2009

ALKA SA

Raphaël Roose

[PRÉSENTATION SERVER 2008]

Sommaire

Les différentes versions

Specification	Web	Standard	Enterprise	Datacenter
X86 Sockets	4	4	8	32
X64 Sockets	4	4	8	64
IA64 Sockets	●	●	●	●
X86 RAM	4 GB	4 GB	64 GB	64 GB
X64 RAM	32 GB	32 GB	2 TB	2 TB
IA64 RAM	●	●	●	●
Hot Add Memory	○	○	●	●
Failover Cluster Nodes (Nodes)	○	○	16	16
Fault Tolerance Memory Sync	●	●	○	○
Cross-File Replication (DFS-R)	○	○	●	●
Network Access Connections (RRAS)	○	250	Unlimited	Unlimited
Network Access Connections (IAS)	○	50	Unlimited	Unlimited
Terminal Services Gateway	○	250	Unlimited	Unlimited
Virtual Image Use Rights	Unlimited	1	4	Unlimited
Remote Desktop Admin Connections	2	2	2	2

Estimation des prix :

Web ±400 €

Standard ±800 €

Enterprise ±4000€

Il y a toujours également une version de **SBS** limité à 75 utilisateurs, sans terminal serveur, sans trust avec un maximum de 2 serveurs.

Nouveauté de cette version 2008, l'apparition d'une **EBS** limité à 300 utilisateurs avec 3 licences serveurs pour mettre en place un Domain controler, serveur mail, un serveur sécurité avec ISA Server et Anti-spam Exchange.

Note :

Au niveau de la virtualisation, il faut retenir que la version standard ne permet que 4 OS Virtuel et Hyper-V ne fonctionne qu'en 64 bit. Le système Hyper-V entraine un surplus de coût au niveau des licences.

Le système d'activation

Deux grands types selon la structure de la société, le MAK (Multiple Activation Key) et le KMS (Volume License Keys).

MAK (Multiple Activation Key)

On doit encore introduire la clé manuellement mais la même clé peut servir pour un ensemble de machines. On achète donc une clé pour X machines (Vista ou Seven) ou pour X Serveurs 2008. Ce qui permet une meilleure gestion des licences. Les machines clientes s'enregistrent via une connexion internet. Les administrateurs peuvent voir les MAK dans le portail en ligne approprié (MVLS, eOpen ou MSDN). Les administrateurs peuvent voir le nombre d'activations par rapport à chaque clé et obtenir un rapport sur le nombre de systèmes activés qui sont gérés. Ce nombre augmente à mesure que les systèmes sont reconfigurés, et il convient de le surveiller pour veiller à ce qu'il reste suffisamment d'activations pour prendre en charge l'organisation.

KMS (Volume License Keys)

Le KMS est un service qui tourne sur un serveur hôte. Les machines s'authentifient directement à lui d'une manière automatique et transparente. Le poste client n'a donc pas besoin d'une connexion Internet car c'est le serveur qui procèdera à son activation. Par défaut, des clients en volume Windows Vista convenablement configurés recherchent un hôte KMS en utilisant des requêtes DNS, sauf s'ils sont préconfigurés avec l'adresse d'un ou plusieurs hôtes KMS. Les systèmes activés par un hôte KMS renouvellent leurs clés d'activation à des intervalles de sept jours en utilisation normale,

fonctionnant jusqu'à 180 jours (ou 210 jours lorsque la période de grâce de 30 jours est prise en compte) sans renouvellement lorsqu'ils sont incapables de contacter un hôte KMS. Cette approche permet aux systèmes itinérants de continuer à fonctionner entièrement pendant un maximum de sept mois sans nécessiter de contact avec un hôte KMS.

Méthodes d'administration

Les consoles

Les consoles d'administration qui fonctionnent grâce à l'ouverture de port multiples comme le très dangereux 445. Ces ports ne doivent être ouverts qu'en réseau local.

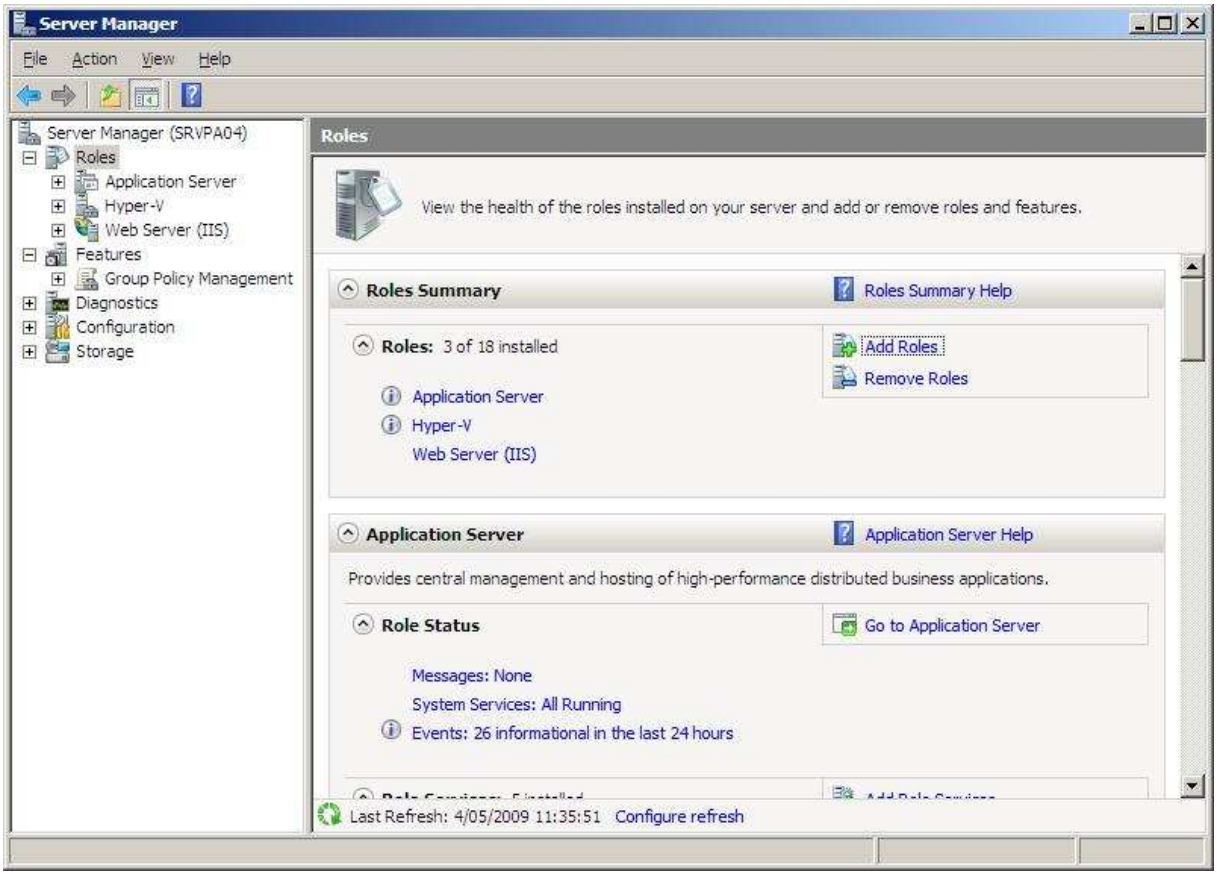
Il faut les installer sur le serveur ou sur le client vista (minimum SP1) grâce au Pack RSAT (Remote Server Administration Tools for Windows Vista).

Remote Desktop

Prise de contrôle à distance suivis d'une utilisation de console ou ligne de commande sur le serveur. Nouveauté de la version 2008, toutes les sessions fonctionnent en mode console. Il y a une session unique par utilisateur ce qui réduit le problème de session non fermée. On est toujours limité à 2 connexions mais la politique est beaucoup plus souple car c'est deux connexions sortantes. Il n'y a pas de limitation en interne.

Pour rappel, le port est 3389 et la commande pour se connecter directement via un Shell est **« mstsc /v :NomDuHote /admin»**

Roles + Features

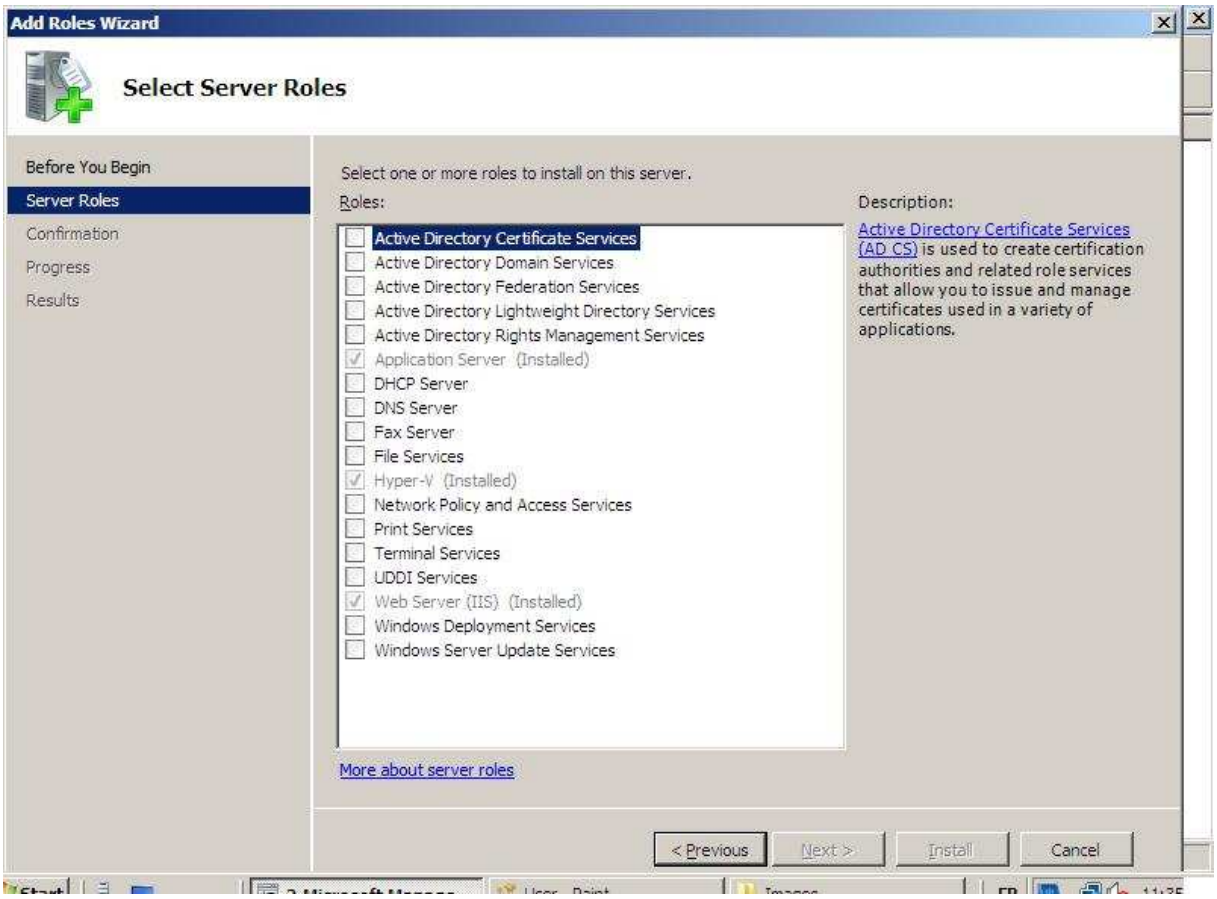


L'outil principal pour la gestion des rôles et des features se réalise via le « Server Manager » qui reprend beaucoup d'informations sur le système. Il met à disposition également de nombreux outils qui permettent de réaliser les tâches quotidiennes.

La différence entre les rôles et les features est très relatif… On remarque par exemple le failover Clustering dans les features. C'est lui qui permet le clustering.

Le Server Manager de Windows Server 2008 prend en charge les rôles Active Directory Certificates Services (AD CS), Active Directory Domain Services (AD DS), Active Directory Federation Services (AD FS), Active Directory Lightweight Directory Services (AD LDS), Active Directory Rights Management Services (AD RMS), Application Server, DHCP Server, DNS Server, Fax Server, File Services, Network Policy and Access Services, Windows Internal DataBase , Print Services, Terminal Services, UDDI Services, Web Server, Windows Deployment Services et enfin, Windows Sharepoint Services. Bien évidement, par défaut aucun rôle n'est installé.

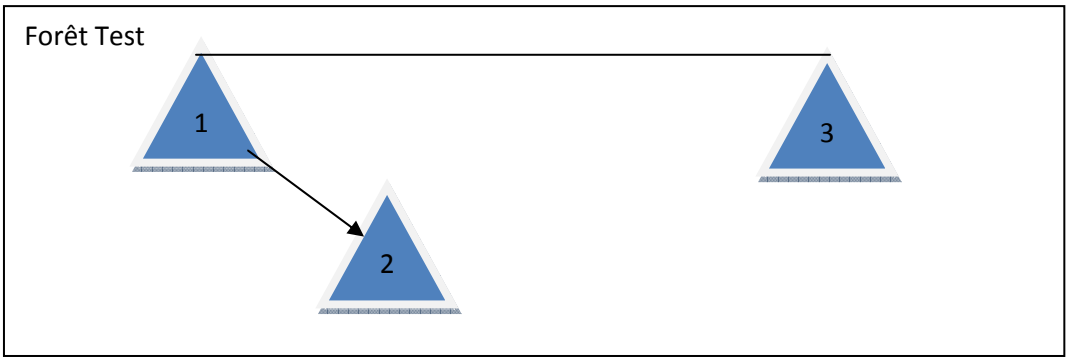
Windows Internal DataBase fonctionne uniquement avec des produits de Micosoft. Par exemple, lors de l'installation de WSUS, il installera ce rôle ce qui est loin d'être l'idéal. Il vaut mieux installer préalablement la version Express de SQL 2008 pour pouvoir supporter les programmes tiers et n'avoir qu'une seule instance.



Gestion de l'Active Directory (AD)

Rappel

La création du premier domain controller crée automatique une forêt et un arbre. Les serveurs suivants pourront donc rejoindre cette forêt et cet arbre. Ils pourront également créer d'autres arbres dans cette forêt. Notez que l'administrateur de la racine (du premier domain controller) peut tout faire sur l'ensemble de la forêt.



1. Domain Controler (Racine)
2. Domain enfant
3. Domain d'un autre arbre

Constitution idéal et minimal pour une infrastructure professionnelle. Deux Serveurs qui jouent le rôle de domaine Controller, de global catalog et de DNS. La synchronisation entre ces deux serveurs fonctionne d'une manière incrémentale.

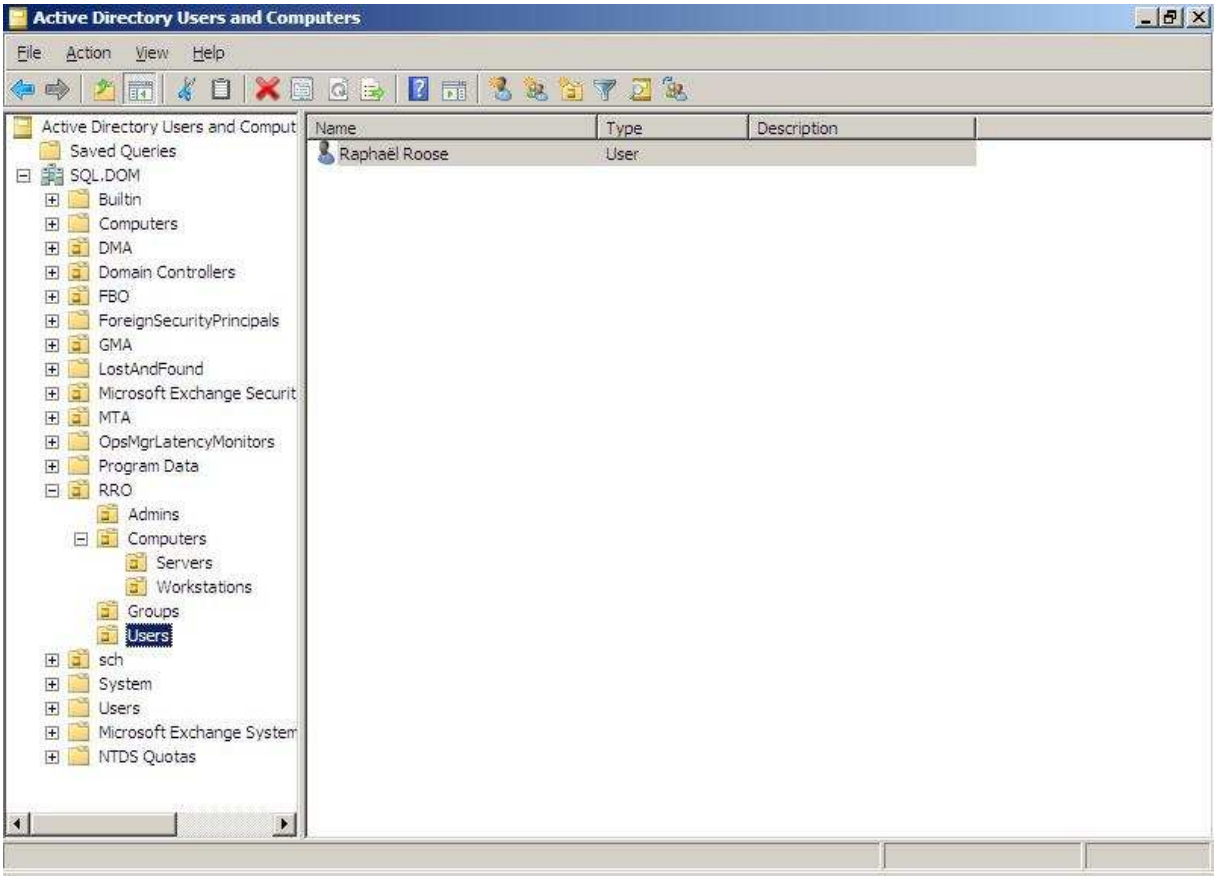
Organization Unit (O.U)

Une OU sert principalement à structure l'active directory en rendant de grosse structure plus visible mais elle sert aussi à appliquer des groupes Policy.

Un exemple d'une bonne structure :

Belgique \ Admins
\Users
\Computers \ Servers
\Workstations

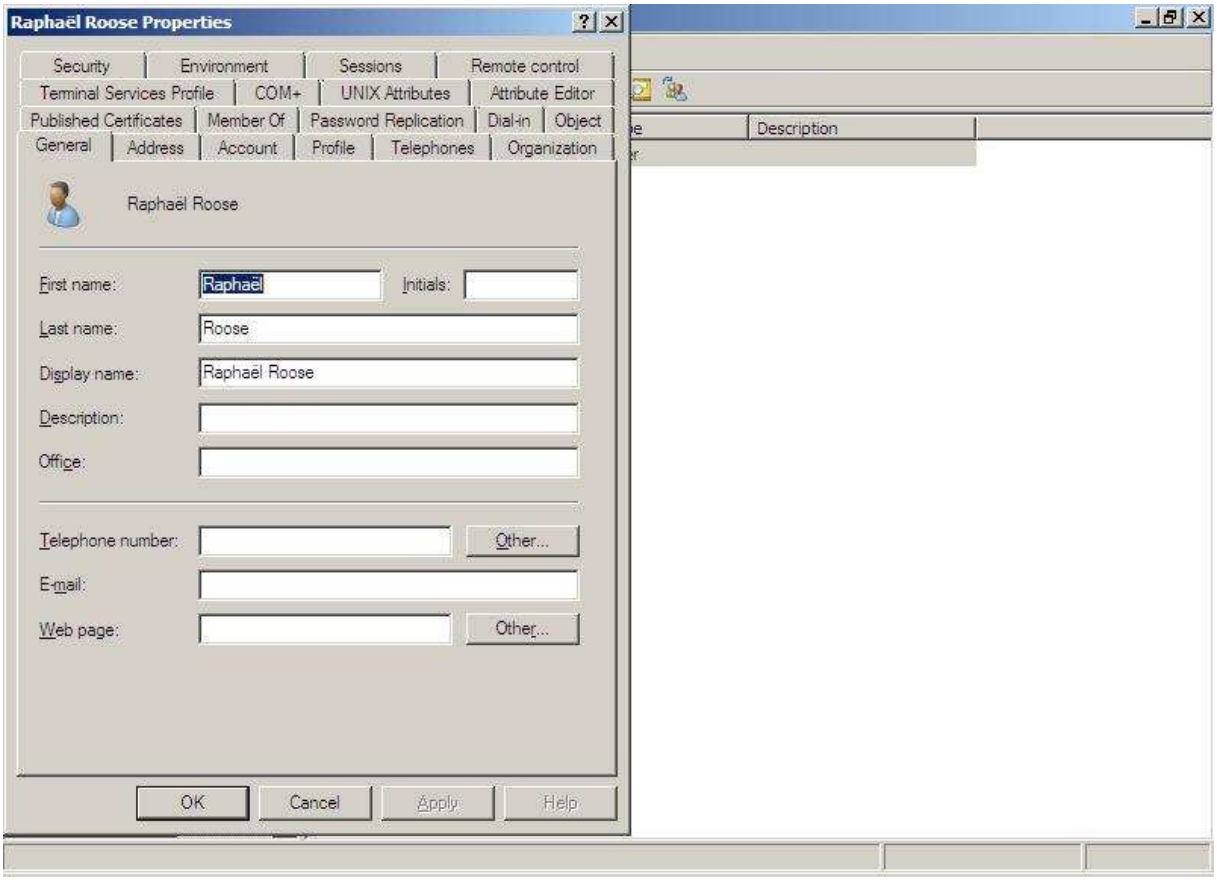
\Groupes



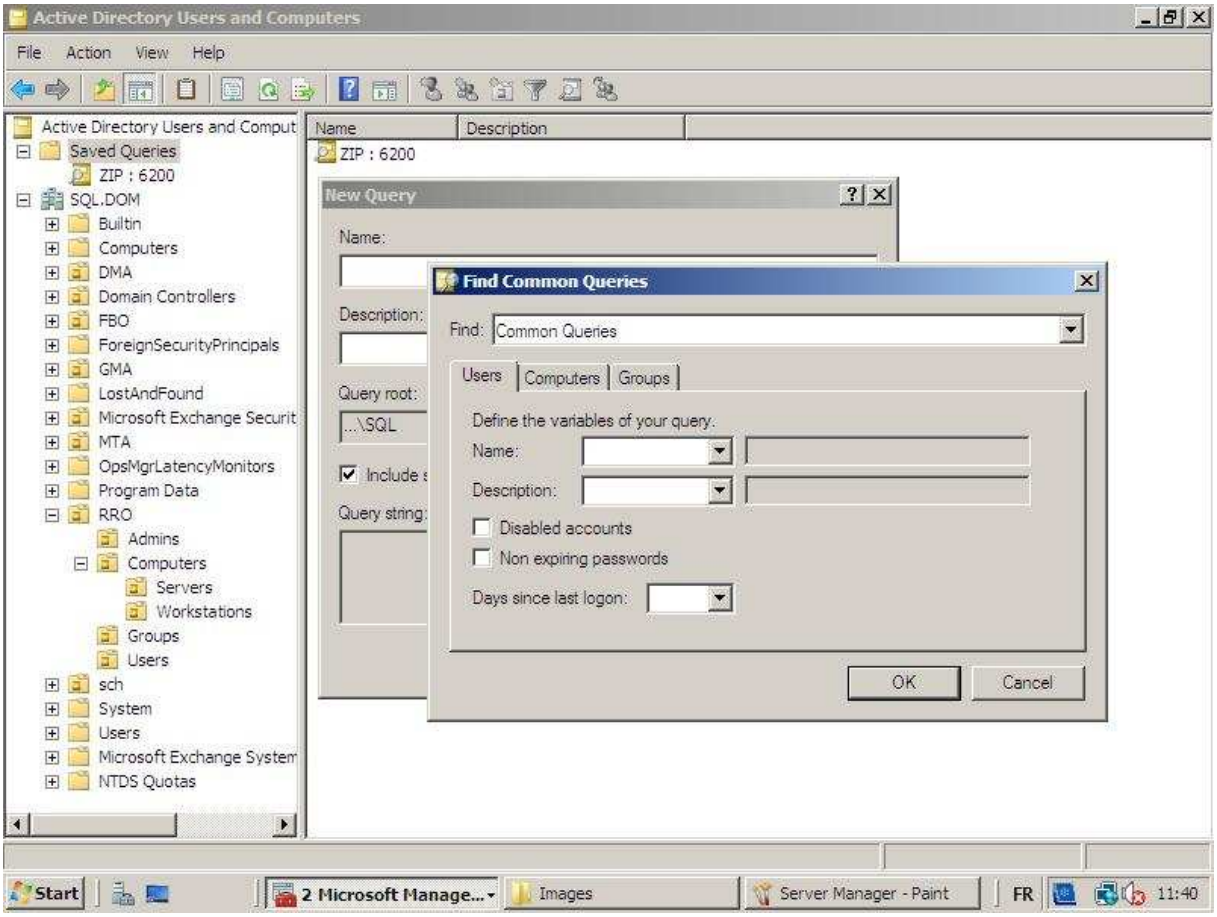
Pour une meilleure visibilité et pour avoir accès à l'ensemble des options, il est conseillé de cocher dans View l'option advanced et voir en tant que container.

Les différents objets de l'active directory

Users



Les **users** représentent les comptes des utilisateurs mais aussi des services tiers (Exemple : BackupExec) . Il est conseillé de réaliser un compte par utilisateur, un compte par service tiers, deux comptes pour les administrateurs (Un simple et un admin). Notez qu'il y a possibilité de créer des requêtes sur les utilisateurs. Pour ce faire, il faut aller dans Saved Queries → News Queries.



InetOrgPerson

L'inetOrgPerson est identique a un user classique de Windows et présente les mêmes options mais ce type d'objet est plus compatible avec les autres annuaires comme ceux de Novel, Mac, etc.
Il est donc plus que conseillé de créer ce type de compte dans les réseaux hétérogènes.

Computers

Représente une machine ou un serveur. Il s'ajoute automatiquement dans l'active directory lors de l'ajout dans le domaine. Par défaut, ils tombent tous dans le container Computers mais il y a possibilité de les faire tomber ailleurs via une ligne de commande (voir astuces).

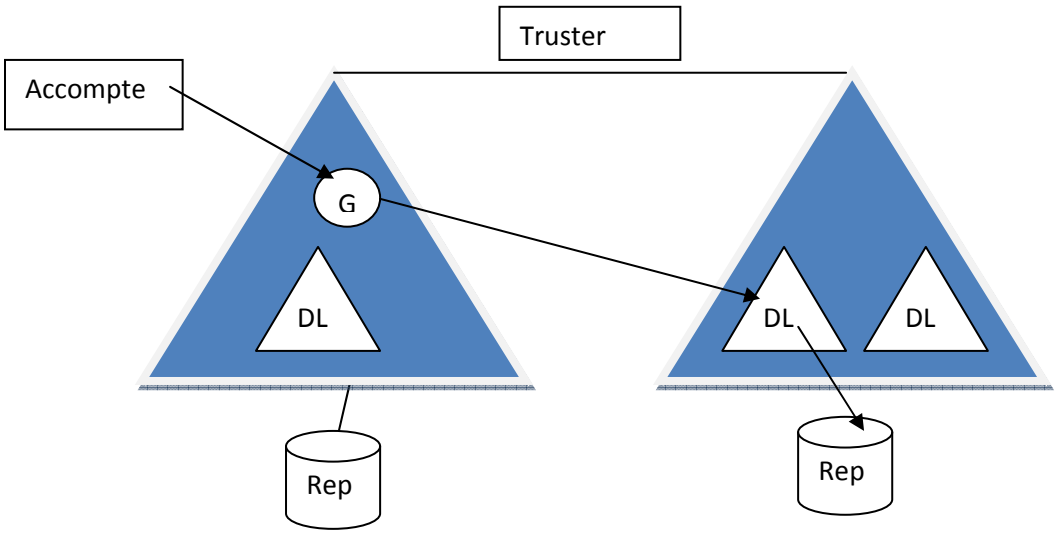
Les groupes

Il y a deux types de groupe et trois types de scope.

Le type **distribution** qui n'est important que dans les organisations qui possède Exchange.

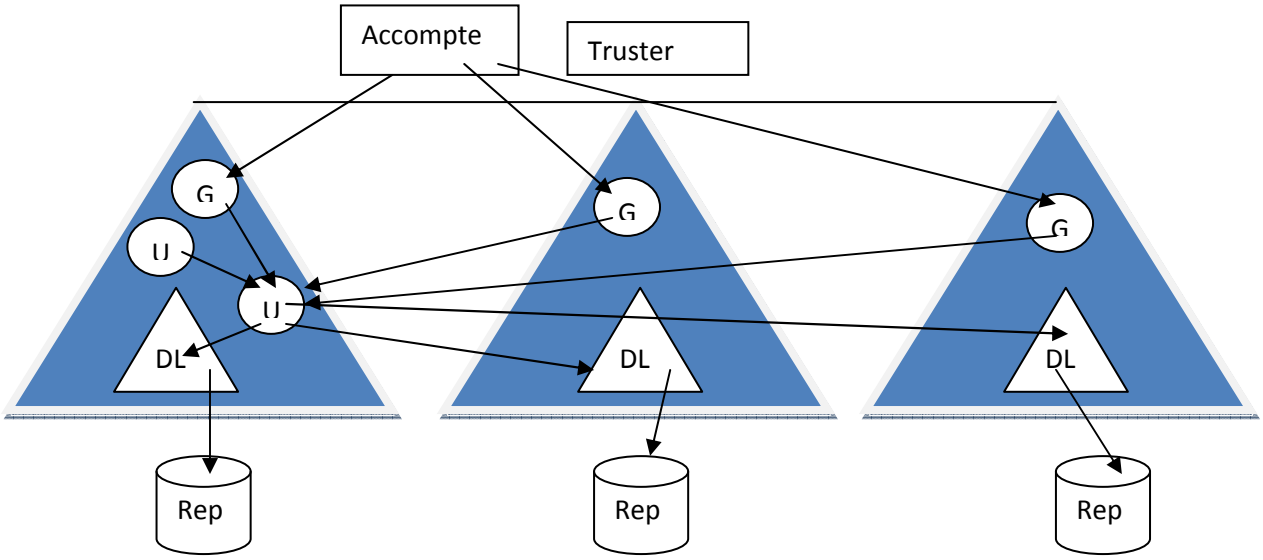
Le type **Security** qui sert à appliquer des permissions. Notez que le type Security fait automatiquement le même qu'un type distribution.

Les scopes : Domain local (permission), Global (réunir des users), universal (pour plusieurs arbres).

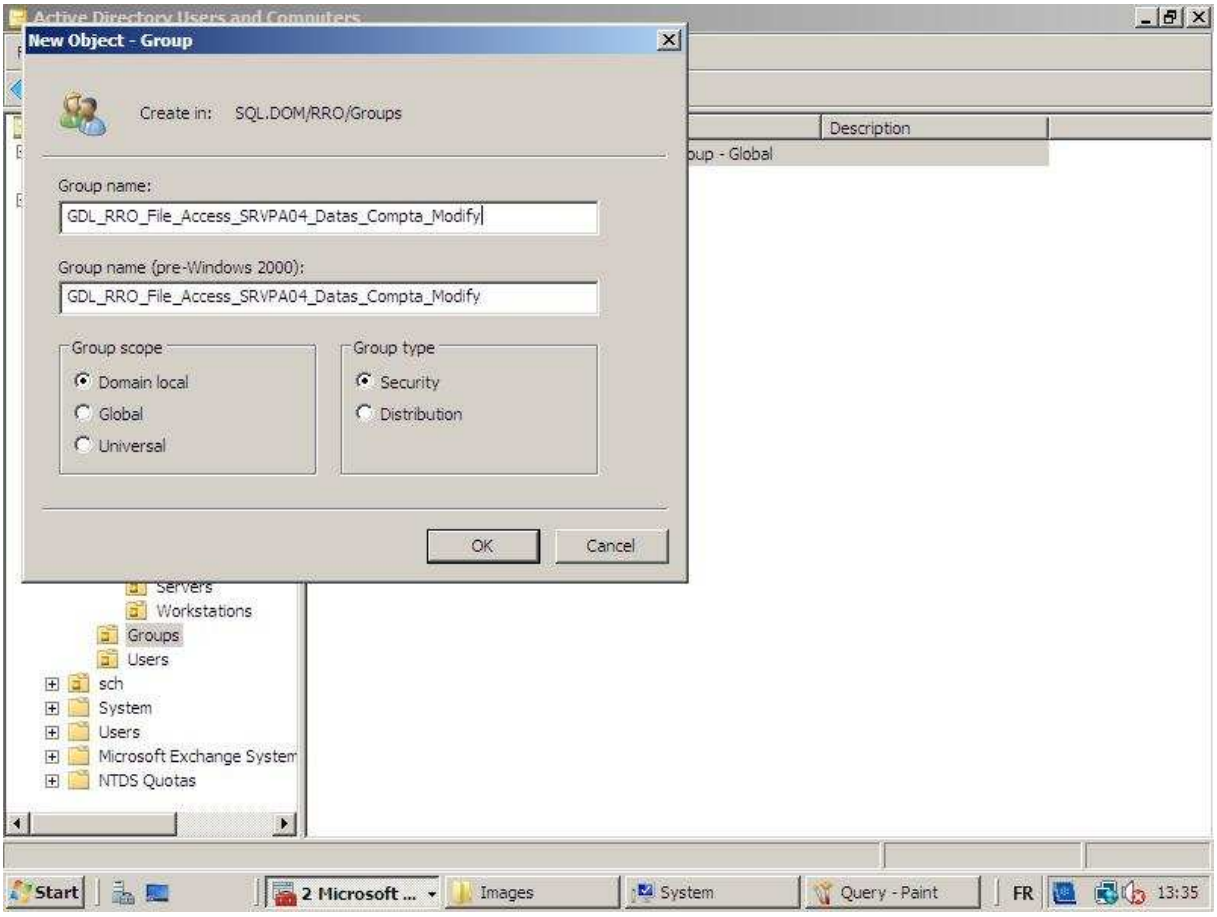


Microsoft recommande pour des raisons de sécurité de toujours mettre des accomptes dans un Global et ensuite d'appliquer celui-ci dans un domaine local. Vous ajoutez de cette manière une couche de sécurité.

Toujours pour une question de sécurité, vous devez créer un DL par ressources et par type de ressource.



L'universal est utilisé pour les grandes forêts ou la gestion de la sécurité doit être plus poussée.



Permission dans l'Active Directory

Les Bultin contiennent tous les groupes de domaines locaux pour attribuer des droits aux utilisateurs ayant un rôle administratif.

Les plus utilisés :

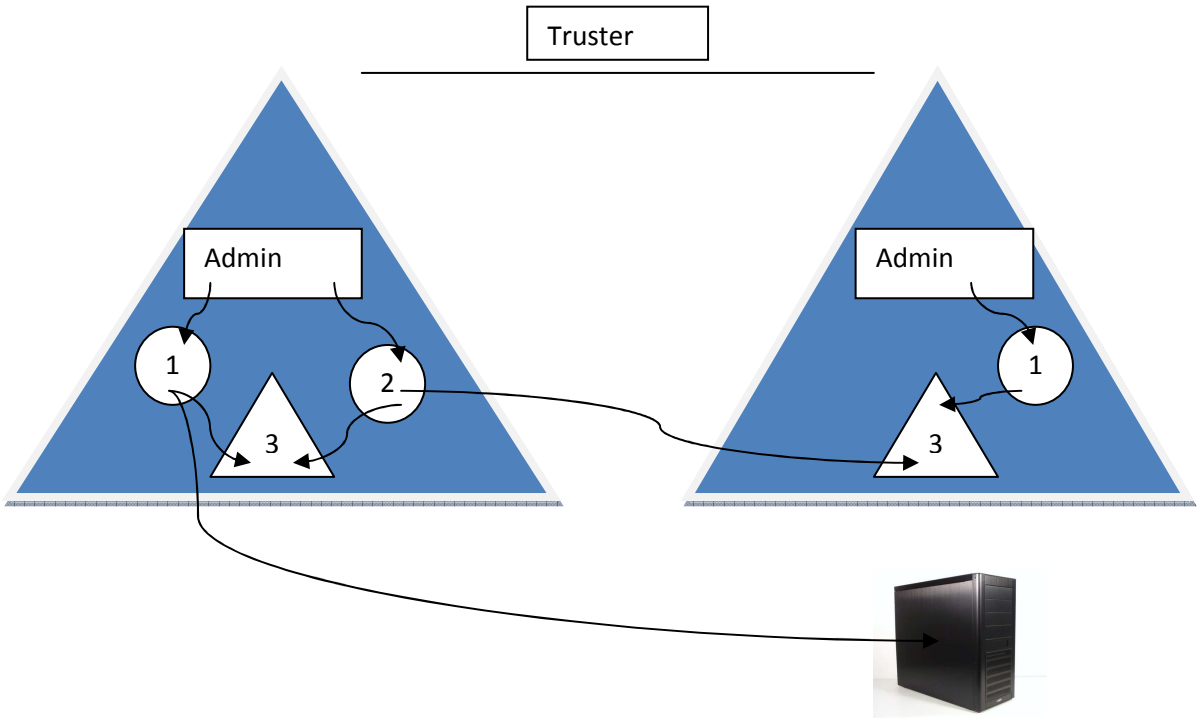
Entreprise admins : Droit sur l'ensemble de la forêt

Schema admins : Responsable de l'AD

Acompte operators : Création des groupes, users.

Server operators : Opération de maintenance mais aucun accès à l'AD.

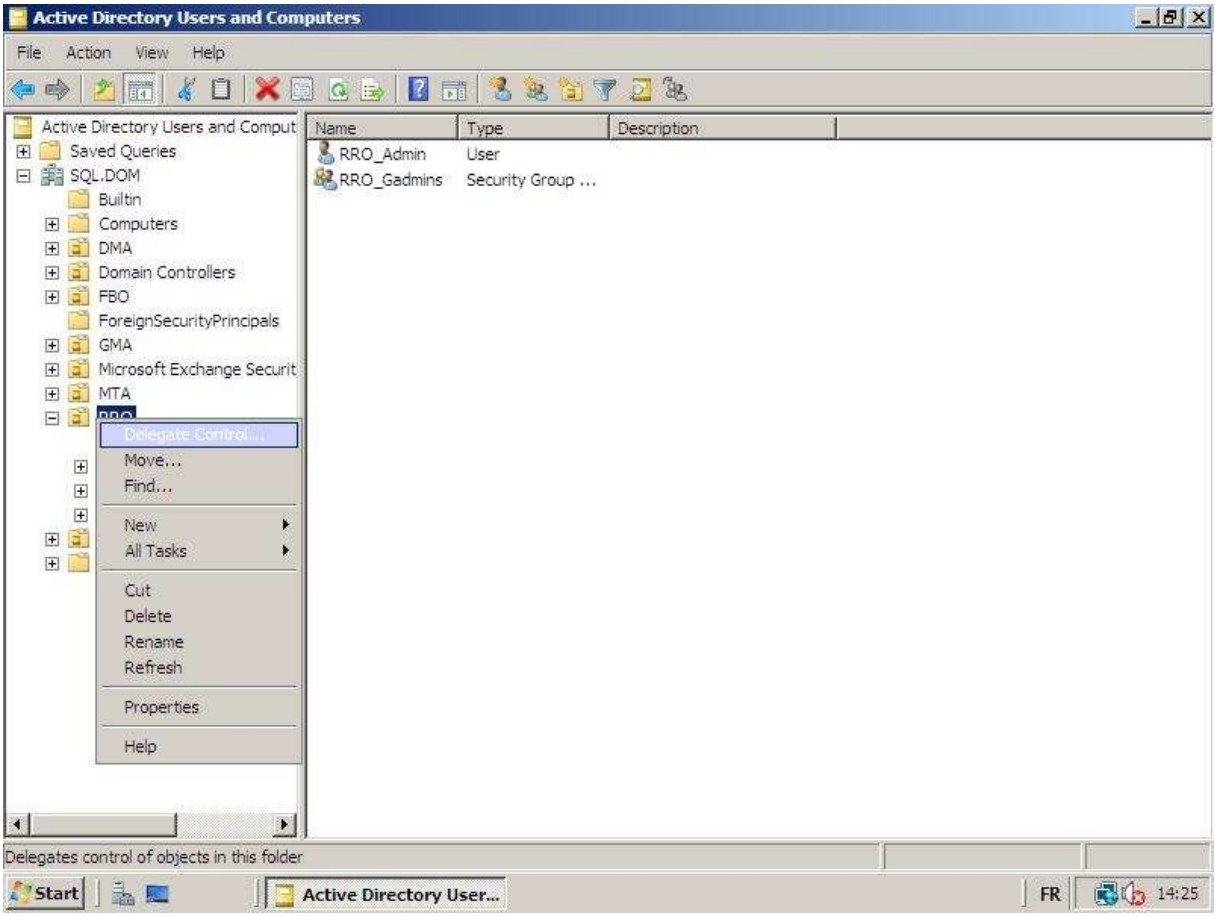
Configuration par défaut dans une forêt.



1. Domain Admin (groupe global)
2. Entreprise admin (Groupe universel)
3. Administrators (Domain Local)

Délégation des droits AD

Comme son nom l'indique ceci permet de déléguer des rôles dans l'active directory. Une délégation peut se faire sur une OU, un type d'objet, une tâche, une propriété d'un objet. Pour une question de sécurité, les OU doivent être bien structuré et les personnes qui auront des rôles déléguer ne devront jamais avoir la possibilité de s'en ajouter des nouveaux.

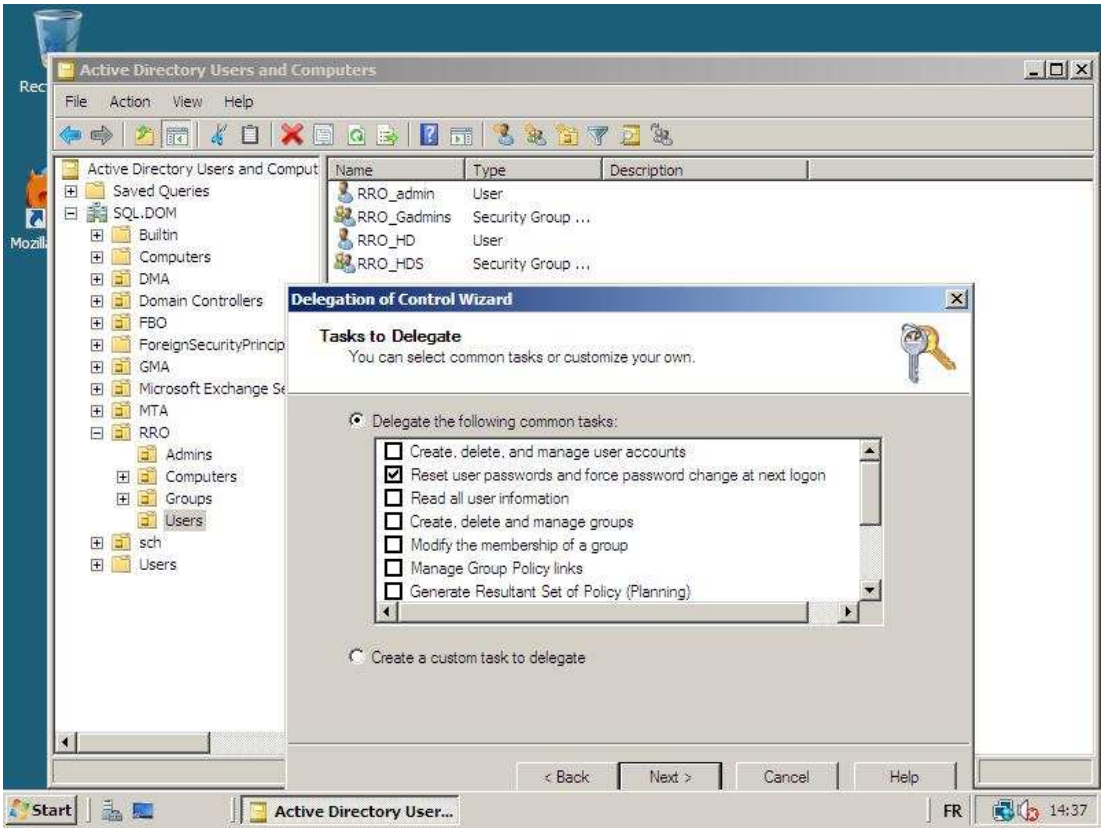


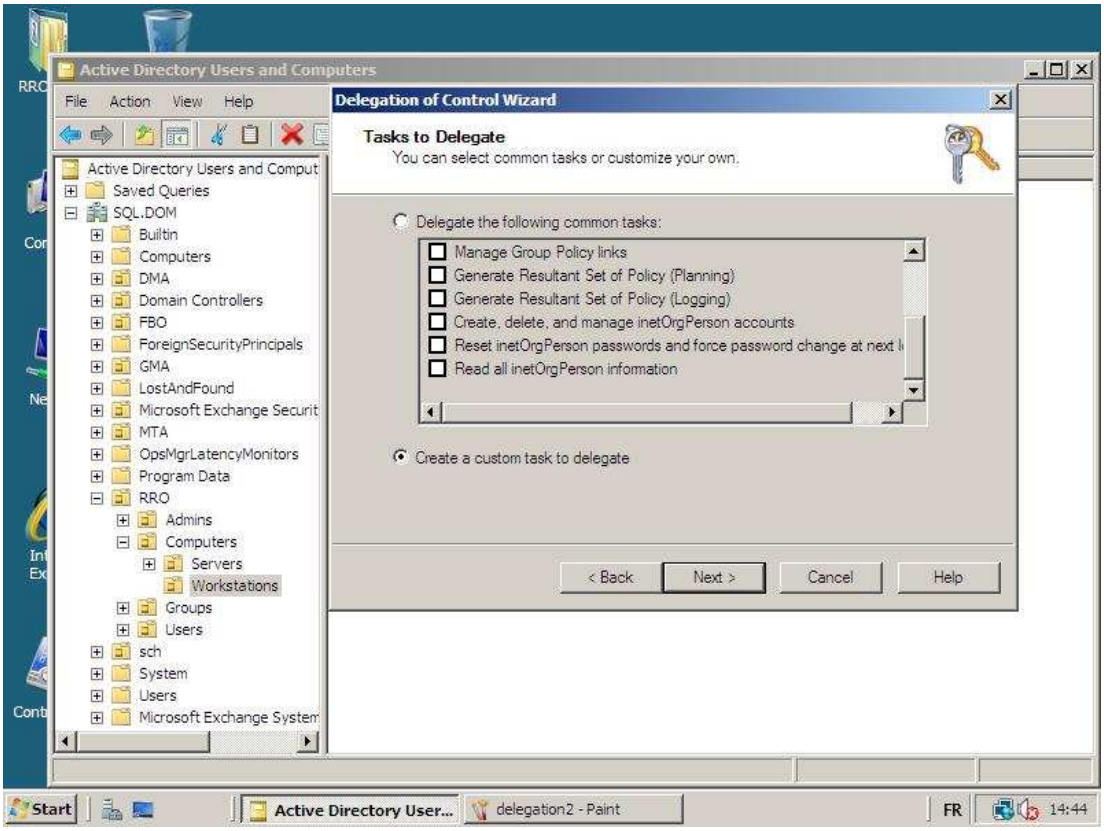
Exemple de bonne OU :

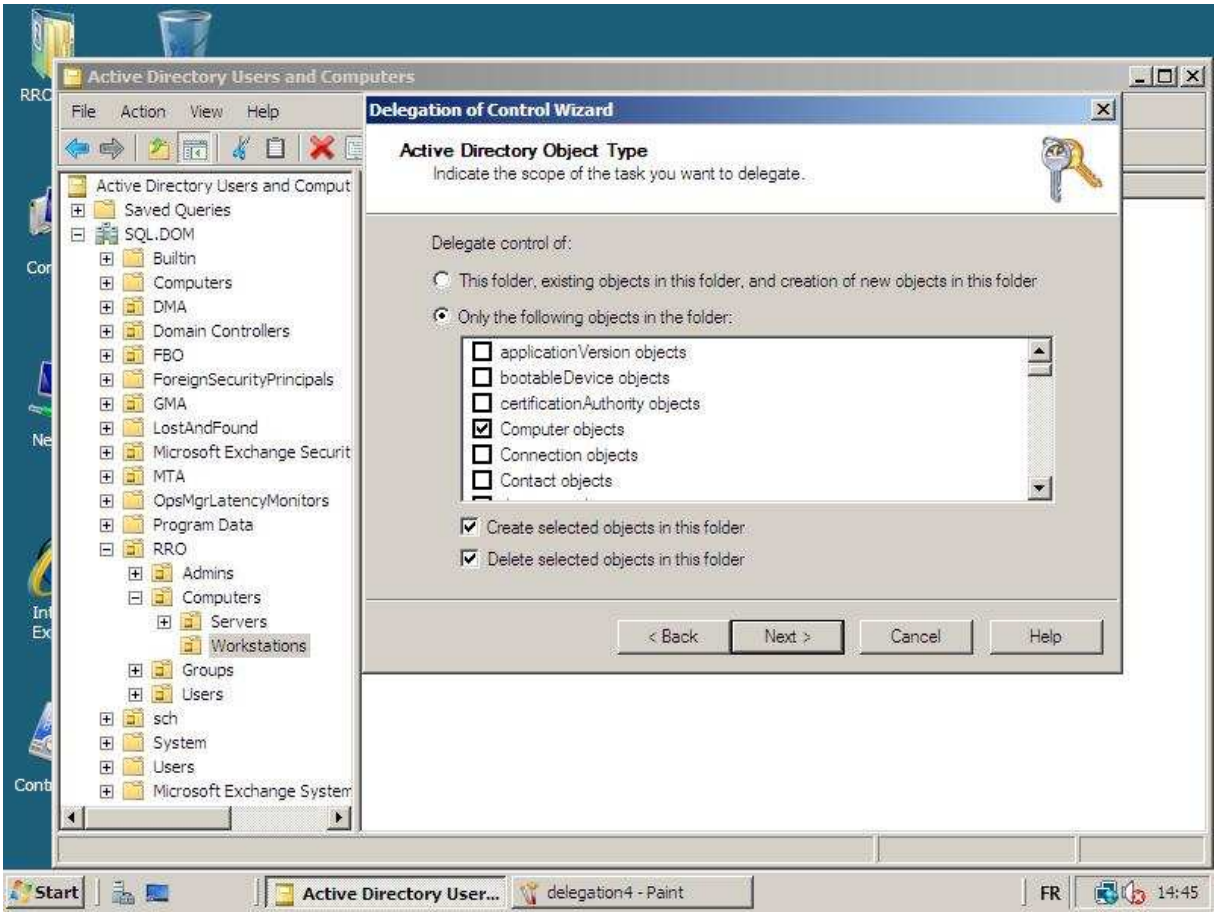
Belgique \ Admins
\Users
\Computers \ Servers
\Workstations

\Groupes

Cas pratique : Imaginons qu'on veut permettre à l'équipe Help Desk de faire un reset des Passwords des utilisateurs et qu'ils ont la possibilité d'ajouter des machines au domaine. On va donc créer un groupe global HelpDesk qui recevra la délégation sur l'OU User et l'OU Workstation.


Active Directory Users and Computers
File Action View Help
Active Directory Users and Comput
Saved Queries
SQL.DOM
Builtin
Computers
DMA
Domain Controllers
FBO
ForeignSecurityPrincip
GMA
Microsoft Exchange Se
MTA
RRO
Admins
Computers
Groups
Users
sch
Users
Name Type Description
RRO_admin User
RRO_Gadmins Security Group ...
RRO_HD User
RRO_HDS Security Group ...
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
Start
Active Directory User...
FR
14:37


Active Directory Users and Computers
File Action View Help
Delegation of Control Wizard
Tasks to Delegate
You can select common tasks or customize your own.
Delegate the following common tasks:
Manage Group Policy links
Generate Resultant Set of Policy (Planning)
Generate Resultant Set of Policy (Logging)
Create, delete, and manage inetOrgPerson accounts
Reset inetOrgPerson passwords and force password change at next l
Read all inetOrgPerson information
Create a custom task to delegate
< Back
Next >
Cancel
Help
Active Directory Users and Comput
Saved Queries
SQL.DOM
Builtin
Computers
DMA
Domain Controllers
FBO
ForeignSecurityPrincipals
GMA
LostAndFound
Microsoft Exchange Securit
MTA
OpsMgrLatencyMonitors
Program Data
RRO
Admins
Computers
Servers
Workstations
Groups
Users
sch
System
Users
Microsoft Exchange System
Start
Active Directory User...
delegation2 - Paint
FR
14:44


Active Directory Users and Computers
File Action View Help
Delegation of Control Wizard
Active Directory Object Type
Indicate the scope of the task you want to delegate.
Delegate control of:
This folder, existing objects in this folder, and creation of new objects in this folder
Only the following objects in the folder:
applicationVersion objects
bootableDevice objects
certificationAuthority objects
Computer objects
Connection objects
Contact objects
Create selected objects in this folder
Delete selected objects in this folder
< Back
Next >
Cancel
Help
Active Directory Users and Comput
Saved Queries
SQL.DOM
Builtin
Computers
DMA
Domain Controllers
FBO
ForeignSecurityPrincipals
GMA
LostAndFound
Microsoft Exchange Securit
MTA
OpsMgrLatencyMonitors
Program Data
RRO
Admins
Computers
Servers
Workstations
Groups
Users
sch
System
Users
Microsoft Exchange System
Start
Active Directory User...
delegation4 - Paint
FR
14:45

Accès aux ressources

L'accès aux ressources se configure en trois étapes : Le partage, la publication et la permission.

Le partage

Pour réaliser un partage, il suffit de cliquer sur propriétée et d'aller dans l'onglet share. On peut ensuite configurer le nom de celui-ci ainsi que ses permissions que nous verrons plus loin. Vous pouvez bien entendu créer des partages invisibles par les utilisateurs en ajoutant le signe $ à la fin du nom de partage. Ce genre de partage est très utile pour créer des répertoires contenant des sources, des packages d'installations, etc.

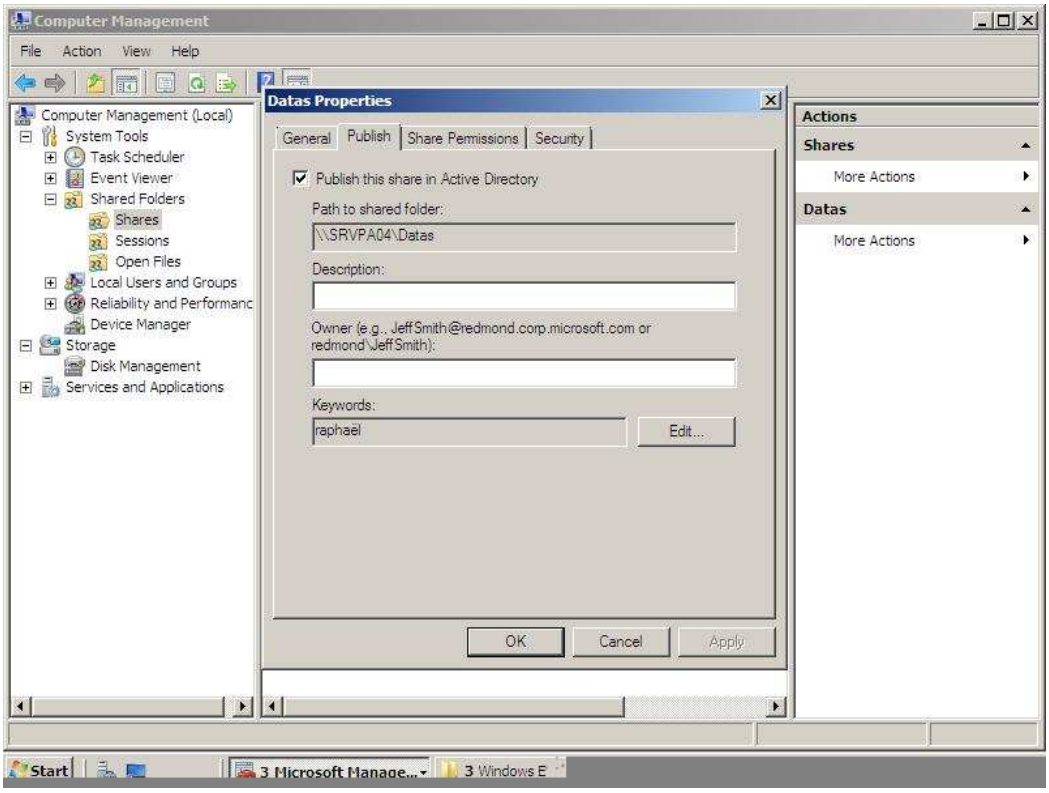
Notez qu'on voit toujours l'ensemble des partages via le computer management.

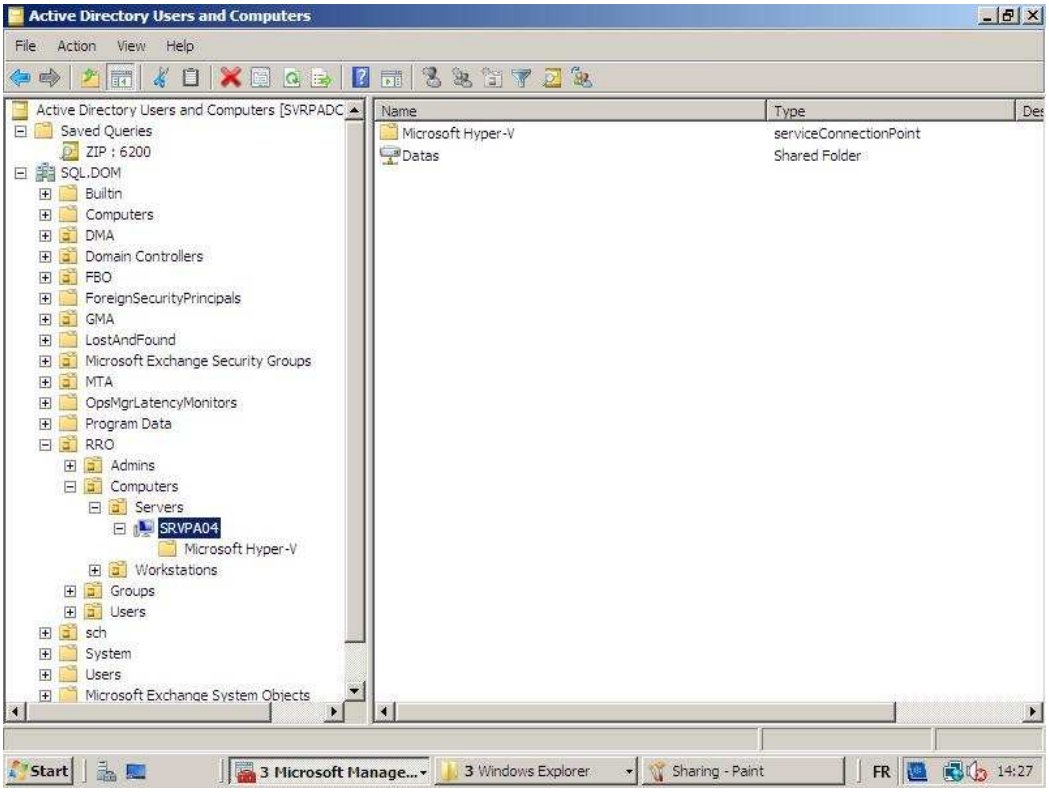
La publication

La publication représente la possibilité de rendre facilement un partage accessible à un utilisateur. Soit via un mapping, soit via un raccourci. Cette procédure se réalise souvent via un script de démarrage ou via une policy.

Vous pouvez également publier le partage dans l'active directory. On peut voir rapidement et d'une manière centraliser les partages sur une machine ou surtout sur les serveurs.

Pour ce faire, il faut aller dans le computer management et cliquer sur publish dans les propriétés du partage.


Computer Management
File Action View Help
Computer Management (Local)
System Tools
Task Scheduler
Event Viewer
Shared Folders
Shares
Sessions
Open Files
Local Users and Groups
Reliability and Performanc
Device Manager
Storage
Disk Management
Services and Applications
Datas Properties
General Publish Share Permissions Security
Publish this share in Active Directory
Path to shared folder:
\\SRVPA04\Datas
Description:
Owner (e.g., JeffSmith@redmond.corp.microsoft.com or redmond\JeffSmith):
Keywords:
raphael
Edit...
OK Cancel Apply
Actions
Shares
More Actions
Datas
More Actions
Start
3 Microsoft Manage...
3 Windows E


Active Directory Users and Computers
File Action View Help
Active Directory Users and Computers [SVRPADC
Saved Queries
ZIP : 6200
SQL.DOM
Builtin
Computers
DMA
Domain Controllers
FBO
ForeignSecurityPrincipals
GMA
LostAndFound
Microsoft Exchange Security Groups
MTA
OpsMgrLatencyMonitors
Program Data
RRO
Admins
Computers
Servers
SRVPA04
Microsoft Hyper-V
Workstations
Groups
Users
sch
System
Users
Microsoft Exchange System Objects
Name
Type
Microsoft Hyper-V
serviceConnectionPoint
Datas
Shared Folder
Start
3 Microsoft Manage...
3 Windows Explorer
Sharing - Paint
FR
14:27

Les permissions

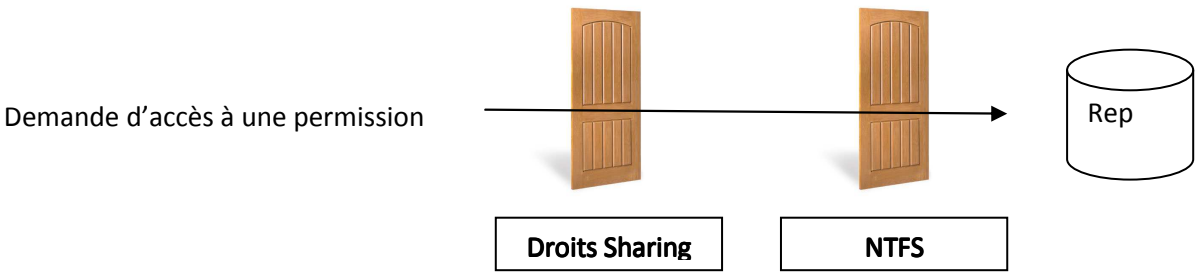
L'utilisateur reçoit une série de clé (token) lors de son identification sur le réseau. Ses clés sont représentées par des SID. Exemple : User test : SID …..- 1307, global compta : SID …..-1334

Quand on demande une ressource, il y a vérification via les ACL ou sont vérifié les permissions (grant).

Notez qu'un deny explicite est toujours le plus restrictif concernant les ACL.

La gestion des permissions

Il y a deux possibilités de gérer les permissions, soit via le sharing, soit via les droits NTFS. Ceux-ci sont complémentaires et la meilleure représentation est sans doute une double porte.



C'est toujours le plus restrictif qui l'emporte. Même si le sharing vous laisse passer en écriture si le NTFS ne l'autorise pas vous serez bloqué et inversement.

Droites Sharing

Read : Lecture

Change : Lecture, écriture, suppression

Full Control : Lecture, écriture, suppression + modification des permissions

Conseil : Au lieu de laisser Everyone, il vaut mieux mettre Authenticated Users ce qui renforce un peu la sécurité.

NTFS

Read : On peut voir le contenu d'un dossier et ses propriétés ainsi que des fichiers.

Read & Exécute : On peut exécuter des fichiers exécutable (Exe,bat, cmd, vbs,…) et on peut lire les fichiers. Au niveau des répertoires, on a les droits de traverse.

List Folder Contents : Traverse et read des dossiers.

Write : Création de fichier, répertoires, possibilité de renommer et de modifier les contenus.

Modify : Toutes les options et en plus, on peut supprimer les fichiers. Idem sur les répertoires mais ceux-ci doivent être vide.

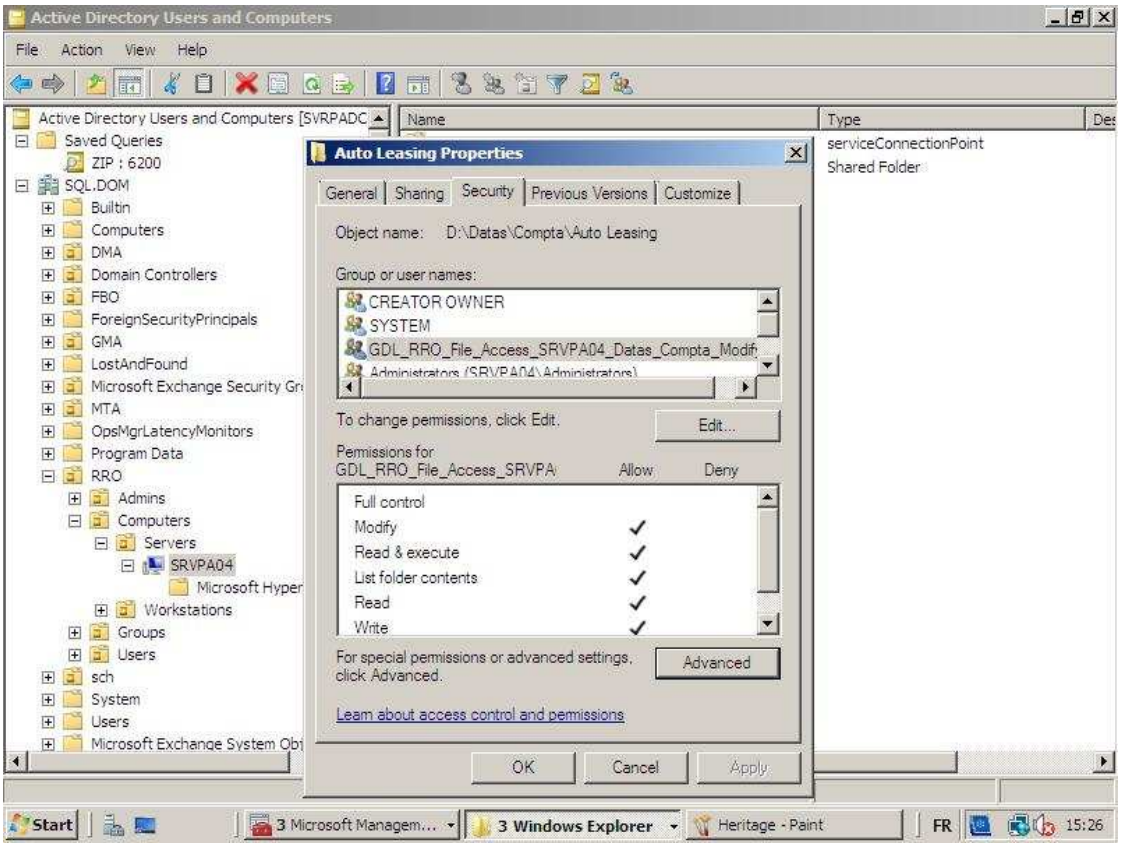
Full control : Toutes les options + modification des permissions.

On peut également ajouter des permissions spéciales via l'onglet advanced. On peut par exemple empêcher de lire les propriétés des fichiers et répertoires. Les options sont vastes et permettent une configuration très adaptées.

La notion d'héritage

Par défaut, l'héritage sur les dossiers est activé. Un nouveau dossier héritera donc des permissions de son parent. On peut couper cet héritage en vidant les permissions ou en recopiant les permissions dans l'onglet advanced du NTFS.

Attention au groupe users qui a des droits par défaut sur tous les répertoires. Il est plus que conseiller de le changer. Attention également au Creator Owner qui a des droits full control par défaut. Il vaut mieux limiter le creator owner en lui donnant les mêmes permissions que son groupe sur la ressource.



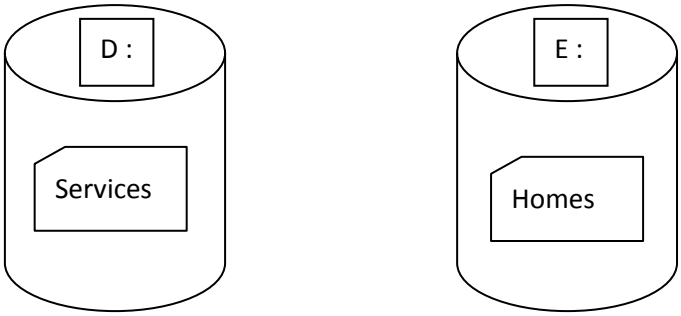
Gestion des données

Limitation de l'espace disque

Il y a deux manière pour limiter l'espace disque consommée par les utilisateurs.

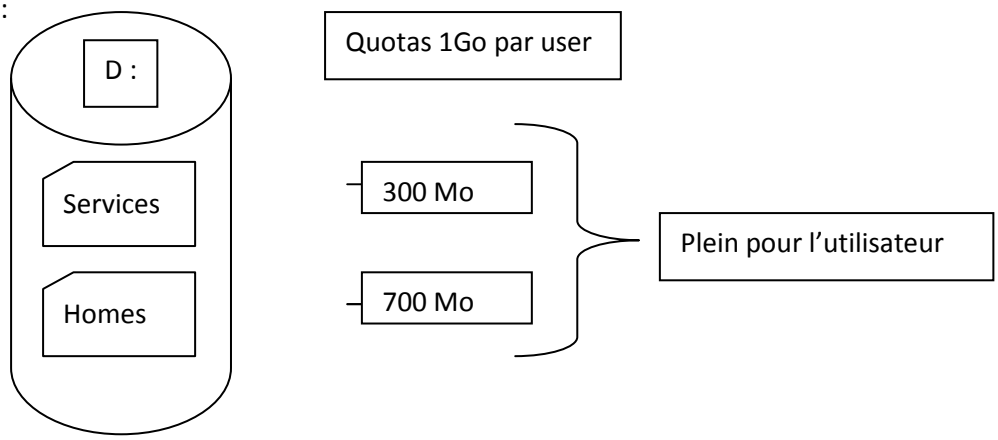
Quotas	File Server Ressource Manager
Basé sur le propriétaire des fichiers	Installer le service « File service Ressour Manager » du rôle File Server.
Une gestion par partition	Limite la taille de certain dossier
	Bloquer des extensions (File screening manager)
	Reporting d'activité

Solution idéal :



Du File Server Ressource Manager sur les services et de la gestion de quotas classique sur les homes.

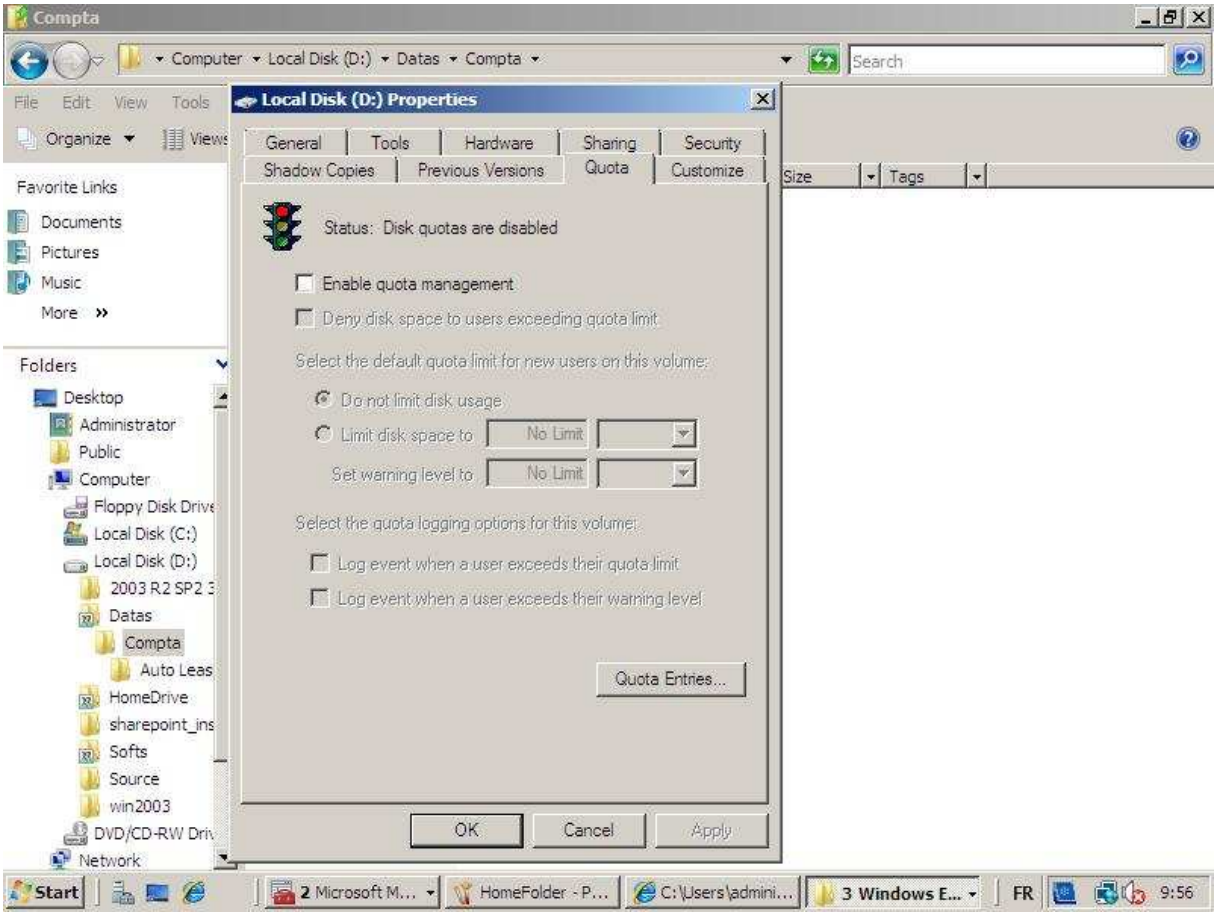
Solution moins idéal :

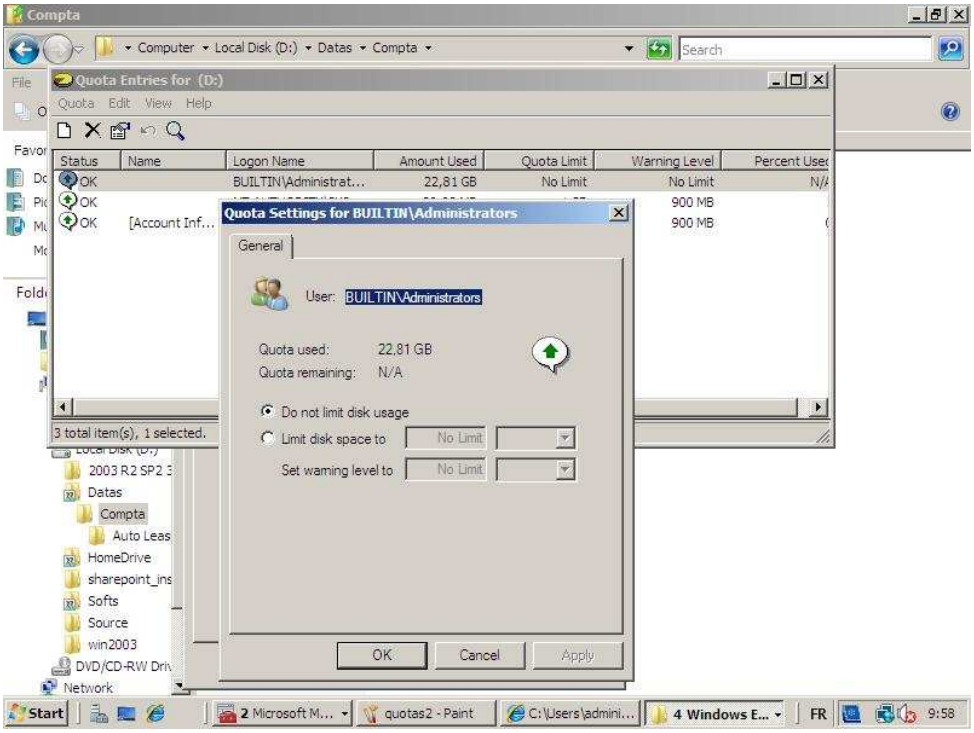


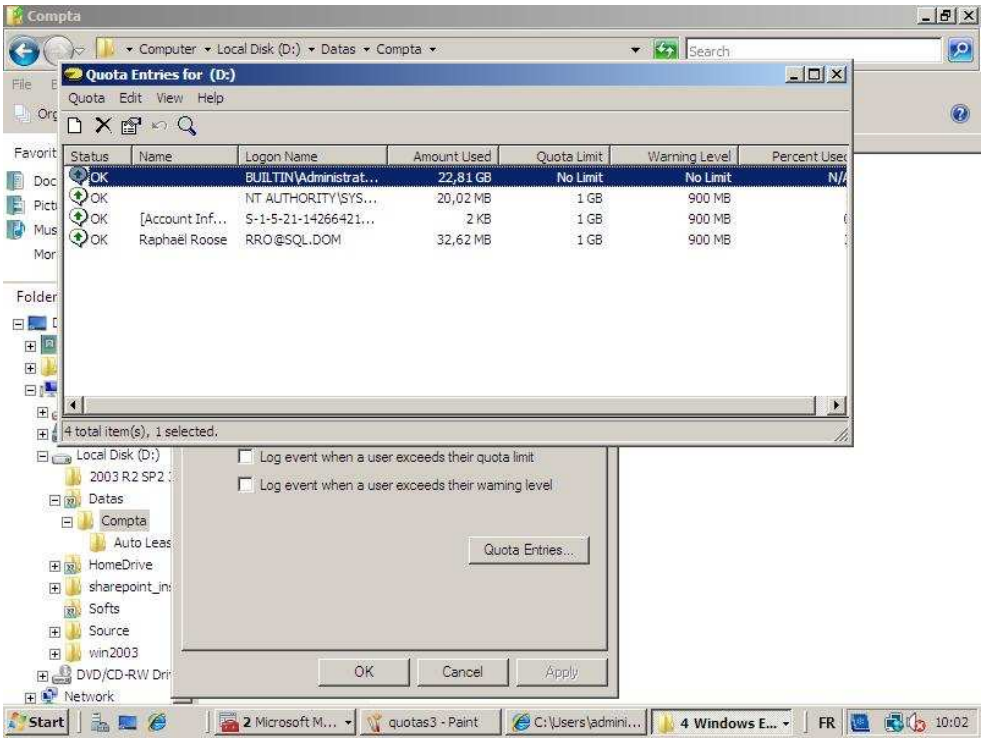
Les quotas

Les quotas s'activent directement sur la partition. C'est une configuration générale pour l'ensemble de la partition mais on peut néanmoins spécifier une taille plus grande pour certains utilisateurs. On a également une partie qui peut servie de « reporting » sur l'espace déjà consommé.

Si vous décidez de modifier les quotas, les nouvelles modifications ne seront effectivement que sur les nouveaux utilisateurs. Il faudra repasser manuellement sur les utilisateurs déjà existants.

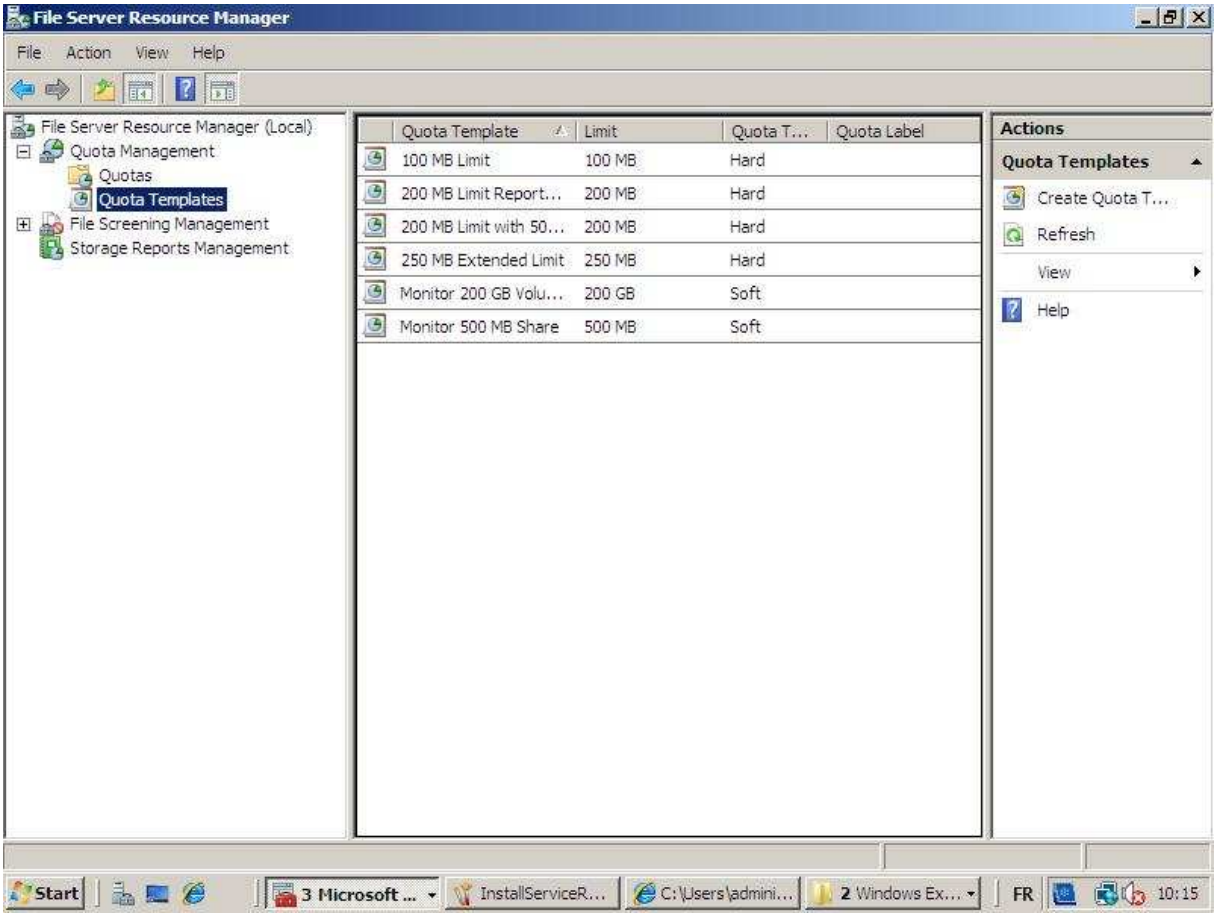

Compta
Computer ▸ Local Disk (D:) ▸ Datas ▸ Compta
Search
File Edit View Tools
Organize
Views
Local Disk (D:) Properties
General Tools Hardware Sharing Security
Shadow Copies Previous Versions Quota Customize
Status: Disk quotas are disabled
Enable quota management
Deny disk space to users exceeding quota limit
Select the default quota limit for new users on this volume:
Do not limit disk usage
Limit disk space to No Limit
Set warning level to No Limit
Select the quota logging options for this volume:
Log event when a user exceeds their quota limit
Log event when a user exceeds their warning level
Quota Entries...
OK Cancel Apply
Favorite Links
Documents
Pictures
Music
More »
Folders
Desktop
Administrator
Public
Computer
Floppy Disk Drive
Local Disk (C:)
Local Disk (D:)
2003 R2 SP2 3
Datas
Compta
Auto Leas
HomeDrive
sharepoint_ins
Softs
Source
win2003
DVD/CD-RW Driv
Network
Size
Tags
Start
2 Microsoft M...
HomeFolder - P...
C:\Users\admini...
3 Windows E...
FR
9:56


Compta
Computer ▸ Local Disk (D:) ▸ Datas ▸ Compta
Search
Quota Entries for (D:)
Quota Edit View Help
Status Name Logon Name Amount Used Quota Limit Warning Level Percent Use
OK BUILTIN\Administrat... 22,81 GB No Limit No Limit
OK 900 MB 900 MB
OK [Account Inf...
3 total item(s), 1 selected.
Quota Settings for BUILTIN\Administrators
General
User: BUILTIN\Administrators
Quota used: 22,81 GB
Quota remaining: N/A
Do not limit disk usage
Limit disk space to No Limit
Set warning level to No Limit
OK Cancel Apply
2003 R2 SP2 3
Datas
Compta
Auto Leas
HomeDrive
sharepoint_ins
Softs
Source
win2003
DVD/CD-RW Driv
Network
Start
2 Microsoft M...
quotas2 - Paint
C:\Users\admini...
4 Windows E...
FR
9:58

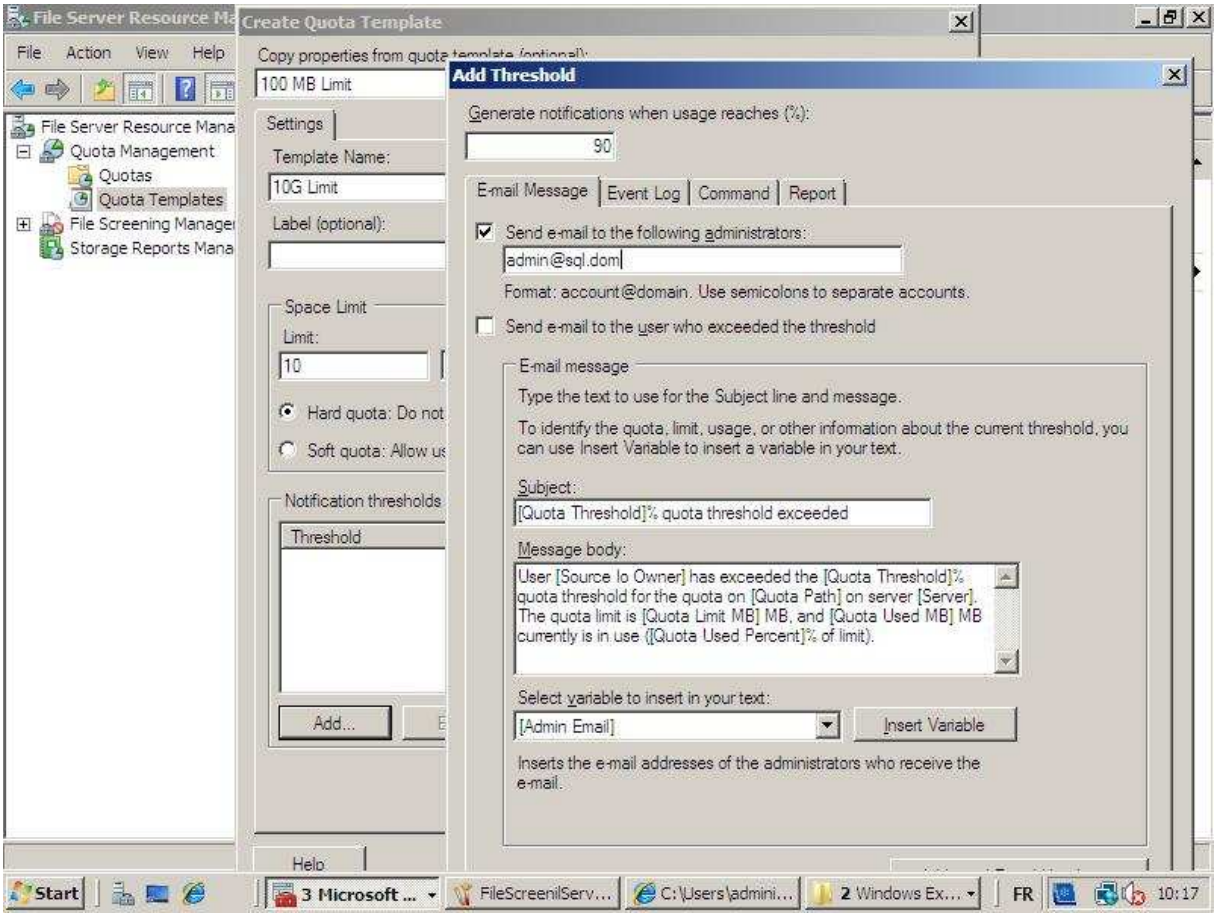


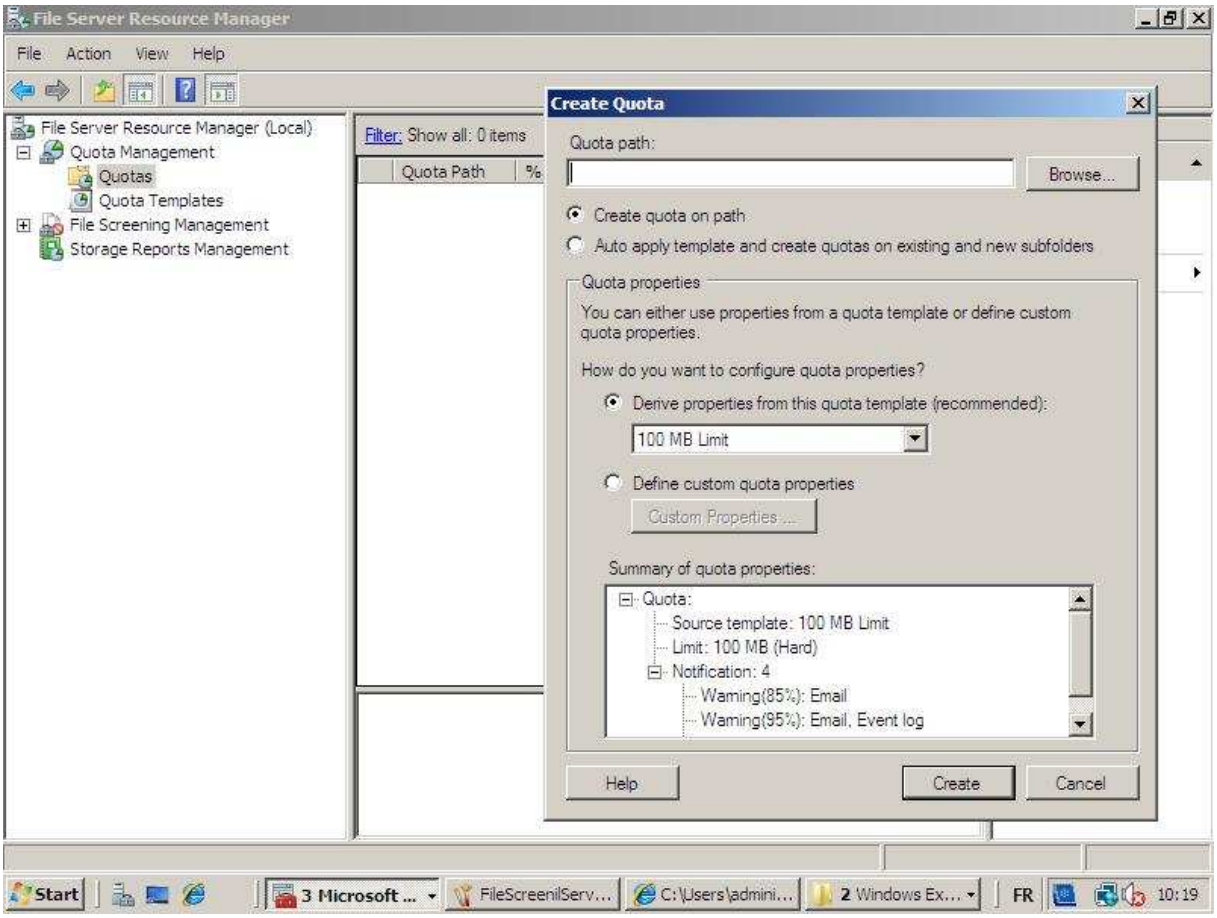
File Server Ressource Manager

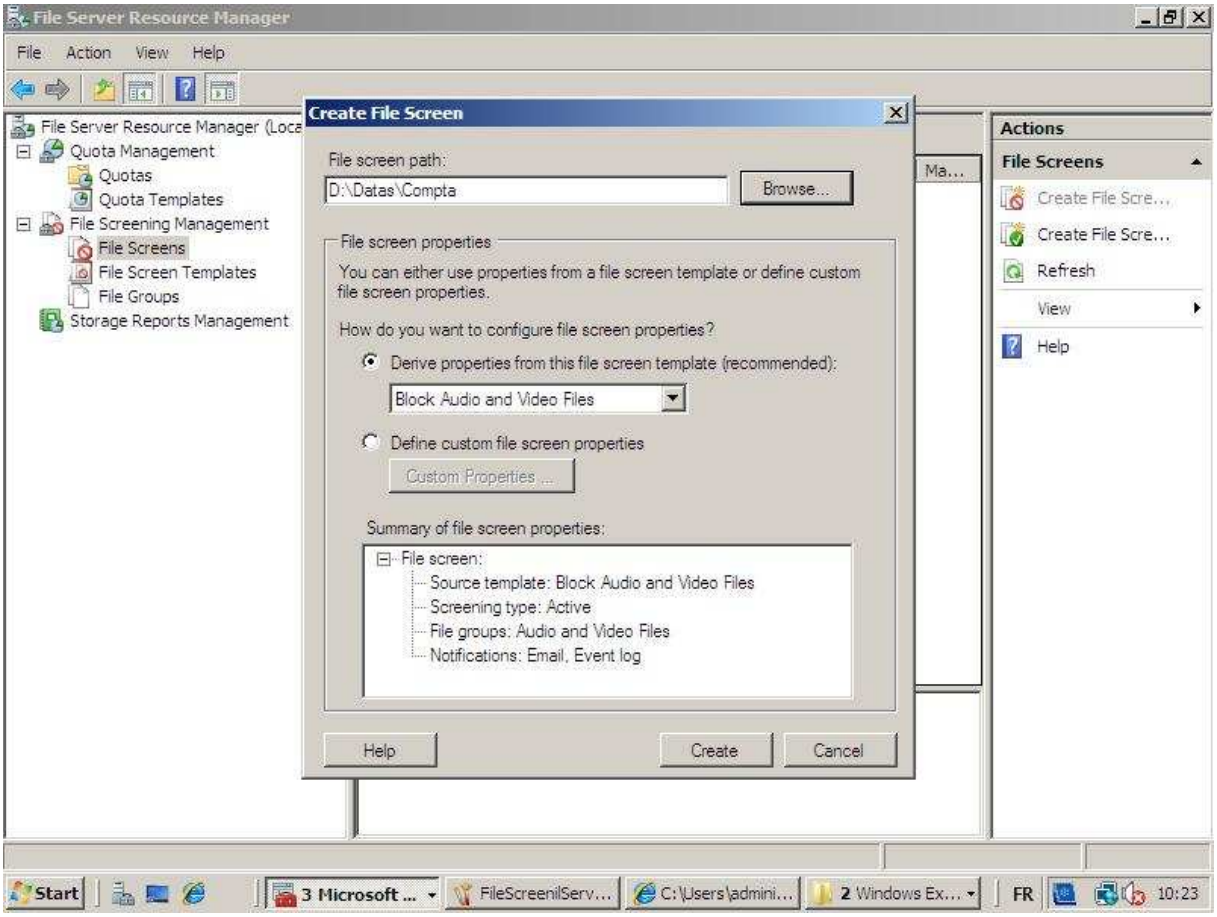
Vous trouverez le « File Server Ressource Manager » dans les outils d'administration à condition que le service soit installé. Vous pourrez soit utiliser un Quota Template qui est définit soit en créer un nouveau et l'appliquer sur un répertoire.



Vous également envoyer des messages à l'administrateur ou l'utilisateur quand celui-ci arrive à la taille limite. C'est également via le « File Server Ressource Manager » que vous pourrez empêcher l'écriture de fichier à extension bien définie. Comme par exemple des MP3 ou des fichiers vidéos.


File Server Resource Ma
Create Quota Template
File Action View Help
Copy properties from quota template (optional):
100 MB Limit
Add Threshold
File Server Resource Mana
Quota Management
Quotas
Quota Templates
File Screening Manager
Storage Reports Mana
Settings
Template Name:
10G Limit
Label (optional):
Space Limit
Limit:
10
Hard quota: Do not
Soft quota: Allow us
Notification thresholds
Threshold
Add...
Help
Generate notifications when usage reaches (%):
90
E-mail Message
Event Log
Command
Report
Send e-mail to the following administrators:
admin@sql.dom
Format: account@domain. Use semicolons to separate accounts.
Send e-mail to the user who exceeded the threshold
E-mail message
Type the text to use for the Subject line and message.
To identify the quota, limit, usage, or other information about the current threshold, you can use Insert Variable to insert a variable in your text.
Subject:
[Quota Threshold]% quota threshold exceeded
Message body:
User [Source Io Owner] has exceeded the [Quota Threshold]% quota threshold for the quota on [Quota Path] on server [Server]. The quota limit is [Quota Limit MB] MB, and [Quota Used MB] MB currently is in use ([Quota Used Percent]% of limit).
Select variable to insert in your text:
[Admin Email]
Insert Variable
Inserts the e-mail addresses of the administrators who receive the e-mail.
Start
3 Microsoft ...
FileScreenilServ...
C:\Users\admini...
2 Windows Ex...
FR
10:17


File Server Resource Manager
File Action View Help
File Server Resource Manager (Local)
Quota Management
Quotas
Quota Templates
File Screening Management
Storage Reports Management
Filter: Show all: 0 items
Quota Path
%
Create Quota
Quota path:
Browse...
Create quota on path
Auto apply template and create quotas on existing and new subfolders
Quota properties
You can either use properties from a quota template or define custom quota properties.
How do you want to configure quota properties?
Derive properties from this quota template (recommended):
100 MB Limit
Define custom quota properties
Custom Properties ...
Summary of quota properties:
Quota:
Source template: 100 MB Limit
Limit: 100 MB (Hard)
Notification: 4
Warning(85%): Email
Warning(95%): Email, Event log
Help
Create
Cancel
Start
3 Microsoft ...
FileScreenilServ...
C:\Users\admini...
2 Windows Ex...
FR
10:19



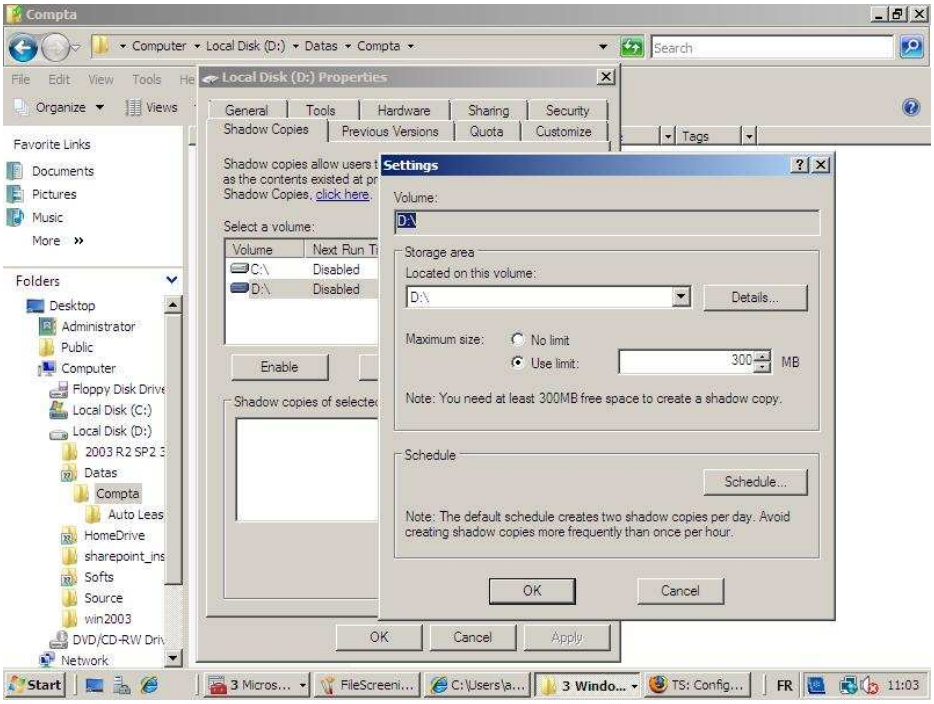
Le Shadow Copy

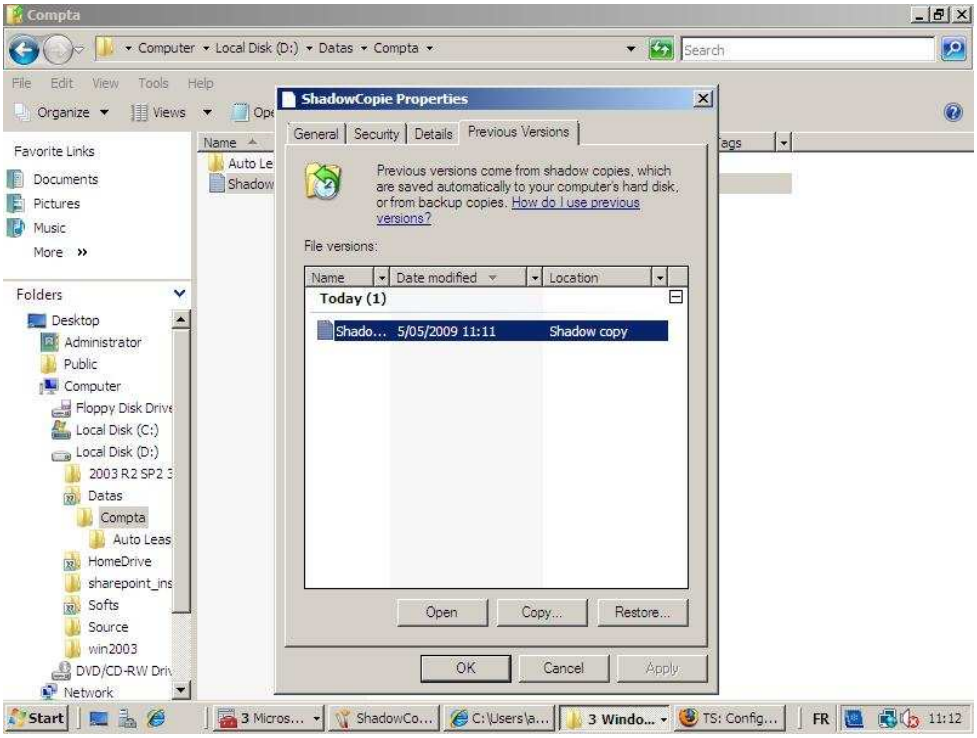
Le service Shadow-Copy est destiné au stockage de fichiers sur des dossiers partagés.

Il permet :

- De récupérer les fichiers accidentellement effacés.
- De récupérer les fichiers malencontreusement écrasés ou mis à jour.
- D'implémenter la notion de version sur les documents sur lesquels on travaille.
- De limiter les accès physiques aux serveurs pour effectuer des backups de fichiers à restaurer, en offrant des possibilités de récupération de fichiers directement sur un poste client supportant le client VSS.

Lors de la configuration de ce service, il faut lui attribuer une taille maximale comme par exemple 15% de la partition.

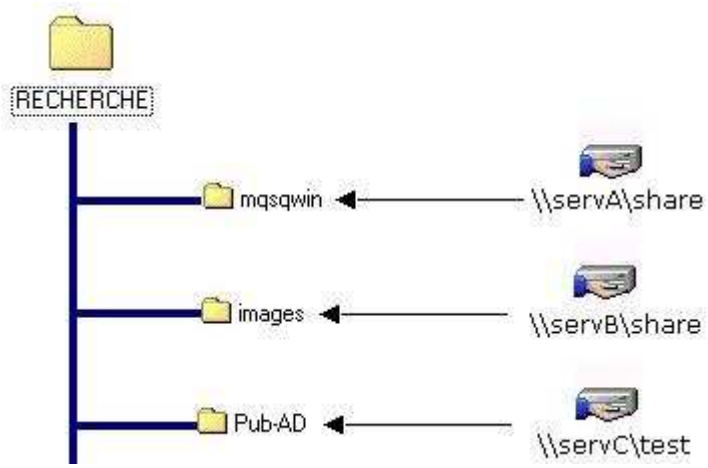

Compta
Computer ▸ Local Disk (D:) ▸ Datas ▸ Compta ▸
Search
Local Disk (D:) Properties
General
Tools
Hardware
Sharing
Security
Shadow Copies
Previous Versions
Quota
Customize
Settings
Volume:
D:\
Storage area
Located on this volume:
D:\
Details...
Maximum size:
No limit
Use limit:
300
MB
Note: You need 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
Apply
Select a volume:
Volume
Next Run T
C:\
Disabled
D:\
Disabled
Enable
Favorite Links
Documents
Pictures
Music
More
Folders
Desktop
Administrator
Public
Computer
Floppy Disk Drive
Local Disk (C:)
Local Disk (D:)
Datas
Compta
HomeDrive
Softs
Source
win2003
Network
Start
FR
11:03


Compta
Computer ▸ Local Disk (D:) ▸ Datas ▸ Compta ▸
Search
ShadowCopie Properties
General
Security
Details
Previous Versions
Previous versions come from shadow copies, which are saved automatically to your computer's hard disk, or from backup copies. How do I use previous versions?
File versions:
Name
Date modified
Location
Today (1)
Shado... 5/05/2009 11:11
Shadow copy
Open
Copy...
Restore...
OK
Cancel
Apply
Favorite Links
Documents
Pictures
Music
More
Folders
Desktop
Administrator
Public
Computer
Floppy Disk Drive
Local Disk (C:)
Local Disk (D:)
Datas
Compta
HomeDrive
Softs
Source
win2003
Network
Start
FR
11:12

On ne sait pas déplacer un « Shadow Copy » ou même en faire un backup. En cas de crash disque, les données sont perdues et il faudra que les utilisateurs repartent de 0. Il est donc bien important de ne pas confondre le « Shadow Copy » avec un système de backup. Notez qu'on peut très bien dédier un disque dur en SATA pour jouer ce rôle. Ce qui permet donc de délocaliser les données.

DFS : Distributed File System

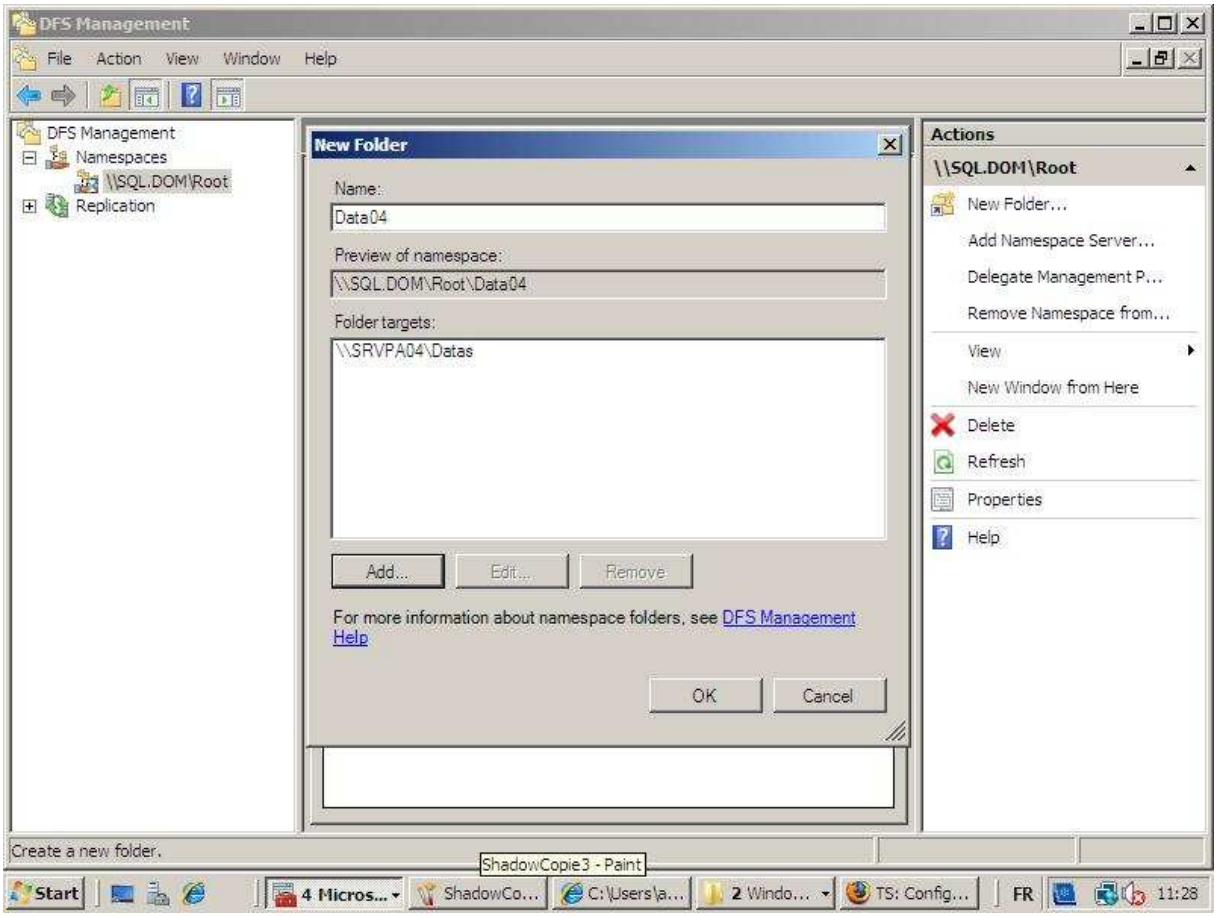
DFS (Distributed File System) fournit aux utilisateurs un moyen simple d'accéder à des données reparties et distribuées sur un réseau. Un dossier partagé DFS sert de point d'accès à d'autres dossiers sur le réseau. Il permet par exemple de regrouper différents partages stockés sur des différents serveurs à un seul point.



Il permet également une réplication de données entre deux serveurs.

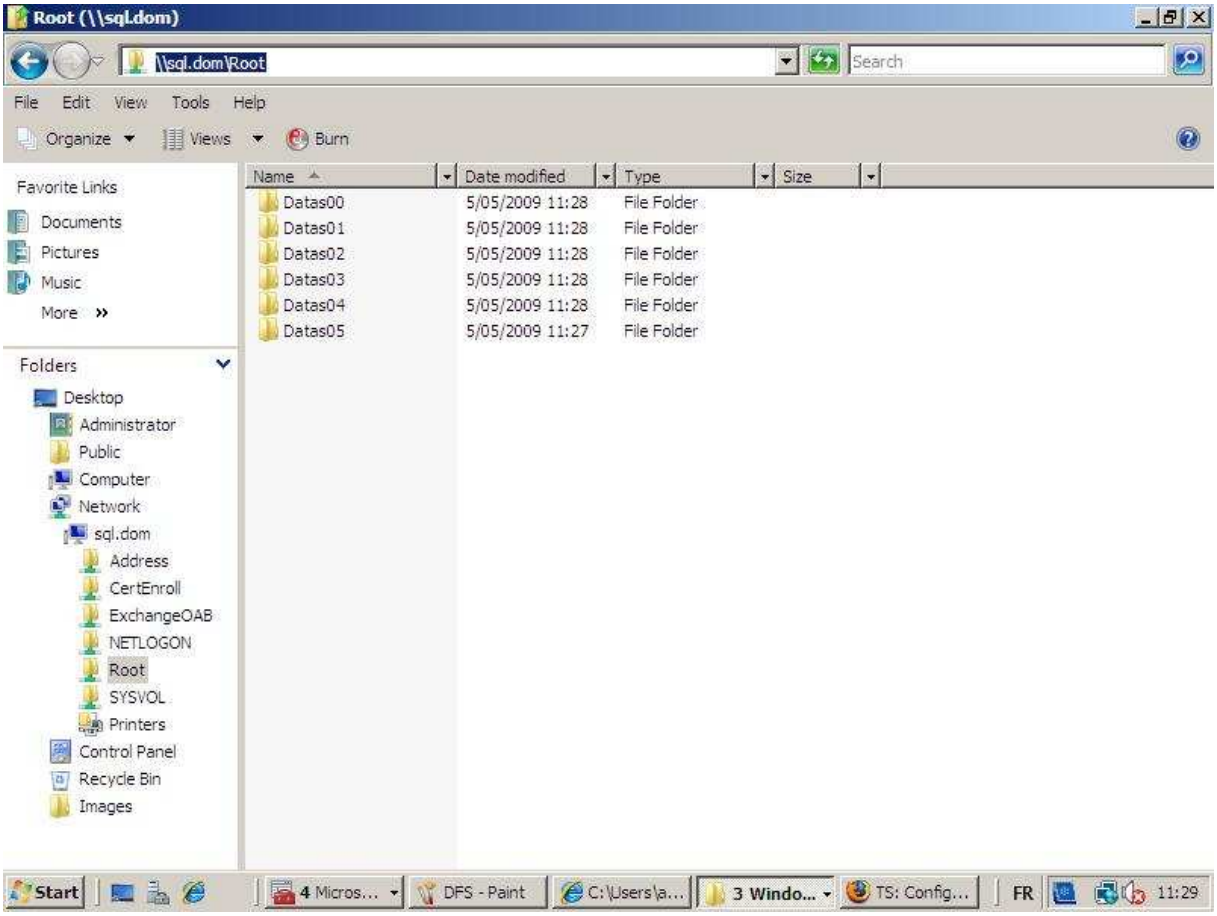
- Idéal pour avoir les données proches des utilisateurs.
- Un backup centralisé.
- Fault Tolerance mais il est loin d'être idéal dans cette tâche. Le mieux sera toujours d'avoir un système de clustering.

Il faut d'abord définir un « name space » ou un « root » sur le Domain Controler. Ensuite, on crée le lien qui se rattache a ce « name space ». C'est évidement un répertoire partagé.



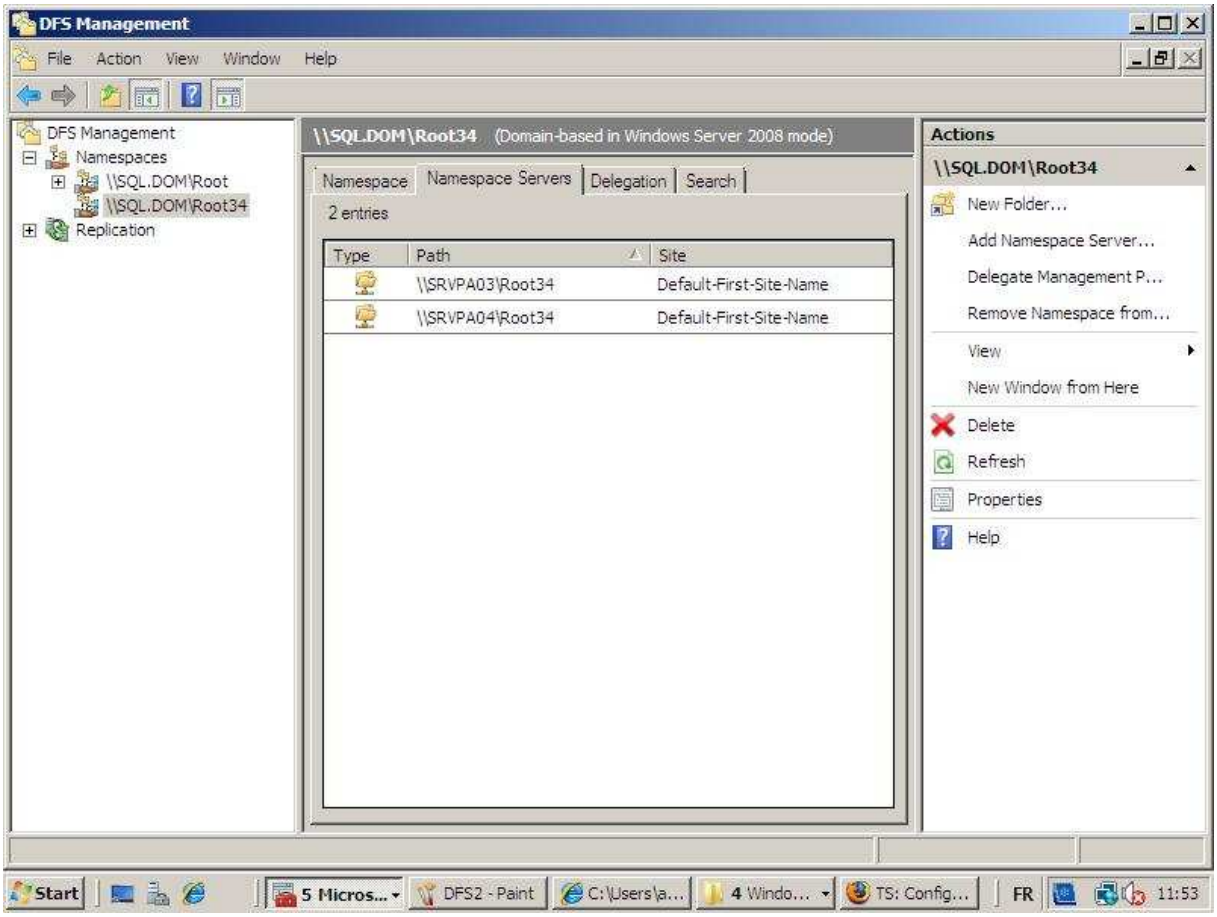
Il suffit ensuite de browser le réseau directement via le nom du domaine.

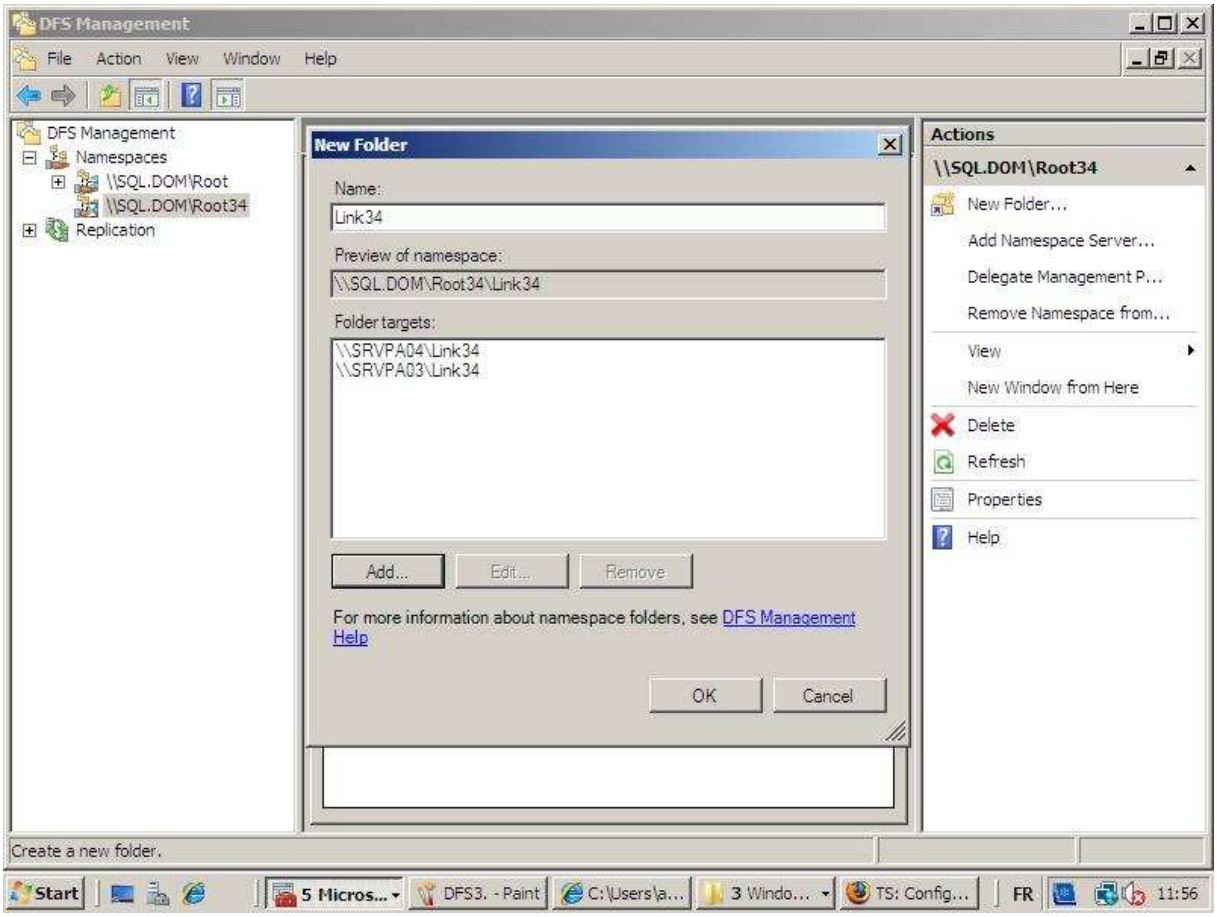
\\NomDomain



Dans le cas de la synchronisation :

1. Créer deux « name space » identiques sur chaque serveur.
2. Créer des links sur les serveurs.
3. On crée la réplication en définissant un domain controler comme primaire et la topology de la synchronisation.


DFS Management
File Action View Window Help
DFS Management
Namespaces
\\SQL.DOM\Root
\\SQL.DOM\Root34
Replication
\\SQL.DOM\Root34 (Domain-based in Windows Server 2008 mode)
Namespace
Namespace Servers
Delegation
Search
2 entries
Type
Path
Site
\\SRVPA03\Root34
Default-First-Site-Name
\\SRVPA04\Root34
Default-First-Site-Name
Actions
\\SQL.DOM\Root34
New Folder...
Add Namespace Server...
Delegate Management P...
Remove Namespace from...
View
New Window from Here
Delete
Refresh
Properties
Help
Start
5 Micros...
DFS2 - Paint
C:\Users\a...
4 Windo...
TS: Config...
FR
11:53


DFS Management
File Action View Window Help
DFS Management
Namespaces
\\SQL.DOM\Root
\\SQL.DOM\Root34
Replication
New Folder
Name:
Link34
Preview of namespace:
\\SQL.DOM\Root34\Link34
Folder targets:
\\SRVPA04\Link34
\\SRVPA03\Link34
Add...
Edit...
Remove
For more information about namespace folders, see DFS Management Help
OK
Cancel
Actions
\\SQL.DOM\Root34
New Folder...
Add Namespace Server...
Delegate Management P...
Remove Namespace from...
View
New Window from Here
Delete
Refresh
Properties
Help
Create a new folder.
Start
5 Micros...
DFS3. - Paint
C:\Users\a...
3 Windo...
TS: Config...
FR
11:56

Hyper-V

Hyper-V sert à la virtualisation de serveur ou de client. Il ne fonctionne que sous la version 64 bit avec un CPU adapté à la virtualization. Contrairement à Vmware, il n'est capable de faire tourner que des OS Microsoft.

Recommandation :

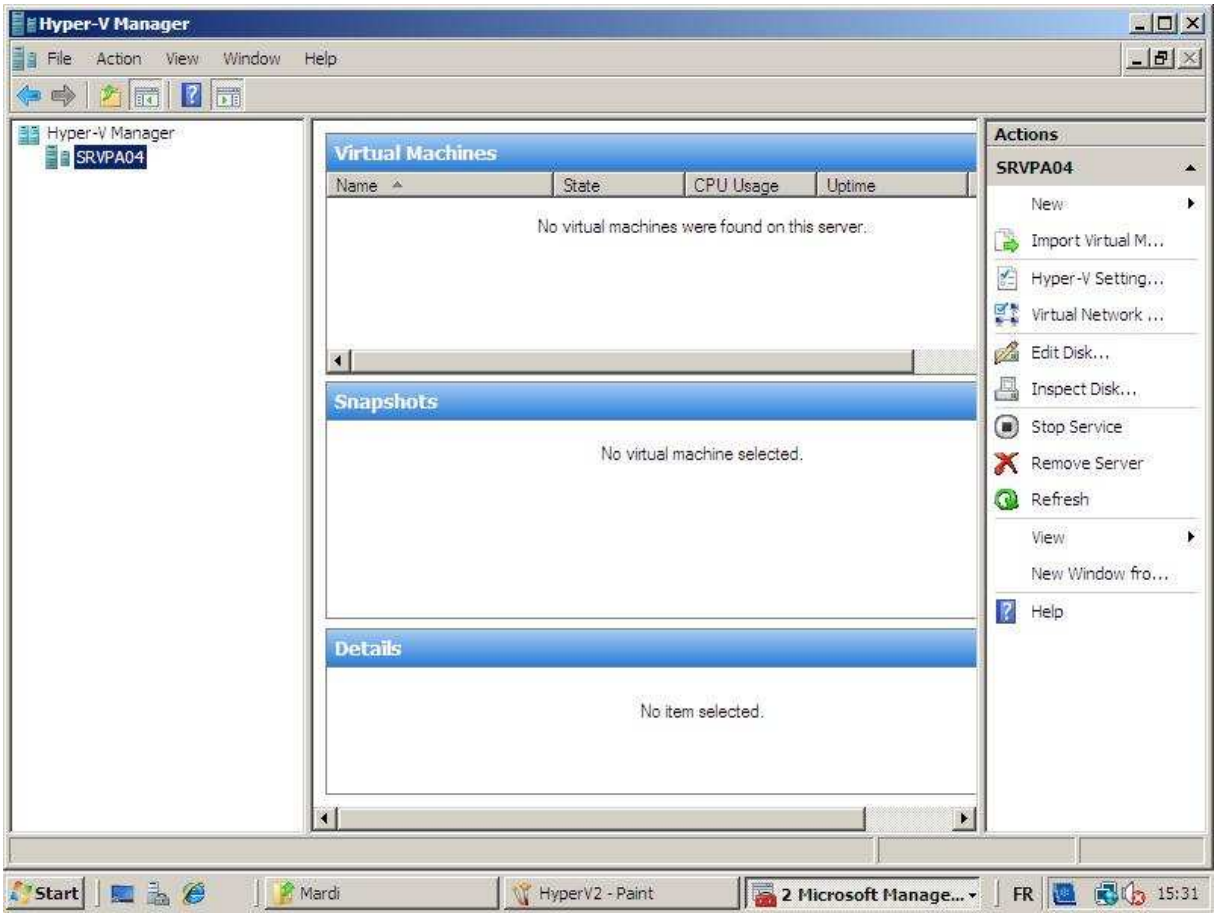
Plusieurs cartes réseaux dont une toujours disponible en dehors de la Virtualisation.

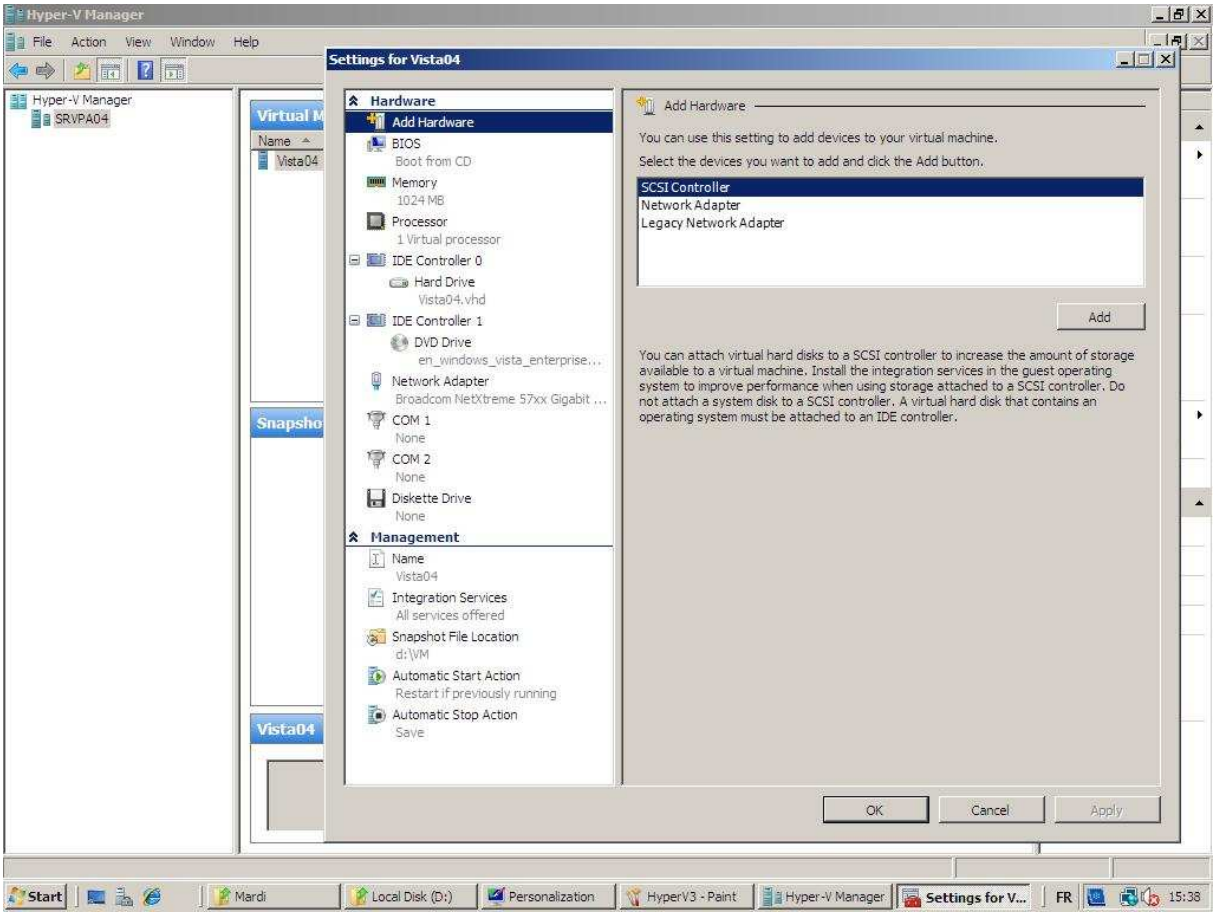
De la Ram en conséquence avec une fréquence et un bus élevé.

Des disques durs très rapides pour limiter les temps d'accès.

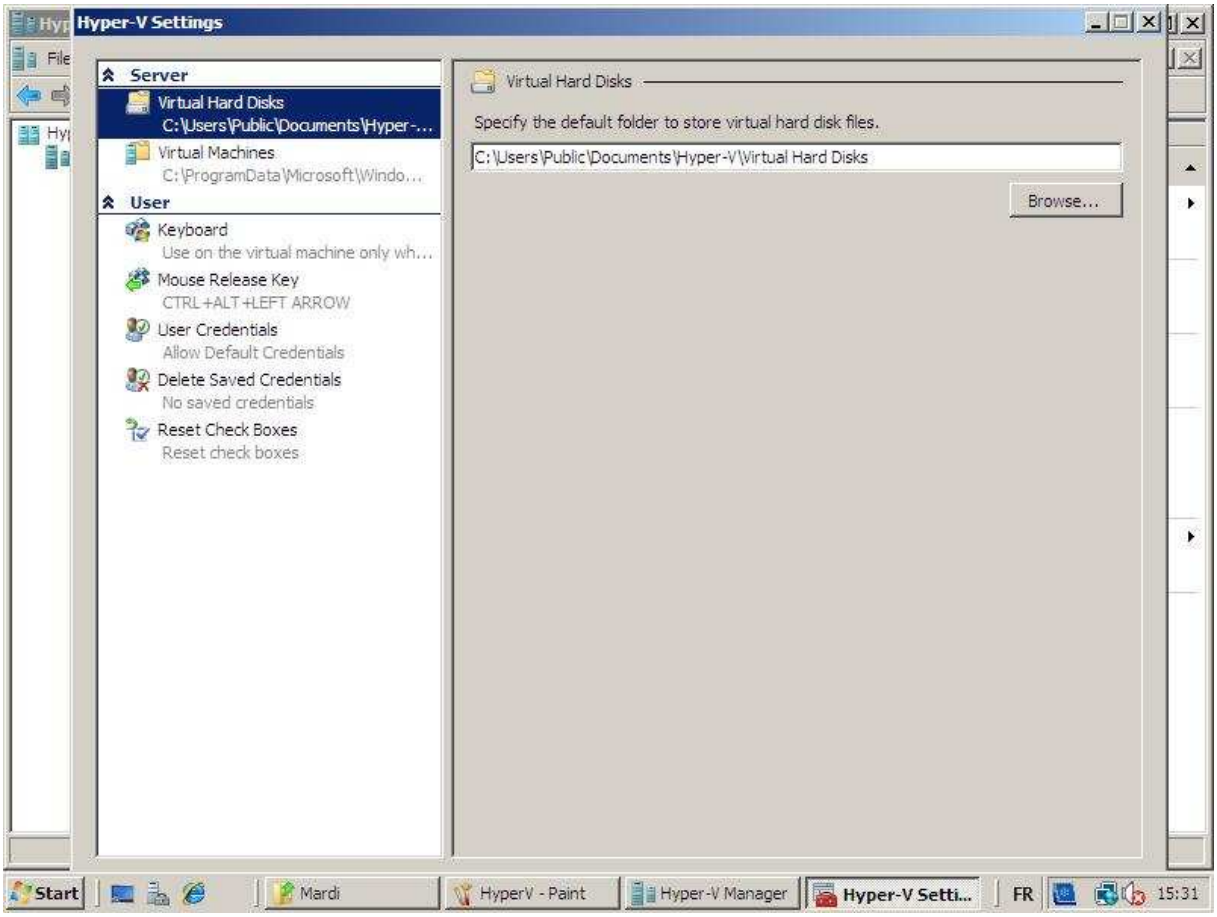
Un CPU adapté à la virtualisation comme les Core I7 de chez Intel (pas de version serveur pour l'instant). Cette nouvelle génération de processeur (5 mai 09) qui permet un accès à la mémoire plus rapide grâce à l'apparition du mode triple canal.

Hyper-V manager





C'est via le « **Hyper-V manager** » qu'on configure l'ensemble des OS virtuels. Il faut tout d'abord définir un disque virtuel (VHD) qui accueillera les images virtuelles. Un VHD est limité à 2 TB de données. Ensuite, il suffira de créer une machine virtuelle.



Ces VHD peuvent être de plusieurs types « dynamique », « fixe », « différence », « Pass-through ».

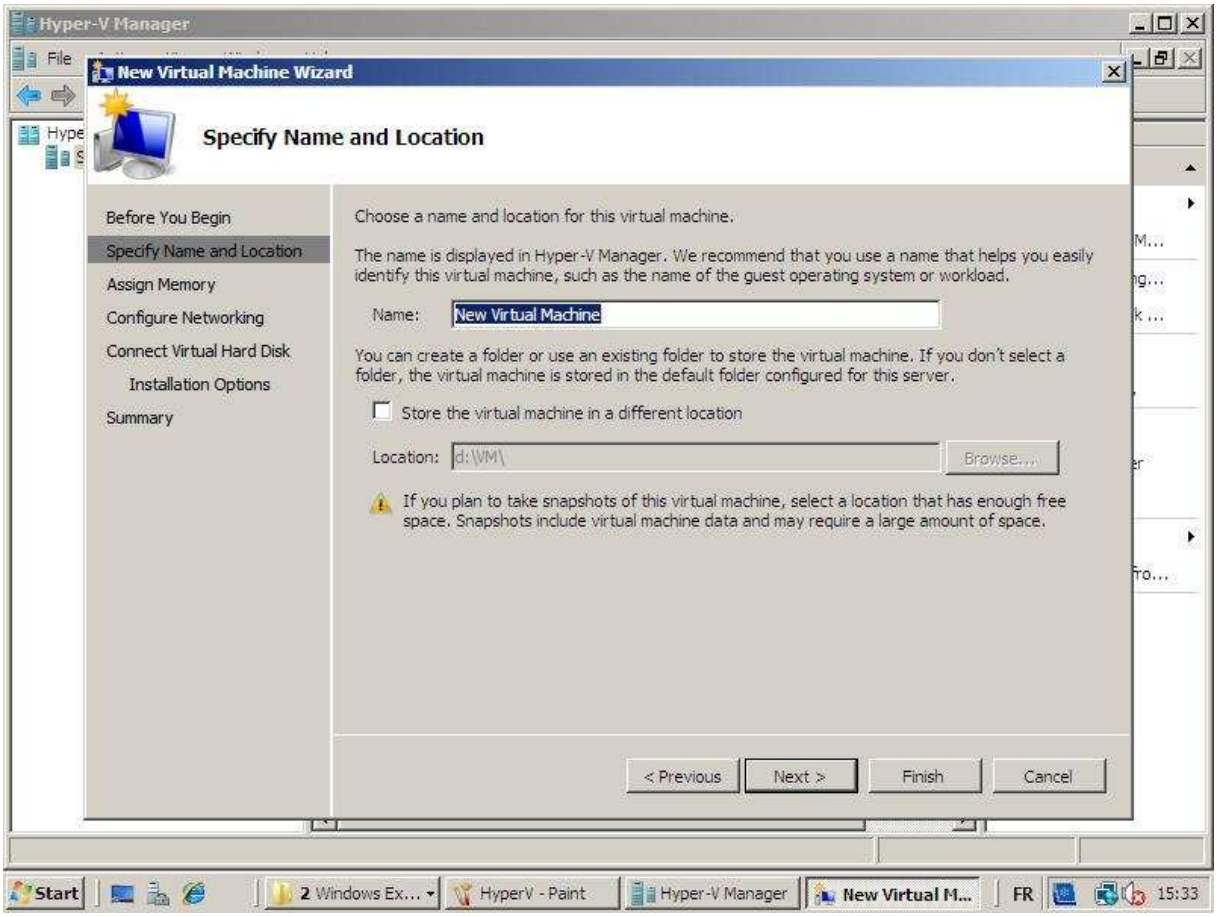
- Le dynamique comme son nom l'indique se redimensionne selon les besoins. Ce mode de fonctionnement entraine des chutes de performances.

- Le Fixe qui a sa taille de définie et qui ne varie pas. Après le « Pass-through », il donne les meilleures performances qu'on peut attendre.

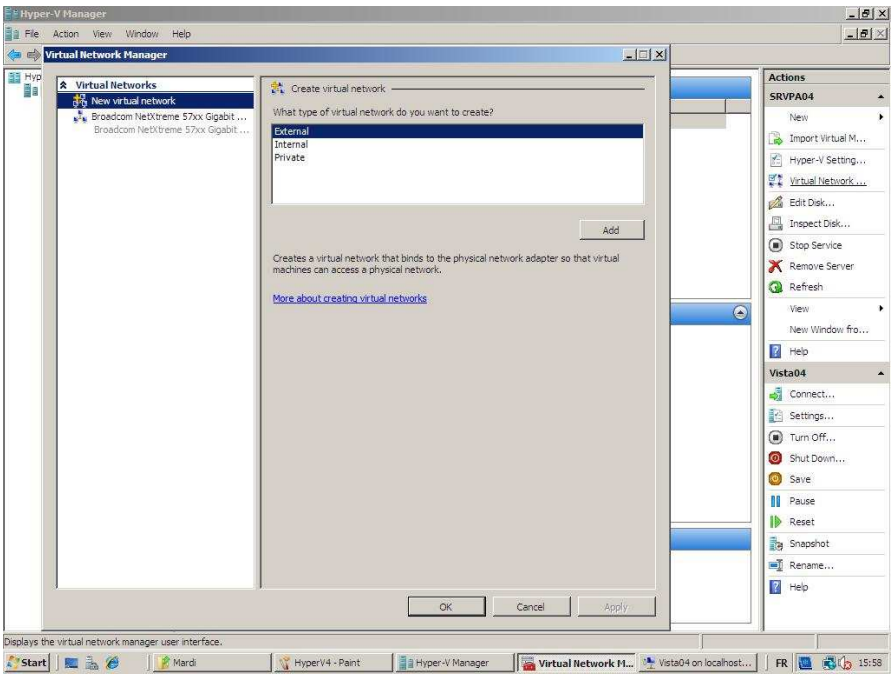
- Disques d'annulation ou disques de différence, l'objectif du disque de différence est de permettre à une image virtuelle d'avoir comme base une autre image afin que seules les modifications soient enregistrées. Il s'agit d'un cliché différentiel. Cette fonction permet de personnaliser des configurations virtuelles existantes sans modifier les fichiers originaux du disque de la configuration. Il existe une différence entre les disques d'annulation et les disques de différence : un disque de différence s'applique à un disque dur virtuel uniquement alors que les disques d'annulation s'appliquent à tous les disques durs virtuels associés à une machine virtuelle. Une fois le type de disque sélectionné, il faut alors choisir entre :

- La création d'un nouveau disque virtuel (Spécifier la taille du disque virtuel).
- La copie des données d'un disque physique existant : (crée un VHD qui contient les données du disque physique).

- « Pass-trough » qui permet de dédicacer un disque physique a un OS virtuel. Il donne les meilleures performances possibles.


Hyper-V Manager
File
New Virtual Machine Wizard
Specify Name and Location
Before You Begin
Specify Name and Location
Assign Memory
Configure Networking
Connect Virtual Hard Disk
Installation Options
Summary
Choose a name and location for this virtual machine.
The name is displayed in Hyper-V Manager. We recommend that you use a name that helps you easily identify this virtual machine, such as the name of the guest operating system or workload.
Name:
New Virtual Machine
You can create a folder or use an existing folder to store the virtual machine. If you don't select a folder, the virtual machine is stored in the default folder configured for this server.
Store the virtual machine in a different location
Location:
d:\VM\
Browse...
If you plan to take snapshots of this virtual machine, select a location that has enough free space. Snapshots include virtual machine data and may require a large amount of space.
< Previous
Next >
Finish
Cancel
Start
2 Windows Ex...
HyperV - Paint
Hyper-V Manager
New Virtual M...
FR
15:33

Virtual Networks



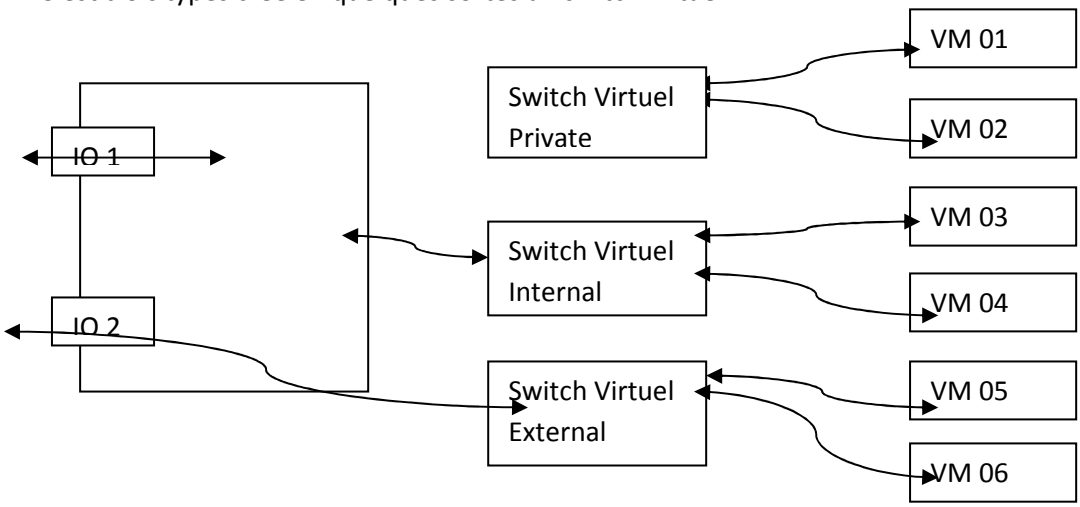
Trois types de virtual Networks « **private** », « **Internal** », « **External** ».

Le « **private** » permet à des machines virtuelles de communiquer ensemble mais pas l'hôte ou avec le reste du réseau.

L' « **Internal** » permet à des machines virtuelles de communiquer ensemble et avec l'hôte mais pas avec le reste du réseau.

L' « **External** » permet à des machines virtuelles de communiquer ensemble avec l'hôte et l'ensemble du réseau.

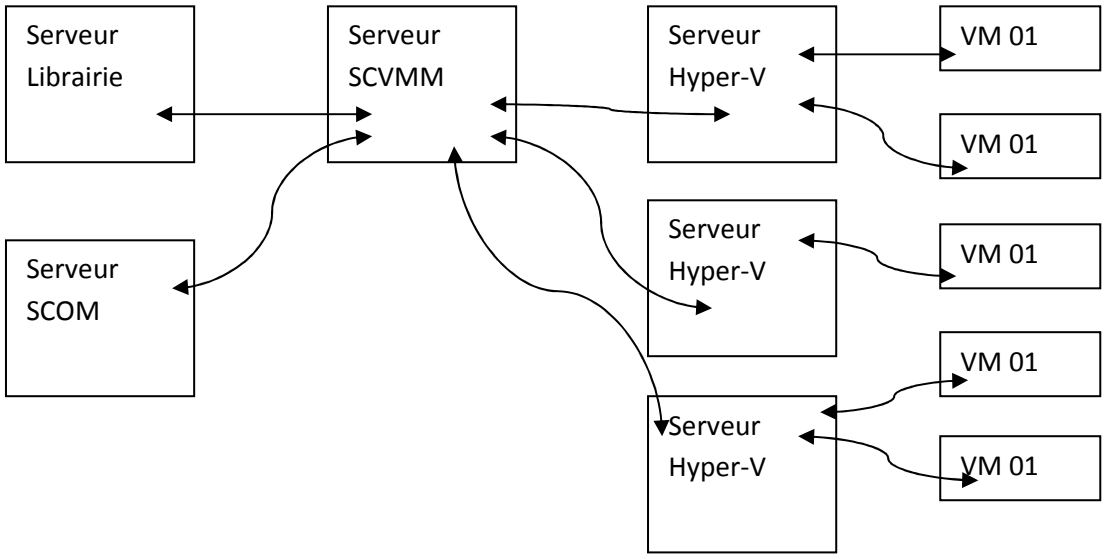
C'est trois types crée en quelques sortes un switch virtuel.



Le type « private » et « internal » permettent de faire des machines de tests qui ne perturberont pas le réseau.

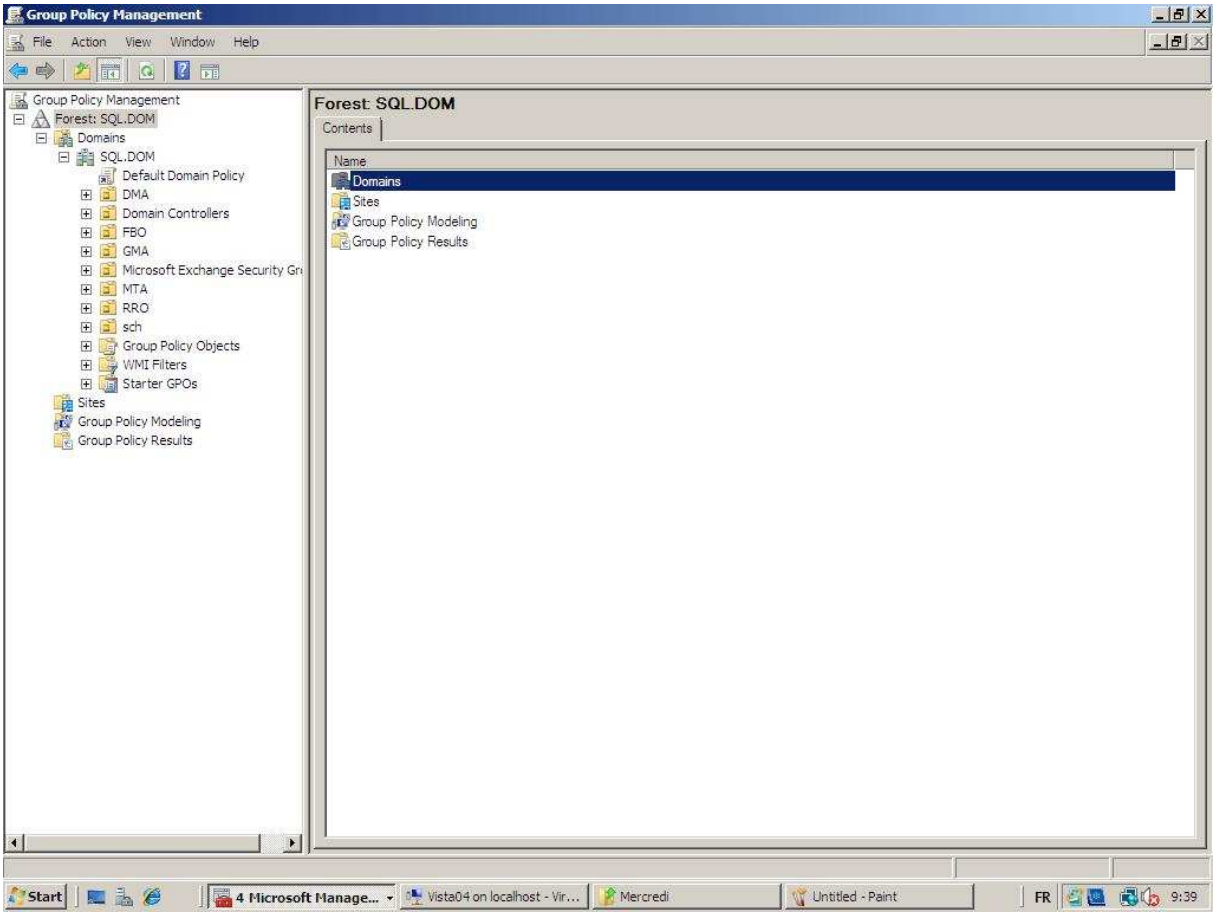
System Center Virtual Machine Manager

C'est un service qui doit tourner sur un serveur à part son rôle sera d'administrer une série de serveurs Hyper-V. On peut également le coupler à un système de Self service qui met à disposition aux utilisateurs autorisés des machines virtuelles à la demande grâce à l'utilisation d'un serveur de librairie. Les utilisateurs commandent des machines virtuelles en dépensant des points et le « SCVMM » met à disposition une machine virtuelle automatiquement. Le « SCVMM » peut également être couplé à Scom (System Center Operations Manager) qui sera en mesure de répartir les tâches entre les différents Hyper-V.



Note : System Center Operations Manager permet de surveiller vos services informatiques.

Group Policy

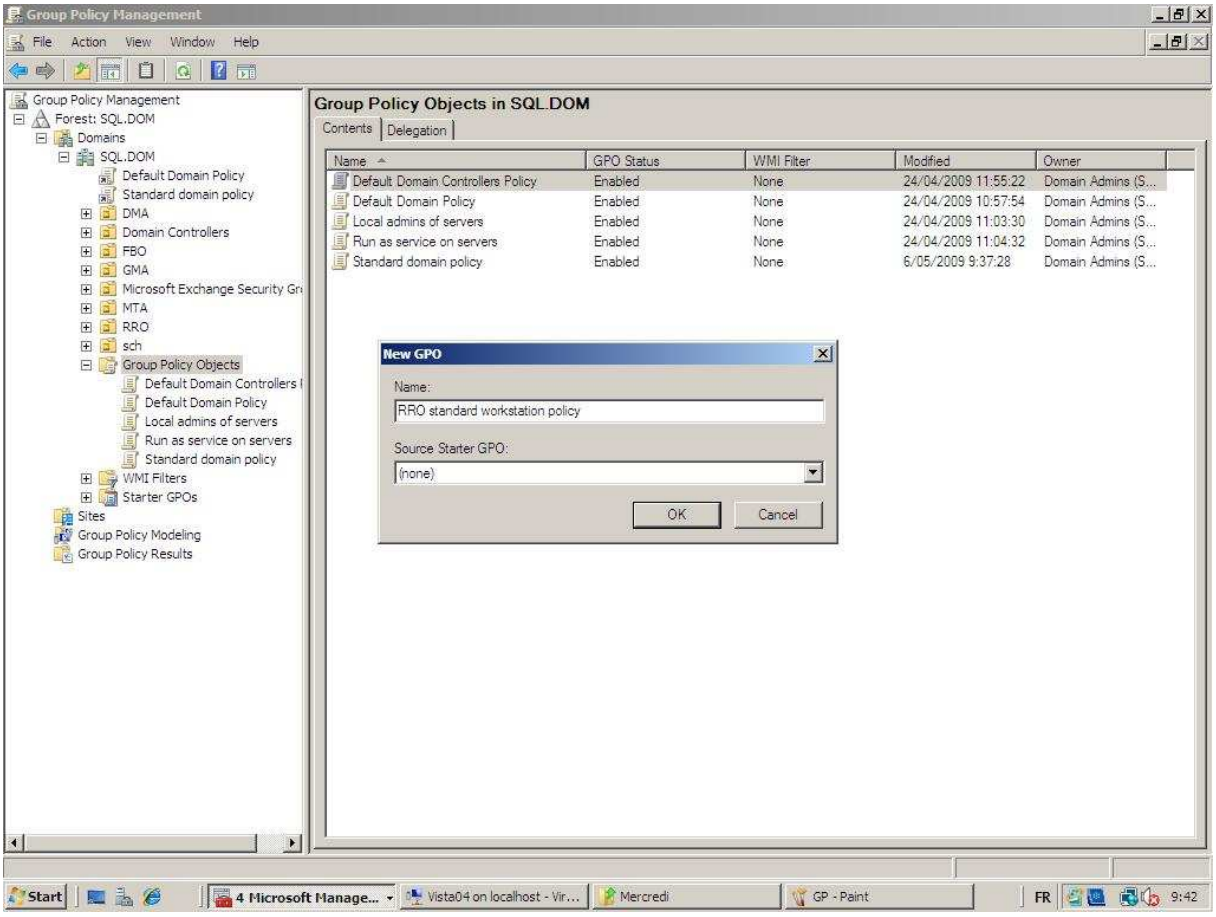


Elles sont utilisées pour la restriction, les scripts, la configuration.

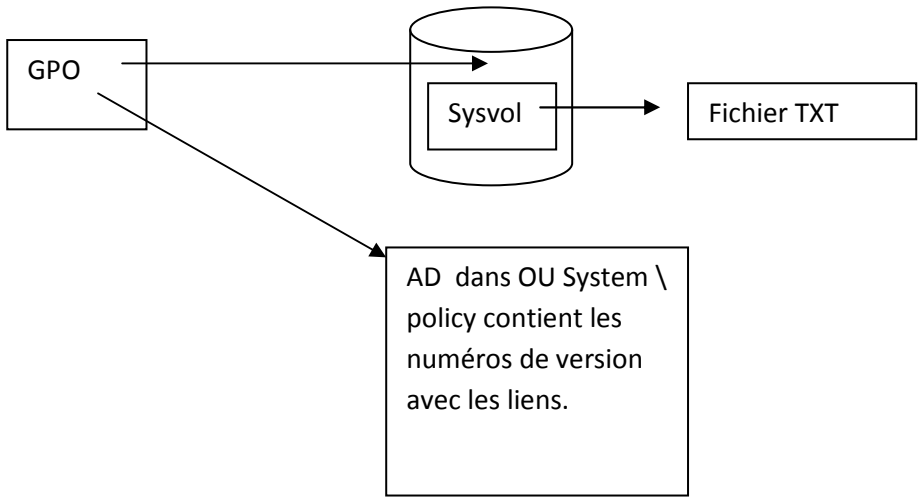
Dans la catégorie configuration, on retrouve les services, les softs, la sécurité, le paramétrage.

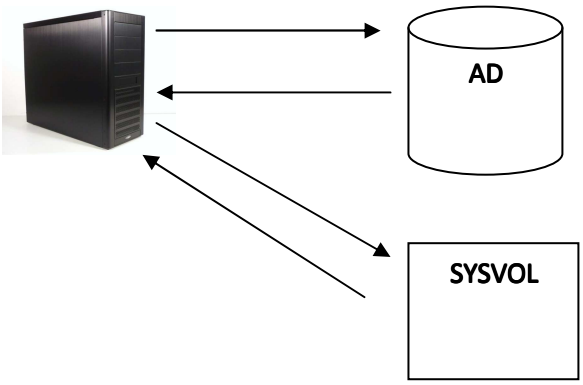
Elles peuvent s'appliquer à une machine, une OU, un groupe, un objet. Elles s'appliquent automatiquement toute les 90 à 120 minutes mais elles peuvent être forcée via la commande "**gpupdate /force**"

L'outil pour les administrer est Group policy Management. Le concept consiste à créer un template de police et puis de l'appliquer sur une OU.



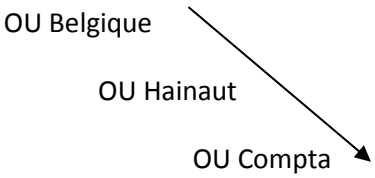
Fonctionnement





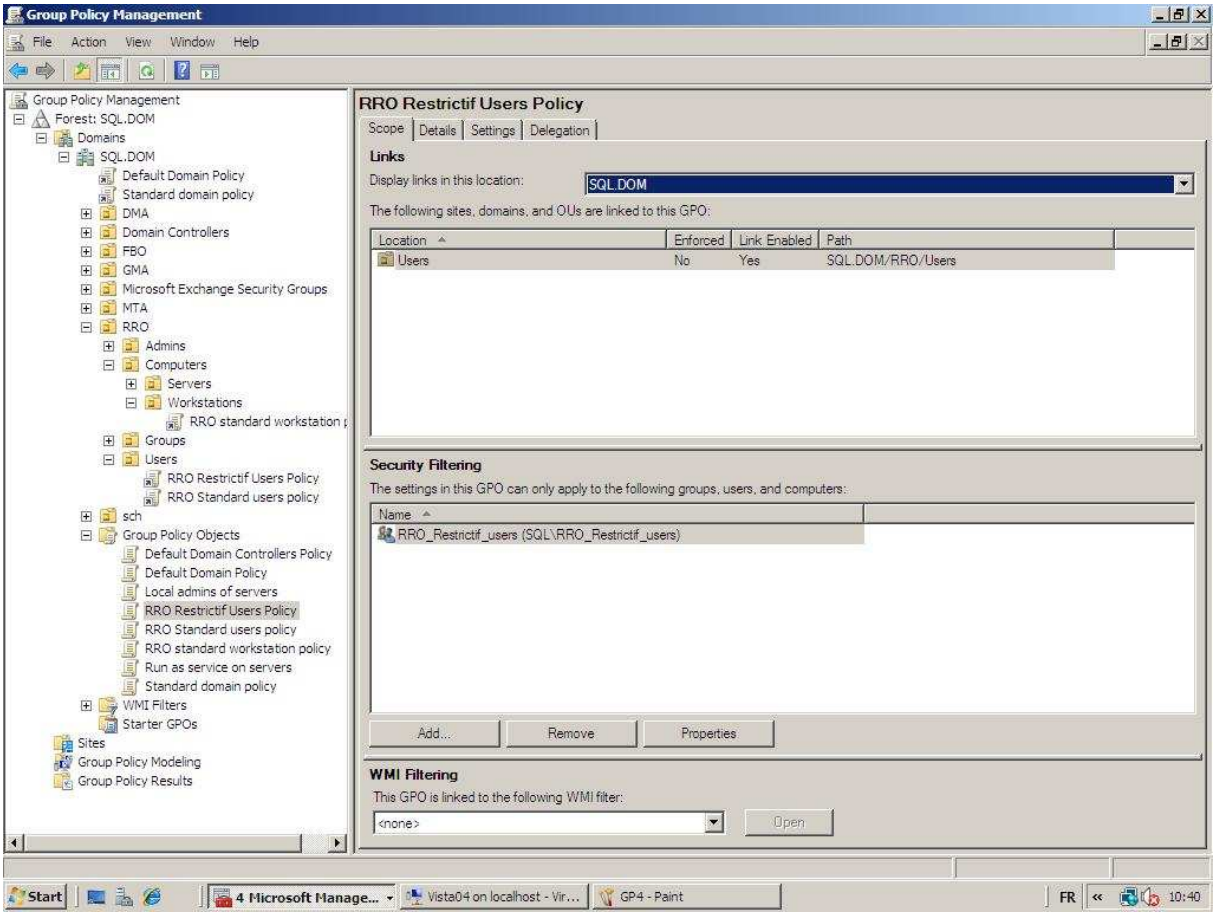
Les polices de sécurité ne sont en fait que des fichiers textes qui sont indexé dans l'active Directory. A chaque fois qu'un pc démarre ou qu'un utilisateur s'authentifie, il y a échange avec l'active Directory pour voir s'il y a eu des changements. Si c'est le cas, la machine télécharge les fichiers qui ont été ajoutés ou qui ont été modifiés. La commande « **gpupdate /force** » oblige la machine à télécharger de nouveau l'entièreté des fichiers textes.

Par défaut, une GPO s'applique à tout ce qui est en-dessous d'elle.



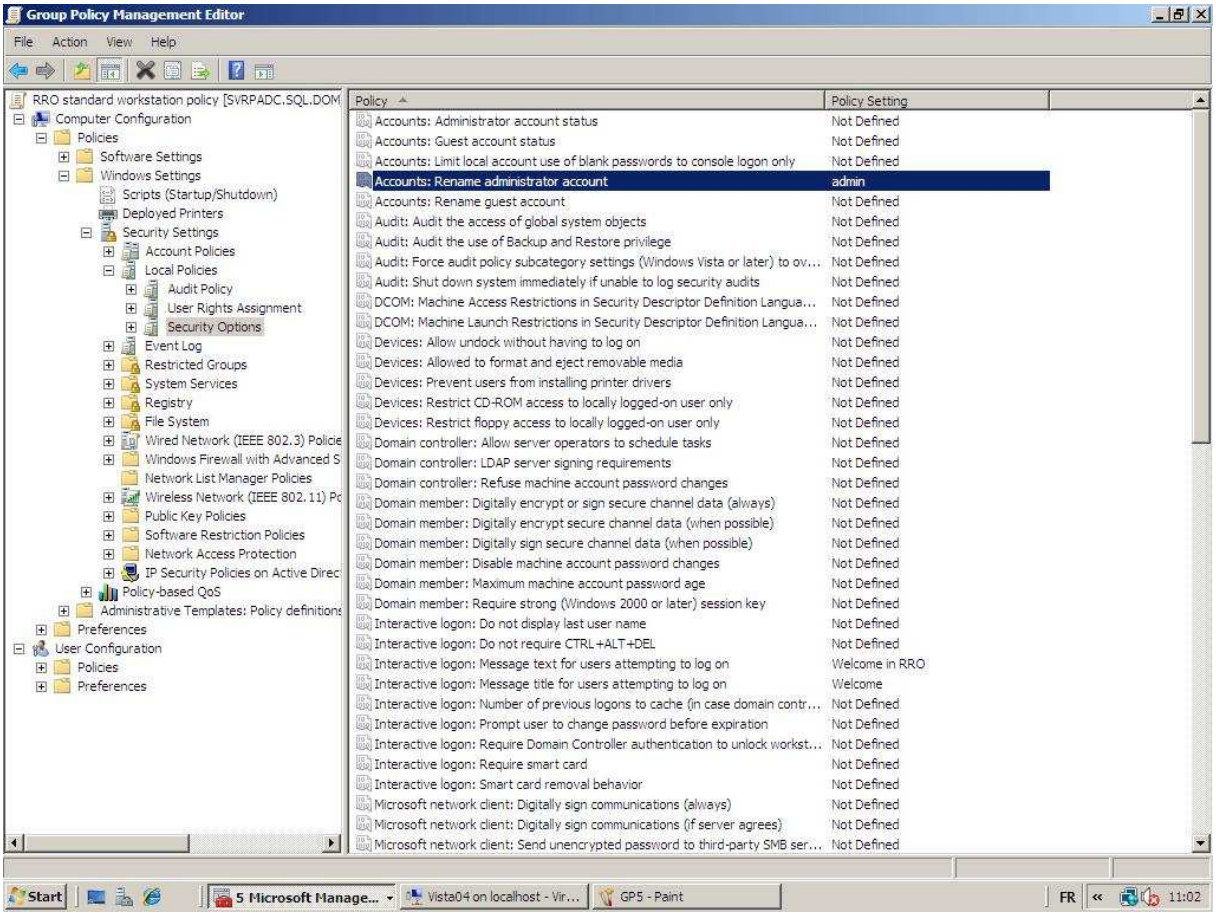
On peut néanmoins forcer le système pour que ce soit une police ascendante qui domine avec la commande force.

On peut également appliquer une policy à un groupe de personne. Pour ce faire, pendant l'édition de la GPO, il faut sélectionner propriété sur le nom de la GPO et mettre les droits nécessaires dans l'onglet sécurité.



Exemple de policy sur les computers :

On peut par exemple renommer les comptes de l'administrator local des machines mais on ne peut malheureusement pas changer son mot de passe. Pourquoi faire ça ? Simplement par ce que ce compte est connu par tout le monde et qu'il a tout les droits. On ne peut pas le bloquer car son SSID finit par 500.



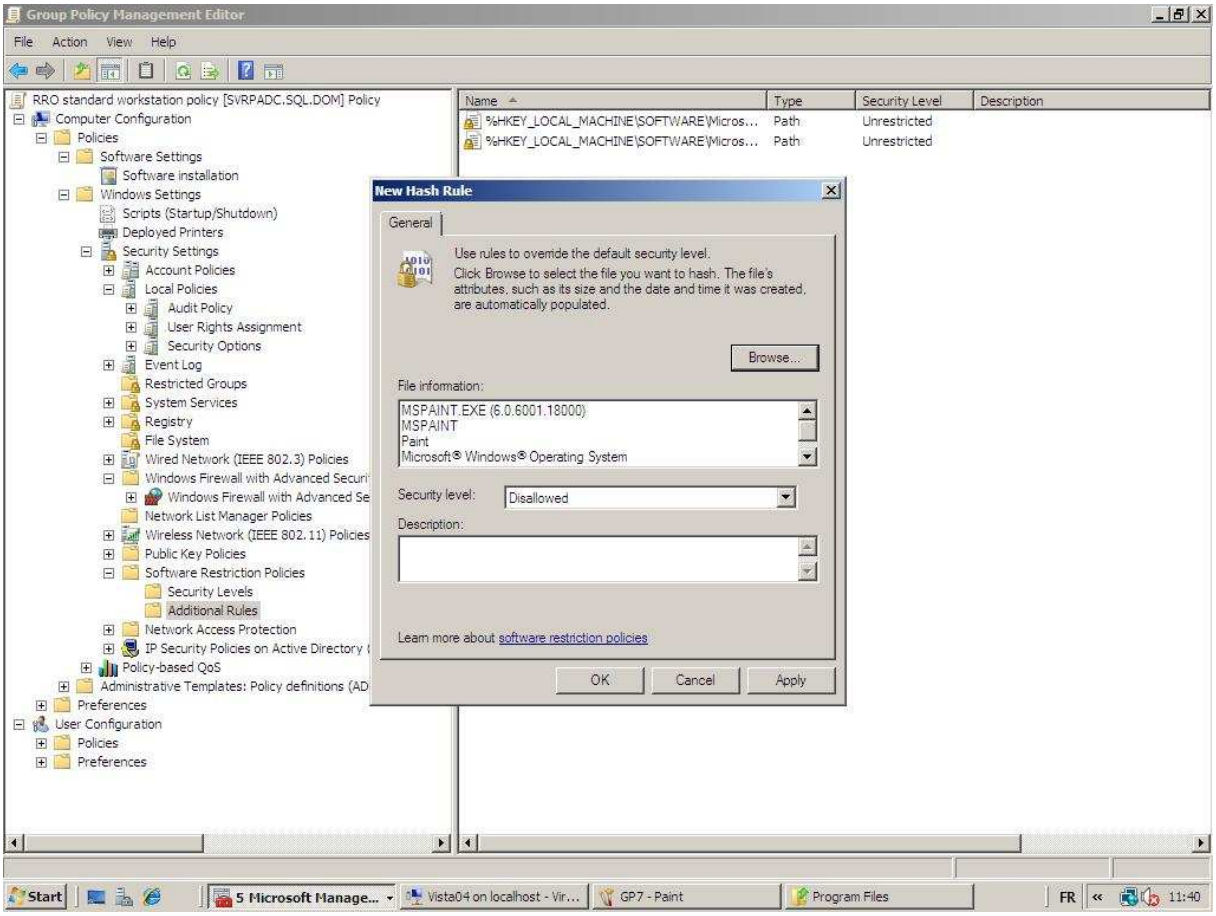
On pourrait aussi mettre le Number of previous logon pour empêcher les machines de se loger sans la présence d'un domaine. Surtout les Workstation qui n'ont pas besoin de cette option car une personne qui aurait son compte désactivé pourrait très bien se connecter à sa machine en retirant simplement le câble réseau. En désactivant cette option, il ne sera plus en mesure de se loger sur la machine.

On pourrait aussi injecter des groupes d'utilisateurs dans un groupe local sur des machines via le Restricted groups. Par exemple, l'équipe de l'Help-Desk qui a besoin d'avoir l'ensemble des droits admins en local pour effectuer des tâches de maintenance.

Il arrive parfois que certains programmes mal conçus doivent avoir les droits administrateurs pour s'exécuter. Il est bien entendu très dangereux de donner ces droits à des simples utilisateurs. Via les GP dans "File System", vous pouvez donner des droits sur certains répertoires des machines de votre parc sans pour autant donner plus de droits. Pour se rendre compte exactement des droits d'un programme, il faut le faire tourner en même temps que « **FileMon** » et « **RegMon** » (produit gratuit de Microsoft) qui donnent un rapport exact des accès du programme sur la machine.

On peut également bloquer des programmes via le software restriction policies qui se définit via des règles. Ces règles sont divisées suivant des certificats, des « network zone », des « path rule » et des « hash rule ». Le path rule permet de dire qu'on ne peut plus exécuter tel fichier exécutable mais on peut toujours contourner le problème en renommant l'exécutable à la différence du « Hash Rue »

qui fait d'une certaine façon une photo de l'exécutable. Il est alors impossible de lancer l'exécutable et ce même en le renommant.

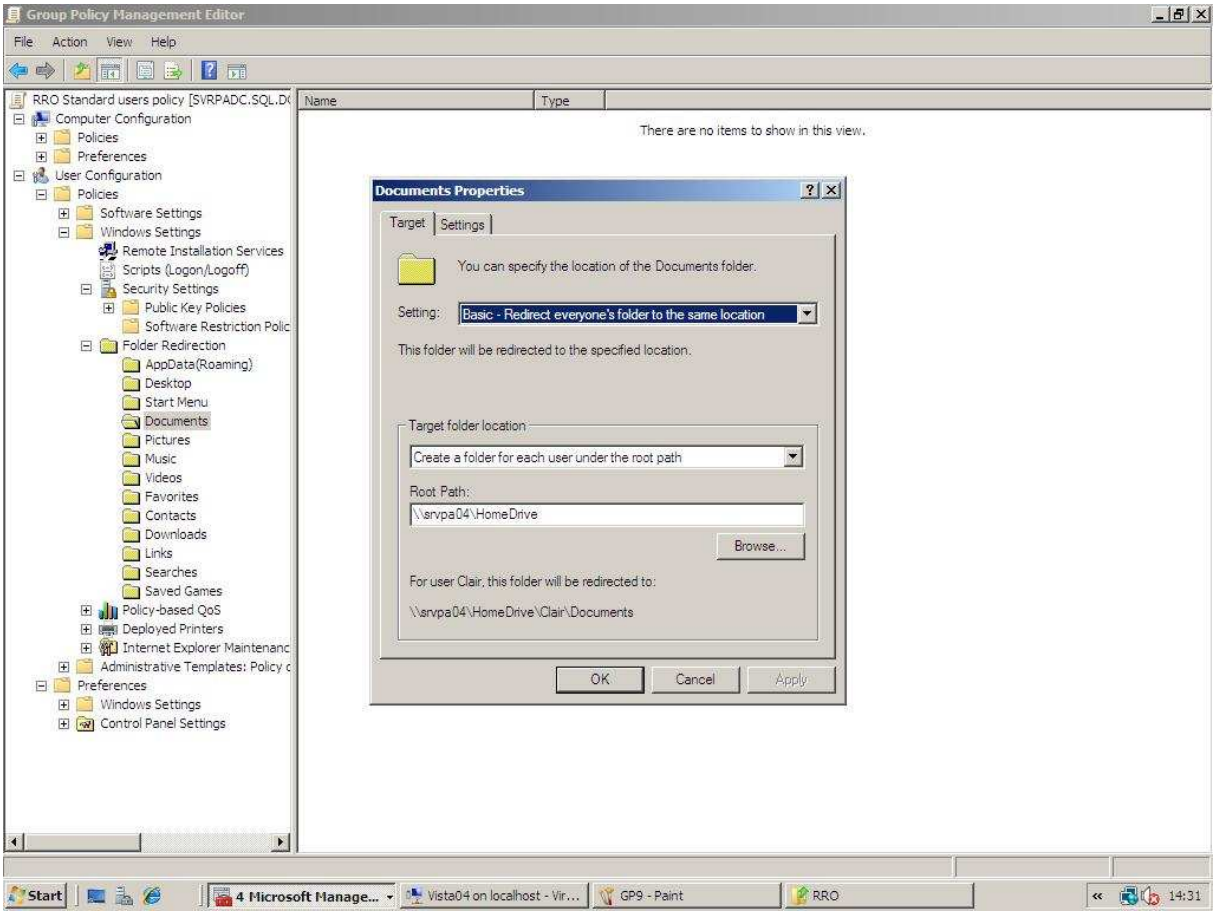


On peut limiter la bande passante d'un programme en upload sur le réseau via la « policy-based QOS ».

On peut alléger la charge réseau générée par les « Vista » et les « Seven » en désactivant les services Link-layer Topologie et Microsoft peer to peer dans l'administrative.

Exemple de GPO sur les utilisateurs :

Rediriger directement les « Mes documents » vers son Home Directory via le Folder Redirection.



Couper l'auto play via Windows components qui est souvent responsable de la propagation des virus.

Cacher certains drives via Windows explorer voir même de bloquer via le prevent acces to driver for my computer.

A chaque apparition d'un nouvel OS, des nouvelles GP font leurs apparitions. Nous avons vu que les GP ne sont en fait que des fichiers TXT avec l'information de la GP. Si vous voulez donc appliquer des nouveautés de GP, vous devez aller sur le nouvel OS et fabriquer directement la GP sur ce post via le RSAT. Cette GP s'appliquera à l'ensemble du parc qui est en mesure de supporter ces modifications. Il faut retenir que la GP doit toujours se faire sur l'OS le plus récent.

Les préférences

Nouveauté du système server 2008, les préférences permettent d'ajouter quelques fonctionnalités intéressantes aux GPO.

Policies	Preferences
Ne modifie jamais une clé de registre, elles placent une clé masque qui empêche les modifications par l'utilisateur.	Modifie directement les clés du registre. L'utilisateur peut remodifier les options mais elles seront réappliquées à chaque démarrage de la machine ou à chaque login.
Aucune installation sur les clients	Installation du Client Side Extension sur l'ensemble du parc informatique. (y compris sur les vista)
	Complément intéressant aux policies.

Quelques exemples de préférences computer :

Possibilité de recopier un dossier sur une machine automatique via les préférences.

Ajouter directement une clé dans la base de registre comme par exemple la clé qui offre la possibilité de restaurer un mail supprimé dans n'importe quel dossier. Fonctionne uniquement si on a un Exchange derrière.

Quelques exemples de préférences user :

Création automatique d'un mapping sans l'utilisation de script.

Toujours la possibilité de recopier ou modifier un répertoire, un fichier, une clé de registre mais limiter par les droits de l'utilisateur.

Modifier directement les folder options.

Password policy

Une Password policie ne peut s'attacher que sur le domaine. Si on l'attache sur une OU plus bas, ça ne sera appliqué que sur les comptes locaux. On peut quand même créer une police **Fine Grained PWD** sur des groupes d'utilisateurs mais il faut être totalement en domaine level 2008.

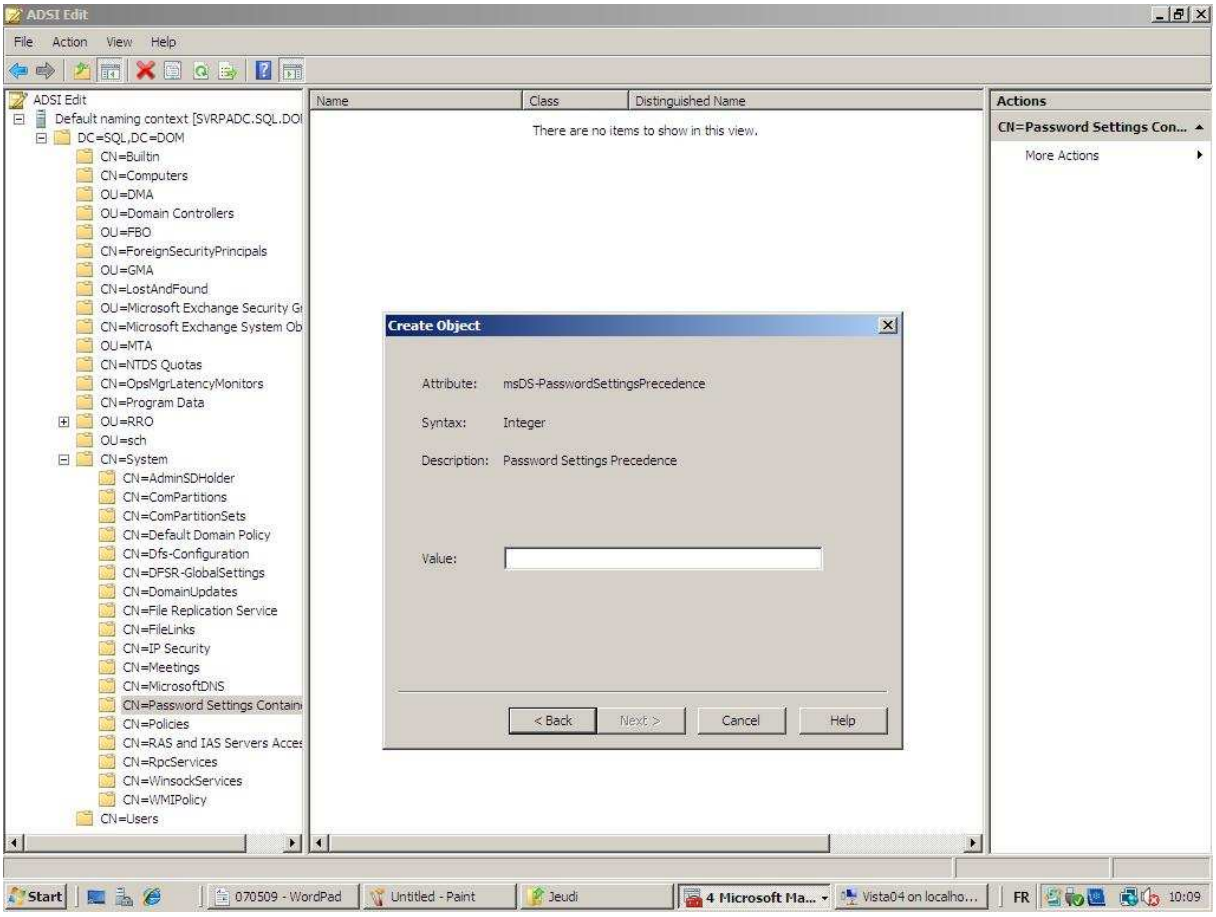
Quelques options :

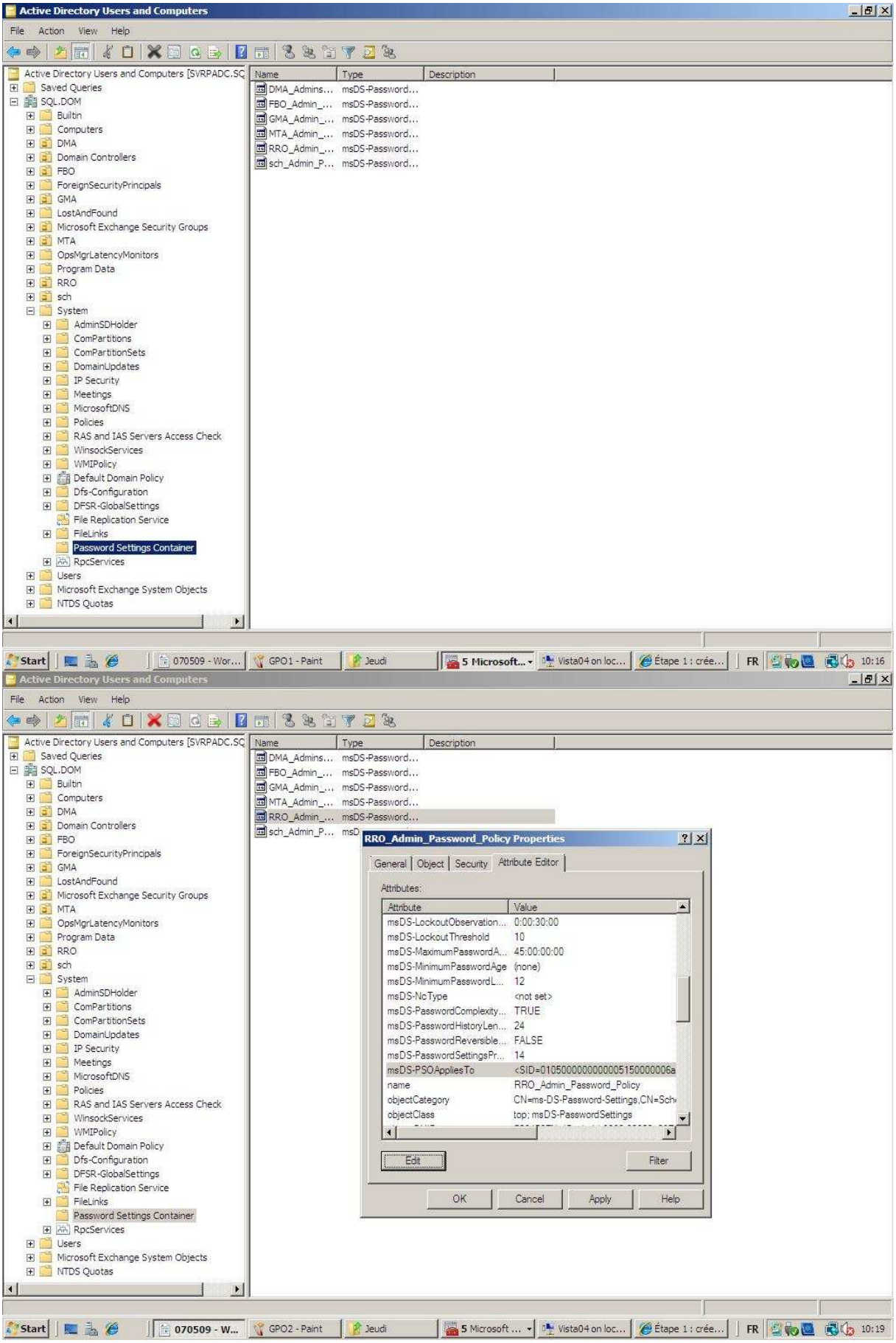
Account lockout duration : Bloque le compte pendant X minutes. Si on le met sur 0, c'est un blocage infini. Recommandation 30 min.

Account lockout threshold : Nombre d'erreurs qu'on permet à l'utilisateur. Recommandation entre 3 à 10 erreurs.

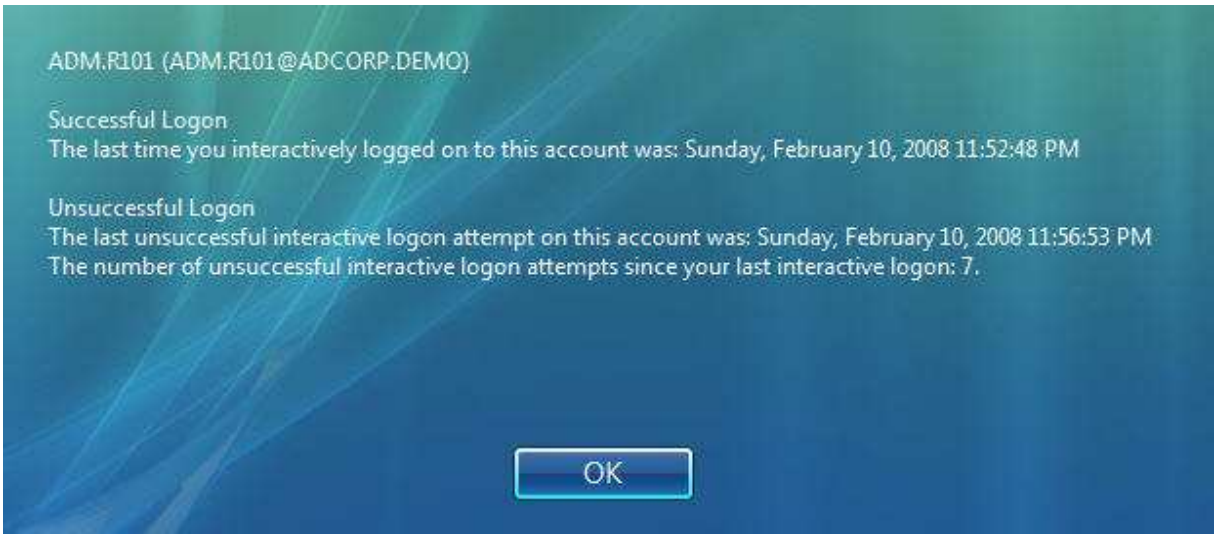
Reset account lockout counter after : Temps d'observation des erreurs. Exemple : 30 minutes

Fine Grained PWD : Pour ce faire, il faut utiliser **ADSI Edit** (sorte de registery pour l'AD) qui permet de voir l'ensemble des attributs de l'AD et de les modifier. Il faut aller sur le container System, Password Settings container, création d'un nouvel objet. La première valeur permet seulement de donner un ordre entre différentes policie. Les autres valeurs représentent la configuration de celle-ci. Une fois la police créée, il faut l'appliquer dans l'active directory au même endroit et aller sur les propriété et puis dans l'onglet Attribute Editor à la ligne msDS-PSOAppliesTO et rajouter le compte ou le groupe. La dernière étape consiste à forcer les gens à changer les mots de passe pour que celle-ci soit appliquée.


ADSI Edit
File Action View Help
ADSI Edit
Default naming context [SVRPADC.SQL.DOM
DC=SQL,DC=DOM
CN=Builtin
CN=Computers
OU=DMA
OU=Domain Controllers
OU=FBO
CN=ForeignSecurityPrincipals
OU=GMA
CN=LostAndFound
OU=Microsoft Exchange Security Gr
CN=Microsoft Exchange System Ob
OU=MTA
CN=NTDS Quotas
CN=OpsMgrLatencyMonitors
CN=Program Data
OU=RRO
OU=sch
CN=System
CN=AdminSDHolder
CN=ComPartitions
CN=ComPartitionSets
CN=Default Domain Policy
CN=Dfs-Configuration
CN=DFSR-GlobalSettings
CN=DomainUpdates
CN=File Replication Service
CN=FileLinks
CN=IP Security
CN=Meetings
CN=MicrosoftDNS
CN=Password Settings Contain
CN=Policies
CN=RAS and IAS Servers Acces
CN=RpcServices
CN=WinsockServices
CN=WMIPolicy
CN=Users
Name
Class
Distinguished Name
There are no items to show in this view.
Actions
CN=Password Settings Con...
More Actions
Create Object
Attribute: msDS-PasswordSettingsPrecedence
Syntax: Integer
Description: Password Settings Precedence
Value:
< Back
Next >
Cancel
Help
Start
070509 - WordPad
Untitled - Paint
Jeudi
4 Microsoft Ma...
Vista04 on localho...
FR
10:09


Active Directory Users and Computers
File Action View Help
Active Directory Users and Computers [SVRPADC.SQ
Saved Queries
SQL.DOM
Builtin
Computers
DMA
Domain Controllers
FBO
ForeignSecurityPrincipals
GMA
LostAndFound
Microsoft Exchange Security Groups
MTA
OpsMgrLatencyMonitors
Program Data
RRO
sch
System
AdminSDHolder
ComPartitions
ComPartitionSets
DomainUpdates
IP Security
Meetings
MicrosoftDNS
Policies
RAS and IAS Servers Access Check
WinsockServices
WMIPolicy
Default Domain Policy
Dfs-Configuration
DFSR-GlobalSettings
File Replication Service
FileLinks
Password Settings Container
RpcServices
Users
Microsoft Exchange System Objects
NTDS Quotas
Name
Type
Description
DMA_Admins...
FBO_Admin_...
GMA_Admin_...
MTA_Admin_...
RRO_Admin_...
sch_Admin_P...
msDS-Password...
Start
070509 - Wor...
GPO1 - Paint
Jeudi
5 Microsoft...
Vista04 on loc...
Étape 1 : crée...
FR
10:16
Active Directory Users and Computers
File Action View Help
RRO_Admin_Password_Policy Properties
General
Object
Security
Attribute Editor
Attributes:
Attribute
Value
msDS-LockoutObservation...
0:00:30:00
msDS-LockoutThreshold
10
msDS-MaximumPasswordA...
45:00:00:00
msDS-MinimumPasswordAge
(none)
msDS-MinimumPasswordL...
12
msDS-NcType
<not set>
msDS-PasswordComplexity...
TRUE
msDS-PasswordHistoryLen...
24
msDS-PasswordReversible...
FALSE
msDS-PasswordSettingsPr...
14
msDS-PSOAppliesTo
<SID=0105000000000005150000006a
name
RRO_Admin_Password_Policy
objectCategory
CN=ms-DS-Password-Settings,CN=Sch
objectClass
top; msDS-PasswordSettings
Edit
Filter
OK
Cancel
Apply
Help
Start
070509 - W...
GPO2 - Paint
Jeudi
5 Microsoft ...
Vista04 on loc...
Étape 1 : crée...
FR
10:19

Public last logon information " ('windows componement \ windows logon options à activé sur le domain et sur OU des PC) qui ne fonctionne qu'avec Vista ou Seven. Cette option permet de voir quand on s'est authentifié la dernière fois avec succès et quand la dernière fois, il y a eu quelqu'un qui a essayer de se connecter sans succès avec son login.



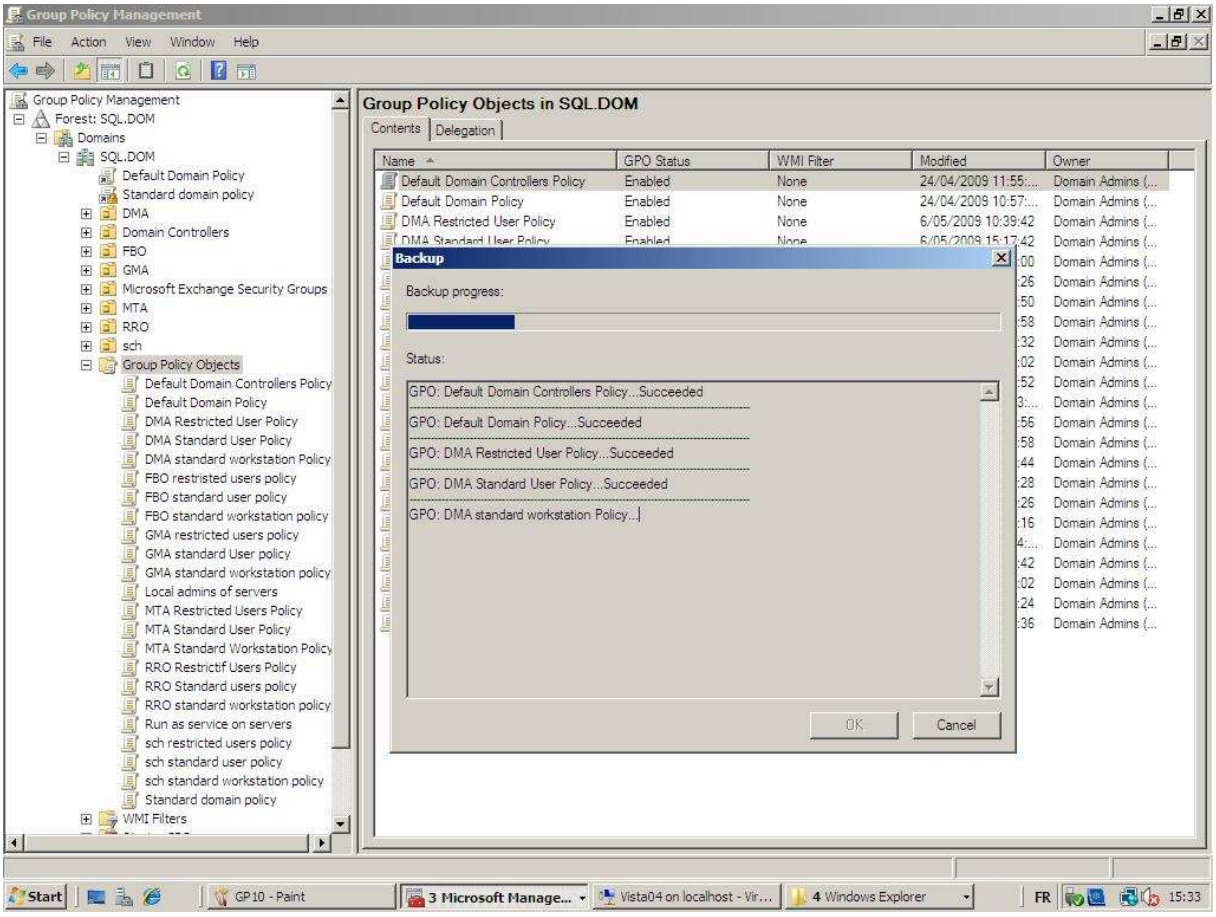
Outils pratique : Admodify.net qui permet d'éditer les attributs de tous les objets qu'on désire.

GPO Management (nouveauté de 2008)

Mise en place d'une fonction de recherche dans les polices mais la version actuelle ne fonctionne pas bien. On peut espérer la correction de ce problème avec le R2.

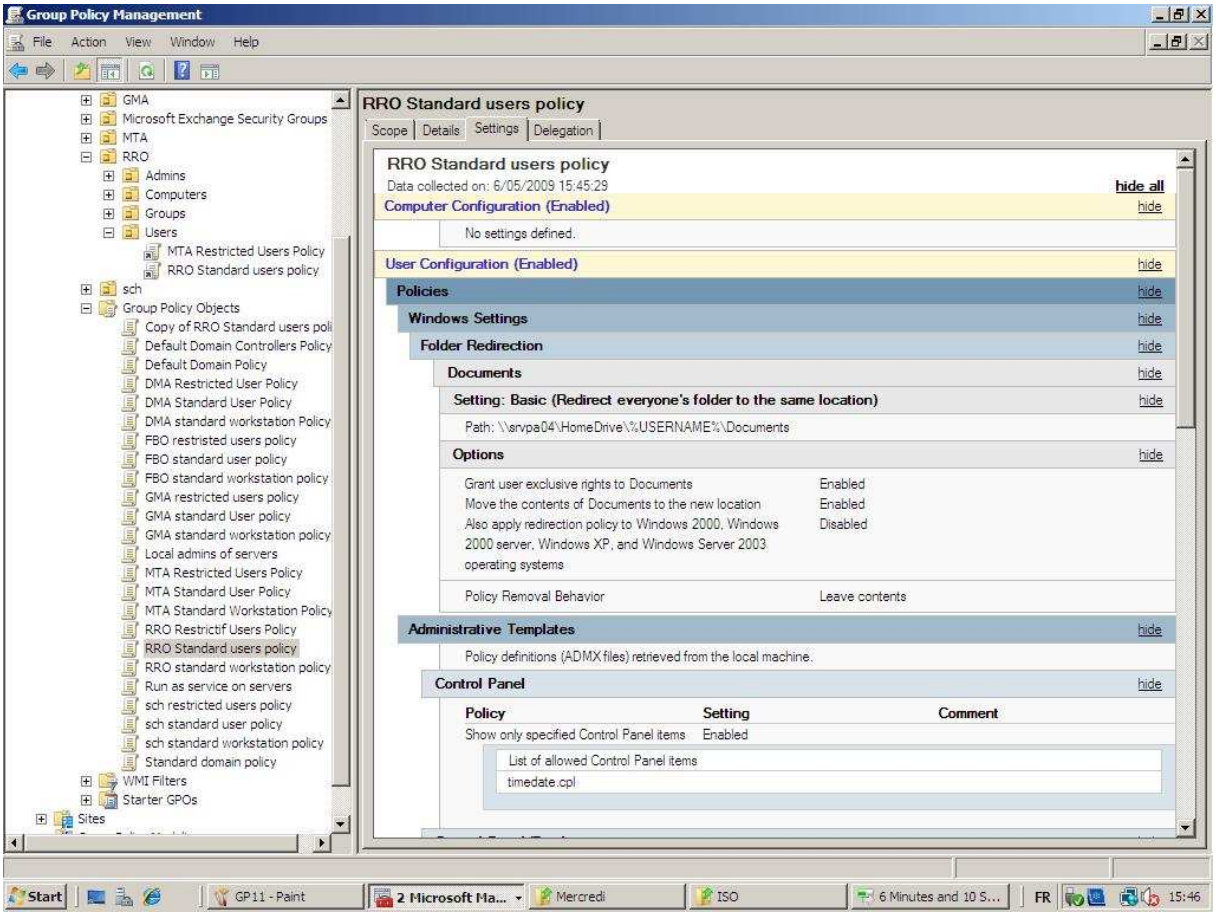
Ajouter des commentaires sur les GPO ce qui est très utile pour la documentation.

Système de backup et de restore des GPO. Attention, après une restauration, il ne faut pas oublier de rattacher la police a son OU.



Possibilité de copier des GPO entre différents domaines ou forêt.

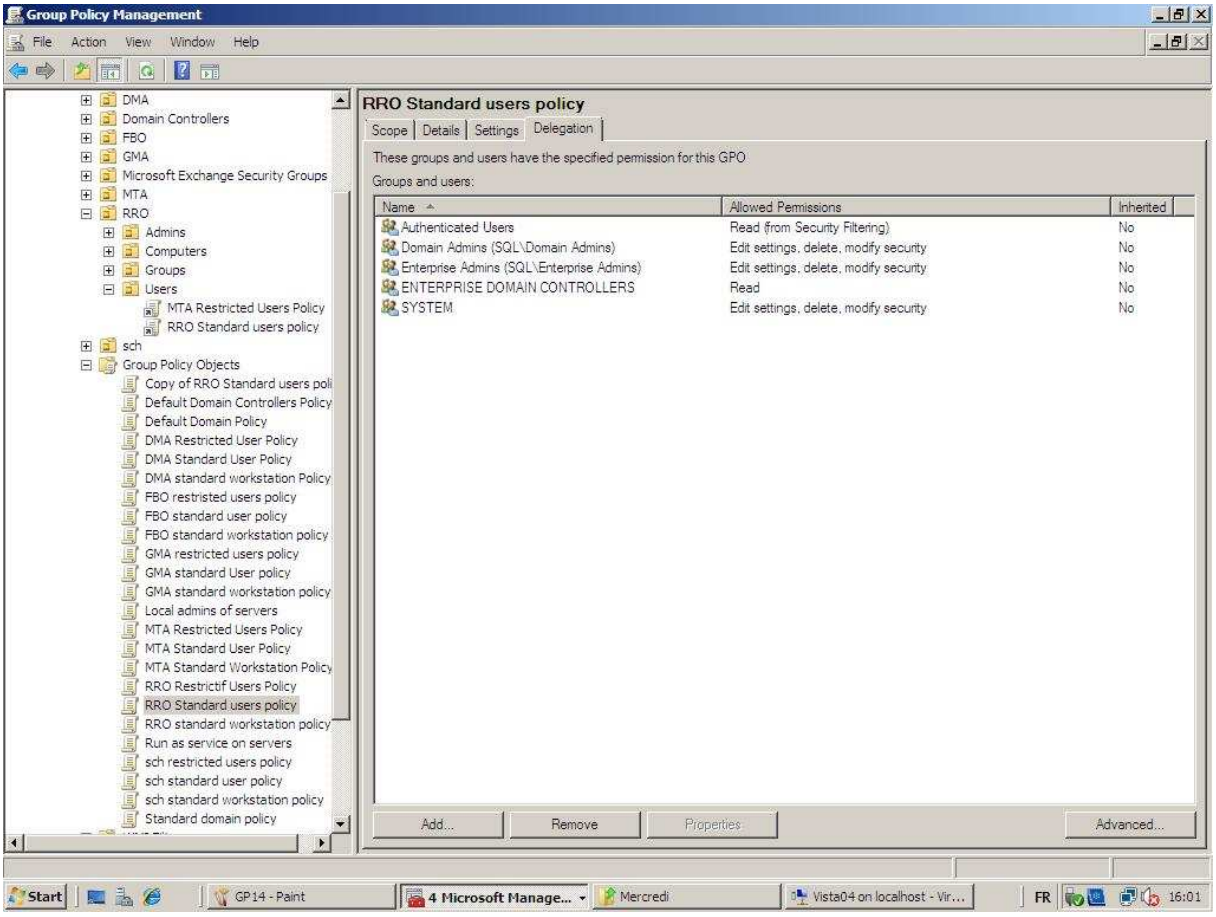
Le RSOP permet de faire de la documentation. La fonctionnalité est directement accessible sur le template dans l'onglet Settings.



Le modeling qui permet de faire une simulation avec un user X sur une machine Y.

Le group Policy Results qui ne fonctionne que si la personne s'est déjà authentifiée sur la machine. Le rapport généré donne les erreurs provoquées lors de l'application de la police. Il tient compte de l'event viewer de la machine.

La possibilité de faire une délégation de droit sur la GPO. Pour ce faire, il faut ajouter le user dans le groupe **Policy creator owners** de l'AD. Il faut également avoir le droit d'attacher la police sur une OU. Par contre, il ne pourra modifier que les polices dont il est le propriétaire et inversement pour les autres membres de ce groupe. Il faudra donc faire une délégation des GPO vers les autres admins.



Migration Server 2003 vers Server 2008 AD

Situation de départ : 2 Domain Controller en 2003 auquel on ajoute un Domain Controller 2008

Pré-requis migration avant de mettre un 2008 dans la forêt

- Le domain level doit être en minimum en 2000 natif. On ne peut donc plus être en 2000 mixte ou 2003 intérim. On peut voir ça directement dans l'Active directory dans les propriétés du domain et on peut le changer via la commande Raise Domain Functional Level.

- " Run adprep /forestprep " via le CD de 2008 1 fois par forêt. Il ajoute des nouveaux attributs et des objets.

- " Run adprep /domainprep " via le CD de 2008, 1 fois par domain. Il ajoute des nouveaux groupes et la sécurité en fonction de ces groupes.

- " Run adprep /gpoprep " uniquement si le domaine est encore en 2000. Il fait des modifications au niveau de la réplication des GPO.

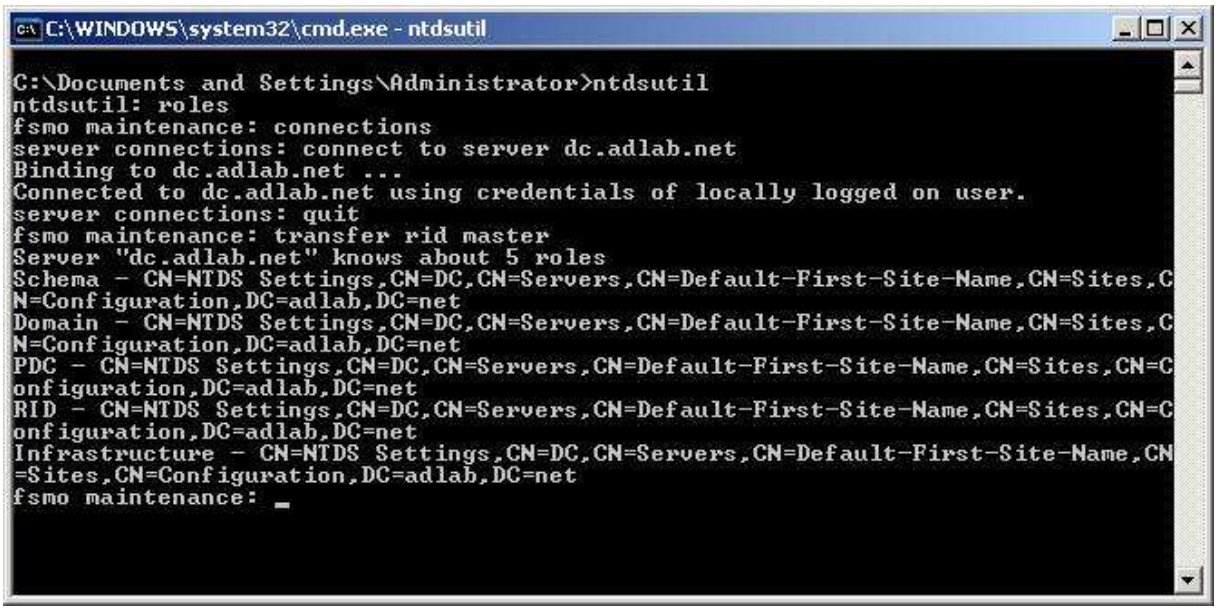
- " Run adprep /rodcprep " uniquement si on veut des RODC (Read Only Domain Controller)

Migration

Etape 1 : Ajouter un domain Controller 2008 via la commande " DCPROMO ". Il est conseiller d'attendre un ou deux jours pour être sûr qu'il soit bien intégré dans la forêt.

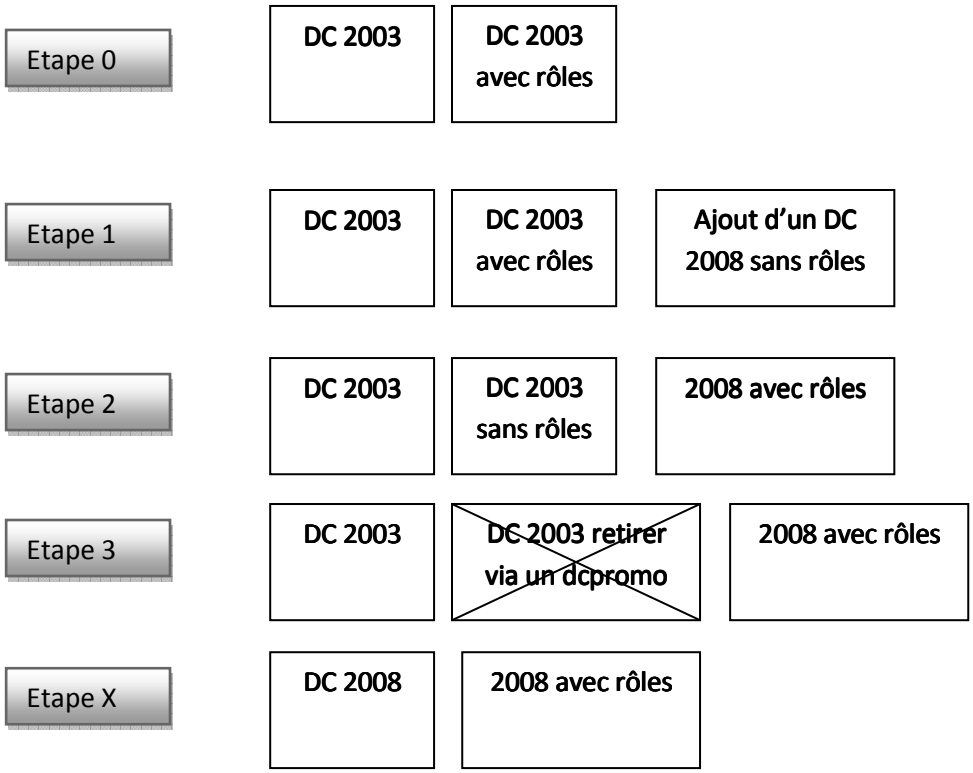
Etape 2 : Déplacer les rôles vers le 2008. Les rôles sont retirés du serveur source et transféré vers le serveur destination. Pour éviter d'oublier des rôles, il vaut mieux le faire en ligne de commande via " ntdsutil " (permet de faire des tâches sur un DC). Vérifier qu'il est bien en global catalog. Il est conseillé d'attendre un ou deux jours pour être sûr qu'il joue bien ses différents rôles.

\ntdsutil
\roles
\connect
\con to server "DC2008"
\quit
\transfert infrastructure master
\transfert naming master
\etc (Bien vérifier les rôles avant de le faire)



Etape 3 : Rajouter un autre DC 2008 ou Retirer un Server 2003 mais avant tout, il faut faire un DCPROMO pour le retirer l'AD.

Etape 4 : Une fois qu'on n'a plus d'autres Domaines Controller en ancien OS, on peut changer le domain functionnal level. Pour bénéficier de toutes les options de 2008 comme le " **Fine Grained PWD** " ou encore la GPO " **Public last logon information** ".



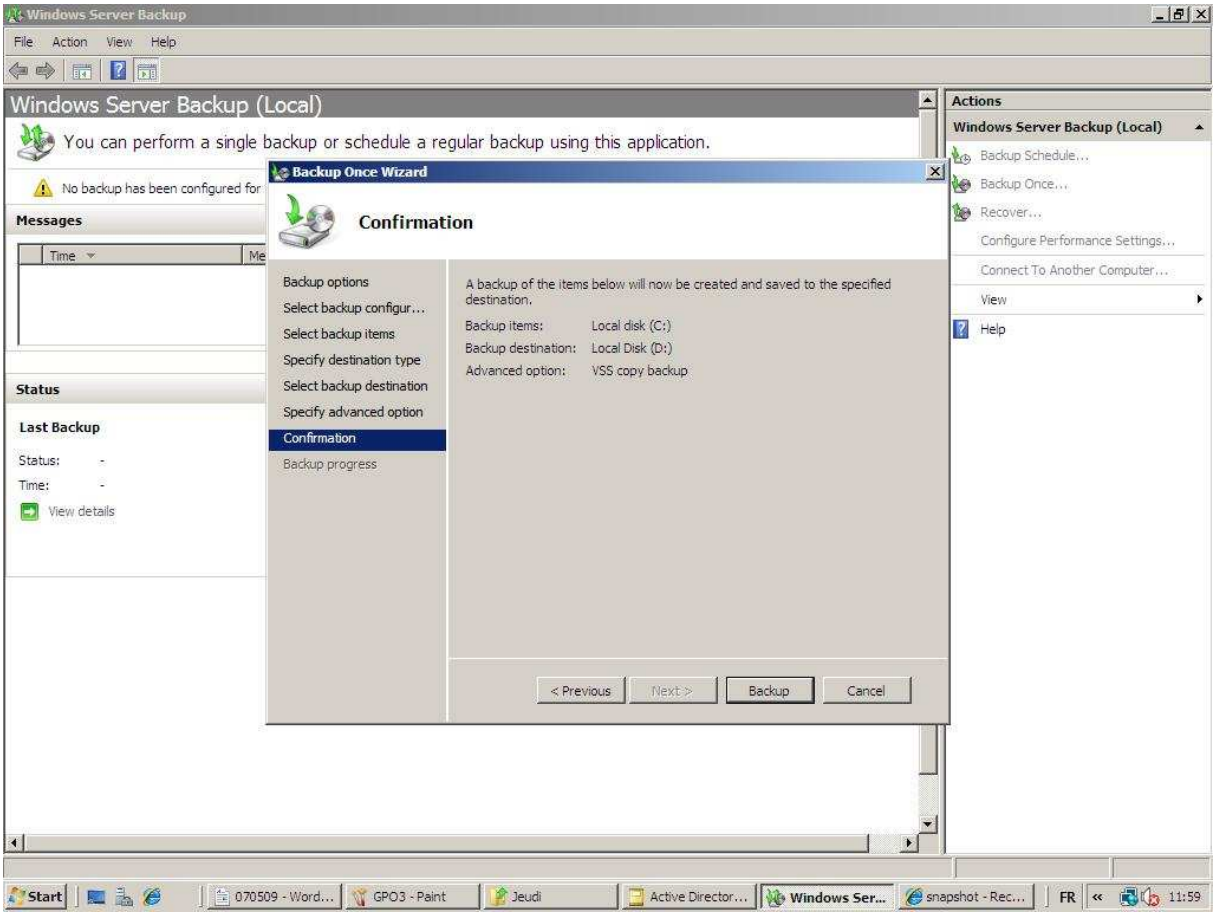
Inconvénient

Lors de la migration, il garde les sécurités de l'ancien système. Il faut revoir les polices de sécurité du domaine pour les mettre aux goûts du jour.

Backup Server 2008

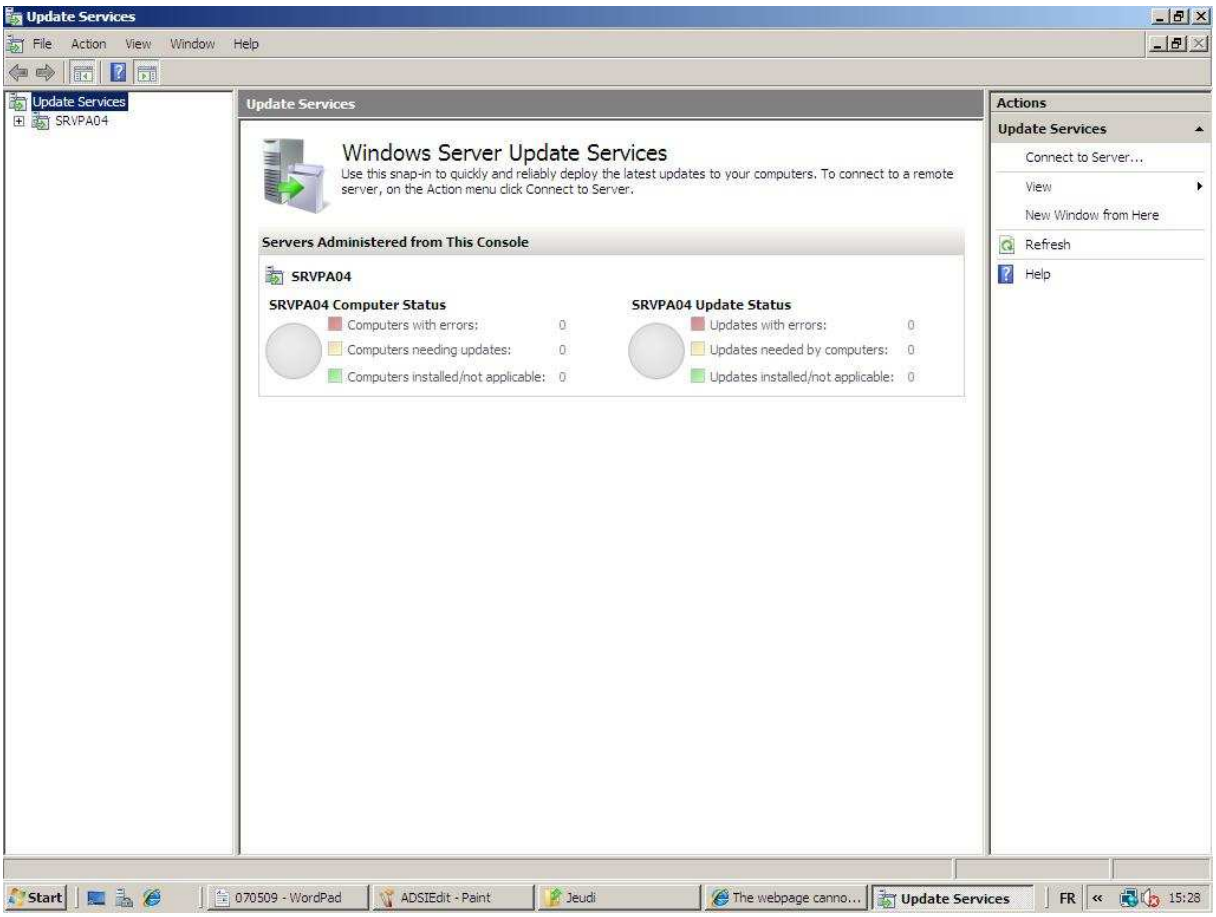
- L'ancien NTbackup travaillait au niveau des fichiers. On savait faire des backups et restaurer d'une partition, d'un répertoire ou d'un fichier. Le restaure système était très difficile car il fallait réinstaller le Windows de base et les drivers avant d'appliquer le restore.

- Windows Server Backup 2008 travail au niveau des clusters (fonction snapshot). On ne sait que prendre des partitions au niveau du backup. Par contre, il est bien entendu possible de restaurer seulement un répertoire, un fichier ou l'ensemble de la partition. Le restore système s'exécute via le DVD de 2008 et on lui donne le chemin du backup. La phase de réinstallation est supprimée ou du moins, elle se fait automatiquement avec les données backup.



Lors de la restauration, il faudra peut être rajouter les drivers dans le DVD de 2008 pour qu'il reconnaissance le matériel de stockage. Pour ce faire, il faudra modifier le fichier boot.wim du DVD via le " **windows automatique installation kit** " version serveur 2008. Ce fichier boot.wim est responsable du lancement du Windows PE chargé en mémoire. Celui-ci sert à réinstaller le système ou à utiliser des outils comme le restore de backup. Le même fichier install.wim existe pour que des drivers ou des patchs soient déjà compris dans l'installation de base. Le fait de fonctionner avec des fichiers .wim qui sont des images augmente les performances lors de l'installation en comparaison à un Server 2003.

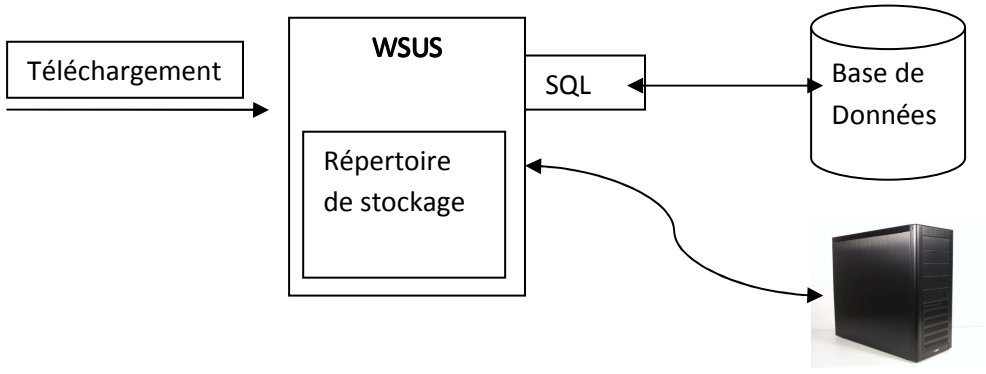
W.S.U.S (Microsoft Windows Server Update Services version 3 SP1)



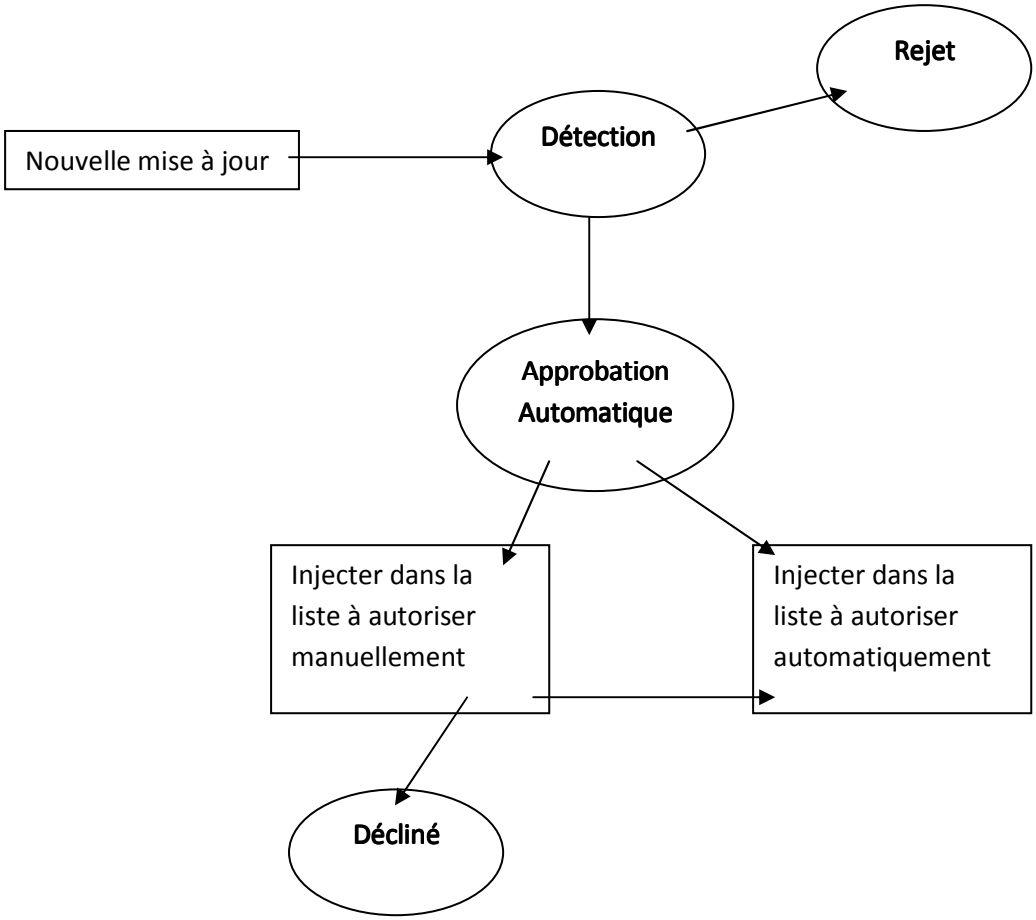
Le but du WSUS est de limité la charge réseau mais aussi de mettre en place une politique d'application des patchs car on peut choisir les patchs qu'on désire appliquer ou non. WSUS permet d'avoir un parc informatique homogène.

Le réseau risque par contre d'être un peu plus lent lors de la mise en place car l'ensemble des machines va se mettre à jour. Il y a également des petits soucis quand on a plusieurs équipes qui doivent gérer les mise à jours. Il vaut mieux dans ce cas d'en avoir un par équipe.

Il faudra prévoir sur le serveur un IIS, un SQL et un grand espace disque pour stocker les patchs et le " report viewer 2005 ". On retrouvera dans la base de données, la configuration du WSUS, la liste des machines, la liste des patchs, le reporting pour savoir quelle machine à quel patch.



Fonctionnement



Configuration

Dans la pratique, il vaut mieux éviter le Wizard de WSUS pour la configuration car celui-ci skip l'Automatic Approvals. Pour le configurer, il faut aller dans "Options".

Etape 1 - Configuration de la source : Configuration de la source via " **Update Source and Proxy Server** ". La source peut être Microsoft ou un autre WSUS et on peut configurer le serveur proxy si nécessaire.

Etape 2 - La détection : Sélection des produtis et la classification via " **Products and Classificaions** " qui devra se faire en deux étapes car tant qu'il n'a pas synchronisé une première fois avec les serveurs de Microsoft ou l'autre WSUS la liste des produits n'est pas complète. La classification sert à être prévenu des types de mise à jour de notre choix (peut être décocher les drivers). On doit également configurer la détection dans " **Update Files and Languages** ". Il faut limiter le plus possible les langues d'updates.

Etape 3 - Automatic Approvals : Il faut editer le default Automatic en sélectionnant les types de mises à jours automatiquement autorisées. Il est recommandé de sélectionner le critical updates, security updates, definition updates, updates. Le reste doit être en manuel.

Etape 4 - Synchronisation : Définir quand il regarde les mise à jours.

Etape 5 - E-mail Notifications : Eventuellement mettre un reporting par mail.

Etape 6 - Les groupes d'ordinateurs : Eventuellement la configuration de groupe d'ordinateur. Elle se fait soit à la main ou soit par Registry.

Etape 7 - Configuration de la partie client : Elle se réalise via une **GPO** dans "computer \ administrative templates \ windows components \ windows update "

Deux GPO selon la catégorie de machine : Server et Workstation

Server :

Configure Automatic updates properties choisir le 3. On peut laisser l'heure.
Specify Intranet Microsoft Update Service location : Exemple : http//srvpa04:8530 (selon le port choisit) Si on ne met pas ça, les clients vont directement sur le site de Microsoft et ne passe pas par Wsus.

Workstation :

Configure Automatic updates properties choisir le 4. On peut laisser l'heure.
Specify Intranet Microsoft Update Service location : http//srvpa04:8530
Reschedule Automatic Updates scheduled installations : Enabled 5 minutes (dans le cas ou si la machine était coupée lors de l'update)
No auto-restart with logged on users for scheduled automatic updates installation : Enable
Re-prompt for restart with scheduled installations : Enabled 120 minutes par exemple
Allow Automatic Updates immediate installation : Enabled

Rappel : Il est importance d'avoir des OU séparée.

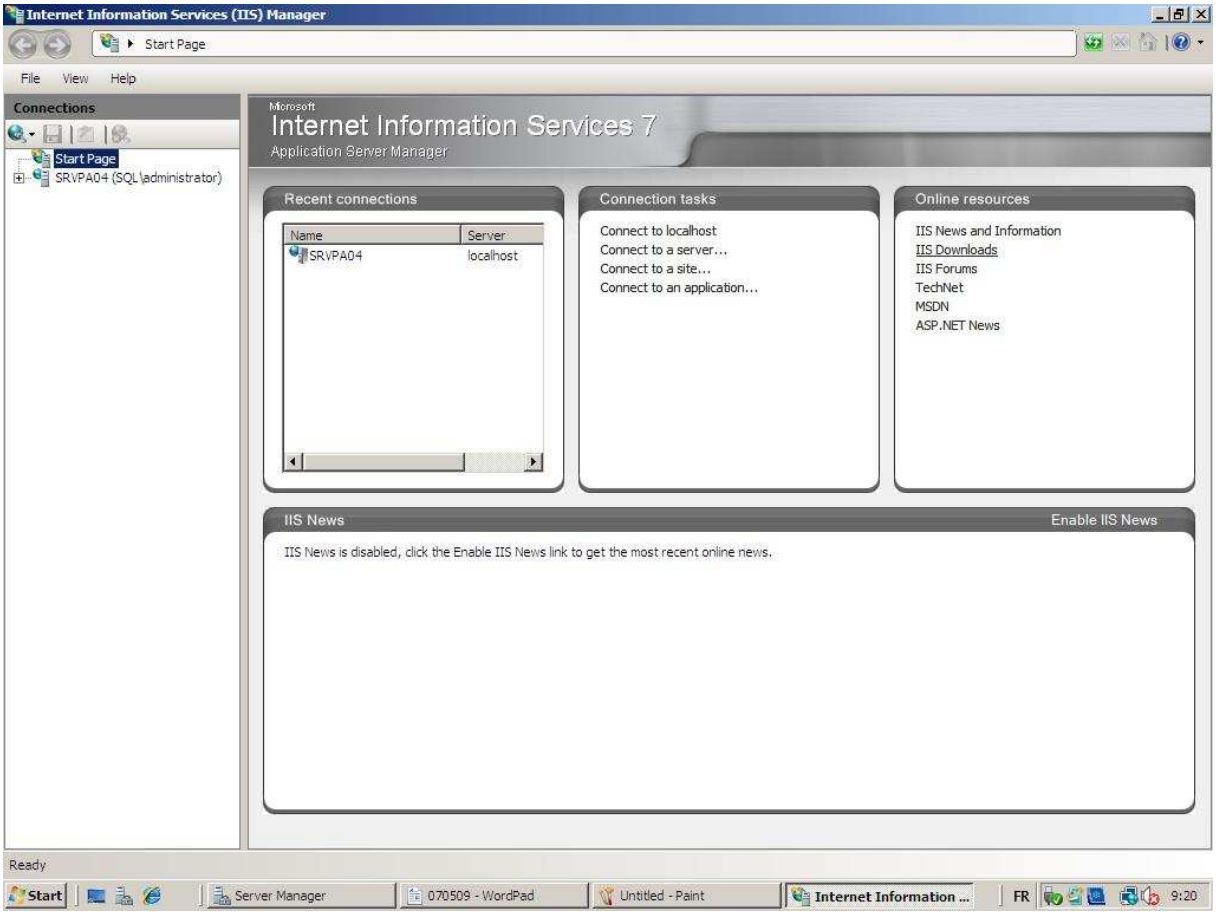
Etape 8 - Regarder régulièrement les patchs qui n'ont pas été autorisés automatiquement selon vos préférences.

Etape 9 - Faire un wizzard cleaned quand on n'a plus aucune machine d'un OS.

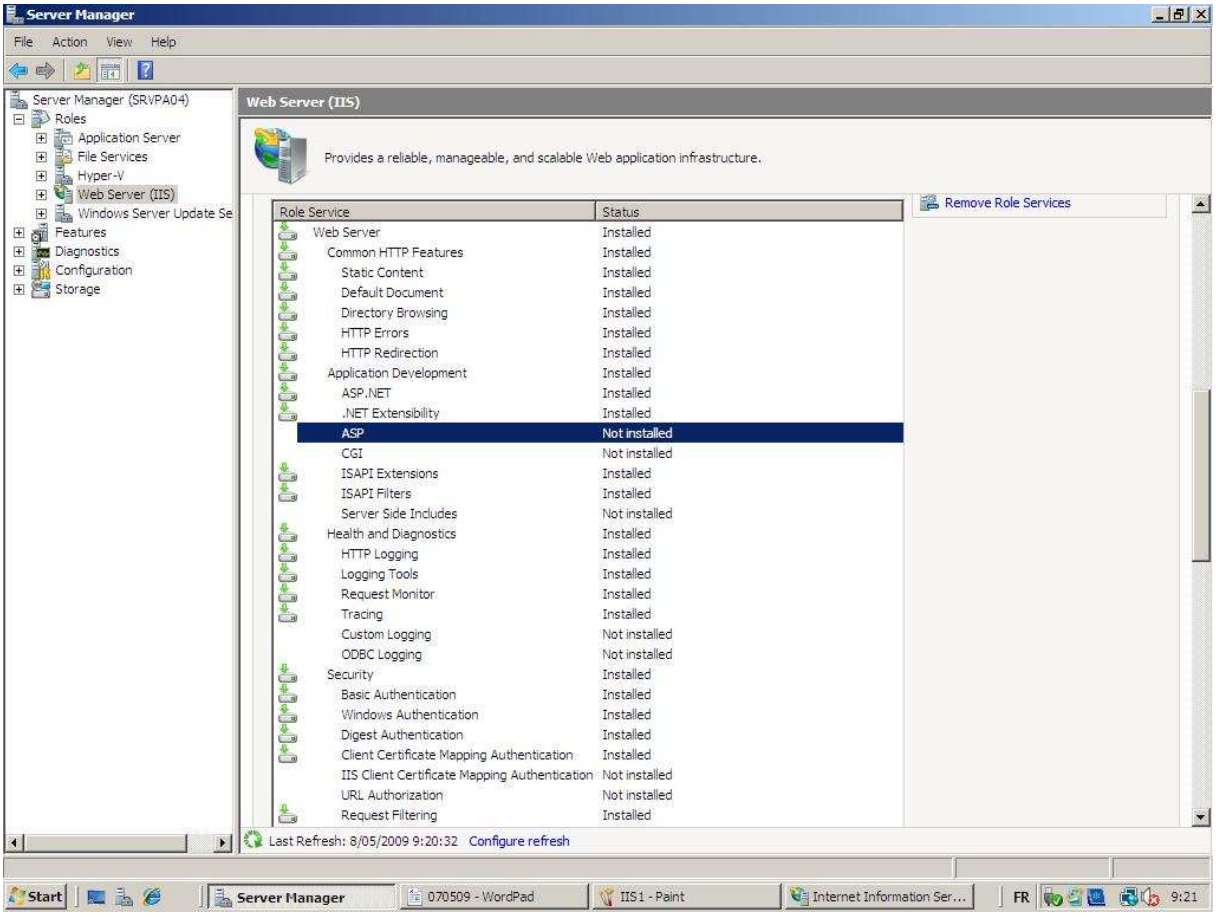
Par défaut dans la version SMB 2008, il est installé. Attention, il faut que le SSID de la machine soit bien différent d'une machine à l'autre. Attention donc lors de l'utilisation des ghost, il faudra bien prévoir un " sysprep " pour différentier les machines.

Note : Vu les données, celles-ci peuvent tout à fait être stocké sur un simple disque. Inutile de prévoir du RAID5 pour ce genre de chose. L'idéal est de partir sur un disque de 250 Giga.

IIS

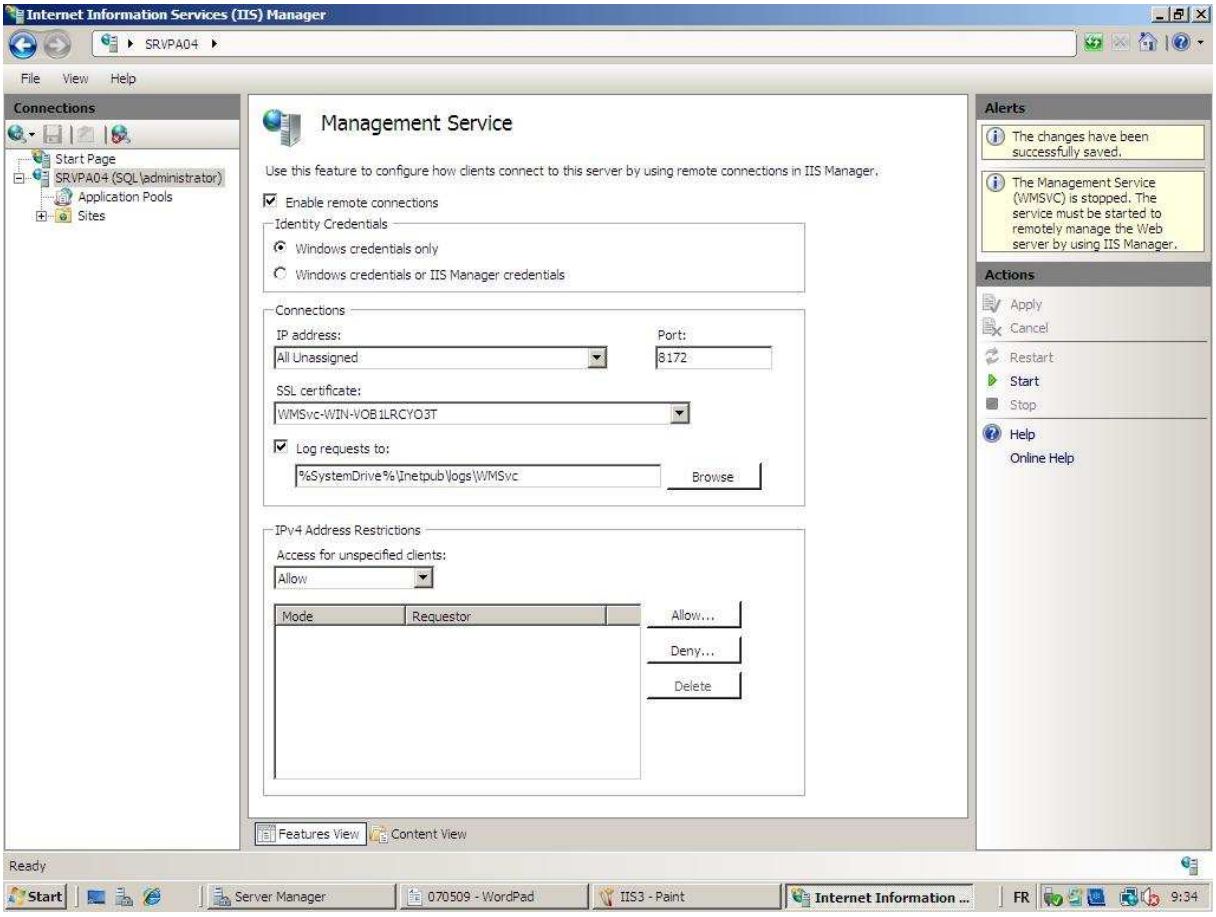


Par défaut celui-ci n'est pas installé. Toutes les options doivent être installées et activées manuellement même celles qui étaient présentes de base en Server 2003 comme l'authentification, la restriction d'IP ou le remote management.



Deux outils d'administrations d'IIS "Internet Information Services (IIS) 6.0 Manager" et le "Internet Information Services (IIS) Manager". Le premier sert principalement à configurer le FTP qui n'a pas changé depuis 2003.

La nouvelle version d'IIS apporte beaucoup de changements surtout dans la gestion à distance. Lors de l'installation celle-ci n'est pas activé et même après installation de cette option, le IP$ port 445 ne fonctionne plus. Deux possibilités pour l'administrer, la classique Remote Desktop qui ne demande pas d'installer le « management service d'IIS » ou l'autre possibilité serait d'installer cette option à IIS. Pour se connecter à IIS via le "management service», il faut par exemple avoir un Vista avec le RSAT. On peut également faire des délégations via " IIS Manger Permissions "sur un site web pour des webmasters par exemple.



Autre nouveauté intéressante le " Output Caching " qui permet de faire un cache des pages fort demandées.

Fonctionnalités

SSL

Le but de SSL est de crypter le trafic mais également selon les certificats d'être reconnu dans certain cas.

La création d'un certificat :

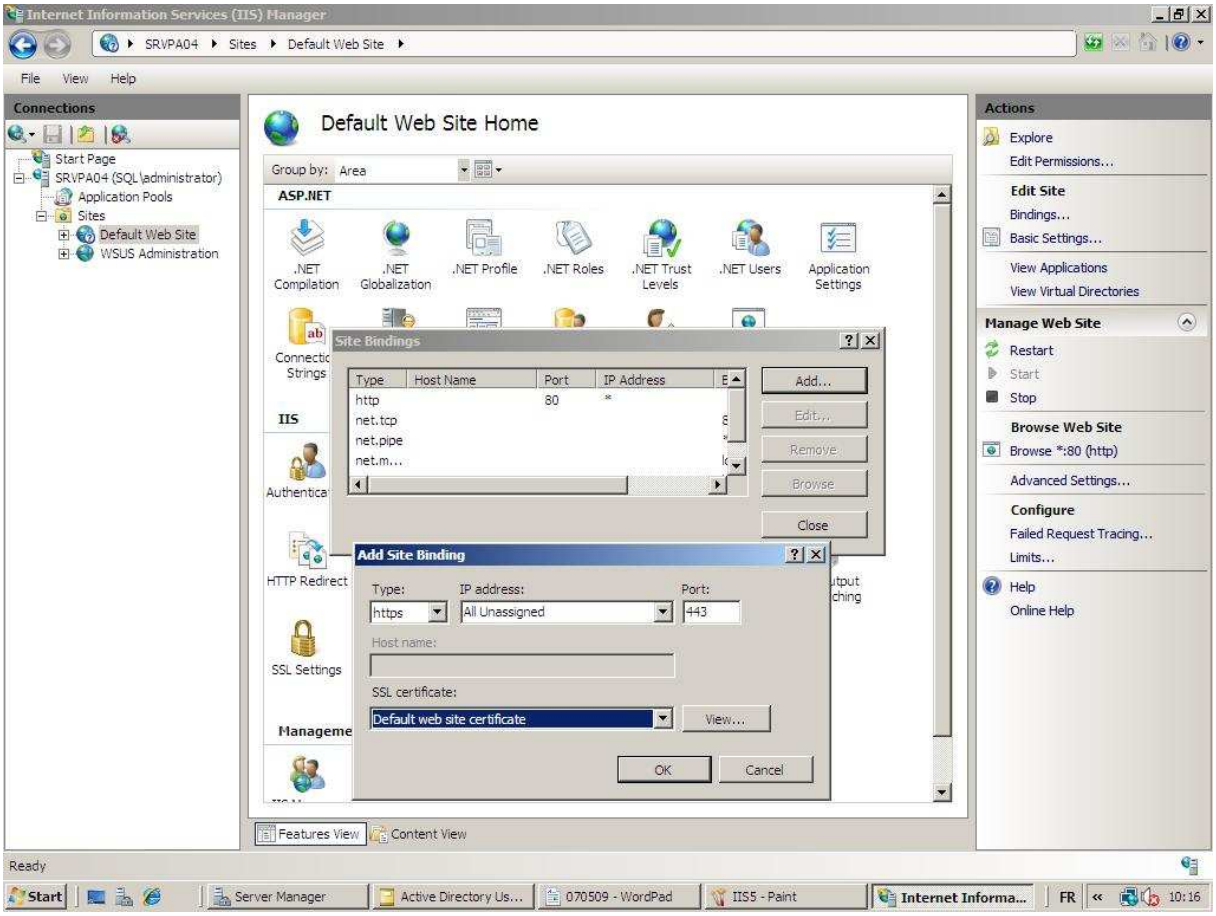
Il y a trois types de certificat.

Les certificats publics qui demandent un enregistrement dans un organisme accrédité. Ils sont l'avantage d'être reconnu par tout le monde. Le certificat vérifie la date de validité, si le nom correspond bien, une vérification de certificat en cascade, etc.

Les certificats domaine qui demande un serveur de certificat en interne. On fait la demande a ce serveur qui autorise automatiquement le certificat si le user est reconnu. C'est uniquement les machines dans le domaine qui lui fera confiance.

Les certificats auto-signed mais personne ne lui fait confiance. Il ne sert qu'à crypter de l'information. Le but est simplement d'avoir une paire de clé pour échanger de l'information.

Une fois la certification crée, il faut l'activé au niveau du web site via l'outil "bindings" du site web. Ensuite, on peut obliger le SSL sur le web site dans les "SSL Settings".



Note : Le common name représente l'url ce qui est très important lors de la demande d'un certificat public.

Plusieurs web site

Si les web site doivent être en interne, il suffit d'appliquer un site web par adresse IP via le l'outil "bindings". On peut également le faire pour des sites externes mais la mise en place sera un peu plus compliquée.

Si les Web Site doivent être accessibles depuis l'extérieur, on peut utiliser une IP avec un Host Name différent mais il y a parfois des incompatibilités et c'est sans doute un peu plus lent dans le trafic mais ce n'est visible que sur des serveurs avec des milliers de requêtes. C'est généralement le genre de configuration choisie par les hébergeurs web.

IIS + WSUS

Il est conseillé de limiter le nombre de connexions concurrentes sur le site WSUS pour éviter de saturer le réseau quand les clients viennent chercher les mises à jour sur le Serveur. On peut penser de cette manière diffuser des services packs de cette manière.

Terminal Server

Il y a également eu beaucoup d'avancées dans ce rôle en Server 2008. Un travail important a été exécuté pour rattraper le retard sur du Citrix. Comme par exemple TS Gateway. Session Broker qui permet l'équilibrage de charge permettant aux utilisateurs de se (re-)connecter à des serveurs TS de manière transparente. TS Web Access qui permet une interface Web permet d'accéder aux applications (intégrable dans un portail SharePoint**).** RemoteApp donne la possibilité d'intégrer des applications distantes à l'environnement local de l'utilisateur (y compris l'association des extensions de fichiers locaux à des applications distantes).

Rappel des avantages

Soft central mais de plus en plus difficile.
Client léger.
TeleWorking.
Maintenance à distance.

Ne pas oublier avant de faire l'installation de programme de basculer en mode installation pour que le programme tourne en monde multiutilisateur. "**change user /install**" fait l'installation et puis quitter le mode "**change user /execute**"

Installation

Il faut installer le serveur de licence, le plus haut possible, c'est à dire dans la forêt. Ne pas oublier de faire des backups de ces licences.

Nouveauté

TS Gateway

Fournir un accès depuis l'extérieur de l'entreprise à des serveurs Terminal Server interne était jusqu'à présent relativement risqué. Le TS Gateway offre une méthode sûre pour publier les terminals serveurs.

Il permet de faire une translation du port 3389 d'une adresse publique vers un serveur TS interne. Cela limitait la connexion à un unique serveur, mais surtout exposait potentiellement celui-ci au "premier venu".

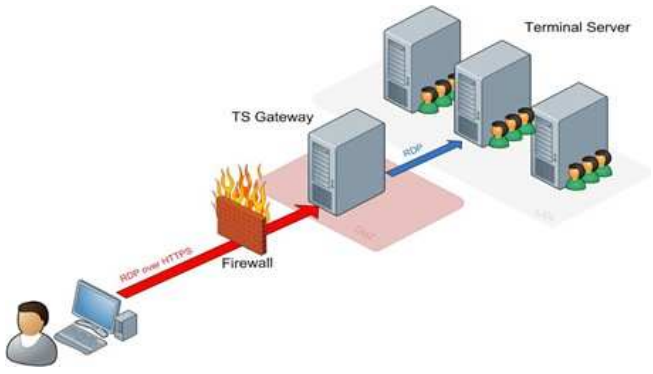
il permet de forcer l'établissement d'un VPN avant la connexion Terminal Server, ce qui complique les procédures de login pour les utilisateurs, mais donne une niveau de sécurité satisfaisant.

Sur le Terminal Gateway, on définit des policies les CAP (Connection Autorization Policies) et les RAP (Ressource Autorization Policies).

La CAP permet par exemple de définir les mappings par groupes d'utilisateurs comme les imprimantes, clé USB. On peut donc avoir des CAP différents par groupe d'utilisateurs (Administrateurs et utilisateurs par exemple). L'ordre des polices de sécurité est très important.

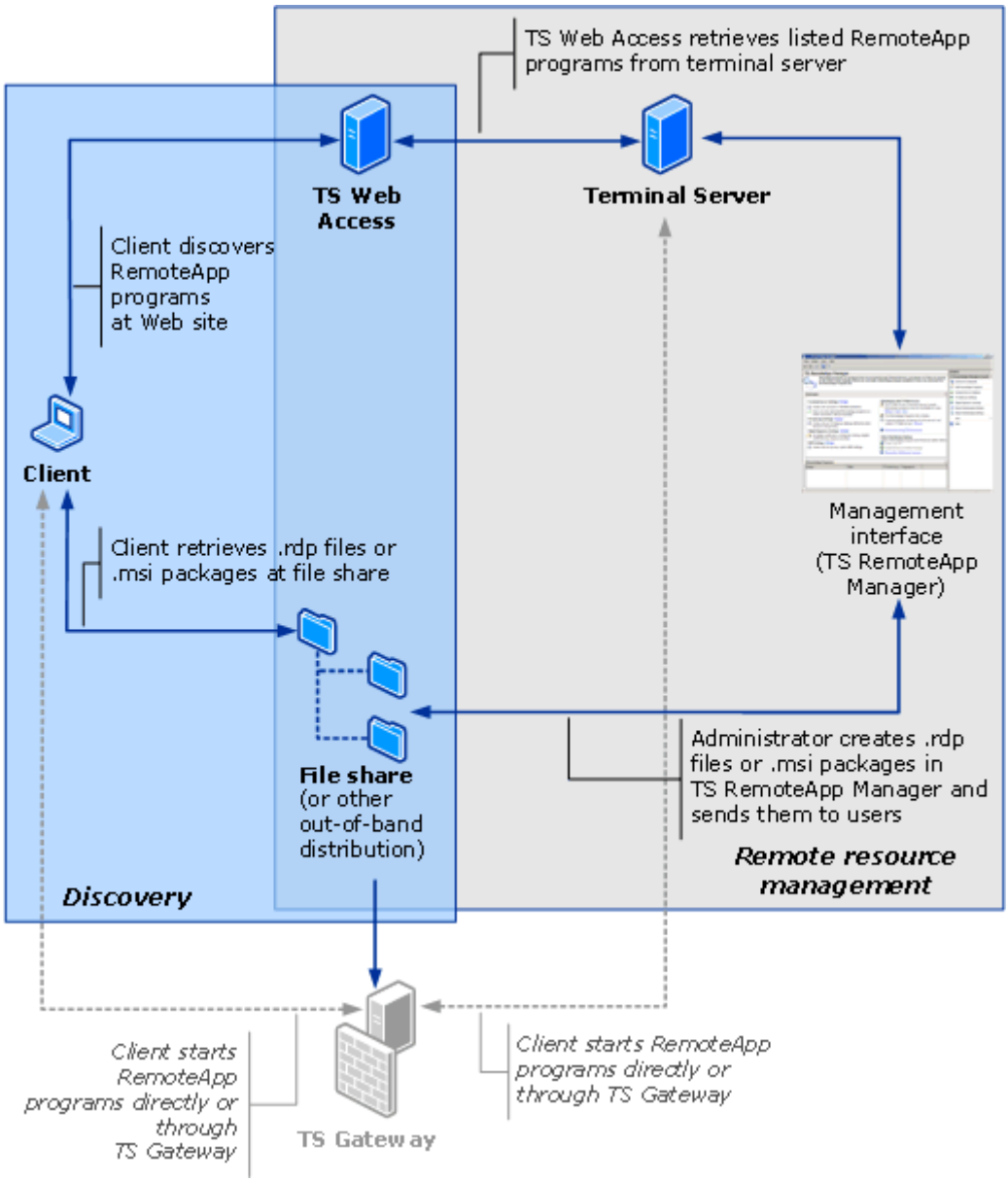
La RAP permet de définir les connexions vers les différents serveurs. Même principe que précédemment, on peut donc dire qu'un administrateur a accès à l'ensemble des serveurs tandis que les utilisateurs ont accès a un serveur TS classique. L'ordre n'a pas d'importance dans cette partie.

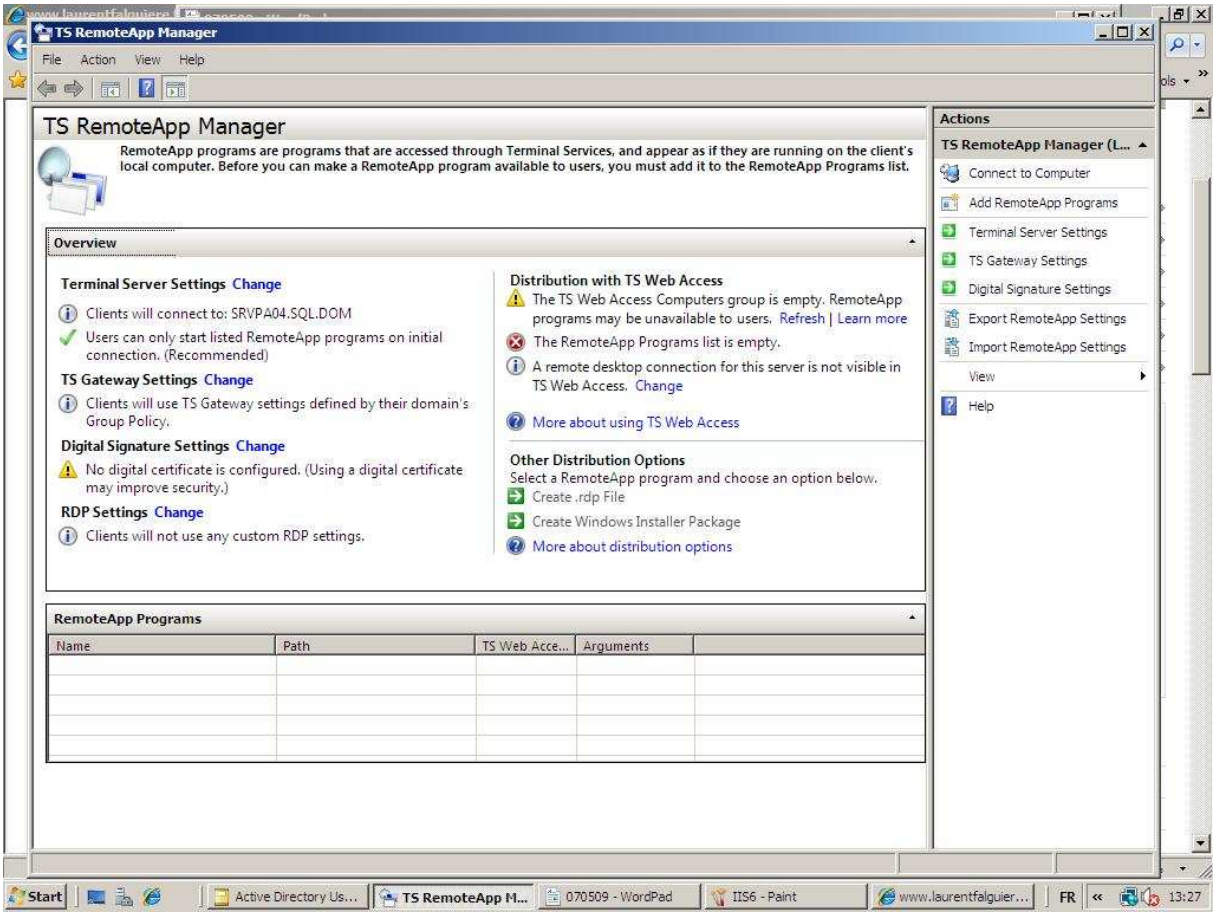
Attention : Il faut faire une configuration du client quand on passe par un TS Gateway. Il faut aller dans les options et puis cliquer sur advanced. Il faut alors préciser au client de passer par le TSG "srvpa01.sql.dom", il faut que le nom correspondant au certificat qui a été attribué par le TSG. Ensuite, on met l'adresse du serveur au quel on veut accéder.



TS RemoteApp Manager

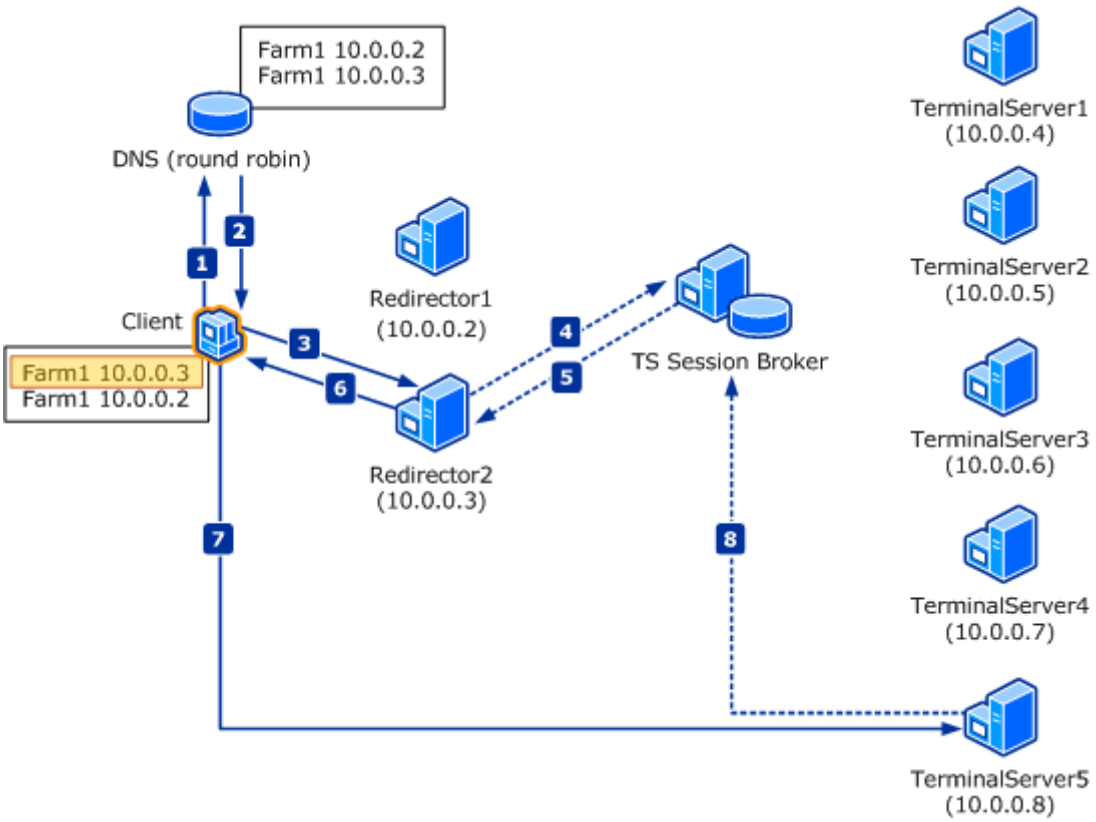
On peut publier un programme via cette application. Pour ce faire, on ajoute un programme via Add Remote/ APP Programs pour la mettre dans la liste de publication. Il va falloir créer un package MSI pour que les gens puissent installer avoir un raccourcis. On peut lors de la configuration le faire passer par un TS Gateway pour les personnes à l'extérieur de l'entreprise. Le programme est donc exécuté sur le serveur et l'utilisateur à l'impression que l'application tourne sur sa machine.





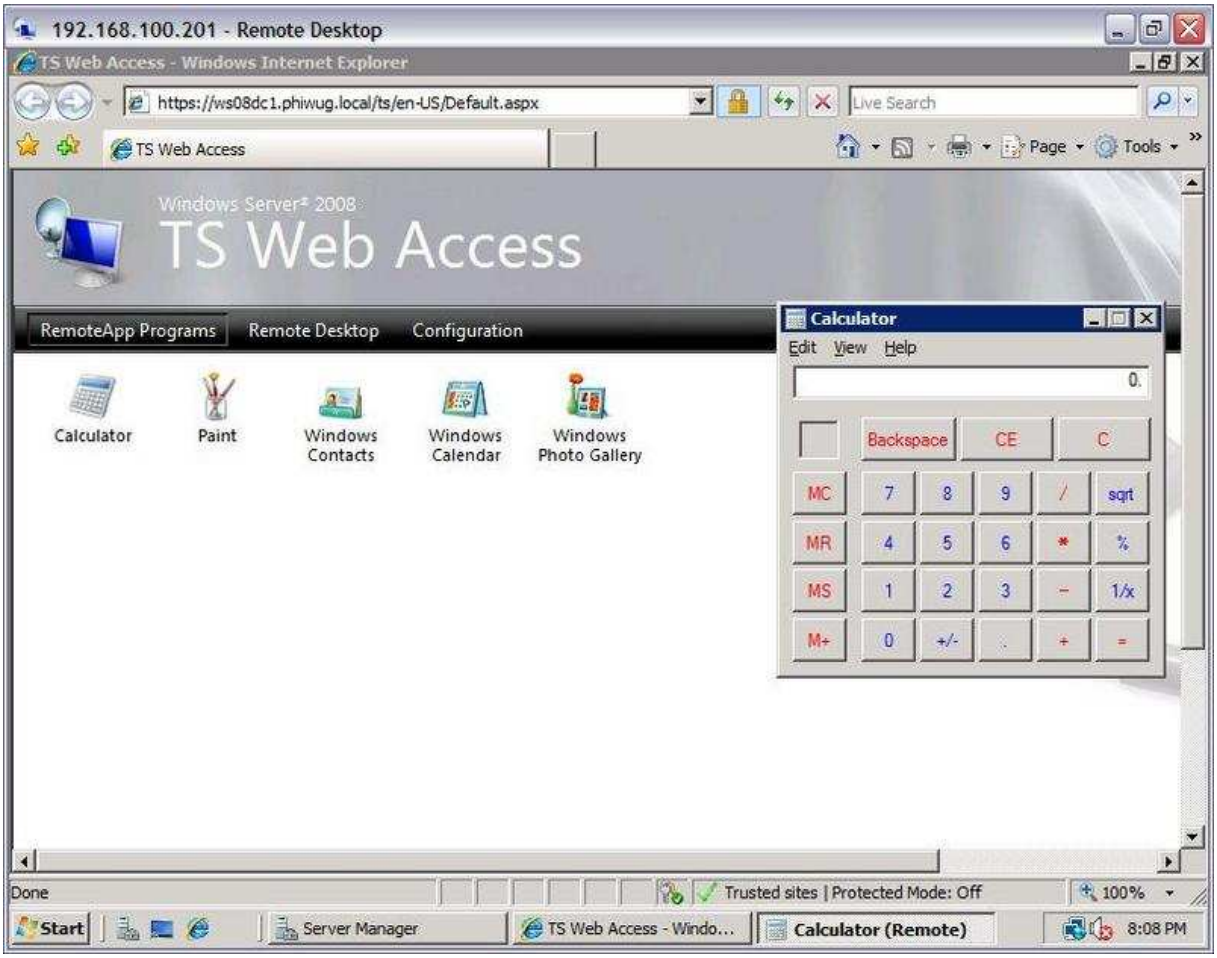
TS Broker

Prenons un cas pratique : Imaginons trois terminal server identiques et qu'ils répondent au même nom via un record DNS. Un serveur TS Broker qui sait si une session A existe ou pas. S'il n'y pas de session existante, il tient à jour sa liste A sur le Serveur 2. Lors de la prochaine demande, si la session n'a pas été fermée le client A sera redirigé automatiquement sur le Serveur 2. L'utilisateur récupéra donc sa session avec ses programmes lancés. C'est une gestion de ferme comme Citrix le permet.


Farm1 10.0.0.2
Farm1 10.0.0.3
DNS (round robin)
1
2
Client
Farm1 10.0.0.3
Farm1 10.0.0.2
3
6
Redirector1
(10.0.0.2)
Redirector2
(10.0.0.3)
4
5
TS Session Broker
7
8
TerminalServer1
(10.0.0.4)
TerminalServer2
(10.0.0.5)
TerminalServer3
(10.0.0.6)
TerminalServer4
(10.0.0.7)
TerminalServer5
(10.0.0.8)

TS Web Access

Permet de créer une page web qui centralise les applications qui tourne sur terminal Server.



Server Core :

Server 2008 sans "interface graphique" gérer par lignes de commandes ou par console externe. Il y a encore moyen de lancer beaucoup d'interfaces graphiques.

Les Avantages

Le système est moins gourment en ressources.

Plus de sécurité car il y a moins de rôles donc moins de failles.

Les Inconvénients

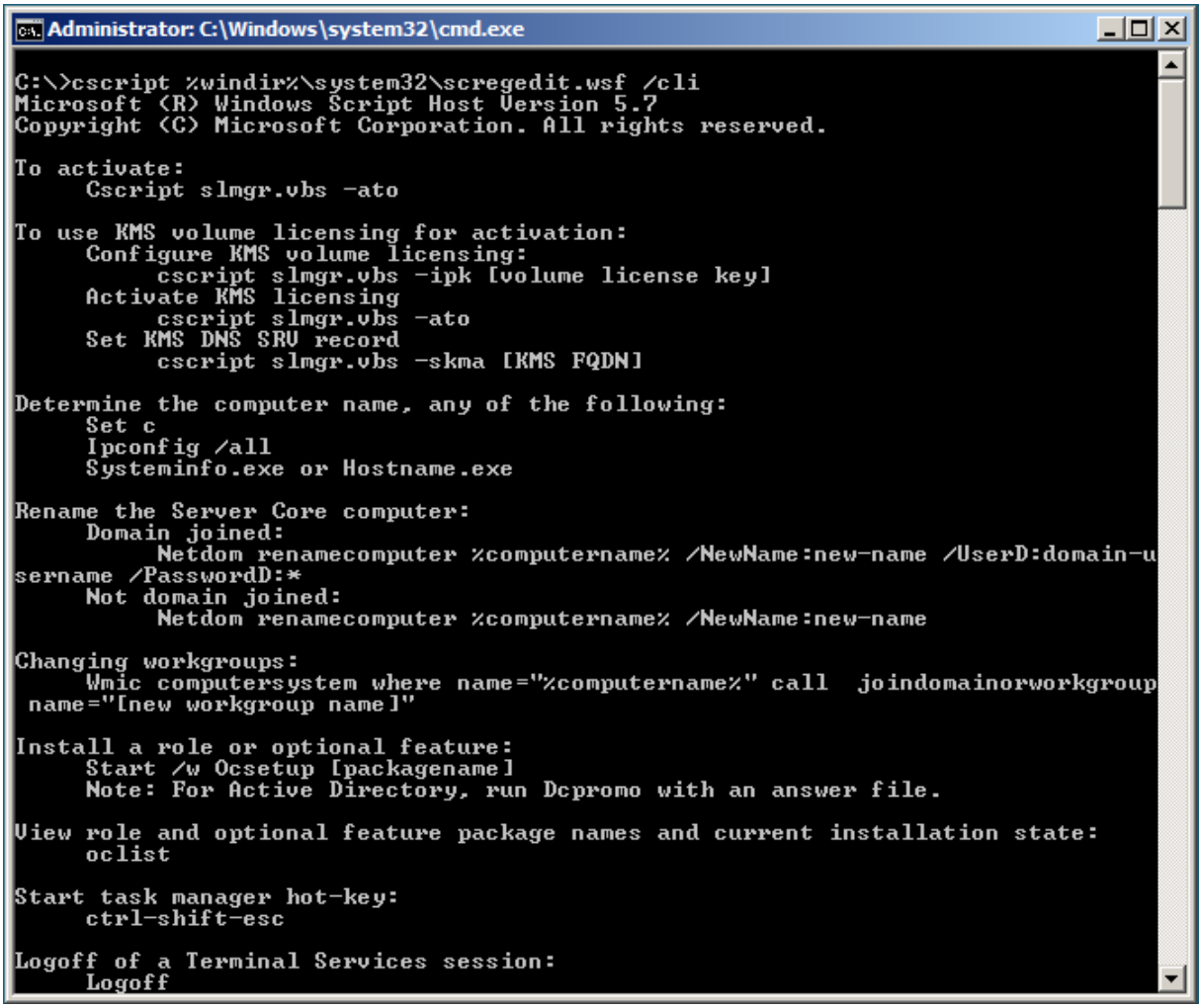
Le PowerShell ne fonctionne pas mais il sera présent avec plus de commandes dans la version 2008 R2.

Les programmes de support qui ne sont tous compatible comme les anti-virus, les backups.

Utilités

File Server, Domain controler, DHCP, DNS , Web, Hyper-V, PrintServer.

Fonctionne très bien pour le File Server, Domain Controler, DHCP. Pour le reste, la gestion devient un peu plus difficile.



Exemple création d'un FileServer

Etape 1 - Changer le nom de la machine :

" netdom renamecomputer %computername% /newname:NomServerCore

Etape 2 - intégration des drivers.

Etape 3 - Attribution d'une IP :

" netsh " pour rentrer dans le shell réseau en mode interactif.
" inter "
" ipv4 "
set address "Local Area Connection" static IP MASK Gateway Metric
set dsnserver "Local Area Connection" static IP Primary

Etape 4 - Mise en domain :

"netdom join core04 /domain:sql.dom /userd:sql\administrator /passwordd:passe "

Etape 5 - Désactivé le firewall si nécessaire

" netsh firewall set opmode disable "

Etape 6 - Soit le configurer en ligne de commande, soit passé par les consoles d'un autre Server 2008 via le computer management.

Quelques produits complémentaires payants

SCOM (System Center Operations Manager)

Permet de faire une surveillance des serveurs. Il peut surveiller les services d'un serveur comme l'Exchange, le SQL ou d'autres produits tiers mais c'est généralement payant. Il peut surveiller l'Active Directory, le matériel dans certain cas. Il est capable d'apprendre du système et de travailler sur des statistiques générées par le réseau. Lors de la détection d'un problème, il peut bien entendu prévenir l'équipe admins par mail, par du messenger "interne", par SMS. Il peut exécuter des scripts et faire de la délégation d'action à un utilisateur. Il peut également faire des reportings et de l'audit des différents serveurs.

SCCM (System Center Configuration Manager 2007)

Permet de gérer le parc clients via une gestion d'inventaire sur les machines hardware et software. Il fonctionne également très bien pour le déploiement de soft ou de patch.

SCE (System Center Essentials)

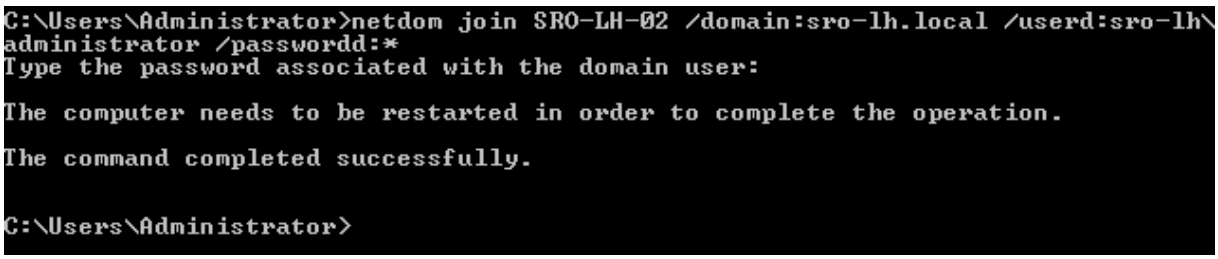
Identique que SCOM mais pour un maximum de 50 serveurs et un SCCM pour un maximum de 250 clients. Néanmoins, celui-ci est limité dans ses options.

Astuces

1. Pour accéder directement au panneau de configuration des cartes réseaux. Il suffit de lancer la commande ncpa.cpl

2. « **servermanagercmd –q** » donne l'ensemble des composants installé sur la machine 2008.

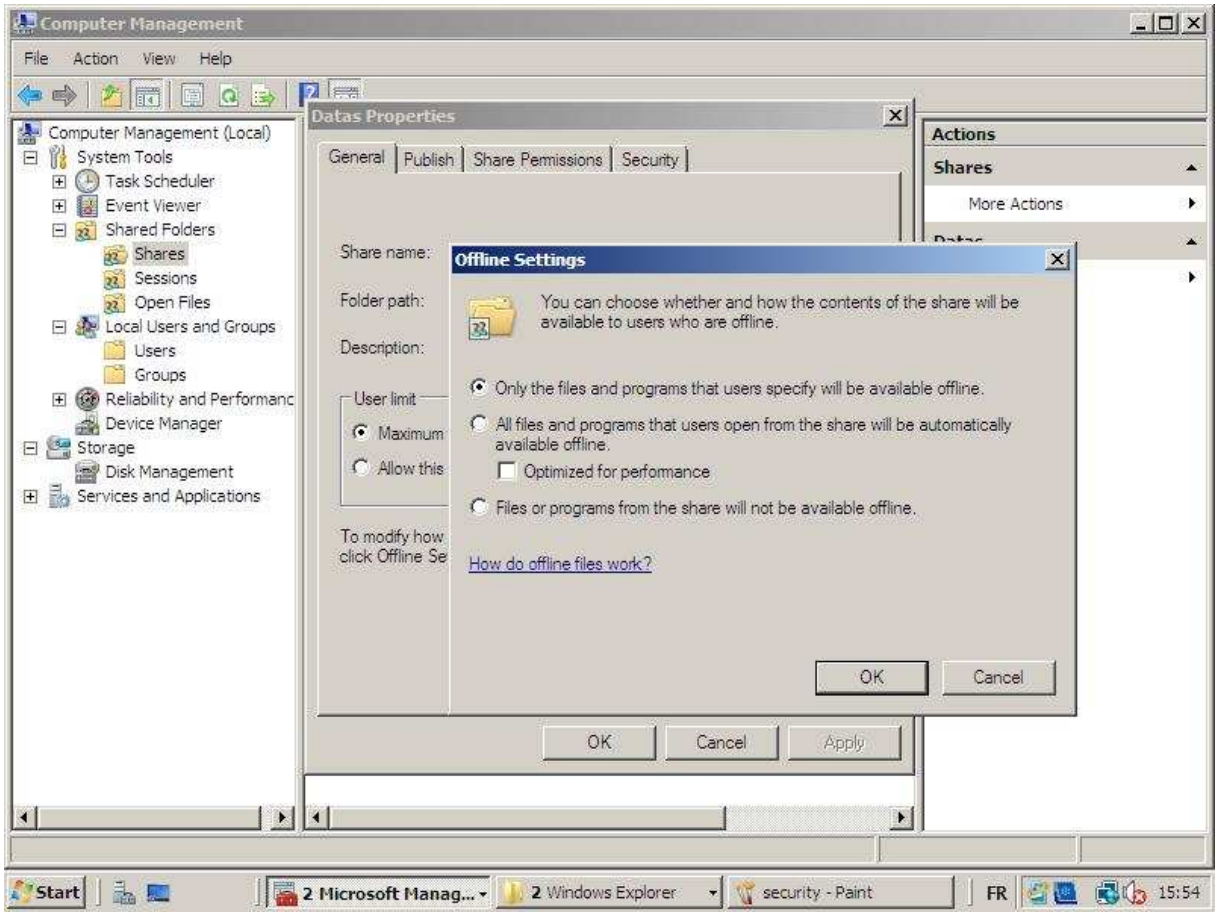
3. La ligne de commande « **netdom join** » permet de joindre un client a un domaine en spécifiant des paramètres de base comme l'OU de destination. Cette commande fonctionne de base sous Vista, Seven et Server 2008. Pour XP, il faut installer la ressource Kit.



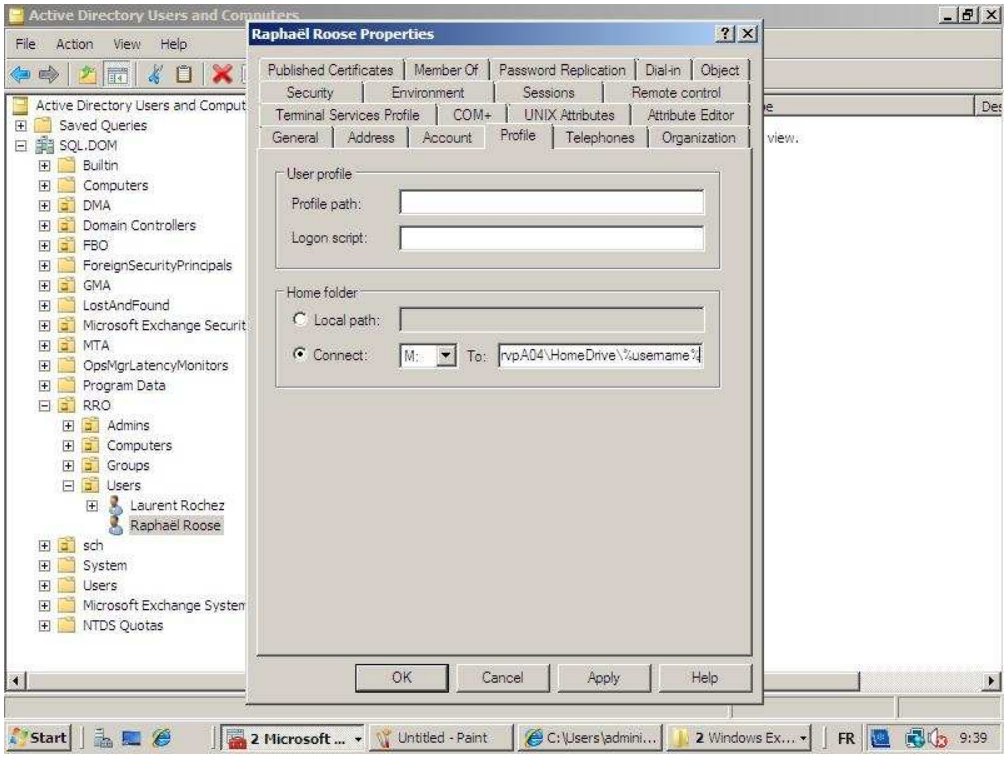
4. Les permissions NTFS ne sont gardées que via un « move » sur la même partition. Pour palier à ce problème, vous plusieurs solutions :
   1. Utilisez la restauration via votre programme de backup.
   2. Utilisez la commande **XCOPY « Source » « destination » /S /H /O /E**
   3. Utilisez un programme tiers comme Secure Copy.

5. Offline file : Par défaut, le système accepte les synchronisations des répertoires partagés ce qui n'est pas toujours idéal. On peut imaginer qu'on ne désire pas donner la possibilité à un utilisateur de synchroniser un répertoire service (exemple : répertoire compta) sans pour autant l'empêcher de synchroniser ses documents. Pour ce faire, il faut aller dans le « **Computer Management** », clic droit sur le sharing, propriété, offlines settings et refuser la

synchronisation de ce dossier.



6. Home Folder dans l'onglet profile permet de créer un mapping pour l'utilisateur. \\server\HomeFolder\%username%



7. Installer le Remote Server Administration Tools sur votre workstation ou portable en vista ou Seven. Il vous facilitera la vie lors de vos maintenances.

Lexique

DC : Domain Controller
GPO : Groupe Policy
IIS : Internet Information Services
WSUS : Microsoft Windows Server Update Services
SCOM : System Center Operations Manager 2007
SCCM : System Center Configuration Manager 2007
SCE : System Center Essentials
IIS : Internet Information Service
RSAT : Remote Server Administration Tools

Source

Lien GPO

http://technet.microsoft.com/fr-fr/library/cc754461(WS.10).aspx
http://www.microsoft.com/france/technet/prodtechnol/exchange/2003/insider/admodifynet.mspx.
http://blogs.dirteam.com/blogs/jorge/archive/2008/02/10/showing-last-logon-info-at-logon-in-windows-server-2008.aspx

Lien Migration

http://support.microsoft.com/kb/255504/fr
http://www.system-it.net/articles.php?lng=fr&pg=343

Lien Backup

http://www.microsoft.com/downloads/details.aspx?FamilyID=C7D4BC6D-15F3-4284-9123-679830D629F2&displaylang=en
http://josvanrijn.spaces.live.com/Blog/cns!50BFE3679B82A2FA!128.entry

Lien Général

http://technet.microsoft.com/fr-fr/library/default.aspx
http://technet.microsoft.com/fr-fr/library/dd349801(WS.10).aspx
SCCM : http://www.microsoft.com/france/systemcenter/sccm/default.mspx
SharePoint : http://office.microsoft.com/fr-fr/training/CR102146081036.aspx
SharePoint : http://msdn.microsoft.com/fr-fr/office/msdn.coach.sharepoint.aspx

MSDN Office : http://msdn.microsoft.com/fr-fr/office/default.aspx
MSDN Library :http://msdn.microsoft.com/en-us/library/cc203350.aspx

Lien Utile

http://www.petri.co.il/add_unlock_user_option_to_dsa.htm
http://www.system-it.net/articles.php?lng=fr&pg=343
http://blogs.dirteam.com

Commandes pour Server Core

Voir le fichier Server Core Installation Option of Windows Server 2008 Step ou directement sur la technet http://technet.microsoft.com/en-us/library/cc753802.aspx