

EXCHANGE SERVEUR 2019



SOMMAIRE

Introduction.....	2
Prérequis.....	2
La conception de votre environnement Exchange 2019.....	2
Préparation des partitions et configuration d'Active Directory.....	12
Préparation de la partition de Domaine.....	12
Installation d'Exchange 2019 en Mode Non Surveillé.....	14
Demander un certificat SSL avec Win-ACME.....	17
Conclusion.....	22

Introduction

Exchange Server est une plateforme de messagerie et de collaboration développée par Microsoft. Il permet aux utilisateurs de gérer leurs courriels, calendriers, contacts et tâches de manière centralisée. Exchange offre également des fonctionnalités avancées telles que la sécurité des données, la gestion des ressources et la synchronisation multi-appareils.

Prérequis

Installé une machine serveur 2022 avec un rôle AD installé, installé une machine serveur 2022 en core.

La conception de votre environnement Exchange 2019

- On commence par changer le nom de l'ordinateur. On sélectionne l'option 2 et on change le nom de la machine :

```

=====
                          Nom de l'ordinateur
=====
Nom de l'ordinateur actuel : WIN-JNJUBS36KDB
Entrer un nouveau nom d'ordinateur (Vide = annuler): EXCH1
  
```

- On met à jour la machine avec l'option 6, 1 et T :

```

=====
                Bienvenue dans Windows Server 2022 Standard
=====
1)  Domaine ou groupe de travail :      Groupe de travail : WORKGROUP
2)  Nom de l'ordinateur :                EXCH1
3)  Ajouter l'administrateur local
4)  Gestion à distance :                 Activé
5)  Paramètre de mise à jour :           Téléchargez uniquement
6)  Installer les mises à jour
7)  Bureau à distance :                  Désactivé
8)  Paramètres réseau
9)  Date et heure
10) Paramètre de télémétrie :            Requis
11) Activation de Windows
12) Fermer la session utilisateur
13) Redémarrer le serveur
14) Arrêter le serveur
15) Quitter vers la ligne de commande (PowerShell)

Entrez un nombre pour sélectionner une option: 6
  
```

```

=====
                Installer les mises à jour
=====
Rechercher :

1) Toutes les mises à jour qualité
2) Mises à jour de qualité recommandées uniquement
3) Mises à jour des fonctionnalités

Sélectionnez une catégorie de mise à jour (Vide = annuler): 1
Recherche de toutes les mises à jour applicables... Merci de patienter.

Mise(s) à jour disponible(s) :
1) 2022-02 Préversion de la mise à jour cumulative pour .NET Framework 3.5 et 4.8 pour Microsoft server operating system version 21H2 pour systèmes x64 (KB5010475)
2) 2024-01 Mise à jour cumulative de .NET Framework 3.5, 4.8 et 4.8.1 Microsoft server operating system version 21H2 pour x64 (KB5034272)
3) Mise à jour de la sélection disjointe pour Microsoft Defender Antivirus - 2267602 Ko (version 1.403.3409.0) - Canal actuel (large)
4) 2024-01 Mise à jour cumulative pour Microsoft server operating system version 21H2 de x64 avec systèmes basés dessus (KB5034129)

Installer (t)outes les mises à jour, (A)ucune mise à jour ou sélectionner une (M)ise à jour unique ? (Vide = annuler): t
  
```

- Un message de redémarrage va apparaître taper 'O' et la mise à jour va se lancer au redémarrage :

```
C:\Windows\system32\LogonUI.exe
Installation des mises à jour 30% effectués N'éteignez pas l'ordinateur.
```

- Choisissez l'option 8 pour la reconfiguration du réseau en ip fixe et en associant le dns de votre active directory :

```

=====
                    Bienvenue dans Windows Server 2022 Standard
=====

1) Domaine ou groupe de travail :      Groupe de travail : WORKGROUP
2) Nom de l'ordinateur :                EXCH1
3) Ajouter l'administrateur local
4) Gestion à distance :                Activé

5) Paramètre de mise à jour :          Téléchargez uniquement
6) Installer les mises à jour
7) Bureau à distance :                Désactivé

8) Paramètres réseau
9) Date et heure
10) Paramètre de télémétrie :          Requis
11) Activation de Windows

12) Fermer la session utilisateur
13) Redémarrer le serveur
14) Arrêter le serveur
15) Quitter vers la ligne de commande (PowerShell)

Entrez un nombre pour sélectionner une option: 8_
```

- Choisissez l'adaptateur 1 et configurer le correctement :

```

=====
                    Paramètres réseau
=====

Cartes réseau disponibles :

Index numéro | Adresse IP      | Description
1            | 192.168.128.176 | Intel(R) 82574L Gigabit Network Connection

Sélectionnez le numéro d'index de la carte réseau (Vide = annuler): 1
```

- Choisissez l'option 2, configurer votre serveur DNS avec l'adresse IP du serveur AD.

```

=====
                          Paramètres de carte réseau
=====

Index NIC :                1
Description :              Intel(R) 82574L Gigabit Network Connection
Adresse IP :               192.168.128.176,
                          fe80::2a7a:27a4:37e:877e
Masque de sous-réseau :   255.255.255.0
DHCP activé :              True

Passerelle par défaut :   192.168.128.2
Serveur DNS préféré :     192.168.128.2
Serveur DNS auxiliaire :

1) Définir l'adresse de la carte réseau
2) Définir les serveurs DNS
3) Effacer les paramètres du serveur DNS

Entrez la sélection (Vide = annuler): 2
Entrer un nouveau serveur DNS préféré (Vide = annuler): 192.168.128.175
Entrer un autre serveur DNS (vide=aucun):
Le ou les serveurs DNS ont été assignés.
(Appuyez sur ENTRÉE pour continuer):

```

- Enfin pour joindre la machine au domaine, faite l'option 1:

```

12) Fermer la session utilisateur
13) Redémarrer le serveur
14) Arrêter le serveur
15) Quitter vers la ligne de commande (PowerShell)

Entrez un nombre pour sélectionner une option: 1

```

- Choisissez l'option D, entrez votre domaine, votre compte administrateur, renommer votre pc si vous le souhaitez :

```

=====
                          Changer l'appartenance au domaine ou groupe de travail
=====

Actuel groupe de travail : WORKGROUP

Souhaitez-vous adhérer à un (D)omaine ou Groupe de (t)ravail? (Vide = annuler): D
Nom de domaine à joindre (Vide = annuler): exchanges.local
Spécifier un domaine\utilisateur autorisé: (Vide = annuler): administrateur
Mot de passe de administrateur: *****
Vous rejoignez exchanges.local... Merci de patienter.
AVERTISSEMENT : Les modifications seront prises en compte après le redémarrage de l'ordinateur EXCH1.
Vous avez correctement rejoint le domaine.
Voulez-vous modifier le nom de l'ordinateur avant de redémarrer ? (O)ui ou (N)on: O
Entrer un nouveau nom d'ordinateur (Vide = annuler): exch1
Mot de passe de administrateur: *****

```


- Cette commande permet de voir les mises à jour :

```
PS C:\> Get-Hotfix
```

Source	Description	HotFixID	InstalledBy	InstalledOn
EXCH1	Update	KB5033914	EXCH1\Administrateur	08/02/2024 00:00:00
EXCH1	Security Update	KB5034129	AUTORITE NT\Systeme	08/02/2024 00:00:00
EXCH1	Update	KB5034286	AUTORITE NT\Systeme	08/02/2024 00:00:00

- On installe RSAT-AD, c'est un complément d'installation utile :

```
PS C:\Users\Administrateur> Get-WindowsFeature | Where{ $_.Name -like "RSAT-ad*" }
```

Display Name	Name	Install State
[] Outils AD DS et AD LDS	RSAT-AD-Tools	Available
[] Composants logiciels enfichables et ...	RSAT-ADLDS	Available
[] Module Active Directory pour Windows...	RSAT-AD-PowerShell	Available
[] Outils AD DS	RSAT-ADDS	Available
[] Centre d'administration Active D...	RSAT-AD-AdminCenter	Available
[] Composants logiciels enfichables...	RSAT-ADDS-Tools	Available

```
PS C:\Users\Administrateur> Add-WindowsFeature -Name RSAT-AD-Tools
```

Success	Restart Needed	Exit Code	Feature Result
True	No	Success	{Outils d'administration de serveur distan...

```
PS C:\Users\Administrateur> Add-WindowsFeature -Name RSAT-DNS-Server
```

Success	Restart Needed	Exit Code	Feature Result
True	No	Success	{Outils du serveur DNS}

- On effectue la configuration du disque en attribuant le Z:\ pour le lecteur de DVD :

Get-WmiObject -Class Win32_volume -Filter "DriveType=5" | Select -First 1 | Set-WmiInstance -Arguments @({DriveLetter="Z:"})

```
PS C:\Users\Administrateur> Get-WmiObject -Class Win32_volume -Filter "DriveType=5" | Select -First 1 | Set-WmiInstance -Arguments @({DriveLetter="Z:"})
```

```

_GENUS           : 2
_CLASS          : Win32_Volume
_SUPERCLASS     : CIM_StorageVolume
_DYNASTY        : CIM_ManagedSystemElement
_RELPATH        : Win32_Volume.DeviceID="\\\\?\\Volume{ac9ab18e-c65d-11ee-96c2-806e6f6e6963}\\\"
_PROPERTY_COUNT : 44
_DERIVATION     : {CIM_StorageVolume, CIM_StorageExtent, CIM_LogicalDevice, CIM_LogicalElement...}
_SERVER         : EXCH1
_NAMESPACE      : root\cimv2
_PATH           : \\EXCH1\root\cimv2:Win32_Volume.DeviceID="\\\\?\\Volume{ac9ab18e-c65d-11ee-96c2-806e6f6e6963}\\\"
Access          :
Automount       : True
Availability    :
BlockSize      : 2048
BootVolume     : False
Capacity       : 5566558208
Caption        : Z:\
Compressed      :
ConfigManagerErrorCode :
ConfigManagerUserConfig :
CreationClassName :
Description    :
DeviceID       : \\?\\Volume{ac9ab18e-c65d-11ee-96c2-806e6f6e6963}\\
DirtyBitSet    : False
DriveLetter    : Z:
DriveType     : 5
ErrorCleared   :
ErrorDescription :
ErrorMethodology :
FileSystem     : UDF
FreeSpace      : 0
IndexingEnabled :
InstallDate   :
Label         : SSS_X64FRE_FR-FR_DV9
LastErrorCode  :
MaximumFileNameLength : 254
Name          : Z:\
NumberOfBlocks :
PageFilePresent : False

```

- On vérifie les disques installés avec la commande Get-Disk :

```
PS C:\Users\Administrateur> Get-Disk
```

Number	Friendly Name	Serial Number	HealthStatus	OperationalStatus	Total Size	Partition Style
2	VMware Vir...	VMWare NVME_0000	Healthy	Online	50 GB	GPT
0	VMware, VM...		Healthy	Offline	30 GB	RAW
1	VMware, VM...		Healthy	Offline	30 GB	RAW

- Disque 2 est mon disque de démarrage donc le système est installé dessus.
- Disque 1 sera utilisé pour stocker les bases de données de la file d'attente du SMTP du lecteur D:\.
- Pour activer le disque et l'initialiser, on utilise la commande suivante :

```
PS C:\Users\Administrateur> Initialize-Disk -Number 0 -PartitionStyle GPT
```

```
PS C:\Users\Administrateur> New-Partition -DiskNumber 0 -UseMaximumSize
```

```
DiskPath : \\?\scsi#disk&ven_vmware_&prod_vmware_virtual_s#5&1ec51bf7&0&000000#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}
```

PartitionNumber	DriveLetter	Offset	Size	Type
2		16777216	29.98 GB	Basic

```
PS C:\Users\Administrateur> Get-Partition -DiskNumber 0 -PartitionNumber 2 | Format-Volume -FileSystem NTFS -NewFileSystemLabel "Queue Database" -AllocationUnitSize 65536 -Confirm:$false
```

DriveLetter	FriendlyName	FileSystemType	DriveType	HealthStatus	OperationalStatus	SizeRemaining	Size
D	Queue Database	NTFS	Fixed	Healthy	OK	29.92 GB	29.98 GB

- On peut vérifier les disques :

```
PS C:\Users\Administrateur> Get-Disk
```

Number	Friendly Name	Serial Number	HealthStatus	OperationalStatus	Total Size	Partition Style
2	VMWare NVME_0000		Healthy	Online	50 GB	GPT
0	V		Healthy	Online	30 GB	GPT
1	V		Healthy	Offline	30 GB	RAW

- On peut vérifier les partitions :

```
PS C:\Users\Administrateur> Get-Partition

DiskPath :
\\?\scsi#disk&ven_nvme&prod_vmware_virtual_n#5&2d15267&0&000000#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}

PartitionNumber  DriveLetter Offset                Size Type
-----
1                1048576          100 MB System
2                105906176        16 MB Reserved
3                122683392        49.33 GB Basic
4                53089402880      568 MB Recovery

DiskPath : \\?\scsi#disk&ven_vmware_&prod_vmware_virtual_s#5&1ec51bf7&0&000000#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}

PartitionNumber  DriveLetter Offset                Size Type
-----
1                17408            15.98 MB Reserved
2                16777216         29.98 GB Basic
```

- On formate les disques qui contient les bases de données des boites aux lettres dans des points de montage.
- On procède comme les commandes précédentes, mais il y aura une différence bien faire attention à la commande :

```
PS C:\> MD C:\ExchDbs\Disk0

Répertoire : C:\ExchDbs

Mode                LastWriteTime         Length Name
----                -
d-----           08/02/2024   14:27         Disk0
```

```
PS C:\> Initialize-Disk -Number 1 -PartitionStyle GPT
PS C:\> New-Partition -DiskNumber 1 -UseMaximumSize

DiskPath :
\\?\scsi#disk&ven_vmware_&prod_vmware_virtual_s#5&1ec51bf7&0&000100#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}

PartitionNumber  DriveLetter Offset                Size Type
-----
2                16777216         29.98 GB Basic

PS C:\> Get-Partition -DiskNumber 1 -PartitionNumber 2 | Format-Volume -FileSystem NTFS -NewFileSystemLabel
"Queue Database" -AllocationUnitSize 65536 -Confirm:$false

DriveLetter FriendlyName  FileSystemType DriveType HealthStatus OperationalStatus SizeRemaining  Size
-----
Queue Database NTFS          Fixed      Healthy    OK              29.92 GB 29.98 GB
```

- On installe .NET framework 4.8 avec les commandes :

```
PS C:\> New-Item C:\Install -ItemType Directory

Répertoire : C:\

Mode                LastWriteTime         Length Name
----                -
d-----          08/02/2024   14:34             Install

PS C:\> Start-BitsTransfer -Source "https://download.visualstudio.microsoft.com/download/pr/7afca223-55d2-470a-8edc-6a1739ae3252/abd170b4b0ec15ad0222a809b761a036/ndp48-x86-x64-allos-enu.exe" -Destination C:\Install
```

- On installe Visual C++ Redistributable Package for Visual Studio 2012 :

```
PS C:\> New-Item C:\Install\VS2012 -ItemType Directory

Répertoire : C:\Install

Mode                LastWriteTime         Length Name
----                -
d-----          08/02/2024   14:37             VS2012

PS C:\> Start-BitsTransfer -Source "https://download.microsoft.com/download/1/6/B/16B06F60-3B20-4FF2-B699-5E9B7962F9AE/VSU4/vcredist_x64.exe" -Destination C:\Install\VS2012
```

- On installe Visual C++ Redistributable Package for Visual Studio 2013 :

```
PS C:\> New-Item C:\Install\VS2013 -ItemType Directory

Répertoire : C:\Install

Mode                LastWriteTime         Length Name
----                -
d-----          08/02/2024   14:38             VS2013

PS C:\> Start-BitsTransfer -Source "https://download.microsoft.com/download/2/E/6/2E61CFA4-993B-4DD4-91DA-3737CD5CD6E3/vcredist_x64.exe" -Destination C:\Install\VS2013
```

- On installe URL Rewriter :
- On installe Microsoft Unified Communications Managed API 4.0, Core Runtime 64-Bit :

```
PS C:\> Start-BitsTransfer -Source "https://download.microsoft.com/download/1/2/8/128E2E22-C1B9-44A4-BE2A-5859ED1D4592/rewrite_amd64_en-US.msi" -Destination C:\Install
PS C:\> Start-BitsTransfer -Source "http://download.microsoft.com/download/2/C/4/2C47A5C1-A1F3-4843-B9FE-84C0032C61EC/UcmaRuntimeSetup.exe" -Destination C:\Install
```

- On peut les exécuter une fois qu'elles sont toutes installées :

```
PS C:\> Start-Process -FilePath "C:\Install\ndp48-x86-x64-allos-enu.exe" -ArgumentList "/q" -Wait
PS C:\> Start-Process -FilePath "C:\Install\VS2012\vcredist_x64.exe" -ArgumentList "/q" -Wait
PS C:\Install\VS2013> Start-Process -FilePath "C:\Install\VS2013\vcredist_x64.exe" -ArgumentList "/q" -Wait
PS C:\Install\VS2013>
PS C:\> Start-Process -FilePath "C:\Install\UcmaRuntimeSetup.exe" -ArgumentList "/q" -Wait
PS E:\> Start-Process -FilePath "E:\UcmaRedist\setup.exe" -ArgumentList "/q" -Wait
```

- On installe les rôles et fonctionnalités de Windows Server sur Windows Server 2019 Server Core :

```
PS E:\> Install-WindowsFeature Server-Media-Foundation, NET-Framework-45-Features

Success Restart Needed Exit Code      Feature Result
-----
True      No              Success          {Message Queuing, Serveur Message Queuing,...
```

- Avec l'option 12, on se connecte à notre domaine afin d'installer le serveur Exchanges 2019 pour préparer la partition du schéma, configuration et domaine.
- Pour la préparation du schéma pour Exchange 2019, on se connecte en utilisant le compte qui fait partie du groupe de sécurité des administrateurs de schéma. Donc on ouvre une invite de commande avec des privilèges élevé et tapez les commandes suivantes :

```
Entrez des informations d'identification pour Autre utilisateur ou appuyez sur la touche Échap pour changer d'utilisateur ou de méthode de connexion.
Nom d'utilisateur : exchangeslocal\Administrateur
Mot de passe : *****
Connectez-vous à exchangeslocal
Comment me connecter à un autre domaine ?
```

- On réinstalle les mêmes prérequis que sur les étapes précédentes :

```
PS C:\Install> Start-BitsTransfer -Source "https://download.microsoft.com/download/2/E/6/2E61CFA4-993B-4DD4-91DA-3737CD5CD6E3/vcredist_x64.exe" -Destination C:\Install\VS2013
PS C:\Install> Start-BitsTransfer -Source "https://download.microsoft.com/download/1/2/8/128E2E22-C1B9-44A4-BE2A-5859ED1D4592/rewrite_amd64_en-US.msi" -Destination C:\Install
PS C:\Install> Start-BitsTransfer -Source "http://download.microsoft.com/download/2/C/4/2C47A5C1-A1F3-4843-B9FE-84C0032C61EC/UcmaRuntimeSetup.exe" -Destination C:\Install
PS C:\Install> Start-BitsTransfer -Source "https://download.visualstudio.microsoft.com/download/pr/7afca223-55d2-470a-8edc-6a1739ae3252/abd170b4b0ec15ad0222a809b761a036/ndp48-x86-x64-allos-enu.exe" -Destination C:\Install
PS C:\Install> Start-BitsTransfer -Source "https://download.microsoft.com/download/1/6/B/16B06F60-3B20-4FF2-B699-5E9B7962F9AE/VSU_4/vcredist_x64.exe" -Destination C:\Install\VS2012
PS C:\Install> Start-Process -FilePath "C:\Install\ndp48-x86-x64-allos-enu.exe" -ArgumentList "/q" -Wait
PS C:\Install> Start-Process -FilePath "C:\Install\VS2012\vcredist_x64.exe" -ArgumentList "/q" -Wait
PS C:\Install>
```

- On lance l'installation du serveur Exchange :

```
PS E:\> E:\Setup.EXE /PrepareSchema /IAcceptExchangeServerLicenseTerms_DiagnosticDataON

Microsoft Exchange Server 2019 Mise à jour cumulative 12 Installation sans assistance

Copie des fichiers...
Copie du fichier terminée. Le programme d'installation va maintenant recueillir des informations supplémentaires nécessaires à l'installation.

Exécution de la vérification des conditions Microsoft Exchange Server

Analyse des conditions préalables                                TERMINÉ

Configuration de Microsoft Exchange Server

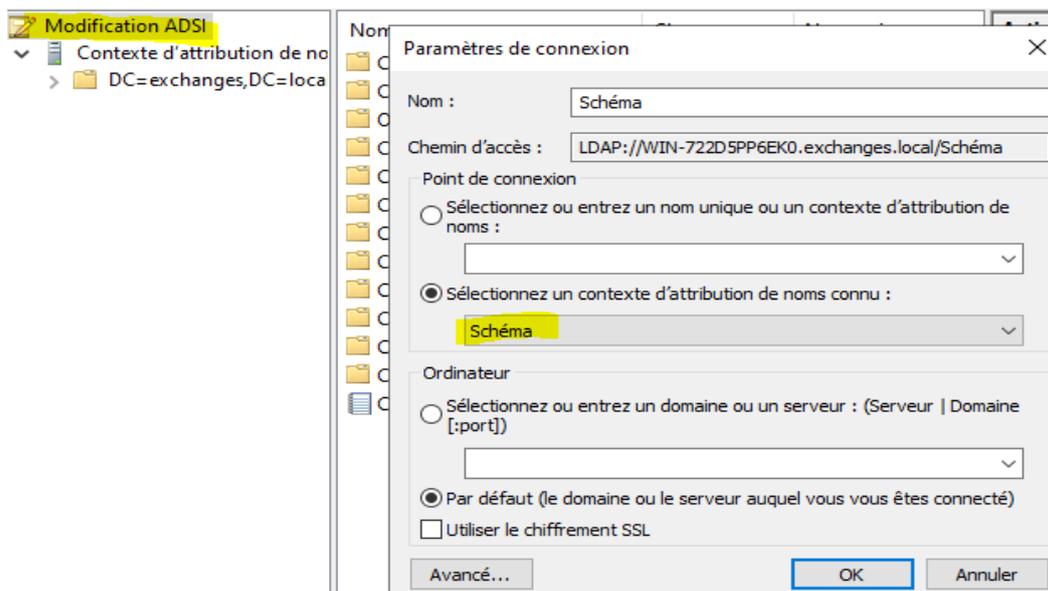
Extension du schéma Active Directory                            TERMINÉ

L'opération d'installation d'Exchange Server s'est terminée correctement.
```

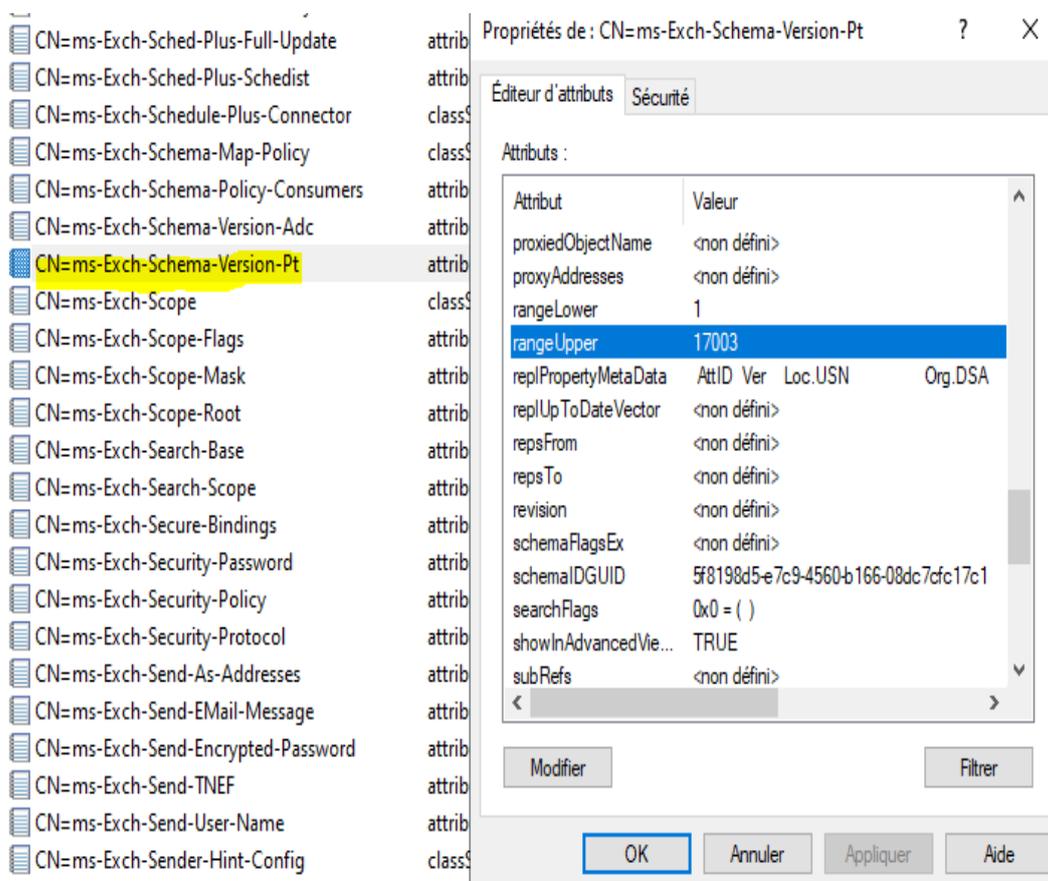
- On vérifie la version et le fonctionnement d'Exchange :

```
PS C:\> $root = [ADSI]"LDAP://RootDSE"
PS C:\> ([ADSI]("$root.schemaNamingContext)).rangeUpper
```

- On retourne sur l'AD, on ouvre 'Modification ADSI', donc on ajoute les schémas avec un clique droit sur Modification ADSI, on sélectionne Schéma :



- On recherche ms-Exch-Schema-Version-Pt, on ouvre ces propriétés et on vérifie le rangeUpper et elle devrait avoir une valeur de 17003 pour Exchanges 2019 CU8 et CU9 :



Préparation des partitions et configuration d'Active Directory

- Donc la partition du Schéma de l'AD est préparée pour Exchange et les modifications sont toutes répliquées dans toutes la forêt, on prépare la partition de la configuration de l'AD.
- Il faut toujours être connecté en admin au domaine pour que la commande suivante fonctionne :

```
PS E:\> E:\Setup.exe /PrepareAD /OrganizationName:exchanges /IAcceptExchangeServerLicenseTerms_DiagnosticDataON

Microsoft Exchange Server 2019 Mise à jour cumulative 12 Installation sans assistance

Copie des fichiers...
Copie du fichier terminée. Le programme d'installation va maintenant recueillir des informations supplémentaires
nécessaires à l'installation.

Exécution de la vérification des conditions Microsoft Exchange Server

    Analyse des conditions préalables                                100%

Le programme d'installation va préparer l'organisation pour Exchange Server 2019 à l'aide de « Setup /PrepareAD ».
Aucun rôle Exchange Server 2016 n'a été détecté dans cette topologie. Après cette opération, vous ne pourrez plus
installer de rôles Exchange Server 2016.
Pour plus d'informations, visitez : https://docs.microsoft.com/Exchange/plan-and-deploy/deployment-ref/readiness-checks?view=exchserver-2019

Le programme d'installation va préparer l'organisation pour Exchange Server 2019 à l'aide de « Setup /PrepareAD ».
Aucun rôle Exchange Server 2013 n'a été détecté dans cette topologie. Après cette opération, vous ne pourrez plus
installer de rôles Exchange Server 2013.
Pour plus d'informations, visitez : https://docs.microsoft.com/Exchange/plan-and-deploy/deployment-ref/readiness-checks?view=exchserver-2019

Configuration de Microsoft Exchange Server

    Préparation de l'organisation                                    TERMINÉ

L'opération d'installation d'Exchange Server s'est terminée correctement.
```

Préparation de la partition de Domaine

- Cette étape consiste à préparer la partition de Domaine Active Directory avant l'installation d'Exchange 2019.
- On exécute donc la commande suivante pour accepter le CLA et activer l'envoi de données à Microsoft :

Setup.exe /PrepareDomain /IAcceptExchangeServerLicenseTerms_DiagnosticDataON

```
PS E:\> E:\Setup.EXE /PrepareDomain /IAcceptExchangeServerLicenseTerms_DiagnosticDataON

Microsoft Exchange Server 2019 Mise à jour cumulative 12 Installation sans assistance

Copie des fichiers...
Copie du fichier terminée. Le programme d'installation va maintenant recueillir des informations supplémentaires nécessaires à l'installation.

Exécution de la vérification des conditions Microsoft Exchange Server

    Analyse des conditions préalables                                TERMINÉ

Configuration de Microsoft Exchange Server

    Préparer la progression du domaine                                TERMINÉ

L'opération d'installation d'Exchange Server s'est terminée correctement.
```

- On peut vérifier la version de la partition de domaine sur notre serveur AD, dans 'Modification ADSI' et on recherche le conteneur 'CN=Microsoft Exchange System Objects' et

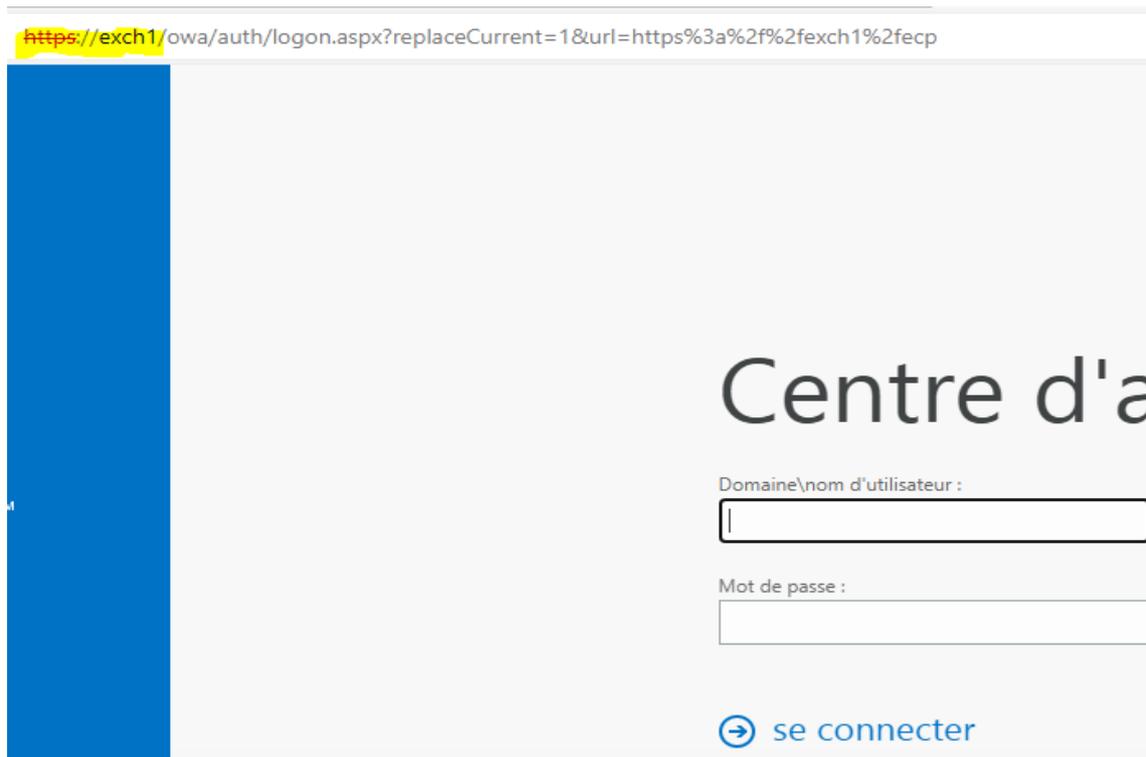
The screenshot shows the 'Modification ADSI' tool interface. On the left, a tree view shows the directory structure under 'Contexte d'attribution de no', with 'DC=exchanges,DC=loca' expanded to show 'CN=Microsoft Excha'. The right pane displays the 'Propriétés de : CN=Microsoft Exchange System Objects' dialog box. The 'Sécurité' tab is selected, and the 'Attributs' list shows the following attributes and values:

Attribut	Valeur
objectCategory	CN=ms-Exch-System-Objects-Container,CN=...
objectClass	top; container; msExchSystemObjectsContair
objectGUID	d6ada6b3-f87c-402f-bfd8-25fbc5c76f01
objectVersion	13243
otherWellKnownObje...	<non défini>
partialAttributeDeletio...	<non défini>
partialAttributeSet	<non défini>
proxiedObjectName	<non défini>
proxyAddresses	<non défini>
replicatedObjectVersion	<non défini>
replicationSignature	<non défini>
replPropertyMetaData	AttID Ver Loc.USN Org.DSA
replUpToDateVector	<non défini>
repsFrom	<non défini>

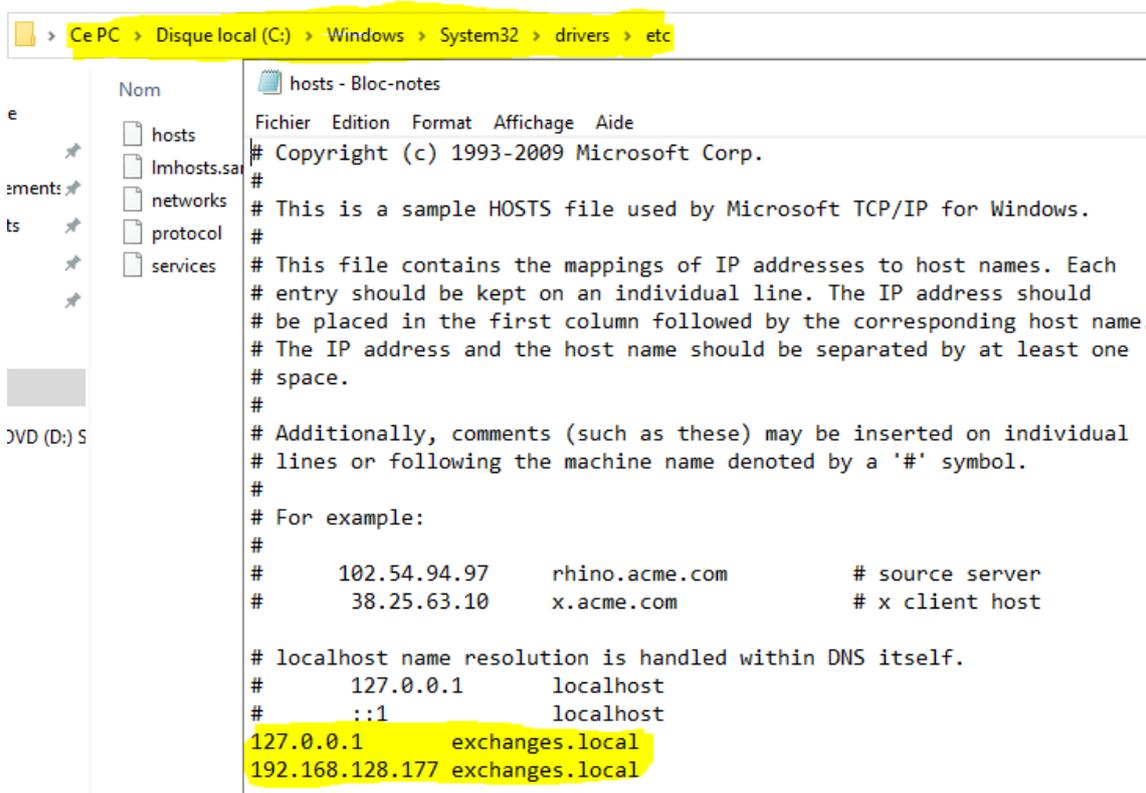
- On peut aussi vérifier en ligne de commande l'étape au-dessus :

```
PS C:\> $RootDSE= ([ADSI] "").distinguishedName
PS C:\> ([ADSI]("LDAP://CN=Microsoft Exchange System Objects, $RootDSE")).objectVersion
13243
```

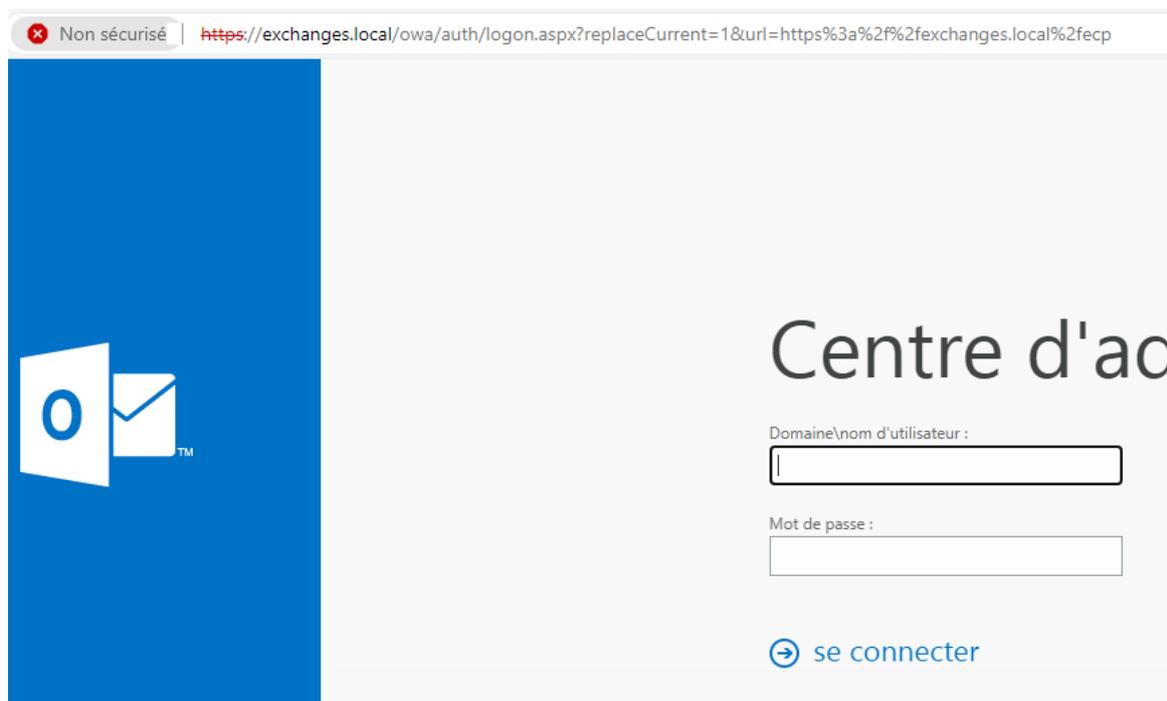

- On peut le tester avec le nom de la machine :



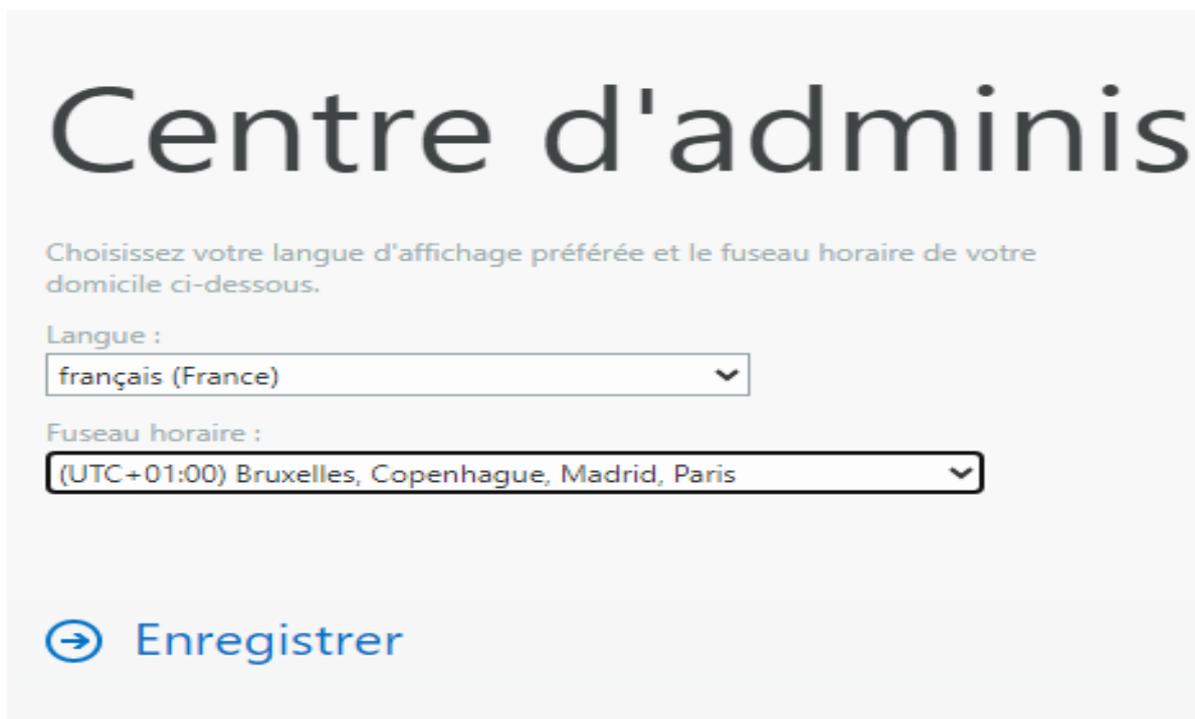
- On rajoute dans le fichier 'hosts' notre nom de domaine afin d'avoir accès en local à notre serveur Exchange :



- Une fois le fichier 'hosts' enregistré on a bien accès à l'interface web d'Exchange via notre nom de domaine 'exchanges.local/ecp' :



- On configure notre Exchange :



- On a bien accès à notre centre d'administration d'échange :

Demander un certificat SSL avec Win-ACME

- On télécharge le client Win-ACME qui va nous permettre de demander un certificat Let's Encrypt :

```
PS C:\Users\administrateur.EXCHANGES> Start-BitsTransfer -Source "https://github.com/win-acme/win-acme/releases/download/v2.2.7.1612/win-acme.v2.2.7.1612.x64.pluggable.zip" -Destination C:\Install
```

```
PS C:\Install> tar.exe -xf .\win-acme.v2.2.7.1612.x64.pluggable.zip
```

- On exécute wacs.exe avec la commande précédente :

```
PS C:\Install> start wacs.exe
```

```
win-acme 2.2.7.1612

A simple Windows ACMEv2 client (WACS)
Software version 2.2.7.1612 (release, pluggable, standalone, 64-bit)
Connecting to https://acme-v02.api.letsencrypt.org/...
Connection OK!
Scheduled task not configured yet
Please report issues at https://github.com/win-acme/win-acme

N: Create certificate (default settings)
M: Create certificate (full options)
R: Run renewals (0 currently due)
A: Manage renewals (0 total)
O: More options...
Q: Quit

Please choose from the menu:
```

- On choisit l'option "M" correspondante à "Create certificate (full options)" :
- On précise quels sont les noms DNS à couvrir avec le certificat. Pour cela, on indique "2" pour effectuer une saisie manuelle :
- Ici, on indique l'ensemble des adresses Web utilisées par votre serveur Exchange. Dans mon cas, ça sera l'adresse IP de mon Exchange. Puis, on a la possibilité d'indiquer un nom convivial pour le certificat mais ce n'est pas obligatoire : on peut appuyer directement sur Entrée :

```

N: Create certificate (default settings)
M: Create certificate (full options)
R: Run renewals (0 currently due)
A: Manage renewals (0 total)
O: More options...
Q: Quit

Please choose from the menu: M

Running in mode: Interactive, Advanced

Please specify how the list of domain names that will be included in the
certificate should be determined. If you choose for one of the "all bindings"
options, the list will automatically be updated for future renewals to
reflect the bindings at that time.

1: Read bindings from IIS
2: Manual input
3: CSR created by another program
C: Abort

How shall we determine the domain(s) to include in the certificate?: 2

Description:      A host name to get a certificate for. This may be a
                  comma-separated list.

Host: 192.168.128.177

```

- On choisit l'option 4 :

```

By default your source identifiers are covered by a single certificate. But
if you want to avoid the 100 domain limit, want to prevent information
disclosure via the SAN list, and/or reduce the operational impact of a single
validation failure, you may choose to convert one source into multiple
certificates, using different strategies.

1: Separate certificate for each domain (e.g. *.example.com)
2: Separate certificate for each host (e.g. sub.example.com)
3: Separate certificate for each IIS site
4: Single certificate
C: Abort

Would you like to split this source into multiple certificates?: 4

```

- En ce qui concerne la méthode de validation, on teste avec la méthode par défaut en effectuant le choix "2". Si cela ne fonctionne pas, on vérifie que notre serveur Web est bien accessible de l'extérieur (OWA depuis l'extérieur), sinon choisissez une autre méthode de validation :

```
The ACME server will need to verify that you are the owner of the domain
names that you are requesting the certificate for. This happens both during
initial setup *and* for every future renewal. There are two main methods of
doing so: answering specific http requests (http-01) or create specific dns
records (dns-01). For wildcard identifiers the latter is the only option.
Various additional plugins are available from
https://github.com/win-acme/win-acme/.

1: [http] Save verification files on (network) path
2: [http] Serve verification files from memory
3: [http] Upload verification files via FTP(S)
4: [http] Upload verification files via SSH-FTP
5: [http] Upload verification files via WebDav
6: [dns] Create verification records manually (auto-renew not possible)
7: [dns] Create verification records with acme-dns (https://github.com/joohoi/acme-dns)
8: [dns] Create verification records with your own script
9: [tls-alpn] Answer TLS verification request from win-acme
C: Abort

How would you like prove ownership for the domain(s)?: 2
```

- Ensuite, on doit choisir le type de clé privée à utiliser. On choisit "RSA Key" avec le choix "2" :
- Puis, l'assistant nous demande où on souhaite stocker le certificat donc on indique "4" pour qu'il soit stocké dans le **magasin des certificats de Windows** :
- On doit préciser le magasin à utiliser, on indique "2" pour que ce soit stocké dans le **magasin personnel** : ce qui est recommandé pour Exchange, d'après l'assistant :

```
After ownership of the domain(s) has been proven, we will create a
Certificate Signing Request (CSR) to obtain the actual certificate. The CSR
determines properties of the certificate like which (type of) key to use. If
you are not sure what to pick here, RSA is the safe default.

1: Elliptic Curve key
2: RSA key
C: Abort

What kind of private key should be used for the certificate?: 2

When we have the certificate, you can store in one or more ways to make it
accessible to your applications. The Windows Certificate Store is the default
location for IIS (unless you are managing a cluster of them).

1: IIS Central Certificate Store (.pfx per host)
2: PEM encoded files (Apache, nginx, etc.)
3: PFX archive
4: Windows Certificate Store (Local Computer)
5: No (additional) store steps

How would you like to store the certificate?: 4

1: [WebHosting] - Dedicated store for IIS
2: [My] - General computer store (for Exchange/RDS)
3: [Default] - Use global default, currently WebHosting

Choose store to use, or type the name of another unlisted store: 2
```

- Enfin, on indique "5" pour passer à la suite car il n'y pas d'autres endroits où nous avons besoin de stocker le certificat :

```

1: IIS Central Certificate Store (.pfx per host)
2: PEM encoded files (Apache, nginx, etc.)
3: PFX archive
4: Windows Certificate Store (Local Computer)
5: No (additional) store steps

Would you like to store it in another way too?: 5_

```

- Win-ACME propose de **mettre à jour les liaisons dans IIS de manière à intégrer le certificat SSL**. Pour que ce soit fait, on indique "1", puis "2" pour que ce soit mis en place au niveau du site "Exchange Back End" de IIS :

```

With the certificate saved to the store(s) of your choice, you may choose one
or more steps to update your applications, e.g. to configure the new
thumbprint, or to update bindings.

1: Create or update bindings in IIS
2: Start external script or program
3: No (additional) installation steps

Which installation step should run first?: 1

This plugin will update *all* binding using the previous certificate in both
Web and FTP sites, regardless of whether those bindings were created manually
or by the program itself. Therefore you'll never need to run this installation
step twice.

During initial setup, it will try to make as few changes as possible to IIS
to cover the source identifiers. If new bindings are needed, by default it
will create those at the same site where the HTTP binding for that host was
found.

1: Default Web Site
2: Exchange Back End

Choose site to create new bindings: <Enter>

Choose site to create new bindings: 2

```

- L'assistant nous pose la question suivante : "**Souhaitez-vous ajouter une étape d'installation supplémentaire ?**". La réponse est oui, nous devons exécuter un script supplémentaire donc on indique "2" :

```

1: Create or update bindings in IIS
2: Start external script or program
3: No (additional) installation steps

Add another installation step?: 2

```

- Il s'agit du script PowerShell "**ImportExchange.ps1**" intégré à Win-ACME donc précisez le chemin suivant :
- Après, on doit préciser les paramètres à utiliser lors de l'exécution de ce script. On Précise ceci pour Microsoft Exchange Server '{CertThumbprint}' 'IIS,SMTP,IMAP' 1 '{CacheFile}' '{CachePassword}' '{CertFriendlyName}' :

```
File: ./Scripts/ImportExchange.ps1

{CertCommonName}: Common name (primary domain name)
{CachePassword}: .pfx password
{CacheFile}: .pfx full path
{CertFriendlyName}: Certificate friendly name
{CertThumbprint}: Certificate thumbprint
{StoreType}: Type of store (e.g. CentralSsl, CertificateStore,
PemFiles, ...)
{StorePath}: Path to the store
{RenewalId}: Renewal identifier
{OldCertCommonName}: Common name (primary domain name) of the previously
issued certificate
{OldCertFriendlyName}: Friendly name of the previously issued certificate
{OldCertThumbprint}: Thumbprint of the previously issued certificate
{vault://json/mysecret}: Secret from the vault

Description: Parameters for the script to run after retrieving the
certificate. Refer to
https://win-acme.com/reference/plugins/installation/script
for further instructions.

Parameters: '{CertThumbprint}' 'IIS,SMTP,IMAP' 1 '{CacheFile}' '{CachePassword}' '{CertFriendlyName}'
```

- Ensuite, on doit indiquer "3" car nous n'avons pas d'autres étapes d'installation à ajouter.
- **A partir de là, le client Win-ACME va émettre une requête pour demander un certificat.** Si la requête est acceptée, le certificat sera mis en place dans le magasin de certificats du serveur et le serveur IIS sera configuré de manière à utiliser le certificat au sein des liaisons HTTPS. En complément, une tâche planifiée nommée "*win-acme renew (acme-v02.api.letsencrypt.org)*" sera créée sur le serveur pour assurer **le renouvellement automatique du certificat (valide 90 jours à chaque fois)**.
- Dans mon cas, je n'ai pas un domaine publique donc sa ne fonctionne pas car j'ai un domaine local !

```
1: Create or update bindings in IIS
2: Start external script or program
3: No (additional) installation steps

Add another installation step?: 3

Terms of service: C:\ProgramData\win-acme\acme-v02.api.letsencrypt.org\LE-SA-v1.3-September-21-2022.pdf

Open in default application? (y/n*) - yes

Unable to start application

Do you agree with the terms? (y*/n) - yes

Enter email(s) for notifications about problems and abuse (comma-separated): selim.akalan@campus-mewo.fr

Plugin Manual generated source 192.168.128.177 with 1 identifiers
Plugin Single created 1 order
[HTTP] Request completed with status BadRequest
Failed to create order: NewOrder request included invalid non-DNS type identifier: type "ip", value "192.168.128.177"

Create certificate failed, retry? (y/n*)
```

Conclusion

- En conclusion, la conception minutieuse de l'environnement Exchange 2019, la préparation des partitions et la configuration d'Active Directory, ainsi que l'installation en mode non surveillé ont été des étapes essentielles pour établir un système de messagerie fiable et performant. Ces processus ont permis de créer une base solide, garantissant la stabilité et la sécurité des communications au sein de notre TP. En suivant ces étapes avec rigueur, on a mis en place une infrastructure de messagerie qui n'est pas totalement terminée mais qui est déjà en très grande partie terminée.