

# Administration des systèmes (INFO-F-309)

## Résumé (?) Windows

Markus Lindström

16 juin 2007

# Table des matières

<b>1</b>	<b>Concepts de Windows NT 4</b>	<b>3</b>
1.1	Introduction	3
1.2	Le noyau NT	3
1.3	Windows NT 4	4
1.3.1	Windows NT 4 Server	4
1.3.2	Windows NT 4 Workstation	4
1.4	Windows NT 4 en réseau	4
1.4.1	Workgroups	4
1.4.2	Domains	5
1.4.3	Les quatre modèles Microsoft de domaines NT	5
1.5	User accounts et groupes	6
1.5.1	Groupes globaux et locaux	6
1.5.2	Gestion des utilisateurs	6
1.5.3	Policies	7
1.6	Fichiers et partages	7
1.6.1	Permissions NTFS	7
1.6.2	Shares	8
1.7	RAID sur NT 4	8
1.8	Print service	8
1.9	Déploiement	8
1.10	Gestion des backups	9
<b>2</b>	<b>Windows 2000 et Active Directory (en construction)</b>	<b>10</b>
2.1	Introduction	10
2.2	File services	10
2.3	Architecture réseau	10
2.4	Active Directory	11
2.4.1	Organisation logique et physique	11
2.4.2	Délégation administrative	12
2.4.3	Global Catalog	12
2.4.4	Autres features intéressantes	12
2.5	Outils d'administration : la MMC	12
2.6	Gestion des utilisateurs et des groupes	13
2.6.1	Les groupes	13
2.7	Group Policies Object	14
2.7.1	Catégories de GPO	14
2.7.2	Héritage	15
2.8	Terminal Services	15
2.9	Gestion des disques	15
2.10	Windows Server 2003	16

# Disclaimer

Ce résumé ne se veut en aucun cas être un syllabus complet pour la partie Windows du cours de M. Alain Delava, mais tente d'en synthétiser l'essentiel (tout en le garnissant de potins croustillants) ; il est un complément aux notes manuscrites et aux slides. Les étudiants sont donc toujours fortement encouragés à se rendre au cours ! ;-)

Il est important de souligner que ce résumé a été créé assez rapidement, il est donc probable qu'il contienne des erreurs (et pas seulement linguistiques !), en particulier dans le chapitre consacré à Windows 2000. Le lecteur est donc invité à y jeter un œil critique.

Pour toutes remarques, suggestions d'ajouts ou corrections d'erreurs, n'hésitez pas à me contacter !

— Markus <[mlindstr@ulb](mailto:mlindstr@ulb)>

# Chapitre 1

## Concepts de Windows NT 4

### 1.1 Introduction

*Windows NT* est un système d'exploitation dont le développement a débuté chez Microsoft en 1988, et qui à la base aurait dû devenir *OS/2 3.0*. Cet OS était construit from scratch ; se débarrassant de la base 16-bits de MS-DOS, NT devint le premier OS purement 32-bits de Redmond.

Plusieurs objectifs guidaient le développement de l'OS : la portabilité du code (les développeurs ont ainsi eu recours au C et C++, avec seules quelques petites parties codées en langages d'assemblage), la modernité (une gestion de mémoire virtuelle, une certaine orientation-objet, l'emploi en réseaux divers et variés, le support des machines multiprocesseurs, etc.) et la compatibilité avec certains autres gros systèmes d'exploitation contemporains comme OS/2 et MS-DOS.

Windows NT empruntera certains concepts d'architecture à UNIX, notamment l'intégration d'une partie des normes POSIX (Portable Operating System Interface) qui se font sentir dans l'API de NT. En effet, certaines des fonctions offertes portent le même nom que certains system calls bien connus d'UNIX, ce qui facilite grandement le portage de programmes. De plus, NT souhaitera se débarrasser des problèmes innombrables qu'impliquent l'emploi des *code pages* sous MS-DOS, et adoptera la norme *Unicode* pour faciliter l'échange de données entre utilisateurs internationaux.

Niveau sécurité, Windows NT vise le niveau C2 de l'*Orange Book* – surnom donné à la norme TCSEC (Trusted Computer System Evaluation Criteria) du département de la Défense américaine – qui implique certaines fonctionnalités sécuritaires dont, notamment, la séparation des utilisateurs et des données et la capacité d'imposer des limitations d'accès aux diverses ressources disponibles. Cette certification encourage notamment l'utilisation de cet OS dans les banques et à l'Armée.

NT se veut être rapide, efficace (sans toutefois trop se préoccuper de l'espace occupé en mémoire), extensible, et favorisant le travail en réseau.

### 1.2 Le noyau NT

Le noyau de Windows NT est basé sur *Mach*, un micronoyau développé à l'Université Carnegie Mellon de 1985 à 1994. Un micronoyau est un noyau n'offrant que quelques services de base et étant donc de taille très réduite, mais dont la simplicité implique également la stabilité. Les autres services sont fournis par des *serveurs* fonctionnant en *mode utilisateur*, et non en mode kernel comme on pourrait s'y attendre. On peut ainsi avoir des serveurs gérant la mémoire, l'affichage, les processus, les fichiers, le réseau, etc.

Le kernel NT fonctionne purement en 32-bits, ce qui correspond au mode protégé des processeurs Intel 80386 et supérieurs, et offre enfin un espace mémoire distinct pour chaque processus. Contrairement aux Windows basés sur MS-DOS, il n'est donc plus possible pour un processus quelconque d'aller lire et écrire dans la mémoire d'un autre impunément.

## 1.3 Windows NT 4

Sorti en juillet 1996, Windows NT 4.0 arbore la même interface graphique que Windows 95, justement sorti en août 1995. L'OS était disponible en deux variantes : *Workstation* et *Server*. Il pouvait de plus se vanter de supporter un grand éventail d'hardware, d'être *scalable*, et de supporter OpenGL.

### 1.3.1 Windows NT 4 Server

Windows NT 4 Server permet la mise en œuvre d'applications ou services *client/serveur*, comme des bases de données, des services de messagerie, d'impression, etc.

De base, NT 4 Server fournit quelques services :

- *File and print services* : permettent de partager des fichiers et imprimantes avec divers OS, dont MS-DOS, Windows 3.1/95, Unix, OS/2 et Mac OS ;
- Support de plusieurs protocoles, dont TCP/IP, IPX, DLC, NetBIOS sur TCP/IP, etc. ;
- Un serveur DHCP (NT 4 Workstation est fourni avec un client) ;
- *Windows Internet Naming Service* (WINS) : un système ressemblant un peu à DNS, qui sert à donner des noms à des machines Windows d'un réseau local par exemple ;
- Des outils de protection de données par RAID (*Redundant Array of Independent Disks*) software : RAID-0 (*striping*), RAID-1 (*mirroring*), RAID-5 (*striping with parity*) ;
- *Remote Access Service* (RAS) : service permettant d'accéder à des services réseau offerts par le serveur via une connexion modem ;
- Des interfaces permettant de communiquer avec d'autres OS tels Novell NetWare et Mac OS.

Outre cela, NT 4 Server offre d'autres fonctionnalités sympathiques comme la possibilité de se protéger contre les attaques sur les mots de passe des utilisateurs, par exemple en bloquant un compte après trois tentatives de login échouées, et offre aussi des outils d'administrations tels les *Server Manager*, *User Manager*, et *User Manager for Domains*. Nous présenterons le concept de domaines plus loin.

Microsoft avait de plus développé une suite de divers serveurs utiles pour les entreprises, que celles-ci pouvaient acheter conjointement avec Windows NT 4 Server dans un package nommé *BackOffice Server*. Cette version « deluxe » comprenait notamment un serveur de bases de données compatible SQL, le serveur de messagerie Exchange, le serveur HTTP IIS (*Internet Information Services*), et *Systems Management Server* (SMS) qui est un outil d'administration facilitant la gestion de parcs de machines NT.

### 1.3.2 Windows NT 4 Workstation

Le pendant client de la variante Server, *NT 4 Workstation* est prévu pour les stations de travail, et peut fonctionner en *standalone* (sur une machine isolée), mais également dans un réseau. Pour ce dernier cas de figure, deux façons de procéder sont possibles : soit l'emploi de *workgroups* qui engendrent une forme de réseau peer-to-peer, soit l'emploi de *domaines*.

Le kernel Workstation est exactement le même que celui de Server, mais l'OS est optimisé pour le client. Ainsi, on a des outils d'administration de la machine locale permettant de gérer utilisateurs, permissions, etc. La ressemblance flagrante entre les variantes Workstation et Server porte à croire qu'une seule clef de registre modifiée pourrait changer l'un en l'autre...

## 1.4 Windows NT 4 en réseau

### 1.4.1 Workgroups

Introduit en 1992 avec *Windows 3.1 for Workgroups*, le modèle des *workgroups* (groupes de travail) est peer-to-peer. L'idée générale est que chaque machine du réseau peut partager des ressources et préciser qui peut y accéder. Le système des workgroups a le grand désavantage de ne fonctionner que dans de très petits réseaux ; en effet, l'administration reste locale à chaque station du réseau et est donc décentralisée.

Par exemple, si Alain veut partager son imprimante avec Raymond, il faut qu'Alain crée un compte utilisateur pour Raymond sur sa machine ; à chaque fois que quelqu'un d'autre veut y accéder, il devra faire de même. Il est toutefois possible de donner accès à une ressource partagée à tout le monde, mais il est dès lors impossible d'interdire l'accès à quelqu'un.

## 1.4.2 Domains

Pour pallier aux inconvénients des workgroups, le concept de *domaines* a vu le jour avec *Windows NT 3.1* en 1993. Sa plus grande différence vis-à-vis des workgroups est sa faculté de *centraliser l'administration* des ressources (y compris des utilisateurs !). Une seule base de données plate nommée SAM (*Security Accounts Manager*) comprend les informations concernant les utilisateurs, les groupes, les machines du réseau, etc.

Les informations concernant le domaine sont distribuées sur des machines particulières auxquelles on donne les noms de *Domain Controllers*. En particulier, sur NT 4, un domaine comprend un et un seul *Primary Domain Controller* (PDC) et un nombre quelconque de *Backup Domain Controllers* (BDC).

Dans le modèle du domaine, un utilisateur ne se logue plus sur sa machine locale ou sur un serveur particulier, mais bien *dans le domaine*, et l'authentification se passe sur un des DC.

Le PDC contient la copie « autoritative » de la SAM pour tout le domaine, qui est répliquée sur les BDC. Il est donc évident que les BDC servent à créer de la redondance, comme leur nom l'indique ; mais ils présentent un autre avantage : puisque les BDC ont une copie en lecture seule de la SAM, ils peuvent remplir certaines fonctions comme permettre les *logons*, et de ce fait décharger le PDC d'une charge certaine. De plus, si des sites physiques sont géographiquement éloignés, il y a intérêt à mettre un BDC par site afin d'accélérer les opérations d'authentification notamment.

En cas de panne du PDC, un des BDC peut être « promu » et effectivement devenir PDC.

Noter qu'il peut exister d'autres serveurs dans un domaine, par exemple un serveur de messagerie, qui n'est pas un DC. Un tel serveur est appelé « member server ».

Bien que la SAM soit read-only sur les BDC, il n'empêche qu'il est possible d'employer les outils d'administration sur ceux-ci, et d'ailleurs sur n'importe quelle station du domaine ; ils communiqueront alors avec le PDC qui répercutera les changements éventuels sur la SAM.

Le PDC doit bien sûr être le premier serveur à être installé pour créer un domaine, puisqu'il contient toutes les informations à son sujet. Tous les DC partagent le même *domain SID* (*Security Identifier*), tandis que les member servers ont un *machine SID*. Ces derniers peuvent aussi changer de domaine, contrairement aux DC.

La SAM est *pushée* depuis la PDC vers les BDC toutes les cinq minutes par défaut.

### Les trusts

Il est possible de faire interagir plusieurs domaines en jouant sur des *trusts*, ou bails de confiance. Typiquement, au sein d'une même entreprise, on crée un domaine gérant utilisateurs et groupes, et un autre domaine contenant des ressources telles des imprimantes, des file servers, etc. Les accounts du domaine « trusté » sont utilisables pour l'accès aux ressources du domaine « trustant ». Les trusts sont *unidirectionnels* et *non transitifs*, mais il est possible d'en faire dans les deux sens entre deux domaines donnés. Dans les diagrammes, un trust est représenté par une flèche partant d'un domaine *trustant* vers un domaine *trusté*.

## 1.4.3 Les quatre modèles Microsoft de domaines NT

Quel intérêt y a-t-il à recourir à des domaines multiples ? Tout d'abord, la SAM n'est pas extensible à l'infini. En effet, sa taille maximale permise est de 40 Mo, ce qui correspond à environ 40 000 accounts ou objets.

Il est possible de construire plusieurs topologies avec un nombre donné de domaines, et Microsoft a défini quatre canevas permettant aux administrateurs de s'en inspirer pour construire la configuration étant la mieux adaptée à leurs besoins.

### Single domain model

Utile pour les petites réseaux, ce modèle, comme son nom l'indique, ne comprend qu'un seul domaine. Il n'y a donc pas de trusts à gérer, et l'administration est la plus centralisée possible. Malheureusement, ce modèle n'est pas échellonnable puisque la taille de la SAM est limitée.

## Master domain model

Dans ce modèle, un domaine appelé *master domain* gère seul les user accounts, et toutes les autres ressources auxquelles les utilisateurs ont accès sont gérées par des *resource domains*. Il y aura donc des trusts depuis les resource domains vers le master domain.

## Multiple master domain model

Ce modèle permet de surmonter la limite des 40 000 comptes utilisateurs que peut contenir la SAM. Les comptes sont répartis sur une multitude de DC, avec des trusts bidirectionnels entre ceux-ci ce qui permet notamment de grouper des utilisateurs dispersés sur ceux-ci. Ce modèle est également utile pour les environnements dispersés géographiquement.

## Complete trust domain model

Dans ce modèle, il y aura, comme son nom l'indique, des trusts bidirectionnels entre tous les domaines. C'est un modèle décentralisé, typique des entreprises où les départements informatique sont éclatés. C'est un modèle qui n'est absolument pas propre, et il n'apparaît typiquement que lors de transitions entre autres modèles.

## 1.5 User accounts et groupes

Le domaine définit users et groupes globaux, mais rien n'empêche la création d'entités locales sur une machine donnée du réseau. Il faut ainsi distinguer *administrateur local* (qui n'est propre qu'à une machine donnée) et *administrateur du domaine* (qui est propre au domaine entier).

### 1.5.1 Groupes globaux et locaux

Un *groupe global* est une liste de user accounts du seul domaine dans lequel le groupe a été créé. Il ne peut donc contenir ni users d'un autre domaine, ni d'autres groupes. Par contre, d'autres domaines peuvent donner des droits à un groupe global que celui où il a été créé, à condition que les premiers *trustent* ce dernier. Il est évident que le domaine où est créé le groupe global peut également donner des permissions à ce dernier. L'adjectif *global* provient donc du fait qu'il est possible de lui attribuer des droits n'importe où sur le réseau, tant que les trusts nécessaires existent.

Un *groupe local*, par contre, ne peut se voir attribuer des permissions qu'au niveau du seul domaine où il est contenu ; il n'est pas exposé aux autres domaines, malgré les trusts éventuels. Toutefois, un tel groupe peut contenir des user accounts et des groupes globaux d'autres domaines, en plus de ceux définis sur le domaine-même. Il est ainsi possible de regrouper des ressources de divers domaines et de leur attribuer des droits *localement* sur son propre domaine. Noter qu'il n'est pas possible d'inclure des groupes locaux dans un groupe local.

Il semblerait<sup>1</sup> que les groupes locaux de NT 4 soient locaux à *une machine*, et non pas au domaine (comme c'est notamment le cas sur Windows 2000). Il serait donc nécessaire d'aller créer des groupes locaux à la main sur toutes les machines du domaine.

### 1.5.2 Gestion des utilisateurs

Sur NT 4, deux utilisateurs sont prédéfinis : *administrator* et *guest*. Chaque utilisateur peut se voir attribuer un *profil*, un *logon script*, et une *home directory*.

---

<sup>1</sup>Aucune information concrète n'a été trouvée dans la documentation de Microsoft à ce sujet, ces informations ont été recoltées via Google Groups... Merci, Pilou !

## Profils

Le profil d'un utilisateur contient diverses informations propres à celui-ci, comme par exemple ses préférences d'affichage, ses imprimantes, ses marque-pages Internet, sa mailbox, ses mappings réseau, etc.

Il y a trois types de profils possibles :

- *Local* : local à la machine (par défaut sur Windows NT 4 Workstation) ;
- *Roaming* : récupéré sur un serveur (pas nécessairement un DC) au logon, et resynchronisé au logoff ;
- *Mandatory* : récupéré sur un serveur (pas nécessairement un DC) au logon, mais n'est pas resynchronisé au logoff ; tous les changements éventuels sont perdus.

## Logon script

Si un *logon script* est spécifié pour l'utilisateur, il s'exécutera, comme son nom l'indique, au logon sur la machine.

## Home directory

Dans un environnement réseau, la *home directory* d'un utilisateur sera typiquement un share Windows mappé sur H : , par exemple.

### 1.5.3 Politiques

Une *policy* est une règle appliquée à des user accounts ou à des machines. Les politiques permettent notamment d'obliger l'utilisateur à utiliser un mot de passe de complexité « suffisante », de verrouiller certaines clefs du registre, des préférences utilisateur (par exemple, forcer l'utilisation du wallpaper de l'entreprise), etc.

Il existe toute une série de templates livrées avec NT 4 permettant de configurer les politiques assez facilement. Le travail le plus dur reste l'adaptation des politiques aux catégories de personnes employant le réseau.

## 1.6 Fichiers et partages

Contrairement à la famille basée sur MS-DOS qui utilise *FAT*, la lignée des Windows NT utilise un filesystem avancé : *NTFS*. Ce dernier procure divers services utiles, dont un système de permissions évolué applicable à fichiers comme directories, où chaque objet a un et un seul *owner* (propriétaire). Les permissions sont beaucoup plus évoluées que sur *FAT*, qui se limitait essentiellement à interdire ou non l'écriture sur un fichier.

### 1.6.1 Permissions NTFS

Les permissions existant sur NTFS sont les suivantes :

- *No Access* ;
- *List* : permet juste de lister le contenu d'une directory ; correspond au droit *read* sur une directory sous \*nix ;
- *Read* : permet d'ouvrir des fichiers et d'exécuter des applications ; correspond aux droits *read* et *execute* sur des fichiers sous \*nix ;
- *Add* : permet la création de fichiers et de directories sans toutefois avoir la permission *read* ;
- *Change* : équivaut à la conjugaison des droits *read* et *add*, et permet en plus la suppression de fichiers ;
- *Full Control* : équivaut à *change*, mais permet en plus de s'approprier des fichiers et de changer les permissions.

## 1.6.2 Shares

Pour donner accès une ressource sur le réseau, il faut créer un *share* (partage), qui sera référencé par un nom *UNC* (Universal Naming Convention), qui adopte la forme `\\SERVER\SHARE`. Il n'est possible de partager que des directories, et pas des fichiers isolés.

Quand on crée un share, il faut également lui fixer des permissions (No Access, Read, Change, ou Full Control). Quand un utilisateur se connecte au share, ses permissions réelles sont en fait une sorte de conjonction logique (*AND*) entre ses permissions sur le share et ses permissions sur le directory au niveau du file-system.

## 1.7 RAID sur NT 4

Windows NT 4 Server offre une solution de *RAID* (Redundant Array of Independent Disks) en software, qui permet de faire du RAID de niveaux 0, 1 et 5.

- RAID-0 (*disk striping without parity*) : permet d'utiliser plusieurs disques comme un seul disque logique. On peut donc imaginer créer une partition qui s'étend sur plusieurs disques. Ce niveau augmente la performance, puisqu'il est possible d'accéder aux disques indépendamment, mais multiplie également la probabilité qu'il y ait une panne : si un disque fait grève, c'est tout le disque logique qui s'écroule.
- RAID-1 (*disk mirroring*) : typiquement utilisé sur deux disques de tailles équivalentes, le mirroring consiste simplement à assurer que le contenu des disques est à tout moment le même. Si un des disques meurt, il reste ainsi toujours une copie (noter que la mort d'un disque n'a aucun impact visible pour l'utilisateur ; le système continue à fonctionner comme si ne rien était). Outre cet aspect, le RAID-1 procure également une amélioration considérable des performances, puisqu'il est théoriquement possible d'accéder en parallèle à des régions différentes du disque logique.
- RAID-5 (*disk striping with parity*) : dans ce modèle, une information de parité est stockée sur tous les  $n$  disques physiques. Celle-ci permet de gérer la mort d'un disque sur les  $n$ , car les informations qui y étaient stockées peuvent être reconstruites grâce aux informations contenues sur les  $n - 1$  autres disques. Toutefois, si deux disques meurent en même temps, le disque logique est perdu.

Il est important de noter que des RAID de niveaux différents peuvent être combinés. Par exemple, si le système possède quatre disques durs de tailles égales, il est possible de *stripe* (RAID-0) les deux premiers, et de faire un *mirror* (RAID-1) du disque logique précédemment formé sur un *stripe* (RAID-0) formé par les deux derniers disques durs.

Le RAID software est inhéremment moins performant que le RAID hardware, puisque dans le premier cas, c'est le processeur qui doit tout gérer, tandis que dans le second le travail est délégué à un contrôleur RAID.

## 1.8 Print service

Windows NT 4 Server peut également agir en tant que *print server* (serveur d'impressions), ce qui permet de partager des imprimantes sur le réseau (workgroup ou domaine). Le serveur se charge alors de tout l'aspect *spooling* et des files d'attente.

## 1.9 Déploiement

Il existe plusieurs méthodes pour déployer NT 4 sur un grand nombre de machines de manière automatisée :

- *NT 4 unattended installation* : installation automatisée par des scripts ;
- *sysprep + outils commerciaux* : *sysprep* est un outil de Microsoft qui permet de préparer un disque avec un Windows NT installé et configuré comme on le veut tel qu'il puisse être cloné (via Symantec Ghost par exemple) sur toutes les machines nécessaires. *sysprep* retire les informations tels le nom de l'ordinateur et son SID, qui seront alors générés au démarrage sur une machine cible.

Après déploiement de l'OS, il est aussi parfois nécessaire de pouvoir déployer des applications. Ici également, plusieurs méthodes peuvent être employées :

- *sysdiff* : utilitaire de Microsoft qui permet de prendre un *snapshot* de l'état d'une machine, puis de reprendre un snapshot après installation d'une ou plusieurs applications par exemple, et finalement de calculer une *différence* entre ces deux images, ce qui crée finalement un *paquetage*. Ce dernier peut alors être appliqué sur toutes les machines d'un réseau.
- *Outils commerciaux* : on trouve notamment parmi ceux-ci *Systems Management Server* (SMS) de Microsoft et *ZENWorks* de Novell.

## 1.10 Gestion des backups

Pour effectuer des backups, on peut employer l'utilitaire *ntbackup* fourni avec NT 4. Il permet de faire les backups de diverses manières, en consultant ou en agissant sur le bit *archive* compris dans les attributs<sup>2</sup> des fichiers.

---

<sup>2</sup>Les attributs sont distincts des *permissions* sur les fichiers ; on trouve notamment les attributs *hidden* et *archive* sous NTFS. Sur FAT, il y avait aussi l'attribut *read-only*.

## Chapitre 2

# Windows 2000 et Active Directory (en construction)

### 2.1 Introduction

Le nom initialement prévu du nouvel OS de la famille NT devait logiquement être *Windows NT 5*, mais il est devenu *Windows 2000*, probablement pour rester en vogue au niveau marketing puisqu'il est sorti en février 2000. Windows 2000 est sorti en quatre arômes différents, chacun ajoutant quelque chose au précédent : *Professional* (qui remplace *Workstation*), *Server*, *Advanced Server* et *Datacenter Server* (supporte jusqu'à 32 processeurs et 64 Go de RAM).

Le changement majeur entre NT 4 et 2000 est l'introduction d'*Active Directory*, qui est un service d'annuaire compatible LDAPv3 qui remplace la SAM de NT 4. Outre cela, Windows 2000 Server propose d'autres nouveautés, dont *Dynamic DNS* et les GPO (*Group Policy Objects*) dont il sera question plus loin.

### 2.2 File services

Windows 2000 offre toute une série de nouveaux outils pour gérer les fichiers :

- La nouvelle mouture de NTFS (3.0) fournie avec Windows 2000 offre un support limité des quotas (on peut en assigner que par utilisateur et par volume), et permet aussi des montages à la \*nix via ce qu'on appelle des *junction points* ;
- DFS (*Distributed File System*) permet de créer des arborescences virtuelles cachant la position physique des file servers éventuels ;
- EFS (*Encrypted File System*) permet d'encrypter des données ;
- DLT (*Distributed Link Tracking*) permet de retrouver la trace d'un fichier déplacé ;
- L'*indexing service* permet d'accélérer la recherche de fichiers localement ou sur le réseau ;
- Gestion de volumes logiques (voir section sur la gestion des disques).

### 2.3 Architecture réseau

Le concept de domaines de NT 4 a été repris, mais on se débarrasse de la notion de *primary/backup domain controllers* ; on n'a plus que des *domain controllers* (DC). De plus, les domaines peuvent maintenant fonctionner en deux modes différents :

- *Mode natif* : permet uniquement d'avoir des DC sous Windows 2000 et ultérieurs ;
- *Mode mixte* : permet l'utilisation de BDC fonctionnant sous NT 4 dans le domaine. En réalité, le DC Windows 2000 se fait passer pour un PDC tel que sur NT 4. Ce mode est donc plus compatible, mais empêche l'utilisation des nouvelles fonctionnalités : il n'est par exemple pas possible d'utiliser une authentification employant Kerberos, ni d'utiliser le système des GPO. De plus, pour que les BDC éventuels puissent répliquer les données, le mode mixte force la limite des 40 000 objets qui existait sur NT 4. Le mode mixte n'est typiquement utilisé que temporairement le temps de migrer tous les BDC fonctionnant encore sous NT 4 vers Windows 2000.

Il est important de noter que le mode natif n'interdit que la présence de DC fonctionnant sous NT 4 ; il est possible *a priori* d'avoir des workstations ou member servers fonctionnant en NT 4 voire Windows 9x sur le domaine même s'il fonctionne en mode natif<sup>1</sup> ; il faut alors se contenter d'installer le client Active Directory sur ces machines. Toutefois, ce client ne leur permet pas d'utiliser Kerberos pour se loguer sur le domaine ; ils sont obligés de se contenter de l'ancien protocole utilisé sur NT, NTLM (*NT LAN Manager*).

Un nouveau domaine crée sur Windows 2000 (ou Windows Server 2003 d'ailleurs) est par défaut mis en mode mixte ; l'administrateur peut facilement le faire basculer en mode natif, mais c'est une opération à sens unique.

## 2.4 Active Directory

*Active Directory* (AD) est un service d'annuaire compatible LDAPv3 qui remplace la SAM vue sur les domain controllers de NT 4. La compatibilité LDAP implique notamment une hiérarchisation des données (avec objets, attributs, conteneurs organisés en structure arborescente), un namespace bien défini, et permet aussi la *distribution* et la *réplication* des données. Nous renvoyons le lecteur au chapitre sur LDAP du cours pour des informations concernant ces possibilités.

La flexibilité introduite par l'architecture de LDAP rend Active Directory extrêmement échelonnable. Un simple serveur peut ainsi gérer quelques centaines d'objets (par exemple les données relatives à une petite entreprise), mais on peut aussi distribuer l'annuaire sur un nombre arbitraire de serveurs afin de gérer un nombre colossal d'objets (entreprise multinationale).

### 2.4.1 Organisation logique et physique

Active Directory permet à la fois de gérer la structure *physique* de son réseau (c'est-à-dire savoir où se trouvent telles machines, par exemple) et la structure *logique* ou *administrative* de son entreprise. Cette séparation procure plusieurs avantages :

- Il est possible de concevoir et de gérer les structures physiques et logiques de manière indépendante ;
- Il n'y a pas besoin de baser ses noms de domaines sur la topologie physique du réseau ;
- Il est possible de déployer des DC pour plusieurs domaines au sein d'un même site physique ; il est aussi possible de déployer plusieurs DC d'un seul domaine sur plusieurs sites physiques.

#### Organisation logique : forêts, arbres, domaines, OU

L'Active Directory est logiquement structuré en forêts, arbres, domaines et *organizational units* (OU). Tout AD contient au moins une forêt avec un arbre avec un domaine, et ce dernier peut lui-même être découpé en OU. Il est important de souligner qu'un annuaire n'est absolument pas lié à un domaine ; AD est très bien capable de gérer plusieurs domaines simultanément en les organisant en arbres et forêts.

Comme sur NT 4, un domaine contient divers objets (comptes utilisateurs, informations sur les machines du domaine, les imprimantes, etc.).

Avec Active Directory, il n'est plus question de PDC/BDC comme sous NT 4 ; il n'y a plus que des *domain controllers* (DC). Ainsi, il est possible d'aller mettre à jour l'annuaire sur n'importe quel DC du domaine, et les modifications seront répercutées sur tous les autres DC via un mécanisme de *réplication multi-master*.

- Un arbre est une topologie hiérarchique de domaines, où il y a des trusts bidirectionnels et transitifs entre domaines du même arbre ; un domaine plus bas dans l'arbre n'est pas moins important qu'un autre, c'est juste une manière d'organiser. Les domaines forment un namespace continu. (par exemple, un domaine *example.com* peut avoir deux fils dans l'arbre ; ils doivent alors avoir un nom se terminant par *.example.com*, par exemple *files1.example.com* et *files2.example.com*).
- Une forêt est un ensemble d'arbres sans namespace commun (en d'autres termes, sans racine commune). On peut ainsi avoir un domaine *example.com* et un autre *example.net* dans le même annuaire. Il y a des trusts bidirectionnels et transitifs entre tous les arbres d'une même forêt, et ces derniers partagent aussi un même schéma, partagé aussi par les domaines les composant. Ainsi, une modification du schéma d'une forêt modifie le schéma de tous les arbres et de tous les domaines y étant contenus.

---

<sup>1</sup><http://www.microsoft.com/technet/prodtechnol/windows2000serv/evaluate/w2khost/w2ktad.mspx>

En clair, il y a peu de différences entre forêt et arbre, si ce n'est le nommage discontinu dans le premier. De plus, même si des forêts sont *a priori* disjointes, il est possible d'établir des trusts transitifs uni- ou bidirectionnels entre elles.

### Organisation physique : sous-réseaux et sites

Pour la structure physique, Active Directory peut subdiviser les entités réseau en *sous-réseaux* (au sens d'IP), eux-mêmes groupés en *sites*. Ceci permet par exemple d'informer AD de la découpe géographique entre le siège d'une entreprise à Kyoto et sa représentation européenne à Arlon.

Active Directory utilise ces informations pour optimiser la *réplication* de l'annuaire, ainsi que pour permettre aux utilisateurs se connectant à un site précis de tomber sur le DC le plus proche physiquement, réduisant ainsi les temps de latence réseau.

### 2.4.2 Délégation administrative

Une des grandes forces d'Active Directory est de permettre la *délégation* de l'administration de parties de l'annuaire, faculté qui découle directement de l'organisation logique de celui-ci, et qui était impossible sur NT 4. Imaginons que l'ULB administre le domaine *ulb.ac.be*, et qu'il y a au sein de ce domaine une OU correspondant au Département d'Informatique. Il est alors possible pour les administrateurs de transmettre les pouvoirs administratifs pour cette seule OU à un utilisateur du domaine, par exemple le Président du Département, qui peut alors à sa guise créer des utilisateurs, créer des OU (correspondant par exemple aux divers services de recherche), appliquer des GPO sur ceux-ci, etc.

L'OU est la plus petite unité logique pour laquelle il est possible de déléguer les pouvoirs administratifs ; il est toutefois aussi possible de déléguer des domaines entiers.

### 2.4.3 Global Catalog

Un Global Catalog (GC) est un DC qui stocke une copie de tous les objets Active Directory au sein d'une forêt. Plus précisément, il stocke une copie complète de tous les objets du domaine dont il fait partie, ainsi qu'une copie partielle de tous les objets de tous les autres domaines de la forêt. Le sous-ensemble des attributs (*partial attribute set*) contenus dans ces copies partielles est défini par Microsoft, mais sont typiquement ceux que les utilisateurs cherchent le plus souvent (nom, adresse courriel, numéro de téléphone, etc.). Il est toutefois possible de modifier ce sous-ensemble via un snap-in approprié de la MMC qui permet de modifier le schéma de la forêt. Un GC agit donc comme une forme de cache qui permet d'effectuer des recherches rapidement dans l'annuaire, sans devoir nécessairement aller poser des questions à des DC d'autres domaines de la forêt, qui peuvent être physiquement distants.

Outre l'aspect d'accélération des recherches, un GC est également indispensable pour l'authentification des utilisateurs sur un domaine en mode natif ; il est donc bon d'en placer un sur chaque site physique d'une entreprise pour éviter de générer du trafic inutile de bout en bout du monde. Permettre à un DC d'endosser le rôle de GC se limite à cocher une case dans sa configuration.

### 2.4.4 Autres features intéressantes

- Active Directory s'intègre complètement avec DNS afin de permettre nommage et localisation des machines du domaine. Les noms de domaines correspondent simplement à des noms DNS ; et le DNS est de plus mis à jour dynamiquement lors de modifications dans l'AD (*Dynamic DNS*) ;
- AD permet l'authentification des utilisateurs via Kerberos 5 (ceci ne fonctionne toutefois qu'avec des clients Windows 2000 et ultérieurs) ;
- Comme dit précédemment, la compatibilité LDAP de Active Directory permet d'y faire des requêtes LDAP et d'employer des facultés de réplication.

## 2.5 Outils d'administration : la MMC

La *Microsoft Management Console* (MMC) est un outil qui n'offre aucune fonction d'administration en soi, mais qui permet de charger divers *snap-ins* remplissant ces fonctions. On trouve notamment des snap-ins pour gérer Active Directory, les serveurs DNS, DHCP, la configuration du hardware, etc.

Ces outils peuvent être utilisés sur un DC, mais aussi sur n'importe quelle machine du domaine à condition d'être connecté en tant qu'administrateur (du domaine!).

## 2.6 Gestion des utilisateurs et des groupes

Les OU contenus dans l'Active Directory ne sont pas des groupes; ils ne permettent pas de gérer droits (c'est-à-dire permettre d'effectuer une tâche système, comme régler l'heure ou gérer une zone DNS) et permissions (c'est-à-dire régler l'accès à une ressource, tel un fichier ou une imprimante) pour les entités s'y trouvant. Par contre, ils permettent l'application de GPO (voir plus loin) et la délégation de l'administration.

Chaque objet de l'AD a un *security identifier* (SID), qui est un nombre *unique* généré à la création de l'account, du groupe, de la machine, etc; la première partie de ce nombre identifie le domaine, tandis que la seconde identifie l'account relativement au domaine (on appelle aussi cette partie *relative SID*, ou RID).

De plus, chaque objet de l'AD ainsi que tous les objets *securables*<sup>2</sup> (fichier, directory, imprimante, etc.) possède un *security descriptor* (SD), qui définit un *owner* (propriétaire, qui peut être un utilisateur ou un groupe) ainsi que des permissions d'accès. En réalité, un SD est composé d'*access control lists* (ACL) qui sont elles-mêmes une liste d'*access control entries* (ACE). Un SD peut contenir deux types d'ACL :

- *Discretionary ACL* (DACL) : permet d'identifier utilisateurs et groupes qui ont accès ou non. Cette liste est contrôlée par le owner de la ressource ;
- *System ACL* (SACL) : permet de contrôler de quelle manière les accès sont audités, s'il y a lieu (ceci permet de remplir le critère d'auditing nécessaire pour respecter la norme *Orange Book*, cf. NT 4). Cette ACL est contrôlée par les administrateurs.

Un ACE permet de donner ou d'interdire explicitement un *droit* ou une *permission* sur un objet, mais aussi à une partie d'objet (par exemple, certains mais pas tous les administrateurs pourraient modifier les adresses e-mail d'utilisateurs); et il n'en existe que deux types : *AccessAllowed* et *AccessDenied*.

Au logon, l'utilisateur reçoit un *access token* (jeton d'accès) contenant son SID, le SID des groupes dont il est membre, ainsi que les privilèges qu'il possède. Le jeton forme en quelque sorte la carte d'identité de sa session. Dès lors, lorsque l'utilisateur veut accéder à un objet, Windows va vérifier si un des SID du token est dans l'ACL de l'objet en question. S'il est dans un ACE de type *AccessAllowed* (et dans aucun *AccessDenied*), l'utilisateur aura accès à l'objet de la manière décrite dans l'ACE.

Le système de l'access token explique pourquoi un utilisateur doit se déloguer puis se reloguer sur le domaine pour qu'il puisse obtenir les droits et permissions attachés à un groupe dont il a été fait membre pendant sa session. De même, si un utilisateur se logue alors qu'il s'est retrouvé accidentellement dans le groupe des administrateurs, il aura leurs privilèges tant qu'il ne se sera pas délogué !

### 2.6.1 Les groupes

Sur Windows 2000, les groupes sont caractérisés par un et un seul *type* ainsi qu'un et un seul *scope*.

#### Types de groupes

- *Groupe de sécurité* : peut se retrouver dans une DACL afin de régler l'accès à un objet, mais peut également servir à créer une liste de diffusion de courrier électronique (qui peut être utilisée en combinaison avec Microsoft Exchange ou une autre application de messagerie supportant Active Directory);
- *Groupe de distribution* : sert uniquement à créer une liste de diffusion de courrier électronique, et ne peut se retrouver dans des DACL; un tel groupe ne peut donc pas servir à limiter l'accès à quoi que ce soit.

Un groupe de sécurité est donc aussi un groupe de distribution, mais l'inverse n'est pas vrai.

#### Scopes de groupes

Pour rappel, sur NT 4, on distinguait groupes *globaux* et *locaux*. Sur Windows 2000, un troisième type est apparu : le groupe *universel*, une sorte d'hybride des deux autres. De plus, il est maintenant possible

<sup>2</sup>Terme employé *verbatim* par Microsoft dans sa documentation.

d'imbriquer tout groupe dans un autre, à condition que le domaine où ils sont créés fonctionne en mode natif.

- *Groupe universel* : le type de groupe le plus simple. Peut apparaître dans des ACL n'importe où dans la forêt, et peut contenir d'autres groupes universels ou globaux, ainsi que des utilisateurs de n'importe où dans la forêt. Un groupe universel ainsi que la liste de ses membres apparaissent dans le Global Catalog. Ils ne peuvent être utilisés que si le domaine fonctionne en mode natif.
- *Groupe global* : peut apparaître dans des ACL n'importe où dans la forêt. Un groupe global peut contenir des utilisateurs de toute la forêt ainsi que d'autres groupes globaux du domaine dans lequel le groupe global existe (à condition que le domaine fonctionne en mode natif). Le nom des groupes globaux apparaît dans le Global Catalog, mais pas la liste de leurs membres.
- *Groupe local au domaine* : ne peut apparaître que dans des ACL sur les serveurs de son propre domaine. Un groupe local peut contenir d'autres groupes locaux du même domaine, ainsi que des utilisateurs, groupes globaux ou groupes universels de n'importe quel domaine de la forêt. Il n'est, comme sur NT 4, défini que dans son seul domaine ; il n'apparaît donc pas dans le Global Catalog.

L'emploi de groupes universels n'est pas à recommander pour un réseau de taille un peu sérieuse ; en effet, la modification de la composition d'un groupe peut mettre très longtemps à se répliquer du fait que la liste des membres est alors contenue dans les GC, qui peuvent se trouver aux antipodes les uns des autres.

## 2.7 Group Policies Object

Les GPO sont l'autre grande amélioration de Windows 2000, mais qui n'est visible que pour l'administrateur système. De manière analogue aux *policies* de NT 4, le rôle des GPO est d'appliquer automatiquement un ensemble de règles ou propriétés à des machines ou à des utilisateurs.

La puissance des GPO provient du fait qu'ils peuvent être appliqués à différents niveaux de l'Active Directory : site physique, domaine ou OU ; ce dernier étant l'unité la plus petite à laquelle une GPO est applicable. On utilise souvent l'acronyme *SDOU* pour se rappeler des trois entités auxquelles on peut appliquer une GPO.

L'application de GPO différentes sur des sites physiques différents permet par exemple d'appliquer des polices de sécurité extrêmement strictes au QG d'une entreprise à Melbourne, mais de quand même permettre à l'employé de choisir son papier peint le jour où il transite par leur succursale à Charleroi.

Il est important de noter qu'une GPO n'est rien d'autre qu'un objet de l'Active Directory, comme son nom l'indique ; on *link* une GPO à des SDOU pour l'appliquer (ce qui, au niveau de l'implémentation, consiste simplement à rajouter un attribut à l'objet SDOU concerné). Toutefois, il n'est pas possible d'hiérarchiser les GPO, elles forment une liste plate dans l'annuaire ; d'où l'intérêt de leur donner des noms qui ont un sens<sup>3</sup>.

### 2.7.1 Catégories de GPO

Une GPO est en ensemble de polices choisies méticuleusement par l'administrateur système dans une vaste palette ; il y aura, comme sur NT 4, une multitude de *templates* prêts à l'utilisation. En voici une liste non exhaustive :

- Installation d'applications : polices permettant l'installation automatique de paquetages au format MSI (Microsoft Installer) ;
- Polices de sécurité : contraintes sur la complexité des mots de passe, blocage des comptes après *n* échecs de logon, gestion des logs, des services NT, verrouillage de clefs de registre particulières, polices de configuration Wi-Fi<sup>4</sup>, etc. ;
- Templates administratifs : polices permettant notamment de contrôler l'utilisation des applications Windows (Internet Explorer, Windows Messenger, Windows Media Player, etc.) en bloquant par exemple certaines fonctionnalités (par exemple forcer la page d'accueil d'IE), mais aussi d'autres polices telles la configuration du client DNS, ou encore la configuration du bureau (dont verrouillage du sacrosaint papier peint) ;
- *Folder redirection* : notamment employé pour le roaming des profils, cette fonction permet de rediriger des dossiers locaux (comme « Mes documents » et « Bureau ») vers un espace sur un serveur de manière transparente pour l'utilisateur ;
- Scripts de logon/logoff (de l'utilisateur) ou startup/shutdown (de la machine).

<sup>3</sup>« My GPO » est à éviter.

<sup>4</sup>N'est possible que sur Windows Server 2003.

## 2.7.2 Héritage

Les GPO appliqués sur un SDOU ont la propriété de se propager à toutes les entités contenues dans le SDOU. Ainsi, si l'ULB décide de bloquer les comptes utilisateurs après un seul échec de connexion en appliquant une GPO appropriée à leur domaine, alors toutes ses OU, dont le Département d'Informatique, seraient également impactées par cette police de sécurité.

Une question vient alors naturellement : si une autre GPO est appliquée sur l'OU du Département d'Informatique qui contrecarre la police appliquée au domaine, laquelle sera finalement d'application ? Le processus de lecture des GPO les applique dans un ordre bien précis :

1. Les GPO liées aux sites ;
2. Les GPO liées aux domaines ;
3. Les GPO liées aux OU. Dans le cas d'OU imbriquées, les GPO liées aux parents sont appliquées avant celles des enfants.

Il s'avère que les GPO lues en derniers ont priorité sur celles lues en premier, c'est un système « *last writer wins* ». Toutefois, il est possible de *forcer* l'application de GPO précédentes en les marquant de l'attribut *enforce* (alias *no override*).

Il est également possible pour un OU de complètement bloquer l'héritage d'une GPO parente, à condition qu'elle ne soit pas *enforced*.

## 2.8 Terminal Services

La motivation de base des *Terminal Services* est de permettre à l'administrateur système de ne pas devoir descendre dans la cave délabrée du bâtiment pour configurer un serveur. TS permet de se connecter à distance sur un serveur *avec sa propre session*, ce qui n'est pas du tout la même chose qu'un système de *remote display* tel VNC (Virtual Network Computing) notamment. En effet, le *remote display* se contente de recopier l'output de la carte graphique de la machine vers le client ; l'authentification se fait *a priori* de manière indépendante d'Active Directory.

Le serveur de Terminal Services est livré en standard sur Windows 2000, Windows Server 2003 ainsi que Windows XP Professionnel. Le client, rebaptisé *Remote Desktop Connection*, est livré avec les Windows récents, mais peut également être téléchargé gratuitement sur le site Web de Microsoft pour les plus vieilles versions (Windows 9x notamment).

## 2.9 Gestion des disques

Introduit avec Windows 2000, le *Logical Disk Manager* (LDM) est l'implémentation Microsoft d'un gestionnaire de volumes logiques. La gestion par volumes logiques est une approche différente de celle habituellement utilisée sur les disques durs des PC, où on procède à une découpe en partitions primaires, étendues et logiques. Sans rentrer dans les détails, disons simplement que cette approche partitionne le disque de manière beaucoup plus « fluide » en *volumes* dits logiques, qui peuvent être redimensionnés et déplacés à chaud.

Les disques, tant basiques que dynamiques, sont gérés via la console *Disk Management*, qui existe sous la forme d'un snap-in<sup>5</sup> pour la MMC.

Microsoft appelle *volume basique* une partition sur un disque partitionné de manière classique (dit un *disque basique*). Par opposition, un *disque dynamique* est un disque géré par LDM dont les volumes logiques sont appelés des *volumes dynamiques*. Microsoft déconseille fortement de placer les fichiers de boot et système sur un volume dynamique.

Les volumes dynamiques permettent notamment à Windows 2000 d'implémenter du RAID software. Attention toutefois, un disque dynamique créé avec Windows 2000 est totalement illisible sur un autre OS que Windows 2000 et ultérieur<sup>6</sup>.

<sup>5</sup>Snap-out !

<sup>6</sup>D'après les légendes de Wikipédia, Linux serait capable de manipuler de tels disques depuis sa version 2.4.8, autrement dit depuis août 2001. Prudence quand même !

## 2.10 Windows Server 2003

Sorti en avril 2003, *Windows Server 2003* est sorti en quatre déclinaisons : Standard Edition, Enterprise Edition, Datacenter Edition et Web Edition. Cette dernière mouture s'oriente principalement vers le développement d'applications Web sur base du framework ASP.NET, et ne peut pas notamment pas être utilisée comme contrôleur de domaine.

Il n'apporte aucune fonctionnalité vraiment majeure par rapport à son prédécesseur, Windows 2000 ; toutefois, de nombreuses améliorations ont été apportées par l'équipe de Redmond, dont voici une liste non exhaustive :

- Une configuration par défaut beaucoup plus sécurisée que sur Windows 2000 (qui activait essentiellement tous les services possibles) ;
- Des petites améliorations à Active Directory, dont l'ajout d'un outil de migration de domaines NT vers des domaines 2000/2003 ;
- Support de WebDAV (*Web-based Distributed Authoring and Versioning*), une extension du protocole HTTP permettant d'agir de manière plus active avec des ressources (copier, déplacer des ressources d'un URI à un autre, manipuler des verrous, etc.) ;
- *Shadow Copy* : système qui permet de créer des backups ou de prendre des snapshots d'un fichier ou d'un directory, de sorte à facilement pouvoir procéder à des *rollbacks* si un fichier est perdu par mégarde, notamment.

Une mise à jour de Server 2003, baptisée *Windows Server 2003 R2*, est sortie en décembre 2005, mais elle n'apporte rien de fondamental.