

# Administration Active Directory

Guillaume MATHIEU  
Directeur Technique Flexsi

# Sommaire (1/2)

## 1. Présentation de Windows Server

- Les nouveautés
- Les Best Practice

## 2. Présentation Active Directory

- Qu'est ce qu'un annuaire.
- Les notions de forêt / domaine / OU / schéma Active Directory.

## 3. Les comptes utilisateurs

- Propriétés d'un compte utilisateur.
- Les modèles de compte utilisateur.

## 4. Les comptes ordinateurs

- Présentation compte ordinateur.
- Joindre un domaine

## 5. Les groupes

- Les étendues et les types de groupe.
- Les Best Practice.

## 6. Les Unités d'organisation

- Présentation générale
- Délégation d'administration.

# Sommaire 2/2

## 7. Les stratégies de groupe

- Les grands principes
- Présentation de GPMC
- Les outils de diagnostics

## 8. Les mécanismes de réplication

- Présentation de la console Sites et Services Active Directory
- La topologie de réplication

## 9. Sauvegarde et restauration Active Directory

- Sauvegarde Active Directory
- Restauration autoritaire / la corbeille Active Directory

## 10. Notions avancées Active Directory

- Les outils de supervision / dépannage (DCDIAG, ASIEDIT, REPMON, REPADMIN).

## 11. Les services réseaux

- Le service DHCP
- Le service WINS

## 12. Sécuriser son annuaire Active Directory

- Les bonnes pratiques pour sécuriser un annuaire Active Directory

# 1. Présentation de Windows Server

# Ouverture session 1/2

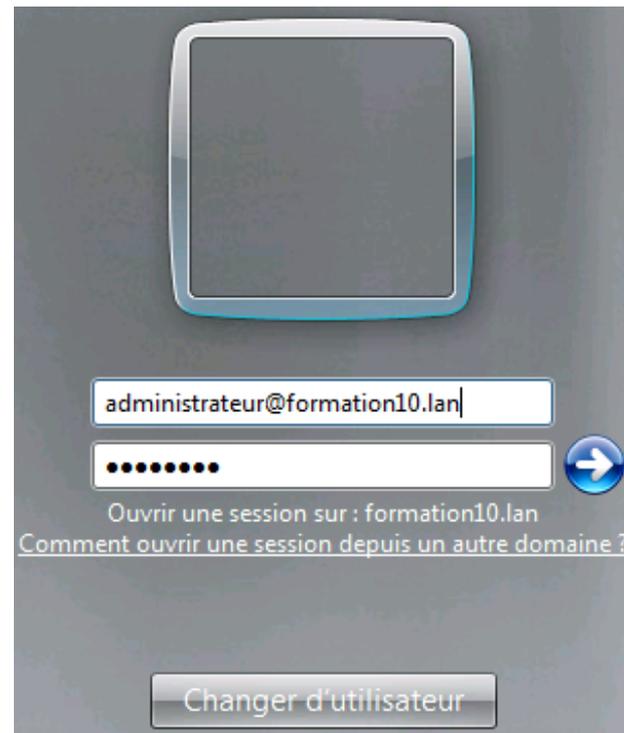
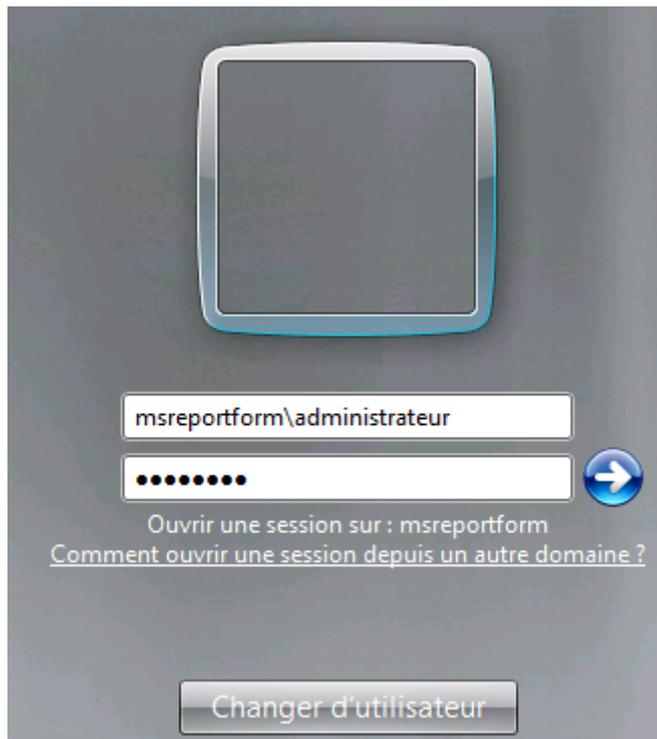
Le champ « Se connecter A » n'existe plus depuis Windows Server 2008.  
Pour se connecter à la base SAM local sur Windows Server 2008, taper :

*nom\_machine\utilisateur* ou *.\utilisateur*

Si la machine est membre d'un domaine, se connecter au domaine en tapant :

*Nom\_NETBIOS\SamAccountName* (*msreportform\administrateur*)

*UserPrincipalName* (*administrateur@formation10.lan*)



# Ouverture session 2/2

Il est possible de définir des noms de domaine DNS supplémentaires appelés suffixes UPN.

Intérêt : le login de l'utilisateur = l'adresse de messagerie (plus simple à retenir).  
Toujours vérifier que le suffixe UPN n'est pas déjà utilisé au niveau d'une autre forêt que l'on approuve.

The image shows two overlapping windows from the Windows Server management console. The background window is 'Active Directory Domains and Trusts' for the domain 'oimmil.intra'. The foreground window is 'Active Directory Users and Computers' for the same domain, showing the 'Mathieu Amelie Properties' dialog box. The 'UPN Suffixes' tab is active in the foreground window, displaying a list of alternative UPN suffixes. The 'User logon name' field in the foreground window is set to 'AMELIE.MATHIEU', and the 'User logon name (pre-Windows 2000)' field is set to 'OIMMIL\'. The 'Alternative UPN suffixes' list contains '@msreport.fr'.

Active Directory Domains and Trusts [ MILDC1.oi... ? x

UPN Suffixes

The names of the current domain and the root domain are the default user principal name (UPN) suffixes. Adding alternative domain names provides additional logon security and simplifies user logon names.

If you want alternative UPN suffixes, add them to the following list.

Alternative UPN suffixes

msreport.fr

Active Directory Users and Computers

Mathieu Amelie Properties ? x

Published Certificates	Member Of	Password Replication	Dial-in	Object
Security	Environment	Sessions	Remote control	
Remote Desktop Services Profile		COM+	Attribute Editor	
General	Address	Account	Profile	Telephones
Organization				

User logon name: AMELIE.MATHIEU @msreport.fr

User logon name (pre-Windows 2000): OIMMIL\ @msreport.fr

AMELIE.MATHIEU

# Gestionnaire de Server

## La console **Server Manager** permet :

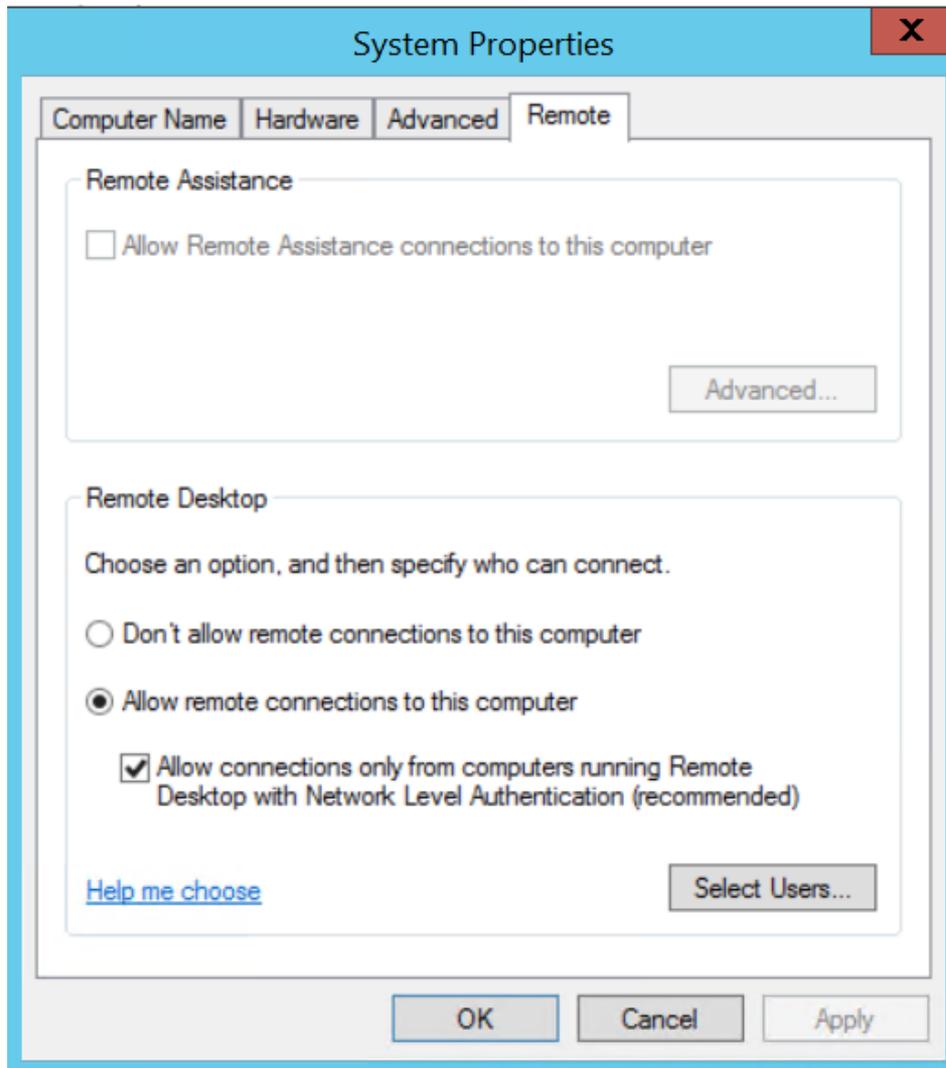
- De paramétrer le serveur (adresse IP, pare feu, bureau à distance, Windows Update).
- D'ajouter les composants Windows répartis entre rôles et fonctionnalités.
- D'activer ou de désactiver la configuration renforcée de la sécurité d'Internet Explorer (IE ESC).
- De configurer les paramètres de mises à jour.
- De se connecter à un autre serveur à distance.
- D'accéder depuis un point unique aux principales consoles pour gérer chaque rôle / fonctionnalité.

The screenshot displays the Windows Server Manager interface. The title bar reads "Server Manager". The breadcrumb navigation shows "Server Manager > Local Server". The left-hand navigation pane includes "Dashboard", "Local Server" (selected), "All Servers", "AD CS", "AD DS", "DNS", "File and Storage Services", and "IIS". The main area is titled "PROPERTIES For MILDC1" and contains a table of system settings.

Computer name	MILDC1	Last installed updates	24/01/2019 10:46
Domain	oimmil.intra	Windows Update	Install updates aut
		Last checked for updates	04/03/2019 14:53
Windows Firewall	Private: Off	Windows Error Reporting	Off
Remote management	Enabled	Customer Experience Improvement Program	Not participating
Remote Desktop	Enabled	IE Enhanced Security Configuration	Off
NIC Teaming	Disabled	Time zone	(UTC+01:00) Brussels, Copenhagen, Madrid, Paris
Ethernet	192.168.140.91, IPv6 enabled	Product ID	00252-80025-06751-AA978 (activated)

A context menu is open over the "Manage" tab, listing options: "Add Roles and Features", "Remove Roles and Features", "Add Servers", "Create Server Group", and "Server Manager Properties".

# Le bureau à distance



A ne pas confondre avec le rôle Bureau à distance (anciennement appelé Terminal Server / Terminal Server mode serveur d'applications).

La connexion entre un client RDP et le serveur RDP est chiffrée maintenant. Windows Server génère un certificat auto-signé d'où le message d'erreur lorsque que l'on se connecte à distance. Pour ne plus avoir de message d'erreur, installer un certificat reconnu qui n'a pas expiré et se connecter au serveur avec le nom indiqué au niveau du certificat.

Activer l'authentification NLA (plus sécurisé).

# PowerShell

## Présentation PowerShell :

Nouvelle interface ligne de commande / s'appuie sur le .Net Framework.  
Active Directory Center exécute en fait des commandes PowerShell.  
Extensible (ajout de CMDLETS via l'ajout de modules / snapins)

## Les commandes PowerShell indispensables :

*Get-Help nom\_cmdlet :*

*Get-Help Get-Aduser -full*

*Get-Help Get-Aduser -examples*

*Get-Modules -ListAvailable :* liste des modules installés

*Select-object :* permet de sélectionner que certains attributs de l'objet de sortie

*Install-Module XXX :* permet d'installer le module XX (nécessite MPowerShell V5).

## Les opérateurs ( < > | where -ne ), les variables \$\_.attributs et les filtres

La sortie de la première réponse devient un paramètre en entrée de la seconde commande.

Exemple (lister les utilisateurs et afficher certains attributs)

```
Get-ADUser -Filter * -SearchBase "DC=MSREPORT,DC=INTRA" -Properties * |Select-Object  
CN,LastLogonDate,MemberOf,Manager,Name,SamAccountName,  
UserPrincipalName,HomePhone | Export-Csv -UseCulture -Encoding UTF8 -Path c:\export.csv
```

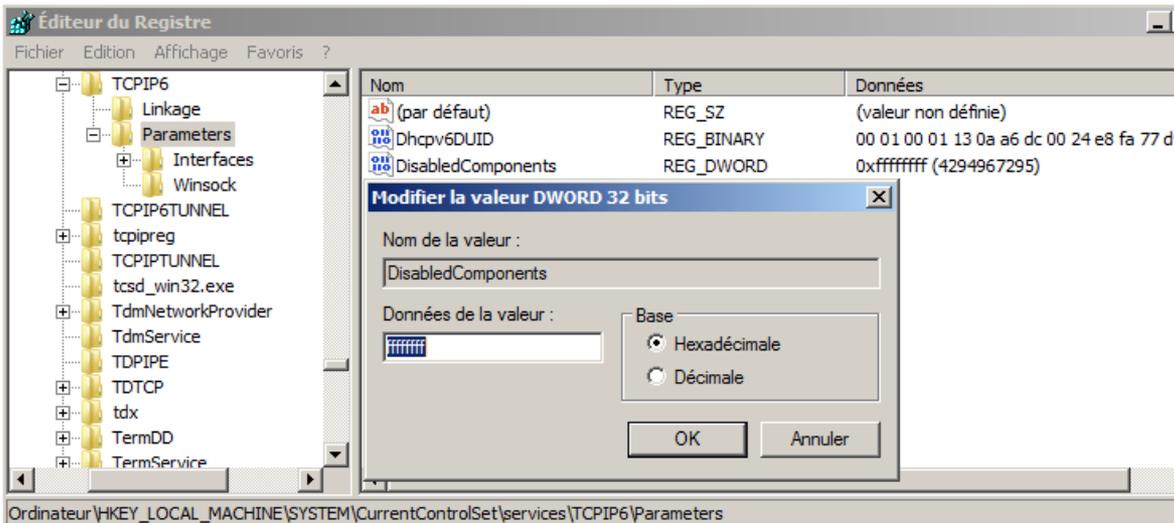
# IPV6

Les adresses IPV6 sont en DHCP. Cela génère donc des messages d'erreurs lorsque l'on fait un DCPROMO (Windows 2008 R2)

Pour désactiver IPV6, il ne faut pas décocher la case IPV6 au niveau des propriétés TCP/IP de chaque carte réseau. Créer la valeur DWORD 32 Bits *DisabledComponents* avec la valeur *FF*.

En fixant *DisabledComponents* à 0x20, on configure IPV4 comme protocole prioritaire sur IPV6 (configuration recommandée)

<http://support.microsoft.com/kb/929852/en-us>



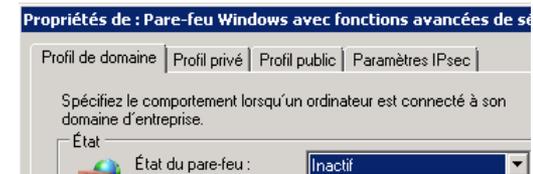
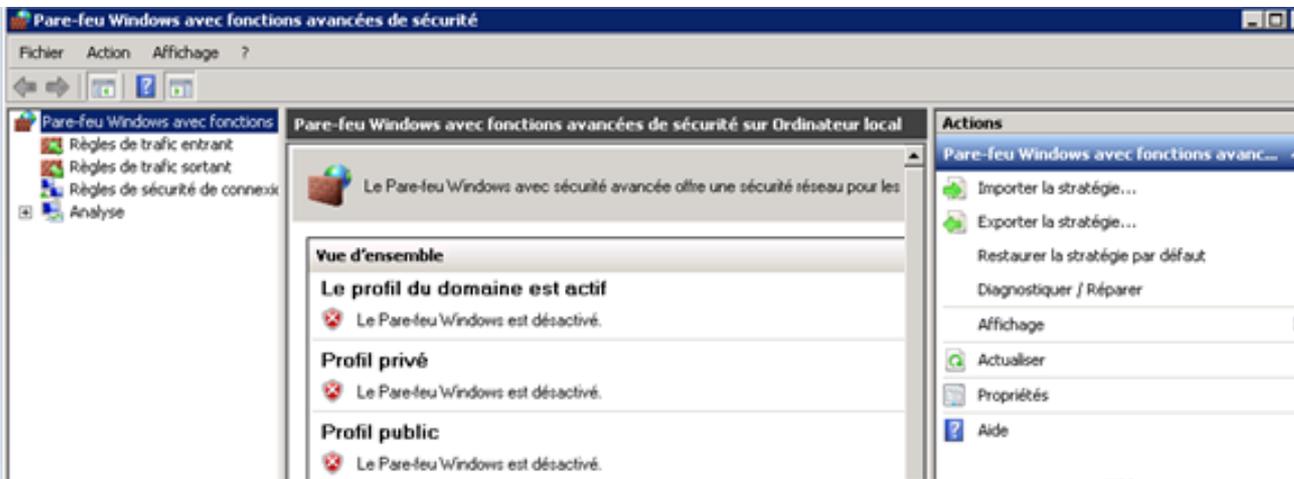
# Le pare feu Windows

Par défaut depuis Windows Server 2008 / 2008 R2 le pare feu est activé. Il est recommandé de conserver le pare feu actif.

## Si vous souhaitez désactiver le pare-feu Windows :

Toujours passer par la console « *Pare feu avec Fonctionnalités avancées* ». En effet, le pare feu de Windows Server 2008 / 2008 R2 dispose de 3 profils (public, privé, domaine).

Il faut bien penser à désactiver la pare-feu pour les 3 profils.

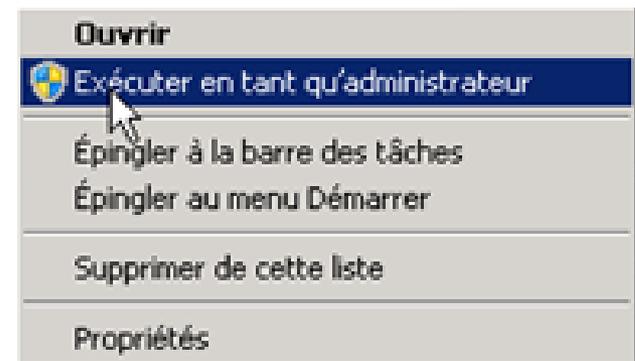
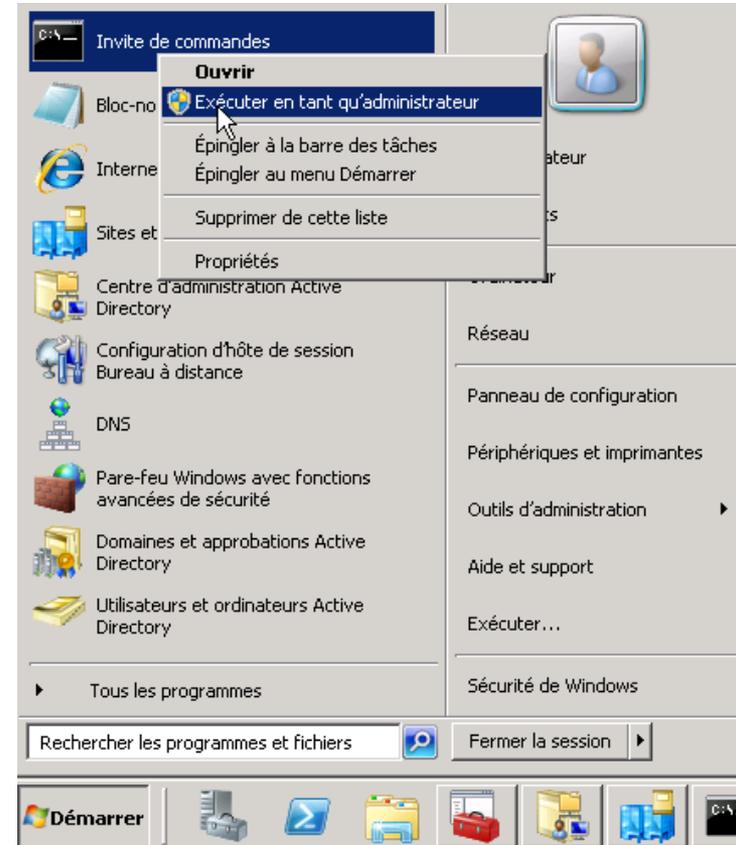
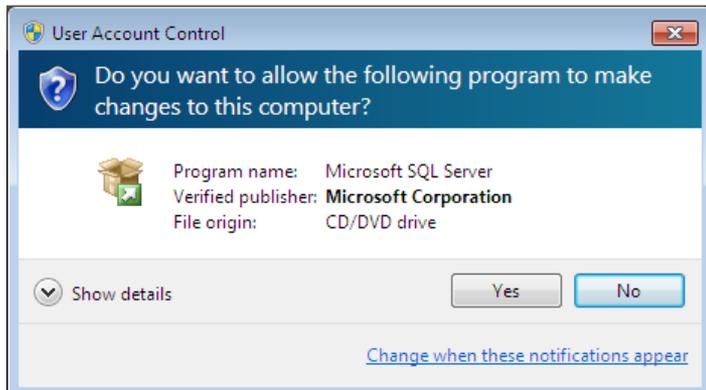


# L'UAC (1/2)

Quand on se logue sur une machine, un TGT est créé. Ce dernier liste le ou les SID du compte utilisateur et de tous les groupes auxquels le compte utilisateur appartient.

L'UAC permet de générer un second ticket. Tous les SID des groupes avec des privilèges importants comme « *Administrateurs* » sont supprimés. L'utilisateur utilise par défaut ce second ticket.

Pour pouvoir bénéficier de toutes les fonctionnalités, il faut cliquer sur OK ou exécuter le programme en tant qu'administrateur. L'UAC est paramétrable par stratégie de groupe.



# L'UAC (2/2)

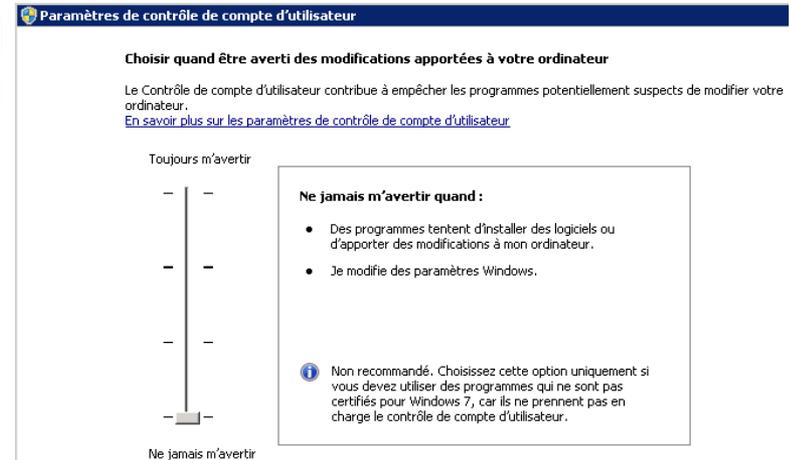
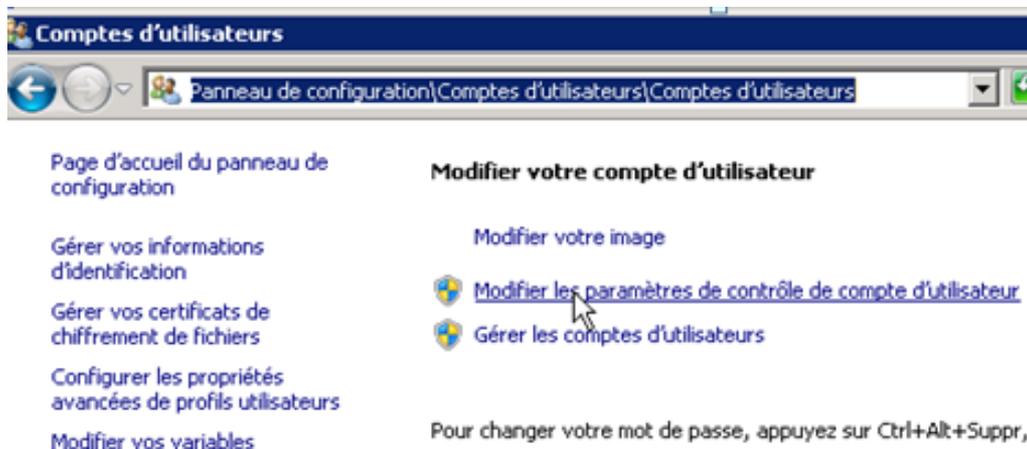
Par défaut depuis Windows Server 2008 / 2008 R2 l'UAC est activé.

Il est recommandé de laisser actif l'UAC. Cependant ce dernier peut générer des problèmes avec certains scripts ou des applications qui lancent des scripts. On peut avoir des accès refusés par exemple lors de l'exécution de certains scripts.

## Comment désactiver l'UAC

Sous Windows 2008 R2, aller dans le *Panneau de configuration | Comptes utilisateurs*. Il faut redémarrer obligatoirement.

A partir de Windows 2012, lancer la console GPEDIT et définir l'option de sécurité *User Account Control: Run all administrators in Admin Approval Mode*.

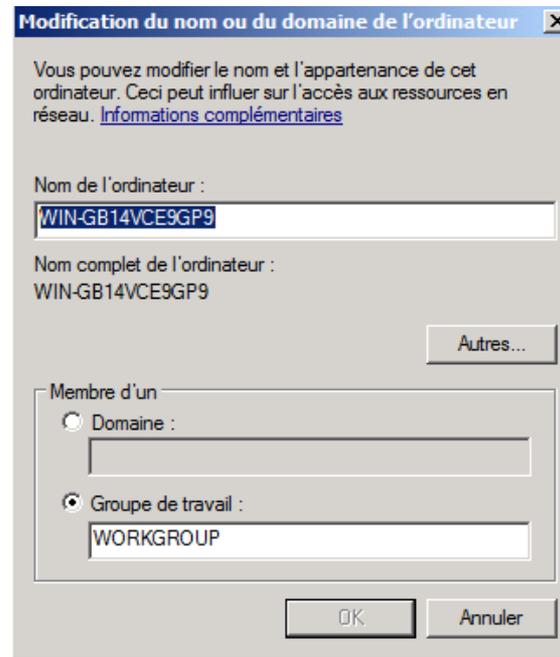
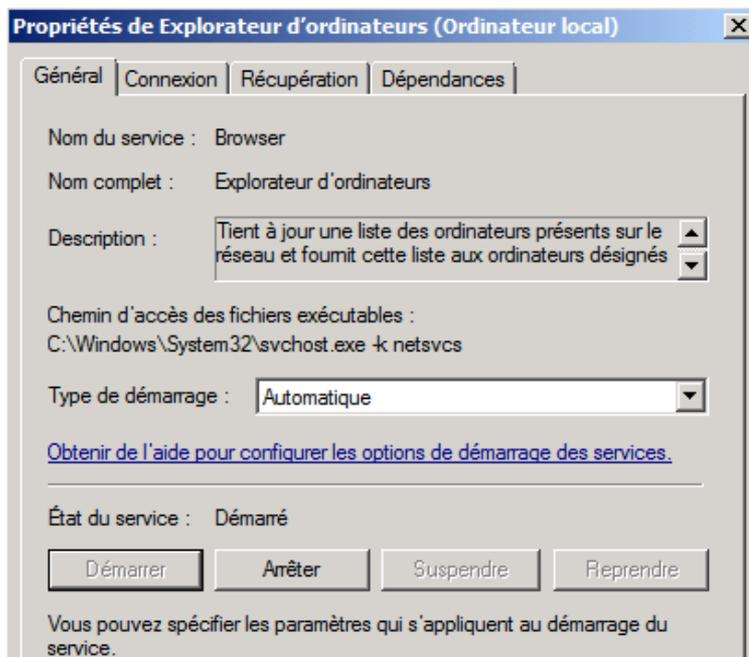


# Renommer / activer Windows

## Renommer la machine :

A l'installation, Windows génère un nom aléatoire. Penser à renommer.  
Ne pas renommer un serveur déjà promu en tant que contrôleur de domaine.

Pour activer Windows, il faut aller dans *Panneau de configuration* | *Systeme et sécurité* puis cliquer sur « *Systeme* ». Cliquer ensuite sur « *Modifier la clé produit* ». Cela va lancer automatiquement l'activation par Internet. Penser à configurer un proxy auparavant si besoin. Pour plus d'informations, voir :  
<http://msreport.free.fr/?p=153>



# TP : Windows Server

Installer Windows Server 2008 R2 ou versions ultérieures.

Renommer la machine.

Configurer la machine en IP fixe. A quoi sert un masque de sous réseau, une passerelle, un serveur DNS, un serveur Wins ?

Qu'est ce que l'APIPA, la configuration alternative (visible si station en DHCP).

Installer le rôle serveur de fichiers (installer tous les services de rôles).

Installer le rôle IIS. N'installer que les services de rôles proposées par défaut.

Quels sont les modules IIS installés par défaut ?

Activer le bureau à distance sur son serveur et accéder au serveur d'un collègue de son choix. Pourquoi y a-t-il un message d'avertissement ?

Désactiver la configuration renforcée de la sécurité d'Internet Explorer pour les administrateurs. Quels risques en terme de sécurité ?

Lancer PowerShell.

Exécuter la commande PowerShell *Get-Modules -ListAvailable*

Exécuter la commande Powershell *Get-Alias dir* et *Get-Alias ls*

Comparer PowerShell avec l'invite de commande CMD.

# **2. Présentation Active Directory**

# Qu'est ce qu'un service d'annuaire ?

## Un service d'annuaire permet :

D'identifier des ressources.

Offre une méthode cohérente pour nommer, décrire, rechercher, accéder, gérer et sécuriser l'accès aux ressources de l'entreprise.

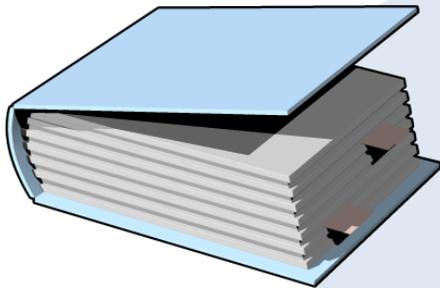
## Les limites Active Directory (taille, nombre d'objets...) :

<http://technet2.microsoft.com/windowsserver/en/library/d2fc40d8-50ba-450c-959b-28fd7e31b9961033.msp?mfr=true>

## Fonctionnement avancé :

[http://technet.microsoft.com/en-us/library/cc772829\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc772829(WS.10).aspx)

**Différence base SAM avec AD :** AD est annuaire centralisé (accessible depuis plusieurs machines). Une base SAM est un annuaire local.



## Les atouts d'Active Directory

- Intégration DNS
- Administration déléguée
- Gestion centralisée
- Intégration standards LDAP, DNS, KERBEROS
- Les GPO
- Tolérance au panne.
- PowerShell
- Extensible (mise à jour schéma)

# Les consoles d'administration 1/2

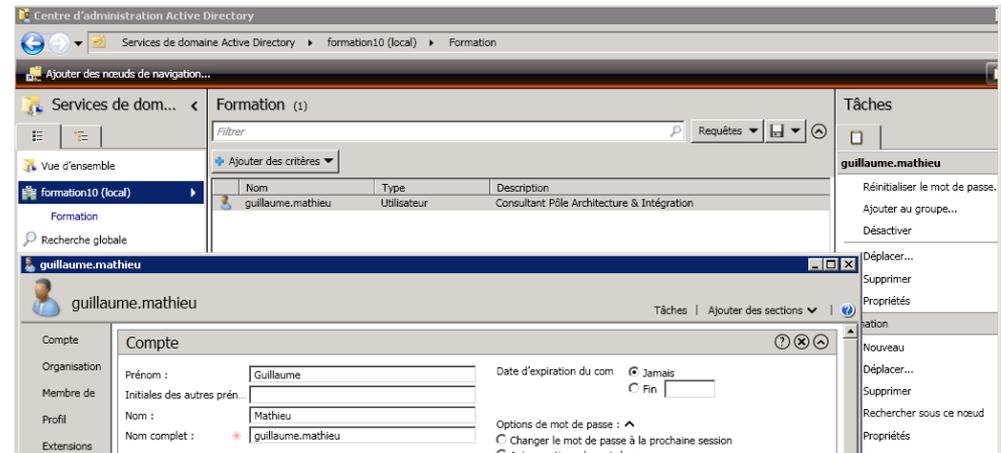
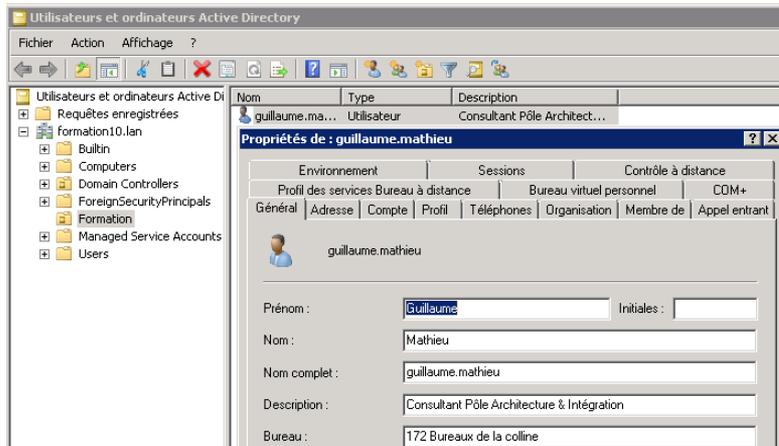
**Utilisateurs et Ordinateurs Active Directory** : permet de créer les comptes utilisateurs, groupe, compte ordinateur, OU.

**Active Directory Centre d'administration** : permet de créer les comptes utilisateurs / ordinateurs, groupes, unités d'organisation (OU). Console très orientée tâches d'administration quotidiennes (créations de comptes...).

**Sites et Services Active Directory** : permet de forcer la réplication Active Directory et de gérer les services qui se basent sur Active Directory.

**Domaine et Approbation Active Directory** : permet de gérer les suffixes UPN et les relations d'approbation.

**Active Directory Module for Windows PowerShell** : permet de créer les comptes utilisateurs / ordinateurs, groupes, unités d'organisation (OU) en ligne de commande ou à l'aide de script.

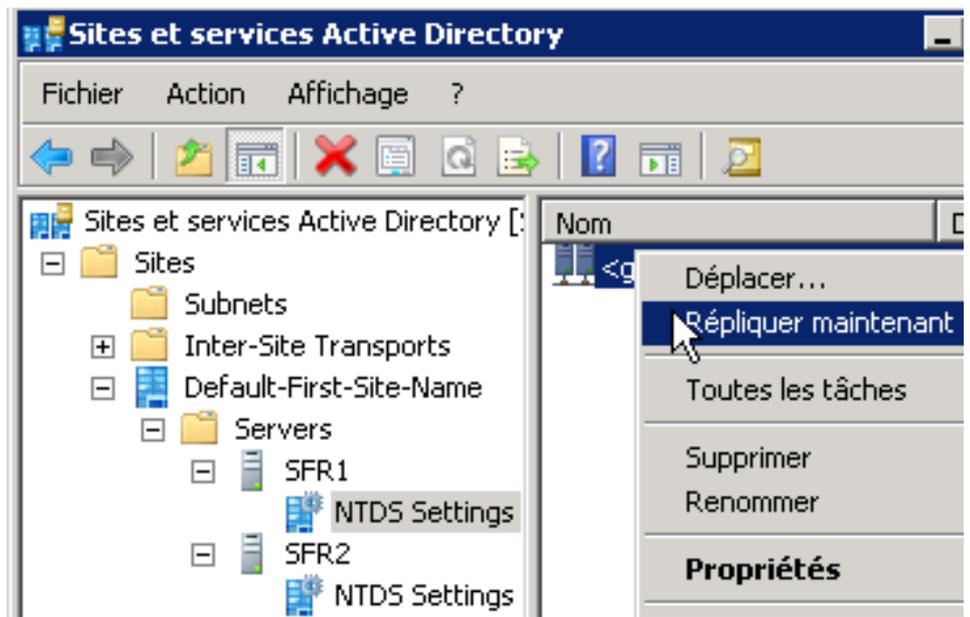
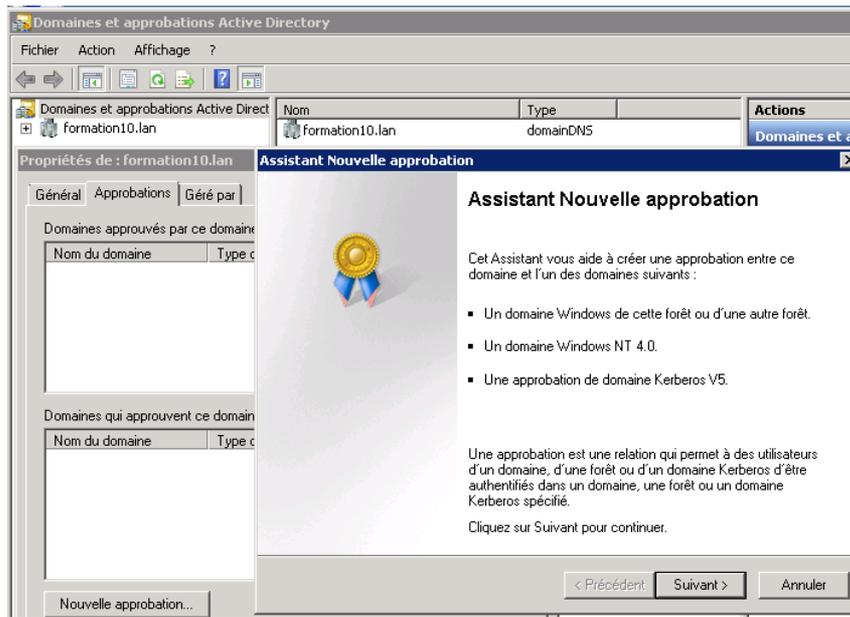


# Les consoles d'administration 2/2

```
Administrator: Active Directory Module for Windows PowerShell
PS C:\Users\guillaume.mathieu> New-ADUser

cmdlet New-ADUser at command pipeline position 1
Supply values for the following parameters:
Name: PS C:\Users\guillaume.mathieu> New-ADUser

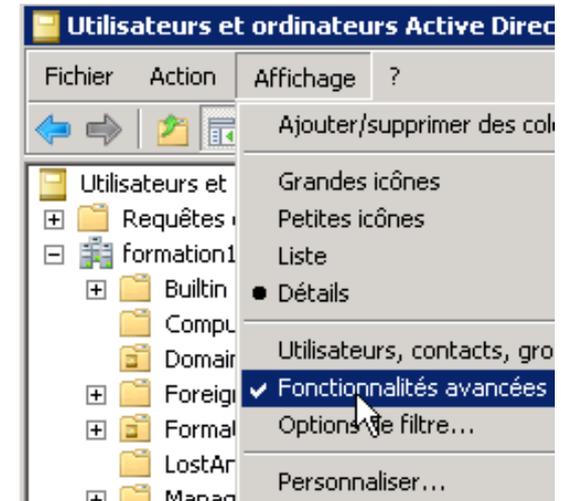
cmdlet New-ADUser at command pipeline position 1
Supply values for the following parameters:
Name: guillaume.mathieu2
PS C:\Users\guillaume.mathieu> New-ADUser -name guillaume.msreport -GivenName guillaume
PS C:\Users\guillaume.mathieu> _
```



# TP : Zoom sur ADUC 1/2

Si l'on active le mode d'affichage « Fonctionnalités avancées », les conteneurs suivants apparaissent :

- Lost and Found : contient tous les objets en conflits.
- Program Data : conteneur vide, permet à des applications de stocker des données spécifiques à une application.
- NTDS Quota : contient les objets quotas qui permettent de limiter le nombre d'objets que peut créer un compte utilisateur. Le but est de se protéger des attaques par déni de service.
- System : contient tous les dossiers systèmes nécessaires aux bons fonctionnement d'Active Directory (les objets pour les stratégies de groupe...).

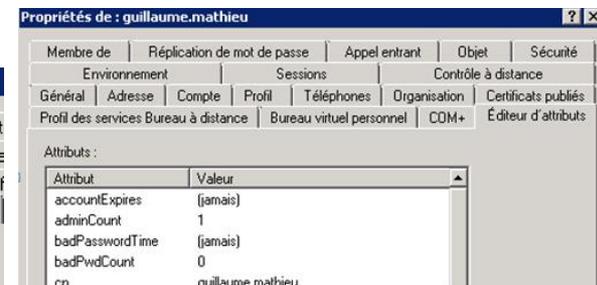


# TP : Zoom sur ADUC 2/2

**MSA / gMSA** : comptes de services gérés (nouveau 2008 R2 / 2012). Cela permet de changer le mot de passe d'un compte de service sans avoir à changer le mot de passe dans la configuration du service.

**Passer en mode « Fonctionnalités avancées » permet d'afficher des onglets supplémentaires au niveau des propriétés des objets :**

- Editeur d'attributs: sorte d'ADSIEDIT intégré au niveau des propriétés d'un compte utilisateur.
- Objet : permet de déterminer où se trouve l'objet (pratique pour les recherches) et de désactiver la protection contre la suppression accidentelle.
- Réplication des mots de passe : permet de déterminer si l'on peut mettre en cache le mot de passe sur les RODC.



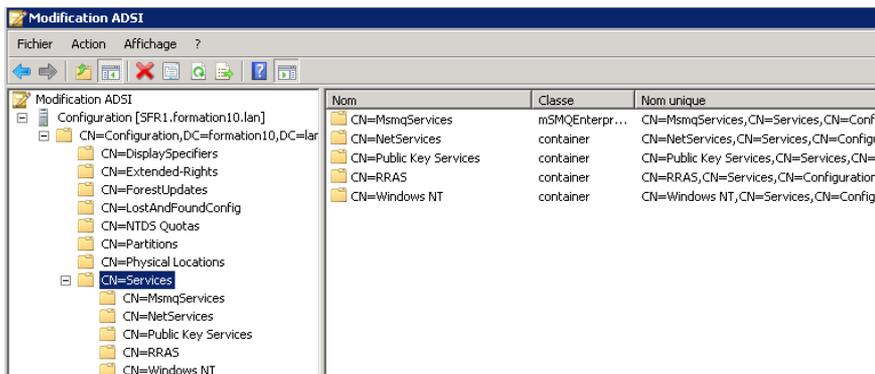
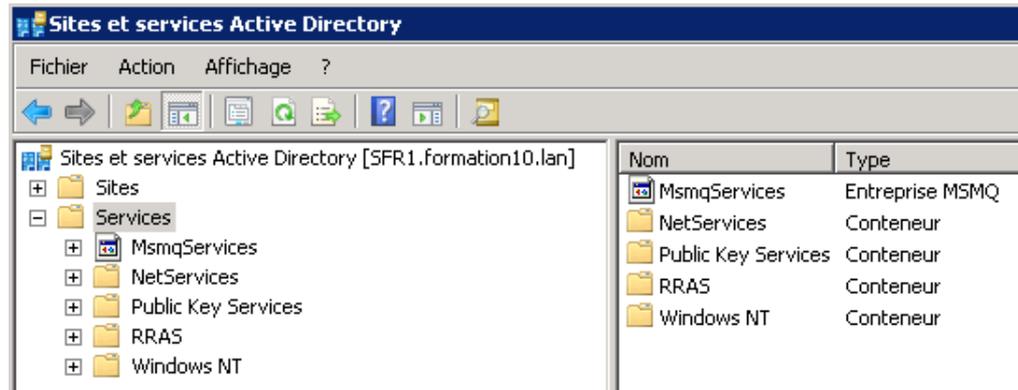
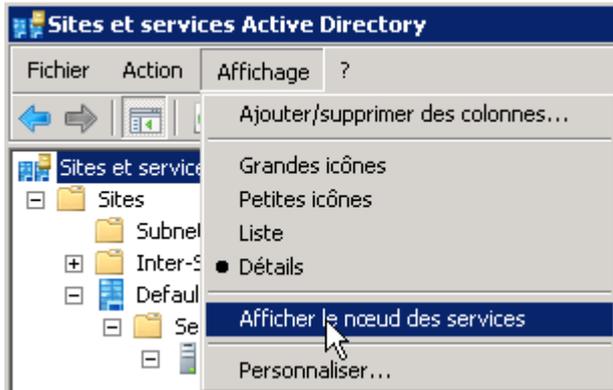
# TP : Zoom sur la console Sites et Services

**La console Sites et Services n'affichent pas par défaut le nœud « services » :**

Ce nœud permet d'avoir une vue simplifiée du conteneur « Services » dans la partition de configuration de l'annuaire Active Directory.

**Pour afficher le nœud services :**

Ouvrir la console Sites et Services Active Directory. Sélectionner la racine de la console et cliquer sur *Affichage | Afficher le nœud des services*.



# Le service DNS 1/3

Protocole permettant de résoudre un nom DNS ([www.google.fr](http://www.google.fr)) en une adresse IP et inversement.

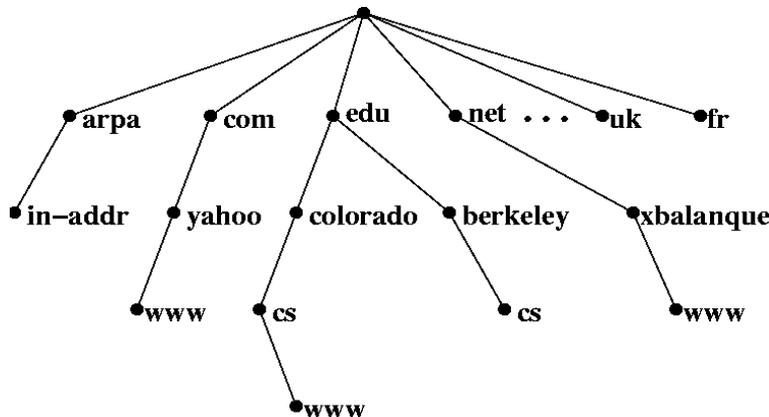
Deux systèmes de résolution de noms :

- Zone de recherche directe : résout un nom en IP.
- Zone de recherche inversée : résout une IP en nom.

L'espace de noms DNS est découpé en zones DNS. Ces zones sont réparties sur des milliers de serveurs DNS.

L'interconnexion entre serveurs DNS se fait via le mécanisme de délégation et de redirection.

Afin de fournir une tolérance de panne et de répartir la charge, un serveur DNS peut disposer d'une copie en lecture seule (zone secondaire) de la zone d'un autre serveur en lecture / écriture (zone principale).



La capture d'écran montre l'interface 'Gestionnaire DNS' d'un serveur Windows. À gauche, l'arborescence de la console affiche 'DNS' > 'SFR1' > 'Zones de recherche directe' > 'Formation10.lan'. À droite, une table liste les enregistrements de la zone.

Nom	Type	Données
_msdcs		
_sites		
_tcp		
_udp		
_msdcs.formation10.lan		
Formation10.lan		
DomainDnsZones		
ForestDnsZones		
(identique au dossier parent)	Source de nom (SOA)	[43], sfr1.formation10.lan,...
(identique au dossier parent)	Serveur de noms (NS)	sfr1.formation10.lan.
(identique au dossier parent)	Serveur de noms (NS)	sfr2.formation10.lan.
(identique au dossier parent)	Hôte (A)	192.168.0.161
(identique au dossier parent)	Hôte (A)	192.168.0.160
sfr1	Hôte (A)	192.168.0.160
SFR2	Hôte (A)	192.168.0.161

# Le service DNS 2/3

La redirection : un serveur DNS peut rediriger les requêtes non résolues vers un autre serveur DNS.

La délégation : un serveur DNS peut déléguer une partie de l'espace de noms qu'il gère à un autre serveur (payant).

Interface : serveur DNS ne répond aux requêtes que sur certaines interfaces / IP. Un serveur DNS génère toujours une entrée de type A (Nom -> IP) pour ses interfaces en écoute même si on désactive la mise à jour dynamique DNS au niveau de la carte réseau. Problématique si des stations de travail ne peuvent pas accéder aux serveurs via certaines IP / cartes.

Le round Robin : quand on dispose de plusieurs entrées A, le serveur répond aléatoirement sur les différentes entrées.

Le TRI DNS : si plusieurs réponses possibles, le serveur DNS répond toujours avec une IP qui est dans le même réseau IP que la machine qui a fait la requête (prioritaire sur le Round Robin).

Mise à jour dynamique DNS : activable au niveau des zones DNS. Commande `ipconfig /registerdns` permet de forcer création enregistrement A et PTR d'une machine Windows (mise à jour dynamique DNS).

# Le service DNS 3/3

**Propriétés de : SFR1**

Enregistrement des événements | Ancres d'approbation | Analyse | Sécurité

Interfaces | Redirecteurs | Avancé | Indications de racine | Enregistrement de débogage

Les indications de racine résolvent les requêtes concernant des zones qui n'existent pas sur le serveur DNS local. Elles sont uniquement utilisées si les redirecteurs ne sont pas configurés ou s'ils ne répondent pas.

Serveurs de noms :

Nom de domaine pleinement qualifié du serveur (FQDN)	Adresse IP
a.root-servers.net	[198.41.0.4]
b.root-servers.net	[192.228.79.201]
c.root-servers.net	[192.33.4.12]
d.root-servers.net	[128.8.10.90]
e.root-servers.net	[192.203.230.10]
f.root-servers.net	[192.5.5.241]
g.root-servers.net	[192.112.36.4]
h.root-servers.net	[128.63.2.53]
i.root-servers.net	[192.36.148.17]

**Propriétés de : SFR1**

Enregistrement des événements | Ancres d'approbation | Analyse | Sécurité

Interfaces | Redirecteurs | Avancé | Indications de racine | Enregistrement de débogage

Numéro de version du serveur : 6.1 7600 (0x1 db0)

Options de serveur :

- Désactiver la récursivité (désactive également les redirecteurs)
- Lier les zones secondaires
- Échec de chargement si les données de zone sont erronées
- Activer la fonction Round Robin
- Activer le tri de masques réseau
- Sécuriser le cache contre la pollution

Vérification de nom : Sur plusieurs octets (UTF8)

Charger les données de zone au démarrage : À partir de Active Directory et du Registre

Activer le nettoyage automatique des enregistrements obsolètes

Délai de nettoyage : 0 jours

Restaurer les paramètres par défaut

**Propriétés de : formation10.lan**

WINS | Transferts de zone | Sécurité

Général | Source de noms (SOA) | Serveurs de noms

État : En cours d'exécution [Suspendre]

Type : Intégré à Active Directory [Modifier...]

Réplication : Tous les serveurs DNS de ce domaine [Modifier...]

Données enregistrées dans Active Directory.

Mises à jour dynamiques : Sécurisé uniquement

Autoriser les mises à jour dynamiques :
 

- Aucun
- Non sécurisé et sécurisé
- Sécurisé uniquement

**Propriétés de : formation10.lan**

WINS | Transferts de zone | Sécurité

Général | Source de noms (SOA) | Serveurs de noms

Numéro de série : 48 [Incrémentier]

Serveur principal : sfr1.formation10.lan [Parcourir...]

Personne responsable : hostmaster.formation10.lan [Parcourir...]

Intervalle d'actualisation : 15 Minutes

Intervalle avant nouvelle tentative : 10 Minutes

Expire après : 1 Jours

Durée de vie minimale (par défaut) : 1 Heures

Durée de vie pour cet enregistrement : 0 : 1 : 0 : 0 (JJJ:HH:MM:SS)

**Propriétés de : formation10.lan**

Général | Source de noms (SOA) | WINS | Transferts de zone

Un transfert de zone envoie une copie de la zone aux serveurs qui font la demande.

Autoriser les transferts de zone :

- Vers n'importe quel serveur
- Uniquement vers les serveurs listés dans l'onglet Serveurs
- Uniquement vers les serveurs suivants

Adresse IP	Nom de domaine complet
192.168.0.161	SFR2

**Propriétés de : SFR1**

Enregistrement des événements | Ancres d'approbation | Interfaces | Redirecteurs | Avancé | Indications de racine

Les redirecteurs sont des serveurs DNS qui permettent à résoudre les requêtes DNS liées aux enregistrements n'ayant pas été résolus.

Adresse IP	Nom de domaine complet
212.27.40.240	dns1.proxad.net

**Modifier les redirecteurs**

Adresses IP des serveurs de redirection :

Adresse IP	Nom de domaine complet du serveur	Validé
<a href="#">&lt;Cliquez ici&gt; pour ajouter une adresse IP ou un nom DNS</a>		
212.27.40.240	dns1.proxad.net	OK

**Gestionnaire DNS**

Fichier | Action | Affichage ?

- Configurer un serveur DNS...
- Créer des partitions de l'annuaire d'applications par défaut...
- Nouvelle zone...
- Définir le vieillissement/nettoyage pour toutes les zones...
- Nettoyer les enregistrements de ressources obsolètes
- Mettre à jour les fichiers de données du serveur
- Effacer le cache

**Propriétés de : formation10.lan**

Général | Source de noms (SOA) | WINS | Transferts de zone

Vous pouvez utiliser WINS pour résoudre les requêtes DNS liées aux enregistrements n'ayant pas été résolus.

Utiliser la recherche directe WINS

Ne pas répliquer cet enregistrement

**Propriétés de : SFR1**

Enregistrement des événements | Ancres d'approbation | Interfaces | Redirecteurs | Avancé | Indications de racine

Sélectionnez les adresses IP qui serviront à résoudre les requêtes DNS sur toutes les adresses IP définies ou limiter aux adresses IP sélectionnées.

Écouter sur :

- Toutes les adresses IP
- Uniquement les adresses IP suivantes :

Adresses IP :

- 192.168.0.160

# Le service DNS 3/4

Transfert de zones : permet à un serveur hébergeant une zone secondaire (en lecture seule) de télécharger la zone depuis un autre serveur.

Wins-R : le serveur DNS s'appuie les enregistrements d'un serveur WINS.

Phénomène d'Ilot DNS : <http://support.microsoft.com/kb/291382/fr>

Cache Wins sur le serveur DNS :

<http://technet2.microsoft.com/windowsserver/en/library/92654b58-b10f-4c35-ab22-389b70d94a521033.mspx?mfr=true>

Zones DNS en double : <http://support.microsoft.com/kb/867464>

Bug au niveau des zones secondaires sous Windows 2008 :

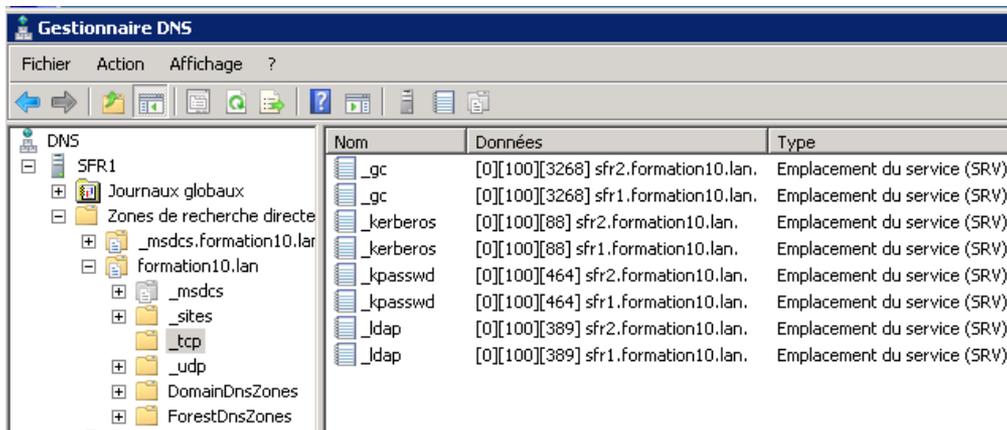
<http://msreport.free.fr/?p=145>

# Interaction DNS / Active Directory

Les stations de travail localisent les contrôleurs de domaine en effectuant des requêtes sur les enregistrements DNS suivants :

- `_ldap._tcp.org2.lan`
- `_ldap._tcp.le_nom_du_site_de_rattachement.Lan`

Les contrôleurs de domaine se servent du DNS comme d'un fichier de configuration en mettant à jour leurs enregistrements. C'est le service « *CLIENT DHCP* » qui gère cela (ne jamais désactiver ce service).

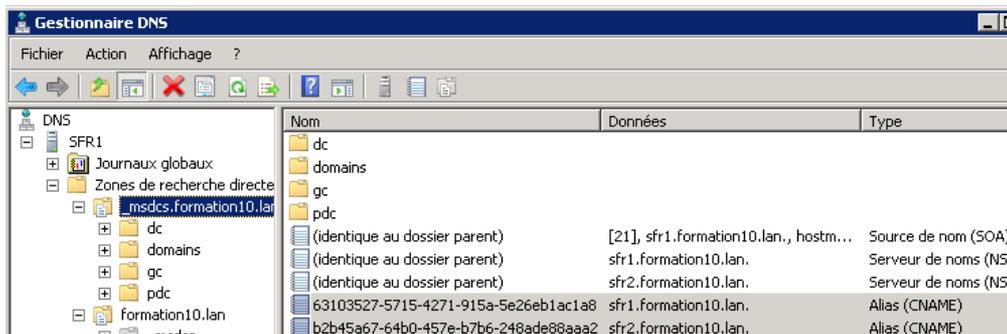


Pour localiser qui est Emulateur PDC (lors changement mot de passe...):

`_ldap._tcp.pdc._msdcs.org2.lan`

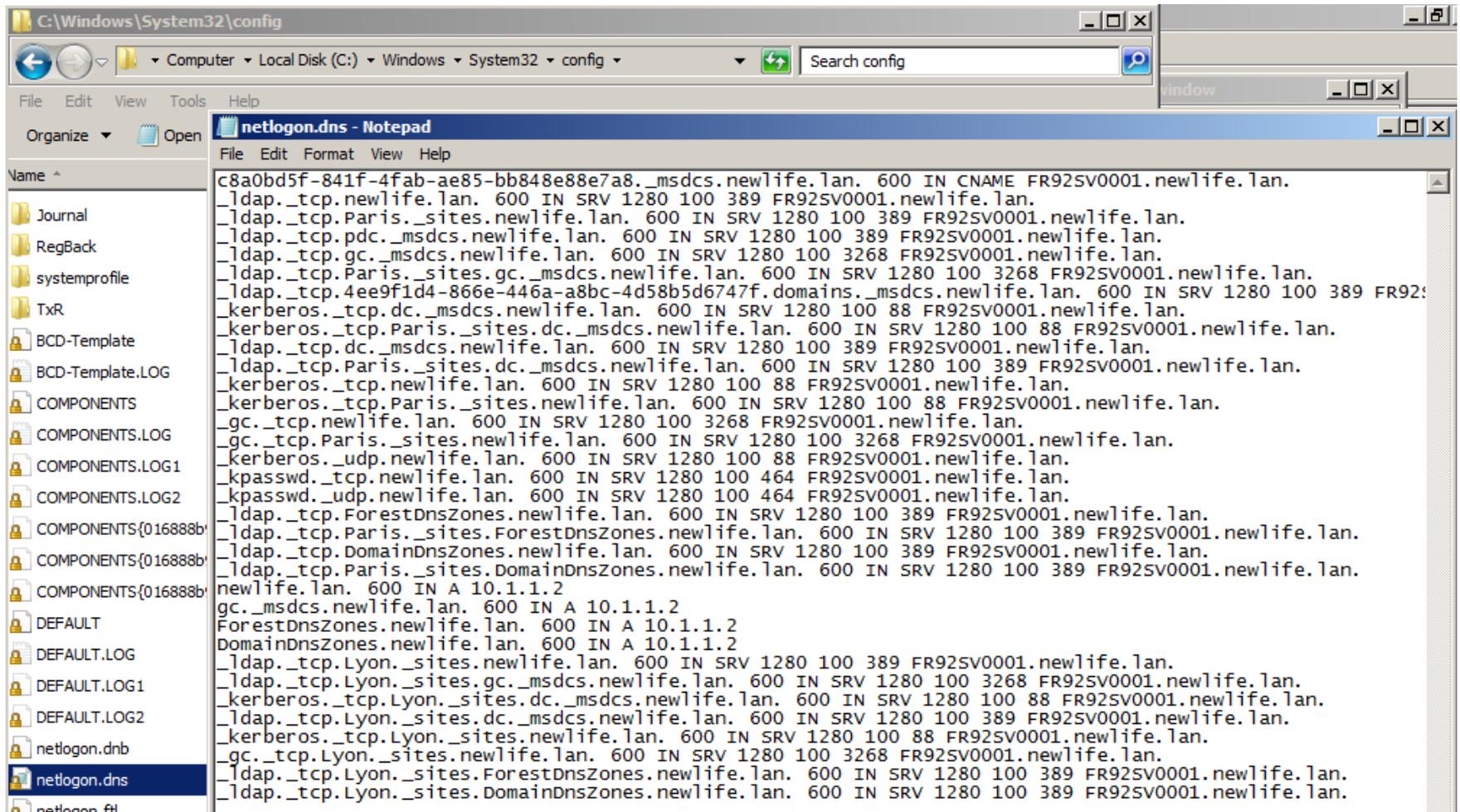
Pour forcer l'actualisation des enregistrements de services des contrôleurs de domaine (par défaut toutes les 5 minutes), taper les commandes suivantes :

*Net stop netlogon & net start netlogon*



# Le fichier Netlogon.dns

Les entrées du fichier `C:\Windows\System32\Config\Netlogon.dns` sont chargées au démarrage du service NETLOGON (`lsass.exe`) du contrôleur de domaine.



```
c8a0bd5f-841f-4fab-ae85-bb848e88e7a8._msdcs.newlife.lan. 600 IN CNAME FR92SV0001.newlife.lan.
_ldap._tcp.newlife.lan. 600 IN SRV 1280 100 389 FR92SV0001.newlife.lan.
_ldap._tcp.Paris._sites.newlife.lan. 600 IN SRV 1280 100 389 FR92SV0001.newlife.lan.
_ldap._tcp.pdc._msdcs.newlife.lan. 600 IN SRV 1280 100 389 FR92SV0001.newlife.lan.
_ldap._tcp.gc._msdcs.newlife.lan. 600 IN SRV 1280 100 3268 FR92SV0001.newlife.lan.
_ldap._tcp.Paris._sites.gc._msdcs.newlife.lan. 600 IN SRV 1280 100 3268 FR92SV0001.newlife.lan.
_ldap._tcp.4ee9f1d4-866e-446a-a8bc-4d58b5d6747f.domains._msdcs.newlife.lan. 600 IN SRV 1280 100 389 FR92:
_kerberos._tcp.dc._msdcs.newlife.lan. 600 IN SRV 1280 100 88 FR92SV0001.newlife.lan.
_kerberos._tcp.Paris._sites.dc._msdcs.newlife.lan. 600 IN SRV 1280 100 88 FR92SV0001.newlife.lan.
_ldap._tcp.dc._msdcs.newlife.lan. 600 IN SRV 1280 100 389 FR92SV0001.newlife.lan.
_ldap._tcp.Paris._sites.dc._msdcs.newlife.lan. 600 IN SRV 1280 100 389 FR92SV0001.newlife.lan.
_kerberos._tcp.newlife.lan. 600 IN SRV 1280 100 88 FR92SV0001.newlife.lan.
_kerberos._tcp.Paris._sites.newlife.lan. 600 IN SRV 1280 100 88 FR92SV0001.newlife.lan.
_gc._tcp.newlife.lan. 600 IN SRV 1280 100 3268 FR92SV0001.newlife.lan.
_gc._tcp.Paris._sites.newlife.lan. 600 IN SRV 1280 100 3268 FR92SV0001.newlife.lan.
_kerberos._udp.newlife.lan. 600 IN SRV 1280 100 88 FR92SV0001.newlife.lan.
_kpasswd._tcp.newlife.lan. 600 IN SRV 1280 100 464 FR92SV0001.newlife.lan.
_kpasswd._udp.newlife.lan. 600 IN SRV 1280 100 464 FR92SV0001.newlife.lan.
_ldap._tcp.ForestDnsZones.newlife.lan. 600 IN SRV 1280 100 389 FR92SV0001.newlife.lan.
_ldap._tcp.Paris._sites.ForestDnsZones.newlife.lan. 600 IN SRV 1280 100 389 FR92SV0001.newlife.lan.
_ldap._tcp.DomainDnsZones.newlife.lan. 600 IN SRV 1280 100 389 FR92SV0001.newlife.lan.
_ldap._tcp.Paris._sites.DomainDnsZones.newlife.lan. 600 IN SRV 1280 100 389 FR92SV0001.newlife.lan.
newlife.lan. 600 IN A 10.1.1.2
gc._msdcs.newlife.lan. 600 IN A 10.1.1.2
ForestDnsZones.newlife.lan. 600 IN A 10.1.1.2
DomainDnsZones.newlife.lan. 600 IN A 10.1.1.2
_ldap._tcp.Lyon._sites.newlife.lan. 600 IN SRV 1280 100 389 FR92SV0001.newlife.lan.
_ldap._tcp.Lyon._sites.gc._msdcs.newlife.lan. 600 IN SRV 1280 100 3268 FR92SV0001.newlife.lan.
_kerberos._tcp.Lyon._sites.dc._msdcs.newlife.lan. 600 IN SRV 1280 100 88 FR92SV0001.newlife.lan.
_ldap._tcp.Lyon._sites.dc._msdcs.newlife.lan. 600 IN SRV 1280 100 389 FR92SV0001.newlife.lan.
_kerberos._tcp.Lyon._sites.newlife.lan. 600 IN SRV 1280 100 88 FR92SV0001.newlife.lan.
_gc._tcp.Lyon._sites.newlife.lan. 600 IN SRV 1280 100 3268 FR92SV0001.newlife.lan.
_ldap._tcp.Lyon._sites.ForestDnsZones.newlife.lan. 600 IN SRV 1280 100 389 FR92SV0001.newlife.lan.
_ldap._tcp.Lyon._sites.DomainDnsZones.newlife.lan. 600 IN SRV 1280 100 389 FR92SV0001.newlife.lan.
```

# TP : le service DNS

Avec le bloc Note, ouvrir le fichier C:\WINDOWS\system32\drivers\etc\hosts. A quoi sert ce fichier ?

Installer le service DNS (*Gestionnaire de Server | Ajout de rôles*).

Créer la zone formationXX.fr où XX est correspond à vos initiales. Autoriser les mises à jour dynamiques non sécurisées et sécurisées.

Créer un enregistrement www avec comme IP 192.168.140.2. Faire un ping de www.formationXX.fr puis un ipconfig /displaydns puis ipconfig /flushdns puis de nouveau ipconfig /displaydns. A quoi sert le cache DNS ?

Au niveau du serveur DNS, purger le cache DNS. Expliquer la différence avec la commande ipconfig /flushdns.

Définir un suffixe DNS sur une machine en groupe de travail (*Panneau de configuration | Propriétés Systèmes | Nom de l'ordinateur | Avancé*).

Faire un ipconfig /registerdns. Que fait cette commande ?

Aller dans les paramètres avancés TCP/IP, onglet DNS et désactiver la case « *Enregistrer les adresses de cette connexion dans le système DNS* ».

Créer une entrée dans le fichier HOST et faire un ipconfig /displaydns.

Se mettre par deux. Créer la zone « . » sur le serveur 1. Créer une nouvelle délégation pour la zone « fr » en indiquant l'IP du serveur 2.

Sur le serveur 2, créer la zone « fr » et le sous domaine *google*. Créer un entrée www dans « *google.fr* ». Faire un ping [www.google.fr](http://www.google.fr) depuis le serveur 1 et 2.

# Les notions fondamentales 1/2

**Forêt (symbole : rectangle)** : limite de réplication et de sécurité. Ensemble d'arborescences de domaine. Créer deux forêts pour séparer deux entités pour des raisons de sécurité (créer ensuite une relation d'approbation avec authentification sélective).

**Arborescence de domaine (symbole plusieurs triangles reliés ensemble)** : Ensemble de domaine avec une même racine de noms (noms contigus).

**Domaine (symbole : triangle)** : contient les objets (comptes utilisateur / ordinateur, groupes, unités d'organisation...).

**Unité d'organisation (OU, symbole : le rond)** : C'est un conteneur. Permet d'organiser l'annuaire, déléguer l'administration et créer des objets de stratégie de groupe.

**DCPROMO** : permet de convertir un serveur en groupe de travail / membre du domaine en un contrôleur de domaine et inversement (exécuter DCPROMO sur un contrôleur de domaine).

**Serveur de Catalogue global** : contient un réplique partielle de tous les objets de la forêt (que certains attributs). Permet de résoudre les membres des groupes universels et de faire de recherche dans l'annuaire.

**SYSVOL** : répertoire spécial contenant les scripts et les GPO qui répliquent sur tous les contrôleurs de domaine.

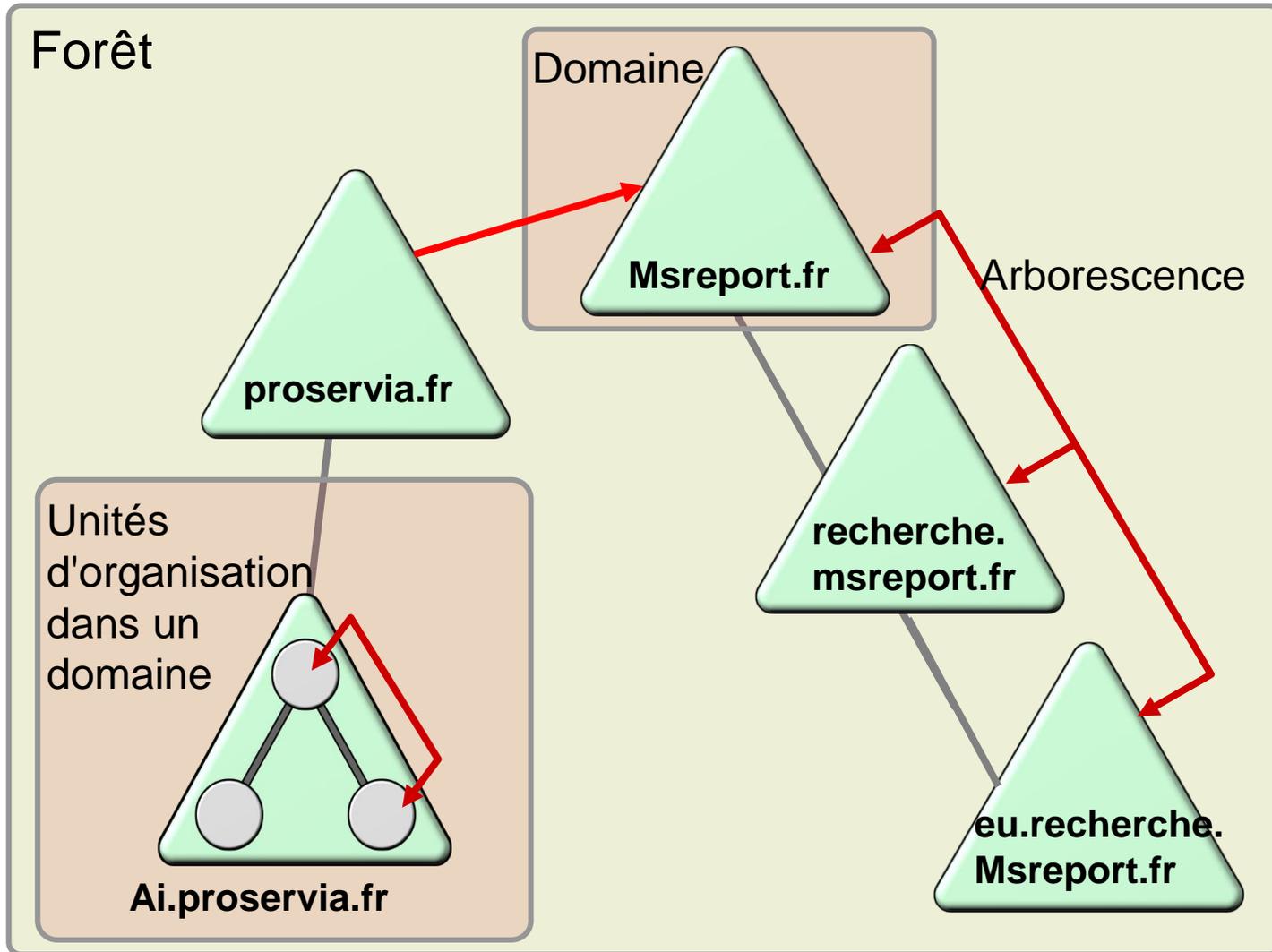
# Les notions fondamentales 2/2

**NTDS.DIT** : il s'agit de la base de données Active Directory (NTDS : New Technology Directory Service). Cette base est un dérivé des bases JET (moyennement fiable mais très rapide en lecture).

**Compte de restauration des services d'annuaires** : un contrôleur de domaine n'a plus de base SAM locale. Le compte de restauration des services d'annuaire permet de démarrer en mode restauration des services d'annuaire sur un résidu de base SAM. Cela peut être utile pour effectuer certaines opérations de maintenance pour Active Directory (restauration...).

**Exportation des paramètres** : permet de créer un fichier de réponse au format TXT pour faire une installation en mode « *Serveur CORE* » (Windows 2008 R2 sans interface graphique).

# La structure logique Active Directory 1/2



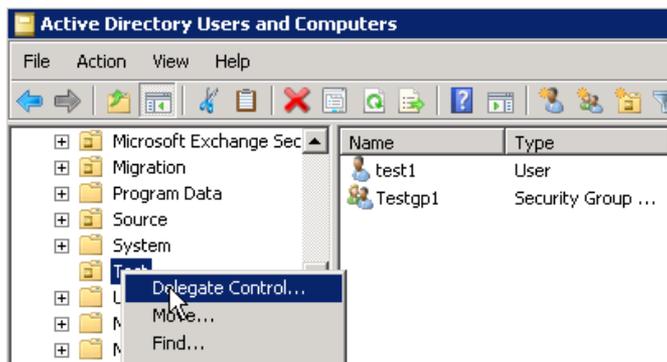
# La structure logique Active Directory 2/2

## Toujours faire un domaine dans une forêt sauf :

- Si les administrateurs ne doivent pas pouvoir gérer toutes les ressources.
- Si vous devez avoir un nom NETBIOS différent pour chaque entité. Il n'existe pas d'équivalent des suffixes UPN pour le nom NETBIOS. L'alternative est de faire en sorte que les utilisateurs ouvrent une session avec le nom DNS de domaine.
- En mode natif 2008, il est possible de créer plusieurs stratégies de mots de passe alors qu'en mode natif 2003 on ne peut créer qu'une stratégie de mot de passe par domaine.

## Best Practice :

- **Faire un domaine dans une forêt puis créer une OU par entités / services.**
- Ne pas dépasser 4 à 5 niveaux d'imbrication pour les OU si possible.
- Déléguer l'administration au niveau des unités d'organisation.
- Faire une OU pour les comptes ordinateurs et une autre pour les comptes utilisateurs. Mapper les GPO sur ces OU.



# Le choix des noms de domaine

## **Un domaine Active Directory dispose toujours de deux noms :**

Le nom NETBIOS : permet aux stations antérieurs à Windows 2000 de se connecter au domaine.

Le nom DNS : peut être utilisés par les stations de travail  $\geq$  Windows 2000.

Le nom NETBIOS et le nom DNS peuvent être complètement différents.

Le nom NETBIOS apparaît au niveau du champ « *Se connecter à* » sur les machines Windows NT4, 2000, XP et 2003.

En mode natif 2003, on peut renommer un domaine Active Directory (utilitaire RENDOM). Cela est très déconseillé, voir impossible (avec Exchange 2007).

## **Les Best Practice :**

Définir un nom de domaine DNS générique qui ne reprend pas le nom de la société (sauf si la probabilité que le nom de domaine change est très faible).

Utiliser les suffixes UPN pour ajouter des noms de domaine DNS.

Choisir un nom NetBIOS qui définit l'activité de la société.

**Attention, pas de nom de domaine DNS de type SINGLE LABEL DNS NAME.**

<http://msreport.free.fr/?p=149>

<http://www.msexchange.org/tutorials/Domain-Rename.html>

<http://support.microsoft.com/kb/925822/en-us>

# Les modes de domaine

Définit qui peut être contrôleur au niveau d'un domaine. Débloque des fonctionnalités (groupes globaux membres d'autres groupes globaux...). Pas de retour arrière possible.

Mode de domaine	Fonctionnalités	Type de DC
2000 mixte	Fonctionnalité de base	BDC NT4, DC 2000 / 2003
2000 natif	Groupe global membre d'un autre groupe global.	2000 / 2003 / <b>2008 / 2008 R2</b>
2003 natif	Nouveau algorithme de réplication / attribut LastlogonTimestamp / authentification sélective.	2003 / <b>2008 / 2008 R2</b>
2008 natif	DFS-R remplace NTFRS pour la réplication de SYSVOL. AES 128 / 256. Nouveaux attributs sur les logons.Fine Grained Password Policy.	<b>2008 / 2008 R2</b>
2008 R2 natif	Comptes de service gérés.	<b>2008 R2</b>

<http://msreport.free.fr/?p=128>

<https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/active-directory-functional-levels>

# Les modes de forêt

Définit qui peut être contrôleur dans la forêt Active Directory. Permet de débloquent des fonctionnalités (relation d'approbation inter-forêts...)

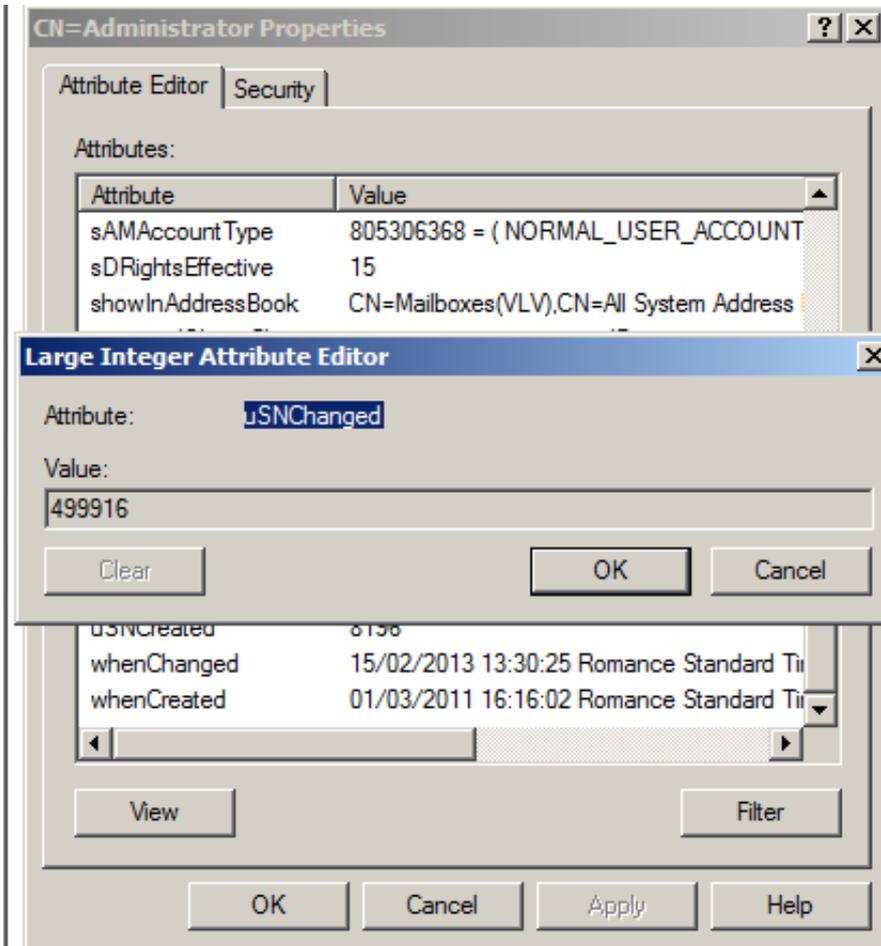
Pas de retour arrière possible sauf depuis le mode natif 2008 R2. Le retour en mode 2008 natif est possible si l'on a pas activé la corbeille Active Directory.

Mode de forêt	Fonctionnalités	Type de DC
2000 natif	Fonctionnalités de base.	BDC NT4 / 2000 / 2003 / <b>2008 / 2008 R2</b>
2003 natif	Approbation de forêt / Renommage de domaine (à éviter) / support des RODC / amélioration au niveau du KCC et de l'ISTG / désactivation d'attribut.	2003 / <b>2008 / 2008 R2</b>
2008 natif	Même fonctionnalités que le mode natif 2003.	<b>2008 / 2008 R2</b>
2008 R2 natif	Corbeille Active Directory	<b>2008 R2</b>

<http://msreport.free.fr/?p=128>

<https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/active-directory-functional-levels>

# La replication NTDS (1/2)



A chaque modification, l'attribut *USNChanged* est incrémenté. Les contrôleurs de domaine comparent ce numéro et déterminent ainsi quel contrôleur de domaine dispose de la version la plus récente.

<https://www.morgantechspace.com/2014/12/Active-Directory-whenChanged-vs-usnChanged.html>

# La replication NTDS (2/2)

Comment un objet est-il supprimé ?

L'attribut *USNChanged* est incrémenté et l'objet est déplacé dans le conteneur *Deleted Users* pendant la *TombstoneLifeTime*.

Durée de la *TombstoneLifeTime* : paramétrable, 60 jours par défaut pour un domaine créé avec Windows 2000, 180 pour un domaine créé avec Windows 2003 ou versions ultérieures.

[https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/dd379509\(v=ws.10\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/dd379509(v=ws.10))

Une fois la période passée, l'objet est réellement supprimé

## **Pourquoi ce fonctionnement :**

C'est pour pouvoir répliquer la suppression d'un objet

## **Lingering object :**

C'est quand un objet apparaît comme définitivement supprimé (après la période de *TombstoneLifeTime* et qu'il apparaît comme présent sur un autre dc

Le dc sur lequel il apparaît a comme *lingering object* (zombie). La réplication est bloquée automatiquement

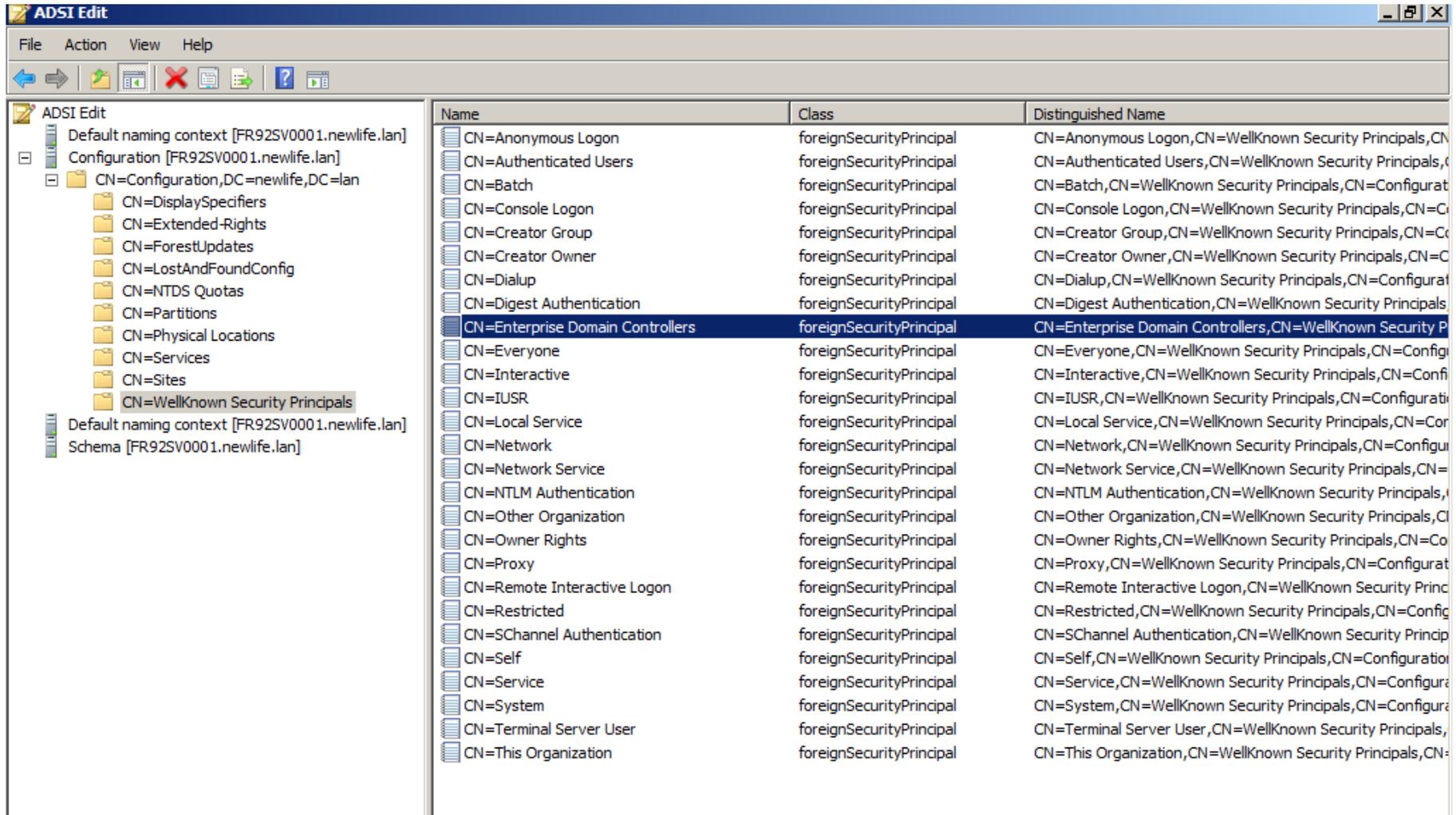
<https://support.microsoft.com/en-us/help/3141939/description-of-the-lingering-object-liquidator-tool>

<https://support.microsoft.com/en-gb/help/910205/information-about-lingering-objects-in-a-windows-server-active-directo>

# Well-known Security Principals

Ils sont au niveau de la partition de configuration Active Directory.

<https://docs.microsoft.com/en-us/windows/desktop/secauthz/well-known-sids>



The screenshot shows the ADSI Edit tool interface. The left pane displays the tree structure of the Active Directory configuration partition, with 'CN=WellKnown Security Principals' selected. The right pane shows a table of these principals.

Name	Class	Distinguished Name
CN=Anonymous Logon	foreignSecurityPrincipal	CN=Anonymous Logon,CN=WellKnown Security Principals,CN=...
CN=Authenticated Users	foreignSecurityPrincipal	CN=Authenticated Users,CN=WellKnown Security Principals,CN=...
CN=Batch	foreignSecurityPrincipal	CN=Batch,CN=WellKnown Security Principals,CN=Configurat
CN=Console Logon	foreignSecurityPrincipal	CN=Console Logon,CN=WellKnown Security Principals,CN=Ci
CN=Creator Group	foreignSecurityPrincipal	CN=Creator Group,CN=WellKnown Security Principals,CN=Cc
CN=Creator Owner	foreignSecurityPrincipal	CN=Creator Owner,CN=WellKnown Security Principals,CN=C
CN=Dialup	foreignSecurityPrincipal	CN=Dialup,CN=WellKnown Security Principals,CN=Configurat
CN=Digest Authentication	foreignSecurityPrincipal	CN=Digest Authentication,CN=WellKnown Security Principals
<b>CN=Enterprise Domain Controllers</b>	foreignSecurityPrincipal	<b>CN=Enterprise Domain Controllers,CN=WellKnown Security P</b>
CN=Everyone	foreignSecurityPrincipal	CN=Everyone,CN=WellKnown Security Principals,CN=Configi
CN=Interactive	foreignSecurityPrincipal	CN=Interactive,CN=WellKnown Security Principals,CN=Conf
CN=IUSR	foreignSecurityPrincipal	CN=IUSR,CN=WellKnown Security Principals,CN=Configurati
CN=Local Service	foreignSecurityPrincipal	CN=Local Service,CN=WellKnown Security Principals,CN=Cor
CN=Network	foreignSecurityPrincipal	CN=Network,CN=WellKnown Security Principals,CN=Configu
CN=Network Service	foreignSecurityPrincipal	CN=Network Service,CN=WellKnown Security Principals,CN=
CN=NTLM Authentication	foreignSecurityPrincipal	CN=NTLM Authentication,CN=WellKnown Security Principals,CN=
CN=Other Organization	foreignSecurityPrincipal	CN=Other Organization,CN=WellKnown Security Principals,CN=
CN=Owner Rights	foreignSecurityPrincipal	CN=Owner Rights,CN=WellKnown Security Principals,CN=Co
CN=Proxy	foreignSecurityPrincipal	CN=Proxy,CN=WellKnown Security Principals,CN=Configurat
CN=Remote Interactive Logon	foreignSecurityPrincipal	CN=Remote Interactive Logon,CN=WellKnown Security Princ
CN=Restricted	foreignSecurityPrincipal	CN=Restricted,CN=WellKnown Security Principals,CN=Config
CN=SChannel Authentication	foreignSecurityPrincipal	CN=SChannel Authentication,CN=WellKnown Security Princip
CN=Self	foreignSecurityPrincipal	CN=Self,CN=WellKnown Security Principals,CN=Configurati
CN=Service	foreignSecurityPrincipal	CN=Service,CN=WellKnown Security Principals,CN=Configur
CN=System	foreignSecurityPrincipal	CN=System,CN=WellKnown Security Principals,CN=Configur
CN=Terminal Server User	foreignSecurityPrincipal	CN=Terminal Server User,CN=WellKnown Security Principals,CN=
CN=This Organization	foreignSecurityPrincipal	CN=This Organization,CN=WellKnown Security Principals,CN=

# TP : Création d'un domaine 1/2

Renommer la machine suivant la convention de nommage indiquée par le formateur (DCTESTLABX).

Configurer le serveur en adressage IP fixe (valider la configuration DNS).

Installer le rôle serveur DNS.

Installer le rôle Active Directory Domain Services.

Jusqu'à Windows Server 2008 R2, exécuter l'assistant DCPROMO (Domain Controller Promotion).

A partir de Windows Server 2012, utiliser le Server Manager (ajout du rôle Active Directory Domain Services).



Assistant Installation des services de domaine Active Directory

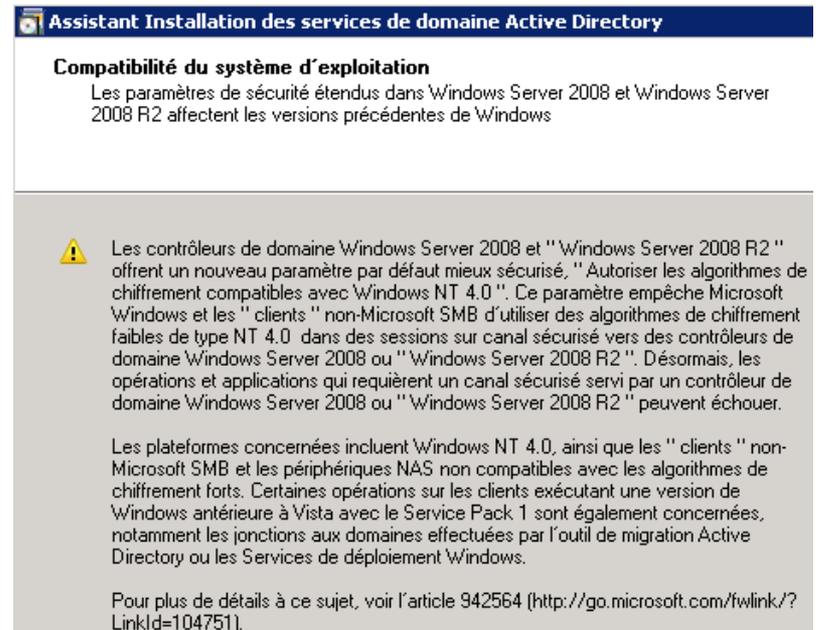
**Assistant Installation des services de domaine Active Directory**

Cet Assistant vous aide à installer les services de domaine Active Directory (AD DS) sur ce serveur, faisant du serveur un contrôleur de domaine Active Directory. Pour continuer, cliquez sur Suivant.

Utiliser l'installation en mode avancé

En savoir plus sur les options supplémentaires disponibles dans l'[installation en mode avancée](#).

En savoir plus sur les [services de domaine Active Directory](#)



Assistant Installation des services de domaine Active Directory

**Compatibilité du système d'exploitation**

Les paramètres de sécurité étendus dans Windows Server 2008 et Windows Server 2008 R2 affectent les versions précédentes de Windows

 Les contrôleurs de domaine Windows Server 2008 et "Windows Server 2008 R2" offrent un nouveau paramètre par défaut mieux sécurisé, "Autoriser les algorithmes de chiffrement compatibles avec Windows NT 4.0". Ce paramètre empêche Microsoft Windows et les "clients" non-Microsoft SMB d'utiliser des algorithmes de chiffrement faibles de type NT 4.0 dans des sessions sur canal sécurisé vers des contrôleurs de domaine Windows Server 2008 ou "Windows Server 2008 R2". Désormais, les opérations et applications qui requièrent un canal sécurisé servi par un contrôleur de domaine Windows Server 2008 ou "Windows Server 2008 R2" peuvent échouer.

Les plateformes concernées incluent Windows NT 4.0, ainsi que les "clients" non-Microsoft SMB et les périphériques NAS non compatibles avec les algorithmes de chiffrement forts. Certaines opérations sur les clients exécutant une version de Windows antérieure à Vista avec le Service Pack 1 sont également concernées, notamment les jonctions aux domaines effectuées par l'outil de migration Active Directory ou les Services de déploiement Windows.

Pour plus de détails à ce sujet, voir l'article 942564 (<http://go.microsoft.com/fwlink/?LinkId=104751>).

# TP : Création d'un domaine 2/2

**Assistant Installation des services de domaine Active Directory**

**Choisissez une configuration de déploiement**  
Vous pouvez créer un contrôleur de domaine pour une forêt nouvelle ou existante.

Forêt existante

- Ajouter un contrôleur de domaine à un domaine existant.
- Créer un nouveau domaine dans une forêt existante.  
Ce serveur va devenir le premier contrôleur de domaine du nouveau domaine.
- Créer une nouvelle racine d'arborescence de domaine au lieu d'un nouveau domaine existant.

Créer un domaine dans une nouvelle forêt

**Assistant Installation des services de domaine Active Directory**

**Nommez le domaine racine de la forêt**  
Le premier domaine de la forêt est le domaine racine de la forêt. Il porte le nom de la forêt.

Entrez le nom de domaine complet du nouveau domaine racine de forêt.

Nom de domaine complet du domaine racine de forêt :

  
Exemple : corp.contoso.com

**Assistant Installation des services de domaine Active Directory**

**Nom de domaine NetBIOS**  
Il s'agit du nom que les utilisateurs des versions antérieures de Windows utiliseront pour identifier le nouveau domaine.

L'Assistant génère un nom NetBIOS par défaut. Cette page de l'Assistant ne s'affiche que si vous avez sélectionné le mode avancé ou si l'Assistant a détecté un conflit dans le nom par défaut.

Acceptez le nom généré par l'Assistant ou tapez un nouveau nom, puis cliquez sur Suivant.

Nom de domaine NetBIOS :

**Assistant Installation des services de domaine Active Directory**

**Définir le niveau fonctionnel de la forêt**  
Sélectionnez le niveau fonctionnel de la forêt.

Niveau fonctionnel de la forêt :

- Windows 2000
- Windows 2000**
- Windows Server 2003
- Windows Server 2008
- Windows Server 2008 R2

**Assistant Installation des services de domaine Active Directory**

**Définir le niveau fonctionnel du domaine**  
Sélectionnez le niveau fonctionnel du domaine.

Niveau fonctionnel du domaine :

- Windows 2000 natif
- Windows 2000 natif**
- Windows Server 2003
- Windows Server 2008
- Windows Server 2008 R2

**Assistant Installation des services de domaine Active Directory**

**Options supplémentaires pour le contrôleur de domaine**

Sélectionnez des options supplémentaires pour ce contrôleur de domaine.

- Serveur DNS
- Catalogue global
- Contrôleur de domaine en lecture seule (RODC)

Informations supplémentaires :

Le premier contrôleur de domaine d'une forêt doit être un serveur de catalogue global et ne peut pas être un contrôleur de domaine en lecture seule (RODC).

Nous vous recommandons d'installer le service Serveur DNS sur le premier contrôleur de domaine.

**Assistant Installation des services de domaine Active Directory**

 Il est impossible de créer une délégation pour ce serveur DNS car la zone parente faisant autorité est introuvable ou elle n'exécute pas le serveur DNS Windows. Si vous procédez à l'intégration avec une infrastructure DNS existante, vous devez manuellement créer une délégation avec ce serveur DNS dans la zone parente pour activer une résolution de noms fiable en dehors du domaine « formation10.lan ». Sinon, aucune action n'est requise.

Voulez-vous continuer ?

**Assistant Installation des services de domaine Active Directory**

**Emplacement de la base de données, des fichiers journaux et de SYSVOL**  
Spécifiez les dossiers qui contiendront la base de données du contrôleur de domaine Active Directory, les fichiers journaux et SYSVOL.

Pour de meilleures performances et une meilleure récupération, stockez la base de données et les fichiers journaux sur des volumes séparés.

Dossier de la base de données :

Dossier des fichiers journaux :

Dossier SYSVOL :

**Assistant Installation des services de domaine Active Directory**

**Mot de passe administrateur de restauration des services d'annuaire**

Le compte d'administration de restauration des services d'annuaire est différent du compte d'administrateur de domaine.

Attribuez un mot de passe au compte d'administrateur qui sera utilisé lors du démarrage de ce contrôleur de domaine en mode Restauration des services d'annuaire. Nous vous recommandons de choisir un mot de passe fort.

Mot de passe :

Confirmer le mot de passe :

En savoir plus sur le [mot de passe de restauration des services d'annuaire](#)

**Assistant Installation des services de domaine Active Directory**

**Résumé**

Vérifiez vos sélections :

- Configurer ce serveur en tant que premier contrôleur de domaine Active Directory d'une nouvelle forêt.
- Le nouveau nom de domaine est « formation10.lan ». C'est aussi le nom de la nouvelle forêt.
- Le nom NetBIOS du domaine est « MSREPORTFORM ».
- Niveau fonctionnel de la forêt : Windows 2000
- Niveau fonctionnel du domaine : Windows 2000 natif
- Site : Default-First-Site-Name

Pour modifier une option, cliquez sur Précédent. Pour commencer l'opération, cliquez sur Suivant.

Vous pouvez exporter ces paramètres dans un fichier de réponses pour les utiliser avec d'autres opérations d'installation sans assistance.

En savoir plus sur l'utilisation d'un fichier de réponse

# TP : Ajout d'un second DC 1/3

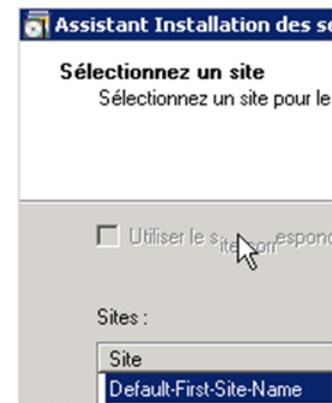
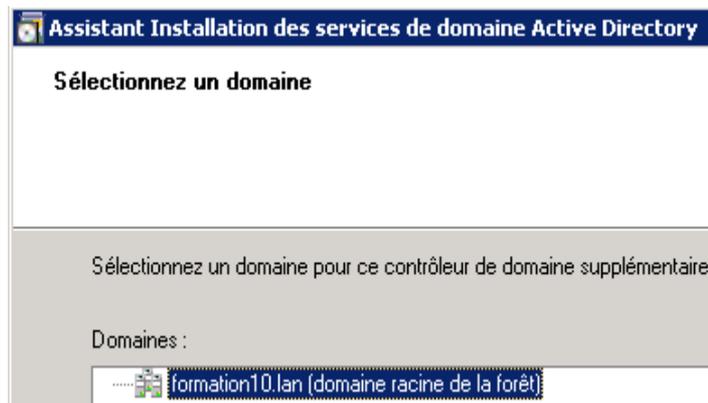
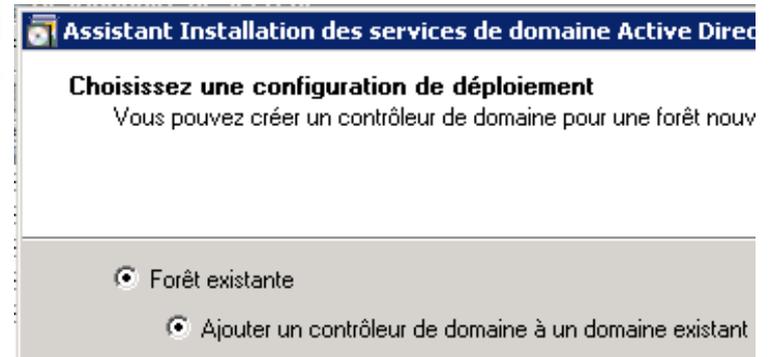
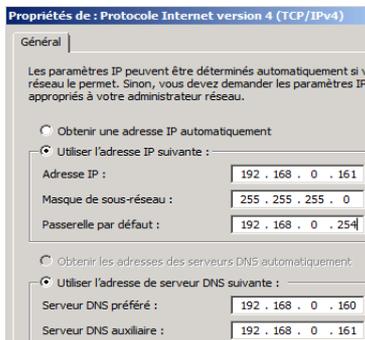
Définir comme serveur DNS principal, l'IP du premier contrôleur de domaine.  
Expliquer pourquoi ?

Faire un ping DCTESTLABX.formationX.lan puis ipconfig /displaydns

Faire ensuite un ipconfig /flushdns puis ipconfig /displaydns. Expliquer.

Lancer l'assistant DCPRIMO. Une fois l'écran de bienvenue se lance, aller le gestionnaire de rôle dans la section Rôles de Server. Que constatez vous ?

Suivre les indications sur les captures d'écran.



# TP : Ajout d'un second DC 2/3

En mode avancé, il est possible de spécifier depuis quel contrôleur de domaine on réplique. Pour les sites avec une très faible bande passante, il est même possible de répliquer depuis une sauvegarde. Pour plus d'informations :

[http://www.laboratoire-microsoft.org/articles/win/dcpromo\\_adv/](http://www.laboratoire-microsoft.org/articles/win/dcpromo_adv/)

Les cases « *Serveurs DNS* » et « *Catalogue Global* » doivent être cochées.

Sans catalogue global, seul l'administrateur du domaine peut ouvrir une session.

Sans serveur DNS, les stations de travail ne peuvent pas localiser les contrôleurs de domaine.

# TP : Ajout d'un second DC 3/3

Vérifier le fonctionnement de la réplication avec Sites et Services Active Directory

Si la réplication n'est pas fonctionnelle :

Définir sur tous les DC le même serveur DNS principal.

Vérifier sur ce dernier qu'il existe une zone DNS correspondant au nom de domaine DNS.

Vérifier si cette zone autorise les mises à jour dynamiques.

Taper les commandes suivantes :

```
Ipconfig /flushdns
```

```
Ipconfig /registerdns
```

```
Net stop netlogon
```

```
Net start netlogon
```

```
Repadmin /kcc
```

# Les chemins LDAP :

Nom unique relatif LDAP : OU=Production

Nom unique LDAP :

*CN=sophie mathieu2,Ou=enfant,OU=Migration,DC=ORGA2,DC=LAN*

Nom canonique : orga2.lan/Production

Commutateur	Signification
OU=	Unités d'organisation
CN=	Objets
DC=	Domaine
O=	Organisation (Exchange).

## Mise en pratique :

Créer deux comptes utilisateurs appelés Sophie Mathieu2 et guillaume.mathieu. Aller dans l'éditeur d'attribut de la console Utilisateurs et Ordinateurs Active Directory. Prendre la valeur du champ *DistinguishedName*.

# Les rôles FSMO et le Catalogue Global 1/2

5 rôles FSMO (*Flexible Single Master Operation*) et le Catalogue Global :

- Emulateur PDC : serveur de temps du domaine. Gère les changements de mots de passe. En mode 2000 mixte, permet aux BDC NT4 de se synchroniser avec le DC jouant le rôle d'Emulateur PDC. Gère la création des relations d'approbation. Gère la topologie DFS.
- Maître RID : permet d'allouer des pool de 500 SID. Si ce rôle n'est plus en ligne, les contrôleurs de domaine ne peuvent plus obtenir de nouveau pool de SID. Si leur pool est épuisé, ils ne peuvent plus créer de nouveaux objets.
- Maître d'infrastructure : permet de gérer les objets fantômes (un objet fantôme est créé lorsque l'on joint un objet du domaine B dans un groupe du domaine A).
- Maître d'attribution de noms de domaine : valide s'il n'y a pas de conflit(s) de noms DNS au niveau des domaines de la forêt et des domaines approuvés.
- Maître de schéma : permet de gérer les modifications effectuées au niveau du schéma Active Directory.

# Les rôles FSMO et le Catalogue Global 2/2

Le serveur de Catalogue Global : contient une réplique des principaux attributs de tous les objets de la forêt. Permet de faire des recherches dans l'annuaire. Gère les groupes universels. Si plus de serveur de Catalogue global, on ne peut plus ouvrir de sessions (sauf les administrateurs du domaine).

Mettre tous les DC en tant que serveur de « *Catalogue global* » **ou** ne pas mettre le contrôleur de domaine qui joue le rôle de Maître d'Infrastructure en tant que serveur de Catalogue Global.

<http://support.microsoft.com/kb/324801/en-us>

<http://support.microsoft.com/kb/223346/en-us>

<http://support.microsoft.com/kb/839879/en-us>

<http://support.microsoft.com/kb/910202/en-us>

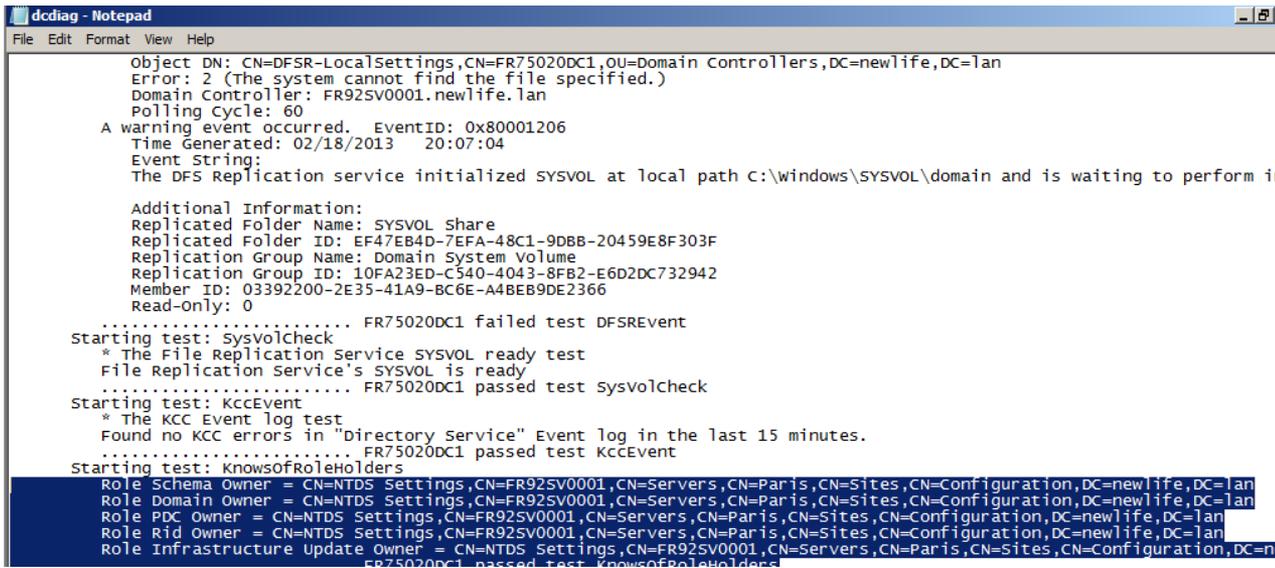
<http://support.microsoft.com/kb/839879/en-us>

# TP : déterminer qui a les rôles FSMO

Pour déterminer qui a les 5 rôles FSMO en ligne de commande :

*netdom query fsmo*

Utiliser la commande *Dcdiag*.



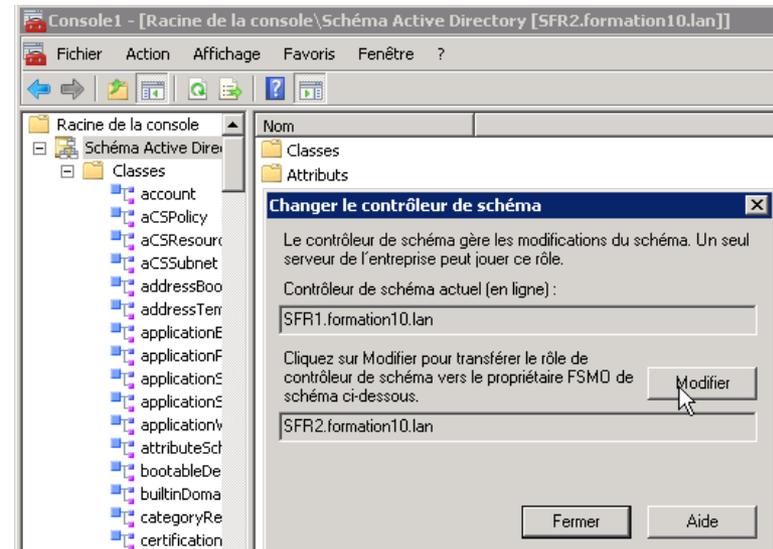
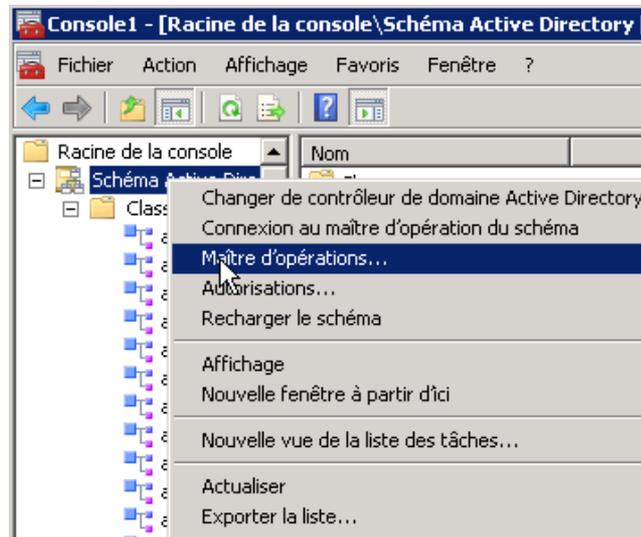
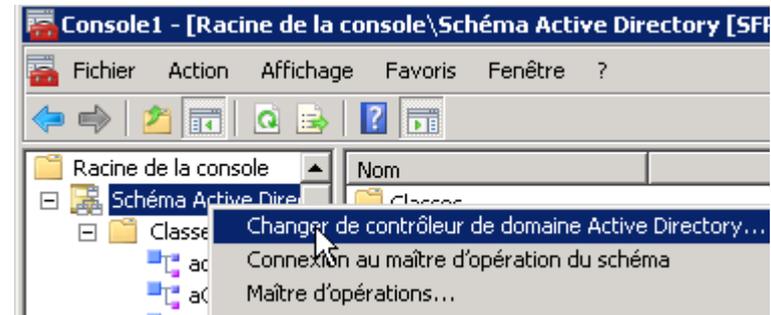
```
dcdiag - Notepad
File Edit Format View Help
Object DN: CN=DFSR-LocalSettings,CN=FR75020DC1,OU=Domain Controllers,DC=newlife,DC=lan
Error: 2 (The system cannot find the file specified.)
Domain Controller: FR92SV0001.newlife.lan
Polling Cycle: 60
A warning event occurred. EventID: 0x80001206
Time Generated: 02/18/2013 20:07:04
Event String:
The DFS Replication service initialized SYSVOL at local path C:\windows\sysvol\domain and is waiting to perform i

Additional Information:
Replicated Folder Name: SYSVOL Share
Replicated Folder ID: EF47EB4D-7EFA-48C1-9DBB-20459E8F303F
Replication Group Name: Domain System Volume
Replication Group ID: 10FA23ED-C540-4043-8FB2-E6D2DC732942
Member ID: 03392200-2E35-41A9-BC6E-A4BEB9DE2366
Read-Only: 0
..... FR75020DC1 failed test DFSREvent
Starting test: SysvolCheck
* The File Replication Service SYSVOL ready test
File Replication Service's SYSVOL is ready
..... FR75020DC1 passed test sysvolcheck
Starting test: KccEvent
* The KCC Event log test
Found no KCC errors in "Directory Service" Event log in the last 15 minutes.
..... FR75020DC1 passed test KccEvent
Starting test: KnowsofRoleholders
Role Schema Owner = CN=NTDS Settings,CN=FR92SV0001,CN=Servers,CN=Paris,CN=Sites,CN=Configuration,DC=newlife,DC=lan
Role Domain Owner = CN=NTDS Settings,CN=FR92SV0001,CN=Servers,CN=Paris,CN=Sites,CN=Configuration,DC=newlife,DC=lan
Role PDC Owner = CN=NTDS Settings,CN=FR92SV0001,CN=Servers,CN=Paris,CN=Sites,CN=Configuration,DC=newlife,DC=lan
Role Rid Owner = CN=NTDS Settings,CN=FR92SV0001,CN=Servers,CN=Paris,CN=Sites,CN=Configuration,DC=newlife,DC=lan
Role Infrastructure Update Owner = CN=NTDS Settings,CN=FR92SV0001,CN=Servers,CN=Paris,CN=Sites,CN=Configuration,DC=newlife,DC=lan
..... FR75020DC1 passed test KnowsofRoleholders
```

# TP : transfert du *Schema Master* via console

Taper la commande “*regsvr32 schmmgmt.dll*” pour afficher la composant logiciel enfichable “Maître de schéma”,  
Aller dans me menu *Démarrer*, cliquer « *Exécuter* » puis taper MMC. Cela permet de lancer une console MMC vierge. « *Cliquer sur Ajouter un composant logiciel enfichable* ».  
Sélectionner le composant « *Maître de Schéma* ».

Astuce : il faut se connecter sur le DC cible sur lequel on veut transférer le rôle car par défaut la console Maître de Schéma se connecte sur le contrôleur de domaine qui joue le rôle de Maître de Schéma.

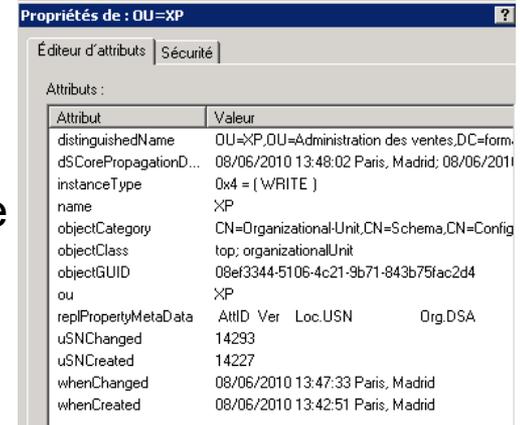


# Les partitions d'annuaires 1/4 :

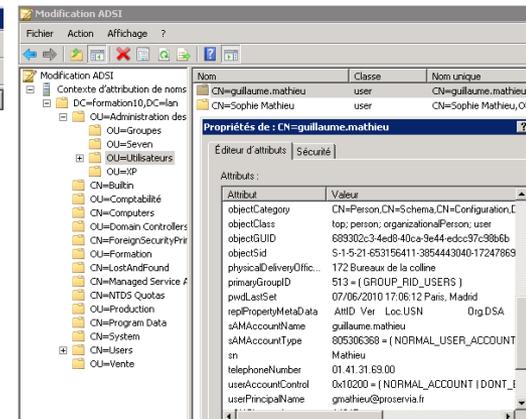
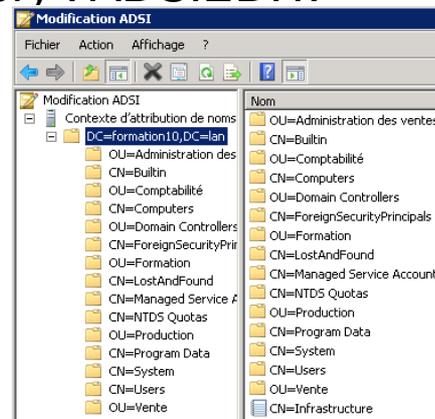
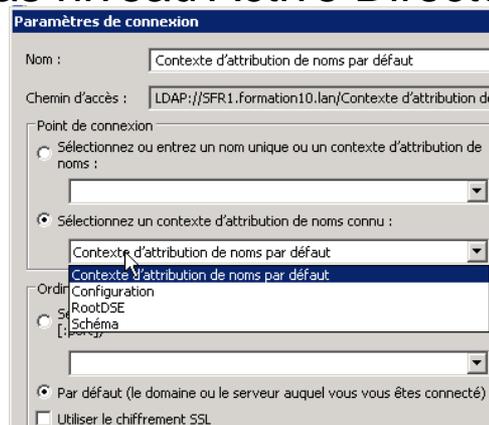
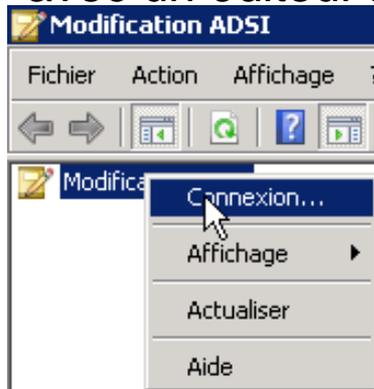
## Active Directory est découpé en partitions :

- Schéma : contient l'ensemble des attributs et des classes (extensible).
- Configuration : contient la configuration de l'annuaire Active Directory (les sites, les partitions d'annuaires...).
- Domaine (1 par domaine) : contient les données utiles (les comptes utilisateur / ordinateur, les groupes...).
- ForestDnsZones : contient les entrées des zones DNS publiées sur tous les serveurs DNS de la forêt.
- DomainDnsZones (1 par domaine) : contient les entrées des zones DNS publiées sur tous les serveurs DNS du domaine.

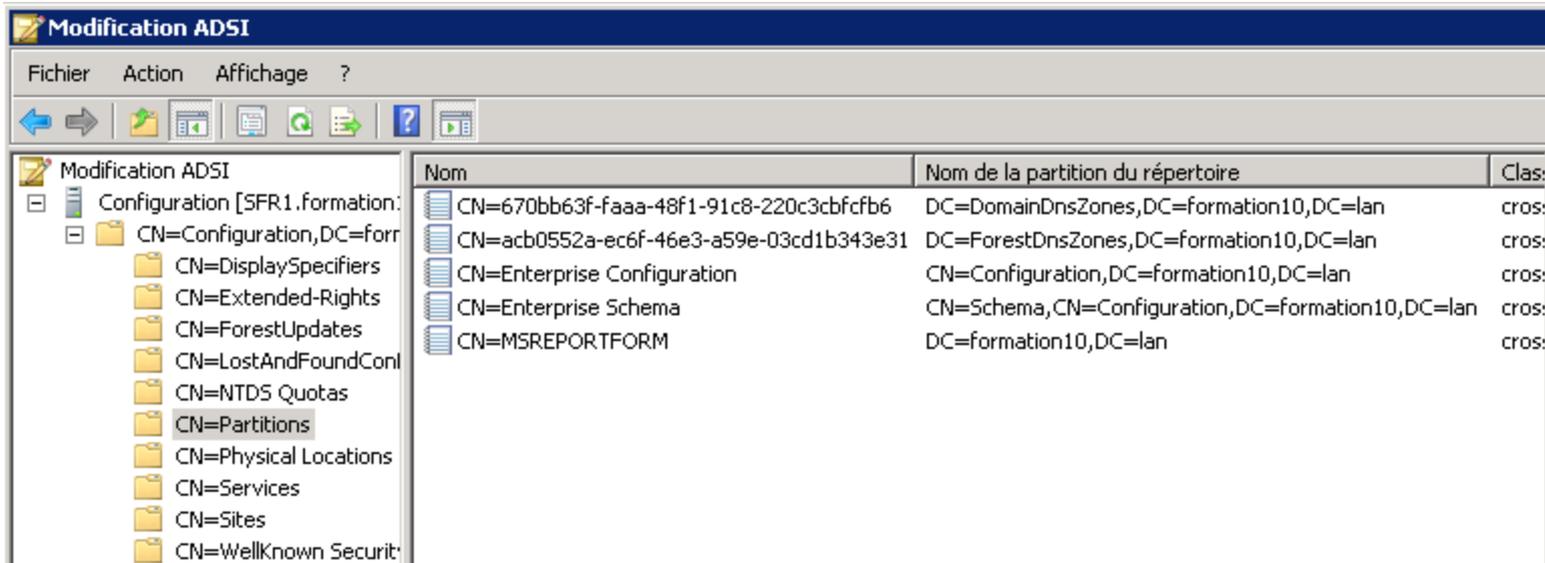
Pour se connecter à certaines partitions, il faut se connecter avec un éditeur bas niveau Active Directory : ADSIEDIT.



Attribut	Valeur
distinguishedName	OU=XP,OU=Administration des ventes,DC=form...
dSCorePropagationD...	08/06/2010 13:48:02 Paris, Madrid; 08/06/2011
instanceType	0x4 = (WRITE )
name	XP
objectCategory	CN=OrganizationalUnit,CN=Schema,CN=Config
objectClass	top; organizationalUnit
objectGUID	08ef3344-5106-4c21-9b71-843b75fac2d4
ou	XP
repPropertyMetaData	AttrID Ver Loc.USN Org.DSA
uSNChanged	14293
uSNCreated	14227
whenChanged	08/06/2010 13:47:33 Paris, Madrid
whenCreated	08/06/2010 13:42:51 Paris, Madrid



# Les partitions d'annuaires 2/4 :



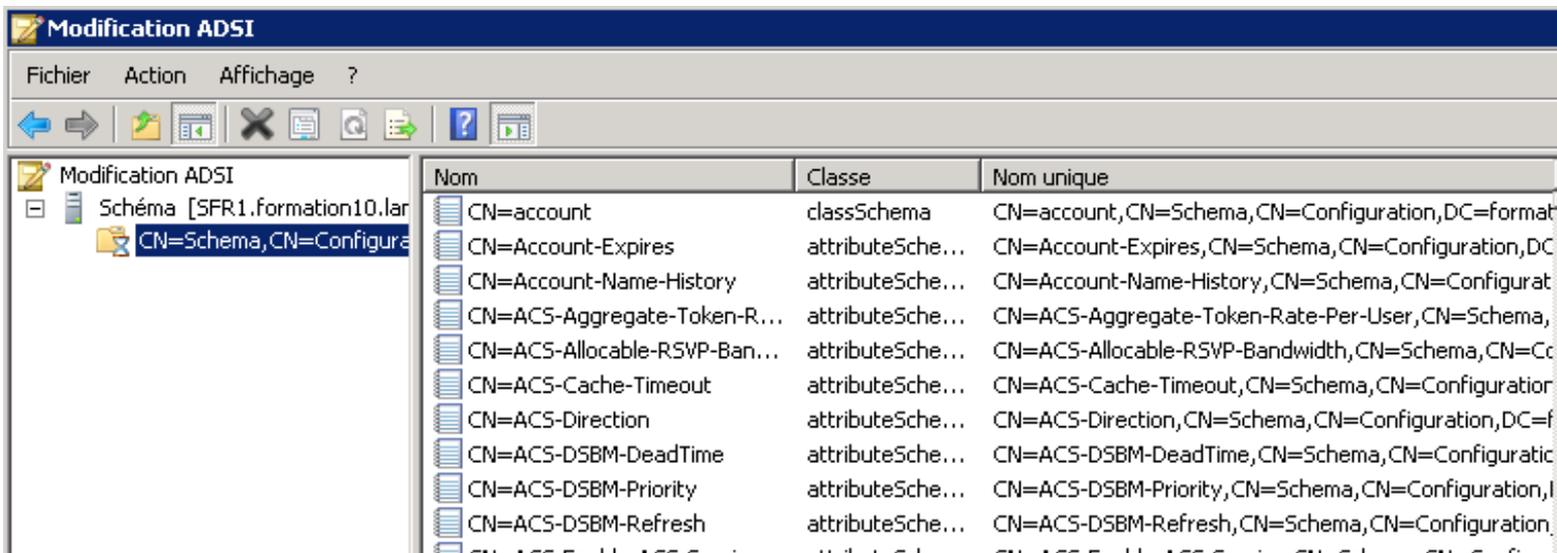
**Modification ADSI**

Fichier Action Affichage ?

Modification ADSI

- Configuration [SFR1.formation10.lan]
- CN=Configuration,DC=formation10,DC=lan
  - CN=DisplaySpecifiers
  - CN=Extended-Rights
  - CN=ForestUpdates
  - CN=LostAndFoundConf
  - CN=NTDS Quotas
  - CN=Partitions**
  - CN=Physical Locations
  - CN=Services
  - CN=Sites
  - CN=WellKnown Security

Nom	Nom de la partition du répertoire	Clas:
CN=670bb63f-faaa-48f1-91c8-220c3cbfcfb6	DC=DomainDnsZones,DC=formation10,DC=lan	cross
CN=acb0552a-ec6f-46e3-a59e-03cd1b343e31	DC=ForestDnsZones,DC=formation10,DC=lan	cross
CN=Enterprise Configuration	CN=Configuration,DC=formation10,DC=lan	cross
CN=Enterprise Schema	CN=Schema,CN=Configuration,DC=formation10,DC=lan	cross
CN=MSREPORTFORM	DC=formation10,DC=lan	cross



**Modification ADSI**

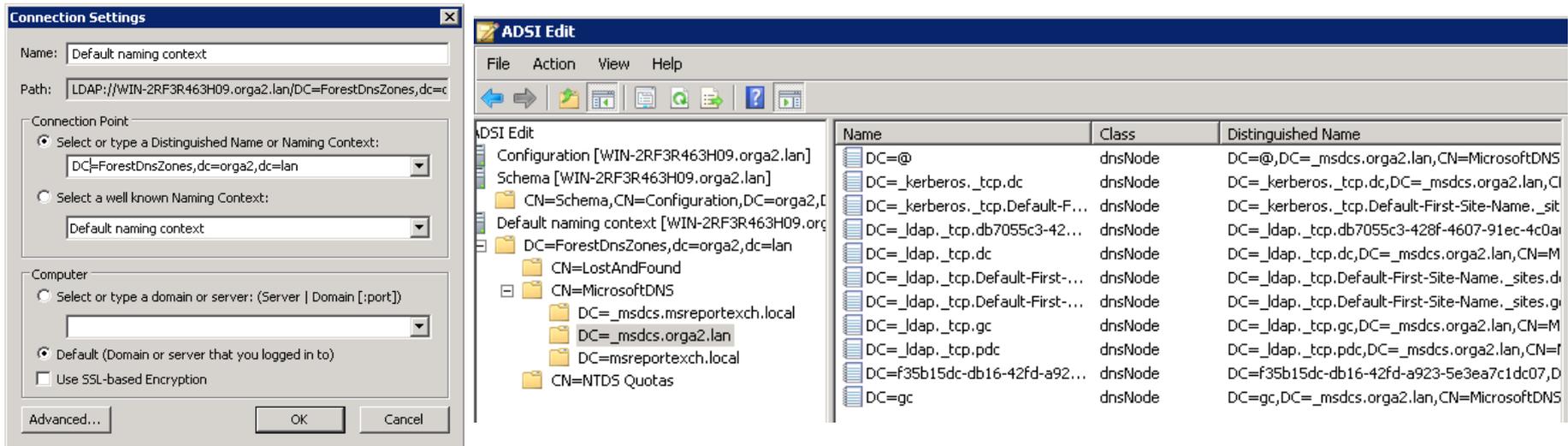
Fichier Action Affichage ?

Modification ADSI

- Schéma [SFR1.formation10.lan]
- CN=Schema,CN=Configuration,DC=formation10,DC=lan

Nom	Classe	Nom unique
CN=account	classSchema	CN=account,CN=Schema,CN=Configuration,DC=formation10,DC=lan
CN=Account-Expires	attributeSchema	CN=Account-Expires,CN=Schema,CN=Configuration,DC=formation10,DC=lan
CN=Account-Name-History	attributeSchema	CN=Account-Name-History,CN=Schema,CN=Configuration,DC=formation10,DC=lan
CN=ACS-Aggregate-Token-R...	attributeSchema	CN=ACS-Aggregate-Token-Rate-Per-User,CN=Schema,CN=Configuration,DC=formation10,DC=lan
CN=ACS-Allocable-RSVP-Ban...	attributeSchema	CN=ACS-Allocable-RSVP-Bandwidth,CN=Schema,CN=Configuration,DC=formation10,DC=lan
CN=ACS-Cache-Timeout	attributeSchema	CN=ACS-Cache-Timeout,CN=Schema,CN=Configuration,DC=formation10,DC=lan
CN=ACS-Direction	attributeSchema	CN=ACS-Direction,CN=Schema,CN=Configuration,DC=formation10,DC=lan
CN=ACS-DSBM-DeadTime	attributeSchema	CN=ACS-DSBM-DeadTime,CN=Schema,CN=Configuration,DC=formation10,DC=lan
CN=ACS-DSBM-Priority	attributeSchema	CN=ACS-DSBM-Priority,CN=Schema,CN=Configuration,DC=formation10,DC=lan
CN=ACS-DSBM-Refresh	attributeSchema	CN=ACS-DSBM-Refresh,CN=Schema,CN=Configuration,DC=formation10,DC=lan
CN=ACS-Enable-ACS-Service	attributeSchema	CN=ACS-Enable-ACS-Service,CN=Schema,CN=Configuration,DC=formation10,DC=lan

# Les partitions d'annuaires 3/4 :



## Mise en pratique :

Lancer la console « *Utilisateurs et Ordinateurs Active Directory* ».

Créer l'OU Test à la racine du domaine.

Créer le compte utilisateur test1 (mot de passe : P@ssword) dans l'OU Test.

Créer le groupe global testgp1 dans l'OU Test.

Ajouter l'utilisateur test1 au groupe global testgp1.

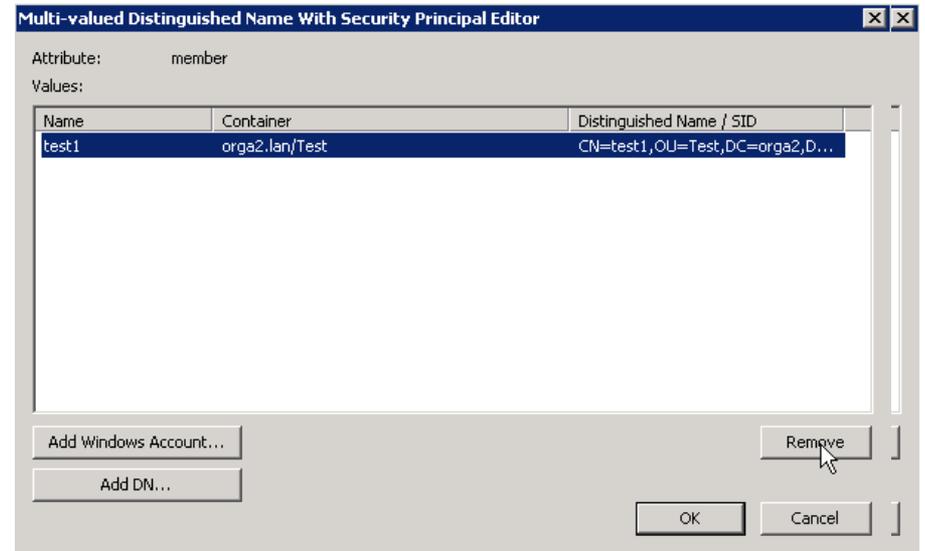
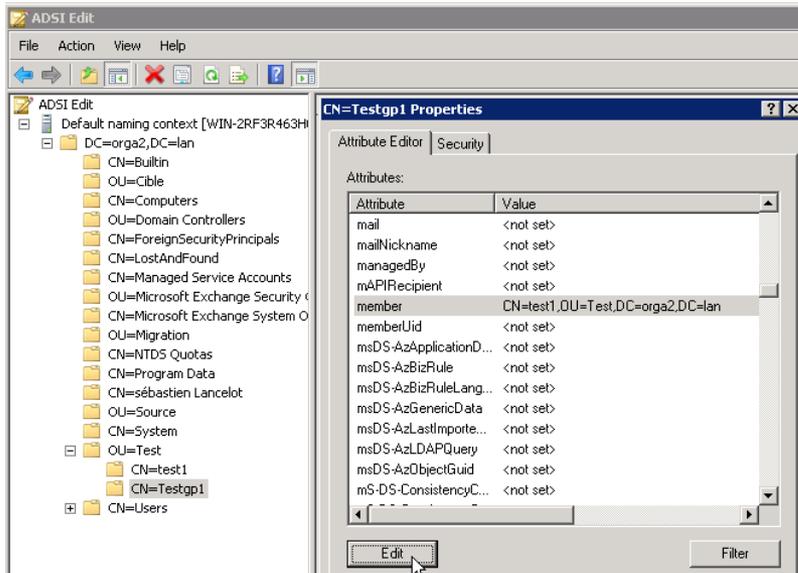
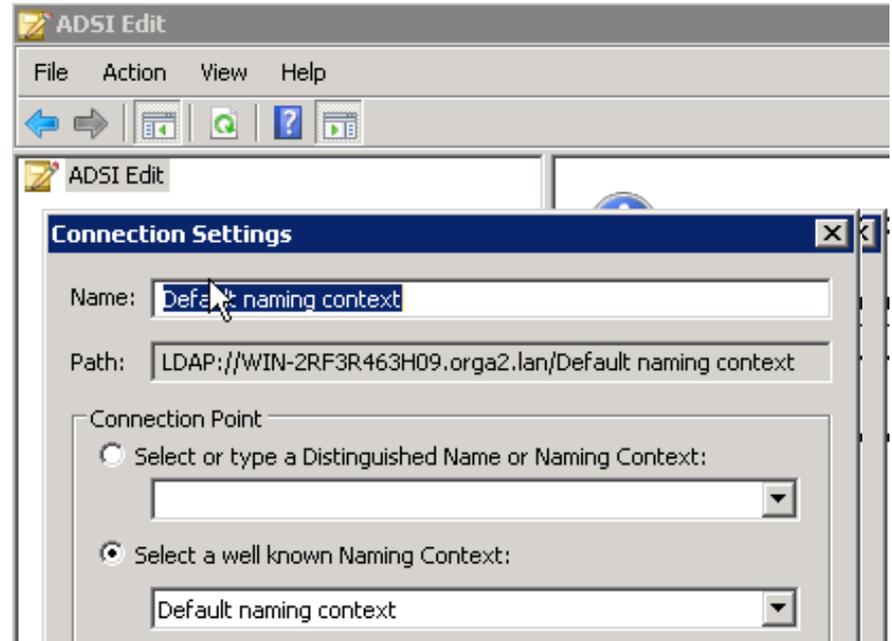
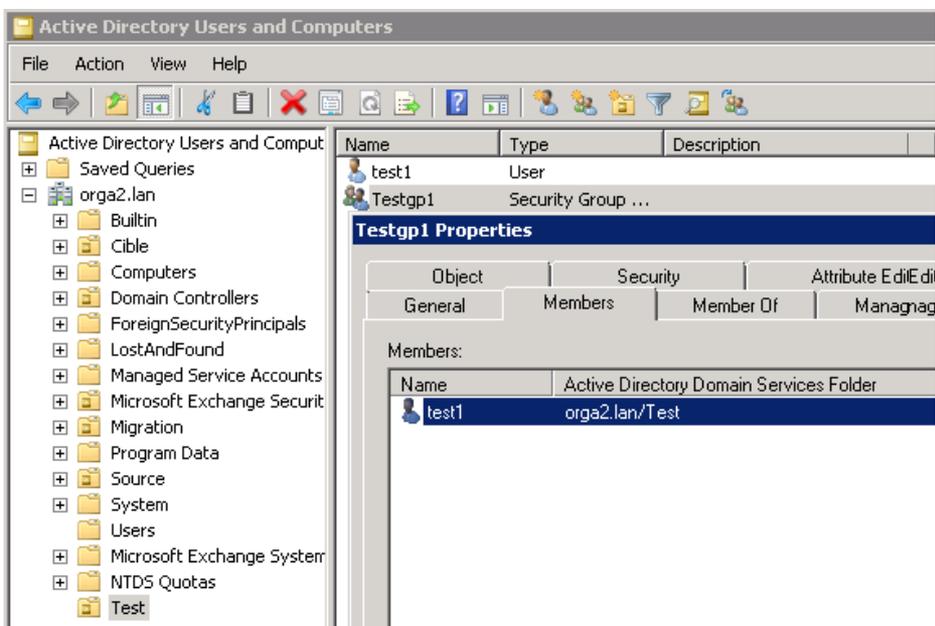
Lancer *ADSIEDIT*. Se connecter à la partition de domaine.

Localiser la ressource testgp1 et éditer l'objet utilisateur (bouton droit, *Propriétés*).

Aller au niveau de l'attribut « *member* » et supprimer l'entrée test1.

Relancer la console « *Utilisateurs et Ordinateurs Active Directory* » et valider que l'utilisateur test1 n'est plus membre du groupe testgp1.

# Les partitions d'annuaires 4/4 :



# TP : déplacement de zone DNS

Créer une zone DNS appelée *google2.fr*.

Intégrer la zone dans l'annuaire. Cocher la case « *Enregistrer la zone dans Active Directory ...* ». Sélectionner ensuite « *Vers tous les contrôleurs de domaine dans ce domaine ...* »

Créer un enregistrement de type A appelé *www* avec l'IP *192.168.0.1*.

Cela va créer une entrée dans *System\Microsoft DNS*.

Publier maintenant cette zone dans la *ForestDnsZones* puis dans la *DomainDnsZones*. Pour cela, aller dans les propriétés de la zone, onglet « Général ». Au niveau de Réplication, cliquer sur Propriétés. Sélectionner choix 1 puis choix 2.

**Assistant Nouvelle zone**

**Nom de la zone**  
Quel est le nom de la nouvelle zone ?

Le nom de la zone spécifie la partie de l'espace de noms DNS pour laquelle ce serveur fait autorité. Il peut s'agir du nom de domaine de votre société (par exemple, microsoft.com) ou d'une partie du nom de domaine (par exemple, nouvelle\_zone.microsoft.com). Le nom de zone n'est pas le nom du serveur DNS.

Nom de la zone :

**Assistant Nouvelle zone**

**Type de zone**  
Le serveur DNS prend en charge différents types de zones et de stockages.

Sélectionnez le type de zone que vous voulez créer :

- Zone principale  
Crée une copie d'une zone qui peut être mise à jour directement sur ce serveur.
- Zone secondaire  
Crée une copie de la zone qui existe sur un autre serveur. Cette option aide à équilibrer la charge de travail des serveurs principaux et autorise la gestion de la tolérance de pannes.
- Zone de stub  
Crée une copie d'une zone contenant uniquement des enregistrements Nom de serveur (NS), Source de nom (SOA), et éventuellement des enregistrements « glue Host (A) ». Un serveur contenant une zone de stub ne fait pas autorité pour cette zone.
- Enregistrer la zone dans Active Directory (disponible uniquement si le serveur DNS est un contrôleur de domaine accessible en écriture)

**Assistant Nouvelle zone**

**Mise à niveau dynamique**  
Vous pouvez spécifier que cette zone accepte les mises à jour sécurisées, non sécurisées ou non dynamiques.

Les mises à jour dynamiques permettent au client DNS d'enregistrer et de mettre à jour de manière dynamique leurs enregistrements de ressources avec un serveur DNS dès qu'une modification a lieu.  
Sélectionnez le type de mises à jour dynamiques que vous souhaitez autoriser :

- N'autoriser que les mises à jour dynamiques sécurisées (recommandé pour Active Directory)  
Cette option n'est disponible que pour les zones intégrées à Active Directory.
- Autoriser à la fois les mises à jours dynamiques sécurisées et non sécurisées  
Les mises à jour dynamiques d'enregistrement de ressources sont acceptées à partir de n'importe quel client.  
 Cette option peut mettre en danger la sécurité de vos données car les mises à jour risquent d'être acceptées à partir d'une source non approuvée.
- Ne pas autoriser les mises à jour dynamiques  
Les mises à jour dynamiques des enregistrements de ressources ne sont pas acceptées par cette zone. Vous devez mettre à jour ces enregistrements manuellement.

**Assistant Nouvelle zone**

**Étendue de la zone de réplication de Active Directory**  
Vous pouvez sélectionner la façon dont les données DNS doivent être répliquées sur votre réseau.

Choisissez la façon dont les données de la zone doivent être répliquées :

- Vers tous les serveurs DNS exécutés sur des contrôleurs de domaine dans ce domaine : formation10.lan
- Vers tous les serveurs DNS exécutés sur des contrôleurs de domaine dans ce domaine : formation10.lan
- Vers tous les contrôleurs de ce domaine (compatibilité avec Windows 2000) : formation10.lan
- Vers tous les contrôleurs de domaine spécifiés dans l'étendue de cette partition d'annuaire :

**Nouvel hôte**

Nom (utilisez le domaine parent si ce champ est vide) :

Nom de domaine pleinement qualifié (FQDN) :

Adresse IP :

Créer un pointeur d'enregistrement PTR associé

Autoriser tout utilisateur identifié à mettre à jour les enregistrements DNS avec le même nom de propriétaire

# Le schéma

## Vocabulaires :

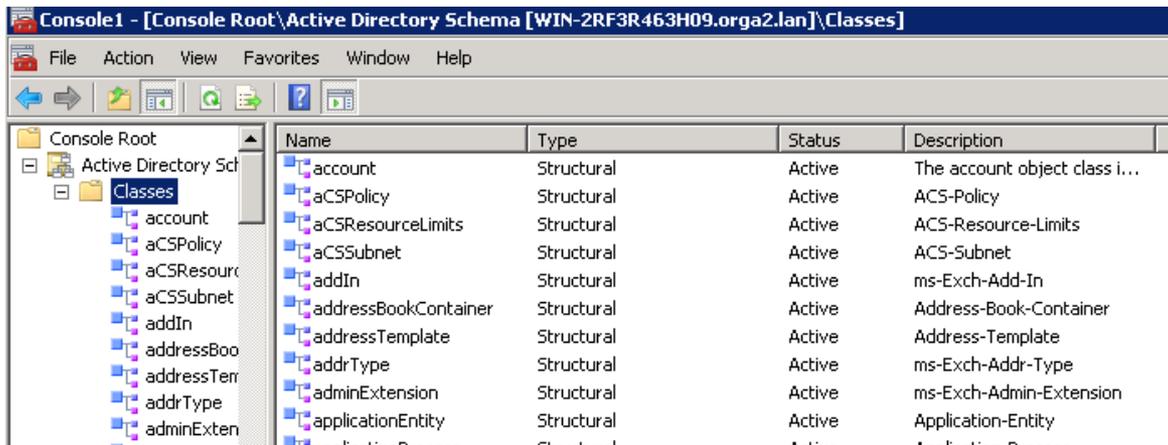
- Attributs : propriétés d'un objet (exemple : description, société, numéro de fax...).
- Méthodes : actions que l'on peut faire sur un objet (déplacer, supprimer..)
- Classes : types d'objets (exemple de classe d'objet : groupe, utilisateur).
- Schéma : ensemble des attributs, des méthodes et des classes.

Le schéma Active Directory est extensible. Cela permet d'ajouter des attributs ou des classes. On ne peut pas modifier les méthodes. Certaines applications comme Exchange (setup.com/PrepareAD) nécessite d'étendre le schéma.

<http://technet.microsoft.com/fr-fr/library/bb727029.aspx>

<http://technet.microsoft.com/en-us/library/bb727064.aspx>

[http://technet.microsoft.com/en-us/library/cc784557\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc784557(WS.10).aspx)



The screenshot shows the Active Directory Schema console window. The title bar reads "Console1 - [Console Root\Active Directory Schema [WIN-2RF3R463H09.org2.lan]\Classes]". The window has a menu bar with "File", "Action", "View", "Favorites", "Window", and "Help". Below the menu bar is a toolbar with various icons. The main area is a table with columns "Name", "Type", "Status", and "Description". The table lists various classes such as "account", "aCSPolicy", "aCSResourceLimits", "aCSSubnet", "addIn", "addressBookContainer", "addressTemplate", "addrType", "adminExtension", and "applicationEntity".

Name	Type	Status	Description
account	Structural	Active	The account object class i...
aCSPolicy	Structural	Active	ACS-Policy
aCSResourceLimits	Structural	Active	ACS-Resource-Limits
aCSSubnet	Structural	Active	ACS-Subnet
addIn	Structural	Active	ms-Exch-Add-In
addressBookContainer	Structural	Active	Address-Book-Container
addressTemplate	Structural	Active	Address-Template
addrType	Structural	Active	ms-Exch-Addr-Type
adminExtension	Structural	Active	ms-Exch-Admin-Extension
applicationEntity	Structural	Active	Application-Entity

# Mise à jour/extension du schéma

## Pourquoi mettre à jour son schéma Active Directory :

Installation de produit qui s'appuie sur Active Directory comme Exchange.

ADPREP /Forestprep : permet d'ajouter les attributs et les classes permettant l'installation des contrôleurs de domaine de version Windows supérieur (exemple, DC 2008 R2 dans un domaine géré initialement par des DC Windows 2000).

## Best Practice :

Effectuer la manipulation sur le maître de Schéma.

Désactiver la réplication entrante et sortante sur le maître de schéma pendant la phase de mise à niveau du schéma (voir commande ci-dessous).

```
C:\Users\Administrator>repadmin /options WIN-2RF3R463H09 +DISABLE_OUTBOUND_REPL
Current DSA Options: IS_GC
New DSA Options: IS_GC DISABLE_OUTBOUND_REPL
```

```
C:\Users\Administrator>repadmin /options WIN-2RF3R463H09 +DISABLE_INBOUND_REPL
Current DSA Options: IS_GC DISABLE_OUTBOUND_REPL
New DSA Options: IS_GC DISABLE_INBOUND_REPL DISABLE_OUTBOUND_REPL
```

```
C:\Users\Administrator>repadmin /options WIN-2RF3R463H09 -DISABLE_INBOUND_REPL
Current DSA Options: IS_GC DISABLE_INBOUND_REPL DISABLE_OUTBOUND_REPL
New DSA Options: IS_GC DISABLE_OUTBOUND_REPL
```

```
C:\Users\Administrator>repadmin /options WIN-2RF3R463H09 -DISABLE_OUTBOUND_REPL
Current DSA Options: IS_GC DISABLE_OUTBOUND_REPL
New DSA Options: IS_GC
```

# TP schéma : paramétrage des attributs

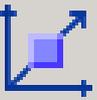
Créer une MMC vierge et ajouter le composant logiciel enfichable « *Maître de Schéma* ».

Vérifier si les attributs « *Description* » et « *Department* » sont dans le Catalogue Global (case « Répliquer cet attribut dans le catalogue global »).

Sélectionner l'attribut « *Title* ». Cocher la case pour que ce dernier soit conservé lors de la copie d'objet (compte utilisateur).

Propriétés de : title

Général



title

Description :	Title
Nom commun :	Title
ID d'objet X.500 :	2.5.4.12

Syntaxe et étendue

Syntaxe :	Chaîne Unicode
Minimum :	1
Maximum :	128

Cet attribut est à valeur simple.

- L'attribut est actif
- Indexer cet attribut
- Résolution de noms ANR (Ambiguous Name Resolution)
- Répliquer cet attribut dans le catalogue global
- L'attribut est copié lors de la duplication de l'utilisateur
- Indexer cet attribut pour des recherches en conteneur

# Les relations d'approbation 1/4

Les relations d'approbations permettent de partager des accès entre deux annuaires différents. Tous les domaines de la même forêt s'approuvent.

A approuve B : on peut définir des permissions sur les ressources du domaine A avec des utilisateurs / groupes du domaine B. Les utilisateurs de la forêt B sont automatiquement membres du groupe « *Utilisateurs authentifiés* » du domaine A.

L'authentification sélective permet de donner aucun droit par défaut entre deux domaines qui s'approuvent. Il faut déléguer au niveau de chaque compte ordinateur les droits « *Lire* » et « *Authentifier* » pour permettre un accès avec des permissions équivalentes à « *Utilisateurs Authentifiés* »

Pas d'approbation entre deux domaines avec un nom de domaine NETBIOS ou un nom de domaine DNS identique.

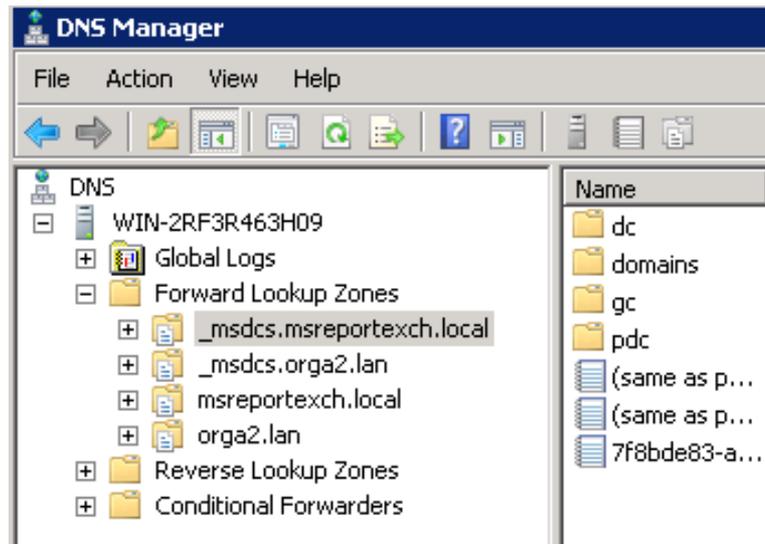
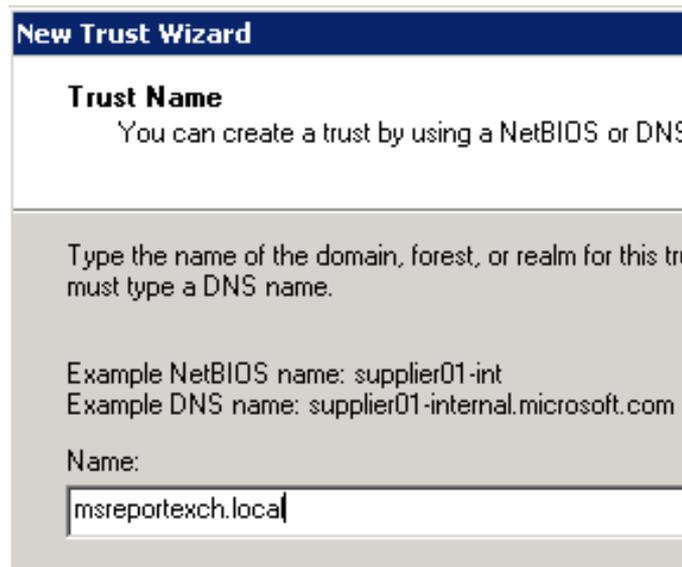
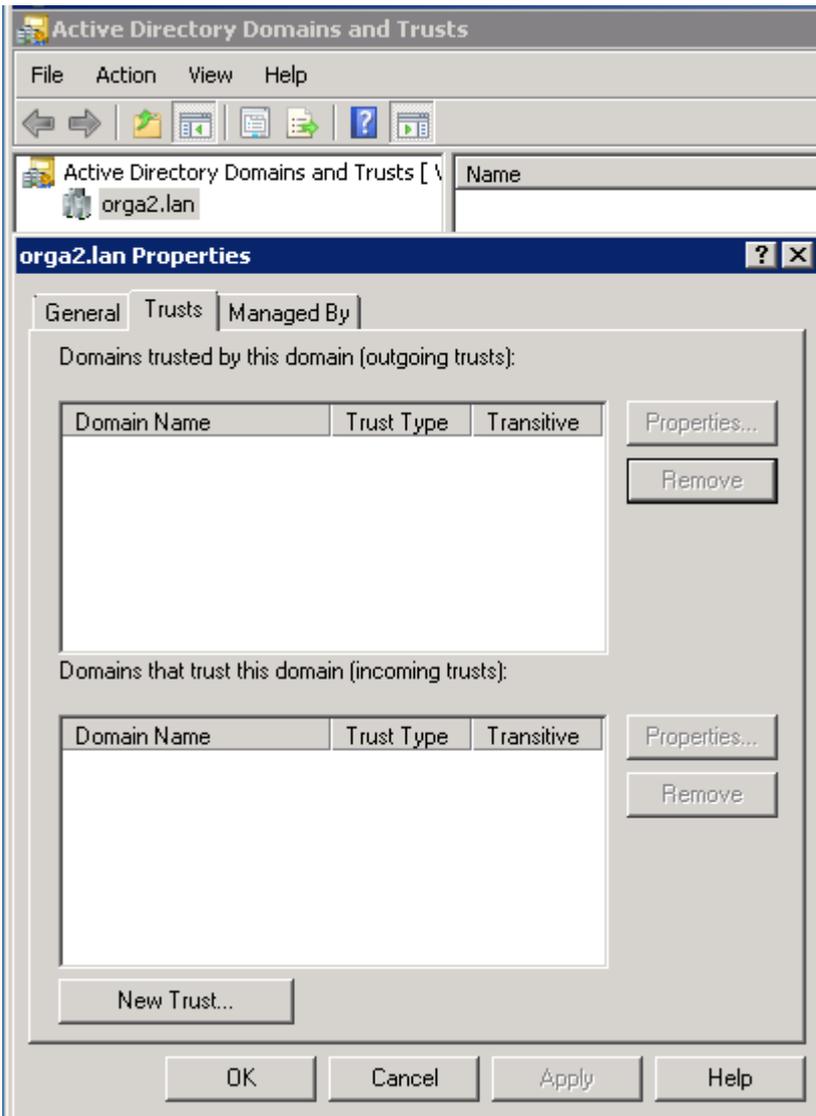
L'Emulateur PDC de chaque domaine doit être en ligne lorsque l'on crée une relation d'approbation entre deux domaines.

Les relations d'approbations peuvent être :

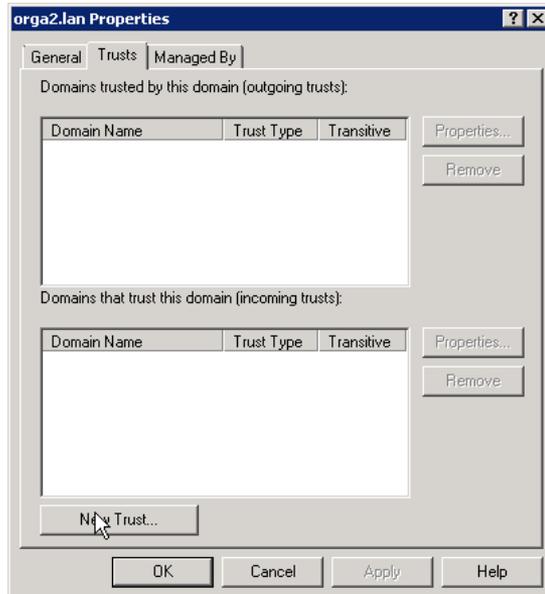
- Transitive : si A approuve B et que B approuve C, alors A approuve C.
- Implicite : automatique (relation d'approbation entre domaines de la même forêt).
- Bidirectionnelle : A approuve B et B approuve A.

Les relations d'approbations entre domaines de la même forêt sont transitives, implicites et bidirectionnelles.

# Les relations d'approbation 2/4



# Les relations d'approbation 3/4



## New Trust Wizard

### Trust Type

This domain is a forest root domain. If the specified domain qualifies, you can create a forest trust.

Select the type of trust you want to create.

- External trust  
An external trust is a nontransitive trust between a domain and another domain outside the forest. A nontransitive trust is bounded by the domains in the relationship.
- Forest trust  
A forest trust is a transitive trust between two forests that allows users in any of the domains in one forest to be authenticated in any of the domains in the other forest.

## New Trust Wizard

### Trust Name

You can create a trust by using a

Type the name of the domain, forest, or trust. The name must be a DNS name.

Example NetBIOS name: supplier01-ir  
Example DNS name: supplier01-intern

Name:

## New Trust Wizard

### Direction of Trust

You can create one-way or two-way trusts.

Select the direction for this trust.

- Two-way  
Users in this domain can be authenticated in the specified domain, realm, or forest, and users in the specified domain, realm, or forest can be authenticated in this domain.
- One-way: incoming  
Users in this domain can be authenticated in the specified domain, realm, or forest.
- One-way: outgoing  
Users in the specified domain, realm, or forest can be authenticated in this domain.

# Les relations d'approbation 4/4

## New Trust Wizard

### Sides of Trust

If you have appropriate permissions in both domains, you can create both sides of the trust relationship.

To begin using a trust, both sides of the trust relationship must be created. For example, if you create a one-way incoming trust in the local domain, a one-way outgoing trust must also be created in the specified domain before authentication traffic will begin flowing across the trust.

Create the trust for the following:

- This domain only  
This option creates the trust relationship in the local domain.
- Both this domain and the specified domain  
This option creates trust relationships in both the local and the specified domains. You must have trust creation privileges in the specified domain.

## Ouvrir le dossier



\\10.0.0.1 n'est pas accessible. Vous ne disposez peut-être pas des autorisations nécessaires pour utiliser cette ressource réseau. Contactez l'administrateur de ce serveur pour savoir si vous disposez des autorisations d'accès.

Échec de l'ouverture de session : l'ordinateur sur lequel vous êtes connecté est protégé par un pare-feu d'authentification. Le compte spécifié n'est pas autorisé à s'authentifier sur l'ordinateur.

OK

Utilisateurs et ordinateurs Active Directory

Sélectionnez des utilisateurs, des ordinateurs, des comptes de service ou des requêtes communes

Sélectionnez le type de cet objet :  
des utilisateurs ou des groupes

À partir de cet emplacement :  
formation3.lan

Requêtes communes

Nom : Commence par

Description : Commence par

Comptes désactivés  
 Mot de passe sans date d'expiration

Nombre de jours depuis la dernière session :

### Sécurité de Windows

#### Saisie du mot de passe réseau

Entrez le nom et le mot de passe d'un compte avec les autorisations pour formation3.lan.

Par exemple Utilisateur, Utilisateur@microsoft.com ou Domaine\Nom d'utilisateur

administrateur@formation3.lan

Domaine : formation3.lan

### Propriétés de : DCFORM1

Général | Système d'exploitation | Membre de | Délégation | Emplacement

Géré par | Objet | Sécurité | Appel entrant | Éditeur d'attributs

Noms de groupes ou d'utilisateurs :

- Administrateur (formation3\Administrateur)
- Tout le monde
- SELF
- Utilisateurs authentifiés
- Système
- Admins du domaine (FORMATION1\Admins du domaine)
- Éditeurs de certificats (FORMATION1\Éditeurs de certificats)

Ajouter... Supprimer

#### Autorisations pour Administrateur

	Autoriser	Refuser
Contrôle total	<input type="checkbox"/>	<input type="checkbox"/>
Lire	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Écrire	<input type="checkbox"/>	<input type="checkbox"/>
Créer tous les objets enfants	<input type="checkbox"/>	<input type="checkbox"/>
Supprimer tous les objets enfants	<input type="checkbox"/>	<input type="checkbox"/>
Autorisation d'authentifier	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Écriture validée vers le serveur d'hôte DNS	<input type="checkbox"/>	<input type="checkbox"/>

# TP : création d'une relation d'approbation

Ouvrir la console DNS.

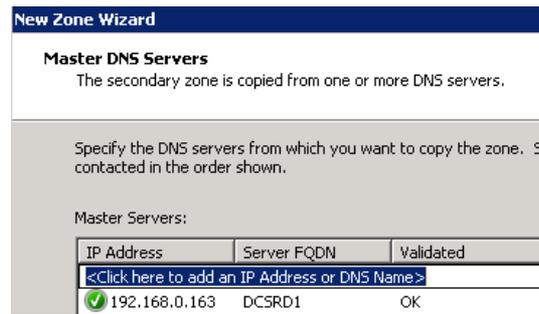
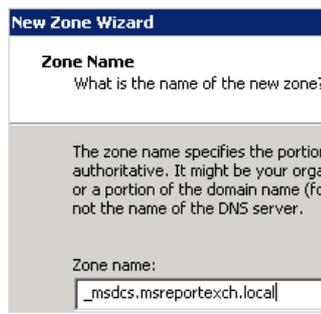
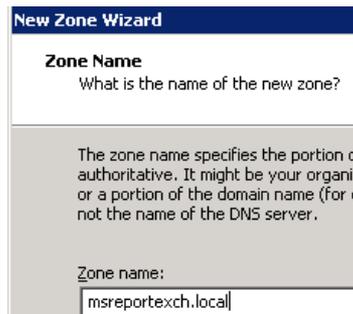
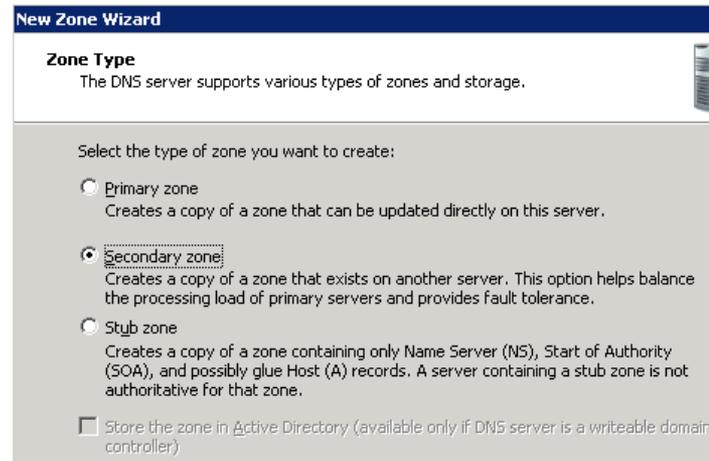
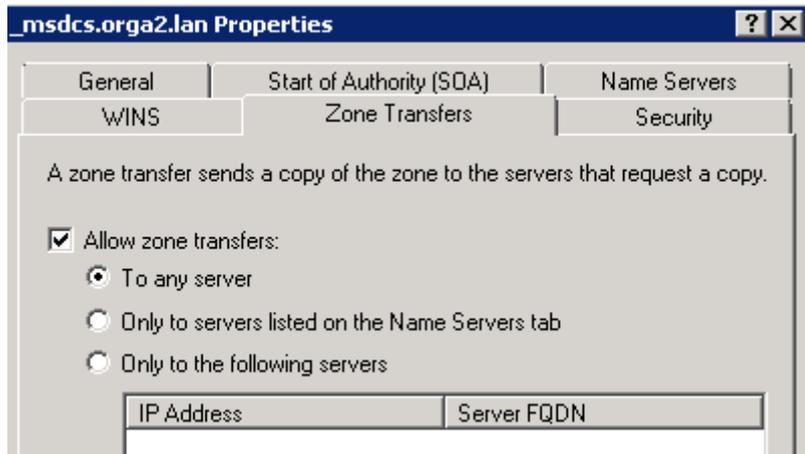
Autoriser sur toutes les zones le transfert de zones.

Sur le DC1 (domaine 1), ajouter les zones DNS du DC2 (domaine 2).

Ouvrir la console « *Domaines et Approbation Active Directory* ».

Créer une relation d'approbation bidirectionnelle.

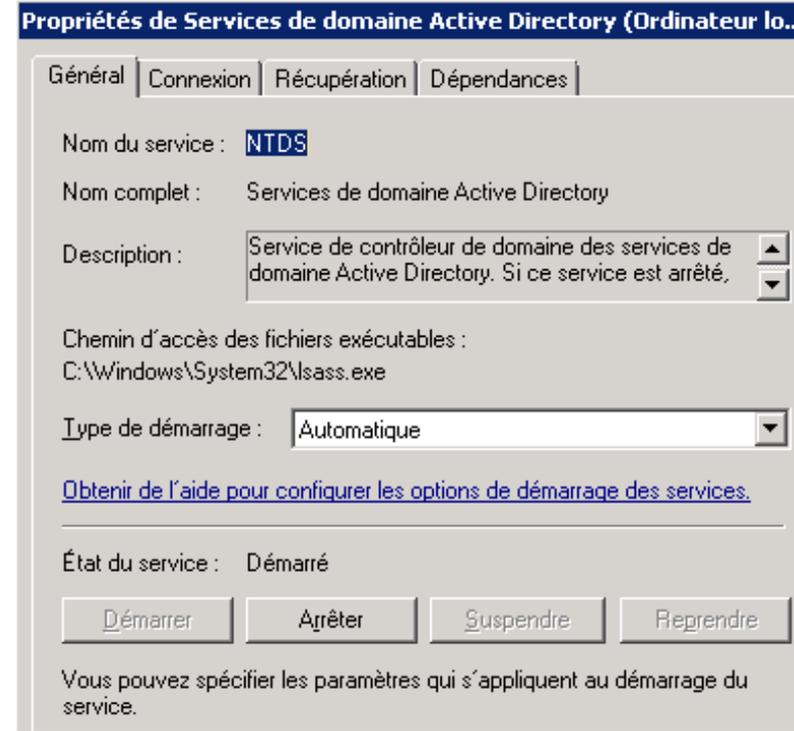
Activer l'authentification sélective.



# Les services Active Directory

Services d'un contrôleur de domaine :

- Netlogon (lsass.exe) : client d'authentification
- Active Directory Services / NTDS (lsass.exe) : service d'authentification. Existe sous forme d'un service depuis Windows 2008.
- Kerberos Key Distribution Center : service de distribution de clés Kerberos ( délivre les TGTs, tickets de service)
- Service de réplication de fichiers (NTFRS) ou service DFSR : en charge de la réplication du dossier SYSVOL.
- Service DNS : héberge la zone DNS qui dispose des entrées permettant aux clients de localiser les contrôleurs de domaine.
- Client DHCP : ce service permet au contrôleur de domaine d'enregistrer dynamiquement les entrées DNS du fichier netlogon.dns.



# Le répertoire SYSVOL

Contient les scripts et les fichiers des stratégies de groupe (GPO).  
L'emplacement de SYSVOL se définit au DCPROMO (modification avec NTDSUTIL).

Réplique sur tous les contrôleurs de domaine.

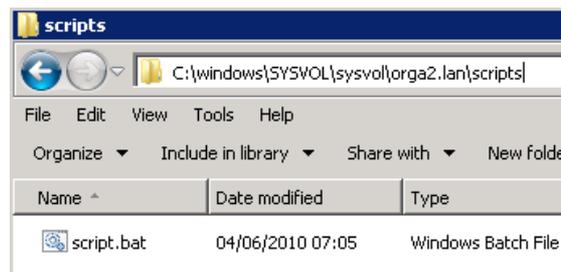
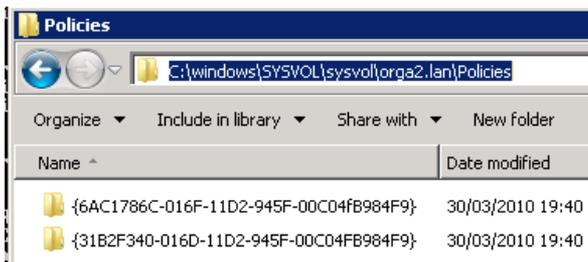
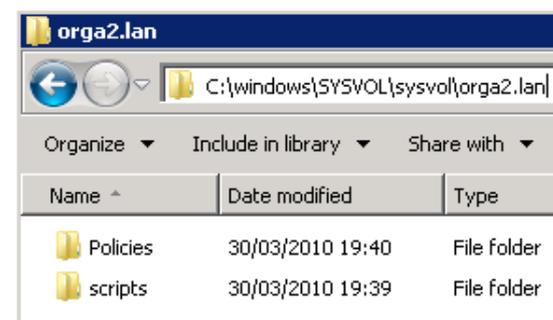
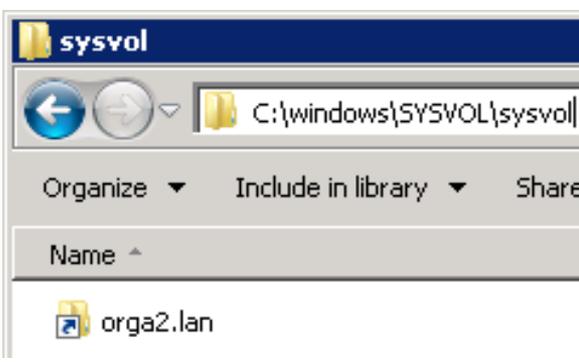
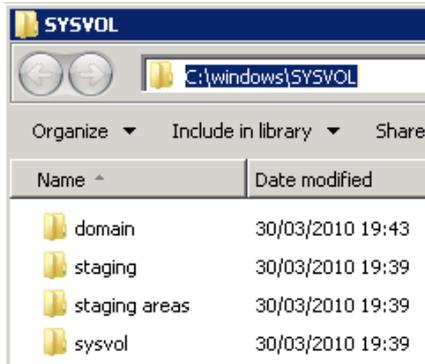
En mode natif 2003 et antérieur : utilisation du moteur NTFRS

En mode natif 2008 et ultérieur : utilisation du moteur DFSR

(recommandée, procédure de migration en 3 étapes).

Le partage NETLOGON correspond au répertoire  
*c:\windows\sysvol\sysvol\nom\_domaine\scripts*.

Le partage SYSVOL correspond au répertoire *c:\windows\sysvol\sysvol*.



# Le répertoire NTDS

Contient l'annuaire (fichier NTDS.DIT)

**Pour sauvegarder l'annuaire, il faut obligatoirement une sauvegarde de l'Etat du système.** Une sauvegarde du lecteur C n'est pas suffisante.

Les modifications sont effectuées dans les logs puis inscrits ensuite dans le fichier NTDS.DIT.

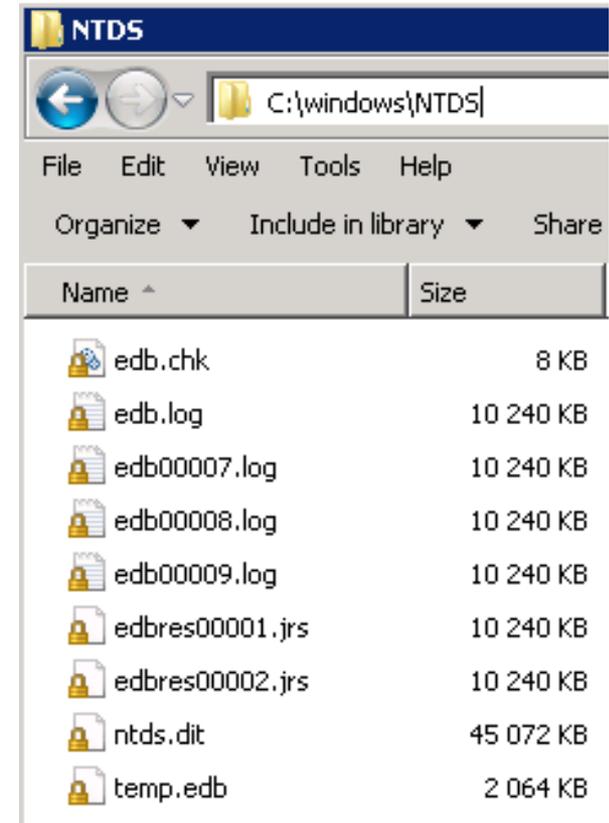
Le fichier .chk permet de connaître le log en cours.

Les fichiers .jrs sont des fichiers de logs utilisés en cas de saturation de l'espace disque.

Le fichier temp.edb est une base de données temporaire utilisée pour certaines opérations.

Pour réparer la base de données Active Directory, il faut utiliser l'utilitaire ESEUTIL (défragmentation....).

Windows effectue tous les soirs une défragmentation en ligne de l'annuaire. Cette dernière ne permet cependant pas de récupérer de l'espace disque. Il faut une défragmentation hors ligne.



# TP SYSVOL & NTDS 1/2

**Prérequis** : Un domaine avec deux contrôleurs de domaine.

Sur le premier contrôleur de domaine, créer un fichier test.txt (contenu test1) dans c:\windows\sysvol\sysvol\nom\_domaine. Attendre environ 5 minutes.

Valider que ce dernier est apparu dans le même répertoire sur le second contrôleur de domaine.

Sur les deux contrôleurs de domaine, éditer le même fichier, le modifier (mettre une valeur différente) et l'enregistrer au même moment. Que se passe t'il ?

Arrêter le service « *DFS Replication* » sur le second contrôleur de domaine. Créer un nouveau fichier sur le premier contrôleur de domaine. Que se passe t'il ?

# TP SYSVOL & NTDS 2/2

Taper les commandes suivantes :

*Ntdsutil*

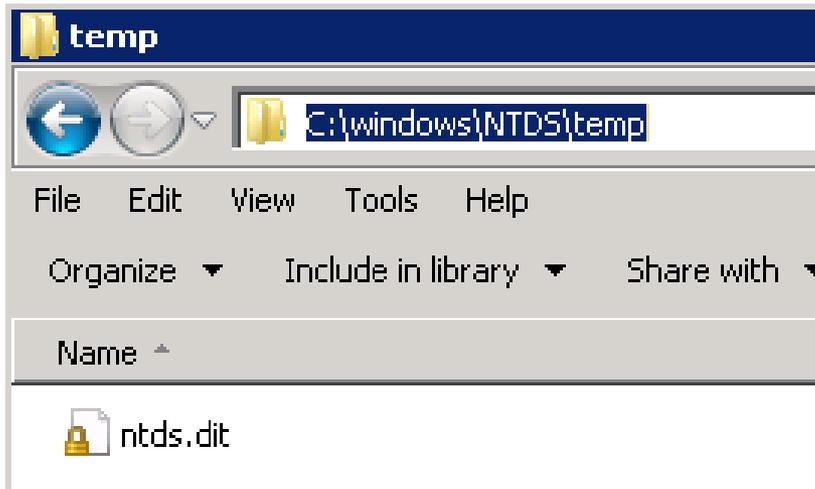
*Activate Instance NTDS*

*Files*

*Info*

*Compact to c:\Windows\NTDS\temp*

Remplacer le fichier NTDS.DIT.



```
ntdsutil: activate Instance ntds
Error parsing Input - Invalid Syntax.
ntdsutil: activate Instance NTDS
Error parsing Input - Invalid Syntax.
ntdsutil: Activate Instance NTDS
Active instance set to "NTDS".
ntdsutil: files
Error parsing Input - Invalid Syntax.
ntdsutil: Activate Instance NTDS
Active instance set to "NTDS".
ntdsutil: files
file maintenance: info

Drive Information:

        C:\ NTFS <Fixed Drive  > free<31.3 Gb> total<39.8 Gb>

DS Path Information:

Database       : C:\Windows\NTDS\ntds.dit - 44.1 Mb
Backup dir    : C:\Windows\NTDS\dsadata.bak
Working dir   : C:\Windows\NTDS
Log dir       : C:\Windows\NTDS - 60.0 Mb total
                edbres00002.jrs - 10.0 Mb
                edbres00001.jrs - 10.0 Mb
                edb00009.log - 10.0 Mb
                edb00008.log - 10.0 Mb
                edb00007.log - 10.0 Mb
                edb.log - 10.0 Mb
file maintenance: Compact to c:\Windows\NTDS\temp
Initiating DEFRAGMENTATION mode...
        Source Database: C:\Windows\NTDS\ntds.dit
        Target Database: c:\Windows\NTDS\temp\ntds.dit

                Defragmentation Status (% complete)

                0    10    20    30    40    50    60    70    80    90   100
                |----|----|----|----|----|----|----|----|----|----|
                .....

It is recommended that you immediately perform a full backup
of this database. If you restore a backup made before the
defragmentation, the database will be rolled back to the state
it was in at the time of that backup.

Compaction is successful. You need to:
copy "c:\Windows\NTDS\temp\ntds.dit" "C:\Windows\NTDS\ntds.dit"
and delete the old log files:
del C:\Windows\NTDS\*.log

file maintenance: _
```

# 3. Les comptes utilisateurs

# Présentation compte utilisateur 1/3

Les comptes utilisateurs sont identifiés par le SID / GUID et non par le login. Il est donc possible de changer le login / renommer un compte utilisateur.

Il existe deux types de login (un pour nom NETBIOS et un pour nom DNS).

Toujours cocher la case « *Le mot de passe n'expire jamais pour un compte de service* » ou utiliser la nouvelle fonctionnalité de « *Compte de services gérés* ».

Propriétés de : guillaume.mathieu

Membre de	Réplication de mot de passe	Appel entrant	Objet	Sécurité		
Environnement		Sessions	Contrôle à distance			
Profil des services Bureau à distance		Bureau virtuel personnel	COM+	Éditeur d'attributs		
Général	Adresse	Compte	Profil	Téléphones	Organisation	Certificats publiés

 guillaume.mathieu

Prénom :  Initiales :

Nom :

Nom complet :

Description :

Bureau :

Numéro de téléphone :

Adresse de messagerie :

Page Web :

Propriétés de : guillaume.mathieu

Membre de	Réplication de mot de passe	Appel entrant	Objet	Sécurité		
Environnement		Sessions	Contrôle à distance			
Profil des services Bureau à distance		Bureau virtuel personnel	COM+	Éditeur d'attributs		
Général	Adresse	Compte	Profil	Téléphones	Organisation	Certificats publiés

Nom d'ouverture de session de l'utilisateur :

Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000) :

Déverrouiller le compte

Options de compte :

- L'utilisateur devra changer le mot de passe
- L'utilisateur ne peut pas changer de mot de passe
- Le mot de passe n'expire jamais
- Enregistrer le mot de passe en utilisant un chiffrement réversible

Date d'expiration du compte

- Jamais
- Fin de :

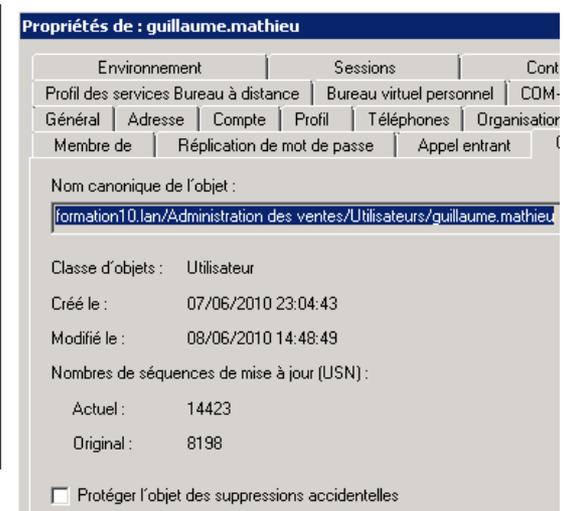
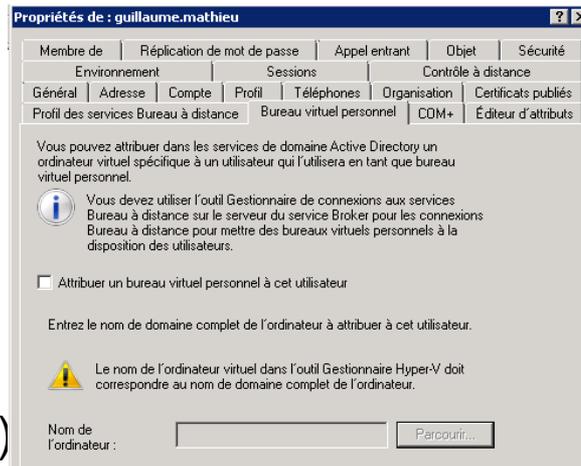
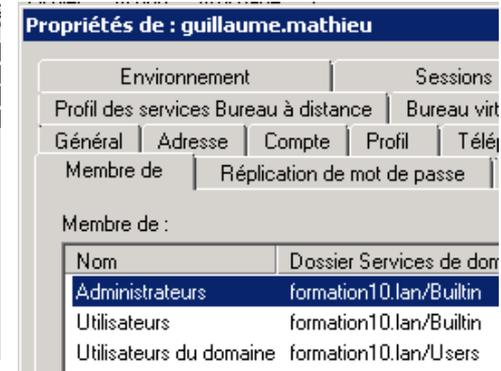
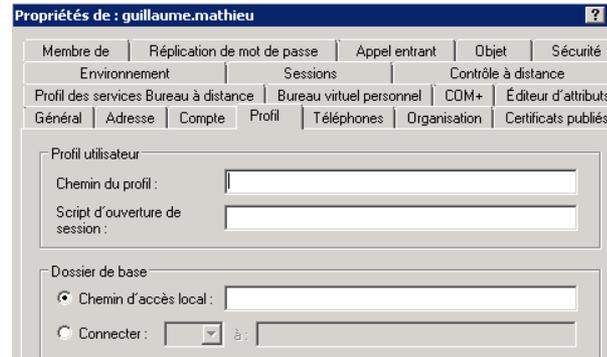
# Présentation compte utilisateur 2/3

Pour le chemin des profils itinérants, il est possible d'utiliser la variable %username% et faire une sélection multiple.

Indiquer juste le nom du script de login. Ce dernier doit se trouver dans  
c:\windows\sysvol\sysvol\nom\_domaine\_dns\scripts

Depuis Windows Server 2008, il est possible de protéger les comptes utilisateurs contre une suppression accidentelle. Cela positionne des permissions « *Refusé* » pour l'opération de suppression au niveau de l'onglet « *Sécurité* » du compte utilisateur (il faut être en mode d'affichage « *Fonctionnalités avancées* »).

Avec les RODC, il est possible de dire si le mot de passe peut être mis en cache (en mémoire) ou non.



# Présentation compte utilisateur 3/3

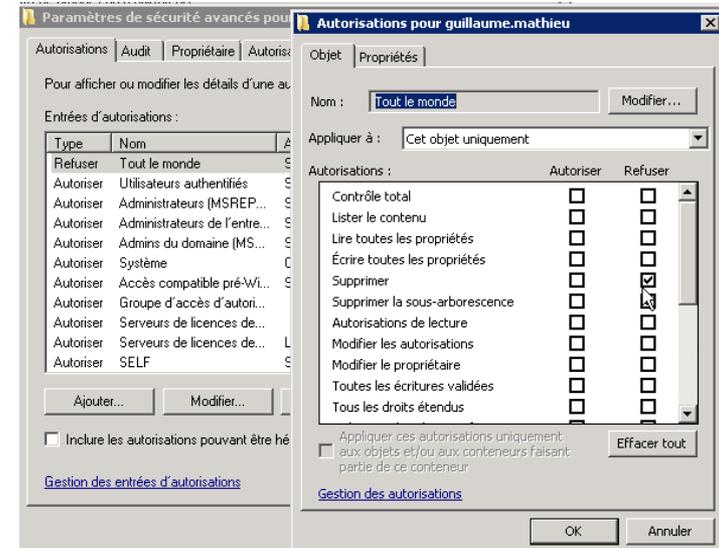
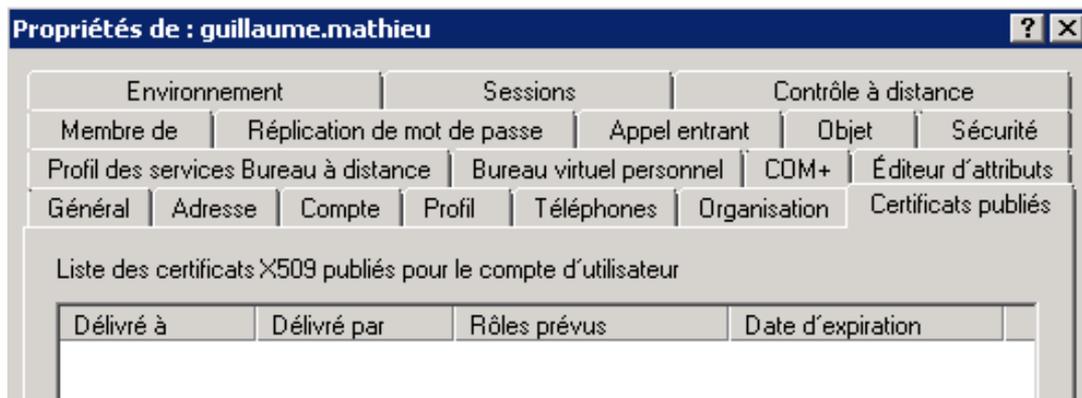
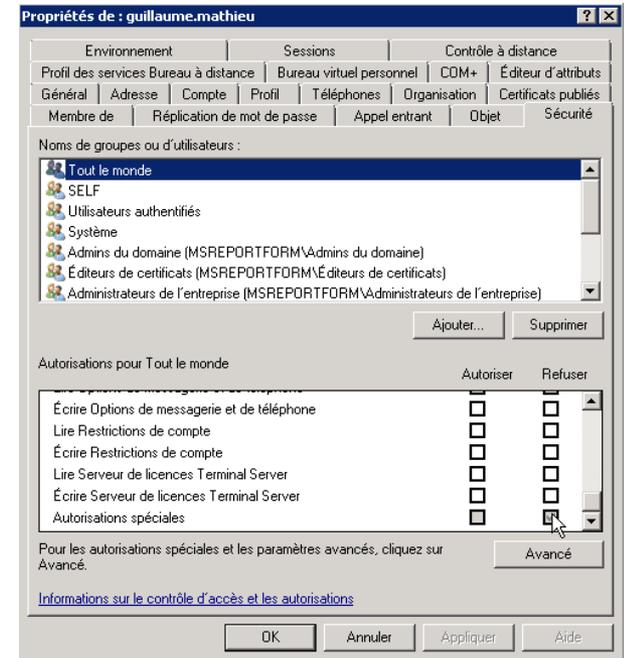
La console Utilisateurs et Ordinateurs Active Directory intègre maintenant un éditeur ADSIEDIT (onglet « *Editeur d'attributs* »).

Les deux captures de droite montrent les permissions positionnées par la case « *Protéger contre la suppression accidentelle* ».

L'onglet « *Bureau Virtuel* » est lié à la solution Microsoft Virtual Desktop Infrastructure (VDI).

<http://www.laboratoire-microsoft.org/articles/Microsoft-VDI/4/>

Il est possible de visualiser les certificats associés aux comptes utilisateurs comme pour EFS (clé publique uniquement)

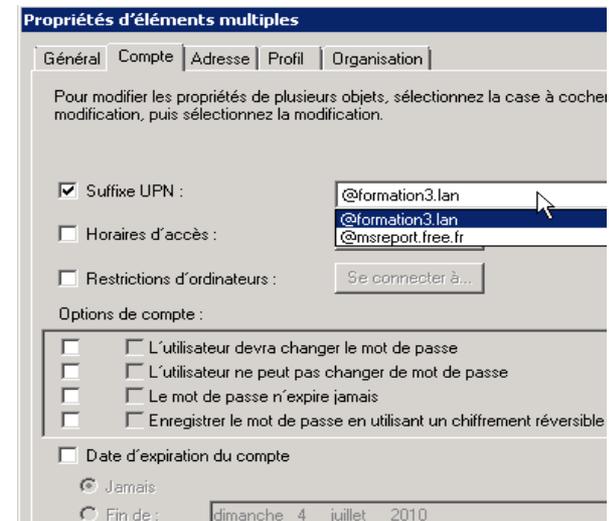
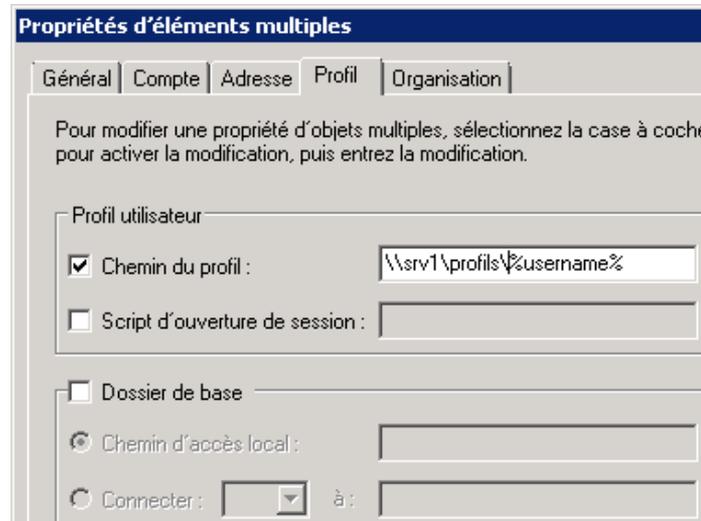
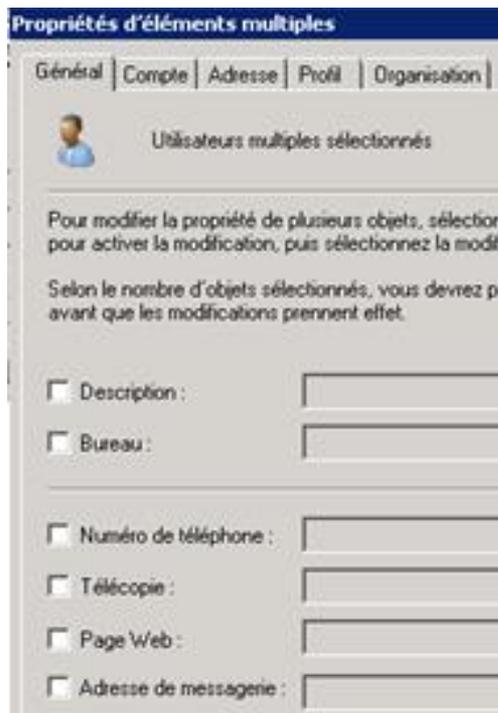
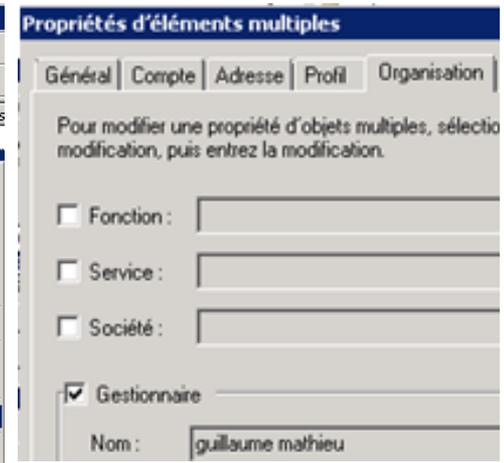
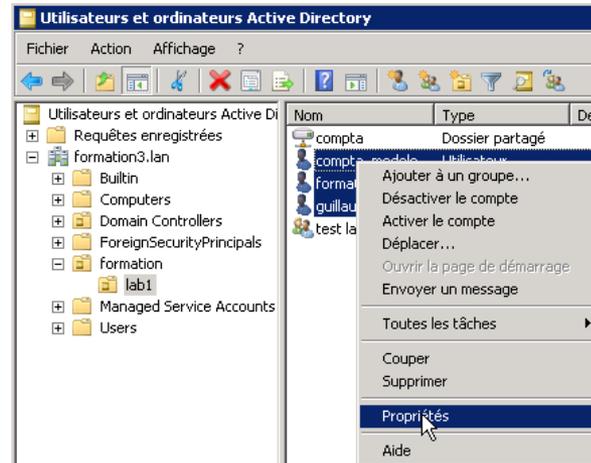


# Modifications multiples

Il est possible d'effectuer des modifications sur plusieurs comptes en même temps en appuyant sur la touche contrôle et en sélectionnant les comptes utilisateurs. On peut aussi utiliser un outil comme *ADMODIFY*.

Pour plus d'informations sur ADMODIFY, voir :

[http://msreport.free.fr/?page\\_id=124](http://msreport.free.fr/?page_id=124)

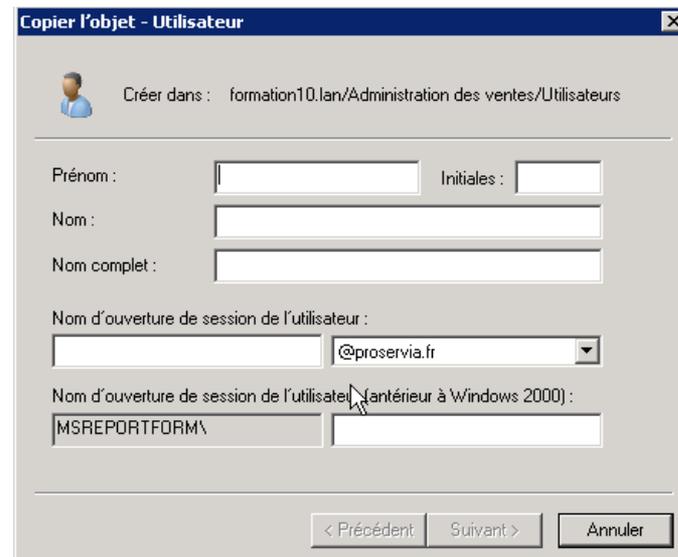
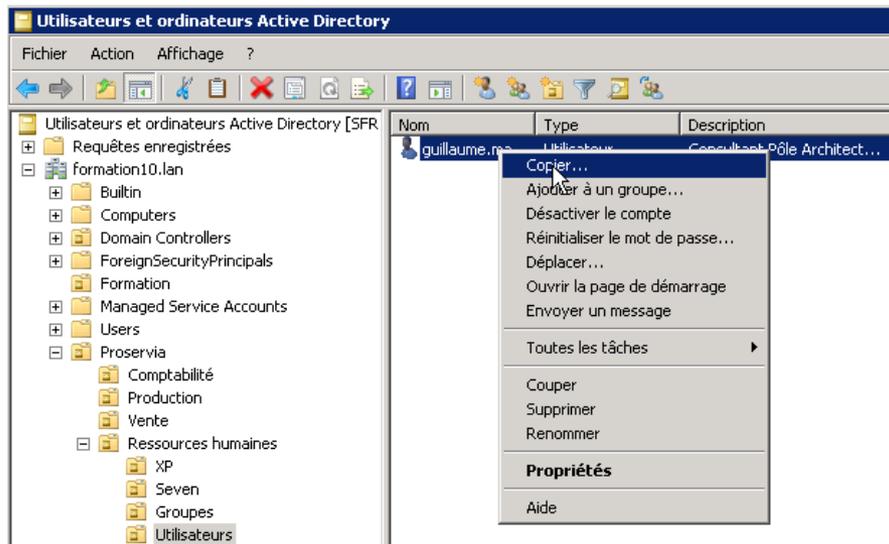


# Les modèles de comptes utilisateurs

Modèle de compte : on passe par la fonction Copier. L'assistant classique se lance ensuite et demande de saisir les informations spécifiques au compte utilisateur. On peut modifier dans la console « Schéma », les valeurs des attributs qui sont conservés lors d'un copie.

Intérêt : permet de conserver la valeur de certains attributs (appartenances aux groupes, certains champs de l'adresses...). D'où un gain de temps.

Best Practice : les modèles de comptes utilisateurs doivent être des comptes désactivés



# Best Practice compte utilisateur :

Valider avec la direction la convention de nommage et la stratégie de mots de passe.

Intégrer si possible une chaîne de caractère aléatoire dans le login pour éviter les attaques par verrouillage (en déterminant le login d'un utilisateur).

Créer des modèles de comptes utilisateurs.

**Désactiver les comptes au lieu de les supprimer.** En effet en cas de suppression, il ne sera pas possible de récupérer le SID sauf si l'on effectue une restauration autoritaire (avec NTDSUTIL).

Ne pas activer le verrouillage de comptes avec un seuil trop faible (mettre environ 50 échecs avant le verrouillage).

Pour les comptes de services, cocher la case « *Le mot de passe n'expire jamais* » afin d'éviter que le mot de passe des comptes de services n'expire. Cela bloquera en effet le démarrage du service. Il est aussi possible d'utiliser les nouveaux comptes de services gérés.

Il existe des outils comme *Active Roles* qui permettent de forcer la saisie de certains champs lors de la création des comptes utilisateurs ou qui permettent d'imposer un certain formalisme lors de la saisie des champs.

# TP : création compte utilisateur

Créer un compte utilisateur sans mot de passe. On obtient le message d'erreur ci-dessous. Réessayer en utilisant le mot de passe « *P@ssword* ».

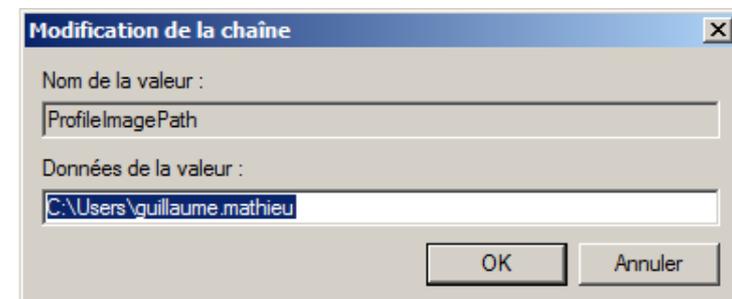
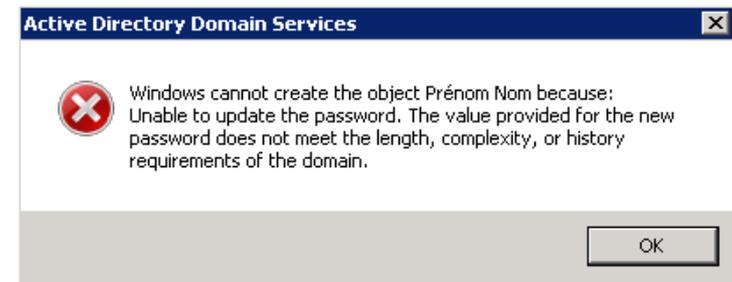
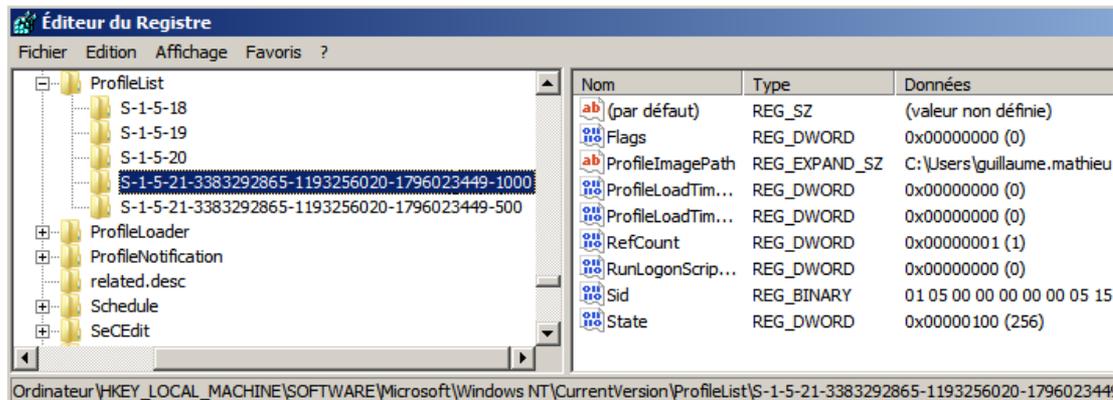
Ouvrir une session avec ce compte sur une machine membre du domaine. Un nouveau profil est généré.

Lancer l'éditeur de base de registre (REGEDT32). Faire une recherche sur la valeur « *profileimagepath* ». Cette clé permet de mapper le SID du compte au profil utilisateur. Personnaliser le profil (fond d'écran, création de fichiers sur le bureau...). Fermer la session.

Renommer le compte utilisateur (champ prénom, nom, description, **login**).

Ouvrir la session. Vous devez récupérer votre profile. Pourquoi ?

<http://msreport.free.fr/?p=86>



# La gestion des mots de passe 1/2

## Les paramètres de stratégies de mots de passe :

- Historique des mots de passe / durée de vie minimale du mot de passe : permet d'empêcher les utilisateurs de réutiliser le même mot de passe. Le paramètre durée de vie minimale du mot de passe empêche l'utilisateur de changer X fois son mot de passe jusqu'à pouvoir ressaisir son ancien mot de passe.
- Durée de vie maximale du mot de passe : le mot de passe devra être changé tous les X jours.
- Longueur minimum du mot de passe : le mot de passe doit faire au minimum X caractères.
- Les mots de passe doivent respecter les exigences de complexité : permet d'obliger les utilisateurs à saisir un mot de passe avec un caractère spécial ou une majuscule ou un chiffre. Les paramètres de complexité ne sont pas configurables. La complexité des mots de passe est gérée via le fichier passfit.dll. Des outils tiers comme *One Identity Password Manager* permettent de disposer d'une Passfit.dll personnalisée (dictionnaire de mots de passe interdit, caractères interdits...). Il existe aussi une solution gratuite alternative : <https://blog.scrt.ch/2017/08/23/passfilt-dll-complexifier-sa-politique-de-mot-de-passe-windows/>

## Quelle stratégie de mots de passe adoptée ?

Depuis Windows Server 2008, les « *Fine Grained Password Policy* » permettent de définir des stratégies de mots de passe spécifiques pour un utilisateur ou un groupe.

[http://technet.microsoft.com/en-us/library/cc770842\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc770842(WS.10).aspx)

# La gestion des mots de passe 2/2

## **Les risques :**

Une politique de mots de passe trop faible risque de compromettre le niveau de sécurité de la société tout comme une politique de mots de passe trop complexe (les utilisateurs écrivent sur papier leur mot de passe).

## **Réinitialisation de mots de passe ≠ Changement de mot de passe :**

Attention la réinitialisation de mot de passe fait perdre l'accès aux données chiffrées avec EFS dans certains cas (si compte de la base SAM local par exemple).

## **Self Service Password Reset :**

De nombreux outils comme *One Identity Password Manager* ou Microsoft Azure AD Premium (SSPR) permettent aux utilisateurs de réinitialiser eux même leur mot de passe via des questions réponses, l'envoi de Passcode par SMS ou messagerie personnelle. L'utilisation de questions / réponses peut abaisser fortement le niveau de sécurité ou générer des problèmes de conformité avec le RGPD. L'envoi de Passcode sur téléphone portable Pro est donc à privilégier.

## **Quel politique adoptée ?**

Toujours faire valider la stratégie de mots de passe par la direction.

Il faut trouver un juste milieu (complexité activé, historique : 5 mots de passe, durée de vie minimale du mot de passe : 1 journée, durée de vie maximale du mot de passe : 42 jours).

## **L'option « Le mot de passe n'expire jamais » :**

A définir uniquement pour les comptes de services (pas pour les autres comptes)

# MSA et gMSA

## MSA :

- Prise en charge avec machine Windows Server 2008 R2 / Windows Seven.
- Un *Managed Service Account* par machine (pas de partage d'un même « *Managed Service Account* » entre machines).
- Pas de pris en charge des cluster (services mis en haute disponibilité).
- *msDS-ManagedServiceAccount* : nouvelle classe pour gérer les *Managed Service Accounts*.
- *Managed Service Account* : c'est une sorte d'intermédiaire entre un compte utilisateur et un compte ordinateur.
- Changement du mot de passe : même fonctionnement qu'un compte ordinateur (changement tous les 30 jours). Nécessite mode 2008 R2 pour changement automatique du mot de passe.
- Pas de login interactif ou de verrouillage de compte.
- Possibilité d'ajouter un *Managed Service Account* à un groupe (pour le contrôle des accès).

<http://blogs.technet.com/b/askds/archive/2009/09/10/managed-service-accounts-understanding-implementing-best-practices-and-troubleshooting.aspx>

## gMSA :

Disponible depuis Windows Server 2012.

<https://blogs.technet.microsoft.com/askpfeplat/2012/12/16/windows-server-2012-group-managed-service-accounts/>

**Toujours vérifier que l'application supporte l'usage des MSA ou gMSA !**

# 4. Les comptes ordinateurs

# Les comptes ordinateurs 1/2

Les comptes ordinateurs disposent d'un mot de passe.

Permet d'authentifier la machine dans le domaine. La machine envoie le mot de passe du compte ordinateur (qui est mis en cache) au contrôleur de domaine. Ce dernier le compare au mot de passe contenu dans l'annuaire.

Permet d'attribuer des GPO de type « *Configuration Ordinateur* ».

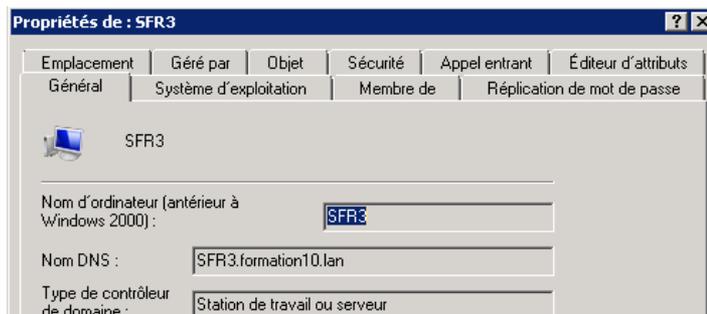
Le mot de passe du compte ordinateur change par défaut tous les 30 jours (configurable via registre / GPO).

Lorsque l'on joint une machine au domaine, par défaut le compte ordinateur est ajouté dans le conteneur « Computer » à la racine du domaine.

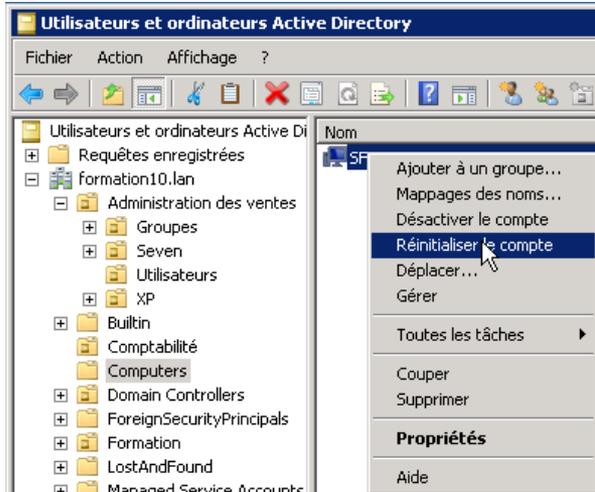
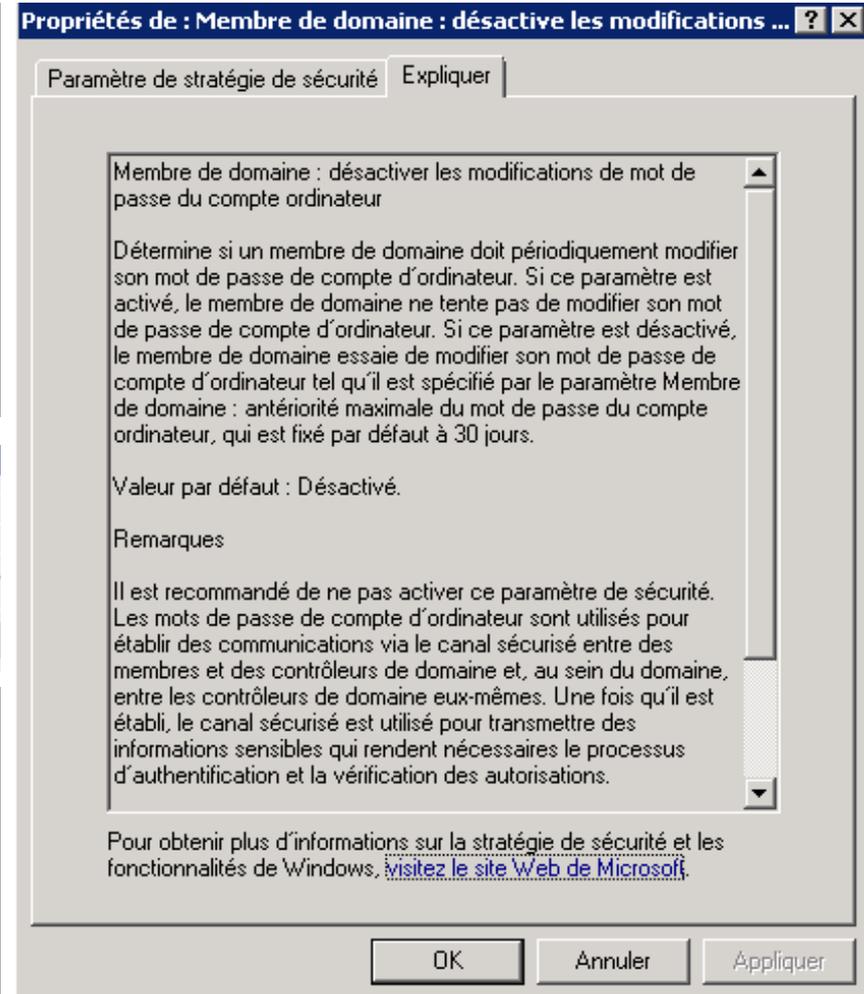
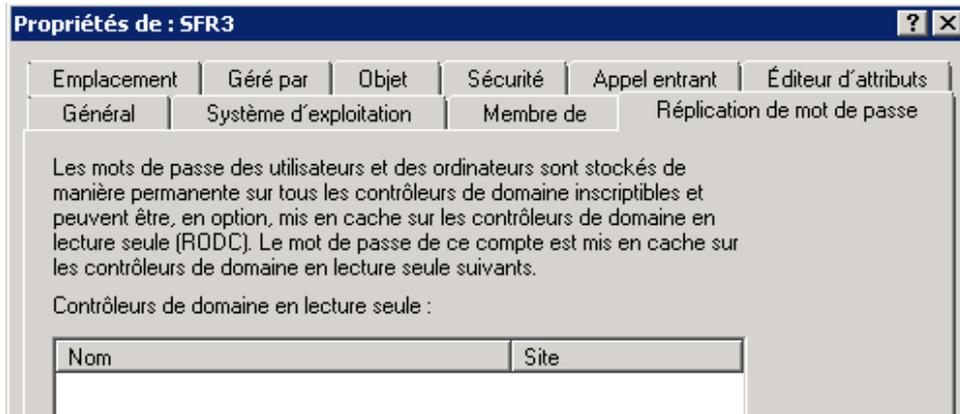
En cas de problème avec le compte ordinateur, une erreur NETLOGON apparaît sur la station de travail et le contrôleur de domaine.

Il est possible de pré-créer le compte ordinateur dans une OU spécifique.

Quand la machine joint le domaine, elle complète les informations (version de l'OS...).



# Les comptes ordinateurs 2/2



# TP : Les comptes ordinateurs

Installer Windows 10 Pro ou Enterprise. Ne pas mettre de serveur DNS. Joindre la machine avec le nom DNS de domaine. Cela échoue. Pourquoi ?

Mettre vos contrôleurs de domaine comme serveur DNS sur la machine Windows 10. Pourquoi faut-il définir plusieurs serveurs DNS ?

Sortir la machine du domaine. Redémarrer la machine.

Créer un compte utilisateur standard.

Joindre la machine au domaine en utilisant le nom de DNS de domaine. Utiliser le compte standard pour vous authentifier. Redémarrer la machine.

Ouvrir la console « *Utilisateurs et Ordinateurs Active Directory* ». Aller dans le conteneur « *Computers* ».

Aller dans les propriétés du compte ordinateur et parcourir les différents onglets. À quoi sert le groupe « *Ordinateurs du domaine* ».

Supprimer le compte ordinateur. Redémarrer la station de travail. Essayer d'ouvrir une session avec le compte utilisateur. Cela échoue. Pourquoi ? Ouvrir les observateurs d'événements et chercher une erreur Netlogon.

Joindre de nouveau la machine dans le domaine (la repasser en workgroup au préalable).

Réinitialiser le mot de passe du compte ordinateur. Redémarrer la station de travail.

Ouvrir les observateurs d'événements. Une erreur NETLOGON apparaît de nouveau.

Pourquoi ?

# 5. Les groupes

# Présentation générale des groupes

## **Qu'est ce qu'un groupe ?**

Un groupe est un ensemble de ressources.

Un groupe n'est pas un conteneur (ne pas confondre avec les OU).

On ne peut pas affecter de GPO à un groupe. On peut cependant filtrer l'application des GPO à des groupes en définissant les droits « *Lire* » et « *Appliquer les stratégies de groupes* » à un groupe (dans l'onglet Sécurité).

## **2 types de groupes :**

Les groupes de sécurité : utilisés pour la messagerie et gérer les droits.

Les groupes de distribution : utilisés pour la messagerie (liste de diffusion)

## **3 étendues différentes :**

Les groupes globaux de domaine

Les groupes locaux de domaine

Les groupes universels

## **Fonctionnement selon le niveau fonctionnel de domaine / forêt :**

Pour créer des groupes universelles : mode natif 2000 obligatoire.

Pour encapsuler des groupes globaux (groupes globaux membres d'autres groupes globaux) : mode natif 2000 obligatoire.

A partir du mode natif 2003, si l'on ajoute un objet comme membre d'un groupe, seul l'ajout du membre réplique. Auparavant l'objet groupe répliquait complètement.

On va pouvoir changer l'étendue d'un groupe à partir du mode natif 2000.

# Les étendues de groupes

Etendue	Membres	Visibilité	Intérêt
Globale	Objet du même domaine Ne peut pas contenir de groupe universel.	Visible sur le domaine locale et tous les domaines approuvées.	Groupe d'utilisateurs
Locale	Objet du domaine locale et de tous les domaines approuvées.	Visible sur le domaine locale uniquement.	Pour définir des permissions.
Universelle	Objet de tous les domaines de la forêt ( <b>pas sur les domaines approuvées hors de la forêt</b> )	Visible sur le domaine locale et tous les domaines approuvées	Liste des distributions pour Exchange.

# Notions avancées sur les groupes

Les propriétaires d'un groupe : peut gérer les appartenances aux groupes.

L'imbrication des groupes : un groupe peut avoir comme membre d'autres groupes selon le niveau fonctionnel du domaine.

Pour modifier l'étendue d'un groupe : convertir un groupe globale en groupe universel puis le repasser en groupe local. **Attention aux permissions définies sur les serveurs à l'aide des groupes !** Un groupe globale est visible depuis le domaine locale et tous les domaines approuvés. Un groupe locale n'est visible que depuis son domaine ! Attention aux incohérences.

On peut aussi changer le type d'un groupe. Attention si l'on passe un groupe de sécurité en groupe de distribution, toutes les permissions définies ne fonctionneront plus mais elles continueront de s'afficher dans l'onglet « Sécurité ».

Pas de synchronisation entre le système de fichiers et l'annuaire.

Permission accès partage = cumul le plus restrictif permissions Partages / NTFS.

Nouvel objet - Groupe

Créer dans : formation10.lan/Administratio

Nom du groupe : GG\_Administration des groupes

Nom de groupe (antérieur à Windows 2000) : GG\_Administration des groupes

Étendue du groupe

- Domaine local
- Globale
- Universelle

Type de groupe

- Sécurité
- Distribution

Propriétés de : GG\_Administration des groupes

Général Membres Membre de Géré par

GG\_Administration des groupes

Nom de groupe (antérieur à Windows 2000) :

Description :

Adresse de messagerie :

Étendue du groupe

- Domaine local
- Globale
- Universelle

Propriétés de : GDL\_Partage\_AdminsVent

Général Membres Membre de Géré par

GDL\_Partage\_AdminsVente

Nom de groupe (antérieur à Windows 2000) :

Description :

Adresse de messagerie :

Étendue du groupe

- Domaine local
- Globale
- Universelle

Propriétés de : GU\_Administration des ventes

Général Membres Membre de Géré par

GU\_Administration des ventes

Nom de groupe (antérieur à Windows 2000) :

Description :

Adresse de messagerie :

Étendue du groupe

- Domaine local
- Globale
- Universelle

# Les Best Practice

Eviter de convertir les groupes de sécurités en groupe de distribution.

Eviter d'utiliser les groupes universels. Les groupes universels augmentent la taille du « *Catalogue globale* ».

Utiliser les groupes locaux de domaine pour définir des permissions sur les serveurs de fichiers et au niveau de l'annuaire.

Utiliser les groupes globaux comme des groupes d'utilisateurs.

Définir une topologie de groupe globaux sur papier. Elle doit correspondre à la structure administrative de l'entreprise. Un groupe par sous-services par exemple...

Pas plus de 5 niveaux d'encapsulation (pour des raisons de performance).

Convenir avec la direction d'une convention de nommage.

## **Pour gérer les accès à une ressource :**

L'administration des accès doit se faire depuis la console *Utilisateurs et Ordinateurs du domaine* ou *Centre d'administration Active Directory*.

Créer 3 groupes locaux de domaine, un pour l'accès en lecture, un pour l'accès en lecture et écriture (Modifier), un pour l'accès en Contrôle Totale.

Définir les permissions à ces 3 groupes au niveau de la ressource (onglet Sécurité).

Ajouter « *Contrôle Total* » aux groupes SYSTEM et au groupe Administrateurs.

Créer vos groupes d'utilisateurs (groupes globaux).

Pour définir des accès à la ressource, ajouter des groupes globaux ou des comptes utilisateur / ordinateur en tant que membres des groupes locaux de domaine.

# TP : Gestion accès avec les groupes 1/2

Créer 3 dossiers imbriqués les uns dans les autres (Niveau1, Niveau 2 et Niveau 3).

Désactiver l'héritage au niveau du dossier Niveau 1.

Partager Niveau 1 (contrôle Total pour tout le monde).

Sécuriser le répertoire Niveau 1 selon les Best Practice (utiliser les groupes locaux de domaine pour définir des permissions). Création groupes *GDL\_Niveau1\_L*, *GDL\_Niveau1\_M* et *GDL\_Niveau1\_CT*.

Créer des comptes utilisateurs *compta1* et *compta2* et le groupe globale (*GG\_Comptaabilité*). Ajouté les utilisateurs *compta1* et *compta2* dans ce groupe globale.

Définir des permissions « Modifier » sur le répertoire Niveau1 à l'utilisateur « *Compta1* ».

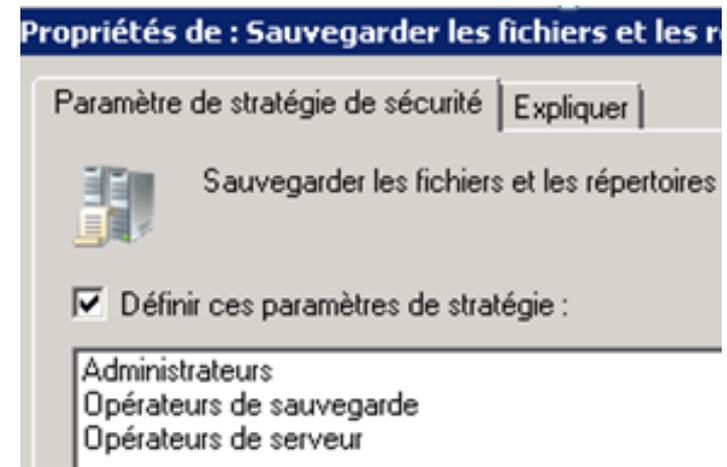
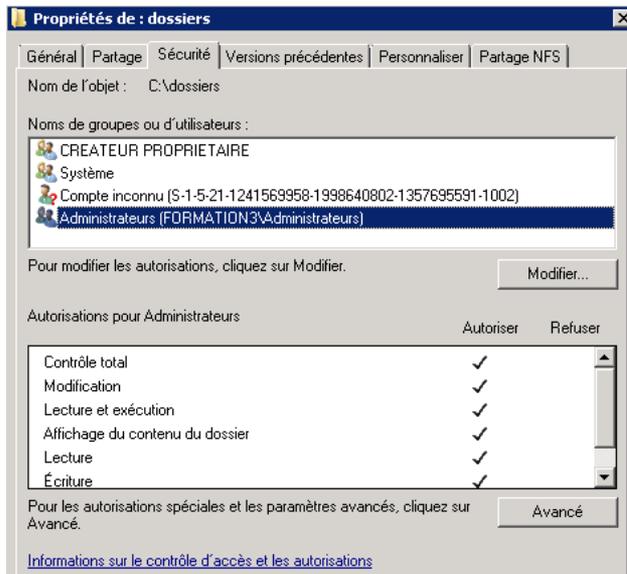
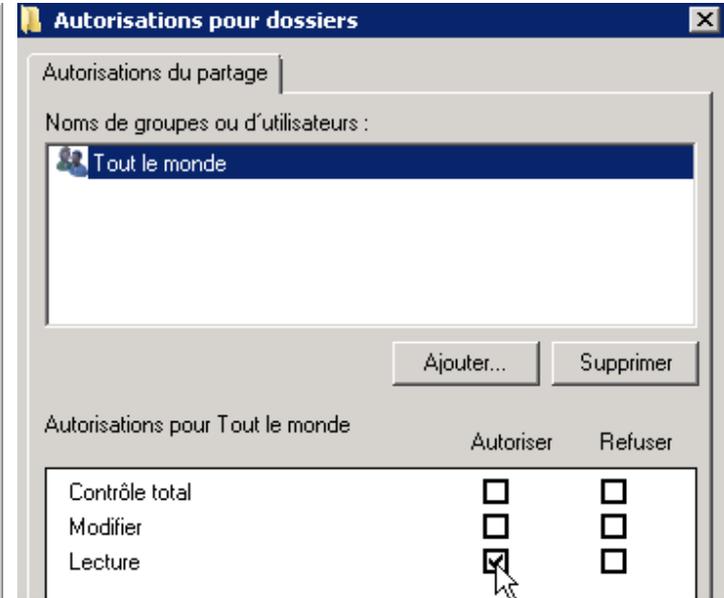
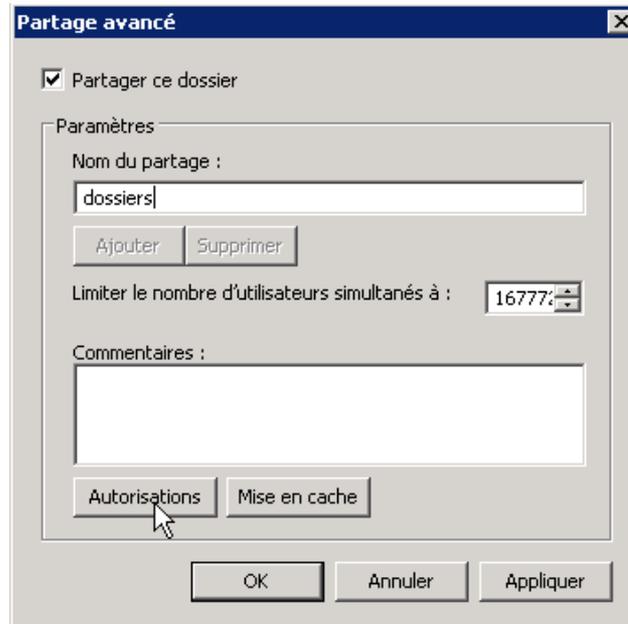
Supprimer le compte *Compta1*. Observer ce qui se passe au niveau des groupes et des permissions de la ressource Niveau1, Niveau 2 et Niveau 3.

Ajouter le groupe *GG\_Comptaabilité* en tant que membre du groupe « *GDL\_Niveau1\_M* ».

Se loguer avec le compte *Compta2* sur une machine membre du domaine et accéder au partage Niveau1.

# TP : Gestion accès avec les groupes 2/2

Peut on sauvegarder un répertoire sur lequel on a pas d'accès. La réponse est oui si on est opérateur de sauvegarde, Opérateur de Server et administrateurs. Voir la capture de droite. Expliquer ?

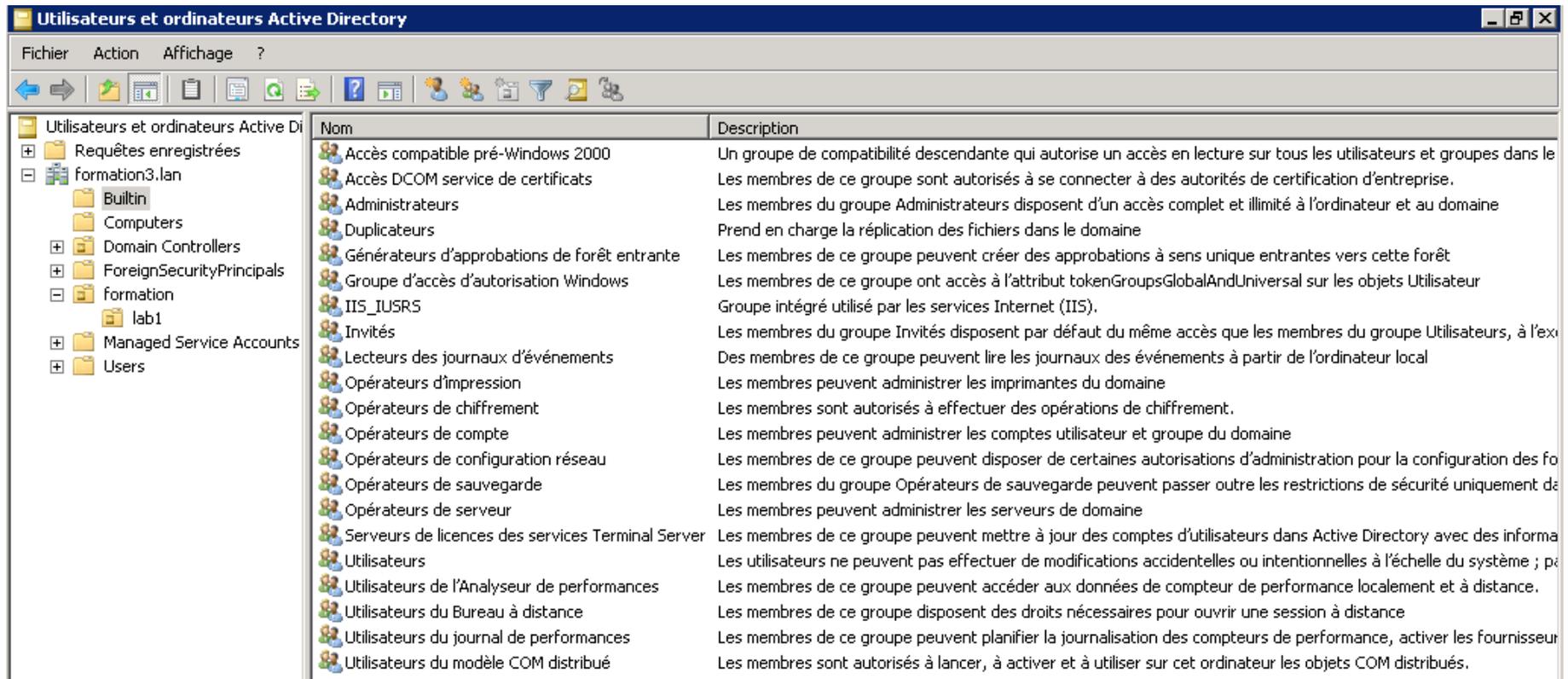


# Les groupes BUILTIN 1/2

Ne pas déplacer.

Equivalent des groupes locaux de domaine.

Ne pas utiliser si possible car on ne peut pas les migrer avec des outils comme ADMT.



The screenshot shows the 'Utilisateurs et ordinateurs Active Directory' console window. The left pane displays a tree view of the Active Directory structure, with the 'Builtin' folder expanded under 'formation3.lan'. The main pane shows a list of built-in groups with their names and descriptions.

Nom	Description
Accès compatible pré-Windows 2000	Un groupe de compatibilité descendante qui autorise un accès en lecture sur tous les utilisateurs et groupes dans le
Accès DCOM service de certificats	Les membres de ce groupe sont autorisés à se connecter à des autorités de certification d'entreprise.
Administrateurs	Les membres du groupe Administrateurs disposent d'un accès complet et illimité à l'ordinateur et au domaine
Duplicateurs	Prend en charge la réplication des fichiers dans le domaine
Générateurs d'approbations de forêt entrante	Les membres de ce groupe peuvent créer des approbations à sens unique entrantes vers cette forêt
Groupe d'accès d'autorisation Windows	Les membres de ce groupe ont accès à l'attribut tokenGroupsGlobalAndUniversal sur les objets Utilisateur
IIS_IUSRS	Groupe intégré utilisé par les services Internet (IIS).
Invités	Les membres du groupe Invités disposent par défaut du même accès que les membres du groupe Utilisateurs, à l'ex
Lecteurs des journaux d'événements	Des membres de ce groupe peuvent lire les journaux des événements à partir de l'ordinateur local
Opérateurs d'impression	Les membres peuvent administrer les imprimantes du domaine
Opérateurs de chiffrement	Les membres sont autorisés à effectuer des opérations de chiffrement.
Opérateurs de compte	Les membres peuvent administrer les comptes utilisateur et groupe du domaine
Opérateurs de configuration réseau	Les membres de ce groupe peuvent disposer de certaines autorisations d'administration pour la configuration des fo
Opérateurs de sauvegarde	Les membres du groupe Opérateurs de sauvegarde peuvent passer outre les restrictions de sécurité uniquement de
Opérateurs de serveur	Les membres peuvent administrer les serveurs de domaine
Serveurs de licences des services Terminal Server	Les membres de ce groupe peuvent mettre à jour des comptes d'utilisateurs dans Active Directory avec des informa
Utilisateurs	Les utilisateurs ne peuvent pas effectuer de modifications accidentelles ou intentionnelles à l'échelle du système ; p
Utilisateurs de l'Analyseur de performances	Les membres de ce groupe peuvent accéder aux données de compteur de performance localement et à distance.
Utilisateurs du Bureau à distance	Les membres de ce groupe disposent des droits nécessaires pour ouvrir une session à distance
Utilisateurs du journal de performances	Les membres de ce groupe peuvent planifier la journalisation des compteurs de performance, activer les fournisseur
Utilisateurs du modèle COM distribué	Les membres sont autorisés à lancer, à activer et à utiliser sur cet ordinateur les objets COM distribués.

# Les groupes BUILTIN 2/2

## Rôle de ces groupes :

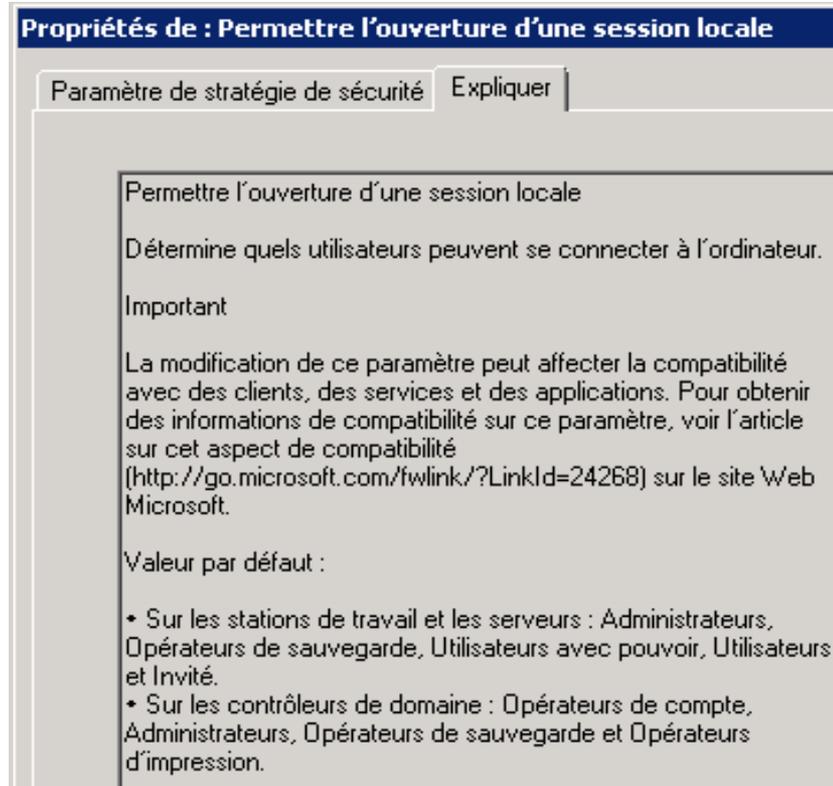
Builtin\Administrateurs : administrateur local sur tous les contrôleurs de domaine. Droits presque équivalents à *Admins du domaine*.

Les membres de ce groupe ne sont pas administrateur local des stations de travail membre du domaine.

- BUILTIN\Duplicateurs
- Builtin\Opérateurs de compte : peut créer des comptes. Peut être utilisé pour faire un premier niveau
- Builtin\Opérateurs de sauvegarde : peut sauvegarder des données même si ce dernier n'a pas d'accès.

- Builtin\Opérateurs de Server : peut effectuer certaines actions au niveau des contrôleurs de domaine comme changer la configuration IP.

**Seul les groupes BUILTIN Opérateurs de sauvegarde, Administrateurs, Opérateurs de comptes et Opérateurs d'impression peuvent ouvrir une session sur un contrôleur de domaine (configurable via GPO).**

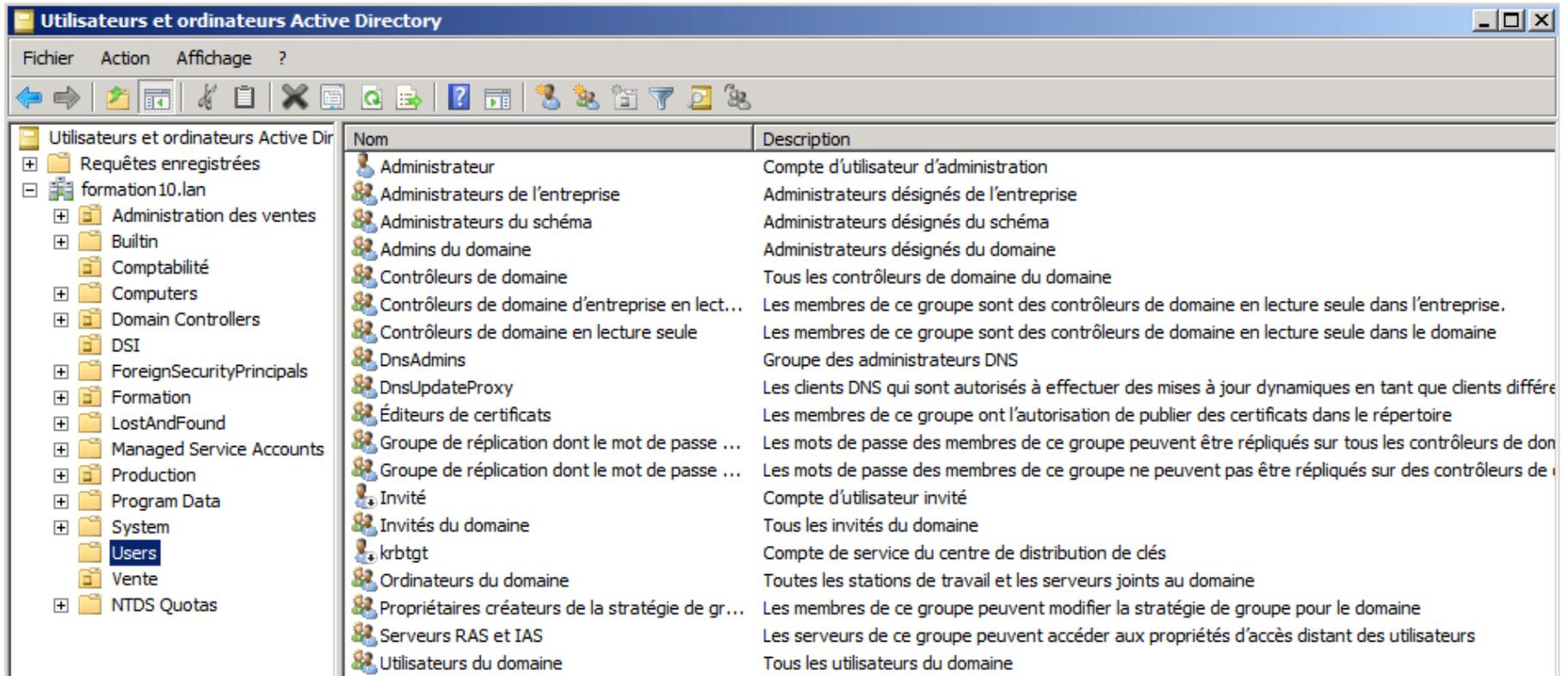


# Les groupes dans conteneur Users :

Admins du domaine : n'a des droits que sur le domaine. Il n'a que des droits partiels sur la partition de configuration. Il est administrateurs de tous les serveurs et stations de travail du domaine.

Administrateur de l'entreprise : administrateur de tous les domaines de la forêt

Administrateur du schéma : seul groupe habilité à modifier le schéma Active Directory



The screenshot shows the 'Utilisateurs et ordinateurs Active Directory' console. The left pane shows the tree structure with 'Users' selected. The right pane displays a table of users and groups with their names and descriptions.

Nom	Description
Administrateur	Compte d'utilisateur d'administration
Administrateurs de l'entreprise	Administrateurs désignés de l'entreprise
Administrateurs du schéma	Administrateurs désignés du schéma
Admins du domaine	Administrateurs désignés du domaine
Contrôleurs de domaine	Tous les contrôleurs de domaine du domaine
Contrôleurs de domaine d'entreprise en lect...	Les membres de ce groupe sont des contrôleurs de domaine en lecture seule dans l'entreprise.
Contrôleurs de domaine en lecture seule	Les membres de ce groupe sont des contrôleurs de domaine en lecture seule dans le domaine
DnsAdmins	Groupe des administrateurs DNS
DnsUpdateProxy	Les clients DNS qui sont autorisés à effectuer des mises à jour dynamiques en tant que clients différés
Éditeurs de certificats	Les membres de ce groupe ont l'autorisation de publier des certificats dans le répertoire
Groupe de réplication dont le mot de passe ...	Les mots de passe des membres de ce groupe peuvent être répliqués sur tous les contrôleurs de domaine
Groupe de réplication dont le mot de passe ...	Les mots de passe des membres de ce groupe ne peuvent pas être répliqués sur des contrôleurs de domaine
Invité	Compte d'utilisateur invité
Invités du domaine	Tous les invités du domaine
krbtgt	Compte de service du centre de distribution de clés
Ordinateurs du domaine	Toutes les stations de travail et les serveurs joints au domaine
Propriétaires créateurs de la stratégie de gr...	Les membres de ce groupe peuvent modifier la stratégie de groupe pour le domaine
Serveurs RAS et IAS	Les serveurs de ce groupe peuvent accéder aux propriétés d'accès distant des utilisateurs
Utilisateurs du domaine	Tous les utilisateurs du domaine

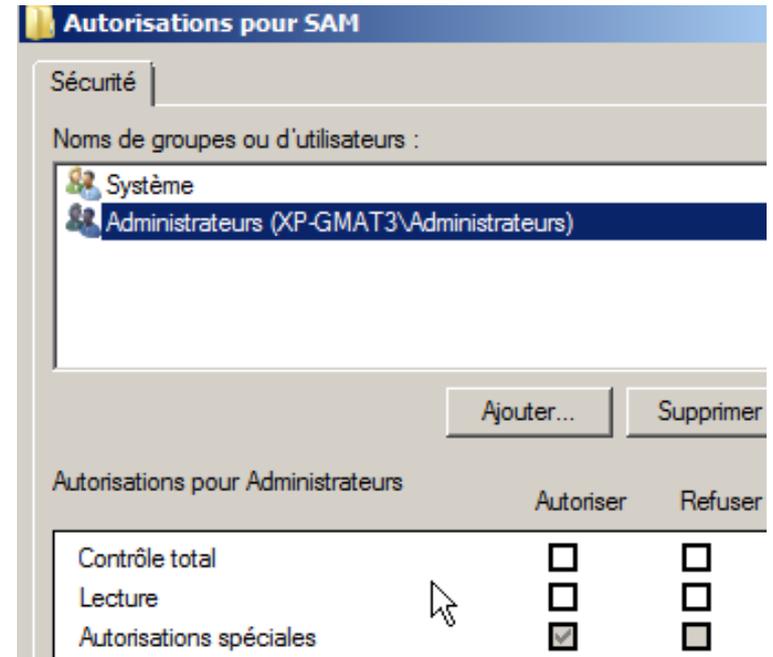
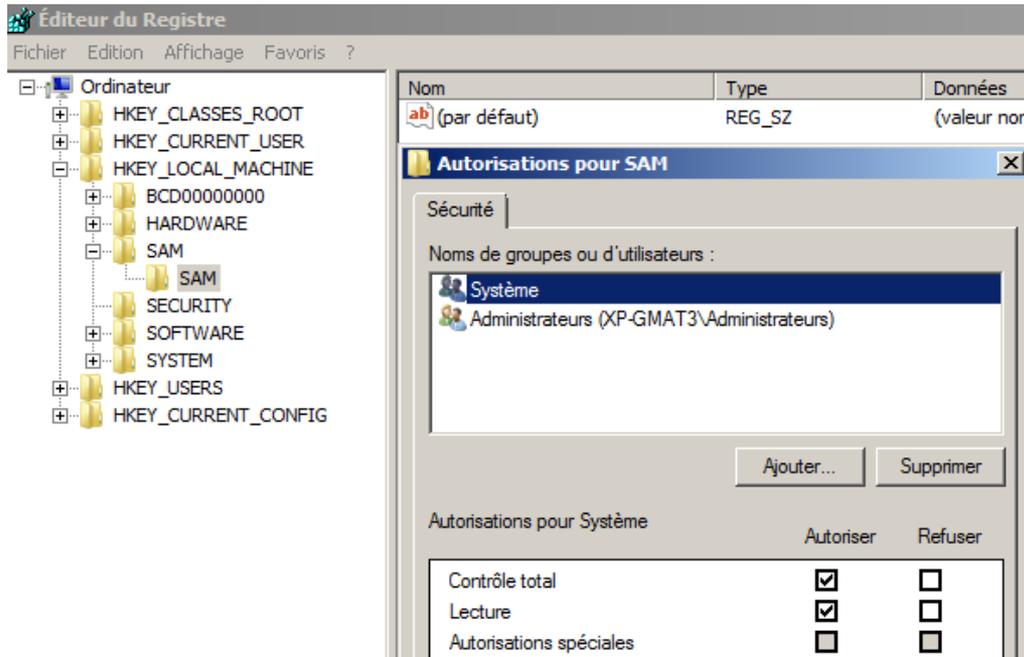
# Les entités système

Tout le monde : tout le monde.

Utilisateurs authentifiés : tout ordinateur ou tout utilisateurs qui a ouvert une session est membre du groupe « *utilisateurs authentifiés* ». Groupe avec privilège important comme créer des dossiers / fichiers sur la partition C des serveurs.

Créateur propriétaire : par défaut le créateur d'un fichier et d'un dossier est le propriétaire. Il a le droit de modifier les permissions.

System : droit presque équivalent à administrateur local. C'est par exemple le seul à pouvoir modifier le contenu de la base SAM dans la base de registre.



# 6. Les unités d'organisation

# Présentation générale des OU 1/2

OU = unité d'organisation

C'est un conteneur (rien à voir avec les groupes).

On peut créer dans une OU tout type d'objet dont d'autres OU.

La topologie d'unités d'organisation doit correspondre à l'organisation administrative de l'entreprise. Elle est à faire sur papier et doit être validée par la direction.

Les OU permettent aussi de faire de la délégation d'administration et de créer des GPO.

Depuis Windows 2008, la console « *Gestion des stratégies de groupe* » est installé par défaut. On ne peut donc plus créer d'objets stratégies de groupe depuis la console « *Utilisateurs et Ordinateurs Active Directory* ».

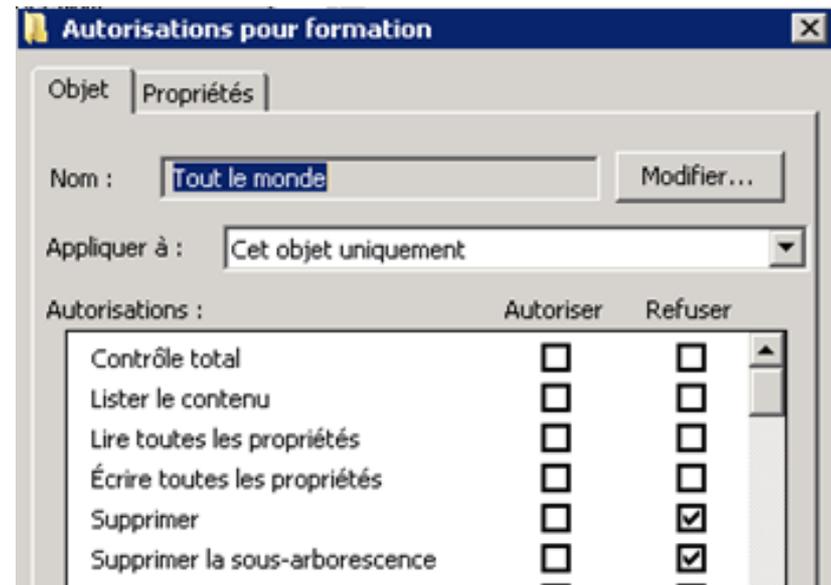
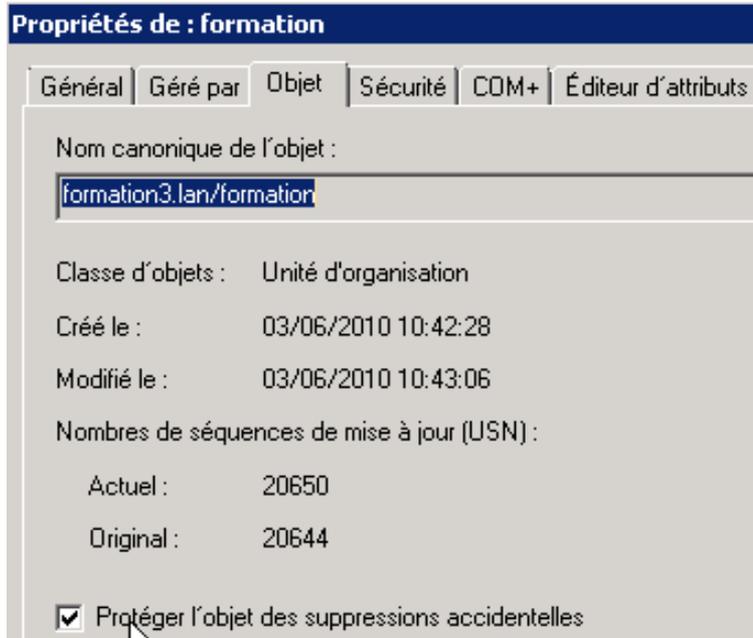
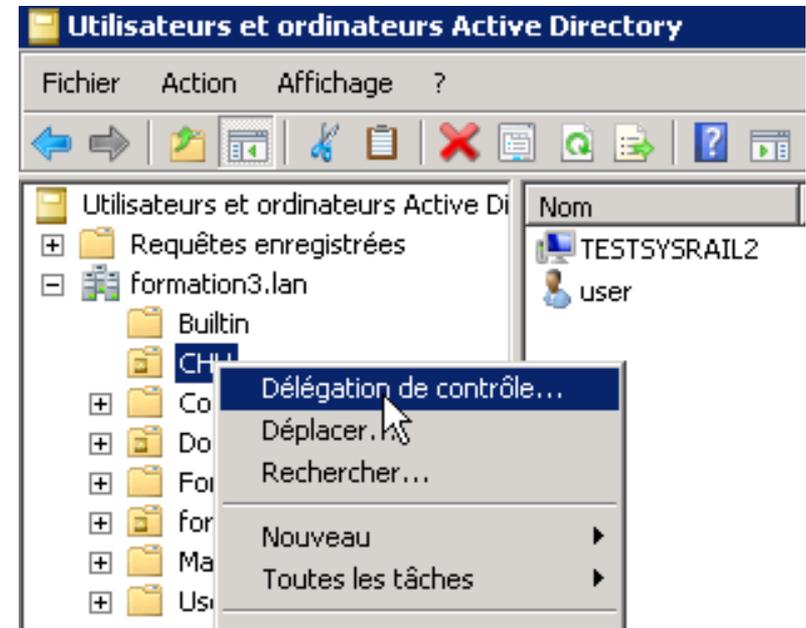
## **Nouveauté sur les contrôleurs de domaine :**

Quand on crée une nouvelle OU sur un DC 2008 / 2008, par défaut la protection renforcée contre la suppression accidentelle est activée. Cette protection met des permissions « Refusé » à Tout le monde pour la suppression d'objet.

Si on essaie de déplacer ou supprimer une OU, on a donc un message « *Accès Refusé* ».

Passer en mode d'affichage « *Fonctionnalités avancées* » pour cocher ou décocher cette case.

# Présentation générale des OU 2/2



# TP : délégation d'administration 1/4

Il est possible de déléguer des droits au niveau de chaque attribut (chaque champ) pour chaque type d'objet.

**Méthode 1** : utilisateurs membres d'*Opérateur de Comptes*. Ces comptes utilisateur peuvent créer des groupes / comptes utilisateur / ordinateur dans l'AD.

**Méthode 2** : Utilisateur l'assistant « *Délégation d'administration* » en mode basique. Cette méthode permet de déléguer des tâches basiques au niveau d'un OU particulière. Il n'est pas possible de déléguer les droits pour un ou plusieurs attributs.

**Méthode 3** : Utiliser l'assistant Délégation en mode avancé « *Créer une tâche personnalisée à déléguer* ». Cette méthode permet de déléguer la gestion de certains attributs pour certains types d'objets.

**Méthode 4** : lancer la console « *Utilisateurs et Ordinateurs Active Directory* » en mode d'affichage « *Fonctionnalités avancées* ». Aller au niveau d'une OU, cliquer sur « *Propriétés* » et aller dans l'onglet « *Sécurité* » puis passer en mode *Advanced*.

Microsoft propose maintenant une méthode appelée Tier 0, Tier 1 et Tier 2 pour déléguer l'administration Active Directory. L'idée principale est de séparer l'administration du service Active Directory (Tier 0), l'administration des serveurs (Tier 1) et l'administration des stations de travail et des comptes standards (Tier 2).

<https://www.petri.com/keep-active-directory-secure-using-privileged-access-workstations>  
<https://social.technet.microsoft.com/wiki/contents/articles/37509.active-directory-red-forest-design-aka-enhanced-security-administrative-environment-esae.aspx>

# TP : délégation d'administration 2/4

Créer une OU appelée Msreport1.

Créer un compte utilisateur dans cette OU appelé *admin1\_msreport*.

Faire un clic droit au niveau de l'OU CHU et cliquer « *Délégation de contrôle* ».

Ajouter le utilisateur ou le groupe à qui vous souhaitez déléguer des droits d'administration.

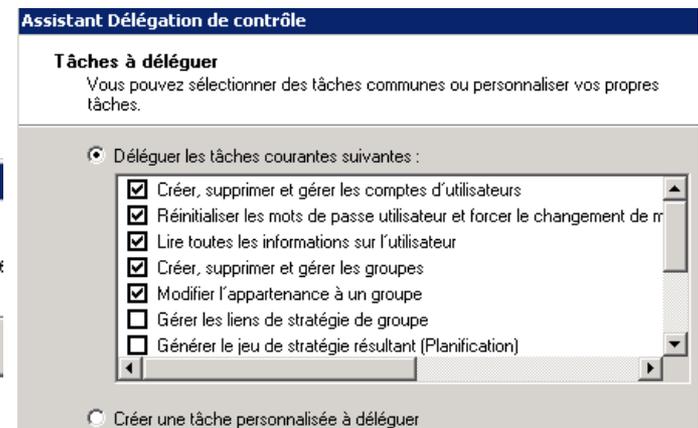
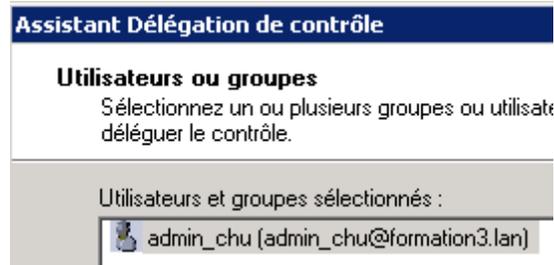
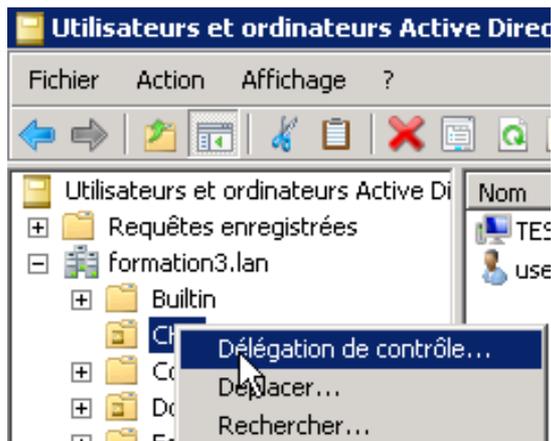
Sélectionner le ou les droits à déléguer.

Se loguer sur une station de travail membre du domaine avec le compte *admin1\_msreport*.

Installer les outils d'administration (RSAT) sur la station d'administration

<https://www.microsoft.com/en-us/download/details.aspx?id=45520>

Tester la création d'un compte utilisateur.



# TP : délégation d'administration 3/4

Créer une OU appelée MSREPORT2.

Créer un compte utilisateur dans cette OU appelé *admin2\_msreport*.

Clic droit sur l'OU CHU et cliquer « *Délégation de contrôle* ».

Ajouter le utilisateur ou le groupe à qui vous souhaitez déléguer des droits d'administration.

Sélectionner « *Créer une tâche d'administration personnalisée à déléguer* ».

Sélectionner « *Seulement les objets suivants dans le dossier* ».

Cocher les cases « *Créer et supprimer des objets* ».

Sélectionner « *générales* » dans la fenêtre « *Afficher les autorisations* ».

Si vous souhaitez déléguer l'accès en écriture que pour certains attributs, cocher la case « *Spécifique aux propriétés* ».

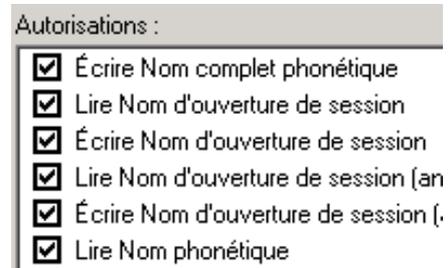
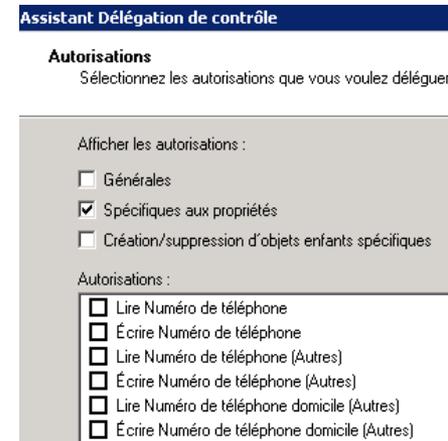
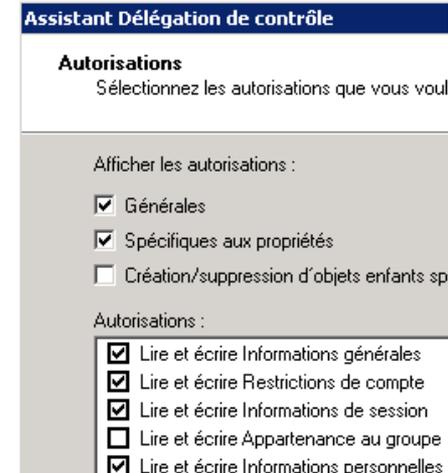
Sélectionner les propriétés de votre choix.

Se loguer sur une station de travail membre du domaine avec le compte *admin2\_msreport*.

Installer les outils d'administration (RSAT) sur la station d'administration

<https://www.microsoft.com/en-us/download/details.aspx?id=45520>

Tester la création d'un compte utilisateur.





# 7. Les stratégies de groupe

# La base de registre 1/2

**La base de registre est la base de configuration de Windows.**

Pour éditer la base de registre, on utilise REGEDIT ou REGEDT32 (c'est le même exécutable depuis Windows XP).

Ruche : ensemble de clés et de valeurs qui correspondent à un fichier au niveau du système.

Clés : c'est un conteneur de valeur.

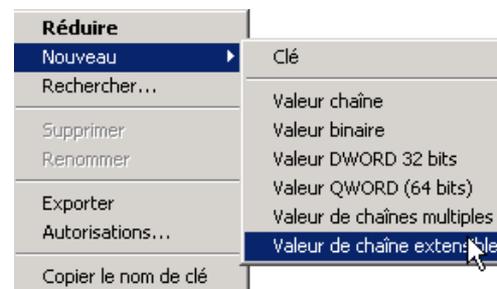
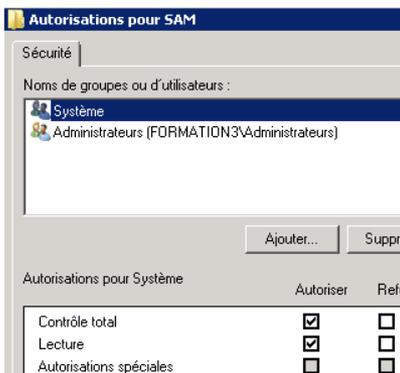
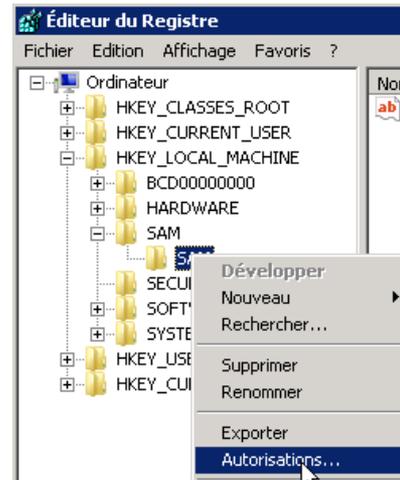
Valeur : variable. Il existe différents types de valeur (binaire, chaîne de caractères, tableaux de chaînes de caractères...).

La base de registre est organisée en deux grandes sections *HKEY LOCAL MACHINE* et *HKEY USERS*.

La ruche *HKEY\_CURRENT\_CONFIG* est une sous ruche de *HKEY\_LOCAL\_MACHINE*

Il est possible de charger des ruches (fichier *NTUSER.DAT* d'un autre utilisateur...).

Il est possible de définir des permissions au niveau des clés de registre



Autorisations pour Système		
	Autoriser	Refu
Contrôle total	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Lecture	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Autorisations spéciales	<input type="checkbox"/>	<input type="checkbox"/>

# La base de registre 2/2

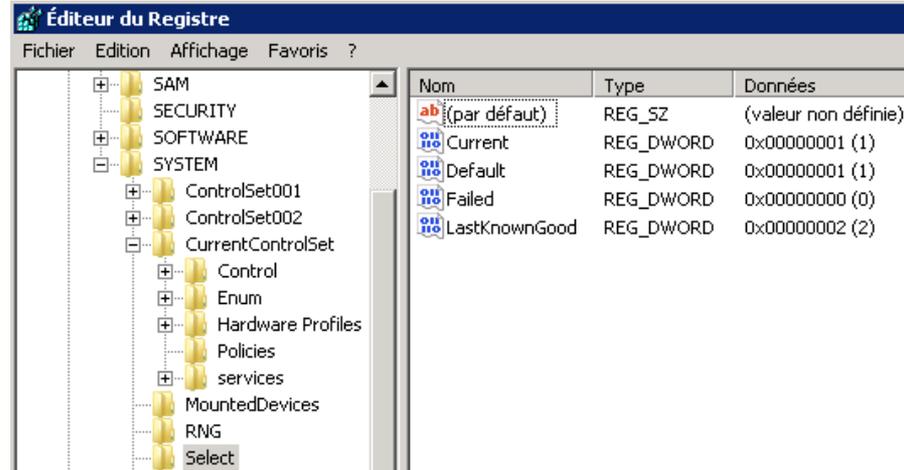
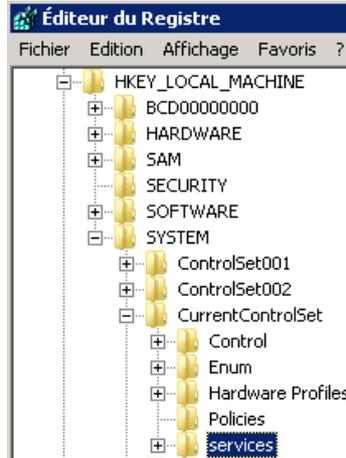
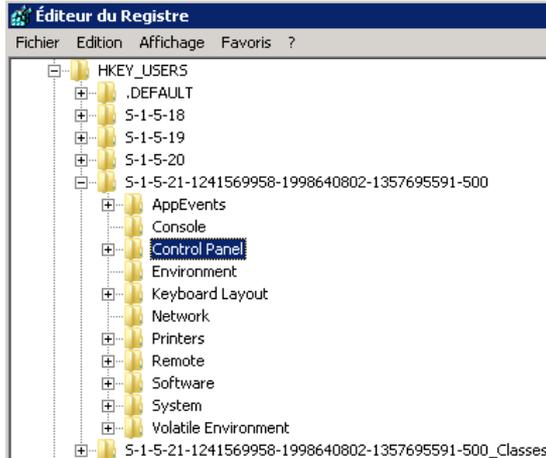
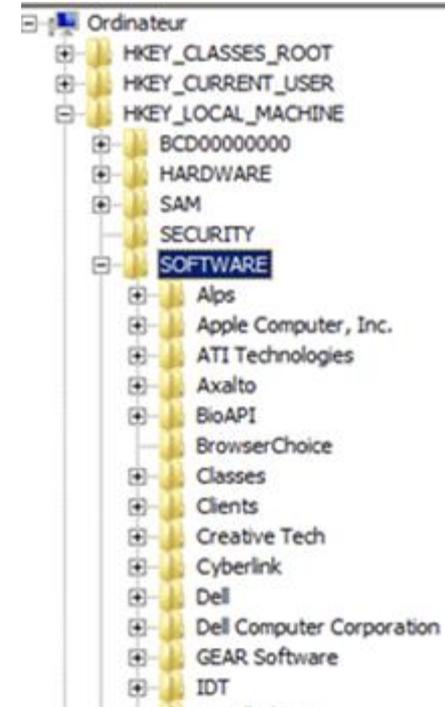
Les paramètres de *HKEY\_USERS* correspondent à la configuration spécifique au niveau des utilisateurs.

Les paramètres de *HKEY\_LOCAL\_MACHINE* correspondent à la configuration de la machine (commune pour tous les utilisateurs).

Dans *HKEY\_LOCAL\_MACHINE | SYSTEM | CurrentControlSet | Services*, on retrouve la configuration des services.

Dans *HKEY\_LOCAL\_MACHINE | SOFTWARE*, on retrouve la configuration des logiciels commun à tous les utilisateurs.

Dans *HKEY\_USERS | SOFTWARE*, on retrouve la configuration des logiciels commun spécifique à un utilisateur.



# TP : base de registre

Sur une station de travail Windows XP Pro, lancer l'éditeur de base de registre.

Aller dans HKEY\_LOCAL\_MACHINE | SAM | SAM.

Faire un clic droit sur le dossier SAM et cliquer sur « *Autorisation* ».

Ajouter les droits *Control Total* au groupe *Administrateurs* de la base SAM locale.

Vous pouvez maintenant visualiser le contenu de la base SAM locale.

Créer un compte utilisateur appelé « *testregistre* » au niveau du domaine et se loguer avec ce compte sur la station de travail. Personnaliser puis fermer la session (ajout imprimante réseau...).

Ouvrir une session avec le compte administrateur local sur cette station de travail.

Lancer l'éditeur de base de registre.

Sélectionner « *HKEY\_USERS* » puis aller dans le menu « *Fichier* » et cliquer sur « *Charger la ruche* ». Aller dans « *c:\Documents and settings\testregistre* » et sélectionner le fichier « *NTUSER.DAT* ». A quoi correspond ce fichier ?

Faire une recherche au niveau de « *HKEY\_LOCAL\_MACHINE* » sur la clé « *PROFILEIMAGEPATH* ». A quoi sert cette clé. On se rend compte que toute la sécurité est basé sur le SID. Il est possible de réassocier un compte utilisateur avec le profil d'un autre utilisateur. Pour plus d'informations, voir <http://msreport.free.fr>.

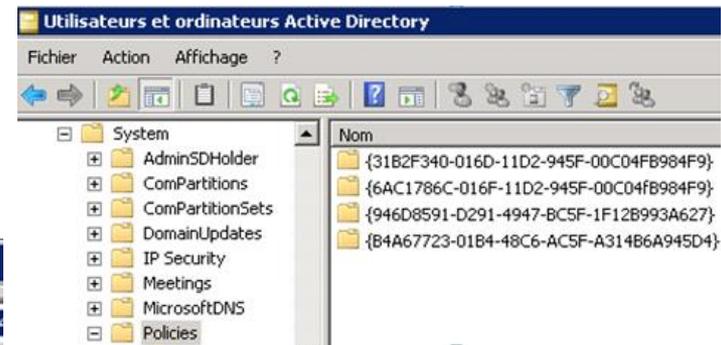
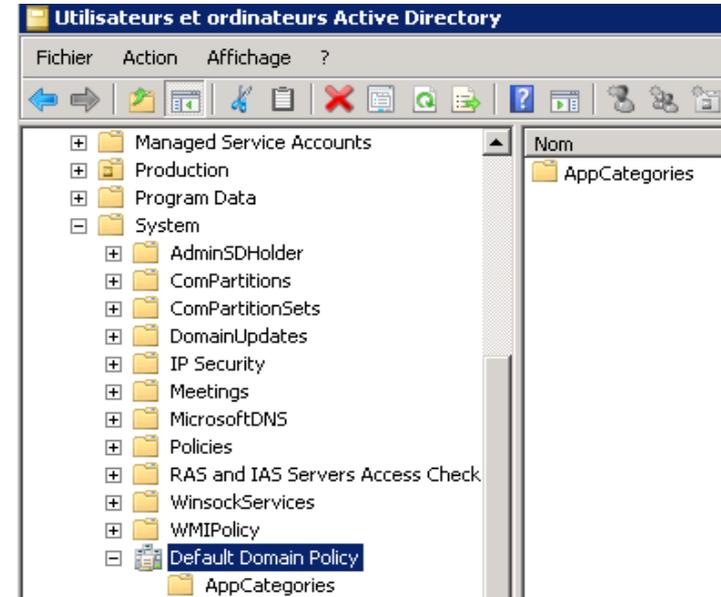
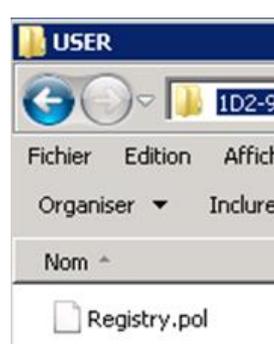
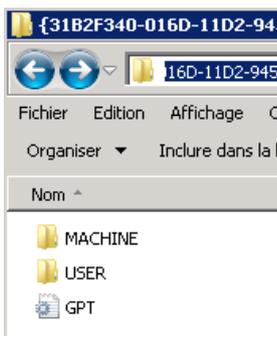
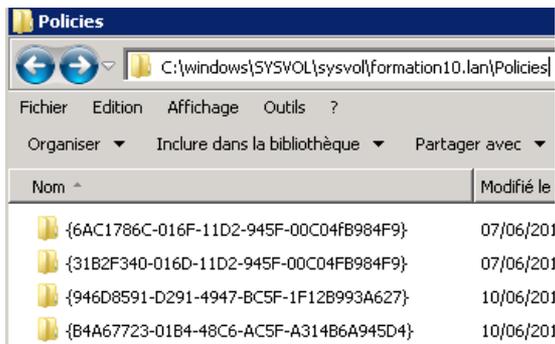
Aller dans *c:\windows\system32\config*. On y retrouve tous les fichiers des ruches de la base de registre.

# Qu'est ce qu'une stratégie de groupe ?

Les stratégies de groupes (GPO) : se sont des clés et valeurs de registre.

Deux sections pour les stratégies de groupe : *Configuration ordinateur* (modifie HKEY\_LOCAL\_MACHINE) et *Configuration utilisateur* (modifie HKEY\_USERS).

Les stratégies de groupe se décomposent en deux composants, les fichiers de stratégie de groupe (dans le répertoire SYSVOL\SYSVOL\nomdomainedns\Policies), un objet stratégie de groupe (dans le conteneur SYSTEM au niveau de la partition de domaine).



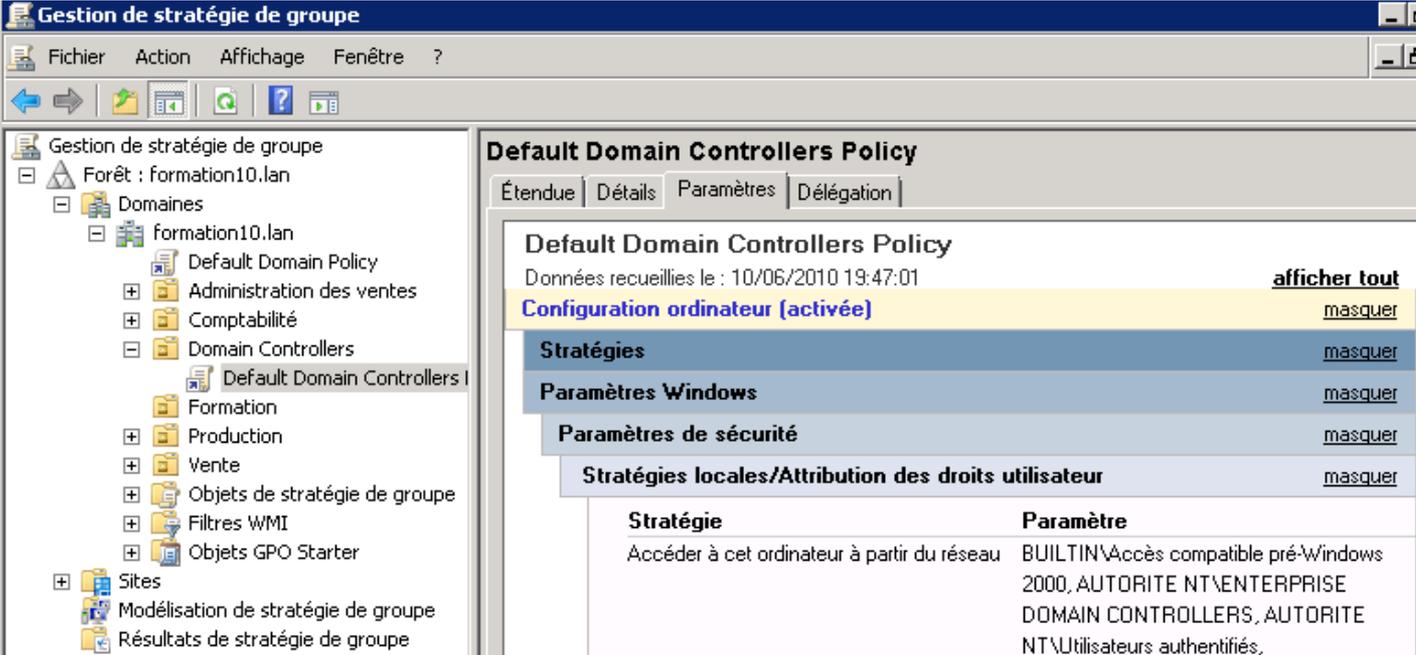
# Présentation de la console GPMC

La console *Gestion des stratégies de groupe* : permet d'ajouter, lier, modifier et supprimer les GPO.

Il est possible d'ajouter de créer des stratégies de groupes personnalisées (fichier ADM ou ADMX).

A la création du domaine, deux GPO, la « *Default Domain Policy* » (configuration du domaine ) et la *Default Domain Controller Policy* (configurer des DC). **Ne pas supprimer ces deux GPO. Eviter de les modifier.**

Possibilité d'exporter / importer des GPO via GPMC.



The screenshot displays the Group Policy Management Console (GPMC) interface. The left pane shows the tree structure of the Group Policy Objects (GPOs) for the domain 'formation10.lan'. The right pane shows the configuration details for the 'Default Domain Controllers Policy', which is currently active. The configuration is organized into sections: 'Configuration ordinateur (activée)', 'Stratégies', 'Paramètres Windows', 'Paramètres de sécurité', and 'Stratégies locales/Attribution des droits utilisateur'. A table at the bottom lists the specific policies and their parameters.

Stratégie	Paramètre
Accéder à cet ordinateur à partir du réseau	BUILTIN\Accès compatible pré-Windows 2000, AUTORITE NT\ENTERPRISE DOMAIN CONTROLLERS, AUTORITE NT\Utilisateurs authentifiés,

# Les stratégies de groupe

Déployer des logiciels (installeur au format .MSI obligatoire). Pas de rapport, risque saturation réseau si gros logiciels.

Déposer les exécutables dans le partage NETLOGON ou SYSVOL.

D'exécuter des scripts au démarrage / arrêt de la machine (sous compte SYSTEM).

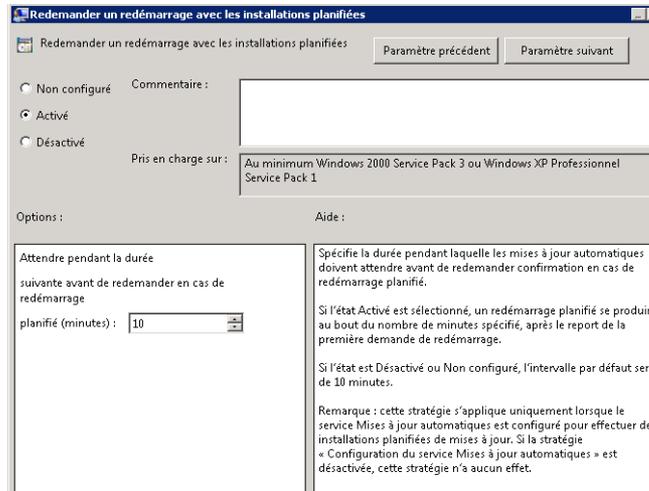
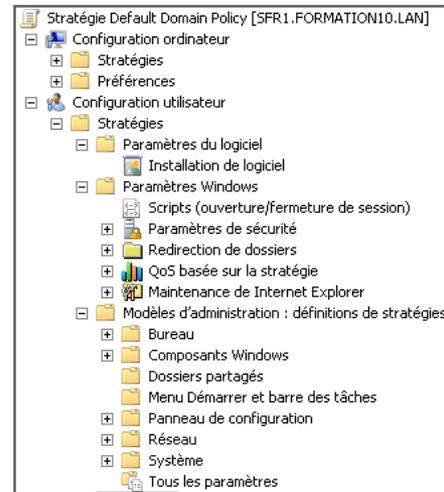
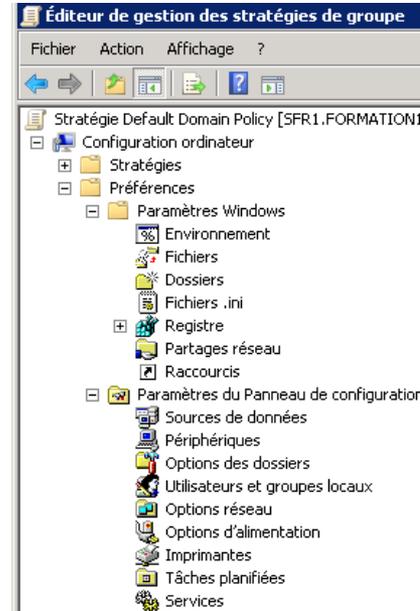
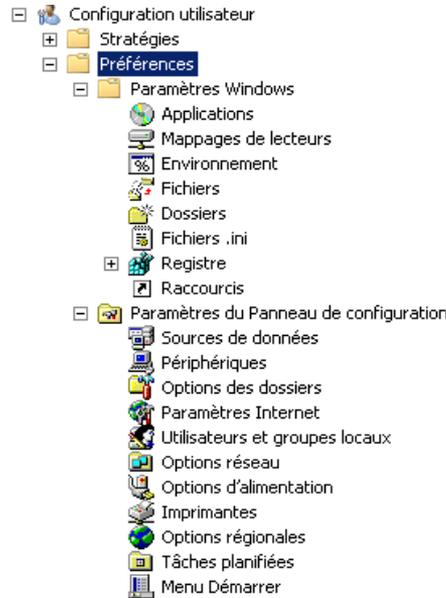
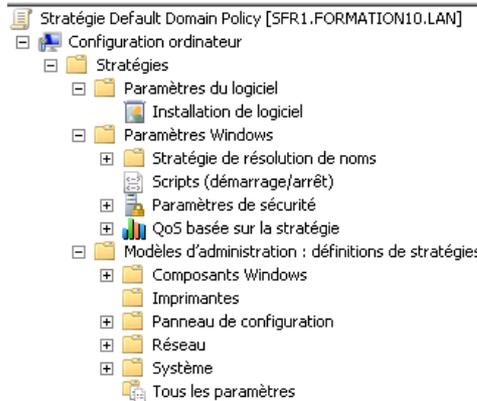
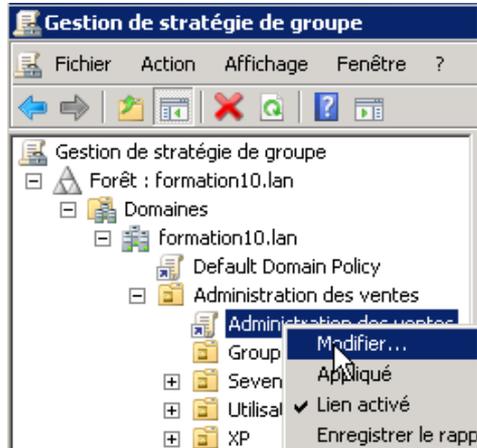
De configurer les stratégies de mots de passe, Kerberos et de verrouillage de comptes. Les paramètres de stratégie de mot de passe pour les comptes du domaine se définissent uniquement au niveau de la « *Default Domain Policy* ». Si on définit ce paramètre dans une autre stratégie, cela s'applique pour les comptes locaux. Voir <http://msreport.free.fr/?p=156>.

De configurer les paramètres et options de sécurité (qui peut ouvrir une session localement, arrêter la machine, accéder à la machine via le réseau, changer l'heure, les protocoles d'authentification autorisés...).

De configurer les paramètres des logiciels et du système (configuration Windows Update, panneau de configuration, pare feu). Il est possible d'ajouter des fichiers ADM / ADMX supplémentaires pour ajouter de nouvelles stratégies (configuration Adobe, Citrix, Office...) : <http://www.microsoft.com/downloads/details.aspx?familyid=92d8519a-e143-4aee-8f7a-e4bbaeba13e7&displaylang=en>

Depuis Windows 2008, L inclut GPO de préférences. Nécessite déploiement d'un correctif sur Windows XP / Vista / 2003. Voir <http://support.microsoft.com/kb/943729/en-us>

# Les paramètres de stratégie de groupe

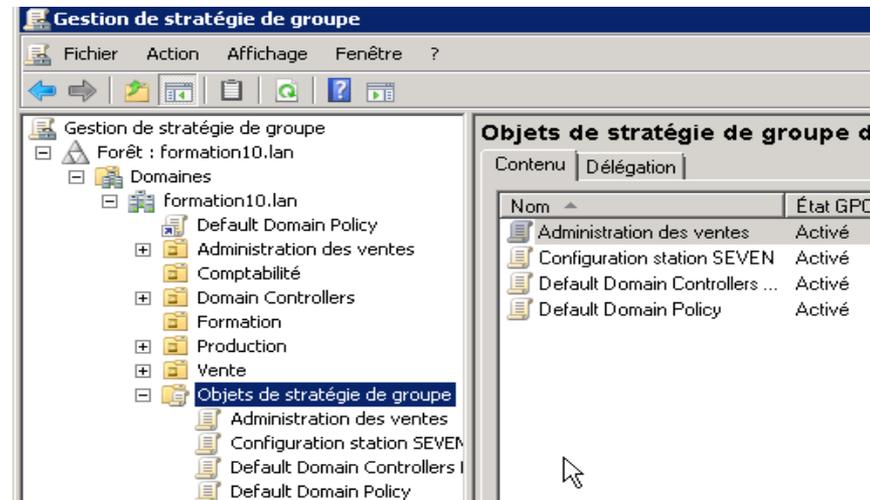
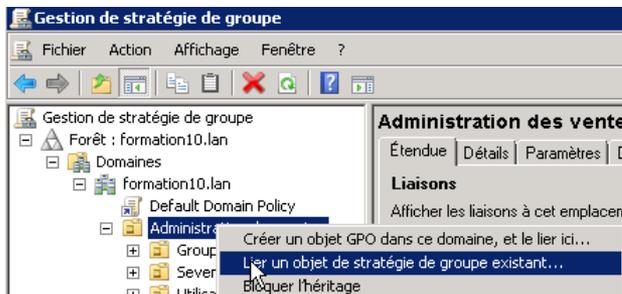
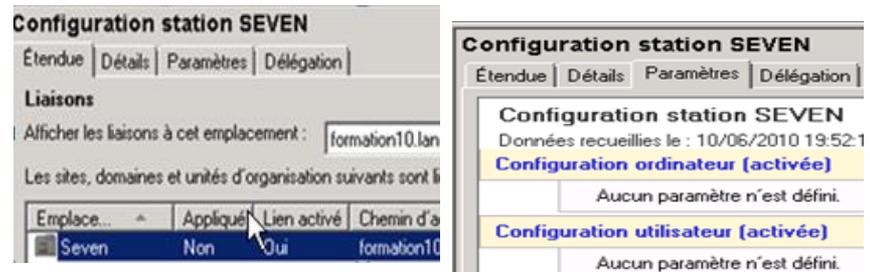
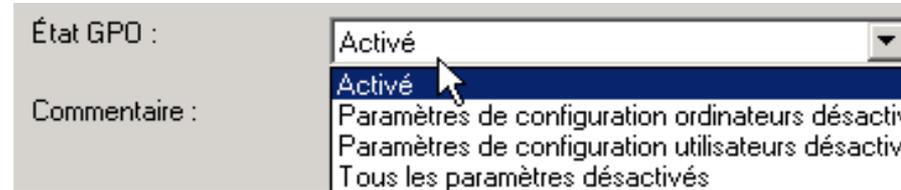


# Comment s'appliquent les GPO ?

Une GPO « *Configuration Ordinateur* » s'applique à une machine (si compte ordinateur est dans OU où est liée la GPO et si le compte ordinateur a les droits « *Lire* » et « *Appliquer la stratégie de groupe* »).

Une GPO « *Configuration Utilisateur* » s'applique aux utilisateurs (si compte utilisateur est dans OU où est liée la GPO et si le compte utilisateur a les droits « *Lire* » et « *Appliquer la stratégie de groupe* »).

Par défaut « *Utilisateurs authentifiés* » (toutes les comptes ordinateurs et utilisateurs qui ont ouvert une session) a les droits « *Lire* » et « *Appliquer la stratégie de groupe* ». Possibilité filtrage en supprimant cet entité de sécurité.



# Ordre d'application des GPO

Possibilité de fixer des GPO avec des paramètres contradictoires à différents niveaux.

Pour gérer les conflits, les GPO s'appliquent dans un certains ordre :

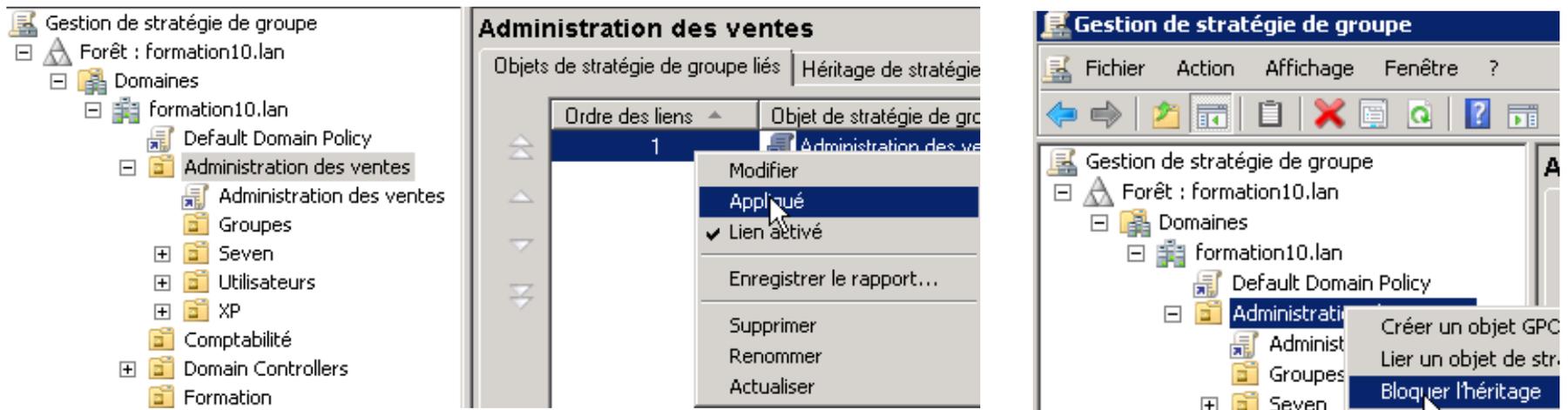
*Local, Site, Domaine, unités d'organisation, unités d'organisation enfant*

En cas de conflit c'est la dernière stratégie qui s'applique qui l'emporte sauf si les paramètres « *Appliquer* » (ne pas passer outre) et « *Bloquer l'héritage* » ont été définis.

Paramètre « *Appliquer* » : force l'application de la GPO.

Paramètre « *Bloquer l'héritage* » : si ce paramètre est fixé au niveau d'une OU enfant, les GPO au niveau des sites, domaines et des OU parent ne s'appliquent pas (sauf les paramètres de sécurité).

Le paramètre « *Appliquer* » prime sur le paramètre « *Bloquer l'héritage* ».



# Les stratégies de mots de passe 1/2

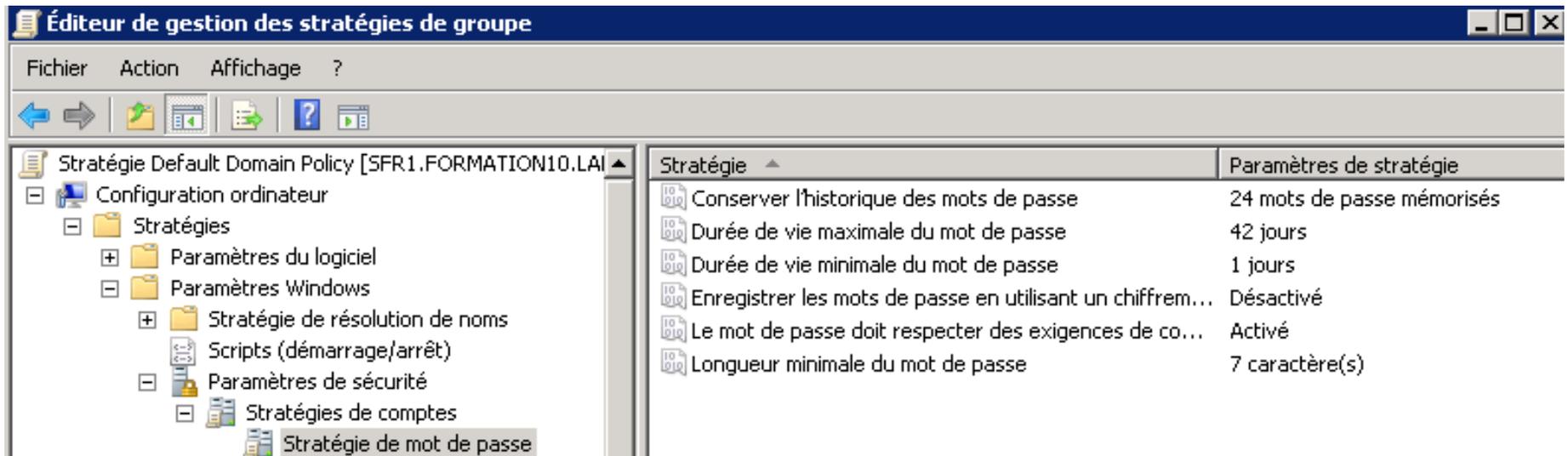
Paramètres de stratégies de mots de passe : configurable au niveau de la stratégie « *Default Domain Policy* ».

Utiliser les *Fine Grained Password Policy / Granular Password Policy* pour créer des stratégies de mots de passe spécifiques pour un groupe d'utilisateurs :

Permet d'attribuer une stratégie de mots de passe à un compte utilisateur ou à un groupe.

Nécessite domaine en mode Fonctionnalité Windows 2008.

[http://technet.microsoft.com/en-us/library/cc770394\(W.S.10\).aspx](http://technet.microsoft.com/en-us/library/cc770394(W.S.10).aspx)



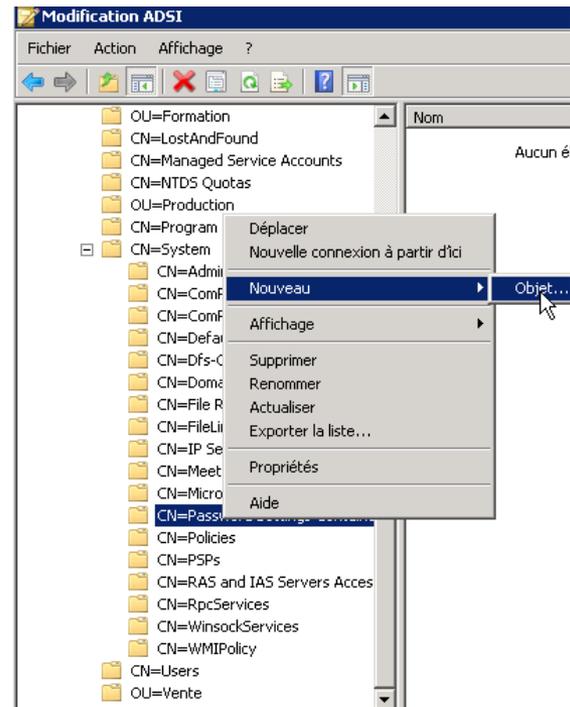
The screenshot shows the Group Policy Editor window titled "Éditeur de gestion des stratégies de groupe". The left pane displays a tree view of the Group Policy Objects (GPOs) for the domain "SFR1.FORMATION10.LAI". The "Stratégies" folder is expanded, showing "Stratégie de mot de passe" selected. The right pane displays the configuration for the "Stratégie" selected, with the following parameters:

Stratégie	Paramètres de stratégie
Conservé l'historique des mots de passe	24 mots de passe mémorisés
Durée de vie maximale du mot de passe	42 jours
Durée de vie minimale du mot de passe	1 jours
Enregistrer les mots de passe en utilisant un chiffrem...	Désactivé
Le mot de passe doit respecter des exigences de co...	Activé
Longueur minimale du mot de passe	7 caractère(s)

# Les stratégies de mots de passe 2/2

Attribute	Value	Quick explanation
Cn	PassPolAdmins	This is the name of the policy. Try to come up with a naming convention for these policies if you will have lots of them.
msDS-PasswordSettingsPrecedence	10	This number is used as a 'cost' for priority between different policies in case a user is hit by multiple PSOs. Be sure to leave space below and above for future use. The stronger the PSO password settings are, the lower the 'cost' should be.
msDS-PasswordReversibleEncryptionEnabled	False	Boolean value to select if passwords should be stored with reversible encryption (usually not a good idea).
msDS-PasswordHistoryLength	32	How many previously used passwords should the system remember?
msDS-PasswordComplexityEnabled	True	Should the users use a complex password? (Boolean value)
msDS-MinimumPasswordLength	16	What should be the minimum number of characters in the user accounts password?
msDS-MinimumPasswordAge	-864000000000 (9 zeros)	What is the minimum password age? (in this case 1 day) NB! Minus sign
msDS-MaximumPasswordAge	-3628800000000 (9 zeros)	What is the maximum password age? (in this case 42 days) NB! Minus sign

msDS-LockoutTreshhold	30	How many failed attempts before the user account will be locked?
msDS-LockoutObservationWindow	-18000000000 (9zeros)	After how long should the counter for failed attempts be reset? (in this case 6 minutes) NB! Minus sign
msDS-LockoutDuration	-18000000000 (9zeros)	For how long should the user account object be locked in case of too many bad passwords entered? (in this case 6 minutes) NB! Minus sign



# Bloquer les applications non autorisées

Permet de définir quels sont les applications que l'on peut exécuter sur une station de travail.

APPLOCKER ne fonctionne qu'avec Windows Seven ou Windows 2008 R2.

Utiliser le mode d'inventaire avant de mettre des stratégies restrictives.

[http://technet.microsoft.com/fr-fr/library/ee424367\(WS.10\).aspx](http://technet.microsoft.com/fr-fr/library/ee424367(WS.10).aspx)

# Dépannage des stratégies de groupes 1/2

Utiliser l'outil GPRESULT ou le composant logiciel enfichable « *Jeu de stratégies résultants* » pour déterminer quels sont les paramètres de stratégies de groupe qui s'appliquent.

Toujours consulter l'onglet « *Aide* » au niveau d'un paramètre de stratégie de groupe (désactiver une stratégie qui masque le panneau de configuration active le panneau de configuration...).

Pour les scripts de déploiement réseau, configurer la stratégie « *Ouverture de session : attendre les connexions réseau* » pour forcer l'application des scripts de démarrage avant l'ouverture de session.

<http://support.microsoft.com/kb/887303>

<http://technet.microsoft.com/en-us/library/bb727058.aspx>

<http://support.microsoft.com/kb/555982/en-us>

Pour bloquer l'application des stratégies pour les administrateurs : supprimer l'entité « *Utilisateurs authentifiés* » et ajouter les droits lire et appliquer la stratégie à des groupes utilisateurs et des groupes d'ordinateurs. Pour plus d'informations, voir <http://support.microsoft.com/kb/816100/en-us>

En cas de suppression des stratégies *Default Domain Policy* et *Default Domain Controller Policy*, appliquer l'article : <http://support.microsoft.com/kb/555647/en-us>

Pour réinitialiser stratégie sécurités :

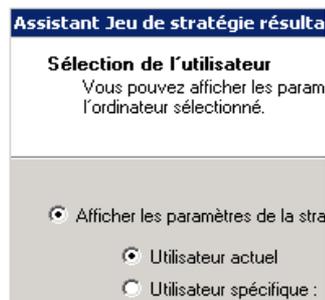
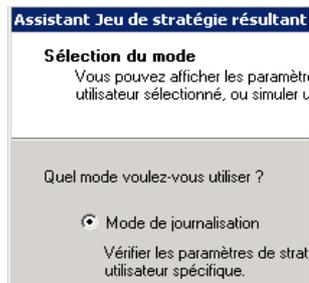
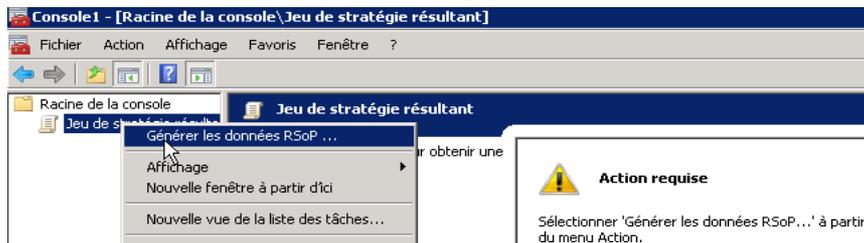
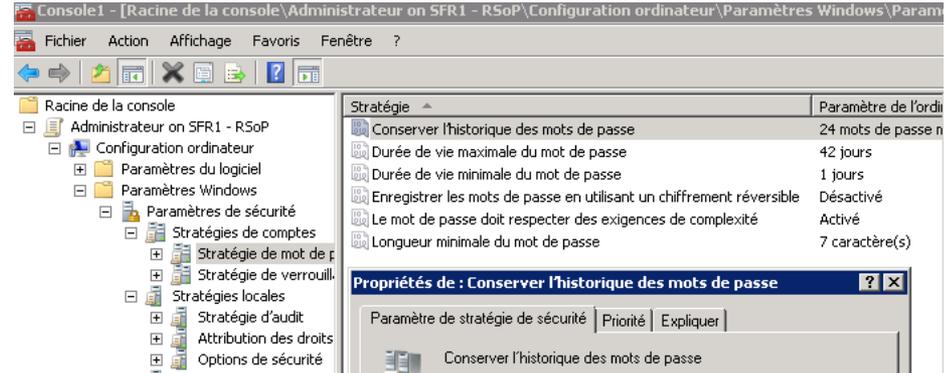
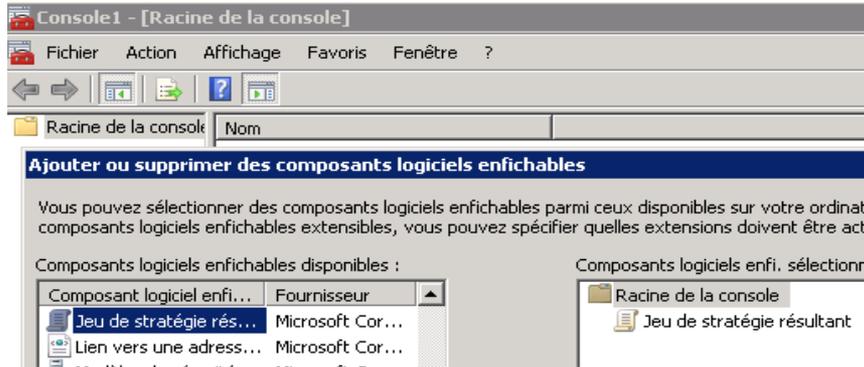
<http://support.microsoft.com/kb/324800/en-us>

# Dépannage des stratégies de groupes 2/2

Bug GPRESULT : <http://support.microsoft.com/kb/837129/en-us> et <http://support.microsoft.com/kb/927908/en-us>

Pour afficher les stratégies de mots de passe : `net accounts /domain`

Les stratégies de préférence : <http://support.microsoft.com/kb/943729/en-us>



```
c:\>gpresult /R

Outil de résultat du système d'exploitation Microsoft (R) Windows (R) v2.0
Copyright (C) Microsoft Corp. 1981-2001

Jeu créé le 10/06/2010 à 21:26:39

Données RSOP pour MSREPORTFORM\Administrateur sur SFR1 : mode journalisation
-----
Configuration du système d'exploitation : Contrôleur principal de domaine
Version du système d'exploitation..... : 6.1.7600
Nom du site..... : Default-First-Site-Name
Profil itinérant : N/A
Profil local..... : C:\Users\Administrateur
Connexion via une liaison lente ? : Non

Paramètre de l'ordinateur
-----
CN=SFR1,OU=Domain Controllers,DC=formation10,DC=lan
Heure de la dernière application de la stratégie de groupe : 10/06/2010 à 21:23:25
```

# 8. Les mécanismes de répllication :

# Les sites Active Directory

Réplication Active Directory : basée sur numéro USN (Unique Séquence Number). La restauration autoritaire (avec NTDSUTIL) permet d'augmenter numéro USN. Par défaut, les DC d'un même site réplique toutes les 15 secondes entre eux.

Intérêt de créer plusieurs sites Active Directory : définir avec quels DC les stations de travail s'authentifient et configurer l'intervalle de réplication entre contrôleurs de domaine.

Chaque site est associé à un ou plusieurs sous réseaux IP.

Un sous réseau IP ne peut pas être associé à deux sites Active Différents.

Pour configurer 2 sites AD différents, il faut 2 sous réseaux IP (un pour chaque site).

Les DC répliquent entre eux via des objets « *Connexion* » (unidirectionnel).

Les objets « *Connexion* » sont générés par le KCC (DC dans même site) et par l'ISTG entre 2 sites. Pour forcer la génération objets « *Connexion* » : *repadmin /KCC*.

Best Practice : prévoir un serveur de Catalogue Global dans chaque site ou activer la mise en cache des groupes universels.

<http://support.microsoft.com/kb/242780/en-us>

<http://support.microsoft.com/kb/305179/en-us>

<http://www.tech-faq.com/lang/fr/active-directory-replication.shtml>

# TP : Les sites Active Directory 1/5

Le service RRAS permet de transformer Windows Server en routeur IP, serveur NAT, serveur VPN et en serveur RAS.

Depuis Windows Server 2008 R2, il est nécessaire d'installer le rôle « Services de stratégies et d'accès distants » et de configurer ensuite le service RRAS en tant que routeur IP.

Installer le rôle « *Services de stratégies et d'accès réseau* » avec les services de rôles « *Service de routage et accès distant* ».

Aller dans les outils d'administration et lancer la console « *Routage et Accès distants* ».

Assistant Ajout de rôles

Sélectionnez des rôles de serveurs

Avant de commencer

Rôles de serveurs

Stratégie et accès réseau

Services de rôle

Confirmation

État d'avancement

Résultats

Sélectionnez un ou plusieurs rôles à installer s

Rôles :

- Hyper-V
- Serveur d'applications
- Serveur de télécopie
- Serveur DHCP
- Serveur DNS
- Serveur Web (IIS)
- Services AD LDS (Active Directory Lightb
- Services AD RMS (Active Directory Rights
- Services ADFS (Active Directory Federati
- Services Bureau à distance
- Services de certificats Active Directory
- Services de déploiement Windows
- Services de documents et d'impression
- Services de domaine Active Directory
- Services de fichiers
- Services de stratégie et d'accès réseau
- Services WSUS (Windows Server Update

Assistant Ajout de rôles

Sélectionner les services de rôle

Avant de commencer

Rôles de serveurs

Stratégie et accès réseau

Services de rôle

Confirmation

État d'avancement

Résultats

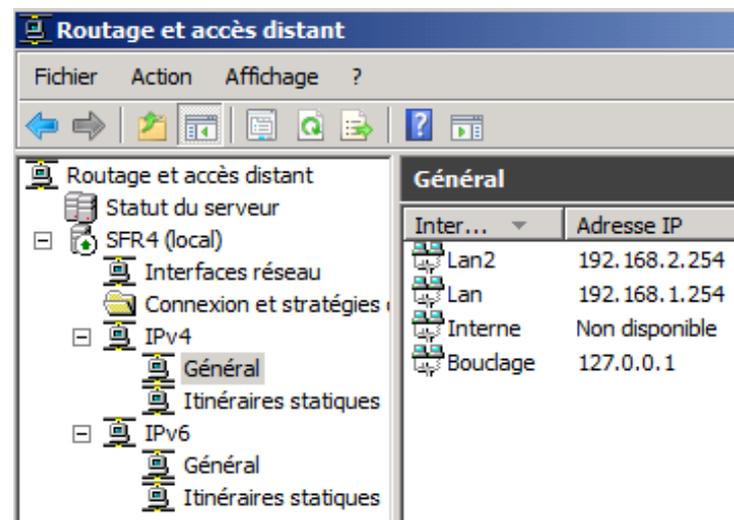
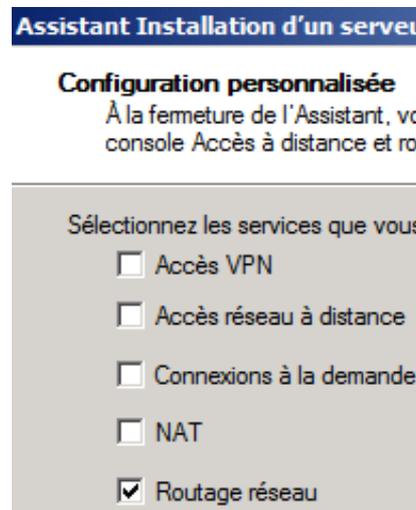
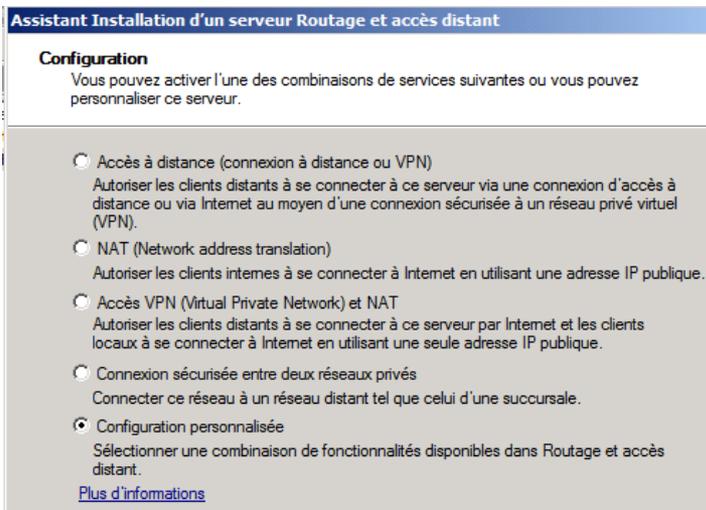
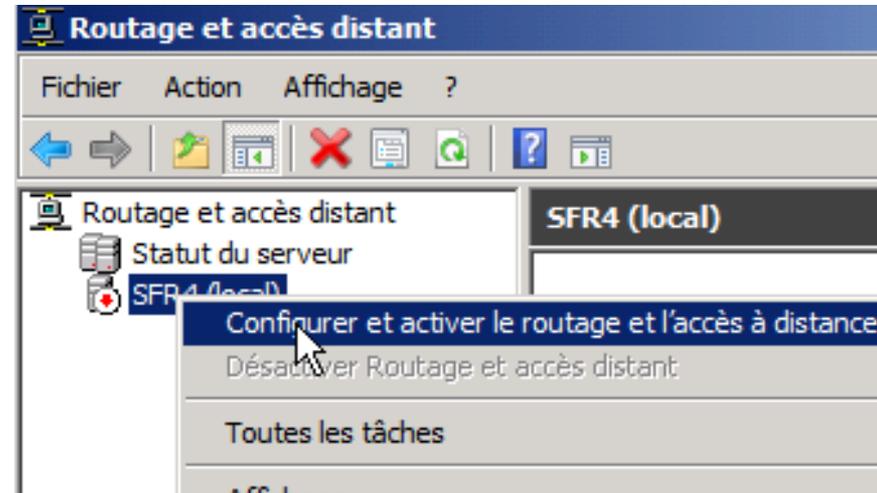
Sélectionner les services de rôle à installer pour Services

Services de rôle :

- Serveur NPS (Network Policy Server)
- Services Routage et accès distant
  - Service d'accès à distance
  - Routage
- Autorité HRA (Health Registration Authority)
- HCAP (Host Credential Authorization Protocol)

# TP : Les sites Active Directory 2/5

Démarrer la console « *Routage et Accès distant* » (dans les outils d'administration).  
Cliquer sur « Configurer et activer le routage et l'accès distant ».  
Sélectionner « *Configuration personnalisée* » puis « *Routage IP* ».  
Cliquer sur « *Démarrer le service* ».  
Valider que les deux contrôleurs de domaine peuvent communiquer ensemble (ping).



# TP : Les sites Active Directory 3/5

Définir 1<sup>er</sup> DC avec IP : 192.168.1.1 /24 et 2<sup>ème</sup> DC avec IP : 192.168.2.1 /24.

Changer les adresses de serveur DNS et indiquer une passerelle (routeur RRAS).

Supprimer les anciennes entrées dans le DNS (anciennes IP des DC).

Taper les commandes suivantes :

```
Ipconfig /registerdns
```

```
Net stop netlogon & Net start netlogon
```

```
Ipconfig /flushdns
```

Valider que les deux DC peuvent communiquer ensemble (PING).

Lancer « *Sites et Services Active Directory* ». Forcer la réplication entre les 2 DC.

Renommer le site par défaut en « Nemours ». Créer un second site appelé « Meudon ». Créer 2 SUBNETs 192.168.1.0./24 et 192.168.2.0 /24. Lier 1<sup>er</sup> SUBNET au site Nemours, lier 2<sup>ème</sup> SUBNET à Meudon.

Renommer le lien inter-sites par défaut en Nemours-Meudon. Configurer la réplication sur 15 minutes. Permettre la réplication à toutes heures.

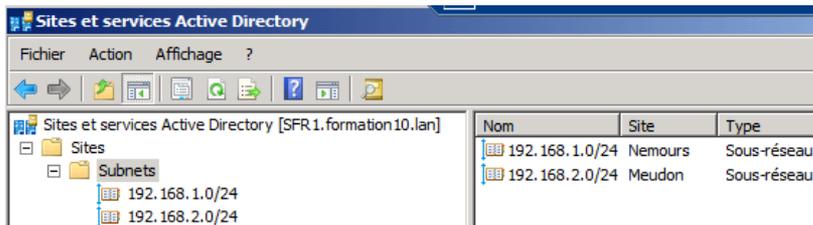
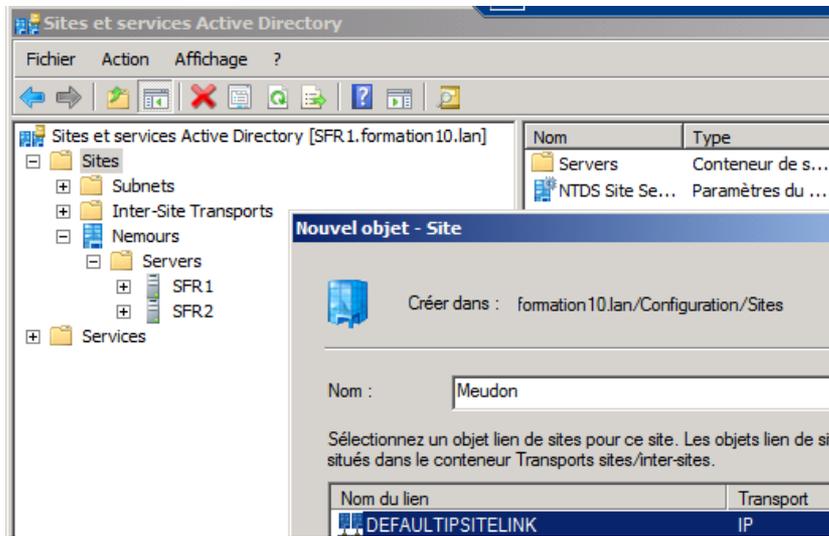
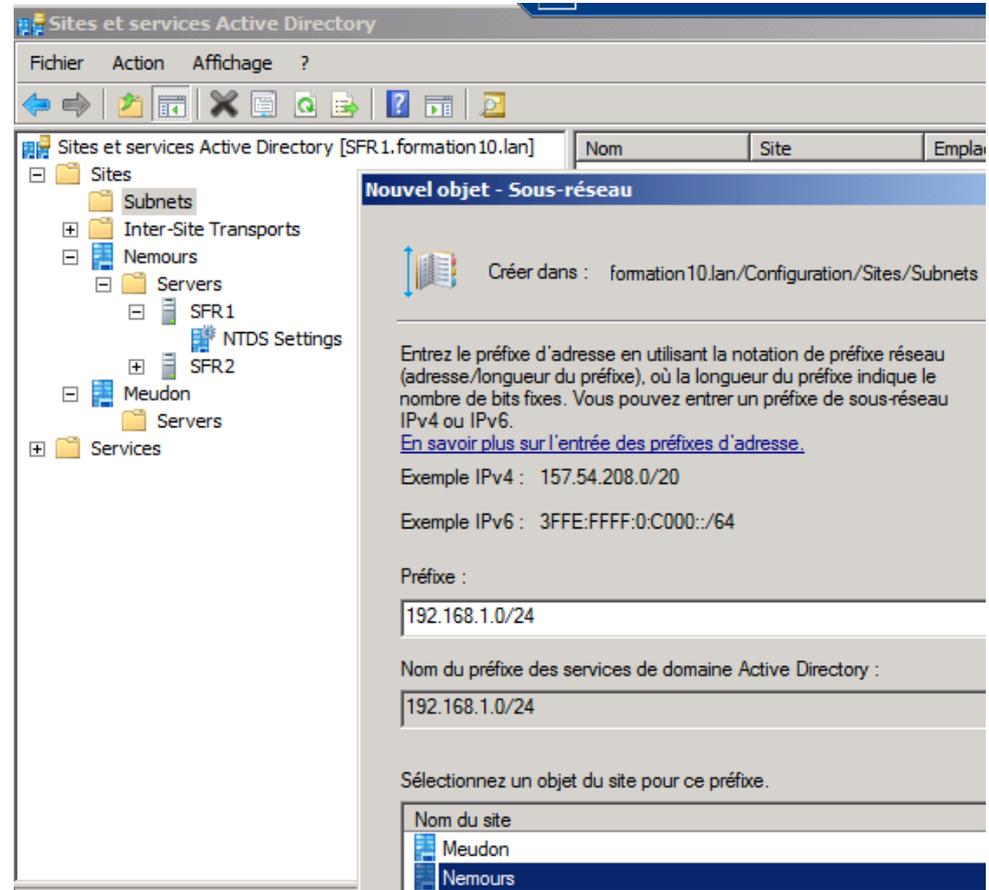
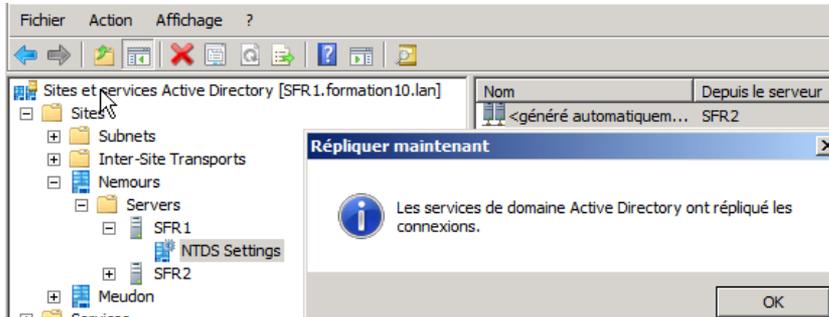
Déplacer le 2<sup>ème</sup> contrôleur de domaine dans le site Meudon. Lancer la commande repadmin /kcc pour forcer l'ISTG à générer les objets Connexion.

Supprimer les liens connexions. Désactiver le KCC / ISTG :

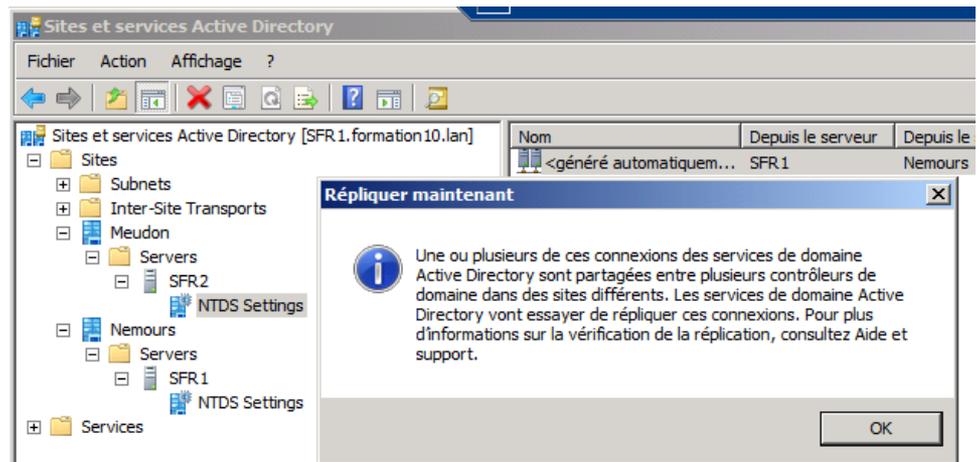
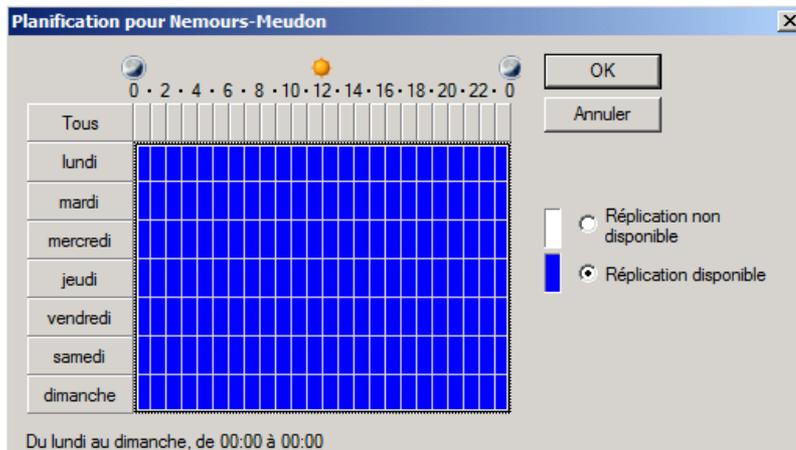
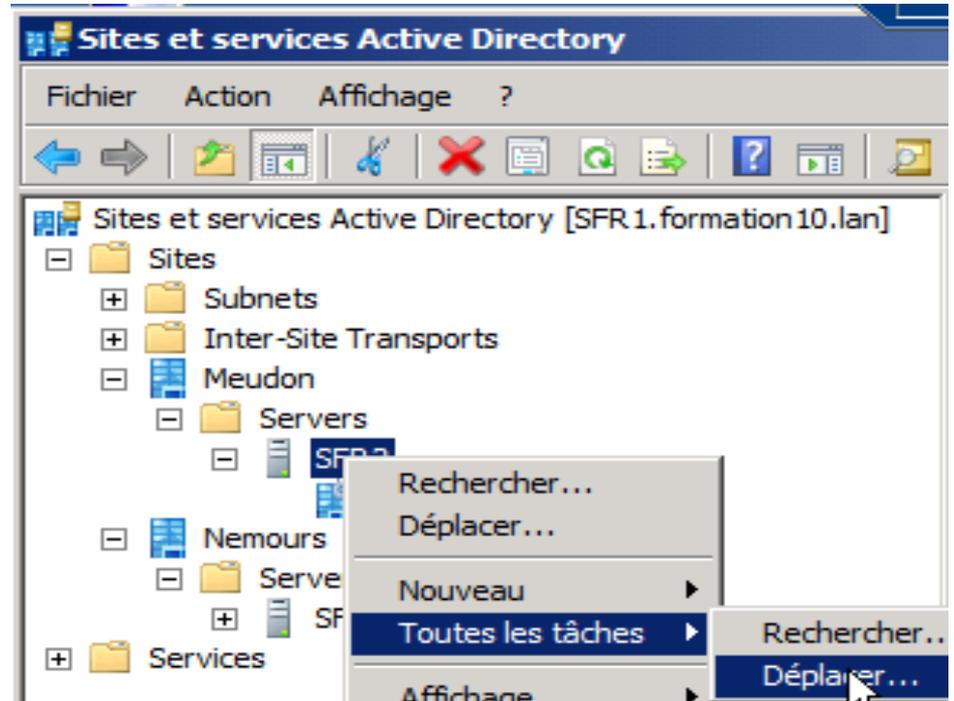
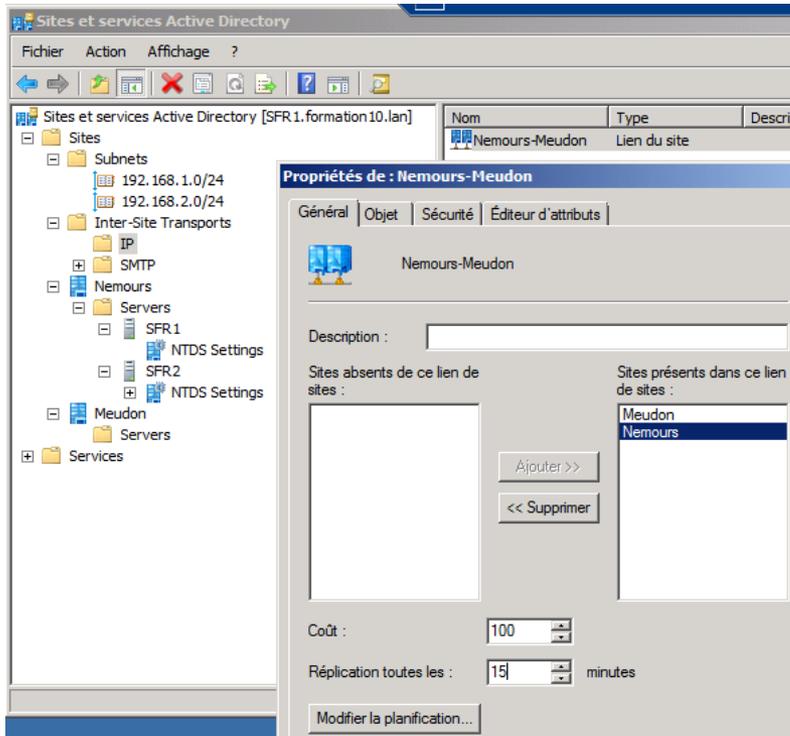
<http://support.microsoft.com/kb/242780/en-us>

Taper la commande repadmin /KCC. Que se passe t'il ? Créer les liens de connexion manuellement.

# TP : Les sites Active Directory 4/5



# TP : Les sites Active Directory 5/5



# 9. Sauvegarde et restauration Active Directory

# Windows Server Backup 1/5

NTBACKUP a été remplacé par « *Windows Server Backup* ».

Windows Server Backup permet prendre en charge la déduplication quand on sauvegarde sur une partition dédiée. On peut donc exécuter des sauvegardes complètes toutes les heures. Seuls les blocs modifiés sont sauvegardés.

Windows Server Backup ne permet pas de sauvegarder sur bande. Pour faire une sauvegarde sur bande, sauvegarder vers un partage et sauvegarder ensuite les fichiers produits par « *Windows Server Backup* ».

Quand on fait une sauvegarde sur disque local, le disque est formaté en NTFS mais n'est pas monté. Il est alors réservé par Windows Server Backup.

## Mise en pratique :

Prérequis : Il faut disposer d'un second disque sur le serveur (dédié).

Lancer la détection des disques et à le mettre en ligne.

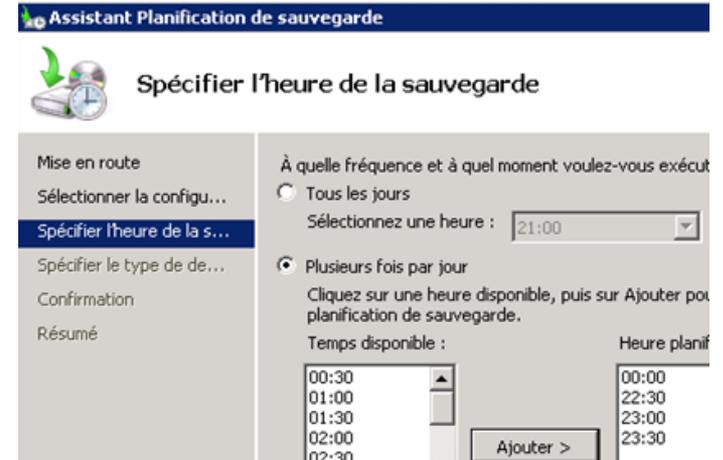
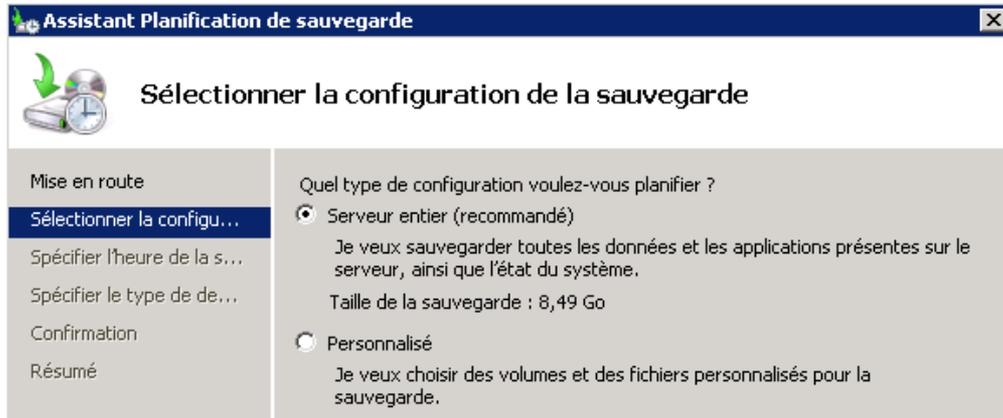
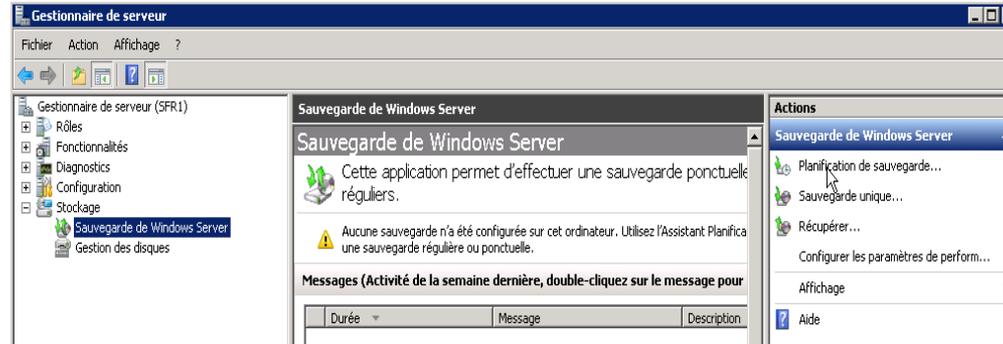
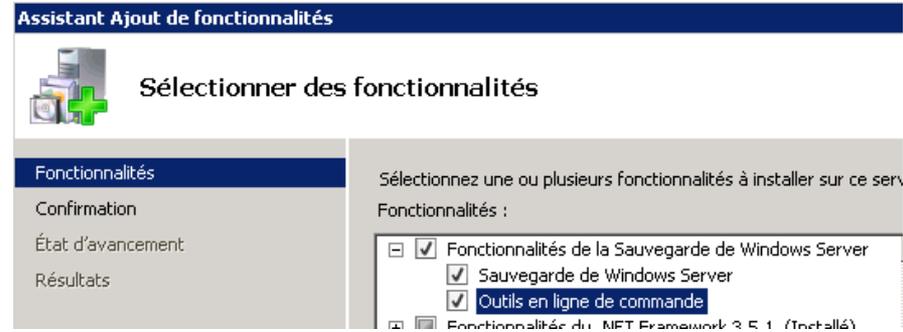
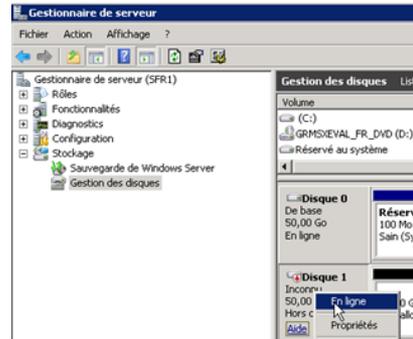
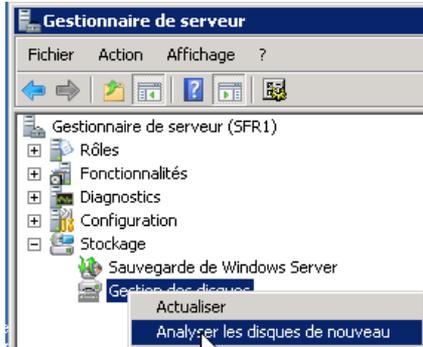
Installer la fonctionnalité « *Windows Server Backup* » (avec la partie PowerShell).

Lancer la console « *Windows Server Backup* » et cliquer sur Planifier une sauvegarde. Cliquer sur sauvegarde complète (inclue la sauvegarde de l'Etat du système). Faire une sauvegarde plusieurs fois par jour vers un disque dédié.

Aller dans les tâches planifiées, dans la section backup. Modifier la tâche pour qu'elle autorise les actions manuelles et lancer une sauvegarde.

Ouvrir la console Windows Server Backup et valider l'état d'avancement de la sauvegarde.

# Windows Server Backup 2/5



# Windows Server Backup 3/5

**Assistant Planification de sauvegarde**

## Spécifier le type de destination

Mise en route

Sélectionner la configu...

Spécifier l'heure de la s...

**Spécifier le type de de...**

Sélectionner le disque ...

Confirmation

Résumé

Où voulez-vous stocker les sauvegardes ?

- Sauvegarder vers un disque dur dédié aux sauvegardes (recommandé)  
Sélectionnez cette option pour stocker de la manière la plus sûre les sauvegardes. Le disque dur utilisé sera formaté, puis utilisé uniquement pour stocker les sauvegardes.
- Sauvegarder vers un volume  
Sélectionnez cette option si vous ne pouvez pas dédier tout un disque à la sauvegarde. Notez que cette option peut réduire les performances du volume de 200 pour cent durant le stockage des sauvegardes. Il est recommandé de ne pas stocker d'autres données de serveur sur le même volume.
- Sauvegarder sur un dossier réseau partagé  
Sélectionnez cette option uniquement si vous ne voulez pas stocker les sauvegardes sur le serveur lui-même. Notez que vous ne disposerez que d'une sauvegarde à la fois lorsque vous créez une nouvelle sauvegarde, car celle-ci remplace la précédente.

**Assistant Planification de sauvegarde**

## Sélectionner le disque de destination

Mise en route

Sélectionner la configu...

Spécifier l'heure de la s...

Spécifier le type de de...

**Sélectionner le disque ...**

Confirmation

Résumé

Sélectionnez un ou plusieurs disques pour stocker vos sauvegardes. Vous pouvez utiliser plusieurs disques de sauvegarde si vous souhaitez stocker des disques hors site.

Disques disponibles :

Disque	Nom	Taille	Espace uti...	Volumes prés...
<input checked="" type="checkbox"/> 1	Msft Virtual...	50,00 Go	0 Ko	

Afficher tous les disques disponibles...

**Sauvegarde de Windows Server**

 Une fois que vous avez terminé cet Assistant, les disques sélectionnés seront reformatés et tous les volumes et données des disques seront supprimés. Pour permettre aux utilisateurs de déplacer les sauvegardes hors site à des fins de protection en cas d'urgence et pour garantir l'intégrité des sauvegardes, l'intégralité des disques sera dédiée au stockage des sauvegardes et ne sera pas visible dans l'Explorateur Windows.

Cliquez sur Oui pour utiliser le ou les disques sélectionnés.

**Planificateur de tâches**

Fichier Action Affichage ?

Planificateur de tâches (Local)

- Bibliothèque du Planificateur de tâches
  - Microsoft
    - Windows
      - Active Directory Rights Management Ser
      - AppID
      - Application Experience
      - Autochk
      - Backup
      - CertificateServicesClient
      - Customer Experience Improvement Prog
      - Defrag
      - MemoryDiagnostic
      - MUI
      - Multimedia
      - NetTrace

Nom	Statut	Déclencheurs
Microsoft-Windows-WindowsBackup	Prêt	Plusieurs déclencheurs sont définis.

**Propriétés de Microsoft-Windows-WindowsBackup (Ordinateur local)**

Général Déclencheurs Actions Conditions Paramètres Historique

Lorsque vous créez une tâche, vous pouvez spécifier les conditions qui la déclent

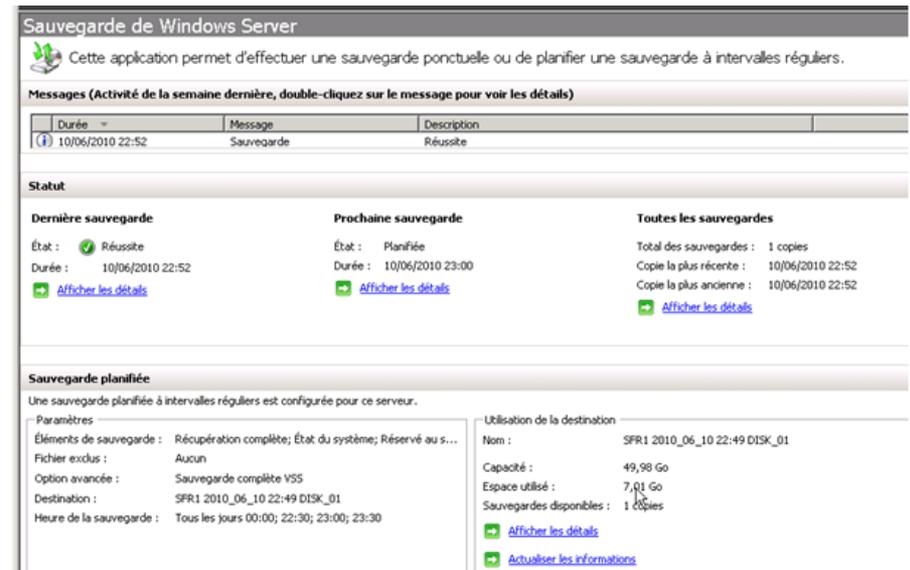
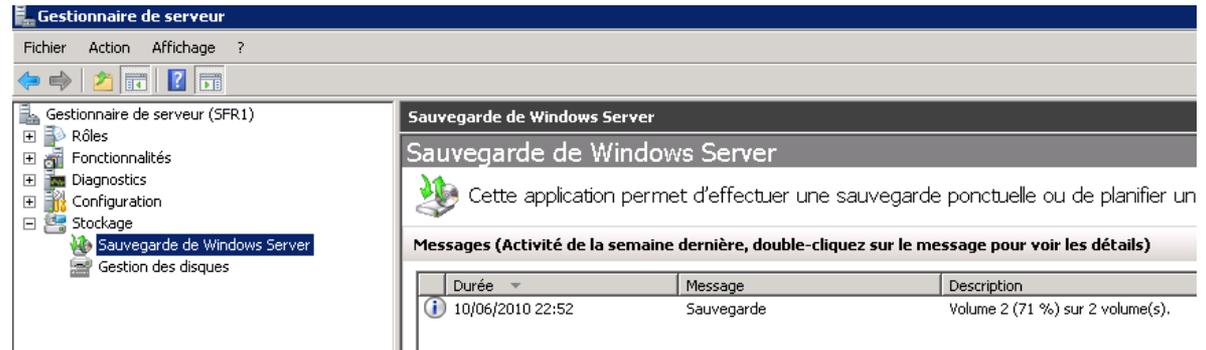
Déclenchement	Détails	Statut
Tous les jours	À 00:00 tous les jours	Activé
Tous les jours	À 22:30 tous les jours	Activé
Tous les jours	À 23:00 tous les jours	Activé
Tous les jours	À 23:30 tous les jours	Activé

# Windows Server Backup 4/5

Une fois la sauvegarde terminée, relancer une seconde fois la sauvegarde. L'espace disque évolue t'il ? Le fait de faire une seconde sauvegarde nous fait passer de 7,01 Go à 7,03 Go.

Lancer PowerShell et taper la commande suivante : `add-pssnapin windows.serverbackup`. Cela ajoute les CMDLET Windows Server backup à PowerShell.

Taper ensuite la commande `get-command -module windows.serverbackup` pour afficher les commandes Windows Server Backup.



# Windows Server Backup 5/5

Pour externaliser la sauvegarde, faire une sauvegarde sur un LUN hébergé sur un SAN (Fibre Channel / DAS obligatoire). Cela permet de conserver la déduplication.

Vérifier qu'il est possible de charger le pilote de la carte Fibre / DAS depuis le CD d'installation (en mode récupération).

[http://technet.microsoft.com/en-us/library/ee849849\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/ee849849(WS.10).aspx)

[http://technet.microsoft.com/en-us/library/cc771290\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc771290(WS.10).aspx)

<http://www.winserverhelp.com/2010/03/windows-server-2008-r2-backup-and-restore/>

<http://unifiedit.wordpress.com/2009/12/17/forest-recovery-ad-2008/>

## Sauvegarde planifiée

Une sauvegarde planifiée à intervalles réguliers est configurée pour ce serveur.

### Paramètres

Éléments de sauvegarde : Récupération complète; État du système; Réserve au s...

Fichier exclus : Aucun

Option avancée : Sauvegarde complète VSS

Destination : SFR1 2010\_06\_10 22:49 DISK\_01

Heure de la sauvegarde : Tous les jours 00:00; 22:30; 23:00; 23:30

### Utilisation de la destination

Nom : SFR1 2010\_06\_10 22:49 DISK\_01

Capacité : 49,98 Go

Espace utilisé : 7,03 Go

Sauvegardes disponibles : 2 copies

 [Afficher les détails](#)

 [Actualiser les informations](#)

# Restauration Windows Server Backup 1/2

On ne peut pas restaurer un DC à une date antérieure à la période de Tombstone

Depuis Windows 2008, il est possible de faire une restauration complète d'un DC en démarrant depuis le DVD d'installation.

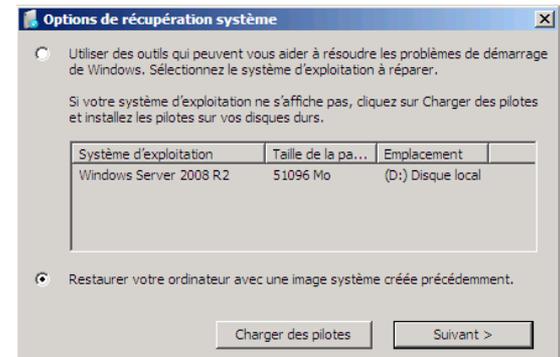
Vérifier une fois que la restauration est effectuée que tout réplique bien et qu'il n'y a pas d'erreurs dans les logs. Faire un DCDIAG /V /E pour valider le bon fonctionnement de l'annuaire.

Pour faire une restauration autoritaire (restaurer un objet supprimé par exemple), il faut redémarrer en mode « *Restauration des services d'annuaire* ».

[http://technet.microsoft.com/en-us/library/cc816878\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc816878(WS.10).aspx)

## Mise en pratique :

Démarrer sur le CD d'installation et cliquer sur « Réparer l'ordinateur ». Restaurer avec la sauvegarde disque.



# Restauration Windows Server Backup 2/2

**Réimager l'ordinateur**

**Sélectionnez la date et l'heure de l'image système à restaurer**  
Si plusieurs images système sont disponibles et si vous ne savez pas laquelle restaurer, choisissez la plus récente.

Sauvegardes disponibles pour SFR.1 sur SFR.1 2010\_06\_10 22:49 DISK\_01 (F:)  
Fuseau horaire actuel : GMT+01:00

Date et heure	Lecteurs dans la sauvegarde
10/06/2010 22:30:06	\\?\Volume{a427cd07-7200-11df-a227-806e6f6e6963}, C:
10/06/2010 21:58:23	\\?\Volume{a427cd07-7200-11df-a227-806e6f6e6963}, C:
10/06/2010 21:52:33	\\?\Volume{a427cd07-7200-11df-a227-806e6f6e6963}, C:

**Réimager l'ordinateur**

Votre ordinateur sera restauré depuis l'image système suivante :

Date et heure : 10/06/2010 22:30:06 (GMT+01:00)  
Ordinateur : SFR.1  
Lecteurs à restaurer : \\?\Volume{a427cd07-7200-11df-}

**Réimager l'ordinateur**

 Tous les disques à restaurer seront formatés et remplacés par la disposition et les données de l'image système. Êtes-vous sûr de vouloir continuer ?

Qui Non

**Réimager l'ordinateur**

**Choisir des options de restauration supplémentaires**

Formater et repartitionner les disques  
Sélectionnez cette option pour supprimer toutes les partitions existantes et reformater tous les disques sur cet ordinateur afin de correspondre à la disposition de l'image système.

Exclure les disques...

**Réimager l'ordinateur**

Windows restaure votre ordinateur depuis l'image système. Cette opération peut durer de plusieurs minutes à plusieurs heures.

Restoration du disque (C:)...

Arrêter la restauration

# TP : restauration autoritaire

Au redémarrage, appuyer sur F8.

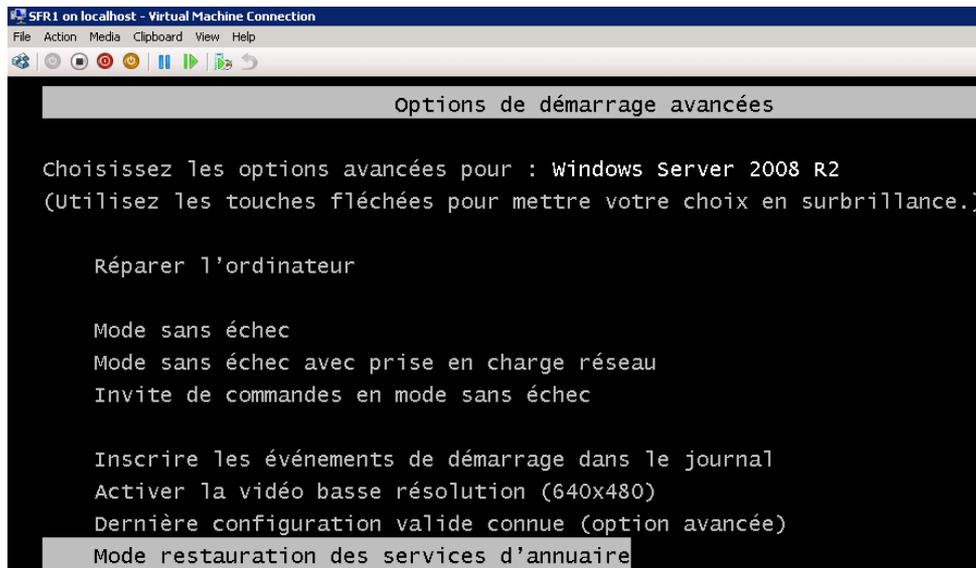
Démarrer en mode « *Restauration des services d'annuaire* ».

Lancer Windows Server Backup et faire une restauration classique.

Lancer l'utilitaire NTDSUTIL pour marquer les objets qui sont à restaurer de manière autoritaire (cela incrémente le numéro USN de l'objet).

Appliquer la procédure suivante : [http://technet.microsoft.com/en-us/library/cc816878\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc816878(WS.10).aspx)

Attention aux problèmes d'appartenance des groupes. Préférer utiliser la corbeille Active Directory quand cela est possible.



# La corbeille Active Directory 1/3

Avant la corbeille Active Directory, il était déjà possible de récupérer les objets qui étaient en mode Tombstone. Lorsque un objet est supprimé, il passe en mode Tombstone pendant 60 jours ou 180 jours. Il est alors possible de le restaurer. Cependant, lors de la restauration on ne pouvait récupérer que 5 attributs dont le SAMACCOUNTNAME (login pré Windows 2000), le SID et le GUID. Les appartenances aux groupes étaient perdues.

L'activation de la corbeille est irréversible

La forêt doit être en mode natif 2008 R2 pour activer cette fonctionnalité.

La durée de vie pendant laquelle les objets peuvent être restaurés est contrôlés par le paramètre « *msDS-deletedObjectLifetime* ». Ne pas oublier de définir la valeur souhaitée.

<http://www.hyperv.fr/blog/2009/04/11/windows-server-2008-r2-et-powershell-restauration-dobjets-active-directory-1273.html>

# TP : la corbeille Active Directory 1/2

Vérifier que la forêt est en mode natif 2008 R2 (en PowerShell)

Activer la corbeille Active Directory en tapant la commande suivante (remplacer le nom de domaine, ici *formation10.lan* par le nom de votre domaine) :

```
Enable-ADOptionalFeature -Identity 'Recycle Bin Feature' -Scope ForestOrConfigurationSet -Target formation10.Lan
```

Configurer la durée de vie de la corbeille.

```
Set-ADObject -Identity "CN=Directory Service,CN=Windows NT,CN=Services,CN=Configuration,DC=formation10,DC=Lan" -Partition "CN=Configuration,DC=formation10,DC=Lan" -Replace: @{msDS-DeletedObjectLifeTime = 365}
```

Créer un compte utilisateur testsuppr1 et un groupe Testlab2. Ajouter l'utilisateur dans le groupe. Ouvrir une session avec ce compte et personnaliser la session.

Supprimer ce compte utilisateur. Lister les objets supprimés :

```
Get-ADObject -Filter 'isdeleted -eq $true -and name -ne "Deleted Objects" -IncludeDeletedObjects -Properties *
```

```
Get-ADObject -filter 'samaccountname -eq « guillaume.mathieu' -IncludeDeletedObjects
```

Restaurer l'objet en tapant la commande suivante :

```
Get-ADObject -filter 'samaccountname -eq "dominique.mathieu" -IncludeDeletedObjects | Restore-ADObject
```

<http://www.hyperv.fr/blog/2009/04/11/windows-server-2008-r2-et-powershell-restauration-dobjets-active-directory-1273.html>

<http://blogs.technet.com/b/askds/archive/2009/08/27/the-ad-recycle-bin-understanding-implementing-best-practices-and-troubleshooting.aspx>

# TP : la corbeille Active Directory 2/2

```
Administrateur : Module Active Directory pour Windows PowerShell
PS C:\Users\Administrateur> Set-ADForestMode -Identity formation10.Lan -ForestMode Windows2008Forest

Confirmer
Êtes-vous sûr de vouloir effectuer cette action ?
Opération « Set » en cours sur la cible
« CN=Partitions,CN=Configuration,DC=formation10,DC=lan ».
[O] Oui [I] Oui pour tout [N] Non [U] Non pour tout [S] Suspendre
[?] Aide<la valeur par défaut est « 0 »> : o
PS C:\Users\Administrateur> _
```

```
PS C:\Users\Administrateur> Enable-ADOptionalFeature -Identity 'Recycle Bin Feature' -Scope ForestOrConfigurationSet -Target formation10.lan
Avertissement : L'activation de « Recycle Bin Feature » sur
« CN=Partitions,CN=Configuration,DC=formation10,DC=lan » est une action
irréversible ! Vous ne pourrez pas désactiver « Recycle Bin Feature » sur
« CN=Partitions,CN=Configuration,DC=formation10,DC=lan » si vous continuez.

Confirmer
Êtes-vous sûr de vouloir effectuer cette action ?
Opération « Enable » en cours sur la cible « Recycle Bin Feature ».
[O] Oui [I] Oui pour tout [N] Non [U] Non pour tout [S] Suspendre
[?] Aide<la valeur par défaut est « 0 »> : o
Enable-ADOptionalFeature : La méthode spécifiée n'est pas prise en charge
Au niveau de ligne : 1 Caractère : 25
+ Enable-ADOptionalFeature <<<< -Identity 'Recycle Bin Feature' -Scope ForestOrConfigurationSet -Target formation10.lan
+ CategoryInfo          : NotSpecified: (Recycle Bin Feature:ADOptionalFeature) [Enable-ADOptionalFeature], ADException
+ FullyQualifiedErrorId : La méthode spécifiée n'est pas prise en charge,Microsoft.ActiveDirectory.Management.Commands.EnableADOptionalFeature
```

```
PS C:\Users\Administrateur> Enable-ADOptionalFeature -Identity 'Recycle Bin Feature' -Scope ForestOrConfigurationSet -Target formation10.lan
Avertissement : L'activation de « Recycle Bin Feature » sur
« CN=Partitions,CN=Configuration,DC=formation10,DC=lan » est une action
irréversible ! Vous ne pourrez pas désactiver « Recycle Bin Feature » sur
« CN=Partitions,CN=Configuration,DC=formation10,DC=lan » si vous continuez.

Confirmer
Êtes-vous sûr de vouloir effectuer cette action ?
Opération « Enable » en cours sur la cible « Recycle Bin Feature ».
[O] Oui [I] Oui pour tout [N] Non [U] Non pour tout [S] Suspendre
[?] Aide<la valeur par défaut est « 0 »> : o
PS C:\Users\Administrateur> _
```

```
PS C:\Users\Administrateur> Set-ADObject -Identity "CN=Directory Service,CN=Windows NT,CN=Services,CN=Configuration,DC=formation10,DC=Lan" -Partition "CN=Configuration,DC=formation10,DC=Lan" -Replace:@{"msDS-DeletedObjectLifeTime" = 365}
PS C:\Users\Administrateur> _
```

# **10. Notions avancées**

## **Active Directory :**

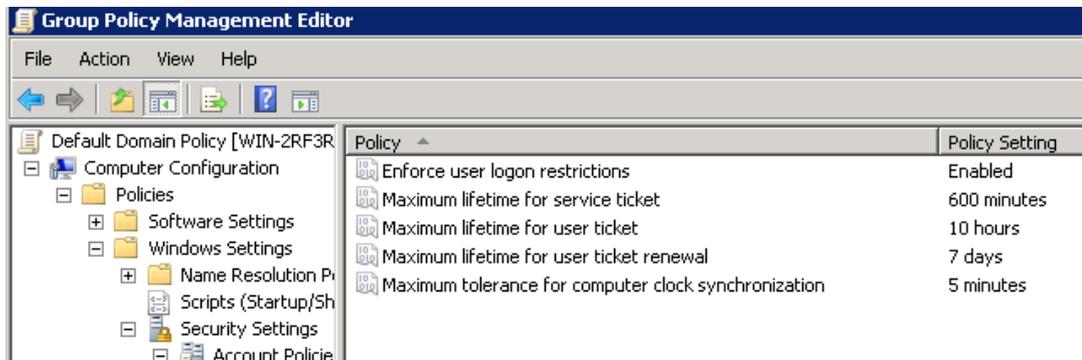
# Les paramètres avancées

Compléments d'informations sur les paramètres de sécurité Active Directory (quotas...) :  
<http://www.serverwatch.com/tutorials/article.php/3075971/Exploring-Windows-2003-Security-More-Active-Directory-Security-Improvements.htm>

Réinitialiser le mot de passe administrateur du domaine depuis le mode Restauration des services d'annuaire :  
<http://blog.portail-mcse.net/index.php?post/2008/02/27/Reset-du-mot-de-passe-Admin-du-domaine-sous-Windows-Server-2003>

Visibilité du champ UserPassword :  
<http://blog.portail-mcse.net/index.php?post/2009/11/23/l-attribut-UserPassword-en-clear-text>

Configuration des paramètres KERBEROS :  
Lorsque l'on rencontre des problèmes de désynchronisation horaire sur les stations de travail, il peut être intéressant d'augmenter le paramètre « *Maximum tolerance for computer clock synchronisation* » à plus de 5 minutes.



# Méthodologie dépannage AD 1/2

## **Etape 1 : Faire une sauvegarde de l'Etat du Système avant toutes modifications.**

Avant d'effectuer la moindre modification, valider qu'il existe une sauvegarde de l'Etat du système pour chaque contrôleur de domaine (au moins un DC par domaine). Valider le bon fonctionnement de la sauvegarde en lançant la console « *Windows Server Backup* ».

## **Etape 2 : reproduction du problème :**

Reproduire le problème : généralement quand on arrive à reproduire le problème, l'incident à 90% de chance d'être résolu.

## **Etape 3 : Vérification préliminaire :**

Valider que les services suivants sont démarrés sur tous les DC :

*Appel de procédure distante (RPC), Assistance NetBIOS sur TCP/IP, Centre de Distribution de Clés Kerberos, Client DHCP (gère la mise à jour dynamique DNS, Explorateur d'ordinateurs (pour le voisinage réseau), Messagerie Inter-site Netlogon, Registre à distance, Réplication de fichiers (si niveau fonctionnelle domaine < 2008 natif), Réplication DFS (si niveau fonctionnelle domaine > 2003 R2), Serveur DNS, Services de domaine Active Directory, Services Web Active Directory*

Désactiver temporairement UAC et le pare Windows.

Vérifier que les stations de travail peuvent communiquer avec les contrôleurs de domaine (ping).

# Méthodologie dépannage AD 2/2

## Etape 4 : Analyse :

Analyser les observateurs d'événements. Filtrer sur les erreurs et les avertissements uniquement dans un premier temps. Attention, de nombreuses erreurs risquent de remonter. Il faut trouver la cause du problème et ne pas se focaliser sur les conséquences.

Validation la configuration DNS (tous les DC ont le même serveur DNS principal).

Valider le bon fonctionnement de la réplication Active Directory (NTDS) et SYSVOL. Pour cela, lancer la console « *Sites et Services Active Directory* » et forcer la réplication. Copier un fichier dans c:\windows\sysvol\sysvol et valider que ce fichier apparaît dans sur tous les DC.

Valider qu'il n'y a pas plus de 5 minutes de décalage horaire entre les différentes machines (DC comme stations de travail).

Lancer les outils de diagnostics DCDIAG, REPADMIN, MPSREPORT, REPLMON...

## Etape 5 : recherche et validation solution :

Vous pouvez vous appuyer sur les sites communautaires ([www.google.fr/microsoft](http://www.google.fr/microsoft)), les NEWGROUP et la base de connaissance Microsoft (<http://support.microsoft.com/search>) . Pour plus d'informations, voir l'article « *A la découverte de la communauté Microsoft* » sur <http://msreport.free.fr>.

Une fois la solution trouvée, il faut monter une maquette pour valider la solution.

Faire une sauvegarde avant toute application de la solution sur l'environnement de production.

# Les observateurs d'événements 1/2

Analyser le contenu des journaux Systèmes, Application, Key Management Service, Réplication DFS (pour SYSVOL et le DFS), Service DNS, Services d'annuaire, Services Web Active Directory.

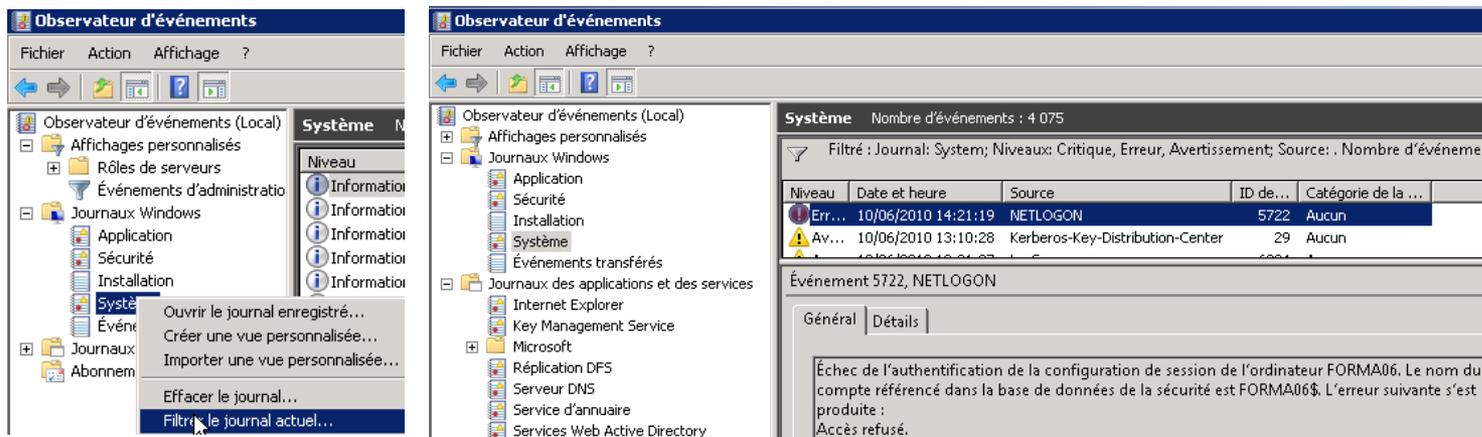
Configurer les filtres pour n'afficher que les avertissements, les erreurs et les messages critiques.

Quelques erreurs à rechercher : USERENV, NTDS REPLICATION, NETLOGON, SAM, NTDS, DNS-SERVER-SERVICE, DFS-REPLICATION, SCECLI.

De nombreuses erreurs vont remonter. Chercher les causes pas les conséquences.

Astuces : Aller sur [www.google.fr](http://www.google.fr) et taper la source de l'événement et le code d'erreur après (exemple : NETLOGON 5722).

Pour les recherches dans la base de connaissance Microsoft (<http://support.microsoft.com/search>, toujours en anglais).



Observateur d'événements

Fichier Action Affichage ?

Observateur d'événements (Local)

Affichages personnalisés

Rôles de serveurs

Événements d'administratio

Journal Windows

Application

Sécurité

Installation

Système

Événements

Journal des applications et des services

Internet Explorer

Key Management Service

Microsoft

Réplication DFS

Serviceur DNS

Service d'annuaire

Services Web Active Directory

Système

Niveau

Information

Information

Information

Information

Information

Ouvrir le journal enregistré...

Créer une vue personnalisée...

Importer une vue personnalisée...

Effacer le journal...

Filtrer le journal actuel...

Système

Nombre d'événements : 4 075

Filtré : Journal: System; Niveaux: Critique, Erreur, Avertissement; Source: . Nombre d'événements

Niveau	Date et heure	Source	ID de...	Catégorie de la ...
Err...	10/06/2010 14:21:19	NETLOGON	5722	Aucun
Av...	10/06/2010 13:10:28	Kerberos-Key-Distribution-Center	29	Aucun

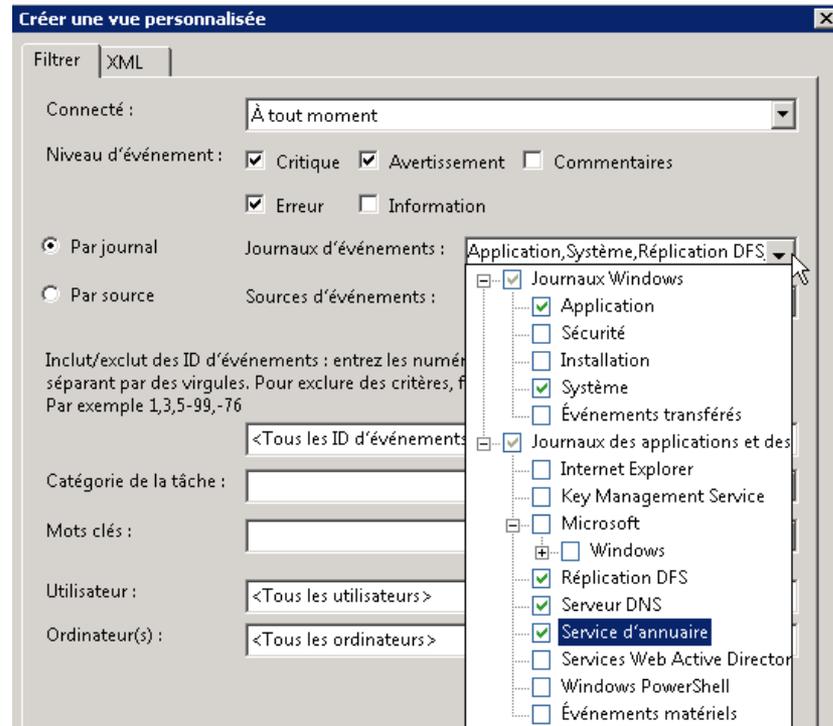
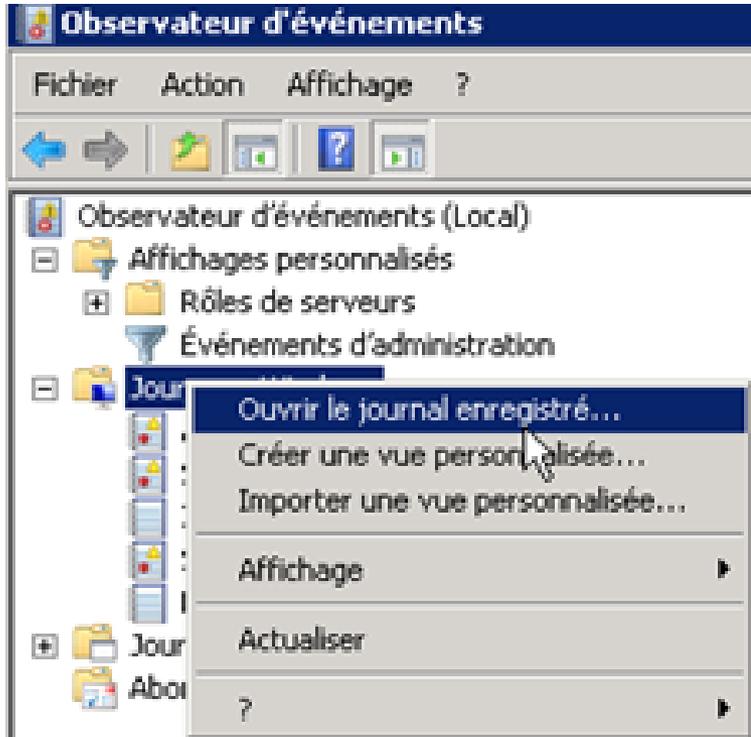
Événement 5722, NETLOGON

Général Détails

Échec de l'authentification de la configuration de session de l'ordinateur FORMA06. Le nom du compte référencé dans la base de données de la sécurité est FORMA06\$. L'erreur suivante s'est produite : Accès refusé.

# Les observateurs d'événements 2/2

Pour afficher les événements de plusieurs journaux, passer par les vues !



# Les outils de dépannage 1/3

## NTDSUTIL :

- Réinitialisation du mot de passe compte restauration des services d'annuaire.
- Supprimer un contrôleur de domaine ou un domaine.
- Permet de défragmenter l'annuaire.
- Permet de faire une restauration autoritaire.
- Permet de forcer le transfert d'un rôle.
- Permet de créer des SNAPSHOT d'Active Directory (que l'on peut monter en lecture seule).
- Permet de créer des partitions d'application.

## DCDIAG /V /E > c:\DCDIAG.TXT :

- Permet de valider la configuration des contrôleurs de domaine de toute la forêt. Attention ce dernier s'appuie sur les noms NETBIOS. Donc il faut pouvoir résoudre tous les contrôleurs de domaine avec leurs noms NETBIOS.
- Faire une recherche sur le mot « Fail » ou « Echec » au niveau du fichier de sortie.

## DCPROMO /FORCEREMOVAL :

- Permet de forcer la suppression d'un contrôleur de domaine. Ce dernier ne contacte pas les autres DC qui référencent donc toujours le DC. Il faut faire ensuite un NTDSUTIL METADATACLEANUP

# Les outils de dépannage 2/3

## DFSDIAG :

Permet de valider le bon fonctionnement de la réplication DFS-R (SYSVOL).

## REPADMIN :

- Repadmin /KCC : permet de forcer l'ISTG / KCC a régénérer la topologie de réplication (liens connexions dans la console *Sites et Services Active Directory*).
- Repadmin /showrepl : permet de valider le bon fonctionnement de la réplication.
- Repadmin /options nom\_serveur +Disable\_Outbound\_REPL
- Repadmin /options nom\_serveur +Disable\_Inbound\_REPL

```
ca:\Administrateur: C:\Windows\system32\cmd.exe - ntdsutil
Microsoft Windows [version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. Tous droits réservés.
C:\Users\Administrateur.FORMATION3>ntdsutil
ntdsutil: ?
? - Afficher ces informations d'aide
Activate Instance %s - Définissez « NTDS » ou une instance AD LDS spéc
ifique
Authoritative restore - Restauration faisant autorité de la base
de données DIT
Change Service Account %s1 %s2 - Changez le compte de service AD DS/AD LDS en
non d'utilisateur %s1 et mot de passe %s2.
Utilisez « NULL » pour un mot de passe vide. *
pour
Configurable Settings - Gérer les paramètres configurables
DS Behavior - Afficher et modifier le comportement AD DS/AD L
Files - Gère les fichiers de base de données AD DS/AD L
DS
Group Membership Evaluation - Évaluer des SID dans un jeton pour un utilisateur
ou un groupe
Help - Afficher ces informations d'aide
IPM - Création d'un support IPM
LDAP policies - Gérer les stratégies de protocole LDAP
LDAP Port %d - Configurer le port LDAP pour une instance AD LD
S
List Instances - Répertoire toutes les instances AD LDS installé
es
Local Roles - Gestion des rôles RODC locaux
Metadata cleanup - Nettoyer les objets des serveurs désaffectés
Partition management - Gérer des partitions de répertoire
Popups off - Désactiver les messages
Popups on - Activer les messages
Quit - Quitter l'utilitaire
Roles - Gérer les jetons du propriétaire du rôle NTDS
Security account management - Gérer la base de données de comptes de
sécurité - nettoyage des SID en double
Semantic database analysis - Vérificateur sémantique
Set DSRM Password - Réinitialise le mot de passe du compte
Administrateur du mode Restauration du service
d'annuaire
Snapshot - Gestion des captures instantanées
SSL Port %d - Configurez le port SSL pour une instance AD LDS
.
ntdsutil: _
```

```
c:\>repadmin /showrepl
Repadmin : exécution de la commande /showrepl sur le contrôleur de domaine compl
et localhost
Default-First-Site-Name\DCFORM2
Options DSA : IS_GC
Options de site : (none)
GUID de l'objet DSA : 7bcfcc44-576f-4c82-a883-ca67c10cc68e
ID de l'invocation DSA : df34aaad-b849-4055-96e8-3bb61cecdc91

=== INSTANCES VOISINES ENTRANTES ===

DC=formation3,DC=lan
Default-First-Site-Name\DCFORM3 via RPC
GUID de l'objet DSA : 08d9a86b-2714-46f5-a4b6-82cf919b4016
La dernière tentative, le 2010-06-11 13:55:28, a réussi.

CN=Configuration,DC=formation3,DC=lan
Default-First-Site-Name\DCFORM3 via RPC
GUID de l'objet DSA : 08d9a86b-2714-46f5-a4b6-82cf919b4016
La dernière tentative, le 2010-06-11 13:55:28, a réussi.

CN=Schema,CN=Configuration,DC=formation3,DC=lan
Default-First-Site-Name\DCFORM3 via RPC
GUID de l'objet DSA : 08d9a86b-2714-46f5-a4b6-82cf919b4016
La dernière tentative, le 2010-06-11 13:55:28, a réussi.

DC=DomainDnsZones,DC=formation3,DC=lan
Default-First-Site-Name\DCFORM3 via RPC
GUID de l'objet DSA : 08d9a86b-2714-46f5-a4b6-82cf919b4016
La dernière tentative, le 2010-06-11 13:55:28, a réussi.

DC=ForestDnsZones,DC=formation3,DC=lan
Default-First-Site-Name\DCFORM3 via RPC
GUID de l'objet DSA : 08d9a86b-2714-46f5-a4b6-82cf919b4016
La dernière tentative, le 2010-06-11 13:55:28, a réussi.
```

# Les outils de dépannage 3/3

```
dcdiag.txt - Bloc-notes
Fichier Edition Format Affichage ?

Diagnostic du serveur d'annuaire

Exécution de l'installation initiale:
Tentative de recherche de serveur associé,...
* Vérification que l'ordinateur local DCFORM2 est un serveur d'annuaire
Serveur associé: DCFORM2
* Connexion au service d'annuaire sur le serveur DCFORM2.
* Format AD identifié.
Collecting AD specific global data
* Collecte des informations sur le site.
Calling ldap_search_init_page(hld,CN=Sites,CN=Configuration,DC=formation3,DC=lan
(objectCategory=ntDSSitesSettings),.....
The previous call succeeded
Iterating through the sites
Looking at base site object: CN=NTDS Site Settings,CN=Default-First
Name,CN=Sites,CN=Configuration,DC=formation3,DC=lan
Getting ISTG and options for the site
* Identification de tous les serveurs.
Calling ldap_search_init_page(hld,CN=Sites,CN=Configuration,DC=formation3,DC=lan
(objectClass=ntDSDsa),.....
The previous call succeeded....
The previous call succeeded
Iterating through the list of servers
Getting information for the server CN=NTDS Settings,CN=DCFORM3,CN=
Name,CN=Sites,CN=Configuration,DC=formation3,DC=lan
objectGuid obtained
InvocationID obtained
dnsHostname obtained
site info obtained
All the info for the server collected
Getting information for the server CN=NTDS Settings,CN=DCFORM2,CN=
Name,CN=Sites,CN=Configuration,DC=formation3,DC=lan
objectGuid obtained
InvocationID obtained
dnsHostname obtained
site info obtained
All the info for the server collected
* Identification de toutes les références croisées NC.
* 2 contrôleurs de domaine ont été trouvés. Test de 2 d'entre eux.
Collecte des informations initiales terminée.
```

Attention, en Français il y a un bug avec l'invite de commande quand on redirige une commande vers un fichier de sortie. En fait le fichier est chiffré en UTF8. Il faut donc l'enregistrer dans le bon format.

# Suppression d'un DC et nettoyage AD 1/2

## Pré-requis :

Disposez de 2 DC qui répliquent et qui sont serveur de « Catalogue Global ».

Déterminer sur quel DC les rôles FSMO sont installés. Si les rôles sont répartis, les transférer sur un unique contrôleur de domaine.

## Mise en pratique :

Sur le contrôleur de domaine qui dispose de tous les rôles FSMO, taper la commande : *DCPROMO /FORCEREMOVAL*.

De nombreux messages apparaissent expliquant quels sont les conséquences de la suppression en mode forcée du contrôleur de domaine qui héberge les rôles FSMO / Catalogue global.

Saisir un nouveau mot de passe administrateur local (la base SAM va être recréée).

### Assistant Installation des services de domaine Active Directory



Ce contrôleur de domaine Active Directory tient actuellement le rôle de maître d'opérations de l'émulateur du contrôleur de domaine principal (PDC). Si vous supprimez les services de domaine Active Directory (AD DS) de cet ordinateur, les opérations réalisées par l'émulateur PDC, telles que les mises à jour des stratégies de groupes et les réinitialisations de mots de passe pour les comptes ne faisant pas partie des services de domaine Active Directory, ne fonctionneront pas correctement.

Avant de continuer, transférez le rôle de maître d'émulateur PDC vers un contrôleur de domaine appartenant au même domaine que ce contrôleur de domaine.

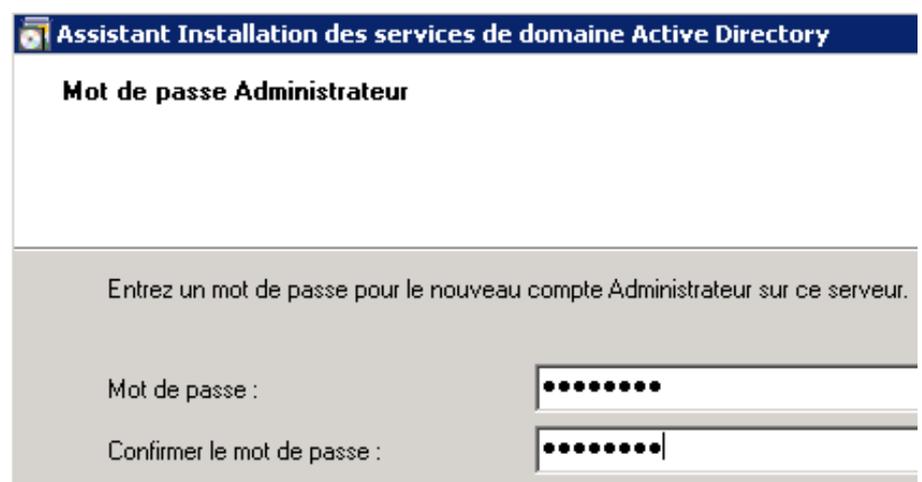
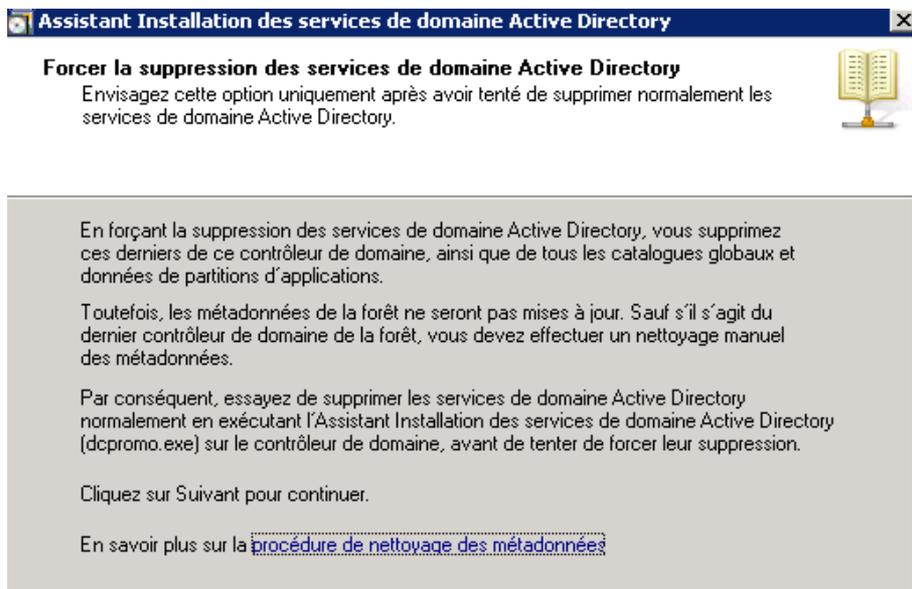
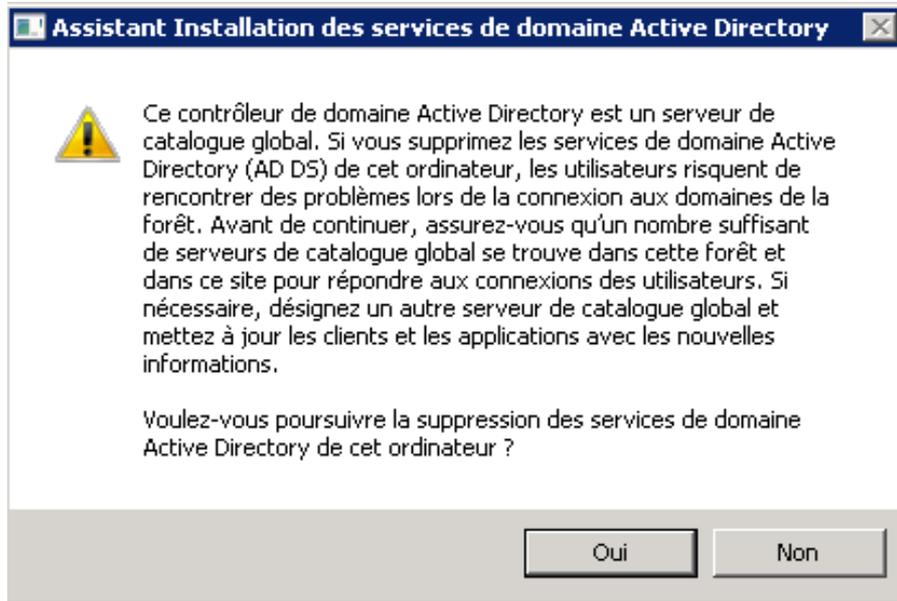
Si le transfert est impossible, supprimez d'abord les services de domaine Active Directory de cet ordinateur, puis utilisez Ntdsutil.exe pour prendre le rôle. Ntdsutil.exe s'utilise sur le contrôleur de domaine qui va prendre le rôle ; si possible, utilisez un partenaire de réplication récent appartenant au même site que ce contrôleur de domaine.

Important : le rôle de maître d'émulateur PDC est le seul rôle que vous pouvez prendre avant de supprimer les services de domaine Active Directory. Pour tous les autres rôles de maître d'opérations, vous devez supprimer les services de domaine Active Directory avant de prendre le rôle.

Pour plus d'informations sur le transfert et la prise de rôles de maître d'opérations, voir l'article 255504 de la Base de connaissances Microsoft (<http://go.microsoft.com/fwlink/?LinkId=80395>).

Voulez-vous poursuivre la suppression des services de domaine Active Directory de cet ordinateur ?

# Suppression d'un DC et nettoyage AD 2/2



# Suppression d'un DC en mode forcé

A ne faire que si la suppression du contrôleur de domaine échoue !

Toujours faire une sauvegarde de l'annuaire (sauvegarde complète avec Windows Server Backup).

Configurer l'ancien DC en tant que serveur en groupe de travail :  
Exécution de la commande *DCPROMO /FORCEREMOVAL*

Ouvrir un invite de commande et lancer l'utilitaire NTDSUTIL.

Utiliser l'utilitaire NTDSUTIL pour supprimer les références à l'ancien contrôleur de domaine. **Attention une simple suppression du compte ordinateur en suffit pas!** Pour cela appliquer l'article Microsoft suivant :

<http://support.microsoft.com/kb/216498/en-us>

Ne pas se tromper au niveau de la partie « *Select Operation target* ». On sélectionne le DC que l'on veut supprimer.

Forcer le transfert des rôles FSMO (avec l'outil NTDSUTIL). Pour cela appliquer l'article Microsoft suivant : <http://support.microsoft.com/kb/255504>

Procédure à appliquer avec les DC 2012 et versions ultérieures :

<https://www.petri.com/demoting-a-windows-server-2016-domain-controller>

# Les outils de migration / restructuration 1/2

## **Migration de ressources entre forêts / fusion de deux forêts en une seule :**

Utilisation de l'outil ADMT 3.1 / ADMT 3.2 (pas de prise en charge des annuaires gérés par des contrôleurs de domaine Windows 2000).

Utilisation de l'attribut SID History.

Les ressources sont copiés entre le domaine source et le domaine cible. Commencer par migrer tous les groupes, puis tous les comptes utilisateurs. Migrer ensuite les comptes ordinateurs par lots.

Attention lors de la suppression de l'ancien domaine, les anciens SID ne sont plus résolus. Il faut donc lancer l'assistant translation des SID sur tous les serveurs. Voir outil tiers pour les NAS NETAPP / EMC...

L'agent ADMT exécute un script qui va permettre de changer la machine de domaine et de translater les SID. Lancer l'outil avec un compte utilisateur du domaine source (compte membre du groupe administrateur du domaine source et BUILTIN\Administrateurs dans le domaine cible).

<http://msreport.free.fr/?p=131>

<http://msreport.free.fr/?p=145>

# Les outils de migration / restructuration 2/2

## **Fusion de deux domaines dans la même forêt :**

Outils : Microsoft ADMT (gratuit) ou Quest Migration Manager (payant).

Les ressources sont déplacées avec ADMT. Il faut migrer les groupes (les passer en groupes universelles) puis migrer par les lots les comptes utilisateurs / comptes ordinateurs.

L'agent ADMT exécute un script qui va permettre de changer la machine de domaine et de traduire les SID. Lancer l'outil avec un compte utilisateur du domaine source (administrateur du domaine source et BUILTIN\Administrateurs dans le domaine cible).

<http://www.microsoft.com/downloads/details.aspx?familyid=6D710919-1BA5-41CA-B2F3-C11BCB4857AF&displaylang=en>

## **Mise à jour des contrôleurs de domaine :**

Utilisation de l'outil ADPREP pour mettre à jour le schéma Active Directory.

Migration par ajout et suppression de contrôleurs de domaine.

[http://technet.microsoft.com/en-us/library/cc731728\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc731728(WS.10).aspx)

<http://www.petri.co.il/windows-server-2008-adprep.htm>

# 11. Les services réseaux :

# Le service DHCP

Permet d'affecter dynamiquement une adresse IP à des stations de travail.

Réservation IP : affectation d'une IP à une adresse MAC (utile pour les imprimantes ou les éléments dont l'IP ne doit pas changer).

Le service DHCP de Windows s'interface avec le service DNS. Le serveur DHCP peut mettre à jour les enregistrements DNS dynamiques à la place des stations de travail.

Il est nécessaire d'autoriser le serveur DHCP sur une machine membre / contrôleur d'un domaine (nécessite les droits administrateur de l'entreprise).

Activer la détection des conflits IP (au niveau des propriétés du serveur DNS).

Cocher la case « *Ignorer les enregistrements A et PTR lorsque le bail est supprimé* ».

Pour les problèmes avec les mises à jour dynamiques DNS : voir

<http://msreport.free.fr/?p=208>

## **Quelques problèmes connus :**

Croix rouge au niveau des baux DHCP : <http://msreport.free.fr/?p=120>

Erreurs DHCP 1010 / 1014 : <http://msreport.free.fr/?p=95>

Doublons dans les zones DNS : <http://msreport.free.fr/?p=75>

# TP : le service DHCP

**Déconnecter la salle du cours du réseau d'entreprise ou faire sur des machines virtuelles dans un réseau isolé.**

**Faire ce TP par groupe de 2.**

Installer le service DHCP (ajout du rôle depuis le Gestionnaire de Server).

Créer une étendue DHCP avec deux adresses (voir formateur) et la configurer pour affecter une adresse de serveurs DNS / Wins / passerelle).

Tester le fonctionnement de l'étendue. Que se passe t'il ?

Tester les commandes `ipconfig /release` et `ipconfig /renew` et `ipconfig /all`

Arrêter tous les serveurs DHCP. Faire un `ipconfig /release` et un `ipconfig /renew`.

Que se passe t'il ?

Créer une réservation IP.

# Le WINS / LMHOST

Wins : *Windows Internet Naming Service*

Protocole permettant de résoudre des noms NETBIOS (toto) en adresse IP.  
Utiliser aujourd'hui encore pour accélérer l'affichage du voisinage réseau.

## Mise en pratique :

Avec le bloc Note, ouvrir le fichier *C:\WINDOWS\system32\drivers\etc\lmhosts.sam*. A quoi sert ce fichier ?

Installer le service WINS (Ajout de fonctionnalités dans le Gestionnaire de Server).

Configurer le serveur pour s'enregistrer dans la base WINS (paramètres TCP / IP, paramètres avancées).

Créer un enregistrement www avec comme IP 192.168.0.1. Faire un ping de www puis un nbstat -n puis nbtstat -R. Qu'est ce qu'est le cache Wins.

Configurer votre serveur WINS pour être partenaire de réplication avec un autre serveur WINS.

Renommer le fichier LMHOST.SAM en LMHOST et configurer Windows pour utiliser ce fichier. Créer une entrée dans ce fichier et conclure.

Présenter le fonctionnement du voisinage réseau et exécuter la commande « *Browstat status* ». Qu'est ce qu'un master browser ?

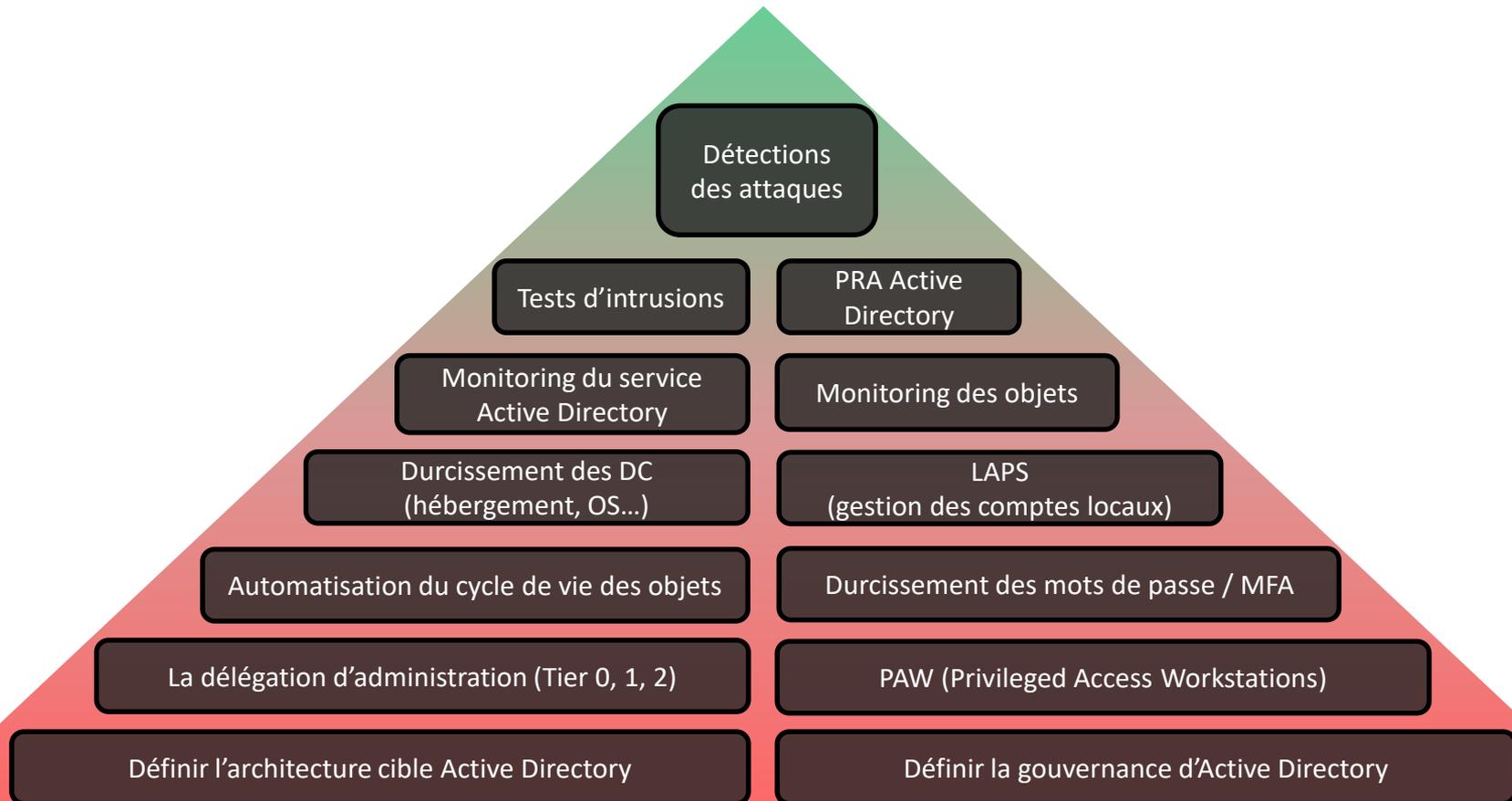
Lire article <http://msreport.free.fr/?p=129>.

# **11. Sécuriser son annuaire Active Directory :**

# La sécurité en 2019 : quelques chiffres

- **280 jours** : délais pour détecter une attaque
- **63 jours** : délais pour s'en remettre
- **20 minutes** (Petya) : 2000 machines, 100 serveurs, sauvegarde HS
- **81 %** : les entreprises françaises ciblées par une attaque informatique en 2015.
- **35 %** : source de l'incident de sécurité, l'équipe IT
- **800 000 euros** : prix (moyenne) pour s'en remettre

# La méthodologie pour sécuriser son AD



# Faire un état des lieux de la sécurité de son AD

Avec Ping Castle, c'est gratuit et automatique !

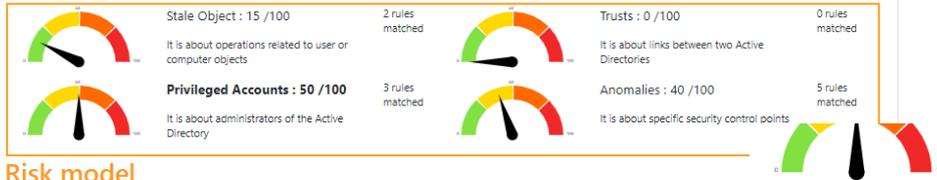
<https://www.pingcastle.com/>

## Indicators



Domain Risk Level: 50 / 100

It is the maximum score of the 4 indicators and one score cannot be higher than 100. The lower the better



## Risk model

Stale Objects	Privileged accounts	Trusts	Anomalies
Inactive user or computer	ACL Check	Old trust protocol	Backup
Network topography	Admin control	SID Filtering	Certificate take over
Object configuration	Irreversible change	SIDHistory	Golden ticket
Obsolete OS	Privilege control	Trust impermeability	Local group vulnerability
Old authentication protocols		Trust inactive	Network sniffing
Provisioning			Pass-the-credential
Replication			Password retrieval
Unfinished migration			Reconnaissance
Vulnerability management			Temporary admins
			Weak password

Legend:

- score is 0 - no risk identified but some improvements detected
- score between 1 and 10 - a few actions have been identified
- score between 10 and 30 - rules should be looked with attention
- score higher than 30 - major risks identified

## Privileged Accounts rule details [3 rules matched]

Presence of Admin accounts which have not the flag "this account is sensitive and cannot be delegated": 1 + 20 Point(s)

The native administrator account has been used recently: 0 day(s) ago + 20 Point(s)

### Check for Native administrator usage

**Description:**  
The purpose is to verify if the Native Administrator account is used.

**Technical explanation:**  
The Native Administrator account is the main administrator account, and it is sharing its password with Directory Services Restore Mode password. Since it is the same password, it can be used to take control of the domain even if the account is disabled, notably through a DSsync attack. The last login date is retrieved through the LastLogonTimestamp LDAP attribute retrieved from the Active Directory. There is an exception for 35 days to avoid this rule to be triggered at the domain creation.

**Advised solution:**  
To mitigate the security risk, a good practice is to use the Native Administrator account only for emergency, while the daily work is performed through other accounts. It is indeed strongly recommended to not use this account but to use nominative account for administrators and dedicated account for services. Do note that the anomaly will be removed 35 days after the last native administrator login.

To track where the administrator account has been used for the last time, we recommend to extract the attribute LastLogon of the administrator account on ALL domain controllers. It can be done with tools such as ADSIEdit or ADEplorer. Then, for each domain controller, extract the events 4624 at the date matching the LastLogon date. You will identify the computer and the process at the origin of the logon event.

Please note that PingCastle relies on the attribute LastLogonTimestamp to perform this check. The LastLogonTimestamp attribute is replicated but has a latency of a maximum of 14 days, while LastLogon is updated at each logon and is more accurate but not replicated.

**Points:**  
20 points if the occurrence is strictly lower than 35

**Documentation:**  
<https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/implementing-least-privilege-administrative-models>

# Outils pour faire des tests d'intrusion Active Directory

## Principaux outils de tests d'intrusion :

*Cain, DSInternal, Metasploit, Mimikatz, PowerSploit, PSEXEC*

## Méthodologie d'attaques :

Élévation de privilèges, mouvement latéral, social engineering, altération des fichiers du système.

## Scénario d'attaque :

Je deviens administrateur local de la machine (via une faille de sécurité, en copiant / renommant *CMD.EXE* par *SETHC.EXE* en console de récupération).

Une fois administrateur local, j'escalade en tant que *SYSTEM* (*PSEXEC -i -s cmd*).

Une fois *SYSTEM*, je me connecte à la mémoire du processus *LSASS.EXE* de la machine pour des Hash de mots de passe de compte à fort privilège.

Je me connecte via ses comptes à fort privilèges à d'autres machines.

Je fouille la mémoire du processus *LSASS.EXE* d'autres machines jusqu'à devenir *Domain Admins / Enterprise Admins*.

Je me crée un Golden Ticket pour disposer d'une porte dérobée pour rentrer sur l'annuaire AD quand je le souhaite.

# Les actions pour sécuriser son AD

Visionner les vidéos suivantes :

Msreport - durcissement de la sécurité Active Directory - vue d'ensemble

<https://youtu.be/RoD1w5nQck4>

Msreport - les élévations de privilèges Active Directory et comment les détecter

<https://youtu.be/qHKVQ76lpAU>

Lire le guide “*Tester la sécurité de son annuaire Active Directory*”.

<http://msreport.free.fr/articles/Securite->

[AD/TESTER\\_SECURITE\\_ACTIVE\\_DIRECTORY\\_V\\_2.0.pdf](http://msreport.free.fr/articles/Securite-AD/TESTER_SECURITE_ACTIVE_DIRECTORY_V_2.0.pdf)