25 Aou 20 11:28
✓ zimbra	25 Aou 20 11:28
✓ zimlet	25 Aou 20 11:28

Figure 3. 28: Vérification de l'état du serveur.

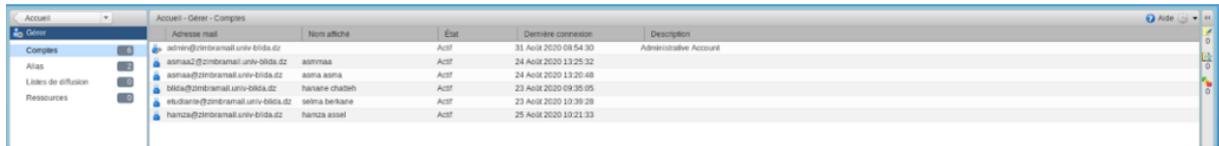
### 4. Création compte d'utilisateur :

Pour ajouter un compte, nous utilisons l'option 3 « Ajouter des comptes » et « ajouter un compte ». Il nous suffit ensuite de remplir les différents champs et d'appuyer sur « terminer » (figure 3.29) :

Figure 3. 29: Création d'un compte utilisateur.

## 5. Présentation des comptes Zimbra :

Dans cette étape on vérifie l'existence des comptes déjà créés précédemment (figure 3.30).



Comptes	Adresse mail	Nom affiché	État	Dernière connexion	Description
Administrative Account	admin@zimbramail.univ-blida.dz	admin	Actif	31 Août 2020 08:54:30	Administrative Account
asimaa	asimaa@zimbramail.univ-blida.dz	asimaa	Actif	24 Août 2020 13:25:32	
asima asima	asima@zimbramail.univ-blida.dz	asima asima	Actif	24 Août 2020 13:20:48	
hanane chatteh	blida@zimbramail.univ-blida.dz	hanane chatteh	Actif	23 Août 2020 09:35:05	
selma berkane	selma@zimbramail.univ-blida.dz	selma berkane	Actif	23 Août 2020 19:38:28	
hamza essel	hamza@zimbramail.univ-blida.dz	hamza essel	Actif	25 Août 2020 10:21:33	

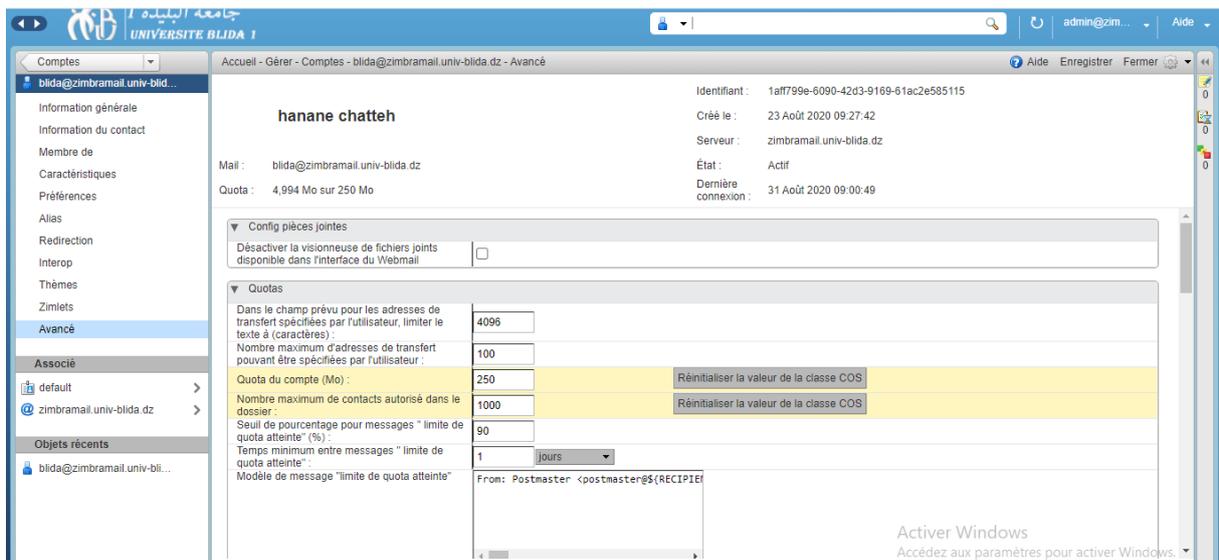
Figure 3. 30: Listes des comptes créés.

## 6. Ajouter Quota du compte à l'utilisateur :

Chaque utilisateur dispose, sauf exception, d'un **quota de X MO** pour stocker tous les éléments de son compte Zimbra (messages, calendriers, ...).

Seul Administrateur peut appliquer des quotas pour limiter la quantité d'espace disque que votre boîte mail peut consommer.

Dans notre cas, nous avons un disque dur d'une capacité de 500 Go si nous utilisons 450 Go pour les utilisateurs et nous avons donné à chacun d'eux 250 Mo, alors le nombre d'utilisateur ça sera autour de 1800 (figure 3.31).



hanane chatteh

Identifiant : 1aff799e-6090-42d3-9169-61ac2e585115  
Créé le : 23 Août 2020 09:27:42  
Serveur : zimbramail.univ-blida.dz  
État : Actif  
Dernière connexion : 31 Août 2020 09:00:49

Mail : blida@zimbramail.univ-blida.dz  
Quota : 4,994 Mo sur 250 Mo

Config pièces jointes  
Désactiver la visionneuse de fichiers joints disponible dans l'interface du Webmail

Quotas

Dans le champ prévu pour les adresses de transfert spécifiées par l'utilisateur, limiter le texte à (caractères) :	4096	
Nombre maximum d'adresses de transfert pouvant être spécifiées par l'utilisateur :	100	
Quota du compte (Mo) :	250	Réinitialiser la valeur de la classe COS
Nombre maximum de contacts autorisé dans le dossier :	1000	Réinitialiser la valeur de la classe COS
Seuil de pourcentage pour messages " limite de quota atteinte" (%) :	90	
Temps minimum entre messages " limite de quota atteinte" :	1	jours
Modèle de message "limite de quota atteinte"	From: Postmaster <postmaster@RECIPIE>	

Figure 3. 31: Les informations de compte.

Pendant l'utilisation, le disque dur commence à se saturer de temps en temps, pour résoudre ce problème nous suggérons une solution, qui consiste à ajouter un autre disque dur pour les utilisateurs uniquement, Où nous bénéficierons également de l'introduction d'un plus grand nombre d'utilisateurs.

Si vous avez dépassé le quota, voici ce qui pourrait se passer :

- Vous recevez un mail de notification.
- Votre interface mail affiche une notification lorsque vous vous connectez.
- Les mails qui vous sont envoyés peuvent être renvoyés à l'expéditeur accompagnés d'une notification leur indiquant que votre boîte aux lettres est saturée.

La barre de progression montre le quota d'espace occupé de la messagerie d'un utilisateur (figure 3. 32).



Figure 3. 32: Quota d'utilisateur.

**Zimbra Open Drive** :est un interface Zimbra avec les produits tiers, Nextcloud et ownCloud, qui sont externes à Zimbra. Zimbra Open Drive comprend trois parties: Zimbra Extension, Zimlet et Cloud App. Ces pièces intègrent des services de stockage externe et un mécanisme d'authentification dans l'interface Web Zimbra.

## 7. Modification du LOGO via commande Line

Pour modifier LOGO :

**A-** On va d'abord montrer le dossier dans lequel se trouve le fichier logo à modifier, et enregistrer les deux photo (Myappbanner.png ; Myloginebanner.png) dans fichier logo.

**B-** Ajoutez les commandes suivantes dans le terminal (figure 3.33).

```
#mkdir /opt/zimbra/jetty/webapps/zimbra/logos/  
# chown zimbra:zimbra /opt/zimbra/jetty/webapps/zimbra/logos/MyLoginBanner.png  
# chown zimbra:zimbra /opt/zimbra/jetty/webapps/zimbra/logos/MyAppBanner.png  
# su zimbra
```

```
[root@zimbra]# mkdir /opt/zimbra/jetty/webapps/zimbra/logos/  
[root@zimbra]# chown zimbra:zimbra /opt/zimbra/jetty/webapps/zimbra/logos/  
MyLoginBanner.png  
[root@zimbra]# chown zimbra:zimbra /opt/zimbra/jetty/webapps/zimbra/logos  
/MyAppBanner.png  
chown: impossible d'accéder à = /opt/zimbra/jetty/webapps/zimbra/logos/MyAppBann  
er.png =: Aucun fichier ou dossier de ce type  
[root@zimbra]# chown zimbra:zimbra /opt/zimbra/jetty/webapps/zimbra/logos  
/MyAppBanner.png  
[root@zimbra]# su zimbra  
[zimbra@zimbra root]$ zmprov md univ-blida.dz zimbraSkinLogoURL https://univ  
-blida.dz  
ERROR: account.NO SUCH DOMAIN (no such domain: univ-blida.dz)  
[zimbra@zimbra root]$ zmprov md zimbra.univ-blida.dz zimbraSkinLogoURL h  
ttps://univ-blida.dz
```

Figure 3. 33: Le fichier LOGO.

Le logo Zimbra sur la page d'accueil a été remplacé avec succès par le logo de l'Université Saad Dahlab Blida 1 (figure 3.34).



Figure 3. 34: Interface web de l'administrateur.

Lorsque nous cliquons sur le logo Saad Dahlab, cela nous amènera à la page de lien Zimbra donc, on doit désactiver le lien vers Zimbra et on réaliser un lien vers l'adresse web de l'université par la procédure suivante :

```
# zmprov md univ-blida.dz zimbraSkinLogoURL https://univ-blida.dz
# zmprov md univ-blida.dz zimbraSkinLogoLoginBanner /logos/MyLoginBanner.png
# zmprov md univ-blida.dz zimbraSkinLogoAppBanner /logos/MyAppBanner.png
# zmcontrol restart
```

### 3.5 Client de messagerie Zimbra

Le client web de Zimbra est très apprécié pour son interface intuitive. Basé sur les dernières technologies web 2.0 (Ajax), il s'agit un outil de productivité personnelle aux fonctionnalités riches :

Organisation des emails par message ou par conversation

- Recherche simple ou avancée
- Étiquettes ("tags") pour classer ou mettre en avant les messages importants
- Visionneuse de pièces jointes
- Carnets d'adresses partagés, autocomplétion (GAL), liste de distributions personnelles
- Agendas partagés, délégation
- Création, partage, publication de documents riches en ligne, wiki
- Ajout de comptes mail externes
- VOIP et messagerie unifiée
- Intégration aux applis métiers ("Zimlets")
- Personnalisation

Avec Zimbra Web, vous pouvez utiliser un navigateur Web (Internet Explorer/Chrome/Safari/Firefox) pour accéder à votre Boîte aux lettres à distance. Après authentification, tous les dossiers de votre BAL (Boîte aux lettres) sont accessibles.

### Remarque

Firefox convient parfaitement à l'utilisation de Zimbra et permettra de profiter pleinement de l'ensemble des fonctionnalités.

1-Pour se connecter via un navigateur, voici L'url (figure 3.35) :

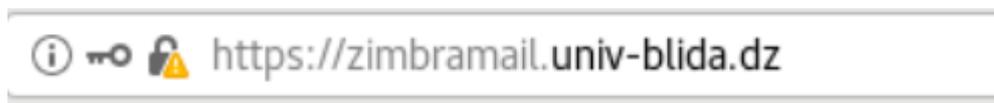


Figure 3. 35: Accéder au console utilisateur.

2-Pour une première connexion vous êtes invité à changer le mot de passe qui vous a été fourni Par l'administrateur, le mot de passe doit être composé au minimum 6 caractères (figure 3.36).

A screenshot of the Zimbra user interface for password change. The page has a blue background. At the top left is the logo of Université Blida 1. Below the logo is a yellow error message box with a red 'X' icon: "Votre mot de passe n'est plus valide : vous devez spécifier un nouveau mot de passe". Below the error message are four input fields: "Utilisateur:" with the value "blida@zimbramail.univ-blida.dz", "Mot de passe:" with a masked password "\*\*\*\*\*", "Nouveau mot de passe:" with a masked password "\*\*\*\*\*", and "Confirmez:" with a masked password "\*\*\*\*\*". Below the input fields is a checkbox labeled "Mémoriser mes valeurs d'accès" and a "Connexion" button. At the bottom left is a "Version:" label and a dropdown menu showing "Par défaut" with a "En savoir plus" link.

Figure 3. 36: Modification d'un mot passe par l'utilisateur.

### 3-Voilà l'interface de client Web

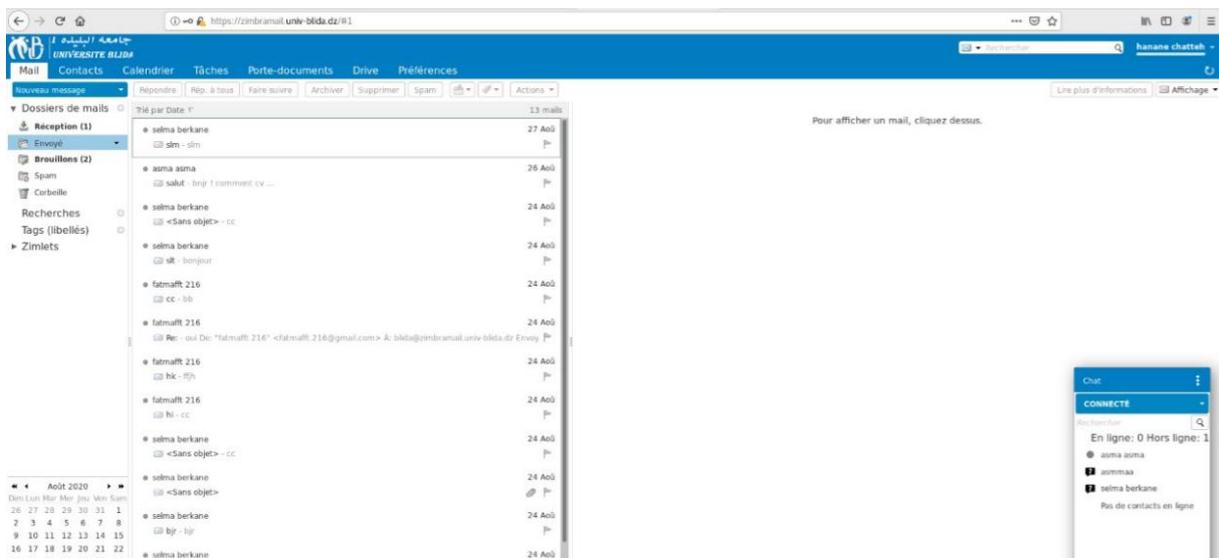


Figure 3. 37: Page d'accueil d'utilisateur.

#### 3.5.1 Fonctionnalités d'utilisateur

##### 1-L'envoi et la réception des emails

Avec l'onglet Mail l'utilisateur pourra envoyer des emails à tous types de messagerie (figure 3.38 à 3.40).

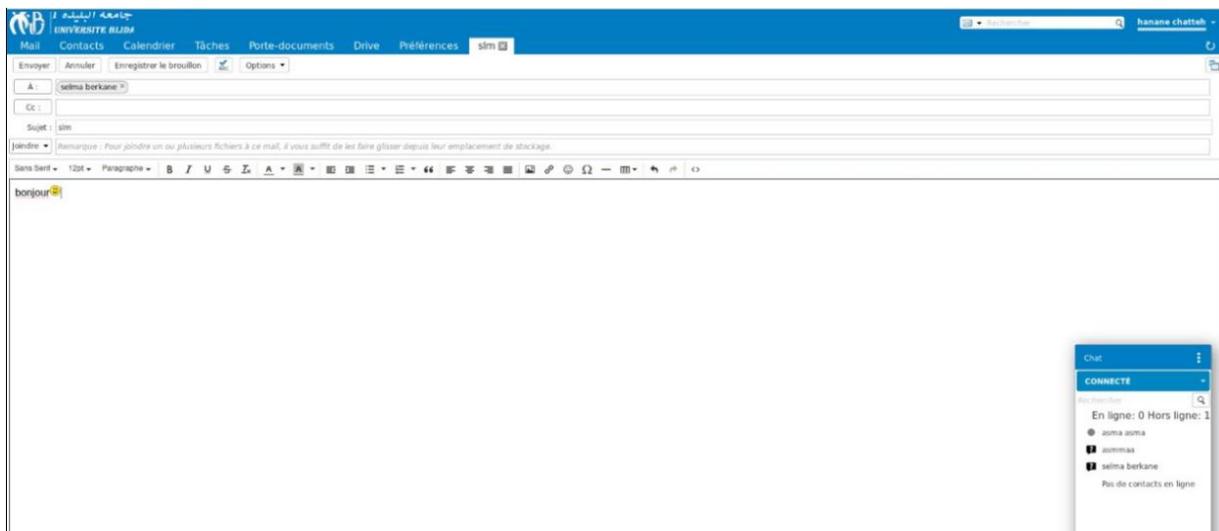


Figure 3. 38: L'envoi d'un email.

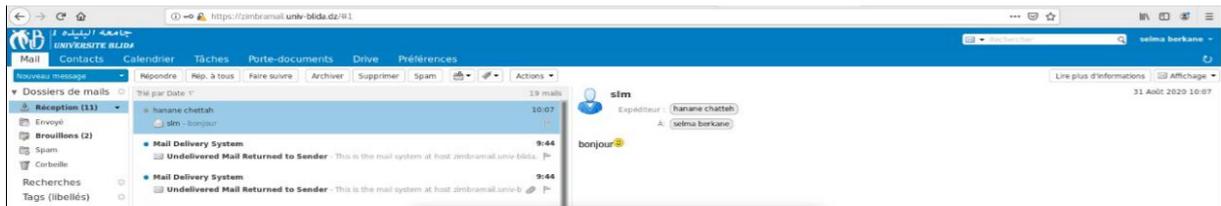


Figure 3. 39: Réception d'email.

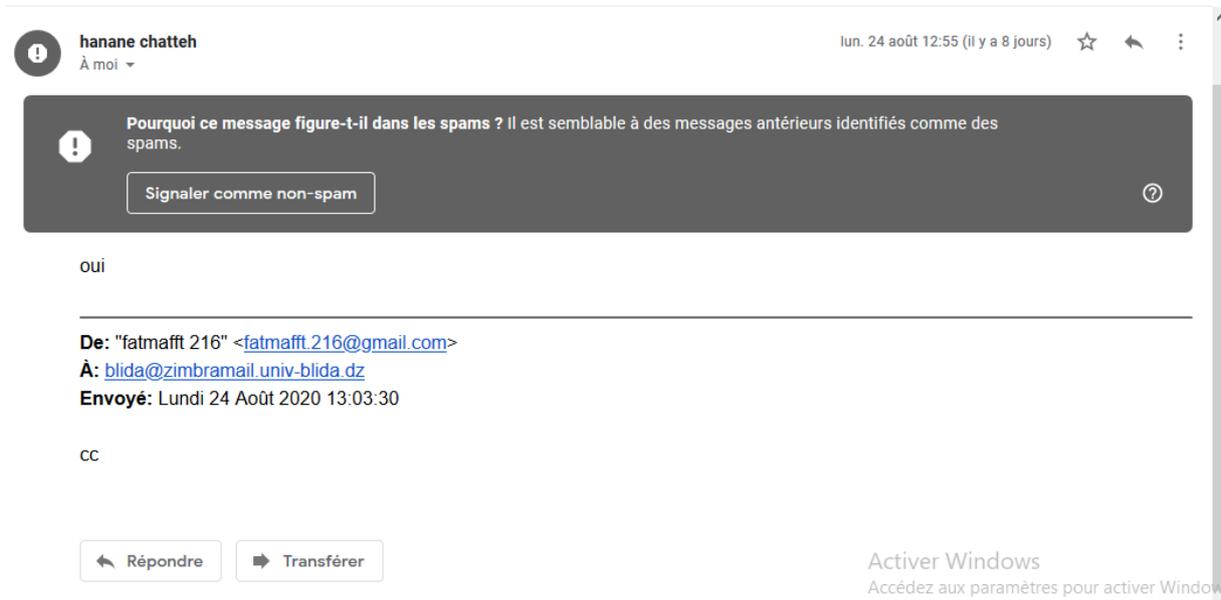


Figure 3. 40: Réception d'un mail par un utilisateur.

## 2-Ajouté un contact

L'utilisateur pourra ajouter un nombre limité de contact sur l'onglet Contacts selon le quota attribué par l'administrateur (figure 3.41).

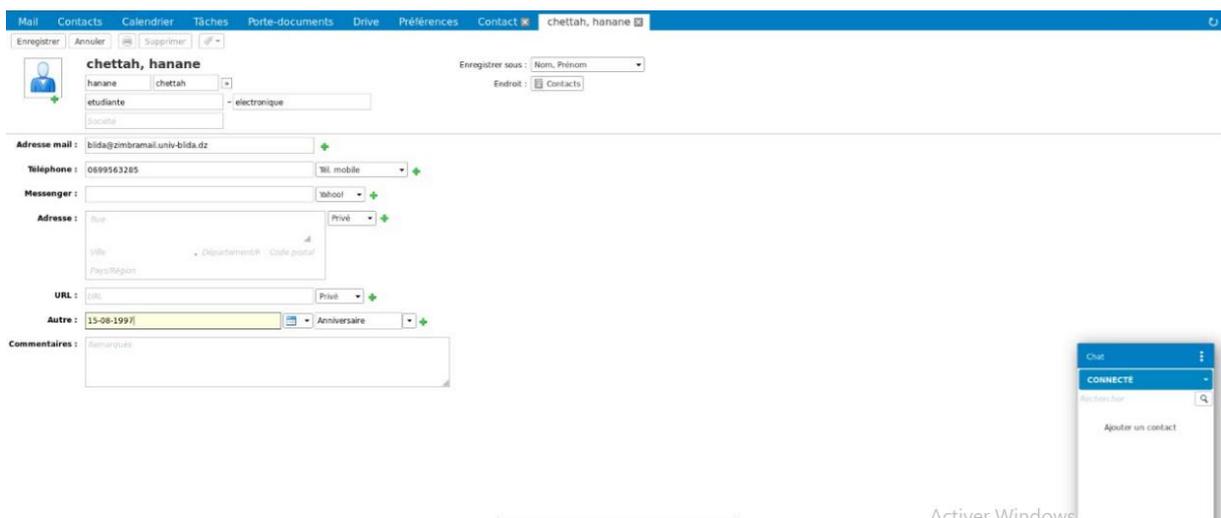


Figure 3. 41: Ajoute un contact.

### 3-Crée un groupe de contact

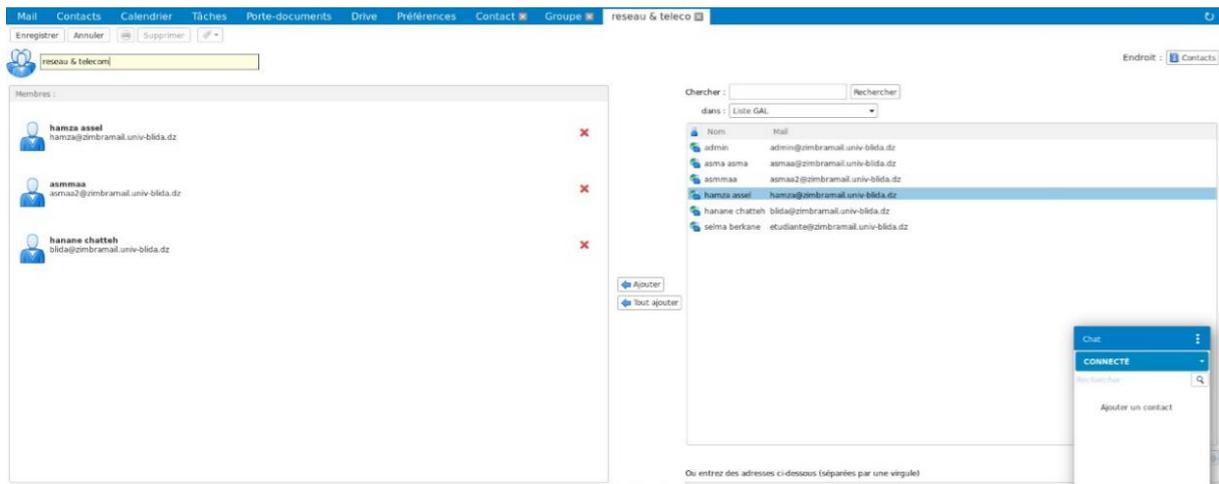


Figure 3. 42: Création un groupe de contact.

### 4-Stoker un documente

Le logiciel de messagerie Zimbra met à notre disposition l’outil Porte-documents qui nous permet de créer, de stocker ou encore de partager les documents (figure 3.43 à figure 3.45).

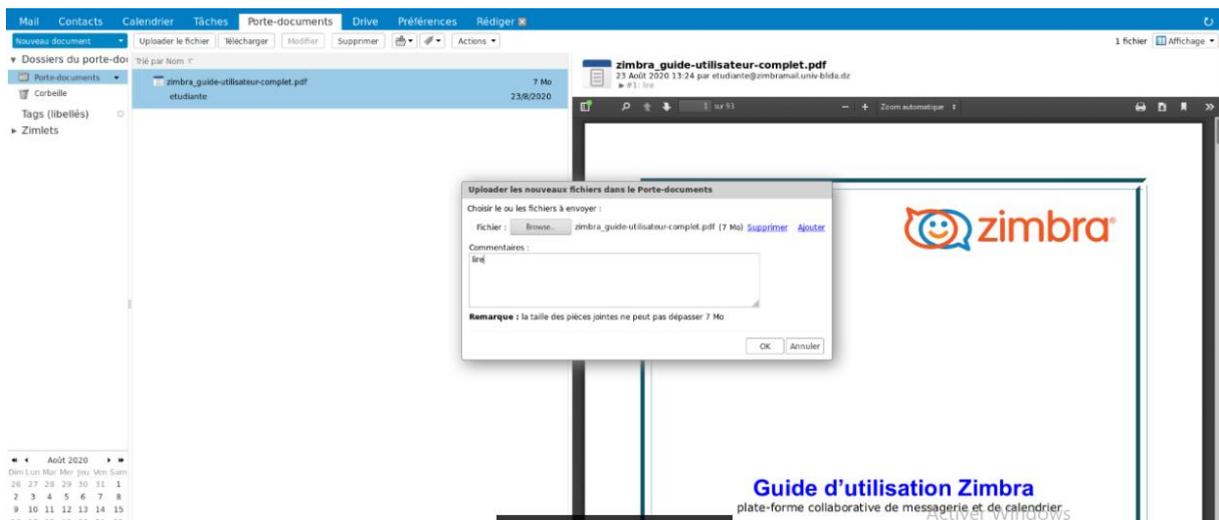


Figure 3. 43: Stocker un document.

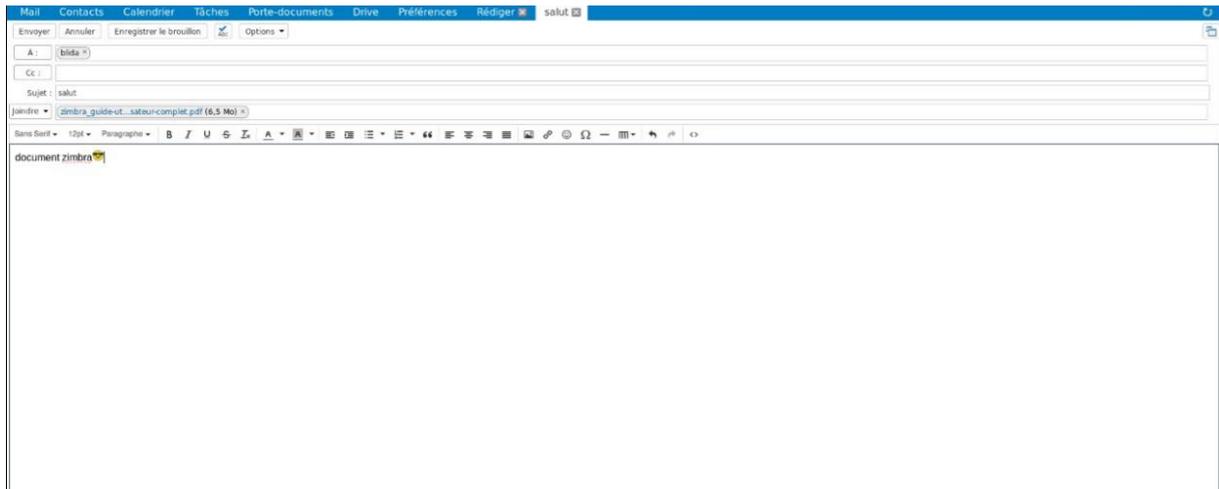


Figure 3. 44: L'envoi d'un document stocké.

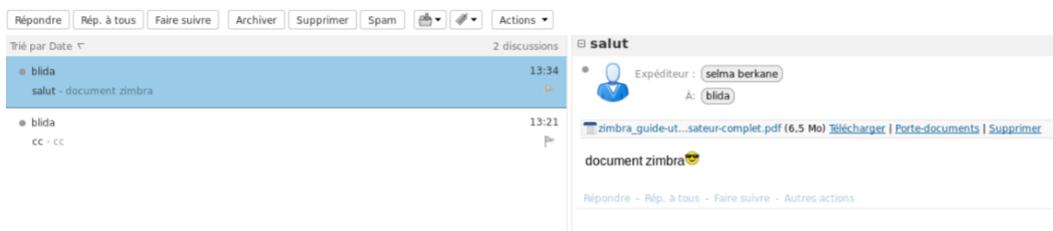


Figure 3. 45: Réception d'un document.

## 5-Gestion des rendez-vous

L'utilisateur pourra ajouter des événements ou des rendez-vous dans votre calendrier et, également, y Inviter des participants ou configurer des rappels (figure 3.46 à figure 3.48).

### ➤ Créer un rendez-vous Simple

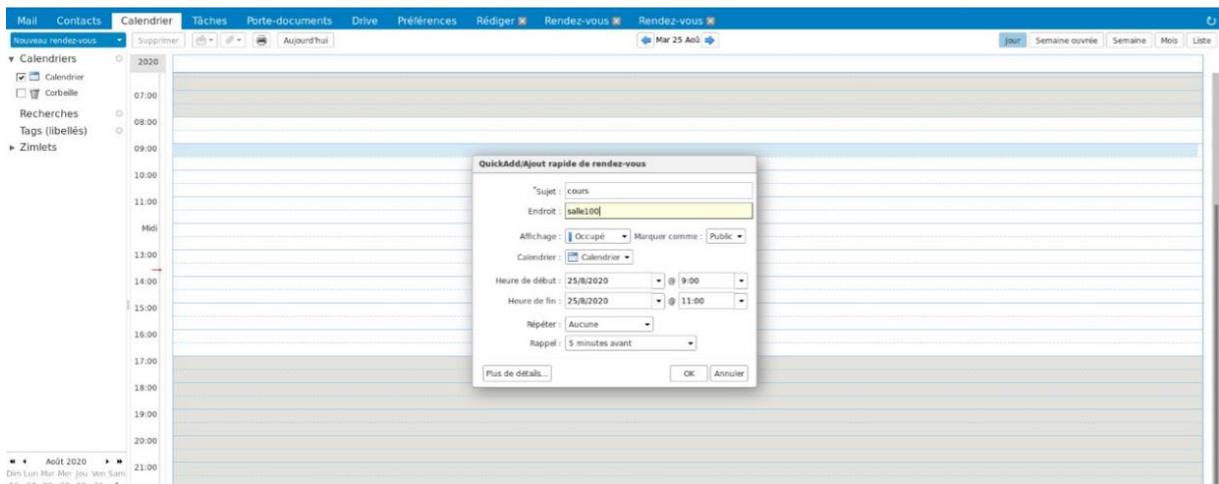


Figure 3. 46: Création d'un rendez-vous simple.

➤ Créer un rendez-vous détaillé

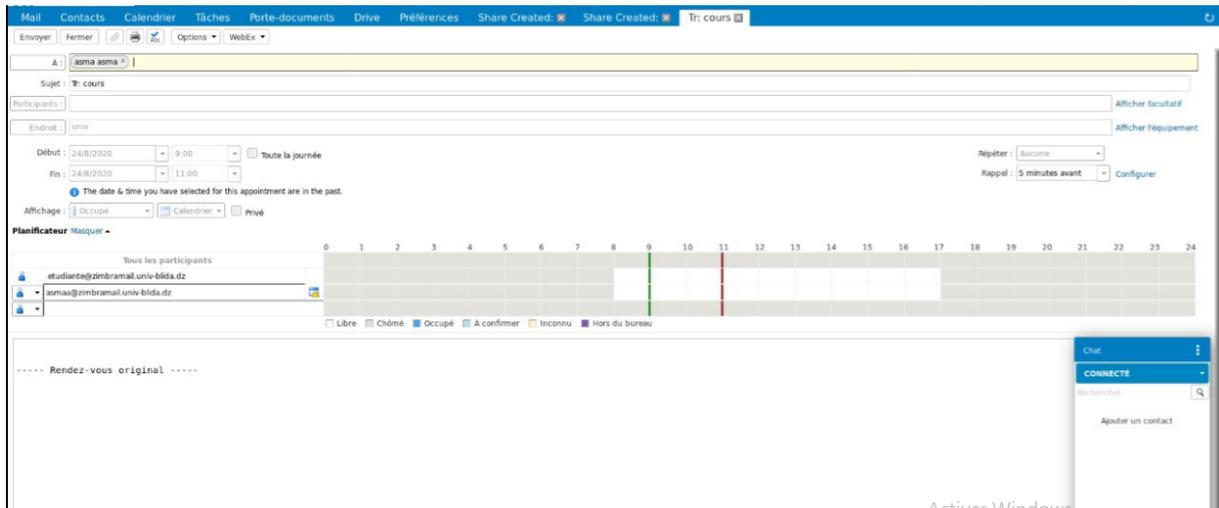


Figure 3. 47: Création d'un rendez-vous détaillé.

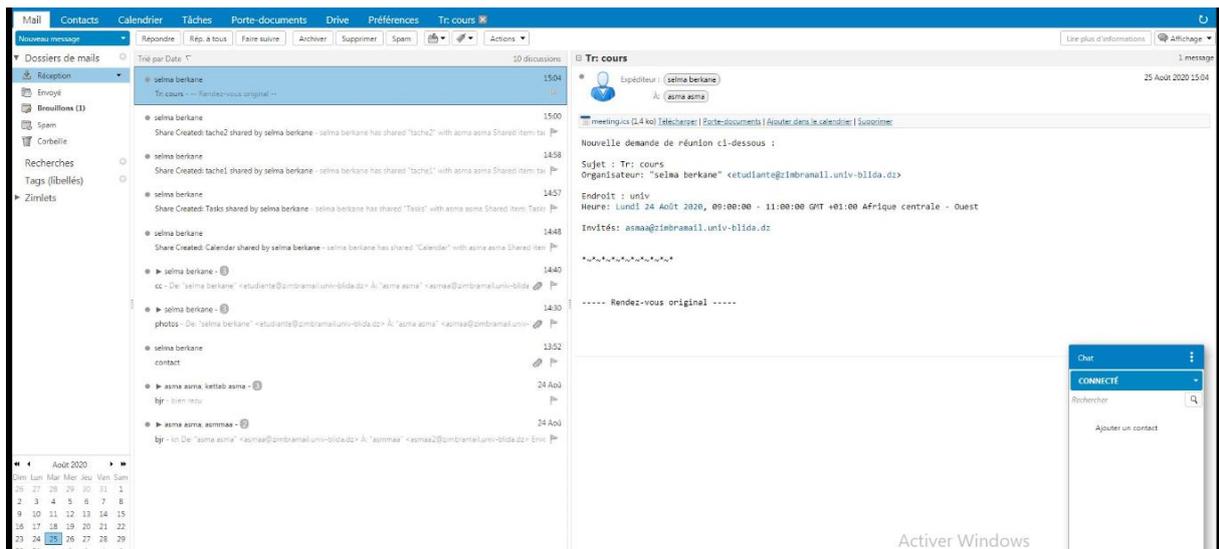


Figure 3. 48: Réception d'un rendez- vous.

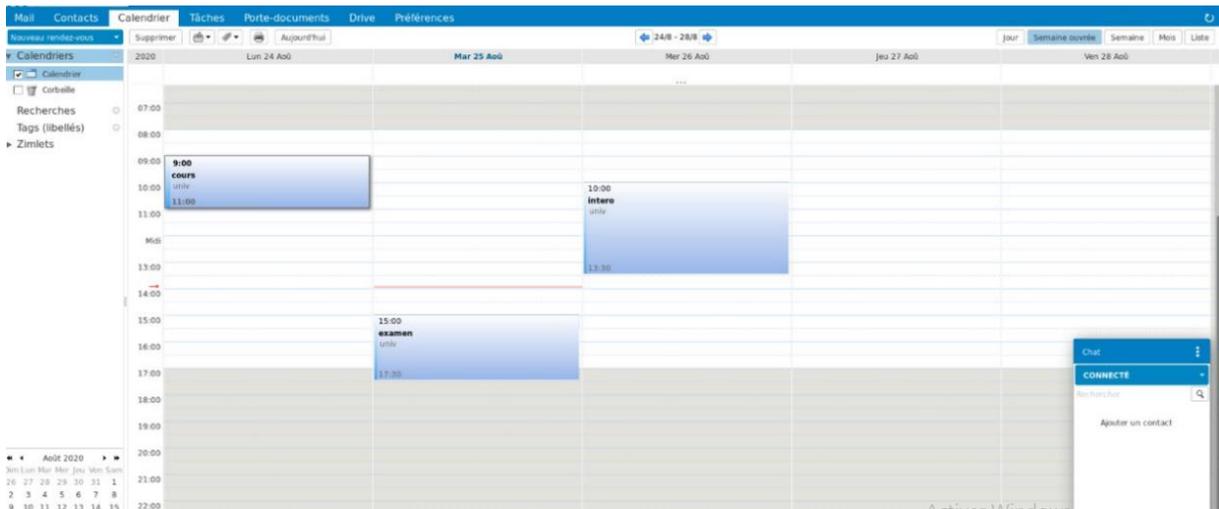


Figure 3. 49: Divers calendrier.

## 7- Gestion des Tâches

La fonction de tâches de créer des listes de tâches « à effectuer » et d’optimiser leur suivi (figure 3.50 à figure 3.52).

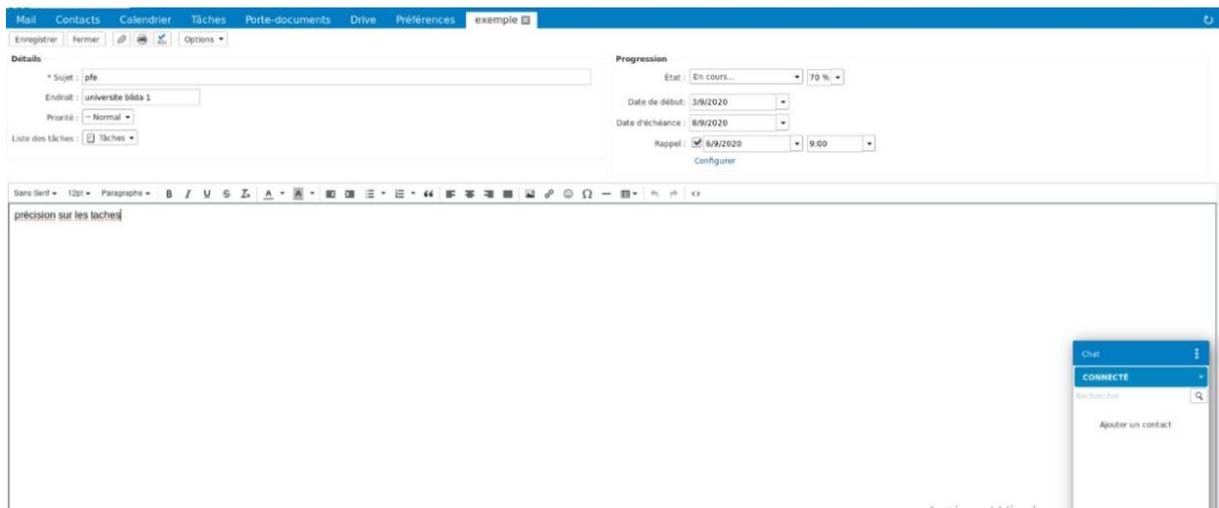


Figure 3. 50: Création d’une tâche

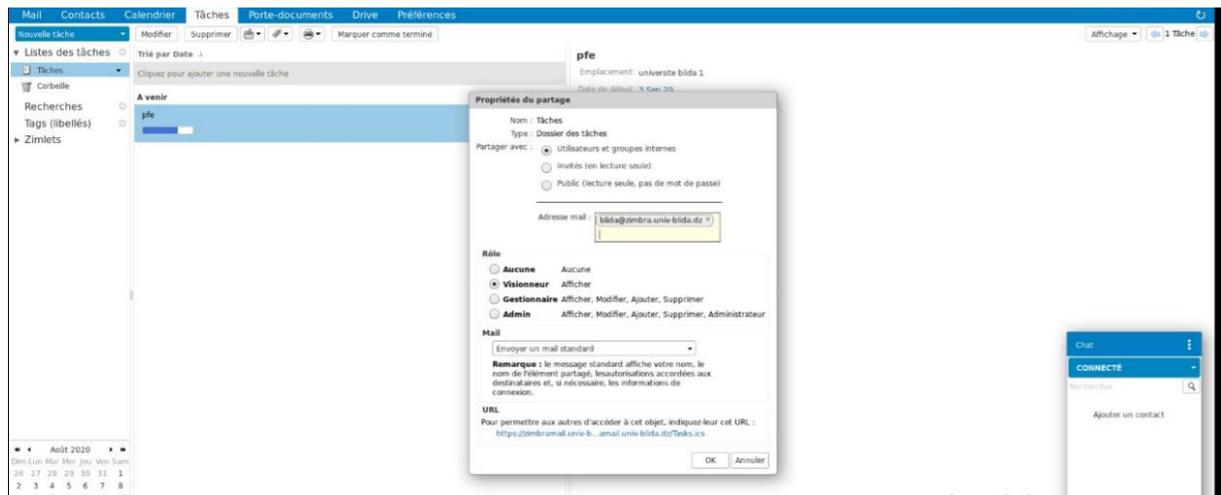


Figure 3. 51: L'envoi d'une tâche

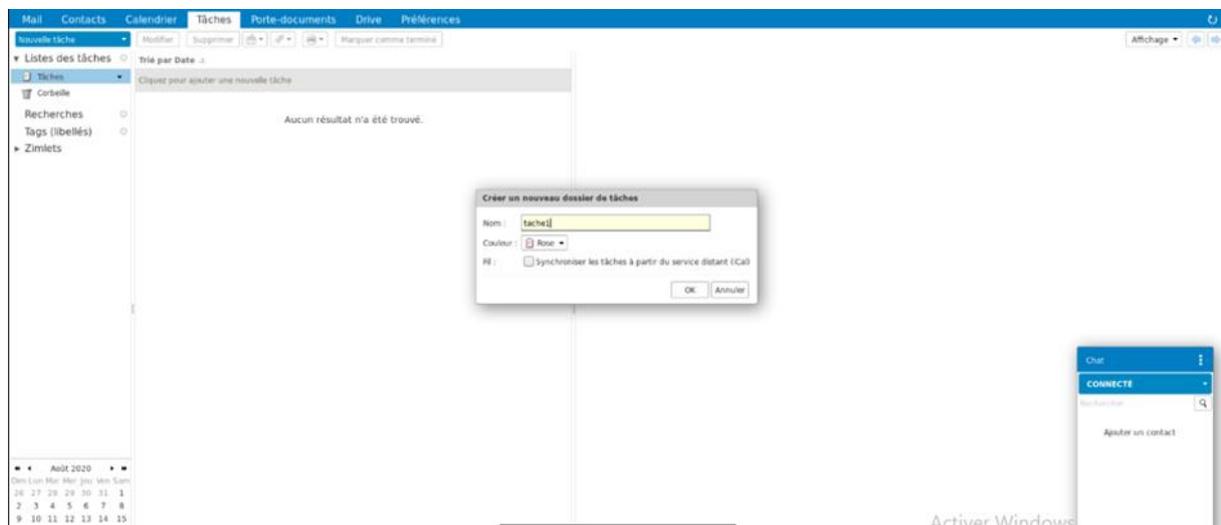


Figure 3. 52: Création une liste de tâche

## 8-Zimlets

Une zimlet est une extension rajoutée à votre webmail. Elles ajoutent de nouvelles fonctionnalités à votre serveur de messagerie (figure 3.53).

Cette table permet d'activer et de désactiver les Zimlets disponibles :

Zimlets		
Les "zimlets" sont des applications complémentaires qui améliorent les fonctionnalités de votre client. Cette table permet d'activer et de désactiver les zimlets disponibles.		
Actif	Nom	Description
<input checked="" type="checkbox"/>	Archiver	D'un simple clic, déplacez des objets vers un dossier d'archivage (allégez votre Boîte de réception).
<input checked="" type="checkbox"/>	OpenChat Zimlet	OpenChat Zimlet for Zimbra
<input checked="" type="checkbox"/>	Surligneur de recherche	Après une recherche de mail, ce Zimlet surligne les termes de la recherche en jaune
<input checked="" type="checkbox"/>	Téléphone	Souligne les numéros de téléphone pour autoriser les appels Skype
<input checked="" type="checkbox"/>	WebEx	Programmez, lancez ou rejoignez facilement des réunions WebEx
<input checked="" type="checkbox"/>	Zimbra Drive	Cloud integration for Zimbra
<input checked="" type="checkbox"/>	Émoticônes Yahoo!	Affiche des images Émoticônes Yahoo! dans les mails

Figure 3. 53 : Menu Zimlets.

L'utilisateur peut modifier l'activation des zimlets dans l'onglet préférences, par exemple pour désactiver la messagerie instantané(chat) sous Zimbra il doit décocher la case « open chat zimlet » Une fenêtre de chat est désormais invisible (figure 3.54)

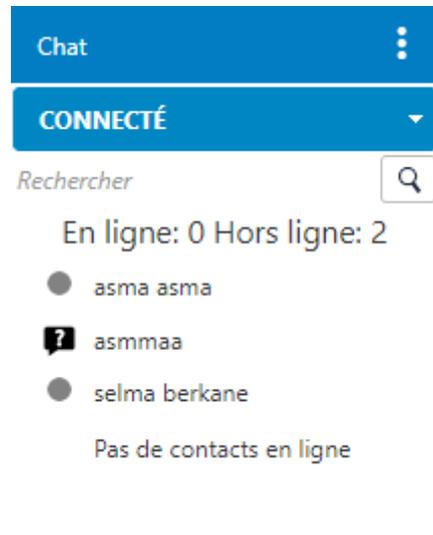


Figure 3. 54 : Fenêtre chat

## 9-Gestion du Spam

**Spam** : technique de prospection consistant à diffuser massivement par courrier électronique des informations, souvent de nature publicitaire, non sollicitées par les destinataires.

Les mails pouvant être considérés comme spam (mais avec le bénéfice du doute) sont placés automatiquement ou manuellement dans le dossier Spam. Vous pouvez consulter ces mails, les déplacer hors du dossier Spams ou les supprimer. Si vous ne déplacez ou ne supprimez pas ces mails, ils seront purgés après un délai défini par votre administrateur.

## 10-Filtrer les indésirables « spams »

L'objectif de filtrer les messages identifiés comme indésirables « spams » est de les ranger dans une boîte distincte de la boîte de réception des messages

- Créer le dossier « \_PUB\_RENATER »

Dans la boîte de dialogue qui s'ouvre, nous avons saisi le nom de dossier et sa couleur puis ok (figure 3.55) :

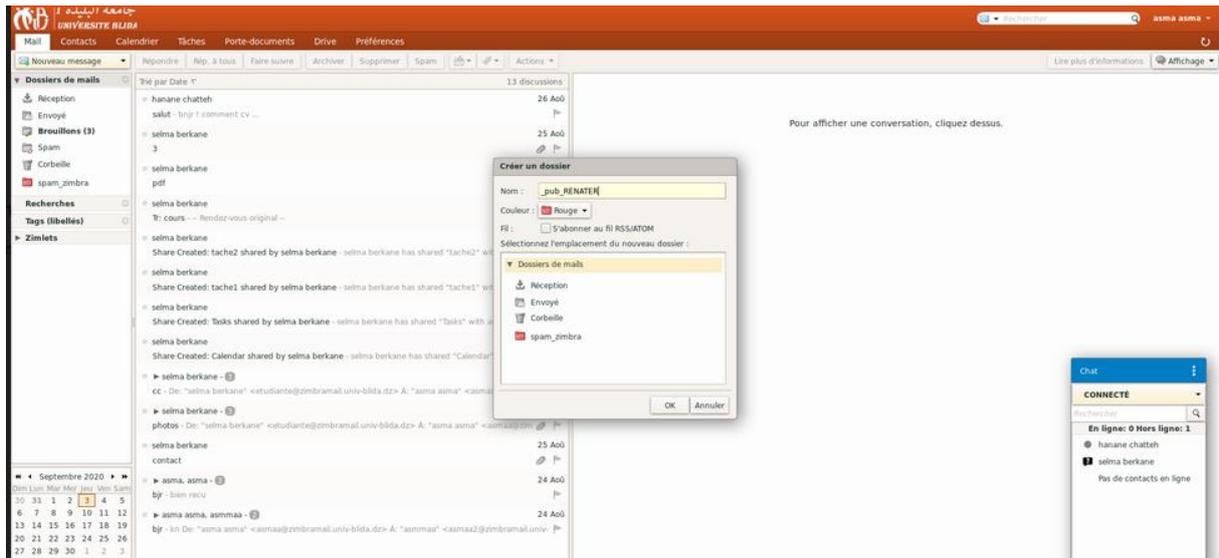


Figure 3. 55: Création dossier spam.

➤ Crée un nouveau filtre « PUB »

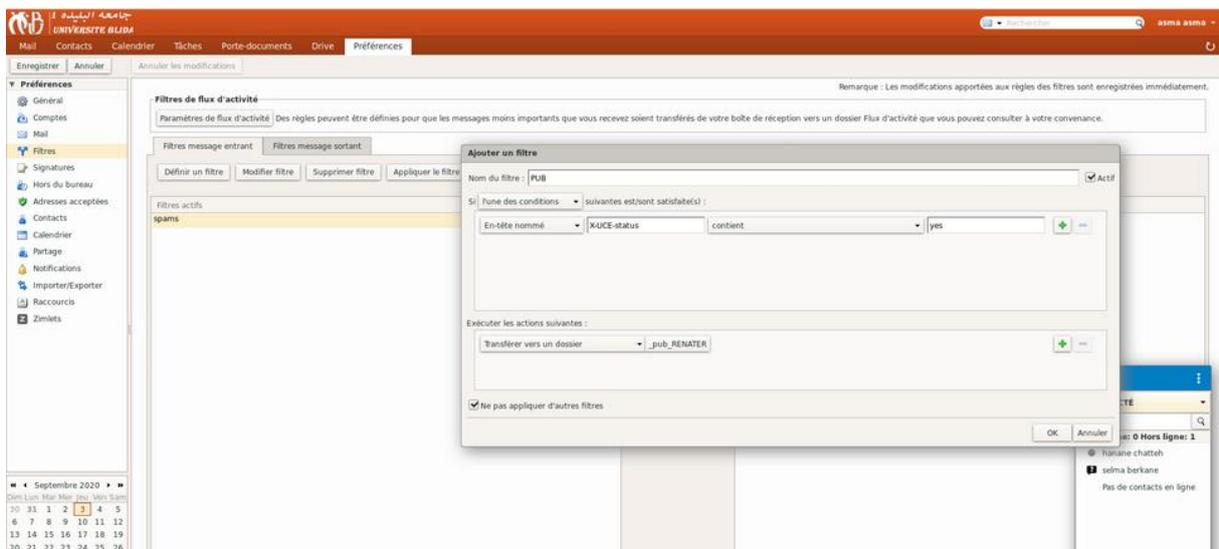


Figure 3. 56: Création filtre.

Si le dossier « \_pub\_renater » contient un email qui vous intéresse, il est possible d'exclure du filtre l'expéditeur du mail (figure 3.57).

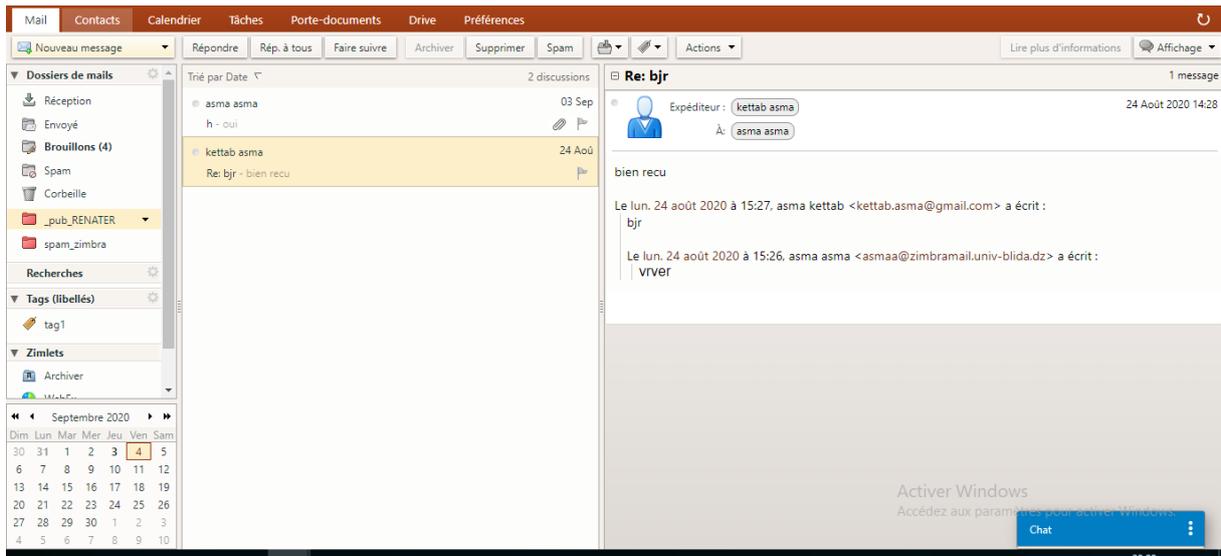


Figure 3. 57: Réception d'un message spam.

La fenêtre de modification du filtre « PUB » s'affiche

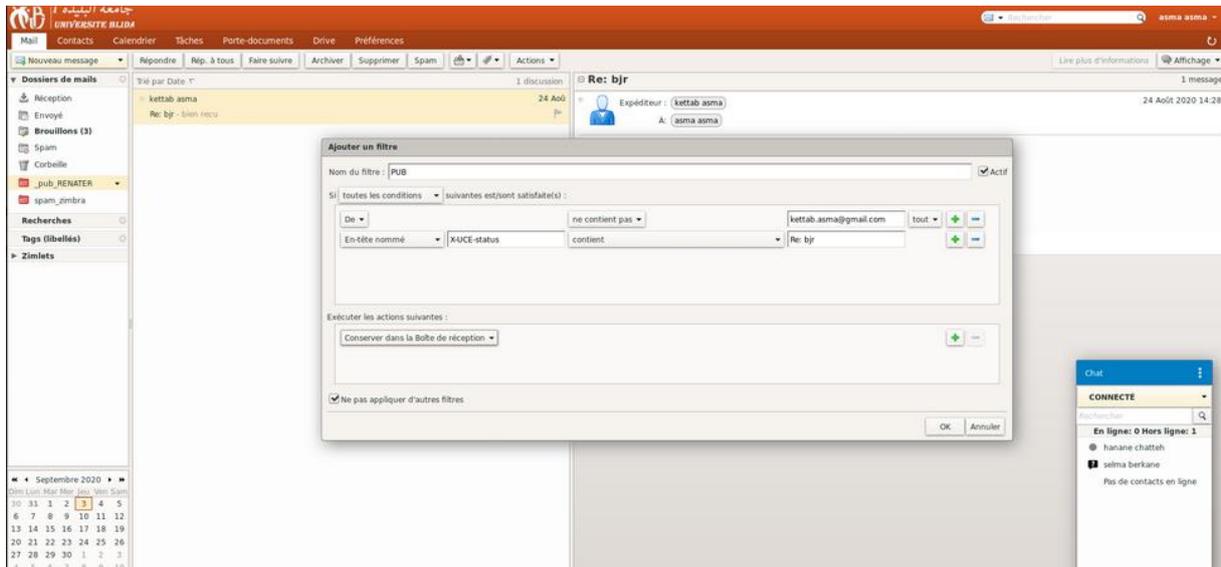


Figure 3. 58 : Affichage fenêtre de filtre

### 11-Affecter des tags

Les tags servent de système de classement personnel pour vos mails, contacts et rendez-vous. Les tags vous permettent de rechercher ces éléments. Les mails qui sont marqués d'un tag peuvent se trouver dans différents dossiers. Ils fournissent un moyen d'afficher tous les mails portant un tag spécifique, où qu'ils se trouvent.

Vous pouvez créer et appliquer plusieurs tags à un seul élément afin de le classer simultanément dans plusieurs catégories. Après la création d'un tag, vous pouvez l'appliquer à des conversations, des mails ou des contacts (figure 3.59 et figure 3.60).

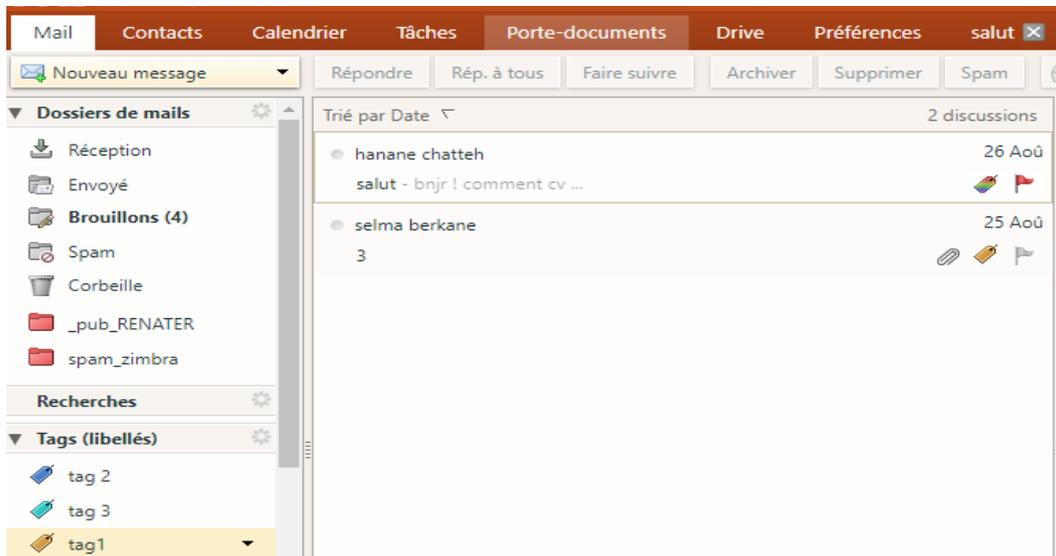


Figure 3. 59: Création de tag d'un mail.

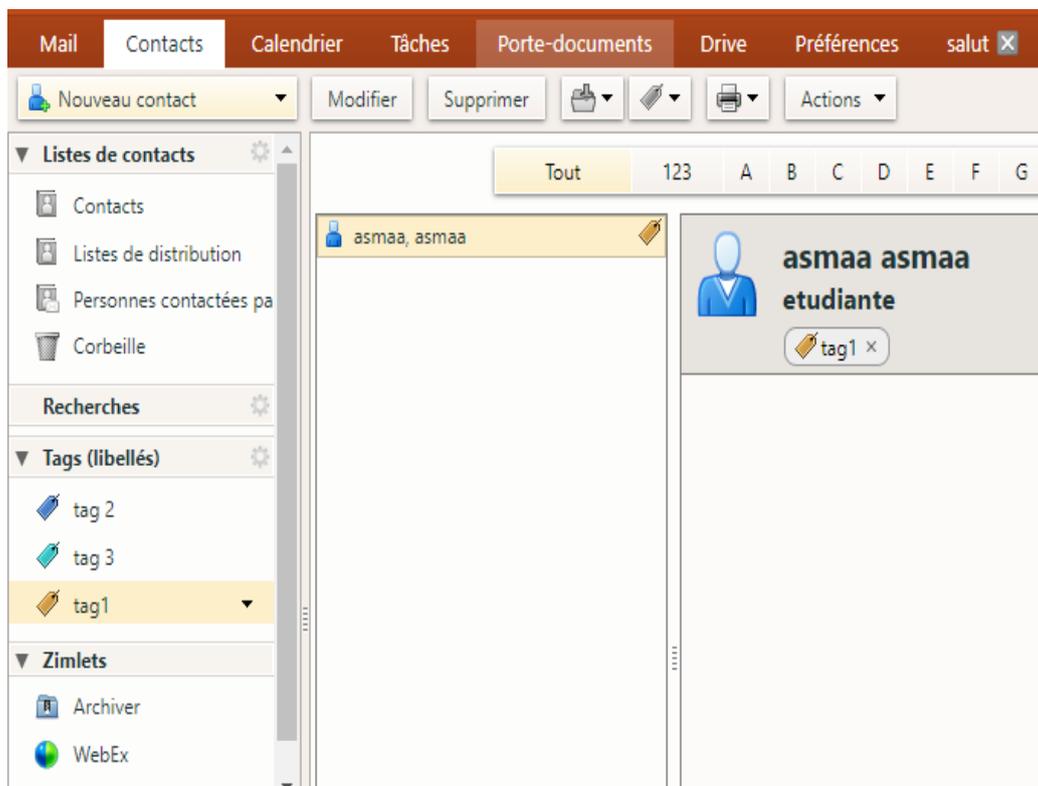


Figure 3. 60: Création de tag d'un contact.

## 12-WebEx

Ce Zimlet intègre WebEx avec la Zimbra Collaboration Suite. Le Zimlet vous permet de lister vos prochaines réunions WebEx, ainsi que d'héberger et de rejoindre une réunion WebEx en 1 clic. Faites glisser et déposez des contacts et des rendez-vous pour créer de nouvelles réunions WebEx.

- Faites un clic droit sur l'icône du panneau Zimlet pour gérer vos comptes et réunions WebEx

Gestion des comptes

réunion réunion1

**Paramètres du compte :**

Nom du compte : réunion **Supprimer**

Nom d'utilisateur WebEx :\* hanane

Mot de passe WebEx :\* .....

Identifiant Société WebEx :\* zimbramail aide

Mot de passe de réunion WebEx : 123456 (facultatif)

Hôte(s) alternatif(s) aide

Utiliser ce compte WebEx pour : Tous les calendriers ▼

Valider Compte 1 Ajouter les paramètres de téléphonie

Ajouter un compte OK Annuler

Figure 3. 61: Gestion des comptes.

- Créer une réunion WebEx lors de la création d'un rendez-vous

UNIVERSITE BLIDA

Mail Contacts Calendrier Tâches Porte-documents Drive Préférences pfe

Envoyer Enregistrer Fermer Options WebEx

Sujet : pfe

Participants : hanane chatteh x Afficher facultatif

Suggérer une heure

Endroit : univ Afficher l'équipement

Suggérer un emplacement

Début : 12/9/2020 9:00 Toute la journée

Fin : 12/9/2020 11:00

Répéter : Chaque jour

Rappel : 15 minutes avant Configurer

Affichage : Occupé Calendrier Privé

Planificateur Masquer

Tous les participants

asmaa@zimbramail.univ-blida.dz

blida@zimbramail.univ-blida.dz

Sans Serif 12pt Paragraphe B I U S Z A

bon courage...!!!!

Activer Windows Accédez aux paramètres de votre ordinateur

Chat

Figure 3. 62 : Création d'une réunion.

- Démarrez facilement une réunion rapide

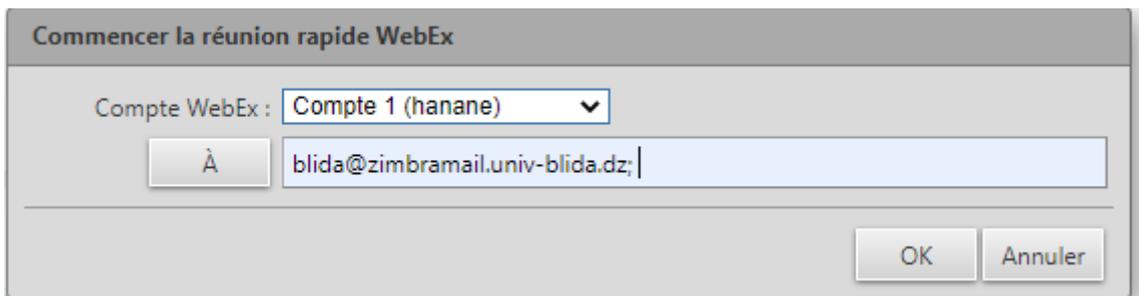


Figure 3. 63 : Réunion rapide.

### 13-L'interface client

Administrateur peut tout faire. Y compris modifier les thèmes, extensions, options de sécurité, etc.

Nous avons changé le thème de l'interface client (figure 3.64) .

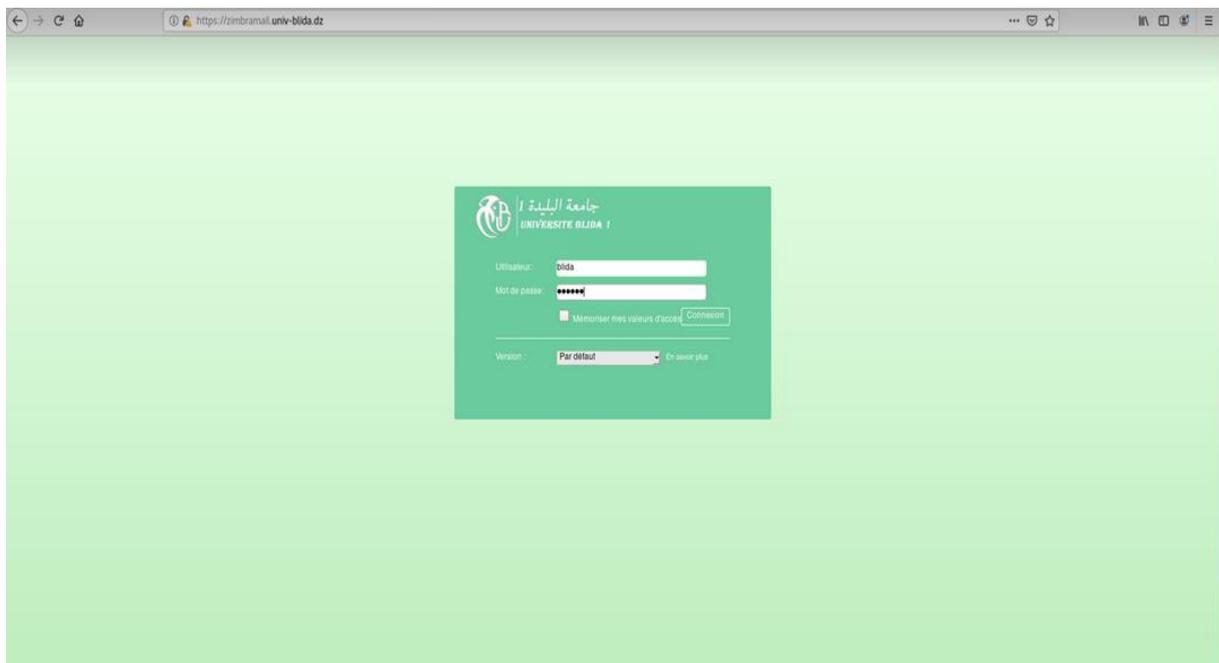


Figure 3. 64 : Page d'accueil de client.

## 14-L'interface de l'administrateur

Nous avons changé l'arrière-plan pour l'interface d'administrateur à l'aide d'un programme css (figure 3.65).

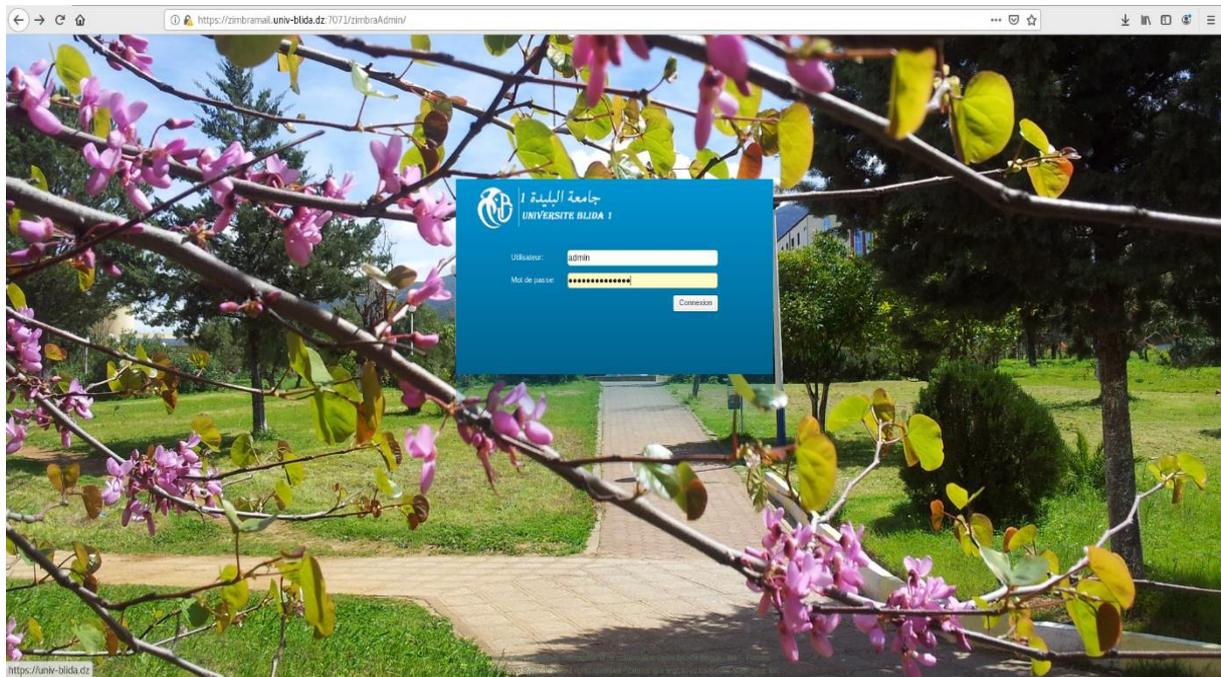


Figure 3. 65 : Page d'accueil d'administrateur.

## 3.6 Conclusion

Dans ce chapitre on a vu les détails de la configuration et installations de notre serveur de messagerie Zimbra et quelques utilités de serveur et un de ces derniers qui sera utilisé au niveau de l'université de blida.

# Conclusion Générale

## **Conclusion générale**

Dans ce modeste travail, nous avons réalisé un système de messagerie pour l'université Saad Dahlab, qui permet aux différents utilisateurs d'échanger (des mails et des différents documents etc...) entre eux.

La mise en œuvre d'une messagerie électronique interne ou externe, devient de plus en plus la solution de communication et d'échanges de données au sein des grandes entreprises, des grandes institutions

Le programme permet déjà d'effectuer un certain nombre d'actions :

- envoyer et recevoir des emails
- Créer, trier et partager une liste des tâches
- Afficher et ajouter un carnet d'adresse
- Créer un calendrier, des réunions et des rendez-vous

Ce projet a été une expérience, pour exploiter nos connaissances, nos capacités et d'affronter le domaine professionnel. Enfin, nous espérons que notre travail saurait satisfaire l'université Saad Dahlab blida 1 et qu'il leur serait d'un bénéfice.

# Bibliographie

## Bibliographie

- [1] Kæoü Thâr, « Les Avantages et les inconvénients des réseaux informatiques », *prezi.com*, mai 06, 2015. <https://prezi.com/55gbvaq1aitg/les-avantages-et-les-inconvenients-des-reseaux-informatiques/> (consulté le août 06, 2020).
- [2] D. Dromard et D. Seret, *Architecture des réseaux*. Paris: Pearson Education, 2010.
- [3] Jérôme Abel, « XBee & Arduino », janv. 23, 2013. <http://jeromeabel.net/files/ressources/xbee-arduino/xbee-arduino.xhtml> (consulté le août 06, 2020).
- [4] « Topologie en bus - IT Technologies ». <https://sites.google.com/site/technologiesti/les-topologies/topologie-physique/topologie-en-bus> (consulté le août 06, 2020).
- [5] L. Audibert, « Base de Données et langage SQL », p. 114.
- [6] A. KOUIS, « Différence entre le modèle TCP / IP et le modèle OSI », *WayToLearnX*, juill. 22, 2018. <https://waytolearnx.com/2018/07/difference-entre-le-modele-tcp-ip-et-le-modele-osi.html> (consulté le août 06, 2020).
- [7] « L’Opendoc ». <http://www.lopendoc.org/> (consulté le août 07, 2020).
- [8] « Conception et réalisation d’un système de messagerie.pdf ». Consulté le: août 07, 2020. [En ligne]. Disponible sur: <http://www.univ-bejaia.dz/jspui/bitstream/123456789/1249/1/Conception%20et%20r%C3%A9alisation%20d%E2%80%99un%20syst%C3%A8me%20de%20messagerie.pdf>.
- [9] « Bienvenue chez les VIVIANI ». <http://www.viviani.org/> (consulté le août 06, 2020).
- [10] Kitambala OMARI, « La réalisation d’une application de contrôle total des processus d’un ordinateur distant », *Memoire Online*, 2010. [https://www.memoireonline.com/05/12/5812/m\\_La-realisation-dune-application-de-contrle-total-des-processus-dun-ordinateur-distant0.html](https://www.memoireonline.com/05/12/5812/m_La-realisation-dune-application-de-contrle-total-des-processus-dun-ordinateur-distant0.html) (consulté le août 06, 2020).
- [11] « L’informatique au service des archives - Ce blog est destiné aux professionnels de l’information et de la communication. Il traite des archives, de l’informatique, et de tout autre domaine susceptible d’intéresser l’informatiste. » <http://josich.over-blog.com/> (consulté le août 06, 2020).
- [12] Jean-François Pillou, « Réseaux - Architecture client/serveur à 3 niveaux », *CommentCaMarche*, oct. 14, 2008. <https://www.commentcamarche.net/contents/221-reseaux-architecture-client-serveur-a-3-niveaux> (consulté le août 06, 2020).
- [13] « Chap1.7 : les réseaux ». <https://rmdiscala.developpez.com/cours/LesChapitres.html/Cours1/Chap1.7.htm> (consulté le août 06, 2020).
- [14] « Réseaux informatiques et télécommunications », *Offre de formation*. <http://formation.univ-fcomte.fr/licence-professionnelle/metiers-des-reseaux-informatiques-et-telecommunications-charge-daffaires-en> (consulté le août 07, 2020).
- [15] « routage-statique.pdf ». Consulté le: août 06, 2020. [En ligne]. Disponible sur: <https://nsr.org/wrc/data/2006/10980603514482363472620/routage-statique.pdf>.
- [16] ALLOUNE Mehdi Younes et DJOUDI Lakhdar, « Installation et configuration d’un serveur de messagerie Zimbra | Topologie de réseau | Modèle OSI », *Scribd*. <https://fr.scribd.com/document/461942868/Installation-et-configuration-d-un-serveur-de-messagerie-Zimbra> (consulté le août 06, 2020).
- [17] Jean-François Challe, « Administration et sécurité des réseaux. - PDF Téléchargement Gratuit ». <https://docplayer.fr/16401455-Administration-et-securite-des-reseaux.html> (consulté le août 06, 2020).

- [18] S. Lohier et A. Quidelleur, *Le réseau Internet: des services aux infrastructures : IUT, IUP, licence, master*. Paris: Dunod, 2010.
- [19] « DNS - serveur DNS (Domain Name System): définition, traduction ». <https://www.journaldunet.fr/web-tech/dictionnaire-du-webmastering/1203373-dns-serveur-dns-domain-name-system-definition-traduction/> (consulté le août 07, 2020).
- [20] cheikh, « Introduction au sécurité des messages électroniques | », août 23, 2012. <https://bencherifcheikh.wordpress.com/2012/08/23/introduction-au-securite-des-messages-electroniques/> (consulté le août 06, 2020).
- [21] Alexandre Serres, « Principes de fonctionnement de la messagerie électronique | URFIST de Bretagne et des Pays de la Loire », janv. 30, 2006. [https://www.sites.univ-rennes2.fr/urfist/messagerie\\_electronique\\_fonctionnement](https://www.sites.univ-rennes2.fr/urfist/messagerie_electronique_fonctionnement) (consulté le août 07, 2020).
- [22] Papa Cheikh Cisse, « Mise en place d'un système de messagerie sécurisée pour une PME/PMI », 21:06:14 UTC, Consulté le: août 07, 2020. [En ligne]. Disponible sur: <https://fr.slideshare.net/pacheikhcisse/mise-en-place-dun-systme-de-messagerie-scurise-pour-une-pmepmi>.
- [23] S. Azoulay-Bismuth, *Être un pro de l'e-mail: 7 étapes pour rédiger des e-mails efficaces*. 2018.
- [24] « les courriers électroniques et les différents serveurs de messageries. » <http://michel-vause.infographie-heaj.eu/H20/2.Les-differents-serveurs-de-messageries.html> (consulté le août 06, 2020).
- [25] Djob Pierre NJOKY, « Mise en place d'un système de messagerie électronique: Cas du fonds de prévoyance militaire - », 2008. <https://www.memoireonline.com/01/10/3072/Mise-en-place-dun-systeme-de-messagerie-electronique-Cas-du-fonds-de-prevoyance-militaire.html> (consulté le août 06, 2020).
- [26] Y. CHTOUROU, « Client lourd / Client Léger | SUPINFO, École Supérieure d'Informatique », oct. 30, 2016. <https://www.supinfo.com/articles/single/3424-client-lourd-client-leger> (consulté le août 06, 2020).
- [27] « zimbra\_guide-utilisateur-complet.pdf ». Consulté le: août 06, 2020. [En ligne]. Disponible sur: [http://www.univ-bpclermont.fr/tpl\\_ent/IMG/zimbra\\_guide-utilisateur-complet.pdf](http://www.univ-bpclermont.fr/tpl_ent/IMG/zimbra_guide-utilisateur-complet.pdf).
- [28] Boni Willy Enderson YEYE, « Mise en place d'un système de messagerie: cas de l'ITA », *Memoire Online*, 2011. [https://www.memoireonline.com/11/13/7972/m\\_Mise-en-place-d-un-systeme-de-messagerie-cas-de-l-ITA--Institut-des-technologies-d-Abidjan-0.html](https://www.memoireonline.com/11/13/7972/m_Mise-en-place-d-un-systeme-de-messagerie-cas-de-l-ITA--Institut-des-technologies-d-Abidjan-0.html) (consulté le août 06, 2020).
- [29] Jean-François Pillou, « Structure d'un courrier électronique (enveloppe, en-têtes et cor », *CommentÇaMarche*, oct. 14, 2008. <https://www.commentcamarche.net/contents/173-structure-d-un-courrier-electronique-enveloppe-en-tetes-et-cor> (consulté le août 06, 2020).
- [30] Jean-François Pillou, « Standard MIME (Multipurpose Internet Mail Extensions) - Comment Ça Marche », mai 26, 2015. <https://www.commentcamarche.net/contents/175-standard-mime-multipurpose-internet-mail-extensions> (consulté le août 06, 2020).
- [31] « SSL - Définition du glossaire », [https://www.ecommercemag.fr/https://www.ecommercemag.fr/Definitions-Glossaire/SSL-245368.htm#&utm\\_source=social\\_share&utm\\_medium=share\\_button&utm\\_campaign=share\\_button](https://www.ecommercemag.fr/https://www.ecommercemag.fr/Definitions-Glossaire/SSL-245368.htm#&utm_source=social_share&utm_medium=share_button&utm_campaign=share_button) (consulté le août 06, 2020).
- [32] Red Hat, Inc., « Protocole SSH », 2005. <http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-rg-fr-4/ch-ssh.html?fbclid=IwAR0EXO4Ngb9t41Tx0ppss4u0B8uIIIfm62AhWKSZGZbyEVUU9k-a05EkxhM> (consulté le août 06, 2020).