UNIVERSITÉ NAZI BONI

ÉCOLE SUPÉRIEURE D'INFORMATIQUE

PROJET DE FIN DU MODULE D'ADMINISTRATION DES RÉSEAUX

THÊME : MISE EN PLACE D'UN SERVICE DE MESSAGERIE

PROFESSEUR : M. PATRICE KAFANDO

MENBRES DU GROUPE :

BITIBALY Clément Alex

HIEN Nifabobio

NEBIE Aminata

TRAORE Siaka

INTRODUCTION

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. C'est dans ce cadre que ce thème : Mise en place d'un service de messagerie nous a été confié.

I. Eléments de la Messagerie Electronique

La messagerie est effective entre interlocuteurs c'est-à-dire des utilisateurs désirant communiquer entre eux. De ce fait, deux concepts clés constituent les éléments principaux de la messagerie :

Le serveur de messagerie Et le client de messagerie.

I.1. Le Serveur de messagerie

Un serveur de messagerie électronique est un logiciel serveur de courrier électronique. Il a pour vocation de transférer les messages électroniques d'un serveur à un autre. Un utilisateur n'est jamais en contact direct avec ce serveur mais utilise soit un client de messagerie, soit un courrielleur web, qui se charge de contacter le serveur pour envoyer ou recevoir les messages.

Comme exemple de serveur de messagerie nous avons :

- Sendmail : Est un serveur de messagerie dont le code source est ouvert. Il se charge de la livraison des messages électroniques.

- MailEnable : MailEnable est une solution de messagerie puissante, évolutive et rentable pour Microsoft Windows NT 4, 2000, XP ou supérieur. MailEnable est conçu pour fournir un message système basé sur la simplicité, la fiabilité et l'évolutivité plutôt que sur des fonctionnalités souvent inutilisées.

  MailEnable fournit également un environnement très extensible et favorise le développement via des bibliothèques COM, des DLL et des fichiers de configuration. Son architecture par composants favorise la personnalisation et le développement, ce qui en fait une solution parfaite en cas de besoin d'intégrer des systèmes existants.

  MailEnable facilite l'hébergement du système de messagerie et peut être utilisé par les FAI à la recherche d'une solution de messagerie bon marché/gratuite sur la plate-forme Windows. Sans licences d'accès client, avec des composants de base gratuits et une mise en œuvre rapide, c'est la solution de messagerie idéale.

- HmailServer : HmailServer est un serveur de messagerie électronique gratuit, open source pour Microsoft Windows. Il est utilisé par les fournisseurs de services Internet, les entreprises, les gouvernements, les écoles et les passionnés dans toutes les régions du monde.

  Il prend en charge les protocoles communs de courrier électronique (IMAP, SMTP et POP3) et peut facilement être intégré à de nombreux systèmes de courrier Web existants. Il dispose d'une protection contre le

spam basée sur le score flexible et peut s'attacher à votre scanner de virus pour analyser tous les courriels entrants et sortants.

I.2. Le Client de messagerie

Un client de messagerie est un logiciel qui sert à lire et envoyer des courriers électroniques. Ce sont en général des clients lourds mais il existe aussi des applications Web (les webmails) qui offrent les mêmes fonctionnalités.

2.1 Les clients lourds

Les clients lourds sont des logiciels qui permettent de lire, d'écrire et d'expédier des courriers électroniques. Ils s'installent sur des postes clients qui se connectent au serveur de messagerie. Les clients lourds ont l'avantage de récupérer nos messages et de les copier sur nos postes locaux, en mode connecté au serveur. Ainsi en mode hors connexion, nous avons accès à nos messages.

Quelques exemples de clients lourds :

a. Thunderbird de Mozilla

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

b. Zimbra Desktop :

- Multi plateforme (Windows, Mac OS, Linux).
- Codes sources libres.
- Regroupe tous les comptes dans un seul répertoire.

- Installation et configuration rapide et facile.
- Transfert des messages avec des pièces jointes.
- Extensible.

2.2. Les clients légers

Des clients de messagerie de type léger sont des logiciels qui sont installés sur des postes clients, permettent de se connecter au serveur de messagerie via un navigateur web. Ils fonctionnent uniquement en mode connecté et ne copie pas en local les messages stockés sur le serveur. Ainsi, en mode hors connexion nous n'avons plus accès à nos courriers.

a. Outlook Web Access :

Outlook Web App est basée sur le Web du client de messagerie de Microsoft Exchange Server 2010. Anciennement connu sous Outlook Web Access dans les itérations précédentes de Exchange Server, Outlook Web App permet aux utilisateurs une expérience similaire à Microsoft Outlook sans nécessiter la présence du client de messagerie complète. Il se caractérise par :

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

b. Web Mail Ajax de Zimbra :

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

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

- Permet les messages instantanés.

I.3. Les agents de messagerie

3.1. Le Mail Transfert Agent (MTA)

Le MTA est un programme qui permet d'envoyer le message d'un serveur à un autre. Ce logiciel est situé sur chaque serveur de messagerie. Il est composé d'un agent de routage et d'un agent de transmission. Il envoie le message via un protocole sortant. Notons que les protocoles sortants permettent de gérer la transmission du courrier entre les systèmes de messagerie. Le protocole sortant généralement utilisé est Simple Mail Transfert Protocol (SMTP)

3.2. Le Mail User Agent (MUA)

Le MUA sert pour l'expéditeur et le destinataire, est un logiciel client pour le MTA. Il formate les messages en partance afin de les donner au MTA, est un client pour le MDA il formate les messages de la boîte aux lettres afin de les afficher à l'écran.

3.3. Le Mail Delivery Agent (MDA)

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

I.4. Les protocoles de la messagerie

4.1. SMTP (Simple Mail Transfert Protocol)

Le protocole SMTP est un protocole standard permettant de transférer le courrier d'un serveur à un autre en connexion point à point. Il s'agit d'un protocole fonctionnant en mode connecté, encapsulé dans une trame TCP/IP. Le courrier est remis directement au serveur de courrier du destinataire. Le protocole SMTP fonctionne grâce à des commandes textuelles envoyées au

serveur SMTP (par défaut sur le port25). Chacune des commandes envoyées par le client est suivi d'une réponse du serveur SMTP composée d'un numéro et d'un message descriptif.

4.2. POP (Poste Office Protocol)

Le protocole POP permet comme son nom l'indique d'aller récupérer son courrier sur un serveur distant (le serveur POP). Il est nécessaire pour les personnes n'étant pas connectées en permanence à Internet afin de pouvoir consulter les mails reçus hors connexion. Il existe deux principales versions de ce protocole, POP2 et POP3, auxquels sont affectés respectivement les ports 109 et 110 et fonctionnant à l'aide de commandes textuelles radicalement différentes tout comme dans le cas du protocole SMTP.

4.3. IMAP (Internet Mail Access Protocol)

Le protocole IMAP (Internet Message Access Protocol) est un protocole alternatif au protocole POP3 mais offrant beaucoup plus de possibilités :

- Permet de gérer plusieurs accès simultanés.
- Permet de gérer plusieurs boîtes aux lettres.
- Permet de trier le courrier selon plus de critères

I.5. Le principe de fonctionnement d'une messagerie électronique

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

1. L'expéditeur communique son courriel via le MUA.
2. Le MUA transmet ce courriel au MTA (la plupart des MUA intègre des clients SMTP).
3. Le MTA du système de l'émetteur établit un canal de transmission avec le MTA du système du destinataire, par émissions successives de requêtes bidirectionnelles.
4. Une fois le canal établit, le courriel est transmis d'un système à un autre par les MTA.

5. Dans le système du destinataire, Le MTA transmet le courrier reçu au serveur IMAP ou POP3.

6. Le MDA récupère le courriel du serveur IMAP / POP 3, et le met à disposition du MUA.

7. Le MUA dépose le courriel dans les boîtes aux lettres du destinataire qui pourra le consulter à tout moment, sur authentification.

I.6. La sécurité de la messagerie

6.1. Menaces et risques

Comme tout système informatique, la messagerie se trouve face à des risques et menaces qui touchent à l'intégrité et la confidentialité des données et tout autre risque, parmi ces risques :

6.1.1. Les atteintes aux flux identifiés par l'entreprise

• Perte d'un e-mail : Soit au cours de sa transmission ou bien à l'arrivé.

• Perte de confidentialité : Se fait par une divulgation accidentelle ou par négligence provoqué par l'émetteur, en envoyant des données et des fichiers sans s'assurer de l'identité des destinataires, ou par un espionnage de message lors de la transmission.

• Perte d'intégrité : Un message peut être altéré, accidentellement ou par malveillance pendant sa transmission ou son stockage.

• Usurpation de l'identité de l'émetteur : Un utilisateur peut prendre l'identité d'un autre en lui volant son mot de passe et son nom d'utilisateur par exemple.

6.1.2. Les atteintes à l'infrastructure et au système d'information

• Programme malveillants : La messagerie permet d'introduire des fichiers dans un ordinateur qui peuvent être malveillants comme l'introduction d'un virus par le biais d'une pièce jointe ou bien par un code malicieux dans le corps

même du message et aussi les faux virus (hoax) qui propagent de fausses informations.

• Spam : Elle consiste à inonder les boites aux lettres de courriers indésirables et non sollicités, il est aussi utilisé pour diffuser les faux virus.

6.2. Solution de sécurité

6.2.1. Sécurisation des flux légitimes

• Chiffrement et signature électronique des messages : La cryptographie permet d'apporter des réponses efficaces aux problématiques de sécurisation des flux légitimes. Elle permet d'assurer la confidentialité, l'intégrité des messages et l'authentification de l'émetteur.

• La sécurisation des protocoles : Permet de sécuriser les communications entre les MTA et entre le serveur et le client de messagerie, parmi ces protocoles :

– SSL (Secure Socket Layer) qui est développé pour permettre de la communication sécurisée en mode client/serveur pour des applications réseaux utilisant TCP/IP.

– Le protocole TLS (Transport Layer Security) est une évolution de SSL réalisé par l'IETF et qui sert de base à HTTPS par exemple.

6.2.2. Sécurisation des infrastructures

Le filtrage et analyse de contenu se fait par la protection contre les virus et les spam.

• Protection contre les virus : Pour qu'elle soit efficace, doit vérifier les points suivants :

– Le filtrage des e-mails sur les deux niveaux dès leur entrée sur le réseau. – Utilisation de plusieurs antivirus.

– La procédure d'alerte paramétrable.

• Protection contre les spam : Les techniques principales sont :

– L’analyse lexicale et la mise en place d’une liste noire et l’autre blanche.

– L’utilisation de RBLs (Realtime Blackhole List) pour les adresses ou de relais SMTP

I. INSTALLATION ET CONFIGURATION

Pour le déploiement de ce serveur de messagerie nous utiliserons le serveur de messagerie MailEnable, et les clients Thunderbird et Outlook.

Le déploiement de ces services a besoins de serveurs prérequis : les serveurs DHCP et DNS.

II.1. Active Directory

Active Directory sert d’annuaire des objets du réseau, il permet aux utilisateurs de localiser, de gérer et d’utiliser facilement les ressources. Il permet de réaliser la gestion des objets sans liens avec la disposition réelle ou les protocoles réseaux employés. Active Directory organise l’annuaire en sections, ce qui permet de suivre le développement d’une société allant de quelques objets à des millions d’objets. Combiné aux stratégies de groupes, Active Directory permet une gestion des postes distants de façon complètement centralisée.

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, etc. Pour installer Active Directory et DHCP, nous suivons les étapes ci-dessous :

* Cliquer sur le bouton Gérer de l’interface de gestionnaire de serveur Windows Server.

* Cliquer sur Ajouter des rôles et fonctionnalités.

* Cocher les deux rôles Active Directory et DHCP.

* Cliquer sur suivant. Concernant le DNS il sera installé automatiquement avec le rôle Active Directory.

La figure suivante représente Active Directory et DHCP en cours d'installation :

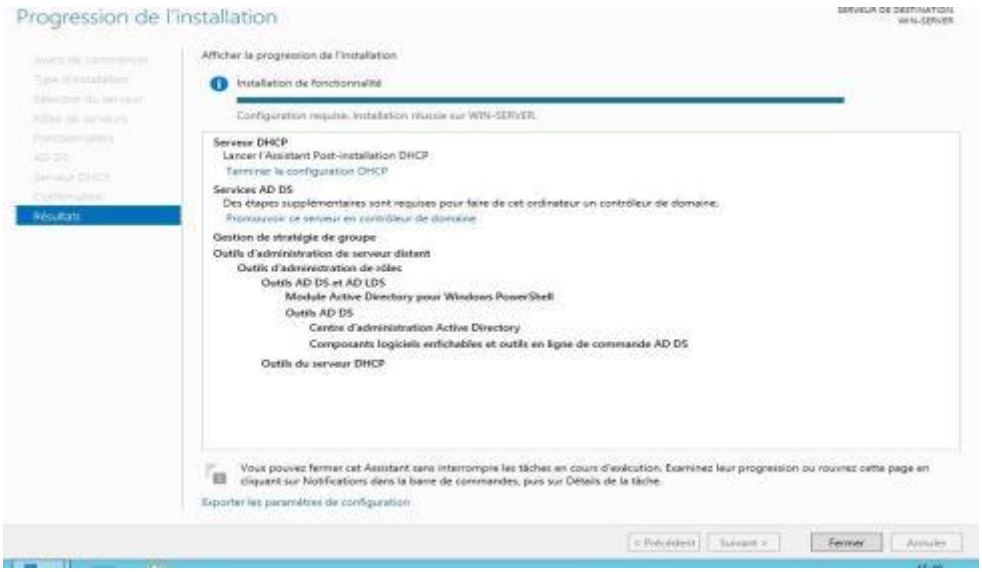


Figure1 : Installation d'Active Directory et DHCP

Après avoir installé Active Directory, le message suivant est affiché : « configuration requise pour Services AD DS à win-server», nous avons cliqué sur Promouvoir ce serveur en contrôleur de domaine pour créer un nouveau nom de domaine, nous l'avons nommé « portdebejaia.dz », et sécurisé avec un mot de passe.

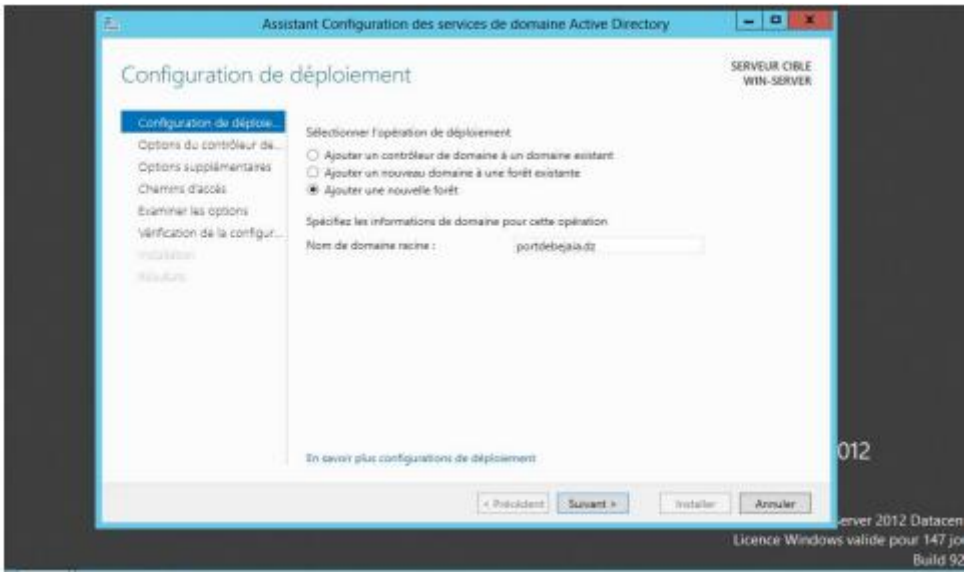


Figure 2 : Ajout d'une nouvelle forêt

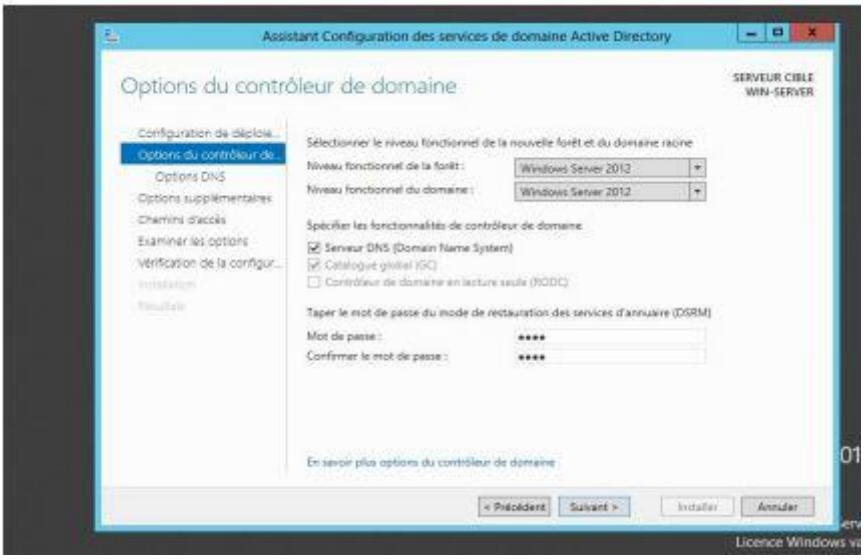


Figure 3 : Option du contrôleur de domaine

II.2. Serveur DNS

DNS (Domaine Name Server) est un serveur permettant d'assurer la correspondance entre un nom de domaine qualifié (FQDN : Fully Qualified Domain Name) et une adresse IP par exemple www.portdebejaia.dz = 128.65.195.18. Ainsi, grâce à DNS, il n'est pas nécessaire de se souvenir des adresses IP. Ce protocole sera utilisé par le Serveur de messagerie. La figure suivante représente le fonctionnement du serveur DNS où un client utilisant l'hôte A saisi le nom de domaine « www.nomDomaine.dz », une requête sera envoyée en lui disant au serveur DNS donnez-moi l'adresse IP du nom de domaine correspondant. Le serveur repend en lui attribuant l'adresse IP 128.65.195.18. L'autre méthode est l'inverse de la première, dans ce cas le client saisi l'adresse IP 128.65.195.18 et le serveur DNS repend en lui envoyant le nom de domaine correspondant à cette adresse IP.

Sa configuration suit la même étape que le DHCP, seulement cette fois ci au lieu de cliquer sur DHCP après avoir cliqué sur outils, nous sélectionnons sur DNS, puis clic droit sur zone de recherche inversé puis puis nouvelle zone.

Une autre fenêtre apparaîtra comme le montre la figure suivante :

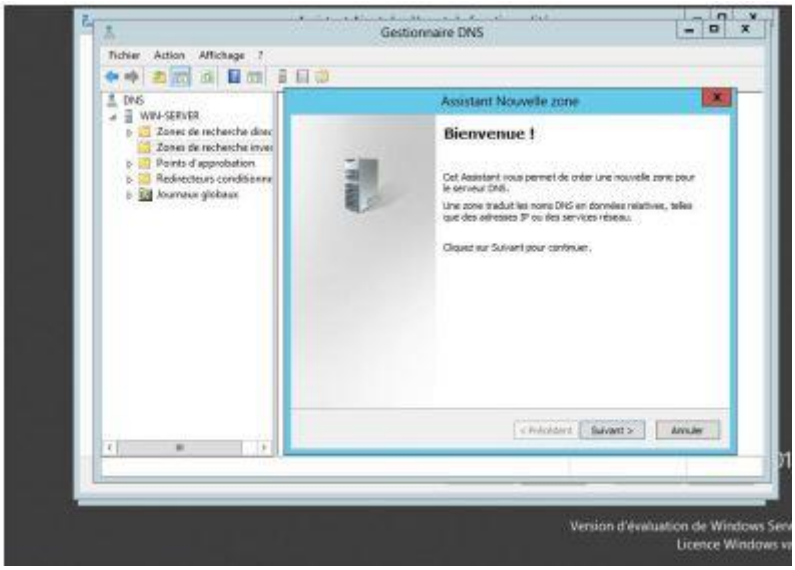


Figure 6 : Création d'une zone de recherche inversée

Après cela, nous cliquons sur suivant puis nous saisissons l'adresse DNS de notre nom de domaine « nomDomaine.dz ».

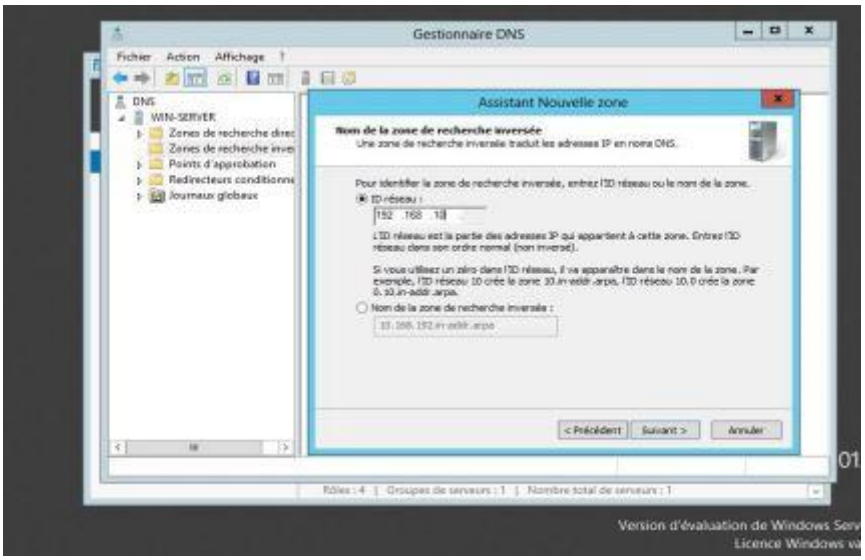


Figure 7 : Saisis de l'identifiant réseau

Une fois terminé de créer une nouvelle zone inversée, cette option authentifie les requêtes DNS en résolvant des adresses IP en nom de domaine ou hôte. La zone de recherche directe résolve les noms de domaine en adresse IP, cette option a été configuré automatiquement après avoir installé active Directory.

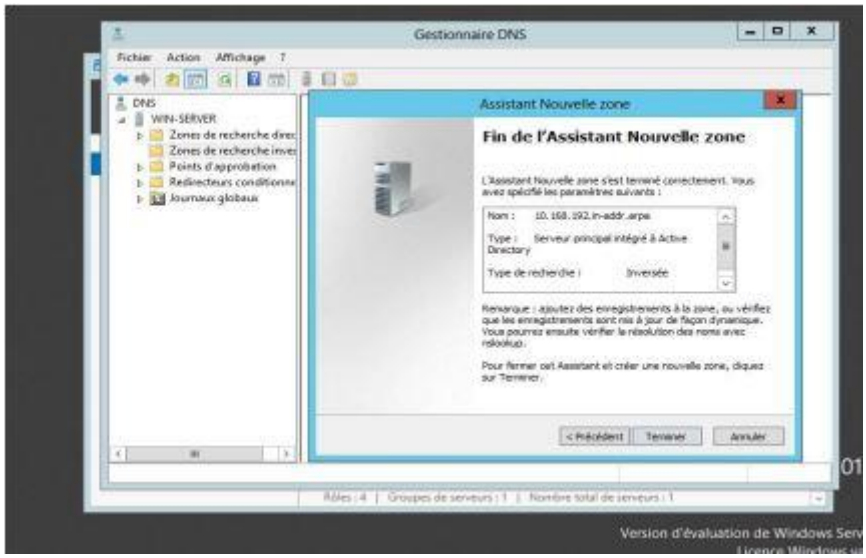


Figure 8 : Fin de création d'une zone de recherche inversée

Puis nous allons créer un enregistrement MX. Pour le faire, nous allons d'abord ajouter un nouvel hôte « mail » après un clic droit sur le dossier « nomDomaine.dz » puis sur ajouter un nouvel hôte après nous lui attribuons une adresse IP qui correspond à notre nom de domaine comme le montre la figure ci-dessous :

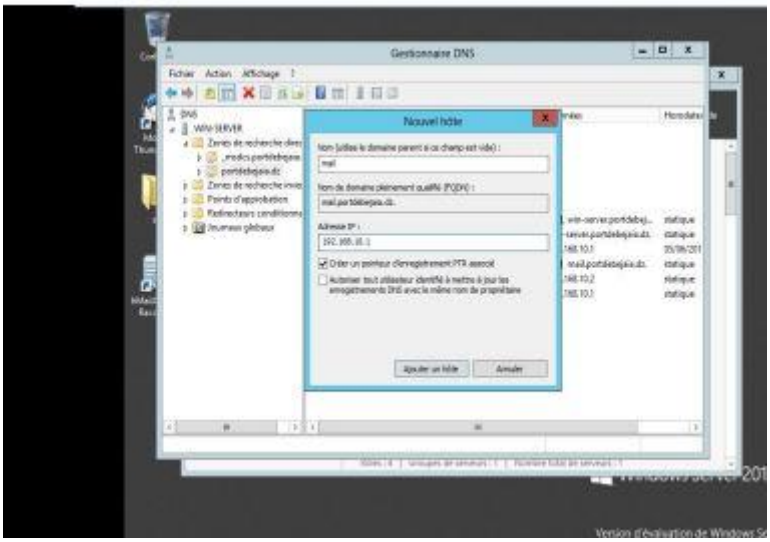


Figure 9 : Création d'un nouvel hôte

Une fois l'hôte créé nous passons à l'enregistrement MX toujours en effectuant un clic droit sur le dossier « nomDomaine.dz » puis sur nouveau serveur de messagerie MX. Après cela nous saisissons le nom de domaine complet « mail. nomDomaine.dz » comme le montre la figure ci-dessous :

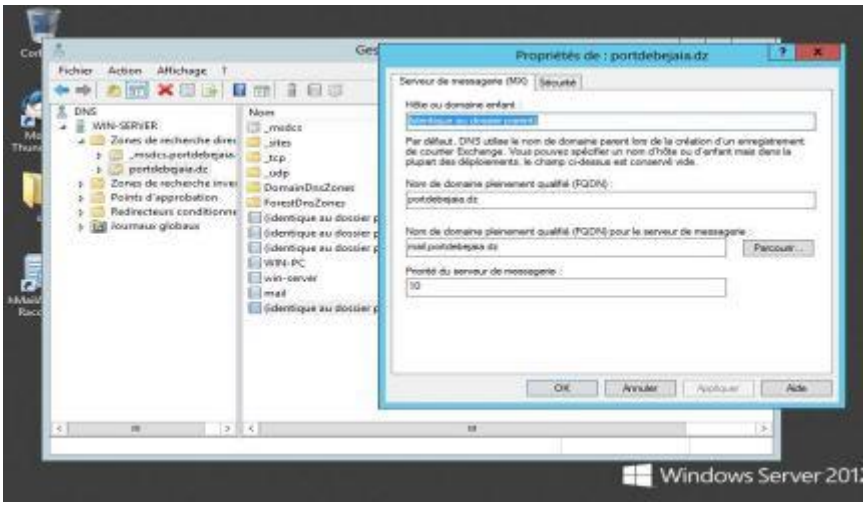


Figure 10 : Création d'un enregistrement MX

Ces enregistrements permettent de déterminer vers quel serveur un courrier électronique doit être acheminé lorsque le protocole SMTP est utilisé.

II.3. Serveur DHCP

Domaine Host Transfert Protocole

Après avoir configuré Active Directory et créé un nom de domaine, nous passons à la définition des paramètres du serveur DHCP en cliquant sur outils de l'interface gestionnaire de serveur puis DHCP. Une fenêtre apparaîtra comme le montre la figure ci-dessous :

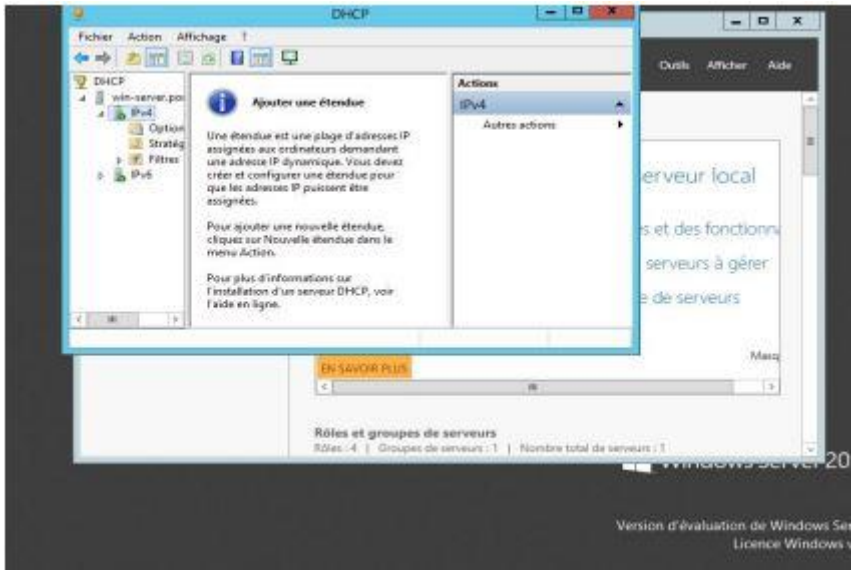


Figure 4 : Configuration de serveur DHCP

Après cela nous cliquons sur ajouter une étendue puis une nouvelle fenêtre apparaîtra comme le montre la figure suivante où nous avons saisi l'intervalle des adresses IPv4 avec une adresse de début et de fin, cet intervalle sera utilisé par le serveur DHCP en prenant une adresse de manière aléatoire puis la distribuer aux clients et administrateurs.

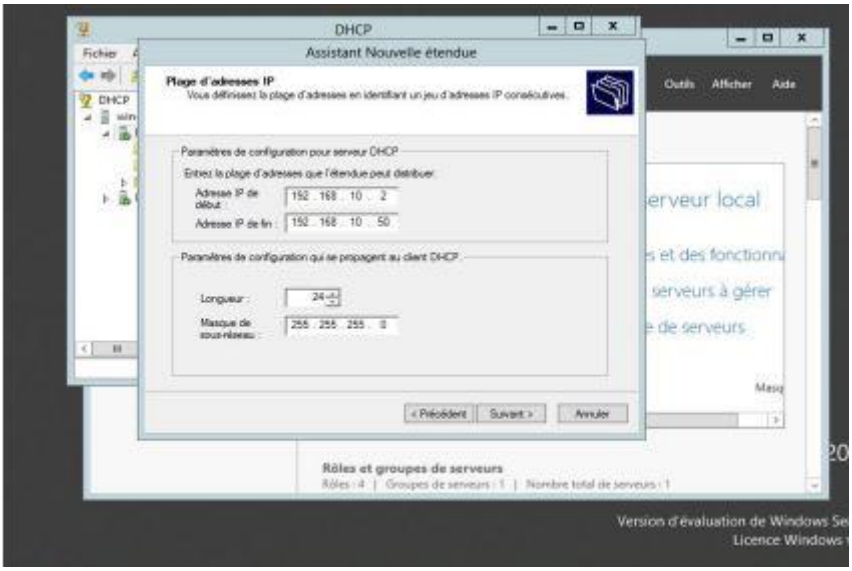
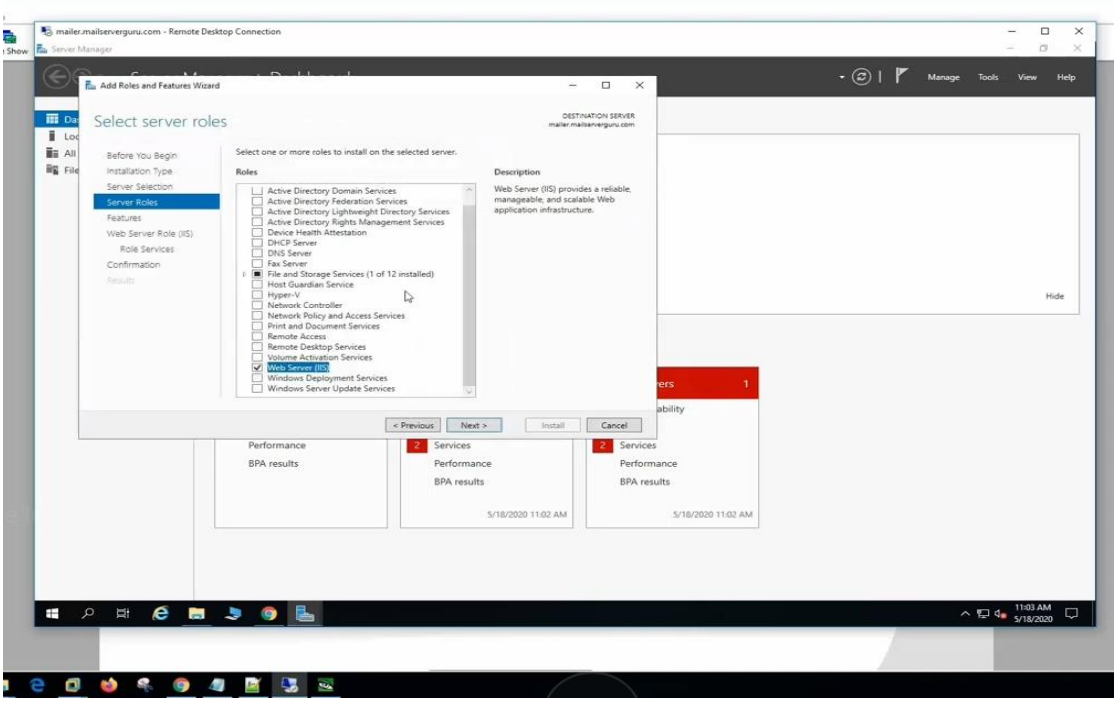


Figure 5 : Ajout d'une nouvelle étendue

II.4. Installation de MailEnable

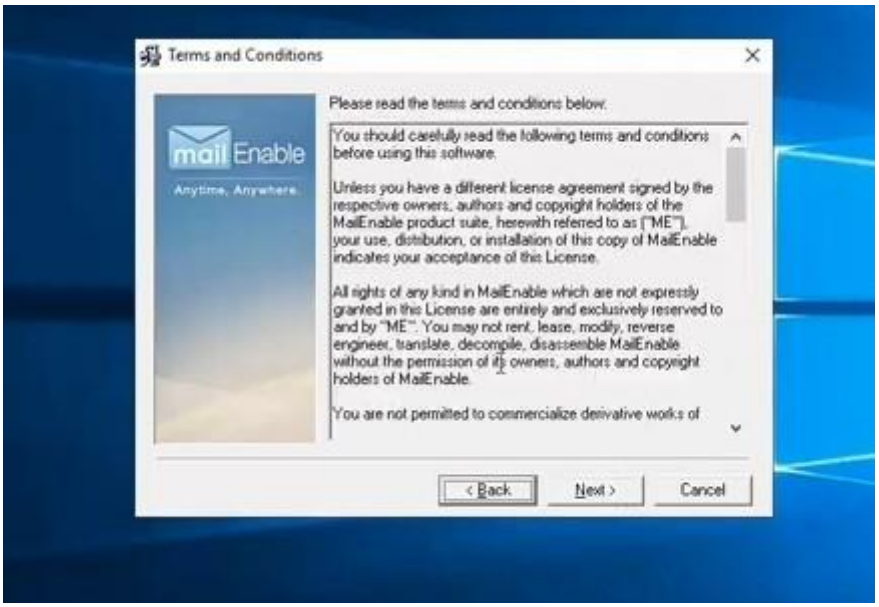
1- **Installation de mailEnable**

Il faut installer un serveur web c'est-à-dire **web server (IIS)** dans le gestionnaire de serveur Active Directory.



Ensuite il faut télécharger **mailEnable** à l'adresse suivante : https://www.mailenable.com/download-thank-you.asp?prod=1&v=1048.
Après le téléchargement on peut exécuter le logiciel puis on clique sur **OK**

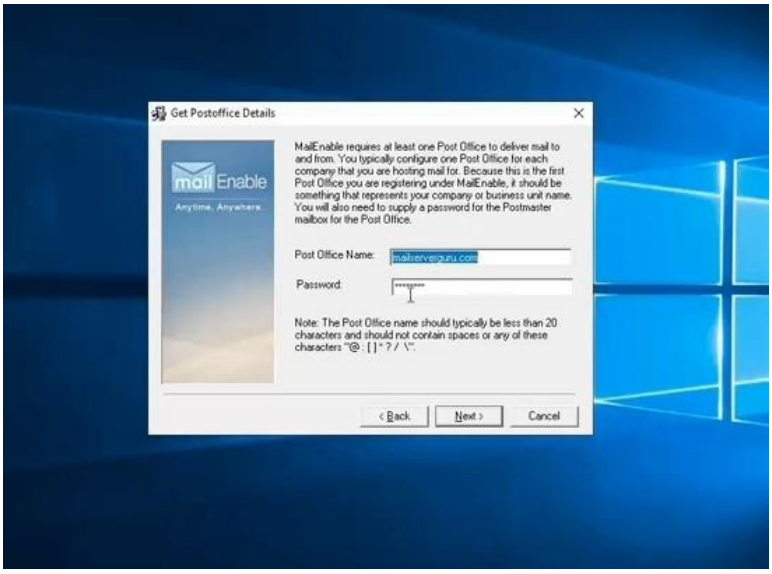
Après avoir validé cette étape, on clique sur **next** encore.



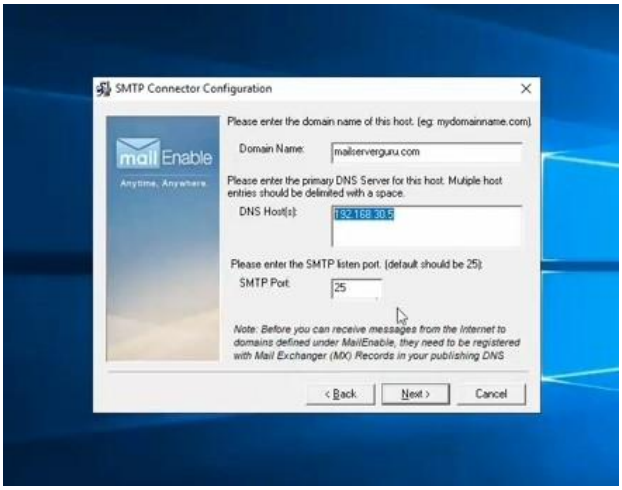
Puis dans la fenêtre suivante on accepte les termes et conditions en cliquant sur **next.**

Ensuite on clique sur **next** pour l'installation de composants supplémentaires.

Le programme sera installé dans le dossier **C:\Program Files (x86)\Mail Enable** par défaut, on valide avec **next.**



Dans la nouvelle fenêtre, on indiquera le nom de notre Post Office c'est-à-dire le nom de notre serveur ainsi qu'un mot de passe pour l'administrateur.



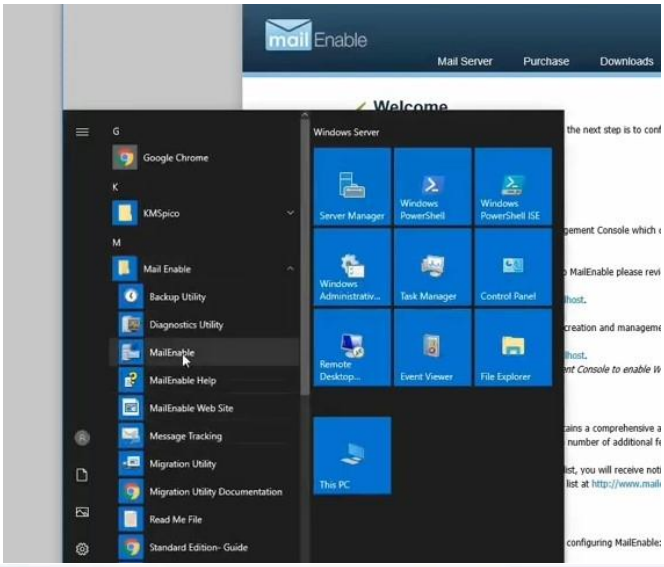
On clique sur **next.**

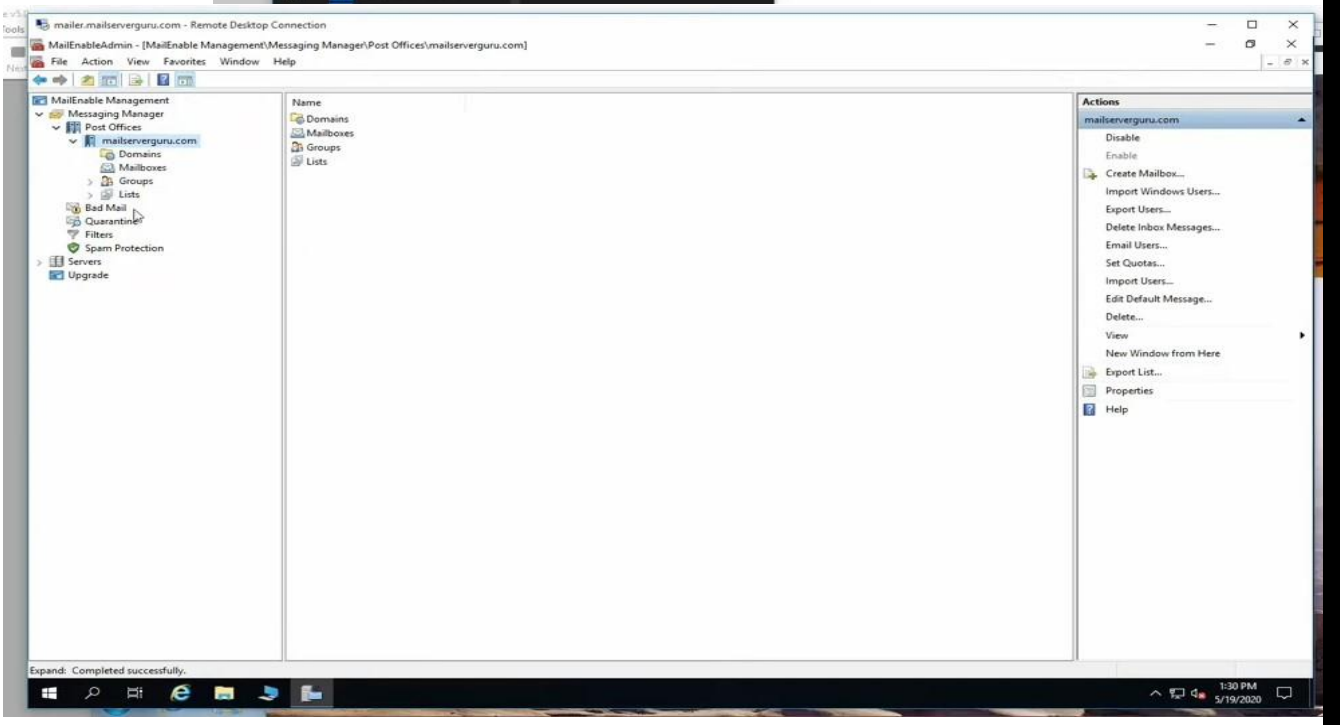
À ce stade on indique notre nom de domaine ainsi que l'adresse IP de notre serveur DNS. Par défaut le serveur SMTP écoute sur le port 25.

Après cette étape on valide les prochaines étapes en cliquant sur **next** pour les toutes les nouvelles fenêtres qui s'afficheront. Ainsi après l'installation du programme, on peut l'exécuter ouvrant le menu démarrer.

2- Interface

Dans l'interface du server, on clique sur **messaging Manager**, ensuite sur **Post offices** ainsi on verra le nom de notre organisation qu'on a renseigné lors de l'installation.



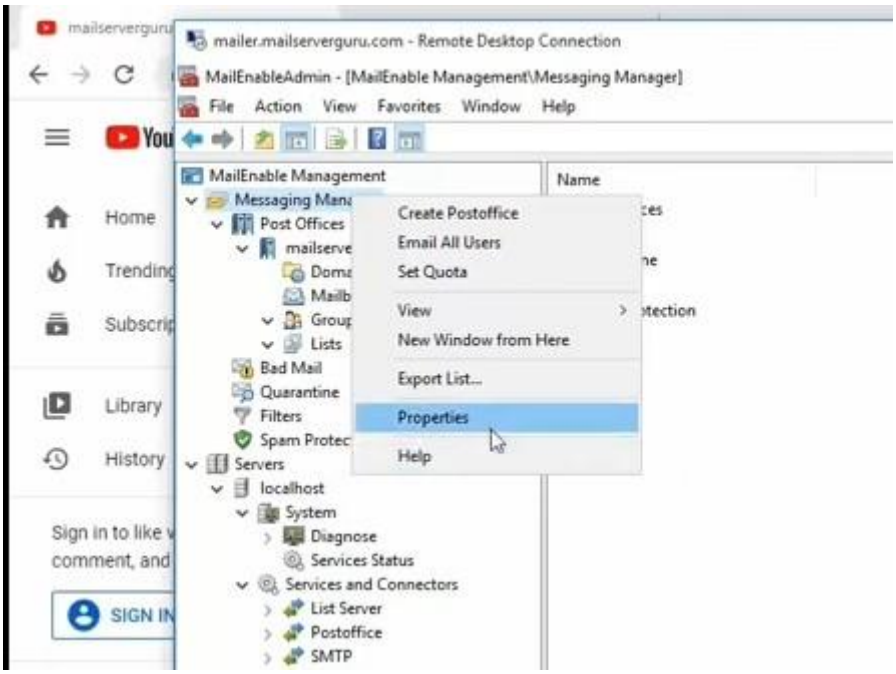


3- MailEnable Active Directory intégration

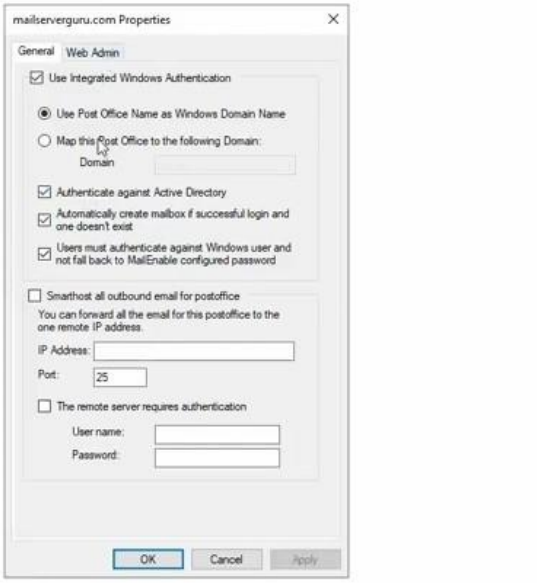
Dans cette partie on verra comment intégrer le système d'authentification d'AD dans notre serveur de messagerie ce qui permettra de créer

automatiquement un mailbox pour un utilisateur de notre domaine qui n'en avait pas.

Clic droit sur **messaging manager** puis sur **properties**.



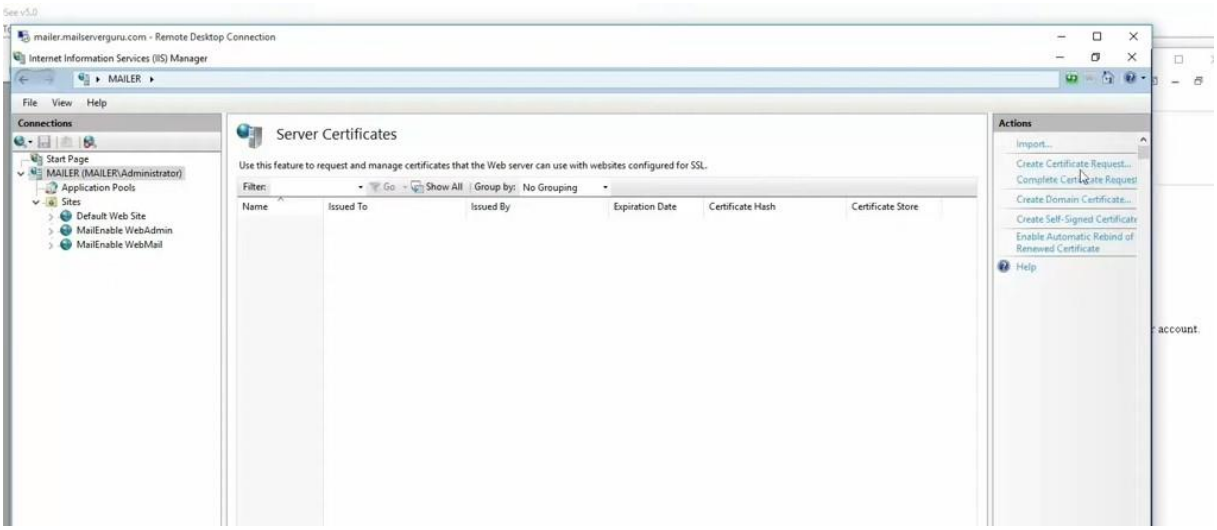
Dans la nouvelle fenêtre, on sélectionne l'onglet **security** puis on coche **enable integrated Authentication** puis sur **apply** et **ok.** Cela va permettre d'utiliser le système d'authentification de windows pour vérifier l'identité d'un utilisateur. Après cette étape, on effectue un clic droit sur le nom de notre organisation puis on ouvre l'onglet **général**, ensuite on coche la case **Use integrated Windows Authentication** puis on coche aussi les trois dernières cases.

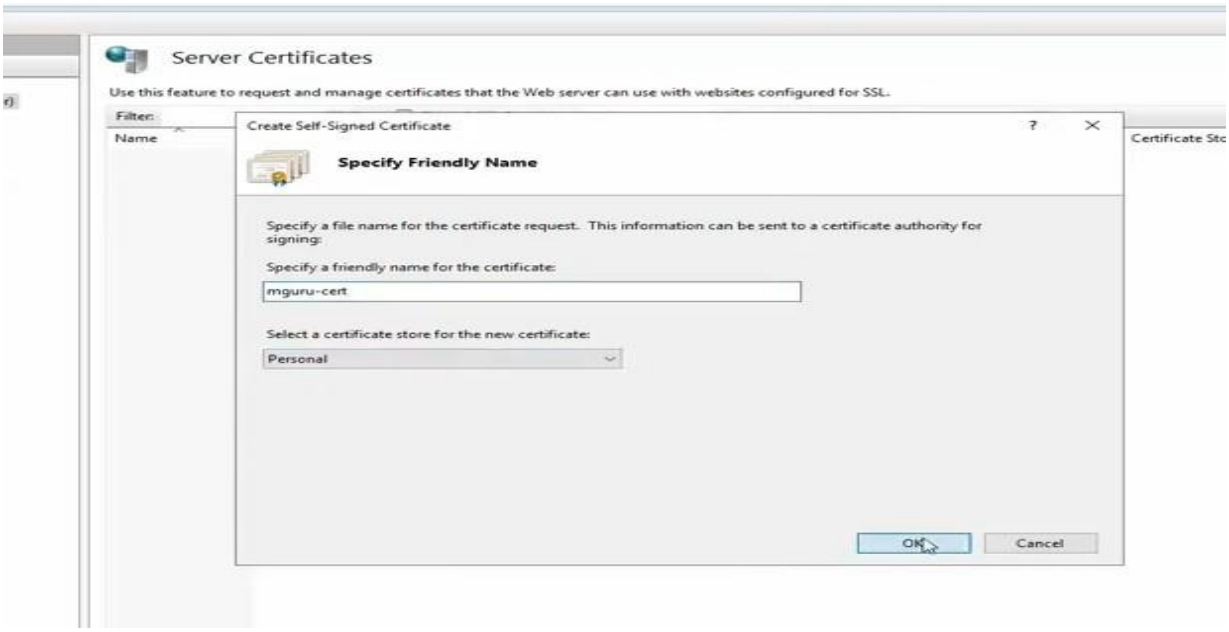


Ici quand un utilisateur va essayer de se connecter dans un client de messagerie et qu'il se sera bien authentifié, MailEnable va créer un mailbox pour cet utilisateur. On aura plus besoin de créer un mailbox pour chaque utilisateur de notre domaine qui permet de gain de temps pour l'administrateur réseau.

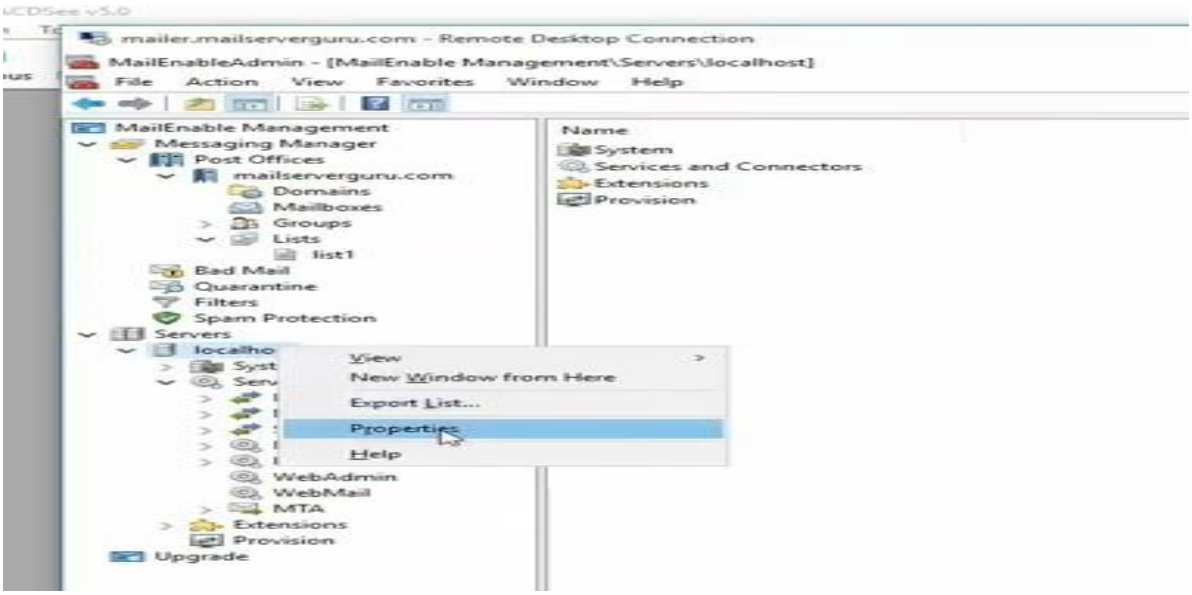
4- Chiffrement des messages

Pour mener à bien cette étape on a besoin d'un certificat pour le chiffrement qui permettra de faire le chiffrement des messages, l'installation se fera grâce au serveur IIS. Dans l'interface du serveur IIS, on sélectionnera notre serveur et dans la colonne **Action** et on choisira **Create self-signed certificate** puis on indiquera le nom de notre certificat et on gardera les options par défaut dans la fenêtre qui va s'afficher.

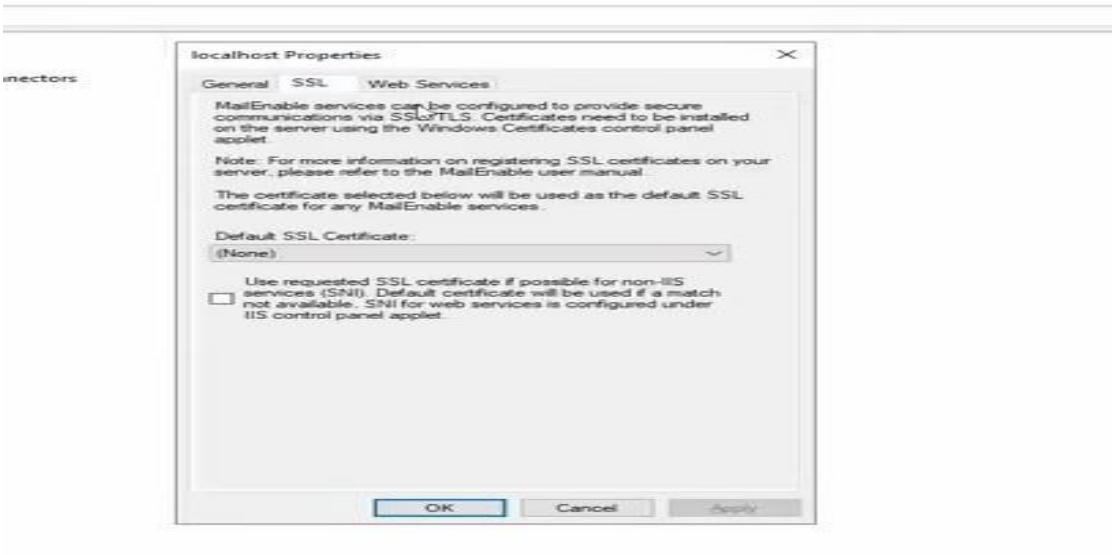




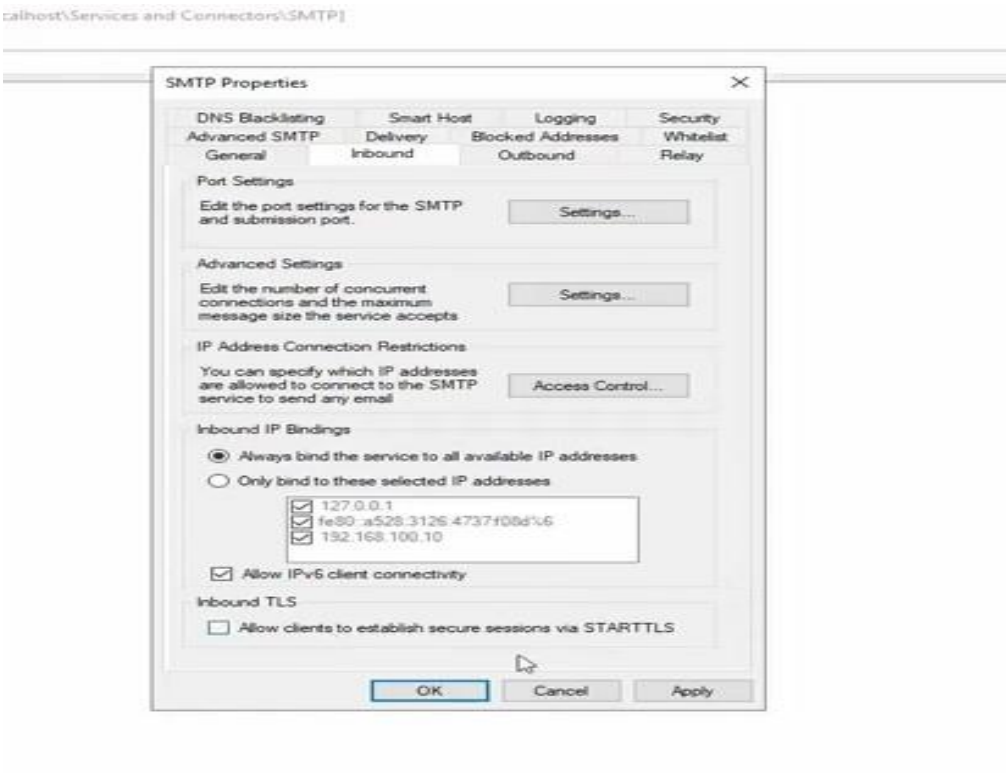
On ouvre ensuite notre serveur de messagerie pour la configuration, on fait un clic droit sur **localhost** qui est dans **Servers** suivi de **properties.**



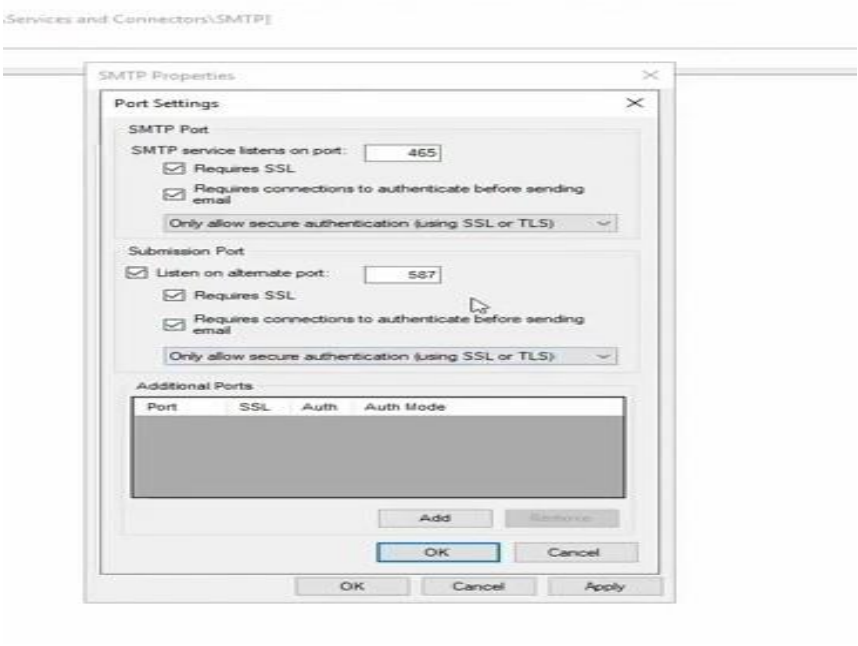
Dans la boîte de dialogue on sélectionnera l'onglet **SSL** puis au niveau de **default SSL certificate** on sélectionnera le nom qu'on a donné à notre certificat puisque ce dernier sera automatiquement détecté par le serveur grâce au serveur IIS. On valide avec **Apply** et **Ok.**



Après cette étape on effectue une clique droite sur **SMTP** dans **Servers > localhost > services and connectors** puis **properties**, puis dans la boîte de dialogue, on sélectionne l'onglet **inbound.** Ainsi dans la première partie **Port Settings** on clique sur **settings.**

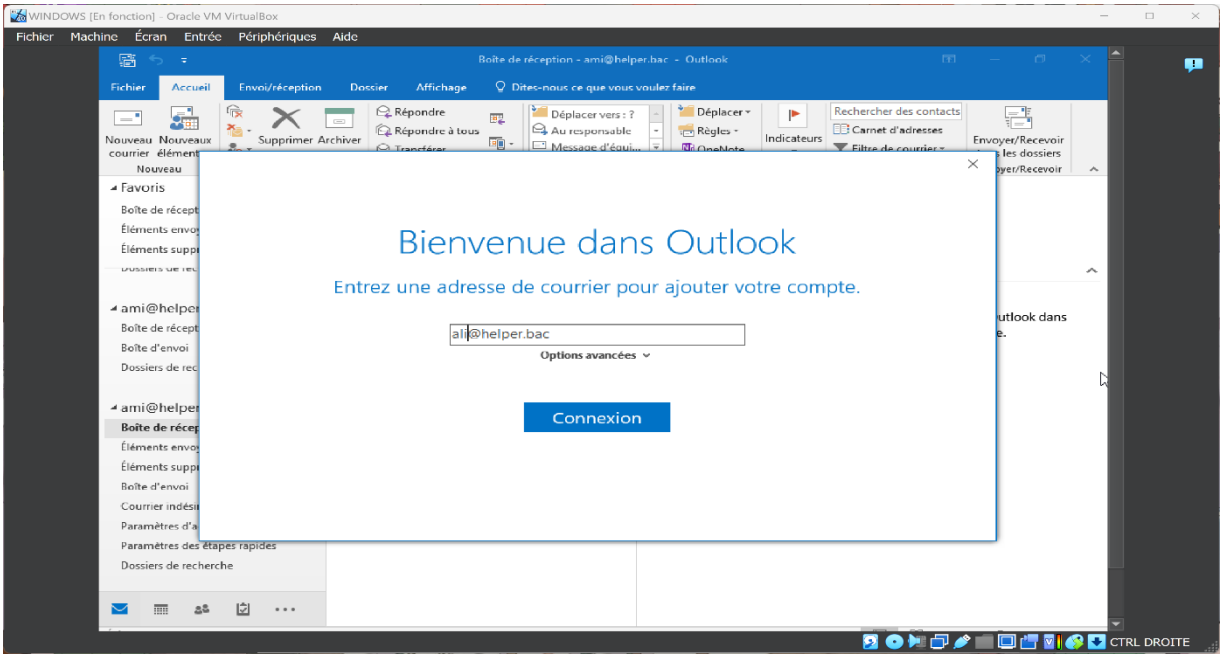


Dans la nouvelle boîte de dialogue, on change le port 25 par le port 465 qui permettra d'utiliser SMTPs et on coche les deux cases qui suivent puis on sélectionnera la troisième option dans le menu déroulant. Cet option va permettre au serveur d'accepter uniquement les connexions SSL ou TLS puis on valide avec **apply** et **ok.** Le serveur va redémarrer pour prendre les modification en compte.

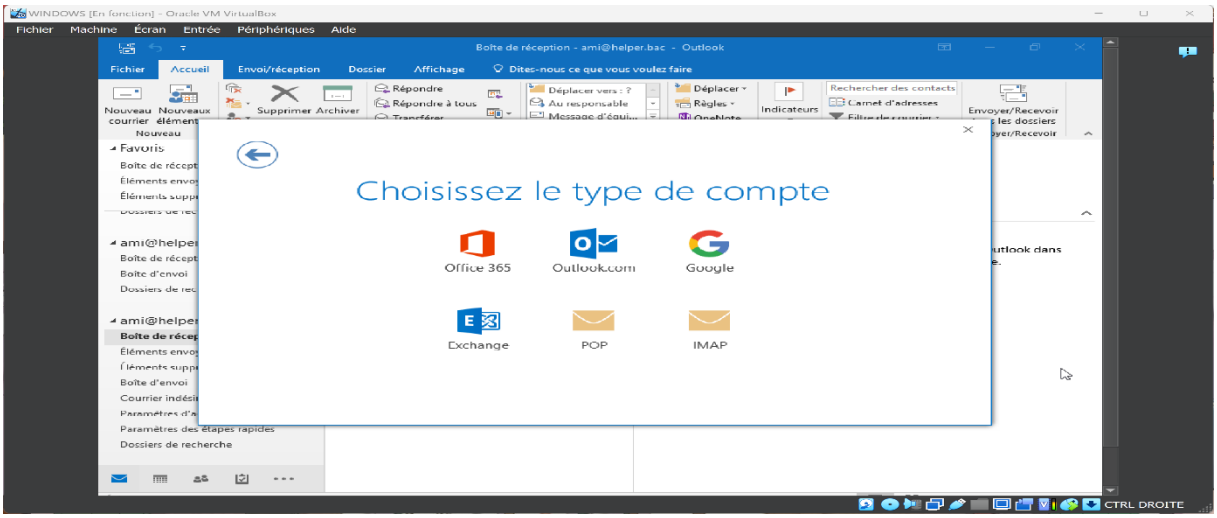


5- Connexion d'un utilisateur

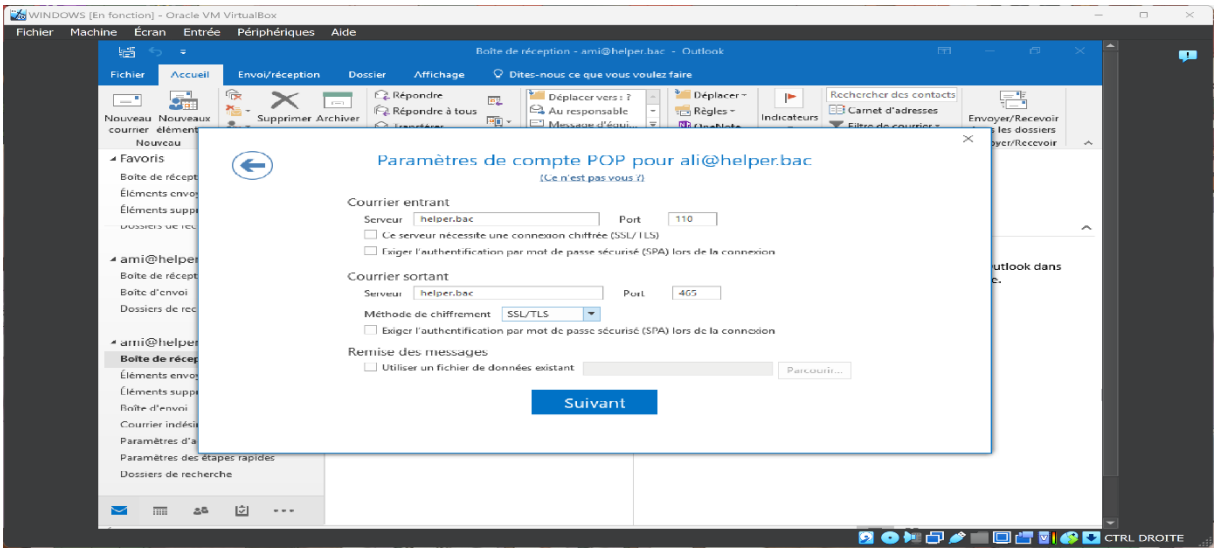
Dans notre domaine on a créé un utilisateur **Ali** qui a pour adresse mail **ali@helper.bac.** On ouvre notre client de messagerie, dans notre cas sera Outlook puis on saisit l'adresse ci-dessus.

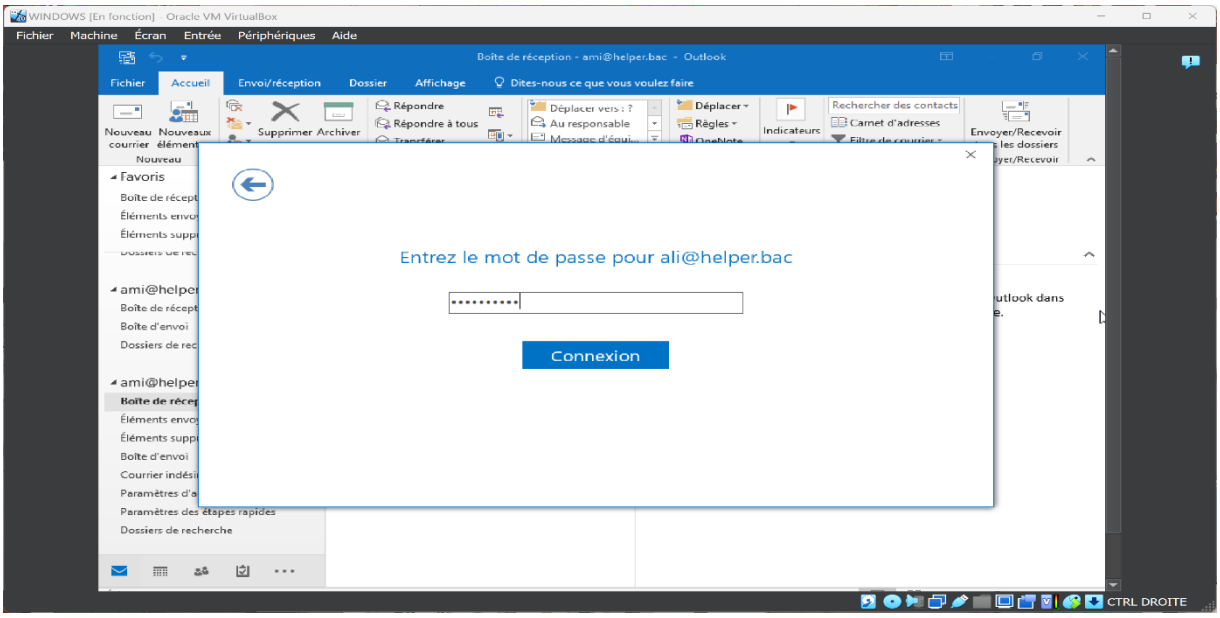


Puis nous devons choisir notre type de compte, dans notre cas ce sera **POP** ou **IMAP**

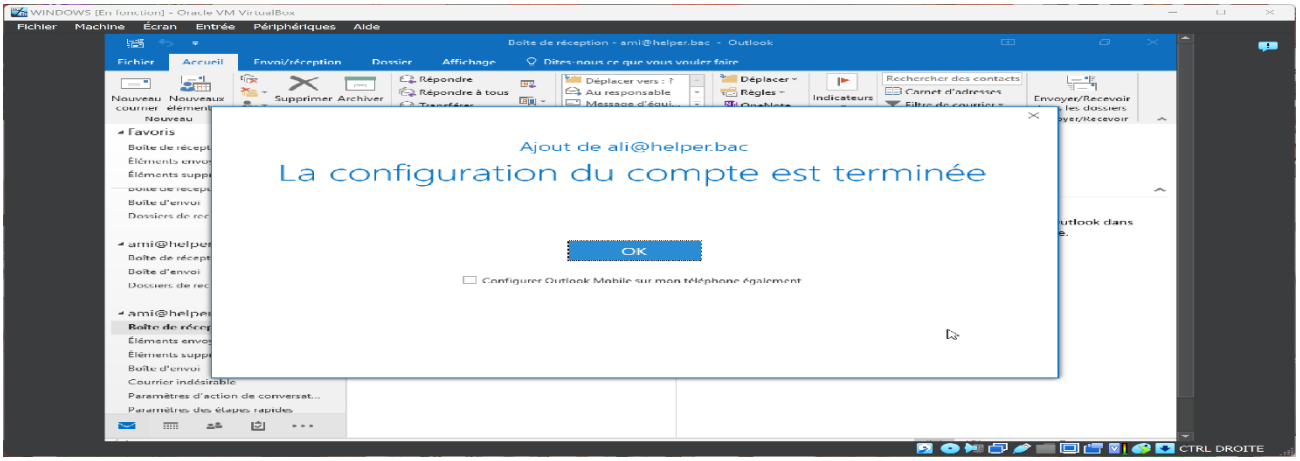


Dans la prochaine étape nous devons indiquer le serveur entrant et le serveur sortant, dans notre cas ce sera le même serveur qui jouera ce rôle et le nom sera **helper.bac.** Le serveur entrant écoutera sur le port 110 et le serveur sortant écoutera sur le port 465 et la méthode de chiffrement sera SSL/TLS. Puis nous devons saisir le mot de passe de Ali.

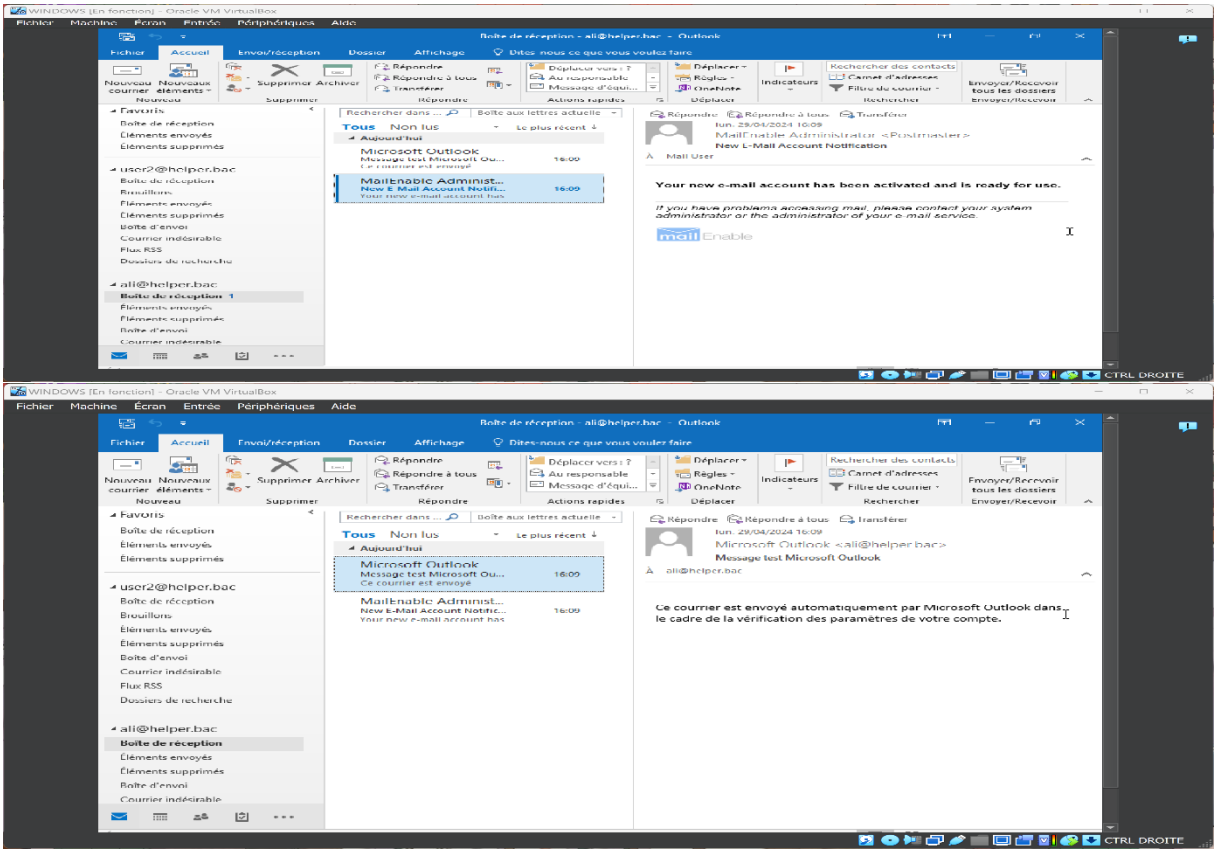




On valide la configuration en cliquant sur ok



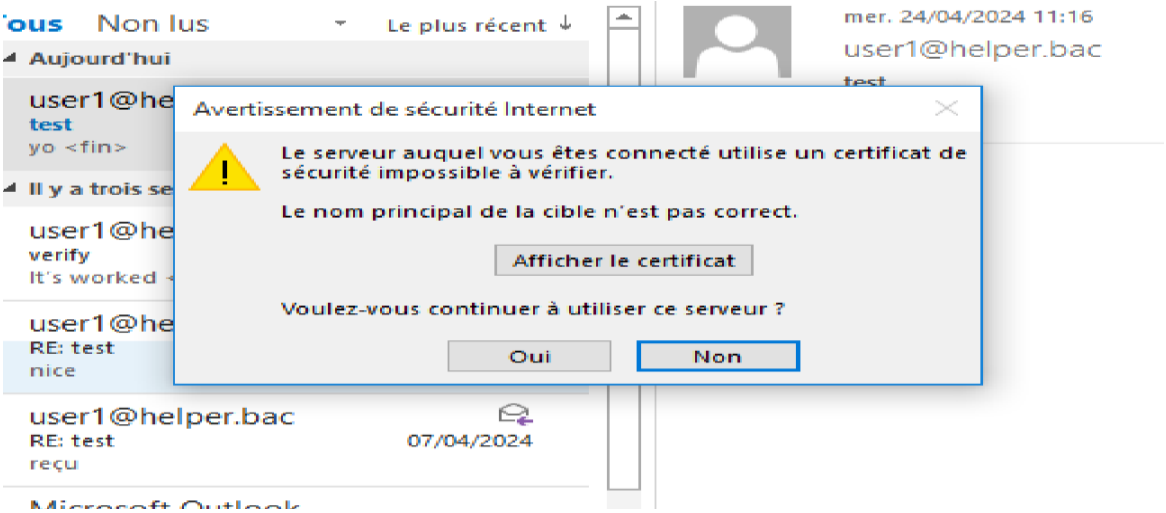
On recevra un mail de la part de notre serveur pour nous informer qu'il a bien créé un mailbox pour Ali et un autre mail de la part de outlook pour la vérification de notre compte ce qui veut dire qu'on a pu se connecter.



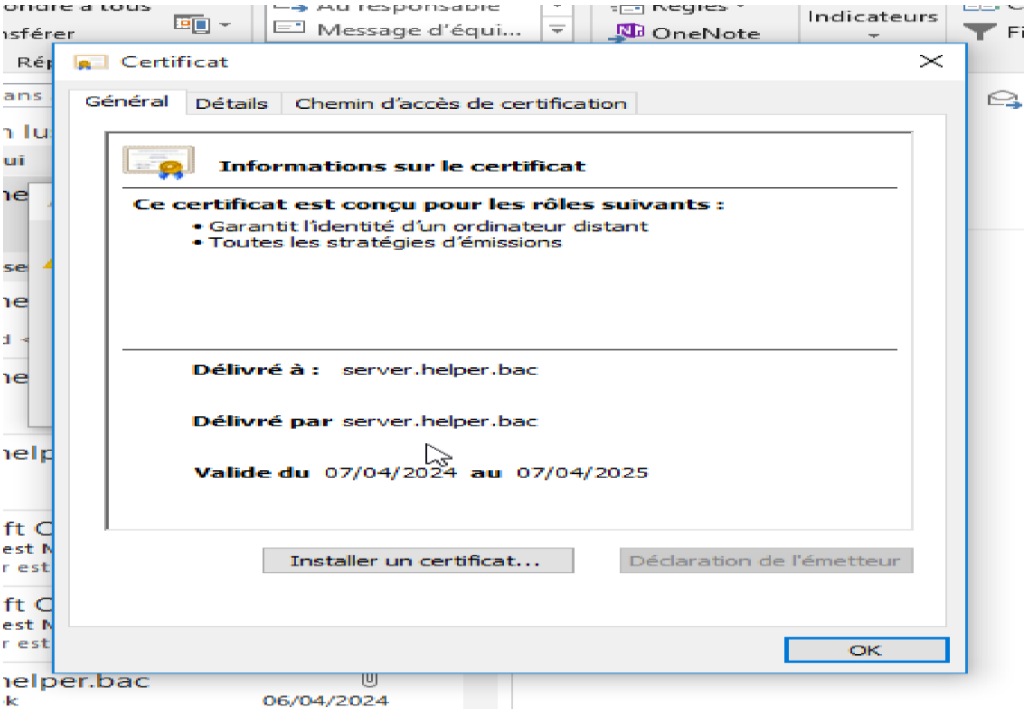
Quand Ali va essayer d'envoyer son premier on lui demandera d'installer un certificat car notre serveur utilise un certificat de sécurité.

6- Installation d'un certificat de sécurité

Dans la boite de dialogue d'avertissement de sécurité, on sélectionnera **afficher le certificat**



Ensuite on clique sur **installer un certificat**



Puis on clique sur **suivant** dans les autres boites qui se présenteront jusqu'à la dernière étape où on se retrouvera sur la boite qui demande d'installer un certificat on clique sur **ok** pour valider l'installation. Puis on sera encore la toutes premières boite c'est-à-dire la boîte avertissement, on valide en cliquant sur **Oui** pour terminer l'installation du certificat. Ainsi Ali pourra envoyer des mails en toute sécurité via notre serveur.

CONCLUSION

Au cours des deux dernières décennies, la messagerie électronique s'est imposée comme un moyen de communication de prédilection dans le milieu professionnel 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.