# Installation du serveur Exchange

Installation

## Base

1. Installez le contrôleur de domaine selon la procédure sur ce serveur (uniquement le DC, aucun autres services)
2. Formatez la partition secondaire "D: Data"
3. Créez une zone DNS "owa.domaine.ch" sans mises à jour dynamique avec un hôte pointant sur le serveur Exchange en interne et créez cette entrée sur le DNS externe avec l'IP publique
4. Créez un DNS SRV avec comme nom d'hôte "\_autodiscover.\_tcp" et comme valeur "0 0 443 owa.domaine.ch" sur le DNS externe uniquement
5. Ouvrez les ports 80 et 443 sur le firewall et faire un NAT sur ce serveur
6. Installez "Microsoft Office 2010 Filter Packs 64 bits"
7. Ouvrez "Exchange Management Shell" en mode administrateur :
   1. Import-Module ServerManager
   2. Add-WindowsFeature NET-Framework,RSAT-ADDS,Web-Server,Web-Basic-Auth,Web-Windows-Auth,Web-Metabase,Web-Net-Ext,Web-Lgcy-Mgmt-Console,WAS-Process-Model,RSAT-Web-Server,Web-ISAPI-Ext,Web-Digest-Auth,Web-Dyn-Compression,NET-HTTP-Activation,RPC-Over-HTTP-Proxy -Restart
   3. Set-Service NetTcpPortSharing -StartupType Automatic
   4. Start-Service NetTcpPortSharing
8. Depuis le dossier d'installation de "MS Exchange 2010 SP1 MUI"
   1. setup.com /PrepareSchema
   2. setup.com /PrepareAD /OrganizationName:COMPANY
9. Installez les mises à jour Windows Update
10. Installez les hot-fixes suivantes :
    1. KB982867 : <http://code.msdn.microsoft.com/KB982867>
    2. KB979744 : <http://go.microsoft.com/fwlink/?linkid=3052&kbid=979744>
    3. KB983440 : <http://code.msdn.microsoft.com/KB983440>
    4. KB977020 : <http://support.microsoft.com/kb/977020>
11. Redémarrez le serveur
12. Lancez l'installation de "MS Exchange 2010 SP1 MUI"
    1. Installez toutes les langues depuis le bundle et téléchargez depuis Microsoft
    2. Installez Exchange
       1. Désactivez le rapport d'erreur
       2. Choisissez une installation personnalisée
       3. Installez uniquement les 3 premiers rôles
       4. Ne pas automatiser l'installation des composants manquants
       5. Ne pas activer les clients Outlook 2003
       6. URL pour utilisation depuis Internet : owa.domaine.ch
       7. Ne pas joindre le programme d'amélioration
13. Installez les mises à jour Windows Update
14. Ajoutez le groupe "Organization Management" pour l'utilisateur Admin
15. Redémarrez le serveur

## Configuration

1. Ouvrez "Exchange Management Shell" en mode administrateur :
   1. cd "C:\Program Files\Microsoft\Exchange Server\V14\Scripts"
   2. .\install-AntispamAgents.ps1
   3. Restart-Service MSExchangeTransport
2. Ouvrez "Exchange Management Console"
   1. Organization Configuration
      1. Mailbox
         1. Créez une nouvelle base de données de dossiers publics
            1. Name : "Public Folders DB1"
            2. Dossier : D:\Exchange\Public Folders DB1\Public Folders DB1.edb
            3. Logs : D:\Exchange\Public Folders DB1
         2. Ouvrez la base de données des boites aux lettres
            1. Renommez la base de données en "Mailbox DB1"
            2. Déplacez-là dans "D:\Exchange\Mailbox DB1\Mailbox DB1.edb" avec "D:\Exchange\Mailbox DB1" pour les logs
            3. Changez les limites :

Issue warning at : 25600 (25GB)

Prohibit send at : 30720 (30GB)

Prohibit send and receive at : 32768 (32GB)

* + - * 1. Attachez le "Default Offline Address Book" et "Public Folders DB1" à la base de données
    1. Client Access
       1. Activez la stratégie de mots de passe pour ActiveSync :
          1. Activez "Enable password recovery"
          2. Activez "Allow simple password"
          3. Number of failed attempts allowed : 10
          4. Minimum password length : 4
          5. Time without user input before password must be re-entered : 60
    2. Hub Transport
       1. Créez un nouveau "Accepted Domain" :
          1. Name : Internet Domain domaine.ch
          2. Accepted Domain : domaine.ch
          3. Type : Authoritative Domain
       2. Créez un nouveau "E-mail Address Policy" :
          1. Name : Address for users
          2. Recipient : domaine.local
          3. Include this recipient types : Users with Exchange mailboxes
          4. E-mail address local part : First name.lastname
          5. FQDN : domaine.ch
          6. E-mail address local part : Alias
          7. FQDN : domaine.ch
          8. Priorité : 1
       3. Créez un nouveau "E-mail Address Policy" :
          1. Name : Address for resources and groups
          2. Recipient : domaine.local
          3. Include this recipient types : Resource mailboxes, Mail-enabled groups
          4. E-mail address local part : Use alias
          5. FQDN : domaine.ch
          6. Priorité : 2
       4. Créez un nouveau "E-mail Address Policy" :
          1. Name : Address for external email
          2. Recipient : domaine.local
          3. Include this recipient types : Users with external e-mail addresses, Contacts with external e-mail addresses
          4. E-mail address local part : Use alias
          5. FQDN : domaine.local
          6. Priorité : 3
       5. Vérifiez bien que "Default Policy" dans "E-mail Address Policy" ne soit pas appliqué
       6. Créez un nouveau "Send Connector"
          1. Name : Internet Connector
          2. Intended use : Internet
          3. Address space : SMTP, \*, include all subdomains, cost 1
          4. Configurez le Smarthost sur le Barracuda ou le routage via les enregistrements MX
          5. Editez le connecteur et inscrivez le nom FQDN "owa.domaine.ch" avec une taille maximum des messages de 51200 (50MB)
       7. Modifiez le "Transport Settings"
          1. Maximum receive size : 51200 (50MB)
          2. Maximum send size : 51200 (50MB)
          3. Postmaster address : noreply@domaine.ch
          4. Ajoutez "127.0.0.1" dans "Message Delivery"
          5. Ajoutez ces codes DSN à la liste :

5.1.4

5.2.0

5.2.4

5.4.4

5.4.6

5.4.8

* + - 1. Désactivez toutes les fonctionnalités anti-spam sauf "IP Allow List" s'il y a un Barracuda

*Il est possible d'utiliser un certificat Wildcard, pour plusieurs domaines ou uniquement pour owa.domaine.ch. Le certificat mono-domaine nécessite la possibilité de créer des entrées DNS SRV sur le DNS publique.*

1. Dans la console IIS, effectuez une demande pour un nouveau certificat de domaine pour owa.domaine.ch avec le nom convivial "IMAP-POP" *\*nécessaire pour les services IMAP et POP car les wildcard ne sont pas acceptés*
2. Ouvrez "Exchange Management Console"
   1. Server Configuration
      1. Créez un nouveau certificat Exchange
         1. Friendly name : owa.domaine.ch
         2. Activez le wildcard "\*.domaine.ch"
         3. Utilisez le fichier .req afin d'effectuer une demande pour un certificat Wildcard (par ex Trustico RapidSSL Wildcard)
         4. Complétez la demande
         5. Assignez le certificat à IIS uniquement
      2. Client Access
         1. Introduisez la clé d'activation d'Exchange
         2. Activez Outlook Anywhere
            1. External host name : owa.domaine.ch
            2. Client authentification method : NTLM
         3. Modifiez "Outlook Web App"
            1. Inscrivez la même adresse interne qu'externe (<https://owa.domaine.ch/owa>)
            2. Authentification basée sur les formulaires, nom d'utilisateur seulement
         4. Modifiez "Exchange Control Panel"
            1. Inscrivez la même adresse interne qu'externe (<https://owa.domaine.ch/ecp>)
         5. Modifiez "Exchange ActiveSync"
            1. Inscrivez la même adresse interne qu'externe (<https://owa.domaine.ch/Microsoft-Server-ActiveSync>)
         6. Modifiez "Offline Address Book Distribution"
            1. Polling interval : 30
            2. Inscrivez la même adresse interne qu'externe (<https://owa.domaine.ch/OAB>)
         7. Modifiez "IMAP4" et "POP3"
            1. Maximum connections : 2000
            2. Maximum connections from a single IP address : 2000
            3. Définissez le nom X.509 avec owa.domaine.ch
         8. Assignez le certificat "IMAP-POP" aux services IMAP et POP
      3. Hub Transport
         1. Modifiez le connecteur "Default XXXXX"
            1. Maximum message size : 51200 (50MB)
            2. Désactivez toutes les références à IPv6
            3. Receive mail from remote servers : Plage DHCP du client
            4. Modifiez le nom en "Intranet DHCP with authentification"
         2. Modifiez le connecteur "Client XXXXX"
            1. Maximum message size : 51200 (50MB)
            2. Désactivez toutes les références à IPv6
            3. Modifiez le nom en "All network SMTPS with authentification"
         3. Créez un connecteur "Internal without authentification"
            1. Mode : Custom
            2. FQDN : SCOEXCH1.domaine.local
            3. Remote Network settings : Adresses IP des équipements qui n'auront pas besoin de s'authentifier mais pas le Barracuda ni le routeur
            4. Maximum message size : 51200 (50MB)
            5. Authentification : Aucune
            6. Permission Groups : Anonymous users
         4. Créez un connecteur "Internet"
            1. Mode : Internet
            2. FQDN : owa.domaine.ch
            3. Remote Network settings : Adresse IP du Barracuda ou 0.0.0.0 si le serveur reçoit en direct
            4. Maximum message size : 51200 (50MB)
            5. Authentification : TLS
            6. Permission Groups : Anonymous users
         5. Ajoutez dans la liste blanche de l'anti-spam les adresses IP internes autorisées à relayer dans authentification (HP Agents, …)
   2. Recipient Configuration
      1. Créez toutes les boîtes email, contacts, …
3. Ajoutez le composant "ASP" dans le rôle IIS
4. Dans le "Default Web Site" d'IIS.
   1. Supprimez la page welcome et iisstart
   2. Activez "HTTP Redirect"
      1. Redirect requests to this destination : <https://owa.domaine.ch/owa>
      2. Décochez "Redirect all requests to exact destination"
      3. Cochez "Only redirect requests to content in this folder"
   3. Désactivez "Redirect requests to this destination" pour les dossiers virtuels suivants :
      1. aspnet\_client
      2. Autodiscover
      3. ecp
      4. EWS
      5. Microsoft-Server-ActiveSync
      6. OAB
      7. PowerShell
      8. Public
      9. Rpc
      10. RpcWithCert
   4. Désactivez "Require SSL" sur le "Default Web Site"
   5. Réactivez "Require SSL" pour les dossiers virtuels suivants :
      1. Autodiscover
      2. ecp
      3. EWS
      4. Microsoft-Server-ActiveSync
      5. OAB
      6. Owa
      7. Public
      8. Rpc
      9. RpcWithCert
5. Supprimez le fichier "C:\Program Files\Microsoft\Exchange Server\V14\ClientAccess\OAB\web.config.xml"
6. Ouvrez "Exchange Management Shell" :
   1. Set-AutodiscoverVirtualDirectory -Identity \* -internalurl “https://owa.**lemanvisio**.ch/Autodiscover/Autodiscover.xml”
   2. Set-ClientAccessServer -Identity \* -AutodiscoverServiceInternalUri “https://owa.**lemanvisio**.ch/Autodiscover/Autodiscover.xml”
   3. Set-webservicesvirtualdirectory -Identity \* -internalurl “https://owa.**lemanvisio**.ch/EWS/Exchange.asmx”
   4. Get-ReceiveConnector "Internal without authentification" | Add-ADPermission -User “NT AUTHORITY\ANONYMOUS LOGON” -ExtendedRights “ms-Exch-SMTP-Accept-Any-Recipient”

*Si un certificat wildcard a été installé, exécutez la commande ci-dessous afin qu'Outlook Anywhere fonctionne sur les Windows XP en NTLM.*

* 1. Set-OutlookProvider EXPR -Server $null -CertPrincipalName msstd:\*.lemanvisio.ch

1. Si Exchange est installé sur un GC certains services ne démarrent pas automatiquement (<http://support.microsoft.com/kb/940845>) :
   1. Installez le fixe KB940845
   2. Choisissez pour tous les services "Microsoft Exchange" qui sont en démarrage automatiques "Restart the Service" en cas de problème après un délai de 3 minutes et réinitialisez le compteur des échecs après 1 jour
2. Redémarrez le serveur

*Ne pas oublier de décocher "Require that all senders are authenticated" pour les groupes devant recevoir du courrier depuis l'extérieur du réseau.*

*Cachez les utilisateurs et groupes systèmes afin qu'ils ne soient pas visibles dans Outlook.*

## Création automatique des comptes depuis un CSV

1. Créez un fichier à partir de la liste des utilisateurs en se basant sur le modèle "UserList.csv"
   1. Encodage UTF-8 impératif afin de conserver les accents
   2. Utilisation de virgules (pas de points-virgules comme Excel)
   3. Pas d'espaces superflus
   4. Possibilité de laisser les prénoms vides pour les comptes "génériques"
   5. Les comptes ne doivent pas exister dans l'Active Directory (l'activation uniquement de la messagerie ne se fait pas par cette commande)
2. Ouvrez "Exchange Management Shell" :
   1. Personnalisez ci-dessous "Password$" par le mot de passe souhaité pour l'ensemble des comptes
   2. Import-CSV C:\UserList.csv | ForEach-Object -Begin { $Temp = ConvertTo-SecureString "Password$" -asPlainText -force } -Process { If ($\_.FirstName -eq "") { New-Mailbox -LastName $\_.LastName -Initials "" -Alias $\_.Login -Name ($\_.LastName) -UserPrincipalName ($\_.Login + "@" + $\_.DomainName) -DisplayName ($\_.LastName) -OrganizationalUnit ($\_.DomainName + "/" + $\_.OU) -sAMAccountName $\_.Login -ResetPasswordOnNextLogon ([Bool]::Parse($\_.ChangePwdNextLogon)) -Password $Temp -DataBase $\_.DataBase | Set-User -Department $\_.Department } Else { New-Mailbox -FirstName $\_.FirstName -LastName $\_.LastName -Initials "" -Alias $\_.Login -Name ($\_.FirstName + " " + $\_.LastName) -UserPrincipalName ($\_.Login + "@" + $\_.DomainName) -DisplayName ($\_.FirstName + " " + $\_.LastName) -OrganizationalUnit ($\_.DomainName + "/" + $\_.OU) -sAMAccountName $\_.Login -ResetPasswordOnNextLogon ([Bool]::Parse($\_.ChangePwdNextLogon)) -Password $Temp -DataBase $\_.DataBase | Set-User -Department $\_.Department } }