

République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Faculté des Sciences Exactes
Département d'Informatique



Mémoire de fin de cycle
En Vue De L'obtention Du Diplôme du
Master professionnel en Informatique

Option: Administration et sécurité des réseaux

Thème

*Mise en place d'un serveur de
messagerie électronique interne
MS Exchange 2013
cas: "EPB"*

Réalisé par

M^{elle} OULEBSIR Cylia

M^{elle} YOUSFI Wahiba

Encadré par: *M^r LARBI Ali*

Président: *M^r ATMANI Mouloud*

Examineur: *M^r NAFI Mohamed*

Année Universitaire 2015 – 2016

Remerciements

Tous d'abord, nous tenons à remercier le bon Dieu de nous avoir accordé toute la détermination, la volonté et la force pour qu'on puisse réaliser ce modeste travail.

Nous tenons à exprimer notre gratitude pour notre encadreur *M^r* A.LARBI qui nous a orienté et conseillé tout au long de ce travail.

Nous remercions aussi le personnel de " l'EPB ", de nous avoir acceptés au sein de leur organisme pour effectuer notre stage et leur aimable accueil et pour leur disponibilité.

Nous remercions particulièrement les membres de jury qui ont accepté de juger notre travail ainsi que tous les enseignants qui ont contribué à notre formation.

Enfin, Nous remercions aussi nos parents nos amis et collègues qui nous ont soutenu et tous ceux qui ont contribué de près ou de loin à la réalisation de ce travail.

Dédicaces

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

A mes soeurs: Lydia et Hanane.

A mes frères: Massi et Abderrzak.

A toute ma famille.

A tout mes amis .

A ma binôme Wahiba et toute sa famille.

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

Cyilia

Dédicaces

Tout d'abord je remercie Dieu Le Tout Miséricordieux,
Ton amour Ta miséricorde et Tes grâces à notre endroit nous ont fortifié dans
La persévérance et l'ardeur au travail.
Je dédie ce modeste travail à mes Parents qui mon tant soutenu, à mes frère et
soeur, à ma belle familles en particulier mon fiancé, à mes amis en particulier ma
binôme cylvia et toute sa famille
Et à ceux qui croient que leurs pensées peuvent changer leurs vies.

Wahiba

Table des Matières

Table des Matières	i
Liste des Figures	v
Liste des Tableaux	vii
Liste des abréviations	viii
Introduction générale	1
1 Généralités	3
1.1 Introduction	4
1.2 Les réseaux informatiques	4
1.2.1 Définition	4
1.2.2 Les modèles de communication réseau	4
1.2.2.1 Modèle OSI	5
1.2.2.2 Définition	5
1.2.2.3 Description du Modèle OSI	5
1.2.3 Modèle TCP/IP	6
1.2.3.1 Description du modèle TCP/IP	6
1.2.4 Architecture des réseaux	7
1.2.4.1 Architecture Client/Serveur	7
1.2.4.2 Architecture Peer to Peer (poste à poste)	8
1.3 Messagerie électronique	8
1.3.1 Définition	8
1.3.2 Serveur	8
1.3.3 Serveur de messagerie	9
1.3.4 Serveur DNS (Domain Name Server)	9
1.3.5 Les services de la messagerie électronique	10

1.3.6	MIME (Multi-purpose Internet Mail Extensions)	12
1.3.7	Adresses électroniques	12
1.3.8	Structure d'un mail	12
1.3.9	Protocole de messagerie électronique	13
1.3.10	Description de l'architecture d'un système de messagerie électronique	14
1.4	Protocole de Sécurité	16
1.4.1	Protocole SSL/TLS	16
1.4.2	Protocole SSH (Secure SHell)	17
1.5	Principales solutions de messagerie	17
1.5.1	Solutions Open Source	17
1.5.2	Solutions Propriétaires	18
1.6	Conclusion	21
2	Etude de cas	22
2.1	Introduction	23
2.2	Organisme d'accueil	23
2.2.1	Présentation de l'entreprise portuaire de Bejaia(EPB)	23
2.2.1.1	Organisation de l'entreprise	23
2.2.2	Le centre informatique	24
2.2.2.1	Présentation du centre informatique	24
2.2.2.2	L'organisation humaine	25
2.2.3	Le réseau local de l'EPB(LAN)	25
2.2.4	Architecture du réseau local	26
2.3	Cahier de charge	28
2.3.1	Présentation du projet	28
2.3.2	Analyse des besoins	28
2.3.3	Solutions proposés	28
2.3.4	Objectifs	29
2.4	Conclusion	29
3	Outils de développement	30
3.1	Introduction	31
3.2	Windows server 2012	31
3.2.1	Présentation de Windows server 2012	31
3.2.2	Rôle de serveur, services de rôle et fonctionnalités pour Windows server 2012	32
3.2.3	Protocole LDAP (Lightweight Directory Access Protocol)	32

3.2.3.1	Présentation de l'annuaire	32
3.2.3.2	Historique	33
3.2.3.3	Définition	33
3.2.3.4	Fonctionnement	33
3.3	Active directory	33
3.3.1	Définition	33
3.3.2	Vue d'ensemble d'Active Directory	34
3.3.2.1	Structure physique	34
3.3.2.2	Structure logique	35
3.3.3	Relation entre Active Directory et DNS	36
3.3.4	Relation entre Active Directory et LDAP	37
3.4	Exchange server 2013	38
3.4.1	Présentation	38
3.4.1.1	Rôle d'accès client (Client Access rôle)	38
3.4.1.2	Rôle de boîte aux lettres (Mailbox)	39
3.4.2	Les nouveautés d'Exchange server 2013	39
3.5	Conclusion	41
4	Installation, configuration et administration d'Exchange Server 2013	42
4.1	Introduction	43
4.2	Présentation du travail	43
4.3	Installation d'échange server 2013	54
4.4	Présentation des outils de l'administration	56
4.4.1	Exchange Management Shell	56
4.4.2	Exchange Management Console (EMC)	57
4.4.3	Centre d'administration Exchange(CAE)	57
4.5	Gestion des Accès Clients	57
4.5.1	Autodiscover (service de découverte automatique)	57
4.5.2	Exchange ActiveSync	58
4.5.3	Outlook Web App (OWA)	58
4.6	Configuration d'échange server 2013	59
4.6.1	Acceptation des noms de domaines	59
4.6.2	Configuration des domaines acceptés	59
4.6.3	Domaines faisant autorité	59
4.6.4	Stratégie d'adresse de messagerie	61
4.6.5	Règles de transport	62
4.6.5.1	Connecteurs d'envoi	62
4.6.5.2	Connecteur de réception	63

4.6.6	Création de boîtes aux lettres utilisateur	66
4.6.7	Configurer un certificat	66
4.7	Conclusion	68
Conclusion générale		iv
Bibliographie		iv
Résumé		v

LISTE DES FIGURES

1.1	Le modèle OSI	5
1.2	Le modèle TCP/IP	6
1.3	Architecture poste à poste.	8
1.4	Le domaine, la zone et la délégation	10
1.5	Description de l'architecture d'un système de messagerie électronique	15
2.1	Organigramme général de l'EPB	24
2.2	Organigramme du centre informatique.	25
2.3	Architecture actuelle du réseau local de l'EPB.	26
4.1	Installation du rôle Active Directory.	44
4.2	Configuration du service AD DS.	45
4.3	Identification du contrôleur de domaine.	46
4.4	L'ajout d'un logiciel enfichable.	46
4.5	L'ajout du schéma Active Directory.	47
4.6	Indication du serveur contrôleur de domaine.	48
4.7	Installation des outils RSAT.	49
4.8	Préparation du schéma Active Directory.	49
4.9	Préparation de l'Active Directory.	50
4.10	Vérification de l'organisation.	51
4.11	Configuration du serveur DNS.	52
4.12	Installation des rôles boîtes aux lettres et accès client.	53
4.13	Installation du rôle boîte aux lettres	54
4.14	Lancement du setup.	55
4.15	Installation du rôle d'accès client.	55
4.16	Exchange Management Shell.	56
4.17	Centre d'administration Exchange.	57
4.18	Domaines faisant autorité.	60
4.19	Configuration du domaine acceptés.	61

4.20	Format de l'adresse de messagerie.	62
4.21	Ajout d'un connecteur d'envoi.	63
4.22	Ajout d'un connecteur de réception.	64
4.23	Relier un connecteur de réception a une carte réseau.	65
4.24	Configurer un connecteur de réception.	65
4.25	Création de boites aux lettres utilisateurs.	66
4.26	Création d'un certificat auto-signé.	67
4.27	Obtention d'un certificat auto-signé.	68

LISTE DES TABLEAUX

1.1	Le modèle OSI et le modèle TCP/IP	7
1.2	Les principaux types d'enregistrement DNS [1].	11
1.3	Tableau comparatif de quelques solutions de messagerie	20

Liste des abréviations

AD DS	A ctive D irectory D omain S ervices
AD LDS	A ctive D irectory L ightweight D irectory S ervices
ADSI	A ctive D irectory S ervice I nterface
CAS	C lient A ccess S erver
DAG	D atabase A vailability G roups
DHCP	D ynamic H ost C onfiguration P rotocol
DLP	D ata L oss P revention
DNS	D omain N ame S erver
EAC	E xchange A dministration C enter
EOP	E xchange O nline P rotection
IMAP	I nternet M essage A ccess P rotocol
LDAP	L ightweight D irectory A ccess P rotocol
MBX	M ail B o X
MDA	M ail D elivery A gent
MIME	M ulti-purpose I nternet M ail E xtensions
MMC	M icrosoft M anagement C onsole
MTA	M ail T ransfer A gent
MUA	M ail U ser A gent
OBM	O pen B usiness M anagement
OSI	O pen S ystem I nterconnections
OWA	O utlook W eb A pp
POP	P ost O ffice P rotocol
RBAC	R ole B ased A ccess C ontrol
RPC	R emote P rocedure C all
SMTP	S imple M ail T ransfer P rotocol
SSH	S ecure S Hell
SSL	S ecure S ocket L ayer
TCP/IP	T ransmission C ontrol P rotocol / I nternet P rotocol

TLS	T ransport L ayer S ecurity
WIM	W indows I maging F ormat
ZCS	Z imbra C ollaboration S uite

Introduction Générale

Le courrier électronique est aujourd'hui l'une des applications les plus populaires du réseau, utilisés dans des applications très variées : personnelles, professionnelles, associatives, politiques... etc. Le courrier électronique tend à prendre une place de plus en plus prépondérante par rapport aux moyens de communication traditionnels. La messagerie électronique optimise la communication et la diffusion des informations.

L'introduction des technologies de l'information et de la communication (TIC) dans les organisations a représenté un renouvellement des supports utilisés pour la communication d'entreprise. La messagerie électronique en constitue l'application la plus marquante qui a suscité un intérêt direct et évident, grâce aux avantages de coût, de simplicité et d'efficacité qu'elle présente par rapport aux technologies antérieures comme le fax ou le téléphone.

La messagerie électronique s'est vite répandue, et son utilisation s'est généralisée pour devenir un service indispensable à la viabilité des entreprises est un vecteur essentiel de l'ensemble de leurs communications (interne, externe, etc.), ayant un impact direct sur leurs activités. De plus, son perpétuel développement fait qu'elle occupe aujourd'hui une place prépondérante. En effet, d'un simple outil d'échange de mails à son origine, elle est devenue une plateforme quasi universelle dédiée à la coordination du travail collaboratif et à la communication générale au sein de l'entreprise et la tendance est désormais à la convergence et à l'unification des types et des outils de communication qu'ils soient voix (ex. téléphonie, messages vocaux) ou data (ex. fax, SMS, courriel, etc...).

En revanche, si l'implantation de la messagerie électronique est arrivée aujourd'hui à la phase de maturité, son essor n'est pas sans conséquences, puisque il engendre de nombreuses complications telles que l'augmentation des volumes d'informations qui rend leur gestion (stockage, transport) plus difficile ou encore la protection et le partage de ces dernières. Ce à quoi s'ajoutent les besoins croissants des utilisateurs en matière de mobilité et de facilité d'accès aux services auxquels il faut sans cesse s'adapter.

Comme pour tout système informatique, les systèmes de messagerie exigent pour les professionnels une grande maîtrise pour pouvoir les adapter aux besoins spécifiques, les mettre en oeuvre et les exploiter de manière sûre et positive. Dans ce contexte, l'objectif principal de notre travail est d'étudier, sous ses différents aspects théoriques et pratiques, une des solutions de messagerie existantes qui est MS Exchange Server 2013, de la mettre en oeuvre sur un environnement de simulation et de travailler dessus afin de pouvoir en examiner les éléments constitutifs, les fonc-

tionnalités, l'architecture et les mécanismes de fonctionnement.

Ce thème, nous l'avons choisi afin de remédier aux problèmes de l'échange d'informations, au sein de notre organisme d'accueil, l'Entreprise Portuaire de Bejaia, où nous avons effectué notre stage. Ces problèmes seront cités dans le cahier de charge. Dans le but de faciliter leurs tâches nous leur avons suggéré des solutions.

Notre mémoire comprend deux parties principales. La partie théorique se compose de trois chapitres, le premier chapitre sera consacré à la définition de quelques notions fondamentales sur les réseaux, ainsi qu'à la notion de base de la messagerie électronique. Le second chapitre, consiste à présenter l'organisme d'accueil dans le quelle nous présenterons la structure du réseau informatique de l'EPB. Le troisième sera consacré au service d'annuaire Active Directory qui constitue une pierre angulaire pour le fonctionnement de la messagerie à base d'Exchange Server comme nous présenterons Exchange server en lui-même. Dans la deuxième partie nous détaillerons les différentes étapes nécessaires pour la mise en place de notre serveur de messagerie, allant de la planification à l'installation finale en passant par la préparation des prérequis.

Nous terminerons ce mémoire par une conclusion générale qui contiendra une synthèse et quelques perspectives envisagées pour ce travail.

1

Généralités

1.1 Introduction

Le développement de l'informatique représente un atout majeur pour les progrès de la science. En particulier, il a permis de perfectionner les techniques utilisées en automatisation, ainsi que les systèmes de communication. L'ordinateur est l'outil de base qui a contribué fortement à son évolution.

Dans le premier point de ce chapitre nous présentons un préambule sur les réseaux, leurs différentes architectures, ainsi que leurs modèle de communication. Dans le second, nous parlerons de la messagerie électronique, ces services, les protocoles de messagerie ainsi que le fonctionnement. En troisième point nous évoquerons la sécurité informatique, enfin nous parlerons de principales solutions de messagerie électronique.

1.2 Les réseaux informatiques

1.2.1 Définition

Un réseau informatique est une collection d'objets basée sur l'outil informatique (ordinateurs, stations de travail, cartes réseau, modems, imprimantes réseaux et liaisons téléphoniques). Il permet de relier physiquement ou via les ondes radio un ensemble de serveurs et de postes de travail selon une architecture physique bien défini.

Le but des réseaux informatiques est d'assurer le partage des différentes ressources matérielles et logicielles (fichiers, applications, imprimantes...) et la communication par l'échange des informations d'une manière simple, rapide et efficace, entre les stations de façon sécurisée [2].

1.2.2 Les modèles de communication réseau

Les modèles de communication entre utilisateurs réseau les plus répandus sont: le modèle OSI (Open System Interconnections), qui est un modèle de sept couches et le modèle TCP/IP (Transmission Control Protocol / Internet Protocol), qui est un modèle de quatre Couches.

1.2.2.1 Modèle OSI

1.2.2.2 Définition

OSI (Open System Interconnections, Interconnexion de systèmes Ouverts) le modèle d'interconnexion en réseau des systèmes ouverts est un modèle de communications entre ordinateurs proposé par l'ISO (Organisation Internationale de normalisation). Il décrit les fonctionnalités nécessaires à la communication et l'organisation de ses fonctions [3].

1.2.2.3 Description du Modèle OSI

Le modèle de référence OSI comporte sept niveaux(couches), plus un medium physique. Le medium physique, que l'on appelle parfois couche 0, correspond au support physique de communication chargé d'acheminer les éléments binaires d'un point à un autre, jusqu'au récepteur final.

Ce medium physique peut prendre diverses formes, allant du câble métallique aux signaux hertziens, en passant par la fibre optique et l'infrarouge.

Le schéma suivant montre le fonctionnement du modèle [3].

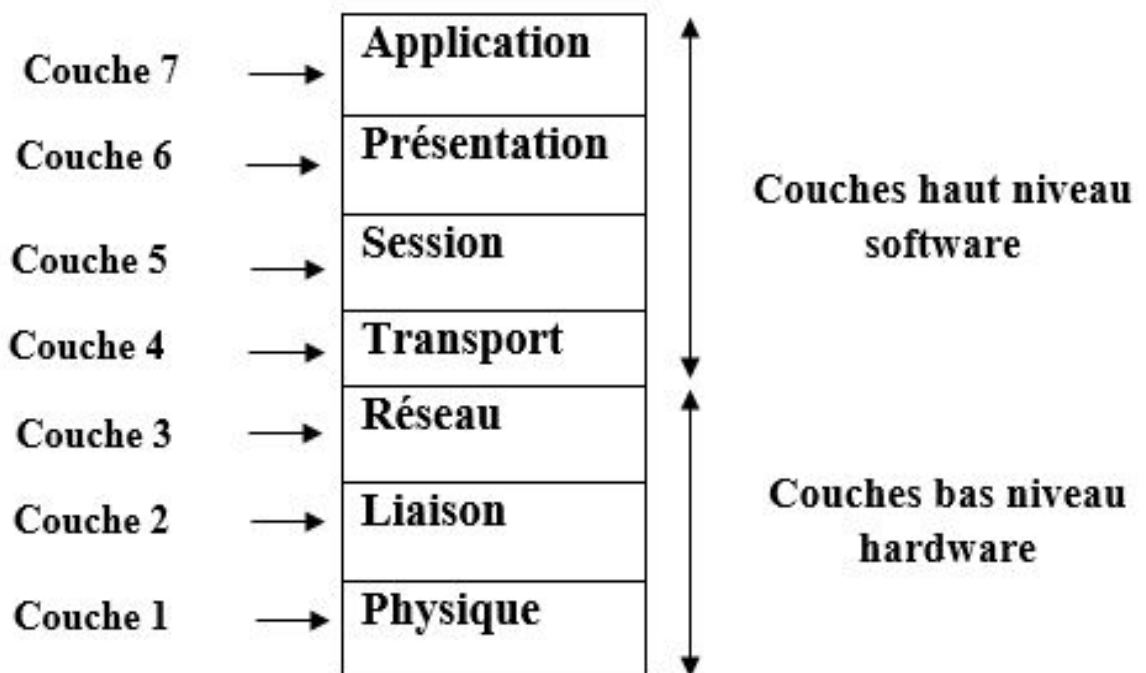


Figure 1.1: Le modèle OSI

1.2.3 Modèle TCP/IP

Le modèle TCP/IP (Transmission Control Protocol/Internet Protocol) est un protocole utilisé sur le réseau Internet pour transmettre des données entre deux machines. Le nom de ce modèle de référence provient de ses deux principaux protocoles : TCP et IP [3].

Les deux principaux protocoles définis dans cette architecture sont les suivants:

- **IP:** de niveau réseau qui assure un service sans connexion.
- **TCP:** de niveau transport qui fournit un service fiable avec connexion.

1.2.3.1 Description du modèle TCP/IP

Le modèle TCP/IP est inspiré du modèle OSI, reprend l'approche modulaire (utilisation de modules ou couches) mais il contient uniquement quatre couches qui sont présentées au niveau du schéma suivant:

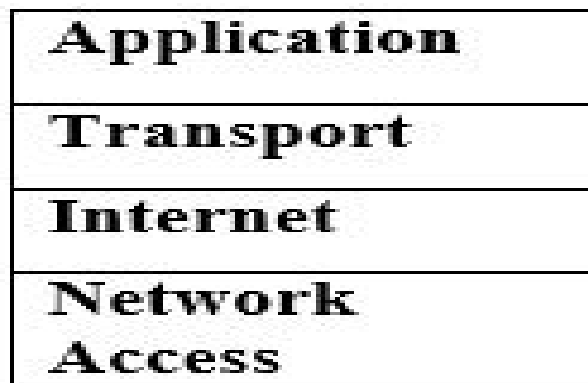


Figure 1.2: Le modèle TCP/IP

Modèle OSI		Modèle TCP/IP	
7	Application	4	Application
6	Présentation		
5	Session		
4	Transport	3	Transport (TCP)
3	Réseaux	2	Internet(IP)
2	Liaison de donnée	1	Accès au réseau
1	Physique		

Table 1.1: Le modèle OSI et le modèle TCP/IP

1.2.4 Architecture des réseaux

Il existe deux types d'architecture réseaux : l'architecture Client/Serveur et l'architecture Peer to Peer ou poste à poste.

1.2.4.1 Architecture Client/Serveur

- **Serveur:** On appelle logiciel serveur un programme qui offre un service sur le réseau. Le serveur accepte des requêtes, les traite et renvoie le résultat au demandeur. Le terme serveur s'applique à la machine sur lequel s'exécute le logiciel serveur.
- **Client:** On appelle logiciel client un programme qui utilise le service offert par un serveur. Le client envoie une requête et reçoit la réponse. Le client peut être raccordé par une liaison temporaire.
- **Architecture client/serveur:** C'est la description du fonctionnement coopératif entre le serveur et le client. Les services internet sont conçus selon cette architecture. Ainsi, chaque application est composée de logiciel serveur et de logiciel client. A un logiciel serveur, peut correspondre plusieurs logiciels clients développés dans différents environnements : Unix, Mac, PC...; la seule obligation est le respect du protocole entre les deux processus communicants.

1.2.4.2 Architecture Peer to Peer (poste à poste)

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

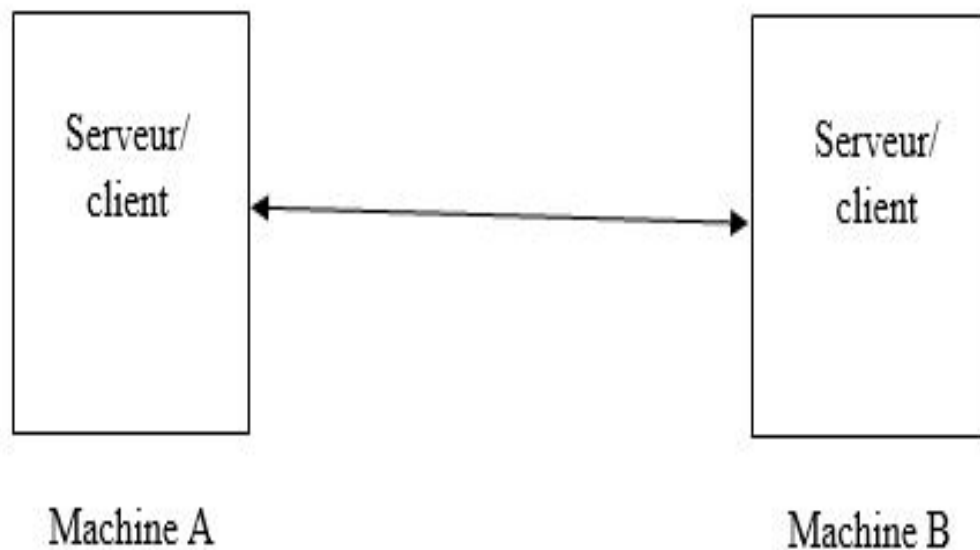


Figure 1.3: Architecture poste à poste.

1.3 Messagerie électronique

1.3.1 Définition

La messagerie électronique est un service de transmission de messages envoyés électroniquement via un réseau informatique dans la boîte aux lettres électronique d'un destinataire choisi par l'émetteur.

1.3.2 Serveur

Un serveur a comme rôle de rendre des services et de répondre aux requêtes des clients. Dans les réseaux, les serveurs se communiquent entre eux. Il existe plusieurs types de serveurs, il y'a des serveurs racines 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 :

- Le port 21 (service ftp).
- Le port 22 (service ssh).
- Le port 23 (le service telnet).
- Le port 25 (service smtp).
- 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.

1.3.3 Serveur de messagerie

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

- Le Mail Transfert Agent ou MTA.
- Le serveur du protocole entrant.
- Le Mail Delivery Agent ou MDA.
- Le Mail User Agent ou MUA.

1.3.4 Serveur DNS (Domain Name Server)

DNS est le service de résolution de nom d'hôte, il permet d'adresser une machine par un nom plutôt que de l'adresser par une adresse IP [1].

La figure 1.4 résume les notations utilisées par le serveur DNS

1. **Domaine:** le nom de domaine identifie une organisation sur internet. Un domaine est un sous arbre de l'espace de nommage. Il peut être organisé en sous domaines, .univ.org est un sous domaine du domaine .org.
2. **Zone:** est une organisation logique (administrative) des domaines. Son rôle est de simplifier l'administration des domaines. Le domaine .com peut être découpé en plusieurs zones, z1.com, z2.com...etc.

3. **Délégation:** consiste à déléguer l'administration d'une zone ou une sous zone aux administrateurs de cette zone.

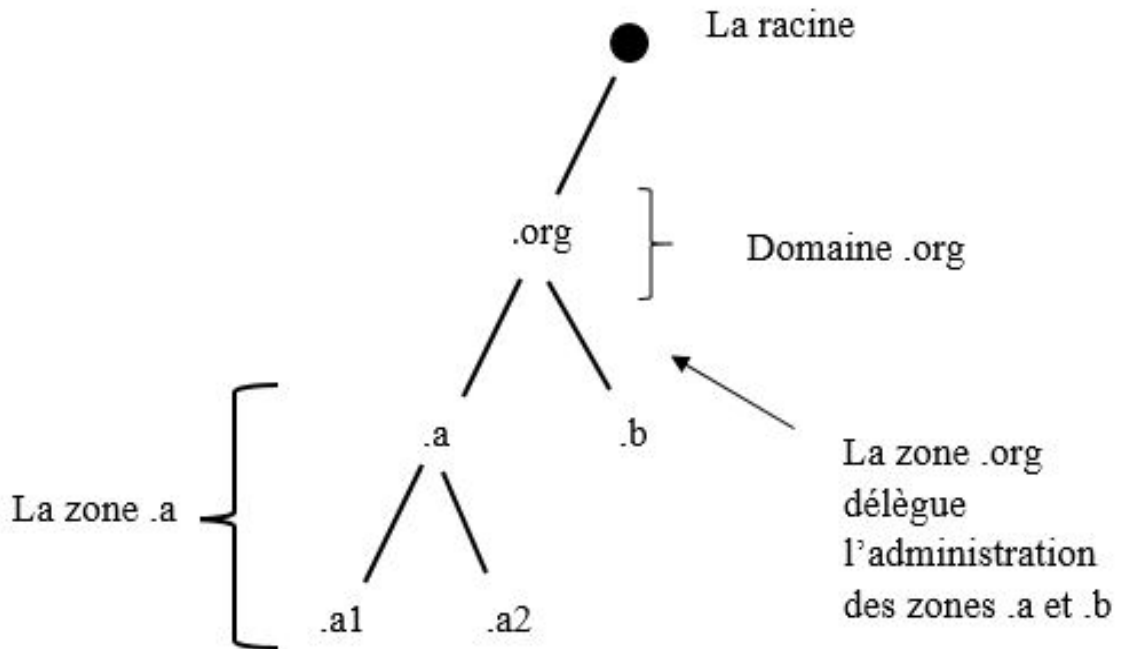


Figure 1.4: Le domaine, la zone et la délégation

Les propriétés de DNS :

- Numéro de port : 53.
- Type d'enregistrement : les principaux types d'enregistrement DNS sont illustrés dans le tableau suivant :

1.3.5 Les services de la messagerie électronique

- **MUA (Mail User Agent ou Agent de Gestion du Courrier 'AGC')** est un programme qui permet à un client de LIRE, ECRIRE un message électronique et de l'envoyer à l'Agent de routage qui va l'injecter dans le système de messagerie via le protocole SMTP (Simple Mail Transfert Protocol).
- **MTA (Mail Transfer Agent ou Agent de Transfert de Courriers 'ATC')** est un programme qui sert à transférer des messages électroniques

Type d'enregistrement	Description
SOA (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 noeuds 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 noeuds existants
PTR (Pointeur)	Il permet la résolution de noms inverse dans le domaine in-addr.arpa

Table 1.2: Les principaux types d'enregistrement DNS [1].

entre des ordinateurs, qui utilisent le protocole SMTP. Il est composé de deux agents:

- Un agent de routage des messages.
- Un agent de transport de messages.
- **MDA (Mail Delivery Agent ou Agent de Distribution de Courriers)** C'est un programme utilisé par l'Agent de Transfert de Courriers ATC pour acheminer le courrier vers la boîte aux lettres du destinataire spécifié. Il distribue le courrier dans les boîtes des utilisateurs spécifiés.

1.3.6 MIME (Multi-purpose Internet Mail Extensions)

A l'origine, les mails étaient prévus pour ne transporter que des caractères du jeu Us-ASCII (American Standard Code for Information Interchange), sans aucun accent, caractères spéciaux... MIME est une spécification décrivant les formats de messages sur internet, il permet :

- L'échange de textes écrits dans des jeux de caractères étendus ou différents.
- L'échange de messages multimédia comme des images, des sons, des séquences vidéos, des données en tous genres [4].

1.3.7 Adresses électroniques

Le courrier électronique repose sur les adresses électroniques des utilisateurs : Les adresses de courrier électronique se présentent toujours de la manière suivante : nom de l'utilisateur@sousdomaine.domaine. Le signe @ (arobase) signifie at (chez), pour indiquer la notion d'hébergement sur un serveur hôte.

1.3.8 Structure d'un mail

L'Email a une structure similaire à celle d'un courrier classique. Il est composé d'une enveloppe que l'on appelle "en-tête" qui contient les données relatives aux adresses des émetteurs et récepteurs, ainsi que le sujet du message, la date, etc... A la suite de l'en-tête s'ajoute le contenu du mail que l'on appelle le "corps du message". C'est également cette partie du mail qui comprend les pièces jointes. L'en-tête du mail contient donc les informations suivantes:

- **From:** contient l'adresse mail de l'expéditeur.

- **To:** une partie de l'en-tête qui contient les adresses de tous les destinataires.
- **CC (Carbon Copies):** détermine la liste des destinataires qui recevront une copie du message.
- **CCI (Carbon Copies Invisible):** appelée également copie cachée, il s'agit d'une simple Copie Carbone à la différence près que le destinataire ne voit pas dans l'en-tête la liste des personnes en copie cachée.
- **Subject:** permet de décrire l'objet du sujet.
- **Date:** la date d'envoi.
- **Replay-To:** pour spécifier l'adresse à laquelle les réponses doivent être expédiées.
- **Message-ID:** une valeur qu'est générée par le programme du transport du système de départ permettant d'identifier le message de manière univoque.
- **Received:** ce champ permet de retracer le chemin emprunté par le message, en effet, tous les hôtes par lesquels le message transite ajoutent ce champ à l'en-tête ; sur ce dernier on trouve les caractères suivants : l'identifiant du site, un identificateur du message, le moment de la réception du message, le site de provenance de message ainsi que le nom du logiciel du transport utilisée.

1.3.9 Protocole de messagerie électronique

- **SMTP (Simple Mail Transfert Protocol) :** est un protocole standard qui permet de transmettre les messages envoyés par les postes clients. Il permet de transmettre soit d'un client à un serveur ou d'un serveur à un autre en connexion point à point. Il fonctionne en mode commuté, encapsulé dans les trames TCP/IP, grâce à des commandes textuelles (chaîne des caractères ASCII terminée par des caractères gestion d'erreurs). Il existe une version améliorée de SMTP qui est l'ESMTP, c'est un protocole simple de transfert des mails ou courriers électroniques vers le serveur, il utilise le port 25 [5].
- **POP (Post Office Protocol):** c'est un protocole de récupération des messages dans un serveur de messagerie électronique, nécessite une connexion à un réseau, utilise le port 110, se présente sous plusieurs versions par rapport à la sécurité et aux générations POP3, POP3S, POP4...etc. Ce protocole permet le dialogue à partir de postes clients afin d'assurer l'interrogation des BAL et

le rapatriement des messages du serveur au poste client. Il permet aussi de récupérer des mails dans des serveurs pour des postes clients, il ne fonctionne qu'en mode connecté. Son avantage est de permettre l'enregistrement des mails dans un poste client pour les consulter de partout même hors connexion à condition de le faire dans le même poste [5].

- **IMAP (Internet Message Access Protocol):** c'est aussi un protocole de récupération de mail dans le serveur pour le mettre à la disposition d'un utilisateur au niveau de MUA de destination, il présente plus d'avantages que POP car il permet la conservation ou l'archivage des messages au poste clients pour qu'ils soient utilisés en local. Il utilise le port 143. Pour la sécurité, IMAP est combiné avec SSL pour donner IMAPS, afin de permettre un accès sécurisé au serveur [5].

1.3.10 Description de l'architecture d'un système de messagerie électronique

Les différents éléments du système de messagerie sont agencés selon une architecture logique, pour en assurer le fonctionnement. Nous représentons cette architecture par le schéma ci-dessous.

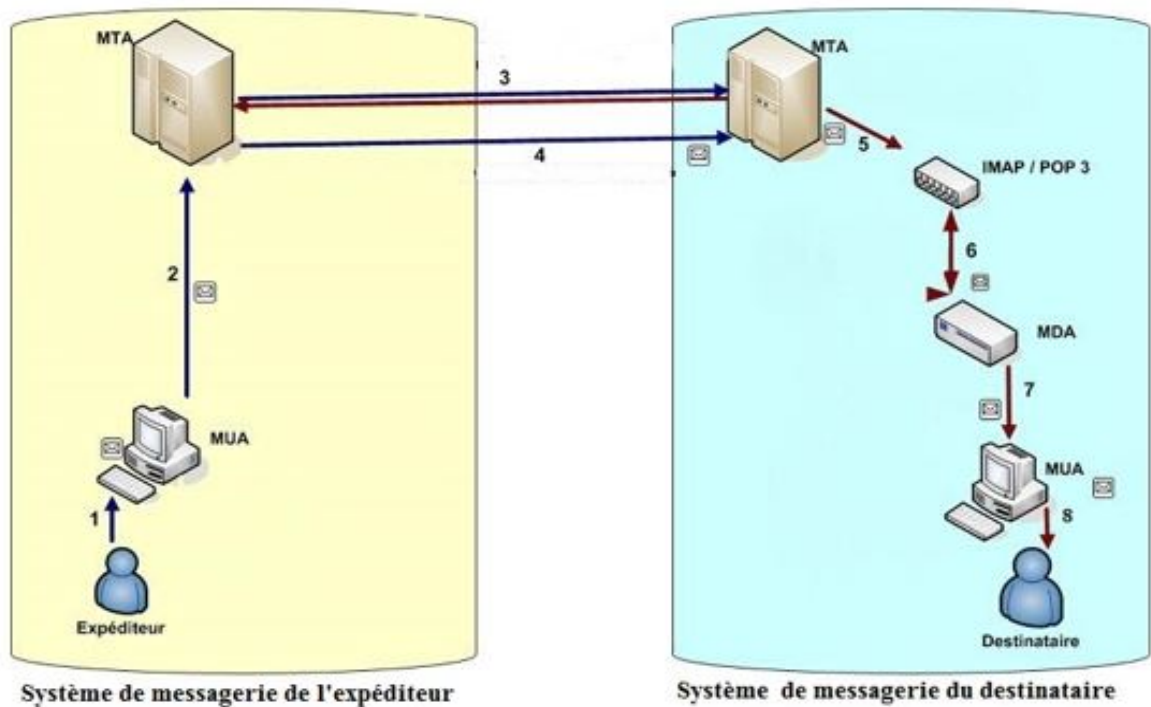


Figure 1.5: Description de l'architecture d'un système de messagerie électronique

Ce schéma présente le transfert d'un courriel d'un expéditeur à un destinataire.

1. L'expéditeur saisit et valide l'envoi de son courriel.
2. Le MUA transmet le courriel au MTA (la plupart des MTA intègre des clients SMTP).
3. Le MTA du système de l'émetteur établit un canal de transmission avec le MTA du système de destinataire, par émission successive de requête bidirectionnelle.
4. Une fois le canal établi, le courriel est transmis d'un système à un autre par les MTA.
5. Dans le système du destinataire, le MTA transmet le courriel reçu au serveur IMAP ou POP3.
6. Le MDA récupère le courriel du serveur IMAP /POP3 par émission successive de requêtes.

7. Le MDA récupère le courriel du serveur IMAP/POP3 par émission successive de requêtes et le met à disposition du MUA.
8. Le MUA dépose le courriel dans la boîte aux lettres du destinataire qui pourra le consulter à tout moment, sur authentification.

1.4 Protocole de Sécurité

1.4.1 Protocole SSL/TLS

On désigne par protocole SSL/TLS deux protocoles distincts, très proches l'un de l'autre:

- **SSL (Secure Socket Layer):** a été développé par Netscape pour offrir un accès sécurisé a des serveurs web, et il permet de sécuriser n'importe quel service base sur TCP, la version actuel est la V3.
- **TLS (Transport Layer Security):** reprise et normalisation du précédent Le protocole SSL/TLS permet d'assurer l'authentification (via des certificats X.509), la confidentialité (via le chiffrement) et l'intégrité des données échangées (via des fonctions de hachage MAC) [5].

Le protocole SSL/TLS permet d'assurer l'authentification (via des certificats X.509), la confidentialité (via le chiffrement) et l'intégrité des données échangées (via des fonctions de hachage MAC).

Il s'intercale entre le protocole de transport (TCP) et les protocoles applicatifs tels que ceux utilisés dans la messagerie (SMTP, POP, IMAP, HTTP).

Le protocole SSL/TLS est constitué des sous protocole suivant :

1. Le sous protocole SSL/TLSHandshake : permet l'authentification des clients et la négociation des paramètres de chiffrement.
2. Le sous protocole SSL/TLSChange CipherSpec : permet de signaler a SSL/TLSRecord les paramètres de chiffrement négocie.
3. Le sous protocole SSL/TLSRecord : met en oeuvre les paramètres de chiffrement, ainsi que la fragmentation des données et leur compression.
4. Le sous protocole SSL/TLSAlert : signale à l'application ; les erreurs rencontrées lors de vérification des messages, les problèmes de compatibilité entre les systèmes cryptographiques qui peuvent survenir lors de Handshake [5].

1.4.2 Protocole SSH (Secure SHell)

SSH est un protocole qui assure la sécurité de communication au sein d'un réseau, il est conçu pour être simple d'implémentation et pas couteux.

Au début il été destiné à assurer un login distant, et remplacer Telnet. SSH offre des possibilités Client/serveur, pour les services réseau et peut être utilisé pour le transfert des fichiers ou des mails [5].

1.5 Principales solutions de messagerie

1.5.1 Solutions Open Source

- **OBM (Open Business Management):** le logiciel de travail collaboratif OBM dispose de plusieurs fonctionnalités : messagerie, travail collaboratif, CRM, annuaire LADP, module de synchronisation.
OBM est base sur les standards SOAP, LADP, iCAL, HTTP, HTTPS, SMTP, IMAP, POP3, SyncML
- **Zimbra Collaboration Suite (ZCS):** est une application de messagerie et de collaboration complète qui offre de grandes possibilités pour les courriels, les carnets d'adresses, les calendriers et les listes de taches.
ZCS est un logiciel serveur collaboratif (" groupware ") qui permet le partage d'informations (courriels, calendriers, contacts et taches) que ce soit entre les membres de ZCS ou avec des collaborateurs externes ou même au grand public. ZCS est développé sur un mode de " Web service ". Toute l'interface " AJAX " est chargée a la première connexion, puis les interactions et ajouts/-modifications sont envoyées au serveur via le protocole " SOAP ".
- **Scalix:** Scalix est une solution logicielle serveur libre de messagerie et de travail collaboratif tournant sous Linux, et publie sous la licence publique Scalix. Il était base à l'origine sur HP OpenMail, dont une licence avait été obtenue d'Hewlett Packard. Il fournit des services de messagerie électronique, de calendriers, et autres logiciels collaboratifs qui sont un standard en matière de groupware. Il est possible d'y accéder depuis différents clients, dont les plus répandus Microsoft Outlook, Novell Evolution et le Scalix Web Access, un client web.

1.5.2 Solutions Propriétaires

- **IBM lotus dominos:** un des grands concourant d'Exchange est le serveur Domino est son client Notes.

C'est une plate-forme de messagerie, de travail collaboratif et de gestion documentaire (GED). C'est un serveur d'application pour le client Notes mais également un serveur de base de documents (format NFS). Le serveur comprend les éléments suivants : serveur Web, serveur POP3/IMAP/ SMTP, annuaire intégré, agenda collectif. Domino peut s'installer sur différents systèmes d'exploitation : Windows, IBM i5/OS, IBM z/OS, IBM AIX, Linux, Sun Solaris.

- **MDaemon Messaging Server:** MDaemon Messaging Server est un serveur de messagerie collaboratif pour Windows développé par Alt-N Technologies. MDaemon compte parmi ses fonctionnalités un filtre anti-spam intégré, le chiffrement SSL et TLS, le support des dossiers publics et partages, des listes de diffusion, un client Webmail (WorldClient), le partage de données (calendrier, contacts, taches et notes), la synchronisation OTA (over-the-air) de terminaux mobiles avec ActiveSync (module additionnel requis), BlackBerry Internet Service, et BlackBerry Enterprise Server (fonctions BES disponibles à l'installation).

- **Microsoft Exchange serveur:** le leader incontesté du marché est le produit Exchange serveur qui s'appuie sur un serveur sous Windows serveur et des clients Outlook ou sur d'autres clients de messagerie. Exchange serveur dispose de plusieurs services packages et disponible après installation: service DNS, Active Directory, Surveillance système, banque d'information Exchange, moteur de transport SMTP, agent de transfert des messages MTA, serveur Web IIS, POP3 , IMAP4, Outlook Web App, ActiveSync Exchange ...

Ce système de messagerie est l'objet de ce travail, il sera détaillé le long de ce mémoire.

Solution de messagerie	Description	Avantages	Inconvénients
Microsoft Exchange serveur	Tourne sous Microsoft Windows server	Messagerie collaborative, Interface OWA(Exchange Outlook Web Access), Accès mobile avec Active Sync et BES, Service de protection, Sauvegarde des boites, Partage de fichiers, Administration avancée.	Les codes sources ne sont pas libres, Uni plate-forme (MS Windows)
IBM lotus dominos	peut s'installer sur : Windows, IBM i5/OS, IBM z/OS, IBM AIX, Linux, Sun Solaris	Flexible, facilité et rapidité de développement, la réplication et la sécurité	Lotus Notes n'est pas une plate-forme de messagerie. C'est une plate-forme application / développement
Zimbra Collaboration Suite (ZCS)	peut-être installer sur : GNU/Linux et Mac OS X	une interface en langage Ajax qui lui donne un avantage en termes de confort d'utilisation, réunit les principales fonctionnalités collaboratives (Une messagerie intégrée, Une gestion des contacts, Des fonctionnalités avancées d'agenda (partage, délégation, gestion de ressources. . .) Le partage et la gestion des documents)	La partie "AJAX" du client fonctionne très bien mais elle est très longue a charge, difficulté de configuration.

Table 1.3: Tableau comparatif de quelques solutions de messagerie

1.6 Conclusion

A l'issu de ce chapitre, nous avons présenté une brève définition sur les réseaux, leurs architectures, leurs modèles de transmission ainsi que les différents concepts liées aux systèmes de messagerie électronique qui sont en relation avec notre travail. Nous avons aussi présenté quelques solutions de messagerie existantes.

Ce chapitre, englobe toutes les généralités que nous aurons besoin. Dans le chapitre suivant, nous présenterons, l'Entreprise Portuaire de Bejaia, notre organisme d'accueil.

2

Etude de cas

2.1 Introduction

Dans ce chapitre nous allons décrire l'organisme d'accueil et ses missions ainsi que son organisation. Nous nous intéresserons en particulier au centre informatique dont l'objectif est de concevoir une plate forme réseau qui répond aux attentes de l'entreprise .

2.2 Organisme d'accueil

2.2.1 Présentation de l'entreprise portuaire de Bejaia(EPB)

Le port de Bejaia joue un rôle très important dans les transactions internationales vu sa place et sa position géographique. Aujourd'hui il est classé premier port d'Algérie en marchandise générales et troisième port pétrolier. Il est également le premier port du bassin méditerranée certifié ISO 9001/2000 pour l'ensemble de ses prestations et a avoir ainsi installé un système de management de qualité. Cela constitue une étape dans le processus d'amélioration continue de ses prestations au grand bénéfice de ses clients. L'entreprise portuaire a connu d'autres succès depuis, elle est notamment certifiée à la Norme ISO 14001/2004 et au référentiel OHSAS 18001/2007, respectivement pour l'environnement et l'hygiène et sécurité au travail.

2.2.1.1 Organisation de l'entreprise

Les différentes structures de l'EPB sont présentées dans l'organigramme suivant :

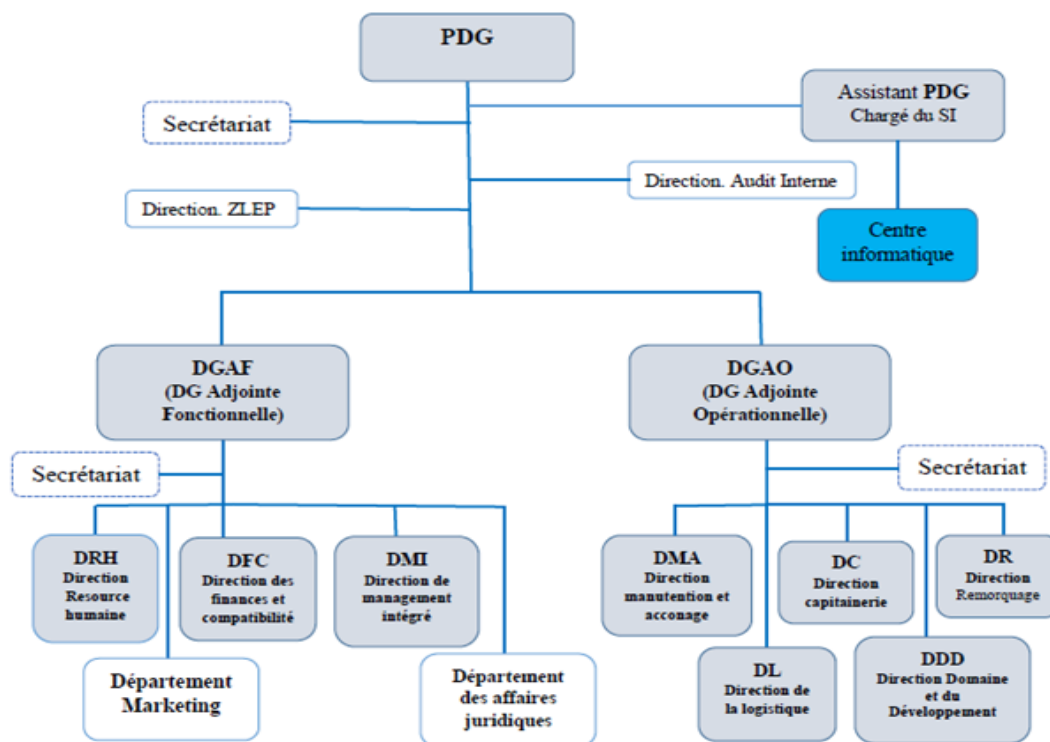


Figure 2.1: Organigramme général de l'EPB

2.2.2 Le centre informatique

2.2.2.1 Présentation du centre informatique

Le centre informatique est une structure l'EPB rattachée directement à la direction générale, elle a pour mission l'automatisation des métiers de l'Entreprise Portuaire de Bejaïa, et cela en mettant en place les logiciels et l'infrastructure nécessaires pour la gestion du système d'information. L'EPB déploie des systèmes d'informations pour accroître la productivité, automatisé les processus métiers et fournir un meilleur service aux clients. Ces systèmes intègrent de plus en plus des fonctionnalités réseau pour relier tous les utilisateurs à l'entreprise ou établir les liens avec la clientèle et les fournisseurs. Le réseau local de l'entreprise apporte aujourd'hui une réelle valeur ajoutée en permettant d'intégrer de nouveaux partenaires, fournisseurs et clients.

2.2.2.2 L'organisation humaine

Le centre informatique se compose de trois départements sous la coupe de l'assistant du PDG chargé du SI, chaque département est structuré en services comme le montre l'organigramme suivant :

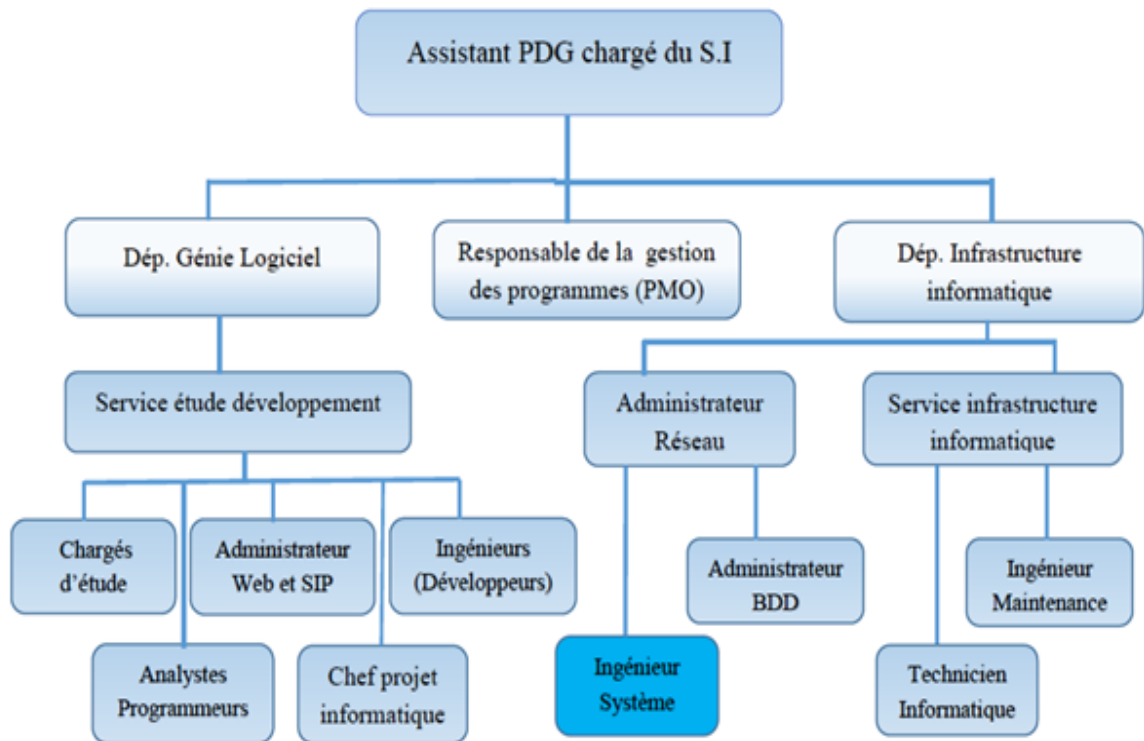


Figure 2.2: Organigramme du centre informatique.

2.2.3 Le réseau local de l'EPB(LAN)

Le réseau local de l'EPB permet au différents postes de travail de s'échanger des informations, de se connecter vers l'extérieur et d'utiliser les applications hébergées en internes nécessaire à l'exécution des tâches quotidiennes des employés. Le réseau du port de Bejaia s'étend du port pétrolier (N°16) aux ports 13 et 18 (port à bois).

2.2.4 Architecture du réseau local

L'architecture du réseau local de l'EPB est représentée dans la figure ci-dessus:

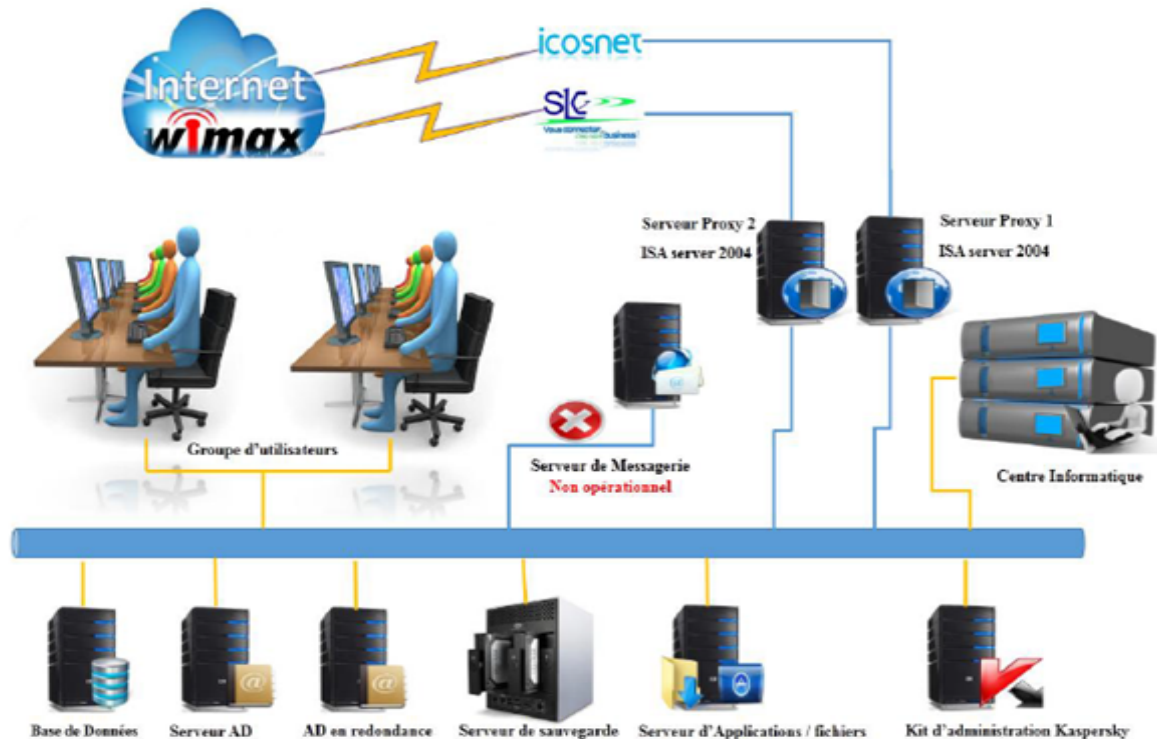


Figure 2.3: Architecture actuelle du réseau local de l'EPB.

Le réseau de l'entreprise portuaire de Bejaia est d'une architecture Client/serveur mais plate. L'armoire de brassage constitue l'essence même du réseau de l'EPB, elle contient les équipements permettant aux employés de l'entreprise d'accéder à Internet et de faire de l'intranet. On y distingue plusieurs switches et platines où arrivent les câbles. Ces câbles qui sont connectés aux différentes armoires de brassage de petite taille, placées dans chaque étage du bâtiment et reliées aux prises murales. Elles permettent aux employés de connecter leurs ordinateurs. Les différents serveurs offrent des services aux différents postes clients.

- **Connexion internet** : l'entreprise portuaire de Bejaia s'est dotée de deux connexions WiMax à savoir Icosnet et Algérie Telecom. Ce type de connexion, permet de connecter à Internet haut-débit grâce à une antenne Outdoor qui communique par ondes hertziennes via une station de bases située au mont Gouraya respectivement, d'une très grande fiabilité permettant ainsi d'éviter l'usage du câble et le risque d'une panne physique par conséquent.

- **Sécurité** : la sécurité est assurée par deux serveurs proxy qui agissent comme un filtre afin de définir les règles d'accès à un réseau comme Internet, à cause des risques que peut représenter une connexion "normale" dans certains cas, d'une part et de deux pare feu logiciels ISA server 2004(Internet Security & Acceleration server) pour appliquer les stratégies d'accès et les règles de routage déterminant la manière dont les clients accèdent a Internet.
- **Salle machine** : la salle machine est le coeur du réseau, toutes les activités du port reposent sur cette salle, elle regroupe en un seul endroit les ressources nécessaires au bon fonctionnement du LAN, en plus des switchs elle comporte les différentes machines serveurs :
 - ✓ *Serveur de base de données (SQL server 2005 & My SQL)*: sert à stocker, à extraire et a gérer les données dans une base de données. Il permet également de gérer la mise à jour des données. Il donne un accès simultané à cette base a plusieurs serveurs Web et utilisateurs.
 - ✓ *Serveur de contrôleur de domaine DC1 (sous Active directory Windows server2003)*: les contrôleurs de domaine stockent les données de l'annuaire et gèrent les interactions entre l'utilisateur et le domaine, y compris les processus d'ouverture de session, l'authentification et les recherches dans l'annuaire.
 - ✓ *Serveur de contrôleur de domaine en redondance(DC2)*: la réplication permet au service d'annuaire Active Directory de conserver des réplicas des données de l'annuaire sur un autre contrôleur de domaine, qui garantit la disponibilité et l'efficacité de l'annuaire pour les utilisateurs.
 - ✓ *Serveur intranet (application/fichiers)*: mettre à disposition des ressources applicatives à distance, sans prise en compte de l'environnement du poste utilisateur : c'est le serveur d'application qui fait tourner les applications qui sont accessibles simplement via un navigateur internet.
 - ✓ *Serveur sauvegarde*: le serveur, en collaboration avec la baie de stockage, ont pour rôle de sauvegarder en continu les données générées par l'entreprise. Si un employé efface par erreur un document, ou qu'il y a un dysfonctionnement d'un ordinateur, le serveur est en mesure de rétablir le fichier perdu.

Il est à noter que l'entreprise s'appuie notamment sur l'utilisation de produits Microsoft sous licence, notamment pour les systèmes d'exploitation. Windows 7 et

XP sont utilisés sur les postes clients et Windows server 2003 sur les serveurs, elle favorise notamment l'exploitation de logiciels et solutions Open source.

2.3 Cahier de charge

2.3.1 Présentation du projet

L'Entreprise Portuaire de Bajaia (EPB) à emprunter une nouvelle approche qui est la numérisation des données en l'occurrence GED/GDI d'où la nécessité d'aller vers une solution de communication électronique entre collaborateurs. C'est dans ce cadre, que nous souhaitons améliorer leurs système d'échange, en leurs installant un serveur de messagerie interne.

2.3.2 Analyse des besoins

Lors de notre passage dans l'Entreprise Portuaire de Bejaia, certain problèmes on été soulevé tels que :

- Le personnel de l'EPB ne peuvent pas consulter leur mail, ni d'envoyé en cas de coupure d'internet.
- Leur serveur de messagerie externe n'est pas sûr,0 pour l'échange d'information confidentiel.
- Le personnel utilise le fax, pour l'échange d'informations. Plus encore, il se déplace pour l'échange de documents confidentiels, ce qui représente une perte de temps.

2.3.3 Solutions proposés

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

- Mise en place d'un serveur de messagerie interne à base de MS Exchange server 2013.
- Sécuriser le serveur, par les deux protocoles SSL et SSH.
- La gestion et l'administration du serveur de messagerie en interne.

2.3.4 Objectifs

- Rédaction et envoi de message très rapide pour un ou plusieurs destinataires à la fois.
- Permettre à l'administrateur de :
 - Créer, supprimer des comptes utilisateurs (boîtes aux lettres).
 - Créer, modifier des listes de diffusion (ensembles de destinataires réunis sous une même dénomination).
 - Démarrer / Stopper un service (Service SMTP ou POP).
- Permettre à l'utilisateur de :
 - Rédiger des messages, leurs attacher des fichiers joints, et les expédier.
 - Consulter les messages qui lui sont destinés.
 - Répondre à un message sans avoir à retaper l'entête.

2.4 Conclusion

Dans ce chapitre nous avons présenté l'organisme d'accueil, nous avons introduit ses différents services et spécifié leurs besoins, ce qui engendre la nécessité de mettre en oeuvre un serveur de messagerie électronique interne dont les caractéristiques seront spécifiées dans le chapitre qui suit.

3

Outils de développement

3.1 Introduction

La mise en place d'un système de messagerie à base de Microsoft Exchange est un projet qui nécessite d'être préparé et planifié avant toute mise en oeuvre. Ce chapitre sera consacré à définir l'environnement de travail de notre projet. Il portera sur les prérequis nécessaires pour l'installation d'Exchange qui sera implémentée sur le système d'exploitation Windows Server 2012. Nous allons à présent nous intéresser de plus près au service d'annuaire de ce dernier, appelé Active Directory, qui constitue un fondement pour le système Exchange Server, ainsi qu'aux principaux protocoles sur lesquels il s'appuie.

3.2 Windows server 2012

3.2.1 Présentation de Windows server 2012

Microsoft Windows server 2012 est un système d'exploitation orienté serveur complet, souple puissant qui se base sur les améliorations que Microsoft a apportées à Windows server 2008 R2. Ces fonctionnalités partagent une base de code commune qui couvre de nombreux domaines du système d'exploitation, notamment la gestion, la sécurité, le réseau et le stockage[6].

En tant que nouvelle génération du système d'exploitation, Windows Server 2012 est conçu pour aider les administrateurs système à rationaliser leurs infrastructures. Il profite de l'évolution des processeurs vers le 64-bits et des architectures multi-cœurs, de la généralisation de la virtualisation, des nouvelles méthodes de développement et de tests sécurisées. Windows server 2012 possède les caractéristiques suivantes :

- **Modularité pour une indépendance linguistique et création d'images disque pour une indépendance matérielle:** chaque composant du système d'exploitation est conçu comme un module indépendant que l'on peut facilement ajouter ou supprimer. Cette fonctionnalité fournit les bases de l'architecture de configuration de Windows Server 2012. Microsoft distribue Windows Server 2012 sur des supports d'images disque au format WIM (Windows Imaging Format) qui utilisent la compression et le stockage d'instance simple pour réduire de manière spectaculaire la taille des fichiers image.
- **Environnement de pré-installation et de prédémarrage:** windows Pré-installation Environment 4.0 (Windows PE 4.0) remplace MS-DOS comme environnement de pré-installation et fournit un environnement de démarrage

amorçable pour l'installation, le déploiement, la récupération et la résolution des problèmes.

3.2.2 Rôle de serveur, services de rôle et fonctionnalités pour Windows server 2012

Windows server 2012 utilise la même architecture de configuration que Windows server 2008 et Windows server 2008 R2. On prépare les serveurs pour le déploiement en installant et en configurant les composants suivant [6]:

- **Rôles de serveur** : un rôle de serveur est un ensemble de composants logiciels apparentés qui permet au serveur d'effectuer une fonction spécifique pour les utilisateurs et les ordinateurs d'un réseau. Un ordinateur peut être dédié à un rôle unique, comme les services de domaine Active Directory (AD DS), ou tenir plusieurs rôles.
- **Services de rôle** : un service de rôle est un composant logiciel qui fournit la fonctionnalité d'un rôle de serveur. Chaque rôle peut avoir un ou plusieurs services de rôle associés. Certains rôles de serveur, comme serveur DNS ou serveur DHCP, ont une fonction unique, et l'installation du rôle installe la fonction. D'autres rôles, comme les services de stratégie et d'accès réseau et les services de certificats Active Directory (AD DS) ont plusieurs services de rôle que nous nous pouvons installer.
- **Fonctionnalités** : une fonctionnalité est un composant logiciel qui offre des fonctions supplémentaires. les fonctionnalités comme chiffrement de lecteur Bitlocker et sauvegarde Windows server s'installent et se suppriment séparément des rôles et des services de rôle. Il est possible d'installer plusieurs fonctionnalités sur un ordinateur ou de n'en installer aucune, selon sa configuration.

3.2.3 Protocole LDAP (Lightweight Directory Access Protocol)

3.2.3.1 Présentation de l'annuaire

L'annuaire est une structure hiérarchique permettant de stocker des objets du réseau : ordinateurs, utilisateurs, groupes mais aussi domaines, applications, services et stratégies de sécurité. Pour chaque objet qu'il contient, l'annuaire stocke différents types d'informations appelées attributs[6].

3.2.3.2 Historique

X.500 est un standard constitué d'un ensemble de protocoles standards, tous issus des travaux de l'ISO. Le standard X.500 a été conçu dès le départ pour offrir aux services d'annuaire des services complets. Véritable annuaire du monde OSI, il repose sur les services de la couche 7 (application) du modèle OSI de l'ISO. Cependant, cet énorme cahier des charges et sa complexité de mise en oeuvre sont les causes des nombreux problèmes de fonctionnement et de performances des premières versions d'annuaire X.500. De par son coût, il est réservé aux grands comptes très demandeurs de ces technologies, comme les opérateurs de télécommunications, pour lesquels il a été initialement conçu.

3.2.3.3 Définition

LDAP est un protocole d'accès aux annuaires qui permet d'ajouter, de modifier et de supprimer des données enregistrées dans un annuaire, et qui permet en outre de rechercher et de récupérer ces données. LDAP est la norme industrielle de l'accès aux annuaires[6].

3.2.3.4 Fonctionnement

LDAP définit comment un client d'annuaire peut accéder à un serveur d'annuaire, mais aussi comment il peut effectuer des opérations d'annuaire et partager des données d'annuaire. Les clients Active Directory utilisent LDAP pour obtenir des données d'Active Directory ou pour y maintenir des données. Il permet à une structure Active Directory de pouvoir lier d'autres applications clientes conforme à sa norme. En disposant d'autorisations appropriées, n'importe quelle application conforme aux règles LDAP peut ajouter, modifier et supprimer des données dans Active Directory c'est le cas notamment d'Exchange. L'utilisation du protocole LDAP permet de positionner Active Directory comme la référence d'annuaire au sein d'une entreprise[6].

3.3 Active directory

3.3.1 Définition

Active Directory est le nom du service d'annuaire de Microsoft apparu dans le système d'exploitation Microsoft Windows Server 2000. Le service d'annuaire Active Directory est chargé de répertorier tout ce qui touche au réseau comme le nom des utilisateurs, des imprimantes, des serveurs, des dossiers partagés, etc. L'utilisateur

peut ainsi trouver facilement des ressources partagées, et les administrateurs peuvent contrôler leurs utilisations grâce à des fonctionnalités de distribution, de duplication, de partitionnement et de sécurisation des accès aux ressources répertoriées, il est basé sur les standards TCP/IP : LDAP, Kerberos... et s'exécute uniquement sur des contrôleurs de domaines. Active Directory se définit sur trois ensembles :

- **Le stockage** : Active Directory enregistre de façon hiérarchique les informations relatives aux objets du réseau et met ces informations à la disposition des administrateurs, des utilisateurs et des applications.
- **La structure** : Active Directory permet d'organiser le réseau et ses objets à l'aide d'entités telles que les domaines, les arborescences, les forêts, les relations d'approbation, les unités d'organisation et les sites.
- **L'intercommunication** : Si une organisation possède des agences éloignées géographiquement, Active Directory assure une cohérence et une disponibilité des informations contenues dans sa base, en répliquant les informations relatives à la structure logique entre tous les contrôleurs de domaines de la forêt.

3.3.2 Vue d'ensemble d'Active Directory

Le rôle Service de domaine Active Directory contient des composants physiques et logiques.

3.3.2.1 Structure physique

Les composants physiques vont englober plusieurs éléments clés dans un domaine Active Directory :

- **Le contrôleur de domaine** : contient une copie de la base de données Active Directory. Il permet d'authentifier les utilisateurs lors de la connexion au réseau et pouvoir ainsi adapter les droits sur les ressources partagées et la politique de sécurité (en fonction de l'utilisateur). Le contrôleur de domaine, donne au poste client un script de connexion (quelques lignes de programme) permettant de gérer une partie des droits et des partages de l'utilisateur authentifié.
- **La base de données et le dossier sysvol** : Le dossier SYSVOL est un dossier partagé sur chaque contrôleur de domaine. Il permet essentiellement le stockage de la partie " fichiers " des objets de stratégie de groupe ainsi que les

scripts de connexion. Sachant que son contenu doit être strictement identique entre chacun des contrôleurs de domaine, le dossier SYSVOL est répliqué. Cela induit que la moindre modification effectuée sur un contrôleur de domaine est propagée sur ses pairs à l'aide d'un service de réplication de fichiers.

- **Le serveur catalogue global :** Le catalogue global est l'ensemble de tous les objets d'une forêt AD DS (Active Directory Domain Services). Un serveur de catalogue global est un contrôleur de domaine qui enregistre une copie complète de tous les objets de l'annuaire pour son domaine hôte et une copie partielle en lecture seule de tous les objets pour tous les autres domaines de la forêt. Les serveurs de catalogue global répondent aux demandes de catalogue global.

3.3.2.2 Structure logique

Est la décomposition de l'entreprise en domaines, arborescences, unités d'organisation. Cette décomposition pourra être guidée par la structure de l'entreprise et, surtout, par les besoins d'administrations, ces composants physiques vont englober plusieurs éléments clés dans un domaine Active Directory :

- **Les partitions :** qui sont des sections de la base de données Active Directory. Il existe trois types de partitions d'annuaire : configuration, schéma et application. Chaque magasin d'annuaire AD LDS (Active Directory Lightweight Directory Services) doit contenir une partition d'annuaire de configuration unique et une partition d'annuaire de schéma unique, et il peut contenir soit zéro soit davantage de partitions d'annuaire d'application.
- **Le schéma Active Directory :** est un composant logiciel enfichable MMC (Microsoft Management Console) que vous pouvez utiliser pour afficher et gérer le schéma des services de domaine Active Directory (AD DS). Il inclut deux conteneurs : le conteneur " Classes " et le conteneur " Attributs ". Ces conteneurs stockent les définitions de classes et d'attributs. Ces définitions prennent la forme d'objets classSchema, qui se trouve dans le conteneur " Classes ", et d'objets attributeSchema, qui se trouve dans le conteneur " Attributs ".
- **Les services de domaine Active Directory (AD DS) :** stockent les données d'annuaire et gèrent les communications entre les utilisateurs et les domaines, y compris les processus d'ouverture de session utilisateur, l'authentification et les recherches dans l'annuaire. Un contrôleur de domaine Active Directory est un serveur qui exécute les services de domaine Active Directory.

- **Une arborescence de domaine** : ensemble de domaines appartenant à une même hiérarchie de nom DNS.
- **La forêt Active Directory** : Une forêt est une collection d'un ou plusieurs domaines Active Directory qui partagent la même structure logique, le même schéma d'annuaire (définitions de classes et d'attributs), la même configuration d'annuaire (informations de site et de réplication) et le même catalogue global (fonctionnalités de recherche à l'échelle de la forêt). Les domaines d'une même forêt sont automatiquement liés par des relations d'approbation transitives bidirectionnelles.
- **Le site Active Directory** : est un composant logiciel enfichable MMC (Microsoft Management Console) qui permet d'administrer la réplication des données d'annuaire parmi tous les sites d'une forêt des services de domaine Active Directory (AD DS). Il fournit également une vue des objets spécifiques aux services qui sont publiés dans les services AD DS.
- **L'unité d'organisation** : Une Unité organisationnelle (Organizational Unit ; OU ; UO) est un objet conteneur qui permet de hiérarchiser Active Directory. Cette notion était inexistante dans les "versions précédentes" d'AD, telle que la base de données SAM. L'AD permet une hiérarchisation des domaines. À l'intérieur de ces domaines, il existe maintenant des possibilités de structuration et de hiérarchisation des utilisateurs qui permet d'appliquer une stratégie de groupe mais également de mettre en place une délégation.

3.3.3 Relation entre Active Directory et DNS

Les services de domaine Active Directory (AD DS) utilisent les services de résolution de noms DNS (Domain Name System) pour que les clients puissent localiser les contrôleurs de domaine et pour que les contrôleurs de domaine hébergeant le service d'annuaire puissent communiquer entre eux.

Les services de domaine Active Directory permettent d'intégrer facilement l'espace de noms Active Directory à un espace de noms DNS existant. Les fonctionnalités telles que les zones DNS intégrées à Active Directory facilitent le déploiement du système DNS en évitant d'avoir à installer des zones secondaires et à configurer des transferts de zone. DNS et AD utilisent tous deux une base de données pour la résolution des noms.

- DNS est un service de résolution de noms d'hôtes. Il résout les noms de domaines et les noms d'ordinateurs en renvoyant les adresses IP via les demandes

reçues par les serveurs DNS en tant que requêtes sur la base de données DNS. DNS n'a pas besoin d'Active Directory pour fonctionner.

- Active Directory utilise le protocole LDAP pour permettre la recherche d'objets de domaine. Afin d'exécuter des recherches dans une architecture complexe, Active Directory utilise le service DNS comme localisateur pour résoudre des noms de domaines, de sites ou de services.
- Les domaines Active Directory et DNS sont organisés suivant des structures hiérarchiques identiques. Bien qu'ils diffèrent et soient mis en oeuvre différemment pour des objectifs séparés, les espaces de noms d'une organisation pour ces deux types de domaines ont une structure identique. Par exemple, masociete.com est à la fois un domaine DNS et un domaine Active Directory.
- Les zones DNS peuvent être enregistrées dans Active Directory. Si on utilise le service DNS de Windows 2008, les zones principales peuvent être enregistrées dans Active Directory pour être répliquées vers d'autres contrôleurs de domaine Active Directory et pour assurer une meilleure sécurité du service DNS.
- Les clients Active Directory utilisent DNS pour localiser les contrôleurs de domaine. Dans le cas d'un domaine particulier, les clients Active Directory demandent à leur serveur DNS les enregistrements de ressources spécifiques.

3.3.4 Relation entre Active Directory et LDAP

LDAP définit les opérations qui peuvent être utilisées pour demander et modifier les informations de l'annuaire. Chaque fois qu'ils ouvrent une session sur le réseau ou cherchent des ressources partagées, les clients Active Directory emploient le protocole LDAP pour communiquer avec les ordinateurs Active Directory. Nous pouvons également utiliser LDAP pour gérer Active Directory.

LDAP est une norme ouverte employée par beaucoup d'autres services d'annuaire. Elle simplifie les communications entre annuaires et la migration des autres services d'annuaire vers Active Directory. Nous pouvons aussi exploiter ADSI (Active Directory Service Interface) pour améliorer l'interopérabilité. ADSI prend en charge les API standard pour LDAP définies dans la RFC 1823. Nous pouvons utiliser ADSI avec l'environnement d'exécution de scripts Windows pour créer et gérer des objets dans Active Directory.

3.4 Exchange server 2013

3.4.1 Présentation

Microsoft Exchange est un logiciel de messagerie propriétaire de Microsoft, fréquemment utilisé par de grandes sociétés ainsi que dans le Cloud. Ce Logiciel a été conçu pour l'échange du courrier, la gestion des calendriers et des contacts. Toutes les informations sont stockées dans une base de données sur le serveur et sont accessibles à partir d'un grand nombre de systèmes clients : Appareils mobiles, clients lourds Outlook, Interface web, etc...

Exchange 2013 Ne possède que 2 rôles. Pour des raisons de sécurité notamment, il est conseillé de séparer les différents rôles fournis par Exchange Sur deux serveurs physiques différents. En effet, nous ne donnons pas l'accès direct au serveur contenant les boîtes mails " Mailbox Server ", mais nous passons par un système de redirection et de gestion des connexions "Client Access Server ".

Exchange 2013, contrairement à ses prédécesseurs, ne possède plus que 2 grands rôles au lieu de 5, dans cette architecture que nous pourrions qualifier de multi-rôles : - Accès client (CAS). -Boîte aux lettres (MBX).

3.4.1.1 Rôle d'accès client (Client Access rôle)

Comme son nom l'indique, ce rôle sert d'intermédiaire entre le client et le Mailbox Server lors de connexions avec Outlook, OWA etc...

- Il Est responsable d'authentifier, de fournir la connexion sécurisée SSL.
- De rediriger et de router les différentes requêtes vers le bon Mailbox Serveur Contenant la boîte mail de l'utilisateur.
- Il Offre également les différents protocoles tels que le POP, SMTP, IMAP, RPC Over HTTPS

De différents services sont assurés:

- Client Access Service : gère les connections entre les clients et la boîte mail.
- Front End Transport Service: Fonction de filtrage des mails, routage de mails entre les serveurs Exchange et les serveurs externes.
- AutoDiscovery: Permet de configurer le client de messagerie (Outlook 2007 et plus) automatiquement en fonction des informations de logon si le client est dans un domaine.

3.4.1.2 Rôle de boîte aux lettres (Mailbox)

Ce rôle permet au serveur Exchange de :

- Stocker la base de données concernant les boîtes mails des clients.
- Stocker les dossiers publics.
- Responsable du stockage et du traitement des données.
- Service Hub Transport permet le routage des mails dans l'organisation et la connexion entre le Front End Transport Service et le Mailbox Transport Service.
- Service Mailbox Transport qui assure la connexion entre le Hub Transport Service et les bases de données de mails.

Aucune connexion n'a lieu entre un client mail (Outlook, OWA...) et ce serveur et il ne doit pas être accessible depuis l'extérieur ou l'intérieur (excepté le CAS). Ce rôle est étroitement lié avec Active Directory, le Client Access Server et la base de données des boîtes mails. Ce rôle peut également bénéficier d'une redondance en ayant plusieurs Mailbox Server Formant un Database Availability Group (DAG).

3.4.2 Les nouveautés d'Exchange server 2013

1. **Exchange Server 2013 réduit les coûts grâce à une optimisation pour les nouvelles générations de hardware :** exchange 2013 est optimisé pour les disques de 8 To, en réduisant les IOPS par base de données de + de 50
2. **Réduction significative des Overheads pour la haute disponibilité :** la gestion des DAG est simplifiée via la configuration réseau automatique des DAGs, des améliorations des commandes de gestion des DAGs, le support de plusieurs bases par disque. Des capacités de récupération automatique (directement intégrées dans les DAGs) sont maintenant étendues au reste d'Exchange et aux protocoles.
3. **Passez moins de temps à gérer les serveurs tout en gardant le contrôle :** Exchange fournit une nouvelle interface d'administration web, simple à utiliser : Exchange Administration Center (l'EAC). La délégation d'administration RBAC (Role Based Access Control) permet de réaliser certaines opérations en mode délégation, sans avoir besoin des permissions élevées.

4. **Protection automatique d'Exchange en cas de surcharges de trafic :** Exchange permet de contrôler les surcharges de trafic. Toute tâche système qui n'est pas impérative est automatiquement différée à des heures " calmes " afin de favoriser les tâches de haute priorité.
5. **Le cloud comme vous le décidez : Exchange 2013 dispose d'un Cloud configurable:** Soit migré la totalité de nos BAL sur le Cloud, soit partir sur un modèle hybride avec des BAL gérées dans l'infrastructure existante et des BAL gérées dans le Cloud. Les utilisateurs pourront dès lors partager des calendriers et des meetings entre ceux qui sont sur la même infrastructure et ceux qui sont hostés sur le cloud. Les BAL peuvent être migrés en douceur sur le Cloud. On garde toujours le contrôle sur le Cloud et nous pouvons tester les mises à jour bien en avance afin de mieux les planifier.
6. **Protection automatique des emails contre les malwares :** Exchange offre une protection anti-malware de base dans le produit. Les administrateurs peuvent configurer et gérer les niveaux de protection depuis la console d'administration Exchange. Cette fonctionnalité peut être arrêtée, remplacée ou renforcée via l'ajout de service premium tel que EOP (Exchange Online Protection).
7. **Protégez les données sensibles et informez proactivement les utilisateurs de la politiques internes de données grâce au DLP (Data Loss Prevention) :** Aidez l'entreprise à se protéger contre les partages et les fuites d'informations sensibles entre les utilisateurs et des personnes non autorisées. La nouvelle fonctionnalité DLP permet d'identifier, de surveiller et protéger les données dites " sensibles " de l'entreprise au travers d'une analyse du contenu de celles-ci. Exchange offre des politiques existantes fondées sur des organismes de régulation standards tels que PII et PCI. Ces politiques sont extensibles à d'autres qui peuvent être nécessaire au bon déroulement des affaires. Le client de messagerie Outlook peut maintenant prévenir les utilisateurs en cas de violation des politiques de sécurité au niveau du contenu alors même que celui-ci est créé et permet d'éduquer ceux-ci au respect des standards tels que définis par l'entreprise.

8. **Permettre aux responsables conformité de lancer un audit eDiscovery sur Exchange, SharePoint et Lync depuis une seule interface :** La capacité de préserver une information avec une garantie d'intégrité et de lancer des recherches au travers de toute l'organisation de l'entreprise est essentielle afin de garantir la conformité interne et réglementaire.

3.5 Conclusion

Nous avons présenté dans ce chapitre les concepts fondamentaux d'Active Directory qui sont particulièrement nécessaires pour la suite de notre travail sur Exchange 2013 puisque le fonctionnement et l'administration de ce dernier sont étroitement liés au service d'annuaire de Windows Server 2012. Comme nous avons aussi présenté Exchange server 2013.

Nous traiterons dans ce qui suit la mise en place et la configuration du système de messagerie sous Exchange 2013 ainsi que les différentes tâches relatives à son administration.

4

Installation, configuration et administration d'Exchange Server 2013

4.1 Introduction

Ce chapitre portera sur les tâches à réaliser afin de mettre en place une organisation Exchange 2013, à travers les différentes étapes nécessaires, allant de la planification jusqu'à l'installation finale. Nous allons décrire étape par étape, et de manière explicite, tout le travail que nous avons effectué dans le cadre de notre projet en commençant ainsi que les prérequis nécessaires pour une bonne configuration d'Exchange 2013.

4.2 Présentation du travail

Notre projet consiste à déployer un système de messagerie basé sur les produits Microsoft Windows server 2012 et Exchange 2013 sur un labo constitué de machine. Le travail se fera sur des environnements windows server 2012 pour les serveurs et windows 7 pour les machines clientes que nous utiliserons pour tester le fonctionnement de la messagerie.

Notre machine est nommée " serveurEPB ", fera office d'un contrôleur de domaine Active Directory ainsi qu'un serveur DNS avec l'adresse IP : 172.16.100.190 et le nom de domaine " portdebejaia.dz " avec le nom NETBIOS " PORTDEBEJAIA " elle hébergera aussi les rôles d'Exchange nécessaires pour faire fonctionner le système de messagerie.

Pour cela nous avons au début effectué un stage pratique de 40 jours au sein du service Informatique de l'Entreprise Portuaire de Bejaia (EPB). Cela nous a permis de nous familiariser, au contact des professionnels, avec les différentes tâches relatives à l'administration d'un système de messagerie mais surtout de connaître les enjeux qui entourent ce dernier en matière de facilité d'accès, de disponibilité continue des données et de suivi des messages échangés.

Bien que cette entreprise a déjà mise en place une version antérieure d'Exchange (2013) mais elle reste non opérationnel, ce stage nous a été très bénéfique dans la mesure où nous avons pu cerner les principaux enjeux et problèmes qu'il faut prendre en considération lors de la résolution de notre travail. Avant de commencer l'installation d'Exchange server 2013, il faut d'abord s'assurer de respecter tous les prérequis nécessaires. Nous allons dresser la liste des prérequis que nous avons vérifié.

1. Installer le rôle Active Directory pour en faire un contrôleur de domaine:

Active Directory est la base d'un réseau Microsoft. Il permet la gestion des ressources : utilisateurs et périphériques, l'authentification et la sécurisation

des accès. Mais c'est aussi la base de nombreux autres services comme DNS, IIS, DHCP,...

Pour ajouter Active Directory, nous avons passé par l'assistant de gestion des Rôles, au niveau des rôles, nous avons sélectionné " Service AD DS " qui correspond au service de domaine Active Directory en cochant la case, puis nous avons cliqué sur " Ajouter des fonctionnalités ".

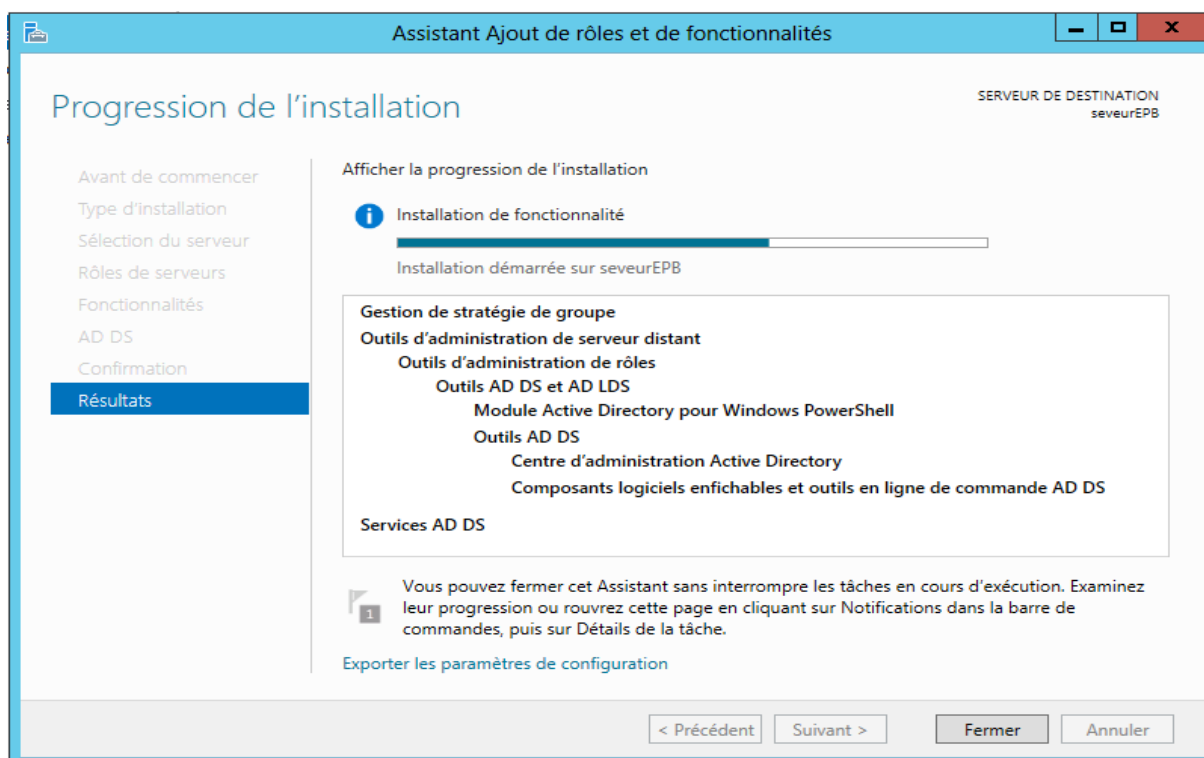


Figure 4.1: Installation du rôle Active Directory.

A la fin de l'installation, le message suivant est affiché : " Configuration requise pour : Services AD DS à SERVEUREPB", nous avons cliqué dessus pour lancé l'assistant de configuration des services de domaine Active Directory afin de promouvoir un serveur au rang d'un contrôleur de domaine et dans notre cas, Ça sera le premier contrôleur de domaine de la forêt et par conséquent, le domaine racine. qu'on a nommé " portdebejaia.dz ".

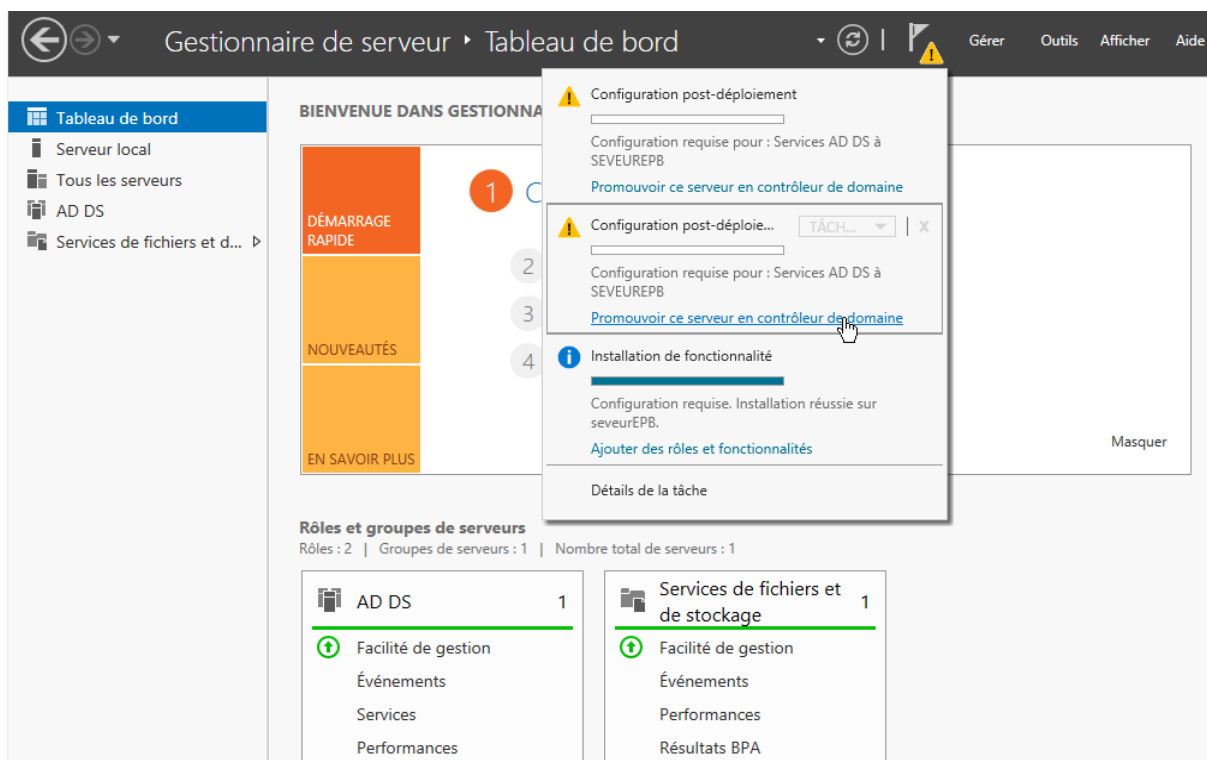


Figure 4.2: Configuration du service AD DS.

2. Préparation du schéma Active Directory:

Pour préparer notre schéma, nous avons besoin d'identifier notre contrôleur de domaine qui héberge le rôle FSMO contrôleur de schéma, et cela en exécutant la commande " regsvr32 schmmgmt " dans la fenêtre d'exécution.

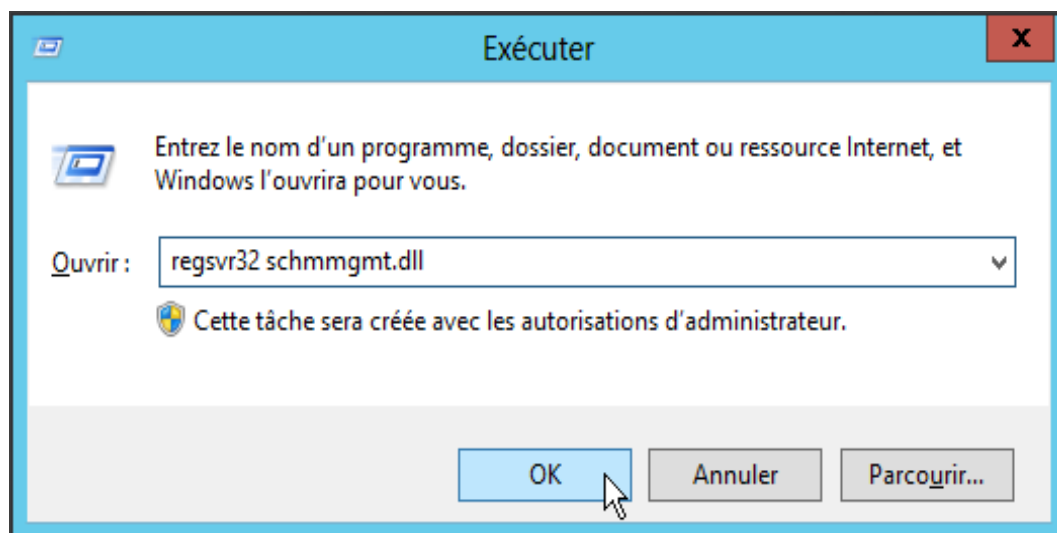


Figure 4.3: Identification du contrôleur de domaine.

Dans la " mmc " dans la fenêtre " console1 ", nous avons sélectionné le menu " Fichier " puis " Ajouter/Supprimer un logiciel enfichable " .

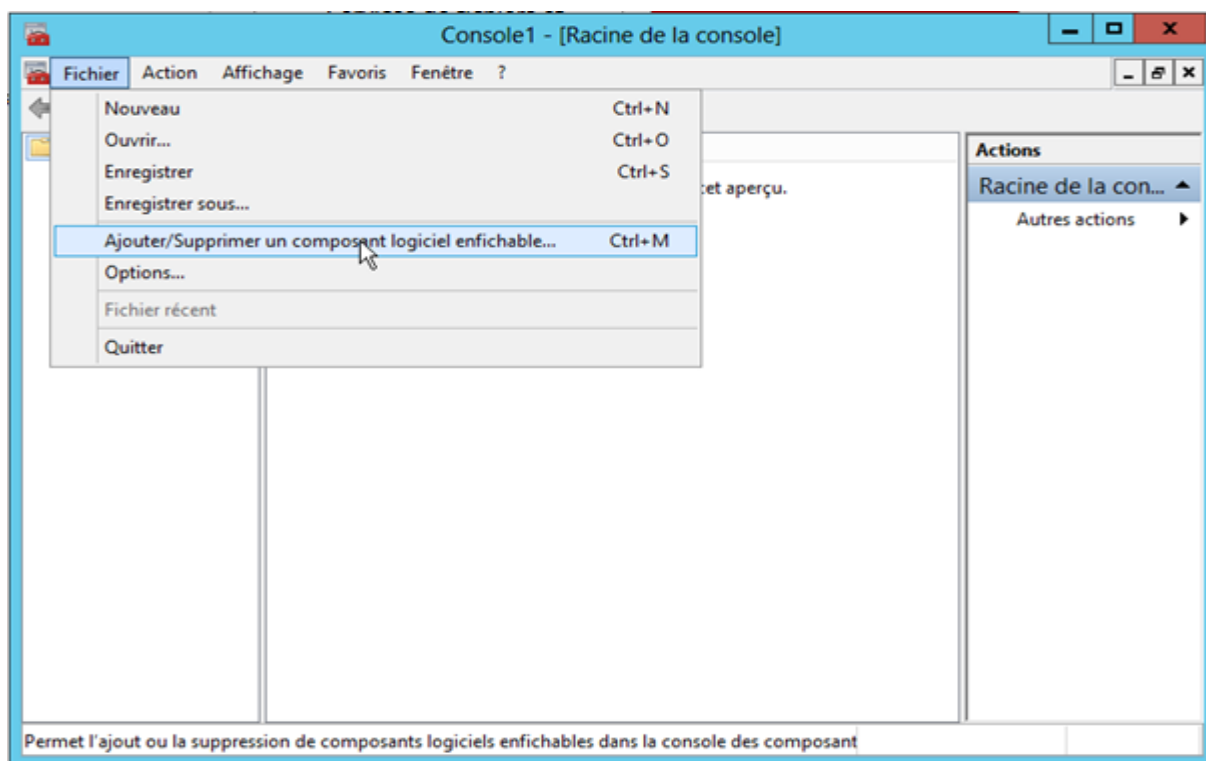


Figure 4.4: L'ajout d'un logiciel enfichable.

Puis dans la colonne " Composant logiciels enfichables ", nous avons sélectionné "Schéma Active Directory " puis " Ajouter " et valider.

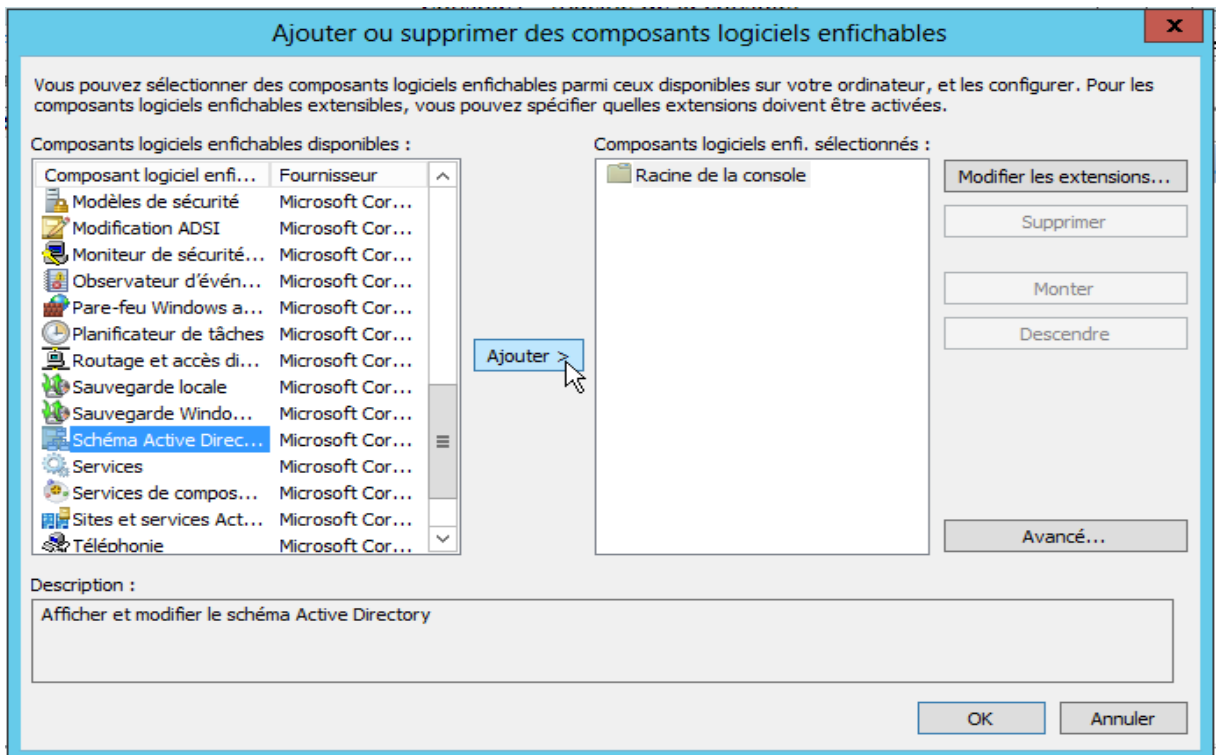


Figure 4.5: L'ajout du schéma Active Directory.

Ensuite dans la " console1 ", nous avons fait un clic droit sur " Schéma Active Directory [serveurEPB.portdebejaia.dz] " puis nous avons sélectionné " Maître d'opération " pour indiquer le serveur qui joue le rôle de contrôleur de domaine.

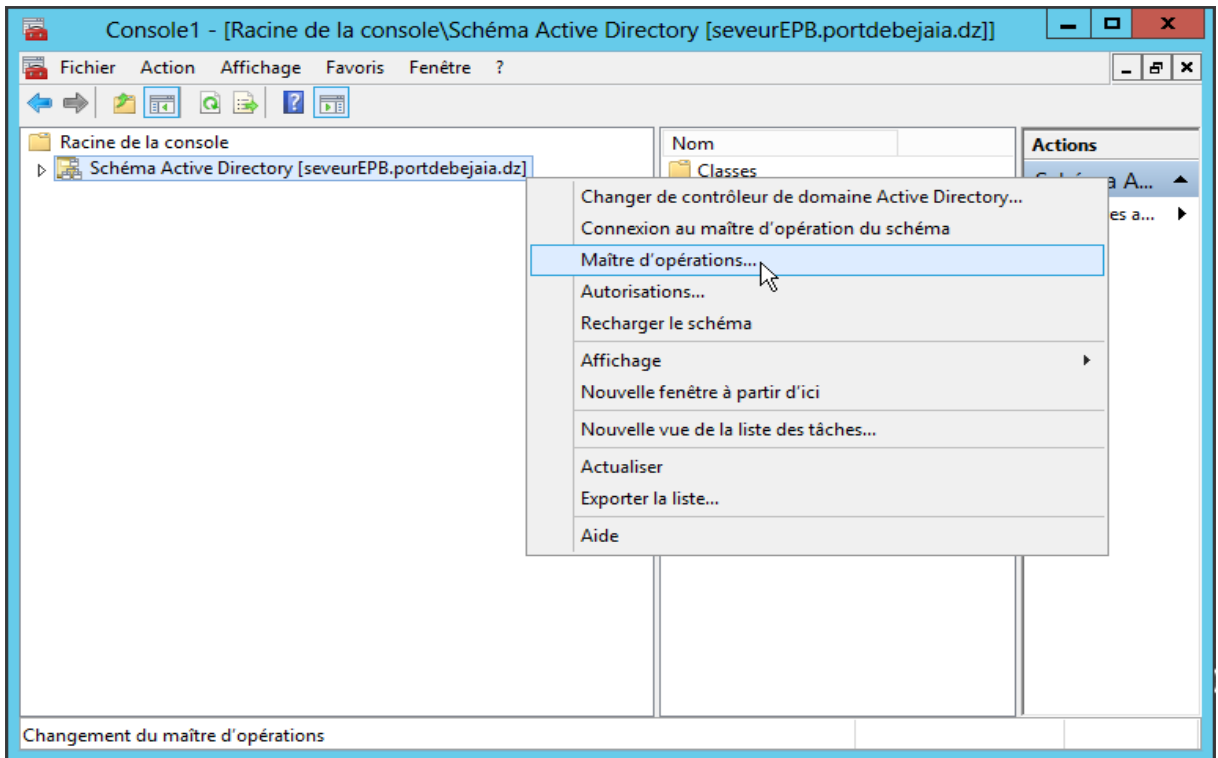


Figure 4.6: Indication du serveur controleur de domaine.

Enfin, pour préparer le schéma Active Directory, nous avons besoin d'installer les outils RSAT. Nous avons ouvert l'invite de commandes " PowerShell ", Puis nous avons exécuté la commande "Install-WindowsFeature RSAT-ADDS ".

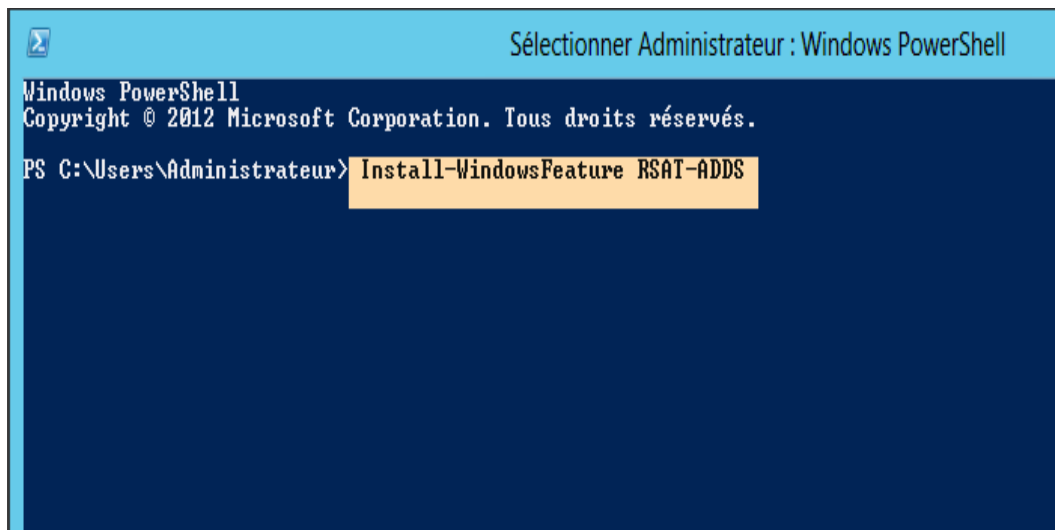


Figure 4.7: Installation des outils RSAT.

Une fois que les outils RSAT sont installés, nous pouvons préparer le schéma Active Directory. Et pour cela nous avons inséré le média d'installation d'Exchange 2013, dans une invite de commande nous avons exécuté la commande " setup.exe /PrepareSchema /IAcceptExchangeServerLicenseTerms ".

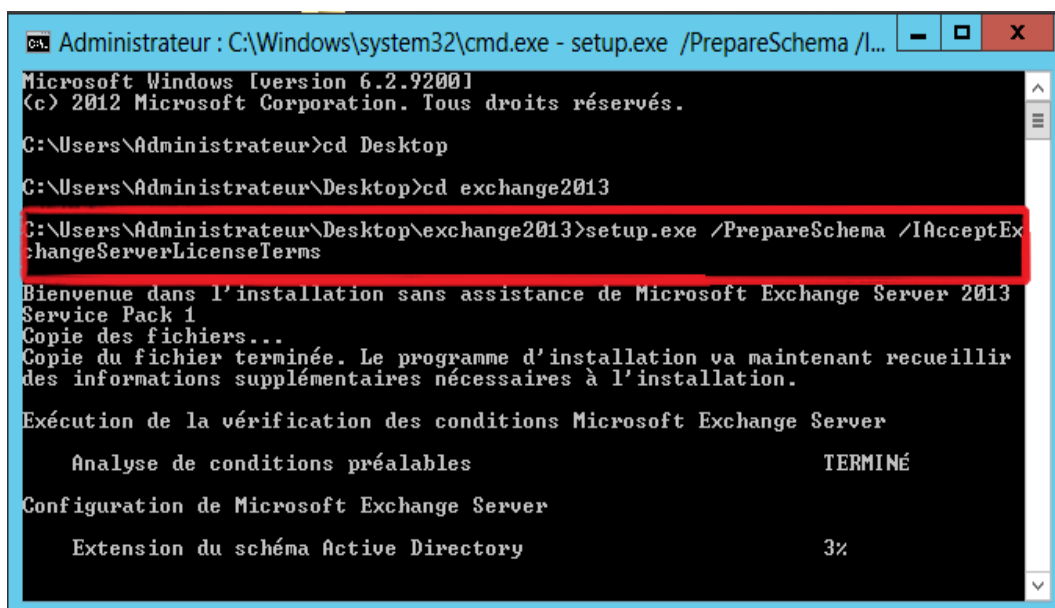
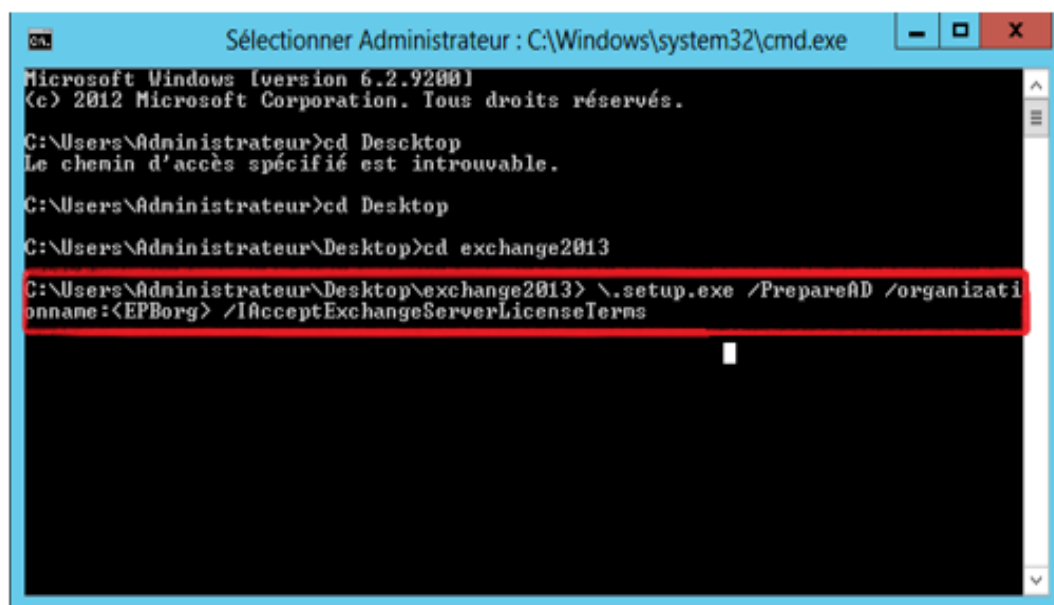


Figure 4.8: Préparation du schéma Active Directory.

3. Préparation de l'Active Directory:

Dans cette étape, nous avons ajouté des objets mais également créer notre organisation. Pour ce faire, nous avons utilisé le média d'installation Microsoft Exchange 2013 et l'invite de commande pour exécuté la commande " Setup.exe /PrepareAD /OrganizationName : <nom de l'organisation> /IAcceptExchangeServerLicenseTerms " (le nom de notre organisation est " EP-Borg ").



```
Microsoft Windows [version 6.2.9200]
(c) 2012 Microsoft Corporation. Tous droits réservés.

C:\Users\Administrateur>cd Desktop
Le chemin d'accès spécifié est introuvable.

C:\Users\Administrateur>cd Desktop

C:\Users\Administrateur\Desktop>cd exchange2013

C:\Users\Administrateur\Desktop\exchange2013> .\setup.exe /PrepareAD /organizationname:<EPBorg> /IAcceptExchangeServerLicenseTerms
```

Figure 4.9: Préparation de l'Active Directory.

Une fois terminé, nous pouvons vérifier que l'organisation à bien été créé via la console " Modification ADSI ", et cela en suivant les étapes ci-dessous :

- On Ouvre la console via la fenêtre " Exécuter ", puis on tape " adsiedit.msc " .
- Dans la fenêtre qui apparait la colonne de gauche, on fait un clic droit sur " Modification ADSI " puis on sélectionne " Connexion " .
- Puis dans la fenêtre " Paramètre de connexion ", dans la liste déroulante " Contexte d'attribution " on sélectionne " Configuration " .
- Dans l'arborescence de gauche, on déplie le conteneur " CN=Configuration, DC=<domaine>, DC=<tld> ", et ensuite le conteneur " CN=Services ", puis " CN=Microsoft Exchange " on vérifie que " CN= epborg " existe.

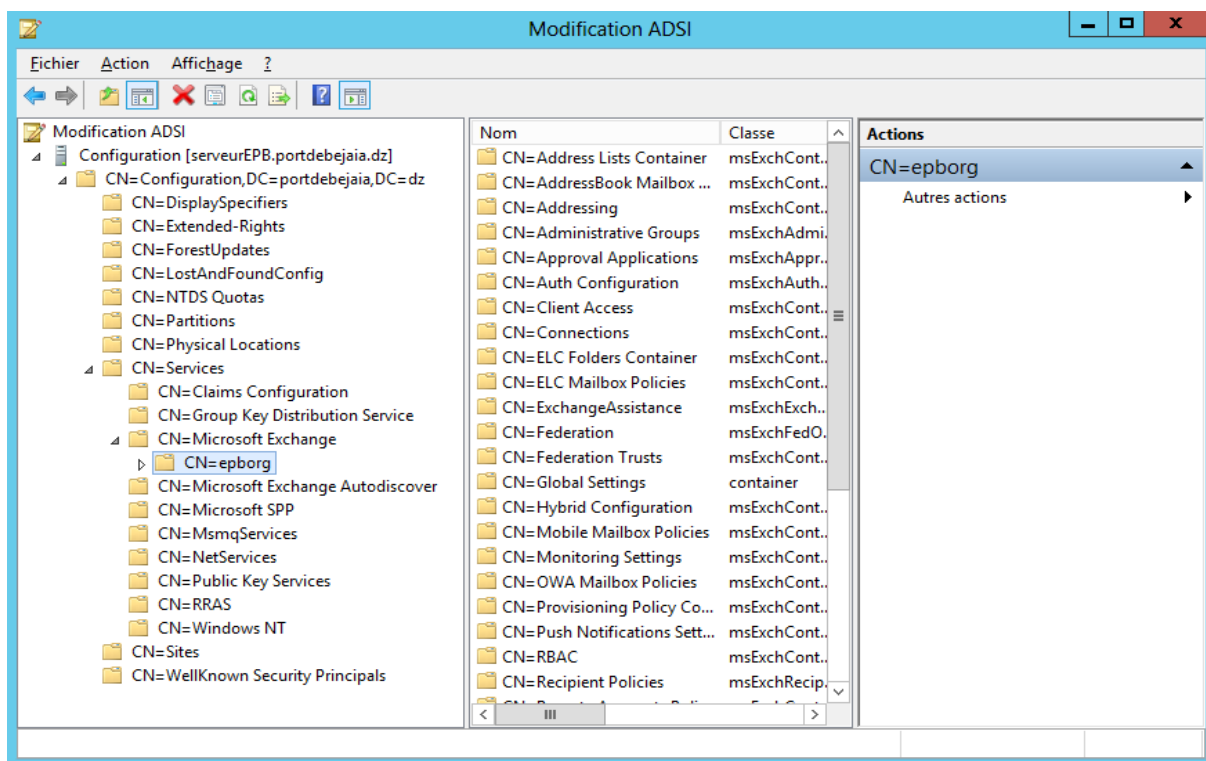


Figure 4.10: Vérification de l'organisation.

4. Installation et configuration du serveur DNS:

Tout domaine doit comporter un serveur DNS principale. Ce serveur peut être intégré à Active Directory ou lui faire jouer le rôle de serveur principale standard. Les serveurs principaux doivent posséder des zones de recherche directe et des zones de recherche inversée. Les recherches directes résolvent les noms de domaine en adresse IP. Les recherches inversées authentifient les requêtes DNS en résolvant des adresses IP en nom de domaine ou hôte.

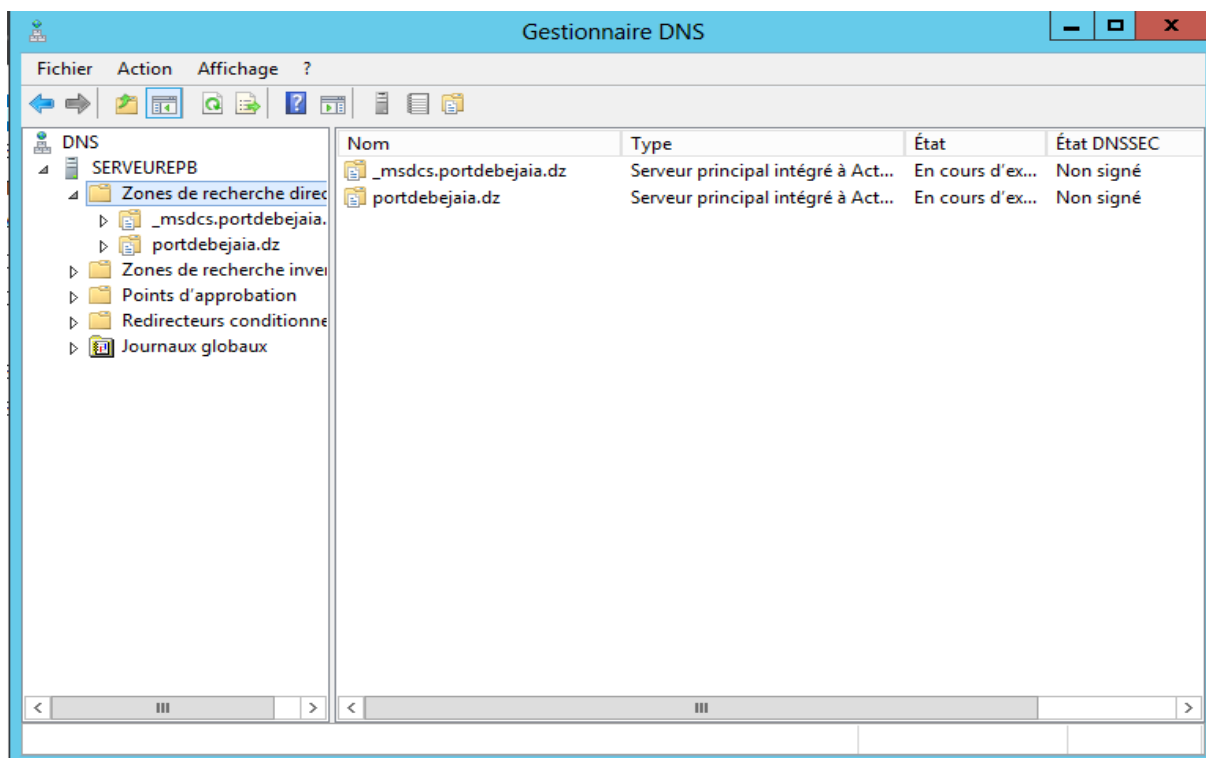


Figure 4.11: Configuration du serveur DNS.

La préparation de l'infrastructure est ainsi achevée.

5. Installation des prérequis sur le serveur qui exécutera Exchange 2013:

Dans notre cas, nous avons installé le rôle serveur de boîtes aux lettres et le rôle serveur d'accès client sur la même machine. Les commandes ci-après se font sur le serveur membre, celui qui exécutera exchange 2013. Nous avons besoin d'installer une série de fonctionnalités, nous le ferons depuis PowerShell. Dans une invite de commandes " PowerShell ", nous avons exécuté les commandes ci-dessous :

```
" Install-WindowsFeature AS-HTTP-Activation, Desktop-Experience, NET-  
Framework-45-Features, RPC-over-HTTP-proxy, RSAT-Clustering, RSAT-Clustering-  
CmdInterface, RSAT-Clustering-Mgmt, RSAT-Clustering-PowerShell, Web-Mgmt-  
Console, WAS-Process-Model, Web-Asp-Net45, Web-Basic-Auth, Web-Client-  
Auth, Web-Digest-Auth, Web-Dir-Browsing, Web-Dyn-Compression, Web-Http-  
Errors, Web-Http-Logging, Web-Http-Redirect, Web-Http-Tracing, Web-ISAPI-  
Ext, Web-ISAPI-Filter, Web-Lgcy-Mgmt-Console, Web-Metabase, Web-Mgmt-  
Console, Web-Mgmt-Service, Web-Net-Ext45, Web-Request-Monitor, Web-Server,  
Web-Stat-Compression, Web-Static-Content, Web-Windows-Auth, Web-WMI,  
Windows-Identity-Foundation -restart"
```

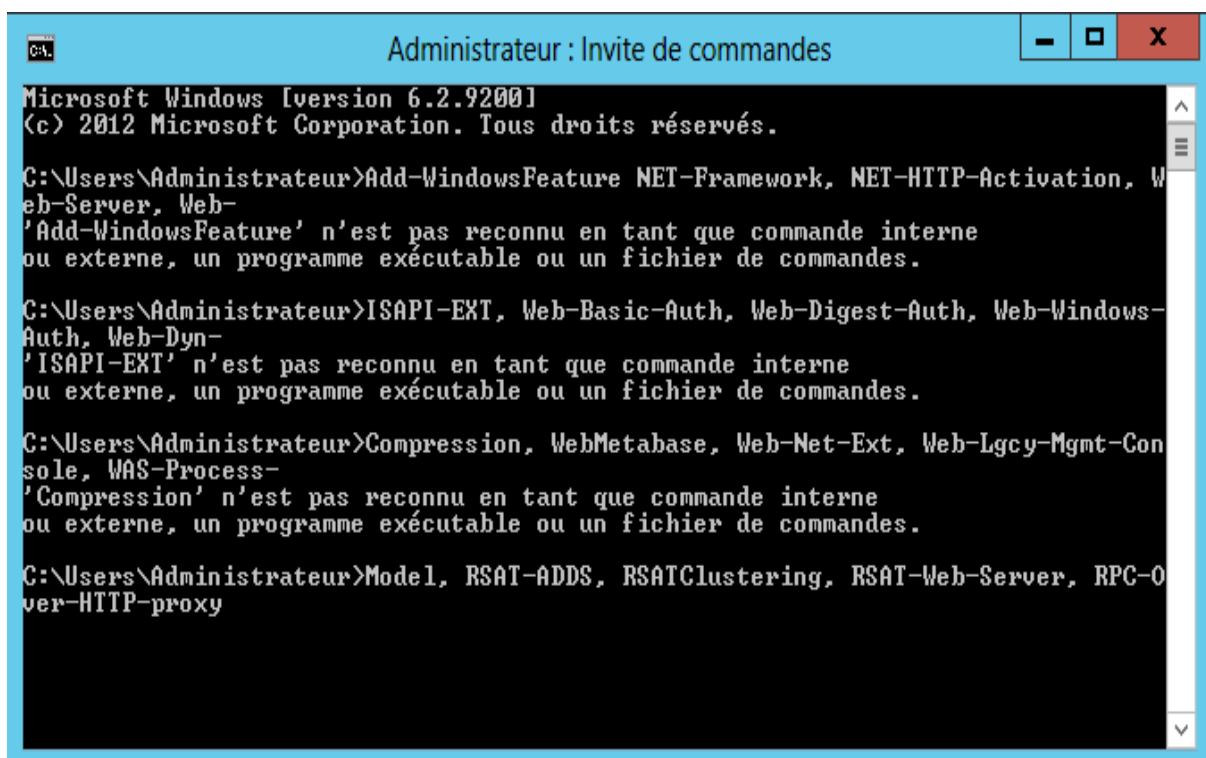


Figure 4.12: Installation des rôles boîtes au lettres et accès client.

Après avoir téléchargé les composants additionnels nous devons les installer dans l'ordre suivant :

- **Microsoft Unified Communications Managed API 4.0** : UCMA 4.0 est une plate-forme de code managé que les développeurs utilisent pour créer des applications qui permettent d'accéder et de contrôler sur l'information Présence renforcée de Microsoft, la messagerie instantanée, les appels téléphoniques et vidéo, et audio / vidéo conférence.

- **Microsoft Office 2010 filter pack 64 bits:** permet d'afficher les documents de type office dans un navigateur web sans avoir besoin de disposer d'un office localement sur la machine.
- **Microsoft Office 2010 filter pack 64 bits SP1:** contient de nouvelles mises à jour permettant d'améliorer la sécurité, les performances et la stabilité. En outre, le SP est un correctif cumulatif de toutes les mises à jour publiées précédemment.

Une fois c'est prérequis sont bien installé nous pouvons lancer l'installation d'Exchange server 2013.

4.3 Installation d'exchange server 2013

On fait un clic droit sur l'exécutable " setup.exe " puis " exécuter en tant qu'administrateur ".

sur la page de " sélection du rôle de serveur ". ici nous avons choisi de séparer les deux rôles sur ce serveur. Donc on va d'abord installer le "rôle de boîte aux lettres" comme le montre la figure suivante.

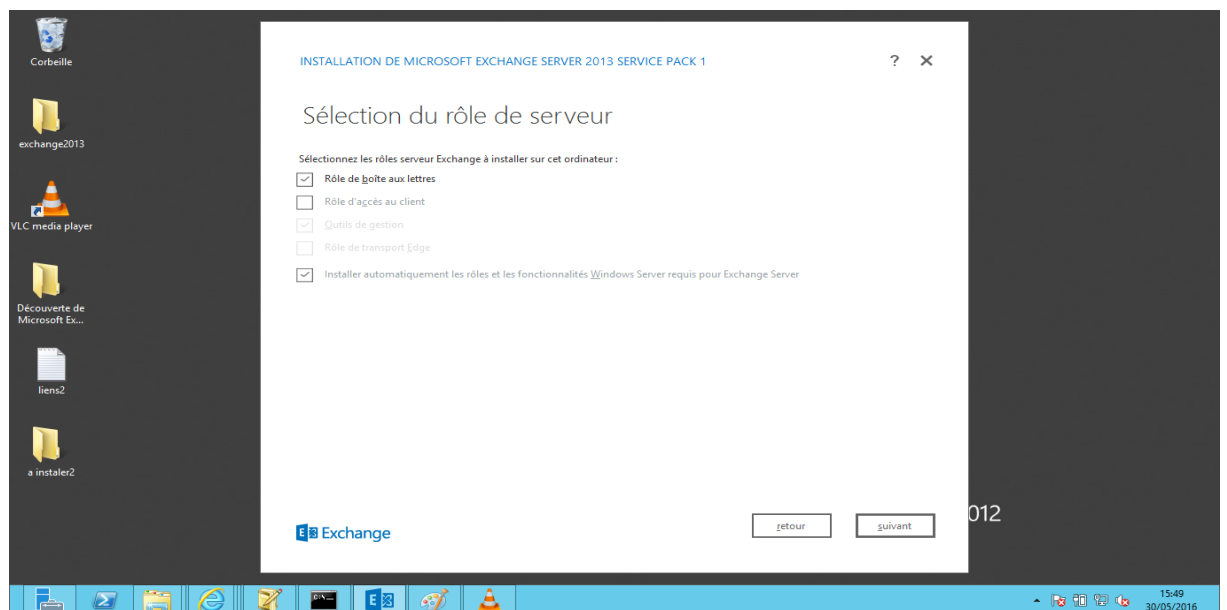


Figure 4.13: Installation du role boite au lettres

On arrive à la phase de tests qui vérifie les différents composants pour pouvoir lancer le setup et à la fin de ce test on clique sur " installer ".

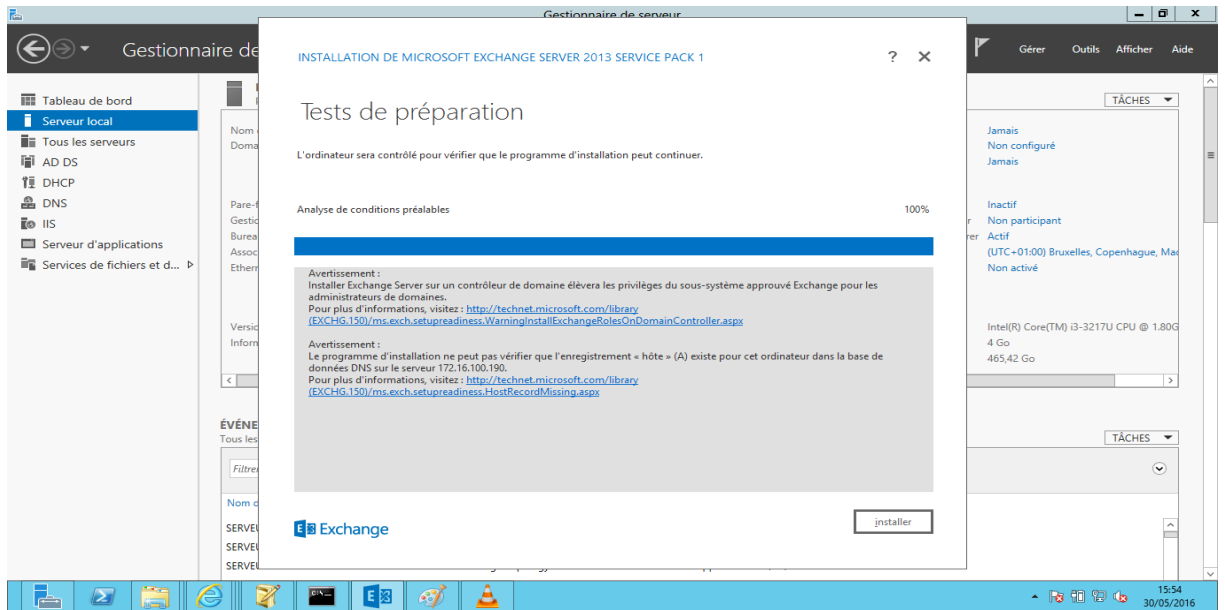


Figure 4.14: Lancement du setup.

Après avoir installé le rôle boîte au lettre on doit installer aussi le rôle accès client et cela on ré-exécutant les mêmes étapes en cochant le " rôle d'accès au client ".

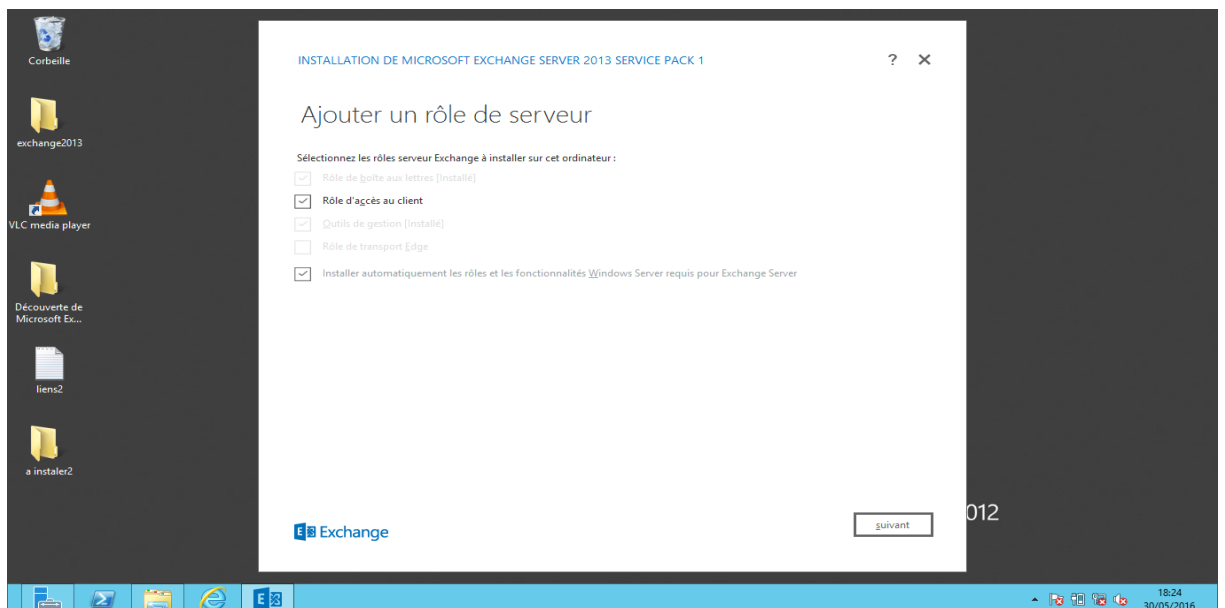


Figure 4.15: Installation du rôle d'accès client.

À la fin de l'installation nous devons redémarrer notre serveur.

4.4 Présentation des outils de l'administration

4.4.1 Exchange Management Shell

L'environnement de ligne de commande Exchange Management Shell, basé sur la technologie Windows PowerShell, fournit une interface de ligne de commande à Microsoft Exchange Server 2013 qui permet d'automatiser les tâches d'administration. Le Shell permet de gérer tous les aspects d'Exchange:

- Activer de nouveaux comptes de messagerie;
- Créer des connecteurs d'envoi et de réception;
- Configurer des propriétés de base de données;
- Gérer des groupes de distribution etc...

L'environnement Shell peut effectuer toutes les tâches que le centre d'administration (EAC) Exchange exécute, plus des actions impossibles à réaliser dans l'EAC.



```
Ordinateur : serveurEPB.portdebejaia.dz
Cmdlets Exchange uniquement : Get-ExCommand
Cmdlets correspondant à une chaîne spécifique : Aide *<string>*
Obtenir de l'aide générale : Aide
Obtenir de l'aide pour une cmdlet : Help <cmdlet name> ou <cmdlet name> -?
Blog de l'équipe Exchange : Get-ExBlog
Afficher la sortie complète pour une commande : <command> ! Format-List
Afficher le guide de référence rapide : QuickRef
Conseil du jour n°44 :
Vous voulez modifier le quota d'interdiction d'envoi par défaut pour une base de données de boîtes aux lettres ? Tapez :
Set-MailboxDatabase <Mailbox Database Name> -ProhibitSendQuota <New Quota Size>
Vous pouvez spécifier un qualificateur d'octets lorsque vous utilisez le paramètre ProhibitSendQuota. Par exemple, si vo
us voulez définir le quota d'interdiction d'envoi sur 200 mégaoctets, tapez :
Set-MailboxDatabase <Mailbox Database Name> ProhibitSendQuota 200MB
Vous pouvez également configurer les paramètres IssueWarningQuota et ProhibitSendReceiveQuota de la même manière.
COMMENTAIRES : Connexion à serveurEPB.portdebejaia.dz.
COMMENTAIRES : Connecté à serveurEPB.portdebejaia.dz.
[PS] C:\Windows\system32>
```

Figure 4.16: Exchange Management Shell.

4.4.2 Exchange Management Console (EMC)

Exchange management console est un outil basé sur Microsoft Management Console (MMC) 3.0, qui fournit aux administrateurs d'Exchange une interface utilisateur graphique pour gérer la configuration des organisations Exchange. Nous pouvons également ajouter le composant logiciel enfichable Console de gestion Exchange aux outils MMC personnalisés. [7]

4.4.3 Centre d'administration Exchange(CAE)

Le Centre d'Administration Exchange (CAE) est la console de gestion web qu'on utilise pour gérer les éléments liés à la messagerie qu'on ne peut pas gérer à l'aide du Centre d'administration Office 365. Le CAE remplace le Panneau de configuration Exchange (PCE), qui était l'interface de gestion de l'organisation Exchange dans les versions antérieures d'Exchange Online.

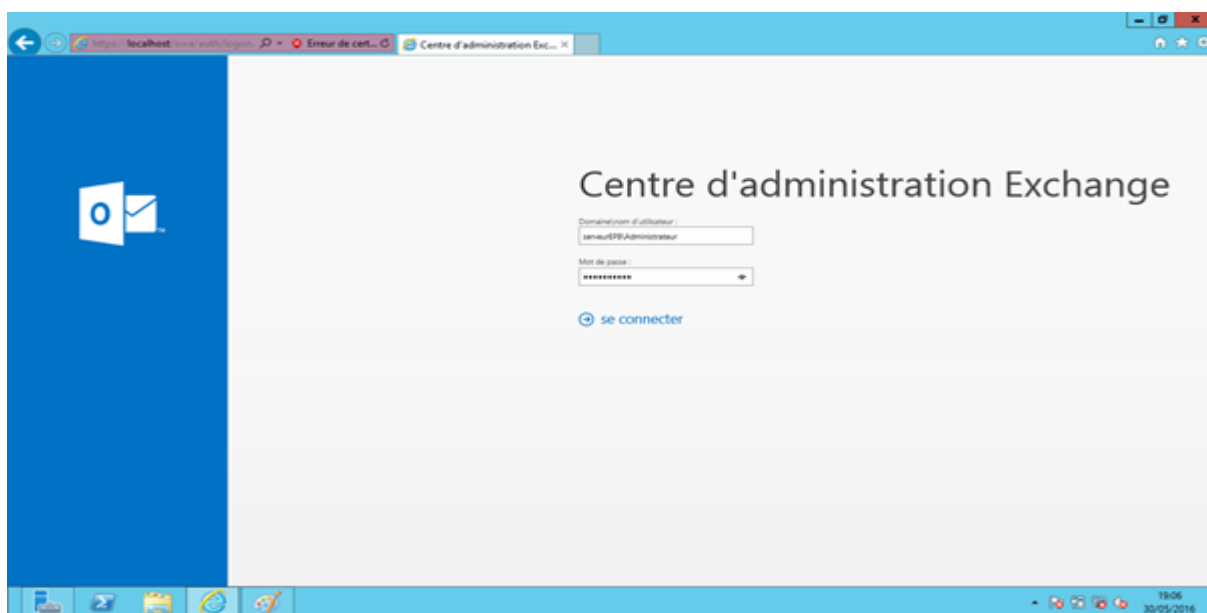


Figure 4.17: Centre d'administration Exchange.

4.5 Gestion des Accès Clients

4.5.1 Autodiscover (service de découverte automatique)

Le service de découverte automatique facilite la configuration d'Outlook et de certains téléphones mobiles. Il permet à Outlook de trouver de nouveaux points de

connexion constitués du GUID de boîte aux lettres de l'utilisateur + @ + la partie de domaine de l'adresse SMTP principale de l'utilisateur.

Le service de découverte automatique effectue ce qui suit:

- Configurer automatiquement des paramètres de profil utilisateur pour des clients qui exécutent MicrosoftOffice Outlook , ainsi que des téléphones mobiles pris en charge. Les téléphones qui exécutent Windows Mobile 6.1 ou une version ultérieure sont aussi pris en charge.
- Fournir un accès aux fonctionnalités d'Exchange à des clients Outlook qui sont connectés à un environnement de messagerie Exchange.
- Utiliser l'adresse de messagerie et le mot de passe d'un utilisateur pour fournir des paramètres de profil aux clients outlook ou aux appareils mobiles pris en charge. Si le client Outlook est connecté à un domaine, le compte de domaine de l'utilisateur est utilisé.

4.5.2 Exchange ActiveSync

Exchange ActiveSync est un protocole de synchronisation Microsoft Exchange optimisé pour fonctionner avec des réseaux à faible bande passante et latence élevée. Le protocole est basé sur HTTP et XML, il permet à des téléphones mobiles d'accéder aux informations d'une organisation sur un serveur exécutant Microsoft Exchange. Exchange ActiveSync permet aux utilisateurs de téléphones mobiles d'accéder à leurs messages électroniques, calendrier, contacts et tâches et de continuer à avoir accès à ces informations lorsqu'ils travaillent hors connexion.

4.5.3 Outlook Web App (OWA)

Outlook Web App est un web mail disponible automatiquement sur le rôle serveur d'accès client. Il permet aux utilisateurs d'accéder à leur boîte aux lettres depuis un navigateur Internet et depuis n'importe quelle machine. Les fonctionnalités présentées dans OWA sont identiques à celles se trouvant dans le client lourd Outlook. Elle permet aussi l'accès à des clients qui sont sur des plateformes non Windows (Linux, Mac OS).

4.6 Configuration d'échange server 2013

4.6.1 Acceptation des noms de domaines

Un domaine accepté est un espace de noms SMTP quel qu'il soit pour lequel une organisation Microsoft Exchange Server 2013 envoie ou reçoit du courrier électronique, il inclut les domaines pour lesquels l'organisation Exchange fait autorité. [7]

4.6.2 Configuration des domaines acceptés

Les domaines acceptés sont configurés en tant que paramètres globaux pour l'organisation Exchange. On doit configurer en tant que domaine accepté d'une organisation chacun des domaines pour lesquels elle relaie ou remet des messages. Il existe trois types de domaines acceptés : domaines faisant autorité, relais internes et relais externes. [7]

Dans notre cas nous avons choisi de configurer notre domaine comme " domaine faisant autorité "

4.6.3 Domaines faisant autorité

Une organisation peut avoir plusieurs domaines SMTP. Les domaines de messagerie d'une organisation sont les domaines faisant autorité. Dans Exchange 2013, un domaine accepté est considéré comme faisant autorité lorsque l'organisation Exchange héberge des boîtes aux lettres pour des destinataires dans ce domaine SMTP.

Par défaut, lorsque le premier serveur de boîtes aux lettres Exchange 2013 est installé, un domaine accepté est configuré comme faisant autorité pour l'organisation Exchange. Le domaine accepté par défaut est le nom de domaine complet de notre domaine racine de la forêt. Souvent, le nom de domaine interne diffère du nom de domaine externe, par exemple, notre nom de domaine interne est " epblocal.dz ", alors que notre nom de domaine externe est portdebejaia.dz. L'enregistrement du serveur de messagerie (MX) DNS fait référence à portdebejaia.dz qui est l'espace de noms SMTP que nous avons affecté aux utilisateurs lorsque nous allons créer une stratégie d'adresse de messagerie. [7]

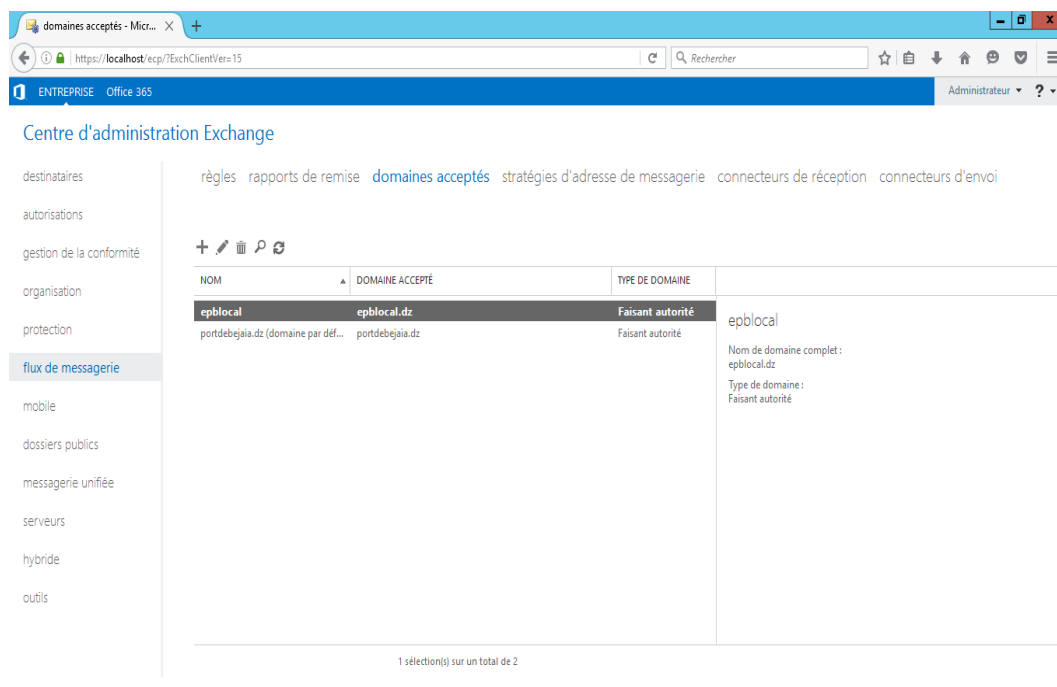


Figure 4.18: Domaines faisant autorité.

Une fois connecté à l'ECP (Exchange Control Panel), dans l'onglet " Flux de messagerie " puis " Domaines acceptés " enfin cliquer sur " Ajouter " (+), nous avons donné un nom convivial au domaine que nous ajoutons, ainsi que le nom de domaine en question (epblocal.dz), et enfin nous avons sélectionné l'option " Domaine faisant autorité "

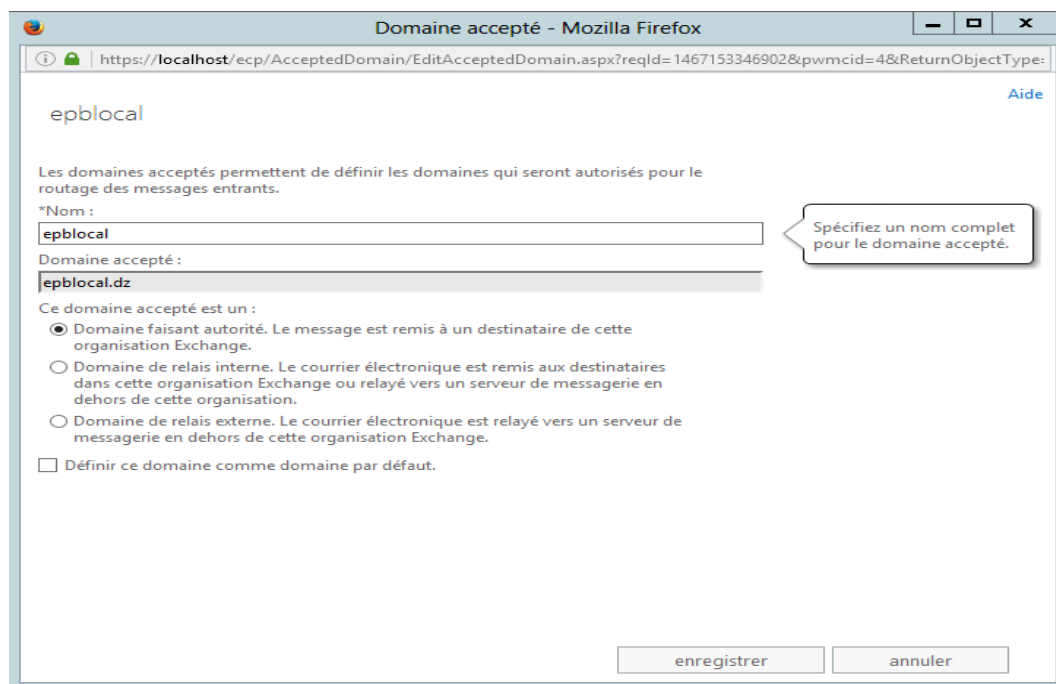


Figure 4.19: Configuration du domaine acceptés.

4.6.4 Stratégie d'adresse de messagerie

Les stratégies d'adresse de messagerie génèrent les adresses de messagerie principales et secondaires pour les destinataires, de façon à ce qu'ils puissent recevoir et envoyer des messages. Par défaut, Exchange contient une stratégie d'adresse de messagerie pour chaque utilisateur à extension messagerie. Cette stratégie par défaut spécifie l'alias du destinataire comme partie locale de l'adresse de messagerie et utilise le domaine accepté par défaut. La partie locale d'une adresse de messagerie correspond au nom qui apparaît devant le signe @. [7]

dans l'ECP, il suffit d'aller dans " Flux de messagerie" ensuite, "Stratégies d'adresse de messagerie " et de modifier la " Default Policy ". Ensuite, en allant dans l'onglet « Format de l'adresse de messagerie », nous pouvons créer toutes les adresses de messagerie de nos utilisateurs :

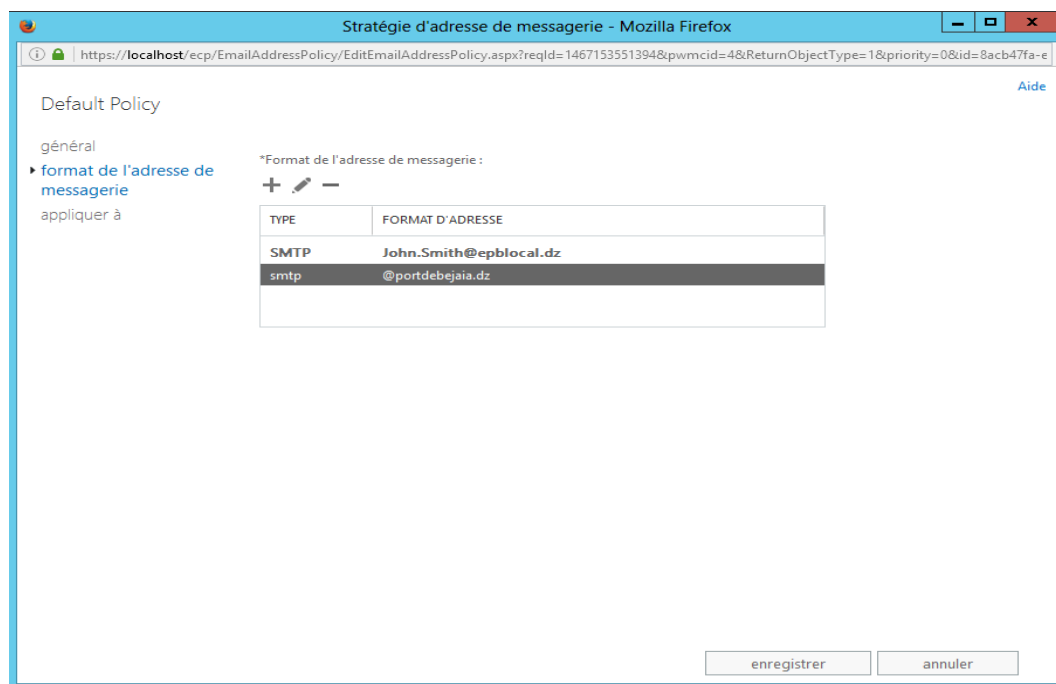


Figure 4.20: Format de l'adresse de messagerie.

Chaque utilisateur se verra attribuer 2 adresses :

- Initiale Prénom, Nom @epblocal.dz
- Initiale Prénom, Nom @portdebejaia.dz

L'adresse dont le SMTP est en majuscule correspond à l'adresse de réponse. Lorsque un utilisateur écrira un email, il sera adressé de la part de `nomprenom@epblocal.dz`, mais il peut recevoir du courrier sur `epblocal.dz` et `portdebejaia.dz` aussi.

4.6.5 Règles de transport

Les actions de règle de transport permettent d'appliquer des stratégies de messagerie aux messages électroniques circulant au sein de l'organisation.

4.6.5.1 Connecteurs d'envoi

Dans Microsoft Exchange Server 2013, un connecteur d'envoi contrôle le flux des messages sortants vers le serveur de réception. Ils sont configurés sur les serveurs de boîtes aux lettres exécutant le service de transport. Le plus souvent, nous configurons un connecteur d'envoi pour envoyer les messages électroniques sortants vers

un hôte actif ou directement vers leur destinataire, via DNS.

Nous avons créé un connecteur d'envoi nommé " envoi " prévu pour une utilisation "Internet " et qui sera autorisé à envoyer à tous les domaines SMTP. Il utilisera la résolution DNS pour l'envoi de mails et les DNS externes pour la résolution de noms des enregistrements MX.

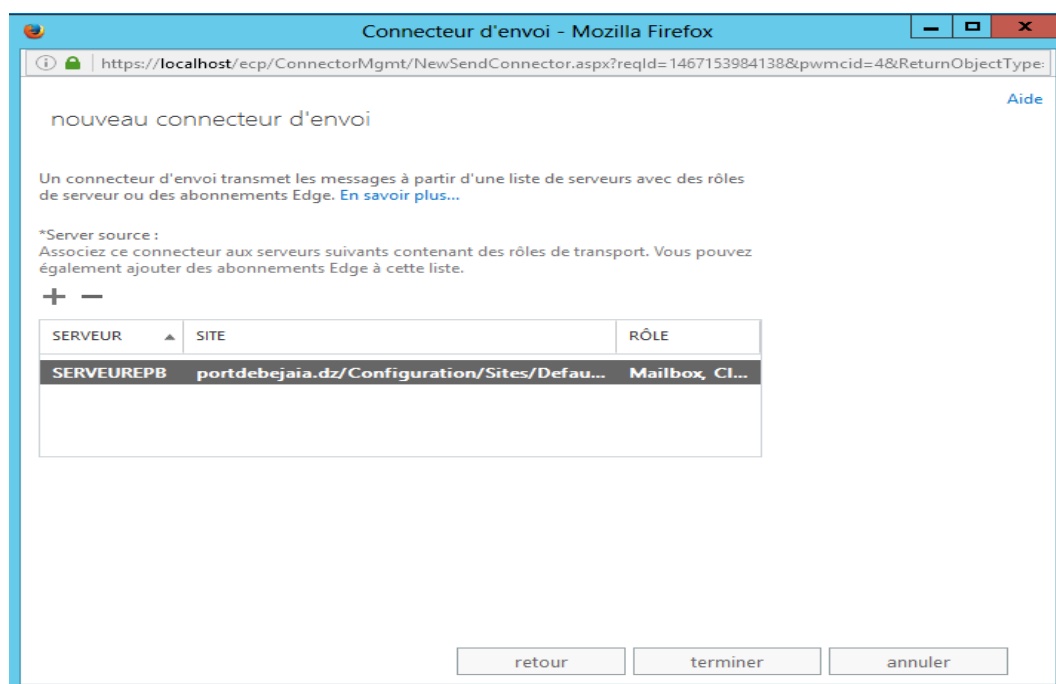


Figure 4.21: Ajout d'un connecteur d'envoi.

4.6.5.2 Connecteur de réception

Les connecteurs de réception contrôlent le flux de messages entrants à destination de l'organisation Exchange. Ils sont configurés sur des ordinateurs exécutant Microsoft Exchange Server 2013 avec le service de transport ou dans le service frontal d'un serveur d'accès au client. Ils peuvent être créés dans le Centre d'administration Exchange ou l'environnement de ligne de commande Exchange Management Shell. Dans la EAC, nous avons accédé au "Flux de messagerie" puis "Connecteurs de réception". Et cliquer sur "Ajouter" pour créer un connecteur de réception. Dans la page "Nouveau connecteur de réception", nous avons spécifié un nom pour le connecteur de réception (reception1), puis sélectionnez Transport hub pour le Rôle puisque il s'agit d'une messagerie interne .

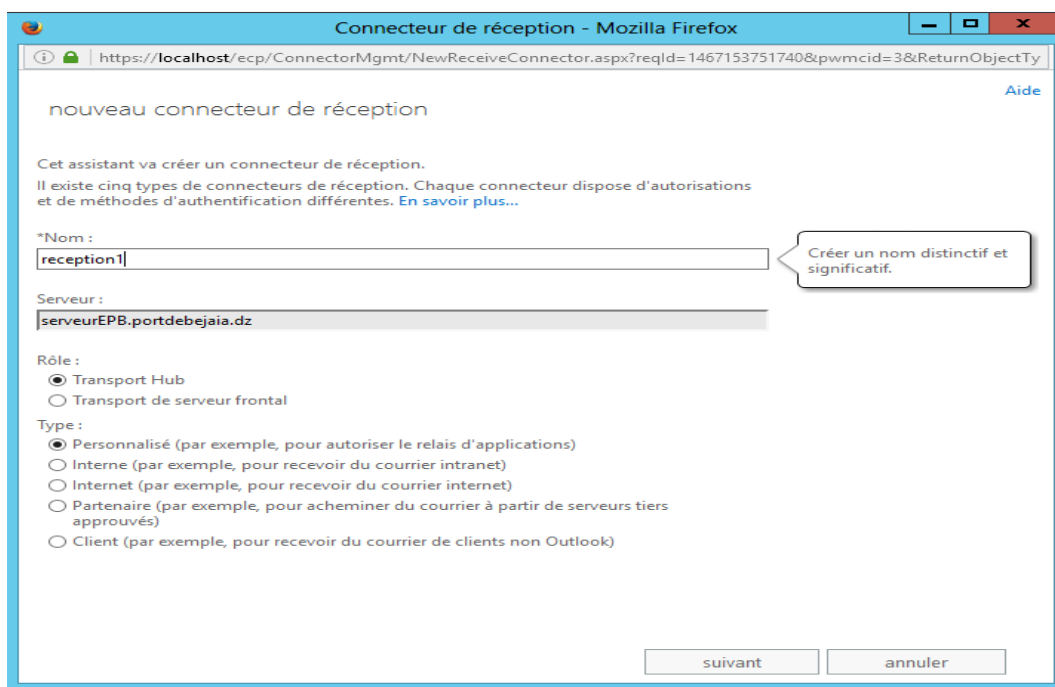


Figure 4.22: Ajout d'un connecteur de réception.

En ce qui concerne les "liaisons de cartes réseau", nous remarquons que l'option "Toutes les IPv4" disponibles se trouve dans la liste des "adresses IP" et que le Port est 25. (le protocole SMTP (Simple Mail Transfer Protocol) utilise le port 25.) Cela indique que le connecteur écoute les connexions sur toutes les adresses IP attribuées aux cartes réseau sur le serveur local.

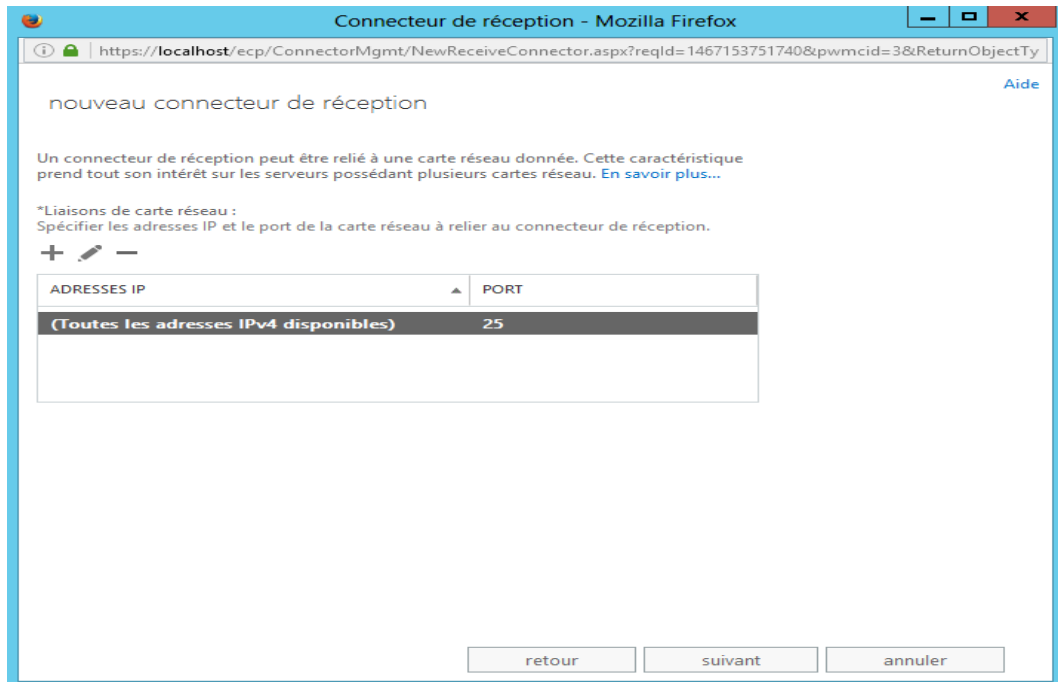


Figure 4.23: Relier un connecteur de réception a une carte réseau.

Enfin cliquer sur le bouton "Terminer" pour créer notre connecteur.

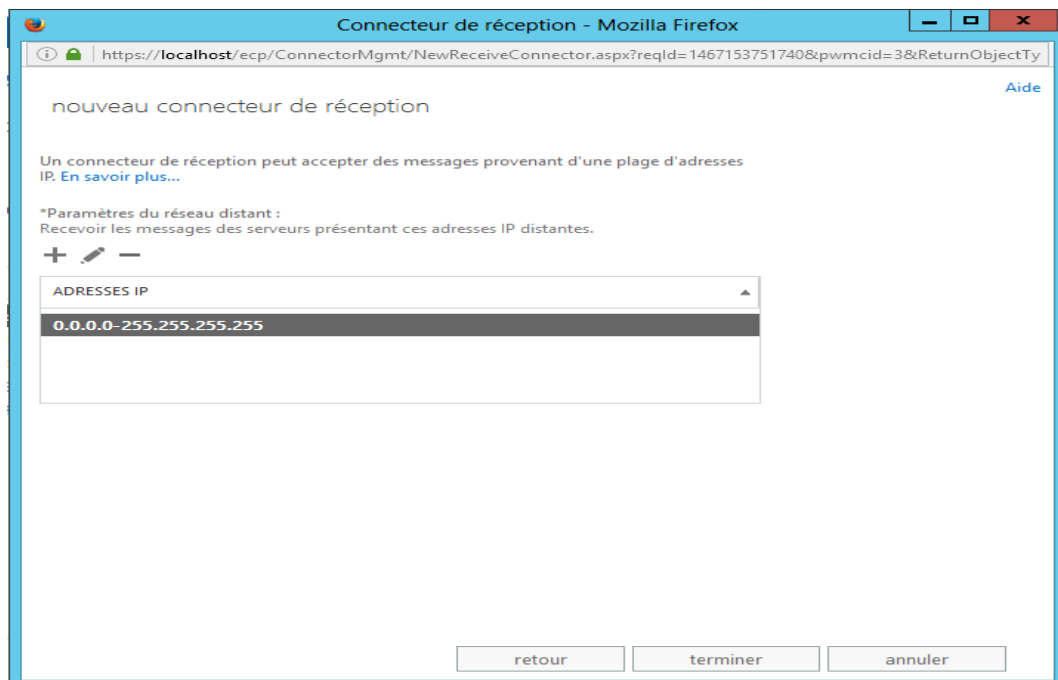


Figure 4.24: Configurer un connecteur de réception.

4.6.6 Création de boîtes aux lettres utilisateur

Les boîtes aux lettres sont le type de destinataire le plus courant utilisé par les professionnels de l'information dans une organisation Exchange. Chaque boîte aux lettres est associée à un compte d'utilisateur Active Directory. L'utilisateur peut se servir de la boîte aux lettres pour envoyer et recevoir des messages, ainsi que pour stocker des messages, des rendez-vous, des tâches, des notes et des documents. Depuis " l'ECP ", et dans "Destinataires puis Boîtes aux lettres " ensuite, " (+) " :

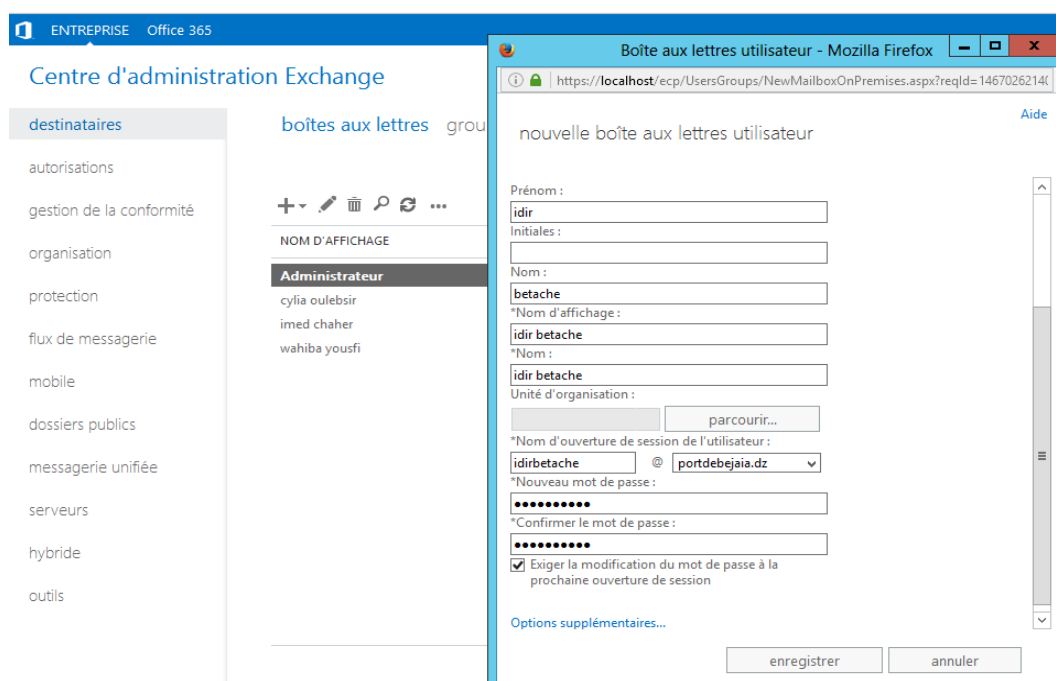


Figure 4.25: Création de boîtes aux lettres utilisateurs.

4.6.7 Configurer un certificat

Configurer des certificats numériques pour autoriser les utilisateurs à se connecter à Outlook web App (OWA) et Outlook anywhere, c'est-à-dire fonction RPC sur HTTPS pour ce faire on pourra utiliser des certificats pour nous gérer nous même dans notre entreprise avec notre propre autorité de certifications. Donc nous avons créer nous meme un certificat. Ici nous avons choisis de créer un certificat auto-signé qu'on a nommé "cer1"

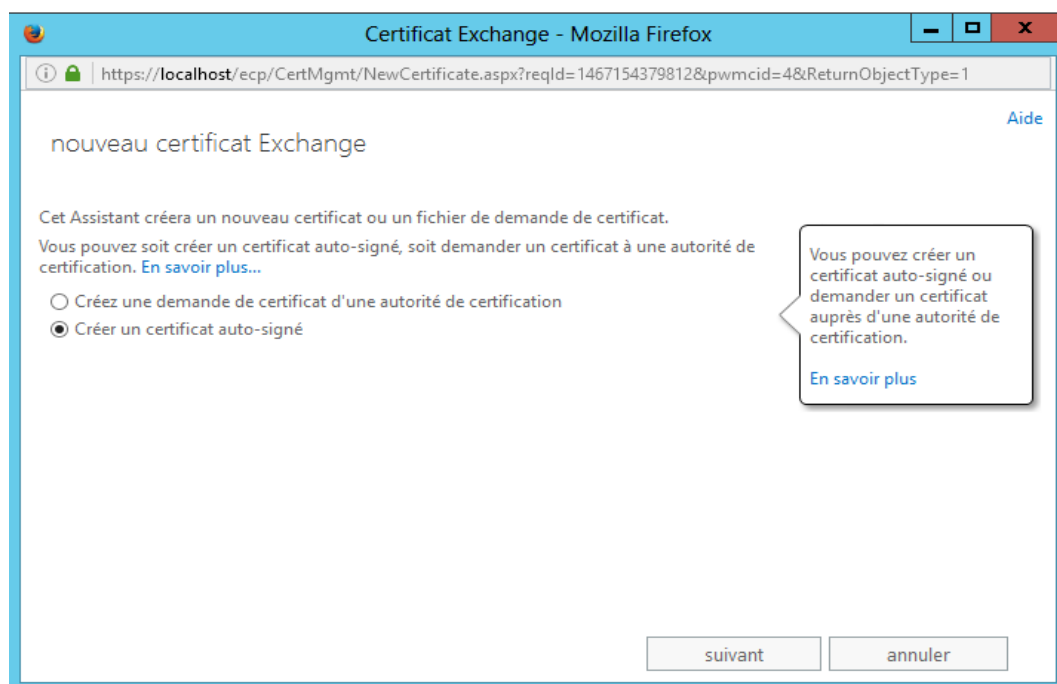


Figure 4.26: Création d'un certificat auto-signé.

Nous avons obtenu un certificat valide après avoir spécifier le serveur auquel appliquer ce certificat et les domaines qui seront inclus dans ce certificat.

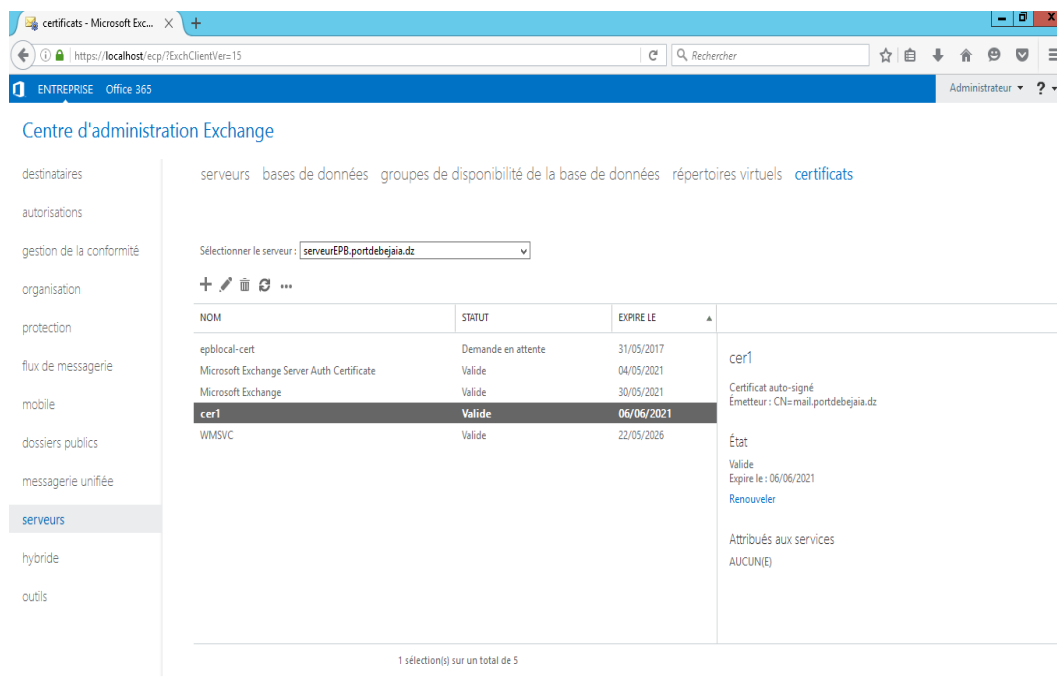


Figure 4.27: Obtention d'un certificat auto-signé.

4.7 Conclusion

Nous avons vu dans ce chapitre que la mise en place d'un système de messagerie à base de Microsoft Exchange 2013 est un projet qui nécessite d'être préparé et planifié avant toute mise en oeuvre, comme nous avons vu aussi les tâches nécessaires pour configurer correctement l'infrastructure Exchange 2013 mais aussi celles correspondant à son administration après sa mise en production afin d'avoir une organisation opérationnelle.

Conclusion Générale

Au cours des deux dernières décennies, la messagerie électronique s'est imposée comme un moyen de communication de prédilection dans les milieux professionnels grâce aux nombreux avantages qu'elle présente. Cependant, elle ne cesse d'évoluer pour s'adapter aux besoins croissants des utilisateurs pour devenir aujourd'hui, beaucoup plus qu'un outil d'échange de mails, une solution pratique et efficace pour le travail collaboratif augmentant ainsi sa rentabilité. La place prépondérante qu'occupe aujourd'hui la messagerie électronique fait que les enjeux auxquels elle doit répondre se multiplient et se diversifient. Nous citons à titre d'exemple la mobilité des utilisateurs, la sécurité du système et des échanges, la conformité aux différentes règles en usage ou encore la disponibilité des informations. De plus, les exigences liées au coût de la mise en oeuvre et la maintenance d'une solution, sa fiabilité et son évolutivité ne peuvent être ignorées.

Dans ce contexte, le travail que nous avons réalisé consiste à faire une étude descriptive et analytique d'une solution de messagerie des plus utilisées dans les entreprises qui est Microsoft Exchange Server 2013.

Notre objectif était d'étudier d'abord les aspects théoriques qui entourent un environnement de messagerie comme les protocoles utilisés, l'architecture logicielle, etc. et de maîtriser les différents concepts techniques liés au déploiement d'un système de messagerie MS Exchange Server 2013 ; et analyser ensuite les rôles et les applications de cette solution pour en étudier l'utilisation et les mécanismes de fonctionnement.

Afin d'aboutir à cet objectif, nous avons dans un premier temps passé en revue les généralités et les notions théoriques relatives à la messagerie électronique ainsi qu'au service d'annuaire Active Directory, fondamental pour le fonctionnement de la solution choisie.

Puis nous avons mis en oeuvre la solution choisie sur un environnement de simulation composée de machines et nous avons réalisé toutes les tâches nécessaires à sa configuration pour ensuite explorer les fonctions d'administration et de configuration d'une infrastructure de messagerie à base d'Exchange Server.

Finalement, nous nous sommes intéressés de plus près à un aspect très important dans tout système informatique et dans un système de messagerie en particulier qui est celui de sa disponibilité en étudiant les mécanismes de sauvegarde et de restauration ainsi que l'installation en cluster du serveur de messagerie. Par ailleurs, les perspectives dégagées pour ce travail sont :

- Etudier de près le rôle de Messagerie Unifiée pour mettre en oeuvre une convergence des types data et voix des communications dans une organisation.

Bibliography

- [1] LOHIER.S et QUIDELLEUR.A. Le réseau internet. 2010.
- [2] N. Salmi A.Abdelli. Réseaux et télétraitements. 2012.
- [3] Notions de base sur les réseaux, ccna exploration.
- [4] CLUB DE LA SECURITE DES SYSTEMES D'INFORMATION FRANÇAIS.
Securite de la messagerie.
- [5] Laurent Fabrice. la mise en place et la sécurisation d'un système de messagerie électronique.
- [6] William R.Stanek. Guide de l'administration windows server 2012. 2013.
- [7] <https://technet.microsoft.com>.

Résumé

La messagerie électronique est l'application la plus importante pour les organisations. Elle est le mécanisme de transport de fichiers principal utilisé par la plupart des organisations.

La messagerie électronique est de plus en plus utilisée comme espace de stockage d'informations critiques pour l'entreprise. Quatre entreprises sur cinq utilisent la messagerie électronique pour mener des transactions commerciales (envoi de contrats, commandes fournisseur, etc...).

Ce mémoire est le résultat d'une étude descriptive et analytique de l'une des principales solutions de messagerie existante aujourd'hui sur le marché mondial des TICs, en l'occurrence MS Exchange Server.

Notre projet consiste à mettre en oeuvre un système de messagerie à base d'Exchange Server 2013 sur un labo de test constituée de machines (serveur et clientes) afin de maîtriser le côté technique de son déploiement ; puis à l'exploration, sur l'environnement de simulation, des différents mécanismes et fonctionnalités offerts par cette solution afin d'en étudier l'utilisation et le fonctionnement.

Mots clés: Serveur Exchange, Serveur de messagerie, Messagerie électronique, Active Directory.

Abstract

Email is the most important application for organizations. E-mail is the primary file transport mechanism used by most organizations.

Email is the most important application for organizations. E-mail is the primary file transport mechanism used by most organizations. It is increasingly used as a storage of critical information to the company. Four out of five companies use email to conduct business transactions (sending contracts, purchase orders, etc...). Par ailleurs, les perspectives dégagées pour ce travail sont :

This memory is the result of a descriptive and analytical study of a major existing messaging solutions today on the global market for ICT in the MS Exchange Server instance. Our project is to implement a messaging system based on Exchange Server 2013 on a test lab is machine (server and client) to master the technical side of their deployment; then the exploration of the simulation environment, different mechanisms and functions provided by this solution in order to study the use and operation.

Keys Word: Exchange Server, Mail server, Email, Active Directory.