TECHNOLOGIES MICROSOFT

Hervé Franco

Table des matières

[1 ACTIVE DIRECTORY 4](#_Toc24464024)

[1.1 Definition 4](#_Toc24464025)

[1.1.1 Active Directory (AD) 4](#_Toc24464026)

[1.1.2 Domaine 4](#_Toc24464027)

[1.1.3 Forêt 4](#_Toc24464028)

[1.2 Eléments dans un domaine 5](#_Toc24464029)

[1.3 Stockage de la base AD 5](#_Toc24464030)

[1.4 Réplication AD 6](#_Toc24464031)

[1.5 Schéma d’un AD 6](#_Toc24464032)

[1.5.1 Structure physique et structure logique 7](#_Toc24464033)

[1.5.2 Schéma de réplication 7](#_Toc24464034)

[1.5.3 Utilisateurs, groupes et OU 8](#_Toc24464035)

[1.6 CONSOLES DISPONIBLES DANS WINDOWS SERVER POUR ADMINISTRER ACTIVE DIRECTORY 10](#_Toc24464036)

[1.6.1 Console Utilisateurs et Ordinateurs AD 10](#_Toc24464037)

[1.6.2 Console Sites et services AD 11](#_Toc24464038)

[1.6.3 Console Gestion de stratégie de groupe 12](#_Toc24464039)

[2 Installation d’un contrôleur de domaine AD 13](#_Toc24464040)

[2.1 Pré requis et bonnes pratiques serveur 13](#_Toc24464041)

[2.2 Installation d’un serveur AD sous 2012 server 13](#_Toc24464042)

[2.3 Installation d’un premier contrôleur de domaine (promotion) 14](#_Toc24464043)

[2.4 Login en domaine 15](#_Toc24464044)

[2.4.1 Se logger en local 15](#_Toc24464045)

[2.4.2 Se logger sur le domaine 15](#_Toc24464046)

[2.5 Vérification du fonctionnement des DNS et DNS Reverse en AD 15](#_Toc24464047)

[2.5.1 Fonctionnement 15](#_Toc24464048)

[2.5.2 Création de la zone DNS Reverse 17](#_Toc24464049)

[3 Joindre un poste client ou un serveur non contrôleur de domaine au domaine 22](#_Toc24464050)

[3.1 Joindre une machine à partir de l’interface graphique 22](#_Toc24464051)

[3.2 Méthodes alternatives 26](#_Toc24464052)

[4 Partage et droits NTFS 27](#_Toc24464053)

[4.1 Partage administratif 27](#_Toc24464054)

[4.2 Partage de dossiers 27](#_Toc24464055)

[4.3 Création d’un partage réseau 28](#_Toc24464056)

[4.4 Attribution de droits et de restrictions à un partage via NTFS 30](#_Toc24464057)

[4.4.1 Ajout des utilisateurs aux groupes 30](#_Toc24464058)

[4.4.2 Attribution de droits aux groupes 32](#_Toc24464059)

[5 Changement d’adressage IP sur des contrôleurs de domaines AD 39](#_Toc24464060)

[6 Mise en place d’une GPO sur un domaine AD 40](#_Toc24464061)

[6.1 Définition 40](#_Toc24464062)

[6.2 Consoles nécessaires pour mettre en place un GPO 40](#_Toc24464063)

[6.3 Contenu d’une GPO 41](#_Toc24464064)

[6.4 Exemple de mise en place d’une GPO 42](#_Toc24464065)

[6.4.1 Ouvrir la console Gestion des stratégies de groupe 42](#_Toc24464066)

[6.4.2 Modification de la GPO Default Domain Policy 43](#_Toc24464067)

[7 LES ROLES FSMO 44](#_Toc24464068)

[7.1 Transférer un rôle FSMO vers un autre contrôleur de domaine 44](#_Toc24464069)

[**7.2** **En powerShell** 46](#_Toc24464070)

[8 Déplacement de la base AD vers un autre dossier ou disque 46](#_Toc24464071)

[8.1 Vérifier l’emplacement des fichiers AD 46](#_Toc24464072)

[8.2 Déplacement des fichiers AD 47](#_Toc24464073)

[8.3 Définir un emplacement de sauvegarde de l’AD 47](#_Toc24464074)

[9 DEPLOIEMENT D’UNE APPLICATION VIA UNE GPO 49](#_Toc24464075)

# ACTIVE DIRECTORY

## Definition

### Active Directory (AD)

Active directory est un service d’annuaire basé sur le protocole LDAP (389 ou 636 en SSL) permettant :

* De gérer de manière centralisée l’ensemble des utilisateurs dans une entreprise
* De définir des droits et des sécurités sur le domaine
* D’appliquer à des groupes d’utilisateurs ou de machines des politiques de sécurité (GPO) par exemple : Définir l’expiration du mot de passe, déployer un logiciel sur le poste utilisateur….
* Mettre en place une tolérance de pannes en déployant AD sur plusieurs serveurs (Contrôleurs de domaine – Domain Controllers DC)
* Synchroniser des noms de domaines dans les zones DNS (tolérance de panne DNS)
* Synchroniser des fichiers utilisateurs à travers l’AD via le rôle DFSr

### Domaine

Un domaine est un espace de sécurité délimité dans lequel chaque utilisateur va avoir des droits.

On distingue l’architecture physique de l’architecture logique.

Ex. Dans une forêt, je possède une maison avec des chambres d’hôtes. Ce domaine est entouré d’une clôture et possède un portail. Il porte un nom. Pour rentrer dans le domaine, il faut des clefs.

En tant que propriétaire du domaine (administrateur), je donne les clefs à qui je veux et ensuite il pourra entrer.

Je peux interdire à telle ou telle personne l’accès à une partie du domaine.

Je peux autoriser un groupe ou une personne à accéder à telle ou telle ressource (ex la piscine)

Le domaine c’est corp.contoso.com (nom de domaine, FQDN Full Qualified Domain Name).

Le domaine AD a une clôture comme la maison, l’administrateur (le propriétaire) possède les clefs et attribue les accès aux utilisateurs (personnel, les invités, etc….). L’administrateur attribue des permissions d’utilisation des ressources (dossiers partagés par exemple).

Les chambres d’hôte peuvent représenter ici les ordinateurs qui sont joints au domaine. La maison principale c’est le serveur.

### Forêt

On appelle une forêt, un élément AD qui regroupe plusieurs domaines. Les domaines peuvent être liés ou pas. On appelle une liaison entre deux domaines, une relation d’approbation.

## Eléments dans un domaine

On trouve dans un domaine les éléments suivants :

* Un ou plusieurs contrôleurs de domaine (DC Domain Controller)
  + Un DC peut être GC (Global Catalog, catalogue global)
  + Un DC peut être RODC (Read Only Domain Controler, Controleur de domaine en lecture seule)
  + Un DC possède des rôles FSMO (Flexible Single Master Operation)
* Des unités d’organisation (UO en français, OU – Organisational Unit)
  + Une unité d’organisation peut regrouper des ordinateurs, des utilisateurs, des groupes de sécurité, des ressources partagées, des imprimantes (OBJETS)
  + Une unité d’organisation permet d’organiser l’annuaire AD en fonction de l’organisation de l’entreprise
  + On applique sur une OU une GPO (Group Policy Object), une stratégie de groupe qui permet d’appliquer à l’ensemble de l’OU une politique de sécurité (ex. Déployer Firefox pour tous les utilisateurs qui sont dans l’OU).
* Des utilisateurs
* Des groupes de sécurité, qui permettent de regrouper des utilisateurs entre eux (par exemple, le groupe Commercial regroupe les membres du service commercial). Le groupe de sécurité permet de gérer via les partages de dossiers les droits sur chaque dossier (droits NTFS)
* Des stratégies de groupe (GPO), **une stratégie de groupe est un ensemble de règles appliquées soit au domaine dans son ensemble, soit aux contrôleurs de domaine, soit à des unités d’organisation (OU).** 
  + Chaque stratégie comporte une partie machine et une partie utilisateur
  + Elle modifie directement des éléments du registre windows (HKLM et HKCU – Hkey Local Machine et Hkey Current user)
  + La gpo permet à l’administrateur de gagner du temps, par exemple :
    - Supprimer l’ensemble des pares-feux d’un parc de machine
    - Déployer un logiciel sur un ensemble de postes
    - Exécuter à l’ouverture des machines des scripts

## Stockage de la base AD

La base AD est stockée par défaut dans c:\windows\NTDS dans Windows 2012R2

Ce répertoire doit être changé à l’installation de l’AD.

Il faut placer ce répertoire sur un autre disque que le disque système.

Le dossier SYSVOL est répliqué entre les DC AD et contient les GPO et les scripts.

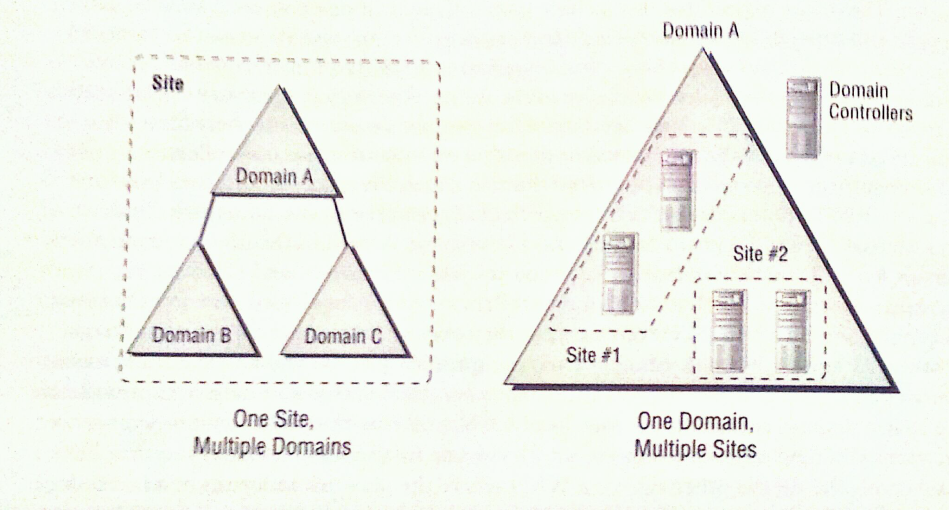
## Réplication AD

On appelle réplication AD, la copie en temps réel des modifications effectuées sur un contrôleur de domaine vers l’ensemble des autres contrôleurs de domaine.

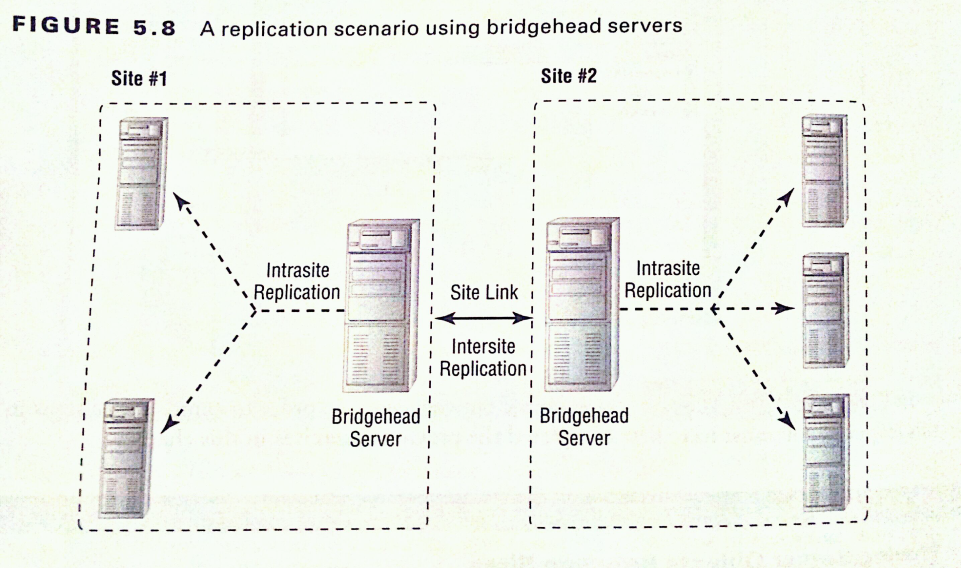
## Schéma d’un AD



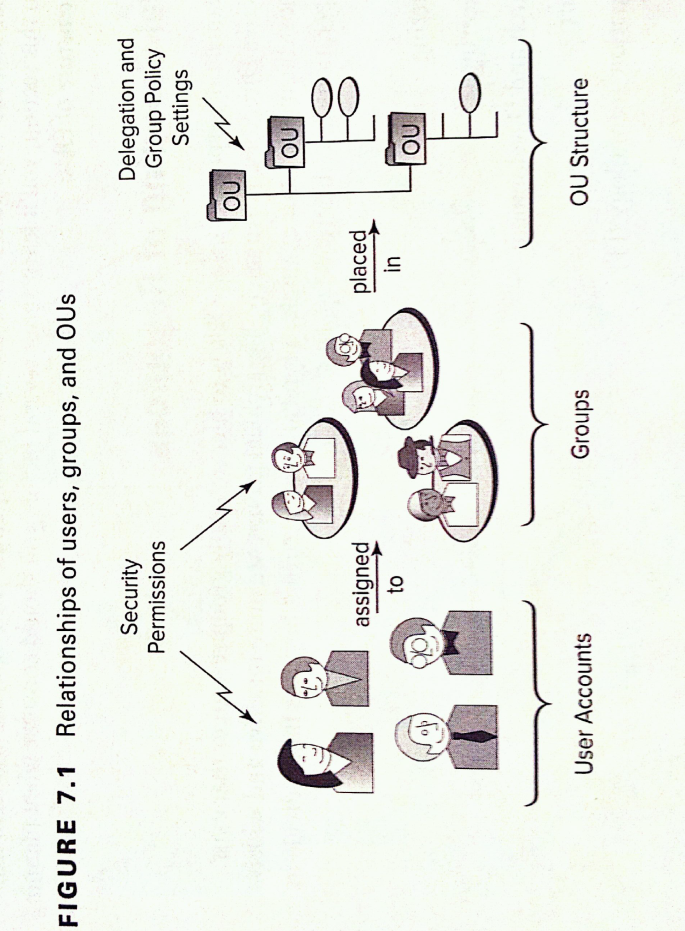
### Structure physique et structure logique

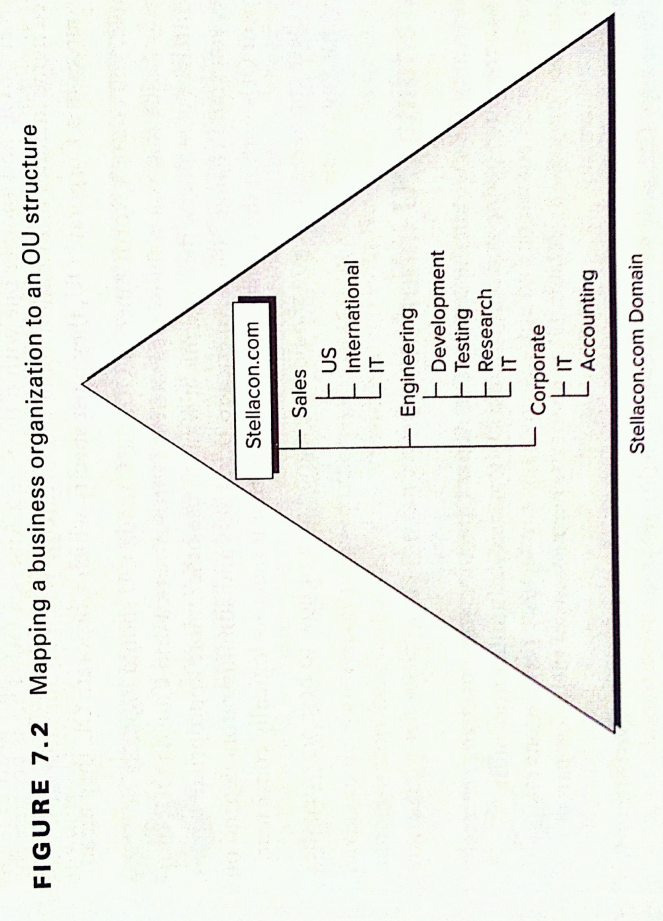


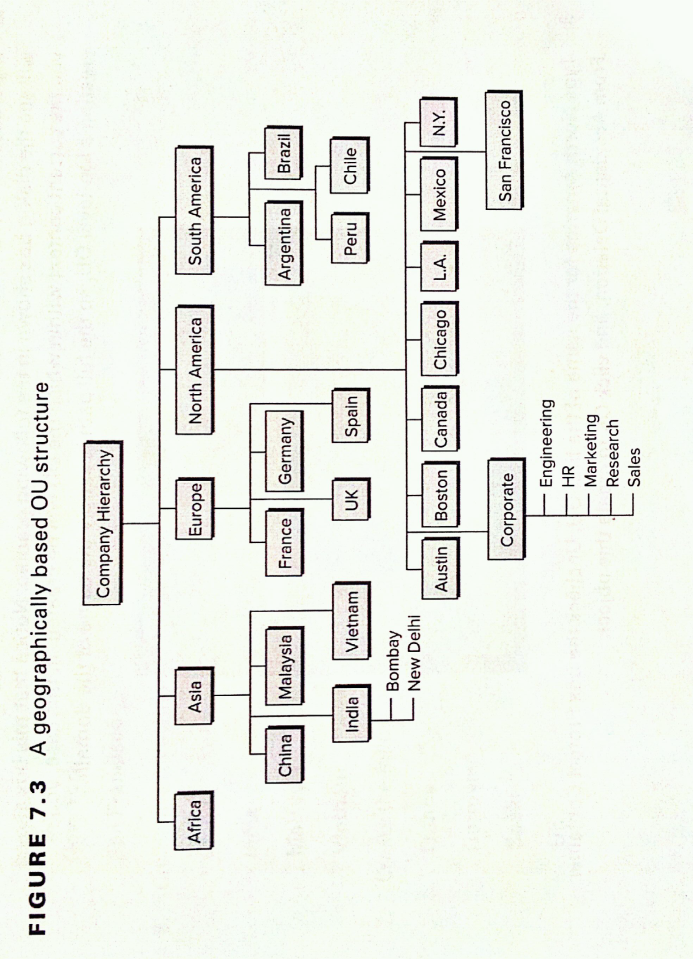
### Schéma de réplication



### Utilisateurs, groupes et OU



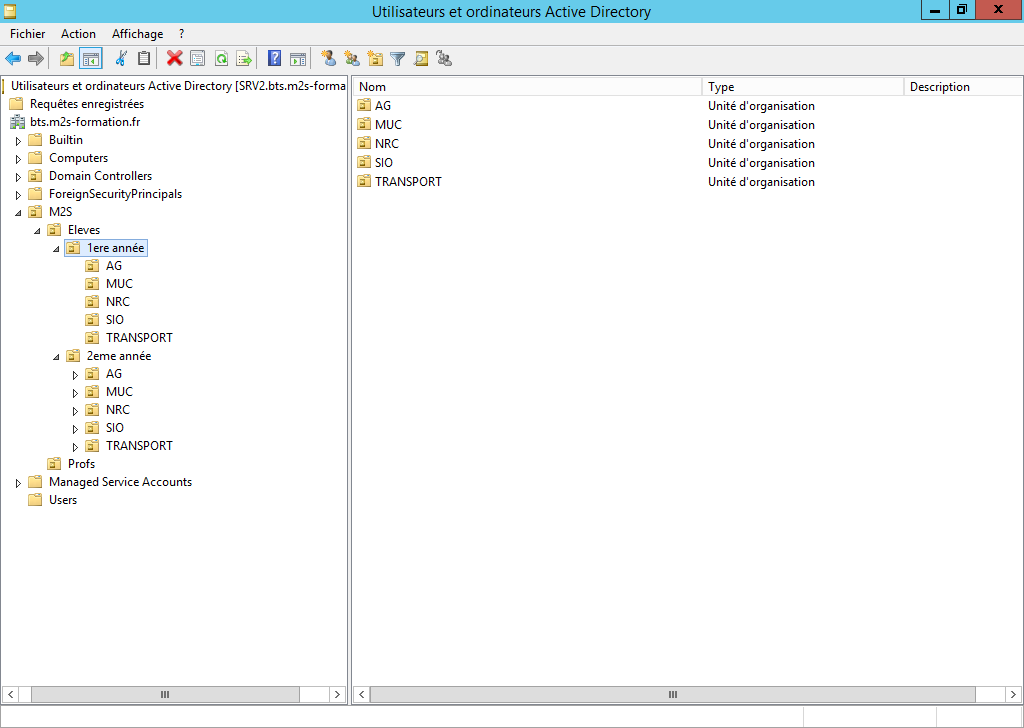




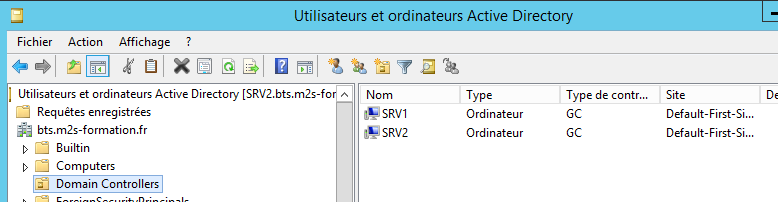
## CONSOLES DISPONIBLES DANS WINDOWS SERVER POUR ADMINISTRER ACTIVE DIRECTORY

### Console Utilisateurs et Ordinateurs AD

Cette console permet de gérer les utilisateurs, les groupes, les ou, les ordinateurs, les contrôleurs de domaine. (CONSOLE ADAC)



Elle est constituée d’au moins une OU, il s’agit de Domain Controllers. Cette OU comporte tous les contrôleurs de domaine du domaine (DC).

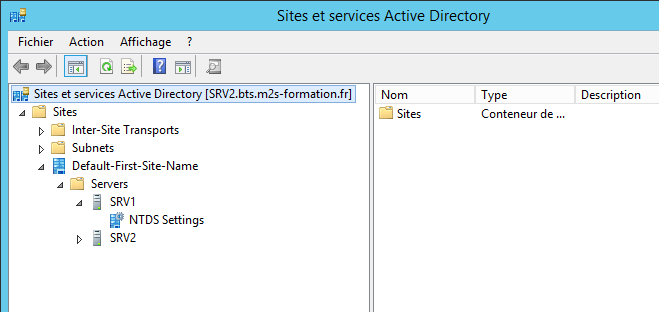


La console comporte également des dossiers (Computer ici n’est **PAS UNE OU**, Domain Controllers **EST UNE OU**, je reconnais une OU d’un dossier à son pictogramme jaune qui est différent).

Il est important de distinguer l’OU du dossier car sur une OU on peut appliquer une GPO mais pas sur un dossier.

### Console Sites et services AD

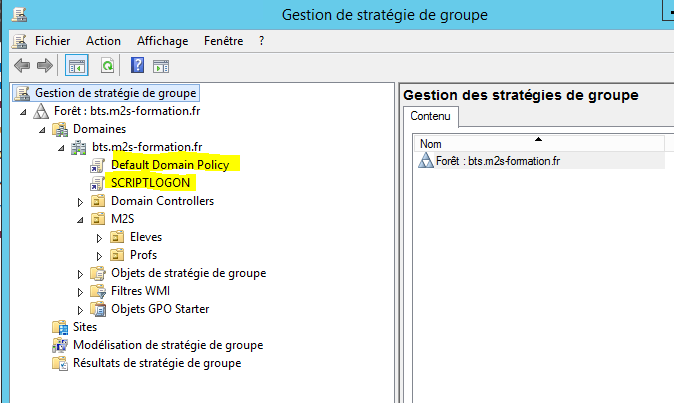
Cette console permet de vérifier entre autres, le processus de réplication entre les contrôleurs de domaine (DC) Active Directory (AD)



### Console Gestion de stratégie de groupe

Cette console permet d’appliquer sur le domaine ou sur les OU une ou plusieurs stratégies de groupe

Une stratégie ne peut être appliquée que sur une ou plusieurs OU ou sur le domaine dans son ensemble.



# Installation d’un contrôleur de domaine AD

## Pré requis et bonnes pratiques serveur

~~Je suppose ici qu’un dhcp est présent sur le réseau et que le serveur à accès à internet via ce dhcp.~~

* Activer la licence
* Renommer le serveur en donnant un nom significatif, ex SRVAD1 ou AD1 (Attention pas de nom de machines en double sur un réseau) – exemple : **RENAME-COMPUTER -newname SRVAD1 -restart**
* Désactiver IPv6
* Désactiver le pare-feu: netsh advfirewall set allprofiles state off ou en PowerShell   
  Get-NetFirewallProfile | Set-NetFirewallProfile -Enabled False
* Mettre à jour le système en appliquant et en installant l’ensemble des mises à jour disponibles
* Vérifier que les horloges sont à l’heure et que le serveur se synchronise avec un serveur ntp
* Une fois que les mises à jour ont été effectuées, on effectue l’adressage ip en attribuant une ip fixe, une adresse de passerelle et en DNS lui-même
  + Ex. SRVAD1, ip 192.168.0.1, passerelle 192.168.0.254, dns 192.168.0.1 ou 127.0.0.1
* ~~Exécuter secpol.msc et paramétrer le réseau en réseau privé~~
* Vérifier que le mot de passe administrateur réponde aux exigences de complexité et de sécurité

## Installation d’un serveur AD sous 2012 server

A partir de la console de gestion des serveurs ajouter les rôles suivants :

* - Ajouter le rôle ADDS (Active Directory Domain Services)
* - Ajouter le rôle DNS

Effectuer la promotion du serveur en Contrôleur de domaine

* En Powershell

Get-WindowsFeature -Name DNS, AD-domain-services | Add-WindowsFeature -IncludeAllSubFeature -IncludeManagementTools

Sous 2008 et 2008R2, exécuter directement DCPROMO

## Installation d’un premier contrôleur de domaine (promotion)

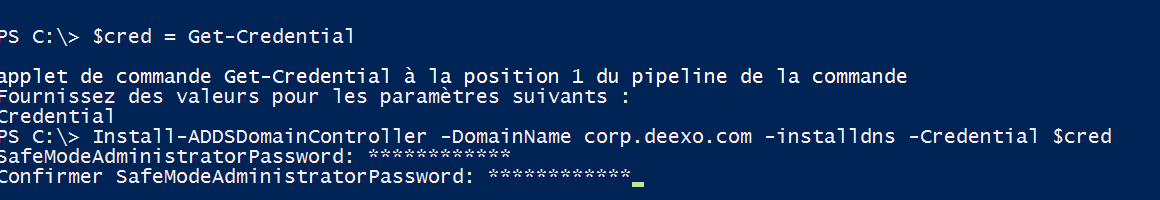
corp.contoso.com

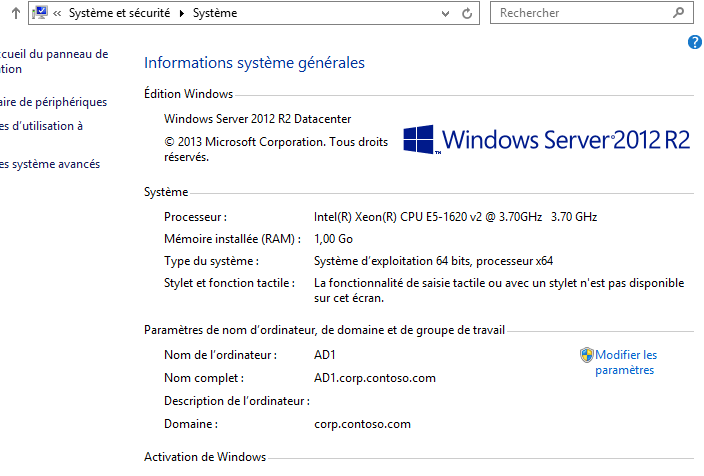
* Choisir l’option créer une nouvelle forêt
* Choisir le nom de domaine (ex. corp.contoso.com)
* Choisir le mot de passe des services de restauration d’annuaire
  + Mettre le mot de passe que l’admin
  + Permet de démarrer le serveur en mode de restauration AD pour par exemple récupérer la base ad ou effectuer des opérations de maintenance sur l’AD
* Par défaut, le 1er DC est serveur DNS et GC (Global Catalog)

Je vérifie ensuite au redémarrage du serveur si les consoles sont disponibles

Une fois que le domaine a été crée, je me logge en administrateur du domaine

Méthode en PowerShell pour un deuxieme DC <http://pbarth.fr/node/86> (attention aux crédentials)





## Login en domaine

Login administrateur

Nom de la machine AD1

Domaine corp.contoso.com

### Se logger en local

Nom machine\nom du user ou .\login

Ex. AD1\administrateur

La connexion locale utilise l’authentification NTLM

### Se logger sur le domaine

Nom de domaine\nom du user ou user@domaine

Ex. CORP\administrateur ou administrateur@corp ou [administrateur@corp.contoso.com](mailto:administrateur@corp.contoso.com)

Quand une machine est contrôleur de domaine ou si elle est sur le domaine, je distingue la connexion en local et la connexion sur le domaine.

La connexion sur le domaine utilise l’authentification Kerberos, pour que l’authentification Kerberos fonctionne parfaitement il faut que l’ensemble du parc soit synchronisé au niveau horloge (Mise en place d’un serveur ntp obligatoire)

## Vérification du fonctionnement des DNS et DNS Reverse en AD

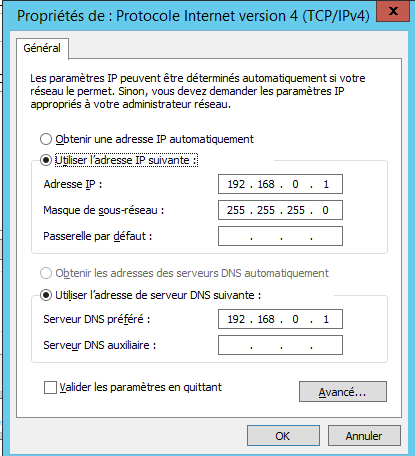
### Fonctionnement

Dans toute mise en place d’un DC AD le DNS est nécessaire. Microsoft recommande un DNS par DC.

Dans la pratique, deux serveurs DNS suffisent sur un réseau.

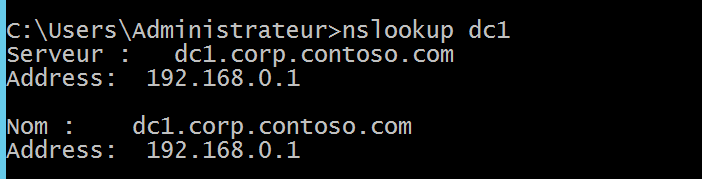
Rappel : Pour l’ensemble des postes clients et des autres serveurs joints au domaine, les DNS préférés et auxiliaires doivent obligatoirement être les contrôleurs de domaine AD.

Dans le cas d’une infrastructure à un seul contrôleur de domaine, seul le DNS préféré sera renseigné.

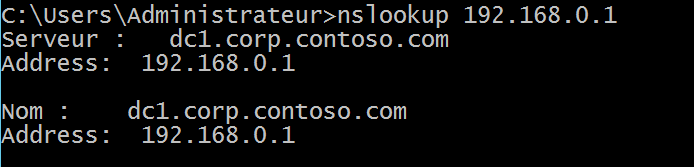


Pour vérifier le bon fonctionnement des DNS :

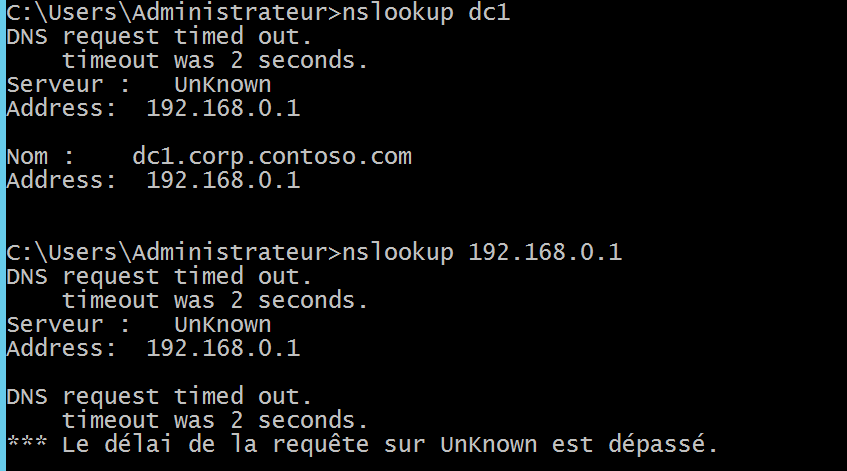
* Passer en mode console
* Exécuter un nslookup nomdc
* La réponse doit être la suivante :



On teste ensuite le dns reverse en faisant un nslookup ip



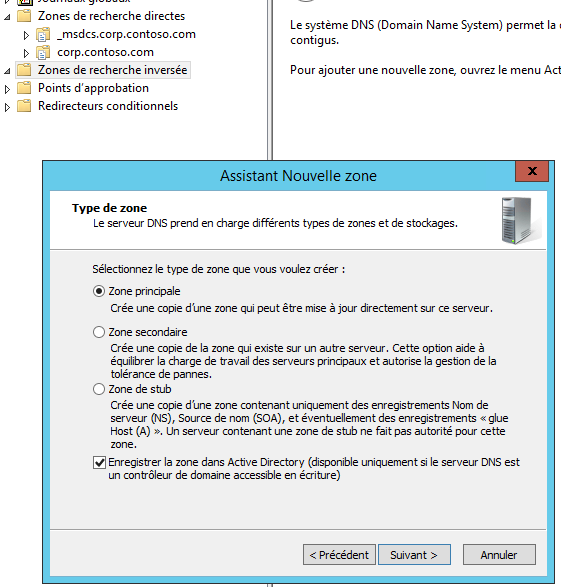
Après la promotion du serveur en DC, si le nslookup reverse ne fonctionne (unknow en retour), il est fort probable que le PTR n’existe pas dans les DNS.



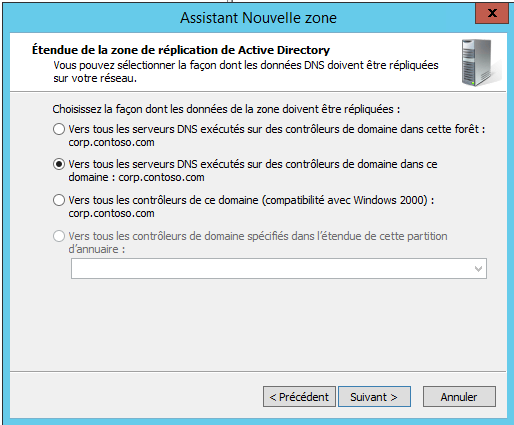
Il faut créer la zone DNS Reverse

### Création de la zone DNS Reverse

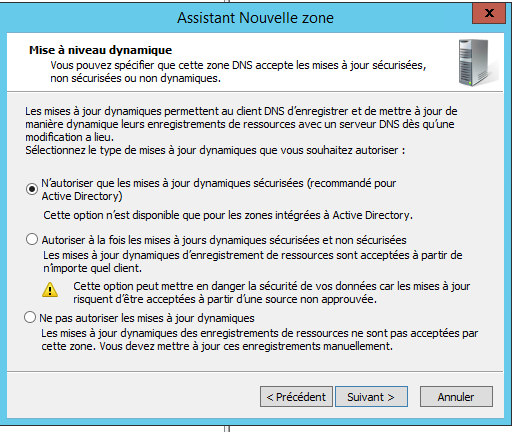
* Lancer la console DNS
* Faire un clic droit dans la zone de recherche inversée et créer une nouvelle zone
* Je crée une zone inversée principale qui doit être intégrée à l’AD



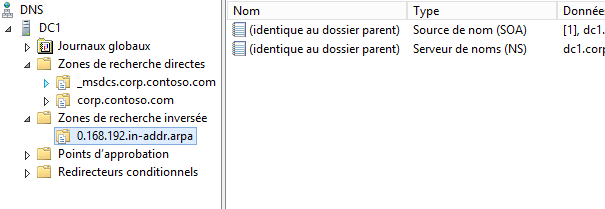
* Je réplique cette zone vers tous les serveurs DNS du domaine (attention, sur Windows 2008R2 un bug affiche un texte identique sur les deux premiers choix de la version française, cela ne change rien dans le choix de l’option 2)



* Spécifier ensuite le mode ipv4 et l’identifiant réseau (ici 192.168.0) et n’autoriser que les mises à jour dynamiques sécurisées



Voici le résultat



Il faut ensuite à partir de la console en élévation admin, exécuter ipconfig /registerdns pour ajouter le ptr correspondant à l’ip reverse.

On reteste ensuite le nslookup qui cette fois renvoie des données correctes (15 mn peuvent être nécessaires)

Cette manip peut être effectuée en PowerShell



# Joindre un poste client ou un serveur non contrôleur de domaine au domaine

Pré requis :

* Disposer d’os clients Pro ou Entreprise
* Etre sur le même réseau en termes d’adressage d’ip
* Vérifier que le poste client a bien en DNS l’ip d’un ou plusieurs controleurs de domaine
* Vérifier la connectivité ip (ping vers le DC1 par exemple)
* Vérifier la résolution DNS avec nslookup nomDC et nslookup ipdns1
* Appliquer les bonnes pratiques Krosoft

Ex. Je veux joindre le serveur IIS sur le domaine

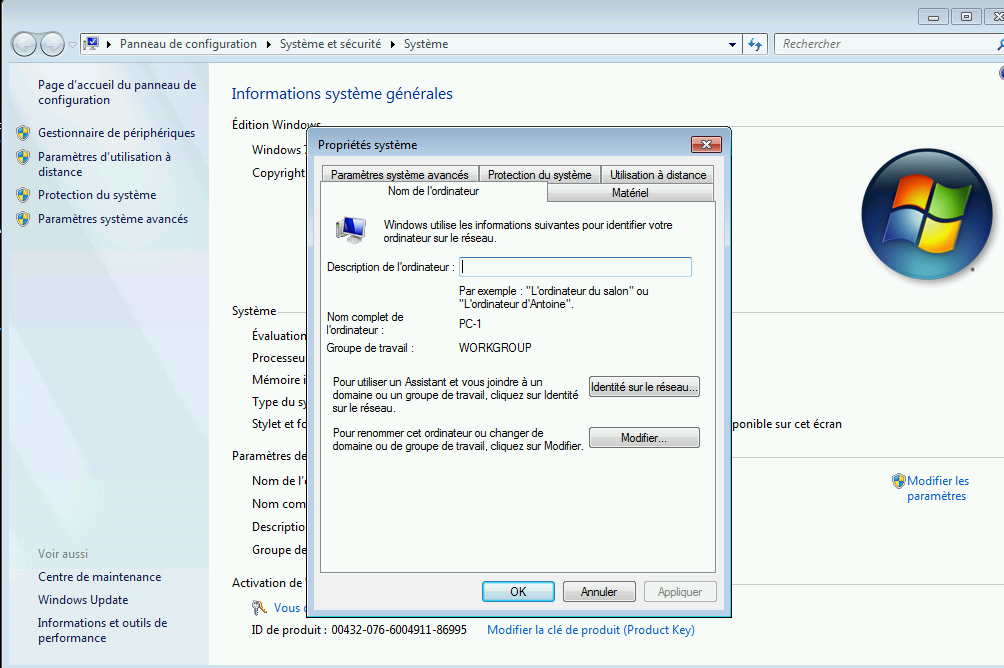
J’effectue ces modifications sur le serveur IIS

Ou le poste client

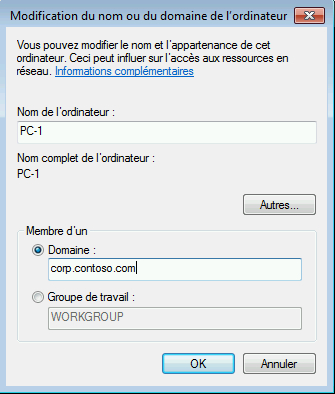
* Renommer le serveur en SRVIIS ou autre nom
* Changer l’adresse IP en 10.0.0.3/24
* Modifier le DNS en 10.0.0.1
* Modifier la passerelle en 10.0.0.254
* Pinger le 10.0.0.1
* Faire un nslookup de DC1
* Joindre le serveur au domaine

## Joindre une machine à partir de l’interface graphique

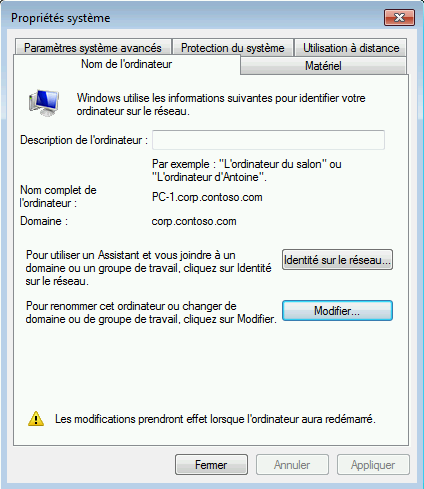
Sur le poste à joindre, aller dans Gestion de l’ordinateur (ou dans explorateur ce PC), Propriétés système et cliquer sur Modifier



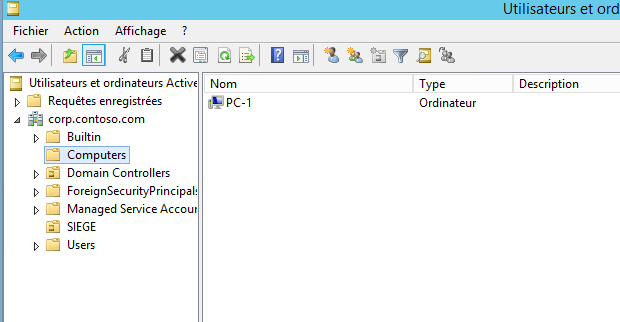
Saisir ensuite le domaine à joindre



Saisir le compte autorisé à joindre le poste au domaine, typiquement l’administrateur du domaine (Corp\administrateur ici)



Je constate dans la console Utilisateurs AD du serveur que le poste est bien présent dans Computers



Je peux ensuite me logger en utilisateur du domaine sur le poste client, les droits et les partages seront gérés dans le domaine.

On vérifie dans la console Utilisateurs AD que le poste client a bien été ajouté dans Computer et dans la zone DNS

## Méthodes alternatives

* En ligne de commande

Netdom join localhost /d:corp.contoso.com /reboot:5

* En PowerShell, add-computer

Add-computer –domainname corp.contoso.com -credential (Get-credential )

# Partage et droits NTFS

## Partage administratif

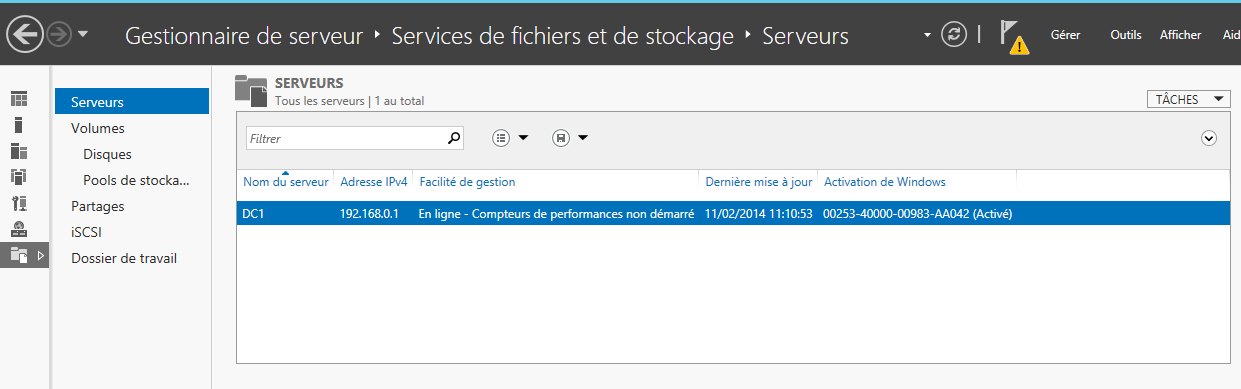
Un partage administratif est la possibilité d’accéder à chaque disque du poste en utilisant sa lettre de lecteur suivi de $

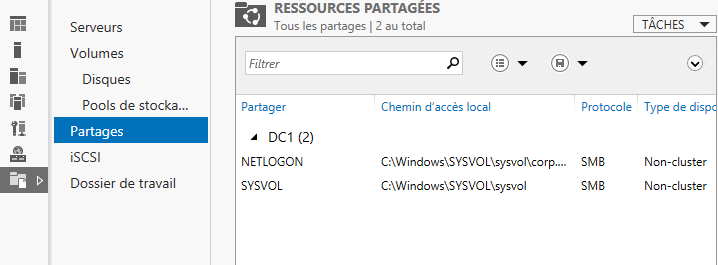
Par exemple : [\\DC1\c$](file:///\\DC1\c$) ou [\\192.168.0.1\c$](file:///\\192.168.0.1\c$) (on appelle cette notation une adresse UNC Universal\_Naming\_Convention)

Pour utiliser le partage vous devez être administrateur du domaine ou de la machine

## Partage de dossiers

Pré requis : Le service de fichiers et de stockage doit être activé (role pré requis)

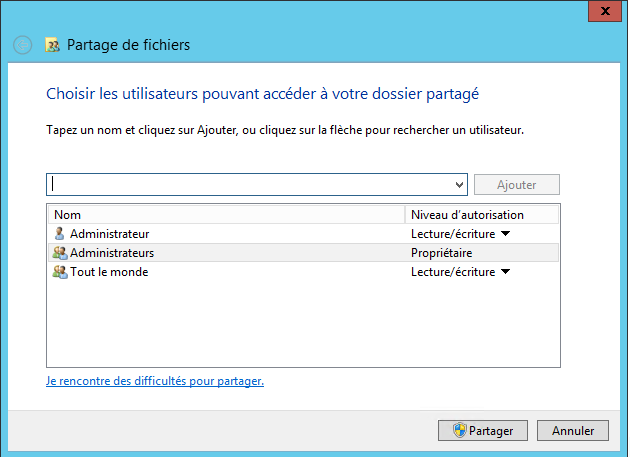


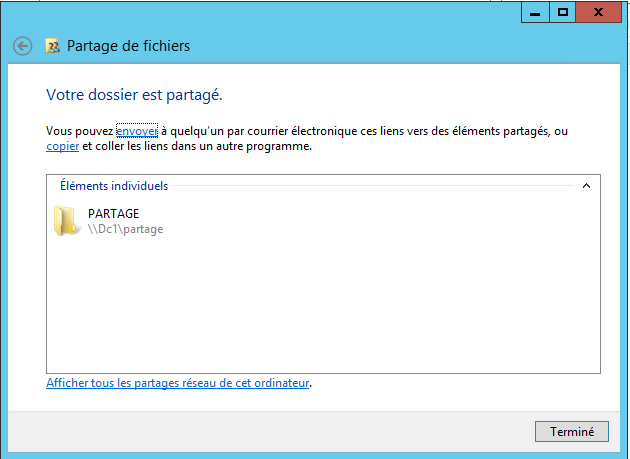


## Création d’un partage réseau

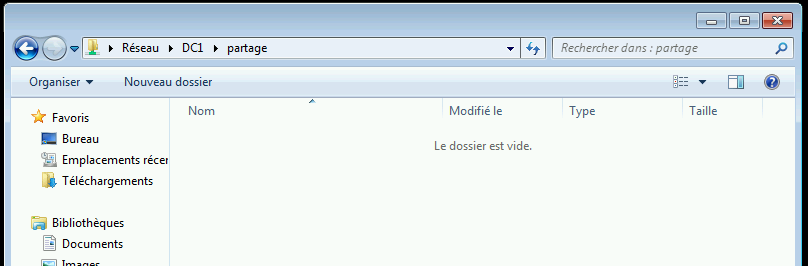
Sur le serveur, je crée un dossier, je fais clic droit partager, j’ajoute tout le monde en lecture écriture

Il est IMPORTANT lors de la création du partage, d’ouvrir le partage à TOUT LE MONDE en lecture écriture. La gestion des permissions se fera par la suite.





On vérifie à partir du poste client que le partage est actif et qu’il fonctionne. On a bien les droits de lecture et d’écriture.

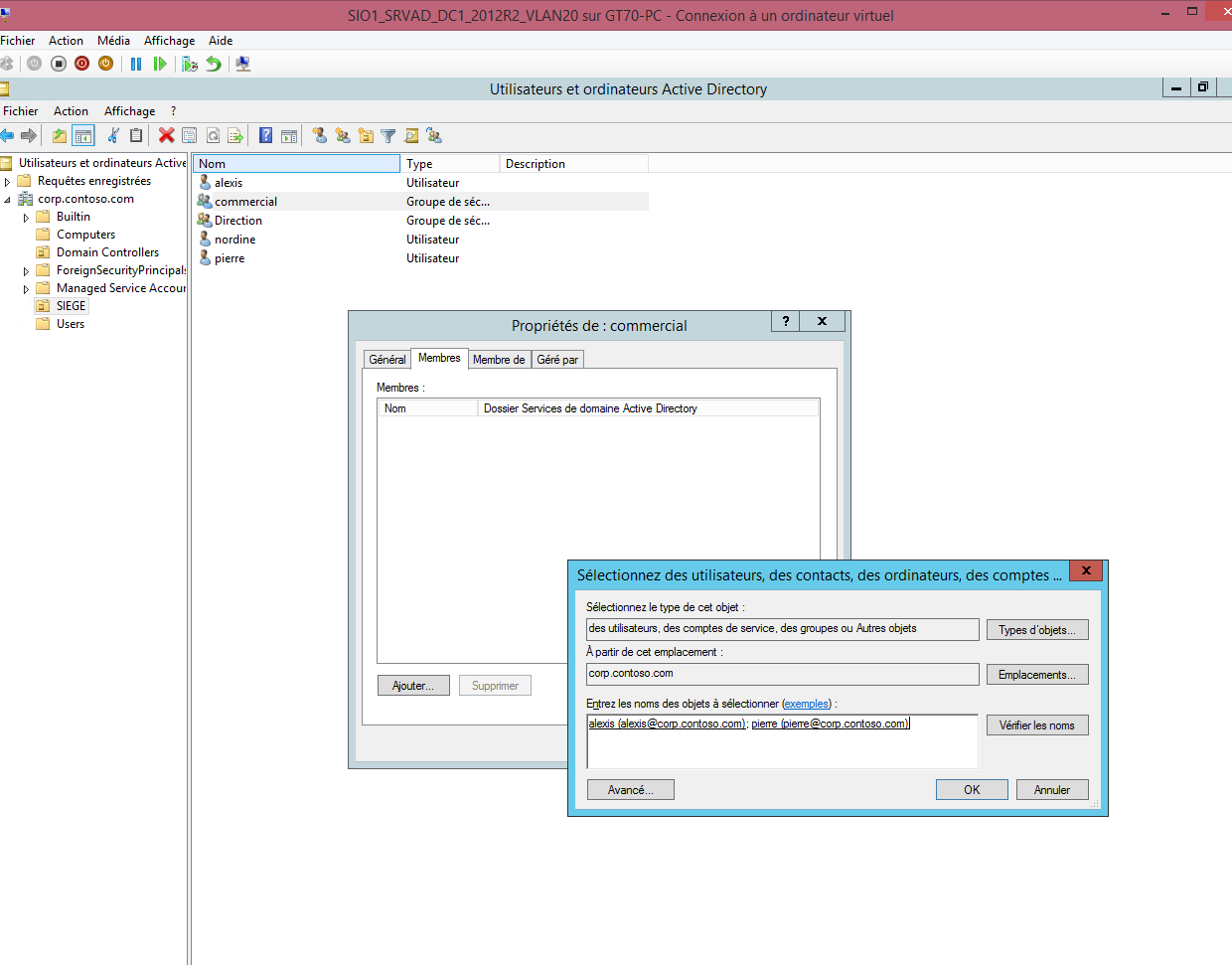


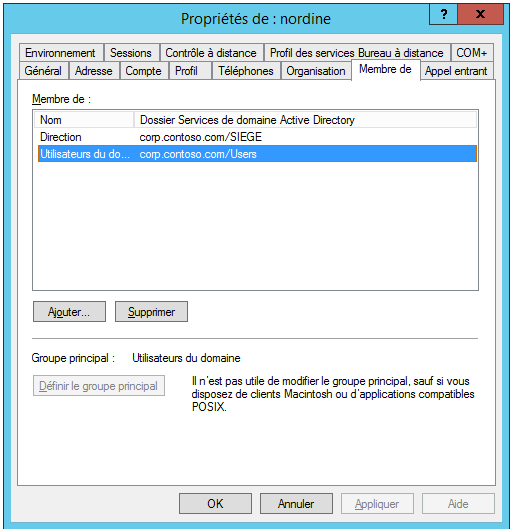
## Attribution de droits et de restrictions à un partage via NTFS

### Ajout des utilisateurs aux groupes

Mes utilisateurs ont été ajoutés à des groupes de sécurité.

Ici Alexis et Pierre font partis du groupe commercial, et Nordine fait partie du groupe Direction



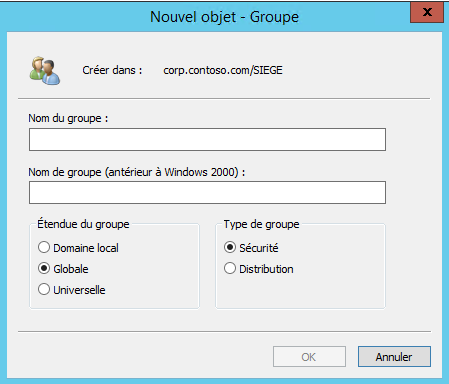


Note sur les groupes de sécurité :

Un groupe peut être de type domaine local, global ou universel

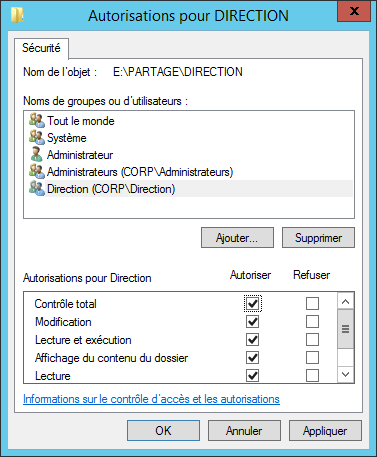
Global = Foret

Universel = Multi forét



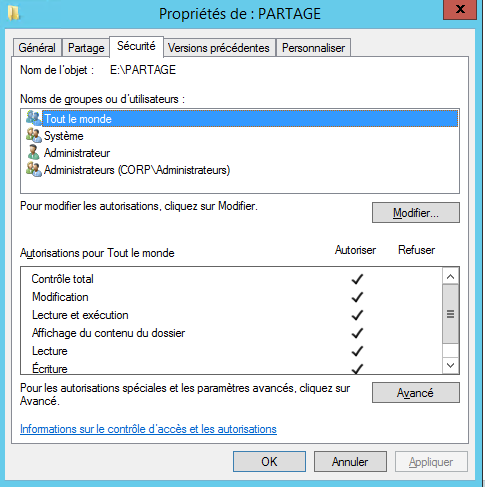
### Attribution de droits aux groupes

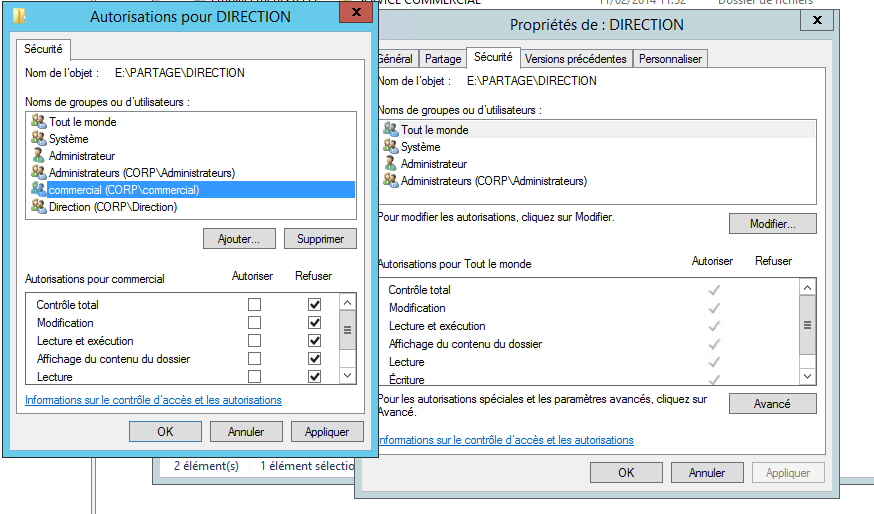
Les droits NTFS se gèrent sur chaque dossier ou fichier en utilisant l’onglet sécurité sur le clic droit.

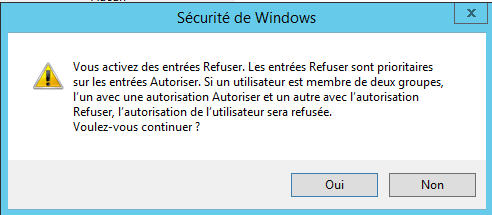


J’ajoute ici aux droits du dossier Direction un contrôle total pour le groupe Direction

J’ajoute ensuite aux droits du dossier Direction le groupe Commercial et je lui refuse tous les droits





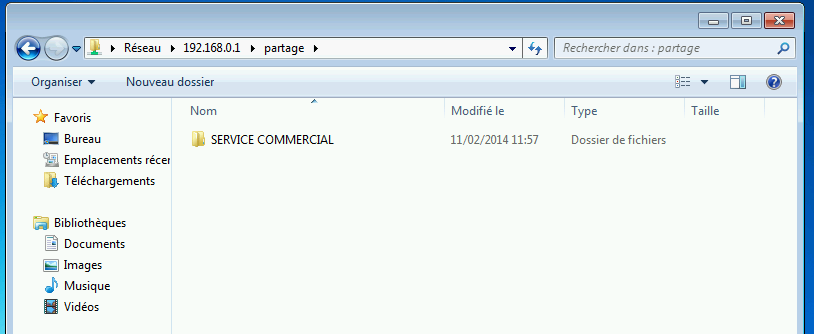


Je valide mon choix

Conséquences de la manip :

Je constate en me connectant sur le poste client, que le membre de direction (ici Nordine) a toujours les droits sur les dossiers.

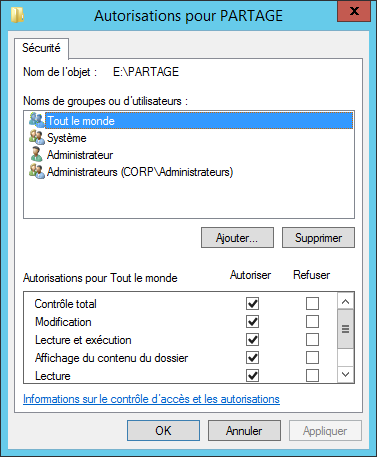
Si maintenant je me connecte en tant que Pierre (utilisateur du service commercial), Pierre n’a pas visuel sur le dossier Direction.



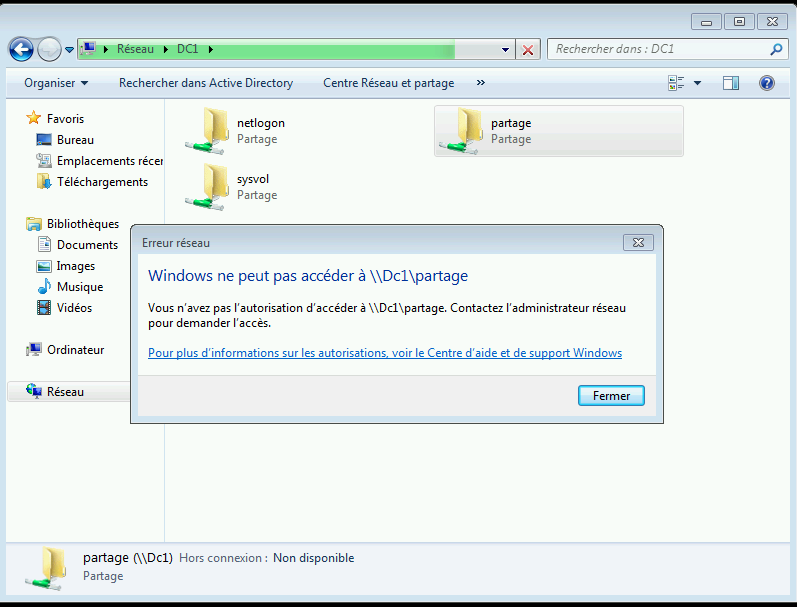
Le problème ici c’est que si un nouvel utilisateur est créé et s’il n’est pas affecté à un groupe par erreur, il aura tous les droits sur le partage

Ce qu’il faut faire, c’est faire en sorte que à part les admins personnes par défaut est d’accés au dossier Partage

Statégie 1 : Enlever le groupe TOUT LE MONDE du répertoire PARTAGE (ATTENTION ENLEVER ET PAS REFUSER !!!! SI VOUS REFUSEZ TOUT LE MONDE LE DOSSIER NE SERA PLUS ACCESSIBLE DU TOUT)



Problème, le partage n’est plus accessible….

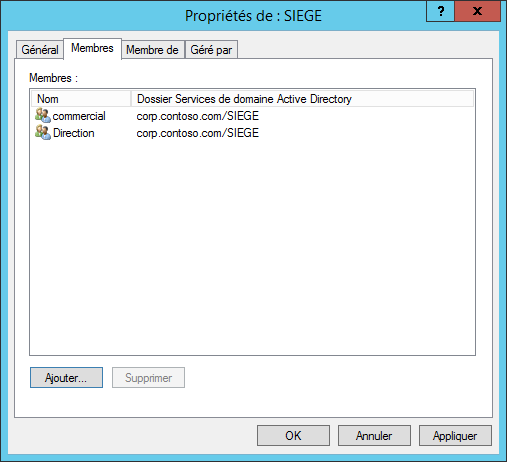


Stratégie N°2 – enlever Tout le monde des sous dossiers Direction, Service Commercial, etc…

Problème on peut en avoir pour 20 ans…..

Bonne pratique pour résoudre le problème de droits et arriver à une solution simple et cohérente :

* Enlever Tout le monde du dossier Partage
* Créer un groupe de sécurité SIEGE
* Ajouter comme membre du groupe SIEGE l’ensemble des groupes (Service Commercial, Direction, etc…)



* Affecte le contrôle TOTAL de partage à SIEGE
* Ensuite pour des dossiers comme direction, je refuse les groupes comme Service commercial

Avec cette pratique, les utilisateurs non membres d’un groupe n’ont pas d’accès aux ressources de l’entreprise.

# Changement d’adressage IP sur des contrôleurs de domaines AD

# Mise en place d’une GPO sur un domaine AD

## Définition

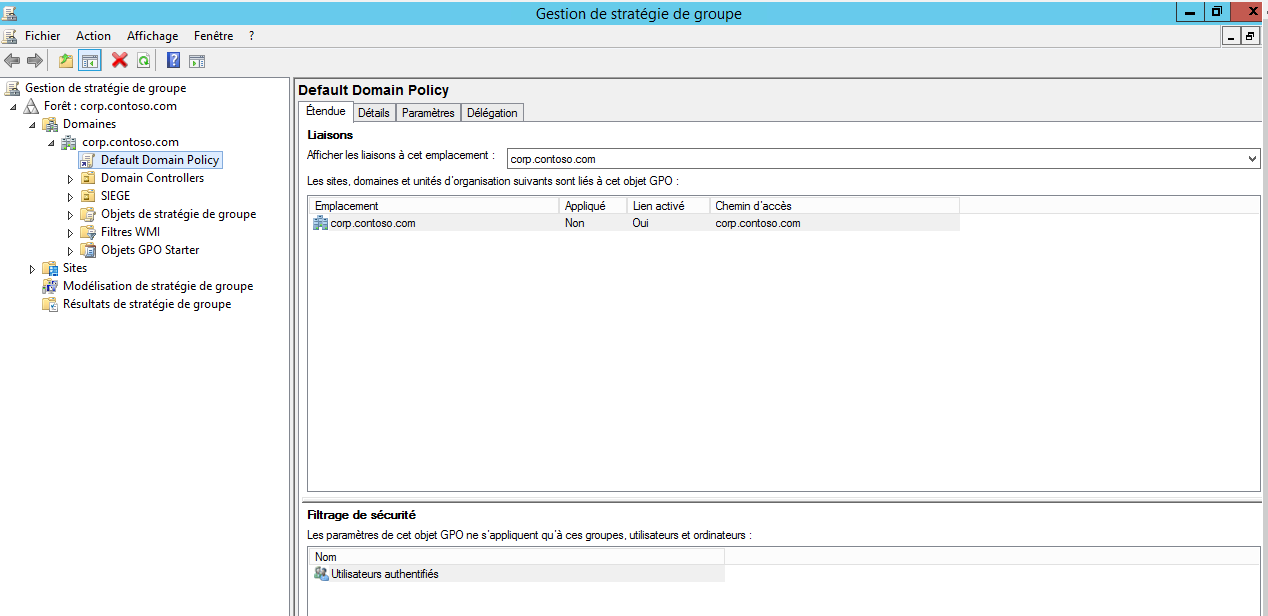
On appelle une GPO (Group Policy Object // Stratégie de groupe) un ensemble de paramètres qui vont être appliqués soit à un domaine, soit à une OU.

Ex : J’ai besoin d’empêcher les utilisateurs de modifier le papier peint du bureau windows, je souhaite que les dossiers Mes Documents et Bureau soit physiquement stockés sur le serveur et pas sur le poste client. Je souhaite installer Mozilla Firefox sur 250 postes…..

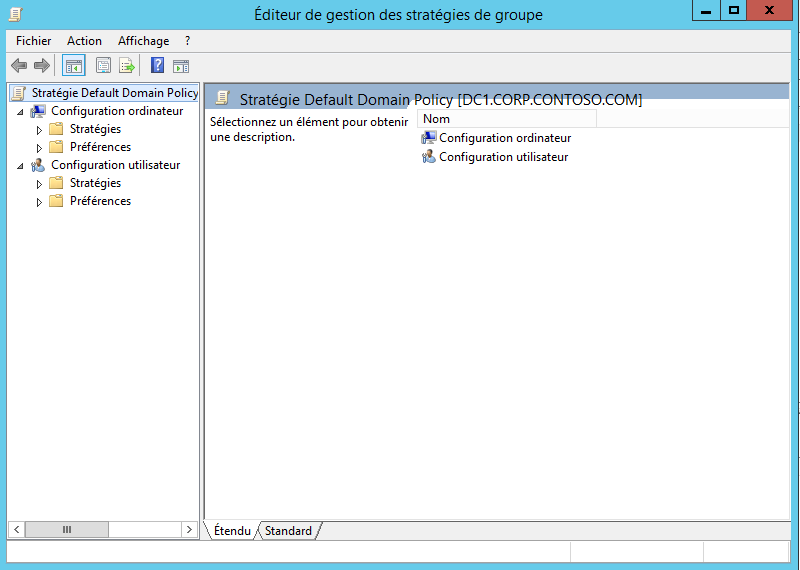
Pour ces taches on va créer une gpo et l’appliquer soit à utilisateurs soit à des machines situées à l’intérieur d’une OU ou sur le domaine.

## Consoles nécessaires pour mettre en place un GPO

La console gestion des stratégies de groupe permet de gérer et de mettre en place les GPO



L’éditeur de gestion de stratégies de groupe permet de paramétrer le contenu d’une GPO



## Contenu d’une GPO

On distingue à l’intérieur d’une GPO, les paramètres Configuration ordinateur et configuration utilisateur.

Ordinateur va modifier des éléments de la base de registre correspondant HKLM (Hkey Local Machine)

Les GPO ordinateurs sont appliquées sur le poste client avant Ctrl Alt Suppr

Utilisateur va modifier des éléments de la base de registre correspondant au HKCU (Hkey Current User)

Les GPO utilisateurs sont appliquées sur le poste client après Ctrl Alt Suppr

Une stratégie ne peut pas être modifiée par l’utilisateur final. La stratégie est automatiquement appliquée.

Une préférence permet d’appliquer certains paramètres aux postes clients, mais l’utilisateur pourra dans ce cas modifier les paramètres.

## Exemple de mise en place d’une GPO

On souhaite à l’aide d’une GPO effectuer sur l’ensemble des machines et serveurs d’un domaine AD les taches suivantes :

* Désactiver l’expiration du mot de passe
* Désactiver les firewalls
* Modifier Internet Explorer en ajoutant le nom de l’entreprise dans la barre de titre
* Rediriger l’ensemble des Mes Documents vers un emplacement partagé sur le réseau
* Rediriger l’ensemble des Bureaux utilisateurs vers emplacement partagé sur le réseau
* Installer Mozilla firefox sur l’ensemble des postes clients (on ne veut pas les serveurs)
* Ajouter dans internet explorer une adresse de proxy pour les postes clients (on ne veut pas les serveurs)

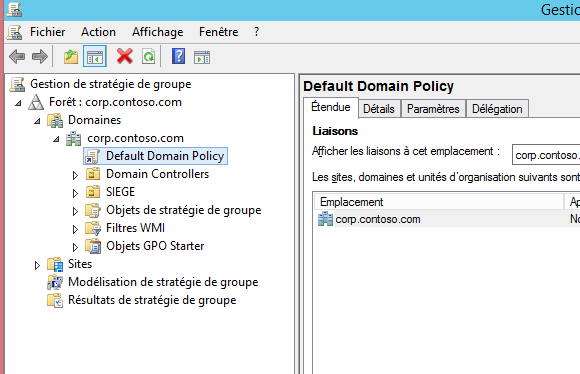
### Ouvrir la console Gestion des stratégies de groupe

Certaines GPO vont être appliquées au Default Domain Policy. Cette gpo représente l’ensemble des éléments de l’AD.

* Désactiver l’expiration du mot de passe
* Désactiver le pare-feu de l’ensemble du parc
* Modifier Internet Explorer en ajoutant le nom de l’entreprise dans la barre de titre
* Rediriger l’ensemble des Mes Documents vers un emplacement partagé sur le réseau
* Rediriger l’ensemble des Bureaux utilisateurs vers emplacement partagé sur le réseau

Les éléments suivants ne seront appliqués qu’à l’OU Siege

* Installer Mozilla firefox sur l’ensemble des postes clients (on ne veut pas les serveurs)
* Ajouter dans internet explorer une adresse de proxy pour les postes clients (on ne veut pas les serveurs)



### Modification de la GPO Default Domain Policy

Par clic droit modifier dans la GPO j’édite la GPO.

* Désactiver le menu imprimer
* Désactiver outil option

Config Utilisateur, Stratégies, Modeles d’administrations, Composants Windows, Internet Explorer, Menu du navigateur, je double clic dans Desactiver le menu imprimer, Activer cette option

Je fais pareil pour l’option Options internet

Pour diffuser la GPO et mettre à jour l’ensemble de l’AD, j’éxécute en élévation de commande, gpupdate /force

# LES ROLES FSMO

Toutes les explications sur le role de chaque role ☺ est sur

<http://www.labo-microsoft.org/articles/win/FSMO/>

## Transférer un rôle FSMO vers un autre contrôleur de domaine

1. Vérifier quel contrôleur de domaine possède tel ou tel rôle

Exécuter en élévation, dsquery server –hasfmo nom du rôle ou nom du rôle prendra une des valeurs suivantes :

* PDC
* Schema
* Name
* Infr
* Rid

On obtient le DN avec la mention du serveur possédant le rôle.

En powershell

Get-ADDomain | Select-Object InfrastructureMaster, RIDMaster, PDCEmulator

Get-ADForest | Select-Object DomainNamingMaster, SchemaMaster

Get-ADDomainController -Filter \* |

     Select-Object Name, Domain, Forest, OperationMasterRoles |

     Where-Object {$\_.OperationMasterRoles} |

     Format-Table -AutoSize

1. Transfer du rôle

On suppose que le contrôleur de domaine possédant le rôle est joignable et fonctionnel

En élévation exécuter NTDSUTIL sur le contrôleur de domaine sur lequel on va transférer les rôles.

Puis

**roles  
connection  
connect to server NOM DU SERVEUR ex. DC2  
quit**

La connexion doit se faire sur le serveur sur lequel on va transférer le role.

On transfère ensuite les roles :

**Transfer naming master  
Transfer infrastructure master  
Transfer PDC  
Transfer RID master  
Transfer schema master  
Quit  
Quit**

On vérifie que chaque role a bien été transféré en éxecutant les commandes suivantes :

dsquery server –hasfmo PDC

dsquery server –hasfmo schema

dsquery server –hasfmo rid

dsquery server –hasfmo infr

dsquery server –hasfmo name

Si le contrôleur de domaine qui possède les rôles n’est pas joignable, la démarche est la même mais en utilisant Seize à la place de Transfer

Cette commande va forcer le rôle à venir sur le DC sur lequel on est connecté

Cette commande permet de rétablir une cohérence dans l’AD dans des cas tels que le contrôleur de domaine possédant les rôles a été supprimé sans dépromotion (DC PROMO REVERSE), ou le contrôleur de domaine a été victime d’une panne matérielle.

**Seize naming master  
Seize infrastructure master  
Seize PDC  
Seize RID master  
Seize schema master  
Quit  
Quit**

## **En powerShell**

[**http://www.nogeekleftbehind.com/2013/05/28/powershell-move-ad-fsmo-roles-in-server-2012/**](http://www.nogeekleftbehind.com/2013/05/28/powershell-move-ad-fsmo-roles-in-server-2012/)

**Dans la console Powershell, lister les roles FSMO**

**Netdom query fsmo**

**Move-ADDirectoryServerOperationMasterRole –Identity ‘’nom du serveur cible’’ –operationMasterrole 0,1,2,3,4**

**Ou**

**Move-ADDirectoryServerOperationMasterRole –Identity ‘’nom du serveur cible’’ –operationMasterRole SchemaMaster, RidMaster, InfrastructureMaster, DomainNamingMaster, PDCEmulator**

# Déplacement de la base AD vers un autre dossier ou disque

## Vérifier l’emplacement des fichiers AD

A partir de NTDSUTIL, effectuer un List Instances

Je vois ainsi l’emplacement de stockage de l’AD

J’identifie également le nom de l’instance (ici NTDS par défaut)

## Déplacement des fichiers AD

A partir de NTDSUTIL, se connecter à l’instance active identifiée précédemment

Instance activate NTDS

Files

j’obtiens le message comme quoi le service est actif.

En Windows 2000 et 2003, vous devez redémarrer le serveur en mode de restauration d’annuaire

En Windows 2008R2 et suivant, il suffit d’arrêter le service ADDS

En Powershell stop-service NTDS –force

Sur ntdsutil, je tape

Files

Move db to emplacement

Move logs to emplacement

Ex:

Move db to c:\AD

Move logs to c:\AD

## Définir un emplacement de sauvegarde de l’AD

NTDSUTIL

Files

Set path backup Emplacement

# DEPLOIEMENT D’UNE APPLICATION VIA UNE GPO

On peut déployer via une GPO du MSI ou de l’exe