e i g
Ecole d'ingénieurs
de Genève

Hes·so
Haute Ecole Spécialisée
de Suisse Occidentale

Server 2008 Active Directory

Délégation de contrôle

Etudiant : Pellarin Anthony

Professeur : Litzistorf Gérald

En collaboration avec : Pictet&Cie

Date du travail : 17.09.2007

Table des matières :

1. Introduction

Le sujet de cette première partie du travail de diplôme proposé par la banque privée Pictet&Cie est basé sur l'annuaire « ***Active Directory* »** dans « ***Windows Server 2008*** » et plus particulièrement sur la délégation de contrôle. Cette technique était déjà présente dans « *Windows Server 2003* » et « *Windows Server 2000* ».

Elle consiste à déléguer l'administration d'une ou plusieurs tâches dans l'annuaire AD à un utilisateur. Elle peut aller de tâches simples comme la gestion des comptes utilisateurs du domaine, à des actions plus complexes comme la gestion du contrôleur de domaine.

Cette technique est basée sur la gestion des autorisations NTFS en accordant ou non la permission d'effectuer une tâche spécifique à un utilisateur. Plusieurs tâches d'administrations peuvent être confiées à un même utilisateur et un objet peut être administré par plusieurs administrateurs.

Cette technique est à utiliser avec précaution et il faut faire confiance aux utilisateurs auxquels on donne le droit d'intervenir sur l'annuaire. Le principe du moindre privilège est à appliquer si l'on veut garantir la sécurité de l'annuaire. L'utilisateur à qui l'on confie une tâche d'administration ne doit pas pouvoir effectuer d'autres actions sur l'annuaire que celles qui lui ont étés confiées. Un utilisateur malveillant pourrait être tenté de corrompre les données de l'annuaire.

Cette solution est utile par exemple lorsque l'on veut isoler l'administration de plusieurs départements, ou lorsque l'on veut séparer les tâches d'administration entre plusieurs administrateurs ou encore lorsque le nombre d'objets dans l'annuaire devient important et que les tâches d'administration deviennent longues.

Le but est donc d'étudier cette délégation de contrôle, de comprendre le fonctionnement, et de présenter les outils servant à réaliser la délégation et comment l'appliquer à un cas réel.

Un scénario pratique est donc mis en place en fin de travail pour montrer pratiquement le fonctionnement de cette technique et présenter les différents éléments mis en place pour assurer la délégation de contrôle.

1.1 Chapitres

- Le **chapitre 1** est donc la présentation du travail de diplôme avec une brève introduction sur le sujet du travail et sur l'objectif de l'étude.

- Le **chapitre 2** présente le système d'exploitation « ***Windows Server 2008*** » ainsi que quelques nouveautés apportées par rapport aux anciennes versions.

- Le **chapitre 3** introduit le concept d'annuaire « Active Directory », présente l'architecture AD ainsi que la notion d'unité d'organisation qui est le point clé de la délégation de contrôle.

- Le **chapitre 4** présente une introduction au schéma AD. Le schéma représente le cœur de l'annuaire et tout les objets créent dans AD se basent sur le schéma AD.

- Le **chapitre 5** est une bref introduction aux groupes crées automatiquement à l'installation d'AD avec une explication sur le rôle des principaux groupes.

- Le **chapitre 6** présente la notion de système de fichiers NTFS. Les nouveautés apportées par ce système ainsi qu'un aperçu des différentes autorisations applicables à des objets.

- Le **chapitre 7** représente le cœur du travail avec la présentation du fonctionnement de la délégation de contrôle. Il introduit d'abord l'utilité de la délégation et pourquoi on peut avoir recours à cette méthode.

  Il est expliqué quels sont généralement les différentes étapes à respecter lorsque l'on veut déléguer le contrôle d'une partie de l'annuaire à un utilisateur.

Un guide à été réalisé sur la mise en place pratique de la délégation en utilisant soit l'assistant automatique, soit en effectuant les modifications manuellement.

Ce chapitre comporte aussi une explication sur la manière dont on peut auditer une action dans l'annuaire avec la procédure pour activer l'audit d'un événement.

Finalement, un scénario pratique est proposé présentant les différentes actions que l'on peut déléguer.

- Le **chapitre 8** explique comment on peut se passer de l'interface graphique pour l'administration d'AD et utiliser les outils CLI à disposition.

- Le **chapitre 9** présente les différents problèmes survenus pendant le travail avec la solution utilisée.

- Le **chapitre 10** est la conclusion avec un rappel des différents éléments vus pendant le travail.

Temps consacré aux différents points de l'énoncé :

Etude théorique des principales fonctions disponibles d'Active Directory ainsi que les outils disponibles et identification des risques

- 3 semaines

Mis en place du scénario pratique

- 3 semaines

2. Windows Server 2008 :

Après la sortie du nouveau système d'exploitation de Microsoft « Windows Vista », la suite logique était donc la sortie du nouveau système d'exploitation serveur de Microsoft « Windows Server 2008 ». Il va donc remplacer à terme l'ancien système d'exploitation Windows Server 2003 aujourd'hui utilisé dans la majorité des entreprises.

Windows Server 2008 et Windows Vista embarquent donc le même *kernel* c'est-à-dire le NT 6.0. On constate donc des similitudes aux niveaux des nouveautés comme par exemple l'introduction de l' « UAC » (User Account Control) qui permet d'appliquer le principe du moindre privilège en accordant des privilèges restreints, et des similitudes au niveau de l'interface avec l'apparition de « Windows Aero » offrant une interface plus conviviale.

La sortie du système d'exploitation « Windows Server 2008 » est prévue pour le début de l'année 2008 en même temps que le Service Pack 1 pour « Windows Vista » et le Service Pack 3 pour « Windows XP ».

La version de « Windows Server 2008 » utilisée pour ce travail est la RC0 qui est la dernière version disponible à ce jour :

Windows Server (R) 2008 Enterprise

Evaluation copy. Build 6001

2.1 Nouveautés de Windows Server 2008 :

Un certain nombre de nouveautés ont été apportées dans Windows Server 2008 comme par exemple :

- **Server Core**

  Dans Windows Server 2008, on a maintenant la possibilité d'installer une version minimale de Windows. Cette version est dépourvue d'interface graphique. De cette façon la sécurité est améliorée puisqu'on va installer que le strict minimum utile.

  Une installation « *Server Core* » permet d'utiliser les mêmes composantes que dans la version « normale » comme le serveur DHCP, DNS ou Active Directory par exemple.

  On administre donc le serveur par des lignes de commande que l'on tape dans une fenêtre de commande.

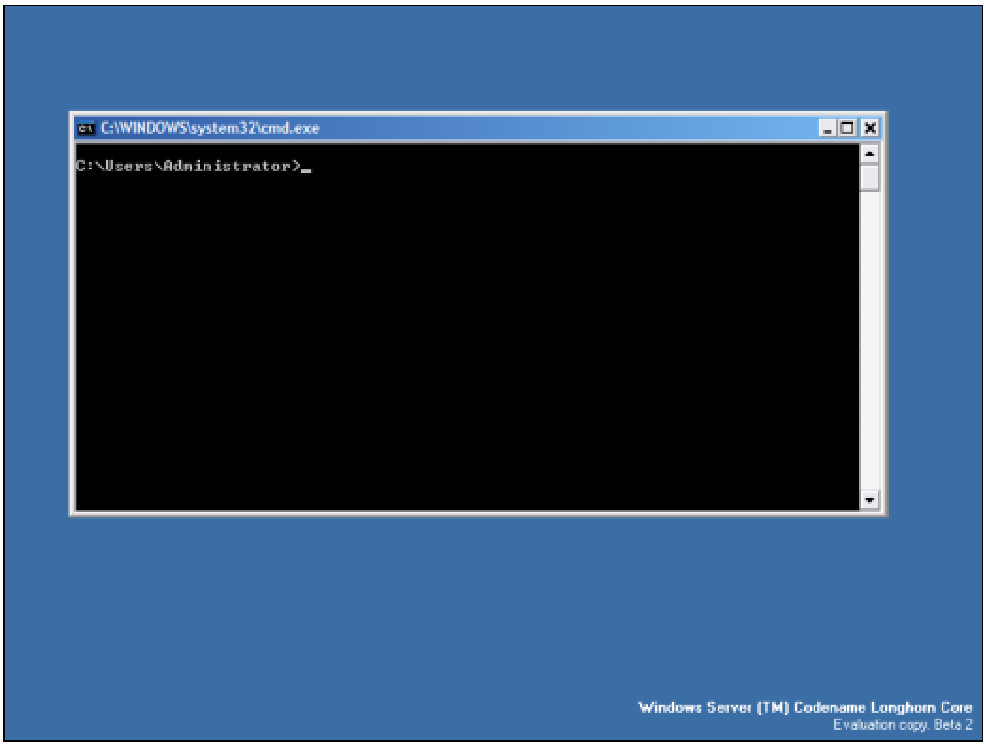

Figure 2.1 Interface de la version « Server Core »

- **Active Directory Domain Services: Read-Only Domain Controller**

  Une nouveauté dans Windows Server 2008 est la possibilité d'installer un contrôleur de domaine en lecture seule.

  En effet, lorsque la sécurité physique du serveur ne peut être garantie comme dans le cas de succursales par exemple, on a la possibilité d'installer un RODC, Read-Only Domain Controller, sur lequel on ne va donc rien pouvoir écrire et qui ne vas stocker aucun mot de passe. Ce RODC est donc une copie du contrôler de domaine « principal ».

- **Auditing Active Directory Domain Services Access**

  Dans Windows Server 2003, il n'y avait qu'une seule catégorie pour l'audit des activités dans Active Directory, qui était donc soit « *enabled* » soit « *disabled* ». Dans Windows Server 2008, la catégorie a été subdivisée en 4 sous-catégories :

  - Directory Service Access
  - Directory Service Change
  - Directory Service Replication
  - Detailed Directory Service Replication

- **Fine-Grained Password Policies**

  Microsoft Windows Server 2008 offre la possibilité de définir plusieurs politiques de mots de passe pour différents utilisateurs.

  Dans les anciennes versions du système d'exploitation serveur de Microsoft, une seule politique de mot de passe était crée pour tous les utilisateurs du domaine, ce qui n'était donc pas très optimisé sachant que certains comptes étaient plus importants que d'autres.

  On peut donc faire en sorte que les comptes sensibles comme les comptes administrateurs requièrent un mot de passe plus complexe qu'un compte normal.

3. Active Directory

Active Directory[1] est le nom du service d'annuaire (au sens informatique) de Microsoft. AD permet de regrouper toutes les informations concernant le réseau, que ce soient les utilisateurs, les machines ou les applications. L'utilisateur peut ainsi trouver facilement des ressources partagées, et les administrateurs peuvent contrôler leurs utilisations grâce à des fonctionnalités de sécurisation des accès aux ressources répertoriées.

AD a pour objectif de permettre la gestion des comptes, des ordinateurs, des ressources et de la sécurité de façon centralisée, dans le cadre d'un domaine. Un domaine constitue un ensemble d'utilisateurs et de machines dont le contrôle est centralisé.

3.1 Arborescence Active Directory

Une arborescence Active Directory est composée de :

- **La forêt** : ensemble de tous les domaines AD
- **L'arbre** : Représente le domaine et toutes ses ramifications. domaine.com, sous1.domaine.com, sous2.domaine.com et projet.sous1.domaine.com forment un arbre
- **Le domaine** : constitue les feuilles de l'arborescence. projet.sous1.domaine.com peut-être un domaine au même titre que domaine.com

[1] http://www.supinfo-projects.com/fr/2002/decouverte_active_directory/0/

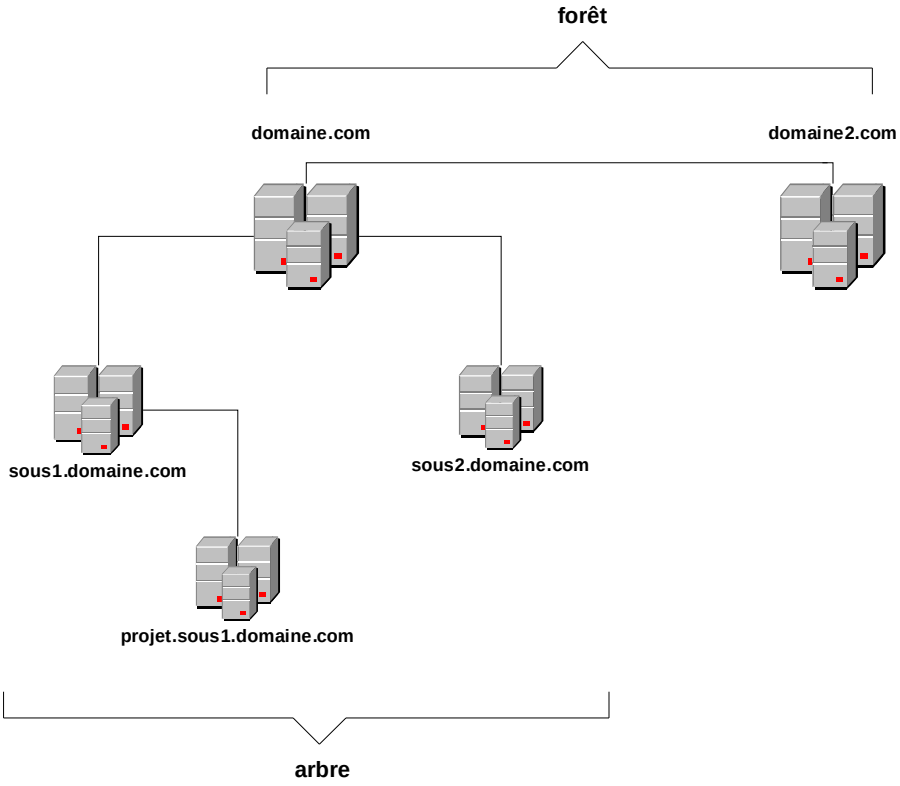

Figure 3.1 Arborescence Active Directory

Dans le cadre du projet, en partant du principe que l'on a qu'un seul domaine, on va donc avoir une forêt composé d'un domaine qui sera le domaine racine.

3.2 Unité d'Organisation

Une unité d'organisation (OU, Organizational Unit) est un conteneur dans lequel on va pouvoir mettre des utilisateurs, des groupes, des ordinateurs ainsi que d'autres OU.

On peut grâce aux OU représenter une certaine architecture pouvant ou non représenter la structure de l'entreprise.

Des stratégies de groupes peuvent être affectées à une OU et on va pouvoir déléguer l'administration de celle-ci et son contenu à un administrateur par exemple. On peut donc donner les autorisations à un utilisateur, de modifier les objets contenus dans une OU par exemple. Avec la structure d'OU que l'on peut mettre en place, la délégation d'administration est simplifiée et la gestion plus facile en séparant les différents privilèges accordées en fonction des différentes OU.

Dans ce travail de diplôme, toute la délégation de contrôle sera basée sur les OU. Une architecture de test sera crée pour simuler l'architecture d'une entreprise.

On va crée ensuite des groupes et des utilisateurs de test que l'on va répartir dans ces OU en fonction de leur rôle.

Des autorisations vont être finalement appliquées aux OU pour accorder ou non aux utilisateurs présents dans ces OU des tâches d'administrations, comme par exemple la gestion des utilisateurs, la gestion des ordinateurs de l'entreprise ou encore la gestion du serveur DNS.

Certains utilisateurs peuvent donc avoir plusieurs rôles d'administration à gérer et l'on peut avoir des utilisateurs avec plus ou moins de privilèges que d'autres. Certaines pourront par exemple crée de nouveaux utilisateurs alors que d'autres ne pourront que modifier les informations de comptes déjà existants.

Il existe beaucoup de scénarios possibles que l'on peut appliquer à l'entreprise. Cela dépend par exemple du niveau de sécurité que l'on veut pouvoir garantir, du nombre d'administrateurs délégués que l'on veut avoir, du nombre de tâches d'administration à effectuer ou encore de la complexité de l'architecture de l'entreprise.

Je vais présenter quelques scénarios possibles dans ce travail de diplôme.

Pour créer une OU il suffit de faire un clique droit à l'endroit où l'on veut créer l'OU et de faire, « ***New*** » puis de choisir « ***Organizational Unit*** » :

Figure 3.2 Création d'une OU

4. Schéma Active Directory :

Le sujet de ce travail de diplôme portant principalement sur Active Directory, et le schéma étant le cœur d'AD, ce paragraphe introduit la notion de schéma d'AD même si dans ce projet, aucune modification du schéma ne sera effectuée.

Le schéma[2] Active Directory décrit toutes les classes ainsi que leurs attributs pour les différents objets que compose le réseau. Un annuaire ne peut stocker que des entrées qui correspondent à une classe d'objet décrite dans le schéma AD. Le schéma peut être modifié pour répondre plus précisément à ses besoins.

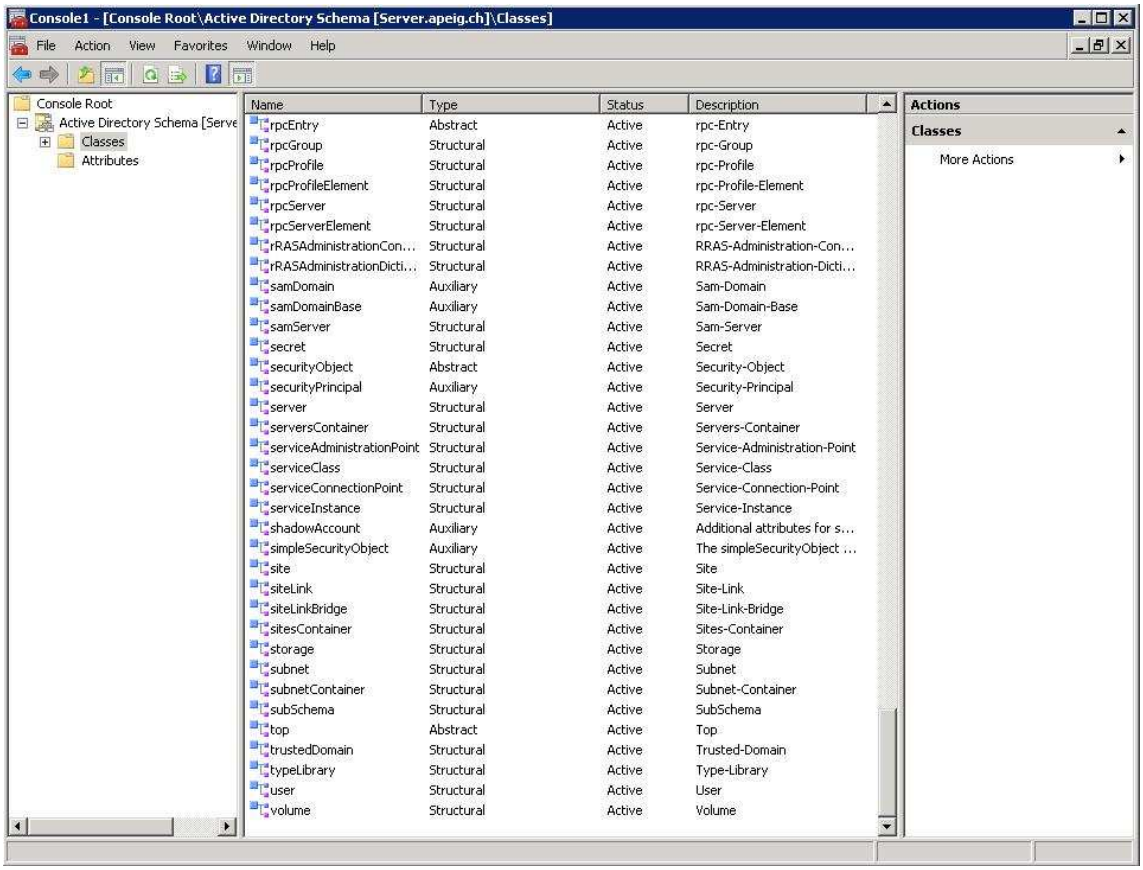

Figure 4.1 Schéma Active Directory

[2] http://msdn2.microsoft.com/en-us/library/ms675085.aspx

4.1 Objets :

Dans un annuaire AD, les objets représentent les éléments du réseau comme les utilisateurs, les serveurs, etc. Lorsqu'AD doit créer un nouvel objet, il va se baser sur le schéma AD pour créer l'objet et plus précisément sur les classes d'objets du schéma.

4.2 Classe d'objets :

Les classes d'objets et leurs attributs forment une structure qui va définir l'objet. Cette structure forme le schéma AD. La classe est constitué d'un numéro unique « *X.500 OID* » pour éviter les conflits entre les différents annuaires.

Une classe est constituée d'attributs. Chaque attribut est défini comme étant obligatoire ou facultatif.

Prenons comme exemple la classe « ***user*** » qui permet de stocker les informations concernant un utilisateur. Celle-ci comporte donc plusieurs attributs comme par exemple :

- **Account-Expires**

  Date à laquelle le compte expire

- **Display-Name**

  Nom de l'utilisateur affiché dans AD, généralement constitué du nom, des initiales et du prénom

- **Control Access Rights**

  Détermine quels sont les opérations permises pour l'utilisateur sur un objet

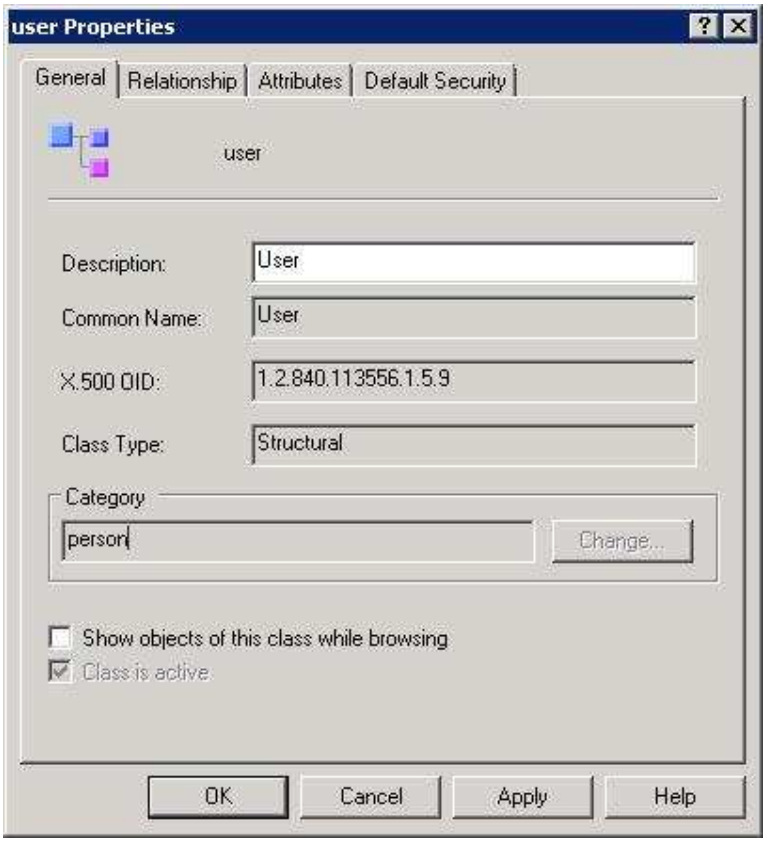

Figure 4.2 Exemple de la classe « user »

4.3 Les attributs :

Une classe a un certain nombre d'attributs mais ceux-ci ne sont pas tous obligatoire, en effet lorsqu'on crée un nouvel objet, on n'est généralement pas obliger de remplir tous les champs.

Par exemple la classe « ***organizationalUnit*** », celle-ci comporte plusieurs attributs mais un seul est obligatoire :

- **ou**

  Renseigne sur le nom de l'unité d'organisation

D'autres sont facultatifs comme par exemple :

- **businessCategory**

  Texte descriptif sur l'unité d'organisation

- **defaultGroup**

  Groupe auquel l'objet est associé lors de sa création

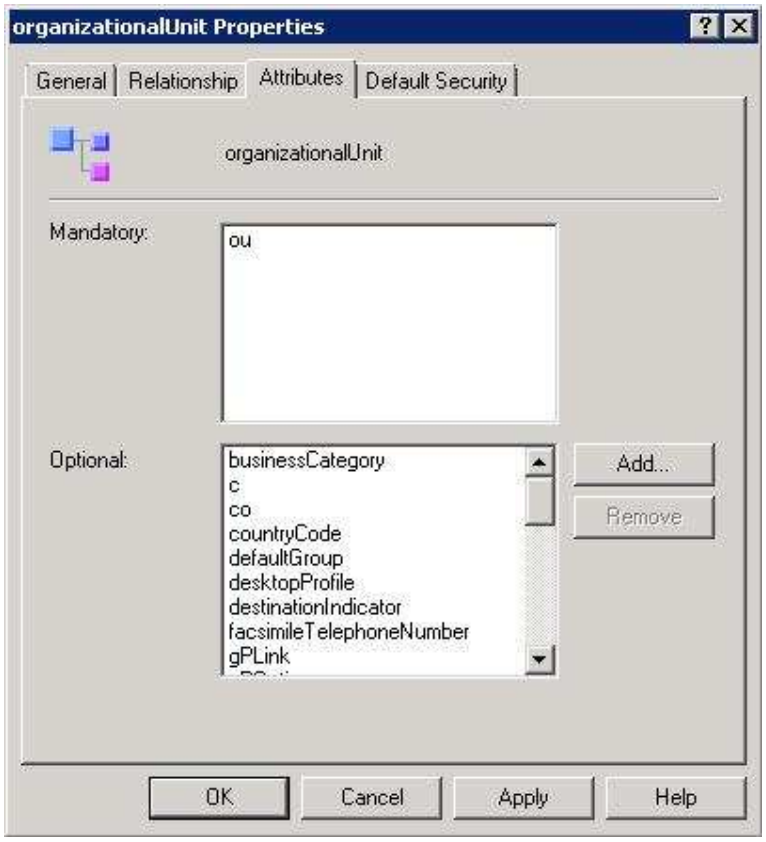

Figure 4.3 Exemple des attributs de la classe « organizationalUnit »

Avec le bouton « ***Add…*** » on remarque que l'on peut ajouter des attributs.

Si on regarde les propriétés d'un attribut, on voit qu'il possède plusieurs champs dont certains que l'on peut modifier.

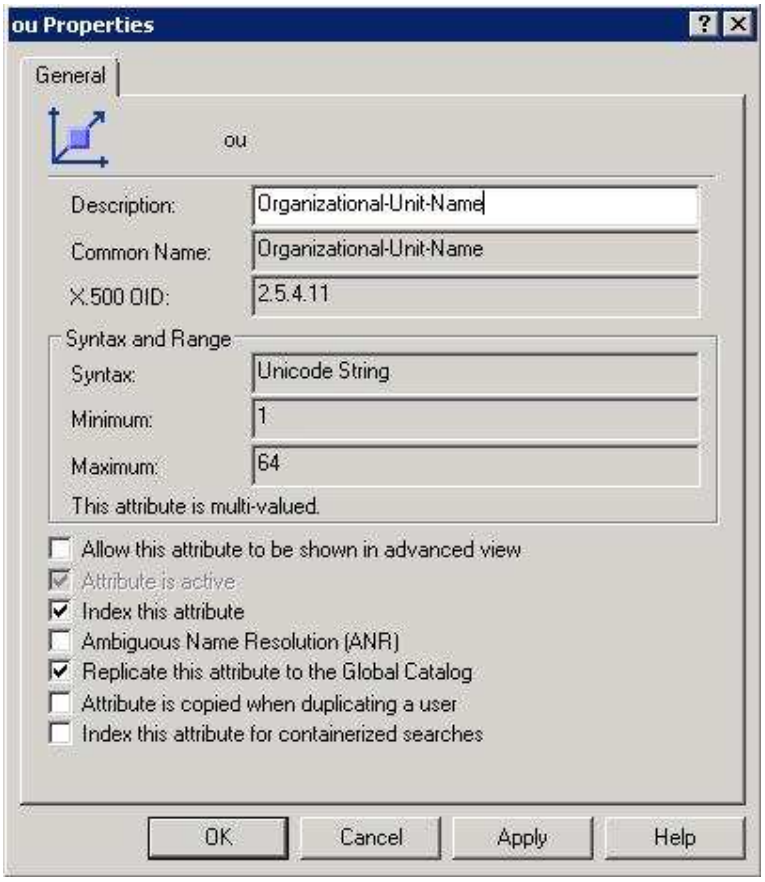

Figure 4.4 Exemple de l'attribut « ou »

Plus d'informations sur le schéma Active Directory :

Active Directory 2nd edition Chapitre 4 : http://www.ellipse.ch/Produit.aspx?Produit=40476

4.4 Accéder au schéma Active Directory

Pour accéder au schéma Active Directory suivez la procédure suivante :

1. Lancer la console **MMC** en appuyant sur « ***Start*** », puis « ***Run…*** ». Vous arriver donc sur la console de management MMC (Microsoft Management Console).

Figure 4.5 Console de management

2. Allez dans File, puis cliquer sur « ***Add/Remove Snap-in…*** **»**.

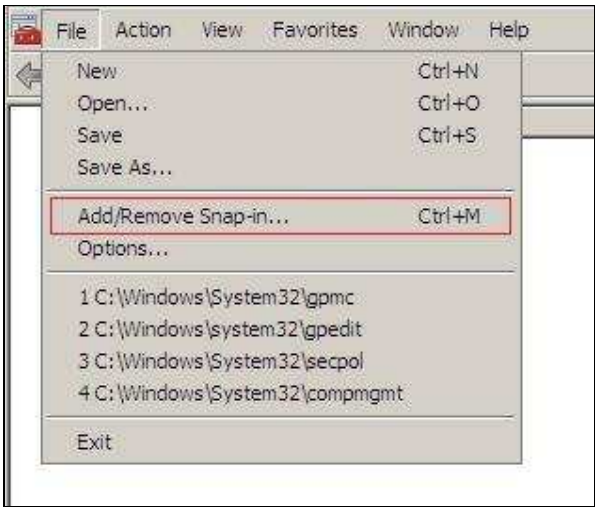

Figure 4.6 Ajout du composant logiciel enfichable

3. Dans l'écran qui apparait, sont listés tous les composants que l'on peut ajouter. Dans notre cas, nous voulons changer le schéma. Choisissez alors **« Active Directory Schema** » puis cliquer sur « ***Add >*** ». Le composant est alors ajouté aux composants sélectionnés. Cliquer enfin sur OK.

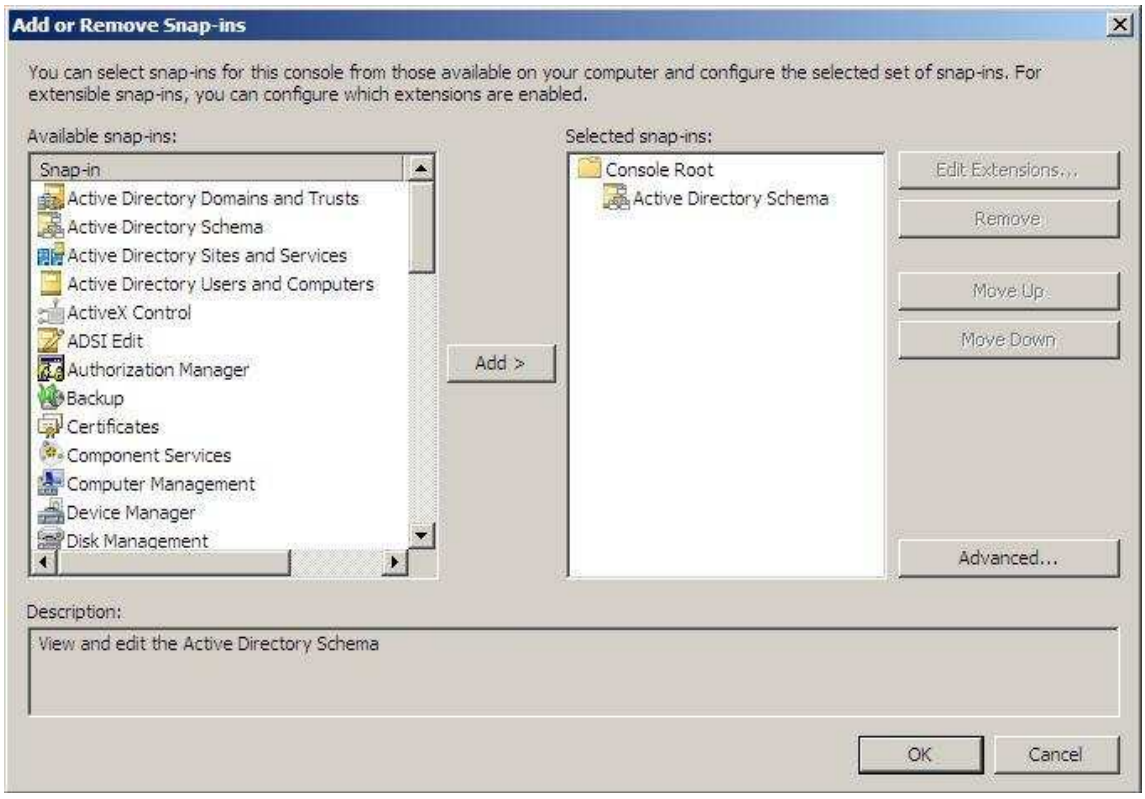

Figure 4.7 Choix du composant à ajouter

5. Groupes Active Directory :

Les groupes[3] dans Active Directory servent à rassembler plusieurs objets comme des utilisateurs[4] ou des ordinateurs dans une même entité pour simplifier l'administration.

Lors de l'installation de l'annuaire AD, le système installe certains groupes et utilisateurs par défaut avec des droits et des autorisations prédéfinis. Comme par exemple à l'installation de Windows Vista où le système installe les comptes « *administrator* » et « *guest* » par défaut.

Il existe plusieurs sortes de groupes, on différentie ceux-ci avec une caractéristique appelée « étendue de groupe » ou « Group Scope ». Celle-ci va permettre de restreindre l'accès à des objets de la forêt.

On peut observer trois sortes de groupes :

- **Domain Local Groups**

  Généralement ce groupe est utilisé lorsque l'on veut appliquer des autorisations pour l'accès à une application. On ne peut assigner des autorisations que sur les ressources se trouvant dans le même domaine que là où le groupe a été crée.

  On peut ajouter des utilisateurs de n'importe quel domaine au groupe « Domain Local Groups ».

- **Global Groups**

  On utilise souvent ce type de groupe pour rassembler des utilisateurs afin de simplifier l'administration. Dans ce groupe, on ne peut ajouter que des utilisateurs faisant partis du même domaine que le « Global Groups » créé.

[3] http://technet.microsoft.com/en-us/library/Bb727067.aspx

[4] http://www.microsoft.com/technet/prodtechnol/windowsserver2003/fr/library/ServerHelp/1631acad-ef34-4f77-9c2e-94a62f8846cf.mspx?mfr=true

- **Universal Groups**

  Ce type de groupe est généralement utilisé lorsque l'on veut partager des ressources entres plusieurs domaines par exemple ou lorsque l'on veut regrouper plusieurs « Global Groups » entre eux. On peut ajouter des utilisateurs de n'importe quel domaine à ce groupe.

  Dans ce projet, l'utilisation de groupes universelle est inutile étant donné que l'on a qu'un seul domaine.

Les différents groupes crées sont rassemblés dans 2 containers différents, le premier est le container « **Builtin** » et le second « **Users** ».

Figure 5.1 Container crées par défaut

Je vais dans le chapitre suivant juste présenter ces deux groupes sachant que dans mon travail je n'ai pas utilisé ces groupes préinstallés.

J'ai utilisé des groupes que j'ai crée moi-même pour une avoir une architecture plus personnalisée et gérer de la façon que je veux, les différentes autorisations accordées aux groupes et utilisateurs.

5.1 Container Builtin :

Le container « **Builtin** » contient les groupes préinstallé avec une étendue au domaine local. On utilise généralement ces groupes pour rassembler des groupes de sécurité globale auxquels ont va attribuer des autorisations d'accès à différentes applications.

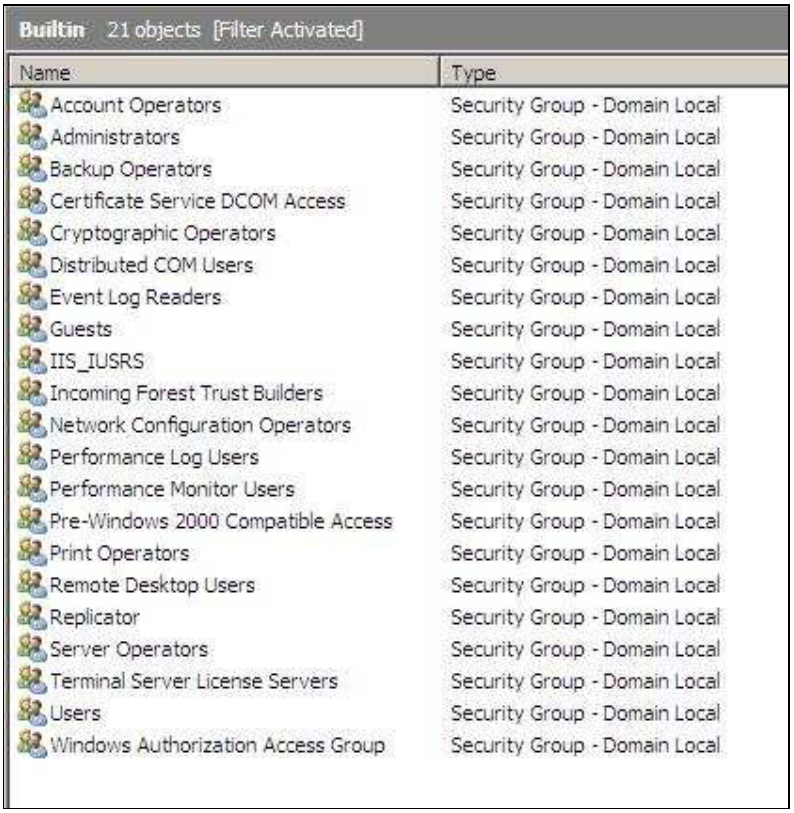

Figure 5.2 Tableau des différents groupes du container « Builtin »

Administrators :

Ce groupe possède le contrôle total des contrôleurs de domaine, il est donc à utilisé avec précaution. Ce groupe contient le compte « Administrator » et les groupes « Domain Admins » et « Enterprise Admins ».

Account Operators :

Ce groupe permet de configurer tous les objets de la forêt comme par exemple les utilisateurs, les ordinateurs et les groupes (ajout, modification, suppression) mais il ne permet pas de modifier le groupe « Administrators », « Domain Admin » ainsi que l'OU « Domain Controllers ».

Backup Operators :

Les membres de ce groupe peuvent sauvegarder et restaurer les fichiers des contrôleurs de domaine.

Print Operators :

Les membres de ce groupe ont la gestion des imprimantes du réseau.

Server Operators :

Les membres qui font partis de ce groupe n'ont que des privilèges simples de maintenance, ils ont la possibilité de lire les informations du domaine et de crée des ressources partagées par exemple.

Users :

Dans ce groupe se trouve les utilisateurs. Ceux-ci sont autorisés à effectuer des tâches courantes, comme lancer certaines applications, utiliser des imprimantes mais n'ont aucune droits de modification du contrôleur de domaine.

Guest :

Ce groupe est généralement utilisé pour accueillir des utilisateurs temporaires avec des droits restreins. Un profil est crée temporairement lorsque l'utilisateur ouvre une session et est supprimé lorsque l'utilisateur ferme la session.

5.2 Container Users :

Le container « **Users** » contient des groupes de sécurité automatiquement créés lors de la création du domaine avec pour la plupart une étendue globale. On va généralement utiliser ces groupes pour rassembler des utilisateurs. On va ensuite donner des autorisations à ces groupes qui se répercuteront sur les utilisateurs pour ne pas devoir donner les autorisations pour chaque utilisateur séparément.

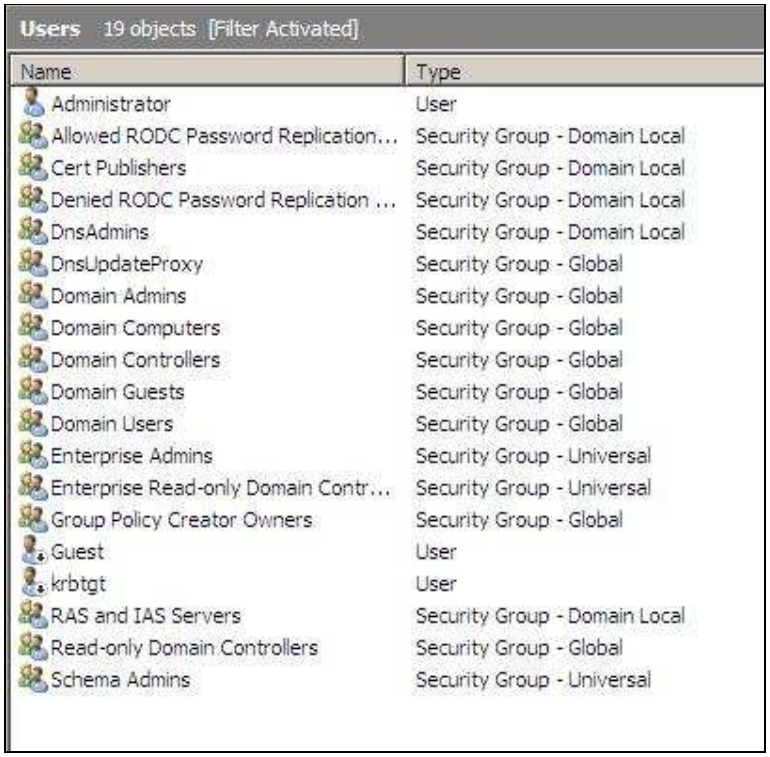

Figure 5.3 Tableau des différents groupes du container « Users »

Domain Admins :

Les utilisateurs de ce groupe ont un contrôle total sur le domaine. Ce groupe est automatiquement ajouté au groupe des administrateurs correspondant dans chacun des domaines.

DnsAdmins :

Les membres de ce groupe sont chargés de la configuration des serveurs DNS du réseau.

Domain Computers :

Ce groupe contient la liste des ordinateurs du domaine.

Domain Guests :

Ce groupe contient la liste des utilisateurs invités du domaine.

Domain Users :

Ce groupe contient la liste des utilisateurs du domaine.

Enterprise Admins :

Les membres de ce groupe ont un accès complet sur la configuration de tous les contrôleurs de domaine de la forêt AD.

Schema Admins :

Ce groupe permet aux utilisateurs de modifier le schéma AD.

6. Autorisations NTFS

6.1 Système de fichier NTFS

NTFS (New Technology File System)[5] est le système de fichiers utilisé par la famille NT, c'est-a-dire Windows NT, 2000, XP et Vista. Il est le remplaçant de l'ancien système de fichiers FAT qui était présent dans les anciennes versions de Windows comme Windows 95, 98 et ME.

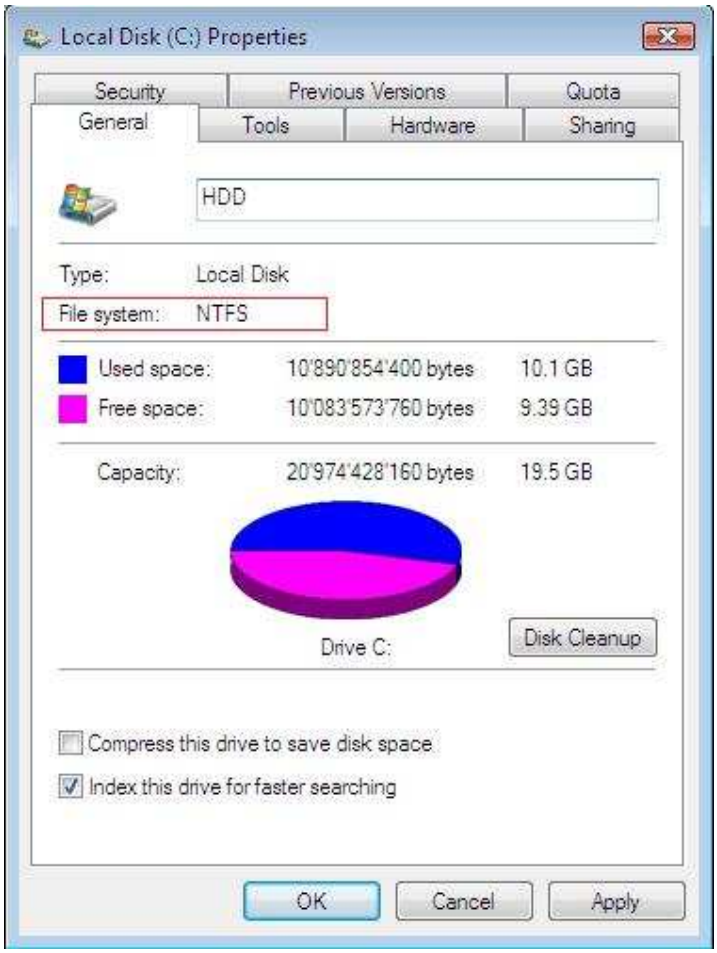

Figure 6.1 Système de fichiers NTFS

L'avantage de cette nouvelle technologie de fichiers est la sécurité apportée. Dans le système de fichier FAT, aucune protection sur les fichiers et dossiers n'était possible.

[5] http://technet2.microsoft.com/windowsserver/en/library/59a9462a-cbdd-45e7-828b-12c6cd9ae4781033.mspx?mfr=true

Document détaillé sur NTFS : http://www.mp-arpajon.ac-versailles.fr/IMG/pdf/Autorisations_NTFS.pdf

Avec le système NTFS on va pouvoir donner des permissions d'accès aux fichiers et aux dossiers ainsi que des actions possibles sur ceux-ci comme par exemple, l'écriture ou la suppression.

Un fichier stocké sur une partition NTFS comporte une « liste de contrôle d'accès discrétionnaire » (DACL)[6] qui répertorie les utilisateurs et les groupes autorisées à accéder à la ressource ainsi que les privilèges possibles sur cette ressource.

Les utilisateurs et les groupes qui composent cette DACL sont appelés « entrées de contrôle d'accès » (ACE)[7].

Les autorisations NTFS disponibles sont répertoriées sous l'onglet « ***Security*** » dans les propriétés de l'objet.

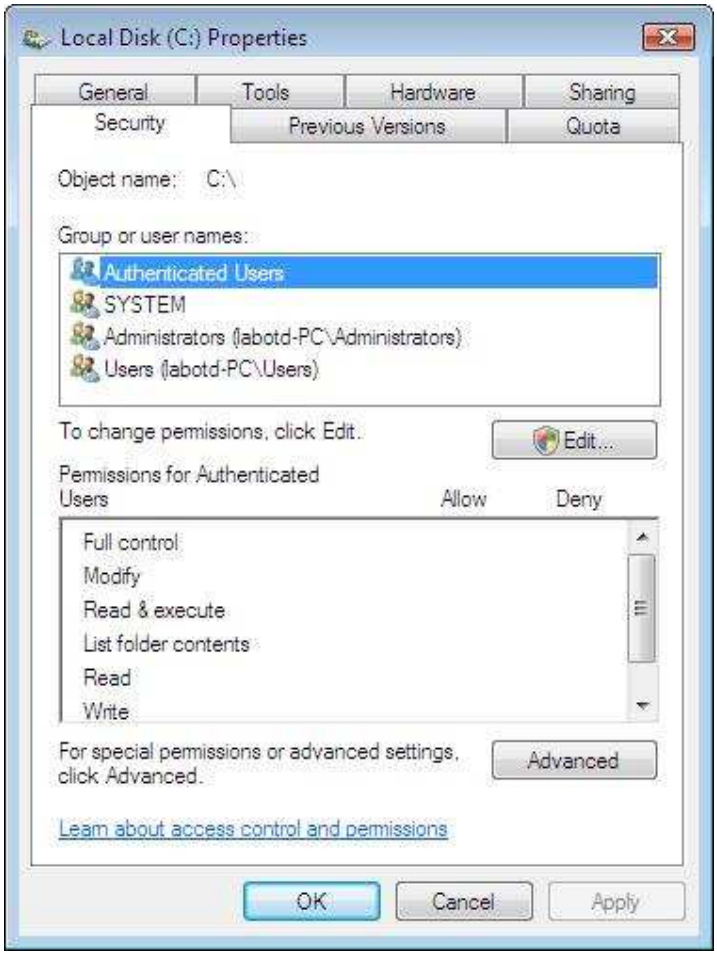

Figure 6.2 Onglet Security

[6] http://msdn2.microsoft.com/en-us/library/aa374872.aspx

[7] http://msdn2.microsoft.com/en-us/library/Aa374868.aspx

6.2 Autorisations de base NTFS

Il existe des autorisations de base NTFS qui permettent d'exécuter des tâches simples sur les objets et des autorisations avancées qui permettent d'effectuer des tâches supplémentaires plus précises.

Les autorisations différents légèrement si on les applique sur un fichier ou sur un dossier.

6.2.1 Autorisations de base NTFS sur un fichier

- Read
- Write
- Read & Execute
- Modify
- Full control

6.2.2 Autorisations de base NTFS sur un dossier

- Read
- Write
- Read & Execute
- Modify
- List folder contents
- Full control

6.3 Autorisations avancées NTFS

Dans l'onglet « ***Security*** » on a donc un aperçu des différentes autorisations de base NTFS mais il existe beaucoup d'autres autorisations plus précises quant à leurs actions.

Lorsqu'on se trouve sur l'onglet « ***Security*** », en appuyant sur le bouton « ***Advanced*** », on accède à une vue plus détaillées des autorisations accordées au dossier ou au fichier.

Figure 6.3 Vue détaillée des autorisations NTFS

En appuyant sur le bouton « ***Edit…*** », on accède donc à toutes les autorisations NTFS que l'on va pouvoir attribuer.

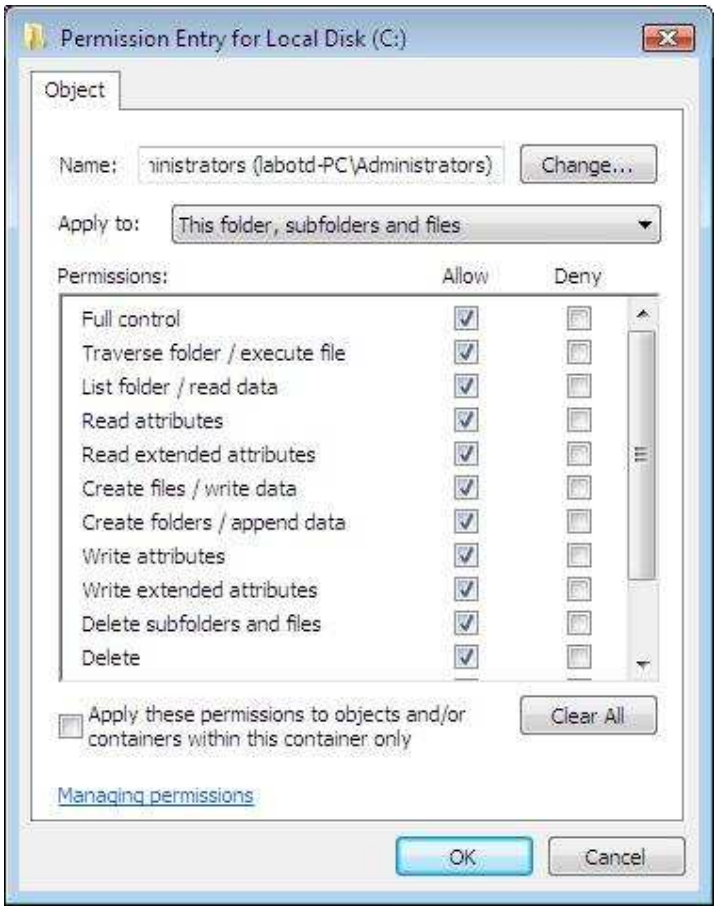

Figure 6.4 Autorisations avancées NTFS

Lors de la délégation de contrôle sur les objets de l'annuaire, on va devoir donc modifier les autorisations NTFS. Les autorisations liées à l'annuaire ne sont pas les mêmes que celle que l'on a pour les fichiers ou dossiers dans Windows.

Ces deux types d'autorisations ne sont donc pas pareils, mais cela reste des autorisations NTFS précisant quels sont les privilèges accordées à tel ou tel objet.

7. Délégation d'administration dans Active Directory

Aujourd'hui, beaucoup d'entreprises possèdent un annuaire Active Directory pour la gestion de ses utilisateurs ainsi que le partage de fichiers ou d'applications.

Les différents secteurs de l'entreprise sont généralement répartis, classés, dans des unités d'organisation différentes par exemple pour faciliter la gestion, l'administration ainsi que la maintenance de l'annuaire AD.

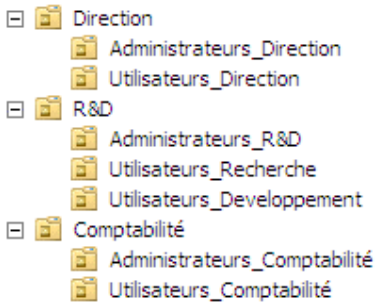

Figure 7.1 Exemple d'architecture Active Directory

Dans chaque unité d'organisation, on va généralement avoir plusieurs groupes composés eux-mêmes de plusieurs utilisateurs dont certains avec des privilèges plus ou moins élevés que d'autres.

Pour organiser et gérer les utilisateurs et les privilèges accordés à ceux-ci, on va donc avoir des personnes qui sont responsables de l'administration de l'annuaire AD. La personne qui a créé l'annuaire, a créé en même temps un compte administrateur qui possède tous les privilèges sur l'annuaire. Ce compte est à utiliser avec précaution étant donné qu'il a tous les droits sur l'annuaire.

Lorsque la taille de l'entreprise est importante et que le nombre d'utilisateurs, de groupes et de ressources est élevé, il est difficile pour une seule personne d'administrer tout l'annuaire AD. Pour simplifier la gestion, on va alors déléguer l'administration d'une ou plusieurs tâches à des « sous-administrateurs ». On peut avoir plusieurs administrateurs pour une même OU si on le souhaite. La délégation d'administration ne s'arrête pas seulement à AD, on peut tout à fait déléguer une personne qui sera responsable de la configuration DNS du serveur par exemple.

Pour déléguer des tâches d'administration[8] à des utilisateurs, on va donc modifier les autorisations NTFS (liées à l'annuaire AD) de ceux-ci pour leurs accorder ou non des privilèges sur les objets de l'annuaire. Cette délégation permet d'appliquer le principe du moindre privilège en ne donnant que les privilèges nécessaire à un administrateur. De cette façon on réduit le risque d'erreur non volontaire dans l'annuaire qui peut dans certains cas, avoir un impact important.

Il existe 2 sortes d'administrations dans Active Directory :

- **Administration des services**

  Consiste en la gestion des composantes d'infrastructure de l'annuaire tel que les contrôleurs de domaine par exemple.

  Les privilèges accordés aux administrateurs de service sont élevés et donc le principe du moindre privilège est recommandé dans ce cas-la.

  On peut par exemple déléguer l'administration du contrôleur de domaine à un administrateur chargé exclusivement de cette tâche.

- **Administration des données**

  Gestion des objets de l'annuaire tel que les comptes utilisateurs, les groupes et les ressources partagées par exemple.

  Pour ces tâches d'administration, des privilèges moins importants sont nécessaires que pour un administrateur de services.

  On peut par exemple avoir une personne chargée de gérer les comptes utilisateurs, une autre les ordinateurs et enfin une chargée des partages de l'entreprise.

[8] http://www.microsoft.com/technet/prodtechnol/windowsserver2003/fr/library/ServerHelp/60096a04-8494-4551-bfd6-3aebadddc3fe.mspx?mfr=true

Best Practices for Delegating AD Administration: http://go.microsoft.com/fwlink/?linkid=22707

Sécurisation des groupes d'administration :
http://www.microsoft.com/france/technet/securite/sec_ad_admin_groups.mspx

La délégation d'administration peut se définir en 3 phases :

- Définition des rôles des administrateurs
- Développement d'un modèle d'architecture
- Utilisation des comptes administrateurs délégués

7.1 Définition des rôles des administrateurs

Pour commencer, il faut définir toutes les tâches d'administration qui vont devoir être effectuée sur l'annuaire AD. Définir les tâches des administrateurs de services ainsi que ceux des administrateurs de données.

Il faut évaluer les tâches pour définir quels sont celles qui seront effectuées le plus souvent, celles qui demandent une plus grande compétence et celles qui demandent des privilèges plus élevés.

Les tâches qui ne demandent pas de privilèges très élevés peuvent être déléguées sans problème à un utilisateur comme par exemple la possibilité de réinitialiser le mot de passe d'un utilisateur, tandis que celle qui sont effectuées moins souvent et qui demande un niveau élevé sont plus difficiles à déléguer pour ne pas mettre en péril la sécurité de l'entreprise comme la gestion du contrôleur de domaine par exemple.

7.2 Développement d'un modèle d'architecture

Deuxièmement, lorsque les rôles administratifs sont définis, il convient de mettre en place un modèle d'unités d'organisation et de groupes de sécurités. Cette partie permet de faciliter la gestion de l'annuaire et d'augmenter la sécurité de l'architecture.

On va crée généralement une OU, dans laquelle on va crée des groupes de sécurité qui eux, contiendront les comptes utilisateurs.

De cette manière l'administration sera simplifié en appliquant les autorisations aux OU et aux groupes. De cette façon, il n'est pas nécessaire de devoir appliquer les

autorisations pour chaque utilisateur séparément. Ce travail deviendrait vite très laborieux si le nombre d'utilisateurs est important.

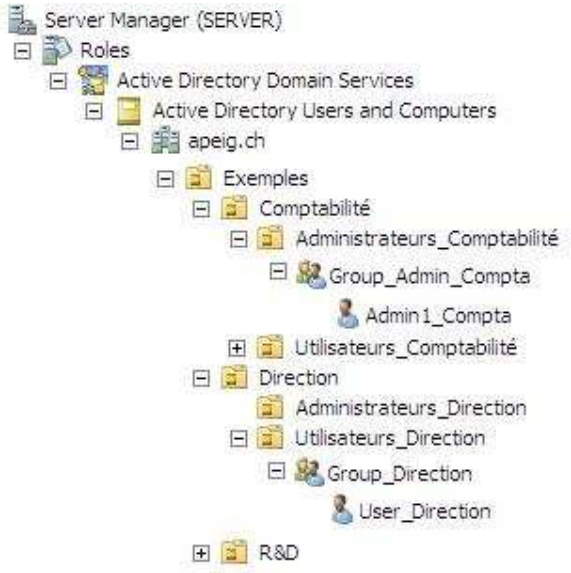

Figure 7.2 Architecture Active Directory avec groupes et comptes

7.3 Utilisation des comptes administrateurs délégués

Finalement, il reste à définir quels sont les tâches administratives que l'on va déléguées, et à qui l'on va les attribuées.

Pour augmenter la sécurité au maximum, il est recommandé d'utiliser le principe du moindre privilège. Un utilisateur à qui on confie une tâche d'administration, doit seulement pourvoir exécuter les tâches associées à son rôle.

On crée donc un compte spécifiquement pour chaque tâche d'administration à qui on attribue un certains nombres d'autorisations en fonction du rôle du compte. Aucune autre action ne doit pouvoir être effectuée à partir de ce compte. De cette façon le principe du moindre privilège est respecté.

Si un utilisateur est chargé de la gestion des comptes par exemple, il ne doit pas pouvoir intervenir sur la configuration DNS du serveur ou pouvoir supprimer des ordinateurs de l'annuaire.

7.4 Procédure de délégation d'administration

Lorsque l'on veut déléguer des droits d'administrations à un utilisateur, il existe 2 méthodes différentes qui aboutissent au même résultat :

- Assistant de délégation de contrôle
- Modification manuelle des autorisations NTFS

7.4.1 Assistant de délégation de contrôle

La première méthode est donc d'utiliser l'assistant de délégation de contrôle qui va crée les autorisations NTFS en fonction des tâches que l'on souhaite pouvoir effectuer avec le compte.

Pour lancer l'assistant de délégation de contrôle :

1. Faites un clic droit sur l'OU auquel vous voulez déléguer le contrôle et sélectionner « ***Delegate Control…*** »

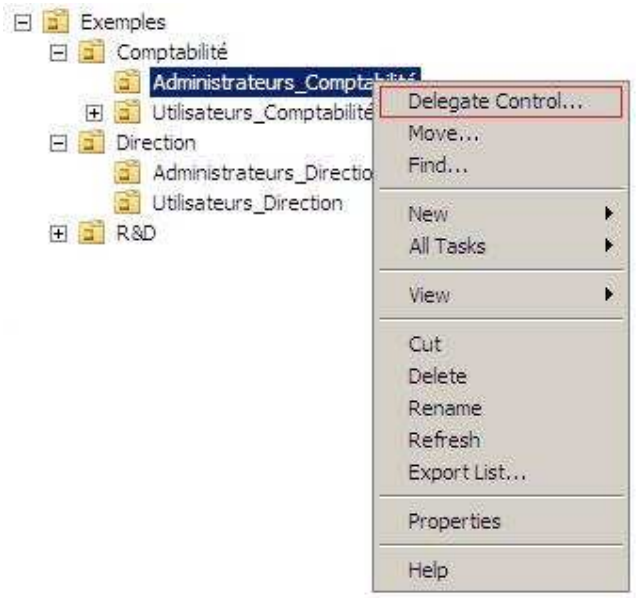

Figure 7.3 Sélectionner Delegate Control…

2. Sur le premier écran qui apparaît cliquez sur « ***Next*** », vous arrivez ensuite sur la fenêtre sur laquelle vous devez ajouter les comptes auxquelles vous voulez déléguer le contrôle. Pour ajouter un compte, appuyer sur le bouton « ***Add…*** ».

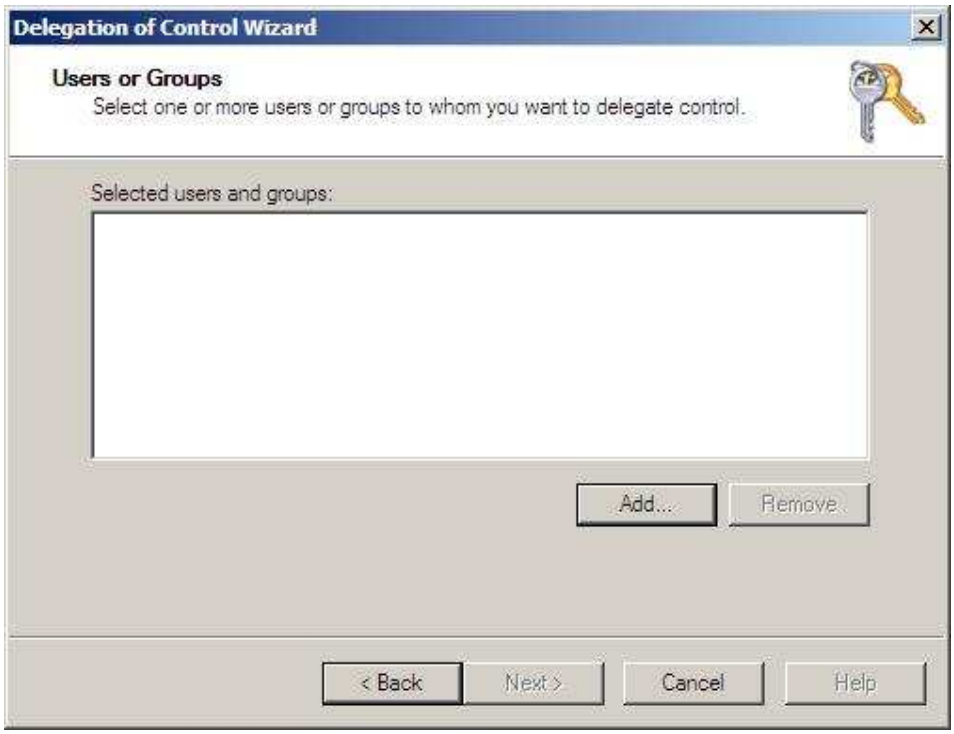

Figure 7.4 Choix des comptes pour la délégation

3. Ajouter les utilisateurs à qui vous voulez octroyer des privilèges d'administration.

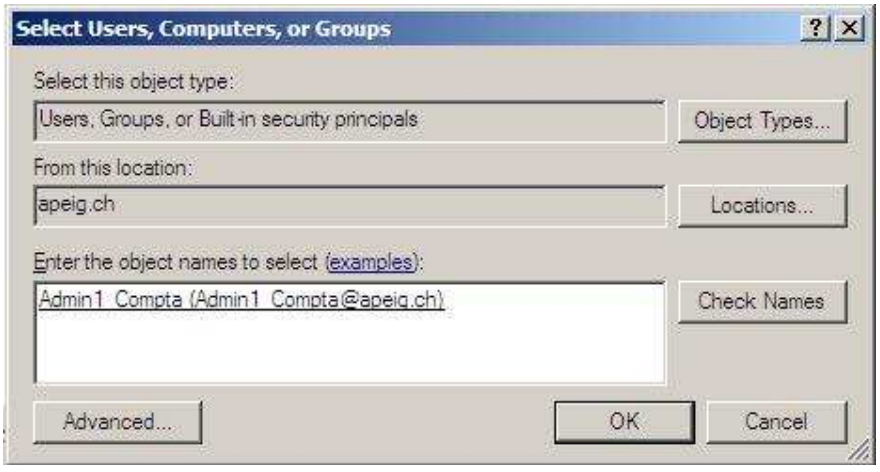

Figure 7.5 Ajout des utilisateurs

4. Sur cet écran vous allez choisir les actions que vont pouvoir exécuter les administrateurs. Sélectionner les actions autorisées en cochant les cases et ensuite cliquez sur « ***Next…*** »

   Pour donner des privilèges avancés, Sélectionner « **Create a custom task to delegate** » et cliquez sur « ***Next…*** ».

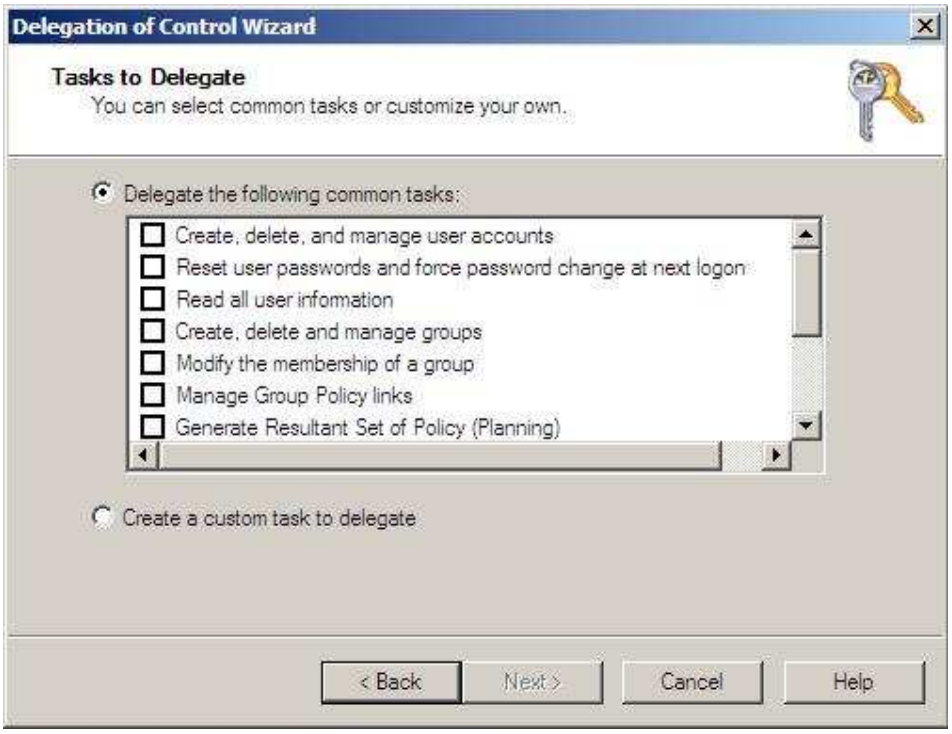

Figure 7.6 Choix des actions autorisées

5. Finalement sur le dernier écran, vous trouvez un résumé des choix effectués. Si cela correspond à la configuration souhaitée, cliquez sur « ***Finish*** » pour terminer l'assistant.

Figure 7.7 Fin de l'assistant

Après avoir effectué la délégation grâce l'assistant, celui-ci a donc crée les autorisations NTFS nécessaire pour correspondre à la configuration indiquée dans l'assistant.

Voici un exemple d'autorisations NTFS crées par l'assistant si on sélectionne à la Figure 7.6 « **Create, delete and manage user accounts** ».

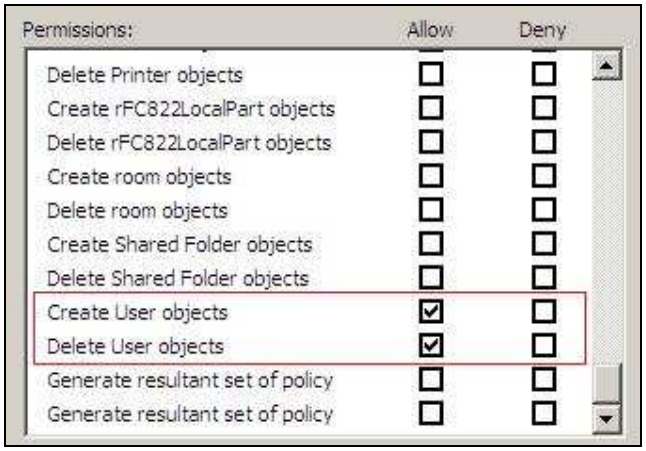

Figure 7.8 Autorisation NTFS crées par l'assistant

L'assistant tente de simplifier la délégation de contrôle en proposant à l'utilisateur le choix des actions sans devoir rentrer dans les permissions NTFS du conteneur auquel on veut ajouter des autorisations.

Dans un premier temps, l'assistant propose un choix de tâche simple comme par exemple :

- L'ajout, la modification ou la suppression de comptes utilisateurs
- La possibilité de réinitialiser les mots de passe des comptes
- Lire les propriétés d'un utilisateur
- L'ajout/modification/suppression de groupes
- Modifier l'appartenance d'un utilisateur à un groupe

Mais on peut, avec l'assistant, assigner des tâches plus spécifiques en allant dans les tâches personnalisées.

A partir de là, on a le choix d'abord d'attribuer les autorisations à tous les objets du conteneur ou seulement à un type précis d'objet comme les utilisateurs ou les imprimantes par exemple.

Lorsque ce choix est fait, on va alors pouvoir choisir le type d'autorisation que l'on veut attribuer avec une granularité beaucoup plus grande comme par exemple :

- La possibilité de créer n'importe quel type d'objets ou alors de ne pouvoir crée qu'un seul type d'objets comme par exemple :
  - Un utilisateur
  - Un groupe
  - Une imprimante

- Choisir quels sont les propriétés d'un objet que l'on va pouvoir lire/modifier
  - Nom
  - Adresse
  - Description

7.4.2 Modification manuelle des autorisations NTFS

La seconde méthode pour déléguer des droits d'administrations, est de modifier les autorisations NTFS manuellement. On peut de cette façon choisir directement les privilèges dont l'administrateur va bénéficier.

Toutes les tâches qui étaient proposées par l'assistant peuvent être configurées manuellement en modifiant directement les autorisations NTFS.

Pour modifier les autorisations NTFS sur une *OU* :

1. Par défaut on ne peut pas accéder aux autorisations NTFS, il faut donc d'abord aller dans l'onglet « ***View*** » et cocher « ***Advanced Features*** ».

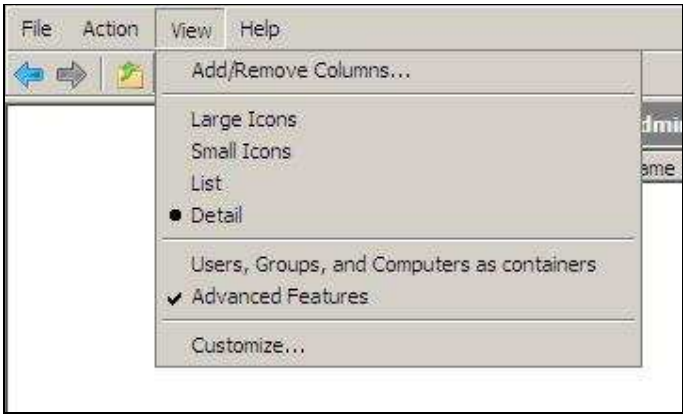

Figure 7.9 Advanced Features

2. Ensuite sélectionnez l'OU à laquelle vous voulez modifier les autorisations NTFS en faisant un clic droit dessus et en sélectionnant « ***Properties*** ».

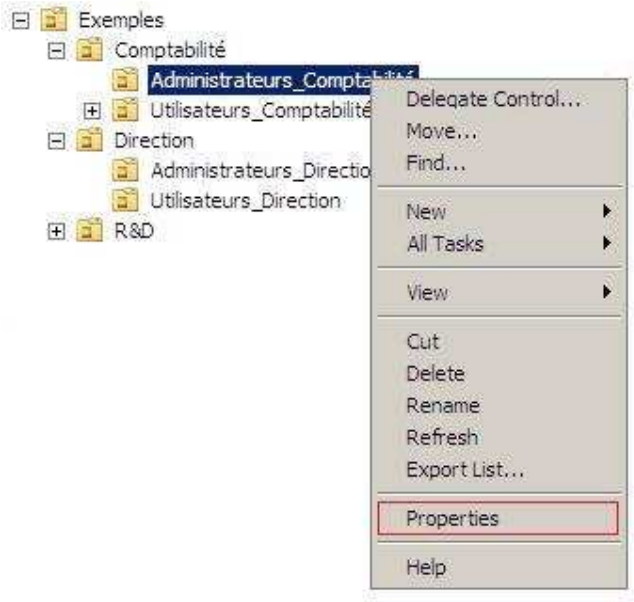

Figure 7.10 Sélectionnez « Properties »

3. Vous arrivez donc dans les propriétés de l'OU. Sélectionnez l'onglet « ***Security »*** maintenant disponible pour accéder aux autorisations NTFS. Vous voyez donc toutes les autorisations NTFS accordées aux utilisateurs et aux groupes sur l'OU que vous avez sélectionnez.

   Vous pouvez à partir de là, ajouter ou supprimer des utilisateurs ainsi que des groupes et leur accorder des autorisations en cochant les cases correspondantes à la tâche souhaitée.

   Sur cette fenêtre se trouve les autorisations NTFS basiques. Pour accéder aux autorisations NTFS avancées, cliquez sur le bouton « ***Advanced…*** »

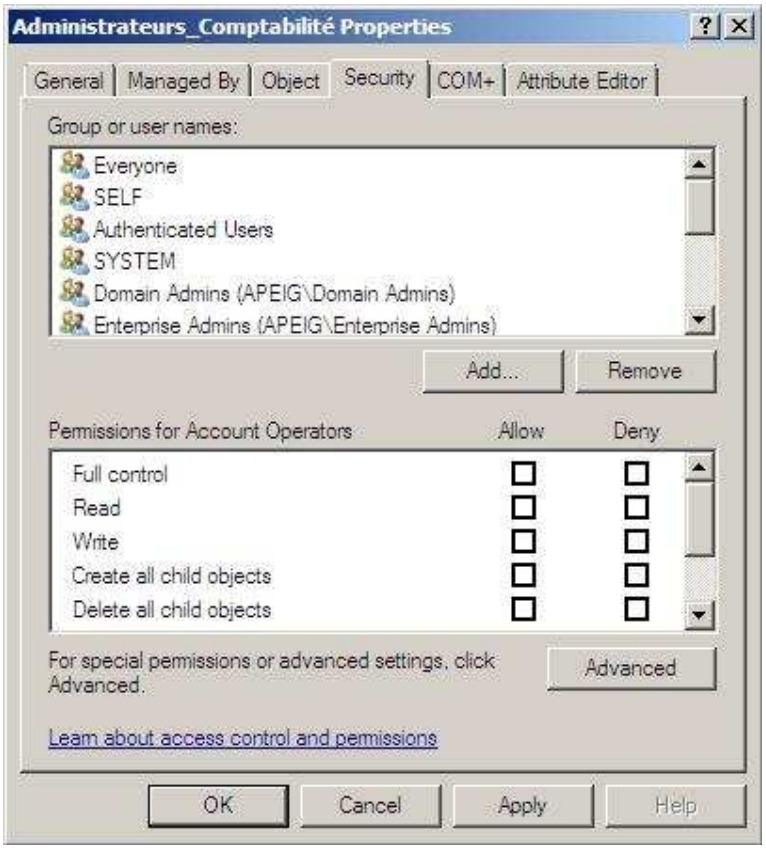

Figure 7.11 Autorisations NTFS

4. Lorsque vous êtes satisfaits des réglages, cliquez sur « ***OK*** » pour appliquer les modifications.

7.5 Taskpad

Lorsque l'on doit modifier les propriétés d'un objet, il faut parcourir l'arborescence de l'annuaire pour arriver à l'endroit où l'on veut effectuer les modifications, choisir l'objet à modifier et effectuer les modifications.

Pour faciliter l'administration de l'annuaire AD et l'accès aux objets, on peut installer une « ***Taskpad View*** » que l'on va placer dans une OU de son choix et qui va permettre d'afficher toutes les actions possibles sur les objets contenus dans cette OU. Les différentes actions affichées vont devoir être configurées.

Pour afficher une « ***Taskpad View*** » sur une OU :

1. Faites « ***Start*** » puis « ***Run…*** » et lancer la console « ***MMC*** ». Ajouter le composant enfichable « ***Active Directory Users and Computers*** ». Vous avez donc l'architecture de votre annuaire AD.

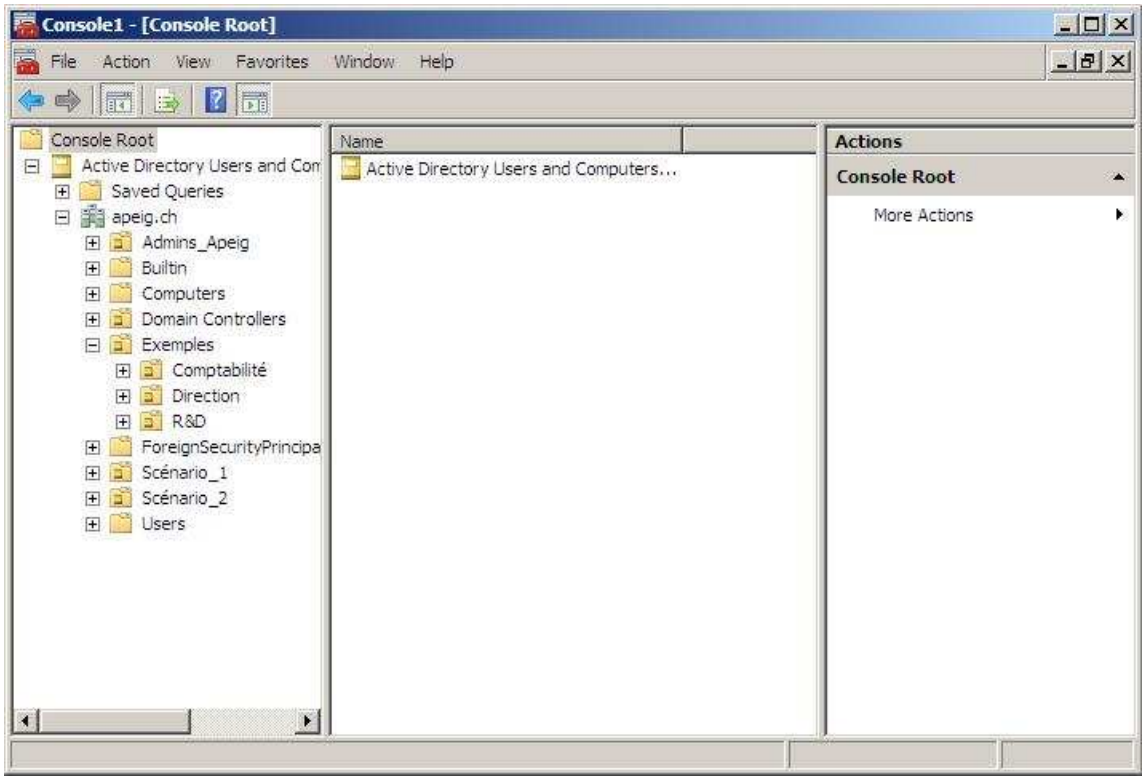

Figure 7.12 Console MMC

2. Sélectionnez l'OU sur laquelle vous voulez ajouter la « *Taskpad View* », puis faites un clic droit sur celle-ci et sélectionnez « ***New Taskpad View…*** » pour lancer l'assistant.

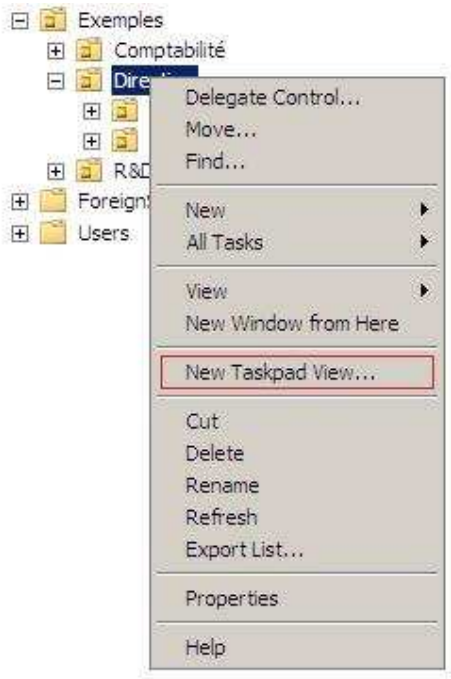

Figure 7.13 Sélectionnez « New Taskpad View… »

3. Dans le premier écran cliquer sur « *Next* », ensuite vous arriver sur un écran sur lequel vous pouvez choisir la disposition de la *Taskpad* (horizontale, verticale,…) et si vous voulez voir apparaitre explicitement la description de la tâche que vous pouvez effectuer. Cliquer sur « *Next* » lorsque vous avez fait votre choix.

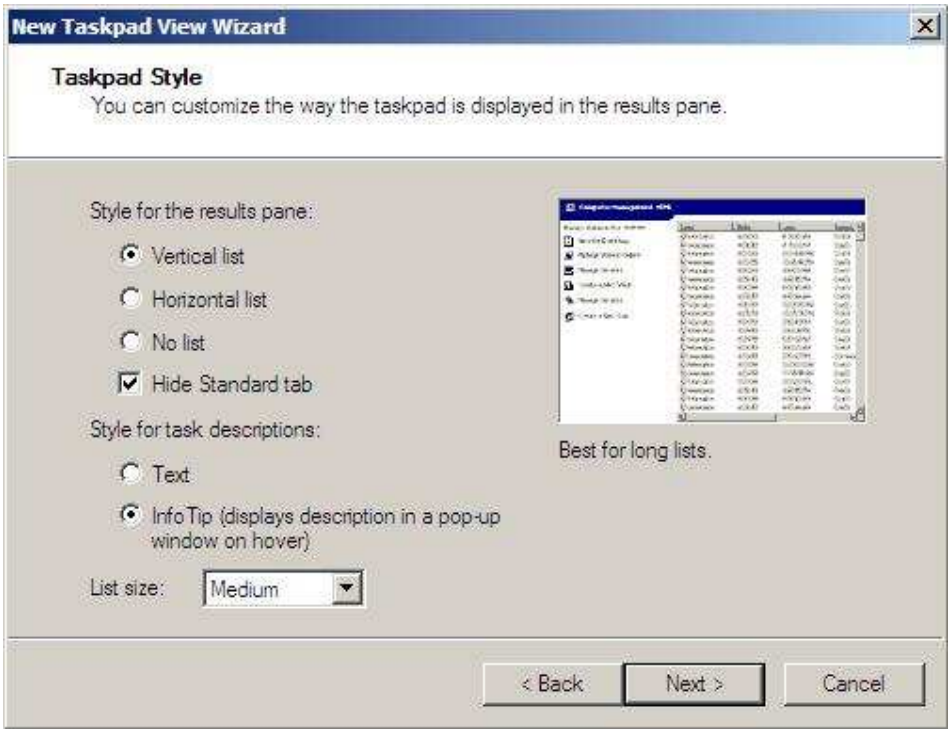

Figure 7.14 Choix de l'affichage de la « Taskpad »

4. Sur cet écran, vous devez choisir si vous voulez que la Taskpad apparaisse seulement sur l'OU que vous avez sélectionnée ou sur toutes les OU de l'annuaire.

Figure 7.15 Choix de l'étendue d'application

5. Ensuite, vous devez indiquer le nom et la description de la « *Taskpad* ». Lorsque c'est fait cliquer sur « *Next* ». Finalement sur le dernier écran, appuyer sur « *Finish* ».

   Après avoir fait ceci, un second assistant se lance pour configurer les tâches. Cliquer sur « *Next* ». Vous arrivez sur un écran vous demandant quel type de commande vous voulez utiliser (menu, shell,…). Cliquer sur « *Next* » lorsque vous avez fait votre choix.

Figure 7.16 Choix du type de commande

6. Dans l'écran suivant, vous allez devoir sélectionner la tâche que vous voulez effectuer. Dans la fenêtre de gauche se trouve les OU sur lequel vous pouvez effectuer une tâche et sur la fenêtre de droite, les tâches disponibles.

   On constate que ces tâches ressemblent aux actions disponibles dans l'assistant de délégation de contrôle. C'est normal puisque en fait ce sont les mêmes actions à savoir par exemple, l'ajout d'un utilisateur ou d'un groupe.

   Les actions disponibles sont celles que l'ont aurait en faisant un clic droit sur l'OU sélectionnée. Cliquez sur « *Next* » lorsque vous avez choisi l'action.

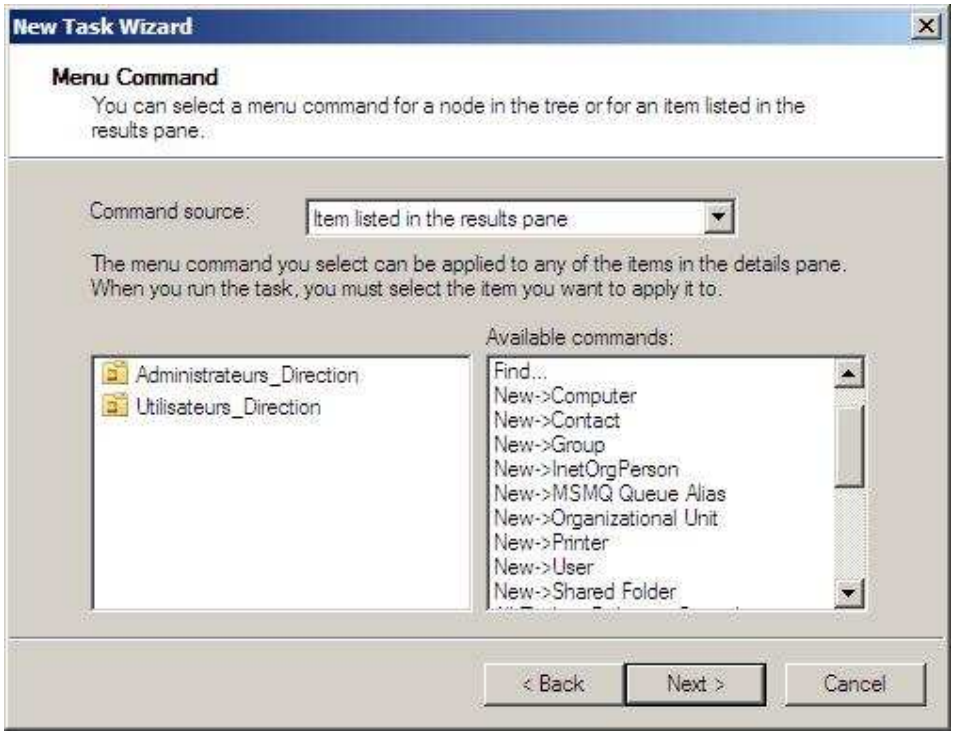

Figure 7.17 Choix de la tâche à appliquer

7. Ensuite, sur l'écran suivant, vous indiquez le nom et la description que vous voulez donner à la tâche sélectionnée. Cliquez sur « *Next* » ensuite.

   Sur l'écran suivant vous devez sélectionnez l'icône que vous voulez donner à l'action. Vous pouvez choisir une icône préinstallée ou une icône personnalisée. Appuyer ensuite sur « *Next* ».

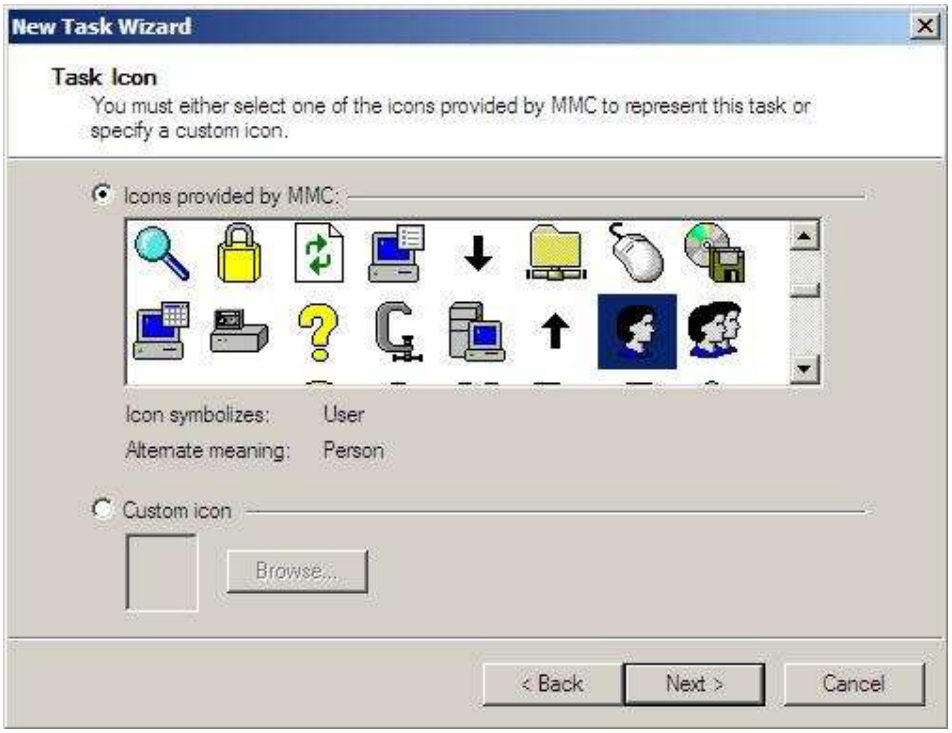

Figure 7.18 Choix de l'icône associée

8. Finalement, sur le dernier écran, vous avez un résumé de ce que vous avez sélectionné. Si cela correspond à la configuration souhaitée, cliquez sur « Finish » pour terminer l'assistant.

Figure 7.19 Résumé de la configuration

On constate alors qu'une liste avec les tâches que l'on peut effectuer est apparu à coté des OU.

Si pendant l'assistant, à la **Figure 7.17**, on a sélectionné par exemple « ***New->User*** », on constate que si on sélectionne une OU, on a une icône qui apparait avec l'action sélectionner qui par exemple ici nous donne l'opportunité de créer un utilisateur dans l'OU.

Figure 7.20 Action crée par l'assistant

On peut tout à fait rajouter des actions en éditant la « *Taskpad* ». Il suffit de faire un clic droit sur l'OU et sélectionnez « ***Edit Taskpad View…*** ». Allez ensuite sous l'onglet « ***Tasks*** » et faites « ***New…*** »

Figure 7.21 Actions rajoutée par l'utilisateur

Pour conserver la configuration crée et pouvoir revenir directement dans l'OU dans laquelle on a crée la « *Taskpad* », on va devoir sauvegarder la console MMC. La sauvegarde est un fichier avec l'extension « **.msc** »

Pour faire ceci, dans la console MMC, cliquez sur « ***File*** », et ensuite « ***Save As…*** », donnez un nom à la sauvegarde et choisissez l'endroit où vous voulez sauvegarder la console. Cliquez sur le bouton « ***Save*** » lorsque vous avez fait votre choix.

Vous avez donc crée un raccourci à la console MMC, qui lorsque vous le lancer, va directement dans l'OU que vous avez sélectionné dans l'assistant avec la configuration de la « *Taskpad* » que vous avez indiquez.

Figure 7.22 Raccourci console MMC

Si vous quitter la console MMC sans sauvegarder, vous ne perdrez pas les configurations que vous avez faits au niveau des OU ou des utilisateurs mais par contre vous perdrez la configuration de la « *Taskpad* » que vous avez faite.

7.6 Scénario pratique

7.6.1 Spécification :

Chaque département à une *OU* spécifique contenant ses administrateurs locaux, ses ordinateurs, ses partages et ses utilisateurs.

Une *OU «* **Admins »** qui contient

- Les utilisateurs du helpdesk
- Les responsables de la gestion des droits d'accès (GDA)
- Les administrateurs du serveur DNS
- Les administrateurs du contrôleur de domaine
- Les administrateurs du scénario

Les administrateurs du scénario ont les mêmes privilèges que les responsables GDA, mais ils peuvent en plus, crée des OU supplémentaires dans l'organisation.

Puis dans chaque département, on trouve un administrateur séparé pour la gestion des ordinateurs, des partages, des imprimantes et des utilisateurs du département réunis dans l'*OU* « **Admins** ». L'administrateur local de l'OU peut crée des utilisateurs et des groupes dans son département.

Pour l'accès à ces ressources, une *OU* différente est crée pour chaque type de ressource à savoir :

- Computers
- Users
- Printers
- Share

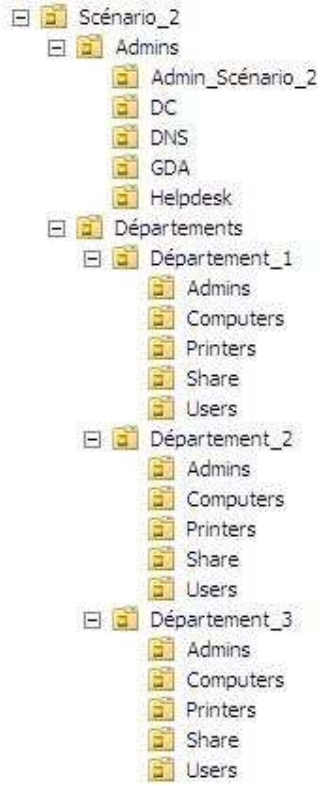

Figure 7.23 Architecture du scénario 2

« *OU* » Admins :

- **Admin_Scénario_2**

  Administrateurs des comptes du scénario avec la possibilité de crée des OU

- **DC**

  Administrateurs du contrôleur de domaine

- **DNS**

  Administrateurs du serveur DNS

- **GDA**

  Administrateurs des comptes utilisateurs

- **Helpdesk**

  Utilisateurs ayant la possibilité de réinitialiser les mots de passes des utilisateurs

« *OU* » Département_X :

- **Admins**

  Administrateurs du département X

  - Comptes
  - Ordinateurs
  - Imprimantes
  - Partages

- **Computers**

  Contient les ordinateurs du département

- **Users**

  Utilisateurs du département

- **Printers**

  Contient les imprimantes du département

- **Share**

  Contient les fichiers et dossiers partagés du département

7.6.2 Réalisation :

	Admin Users	Admin Computers	Admin Printers	Admin Share
Create user object	X			
Delete user object	X			
Create group object	X			
Delete group object	X			
Create OU object				
Delete OU object				
Create Computer object		X		
Delete Computer object		X		
Create Printer object			X	
Delete Printer object			X	
Create Share object				X
Delete Share object				X
Reset Password				

Tableau 7.1 Autorisations NTFS accordées aux comptes administrateurs délégués

	Admin Scénario_2	GDA	Helpdesk
Create user object	X	X	
Delete user object	X	X	
Create group object	X	X	
Delete group object	X	X	
Create OU object	X		
Delete OU object	X		
Create Computer object			
Delete Computer object			
Create Printer object			
Delete Printer object			
Create Share object			
Delete Share object			
Reset Password			X

Tableau 7.6 Autorisations NTFS accordées aux comptes administrateurs délégués (suite)

	Admin Users	Admin Computers	Admin Printers	Admin Share
Read Admins OU	X			
Write Admins OU	X			
Read Computers OU		X		
Write Computers OU		X		
Read Users OU	X			
Write Users OU	X			
Read Printers OU			X	
Write Printers OU			X	
Read Share OU				X
Write Share OU				X

Tableau 7.7 Accès et autorisations aux différentes OU

	Admin Scénario_2	GDA	Helpdesk
Read Admins OU	X	X	X
Write Admins OU	X	X	X
Read Computers OU			
Write Computers OU			
Read Users OU	X	X	X
Write Users OU	X	X	X
Read Printers OU			
Write Printers OU			
Read Share OU			
Write Share OU			

Tableau 7.8 Accès et autorisations aux différentes OU (suite)

7.7 Audit

Lorsque l'on délègue une tâche administrative à un utilisateur, on veut par exemple pouvoir contrôler ses actions, vérifier que l'utilisateur ne fait pas des manipulations qu'il ne devrait pas et en cas d'erreur dans l'annuaire, comme par exemple des privilèges accordés à un groupe incorrect, pouvoir vérifier qui à fait l'erreur.

Pour contrôler les actions effectuées sur l'annuaire, on va donc utiliser les logs. Ces logs sont visibles dans l'onglet « *Event Viewer* » accessibles sur la page principale des rôles du serveur.

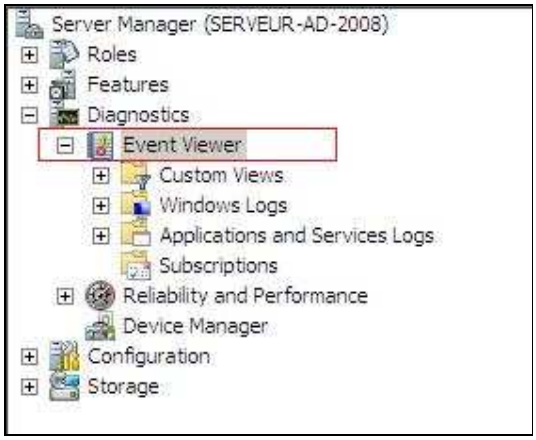

Figure 7.24 « *Event Viewer* »

Lorsqu'une action que l'on aura configurée comme étant à auditer sera effectuée, une trace de cette action sera inscrite dans l'onglet « ***Security*** », dans « ***Windows Logs*** ».

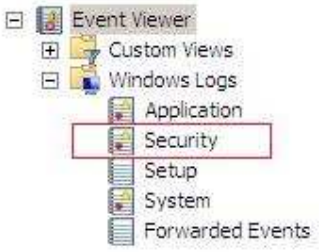

Figure 7.25 onglet « *Security* »

On peut auditer par exemple les événements suivants :

- Création d'un utilisateur
- Modification des privilèges d'un utilisateur
- Réinitialisation du mot de passe d'un utilisateur

Pour activer l'audit dans « Windows Server 2008 » :

1. Allez dans les « ***Administrative Tools*** », dans « ***Local Security Policy*** »

2. Développez l'arborescence « ***Local Policies*** » puis allez dans « ***Audit Policy*** ». Dans cet onglet sont listées toutes les actions que l'on peut auditer. Dans notre cas, nous allons auditer les actions effectuées sur l'annuaire.

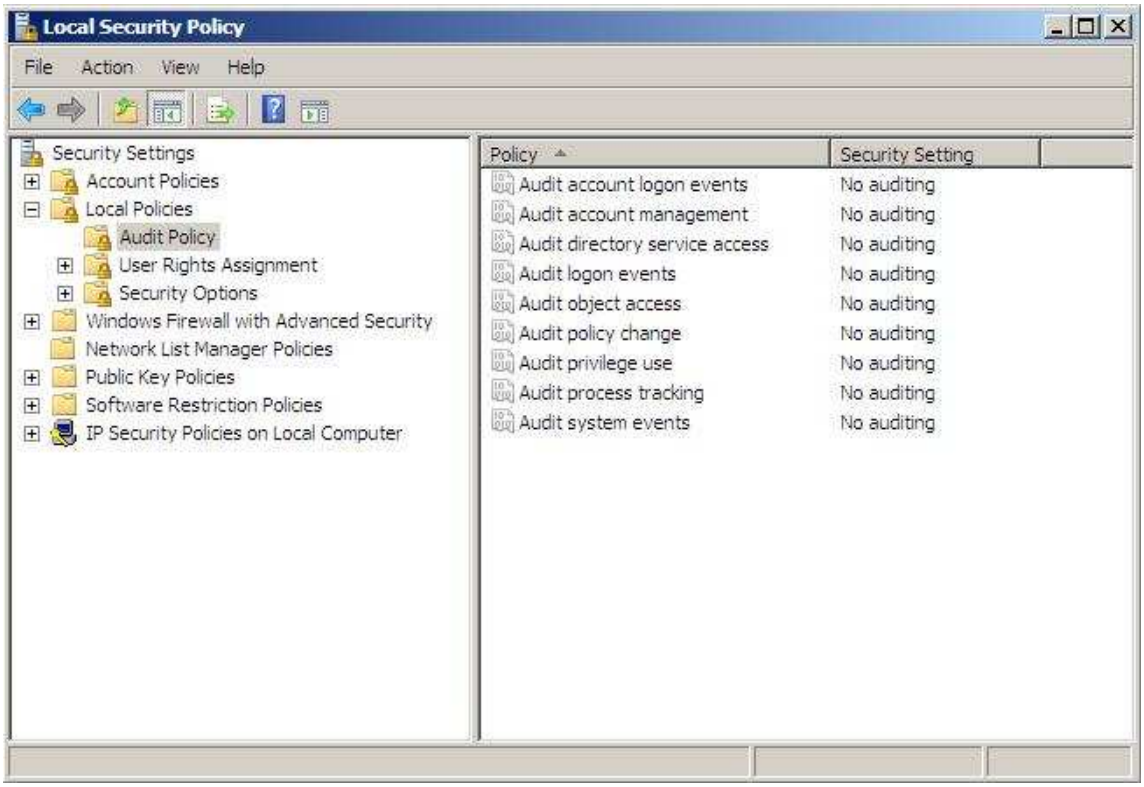

Figure 7.26 « *Audit Policy* »

3. Allez dans les préférences de la police intitulée « ***Audit directory service access*** » et cochez les cases « ***Success*** » et « ***Failure*** ».

Figure 7.27 Propriétés de la police d'audit

Après avoir validé les modifications, on constate que l'audit est maintenant activé. Si une modification sur l'annuaire est effectuée avec succès ou non, une trace sera inscrite dans les logs.

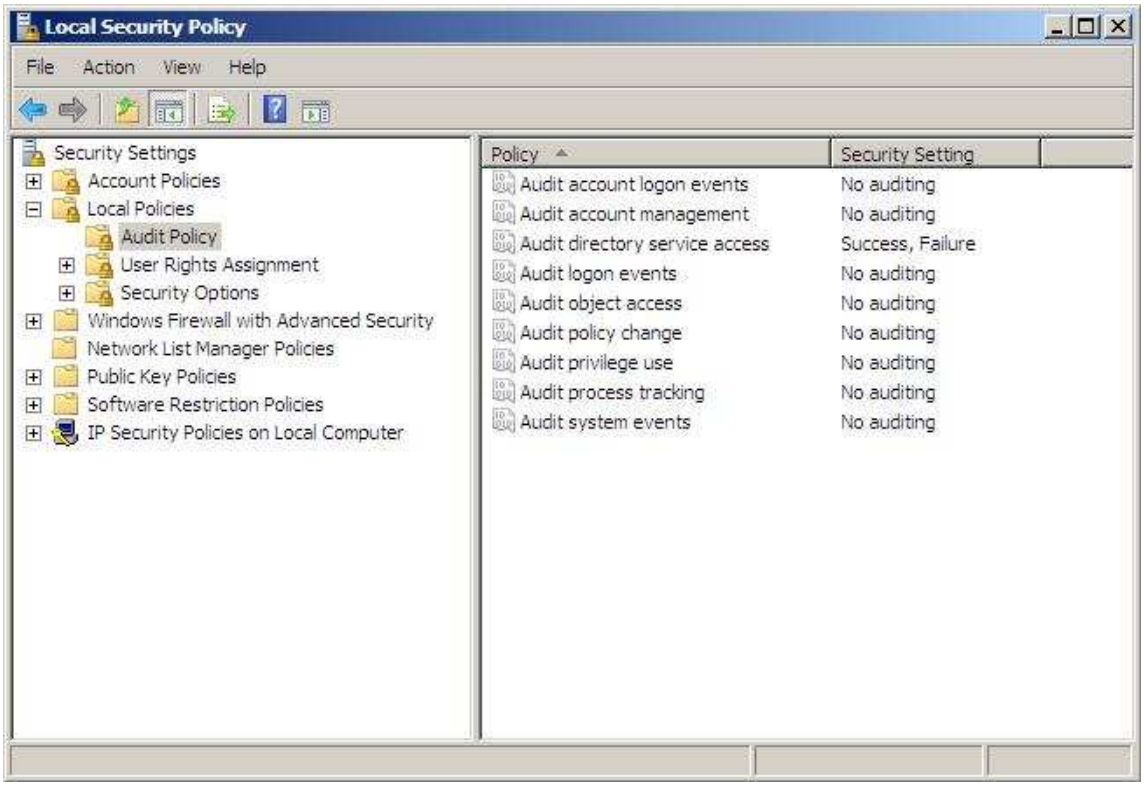

Figure 7.28 Audit activé

Maintenant que l'on a activé l'audit, il faut encore dire quels sont les objets que l'on veut auditer. Dans les propriétés de l'objet que l'on veut auditer, on va rajouter une règle disant quels sont les actions que l'on veut contrôler.

Pour activer l'audit sur une OU :

1. Faites un clic droit sur l'OU que vous voulez auditer et allez dans les propriétés de celle-ci. Rendez vous dans l'onglet « ***Security*** » et appuyer sur le bouton « ***Advanced*** ».

2. Allez dans l'onglet « ***Auditing*** ». Vous pouvez ici mettre les règles sur les actions que vous voulez auditer.

   Par exemple pour auditer la création d'un utilisateur dans l'OU, appuyez sur le bouton « ***Add…*** », choisissez quels sont les utilisateurs dont l'action doit être auditée, choisissez par exemple « ***Everyone*** » pour auditer toute création d'utilisateur.

Figure 7.29 Utilisateurs à auditer

3. Ensuite vous devez sélectionnez les actions à auditer. Pour notre exemple, on va auditer la création d'un utilisateur dans l'OU. Dans « ***Apply onto*** », sélectionnez « ***This object and all descendant objects*** » si vous voulez auditer aussi toutes les sous-OU. Cochez alors la case « ***Create User objects*** ».

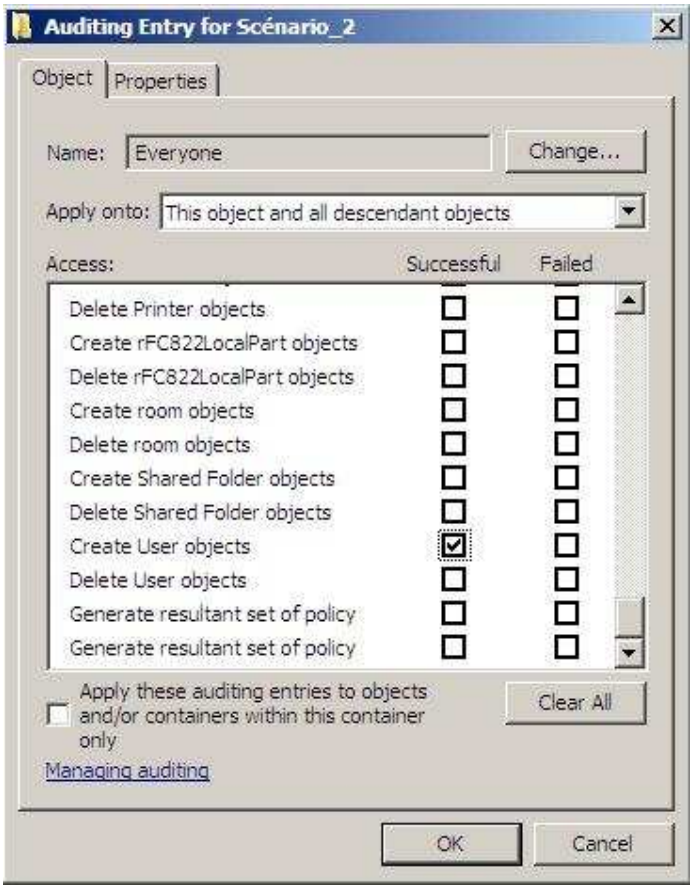

Figure 7.30 Actions à auditer

Maintenant, chaque fois qu'un utilisateur sera crée dans l'OU où l'on a crée la règle une trace de cet ajout sera inscrit dans les logs du serveur.

Voici un exemple d'un log crée après la création d'un utilisateur :

Figure 7.31 Log crée après la création d'un utilisateur

Cette fenêtre renseigne sur :

- L'utilisateur et l'ordinateur qui généré l'événement
- L'actions qui à généré l'événement
- La catégorie du log
- l'ID de l'événement
- Divers informations complémentaires sur l'action réalisée

Voila les informations générées dans le log suite à l'ajout d'un utilisateur

---

An operation was performed on an object.

Subject :

Security ID:	APEIG\u1
Account Name:	u1
Account Domain:	APEIG
Logon ID:	0x3b174e

Object:

Object Server:	DS
Object Type:	organizationalUnit

Object Name:
OU=Users,OU=Département_1,OU=Départements,OU=Scénario_2,DC=apeig,DC=ch

Handle ID: 0x0

Operation:

Operation Type:	Object Access
Accesses:	Create Child
Access Mask:	0x1
Properties:	Create Child

Additional Information:

Parameter 1:
cn=Jean,OU=Users,OU=Département_1,OU=Départements,OU=Scénario_2,DC=apeig,DC=ch

---

8. Gestion d'AD par ligne de commandes

Dans ce travail, la gestion de l'annuaire à été effectuée grâce à l'interface graphique de *Windows*. Mais toutes les tâches réalisées comme par exemple l'ajout d'un utilisateur ou encore la réinitialisation d'un mot de passe peuvent aussi être effectuées en utilisant des commandes en lignes de textes.

Cette solution permet d'automatiser un grand nombre de tâche d'administrations grâce à des scripts.

Pour administrer l'AD sans interface GUI, il existe 2 solutions :

- **L'invite de commande de *Windows***
- **PowerShell**

8.1 Invite de commandes

L'invite de commande est présente par défaut dans Windows. Elle est accessible en exécutant le programme « CMD.EXE ». Elle permet par exemple d'interroger le système, de lancer des programmes en ayant la possibilité de passer des paramètres, ou encore dans notre cas d'administrer l'annuaire AD.

Figure 8.1 Invite de commandes

Il existe donc plusieurs commandes nous permettant d'effectuer les différentes tâches d'administration dans l'annuaire AD.

- **Csvde**

  Importer et exporter des données AD

- **Dsadd**

  Ajouter des utilisateurs, des groupes, des ordinateurs, des contacts et des OU

- **Dsmod**

  Modifier un objet de l'annuaire

- **Dsrm**

  Supprimer des objets de l'annuaire

- **Dsmove**

  Renommer un objet ou modifier l'emplacement d'un objet au sein d'un seul contrôleur de domaine

- **Dsquery**

  Rechercher un objet dans l'annuaire

- **Dsget**

  Afficher les attributs d'un objet

- **Ldifde**

  Créer, modifier et supprimez des objets d'annuaire

- **Ntdsutil**

  Outil de gestion généraliste d'AD. Peut être utilisée pour par exemple exécuter la maintenance de la base de données d'AD

- **Dsacls**

  Permet de gérer les ACL de l'annuaire AD

Exemple de création d'un utilisateur « *Jean* » dans l'OU « *Users* » :

```
---------------------------------------------------------------------------------------------------------

Dsadd user "cn=Jean,cn=Users,dc=apeig,dc=ch" –samID Jean –pwd
p@assword1 –disable no
---------------------------------------------------------------------------------------------------------
```

Exemple de l'ajout de la permissions à "Jean" de créer un utilisateur dans l'OU "Exemples"

```
---------------------------------------------------------------------------------------------------------

Dsacls "OU=Exemples,DC=apeig,DC=ch" /G apeig.ch\Jean:CC;user;
---------------------------------------------------------------------------------------------------------
```

/G : signifie que l'on veut ajouter une permission

CC;user : représente la permission "Create User objects"

Il y'a encore beaucoup de paramètres que l'on peut ajouter pour configurer tous les champs de l'utilisateur. [9]

[9] Pour avoir des informations détaillées sur les commandes pour l'administration d'AD et les paramètres possibles : http://www.microsoft.com/technet/prodtechnol/windowsserver2003/fr/library/ServerHelp/59bec076-01fe-4d09-8b4b-296e7fa9c557.mspx?mfr=true

8.2 PowerShell

PowerShell est une interface en ligne de commande comme « l'invité de commande » de *Windows.* La différence entre les deux est que PowerShell offre beaucoup plus de fonctionnalités en matière d'administration.

On peut enregistrer les commandes à exécuter dans des fichiers de scripts pour automatiser l'administration. Les scripts sont des fichiers textes standards que l'on peut lire avec n'importe quel éditeur de texte. Ces fichiers textes ont l'extension « .ps1 ».

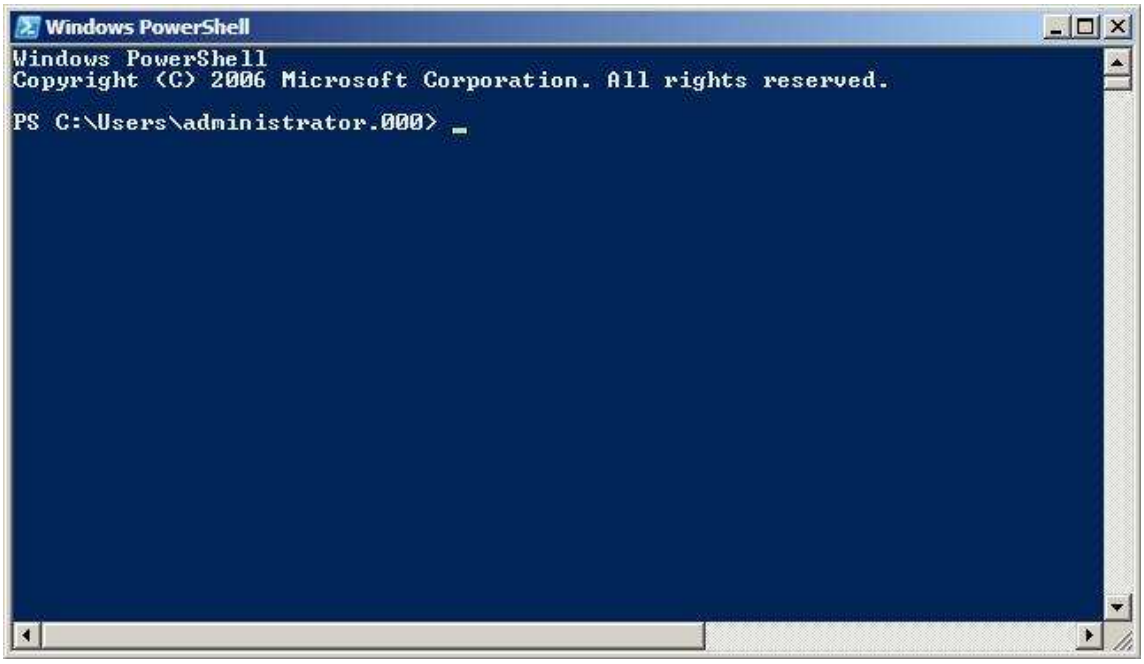

Figure 8.2 Interface de PowerShell

Toutes les tâches d'administration effectuées dans l'annuaire AD en utilisant l'interface graphique comme la création de groupes, d'utilisateurs par exemple, peuvent être effectuées par des commandes dans PowerShell.

Dans Windows Server 2008, PowerShell est directement intégré au système d'exploitation.

Pour utiliser PowerShell :

1. Sur l'interface « ***Server Manager*** », dans « ***Features Summary*** » cliquez sur « ***Add Features*** ».

Figure 8.3 Cliquez sur « *Add Features* »

2. Dans la fenêtre qui s'ouvre, cochez « ***Windows PowerShell*** », cliquez sur « Next » et ensuite « *Install* ».

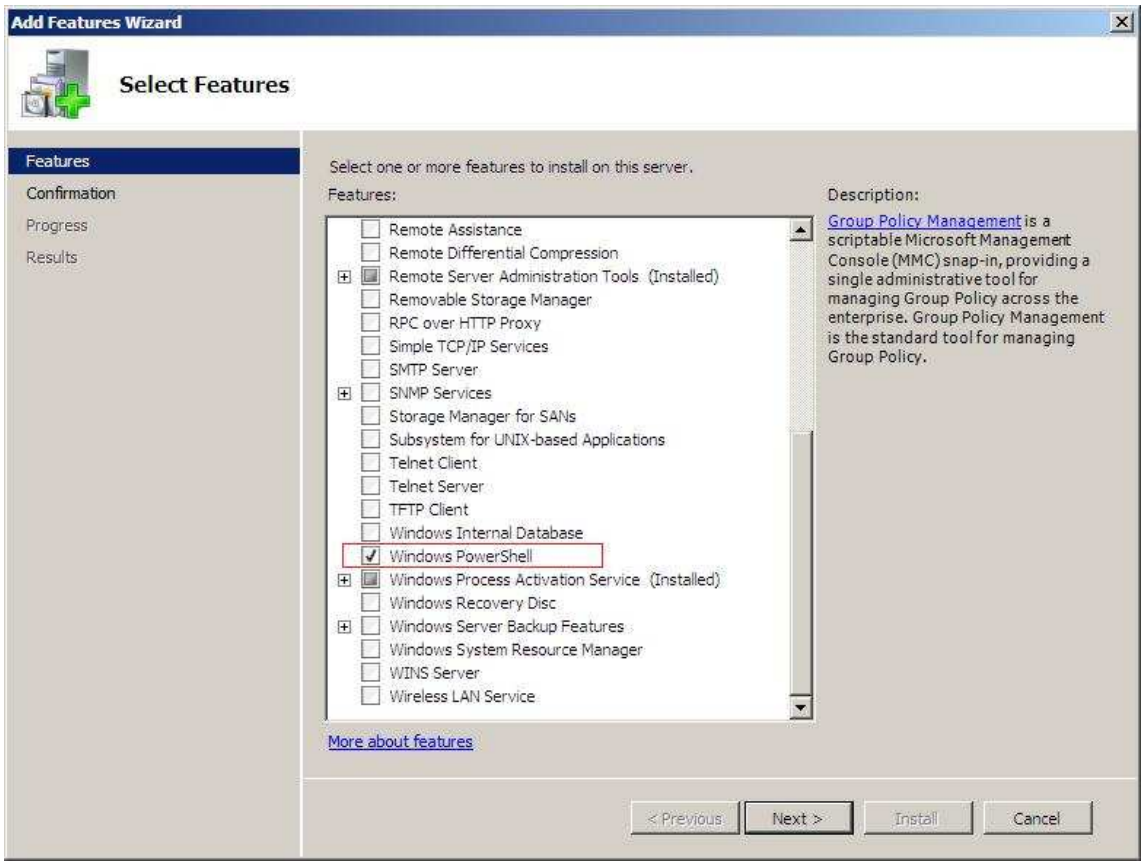

Figure 8.4 Assistant d'ajout de composant

Exemple de création d'un utilisateur dans une OU « Exemples » :

```
$objContainer = [ADSI]"LDAP://ou=Exemples,dc=apeig,dc=ch"
$objUser = $objContainer.Create("user","cn=Jean")

$objUser.Put("sAMAccountName", "Jean")
$objUser.Put("description", "Utilisateur Jean")


$objUser.SetInfo()

$objUser.psbase.InvokeSet('Accountdisabled',$false)

$objUser.psbase.CommitChanges()
```

- **$objContainer** est l'emplacement de l'OU où l'on veut créer l'utilisateur

- **$objUser** est l'objet représentant l'utilisateur

    - Le premiere parametre "`user`" signifie que l'on veut créer un utilisateur
    - Le second "`cn=Jean`" represente le nom que l'on veut donner à l'utilisateur

- **$objUser.Put** va nous permettre de configurer les champs de l'utilisateur

    - Nom
    - Adresse
    - Description

- **$objUser.psbase.InvokeSet('Accountdisabled',$false)** sert à activer le compte

9. Problème rencontrés

Problème 1 : L'utilisateur délégué ne pouvait pas créer de comptes utilisateurs, ses privilèges étaient insuffisants.

Solution 1 : Pour essayer de simplifier l'architecture, les autorisations des conteneurs par défaut (Builtin, Users,…) avait étés modifiés. Pour que les administrateurs délégués puissent créer des utilisateurs ou réinitialiser des mots de passe, il faut laisser les autorisations par défaut pour les conteneurs pré installés.

Problème 2 : Lorsqu'un utilisateur délégué essaie de se loguer sur le serveur, il reçoit un message d'erreur lui indiquant que la méthode d'authentification utilisée n'est pas autorisée.

Solution 2 : Si on décide de ne pas utiliser les comptes par défaut, il ne faut pas oublier d'autoriser les groupe que l'on a crée dans lequel on a mis les utilisateurs de pouvoir se loguer localement sur la machine en modifiant les polices de sécurité du serveur.

10. Conclusion

La délégation d'administration est donc une fonctionnalité très utile dans Active Directory. Elle permet aux entreprises de concevoir une architecture dont l'administration peut être répartie entre plusieurs utilisateurs. Chaque département peut avoir ses propres administrateurs pour ses différents objets.

On constate que l'on peut déléguer l'administration de pratiquement n'importe quelle tâche et de n'importe quel objet :

- Tous les attributs d'un utilisateur peuvent être modifiés indépendamment par plusieurs administrateurs délégués
    - Name
    - Adresse
    - Account Logon

- Chaque OU peut être administrée par un utilisateur différent
    - Création/Modification/Suppression d'utilisateurs
    - Modification des permissions de l'OU

- On peut attribuer des niveaux de privilège différent aux utilisateurs
    - Read/Write
    - Read

- Les rôles du serveur peuvent chacun être délégués à un utilisateur différents
    - DNS
    - DC

Mais, on constate que des risques au niveau de la sécurité apparaissent lorsque l'on délègue le contrôle à des utilisateurs. Ceux-ci vont donc intervenir sur l'annuaire AD, de ce fait si la configuration de la délégation n'est pas correctement effectuée, des trous au niveau de la sécurité apparaissent en offrant par exemple la possibilité à un utilisateur malveillant d'altérer les informations présentes dans l'annuaire AD.

Le principe du moindre privilèges doit donc pouvoir être respecté en s'assurant qu'un utilisateur chargé d'une tâche précise comme par exemple la gestion des comptes utilisateurs ne puisse pas effectuer d'autre modifications dans l'annuaire ou le serveur comme par exemple modifier les polices de sécurité.

On a la possibilité d'utiliser les groupes par défaut crées lors de l'installation avec des autorisations préconfigurées ou utiliser ses propres groupes pour avoir une configuration plus personnalisée de l'annuaire AD et pouvoir gérer les droits accordés aux groupe de manière plus précise.

Toute la délégation de contrôle est donc basée sur les autorisations NTFS. Que l'on utilise l'assistant de délégation qui va simplifier la mise en place des tâches que l'utilisateur va pouvoir exécuter ou que l'on modifie les autorisations manuellement, au final, le résultat est le même.

Toutes les opérations ont étés réalisée sur « *Windows Server 2008* », mais toute la procédure réalisée peut être fait de manière identique sur « *Windows Server 2003* ». La délégation de contrôle n'a donc subi aucune modification dans la nouvelle version de Windows Server.

Avec plus de temps à disposition, le scénario aurait pu être complété avec plus de tâches déléguées par exemple, inclure d'avantages d'organismes pour répartir de manière encore plus détaillées les différentes tâches.

Finalement, cette technique doit donc être mise en place correctement pour ne pas mettre en péril la sécurité de l'annuaire mais si cette opération est bien réalisée, la délégation de contrôle peut devenir une fonctionnalité clé d'Active Directory.