# Installation du serveur contrôleur de domaine

Installation

## Base

1. Modifiez le réseau en réseau de bureau, configurez l'adresse IP "127.0.0.1" en second et en priorité le DNS de l'autre serveur Active Directory
2. Installez le rôle "Active Directory Domain Services"
3. Créez le domaine avec dcpromo, niveau fonctionnel maximal
4. Effectuez les mises à jour
5. Installez le serveur DHCP et le configurer, activez la tentative de conflit à 1, fournissez un identifiant pour les enregistrements DNS (compte dhcpserver)
6. Créez les zone de reverse du DNS, activez le "Aging" sur toutes les zones, activez le "Scavenging period" à 7 jours sur les serveurs, remontez les requêtes sur le routeur, fixez les adresses de réponses sur l'adresse IP principale du serveur
7. Déployez les autres contrôleurs de domaine et vérifiez la synchronisation des DNS
8. Configurez les sites Active Directory

## Active Directory

1. Créez la structure des OU (protégée des effacements accidentels)
   1. COMPANY
      1. Accounts
         1. Administrators
         2. External Users
         3. Internal Users
         4. Misc
         5. Rooms and Equipments
         6. Service Accounts
      2. Computers
         1. Desktops
            1. External
            2. Site location
         2. Laptops
            1. External
            2. Site location
      3. Contacts
      4. Groups
         1. Distribution Lists
         2. Security
      5. Printers
         1. Site location
      6. Servers
         1. Site location
            1. Standard
            2. Terminal Servers
   2. Tests
2. Créer un compte "Admin" pour l'administration du domaine avec les mêmes droits que "Administrator" dans l'OU "Administrators"
3. Importez tous les filtres WMI enregistrés
4. Créez les GPO suivantes selon les rapports enregistrés :
   1. All - NTP Configuration
   2. Computers - Add Computers Administrators \*Créez les groups nécessaires dans l'AD (avec nom court WksAdmin), personnalisez le script annexé
   3. Computers - Enable IPv4 priority on IPv6
   4. Computers - Enable NUMLOCK
   5. Computers - Enable RDP with NLA
   6. Computers - Enable RDP without NLA
   7. Computers - Firewall Advanced \*Importez la configuration
   8. Computers - Firewall Simple
   9. Computers - Misc Configuration \*Créez les groupes nécessaires dans l'AD
   10. Computers - Power Management
   11. DC - NTP Configuration
   12. Default Domain Controllers Policy
   13. Default Domain Policy
   14. Servers - Add Servers Administrators \*Créez les groups nécessaires dans l'AD (avec nom court SrvAdmin), personnalisez le script annexé
   15. Servers - Enable IPv4 priority on IPv6
   16. Servers - Enable RDP with NLA
   17. Servers - Firewall Advanced \*Importez la configuration
   18. Users - Change Background for Administrators \*Personnalisez le script annexé
   19. Users - IE Configuration
   20. Users - Misc Configuration
   21. Users - Office 2007 Configuration \*Ajoutez les ADM pour Office 2007
   22. Users - Office 2010 Configuration \*Ajoutez les ADM pour Office 2010

## Poubelle Active Directory

*La configuration de la poubelle Active Directory doit être effectuée sur le "Domain Naming Master" qui peut être identifié avec la commande "netdom query fsmo". L'utilisateur doit être présent dans les groupes "Enterprise Admins" et "Schema Admins". Le niveau fonctionnel du domaine doit être 2008R2.*

1. Ouvrez "Windows PowerShell" en mode administrateur :
   1. Import-Module ActiveDirectory
   2. Enable-ADOptionalFeature -Identity "CN=Recycle Bin Feature,CN=Optional Features,CN=Directory Service,CN=Windows NT,CN=Services,CN=Configuration,DC=domain,DC=local" -Scope ForestOrConfigurationSet -Target "domain.local"
2. Redémarrez le service "Active Directory Domain Services"

## Autorité de certification

1. Installez le rôle "Active Directory Certificate Services"
   1. Role Services : Certification Authority
   2. Type : Enterprise, Root CA
   3. Key character length : 4096
   4. Common name : NOM\_DU\_CLIENT-CA
   5. Validity : 5 Years
2. Créez un nouveau dossier C:\CertPub
   1. Droits System, Admin, Administrators Full Control
   2. Droits Users Read
   3. Copiez le certificat de la CA dans "C:\CertPub" sous CA.crt depuis "C:\Windows\System32\certsrv\CertEnroll"
3. Créez une zone DNS "ca.domaine.ch" sans mises à jour dynamique avec un hôte pointant sur le DC en interne et créez cette entrée sur le DNS externe avec l'IP publique
4. Ouvrez le port 8080 sur le firewall et faire un NAT sur ce serveur
5. Ouvrez le port 8080 sur le firewall Windows du serveur avec pour nom "Certificate Webservice"
6. Installez le rôle "Web Server (IIS)" par défaut
7. Créez un nouveau site web dans IIS
   1. Site name : CertPub
   2. Physical path : C:\CertPub
   3. Host name : ca.domaine.ch
   4. Type : http, port 8080
   5. Activez "Allow double escaping" dans "Request Filtering"
   6. Redémarrez IIS
8. Allez dans les propriétés de la CA, onglet "Extensions", "CDP"
   1. Ajoutez le chemin : C:\CertPub\<CaName><CRLNameSuffix><DeltaCRLAllowed>.crl
      1. Activez "Publish CRLs" et "Publish Delta CRLs"
   2. Ajoutez le chemin : [http://ca.domaine.ch:8080/<CaName><CRLNameSuffix><DeltaCRLAllowed>.crl](http://ca.domaine.ch:8080/%3cCaName%3e%3cCRLNameSuffix%3e%3cDeltaCRLAllowed%3e.crl)
      1. Activez "Include in CRLs" et "Include in the CDP extension"
9. Allez dans les propriétés de la CA, onglet "Extensions", "AIA"
   1. Ajoutez le chemin : C:\CertPub\CA.crt
   2. Ajoutez le chemin : <http://ca.domaine.ch:8080/CA.crt>
      1. Activez "Include in the AIA extension of issued certificates"
10. Dans "Revokated Certificates", publiez les informations de révocation

*Permet la création d'un certificat machine depuis la console MMC d'un serveur puis l'exportation pour un usage depuis un serveur non-IIS.*

1. Copiez le template de certificat "Web Server" en tant que "Web Server Exportable" de type "Windows Server 2008"
   1. "General"
      1. Validity period : 5 years
   2. "Security"
      1. Ajoutez le nom d'une machine ayant le droit de générer les certificats (par ex : UPD1) avec le droit "Enroll"
2. Copiez le template de certificat "Code Signing" en tant que "WSUSThirdPartySigning" de type "Windows Server 2003"
   1. "Request Handling"
      1. Activez "Allow private key to be exported"
      2. Activez "Prompt the user during enrollment"
   2. "Subject Name"
      1. Activez "Supply in the request"
   3. "Security"
      1. Ajoutez le nom d'un utilisateur ayant le droit de générer les certificats avec le droit "Enroll"
3. Déployez les modèles de certificat sur la CA :
   1. Web Server Exportable
   2. WSUSThirdPartySigning
4. Créez les GPO suivantes selon les rapports enregistrés :
   1. All - Certificates Configuration

## VPN SSTP + PPTP

1. Installez le rôle "Network Policy and Access Services", choisissez "Network Policy Server" et "Remote Access Service"
2. Installez la fonctionnalité "Connection Manager Administration Kit"
3. Créez un groupe "SG\_VPN-SSTP Users" et un groupe "SG\_VPN-PPTP Users"
4. Effectuez une demande pour un nouveau certificat de domaine depuis IIS pour "vpn.domaine.ch"
5. Configurez le "Routing and Remote Access", mode "Custom configuration", choisir uniquement "VPN access"
   1. Désactivez le routage IPv6, utilisez l'authentification EAP et MS-CHAP v2 uniquement, choisissez le routage "Local area network (LAN) routing only", choisissez le certificat "vpn.domaine.local"
   2. Augmentez le nombre de ports SSTP et PPTP au nombre d'utilisateur, désactivez les autres ports
   3. Activez le relai DHCP sur l'adresse IP du serveur (pas 127.0.0.1)
6. Créez une zone DNS "vpn.domaine.ch" sans mises à jour dynamique avec un hôte pointant sur le DC en interne et créez cette entrée sur le DNS externe avec l'IP publique
7. Ouvrez le port 443 sur le firewall et faire un NAT sur ce serveur
8. Ouvrez le port 1723 + GRE sur le firewall et faire un NAT sur ce serveur
9. Dans NPS :
   1. Supprimez toutes les stratégies "Connection Request Policies" et "Network Policies"
   2. Créez une stratégie "Enable VPN SSTP access" dans "Connection Request Policies"
      1. Type of network access server : RAS VPN-Dial up
      2. Conditions :
         1. Tunnel Type : SSTP
         2. Framed Protocol : PPP
         3. NAS Port Type : Virtual (VPN)
      3. Settings :
         1. Authentification Methods :
            1. Microsoft: Protected EAP (PEAP)

Activez uniquement EAP-MSCHAP v2

Activez "Enable Fast Reconnect"

* + - * 1. Aucune autre authentification possible
  1. Créez une stratégie "Enable VPN PPTP access" dans "Connection Request Policies"
     1. Type of network access server : RAS VPN-Dial up
     2. Conditions :
        1. Tunnel Type : PPTP
        2. Framed Protocol : PPP
        3. NAS Port Type : Virtual (VPN)
     3. Settings :
        1. Authentification Methods :
           1. Microsoft Encrypted Authentification version 2 (MS-CHAP v2)
           2. User can change password after it has expired
           3. Aucune autre authentification possible
  2. Créez une stratégie "Rules to get SSTP VPN access" dans "Network Policies"
     1. Access permission : Grant access
     2. Type of network access server : RAS VPN-Dial up
     3. Conditions :
        1. Windows Groups : DOMAIN\SG\_VPN-SSTP Users
        2. Tunnel Type : SSTP
     4. Constraints :
        1. Authentification Methods :
           1. Microsoft: Protected EAP (PEAP)

Activez uniquement EAP-MSCHAP v2

Activez "Enable Fast Reconnect"

* + - * 1. Aucune autre authentification possible
      1. NAS Port Type : Virtual (VPN)
    1. Settings :
       1. Standard :
          1. Framed-Protocol : PPP
          2. Service-Type : Framed
       2. Multilink :
          1. Server settings determine Multilink usage
       3. Encryption :
          1. Uniquement 128-bit
  1. Créez une stratégie "Rules to get PPTP VPN access" dans "Network Policies"
     1. Access permission : Grant access
     2. Type of network access server : RAS VPN-Dial up
     3. Conditions :
        1. Windows Groups : DOMAIN\SG\_VPN-PPTP Users
        2. Tunnel Type : PPTP
     4. Constraints :
        1. Authentification Methods :
           1. Microsoft Encrypted Authentification version 2 (MS-CHAP v2)
           2. User can change password after it has expired
           3. Aucune autre authentification possible
        2. NAS Port Type : Virtual (VPN)
     5. Settings :
        1. Standard :
           1. Framed-Protocol : PPP
           2. Service-Type : Framed
        2. Multilink :
           1. Server settings determine Multilink usage
        3. Encryption :
           1. Uniquement 128-bit

1. Redémarrez le service RRAS
2. Exécutez "Connection Manager Administration Kit" et créez un nouveau profil
   1. OS : Windows 7 ou Vista
   2. Service name : Company SSTP VPN x64
   3. File name : COVSO64
   4. Ne pas spécifier de "Realm Name"
   5. Activez "Phone book from this profile"
   6. VPN server name : vpn.domaine.ch
   7. Editez l'entrée VPN :
      1. Activez uniquement IPv4
      2. Désactivez la passerelle par défaut pour le client
      3. Activez uniquement le VPN SSTP
      4. Activez l'encryption maximum
      5. Activez EAP
         1. Connect to these servers : vpn.domaine.ch
         2. Trusted Root Certification Authorities : choisissez la CA
         3. Laissez le reste par défaut
      6. DNS suffixe : domaine.local
   8. Décochez le téléchargement automatique de phone book
   9. Modifiez l’entrée personnalisée suivante :
      1. Nom du fichier : \*.cms
      2. Nom de section : Connection Manager
      3. Nom de la clé : Dialup
      4. Valeur : 0
3. Exécutez "Connection Manager Administration Kit" et créez un nouveau profil
   1. OS : Windows 7 ou Vista
   2. Service name : Company SSTP VPN DOM x64
   3. File name : COVSI64
   4. Ne pas spécifier de "Realm Name"
   5. Activez "Phone book from this profile"
   6. VPN server name : vpn.domaine.ch
   7. Editez l'entrée VPN :
      1. Activez uniquement IPv4
      2. Désactivez la passerelle par défaut pour le client
      3. Activez uniquement le VPN SSTP
      4. Activez l'encryption maximum
      5. Activez EAP
         1. Connect to these servers : vpn.domaine.ch
         2. Trusted Root Certification Authorities : choisissez la CA
         3. Laissez le reste par défaut
      6. DNS suffixe : domaine.local
   8. Décochez le téléchargement automatique de phone book
   9. Ajoutez l'action personnalisée :
      1. Description : Map network drive
      2. Program to run : DriveMapSSTPInDom.exe
      3. Action type : Post-connected
      4. Laissez le reste par défaut
   10. Ajoutez l'action personnalisée :
       1. Description : Update Group Policies
       2. Program to run : GroupPolicyUpdate.exe
       3. Action type : Post-connected
       4. Laissez le reste par défaut
   11. Ajoutez l'action personnalisée :
       1. Description : Unmap network drive
       2. Program to run : DriveUnMap.exe
       3. Action type : Disconnect
       4. Laissez le reste par défaut
   12. Ajoutez les fichiers personnalisés :
       1. DriveMapSSTPInDom.exe
       2. DriveUnMap.exe
       3. GroupPolicyUpdate.exe
   13. Modifiez l’entrée personnalisée suivante :
       1. Nom du fichier : \*.cms
       2. Nom de section : Connection Manager
       3. Nom de la clé : Dialup
       4. Valeur : 0
4. Exécutez "Connection Manager Administration Kit" et créez un nouveau profil
   1. OS : Windows XP
   2. Service name : Company PPTP VPN x64
   3. File name : COVPO64
   4. Ne pas spécifier de "Realm Name"
   5. Activez "Phone book from this profile"
   6. VPN server name : vpn.domaine.ch
   7. Editez l'entrée VPN :
      1. Activez uniquement IPv4
      2. Désactivez la passerelle par défaut pour le client
      3. Activez uniquement le VPN PPTP
      4. Activez l'encryption maximum
      5. Activez Microsoft CHAP Version 2 (MS-CHAP v2)
   8. Décochez le téléchargement automatique de phone book
   9. Modifiez l’entrée personnalisée suivante :
      1. Nom du fichier : \*.cms
      2. Nom de section : Connection Manager
      3. Nom de la clé : Dialup
      4. Valeur : 0
5. Exécutez "Connection Manager Administration Kit" et créez un nouveau profil
   1. OS : Windows XP
   2. Service name : Company PPTP VPN DOM x64
   3. File name : COVPI64
   4. Ne pas spécifier de "Realm Name"
   5. Activez "Phone book from this profile"
   6. VPN server name : vpn.domaine.ch
   7. Editez l'entrée VPN :
      1. Activez uniquement IPv4
      2. Désactivez la passerelle par défaut pour le client
      3. Activez uniquement le VPN PPTP
      4. Activez l'encryption maximum
      5. Activez Microsoft CHAP Version 2 (MS-CHAP v2)
   8. Décochez le téléchargement automatique de phone book
   9. Ajoutez l'action personnalisée :
      1. Description : Map network drive
      2. Program to run : DriveMapPPTPInDom.exe
      3. Action type : Post-connected
      4. Laissez le reste par défaut
   10. Ajoutez l'action personnalisée :
       1. Description : Update Group Policies
       2. Program to run : GroupPolicyUpdate.exe
       3. Action type : Post-connected
       4. Laissez le reste par défaut
   11. Ajoutez l'action personnalisée :
       1. Description : Unmap network drive
       2. Program to run : DriveUnMap.exe
       3. Action type : Disconnect
       4. Laissez le reste par défaut
   12. Ajoutez les fichiers personnalisés :
       1. DriveMapPPTPInDom.exe
       2. DriveUnMap.exe
       3. GroupPolicyUpdate.exe
   13. Modifiez l’entrée personnalisée suivante :
       1. Nom du fichier : \*.cms
       2. Nom de section : Connection Manager
       3. Nom de la clé : Dialup
       4. Valeur : 0
6. Récupérez les paquets depuis "C:\Program Files\CMAK\Profiles"
7. Effectuez la même chose depuis le point 12 sur un Windows 7 32 bits afin de générer les paquets d'installation 32 bits (x32)
8. Créez les paquets d'installations automatiques en adaptant les configurations selon le client
9. Créez les GPO suivantes selon les rapports enregistrés :
   1. Computers - Disable SSTP Certificate Checking \*ne pas activer sauf si nécessaire
   2. Users - Deploy VPN automatically \*Créez le script AutoIt correspondant et copiez les kits VPN dans le SYSVOL
10. Effectuez les mises à jour

*Il faut au minimum Windows VISTA SP1 pour que la connexion SSTP fonctionne. Attention à exclure des antivirus ESET NOD32 les paquets d'installation qui sont reconnus comme des malwares.*

## Raccourcis pour gestion des scripts

1. Créez le dossier "C:\Windows\SYSVOL\sysvol\domaine.local\scripts\Scripts"
2. Dans ce dossier créez les raccourcis suivants :
   1. "Local SYSVOL" pointant sur "C:\Windows\SYSVOL\sysvol\domaine.local"
   2. Toutes les GPO contenant des scripts AutoIt (pointer dans le dossier du script directement) :
      1. Computers - Add Computers Administrators
      2. Computers - NOD32 deployment
      3. Computers - Strategic Deployment
      4. Servers - Add Servers Administrators
      5. Users - Change Background for Administrators
      6. Users - Define Default Printer
      7. …

## Délégation de la gestion des OU

1. Créez un groupe "SG\_OU Administrators"
2. Effectuez une délégation sur les OU suivantes "Accounts/External Users", "Accounts/Internal Users"
   1. Cliquez sur "Delegate Control" sur l'OU
      1. Choisissez le groupe "SG\_OU Administrators"
      2. Choisissez de déléguer les droits suivants :
         1. Reset user passwords and force password change at next logon
         2. Read all user information
         3. Modify the membership of a group
   2. Cliquez sur "Delegate Control" sur l'OU *\*permet d'activer et de désactiver un compte utilisateur*
      1. Choisissez le groupe "SG\_OU Administrators"
      2. Choisissez "Create a custom task to delegate"
      3. Choisissez "Only the following objects in the folder puis "User objects" uniquement
      4. Cochez "Property-specific"
      5. Cochez "Read userAccountControl" et "Write userAccountControl"
3. Effectuez une délégation sur l'OU "Groups"
   1. Cliquez sur "Delegate Control" sur l'OU
      1. Choisissez le groupe "SG\_OU Administrators"
      2. Choisissez de déléguer les droits suivants :
         1. Modify the membership of a group
4. Créez des consoles MMC sur les PC des administrateurs avec une vue sur les OU "Accounts/External Users", "Accounts/Internal Users", "Groups/Distribution Lists" et "Groups/Security"

## Création des comptes utilisateurs

1. Créez les comptes des utilisateurs dans "Exchange Management Console/Recipient Configuration/Mailbox" :
   1. Organizational Unit : domaine.local/COMPANY/Accounts/Users
   2. First name : Prénom *\*Indiquez uniquement dans Last name si compte pas nominatif*
   3. Initials :
   4. Last name : NOMDEFAMILLE
   5. User logon name : pno
   6. Alias : pno
   7. Ne pas créez d'archive
   8. Ajoutez ensuite les éventuelles adresses emails supplémentaires

## Récupération d'objets Active Directory supprimé

*Les objets Active Directory peuvent être récupérés (par défaut) durant 180 jours, ensuite ils sont supprimés physiquement. Quelques exemples de commande…*

**Recherche d'un utilisateur supprimé :**

Get-ADObject -Filter {(SamAccountName -like "username") -and (ObjectClass -eq "user")} -IncludeDeletedObjects

**Recherche d'un ordinateur supprimé :**

Get-ADObject -Filter {(SamAccountName -like "computername") -and (ObjectClass -eq "computer")} -IncludeDeletedObjects

**Recherche de tous les objets utilisateurs supprimés :**

Get-ADObject -Filter {objectClass -eq "user"} -IncludeDeletedObjects -SearchBase "CN=Deleted Objects,DC=domain,DC=local" | ft

**Recherche de tous les objets ordinateurs supprimés :**

Get-ADObject -Filter {objectClass -eq "computer"} -IncludeDeletedObjects -SearchBase "CN=Deleted Objects,DC=domain,DC=local" | ft

**Restauration d'un objet :**

Restore-ADObject XXX