

Windows Server

Version 2020

Module 1

Résumé de l'adressage IPv4 et IPv6

1. Structure

IPv4

- Adresse de 32 bits
- Codage en 4 paquets de 8 bits
- Notation décimale : xxx.xxx.xxx.xxx
- $2^{32} = 4\ 294\ 967\ 296$ adresses possibles
- Exemples :
 - 193.168.1.10
 - 11000001.10101000.00000001.00001010

IPv6

- Adresse de 128 bits
- Codage en 8 paquets de 16 bits
- Notation hexadécimale :
xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx
- $2^{128} = 3,4 \times 10^{38}$
 6×10^{23} adresses/m²
- Exemples :
 - 5cf0:607c:2d4a:6978:abfe:7d96:a782:ab55
 - 2001::1

2. Types de transmission des données

IPv4

- Unicast
- Multicast
- Broadcast



IPv6

- Unicast
- Multicast
- Anycast (le plus proche ou le plus efficace)



3. Les parties

IPv4

- Net_id de longueur variable
- Host_id de longueur variable
- Longueur déterminée par le masque de sous-réseaux
 - Net_id à 1 et Host_id à 0
 - Notation CIDR
 - Adresse IPv4/longueur du Net_id en bits

IPv6

- 64 premiers bits : le préfixe
- 64 derniers bits : Identifiant de l'interface
- Une machine peut avoir plusieurs préfixes
 - Un lien local
 - Un global
- Le préfixe détermine le type d'adresse (anycast, ...)
- Représentation des préfixes : CIDR
 - Adresse Ipv6/longueur du préfixe en bits

CIDR : Classless Inter-Domain Routing

4. IPv4 - Détail du nombre d'adresses

Classe	Bloc 1	Bloc 2	Bloc 3	Bloc 4	Max de réseaux	Max d'hôtes	Bits de départ	Valeurs Bloc1
A	net_id		host_id		126	16777214	0	1 à 126
B		net_id		host_id	16384	65534	10	128 à 191
C		net_id		host_id	2097152	254	110	192 à 223
D			Multicast			1110		224 à 239
E			Réservée			1111		240 à 255

5. IPv4 - Généralités

- Les sous-réseaux

Adresse IPv4		
Réseau	sous-réseau	Hôte

- Planification des adresses IPv4
 - Ne peut pas commencer par 127 (127.0.0.1 : adresse de loopback)
 - Le net_id et le host_id ne peuvent pas être tout à 0_b ou 1_b
- Notation CIDR à privilégier (/n)
 - Calcul du nombre d'hôtes : $2^{(32-n)} - 2$
 - Calcul du nombre de réseaux : $32 - ((\ln(\text{nbr d'hôtes}+2)) / \ln(2))$

6. IPv4 - Adresses privées

- Adresses ne pouvant pas transiter par Internet
- Adresses routables dans les LAN

Préfixe		Plage IP
10.0.0.0/8	10.0.0.1	10.255.255.255
172.16.0.0/12	172.16.0.0	172.31.255.255
192.168.0.0/16	192.168.0.0	192.168.255.255

8. IPv6 - Préfixes

- Types d'adresses unicast
 - Lien local : Non routable
 - Global : Routable sur Internet
 - Site local supprimée pour les « unicast local unique » : Organisation locale
- Préfixes généraux :

– Lien local :	1111 1110 10	fe80/10
– Site local :	1111 1110 11	fec0/10
– Local Unique:	1111 110	fc00/7
– Multicast :	1111 1111	ff00/8
– Global :	le reste	
	Adresse attribuée par l'IANA :	2000::/3
- Adresses spéciales :
 - Loopback : ::1
 - Any : :: (adresse affectée à une destination, utilisée par les protocoles d'initialisation)

9. IPv6 - Ecriture

- Règles d'écriture
 - 128 bits réduits à 32 caractères hexadécimaux
 - Caractères regroupés par 16 bits (2 octets) séparés par 2 points
 - Les zéros leaders de chaque bloc peuvent être omis
 - Les séquences de 16 bits à 0 peuvent être remplacés par ::
- Forme préférée :

x:x:x:x:x:x:x où x = nbr héxa

5f06 :b500 :89c2 :a100 :0000 :0800 :200a :3ff7
- Forme abrégée : groupe de 16 bits à 0 = « :: »

ff80:0:0:0:800:200a:3ff7

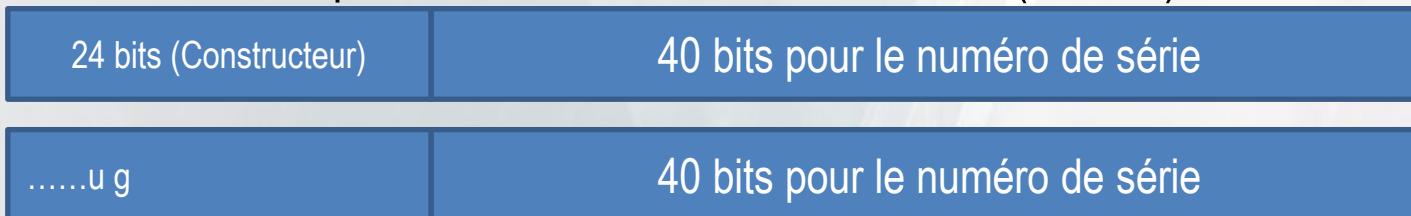
ff80 ::800 :200a :3ff7
- Forme mixée : mélange IPv4 et IPv6

x:x:x:x:x:d.d.d.d

::137.194.168.93

10. IPv6 – AutoConfig Interface (1)

- Règle pour l'auto configuration automatique d'une adresse d'interface
 - Les 64 derniers bits déterminent l'interface déduite de l'adresse MAC
 - Nouvelle norme pour les adresses MAC sur 64 bits (EUI-64)



7 ^e bit : bit u (universel)	→ 0 si universel 1 si affecté manuellement
8 ^e bit : bit g (groupe)	→ 0 si l'adresse est individuelle 1 si adresse de groupe (multicast)

- L'identifiant IPV6 de l'interface est dérivé de cette règle à un détail près la signification du bit u est inversée. Il vaut 1 si universel et 0 si manuel.

10. IPv6 – AutoConfig Interface (2)

– Cas actuel avec adresse MAC de 48 bits (EUI-48)

- 24 premiers bits identifient le constructeur avec inversion du 7^e bit.
- 16 bits ont la valeur FFFE.
- 24 bits suivant identifient le numéro de série.

.....u g 24 bits : constructeur

24 bits : numéro de série

Adresse MAC IEEE

.....u g 24 bits : constructeur

FF FE (16 bits)

24 bits : numéro de série

Identifiant EUI-64

.....1 0 24 bits : constructeur

FF FE (16 bits)

24 bits : numéro de série

Identifiant interface IPv6

11. IPv6 – AutoConfig lien local

- Règle pour l'auto configuration d'une adresse « lien local »
- Adresses dont la validité est restreinte à un lien c'est à dire sans routeur intermédiaire.
- Communication entre nœuds voisins :
 - même réseau de couche 2 (exemple : Vlan Ethernet)
 - connexion point à point (ex PPP)
 - extrémités de tunnel (ex IPSEC)
- Ses caractéristiques sont:
 - unicité (=> protocole de détection de duplication d'adresses : algorithme DAD avec ICMPv6)
 - non routable : un routeur ne retransmet jamais un paquet ayant une adresse source ou destination de type lien local
- On concatène le préfixe **fe80::/64** aux 64 bits de l'identifiant de l'interface.

12. IPv6 – Adresses globales

- Configuration d'une adresse IPv6 globale
- Trois niveaux de hiérarchie dans le préfixe
 - Topologie publique : 48 bits dont 3 fixes (TLA : Top Level Aggregation)
 - Topologie de site : 16 bits (coder les sous-réseaux du site) (SLA : Sub L A)
 - Identifiant de l'interface : 64 bits



13. IPv6 - RIPE

- RIPE : Réseaux IP Européens
- RIPE NCC : RIPE Network Coordination Centre
- 2001:600::/16



14. IPv6 – Windows Autoconfig

- Par défaut Windows fait l'autoconfiguration avec un nombre aléatoire
- Commandes pour mettre l'autoconfiguration « normale »
 - Netsh interface ipv6 set privacy state=disabled store=active
 - Netsh interface ipv6 set privacy state=disabled store=persistent
 - Netsh interface ipv6 set global randomizeidentifiers=disabled store=active
 - Netsh interface ipv6 set global randomizeidentifiers=disabled store=persistent

15. IPv6 - Interfaces

```
Administrator: Command Prompt

WINS Proxy Enabled . . . . . : No
DNS Suffix Search List . . . . . : ioluaxvtysaelltmzrsm3y2wfa.bx.internal.cl
oudapp.net

Ethernet adapter Ethernet:

  Connection-specific DNS Suffix . . . . . : ioluaxvtysaelltmzrsm3y2wfa.bx.internal.cl
oudapp.net
    Description . . . . . : Microsoft Hyper-V Network Adapter
    Physical Address . . . . . : 00-0D-3A-11-8B-B6
    DHCP Enabled . . . . . : Yes
    Autoconfiguration Enabled . . . . . : Yes
    Link-local IPv6 Address . . . . . : fe80::e9c2:1bd8:df9e:4a2a%12(PREFERRED)
    IPv4 Address . . . . . : 10.0.0.4(Preferred)
    Subnet Mask . . . . . : 255.255.255.0
    Lease Obtained . . . . . : Wednesday, March 16, 2016 11:09:50 AM
    Lease Expires . . . . . : Saturday, April 22, 2152 7:57:11 PM
    Default Gateway . . . . . : 10.0.0.1
    DHCP Server . . . . . : 168.63.129.16
    DHCPv6 IAID . . . . . : 301993274
    DHCPv6 Client DUID . . . . . : 00-01-00-01-1E-73-09-8E-00-0D-3A-11-8B-B6

  DNS Servers . . . . . : 168.63.129.16
  NetBIOS over Tcpip . . . . . : Enabled
```

%12 = spécifie l'interface

```
C:\Users\AzureAdmin>netsh interface ipv6 show interface
Idx      Met      MTU      State      Name
---  -----
  1        50    4294967295  connected  Loopback Pseudo-Interface 1
  13       50        1280  disconnected  isatap.1oluaxvtysaelltmzrsm3y2wfa.bx.
internal.cloudapp.net
  14       50        1280  connected   Teredo Tunneling Pseudo-Interface
  12        5        1500  connected   Ethernet
```

15. Exercices IPv4 et IPv6

Module 2

Windows Server

1. Les différents OS

OS Clients

- Win 3.x
- Win 95
- Win 98 et 98 se
- Win Me
- Win 2000 pro
- Win XP (Home + Pro)
- Win Vista (Basique, Premium, Pro, Enterprise, Intégrale)
- Win 7 (familiale, Pro et Intégrale)
- Win 8 et 8.1
- Win 10

OS serveurs

- Win NT 4.0
- Win 2000 server
- Win 2003 server + R2
- Win 2008 server +R2
- Win 2012 server + R2
- Win 2016 server
- Win 2019 server

2. Comparaison des versions server

- Comparaison des différentes versions de Windows server de 2008R2 à 2019
- <https://www.microsoft.com/fr-fr/cloud-platform/windows-server-comparison>

3. Les différentes versions server (1)

Windows server 2008 R2

- Standard avec ou sans Hyper-V
- Enterprise
- Datacenter
- Foundation
- HPC Server
- Web Server
- Storage Server
- Small Business Server
- Essential Business Server
- Pour Systèmes Itanium-based

Windows 2012 R2

- Foundation
 - OEM et pas d'Hyper-V
 - 15 utilisateurs; pas de CAL
 - Pas de CAL
 - Mono-processeur
- Essentials
 - PME
 - Pas d'Hyper-V
 - Virtualisable
 - Mono ou bi processeur
 - 25 utilisateurs pas de CAL
- Standard
 - Hyper-V pour 2 VM
- Datacenter
 - Infra fortement virtualisée
 - Private cloud

3. Les différentes versions server (2)

- Pour Windows Server 2019 :
 - Essentials : petites et moyennes entreprises (25 users et 50 devices)
 - Standard
 - Datacenter : Datacenters et environnement cloud hautement virtualisés
- Tarification et licences : <https://www.microsoft.com/fr-be/cloud-platform/windows-server-pricing>

4. CAL

- CAL : Client Access License
- Définition (source Wikipédia) :

« Les **licences d'accès client** (CAL) sont une sorte de logiciel qui permet à un utilisateur ou à un équipement de se connecter légalement à un serveur Microsoft. Ces licences sont vendues soit à l'achat du serveur (licences OEM), soit sous forme d'un contrat de licence. Certains logiciels, tel que [Windows Small Business Server 2003](#), nécessitent une activation des CAL sur le serveur alors que d'autres, tel qu'[Exchange 2010](#), n'ont pas besoin de cette procédure. Les CAL sont toujours attribués à un utilisateur ou à un équipement, il est donc nécessaire d'avoir autant de CAL que d'utilisateurs et/ou d'équipements. Certains logiciels serveurs, enfin, ne nécessitent pas de CAL du tout, c'est par exemple le cas de Windows Server Web Édition. »

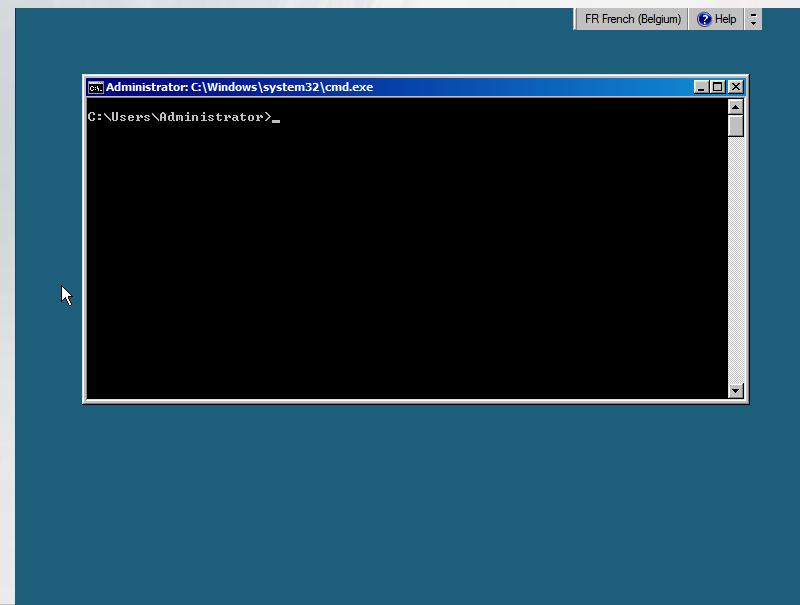
5. Installation OS

- Classique...
- Automatique
 - Service RIS : Remote Installation Services (Win Server 2003)
 - Service WDS : Windows Deployment Services (à partir de Win 2008)
- WDS – Avantages
 - Rapide
 - Déploiement de masse
 - GUI
 - Automatisation
 - ...

6. Types d'installations

A partir de Windows Server 2008

- 2 types d'installations possibles :
 - Installation complète (avec GUI)
 - Installation en mode « Core » (Pas d'interface graphique, toutes les fonctionnalités ne sont pas disponibles)

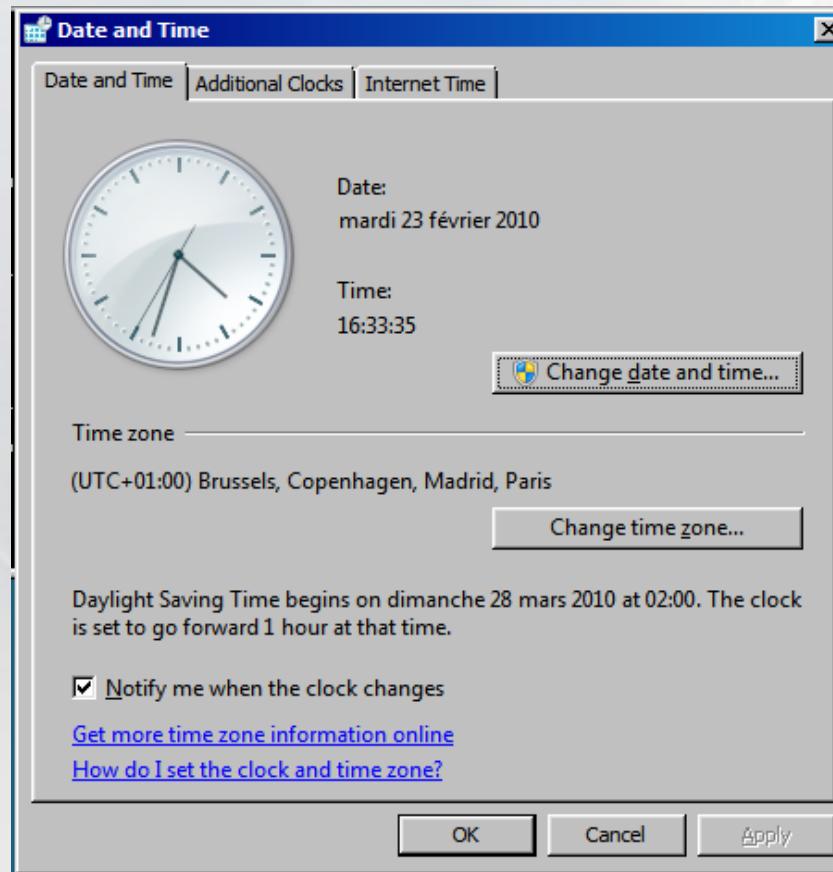


Module 3

Windows Server en mode Core

1. Configuration du fuseau horaire

- Control timedate.cpl



2. Configuration de l'interface réseau

- Netsh interface ipv4 show interfaces
- Adresse IP Fixe
 - Netsh interface ipv4 set address name=« `Idx` » source=static address=<adresse IP> mask=<Masque de sous réseau> gateway=<IPGw>
 - Netsh interface ipv4 add dnsserver name=« `Idx` » address=« `IP` » index=« Position DNS »
- Adresse via DHCP
 - Netsh interface ipv4 set address name=« `Idx` » source=dhcp
 - Netsh interface ipv4 delete dnsserver name=« `Idx` »
 - Netsh interface ipv4 set dnsserver name =« `Idx` » source=dhcp

3. Commandes diverses (1)

- Activation de Windows via Internet
 - Slmgr.vbs –ato
- Renommer l'ordinateur
 - Netdom renamecomputer %computername% /newname : <Nouveau nom>
- Redémarrer le serveur (après 3 sec)
 - Shutdown /r /t 3
- Déconnexion
 - Logoff
- Arrêter le serveur (après 5 sec)
 - Shutdown /s /t 5

3. Commandes diverses (2)

- Activer les mises à jours automatiques
 - Cscript %windir%\system32\scregedit32.wsf /au 4
 - 4 pour activer; 0 pour désactiver
- Modification du mot de passe
 - Net user administrator *
- Modification des paramètres régionaux
 - Control intl.cpl
- Joindre un domaine
 - Netdom join localhost /domain:<nom du domaine> /userd:Domaine\Administrator /passwordd:*
 - Sortir le serveur du domaine remplacer join par remove

3. Commandes diverses (3)

- Activation du bureau à distance
 - Pour RDP 6.1
`Cscript %windir%\system32\scregedit.wsf /ar 0`
 - Pour RDP 6.0
`Cscript %windir%\system32\scregedit.wsf /cs 0`
- Autoriser la gestion du pare-feu à distance
 - `Netsh advfirewall set currentprofile settings remotemanagement enable`
- Autoriser la gestion à distance à l'aide de la console MMC
 - `Netsh advfirewall firewall set rule group=« Administration distante » new enable=yes`
- Activer Windows RemoteShell
 - `Winrm quickconfig`

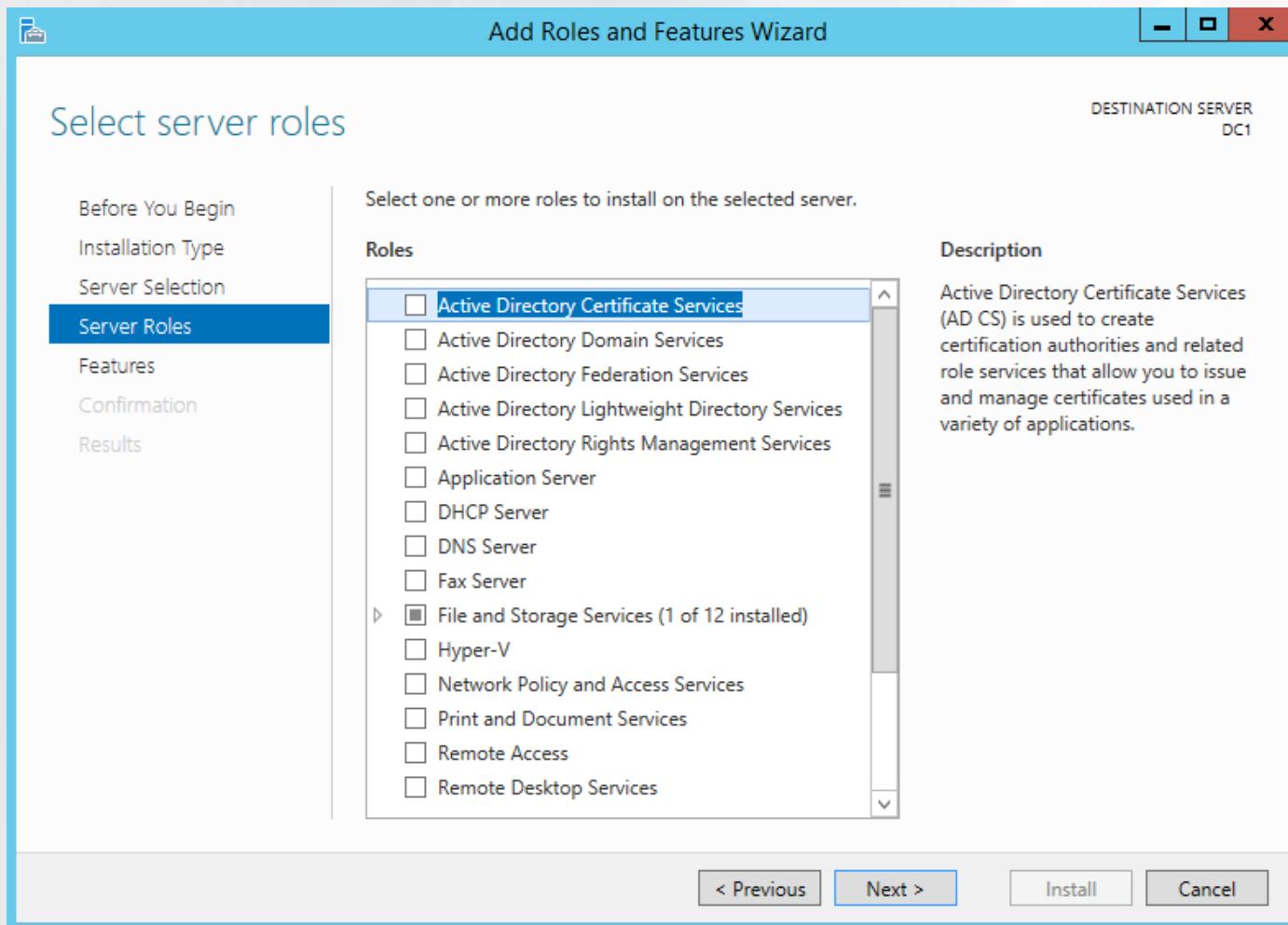
Module 4

Rôles et fonctionnalités

1. Rôles

- **Rôle** : *Un rôle de serveur est un ensemble de programmes logiciels qui, une fois installés et correctement configurés, permettent à un ordinateur de remplir une fonction spécifique pour plusieurs utilisateurs ou pour d'autres ordinateurs sur un réseau.*
- **Service de rôle** : sous-ensemble d'un rôle.
Les services de rôle sont des programmes logiciels qui fournissent la fonctionnalité d'un rôle.
 - Avantage : diminution de la surface d'attaque

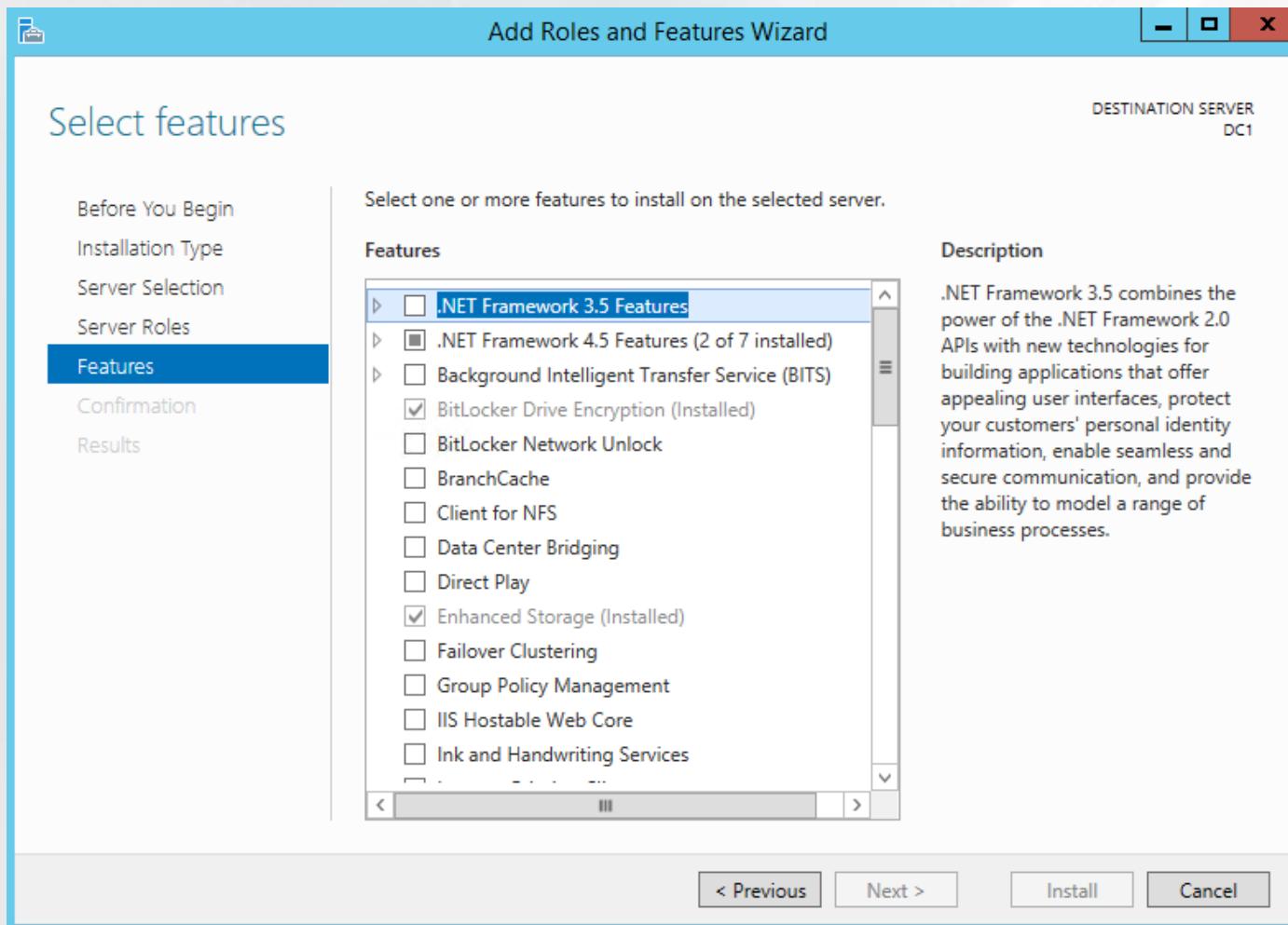
2. Exemples de rôles



3. Fonctionnalités

- Fonctionnalités : *Les fonctionnalités sont des programmes logiciels qui, bien que ne faisant pas directement partie des rôles, peuvent prendre en charge ou augmenter la fonctionnalité d'un ou de plusieurs rôles, ou encore améliorer la fonctionnalité de la totalité du serveur, quels que soient les rôles installés.*
- Composants optionnels

4. Exemples de fonctionnalités

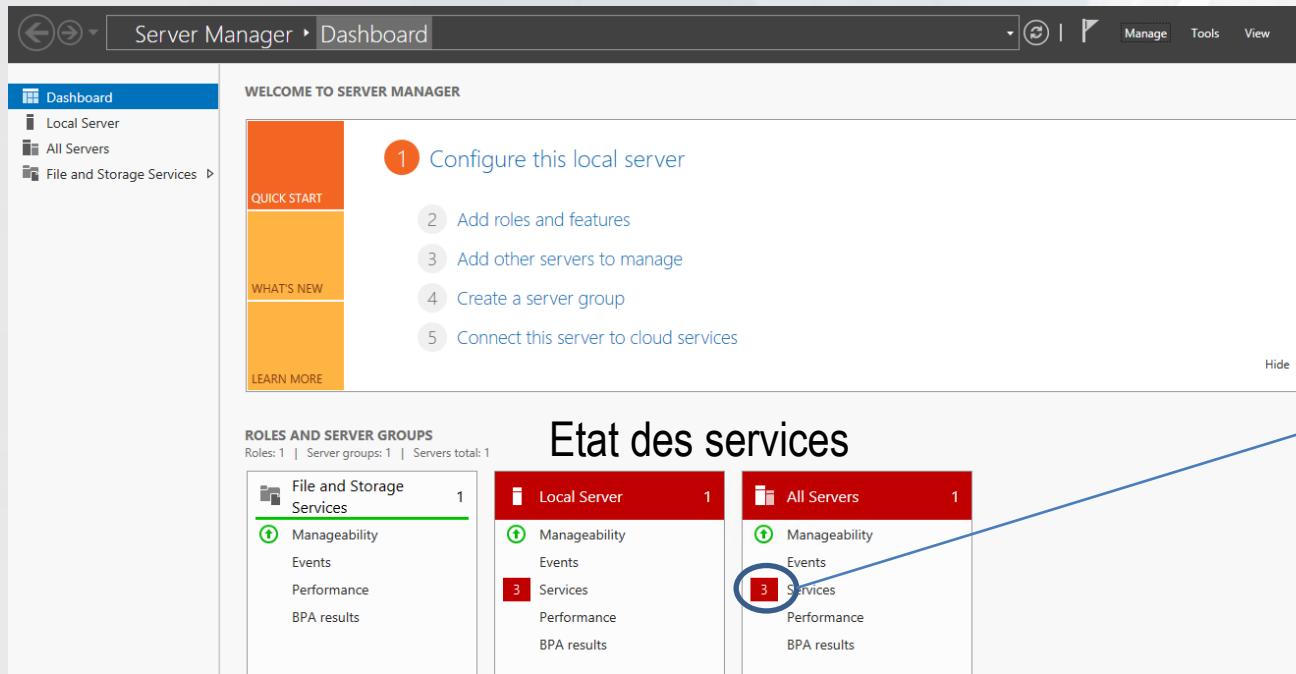


5. Installer/Désinstaller Rôles ou fonctionnalités

- Via le gestionnaire de serveur : **Start – Administrative Tools – Server manager**
- Via la commande : ServerManagerCmd
- Via la commande ocsetup et oclist
- Via la commande pkgmgr

6. Server Manager (1)

- Gestion de l'ensemble du serveur
- Ajout/suppression de rôles et de fonctionnalités
- Gestion des PC distants



The screenshot shows the Microsoft Server Manager dashboard. The top navigation bar includes back, forward, search, and manage buttons, along with links for Tools, View, and Help. The main area is titled "WELCOME TO SERVER MANAGER". It features a "QUICK START" section with five numbered steps: 1. Configure this local server, 2. Add roles and features, 3. Add other servers to manage, 4. Create a server group, and 5. Connect this server to cloud services. Below this is a "WHAT'S NEW" section and a "LEARN MORE" button. A "Hide" link is located in the bottom right corner of the quick start area. The "ROLES AND SERVER GROUPS" section displays the following data:

Category	Count
File and Storage Services	1
Local Server	1
All Servers	1

Under "File and Storage Services", there are four items: Manageability, Events, Performance, and BPA results. Under "Local Server", there are four items: Manageability, Events, Performance, and BPA results. Under "All Servers", there are four items: Manageability, Events, Services (which is circled in red), and BPA results. The "Etat des services" section shows the same service counts: 1 for File and Storage Services, 1 for Local Server, and 1 for All Servers. A blue arrow points from the text "Nombre de service en erreur." to the "Services" item under "All Servers".

Nombre de service en erreur.
En cliquant, une fenêtre présente les détails

6. Server Manager (2)

Configuration du serveur : Nom, Domaine, IP,

- [Dashboard](#)
- [Local Server](#)
- [All Servers](#)
- [File and Storage Services](#)

PROPERTIES For DC1

Computer name	DC1	Last installed updates	Never
Workgroup	WORKGROUP	Windows Update	Install updates automatically using Windows Update
		Last checked for updates	Today at 11:33 AM
Windows Firewall	Public: On	Windows Error Reporting	Off
Remote management	Enabled	Customer Experience Improvement Program	Not participating
Remote Desktop	Enabled	IE Enhanced Security Configuration	On
NIC Teaming	Disabled	Time zone	(UTC) Coordinated Universal Time
Ethernet	IPv4 address assigned by DHCP, IPv6 enabled	Product ID	00253-50000-00000-AA189 (activated)
Operating system version	Microsoft Windows Server 2012 R2 Datacenter	Processors	AMD Opteron(tm) Processor 4171 HE
Hardware information	Microsoft Corporation Virtual Machine	Installed memory (RAM)	1.75 GB
		Total disk space	167 GB

EVENTS

All events | 13 total

Server Name	ID	Severity	Source	Log	Date and Time
DC1	36888	Error	Schannel	System	3/16/2016 1:42:15 PM
DC1	36888	Error	Schannel	System	3/16/2016 1:42:15 PM

Configuration renforcée d'Internet Explorer (par défaut sur les serveurs ON)

Effective User



 WALLONIE-BRUSSLES
 ENSEIGNEMENT



 ENSEIGNEMENT OFFICIEL

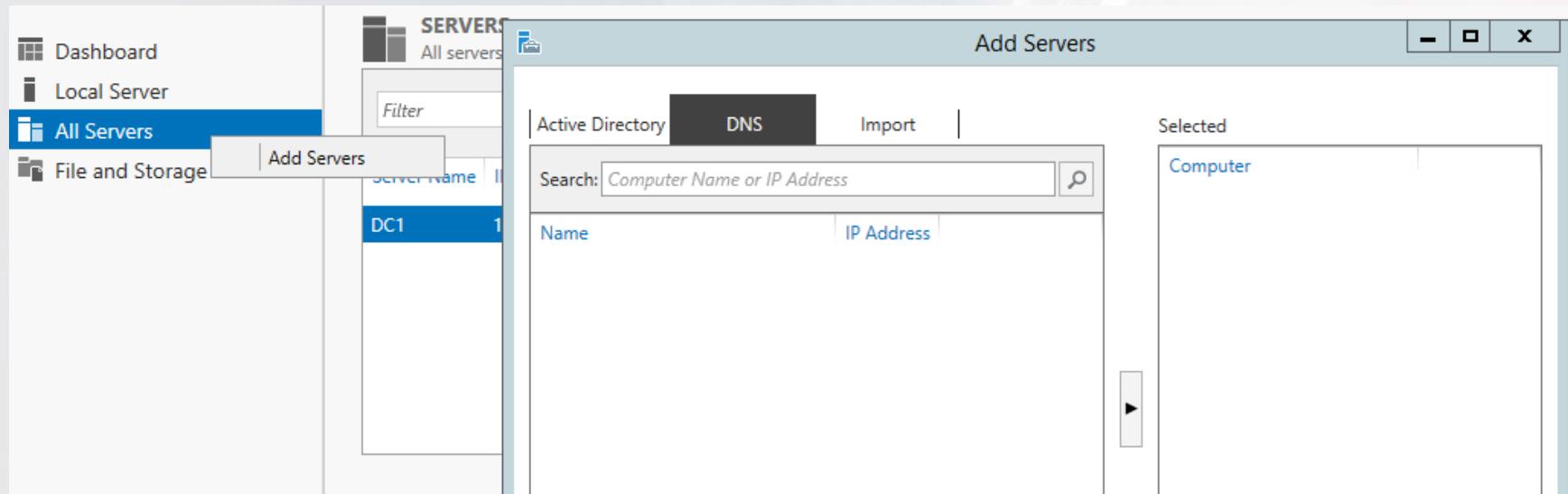
www.heh.be

22-09-20

40

6. Server Manager (3)

Création d'un groupe de serveurs : permet de gérer les serveurs, ajouter des rôles, ...



7. ServerManagerCMD

- -query (liste des rôles ou fonctionnalités)
 - -install DHCP DNS
 - -Whatif (simulation)
 - -restart
 - -allSubFeatures (Installation avec tous les services de rôle)
 - -resultpath c:\result.xml
 - -Remove DNS
 - -Inputpath c:\install\WebCore.xml
 - Exemple de fichier réponse
- ```
<ServerManagerConfiguration Action="Install">
<Role Id="WebServerRole" InstallAllSubFeatures="true" /> </ServerManagerConfiguration>
```

## 8. Ocsetup

- Ocplist pour lister tous les rôles et fonctionnalités
  - Ocsetup DHCP;DNS : c\temp.log
  - Ocsetup DHCP /uninstall
- 
- Attention en mode core : précéder les commandes de start /w

## 9. Pkgmgr

- Installation :
  - Pkgmr /iu :WINS-SC;DHCP
- Désinstallation :
  - Pkgmr /uu :DHCP
- Attention en mode core : précéder les commandes de start /w

## 10. PowerShell

- Liste les Rôles & fonctionnalités :  
*Get-Windowsfeature*  
*Get-WindowsFeature | Where {\$\_.Installed -eq \$true}*
- Installer  
*Install-windowsFeature –Name NOM*
- Installer avec ses dépendances  
*Install-windowsFeature –Name NOM -includeAllSubFeature*
- Désinstaller  
*Uninstall-WindowsFeature*

# Module 5

## Serveur DNS

# 1. Introduction

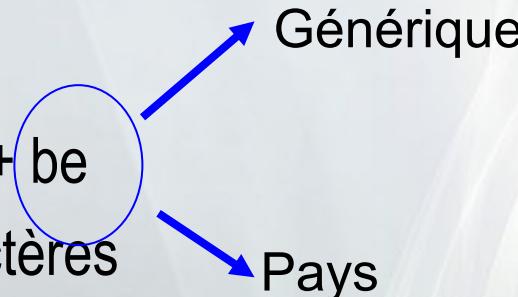
- DNS : Domain Name System
- Whois : <http://www.iana.org/cgi-bin/whois>
- DNS composé de :
  - Espace de noms (Domain Namespace) contient des RR (Ressources Records)
  - Serveur de noms DNS
  - Clients DNS – DNS resolvers (DNR)
- DNS basé sur la demande de résolution de noms (lookup queries)
- DNS peut mettre en cache les requêtes réussies ou échouées

# 1. Introduction

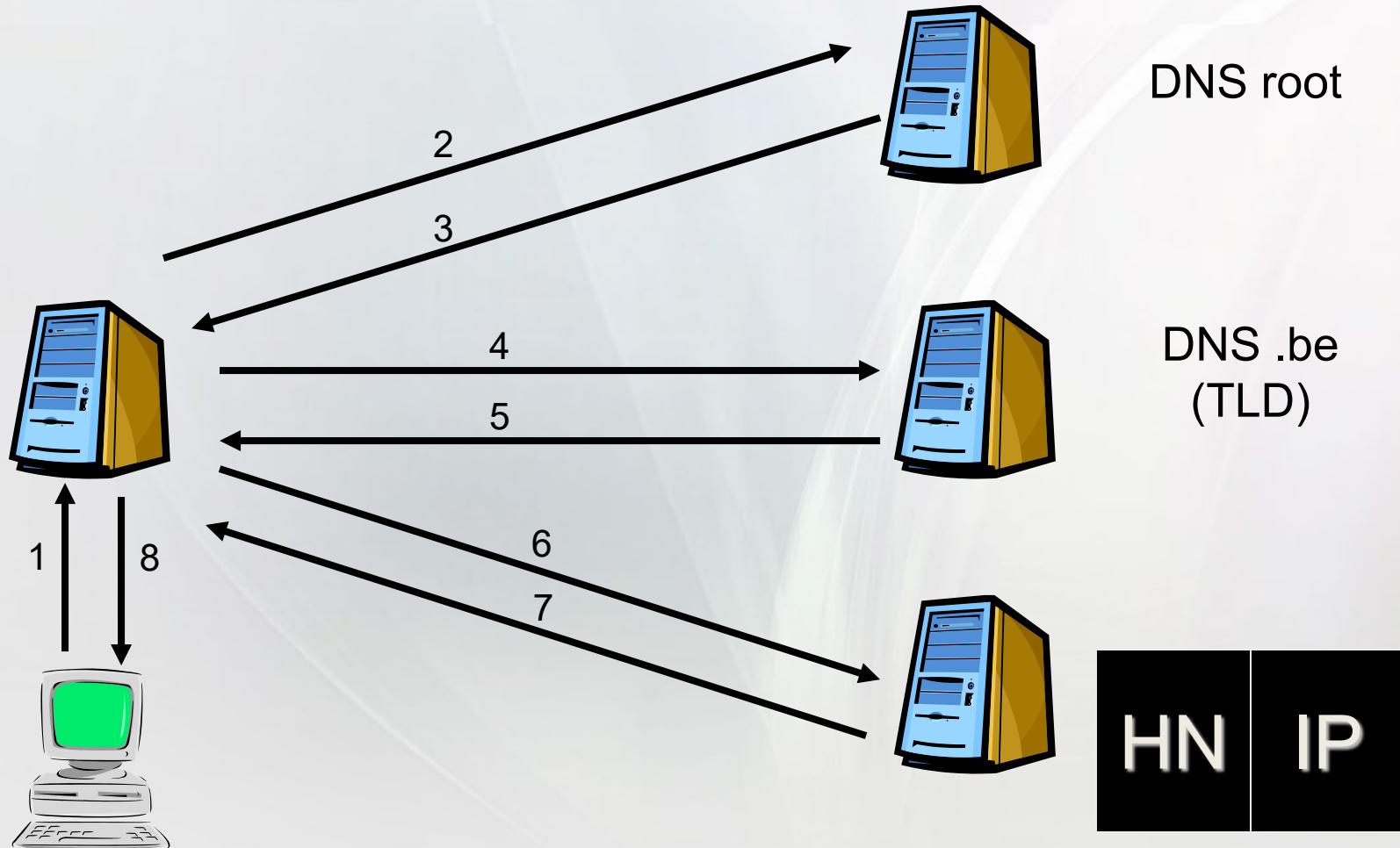
- Depuis 1998 : ICANN (Internet Corporation for Assigned Names and Numbers) gère les noms DNS
- IANA : Internet Assigned Numbers Authority
- ICANN : Autorité de régulation de l'Internet qui gère
  - Les adresses IP
  - Et les noms de domaines de premier niveau (TLD)
- IANA est une composante de l'ICANN qui gère
  - Nom de domaine
  - Adresses IP
  - N° de protocole

## 2. Espace de nom DNS

- Espace de noms : Toute zone délimitée dans laquelle un nom peut être résolu.
- FQHN = HN + FQDN
  - = www + isims + be
- HN maximum 63 caractères
- RFC1123 pour FQDN : caractères A-Z; a-z; 0-9; -  
Max 255 caractères
- RFC1034 : FQDN pas sensible à la case



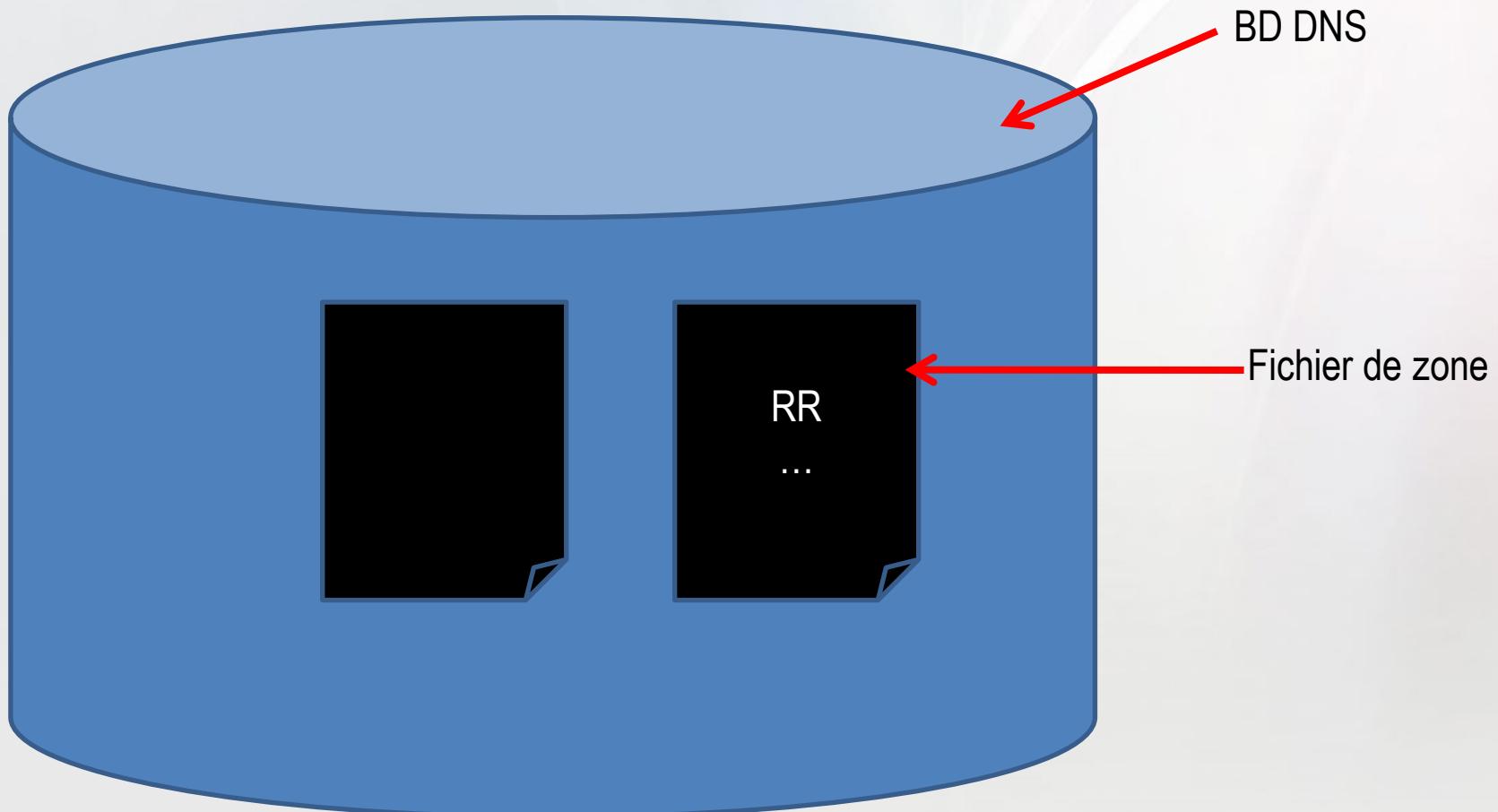
### 3. DNS – BD distribuée



## 4. Structure de l'espace DNS

- Domaine racine : « . »
- Domaine de premier et de deuxième niveau : TLD (Top Level Domain)
- Pour le premier niveau :
  - gTLD (generic TLD)
  - ccTLD (Country Code TLD)

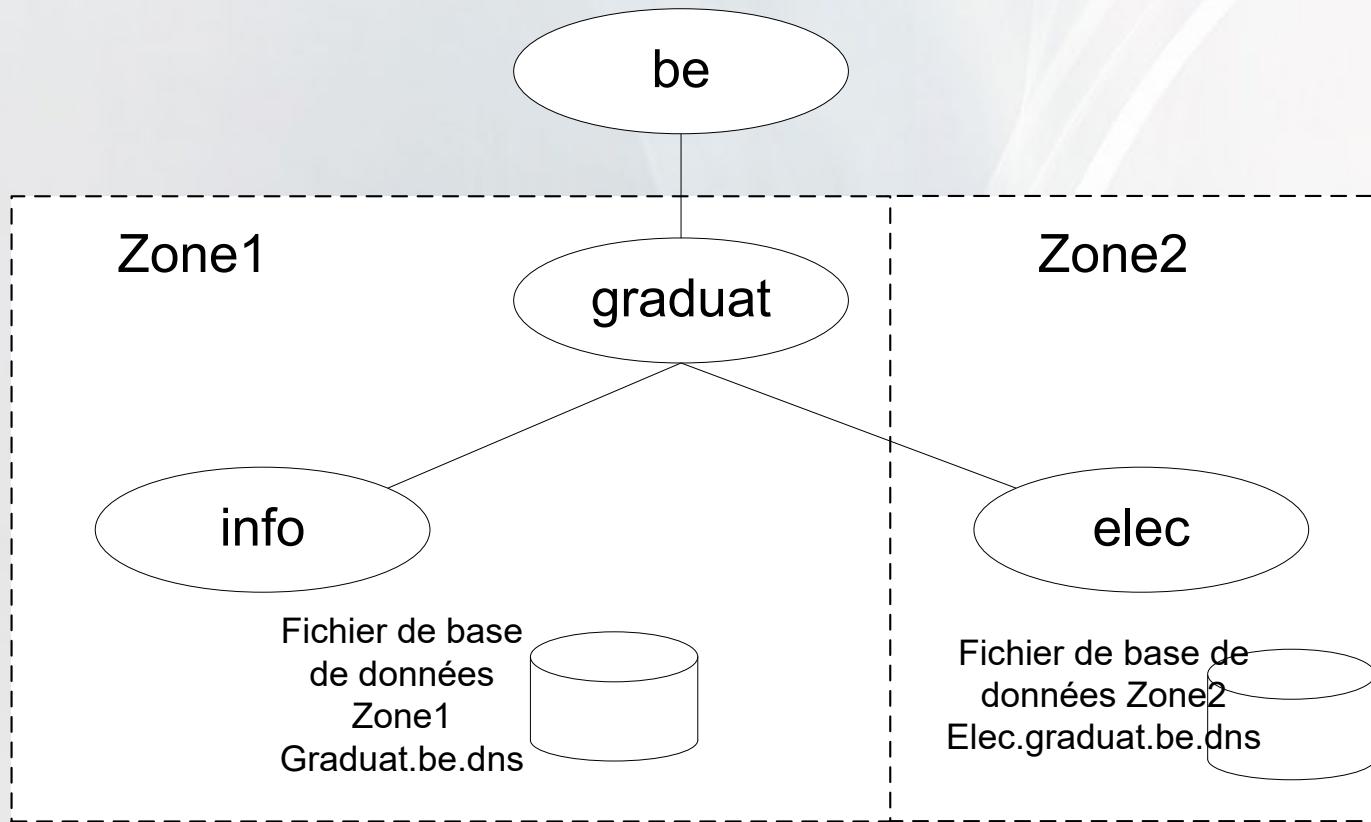
## 5. Les enregistrements (RR)



## 5. Les enregistrements (RR)

- SOA : Start Of authority (Identifie le srv primaire + Transfert de zone + TTL + ...)
- NS : Name Server (Identifie tous les srv désignés pour le domaine)
- A et AAAA : Address Record, les hôtes
- PTR : Pointer Record
- CNAME : Canonical Name
- MX : Mail Exchanger
- SRV : Service locator (Service offert au niveau de l'AD)

## 6. Domaines et zones DNS



## 6. Domaines et zones DNS

- Les zones hébergent des espaces contigus de domaines
- Deux domaines disjoints = 2 fichiers de zones
- SRV DNS ne réplique pas les domaines mais les zones

## 7. Zones et fichiers de zones

- Zones = fichier de BD de zone
  - %systemroot%\system32\dns\nomdomaine.dns
- Si SRV DNS root
  - %systemroot%\system32\dns\root.dns
  - Impossible d'utiliser les redirecteurs sur ce srv
  - Impossible de faire appel à d'autres serveurs racines
- 2 types de zones :
  - Zone de recherche directe
  - Zone de recherche inverse (ex : 1.168.192.in-addr.arpa)

## 7. Zones et fichiers de zones

- Fichiers de configuration d'un serveur DNS
  - Fichier de démarrage
  - Fichier cache DNS
  - Fichier de la zone racine root.dns (si config en root)
  - Les fichiers de zones

## 7. Zones et fichiers de zones

- Exemple de fichier de zone

info.lan - Notepad

File Edit Format View Help

```
; Database file info.lan.dns for info.lan zone.
Zone version: 3

@ IN SOA dctest.test.lan. hostmaster.test.lan. (
 3 ; serial number
 900 ; refresh
 600 ; retry
 86400 ; expire
 3600) ; default TTL

; Zone NS records
;

@ NS dctest.test.lan.

; Zone records
;

pc01 A 10.1.111.45
www CNAME pc01.info.lan.
```

## 8. Types de zones et srv de nom

- Type :
  - Zone primaire (Standard ou ADI)
  - Zone secondaire (Standard ou ADI)
  - Zone de stub
- Commande en ligne : dnscmd.exe
- Dans les propriétés du SOA ne pas utiliser @ pour la personne de contact (@ = la zone elle-même)

## 8. Types de zones et srv de nom

- Zone primaire : copie maître de la zone
- Zone secondaire : réplique de la zone primaire

Serveur de zone principale



Heh.be  
R/W

Serveur de zone secondaire



Heh.be  
R only

## 8. Types de zones et srv de nom

- Types de transfert de zone : DNS Notify
  - AXFR
  - IXFR

Valeur par défaut 15 minutes
- Ports 53 en UDP et TCP
  - UDP : entre serveurs et clients
  - TCP : transfert de zone

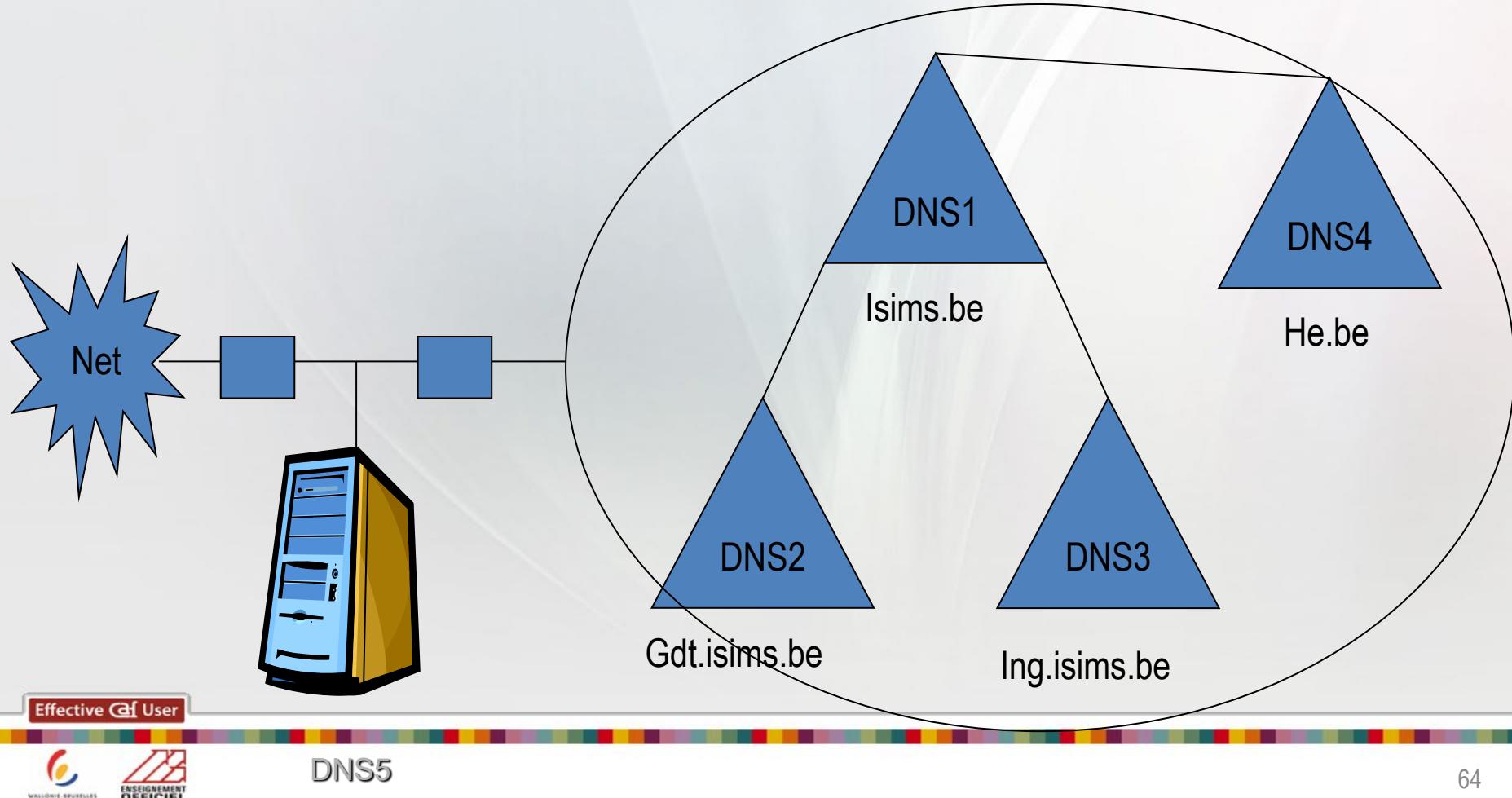
## 8. Types de zones et srv de nom

- Serveur de cache DNS
  - Aucunes zones configurées
  - Par défaut mémorise pendant 1h les résolutions réussies

## 9. Délégation de zone

- Avantages :
  - Déporter la gestion
  - Diviser les zones volumineuses
  - Tolérance de panne
- Fichier de zone

# 10. Les redirecteurs



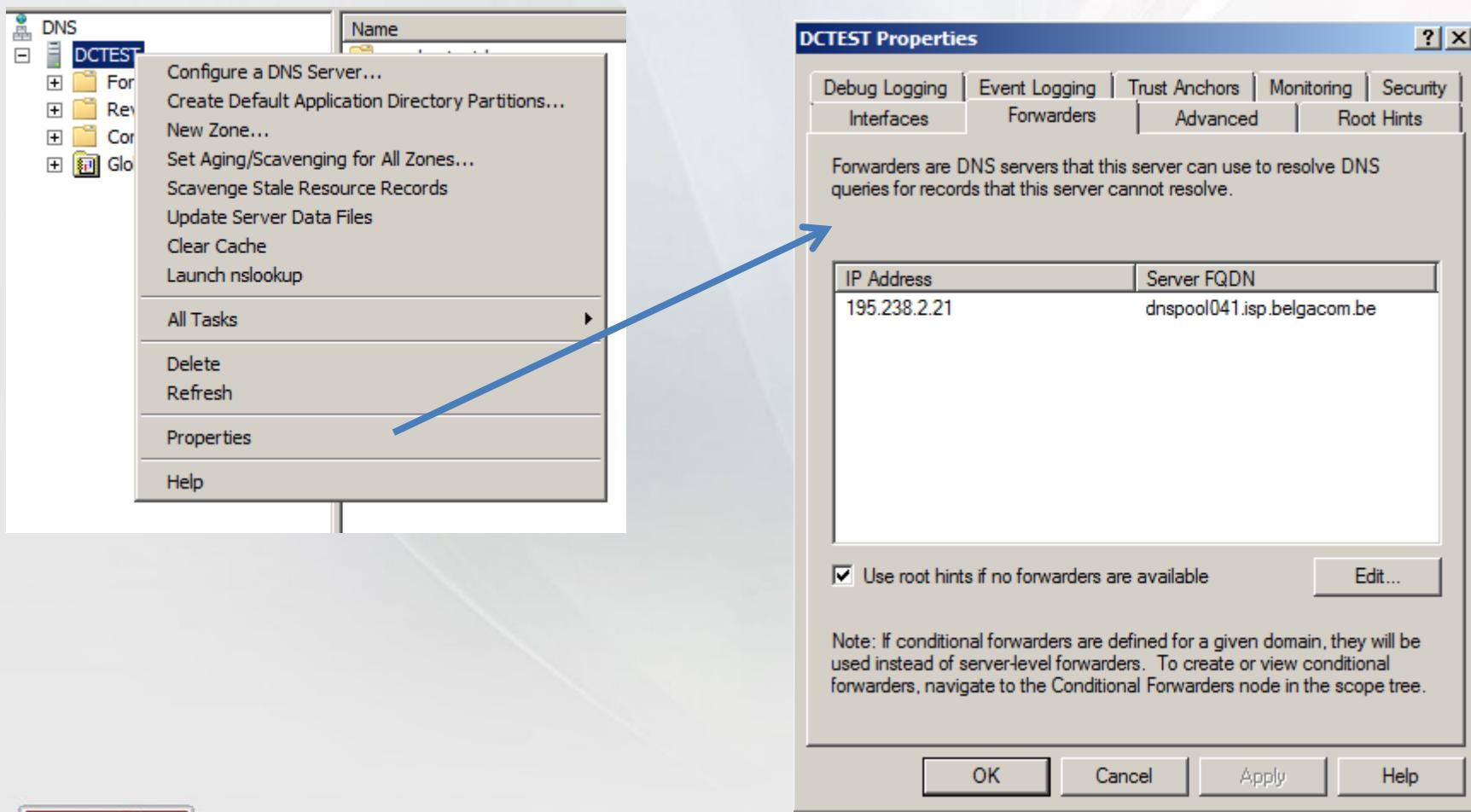
# 10. Les redirecteurs

- Configuration avec redirecteurs simples
  - Les DNS2 et 3 ont comme forward le DNS1
  - Le DNS1 a comme forward le DNS5
  - Le DNS4 a comme forward le DNS5
  - Dans cette situation que se passe t'il si un PC de isims.be cherche un PC de he.be ?
    - Problème
    - La solution : réaliser des forwards en cascades: cela entraîne des baisses de performances et niveau config pas la meilleure chose.

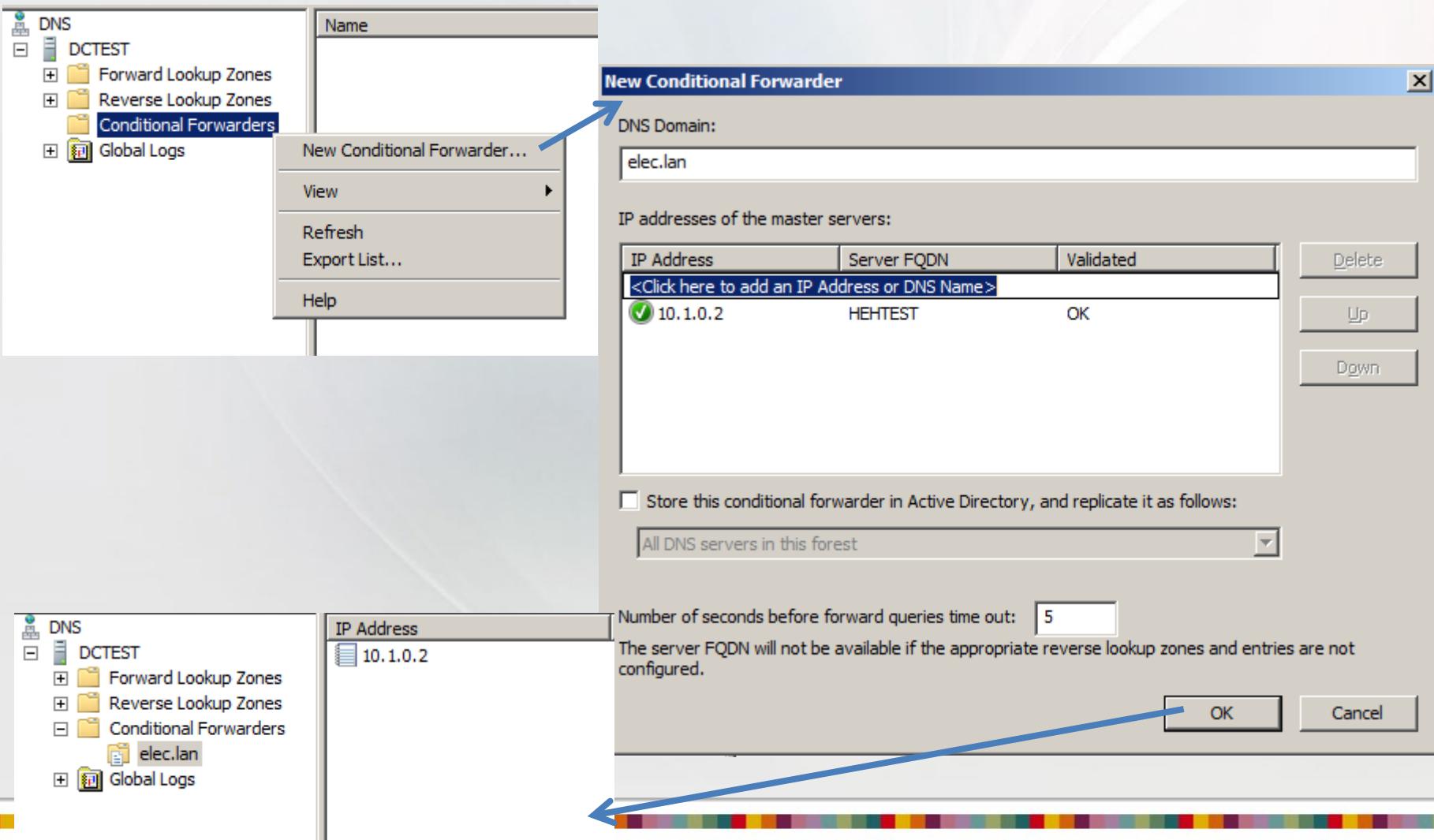
## 10. Les redirecteurs

- Depuis Windows 2003 : possibilité de réaliser des redirecteurs conditionnels
- Exemple :
  - DNS2 et 3 auront comme config :
    - Forward1: DNS1 pour isims.be
    - Forward2: DNS4 pour he.be
    - Forward3: DNS5 pour tous les autres domaines
  - DNS4 aura comme config
    - Forward1: DNS1 pour isims.be
    - Forward2: DNS5 pour tous les autres domaines
  - DNS1 aura comme config
    - Forward1: DNS4 pour he.be
    - Forward2: DNS5 pour tous les autres domaines

# 10. Les redirecteurs normaux (config)



# 10. Les redirecteurs conditionnels (config)



The screenshot shows the Windows DNS Management Console. On the left, the navigation pane shows a tree structure with 'DNS' selected, followed by 'DCTEST' which contains 'Forward Lookup Zones', 'Reverse Lookup Zones', 'Conditional Forwarders' (which is selected and highlighted in blue), and 'Global Logs'. A context menu is open over the 'Conditional Forwarders' node, with the 'New Conditional Forwarder...' option highlighted.

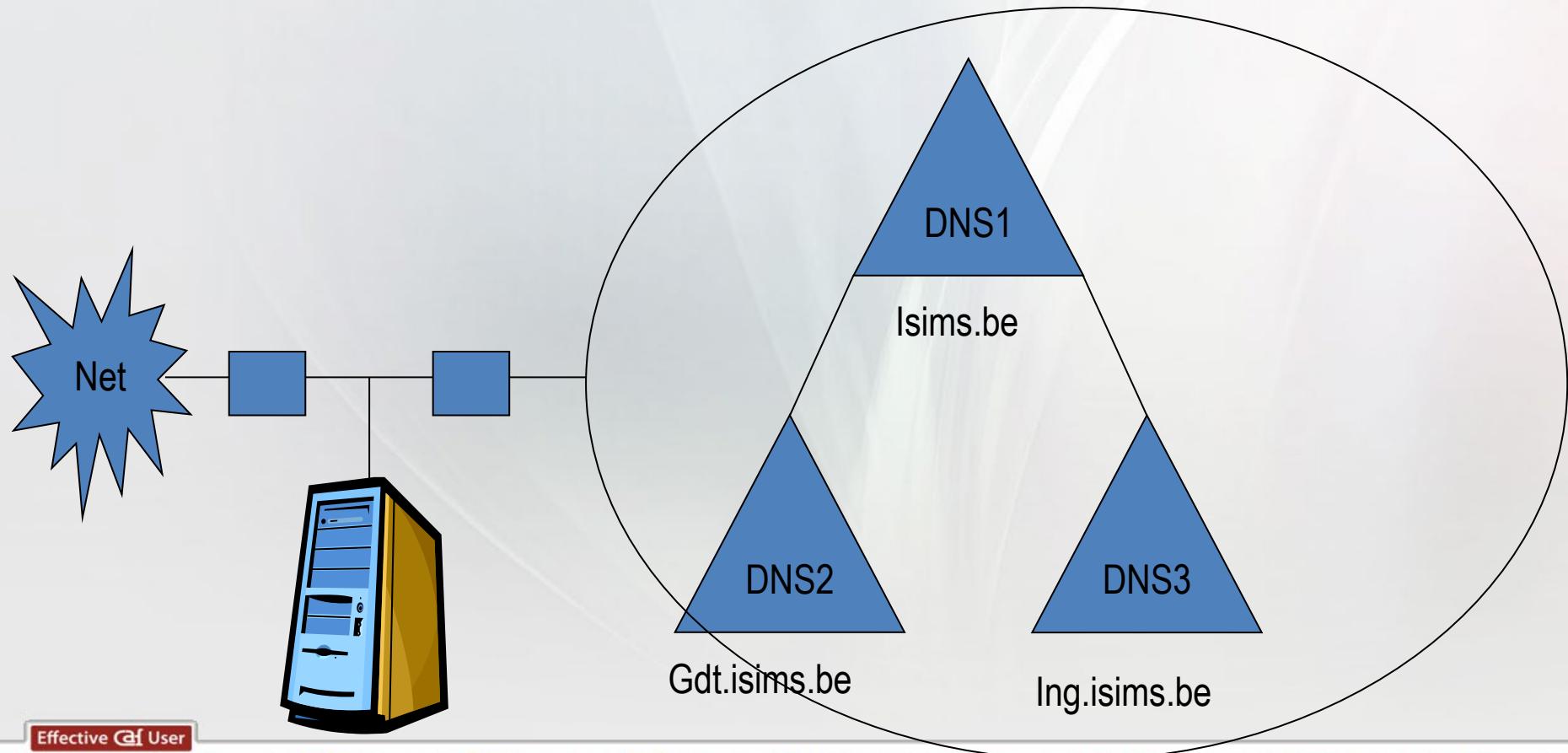
The main pane displays the 'New Conditional Forwarder' dialog box. It has the following fields:

- DNS Domain:** elec.lan
- IP addresses of the master servers:** A table with one entry:

IP Address	Server FQDN	Validated
<Click here to add an IP Address or DNS Name>		
10.1.0.2	HEHTEST	OK
- Buttons:** Delete, Up, Down
- Checkboxes:**  Store this conditional forwarder in Active Directory, and replicate it as follows: (with a dropdown menu set to 'All DNS servers in this forest')
- Text:** Number of seconds before forward queries time out: 5
- Note:** The server FQDN will not be available if the appropriate reverse lookup zones and entries are not configured.
- Buttons:** OK, Cancel

A blue arrow points from the 'New Conditional Forwarder...' option in the context menu to the 'New Conditional Forwarder...' button in the dialog box. Another blue arrow points from the 'Conditional Forwarders' node in the navigation pane to the 'Conditional Forwarders' section in the dialog box.

# 11. Zone de stub



# 11. Zone de stub

- Dans ce cas les DNS1, 2 et 3 sont privés
- Le DNS5 est public, il permet donc aux utilisateurs d'Internet d'accéder au serveurs public de la société (Web, FTP, ...)
- Le problème est que dans ce cas le FQDN public est isims.be qui est donc le même que dans le domaine privé.
- Le DNS5 a donc une zone « isims.be » qui est la même que le DNS1. Etant donné que le DNS5 est public, on ne peut pas avoir dans cette zone certains enregistrements comme SRV, Serveur internes, ...

La solution : réaliser une configuration manuelle sur le DNS5 avec les informations voulues (Stratégie Split Brain)

- Mais à partir de Windows 2003, nous avons la possibilité de créer une stub zone. Qui est une zone de transfert non autoritative. Dans cette zone, seulement une partie des informations sera présentes.

## 11. Zone de stub

- Contient uniquement les IP DNS faisant autorité (SOA, NS et A (Glue records))
- Glue record : A des NS
- Peut-être stocké dans l'AD mais pas dans une ZS

## 12. Round Robin et priorité des sous réseaux

- Round Robin : tourniquet permettant de répartir la charge sur plusieurs serveurs
- Priorité des sous-réseaux : le DNS va donner une IP appartenant au même SR que le client

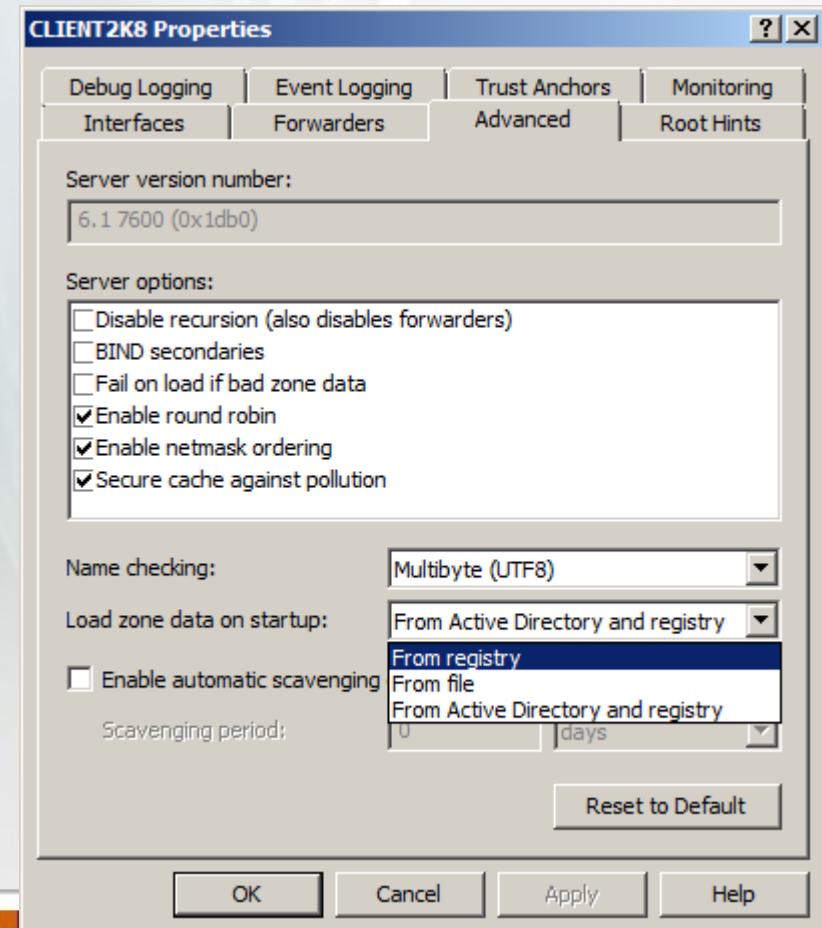
 www	Hôte	192.168.0.250
 www	Hôte	19.30.14.45
 www	Hôte	55.0.10.14

## 13. Vieillissement et nettoyage

- Désactivé par défaut
- Permet le nettoyage des enregistrements A mal déconnectés
- Propriétés – Onglet avancés

# 14. Options de démarrage

- Propriétés – Onglet avancés
  - A partir du registre
  - A partir d'un fichier
  - A partir AD et registre



# 15. Récursivité et protection

- Récursivité : permet au serveur DNS de résoudre des noms qu'il ne connaît pas
- Spoofing DNS
  - Polluer la cache DNS avec un mauvais enregistrement à TTL élevée
- Blocage du spoofing sur les srv DNS internet
  - Plus de récursivité => Plus de redirecteurs

# 16. Commandes de gestion

- Ipconfig : commande client
- Nslookup
- DnsCmd : commande serveur
- DnsLint

## 17. Surveillance

- Définition d'une base de références en utilisant les compteurs
  - Maj dynamique refusée
  - Requête récursive /sec
  - Demande AXFR envoyées
- Utilisation de la MMC Gestion de serveur
- Utilisation des journaux d'événements
  - Serveur DNS à son propre journal
  - %systemroot%\system32\config\dsnevent.evt
  - Explication des différents événements :  
[www.microsoft.com/technet/support/eventserrors.mspx](http://www.microsoft.com/technet/support/eventserrors.mspx) ou [www.eventid.net](http://www.eventid.net)

## 17. Surveillance

- Utilisation des journaux de débogage DNS
  - Pas activé par défaut
  - Propriétés – Onglet Debug logging => Choix du type d'activités
  - Journal : DNS.log
  - Attention consommation importante d'espace

## 18. Questions

- Quel est le rôle du champ TTL d'un enregistrement DNS ?
- Quel type d'enregistrement devez-vous créer afin que les utilisateurs de votre intranet se connectent au serveur Web `srv.société.be` en utilisant le nom [www.société.be](http://www.société.be) ?
- Quelle commande permet de forcer le réenregistrement de son nom d'hôte et adresse IP auprès de son serveur DNS ?
- Quelle commande permet d'afficher le cache DNS d'une station?
- Quelle commande permet de vider le cache DNS d'une machine?

## 18. Questions

- Vous mettez en œuvre deux serveurs DNS. L'un d'eux hébergera une zone principale standard et le second une zone secondaire standard dans un souci de tolérance de panne et de répartition de charge. Les mises à jour dynamiques sont activées. Est-ce qu'un client DNS Windows du serveur DNS hébergeant la zone secondaire standard (donc en lecture seule) sera capable d'enregistrer dynamiquement ses enregistrements auprès de son serveur DNS ?

# 19. DNS en mode Core

- Installation
  - *Start /w ocsetup DNS-server-core-Role*
- Vérifier via *oclist*
- Créer une zone principale
  - *Dnscmd localhost /zoneadd « nom.lan » /Primary /File nom.dns*
- Recharger la zone
  - *Dnscmd localhost /zonereload nom.lan*
- Afficher les zones stockées
  - *Dnscmd localhost /enumzones*
- Infos sur le serveur DNS
  - *Dnscmd localhost /info*
- *Création d'un enregistrement*
  - *Dnscmd localhost /recordadd nom.lan www A 192.168.1.10*

# Module 6

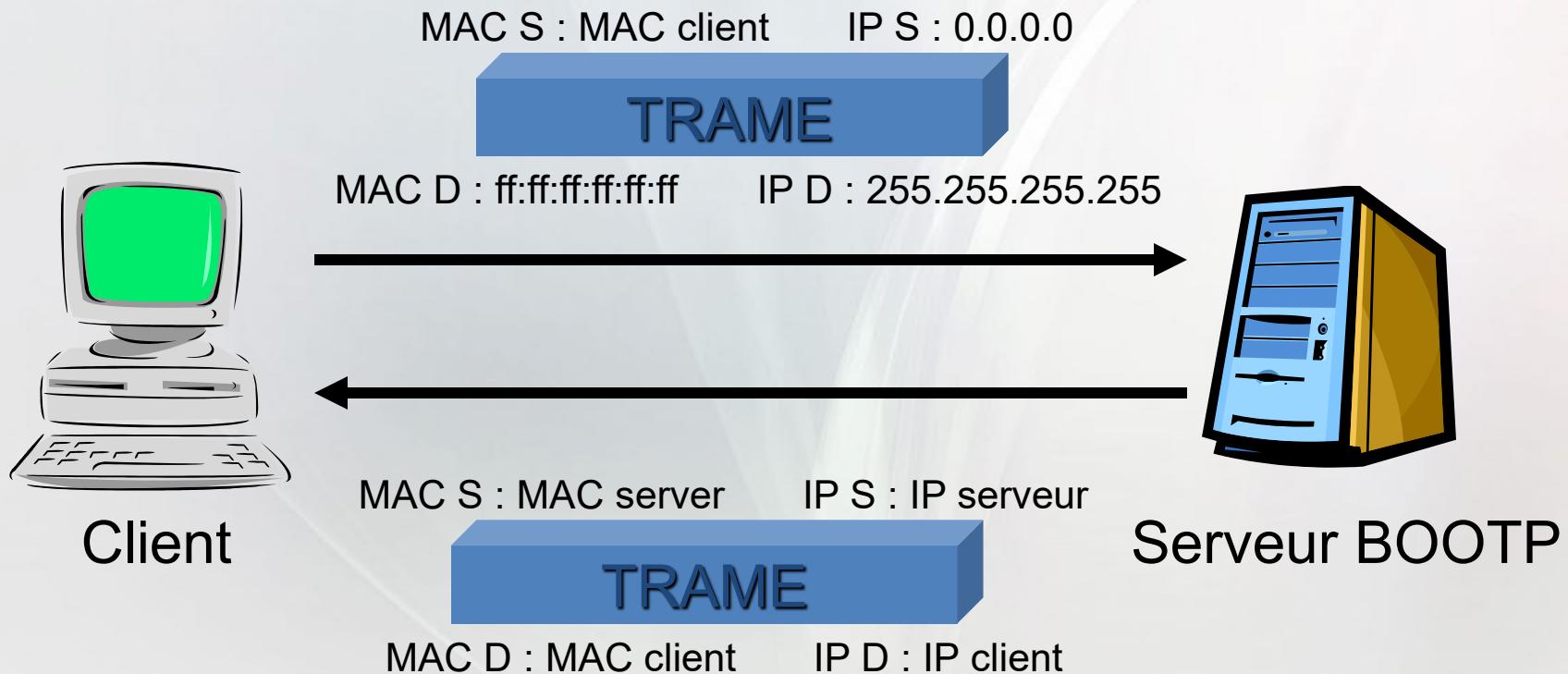
## Serveur DHCP

# 1. Introduction

3 types d'attribution d'adresses IP :

- Serveur RARP (Reverse ARP)
- Serveur BOOTP (Bootstrap Protocol)
- Serveur DHCP (Dynamic Host Configuration Protocol)

## 2. RARP et BOOTP



### 3. DHCPv4 fonctionnement (1)

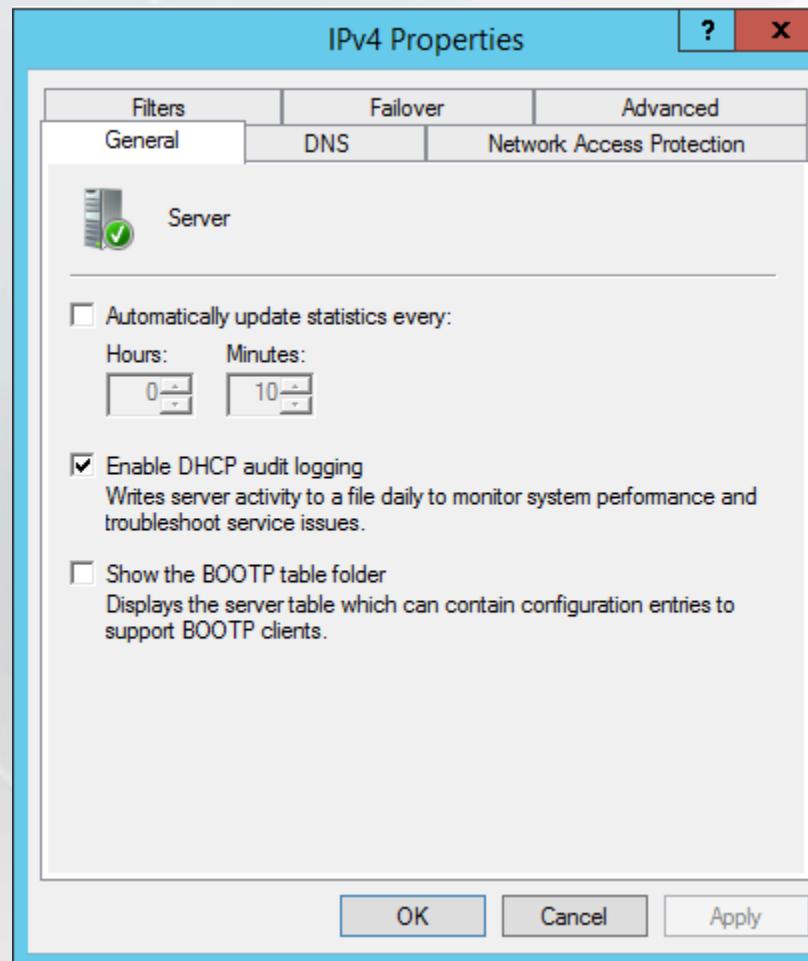


Si pas de réponse : Protocol APIPA (Automatic Private Internet Protocol Addressing).  
Net\_id : 169.254.0.0/16

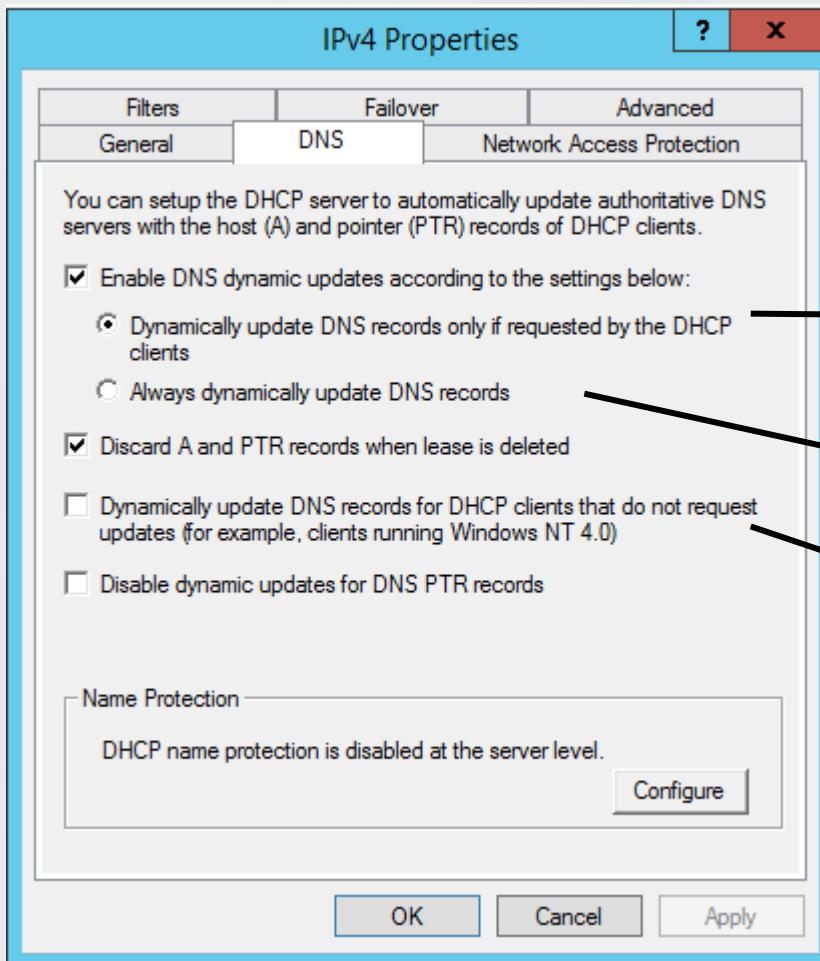
## 3. DHCPv4 Fonctionnement (2)

- Renouvellement du bail à 50%, 75% et 87.5%  
(dhcp request et dhcp ack)
- Démarre PC avec bail valide -> renouvellement
- Ipconfig/renew : renouvellement du bail
- Ipconfig/release : abandon du bail
- Diffusion réalisée en utilisant UDP (Port client = 68, Port serveur = 67)

# 4. Configuration DHCPv4

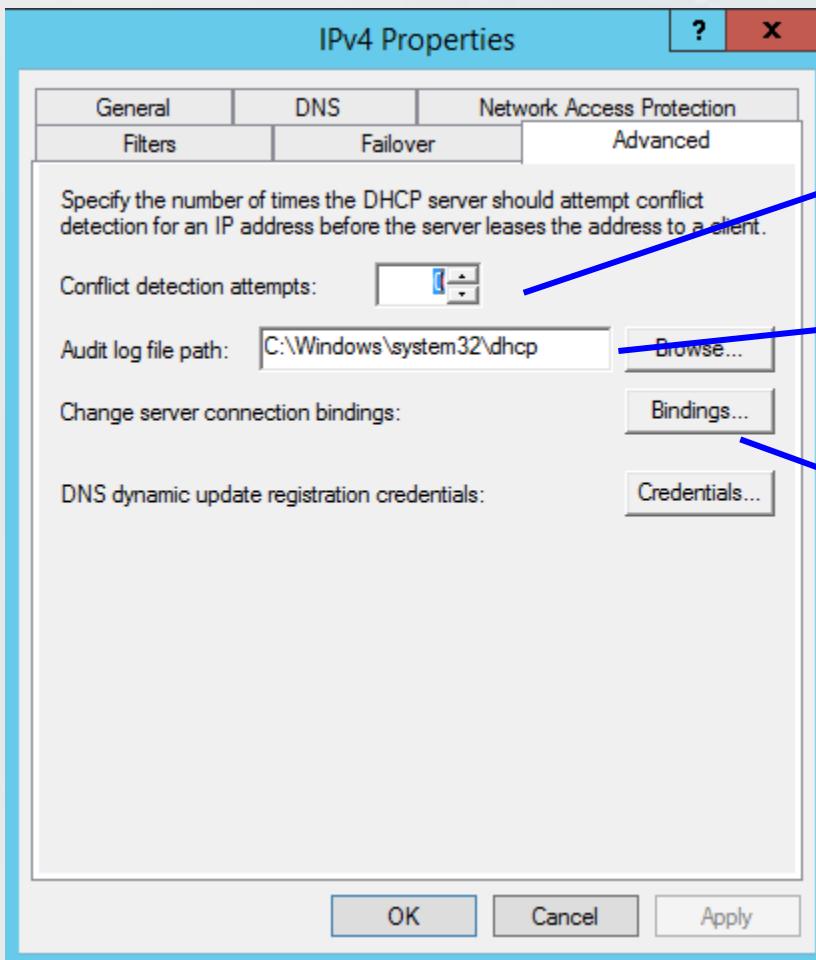


# 4.1. Configuration DNS – DHCPv4



- Enregistrement A réalisé par le client  
Enregistrement PTR réalisé par le DHCP
- Enregistrement A et PTR réalisé par le DHCP
- Enregistrement A et PTR réalisé par le DHCP  
Uniquement pour les clients < Win2K
- Seul les clients  $\geq$  win2k savent s'enregistrer dynamiquement

## 4.2. Configuration avancées DHCPv4

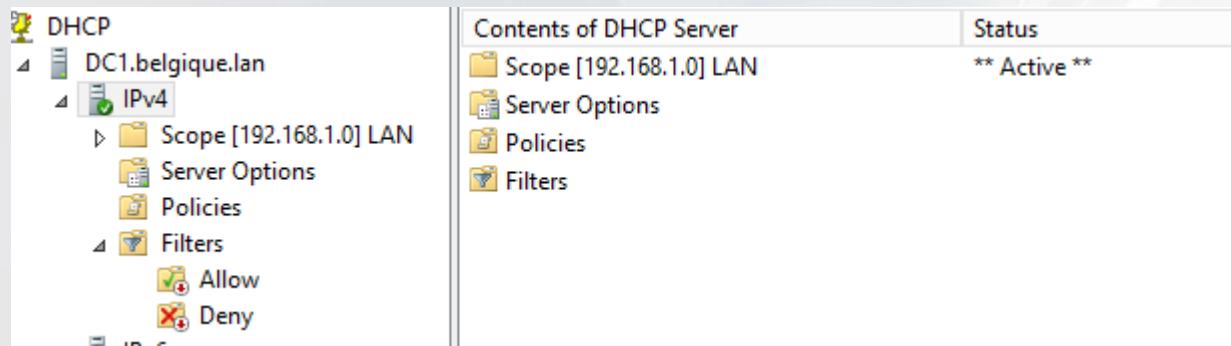


Nbr de ping réalisé avant de donner une IP  
(inutile pour les clients > Win98)

Dossier dans lequel on retrouvera les fichiers Journaux de la forme :DhcpSrvlog.xxx  
(xxx = 3 premières lettres du jour de la semaine)

Liaisons : permet de déterminer sur quel interface réseau Le serveur DHCP va écouter et répondre aux requêtes DHCP

## 4.3. Configuration suite DHCPv4



Contents of DHCP Server	Status
Scope [192.168.1.0] LAN	** Active **
Server Options	
Policies	
Filters	

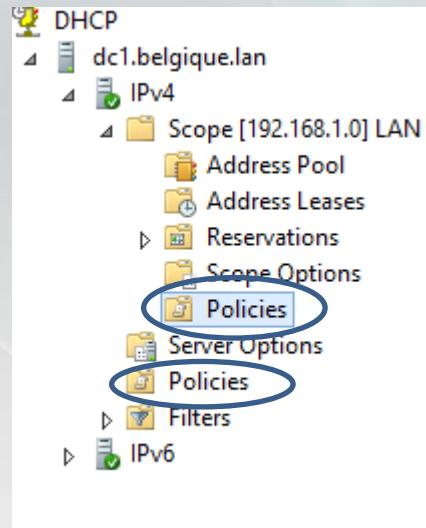
Réservation  
À partir de la  
MAC du client

## 5. Les options

- Les options permettent de rajouter des informations autre que l'IP, le Mask
- Principales options :
- 2 types d'options
  - Options d'étendues : valable uniquement sur l'étendue
  - Options de serveurs : valable pour toutes les étendues du serveurs

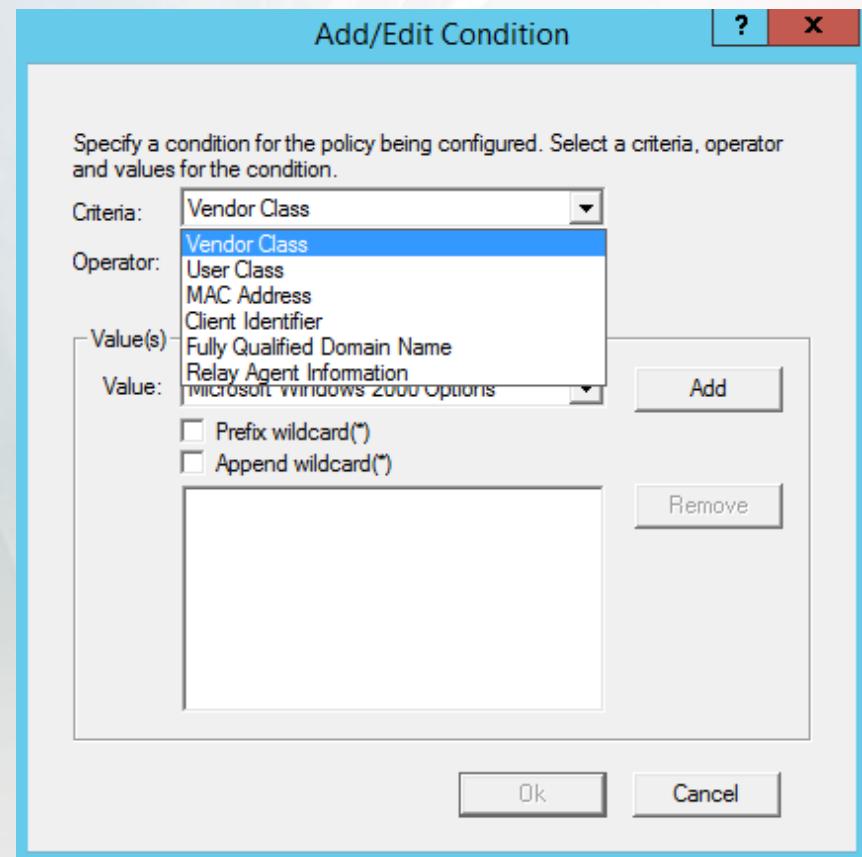
## 6. Attribution par stratégie DHCPv4

- Possibilité d'octroyer des configurations IP différentes aux clients d'un même étendue/serveur DHCP.
  - Certains clients auront la passerelle et d'autre pas.
  - Configuration différente entre les ordinateurs, les téléphones IP, les imprimantes, ...
  - Bail en fonction du type de client



## 7. Créer stratégie DHCPv4

- Créer une nouvelle stratégie
- Donner un nom/description
- Ajouter une condition
- Choix du critère
  - Vendor class (« revendeur »)
  - User class (groupe d'utilisateur)
  - MAC address
  - ...



# 8. Stratégie DHCPv4 basée sur la MAC

Specify a condition for the policy being configured. Select a criteria, operator and values for the condition.

Criteria: **MAC Address**

Operator: **Equals**

Values(in hex)

Value:

Add

Prefix wildcard(\*)  
 Append wildcard(\*)

**0800270C3E04**

Remove

## DHCP Policy Configuration Wizard

### Configure settings for the policy

If the conditions specified in the policy match a client request, the settings will be applied.



A scope can be subdivided into multiple IP address ranges. Clients that match the conditions defined in a policy will be issued an IP Address from the specified range.

Configure the start and end IP address for the range. The start and end IP addresses for the range must be within the start and end IP addresses of the scope.

The current scope IP address range is 192.168.1.100 - 192.168.1.150

If an IP address range is not configured for the policy, policy clients will be issued an IP address from the scope range.

Do you want to configure an IP address range for the policy:  Yes  No

Start IP address: 192.168.1.140

End IP address: 192.168.1.145

Percentage of IP address range: 11.8

Effe

< Back

Next >

Cancel

## DHCP Policy Configuration Wizard

### Configure settings for the policy

If the conditions specified in the policy match a client request, the settings will be applied.



Vendor class:

DHCP Standard Options

#### Available Options

- 002 Time Offset
- 003 Router
- 004 Time Server

#### Description

- UTC offset in seconds
- Array of router addresses order
- Array of time server addresses

#### Data entry

Server name:

Resolve

IP address:

<input type="text" value="192.168.1.250"/>	<input type="button" value="Add"/> <input type="button" value="Remove"/> <input type="button" value="Up"/> <input type="button" value="Down"/>
--------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------

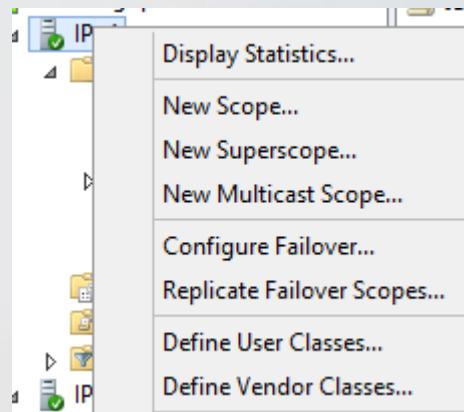
< Back

Next >

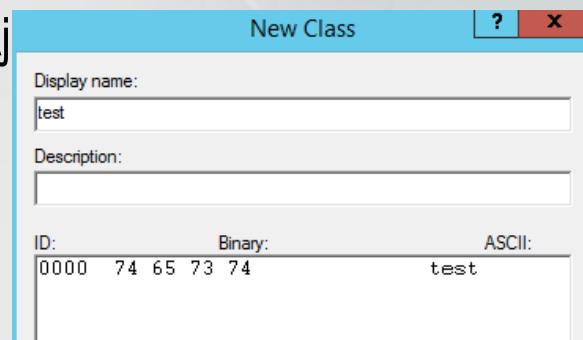
Cancel

# 9. Stratégie DHCPv4 basée sur la classe utilisateur

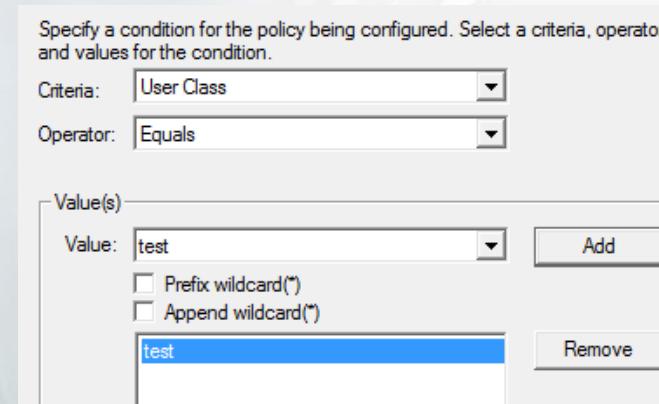
- Créer une classe utilisateur



- Ajouter une nouvelle classe dans le gestionnaire de DHCP.



- Créer la stratégie



- Configurer la stratégie
- Sur le client
  - Attribuer une classe à une interface : `ipconfig/setclassid « interface » classe`
  - Connaître les ID de classe pour une interface : `ipconfig/showclassid « interface »`

## 7. Les réseaux routés

- Routeur RFC 1542
- Agent de relais DHCP
- Serveur DHCP dans chaque segment

## 8. DHCPv6

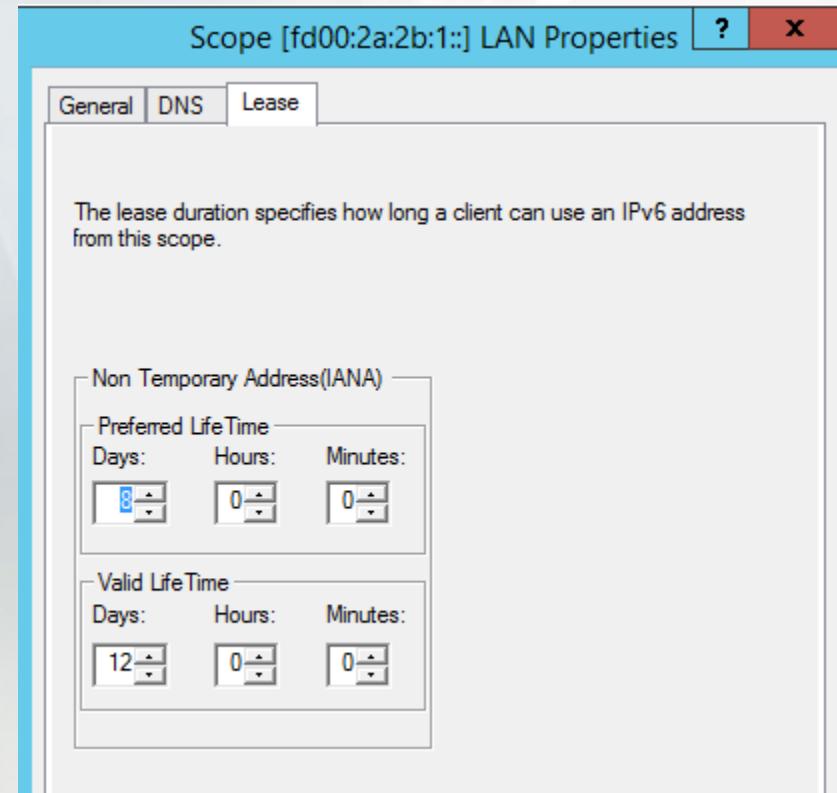


## 8. DHCPv6

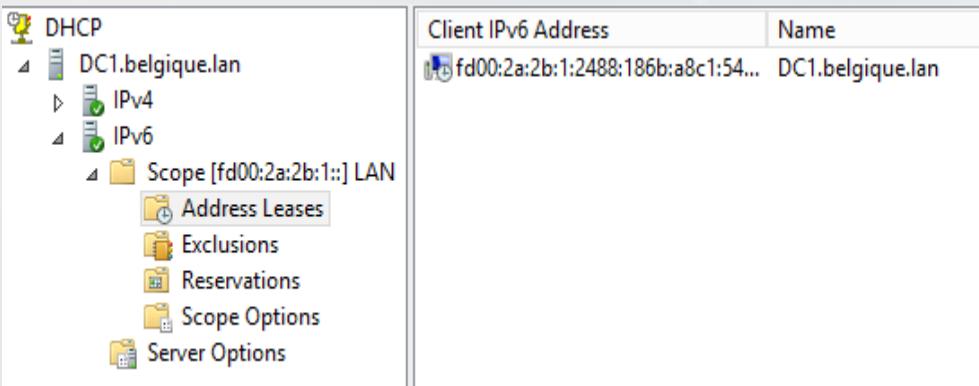
- **SOLICIT** : envoyé par un client pour recenser les serveurs DHCP disponibles (équivalent v4 : **DHCPDISCOVER**).
- **ADVERTISE** : envoyé par un serveur proposant ses services en réponse au message **SOLICIT** (équivalent v4 : **DHCPOFFER**).
- **REQUEST** : envoyé par un client à un serveur pour demander les paramètres de configuration (équivalent v4 : **DCHPREQUEST**).
- **CONFIRM** : envoyé par un client pour vérifier que son adresse ou ses adresses sont toujours valides (pas d'équivalent v4).

## 9. DHCPv6 - Fonctionnement

- Port client : 546
- Port serveur : 547
- Renouvellement du bail



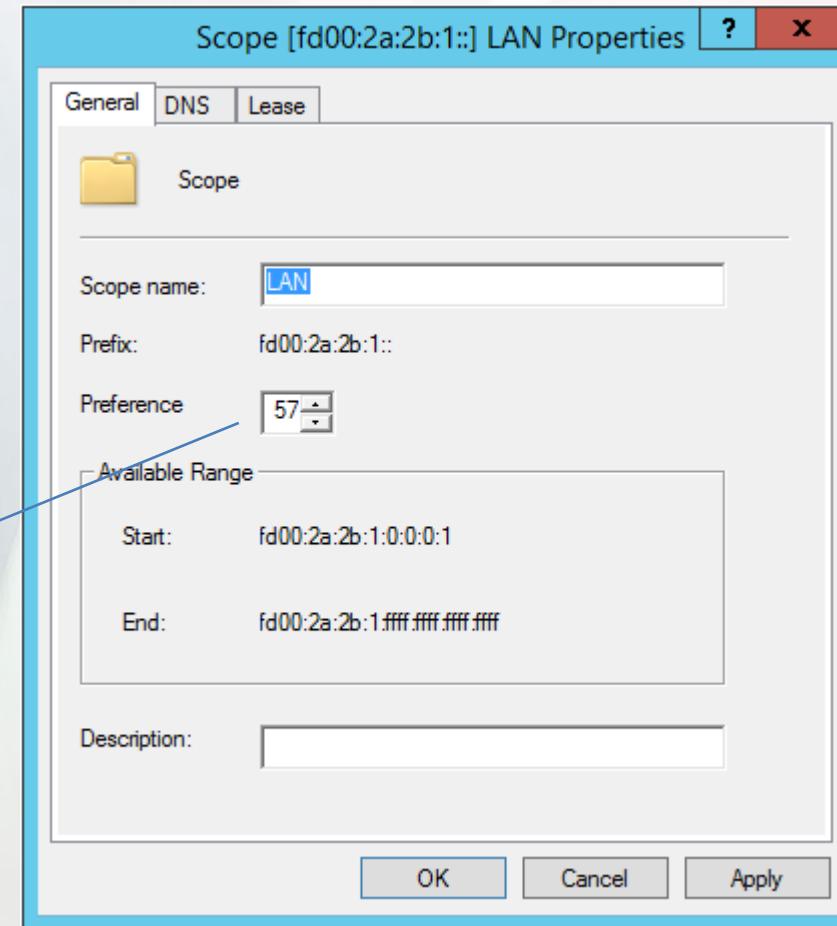
# 10. DHCPv6 - Configuration



Detailed description: This screenshot shows the Windows Server 2012 DHCP console. On the left, the tree view shows a hierarchy under 'DC1.belgique.lan': 'IPv4', 'IPv6', and 'Scope [fd00:2a:2b:1::] LAN'. Under 'Scope LAN', there are sub-options: 'Address Leases' (highlighted), 'Exclusions', 'Reservations', 'Scope Options', and 'Server Options'. In the center pane, a table titled 'Client IPv6 Address' lists one entry: 'fd00:2a:2b:1:2488:186b:a8c1:54...' with 'Name' 'DC1.belgique.lan'. A blue arrow points from the text 'Cas de plusieurs serveurs DHCP' to the 'Scope Options' section of the DHCP console.

Client IPv6 Address	Name
fd00:2a:2b:1:2488:186b:a8c1:54...	DC1.belgique.lan

Cas de plusieurs serveurs DHCP  
Valeur entre 0 et 255  
0 : pas de préférence  
255 :



Detailed description: This screenshot shows the 'Scope [fd00:2a:2b:1::] LAN Properties' dialog box. The 'General' tab is selected. The 'Scope name:' field contains 'LAN'. The 'Prefix:' field contains 'fd00:2a:2b:1::'. The 'Preference' dropdown is set to '57'. The 'Available Range' section shows 'Start:' as 'fd00:2a:2b:1:0:0:0:1' and 'End:' as 'fd00:2a:2b:1:ffff:ffff:ffff:ffff'. The 'Description:' field is empty. At the bottom are 'OK', 'Cancel', and 'Apply' buttons. A blue arrow points from the text 'Cas de plusieurs serveurs DHCP' to the 'Preference' dropdown in the dialog box.

Scope [fd00:2a:2b:1::] LAN Properties

General DNS Lease

Scope

Scope name: LAN

Prefix: fd00:2a:2b:1::

Preference 57

Available Range

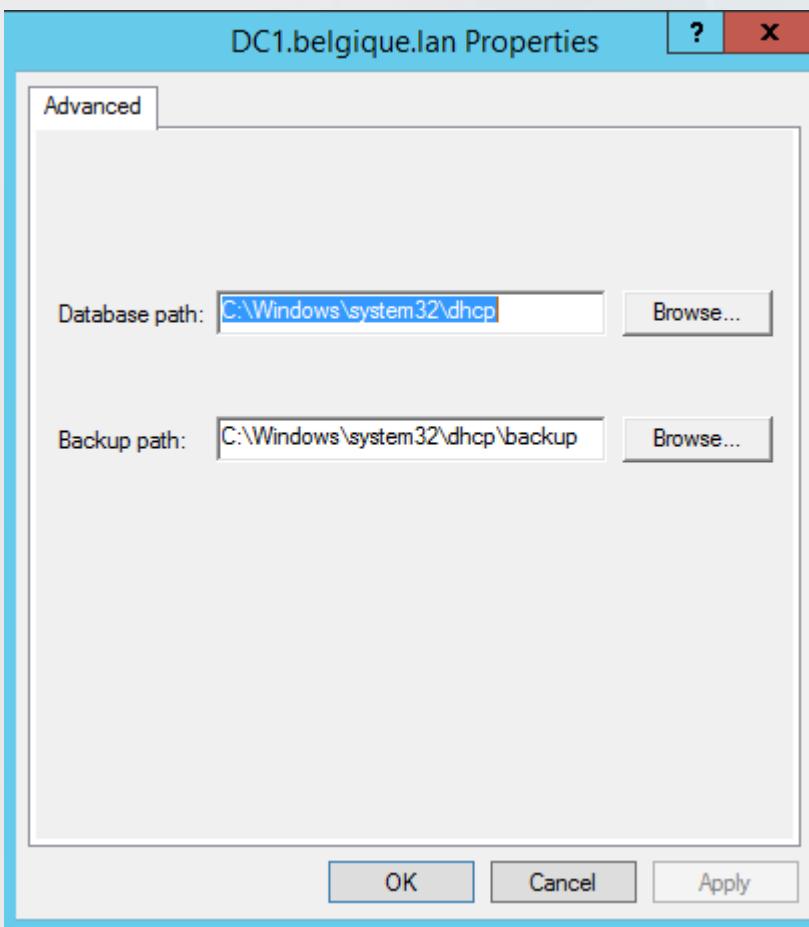
Start: fd00:2a:2b:1:0:0:0:1

End: fd00:2a:2b:1:ffff:ffff:ffff:ffff

Description:

OK Cancel Apply

# 11. Base de données



Dossier dans lequel on retrouvera la BD contenant toutes les Infos du DHCP, elle est régulièrement sauvegardée et compressée en ligne. Afin de gagner un peu de place, il est intéressant de la compresser manuellement à l'aide de la commande : jetpack dhcp.mdb tmp.mdb.  
Attention arrêter le service avec net stop et ensuite le remettre En route avec net start dhcpserver

Dossier dans lequel on retrouvera les fichiers Journaux de la forme :DhcpSrvlog.xxx (xxx = 3 premières lettres du jour de la semaine)

Name	Date modified
backup	18-10-16 17:44
dhcp.mdb	19-10-16 16:40
dhcp.pat	18-10-16 17:44
DhcpSrvLog-Fri.log	16-10-15 16:25
DhcpSrvLog-Mon.log	17-10-16 11:30
DhcpSrvLog-Tue.log	18-10-16 08:25
DhcpSrvLog-Wed.log	19-10-16 16:40

# Module 7

## Introduction à l'Active Directory

# 1. Définition

- Wikipédia :

**Active Directory** (AD) est la mise en œuvre par [Microsoft](#) des services d'[annuaire LDAP](#) pour les [systèmes d'exploitation Windows](#). L'objectif principal d'*Active Directory* est de fournir des services centralisés d'identification et d'authentification à un réseau d'ordinateurs utilisant le système [Windows](#). Il permet également l'attribution et l'application de stratégies, la distribution de logiciels, et l'installation de mises à jour critiques par les administrateurs. *Active Directory* répertorie les éléments d'un [réseau](#) administré tels que les comptes des utilisateurs, les serveurs, les postes de travail, les dossiers partagés, les imprimantes, etc. Un utilisateur peut ainsi facilement trouver des ressources partagées, et les administrateurs peuvent contrôler leur utilisation grâce à des fonctionnalités de distribution, de duplication, de partitionnement et de sécurisation de l'accès aux ressources répertoriées. Si les administrateurs ont renseigné les attributs convenables, il sera possible d'interroger l'annuaire pour obtenir, par exemple, « toutes les imprimantes couleurs à cet étage du bâtiment ».

## 2. Annuaire LDAP

- Annuaire
  - BD pour des données étant très peu mises à jour
  - Coordonnées des utilisateurs
  - E-mails
  - Login/Pswd
  - Centralisation des données
  - Recherche
- LDAP : Lightweight Directory Access Protocol

## 3. Structure logique



- Forêt
- Arbre (arborescence de domaine)
- Domaines
- Unité d'organisation (OU)

## 4. Forêt

- Une forêt est un ensemble d'un ou de plusieurs domaines Active Directory, le premier domaine installé est appelé domaine racine. Son nom DNS (exemple : Belgique.lan) sera également donné à la forêt.
- Aucune donnée (compte utilisateur, ordinateur...) n'est répliquée en dehors de la forêt, la forêt sert donc de frontière de sécurité.

## 5. Domaine et arborescence de domaines

- Une arborescence de domaines est une suite de domaines qui partagent un espace de noms contigu.
- La relation d'approbation entre **les domaines d'une même arborescence** est de type parent/enfant. Lors de l'ajout d'un domaine enfant, une relation d'approbation de type bidirectionnelle et transitive est créée automatiquement.
- Le domaine représente une limite de sécurité où les utilisateurs sont définis.
- Un domaine contient au moins un **contrôleur de domaine** (DC). Mais il est préférable d'en avoir au minimum 2 pour la sécurité
- Le contrôleur de domaine (DC) assure l'authentification des comptes utilisateurs et ordinateurs.

## 6. Unité d'organisation

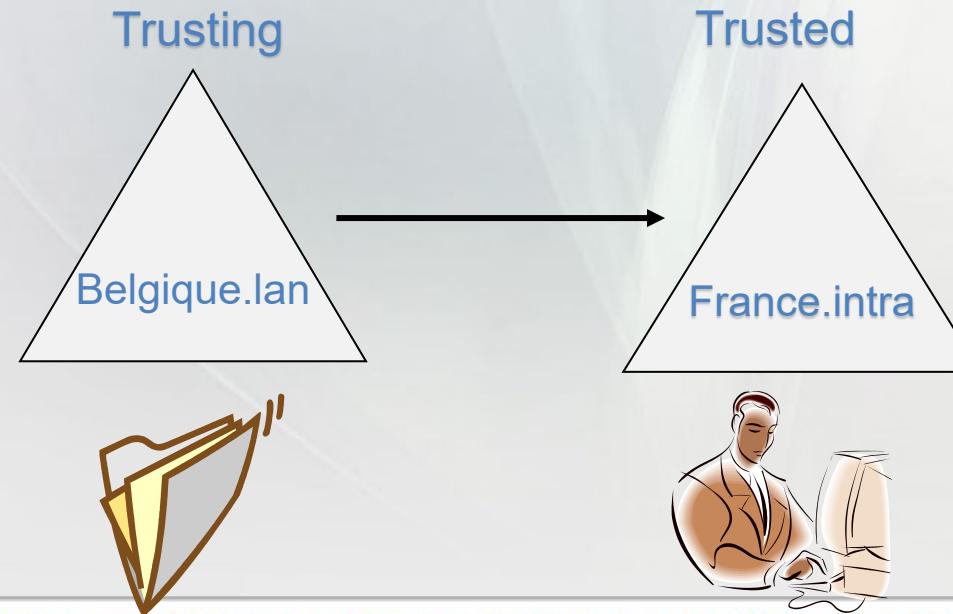
- Une **unité d'organisation (OU, Organizational Unit)** est un objet de type conteneur. Il permet d'effectuer une hiérarchisation dans l'annuaire Active Directory.
- Avantage de regrouper les objets (utilisateurs, ordinateurs) dans une UO :
  - l'application d'une GPO (Group Policy Object - Stratégie de groupe)
  - faciliter l'administration.
  - déléguer l'administration des objets (réinitialiser le mot de passe de l'utilisateur, ajouter des objets,...) à un utilisateur autre que l'administrateur.

## 7. Les objets

- **Utilisateur** : permet d'authentifier les utilisateurs physiques qui ouvrent une session sur le domaine. Des droits et permissions sont associés au compte afin de permettre l'accès à une ressource (dossier partagé, boîte aux lettres mail, imprimante...).
- **Groupe** : permet de rassembler différents objets (utilisateurs ou ordinateurs) qui ont le même accès sur une ressource. L'administration des permissions est plus aisée en utilisant des groupes.
- **Ordinateur** : permet d'authentifier les postes physiques connectés au domaine. Il est possible de positionner le compte ordinateur dans une ACL, cela permettra l'accès à une ressource. Si l'authentification ne peut être effectuée, l'ouverture de session sur le domaine ne sera pas effectuée.
- **Unité d'organisation** : conteneur qui permet l'organisation des objets de façon hiérarchique. Il est possible de lui appliquer une ou plusieurs stratégies de groupe. De plus, cet objet offre la possibilité de mettre en place une délégation.
- **Imprimante** : une imprimante partagée peut être publiée dans Active Directory. Cette action simplifie les étapes de recherche et d'installation pour un utilisateur.

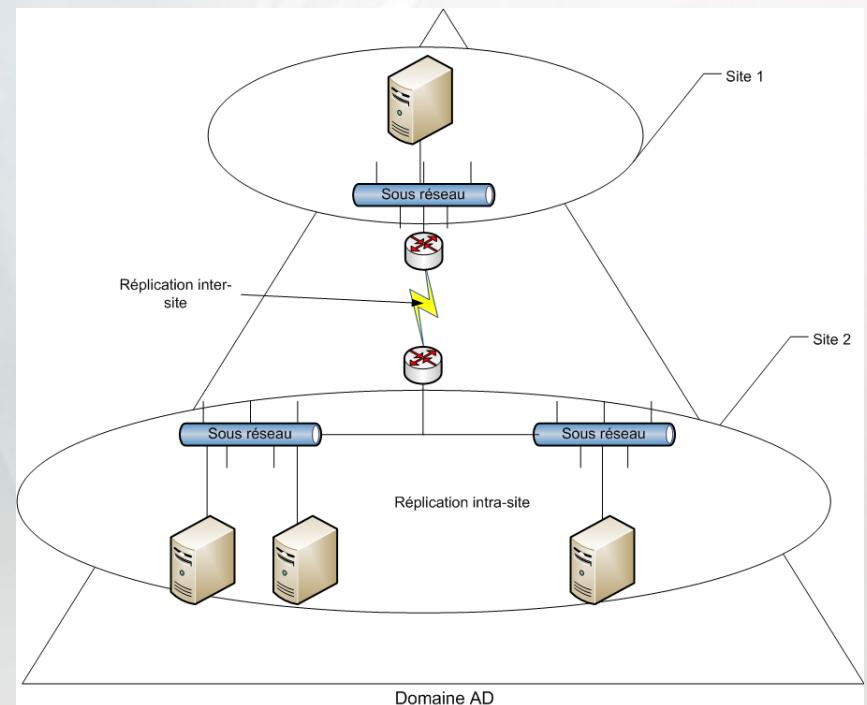
## 8. Relation d'approbation

- 2 types :      transitive : A ap B et B ap C => A ap C  
                      bidirectionnelle : A ap B et B ap A
- Entre domaine et sous domaine : relation transitive bidirectionnelle (automatique)
- Protocole Kerberos v5 (SSO : Single Sign One)



# 9. Structure physique

- Le contrôleur de domaine (DC)
  - Un ou plus DC dans un domaine
  - Redondance
- Sites
  - Sous réseaux connectés par haut débit
  - Optimisation de la duplication



## 10. Indépendance

- Indépendance complète entre la structure physique et logique.
- On peut avoir plusieurs domaines dans un site ou plusieurs sites dans un même domaine.

## 11. Modèle de nommage

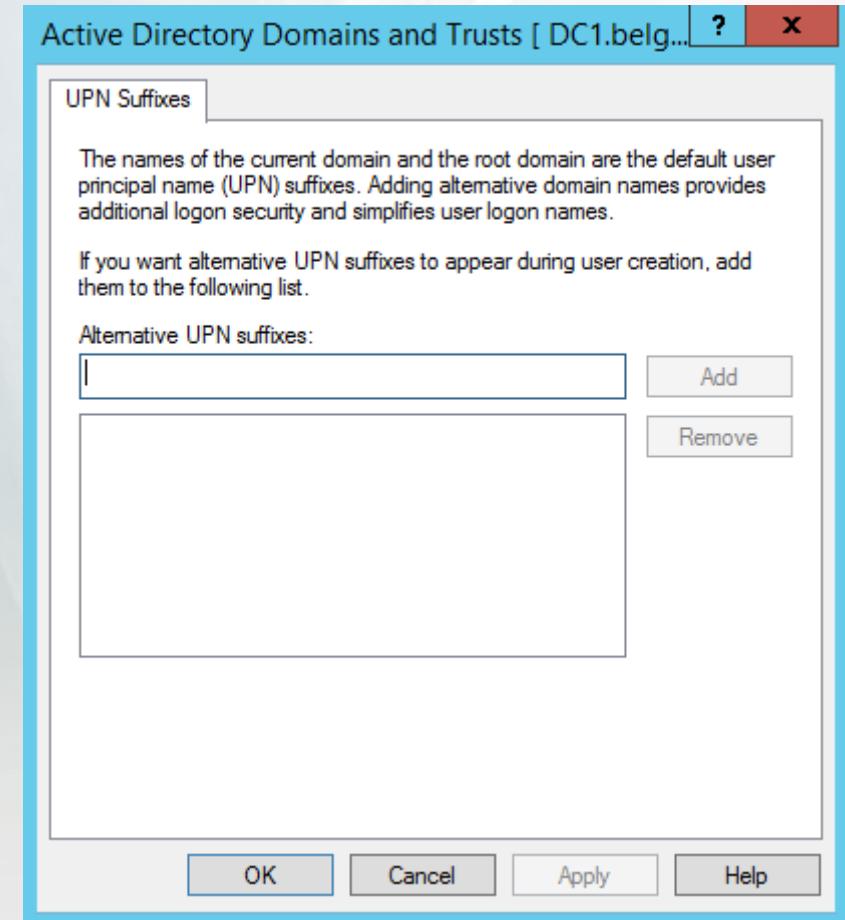
- Protocole LDAP
- Le modèle de nommage (aussi appelé *modèle de désignation*) a pour but de définir la façon selon laquelle les objets de l'annuaire sont nommés et classés.
- DN : Distinguished Name  
 $CN = \text{Jean Dupont}$ ,  $OU = \text{Direction}$ ,  $DC = \text{isims}$ ,  $DC = \text{be}$   
 $CN$  (*Common Name*);  $OU$  (*Organizational Unit*);  $DC$  (*Domain*)
- RDN : Relative Distinguished Name  
 $CN = \text{Jean Dupont}$
- UPN : User Principal Name  
 $\text{deprez@isims.be}$

## 12. Identification des objets

- GUID (128 bits) : Globally Unique Identifier  
N° créé lors de la création d'un objet, il est non renommable et non supprimable même quand on modifie ou supprime l'objet.  
Utile pour la localisation de l'objet, se trouve dans le GC.
- SID (128 bits) : Security Identifier  
DID + RID  
Utilisé dans les ACL (Access Control List)

## 13. UPN

- UPN : User Principal Name
- Utilisé pour l'ouverture de session  
[henri.deprez@heh.be](mailto:henri.deprez@heh.be)
- Lorsque la forêt devient très complexe (beaucoup de domaine enfant), l'UPN d'un utilisateur peut devenir très long. Afin de simplifier son UPN on peut créer de nouveaux suffixe plus simple.
- Domaine et approbation AD > Propriétés de dom. et approb. AD > Onglet Suffixe UPN



# Module 8

Promotion d'un contrôleur de domaine (DC)

# 1. Définition

- Un **contrôleur de domaine** (DC) est un serveur qui a pour fonction l'authentification des utilisateurs et ordinateurs dans un domaine, Il gère également l'accès aux ressources partagées.
- Il faut au minimum 1 DC/domaine
- Pour des raisons de sécurité et de redondance 2 DC/domaine sont conseillés
- Promotion
  - Win2k/2k3 : commande DCPROMO
  - Win2k8/2k12/2k16 : Installation du rôle ADDS
- Le premier domaine est le domaine root de la forêt

## 2. Prérequis

- Système de fichiers NTFS
- Nom du DC ne doit pas être supérieur à 15 caractères (et ne pas utiliser des caractères spéciaux)
- Configuration IPv4/IPv6 en IP fixe
- Nom du domaine sous la forme : domaine.extension
- Serveur DNS

## 3. Installation

- Installer le rôle ADDS via la console server manager
- Ensuite « Promouvoir ce serveur en contrôleur de domaine »

## 4. Outils d'administration

- **Utilisateurs et Ordinateurs Active Directory** : administration des différents objets de l'annuaire (OU, groupe, utilisateur...).
- **Sites et Services Active Directory** : administration des sites AD et de la réPLICATION.
- **Domaine et approbation Active Directory** : création de relations d'approbation entre domaines ou entre forêts.
- **Gestion des stratégies de groupe** : création, administration et maintenance des différentes stratégies de groupe.
- **Modification ADSI** : modification des attributs LDAP.

## 5. Niveaux de fonctionnement

- Un niveau fonctionnel permet l'activation d'une ou plusieurs fonctionnalités pour un domaine ou une forêt. Plusieurs niveaux sont disponibles, toute modification de niveau est irréversible
- Les niveaux de fonctionnement (functional levels) sont possibles
  - Forêt (Forest functional level)
  - Domaine (Domain functional level)
- Ceci a un impact sur le domaine et/ou la forêt mais principalement sur les contrôleurs de domaine. Il est nécessaire d'avoir au minimum tous les contrôleurs de domaine qui exécutent le système d'exploitation correspondant à celui du niveau fonctionnel choisi. Si le niveau choisi est Windows Server 2008, les contrôleurs de domaine doivent au minimum exécuter Windows Server 2008.

## 5.1. Niveaux fonctionnels 2008

### Windows Server 2008

- Activation de la réPLICATION du système de fichiers **DFS** (Distributed File System) pour le dossier **SYSVOL**.
- Protocole AES (Advanced Encryption Services) 128 et 256 bits pour l'authentification Kerberos.
- Mise en place de la stratégie de mot de passe affinée.
- Au niveau de la forêt, aucune nouvelle fonctionnalité n'est apportée.

### Windows Server 2008R2

- Le niveau fonctionnel permet l'utilisation de la **corbeille AD**.

## 5.2. Niveaux fonctionnels 2012

### Windows Server 2012

- Kerberos Armoring
- Au niveau de la forêt, aucune nouvelle fonctionnalité n'est apportée.

### Windows Server 2012R2

- Silos de stratégies d'authentification : cette fonctionnalité permet l'application de stratégie d'authentification pour certains comptes (utilisateurs, ordinateurs, services).
- Stratégies d'authentification : appliquées aux comptes utilisateur, elles permettent d'indiquer sur quelle machine un utilisateur peut ouvrir une session. Cette fonctionnalité utilise un contrôle d'accès basé sur des conditions.
- Au niveau de la forêt, aucune nouvelle fonctionnalité n'est apportée.

## 5.3. Niveaux fonctionnels 2016

### Windows Server 2016

- Aucune nouveauté

## 5.4. Changement du niveau fonctionnel

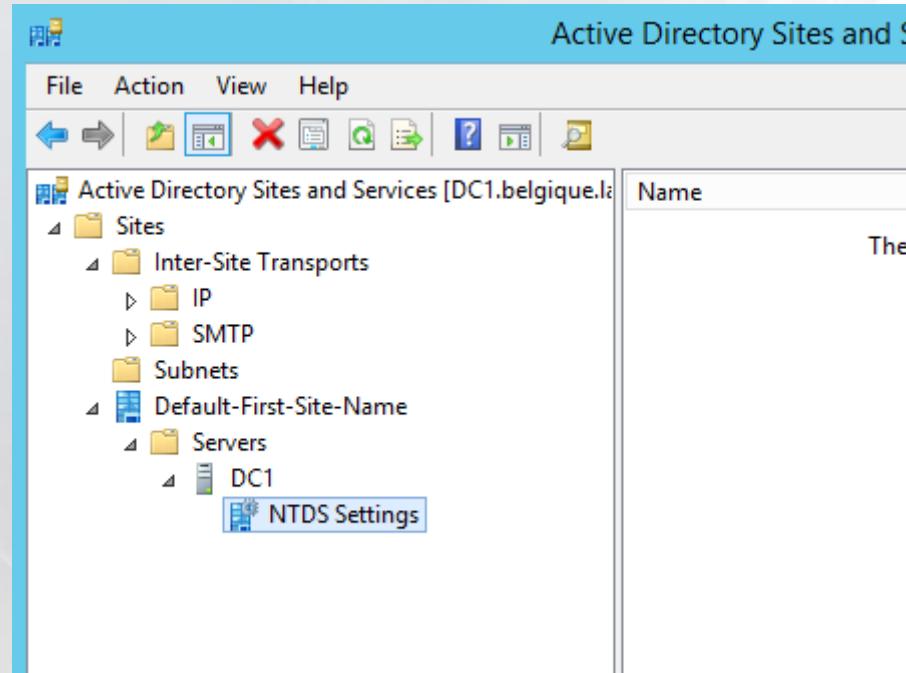
- Changement du Domain Functional Level
  - Console « utilisateurs et ordinateurs AD »
  - Sélectionnez le nom du domaine -> menu Action -> Augmenter le niveau fonctionnel du domaine
- Changement du Forest Functional Level
  - Console « Domaine et approbation AD »
  - Sélectionnez la racine de la console -> menu Action -> Augmenter le niveau fonctionnel de la forêt

## 6. Structure des objets dans l'AD

Builtin	Contient les groupes de sécurité par défaut de Windows.
Computers	Emplacement par défaut des comptes d'ordinateurs.
Domain Controllers (UO)	Emplacement pas défaut des comptes d'ordinateurs contrôleurs de domaine.
ForeignSecurityPrincipals	Contient les identificateurs de sécurité (SID, Security Identifiers).
Users	Emplacement par défaut des comptes d'utilisateurs.
LostAndFound	Contient des objets dont les conteneurs ont été supprimés.
System	Contient les paramètres systèmes intégrés spécifiques.

## 7. Vérification de l'installation – AD S&S

- AD Sites and services



# 7. Vérification de l'installation - DNS

DNS Manager

Name	Type	Data	Timestamp	
_msdcs	Start of Authority (SOA)	[155], dc1.belgique.lan, h...	static	
_sites	Name Server (NS)	dc1.belgique.lan.	static	
_tcp	Host (A)	192.168.1.1	21-10-16 1	
_udp	IPv6 Host (AAAA)	fd00:002a:002b:0001:0000:...	21-10-16 1	
DomainDnsZones	IPv6 Host (AAAA)	fd00:002a:002b:0001:2488:...	21-10-16 1	
ForestDnsZones	Client7	Host (A)	192.168.1.100	26-10-15 0
GlobalNames	dc1	Host (A)	192.168.1.1	static
info.lan	dc1	IPv6 Host (AAAA)	fd00:002a:002b:0001:2488:...	static
test.lan	dc1	IPv6 Host (AAAA)	fd00:002a:002b:0001:0000:...	static

DNS Manager

Name	Type	Data	Timestamp
_gc	Service Location (SRV)	[0][100][3268] dc1.belgique...	21-10-16 1
_kerberos	Service Location (SRV)	[0][100][88] dc1.belgique...	21-10-16 1
_kpasswd	Service Location (SRV)	[0][100][464] dc1.belgique...	21-10-16 1
_ldap	Service Location (SRV)	[0][100][389] dc1.belgique...	21-10-16 1

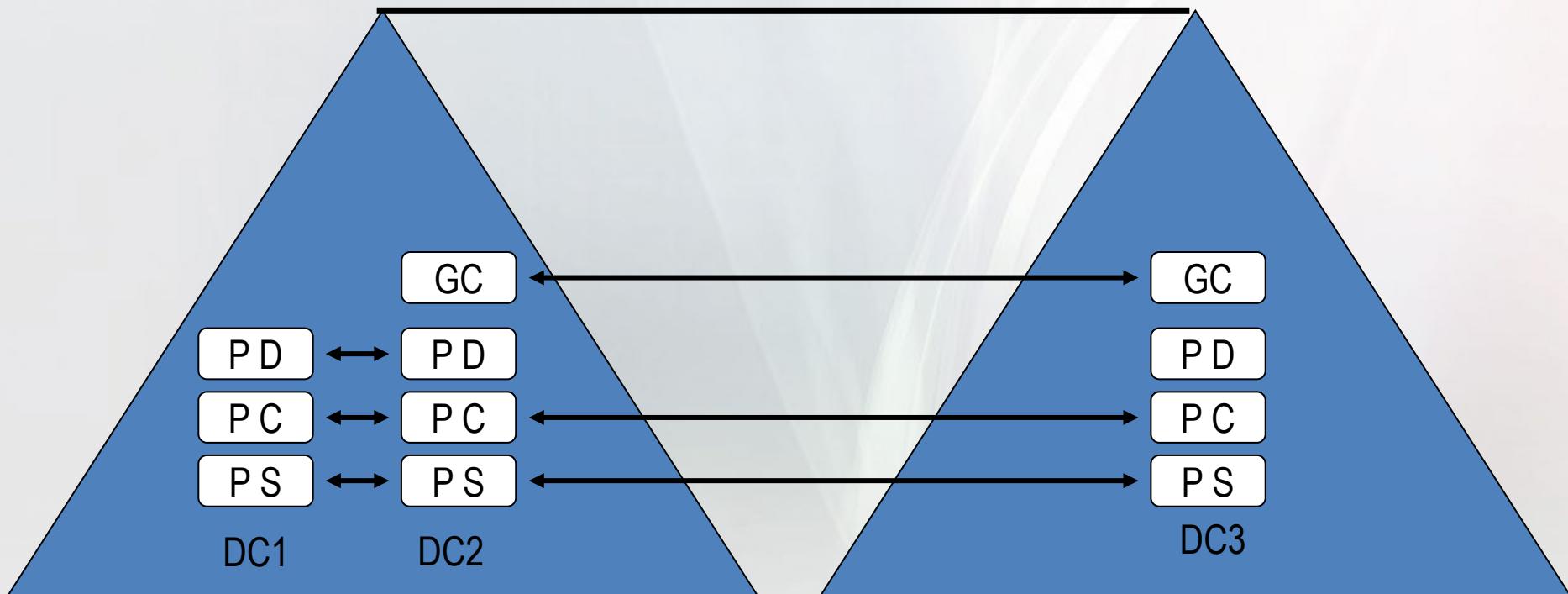
## 7. Vérification de l'installation - réPLICATION

- Vérifier la réPLICATION entre les différents DC  
dcdiag /test:replications

## 8. Les partitions de l'AD

- La BD active directory est divisée en 4 partitions
  - **Partition de domaine** : contient les informations sur les objets qui ont été créés dans un domaine (attributs de compte utilisateur et d'ordinateur...). Ces informations sont présentes uniquement sur l'ensemble des serveurs d'annuaire du domaine concerné.
  - **Partition de configuration** : permet de décrire la topologie de l'annuaire (liste complète des domaines, arborescences et forêt). L'ensemble des contrôleurs de domaine de la forêt se partagent les informations contenues dans cette partition.
  - **Partition de schéma** : contient tous les attributs et classes de tous les objets qui peuvent être créés. Lors de la création d'un compte utilisateur, l'objet et ses propriétés sont dupliqués depuis le schéma. Lors de l'ajout d'un nouveau service (Exchange, sccm,...), il est nécessaire de procéder à la mise à jour de cette partition. Il est intéressant de noter qu'un seul serveur dans la forêt contient le droit d'écriture sur le schéma, les autres étant uniquement en lecture seule.
  - **Partition DNS** (Partition d'application): contient la ou les bases de données DNS. Les informations de la base, les enregistrements y sont stockés.
- Emplacement physique %SystemRoot%\NTDS

## 9. RéPLICATION DES PARTITIONS



Si GC, le DC contient les partitions de son domaine + celle des autres domaines

# 10. Intégration des zones DNS dans l'AD

- ForestDNSZone.NomForêtDNS
  - Partition d'application automatiquement créée
  - Stocke les zones au niveau de la Forêt
  - RéPLICATION sur tous les DC de la Forêt
- DomainDNSZone.NomDomaineDns
  - Partition d'application automatiquement créée
  - Stocke les zones au niveau du domaine
  - RéPLICATION sur tous les DC du domaine
- Possibilité de créer ses propres partitions d'applications

# 11. DNS – zone intégrée dans l'AD

DNS	DNS ADI
Stockage dans un fichier	Stockage dans une BD
\system32\dns	Objet container de type DNSZONE
Enregistrement de ressources (RR)	Objet de type dnsnode

Avantages des ADI :

- Multi-maître
- Sécurité avancée des contrôles d'accès sur la zone et les enregistrements

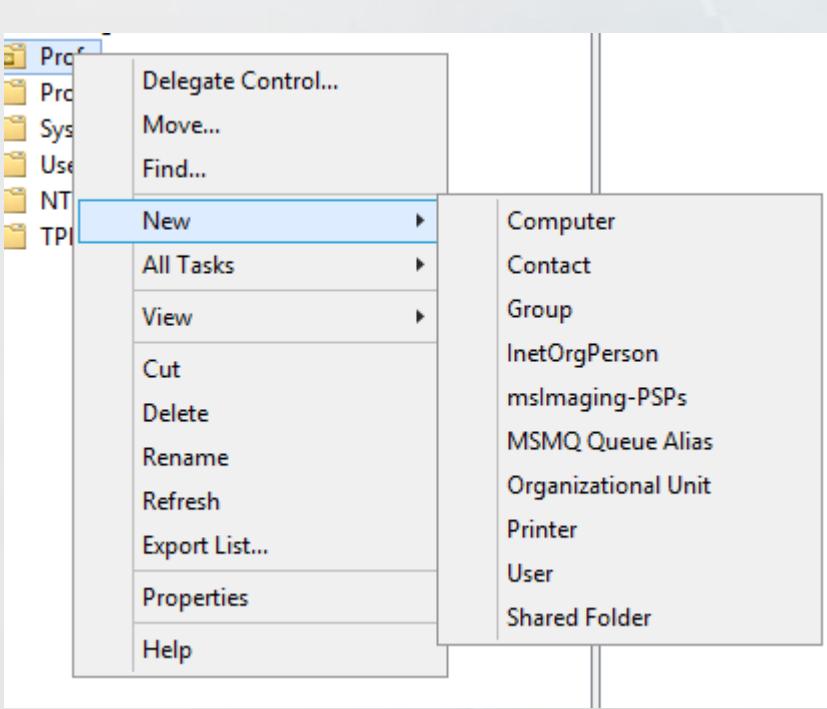
# Module 9

## Les objets de l'Active Directory

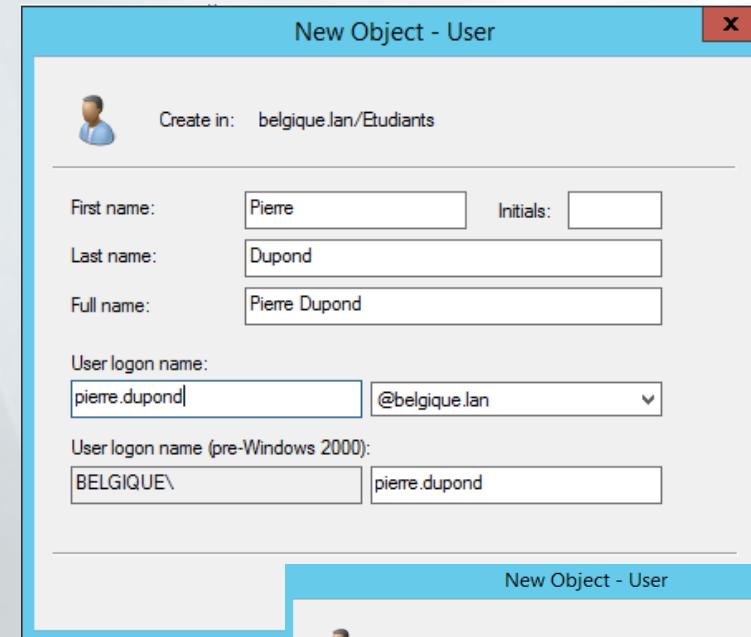
# 1. L'utilisateur

- Création des utilisateurs avec la console AD users & computers
- Utilisateur est authentifié par le DC
- Après l'authentification, un jeton est attribué à la «personne » contenant
  - SID du compte utilisateur
  - Les SID des groupes dont il est membre
- Les comptes utilisateurs peuvent être
  - Locaux : stocké dans la SAM (Security Account Manager)
  - De domaine : stocké dans l'AD

## 2. Crédation d'un utilisateur



New Object - User



Create in: belgique.lan/Etudiants

First name: Pierre Initials:

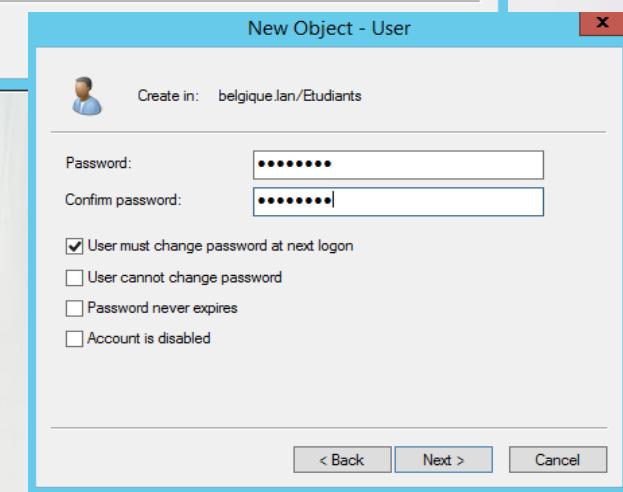
Last name: Dupond

Full name: Pierre Dupond

User logon name:  
pierre.dupond @belgique.lan

User logon name (pre-Windows 2000):  
BELGIQUE\pierre.dupond

New Object - User



Create in: belgique.lan/Etudiants

Password:  Confirm password:

User must change password at next logon  
 User cannot change password  
 Password never expires  
 Account is disabled

< Back Next > Cancel

# 3. Propriétés de l'utilisateur

Pierre Dupond Properties

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		
Pierre Dupond							
First name:	<input type="text" value="Pierre"/>	Initials:	<input type="text"/>				
Last name:	<input type="text" value="Dupond"/>						
Display name:	<input type="text" value="Pierre Dupond"/>						
Description:	<input type="text"/>						
Office:	<input type="text"/>						
Telephone number:	<input type="text"/>	<input type="button" value="Other..."/>					
E-mail:	<input type="text"/>						
Web page:	<input type="text"/>	<input type="button" value="Other..."/>					

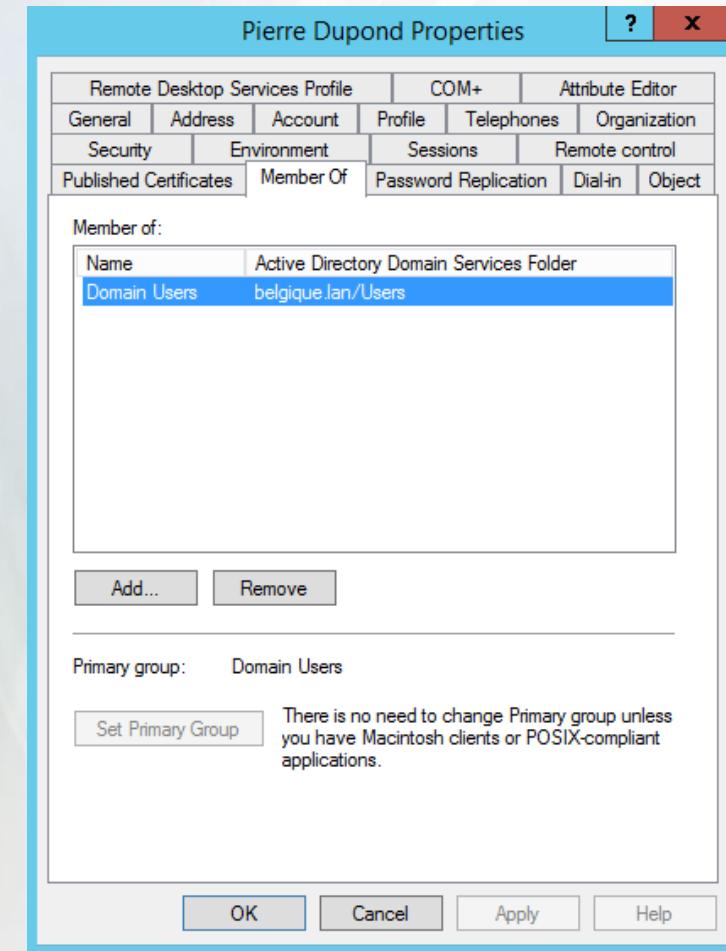
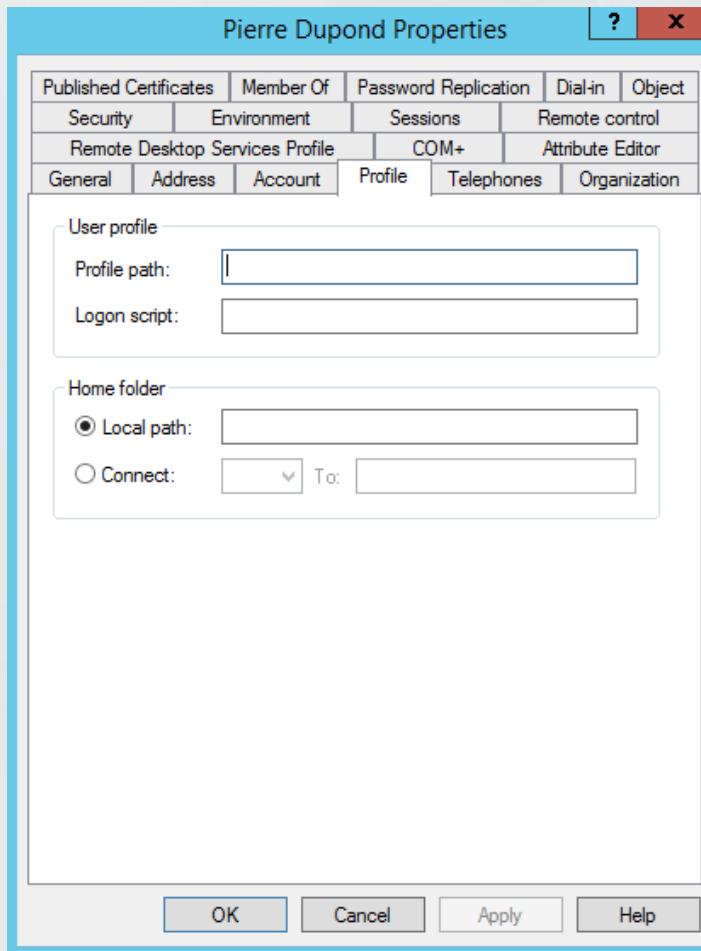
OK Cancel Apply Help

Pierre Dupond Properties

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: <input type="text" value="pierre.dupond"/> @belgique.lan							
User logon name (pre-Windows 2000): <input type="text" value="BELGIQUE\pierre.dupond"/>							
<input type="button" value="Logon Hours..."/> <input type="button" value="Log On To..."/>							
<input type="checkbox"/> Unlock account							
Account options:							
<input checked="" type="checkbox"/> User must change password at next logon							
<input type="checkbox"/> User cannot change password							
<input type="checkbox"/> Password never expires							
<input type="checkbox"/> Store password using reversible encryption							
Account expires							
<input checked="" type="radio"/> Never							
<input type="radio"/> End of: <input type="text" value="dimanche 20 novembre 2016"/>							

OK Cancel Apply Help

# 3. Propriétés de l'utilisateur



### 3. Propriétés de l'utilisateur

Pierre Dupond Properties

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

Attributes:

Attribute	Value
desktopProfile	<not set>
destinationIndicator	<not set>
displayName	Pierre Dupond
displayNamePrintable	<not set>
distinguishedName	CN=Pierre Dupond,OU=Etudiants,DC=belgique
division	<not set>
dSASignature	<not set>
dSCorePropagationD...	0x0 = ( )
dynamicLDAPServer	<not set>
employeeID	<not set>
employeeNumber	<not set>
employeeType	<not set>
extensionName	<not set>
facsimileTelephoneN...	<not set>

Buttons: Edit, Filter, OK, Cancel, Apply, Help

Effective User

## 4. Crédation d'un modèle d'utilisateur

- A partir d'un compte modèle (utilisateur désactivé ou non), créer des utilisateurs du même type
- Compléter les données communes dans les onglets Général, Adresse, Compte, Profil et Organisation
- Clic droit sur le compte modèle > Copier
- Compléter les données individuelles (login, pswd, ...)

## 5. Jeton d'accès

- LSA : Local Security Authority  
traite les requêtes d'authentification
- Protocole d'authentification
  - Kerberos v5 (préféré)
  - NTLM / NTLMv2
- Après authentification création d'un jeton d'accès
  - SID du compte
  - SID des groupes dont fait partie l'utilisateur  
si changement de groupe > prise en compte après réauthentification

Nombre de groupe est élevé → Occupation de la BP

## 6. Les groupes

- 2 types de groupes :
    - Sécurité : possibilité de mettre des permissions.
    - Distribution : groupement logique d'utilisateurs sans permission.
  - 3 étendues des groupes :
    - Groupes Globaux
    - Groupes locaux de domaines
    - Groupes universels
  - Nomenclature
    - L'étendue (G, U ou DL)
    - Le nom
    - Les permissions (w, m, r)
- Exemple : G\_Direction\_w

## 7. Les groupes globaux

- Membres : Comptes utilisateurs et groupes globaux du même domaine
- Membres de : Groupes locaux de domaines
- Etendue : Visibles dans leur domaine et dans tous les domaines approuvés
- Autorisations pour : Tous les domaines de la forêt

## 8. Groupes locaux de domaine

- Membres : Comptes d'utilisateurs, groupes globaux et groupes universels d'un domaine quelconque de la forêt, et groupes locaux de domaine du même domaine
- Membres de : Groupes locaux de domaine du même domaine
- Etendue : Visibles dans leur propre domaine
- Autorisations pour : Le domaine dans lequel le groupe local de domaine existe

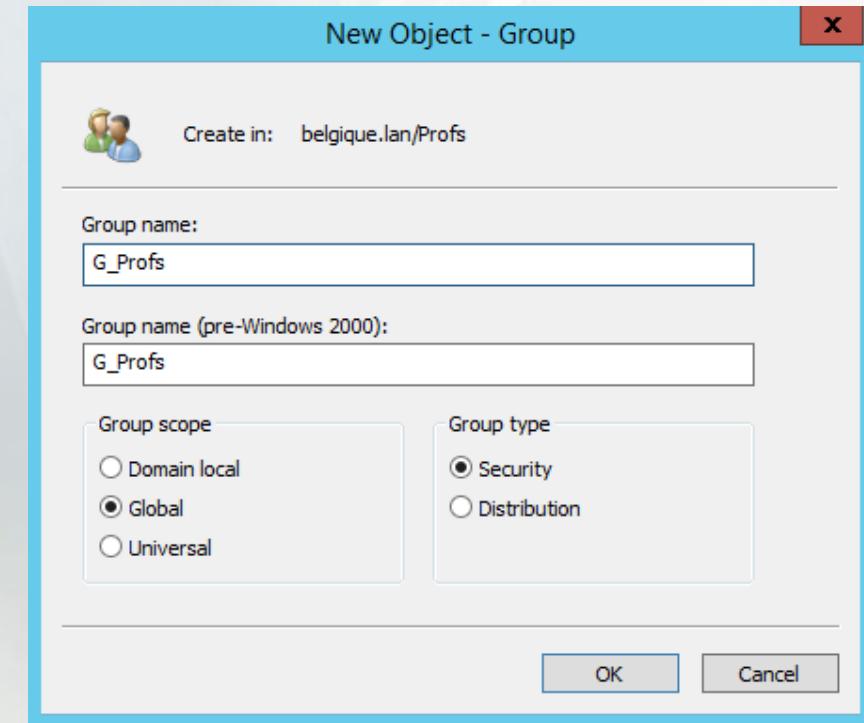
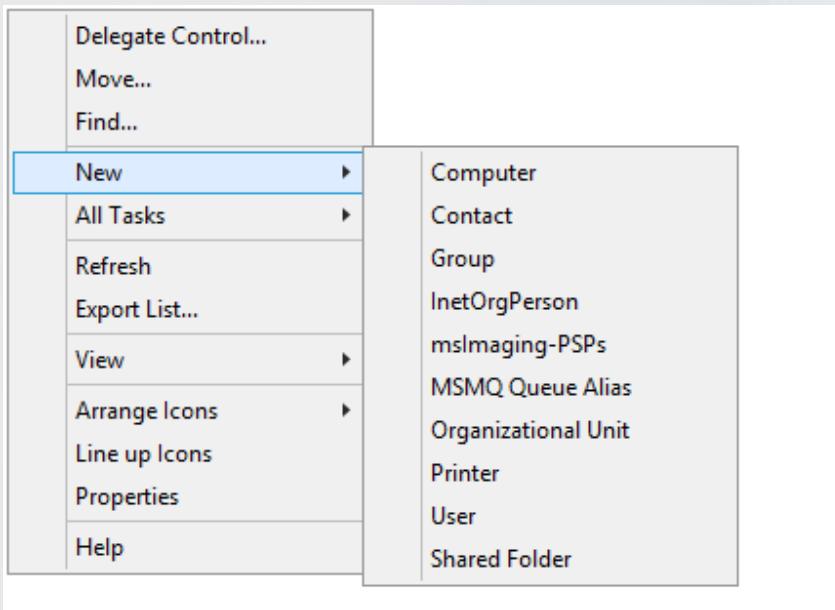
## 9. Les groupes universels

- Membres : Comptes d'utilisateurs, groupes globaux et autres groupes universels d'un domaine quelconque de la forêt
- Membres de : Groupes locaux de domaine et universels de tout domaine
- Etendue : Visibles dans tous les domaines de la forêt
- Autorisations pour : Tous les domaines de la forêt

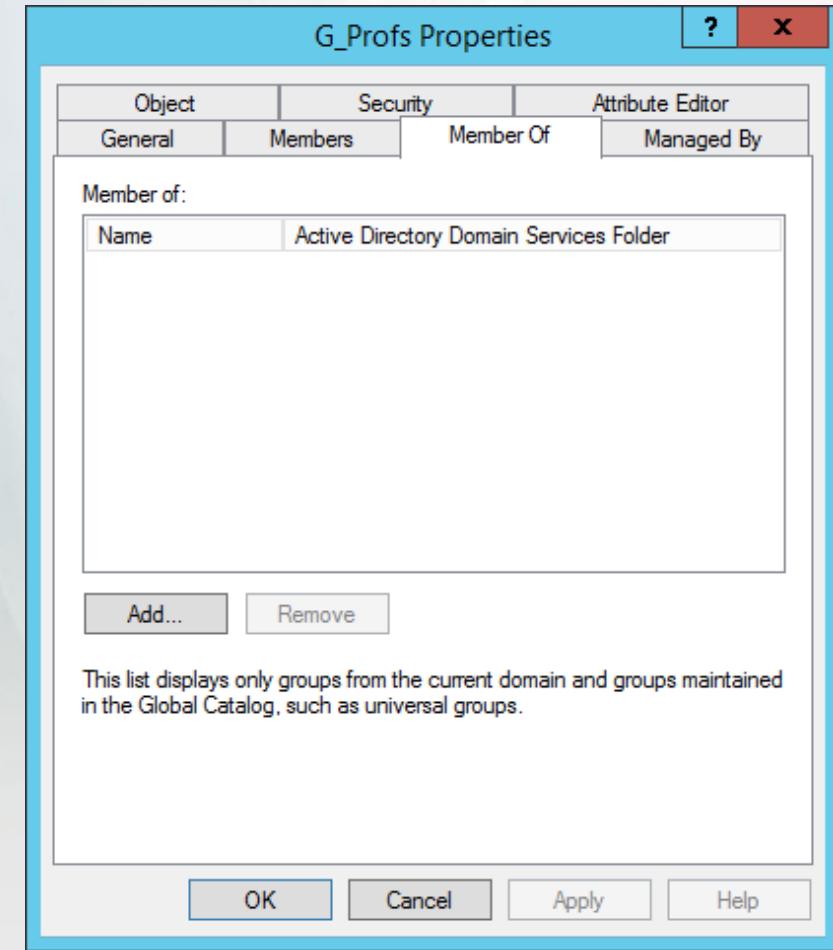
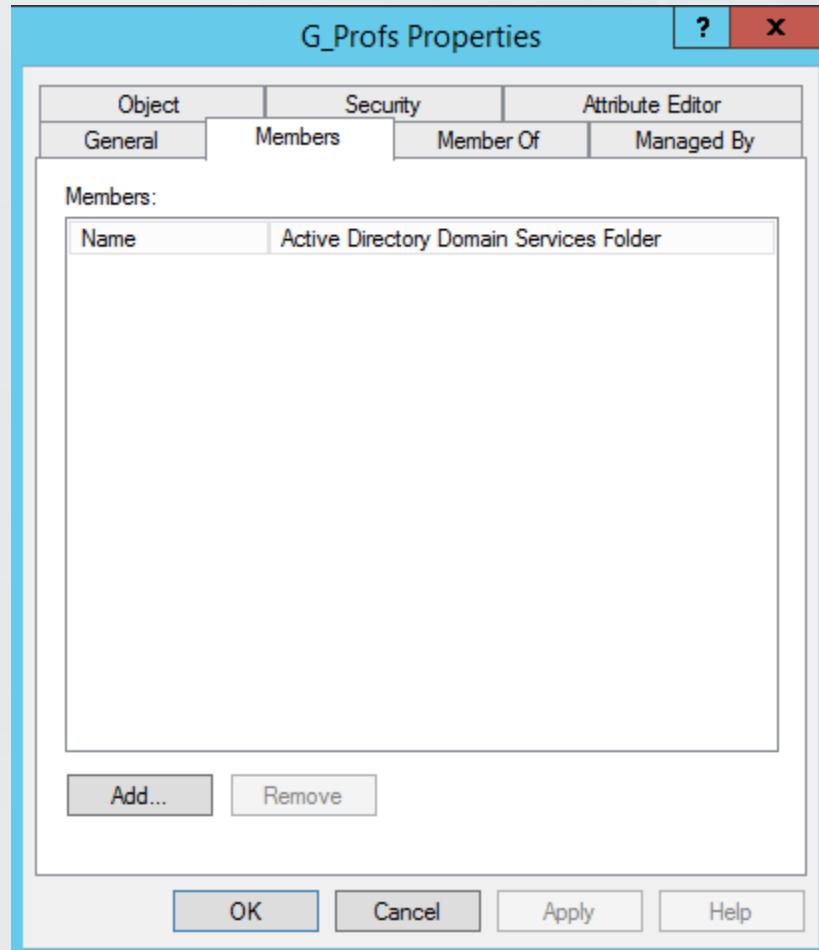
# 10. L'utilisation des groupes

- La stratégie d'utilisation des groupes dans un domaine est A G DL P
  - A : Account
  - G : Global Group
  - DL : Domain Local Group
  - P : Permission
- Si utilisation de groupes universels : A G U DL P

# 11. Crédation d'un groupe



# 12. Propriétés d'un groupe



## 13. Le compte Ordinateur

- Un ordinateur doit être membre du domaine pour pouvoir ouvrir une session dans le domaine
- Un compte ordinateur posséde
  - Un nom d'ouverture de session (sAMAccountName)
  - Un mot de passe
  - Un SID
- Par défaut le mot de passe du compte ordinateur est changé tous les 30 jours par défaut

## 14. Le conteneur Computers

- Par défaut les ordinateurs du domaine sont créés dans le conteneur Computers
- Conteneur Computers
  - Dossier système (pas une UO)
  - Impossible de mettre des GPO (Group Policy Object)
- Déplacer les objets ordinateurs dans une UO
- Modifier l'emplacement de création vers une UO
  - Créer l'UO qui accueillera les comptes ordinateurs (ex : PC)
  - Taper la commande

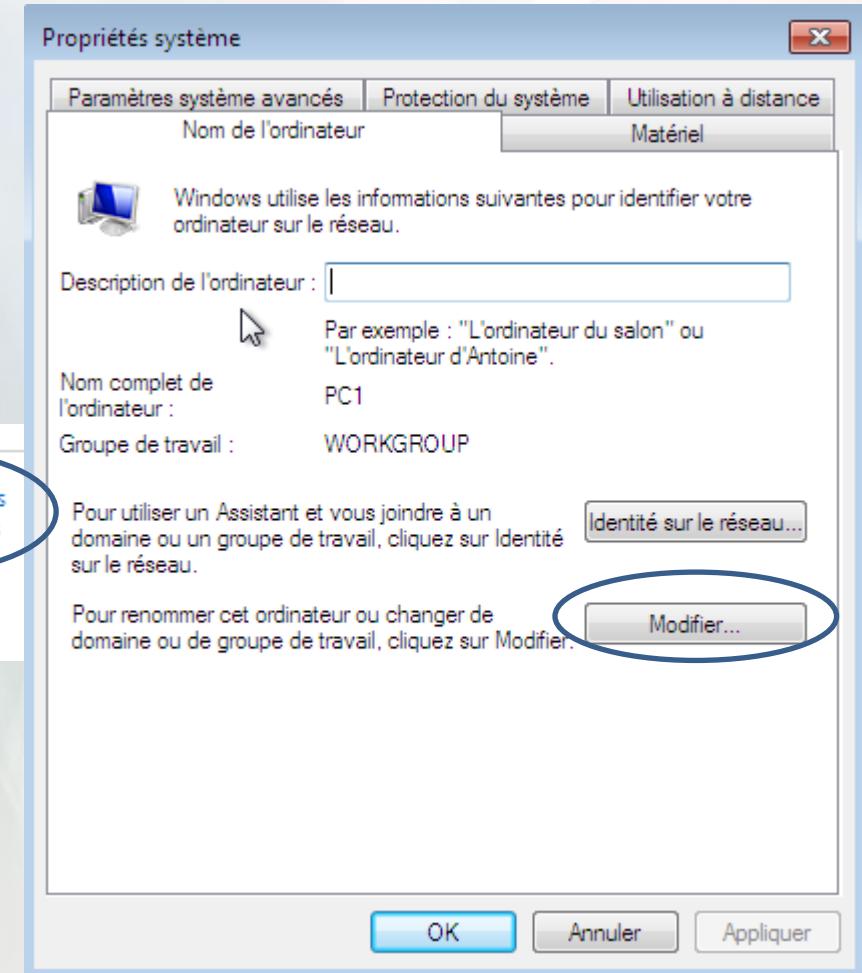
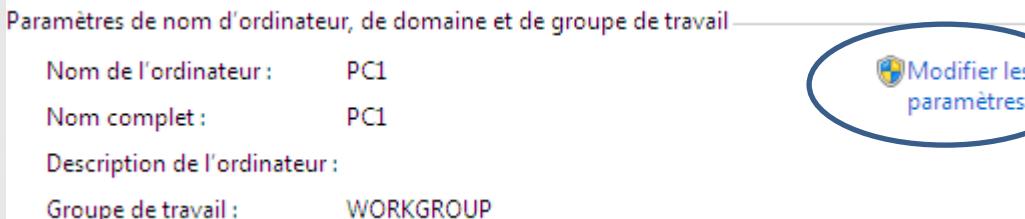
```
redircmp "OU=PC,DC=Belgique,DC=lan"
```

# Module 10

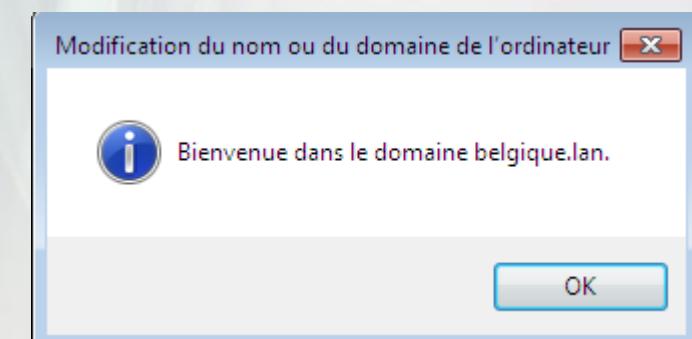
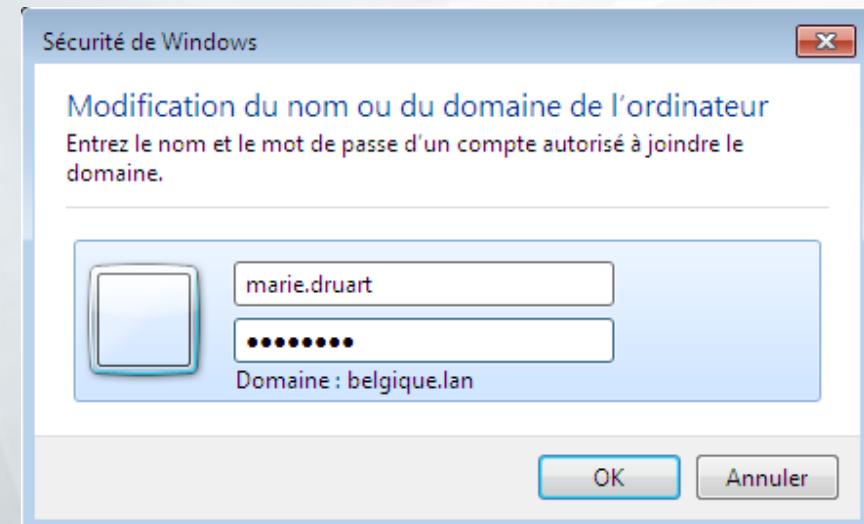
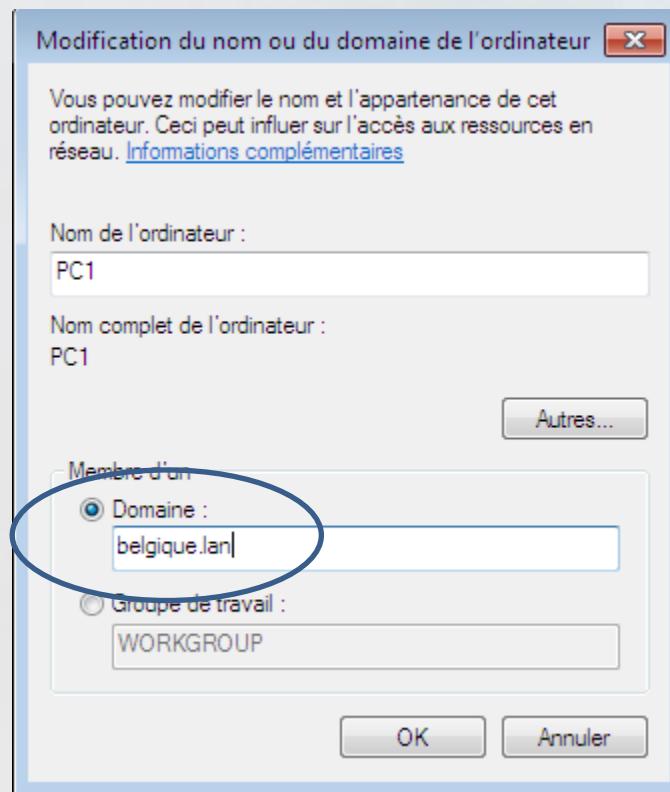
## Utilisation de l'Active Directory

# 1. Ajout d'un ordinateur dans le domaine

- Configuration minimale
  - IP/Mask
  - DNS
- Dans Panneaux de configuration → Système



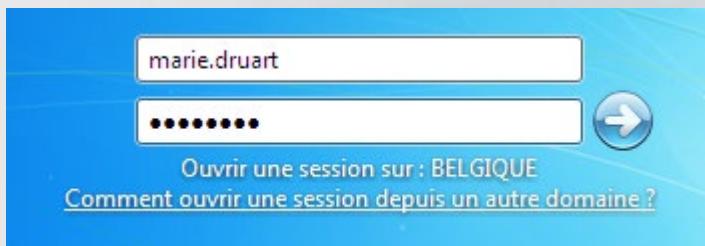
# 1. Ajout d'un ordinateur dans le domaine



L'ordinateur doit redémarrer

## 2. Ouverture de session

Sans UPN



marie.druart

\*\*\*\*\*

Ouvrir une session sur : BELGIQUE

[Comment ouvrir une session depuis un autre domaine ?](#)

Avec UPN



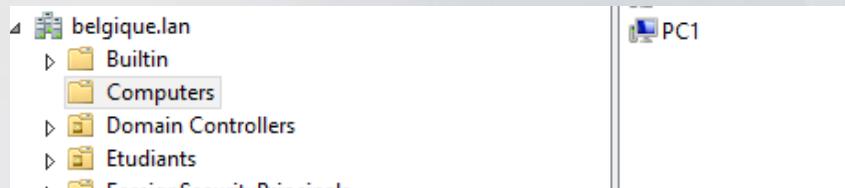
marie.druart@belgique.lan

\*\*\*\*\*

Ouvrir une session sur : belgique.lan

[Comment ouvrir une session depuis un autre domaine ?](#)

# 3. Ordinateur dans le domaine



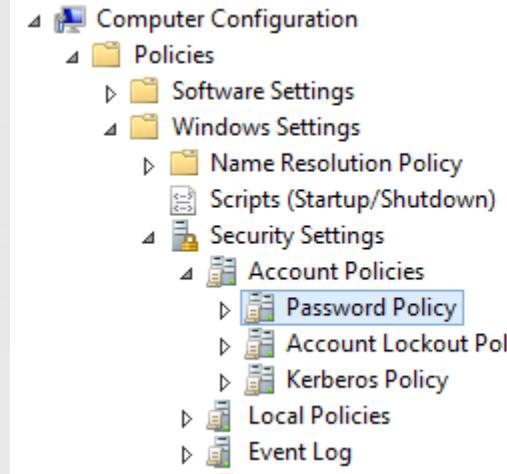
PC1

	Name Server (NS)
(same as parent folder)	Host (A)
(same as parent folder)	IPv6 Host (AAAA)
(same as parent folder)	IPv6 Host (AAAA)
Client7	Host (A)
Client7	IPv6 Host (AAAA)
dc1	Host (A)
dc1	IPv6 Host (AAAA)
dc1	IPv6 Host (AAAA)
PC1	Host (A)
PC1	IPv6 Host (AAAA)

# 4. Gestion des mots de passe

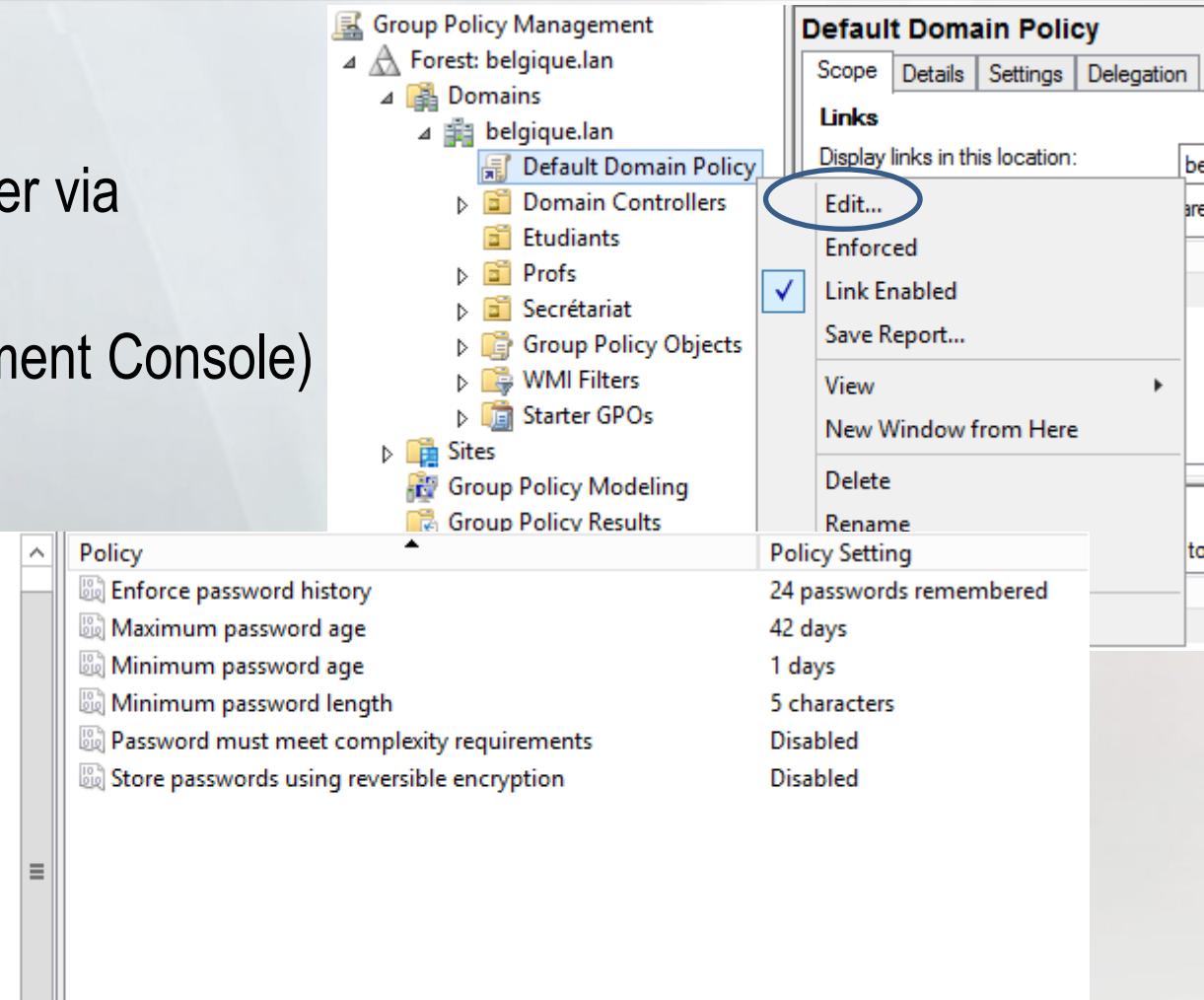
- Règle par défaut
- Possibilité de changer via GPMC

(Group Policy Management Console)



The navigation tree on the left shows the following structure:

- Computer Configuration
  - Policies
    - Software Settings
    - Windows Settings
      - Name Resolution Policy
      - Scripts (Startup/Shutdown)
    - Security Settings
      - Account Policies
        - Password Policy
        - Account Lockout Policy
        - Kerberos Policy
      - Local Policies
      - Event Log

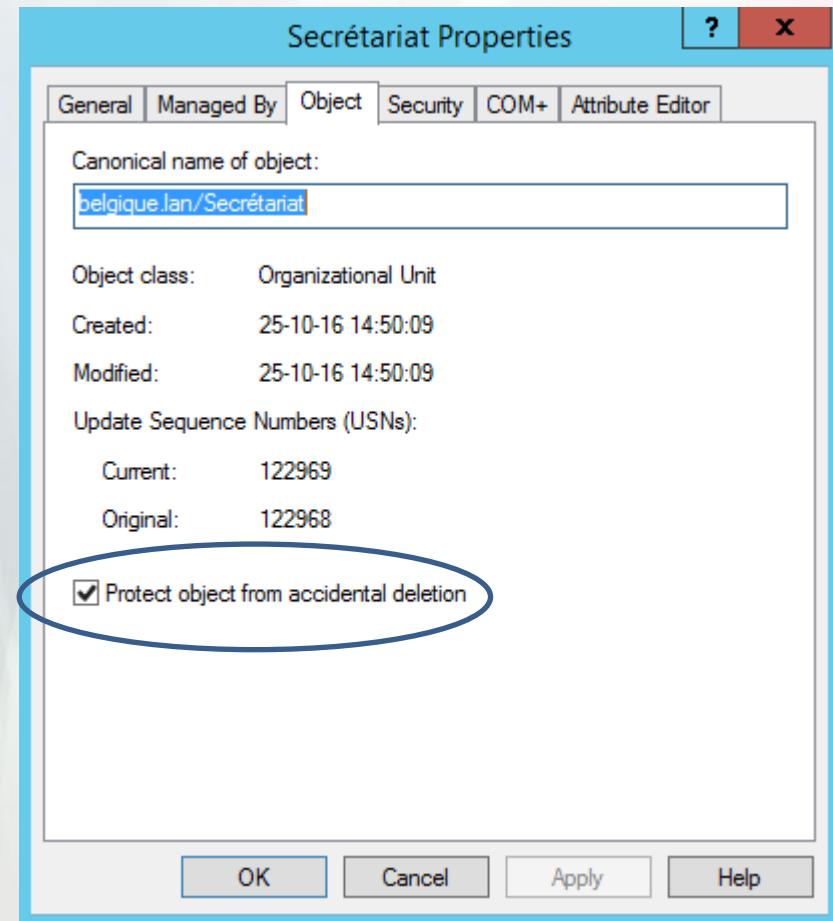
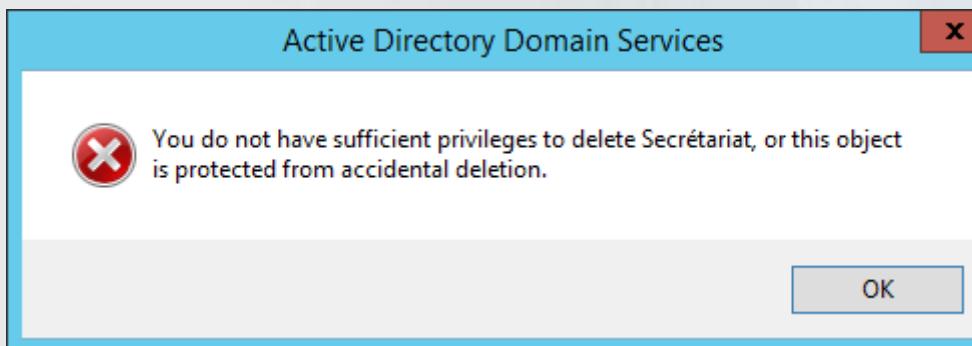


The right pane displays the "Default Domain Policy" settings under the "Policy" tab. A context menu is open over the "Default Domain Policy" node, with the "Edit..." option circled in blue.

Policy Setting	Description
24 passwords remembered	42 days
42 days	1 days
1 days	5 characters
5 characters	Disabled
Disabled	Disabled
Disabled	

## 5. Supprimer un objet

- Exemple une UO



## 6. Déléguer des droits sur une UO (1)

Active Directory Users and Computers [DC1.belgique.lan]

- > Saved Queries
- belgique.lan
  - > Builtin
  - > Computers
- > Domain Controllers
- Etudiants** (selected)
  - Delegate Control...** (circled)
  - Move...
  - Find...
  - New
- > ForeignS
- > LostAndFound
- > Managed
- > Profs
- > Program

Name
Eleve1
Eleve2
Eleve3
Etudiants
GG_Etudiants
Pierre Dupond

### Delegation of Control Wizard

#### Users or Groups

Select one or more users or groups to whom you want to delegate control.



Selected users and groups:

Marie Druart (marie.druart@belgique.lan)

Add...

Remove

### Delegation of Control Wizard

#### Tasks to Delegate

You can select common tasks or customize your own.



Delegate the following common tasks:

- Create, delete, and manage user accounts
- Reset user passwords and force password change at next logon
- Read all user information
- Create, delete and manage groups
- Modify the membership of a group
- Manage Group Policy links
- Generate Resultant Set of Policy (Planning)

Create a custom task to delegate

< Back

Next >

Cancel

Help

# 6. Déléguer des droits sur une UO (2)

Screenshot of the Windows Active Directory Properties window for the "Etudiants" container.

The left sidebar shows a context menu with the following options:

- Delegate Control...
- Move...
- Find...
- New
- All Tasks
- View
- Cut
- Delete
- Rename
- Refresh
- Export List...
- Properties** (circled in blue)
- Help

The main window title is "Etudiants Properties". The "Security" tab is selected. The "Group or user names:" list includes "Everyone", "SELF", "Authenticated Users", "SYSTEM", "Eleve1 (eleve1@belgique.lan)" (selected), and "Domain Admins (BELGIQUE\Domain Admins)". Below this is a table of permissions for "Eleve1".

	Allow	Deny
Create all child objects	<input type="checkbox"/>	<input type="checkbox"/>
Delete all child objects	<input type="checkbox"/>	<input type="checkbox"/>
Generate resultant set of policy (logging)	<input type="checkbox"/>	<input type="checkbox"/>
Generate resultant set of policy (planning)	<input type="checkbox"/>	<input type="checkbox"/>
Special permissions	<input checked="" type="checkbox"/>	<input type="checkbox"/>

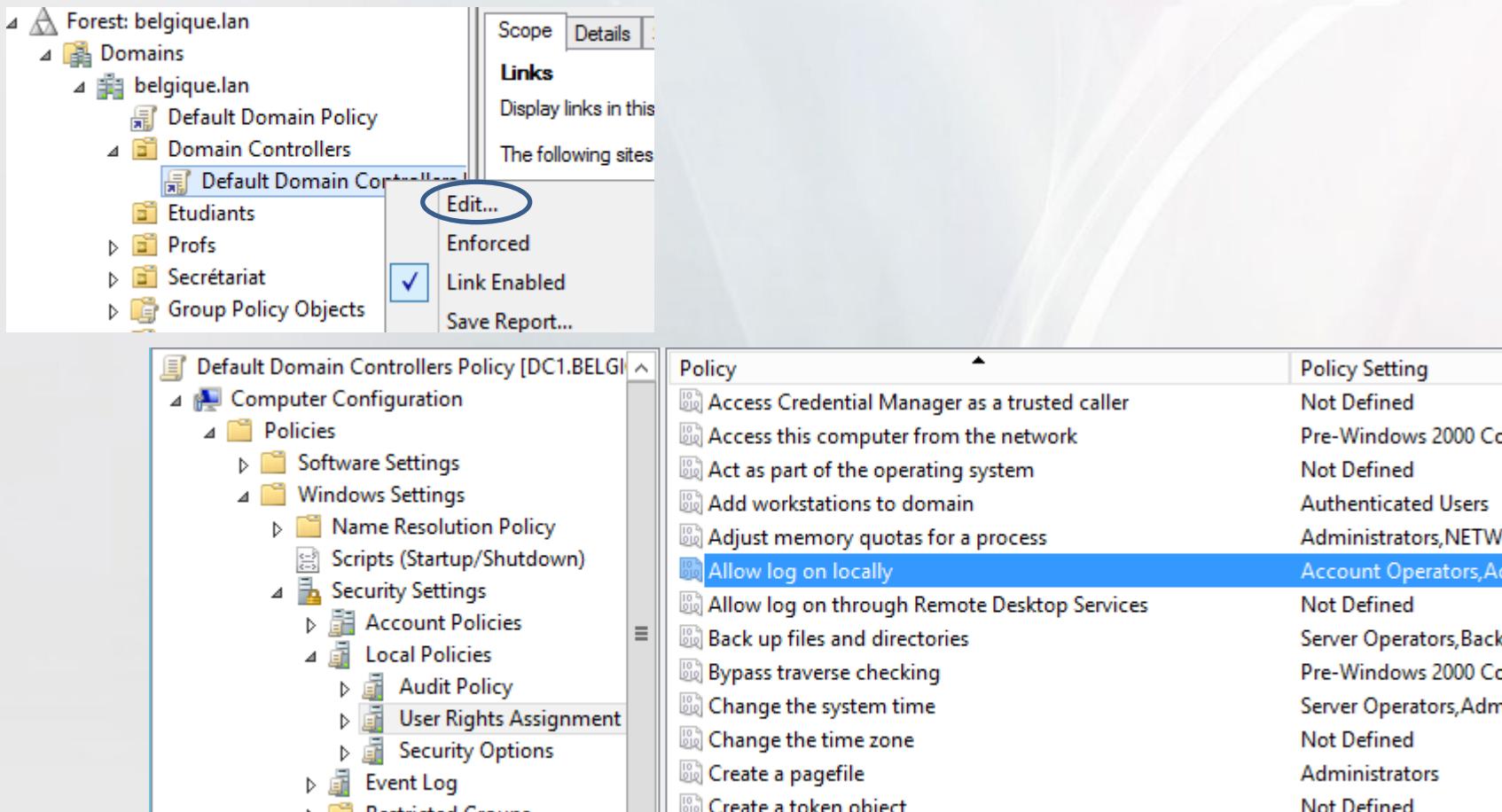
A blue oval highlights the "Advanced" button at the bottom right of the permission table. Below the table, the text "For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available)." is displayed.

The "Owner" is listed as "Domain Admins (BELGIQUE\Domain Admins) [Change](#)". Below the owner information are tabs for "Permissions", "Auditing", and "Effective Access".

The "Permissions" tab displays a table of permission entries:

Type	Principal	Access	Inherited from	Applies to
Deny	Everyone	Special	None	This object only
Allow	Eleve1 (eleve1@belgique.lan)	Reset password	None	Descendant User objects
Allow	Eleve1 (eleve1@belgique.lan)		None	Descendant User objects
Allow	Account Operators (BELGIQUE\Account Operators)	Create/delete InetOrgObj	None	This object only
Allow	Account Operators (BELGIQUE\Account Operators)	Create/delete Computer	None	This object only
Allow	Account Operators (BELGIQUE\Account Operators)	Create/delete Group	None	This object only

# 7. logger un utilisateur sur le DC



The screenshot shows the Group Policy Management console. On the left, the navigation pane displays the forest 'belgique.lan' and its domains, including 'belgique.lan' which contains 'Default Domain Policy', 'Domain Controllers', and 'Group Policy Objects'. The 'Default Domain Controllers Policy' is selected and highlighted with a blue oval around the 'Edit...' option in the context menu.

The main pane shows the policy settings for the 'Default Domain Controllers Policy [DC1.BELGIQUE.LAN]'. The 'Policy' table lists various security settings:

Policy	Policy Setting
Access Credential Manager as a trusted caller	Not Defined
Access this computer from the network	Pre-Windows 2000 Computer Operators
Act as part of the operating system	Not Defined
Add workstations to domain	Authenticated Users
Adjust memory quotas for a process	Administrators,NETWKWGRUPPERS
<b>Allow log on locally</b>	<b>Account Operators,Administrators</b>
Allow log on through Remote Desktop Services	Not Defined
Back up files and directories	Server Operators,Backup Operators
Bypass traverse checking	Pre-Windows 2000 Computer Operators
Change the system time	Server Operators,Administrators
Change the time zone	Not Defined
Create a pagefile	Administrators
Create a token object	Not Defined

# 8. Rechercher dans l'AD à partir d'un client

Screenshot showing the Windows Network window and the Active Directory User Search dialog.

The Network window shows a search results pane for "Réseau". The search results table lists users and groups:

Nom	Type	Description
Denied RODC P...	Groupe	Members in this group cannot ha...
Eleve1	Utilisateur	
<b>prof3</b>	Utilisateur	
Prof2	Utilisateur	
Prof1	Utilisateur	
krbtgt	Utilisateur	Key Distribution Center Service A
Guest	Utilisateur	Built-in account for quest access

The Active Directory User Search dialog is open, showing the results for "prof3".

Properties dialog for user "prof3":

- Général tab selected
- Address: [Empty]
- Boîte postale: [Empty]
- Ville: [Empty]
- Département ou région: [Empty]
- Code postal: [Empty]
- Pays/région: [Empty]

# Module 11

## Les maîtres d'opération FSMO

# 1. Les maîtres d'opération FSMO

Les DC sont multi-maîtres sauf pour 5 choses :

- Contrôleur de schéma
- Maître d'attribution des noms de domaine (DNM)
- Emulateur PDC
- RID master
- Maître d'infrastructure (IM)

Ces DC sont appelés « maître d'opération » ou FSMO (Flexible Single Master Operation)

## 1.1. Le maître de schéma

- Ce rôle doit être unique au sein de la forêt et est joué par le DC root.
- Permet la modification du schéma
- Seul les administrateurs du schéma peuvent modifier le schéma.

## 1.2. Le maître d'attribution des noms de domaines

- Gère la modification (ajout ou suppression) des domaines d'une forêt.
- Unique au sein de la forêt
- DID : Domain ID
- Doit être catalogue global

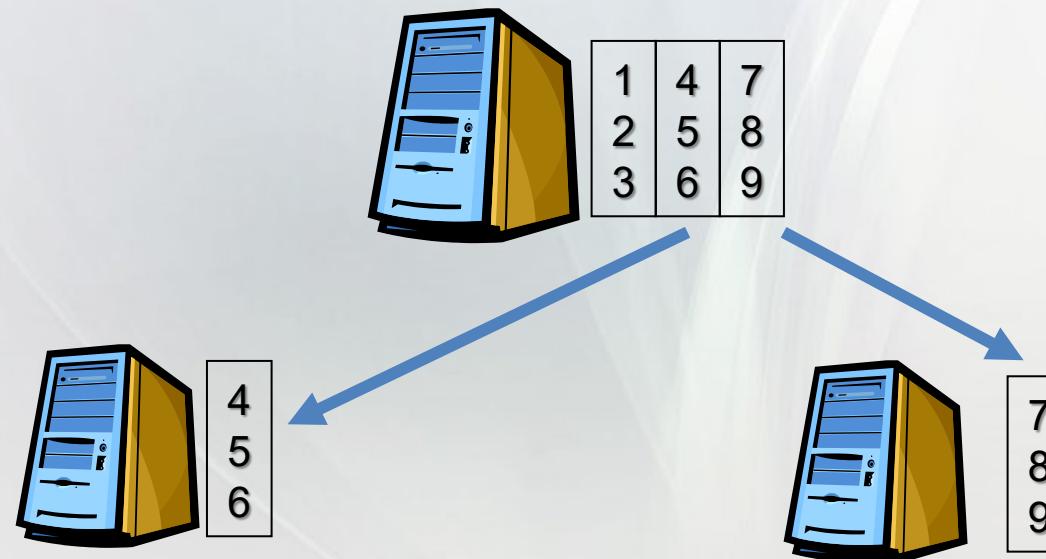
## 1.3. PDC Emulator

- Gestion des BDC de NT4 après migration
- Gestion des mots de passes
  - Pswd changé est envoyé en priorité au PDC Emulator
  - DC ne connaissant pas le pswd, il interroge le PDC emulator
- Synchronisation des horloges
- Unique au sein du domaine

## 1.4. RID master

- Création d'un objet : SID (security ID)

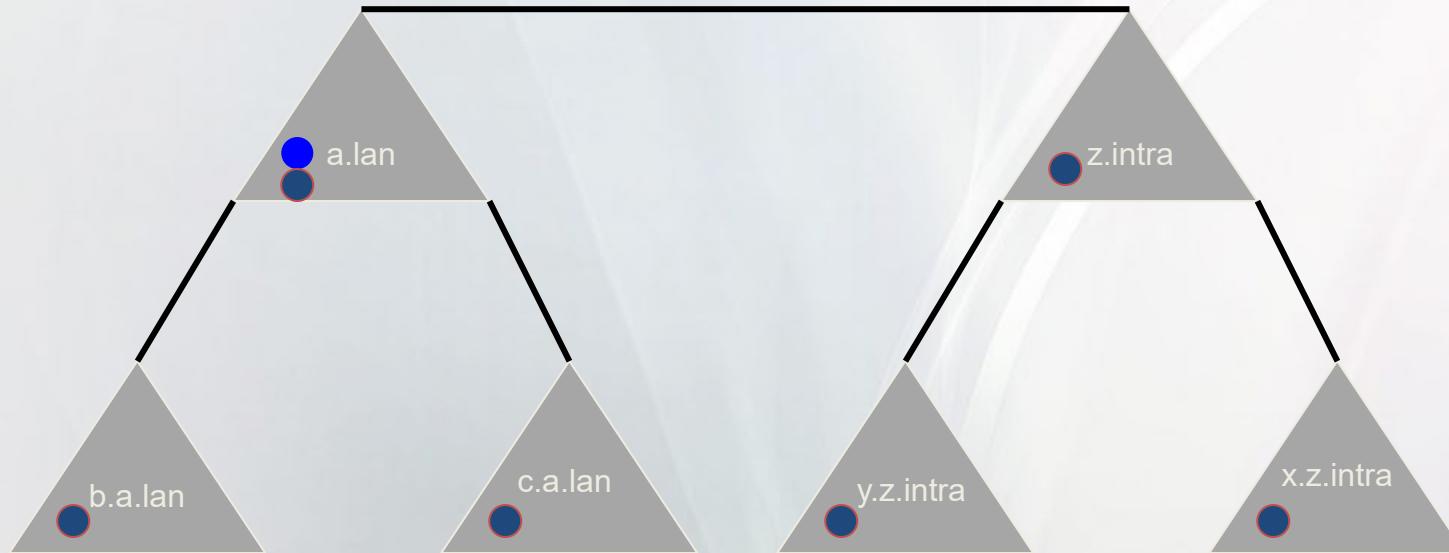
$$\text{SID} = \text{DID} + \text{RID}$$



## 1.5. Infrastructure Master

- Lors d'un changement d'un objet de domaine le SID change.
- L'objet peut être associé à d'autre objet de domaine différents => le SID ne peut changer
- L'IM fait donc mettre à jour les objets avec le nouveau SID

## 1.6. Emplacement



- Contrôleur de schéma + DNM
- RID master + IM + PDC emulator

## 1.7. Contraintes

- Le maître d'attribution des noms de domaine (DNM) doit être catalogue globale.
- Si il y a plusieurs DC dans un même domaine, l'IM et le catalogue globale ne doivent être sur le même DC.

## 2. Outils d'administration

- Afin de trouver les différents maîtres d'opération, vous aurez besoin d'utiliser les trois consoles suivantes :
  - Utilisateurs et ordinateurs Active Directory
  - Domaines et approbations Active Directory
  - Schéma Active Directory

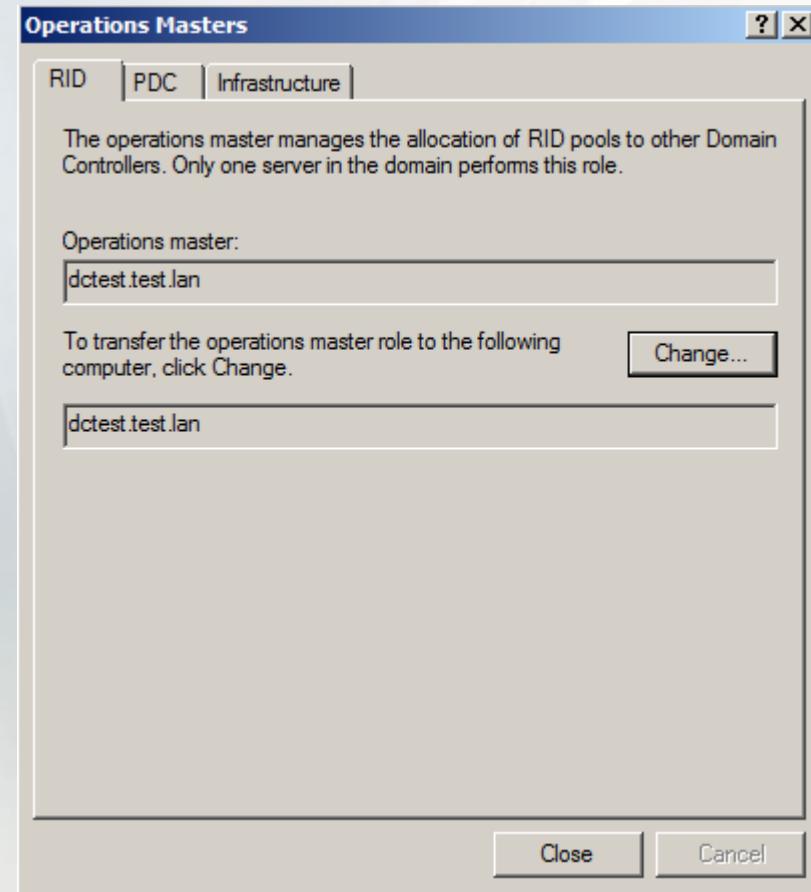
## 2.1. RID, PDC et IM

Utilisateurs et ordinateurs AD

CD Utilisateurs et ordinateurs AD

Maître d'opérations

Choisissez le FSMO



## 2.2. SM

Installer adminpak.msi



Lancer MMC et installer le composant « Schéma AD »



CD Schéma AD



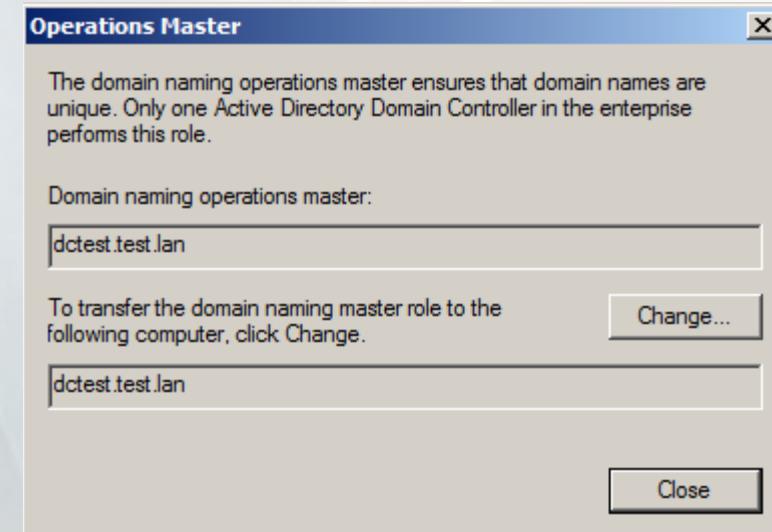
Maître d'opération

## 2.3. DNM

Domaines et approbations AD

CD Domaines et approbations AD

Maître d'opérations



### 3. Problèmes liés aux FSM

- Impossible d'ajouter ou de supprimer un domaine
- Impossible de créer des objets dans l'AD
- Impossible de modifier le schéma
- Les modifications apportées aux membres des groupes ne sont pas appliquées
- Les clients ne peuvent accéder aux ressources d'un autre domaine

## 4. Modifier l'emplacement d'un FSMO (1)

- Transfert de rôle : Les deux DC sont en état de marche
- La prise de contrôle : Lorsque le DC maître d'opération est déconnecté

## 4. Modifier l'emplacement d'un FSMO (2)

- NTDSUTIL
  - Roles
    - Connections
      - Connect to server « Nom de domaine »
      - Set creds « Nom de domaine » « user » « pswd »
      - Quit
    - Seize « nom rôle » (RID master; PDC; infrastructure master; domain naming master; schema master)
    - Quit
  - Quit

## 5. Le catalogue global

- DC ayant une copie des attributs les plus utilisés de tous les objets de l'AD.
- Choix des attributs via la console Schéma AD
- Permet d'effectuer des recherches dans toute la forêt.
- Consultation du GC :
  - Ouverture de session
  - Imbrication de groupe

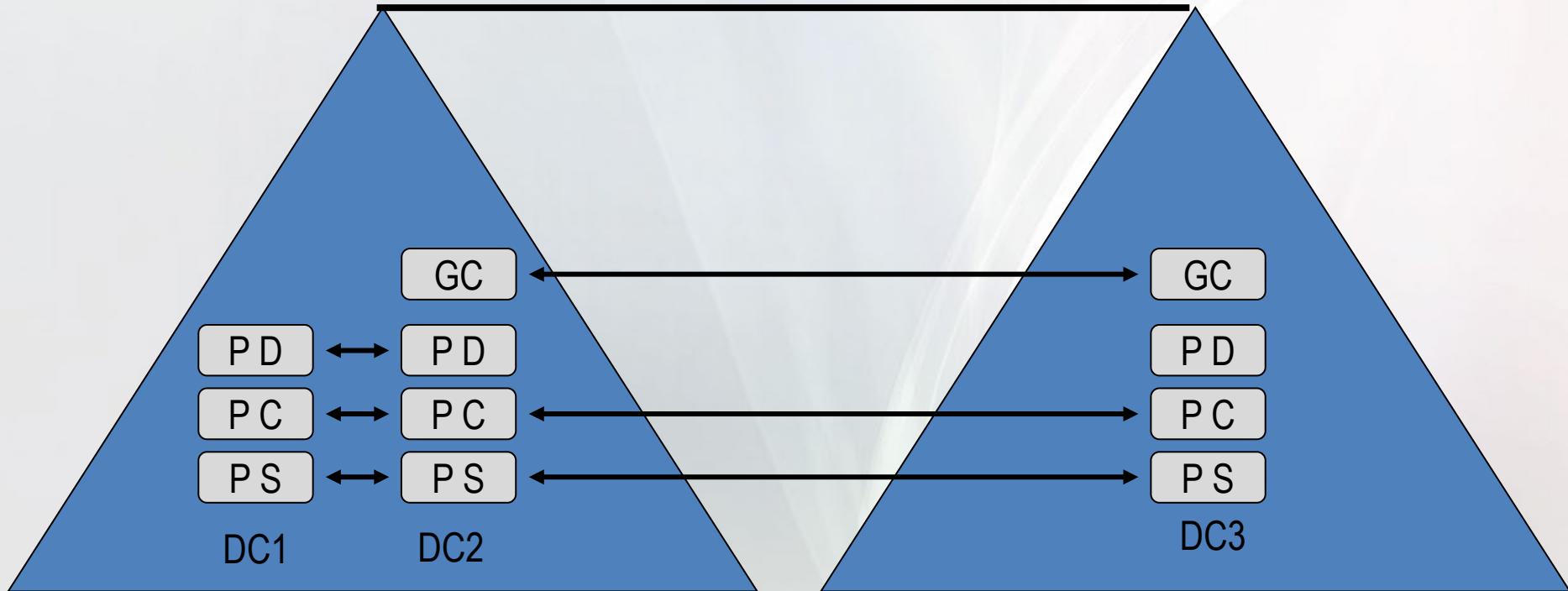
# Module 12

## La réPLICATION de l'Active Directory

# 1. Introduction (1)

- L'AD est une base de données multi-maître
- L'AD est divisé en 4 partitions :
  - de schéma
  - de configuration
  - de domaine
  - La partition d'application (stocke les données sur les applications utilisées dans Active Directory, comme par exemple, les zones intégrées à Active Directory d'un serveur DNS)
- Le GC est un réplique partiel d'objets de l'AD.

# 1. Introduction (2)

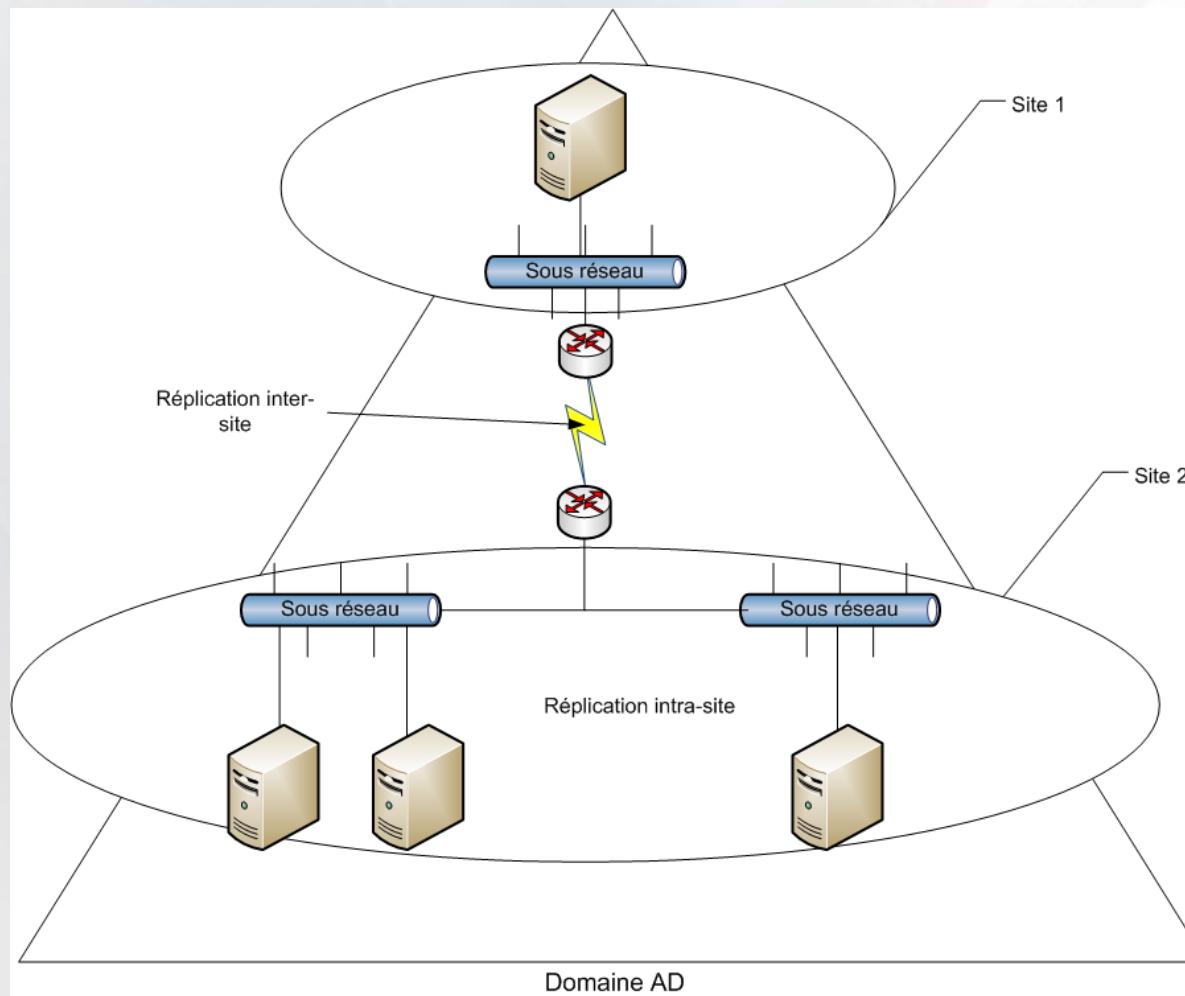


Pour la partition d'application, on choisit vers quels DC cette partition sera répliquée.

## 2. Protocoles de réPLICATION

- Inter-sites : RPC (Remote Procedure Call) sur IP ou SMTP.
- Intra-sites : RPC sur IP
- RéPLICATION par notification asynchrone ou synchrone.
- Intra-sites : réPLICATION rapide, uniforme et non compressée
- Inter-sites : réPLICATION lente, pt à pt et compressée

## 2.1. Types de réPLICATION



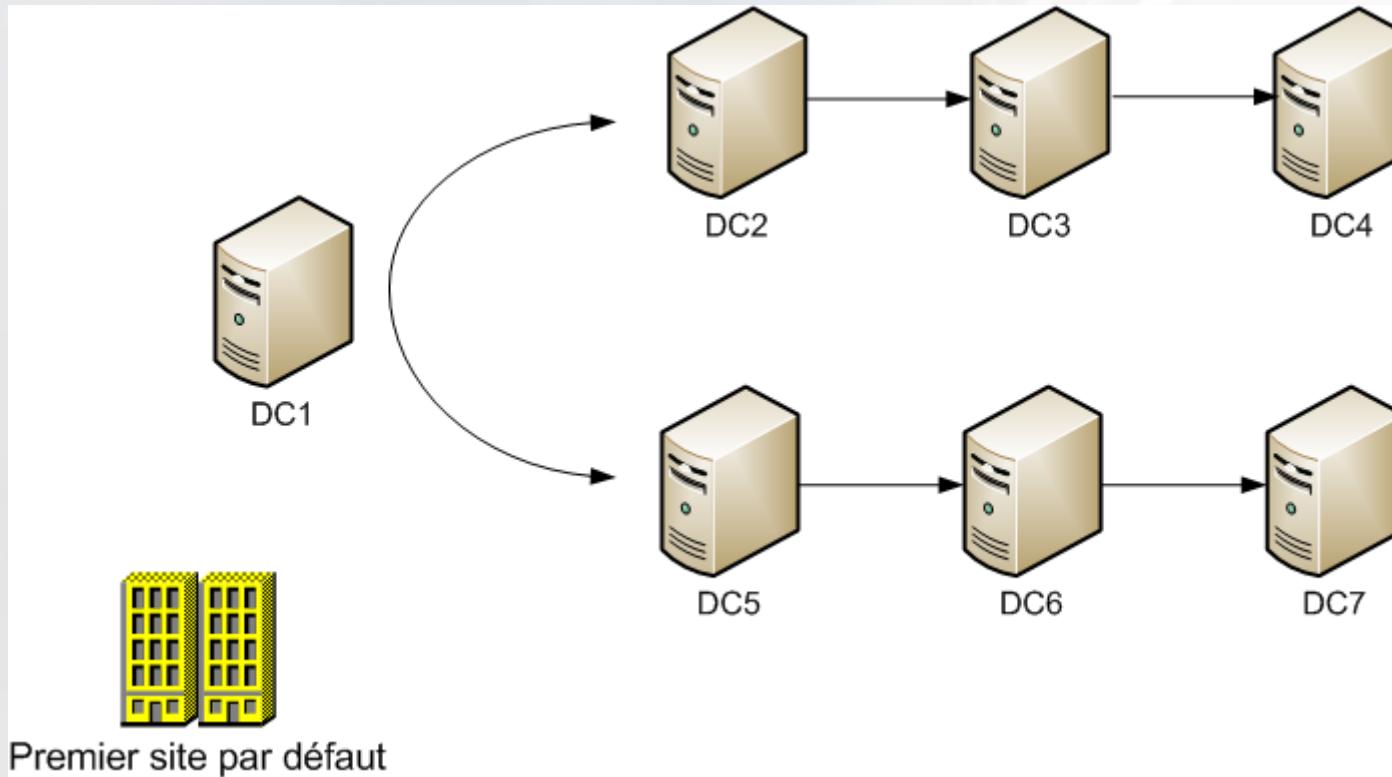
### 3. RéPLICATION INTRA-SITE

- RéPLICATION normale :
  - Lors d'une modif de l'AD, réPLICATION après 5 min au premier partenaire de réPLICATION ensuite toutes les 30 s aux autres DC.
  - Si pas de modif, réPLICATION toutes les heures.
- RéPLICATION urgente :
  - Lors de la modif d'une stratégie de comptes (Pswd, LSA Local Security Authority).
  - N'attend pas les 5 min

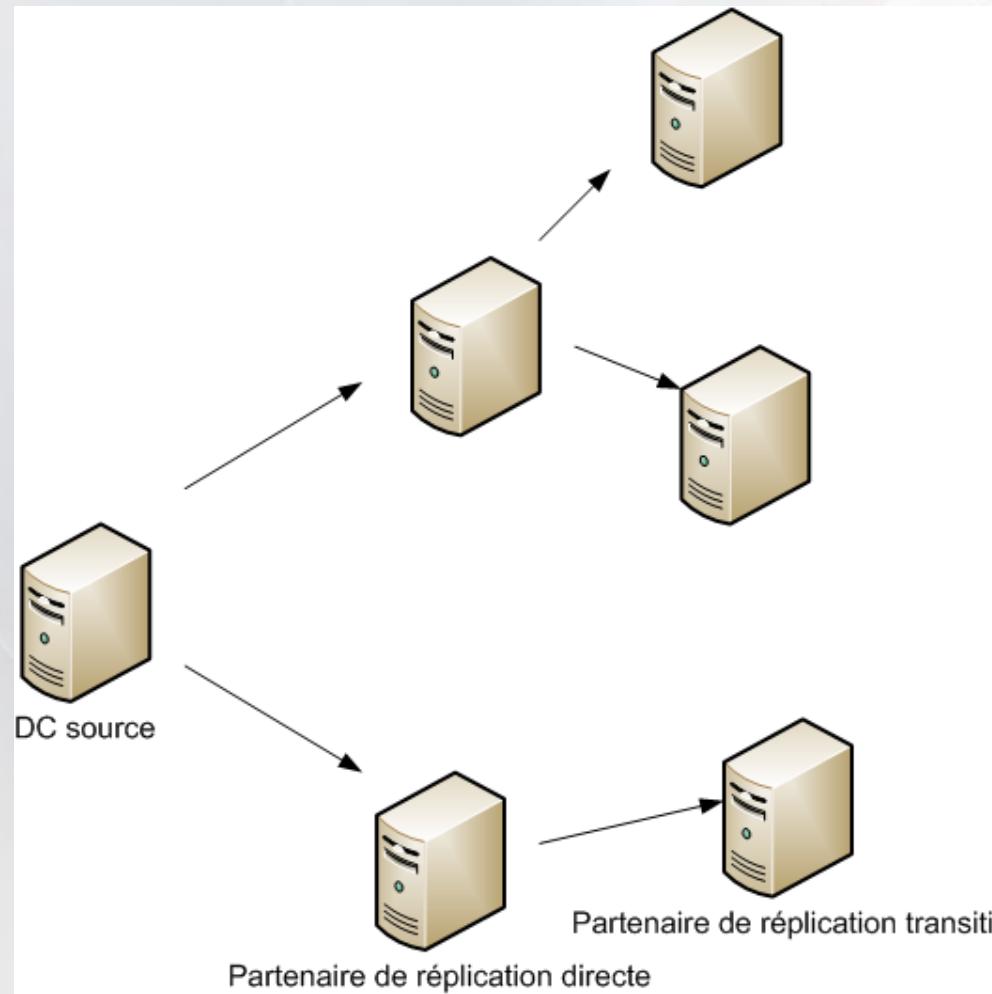
## 3.1. Vérificateur de cohérence (KCC)

- KCC : Knowledge Consistency Checker
- Toutes les 15 minutes
- Intra-site : gestion de la réPLICATION automatique.
- CrÉATION de boucle de rÉPLICATION :
  - Objet serveur
  - Objet NTDS settings
  - Objet connexion
- RéPLICATION de tous les DC en un max de 3 sauts
- Partenaires de réPLICATION directs et transitifs

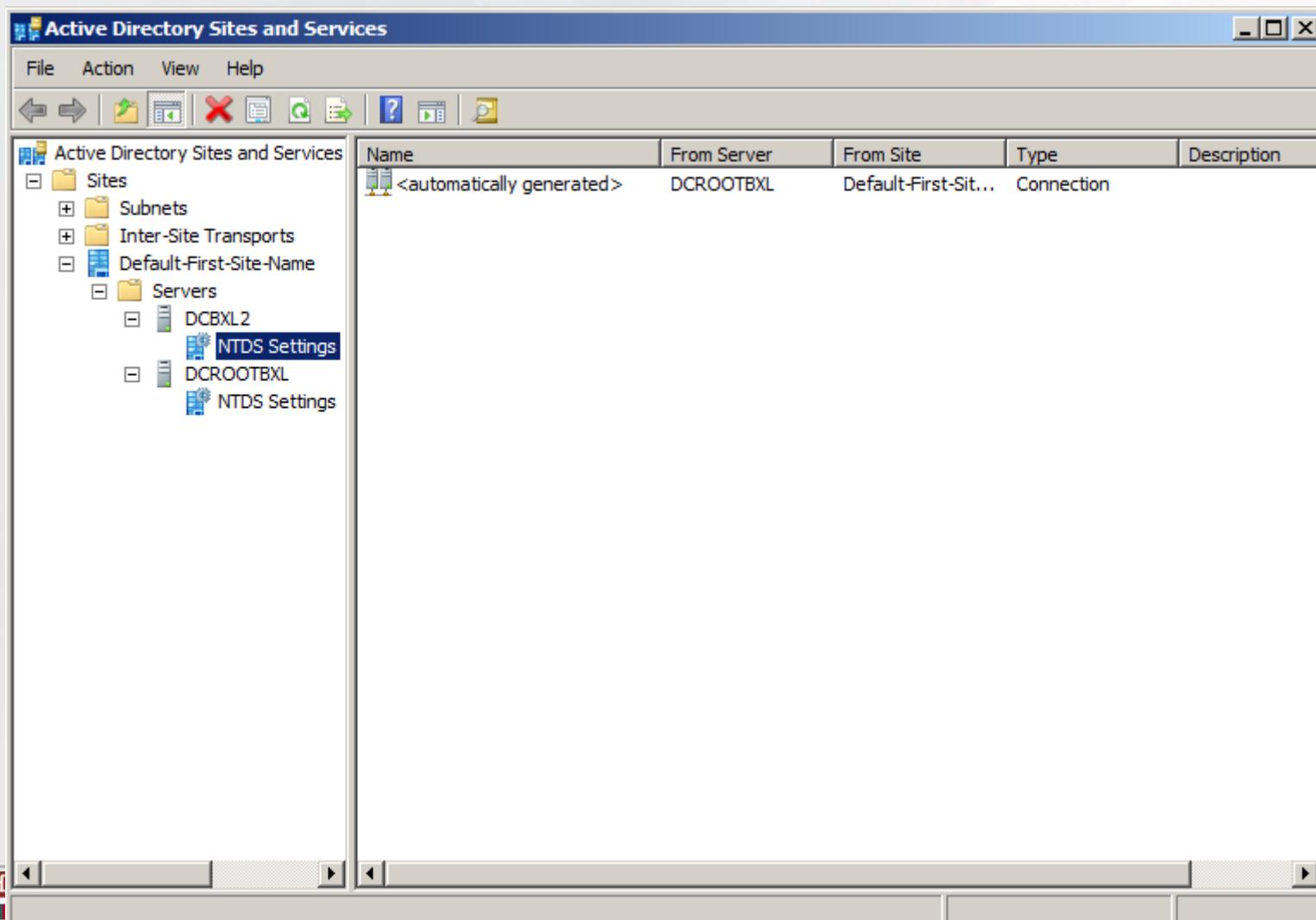
## 3.1. Vérificateur de cohérence (KCC)



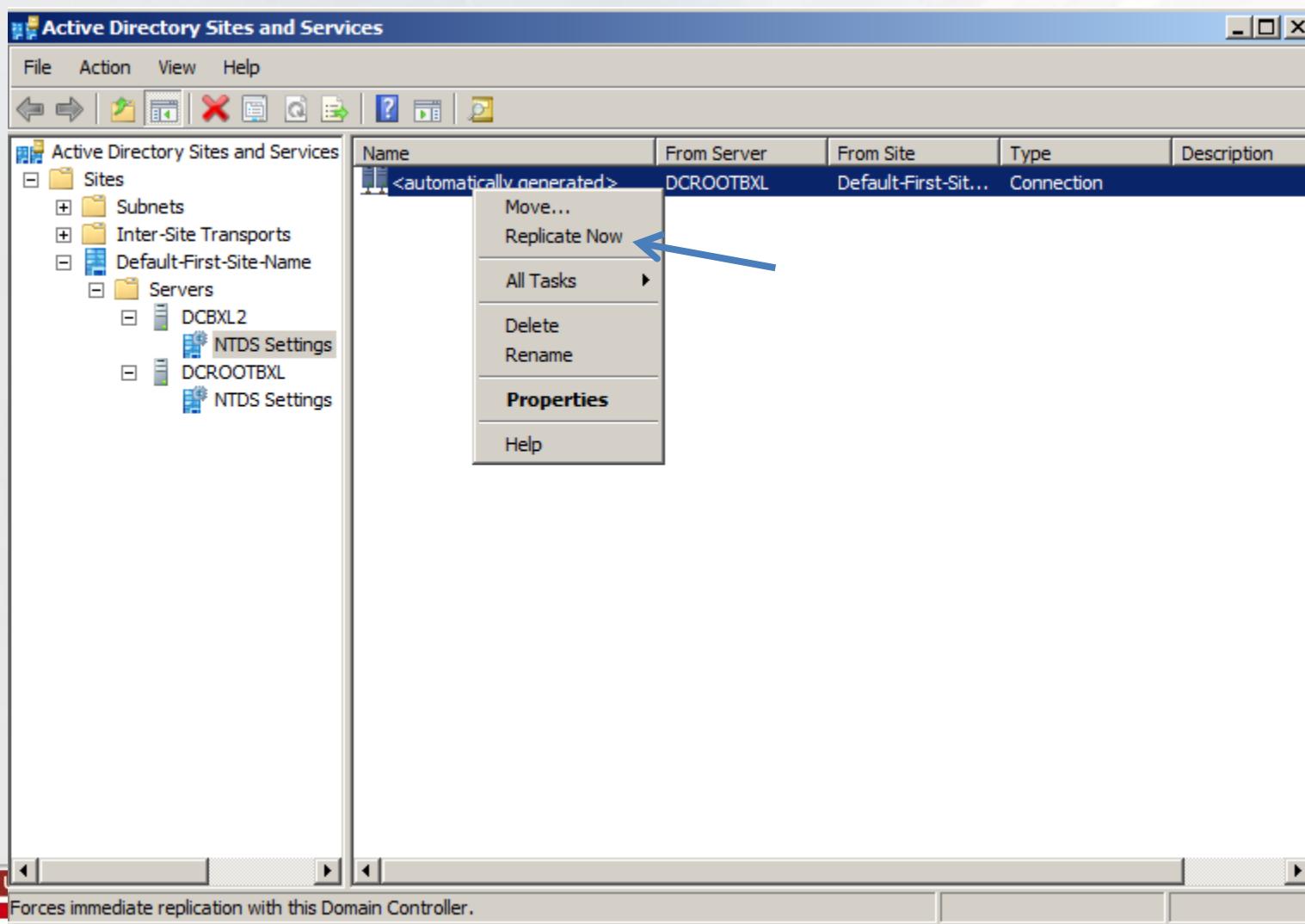
## 3.2. Convergence



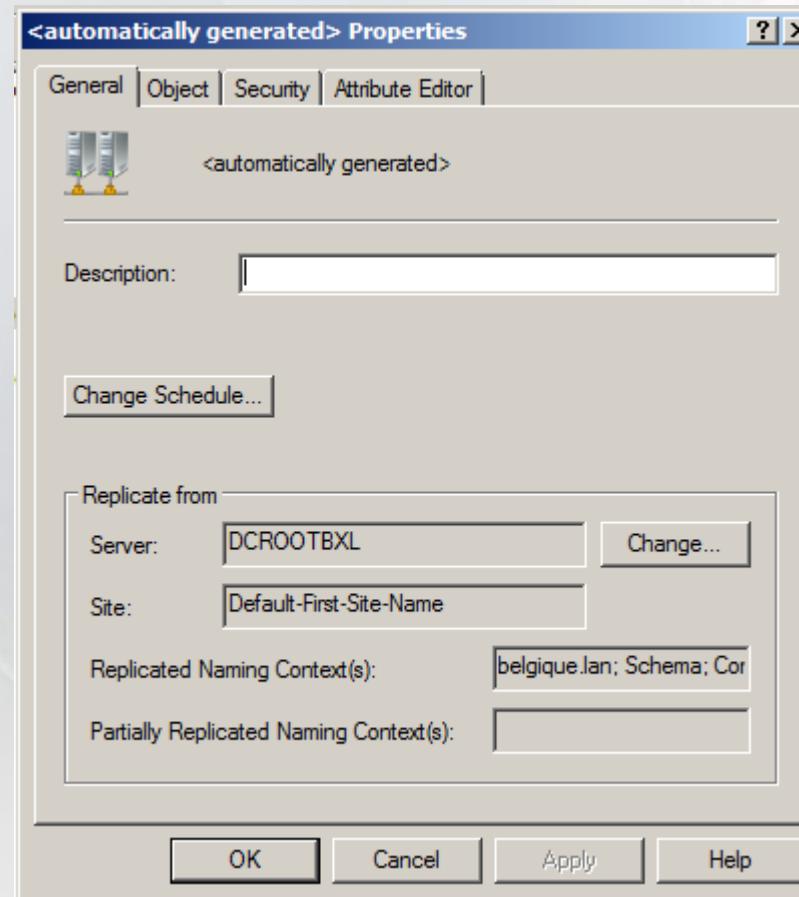
## 3.2. Sites et services AD



## 3.3. RéPLICATION manuelle

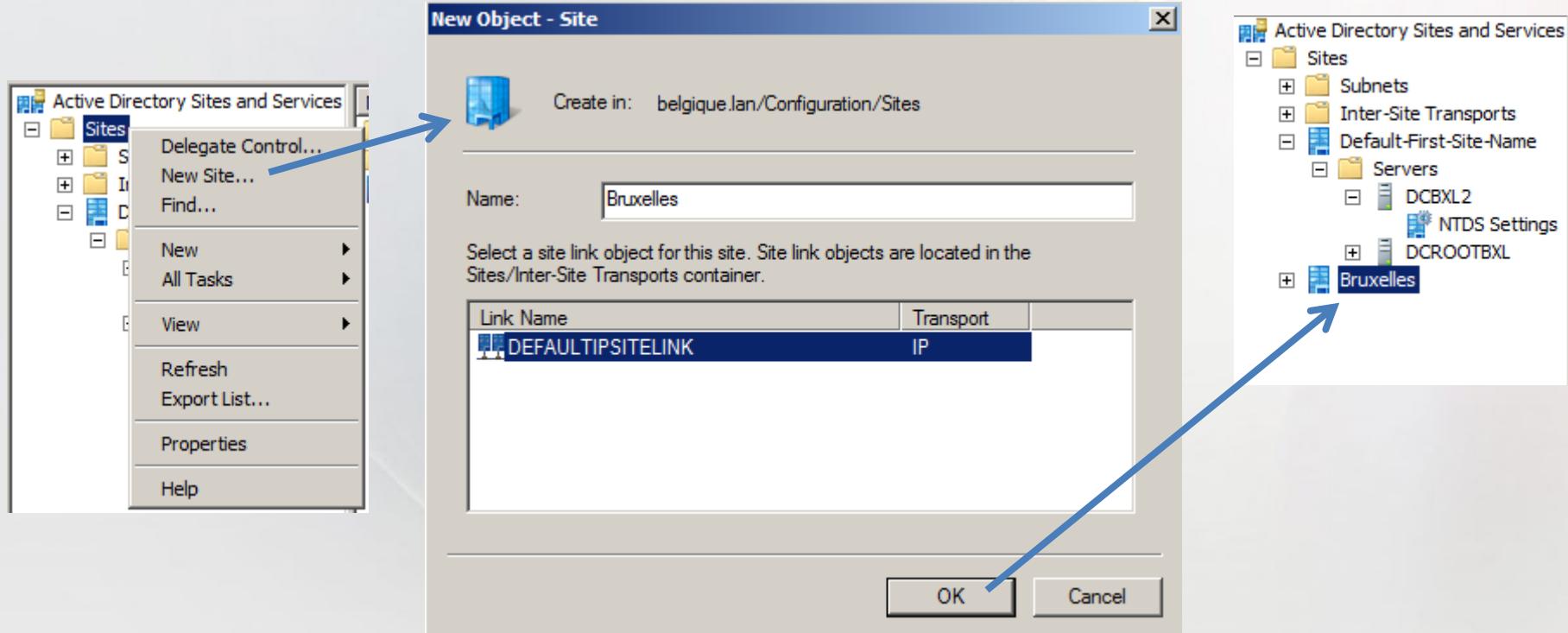


## 3.4. Propriétés Intra-site



## 3.5. Crédation d'un site

### AD Sites & Services



## 3.6. Ajouter des sous-réseaux à un site

The screenshot shows the Windows Server Management Console for Active Directory Sites and Services. On the left, the navigation pane shows the tree structure: Active Directory Sites and Services > Sites > Subnets. A context menu is open over the 'Subnets' folder, with 'New Subnet...' highlighted. A blue arrow points from this menu item to the 'New Object - Subnet' dialog box.

**New Object - Subnet**

Create in: belgique.lan/Configuration/Sites/Subnets

Enter the address prefix using network prefix notation (address/prefix length), where the prefix length indicates the number of fixed bits. You can enter either an IPv4 or an IPv6 subnet prefix.  
[Learn more about entering address prefixes.](#)

IPv4 example: 157.54.208.0/20

IPv6 example: 3FFE:FFFF:0:C000::/64

Prefix::

Prefix name in Active Directory Domain Services:

Select a site object for this prefix.

Site Name

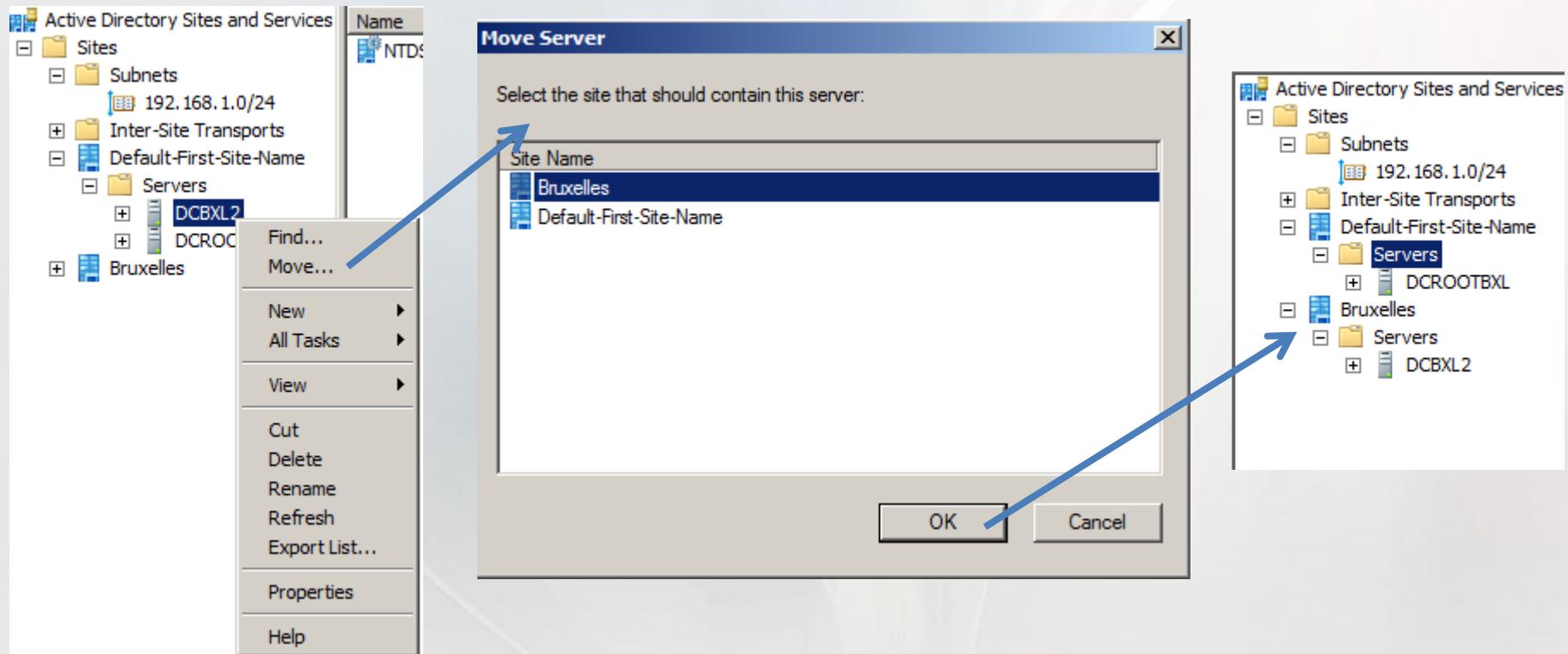
- Bruxelles
- Default-First-Site-Name

OK Cancel Help

A second blue arrow points from the 'Bruxelles' checkbox in the Site Name list to the right-hand navigation pane, which displays the full structure of the Active Directory Sites and Services tree, including the newly created '192.168.1.0/24' subnet under the 'Subnets' folder.

New DC directement  
Ajouté au bon  
sous-réseau

## 3.7. déplacer les DC



## 4. RéPLICATION EN LIGNE DE COMMANDE (1)

- En Windows 2000, les seules possibilités pour forcer la réPLICATION sont d'utiliser :
  - La console « Sites et services AD »
  - Replication Monitor
- A partir de Windows 2003, il existe une commande : Repadmin (support tools)
- A partir de Windows 2008 : Repadmin est une commande système

## 4. RéPLICATION EN LIGNE DE COMMANDE (2)

- Syntaxe :

*Repadmin /syncall DC [Naming Context] [Flags]*

DC : Le DC a répliquer avec tous les autres

Naming Context : DN de la partition à répliquer

Flags : d'autres utilitaires

ex : /A

/e

Exemple : repadmin /syncall dc1.isims.be

## 5. RéPLICATION Inter-site

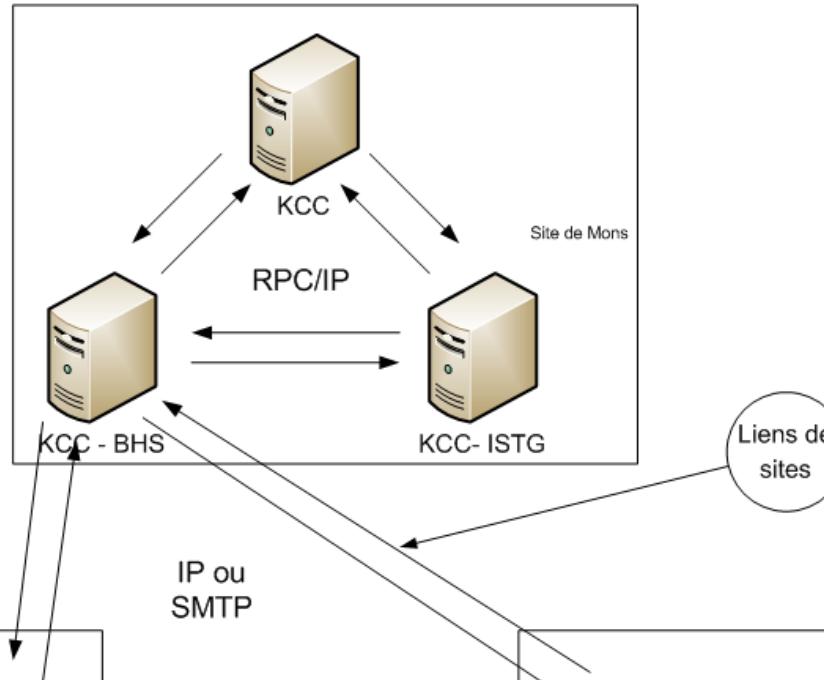
- Site relié par une connexion lente
- RéPLICATION compressée de 80%
- Horaire de réPLICATION
- Authentification sur DC du même site
- Par défaut réPLICATION toutes les 180 minutes
- ISTG : Inter Site Topology Generator
- A chaque lien est associé un coût
- Chemin emprunté = Chemin ayant coût le plus bas

## 5. RéPLICATION Inter-site

- Protocole IP (RPC/IP) ou SMTP
- Attention SMTP n'est pas disponible pour des DC d'un même domaine
- Si BP > 1024 kbps on utilise RPC over IP
- Pas de notification
- Pas de réPLICATION urgente

## 5. RéPLICATION Inter-site

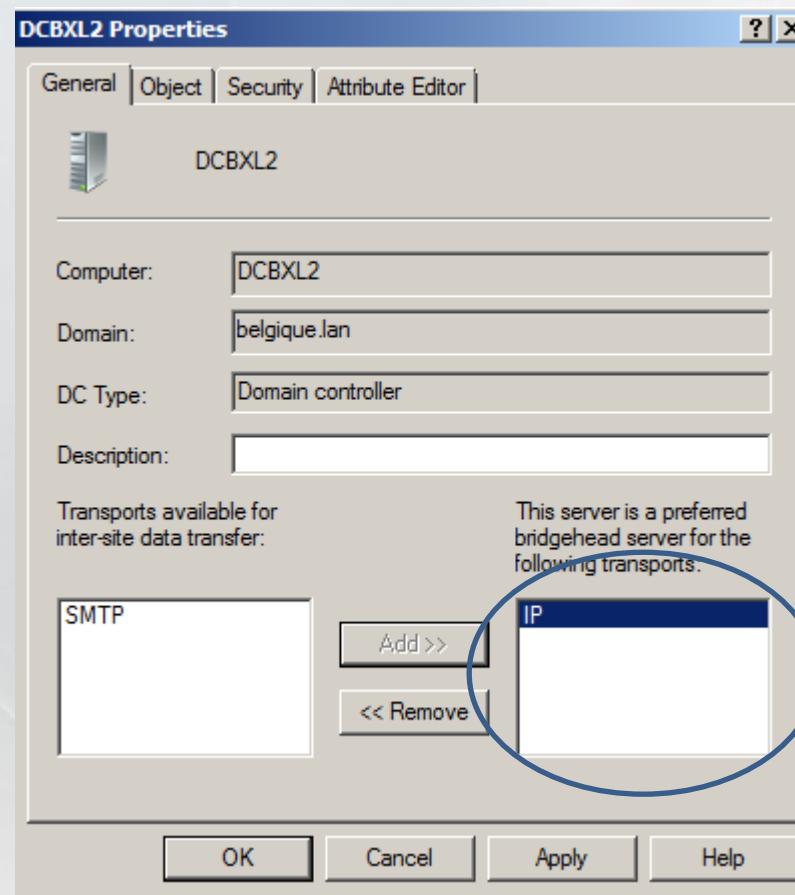
BHS : Bridgehead server  
(Serveur tête de pont)



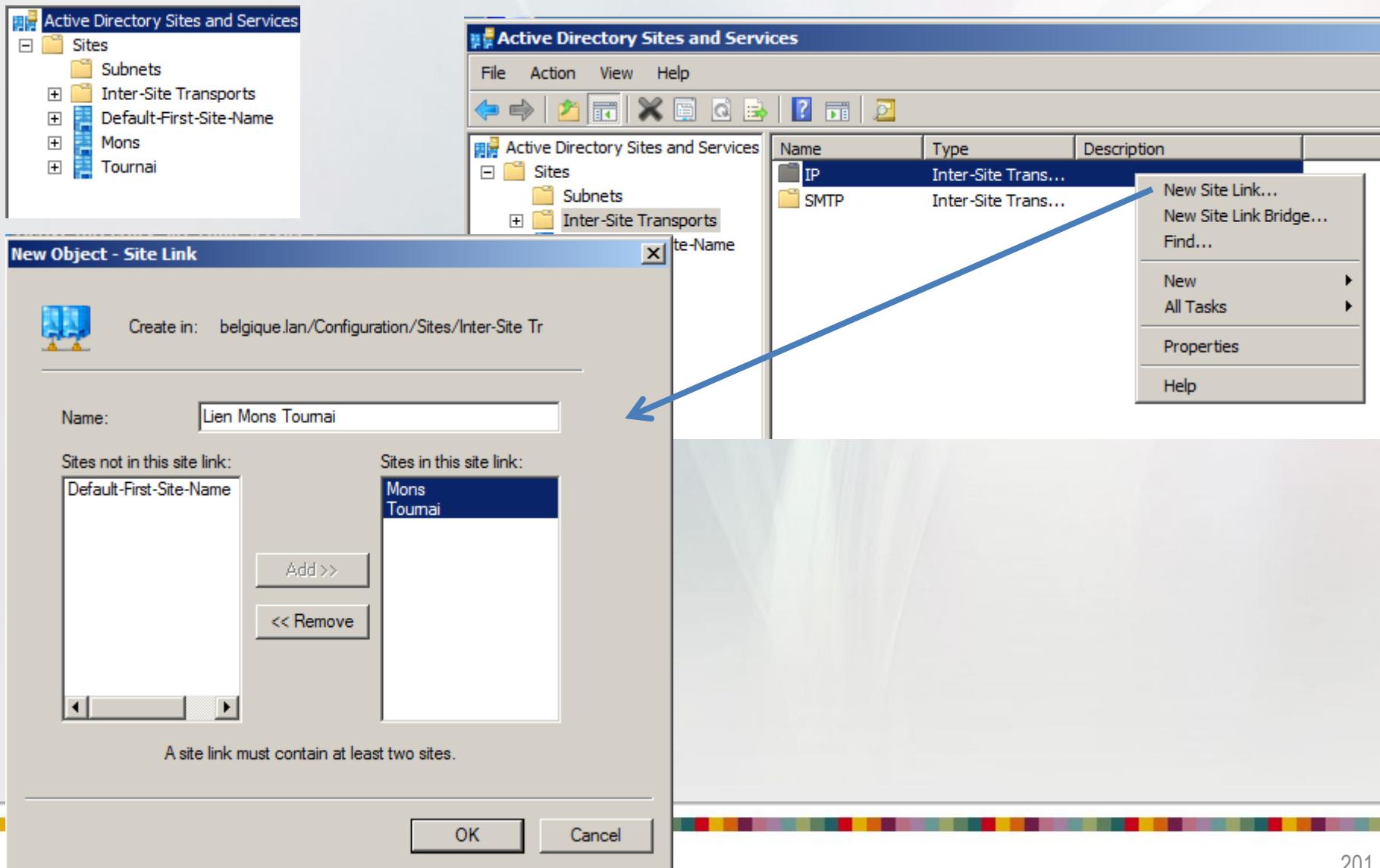
## 5. RéPLICATION Inter-site

- ISTG désigne les serveurs têtes de ponts
- Si plus d'un DC est éligible → ISTG désigne le DC avec le GUID le plus bas
- Possibilité de choisir les serveurs têtes de ponts
  - Dans ce cas l'ISTG ne désignera plus automatiquement
  - Si STP tombe en panne et si il n'y a pas un autre STP choisi → Plus de réPLICATION

## 5. RéPLICATION Inter-site



## 5.1. Crédation d'un lien de site



## 5.2. Configuration du lien

The screenshot shows the 'Active Directory Sites and Services' management console. In the center, a list of site links is displayed. The 'Lien Mons Tournai' entry has a context menu open over it, with the 'Properties' option highlighted. A blue arrow points from this 'Properties' option to the corresponding button in the 'Lien Mons Tournai Properties' dialog box.

**Lien Mons Tournai Properties**

- General Object Security Attribute Editor

**Lien Mons Toumai**

Description:

Sites not in this site link: Default-First-Site-Name

Sites in this site link: Mons Toumai

Cost: 100

Replicate every 180 minutes

**Schedule for Lien Mons Tournai**

0 · 2 · 4 · 6 · 8 · 10 · 12 · 14 · 16 · 18 · 20 · 22 · 0

All	lundi	mardi	mercredi	jeudi	vendredi	samedi	dimanche

OK Cancel Change Schedule... Apply Help

Replication Not Available   
Replication Available

lundi through vendredi from 07:00 to 19:00

## 6. Gestion des conflits

- Gestion des conflits lors de maj simultanée provenant de 2 répliques maîtres distinct.
- Cachet unique global :

N° de version	Dateur	Identificateur universel unique
---------------	--------	---------------------------------

- N° de version incrémentée à chaque modification
- Dateur : date et heure du début de la mise à jour
- L'identificateur unique universel : identifie le DC (GUID) sur lequel a eu lieu la modification

## 6. Gestion des conflits

- 3 Types de conflits (avant réPLICATION)
  - Conflit d'attributs
    - RéPLICATION uniquement des attributs modifiés et pas de l'objet complet
    - Même attribut changé sur 2 DC
    - Attribut avec le numéro de version le plus élevé sera pris
    - Si même numéro de version -> Horodatage (+ récent)
  - Conflit de conteneurs supprimés
    - UO supprimée sur un DC et ajout d'un objet dans cette UO sur un autre DC
    - Objet placé dans le conteneur « LostAndFound »
  - Conflit de noms uniques relatifs
    - Objet avec cachet le plus élevé garde le nom
    - Autre objet est renommé

## 6. Gestion des conflits

- Blocage de la propagation des réplications superflues
- Utilisation de l'USN (update sequence number)
  - Comparaison des USN
  - Envoi des mјj si ces USN sont supérieurs à son partenaire de réPLICATION

## 6. Gestion des conflits

- Modification d'un objet → Numéro de version est incrémenté (USN)
- Visualisation des USN : Repadmin/showmeta

```
C:\>repadmin /showmeta "ou=secrétaire,dc=zan,dc=be"
7 entries.

Loc. USN Originating DSA Org.USN Org.Time/Date Ver Attribute
===== ====== ====== ====== ====== ====== ====== =====
 16788 Premier-Site-par-defaut\SERVER 16788 2004-09-06 10:10.31 1 objectClass
 16788 Premier-Site-par-defaut\SERVER 16788 2004-09-06 10:10.31 1 ou
 16788 Premier-Site-par-defaut\SERVER 16788 2004-09-06 10:10.31 1 instanceType
 16788 Premier-Site-par-defaut\SERVER 16788 2004-09-06 10:10.31 1 whenCreated
 16788 Premier-Site-par-defaut\SERVER 16788 2004-09-06 10:10.31 1 nTSecurityDescriptor
 16788 Premier-Site-par-defaut\SERVER 16788 2004-09-06 10:10.31 1 name
 16788 Premier-Site-par-defaut\SERVER 16788 2004-09-06 10:10.31 1 objectCategory

C:\>
```

```
C:\>repadmin /showmeta "ou=secrétaire,dc=zan,dc=be"
7 entries.

Loc. USN Originating DSA Org.USN Org.Time/Date Ver Attribute
===== ====== ====== ====== ====== ====== ====== =====
 16788 Premier-Site-par-defaut\SERVER 16788 2004-09-06 10:10.31 1 objectClass
 16797 Premier-Site-par-defaut\SERVER 16797 2004-09-06 10:23.09 2 ou
 16788 Premier-Site-par-defaut\SERVER 16788 2004-09-06 10:10.31 1 instanceType
 16788 Premier-Site-par-defaut\SERVER 16788 2004-09-06 10:10.31 1 whenCreated
 16788 Premier-Site-par-defaut\SERVER 16788 2004-09-06 10:10.31 1 nTSecurityDescriptor
 16797 Premier-Site-par-defaut\SERVER 16797 2004-09-06 10:23.09 2 name
 16788 Premier-Site-par-defaut\SERVER 16788 2004-09-06 10:10.31 1 objectCategory

C:\>
```

# Module 13

## Le serveur de fichiers

# 1. Introduction

- 3 systèmes de fichiers supportés
  - FAT
  - exFAT (Disques amovibles)
  - NTFS
- Pourquoi utiliser NTFS (New Technology File System)
  - Permissions
  - Compression
  - Chiffrage EFS
  - Quotas
  - ...

## 2. Disques de base

- Disques de base : structure disque
  - Partition principale
  - Partition étendue
- Sur un disque de base on peut avoir soit :
  - 4 pp
  - 3 pp et 1 pe
- PP : Impossible de créer des lecteurs logiques.
- PE : Autant de lecteurs logiques que de lettres disponibles

## 3. disques dynamiques (1)

- Disques dynamiques : ne possèdent pas de partition mais des volumes.
- Volume : Portion de disque fonctionnant comme un disque seul.
- Avantages des disques dynamiques :
  - Utilisation de la tolérance de pannes sans redémarrer
  - Pas de limitation dans le nombre de volume
  - Possibilité d'étendre des volumes NTFS

## 3. disques dynamiques (2)

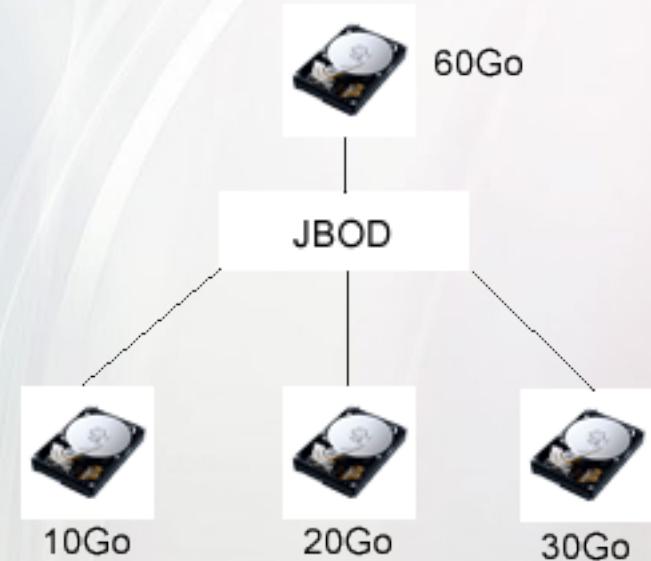
- Sur un disque dynamique, il est possible de créer 3 types de volumes :
  - Simple : espace situé sur un seul disque, pas de limite de taille ni de nombre.
  - Fractionné : regroupement d'espaces libres situés sur min 2 max 32 disques. Les données sont d'abord écrite sur le 1er puis lorsqu'il est plein écriture sur le second, ...
  - Agrégé par bandes : regroupement sur un seul volume d'espaces libres situés sur min 2 max 32 disques. Ecriture par bande de 64Ko. 64Ko sur le 1er puis 64Ko sur le second, ...

## 4. RAID

- RAID : Redundant Array of inexpensive Disks (Ensemble redondant de disques indépendants)
- But :
  - Augmenter la tolérance aux pannes
  - Augmenter la sécurité
  - Augmenter la capacité de stockage
  - Augmenter la vitesse d'écriture
- 1987 : niveau 1 à 5
- ajout des niveaux 6 et 7
- Niveau JBOD et Raid 0 pas réellement du raid car pas de redondance.
- 0 : Striping
- 1 : Mirroring
- 2 : Striping with parity
- 3 : Disk array with bit-interleaved data
- 4 : Disk array with block-interleaved data
- 5 : Disk array with block-interleaved parity
- 6 : Disk array with block-interleaved parity
- 7 : Disk array with block-interleaved parity

## 4.1. JBOD

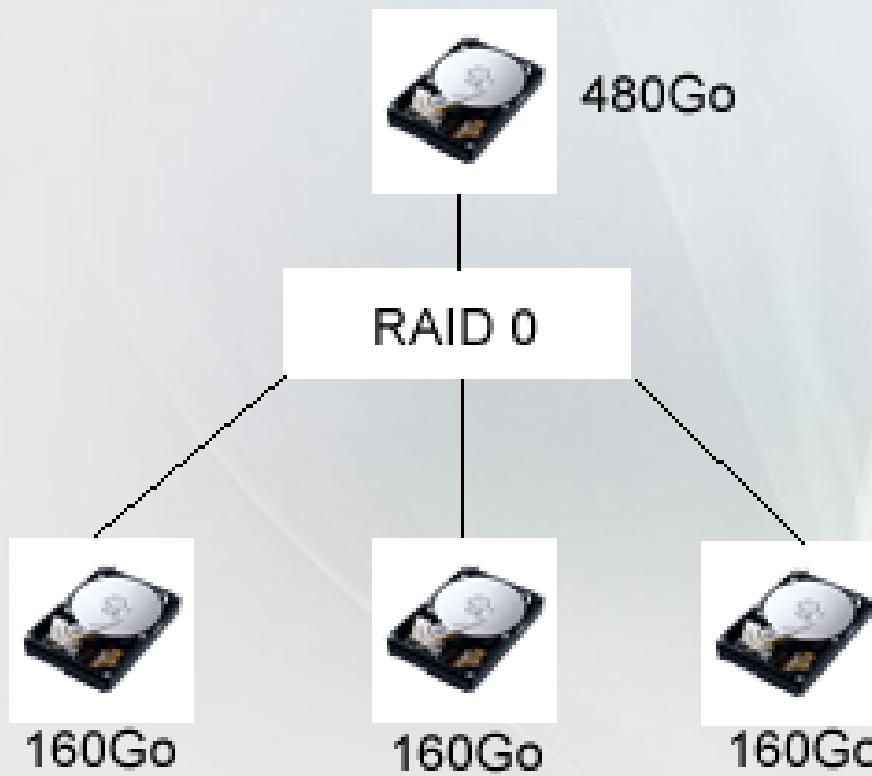
- Just a Bunch Of Disk ou Raid linéaire
- Def. : Regrouper plusieurs HD de capacité différentes sur une seule unité logique
- Ecriture disque par disque



## 4.2. RAID 0 (0)

- Ecriture des données sur plusieurs HD
- Minimum 2 HD
- Toujours utiliser des HD de capacité et de performance identique.
- Exemple :
  - 3 HD de 160Go
  - Débit en lecture de 100 Mo/s
  - Débit en écriture de 80Mo/s

## 4.2. RAID 0 (1)



En RAID 0 :

Capacité totale = 480 Go

Débit en R = 300 Mo/s

Débit en W = 240 Mo/s

## 4.2. RAID 0 (2)

- Calculer la capacité totale ainsi que les débits en R/W de cet exemple :

	HD1	HD2	HD3	HD4
Capacité (Go)	300	18	20	45
Débit en R (Mo/s)	90	160	20	35
Débit en W (Mo/s)	82	125	20	15

**Total en raid 0 :**

Capacité = 72 Go; Débit en R = 80 Mo/s; Débit en W = 60 Mo/s

## 4.2. RAID 0 (3)

- Pour stocker un fichier, la carte RAID 0 découpe le fichier en segments (Block size ou chunk block)
- Segment =  $x \cdot 512$  octets (capacité d'un secteur d'un HD)
- Stockage des fichiers volumineux : augmenter la taille des segments
- Stockage de petits fichiers : diminuer la taille des segments

## 4.2. RAID 0 (4)

- Exemple : 3 HD; segment = 3072 octets (6X512)
- Copie un fichier de 8ko

## 4.3. RAID 1 (1)

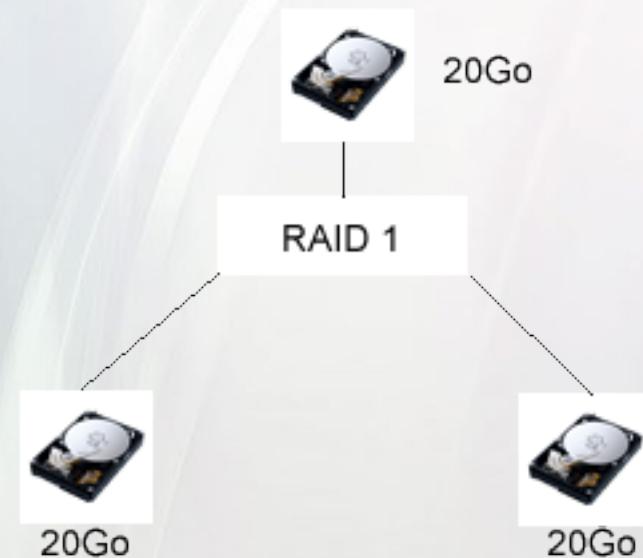
- Dupliquer les données sur plusieurs HD
  - Augmentation de la sécurité
  - Augmentation du débit en R (tous les HD lisent une partie des datas)
  - Pas d'amélioration du débit en W (Ecriture synchrone). Débit en W = débit d'un seul HD
- 2 types de raid1 :
  - Duplexing : Chaque HD à son propre contrôleur
  - Mirroring : Un seul contrôleur

## 4.3. RAID 1 (2)

RAID 1 Duplexing



RAID 1 Mirroring

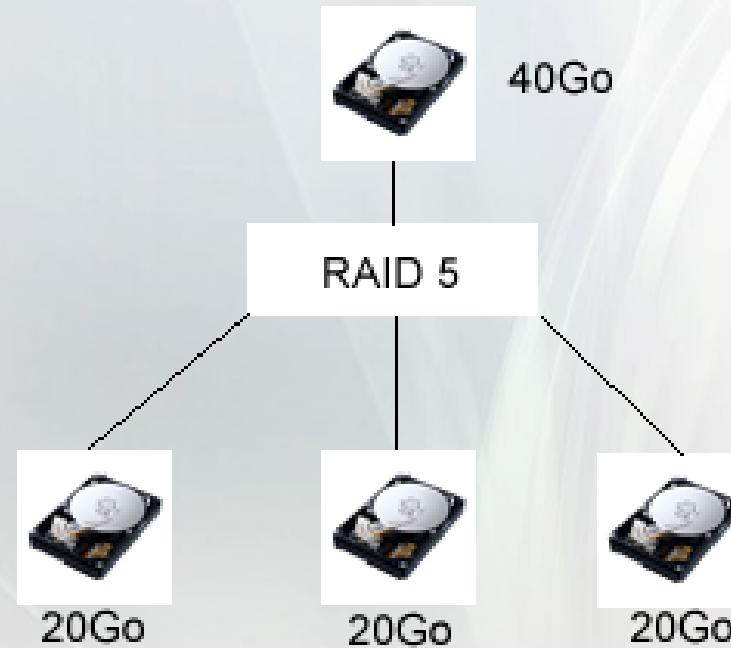


## 4.4. Raid 5 (1)

- Ecriture des données sur  $n-1$  HD, utilisation du  $n^e$  HD pour la parité
- Répartition de la parité sur l'ensemble des HD
- Avantages : augmentation des performances en R/W, les performances sont  $n-1 \times$  supérieure à un seul HD
- Comme en RAID 0 : Choix de la taille des segments

## 4.4. Raid 5 (2)

- Calcul de la capacité totale : taille du plus petit HD X nbr de HD -1



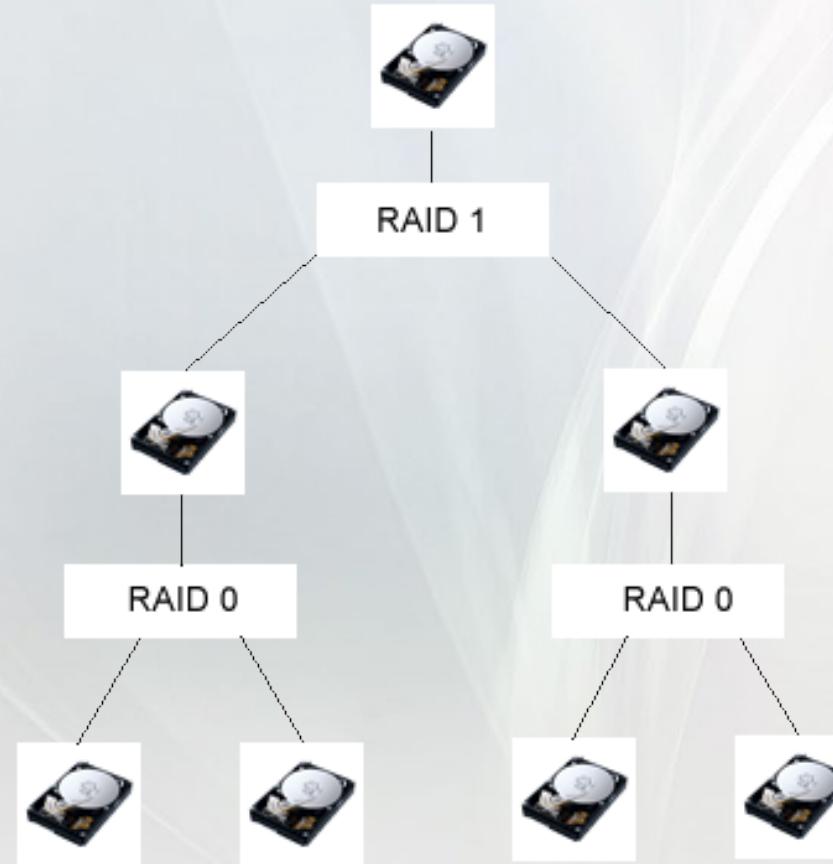
## 4.5. Raid 6 et 7

- Raid 6 : Raid 5 avec 2 HD pour la parité
- Raid 7 : On choisit le nombre de HD pour les données et pour la parité.

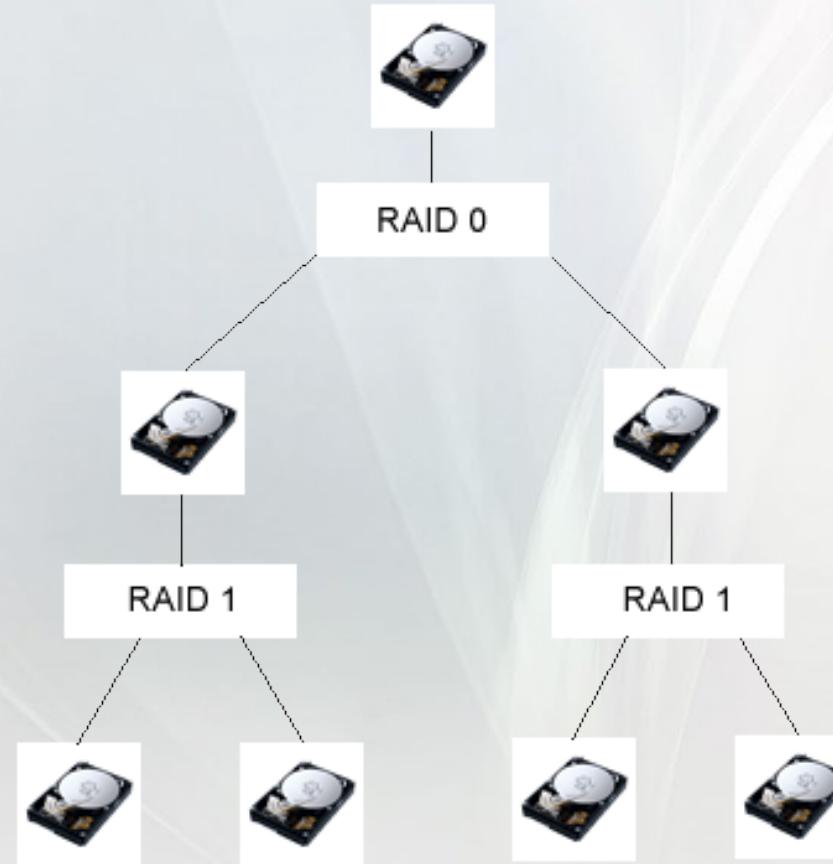
Exemple : 5 HD de data et 4 HD de parité

Tous les transferts se font de manière asynchrone => augmentation de 1,5 à 6 X des performances

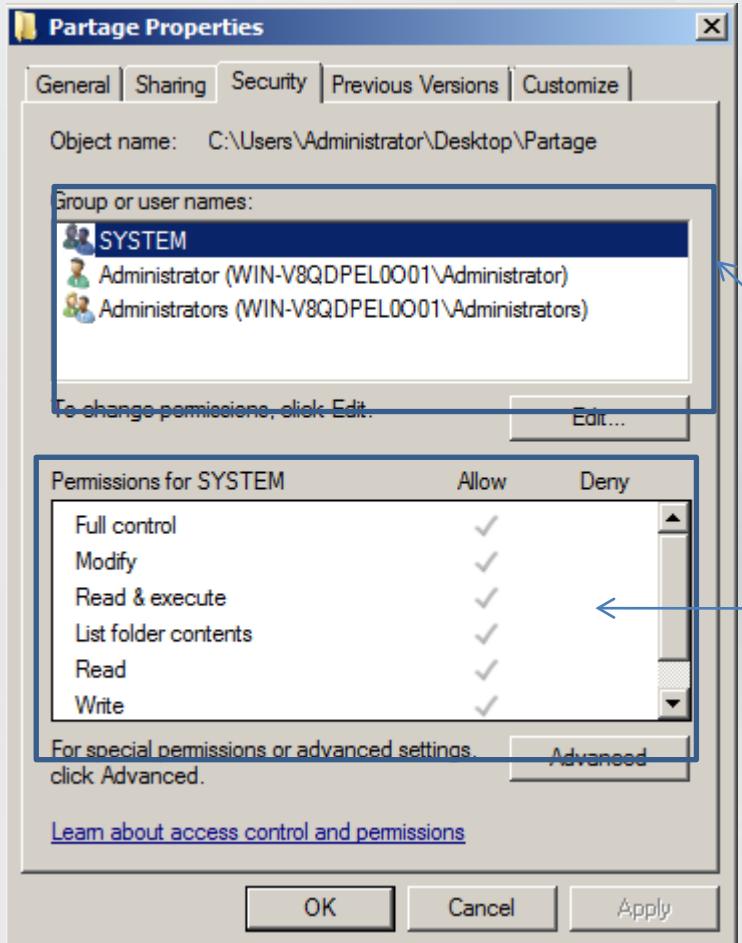
## 4.6. RAID 01



## 4.7. RAID 10



## 5. Les permissions NTFS



- NTFS : New Technology File System
- AAA : Authentification – Autorisation – NTFS – Audit

ACL : Access Control List

ACE de SYSTEM  
ACE : Access Control Entry

## 6. Types de permissions NTFS (1)

Autorisation NTFS	Description	Fichier	Dossier
<b>Lecture</b>	Permet l'affichage du contenu d'un dossier et permet d'ouvrir un dossier ou un fichier.	x	x
<b>Écriture</b>	Permet l'ajout ou la modification d'un fichier ou d'un dossier.	x	x
<b>Lecture et exécution</b>	Reprend l'autorisation de lecture d'affichage du routeur de dossier et permet en plus l'exécution des programmes dans des dossiers.	x	x
<b>Affichage du contenu du Dossier</b>	Reprend l'autorisation de lecture d'affichage du routeur de dossier et permet en plus l'exécution des programmes dans des dossiers.		x
<b>Modification</b>	Reprend l'autorisation de lecture d'écriture de lecture et exécution et d'affichage du contenu d'un dossier et permet en plus la suppression.	x	x
<b>Contrôle total</b>	Reprend l'autorisation de modification et permet en plus l'appropriation la modification des autorisations et la suppression des sous-dossiers ou fichiers.	x	x

## 6. Types de permissions NTFS (2)

	Lecture	Écriture	Affichage du contenu du dossier	Lecture et exécution	Modifier	Contrôle total
Lecture	X					
Écriture		X				
Affichage du contenu du dossier	X		X			
Lecture et exécution	X			X		
Modifier	X	X	X	X	X	
Contrôle total	X	X	X	X	X	X

## 7. Les permissions avancées

- Propriétés du dossier – Sécurité – Avancé
- Il existe 14 permissions avancées

Advanced permissions:

[Show basic permissions](#)

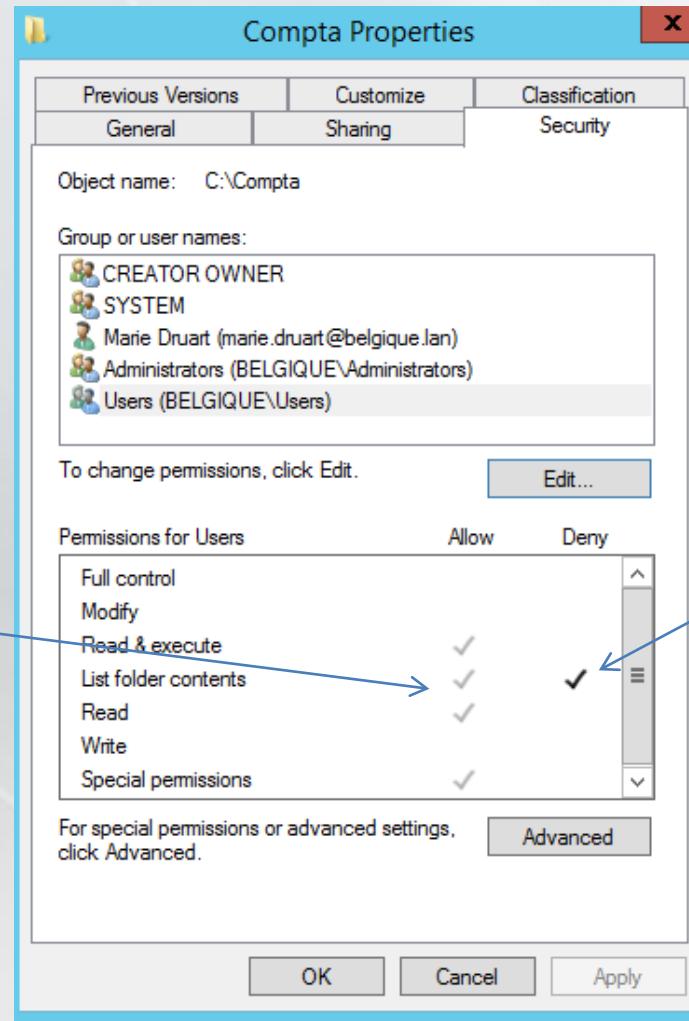
<input type="checkbox"/> Full control	<input type="checkbox"/> Write attributes
<input checked="" type="checkbox"/> Traverse folder / execute file	<input type="checkbox"/> Write extended attributes
<input checked="" type="checkbox"/> List folder / read data	<input type="checkbox"/> Delete subfolders and files
<input checked="" type="checkbox"/> Read attributes	<input type="checkbox"/> Delete
<input checked="" type="checkbox"/> Read extended attributes	<input checked="" type="checkbox"/> Read permissions
<input type="checkbox"/> Create files / write data	<input type="checkbox"/> Change permissions
<input type="checkbox"/> Create folders / append data	<input type="checkbox"/> Take ownership

Only apply these permissions to objects and/or containers within this container

## 8. L'héritage

- Héritage dû au système de fichiers arborescent
- Autorisation affectée à un niveau est automatiquement affectée à ses enfants
- Permissions héritées (grisée)
- Permissions explicites
- Permission héritée s'annule devant une permission explicite

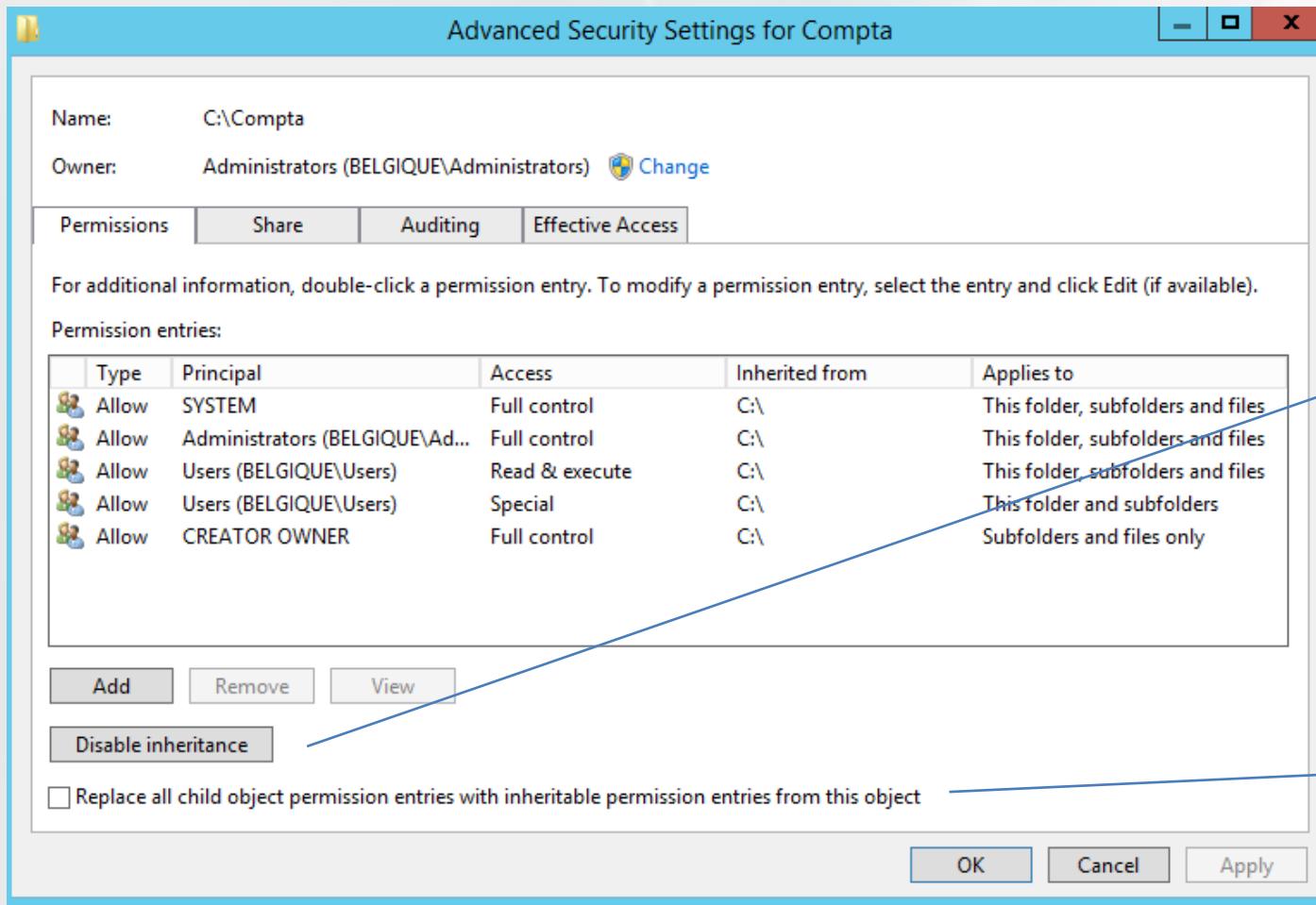
## 8. L'héritage



Autorisation héritées

Autorisation explicites

## 8. L'héritage - blocage



Indique si on conserve  
l'héritage ou non

Permet de propager les  
Autorisations de cet  
objet sur les objets  
enfants

## 9. Autorisations effectives (1)

- Un refus d'autorisation est prioritaire sur une autorisation accordée
- Une autorisation explicite est prioritaire sur une autorisation héritée
- Lorsqu'il existe des autorisations de même type, elles se combinent en effectuant une union

## 9. Autorisations effectives (2)

1. Afficher les groupes et les utilisateurs qui reçoivent une autorisation pour la ressource
2. Déterminer de quels groupes l'utilisateur est membre. Noter les autorisations de l'utilisateurs en divisant les permissions effectives et héritées
3. Noter les autorisations affectées directement à l'utilisateur
4. En utilisant les étapes 2 et 3, Trouver la résultante des autorisations héritées
  - a) Résultante des autorisations
  - b) Résultante des refus
  - c) Résultante totale
5. En utilisant les étapes 2 et 3, Trouver la résultante des autorisations explicites
  - a) Résultante des autorisations
  - b) Résultante des refus
  - c) Résultante totale
6. Déterminer la résultante des autorisations NTFS

## 9. Autorisations effectives (3)

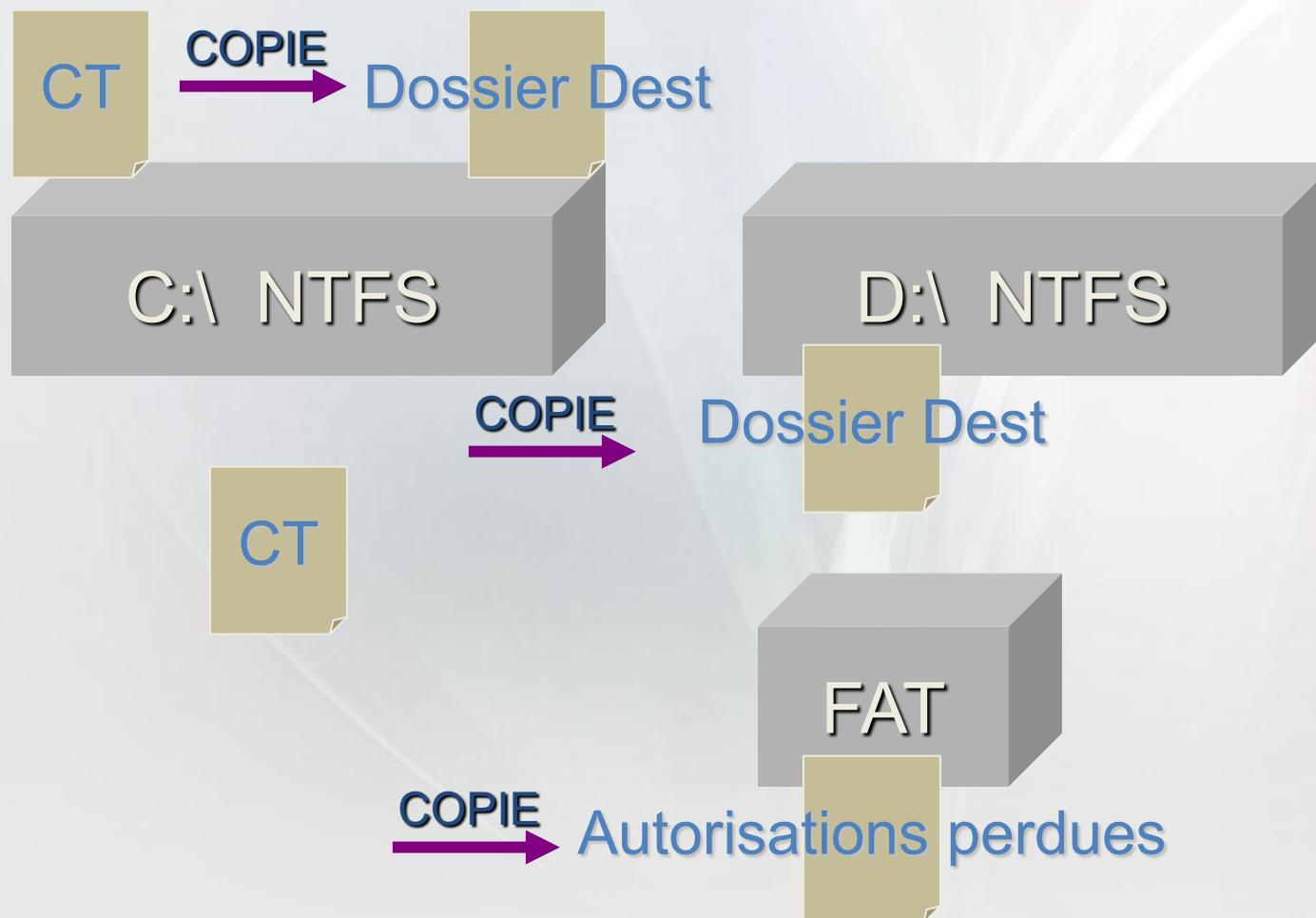
- Exemple :
- User1 membres des groupes GR1, GR2, GR3, GR4

Groupe	Permissions explicites	Permissions héritées
GR1	Lecture et exe	
GR2	Ecriture	
GR3		Modification
GR4		Refus Ecriture
Administrators		Contrôle total

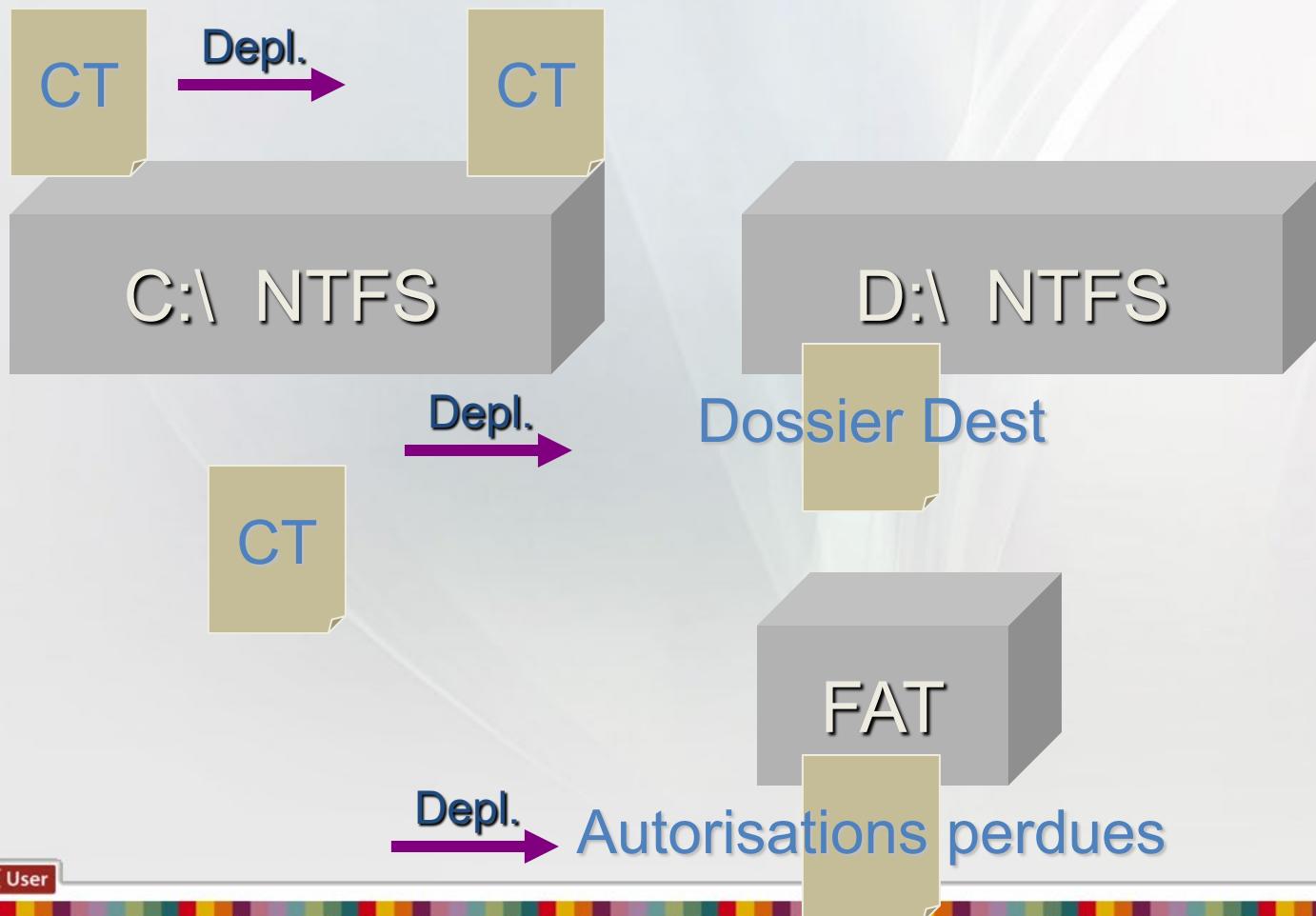
## 9. Autorisations effectives (4)

	Lecture	Ecriture	Affichage du contenu du dossier	Lecture et exécution	Modifier	Contrôle total
Lecture	X					
Ecriture		X				
Affichage	X		X			
Lecture et exe	X			X		
Modifier	X	X	X	X	X	
Contrôle total	X	X	X	X	X	X

## 10. Copier des fichiers



# 11. Déplacer des fichiers

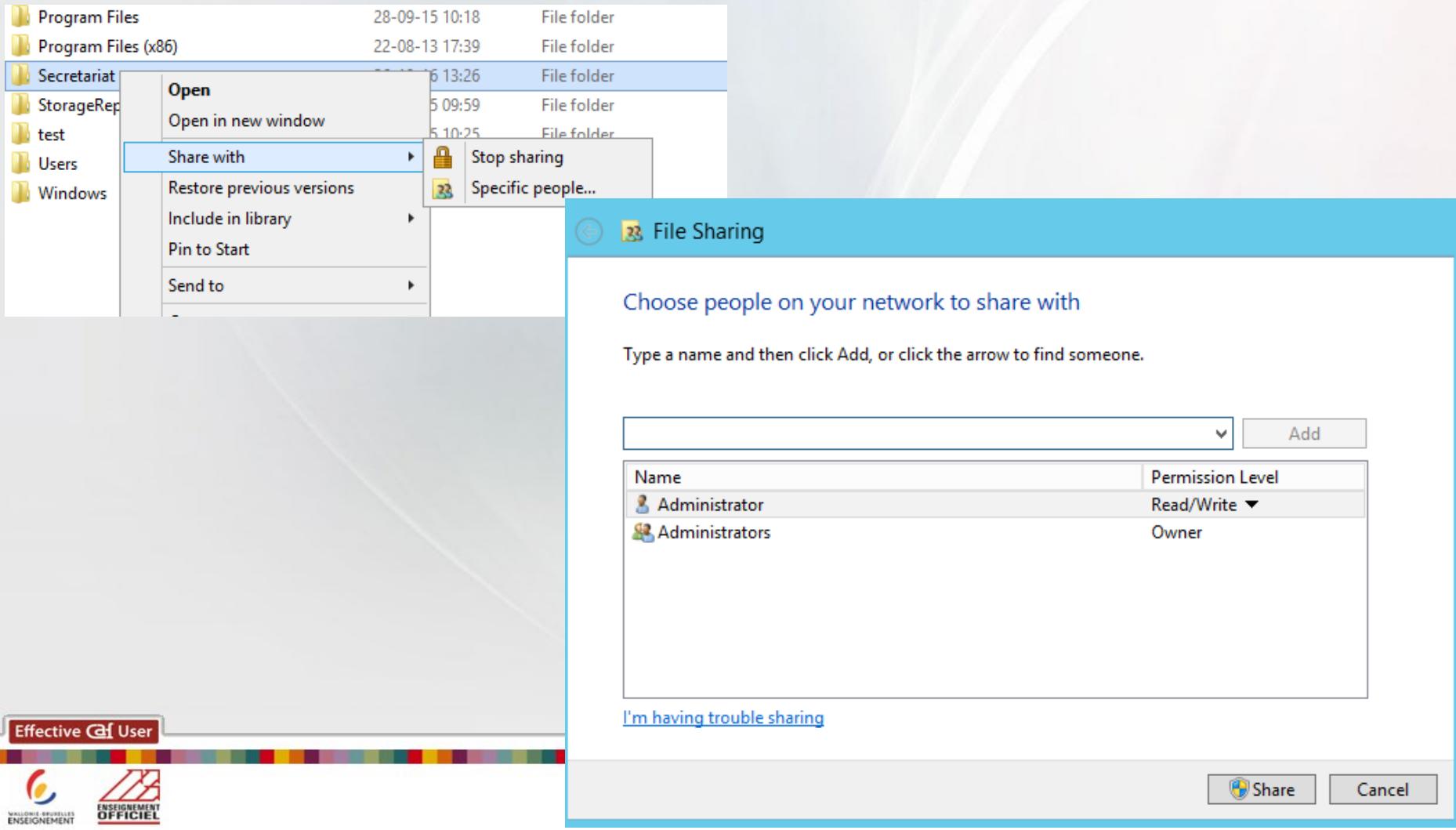


## 12. Les partages

- Dossier partagé : point d'entrée réseau d'un dossier sur un serveur
- UNC (Universal Name Convention)
  - \\NomDuSrv\\NomDu Partage
- \$ à la fin du nom du partage: Partage caché

# 12. Création d'un partage

- Via l'assistant



The screenshot shows a Windows file sharing interface. On the left, a file explorer window displays several folders: Program Files, Program Files (x86), Secretariat, StorageRep, test, Users, and Windows. The 'Secretariat' folder is selected, and its context menu is open. The 'Share with' option is highlighted, showing a submenu with 'Stop sharing' and 'Specific people...'. A 'File Sharing' dialog box is overlaid on the screen. It has a title bar 'File Sharing' with a help icon. The main area contains the text 'Choose people on your network to share with' and 'Type a name and then click Add, or click the arrow to find someone.' Below this is a search input field and an 'Add' button. A table lists sharing permissions:

Name	Permission Level
Administrator	Read/Write ▾
Administrators	Owner

At the bottom of the dialog, there is a link 'I'm having trouble sharing' and two buttons: 'Share' and 'Cancel'.

# 12. Crédit d'un partage – sans assistant

**Secretariat Properties**

General Sharing Security

Network File and Folder Sharing

Secretariat Not Shared

Network Path:  
Not Shared

Share...

Advanced Sharing

Set custom permissions, create multiple shares, and set other advanced sharing options.

Advanced Sharing...

**Advanced Sharing**

Share this folder

Settings

Share name:  
Secretariat

Add Remove

Limit the number of simultaneous users to: 16777

Comments:

Permissions Caching

OK Cancel Apply

**Permissions for Secretariat**

Share Permissions

Group or user names:  
Everyone

Add... Remove

Permissions for Everyone

	Allow	Deny
Full Control	<input type="checkbox"/>	<input type="checkbox"/>
Change	<input type="checkbox"/>	<input type="checkbox"/>
Read	<input checked="" type="checkbox"/>	<input type="checkbox"/>

OK Cancel Apply

# 12. Création d'un partage – Computer Management

Computer Management

File Action View Help

Computer Management (Local)

System Tools

- Task Scheduler
- Event Viewer
- Shared Folders
  - Shares
  - Sessions
  - Open Files
- Performance
- Device Manager

Storage

- Windows Server Backup
- Disk Management

Services and Applications

Share Name	Folder Path	Type	# Client Connections	Description
ADMIN\$	C:\Windows	Windows	0	Remote Admin
CS	C:\	Windows	0	Default share
CertEnroll	C:\Windows\system32\certenroll	Windows	0	Active Directory Certific...
Compta	C:\Compta	Windows	0	
Cours	C:\Cours	Windows	0	
IPC\$		Windows	0	Remote IPC
NETLOGON	C:\Windows\SYSVOL\NETLOGON	Windows	0	Logon server share
Partage	C:\Partage	Windows	0	
SYSVOL	C:\Windows\SYSVOL\SY...	Windows	0	Logon server share

# 13. Les permissions de partage

- Les permissions :
  - Contrôle total
  - Modifier
  - Lire
- Si permission NTFS et de partage = permission la plus restrictive

## 14. partage en ligne de commande

- Utilitaire net share
- Création d'un partage :
  - Net share NomPartage = CheminDossierAPartager
- Suppression :
  - Net share NomPartage \\NomServer /delete

## 15. Bonnes pratiques

- Organiser les dossiers suivant le niveau de confidentialité
- Volume dédié aux fichiers
- Dossier le plus élevé = autorisation la plus restrictive
- Ne pas utiliser les permissions NTFS avancées
- Utiliser les groupes

# 16. Permissions effectives - outils

Advanced Security Settings for Secretariat

Name: C:\Secretariat  
 Owner: Administrators (BELGIQUE\Administrators) [Change](#)

[Permissions](#) [Share](#) [Auditing](#) [Effective Access](#)

Effective Access allows you to view the effective permissions for a user, group, or device account. If the account is a member of a domain, you can also evaluate the impact of potential additions to the security token for the account. When you evaluate the impact of adding a group, any group that the intended group is a member of must be added separately.

User/ Group: Eleve1 (eleve1@belgique.lan) [Select a user](#)  
 Include group membership [Click Add items](#) [Add items](#)

Device: [Select a device](#)  
 Include group membership [Click Add items](#) [Add items](#)

[Include a user claim](#)  
[Include a device claim](#)

[View effective access](#)

Effective access	Permission	Access limited by
	Full control	Share, File Permissions
	Traverse folder / execute file	
	List folder / read data	
	Read attributes	
	Read extended attributes	
	Create files / write data	Share

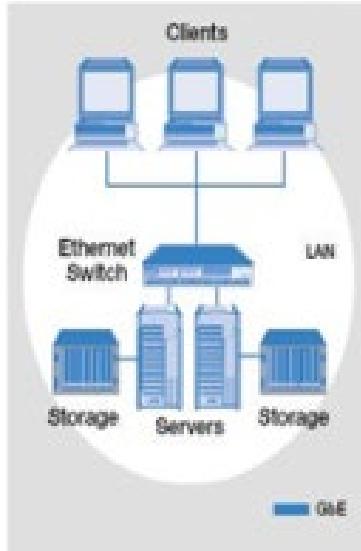
[OK](#) [Cancel](#) [Apply](#)

**Effective User**

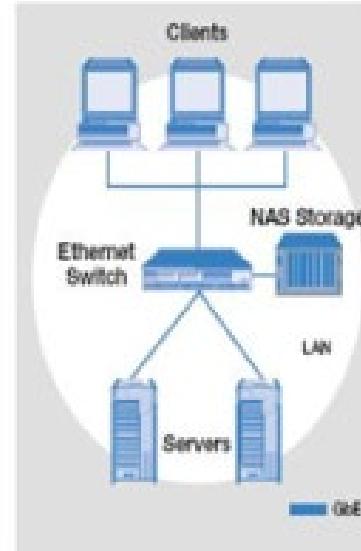
# 17. DAS, NAS, SAN

## Evolution of Network Storage

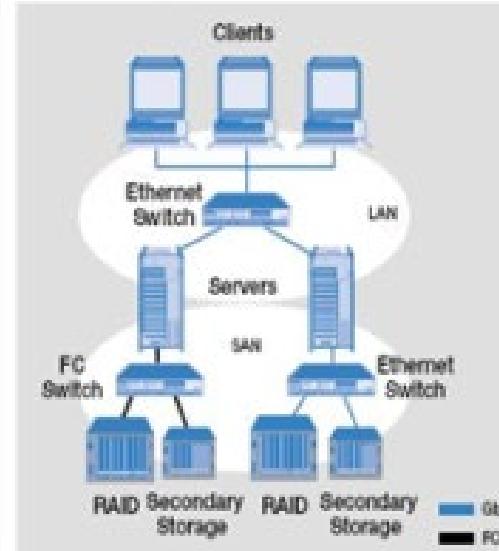
Direct Attached Storage



Network Attached Storage



Storage Area Network



- High cost of management
- Inflexible
- Expensive to scale

- Transmission optimized for file transactions
- Storage traffic travels across the LAN

- Transmission optimized for file transactions
- Separate LAN and SAN
- Increases data availability
- Flexible and scalable

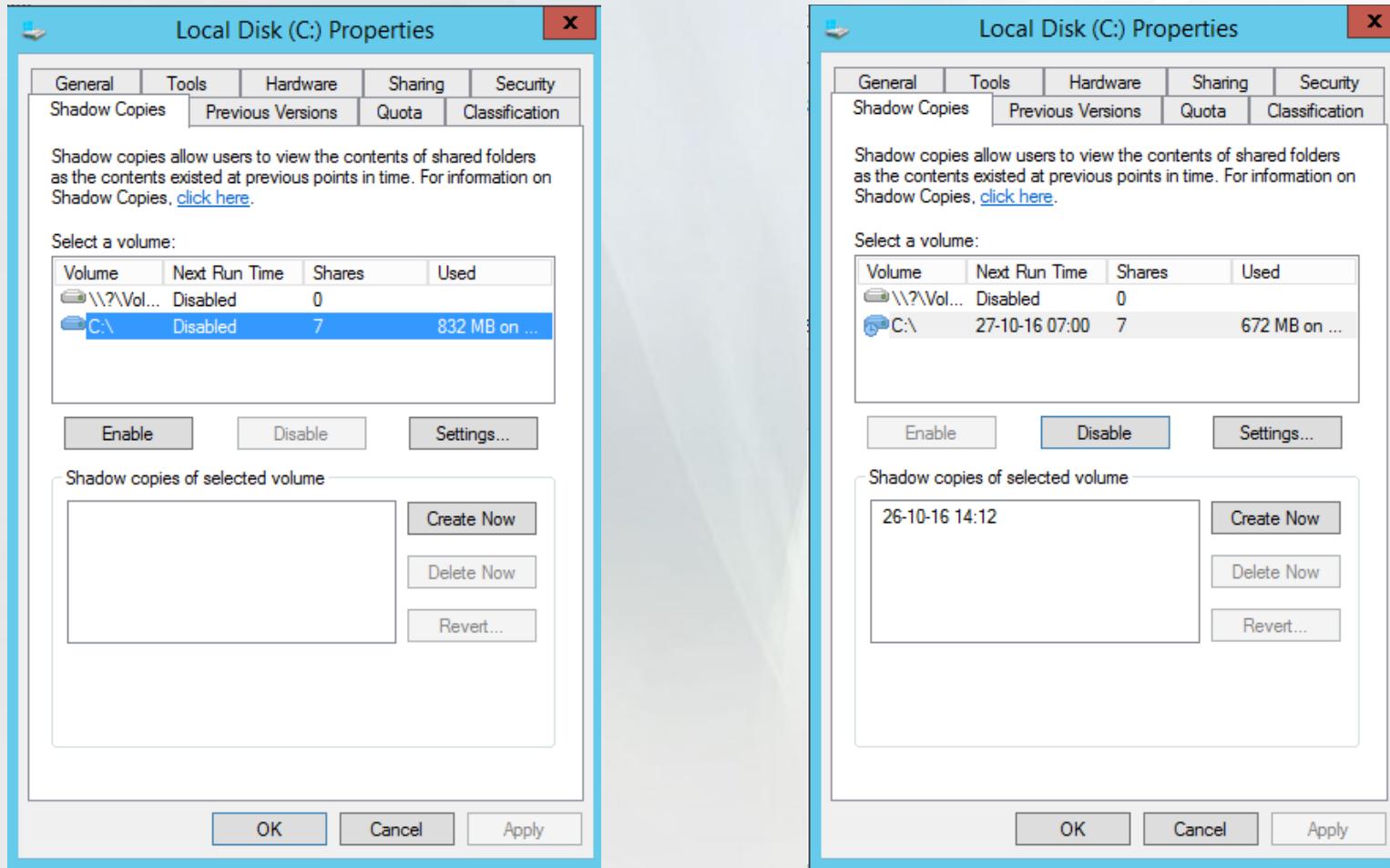
## 18. Les clichés instantanés

- Volume Shadow Copy (VSC)
- Le VSC (clichés instantanés) permet de garder automatiquement une version précédente des fichiers partagés sur un serveur Windows (en Domaine ou en WorkGroup). L'utilisateur peut ainsi aller rechercher lui-même ses fichiers qu'il a supprimés par mégarde.
- Cette option entraîne évidemment une baisse des performances du serveur
- Travail au niveau des clusters disques

## 18. Les clichés instantanés (1)

- Bonnes pratiques :
  - Volume dédié
  - Sauvegarder normalement
  - Pas de planification inférieure à 1 heure
  - Formatage du volume cluster > 16ko

# 18. Les clichés instantanés (2)



# 18. Les clichés instantanés (3)

**Settings**

Volume: C:\

Storage area  
Located on this volume: C:\

Maximum size:  No limit  Use limit: 2524 MB

Note: You need at least 300MB free space to create a shadow copy.

Schedule... **Schedule**

Note: The default schedule creates two shadow copies per day. Avoid creating shadow copies more frequently than once per hour.

OK Cancel

C:\ \ ? X

Schedule

1. At 07:00 every lun., mar., mer., jeu., ven. of every week, starting 26-1

New Delete

Schedule Task: Start time:  
Weekly 07:00 Advanced...

Schedule Task Weekly  
Every 1 week(s) on:  Mon  Sat  
 Tue  Sun

Advanced Schedule Options

Start Date: mercredi 26 octobre 2016

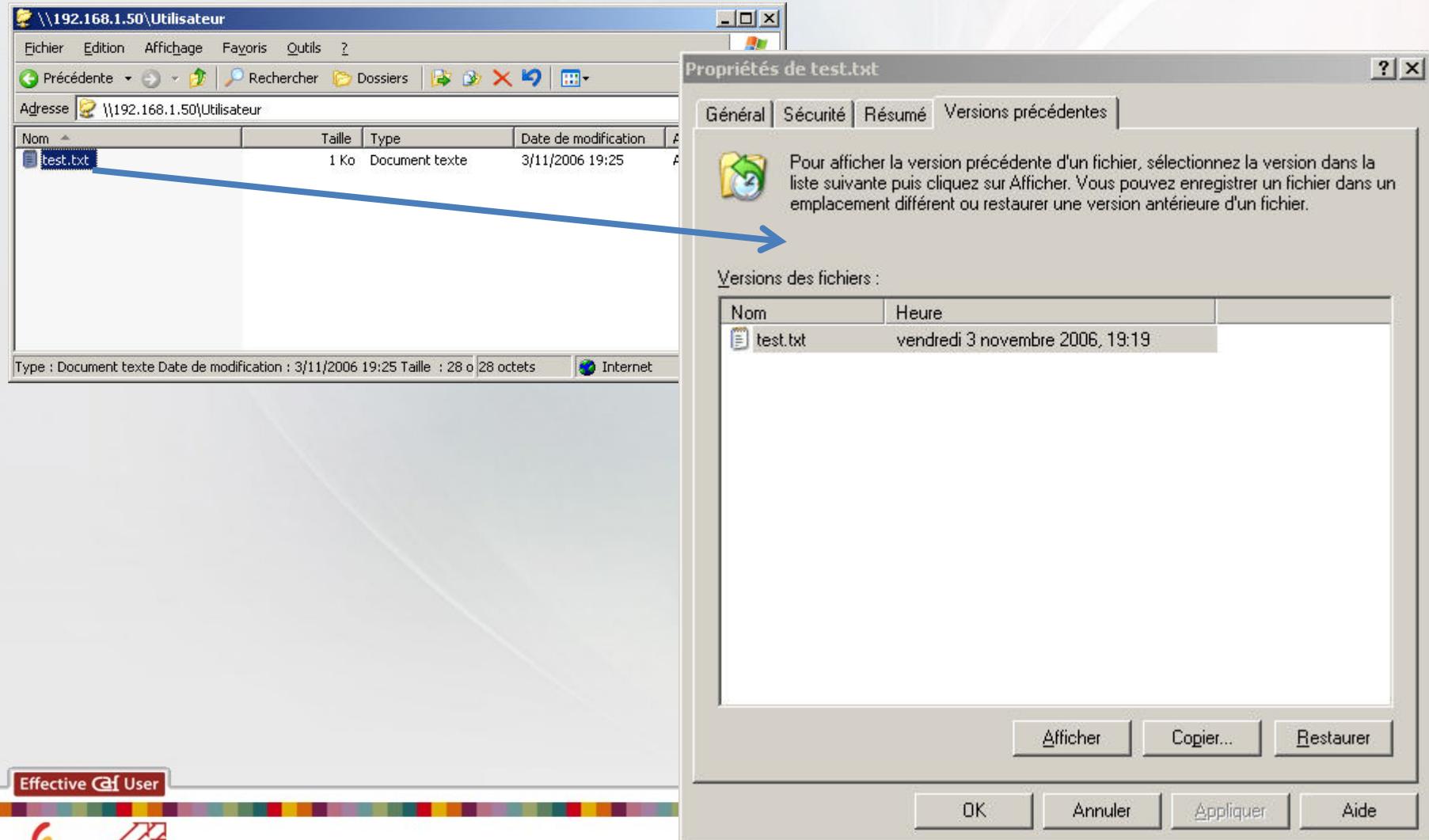
End Date:

Repeat task  
Every:  Time:  Duration:  hour(s) minute(s)

If the task is still running, stop it at this time.

OK Cancel

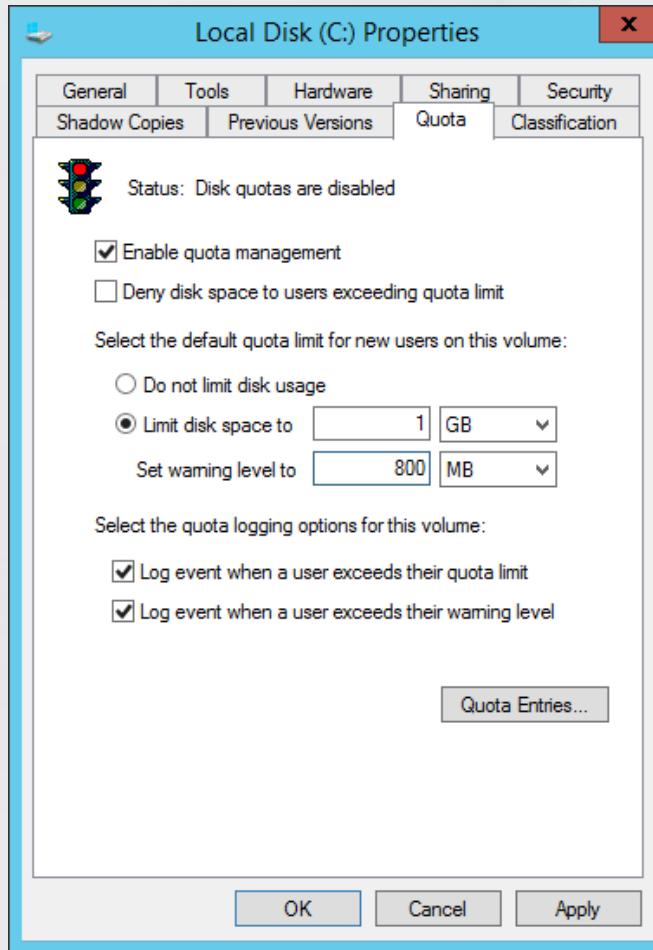
# 18. Les clichés instantanés (4)



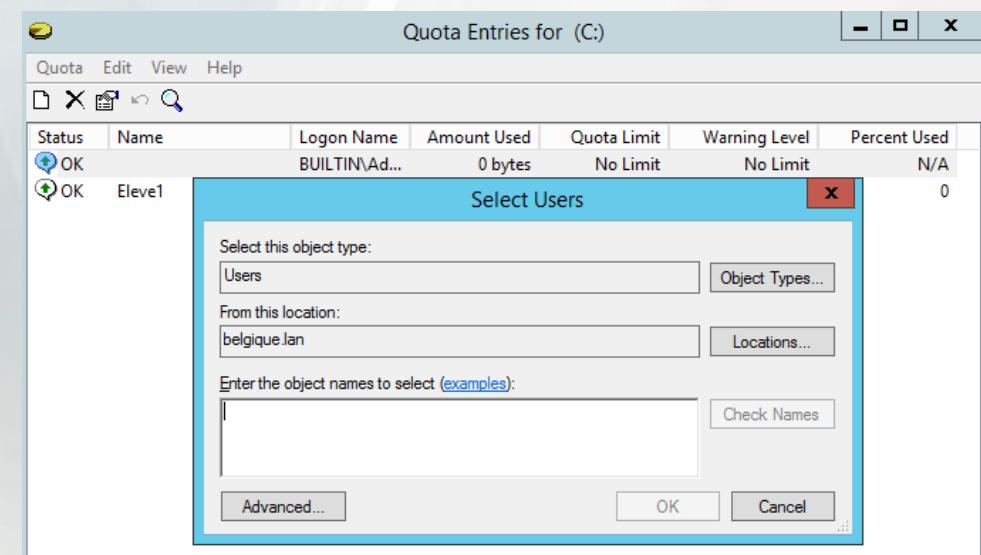
## 18. Les clichés instantanés (5)

- En ligne de commande :
  - Vssadmin (pour activer le VSC)
  - Schtasks (pour la planification)

# 19. Les quotas



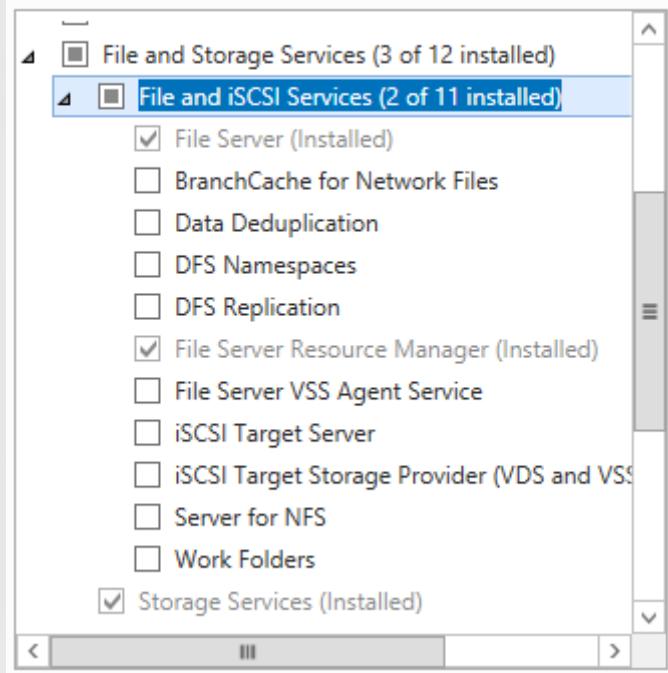
- Limiter la capacité des données stockées par les utilisateurs
- Granularité : le volume



# 20. Rôle de serveur de fichiers

- Services
  - Gestion du partage et du stockage
  - Système de fichiers distribués – DFS
  - Gestionnaire de ressources du serveur de fichiers (FSRM)
  - Service pour NFS
  - Service de recherche Windows
- Outils supplémentaires
  - Sauvegarde de Windows
  - Gestionnaire de stockage pour réseau SAN
  - Clustering avec basculement
  - MPIO

### Roles



The screenshot shows the 'File and Storage Services' section of the Windows Server Roles and Features Wizard. Under 'File and iSCSI Services (2 of 11 installed)', several checkboxes are checked, indicating they are installed:

- File Server (Installed)
- BranchCache for Network Files
- Data Deduplication
- DFS Namespaces
- DFS Replication
- File Server Resource Manager (Installed)
- File Server VSS Agent Service
- iSCSI Target Server
- iSCSI Target Storage Provider (VDS and VSS)
- Server for NFS
- Work Folders
- Storage Services (Installed)

# Module 14

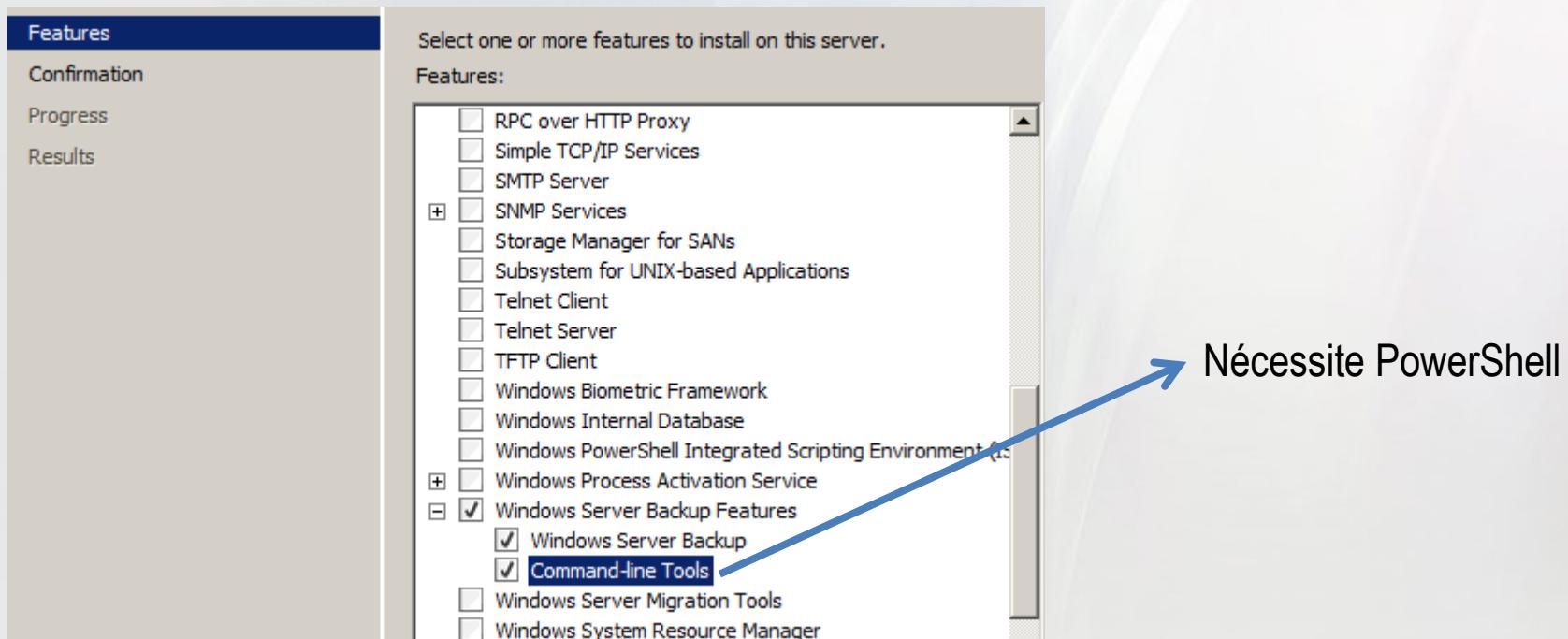
## Sauvegarde de la base de données AD

# 1. La base de données

- Base de données d'annuaire : fichier NTDS.DIT
- Emplacement par défaut : %systemroot%\ntds
- Par défaut la base de données est nettoyée toutes les 12h
  - Inspecte la BD
  - Défragmentation en ligne

## 2. Assistant de sauvegarde

- Wbadmin
- Ocsetup windowsserverbackup



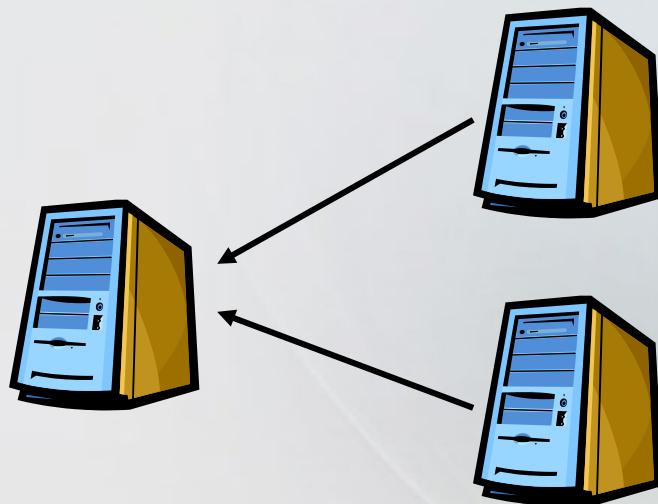
## 3. Sauvegarder l'AD

- Impossible de sauvegarder uniquement l'AD
- Les fichiers suivants seront sauvegardés :
  - Le registre
  - La BD des classes COM+
  - Fichiers de démarrage du système
  - BD du service de certificat
  - La base de donnée d'annuaire (l'AD)
  - Le dossier SYSVOL
- Wbadmin start systemstatebackup –backuptarget:F:

## 4. Restauration

- Tous les fichiers sauvegardés seront restaurés (impossible de ne restaurer que l'AD)
- Il existe deux types de restauration :
  - La forcée
  - La non forcée (par défaut)
- Démarrer le PC « en mode de restauration AD » (F8 au démarrage)

## Restauration non forcée

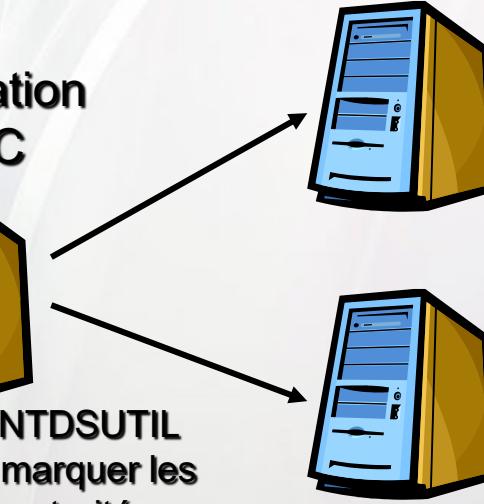


**RéPLICATION sur le DC1 des  
Modifications faites sur  
les aux autres DC**

## Restauration forcée

**Restauration  
du DC**

Rq. : utilitaire NTDSUTIL  
Possibilité de marquer les  
Objets faisant autorités



- Redémarrer en mode « Restauration AD » ou net stop ntds
- Ntdsutil
- Authoritative restore
  - Restore subtree DN\_objet

# Module 15

Renommer un domaine ou un contrôleur de domaine

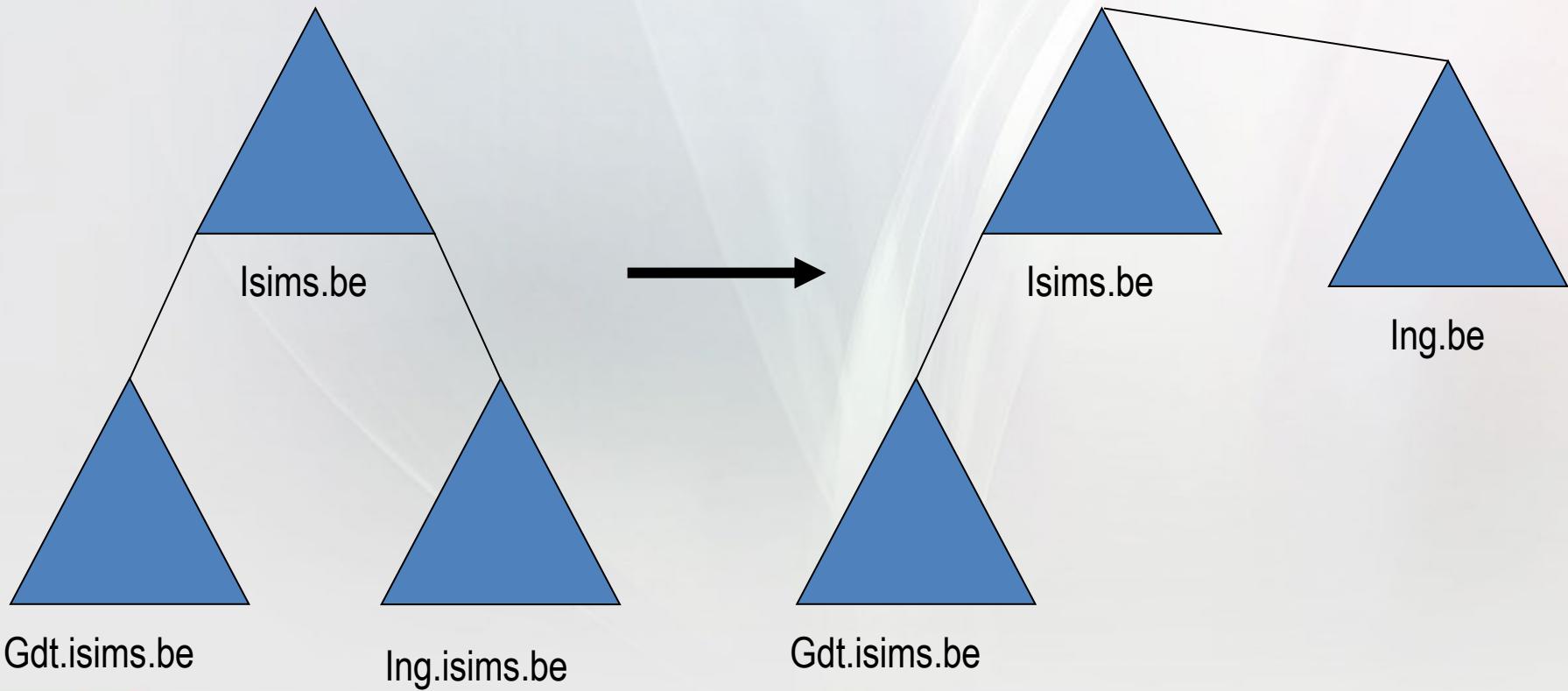
## 1. Renommer un domaine (1)

- A partir de Windows 2003, c'est possible (mais très long et très dangereux)
- Etant donné que l'AD travaille avec les noms de domaine, le changement du nom d'un domaine entraîne la réorganisation complète de la forêt.

## 7. Renommer un domaine (2)

- Impossible de renommer le domaine root
- Renommer un domaine comprend 15 étapes
- Le domaine renommé est HS pendant toute la durée de l'opération
- Outils : Rdom.exe (+gpfixup.exe)
- Liens GPO inter domaines sont cassés, les refaire manuellement
- Tous les DC doivent être des Windows 2k3 et être en « Windows srv 2003 functional Level » minimum

## 7. Renommer un domaine (3)



## 7. Renommer un domaine (4)

1. Créer une zone dynamique afin de recevoir l'enregistrement srv du nouveau domaine.
2. Vérifier le « Functional Level »
3. Créer « shortcut trust » (two-way) afin de créer la nouvelle arborescence (dans l'exemple pas nécessaire)
4. Vérifier les références DFS
5. Utiliser Rdom.exe sur un serveur membre du domaine à renommer (pas sur le DC)
6. Se logger en tant qu'enterprise admin sur le serveur membre
  - Rdom /list
  - Domainlist.xml est créé
7. Editer le fichier et changer le nom de domaine
8. Vérifier avec Rdom /showforest

## 7. Renommer un domaine (5)

9. Rendom /upload ->dclist.xml
10. Rendom /prepare
11. Rendom /execute
12. Rebooter tous les serveurs membres et toutes les PC 2 fois (pour le changement de suffix du domaine)
13. Changer le suffix des DC manuellement
14. Remettre les GPO
  - GPFIXUP /olddns: « name »
  - /newdns: « name »
  - /oldnb: »name »
  - /newnb: »name »
  - /dc: « nom netbios du PDC Emulator »
15. Rendom /clean

Les DC redémarrent automatiquement

## 7. Renommer un domaine (6)

- Exemple de .xml

## 8. Renommer un DC (1)

- A partir de Windows 2003, c'est possible et toujours avec NETDOM.EXE
- Exemple : dc1.isims.be -> dc11.isims.be
- Mode minimum : Domain Functional Level Windows srv 2003

## 8. Renommer un DC (2)

- Netdom computername « CurrentComputerName » /add: « NewComputerName »
- Attendre la réPLICATION
- Netdom computername « CurrentComputerName » /makeprimary: « NewComputerName »
- Redémarrer le serveur
- Netdom computername « NewComputerName » /remove: « OldComputerName »

# Module 16

## Les stratégies de groupes

# 1. Définition (1)

- GPO (Group Policies Object)
- Elles sont utilisées pour distribuer des paramètres de configuration.
- Simplification des tâches administratives
- Permet de définir l'environnement de travail des utilisateurs.
- 2 types de configurations :
  - Utilisateurs : HKCU
  - Ordinateurs : HKLM
- Peuvent être appliquées en local, à un site, à un domaine ou à des UO.

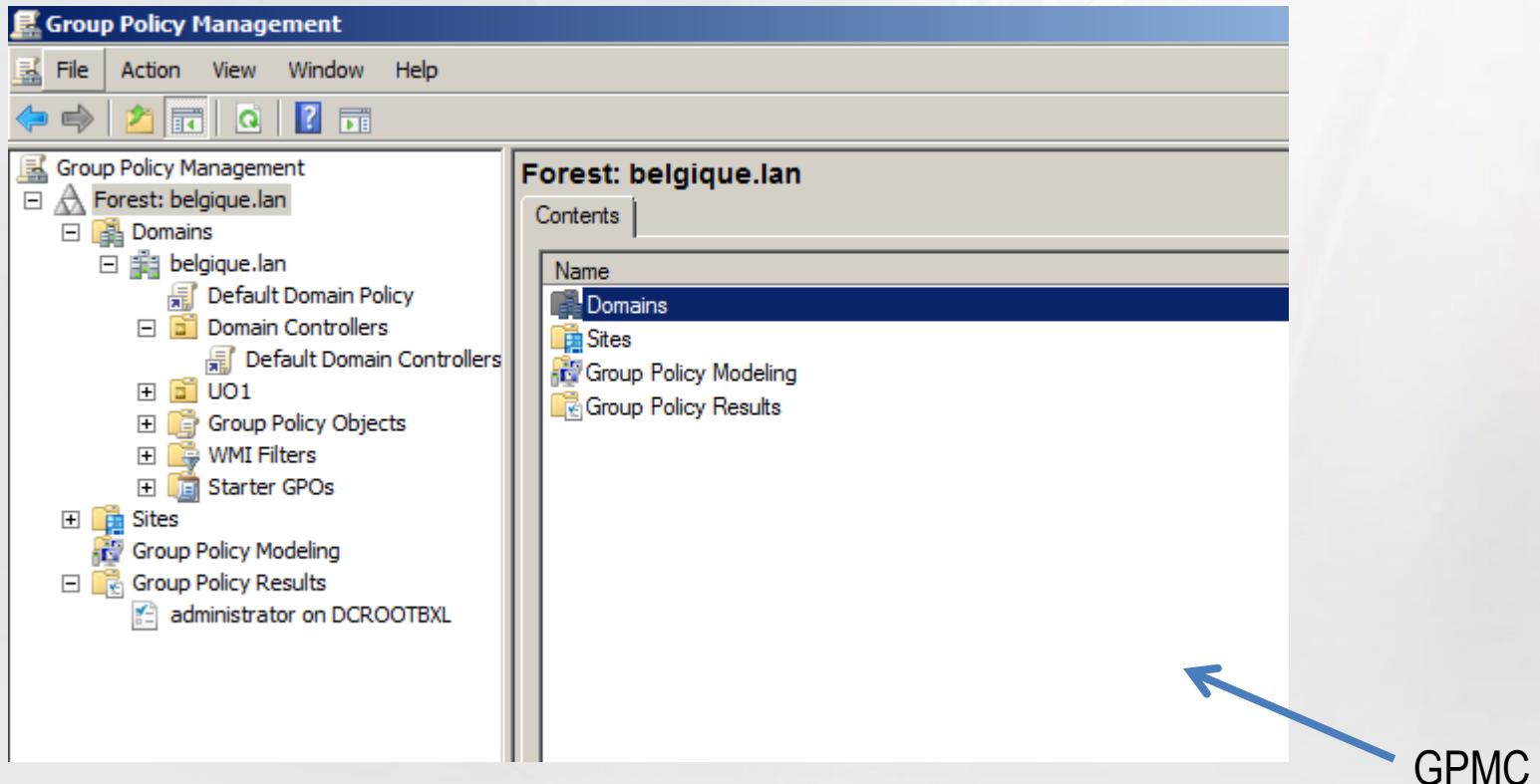
## 1. Définition (2)

- Contient une DACL ainsi qu'un identificateur unique.
- 2 types de GPO :
  - Locale : créée localement sur la machine
  - Non locale : créée dans l'AD
    - GPC (Group Policy Container)
    - GPT (Group Policy Template)

La GPO locale est écrasée par la GPO non locale si elle existe.

## 2. Gestion des GPO

- MMC : Administrative tools – Group Policy Management



## 2.1. GPO non locale

- 2 possibilités de création :
  - Liée directement à un site, un domaine ou une UO.
  - Non liée, elle est ensuite attachée.
- GPO liée : Clic droit sur le conteneur
- GPO non liée : Group Policy Objects -> New

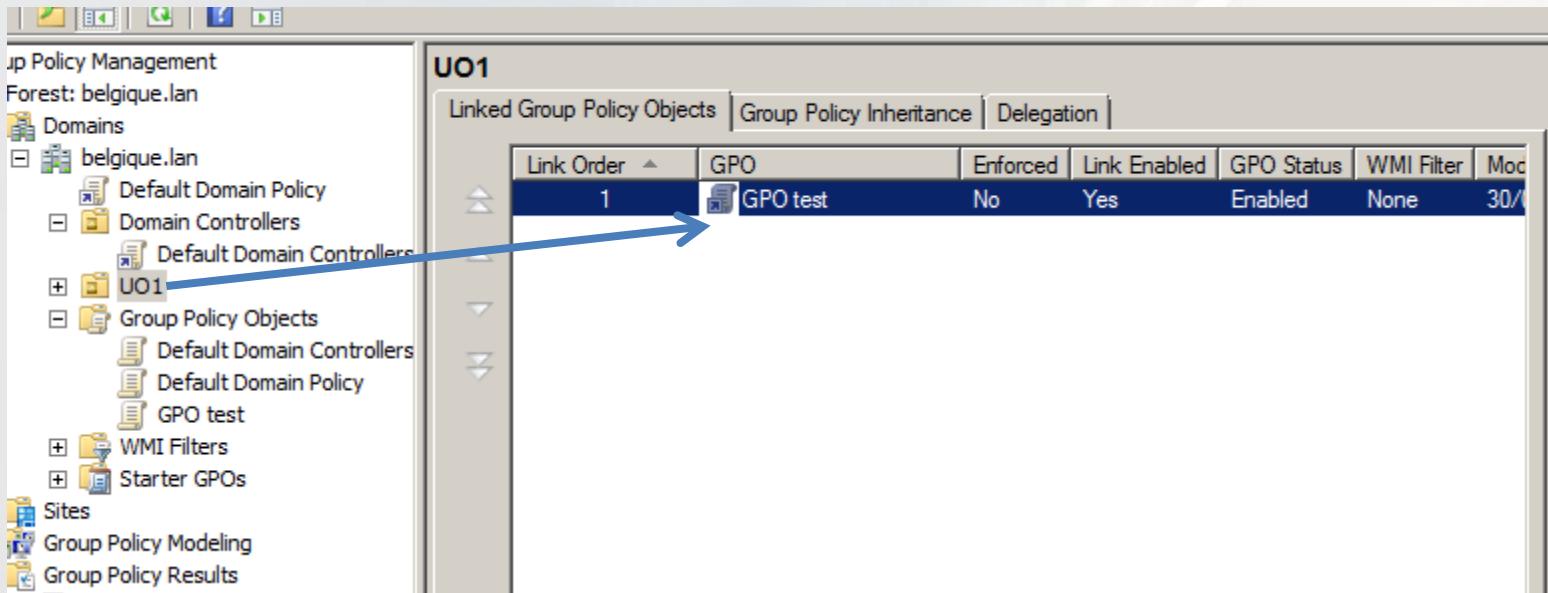
## 3. Modification

- Dans une GPO, nous avons 2 nœuds :
  - Config d'ordinateur (au démarrage)
  - Config d'utilisateur (ouverture de session)
- Configuration d'ordinateur écrase la configuration d'utilisateur.

## 3.1. Liaison d'une GPO existante(1)

- Objets identifiants les GPO attachées à un utilisateurs :
  - gPLink : Liste et ordre des GPO
  - gPOptions : Paramètres de l'héritage
- Possibilité de lier une S, D, OU à plusieurs GPO
- Possibilité de lier une GPO à plusieurs S, D, OU

## 3.1. Liaison d'une GPO existante(2)

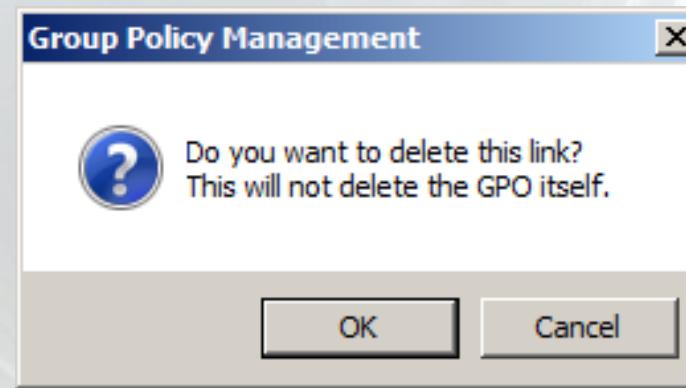


The screenshot shows the Windows Group Policy Management console. On the left, the navigation pane displays the forest 'belgique.lan' and various administrative units (UO1, UO2, UO3) under the 'belgique.lan' domain. The 'Group Policy Objects' node is expanded, showing 'Default Domain Controllers', 'Default Domain Policy', and 'GPO test'. A blue arrow points from the 'GPO test' entry in the navigation pane to its corresponding row in the 'Linked Group Policy Objects' table on the right.

Link Order	GPO	Enforced	Link Enabled	GPO Status	WMI Filter	Mod.
1	GPO test	No	Yes	Enabled	None	30/10/2013

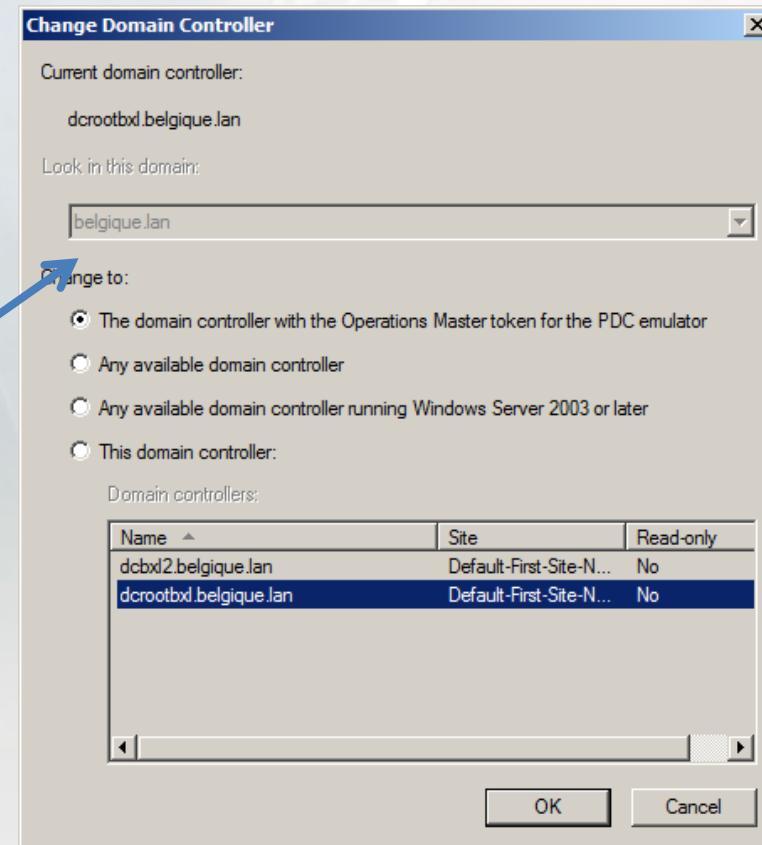
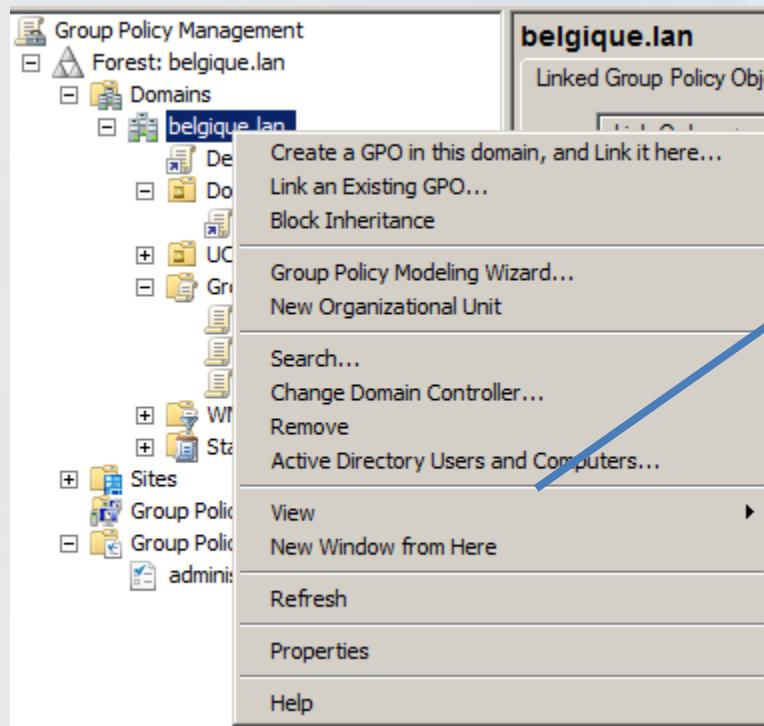
## 3.1. Liaison d'une GPO existante(3)

Lorsque vous désirez supprimer une GPO :



## 3.2. Traitement (1)

- Identification du DC : par défaut le PDC emulator
- Changement de DC



## 3.2. Traitement (2)

- Traitement des GPO :
  - Synchrone : une par une, fiable mais lente
  - Asynchrone : rapide mais dangereux
- Par défaut : traitement synchrone
- Changement du mode :

Config d'ordinateur\Modèle d'admin\System\Stratégie de groupe

	Appliquer la stratégie de groupe pour les ordinateurs de manière asynchrone pendant le démarrage	Non configuré
----------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------	---------------

	Appliquer la stratégie de groupe pour les utilisateurs de manière asynchrone pendant la connexion	Non configuré
-----------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------	---------------

## 3.2. Traitement (3)

- Actualisation périodique des GPO :
  - Entre DC : toutes les 5 min
  - Sur les PC : toutes les 90 min + un temps aléatoire de 30 min
- Mise à jour forcée :
  - Windows 2000 :  
`Secedit/refreshpolicy user_policy /enforce`  
`Secedit/refreshpolicy machine_policy /enforce`
  - Windows 2003, 2008, 2012 et 2016 :  
`GPUPDATE /Force`

# Module 17

## GPO - Fonctionnement

# 1. Règles des GPO (1)

- Ordre d'application des GPO :
  - Site
  - Domaine
  - Unité d'organisation
  - Unité d'organisation enfant
- L'héritage
  - OU1 ← GPO1
    - User1
    - OU2
      - User2
      - OU3
        - » User3

Avec l'héritage, tous les utilisateurs ont la même GPO1

# 1. Règles des GPO (2)

- L'héritage cumulatif : Si plusieurs GPO, on a le cumul des configurations
  - Site (GPO1)
    - Domaine (GPO2)
      - UO (GPO3)
        - » User

L'user aura le cumul de GPO1+GPO2+GPO3

# 1. Règles des GPO (3)

- Conflit de paramètres : Si conflit entre GPO, la dernière GPO sera appliquée
- Conflit de multiples GPO sur un même conteneur: Lecture de bas en haut
- Conflit entre GPO d'users et d'ordinateurs : les paramètres d'ordinateurs sont prioritaires
- Blocage de l'héritage : uniquement au niveau du domaine ou des UO

# 1. Règles des GPO (4)

- Options aucun remplacement : Permet d'imposer une configuration à tous les OU enfants
- Désactiver la stratégie Permet de ne pas activer la GPO au S, D, OU
- Désactiver les paramètres d'user ou d'ordinateur : Permet de désactiver à une GPO ses par. d'user ou d'ordi (sur les OU)

Link Order	GPO	Enforced	Link Enabled	GPO Status
1	Default Domain Policy	No	Yes	Enabled

Location	Enforced	Link Enabled	Path
U01	No	Yes	belgique.lan/U01

Attention avec les GPO liée

# 1. Règles des GPO (5)

## Traitement par bouclage de rappel

- Traitement par défaut

Lorsqu'un utilisateur se connecte sur un PC ne faisant pas partie de son UO, on a cumul des GPO

- Traitement par boucle de rappel

Quand on ne veut pas que la GPO associée à l'utilisateur ne soit pas prise en compte lorsqu'il se connecte à un PC ne faisant pas partie de son UO

2 modes : la fusion (par défaut) et le remplacement (n'applique que la GPO d'ordinateur)

# 1. Règles des GPO (6)

- Permissions des GPO

GPO = Objet -> DACL avec ACE

Accès : Propriétés de l'UO -> Onglet stratégie de groupe -> Bouton « Propriétés » -> Onglet sécurité

Ex : Possibilité d'appliquer une GPO à tous les users d'une UO sauf à 1  
-> ACE : appliquer la stratégie

## 2. Maintenance des GPO (1)

- Journal de diagnostics  
dans la clé :  
HKLM\Software\Microsoft\WindowsNT\CurrentVersion\WinLogon  
ajouter la valeur DWORD : RunDiagnosticLoggingGlobal à 1  
Les événements détaillés seront listés dans le journal des applications

## 2. Maintenance des GPO (2)

- Inscription commentée
  - Journaliser les modifications et configurations affectées à un PC : HKLM\Software\Microsoft\WindowsNT\CurrentVersion créer une clé « UserEnvDebugLevel » de type DWORD et donner la valeur 30002.
- Le fichier se trouvera dans \debug\UserMode\Userenv.log

## 2. Maintenance des GPO (3)

- Outils supports : Netdiag.exe et replmon.exe
- Outils du kit de ressources techniques : GpoTool.exe et Gporesult.exe

# Module 18

## GPO - Paramétrage

# 1. Déploiement d'applications

- GPO permettant de :
  - centraliser les installations de logiciels
  - de les distribuer
  - d'affecter des correctifs ou des mises à jour
  - de les supprimer.
- Sans intervention de l'utilisateur final.

## 1.1. Publication et attribution (1)

- Ne fonctionne qu'avec les packages Windows :
  - MSI = package de base
  - MST = MSI + spécificité du logiciel
  - MSP = MSI + correctif ou maj
  - AAS = fichier de script
  - ZAP = fichier texte informant comment publier l'application

## 1.1. Publication et attribution (2)

- Déploiement d'une application :
  - Créer un partage
  - Copier les fichiers MSI dans le partage
  - Accorder les autorisations aux groupes et utilisateurs
  - Créer une GPO :

Installation de logiciel -> Nouveau -> Package

- 2 possibilités pour créer cette GPO :
  - Config ordinateurs (Application sur le PC quelque soit l'user)
  - Config d'utilisateurs (Application par rapport à l'user quelque soit le PC)

## 1.1. Publication et attribution (3)

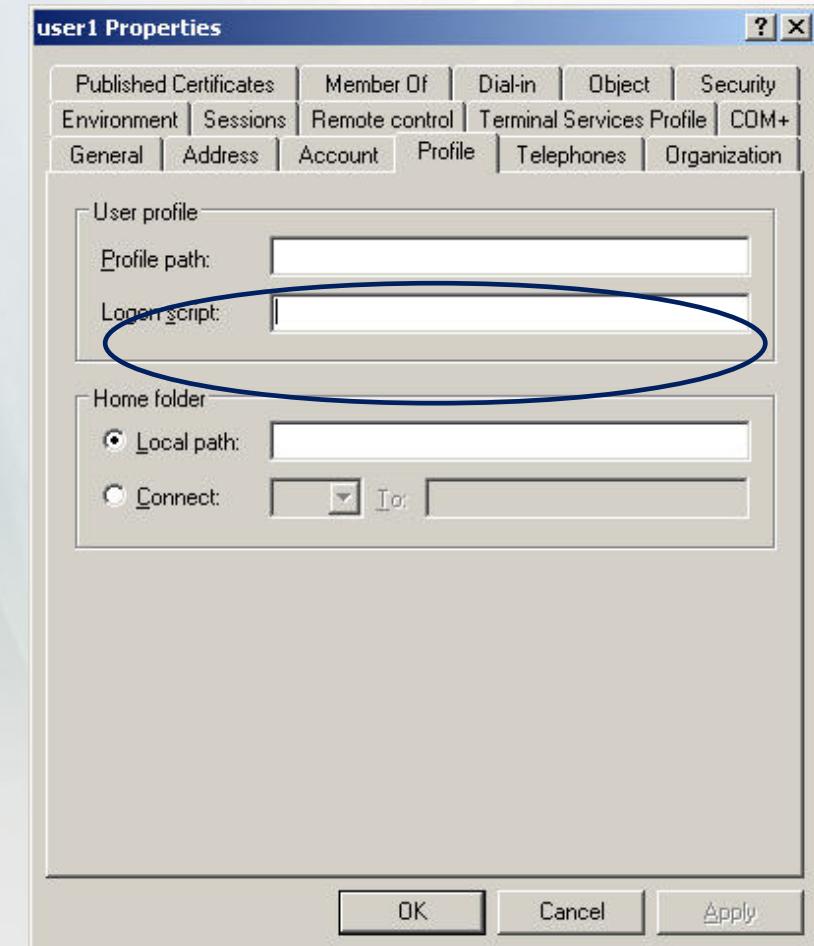
- 2 choix possibles :
  - Publication : l'application se retrouve dans ajout/suppression de programmes. Si l'utilisateur veut l'installer, il doit le faire volontairement (uniquement en C.U.)
  - Attribution :
    - CO : application directement installée
    - CU : application s'installe quand l'user ouvre un fichier de cette extension ou clic sur le raccourcis du pgm se trouvant dans le menu démarre

## 2. Affectation de scripts (1)

- Scripts : .bat, .cmd, WSH (.vbs, js, ...)
- Affectation d'un script
  - Sur l'utilisateur
  - Via les GPO

## 2. Affectation de scripts (2)

- Sur un utilisateur
  - Via les propriétés de l'utilisateur dans l'AD
  - Script stocké :  
%systemroot%\sysvol\sysvol\domain\script



## 2. Affectation de scripts (3)

- Via les GPO
  - Ouverture et fermeture de session
  - Démarrage et arrêt du PC
- Configuration
  - CO – Modèles d'administration – Système – Ouverture de session
  - CU – Modèles d'administration – Système – Ouverture – Fermeture de session
- Associer un script : CO ou CU – Paramètres Windows - Script

### 3. Les profils itinérants

- Paramétrage via les GPO :
  - L'algorithme de fusion (téléchargement des différences entre le profil stocké sur le disque et celui sur le partage) : CO – Modèles d'administration – Système – Ouverture de session
  - La taille des profils : CU – Modèles d'administration – Système – Ouverture – Fermeture de session

## 4. La redirection des dossiers

- Dossiers : Mes documents ; Application Data ; Bureau ; Menu démarrer.
- Exemple du dossier « mes documents » Rediriger en fonction du groupe de sécurité : CU – Paramètres Windows – Redirection de dossiers – Clic droit propriétés de Mes documents – Emplacement où sera stocké ce dossier ([\partage\%username%](\\partage\\%username%))
- Rediriger vers un emplacement centralisé pour tout le monde.

## 5. Les fichiers hors connexions

- Il est possible de permettre aux utilisateurs mobiles de travailler avec les fichiers partagés en étant « hors connexions ».
- Les GPO permettant la configuration de cette options se trouvent dans :
  - CO\Modèles d'administration\Réseau\Fichiers hors connexions
  - CU\Modèles d'administration\Réseau\Fichiers hors connexions

## 6. L'environnement utilisateur

- CO\Modèles d'administration
- CU\Modèles d'administration

## 7. Paramétrage de la sécurité

- Sécurité des comptes et des mots de passe
- Audit
- Droits des utilisateurs
- Options de sécurité
- Groupes restreints
- Services système
- Registre et système de fichier
- Stratégie de clé publique
- Sécurité du trafic réseau IP
- Modèle de sécurité

# Module 19

Contrôleur de domaine en lecture seule

# 1. Introduction

- RODC : Domain Controller Read Only
- Base de donnée AD (ntds.dit) en Ro
- But
  - Augmenter la sécurité sur les sites distants
  - Diminuer les risques d'attaques en cas de vol du DC

## 2. Caractéristiques (1)

- AD en lecture seule
- Si demande d'écriture sur un RODC par un client -> cette demande est envoyée à un DC classique
- Réplication unidirectionnelle
- Administration spécifique : sur un RODC, il existe un compte admin local
- DNS Ro si le service DNS est installé sur un RODC

## 2. Caractéristiques (2)

- Fonctions non disponibles
  - Les rôles FSMO
  - Serveur tête de pont (BHS)
- Mise en cache spécifique des login/pswd des clients

### 3. Sécurisation des Pswd

- Sur un RODC pas de login/pswd en cache  
But : pas de pswd sur le DC en cas de vol
- Authentification : toute authentification envoyée au RODC doit être transférée à un autre DC du domaine
  - Utilisation de la bande passante
  - RODC pas autonome en cas de coupure avec le DC
- Possibilité de spécifier explicitement les login/pswd qui seront répliqués sur le RODC

## 4. Gestion des comptes

- Deux groupes
  - Allowed RODC Password Replication Group
  - Denied RODC Password Replication Group

**Denied RODC Password Replication Group Properties**

General	Members	Member Of	Managed By
Members:			
	Name	Active Directory Domain Services Folder	
	Cert Publishers	belgium.lan/Users	
	Domain Admins	belgium.lan/Users	
	Domain Contr...	belgium.lan/Users	
	Enterprise Ad...	belgium.lan/Users	
	Group Policy ...	belgium.lan/Users	
	krbtgt	belgium.lan/Users	
	Read-only Do...	belgium.lan/Users	
	Schema Admins	belgium.lan/Users	

**Allowed RODC Password Replication Group Properties**

General	Members	Member Of	Managed By
Members:			
	Name	Active Directory Domain Services Folder	

## 5. RéPLICATION DES PSWD

Active Directory Users and Computers

File Action View Help

Active Directory Users and Computers [dcwallonie.be]

Saved Queries

belgium.lan

- Builtin
- Computers
- Domain Controllers
- ForeignSecurityPrincipals
- Managed Service Accounts
- Users

Name	Type	DC Type	Site	Description
DCMONS	Computer	Read-only, GC	Default-First-Sit...	
DCWALLONIE	Computer	GC	Default-First-Sit...	

DCMONS Properties

General	Operating System	Member Of	Delegation
Password Replication Policy	Location	Managed By	Dial-in

This is a Read-only Domain Controller (RODC). An RODC stores users and computers passwords according to the policy below. Only passwords for accounts that are in the Allow groups and not in the Deny groups can be replicated to the RODC.

Groups, users and computers:

Name	Active Directory Dom...	Setting
Account Operators	belgium.lan/Builtin	Deny
Administrators	belgium.lan/Builtin	Deny
Allowed RODC Passw...	belgium.lan/Users	Allow
Backup Operators	belgium.lan/Builtin	Deny
Denied RODC Passwo...	belgium.lan/Users	Deny
Server Operators	belgium.lan/Builtin	Deny

Effective User

Advanced... Add... Remove

WALLONIE-BRUXELLES  
ENSEIGNEMENT  
OFFICIEL

4

# 6. Comptes sur le RODC

**Advanced Password Replication Policy for DCMONS**

Policy Usage | Resultant Policy

Display users and computers that meet the following criteria:

Accounts whose passwords are stored on this Read-only Domain Controller

Users and computers: Objects retrieved: 2

Name	Domain Services Folder	Type	Password Last Changed	Password Ex
DCMONS	belgium.lan/Domain C...	Computer	18/10/2013 12:59:52	Never Expire
krbtgt_8264	belgium.lan/Users	User	18/10/2013 12:59:52	29/11/2013

Export... Prepopulate Passwords...

Comptes stockés sur le DCRo

**Advanced Password Replication Policy for DCMONS**

Policy Usage | Resultant Policy

Display users and computers that meet the following criteria:

Accounts that have been authenticated to this Read-only Domain Controller

Users and computers: Objects retrieved: 3

Name	Domain Services Folder	Type	Password Last Changed	Password Ex
Administrator	belgium.lan/Users	User	18/10/2013 12:28:59	29/11/2013
DCMONS	belgium.lan/Domain C...	Computer	18/10/2013 12:59:52	Never Expire
DCWALLONIE	belgium.lan/Domain C...	Computer	16/10/2013 17:38:57	Never Expire

Permet de prérepliquer les Pswd indispensables  
en cas de prob de contact avec le DC source

Comptes ayant été authentifiés sur le RODC

## 7. Prérequis

- Prérequis pour pouvoir installer un RODC
  - Niveau de fonctionnement de la forêt : Win2003
  - Un DC « normal » en minimum Win2k8 dans le même domaine
  - Installer la kb944043 sur les postes clients XP et Vista et sur les serveurs Win2k3

# Module 20

## Options supplémentaires

## 1. Les avantages

- Kerberos v5 supporte les algorithmes AES128 et 256
- Support des informations de dernière ouverture de session interactive (dans les journaux de sécurité)
- Le nom de la station de travail à partir de laquelle l'utilisateur a ouvert sa session
- Le nombre d'ouvertures de sessions refusées depuis la dernière réussie
- La stratégie de mot de passe granulaire

## 2. Stratégie Pswd granulaire

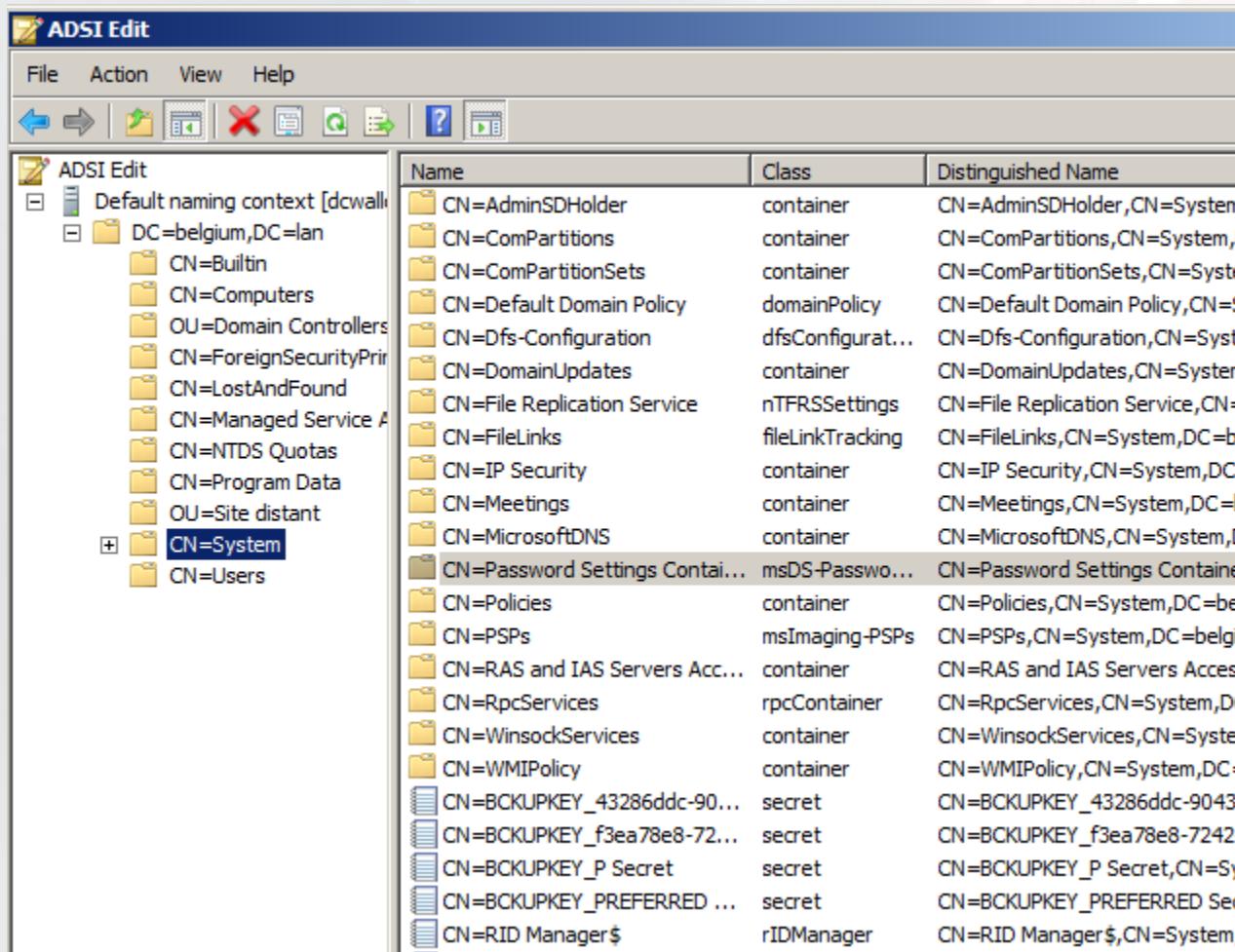
- Win < 2k8 -> Une seule stratégie de pswd pour l'ensemble du domaine
- A partir de Win2k8 : Possibilité d'avoir des stratégies différentes sur les utilisateurs et groupes globaux de sécurité d'un même domaine

## 3. Gestion Pswd granulaire (1)

- En Win2k8 pas de GUI
  - Utilisation de la nouvelle classe PSO (Password Settings Object)
  - Utilisation de l'ADSI Edit
- A partir de Win2k12, une interface graphique permet de gérer la granularité des pswd

## 3. Gestion Pswd granulaire (2)

Via l'utilitaire  
Adsiedit.msc

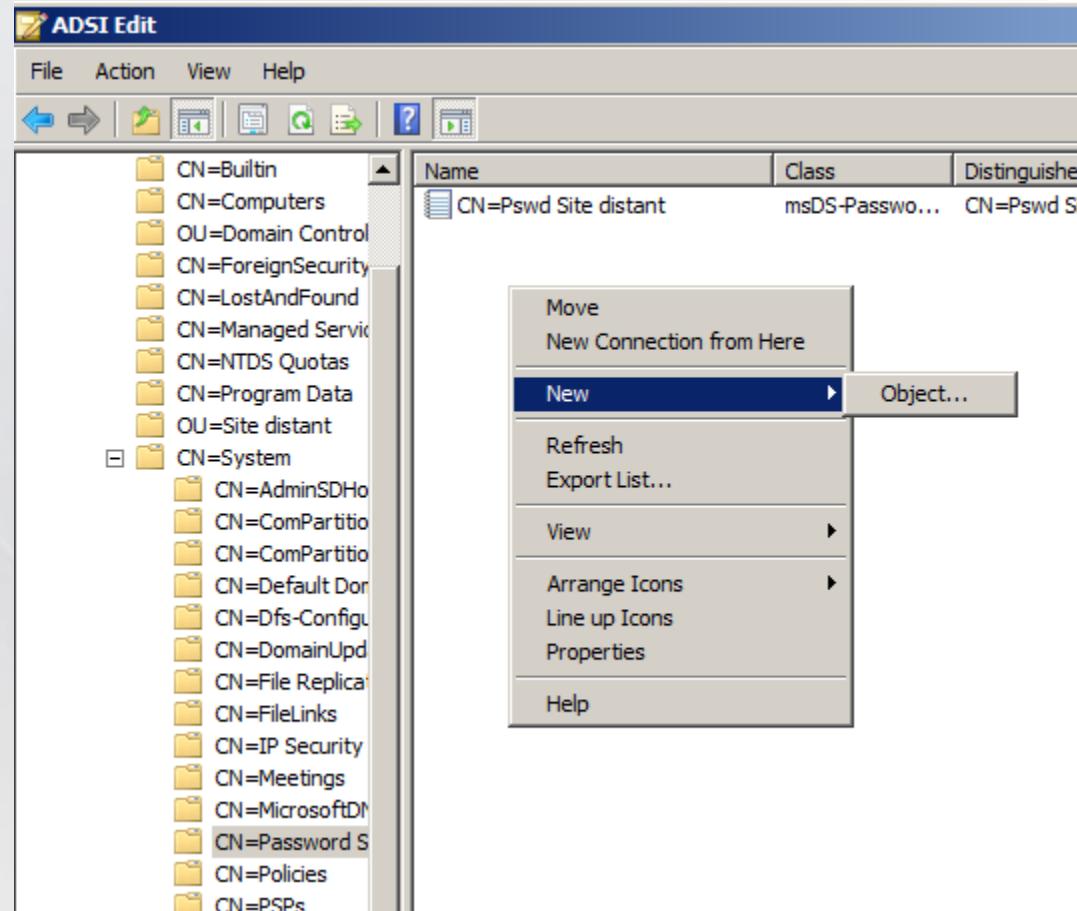


The screenshot shows the ADSI Edit interface. The left pane displays the directory structure under the Default naming context [dc=...]. The CN=System folder is selected and highlighted in blue. The right pane is a table listing various Active Directory objects:

Name	Class	Distinguished Name
CN=AdminSDHolder	container	CN=AdminSDHolder,CN=System
CN=ComPartitions	container	CN=ComPartitions,CN=System,D
CN=ComPartitionSets	container	CN=ComPartitionSets,CN=System
CN=Default Domain Policy	domainPolicy	CN=Default Domain Policy,CN=S
CN=Dfs-Configuration	dfsConfigurat...	CN=Dfs-Configuration,CN=Syste
CN=DomainUpdates	container	CN=DomainUpdates,CN=System
CN=File Replication Service	nTFRSSettings	CN=File Replication Service,CN=
CN=FileLinks	fileLinkTracking	CN=FileLinks,CN=System,DC=be
CN=IP Security	container	CN=IP Security,CN=System,DC=
CN=Meetings	container	CN=Meetings,CN=System,DC=b
CN=MicrosoftDNS	container	CN=MicrosoftDNS,CN=System,D
CN=Password Settings Contai...	msDS-Passwo...	CN=Password Settings Containe
CN=Policies	container	CN=Policies,CN=System,DC=bel
CN=PSPs	msImaging-PSPs	CN=PSPs,CN=System,DC=belgiu
CN=RAS and IAS Servers Acc...	container	CN=RAS and IAS Servers Access
CN=RpcServices	rpcContainer	CN=RpcServices,CN=System,DC=
CN=WinsockServices	container	CN=WinsockServices,CN=System
CN=WMIPolicy	container	CN=WMIPolicy,CN=System,DC=
CN=BCKUPKEY_43286ddc-90...	secret	CN=BCKUPKEY_43286ddc-9043-
CN=BCKUPKEY_f3ea78e8-72...	secret	CN=BCKUPKEY_f3ea78e8-7242-
CN=BCKUPKEY_P Secret	secret	CN=BCKUPKEY_P Secret,CN=Sy
CN=BCKUPKEY_PREFERRED ...	secret	CN=BCKUPKEY_PREFERRED Sec
CN=RID Manager\$	rIDManager	CN=RID Manager\$,CN=System,

### 3. Gestion Pswd granulaire (3)

Créer un nouvel objet  
PSO  
Compléter ensuite le  
Wizard reprenant les  
attributs obligatoires



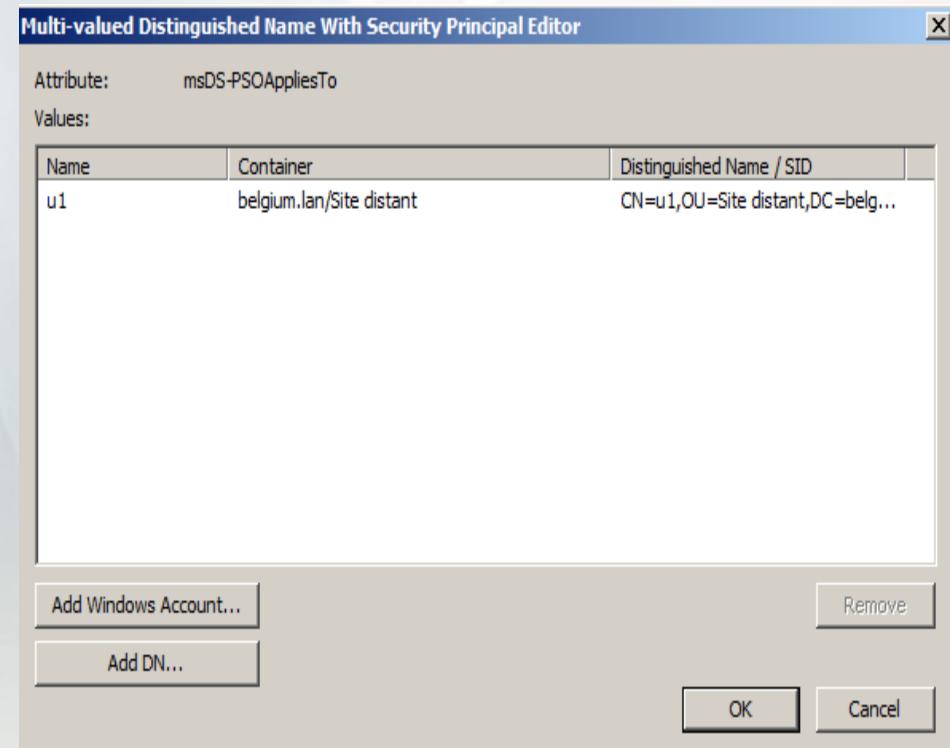
# 3. Gestion Pswd granulaire (4)

## Attributs minimums d'un objet PSO

Nom d'attribut	Description	Plage des valeurs acceptables	Exemple de valeur
msDS-PasswordSettingsPrecedence	Préférence des paramètres de mot de passe	Supérieur à 0	10
msDS-PasswordReversibleEncryptionEnabled	État de chiffrement réversible de mot de passe pour les comptes d'utilisateurs	FALSE / TRUE (Valeur recommandée : FALSE)	FALSE
msDS-PasswordHistoryLength	Longueur de l'historique du mot de passe pour les comptes d'utilisateurs	de 0 à 1 024	24
msDS-PasswordComplexityEnabled	État de complexité du mot de passe pour les comptes d'utilisateurs	FALSE / TRUE (Valeur recommandée : TRUE)	TRUE
msDS-MinimumPasswordLength	Longueur minimale du mot de passe pour les comptes d'utilisateurs	De 0 à 255	8
msDS-MinimumPasswordAge	Durée de vie minimale du mot de passe pour les comptes d'utilisateurs	(Aucune)	
		De 00:00:00 à la valeur msDS-MaximumPasswordAge	1:00:00:00 (1 jour)
		(Jamais)	
msDS-MaximumPasswordAge	Durée de vie maximale du mot de passe pour les comptes d'utilisateurs	De la valeur msDS-MinimumPasswordAge à (Jamais)	42:00:00 (42 jours)
		La valeur de msDS-MaximumPasswordAge ne peut pas être définie à zéro	
msDS-LockoutThreshold	Seuil de verrouillage pour le verrouillage des comptes d'utilisateurs	De 0 à 65 535	10
msDS-LockoutObservationWindow	Fenêtre d'observation pour le verrouillage des comptes d'utilisateurs	(Aucune)	
		De 00:00:01 à la valeur msDS-LockoutDuration	0:00:30:00 (30 minutes)
		(Jamais)	
msDS-LockoutDuration	Durée de verrouillage pour les comptes d'utilisateurs verrouillés	0:00:30:00 (30 minutes)	
		De la valeur msDS-LockoutObservationWindow à (Jamais)	
		(Aucune)	
msDS-PSOAppliesTo	Liens jusqu'aux objets auxquels cet objet PSO s'applique (lien avant)	0 ou plusieurs noms uniques d'utilisateurs ou de groupes de sécurité globaux	

### 3. Gestion Pswd granulaire (5)

- Pour appliquer un objet PSO à un groupe ou à un utilisateur
  - ADSIEdit -> Propriétés de l'objet PSO -> Onglet Attribute Editor -> Editer l'attribut msDS-PSOAppliesTo
  - AD users&computers -> System (contener) -> Password settings Container -> Propriétés de l'objet PSO -> Onglet Attribute Editor -> Editer l'attribut msDS-PSOAppliesTo



## 4. Corbeille AD (1)

- Depuis Win2k8R2, une corbeille pour les objets AD est apparue
- Avantage : facilité de restaurer les objets supprimés
- En Win2k8R2, utilisation via ldp.exe ou PowerShell
- En Win2k12, GUI via le centre d'administration AD
- Attention, les niveaux de fonctionnements (forêt et domaine) doivent être en Win2k8R2

## 4. Corbeille AD (2)

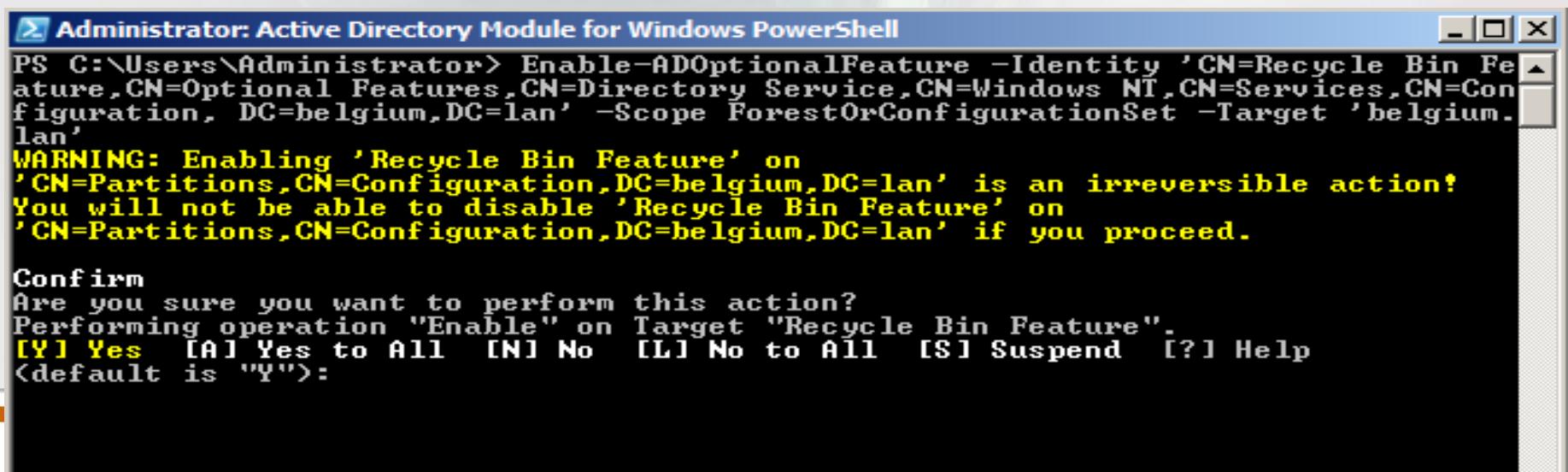
- Pré-requis
  - Préparer la forêt : adprep /forestprep (sur le SM)
  - Préparer le domaine : adprep /domainprep /gpprep (sur le IM)
  - Si RODC → adprep /rodcprep
  - les niveaux de fonctionnements (forêt et domaine) doivent être en Win2k8R2

## 4. Corbeille AD (3)

- Activation de la corbeille

- Via PS et le module Active Directory

```
Enable-ADOptionalFeature -Identity 'CN=Recycle Bin Feature,CN=Optional Features,CN=Directory Service,CN=Windows NT,CN=Services,CN=Configuration, DC=belgium,DC=lan' -Scope ForestOrConfigurationSet -Target 'belgium.lan'
```



```
Administrator: Active Directory Module for Windows PowerShell
PS C:\Users\Administrator> Enable-ADOptionalFeature -Identity 'CN=Recycle Bin Feature,CN=Optional Features,CN=Directory Service,CN=Windows NT,CN=Services,CN=Configuration, DC=belgium,DC=lan' -Scope ForestOrConfigurationSet -Target 'belgium.lan'
WARNING: Enabling 'Recycle Bin Feature' on
'CN=Partitions,CN=Configuration,DC=belgium,DC=lan' is an irreversible action!
You will not be able to disable 'Recycle Bin Feature' on
'CN=Partitions,CN=Configuration,DC=belgium,DC=lan' if you proceed.

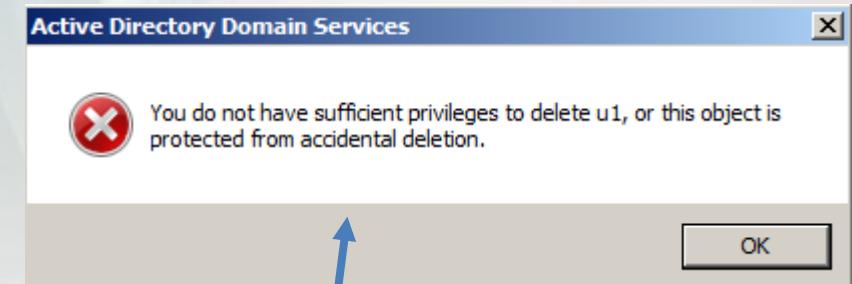
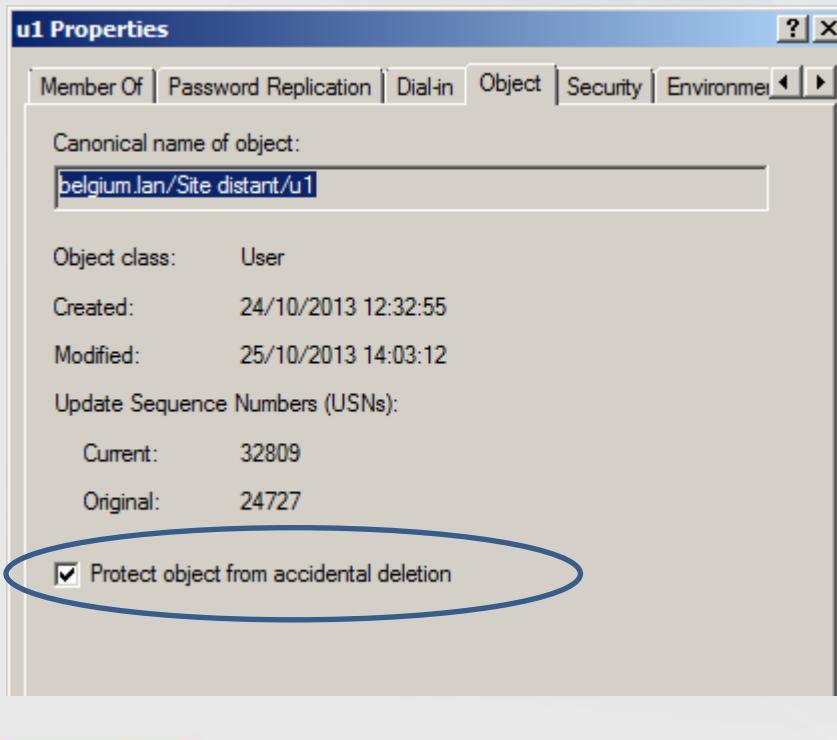
Confirm
Are you sure you want to perform this action?
Performing operation "Enable" on Target "Recycle Bin Feature".
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help
<default is "Y">:
```

## 4. Corbeille AD (4)

- Restauration d'un objet supprimé
  - Get-adobject –Filter {displayName=« Denis »} –includeDeletedObjects | Restore-ADObject
- Outils : Object Restore for Active Directory (sur [www.quest.com](http://www.quest.com))

## 5. Protection des objets AD contre l'effacement

Dans l'onglet Object des objets de l'AD → Cocher Protect object from...



En cas de suppression