2013

Windows Serveur 2008

ADMINISTRATION

OLIVIER D.

Table des matières

1 Prérequis

Ce cours est le 3e de la série TSRIT.

Pour suivre ce cours, l'ouvrage suivant est conseillé :

Support de cours - ENI éditions	
Titre	Windows Serveur 2008 : Administration
Auteur	Philippe Freddi
Collection	Certifications
ISBN	978-2-7460-5811-8

2 Introduction aux taches d'administration dans WS 2008

2.1 Rôle serveur

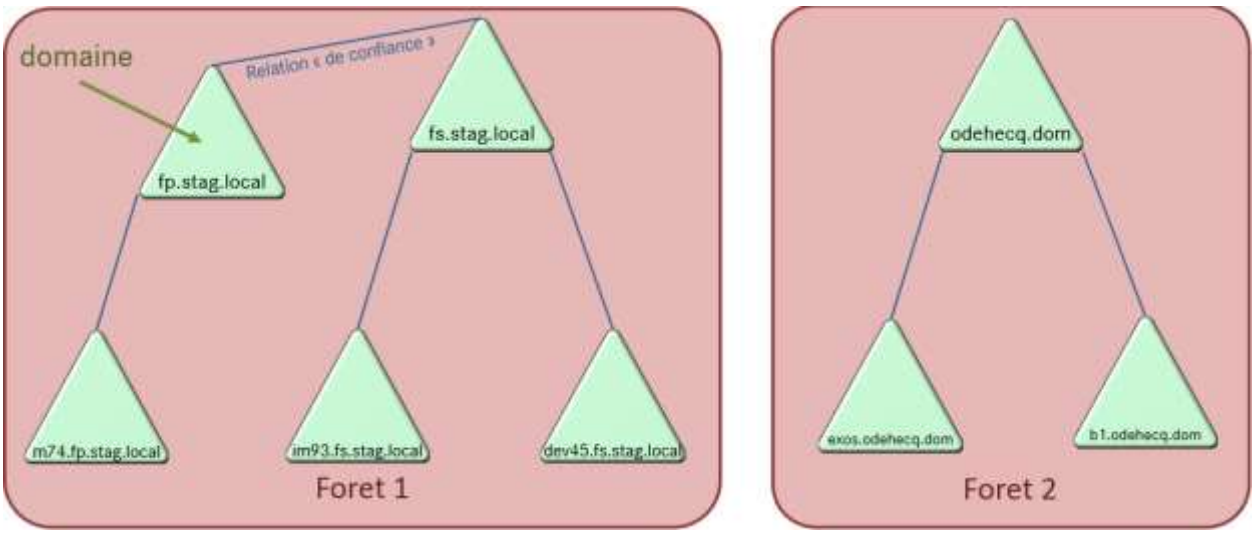
- édition standard et entreprise répandues (entreprise = standard + haute disponibilité)
- Licences d'Accès Clients (LAC ou CAL) → payer pour que les clients accèdent au serveur
- *small business* : ws2008 + Microsoft Exchange + SharePoint + maxi 50 CAL
  - ➢ Au-delà de 50 utilisateurs, on paye tout séparément

Rôles de serveurs (=services rendus à des clients) :

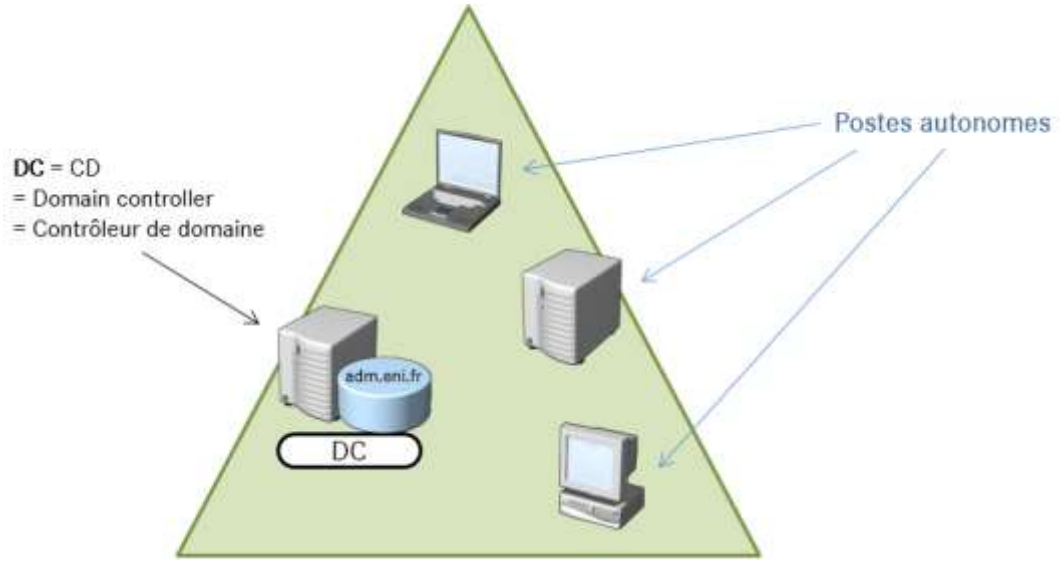
- **Serveur de plateforme :** 1 = install d'un client local ; 2 = TSE/Citrix ; 3 = navigateur web + IIS
- Rôle de serveur AD : annuaire, centralisation … → il faut ADDS avant de mettre le reste (ADDS=AD)
- Serveur Core : pas d'interface graphique. - : pas de services de déploiement, pas de TSE /Citrix.

2.2 Vue d'ensemble d'Active Directory

Une architecture de forêt active directory peut être du style :



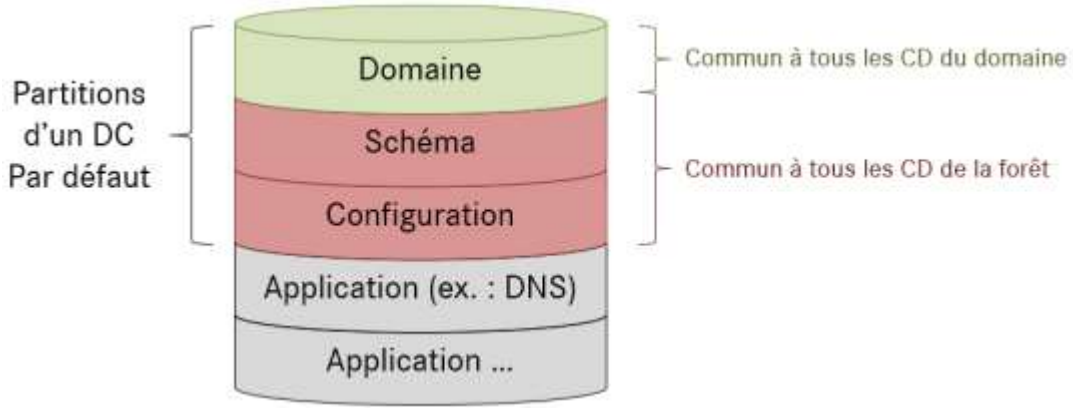
Relations de confiance entre les différents domaines de la foret



Les membres d'un domaine

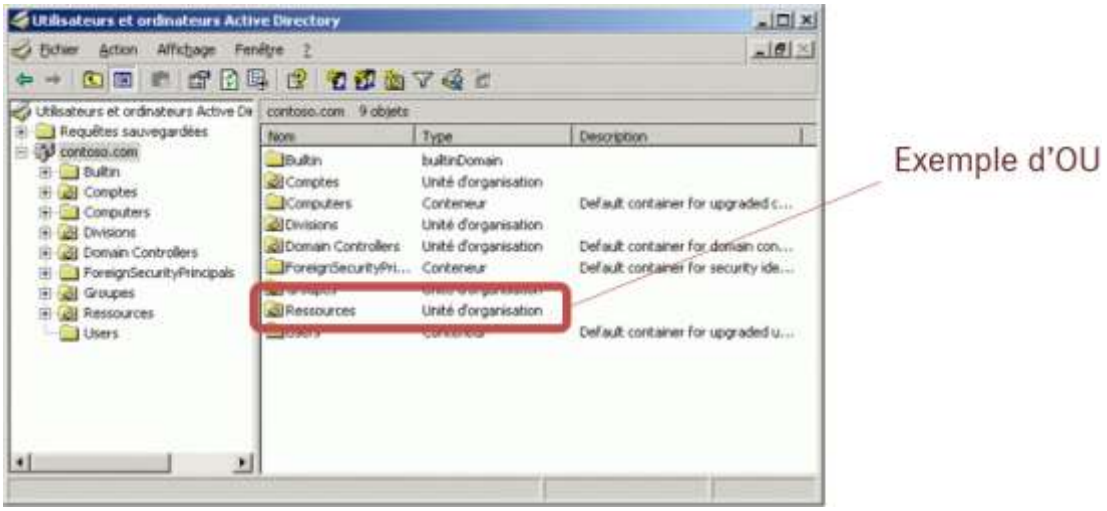
Un contrôleur de domaine peut être :

- CD pour un domaine existant
- CD pour un nouveau domaine dans la forêt
- CD pour un nouveau domaine dans une nouvelle forêt



Partitions de la base ADDS

Unité d'organisation = OU = UO (sous la forme d'un conteneur dans l'arborescence) :



Un exemple (d'ailleurs pas très bon) d'organisation des Unités d'Organisation

Objectifs de l'organisation des unités d'organisation :

- GPO (stratégies de groupe) de ce conteneur
- Délégations d'organisation (délégation administrative)
- Organiser les objets (c'est un objectif SECONDAIRE)

Une forêt (au sens Active Directory) est un ensemble de domaines qui s'approuvent mutuellement (domaine de confiance).

Les serveurs « Core » :

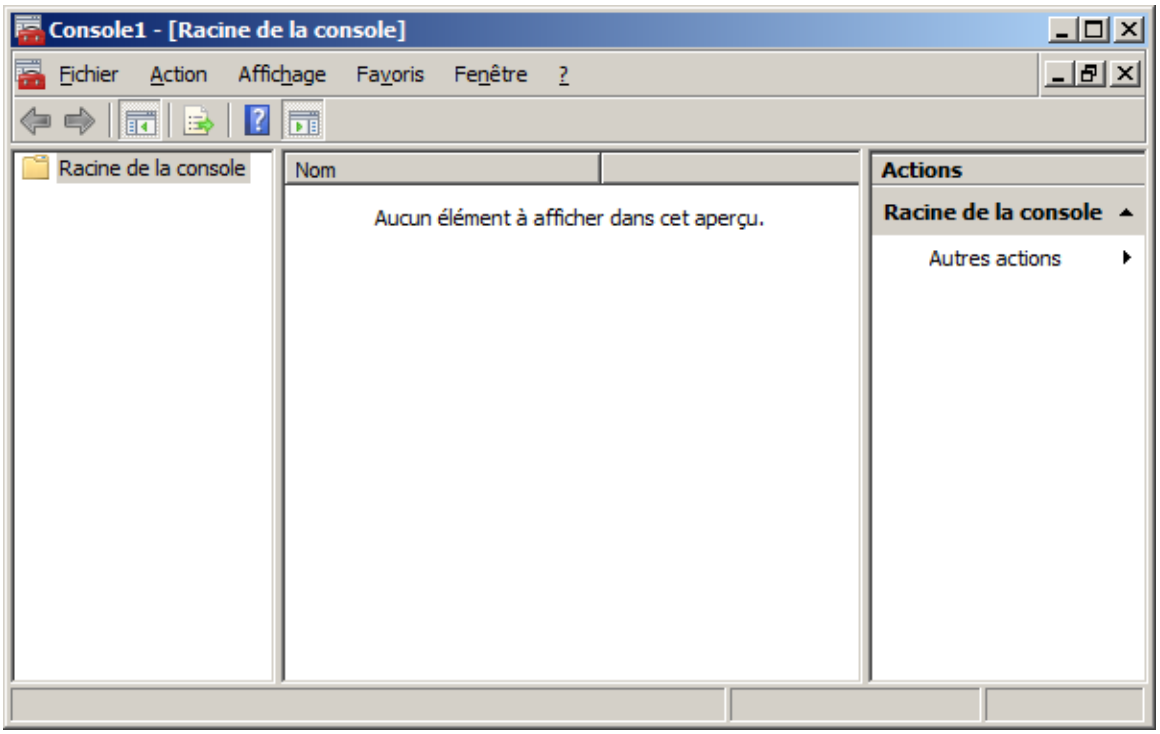
- Ne sont qu'en ligne de commande (pas d'interface graphique du type 'Windows c'est facile'). Objectif : rendre l'administration faisable que par des personnes qualifiées
- Ils conviennent aux petites agences dont les personnels seraient tentés d'utiliser le serveur comme un simple poste de travail

Les Read Only Domain Controller (RODC) :

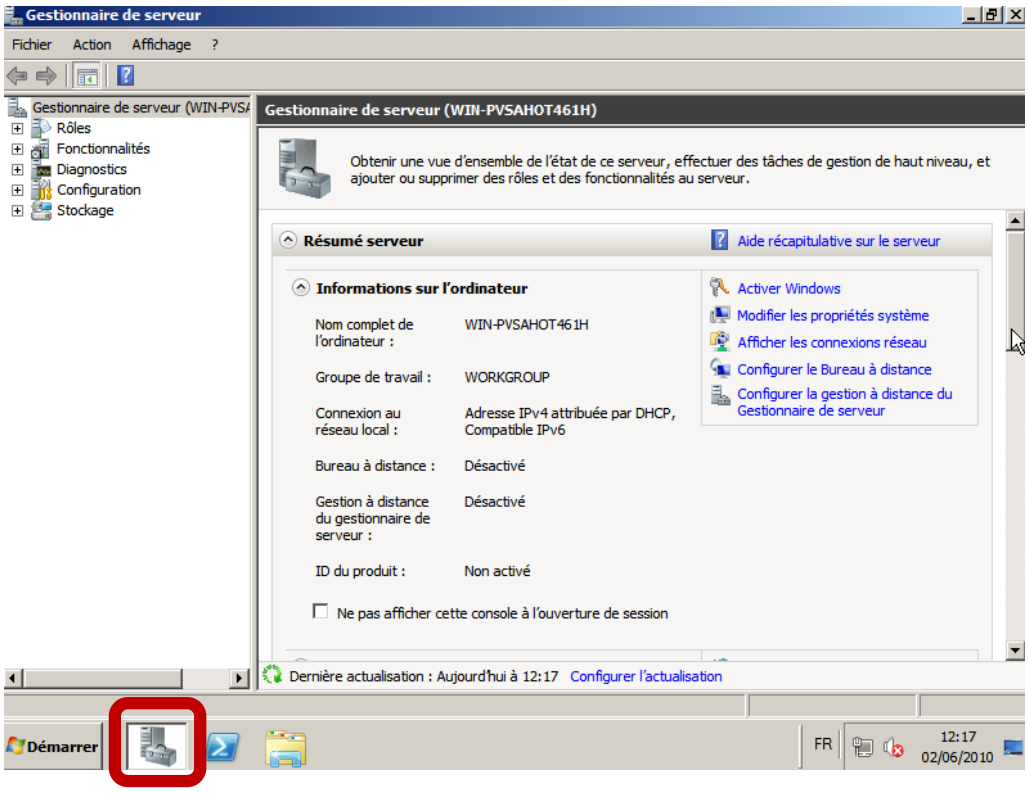
- filtrage des utilisateurs contenus dans l'ADDS, base en lecture seule (pas de piratage = pas d'insertion de données dans la base)
- convient pour des agences où la sécurité des serveurs est minime.
- Ne peut –évidemment- pas être le seul contrôleur du domaine

2.3 Utilisation des outils d'administration WS2008

Les deux principaux outils pour l'administration de Windows Serveur 2008 sont :



La console MMC (accessible en exécutant « mmc.exe »)



Le gestionnaire de serveur

3 Utilisation du bureau à distance pour l'administration des clients

Les étapes à suivre pour se connecter en bureau distant depuis le serveur à des clients en utilisant une console d'administration centralisée sont :

1. Sur le serveur WS2008 : mmc.exe → bureaux à distance
2. Sur le client : autoriser le bureau à distance
3. Sur le client : ajouter des utilisateurs autorisés

4 Création objets utilisateurs et ordinateurs AD

ADDS contient une ancienne base SAM en + de la base LDAP.

Noms associés au compte utilisateur de domaine :

- Nom UPN (nom complet) = guillaume@woodgrovebank.com
- CN=guillaume,OU=CustomerService,OU=Miami,DC=Woodgrovebank,DC=com

  (du plus près de l'utilisateur jusqu'au plus loin)

Verrouillage de compte : mauvais mot de passe (action automatique de la machine)

Désactivation de compte : action de l'administrateur

Copie de compte utilisateur (contient les infos propres à tous les membres du conteneur) :

- Le renommer en « *ModeleDuConteneur* » + *Désactiver* le compte (allège la saisie lors des créations : groupes, bureaux, etc.)
- Faire une copie de ce compte lorsqu'on veut créer un nouvel utilisateur sans le même conteneur

Utilisation du compte d'ordinateur :

- Active Directory (=AD=ADDS) gère chaque nom d'ordinateur en lui attribuant un SID (un identifiant unique). Si 2 ordinateurs on le même nom sur le domaine : l'ancien compte d'ordinateur est supprimé et il faut réparer l'erreur, le sortir du domaine puis le réintégrer dans le domaine.
- On peut désigner un nom d'ordinateur ayant droit d'intégrer une machine dans le domaine (avant même de l'intégrer au domaine, il suffit d'ajouter un objet Ordinateur ayant le même nom que la machine qui sera intégrée).

5 Automatisation de l'administration des objets ADDS

- Console « Utilisateurs et Ordinateurs Active Directory »
- Outils de services d'annuaire (commandes MSDOS : **dsadd**, **dsmod**, **dsrm** ...)
- Commandes MSDOS **csvde** et **ldifde**

Utilisation du Powershell (remplaçant de l'invite de commande MSDOS, le powershell est un language) :

- Pour ajouter un utilisateur :

```
C:\> dsadd user "CN=Lionel,OU=Marketing,OU=Toronto,DC=Woodgrovebank,DC=com"
```

- Pour extraire des informations utilisateur (mode séquentiel)

```
C:\> LDIFDE
```

- Pour extraire des informations utilisateur (mode tableur séparé par des ;) : plus facile pour les exports

```
C:\> CSVDE
```

6 Présentation des groupes

Un groupe est défini par son type :

- groupe de sécurité (dispose d'un SID) permet de tout faire
- groupe de distribution → à des fins de messagerie seulement

Un groupe est aussi défini par son étendue (périmètre d'utilisation) :

- groupes globaux
- groupes de domaine local
- groupes universels

6.1 Niveau fonctionnel (NF)

WS2000, WS2003, WS2008 ont des nouveaux champs à chaque nouvelle version qui sont automatiquement mis à jour. Si des serveurs WS2000/WS2003 cohabitent, il faut s'adapter au plus ancien. Il faut donc désactiver les fonctionnalités des DC plus récents.

Système d'exploitation							Niveau de fonctionnalité (NF) disponible
	NT	2000 mixte					
	2000	2000 mixte	2000 natif				
	2003	2000 mixte	2000 natif	2003			
	2008		2000 natif	2003	2008		
	2008R2		2000 natif	2003	2008	2008R2	

Les serveurs (même 2003) qui fonctionnent en NF 2000 mixte doivent changer de NF avant de passer à 2008 !

Avant de changer de NF :

- sauvegarder
- vérifier sur le site TechNet quelles sont les fonctionnalités disponibles du NF
- Si ça fonctionne, pourquoi changer ?

Il y a un niveau fonctionnel de foret, et un niveau fonctionnel de domaine

- Il peut y avoir une foret NF2008 avec des domaines NF2003.

Groupes globaux :

- membres : utilisateurs du même domaine que celui du groupe global
- c'est un conteneur d'utilisateurs ayant des besoins similaires
- exemple : G_Stagiaires_Prem / G_Stagiaires_Sage

Groupes universel (beaucoup moins utilisés) :

- membres : pas de restriction, dans la même forêt
- c'est une combinaison de groupes présents sur plusieurs domaines
- autorisations sur tous les domaines de la foret
- ils sont dupliqué sur tous les DC des domaines de de la foret → éviter de les utiliser
- Exemple : U_Stagiaires / U_animateurs *(tous les animateurs, tous les stagiaires*)

groupes de domaines locaux :

- membres : de tous les membres de la foret
- autorisations attribuées au sein du domaine ou existe le groupe de domaine local

6.2 Imbrication des groupes (très important)

Microsoft recommande l'imbrication de type **AGDuLP** :

- A (comptes utilisateurs)
- G (Groupes globaux). Ces Groupes globaux peuvent faire partie d'autres Groupes globaux si besoin.
- U (Groupes Universels). Si il y a plusieurs forêts avec des relations d'approbations) : généralement pas le cas
- DL (Groupes de Domaine Local)
- P (permissions sur les répertoires partagés)

Marche à suivre :

1. On crée les utilisateurs
2. On crée les groupes globaux (G_service paye ...) → dans le cas de multi-domaines
3. On crée les groupes de domaine local (DL_accès) en lecture pour SRVFIC1-Partage1
4. On crée les permissions (ACL)

A retenir : AG(U)DLP

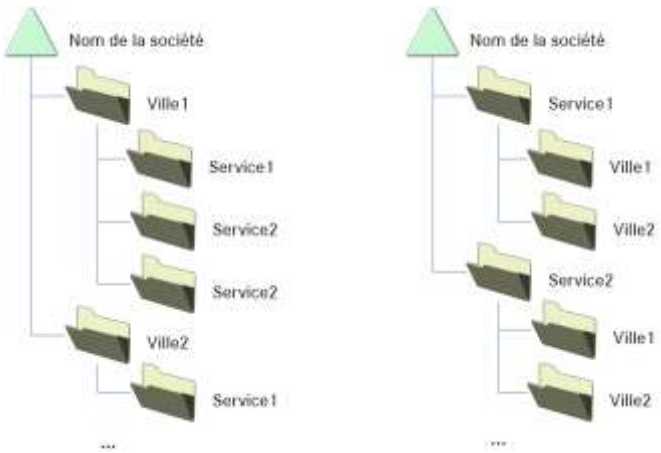
6.3 Administration des groupes

Pour modifier l'appartenance à un groupe (soit on fait à partir de l'utilisateur ou à partir du groupe)

6.4 Création des unités d'organisation (OU)

On crée d'abord les unités d'organisation puis, quand on crée un nouvel utilisateur, on le place directement dans une OU

Exemples d'arborescences :



Une OU sert à :

- Délégation administrative (délégation de droits)
- Stratégies de groupe (GPO)
- Représenter des structures logiques

Pour supprimer une OU protégée contre la suppression :

Gestionnaire de serveur > Affichage > Fonctionnalités avancées

7 Gestion de l'accès aux ressources dans les services de domaine ADDS

7.1 Qu'est-ce qu'une entité de sécurité

S – 1 – 5 – 21 – Id_de_Domaine – Id_de_l'objet_(au_sein_du_domaine)

- S: SID (indique que c'est un SID)
- 1 : version du SID
- 5 : Id de l'autorité de certification
- 21 : Domaine AD (indique que c'est un domaine ActiveDirectory)

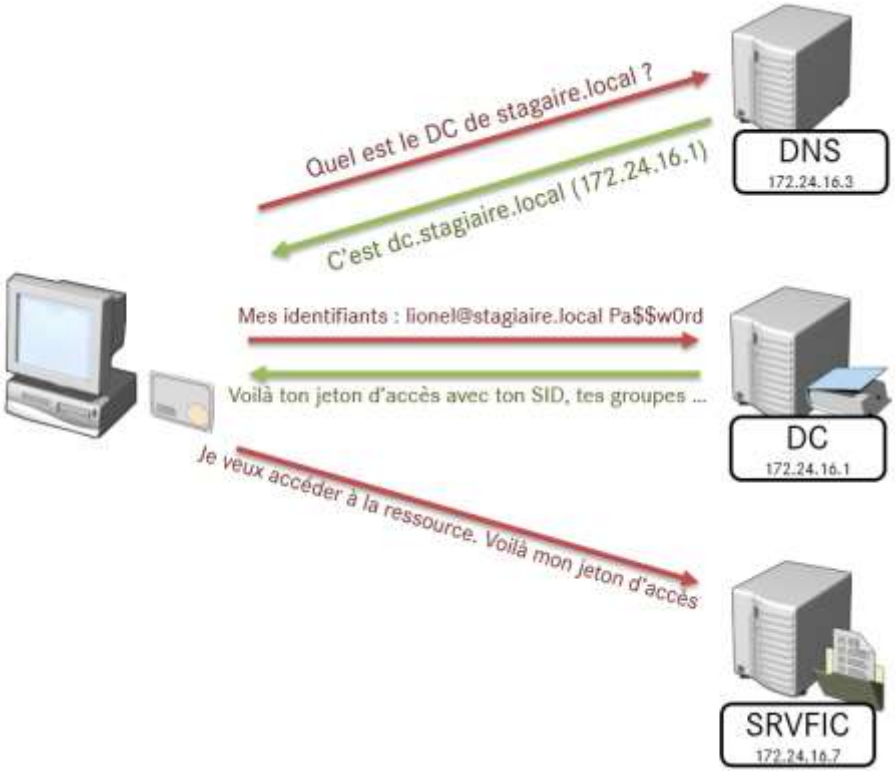
Conséquence : un utilisateur n'aura pas du tout le même SID si on le change de domaine !!!

- Son Id_de_Domaine et son Id_de_l'Objet seront différents !

7.2 Qu'est-ce qu'un Jeton d'Accès

Procédure d'authentification :

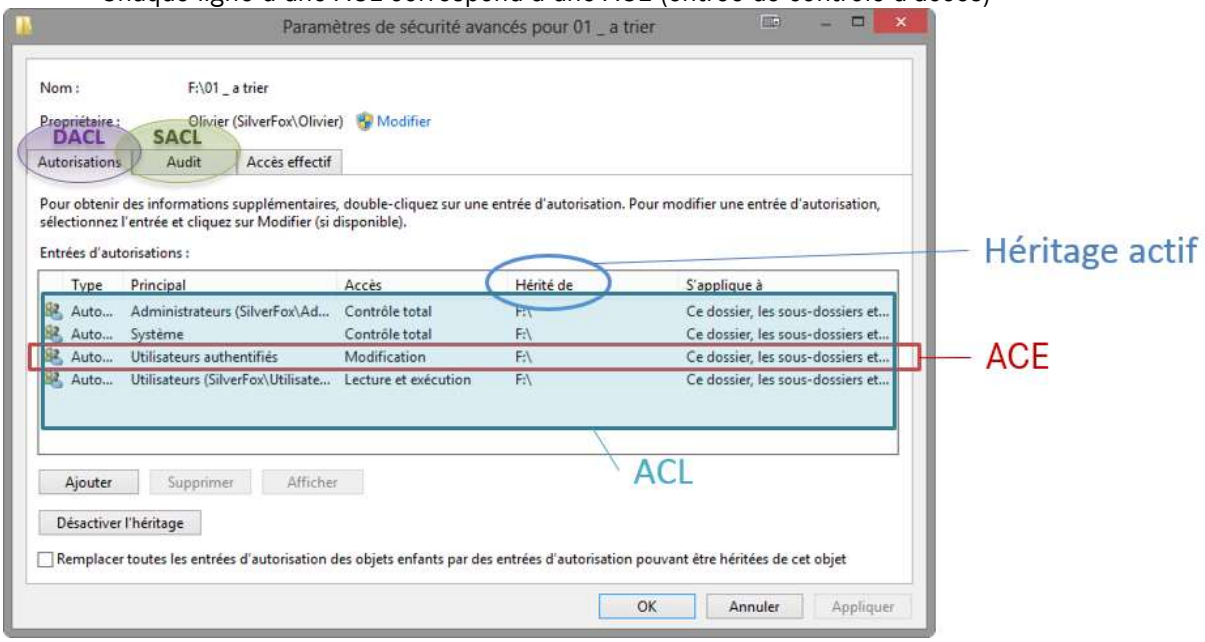
1. Interrogation du DNS : « quel est le poste ADDS pour stagiaires.local ? »
2. DNS répond : « c'est DC.stagiaires.local 172.24.16.1 »
3. envoi des identifiants au DC : « Lionel@stiagiaires.local Pa$$w0rd »
4. DC renvoie le Jeton d'Accès contenant : SID Lionel, SID G_Stagiaires, G_M74 ...)
5. quand Lionel veut accéder à une ressource, il renvoie l'intégralité des SID contenus dans le jeton d'accès.



7.3 En quoi consistent les autorisations

Dossier > Propriétés > Sécurité > Avancés

- Autorisations → DACL
- Audit → SACL
- Chaque ligne d'une ACL correspond à une ACE (entrée de contrôle d'accès)



Paramètres avancés de l'onglet sécurité d'un répertoire

Exemples d'entrées dans les ACL (préconisation Microsoft) :

- DL_accès en lecture sur SRV1-Partage → G_Marketing
- DL_accès en CT sur SRV1-Partage → G_ITAdmins
- DL_REFUS en lecture sur SRV1-Partage → G_BranchManagers
- DL_accès en modification sur SRV1-Partage → G_Investments

On fait les droits en fonction du nom des DL

Les croix grisées (dans la partie Autorisations) sont héritées d'un répertoire parent

- Si on ne modifie pas l'héritage, il y a juste besoin de modifier et appliquer les droits.
- Si on modifier l'héritage. Copie = copie les droits des parents ; Supprimer = enlève tous les droits hérités

Autorisations effectives permet de connaître les autorisations d'un utilisateur en particulier en fonction des autorisations appliquées.

Rappel : un refus explicite prime sur des autorisations explicites.

Les refus hérités d'un répertoire parents ne priment pas sur les autorisations explicites

Remplacer toutes les autorisations (case à cocher) :

- Remplace les autorisations des répertoires enfants par celles du répertoire actuel

7.4 Effets de la copie et du déplacement sur les autorisations NTFS

	Même partition	Partition différente
Copie	hérite	hérite
Déplacement	Conserve	hérite

Le déplacement de fichiers sur une même partition est d'ailleurs plus rapide, non ? ;)

7.5 Les partages

Le filtrage se fait au plus près de la ressource :

- Imaginer le partage comme un gardien de parking de la boite (peu regardant)
- Imaginer les autorisations NTFS comme le videur à l'entrée de la boite (très regardant)

Type de droits de Partage : Lecture / Modification / Contrôle Total (CT)

Conseil : Virer « Tout le monde » → remplacer par : Utilisateurs authentifiés

Éléments à prendre en considération lors de la création d'un partage :

- Attribuer les autorisations aux groupes : **AGuDLP !!!**
- Ajouter « utilisateurs authentifiés », enlever « tout le monde »

Fichier hors connexion :

- Pour UN SEUL utilisateur (le fichier le plus récent écrase le plus ancien)
- On peut rendre un partage indisponible hors connexion à partir du serveur

7.6 Éléments à prendre en compte pour le partage avec NTFS :

- accorder les autorisations aux groupes (AGDLP)
- « refuser » seulement en cas de nécessité
- ne jamais refuser l'accès à « Tout le monde »
- CT au niveau du partage (pour Utilisateurs authentifiés)
- affiner les autorisations au niveau NTFS

8 Configuration des objets et approbations AD

Propriétés de l'OU 'Miami' > Onglet Sécurité → autorisation au niveau de la gestion de l'OU

Délégation administrative :

C:\Windows\System32\delegwiz.inf

- personnaliser si besoin pour ajouter d'autres taches délégables.
- Exemple : autorisation de verrouiller un compte ordinateur

Pour faire de la délégation depuis un client :

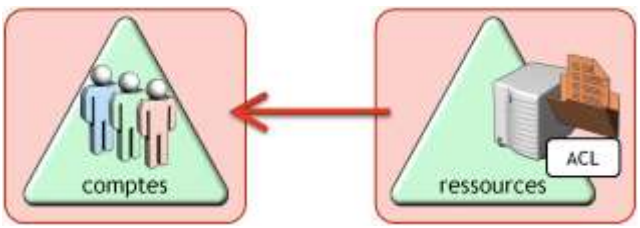
- WinXP / Win2000 → **AdminPak**
- WinVista / Win7 → **RSAT**
- … ainsi que « Délégation de contrôle »

Pour faire une console ergonomique pour le gestionnaire d'OU :

mmc.exe > utilisateurs et ordinateurs AD

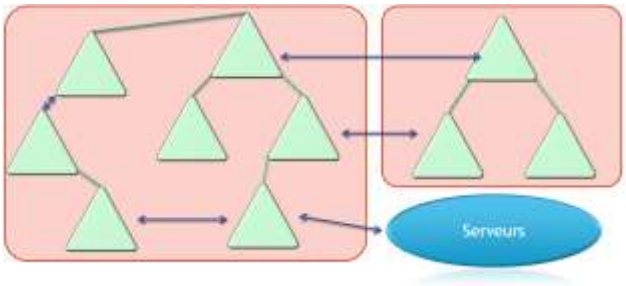
- Sélectionner l'OU
- Nouvelle fenêtre à partir d'ici
- Nouvelle vue de la liste des tâches

8.1 Approbations ADDS



La direction définit le domaine de comptes et le domaine de ressources :

- Ressources → (approuve) → Comptes



Dans une forêt, les domaines s'approuvent mutuellement (bidirectionnelle et transitive)

9 Les GPO (stratégies de groupe)

- TCO (cout total de possession) : fait baisser le déploiement et l'administration (MàJ, dépannages)
- ROI (retour sur investissement) augmente
- Une GPO permet d'automatiser la gestion des ordinateurs et des utilisateurs (pas des groupes !!)
- On peut récupérer les modèles d'administration de logiciels non prévus dans les GPO (.ADM)

Fichiers ADM :

- Attention à la langue utilisée par l'OS (peut créer des incompatibilités)
- Attention aux paramètres de l'OS plus nombreux que ceux du DC quand on utilise adminpak

Sur le serveur : C:\Windows\SYSVOL\Magasin central (pour y placer les .ADMX)

- si un magasin central existe et que l'OS client est > à XP → rechercher un magasin central
- sinon utilise les modèles d'administration locaux

Fichiers modèle client : C:\Windows\Policydefinition (fichiers ADMX)

9.1 Configuration de l'étendue des GPO :

Les GPO peuvent être :

- liées à un domaine
- liées à des OU

Attention : ne gère pas les groupes des OU mais seulement les ordinateurs et utilisateurs présents

Sur l'OU, bloquer l'héritage permet de ne pas faire s'appliquer les GPO des niveaux supérieurs

Sur la GPO appliquée : forcer la GPO la fait s'appliquer aux objets enfants, même en bloquant l'héritage

9.2 Créer une GPO :

1. Objet de stratégie de groupe (gpmc.msc), Nouveau
2. Donner un nom clair à la GPO, cliquer sur OK
3. Clic droit sur la nouvelle GPO, Modifier
4. Stratégies > Modèles d'admin > Tous les paramètres (filtres + options des filtres)
5. Cliquer/glisser la GPO là où on veut qu'elle s'applique

Filtrage de sécurité d'une GPO sélective (à faire en dernier recours) :

- Pour une GPO ne s'appliquant qu'au G_Stagiaires :
  - Ajouter le groupe G_Stagiaires + supprimer le groupe Utilisateurs Authentifiés
- Pour une GPO s'appliquant à tout le monde sauf au G_Directeurs :
  - ajouter le groupe G_Directeurs et mettre un refus explicit, laisser Utilisateurs Authentifiés

Mettre en pause une GPO → Etat GPO > Désactivé | Que la partie ordi | Que la partie utilisateur

Mode de fonctionnement par boucle de rappel :

- $GPO_{ordi\ libre}$ (s'applique avant) $GPO_{de\ l'utilisateur}$ (s'applique avant) partie ordinateur de $GPO_{ordi\ libre}$

Filtrage WMI :

- Application ou non de la GPO en fonction de caractéristiques internes de l'ordi

Résultats de la stratégie de groupe :

- Récupération des infos de GPO (il faut que la session soit active). penser à gpupdate /force

Modélisation de la stratégie de groupe :

- Simulation du résultat (on peut changer OU, Groupes, Utilisateur, Ordinateur ...)

Délégations :

Attention, selon l'objet sélectionné, les possibilités ne sont pas les mêmes

- Objet de stratégies de groupes : délégation : peuvent créer des GPO
- Sur la GPO elle-même : délégation : domaine d'application de la GPO
- OU : délégation : lier des GPO ; lancer des analyses ; lire les résultats

10 Configuration des environnements des utilisateurs et ordinateurs à l'aide de GPO

10.1 Scripts

Modification de la GPO dans gpmc.msc

Ordinateur > Paramètres Windows > Scripts (ne s'applique qu'aux ordinateurs de l'OU)

- Script de démarrage / script d'arrêt d'ordinateur
- Utilisateur > Paramètres Windows > Scripts (ne s'applique qu'aux utilisateurs de l'OU)
- Script de démarrage de session/ script de fermeture de session

10.2 Redirection de dossiers

On peut rediriger certains dossiers ciblés vers un lecteur réseau) : AppData, Bureau, Docs

Utilisateur > Paramètres Windows > Redirection des dossiers

Dossier partagé (utilisateurs authentifiés en CT)

(!) Rediriger vers l'emplacement suivant → gérer les sécurités soi-même

Mettre un chemin réseau type \\NYC-DC1\DocsUsers\ (type UNC)

10.3 Configuration des modèles d'administration

Contrôle l'environnement de l'OS (modification du registre, de l'environnement utilisateurs, etc.)

10.4 Installation de logiciels

- A partir d'un partage réseau
- que des fichiers d'installation de type .MSI
- tester l'installation automatique (ou fichiers réponses si besoin) avant de le déployer
- Attention : « publié » (dans la partie Utilisateur) laisse le choix à l'utilisateur d'installer ou non

10.5 Configuration des préférences des GPO

Préférences : permet de changer des paramètres de GPO (ex. : installation d'imprimante réseau) mais l'utilisateur peut aller à l'encontre de ces préférences.

Si l'OS du client est inférieur à WinVista, il faut installer CSE (client side extention)

10.6 Résolution des problèmes de GPO

Tout d'abord on teste si la GPO est bien récupérée et traitée avec **gpresult**

Cas ou une GPO n'est pas traitée, on lance un test :

- GPO récupérée et/ou traitée : Il y a une autre GPO qui va à l'encontre, paramètre(s) non pris en charge, etc.
- GPO non traitée : Objet non concerné, filtrage de sécurité, WMI, etc.

11 Implémentation de la sécurité à l'aide d'une GPO

11.1 But de DefaultDomainPolicy et de DefaultDomainControllerPolicy

La stratégie de compte/mot de passe se fait dans **DefaultDomainPolicy** car c'est une GPO liée au domaine ET d'ordre des liens niv.1

Ordre des liens : 5 → 1 stratégie 1 est appliquée en dernier (celle qui a le dernier mot)

Verrouillage de mots de passe fait par la GPO **DefaultDomainControllerPolicy** car c'est le DC qui gère les objets ordinateurs du domaine.

11.2 Implémentation de stratégies de mots de passe affinées

Attention : il faut être en Niveau Fonctionnel de Domaine = WS2008

- réservé aux administrateurs « qui s'y connaissent »

« But : modifier les stratégies de mots de passe pour des groupes »

1. Créer la stratégie de mots de passe affinée

Modifications ADSI > Nouveau … (Domaine) > System > Password Setting Configuration > Nouveau … Rentrer les paramètres (attention, la durée est exprimée en JJ:HH:mm:ss)

2. Lier la stratégie à un groupe

Utilisateurs et Ordinateurs AD > (affichage avancé) System > Password Setting Container > Propriétés > Sécurité > Choisir les groupes concernés

11.3 Lier un groupe AD à un groupe type SAM

Méthode :

Dans GPO > Ordinateur > Paramètres Windows > Groupes restreints ; chercher un groupe dans BuiltIn, ajouter le groupe du domaine ciblé

Stratégie de restriction logicielle :

1. Ajouter une stratégie (nouvelle stratégie de sécurité logicielle ; niveau de sécurité :
   - tout autoriser sauf …
   - tout refuser sauf … (**non recommandé**)
2. Définir les exceptions selon : règle de certificat, règle de hachage, chemin d'accès

11.4 Modèles de sécurité

Des modèles existent, mais ils sont surtout utiles pour UN rôle particulier → rare

Création assistée de modèle → tester avant !

12 Configuration de la conformité des serveurs en matière de sécurité

Il faut appliquer la sécurité à tous les niveaux afin de bloquer le niveau supérieur si un niveau est passé (livre 9-5). Le but est de verrouiller toutes les couches. Un administrateur a comme premier objectif la sécurité !

12.1 EFS (Encrypted File System)

Un certificat contient clé privée + une clé publique

Fichier clair → clé symétrique → Fichier crypté

Inconvénient de l'EFS : ne permet pas de chiffrer les données du système d'exploitation (pour ça on utilise BitLocker)

Attention : Avec EFS, si on réinitialise le mot de passe utilisateur → on ne peut utiliser ses clés. Il faut donc définir un agent de récupération

12.2 Configuration d'une stratégie d'audit

Traçabilité : utile sur une OU=Serveurs (cela permet de connaitre les mouvements effectués dans cette OU)

Ordinateur > Paramètres Windows > Sécurité > Stratégie d'audit

Doit être ciblé :

- quelle ressource à auditer ?
- quels évènements ?
- durée de l'audit ?

Exemple : tracer des utilisateurs qui suppriment des fichiers dans un répertoire partagé

- GPO : accès aux objets, réussite
- Dossier : tout le monde, suppression de dossiers
- En invite de commande :

```
C:\> auditpol /[get|list|set] /[category|subcategory]
```

- aller consulter les évènements d'audit

12.3 WSUS (9-21 ; 9-23)

« Serveur de mises à jour Windows update »

Il faut toujours tester les mises à jour avant de les déployer en production :

- Exemple : 1 groupe maquette test ; 1 groupe maquette Prod ; 1 groupe Prod1/Prod2/Prod3

C'est le client qui doit aller chercher les mises à jour. Il faut donc réaliser une GPO si besoin

wuauclt.exe force la recherche des mises à jour Windows sur le serveur WSUS

13 Configuration et gestion des technologies de stockage

La gestion du stockage fait partie des rôles de l'administrateur :

- assurer un suivi (évolution de la consommation pour prévoir les besoins)
- garder un historique : attention au seuil critique
- Augmentation justifiée ou non ? → informer les utilisateurs de la nature des docs à stocker

Analyse : capacité, cout, migration des données, quotas → **FSRM**

Quotas :

- analyser qui occupe quoi sans limiter l'espace disque
- limiter l'espace disque. Attention, l'outil de base se limite aux partitions

FSRM : Gestionnaire de Ressources de Serveur de Fichiers

13.1 Gestionnaire de Ressources de Serveur de Fichiers

Quotas :

- sur les dossiers (un quota sur l'ensemble des données contenues)
- automatique (un quota égal par sous-dossier)
- Rapport sur l'utilisation du disque

13.2 Réseaux de stockage

- Réseaux NAS : disque dur avec partage de ressources intégré → Pas cher
- Réseaux SAN : réseau dédié de stockage. Possibilités élevées, très cher (plusieurs dizaines de milliers d'€ minimum)