WINDOWS
2003
SERVER

TABLES DES MATIERES

I- INTRODUCTION 9
1.1- Différentes versions de Windows 2003 9
1.2- Principales fonctionnalités de Windows 2003 Server 10
1.3- Architecture de Windows 2003 Server 11
1.3.1- Le mode utilisateur 11
1.3.2- Le mode noyau 12

II- INSTALLATION 13
2.1- Présentation 13
2.1.1- Configuration des Périphériques 13
2.1.2- Préparation 14
2.2- Schéma de partitionnement du disque 14
2.3- Choix du système de fichiers 14
2.3.1- FAT (Fat16 < 2 Go) ou FAT32 14
2.3.2- NTFS 5.1 (NT File system) 15
2.4- Groupe de travail ou domaine 15
2.4.1- Présentation 15
2.4.2- Groupe de travail 16
2.4.3- Domaine 16
2.5- Phases de l'installation 16
2.5.1- Choix du système de fichiers 16
2.5.2- Différents types d'installation 16
2.6- Automatiser les installations 23
2.7- Duplication de disque 29
2.8- Service d'installation à distance RIS (Remote Installation Service) 30
2.9- Activation de W2003 Server 31
2.10- Les outils d'administration 32
2.10.1- Installer les outils par défaut 32
2.10.2- Outils d'administration courants 33
2.10.3- Console Gestion de l'ordinateur 34
2.10.4- Les services 35
2.10.5- Outils d'administration spécifiques 36
2.10.6- La console MMC (Microsoft Management Console) 37
2.10.7- Arrêt du Serveur 38

III- CONFIGURATION DE L'ENVIRONNEMENT 39
3.1- La base de registre 39
3.1.1- Définition du Registre WINDOWS 2003 39
3.1.2- Installation 40
3.1.3- Détecteur de matériel 40
3.1.4- Noyau Windows 2003 40
3.1.5- Pilotes de périphériques 40
3.2- Outils administratifs 41
3.3- Structure du registre 41
3.3.1- HKEY_LOCAL_MACHINE 41
3.3.2- HKEY_USERS 42
3.3.3- HKEY_CURRENT_USER 42
3.3.4- HKEY_CLASSES_ROOT 42
3.4- Les types de données 43
3.5- Configurer le système et gestion de l'environnement de travail 45
3.5.1- Affichage 45
3.5.2- Ajout de matériel 48

3.5.3- Ajout/suppression de programmes 49
3.5.4- Barre des tâches et menu Démarrer 49
3.5.5- Clavier 50
3.5.6- Connexions réseau 51
3.5.7- Favoris réseau 51
3.5.8- Contrôleurs de jeu 51
3.5.9- Date et heure 51
3.5.10- Imprimante et télécopieurs 52
3.5.11- Licence 52
3.5.12- Noms et mots de passe utilisateurs enregistrés 52
3.5.13- Options d'accessibilité 53
3.5.14- Options d'alimentation 55
3.5.15- Options de modems et téléphonie 56
3.5.16- Options des dossiers 57
3.5.17- Options Internet 58
3.5.18- Options régionales et linguistiques 58
3.5.19- Outils d'administration 59
3.5.20- Polices 59
3.5.21- Sons et périphériques audio 60
3.5.22- Souris 60
3.5.23- Système 61
3.6- Les consoles d'administration MMC 67
3.6.1- Types de consoles 68
3.6.2- Modes consoles 70

IV- GESTION DES RESSOURCES DISQUES 71
4.1- Configuration des disques durs 71
4.1.1- Stockage de base 71
4.1.2- Stockage dynamique 75
4.2- Systèmes de fichiers 88
4.3- Partage de dossiers 88
4.3.1- Partager un dossier 89
4.4- Système de fichiers NTFS 94
4.4.1- Structure du système de fichiers NTFS 5 94
4.5- Système de fichier CDFS 96
4.5.1- CDFS 96
4.5.2- UDF 96
4.6- Sécurité des systèmes de fichiers 96
4.6.1- Autorisations simples pour les dossiers partagés 96
4.6.2- Autorisations NTFS 98
4.6.3- Partage et publication des dossiers 104
4.6.4- Les clichés instantanés 105
4.6.5- Les fichiers hors connexion 107
4.6.6- Appropriation de fichier/dossier 109
4.6.7- Copie et déplacement de fichiers et de dossiers 110
4.7- Cryptage de documents (EFS) 110
4.7.1- Généralités sur le cryptage EFS 110
4.7.3- Supprimer un cryptage 112
4.7.4- Copie et déplacement de dossiers et fichiers cryptés 112
4.7.5- Utilitaire en ligne de mode commande CIPHER.exe 112
4.8- Compresser des fichiers et des dossiers 112
4.8.1- Compression NTFS 112
4.8.2- Compression ZIP 114
4.9- Défragmenter les disques 115

4.10- Vérification et nettoyage du disque 116
4.11- DFS 116
4.11.1- Présentation de DFS (Distributed File System) 116
4.11.2- Types de racines DFS 117
4.11.3- Exemple de configuration DFS 118
4.12- FRS (File Replication Service) 120
4.13- Quotas de disques 120
4.13.1- Présentation 120
4.13.2- Mise en œuvre 120

V- GESTION DES UTILISATEURS ET DES GROUPES 122
5.1- Comptes utilisateurs 122
5.1.1- Utilisateurs de domaines 122
5.1.2- Utilisateurs locaux 122
5.1.3- Utilisateurs prédéfinis 122
5.1.4- Création d'un compte d'utilisateur sur un ordinateur local 123
5.1.5- Modifier un compte sur un ordinateur local 124
5.1.6- Gestion et configuration des comptes utilisateurs dans un domaine 125
5.2- Profils 132
5.2.1- Profil par défaut et profil utilisateur 132
5.2.2- Profils d'utilisateurs itinérants 134
5.2.3- Dossier de base 136
5.2.4- Scripts d'ouverture de session 137
5.3- Comptes de groupe 139
5.3.1- Qu'est-ce qu'un groupe ? 139
5.3.2- Gestion des Groupes dans un Domaine 143
5.3.3- Types de groupes 143
5.3.4- Etendues de groupe 144
5.3.5- Les groupes par défaut 147

VI- ENVIRONNEMENT RESEAU ET ACTIVE DIRECTORY 154
6.1- Modèles 154
6.1.1- Modèle de Groupe de Travail Windows 2003 154
6.1.2- Modèle de Domaine Windows 2003 154
6.2- Services d'annuaire 155
6.2.1- Structure d'Active Directory 156
6.2.4- Rôle maître d'opérations 165
6.3- Espace de noms DNS 167
6.3.1- Espace de noms de domaine 167
6.3.2- Espace de noms d'objets 167
6.3.3- Règles d'attributions des noms dans Active Directory 169
6.3.4- Présentation générale du processus de résolution de noms 169
6.3.5- Zone 172
6.3.6- Serveurs de nom 172
6.3.7- Réplication et transfert de zones 172
6.3.8- DDNS 173
6.4- Compléments : présentation des zones et du transfert de zone 173
6.4.1- Présentation de la différence entre les zones et les domaines 173
6.4.2- Pourquoi la réplication de zone et les transferts de zones sont-ils nécessaires ? 174
6.4.3- Transferts de zones incrémentiels 174
6.4.4- Exemple : transfert de zone 175
6.4.5- Notification DNS 176

VII- GESTION DES IMPRESSIONS 178
7.1- Introduction 178
7.1.1- Terminologie 178
7.1.2- Configuration minimum 180
7.2- Configuration des imprimantes 180
7.2.1- Périphérique d'impression local 180
7.2.2- Périphérique d'impression en réseau, non distant 180
7.2.3- Périphérique d'impression réseau local, distant 181
7.2.4- Périphériques d'impression réseau, distants 181
7.2.5- Assistant Ajout d'imprimante 181
7.3- Configuration des imprimantes en réseau 182
7.3.1- Installation d'un périphérique d'impression local 182
7.3.2- Installation d'un périphérique d'impression en réseau 184
7.3.3- Ajout d'une imprimante 185
7.3.4- Partage d'une imprimante 185
7.4- Administration des imprimantes réseau 185
7.4.1- Accès aux imprimantes 185
7.4.2- Gestion des imprimantes 187
7.4.3- Propriétés d'une imprimante partagée 188
7.4.4- Configuration des ordinateurs clients 188
7.4.5- Menu contextuel d'une imprimante 189
7.4.6- Administration des imprimantes à partir du navigateur Web 189
7.4.7- Configuration de pool d'imprimante 190
7.4.8- Priorités des imprimantes 191
7.5- Active Directory et les services d'impression 191
7.5.1- Présentation 191
7.5.2- Publication et prise en charge des imprimantes Windows NT 191
7.6- Connexion aux imprimantes réseau Windows 2003 192
7.6.1- Connexion en utilisant l'assistant Ajout d'imprimante 192

VIII- STRATEGIES DE GROUPE 194
8.1- Définitions 194
8.1.1- Qu'est-ce qu'une stratégie de groupe 194
8.1.2- Stratégie de groupe 194
8.1.3- Objets de stratégie de groupe 195
8.2- Démarche pour la création et la gestion de stratégie de groupe 197
8.2.1- Création de Stratégies de groupes 198
8.2.2- Ajouter une stratégie de Groupe 199
8.2.3- Supprimer une stratégie de groupe 199
8.2.4- Création d'un console pour gérer des GPO 200
8.2.5- Délégation du contrôle des GPO 201
8.2.6- Définir les paramètres de chaque GPO 202
8.2.7- Les paramètres de stratégies de compte 211
8.2.8- Modèles d'administration 216
8.2.9- Désactivation des paramètres non utilisés 218
8.2.10- Désigner les exceptions 219
8.2.11- Filtrage de sécurité des stratégies de groupe 222
8.2.12- Filtrage des stratégies de groupe à l'aide de filtres WMI 223
8.2.13- Application de GPO à d'autres objets d'Active Directory 224
8.2.14- Autorisations par défaut d'accès aux GPO 225
8.3- Conseils pour implémenter une stratégie de groupe 225

8.4- Commande Gpupdate sous W2003 Server (XP aussi) 225
8.4.1- gpupdate 225
8.4.2- gpresult 226
8.5- Utilitaire de W2003 Server de diagnostic de Stratégie - Jeu de Stratégie résultant : RSOP 228
8.5.1- Mode journalisation (enregistrement) 228
8.5.2- Mode Planification 230
8.6- Group Policy Management Consol – GPMC 231
8.6.1- Group Policy Management Consol : exécution 232
8.6.2- Utilisation de GPMC : étendue 232
8.6.3- Utilisation de GPMC : détails 232
8.6.4- Utilisation de GPMC : paramètres 233
8.6.5- Utilisation de GPMC : délégation 233
8.6.6- Utilisation de GPMC : paramétrage/options 233
8.6.7- Utilisation de GPMC : propriétés d'un container 234
8.6.8- Utilisation de GPMC : propriétés d'une OU créée 234
8.6.9- Utilisation de GPMC : propriétés d'une OU sous le container à traiter 235
8.6.10- Utilisation de GPMC : sauvegarde d'une stratégie de Groupe 235
8.6.11- Utilisation de GPMC : gestion d'une Sauvegarde 236
8.6.12- Utilisation de GPMC : importer des paramètres 236
8.6.13- Utilisation de GPMC : copier/Coller une Stratégie de Groupe 237
8.6.14- Utilisation de GPMC : tables de Migration 237
8.7- Déploiement d'applications 238
8.7.1- Publication et attribution 238
8.7.2- Déploiement d'une application 238
8.7.3- Stratégie de groupe pour Windows Installer 239
8.8- Création d'une nouvelle stratégie au niveau du site, du domaine ou d'une unité organisationnelle 240
8.8.1- Création d'un nouvel utilisateur chargé du déploiement d'applications 240
8.8.2- Création d'un partage 241
8.8.3- Créer la stratégie de déploiement 242
8.8.4- Ajout d'un Service pack 245
8.8.5- Supprimer des logiciels 246

IX- SERVICES RESEAUX 247
9.1- Rappel sur les protocoles réseau 247
9.1.1- Introduction 247
9.1.2- TCP/IP 247
9.1.3- NWLink 247
9.1.4- NetBEUI 248
9.1.5- AppleTalk 248
9.1.6- DLC 248
9.2- TCP/IP 248
9.2.1- Présentation 248
9.2.2- Services TCP/IP disponibles sur Windows 2003 249
9.2.3- Configuration TCP/IP avec adresse statique 250
9.2- Adressage privé automatique 251
9.2.5- Configuration alternative 252
9.2.6- Dépannage 252
9.3- DHCP 253
9.3.1- Présentation du protocole DHCP 253
9.3.2- Installation et configuration du service DHCP 256
9.3.3- Sauvegarde et restauration des données DHCP 269
9.3.4- Agent de relais DHCP 269

9.4- WINS 270
9.4.1- Présentation 270
9.4.2- Processus de résolution de noms WINS 270
9.4.3- Implémentation du service WINS 271
9.4.4- Configuration des Clients WINS 272
9.4.5- Affichage de la base de donnés du serveur WINS 272
9.4.6- Séquences d'enregistrement NetBIOS WINS d'une station 274
Phase de réponse du serveur 274
9.4.7- Résolution de nom 275
9.4.8- Correspondance statique 276
9.4.9- Déclaration d'un serveur WINS dans la configuration DHCP 277
9.4.10- Partenaires de duplication d'un serveur WINS 277
9.4.11- Maintenance de la base WINS 278
9.5- Système DNS 278
9.5.1- Installation et configuration du service DNS 278
9.5.3- Mise en pratique du DNS - Référencer le serveur DNS 283
9.5.4- Configuration du serveur 284
9.5.5- Outils de gestion, test et dépannage 285
9.6- Sécurisation du trafic réseau : IPSEC 287

X- SUIVI ET OPTIMISATION DES PERFORMANCES 289
10.1- Outils complémentaires du CD-ROM 289
10.2- Diagnostic Réseau 291
10.3- Gestion et optimisation de W2003 294
10.3.1- Observateurs d'événements 294
10.3.2- Gestion des journaux d'événements 296
10.3.4- Ajout de compteurs 297
10.3.5- Utilisation d'alertes 297
10.3.6- Moniteur système 298
10.3.7- Gestionnaire des Tâches 298
10.4- Gérer les processus par ligne de commande 299
10.4.1- Commande START 300
10.4.2- Commande TASKLIST 300
10.4.3- Commande TSKILL 301
10.4.4- Commande TASKILL 301
10.5- Optimiser les Performances 302
10.5.1- Temps Processeur 302
10.4.2- Mémoire Virtuelle 303
10.6- Les outils disques 304
10.6.1- Défragmenteur de Disque 304
10.6.2- Vérification du Disque 305
10.6.3- Nettoyage du disque 306
10.7- Examen des Performances 306

XI- DEPANNAGE 308
11.1- Etapes de démarrage 308
11.1.1- Etape 1 308
11.1.2- Etape 2 : fichier BOOT.INI 308
11.1.3- Etape 3 : chargement et exécution de NTDETECT.com 310
11.1.4- Etape 4 310
11.1.5- Options de démarrage 310
11.1.6- Disquette d'amorçage (démarrage) 311
11.1.7- Démarrage à partir du CD-ROM Windows 2003 312
11.1.8- Console de Récupération 312

11.2- Sauvegardes et Restauration 314
11.2.1- Présentation 314
11.2.2- Planification d'une sauvegarde 315
11.2.3- Sauvegardes des données 315
11.2.4- Types de sauvegardes 315
11.2.5- Sauvegardes des données 316
11.2.6- Sauvegardes de l'état du système 319
11.2.7- Planification des travaux de sauvegarde 319
11.2.8- Restauration des fichiers et des dossiers 319
11.2.9- Restauration de l'état du système 320
11.2.10- Restauration automatique du système ASR (Automatic System Recovery) 320

I- INTRODUCTION

1.1- Différentes versions de Windows 2003

Windows 2003 Server est un système d'exploitation conçu pour tourner avec des processeurs CISC (Complex Instruction Set Computing, Pentium d'Intel) ou RISC (Reduced Instruction Set Computing, Alpha de Digital ou PowerPC de Motorola et IBM), mais seul le développement pour processeur type Intel Pentium ou compatible est disponible. Il prend en charge les réseaux de type client/serveur, mais aussi poste à poste.

➔ Windows 2003 Web Edition

Nouveau dans la famille des systèmes d'exploitation serveur Microsoft.

- Version destinée à développer et héberger des applications Web, pages Web et des services Web XML.
- Repose sur la plateforme .Net Framework.
- Ne peut être utilisée comme contrôleur de domaine.
- Conçue pour héberger essentiellement le serveur Web IIS 6.0 (Internet Information services).
- **2 Go** de RAM max 128 Mo minimum 256 recommandé.
- Processeur 133mhz mini / 550 Mhz recommandé.
- Peut s'exécuter sur une plate-forme **biprocesseurs.**
- S'appuie sur **ASP .Net** de Microsoft pour le développement des applications autour des services Web XML.
- Distribuée uniquement par des partenaires.

➔ Windows 2003 Standard Server Edition

D'après Microsoft il est :

- Plus robuste par une augmentation de la disponibilité (clusters), plus évolutif, plus sécurisé.
- Augmentation de la productivité.
- **4 Go** de RAM max.

Il convient pour des entreprises de petites et moyennes tailles :

- Amélioration des fonctionnalités de services de fichiers et d'impression.
- Amélioration des outils Active Directory.
- Amélioration des Services de Gestion grâce en particulier à la nouvelle console de gestion de la stratégie de groupe (**GPMC**, Group Policy Management Console).
- Amélioration de la Gestion du stockage.
- Système multiprocesseur symétrique à quatre voies (4 processeurs).
- IIS 6.0 (Internet Information Services) en Intranet ou Internet.
- Services d'annuaire (Active Directory).
- Mises à jour automatiques.
- Firewall Internet.
- Accès à distance sécurisé.
- Vérification du matériel du serveur et des applications.
- Services de fichiers améliorés par rapport à NT4 et W2003.
- Assistance directe en ligne avec Microsoft.
- Processeur Intel Pentium III mini 133 MHz 550 Mhz recommandé.
- Quatre processeurs au maximum.
- Mémoire RAM minimale : 128 Mo, 256 Mo recommandé.
- Mémoire RAM maximale : 4 Go.

➔ Windows 2003 Server Enterprise Edition

C'est un système d'exploitation plus puissant pour les serveurs départementaux et applicatifs. Les fonctionnalités de Windows 2003 Standard Server sont reprises et s'y ajoutent d'autres fonctionnalités comme SMP (Symetric MultiProcessing) huit voies et la possibilité de clusters

(groupement d'ordinateurs ayant accès aux mêmes systèmes de disques et répartissant les charges de traitement). Il est destiné aux moyennes et grandes entreprises. Réservé aux serveurs hébergeant des applications importantes comme la gestion des réseaux, la messagerie, les services d'annuaire, les bases de données et les sites de commerce électronique.

- Processeur Intel Pentium III mini 400 MHz 733 Mhz recommandé.
- 8 processeurs mini et 64 au maximum.
- Mémoire RAM minimale : 512 Mo, 1 Go recommandé et 64 Go max en x86.

➔ **Windows 2003 Datacenter Server**

C'est la version haut de gamme de Windows 2003 server. Elle est plus spécialement destinée aux grandes entreprises, adaptée aux grands datawarehouses (systèmes pour le stockage de bases de données très volumineuses), aux applications scientifiques nécessitant des puissances de calcul très importantes.

- Système multiprocesseur symétrique à 32 processeurs en mode SMP 32 bits et 64 processeurs dans l'édition 64 bits.
- Clusters matériels (8 nœuds).
- 64 Go de RAM pour édition 32 bits et 512 Go pour édition 64 bits.

Ce document ne concerne que les fonctionnalités de Windows 2003 Server Standard.

1.2- Principales fonctionnalités de Windows 2003 Server

➔ **Sécurité**

Comme tous les serveurs réseau, Windows 2003 assure l'authentification des utilisateurs avant l'accès aux ressources et aux données du serveur. Un système élaboré de permissions permet d'autoriser l'accès selon certaines règles (lecture, écriture, suppression, modification...) aux utilisateurs ou aux groupes désignés. Possibilité de prise en charge de Kerberos v5 pour l'authentification des utilisateurs, et de l'infrastructure de clé publique PKI (Public Key Infrastructure).

➔ **Service d'Annuaire**

L'annuaire d'Active Directory permet de structurer d'une manière hiérarchisée l'organisation des objets gérés par le système d'exploitation. Tous les objets gérés sont enregistrés dans une base de données (annuaire). Cet annuaire est répliqué sur tous les contrôleurs du même domaine. Mise en œuvre des stratégies de groupes.

➔ **Performance et évolutivité**

Il peut supporter jusqu'à 4 processeurs et 4 Go de RAM. Il est utilisé pour assurer des fonctions de serveur de fichiers, d'impression, de communication, d'applications, mais aussi de Terminal Services (licence en option).

➔ **Réseaux locaux et services de communications**

Il supporte les protocoles IP, IPX et AppleTalk. Par souci de compatibilité avec les anciennes versions de Windows, il supporte aussi NetBEUI. Pour joindre certaines imprimantes réseau (HP en particulier), il gère le protocole DLC (Data Link Control).

- Windows 2003 accepte les connexions de réseau WAN.
- 256 sessions peuvent être ouvertes sur Windows 2003 Server.
- Pour les liaisons sécurisées sur Internet, Windows 2003 intègre IPSec (IP Security).
- Réseaux privés virtuels (VPN : Virtual Private Network).
- Prise en compte d'IPv6 et cohabitation avec IPv4.

➔ **Intégration Internet**

Il intègre tous les utilisateurs du réseau à Internet. Les utilisateurs peuvent rechercher des ressources sur le réseau local (fichiers ou imprimantes) ou sur Internet grâce au navigateur Internet. Il intègre

Microsoft Internet Information Server (IIS) version 6, utilisable pour héberger des sites Internet ou Intranet. Chaque disque ou dossier peut être désigné comme faisant partie du site Web.

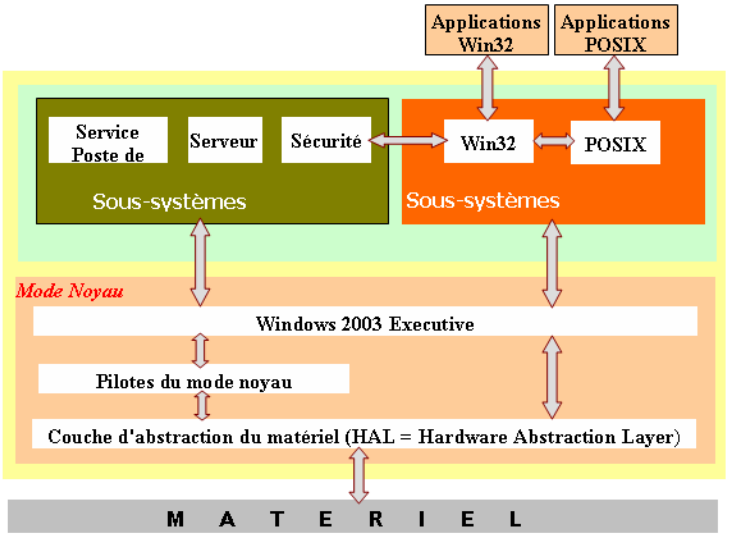
➔ **Outils d'administration intégrés :**
La gestion de l'OS se fait à travers des consoles graphiques appelées **consoles MMC** (Microsoft Management Console). Certaines de ces consoles existent par défaut, mais il est possible de créer des consoles personnalisées adaptées aux besoins spécifiques des administrateurs en ajoutant des **Composants logiciels enfichables**. Des outils de maintenance disques tels que le vérificateur des erreurs, l'outil de défragmentation et l'outil de sauvegarde sont disponibles.

➔ **Support Matériel :**
Contrairement à NT4 Server, Windows 2003 accepte les composants Plug and Play. La liste des drivers fournis est très conséquente. Il gère le bus USB (Universal Serial Bus). Support des plateformes Intel Itanium 64 bits.

➔ **Supports de plusieurs types de systèmes de fichiers et sécurité NTFS :**
Il supporte les systèmes de fichiers suivants : FAT 32 et NTFS v5. Il offre la possibilité de gestion dynamique des disques (création et extension de volumes). En NTFS, la gestion des **Quotas** de disques (limitation de la capacité disque utilisée par chaque utilisateur) peut être mise en place. Sur les partitions NTFS, la compression, l'indexation et le chiffrement des données peuvent être assurés. Cryptage des fichiers (EFS : Encrypting File System). Système de fichiers distribués (DFS : Distribute File System). Service de réplication de fichiers (FRS : File Replication Service). Clichés instantanés permettant la sauvegarde régulière de documents et facilitant leur restauration.

1.3- Architecture de Windows 2003 Server

C'est un OS prévu pour fonctionner avec un à quatre processeurs Intel de type Pentium 133 Mhz minimum. Le système d'exploitation est composé de deux couches principales le **mode utilisateur** et le **mode noyau** comportant elles-mêmes plusieurs sous-systèmes et modules. La figure suivante représente de façon simplifiée l'organisation de couches, des sous-systèmes et des modules.



1.3.1- Le mode utilisateur

Le **mode utilisateur** de Windows 2003 est divisé en deux groupes de sous-systèmes :

- Les **sous-systèmes environnementaux** permettent à Windows 2003 de travailler avec des applications écrites pour d'autres systèmes d'exploitation. Ces sous-systèmes sont composés d'interfaces qui permettent d'émuler les différents systèmes d'exploitation par rapport aux applications. Grâce à ces interfaces, les applications semblent travailler avec le système

d'exploitation pour lequel elles ont été écrites d'une part, et d'autre part Windows 2003 semble voir des applications écrites pour lui. D'origine, Windows 2003 est livré avec deux interfaces, **Win32** et **POSIX**. POSIX est une norme d'interface de système d'exploitation développée par l'lEEE, puis par l'ISO. Certaines versions d'UNIX correspondent à cette norme et les applications écrites pour ces versions d'UNIX peuvent aussi s'exécuter sur Windows 2003.

- Les **sous-systèmes intégraux** prennent en charge les fonctions essentielles du système d'exploitation. Par exemple :
  - La **sécurité** : création des jetons de sécurité, gestion des droits et autorisations. Gestion des demandes de connexion et d'authentification.
  - Le **service poste de travail** : c'est la partie du système d'exploitation qui permet à l'utilisateur d'accéder à la machine locale et au réseau par une interface graphique.
  - Le **service serveur** : c'est le sous-système qui permet le partage des ressources.

1.3.2- Le mode noyau

Le mode noyau de Windows 2003 Server permet l'accès aux données système et au matériel. Il fournit un accès direct à la mémoire et s'exécute en mode protégé dans une partie de la mémoire. C'est lui qui gère les priorités d'exécution des différentes séquences, mais aussi les priorités au niveau des interruptions matérielles ou logicielles.

➔ Windows 2003 Executive

Il comporte plusieurs modules :

- **Le gestionnaire d'entrées/sorties** gère les entrées/sorties au niveau des systèmes de fichiers, des pilotes de périphériques et du gestionnaire de cache.
- **Le moniteur de sécurité** veille aux règles de sécurité au niveau de l'ordinateur local.
- **Le gestionnaire de communications interprocessus (IPC :** InterProcess Communication manager**)** gère les communications client/serveur ainsi que les communications entre les sous-systèmes environnementaux.
- **Le gestionnaire de mémoire virtuelle (VMM :** Virtual Memory Manager**)** assigne et assure la gestion de l'espace réservé à chaque processus. Il gère la mémoire virtuelle composée de mémoire physique et d'emplacements sur le disque dur.
- **Le gestionnaire de processus** lance et met fin aux processus et aux threads. Un processus est un programme ou une partie de programme. Le thread est un jeu particulier de commandes d'un programme.
- **Le gestionnaire Plug and Play** gère la fonction Plug and Play de reconnaissance des périphériques et de leur pilote.
- **Le gestionnaire d'alimentation** gère les requêtes concernant l'alimentation de l'ordinateur.
- **Le gestionnaire d'affichage et l'interface graphique (GDI :** Graphic Device Interface**).** Le **gestionnaire d'affichage** gère les affichages et les fenêtres. Il prend en compte les informations en provenance des périphériques comme le clavier et la souris, et les transmet aux applications. **L'interface graphique** travaille les informations nécessaires aux dessins et aux graphiques.

➔ La couche d'abstraction du matériel (HAL - Hardware Abstraction Layer)

La couche HAL virtualise le détail des interfaces matérielles afin de faciliter la portabilité de 2003 sur différentes architectures matérielles. Théoriquement, cette couche permet de supporter des plateformes autres que INTEL comme Alpha de Digital. Seuls les modules concernant INTEL ont été développés, si bien que Windows 2003 ne tourne qu'avec des processeurs de types Pentium.

➔ Pilotes du mode noyau

Les pilotes du mode noyau sont des composants du système d'exploitation modulaires assurant une fonctionnalité bien précise en rapport avec l'accès aux différents périphériques.

II- INSTALLATION

2.1- Présentation

L'installation de Windows 2003 est identique à celle de NT4 ou de 2000. Elle peut se réaliser soit à partir du CD-ROM, ou à travers le réseau. En plus comme avec 2000, vous pouvez automatiser l'installation via un fichier de réponses permettant de ne pas à répondre aux questions posées.

2.1.1- Configuration des Périphériques

➔ Connaissances de base pour installer un périphérique

Type de carte	Informations nécessaires
Vidéo	référence, quantité de mémoire (pour VGA)
Réseau	IRQ, @dresse I/O, type de connecteur (BNC,TP, AUI ..), DMA !!!
Souris	type, port (COM1, COM2, bus ou PS/2)
Modem externe	port (COM1, COM2...),
Modem interne	port utilisé ou IRQ, éventuellement @dresse E/S
Son	IRQ, @adresse E/S, DMA
Contrôleur SCSI	modèle, type de Bus, IRQ

➔ Table des vecteurs d'interruptions

Numéro IRQ	Occupation
IRQ0	Horloge système
IRQ1	Clavier
IRQ2	Redirigée vers IRQ8 à IRQ15 (peu dans certains cas être utilisée)
IRQ3	Port série COM2
IRQ4	Port série COM1
IRQ5	Port Parallèle LPT2: souvent disponible
IRQ6	Contrôleur de disquette
IRQ7	Port Parallèle LPT1
IRQ8	Horloge Temps réel
IRQ9/10	Disponible
IRQ11	Disponible (sauf si SCSI)
IRQ12	Disponible
IRQ13	Coprocesseur mathématique
IRQ14	contrôleur de disque de type IDE
IRQ15	Second contrôleur de disque EIDE, parfois dispo

➔ Configuration des adresses mémoires

Adresses E/S	Périphériques (en général)
1F0-1F8	contrôleur de disque dur
278-27F	deuxième port parallèle
280-340	libre et utilisable pour tout nouveau périphérique
2F8-2FF	deuxième port série
378-37F	premier port parallèle
3B0-3DF	VGA, SVGA
3F0-3F7	contrôleur du lecteur de disquette
3F8-3FF	premier port série

2.1.2- Préparation

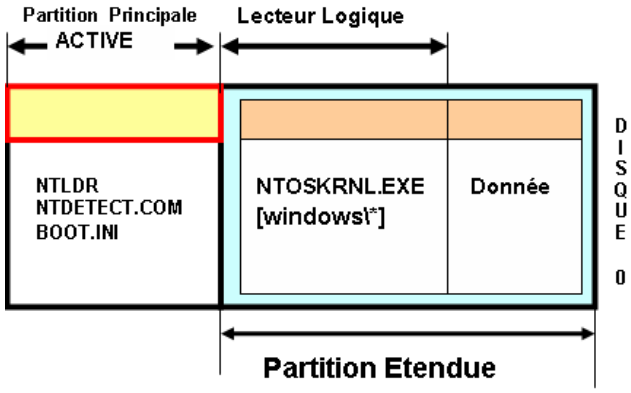
Lors de la phase d'installation, il vous est possible de modifier le schéma des partitions. Vous pouvez aussi réaliser certaines opérations sur vos disques, comme la suppression ou la création de partitions. Une fois que vous aurez installé votre OS, vous pourrez utiliser l'utilitaire **Gestion des disques** pour configurer vos autres partitions ou vos autres disques éventuels.

✋ Installez votre système sur une partition minimale d'au moins 2 Go afin de conserver l'évolutivité de votre environnement. Si vous venez à manquez d'espace sur votre partition système vous risquez malheureusement d'avoir à réinstaller le système. Même si vous avez plusieurs partitions ou disques, bien souvent certaines applications nécessitent obligatoirement de stocker des informations sur la partition système.

2.2- Schéma de partitionnement du disque

Lors de la séquence d'installation de Windows 2003 vous avez la possibilité d'installer le pré chargeur (secteur de démarrage), et le chargeur NTLDR sur une première partition, nommée partition système (ou principale ou active). La taille de la partition peut se satisfaire de 10 Mo.
Si vous souhaitez mettre en œuvre un amorçage multiple vous devez utiliser le système de fichiers FAT. Et cela peut être utile pour résoudre pour un dépannage lors du démarrage.
Vous installerez le reste sur une partition distincte appelée partition d'amorçage. Elle contient le noyau de Win 2003 nommé NTOSKRNL, ainsi que les fichiers système (4 Go min car nombreuses DLL volumineuses). La partition d'amorçage peut être un lecteur logique d'une partition étendue.
La partition système contient les fichiers vitaux pouvant être dupliqués sur une disquette de démarrage. Cela permet d'obtenir une disquette de secours en cas de problème simple d'amorçage du système, et permet aussi d'avoir une copie de ces fichiers. Par contre il est toujours possible à partir du cd-rom d'amorçage, d'accéder au système pour effectuer notamment une réparation.
Bien souvent la partition d'amorçage est convertie en NTFS pour des raisons évidentes de sécurité
✋ Bien souvent vous installez la partition système et d'amorçage sur une seule partition et sur un seul disque dur.

Exemple de Partitionnement avec un seul disque



2.3- Choix du système de fichiers

Les systèmes FAT, FAT32 et NTFS sont supportés.

2.3.1- FAT (Fat16 < 2 Go) ou FAT32

Ce type de système de fichiers permet de conserver le démarrage sous un ancien système d'exploitation DOS, W95/W98 et donc de travailler en multiboot.

- FAT16 ne supporte pas les partitions supérieures à 2 Go. Par contre FAT32 est une évolution de FAT permettant de dépasser cette limite.

- Pour mémoire FAT32 n'est pas pris en charge sous MS-DOS ou W95 OSR1.
- FAT16 utilise un adressage sous 16 bits (2^{16}), tandis que FAT32 utilise un adressage sur 32 bits.

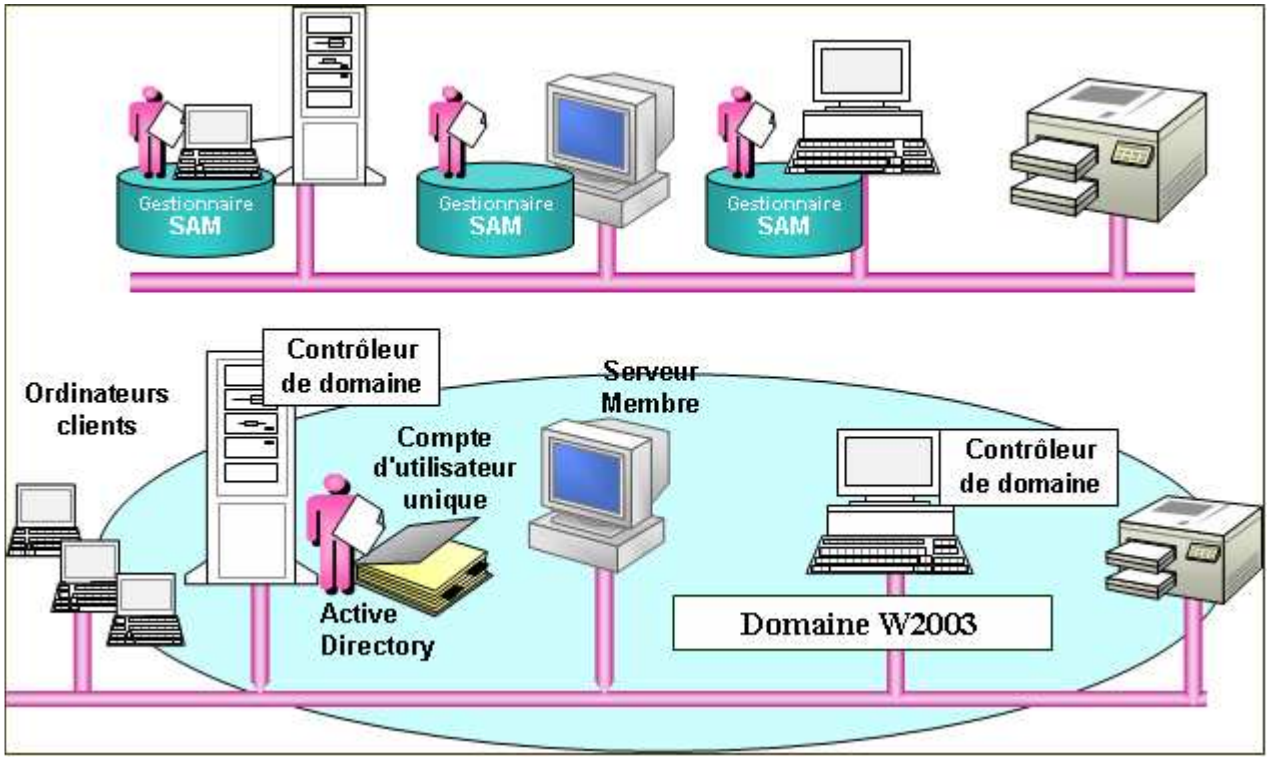
✋ Vous pouvez convertir sans pertes de données un disque du format FAT/FAT32 en NTFS, mais l'opération est unidirectionnelle et irréversible. Pour cela, tapez la commande :
CONVERT lecteur: /FS:NTFS.

2.3.2- NTFS 5.1 (NT File system)

Vous choisirez le système de fichier NTFS dans le cas où :

- La sécurité est primordiale.
- Pour gérer de manière efficace les partitions de grande capacité (> 500 Mo).
- Pour mettre en œuvre l'audit des fichiers.
- Pour gérer la compression des disques ou des fichiers.
- Pour mettre en œuvre les quotas de disques par utilisateur.
- Pour le chiffrement des données (EFS : Encrypting File System).
- Pour monter des volumes.

2.4- Groupe de travail ou domaine



2.4.1- Présentation

Un domaine permet la centralisation de la sécurité et de dédier le rôle des ordinateurs utilisés. Les serveurs ont des fonctionnalités dédiées (partages de ressources, serveurs de fichiers…) qu'ils mettent à disposition du réseau.
Les stations de travail sont clientes du serveur. Elles ont accès aux ressources du serveur par authentification de l'utilisateur (nom et mot de passe) ou de l'ordinateur.
L'accès est individualisé par l'utilisation des listes de contrôle d'accès (ACL) par des autorisations spécifiques à des utilisateurs individuels ou à des ensembles d'utilisateurs.

2.4.2- Groupe de travail

Dans un groupe de travail, chaque micro est géré individuellement. Bien souvent, c'est l'utilisateur qui est administrateur de son poste. Pour la sécurité l'administrateur que vous allez créer automatiquement lors de l'installation ne disposera pas du même mot de passe que l'administrateur général (ni du même nom, normalement). Il n'aura aucun droit sur les autres ordinateurs et aucune possibilité d'accéder aux ressources du réseau. Cela convient pour une dizaine de postes. Tous les postes peuvent être à la fois serveur et station de travail. Chaque ordinateur possède une base de comptes locale appelée SAM (Security Account Manager).

2.4.3- Domaine

Dans un domaine, la sécurité peut être centralisée (services d'annuaire Active Directory). En domaine un ordinateur peut être utilisé par plusieurs utilisateurs avec pour chacun d'eux, un environnement centralisé et des données privées sécurisées inaccessibles pour les autres utilisateurs. L'organisation en domaine nécessite une seule saisie du nom et du mot de passe pour accéder aux différentes ressources du domaine.

2.5- Phases de l'installation

- Choix de la partition et du système de fichiers.
- Options régionales.
- Nom et organisation.
- N° de série.
- Mode de licence : par serveur ou par périphérique ou par utilisateur.
- Nom de l'ordinateur et mot passe de l'administrateur.
- Date et heure.
- Paramètres réseau : par défaut seul TCP/IP est proposé.
- Groupe de travail ou domaine.
- Si l'ordinateur est dans un domaine : il faut saisir le nom et le mot passe de l'utilisateur habilité à créer le compte d'ordinateur.

2.5.1- Choix du système de fichiers

- Rappels : FAT et NTFS.
- FAT 32 pour partition > à 2 GB.
- Seule raison actuelle d'avoir une partition d'amorçage en FAT ou FAT32 est de pouvoir avoir un double amorçage de type W2003 Server et W98...

Choisir NTFS pour :

- Installer des permissions d'accès sur les documents et dossiers.
- Compresser les documents et dossiers.
- Mettre des quotas aux utilisateurs.
- Crypter les fichiers.
- Mettre en œuvre la tolérance de panne.

2.5.2- Différents types d'installation

➔ Installation sur un poste vierge en bootant à partir du CD-ROM

- Premier démarrage en mode texte.
- Premier écran bleu.
- Pilotes additionnels pré-installation (possibilité à ce stade d'installer un pilote SCSI ou Raid tierce partie par appui sur F6).
- Installation (message de bienvenue...) sous réparation du système.
- Contrat de licence W2003 (libre ou non d'accepter… appui sur F8 ou ESC).

- Choix du disque et de la partition, et du type de formatage.
- Examen des disques durs.
- Copie des fichiers.
- Dernière étape en mode texte...

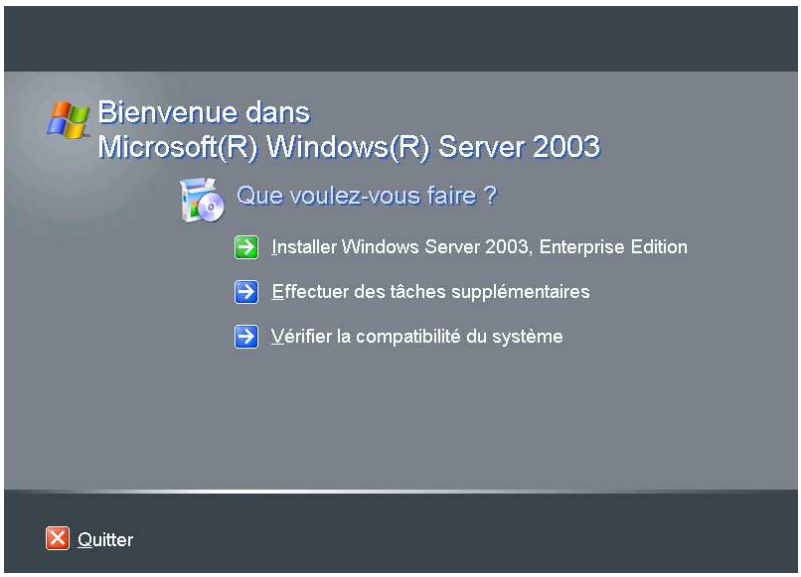
☞ 1er démarrage en mode texte :
- Premier écran → « Le programme d'installation inspecte la configuration matérielle de votre ordinateur …. »
- Pilotes additionnels pré-installation appuyez sur F6 pour installer un pilote SCSI ou RAID tierce partie.
- Installation ou réparation du système.
- Installation → Entrée.
- Réparation appui sur R.
- Annuler installation F3.

☞ Installation se poursuit par :
- Examen des disques durs.
- Copie des fichiers.
- Dernière étape en mode texte pour vous demander de retirer disquette et CD-ROM des lecteurs avant le redémarrage automatique.

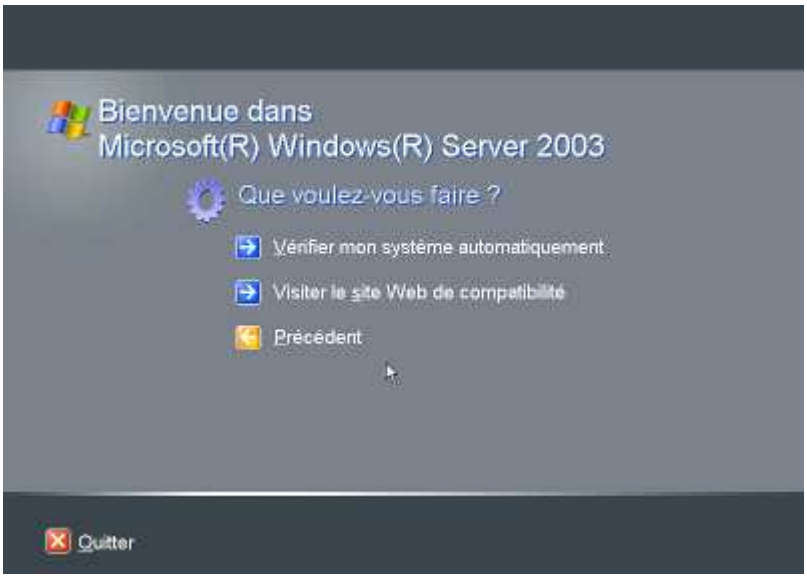
☞ Premier démarrage en mode graphique :
Le menu d'installation apparaît :
- 3 premières étapes de l'installation déjà réalisées en mode texte apparaissent en vert et l'étape en cours apparaît en rouge.
- Installation des périphériques.
- Options régionales et linguistiques.
- Personnaliser le logiciel (nom et éventuellement Société).
- Clé du produit.
- Réglage de la date et l'heure (pourront être paramétrées ultérieurement).
- Paramètres de gestion de Réseau.
- Paramètres par défaut (adresse IP de type APIPA - Automatic Private IP Allocation - dans la gamme 169.254.0.0 à 169.254.255.255).
- Paramètres personnalisés (entrée statique).
- Groupe de Travail ou Domaine.
- Installation des éléments du menu démarrer.
- Inscription des Composants.
- Redémarrage...

➔ Installation à partir d'un système d'exploitation existant en «bootant» sur le CD-ROM

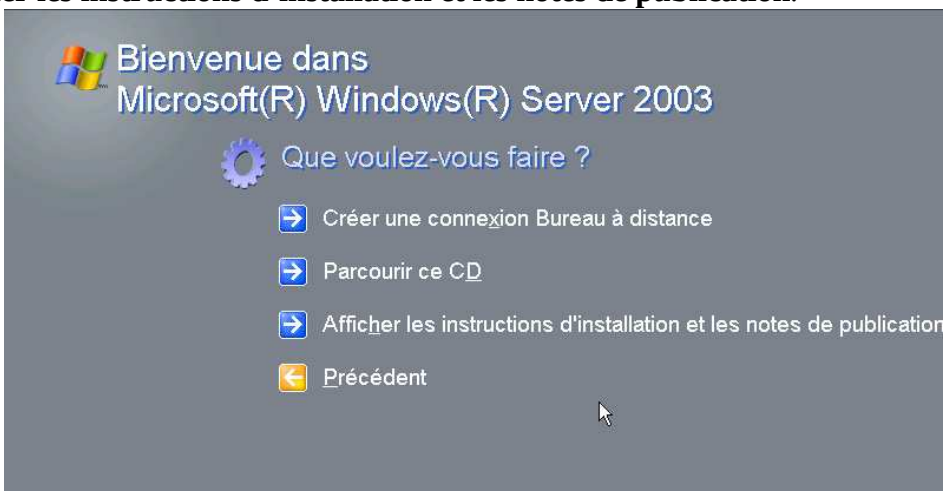
L'installation de W2003 Server à partir du CD-ROM est identique à celle utilisée pour installer Windows NT ou 2000. Si un système d'exploitation est déjà installé, il vous suffit d'introduire le CD dans le lecteur et de lancer le programme setup.exe, s'il ne démarre pas automatiquement. Tout d'abord sélectionnez **Vérifier la compatibilité du système**.



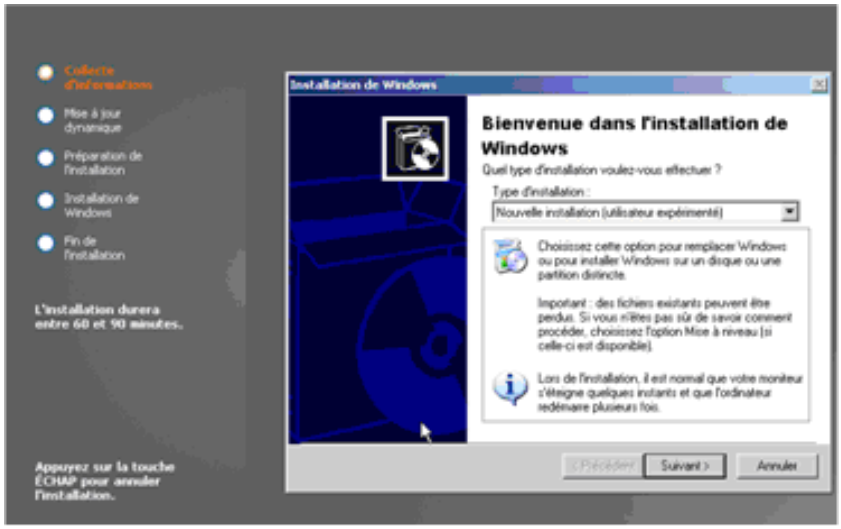
Sélectionnez **Vérifiez mon système automatiquement**.

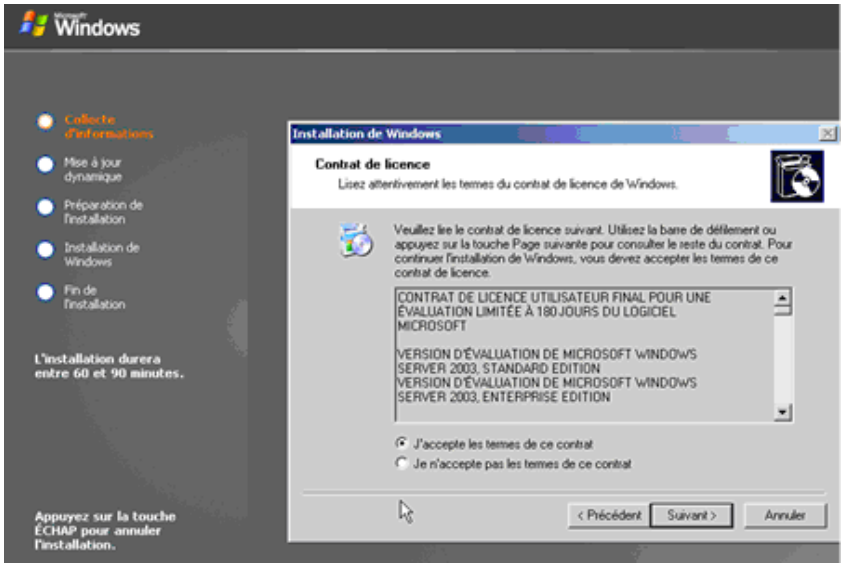


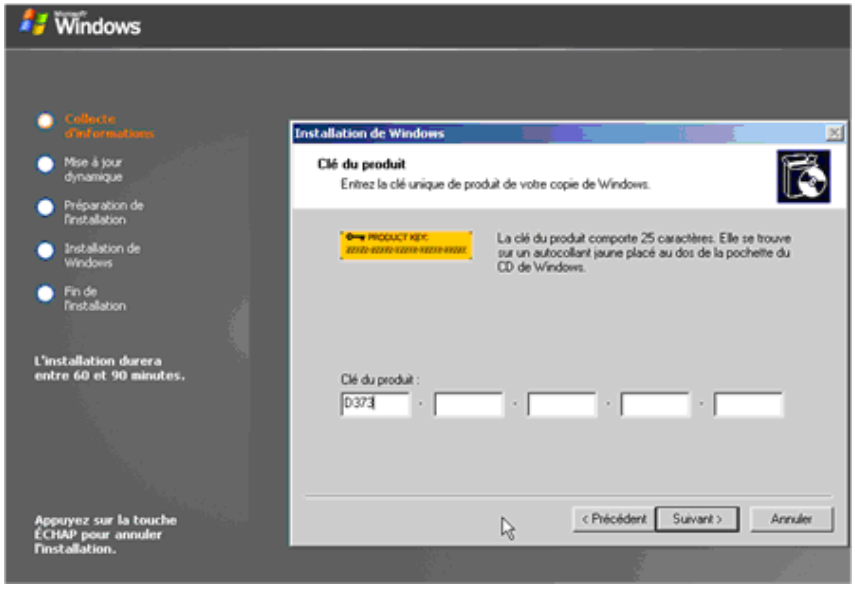
En revenant dans le menu principal vous pouvez cliquer sur **Effectuer des tâches supplémentaires** afin d'**Afficher les instructions d'installation et les notes de publication**.

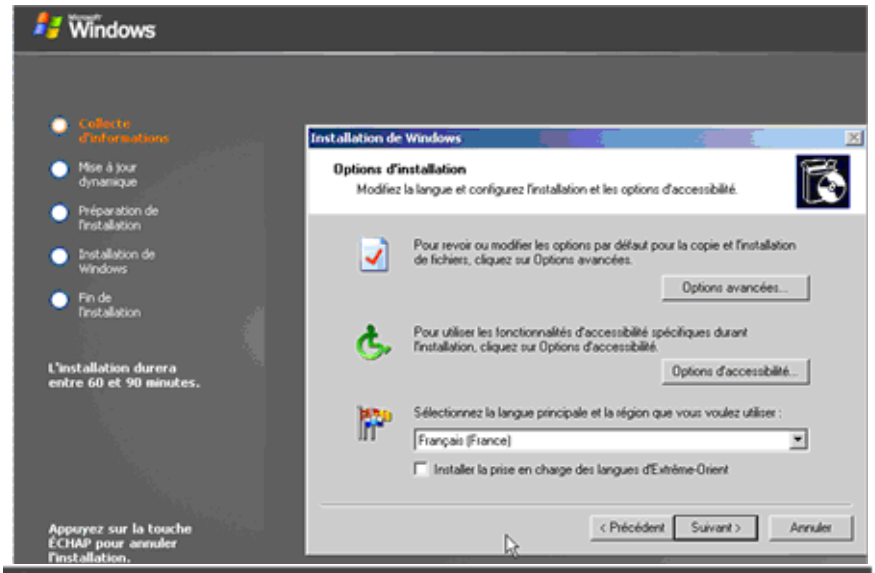


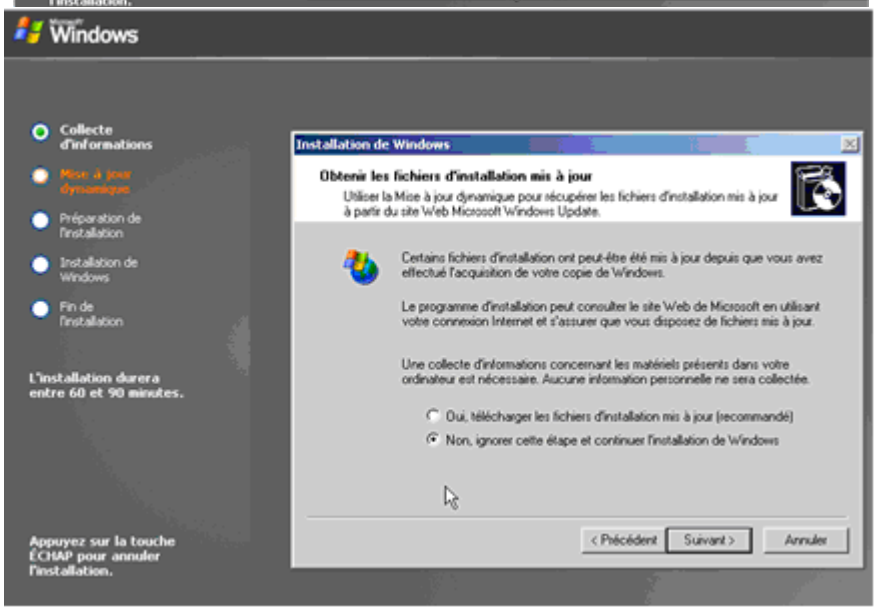
Maintenant revenez au menu principal afin de lancer l'installation.

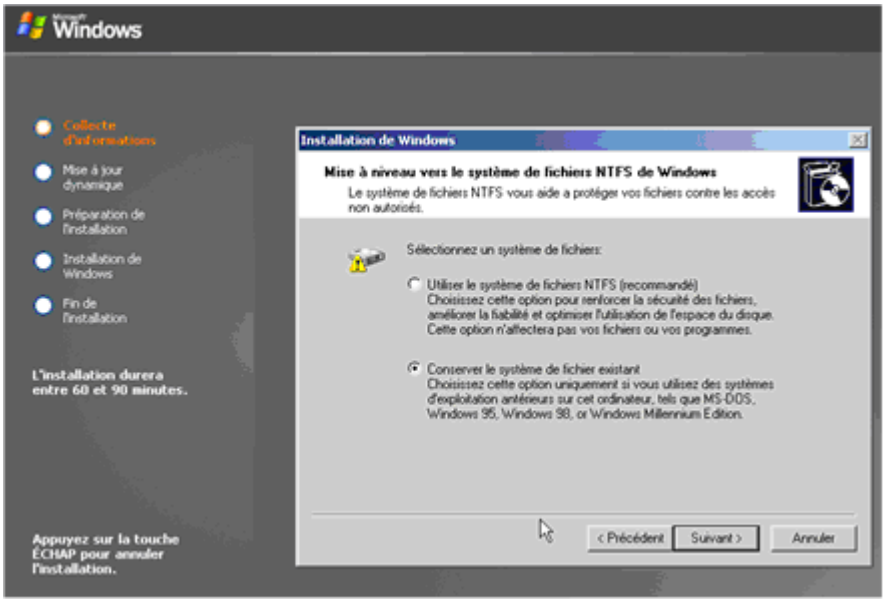


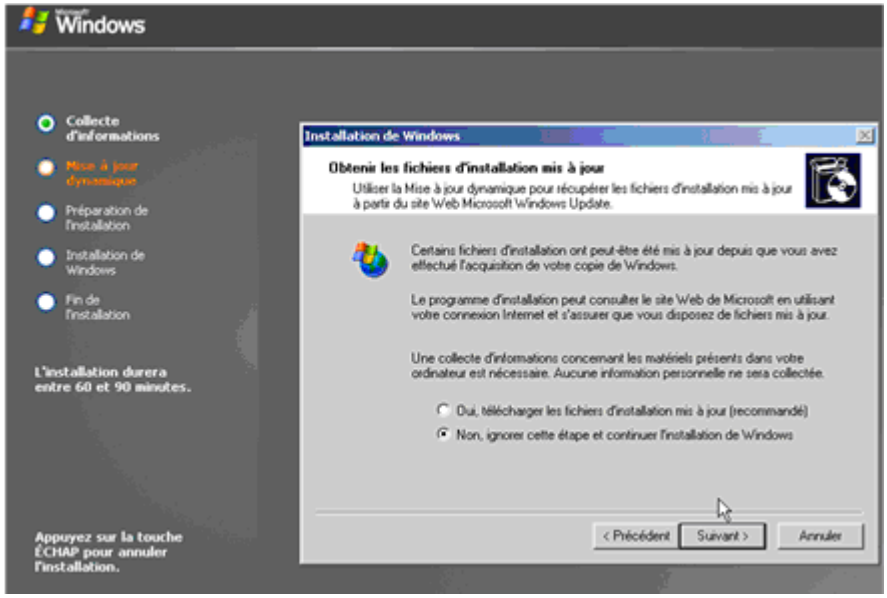



Windows
Collecte d'informations
Mise à jour dynamique
Préparation de l'installation
Installation de Windows
Fin de l'installation
L'installation durera entre 60 et 90 minutes.
Appuyez sur la touche ÉCHAP pour annuler l'installation.
Installation de Windows
Clé du produit
Entrez la clé unique de produit de votre copie de Windows.
PRODUCT KEY:
La clé du produit comporte 25 caractères. Elle se trouve sur un autocollant jaune placé au dos de la pochette du CD de Windows.
Clé du produit :
D373
< Précédent
Suivant >
Annuler


Windows
Collecte d'informations
Mise à jour dynamique
Préparation de l'installation
Installation de Windows
Fin de l'installation
L'installation durera entre 60 et 90 minutes.
Appuyez sur la touche ÉCHAP pour annuler l'installation.
Installation de Windows
Options d'installation
Modifiez la langue et configurez l'installation et les options d'accessibilité.
Pour revoir ou modifier les options par défaut pour la copie et l'installation de fichiers, cliquez sur Options avancées.
Options avancées...
Pour utiliser les fonctionnalités d'accessibilité spécifiques durant l'installation, cliquez sur Options d'accessibilité.
Options d'accessibilité...
Sélectionnez la langue principale et la région que vous voulez utiliser :
Français (France)
Installer la prise en charge des langues d'Extrême-Orient
< Précédent
Suivant >
Annuler


Windows
Collecte d'informations
Mise à jour dynamique
Préparation de l'installation
Installation de Windows
Fin de l'installation
L'installation durera entre 60 et 90 minutes.
Appuyez sur la touche ÉCHAP pour annuler l'installation.
Installation de Windows
Obtenir les fichiers d'installation mis à jour
Utiliser la Mise à jour dynamique pour récupérer les fichiers d'installation mis à jour à partir du site Web Microsoft Windows Update.
Certains fichiers d'installation ont peut-être été mis à jour depuis que vous avez effectué l'acquisition de votre copie de Windows.
Le programme d'installation peut consulter le site Web de Microsoft en utilisant votre connexion Internet et s'assurer que vous disposez de fichiers mis à jour.
Une collecte d'informations concernant les matériels présents dans votre ordinateur est nécessaire. Aucune information personnelle ne sera collectée.
Oui, télécharger les fichiers d'installation mis à jour (recommandé)
Non, ignorer cette étape et continuer l'installation de Windows
< Précédent
Suivant >
Annuler





➔ Installation à partir d'un système d'exploitation à travers le réseau

- Identique à NT4 ou W2000.
- Nécessite un serveur de distribution sur lequel est copié le répertoire I386.
- Nécessite un « Client Réseau » pour se connecter.
- Si client DOS exécuter Winnt.exe.
- Si client 32 bits exécuter Winnt32.exe.

➔ Personnalisation d'installations et de mises à niveau à l'aide de commutateurs

WINNT.EXE

Commutateur	Description
/a	Active les options d'accessibilité
/e[:*commande***]**	Exécute une commande avant la phase finale du programme d'installation
/udf:id **[,***fichier_udb***]**	Modifie le fichier de réponses

/r[:*dossier***]**	Spécifie un dossier facultatif à installer
/rx[:*dossier***]**	Spécifie un dossier facultatif à copier
/s[:*chemin_source***]**	Spécifie l'emplacement des fichiers d'installation de Windows 2003
/t[:*lecteur_temp***]**	Spécifie un lecteur pour l'installation
/u[:*fichier_réponses***]**	Effectue une installation automatisée à l'aide d'un fichier de réponses

WINNT32.EXE

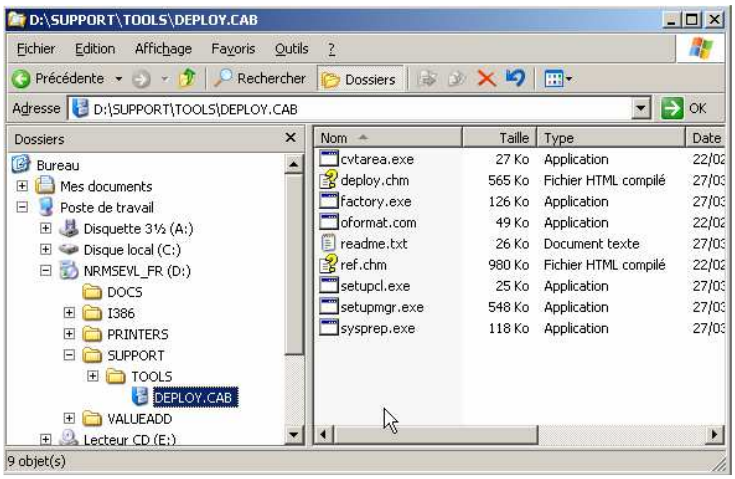
Commutateur	Description
/copydir:*dossier*	Crée un dossier supplémentaire (ou utilisez **/copysource**)
/cmd:*commande*	Exécute une commande avant la phase finale du programme d'installation
/**cmdcons**	Installe des fichiers pour la console de réparation et de récupération
/debug [*niveau***] [:***fichier***]**	Crée un journal de débogage au niveau spécifié
/s:*chemin_source*	Spécifie l'emplacement des fichiers d'installation de Windows 2003
/syspart:*lecteur*	Copie les fichiers d'installation sur un lecteur que vous pouvez déplacer
/tempdrive:*lecteur*	Spécifie un lecteur pour l'installation
/unattend [*nombre* **]** **[:***fichier_réponses* **]**	Réalise une installation automatisée avec un fichier de réponses facultatif
/unattend	Mise à niveau de la version précédente W95 ou Me en mode Installation sans assistance

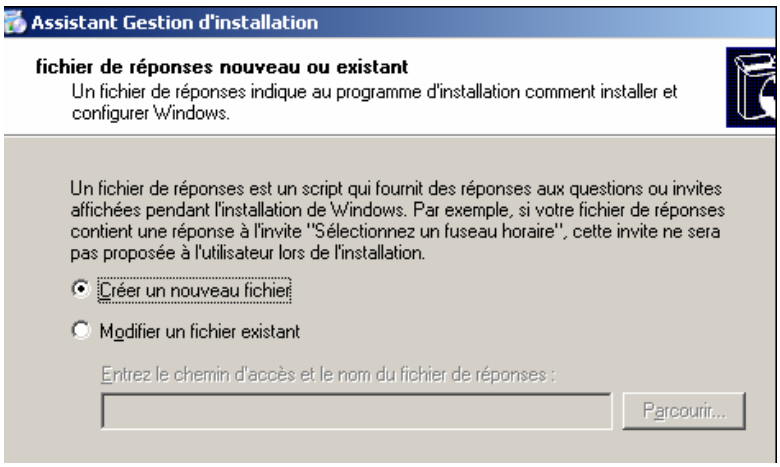
WINNT ET WINNT32

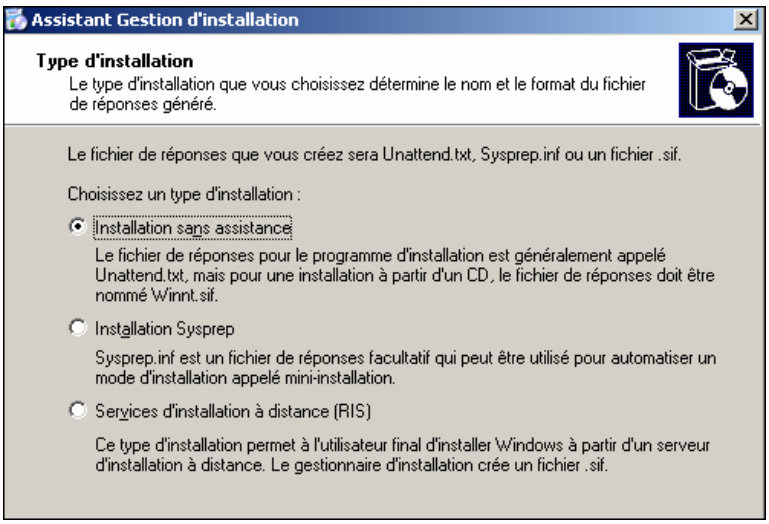
Commutateur	Description
/checkupgradeonly	Vérifie la compatibilité de votre micro pour W2003
/copysource:nom_dossier	Créée un dossier supplémentaire à l'intérieur du dossier où les fichiers W2003 sont installés
/dudisable	Invalide la mise à jour dynamique
/prepare:nomchemin	Indique un partage sur lequel vous avez chargé les fichiers MAJ dynamique à partir du site Web
/m:nom_dossier	Indique que le programme d'installation copie des fichiers de remplacement à partir d'un autre emplacement
/makelocalsource	Demande au programme d'installation de copier tous les fichiers source d'installation sur votre disque local
/noreboot	Demande à l'ordinateur de ne pas redémarrer l'ordinateur à l'issue de la phase de copie de l'installation afin d'exécuter une autre commande
/unattend [*nombre* **]** **[:***fichier_réponses* **]**	Réalise une installation automatisée avec un fichier de réponses facultatif
/udf:*id* **[,***fichier_udf* **]**	Procède à l'installation en utilisant le fichier UDB

2.6- Automatiser les installations

Nous allons utiliser l'utilitaire setupmgr.exe qui permet de créer un fichier de réponses à l'aide d'un assistant. Il est situé sur le CD-ROM de W2003 dans le fichier **deploy.cab** du dossier **support\tools**. Double-cliquez sur le fichier deploy.cab pour afficher son contenu. Vous devez extraire les fichiers dans un dossier (option disponible dans le menu contextuel) en faisant un clic droit dessus. Exécutez setupmgr.exe et paramétrez les écrans successifs.



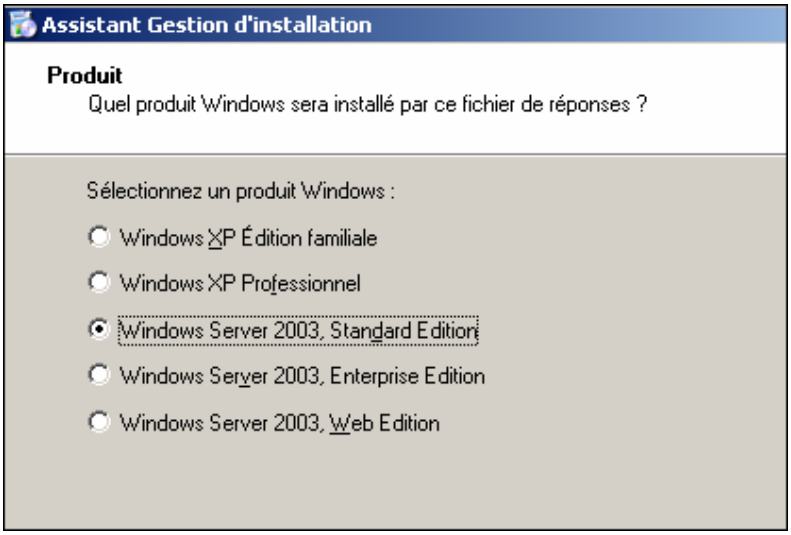




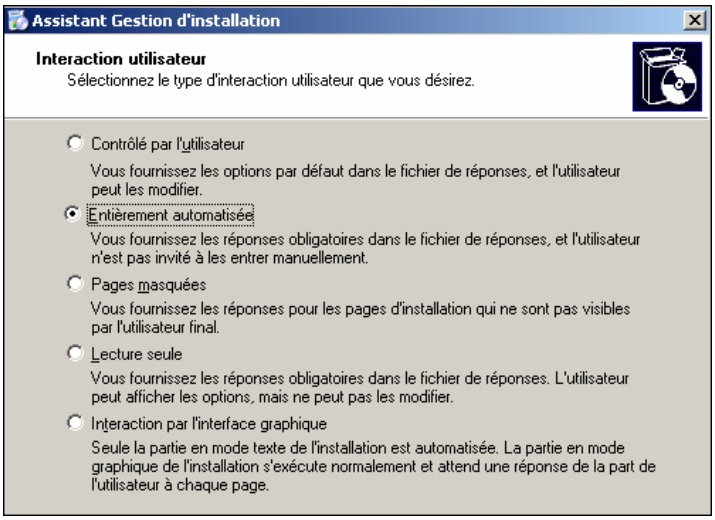
Sur cet écran 3 propositions sont proposées :

- Créer un fichier d'installation sans assistance.
- Créer un fichier pour une installation Sysprep (utilisé pour la duplication de disques).
- Créer un fichier utilisable avec les services d'installation à distance (RIS).

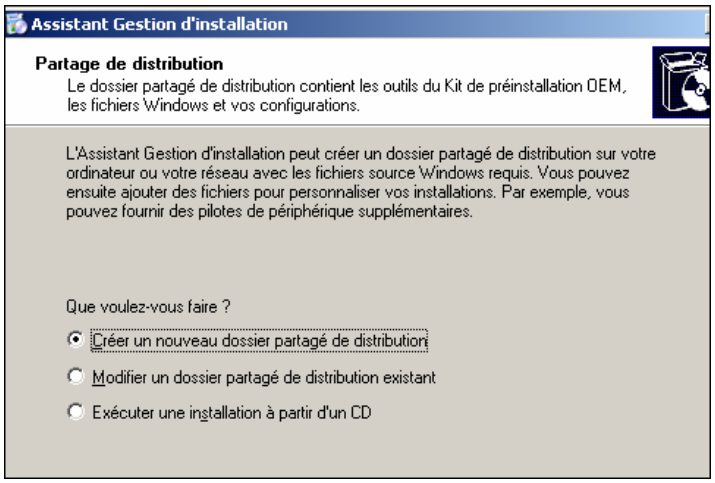
Sélectionnez **Installation sans assistance**, puis cliquez sur **Suivant**.



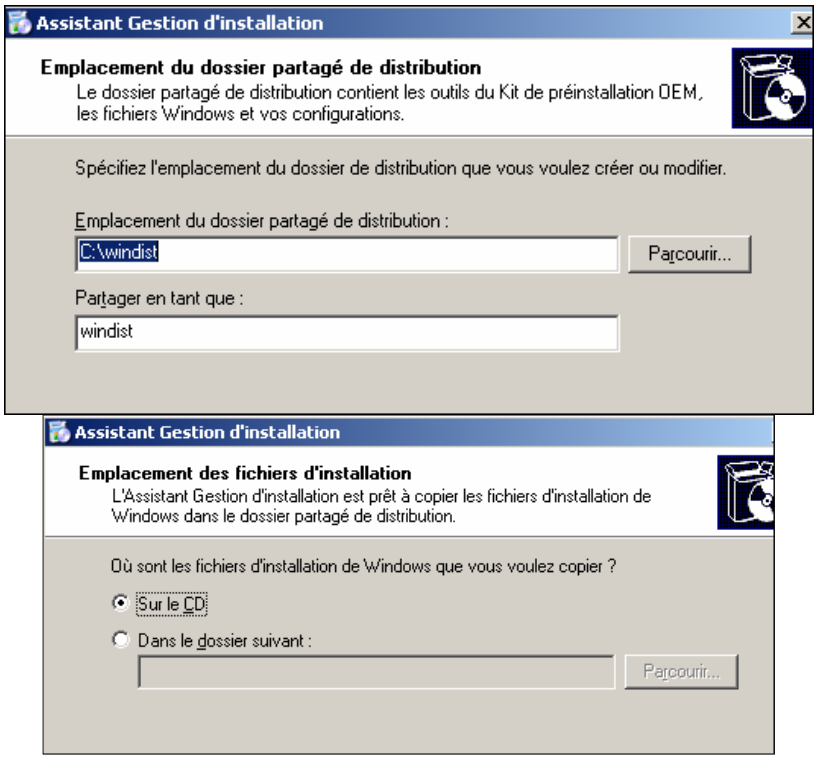
Choisissez le système d'exploitation à installer, puis cliquez sur **Suivant**.



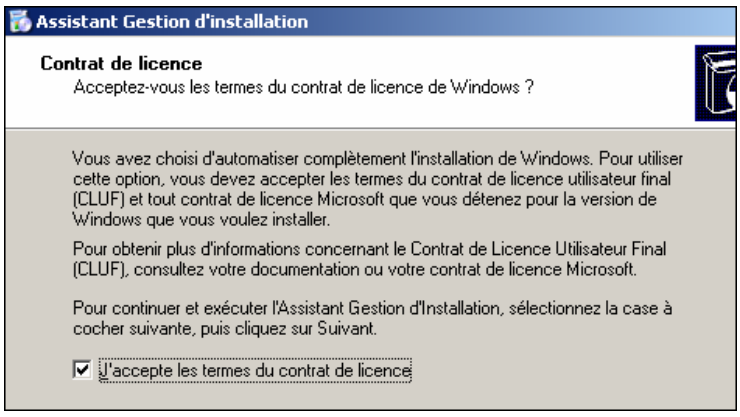
Vous définissez avec cette fenêtre le niveau d'interaction du programme d'installation avec l'utilisateur. Dans notre exemple **Entièrement automatisé** est sélectionné afin de réaliser une installation complète sans intervention de l'utilisateur. Cliquez sur **Suivant**.



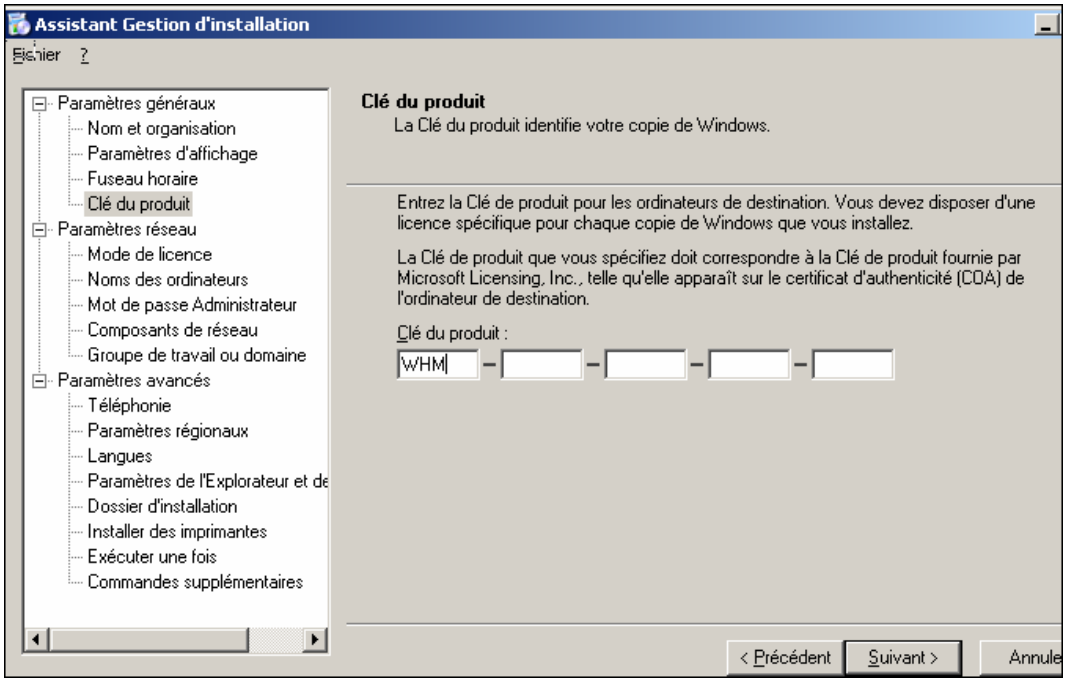
Dans cette fenêtre vous pouvez créer ou modifier un dossier de distribution, ou indiquer que l'installation sera réalisée à partir du CD-ROM. Dans ce cas il vous suffit de nommer le fichier winnt.sif et le copier sur une disquette qu'il faudra insérer dans le lecteur de disquettes au début de l'installation à partir du CD-ROM.

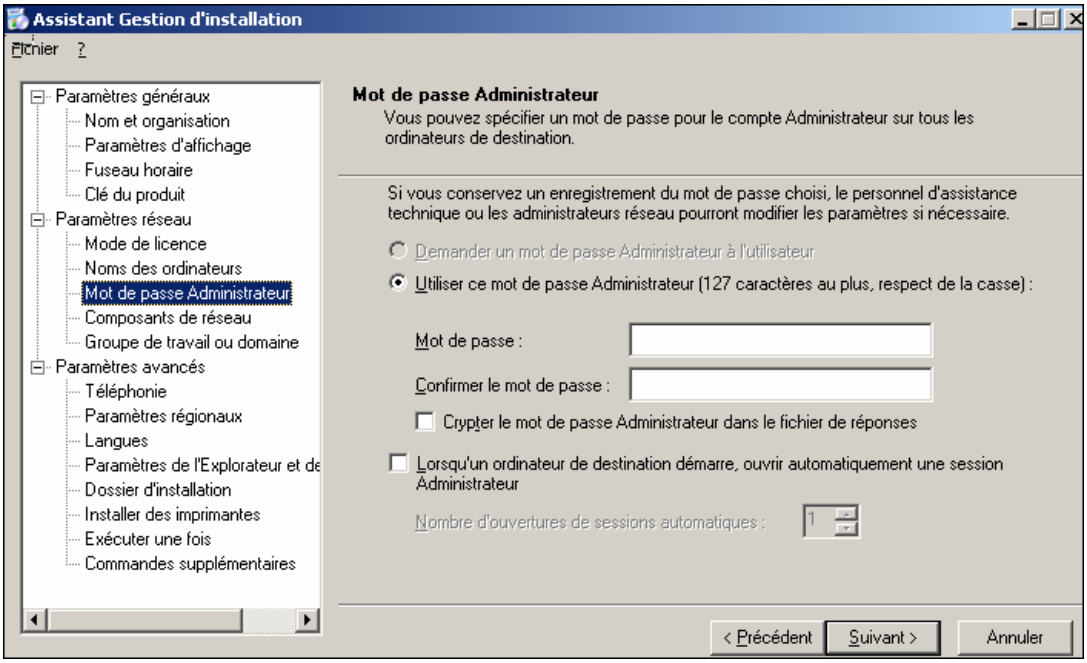


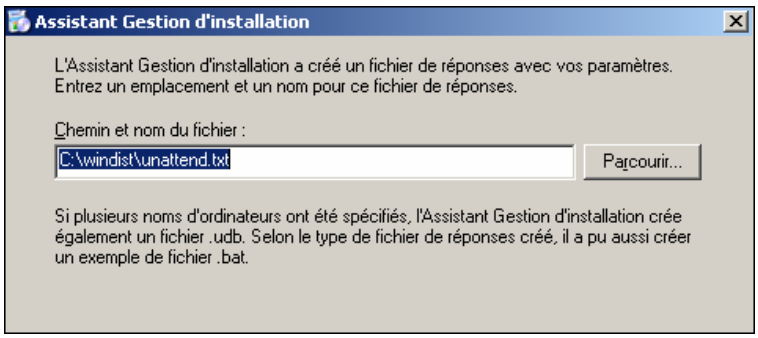
Dans les écrans précédents vous devez indiquer l'emplacement de la source de distribution et le dossier où créer cette distribution. L'écran **Contrat de licence** demande d'accepter le contrat de licence.

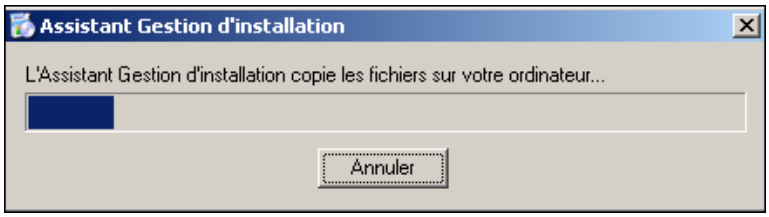


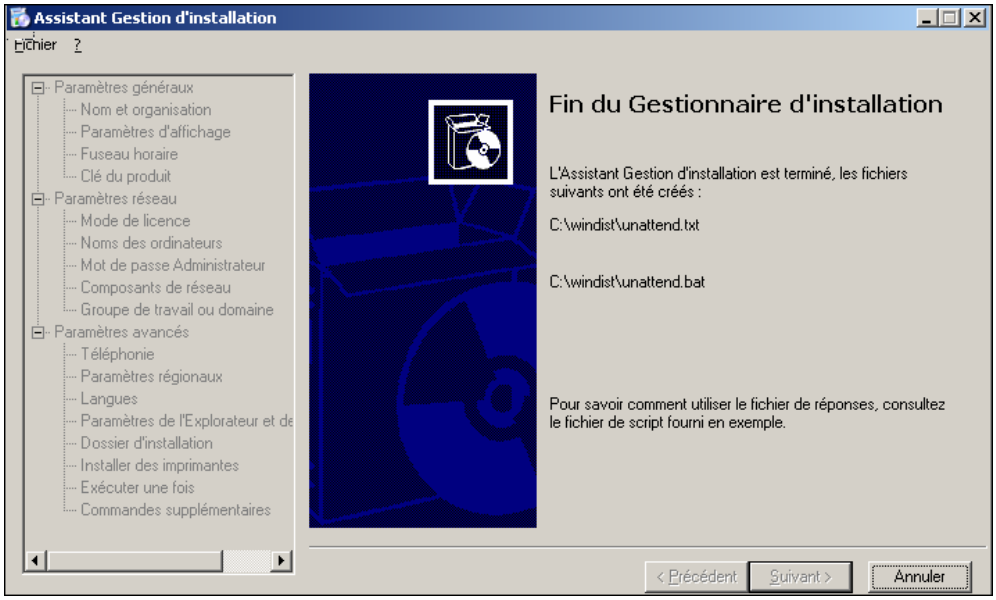
L'écran **Clé de produit** permet d'indiquer le numéro de licence. Dans la partie gauche de cette fenêtre, vous remarquez les différentes étapes de l'assistant.

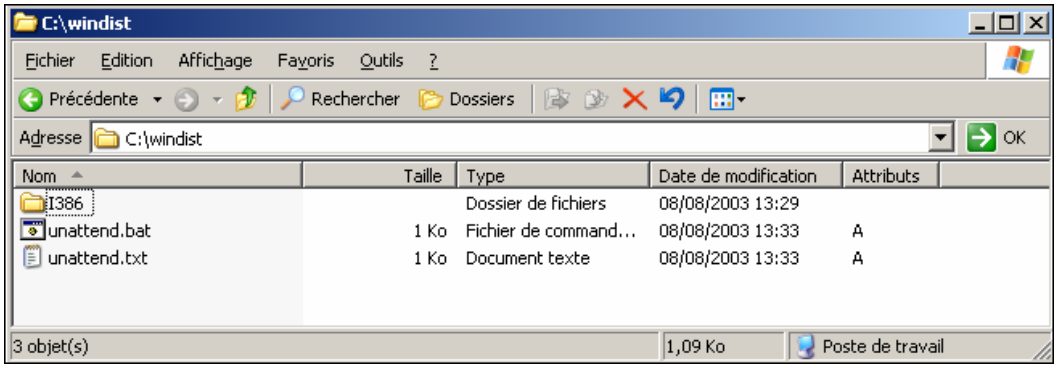





Assistant Gestion d'installation
L'Assistant Gestion d'installation a créé un fichier de réponses avec vos paramètres.
Entrez un emplacement et un nom pour ce fichier de réponses.
Chemin et nom du fichier :
C:\windist\unattend.txt
Parcourir...
Si plusieurs noms d'ordinateurs ont été spécifiés, l'Assistant Gestion d'installation crée également un fichier .udb. Selon le type de fichier de réponses créé, il a pu aussi créer un exemple de fichier .bat.


Assistant Gestion d'installation
L'Assistant Gestion d'installation copie les fichiers sur votre ordinateur...
Annuler


Assistant Gestion d'installation
Fichier ?
Paramètres généraux
Nom et organisation
Paramètres d'affichage
Fuseau horaire
Clé du produit
Paramètres réseau
Mode de licence
Noms des ordinateurs
Mot de passe Administrateur
Composants de réseau
Groupe de travail ou domaine
Paramètres avancés
Téléphonie
Paramètres régionaux
Langues
Paramètres de l'Explorateur et de
Dossier d'installation
Installer des imprimantes
Exécuter une fois
Commandes supplémentaires
Fin du Gestionnaire d'installation
L'Assistant Gestion d'installation est terminé, les fichiers suivants ont été créés :
C:\windist\unattend.txt
C:\windist\unattend.bat
Pour savoir comment utiliser le fichier de réponses, consultez le fichier de script fourni en exemple.
< Précédent
Suivant >
Annuler


C:\windist
Fichier Edition Affichage Favoris Outils ?
Précédente
Rechercher
Dossiers
Adresse C:\windist
OK
Nom
Taille
Type
Date de modification
Attributs
I386
Dossier de fichiers
08/08/2003 13:29
unattend.bat
1 Ko
Fichier de command...
08/08/2003 13:33
A
unattend.txt
1 Ko
Document texte
08/08/2003 13:33
A
3 objet(s)
1,09 Ko
Poste de travail

unattend.txt - Bloc-notes

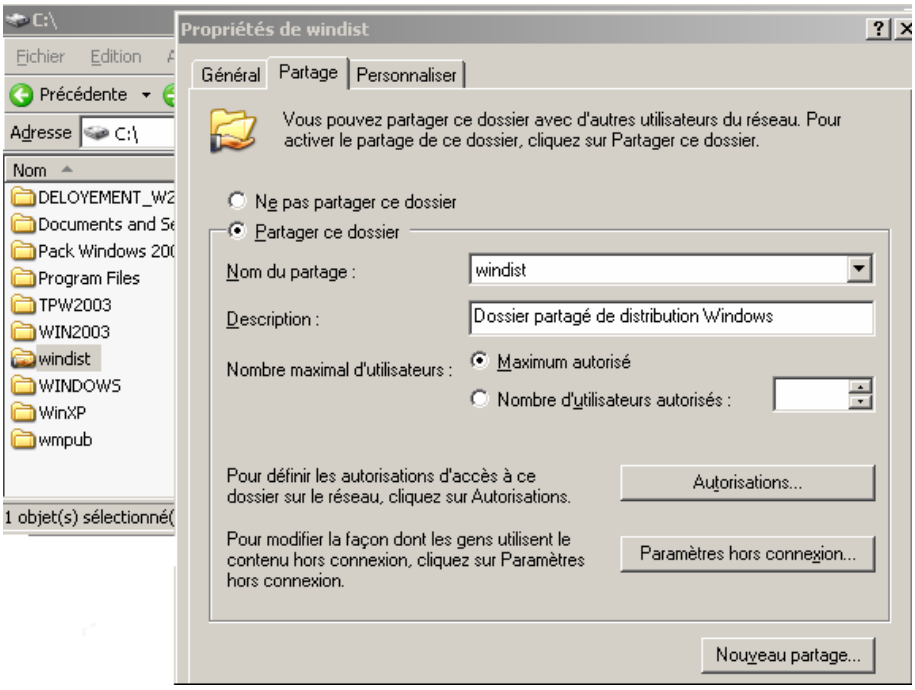
Fichier Edition Format Affichage ?

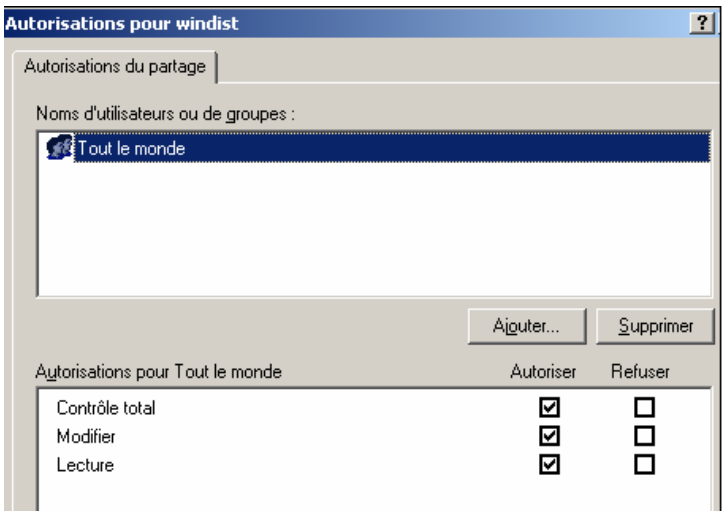
```
;SetupMgrTag
[Data]
    AutoPartition=1
    MsDosInitiated="0"
    UnattendedInstall="Yes"

[Unattended]
    UnattendMode=FullUnattended
    OemSkipEula=Yes
    OemPreinstall=Yes
    TargetPath=\WINDOWS

[GuiUnattended]
    AdminPassword=*
    EncryptedAdminPassword=NO
    OEMSkipRegional=1
    TimeZone=85
    OemSkipWelcome=1

[UserData]
    ProductKey=
    FullName=
    OrgName=
    ComputerName=

[LicenseFilePrintData]
    AutoMode=PerServer
    AutoUsers=5

[SetupMgr]
    DistFolder=C:\windist
    DistShare=windist

[Identification]
    JoinWorkgroup=WORKGROUP

[Networking]
    InstallDefaultComponents=Yes
```

unattend.bat - Bloc-notes

Fichier Edition Format Affichage ?

```
@rem SetupMgrTag
@echo off

rem
rem Ceci est un EXEMPLE de script de commande généré par l'Assistant Gest
rem Si ce script est déplacé de l'emplacement dans lequel il a été créé,
rem

set AnswerFile=.\unattend.txt
set SetupFiles=\\POSTEMF\windist\I386

\\POSTEMF\windist\I386\winnt32 /s:%SetupFiles% /unattend:%AnswerFile%
```

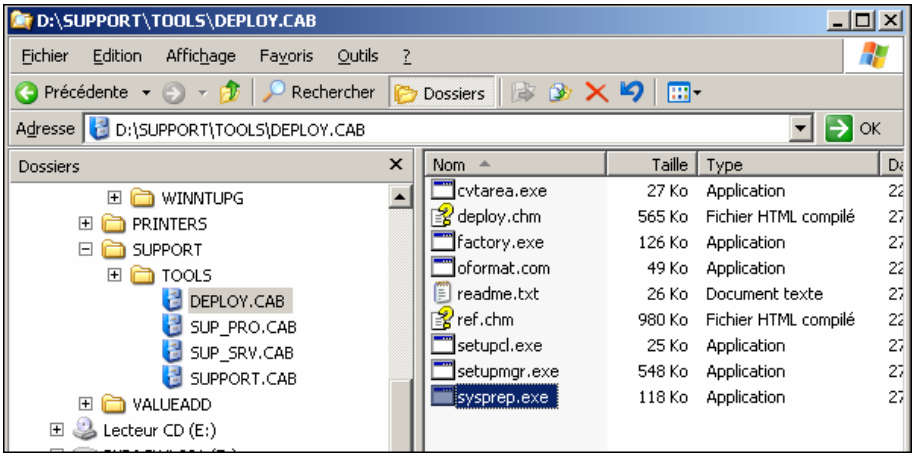




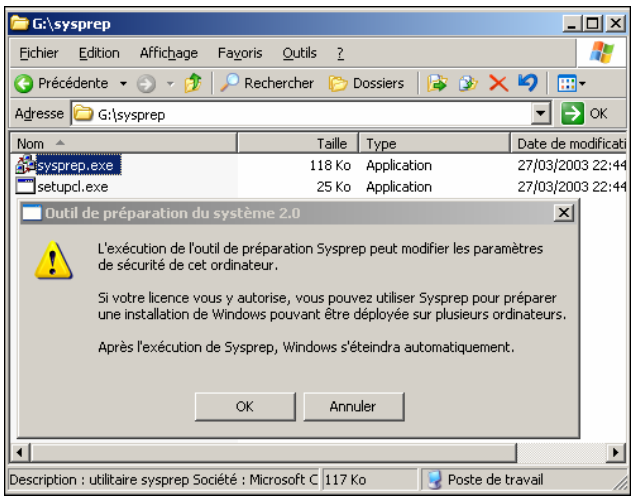
2.7- Duplication de disque

Cette procédure d'installation est bien répandue.

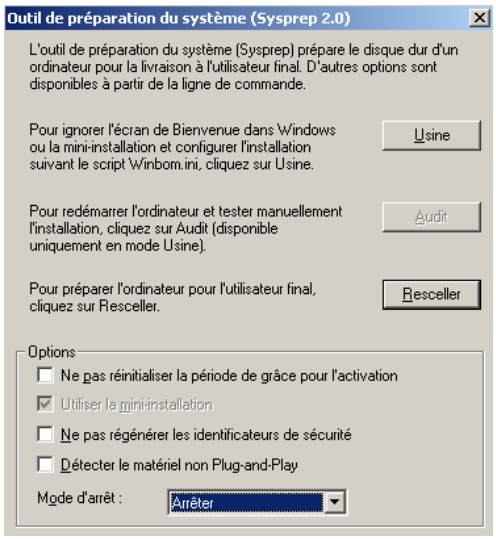
- Préparer une machine de référence complètement installée et paramétrée avec les applications.
- Créer une image disque de cette machine avec un outil tierce partie (Ghost par exemple) et l'enregistrer sur un serveur ou un CD-ROM.
- Copier cette image sur la nouvelle machine avec le même outil.
- Cette procédure a l'inconvénient de conserver le même identifiant de sécurité (SID : Security Identifier) pour tous les postes. Mais ces identifiants doivent être uniques sur le réseau pour un fonctionnement correct.
- En plus Microsoft ne supporte pas les machines installées de cette façon.
- Pour résoudre cela W2003 Server possède l'outil **Sysprep.exe** qui se situe dans le fichier **deploy.cab** du répertoire **support\tools** du CD de W2003 Server.



Cliquez sur **sysprep.exe** afin de lancer l'exécution. Une information s'affiche vous indiquant que les paramètres de sécurité seront modifiés et que la machine sera arrêtée afin de permettre de créer l'image disque.



La fenêtre outil de préparation du système s'ouvre.

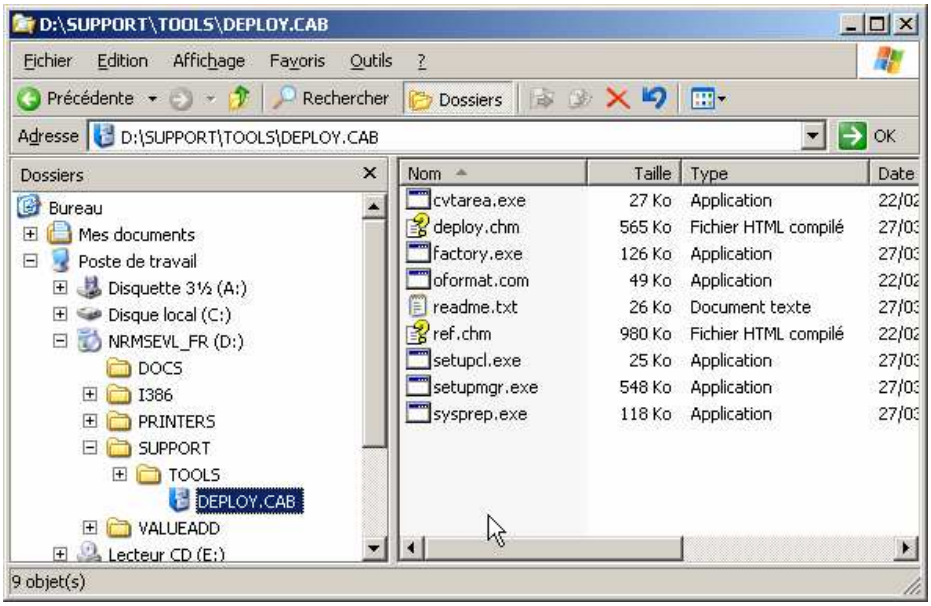


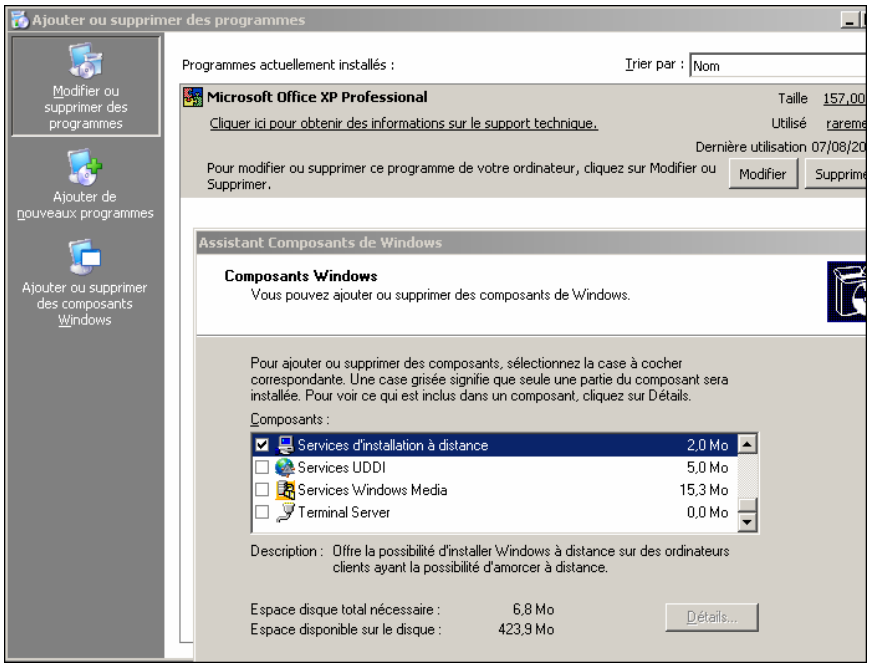
Usine : redémarrage sans afficher la mini installation. Utile pour mettre à jour des pilotes, exécuter l'énumération PnP et diverses configurations spécifiques.
Audit : redémarre la machine en mode Usine sans générer de nouveau SID.
Resceller : prépare la machine pour l'utilisateur final. Nettoie les journaux d'événements.

2.8- Service d'installation à distance RIS (Remote Installation Service)

Une autre méthode d'installation consiste à utiliser le service d'installation à distance RIS (Remote Installation Service). Ce service permet l'installation par le réseau des ordinateurs Windows XP ou de la famille W2003 Server. Il offre la possibilité d'installation du système d'exploitation seulement ou d'une image disque (image d'une machine de référence contenant une configuration avec les applications installées sans avoir besoin d'un outil de type Partition Magic). Un serveur RIS doit avoir Active Directory, serveur DNS et DHCP installés.
L'installation est réalisée à partir du **Panneau de Configuration - Ajout/Suppression de programmes - Ajouter ou Supprimer des composants Windows**. Le service installé, la machine redémarre.
Vous devez ensuite configurer le service soit avec la commande **risetup.exe**, soit en prenant l'option **Installation des services d'installation à distance** dans les **Outils d'administration**. Il faut alors fournir un CD de distribution du système d'exploitation à installer. RIS impose une partition formatée en NTFS autre que la partition système et d'amorçage pour gérer son répertoire de distribution.

Pour fonctionner le poste client démarre et à l'aide du module Pre-Boot Environnement (PXE) de sa carte réseau, il obtient une adresse IP par un serveur DHCP. Les serveurs DNS et Active Directory lui permettent de contacter le serveur RIS.
L'utilisateur qui a en charge l'installation doit alors s'authentifier et les divers types d'installation autorisés lui sont proposés. Avec les fichiers de réponses, l'installation peut être complètement automatisée. Dans le cas de cartes réseau ne possèdent pas du module PXE, la commande **rbfg.exe** permet de créer une disquette d'amorçage capable de l'émuler.

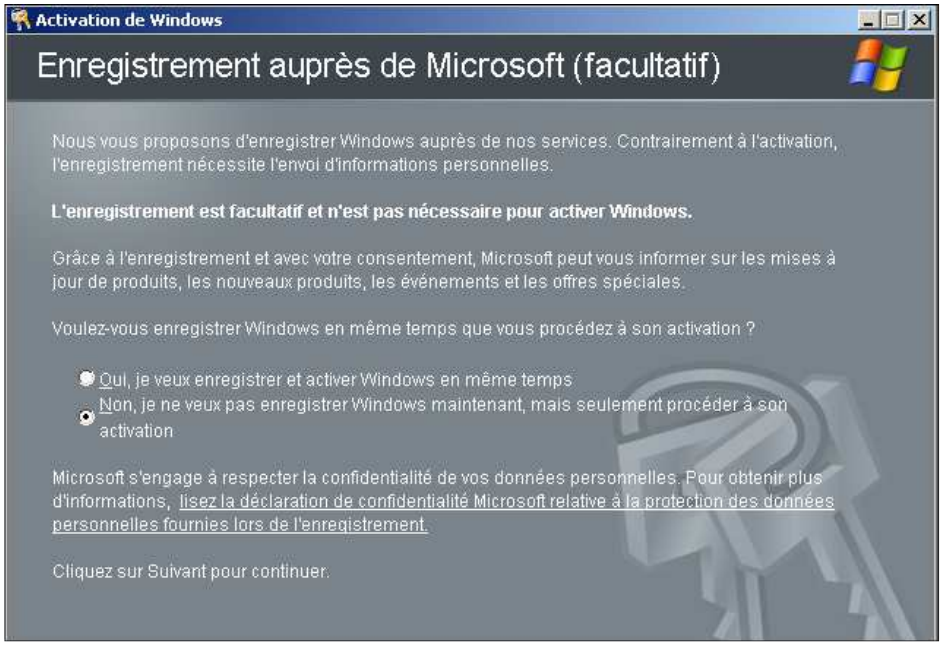




2.9- Activation de W2003 Server

Pour lutter contre le piratage de ses logiciels, Microsoft a institué un processus d'activation (comme sous XP sauf pour les versions VLK, anciennement corporate). Si vous avez choisi la licence de site (en quantité) pas d'activation, sinon un délai de quelques jours est accordé (version d'évaluation 15 jours). Après ce délai de grâce sans activation, vous ne pouvez plus travailler. Le principe de fonctionnement de cette activation repose sur la création d'un code généré par une formule mathématique (hachage...) prenant en compte la configuration matérielle de votre micro, tel la carte mère, le processeur, la carte graphique, le disque dur, la mémoire, la carte réseau… A chaque

activation une vérification est réalisée afin de ne pas retrouver le même produit sur un autre ordinateur. Par contre une petite souplesse est accordée permettant à l'utilisateur de faire évoluer son ordinateur comme l'ajout de la mémoire par exemple… Lors du démarrage de W2003 Server, l'assistant vous propose d'activer le produit. L'assistant d'activation peut être lancé ultérieurement à partir du menu **Démarrer**.



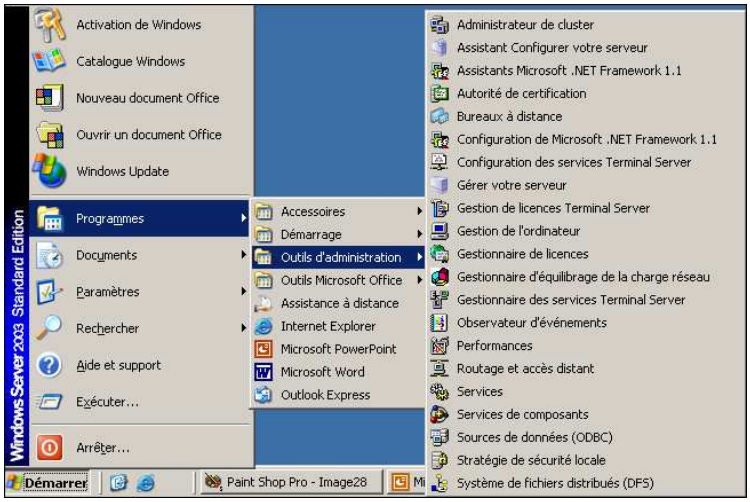
✋ N'activez pas Windows immédiatement après son installation, le nombre d'activations étant limité, attendez d'être sûr que l'installation est définitive.

2.10- Les outils d'administration

2.10.1- Installer les outils par défaut

Un groupe **Outils d'administration** est automatiquement créé avec plusieurs consoles de gestion. Par contre tous les outils ne sont pas installés par défaut. Certains ne le seront uniquement que si les services correspondants sont installés. Un exemple classique est l'installation de la console DHCP

sur un serveur uniquement si le service DHCP est installé. Il est possible d'installer tous les outils qui se trouvent dans le fichier **adminpak.msi**.

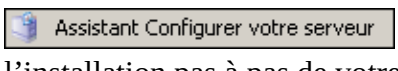


Tous les outils sont disponibles sur le CD-Rom de W2003 Server dans le dossier I386 ou dans le dossier %systemroot%\system32 quand le serveur est installé.

2.10.2- Outils d'administration courants

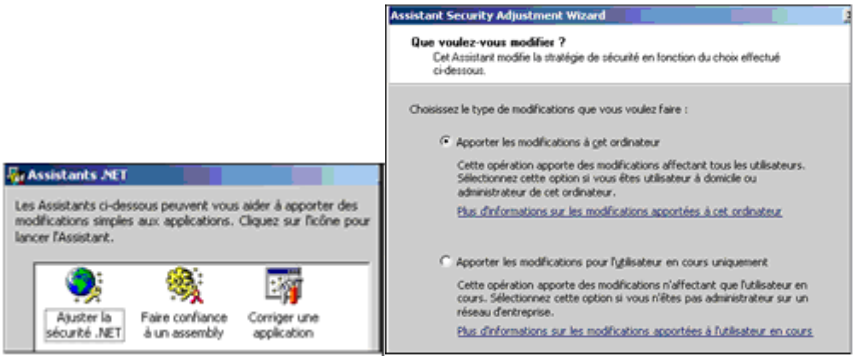
Les assistants

Assistant Gérer votre serveur : permet de lancer le Centre d'Aide et de support afin de vous aider à tout instant dans votre travail au quotidien ou en cas de problème.



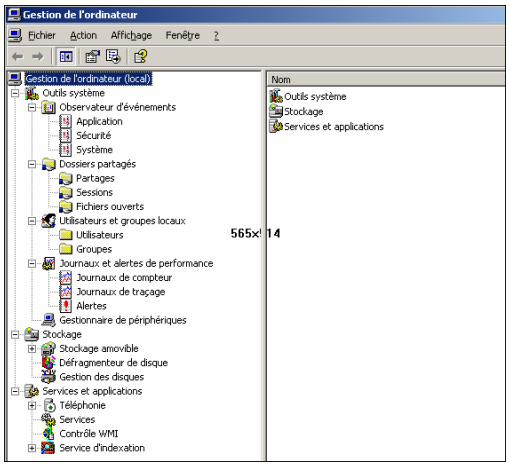
Assistant Configurer votre serveur : cet assistant vous permet l'installation pas à pas de votre serveur.

Assistants Microsoft .NET Framework 1.1 : permet d'accéder aux outils de configuration de la plate-forme de développement .NET de Microsoft.



2.10.3- Console Gestion de l'ordinateur

C'est l'outil le plus utilisé que ce soit sur un poste local ou en réseau. Cette console regroupe tous les outils les plus couramment utilisés. Pour l'exécuter vous devez être logué en Administrateur ou équivalent. Cette console est basée sur le composant logiciel enfichable **compmgmt.msc**.



C'est dans cette console que vous retrouvez les **Outils systèmes** comme :

- **Observateur d'événements** (erreurs et avertissements) avec les journaux Application, Sécurité et Système.
- **Dossiers partagés** avec la possibilité de visualiser, créer ou supprimer des répertoires partagés. Vous pouvez aussi visualiser les fichiers ouverts des sessions en cours.
- **Utilisateurs et groupes locaux** pour gérer et créer les comptes utilisateurs et les groupes locaux de votre micro. Nous verrons que lorsque votre micro a rejoint un domaine cette fonctionnalité est remplacée (en fait elle est barrée pour invalidation) par la console Utilisateurs et ordinateurs d'Active Directory.
- **Journaux et alertes de performances** vous permet de fixer les alertes sur les objets afin de pouvoir visualiser les résultats dans les journaux d'événements.
- **Gestionnaire de périphériques** est très utile pour gérer la totalité des périphériques et drivers de votre micro.

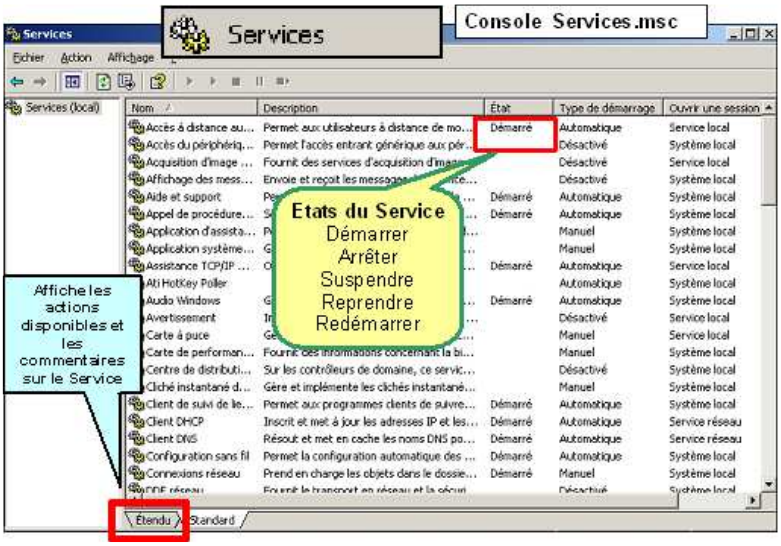
Vous avez aussi les éléments pour gérer le **Stockage** comme :

- **Stockage amovible** afin de gérer les supports de sauvegarde comme les CD-ROM ou lecteurs de bandes magnétiques.
- **Défragmenteur** est l'outil universel chez Microsoft pour réorganiser physiquement les fichiers clairsemés sur votre machine.
- **Gestion des disques** pour gérer, visualiser, créer ou modifier la structure de vos disques et partitions.

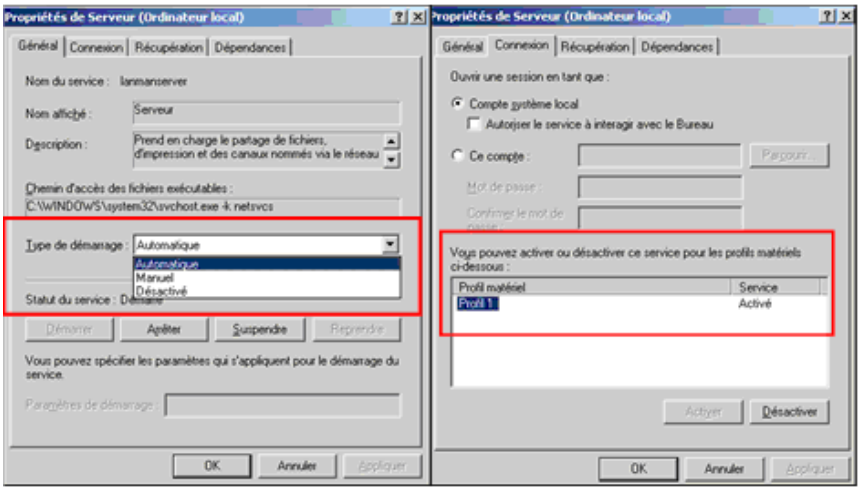
Vous trouvez aussi les éléments **Services et applications** tels :

- **Téléphonie** pour gérer les fournisseurs de services de téléphonie (normes TAPI, H323…).
- **Services** pour gérer l'ensemble des services de votre micro.
- **Contrôle WMI** pour gérer et configurer l'architecture WMI (Windows Management Instrumentation) utile pour les développeurs qui souhaitent développer leurs propres applications ou scripts.
- **Services d'Indexation** permet d'indexer des documents et leurs propriétés sur vos disques et de conserver ces informations dans un catalogue.

2.10.4- Les services



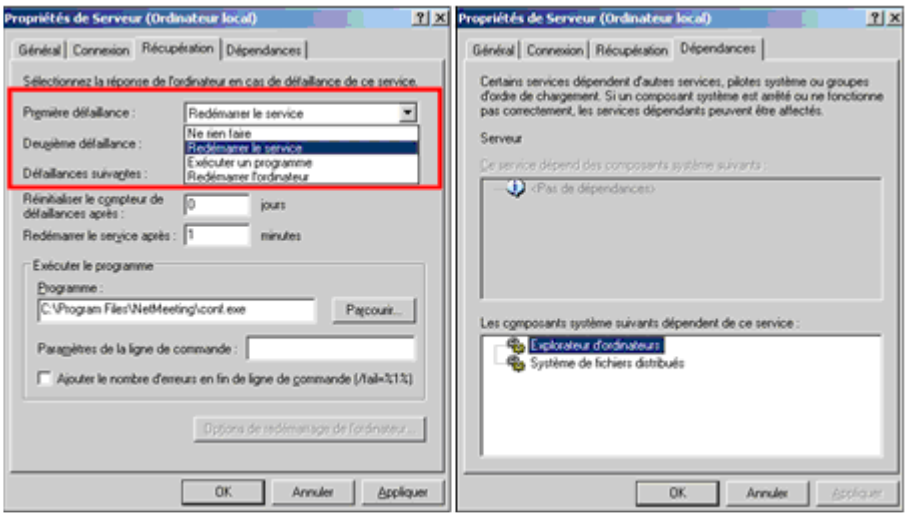
Cet outil disponible dans la console **Gestion de l'ordinateur**, l'est aussi directement dans les outils d'administration. Tous les services installés sont rassemblés dans la console. Vous pouvez les trier en ordre croisant ou décroissant afin de faciliter votre travail de recherche. Deux onglets vous permettent de visualiser soit de façon classique les services (**Standard**) ou avec plus de détails (**Etendu**). En sélectionnant un service vous pouvez l'**Administrer** et lancer une **Action**. Cette action possible sera fonction de l'état du service, de son type ou des droits dont vous disposez.



Vous pouvez :

- **Démarrer :** permet le démarrage du service ainsi que ces dépendances. L'échec du démarrage étant souvent du à une dépendance qui n'a pas démarré. Vous visualisez le résultat dans le journal des événements.
- **Arrêter :** comme son nom l'indique cette action stoppe le service et les éventuelles dépendances.

- **Suspendre :** mise en pause du service sélectionné mais ne stoppe pas les dépendances.
- **Reprendre :** redémarre le service venant d'être mis en pause.
- **Redémarrer :** réinitialise (suite à un arrêt puis un redémarrage) le service et les dépendances.



Vous pouvez modifier le type de démarrage du service dans les **Propriétés** du serveur et dans l'onglet **Général**. Les choix possibles sont :

- **Automatique :** dans ce cas le service sera lancé systématiquement à chaque démarrage du système.
- **Manuel :** lancé par l'action de l'utilisateur ou par une application ou par le système lui-même.
- **Désactivé :** dans ce cas le service n'est jamais lancé.

Les autres onglets disponibles vous permettent d'indiquer avec quel compte utilisateur (lié aux droits) le service va démarrer (onglet **Connexion**).
L'onglet **Récupération** détermine l'action à réaliser si le service rencontre une erreur (ne rien faire, redémarrer le service, exécuter un programme ou redémarrer le micro).
Le dernier onglet, **Dépendances**, vous permet de contrôler les liaisons vis-à-vis des autres services.

2.10.5- Outils d'administration spécifiques

Leur nombre sera fonction de la version du système et du type de fonctionnement du serveur.

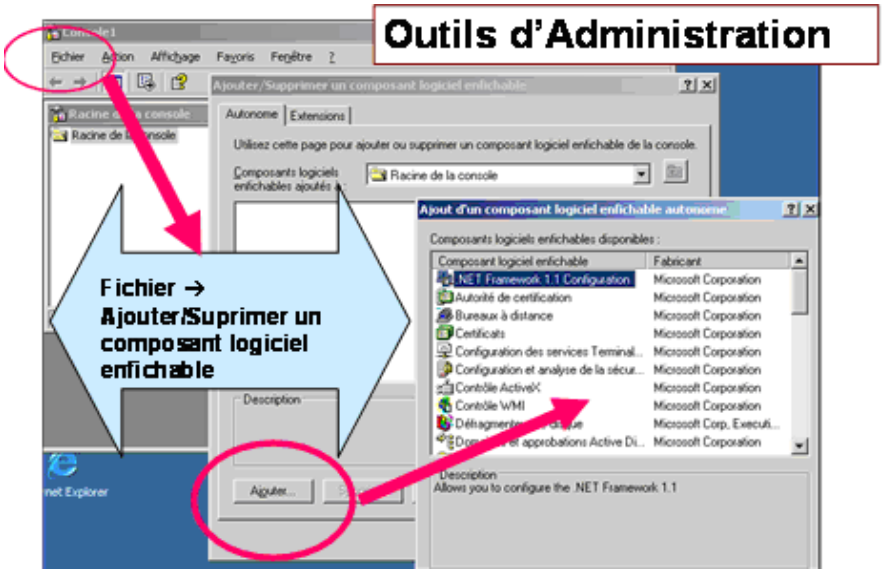
	Gestionnaire d'équilibrage de charge du réseau (NLB: Network Load Balancing) : permet la gestion de la répartition de charge réseau au sein d'un groupe de machines montées en Cluster.
	Administrateur du Cluster : disponible uniquement sur les versions Enterprise et DataCenter.
	Gestionnaire des services Terminal Server : permet d'administrer les sessions ouvertes sur un serveur de terminaux Windows (TSE).
	Gestionnaire des licences Terminal Server : ne pas confondre avec l'outil Licences. Permet la gestion des licences nécessaires pour travailler en client du service Terminal server.
	Configuration des Services Terminal Server (tscc.msc) : permet de contrôler les paramètres de sessions Terminal server basées sur le protocole RDP 5.1.
	Bureaux à Distance (tsmmc.msc) : défini les paramètres de connexion et d'affichage de chaque poste client, afin d'ouvrir une session à distance.

	Système de fichiers distribués (dfsgui.msc) : permet de déclarer et gérer les ressources partagées avec DFS *(Distributed File System).* Type d'architecture permettant de partager des dossiers sans savoir où ils se situent.
	Autorité de certification (certsrv.msc) : disponible uniquement sur les versions Enterprise et DataCenter.
	Services de composants (comesp.msc) : permet de gérer la base de composants COM, COM +, DCOM.
	Sources de données ODBC : permet de déclarer ou supprimer des sources de données ODBC avec des noms de sources de données *(DSN, Data Source Names).*
	Routage et accès distant (rrasmgmt.msc) : permet de configurer les interfaces de routage et l'accès distant.
	Configuration du Framework .NET 1.1 Microsoft : permet la configuration des éléments de la plateforme d'exécution .NET de Microsoft. Utilisé par les développeurs.

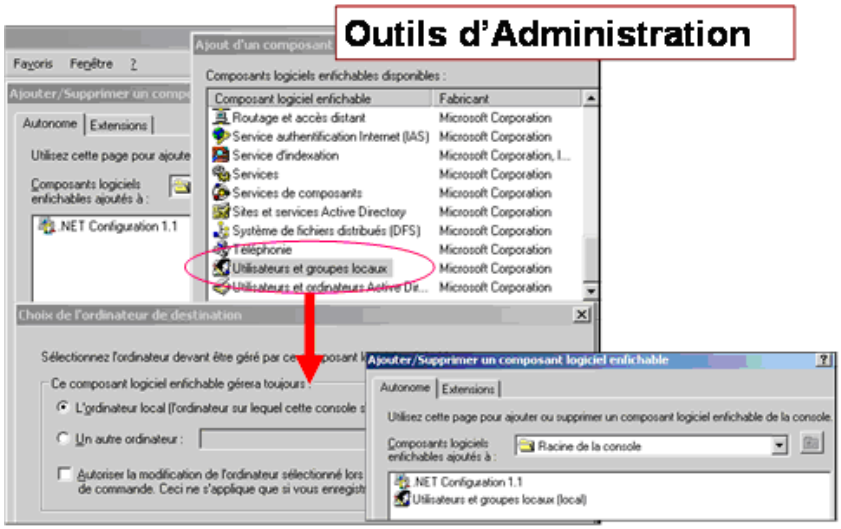
	Gestionnaire des licences : permet d'ajouter, supprimer, connaître l'état des affectations ou libérer des licences allouées aux clients.
	Utilisateurs et ordinateurs d'Active Directory (Dsa.msc) : disponible uniquement sur les serveurs contrôleur de domaine. Permet la gestion des objets d'un domaine Active Directory (utilisateurs, ordinateurs, OU…).
	Sites et services d'Active Directory (Dssite.msc) : permet de gérer les sites d'Active Directory (sites, liens de sites, réplications, sous réseaux IP…).
	Domaines et approbations d'Active Directory (Domain.msc) : permet d'administrer les relations d'approbation entre les domaines d'une forêt.
	Stratégie de sécurité du Contrôleur de domaine.
	Stratégie de sécurité du domaine.

2.10.6- La console MMC (Microsoft Management Console)

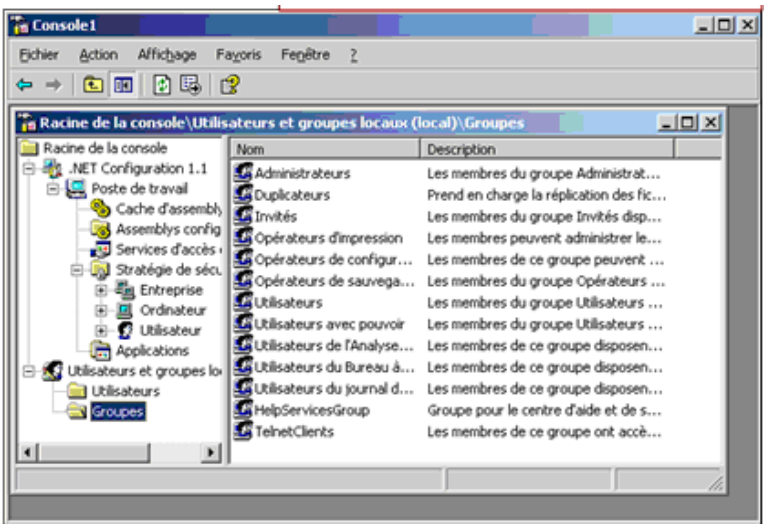
Tous les **Outils d'administration** sont présentés avec une interface commune standard nommée console MMC. Vous avez la possibilité de créer votre propre MMC afin d'avoir plus rapidement à disposition les outils les plus souvent utilisés. Tous les outils contenus dans le package adminpak.msi n'apparaissent pas sous forme de raccourcis dans les outils d'administration. Ils sont par contre installés sous forme de composants logiciels enfichables (snap in en anglais) et utilisables dans une console MMC. Cliquez sur **Démarrer - Exécuter - mmc.exe**. Une console vide s'ouvre, vous permettant d'y ajouter vos outils.



Dans le menu **Fichier**, cliquez sur **Ajouter/Supprimer un composant logiciel enfichable**, puis sur **Ajouter**.



Sélectionnez les outils souhaités, en cliquant sur **Ajouter** pour chacun d'eux. Au final, cliquez sur **Terminer**.



Les outils apparaissent désormais dans une même console. Vous pouvez à tout instant ajouter ou supprimer des outils. Vous pouvez aussi à partir du menu **Fichier** enregistrer votre console dans un fichier portant l'extension .msc. Ce fichier pourra être copié et utilisé sur d'autres machines ayant les logiciels enfichables correspondants installés avec adminpak.msi.

2.10.7- Arrêt du Serveur

C'est une nouveauté de Windows 2003 Server. Lorsque vous l'arrêtez, une fenêtre de dialogue s'ouvre. Une liste déroulante avec choix de la raison qui vous pousse à arrêter s'affiche avec la possibilité d'ajout de commentaires. Les informations sont lisibles dans le journal système de l'**Observateurs d'événements.**
Il est vrai que ce fonctionnement est assez contraignant, mais entre dans la nouvelle optique sécuritaire et de traçabilité de Microsoft. Cette boite de dialogue apparaît automatiquement au premier administrateur qui ouvre une session lors d'un arrêt anormal du serveur afin qu'il indique la raison de cet arrêt. Vous avez la possibilité de supprimer cette contrainte avec les stratégies de groupes.

III- CONFIGURATION DE L'ENVIRONNEMENT

3.1- La base de registre

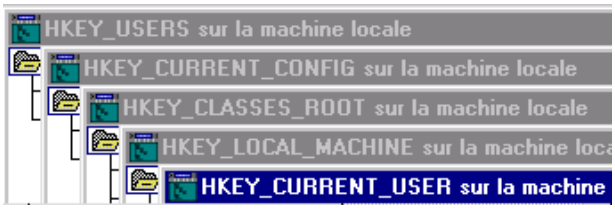
3.1.1- Définition du Registre WINDOWS 2003

Présentation
La base de registre représente l'évolution actuelle des anciens fichiers système de Windows 3.1 et constitue le réceptacle unique dans lequel sont placées toutes les informations de configuration concernant Windows et votre ordinateur. Elle est sensiblement plus complexe qu'un fichier .INI, mais possède une puissance et une souplesse bien supérieures.
Elle intègre de nombreuses notions qui vous permettront de personnaliser et d'optimiser votre ordinateur.

Un peu d'histoire
Si vous avez déjà eu l'occasion de "bidouiller" avec Windows 3.x, vous avez forcément passé un certain temps à éditer des fichiers .INI. Windows 3.x utilisait ces fichiers pour enregistrer les informations concernant la configuration. Les données du système étaient placées dans SYSTEM.INI, celles relevant de l'utilisateur dans USER.INI. Par exemple, tout ce qui touchait au matériel installé et à la configuration du réseau se trouvait dans SYSTEM.INI, tandis que les préférences quant à l'aspect du bureau étaient stockées dans WIN.INI. Vous aviez d'ailleurs bien d'autres fichiers d'extension .INI, créés par la plupart des programmes installés sur votre ordinateur.
Cette méthode fonctionnait de façon tout à fait satisfaisante. En fait, vous avez probablement appris des astuces qui impliquaient de modifier le contenu de fichiers .INI. Pour autant, il existait tout de même certains inconvénients :

- Repérer l'entrée exacte dans le fichier INI et lui affecter la bonne valeur était une tâche difficile pour la plupart des utilisateurs.
- Les fichiers .INI étaient mal organisés.
- Ils ne supportaient pas les configurations utilisateur multiples.
- Ils ne supportaient pas les configurations matérielles multiples : Windows 3.x était donc incapable de supporter la technologie dite du Plug and Play, ou encore le "hot-docking" (action consistant à insérer ou à retirer un portable de sa station d'accueil sans qu'il soit nécessaire de l'éteindre).
- La plupart des programmes écrivaient leurs paramètres dans des fichiers .INI privés, ce qui rendait difficile le partage des informations entre les applications (technologie OLE).

Ci-dessous les 5 clés qui la composent la base de registre :

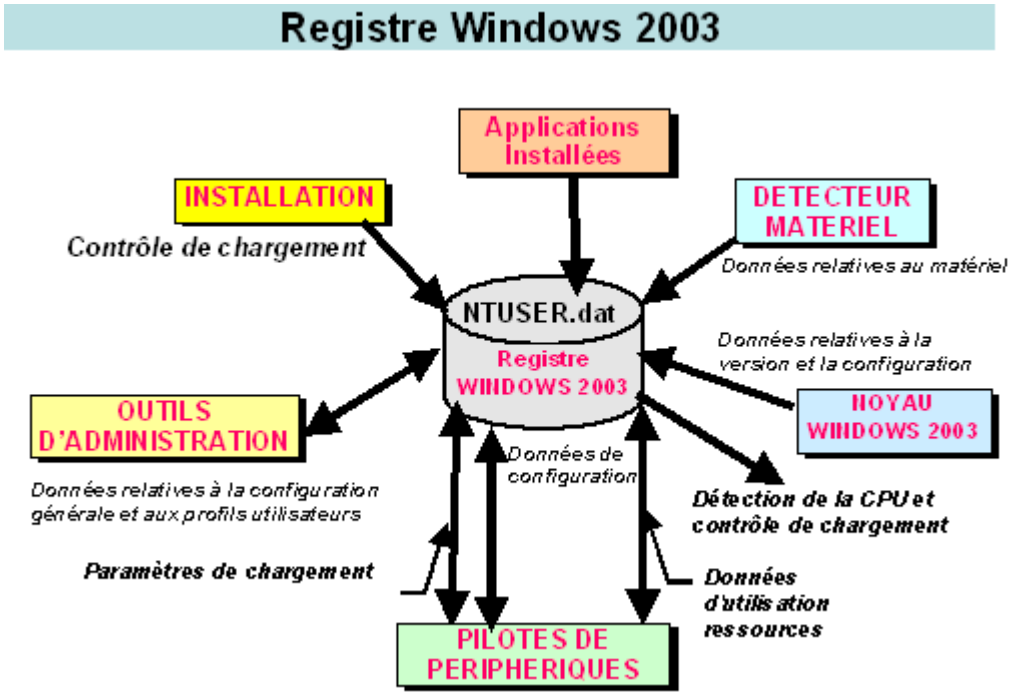


Ruche du registre	Nom de fichier
HKEY_LOCAL_MACHINE**SAM**	SAM, SAM.LOG, SAM .SAV
HKEY_LOCAL_MACHINE**SECURITY**	SECURITY, SECURITY.LOG, SECURITY.SAV
HKEY_LOCAL_MACHINE **SOFTWARE**	SOFTWARE, SOFTWARE.LOG, SOFTWARE.SAV
HKEY_LOCAL_MACHINE\SYSTEM	SYSTEM, SYSTEM.LOG, SYSTEM.SAV, SYSTEM.ALT
HKEY_USER\DEFAULT	DEFAUT, DEFAUT.LOG, DEFAUT.SAV
HKEY_CURRENT_USER	NTUSER.DAT, NTUSER.DAT.LOG

Tous ces fichiers sont dans **WINNT\SYSTEM32\CONFIG.** Les fichiers sans extension renferment une copie de la ruche. Les fichiers qui ont une extension .**LOG** renferment un journal des transactions de modifications apportées aux clés et aux valeurs d'entrées de ruche. Les fichiers qui ont une extension .**SAV** renferment des copies de fichiers de ruche tels qu'ils apparaissent en mode texte. Les fichiers qui ont une extension .**ALT** renferment une copie de sauvegarde de la ruche.

3.1.2- Installation

Le programme d'installation ajoute de nouvelles données de configuration lors de son exécution ou lors d'installation d'applications ou de matériel.



3.1.3- Détecteur de matériel

Lorsque vous démarrez l'ordinateur, le détecteur de matériel place des données de configuration dans le registre. Ces informations incluent la liste des matériels détectés dans votre système. Sur les x86 d'INTEL c'est le programme **NTDETECT.COM** qui s'en charge avec le noyau **NTOSKRNL.EXE**.

3.1.4- Noyau Windows 2003

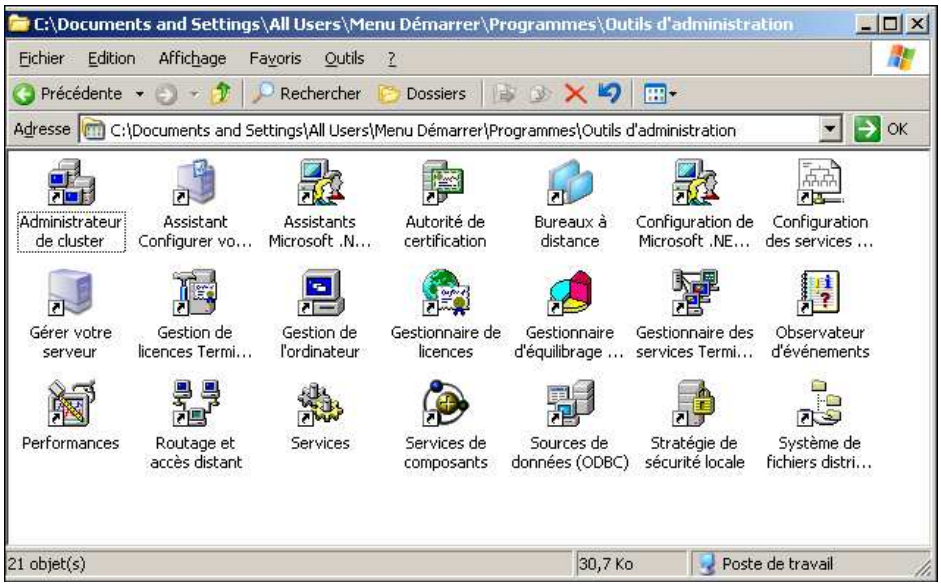
Lors du démarrage du système, **NTOSKRNL** extrait les informations du registre, par exemple les pilotes de périphériques à charger ainsi que l'ordre de chargement à respecter. Il prend aussi des informations telles que le numéro de version du noyau de WINDOWS 2003.

3.1.5- Pilotes de périphériques

Les pilotes de périphériques échangent les paramètres de chargement et les données de configuration stockés dans le registre. Il s'agit des mêmes données que celles figurant dans les lignes DEVICE= du fichier CONFIG.SYS. Tout pilote de périphérique doit indiquer les ressources système qu'il utilise, comme les interruptions matérielles et les canaux de DMA. Ces indications sont ajoutées au registre afin de fournir aux utilisateurs des programmes d'installation et de configuration intelligents.

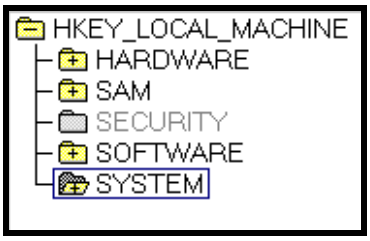
3.2- Outils administratifs

Les outils administratifs du menu **Démarrer** - **Outils d'administration** et le **Panneau de configuration** servent à modifier les données de configuration donc le registre. L'éditeur de registre est utile pour visualiser et apporter des modifications minimes à la configuration du système. Vous pouvez également vous servir de **WINMSD.EXE**. Il s'agit d'un outil de diagnostic qui s'utilise pour voir les informations conservées dans le registre.



3.3- Structure du registre

Le registre est structuré en un ensemble de cinq arborescences de clé, contenant les bases de données requises pour chaque ordinateur et chaque utilisateur du système.



3.3.1- HKEY_LOCAL_MACHINE

Contient les données de configuration requises pour l'ordinateur local.
HARDWARE
Cette sous-clé Hardware n'est pas une ruche ! C'est en fait une clé volatile (stockée en mémoire vive) construite à partir des informations matérielles détectées à l'amorçage du système par NTDETECT.COM. Cette base de données contient les informations sur les composants matériels de l'ordinateur, la manière dont les pilotes de périphériques s'en servent, ainsi que les données de mappage et celles reliant les pilotes en mode noyau.
Toutes les données de cette sous arborescence sont recréées à chaque démarrage.

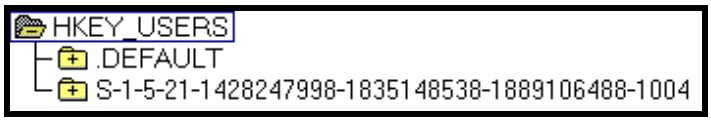
SAM (Security Account Manager)
Elle contient les informations de sécurité concernant les comptes utilisateurs ou de groupes d'utilisateurs et les domaines. Fichiers associés : sam, sam.log.

SECURITY
Elle contient les mesures de sécurité locales, comme les droits spéciaux des utilisateurs. Cette clé sert uniquement au sous-système de sécurité. Fichiers associés : security, security.log.

SOFTWARE
Elle contient les données relatives aux logiciels installés, ainsi que des paramètres de configuration. Fichiers associés : software, software.log.

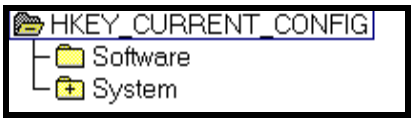
SYSTEM
Elle contient les commandes de démarrage du système, le chargement des pilotes de périphériques, les services et le comportement du système d'exploitation. Fichiers associés : system, system.alt, system.log.

3.3.2- HKEY_USERS



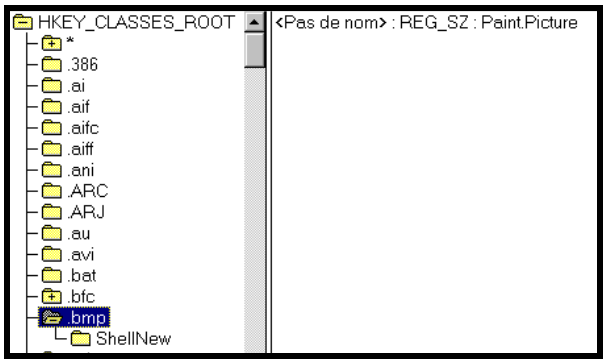
Cette clé renferme tous les profils utilisateurs activement chargés y compris le profil de l'utilisateur en cours qui est aussi dans la clé HKEY_CURRENT_USER et le profil par défaut.

3.3.3- HKEY_CURRENT_USER



Est identique à l'arborescence à partir de HKEY_LOCAl_MACHINE/System/CurrentControlSet /Hardware Profiles/xxxx/. Cette clé renferme le profil d'utilisateur qui a ouvert une session

3.3.4- HKEY_CLASSES_ROOT



Cette clé comporte :

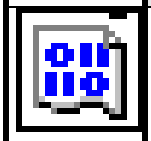
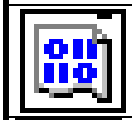
- Les associations entre applications et types de fichiers.
- Les informations d'enregistrement **OLE.**

Chaque clé est divisée en sous clés elles mêmes peuvent contenir d'autres sous clés. Les entrées de valeur dans une sous clé comporte trois parties.

- Le nom.
- Le type de données.
- La valeur.

3.4- Les types de données

Les types de données dans une sous clé peuvent être :

	Types de données	Description
	**REG_BINARY**	Données binaires brutes. La plupart des informations des composants matériels sont stockées en données binaires et peuvent être affichées dans l'éditeur du registre sous un format hexadécimal.
	**REG_WORD**	Données représentées par un nombre de 4 octets. Les paramètres de services, et des pilotes de périphériques peuvent être de ce type.
	**REG_EXPAND_SZ**	Chaînes de données extensibles qui sont un texte comportant une variable à remplacer lors de son appel par une application. Exemple : **File : REG_EXPAND_SZ : %racine-system%\ file.exe**. %racine-system% sera remplacé par le nom du répertoire où est installé WINDOWS 2003.
	**REG_MULTI_SZ**	Chaîne comportant des listes ou des valeurs multiples en format texte lisible. Les entrées sont séparées par des caractères NULL.
	**REG_SZ**	Séquence de caractères représentant un texte humainement lisible. Donc le registre n'est pas forcément humainement compréhensible.

REGEDT32
Vous pouvez utiliser l'**Editeur du Registre** pour afficher les rubriques du registre relatives aux divers composants de Windows 2003, ainsi que pour modifier ou ajouter des rubriques de registre.
Attention : pour apporter des modifications à la configuration du système, il est préférable d'utiliser le **Panneau de configuration** ou les applications du dossier **Outils d'administration (Communs).** Vous risquez dans le cas contraire d'endommager ou de désactiver Windows 2003.
L'application **Editeur du Registre** (Regedt32.exe) n'apparaît dans aucun dossier par défaut. Elle est automatiquement installée dans votre dossier **%SystemRoot%\system32**. Cliquez dans le menu **Démarrer** sur **Exécuter** ou passez à une invite de commandes et tapez **Regedt32**.

Fichiers associés .REG
Ce sont des fichiers qui permettent de sauvegarder, restaurer ou modifier le contenu des clés ou valeur du registre. Ils nécessitent les droits Administrateur ou équivalent
Un double clic sur un fichier .REG permet de mettre à jour **(Fusionner)** le registre avec les valeurs, clés et données qu'il contient.
☞ Il existe la possibilité d'importer ou d'exporter le registre en entier, des branches ou ruches.

Par défaut l'action qui est associée aux fichiers .REG est **Fusionner**. Cela peut être dangereux car dès que vous réalisez un double clic sur un fichier .REG, une modification automatique est réalisée dans le registre (clés, ruches, valeurs…). Alors attention.
La fusion des fichiers de type .REG avec le registre est une méthode pour ajouter ou modifier des valeurs ou clés mais elle n'en supprime pas.

handsafe.reg - Bloc-notes

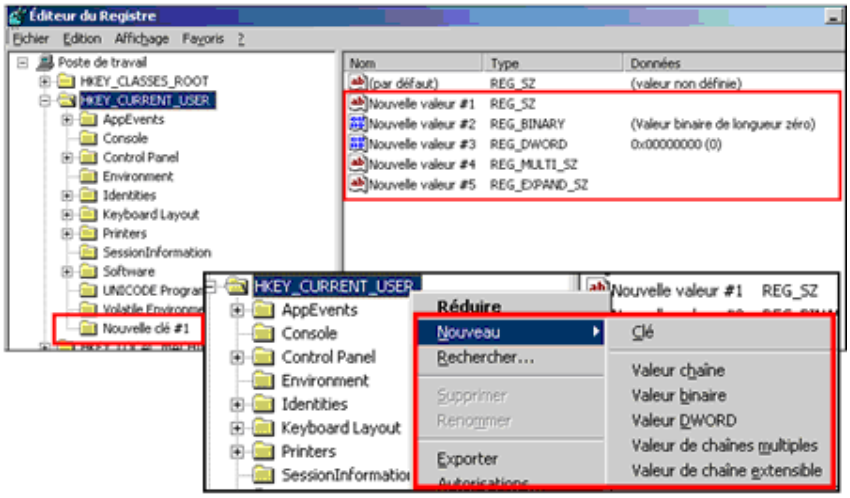
Fichier Edition Format Affichage ?

```
REGEDIT4

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\DataFactory]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\DataFactory\HandlerInfo]
"handlerRequired"=dword:00000001
"DefaultHandler"="MSDFMAP.Handler"

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\DataFactory\HandlerInfo\safeHandlerList]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\DataFactory\HandlerInfo\safeHandlerList\MSDFM

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\DataFactory\HandlerInfo\safeHandlerList\MSDFM

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\DataFactory\HandlerInfo\safeHandlerList\MSDFM
```

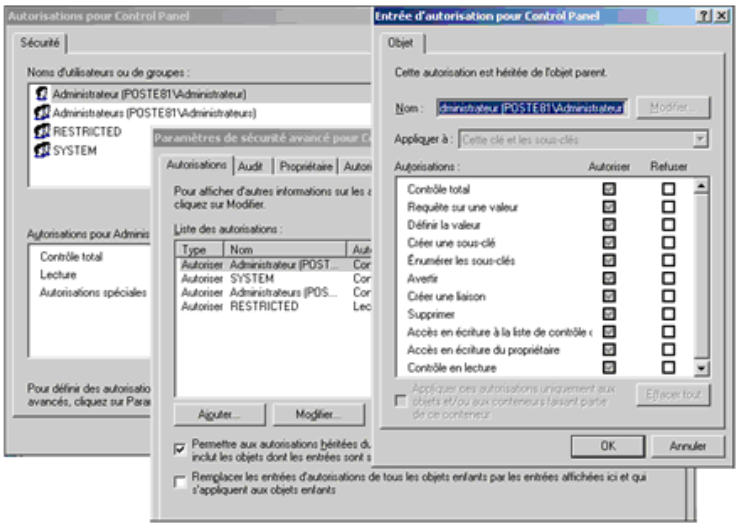
Edition du contenu du registre

Vous pouvez créer à tout instant des nouvelles clés et entrer des nouvelles valeurs. Par contre réalisez des sauvegardes ou exportation de votre registre ou des branches concernées.

Dés que vous exécutez **REGEDIT**, l'ensemble du registre local sera chargé. Il vous est possible de ne charger qu'une ruche spécifique à partir d'un fichier et/ou vous connecter à distance au registre d'une autre machine (uniquement aux branches **HKEY_LOCAL_MACHINE** et **HKEY_USERS** et en ayant les droits administrateurs ou équivalents).

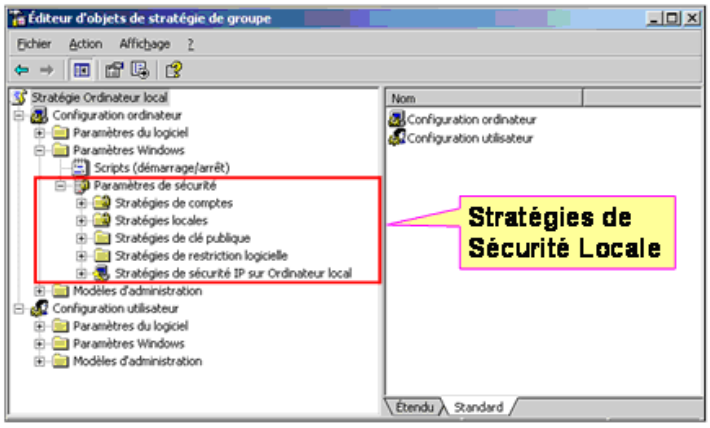


A l'aide du menu **Edition** – **Autorisation** vous pouvez définir la sécurité d'accès au registre.

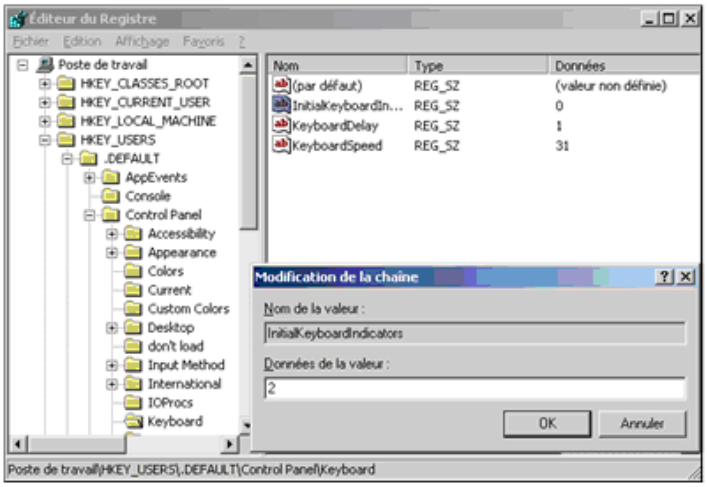


Modification du registre via la stratégie de groupe local (Local GPO)

Il existe une méthode de modification indirecte d'une partie du registre, déjà mise en pratique sous W2000, grâce à l'objet local de stratégie de groupe local (Local GPO). Nous étudierons sa mise en œuvre plus loin dans ce cours.

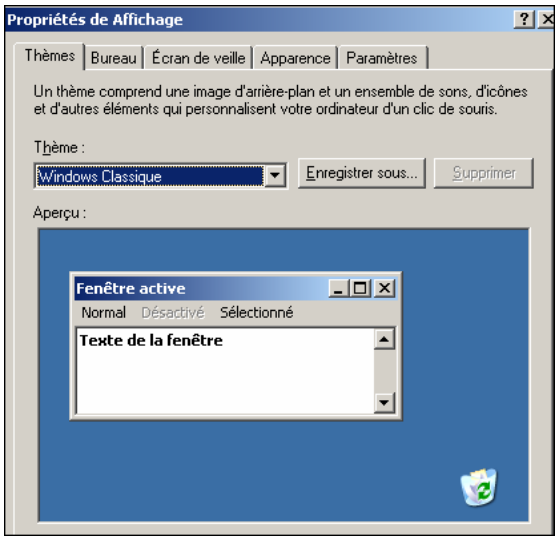


Exemple pratique de modification du registre : verrouillage du pavé numérique au démarrage



3.5- Configurer le système et gestion de l'environnement de travail

3.5.1- Affichage

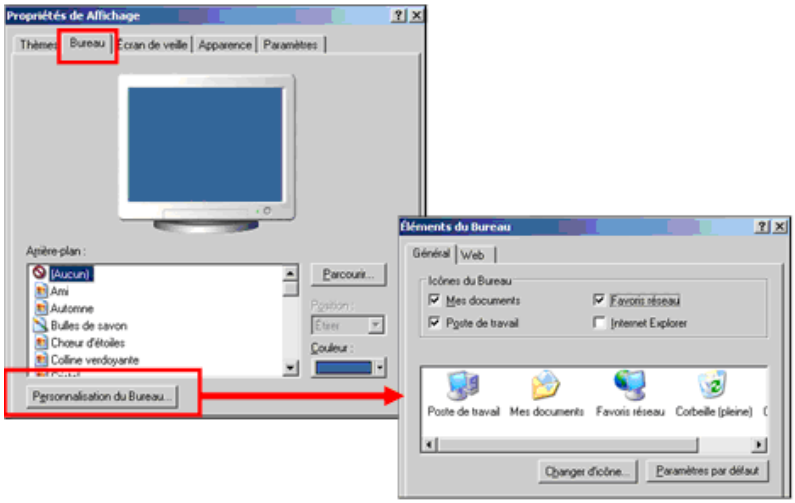


Onglet Thèmes

Il vous permet de choisir les thèmes de Bureau afin de lui donner une apparence générale. Cette apparence fixe la visualisation des icônes, des polices, des images d'arrières plans… Vous pouvez modifier un thème prédéfini en modifiant individuellement les éléments puis l'enregistrer avec **Enregistrer sous**, afin d'en faire un thème personnalisé. Par défaut vous utilisez le thème Windows Standard. Mais vous pouvez aussi en télécharger sur Internet.

Onglet Bureau

Cet onglet vous permet de personnaliser votre Bureau en choisissant une image au format BMP, JPEG ou GIF.

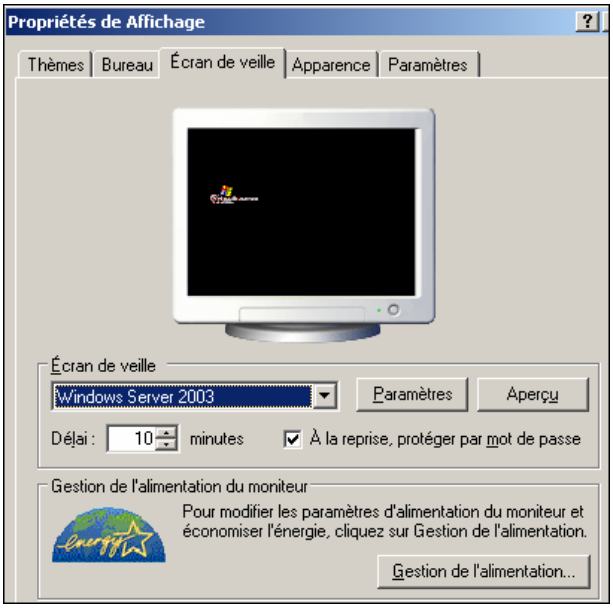


Avec le bouton **Parcourir** vous pouvez importer une image personnalisée, tel vos souvenirs de vacances.

Vous pouvez choisir la position de l'image (centrer, étirer ou afficher en mosaïque). Vous pouvez aussi définir la couleur du fond de Bureau.

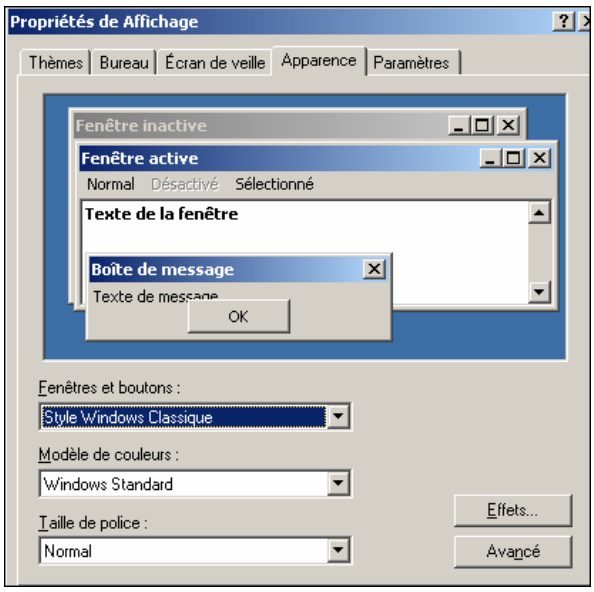
Avec le bouton **Personnalisation du Bureau**, vous ouvrez une fenêtre à deux onglets afin de sélectionner les icônes qui seront présents sur votre Bureau ou bien afficher une page Web au format HTML.

Onglet Ecran de Veille



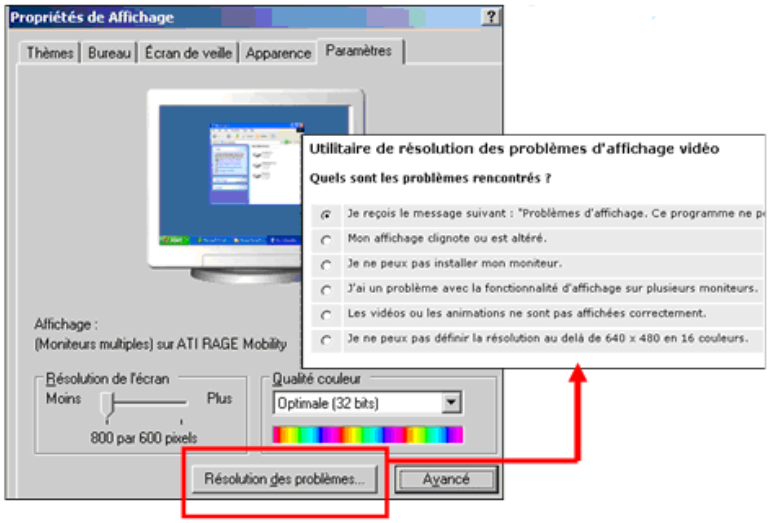
Vous pouvez choisir des économiseurs d'écran variés dont le but est d'animer une image sur l'écran du moniteur afin d'éviter que la couche de phosphore ne soit marquée par une image fixe.
La plupart des écrans de veille sont paramétrables avec la possibilité d'entrer des mots de passe. Vous pouvez indiquer le nombre de minutes avant leur mise en service.
Le bouton **Gestion de l'alimentation** vous permet d'aller directement à la fenêtre de gestion d'économie d'énergie du moniteur. Nous l'étudierons plus loin dans ce cours.

Onglet Apparence

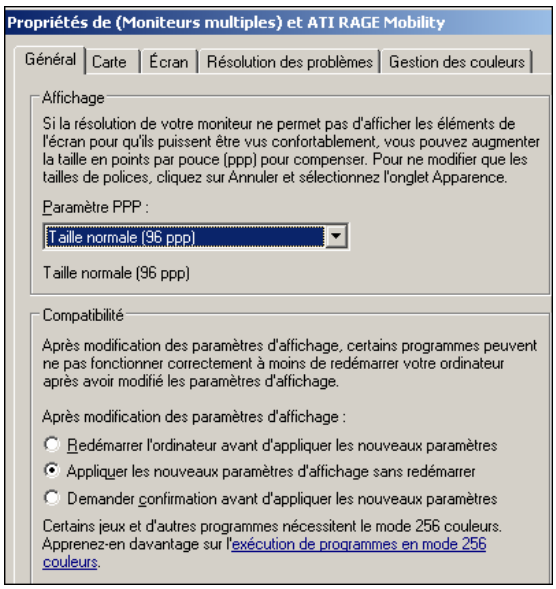


Cette fenêtre vous permet de personnaliser les modèles de couleurs et taille des polices des menus, barres de titres, boites de dialogues. A l'aide du bouton **Avancé** vous pouvez valider des effets visuels pour les transitions des menus et le lissage des polices.

Onglet Paramètres



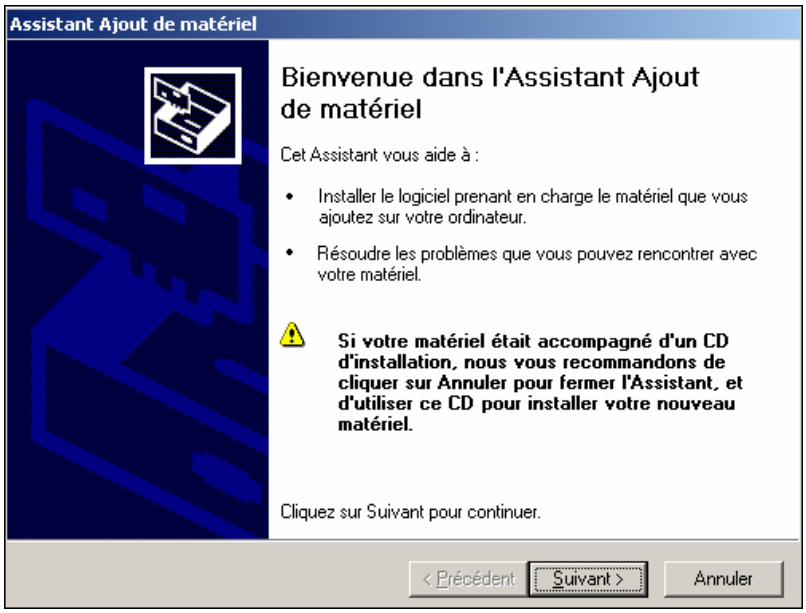
Vous consulterez très souvent cet écran afin de régler le nombre de couleurs et la résolution de votre écran. Le bouton **Résolution des problèmes** vous permet de démarrer **l'Assistant de diagnostic**, contenu dans le **Centre d'aide et de support** afin de vous aider interactivement à résoudre vos problèmes.
Le bouton **Avancé** vous permet à l'aide des différents onglets (Général, Carte, Ecran, Résolutions de problèmes et Gestion des couleurs) d'affiner vos réglages.



Comme avec W2000 et XP, W2003 offre la possibilité de connecter plusieurs écrans (10 au maximum) sur un même micro. Cela permet de travailler sur plusieurs applications en même temps en les déplaçant d'écran en écran. Pour cela vous devez avoir des cartes au format PCI ou AGP reconnues par le système d'exploitation (voir la HCL). Si c'est le cas elles seront détectées automatiquement au redémarrage de votre micro.

3.5.2- Ajout de matériel

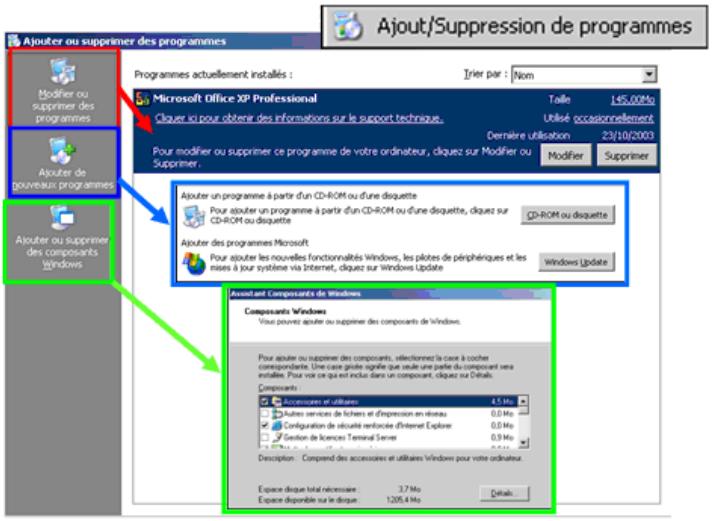
Cette fonctionnalité concerne surtout les périphériques non Plug-and-Play et non détectés par le système au démarrage.
A chaque fois que vous lancez ce programme, l'assistant **Ajout matériel** vous guide dans votre action à tout instant.
Nota : il est impossible de supprimer un périphérique PnP, car la réinstallation est automatique par le système. La solution est de le retirer physiquement ou activer la fonction **DESACTIVER** dans les propriétés du pilote.



3.5.3- Ajout/suppression de programmes

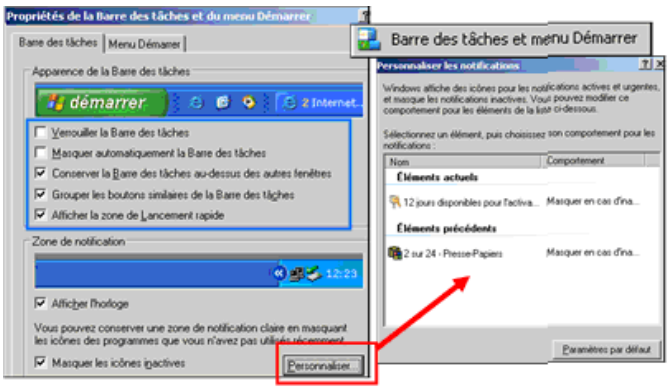
Cet assistant va vous permettre d'installer des applications, des composants Windows, des programmes, des jeux... Dans l'hypothèse où vous souhaitez déployer des applications par la méthode de publication, les utilisateurs pourront consulter les applications que vous aurez décidé de publier avant de décider de les installer. Nous étudierons cette technique plus loin dans le cours.
Trois boutons sont disponibles dans la fenêtre principale.

- **Modifier ou supprimer des programmes :** comme son nom l'indique, cette option permet de réinstaller, supprimer ou ajouter des composants d'une application.
- **Ajouter de nouveaux programmes :** cette option permet d'installer des composants ne faisant pas directement partie de Windows. Vous pouvez installer ces programmes à partir d'un support externe (CD-ROM, disquette...) ou à partir du site Microsoft, via Windows Update.
- **Ajouter ou supprimer des composants Windows** : cette option permet d'ajouter ou de retirer des composants intégrés de Windows.



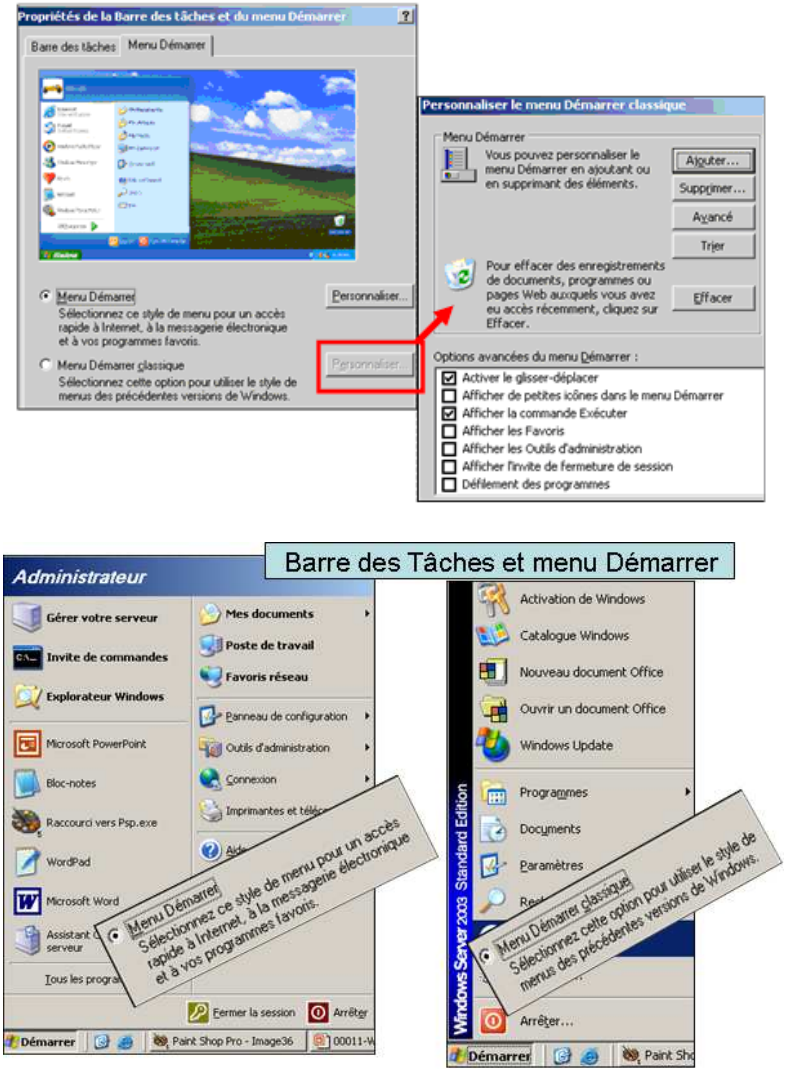
3.5.4- Barre des tâches et menu Démarrer

Avec cet outil vous allez personnaliser la barre des tâches, l'apparence et les actions du menu **Démarrer**. Vous pouvez paramétrer à partir de l'onglet **Barre des tâches** son verrouillage, son masquage automatique, sa position (son maintien au-dessus des autres fenêtres afin qu'elle ne soit pas masquée par les applications), le groupement de boutons similaires de la Barre des tâches pour conserver un maximum de place dans la zone des applications et des programmes, et l'affichage de la zone de lancement rapide (utile pour exécution d'une application par simple clic).Vous pouvez aussi décider ou non de l'affichage de l'horloge (heure, jour et date) dans le bas à droite de votre Barre des tâches. Avec le bouton **Personnaliser** vous ouvrez une fenêtre dont le contenu représente l'historique des applications qui ont échoué à certains instants de leur exécution.



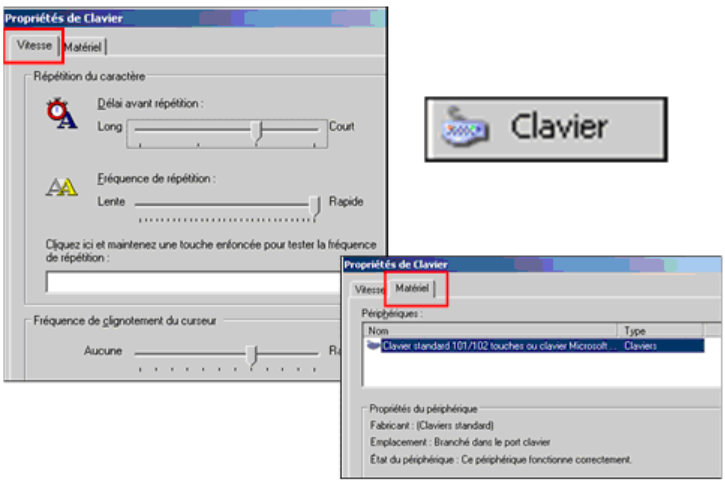
Onglet Menu Démarrer

Il permet soit d'utiliser un menu démarrer de type Windows XP ou un menu démarrer de type classique style W2000. A vous de choisir… Voyez le résultat ci-dessous.



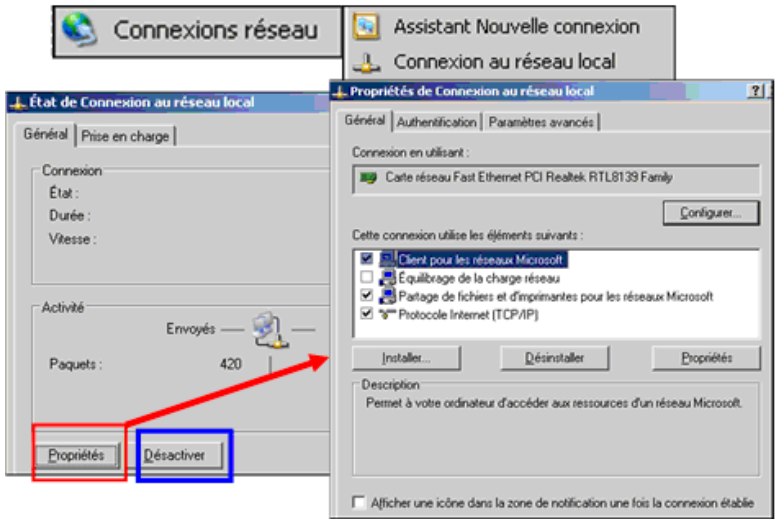
3.5.5- Clavier

Ce programme permet de paramétrer le clavier comme le délai, la fréquence de répétition, le clignotement du curseur. A partir de l'onglet **Matériel** vous accédez aux **Propriétés** du driver qui gère votre clavier.



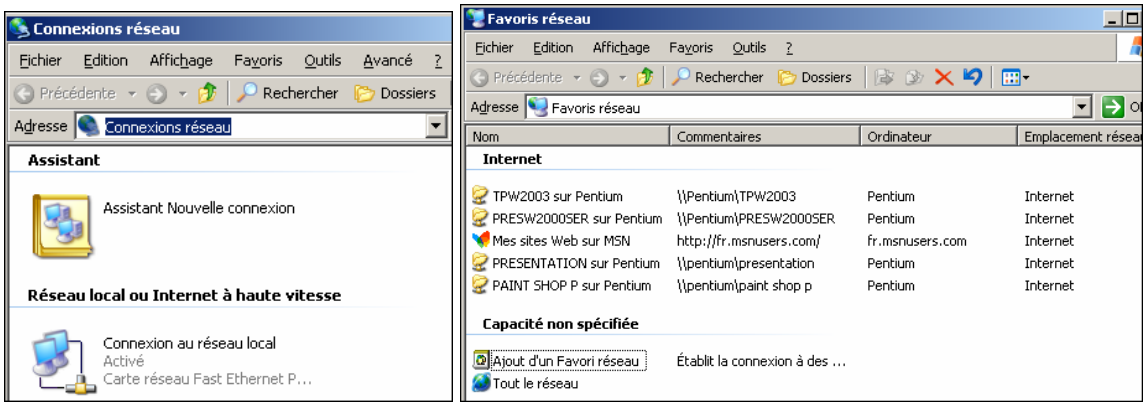
3.5.6- Connexions réseau

Ce programme vous sera très utile car à partir de cette fenêtre vous visualisez et configurez toutes les connexions réseau. Ces connexions réseau peuvent être locales ou distantes. Vous avez un icône **Assistant Nouvelle Connexion** qui vous aide en pas à pas pour installer une connexion distante d'accès entrante ou sortante (Directe, RNIS, VLAN, RTC…). Nous étudierons en détail ces fonctionnalités dans le chapitre Réseau.
Le bouton **Propriétés** permet de paramétrer tous les éléments réseau de votre connexion (cartes, protocoles, services, authentification…). Vous pouvez aussi à partir de cette fenêtre **Désactiver** votre carte réseau sans pour cela la retirer de votre machine.



3.5.7- Favoris réseau

Cette fenêtre permet à tout instant de parcourir le réseau et de visualiser toutes les ressources partagées.

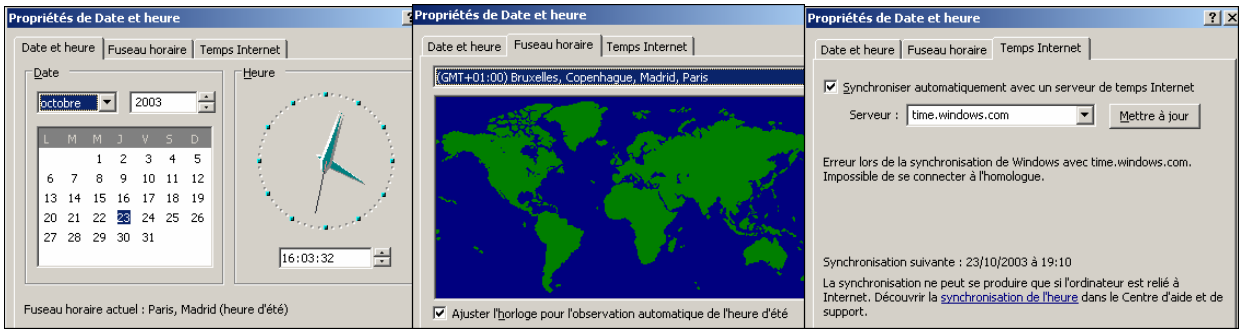


3.5.8- Contrôleurs de jeu

Utilisé pour gérer des manettes de jeu. On peut trouver bizarre de voir cette option sur un serveur W20003. Par contre Microsoft n'a pas mis à disposition en standard les jeux dans les composants Windows Server 2003.

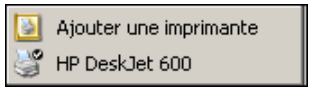
3.5.9- Date et heure

Vous pouvez avec cette option régler la date, l'heure et les fuseaux horaires. L'onglet **Temps Internet** permet de synchroniser le serveur sur une référence Temps à partir d'une adresse Internet.



3.5.10- Imprimante et télécopieurs

Avec cette option vous pouvez ajouter ou supprimer une imprimante ou un télécopieur. Vous pouvez aussi visualiser les paramètres de votre imprimante et les modifier (papier, ruban, format, partage...).

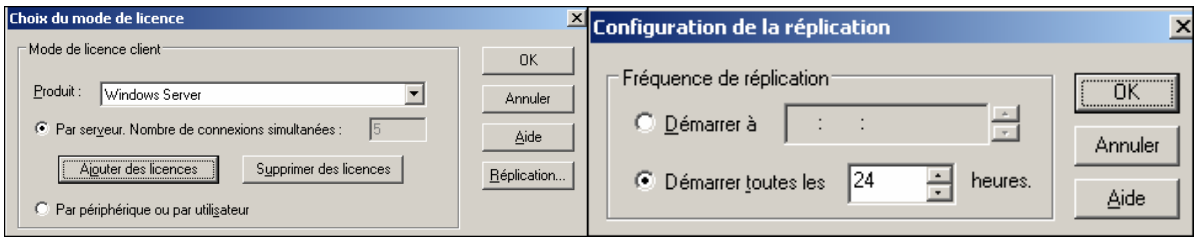


3.5.11- Licence

Avec cet icône vous allez pouvoir gérer vos licences d'utilisation, en accord avec les contrats Microsoft. Il existe deux modes de gestion des licences et de leur comptabilisation.

Par serveur
C'est le mode par défaut. Il indique un nombre de licences par serveur autorisant une quantité équivalente de connexions simultanées aux ressources du serveur. Il correspond au nombre maximal de clients différents qui peuvent se connecter en même temps sur le serveur. Dès que le nombre maximum est atteint, le système envoie un message d'erreur au client (et dans l'**Observateur d'événements**) et la nouvelle connexion est refusée. Vous avez la possibilité d'en ajouter ou en supprimer à tout moment via les boutons **Ajouter** ou **Supprimer des licences**. Cette opération purement **Textuelle** est basée sur un rapport de confiance.

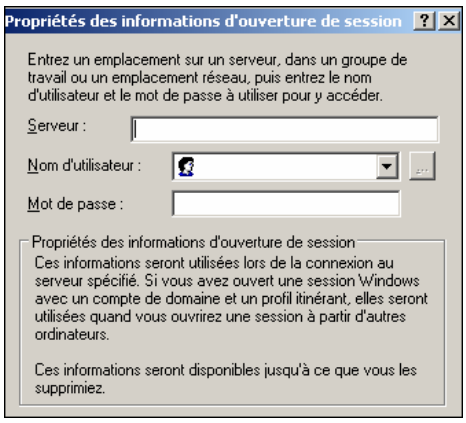
Par poste ou par utilisateur (par siège sous NT4)
Le client spécifique ou siège est concerné par une licence. Il doit posséder une **CAL** (Client Access Licence). Cette licence lui donne un droit de connexion et ne nécessite pas l'ajout d'un logiciel spécifique. Les serveurs n'ont aucune restriction particulière dans le nombre de connexions simultanées maximales dans l'hypothèse où chaque utilisateur possède une CAL reconnue.



Dans les deux cas une **Réplication** afin de contrôler et vérifier l'état des licences doit être réalisé.
Vous pouvez visualiser à tout instant l'état des licences avec le programme **Gestionnaire de licences** des **Outils d'Administration**.

3.5.12- Noms et mots de passe utilisateurs enregistrés

Permet la gestion des informations d'ouverture de session sur les ordinateurs du réseau ou sites Internet.

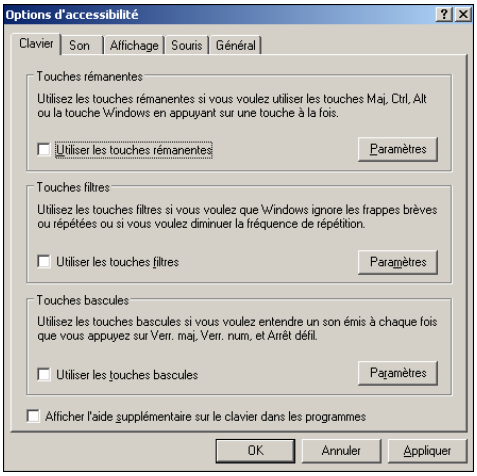


3.5.13- Options d'accessibilité

Cet icône permet de configurer les options d'accessibilité afin d'aider les personnes ayant certaines déficiences physiques (comme une mobilité réduite ou une vue déficiente) à travailler avec leur micro dans les meilleures conditions possibles.

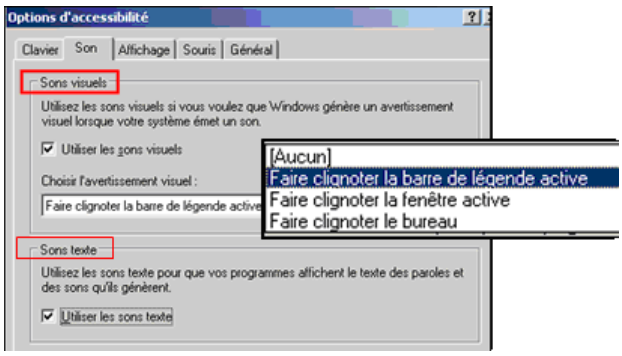
Onglet Clavier : **déficience du toucher ou déficience moteur**

- **Touches rémanentes** : permet une simulation des touches appuyées pendant quelques secondes. L'exemple le plus cocasse, c'est le traditionnel redémarrage à chaud avec Ctrl + Alt + Suppr en appui simultané. Dans ce cas si l'option est validée, il vous faut effectuer un appui successif des touches.
- **Touches Filtres** : permet d'ignorer les appuis successifs trop rapides liés à des tremblements ainsi qu'à la fréquence de répétition.
- **Touches bascules** : permet d'associer un son lorsque les touches de verrouillages changent d'état (majuscule, arrêt défilement, numérique).



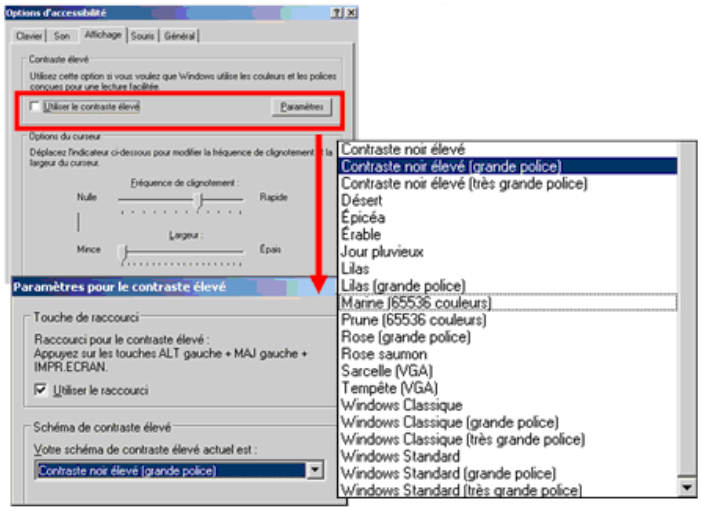
Onglet Son : déficience auditive

- **Sons visuels :** permet l'association d'un avertissement visuel comme le clignotement de la **Barre de titre ou du Bureau** lors de l'émission d'une alarme sonore par le système.
- **Sons texte :** permet d'afficher un texte ou une légende sous la forme de la traditionnelle bulle d'information lorsqu'un son est émis par une application prenant en charge cette fonctionnalité.



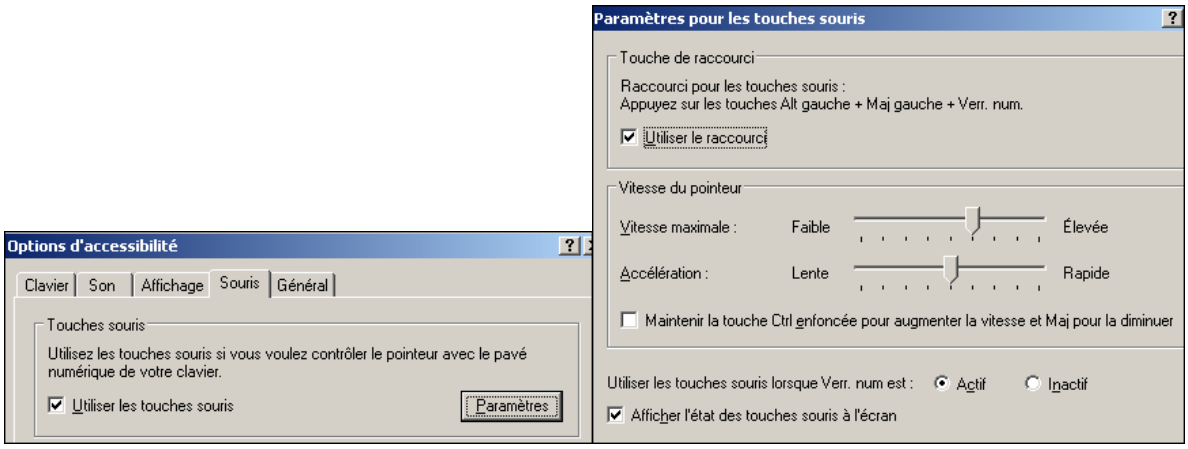
Onglet Affichage : déficience visuelle

- **Contraste élevé** : permet l'activation de thèmes prédéfinis ayant des harmonies de couleurs très nuancées associées à des tailles de polices importantes.
- **Options du curseur :** définit l'épaisseur et la fréquence de clignotement du curseur.



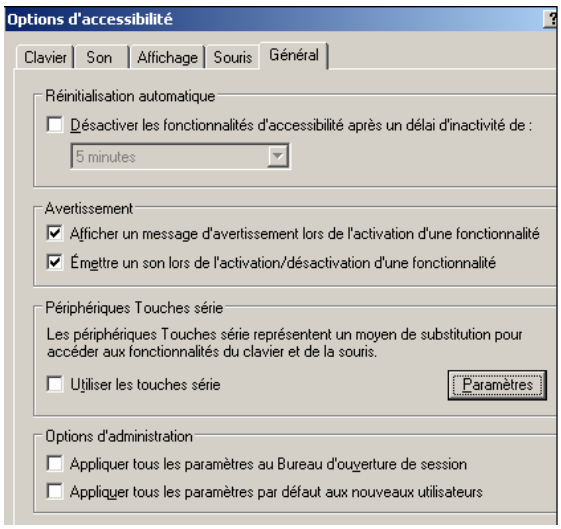
Onglet Souris

Touches souris : option permettant de simuler le déplacement de la souris à l'aide des touches du pavé numérique.

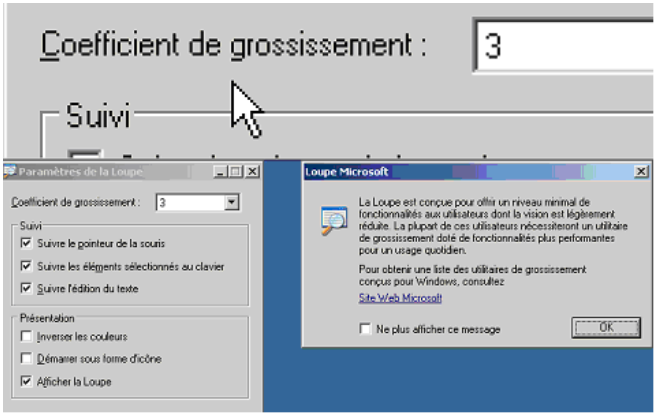


Onglet Général

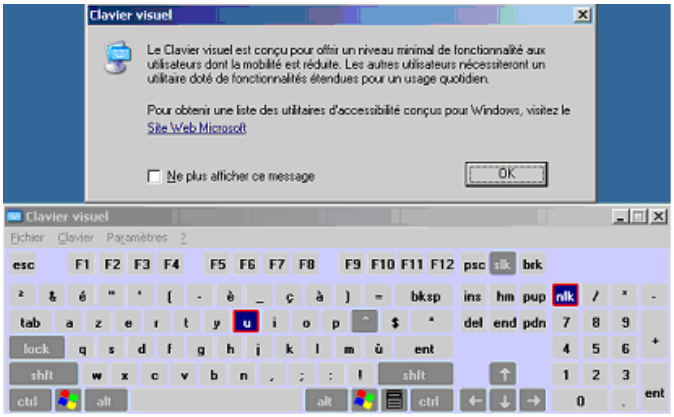
L'onglet général permet de paramétrer le comportement global des options d'accessibilité avant et pendant l'entrée en session. Vous pouvez aussi gérer l'ajout de périphériques spécialisés sur un port série dans le but de compenser des handicaps plus importants, comme un clavier en braille pour les aveugles.



Loupe : à partir **du Menu Démarrer – Accessoires – Accessibilité** vous pouvez sélectionner l'outil **Loupe** afin d'afficher un agrandissement des endroits immédiats du curseur de la souris.

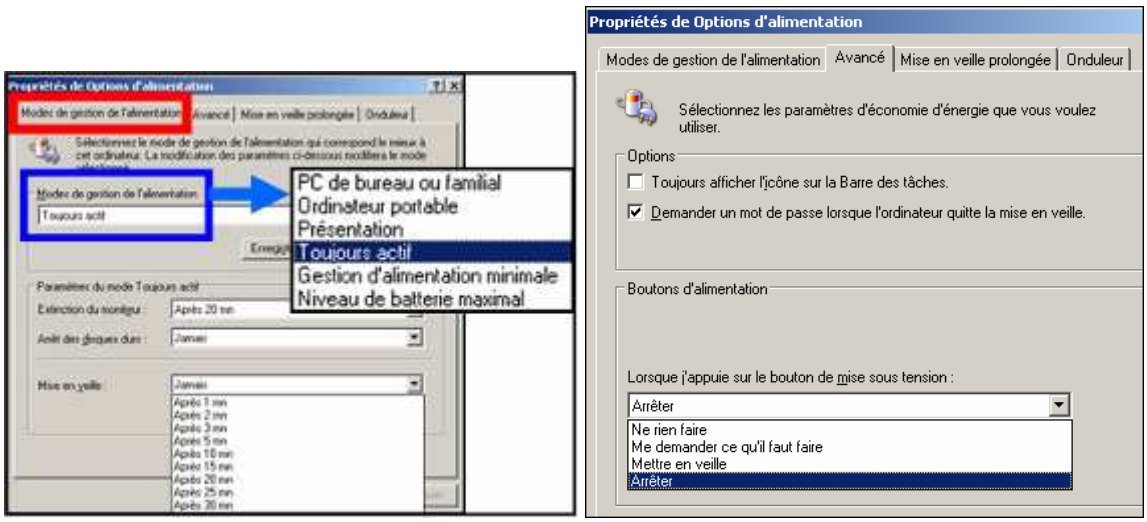


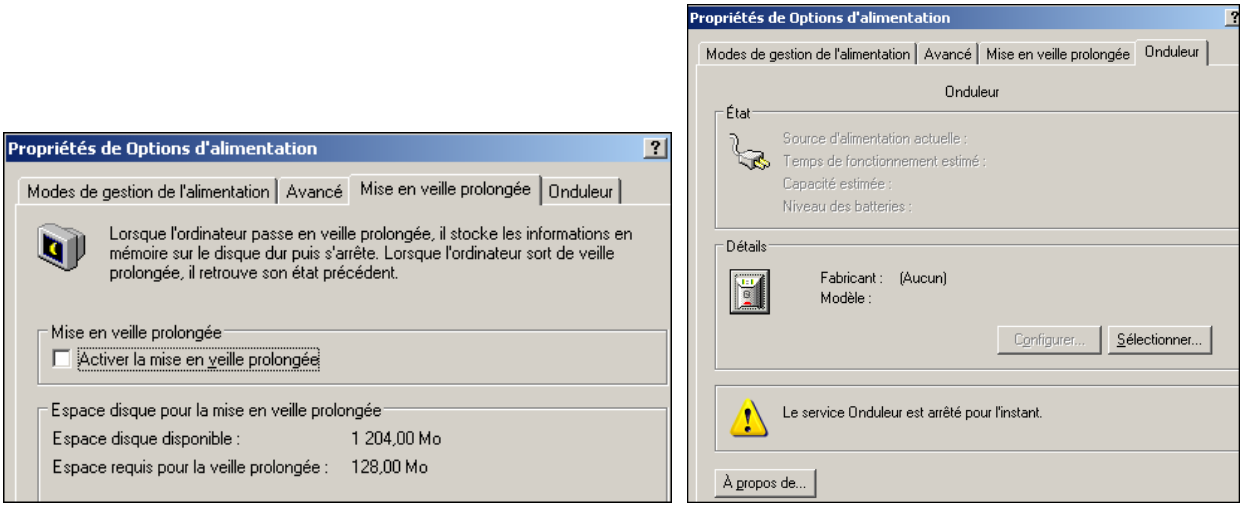
Clavier visuel : affichage d'un clavier à l'écran permettant l'appui des touches à partir de la souris.



3.5.14- Options d'alimentation

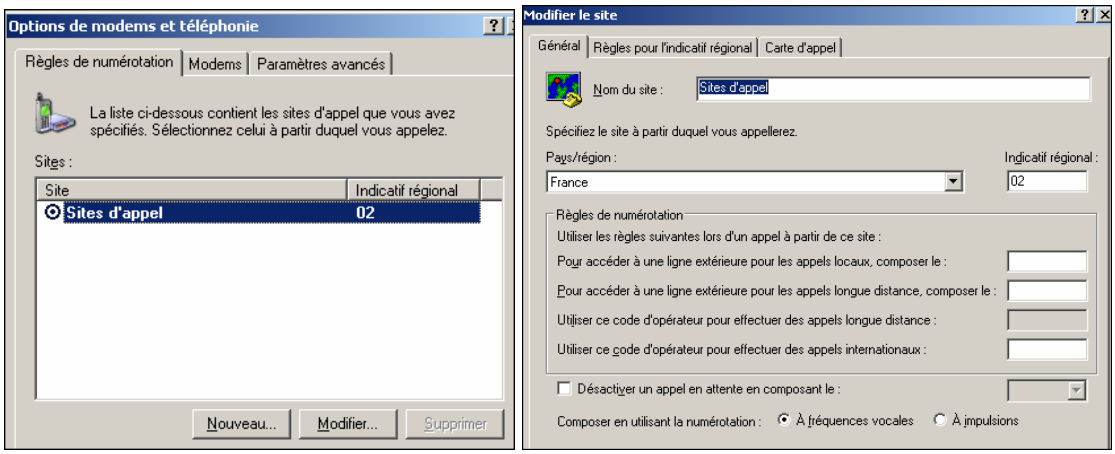
Ce module permet la réduction de la consommation d'énergie utilisée par votre micro en éteignant le moniteur et/ou les disques durs après un certain temps d'inactivité. Ces options ne sont utilisables que si votre matériel le permet.



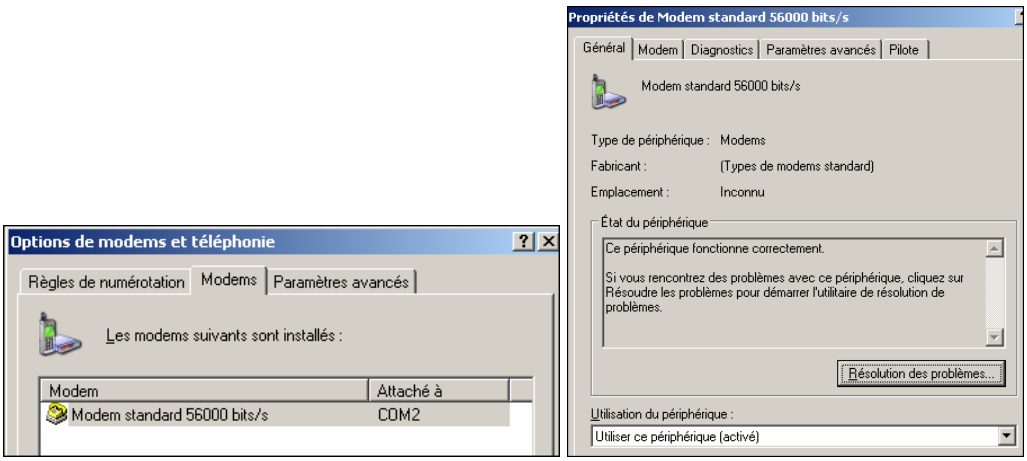


3.5.15- Options de modems et téléphonie

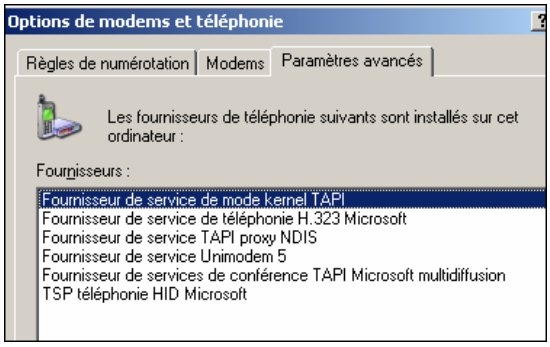
Onglet Règles de numérotation : permet de définir des réglages et propriétés de numérotation pour un lieu donné libellé **Sites d'appel**. Vous pouvez paramétrer les caractéristiques et les règles de la numérotation.



Onglets Modems : permet l'affichage des modems et dispositifs de communications présents sur votre micro. A l'aide du bouton **Propriétés** vous pouvez **Ajouter**, **supprimer** ou accéder aux **propriétés** de votre modem. Vous pouvez réaliser cette action à partir du **Gestionnaire de périphériques**.

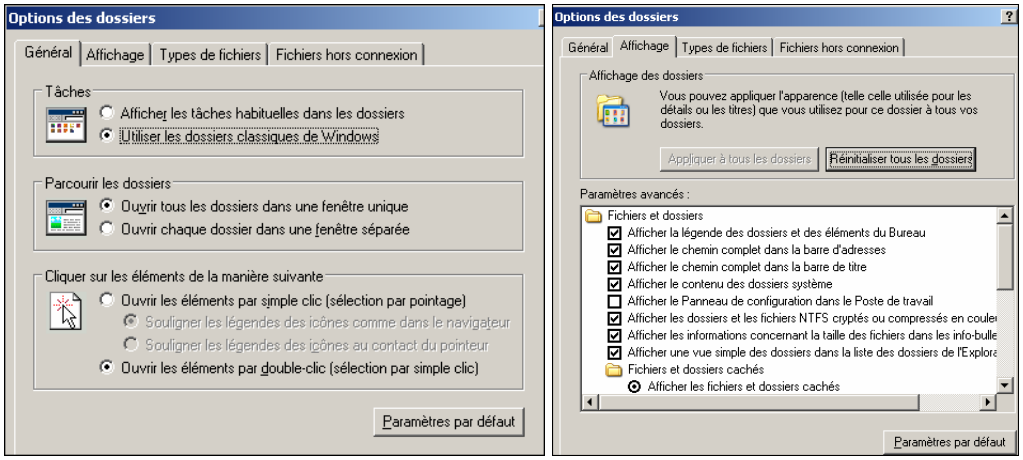


Onglet Paramètres Avancés : permet l'ajout ou la suppression de fournisseurs de services de téléphonie.

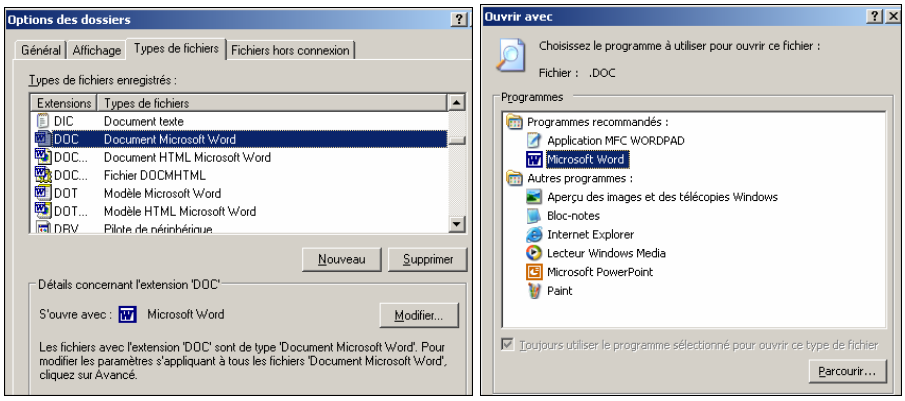


3.5.16- Options des dossiers

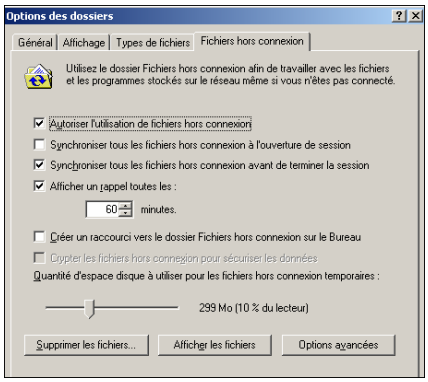
Cette option est très importante et très souvent utilisée, car elle permet de définir comment vos fenêtre seront affichées avec l'explorateur Windows. Les options sont très nombreuses afin de vous aider à paramétrer vos fichiers et dossiers. A partir de l'onglet **Général** vous pouvez valider ou non l'ouverture des dossiers et sous-dossiers dans une fenêtre unique ou séparée. En particulier c'est à partir de l'onglet **Affichage** de cette fenêtre que vous pouvez valider ou non la visualisation des fichiers cachés.



L'onglet **Type de fichiers** permet de visualiser ou modifier les associations d'extension de fichiers avec leurs programmes respectifs. Cela permet aussi de déterminer les actions attachées aux menus contextuels.

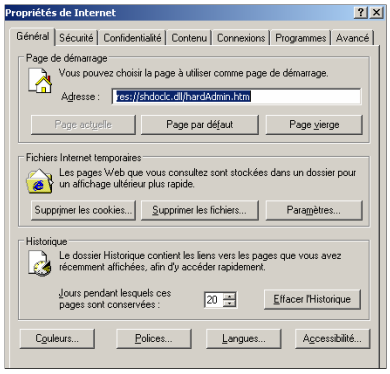


L'onglet **Fichiers hors connexion** permet d'activer l'accès aux ressources partagées en mode déconnecté du réseau.



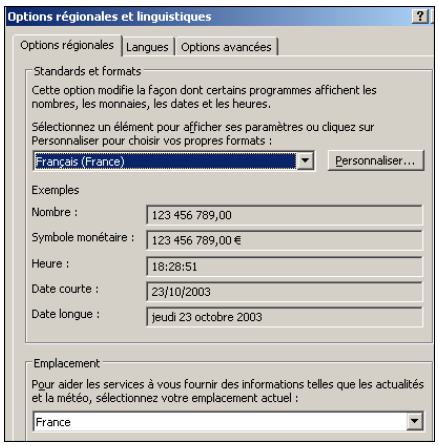
3.5.17- Options Internet

Cette option regroupe toutes les options de comportement et de paramétrage de connexion d'Internet Explorer.

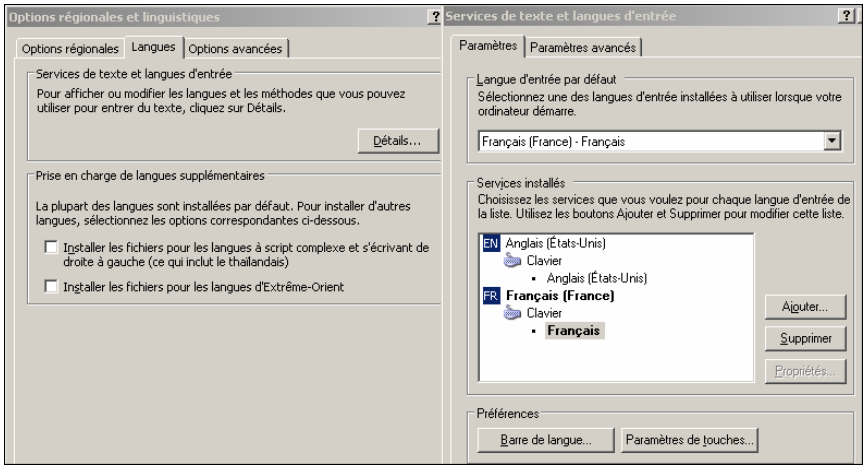


3.5.18- Options régionales et linguistiques

Cette option permet de paramétrer les formats d'affichage des nombres, dates, heures et symboles monétaires en fonction du pays. Vous pouvez aussi paramétrer les jeux de caractères utilisés. Ces réglages pouvant être associés à chaque utilisateur par défaut du poste ou spécifiques à chacun.

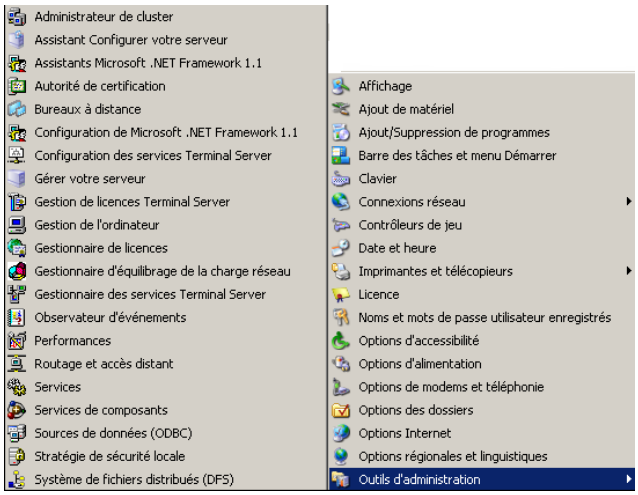


W2003 Server permet de supporter plusieurs claviers différents au niveau de l'onglet **Langues** et en cliquant sur le bouton **Détails**.



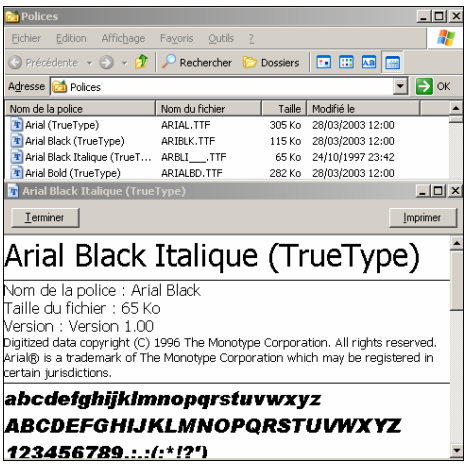
3.5.19- Outils d'administration

Cette option est une des plus importantes de la gestion d'un serveur W2003 Server. Les nombreuses options seront étudiées plus loin dans ce cours avec en particulier celles qui se réfèrent à Active Directory.



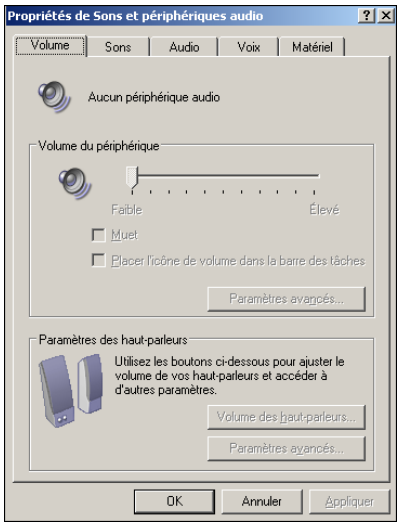
3.5.20- Polices

Cette option vous permet d'ajouter ou de supprimer des polices de caractères. En double-cliquant sur cette icône vous pouvez visualiser la liste des polices installées.



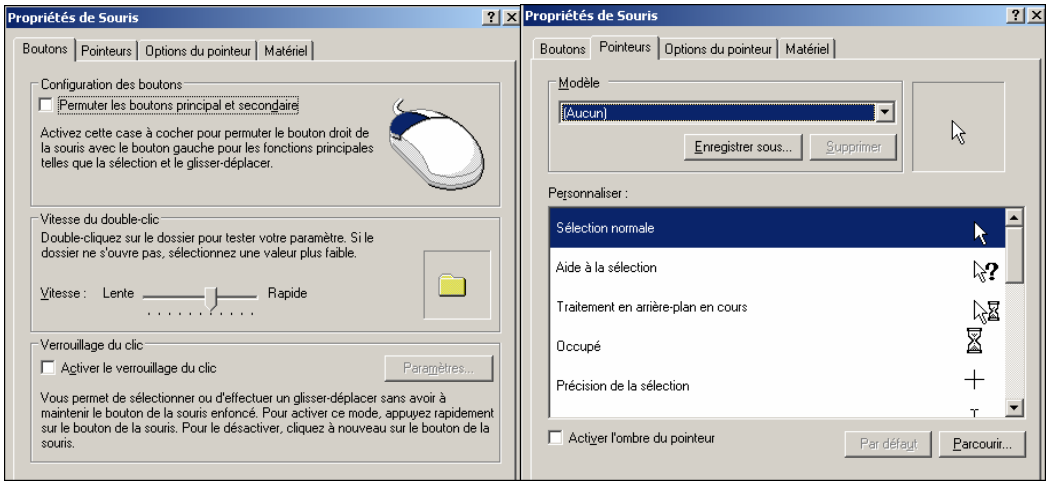
3.5.21- Sons et périphériques audio

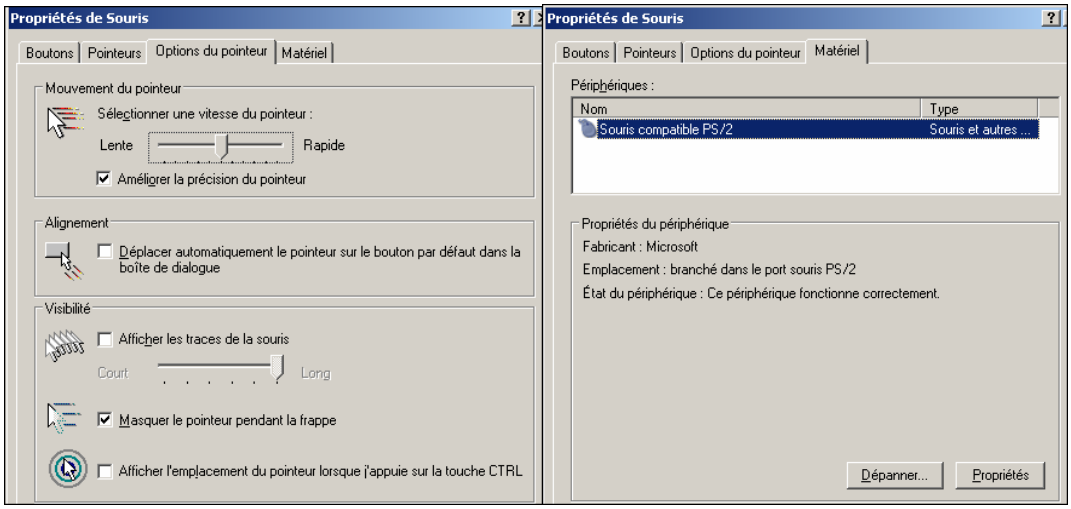
Cette option vous permet de contrôler les périphériques audio ainsi que les effets sonores. Cette option est très peu utilisée sur un serveur de type W2003 Server.



3.5.22- Souris

Cette option permet de personnaliser l'ergonomie d'utilisation de la souris. Vous pouvez régler la vitesse du double clic en indiquant si vous souhaitez configurer votre souris pour un droitier ou un gaucher en inversement les rôles des boutons. Vous pouvez aussi régler la molette de la souris ainsi que la forme des curseurs.

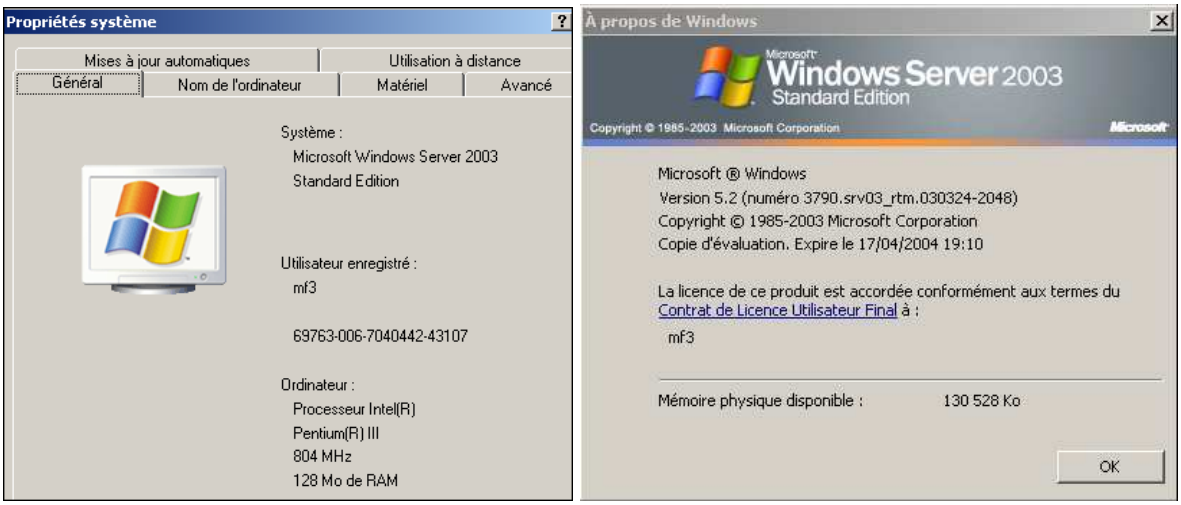




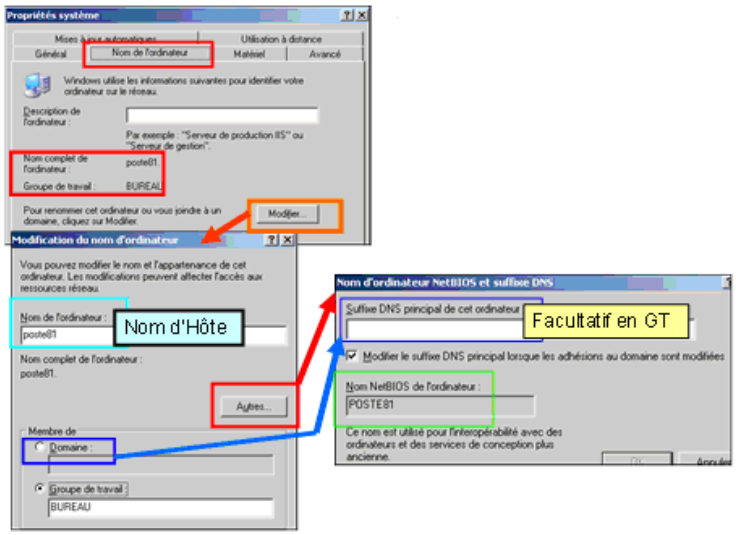
3.5.23- Système

Cette option permet d'accéder aux propriétés du système. Vous pouvez l'exécuter à partir de l'icône **Poste de travail** en activant **Propriétés** après un clic droit.

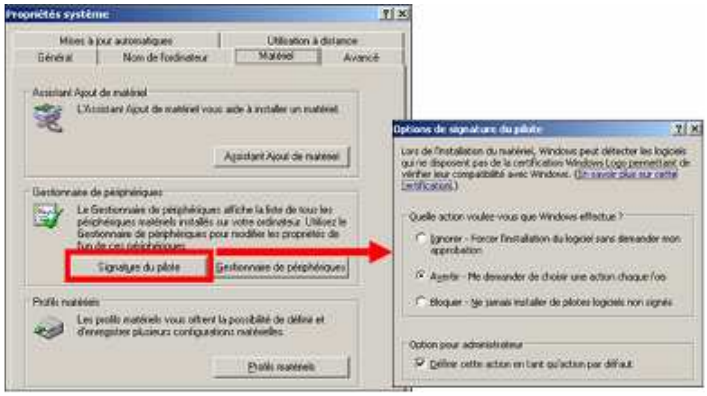
Onglet Général : il est très utile et fréquemment utilisé car il affiche les caractéristiques générales du système comme la version du système d'exploitation, et l'éventuel version du service pack installé. Il indique aussi le nom d'utilisateur et de l'entreprise possédant la licence et l'identificateur unique. Il vous donne aussi le modèle et la fréquence du processeur, ainsi que la capacité de RAM installée. Pour obtenir plus d'informations sur la version du système d'exploitation, tapez en mode commande WINVER.



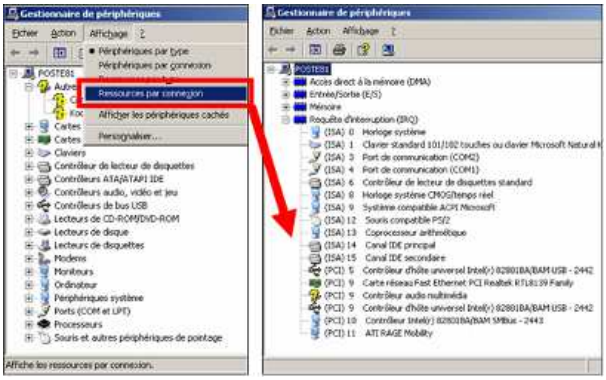
Onglet Nom de l'ordinateur : cette option vous permet de visualiser et modifier le nom de votre ordinateur. Il vous donne aussi a quel groupe de travail ou domaine il appartient. La zone description de l'ordinateur vous permet d'ajouter un commentaire afin de fournir des informations sur votre micro pour les utilisateurs du réseau. Le bouton **Modifier** permet de modifier le nom complet de votre ordinateur. Lorsque vous modifiez un élément de ces fenêtres vous devez **Redémarrer** pour que les modifications soient prises en compte.



Onglet Matériel : cet onglet vous propose de nombreuses fonctionnalités pour vous aider à gérer vos périphériques.
Assistant Ajout de matériel : vous permet comme son nom l'indique d'ajouter un matériel ou de visualiser ses propriétés ou de modifier son paramétrage.
Signature de pilote : nouveauté de W2000 et W2003 permettant de garantir que le pilote que vous installez est supporté et agréé par Microsoft. Les pilotes qui sont signés sont garantis par le WHQL (Windows Hardware Quality Labs) de Microsoft. Bien sûr vous pouvez installer un périphérique non signé mais à vos risques et périls si un dysfonctionnement apparaît. A vous de cocher une des options : Ignorer, Avertir, Bloquer.



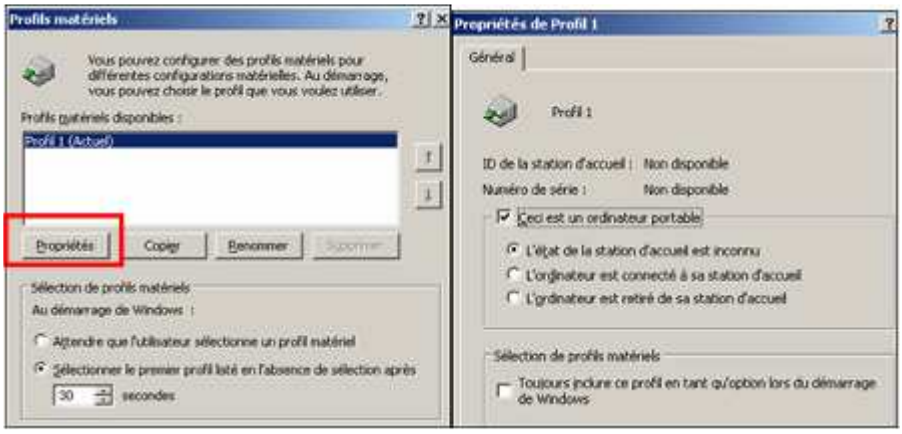
Gestion des périphériques : cette option vous permet de visualiser l'état des périphériques de votre machine, de les désactiver, désinstaller ou d'éditer et modifier leurs propriétés. Cette fenêtre est très utile en cas de problème. Vous pouvez afficher vos périphériques par connexion, par type de ressources (IRQ, DMA, I/O...). Vous pouvez aussi afficher les périphériques **cachés** afin de visualiser les périphériques **virtuels** (Beep, Ipsec, NetBios…).



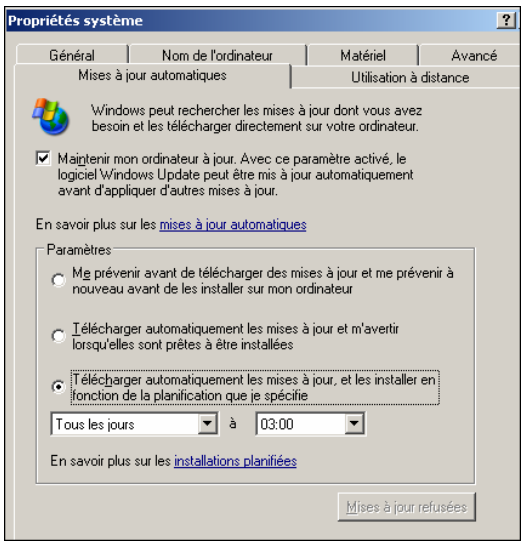
A partir de la fenêtre **Propriétés d'un périphérique**, plusieurs onglets (variable en fonction du périphérique) vous permettent de contrôler, modifier ou désinstaller celui-ci.

Général : affiche des informations sur l'état du périphérique (OK ou en conflit…) Vous pouvez aussi le désactiver dans le profil matériel sélectionné.
Pilote : affiche le détail des informations concernant le pilote. Vous pouvez aussi le mettre à jour avec un pilote plus récent, ou éventuellement revenir à la version précédente en cas de problème. Au final vous pouvez le désinstaller.

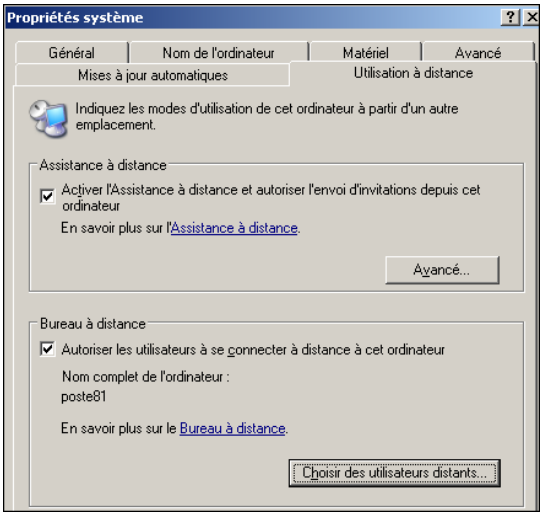
Onglet Profils matériel : il permet de créer plusieurs configuration de démarrage différentes. Surtout utilisé dans le cas où vous utilisez un ordinateur portable avec l'adaptateur réseau désactivé et un autre ordinateur avec la carte réseau activée. Par défaut il existe un profil matériel qui se nomme **Profil 1.** Il contient la configuration par défaut ou courante (Actuel).Vous pouvez créer un nouveau profil en sélectionnant celui existant, puis en cliquant sur le bouton **Copier** et en lui donnant un nom. Lorsque vous redémarrez votre micro, un choix vous sera proposé. En absence de choix de votre part le premier de la liste sera automatiquement démarré après le délai en secondes affiché dans la fenêtre des **Propriétés** (30 secondes par défaut).



Onglet Mises à jour Automatique : cette fenêtre vous permet de paramétrer les mises à jour en ligne sur Internet via Windows Update. Cette mise à jour peut être manuelle ou automatisée via votre programmation.

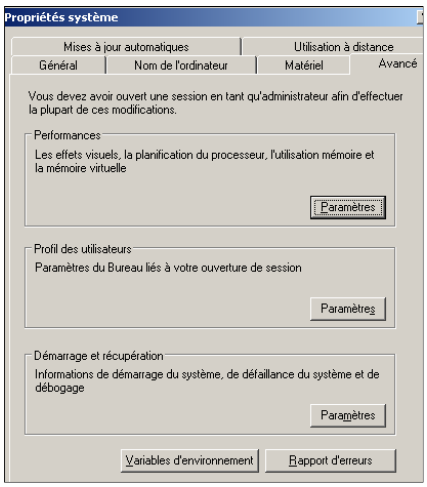


Onglet Utilisation à Distance : cette fenêtre vous permet d'autoriser l'**Assistance à distance** et le **Bureau à distance.** Cette fonctionnalité s'appuie sur le service de type **Terminal Server**.

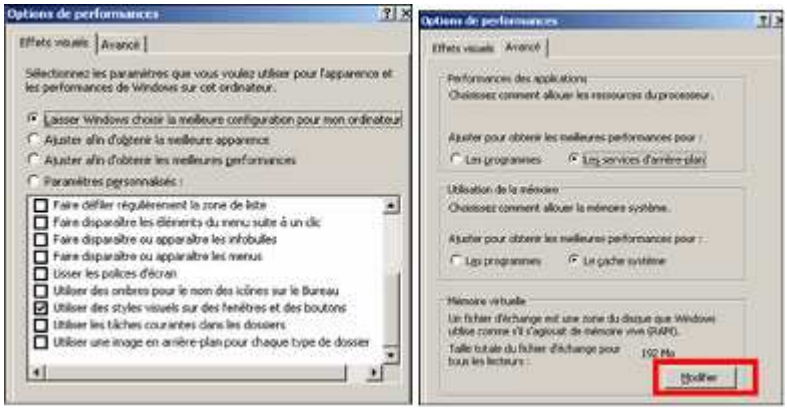


Onglet Avancé

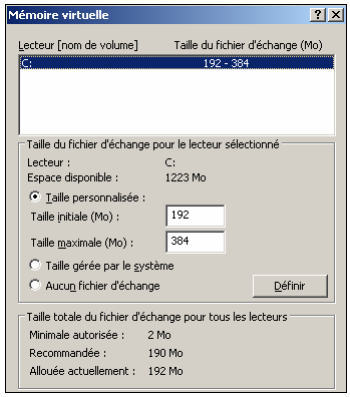
- **Performances** : cette option vous permet d'optimiser la priorité d'exécution pour les applications ou les services fonctionnant en arrière-plan, les effets visuels pouvant entraîner un surcroît d'activité ou en paramétrant la gestion de la mémoire (cache et mémoire virtuelle). Il est conseillé de désactiver les effets visuels si votre ordinateur est utilisé comme serveur.



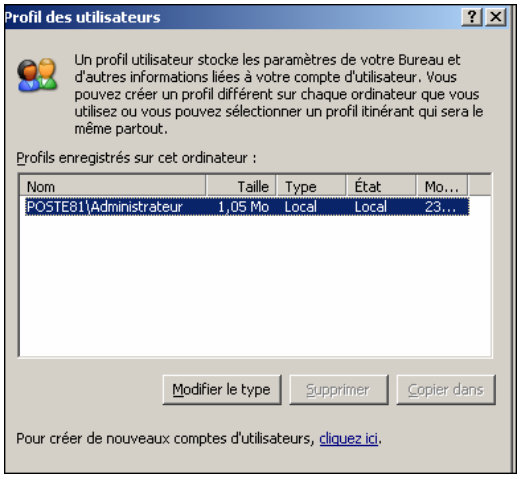
La zone **Performances** des applications vous permet d'optimiser la priorité d'exécution pour les applications ou les services fonctionnant en arrière-plan.



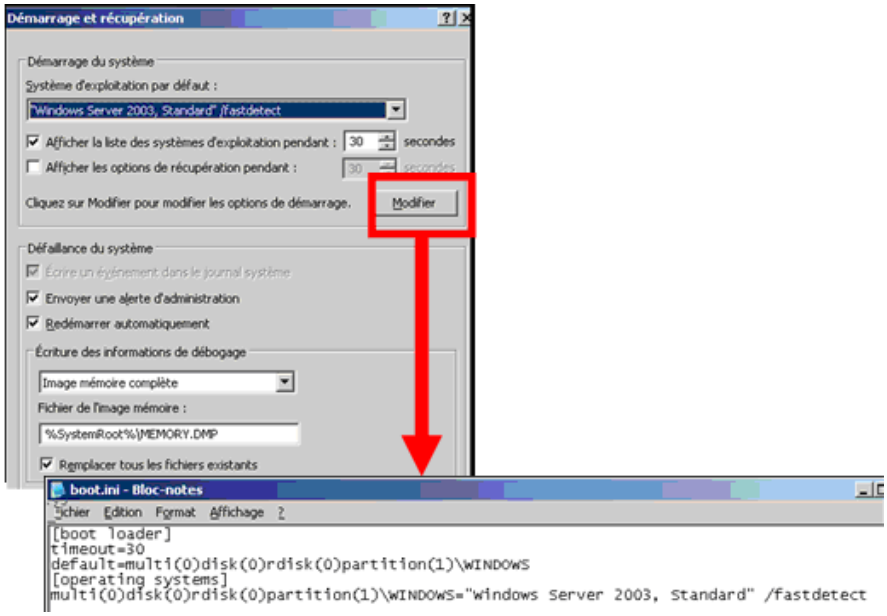
Rubrique Utilisation de la mémoire : vous avez la possibilité à l'aide de cette option de définir implicitement la quantité de mémoire cache attribuée à votre micro. Vous pouvez privilégier soit un meilleur fonctionnement pour les applications locales (l'utilisateur qui travaille sur le poste aura les meilleurs temps de réponses possible), soit pour le poste en tant que serveur.
Mémoire virtuelle : en cliquant sur le bouton **Modifier** vous accéderez à la fenêtre de la configuration de la mémoire virtuelle. Microsoft conseille de configurer la taille du fichier d'échange (swap) entre une à deux fois la quantité de RAM (mémoire physique) installée, bien souvent la taille du fichier d'échange (Pagefile.sys) est égale à la **RAM + 50 %.** W2003 vous propose une valeur dite recommandée. Vous pouvez paramétrer une valeur minimale ou maximale.



- **Profil des utilisateurs :** cette fenêtre permet de gérer les copies locales des profils utilisateurs ayant ouvert une session sur le micro.



- **Démarrage et récupération :** cette fenêtre permet soit de définir et configurer les options lors du démarrage, ou bien comment le système doit réagir en cas d'erreur importante (critique). La rubrique **Démarrage du système** indique quel sera le système d'exploitation de démarrage par défaut ainsi que le temps d'affichage avant démarrage automatique de celui-ci. Le bouton **Modifier** permet d'ouvrir le fichier boot.ini avec le bloc-notes afin de le modifier en mode texte. Par contre les modifications que vous apportées dans l'outil graphique sont automatiquement mises à jour dans le fichier **boot.ini.**



Les options que vous utiliserez le plus couramment sont :

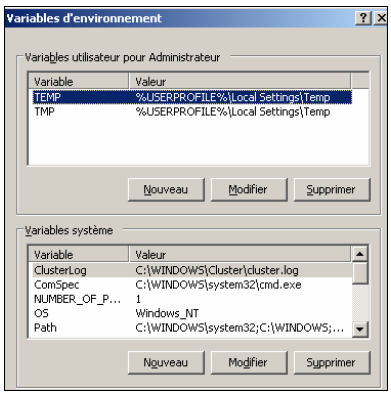
- **Ecrire un événement dans le journal système** afin de visualiser l'erreur dans l'Observateur d'événements.
- **Envoyer une alerte d'administration** pour prévenir les membres du groupe local Administrateurs par un message d'avertissement sur le type de problème.
- **Redémarrer automatiquement** afin de forcer un redémarrage système en mode sans échec (options de récupération) lorsqu'une erreur inattendue arrive.

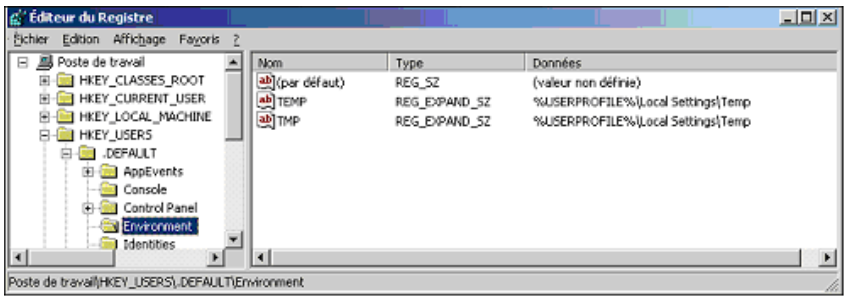
Onglet Variables d'environnement : les variables d'environnement contiennent des valeurs quelconques qui seront utilisées par le système, les applications ou les fichiers de commande. Elles sont stockées dans le registre. Une variable d'environnement est toujours encadrée par le symbole pourcentage **%.** Il existe deux types de variables :

- **Les variables liées à l'utilisateur :** elles sont mémorisées dans les clés Environment du registre sous HKEY_USERS. Vous pouvez ajouter, modifier ou supprimer vos propres variables en fonction de vos besoins. Les plus connues sont celles qui sont créées par défaut. Ce sont TMP et TEMP qui sont utilisées par les applications pour y stocker les fichiers temporaires. Comme vous pouvez le voir sur la figure ci-dessous, ces deux variables pointent vers le répertoire %userprofile%Local Settings\Temp.
- **Les variables système** stockées qui peuvent être ajoutées, modifiées ou supprimées par l'Administrateur ou par un équivalent.

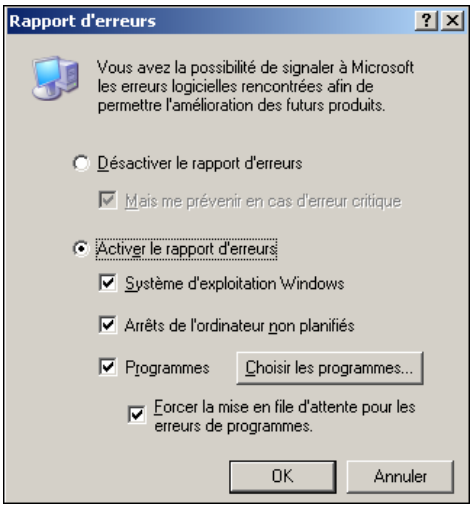
Pour les plus anciens qui ont bien connu le DOS, vous pouvez utiliser ces variables en mode commande ou dans les fichiers batch (.bat) ou dans un fichier .CMD.

ECHO %Variable%	affiche la valeur d'une variable.
SET variable=valeur	déclare une nouvelle variable.
SET variable=	supprime une variable.





Onglet Rapport d'erreurs : cette fenêtre vous permet d'activer ou désactiver le rapport d'erreurs des programmes. Cela se produit lors d'un arrêt imprévu (un plantage !) de votre système. Le contexte alors peut être sauvegardé dans un fichier qui pourra être étudié par vous-même ou envoyé à Microsoft. Vous pouvez choisir les différents éléments qui seront stockés en cas d'erreurs ou bien exclure certaines applications via le bouton **Choisir les programmes**.



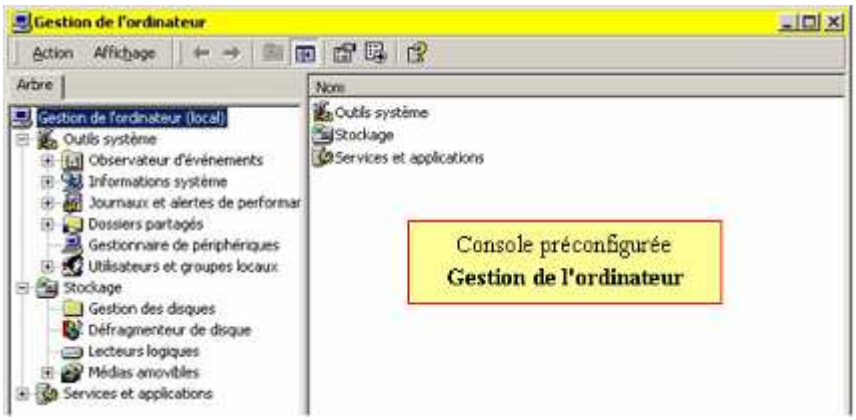
3.6- Les consoles d'administration MMC

La **console MMC** (Microsoft management Console) constitue le principal outil d'administration du serveur Windows 2003. Cette console permet de fédérer les outils de gestion du serveur. La console MMC au départ ne possède aucune possibilité d'administration. Il faut lui ajouter des composants logiciels enfichables (snap-in) pour qu'elle devienne opérationnelle. Un composant logiciel correspond à une seule unité de fonctionnalité de gestion. En ajoutant des composants à une console, on augmente ses possibilités de gestion.
Chaque composant permet d'effectuer une ou plusieurs tâches administratives. La console permet de centraliser l'administration du ou des serveurs. Elle peut être utilisée, avec certains composants logiciels enfichables, pour administrer à distance un ordinateur.
Il existe deux types de consoles : les **consoles préconfigurées** et les **consoles personnalisées**.

3.6.1- Types de consoles

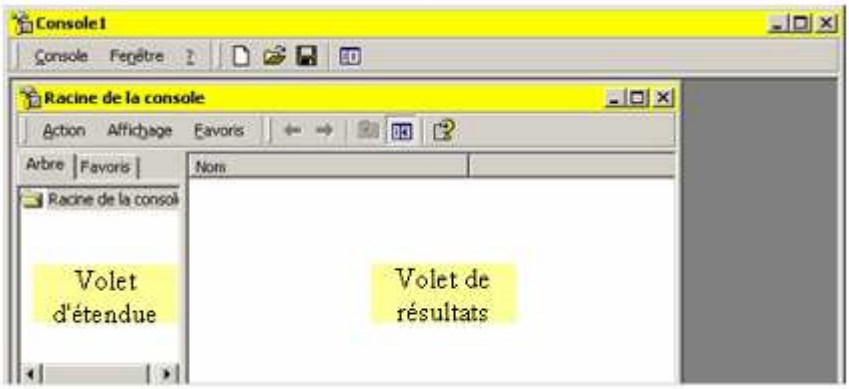
Les consoles préconfigurées

Ces consoles contiennent un composant logiciel enfichable permettant d'assurer une tâche bien déterminée. Elles fonctionnent en mode utilisateur, c'est-à-dire qu'on ne peut pas les modifier, ni leur ajouter de composant logiciel. Elles permettent d'assurer les fonctions de gestion les plus répandues. Le nombre de consoles dépend de la version de Windows 2003 utilisée. Ceci dit, il est possible d'ajouter les consoles d'administration serveur sur une station, en utilisant le programme Adminpak.msi présent sur le CD-ROM du serveur pour pouvoir administrer les serveurs à distance.



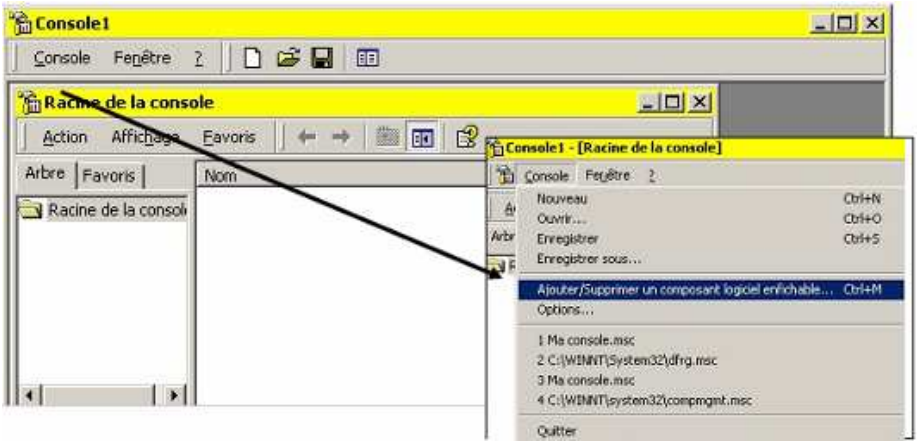
Les consoles personnalisées

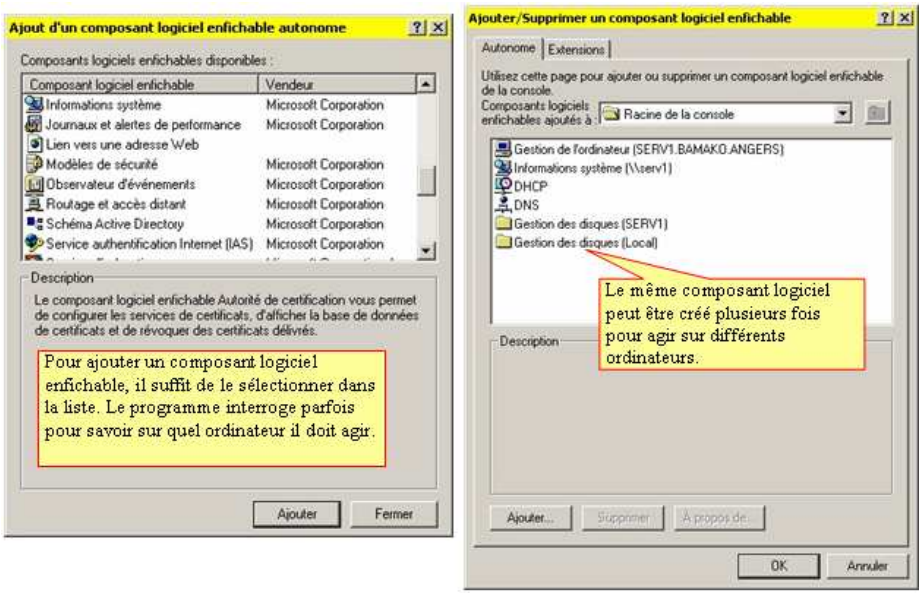
Vous pouvez créer des **consoles personnalisées** dans lesquelles vous positionnez un ou plusieurs composants logiciels enfichables. Vous créez une nouvelle console personnalisée en tapant la commande **mmc** dans **Exécuter** du menu **Démarrer**.

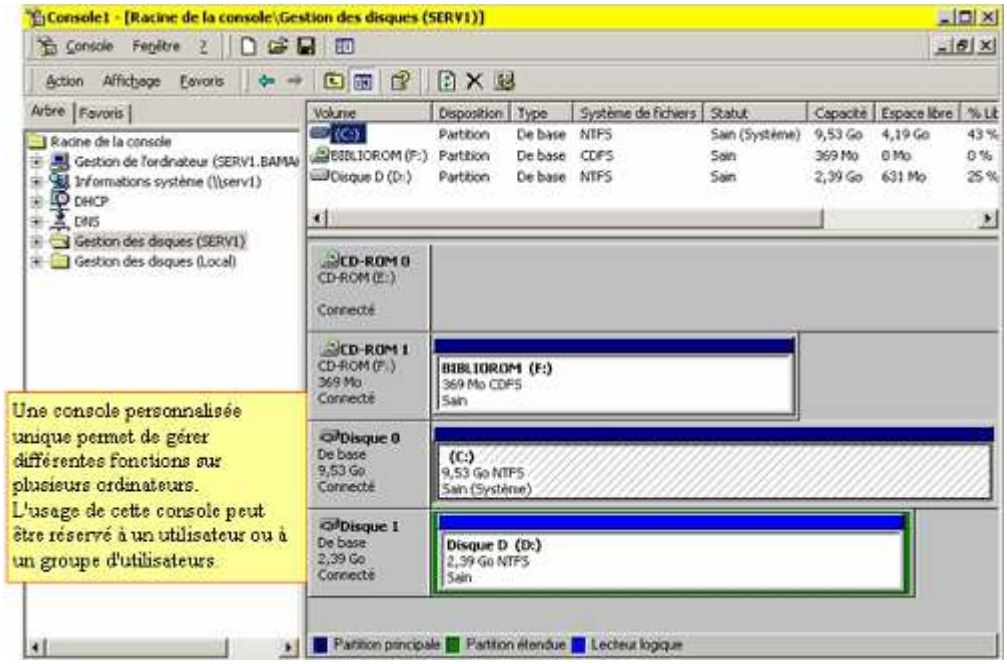


Vous pouvez créer des consoles spécifiques avec certains composants qui permettront aux utilisateurs que vous aurez désignés, d'assurer des tâches de gestion que vous leur aurez affectées. Il est possible de combiner dans une console personnalisée plusieurs composants logiciels enfichables

correspondants à des consoles préconfigurées, et même d'y ajouter des composants logiciels écrits par des tiers. Il est possible aussi de mettre plusieurs fenêtres dans une console pour en faciliter l'utilisation.







3.6.2- Modes consoles

Mode Auteur
Le mode **auteur** permet de créer des consoles, de leur ajouter ou supprimer des composants logiciels enfichables, de créer de nouvelles fenêtres et d'enregistrer les modifications.
Ceci permet de créer des consoles qui peuvent être distribuées sur différents ordinateurs et utilisées par différents utilisateurs jouant un certain rôle d'administration. Au moment de l'enregistrement, on peut choisir l'option de mode de la console de manière à ce qu'elle ne soit plus modifiable par celui qui va l'utiliser.

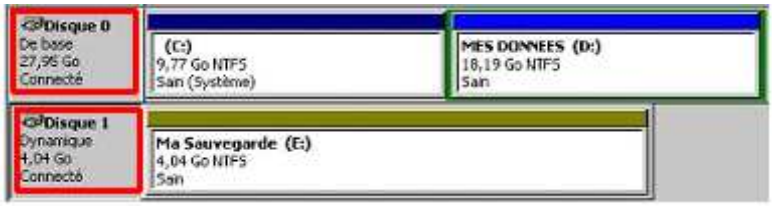
Modes utilisateur
Il existe 3 modes utilisateur :

Type du mode utilisateur	Description
Accès total	Ce mode permet aux utilisateurs de naviguer au sein des différents composants logiciels enfichables, d'ouvrir de nouvelles fenêtres et d'accéder à la totalité de l'arborescence de console
Accès limité, fenêtre multiple	Ce mode empêche les utilisateurs d'ouvrir de nouvelles fenêtres ou d'accéder à une partie de l'arborescence de console. L'utilisateur peut cependant ouvrir plusieurs fenêtres dans la console.
Accès limité, fenêtre unique	Ce mode empêche les utilisateurs d'ouvrir de nouvelles fenêtres ou d'accéder à une partie de l'arborescence de console. L'utilisateur ne peut ouvrir qu'une fenêtre dans la console.

IV- GESTION DES RESSOURCES DISQUES

4.1- Configuration des disques durs

Windows 2003 prend en charge deux types de stockage sur disques durs : le **stockage de base** et le **stockage dynamique**.

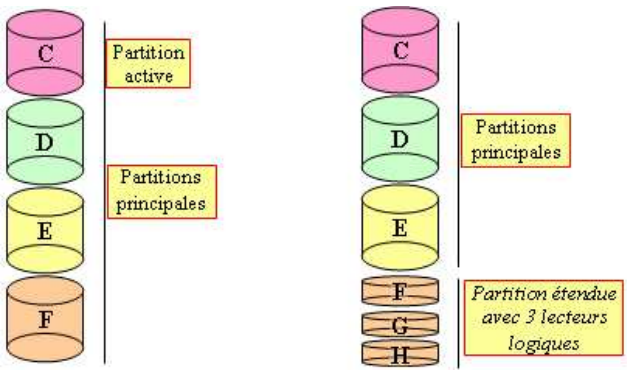


4.1.1- Stockage de base

Le **stockage de base** est la norme traditionnelle d'organisation des disques durs. Elle divise le disque dur en **partitions**. Il peut y avoir des partitions principales et des partitions étendues. C'est le mode de fonctionnement de tous les systèmes d'exploitation Microsoft qui ont précédé WINDOWS 2003. C'est aussi le mode de stockage de Windows 2003 **par défaut** et le restera tant que vous n'aurez pas demandé le type de stockage dynamique.

Types de partitions

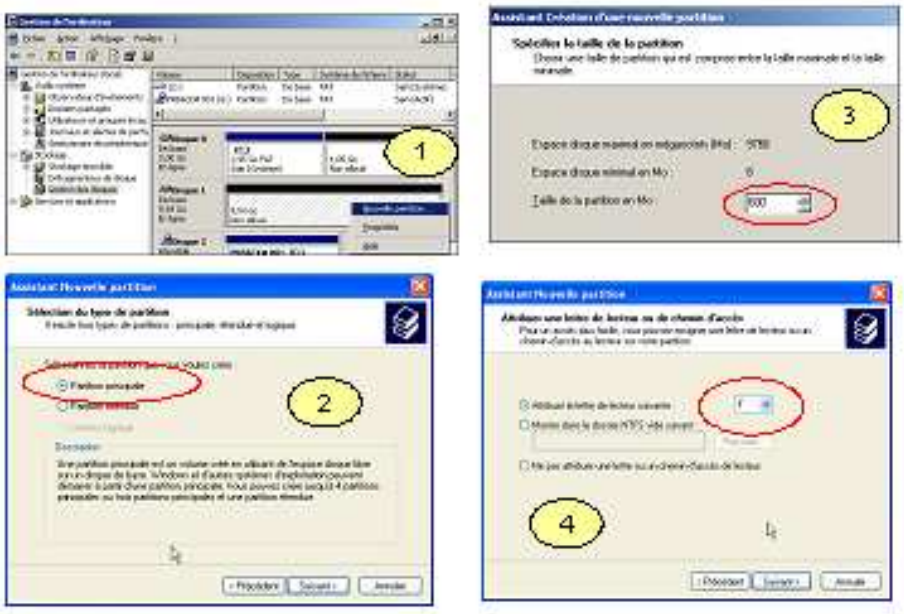
- **Partitions principales :** un disque dur peut comporter jusqu'à 4 partitions. Une **partition principale** est nécessaire pour démarrer le système d'exploitation. La partition principale qui contient les fichiers d'amorçage pour démarrer le système d'exploitation est la partition **principale active**. Au moins une partition principale doit être présente sur le premier disque dur. Si la partition active est formatée NTFS, il ne peut y avoir d'amorçage double avec un autre système d'exploitation (comme W98). Seul un formatage FAT16 permet un amorçage double avec tous les systèmes d'exploitation Windows. La **partition système** de Windows 2003 est la partition active qui contient les fichiers décrivant le matériel et ceux nécessaires au chargement du système d'exploitation. La **partition d'amorçage** de Windows 2003 est la partition, qui contient les fichiers d'exploitation (**Winnt**). La partition d'amorçage et la partition système peuvent être sur la même.
- **Partitions étendues :** une **partition étendue** est créée à partir de l'espace libre sur un disque dur, après création des partitions principales. Il ne peut donc y avoir qu'une seule partition étendue par disque dur. Ce type de partition peut recevoir un système d'exploitation mais ne pourra pas en assurer l'amorçage direct. Elle ne nécessite pas de formatage. Ce type de partition peut être divisé en segments qu'on appelle **lecteurs logiques afin d'être formatés avec le système de fichiers désiré.** Chaque lecteur se voit attribuer une lettre de lecteur.



- **Lecteurs logiques :** les divisions logiques sont structurées au sein d'une partition étendue. Vous devez au minimum créer un lecteur logique dans une partition étendue qui peut dans

ce cas prendre toute (ou partie) de la capacité de celle-ci. Ensuite vous devez formater chaque lecteur logique avec un système de fichiers supporté par W2003 Server (FAT/32 ou NTFS). Par défaut les lettres A, B et C étant réservées, il reste 23 possibilités pour les lecteurs logiques. L'outil permettant de gérer les disques avec W2003 Server est le composant enfichable **Gestion des disques**. Cette console vous permet de créer, supprimer des partitions. Elle vous donne aussi des informations sur le type des disques (de base ou dynamique), sur le système de fichiers de vos partitions, sur la capacité, l'espace et le pourcentage libre des partitions voire l'appartenance des partitions à un ensemble de tolérance de pannes. On verra que vous pouvez aussi utiliser en mode interactif l'utilitaire de ligne de commande **DISKPART**. Cet utilitaire donne en plus la possibilité d'automatiser certaines opérations de gestion des disques via un script.
Exemple : **DISKPART /F Fichier_script** ou Fichier_Script est un fichier de type texte contenant les commandes à exécuter.

Créer une partition principale
Pour créer une partition principale vous devez tout d'abord sélectionner un espace non alloué sur un disque de base. Puis à partir du menu, choisissez **Action** – **Toutes les Tâches** – **Nouvelle partition** ou bien à partir du menu contextuel. L'assistant vous demande de sélectionner le type de partition (partition principale), puis la taille en **Mo** (elle ne peut être **inférieure à 8 Mo**).
Nota : si vous souhaitez prendre tout l'espace disponible restant, conservez au minimum 1 Mo afin de pouvoir convertir votre disque de base en disque dynamique ultérieurement (c'est ce dont a besoin le système pour réaliser cette conversion).
Ensuite W2003, vous propose une lettre de lecteur pour cette partition que vous pouvez conserver ou changer. De toute façon vous pouvez réaliser cette opération ultérieurement.

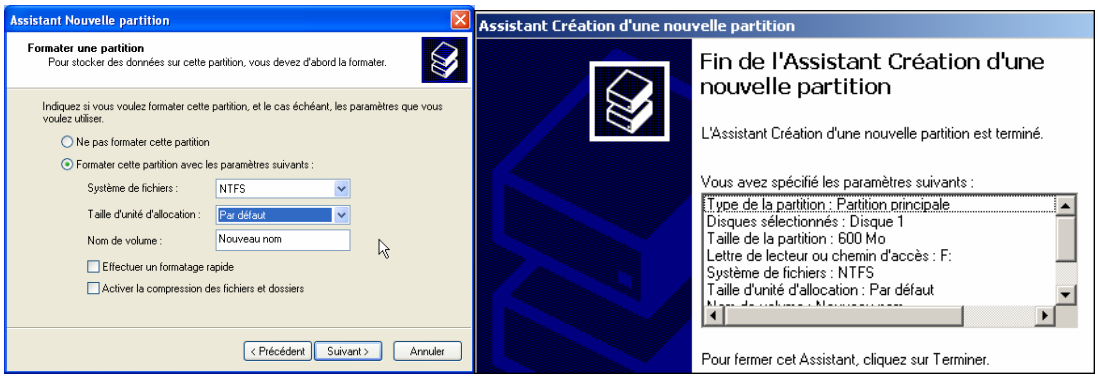


Ensuite vous devez formater la partition en choisissant un des systèmes de fichiers proposés et reconnus par W2003 Server. Vous devez aussi indiquer la **taille d'unité d'allocation** (cluster).

Rappels : le cluster ou unité d'allocation est le plus petit élément pouvant être traité par le système en lecture ou écriture sur un disque. Il est égal à plusieurs secteurs physiques du disque dur. L'unité d'allocation ou cluster est fonction de la taille de la partition et du système de fichiers choisi.
Les valeurs attribuées par défaut peuvent être changées, mais il n'est plus possible ensuite de les modifier sans formater le lecteur …

Taille de la Partition	FAT16	FAT32	NTFS
7 Mo – 16 Mo	2 Ko	Non supporté	512 octets
17 Mo – 32 Mo	512 octets	Non supporté	512 octets
33 Mo – 64 Mo	1 Ko	512 octets	512 octets
65 Mo – 128 Mo	2 Ko	1 Ko	512 octets
129 Mo – 256 Mo	4 Ko	2 Ko	512 octets
257 Mo – 512 Mo	8 Ko	4 Ko	512 octets
513 Mo – 1024 Mo	16 Ko	4 Ko	1 Ko
1025 Mo – 2 Go	32 Ko	4 Ko	2 Ko
2 Go – 4 Go	64 Ko	4 Ko	4 Ko
4 Go – 8 Go	Non supporté	4 Ko	4 Ko
8 Go – 16 Go	Non supporté	8 Ko	4 Ko
16 Go – 32 Go	Non supporté	18 Ko	4 Ko
32 Go – 2 To	Non supporté	Non supporté	4 Ko

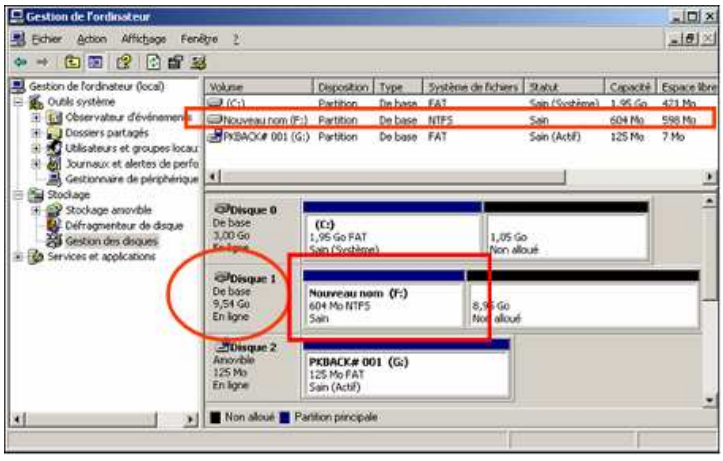
✋ L'option **Formatage Rapide** qui accélère le formatage ne doit être utilisée que lorsque le support est réputé sain.



✋ L'utilitaire **DISKPART** permet de créer une partition principale à partir du prompt de commande.

DISKPART
Select disk n
Create partition primary size=x offset=y
Assign letter=z

n numéro du disque sur lequel sera créé la partition.
x taille de la partition en octets.
y décalage en octets pour le début de la partition. Si cette option est absente, la partition sera créée en début d'espace disponible sur le disque.
z lettre d'unité affectée à la partition.



Activer la partition

Si c'est la première partition principale du premier disque physique que vous venez de créer, elle sera marquée comme étant active. Au démarrage de votre micro le secteur d'amorçage sera recherché sur cette partition. Dans le cas où vous avez plusieurs partitions principales sur un ou plusieurs disques durs, vous avez la possibilité de modifier le statut de chacune d'entre elles pour effectuer l'amorçage sur une autre partition.

Rappel : une seule partition principale peut être activée sur un disque dur.

Pour activer la partition principale allez dans le menu **Action – Toutes les tâches – Marquer la partition comme active**.

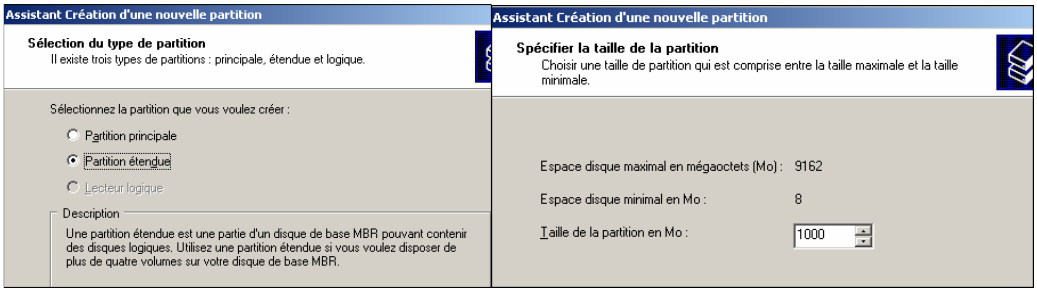
Mise en oeuvre avec la commande DISKPART

DISKPART
Select disk n
Select partition x
active

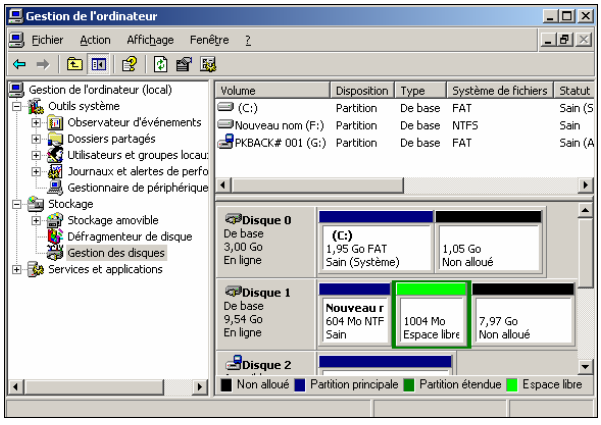
n numéro du disque supportant la partition à activer.
x numéro de la partition à activer.

Créer une partition étendue

Sélectionnez un espace non alloué sur votre disque de base puis activez **Action** – **Toutes les tâches** – **Nouvelle partition** ou à partir du menu contextuel. Cochez **Partition étendue** et entrez la **taille souhaitée**. La partition étendue sera automatiquement créée.



La partition étendue créée devient un espace libre qui attend la création de lecteurs logiques.

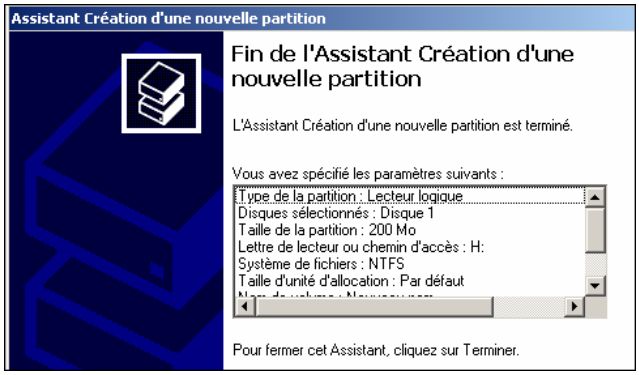


Mise en oeuvre avec la commande DISKPART

DISKPART
Select disk n
Create partition extended size=x offset=y

n numéro du disque sur lequel sera créé la partition.
x taille de la partition en octets.
y décalage en octets pour le début de la partition. Si cette option est absente, la partition sera créée en début d'espace disponible sur le disque.

Créer des lecteurs logiques
Cette opération doit se réaliser après la création de la partition étendue. Vous pouvez créer autant de lecteurs logiques qu'il vous reste de lettres de lecteurs disponibles. Sélectionnez la partition étendue, **Action** – **Toutes les tâches** – **Créer un nouveau lecteur logique** ou à partir du menu contextuel. L'option **Lecteur logique** sera automatiquement sélectionnée. Ensuite entrez la **taille** à affecter à ce lecteur logique puis le type de formatage. Vous pouvez aussi modifier la lettre de lecteur attribuée par défaut.



Mise en oeuvre avec la commande DISKPART
DISKPART
Select disk n
Create partition logical size=x
Assign z

n	numéro du disque sur lequel sera créé le lecteur logique.
x	taille de la partition en octets.
z	lettre d'unité affectée au lecteur logique.

Rappel : les unités de stockage amovible ne contiennent que des partitions principales. Vous ne pouvez pas y créer des partitions étendues, ni des volumes. Vous ne pouvez pas marquer comme active une partition principale située sur un périphérique amovible.

Supprimer une partition
Attention cette opération efface toutes les données qu'elle contient. A partir de la console **Gestion des disques,** sélectionnez la partition à supprimer puis **Action** – **Toutes les tâches** – **Supprimer la partition** ou à partir du menu contextuel.
En mode commande
DISKPART
Select disk n
Select partition x
Delete partition

n	numéro du disque supportant la partition à supprimer.
x	numéro de la partition à supprimer.

4.1.2- Stockage dynamique

Windows 2003, prend en charge une nouvelle forme de stockage sur disques, le **stockage dynamique**. Le stockage dynamique n'est pas formé par des partitions, mais par des volumes. Un **volume** est une portion de disque vue comme un disque physique distinct. Autrement dit, l'utilisateur ne voit pas des disques durs, il ne voit que des volumes. Si un volume est à cheval sur plusieurs disques, l'utilisateur ne peut pas le savoir. Les informations de disque ne sont pas enregistrées dans le registre mais sur le disque lui-même.
✋ Vous pouvez toujours conserver les partitions sur des disques de base afin d'assurer une compatibilité avec l'existant, car les volumes ne sont pas lisibles par les systèmes antérieurs à W2000.

Les avantages du stockage dynamique sont :

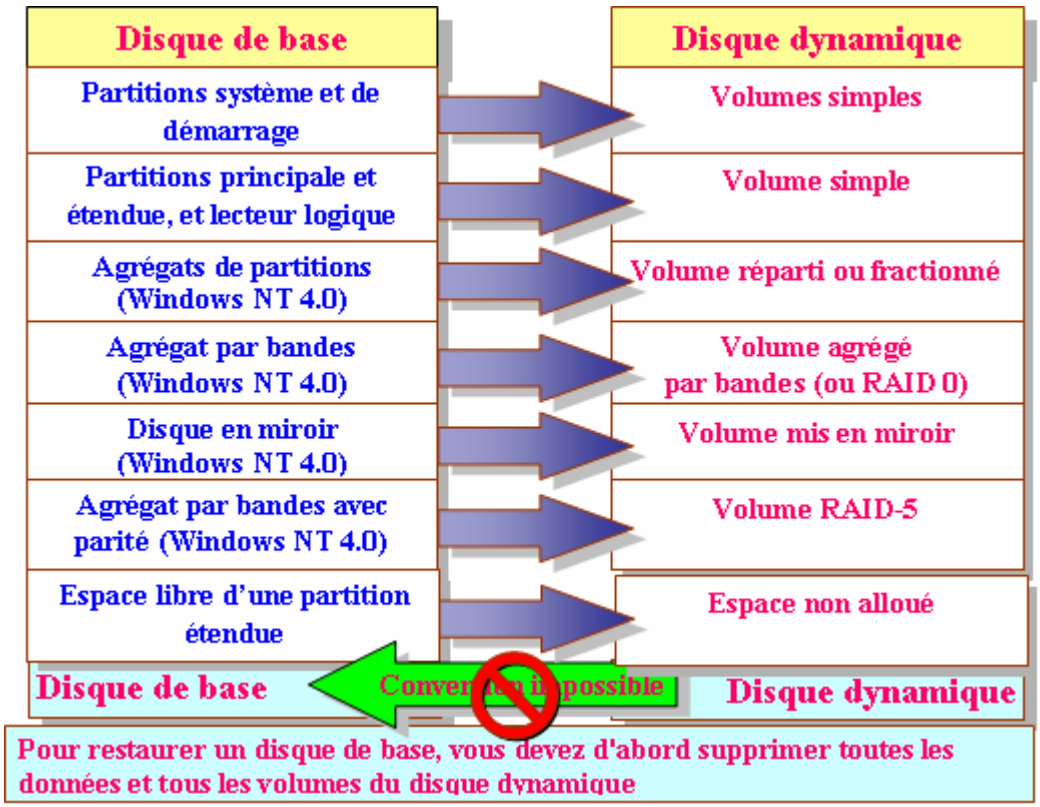
- De pouvoir utiliser la tolérance de panne sans redémarrage du système.
- De pouvoir créer un nombre illimité de volumes.
- De pouvoir étendre un volume NTFS.
- Un volume n'est plus limité au disque physique.

Mise à jour vers un disque dynamique

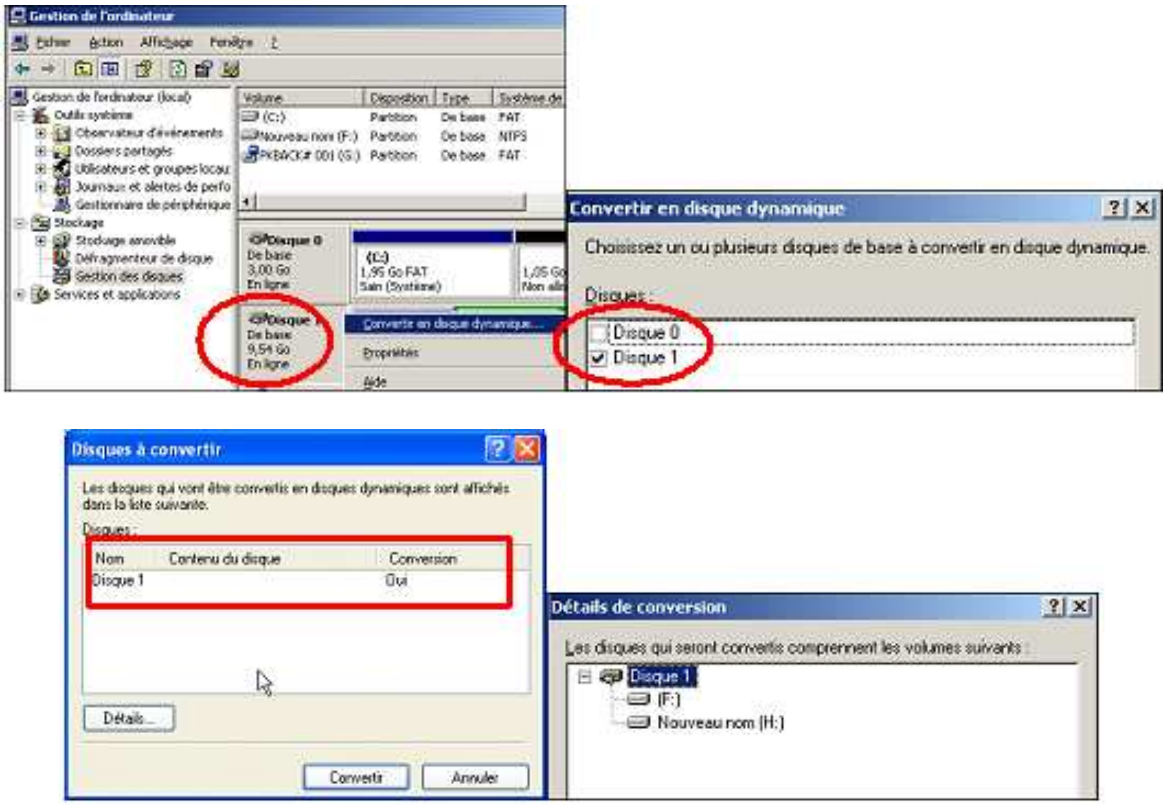
Cette mise à jour se réalise sans perte de données. Par contre le retour en arrière est impossible. Si vous voulez revenir à un disque de base vous devez supprimer tous les volumes du disque.

Cinq types de volumes existent sur des disques dynamiques. Lorsque vous ferez la mise à jour d'un disque de base vers un disque dynamique, les données sont totalement sauvegardées et les partitions deviennent :

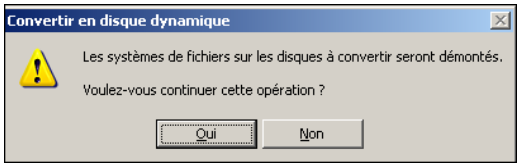
- Une partition principale devient un volume simple.
- Les lecteurs logiques contenus dans une partition étendue deviendront chacun un volume simple.
- L'espace libre à l'intérieur d'une partie étendue deviendra de l'espace non alloué disponible. Vous pourrez créer des volumes ultérieurement dans cet espace libre.
- Les miroirs de partitions deviennent des volumes en miroir.
- Les agrégats par bandes avec parités deviennent des volumes RAID5.
- Les agrégats par bandes deviennent des volumes d'agrégats par bandes.
- Les agrégats de partitions deviennent des volumes répartis ou fractionnés.



La conversion d'un disque de base en dynamique peut se réaliser à partir de la console **Gestion des disques**, puis vous devez sélectionner le disque de base et cliquer sur **Action** – **Toutes les tâches** – **Convertir en disque dynamique** ou directement à partir du menu contextuel.



Cliquez sur le bouton **Convertir** pour démarrer cette mise à niveau. Un message vous indique que pendant la conversion, les disques seront démontés et donc momentanément inaccessibles.



Dès que la conversion est réalisée, vous pouvez visualiser le résultat dans le Gestionnaire de disques. Le terme dynamique est affiché à la place de base au niveau du disque et les partitions sont devenues les volumes décrits précédemment.

En mode commande avec DISKPART.

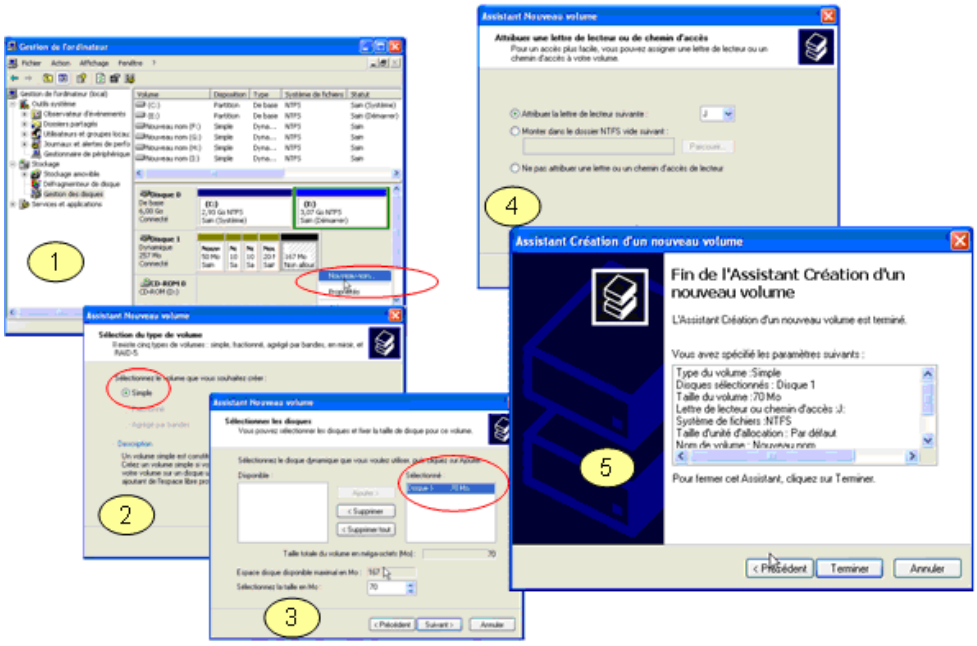
DISKPART
Select disk n
Convert dynamic

Par contre la commande convert basic vous permet de retourner à un disque de base avec comme condition qu'il soit dépourvu de volume.

Types de volumes

⇨ **Volume simple :** un **volume simple** correspond à de l'espace alloué sur un seul disque dur et en entier. Il n'y a aucune tolérance de pannes. A l'inverse des partitions, ils n'ont aucune limite de taille et ne sont pas limités en nombre de volumes. Ils peuvent être formatés en NTFS, FAT 16 ou 32.

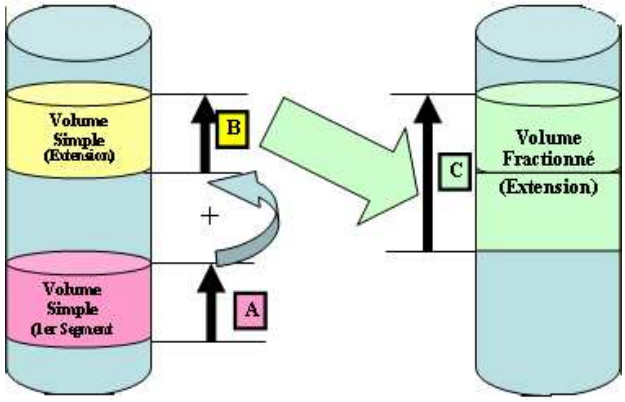
Créer un volume simple : sélectionnez une partie d'un disque dynamique non alloué, puis validez **Action** – **Toutes les tâches** – **Nouveau Nom** ou à partir du menu contextuel. Sélectionnez **Volume simple,** puis le **disque** et fixez la **taille** du futur volume, entrez la **lettre** de lecteur puis le **système de fichiers.**



En mode commande DISKPART.
DISPART
Create volume simple size=x disk=n

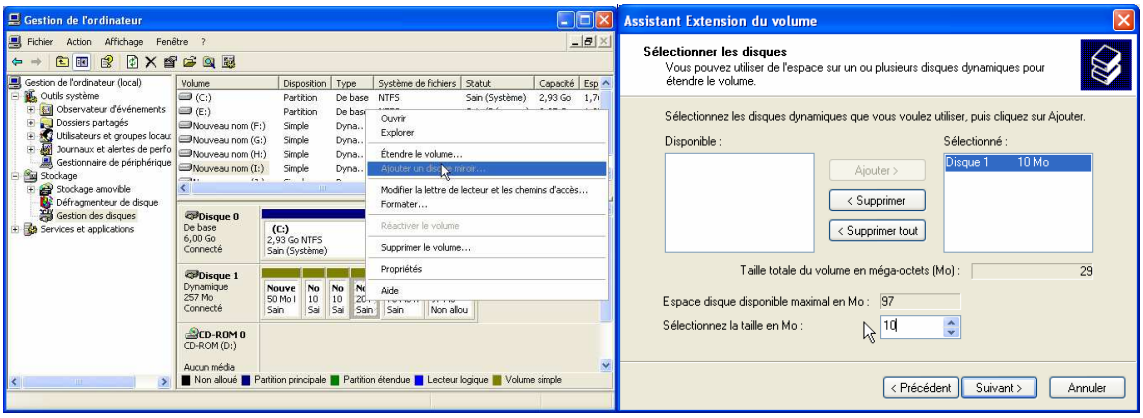
X taille du volume en octets.
N numéro des disques sur lesquels vous désirez créer le volume. Si absent le disque courant sera la cible.

Etendre un volume simple : un volume simple formaté en NTFS pourra être étendu dans le but de créer un volume plus important regroupant l'espace initial du volume et un ou plusieurs espaces de disques non alloués, contigus ou non



Comme à chaque opération allez dans **Action** – **Toutes les tâches** – **Etendre le volume** (ou par le menu contextuel). Sélectionnez le ou les disques avec lesquels vous souhaitez étendre votre volume. Fixez la taille supplémentaire à ajouter au volume initial puis validez.

✋ Il vous est impossible d'étendre un volume avec des espaces résultant de la conversion d'une partition vers un volume, c'est-à-dire résultant de la mise à jour d'un disque de base en dynamique. Il faut obligatoirement que le volume soit créé à l'origine sur un disque dynamique. Cela à pour conséquence qu'il est impossible d'étendre un volume système, ainsi qu'un volume d'amorçage.

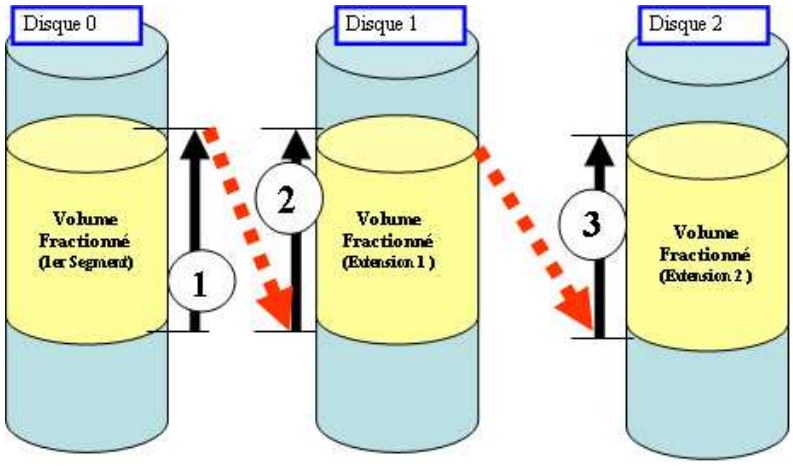


En mode commande avec DISKPART.

DISKPART
Select disk n
Select volume x
Extend size = y

n numéro du disque contenant le volume à étendre.
x numéro du volume à étendre.
y taille en octets de l'extension du volume.
z numéro du disque à ajouter au volume existant.

⇨ **Volume fractionné :** un **volume fractionné** contient des portions (jusqu'à 32) de disques durs. Windows 2003 remplit les portions les unes après les autres. Il n'y a pas de tolérance de pannes. Les volumes fractionnés sont en fait le regroupement d'espaces libres situés sur deux disques minimum et 32 au maximum. Les données sont d'abord écrites sur la partie libre du premier disque dur, puis lorsque ce premier disque est plein, l'écriture se fait sur le second et ainsi de suite…



Pour créer un volume fractionné sélectionnez un espace non alloué, **Action** – **Toutes les tâches** – **Nom de volume** (ou par le menu contextuel). En fait vous retrouvez le même mécanisme que précédemment. L'assistant démarre à chaque fois et dans ce cas il va vous demander de sélectionner

le type de volume que vous souhaitez créer. Dans ce cas cochez **Fractionné**, puis vous devez sélectionner au moins **deux disques dynamiques** afin de créer un volume fractionné. Vous devez bien évidemment indiquer pour chaque disque la taille que vous souhaitez utiliser. Au final vous devez choisir le format du système de fichiers. Comme pour un volume simple vous pouvez étendre un volume fractionné.
En mode commande.

DISKPART
Select disk n
Create volume simple size=x
Select volume m
Extend size=y disk=z

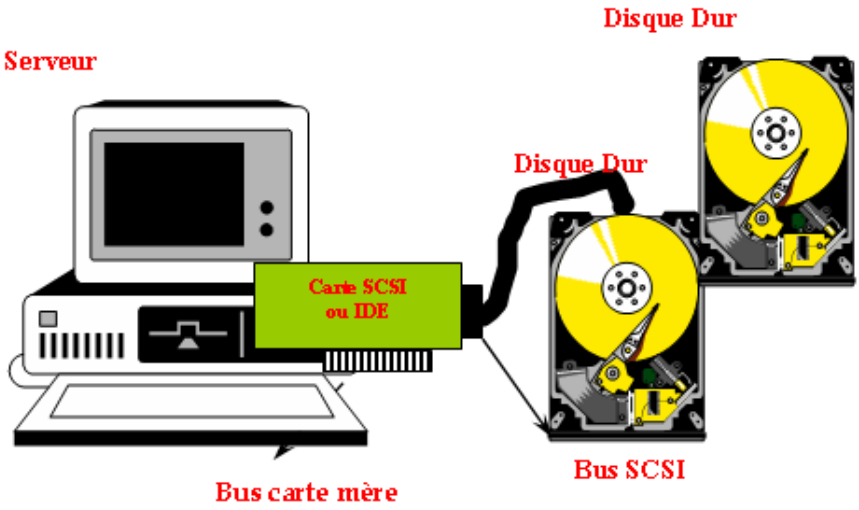
n numéro du disque qui stocke le premier segment du volume fractionné.
x taille en octets du volume initial (volume simple).
m numéro du volume qui vient d'être créé.
y taille en octets de l'extension du volume.
z numéro du disque (différent de n) à ajouter au volume déjà existant..

⇨ **Volume en miroir :** un **volume en miroir** (RAID 1) est composé de deux volumes simples (ou deux groupes de volumes simples) dont l'un est la copie de l'autre. Il y a tolérance de panne. Si l'un des disques tombe en panne, il est possible de récupérer les données sur l'autre volume.

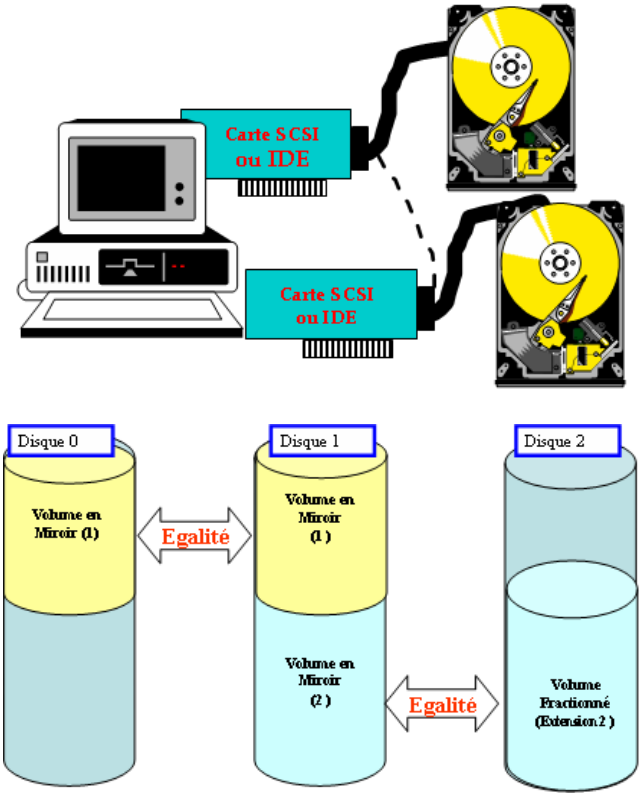
Rappels tolérance de pannes et technologie RAID
RAID (Redundant Array of Inexpensive Disk) résulte de l'expérience informatique et des coûts engendrés par la perte de données. En fait il coûte moins cher à une entreprise d'avoir plusieurs disques de faible coût montés en sécurité que d'en acheter un seul de marque ou de fabrication haut de gamme et onéreux.
Pour cela plusieurs niveaux de RAID ont été créés et ils sont repérés par un chiffre (de 0 à 5). Chacun ayant un rôle bien défini et tous n'interviennent pas au niveau sécurité. Au niveau de la sécurité deux sont largement mis en œuvre c'est le RAID1 et le RAID5.
Pour mettre en place une tolérance de pannes vous devez au minimum mettre en œuvre une redondance des informations. Cette redondance peut être partielle ou totale.

Mise en œuvre d'un miroir ou RAID-1
Deux technologies peuvent être mises en œuvre :

- **Le mirroring** : un seul contrôleur de disque et deux disques durs de préférence identiques. Par contre si le contrôleur de disque tombe en panne, il n'y a plus de sécurité.

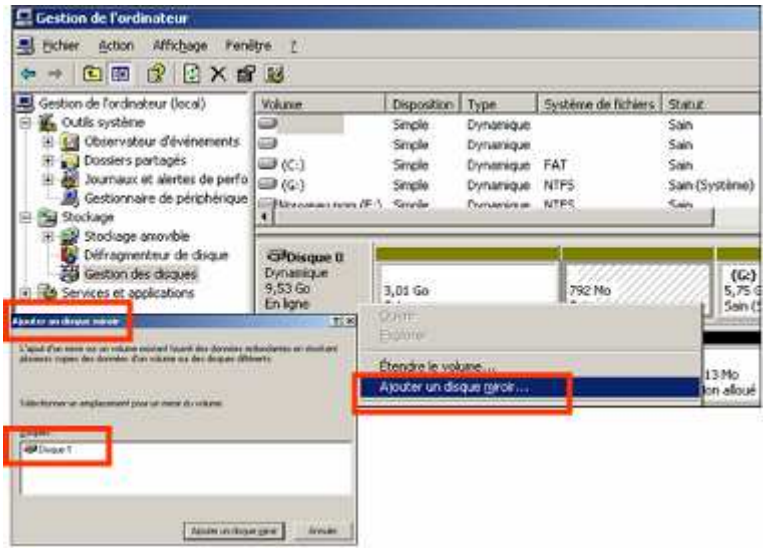


- **Le duplexing** : constitué de deux contrôleurs et de deux disques ayant chacun leur contrôleur de disque. Dans ce cas la fiabilité est accrue.



Mise en œuvre de plusieurs miroirs sur un même disque

La solution de mirroring est une solution qui peut s'avérer coûteuse mais elle vous procure une grande sécurité. Les données sont écrites au même instant sur deux disques de manière identique et transparente pour l'utilisateur. On pourrait presque dire que le système réalise une photocopie en temps réel. Lorsqu'un problème survient il suffit de "**briser le miroir"**, puis de remplacer le disque en panne et rétablir ensuite le miroir. Il n'y aura donc pas de pertes de données (théoriquement). W2003 Server supporte et gère ces deux technologies de façon transparente. Pour créer le miroir vous devez sélectionner le volume à dupliquer, et comme habituellement menu **Action** – **Toutes les tâches** – **Ajouter un disque miroir** (ou menu contextuel). Sélectionnez le disque miroir cible qui va recevoir le miroir du volume sélectionné. Cliquez sur le bouton **Ajouter un disque en miroir**. Le système d'exploitation va démarrer une procédure de régénération des données stockées sur le disque initial vers le nouveau disque cible en miroir.



Pendant cette opération un petit triangle de signalisation va apparaître sur l'icône du disque. Il vous informe que les membres du miroir sont désynchronisés suite à une défaillance de l'un des disques. C'est normal et cela doit disparaître à la fin de la synchronisation. Le disque devrait réapparaître comme sain.

Supprimer et annuler un Miroir

Vous pouvez à tout instant annuler ou supprimer un miroir. Les deux actions se comportent différemment au niveau des données. L'annulation aura pour effet de rompre la relation entre les deux disques, mais les données seront conservées en état sur les deux disques. Le volume du miroir sera séparé en deux volumes ayant les mêmes informations, mais sans tolérance de pannes.

Pour annuler un miroir sélectionnez l'un des volumes du miroir puis comme d'habitude **Action – Toutes les tâches – Annuler le volume en miroir** (ou menu contextuel). Un message va s'afficher pour indiquer que les volumes ne vont plus bénéficier de la tolérance de pannes. De plus une nouvelle lettre va être affectée au membre du miroir sur lequel vous travaillez.

Par contre la suppression du miroir efface automatiquement toutes les données du membre du miroir qui devient de l'espace non alloué.

Pour supprimer un miroir vous devez sélectionner un des volumes concerné puis **Action – Toutes les tâches – Supprimer le disque en miroir** (ou menu contextuel). Sélectionnez le membre du miroir à supprimer et validez **Supprimer le disque miroir**. C'est aussitôt effacé et le membre restant redevient un volume simple.

Amorcer sur une partition secondaire de disque en miroir

Nous venons de voir comment réaliser la mise en miroir d'un disque. Si par contre vous mettez la partition d'amorçage ou du système en miroir il faut être capable de pouvoir démarrer sur le second disque dur à partir d'une disquette de démarrage dans le cas où le premier serait défectueux.

Vous pouvez toujours intervenir physiquement sur vos disques (cavaliers par exemple) ou au niveau du BIOS pour modifier l'ordre des disques dans le cas où vous êtes resté en disque de base. Dans ce cas l'amorce système est toujours recherchée (comme nous l'avons vu au début de ce chapitre) sur la partition active du premier disque. Par contre sur un disque dynamique cette activation n'est à ce jour pas proposée. Vous devez donc comme sous NT4 ou W2000 modifier le contenu du fichier BOOT.INI. Vous devez créer une disquette de démarrage comme décrit ci-dessous :

- Formater une disquette avec Windows Server 2003 (ou W200, NT4 ou XP).
- A partir de la racine du volume système, vous devez recopier comme sous W2000 ou NT4 les fichiers suivants sur la disquette :
  - NTLDR.
  - NTDETECT.COM.
  - BOOT.INI.
  - NTBOOTDD.SYS (si le Bios du contrôleur SCSI est désactivé).

Ensuite avec cette disquette vous pouvez amorcer le démarrage de votre machine mais le noyau du système sera toujours recherché sur le mauvais disque. Il faut éditer le fichier BOOT.INI de la disquette et modifier le numéro du disque par celui du membre sain.

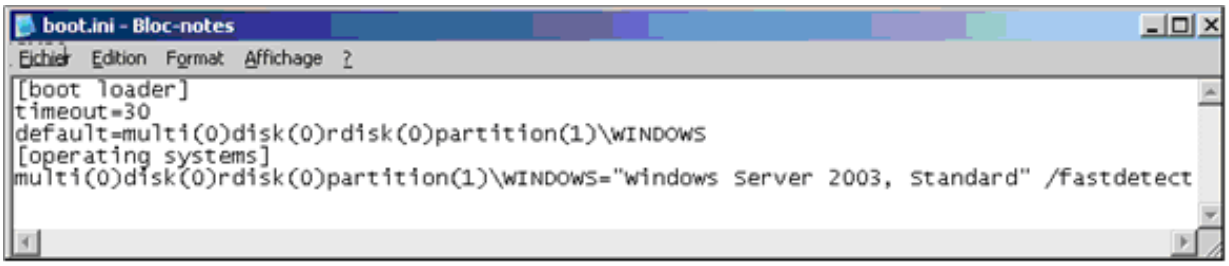
La syntaxe des noms répond à la norme ARC (Advanced RISC Computing).

Elle se présente sous la forme :

SCSI (x) disk (y) rdisk (0) partition (n) ou
MULTI (x) disk (y) rdisk (0) partition (n)

- SCSI (x) ou MULTI (x) : x indique le numéro de contrôleur matériel SCSI dans l'ordre d'initialisation. Sur les disques IDE, c'est toujours MULTI (0).
- Disk (y) correspond pour les cartes SCSI multibus au numéro de bus. Il vaut toujours zéro pour les contrôleurs MULTI.
- RDISK (z) : z indique le numéro de disque sur le contrôleur. Il vaut toujours zéro pour les disques SCSI.
- Partition (n) : n indique le numéro de la partition de 1 à n.

Il suffit de modifier les paramètres en conséquence avec en particulier la valeur RDIS (z) par le numéro du disque contenant le disque en miroir encore sain et éventuellement la PARTITION (n) si le volume n'a pas la même position que sur le premier disque.

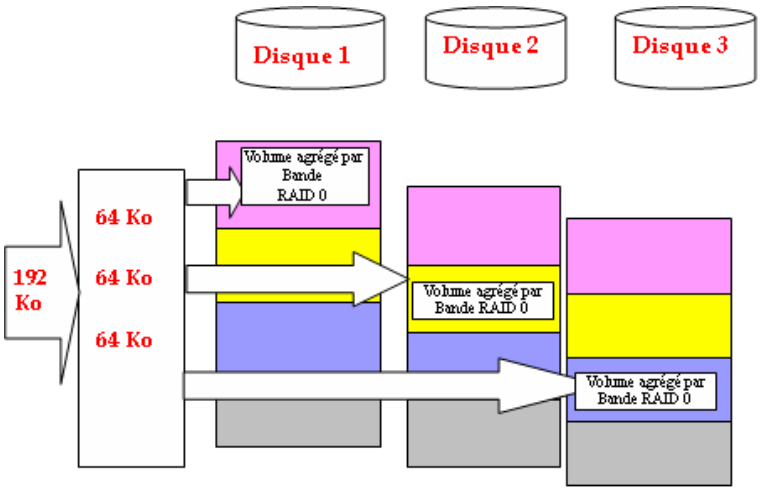


Réparer un disque d'origine

Si un des disques du miroir vient à être défaillant, il ne fonctionne donc plus mais par contre l'autre disque en miroir continue à fonctionner sans tolérances de pannes. Vous allez donc remédier à cette situation en procédant à une réparation du miroir. Dans la console **Gestion des disques** le disque défaillant est représenté comme manquant, déconnecté ou connecté avec erreur. Les causes de défaillances sont multiples. Vous allez donc changer de disque dur et en installé physiquement un nouveau. Il vous faut ensuite réactiver le miroir. Pour cela activez **Action – Toutes les tâches – Réactiver le disque** (ou menu contextuel). Normalement c'est **OK**. Dans le cas contraire il faut supprimer le miroir pour le recréer, mais attention il y des risques.

⇨ Volume agrégé par bande

Un **volume agrégé par bande** (ou RAID 0) est un volume constitué de portions de plusieurs disques durs afin de former un volume logique. L'écriture peut se faire de manière simultanée sur plusieurs disques, ce qui diminue le temps d'écriture et de lecture des données. Il n'y a pas tolérance de pannes, car si un disque est défaillant toutes les données écrites sur tous les membres composant l'agrégat sont perdues. Les volumes agrégés par bandes réunissent dans un seul volume logique des espaces libres situés sur au moins deux disques et 32 au maximum. Les données sont écrites par bandes de 64 Ko. 64 Ko sur le 1er, puis 64 Ko sur le second, puis 64 Ko sur le 3éme...



Pour créer un volume agrégé par bandes, vous devez sélectionner un espace non alloué puis **Action – Toutes les tâches – Nouveau nom** (ou menu contextuel). Dans la fenêtre de l'assistant création d'un nouveau volume cochez **Agrégé par bades**. **Ajoutez** les disques sur lesquels vous souhaitez créer le volume agrégé par bandes. La **taille** qui vous sera proposée par défaut sera toujours égale à l'espace non alloué le plus faible des disques composant votre agrégat. Ensuite affectez une **lettre** de lecteur à votre agrégat, puis le format de fichiers. C'est fini.

Attention : vous ne pouvez pas étendre et mettre en miroir un volume agrégé par bandes.

⇨ Volume Raid 5

Un **volume RAID 5** est un volume constitué de plusieurs disques durs. Une information de parité est inscrite sur un des disques de manière à pouvoir reconstituer les données en cas de panne de l'un des disques. Il y a tolérance de pannes. Il faut au minimum 3 disques durs pour mettre en œuvre ce type de stockage dynamique. Dans ce cas, le RAID 5 est assuré par le système d'exploitation Windows 2003. Le RAID 5 peut aussi être assurer de manière matérielle par une carte contrôleur de disques appropriée, ce qui décharge d'autant le processeur du serveur Windows 2003 et rend inutile le RAID 5 de Windows 2003.

Cette solution revient moins cher que le mirroring en terme d'espace disque occupé par les informations de sécurité. Cette technique permet l'enregistrement d'informations supplémentaires de parité qui sont calculées à partir des données enregistrées. Cela procure une amélioration des performances de lecture/écriture sur le disque. Vous pouvez constater que dans l'exemple ci-dessous où il y a 3 disques durs mis en jeu, 1/3 de la capacité est requise pour le calcul de parité ce qui fait 66% restant pour les données. Plus le nombre de disques constituant l'agrégat sera grand, plus faible sera la perte d'espace. W2003 Server gère le RAID5 de façon logicielle, mais elle ne peut traiter la partition système. Par contre plusieurs constructeurs proposent une solution matérielle qui permet d'englober la partition système.

Créer l'agrégat par bandes avec parité

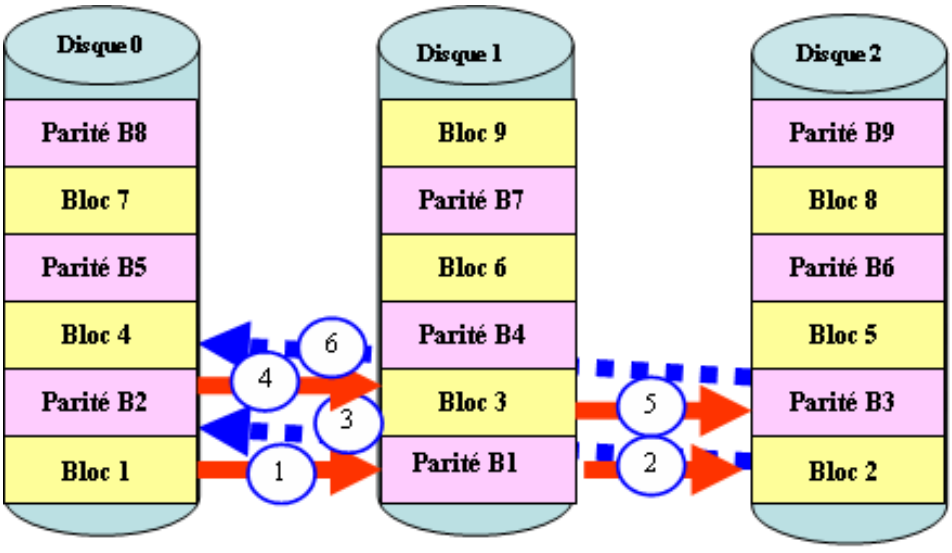
Lancez la console **Gestion des disques**, puis sélectionnez un espace non alloué sur l'un des disques à intégrer au volume RAID5. Validez **Action – Toutes les tâches – Nouveau nom** (ou menu contextuel). Dans la fenêtre de l'assistant création d'un nouveau volume, sélectionnez RAID 5. Validez **Ajoutez des disques** pour définir les disques qui feront partie du volume agrégé par bandes avec parité. Comme précédemment, la taille proposée par défaut est égale à l'espace non alloué sur le plus petit des disques constituant l'agrégat. Terminez cette opération en ayant auparavant choisi une lettre de lecteur et le format pour le système de fichiers.

Récupérer un volume défaillant en RAID5

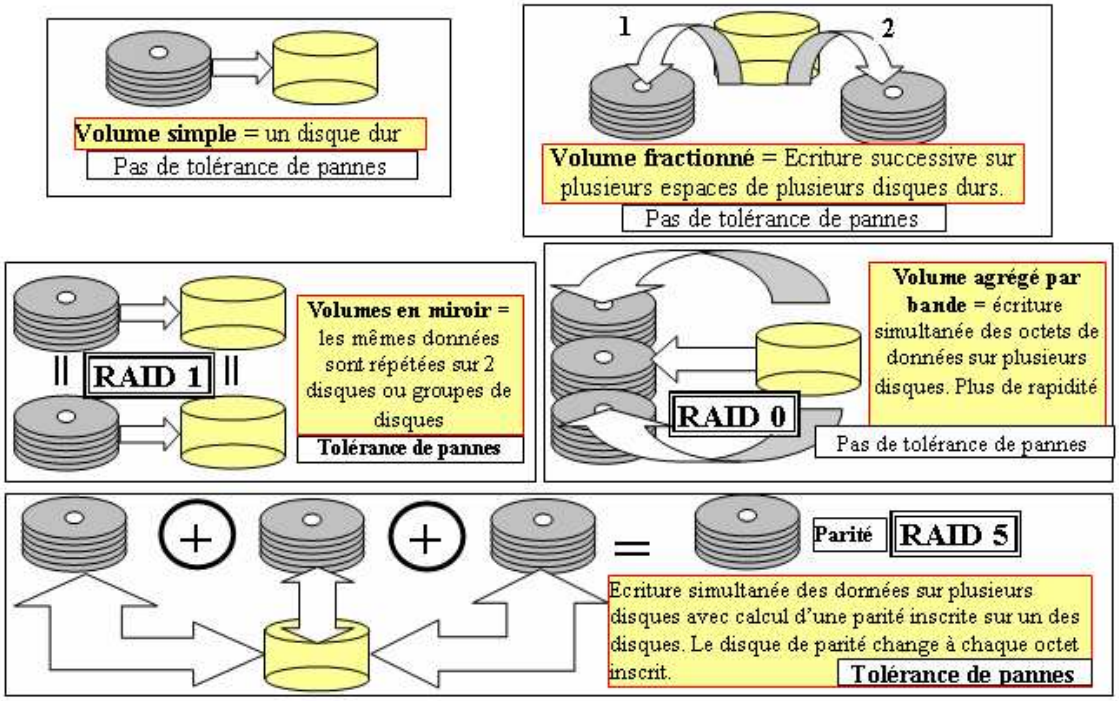
Si un problème survient avec un des disques constituant l'agrégat, les données peuvent toujours être récupérées. Pour cela le driver gérant la tolérance de panne **ftdisk.sys** doit régénérer à partir des informations de parité les informations manquantes ou erronées.

Si vous visualisez qu'un disque est dans l'état **Déconnecté** ou **Absent** vous devez le sélectionner puis validez l'option **Réactiver** le disque du menu **Action**.

Dans le cas où cela ne fonctionne toujours pas, il faut remplacer le disque défaillant.



⇨ Résumé des types de volumes dynamiques



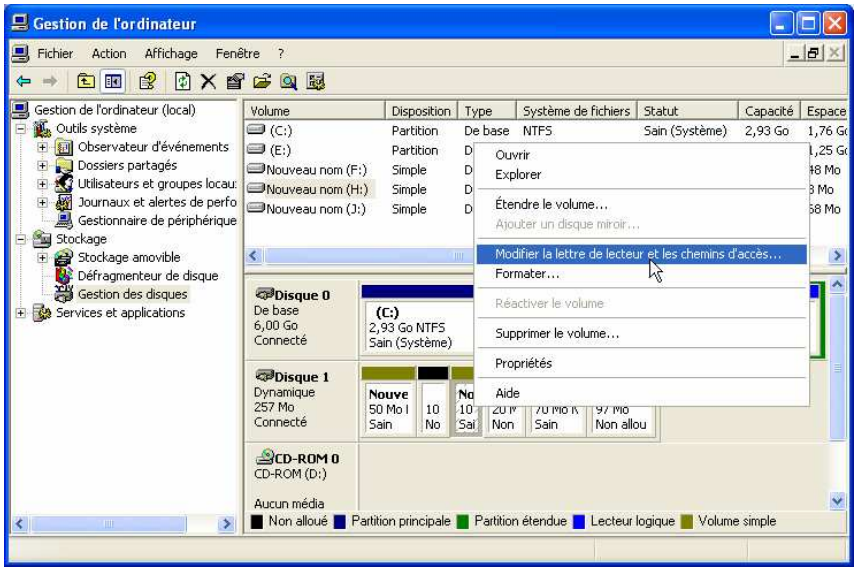
Montage de volumes

A la création d'un volume nous avons la possibilité d'associer une lettre à celui-ci ou bien le monter dans un dossier d'un autre volume NTFS. Cela s'appelle dans le jargon informatique 2003 Server **Montage de volume**. Son avantage essentiel est qu'il permet de dépasser la limité des 26 lettres de lecteurs. Il permet aussi de rediriger un dossier vide vers un autre volume. Cela donne la possibilité de monter des volumes dans des répertoires vides situés sur des partitions ou volumes NTFS en local. Ce qui est intéressant pour l'utilisateur, c'est que bien que ces volumes soient montés dans des partitions ou volumes NTFS, l'utilisateur peut les formater en NTFS ou en FAT ou FAT32.

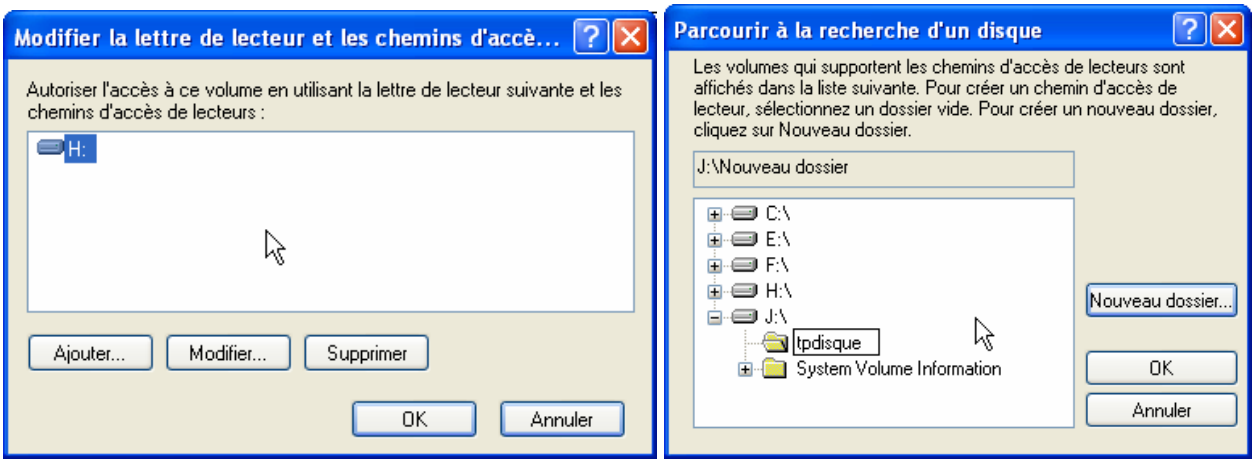
Par contre un volume en FAT ou FAT32 **monté** dans un répertoire NTFS ne pourra pas bénéficier des avantages apportés par ce système de fichiers. En particulier tous les aspects sécurité,

compression, quotas de disques… ne pourront s'appliquer.
L'utilisateur ou les applications accéderont aux volumes montés de façon transparente. Ils auront juste à solliciter le dossier de montage. Cela permet à l'utilisateur de rediriger un répertoire vers un nouveau volume afin d'étendre la capacité, ou bien pour y stocker des données sensibles sur un volume supportant la tolérance de pannes, tandis que le volume hébergeant le point de montage n'est pas tolérant aux pannes.

Création d'un point de montage
Vous pouvez créer un montage de volume ou de partition lors de sa création ou en différé. Pour réaliser cette opération vous devez exécuter la console **Gestion des disques**.
Sélectionnez un volume existant, puis à partir du menu **Action – Toutes les tâches – Modifier la lettre de lecteur et les chemins** (ou menu contextuel).



Une fenêtre affiche les lettres de lecteur et points de montages existants. Vous pouvez à partir de cette fenêtre modifier ou supprimer chacun d'eux. A partir du bouton **Ajouter** ou du bouton **Parcourir** vous pouvez sélectionner ou créer un nouveau dossier sur l'emplacement choisi (uniquement les volumes ou partitions NTFS seront affichés).

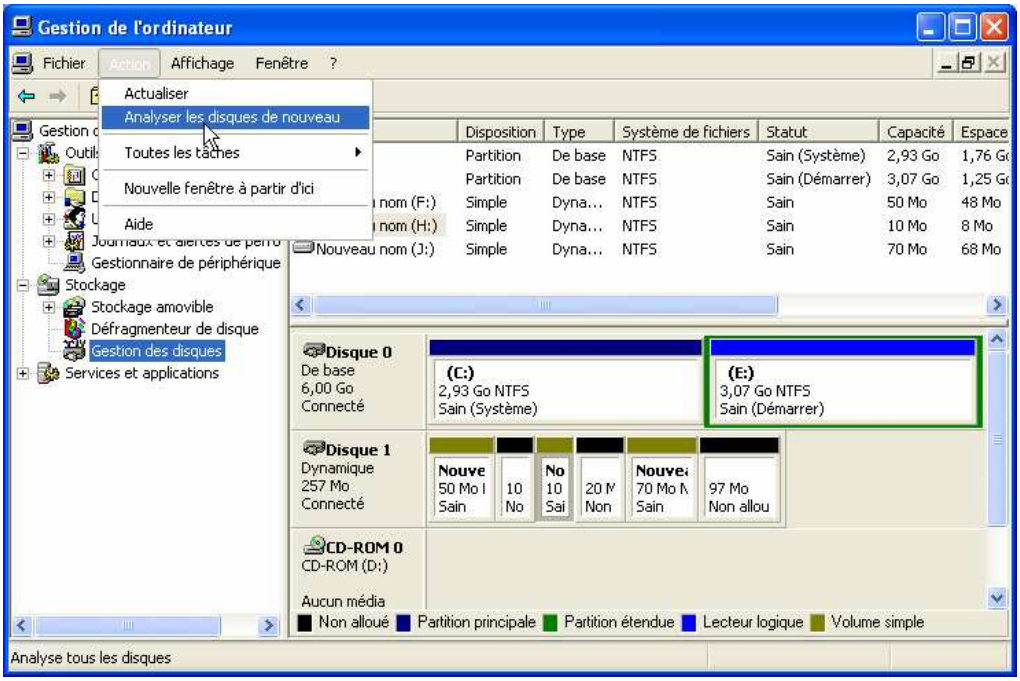


Au final l'icône du dossier correspondant au point de montage est symbolisé par un disque et non par un dossier standard.

Pour supprimer un point de montage sélectionnez le, puis **Action – Toutes les tâches – Modifier la lettre de lecteur et les chemins d'accès** (ou menu contextuel). A partir de la boite de dialogue sélectionnez le point de montage (ou la lettre de lecteur) à retirer, puis validez **Supprimer**.
Lorsque vous supprimez un point de montage, les données sont conservées sur le volume qui était monté. Seul la jonction se trouve supprimez.

4.1.3- Ajout de disques

Pour ajouter un disque sur de nombreux systèmes, il faut éteindre le micro puis installer le nouveau disque dur et redémarrer le l'ordinateur sauf si votre matériel supporte la technologie **Hot plug.** W2003 reconnaît automatiquement le nouveau disque et l'ajoute dans la console **Gestion des disques**. Par contre il peut arriver quelquefois que la reconnaissance soit automatique. Dans ce cas vous pouvez à partir du **Gestionnaire des disques** valider **Action – Analyser les disques de nouveau** (ou menu contextuel). Le nouveau disque devrait apparaître dans la console sans avoir à redémarrer le micro. Au final si ce n'est pas OK vous devez redémarrer le micro. Dans le cas où vous ajoutez un disque dynamique venant d'un autre micro, il sera reconnu automatiquement par le système mais il sera marqué comme **Etranger**. Comme nous l'avons déjà dit au début de ce cours, la topologie des disques dynamiques est enregistrée sur le disque lui-même et non dans le registre. Donc le système sera capable d'importer tout ou partie d'un disque étranger en se l'appropriant (il doit modifier la signature). Pour cela vous devez sélectionner le disque inconnu puis **Action – Importer des disques étranger** (ou menu contextuel). W2003 Server va afficher les informations de signature des disques étrangers. Normalement le disque sera disponible pour travailler.



4.2- Systèmes de fichiers

Système de fichiers FAT
Le système de gestion FAT (File Allocation Table) est simple, car prévu à l'origine pour gérer des disques durs de petites tailles avec des impératifs de sécurité très limités.
Windows 2003 peut utiliser les systèmes de fichiers FAT 16 et FAT 32, mais les dispositifs de sécurité disponibles sur NTFS 5 ne sont pas mis en œuvre.

FAT 16 : avec FAT 16, le nombre de bits utilisés pour décrire l'organisation des répertoires et des fichiers est faible, et on ne peut gérer des partitions dont la taille est supérieure à 4 Go. Ce système est celui utilisé sous DOS, Windows 3.x et dans la première version de Windows 95. Par souci de compatibilité, il peut être utilisé sous Windows 95 OSR2, 98, 95 et même Windows 2003.
Le format des noms de fichiers est 8.3. Les attributs gérés sont A, S, H et R.

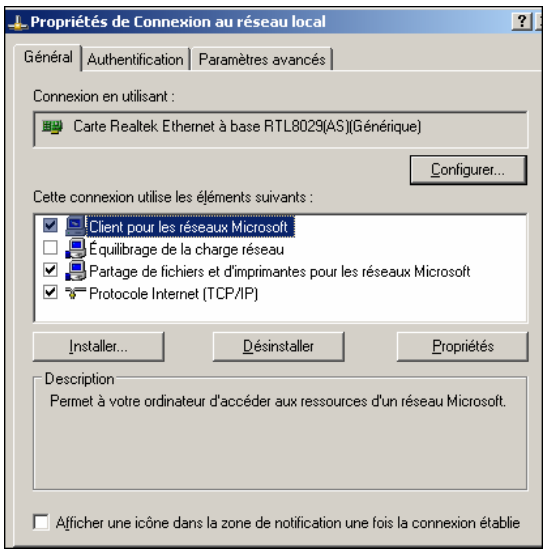
FAT 32 : le système FAT 32 est une extension du système FAT 16. Il permet la gestion des partitions de capacité supérieure à 4 Go, en principe 2047 Go, mais au plus de 32 Go. Il est utilisé sous Windows 95 OSR2 et Windows 98. Il n'est pas reconnu par Windows NT, mais l'est par Windows 2003. Le système FAT 32 gère les noms longs de fichiers.

En résumé, bien qu'il soit possible d'utiliser l'un ou l'autre des systèmes de fichiers FAT sous Windows 2003, il est préférable d'utiliser NTFS 5, **sauf** si l'on désire garder la possibilité d'un **amorçage double** (par exemple Windows 3.11 et Windows 2003).

4.3- Partage de dossiers

L'objectif principal d'un réseau est bien évidemment de pouvoir utiliser les fichiers ou dossiers situés sur un autre ordinateur (station ou serveur). Pour cela l'administrateur ou son équivalent devra mettre en place le partage des ressources afin de les rendre accessibles via le réseau aux utilisateurs. Il mettra ces ressources disponibles avec des droits différents (lecture, lecture, contrôle total…) en fonction du profil des utilisateurs.
Deux grandes familles de sécurité existent dans le monde des réseaux et particulièrement dans le monde Microsoft Windows :

- **Sécurité au niveau ressource :** c'est le type de sécurité des premiers systèmes d'exploitation Windows comme Windows pour Workgroups, Win 9X. Dans cette **topologie** la sécurité d'accès à une ressource est conditionnée par un mot de passe. Ce mot de passe est attribué par type d'accès et par ressource de façon totalement indépendante des utilisateurs (c'est-à-dire indépendant de celui qui accède à la ressource). L'administrateur ou vous-même pouvez décider qu'un répertoire ne sera accessible en accès complet en entrant un mot de passe défini par vous-même, et par contre qu'un autre dossier sera accessible en lecture sans aucun mot de passe. Avec des systèmes d'exploitation comme Windows For Workgroups ou Win 9x la sécurité d'accès à une ressource repose à la saisie d'un mot de passe qui stocké dans un fichier **PWL** (Password List). Avec SMB (Server MEssage Block) un client Windows 2003 pour ce protocole sera nommé **Client pour les réseaux Microsoft.** Le composant serveur sera nommé **Partage de fichiers et d'imprimantes pour les réseaux Microsoft**

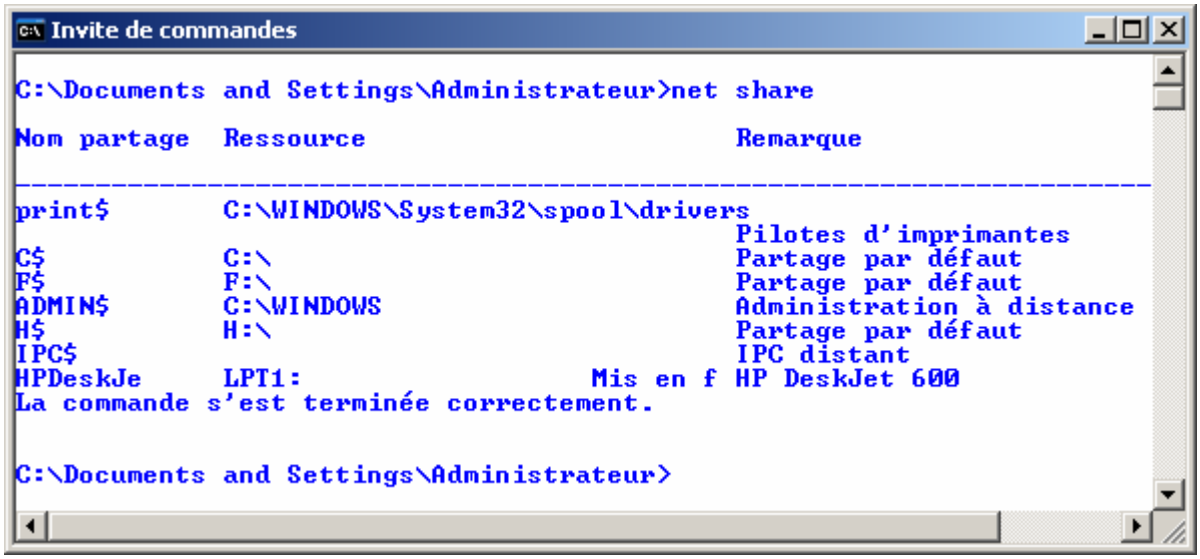


- **Sécurité au niveau utilisateur :** sur les systèmes d'exploitation de type NT, W2000 seule la sécurité au niveau utilisateur est possible. Par contre sous Win95/98 les deux sont possibles. Dans une sécurité utilisateur de type NT ou W2000/2003 vous devez vous authentifier avant de pouvoir prétendre accéder à une ressource partagée. Avec ce mode l'utilisateur va pouvoir être désigné comme utilisateur autorisé à accéder à une ressource avec un type d'accès particulier. En plus les utilisateurs pourront être regroupés en groupe avec pour chacun des types d'accès particuliers.

4.3.1- Partager un dossier

Rappel : comme sous W2K et XP les **fichiers ne sont pas partagés sous** Windows 2003, ce sont uniquement les dossiers.

- Par défaut certaines ressources sont partagées. Elles sont appelées partages administratifs prédéfinis et sont réservées aux administrateurs pour la gestion, et la réalisation de tâches administratives (en particulier pour les stations distantes).
- Ils sont cachés aux utilisateurs sans droits administratifs et uniquement accessibles par l'administrateur ou son équivalent.
- Le caractère **$** rend les partages invisibles avec les Favoris Réseau.
- Par défaut, les administrateurs disposent de l'autorisation **Contrôle total.**



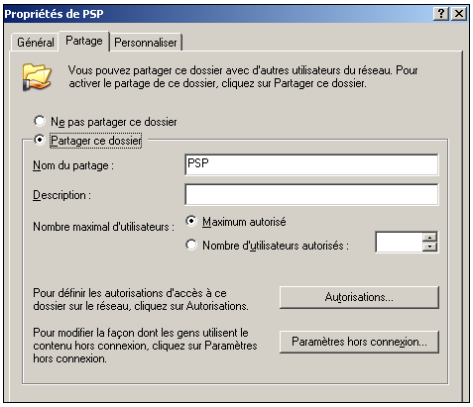
Partage	Objet
C$, D$, E$	La racine de chaque volume est automatiquement partagée. Ceci permet aux administrateurs d'accéder à distance aux volumes des ordinateurs du réseau. L'autorisation Contrôle Total, est accordée aux membres du groupe Administrateurs. Ce partage administratif n'existe pas pour les supports amovibles (CR-ROM, DVD…).
Admin$	Ce partage correspond au dossier qui contient les fichiers système, en principe C:\Winnt. L'autorisation Contrôle Total, est accordée aux membres du groupe Administrateurs.
IPC$	Sert pour la communication entre les processus.
Print$	Le dossier C:\winnnt\System32\Spool\Drivers est partagé à l'installation de la première imprimante sous le nom de partage Print$. Il contient les pilotes d'imprimantes pour Windows 2003. L'autorisation Contrôle Total, est accordée aux membres des groupes Administrateurs, Opérateurs de serveur et Opérateurs d'impression. L'autorisation Lecture Seule est accordée à Tout le Monde.
Netlogon	Ce partage contient les scripts utilisateurs et stratégies pour la compatibilité des clients antérieurs à Windows 2000.
Sysvol	Partage utilisé pour synchroniser des scripts et stratégies du domaine entre les contrôleurs de domaine. Attention car ce n'est pas le premier répertoire Sysvol qui est partagé mais %systemroot%\sysvol\sysvol

Pour partager un dossier sous W2003 vous devez posséder certains privilèges. Sur un contrôleur de domaine vous devez faire partie soit du groupe administrateurs, soit du groupe opérateurs de serveurs. Par contre sur un serveur ou une station travail vous devez être membre du groupe administrateurs ou utilisateurs avec pouvoirs.

Partage à partir de l'Explorateur

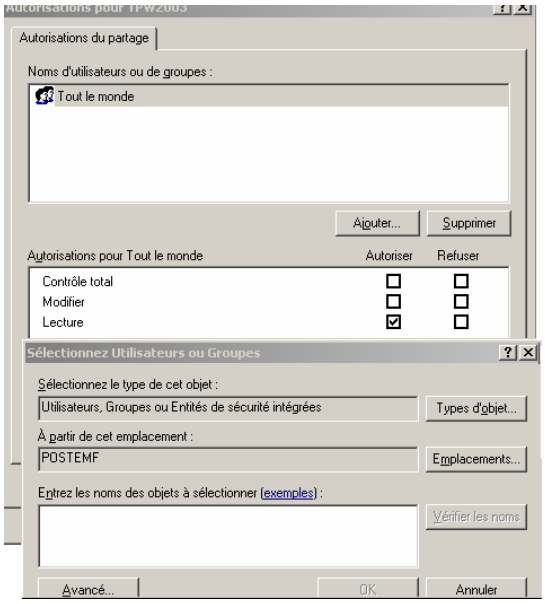
Sélectionnez le dossier à partager, puis menu **Fichier** – **Partage et sécurité** ou à partir du menu contextuel :

- Clic droit dossier à partager ➔ option **Partager**.
- Cochez **Partager ce dossier**.
- Possibilité de changer le nom du partage (visible sur le réseau).
- Commentaire éventuel.
- Possibilité de restreindre ou non le nombre de connexions simultanées sur ce partage. Par défaut la limite est égale à 10 connexions simultanées ce qui correspond au **Maximum autorisé** pour Windows XP ou jusqu'à concurrence des licences pour un serveur W2003.
- Possibilité de plusieurs noms partage différents pour un même dossier.
- Si vous avez (encore) des clients DOS et Windows for Workgroups vous devez utiliser des noms de partages sous la forme 8.3 caractères.



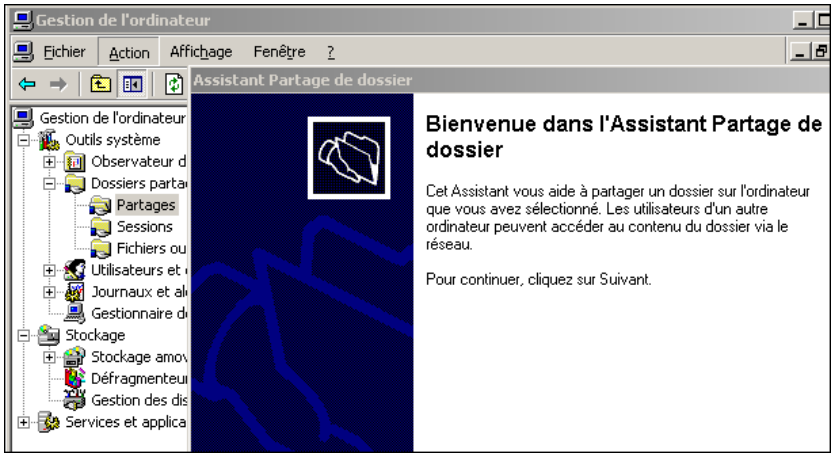
Pour modifier les **Autorisations** d'accès à travers le réseau cliquez sur le bouton **Autorisations.** Par défaut Lecture pour le groupe **Tout le Monde** est appliquée.

- Permissions de dossier partagé :
  - **Lecture**: l'utilisateur peut lire les fichiers, exécuter des programmes et parcourir les sous-dossiers.
  - **Modifier:** Lecture + créer, modifier ou supprimer des dossiers et fichiers.
  - **Contrôle total :** Modifier + droit de changer les permissions.
- Possibilité d'**Autoriser** ou **Refuser** une permission.
- Si appartenance à plusieurs groupes, combinaison des permissions. La permission finale pour l'utilisateur sera une combinaison de ces permissions (en résumé la plus élevée). Avec pour exception le cas ou une permission est positionnée sur la colonne **Refuser**. Dans ce cas **Refuser** est prioritaire.
- Vous avez pour un même dossier le droit de créer plusieurs noms de partage différents. Il vous suffit de cliquer sur le bouton **Nouveau Partage.**
- Possibilité d'**Ajouter** de nouveaux **Utilisateurs** ou groupes d'utilisateurs.

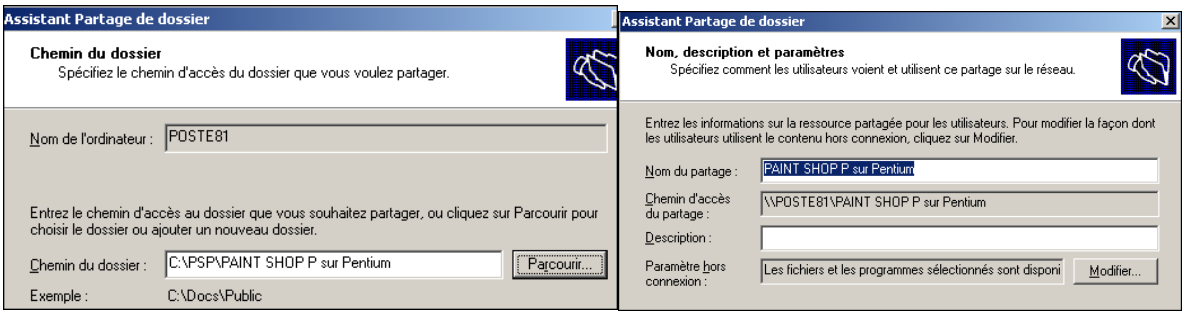


A partir de la console Gestion de l'ordinateur

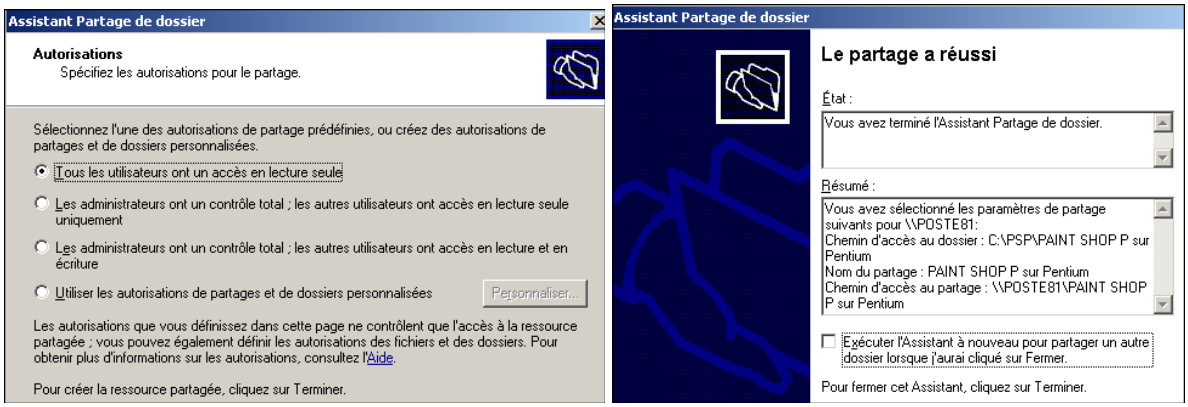
Allez dans la fenêtre **Gestion de l'ordinateur**, puis dans la rubrique **Dossiers partagés**, sélectionnez **Partages**. Allez dans le menu **Action** – **Nouveau partages de fichiers** pour démarrer l'assistant de création d'un partage.



Dans l'écran suivant vous devez saisir le chemin local à partager ou via le bouton **Parcourir** afin d'entrer un dossier existant ou en créer un nouveau.



Ensuite vous devez entrer ou modifier les autorisations à apporter au dossier. Vous pouvez choisir l'un des trois réglages prédéfinis ou personnaliser (Modifier) selon vos souhaits. Au final une fenêtre récapitule l'opération de création du partage.



Cesser ou supprimer un partage

Cette opération est équivalente à en supprimer l'accès à travers le réseau, ainsi que toutes les permissions associées. Vous pouvez réaliser cette cessation de partage soit à partir de l'**Explorateur** ou via la console de **Gestion de l'ordinateur.**

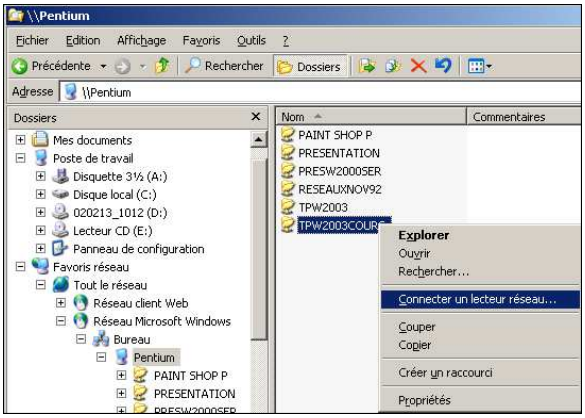
A partir de l'explorateur sélectionnez le **dossier partagé**. Puis à partir du menu contextuel sélectionnez **Propriétés**. Sélectionnez le partage puis cliquez sur le bouton **Supprimer le partage**.

Vous pouvez aussi réaliser cette opération à partir de la fenêtre **Gestion de l'ordinateur**. Dans la rubrique **Outils système – Dossiers partagés – Partage**, sélectionnez le nom du partage à supprimer puis à partir du menu contextuel validez **Arrêter le partage**.

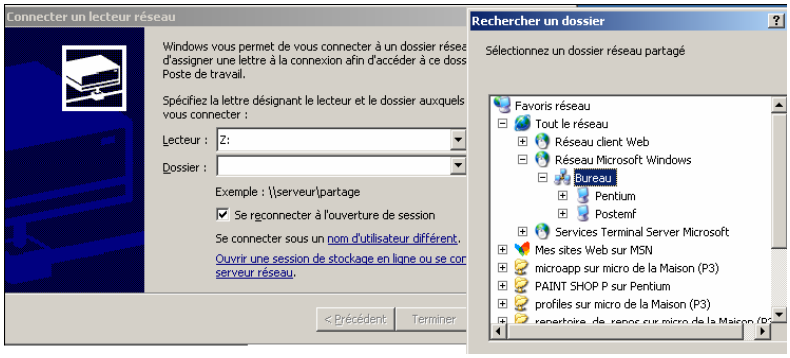
Se connecter à une ressource partagée

Plusieurs possibilités s'offrent à vous pour vous connecter à une ressource partagée sur le réseau.

Vous pouvez par exemple utiliser à partir de **l'Explorateur** la navigation directe avec les noms **UNC**. Sélectionnez **Favoris réseaux – Tout le réseau – Réseau Microsoft Windows**, puis l'endroit où se situe la ressource partagée (domaine ou groupe de travail, puis le nom de machine).



Les ressources mémorisées et déjà partagées apparaissent. Sélectionnez la ressource apparaissant comme déjà partagée. Puis clic droit afin de faire apparaître le menu contextuel. Validez **Connecter un lecteur réseau.**



Ensuite vous devez :

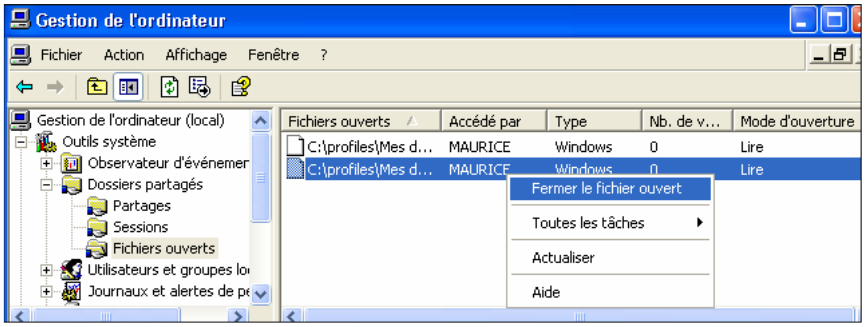
- Choisir une **lettre de lecteur.**
- Choisir le **Chemin de la ressource partagée de type UNC** (\\serveur\partage).
- Cocher **Se reconnecter à l'ouverture de session.**
- La **Possibilité** de se connecter sur un **Nom d'utilisateur différent**.

Le répertoire que vous venez de partager est maintenant accessible par un double clic sur l'icône **Favoris réseau**. L'ajout de favoris réseaux peut se réaliser directement à partir de l'icône **Ajout d'un Favori réseau**.

Contrôler les partages

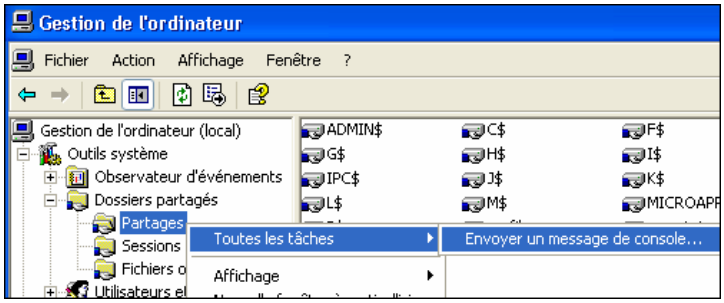
Vous pouvez contrôler les partages à partir de la console **Gestion de l'ordinateur**. Ce contrôle des partages permet à l'utilisateur ou à l'administrateur d'afficher les utilisateurs du réseau accédant à une ressource partagée et permet aussi de contrôler l'accès à cette ressource.

Le dossier **Fichiers ouverts** donne la liste de tous les fichiers ouverts sur le serveur. Vous pouvez directement à partir de cette fenêtre fermer certains fichiers. Avec cette action si le fichier était ouvert en lecture/écriture toutes les modifications seront perdues. Par contre cette connexion ne peut être que temporaire car s'il le souhaite, l'utilisateur peut réutiliser la ressource.

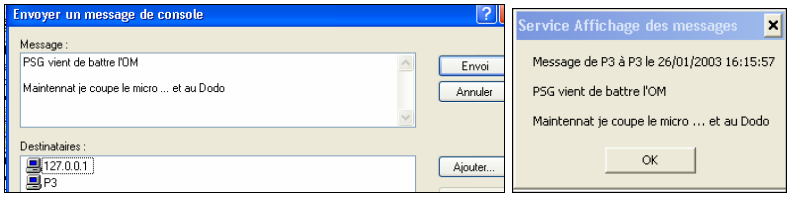


La rubrique **Sessions** permet la visualisation de toutes les sessions ouvertes sur l'ordinateur. En fait vous visualisez toutes les personnes effectuant des connexions sur l'ordinateur.

La rubrique **Partage** permet de partager ou cesser le partage de ressources.



Envoi de messages administratifs
Avec la console **Gestion de l'ordinateur** vous pouvez envoyer un message pour prévenir les utilisateurs. Vous pouvez les inviter au café… ou si vous êtes technicien de maintenance vous pouvez les prévenir que vous allez couper le serveur et qu'ils doivent sauvegarder leurs données. A partir de la rubrique **Dossiers partagés** (ou menu contextuel), **Action – Toutes les tâches – Envoyer un message de console** – puis saisissez votre message. Dans la fenêtre inférieure (**Destinataires**) apparaît toutes les stations connectées. Utilisez les boutons **Ajouter** ou **Supprimer** pour modifier la liste.



Le service **Affichage** de message doit être démarré sur les postes destinataires.

4.4- Système de fichiers NTFS

Ce système de fichiers existait déjà sous NT4, mais on le trouve dans sa version 5 sous Windows 2003. Le formatage NTFS 5 est recommandé par Microsoft, car il permet des fonctions supplémentaires par rapport aux systèmes FAT :

- De récupération des données.
- De compression dossier par dossier en temps réel.
- De limitation de la capacité disque par utilisateur (quotas de disque).
- D'individualisation des répertoires du disque (sécurité individuelle).
- De sécurité. Les autorisations NTFS sur les dossiers et les fichiers garantissent leur accès aussi bien par rapport aux utilisateurs travaillant sur l'ordinateur qu'à ceux qui y accèdent par le réseau.
- D'encryptage, NTFS 5 permet d'encrypter les données inscrites sur les partitions.

4.4.1- Structure du système de fichiers NTFS 5

Structure de volume ou de partition
NTFS 5 utilise des clusters (ou unités d'allocation) constitués de un ou plusieurs secteurs. La taille des clusters varie en fonction de la taille de la partition NTFS. Par exemple, pour une partition de 512 Mo, il n'y qu'un secteur par cluster et la taille de ce cluster est de 512 octets. Pour une partition (stockage de base) ou un volume (stockage dynamique) de 32 Go, il y a 128 secteurs par cluster et la taille des clusters est donc de 64 Ko.

Secteur d'amorçage
Le secteur d'amorçage contient le code qui permet de localiser et charger les fichiers de démarrage de Windows 2003 tel que le fichier **Ntdlr**.

MFT (Master File Table)
Cette table contient pour chaque volume les informations concernant chaque fichier : son nom, sa taille, sa date de création et celle de mise à jour, les autorisations, les attributs et autres.
Pour chaque répertoire et chaque fichier, il y a un enregistrement dans la table MFT.

Conversion d'un volume au format NTFS
La conversion FAT (16 ou 32) vers NTFS est possible sans perte de données. Pour cela vous devez exécuter l'utilitaire nommé **Convert.exe** qui se trouve dans le dossier %systemroot%. Lorsque vous convertissez un volume avec cet outil, la structure des fichiers et des répertoires est préservée et aucune donnée n'est perdue.

Syntaxe complète de la commande :
CONVERT Volume /FS:NTFS [/V] [/X] [/CvtArea :nomfichier] [NoSecurity]

Volume:	spécifie la lettre de lecteur (C:, D: …) ou le nom de volume.
/FS:NTS	spécifie que le volume va être converti en NTFS.
/V	indique que CONVERT va s'exécuter en mode bavard.
/X	force le démontage du volume avant la conversion (si nécessaire).
/CvtArea : nomfichier	définit le nom d'un fichier à secteurs contigus dans le répertoire racine qui recevra les fichiers système NTFS.
/NoSecurity	supprime tous les attributs de sécurité et rend les fichiers et les répertoires accessibles au groupe Tout le monde.

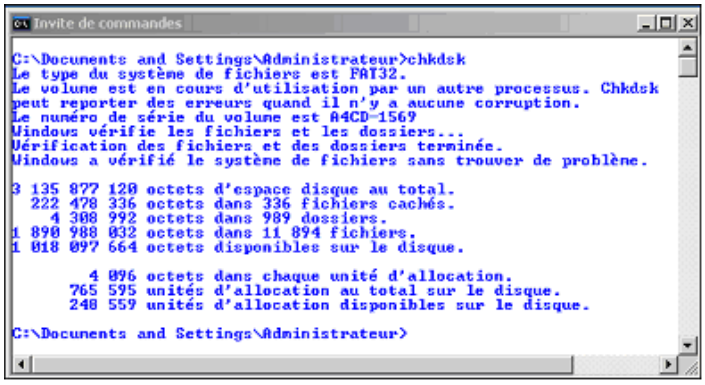
Par contre le passage de NTFS vers FAT n'est pas possible.

Solution : sauvegarde complète de vos données, formater une nouvelle partition en FAT, restaurer vos données sur cette partition.

Exécution de Check Disk depuis la ligne de commande

Cet utilitaire peut être exécuté à partir de l'invite de commande ou depuis d'autres utilitaires. A partir de l'invite de commande tapez : **CHKDSK** pour vérifier le lecteur courant.
Cette commande possède de nombreuses options :

Volume:	indique le volume à manipuler.
Nomdefichier	FAT/FAT 32 uniquement : indique les fichiers à contrôler du point de vue de la fragmentation.
/F	Répare les erreurs du disque.
/V	sur FAT/FAT 32 : affiche le chemin d'accès complet et le nom de chaque fichier du disque. Sur NTFS : affiche les éventuels messages de nettoyage.
/R	Localise les secteurs défectueux et récupère les informations lisibles (implique l'utilisation du commutateur /F).
/L :taille	NTFS seulement : modifie la taille du fichier journal.
/X du	Entraîne le démontage préalable du disque si nécessaire (implique l'utilisation commutateur /F).
/I	NTFS seulement : effectue une vérification minimale des entrées d'index.
/C	NTFS seulement : saute la vérification des cycles au sein de la structure de dossiers.



Exécution de Check Disk de manière interactive

Vous pouvez exécuter Check Disk de manière interactive à l'aide de l'**explorateur** de Windows ou de l'outil **Gestion des disques**. A partir du lecteur à tester, cliquez droit dessus puis sélectionnez **Propriétés**, puis cliquez sur **Vérifier maintenant**. Dans la fenêtre interactive Check Disk vous pouvez cocher :

- Rechercher et tenter une réparation des secteurs défectueux.
- Réparer automatiquement les erreurs du système de fichiers.

4.5- Système de fichier CDFS

Windows 2003 prend en charge les CD-ROM et les DVD.

4.5.1- CDFS

Windows 2003 permet la lecture des CD-ROM conformes aux normes ISO 9660 et ISO 9660 niveau 2 avec noms de fichiers longs. Les noms des fichiers et répertoires doivent être en majuscules.

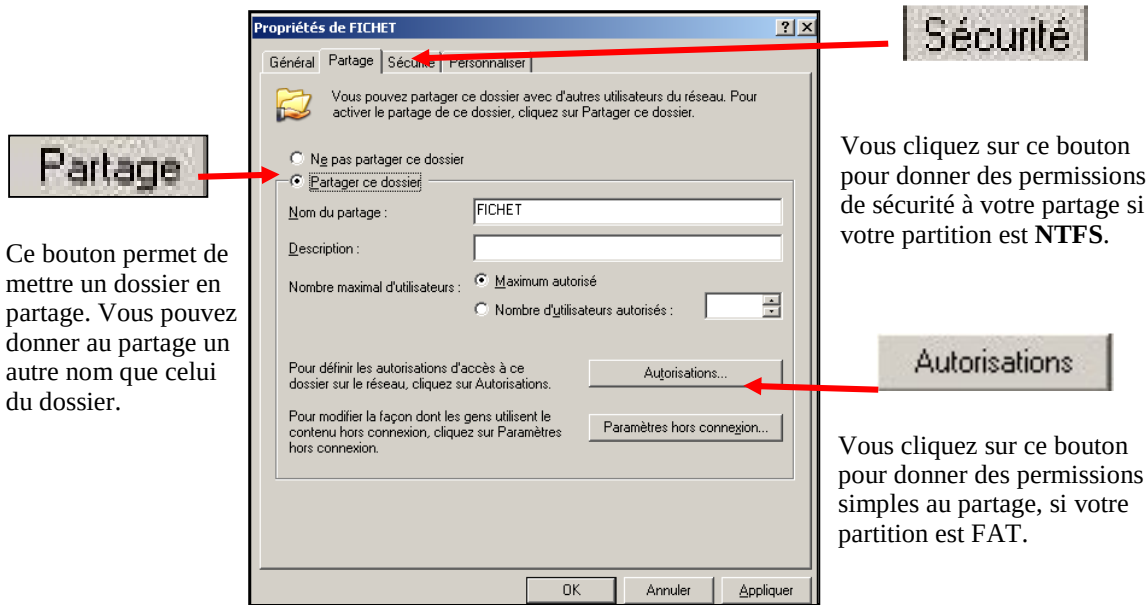
4.5.2- UDF

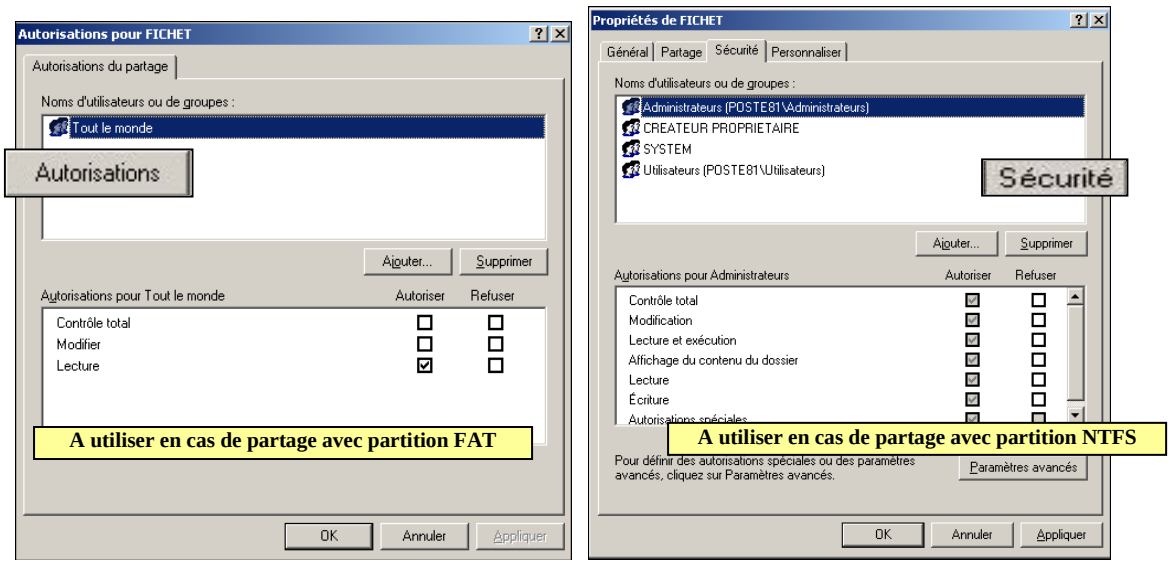
Le format UDF (Universal Disk Format) permet la lecture de certains CD-ROM, mais surtout des DVD (Digital Versatil Disc). Il permet aussi l'écriture sur des supports réinscriptibles CD-RW ou à écriture unique CD-R ou WORM (WriteOnce Many Read). Le système Windows 2003 permet la lecture directe de ce type de support. Pour l'écriture, il faut lui adjoindre une application spécifique (type NERO). La prise en charge des DVD en lecture seule permet de disposer de supports de grande capacité. Ainsi, le support technique Microsoft TechNet est fourni sur ce support.

4.6- Sécurité des systèmes de fichiers

Les permissions vues précédemment s'appliquent aux utilisateurs accédant aux ressources via le réseau. Par contre aucune limite de partage n'est mise en œuvre pour les utilisateurs accédant localement à l'ordinateur. Nous allons voir comment sécurisé les données contre un accès non autorisé et cela localement. Cela n'est possible qu'avec le système de fichier NTFS car il permet la mise en œuvre des attributs de sécurité et d'audit. NTFS permet de maintenir à jour par fichier ou dossier une liste de contrôles d'accès ou ACL contenant au niveau système de fichiers les numéros d'utilisateurs (SID), ainsi que leurs permissions sur la ressource. Les systèmes de fichiers utilisés sur Windows 2003 permettent le partage des dossiers et de leur contenu. Ceci permet aux utilisateurs en réseau de travailler sur les fichiers du serveur Windows 2003. L'accès aux répertoires partagés ou non, d'un serveur Windows 2003 est régit par des **autorisations**. On distingue les **autorisations simples**, utilisées pour les partitions **FAT** et les **autorisations de sécurité** utilisables uniquement avec les partitions **NTFS**.

4.6.1- Autorisations simples pour les dossiers partagés



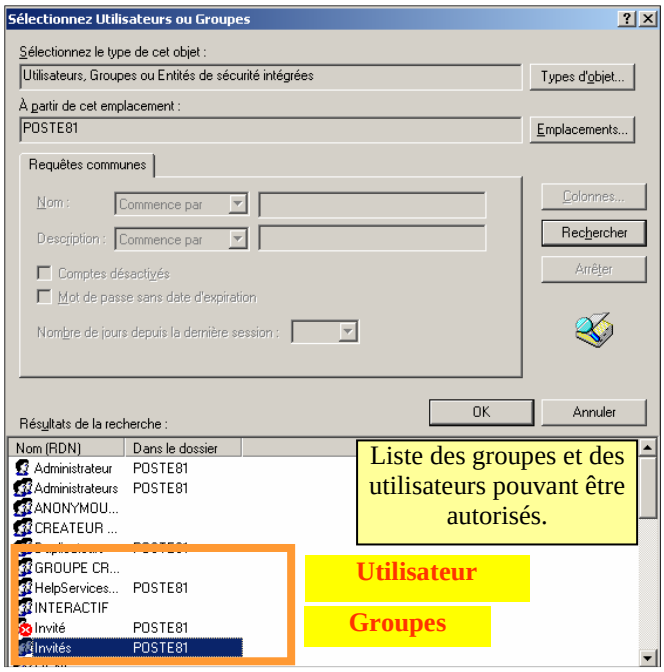


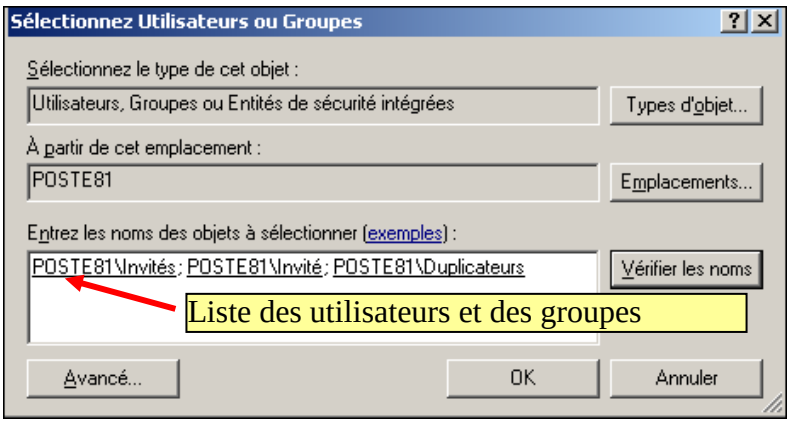
Les autorisations simples s'appliquent aux dossiers, en aucun cas aux fichiers. Elles s'appliquent aux utilisateurs utilisant le partage à partir du réseau, mais pas aux utilisateurs ayant ouvert une connexion sur la station. L'autorisation appliquée par défaut est **Contrôle total** et elle est donnée au groupe **Tout le monde**. L'icône d'un dossier partagé est la suivante dans l'explorateur Windows. Un dossier peut être partagé avec des autorisations et des noms différents pour des utilisateurs ou des groupes distincts. Il est possible de limiter l'accès à un partage à un nombre donné d'utilisateurs (bouton nombre d'utilisateurs du panneau partage).

Il existe **3 types d'autorisations simples** :

Lecture	Les utilisateurs peuvent afficher les noms des dossiers et des fichiers, lire ou exécuter les fichiers.
Modifier	Donne l'autorisation de lecture, plus la possibilité de modifier le nom des dossiers et des fichiers, ainsi que leur contenu.
Contrôle total	Donne l'autorisation de modifier, plus l'autorisation de modifier les autorisations sur le partage.

Ces autorisations peuvent être accordées soit à des groupes, soit à des utilisateurs particuliers.



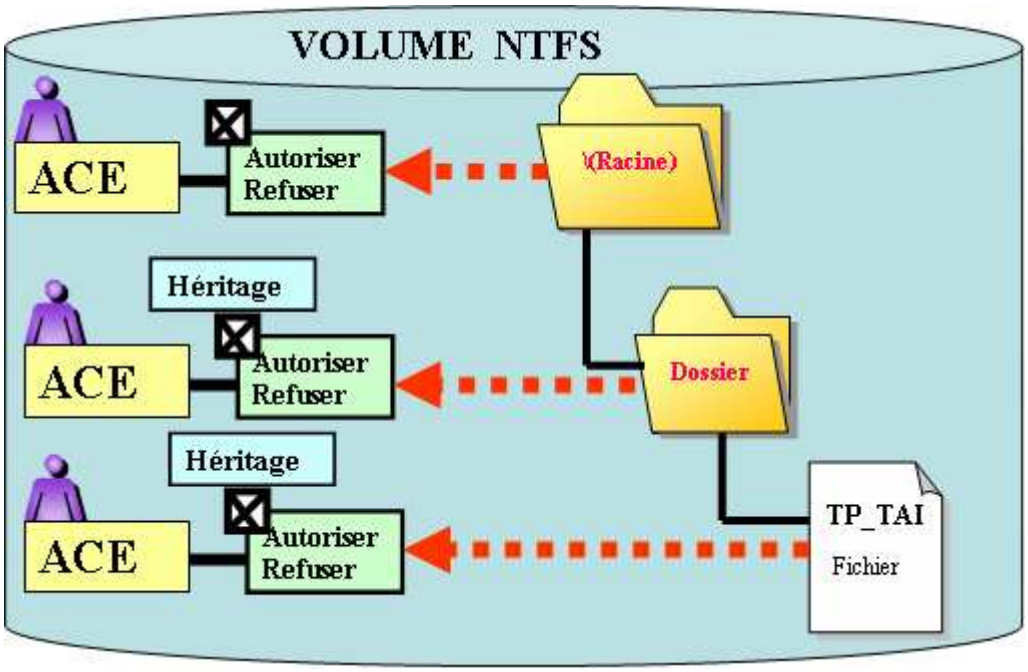


4.6.2- Autorisations NTFS

Comme les autorisations sur les partages, les listes de contrôles d'accès (ACL) reposent sur deux éléments :

- Les entrées de contrôle d'accès (ACE) qui correspondent à des comptes d'utilisateurs, d'ordinateurs ou des groupes.
- Les autorisations NTFS standard ou spéciales qui sont données ou refusées par chacune des entrées ACE.

Ces listes de contrôles d'accès sont établies à chaque niveau du volume NTFS, en partant de la racine du disque dur pour aller jusqu'au niveau le plus profond c'est-à-dire le fichier.
En standard sous W2000/2003 les listes de contrôle d'accès de chaque niveau se cumulent avec l'ACE du dossier parent. Cette notion déjà en vigueur sous NT4 se nomme l'héritage auquel il faudra ajouter ou prendre en compte les autorisations explicites. Celles-ci étant définies au niveau d'un dossier ou d'un fichier tandis que celles héritées proviennent des parents (ou grands-parents...). Le cumul de tous ces droits explicites et hérités donne les autorisations effectives.



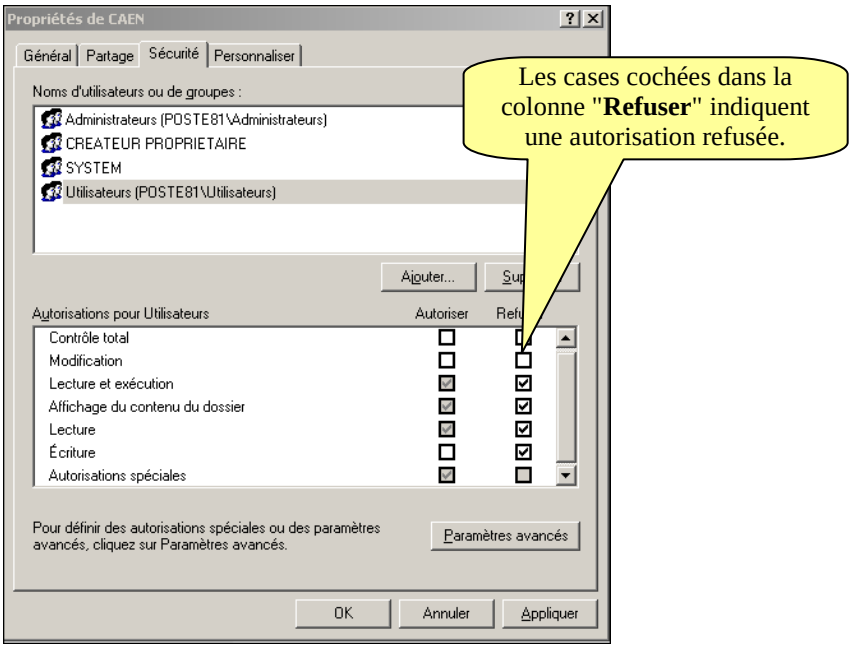
Lorsqu'un utilisateur veut accéder à une ressource, un calcul de ses autorisations va être effectué par le système afin de déterminer les autorisations effectives qu'il va avoir sur cette ressource. Ce calcul est fait en prenant en compte ses appartenances aux différents groupes et les refus qui sont prioritaires sur les attributions. Les autorisations NTFS assurent la sécurité d'accès des dossiers partagés et des fichiers.

On distingue :

- Les **autorisations de dossiers** NTFS. Elles sont accordées soit dans le panneau **Partage**, onglet **Sécurité**, soit dans le panneau **Propriétés** du dossier, onglet **Sécurité**. Pour affecter des permissions NTFS sur un fichier ou un dossier, il faut soit en être le **propriétaire**, soit être **l'administrateur** ou avoir les **autorisations** requises. Ces autorisations sont **Contrôle total**, **Modifier les autorisations** ou **Appropriation** (autorisation permettant de devenir le propriétaire d'un document).
- Les **autorisations de fichiers** NTFS. Elles sont accordées dans le panneau **Propriétés** du fichier, onglet **Sécurité**.

Les autorisations de base sont des autorisations pratiques à utiliser qui regroupent des autorisations avancées (ou individuelles). Les autorisations de base sont légèrement différentes sur les dossiers et les fichiers.

Autorisation sur un Dossier



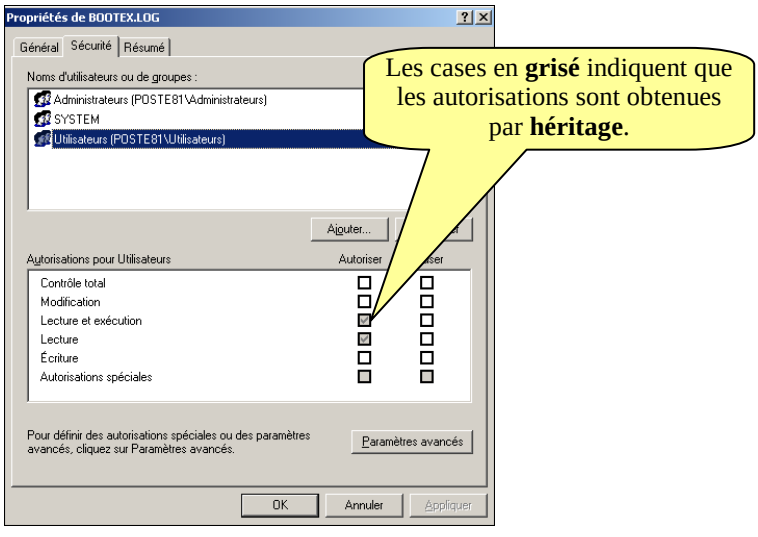
- **Ecriture** : créer des fichiers et des dossiers et modifier les attributs.
- **Lecture** : lire le contenu du dossier et les fichiers du dossier ainsi que les attributs.
- **Affichage du contenu du dossier** : **Lecture** + droit de parcourir le dossier.
- **Lecture et exécution : Lecture** + **Affichage du contenu du dossier** + droit de se déplacer à travers les dossiers pour atteindre d'autres fichiers et dossiers.
- **Modification : Lecture** + **exécution** + droit de supprimer le dossier.
- **Contrôle Total : Toutes les permissions précédentes** + changer les permissions + prendre possession + supprimer.
- **Autorisation Spéciale :** ce n'est pas une autorisation standard. Elle correspond à une combinaison spéciale d'attributs NTFS.

Chacune de ces autorisations résulte de la combinaison d'attributs NTFS. Si vous voulez connaître la liste des attributs utilisés pour une autorisation, affectez une autorisation à l'utilisateur (et seulement une) puis cliquez sur le bouton **Paramètres avancés.**

Certaines autorisations (autorisation ou refus) peuvent être grisées et ne peuvent être modifiées. Cela vient du fait que ces autorisations proviennent du dossier parent et ne peuvent modifiées que si l'héritage est rompu.

Autorisations sur un fichier

- **Ecriture** : permet d'écrire dans le fichier, de changer les attributs, visualiser les autorisations et le propriétaire du fichier.
- **Lecture** : permet de lire le fichier, ses attributs ainsi que les autorisations associées et le propriétaire.
- **Lecture et exécution :** c'est l'autorisation Lecture avec en plus l'autorisation d'exécuter les programmes.
- **Modification :** permet en plus des autorisations **Ecriture** et **Lecture** + **exécution** de supprimer les fichiers.
- **Contrôle Total : toutes les permissions précédentes** + changer les autorisations + prendre possession du fichier.
- **Autorisations Spéciales :** ce n'est pas une autorisation standard. Elle correspond à une combinaison spéciale d'attributs NTFS.



Autorisations avancées

Au cas où les autorisations standard ne vous conviennent pas vous pouvez toujours établir vos propres autorisations en combinant les attributs NTFS. Bien évidemment ne créez pas d'incohérence.

Pour cela ouvrez la fenêtre **Propriétés** de la ressource sur laquelle vous souhaitez appliquer les autorisations NTFS. Activez l'onglet **Sécurité** puis ajoutez l'utilisateur ou le groupe d'utilisateurs concerné par l'autorisation. Sélectionnez cet utilisateur ou ce groupe puis cliquez sur le bouton **Paramètres Avancés**.

La fenêtre ci-dessous s'ouvre. Vous retrouvez dans les colonnes **Type**, **Nom** et **Autorisation** les autorisations et utilisateurs affichés dans la fenêtre précédente mais avec plus de détail.

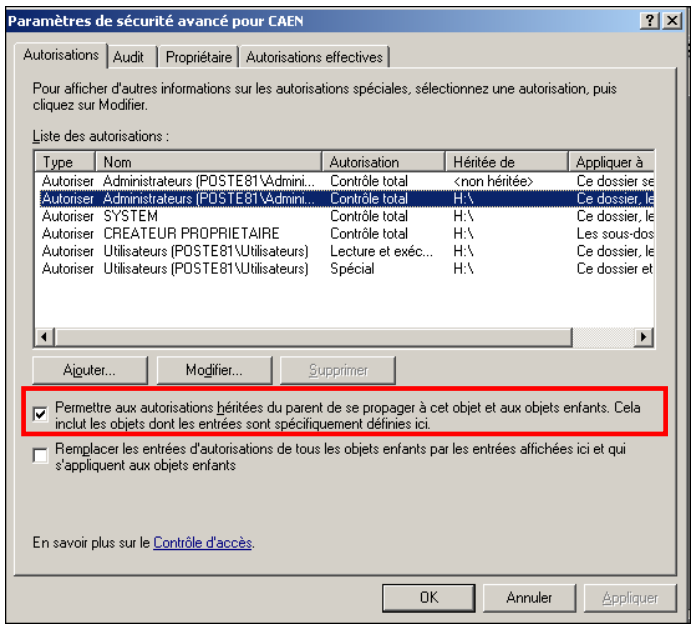
La colonne **Héritée** indique la provenance des autorisations. Cela vous aidera dans la recherche du niveau de dossier sur lequel les autorisations ont été appliquées et à quel niveau vous pouvez les bloquer.

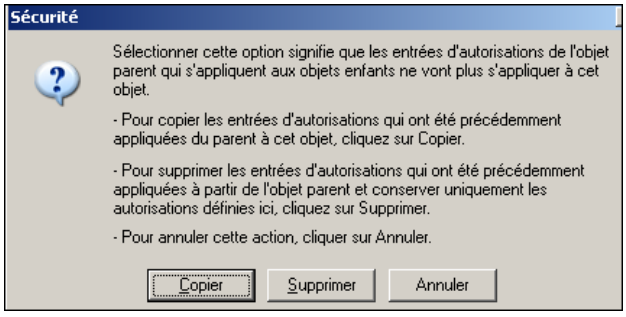
Lorsque le libellé <**non héritée**> est mentionné cela indique que l'autorisation est **explicite** donc au niveau de la ressource en cours de consultation.

La colonne **Appliquer** indique l'étendue d'application de l'autorisation. Lorsque vous ajoutez une autorisation vous pouvez indiquer à quels objets elle s'applique.

La case à cocher **Permettre aux autorisations héritées du parent de se propager à cet objet et aux objets enfants** force la fonction **d'héritage** (est cochée par défaut). Cela a pour effet que les autorisations mentionnes sur les niveaux supérieurs (parents) sont cumulés avec les autorisations explicites sur l'objet courant.

Si vous souhaitez modifier une autorisation héritée vous ne pouvez pas le faire sans avoir auparavant rompu l'héritage en **décochant** l'option **Permettre aux autorisations héritées du parent de se propager à cet objet et aux objets enfants.** Aussitôt vous verrez une fenêtre s'ouvrir vous demandant comment vous souhaitez traiter les autorisations qui ne seront plus héritées.





Copier : si vous validez ce bouton l'intégralité des autorisations qui provenaient de l'héritage sera conservée, mais vous pouvez ensuite les modifier ou les supprimer. Les autorisations deviennent de ce fait explicites à l'objet.
Supprimer : si vous validez ce bouton vous allez détruire l'intégralité des autorisations provenance de l'héritage. Vous devrez manuellement ajouter les nouvelles autorisations explicites car sans cela il n'y a plus personne qui peut accéder à cet objet.

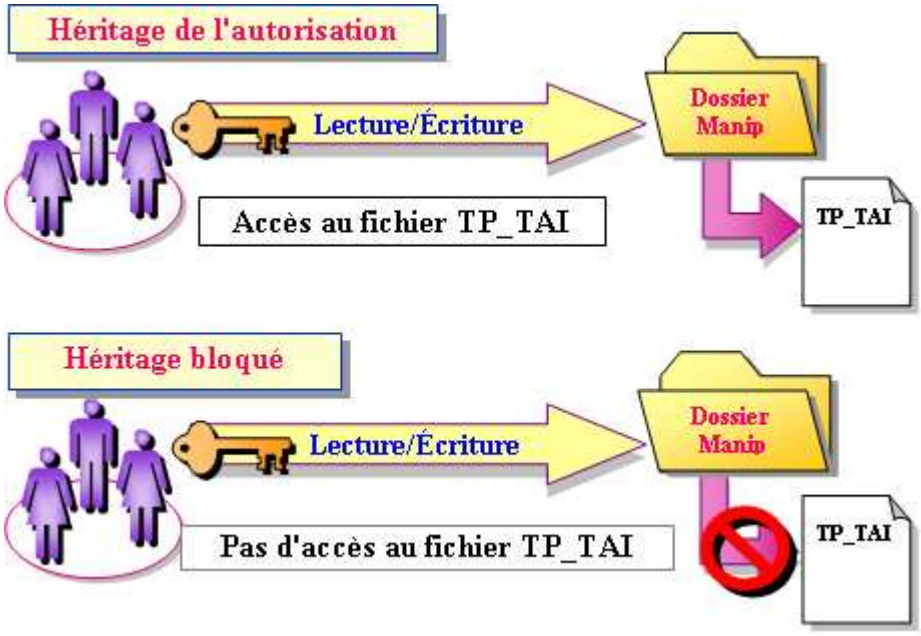
Règles concernant les autorisations NTFS

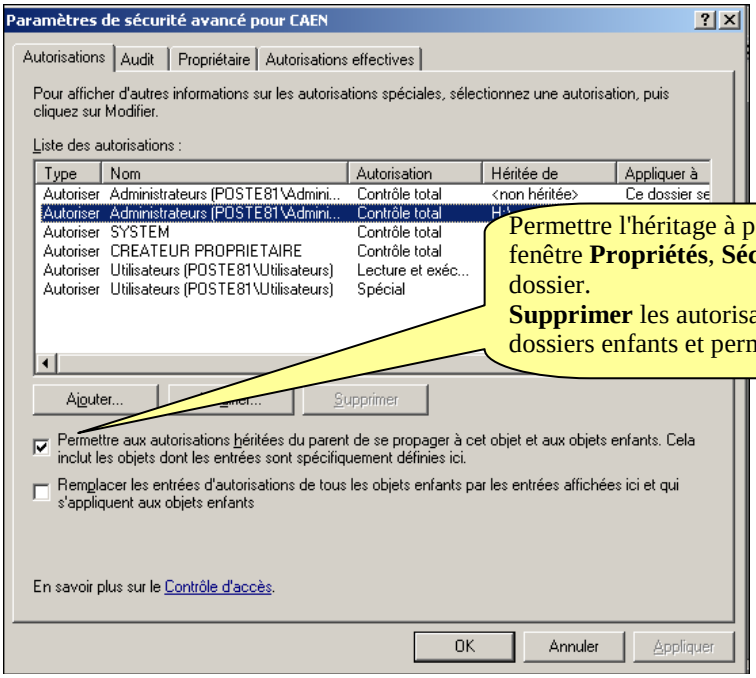
Contrôle total : cette autorisation accorde toutes les autorisations d'accès à un dossier ou à un fichier. Par défaut, elle est attribuée de la manière suivante :

- Lorsqu'un utilisateur crée un dossier ou un fichier. Il en est le propriétaire créateur.
- Lorsqu'un volume est formaté en **NTFS**, l'autorisation NTFS est accordée à **Tout le monde** sur le répertoire racine.

Autorisations multiples : des autorisations sur un dossier ou un fichier peuvent être accordées à un groupe ou à un utilisateur. L'autorisation qui en résulte est la combinaison des différentes autorisations.

- Si un utilisateur fait partie d'un groupe qui a l'autorisation de lecture sur un dossier, et qu'il a lui-même l'autorisation d'écriture, il a en fait les autorisations de lecture et d'écriture. Les autorisations d'utilisateur et de groupe se cumulent.
- Une autorisation accordée à un utilisateur sur un fichier est prioritaire à une autorisation accordée sur un dossier qui contient ce fichier. Les autorisations de fichiers sont prioritaires sur les autorisations de dossier.
- Les sous-dossiers héritent par défaut des autorisations accordées au dossier parent. Il est possible de supprimer cet héritage.



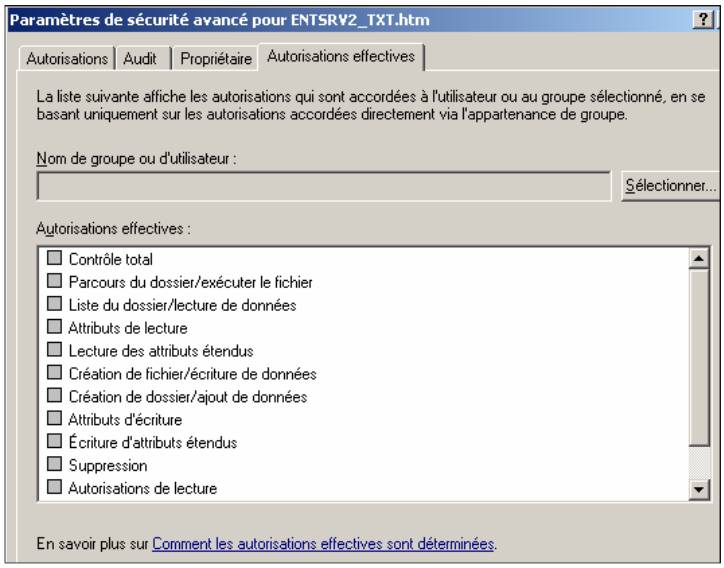


Héritage des autorisations

Le **propriétaire** d'un dossier (ou d'un fichier) ou un **administrateur** ou un utilisateur ayant l'autorisation **Contrôle total** peuvent accorder, supprimer ou modifier des autorisations sur ce dossier ou ce fichier.

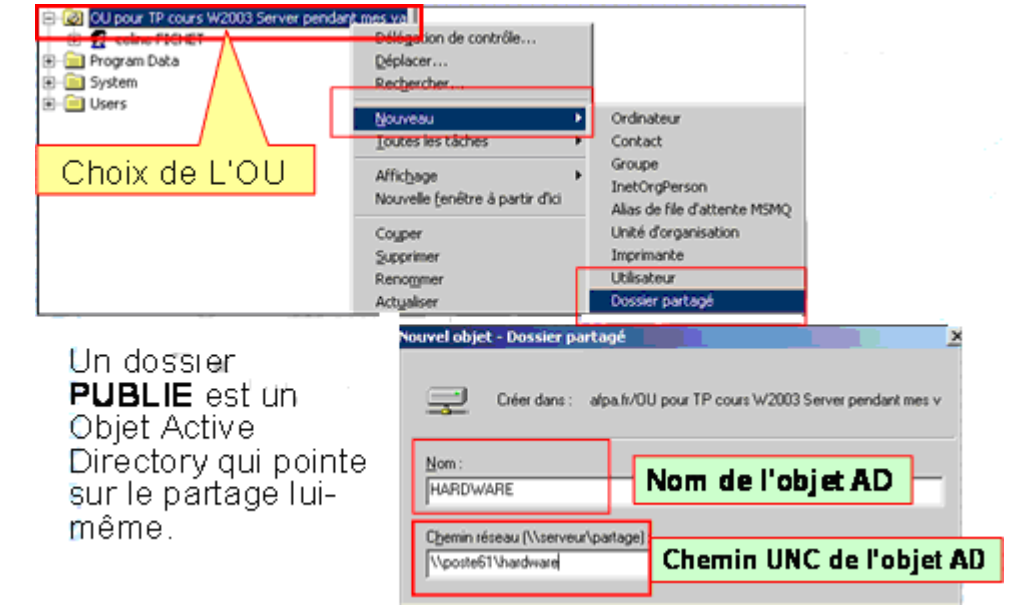
Si un utilisateur est le propriétaire d'un dossier (ou d'un fichier), il peut accorder des autorisations à d'autres utilisateurs. Un administrateur n'a pas forcément des autorisations sur un dossier ou fichier dont il n'est pas propriétaire. Pour changer les autorisations sur ce dossier ou fichier, il doit d'abord en devenir propriétaire en utilisant l'onglet **Propriétaire** de la fenêtre **Propriétés** d'un dossier ou d'un fichier.

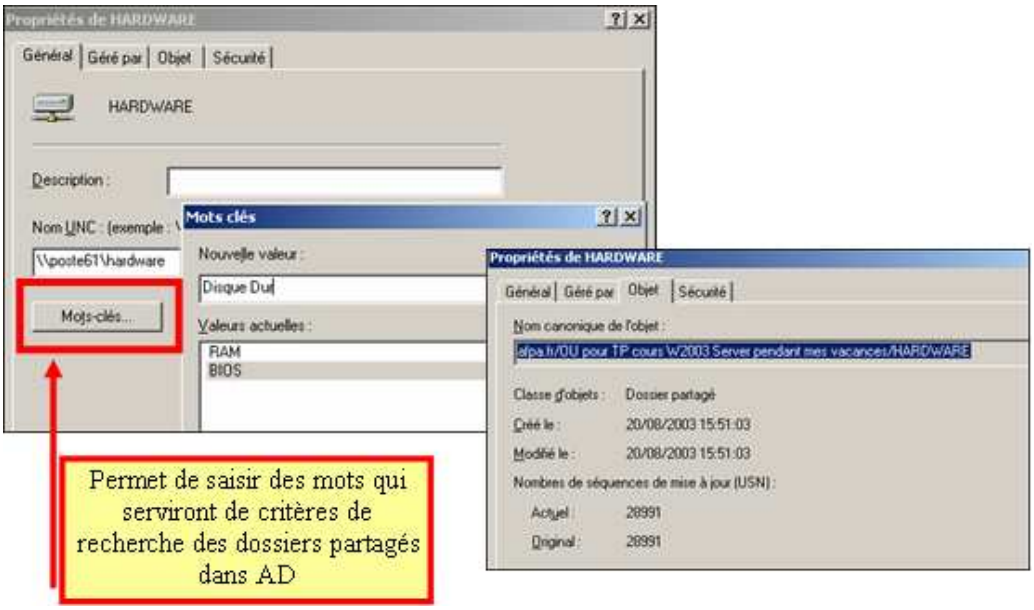
Depuis Windows XP la fenêtre de sécurité d'un fichier ou d'un dossier **Paramètres Avancés** comporte un onglet supplémentaire **Autorisations effectives.** Cet onglet vous permet de calculer les autorités dont dispose un utilisateur ou un groupe sur un dossier ou un fichier en tenant compte de toutes les sources d'autorisation possibles.



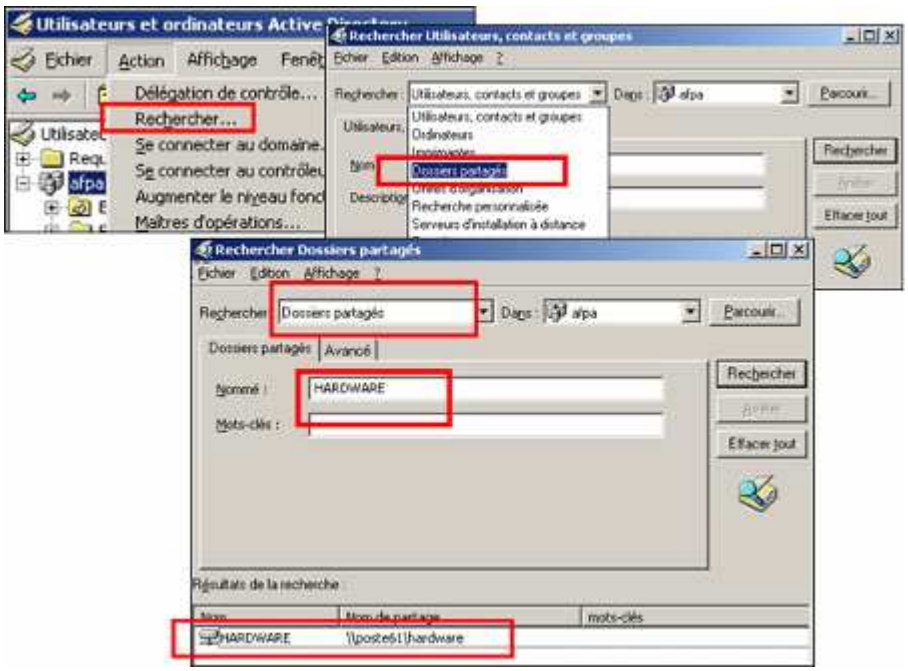
4.6.3- Partage et publication des dossiers

Vous avez la possibilité d'accéder aux dossiers partagés par l'icône **Favoris Réseau** ou Voisinage Réseau. Vous pouvez de cette façon afficher toutes les ressources partagées des serveurs du réseau.
C'est le service **Explorateur** qui est exécuté grâce au protocole NetBios disponible pour tous les protocoles (NetBeui, Nwlink compatible IPX/SPX et TCP/IP).
Depuis W2000 il est possible de désactiver NetBios sur TCP/IP. Cela invalide le service explorateur.
Active Directory permet de faire des recherches sur les dossiers partagés dans tout le domaine et uniquement sur les dossiers dont l'utilisateur a un minimum de droit de lecture.
Cette technique ou outil de recherche porte le nom de publication de ressources. Ces ressources peuvent être des dossiers partagés ou bien des imprimantes.



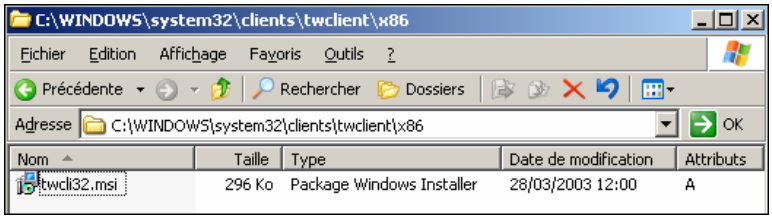


La recherche de dossiers partagés peut se faire dans toute la forêt, le domaine ou dans une UO. Cette recherche peut être réalisée sur le nom du dossier publié et/ou sur des critères de mots-clés.
Le résultat de la recherche affichera les objets existants par rapport à la sélection mais sera fonction des droits sur ces objets de l'utilisateur.

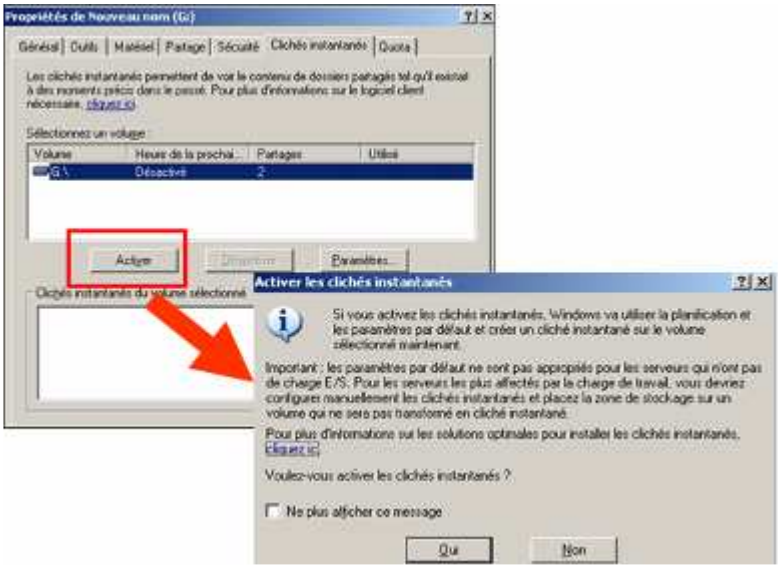


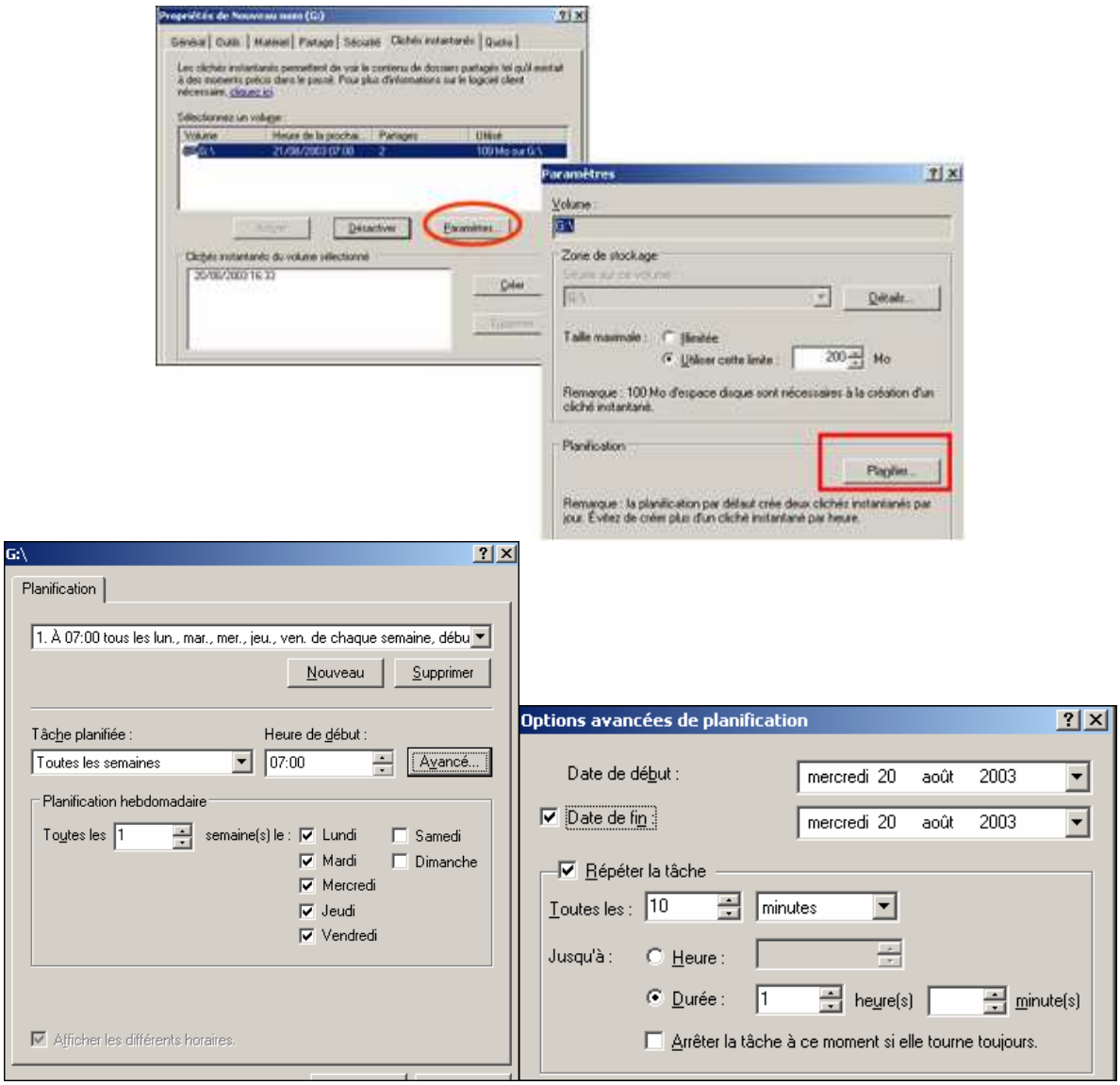
4.6.4- Les clichés instantanés

Ils permettent de réaliser de façon automatique des sauvegardes régulières des documents. Cela permet d'obtenir une sorte de gestion ou de maintenir à jour les versions des documents.
Les clichés instantanés sont activés uniquement sur un volume formaté en NTFS.
Par contre le client doit être un poste Windows XP Pro (SP1) ou bien Windows Server 2003.
Le logiciel client doit être installé dans le dossier %systemroot%\system32\clients\twclient\x86\twcli32.msi.



Les copies de sauvegardes peuvent être planifiées à l'aide d'un calendrier paramétrable. Vous pouvez aussi forcer cette sauvegarde en cliquant sur le bouton **Activer**.





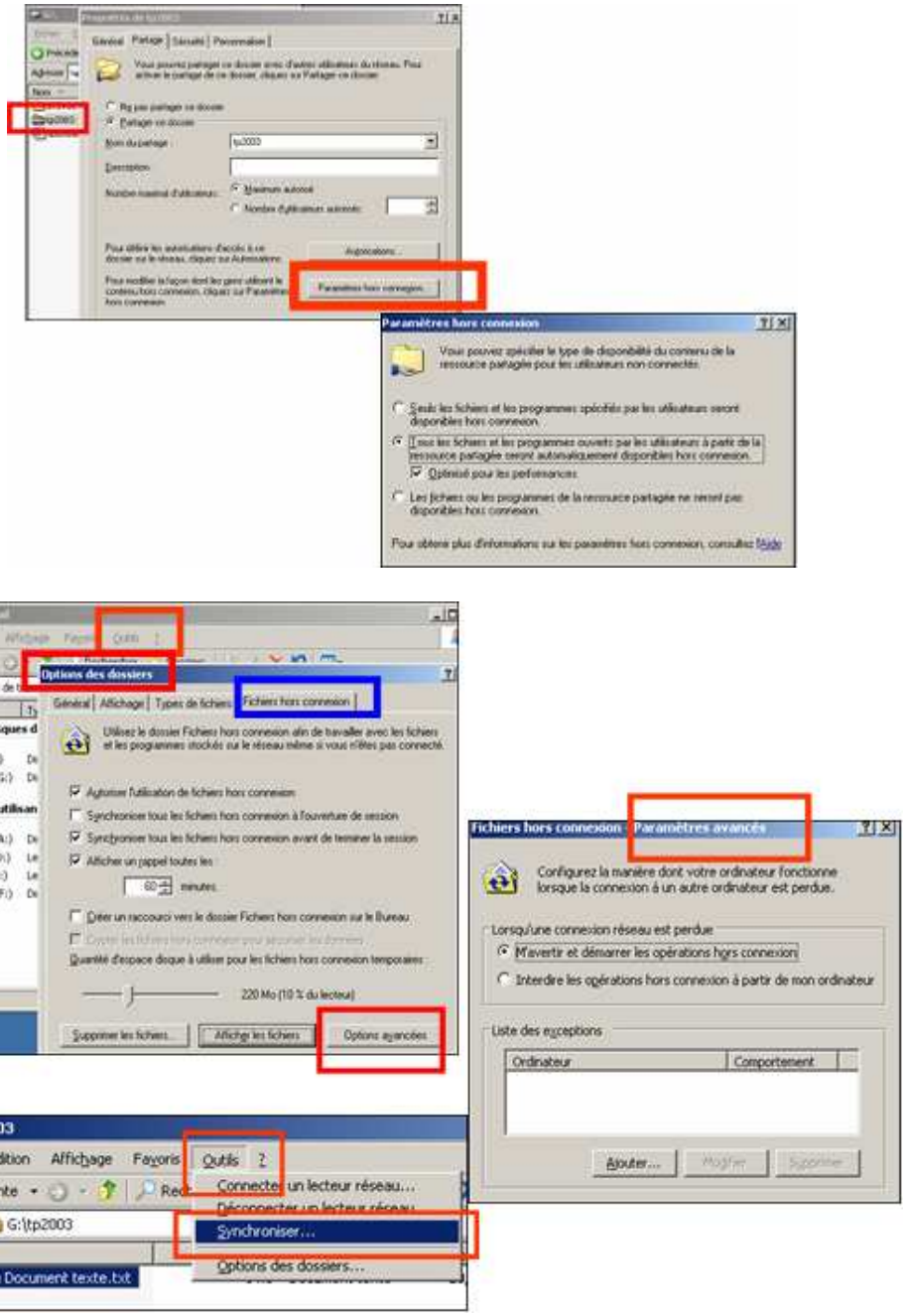
Si vous avez un problème avec une version antérieure d'un document et que vous avez activé les **Clichés Instantanés**, vous pouvez visualiser leur contenu, les copier et les restaurer.
Vous avez aussi la possibilité de réaliser cette opération en mode commande. Pour cela vous devez exécuter la commande Vssadmin.

4.6.5- Les fichiers hors connexion

Cette fonctionnalité est très utile pour les ordinateurs portables. Cela permet à un utilisateur de se connecter au réseau, et les documents sur lesquels il travaille sont copiés localement. Ensuite il peut travailler en autonome (hors connexion) sur ses documents de façon transparente à partir des copies locales qui auront étés auparavant copiées. Puis lorsqu'il se reconnectera au réseau, une synchronisation automatique démarrera. Le résultat sera que :

- Les fichiers modifiés sur le serveur sont recopiés sur le portable.
- Ceux modifiés sur le portable sont recopiés sur le serveur.
- Si un fichier est modifié sur les deux micros une fenêtre demande à l'utilisateur quel fichier il souhaite conserver.

Dans la fenêtre **Paramètres hors connexion** vous pouvez définir le mode de fonctionnement des fichiers **Hors connexion**. Ceux-ci pourront être disponibles hors connexion dès ouverture de ceux-ci par l'utilisateur ou bien celui-ci peut décider lesquels seront disponibles off-line.



Avec le paramétrage du client vous allez pouvoir activer l'utilisation et la disponibilité des fichiers en mode hors connexion. Vous pouvez aussi paramétrer le type de synchronisation (soit à l'ouverture ou à la fermeture de session).
D'autres paramètres sont disponibles comme la création d'un raccourci sur le bureau pour l'ouverture des fichiers, de crypter les fichiers hors connexion sur le poste client, d'indiquer un espace disque maximal pour les fichiers hors connexion...

Correspondances entre autorisations de base NTFS pour les dossiers et les autorisations avancées

	Autorisations de base					
Autorisations avancées	**Contrôle total**	**Modifier**	**Lecture et exécution**	**Afficher le contenu du dossier**	**Lecture**	***Écriture***
Parcourir le dossier/ Exécuter le fichier	**x**	**x**	**x**	**x**		
Liste du dossier / Lecture de données	**x**	**x**	**x**	**x**	**x**	
Attributs de lecture	**x**	**x**	**x**	**x**	**x**	
Lire les attributs étendus	**x**	**x**	**x**	**x**	**x**	
Création de fichiers / Écriture de données	**x**	**x**				**x**
Création de dossiers / Ajout de données	**x**	**x**				**x**
Attributs d'écriture	**x**	**x**				**x**
Écriture d'attributs étendus	**x**	**x**				**x**
Suppression de sous-dossiers et de fichiers	**x**					
Supprimer	**x**	**x**				
Autorisations de lecture	**x**	**x**	**x**	**x**	**x**	**x**
Modifier les autorisations	**x**					
Appropriation	**x**					

Ce tableau explique pour chaque autorisation NTFS de base, quelles sont les autorisations avancées qui la composent. Par exemple, l'autorisation de base **Lecture et Exécution** est composée des autorisations avancées suivantes :

- Parcourir le dossier/ Exécuter le fichier.
- Liste du dossier / Lecture de données.
- Attributs de lecture.
- Autorisations de lecture.
- 3 autorisations spéciales.

L'autorisation **Attribut de lecture** permet ou interdit **l'affichage des attributs** d'un fichier ou d'un dossier, tels que les attributs **Lecture seule** ou **Masqué**. Les attributs sont définis par le système de fichiers NTFS.
L'autorisation **Lire les attributs étendus** permet ou interdit **l'affichage des attributs étendus** d'un fichier ou d'un dossier. Les attributs étendus sont définis par des programmes et peuvent varier selon le programme utilisé.

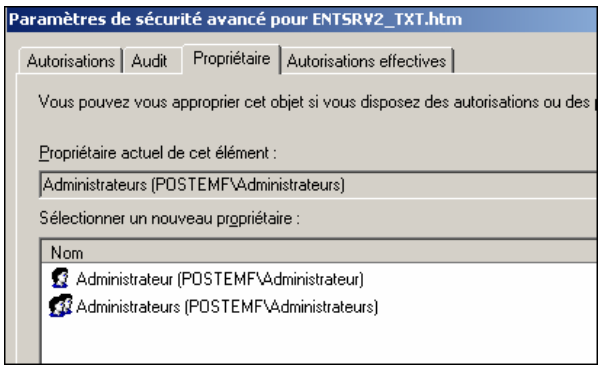
L'autorisation **Attributs d'écriture** permet ou interdit de **modifier les attributs** d'un fichier ou d'un dossier tels que les attributs **Lecture seule** ou **Masqué**. Les attributs sont définis par le système de fichiers NTFS.
L'autorisation **Ecriture d'attributs étendus** permet ou interdit la **modification des attributs étendus** d'un fichier ou d'un dossier. Les attributs étendus sont définis par des programmes et peuvent varier selon le programme utilisé.
L'autorisation **Autorisations de lecture** permet ou interdit les **autorisations de lecture du fichier ou du dossier**, telles que **Contrôle total**, **Lecture** et **Écriture**.
L'appropriation est l'autorisation qui permet ou interdit de prendre possession du fichier ou du dossier. Le propriétaire d'un fichier ou d'un dossier peut en modifier les autorisations à tout moment, indépendamment des autorisations existantes.
L'autorisation **Synchroniser** ne concerne que certains programmes exécutables.
Vous pouvez donner des autorisations NTFS de base et les modifier avec des autorisations avancées.

Correspondances entre autorisations de base NTFS pour les fichiers et les autorisations avancées

	Autorisations de base				
Autorisations avancées	**Contrôle total**	**Modifier**	**Lecture et exécution**	**Lecture**	**Écriture**
Parcourir le dossier / Exécuter le fichier	x	x	x		
Liste du dossier / Lecture de données	x	x	x	x	
Attributs de lecture	x	x	x	x	
Lire les attributs étendus	x	x	x	x	
Création de fichiers / Écriture de données	x	x			x
Création de dossiers / Ajout de données	x	x			x
Attributs d'écriture	x	x			x
Écriture d'attributs étendus	x	x			x
Suppression de sous-dossiers et de fichiers	x				
Supprimer	x	x			
Autorisations de lecture	x	x	x	x	x
Modifier les autorisations	x				
Appropriation	x				

4.6.6- Appropriation de fichier/dossier

Par défaut le propriétaire d'une ressource est celui qui l'a créée et fait partie automatiquement du groupe créateur propriétaire. Dés qu'un utilisateur est propriétaire d'une ressource il peut en modifier les permissions pour écrire, lire… Pour s'approprier une ressource un utilisateur doit posséder la permission spéciale **Prendre possession**. Il ne peut s'approprier que la ressource mais ne peut pas rendre un autre utilisateur propriétaire. Clic droit sur le fichier ➔ **Propriétés** ➔ **Sécurité** ➔ **Paramètres avancés** ➔ **Propriétaire.** Si l'utilisateur possède la permission prendre possession, son compte s'affiche dans la liste. Le sélectionner puis cliquez sur **Appliquer.**



Par défaut les **Administrateurs** sont toujours présents à la candidature pour l'appropriation d'un fichier ou d'un dossier. C'est normal car le compte administrateur possède toujours l'autorisation **Appropriation** et elle ne peut pas lui être retirée. Vous n'avez plus qu'à cliquer sur le bouton **Autres utilisateurs** ou **groupes** pour ajouter un nouveau propriétaire ne figurant pas dans la liste.

4.6.7- Copie et déplacement de fichiers et de dossiers

Pour réaliser une copie ou un déplacement de fichiers ou dossier l'utilisateur doit avoir les permissions nécessaires.
Si la copie d'un fichier ou d'un répertoire se fait vers une partition NTFS différente, le fichier ou répertoire hérite des permissions de destination.
Pareil si vous le copiez à l'intérieur d'une même partition.
Si le déplacement d'un fichier ou d'un dossier se fait vers une partition NTFS différente, le fichier ou dossier hérite toujours des permissions de destination.
Par contre, c'est différent si vous déplacez un fichier ou répertoire sur une même partition NTFS, il y a conservation des permissions.
Si vous copiez ou déplacez des fichiers ou dossiers d'une partition NTFS vers une partition non NTFS toutes les permissions seront perdues.
Lorsque vous copiez un fichier ou un dossier vous devenez le propriétaire de cette copie.

En résumé : les opérations de copie héritent des autorisations initiales, seul le déplacement vers la même partition permet le maintien des autorisations

	Sur un même volume NTFS	Entre volumes NTFS différents
Copie	Héritage des autorisations de la destination.	Héritage des autorisations de la destination.
Déplacement	Conservation des autorisations d'origine.	Héritage des autorisations de la destination.

4.7- Cryptage de documents (EFS)

4.7.1- Généralités sur le cryptage EFS

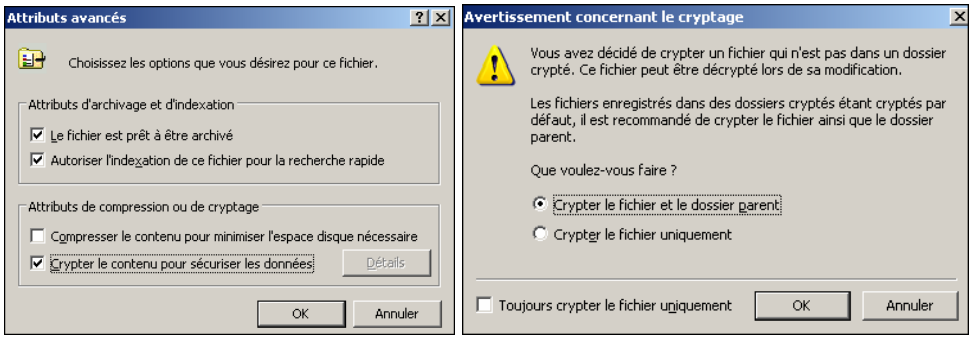
Windows 2003 permet de **Crypter les données** afin qu'elles ne soient accessibles qu'aux utilisateurs disposant de la clé permettant un déchiffrage du document
Dès qu'un document est crypté les utilisateurs autorisés à le décrypter peuvent accéder à ce document et de façon transparente. Le cryptage s'applique sur des permissions NTFS mais reste totalement indépendant des permissions NTFS qui pourraient être appliquées à ce même document.
Le système de cryptage utilisé est **EFS** (Encrypting File System).

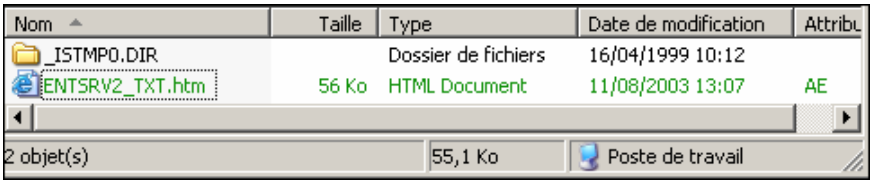
Les caractéristiques principales du système EFS sont :

- Fonctionne en arrière-plan.
- Utilise des clés symétriques (clé d'encryptage et décryptage identiques et faisant partie du fichier).
- Uniquement accessible par un utilisateur autorisé.
- Intègre la prise en charge de la récupération des données.
- Nécessite au moins un agent de récupération.
- **EFS** permet de crypter des fichiers ou dossiers sur un micro, mais pas les données qui transitent sur le réseau. Windows Server 2003 propose **IPSec** ou **SSL**.

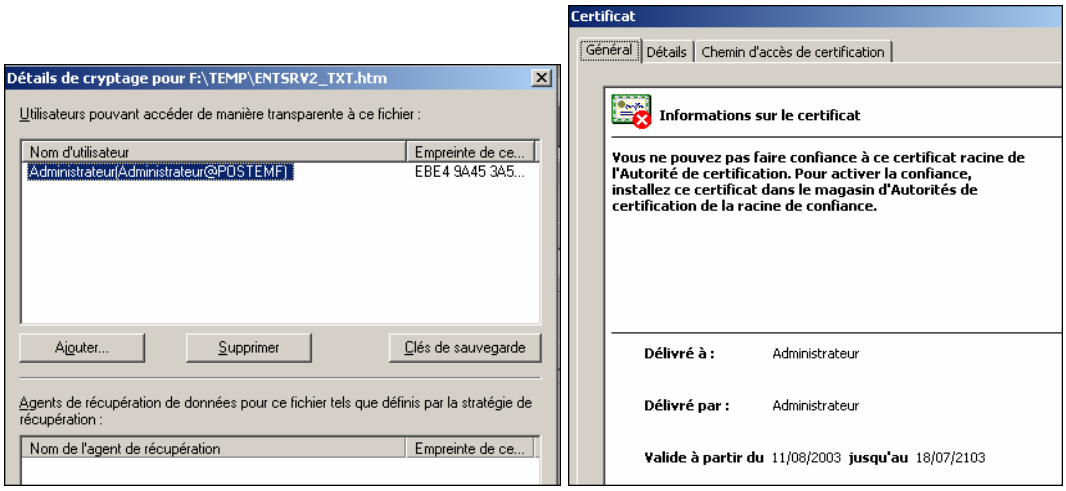
4.7.2- Mise en ouvre du cryptage des fichiers et des dossiers

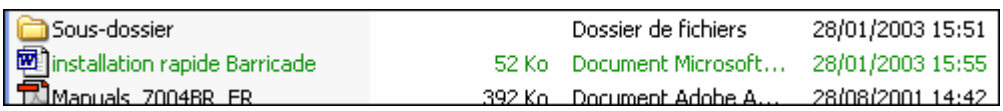
Cliquez droit sur le **fichier** ou **dossier** à crypter (volume ou partition NTFS). Puis cliquez sur **Propriétés ➔ Avancés ➔ Crypter le contenu pour sécuriser les données.**
Vous avez la possibilité de choisir de crypter le **dossier seul** ou **inclure** son contenu.
✋ Vous ne pouvez pas crypter et compresser un fichier ou dossier. Si le fichier que vous désirez crypter est compressé, il va automatiquement perdre son attribut de compression.





Après activation du cryptage, il est possible d'ajouter des utilisateurs du domaine pouvant accéder au document EFS. Il devra auparavant avoir obtenu un certificat soit auprès d'Active Directory ou d'une autorité de certification.





4.7.3- Supprimer un cryptage

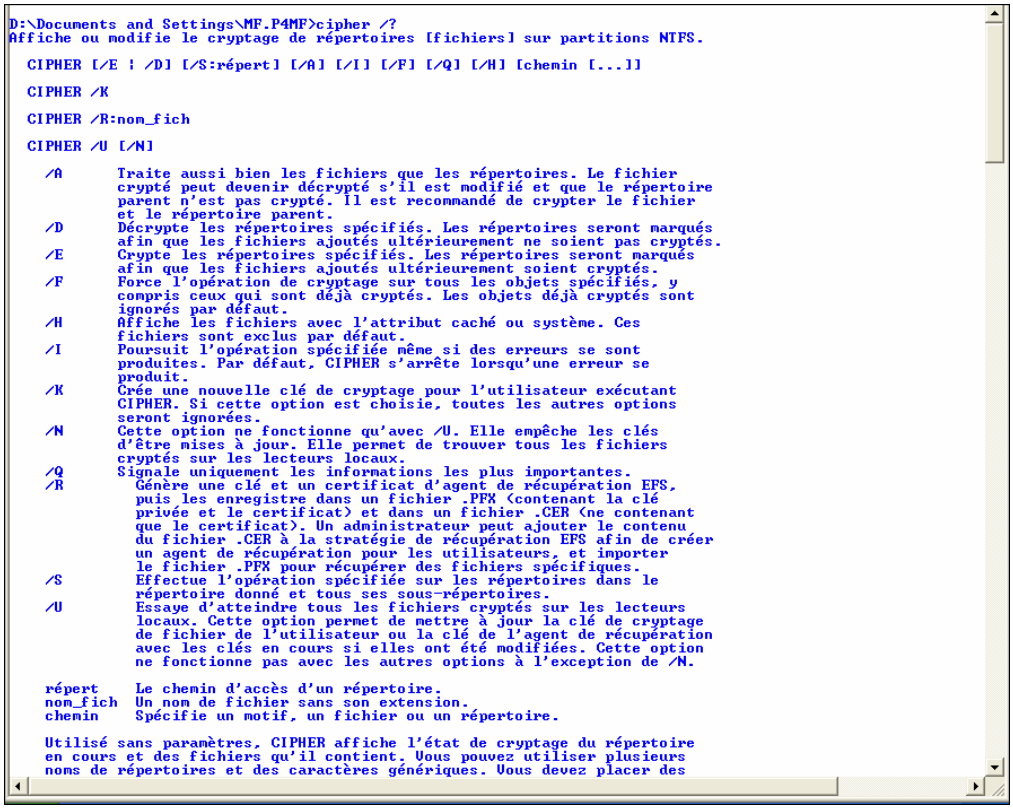
Pour supprimer le cryptage d'un fichier ou d'un dossier il vous suffit à partir de l'explorateur de le sélectionner, puis ouvrez le menu contextuel et dans le menu **Général**, cliquez sur **Avancé** et décochez l'option **Crypter le contenu pour sécuriser les données.**
Si vous avez décidé de **décrypter** un dossier contenant des fichiers ou sous dossiers vous devez choisir si vous souhaitez **décrypter son contenu**.

4.7.4- Copie et déplacement de dossiers et fichiers cryptés

Lorsque vous copiez ou déplacez un document crypté il restera crypté que la destination le soit ou non.
Si ce déplacement ou cette copie se fait sur un autre système de fichier différent de NTFS le document ne sera plus crypté sur la destination.
De même si vous déplacez ou copiez un fichier non crypté dans un répertoire crypté il le deviendra aussi. Sauf si vous mettez en œuvre une stratégie qui empêche de le faire.

4.7.5- Utilitaire en ligne de mode commande CIPHER.exe

Si vous entrez cipher sans commutateur vous obtenez l'état de cryptage du répertoire courant.



```
D:\Documents and Settings\MF.P4MF>cipher /?
Affiche ou modifie le cryptage de répertoires [fichiers] sur partitions NTFS.

  CIPHER [/E | /D] [/S:répert] [/A] [/I] [/F] [/Q] [/H] [chemin [...]]

  CIPHER /K

  CIPHER /R:nom_fich

  CIPHER /U [/N]

    /A      Traite aussi bien les fichiers que les répertoires. Le fichier
            crypté peut devenir décrypté s'il est modifié et que le répertoire
            parent n'est pas crypté. Il est recommandé de crypter le fichier
            et le répertoire parent.
    /D      Décrypte les répertoires spécifiés. Les répertoires seront marqués
            afin que les fichiers ajoutés ultérieurement ne soient pas cryptés.
    /E      Crypte les répertoires spécifiés. Les répertoires seront marqués
            afin que les fichiers ajoutés ultérieurement soient cryptés.
    /F      Force l'opération de cryptage sur tous les objets spécifiés, y
            compris ceux qui sont déjà cryptés. Les objets déjà cryptés sont
            ignorés par défaut.
    /H      Affiche les fichiers avec l'attribut caché ou système. Ces
            fichiers sont exclus par défaut.
    /I      Poursuit l'opération spécifiée même si des erreurs se sont
            produites. Par défaut, CIPHER s'arrête lorsqu'une erreur se
            produit.
    /K      Crée une nouvelle clé de cryptage pour l'utilisateur exécutant
            CIPHER. Si cette option est choisie, toutes les autres options
            seront ignorées.
    /N      Cette option ne fonctionne qu'avec /U. Elle empêche les clés
            d'être mises à jour. Elle permet de trouver tous les fichiers
            cryptés sur les lecteurs locaux.
    /Q      Signale uniquement les informations les plus importantes.
    /R      Génère une clé et un certificat d'agent de récupération EFS,
            puis les enregistre dans un fichier .PFX (contenant la clé
            privée et le certificat) et dans un fichier .CER (ne contenant
            que le certificat). Un administrateur peut ajouter le contenu
            du fichier .CER à la stratégie de récupération EFS afin de créer
            un agent de récupération pour les utilisateurs, et importer
            le fichier .PFX pour récupérer des fichiers spécifiques.
    /S      Effectue l'opération spécifiée sur les répertoires dans le
            répertoire donné et tous ses sous-répertoires.
    /U      Essaye d'atteindre tous les fichiers cryptés sur les lecteurs
            locaux. Cette option permet de mettre à jour la clé de cryptage
            de fichier de l'utilisateur ou la clé de l'agent de récupération
            avec les clés en cours si elles ont été modifiées. Cette option
            ne fonctionne pas avec les autres options à l'exception de /N.

    répert    Le chemin d'accès d'un répertoire.
    nom_fich  Un nom de fichier sans son extension.
    chemin    Spécifie un motif, un fichier ou un répertoire.

    Utilisé sans paramètres, CIPHER affiche l'état de cryptage du répertoire
    en cours et des fichiers qu'il contient. Vous pouvez utiliser plusieurs
    noms de répertoires et des caractères génériques. Vous devez placer des
```

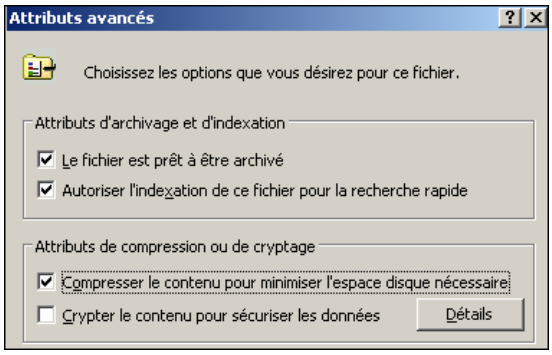
4.8- Compresser des fichiers et des dossiers

4.8.1- Compression NTFS

- Permet l'allocation d'espace.
- Compression ou décompression possible d'un fichier, dossier ou une partition entière.
- Clic droit sur le fichier ou dossier à compresser ➔ **Avancés** ➔ cocher **Compresser le contenu pour minimiser l'espace disque nécessaire**.
- Le fichier ou dossier compressé est accessible de façon transparente par les clients.
- Pour les repérer mettre des couleurs différentes : **Outils** ➔ **Affichage** ➔ **Option des**

dossiers ➔ Cocher **Donner une couleur différente aux fichiers et dossiers compressés**.

- Si vous désirez compresser un dossier qui n'est pas vide W2003 demande si vous voulez appliquer cette compression à l'ensemble des dossiers et fichiers enfants ou uniquement au dossier courant.
- Vous avez le choix de compresser ou crypter un fichier mais pas les deux (le choix d'une action exclut l'autre de fait).



Win 2003 ne supporte que la compression des volumes NTFS.
Lorsque la compression est activée, les utilisateurs continueront à employer les fichiers de façon transparente. Seul la couleur bleue des dossiers et fichiers compressés permettra de les distinguer de la couleur verte des fichiers cryptés.

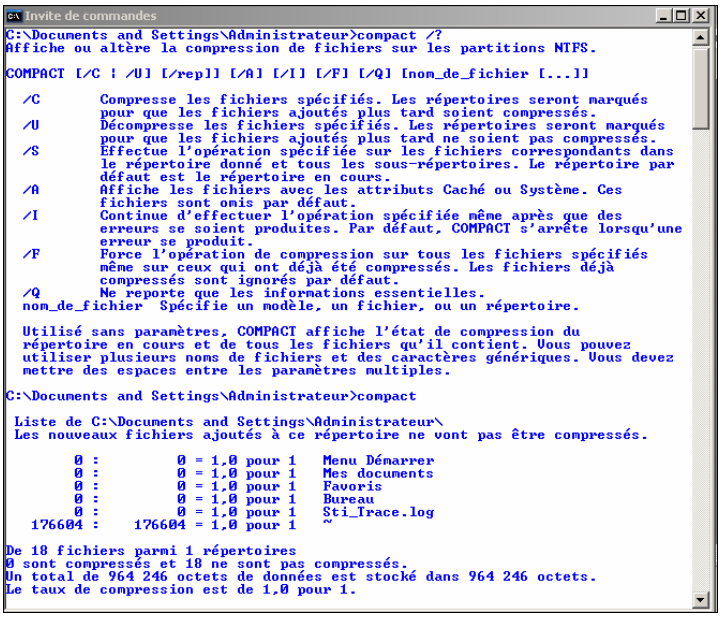
Copie et Déplacement de fichiers compressés

Les règles de copie et de déplacement des fichiers compressés sont identiques à celles des autorisations NTFS.

	Sur un même volume NTFS	Entre volume NTFS différents
COPIE	Héritage de l'attribut de la destination	Héritage de l'attribut de la destination
DEPLACEMENT	Conservation de l'attribut compression	Héritage de l'attribut de la destination

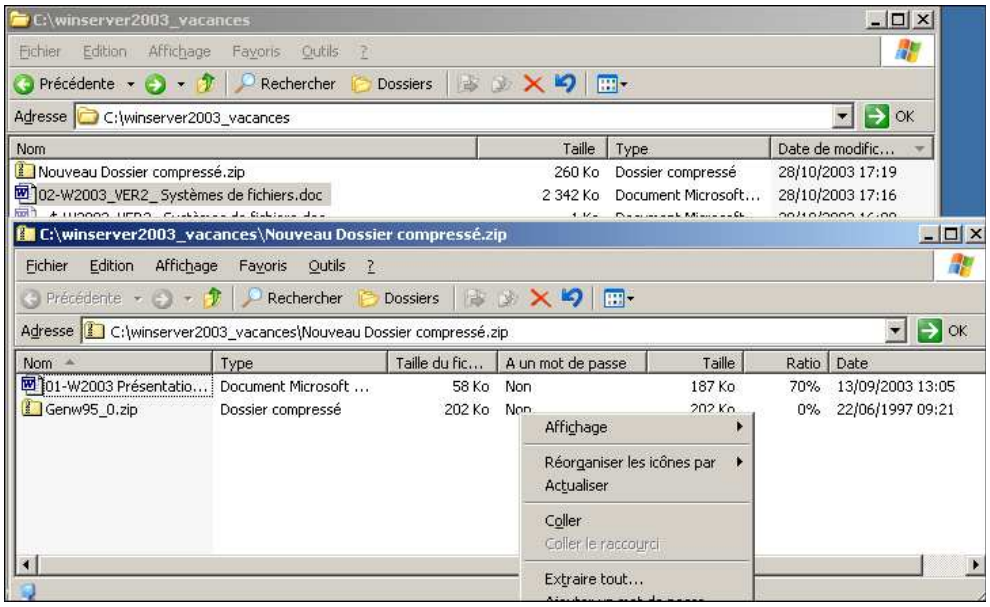
Utilitaire de compression Compact.exe

Compression en ligne de commande avec la commande **COMPACT.exe.**

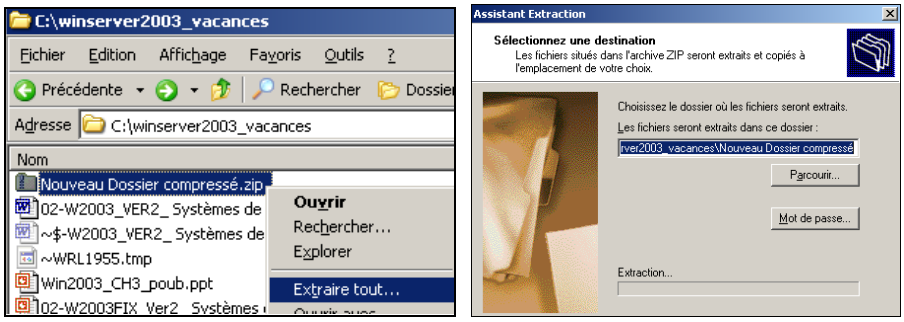


4.8.2- Compression ZIP

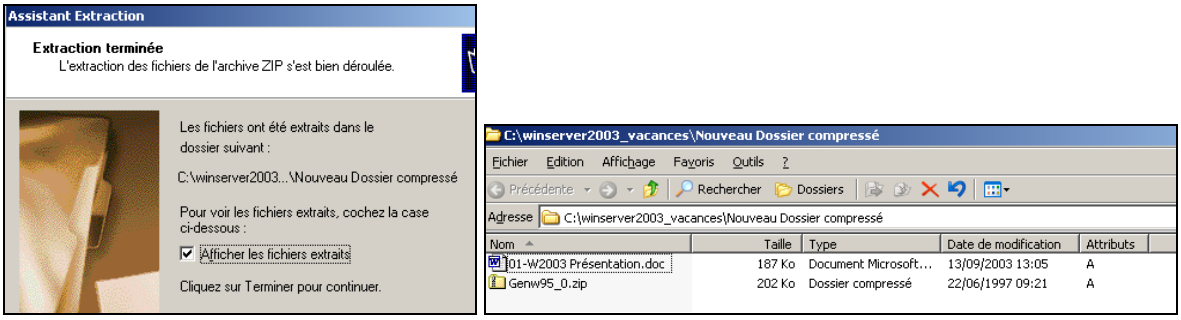
La possibilité de gérer nativement les fichiers au format ZIP est disponible depuis Windows XP et s'applique à tous les systèmes de fichiers FAT ou NTFS.
A partir de l'explorateur, les fichiers ayant l'extension .ZIP sont considérés comme des dossiers au niveau navigation comme les fichiers CAB de MS-DOS.
Le contenu de ce dossier est affiché et vous pouvez ouvrir, couper ou extraire un ou plusieurs fichiers compressés. Ce qui très intéressant c'est lorsque vous exécutez une recherche de fichier, W2003 va scruter automatiquement le contenu des fichiers .ZIP.
Les fichiers compressés par Windows 2003 sont compatibles avec les logiciels tels Winzip utilisant ce format de façon native.
L'exécution de certains programmes à partir des dossiers compressés est possible directement sans avoir besoin de les décompresser.
Lorsque vous ouvrez ou copiez un fichier contenu dans un fichier compressé il sera automatiquement décompressé dans le répertoire temporaire de l'utilisateur (variable TEMP).
Pour créer un nouveau fichier compressé sélectionnez le ou les fichiers ou dossiers à compresser puis à partir du menu contextuel sélectionnez **Envoyez vers – Dossier compressé.**
Le nom du fichier compressé sera le nom du premier fichier ou dossier sélectionné auquel est ajouté l'extension .ZIP. Si votre sélection inclus des sous-dossiers, il y a conservation de l'arborescence dans le fichier compressé.



Pour extraire tout le contenu d'un fichier compressé vous devez le sélectionner puis à partir du menu **Fichier** valider **Extraire Tout** (ou du menu contextuel).
L'assistant démarre, vous pouvez modifier le dossier de destination pour les fichiers extraits ou utiliser le bouton **Parcourir** (par défaut l'extraction se fera dans le répertoire courant).
Si le fichier compressé est protégé par mot de passe vous devez le saisir.



Au final la case à cocher **Afficher les fichiers extraits** permet d'ouvrir automatiquement l'explorateur vers le dossier cible à la fin de l'extraction.

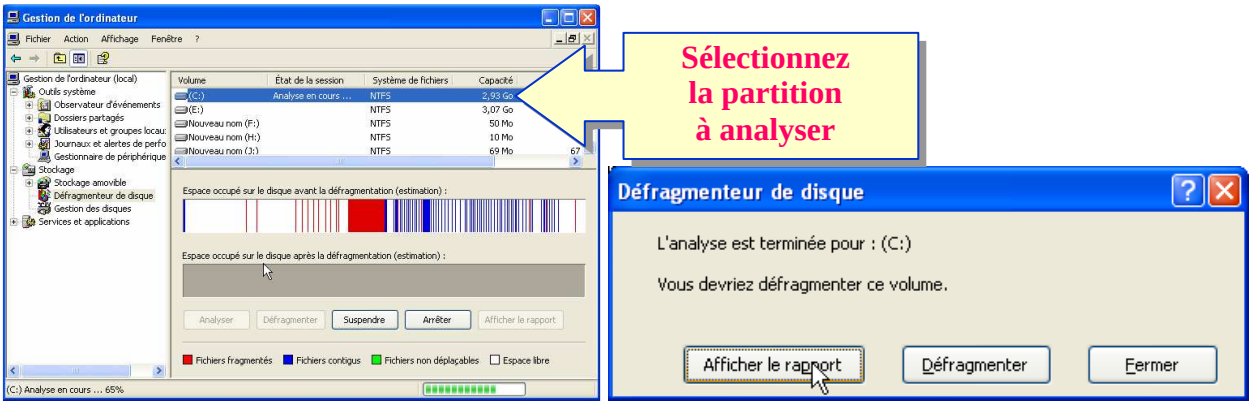


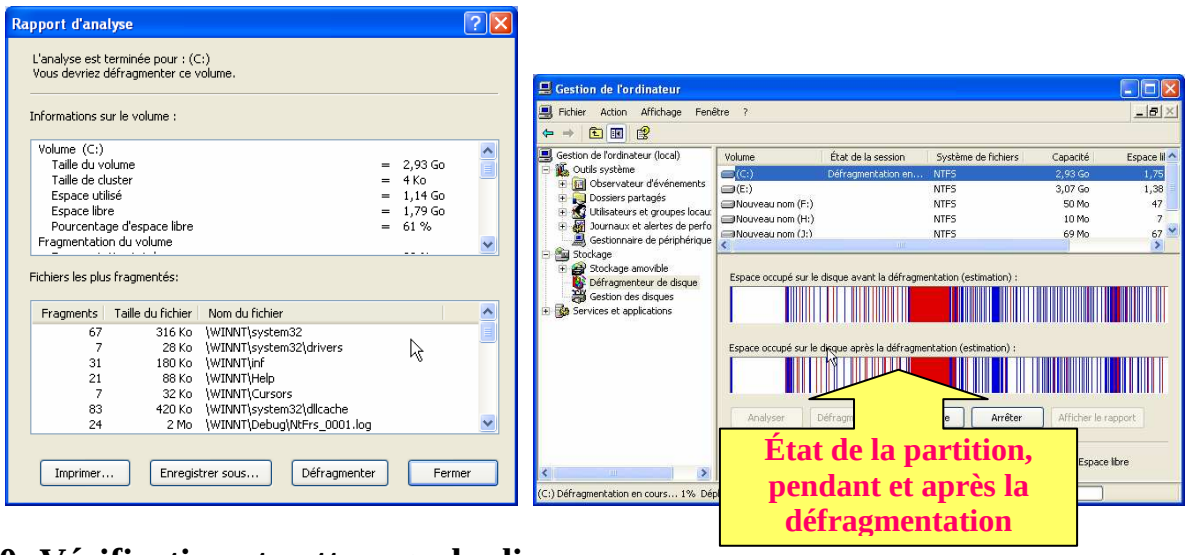
4.9- Défragmenter les disques

Les données sont stockées sur le disque dans des unités nommées clusters. Lorsque vous ajoutez ou supprimez des fichiers sur un disque, les données et l'espace libre de ce disque peuvent se fragmenter. Si c'est le cas, les fichiers de taille importante ne peuvent pas être écrits dans une zone contiguë du disque. Ils seront écrits dans plusieurs zones plus petites ce qui ralentira leur lecture. Pour réduire cette incidence vous devez défragmenter votre disque et utiliser le programme de défragmentation. Si les fichiers sont stockés de façon contiguë l'accès au fichier sera rapide

Comme les fichiers sont stockés de façon dynamique ils se fragmentent

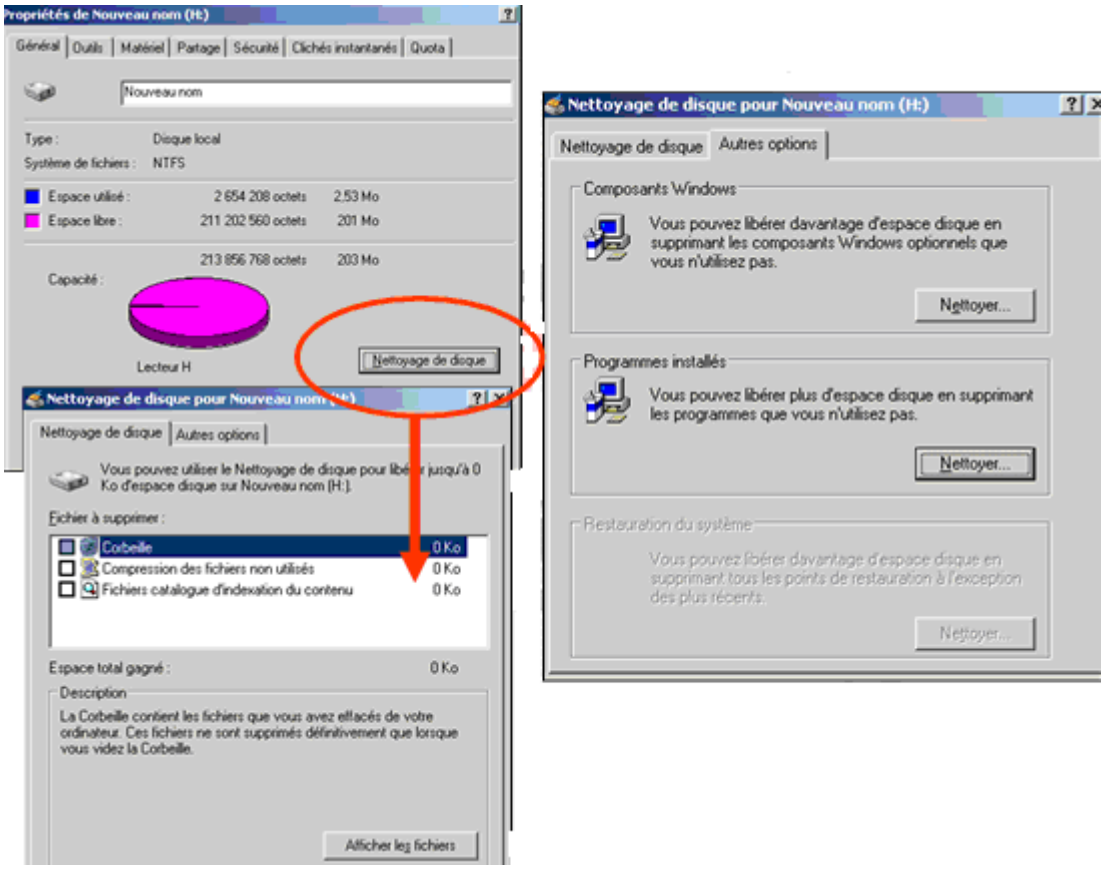
Utilisation de l'utilitaire de défragmentation fournit avec W2003 qui fonctionne sous FAT, FAT32 et NTFS.





4.10- Vérification et nettoyage du disque

- Vérification et analyse du disque.
- Libération d'espace.

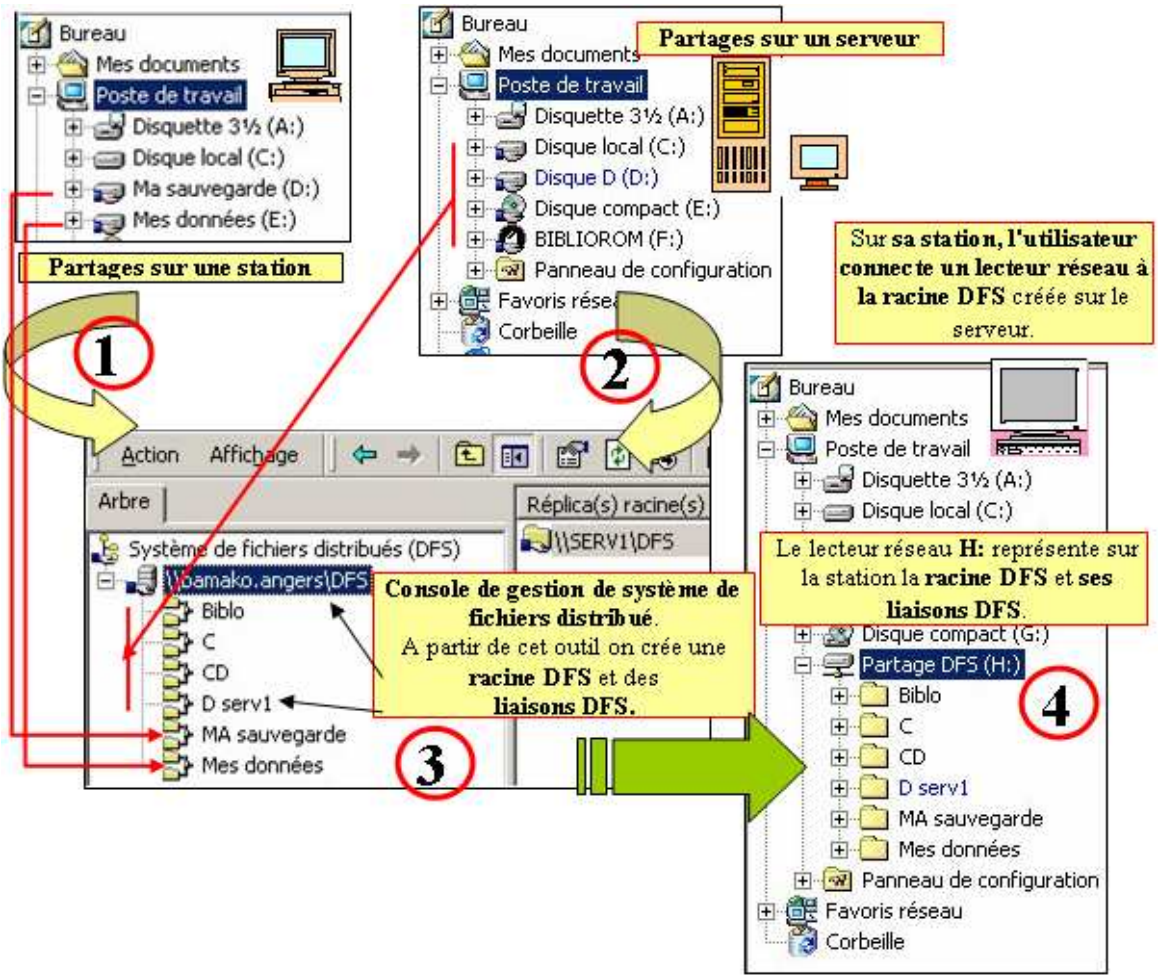


4.11- DFS

4.11.1- Présentation de DFS (Distributed File System)

Le système de fichiers distribués DFS permet à l'administrateur d'organiser les ressources de dossiers partagés du réseau, et ainsi créer une seule arborescence logique. Pour l'utilisateur les ressources semblent résider sur un seul serveur et cela de façon transparente. Le service DFS redirige les demandes vers le serveur qui stocke les informations.
L'administrateur ou son équivalent peut quand il le désire déplacer les données d'un serveur vers un

autre en modifiant simplement le lien (le chemin d'accès). Il n'est pas nécessaire de modifier quoique ce soit du côté utilisateur.
Il existe aussi la possibilité de créer des répliquas. Cela consiste à avoir les mêmes ressources sur plusieurs serveurs différents. Une réplication automatique peut être paramétrée. Cela permet d'obtenir une tolérance de panne car si un lien devient indisponible un utilisateur pourra être connecté à un autre serveur.
De même si les liens se situent sur des sites différents, l'utilisateur sera redirigé vers le lien DFS situé sur le même site que lui.
DFS permet de présenter pour l'utilisateur un seul partage pour des répertoires situés sur des ordinateurs différents. Ainsi, toutes les informations nécessaires à un utilisateur, mais situées sur des ordinateurs différents, peuvent être regroupées sous une seule arborescence.



Un partage **DFS** est constitué d'une **racine** et de **liaisons DFS**. Le système de fichiers DFS se gère en utilisant la console **Système de fichiers distribués**.
La configuration consiste à créer une racine de domaine sur un serveur, et définir ensuite un lien DFS pointant sur les diverses ressources du réseau afin de constituer les branches de l'arborescence.
DFS nécessite un service serveur DFS, et bien sur un client DFS. Les clients peuvent être W98, NT, 2000, XP et W2003.

4.11.2- Types de racines DFS

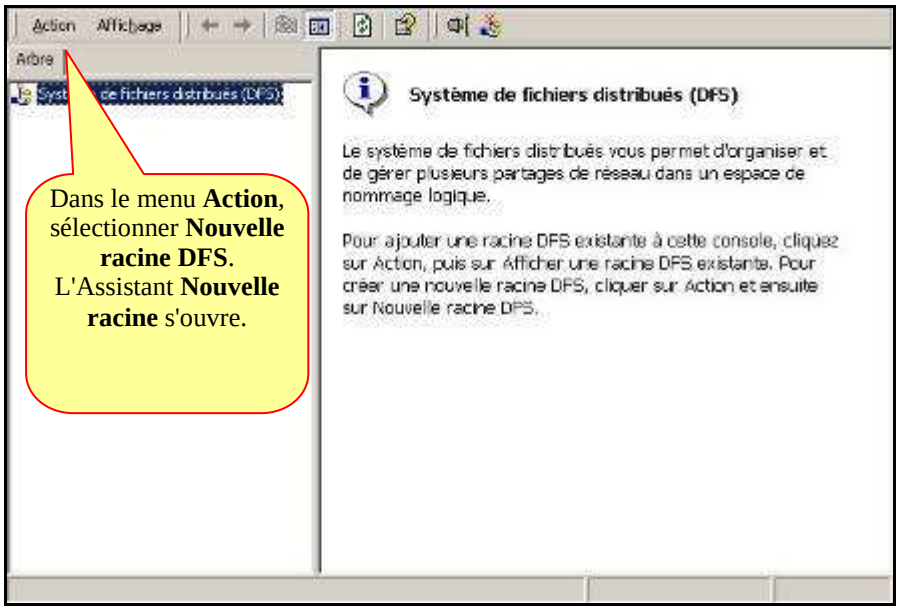
Le **service DFS** est installé automatiquement sur les serveurs Windows 2003. Ce service peut être interrompu ou arrêté et redémarré, mais il ne peut pas être supprimé.
Il existe deux types de racines DFS.

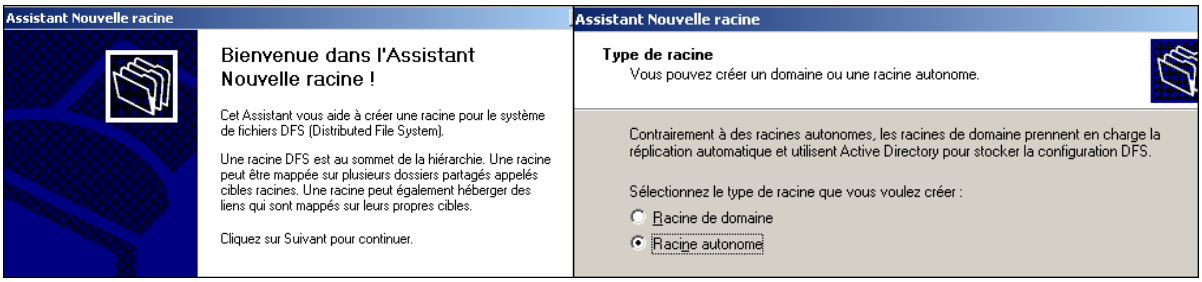
Racines DFS autonomes : les racines DFS stockent la structure DFS sur un **seul serveur** et n'offrent pas de tolérance de panne. Il n'y a pas de réplication des fichiers composant le partage DFS, puisqu'il n'y a qu'un seul serveur sur le réseau.

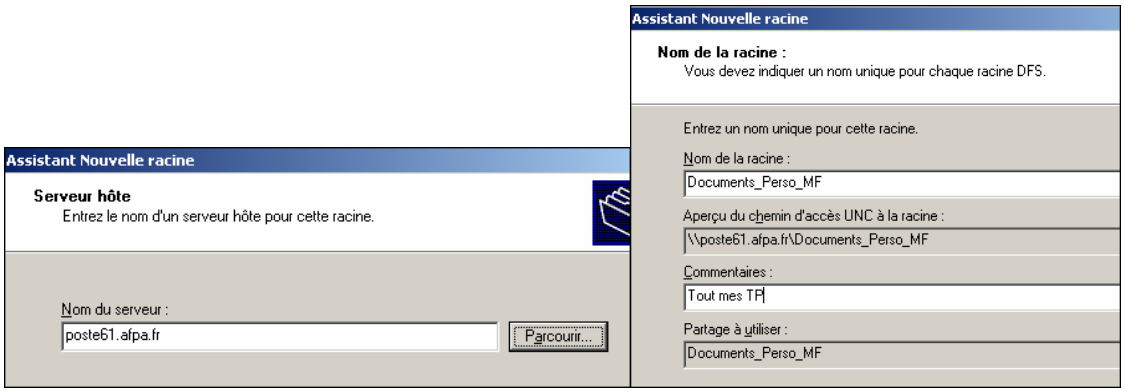
Racines DFS de domaine : les racines DFS de domaine enregistrent automatiquement les informations concernant la structure DFS dans la base Active Directory. Si le serveur qui héberge normalement la **structure DFS** tombe en panne, elle est alors accessible à partir d'un autre serveur. Les fichiers de la racine DFS et des liaisons peuvent être répliqués sur d'autres serveurs du domaine. Il y a tolérance de panne.

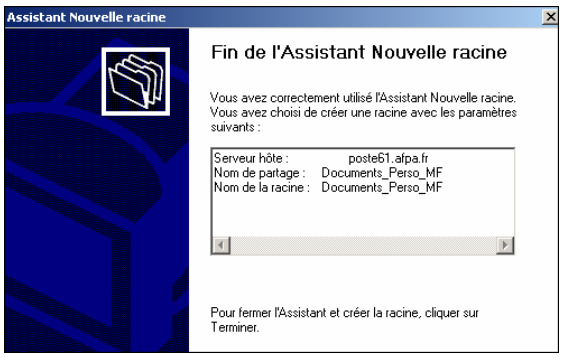
4.11.3- Exemple de configuration DFS

Racine DFS Autonome : ouvrir la console **Système de fichiers distribués** dans **Programmes** – **Outils d'administration**.



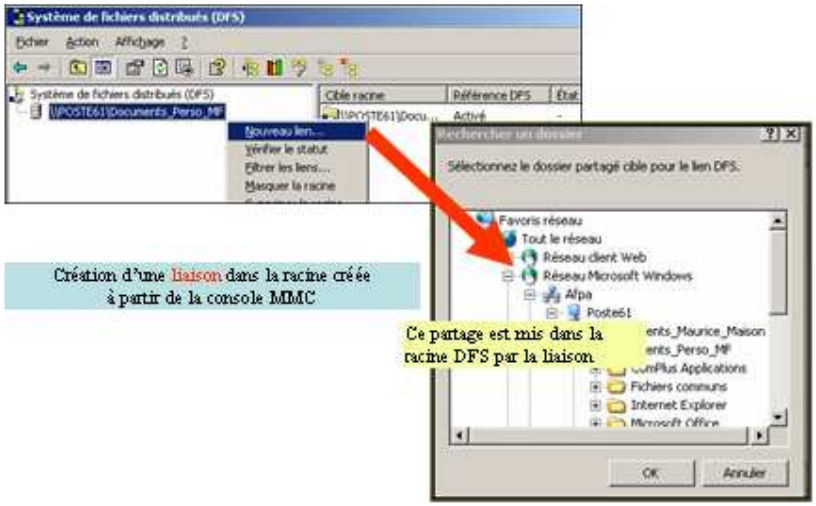


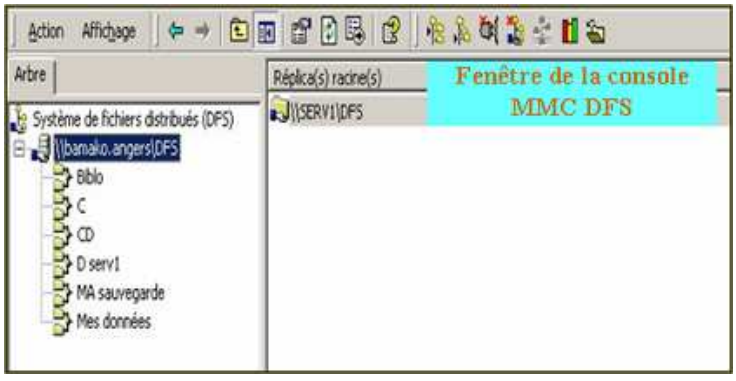




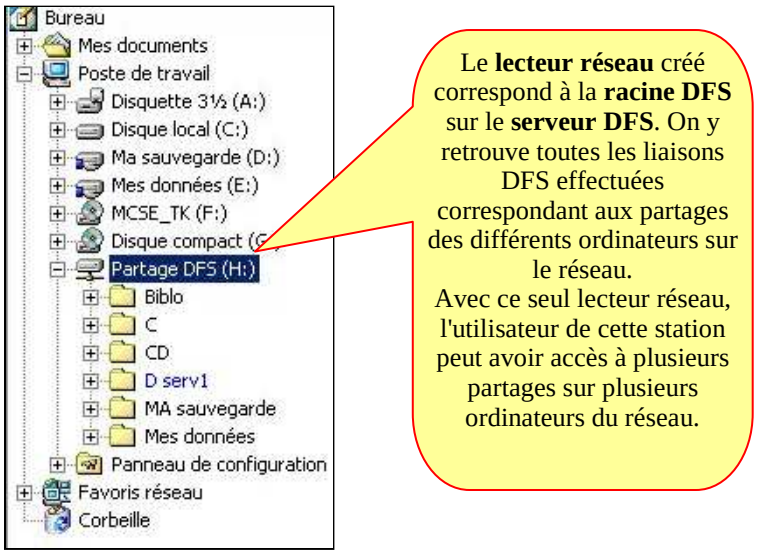
Racine DFS de domaine : dans ce cas, vous aurez à préciser le nom du domaine. Le panneau final sera :

Création des liaisons DFS : il faut ensuite créer une à une, les liaisons avec les partages sur les différents serveurs (ou station).





Création d'un lecteur réseau sur une station à partir d'une racine DFS : en utilisant le voisinage réseau et la commande **Connecter un lecteur réseau**, on crée un lecteur réseau à partir du partage racine DFS et on a accès (sous réserve des autorisations nécessaires) à tous les partages des différents serveurs représentés dans cette racine DFS.



Répliqua de dossiers et fichiers DFS : si l'on a plusieurs serveurs et que l'on a créé une ou plusieurs racines de domaine DFS, il est possible d'avoir une copie des dossiers et fichiers sur un autre serveur. Pour cela on utilise la commande **Nouveau répliqua** dans le menu **Action** de la console **DFS**.

4.12- FRS (File Replication Service)

File Replication Service est le service de duplication de dossiers et fichiers de Windows 2003. Il permet d'effectuer une réplique du volume système Windows 2003 (Sysvol) sur tous les contrôleurs de domaine. Il peut aussi être utilisé pour la réplication des racines DFS.
Chaque domaine peut posséder plusieurs contrôleurs de domaines. Chacun d'eux héberge une copie de la base de données d'Active Directory. FRS gère automatiquement les mises à jour des différentes copies.

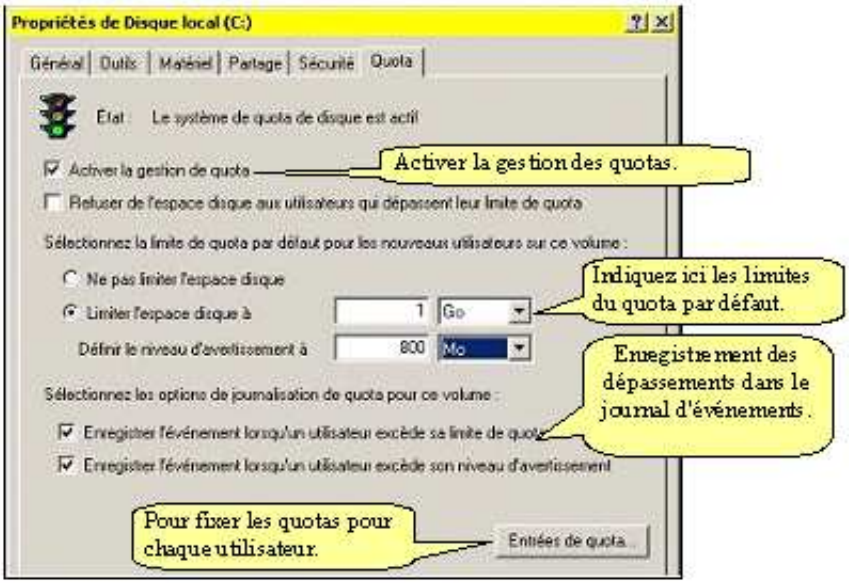
4.13- Quotas de disques

4.13.1- Présentation

Il peut être intéressant de limiter sur un serveur (ou une station), pour chaque utilisateur, la quantité d'espace disque utilisable. Windows 2003 gère la fonction **Quotas de disques**. Les administrateurs peuvent pour chaque utilisateur fixer la taille disque utilisée. Cette fonction se base sur la notion de propriétaire d'un fichier pour définir son appartenance à tel ou tel utilisateur. Cet état de fait est à prendre en compte en cas de copie de fichiers appartenant à un autre utilisateur
Même si les fichiers sont compressés, la fonction **Quotas de disques** prend en compte la taille réelle des fichiers.

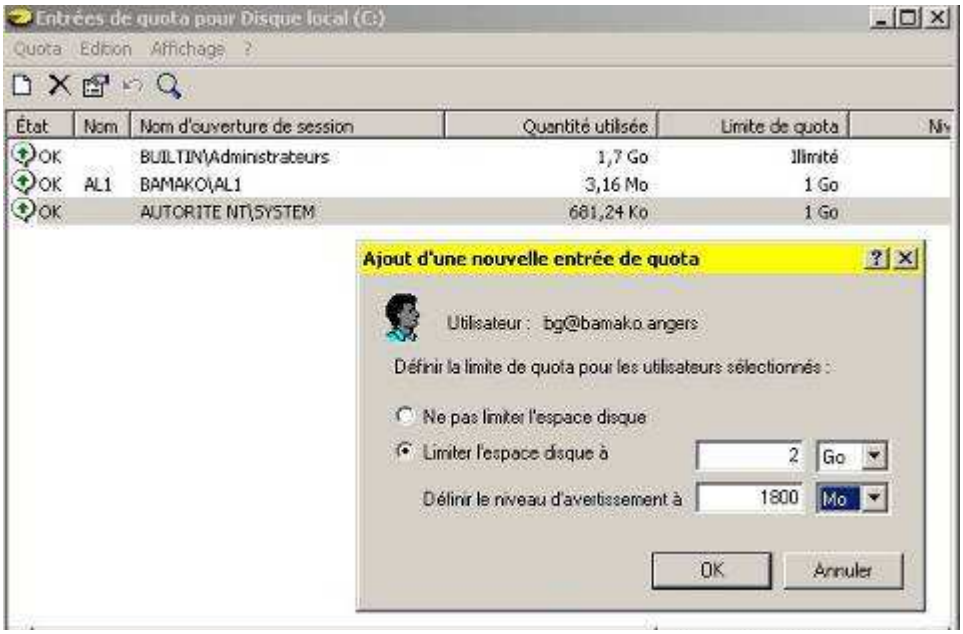
4.13.2- Mise en œuvre

Sélectionnez l'icône de la partition ou du volume sur lequel vous souhaitez appliquer les quotas. Sélectionnez **Propriétés** et dans le panneau qui s'ouvre, cliquez sur l'onglet **Quotas**.



- Activez le quota.
- Limitez l'espace disque.
- Sélectionnez ou non les options d'enregistrements d'événements.
- Si vous validez, le quota est appliqué à tous les utilisateurs existants. Vous pouvez cependant modifier les valeurs pour chaque utilisateur existant ou à créer.
- Sélectionnez **Entrées de quota…**

La fenêtre ci-dessous apparaît avec le nom des utilisateurs ayant un quota. Pour ajouter un utilisateur à la liste, utilisez le menu **Quota**, commande **Nouvelle entrée de Quota**.



V- GESTION DES UTILISATEURS ET DES GROUPES

5.1- Comptes utilisateurs

Un compte utilisateur est un enregistrement dans une base de données qui définit un utilisateur auprès de Windows 2003. Cet enregistrement comporte le nom de l'utilisateur sous ses différentes formes, son mot de passe, les groupes dont il est membre et d'autres informations comme ses droits et autorisations. Un compte utilisateur permet d'ouvrir une session dans un domaine ou sur l'ordinateur sur lequel l'utilisateur travaille.

5.1.1- Utilisateurs de domaines

Avec un **compte d'utilisateur de domaine**, l'utilisateur peut ouvrir une session pour accéder aux ressources autorisées du réseau. L'utilisateur fournit son nom de compte et son mot de passe, Windows 2003 l'authentifie, et lui renvoie un jeton d'accès qui contient les éléments relatifs à l'utilisateur et ses paramètres de sécurité. Ce jeton d'accès permet à l'utilisateur d'accéder aux différents ordinateurs sur lesquels se situent les ressources auxquelles il peut parvenir.
Le compte utilisateur est stocké dans la base de données d'Active Directory, l'**Annuaire**, présente sur les contrôleurs de domaine. La duplication des comptes sur les différents contrôleurs est effectuée automatiquement, mais peut prendre plusieurs minutes. Une remise à jour de la liste des comptes sur chaque contrôleur de domaine est effectuée toutes les cinq minutes.

5.1.2- Utilisateurs locaux

Un **compte d'utilisateur local** (c'est-à-dire un utilisateur qui travaille directement sur la machine sans passer par le réseau) permet d'ouvrir une session uniquement sur l'ordinateur qui contient le compte de l'utilisateur créé. Le compte est contenu dans une base de données **locale** et n'est pas dupliquée sur d'autres ordinateurs.
Pour créer un compte d'utilisateur local sur une station, n'utilisez pas la console **Utilisateurs et mots de passe** dans le panneau de configuration, mais la console **Gestion de l'ordinateur**, puis **Utilisateurs et groupes locaux** (sur une station ou un serveur autonome).

5.1.3- Utilisateurs prédéfinis

Windows 2003 créé automatiquement des comptes utilisateurs appelés **comptes utilisateurs prédéfinis**. Par exemple, **Administrateur** et **Invité** sont des comptes d'utilisateur prédéfinis. Ces comptes ne peuvent pas être supprimés, par contre, ils peuvent être renommés.
Administrateur

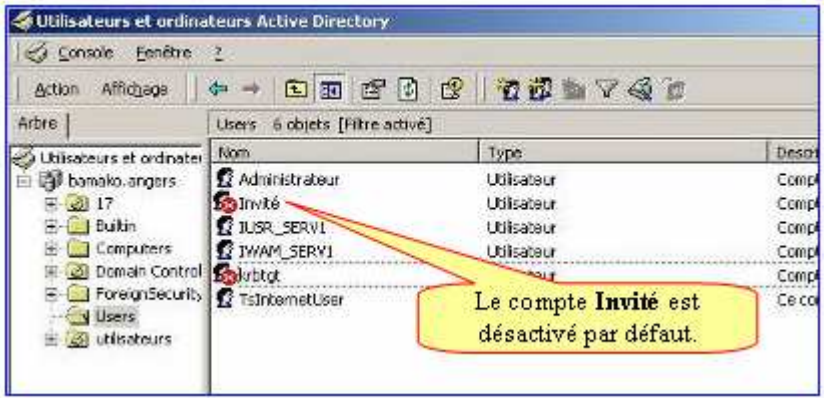
A des fins de sécurité, il est conseillé de renommer le compte Administrateur. Ce compte permet de gérer l'ensemble de la configuration des ordinateurs et du domaine et en particulier la création, modification et suppression des comptes d'utilisateurs et de groupes. Ce compte ne peut être désactivé, sauf si vous avez au préalable créé un utilisateur équivalent. C'est donc la personne qui possède le plus de privilèges sur le micro. Le résumé de ses fonctions est :

- La gestion des comptes d'utilisateurs et des comptes de groupes.
- La gestion des stratégies de groupes.
- La création de dossiers et l'installation de fichiers ou d'applications sur le disque dur.
- La modification logicielle du système d'exploitation.
- L'installation et la configuration des imprimantes.
- La gestion des ressources partagées (création, droits).
- La sauvegarde et restauration des données…

✋ Il est vivement conseillé de renommer **l'Administrateur** car il sera plus difficile à une personne malveillante de trouver le mot de passe d'un compte lorsqu'on ne connaît pas le nom du compte. Il est possible à partir des stratégies de groupe ou du registre de ne pas afficher le nom du dernier utilisateur ayant ouvert une session.

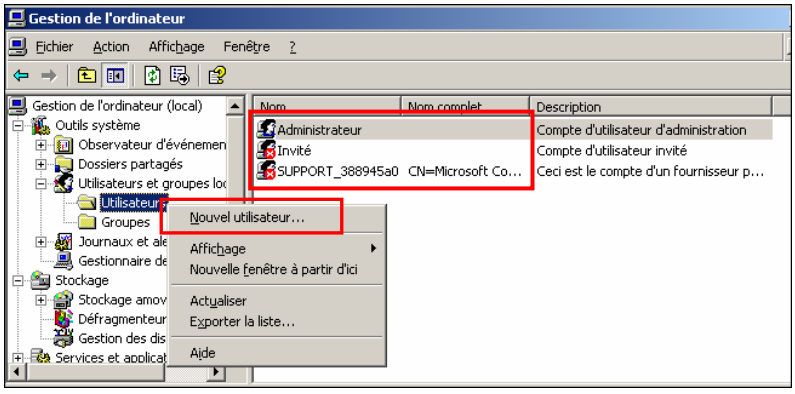
Invité

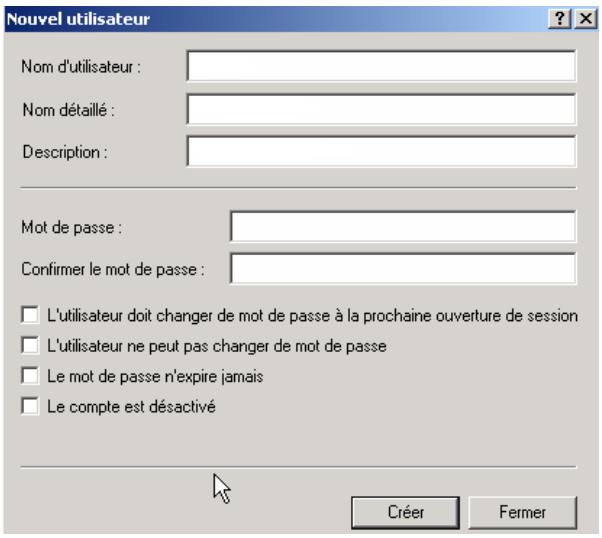
Ce compte d'utilisateur prédéfini permet d'autoriser des utilisateurs occasionnels à ouvrir une session et à accéder aux ressources autorisées. Par défaut, ce compte est désactivé et doit être doté d'un mot de passe. Par mesure de sécurité, il est conseillé de laisser ce compte désactivé, s'il n'est pas utilisé.



5.1.4- Création d'un compte d'utilisateur sur un ordinateur local

Se fait en utilisant la console **Gestion de l'ordinateur** et l'extension **Utilisateurs et groupes locaux**

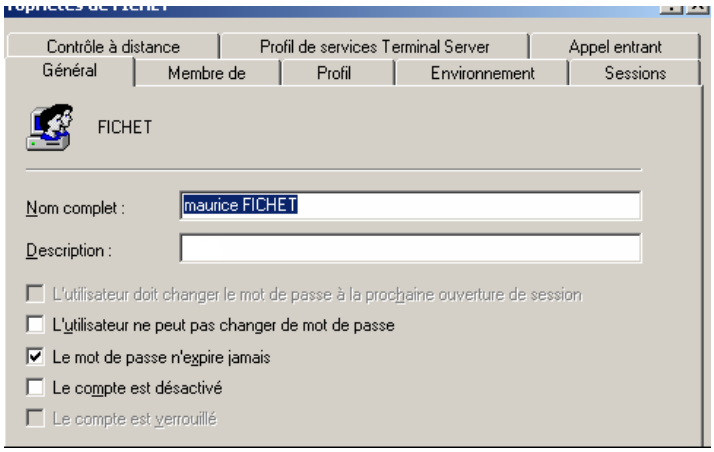




- **Nom d'utilisateur** (obligatoire) : nom saisi par l'utilisateur pour entrer en session (< 20 caractères).
- **Nom détaillé :** c'est le nom complet de l'utilisateur (utilisé à des fins administratives).
- **Description :** indique la fonction de l'utilisateur, sa situation géographique.
- **Mot de passe et confirmer le mot de passe :** à la création du compte, l'administrateur peut définir un mot de passe qu'il devra communiquer à l'utilisateur. Ils n'est jamais visible même par un administrateur.
- **Options de mot de passe :** précisent comment le mot de passe de l'utilisateur doit être changé.
  - **L'utilisateur doit changer le mot de passe à la prochaine ouverture de session :**
    - Concerne la majorité des utilisateurs.
    - Lorsque le compte est créé par l'administrateur, ce dernier force le mot de passe d'ouverture de session.
    - Obliger l'utilisateur à le changer immédiatement garantit que l'administrateur n'en aura plus connaissance et ne pourra pas utiliser l'identité de l'utilisateur (règles sur mot de passe).
  - **L'utilisateur ne peut pas changer le mot de passe** (compte sensible) : utilisé pour les comptes partagés par plusieurs utilisateurs. Garantir qu'un utilisateur ne peut pas changer le mot de passe, c'est s'assurer que les autres auront toujours accès à ce compte.
  - **Le mot de passe n'expire jamais** : cette option outrepasse les paramètres de la Stratégie de Compte (par défaut les mots de passe expirent après 42 jours, option définie dans la stratégie de sécurité locale ou du domaine). Utilisé pour certains comptes qui ne sont pas souvent utilisés (compte système ou compte de secours pour l'administrateur). Lorsque le compte a expiré l'utilisateur est invité à le changer lors de l'ouverture de session.
  - **Le compte est désactivé** : permet d'interdire l'accès aux ressources pour un compte particulier. Les comptes des utilisateurs momentanément absents doivent être désactivés. Un compte désactivé est marqué par une croix rouge sur son icône.

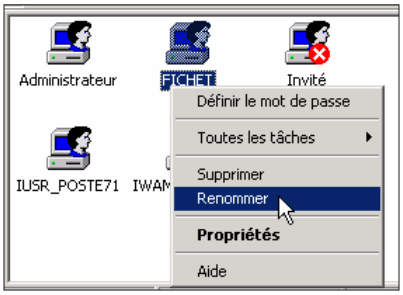
5.1.5- Modifier un compte sur un ordinateur local

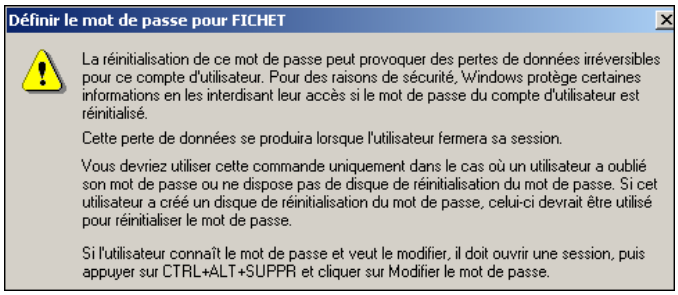
Dés que vous venez de créer un compte local il sera visible dans la liste des utilisateurs de la console **Gestion de l'ordinateur** dans la rubrique **Utilisateur**. Pour modifier les paramètres d'un utilisateur il vous suffit de le sélectionner puis à partir du menu **Action** – **Propriétés** (ou menu contextuel). L'option **Le compte est verrouillé** apparaît en grisé. Cette option sera active avec la mise en place d'une stratégie de groupe qui indiquera de désactiver le compte après un trop grand nombre de tentatives infructueuses d'ouverture de session.

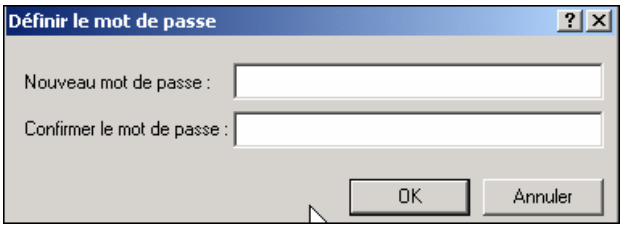


- **Général :** vous permet de modifier les options de base.
- **Membre de :** permet de connaître de quel(s) groupe(s) l'utilisateur fait partie.
- **Profil :** indique le chemin pointant sur le profil de l'utilisateur.
- **Environnement, Sessions, Contrôle à distance et Profil de services Terminal Server :** permettent le paramétrage des propriétés de l'utilisateur lors de l'ouverture de session Terminal Server.
- **Contrôle à distance :** permet d'indiquer si la session de l'utilisateur est sous le contrôle du service Terminal à distance.
- **Appel entrant :** permet de contrôler la façon dont le compte sera gérer lors des accès réseau à distance ou VPN.

Cette fenêtre ne vous donne pas la possibilité de définir le mot de passe ou de renommer un compte utilisateur. Pour renommer, supprimer un compte d'utilisateur ou modifier un mot de passe utilisateur vous devez le sélectionner puis **Action** – **Renommer** – **Action** – **Supprimer** – **Action** – **Définir le mot de passe** (ou via le menu contextuel).







- Si vous renommez un compte utilisateur, les informations rattachées à ce compte ne sont pas perdues (appartenance aux groupes, permissions...).
- Le numéro d'identification de sécurité (**SID**) est unique et n'est pas modifié.
- Modification du nom de Login, mais pas du **SID** (n° identification de sécurité).
- S-1-6-56-34634…/……

5.1.6- Gestion et configuration des comptes utilisateurs dans un domaine

Tout utilisateur souhaitant se connecter sur le réseau et avoir accès à ses ressources doit avoir un compte d'utilisateur de domaine.

Rappels : comme nous l'avons vu précédemment lorsqu'un utilisateur se connecte au domaine, les informations d'ouverture de session sont envoyées à un contrôleur de domaine pour qu'elles soient comparées avec celles contenues dans la base d'annuaire Active Directory. Dès l'identification validée l'utilisateur pourra accéder à toutes les ressources correspondantes à ses permissions.

Compte d'utilisateur de domaine

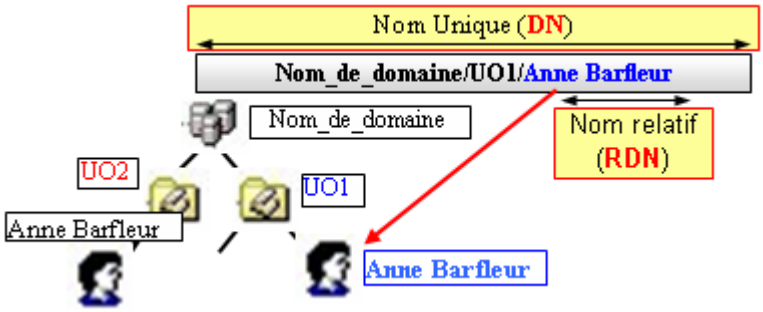
Dans le but de créer de nouveaux utilisateurs, vous devez prendre en compte les trois points suivants :

- Respecter les conventions de dénomination de comptes utilisateurs.
- Planifier la configuration des mots de passe.
- Définir les options de compte.

Comme pour la base locale il existe plusieurs comptes et groupes prédéfinis dans la base **Active Directory**. Parmi ces utilisateurs on retrouve bien évidemment **Administrateur** et **Invité**.

Conventions de noms

- Noms d'utilisateurs uniques. Il peut exister 2 **noms relatifs** dans un même domaine, mais pas dans une même **UO**. Par contre, il ne peut pas y avoir 2 **noms uniques** dans un même annuaire.



- La longueur maximale du nom est de 20 caractères en majuscules ou minuscules. La casse n'est pas prise en compte.
- Certains caractères sont interdits / \ [ ] : ; , + * , < >

Mot de passe

- Il faut systématiquement attribuer un mot de passe à l'administrateur.
- Il faut déterminer si ce sont les administrateurs ou les utilisateurs qui gèrent les mots de passe. En général, ce sont ces derniers qui gèrent leur mot de passe, mais l'administrateur peut les obliger à en changer de manière régulière.
- Les mots de passe doivent être difficiles à deviner pour un intrus éventuel.
- La longueur des mots de passe peut atteindre 128 caractères, une longueur de 5 caractères minimum est recommandée.

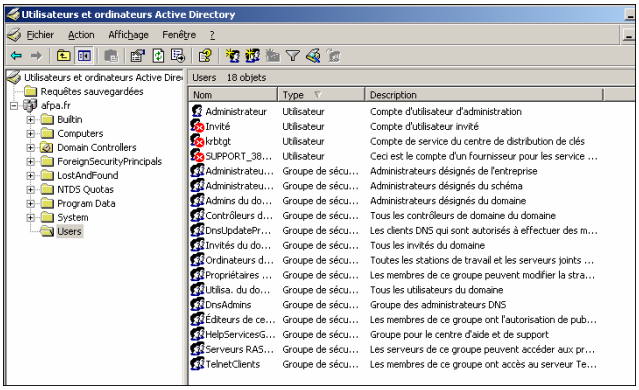
Désormais W2003 comprend des options pour créer des **contrôles de mots de passes** supplémentaires. Ces options sont accessibles dans des filtres de mots de passe pouvant être installés sur un contrôleur de domaine. Exemple de paramètres possibles :

- Les mots de passe doivent comporter au moins 6 caractères.
- Le nom de l'utilisateur ou même une partie de ce nom, ne doit pas apparaître dans le mot de passe.
- Les mots de passe doivent employer trois des quatre types de caractères disponibles : minuscules, majuscules, chiffres et symboles.

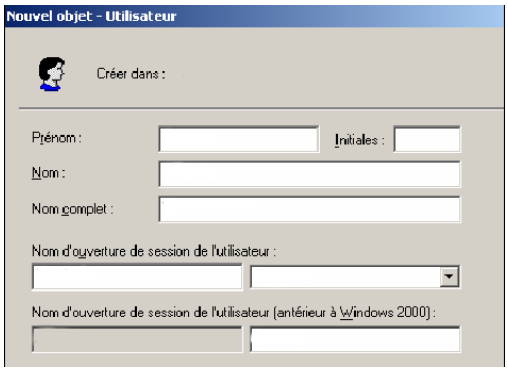
Pour appliquer ces règles il faut activer la stratégie. Le mot de passe doit respecter des exigences de complexité.

Création d'un compte utilisateur de domaine

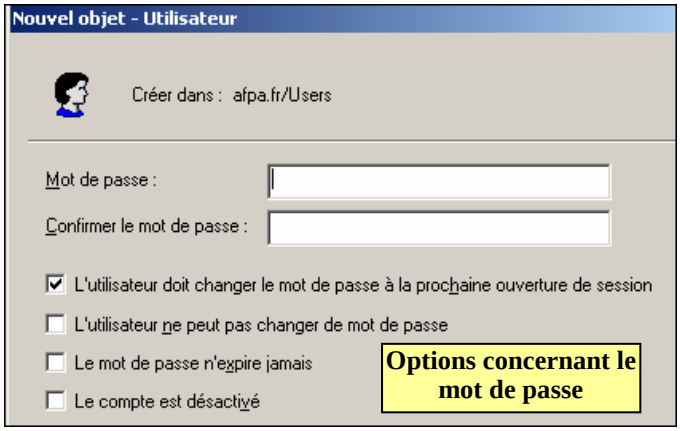
La création de compte d'un domaine se réalise à partir de la console **Utilisateurs et Ordinateurs Active Directory**. Un utilisateur peut être créé dans n'importe quel conteneur. Il suffit de sélectionner l'OU ou le conteneur système cible et à partir du menu contextuel valider **Action – Nouveau – Utilisateur**.



On peut remarquer la création de l'utilisateur **krbtg** qui est un compte ne pouvant être activé. Il est utilisé par le protocole d'authentification Kerberos qui se sert de son mot de passe pour des fonctions de cryptage (nécessite d'activer **Fonctionnalités avancées** du menu **Affichage**).



- **Prénom, Initiales, Nom** : champs permettant de renseigner les prénom, initiales et nom de famille de l'utilisateur.
- **Nom complet** : nom complet de l'utilisateur. Il est obligatoire et unique dans le conteneur (U.O) où l'on crée le compte. Ne doit pas dépasser 64 caractères. Si les champs précédents ont été renseignés, il contient par défaut les champs PRENOM + INITIALES + NOM. Il peut être modifié de façon indépendante des noms précédents.
- **Nom d'ouverture de session de l'utilisateur - UPN** (User Principal Name) : zone de gauche dans laquelle on renseigne le nom d'ouverture de session de l'utilisateur et une zone indiquant le nom de domaine dans lequel on crée l'utilisateur. Les deux réunis constituent le nom principal d'utilisateur, permettant d'ouvrir une session. Obligatoire et unique dans la forêt.
- **Nom d'ouverture de session de l'utilisateur (avant l'installation de Windows 2000)** : nom que devra saisir un utilisateur voulant ouvrir une session d'une station NT4 par exemple. Il doit être unique dans le domaine.
-

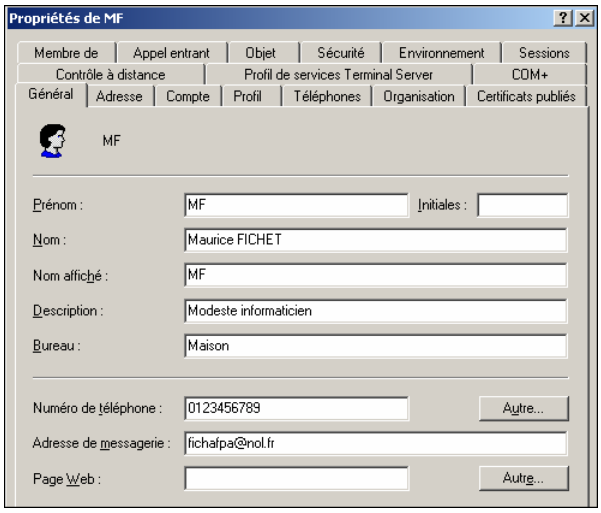


- **Mot de passe et Confirmer le mot de passe :** l'administrateur peut donner un mot de passe à l'utilisateur.
- **L'utilisateur doit changer le mot de passe à la prochaine ouverture de session :** concerne la majorité des utilisateurs. Lorsque le compte est créé par l'administrateur, ce dernier force le mot de passe d'ouverture de session. Cela oblige l'utilisateur à le changer immédiatement. Cela garantit que l'administrateur n'en aura plus connaissance et ne pourra pas utiliser l'identité de l'utilisateur.
- **L'utilisateur ne peut pas changer le mot de passe (compte sensible) :** utilisé pour les comptes partagés par plusieurs utilisateurs. Cela garanti qu'un utilisateur ne peut pas changer le mot de passe, et que les autres auront toujours accès à ce compte.
- **Le mot de passe n'expire jamais :** option qui outrepasse les paramètres de la Stratégie de Compte. Utilisé pour certains comptes qui ne sont pas souvent utilisés (compte système ou compte de secours pour l'administrateur).
- **Le compte est désactivé :** permet d'interdire l'accès aux ressources pour un compte particulier. Les comptes des utilisateurs momentanément absents doivent être désactivés.

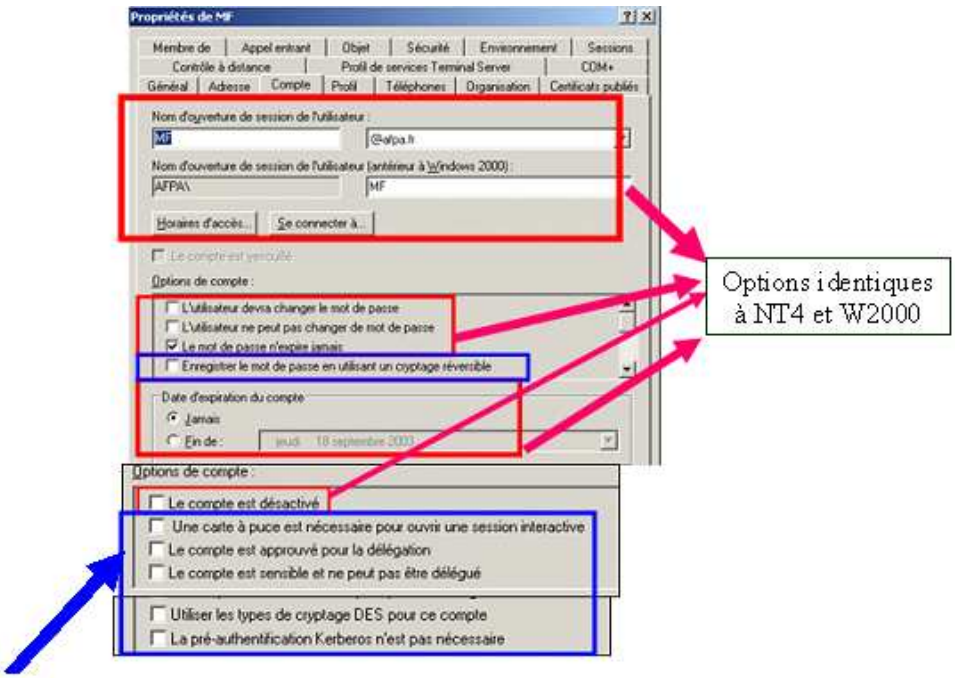
Il est possible d'utiliser la création en ligne de commande d'un compte utilisateur. Pour cela entrez la commande : **User cn=utilisateur, ou=unité_organisationelle, dc=domaine**.

Propriétés d'un compte utilisateur

Sélectionnez l'utilisateur puis **Action** – **Propriétés** (ou menu contextuel).



- **Propriétés personnelles** sont les **attributs** des utilisateurs (@dresse, n° téléphone, email...). Ces informations sont stockées dans la base d'annuaire. Elles permettent de localiser un utilisateur dans AD.
- **Environnement, Sessions, Contrôles à Distance, profiles de services Terminal Server** sont utilisés pour le service Terminal Server.
- **Certificats publiés :** gère les certificats de l'utilisateur.
- **Membre de :** groupe auquel appartient l'utilisateur.
- **Appel entrant :** paramétrage de l'utilisateur d'accès distant.
- **Objet :** informations sur les dates de création, modification de l'objet et affichage du N° USN.
- **Sécurité :** droits d'accès sur l'objet utilisateur.
- **Général :** infos générales de type nom, prénom….
- **Adresse, Téléphone, Organisations :** informations de types générales sur l'utilisateur.



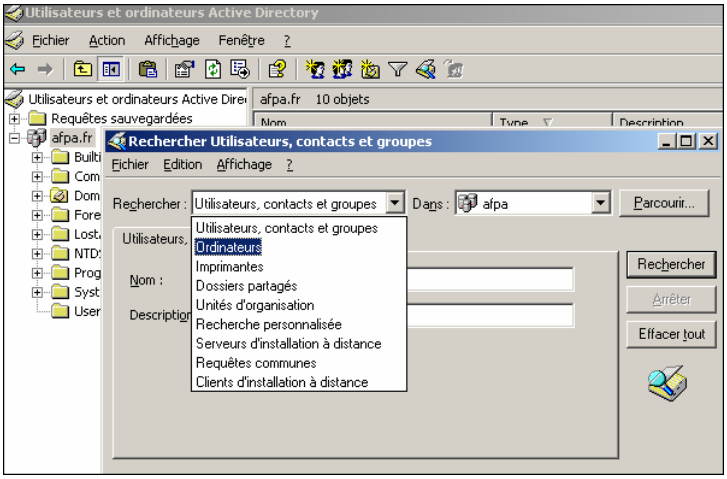
Nouvelles options de Windows 2003 Server

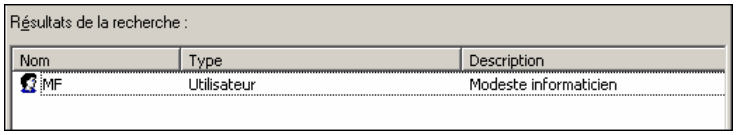
- **Enregistrer le mot de passe en utilisant un cryptage réversible :** permet à un utilisateur de MAC d'ouvrir une session.
- **Une carte à puce est nécessaire pour ouvrir une session interactive.**
- **Le compte est approuvé pour la délégation :** permet à un service exécuté au moyen de ce compte d'effectuer des opérations au nom d'autres comptes d'utilisateurs du réseau.
- **Le compte est sensible et ne peut être délégué :** s'il n'est pas souhaitable d'utiliser la délégation pour ce compte pour des raisons de sécurité.
- **Utiliser les types de cryptage DES pour ce compte.**
- **La pré-authentification Kerberos n'est pas nécessaire :** dans le cas de certaines implémentations différentes de Kerberos.

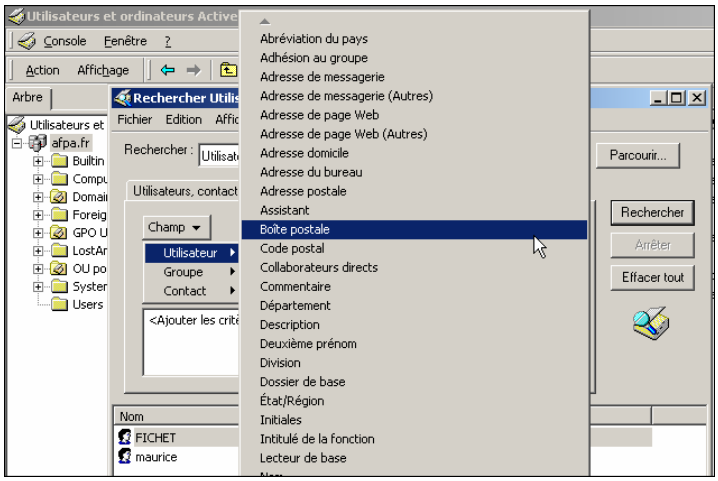
Rechercher des personnes, ordinateurs ou objets dans Active Directory

A l'aide des renseignements que vous venez de rentrer dans la saisie du compte utilisateur par exemple, vous pouvez retrouver un utilisateur dans tout Active Directory. Et ce de deux façons. **Menu Action** – **Rechercher** de la console **Utilisateurs et ordinateurs Active Directory**. Validez le menu **Action** – Rechercher ou utiliser les requêtes enregistrées dans la rubrique **Requêtes sauvegardées.** Ou à partir des fonctions classiques du menu **Démarrer** – **Rechercher** en indiquant de réaliser cette recherche dans Active Directory.

Dès le contact établi avec la personne recherchée ou l'objet de nombreuses actions peuvent être entreprises telles que : envoi d'un message électronique, ouvrir sa page Internet...





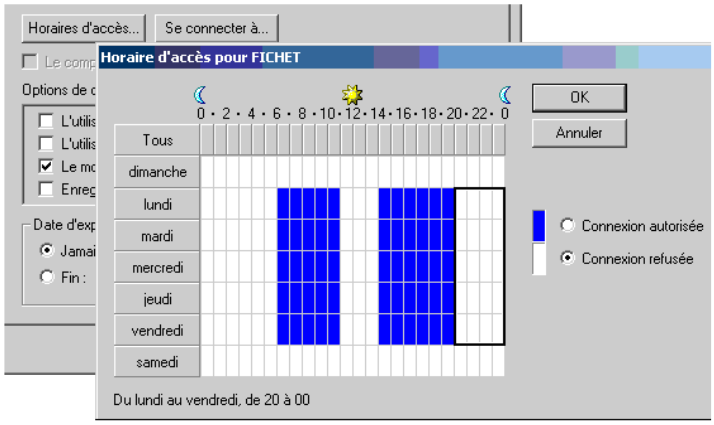


Cette recherche peut être réalisée en mode commande en tapant la commande en ligne **DSQUERY**.

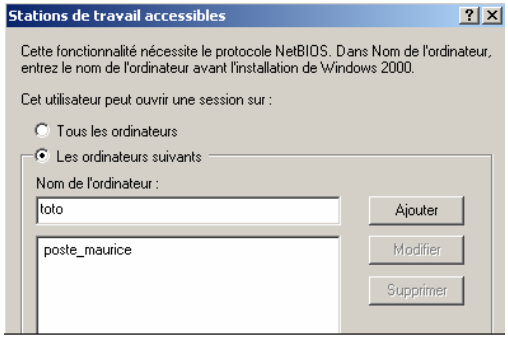
Options de compte

Vous pouvez attribuer certaines options au compte de chaque utilisateur.

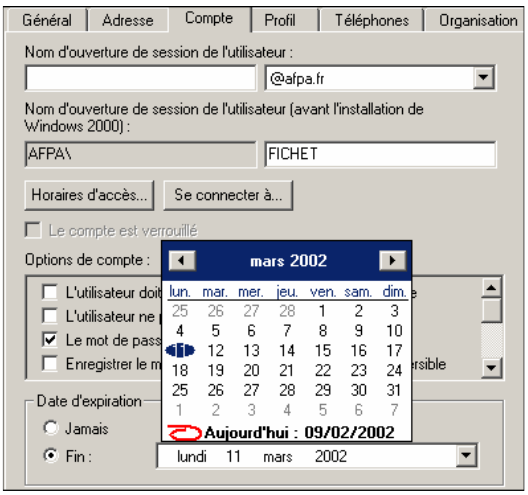
- **Heures de disponibilité ou restrictions d'horaires :** vous pouvez restreindre les heures d'accès de l'ordinateur de manière à ce que des intrus ne puissent utiliser l'ordinateur pendant l'absence de l'utilisateur autorisé. Il vous suffit de définitif des heures d'ouverture de session (**Horaire d'accès**).



- **Ordinateurs autorisés :** vous pouvez autoriser la connexion au réseau à certains utilisateurs qu'à partir d'un seul ou de plusieurs ordinateurs. Cette fonction nécessite que le protocole NetBIOS sur TCP/IP soit activé (onglet **Propriétés avancées** de TCP/IP). C'est ce protocole qui permet d'identifier les ordinateurs par leurs noms. Par défaut, les utilisateurs peuvent travailler en réseau à partir de n'importe quel ordinateur du domaine.

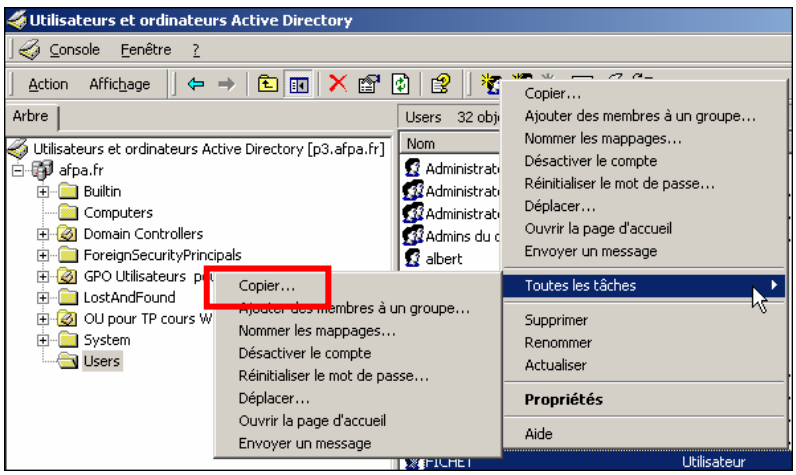


- **Expiration de compte :** si votre entreprise embauche des employés temporaires, ajoutez l'option **Date d'expiration de compte**. A la fin de leur contrat, leur compte est automatiquement désactivé.



Copie d'un compte utilisateur : c'est utile si vous avez de nombreux utilisateurs identiques à créer. Vous devez choisir un compte modèle puis à partir du menu **Action** – **Copier** (ou menu contextuel). Avec une copie les éléments suivants sont conservés :

- Restrictions d'horaires.
- Majorité des options de comptes sur le mot de passe.
- Restriction d'accès.
- Date d'expiration.
- Appartenance aux groupes.
- Options de profil et de dossier de base (à condition que la variable %username% soit utilisée à la place du nom d'utilisateur).



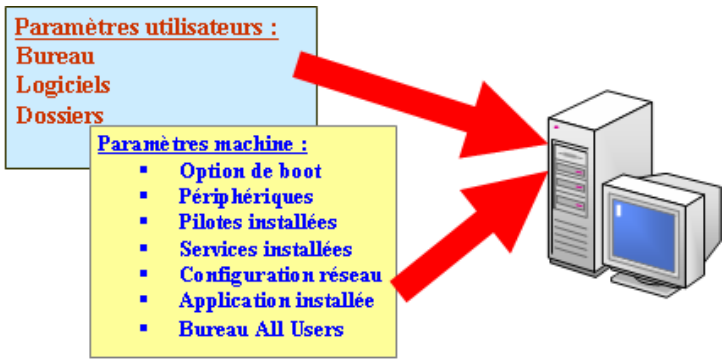
5.2- Profils

5.2.1- Profil par défaut et profil utilisateur

Un **profil utilisateur** est un ensemble de dossiers et de données qui représentent :

- L'environnement du bureau.
- Les paramètres d'un utilisateur.
- Ses données personnelles.
- Ses connexions réseau.
- La liste des programmes qui apparaissent dans le menu **Démarrer**.

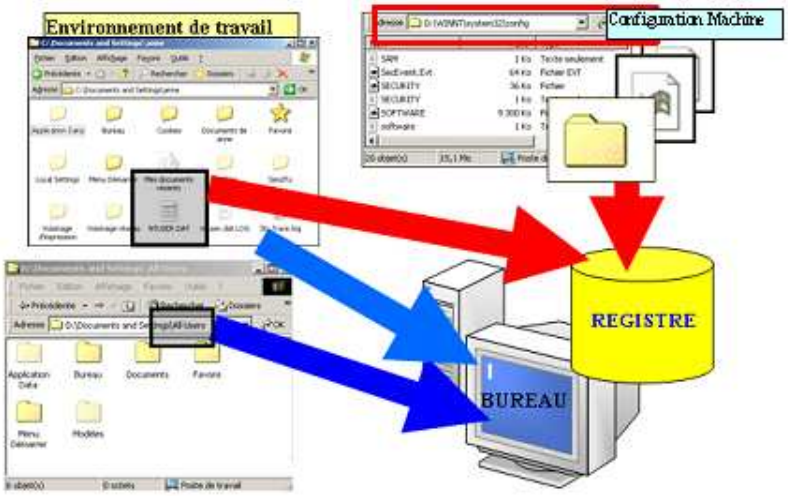
Le profil utilisateur permet à chaque utilisateur à l'ouverture de chaque session de retrouver un environnement de travail identique. Lorsqu'un utilisateur se connecte, l'environnement de travail se compose de paramètres spécifiques à l'utilisateur et de paramètres spécifiques à la machine. Tous les paramètres utilisateurs sont désignés sous le nom profil utilisateur. Dossiers personnels et données du registre, à l'exception des paramètres du bureau pour All Users, les paramètres machine résident dans le Registre local.

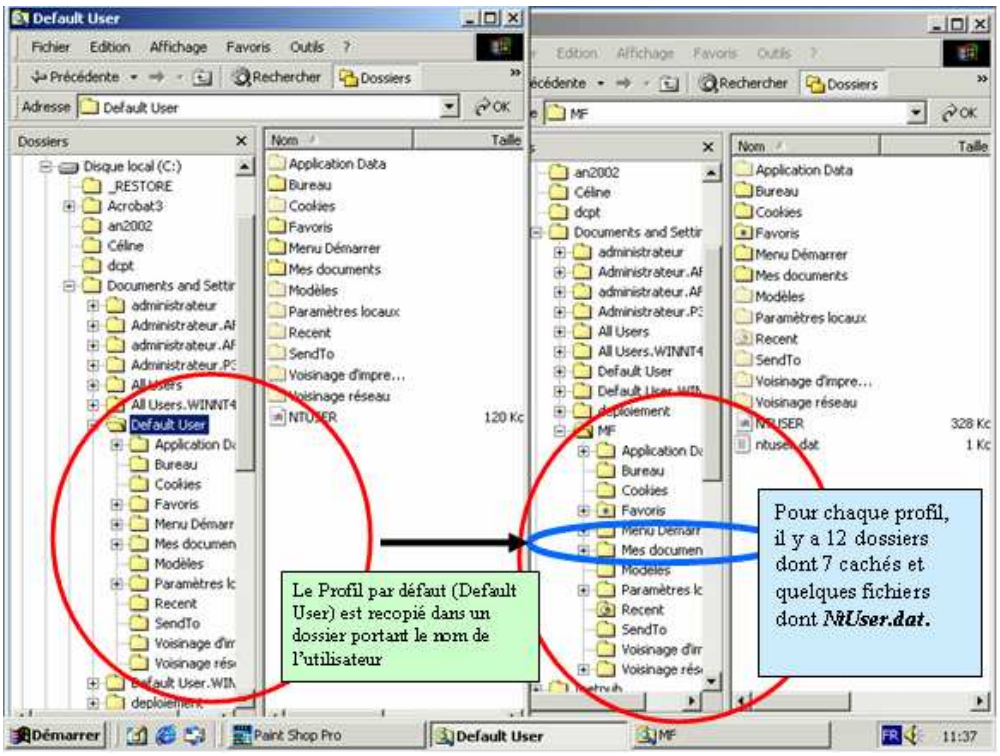


- Pour une nouvelle installation de W2003, les profils sont stockés dans **%SystemDrive%\Documents and Settings.**
- Pour une mise à jour de Windows NT ou 9x les profils sont stockés dans **%SystemRoot%\Profiles.**

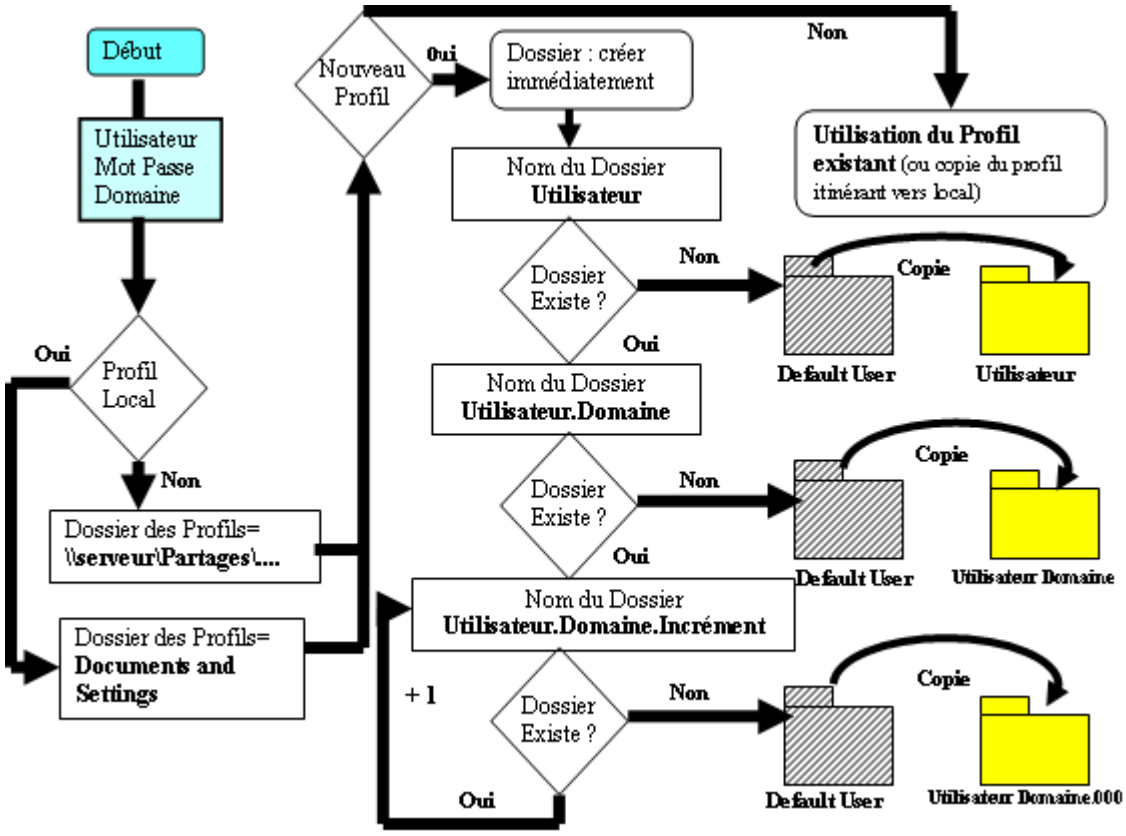
Lorsqu'un utilisateur ouvre la première fois une session sur un ordinateur, le profil par défaut (profil Default User) est copié dans un répertoire C:\Winnt\Documents and Settings\<nom_de_l'utilisateur>.

Si des modifications sont apportées à l'environnement (bureau, données, lecteurs réseaux…), elles sont enregistrées dans le profil de l'utilisateur. Le dossier **Mes Documents** contient tous les fichiers créés par un utilisateur. En effet, par défaut, les commandes **Ouvrir** et **Enregistrer sous…** des applications Microsoft pointent vers le dossier **Mes Documents**. Pour chaque profil, il y a 12 dossiers dont 7 cachés et quelques fichiers dont **NtUser.dat.**

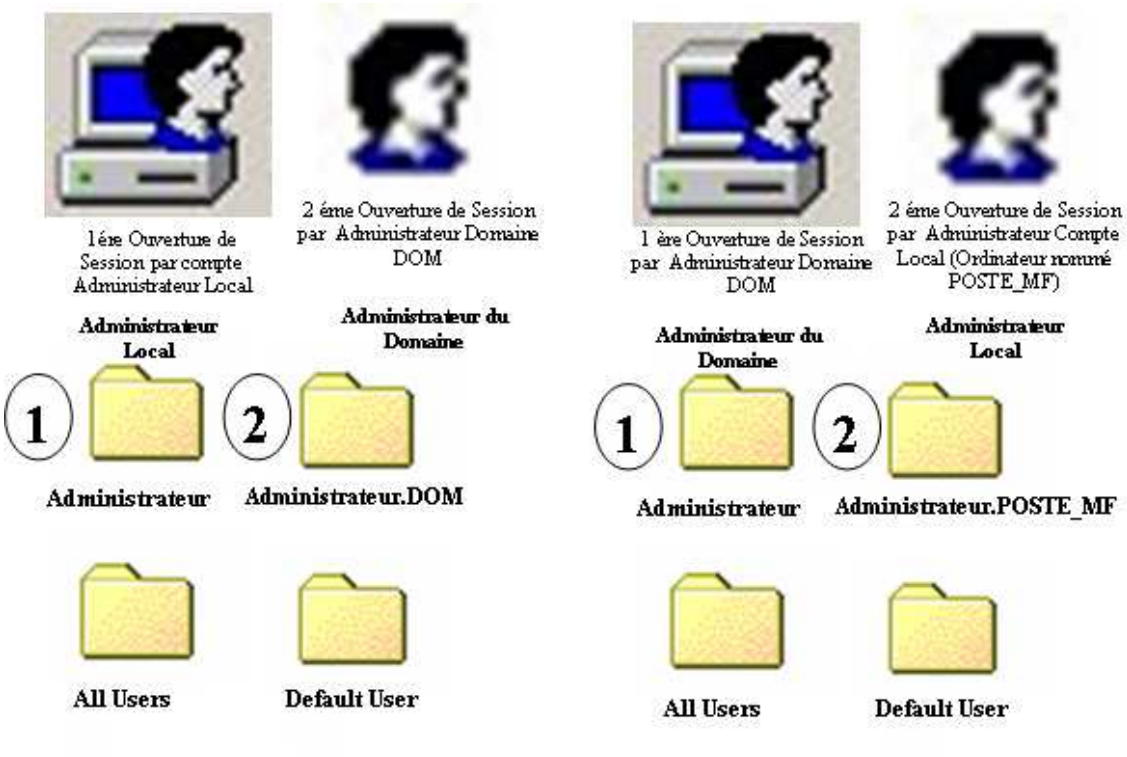




Résumé Profil par défaut



Nous avons vu qu'un utilisateur retrouve son environnement de travail à chaque ouverture de session. Par contre si un utilisateur dispose d'un même nom pour se connecter en local et sur un domaine, deux dossiers différents seront créés. En fait lors de l'ouverture de session le système va essayer de créer un dossier portant le nom de l'utilisateur, mais si un dossier portant le même nom existe déjà, W2003 va automatiquement ajouter le nom du fournisseur de sécurité (domaine ou local) en tant qu'extension.

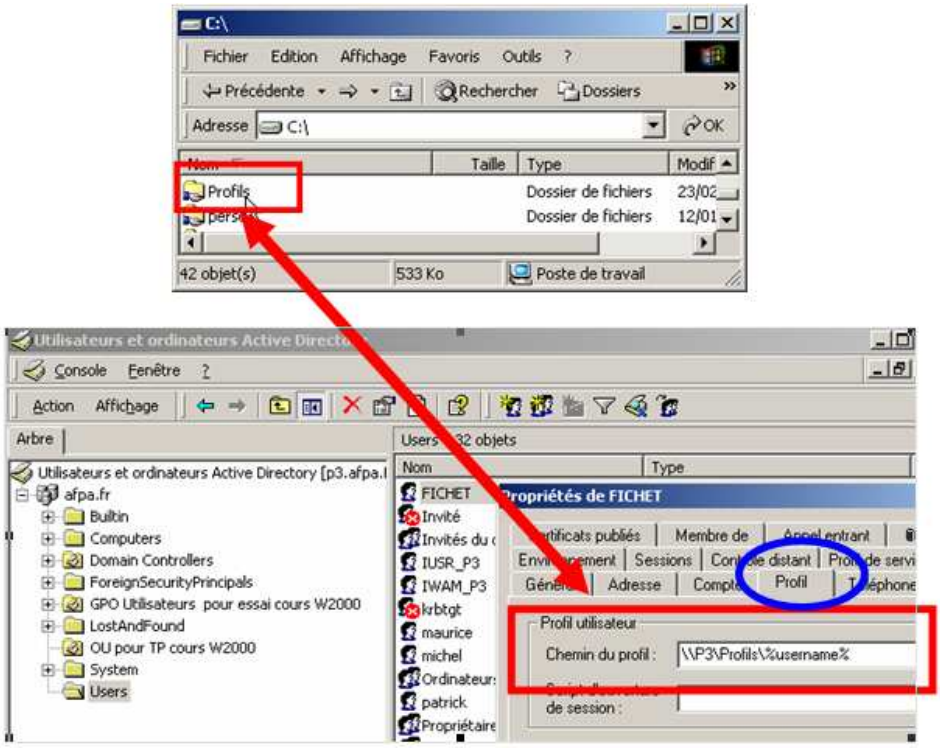


5.2.2- Profils d'utilisateurs itinérants

Si un utilisateur travaille sur plusieurs ordinateurs, il risque d'avoir des profils différents sur chaque machine. Pour qu'il puisse retrouver un environnement identique, son profil va être stocké sur un serveur. Lorsque le profil itinérant existe sur le serveur, au moment de la connexion de l'utilisateur, son profil est transmis du serveur vers l'ordinateur sur lequel la session a été ouverte. L'utilisateur retrouve ainsi tous ses paramètres de travail et en particulier son bureau habituel. Le fichier qui contient le profil itinérant est nommé **Roaming User Profil**, RUP. A la première session ouverte sur un ordinateur par un utilisateur itinérant, le fichier RUP est copié sur l'ordinateur ainsi que les données contenues dans le profil de l'utilisateur. A l'ouverture des sessions suivantes, le contenu du profil local est comparé au contenu du profil sur le serveur. La mise à jour est effectuée automatiquement. A chaque fermeture de session, les modifications apportées au profil local sont envoyées au profil contenu sur le serveur.

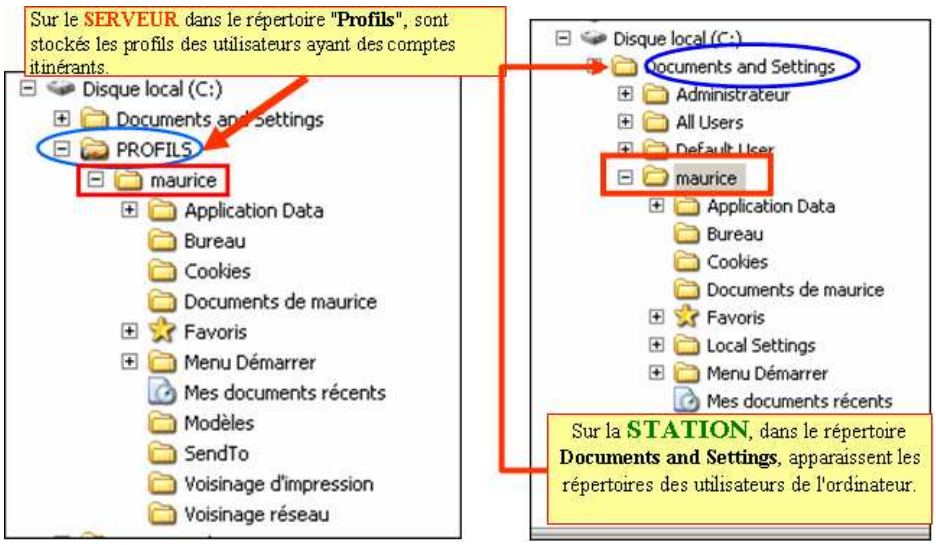
Profils obligatoires
Si vous avez créé des profils d'utilisateurs itinérants et que vous souhaitez qu'ils ne soient pas modifiés, vous les positionnez en **mode lecture seule**. De cette manière, les utilisateurs travaillent dans l'environnement qui leur a été assigné. Le fichier **Ntuser.dat** contient les paramètres d'environnement de l'utilisateur. Si l'accès de ce fichier sur le serveur est en lecture seule, l'utilisateur recharge toujours le même environnement, et le fichier sur le serveur ne peut être modifié, même si l'utilisateur a opéré des modifications en cours de session. Cette opération s'effectue en renommant le fichier **NtUser.dat** en **NtUser.man**.

Configuration d'un profil d'utilisateur itinérant
Les fichiers RUP peuvent être placés soit sur le serveur contrôleur de domaine, soit si la charge de ce serveur est importante, sur un autre serveur membre. Les fichiers RUP sont à positionner dans un dossier partagé \\serveur\partage. Il est conseillé de nommer le partage profils.
Dans l'onglet **Profil** de la boîte de dialogue **Propriétés** du compte utilisateur, indiquez le chemin, suivi du nom de l'utilisateur \\serveur\profils\NomUtilisateur ou encore \\serveur\profils|%uservame%. **%username%** sera remplacé par le nom de l'utilisateur.
Ce travail se fait de préférence sur le serveur en ouvrant la console **Utilisateurs et ordinateurs Active Directory** dans **Outils d'administration**.



Profils itinérants

Sur la station, à la première connexion de l'utilisateur, s'il est reconnu par la station, le profil par défaut est copié dans le profil utilisateur. Au moment de la déconnexion, le profil de l'utilisateur est recopié sur le serveur dans le chemin indiqué.

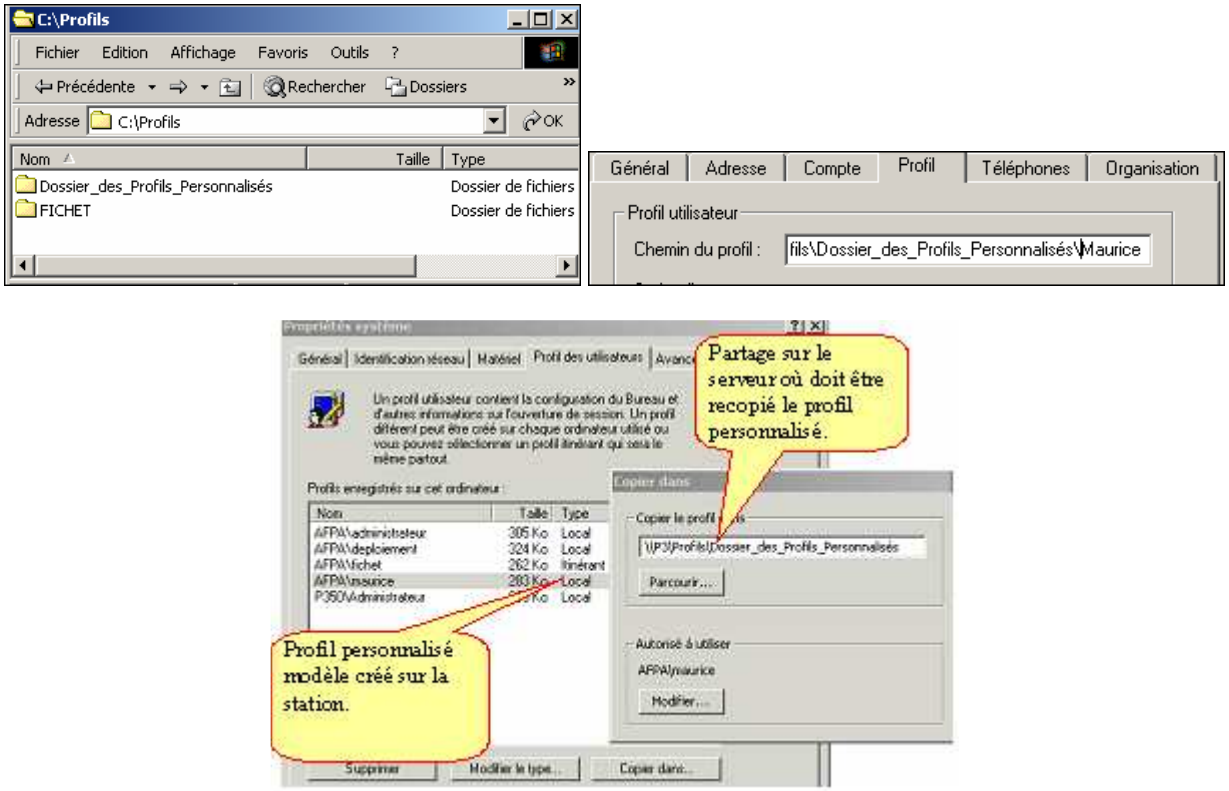


Création d'un profil itinérant personnalisé

Il est possible par ailleurs de créer des profils RUP préconfigurés que vous attribuez à tous les comptes utilisateurs. Vous pouvez aussi rendre les profils d'utilisateurs itinérants obligatoires en les mettant en lecture seule de manière à ce que les utilisateurs ne puissent modifier leur environnement. Intérêts des profils d'utilisateurs itinérants RUP personnalisés :

- Fournir un environnement standard aux utilisateurs itinérants, et supprimer l'accès à des ressources et applications dont ils n'ont pas besoin.
- Fournir un environnement standard à un groupe d'utilisateurs assurant dans l'entreprise des fonctions similaires.
- Faciliter la maintenance logicielle en connaissant l'environnement logiciel de chaque utilisateur.

Pour créer un profil itinérant personnalisé, sur la station, il suffit de créer un profil type. Puis, vous vous connectez en tant qu'Administrateur et dans **Système** du **Panneau de configuration**, vous recopiez le profil dans un partage du serveur en utilisant l'onglet **Profil des utilisateurs** et la commande **Copier le profil dans…**. Le profil est attribué automatiquement au groupe prédéfini Users du domaine.



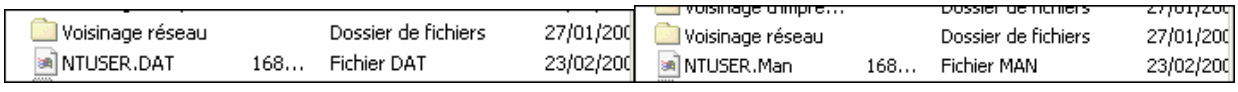
Ensuite, sur le serveur, vous ouvrez la console **Utilisateurs et ordinateurs Active Directory**. Puis dans **Propriétés** du compte utilisateur, vous indiquez le chemin de son profil.

Profil itinérant personnalisé obligatoire

Si vous voulez toujours utiliser le même profil utilisateur itinérant et que vous désirez qu'il ne soit pas modifié, vous devez mettre ce profil en mode lecture seule. Dans ce cas, les utilisateurs travailleront dans l'environnement qui leur a été assigné. Le fichier **Ntuser.dat** stocke les paramètres d'environnement de l'utilisateur. Si l'accès de ce fichier sur le serveur est en lecture seule, l'utilisateur recharge toujours le même environnement.

Le fichier sur le serveur ne pourra jamais être modifié, même si l'utilisateur a opéré des modifications en cours de session.

Sur le serveur, pour éviter les modifications du profil personnalisé obligatoire, modifiez le nom du fichier caché **NtUser.dat** en **NtUser.man.**



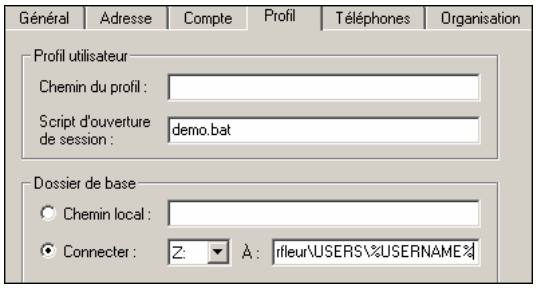
5.2.3- Dossier de base

En plus du dossier **Mes Documents**, il est possible sous Windows 2003 de créer un **dossier de base** pour chaque utilisateur. C'est le répertoire par défaut local (utilisateur sédentaire) ou distant (utilisateur itinérant ou nomade) sur un répertoire partagé du serveur réseau où le système va placer l'utilisateur à l'ouverture de session Le **dossier de base** peut se situer soit sur l'ordinateur de travail, soit dans un partage sur un serveur. Le dossier de base peut être une racine DFS. De cette façon les utilisateurs itinérants peuvent accéder à leurs données à partir de plusieurs ordinateurs.

Les utilisateurs peuvent s'en servir pour stocker, ou récupérer des dossiers personnels
De nombreuses applications utilisent ce dossier comme destination par défaut des opérations **Enregistrer** ou **Enregistrer sous**, ce qui fait que les données sont faciles à retrouver.
Par défaut, ils seront placés dans ce dossier de base à l'ouverture d'une **Invite de commande**.
Cette méthode de travail facilite les sauvegardes. Pour utiliser un dossier de base, il faut :

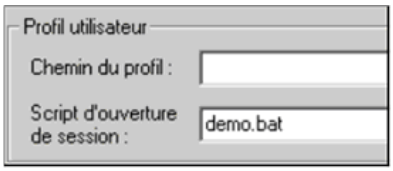
- Créer un dossier partagé sur le serveur. Les dossiers de base de chaque utilisateur y seront stockés.
- Donner l'autorisation **Contrôle total** aux groupes **Users** sur ce partage.
- Sur le serveur, indiquez le chemin du dossier de base dans l'onglet **Profil** des **Propriétés** du compte de chaque utilisateur.

Profil ➔ Dossier de Base➔ Connecter lettre de lecteur ➔ entrez un chemin d'accès réseau vers un répertoire partagé sur le serveur.
La connexion au répertoire de base sera restaurée automatiquement à chaque ouverture de session
Exemple : lecteur **Z:** chemin: **\\Barfleur\Users\%UserName%.**
La variable d'environnement \%UserName% prend le nom de l'utilisateur courant.

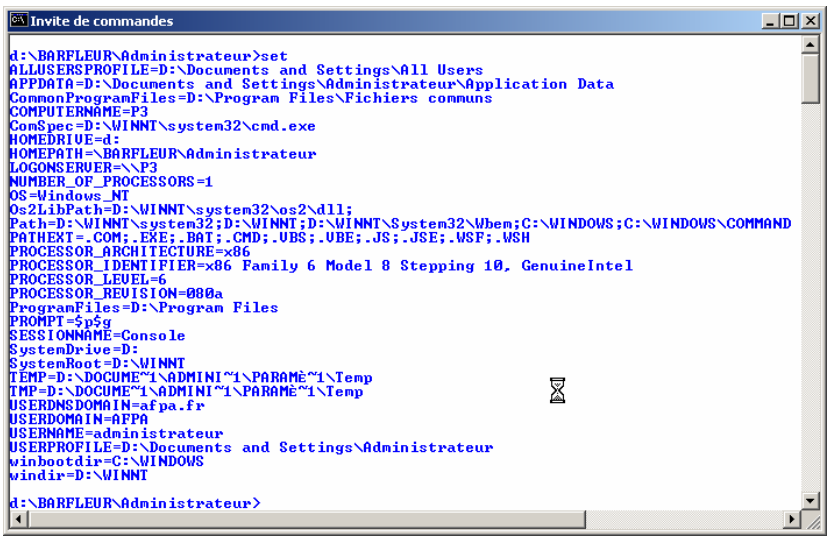


5.2.4- Scripts d'ouverture de session

Windows Server 2003 cherche les scripts d'ouverture de session toujours au même endroit : dans le dossier **%systemroot%\SYSVOL\sysvol\domaine\scripts** du contrôleur utilisé pour l'authentification..
Quand vous tapez le nom d'un script dans la zone **Script d'ouverture de session** de la rubrique **Profil utilisateur** vous n'avez pas besoin de taper le chemin du dossier.



C'est un fichier de commandes exécuté à l'ouverture de session de type **Windows script** ou **Javascript, .vbs** ou de type fichier de commande **.bat, .cmd ou .exe**
Il est facultatif, stocké sur le contrôleur de domaine, téléchargé et exécuté à l'ouverture de session par l'utilisateur.
Aspect procédure : possibilités de tests, d'établissement de connexions réseau, de lancement d'applications, réglage de l'horloge du système, définir les chemins des lecteurs du réseau...
Pour définir un **script**, entrez son nom dans **Script d'ouverture de session**, ne donnez que le nom du script sans le chemin. Pour créer des scripts communs à plusieurs utilisateurs, utiliser des variables d'environnement. Pour visualiser la valeur de ces variables, utilisez la commande **set** dans une fenêtre **Invite de commande** :

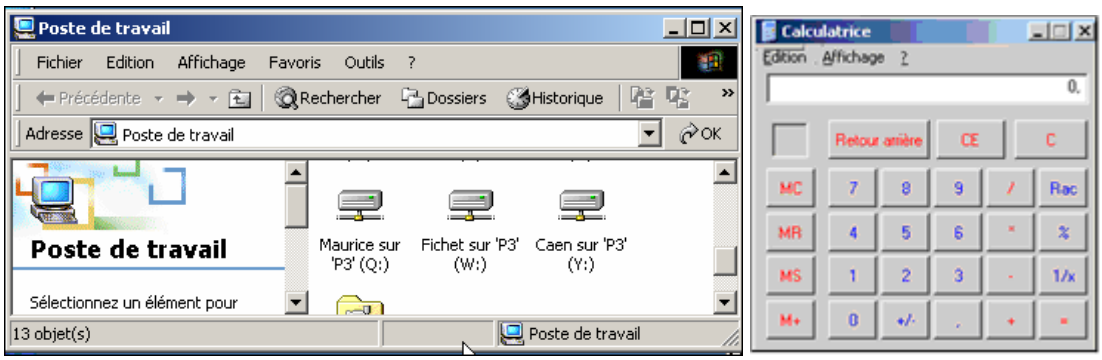


Principales variables d'environnement utilisables dans un script

%HOMEDRIVE%	Lecteur du répertoire de base (disque local ou unité réseau).
%HOMEPATH%	Répertoire de base.
%HOMESHARE%	Nom de partage contenant le répertoire de base.
%OS%	Système d'exploitation.
%PROCESSOR_ ARCHITECTURE%	Type de processeur (par exemple x86).
%USERDOMAIN%	Domaine contenant le compte de l'utilisateur.
%USERNAME%	Nom de l'utilisateur.

Exemple de Script.

```
Rem "Fichier de démo pour cours Windows 2003"
@echo off
if ¨%Username%¨ == ¨Administrateur¨ goto Admin
Goto end
:Admin
@echo off
@Echo Vous êtes l'utilisateur (connecté)  ayant le compte utilisateur:   %USERNAME%
@Echo  L'ordinateur  sur  lequel  est  exécuté  ce  script  de  connexion  porte  le  nom  de:
%computername%
@Echo Le nom du système d'exploitation installé sur l'ordinateur sur lequel vous exécutez le script
d'ouverture de session est:  %OS%
NET view
pause
Net ver
pause
NET USE  w: \\P3\FICHET
net use q: \\P3\MAURICE
net use y: \\P3\CAEN
time
date
calcl.exe
echo on
:end
```



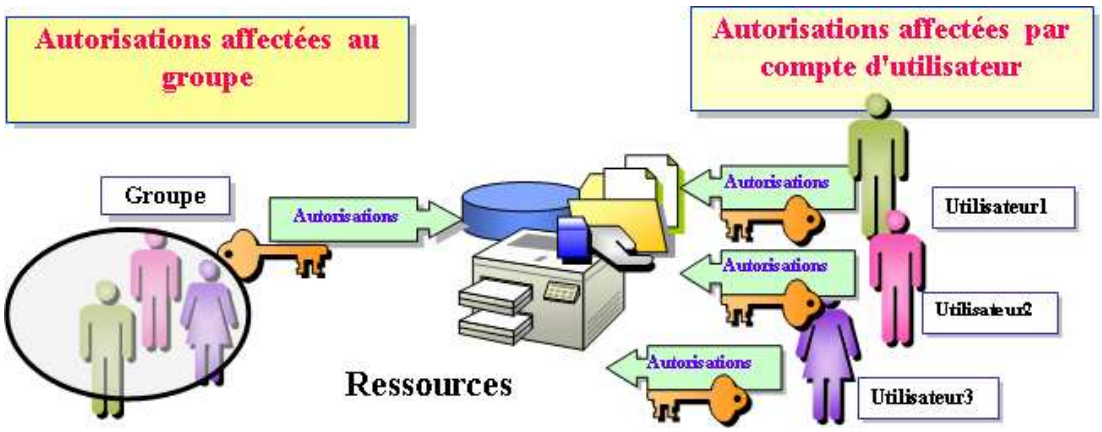
5.3- Comptes de groupe

5.3.1- Qu'est-ce qu'un groupe ?

Un groupe est un ensemble de comptes d'utilisateurs. Cette notion permet de simplifier la gestion des autorisations et des droits sur les ressources partagées. Il est en effet plus rapide et plus sûr de donner des autorisations à un groupe d'utilisateurs sur un partage que de le faire utilisateur par utilisateur. Un même utilisateur peut être membre de plusieurs groupes.

- Simplifie l'administration
- Ensemble de comptes utilisateurs avec des besoins identiques au niveau administration.
- Plus facile de donner des permissions au groupe qu'individuellement à chaque utilisateur.
- Les permissions et droits imputés à un groupe sont affectés à tous les utilisateurs de ce groupe.
- Un utilisateur peut faire partie de plusieurs groupes.

☞ Sur un serveur membre/autonome ou une station un seul type de groupe peut être créé, ce sont des groupe **locaux.**



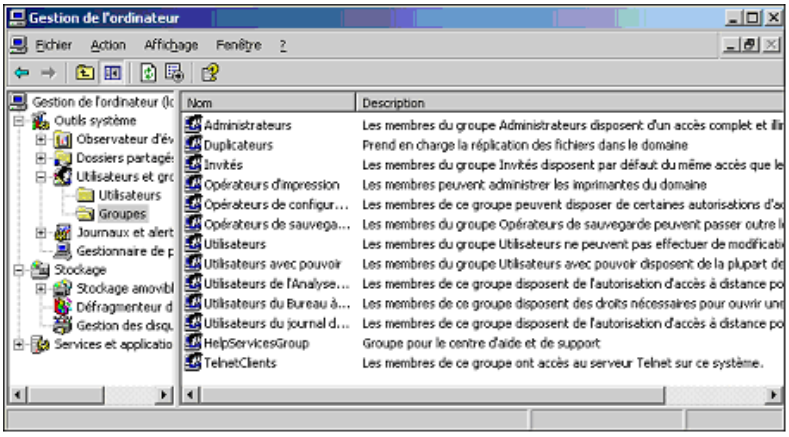
- Les groupes sont des ensembles de comptes d'utilisateurs.
- Les membres d'un groupe bénéficient des autorisations accordées au groupe.
- Les utilisateurs peuvent être membres de plusieurs groupes.
- Les groupes et les ordinateurs peuvent être membres d'autres groupes.

Groupes prédéfinis sur un ordinateur local

Lors de l'installation de W2003 Server (serveurs membres/autonomes) des groupes appelés prédéfinis sont automatiquement créés.

Ils possèdent des droits prédéterminés pour réaliser certaines tâches sur le micro local : sauvegardes, administration et gestion des ressources et ils ne peuvent pas être supprimés.

➡ **Groupes prédéfinis standards**



Administrateurs

- Les membres peuvent réaliser toutes les tâches d'administration du micro.
- A l'installation seul le compte Administrateur en fait partie.
- Lorsque votre station/serveur autonome intègre un domaine, vous constatez que le groupe Global administrateurs du domaine est automatiquement intégré au groupe local administrateurs de votre station ou serveur. Les administrateurs du domaine pourront gérer toutes les stations de leur domaine.
- Identificateur de sécurité (S-1-5-32-544).

Invités

- Utilisation occasionnelle avec un minimum de droits.
- Par défaut le compte Invité est inclus dans ce groupe.
- Identificateur de sécurité (S-1-5-32-546).

Opérateurs de sauvegardes

- Les membres gèrent les sauvegardes et restauration des données avec le **Gestionnaire de sauvegarde** de W2003.
- Identificateur de sécurité (S-1-5-32-551).

Utilisateurs

- Dès que vous créez un compte utilisateur il fait partie de ce groupe.
- Exécutent les tâches que vous avez indiquées.
- N'accèdent qu'aux ressources auxquelles vous avez donné des permissions.
- Lorsque votre station/serveur autonome intègre un domaine, vous constatez que le groupe Global utilisateurs du domaine est automatiquement intégré au groupe utilisateurs de votre poste.
- Identificateur de sécurité (S-1-5-32-545).

Utilisateurs avec pouvoir

- Les membres de ce groupe peuvent partager les ressources, créer et modifier les comptes utilisateurs de la SAM locale.
- Peuvent effectuer des tâches administratives sans avoir un contrôle total sur la machine.
- Identificateur de sécurité (S-1-5-32-547).

Opérateurs d'impression :

- Les membres peuvent gérer, créer, partager des imprimantes. Ils peuvent aussi installer/supprimer les pilotes d'imprimantes. Il ne contient aucun membre par défaut.
- Identificateur de sécurité (S-1-5-32-550).

Opérateurs de configuration réseau :

- Les membres peuvent modifier tous les paramètres réseau du micro, renouveler ou libérer une adresse IP dynamique, activer/désactiver une interface ou créer une connexion d'accès distant ou réseau. Il ne contient aucun membre par défaut.
- Identificateur de sécurité (S-1-5-32-556).

Utilisateurs des journaux de performances

- Les membres de ce groupe peuvent utiliser ou modifier les compteurs, alertes et journaux de performances pour surveiller ou diagnostiquer un dysfonctionnement du micro local ou à distance. Ils peuvent aussi utiliser le moniteur système. Par défaut le groupe **Système Réseau** est membre de ce groupe.
- Identificateur de sécurité (S-1-5-32-559).

Utilisateurs de l'Analyseur de performances

- Les membres de ce groupe peuvent utiliser le moniteur système situé dans l'analyseur de performances localement ou à distance. Par contre la modification des journaux de performances leur est interdite. Aucun membre par défaut.
- Identificateur de sécurité (S-1-5-32-558).

Utilisateurs du Bureau à distance

- Les membres de ce groupe peuvent ouvrir une session de type Terminal serveur sur le micro à partir du moment où la fonctionnalité bureau à distance est activée. Les membres peuvent être aussi gérés la configuration du bureau à distance. Aucun membre par défaut.
- Identificateur de sécurité (S-1-5-32-555).

D'autres groupes sont créés en fonction des services installés :

- **Administrateurs DHCP :** les membres de ce groupe peuvent administrer le service DHCP.
- **Utilisateurs Terminal Server :** les utilisateurs ayant ouvert une session Terminal Server font partie de ce groupe.
- **Utilisateurs Wins :** les utilisateurs de ce groupe ont accès en lecture seule aux informations du service Wins.

➡ **Groupes Prédéfinis Spéciaux ou Groupes dits Systèmes**

Ils existent sur tous les ordinateurs W2003. Ce sont des groupes non administrables car ils sont gérés par le système d'exploitation. Ils représentent les utilisateurs dans des circonstances particulières telles l'accès à des ressources partagées ou à certains ordinateurs du réseau.

Tout le Monde

- Inclus tous les utilisateurs, ceux que vous avez créés, le compte invité plus les autres utilisateurs des domaines.
- Dispose par défaut la permission contrôle total lorsque vous partagez une ressource.
- Identificateur de sécurité (S-1-1-0).

Utilisateurs authentifiés

- Inclus tout utilisateur possédant un compte d'utilisateur et un mot de passe pour la machine locale ou Active Directory. Donnez de préférence des permissions à ce groupe plutôt qu'au groupe Tout le Monde.
- Identificateur de sécurité (S-1-5-11).

Créateur Propriétaire

- Inclus toute personne ayant créé ou pris possession d'une ressource, est membre de ce groupe pour la ressource concernée.
- Il possède les pleins pouvoirs sur cette ressource.
- Identificateur de sécurité (S-1-3-0).

Réseau

- Inclus toute personne accédant à une ressource par le réseau.
- Identificateur de sécurité (S-1-5-2).

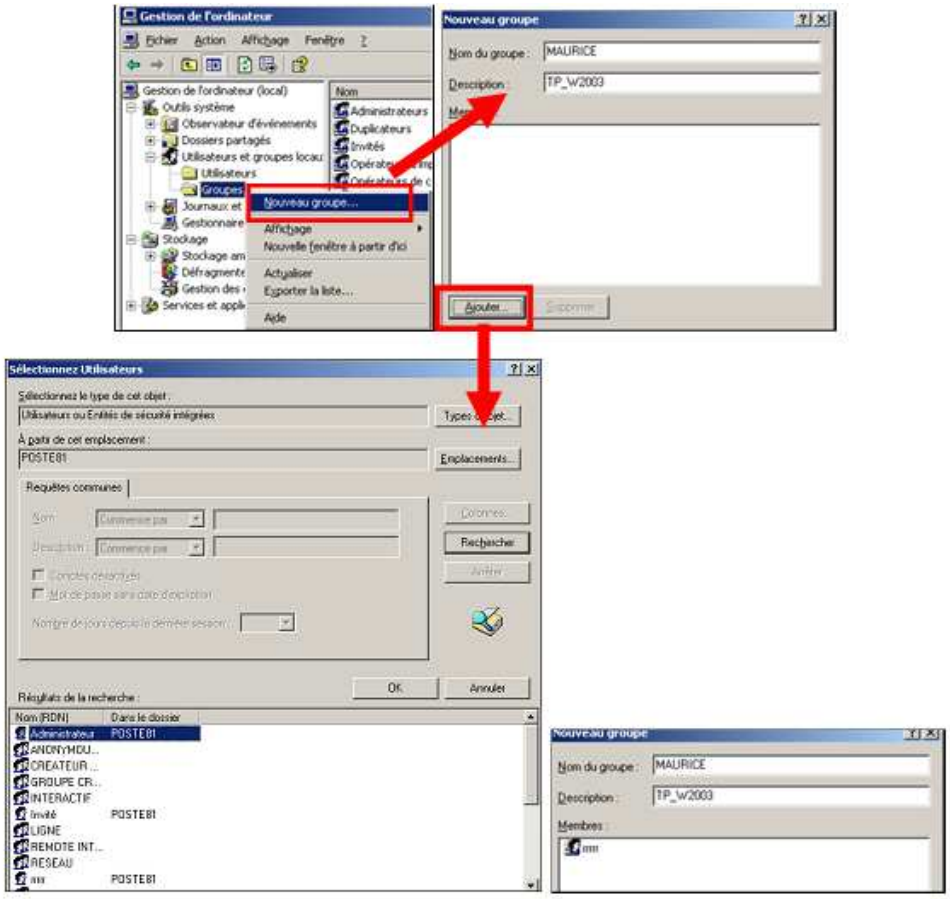
Interactif

- Tous les utilisateurs qui ont ouvert une session localement sont membres de ces groupes.
- Identificateur de sécurité (S-1-5-4).

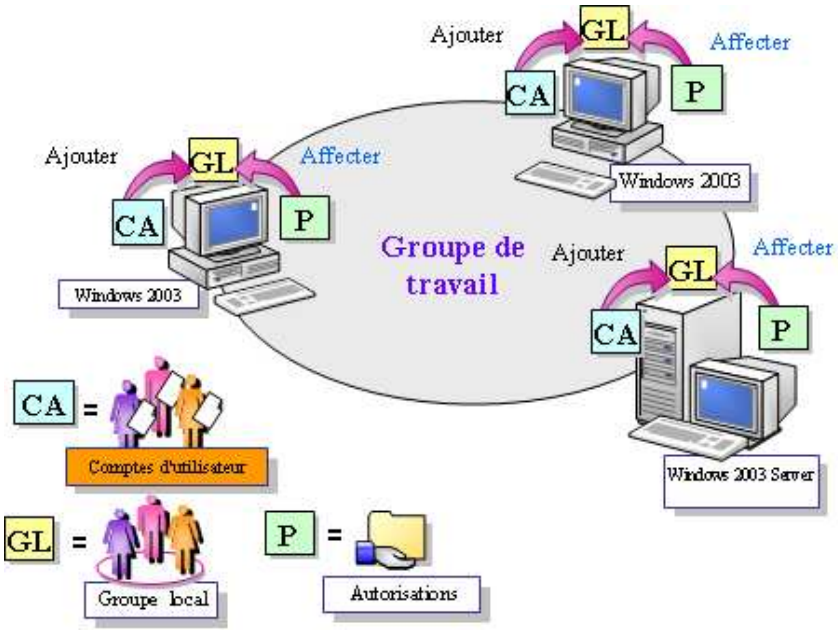
➡ **Création d'un groupe**

Ce sont des groupes locaux car ils sont présents uniquement sur des ordinateurs non membres d'un domaine. Ils permettent le contrôle d'accès aux ressources du micro local. Ils réalisent des tâches système pour l'ordinateur local. Les **groupes locaux** ne peuvent contenir que des comptes d'utilisateur locaux présents sur le micro où les groupes sont créés

Un **Groupe Local** ne peut pas être membre d'un autre groupe.
Créés par les utilisateurs membres des groupes **Administrateurs** et **Opérateurs de compte** de l'ordinateur local.
Un **groupe local** (à ne pas confondre avec le groupe de domaine local) est un groupe créé sur un ordinateur serveur Windows 2003 membre ou autonome. Il permet d'accorder aux membres du groupe des autorisations d'accès aux ressources de l'ordinateur sur lequel le groupe a été créé à l'aide de la console **Gestion de l'ordinateur**.

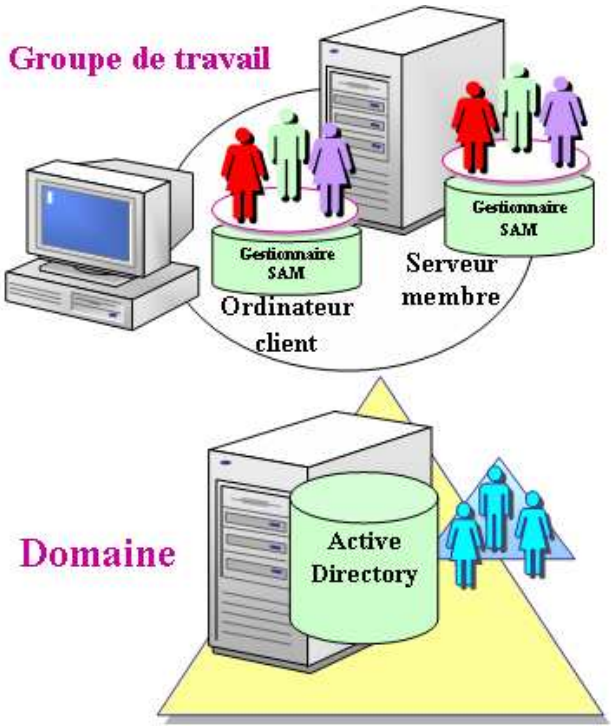


➡ **Stratégie d'utilisation de groupes locaux dans un groupe de travail**



5.3.2- Gestion des Groupes dans un Domaine

- Groupe de travail
  - Créés sur des ordinateurs non contrôleurs de domaine.
  - Résident dans le Gestionnaire de comptes de sécurité (SAM).
  - Permettent de contrôler l'accès aux ressources de l'ordinateur.
- Domaine
  - Créés sur des contrôleurs de domaine.
  - Résident dans Active Directory.
  - Contrôlent les ressources du domaine.



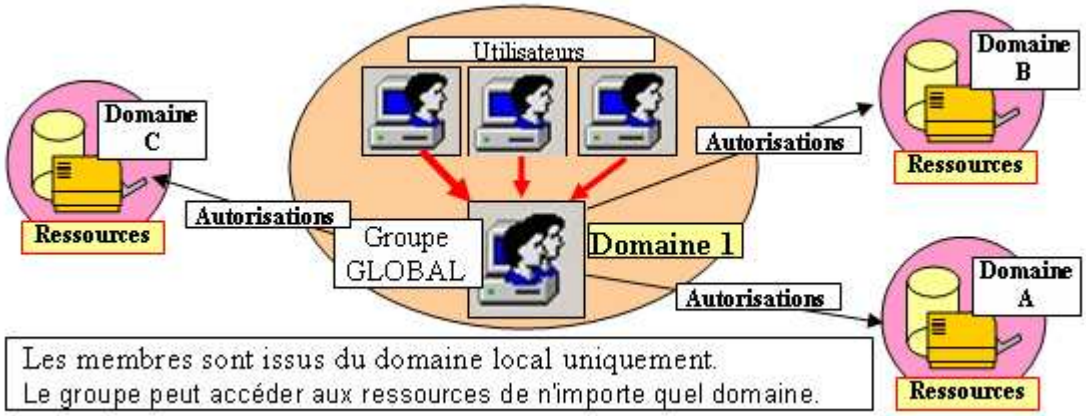
5.3.3- Types de groupes

Il existe deux types de groupes, les **groupes de sécurité**, gérés par Windows 2003, répondant à des objectifs de sécurité et les **groupes de distributions** gérés par certaines applications récentes, par exemple des applications de messagerie qui utilisent de listes de distribution et s'appuient sur Active Directory.

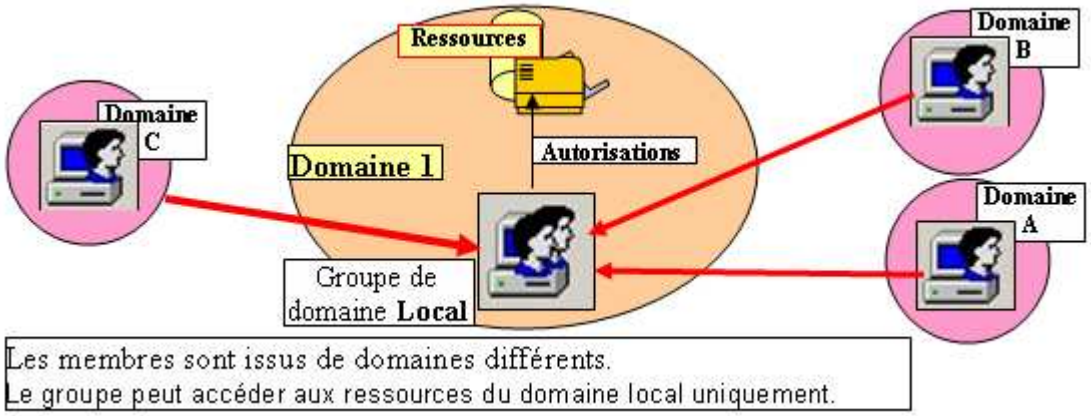
5.3.4- Etendues de groupe

Les **étendues de groupes** permettent d'utiliser les groupes de domaine de manière différente pour attribuer les autorisations. On crée ces groupes avec la console **Utilisateurs et ordinateurs Active Directory** dans **Outils d'administration**.
Sur les **serveurs Windows 2003 contrôleurs de domaine**, il existe 3 types d'étendues :

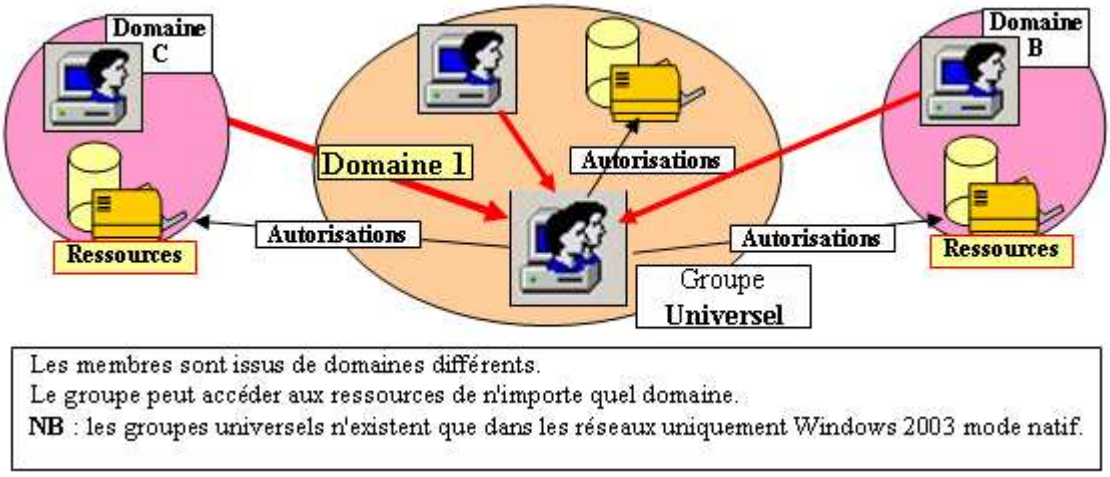
Groupe global



Groupe de domaine local



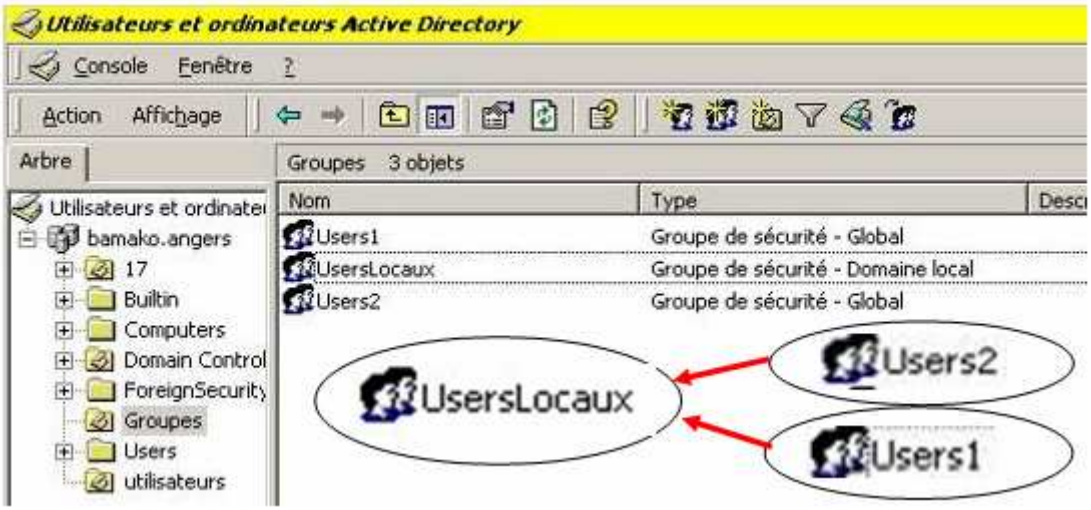
Groupes universels



Imbrication de groupes

Un groupe peut contenir un autre groupe dans la limite des règles ci-dessous. En mode natif (c'est le mode d'un serveur qui ne communique qu'avec d'autres serveurs Windows 2003 : utilisation d'Active Directory seulement, le **mode mixe** suppose qu'il existe encore sur le réseau des serveurs NT 3.51 ou 4 : utilisation de WINS), le nombre de niveaux d'imbrication est théoriquement illimité, mais dans la pratique, il est sage pour des raisons de complexité de gestion de se limiter à un nombre minimum de niveaux.

Etendue de groupe	En **mode natif**, l'étendue peut contenir les éléments suivants	En **mode mixte**, l'étendue peut contenir les éléments suivants
Globale	Comptes utilisateurs Groupes globaux issus du même domaine	Utilisateurs issus du même domaine
De domaine local	Compte utilisateurs Groupes universels Groupes globaux issus de n'importe quel domaine Groupes de domaines locaux issus du même domaine	Comptes utilisateurs Groupes globaux issus de n'importe quel domaine
Universelle	Comptes utilisateurs Autres groupes universels Groupes globaux issus de n'importe quel domaine	Les groupes universels n'existent pas en mode mixte.



Méthodologies d'utilisation des groupes selon Microsoft

A	(Account)	Compte d'utilisateur
L	(Domain Local Group)	Groupe Local
G	(Global group)	Groupe Global
DL	(Domain Local Group)	Groupe Local de domaine
U	(Universal Group)	Groupe Universel
P	(Permissions)	Droits et autorisations

Méthode A, G, L

Méthode où vous devez inclure les comptes utilisateurs dans un groupe global, puis donner les autorisations et privilèges sur ce même groupe global.

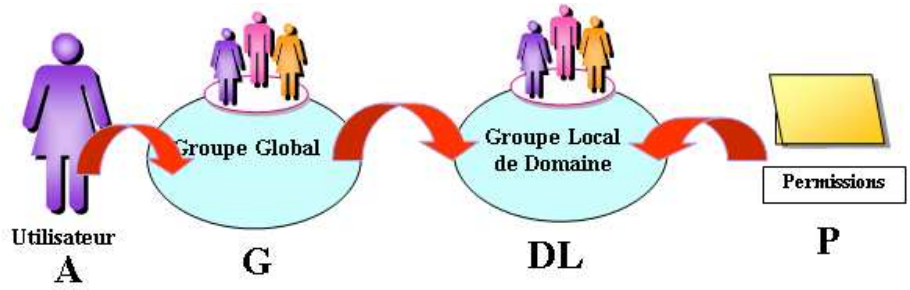
- **Avantages**
  - Simplicité surtout pour l'attribution de droits.
  - Adapté pour un domaine unique.
  - Utilisé avec un faible nombre d'utilisateurs et avec des contraintes d'autorisations faibles.
- **Inconvénients**
  - Gestion difficile en cas de domaines multiples.
  - Ralentissement des performances car le serveur doit vérifier les appartenances de groupe global à chaque connexion d'un utilisateur.

Méthode A, DL, P

Méthode où vous devez inclure les comptes utilisateurs dans un groupe local de domaine, puis donner les autorisations et privilèges sur ce même groupe local de domaine.

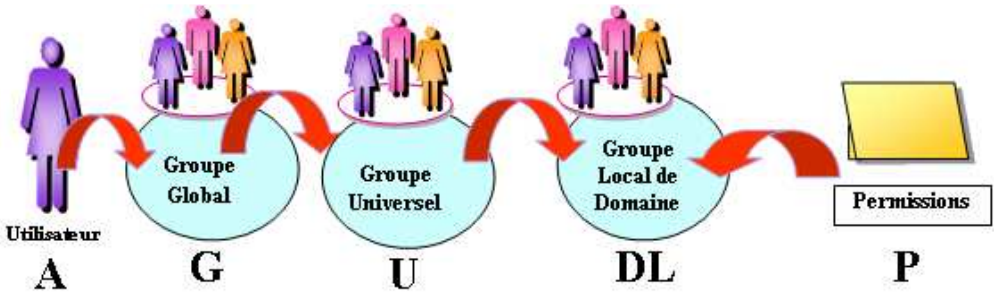
- **Avantages**
  - Méthode peu recommandée, mais adaptée pour un domaine unique et qui n'évoluera pas vers une forêt multi domaine.
  - Utilisé avec un faible nombre d'utilisateurs d'où sa simplicité à gérer un seul type de groupe facilitant les diagnostics et la détermination des droits effectifs.
- **Inconvénients**
  - Manque de flexibilité et d'évolution de la structure.
  - Pas de possibilité d'affecter des autorisations sur le groupe en dehors du domaine.
  - Pas possible d'utiliser ces groupes pour gérer les ressources partagées par des serveurs membres sous NT4.

Méthode A, G, DL, P
Méthode où vous devez inclure les comptes utilisateurs dans un groupe Global, puis les groupes globaux dans un groupe local, puis donner les autorisations et privilèges sur ce même groupe local de domaine.



- **Avantages**
  - Méthode s'adapte à toutes les structures de domaine (mono ou multi domaines).
  - Permet la réduction des temps d'administration car les autorisations sont exclusivement gérées par les groupes locaux de domaines tandis que les utilisateurs appartiennent aux groupes globaux.
  - Méthode applicable quel que soit le mode fonctionnel du domaine.
- **Inconvénients**
  - Sa complexité de mise en œuvre pour les administrateurs.

Méthode A, G, U, DL, P
Méthode où vous devez inclure les comptes utilisateurs dans un groupe Global, puis les groupes globaux dans un groupe universel, ce groupe universel dans un groupe local de domaine, puis donner les autorisations et privilèges sur ce même groupe local de domaine.



- **Avantages**
  - Méthode s'adapte à toutes les structures de domaine (mono ou multi domaines).
  - Permet la réduction des temps d'administration (comme précédemment).
  - Permet de mutualiser des besoins déjà définis dans un groupe global, par l'imbrication de celui-ci dans un autre groupe global ou universel fédérateur.
  - Méthode applicable quel que soit le mode fonctionnel du domaine.
- **Inconvénients**
  - Sa complexité de mise en œuvre pour les administrateurs.

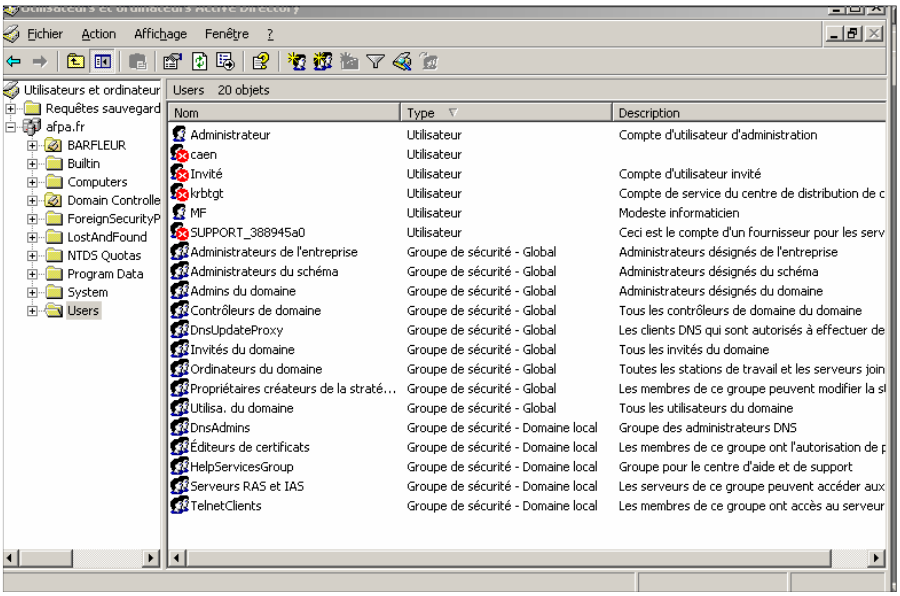
5.3.5- Les groupes par défaut

Windows 2003 comporte un certain nombre de groupes par défaut. Ils disposent d'appartenances à d'autres groupes et de droits d'utilisateurs prédéfinis. Ces droits définissent des tâches administratives que les membres de ces groupes peuvent accomplir.

➡ **Sur les serveurs Contrôleurs de Domaine**

Groupes prédéfinis

Lors de la création du premier serveur Active Directory, Windows 2003 crée dans le dossier User de la console **Utilisateurs et ordinateurs Active Directory,** un certain nombre de groupes globaux.

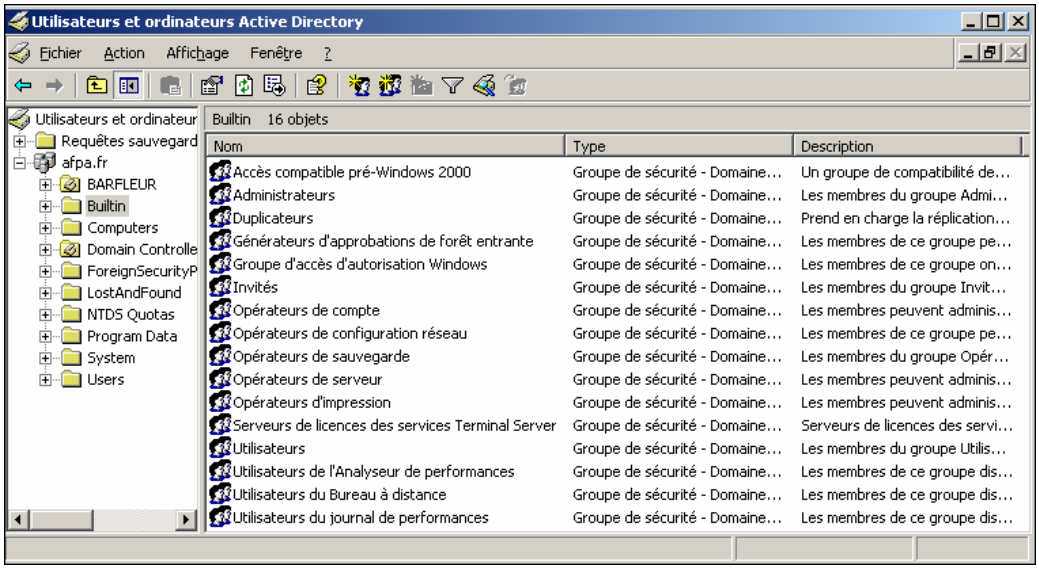


Groupe global prédéfini	Description
Admins du domaine	Ce groupe global est imbriqué automatiquement au groupe de domaine local intégré **Administrateurs,** afin que ses membres puissent effectuer des tâches administratives sur n'importe quel ordinateur du domaine. Par défaut le compte utilisateur **Administrateur** est membre du groupe **Admins du domaine**
Invités du domaine	Ce groupe est imbriqué dans le groupe de domaine local intégré **Invités**. Par défaut le compte utilisateur **Invité** est membre du groupe **Invités du Domaine**.
Utilisa. du domaine	Tous les comptes d'utilisateurs que vous créez font partie par défaut de ce groupe. Ce groupe est imbriqué dans le groupe local intégré **Utilisateurs**. Les membres de ce groupe réalisent les tâches spécifiées et ils n'ont accès qu'aux ressources affectées au niveau du groupe local de domaine **utilisateurs**. Par défaut les comptes utilisateurs suivants sont membres du groupe **Utilisateurs du domaine** : • Administrateur. • Invité. • IUSR_nom_ordinateur. • IWAM_nom_ordinateur. • Krbtgt. • TsInternetUser. • Tout nouvel utilisateur.
Administrateurs de l'entreprise	Les utilisateurs faisant partie de ce groupe possèdent des droits d'administrateur sur toute la forêt (et non plus uniquement sur le domaine). Ils peuvent aussi modifier le schéma et la topologie des sites Active Directory. Par défaut le compte administrateur du premier contrôleur de domaine de la forêt fait partie de ce groupe. Ce groupe global est modifié en groupe universel lorsque le domaine est en mode natif Windows 2000 ou 2003.

Administrateurs du schéma	Les utilisateurs faisant partie de ce groupe possèdent des droits pour modifier le schéma Active Directory. Ils peuvent ajouter ou supprimer toute classe ou attribut d'objet. Ce groupe global est modifié en groupe universel lorsque le domaine est en mode natif W2000 ou W2003.
Contrôleurs de domaine	Il contient tous les comptes d'ordinateurs des contrôleurs du domaine. Il permet la gestion des besoins spécifiques aux contrôleurs du domaine car en général ils sont différents des besoins des autres ordinateurs membres.
Propriétaires créateurs de la stratégie de groupe	Le compte Administrateur fait automatiquement partie de ce groupe. Tous les membres de ce groupe sont le regroupement des créateurs/propriétaires des stratégies de groupe permettant la modification de celles-ci.
DnsUpdateProxy	Les membres de ce groupe peuvent inscrire ou modifier un enregistrement dans les zones DNS intégrée Active Directory.

Groupes intégrés à étendue de domaine locale

Des groupes intégrés dotés d'une étendue de domaine locale sont créés par Windows 2003 dans le dossier **Builtin** de la console **Utilisateurs et ordinateurs Active Directory**. Les utilisateurs membres de ces groupes se voient autoriser à assurer des tâches administratives sur les contrôleurs de domaine et sur Active Directory.



Groupe de domaine local intégré	Description
Opérateurs de compte	Les membres de ce groupe peuvent créer, supprimer et modifier les comptes d'utilisateurs et de groupes. Ils ne peuvent agir sur les groupes Administrateurs et les groupes d'opérateurs (Opérateurs de sauvegarde ou d'impression)
Administrateurs	Les membres de ce groupe peuvent effectuer l'ensemble des tâches administratives sur les contrôleurs de domaine et sur le domaine. Par défaut sont membres de ce groupe : ➢ Le compte utilisateur Administrateur. ➢ Groupe global prédéfini Admins du domaine. ➢ Groupe global prédéfini Administrateurs de l'entreprise.
Opérateurs de sauvegarde	Les membres de ce groupe peuvent sauvegarder et restaurer tous les contrôleurs de domaine à l'aide de l'utilitaire **Gestion de sauvegarde** de Windows 2003.

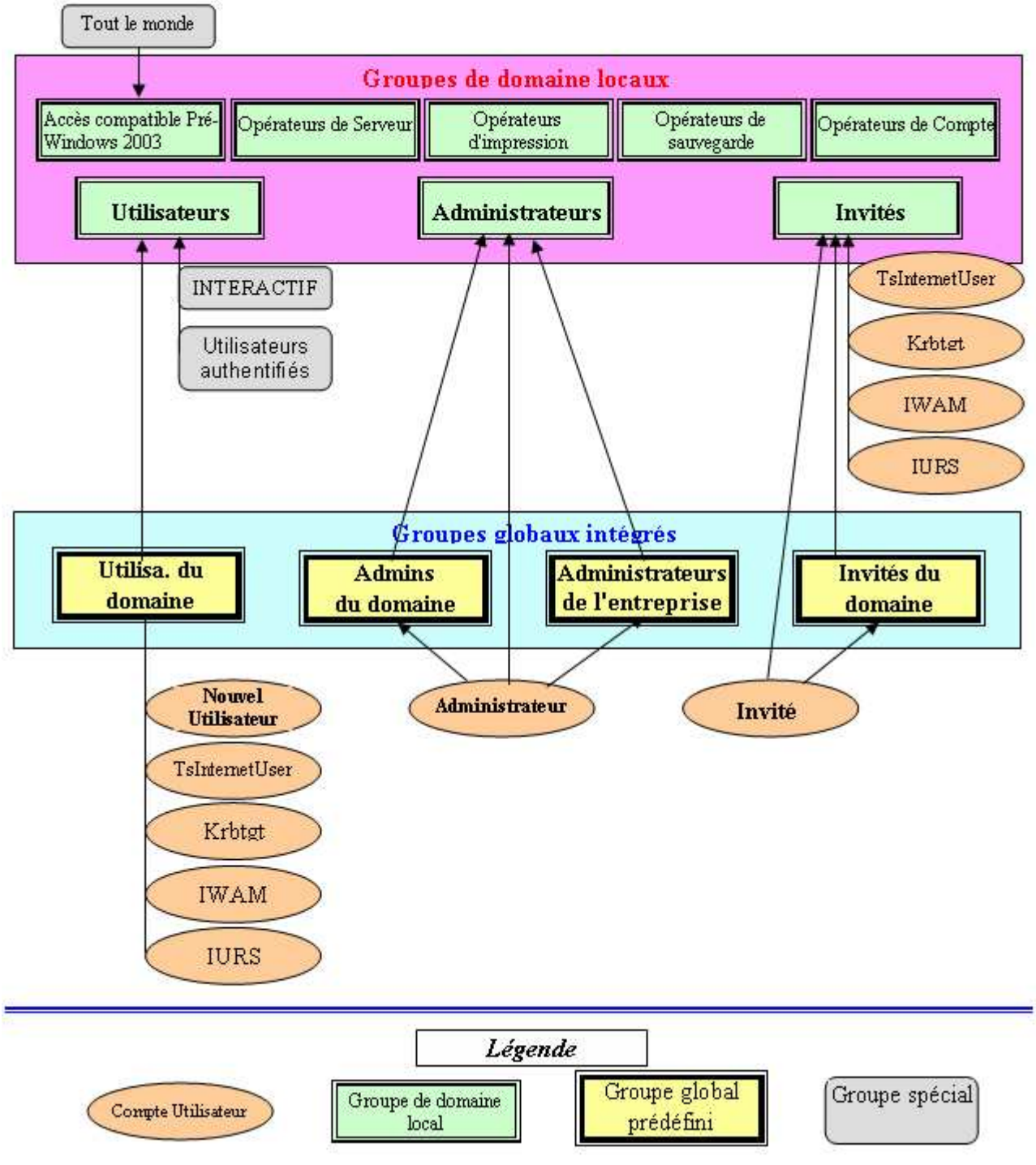
Invités	Les membres de ce groupe ont des droits restreints qui leur ont été accordés par les Administrateurs. Ce groupe contient par défaut les membres suivants : ➢ Comptes Utilisateurs Invités. ➢ IUSR_nom_d'ordinateur. ➢ IWAM_nom d'ordinateur. ➢ TsInternetUser. ➢ Groupe global prédéfini Invités du domaine.
Accès compatible Pré-Windows 2000	Les membres de ce groupe se voient accorder les autorisations de lecture. Le groupe pré Windows 2003 **Tout le monde** fait partie par défaut de ce groupe.
Opérateurs d'impression	Les membres de ce groupe peuvent configurer et gérer les imprimantes du réseau sur les contrôleurs de domaine.
Duplicateurs	Les membres de ce groupe assurent la réplication d'annuaire. Le seul membre de ce groupe est un compte utilisateur système. Il ne faut pas ajouter d'autres utilisateurs à ce groupe.
Opérateurs de serveur	Les membres de ce groupe peuvent partager les ressources disques et assurer les sauvegardes et restauration sur un contrôleur de domaine.
Utilisateurs	Les membres de ce groupe ne peuvent effectuer que les tâches qui leur sont assignées et ne possèdent que les autorisations qui leur ont été attribuées. Par défaut, les groupes suivant font partie de ce groupe : ➢ Groupe Pré-Windows 2003 **INTERACTIF.** ➢ Groupe Pré-Windows 2003 **Utilisateurs authentifiés.** ➢ Utilisateurs du domaine.
Générateurs d'accès d'autorisation Windows	Les membres de ce groupe ont accès à l'attribut **tokenGroupsGlobalAndUniversal** sur les objets utilisateur. Ils ont aussi la possibilité de consulter les appartenances de groupes pour les comptes d'utilisateurs. Par défaut l'entité spéciale **Enterprise Domain Controlers** est membre de ce groupe.
Serveurs de licences des services Terminal Server	Les membres de ce groupe peuvent gérer les attributions de licences Terminal Server.
Utilisateurs des journaux de performances	Les membres de ce groupe peuvent définir ou modifier les compteurs, alertes et journaux de performances pour diagnostiquer un dysfonctionnement de votre micro local ou distant. Ils peuvent utiliser le moniteur système. Le groupe système **Service Réseau** est membre par défaut.
Utilisateurs du moniteur de performances	Les membres de ce groupe peuvent utiliser le moniteur système de l'analyseur de performances localement ou à distance. Il ne possède aucun membre.
Utilisateurs du bureau à distance	Les membres de ce groupe peuvent ouvrir une session de type **Terminal Server** sur le micro à condition que la fonctionnalité du **Bureau à distance** soit activée. Aucun membre par défaut.

Vous avez aussi des groupes locaux de domaine dans le conteneur Users. Ces groupes proviennent de la migration de la base locale d'origine et/ou sont ajoutés en fonction de l'installation de certains services ou applications.

Groupe de domaine local dans le conteneur Users	Description
Cert Publishers	Les membres de ce groupe peuvent publier des certificats dans Active Directory.

DnsAdmins	Les membres de ce groupe peuvent administrer les services DNS de l'ordinateur.
Administrateurs DHCP	Les membres de ce groupe peuvent administrer les services DHCP de l'ordinateur.
Serveurs RAS et IAS	Les membres de ce groupe peuvent accéder aux propriétés d'accès distant des utilisateurs.
Utilisateurs DHCP	Les membres de ce groupe peuvent accéder uniquement en consultation aux services DHCP du micro.
Utilisateurs WINS	Les membres de ce groupe peuvent accéder uniquement en consultation aux services WINS du micro.

Schéma d'imbrication des groupes et comptes utilisateurs dans un domaine.



➡ **Sur tous les ordinateurs**

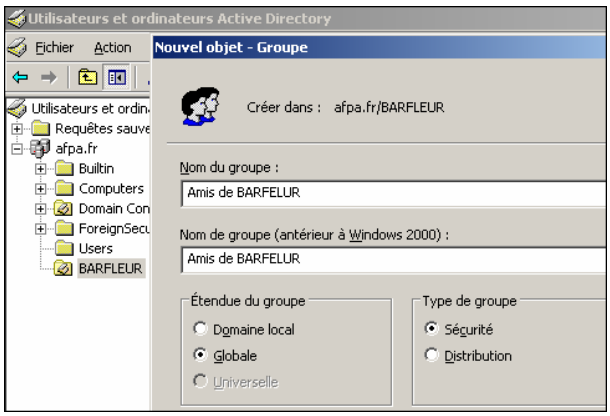
Groupes spéciaux
Les groupes spéciaux existent sur tous les ordinateurs sous Windows 2003. Ces groupes ne sont pas administrables et sont gérés par le système d'exploitation. Ils représentent les utilisateurs dans des circonstances particulières lorsqu'ils accèdent à certains ordinateurs ou certaines ressources.

Groupe spécial	Description
ANONYMOUS LOGON *(Ouverture de session anonyme)*	Inclut les comptes d'utilisateurs que Windows 2003 n'a pu identifier. Avec W2003 ce groupe n'est plus intégré par défaut au groupe **Tout le Monde.** Identificateur de sécurité (S-1-5-7).
Utilisateurs authentifiés *(Authenticated Users)*	Remplace le groupe Tout le monde qui existait dans les versions pré-Windows (donnez donc des permissions à ce groupe plutôt qu'au groupe Tout le Monde). Contient tout utilisateur possédant un compte d'utilisateur et un mot de passe pour la machine locale ou Active Directory. Le compte Invité est intégré si un mot de passe lui est associé. Identificateur de sécurité (S-1-5-11).
CREATEUR PROPRIETAIRE *(creator owner)*	Inclut le compte de l'utilisateur auquel appartient une ressource. Cela peut être le créateur comme celui qui a pris possession de cette ressource. Identificateur de sécurité (S-1-3-0).
LIGNE ou APPEL ENTRANT *(Dialup)*	Inclut tout utilisateur qui accède par une connexion distante. Permet de contrôler l'accès des utilisateurs sur vos connexions entrantes. Identificateur de sécurité (S-1-5-1).
Tout le monde *(Everyone)*	Inclut tout utilisateur qui accède à un ordinateur y compris le compte Invité et tous les utilisateurs des autres domaines. Attention lorsque vous partagez une ressource ce groupe dispose par défaut de la permission contrôle total. Avec W2003 Server la sécurité a été renforcée car le groupe Ouverture de session anonyme n'est plus intégré par défaut au groupe **Tout le monde.** Identificateur de sécurité (S-1-1-0).
INTERACTIF *(Interactive)*	Inclut le compte de l'utilisateur qui a ouvert une session localement sur l'ordinateur. Les membres du groupe INTERACTIF sont les utilisateurs qui accèdent à une ressource locale. Identificateur de sécurité (S-1-5-4).
SERVICE RESEAU (*Network Service)*	Inclut tout une utilisateur qui accède à un partage à partir d'un autre ordinateur (via le réseau). Le groupe Interactif ne fait pas partie de ce groupe car il identifie un accès réseau sur une ressource et non sur une ouverture de session. Identificateur de sécurité (S-1-5-2).
Batch *(Batch)*	Contient tout utilisateur sollicitant la file d'attente des tâches planifiées. Identificateur de sécurité (S-1-5-3)
Contrôleurs de domaine d'Entreprise *(Enterprise Domain Controlers)*	Contient tous les contrôleurs de domaine de la forêt utilisant Active Directory. Identificateur de sécurité (S-1-5-9).
Autre organisation *(Other Organisation)*	Permet de contrôler les accès des utilisateurs provenant de domaines ou forêt externes lorsqu'ils sollicitent un service du système. Identificateur de sécurité (S-1-5-1000).
Soi-même *(Self ou Principal Self)*	Si ce groupe est ajouté dans la liste de contrôle d'accès d'une ressource, les autorisations qui lui sont données sont transportées vers l'identifiant associé à l'objet utilisateur, groupe ou ordinateur accédant à la ressource. Identificateur de sécurité (S-1-5-10).

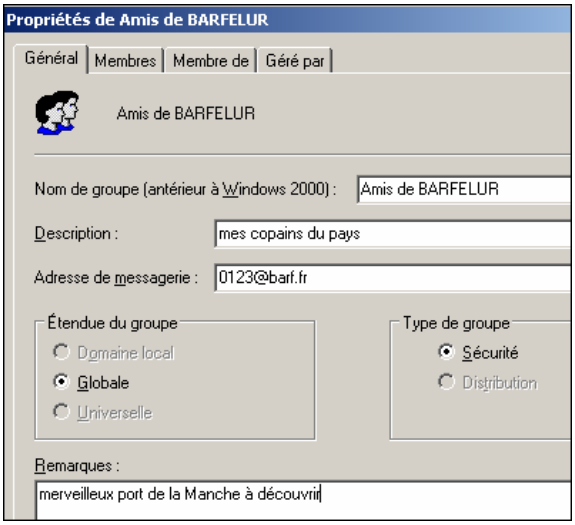
Service *(Service ou local service)*	Contient tous les identifiants principaux de sécurité sollicitant ou exécutant un processus du système en tant que service Identificateur de sécurité (S-1-5-6).
Système *(System ou Local system)*	Ce n'est pas un groupe mais le compte system local. Plusieurs ressources ou fonctionnalité du micro ne pourront être accessibles que via ce compte (clé du registre, dossiers spéciaux …). Identificateur de sécurité (S-1-5-18).
Utilisateurs de Terminal Server **(***Terminal servers Users)*	Contient tous les utilisateurs connectés aux services Terminal Server et Bureau à distance. Il est inclus dans le groupe Interactif. Identificateur de sécurité (S-1-5-13).

➡ Création de groupes

Console **Utilisateurs et ordinateurs Active Directory**. Sélectionnez l'**OU** cible ➔ **Action** ➔ **Nouveau** ➔ **Groupe** ➔ **Type de Groupe** (Sécurité ou Distribution) et l'étendue (Domaine Local, Globale ou Universelle). Entrez un **nom** pour le groupe. Validez par **OK.**



Si le domaine est en mode natif, vous pouvez à tout instant **modifier** le type de groupe et son étendue (sous certaines conditions d'appartenances à d'autres types de groupes incompatibles). La fenêtre **Propriétés** vous permet de gérer, paramétrer ou modifier la sécurité du groupe



VI- ENVIRONNEMENT RESEAU ET ACTIVE DIRECTORY

6.1- Modèles

Sous Windows 2003, on distingue deux modèles d'environnement réseau :

- Groupe de Travail.
- Domaine Windows 2003.

6.1.1- Modèle de Groupe de Travail Windows 2003

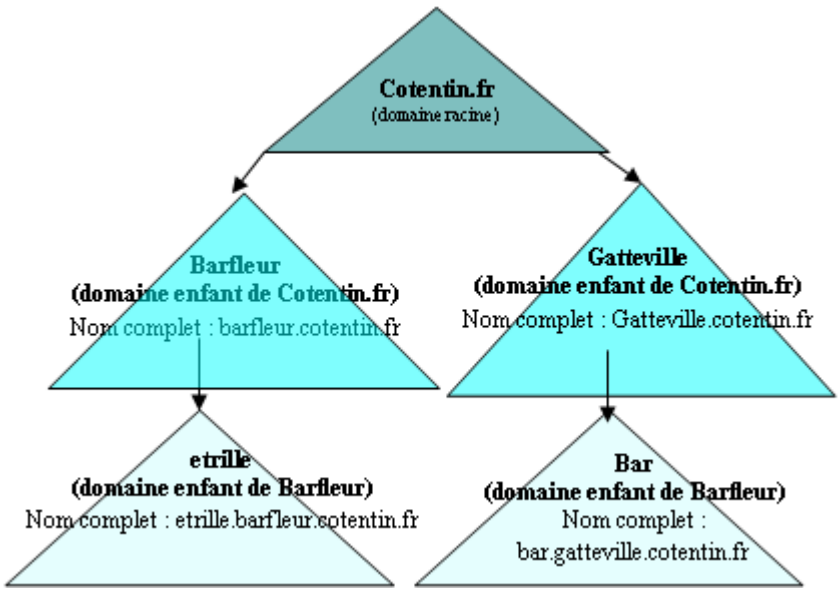
Un **groupe de travail** est un ensemble d'ordinateurs en réseau qui partagent leurs ressources. Chaque ordinateur possède sa propre base de données concernant les noms des utilisateurs, leur mot de passe et leur profil. On y trouve aussi bien des ordinateurs avec Windows 2000 Pro ou Windows 2000/2003 Server. Il n'y a pas d'administration centralisée, aussi chaque utilisateur qui veut utiliser un autre ordinateur que le sien doit être autorisé sur cet autre ordinateur. Ce qui veut dire par exemple, qu'un utilisateur qui veut modifier son mot de passe doit le faire sur son ordinateur, mais aussi sur tous les ordinateurs auxquels il a accès. Le partage des périphériques se fait à partir de chaque ordinateur par son administrateur. Un **serveur Windows 2003** qui ne fait pas partie d'un domaine, est un **serveur autonome**.

6.1.2- Modèle de Domaine Windows 2003

Un **domaine** Windows 2003 est un groupe d'ordinateurs qui utilisent la même base de données d'annuaire centrale.
Un domaine est constitué de :

- Une **unité de réplication** et tous les contrôleurs de domaines sont membres actifs de la réplication en recevant toutes les 5 mm les modifications de l'annuaire d'Active Directory. Le domaine régule le trafic de réplication réseau.
- Une **limité de sécurité** car chaque domaine dispose de paramètres de sécurité (tels des stratégies de compte : mot de passe, verrouillage de comptes...) qui le caractérise.
- Une **unité d'administration** avec pour chaque domaine un administrateur disposant des droits et autorisations obligatoires pour gérer, administrer et contrôler tous les objets du domaine concerné.

Un administrateur à la possibilité de déléguer des tâches administratives aux utilisateurs du domaine qu'il choisit.

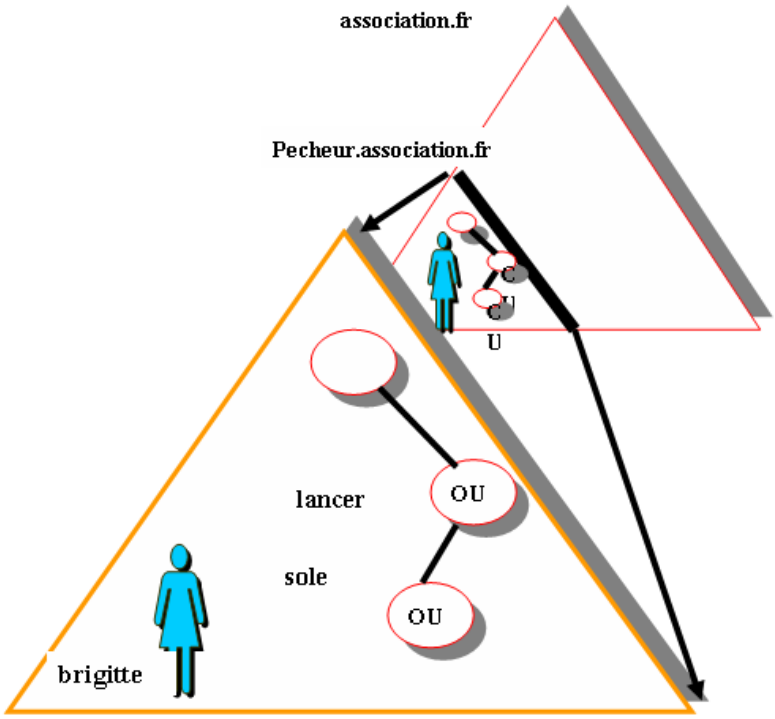


Le contrôleur de domaine est un ordinateur qui contient un exemplaire de la base de données (annuaire). Seuls les ordinateurs exécutant Windows 2003 Server (ou supérieure) peuvent être contrôleur de domaine.
Ceci autorise une gestion centralisée des utilisateurs, le partage des fichiers et des périphériques raccordés au serveur. Chaque contrôleur de domaine stocke un exemplaire de l'annuaire.
Un **serveur membre** est un serveur qui fait partie du domaine, mais qui n'est pas contrôleur de domaine.
Dans Windows NT4, il existe des contrôleurs de domaines principaux et des contrôleurs de domaines secondaires. Dans Windows 2003, tous les contrôleurs de domaine sont au même niveau.
Les ordinateurs qui exécutent Windows 2000 Pro ou XP sont les stations de ce domaine.

6.2- Services d'annuaire

Un **annuaire** est une base de données qui contient des informations sur les différents objets et liens gérés au niveau du domaine.
Le **service d'annuaire** est un service du réseau qui permet d'utiliser l'**annuaire** : **Active Directory** est le service d'annuaire utilisé sur Windows 2003.
Active Directory utilise le système de noms de domaine **DNS**. Par conséquent, il doit exister un service DNS sur un des serveurs Windows 2003 Server du réseau.
Active Directory utilise le protocole normalisé **LDAP** (Lightweight Directory Access Protocol), ce qui permet d'accéder à d'autres services annuaires comme celui de Novell.
Active Directory comprend l'**annuaire** qui stocke les informations relatives aux ressources réseau comme les données utilisateurs, les imprimantes, les serveurs, les bases de données, les groupes, les ordinateurs et les stratégies de sécurité. Toutes ces entités sont désignées sous le nom d'**objets**.
Active Directory permet :

- Une **administration simplifiée**. Active Directory permet une administration à partir de n'importe quel point du réseau avec un outil unique. Tous les contrôleurs de domaine sont placés sur le même pied d'égalité. Toute modification apportée sur un contrôleur de domaine est répercutée sur les autres contrôleurs de domaine.
- Une **évolutivité**. L'annuaire est organisé en sections capables de stocker un grand nombre d'objets de l'entreprise. Si l'entreprise se développe, l'annuaire peut évoluer en même temps.
- Une **prise en charge des normes ouvertes**. Active Directory utilise le nommage de noms type **DNS**. Ceci permet d'échanger des informations avec n'importe quelle application utilisant ce système de nommage. Les noms de domaine Windows 2003 sont des noms de type DNS. Windows 2003 utilise un DNS dynamique (**DDNS**) qui permet la mise à jour des tables DNS de façon automatique. Active Directory prend en charge les protocoles LDAP et HTML. Ceci veut dire que les propriétés des objets peuvent être affichées dans une page HTML.
- Une **prise en charge des noms standards**. Les services d'annuaire Active Directory utilisent les formats de noms les plus répandus comme :
  - Les noms de courrier (RFC 822) du type nom@ domaine.
  - Les noms URL http http://domaine.nomdepage.
  - Les noms UNC \\domaine\partage.
  - Les noms URL LDAP de type //domaine/CN=PrénomNom.OU=org.OU=prod…

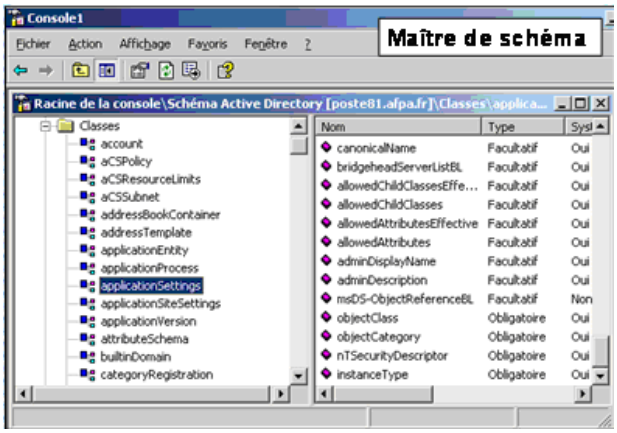


6.2.1- Structure d'Active Directory

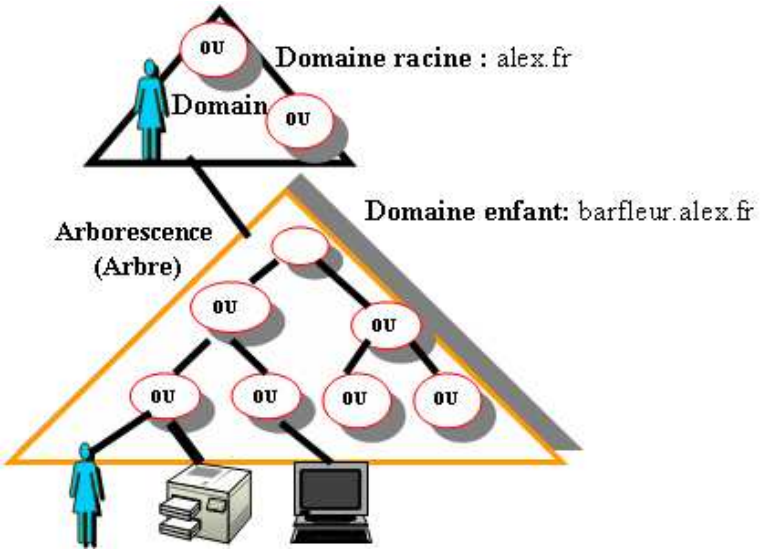
➡ **Structure Logique**

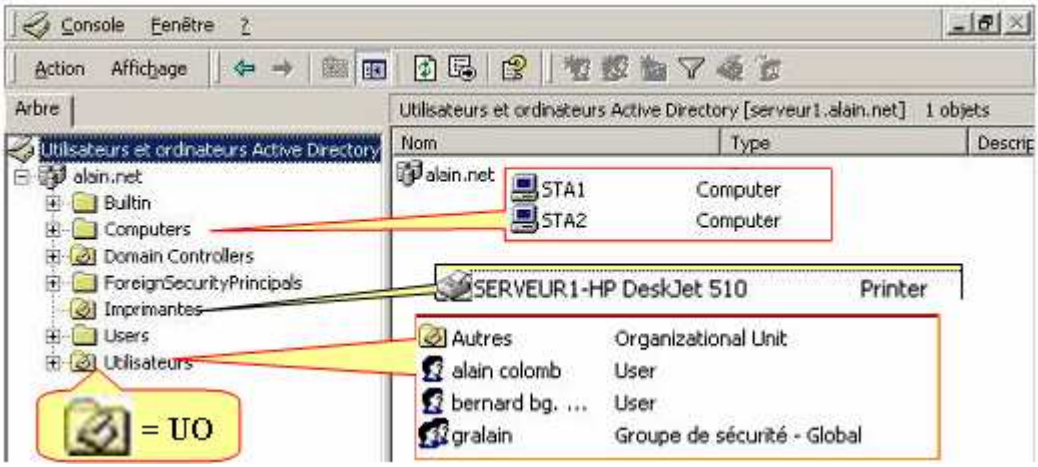
Objet

Un **objet** représente une entité gérée par Active Directory (ordinateur, groupe d'utilisateurs, utilisateur...). La structure logique de la base d'annuaire est constituée de forêt, d'arbres, de domaines et d'OU permettant de stocker des objets. La règle régissant la création des objets sont contenues dans le schéma qui est stocké dans la base de données Active Directory. L'objet Active Directory étant une instance d'une classe. Une classe est définie dans le Schéma Active Directory avec un ensemble d'attributs représentatifs de l'objet. Tous ces attributs sont définis dans le schéma et il y a qu'un seul schéma, ce qui implique une seule règle pour tous les objets de la forêt.

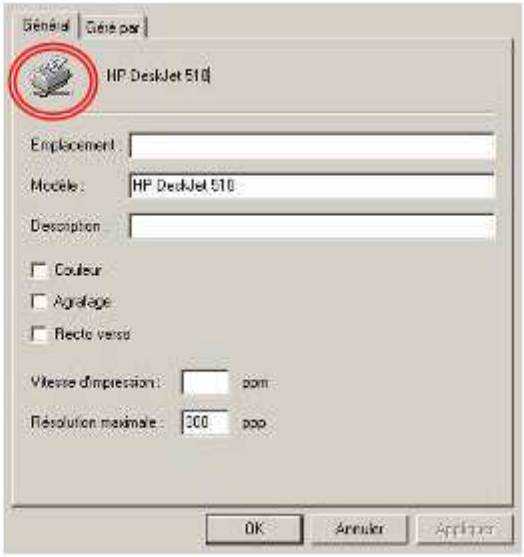


Le **schéma** définit les classes d'objets (différents types d'objets Active Directory), la liste des **attributs** disponibles dans l'annuaire, les contraintes et restrictions qui s'appliquent aux objets et au format de leur nom. Certains de ces attributs devront **obligatoirement** être saisis lors de leur création (par exemple un nom d'utilisateur) tandis que d'autres seront **facultatifs** (n° téléphone).





Chaque objet possède des propriétés appelées **attributs**. Par exemple, les attributs d'un utilisateur sont : son nom, son prénom, son adresse, son email...



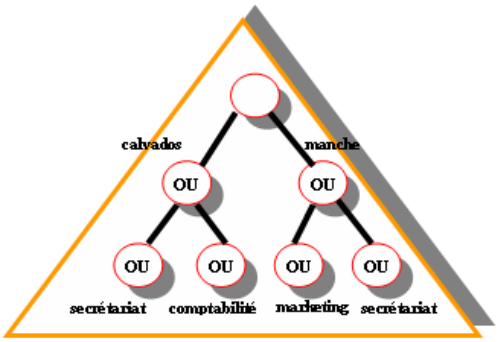
La liste des attributs est différente pour chaque type (**classe**) d'objet. La liste des attributs de la **classe utilisateur** comporte nom, mot de passe, membre d'un groupe..., alors que la liste des attributs pour la **classe imprimante** contient modèle, couleur, résolution maximale...

Les conteneurs

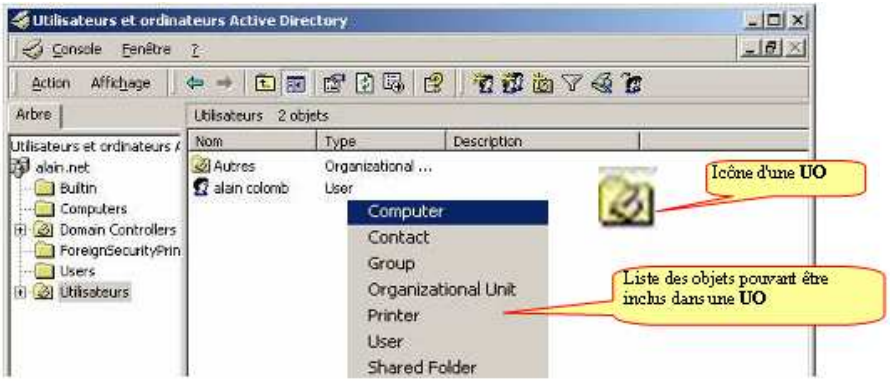
Les **conteneurs** sont des objets qui peuvent contenir d'autres objets (objets **Feuilles**). Les **domaines** et les **unités d'organisation** (**UO ou OU**) sont des conteneurs. Une **OU** est une organisation logique qui représente le plus souvent une structure géographique, ou alors une structure par services regroupant les objets d'un domaine. Une **OU** regroupe des comptes utilisateurs, des ordinateurs, des groupes, des ressources partagées. Leur rôle étant de :

- Permettre la **délégation** de pouvoirs à certains utilisateurs afin de leur donner certaines responsabilités administratives sur les objets de l'OU
- **Simplifier la sécurité** en autorisant par exemple l'affichage des objets auxquels ils ont droit dans Active Directory.
- **Définir une Stratégie** appliquée aux comptes utilisateurs ou aux ordinateurs faisant partie de l'OU concernée.

✋ Dans le cas où vous ne créez pas d'OU tous les utilisateurs se trouveront dans le conteneur Users, et les stratégies de sécurité ne s'appliqueront qu'au niveau du site ou bien de l'ensemble du domaine.



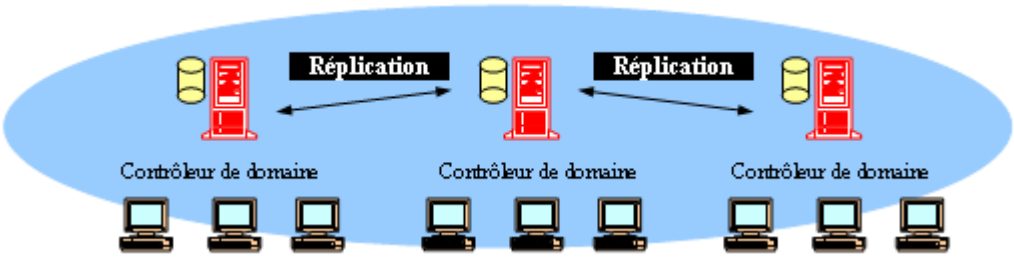
Un **domaine** est un objet d'Active Directory qui contient des objets inscrits dans la même **ACL** (Access Control List). Au niveau d'Active Directory, un domaine correspond à une **partition**. S'il y a plusieurs domaines sur le réseau géré par les services d'annuaire, il y a plusieurs partitions dans Active Directory. Une **forêt** correspond à **l'annuaire entier** et **chaque domaine** a une **partition**. Le conteneur **unité d'organisation** (**UO**) est un sous-ensemble du domaine qui permet de ranger des objets de même nature ou ayant des rapports entre eux. Une unité d'organisation peut en contenir d'autres.



➡ Structure physique

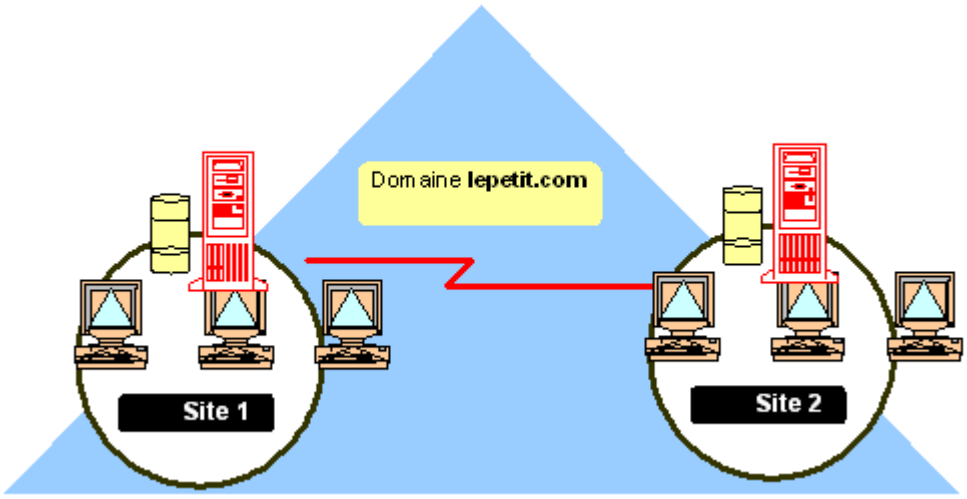
La structure **physique** d'Active Directory permet de représenter l'aspect physique du réseau.
Son rôle essentiel étant de **configurer** et **gérer** le trafic réseau. Les sites et les contrôleurs de domaines constituent les composants physiques de Active Directory et ils ont pour rôle d'optimiser la réplication et les ouvertures de session, et de pouvoir retrouver facilement les objets Active Directory.

Contrôleurs de domaine
Chaque contrôleur de domaine stocke une copie complète de toutes les informations Active Directory relatives au domaine. Une **réplication** (copie) de tous les objets d'un domaine se fait automatiquement sur les autres contrôleurs du domaine. Le **contrôleur de domaine** (micro tournant sous W2003 Server) appelé aussi serveur **LDAP** (qui est le protocole standard de recherche Active Directory) stocke la base d'annuaire W2003, et surtout possède le service **KDC** (Key Distribution Center) qui distribue les tickets d'accès aux services réseau via **l'authentification Kerberos V5**. C'est lui aussi qui gère les modifications d'annuaire et les duplique vers les autres contrôleurs du même domaine. Dans le cas de grosses organisations ou pour un aspect sécuritaire, il est recommandé de mettre en service plusieurs contrôleurs de domaines. Cela permet en plus une meilleure répartition de charge (pour l'ouverture de session).

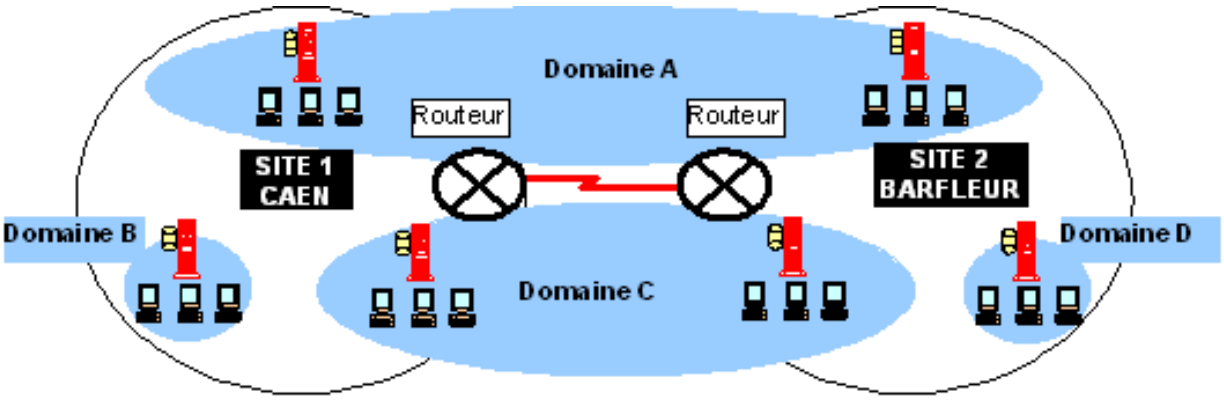


➡ **Les sites**

Un **site** est un ensemble de **sous réseaux IP** reliés entre eux par des connexions fiables et rapides. La structure de site est indépendante du domaine, car un domaine peut contenir un ou plusieurs sites et inversement un seul site peut contenir plusieurs domaines ou plusieurs parties du domaine. En général, un **site correspond à un réseau local**. Si deux réseaux locaux sont reliés par une liaison **WAN**, on crée deux sites qui peuvent ou non faire partie du même domaine.
Le **rôle** d'un site est **l'optimisation du trafic de réplication** (qui est entièrement paramétrable) en permettant aux utilisateurs de se connecter à un contrôleur de domaine par l'utilisation d'une connexion rapide et fiable afin d'optimiser les ouvertures de session.

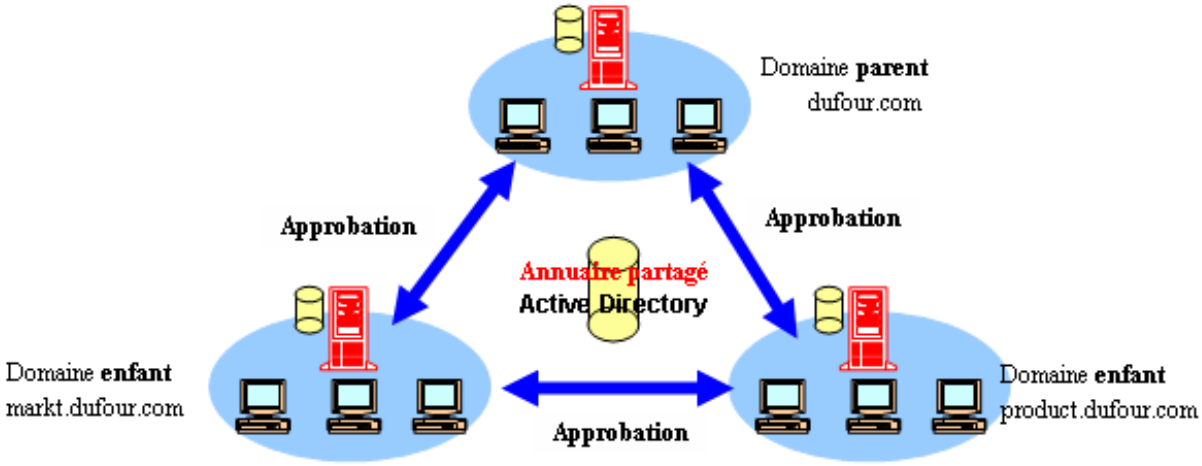


Il peut exister une totale **indépendance** entre la **structure logique** et la **structure physique**. Cela implique qu'il n'y a aucune corrélation entre la structure physique du réseau et la structure des domaines. En conséquence **Active Directory** peut autoriser **plusieurs domaines** dans un **même site**, ainsi que **plusieurs sites** dans un **même domaine**. De même aucune corrélation n'est nécessaire entre les espaces de noms de sites et des domaines.



6.2.2- Arborescences et forêts

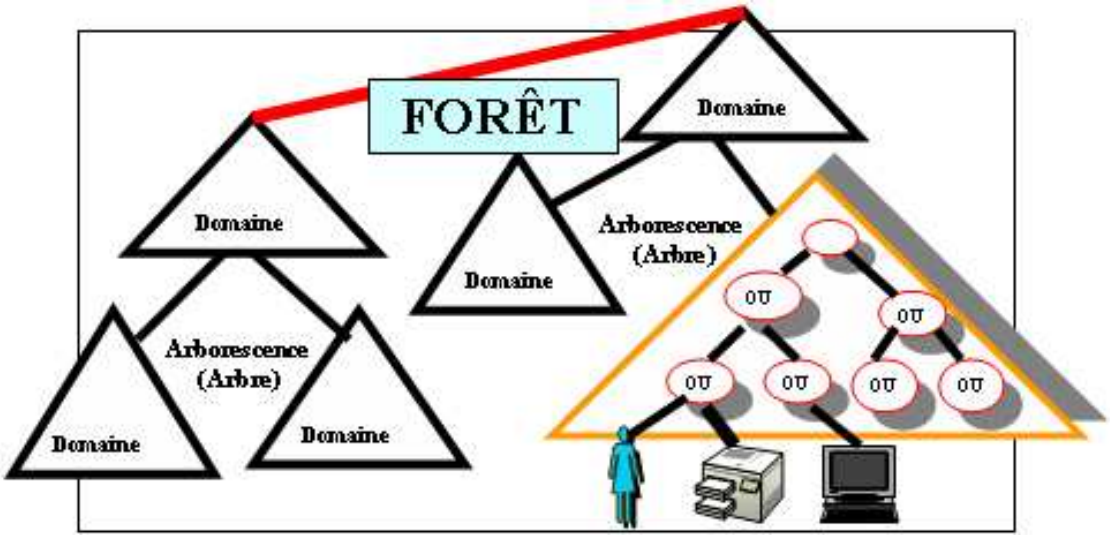
➡ **Arborescence**



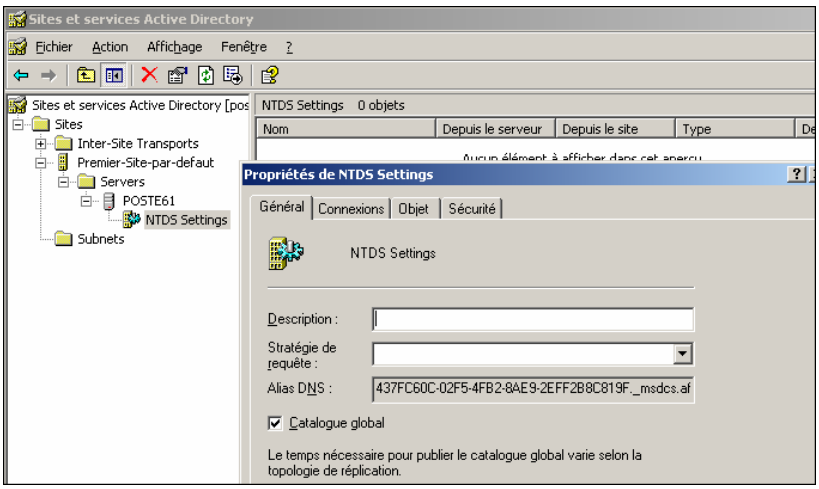
Une **arboresecence** (ou arbre) est un ensemble d'un ou plusieurs domaines Windows 2003 hiérarchisés permettant un partage global des ressources de chaque domaine. Un arbre regroupe un ou plusieurs domaines W2003 Server partageant un même espace de noms.
Rappel : dans Active Directory, les noms de domaines correspondent à des noms **DNS** avec le premier domaine qui porte le **nom de domaine racine de la forêt** (il est non renommable et non supprimable...).
Le domaine de premier niveau est appelé domaine **parent**, les domaines des niveaux inférieurs sont appelés domaines **enfants**.
Un **annuaire partagé** unique est créé pour l'ensemble des domaines de l'arborescence. Chaque domaine possède une partition de l'annuaire principal.

➡ **Forêt**

Une **forêt** est un regroupement d'arborescences indépendantes, mais elle permet une communication entre les différents arbres de la forêt. Vous n'avez la possibilité de planifier qu'une **seule arborescence dans la forêt**. Par contre il peut **exister plusieurs arbres dans la forêt.**

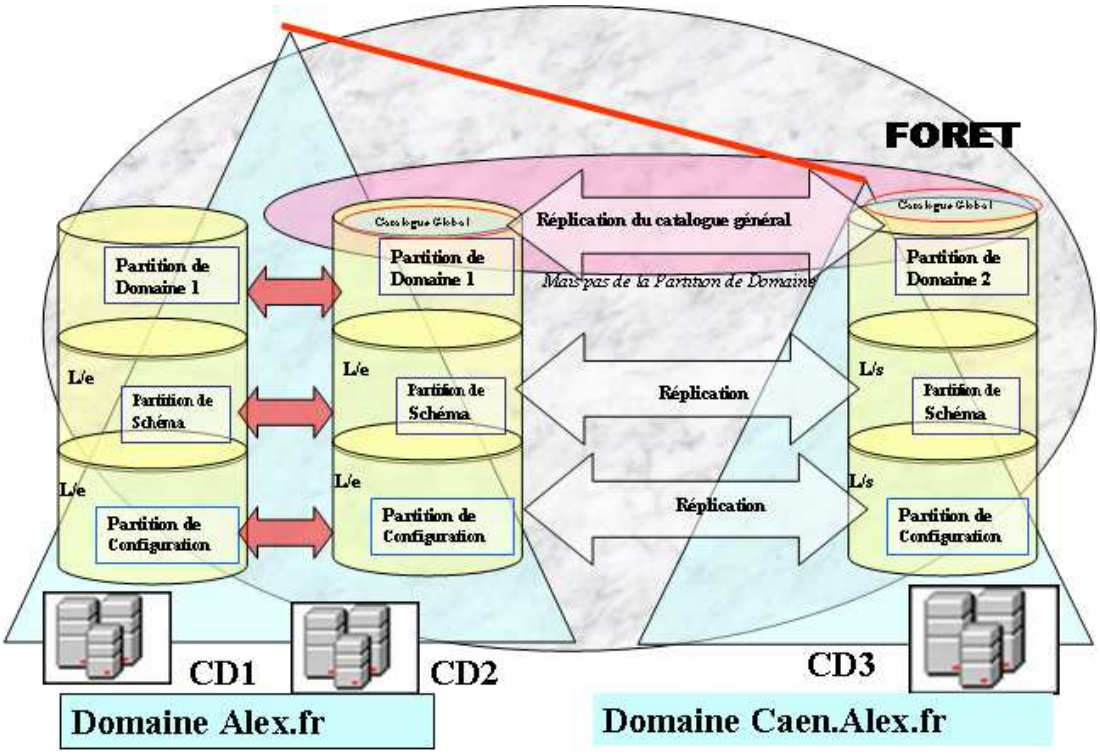


Le **catalogue global** contient les informations qui permettent à chaque utilisateur de s'identifier et de se connecter à chaque domaine de la forêt (sous réserve qu'il en ait les droits). Ce catalogue global est stocké par **défaut dans le premier serveur de domaine installé**.
Un serveur de catalogue global est un contrôleur de domaine possédant un **Catalogue** dans lequel sont répertoriés les **attributs** les plus **couramment** utlisés de tous les objets Active Directory afin de déterminer l'emplacement de tout objet de la forêt.
La base de données Active Directory est partagée en **2 parties** qui sont la **Partition de Domaine** et la **partition de Configuration.**
Seules les informations du schéma et de la la configuration sont dupliquées entre les domaines.
Il en résulte que comme les informations des objets d'un domaine ne sont pas dupliquées vers les autres domaines de la forêt, le serveur de catalogue global va être utilisé pour effectuer des recherches à l'échelle de la forêt. Il est recommandé d'avoir un **serveur de catalogue global** de chaque côté d'une liaison lente et au moins un serveur de catalogue global par domaine.
Lorsque vous lancez la recherche d'un objet à l'intérieur d'un domaine ou d'une OU, une **requête LDAP** est résolue dans la partition du domaine contenant la base d'annuaire de tous les objets du domaine. Par contre si vous lancez la recherche d'un objet dans toute la forêt, c'est le serveur de catalogue global qui sera interrogé et qui retournera le résultat de votre requête.
Le serveur de catalogue global est **systématiquement interrogé à chaque ouverture de session** afin de trouver le nom du domaine et le compte utlisateur. Il fournit aussi des informations sur l'appartenance à des groupes universels (dans l'hypothése où vous êtes en mode natif), afin de créer le jeton d'accès de sécurité contenant les groupes avec **ACL**. De même le serveur global sera interrogé lorque vous insérez dans un groupe un membre d'un autre domaine.



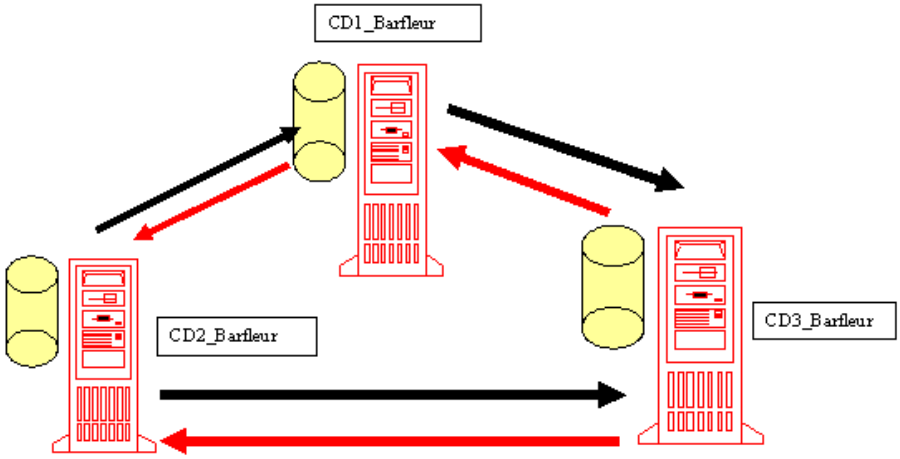
➡ Réplication Active Directory

La **réplication** est la technique de copie permettant à tous les contrôleurs de domaine d'avoir une base **d'annuaire à jour** (on la définit comme un **répliqua**). Cela permet aux utlisateurs et aux services d'accéder à tous moments aux informations de l'annuaire à partir de n'importe quel ordinateur de la forêt. La réplication de W2003 Server est **multimaitre** (c'est-à-dire sur les autres controleurs de domaine) : avec Active Directory, chaque contrôleur de la forêt stocke une copie de la base d'annuaire en lecture/écriture et peut dupliquer la base vers des partenaires de réplication. Un contrôleur de domaine réplique les informations du schéma de la forêt, les informations de configuration pour tous les domaines de la forêt, ainsi que tous les objets et attributs de l'annuaire pour le domaine. La réplication est capable de gérer les conflits qui peuvent arriver (ce peut être le cas où le même compte utlisateur est créé sur deux contrôleurs de domaines au même instant). Par contre entre domaines différents, seules les informations de la partition de schéma et de configuration sont dupliquées. Un serveur de catalogue global stocke les **répliquas partiels** d'objet de partition d'annuaire d'autres domaines (exemple : liste des objets, certains attributs de ces objets ou l'appartenance aux groupes universels). Ces répliquas partiels sont répliqués entre catalogue globaux.



L/s : Lecture seule **L/e :** Lecture écriture

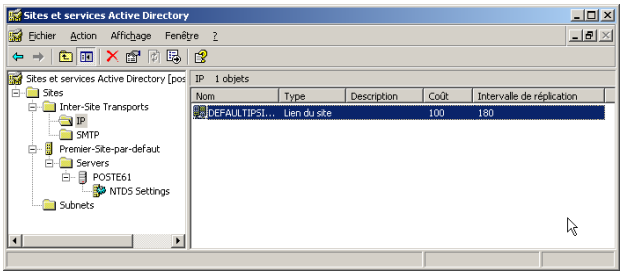
➡ Processus de Réplication



Exemple de 3 contrôleurs de domaine apparetenant au même domaine devant répliquer. Chaque contrôleur de domaine réplique avec chacun des autres. Ce qui permet en cas de modification, d'ajout, de suppression d'élément sur un controleur de domaine de le répliquer sur les autres. Dans notre cas une mise à jour effectuée sur le contrôleur CD1_Barfleur sera nommée **mise à jour d'origine**. Par contre lorsque cette mise à jour sera répliquée sur vers CD2_Barfleur, elle sera nommée mise à jour **répliquée** sur CD2_Barfleur et de même pour CD3_Barfleur.
Il peut arriver la situation où CD3_Barfleur reçoive la mise à jour réalisée sur CD1_Barfleur, par l'intermédiaire de CD2_Barfleur. Prenons comme hypothèse que CD2_Barfleur envoie au contrôleur de domaine CD3_Barfleur une mise à jour déjà réalisée sur CD1_Barfleur, tandis que CD3_Barfleur a déjà reçu cette mise à jour répliquée depuis CD1_Barfleur… Problème, car cette réplication fera office de doublon et engorgera le trafic. Pour éviter cette situation (qui peut sembler théorique), chaque contrôleur de domaine posséde et gére un **USN** (Update Sequence Number) qui est un numéro d'ordre ou numéro de modification. Chaque contrôleur de domaine gére son propre USN et surtout conserve en mémoire l'USN le plus récent reçu de chaque autre contrôleur de domaine du domaine. Dans l'hypothèse où il recevrait un objet en mise à jour dont l'USN est plus ancien que le sien, cela indique qu'il a déjà reçu la mise à jour depuis un autre contrôleur de domaine, et la réplication n'aura pas lieu.

➡ Les protocoles de réplication

Différents protocoles réseaux sont utlisés pour l'échange des informations d'annuiare d'Active Directory. Les protocoles réseaux utlisés peuvent être de type synchrones ou asynchrones sur les liaisons de sites (inter-sites) et dans un site (intrasite). W2003 server posséde 2 protocoles différents pour la réplication. En **inter-sites**, les protocoles **RPC** sur **IP** (Remote Procedure Call) ou **SMTP** (Simple Mail Transfer Protocol). En **intrasite**, seul le protocole **RPC** sur **IP**.
La réplication peut être de type **synchrone** et dans ce cas le contrôleur de domaine envoie une notification, puis attend une réponse avant de contacter un autre contrôleur de domaine. En réplication de type **asynchrone** le contrôleur n'attend pas la réponse à sa demande pour transmettre une notification à un autre contrôleur de domaine. La réplication **IP** utlise les appels de procédures distantes synchrones **RPC** dans une réplication intrasite ou intersite. La réplication **SMTP** est lente, asynchrone et ne peut être planifiée.



➡ **Réplication intrasite**

Elle est utlisée pour la **mise à jour de la base d'annuaire** à l'intérieur d'un site entre contrôleurs de domaines connectés par des liens rapides. Le protocole utilisé est **RPC** sous **IP**.
Deux types de réplication peuvent être mises en œuvre : la réplication normale et la réplication automatique.
Lors d'une modification d'un élément d'Active Directory sur un contrôleur de domaine, il attendra 5 minutes avant d'envoyer un message de notification au premier partenaire de réplication paramétré auparavant, puis il en envoie toutes les 30 secondes aux autres partenaires (s'ils existent).
Les contrôleurs de domaine, prenant connaissance de la requête de notification, vont copier les modifications d'annuaire à partir du contrôleur leur ayant envoyé le message.
Dans le cas où les contrôleurs de domaine partenaires ne reçoivent pas de notification pendant une heure (parce qu'il n'y a eu aucune modification de la base d'annuaire Active Directory), ils démarrent malgré tout le processus de réplication pour être sûrs d'être à jour.
Par contre certaines modifications importantes peuvent être réalisées dans la base d'annuaire comme une stratégie de verrouillage de compte, une stratégie de mot de passe ou des modifications de LSA (Local Security Authority). Dans ce cas les informations sont automatiquement dupliquées sans attendre les 5 mm de latence.
Un outil appelé vérificateur de cohérence (**KCC**) se charge de démarré cette réplication et de définir une boucle de réplication entre tous les contrôleurs de domaine d'un même site afin de garantir que la réplication est rélaisée dans son intégralité. Cela est utile dans le cas où un contrôleur tombe en panne, le **KCC** récrée une nouvelle boucle afin d'obtenir et garantir une réplication compléte.

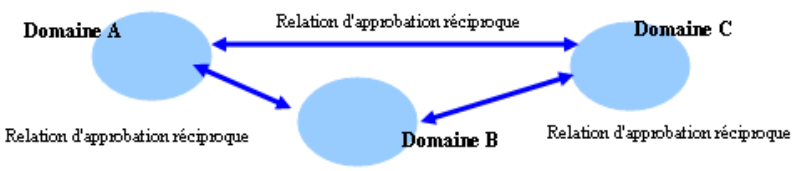
➡ **Réplication inter-sites**

Ce type de réplication est utlisée lorsqu'il existe des liens lents afin d'optimiser le trafic d'ouverture de session et le trafic de réplication. Un site est toujours créé par défaut : **Premier-Site-par-Défaut**, mais il est possible d'en créer d'autres. Cela dépend de l'architecture physque de votre réseau. Un site est toujours composé de zéro, un ou plusieurs sous-réseaux (en fonction de l'adresse IP et du masque de sous-réseau). Quand les sites sont créés, il faut créer les liens de sites et les paramétrer afin de définir et planifier à quel moment la réplication inter-site va s'effectuer.
Dans la structure de duplication inter-site, sur chaque site, un serveur sera défini comme tête de pont de façon manuelle ou automatique. C'est ce serveur dit en **tête de pont**, qui va répliquer avec le serveur tête de pont de l'autre site. En résumé pour gérer la réplication entre les sites, vous devez :

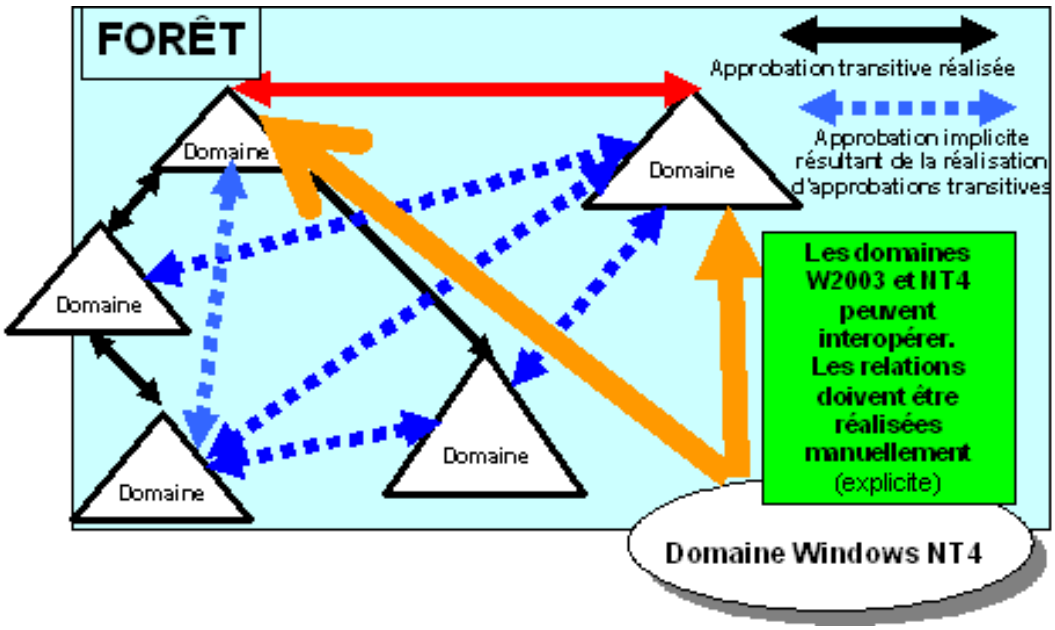
- Créer les sites.
- Créer les sous-réseaux avec leur masque et les associer aux sites.
- Créer des liens entre les sites.
- Eventuellement créer des ponts entre les liens de sites.

6.2.3- Relations d'approbation

Les domaines d'une arborescence sont liés par des **approbations transitives réciproques Kerberos**. Cela signifie que tout utilisateur reconnu dans un domaine l'est automatiquement dans les autres domaines de l'arborescence. **Kerberos** est un protocole de sécurité utilisé sur Internet qui permet d'authentifier un utilisateur. Dans Kerberos V5, les mots de passe en ligne sont encryptés.
Les relations d'approbation vont permettrent aux administrateurs de deux domaines de désigner le domaine qui va partager ses ressources et celui qui mettra en jeu ses comptes utlisateurs.



Dans la figure précédente, tout utilisateur de chaque domaine est reconnu par les autres domaines. Ainsi, un utilisateur du domaine A est reconnu par les contrôleurs de domaines B et C.
Il existe des relations d'approbation **bidirectionnelles** ou **unidirectionnelles**, **automatiques** ou **manuelles** et **transitives** ou non.
Une relation transitive indique que les domaines qui n'ont pas de relation d'approbation **explicite** peuvent contrairement aux domaines NT4 s'approuver **mutuellement** via des **relations** de types **approbations arborescence racine** et **approbations parent enfants.**

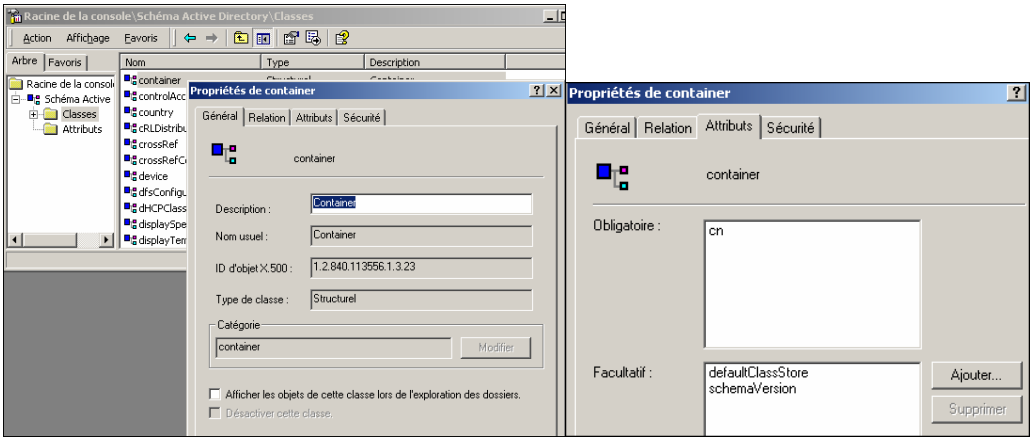


6.2.4- Rôle maître d'opérations

Les **rôles de maîtres d'opération** sont des rôles particuliers affectés à certains contrôleurs de domaine Windows 2003. Certaines fonctions d'Active Directory doivent être confiées de manière unique à certains contrôleurs de domaine d'un domaine ou d'une forêt.

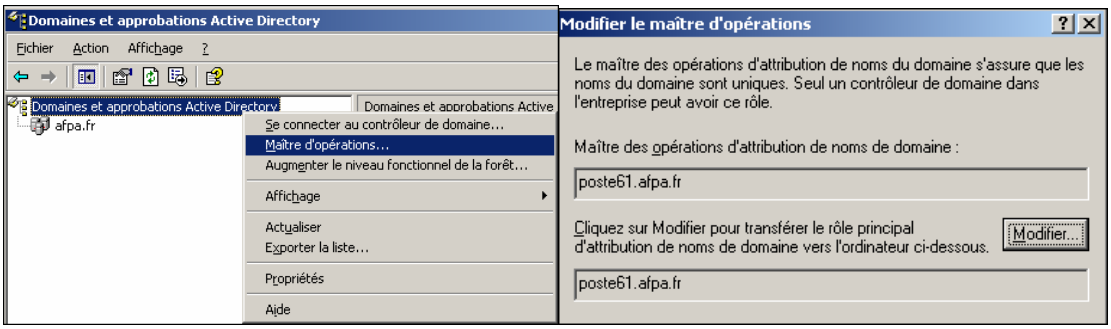
➡ **Au niveau d'une forêt**

Maître de schéma
Le **schéma** Active Directory est la description des types d'objets gérés par Active Directory et la liste des informations relatives à chaque type d'objet. Le **schéma** contient donc la définition des **classes** (types d'objets) et de leurs **attributs** (propriétés de chaque type d'objet).
Une classe est un type d'objet qui partage un ensemble de caractéristiques communes. Et les attributs définissent des propriétés qui peuvent être associées à une ou plusieurs classes. Comme nous l'avons déjà vu certains attributs sont obligatoires et d'autres sont facultatifs. Ces attributs peuvent être hérités de la classe parent ou bien définis de façon explicite pour cette classe. Seul l'Administrateur du Schéma peut accéder en écriture sur le contrôleur maître de schéma, afin d'ajouter ou modifier un attribut, ou ajouter ou modifier une classe. Les mises à jour sont répliquées sur tous les contrôleurs de domaine de la forêt. Il n'existe qu'un seul Maître de schéma par forêt qui par défaut est le premier contrôleur de domaine de la forêt.



La fonction **Maître de schéma** consiste à contrôler les modifications du **schéma**. Le contrôleur de domaine Maître de schéma assure cette fonction pour l'ensemble de la forêt.

Maître d'attribution de noms de domaine
Un autre rôle d'Active Directory est de s'assurer que dans une forêt, les noms des domaines sont uniques. Le maître d'attribution de noms de domaines contrôle en particulier l'ajout ou la suppression de domaines dans une forêt Un seul des contrôleurs de domaine joue le rôle de **maître d'attribution des noms de domaine**. Il assure aussi l'unicité des noms de domaines et interroge le serveur de catalogue global pour vérifier le nom de tous les objets contenus dans Active Directory. Pour cette raison il est recommandé que le maître d'attribution de noms de domaine soit aussi serveur de catalogue global.

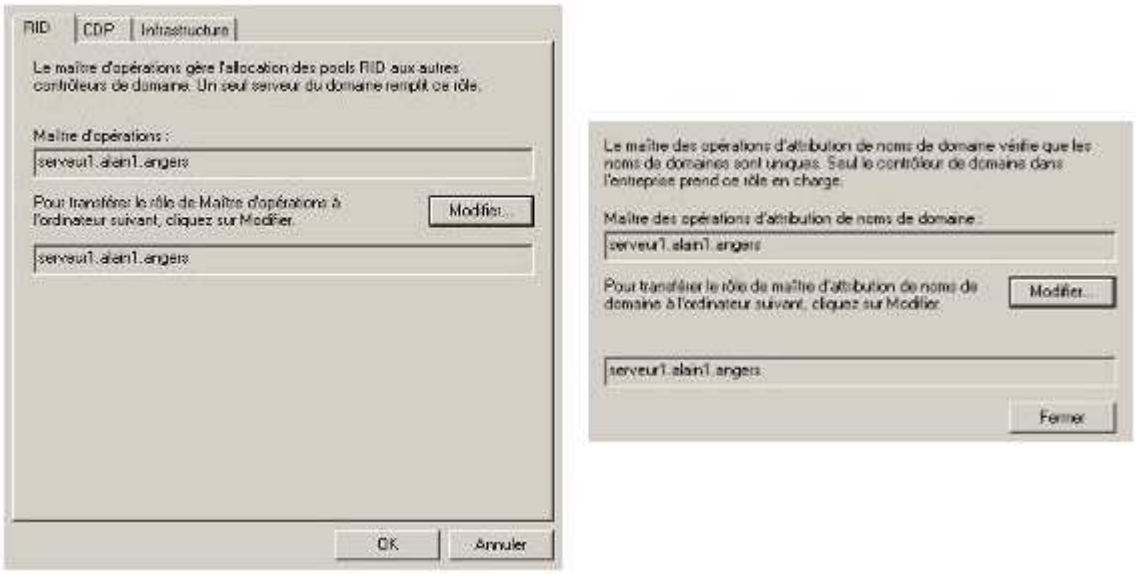


➡ **Au niveau d'un domaine**

Maître RID
Les noms relatifs d'objets doivent être uniques dans un domaine. Un contrôleur est chargé d'assurer l'unicité des noms relatifs à l'intérieur d'un domaine. Il joue le rôle de **maître RID** (Relative Identifier).

Emulateur PDC
En mode client serveur, dans les versions antérieures de client Windows 95, 98 et NT, le logiciel client recherchait à se faire identifier auprès d'un serveur de domaine principal NT (PDC). Dans le cas où le réseau Windows 2003 comporterait ce type de client, il faut qu'un contrôleur de domaine Windows 2003 joue le rôle de Contrôleur principal de domaine (PDC). Un seul contrôleur joue le rôle d'**Emulateur PDC** dans un domaine.

Maître d'infrastructure
Un seul serveur de domaine joue le rôle de **maître d'infrastructure** qui consiste à contrôler les modifications sur les noms et attributs des utilisateurs membres d'un groupe. Le maître d'infrastructure est responsable de la cohérence des informations sur le nom des objets Active Directory en fonction de leur SID.



6.3- Espace de noms DNS

Un **espace de noms** est une zone où peut se faire la résolution de noms. La résolution de noms est l'opération qui consiste à convertir un nom en une autre information qui lui est associée comme par exemple un objet ou une adresse IP. Active Directory utilise sur l'espace de noms DNS (Domain Name System).

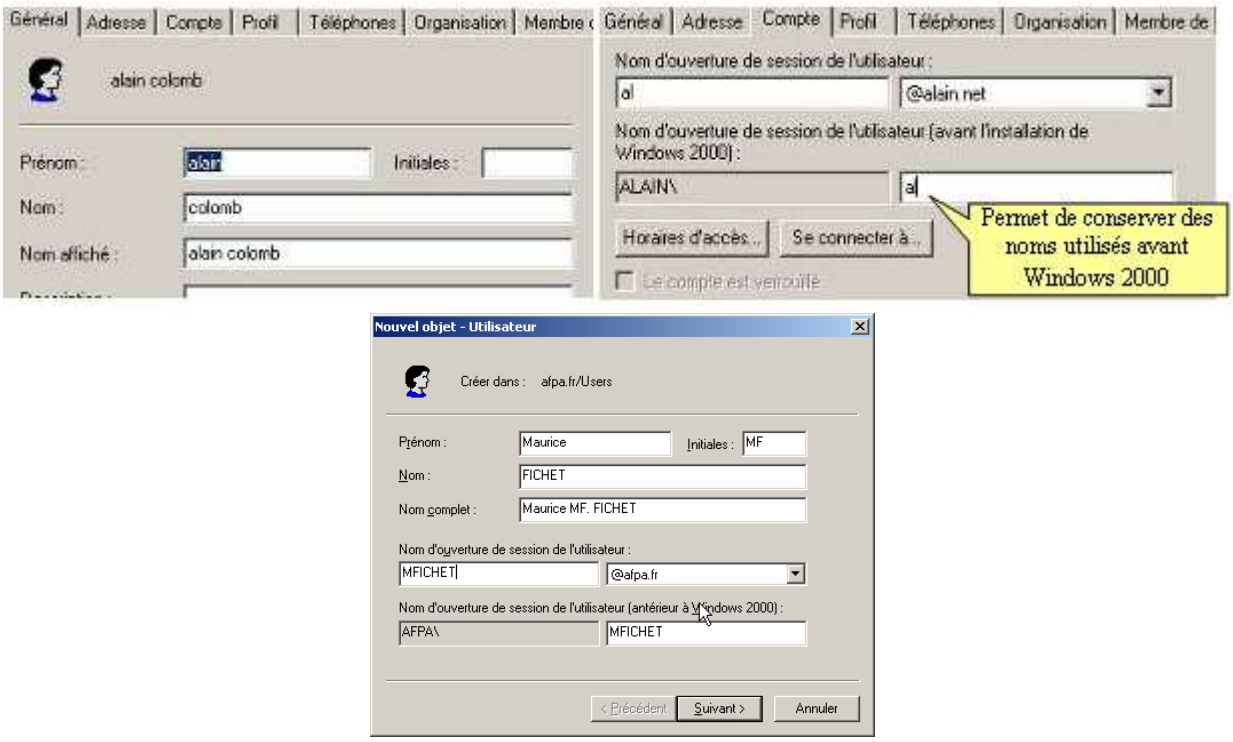
6.3.1- Espace de noms de domaine

Active Directory utilise le système de noms DNS pour identifier les noms des domaines. Ceci permet une intégration parfaite de Windows 2003 dans la technologie **Internet**. En ce qui concerne les domaines, on distingue 2 types d'espaces de noms :
Espaces de noms contigus : c'est le cas des domaines d'une arborescence entre le nom d'un domaine enfant et le nom d'un domaine parent.
Espaces de noms disjoints : c'est le cas d'un domaine d'un arbre dans une forêt et un autre domaine dans un autre arbre de la même forêt.

6.3.2- Espace de noms d'objets

Chaque objet d'Active Directory possède un nom qui est mémorisé sous différentes formes :

- **Nom unique** : c'est une chaîne de caractères qui identifie de manière unique, par exemple, un utilisateur. La chaîne se présente sous la forme :
  /DC=COM/DC=dufour/OU=Secret/CN=Users/CN=Brigitte Dufour
  DC signifie Composant du Domaine, OU signifie Unité d'Organisation et CN signifie Canonical Name (Nom courant)
- **Nom unique relatif** (RDN : Relative Distinguished Name) : c'est un nom d'objet alors que l'on a déjà référencé le contexte dans lequel il se trouve (c'est à dire son nom de domaine et son organisation). Dans l'exemple ci-dessus, le nom relatif est Brigitte Dufour. Il ne peut y avoir qu'un seul nom Brigitte Dufour dans un contexte donné, mais il peut y avoir plusieurs objets Brigitte Dufour dans l'espace de nom d'Active Directory.
- **Nom d'utilisateur principal** : c'est un nom abrégé utilisé pour se connecter. Par exemple : pour Brigitte Dufour, le nom d'utilisateur est Bduf dans le domaine dufour.com. Son nom de connexion est Bduf@dufour.com. En fait, il suffit de taper Bduf, le système ajoutant le nom de domaine.



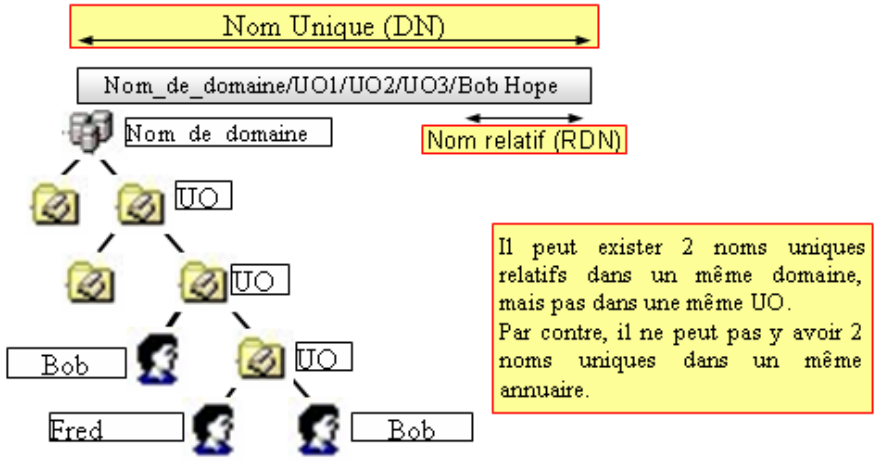
Autre exemple :

- **Nom principal de l'utilisateur :** il est constitué du nom d'ouverture de session suivi du nom de domaine où il est situé. Exemple : utilisateur **MFICHET** membre du domaine afpa**.**fr aura comme nom **MFICHET@afpa.fr**
- **Nom unique relatif** (RDN : Relative Distinguished Name) est le nom complet permettant de situer l'objet dans un domaine et dans une unité d'organisation. Dans l'exemple précédent le nom complet de l'utilisateur **Maurice FICHET** créé dans l'UO, **users et dans le domaine afpa.fr est inscrit sous la forme suivante :**
  - **Nom canonique :** Maurice MF.FICHET.users.afpa.fr
  - **Nom unique LDAP : CN**=Maurice MF.FICHET, **OU**=users, **DC**=afpa, **DC**=fr, Avec **CN**=nom commun (Commun Name), **OU**=unité organisationnelle **DC**=composant de domaine (Domain Component).
- Les noms **LDAP** utilisent la convention de nom X500 appelés nommage avec attributs (attributed naming) qui normalise l'annuaire.

En plus chaque objet possède une identité unique : le **GUID** (Globally Identifier).

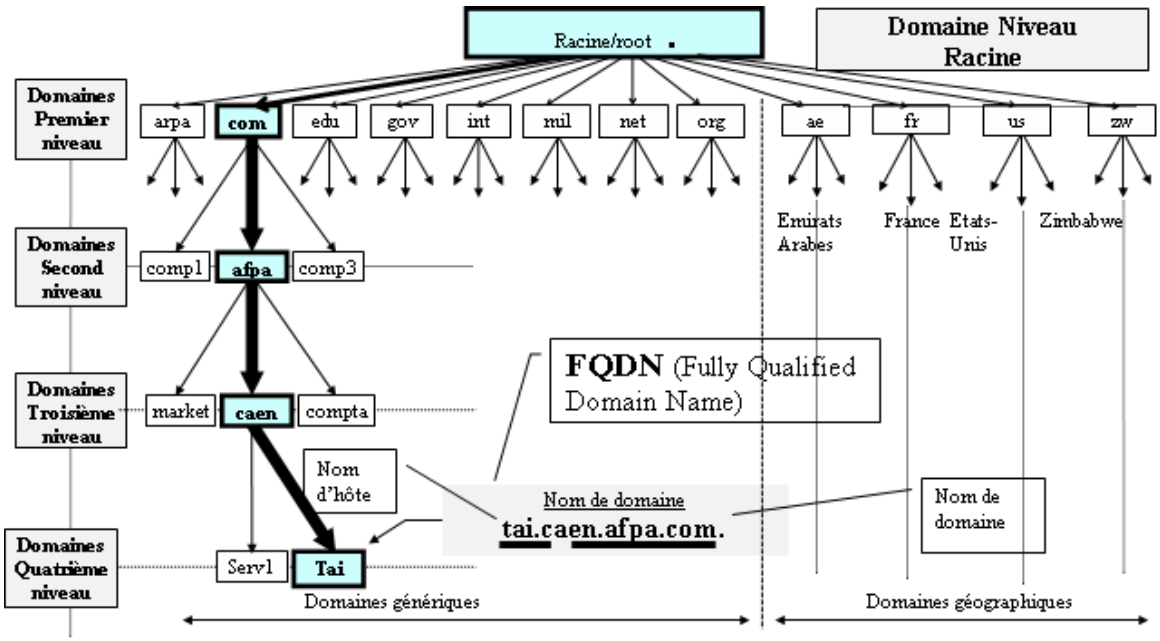
- **GUID** (Global Unique IDentifier) : c'est un nombre codé sur 128 bits qui est unique. Lorsqu'on crée un objet, le système lui attribue automatiquement un **Identificateur**. Cet identificateur ne sera jamais modifié, même en cas de renommage de l'objet ou déplacement dans un domaine ou un arbre. Par contre si l'objet est supprimé, le **GUID** est détruit et ne sera jamais plus utilisé, même si l'on crée un autre objet portant le même nom que celui supprimé. Ce nombre n'est pas visible aux utilisateurs et n'est accessible qu'au seul système.
- Le **GUID** d'un objet est utilisé par AD pour **localiser** les objets recherchés. Il est automatiquement publié dans le catalogue global et est utilisé lors de la réplication.
- Le **SID** qui est une valeur unique codée sur 128 bits composée d'un **RID** (Identificateur Relatif) et d'un identificateur de domaine. Le SID peut changer si l'utilisateur ou le groupe est déplacé dans un autre domaine. Dans ce cas, l'objet garde le même RID mais il obtient un nouvel identificateur de domaine. Le SID fait partie du jeton d'accès créé à l'ouverture de session et identifie l'utilisateur et le groupe dans les ACL (Acess Control List) des ressources.
- Le **SID** a été conservé sous W2003 pour des raisons de compatibilité avec NT4 qui ne connaît pas le **GUID** d'Active Directory.

6.3.3- Règles d'attributions des noms dans Active Directory

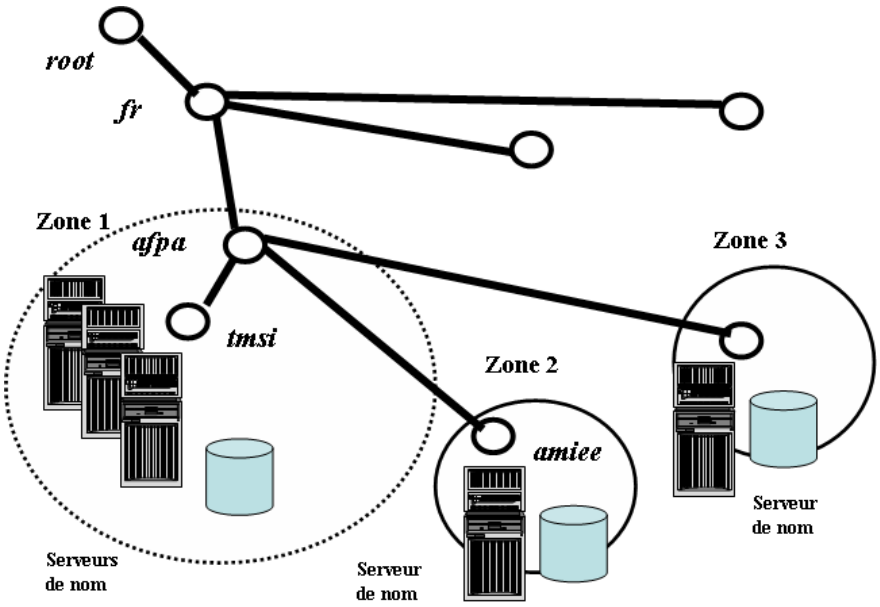


6.3.4- Présentation générale du processus de résolution de noms

Le **DNS** ou système de nom de domaines est le service de résolution obligatoire (sinon vous ne pouvez installer Active Directory) pour les domaines Active Directory depuis W2000 Server. Sous **NT4** le service de résolution de noms Internet Windows le plus couramment utilisé est **WINS**. Mais il a perdu de son utilité sous W2000 et W2003. Il est conservé uniquement pour la compatibilité.
Au début des réseaux et d'Internet la communication entre machine était réalisée à l'aide de son adresse IP et c'est toujours le cas. Mais il est beaucoup plus facile de retenir des noms plutôt que des adresses IP. Mais comme le protocole TCP/IP a besoin des adresses IP pour fonctionner, il faut donc associer une adresse IP à chaque nom. Cette technique est appelée la résolution de noms.
Autrefois, un fichier texte (**hosts.txt**) servait à mémoriser l'association **@dresse IP et nom**. Chaque machine devait être manuellement référencée dans ce fichier, et ce fichier devait être recopié sur chaque machine... Le nombre des machines ayant augmenté rapidement, la gestion de ce fichier est devenue impossible. De plus sa mise à jour était difficile et engorgeait le réseau.
Quelques années plus tard, c'est-à-dire aujourd'hui, pouvez–vous imaginer qu'un seul fichier texte puise contenir les millions de machines sur Internet. Il a donc fallu imaginer une **structure hiérarchique** pouvant répartir la charge de gestion des noms de machines sur plusieurs serveurs **DNS** (nota : encore aujourd'hui et sur un petit réseau vous pouvez utilisé le fichier Hosts qui est situé dans **%systemroot%\system32\drivers\etc**).

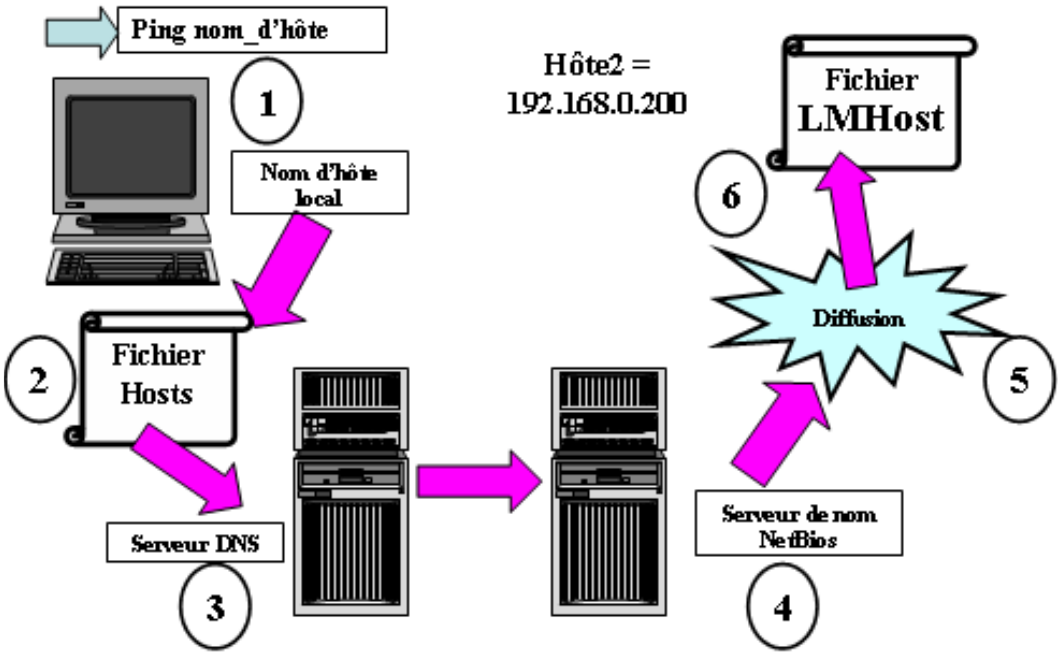


Au niveau le plus haut de l'arborescence, le domaine racine est représenté par un point. A ce jour il existe **13 serveurs DNS** à ce niveau dans le monde entier (liste consultable sur Internet sur le site de l'Internic). Ensuite vous avez le **1er niveau** où sont situées les extensions : .**com, .edu, .gov, .mil, .net, .org**... et les codes de pays : .**fr, .us, .be**...
Au **deuxième niveau** vous trouvez le nom des domaines comme ci-dessus : **afpa, comp1, comp2**...
Au **3éme niveau** vous pouvez trouver d'autres niveaux comme ci-dessus : **caen, market, compta**...
Vous pouvez continuer les niveaux afin d'obtenir votre machine. Elle sera référencée par un **FQDN** (Full Qualified Domain Name ou Nom de domaine pleinement qualifié).
Ce qui donne dans notre exemple le serveur **tai** du domaine enfant ayant pour nom **caen**, du centre de formation ayant pour nom de domaine de second niveau **afpa**, avec **com** comme nom de domaine de 1er niveau aura le nom **FQDN** : **tai.caen.afpa.com** (le dernier **.** indiquant la racine).



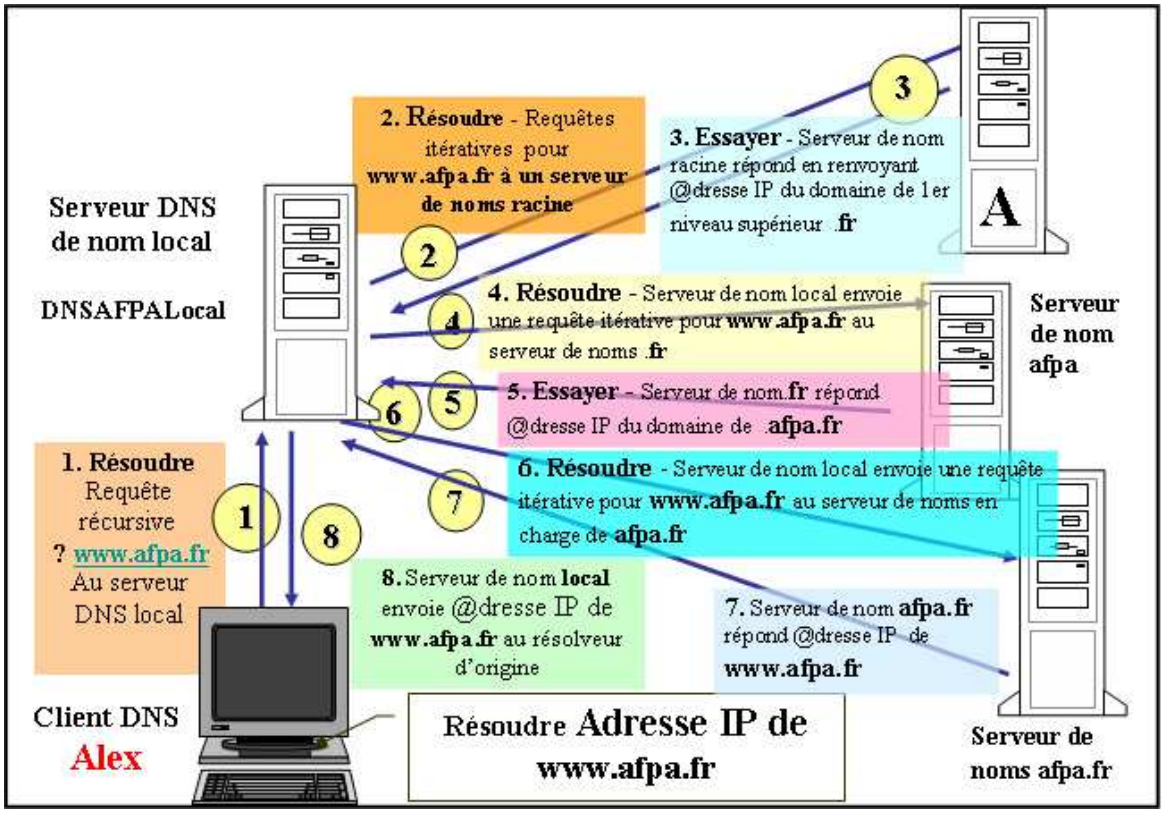
Chaque serveur **DNS** ne gère pas toute l'arborescence, mais seulement son domaine. Mais il peut aussi gérer un domaine enfant ou une **zone** (zone = nœud de l'arborescence ou plusieurs nœuds de l'arborescence). Il peut aussi déléguer cette gestion à un autre serveur DNS.

Technique de la résolution de noms



Dans l'exemple ci-dessous, prenons le client Maurice désirant accéder au serveur Web www.afpa.fr pour récupérer les informations sur le dernier cours **W2003 Server.** Maurice tape à partir de la zone adresse de son navigateur Internet : http://www.afpa.fr.
Il faut donc que le micro client de Maurice puisse **récupérer l'adresse IP du serveur Web**.
Nous allons voir le déroulement de la séquence :

- Le **client** fait une demande de résolution de nom à son **serveur DNS de nom local** portant le nom **DNSAFPALocal**. Mais il ne gère pas cette zone (on emploie le terme **autorité**).
- Le serveur DNS va **interroger alors un serveur DNS** (parmi les 13) situé à la **racine d'Internet**.
- Ce serveur DNS racine n'a pas non plus autorité sur la zone demandée, mais il a délégué la gestion du **.fr**. Il retourne au serveur **DNSAFPALocal** la **liste** des serveurs DNS ayant **autorité** sur la zone **.fr**.
- **DNSAFPALocal** interroge alors un serveur ayant autorité sur la zone **.fr**.
- Ce serveur DNS n'a pas non plus autorité sur la zone afpa.fr. Il retourne au serveur **DNSAFPALocal** la liste des serveurs DNS ayant autorité sur la zone **afpa.fr**.
- **DNSAFPALocal** interroge alors un serveur ayant autorité sur la zone **afpa.fr**.
- Il renvoie alors au serveur **DNSAFPALocal l'adresse IP du serveur Web** demandé (www.afpa.fr).
- **DNSAFPALocal** renvoie à son client (le micro de Maurice) l'adresse IP de www.afpa.fr.
- Maurice peut maintenant télécharger ce qu'il veut sur le serveur Web (bien sur en fonction de ses droits).



Les demandes ou requêtes précédentes sont de deux types :

- **Récursive** comme celle réalisée par Alex à partir de son poste client pour son serveur DNS local. Cette requête est appelée récursive car le DNS doit retourner une réponse complète. Cette réponse peut-être positive comme l'adresse IP du serveur Web ou négative indiquant qu'il ne l'a pas trouvée.
- Par contre le serveur DNS DNSAFPALocal a réalisé plusieurs requêtes de type **itératives** auprès des différents serveurs DNS. En effet chacun des serveurs DNS interrogés n'ont pu retourner que des réponses partielles (telle la liste des serveurs ayant autorité sur .fr).

6.3.5- Zone

L'espace de noms DNS peut être divisé en **zones**. Chaque zone représente une base de données placée sous une autorité qui contient tout ou partie des noms et adresses des ordinateurs du réseau. Si le nombre de noms d'ordinateurs et d'adresses qui sont liés est très important pour un réseau donné, il est possible de diviser la base de données en plusieurs zones stockées sur un ou plusieurs serveurs DNS.

Zone de recherche directe
Une **zone de recherche directe** permet de retrouver l'adresse IP d'un ordinateur du réseau dont le nom est fourni dans une requête au serveur de noms DNS.
Un **fichier de zone** est créé pour contenir la liste des noms d'ordinateurs du domaine et leurs adresses IP respectives.

Zone de recherche inversée
Une recherche inversée permet de trouver le nom d'ordinateur du domaine lorsqu'on fait une requête avec l'adresse IP. L'utilitaire **NSLOOKUP**, entre autres, utilise la recherche inversée. Il peut exister un fichier de zone pour chaque sous réseau du domaine.

Types de zone
Dans Windows 2003 pour les zones de recherche directe ou inversée, il existe 4 types de zones :

- **Zone intégrée à Active Directory :** les fichiers zone de recherche sont intégrés dans Active Directory. Ils ne sont pas accessibles en mode texte et ne conviennent que pour un réseau purement Windows 2003.
- **Zone principale standard :** un fichier est créé dans le répertoire C:\WINNT\system32\DNS. Son nom reprend le nom de domaine et y ajoute le suffixe DNS. Par exemple dufour.com.dns. Ce fichier est un fichier texte, il y est possible d'y rajouter des noms et adresses IP d'ordinateurs non Windows 2003 (Unix par exemple).
- **Zone secondaire standard :** une copie du fichier en lecture seule de la zone principale est créée sur un serveur de noms secondaire. Ceci permet d'avoir une copie en cas de problème sur le serveur principal.
- **Zone Stub :** c'est une nouveauté de W2003 Server. La zone **Stub** ne contient que les enregistrements nécessaires permettant d'identifier les serveurs DNS ayant autorité sur une zone. Cette zone Stub contient les enregistrements de type **SOA** (Start of Autority), **NS** (Name Server) ainsi que les enregistrements de type **A** (Adresse) nécessaires. Cette zone permet de retourner les adresses des serveurs DNS d'une zone comme lors des recherches de type itératives entre serveurs DNS.

6.3.6- Serveurs de nom

Les serveurs de noms sont des serveurs Windows ou non Windows (Unix, Linux) qui contiennent les fichiers de zones. Un serveur principal contient le fichier de la zone principale standard et un serveur secondaire le fichier de zone secondaire.

6.3.7- Réplication et transfert de zones

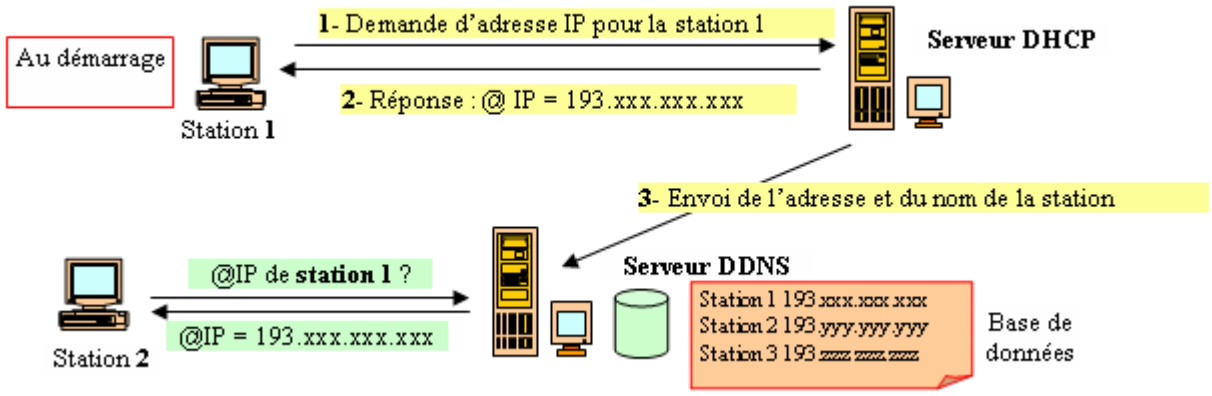
Réplication
La présence de serveurs de noms de domaine secondaires DNS permet la réplication des fichiers de zones. Cette pratique se justifie dans les cas suivants :

- Offrir une redondance en cas de panne du serveur DNS principal.
- Réduire le trafic lorsque le domaine est dans des sites différents reliés par des liaisons WAN.
- Réduire la charge du serveur de noms DNS principal.

Transfert de zone
La réplication des fichiers de zones se fait au cours d'une opération appelée transfert de zone.
Transfert de zone complet
Il y a un transfert complet du fichier de zone lorsqu'un nouveau serveur de noms DNS secondaire est installé. On parle de transfert de zone complet (**AXFR**).
Transfert de zone incrémentiel
Une fois le transfert de zone complet effectué, il se fait une mise à jour des fichiers de zones dans les serveurs de noms secondaire au cours d'une opération nommée transfert de zone incrémentiel (**IXFR**).

6.3.8- DDNS

Le service DNS inclut une possibilité de mise à jour dynamique des fichiers de zone, c'est le service **DDNS** Dynamic Domain Name System. Dès qu'un nouvel ordinateur apparaît dans le domaine, le serveur DNS ajoute automatiquement un **enregistrement A** avec son nom et son adresse IP dans le fichier de zone. Ce service s'appuie sur le service DHCP (Dynamic Host Configuration Protocol).

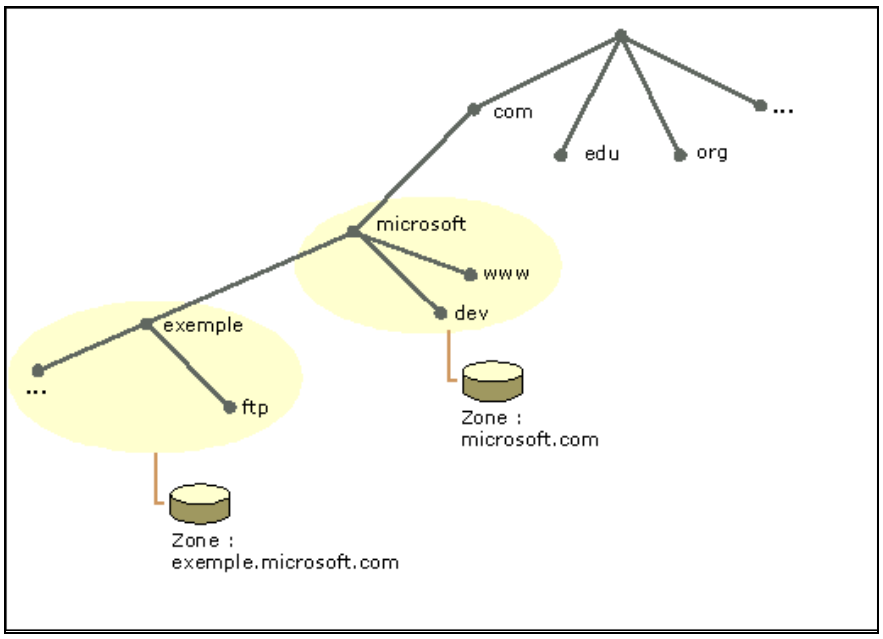


6.4- Compléments : présentation des zones et du transfert de zone

Le système de nom de domaine (DNS, Domain Name System) permet de diviser un espace de noms DNS en zones. Ces zones stockent des informations de nom relatives à un ou plusieurs domaines DNS. Pour chaque nom de domaine DNS inclus dans une zone, la zone devient la source de référence d'informations sur ce domaine.

6.4.1- Présentation de la différence entre les zones et les domaines

Initialement, une zone est une base de données de stockage pour un seul nom de domaine DNS. Si d'autres domaines sont ajoutés au dessous du domaine utilisé pour créer la zone, ils peuvent faire partie de cette même zone ou appartenir à une autre zone. Un sous domaine ajouté à une zone peut être géré et inclus dans les enregistrements de la zone d'origine, ou délégué à une autre zone créée pour prendre en charge ce sous domaine.
Par exemple, l'illustration suivante indique le domaine microsoft.com qui contient des noms de domaines pour Microsoft. À sa création sur un serveur particulier, le domaine microsoft.com est configuré en tant que zone unique pour l'ensemble de l'espace de noms DNS de Microsoft. Si le domaine microsoft.com a besoin d'utiliser des sous domaines, ces derniers doivent être inclus dans la zone ou délégués à une autre zone.



Dans cet exemple, le domaine microsoft.com contient un nouveau sous domaine, le domaine exemple.microsoft.com, délégué en dehors de la zone microsoft.com et géré dans sa propre zone. La zone microsoft.com doit néanmoins contenir quelques enregistrements de ressources afin de fournir les informations de délégation indiquant les serveurs DNS qui font autorité pour le sous domaine exemple.microsoft.com délégué.
Si un sous domaine de la zone microsoft.com n'est pas délégué, toutes les données du sous domaine sont conservées dans la zone microsoft.com. Par exemple, le sous domaine dev.microsoft.com n'est pas délégué et est géré par la zone microsoft.com.

6.4.2- Pourquoi la réplication de zone et les transferts de zones sont-ils nécessaires ?

En raison de leur rôle essentiel dans DNS, les zones sont supposées être disponibles sur plusieurs serveurs DNS du réseau afin de garantir la disponibilité et la tolérance de pannes lors de la résolution de requêtes de noms. Dans le cas contraire, si un seul serveur est utilisé et que ce serveur ne répond pas, les requêtes de noms réalisées dans la zone risquent d'échouer. Pour que d'autres serveurs puissent héberger une zone, il est nécessaire de transférer la zone de manière à répliquer et à synchroniser toutes les copies de la zone utilisées sur chaque serveur configuré pour l'héberger.
Lorsqu'un nouveau serveur DNS est ajouté au réseau et est configuré en tant que nouveau serveur secondaire d'une zone existante, il effectue un transfert initial complet de la zone de manière à obtenir et à répliquer une copie complète des enregistrements de ressources de cette zone. Pour les implémentations de serveurs DNS plus anciennes, cette méthode de transfert complet d'une zone est également utilisée lorsque la zone change et doit être mise à jour. Pour les serveurs DNS exécutant Windows Server 2003, le service DNS prend en charge le transfert de zone incrémentiel, un processus de transfert de zone DNS qui s'intéresse aux changements intermédiaires.

6.4.3- Transferts de zones incrémentiels

Les transferts de zones incrémentiels sont décrits dans la RFC (Request for Comments) 1995. Ils constituent une norme DNS supplémentaire pour la réplication des zones DNS. Lorsqu'ils sont pris en charge à la fois par un serveur DNS jouant le rôle de source pour une zone et par tous les serveurs qui copient la zone à partir de ce serveur, les transferts incrémentiels constituent une méthode plus efficace de diffusion des changements et des mises à jour des zones.
Dans les implémentations DNS plus anciennes, toute requête de mise à jour des données d'une zone nécessitait le transfert complet de l'ensemble de la base de données de la zone à l'aide d'une requête AXFR. Avec le transfert incrémentiel, un type de requête différent (IXFR) peut être utilisé. Celui-ci permet au serveur secondaire de recevoir uniquement les changements intervenus sur une zone dont

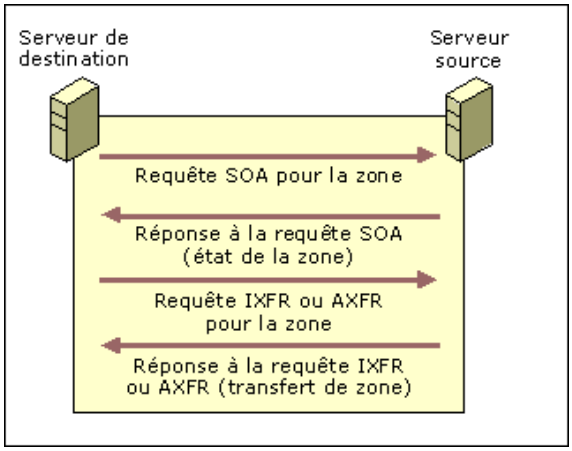
il a besoin pour synchroniser sa copie de la zone avec la source de la zone (une copie principale ou secondaire de la zone gérée par un autre serveur DNS).
Avec les transferts de zones IXFR, les différences entre la version source et les versions répliquées de la zone sont tout d'abord déterminées. S'il s'avère que les versions sont identiques (cette indication est fournie par le champ de numéro de série dans l'enregistrement de ressource SOA (start of authority) de chaque zone) aucun transfert n'est effectué.
Si le numéro de série de la zone est plus élevé sur le serveur source que sur le serveur secondaire effectuant la requête, un transfert est réalisé, mais seuls les changements des enregistrements de ressources (RR) pour chaque version incrémentielle de la zone sont transférés. Pour qu'une requête IXFR réussisse et que les changements soient envoyés, le serveur DNS source de la zone doit conserver un historique des changements incrémentiels intervenus sur la zone et l'utiliser pour répondre à ces requêtes. Le processus de transfert incrémentiel engendre un trafic beaucoup moins élevé sur le réseau et les transferts de zones sont réalisés beaucoup plus rapidement.

6.4.4- Exemple : transfert de zone

Un transfert de zone peut se produire dans chacune des situations suivantes :

- Lorsque l'intervalle d'actualisation de la zone arrive à expiration.
- Lorsqu'un serveur secondaire est averti par son serveur maître que la zone a changé.
- Lorsque le service Serveur DNS est démarré sur un serveur secondaire de la zone.
- Lorsque la console DNS est utilisée sur un serveur secondaire de la zone pour lancer manuellement un transfert à partir de son serveur maître.

Les transferts de zones sont toujours lancés sur le serveur secondaire d'une zone et envoyés aux serveurs maîtres configurés qui jouent le rôle de source pour la zone. Les serveurs maîtres peuvent être tout autre serveur DNS qui charge la zone, tel que le serveur principal de la zone ou un autre serveur secondaire. Lorsque le serveur maître reçoit la requête relative à la zone, il peut répondre par un transfert partiel ou complet de la zone vers le serveur secondaire.
Comme le montre l'illustration suivante, les transferts de zones entre les serveurs sont réalisés selon un processus bien précis. Ce processus peut varier selon qu'une zone a été antérieurement répliquée ou qu'une réplication initiale d'une nouvelle zone est effectuée.



Dans cet exemple, la séquence suivante est réalisée pour un serveur secondaire effectuant une requête - le serveur de destination - pour une zone et son serveur source, un autre serveur DNS qui héberge la zone.
Dans la nouvelle configuration, le serveur de destination envoie une requête initiale de transfert (AXFR) de type « zone complète » au serveur DNS maître configuré comme source de la zone.
Le serveur maître (source) répond et effectue un transfert complet de la zone vers le serveur secondaire (destination).
La zone est transférée vers le serveur de destination demandant le transfert et sa version est établie à l'aide d'un champ **Numéro de série** des propriétés de l'enregistrement de ressources (RR) SOA (start of authority). L'enregistrement de ressources SOA (start of authority) contient également un

intervalle d'actualisation défini en secondes (par défaut, 900 secondes ou 15 minutes) indiquant à quel moment le serveur de destination doit de nouveau demander le renouvellement de la zone avec le serveur source.
À expiration de l'intervalle d'actualisation, une requête SOA est utilisée par le serveur de destination pour demander le renouvellement de la zone à partir du serveur source.
Le serveur source répond à la requête relative à son enregistrement SOA (start of authority).
Cette réponse contient le numéro de série actuel de la zone au niveau du serveur source.
Le serveur de destination vérifie le numéro de série de l'enregistrement SOA (start of authority) fourni en réponse et détermine comment renouveler la zone.
Si le numéro de série indiqué dans la réponse de la requête SOA est égal au numéro de série local actuel, il en conclut que la zone est identique sur les deux serveurs et qu'un transfert de zone n'est pas nécessaire. Le serveur de destination renouvelle ensuite la zone en redéfinissant son intervalle d'actualisation en fonction de la valeur de ce champ dans la réponse de la requête SOA obtenue du serveur source.
Si le numéro de série indiqué dans la réponse de la requête SOA est supérieur au numéro de série local actuel, il en conclut que la zone a été mise à jour et qu'un transfert est nécessaire.
Si le serveur de destination conclut que la zone a changé, il envoie une requête IXFR au serveur source, contenant la valeur locale actuelle du numéro de série dans l'enregistrement SOA (start of authority) de la zone.
Le serveur source répond par un transfert incrémentiel ou un transfert complet de la zone.
Si le serveur source prend en charge le transfert incrémentiel en conservant un historique des changements incrémentiels récents intervenus sur une zone pour les enregistrements de ressources modifiés, il peut répondre par un transfert incrémentiel (IXFR) de la zone.
Si le serveur source ne prend pas en charge le transfert incrémentiel, ou qu'il ne conserve pas un historique des changements intervenus sur une zone, il peut répondre par un transfert complet (AXFR) de la zone.

Remarques
Le transfert de zone incrémentiel réalisé par le biais d'une requête IXFR est pris en charge dans les serveurs exécutant Windows 2003 et Windows Server 2003. Dans les versions antérieures du service DNS et dans beaucoup d'autres implémentations de serveurs DNS, le transfert de zone incrémentiel n'est pas disponible et seuls les requêtes et les transferts de type « zone complète » (AXFR) sont utilisés pour répliquer les zones.

6.4.5- Notification DNS

Les serveurs DNS Windows prennent en charge la notification DNS (DNS Notify), une mise à jour de la spécification originale du protocole DNS qui permet d'avertir les serveurs secondaires lorsque des changements interviennent sur une zone (RFC 1996). La notification DNS met en œuvre un mécanisme de diffusion permettant d'avertir un ensemble spécifique de serveurs secondaires pour une zone lorsque cette dernière est mise à jour. Les serveurs qui sont avertis peuvent alors lancer un transfert de zone comme décrit précédemment pour extraire du serveur maître les changements intervenus sur une zone et mettre à jour leurs réplicats locaux de la zone.
Pour que les serveurs secondaires soient avertis par le serveur DNS jouant le rôle de serveur source configuré pour une zone, l'adresse IP de chaque serveur secondaire doit dans un premier temps être incluse dans la liste de notification du serveur source. Si vous utilisez la console DNS, cette liste est gérée dans la boîte de dialogue **Avertir**, accessible sous l'onglet **Transferts de zone** des **Propriétés** de zone.
La console DNS permet non seulement d'avertir les serveurs répertoriés, mais aussi d'utiliser le contenu de la liste de notification pour restreindre ou limiter l'accès au transfert de zone uniquement aux serveurs secondaires spécifiés dans la liste. De cette manière, les serveurs DNS inconnus ou non approuvés ne pourront pas extraire, ou demander, les mises à jour d'une zone.
Le processus de notification DNS par défaut utilisé pour les mises à jour de zone est brièvement résumé ci-dessous.

La zone locale sur un serveur DNS jouant le rôle de serveur maître (source de la zone pour les autres serveurs) est mise à jour. Lorsque la zone est mise à jour sur le serveur maître ou source, le champ de numéro de série de l'enregistrement de ressource (RR) SOA (start of authority) est également mis à jour pour indiquer une nouvelle version locale de la zone.
Le serveur maître envoie un message de notification DNS aux autres serveurs figurant sur la liste de notification configurée.
Tous les serveurs secondaires qui reçoivent le message de notification peuvent répondre en lançant une requête de transfert de zone auprès du serveur maître.
Le processus normal de transfert de zone peut alors continuer comme décrit dans la section précédente.
Vous ne pouvez pas configurer de liste de notification pour une zone de stub.

Important
Utilisez la notification DNS uniquement pour avertir les serveurs fonctionnant en tant que serveurs secondaires pour une zone. Pour la réplication des zones intégrées à l'annuaire, la notification DNS n'est pas nécessaire.
En effet, tout serveur DNS qui charge une zone à partir d'Active Directory sonde automatiquement l'annuaire (spécifié dans l'intervalle d'actualisation de l'enregistrement de ressource SOA) pour mettre à jour et actualiser la zone.
Dans ce cas, la configuration d'une liste de notification peut en fait nuire aux performances du système en créant inutilement des requêtes de transfert supplémentaires pour la zone mise à jour.

Remarques
Par défaut, le serveur DNS autorise uniquement un transfert de zone vers les serveurs DNS faisant autorités et mentionnés dans les enregistrements de ressources du serveur de nom de cette zone.

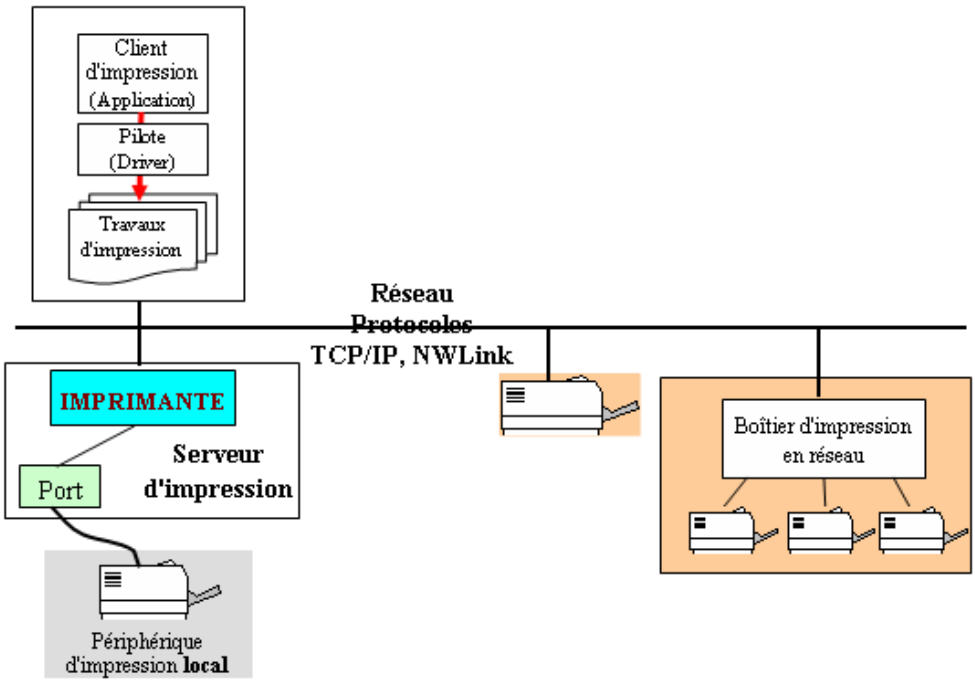
VII- GESTION DES IMPRESSIONS

7.1- Introduction

Windows 2003, comme ses prédécesseurs, est conçu pour une impression en réseau. Les applications tournant sur différentes plateformes envoient les travaux d'impression au serveur d'impression, puis aux périphériques d'impression. Avec un serveur d'impression Windows 2003, il est possible d'imprimer à partir d'ordinateurs tournant sur différents systèmes d'exploitation Microsoft : Dos, Windows 3.x, Windows 95 ou 98, Windows NT 3.51 ou 4, Windows 2003, mais aussi Macintosh, NetWare ou Unix.

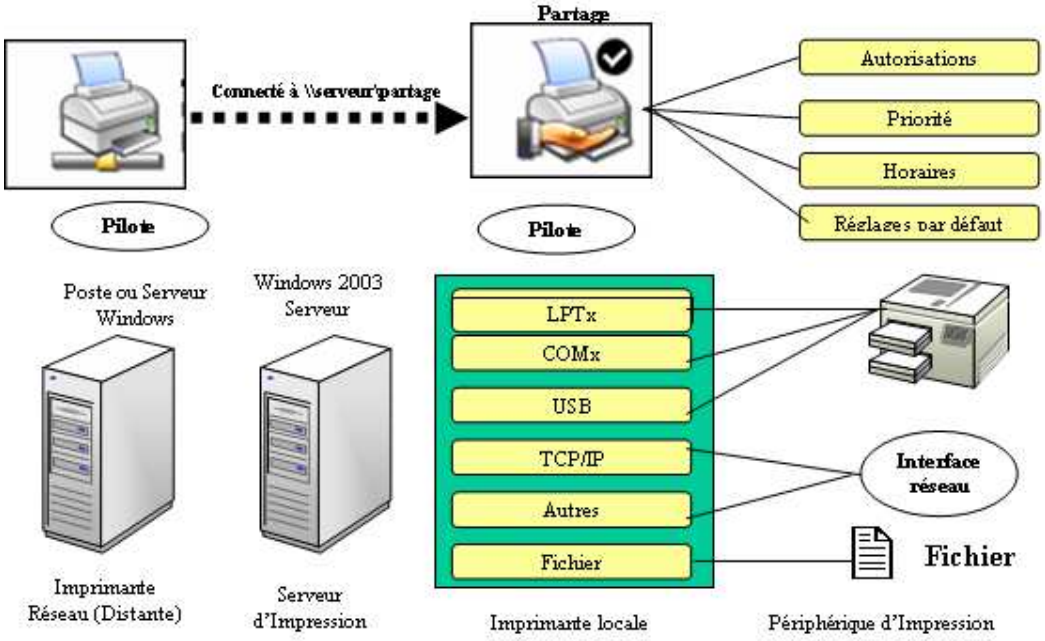
7.1.1- Terminologie

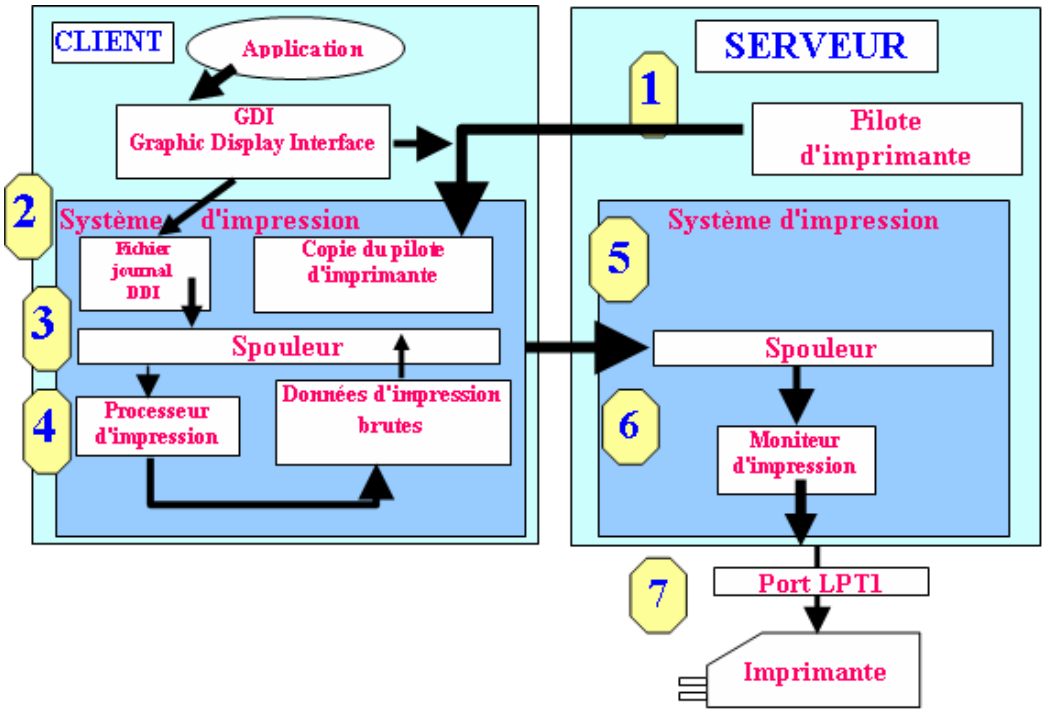
Avant d'aborder les services d'impression sous Windows 2003, il est important de bien comprendre la **terminologie** employée par Microsoft, en particulier à propos du terme imprimante.

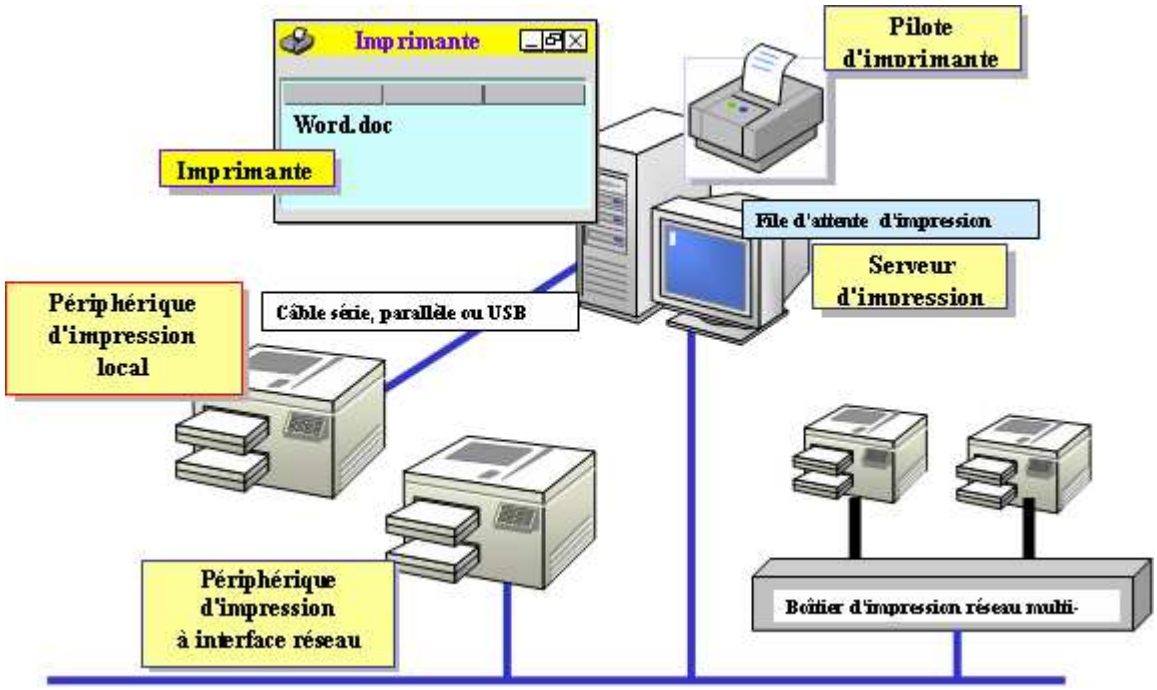


Terme	Signification au sens Microsoft
Imprimante	Comme on le voit sur le dessin ci-dessus, le terme imprimante au sens Microsoft, représente une interface logicielle entre le système d'exploitation et le périphérique d'impression. Quand vous installez une imprimante, vous installez tout le logiciel nécessaire pour assurer le lien entre l'application qui envoie les travaux d'impression, le système d'exploitation, le driver et le périphérique d'impression rattaché à l'imprimante.
Périphérique d'impression	Le périphérique d'impression est le dispositif matériel qui sert à imprimer. Ce peut être une imprimante matricielle, à jet d'encre ou laser, mais cela peut être tout autre dispositif, par exemple une table traçante. Périphériques d'impression locaux : ce sont les périphériques d'impression connectés à un port du serveur d'impression. Ce port peut être un port parallèle, série, infrarouge (IrDA), USB ou SCSI. Périphériques d'impression réseau : ce sont des périphériques d'impression reliés au réseau. Ce peut être une imprimante laser équipée d'une carte réseau (Ethernet ou Token–Ring) ou encore un boîtier adaptateur pour interfacer des imprimantes série ou parallèle au réseau. Dans tous les cas, ces périphériques réseau doivent avoir une adresse réseau (IP, IPX ou MAC).

Serveur d'impression	Un serveur d'impression Windows 2003 est un ordinateur Windows 2003 Server, sur lequel sont installées des imprimantes associées à des périphériques d'impression. Le serveur traite les travaux d'impression reçus des applications et les renvoie vers les périphériques d'impression concernés.
Pilote d'impression	Un pilote d'impression a pour rôle d'interfacer les informations à imprimer issues des applications et de les convertir pour quelles puissent être présentées à un type de périphérique d'impression particulier. Exemple : si vous voulez imprimer un document Word, l'application envoie toujours les mêmes informations à imprimer quelque soit le type de périphérique d'impression. C'est au pilote (driver) de convertir les informations Word en codes compréhensibles pour le périphérique d'impression. Ces informations ne peuvent évidemment être les mêmes pour une imprimante matricielle monochrome et pour une imprimante laser couleur, d'où des pilotes spécifiques pour chaque périphérique d'impression.







7.1.2- Configuration minimum

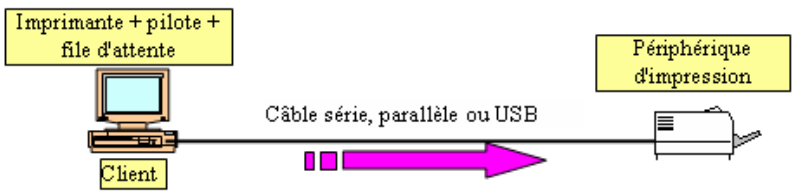
Pour imprimer en réseau Windows 2003, il faut au minimum :

- Un ordinateur pour jouer le rôle du serveur d'impression. Si il y a beaucoup de travaux d'impression et beaucoup de périphériques d'impression, il faudra peut-être un serveur d'impression dédié ou plusieurs.
- La mémoire RAM doit être importante pour pouvoir traiter plusieurs tâches d'impression de manière simultanée.
- Un espace disque important, sachant que les fichiers à imprimer sont mis dans des files d'attente d'impression qui sont stockées sur le disque dur du serveur d'impression. Un fichier dans la file d'attente, en sortie du pilote d'impression peut être beaucoup plus volumineux que le document généré par l'application.

7.2- Configuration des imprimantes

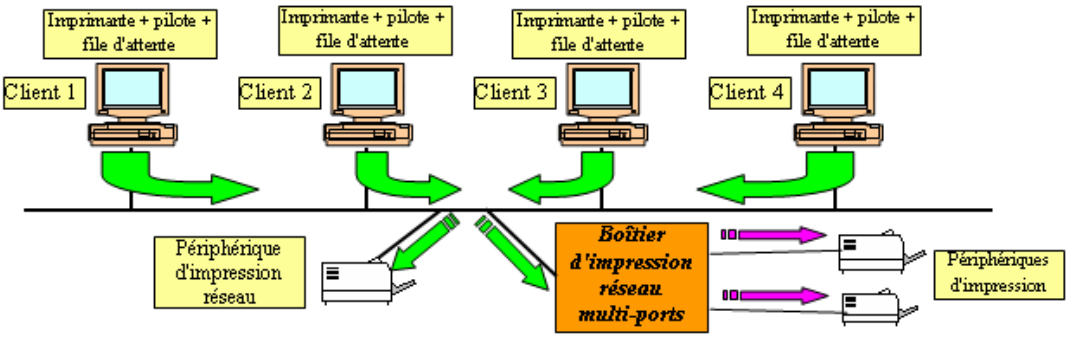
Windows 2003 autorise plusieurs configurations d'impression pour pouvoir s'adapter à chaque cas particulier.

7.2.1- Périphérique d'impression local



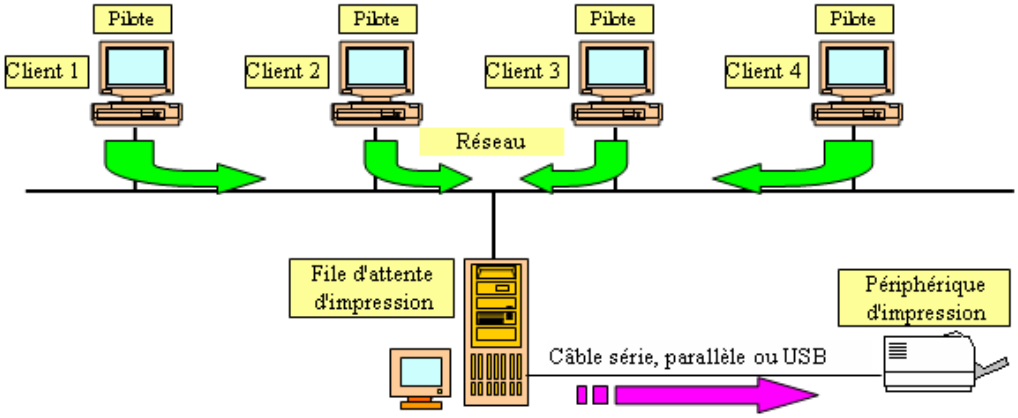
7.2.2- Périphérique d'impression en réseau, non distant

Il s'agit d'un réseau de type Workgroup. Ce type de réseau d'impression convient seulement pour de petits groupes de travail. Il risque d'y avoir des conflits entre les files d'attente de chaque ordinateur.



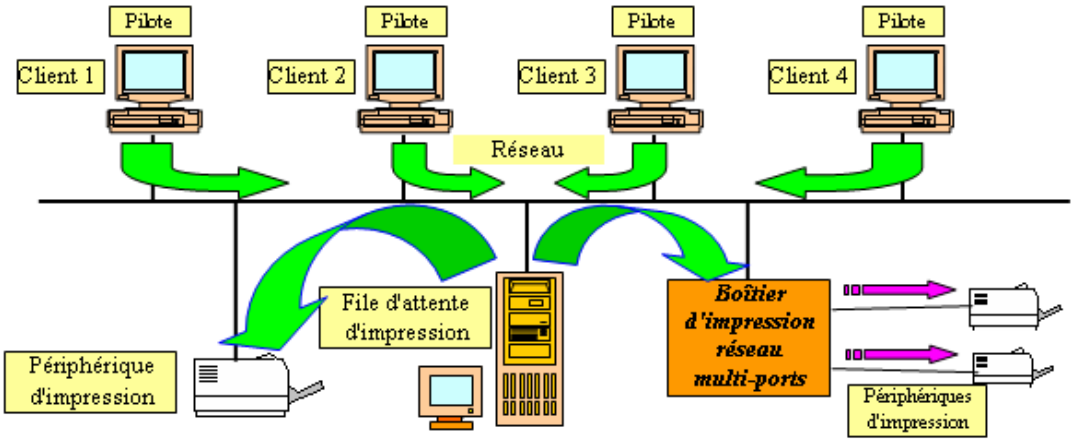
7.2.3- Périphérique d'impression réseau local, distant

Le périphérique est connecté localement au serveur d'impression. Il est distant par rapport aux clients. Les clients envoient les travaux d'impression par le réseau.



7.2.4- Périphériques d'impression réseau, distants

Les périphériques d'impression sont des périphériques munis de cartes réseau ou connectés à un boîtier d'impression. Les files d'attente d'impression sont à l'intérieur du serveur d'impression et gérées par ce dernier.



7.2.5- Assistant Ajout d'imprimante

Pour créer et partager des imprimantes, il faut utiliser l'outil assistant **Ajout d'imprimante** qui se trouve dans le menu **Démarrer**, **Paramètres**, **Imprimantes**.

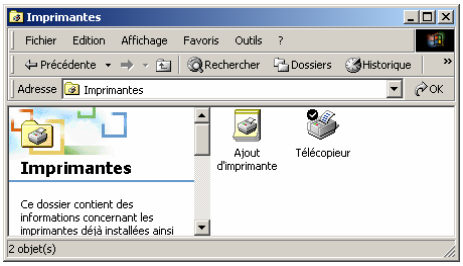
Dans le cas du serveur d'impression :

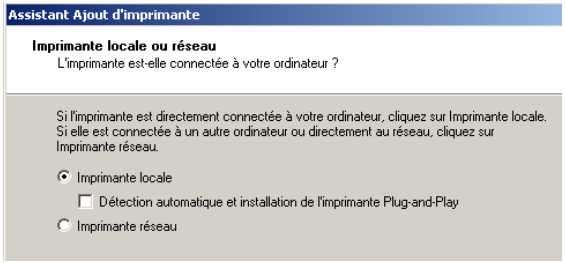
- **Créer une imprimante signifie :** installer le périphérique d'impression relié directement au serveur ou par l'intermédiaire du réseau. Configurer le logiciel d'imprimante contrôlant le périphérique d'impression.
- **Se connecter à une imprimante signifie** : se connecter au partage de l'imprimante qui a créé l'imprimante.

7.3- Configuration des imprimantes en réseau

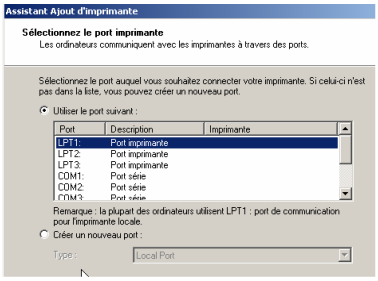
7.3.1- Installation d'un périphérique d'impression local

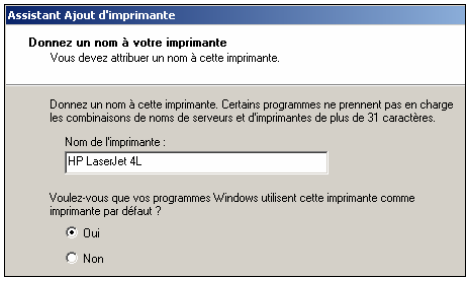
Pour installer un périphérique d'impression en local, il suffit d'ouvrir l'assistant **Ajout d'Imprimante**. Dans le premier panneau, cliquer sur **Suivant**. Dans le nouveau panneau, cliquer sur **Imprimante locale**. Si le périphérique d'impression est Plug and Play, cliquer sur **Suivant**.

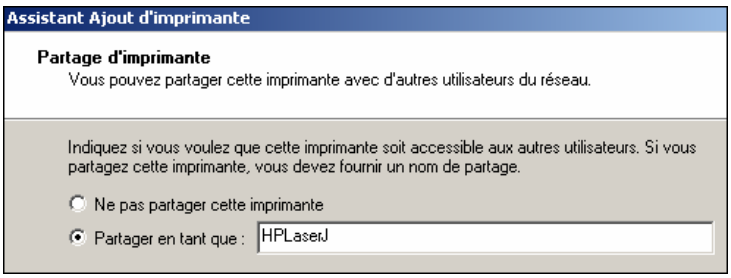




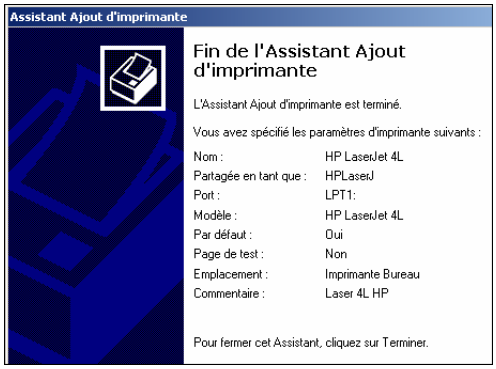
Sélectionnez le port matériel. Le nombre de périphériques pouvant être connectés directement sur l'ordinateur dépend du nombre de ports matériels **(série, parallèle ou USB)** présents sur l'ordinateur. Si le périphérique d'impression n'est pas PnP, ou si la case n'a pas été cochée, il faut choisir le type de périphérique d'impression manuellement.

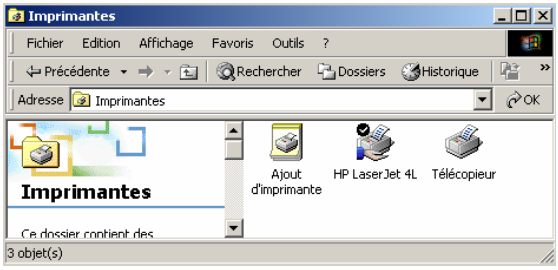






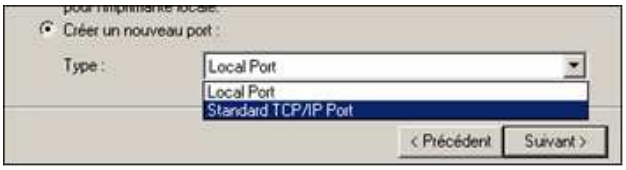
Dans le panneau suivant, donnez un nom au périphérique d'impression. L'imprimante peut être partagée ou non. L'assistant demande ensuite des informations sur l'emplacement et des commentaires, ceci est facultatif. Dans le panneau suivant, l'assistant propose l'impression d'une page de test. Le dernier panneau est le résumé des caractéristiques de l'imprimante.

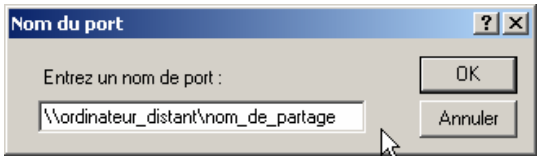




Ajout d'un nouveau port d'impression

Vous pouvez ajouter des ports d'impression supplémentaires. Cela peut être nécessaire si vous avez un périphérique d'impression à interface réseau ou spécifique. Dans ce cas vous devez ajouter le port correspondant à ce périphérique. Il est plus intéressant d'avoir un périphérique d'impression de ce type car il ne nécessite pas de serveur devant jouer le rôle de serveur d'impression. Le transfert de données sur le câble réseau est plus rapide que sur un câble de type parallèle. Par défaut W2003 Server prend en compte le Local Port ou LPR port. Vous pouvez toujours à l'aide d'**Ajout/suppression de programmes** ajouter des **Services d'Impressions Pour Mac ou Unix**. Le port Local Port permet de connecter un périphérique d'impression à un port parallèle, série ou à un fichier. Il vous permet aussi de rediriger les travaux d'impression vers un chemin UNC (\\ordinateur_distant\nom_de_partage) ou le port NULL.





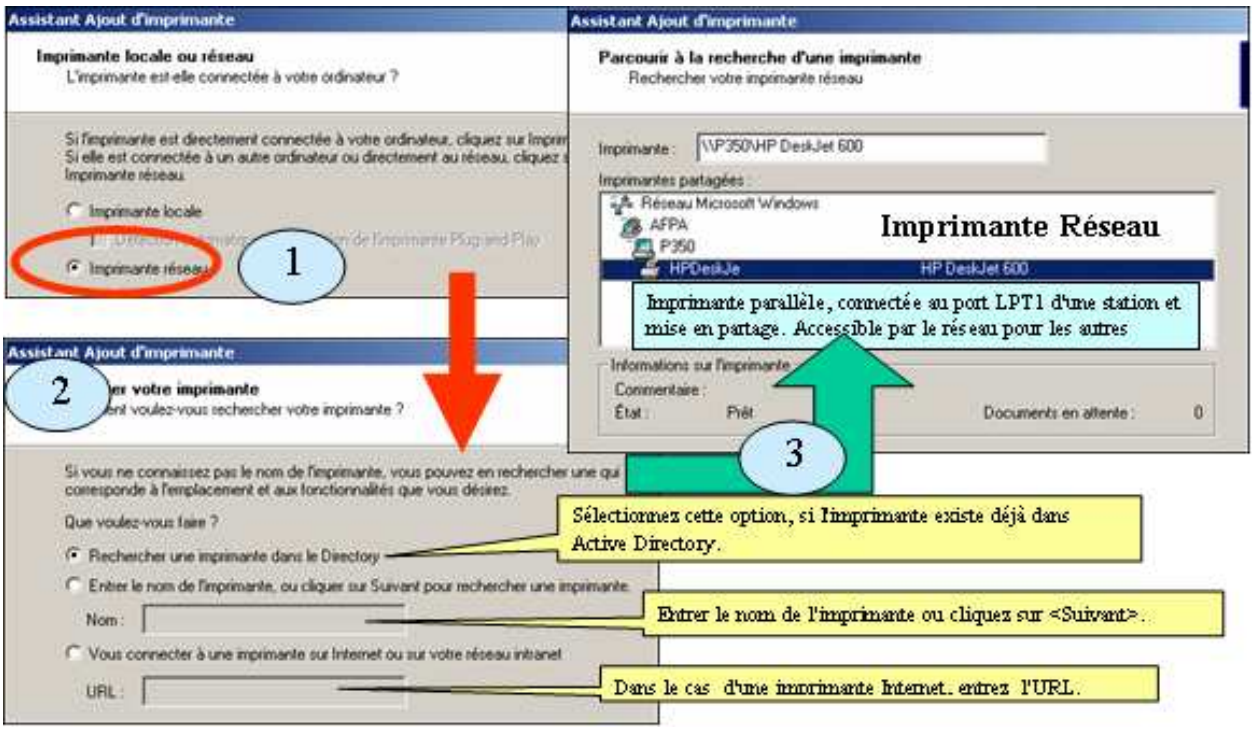
Le port standard TCP/IP vous permet de connecter des périphériques d'impression directement au réseau ou par l'intermédiaire d'un boîtier TCP/IP.

Panneau des paramètres d'une imprimante et visualisation dans la fenêtre **Imprimantes**.

7.3.2- Installation d'un périphérique d'impression en réseau

Dans les cas suivants, sur une station, il faut déclarer **Imprimante réseau** dans l'assistant **Ajout d'Imprimante**.

- Périphérique d'impression équipé d'une carte réseau et connecté sur ce dernier.
- Périphérique parallèle, série ou USB connecté au port d'un boîtier d'impression réseau connecté au réseau.
- Périphérique parallèle, série ou USB connecté à un port série, parallèle ou USB d'un serveur d'impression Windows 2003.



Configuration matérielle requise pour une imprimante réseau
Serveur d'impression exécutant

- L'un des systèmes d'exploitation de la famille Windows 2003, Windows 2000 Server ou Windows 2000 Professionnel avec au maximum 10 ordinateurs clients simultanés.
- Suffisamment de mémoire vive pour traiter les documents.
- Suffisamment d'espace disque sur le serveur d'impression pour stocker les documents.

Instructions à suivre pour installer une imprimante réseau

- Déterminez les besoins de votre entreprise en matière d'impression.
- Déterminez les besoins des utilisateurs de chaque service en termes d'impression.
- Déterminez le nombre de serveurs d'impression requis par votre réseau.
- Déterminez l'emplacement des périphériques d'impression.
- Déterminez la priorité des travaux d'impression.

7.3.3- Ajout d'une imprimante

Option	Description
Imprimante locale	Indique que vous ajoutez une imprimante à l'ordinateur qui est devant vous
Utiliser le port suivant	Port du serveur d'impression auquel vous avez connecté le périphérique d'impression
Fabricants et Imprimantes	Pilote d'impression approprié au périphérique d'impression local
Nom de l'imprimante	Nom qui identifie l'imprimante auprès des utilisateurs
Imprimante par défaut	Imprimante par défaut pour toutes les applications Windows
Partagé en tant que	Nom de partage dont les utilisateurs peuvent se servir pour établir une connexion à l'imprimante par l'intermédiaire du réseau
Emplacement et commentaires	Informations sur le périphérique d'impression
Voulez-vous imprimer une page de test ?	Vérifie que l'imprimante est installée correctement

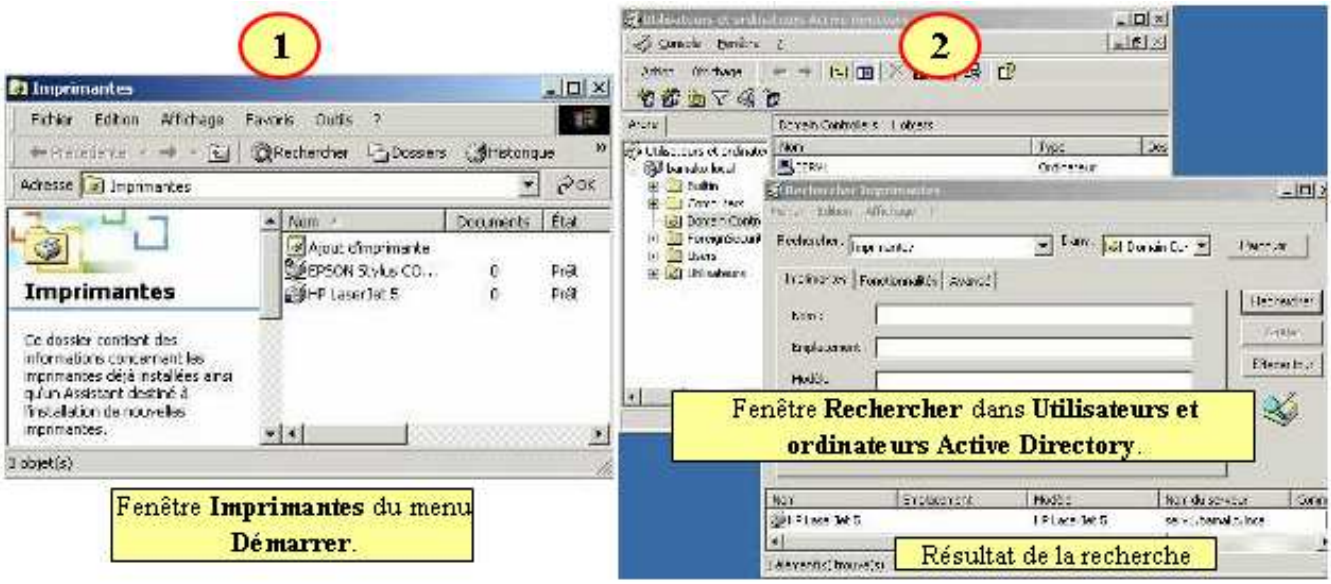
7.3.4- Partage d'une imprimante

Pour partager une imprimante, sur un serveur ou une station, il suffit de cliquer avec le bouton droit sur l'icône de l'imprimante à partager et de sélectionner **Partage** dans le menu contextuel.

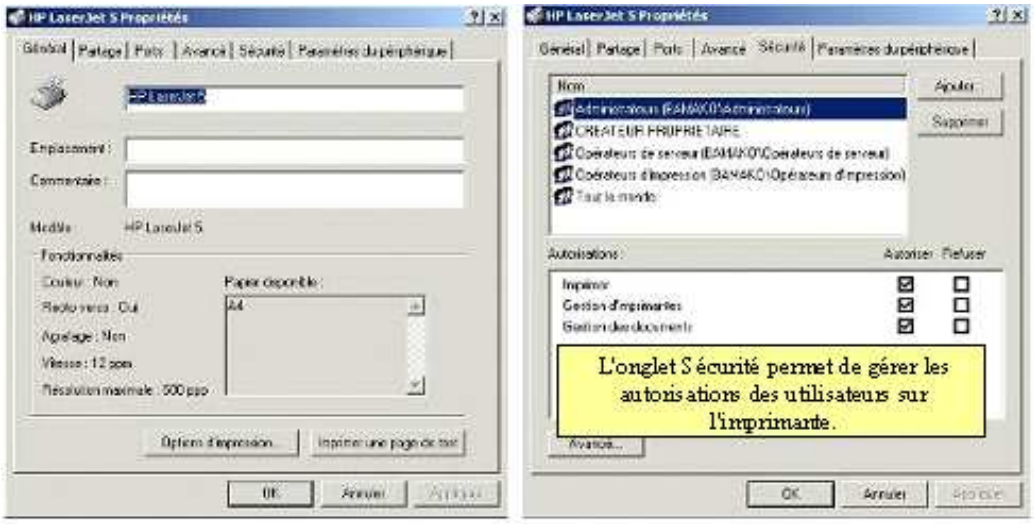
7.4- Administration des imprimantes réseau

7.4.1- Accès aux imprimantes

La gestion des imprimantes peut se faire à partir de **Imprimantes** dans le menu **Démarrer** (1) ou en utilisant l'option **Rechercher** dans **Utilisateurs et ordinateurs Active Directory** (2).



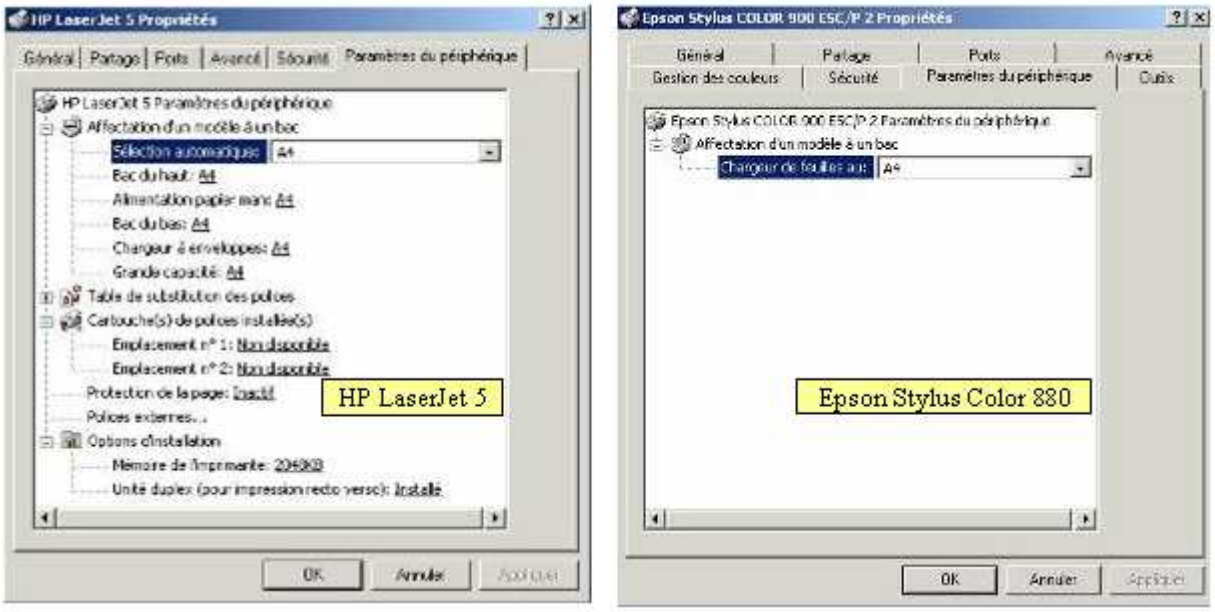
Dans la fenêtre **Imprimantes**, après avoir sélectionner l'imprimante, la boîte de dialogue **Propriétés** permet d'accéder aux caractéristiques de l'imprimante et de les **modifier**.
Vous pouvez définir le nom de l'emplacement et d'éventuels commentaires pour l'imprimante. Vous avez aussi la possibilité d'installer des pilotes supplémentaires. Vous pouvez aussi imprimer une page de test.



L'onglet **Sécurité** permet de définir les autorisations d'utilisation et de gestion des utilisateurs sur chaque imprimante. Il vous permet de désigner certains utilisateurs, qui ne sont pas Administrateurs, en tant que **Gestionnaire d'imprimante** ou **Gestionnaires de documents**. Par défaut le groupe **Tout le monde** est autorisé à se servir d'une imprimante.
N.B. : si vous refusez l'autorisation d'imprimer au groupe **Tout le monde**, aucun utilisateur ne pourra imprimer même si il fait partie d'un groupe autorisé à imprimer. Le refus prime sur l'autorisation.

7.4.2- Gestion des imprimantes

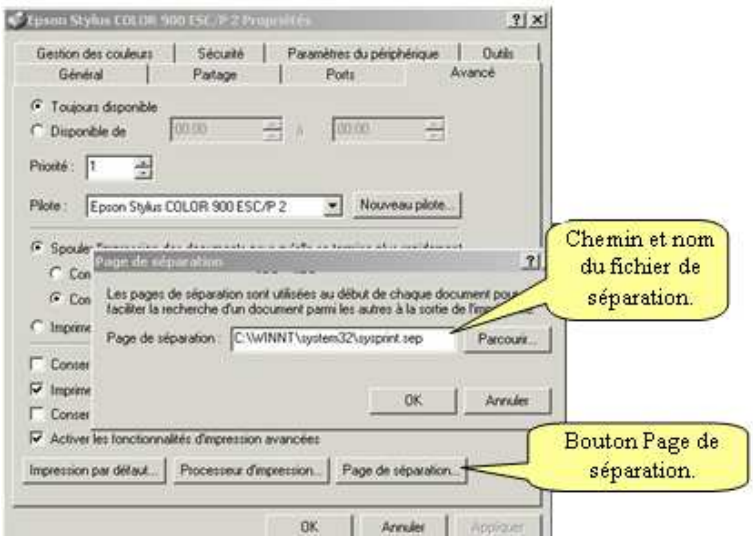
La gestion des imprimantes comporte l'attribution des formats de papier et le choix des bacs, les choix des cartouches additionnelles de polices et d'autres options, ainsi que la configuration de la page de séparation appelée aussi bannière.



Les options d'impression permettent de définir la position du document, l'ordre d'impression des pages, la source du papier, le nombre de pages à imprimer par feuille et des options avancées pour des paramètres propres à chaque imprimante.
La page de séparation ou bannière permet de séparer les documents et éventuellement permettre le changement de mode d'impression d'un document à l'autre.
Windows 2003 comprend quatre fichiers de page de séparation. Ils sont stockés dans le dossier **%systemroot%System32**. Le tableau ci-dessous résume le rôle de chacun.

Nom du fichier	Fonction
Pcl.sep	Permet de passer en mode d'impression PCL sur les périphériques d'impression HP et d'imprimer une page avant chaque document.
Pscript.sep	Permet de passer en mode d'impression PostScript sur les périphériques d'impression HP, mais ne permet pas d'imprimer une page avant chaque document
Sysprint.sep	Imprime une page avant chaque document. Compatible PostScript.
Sysprtj.sep	Pour les caractères Japonais.

Il est possible d'écrire ces propres fichiers **.sep** en consultant la documentation.
Pour choisir un fichier **.sep** particulier, ouvrir la fenêtre **Propriétés** d'une imprimante et sélectionner l'onglet **Avancé**, puis le bouton **Page de séparation**. Entrer ensuite le chemin du fichier de séparation.

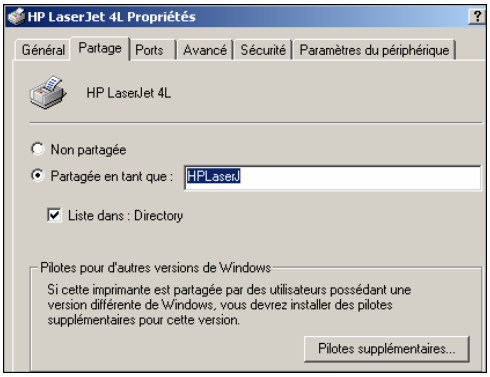


7.4.3- Propriétés d'une imprimante partagée

Le partage d'une imprimante permet de rendre disponible cette imprimante pour des clients voulant imprimer via le réseau en se connectant dessus.
Le nom de la zone **Partagée en tant que** est celui que verront les clients à travers le réseau.
Liste dans :

- Active Directory : permet de publier l'imprimante partagée dans Active Directory.
- Pilotes supplémentaires permet d'ajouter des pilotes supplémentaires pour d'autres clients tournant sous d'autres systèmes d'exploitation que W2003. Dans ce cas il y a un téléchargement automatique des pilotes nécessaires lors de la connexion à cette imprimante.

Le bon pilote est stocké dans un sous répertoire du répertoire partagé du serveur d'impression ➔ print$ (%systemroot%\system32\spool\drivers).



7.4.4- Configuration des ordinateurs clients

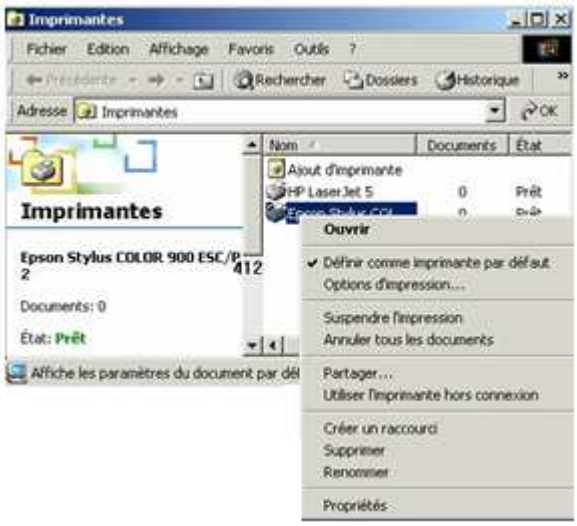
Les ordinateurs clients exécutant les systèmes d'exploitation suivants téléchargent automatiquement le pilote d'imprimante :

- Windows 95 ou Windows 98.
- Windows NT 4.0.

Les ordinateurs clients exécutant d'autres systèmes d'exploitation Microsoft nécessitent l'installation d'un pilote d'imprimante. Les ordinateurs clients exécutant des systèmes d'exploitation non Microsoft nécessitent l'installation des éléments suivants :

- Pilote d'imprimante sur l'ordinateur client.
- Service d'impression sur le serveur d'impression.

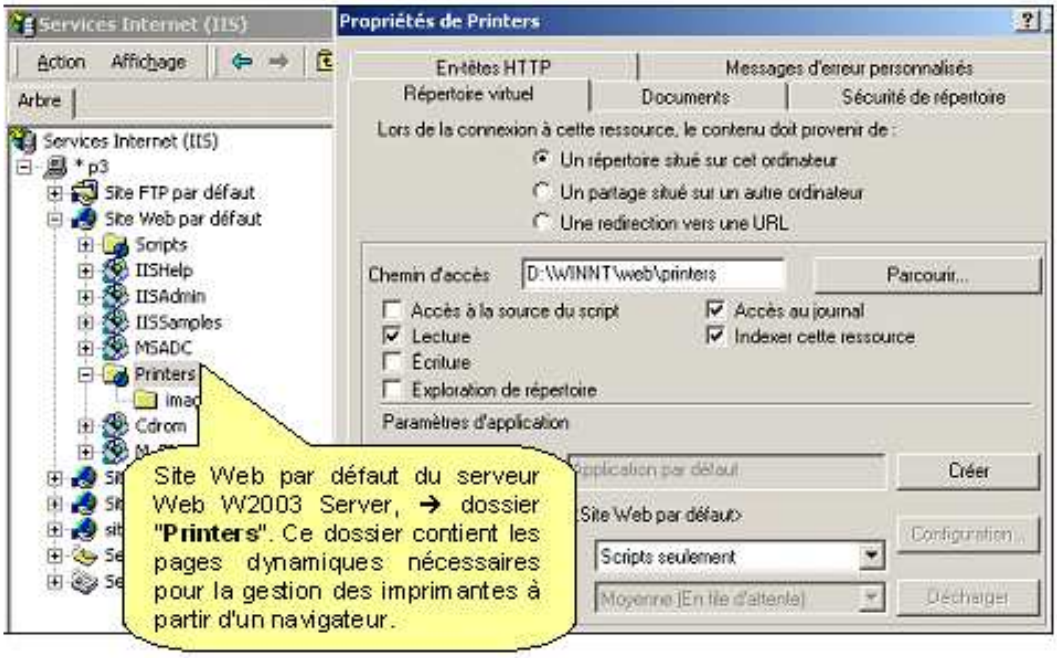
7.4.5- Menu contextuel d'une imprimante



En utilisant le menu contextuel, vous pouvez **suspendre** l'impression, la **reprendre** ou **annuler** tous les documents en attente d'impression.

7.4.6- Administration des imprimantes à partir du navigateur Web

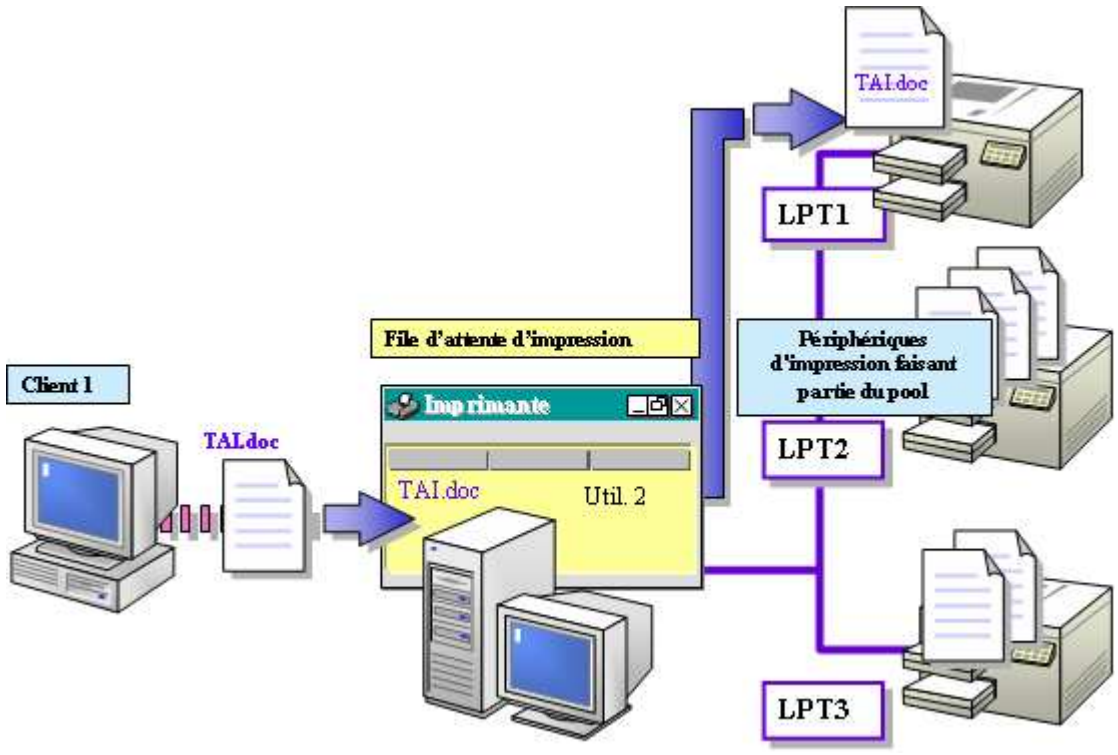
Les imprimantes déclarées sous Windows 2003 peuvent être gérées à partir d'un navigateur Web, même si ce navigateur fonctionne sur un ordinateur non Windows 2003. Pour qu'un serveur d'impression puisse prendre en charge la gestion Web, il faut que l'ordinateur Windows 2003 Server soit équipé d'un serveur IIS (Microsoft Internet Information).



Dans le navigateur Web, il suffit d'indiquer le chemin http://serveur_impression/printers. La page d'accueil Web est ouverte. Il suffit ensuite de cliquer sur le nom de l'imprimante. La page suivante affiche toutes les actions possibles sur l'imprimante. **Seules les imprimantes partagées apparaissent**.

7.4.7- Configuration de pool d'imprimante

Un **pool d'imprimante** est un ensemble de périphériques d'impression géré par la même imprimante. Il est souhaitable que les périphériques d'impression soient identiques. Un pool d'imprimante permet aux utilisateurs d'imprimer sans se préoccuper du périphérique d'impression disponible. Le pool sélectionne automatiquement le périphérique libre, ce qui permet d'améliorer les temps nécessaires pour imprimer les documents. Un pool d'imprimante peut comporter des périphériques locaux et à interface réseau. Un document est dirigé vers le premier périphérique d'impression disponible.



Pour créer un pool, déclarez une imprimante, puis dans l'onglet **Ports**, cochez la case **Activer le pool d'imprimante**. Ensuite, cochez les ports sur lesquels sont connectés les périphériqus d'impression

7.4.8- Priorités des imprimantes

Dans l'exemple précédent, trois périphériques sont connectés à la même imprimante. Mais il est aussi possible de connecter plusieurs imprimantes sur le même périphérique d'impression ou le même groupe de périphériques d'impression. On peut alors dans ce cas donner une **priorité** sur une imprimante par rapport à une autre. Déclarer plusieurs imprimantes sur le même port, puis dans les **Propriétés** de chaque imprimante, onglet **Avancé**, indiquer une priorité différente pour chaque imprimante.

7.5- Active Directory et les services d'impression

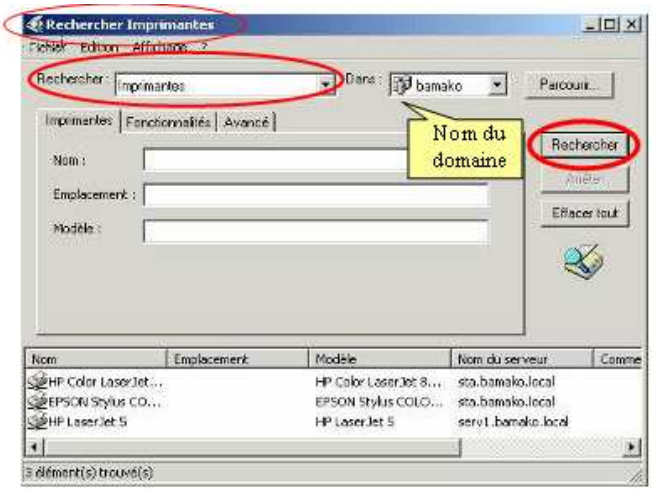
7.5.1- Présentation

Active Directory constitue une base de donnée hiérarchisée, distribuée et partagée sur les contrôleurs du domaine. Cette base de données contient les éléments d'impression comme les files d'attente. Par défaut, toute imprimante partagée est automatiquement publiée dans Active Directory.

7.5.2- Publication et prise en charge des imprimantes Windows NT

Lorsqu'une imprimante est partagée, elle est automatiquement publiée dans Active Directory. Vous pouvez enlever cette publication en décochant la case **Liste dans : Active Directory** de l'onglet **Partage** des **Propriétés** de l'imprimante.

La recherche des imprimantes dans Active Directory se fait en allant dans le composant enfichable **Utilisateurs et ordinateurs Active Directory**, puis dans le menu **Action**, **Rechercher**. Dans la fenêtre qui s'ouvre, sélectionner **Rechercher : Imprimantes**, puis cliquer sur le bouton **Rechercher**. Toutes les imprimantes du domaine, déclarées dans Active Directory apparaissent avec leur emplacement.



7.6- Connexion aux imprimantes réseau Windows 2003

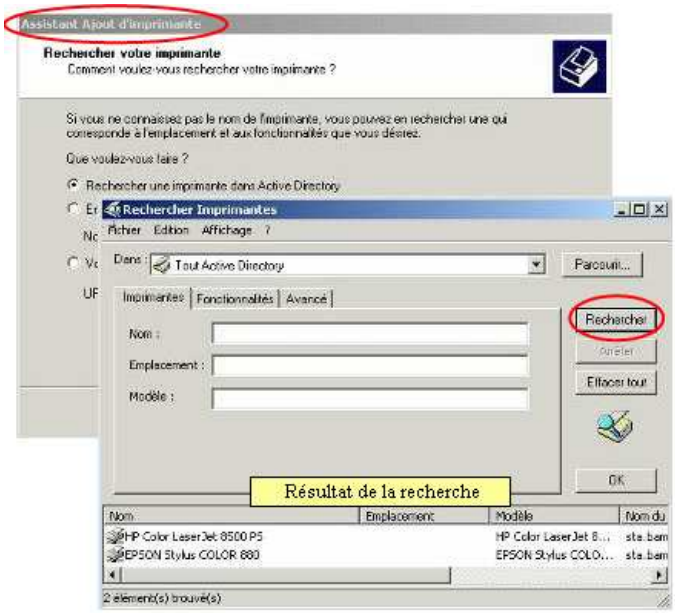
Dès qu'un serveur d'impression a été installé et que des imprimantes ont été partagées, il devient possible à partir de n'importe quelle station Windows de se connecter à une ou plusieurs de ces imprimantes.

7.6.1- Connexion en utilisant l'assistant Ajout d'imprimante

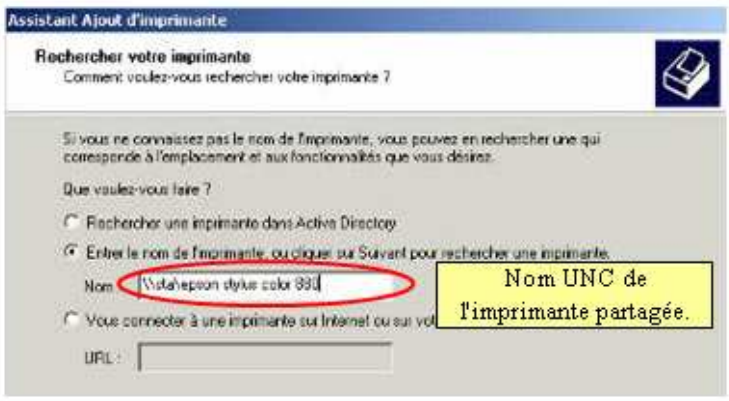
Clients Windows 2003

Pour ces clients la connexion se réalise avec l'assistant **Ajout d'imprimante** de plusieurs manières :

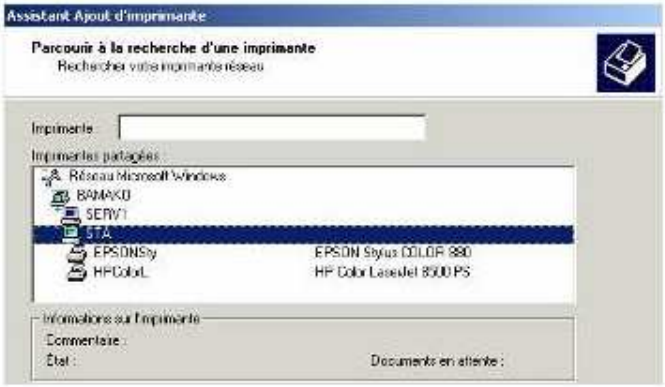
- Rechercher une imprimante dans Active Directory : dans la page **Rechercher votre imprimante** de l'assistant, sélectionner **Rechercher une imprimante dans Active Directory**. Dans la fenêtre suivante, l'onglet **Imprimantes** étant sélectionné, lancer la recherche en cliquant sur le bouton **Rechercher**.



- Utilisation du nom de convention universelle UNC : toujours dans la fenêtre **Rechercher votre imprimante** de l'assistant Ajout d'imprimante, taper le nom UNC de cette imprimante sous la forme **\\serveur_d'impression\partage**.



- Utilisation du **Voisinage réseau** : dans la page **Rechercher votre imprimante**, sélectionner **Entrer le nom de l'imprimante…** et cliquer sur **Suivant**. La Page **Parcourir…** s'ouvre. Dans la case **Imprimantes partagées**, vous pouvez entreprendre une recherche manuelle de l'imprimante à connecter.



Clients Windows 95, 98 et NT
Vous pouvez utiliser l'assistant **Ajout d'imprimante** ou entrer le nom UNC ou vous servir de l'option **Parcourir**.

Client Windows 3.11
Vous ne pouvez qu'utiliser la commande :
net use lptx: \\serveur_impression\partage
où **x** est un numéro de port LPT. La procédure de chargement automatique du pilote de l'imprimante n'est pas automatique. Il faut la faire manuellement.

VIII- STRATEGIES DE GROUPE

8.1- Définitions

8.1.1- Qu'est-ce qu'une stratégie de groupe

Ensemble de paramètres appartenant à l'un des 3 groupes suivant :

- Utilisateurs.
- Ordinateurs.
- Modèle d'administration.

La stratégie de groupe permet de gérer les paramètres utilisateur et ordinateur de votre réseau :

- Paramètres du Bureau.
- Paramètres Windows.
- Paramètres Logiciels.
- Paramètres de Sécurité.

8.1.2- Stratégie de groupe

Les stratégies de groupe sont des ensembles de paramètres de configuration des utilisateurs et des ordinateurs qui peuvent être appliqués à :

- Un site.
- Un domaine.
- Une Unité d'Organisation (UO).

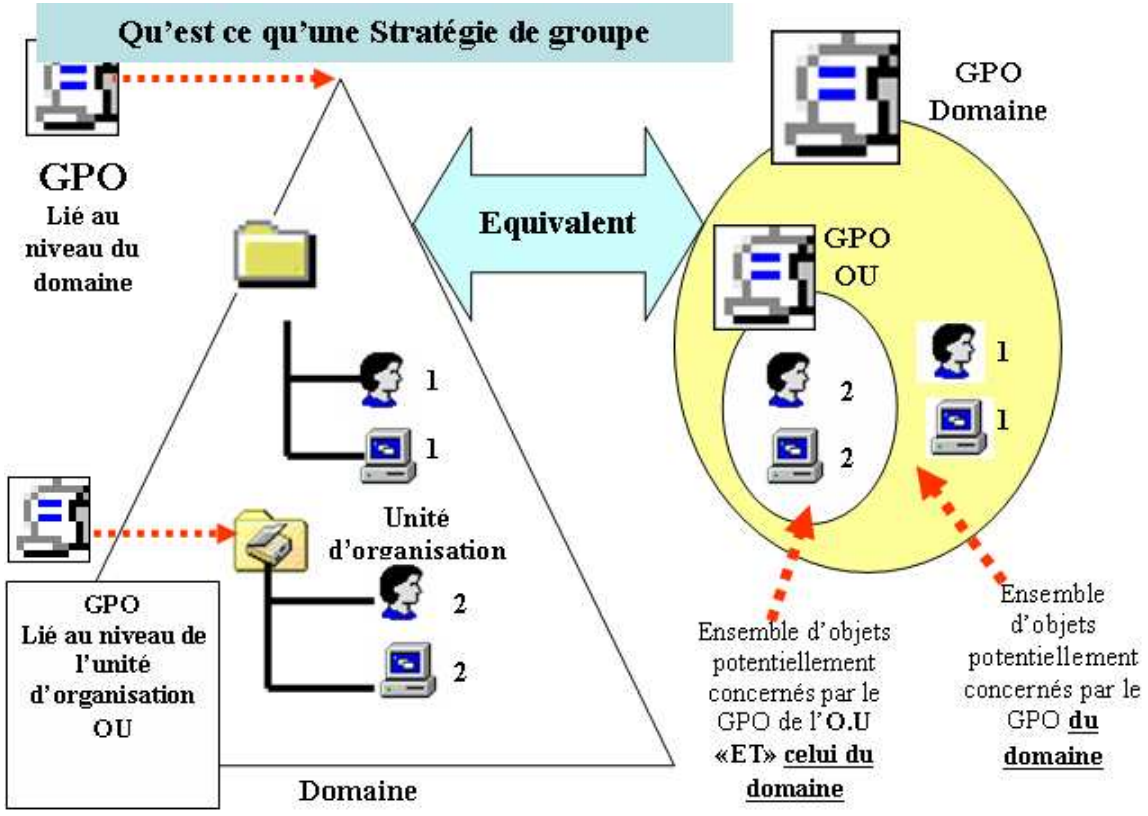
Elles s'appliquent à tous les objets réseaux du conteneur où elle est appliquée. Il existe la possibilité de lier le même GPO à plusieurs conteneurs et lier plusieurs GPO à un même conteneur.
Il existe différentes options de stratégies qui concernent :

- Le Registre.
- Les paramètres de sécurité.
- La gestion des applications.
- Les scripts.
- La mise sous et hors tension de l'ordinateur.
- L'ouverture et la fermeture des sessions.
- La redirection des dossiers.

Windows 2003 Server comporte des centaines de paramètres de stratégies de groupe configurables. Appliquer des stratégies de groupes permet de gagner du temps de gestion et par là même, réduire les coûts d'administration (TCO = Total Cost of Ownership).

Une stratégie de groupe permet par exemple de :

- Mettre en œuvre de modèles d'administration.
- Appliquer des stratégies de compte et de mot de passe.
- Restreindre le bureau des utilisateurs.
- Mettre en ouvre des audits.
- Changer les droits des utilisateurs.
- Exécuter des scripts, (ouverture de session, fermeture de session, démarrage et arrêt de machine
- Paramétrer la sécurité.
- Déployer et mettre en œuvre des applications.
- Paramétrer Internet Explorer (type de connexion, paramètres du proxy...).



C'est un Objet Active Directory qui s'applique (lié) au niveau d'un site, d'un domaine, des unités d'organisation, et à tous les objets réseaux du conteneur.
Possibilité de lier le même GPO à plusieurs conteneurs et lier plusieurs GPO à un même conteneur.
Par défaut Active directory implémente deux objets de stratégie :

- Default Domain Policy lié au niveau domaine dont les paramètres définis sous cette stratégie s'appliquent pratiquement à tous les utilisateurs et ordinateurs du domaine.
- Default Domain Controlers Policy lié au niveau de l'OU Domain Controlers (paramètres concernent les contrôleurs de domaines).

8.1.3- Objets de stratégie de groupe

Réduire le TCO (Total Cost of Ownership), coût total de possession

- Coût lié à l'administration de réseaux d'ordinateurs personnels distribués.
- Résoudre les éventuelles baisses de productivité.

Les stratégies de groupe sont des éléments représentés comme des objets d'Active Directory.
Pour appliquer une stratégie de groupe sur un site, un domaine ou une UO, il faut créer un ou plusieurs **Objets de stratégie de groupe** (**GPO** : Group Policy Objects). C'est un ensemble de paramètres qui peut être appliqué pour une stratégie de groupe. Ce GPO peut être réutilisé afin d'être appliqué sur d'autres objets d'Active Directory.

GPO local
Chaque station Windows 2003 possède un seul GPO qui est appelé GPO local (stocké sur chaque ordinateur local, valable dans un environnement non connecté)

GPO non locaux
Les GPO non locaux sont des GPO qui sont stockés sur un serveur Windows 2003 dans Active Directory. Les GPO non locaux s'appliquent aux sites, aux domaines et aux UO contenus dans l'annuaire d'Active Directory.

Priorité des GPO non locaux

Si une station contenant un GPO local est connecté en réseau à un serveur Windows 2003 contenant des GPO qui s'appliquent à la station, les GPO non locaux (ceux contenus dans le serveur) sont prioritaires au GPO contenu dans la station.

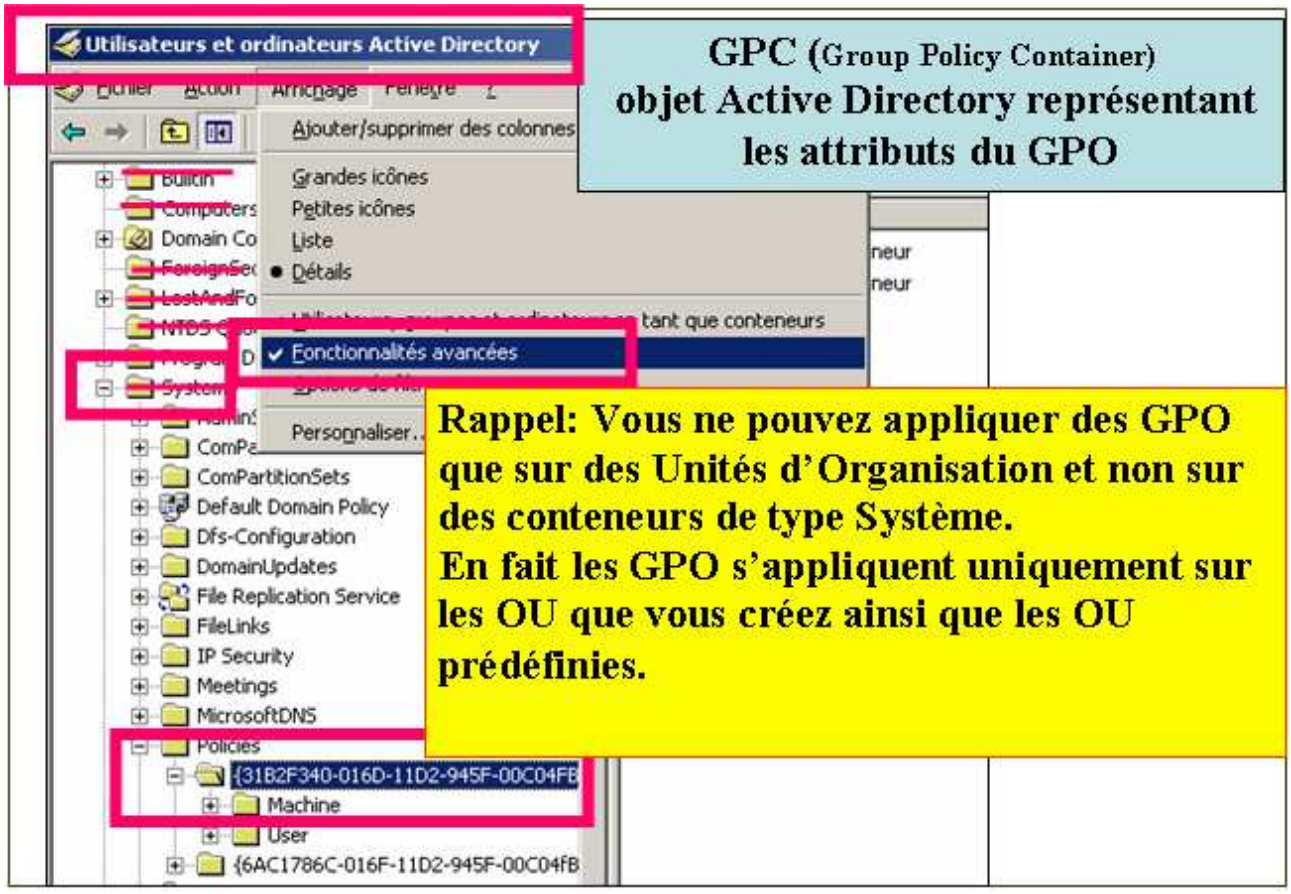
La même GPO peut être liée à plusieurs conteneurs et plusieurs GPO peuvent être liées au même conteneur. Une stratégie de groupe est un objet qui est référencé dans Active Directory et dans le dossier Sysvol. Active Directory va référencer le numéro de version de la stratégie dans le sous container Policies du container System.

Stratégie de groupe GPC (Group Policy Conteneur)

GPC est un objet d'Active Directory contenant les attributs des objets GPO, il inclut des sous conteneurs pour les informations relatives aux ordinateurs, ainsi qu'aux utilisateurs.

Il contient :

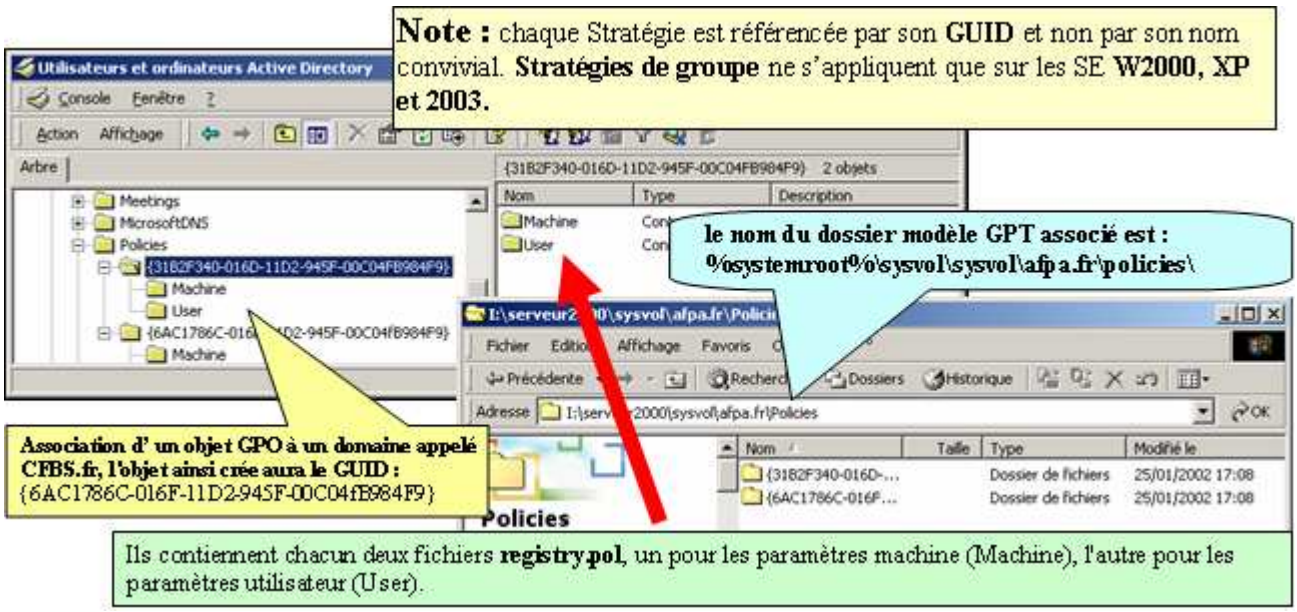
- Les informations de numéro de version pour garantir la synchronisation des informations du GPC et du GPT.
- Les informations d'état (objet activé ou non).
- La liste des extensions de la console **Stratégie de groupe** utilisées dans l'objet GPO.
- Il est possible de trouver ces informations en passant par la console **Utilisateurs et ordinateurs Active Directory**. Dans le menu **Affichage**, cliquer sur **Fonctionnalités avancées**, le dossier **System** apparaît.
- Développer le répertoire **Policies**.



Stratégie de groupe GPT (Group Policy Template)

Un GPT est une hiérarchie de dossiers stockés dans le répertoire sysvol. Il contient toutes les informations applicables à une GPO (stratégie de groupe).

A la création d'un objet GPO, W2003 crée en même temps un GPT correspondant. Le nom de ce modèle est son GUID (GUID, Globaly Unique IDentifier) qui est le **N° d'identificateur universel unique.**



Les paramètres de stratégies de groupes peuvent être définis au niveau ordinateur et au niveau utilisateur. Des fichiers registry.pol sont créés dans les sous-dossiers Machine et User si des paramètres ordinateur ou utilisateur sont définis.

8.2- Démarche pour la création et la gestion de stratégie de groupe

Il existe trois catégories de GPO :

- **La stratégie unique :** les GPO créés ne porte que sur un seul type de paramètres de stratégie de groupe. Ex : seul les paramètres de sécurité sont concernés.
- **La stratégie multiple :** les GPO créés influent sur plusieurs types de paramètres de stratégie de groupe. Ex : paramètres de sécurité et de script.
- **La stratégie dédiée :** les GPO créés portent sur les stratégies de groupe de configuration, soit de l'ordinateur, soit de l'utilisateur.

1	**Création d'un ou plusieurs GPO** pour un site, un domaine ou une UO dans Active Directory.
2	**Création d'une console** pour gérer les GPO.
3	Indiquer les **utilisateurs qui peuvent administrer** les GPO par l'intermédiaire des consoles.
4	**Définir la valeur des paramètres** dans chaque GPO.
5	**Désactiver les paramètres non utilisés** (pour gagner en vitesse d'exécution).
6	Indiquer les éventuelles **exceptions** des traitements des GPO.
7	**Filtrage** de l'étendue du GPO.
8	**Application** éventuelle du **GPO** à d'autres **Objets** dans Active Directory.

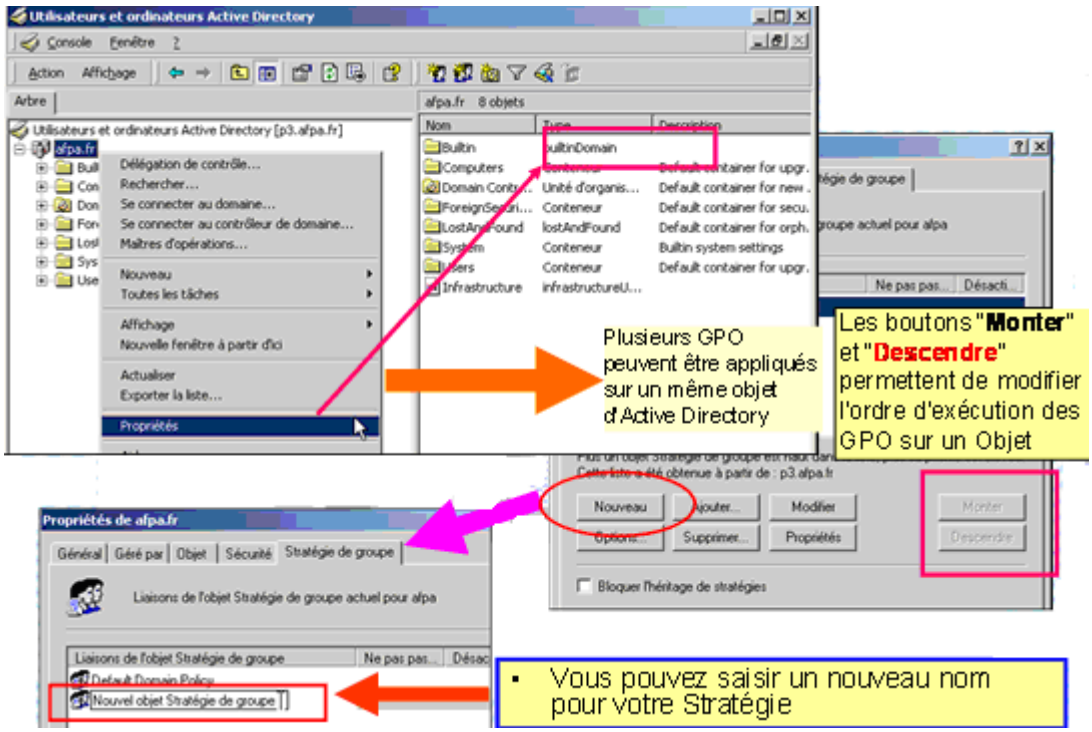
Pour créer et gérer des stratégies de groupes, il faut suivre les étapes ci-dessus.

8.2.1- Création de Stratégies de groupes

Pour appliquer une stratégie de groupe sur un site, il faut utiliser l'outil **Sites et services Active Directory** dans les **Outils d'administration**. Pour appliquer une stratégie sur un domaine ou une UO, il faut utiliser l'outil **Utilisateurs et ordinateurs Active Directory**.
Dans un de ces outils, sélectionnez le site, le domaine ou l'UO sur lequel il faut appliquer la stratégie. Puis ouvrez les **Propriétés** de l'objet et l'onglet **Stratégie de groupe**.
Il est alors possible de créer un ou plusieurs GPO qui s'appliqueront à l'objet d'Active Directory sélectionné.
Dans l'exemple ci-dessous, 2 GPO sont créés pour être appliqués sur l'UO **Marketing**. La console **Utilisateurs et ordinateurs Active Directory** est ouverte, l'UO **Marketing** sélectionnée et l'onglet **Stratégie de groupe** des **Propriétés** est sélectionné.
Avec Active Directory, deux GPO sont automatiquement créés à l'installation et proposés par défaut :

- **Default Domain Controllers Policy :**
  - Positionné sur le conteneur dans lequel se trouvent tous les contrôleurs de domaine (Domain Controllers).
  - Gère toute la stratégie des contrôleurs de domaine.
- **Default Domain Policy :**
  - Positionné sur l'objet représentant le domaine.
  - Gère la stratégie appliquée à tout le domaine.
  - Ne peut pas être supprimé, par aucun administrateur, car il contient des paramètres importants et obligatoires pour le domaine.

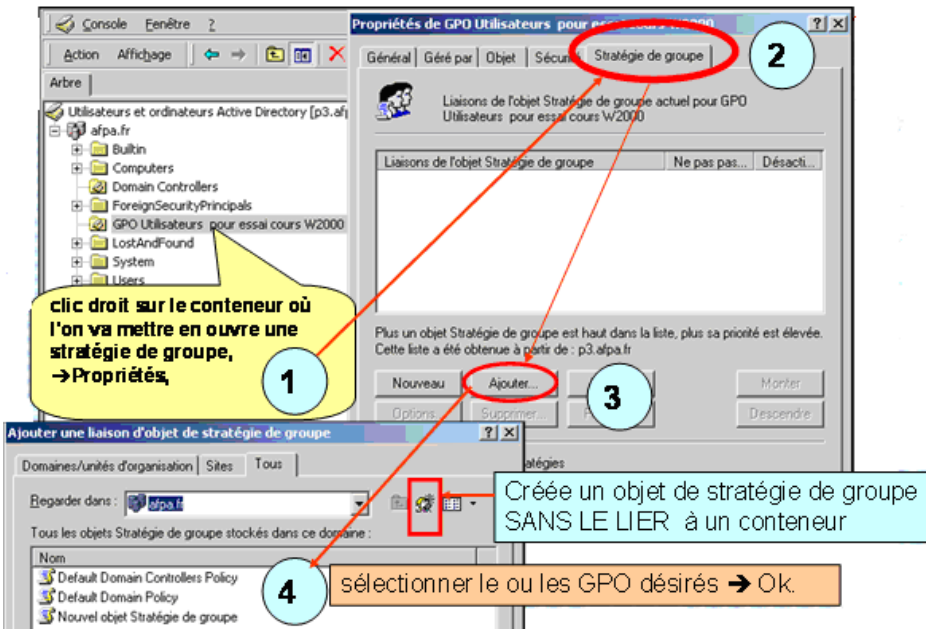
Les stratégies de groupes peuvent être créées sur un conteneur au niveau du domaine ou d'une OU.
Un GPO ne peut être crée que sur une OU que vous créez vous-même ou une déjà créée par les contrôleurs de domaine.



Le bouton **Nouveau** est utilisé pour créer un nouveau GPO. Le bouton **Ajouter** permet d'utiliser des GPO déjà créés.

8.2.2- Ajouter une stratégie de Groupe

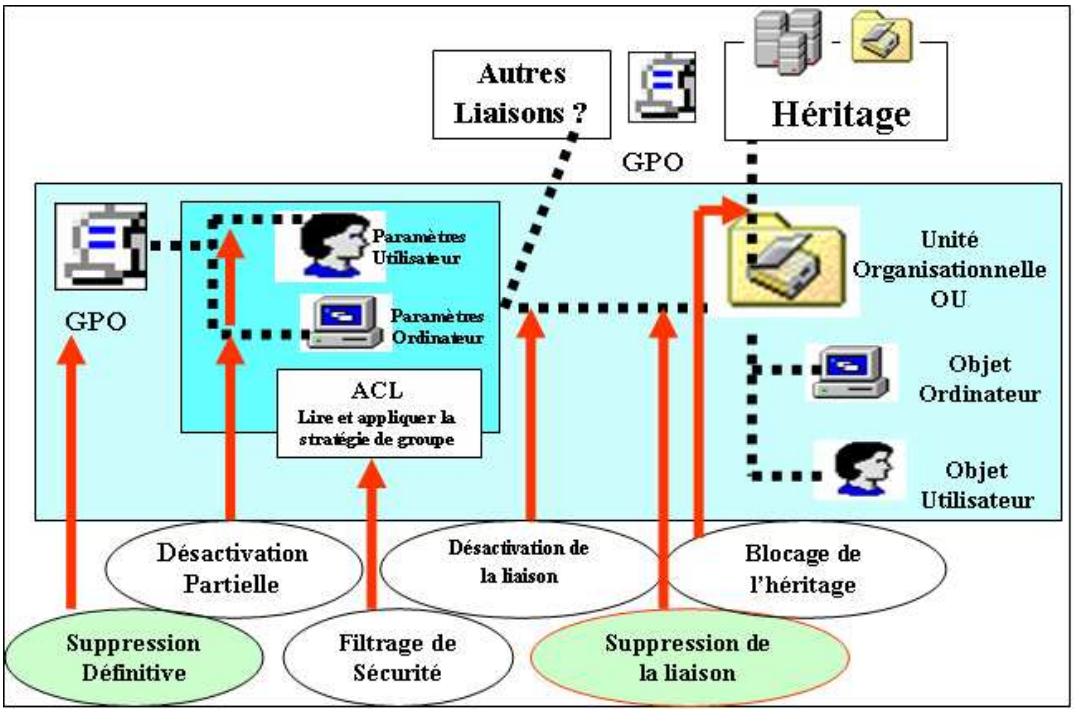
Il vous suffit de sélectionner le conteneur (1) (OU par exemple), puis sélectionnez à partir d'un clic droit **Propriétés**, puis l'onglet **Stratégie de groupe** (2), puis cliquez sur le bouton **Ajouter** (3). Sélectionnez (4) votre stratégie de groupe dans la liste qui s'affiche. Sélectionnez auparavant l'onglet **Tous**, car cela vous permet de visualiser tous les objets de stratégie de groupe disponible. Validez par **OK**.



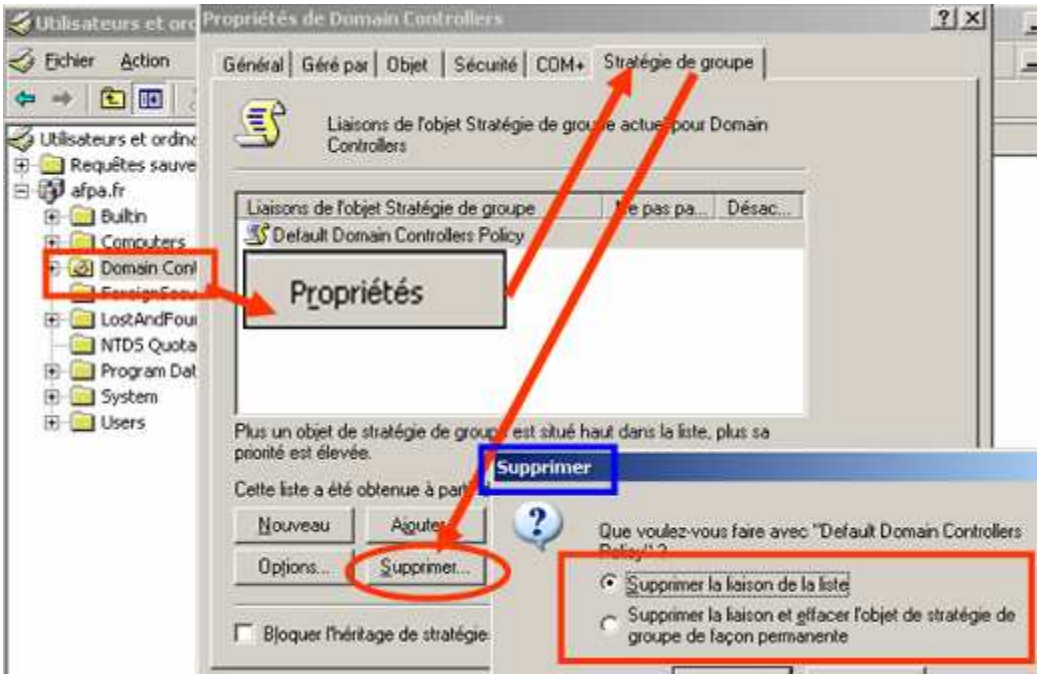
8.2.3- Supprimer une stratégie de groupe

Vous pouvez très simplement supprimer une stratégie de groupe afin qu'elle ne soit plus appliquée à un conteneur. Vous verrez que vous avez deux possibilités :

- Soit en supprimant le lien vers cette stratégie.
- Soit en supprimant complètement cette stratégie.

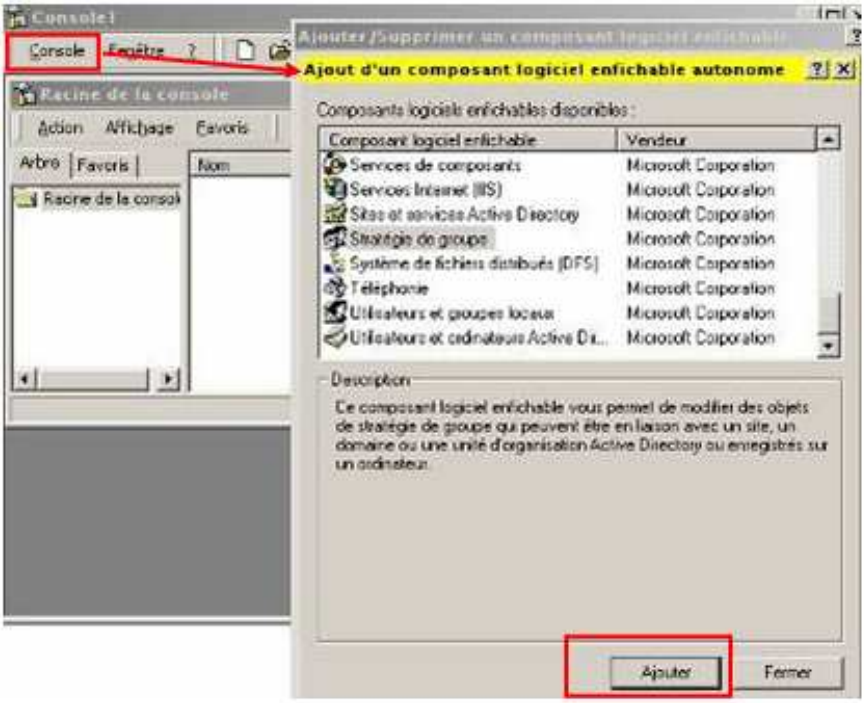


Sélectionnez le conteneur, puis clic droit avec **Propriétés**, sélectionnez l'onglet **Stratégie de groupe**, puis cliquez sur le bouton **Supprimer**. Vous avez le choix de supprimer la liaison de la liste ou bien de supprimer totalement le lien et la stratégie entièrement.
NOTA : auparavant assurez-vous, si vous réalisez une suppression totale d'une stratégie, qu'elle ne soit pas liée avec d'autres conteneurs.



8.2.4- Création d'un console pour gérer des GPO

Si l'on veut gérer les GPO existants, il faut créer une console appropriée. Tapez **mmc**, dans la commande **Exécuter** de Windows 2003. Une console vide s'ouvre. Il faut alors ajouter le composant logiciel enfichable **Stratégie de groupe** à partir du menu **Console**.

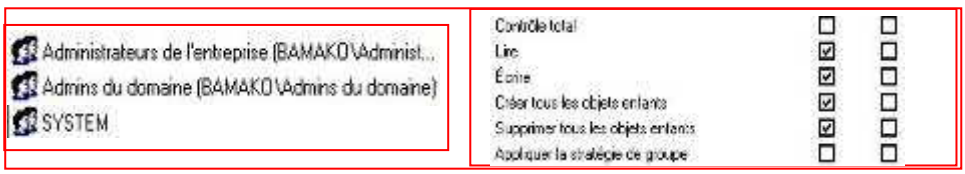


Création de la console en ajoutant le composant **Stratégie de Groupe**. Il faut ensuite définir les éléments. Cliquez sur le bouton **Ajouter** pour faire apparaître la fenêtre **Sélection des Objets de stratégie de groupe**. Cliquez sur le bouton **Parcourir** et dans la fenêtre **Rechercher un objet…**, sélectionner l'onglet **Tous**. Sélectionnez le premier GPO à installer dans la console, puis faire **OK**. Recommencez si il y a plusieurs GPO à gérer dans la même console.

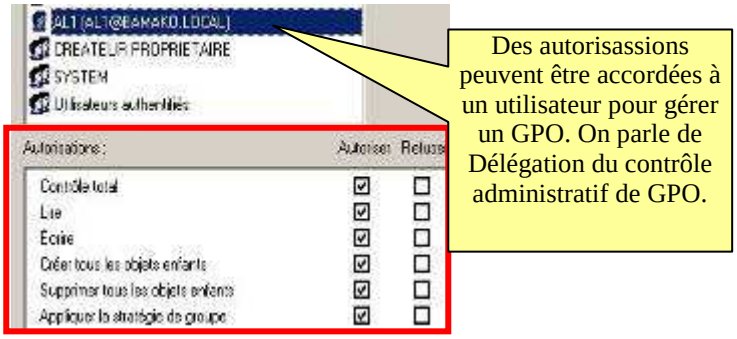
Appuyer sur **Terminer**. Enregistrer le nom de la console avec **Enregistrer sous…**. La console apparaît avec les GPO sélectionnés.

8.2.5- Délégation du contrôle des GPO

L'administrateur peut désigner des utilisateurs pour gérer les GPO par délégation. Certains groupes ont, par défaut, des **autorisations** sur les GPO.



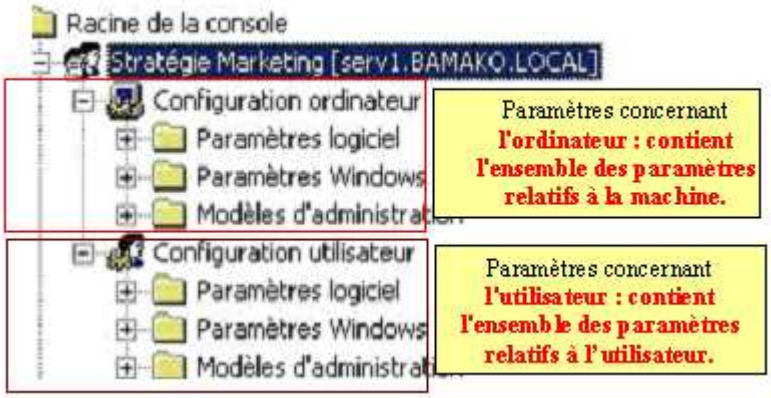
Mais vous pouvez dans l'onglet **Sécurité** des **Propriétés** d'un GPO, donner des autorisations à un utilisateur ou à un groupe particulier.



8.2.6- Définir les paramètres de chaque GPO

Pour chaque GPO, il existe deux classes de configuration :

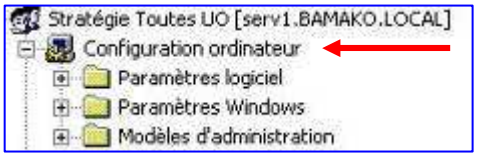
- La configuration concernant l'ordinateur.
- La configuration concernant l'utilisateur.



➡ Paramètres concernant l'ordinateur

Les paramètres concernant l'ordinateur pour un GPO donné se divise en 3 sous-groupes :

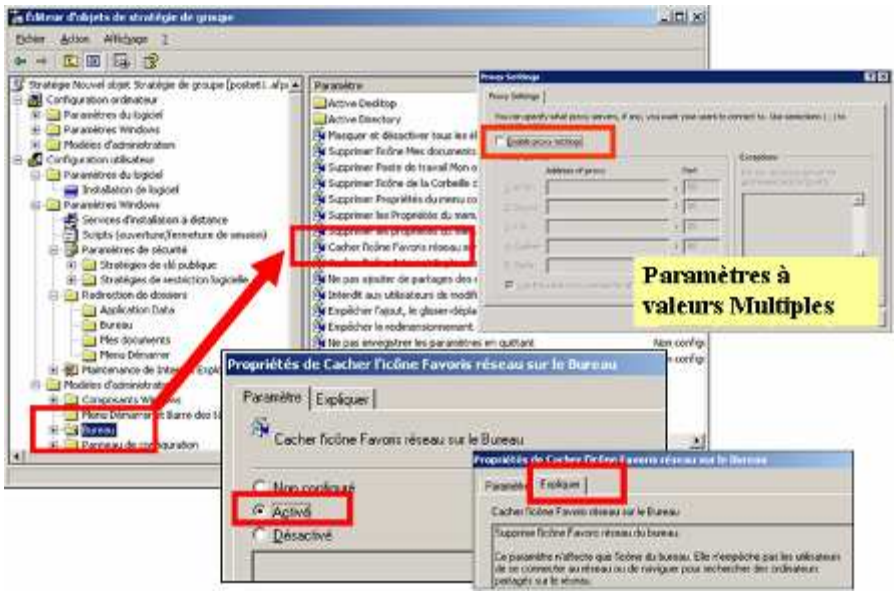
- Les paramètres logiciels.
- Les paramètres Windows.
- Les modèles d'administration.



Groupes de paramètres Ordinateur.

Paramètres logiciels

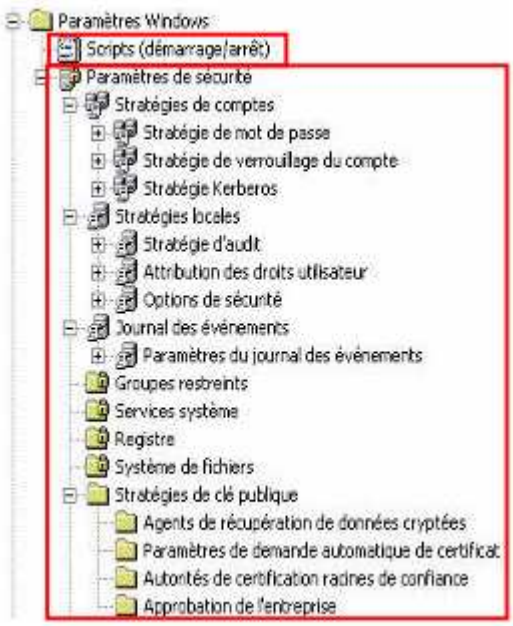
Le dossier **Paramètres logiciel** ne contient par défaut que les paramètres **Installation du logiciel**. Ces paramètres permettent de définir pour un ordinateur donné le mode d'installation et de gestion des applications. Il est possible de gérer les applications en mode **attribué** pour que les ordinateurs disposent de celles-ci. Il est possible de gérer les applications en mode **publié** pour que les utilisateurs puissent disposer de celles-ci.



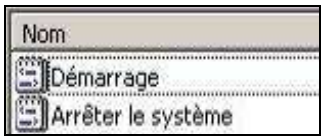
Paramètres Windows

Les paramètres Windows se divisent en deux groupes :

- Les scripts.
- Les paramètres de Sécurité.



Les Scripts

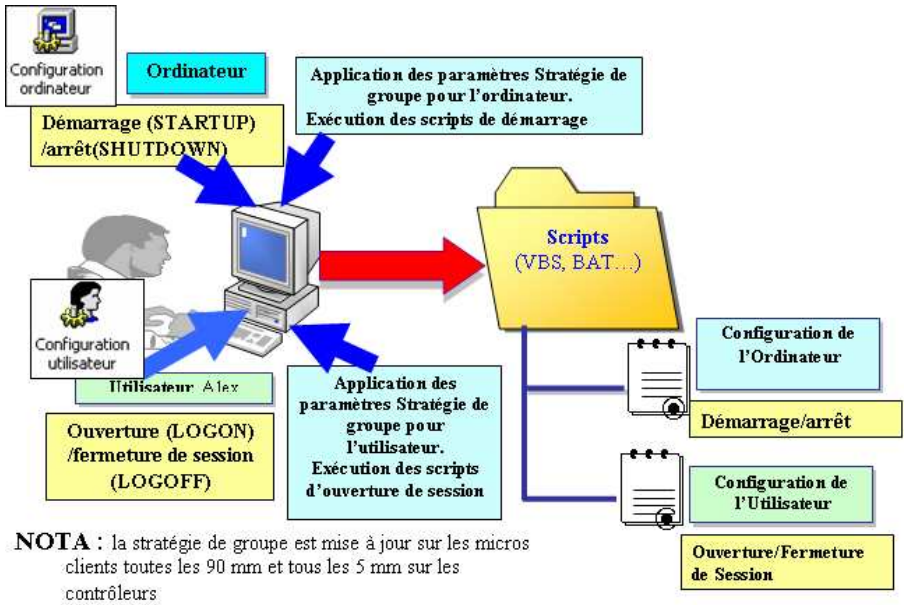
Il existe deux scripts possibles : 

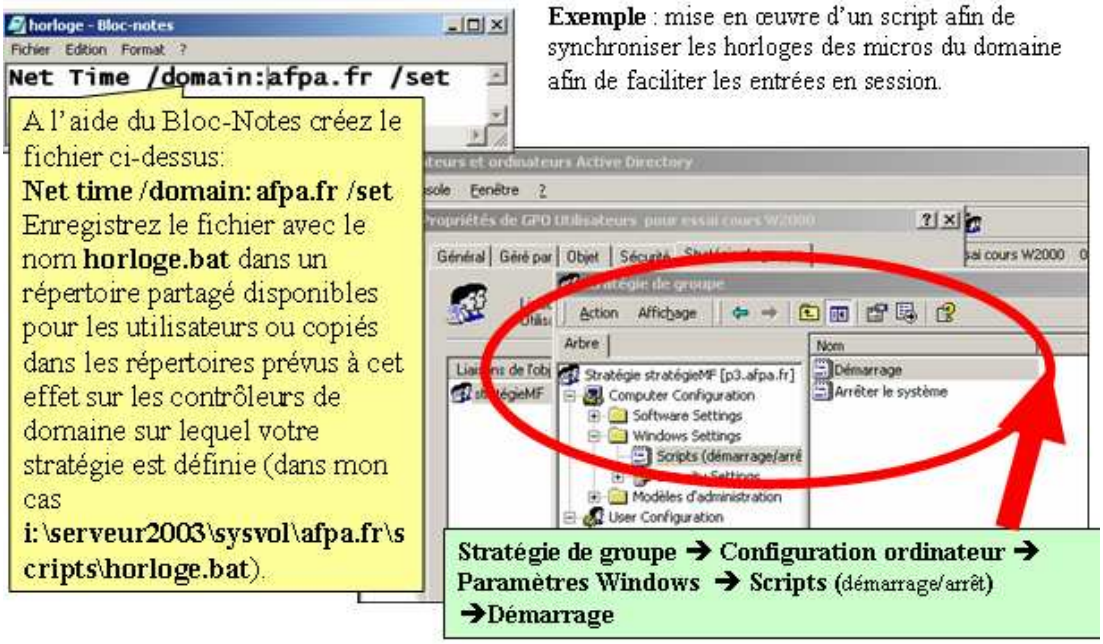
Les scripts peuvent être des fichiers commandes MS-DOS de type .bat ou .cmd ou VBScript, JScript ou Perl.

Paramètres Windows Scripts 

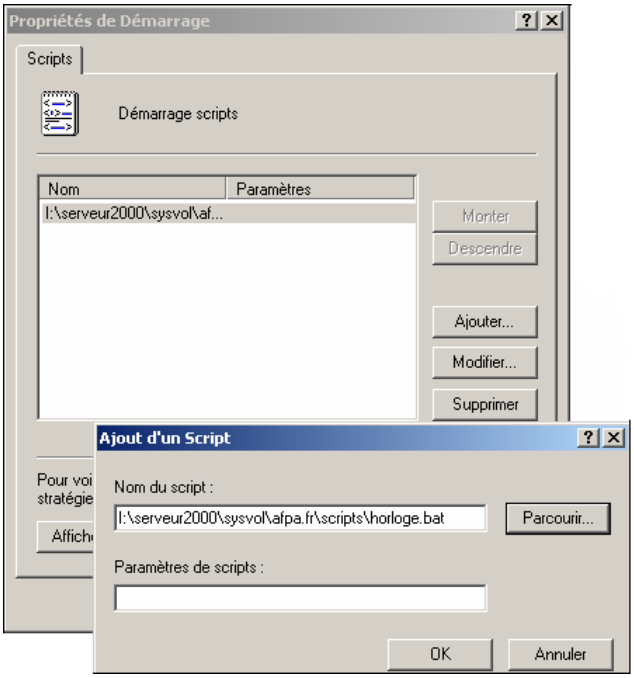
et 

Les scripts possèdent l'extension *.bat, *.cmd, *.exe, *.vbs …
Sont enregistrés dans le dossier SCRIPTS de chaque stratégie de groupe.
✋ Ils n'ont aucun rapport avec les scripts utilisateur (définis au niveau des propriétés d'un compte utilisateur) qui sont stockés dans le partage NETLOGON.
Ces scripts peuvent être écrits en DOS, VB Script, JavaScript, Perl ou WSH (Windows Scripting Host).

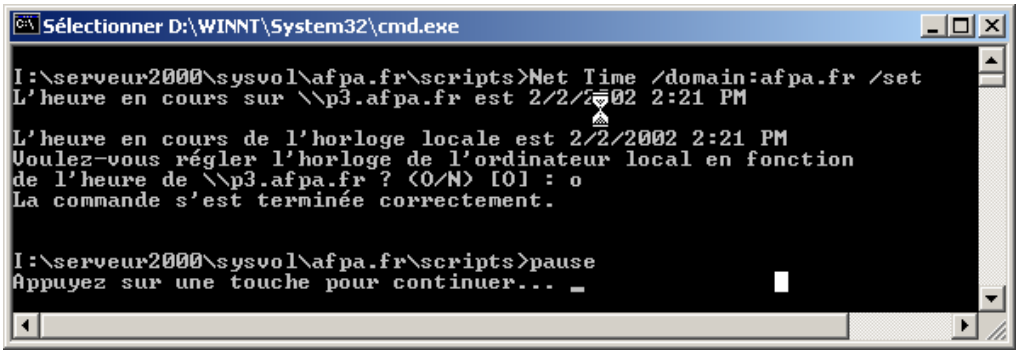




Exemple : mise en œuvre d'un script afin de synchroniser les horloges des micros du domaine afin de faciliter les entrées en session.



Cliquez sur **Ajouter** pour utiliser le fichier venant d'être créé, puis entrez le **Nom du Script**, cliquez sur **Parcourir**, sélectionnez le fichier batch (horloge.bat). Entrez les éventuels paramètres dans la zone **Paramètres de Script**, puis validez par **OK**. Vous pouvez mettre en œuvre plusieurs scripts. Ils seront exécutés du bas vers le haut (utilisation des boutons **Monter** et **Descendre**).



Les paramètres de sécurité

Les paramètres de sécurité comprennent les paramètres :

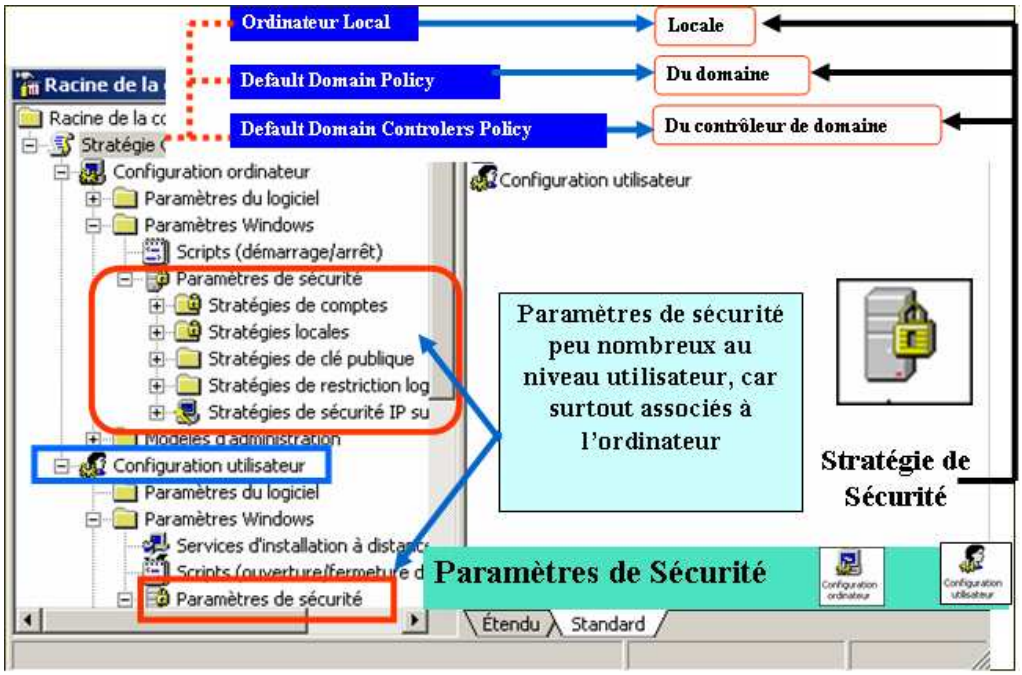
- De stratégies de comptes.
- De stratégies locales.
- De journal d'événements.

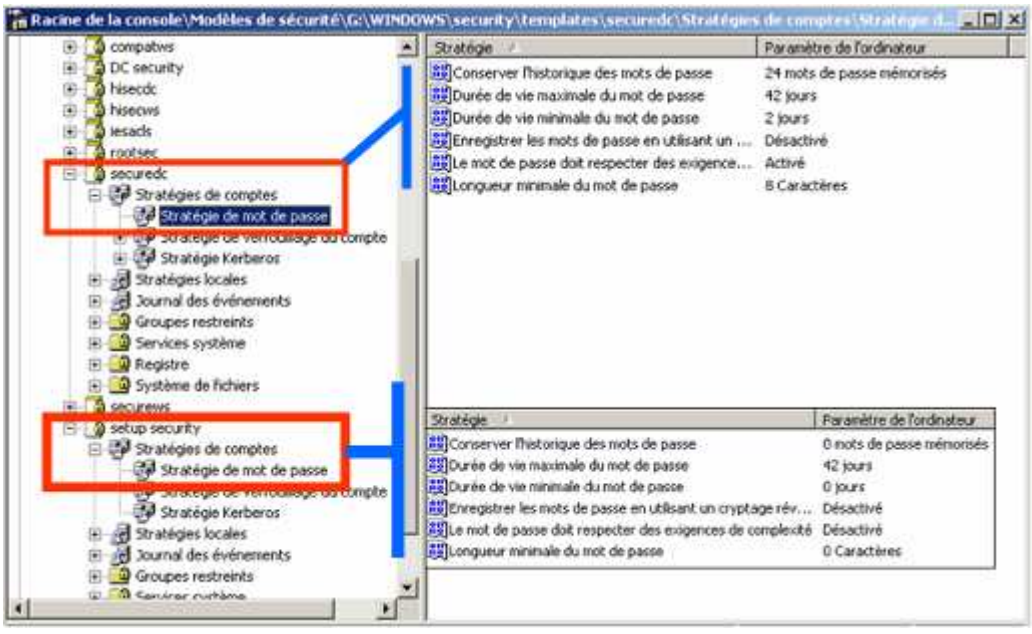
Chaque paramètre fait appel à une fenêtre pour entrer la valeur correspondante. Les paramètres de sécurité sont associés principalement au niveau de l'ordinateur, bien qu'il existe quelques paramètres au niveau utilisateur.

Nous verrons que vous avez la possibilité d'utiliser vos propres modèles de sécurité ou ceux fournis par défaut dans le répertoire %windir%\security\template*.inf.

La sécurité appliquée aux ordinateurs est exécutée via des consoles **MMC** prédéfinies dans les **Outils d'Administration** soit :

- Stratégie de sécurité locale (ordinateur local).
- Du domaine (Default Domain Policy).
- Du Contrôleur de Domaine (Default Domain Controlers Policy).





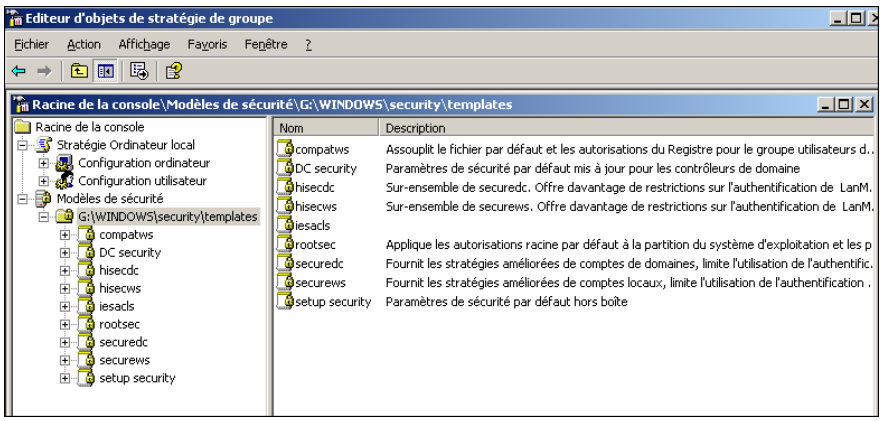
Utiliser des modèles de sécurité pour sécuriser des ordinateurs
Les modèles de sécurité vous permettent d'appliquer les paramètres de sécurité au niveau du réseau.

- **Stratégie de comptes :**
  - Stratégies de mot de passe (longueur, durée, historique…).
  - Stratégie de verrouillage de compte.
  - Stratégie Kerberos.
- **Stratégies locales :**
  - Stratégies d'audit.
  - Attribution des droits utilisateurs.
  - Options de sécurité.
- **Journal des événements :** permet de définir la taille et le mode de fonctionnement des journaux de sécurité.
- **Groupes restreints :** définit les membres de groupes d'utilisateurs.
- **Service système :** définit le mode de fonctionnement de services systèmes (activé/désactivé).
- **Registre :** définit les permissions d'accès aux clés de registre.
- **Système de fichiers :** définit les permissions d'accès aux dossiers et fichiers sur des partitions NTFS.

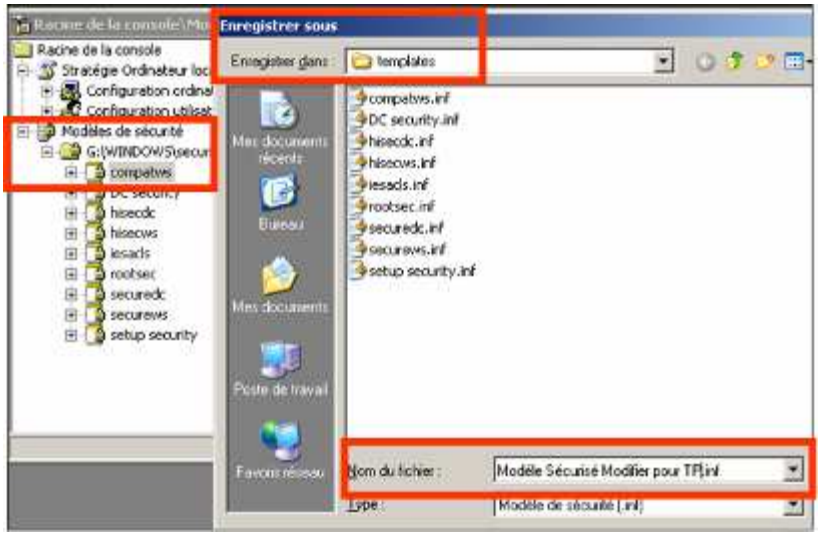
Utiliser des Modèles de sécurité prédéfinis pour sécuriser des ordinateurs
Le composant logiciel enfichable **Modèles de sécurité** affiche les modèles prédéfinis vous permettant de modifier et d'enregistrer vos propres modèles. Vous pouvez utiliser ces modèles tels quels ou bien vous en servir comme base de travail en les modifiant suivant vos besoins. Ils se trouvent par défaut dans le dossier %systemroot%\security\Templates.

Console MMC Modèles de sécurité pour sécuriser des ordinateurs

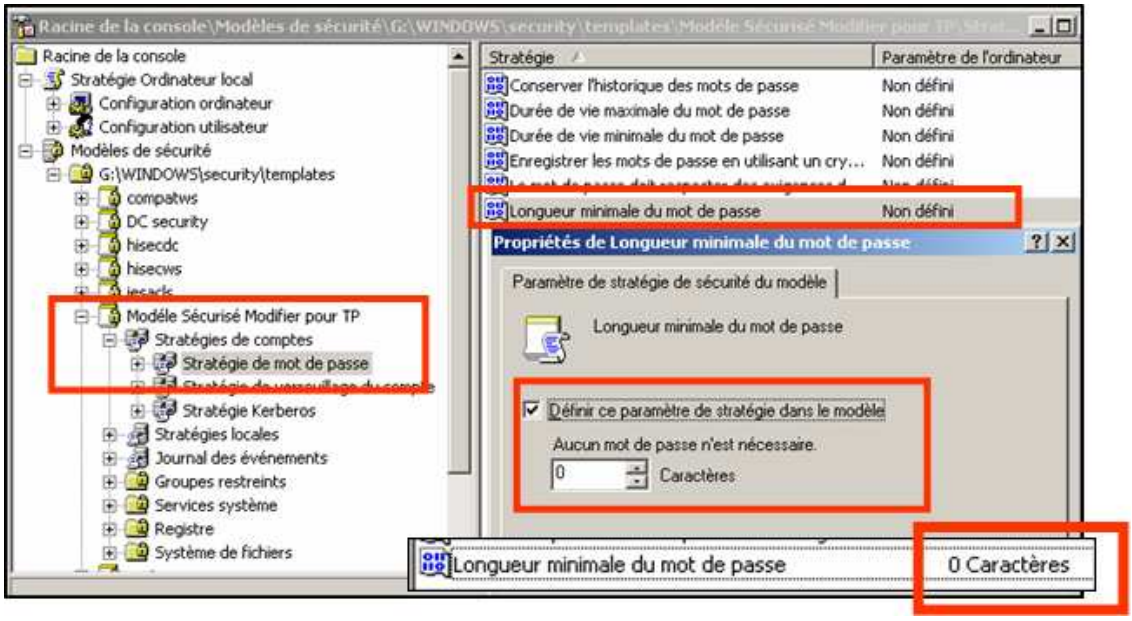
Modèle	Description
Sécurité par défaut (Setup security.inf)	Donne les paramètres de sécurité par défaut.
Sécurité par défaut du contrôleur de domaine (DC security.inf)	Affecte les paramètres de sécurité par défaut actualisés à partir de Setup security.inf pour un contrôleur de domaine.
Compatible (Compatws.inf)	Modifie les autorisations et les paramètres de registre pour le groupe Utilisateurs pour permettre une compatibilité maximale des applications.
Sécurisé (Securedc.inf and Securews.inf)	Améliore les paramètres de sécurité ayant le moins d'impact sur la compatibilité des applications.
Hautement sécurisé (Hisecdc.inf and Hisecws.inf)	Augmente les restrictions affectant les paramètres de sécurité.
Sécurité racine du système (Rootsec.inf)	Indique les spécifications pour la racine du lecteur système.



Personnaliser et créer un Modèle Personnalisé à partir d'un Modèle Défini
Sélectionnez un modèle de sécurité en développant **Modèles de sécurité**, cliquez droit dessus puis choisissez **Enregistrer** ou **Enregistre sous** en fonction de votre souhait de modifier ou non le modèle. Entrez un nouveau nom de fichier.



Modifiez les différents paramètres que vous désirez de votre modèle puis sauvegardez-le.



Créer un Nouveau Modèle de Sécurité

A partir de la console **Modèles de sécurité**, faites un clic droit sur le dossier dans lequel vous souhaitez enregistrer le modèle. Sélectionnez l'option **Nouveau Modèle**. Entrez son nom et une description, puis entrez les différents paramètres.

✋ Vous pouvez de la même façon créer une copie d'un modèle existant en l'Enregistrant sous un autre nom.

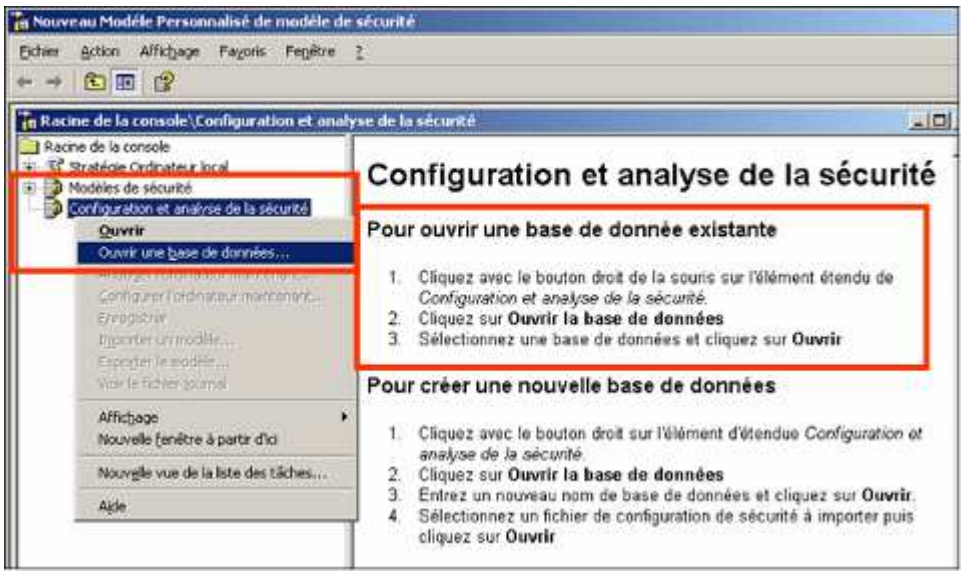
Configurer et analyser la sécurité : exécutez la console Gestion des stratégies de Groupe

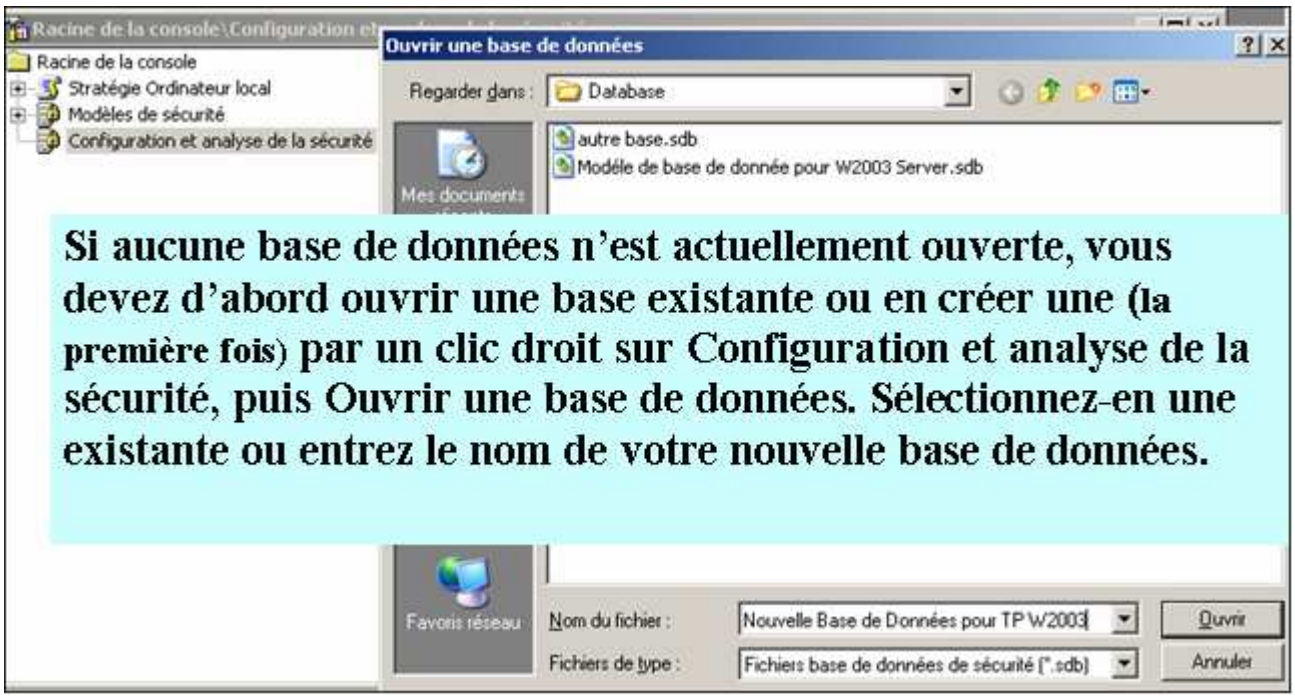
A partir de la console **Configuration et analyse de la sécurité**, vous pouvez :

- Vérifier les paramètres de sécurité de votre ordinateur en référence à un modèle de sécurité.
- Configurer un micro avec les paramètres du modèle.

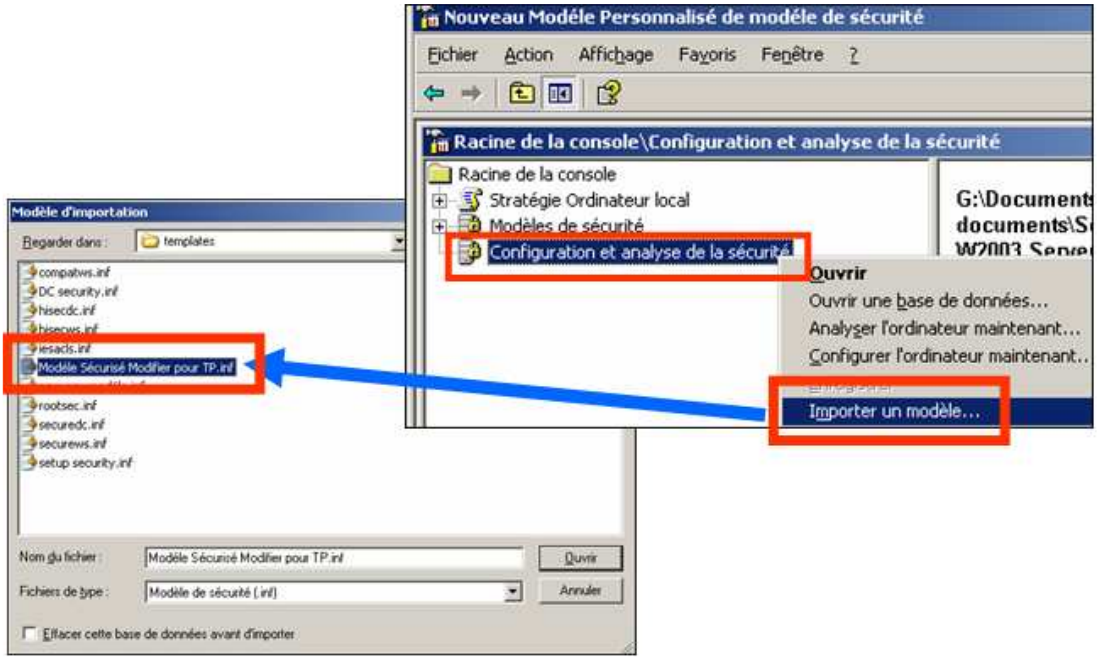
Analyse de la sécurité

A partir d'une console **MMC** dans laquelle vous avez ajouté le composant logiciel enfichables **Configuration et analyse de la sécurité**, cliquez droit sur **Configuration et analyse de la sécurité**. Sélectionnez l'option **Ouvrir une base de données**. Entrez dans la zone **Nom du fichier** un nouveau nom de fichier. Il aura par défaut l'extension .sdb. L'outil de configuration en a besoin car il l'utilise pour stocker ses paramètres et informations du modèle de sécurité. Cliquez ensuite sur le bouton **Ouvrir**.

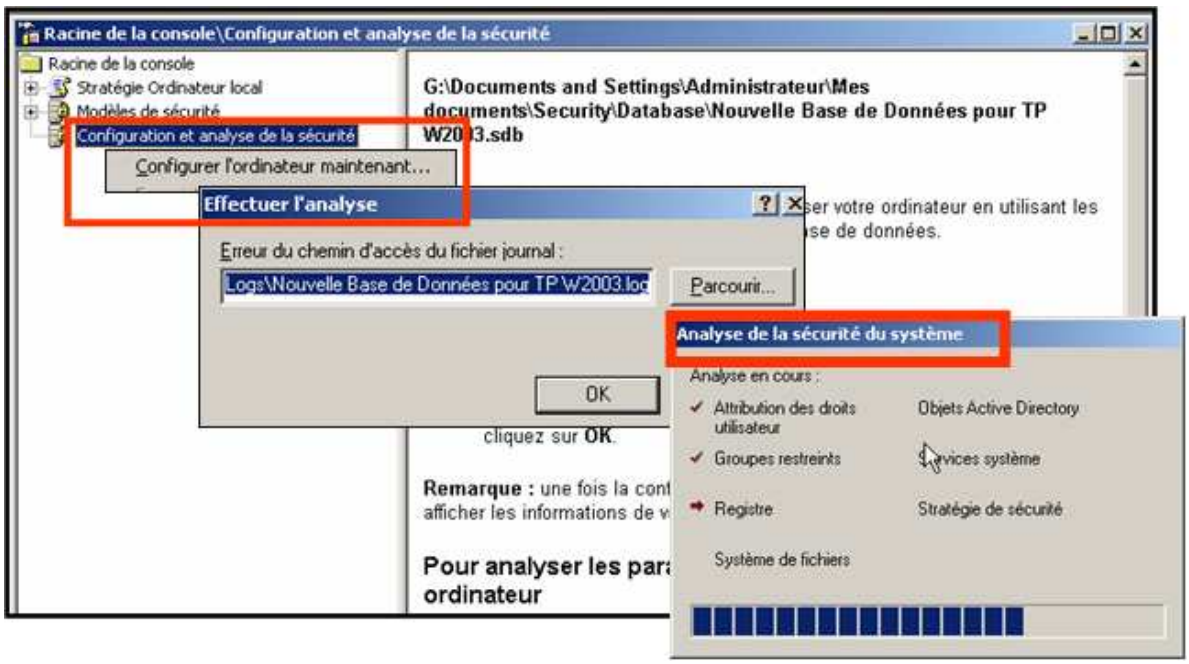




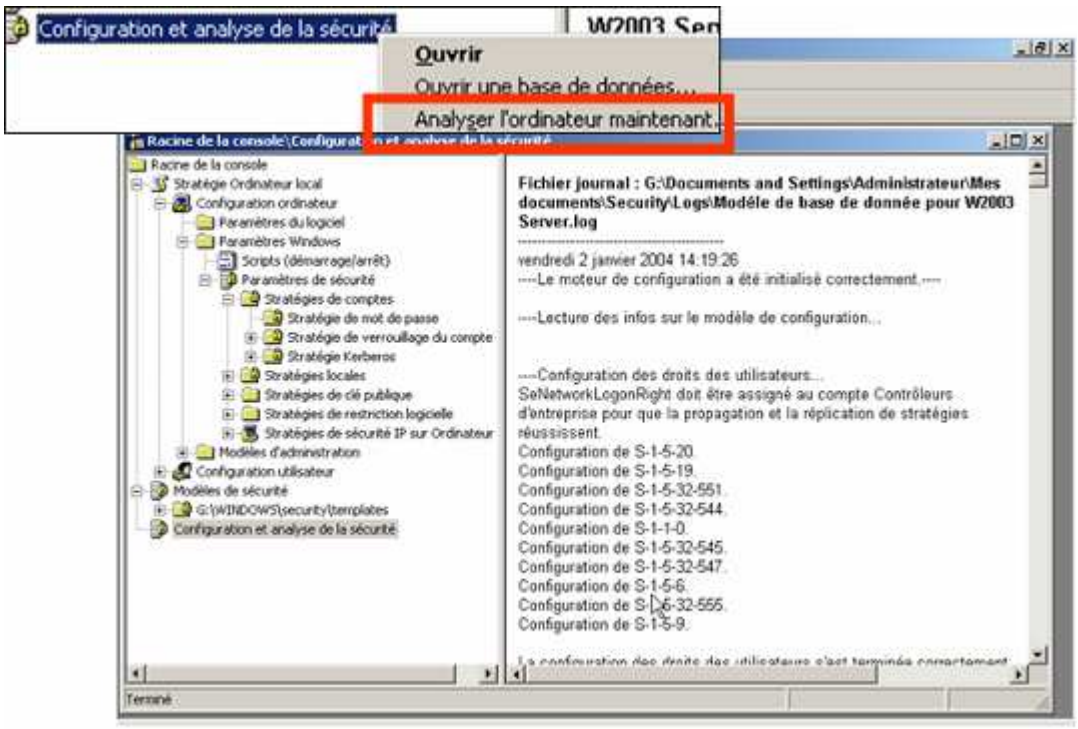
Comment importer un modèle de sécurité
Faites un clic droit sur la stratégie de groupe souhaitée puis validez **Importer une stratégie**. Sélectionnez le modèle que vous souhaitez importer. La case à cocher **Effacer cette base de données avant d'Importer** vous permet d'effacer les paramètres de sécurité existants avant d'intégrer les paramètres du nouveau modèle. Dans le cas où elle n'est pas cochée les paramètres du modèle seront additionnés avec les paramètres de la stratégie de groupe. Cliquez sur **Ouvrir** pour importer les paramètres.



Analyse de la sécurité
Cette analyse se fait à partir de la console **Configuration et analyse de la sécurité**. Cela vous permet de vérifier les paramètres de sécurité de votre machine en prenant un modèle de sécurité comme référant. Cela vous permet aussi configurer un ordinateur avec les paramètres du modèle de votre choix.



A partir de la console **Configuration et analyse de la sécurité**, cliquez droit sur **Configuration et analyse de la sécurité**. Choisissez **Analyser l'ordinateur maintenant.** Dans la fenêtre **Effectuer une analyse**, entrez le nom d'un fichier journal dans lequel sera enregistré le résultat de votre analyse. Vous pouvez vérifier le résultat dans un fichier journal.



A la fin de l'analyse une fenêtre affiche les paramètres actuels de l'ordinateur et ceux de votre modèle. Vous verrez apparaître par un point rouge les non concordances et en vert les concordances. Par un simple double-clic sur un paramètre vous pouvez modifier celui-ci.

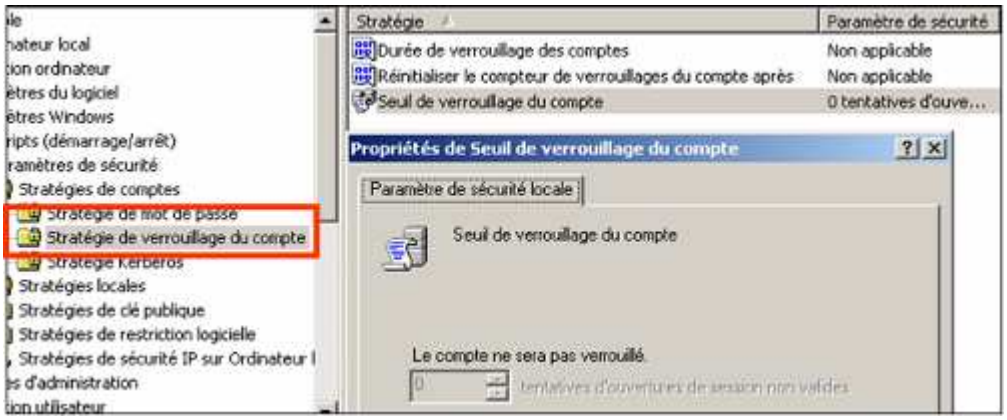
8.2.7- Les paramètres de stratégies de compte

Les paramètres concernant les mots de passe

Important :
Il existe une contrainte sur les mots de passe lorsque la complexité est activée :

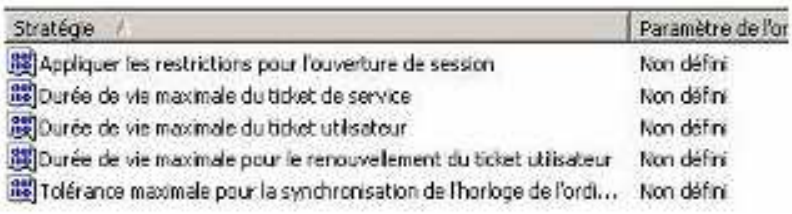
- **Ne pas contenir tout ou partie du nom du compte de l'utilisateur,**
- **Avoir une longueur d'au moins 6 caractères,**
- **Contenir une combinaison d'au moins trois des types de caractères suivants : majuscules (A à Z), minuscules (a à z), chiffres (0 à 9), caractères non alphabétiques (ex : @, ?, !, *, $, #, %).**

Les paramètres concernant le verrouillage de compte



Permet l'activation des comptes et les durées de réinitialisation suite à un mot de passe erroné. Par défaut pas de blocage car le seuil est à 0.

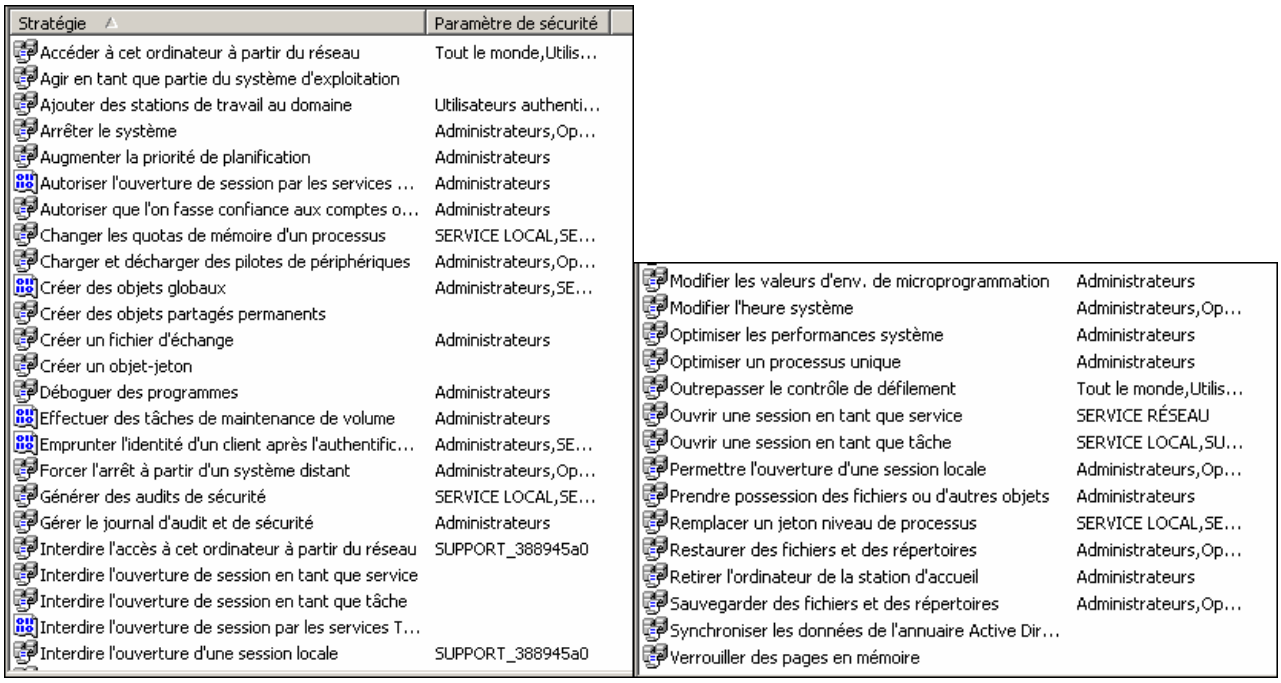
Les paramètres Kerberos
Le protocole de sécurité Kerberos V5 est la technologie d'authentification par défaut. Cette méthode peut être utilisée pour n'importe quel client exécutant le protocole Kerberos (qu'il s'agisse de clients équipés de Windows 2003 ou non) membre d'un domaine approuvé.



Les paramètres concernant la Stratégie d'audit

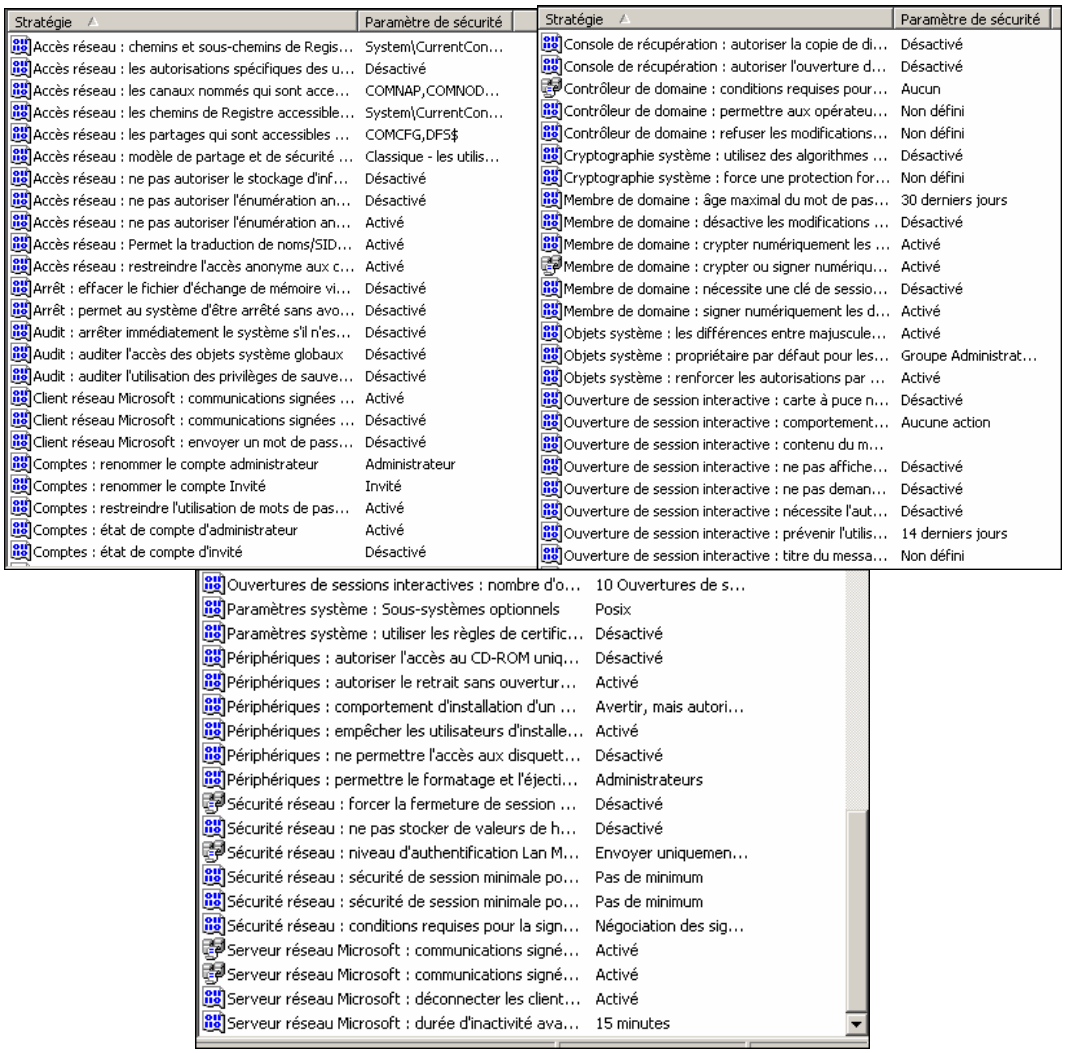
Active ou désactive les stratégies d'audit pour stocker les échecs et/ou les réussites dans le journal de sécurité (journal des événements).

Les paramètres concernant l'attribution des droits utilisateur



Définit les nombreux paramètres affectés à l'utilisation de votre micro comme l'ouverture de session locale ou via le réseau, l'arrêt de la machine...

Les paramètres concernant les options de sécurité

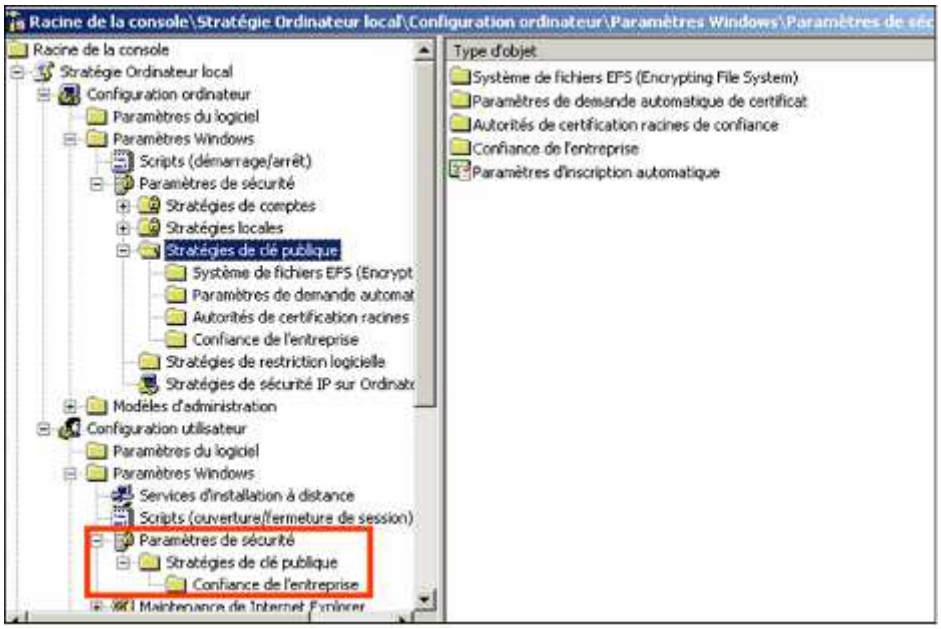


Stratégie	Paramètre de sécurité
Accès réseau : chemins et sous-chemins de Regis…	System\CurrentCon…
Accès réseau : les autorisations spécifiques des u…	Désactivé
Accès réseau : les canaux nommés qui sont acce…	COMNAP,COMNOD…
Accès réseau : les chemins de Registre accessible…	System\CurrentCon…
Accès réseau : les partages qui sont accessibles …	COMCFG,DFS$
Accès réseau : modèle de partage et de sécurité …	Classique - les utilis…
Accès réseau : ne pas autoriser le stockage d'inf…	Désactivé
Accès réseau : ne pas autoriser l'énumération an…	Désactivé
Accès réseau : ne pas autoriser l'énumération an…	Activé
Accès réseau : Permet la traduction de noms/SID…	Activé
Accès réseau : restreindre l'accès anonyme aux c…	Activé
Arrêt : effacer le fichier d'échange de mémoire vi…	Désactivé
Arrêt : permet au système d'être arrêté sans avo…	Désactivé
Audit : arrêter immédiatement le système s'il n'es…	Désactivé
Audit : auditer l'accès des objets système globaux	Désactivé
Audit : auditer l'utilisation des privilèges de sauve…	Désactivé
Client réseau Microsoft : communications signées …	Activé
Client réseau Microsoft : communications signées …	Désactivé
Client réseau Microsoft : envoyer un mot de pass…	Désactivé
Comptes : renommer le compte administrateur	Administrateur
Comptes : renommer le compte Invité	Invité
Comptes : restreindre l'utilisation de mots de pas…	Activé
Comptes : état de compte d'administrateur	Activé
Comptes : état de compte d'invité	Désactivé

Stratégie	Paramètre de sécurité
Console de récupération : autoriser la copie de di…	Désactivé
Console de récupération : autoriser l'ouverture d…	Désactivé
Contrôleur de domaine : conditions requises pour…	Aucun
Contrôleur de domaine : permettre aux opérateu…	Non défini
Contrôleur de domaine : refuser les modifications…	Non défini
Cryptographie système : utilisez des algorithmes …	Désactivé
Cryptographie système : force une protection for…	Non défini
Membre de domaine : âge maximal du mot de pas…	30 derniers jours
Membre de domaine : désactive les modifications …	Désactivé
Membre de domaine : crypter numériquement les …	Activé
Membre de domaine : crypter ou signer numériqu…	Activé
Membre de domaine : nécessite une clé de sessio…	Désactivé
Membre de domaine : signer numériquement les d…	Activé
Objets système : les différences entre majuscule…	Activé
Objets système : propriétaire par défaut pour les…	Groupe Administrat…
Objets système : renforcer les autorisations par …	Activé
Ouverture de session interactive : carte à puce n…	Désactivé
Ouverture de session interactive : comportement…	Aucune action
Ouverture de session interactive : contenu du m…	
Ouverture de session interactive : ne pas affiche…	Désactivé
Ouverture de session interactive : ne pas deman…	Désactivé
Ouverture de session interactive : nécessite l'aut…	Désactivé
Ouverture de session interactive : prévenir l'utilis…	14 derniers jours
Ouverture de session interactive : titre du messa…	Non défini

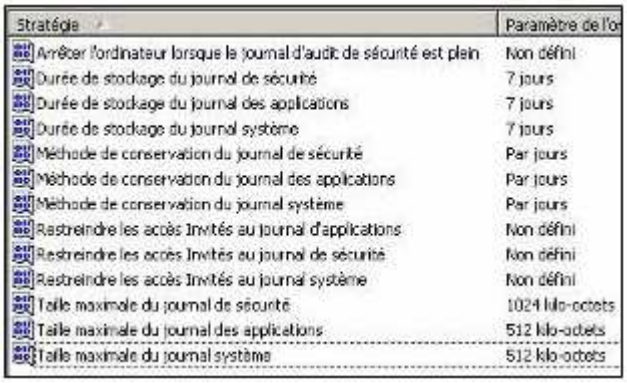
Ouvertures de sessions interactives : nombre d'o…	10 Ouvertures de s…
Paramètres système : Sous-systèmes optionnels	Posix
Paramètres système : utiliser les règles de certific…	Désactivé
Périphériques : autoriser l'accès au CD-ROM uniq…	Désactivé
Périphériques : autoriser le retrait sans ouvertur…	Activé
Périphériques : comportement d'installation d'un …	Avertir, mais autori…
Périphériques : empêcher les utilisateurs d'installe…	Activé
Périphériques : ne permettre l'accès aux disquett…	Désactivé
Périphériques : permettre le formatage et l'éjecti…	Administrateurs
Sécurité réseau : forcer la fermeture de session …	Désactivé
Sécurité réseau : ne pas stocker de valeurs de h…	Désactivé
Sécurité réseau : niveau d'authentification Lan M…	Envoyer uniquemen…
Sécurité réseau : sécurité de session minimale po…	Pas de minimum
Sécurité réseau : sécurité de session minimale po…	Pas de minimum
Sécurité réseau : conditions requises pour la sign…	Négociation des sig…
Serveur réseau Microsoft : communications signé…	Activé
Serveur réseau Microsoft : communications signé…	Activé
Serveur réseau Microsoft : déconnecter les client…	Activé
Serveur réseau Microsoft : durée d'inactivité ava…	15 minutes

Définit les paramètres globaux de l'ordinateur qui conditionnent son comportement, de façon indépendante de l'utilisateur entré en connexion (périphérique, ouverture de session, comptes, sécurité…).

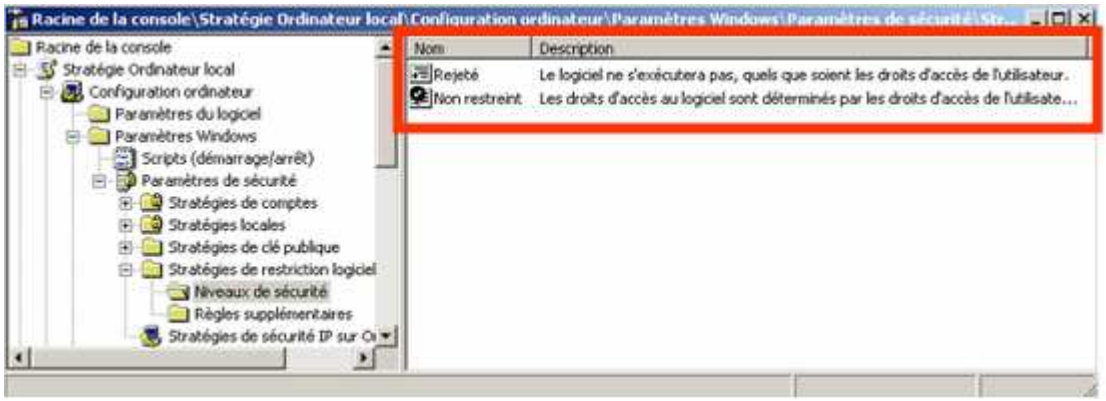


Définit les règles de demande ou d'obtention des certificats de clé publique et les autorités de certification racine ou approuvées de l'entreprise. Stratégie partiellement disponible au niveau utilisateur.

Les paramètres du journal des événements
Ces paramètres permettent de modifier les conditions de stockage des événements enregistrés dans les différents journaux.

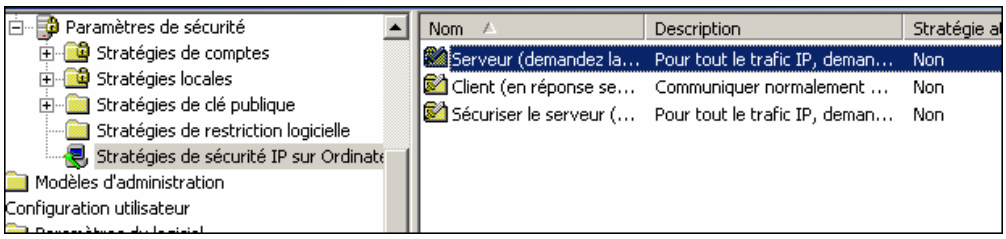


Paramètres de Sécurité Stratégies de Restriction Logicielle



Stratégie nouvelle sous W2003 Server. Les stratégies de restriction logicielle permettent de protéger votre environnement informatique contre des logiciels non approuvés en identifiant et spécifiant les logiciels autorisés à être exécutés. Applicable comme Stratégie Ordinateur et Utilisateur.

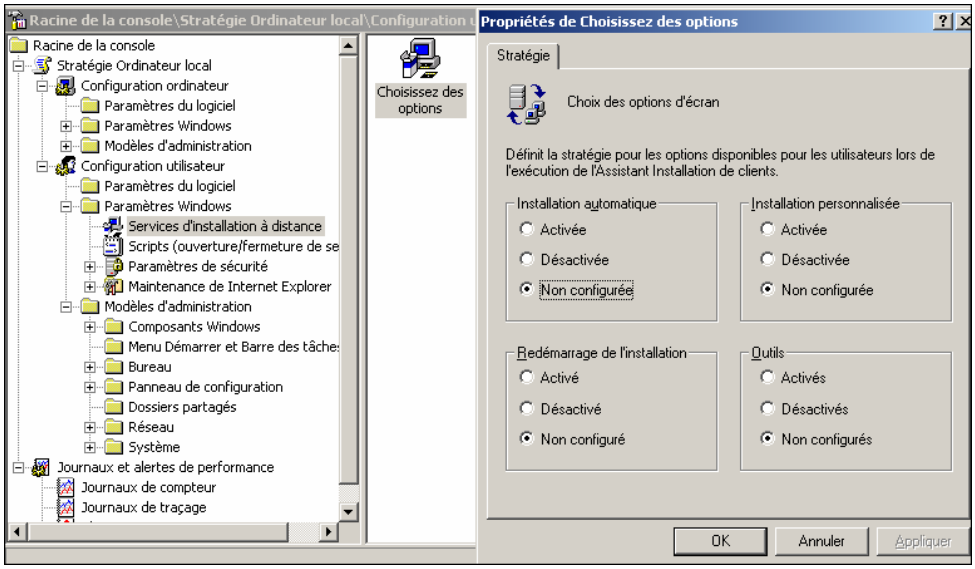
Paramètres de Sécurité Stratégies de sécurité IP sur Ordinateur



Cette stratégie met en œuvre le protocole IPSec afin de sécuriser les échanges de données sur un réseau local ou sur un VPN (Virtual Private Network). Pour être sécurisés, les micros qui dialoguent avec le protocole IPSec doivent utiliser et activer des stratégies compatibles qu'elles devront **Négocier** ou **Filtrer** avant transfert.
Server : il demande la sécurité IP et l'utilise si le client la supporte, sinon la communication se fait classiquement.

Client : dans ce cas le serveur utilise la sécurité IP si le client en fait la demande, sinon la communication se fait classiquement.
Sécuriser le Serveur : le serveur impose la sécurité IP, sinon refus de tout autre communication.

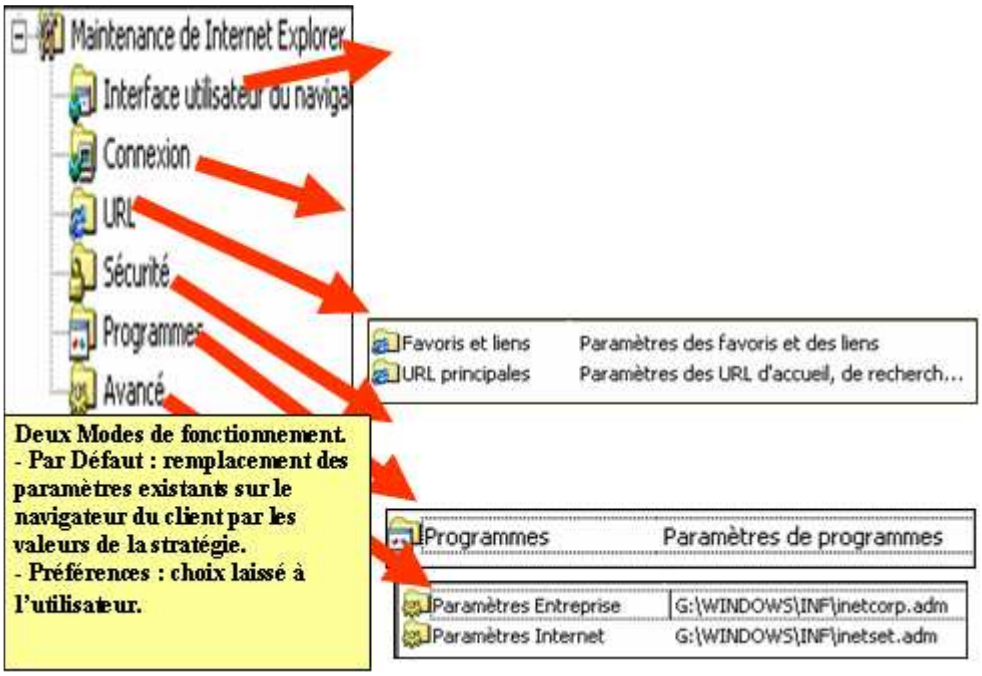
Paramètres de Configuration UTILISATEUR Services d'Installation à distance



Permet de définir les options disponibles pour un utilisateur des services d'installation à distance. Ces options sont généralement installées à partir d'un serveur RIS (Remote Installation Services).

Maintenance de Internet Explorer

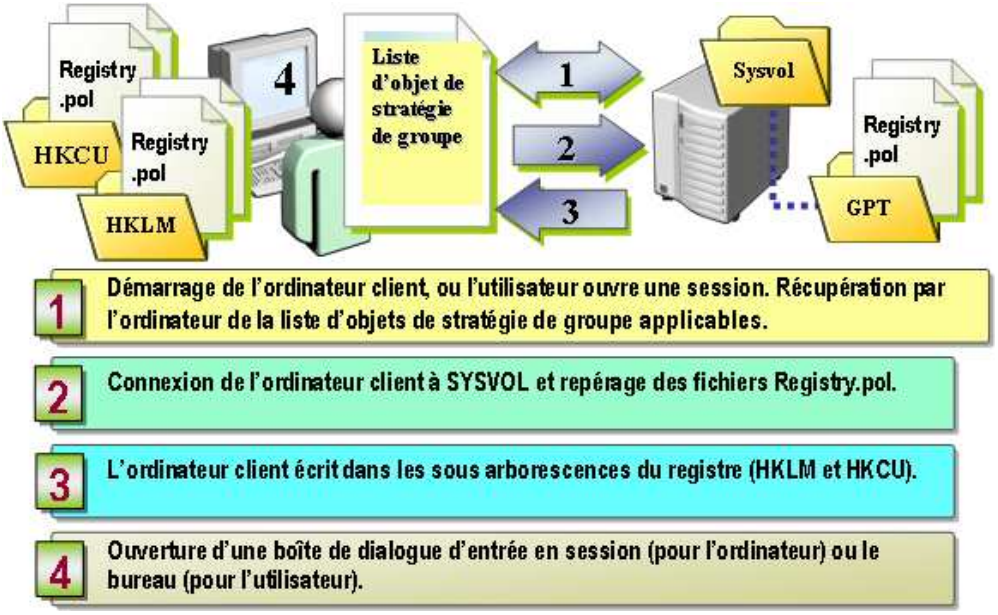
Cet élément permet d'administrer et de personnaliser **Microsoft Internet Explorer** sur les ordinateurs Windows 2003 pour les utilisateurs pour lesquels est appliquée la stratégie de groupe.



8.2.8- Modèles d'administration

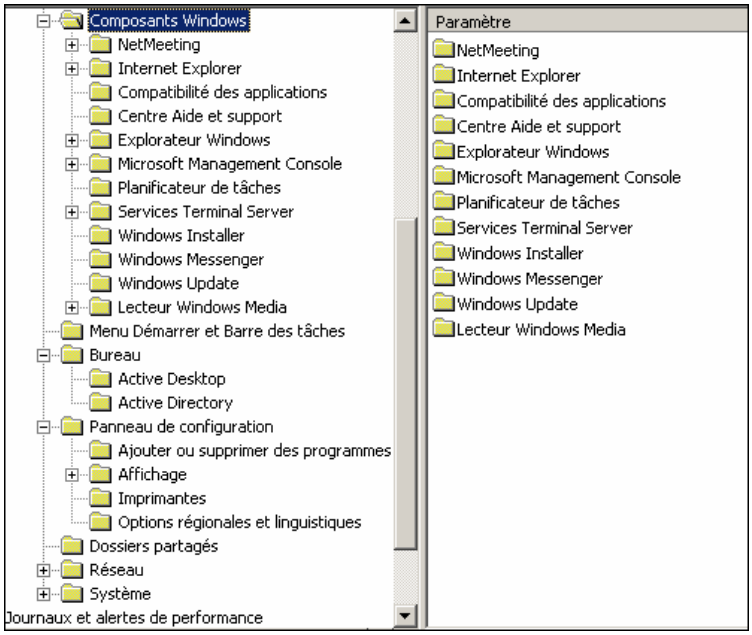
Ce sont des fichiers modèles contenant les paramètres de stratégie de groupe basés sur le registre. Les paramètres sont stockés sur les contrôleurs de domaines dans un fichier Registry.pol du modèle de **Stratégie de groupe**. Ils permettent de paramétrer l'environnement des utilisateurs, l'accès au panneau de configuration, le menu Démarrer, les quotas de disques… Ces fichiers modèles sont stockés sous %windir%\inf et ont pour extension .ADM. Plus de 450 paramètres sont disponibles dans ce dossier. Ils réalisent une mise à jour de la base de registre :

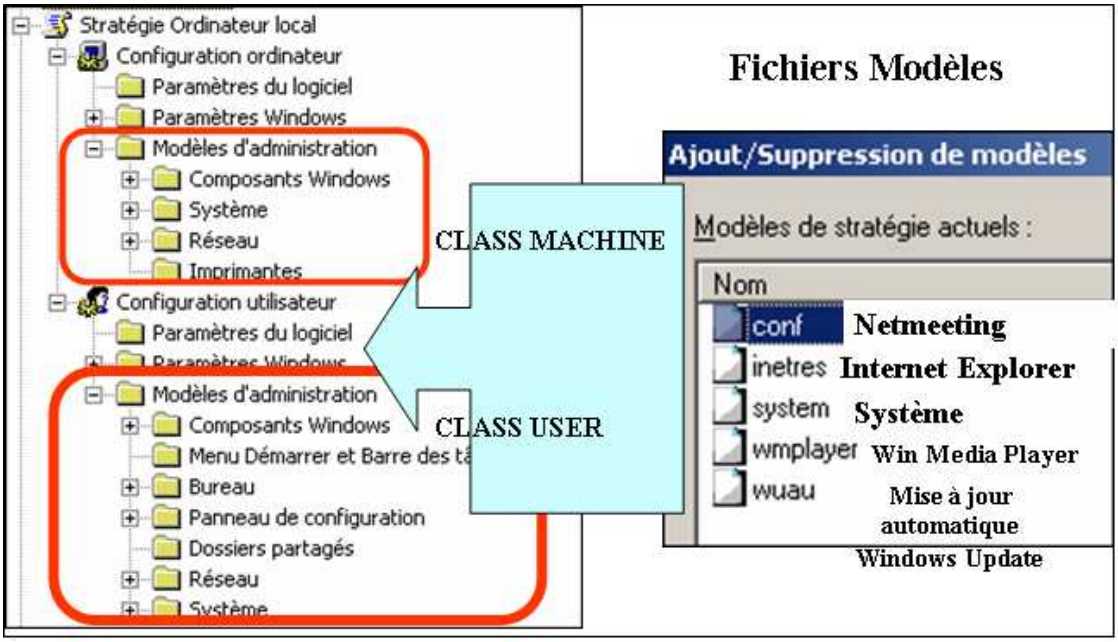
- Niveau ordinateur : HKEY_LOCAL_MACHINE pour la configuration ordinateur.
- Niveau utilisateur : HKEY_CURRENT_USER pour celle des utilisateurs.



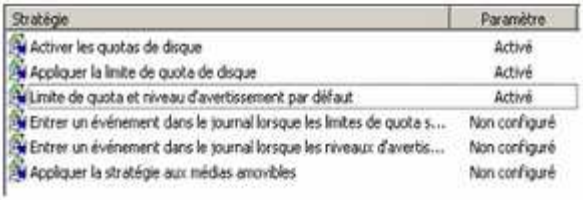
Type de paramètres	Eléments contrôlés	Disponible pour
Composants Windows	Accès utilisateur aux composants Windows.	Ordinateurs ou utilisateurs
Système	Ouverture et fermeture de session, stratégie de groupe, intervalles d'actualisation, quotas de disque, et stratégie de bouclage.	Ordinateurs ou utilisateurs
Réseau	Propriétés du réseau et des connexions d'appels entrants.	Ordinateurs ou utilisateurs
Imprimantes	Publication d'Active Directory et fonctionnalités d'impression basées sur le Web des imprimantes.	Ordinateurs
Menu Démarrer et barre des tâches	Apparence et accès au menu Démarrer et à la barre des tâches.	Ordinateurs ou utilisateurs
Bureau	Active Desktop : ce qui se visualise sur les bureaux, et ce que les utilisateurs peuvent réaliser avec le dossier Mes Documents.	Utilisateurs
Panneau de configuration	Utilisation de Ajoute/Supprimer des programmes, Affichage, Options régionales et linguistiques et Imprimantes.	Utilisateurs
Dossiers Partagés	Indique si les dossiers partagés ou les racines DFS sont publiés dans Active Directory.	Uitlisateurs

Le dossier **Modèles d'administration** contient plus de 45O paramètres de stratégie de groupe basés sur le Registre.





L'outil **Composants Windows** permet d'administrer les composants de Windows 2003 tels NetMeeting, Internet Explorer, le planificateur de tâches et Windows Installer.

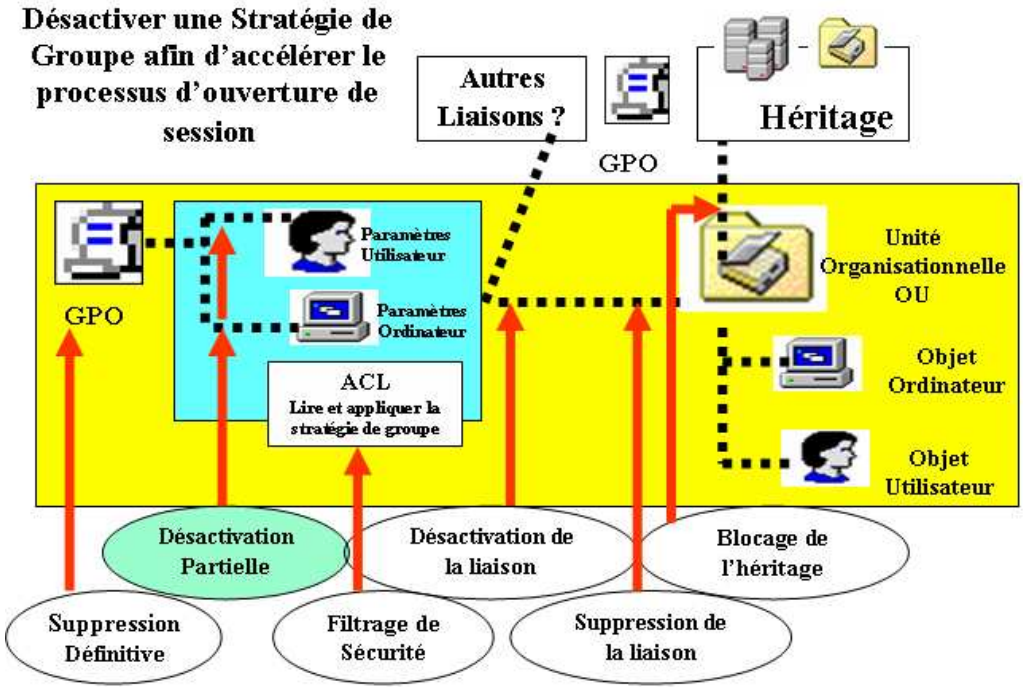


Système comme le montre la figure ci-dessus se divise en 5 dossiers contenant chacun un certain nombre de paramètres. Par exemple, le dossier **Quotas de disque** contient les paramètres suivants :

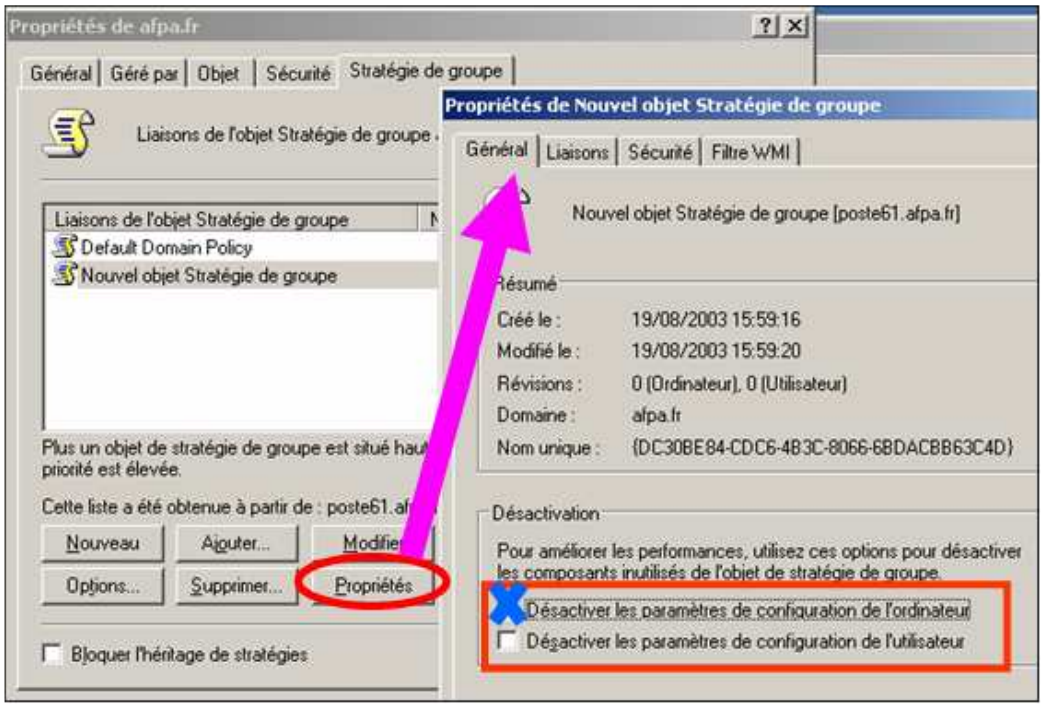
- Réseau contient des paramètres relatifs aux fichiers en réseau.
- Imprimantes contient des paramètres relatifs à l'utilisation et la gestion des imprimantes.

8.2.9- Désactivation des paramètres non utilisés

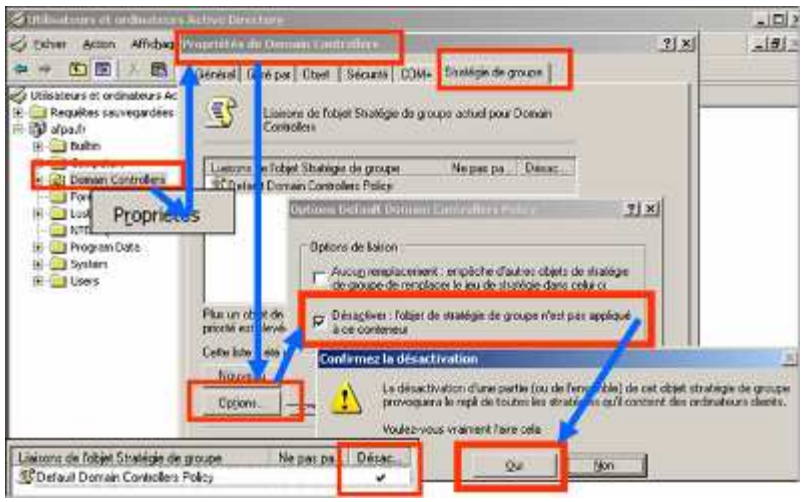
Si vous n'avez pas utilisé dans votre stratégie de groupe de paramètres concernant l'ordinateur, mais seulement l'utilisateur, vous pouvez désactiver l'ensemble des paramètres concernant l'ordinateur. L'inverse est également réalisable. Ceci entraîne un gain de temps dans l'application de la stratégie de groupe.



Par exemple, si vous n'avez pas utilisé de paramètres concernant l'ordinateur, pour désactiver ces paramètres, cliquez sur le GPO, puis sélectionnez **Propriétés**. Dans l'onglet **Général**, cochez la case correspondante à votre demande.



Rappel : les GPO sont consultés à chaque démarrage puis à l'ouverture de session pour définir les paramètres à mettre en oeuvre.



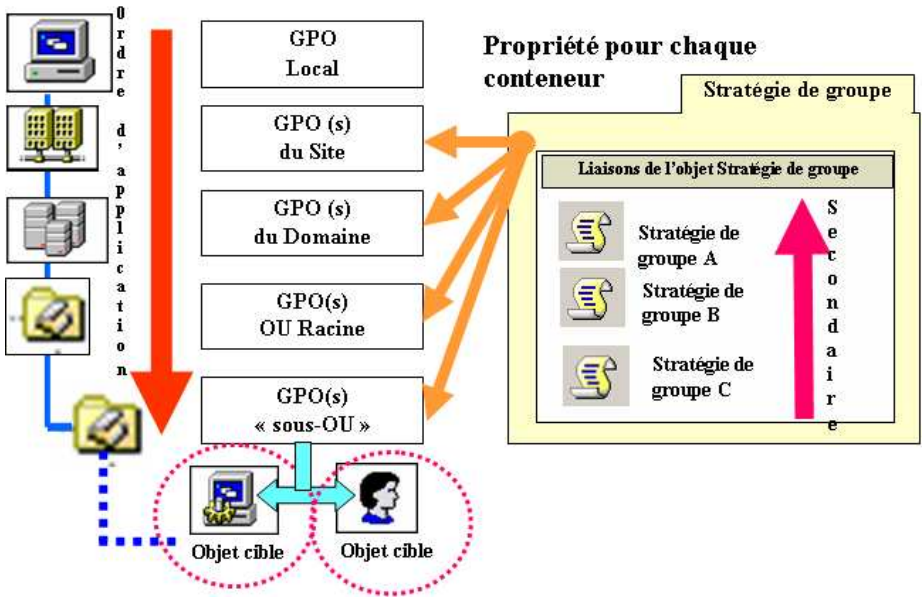
8.2.10- Désigner les exceptions

Ordre d'application des GPO dés le démarrage du système :

- En premier sont appliqués les Paramètres de stratégies de groupes ordinateurs dés le démarrage de la machine, puis Scripts de démarrage. Rafraîchis périodiquement en cours de fonctionnement. Par défaut toutes les 5 mm pour les contrôleurs de domaine. Toutes les 90 mm +/- un délai aléatoire de 0 à 30 mm pour les clients et serveurs membres
- Puis ouverture de Session par l'Utilisateur, application des Paramètres de l'utilisateur, puis Scripts d'ouverture de Session. Même périodicité de rafraîchissement que pour les paramètres de stratégies Ordinateurs. Paramétrage modifiable avec les stratégies de groupe. S'il y a un conflit entre la stratégie de l'ordinateur et de l'utilisateur, ce sont les paramètres définis au niveau ordinateur qui ont la priorité.

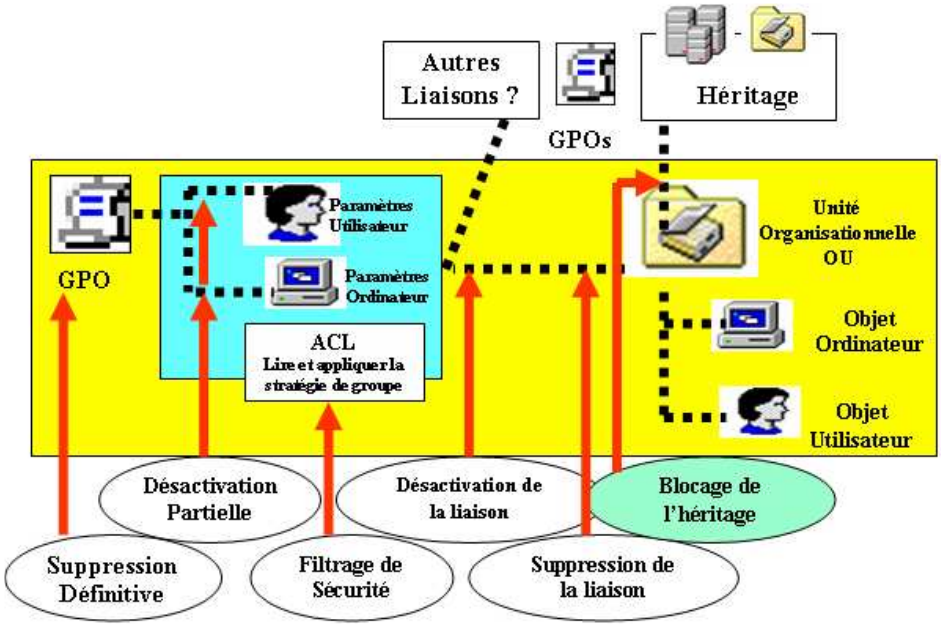
Ordre de traitement des paramètres de stratégies de groupe :

- **Local :** le GPO local est traité en premier.
- **Site :** si il existe un ou plusieurs GPO appliqués à un site, ils sont exécutés ensuite. Les GPO de site sont appliqués dans l'ordre indiqué par l'administrateur.
- **Domaine :** si il existe un ou plusieurs GPO appliqués au domaine dans lequel se trouve l'ordinateur ou l'utilisateur, ils sont appliqués à la suite dans l'ordre prévu.
- **UO :** les GPO appliqués à l'UO la plus élevée du niveau hiérarchique, sont appliqués ensuite dans l'ordre prévu. Si il existe des UO de niveaux inférieurs, ils sont exécutes ensuite.

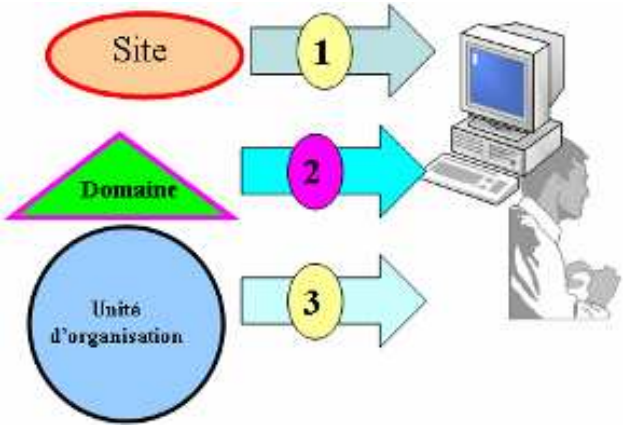


Dans le cas où plusieurs GPO sont définis sur une UO, c'est le plus bas dans la liste qui sera exécuté en premier et ainsi de suite jusqu‘au niveau le plus élevé. Ceci est modifiable avec les boutons **Monter** ou **Descendre**. S'il n'y a pas de conflit dans l’énoncé des stratégies, elles se cumulent. Dans le cas contraire c'est celle la plus proche de l'utilisateur qui sera appliquée (au niveau de la dernière UO).

Héritage des GPO

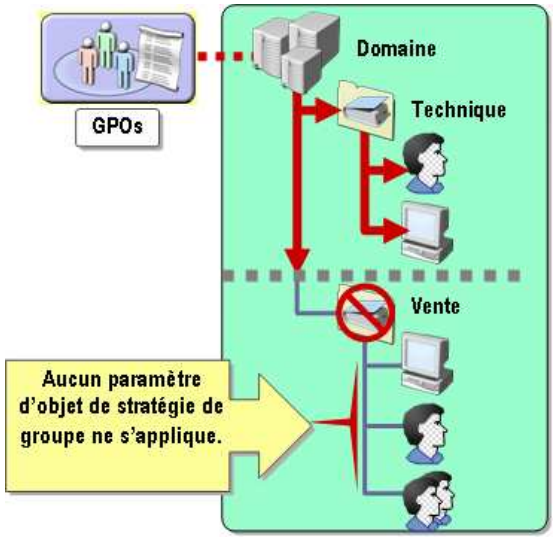


W2003 teste les objets GPO avec le conteneur AD le plus éloigné de l’ordinateur ou de l’utilisateur. Ordre d’héritage : Site / Domaine / UO. Par défaut les stratégies sont automatiquement héritées des conteneurs parents.



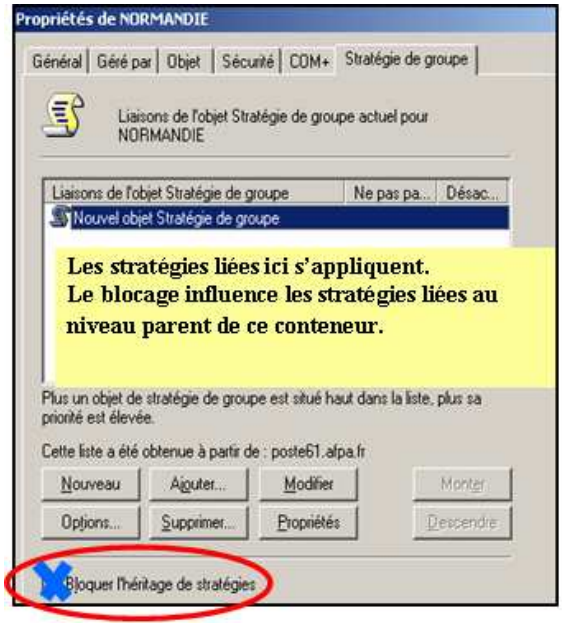
Option Bloquer l'héritage

Elle s'applique à tous les conteneurs de niveau inférieur. Si aucune stratégie n'est définie sur une OU, les utilisateurs de celle-ci peuvent se voir attribuer des paramètres définis au niveau du site, du domaine ou d'une OU parent à son conteneur. Les paramètres des niveaux supérieurs sont appliqués sur les niveaux inférieurs (Héritage). Par exemple, les paramètres d'un GPO appliqués sur un domaine, le sont sur toutes les UO de ce domaine. On dit que les paramètres des GPO des niveaux supérieurs sont hérités.



Blocage du traitement d'un objet de stratégie de groupe

Les paramètres des niveaux supérieurs sont appliqués sur les niveaux inférieurs (Héritage). Par exemple, les paramètres d'un GPO appliqués sur un domaine, le sont sur toutes les UO de ce domaine. On dit que les paramètres des GPO des niveaux supérieurs sont hérités. L'option **Bloquer l'héritage** empêche tous les paramètres de niveau supérieur d'agir sur le domaine ou l'UO dont la case **Bloquer l'héritage** a été cochée dans **Propriétés**. Toutefois les GPO marqués **Ne pas passer outre** sont quand même hérités.



Option Ne pas passer outre

Si cette option est appliquée à un GPO de niveau supérieur, ce sont les paramètres de ce niveau qui seront appliqués, en contradiction à la règle précisée ci-dessus, et ceci même si l'option **Ne pas passer outre** est appliquée sur des GPO de niveaux inférieurs. Si dans l'exemple précédent au niveau des **Propriétés du Domaine**, on coche la case **Aucun remplacement** dans le menu

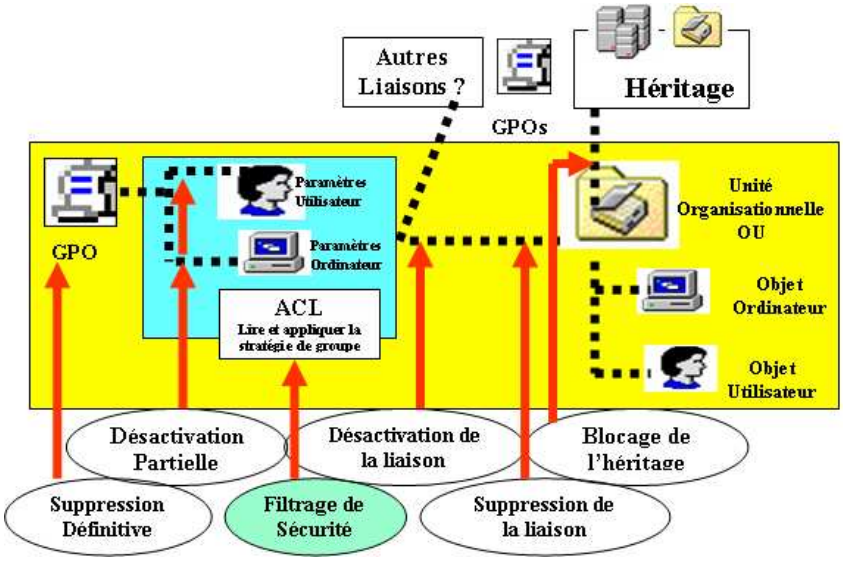
Options, ce sont les paramètres de cette stratégie qui seront appliqués et non ceux des GPO de l'UO **Marketing**.

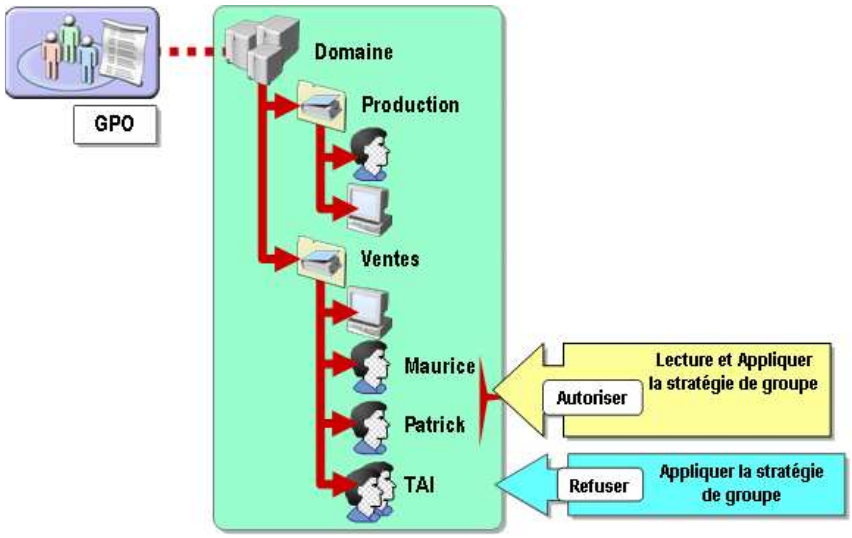
Au niveau parent d'un **container** sur lequel vous avez appliqué une **Stratégie de Groupe** vous pouvez appliquer une stratégie particulière : **Ne pas Passer Outre**

Paramètres de cette GPO sont **OBLIGATOIREMENT** appliqués aux niveaux inférieurs même si un blocage des stratégies est validé au niveau enfant:
➔ **Ne pas passer outre à priorité sur bloquer l'héritage des stratégies.**
➔ **Sauf dans le cas ou le conteneur parent dispose de l'option AUCUN REMPLACEMENT.**

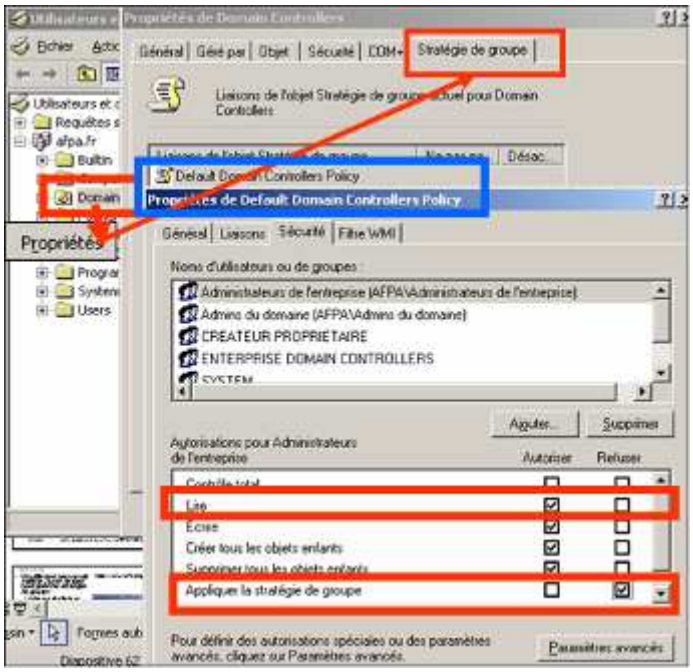
8.2.11- Filtrage de sécurité des stratégies de groupe

Si vous souhaitez exclure de l'application d'une stratégie de groupe, un groupe d'utilisateur ou un utilisateur, vous mettez en place un filtrage. Les paramètres du GPO ne s'appliquent plus à ce groupe ou cet utilisateur.





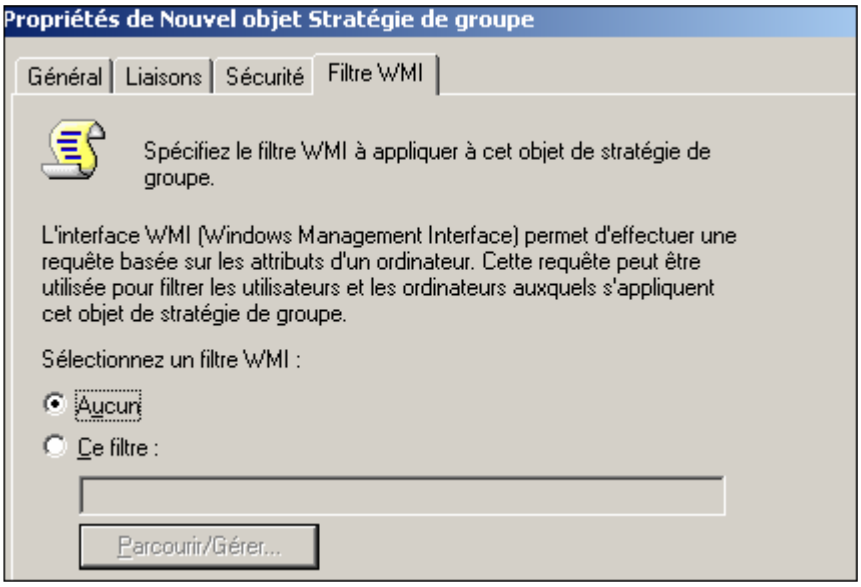
- Pour qu'un GPO s'applique aux utilisateurs d'un conteneur, il faut impérativement qu'ils disposent au minimum des permissions **Lire** et **Appliquer la stratégie de groupe**.
- Possibilité d'appliquer des stratégies à un groupe d'utilisateurs et d'extraire un autre utilisateur de la stratégie définie.
- Possibilité que la stratégie ne s'applique pas à un utilisateur en cochant l'option **Refuser**.



Par défaut les administrateurs ne sont pas soumis aux stratégies.

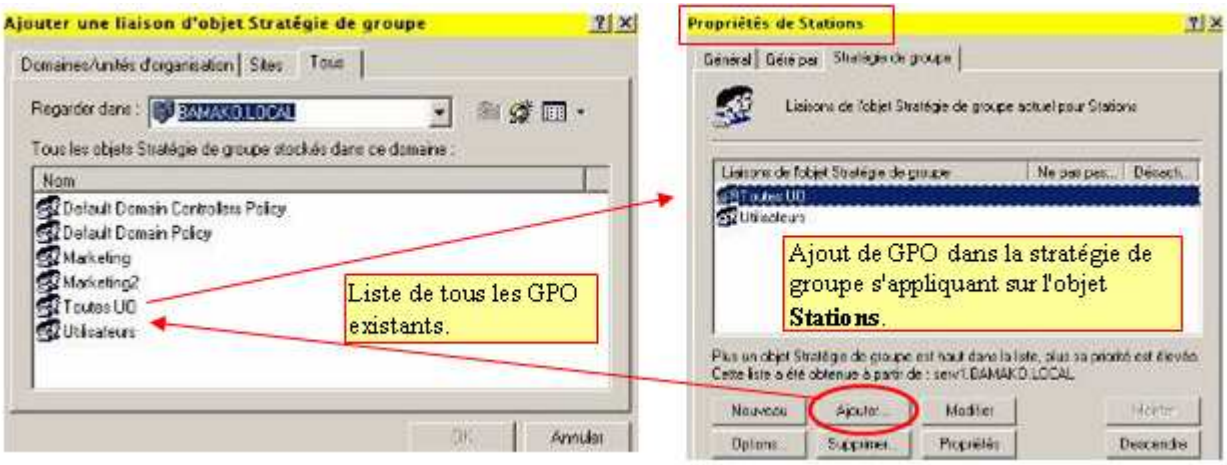
8.2.12- Filtrage des stratégies de groupe à l'aide de filtres WMI (Windows Management Instrumentation)

Infrastructure proposant des outils de développement. Permettent d'effectuer des requêtes sur des attributs spécifiques. Filtres écris en WMI Query Language (WQL).
Possibilité de créer des filtres sur les services, le matériel, type de processeur, mémoire...



8.2.13- Application de GPO à d'autres objets d'Active Directory

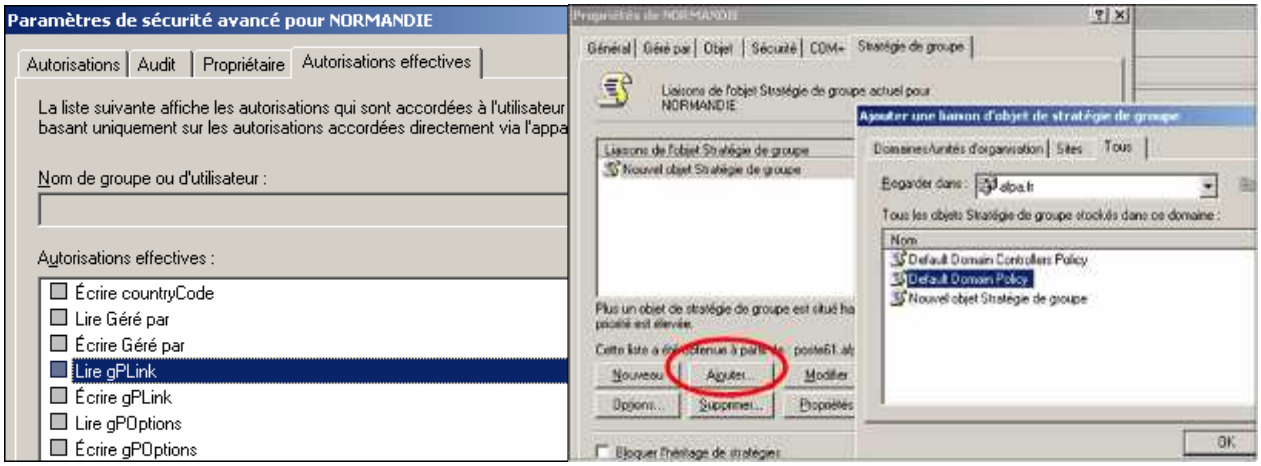
Si vous avez créé des GPO pour des objets d'Active Directory (Site, Domaine, UO), vous pouvez les réutiliser, s'ils conviennent, sur d'autres objets. Il suffit dans l'outil **Sites et Services Active Directory** ou **Utilisateurs et Ordinateurs d'Active Directory** de sélectionner l'objet sur lequel vous voulez appliquer un ou plusieurs GPO, ouvrir les **Propriétés** et dans l'onglet **Stratégie de groupe**, utilisez le bouton **Ajouter**. Vous sélectionnez alors dans la liste de l'onglet **Tous** le ou les GPO que vous voulez appliquer.



Liaison d'une Stratégie de groupe

Un utilisateur peut se voir attribué 3 types de rôles pour gérer des stratégies de groupe.

- **Créer une stratégie de groupe :** doit faire partie du groupe global d'utilisateurs Propriétaires créateurs de la stratégie de groupe.
- **Modifier une stratégie de groupe :** doit avoir le droit d'écrire sur la stratégie de groupe.
- **Lier une stratégie de groupe :** doit avoir les permissions lire écrire sur les propriétés gPlink et gPOptions de l'UO.



8.2.14- Autorisations par défaut d'accès aux GPO

Par défaut un administrateur a tous ces droits :

Groupe de sécurité	Paramètre par défaut
Utilisateurs authentifiés	Lire, Appliquer la stratégie de groupe, autorisations spéciales.
CREATEURS PROPRIETAIRES	Autorisations spéciales.
Admins du domaine	Lire, Ecrire, Créer tous les objets enfants, Supprimer tous les objets enfants, autorisations spéciales.
Administrateurs d'entreprise	Lire, Ecrire, Créer tous les objets enfants, Supprimer tous les objets enfants, autorisations spéciales.
SYSTEM	Lire, Ecrire, Créer tous les objets enfants, Supprimer tous les objets enfants, autorisations spéciales.

8.3- Conseils pour implémenter une stratégie de groupe

- Limiter l'utilisation de :
  - Option **Bloquer l'héritage des stratégies**.
  - Option **Aucun Remplacement**.
  - De la liaison des stratégies de groupe entre domaines.
- Désactiver les arborescences non utilisées (Ordinateur et Utilisateurs).
- Limiter le nombre d'objets GPO.
- Regrouper dans une même stratégie GPO les éléments se rapportant à un même thème.
- ...

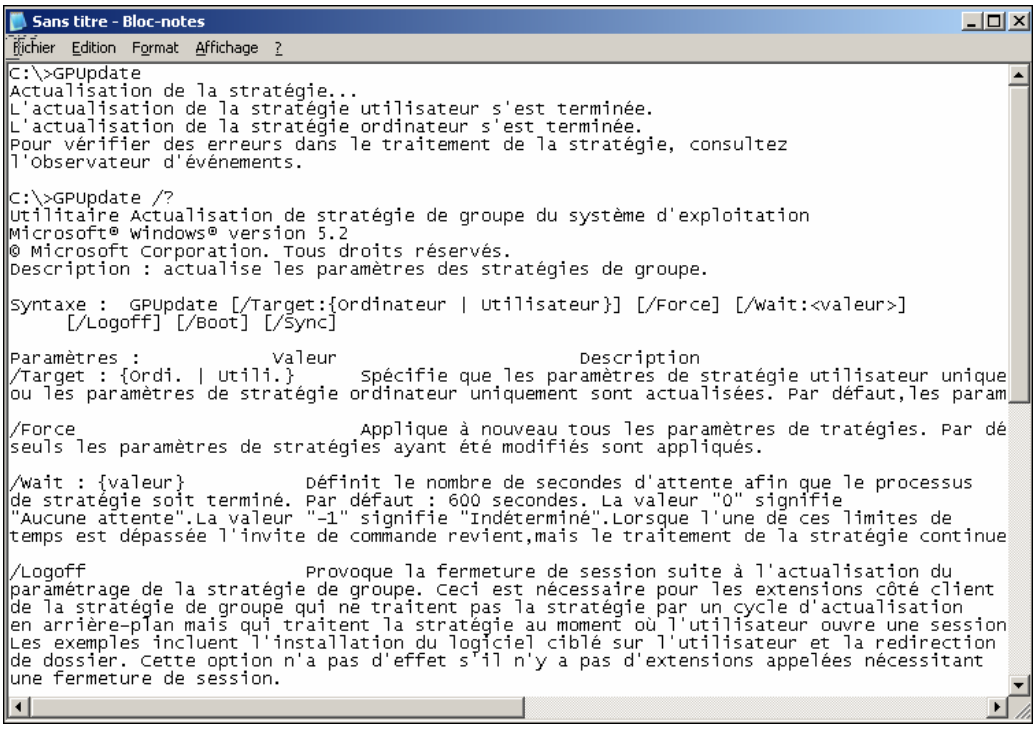
8.4- Commande Gpupdate sous W2003 Server (XP aussi)

8.4.1- gpupdate [/Target:{Computer | User}] [/Force] [/Wait:Value] [/Logoff] [/Boot] [/Sync]

Permet de réappliquer (actualiser) en mode commande les paramètres locaux des stratégies de groupes ou ceux stockés dans Active Directory.
Rappel : par défaut les paramètres sont actualisés toutes les 90 mm sur une station de travail et toutes les 5 mm sur un contrôleur de domaine.

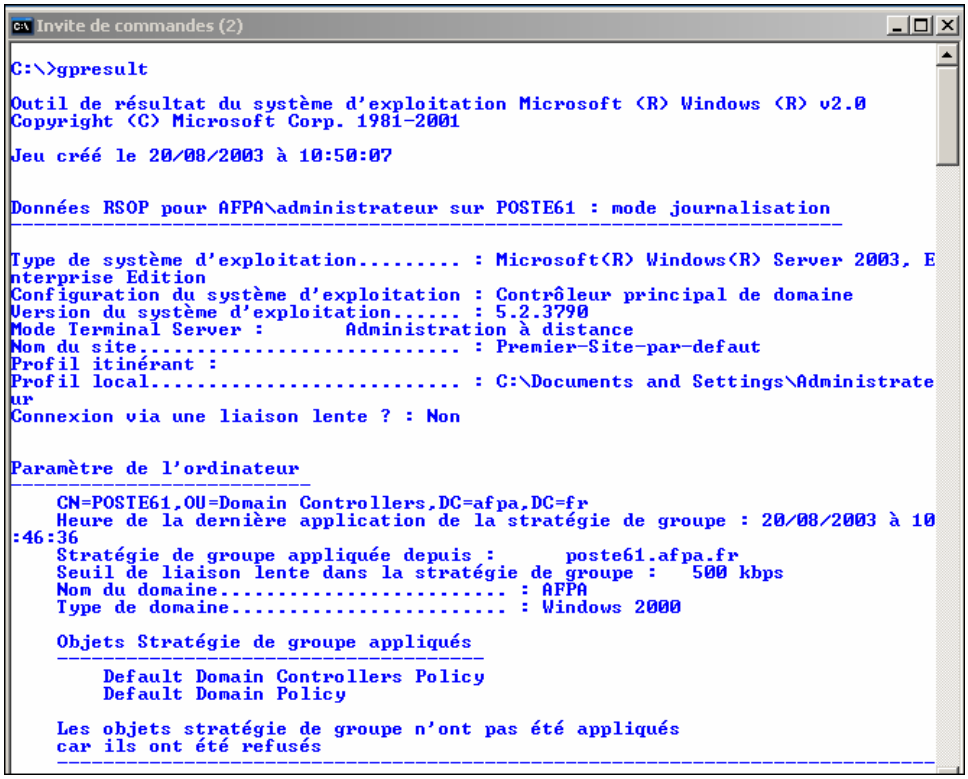
Permet aussi de réaliser des tests et analyses de façon instantanée.
✋ Avec W2000 pour réappliquer les stratégies de groupe, il faut utiliser secedit avec le paramètre refrespolicy. Existe toujours sous W2003 Server pour réaliser des analyses

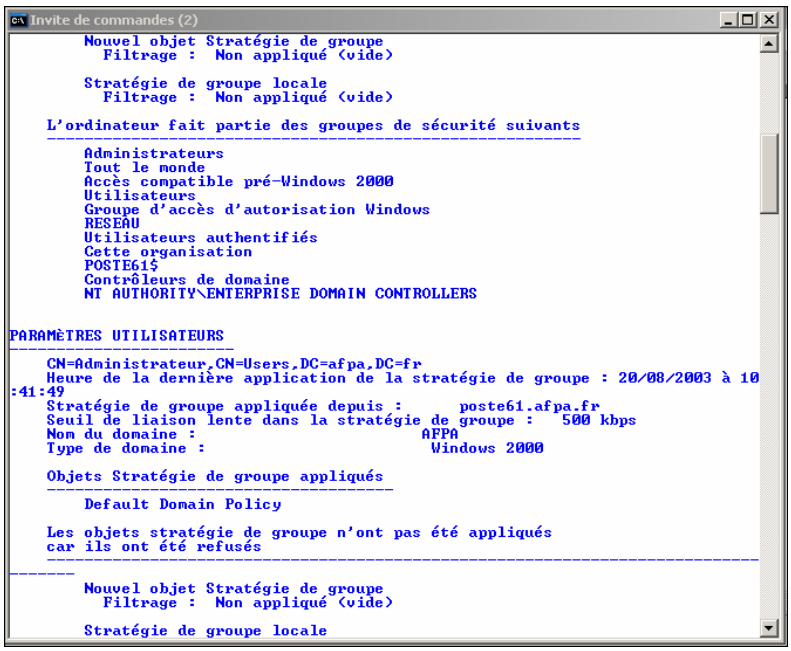
Réactivation en mode commande d'une stratégie de groupe

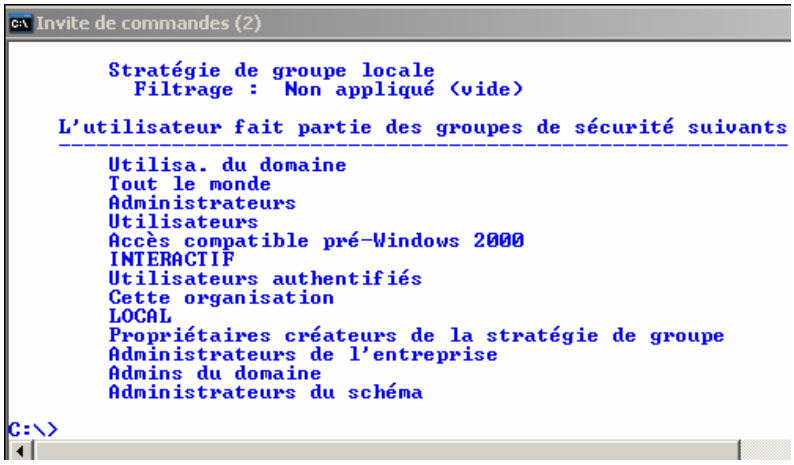


8.4.2- gpresult [/s Computer [/u Domain\User /p Password]] [/user TargetUserName] [/scope {user|computer}] [/v] [/z]

Plusieurs Stratégies pouvant être appliquées, Gpresult affiche le jeu de stratégies résultant appliqué sur l'ordinateur pour l'utilisateur spécifié lors de l'ouverture de session.
Gpresult affiche les paramètres de stratégies de groupe et les données du jeu de stratégies résultant RSoP (Resultant Set of Policy), pour un utilisateur ou un ordinateur.







C:\>gpresult /?

GPRESULT [/S système [/U utilisateur [/P mot_de_passe]]]] [/SCOPE étendue] [/USER utilisateur_cible] [/V | /Z]

Description : cet outil de ligne de commande affiche le jeu de stratégies résultant (RSoP) Information pour ordinateurs et utilisateurs cibles.

Liste de paramètres :

/S système	Spécifie le système distant auquel se connecter.
/U [domaine\]utili.	Spécifie le contexte utilisateur sous lequel cette commande doit s'exécuter.
/P [mot_de_passe]	Spécifie le mot de passe pour le contexte utilisateur donné. Il est demandé s'il est omis.
/SCOPE étendue	Précise si les paramètres de l'ordinateur doivent être affichés. Valeurs autorisées : "USER", "COMPUTER".
/USER [domaine\]utili.	Spécifie le nom d'utilisateur pour lesquelles données RSOP sont affichées.
/V	Indique que les informations détaillées doivent être affichées. Ces informations présentent d'autres paramètres détaillés qui ont été appliqués avec une priorité de 1.
/Z	Spécifie que les informations extrêmement détaillées doivent être affichées. Ces informations présentent d'autres paramètres détaillés qui ont été appliqués avec une priorité de 1 et plus. Ceci vous permet

	de savoir si un paramètre a été appliqué en plusieurs endroits. Consultez l'aide en ligne des stratégies de groupes pour plus de détails.
/?	Affiche cet écran d'aide.

Remarque : si vous exécutez GPRESULT sans paramètre, il renvoie les données RSoP de l'utilisateur en session sur l'ordinateur exécutant le programme.
Exemples :

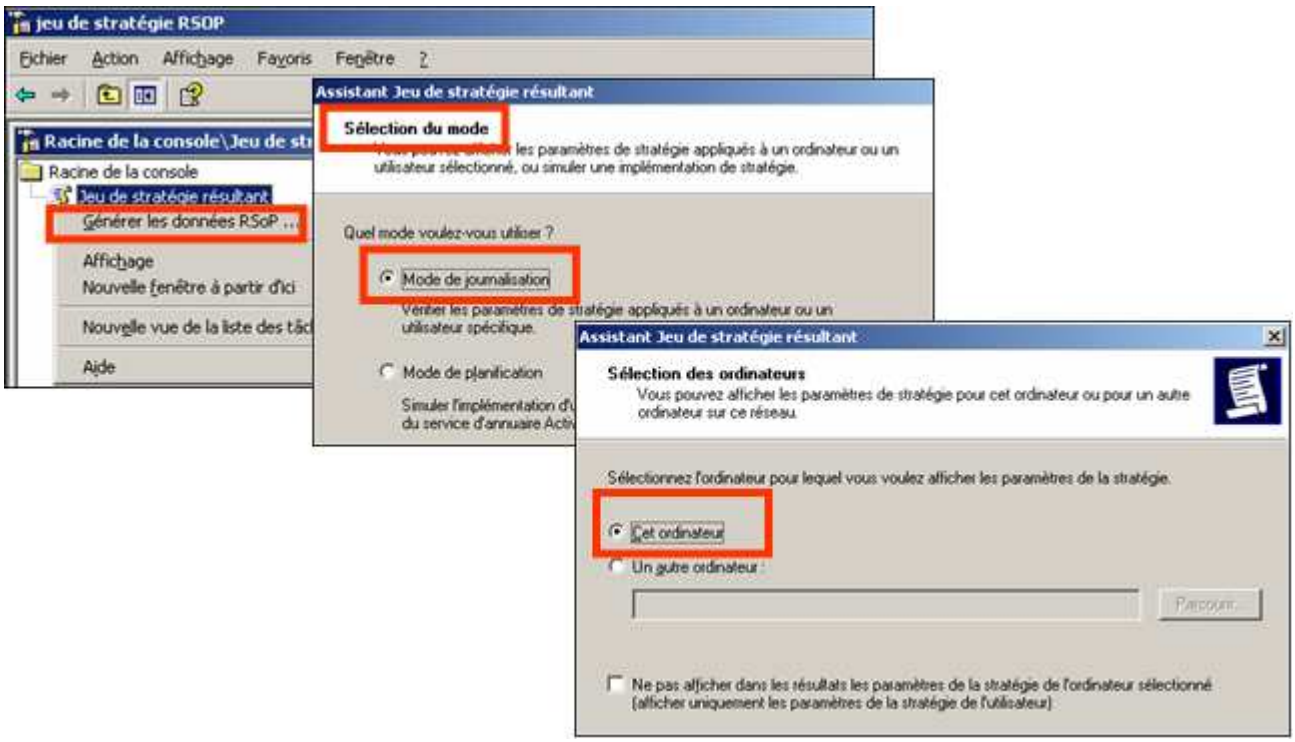
GPRESULT
GPRESULT /USER nom_utilisateur_cible /V
GPRESULT /S système /USER utilisateur_cible /SCOPE ORDINATEUR /Z
GPRESULT /S système /U utilisateur /P mot_de_passe /SCOPE UTILISATEUR /V

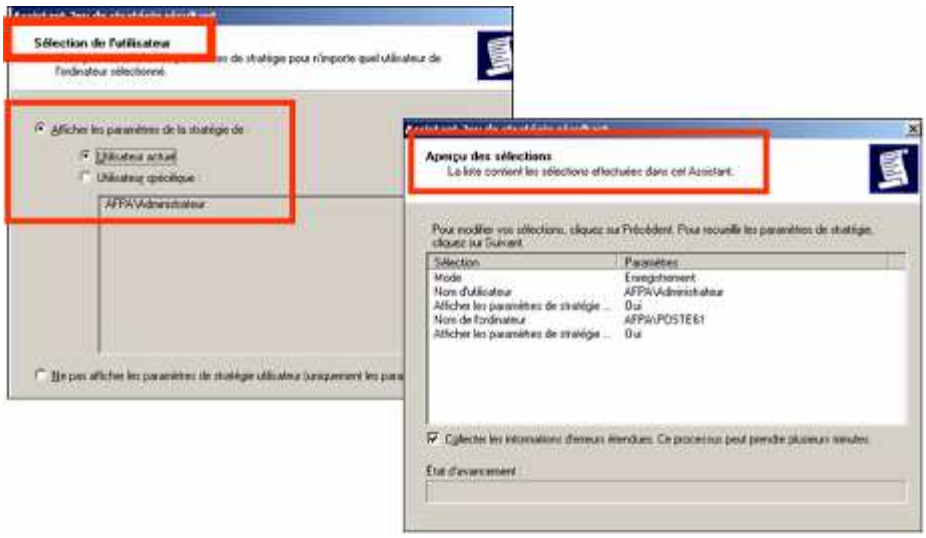
8.5- Utilitaire de W2003 Server de diagnostic de Stratégie - Jeu de Stratégie résultant : RSOP (Resultant Set of Policy)

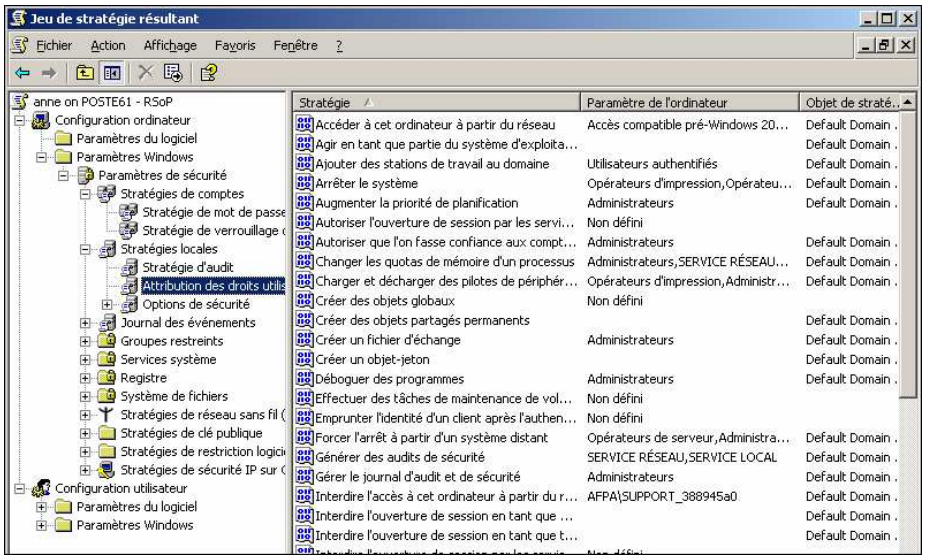
RSOP est un outil intégré à Active Directory permettant de faciliter la gestion bien souvent complexe des stratégies. Il peut calculer et analyser les stratégies appliquées à un utilisateur et/ou un ordinateur cible. Peut être utilisé en 2 modes :

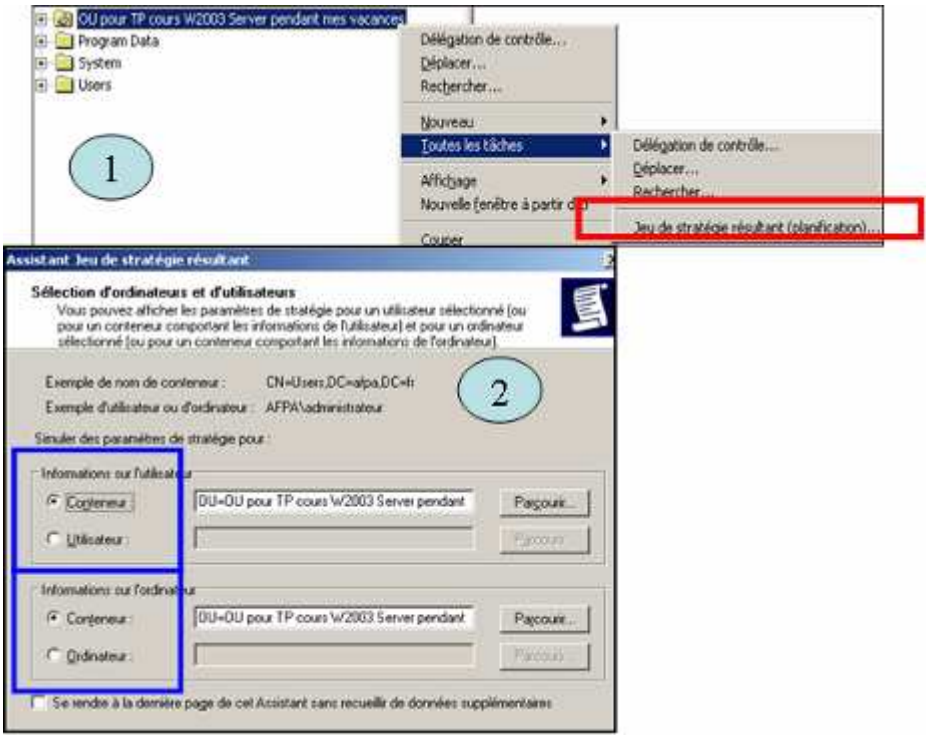
- Mode **journalisation** permettant de voir les paramètres de stratégies effectifs à un moment donné. Mode accessible aux Administrateurs d'entreprise, de domaine et local. Pour ce mode, le client doit être un poste Windows XP ou Win 20003.
- Mode **planification** permettant d'effectuer des simulations en choisissant un ordinateur et un utilisateur et de voir les paramètres de stratégies résultant. Mode accessible aux administrateurs d'entreprise et de domaines. Mode nécessitant un contrôleur de domaine Windows Server 2003, possédant le service nécessaire à cette fonction.

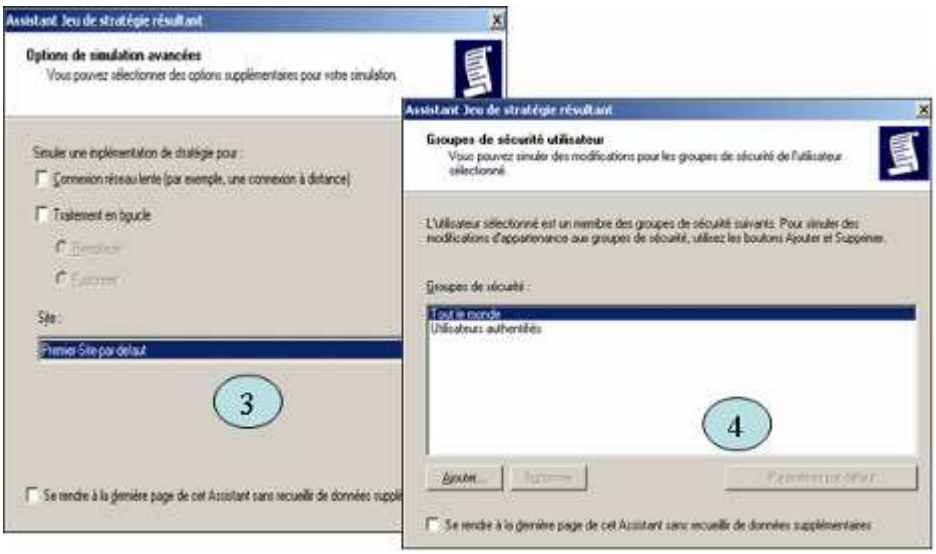
8.5.1- Mode journalisation (enregistrement)



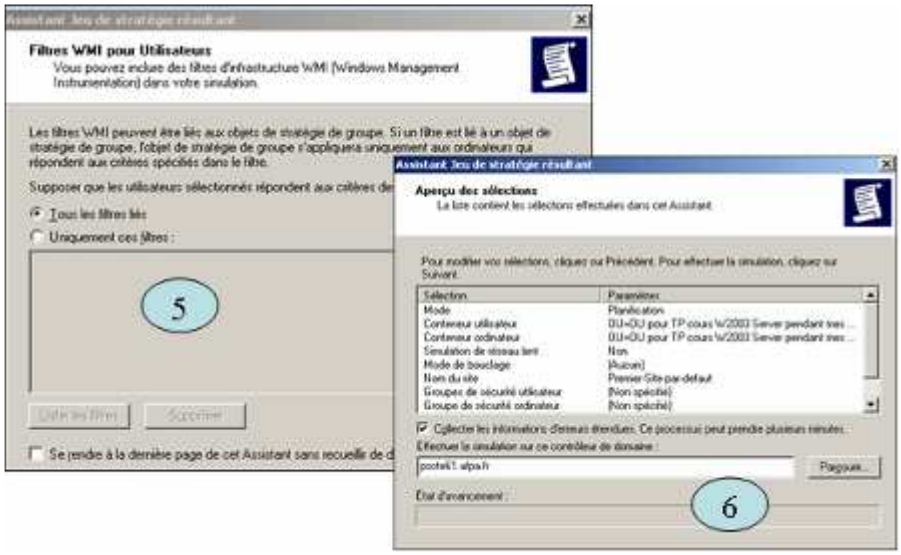

Sélection de l'utilisateur
Afficher les paramètres de la stratégie de :
Utilisateur actuel
Utilisateur spécifique :
AFPA\Administrateur
Aperçu des sélections
Pour modifier vos sélections, cliquez sur Précédent. Pour recueillir les paramètres de stratégie, cliquez sur Suivant.
Sélection
Paramètres
Mode
Enregistrement
Nom d'utilisateur
AFPA\Administrateur
Nom de l'ordinateur
AFPA\POSTE61
Collecte les informations d'erreurs étendues. Ce processus peut prendre plusieurs minutes.
État d'avancement :

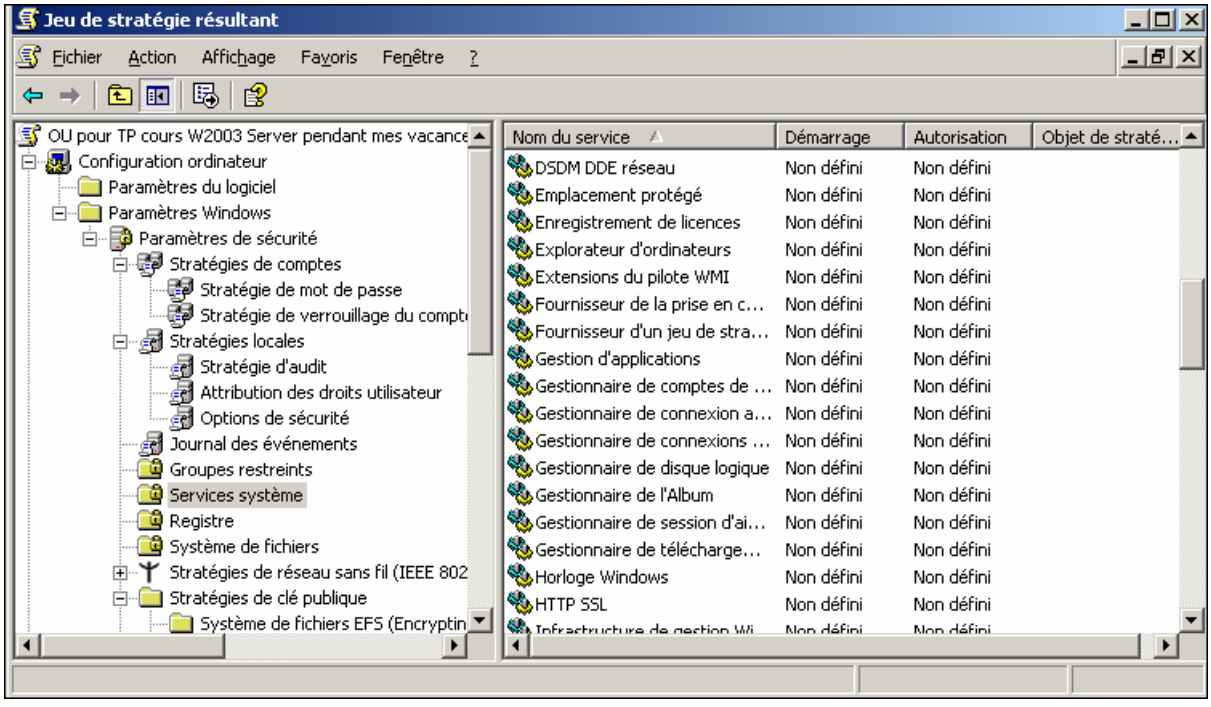

Jeu de stratégie résultant
Fichier Action Affichage Favoris Fenêtre ?
anne on POSTE61 - RSoP
Configuration ordinateur
Paramètres du logiciel
Paramètres Windows
Paramètres de sécurité
Stratégies de comptes
Stratégie de mot de passe
Stratégie de verrouillage
Stratégies locales
Stratégie d'audit
Attribution des droits utilis
Options de sécurité
Journal des événements
Groupes restreints
Services système
Registre
Système de fichiers
Stratégies de réseau sans fil
Stratégies de clé publique
Stratégies de restriction logici
Stratégies de sécurité IP sur
Configuration utilisateur
Paramètres du logiciel
Paramètres Windows
Stratégie
Paramètre de l'ordinateur
Objet de straté...
Accéder à cet ordinateur à partir du réseau
Accès compatible pré-Windows 20...
Default Domain
Agir en tant que partie du système d'exploita...
Ajouter des stations de travail au domaine
Utilisateurs authentifiés
Arrêter le système
Opérateurs d'impression,Opérateu...
Augmenter la priorité de planification
Administrateurs
Autoriser l'ouverture de session par les servi...
Non défini
Autoriser que l'on fasse confiance aux compt...
Administrateurs
Changer les quotas de mémoire d'un processus
Administrateurs,SERVICE RÉSEAU...
Charger et décharger des pilotes de périphér...
Opérateurs d'impression,Administr...
Créer des objets globaux
Non défini
Créer des objets partagés permanents
Créer un fichier d'échange
Administrateurs
Créer un objet-jeton
Déboguer des programmes
Administrateurs
Effectuer des tâches de maintenance de vol...
Non défini
Emprunter l'identité d'un client après l'authen...
Non défini
Forcer l'arrêt à partir d'un système distant
Opérateurs de serveur,Administra...
Générer des audits de sécurité
SERVICE RÉSEAU,SERVICE LOCAL
Gérer le journal d'audit et de sécurité
Administrateurs
Interdire l'accès à cet ordinateur à partir du r...
AFPA\SUPPORT_388945a0
Interdire l'ouverture de session en tant que ...
Interdire l'ouverture de session en tant que t...


OU pour TP cours W2003 Server pendant mes vacances
Program Data
System
Users
1
Délégation de contrôle...
Déplacer...
Rechercher...
Nouveau
Toutes les tâches
Affichage
Nouvelle fenêtre à partir d'ici
Couper
Délégation de contrôle...
Déplacer...
Rechercher...
Jeu de stratégie résultant (planification)...
Assistant Jeu de stratégie résultant
Sélection d'ordinateurs et d'utilisateurs
Vous pouvez afficher les paramètres de stratégie pour un utilisateur sélectionné (ou pour un conteneur comportant les informations de l'utilisateur) et pour un ordinateur sélectionné (ou pour un conteneur comportant les informations de l'ordinateur).
Exemple de nom de conteneur : CN=Users,DC=afpa,DC=fr
Exemple d'utilisateur ou d'ordinateur : AFPA\administrateur
2
Simuler des paramètres de stratégie pour :
Informations sur l'utilisateur
Conteneur :
OU=OU pour TP cours W2003 Server pendant
Parcourir...
Utilisateur :
Informations sur l'ordinateur
Conteneur :
OU=OU pour TP cours W2003 Server pendant
Parcourir...
Ordinateur :
Se rendre à la dernière page de cet Assistant sans recueillir de données supplémentaires



8.5.2- Mode Planification





8.6- Group Policy Management Consol – GPMC

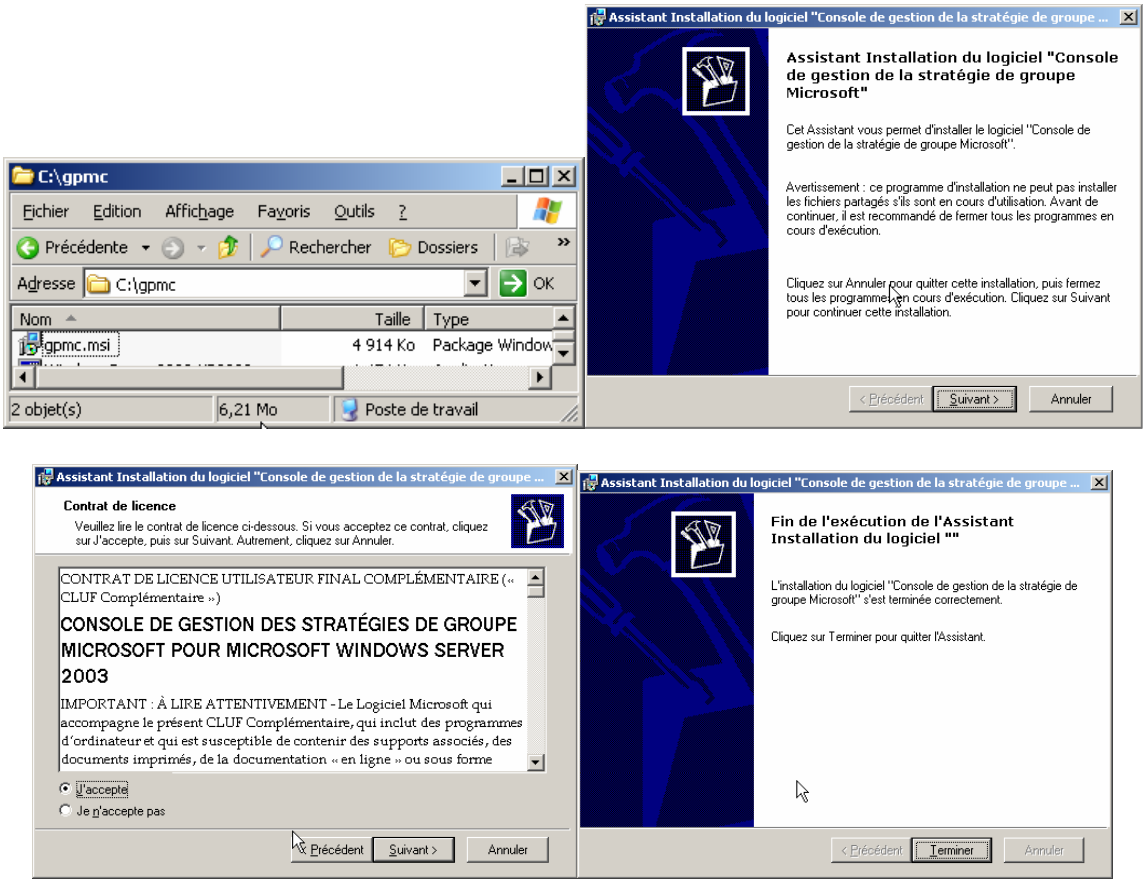
La console GPMC est un outil graphique qui simplifie la gestion de la stratégie de groupe en facilitant la compréhension, le déploiement, la gestion et la résolution des problèmes de mise en œuvre de la stratégie de groupe. Elle permet aussi une automatisation des opérations de la stratégie de groupe à l'aide de scripts. Elle permet aussi de faire les simulations déjà réalisées avec RSOP, Group Policy Modeling pour le mode planification et Group Policy Result pour le mode journalisation. En résumé cette console vous permet de :

- Créer, supprimer, lier éditer des stratégies de groupes.
- Gérer l'héritage, les filtrages, la délégation des stratégies de groupes.
- Réaliser des simulations comme avec les jeux de stratégies résultant RSoP.
- Créer des rapports au format HTML.
- Réaliser des sauvegardes, restauration de stratégies.
- Copier coller de stratégies.
- Importer des paramètres.

GPMC n'est pas disponible (à ce jour) en standard ni même sur le CD de W2003, mais sur le site de Microsoft en téléchargement sous forme de fichier gpmc.msi. Configuration minimale :

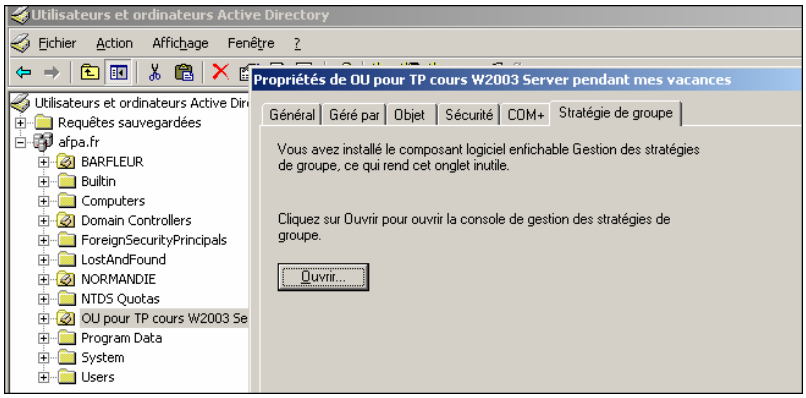
- La console GPMC s'exécute sur Windows XP Professionnel SP1 avec .NET Framework installé. Ainsi que sur Windows Server 2003 (.Net Framework installé en standard).
- Peut gérer une stratégie de groupe dans les domaines W2000 (SP2 ou SP3) ou W2003 Server.
- Attention, dès que GPMC est installé l'onglet Stratégie de Groupe ne permet plus de gérer les stratégies mais vous exécuterez GPMC.

GPMC - Installation

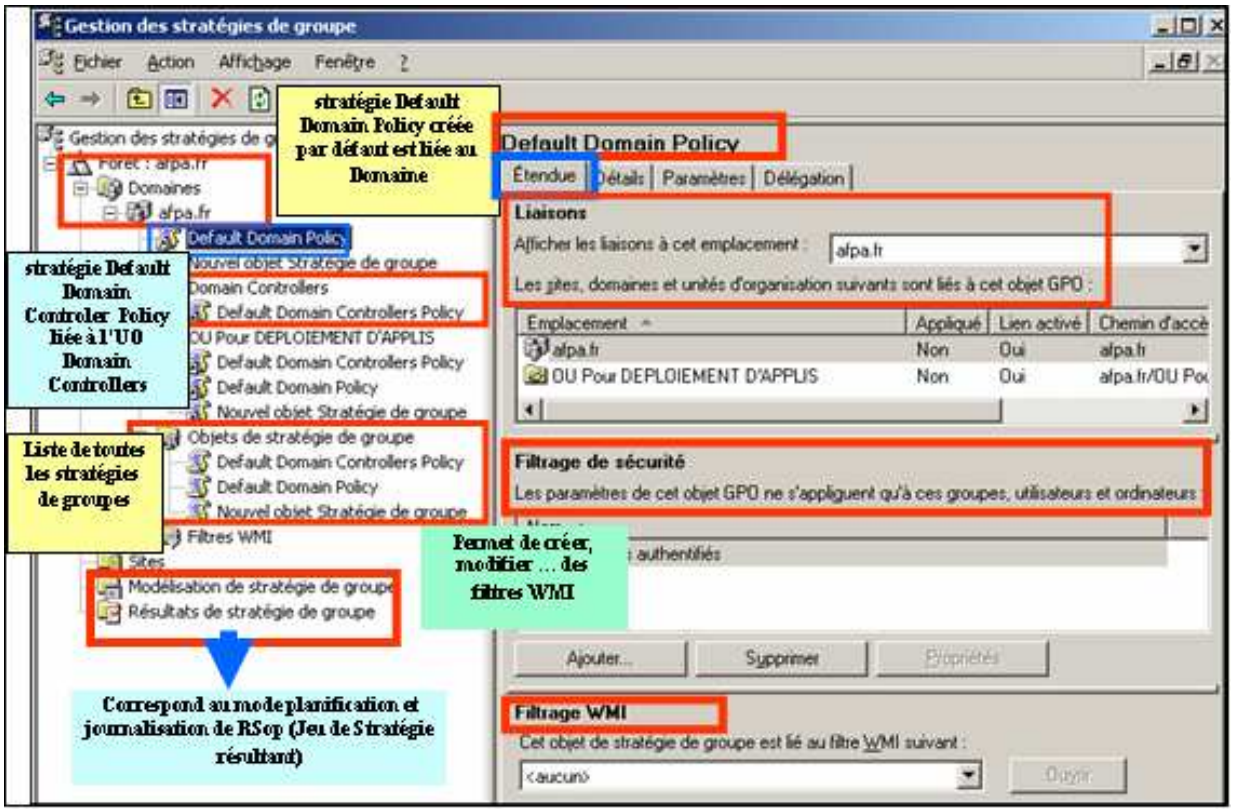


Après installation une console supplémentaire est disponible dans les **Outils d'Administration** :

8.6.1- Group Policy Management Consol : exécution

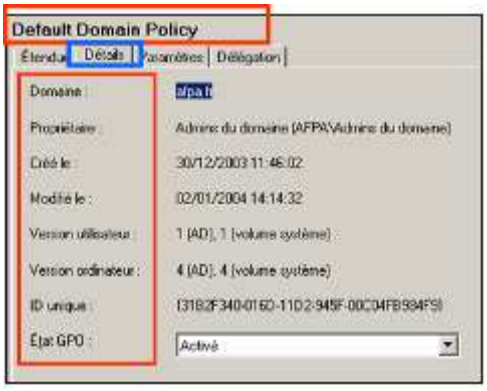


8.6.2- Utilisation de GPMC : étendue



8.6.3- Utilisation de GPMC : détails

N° de version de la stratégie, son GUID et son état d'Activation.

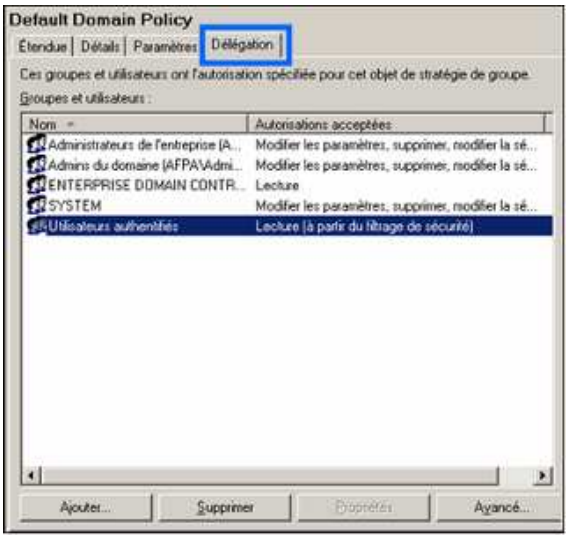


8.6.4- Utilisation de GPMC : paramètres

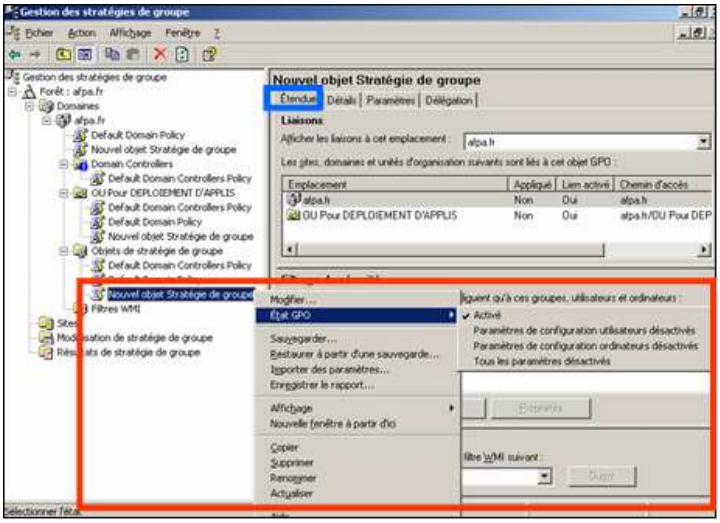
Affichage au format HTML des paramètres effectifs de la stratégie.

8.6.5- Utilisation de GPMC : délégation

Permet de voir et modifier les permissions appliquées à cette stratégie.

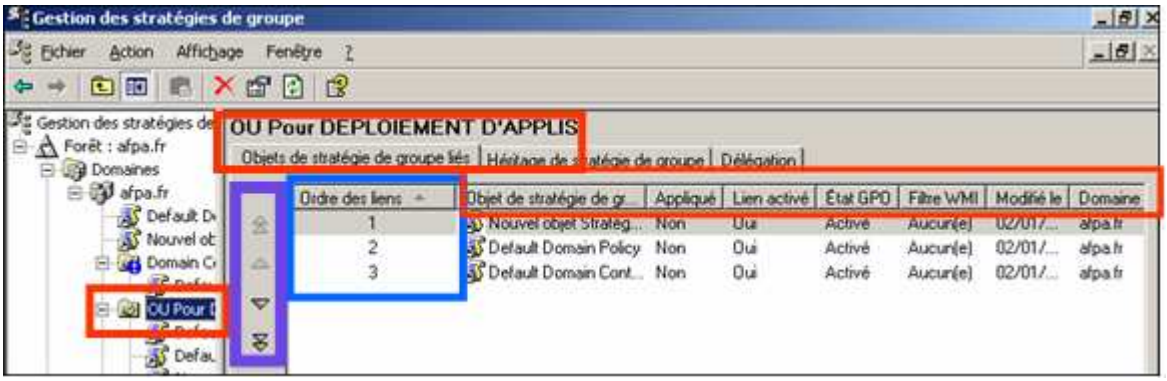


8.6.6- Utilisation de GPMC : paramétrage/options



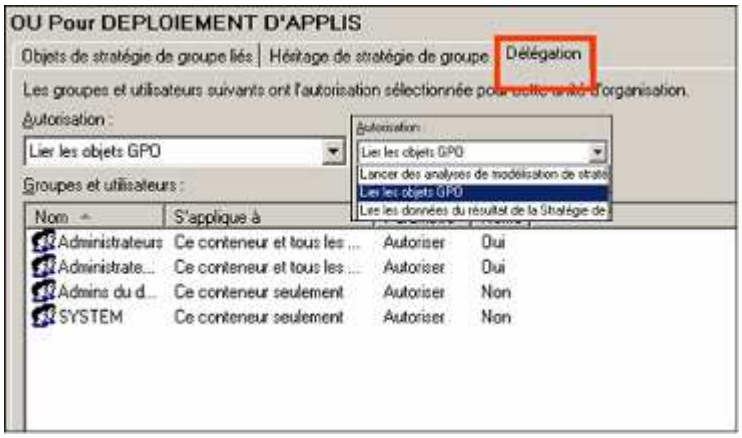
8.6.7- Utilisation de GPMC : propriétés d'un container

Affichage de la liste des stratégies de groupe liée à l'Unité Organisationnelle sélectionnée. Possibilité de modifier leur ordre de priorité en cliquant sur les flèches.



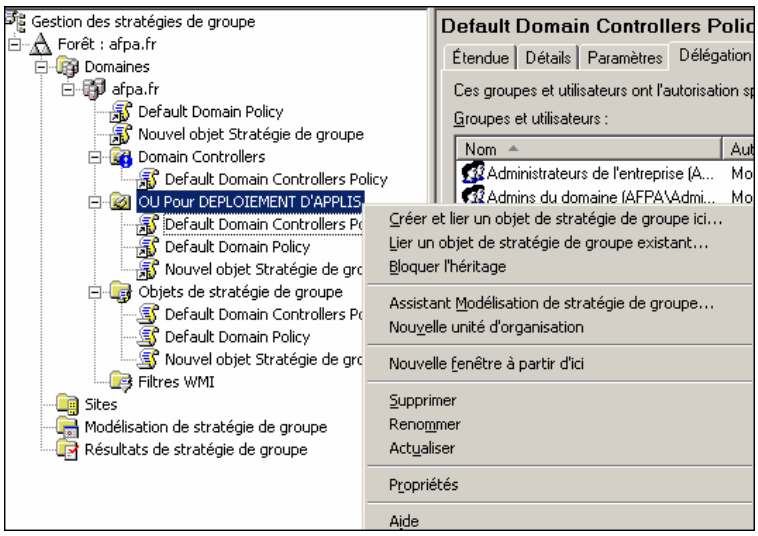
Liste de toutes les stratégies de groupe s'appliquant à l'OU. La colonne **Emplacement** donne le container auquel est liée la stratégie.

Visualisation et modification des autorisations de groupes d'utilisateurs pour l'OU.

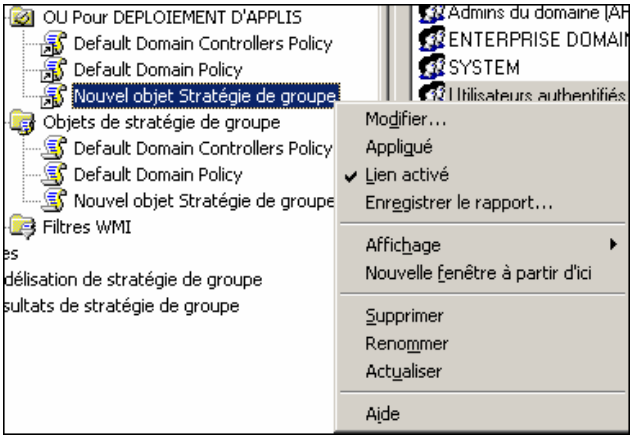


8.6.8- Utilisation de GPMC : propriétés d'une OU créée

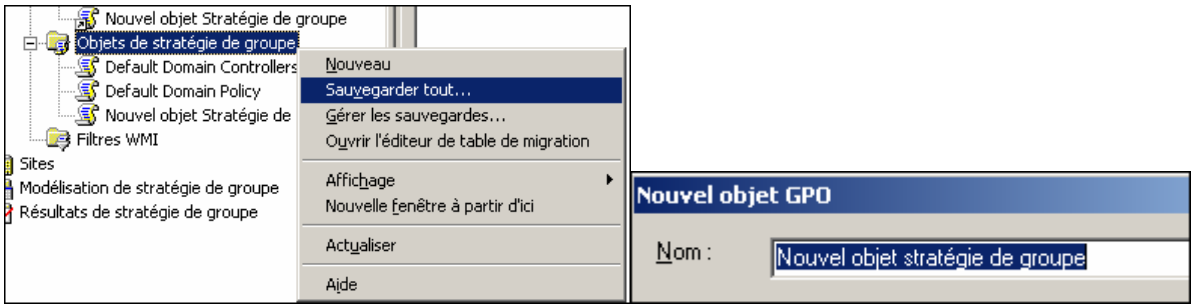
Les options proposées permettent de créer des objets de stratégie de groupe, de lier des objets de stratégie de groupe existants, bloquer l'héritage, réaliser des simulations avec l'**Assistant Modélisation de Stratégie de groupe**.



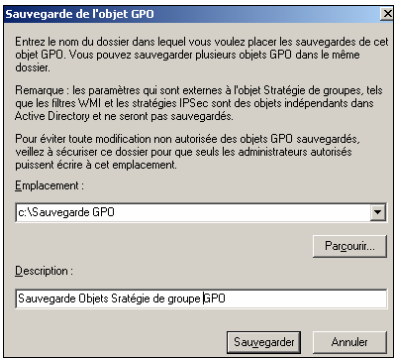
L'option **Appliqué** correspond à la propriété désignée **Ne pas passer outre** ou **Aucun remplacement**.



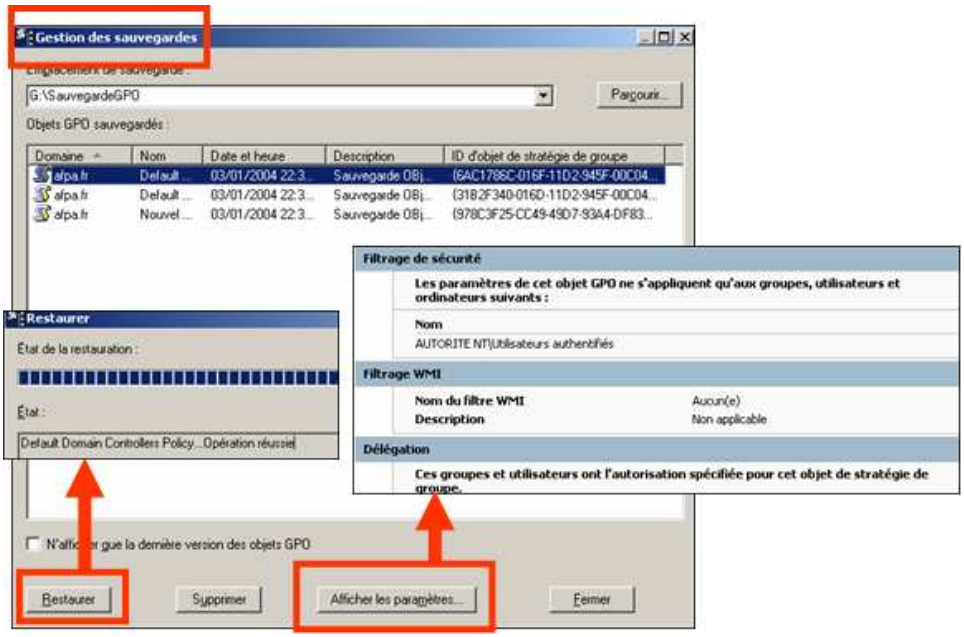
8.6.9- Utilisation de GPMC : propriétés d'une OU sous le container à traiter



8.6.10- Utilisation de GPMC : sauvegarde d'une stratégie de Groupe

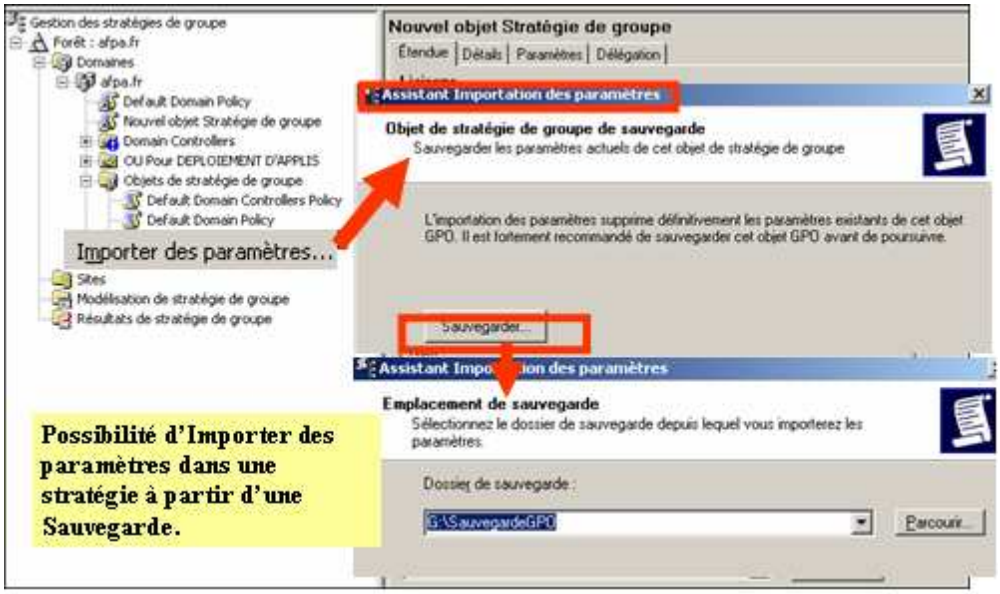


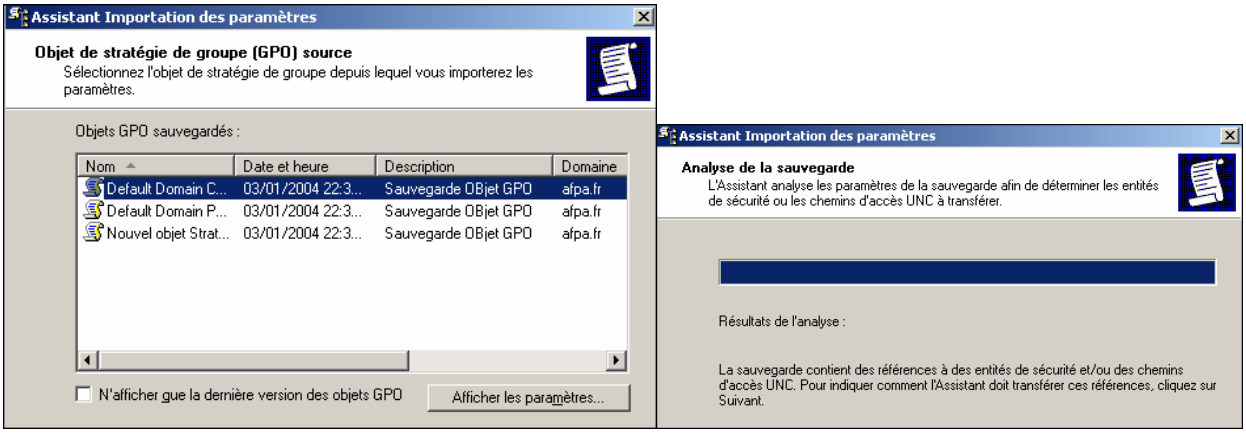
8.6.11- Utilisation de GPMC : gestion d'une Sauvegarde

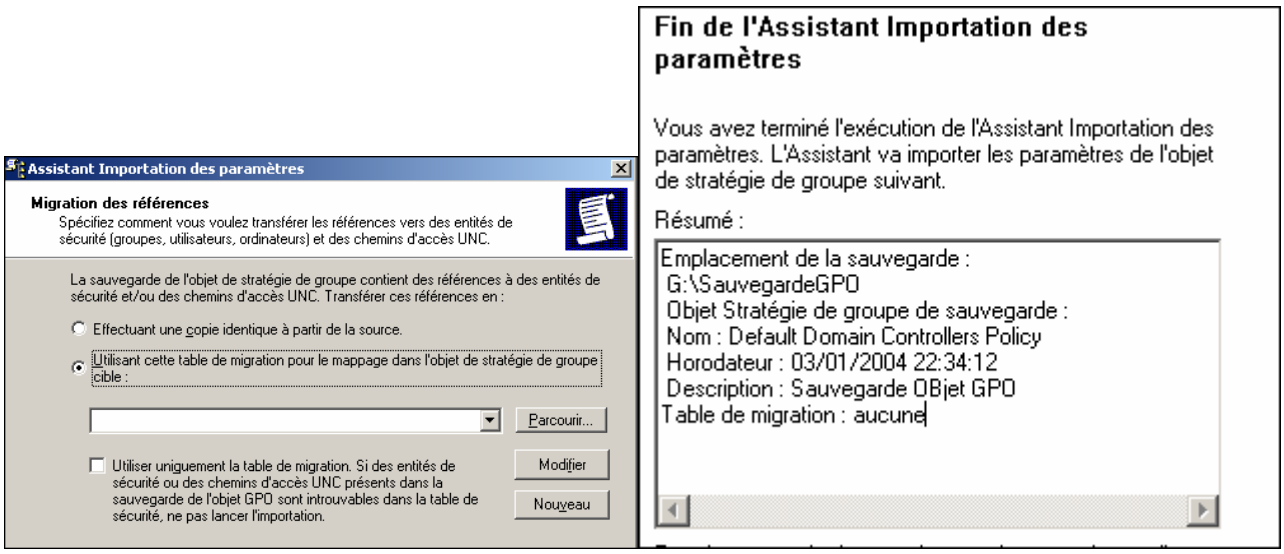


8.6.12- Utilisation de GPMC : importer des paramètres

Possibilité d'importer des paramètres dans une stratégie à partir d'une sauvegarde.

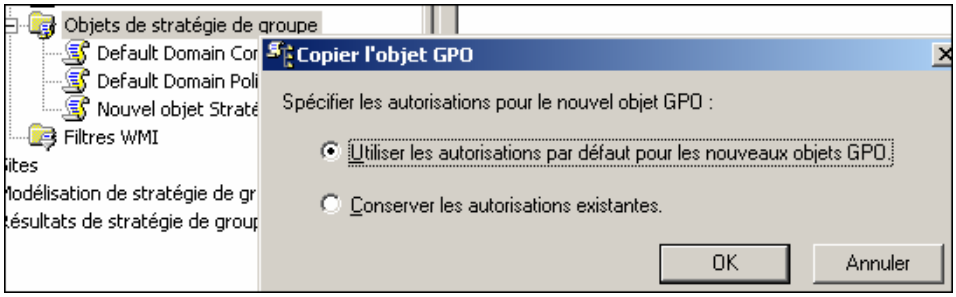






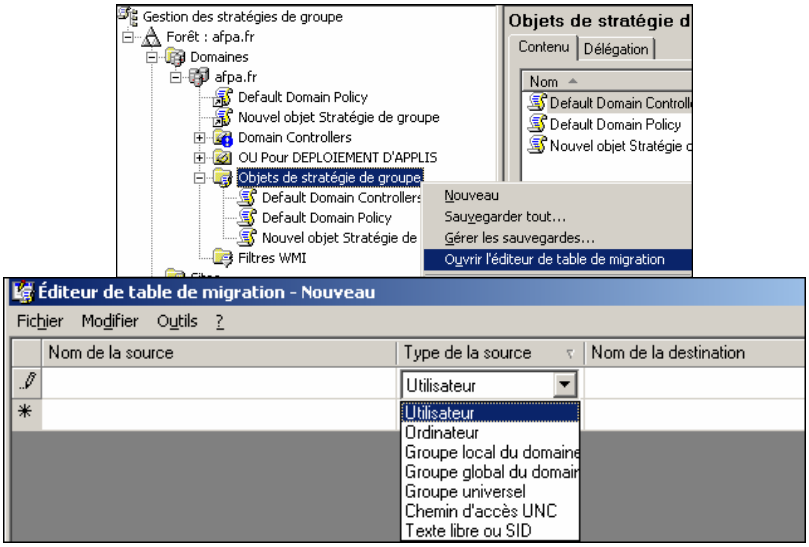
8.6.13- Utilisation de GPMC : copier/Coller une Stratégie de Groupe

Possibilité de créer une nouvelle stratégie de groupe par copie d'une stratégie de groupe existante.

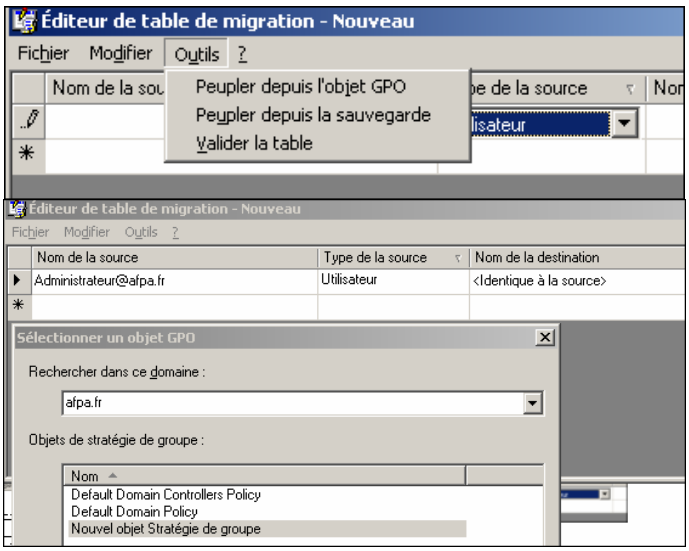


8.6.14- Utilisation de GPMC : tables de Migration

Lors de certaines opérations comme l'importation de paramètres, il peut être nécessaire de modifier certains paramètres se référant à des comptes utilisateurs ou groupes. La table de migration GPMC le permet.



Principe : saisie de la référence de la stratégie de groupe source puis le paramètre correspondant dans la stratégie de destination.



8.7- Déploiement d'applications

8.7.1- Publication et attribution

- Les stratégies de groupe permettent de distribuer des applications ou services packs à des utilisateurs ou ordinateurs.
- C'est une fonctionnalité de W2003 Server/2000 nommée Intellimiror.
- Nécessite un package interprétable par la technologie Windows Installer.
- Service installé par défaut à partir de W2000 ou plus.
- Fichier en général portant l'extension MSI (avec fichiers nécessaires à l'installation de l'application).
- Permet de maintenir et d'installer des applications.
- Les Applications sont capables de se désinstaller complètement et proprement.
- Permet l'installation de nouveaux composants d'applications à la demande d'un utilisateur.
- Permet aussi de réparer des fichiers manquants ou corrompus et cela sans l'intervention de l'utilisateur.
- Recherche automatique des fichiers sur les sources de l'installation.
- Déploiement de logiciel par une stratégie de groupe, facilite la gestion de la sécurité des utilisateurs.
- Les applications utilisées avec les stratégies de groupes s'installent automatiquement en prenant les droits utilisateurs nécessaires à leur installation.

8.7.2- Déploiement d'une application

- Les applications peuvent être déployées au niveau utilisateur et au niveau ordinateur.
- Les distributions des logiciels sont obligatoirement stockées dans des dossiers partagés accessibles aux utilisateurs concernés par le déploiement. Le droit lecture est suffisant.

Étape 1 ➔ Obtenir ou créer un package Windows Installer.
Étape 2 ➔ Stocker le lot dans un répertoire partagé (avec des permissions suffisantes).
Étape 3 ➔ Créer ou modifier une GPO (stratégie de groupe) pour la distribution de l'application.
Étape 4 ➔ Sélectionner une méthode de déploiement.

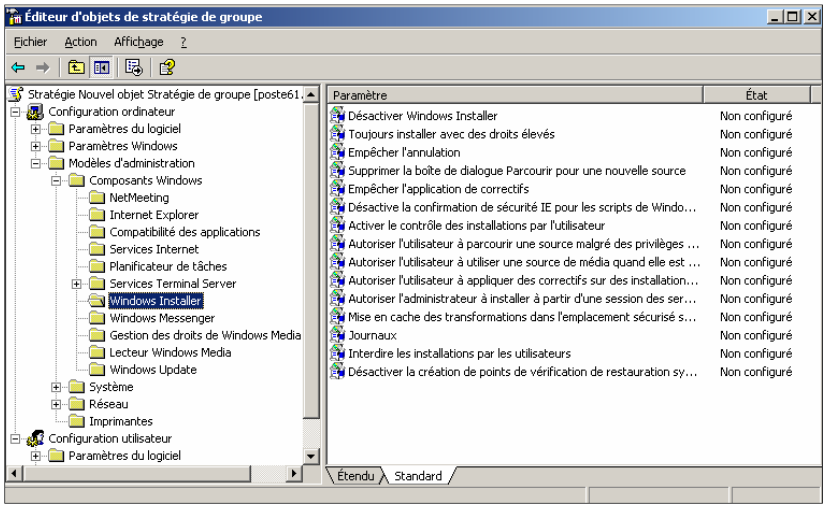
Préparation

- Acquisition de fichiers lots (.msi) auprès d'un revendeur de logiciels, contenant les instructions et informations nécessaires pour installer, modifier et désinstaller le programme.
- Créer un lot en utilisant un logiciel de packaging (packager une application). WinInstall de Veritas par exemple.
- Créer un fichier texte avec l'extension .zap (pour fichiers autres que .msi) : modification du fichier lot.
- Créer un fichier de modification (extension .MST) permettant une configuration spécifique d'une application déployée avec un .MSI.

Phase de déploiement : les logiciels sont installés sur les ordinateurs W2003.
Phase de maintenance : facilité de la mise à niveau ou du redéploiement de logiciels. Il n'est plus nécessaire d'intervenir sur chaque poste de travail pour y installer un Service Pack.
Phase de suppression : deux méthodes automatiques de suppression possible : suppression automatique à la prochaine mise sous tension (stratégie d'ordinateur) ou à la prochaine ouverture de session (stratégie utilisateur).

8.7.3- Stratégie de groupe pour Windows Installer

Stratégie de groupe ➔ Configuration ordinateur ➔ Modèles d'administration ➔ Composants Windows ➔ Windows Installer.

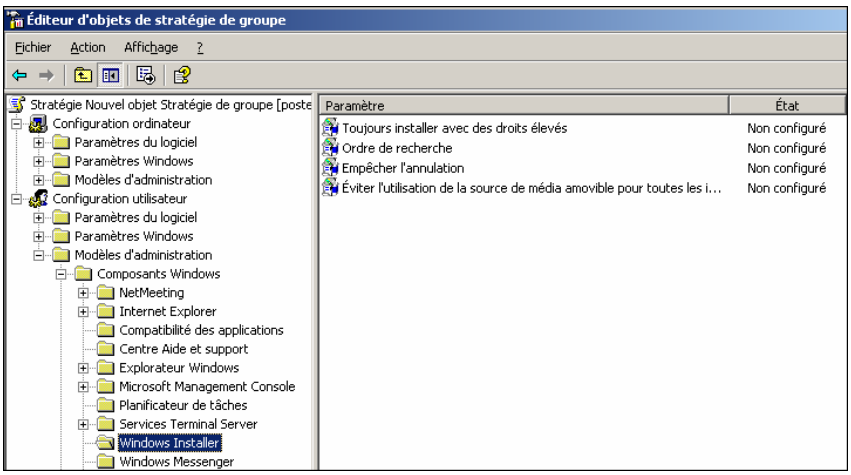


Configuration ordinateur

Désactivez Windows Installer : restriction de l'utilisation de Windows Installer. Les utilisateurs ne peuvent installer un logiciel sur leur système ou ne peuvent installer que les programmes publiés par un administrateur.
Toujours installer avec des droits élevés : stratégie permettant à l'utilisateur d'installer des programmes nécessitant l'accès à des répertoires qu'il n'a pas habituellement le droit d'ouvrir ou de modifier.
Empêcher l'application des correctifs : invalide l'installation de correctifs pour la mise à niveau des programmes par les utilisateurs.
Activer le contrôle des installations par l'utilisateur : permet la modification des options d'installation réservées habituellement aux administrateurs par les utilisateurs eux-mêmes.

Configuration utilisateur

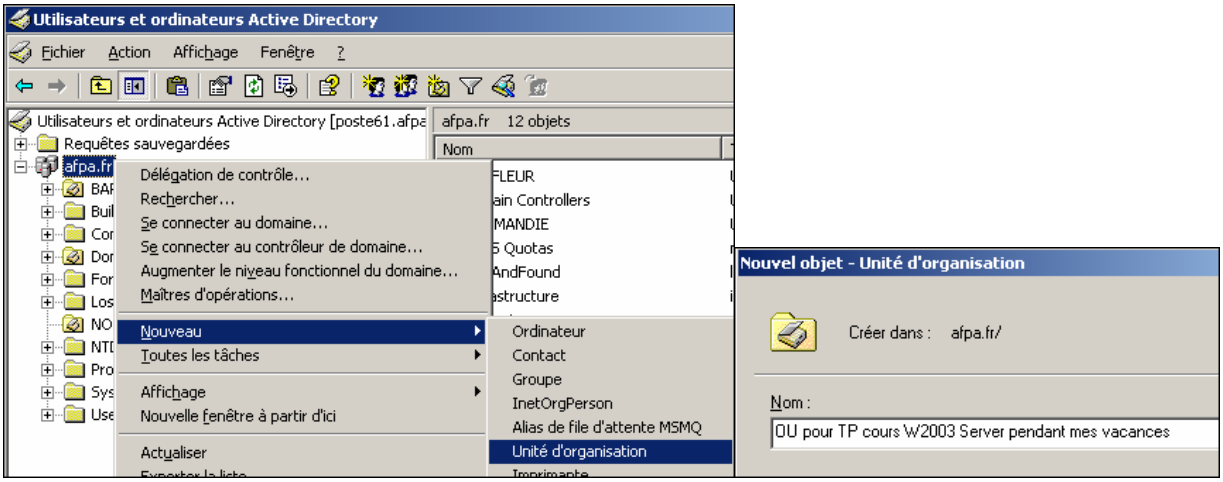
Stratégie de groupe ➔ configuration utilisateur Modèles d'administration ➔ Composants Windows ➔ Windows Installer.



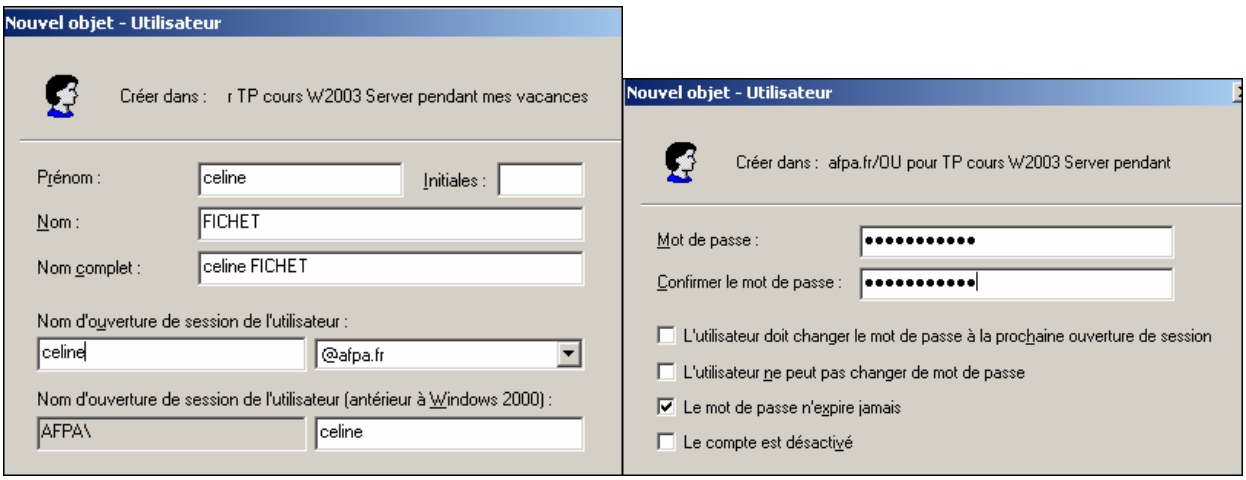
Stratégie de groupe pour Windows Installer
Configuration utilisateur

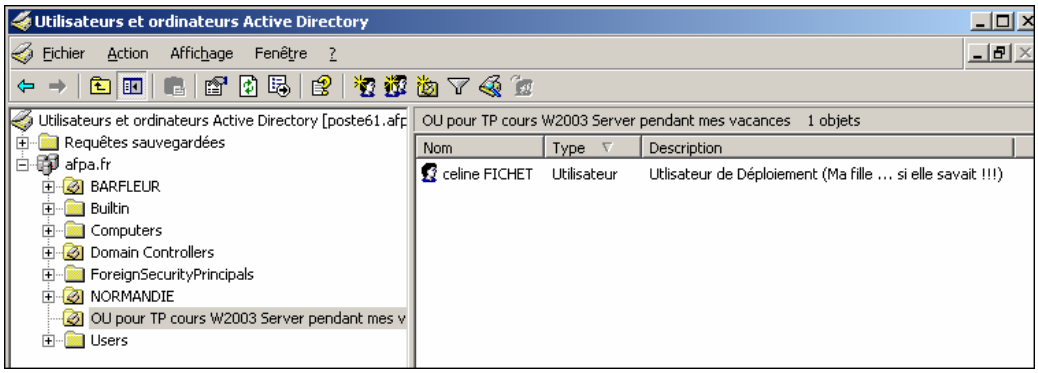
- Toujours installer avec des droits élevés : les utilisateurs avancés peuvent modifier leurs autorisations afin d'obtenir un accès permanent à des dossiers et fichiers sensibles.
- Ordre de recherche : indique l'ordre de recherche pour les fichiers d'installation de Windows Installer.
- Désactiver l'annulation : permet le retour sur une installation interrompue ou ayant échouée.
- Désactiver la source de média pour toutes les installations : interdit l'installation de programmes à partir de média amovibles.

8.8- Création d'une nouvelle stratégie au niveau du site, du domaine ou d'une unité organisationnelle



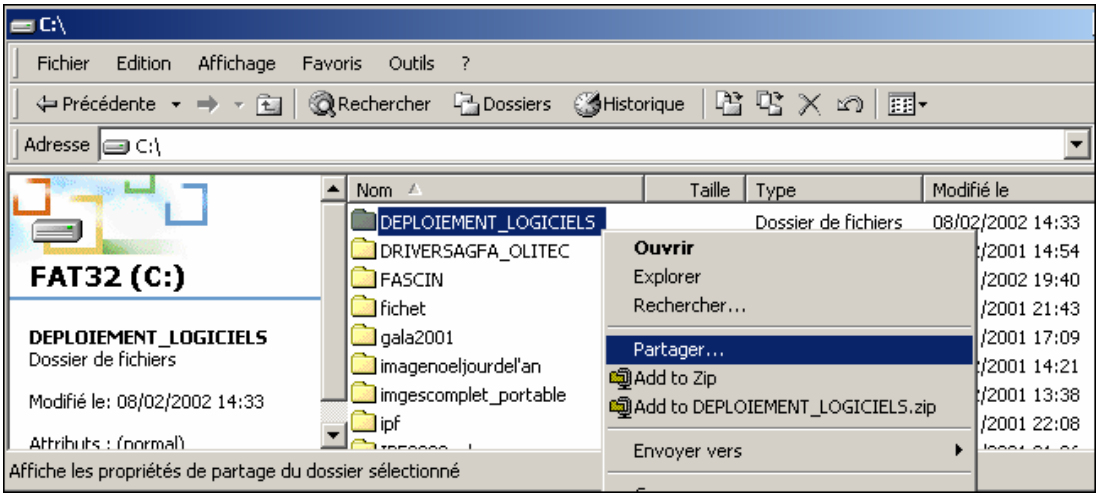
8.8.1- Création d'un nouvel utilisateur chargé du déploiement d'applications

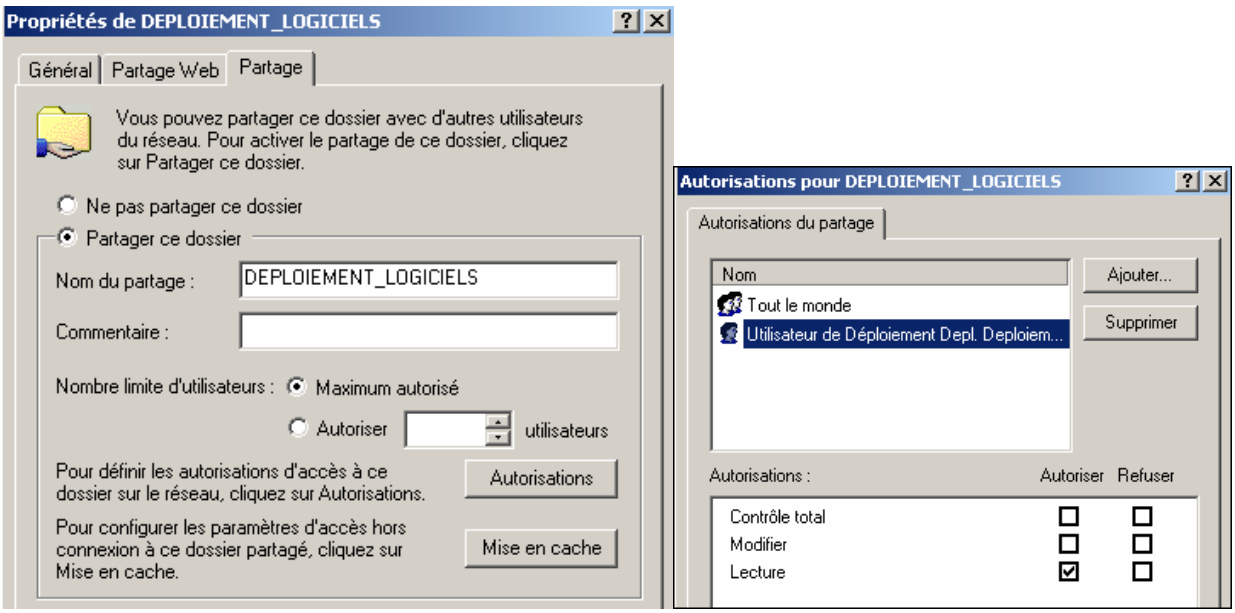




8.8.2- Création d'un partage

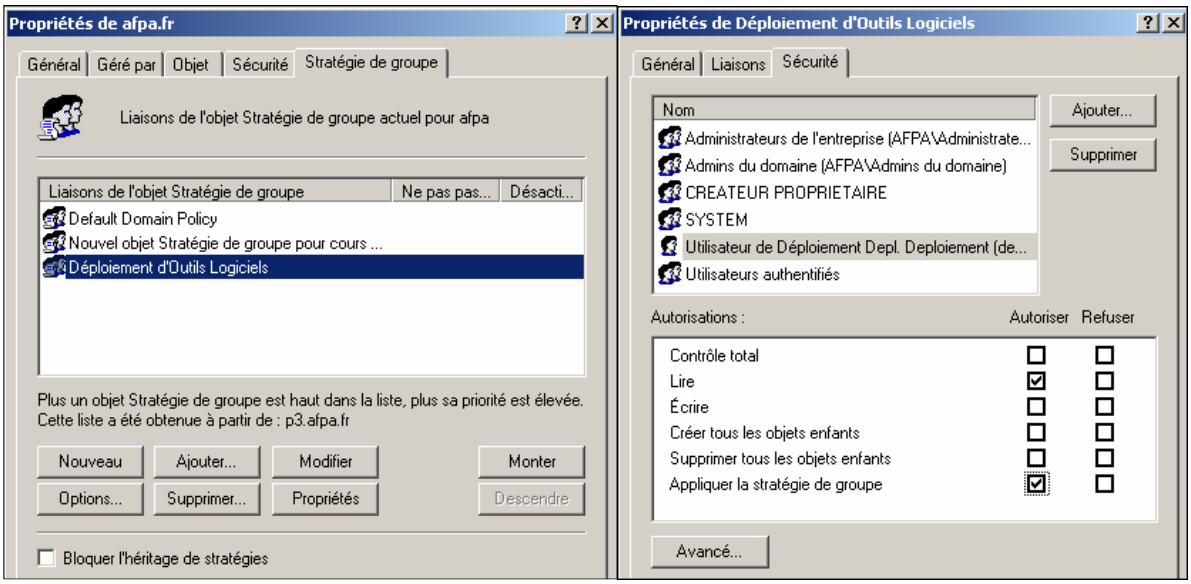
Création d'un partage accessible par le ou les utilisateurs concernés par le déploiement d'applications.

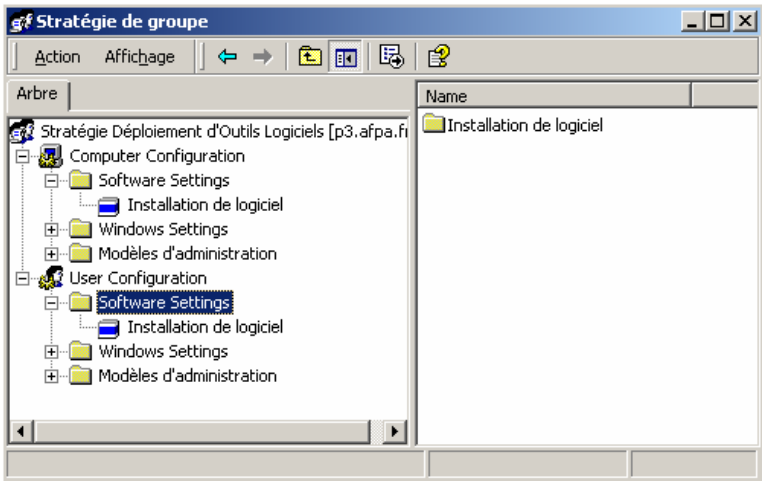




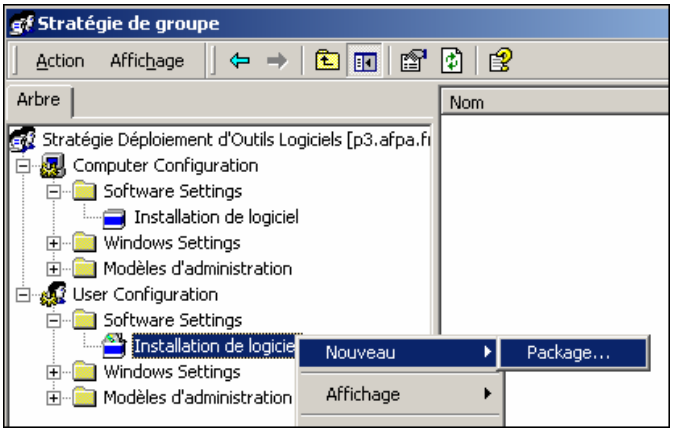
8.8.3- Créer la stratégie de déploiement

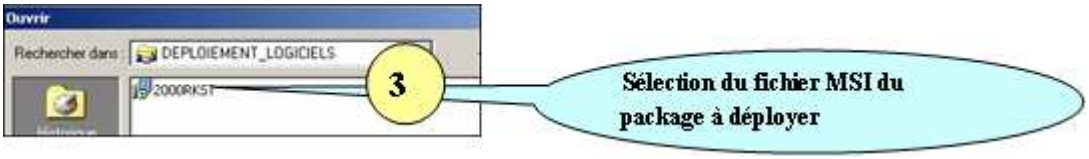
Ajouter l'utilisateur chargé du déploiement en lui affectant à lui seul l'autorisation **Appliquer la stratégie de groupe**.

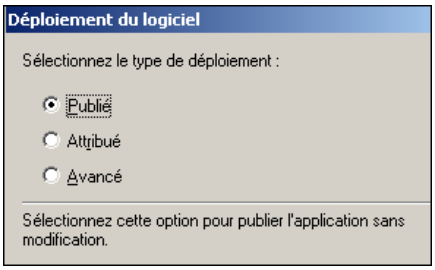




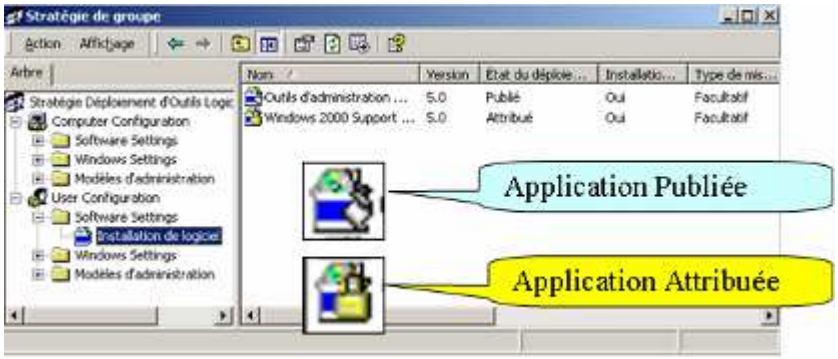
Clic droit sur **Installation du logiciel** sous **Configuration ordinateur** pour déployer les logiciels sur des ordinateurs quelque soit la personne qui les utilise ou sur **Configuration utilisateur** pour le déploiement des logiciels pour les utilisateurs qu'importe la machine utilisée. Clic sur **Nouveau ➔ Package.**



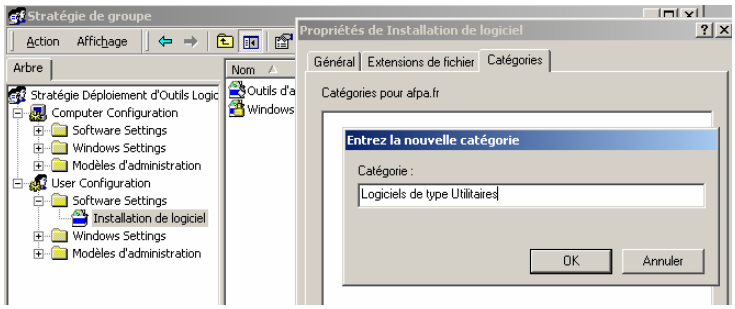




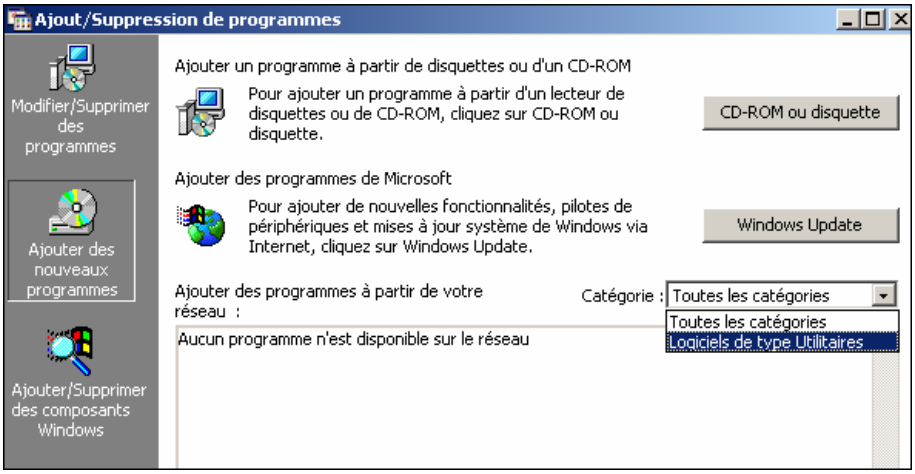
Publication : avec ce choix, l'application sera signalée dan le composant **Ajout/Suppression de programmes** du **Panneau de Configuration**. L'utilisateur doit l'installer explicitement ou en double-cliquant sur un fichier dont l'extension est associée au programme publié (automatique). La publication s'applique à un utilisateur et pas pour un ordinateur.
Application : avec ce choix l'application est indiquée à l'utilisateur par une icône sur le bureau ou dans le menu **Démarrer** sans être installée. Elle le sera uniquement lorsque l'utilisateur y fera appel.
Avance : permet de personnaliser l'installation des logiciels



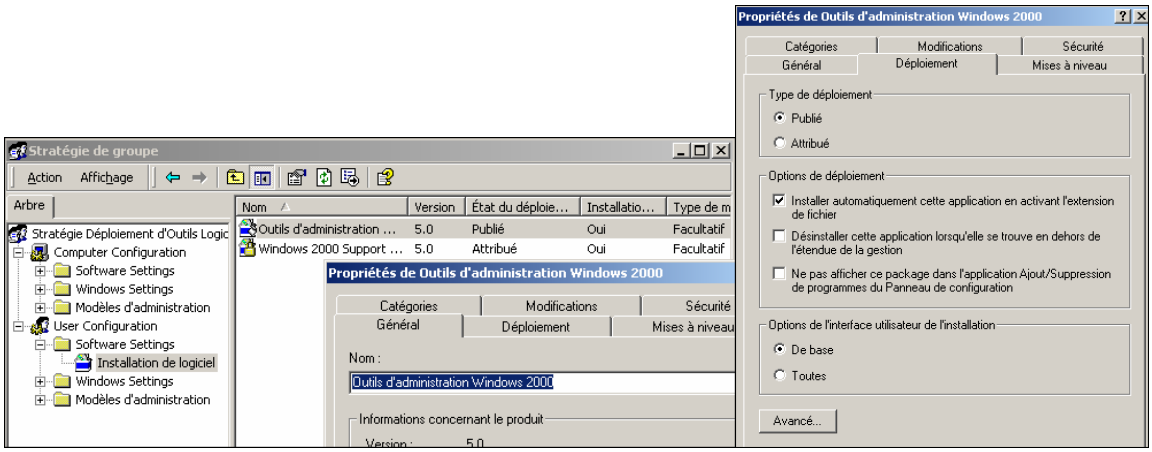
Créer des catégories de logiciels afin de pouvoir classer les applications



Clic droit **Propriétés ➔ Catégories ➔ Ajouter ➔Entrez un nom.**

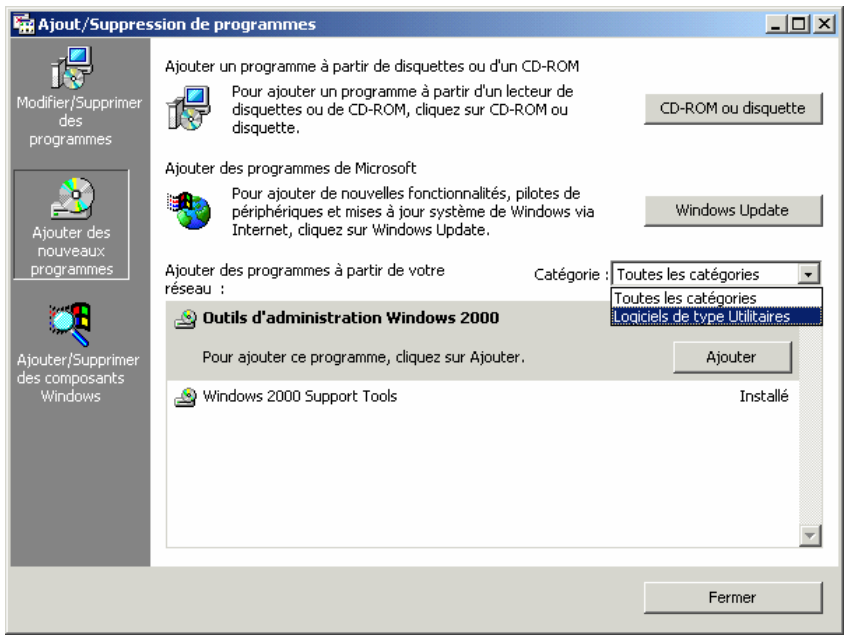


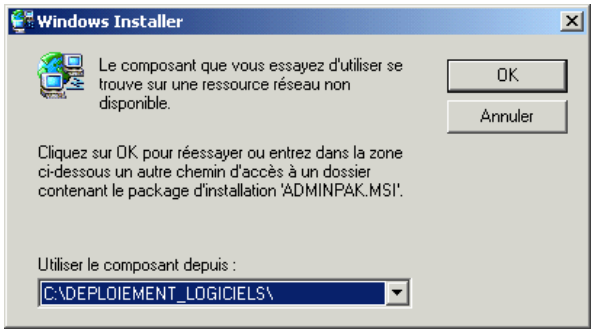
Modifier les paramètres des applications



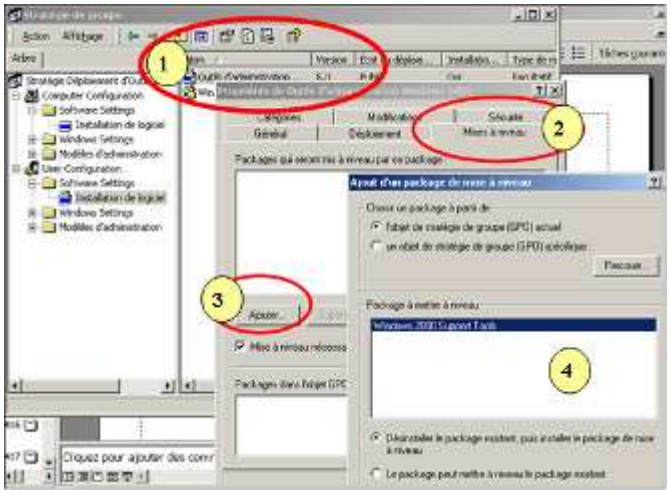
- Général : infos sur le produit.
- Déploiement : définit comment l'application va être déployée.
- Mise à niveau : permet la création de package de mise à niveau d'application (Service pack).
- Catégories : permet un classement des applications publiées dans **Ajout/Suppression de programmes** par catégories.
- Modifications : personnalisation des packages.
- Sécurité : gère les permissions.
- Tester la publication.

A partir d'un ordinateur client ouvrir une session avec le nom d'utilisateur chargé du déploiement.



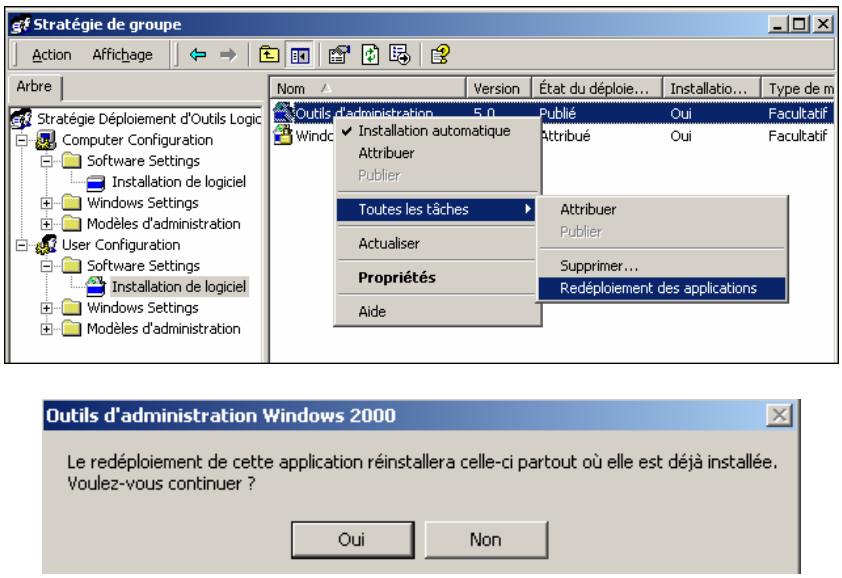


Mise à jour



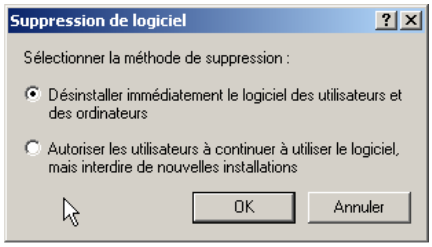
8.8.4- Ajout d'un Service pack

- Mettre les fichiers du service pack au format MSI dans le répertoire contenant les fichiers de distribution du logiciel.
- Clic droit sur le package devant recevoir un Service pack.
- **Toutes les tâches ➔ Redéploiement des applications ➔ Oui**.



8.8.5- Supprimer des logiciels

- Clic droit sur le package à désinstaller ➔ **Toutes les tâches ➔ Supprimer.**
- Forcer la suppression : application désinstallée au démarrage du micro ou à l'ouverture de session.
- Autoriser les utilisateurs à continuer à utiliser le logiciel mais pas de possibilité pour en installer de nouvelles.



IX- SERVICES RESEAUX

9.1- Rappel sur les protocoles réseau

Les protocoles réseau sont des spécifications qui permettent le formatage des données d'une manière normalisée pour permettre les échanges entre les systèmes informatiques connectés en réseau. Ce chapitre a pour but de faire un rappel sur les protocoles utilisés par Windows 2003.

9.1.1- Introduction

Le protocole natif de Windows 2003 est TCP/IP. C'est sur lui que s'appuie sur Windows 2003 pour assurer les ouvertures de session, les services de fichiers et d'impression. Pour permettre la compatibilité avec d'autres ordinateurs en réseau Windows 2003 supporte les protocoles suivants :

- IPX/SPX (Internetwork Packet eXchange/Sequenced Paquet eXchange).
- NetBEUI (NetBIOS Enhanced User Interface).
- AppleTalk.
- DLC (Data Link Control).
- IrDa (Infrared Data Association).

Les protocoles peuvent être ajoutés ou supprimés selon les besoins. Cependant, l'ordre d'installation détermine l'ordre de leur rattachement et donc la priorité du protocole. Cet ordre peut être modifié sur chaque interface en désinstallant, et réinstallant dans un ordre différent.

9.1.2- TCP/IP

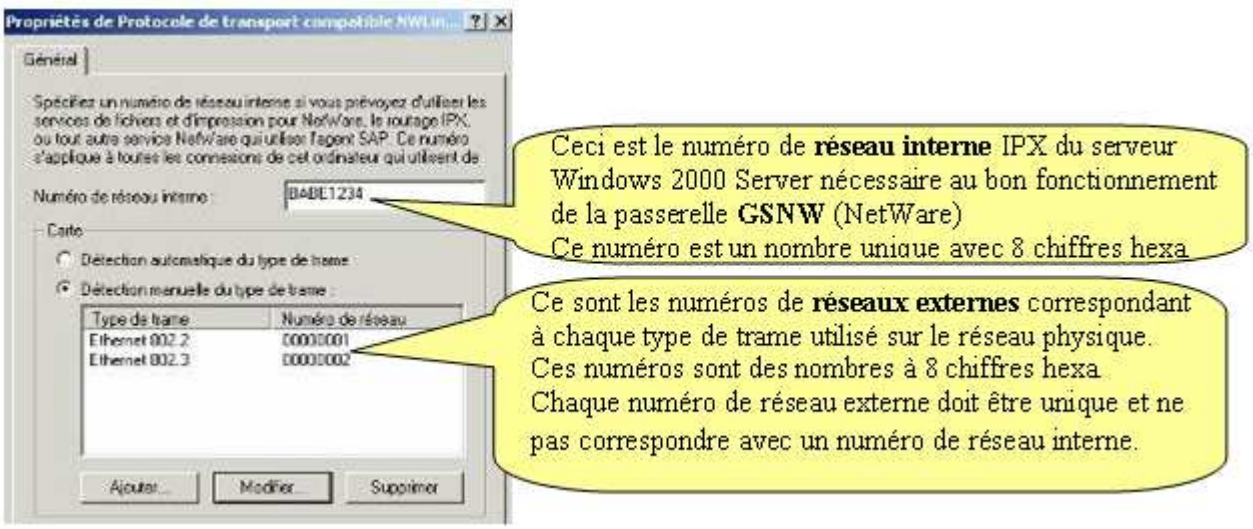
TCP/IP est une famille de protocoles qui sera détaillée au chapitre correspondant. TCP/IP étant le protocole utilisé sur Internet, Microsoft l'a choisi comme protocole natif de Windows 2003. A l'installation de W2003 Server le protocole TCP/IP est installé par défaut, et vous ne pouvez plus le supprimer.

9.1.3- NWLink

Présentation
NWLink est la version Microsoft du protocole IPX/SPX de Novell. Ce protocole est utilisé lorsqu'il existe sur le réseau des clients Microsoft qui ont besoin d'accéder aussi à des serveurs NetWare de Novell. Les clients Microsoft Windows 2003 qui veulent accéder à des serveurs NetWare doivent en plus du protocole NWLink, posséder un client NetWare de Microsoft nommé **CSNW** (Client Service for NetWare) pour Windows 2003 Pro et une passerelle NetWare **GSNW** (Gateway Service for NetWare) pour les ordinateurs Windows 2003 Server.
Paramétrage des types de trame
Les adaptateurs réseau utilisant NWLink peuvent générer des trames différentes selon le type de réseau physique.

Topologie	Type de trame
Ethernet	Ethernet II (pour IP principalement). 802.3 (pour les réseaux NetWare 2 et 3). 802.2 (pour les réseaux NetWare 4 et 5). SNAP (AppleTalk pricipalement).
Token Ring	802.5. SNAP.
FDDI (Fiber Distributed data Interface)	802.2. 802.3.

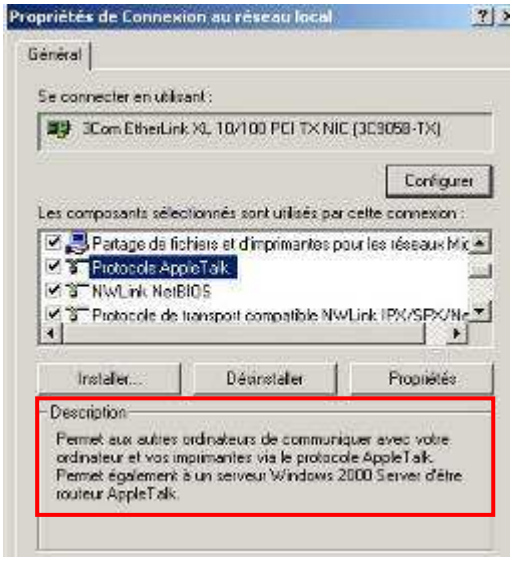
Le choix du type de trame peut se faire manuellement ou automatiquement dans **Propriétés réseau**, puis **Propriétés de Protocole compatible NWLink…**.



9.1.4- NetBEUI

Windows Server 2003 n'assure plus le support du protocole NETBEUI (utilisé sur les anciens réseaux).

9.1.5- AppleTalk



AppleTalk est un protocole développé par Apple Computer Corporation pour la mise en réseau des Macintosh. Windows 2003 supporte ce protocole, ce qui permet le partage de fichiers et d'imprimantes pour des clients MacIntosh. Windows 2003 Server comporte aussi un routeur et un service de connexion distant pour réseau commuté AppleTalk.

9.1.6- DLC

Windows Server 2003 n'assure plus le support du protocole DLC qui était utilisé par certaines imprimantes en réseau ou pour une connexion sur les mainframes IBM.

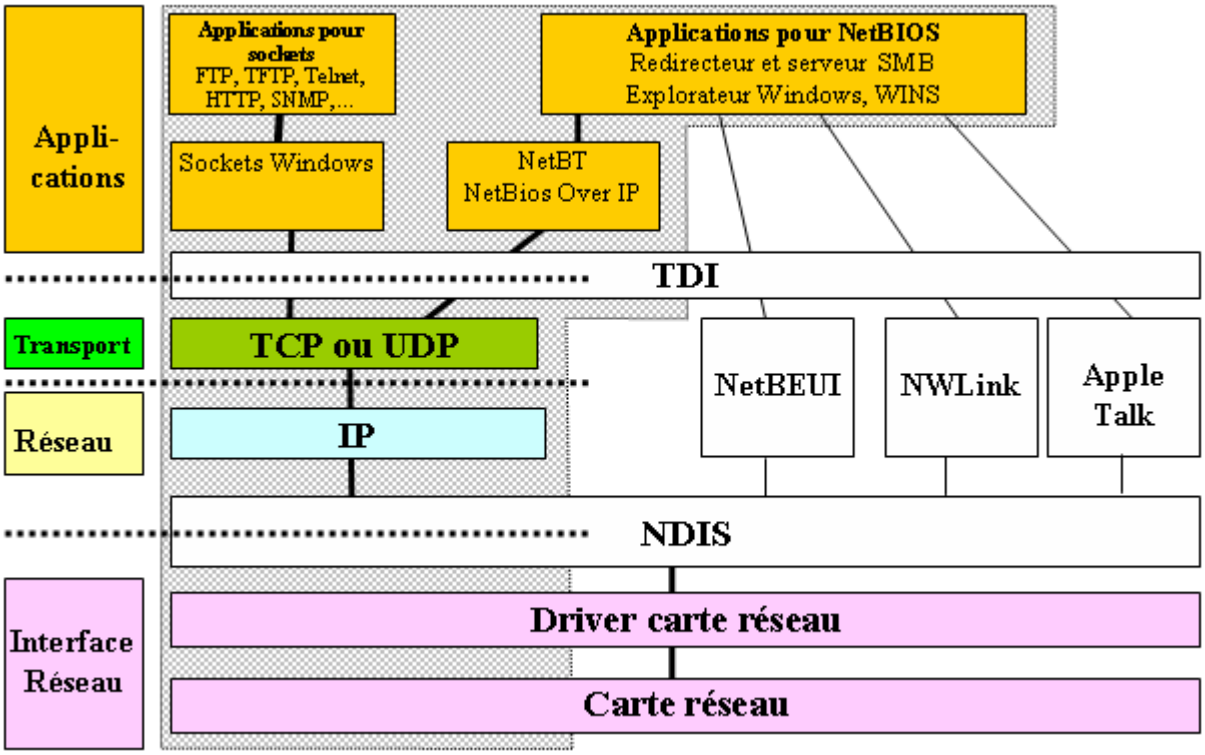
9.2- TCP/IP

9.2.1- Présentation

En quelques années le protocole TCP/IP est devenu le protocole standard parce qu'il est utilisé sur Internet. Or ce réseau mondial permet de relier les réseaux contenant des ordinateurs utilisant des systèmes d'exploitation différents. Si le protocole de connexion inter réseaux est IP, il est logique que le protocole utilisé sur chaque réseau local soit le même. Ceci évite la mise en place de

passerelles coûteuses, difficiles à installer et de toute façon représentant un dispositif qui entraîne des retards et peut-être des erreurs dans les transmissions de données. Le modèle **DoD (**Department of Defence) auquel est conforme TCP/IP est un modèle en quatre couches :

- Interface réseau.
- Internet.
- Transport.
- Application.



Windows Sockets (ou **Winsock**) agit comme interface entre les applications reposant sur les sockets (ports) et les protocoles TCP/IP.
NetBT agit comme une interface pour les services NetBIOS et les applications NetBIOS.
TDI (Transport Driver Interface) est une interface générale entre les applications et presque tous les protocoles transport.
NDIS (Network Driver Interface Spécification) est l'interface entre tous les drivers de cartes réseaux et les protocoles de la couche réseau.
SMB (Server Message Block) est un protocole de haut niveau de messages (commandes) entre clients et serveurs Microsoft.

9.2.2- Services TCP/IP disponibles sur Windows 2003

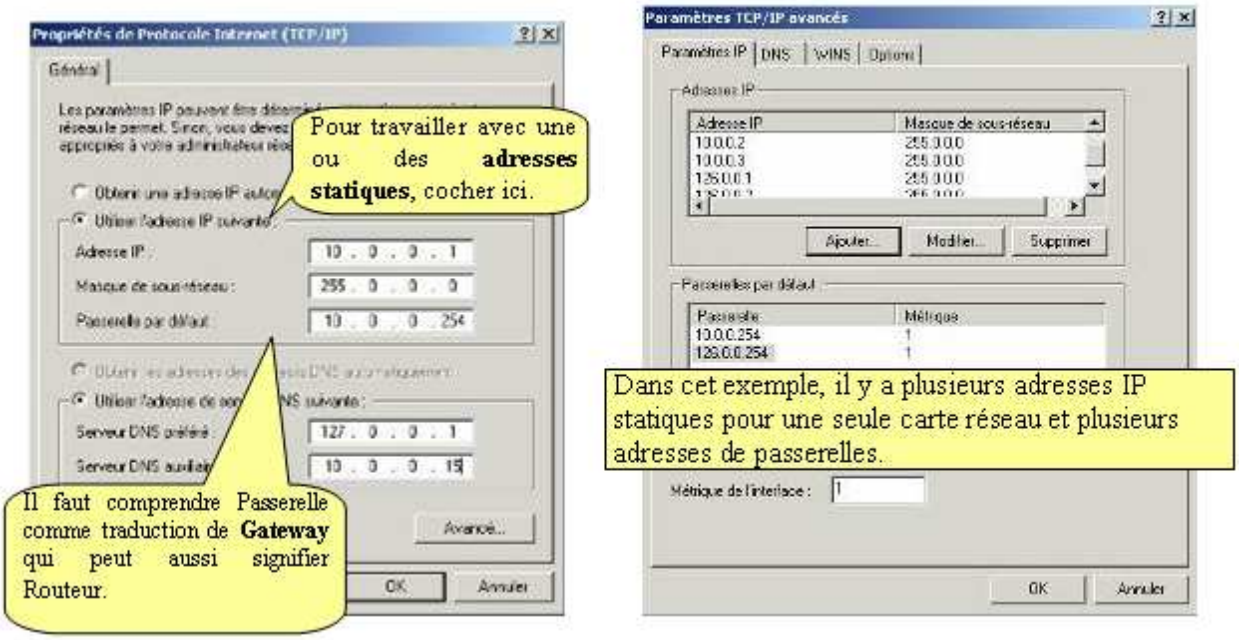
Les services TCP/IP disponibles sous Windows 2003 sont les suivants :

- Service et client **DHCP** (Dynamic Host Configuration Protocol).
- **WINS** (Windows Internet Name Service) : serveur et client de noms NetBIOS.
- **DDNS** (Dynamic Domain Name Server).
- Support d'appel distant sur réseau commuté **PPP** et SLIP.
- Protocole **PPTP** (Point to Point Tunneling Protocol) et protocole **L2TP** (Layer 2 Tunneling Protocol) utilisés pour établir des circuits virtuels vers des réseaux distants.
- Service d'impression TCP/IP (**LPR** et **LPD**).
- Agent **SNMP.**
- Interface **NetBIOS.**
- Support **RCP** (Remote Procedure Call) pour l'administration à distance des ordinateurs.

- Support de navigation WAN.
- Serveur Web et FTP **IIS** (Internet Information Server).
- Utilitaires de connectivités TCP/IP : finger, FTP client, rcp, rexec, rsh, Telnet et TFTP client.
- Outils de diagnostic et de gestion TCP/IP : arp, hostname, ipconfig, lpq, ping, route, nslookup, pathping et tracert.
- Analyseur de protocole Microsoft Network Monitor disponible sur Windows 2003 Server.
- Prise en charge de l'**IPV6** sur 128 bits.
- Configuration alternative permettant à un ordinateur d'utiliser une configuration alternative d'adresse IP configurée manuellement en l'absence de serveur DHCP (Dynamic Host Configuration Protocol). Sinon utilisation de l'adressage APIPA ou statique ou serveur DHCP.
- …

9.2.3- Configuration TCP/IP avec adresse statique

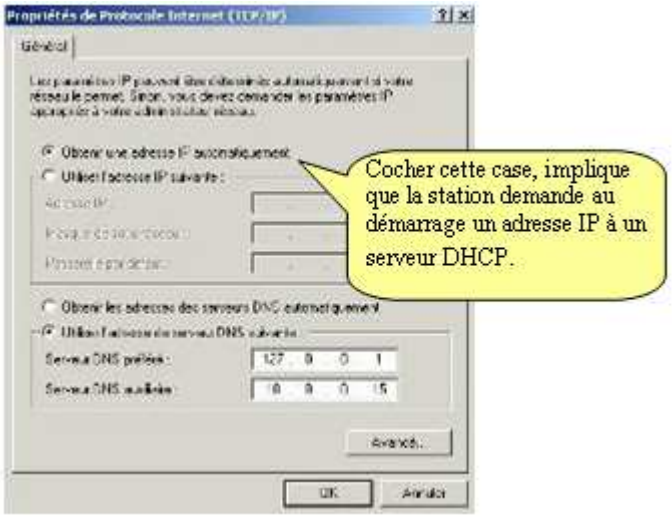
Par défaut, les ordinateurs clients prévus pour travailler avec TCP/IP sous les systèmes d'exploitation Windows 95, 98 et 2003 obtiennent automatiquement leur adresse IP à partir d'un serveur DHCP. Les ordinateurs serveurs, les routeurs et les imprimantes réseaux doivent cependant posséder des adresses IP **statiques**. Les stations elles-mêmes peuvent être installées avec des adresses statiques. Si vous avez demandé **l'adressage statique**, vous devez entrer au minimum, une adresse IP, un masque de sous réseau. Si votre réseau est connecté à un routeur, vous devez précisez son adresse dans la case **Passerelle**.



Il est possible de donner plusieurs adresses IP pour une seule carte réseau. Pour pouvoir communiquer avec des réseaux logiques d'adresses différentes. S'il existe plusieurs cartes réseaux, vous devez donner au moins une adresse IP par carte. Chaque carte est connectée à un réseau physique différent et à au moins un réseau logique IP. Windows 2003 Server comporte une fonction routage IP qui permettra de faire communiquer les différents réseaux entre eux.

Configuration TCP/IP avec obtention automatique d'une adresse

La configuration des ordinateurs sous IP en obtenant une adresse automatiquement à partir d'un serveur DHCP permet de simplifier l'installation et la maintenance des stations dans un réseau Windows. L'adressage dynamique IP est aussi très intéressant pour tous les postes itinérants. En effet, au moment de se connecter sur un des réseaux qu'ils utilisent, les utilisateurs itinérants obtiennent automatiquement une adresse IP appropriée au réseau. Voir plus loin le chapitre DHCP.

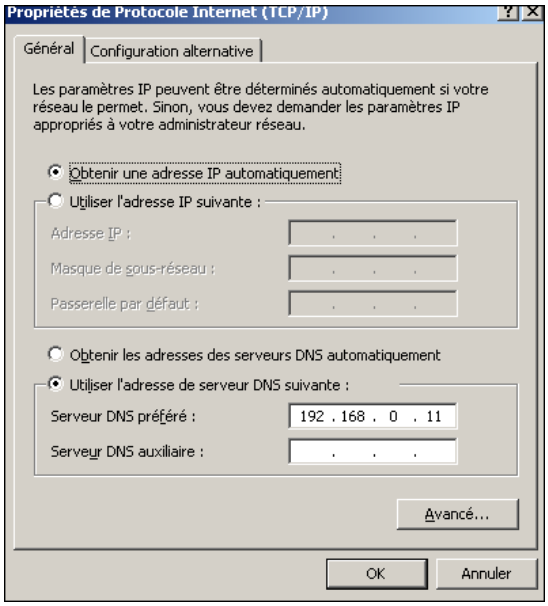


9.2- Adressage privé automatique

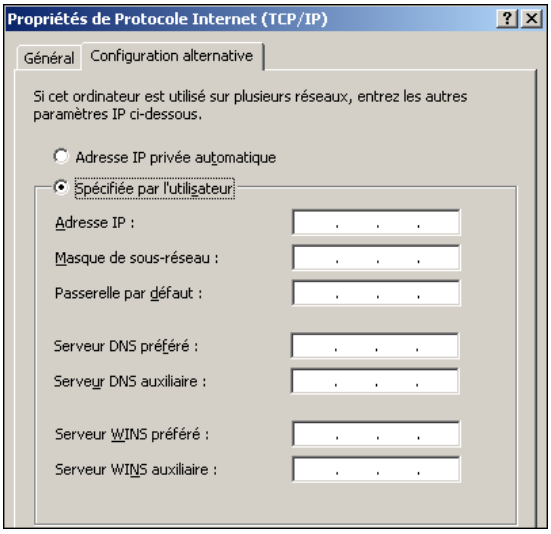
Windows 2003 fournit un nouveau système d'obtention automatique d'adresses IP pour petits réseaux qui ne possèdent pas de serveur DHCP. Il s'agit du système nommé **APIPA** (Automatic Private IP Adressing). Il utilise une plage d'adresses réservée par l'**IANA** (Internet Assigned Numbers Authority) comprise entre 169.254.0.0 et 169.254.255.255. Le masque de sous réseau est 255.255.0.0. Le système fonctionne si la station est configurée pour obtenir une adresse dynamique. Le processus se déroule comme suit :

- La station essaye de contacter un serveur DHCP. Comme il n'en existe pas sur le réseau, le système APIPA se déclenche.
- APIPA génère une adresse 169.254.x.y et un masque de sous réseau 255.255.0.0. Si la valeur x.y est déjà utilisée, APIPA en génère une autre et vérifie à nouveau qu'elle n'existe pas. Il peut y avoir jusqu'à 10 tentatives pour obtenir une adresse correcte. Ceci limite le système à des réseaux de petite taille.

Ce système n'est pas aussi performant qu'un serveur DHCP. En effet, celui-ci peut fournir d'autres informations que l'adresse IP et le masque. Il peut fournir par exemple, l'adresse de la passerelle. Ceci veut dire qu'une station qui utilise APIPA ne peut pas communiquer avec un autre réseau.



Indique que TCP/IP doit utiliser l'adressage APIPA (Automatic Private IP Addressing) si un serveur DHCP (Dynamic Host Configuration Protocol) n'est pas trouvé. L'adressage APIPA affecte une adresse IP à partir de la plage allant de 169.254.0.1 à 169.254.255.254 et un masque de sous-réseau 255.255.0.0. L'adressage APIPA n'affecte pas de passerelle par défaut, de serveurs DNS (Domain Name System) ni de serveurs WINS (Windows Internet Name Service).



Indique que TCP/IP doit utiliser l'autre configuration si aucun serveur DHCP (Dynamic Host Configuration Protocol) n'est trouvé. Cette autre configuration est utile lorsque l'ordinateur est utilisé sur plusieurs réseaux, si au moins un des réseaux ne possède pas de serveur DHCP ou qu'une configuration APIPA (Automatic Private IP Addressing) n'est pas souhaitée. C'est le cas notamment lorsque vous utilisez un ordinateur portable à la fois au bureau et à votre domicile. Au bureau, l'ordinateur portable utilise une configuration TCP/IP avec un serveur DHCP alloué. Au domicile, où vous ne disposez pas d'un serveur DHCP, l'ordinateur portable utilise automatiquement l'autre configuration, qui facilite l'accès aux périphériques réseau de votre domicile et à Internet. De cette façon, l'ordinateur portable fonctionne sans problèmes sur les deux réseaux sans que vous deviez reconfigurer TCP/IP.

9.2.5- Configuration alternative

Lorsqu'un ordinateur est configuré pour employer DHCP mais qu'aucun serveur DHCP n'est présent sur le réseau, Windows Server 2003 assigne automatiquement une adresse IP privée alternative.
Rappel : par défaut cette adresse se situé dans la plage 169.254.0.1 à 169.254.255.254 avec un masque de sous réseau de 255.255.255.0. Il est possible de modifier cette plage et d'imposer une adresse IP alternative spécifique en absence de serveur DHCP, ce qui est très utile pour les ordinateurs portables. En effet lorsque ce portable est connecté à sa station d'accueil dans l'entreprise il reçoit automatiquement son adresse IP par un serveur DHCP et lorsqu'il est utilisé à votre domicile il est configuré avec l'adresse de la configuration alternative.
La configuration alternative permet à un ordinateur d'utiliser une configuration alternative d'adresse IP configurée manuellement en l'absence de serveur DHCP (Dynamic Host Configuration Protocol). Vous pouvez utiliser une configuration alternative lorsque l'ordinateur est utilisé sur plusieurs réseaux, qu'au moins un des réseaux ne possède pas de serveur DHCP et qu'une configuration automatique n'est pas souhaitée.
Par exemple, si vous possédez un ordinateur portable que vous utilisez aussi bien au bureau qu'à votre domicile, il est utile de configurer TCP/IP pour une configuration alternative. Au bureau, l'ordinateur portable utilise une configuration TCP/IP avec un serveur DHCP alloué. Au domicile, où vous ne disposez pas d'un serveur DHCP, l'ordinateur portable utilise automatiquement la configuration alternative, qui facilite l'accès aux périphériques réseau de votre domicile et à Internet et qui permet un fonctionnement transparent sur les deux réseaux sans reconfiguration manuelle des paramètres TCP/IP.
En l'absence de configuration alternative, TCP/IP utilise APIPA (Automatic Private IP Addressing).

9.2.6- Dépannage

Si après configuration de la station et éventuellement redémarrage, il existe des problèmes de connexions TCP/IP, Microsoft fournit avec Windows 2003 une suite d'outils pour assurer le dépannage.

Noms	Rôle
Ping	Cet utilitaire teste la configuration et les connexions. Un test sur l'adresse IP 127.0.0.1 permet de tester la pile IP. Un test sur l'adresse de l'ordinateur permet de tester la pile IP et la carte. Un test avec une adresse d'une autre machine IP permet de vérifier la bonne connexion entre ces deux machines.
Arp	Cet utilitaire affiche la correspondance entre les adresses IP et les adresses MAC. A utiliser avec l'option –a.

Ipconfig	Cet utilitaire permet de vérifier la configuration IP de l'ordinateur. A utiliser avec l'option /all.
PathPing	Cet utilitaire Microsoft Windows 2003 conjugue les commandes ping et route.
Netstat	Cet utilitaire affiche les statistiques et les connexions TCP/IP. Utiliser l'option –a.
Route	Cet utilitaire permet d'afficher ou de modifier la table de routage d'un ordinateur.
Hostname	Cet utilitaire retourne le nom NetBIOS de l'ordinateur sur lequel elle est utilisée.
Tracert	Cet utilitaire affiche et vérifie l'itinéraire emprunté pour atteindre un ordinateur distant en indiquant chaque routeur traversé.

9.3- DHCP

DHCP sous Windows 2003 gère l'attribution d'informations de configuration TCP/IP. Il permet de fournir des adresses IP, des masques et d'autres informations à des ordinateurs clients DHCP. TCP/IP lors de l'installation de W2003 Server est configuré par défaut comme client DHCP. Le serveur DHCP vous permet de gérer de façon centralisée la configuration des postes de travail, voire même des serveurs. Vous pouvez aussi définir une adresse fixe pour un micro en effectuant des réservations. Avec la mise en œuvre d'un serveur DHCP, l'administrateur possède une base centralisée contenant les noms des machines, les adresses TCP/IP et les adresses physiques (MAC) des cartes réseau. Le jour où le réseau doit évoluer avec par exemple l'ajout d'une passerelle, d'un serveur DNS ou le changement complet de l'adressage TCP/IP, le service DHCP vous facilite le travail car il peut gérer la plupart des modifications de façon centralisée.
Avec W2003 Server des évolutions ont été apportées surtout par rapport à Windows NT4 comme :

- La notion d'autorisation de fonctionnement du serveur DHCP.
- Les étendues de multi diffusion.
- Les classes d'options.
- La possibilité de mise à jour dynamique des enregistrements de ressources des serveurs DNS.

En plus la console de gestion de DHCP vous donne la possibilité d'exporter la base du serveur DHCP.

9.3.1- Présentation du protocole DHCP

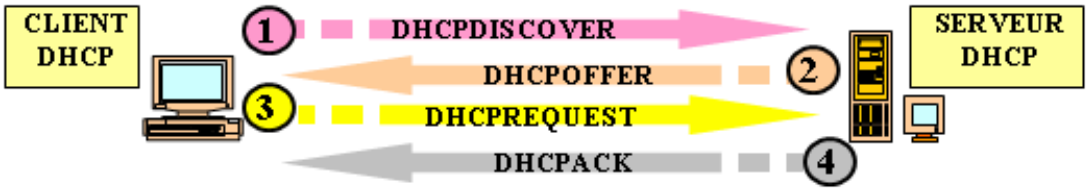
DHCP (Dynamic Host Configuration Protocol) est une norme TCP/IP qui permet de simplifier la gestion et la distribution d'adresses IP sur un réseau. DHCP est une extension du protocole BOOTP qui s'appuie sur UDP/IP. Au démarrage d'une station ou à expiration du bail, le client DHCP demande des informations de configuration au serveur DHCP. Ces informations comprennent :

- Une adresse IP.
- Un masque de sous réseau.
- Des valeurs optionnelles, comme la passerelle par défaut, l'adresse d'un serveur DNS ou WINS.

Chaque serveur DHCP possède un pool d'adresses défini et propose une adresse de la plage au client. Si celui-ci accepte, le serveur accorde un bail pour ce client et cette adresse pour une durée limitée.

Processus DHCP

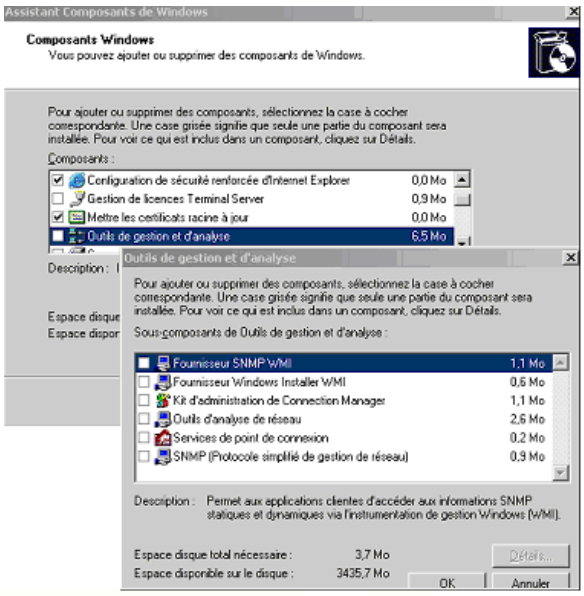
L'attribution d'informations par un serveur DHCP s'appelle un **bail**. Le processus d'attribution d'un bail débute, en particulier, lorsque le client DHCP démarre pour la première fois.
Le processus d'attribution d'un bail comporte quatre étapes :



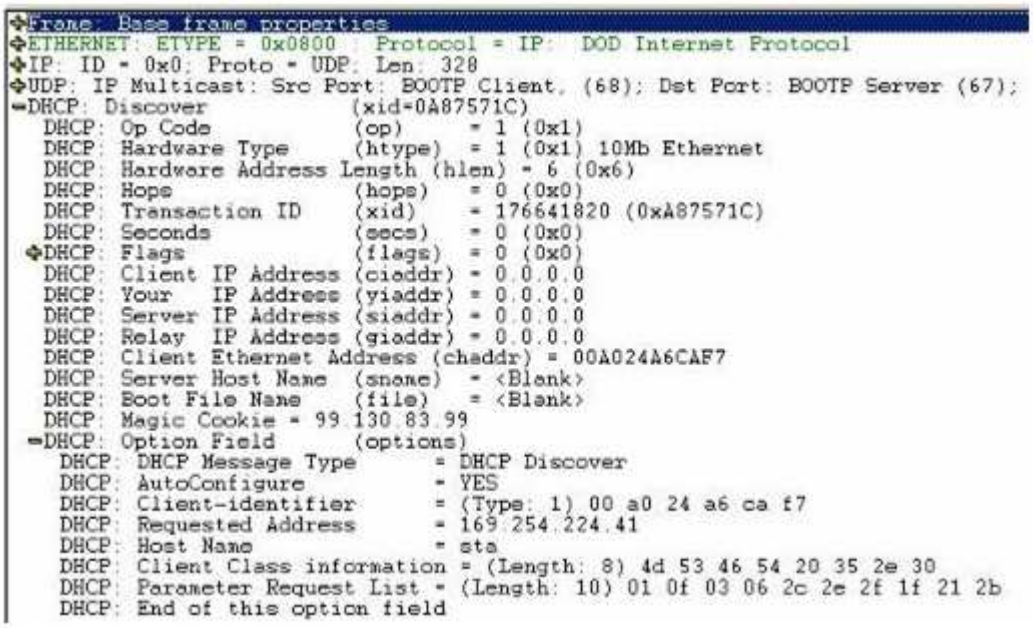
- **DHCP DISCOVER** : le client DHCP sur la station envoie une requête DHCPDISCOVER pour essayer de trouver un serveur DHCP. Il s'agit d'un message Broadcast puisque le client ne connaît pas l'adresse du serveur DHCP. L'adresse source IP est à 0.0.0.0, puisque le client ne connaît pas son adresse IP (c'est ce qu'il recherche).
- **DHCPOFFER :** le ou les serveurs DHCP qui ont reçu la requête DHCPDISCOVER renvoient une réponse DHCPOFFER qui comporte :
  - L'adresse MAC du client.
  - Une proposition d'adresse IP.
  - Un masque de sous réseau.
  - Une durée de bail.
  - L'adresse IP du serveur DHCP.

  Cette réponse est envoyée sous forme de paquet sous réseau puisque l'adresse IP du client n'est pas encore fixée. Le client DHCP accepte la première réponse reçue.
- **DHCPREQUEST :** le client qui a accepté la première adresse reçue diffuse un message DHCPREQUEST pour indiquer qu'il possède une adresse IP. Ce message comporte l'adresse IP du serveur DHCP dont la proposition a été retenue. Celui-ci sait que l'adresse proposée a été retenue. Tous les autres serveurs DHCP annulent leur proposition et peuvent réutiliser l'adresse proposée.
- **DHCPACK ou DHCPNACK :** le serveur DHCP dont l'offre a été acceptée diffuse un accusé de réception réseau Ce message contient un bail valide et éventuellement d'autres informations. A l'arrivée de ce message chez le client le processus est terminé.
- Si le message **DHCPREQUEST** échoue, le serveur DHCP renvoie un accusé de réception négatif DHCPNACK.

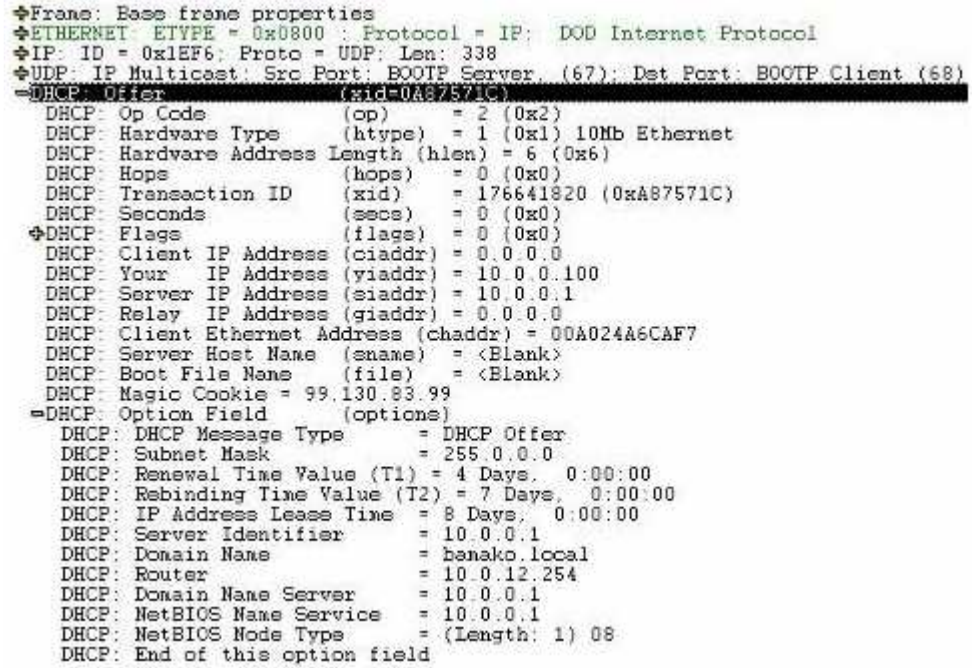
Les figures suivantes sont des copies d'écrans des messages DHCP. La capture de ces messages a été réalisée grâce à la fonction analyseur de protocoles du **Moniteur réseau Microsoft** livré avec chaque Windows 2003 Server.



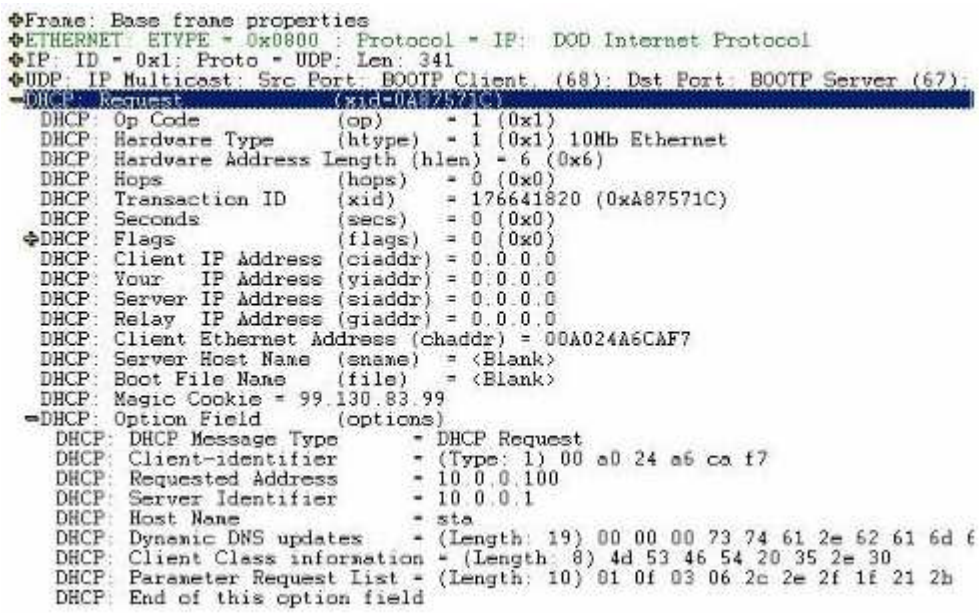
Les 4 messages DHCP permettant d'obtenir une adresse IP pour une station à partir d'un serveur DHCP.



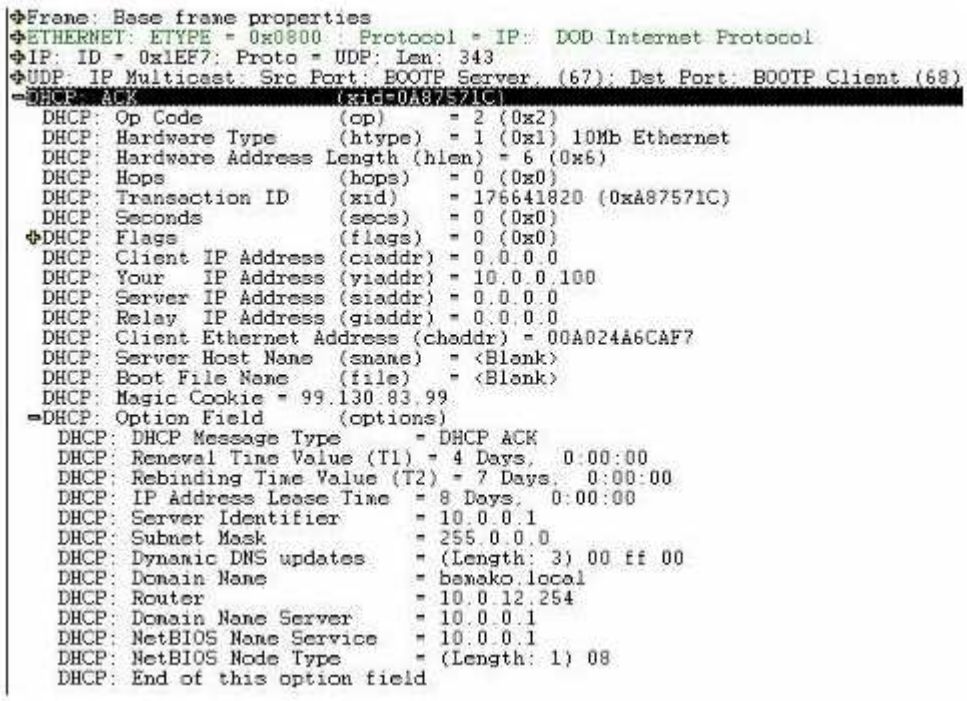
Détails du message DHCPDISVOVER



Message DHCPOFFER



Message DHCPREQUEST.

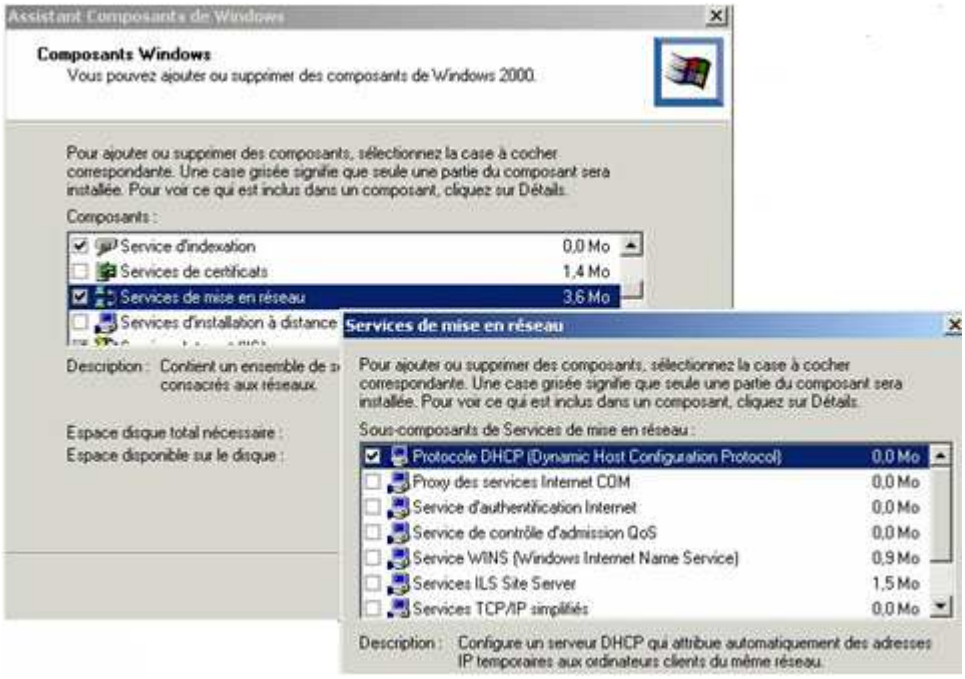


Message réseau

9.3.2- Installation et configuration du service DHCP

Installation

Sur la station, le **client** DHCP est installé par défaut et est activé lorsque vous cochez la case **Obtenir une adresse IP automatiquement**. Pour installer un **serveur DHCP**, vous devez le faire sur un serveur Windows 2003, contrôleur de domaine ou serveur membre. Pour commencer l'installation du serveur DHCP, utilisez le panneau **Configurer votre serveur** dans **Outils d'administration** du **Panneau de configuration**. Sélectionnez la rubrique **Mise en réseau**, puis **DHCP**. Cliquer sur **Démarrer l'assistant Composants de Windows**. Dans le panneau **Composants Windows**, sélectionner **Services de mise en réseau** puis **Détails**. Dans la fenêtre qui s'ouvre **Protocole DHCP…**. Faire **OK** et **Suivant**. L'installation s'effectue.

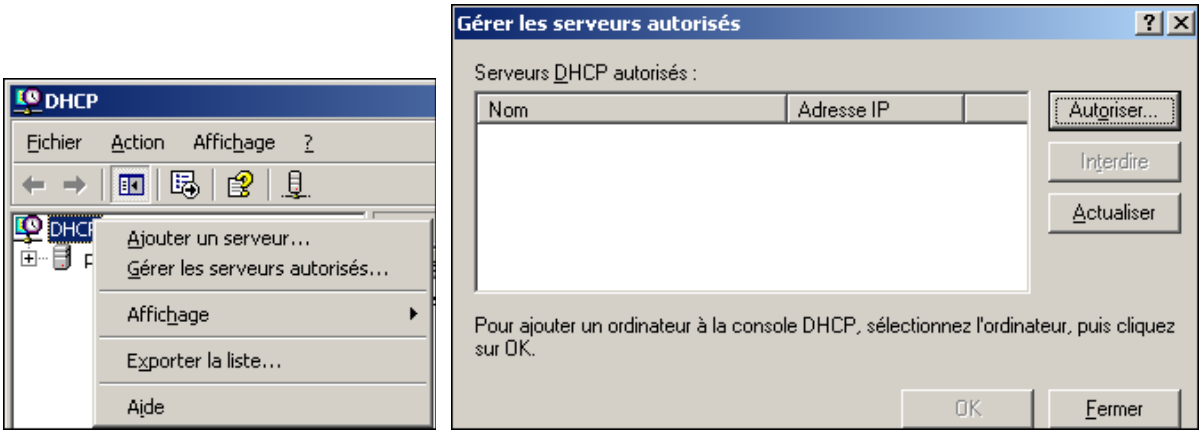


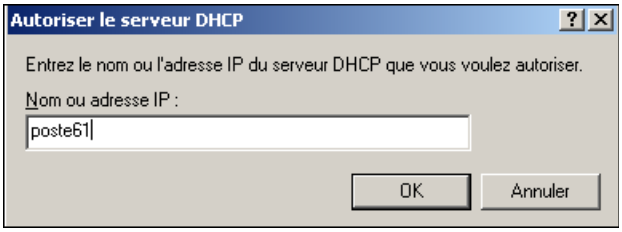
Autorisation

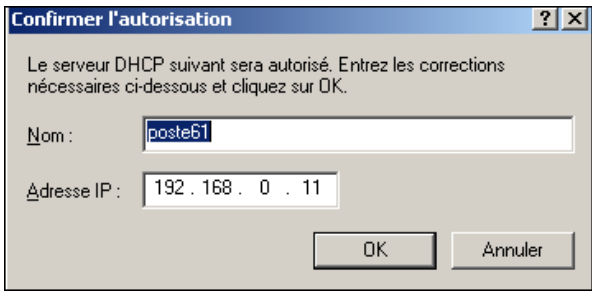
Microsoft met de plus en plus l'accent sur la sécurité. En autre c'est pour cela que vous devez autoriser les serveurs réseaux. En effet, sur un réseau un serveur DHCP mal configuré peut entraîner d'importants dysfonctionnements. Il peut donner des adresses IP erronées ou empêcher un poste client de récupérer un adressage TCP/IP correct. Un serveur DHCP sous W2000 ou 2003 lorsqu'il démarre puis par la suite, envoie des trames réseau afin de vérifier qu'il est bien autorisé à fonctionner. Dans le cas contraire il ne va pas répondre aux requêtes des clients. Cette demande d'autorisation de fonctionnement est liée à Active Directory et cette autorisation ne peut être réalisée que par les membres des groupes administrateurs d'entreprises et administrateurs du domaine. Cette autorisation ne peut se faire que dans une base Active Directory, mais un serveur autonome ou un ordinateur en groupe de travail vérifie aussi son autorisation. Dans le cas où il n'y a pas de domaine Active Directory, il fonctionnera normalement, mais si il y a un domaine Active Directory et s'il n'y est pas autorisé, il ne va pas répondre aux requêtes des clients.

Pour autoriser un serveur DHCP vous avez deux façons de procéder :

- A partir de la console **DHCP** des **Outils d'administration** en cliquant droit sur le **serveur DHCP** et valider l'option **Autoriser.**
- Ou à partir de cette même fenêtre en cliquant droit sur **DHCP** (et non pas sur le serveur).





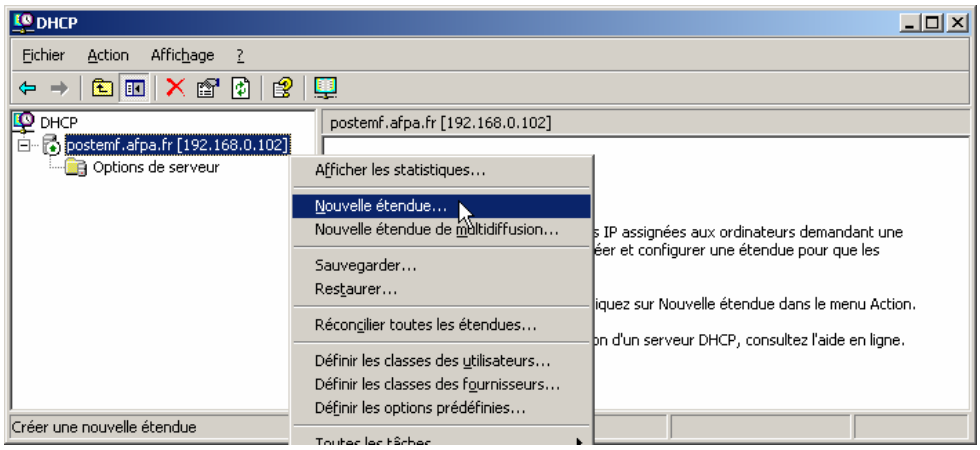


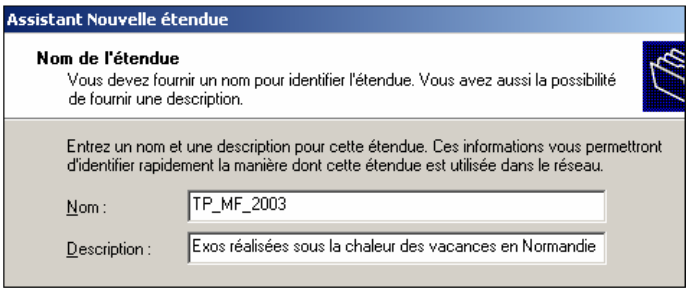
Dans la console DHCP, un serveur qui fonctionne normalement va apparaître avec une flèche verte verticale vers le haut. Dans le cas contraire la flèche sera rouge et dirigée vers le haut.
✋ Vous pouvez désactiver la détection de cette autorisation à partir du registre (voir Kit de ressources...).

Les étendues
Une étendue est une plage d'adresses qui est affectée aux clients réseau.
Trois types d'étendues peuvent être créées :

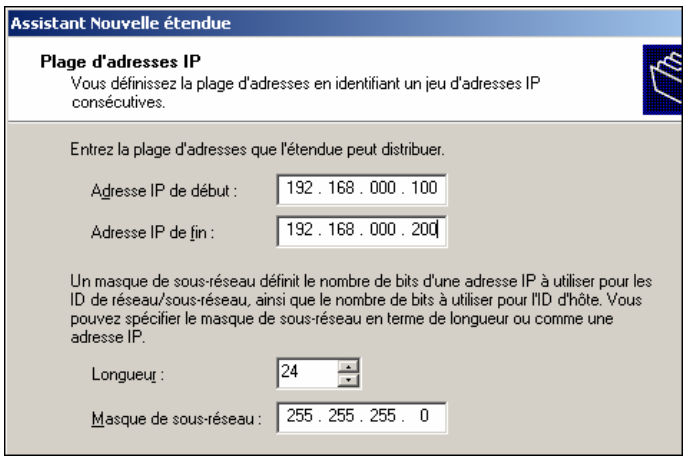
- L'étendue d'adresses simple.
- Les étendues globales.
- Les étendues de multi diffusion.

→ L'étendue d'adresses
Clic droit dans la console **DHCP** sur **Nouvelle étendue.** Un écran de **bienvenue** démarre. Validez **Suivant,** et dans la nouvelle fenêtre de **l'Assistant** entrez les informations de **Nom** pour votre étendue et éventuellement une **description**. Cliquez sur **Suivant**

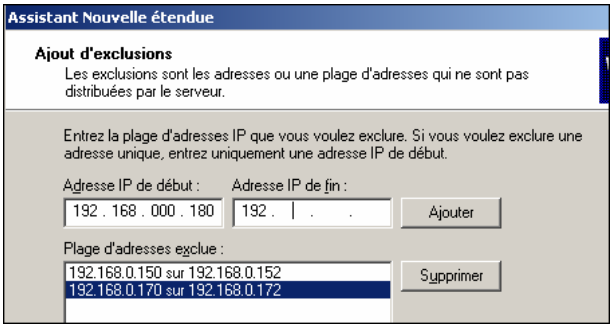




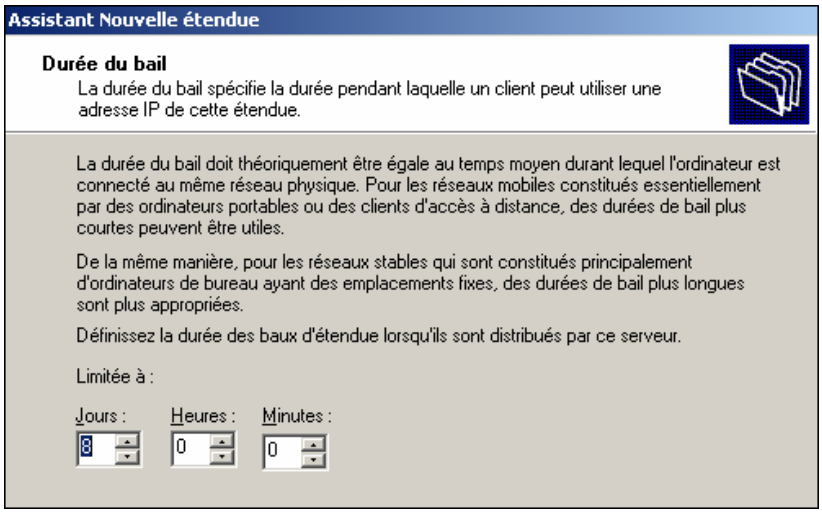
Dans la fenêtre **Plage d'adresse IP**, entrez l'**adresse de début** et de **fin** de la **plage d'adresses**, le **Masque de sous réseau** envoyé aux **clients** DHCP ou le **nombre de bits du masque de sous réseau**. Longueur demandée est le nombre de bits à 1 dans le **masque de sous réseau** (ici 24). Puis cliquez sur **Suivant**



Si vous avez deux plages d'adresses disponibles pour un même sous réseau, vous devez procéder par exclusion. Il ne vous est pas possible de créer plusieurs étendues pour un même sous réseau.
Entrez les adresses ou les plages à exclure qui ne devront pas être attribués aux clients DHCP (soit elles sont déjà attribuées de façon statique ou elles sont déjà attribuées par un autre serveur DHCP si il y en a plusieurs), puis cliquez sur **Suivant**

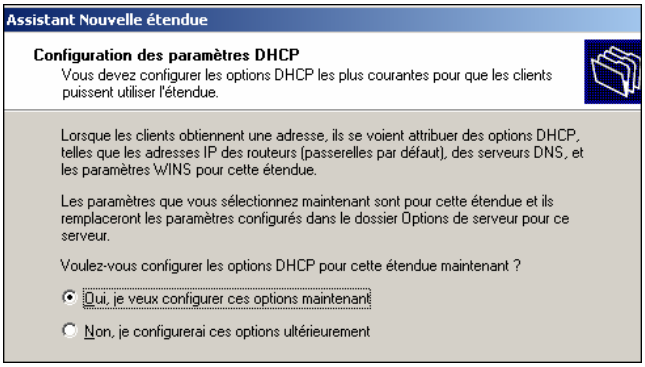


Entrez la durée du bail (Baux) qui par défaut est de 8 jours. Vous pouvez constater que la notion de bail illimité n'est pas proposée. Par contre lorsque l'étendue sera créée cette option sera accessible via les **Propriétés**. Mais il n'est pas conseillé de la valider, car dans ce cas le serveur DHCP ne pourra jamais récupérer une adresse IP attribuée et qui n'est plus utilisée.
Par contre vous pouvez définir un bail très court dans le cas de pénurie d'adresses IP.
Rappel : un micro client d'un serveur DHCP redemande systématiquement dans sa requête DHCP l'adresse IP qu'elle avait précédemment. Si le bail n'est pas expiré, elle récupère la même adresse. Si le bail est expiré et si le serveur DHCP n'a pas attribué l'adresse à un autre client, il pourra la redonner à la même machine. Cliquez sur **Suivant.**

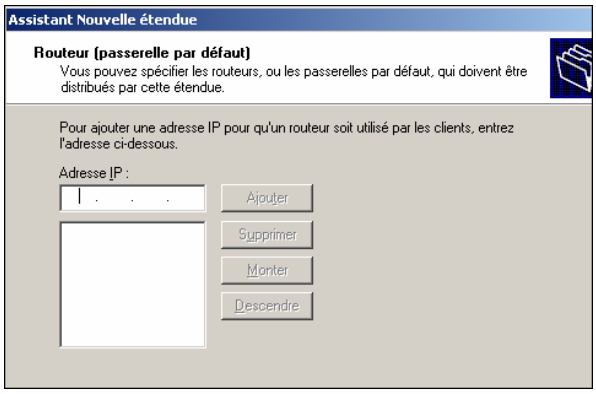


→ Configuration des options d'étendue

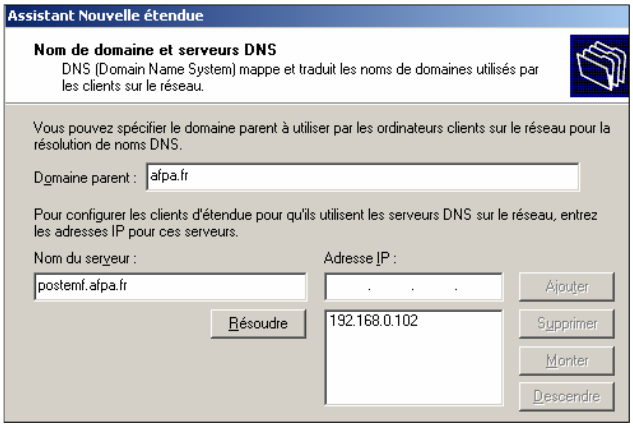
Possibilité ou non de configurer les options supplémentaires **réseau.** La fenêtre suivante demande si l'on veut indiquer les options immédiatement ou plus tard. Ces options sont des informations qui seront envoyées au client pour le configurer. Elles comprennent, entre autres, le nom du domaine, l'adresse de la passerelle, l'adresse des serveurs DNS ou WINS.



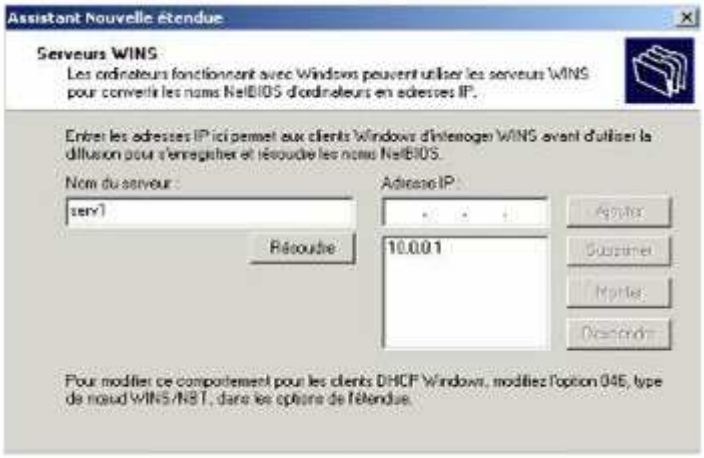
Possibilité de paramétrer l'adresse du routeur (passerelle). Si on désire rentrer les options immédiatement, la fenêtre suivante invite à indiquer une ou plusieurs adresses de passerelles qui permettront au réseau de communiquer avec d'autres réseaux IP.



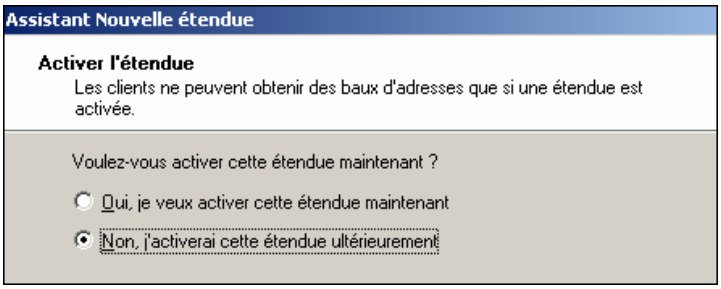
La fenêtre suivante permet d'indiquer le nom du **domaine** et le ou les noms des **serveurs de domaine** ainsi que leurs adresses. Saisissez le **nom de votre domaine** (exemple : afpa.fr) et **l'adresse du serveur DNS.** La saisie du nom du serveur DNS dans le champ **Nom du serveur** est simplement une facilité pour récupérer son adresse IP si vous ne la connaissez pas. Il vous suffit pour cela de cliquer sur le bouton **Résoudre** et l'adresse apparaît immédiatement dans le champ adresse IP. Il vous suffit de cliquer sur le bouton **Ajouter**. Si il existe plusieurs serveurs DNS ou passerelles, vous avez la possibilité d'utiliser sur **Monter** ou **Descendre.**



Vous pouvez configurer la ou les adresses d'un serveur **WINS** avec possibilité ou non de récupérer l'adresse. Si vous indiquez l'adresse d'un serveur WINS, l'assistant va ajouter automatiquement l'option **046** avec le type de nœud **NetBios 0x8** dans les options du serveur **réseau.** Dans ce cas le type de résolution est **NetBIOS Hybride**, ce qui signifie qu'une requête est d'abord effectuée auprès d'un serveur de noms **WINS** avant de faire une diffusion.



Cliquez sur **Suivant** afin d'ouvrir la fenêtre **Activer l'étendue**. Validez l'option **Oui, je veux activer cette étendue maintenant**. Par la suite vous avez la possibilité de **désactiver** ou **réactiver** une étendue. Tant qu'une étendue n'est pas activée le serveur DHCP ne va pas répondre aux requêtes des clients.



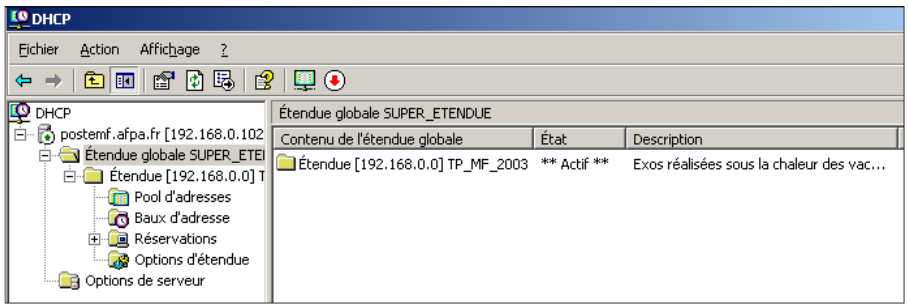
Pour finir votre paramétrage, cliquez sur **Terminer** dans la fenêtre **Fin de l'Assistant Nouvelle Etendue.**

→ L'étendue globale

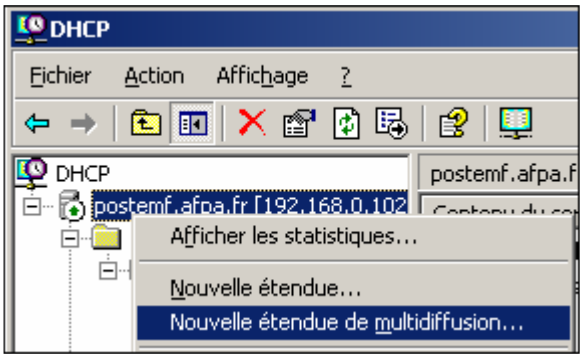
La possibilité de configurer des étendues globales permettant à un serveur DHCP de gérer des adresses IP correspondant à plusieurs adresses de réseaux logiques sur un seul réseau physique (exemple d'adresses réseau 192.168.3.0 et 192.168.4.0 sur le même réseau physique) est offerte dans le monde des serveurs Windows. Pour configurer ces étendues d'adresses, vous allez créer plusieurs étendues d'adresses comme précédemment, puis les regrouper sous une super étendue. Cliquez droit sur le nom du serveur **DHCP**, puis sélectionnez l'option **Nouvelle étendue globale** afin d'ouvrir la fenêtre de **l'Assistant Nouvelle Etendue Globale.** Dans l'écran **Nom de l'étendue globale**, dans le champ **Nom** entrez son nom. Validez **Suivant** afin d'ouvrir la fenêtre **Choix des étendues**. Sélectionnez les étendues à inclure dans la super étendue puis cliquez sur **Suivant** et **Terminer**.

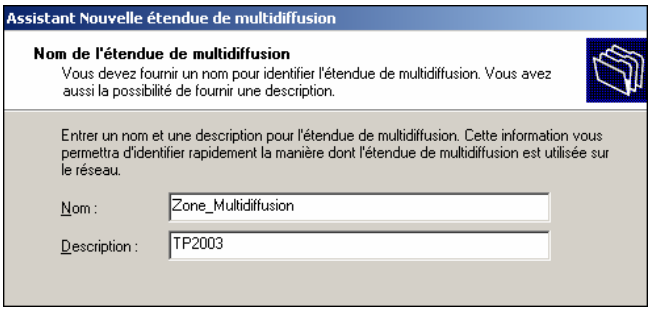
En résumé, vous pouvez mettre en œuvre les super étendues globales :

- Si vous n'avez pas assez d'adresses sur un sous réseau.
- Si vous êtes en période de changement d'adressage IP.
- Si vous n'avez pas la possibilité de remettre en question certaines adresses pour des raisons historiques.

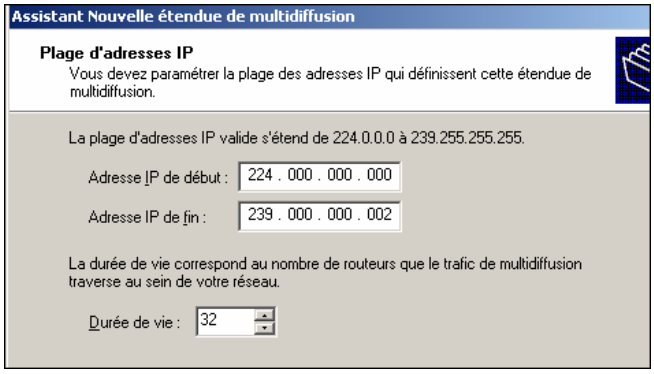


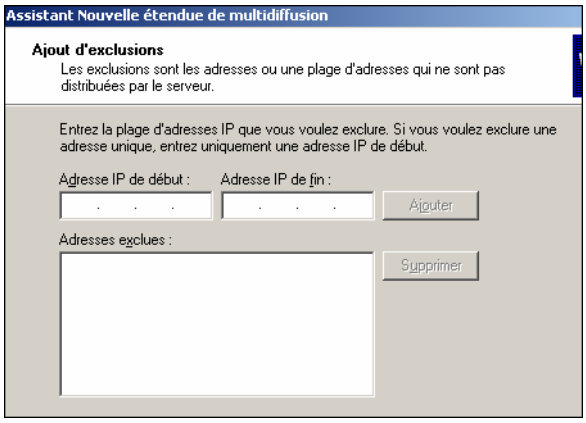
→ Les étendues de multi diffusion
Les adresses de multi diffusion sont utilisées par des applications de conférences audio et/ou vidéo. Les adresses de diffusion de multicast sont de classe D (224.0.0.0 à 239.255.255.255). Les clients possédant cette adresse IP traiteront les messages et seulement eux. Cela permet l'envoi d'informations à plusieurs clients tout en n'envoyant qu'un seul message.



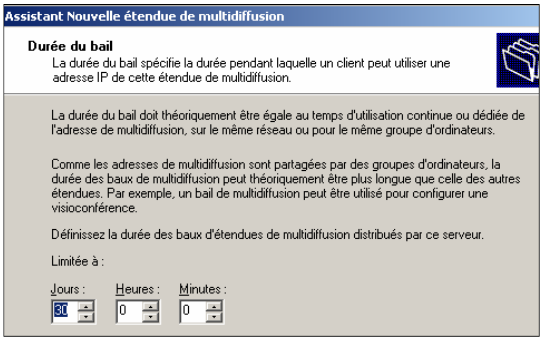


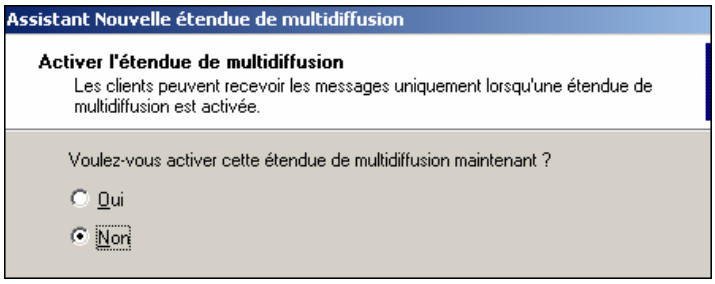
Après avoir donné un nom à l'étendue, il faut entrer l'adresse de début et l'adresse de fin.
Entrer ensuite le masque de sous réseau qui sera envoyé aux clients réseau. La longueur demandée est le nombre de bits à 1 dans le masque de sous réseau.
Si une ou plusieurs plages d'adresses IP sont à exclure de l'étendue, il est possible de les rentrer dans cette fenêtre.

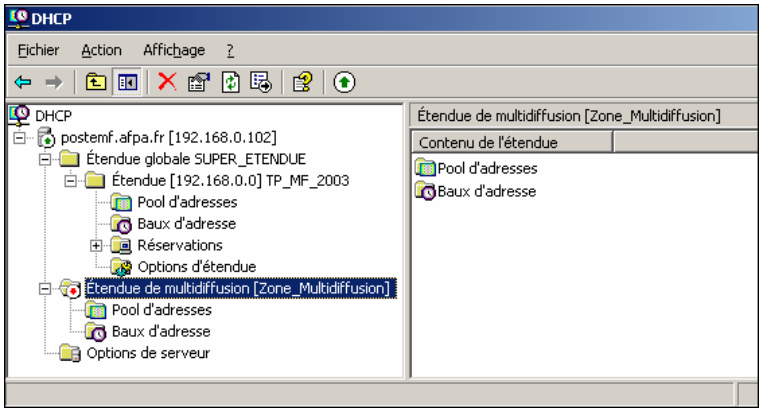




Rappel : la durée de vie correspond au nombre maximal de routeurs susceptible d'être traversé. La valeur par défaut est 32.
Il est possible de fixer la durée des baux. La valeur par défaut est de 8 jours. La fenêtre suivante demande si l'on veut indiquer les options immédiatement ou plus tard.
Ces options sont des informations qui seront envoyées au client pour le configurer. Ces options comprennent, entre autre, le nom du domaine, le nom des serveurs DNS ou WINS

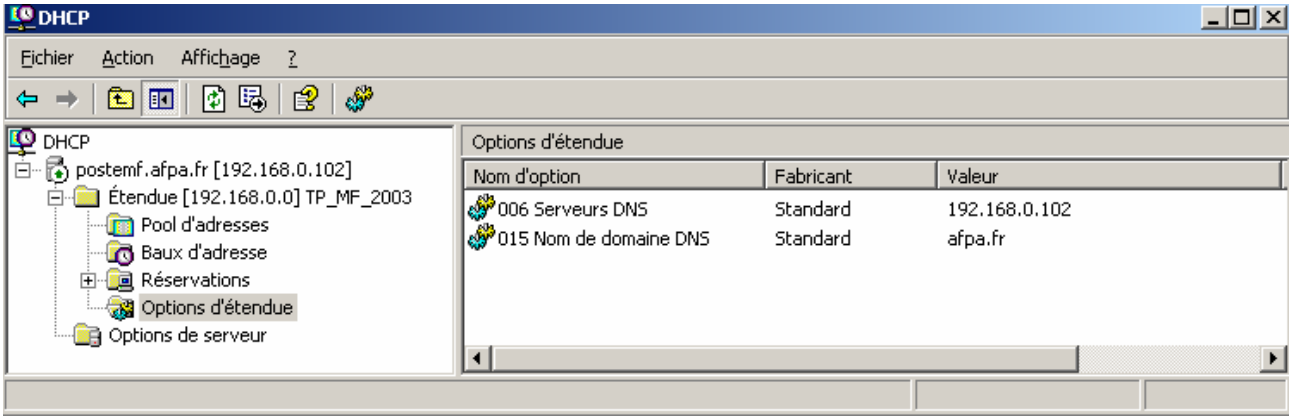




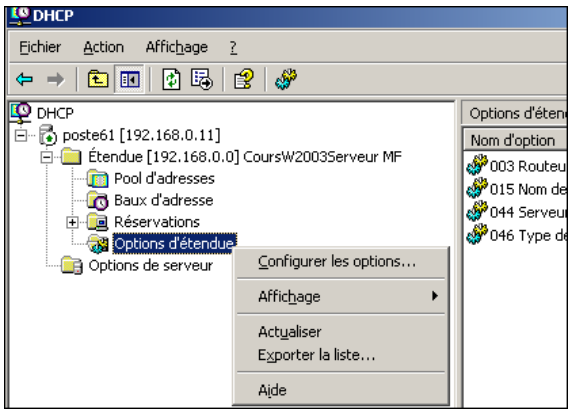


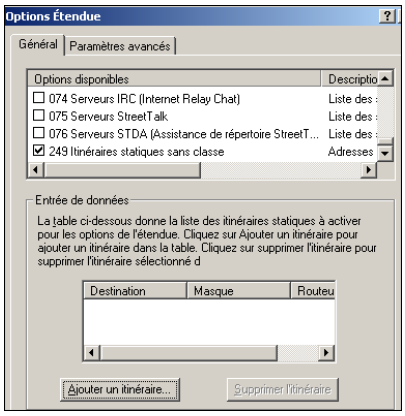
Options et classes d'options
Configuration d'une option
Comme nous l'avons déjà vu lorsqu'il existe un serveur DHCP, celui-ci distribue au minimum une adresse IP et un masque de sous réseau au client. Les autres paramétrages sont optionnels. Les plus courants sont :

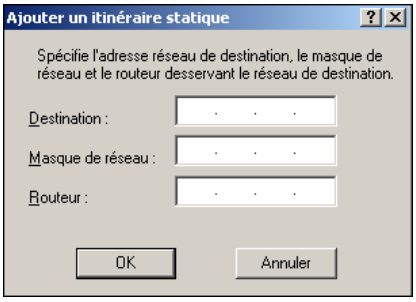
- (003) Adresse de la passerelle.
- (015) Nom de domaine DNS.
- (006) Adresse de serveur DNS.
- (044) Adresse de serveur WINS.
- (046) Type de nœud WINS.
- …



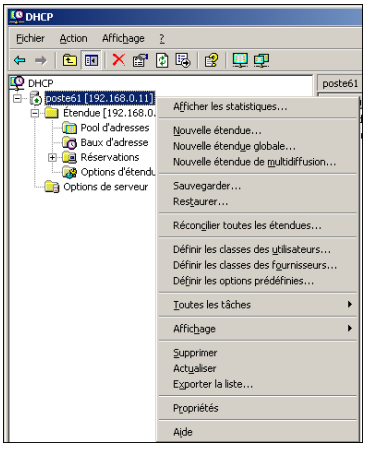
A partir de la console de gestion du serveur **DHCP**, vous pouvez configurer des options d'étendues et des options de serveur qui portaient le nom options globales sous Windows NT. Ces options globales concernées toutes les étendues. Par défaut avec un serveur DHCP, les options d'étendue ont la priorité sur les options globales.
Pour ce qui concerne les réservations vous pouvez définir des options spécifiques qui auront la priorité sur les options d'étendue et de serveur.
Une nouvelle option est désormais disponible avec Windows Server 2003 par rapport à NT4, c'est l'option **Itinéraires statiques sans classe** (249) qui permet l'ajout de routes supplémentaires dans la table de routage des clients réseau.
Lorsqu'il existe un client d'accès distant en VPN (Virtual Private Network ou réseau privé virtuel) que nous verrons plus loin, cela peut l'aider à accéder à d'autres réseaux comme Internet par exemple sans avoir de passer par le réseau d'entreprise. Cela aide aussi à mieux gérer le trafic sur le réseau de l'entreprise.

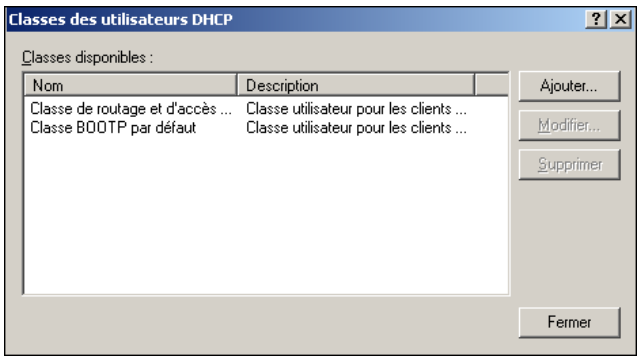


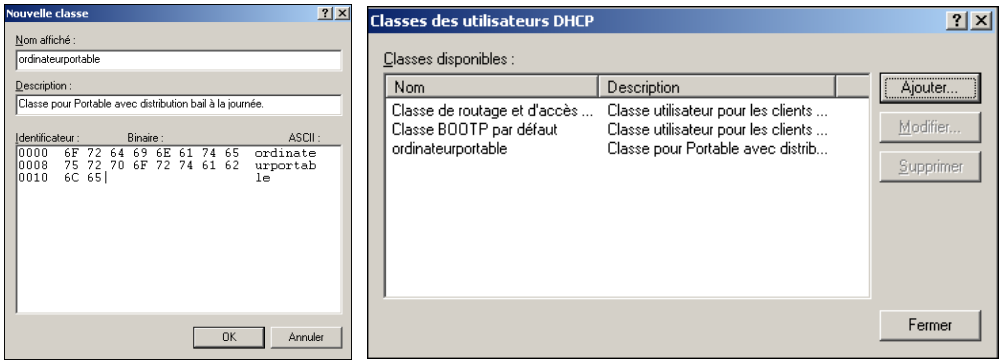


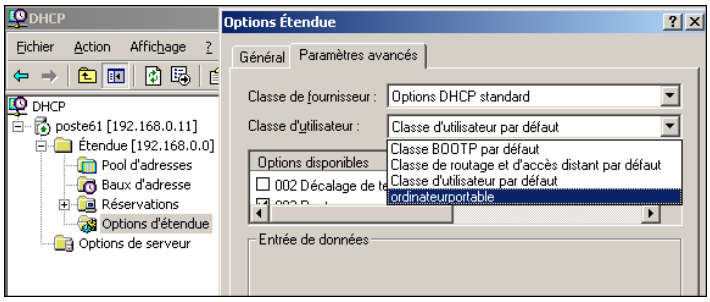


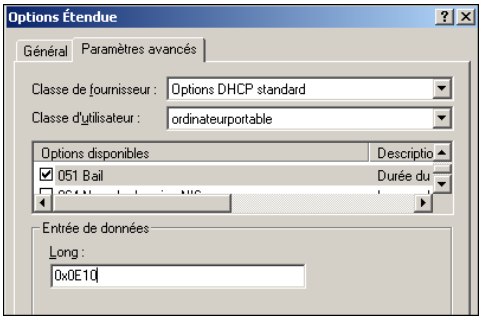
Les classes d'options
Cela permet contrairement à Windows NT4 de distribuer des configurations différentes aux clients. Cette configuration peut être distribuée en fonction du système d'exploitation, c'est ce qu'on nomme options de fournisseurs ou en fonction de critères définis pour ses propres besoins, ce sont les options d'utilisateur.



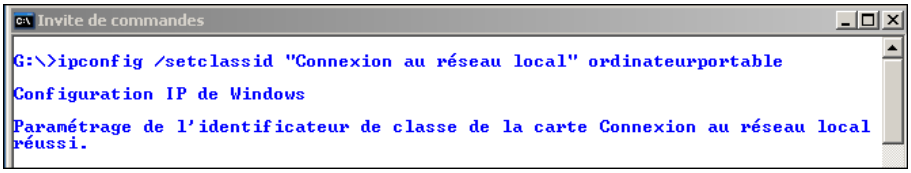




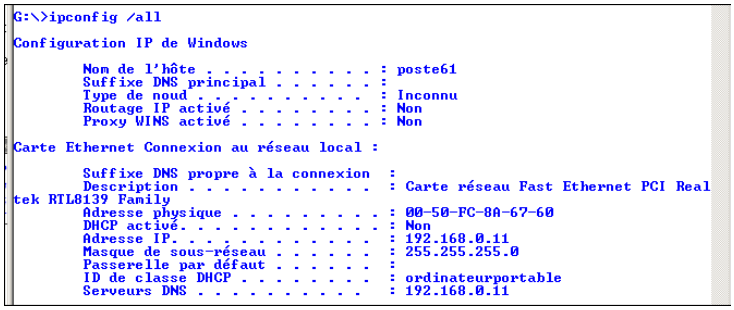




Par exemple, si vous souhaitez que la durée du bail soit d'une heure, tapez 3600 (E10).
Maintenant pour configurer le poste client vous devez utiliser la commande ipconfig :
Ipconfig /setclassid connexion au réseau local ordinateurportable avec connexion **au réseau local** qui représente le nom de votre connexion réseau.

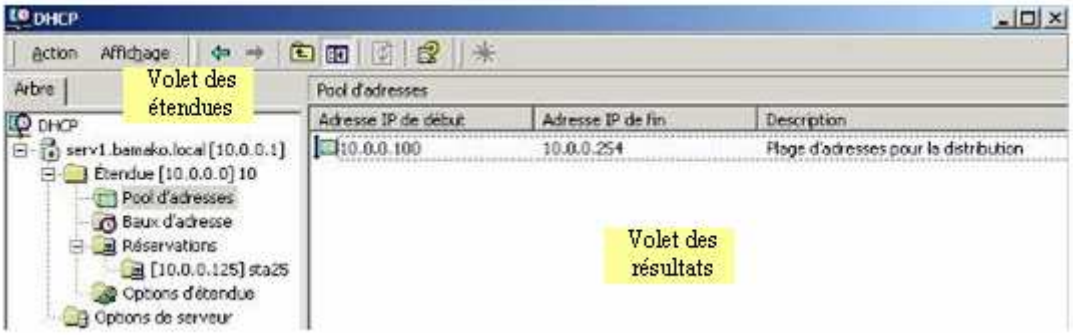


Pour afficher le nom de la classe il vous suffit de taper en mode commande :
Ipconfig /all
Ipconfig /showclassid connexion au réseau local



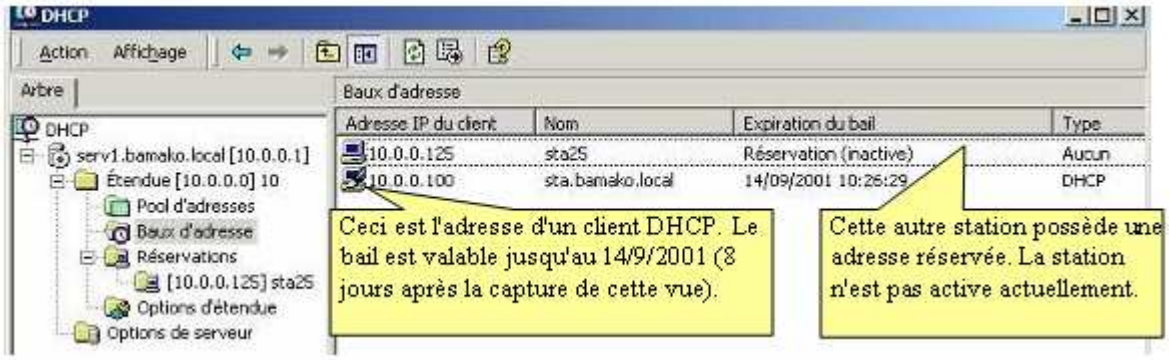
Gestion du serveur DHCP

Une fois l'installation et la configuration d'étendue terminées, on peut gérer le serveur DHCP en utilisant la console **DHCP** qui se trouve dans **Outils d'administration**. La fenêtre se présente sous la forme ci-dessous. Si dans le volet des étendues, on clique sur **Pool d'adresses**, on visualise dans le volet des résultats les plages d'adresses déclarées.

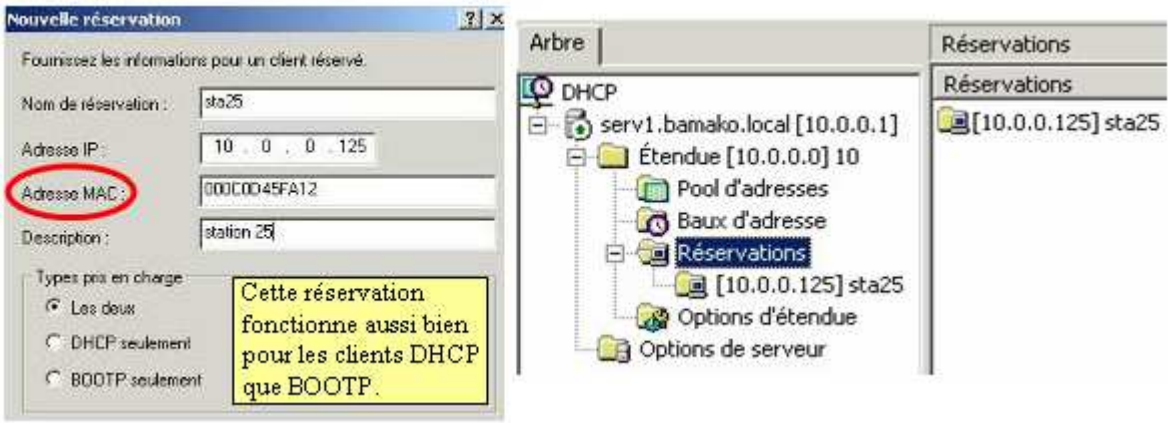


Console DHCP : Pool d'adresses

La sélection du sous-dossier **Baux d'adresses** permet de visualiser les baux actifs.



La sélection du sous-dossier **Réservations** permet d'affecter toujours la même adresse IP à un ordinateur dont on indique l'adresse MAC. Pour ajouter une **Réservation**, sélectionner le sous-dossier **Réservations** et dans le menu **Action**, cliquer sur **Nouvelle réservation…**.



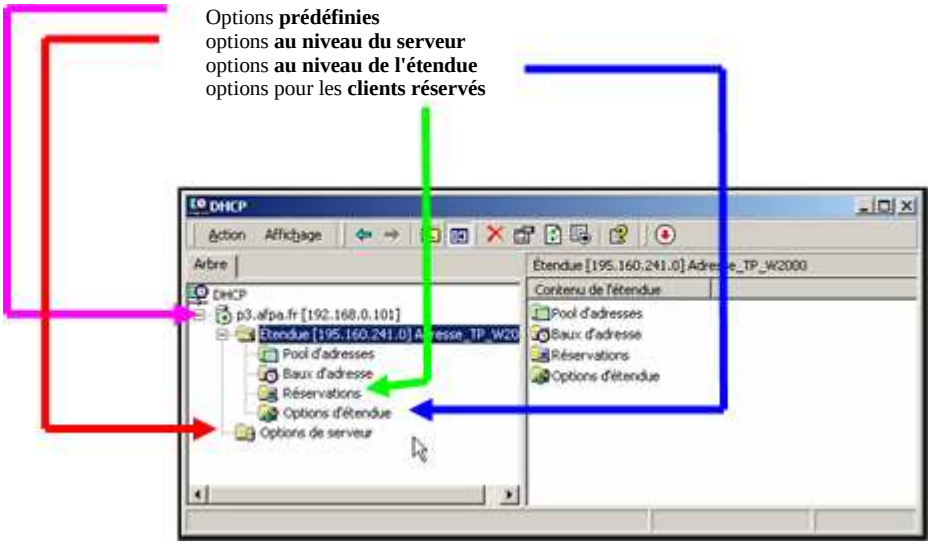
Options DHCP

On peut définir quatre types **d'options DHCP** :

- Des options prédéfinies. Sélectionnez le serveur DHCP dans la console et dans le menu contextuel, validez **Paramétrer les options prédéfinies…**.
- Des options au niveau du serveur en sélectionnant le sous-dossier **Options du serveur**, puis dans le menu contextuel **Configurations des options**, onglet **Général** ou onglet **Avancé**.

- Des options au niveau de l'étendue en développant **Etendue**…, puis en sélectionnant le sous-dossier **Options d'étendue**.
- Des options pour les **clients réservés** en cliquant sur le sous-dossier de l'adresse réservée (réservation).

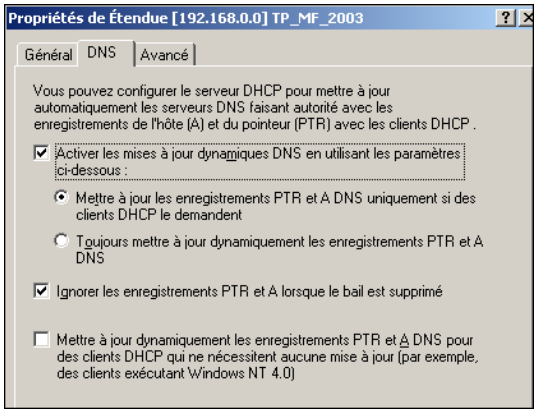
4 types d'options DHCP :



De plus des **Classes** de clients peuvent être définies pour leur appliquer plus facilement des options. Une liste de classes prédéfinies existe et suffit pour la plupart des cas. Les fonctions de base sont décrites dans la RFC 1479 dont il existe des extraits dans l'aide de Windows 2003 (options DHCP, vue d'ensemble). Ces options sont envoyées à l'intérieur des réponses DHCP (DHCPREQUEST et DHCPACK) du serveur, lorsque le client démarre ou renouvelle son bail. Chaque option comporte un code, une valeur, une longueur qui est en relation avec la valeur. Le code et la longueur sont définis chacun par un octet. La longueur du champ valeur peut comporter plusieurs octets (par exemple quatre pour une adresse IP ou un masque).
Le tableau ci-dessous décrit quelques options les plus utilisées :

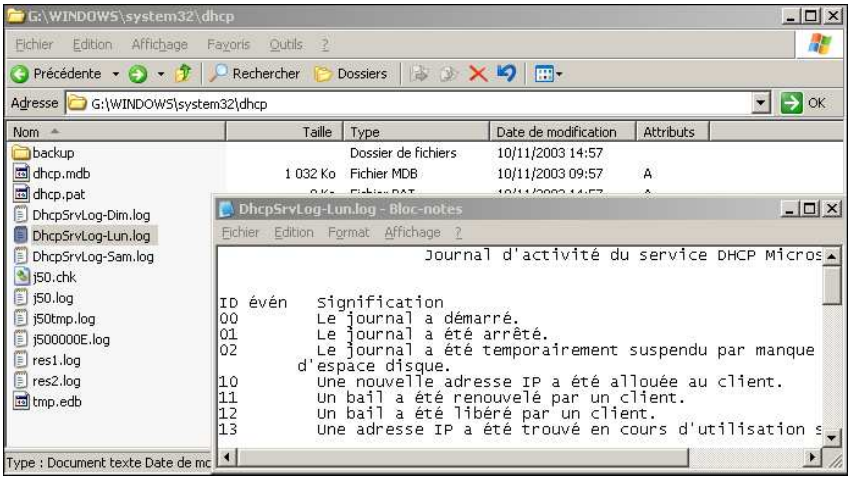
Nom	Code	Valeur	Description
Routeur	003	Adresses IP d'un ou plusieurs serveurs	Spécifie une ou plusieurs adresses IP de routeurs connectés au réseau et accessibles au client.
Serveur DNS	006	Adresses IP d'un ou plusieurs serveurs	Spécifie une ou plusieurs adresses IP de serveurs DNS du réseau.
Nom de domaine	015	Chaîne de caractères	Définit le nom de domaine dans lequel se trouve le client.
Serveur WINS	044	Adresses IP du ou des serveurs	Spécifie une ou plusieurs adresses IP de serveurs WINS du réseau.

Propriétés des serveurs DHCP
Mise à jour des serveurs DNS

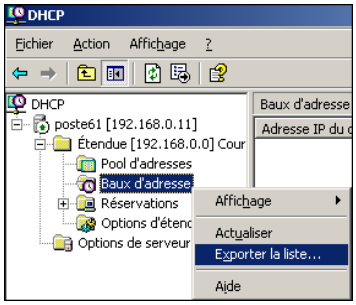


Le serveur DNS de Windows 2003 Server peut être mis à jour de façon dynamique par ses clients. Dans le cas des clients d'un serveur DHCP, celui-ci peut mettre à jour directement le serveur DNS. Pour cela il vous suffit de cliquer **droit** sur le nom du **serveur DNS** et de valider **l'onglet DNS** dans la fenêtre des **Propriétés**. Cochez les options désirées avec en particulier **Activer les mises à jour dynamiques DNS en utilisant les paramètres ci-dessous**. Puis cochez soit dynamiquement ou manuellement la mise à jour des enregistrements de type **PTR et A DNS.**

Suivi de l'activité du serveur DHCP
Le serveur DHCP créée par défaut un journal d'activité dans le dossier **%systemroot%\sytem32\DHCP**. Cela permet d'avoir un historique du déroulement des opérations d'attribution.

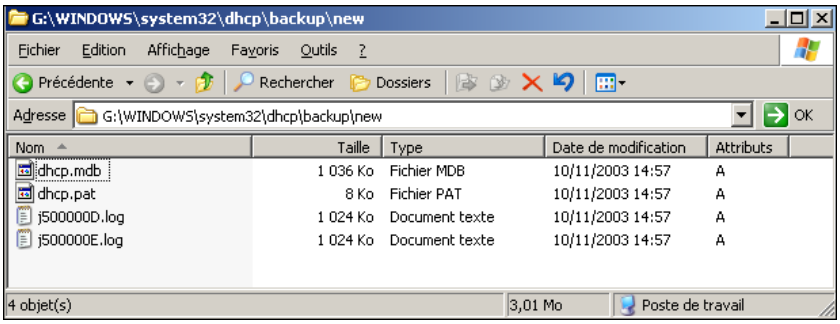


Vous pouvez aussi enregistrer dans un fichier texte délimité par des virgules ou des tabulations, les baux attribués par le serveur DHCP afin de les récupérer avec des applications comme des tableurs ou base de données.

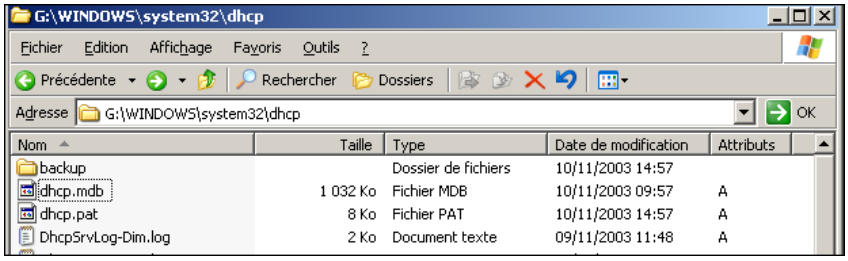


9.3.3- Sauvegarde et restauration des données DHCP

La base de données DHCP est sauvegardée toutes les heures dans le dossier : **\%systemroot%\System32\dhcp\Backup\new.**



La base de données elle-même se situe dans **\%systemroot\System32\Dhcp.**



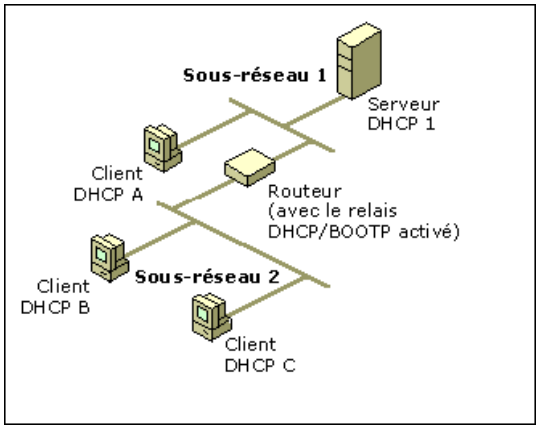
9.3.4- Agent de relais DHCP

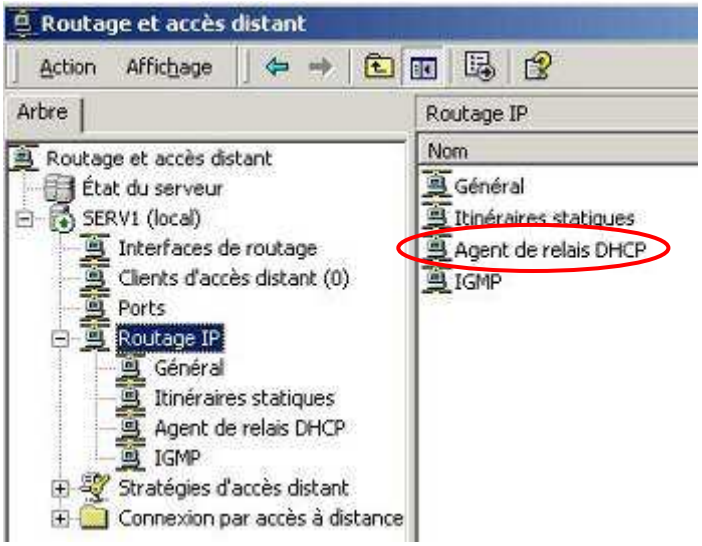
Un agent relais est un petit programme qui relaie les messages **DHCP/BOOTP** entre les clients et les serveurs de différents sous réseaux. Il relaie les messages **DHCP/BOOTP** diffusés sur l'une des interfaces physiques qui lui sont connectées, telle une carte réseau, vers d'autres sous réseaux à distance auxquels il est connecté par d'autres interfaces physiques.

Principe de l'Agent de relais DHCP
Les clients DHCP reçoivent leur bail d'adresses IP de serveurs DHCP via des messages de type sous réseau qui ne sont pas véhiculés systématiquement par les routeurs.
Si vous avez plusieurs segments réseaux séparés par des routeurs vous devez avoir :

- Soit un serveur DHCP par segment.
- Soit faire jouer à un serveur W2003 le rôle d'agent de relais DHCP.

Cet agent est installé en même temps que le **Service de routage et accès distant**.
Un agent relais possède une adresse IP statique et connaît l'adresse IP du serveur DHCP.
Il intercepte les broadcasts DHCP envoyés par les clients afin de les router vers le serveur DHCP





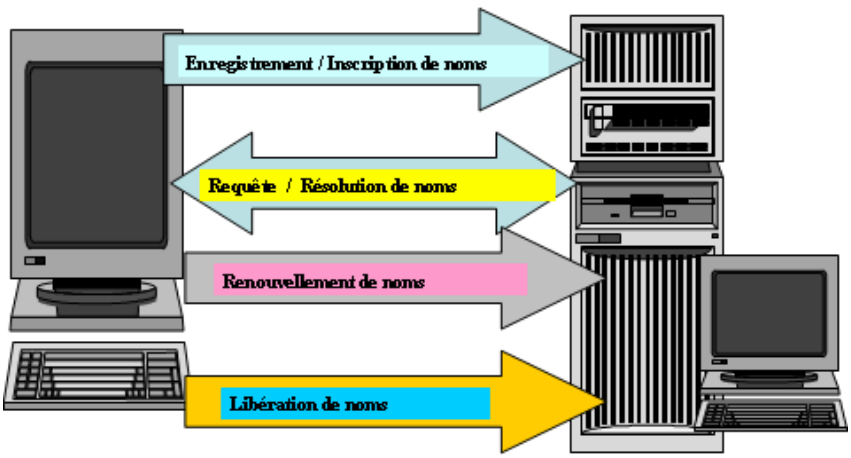
Les messages DHCP étant pour certains des messages de type sous réseau, ils ne sont pas véhiculés systématiquement par les routeurs. Si l'on désire mettre en œuvre un serveur DHCP Windows 2003 pour plusieurs réseaux IP reliés par des routeurs, il faut que ces routeurs possèdent un agent de relais réseau. Si le routeur est un serveur Windows 2003, il est possible d'y installer un agent de relais réseau.
Cet agent est installé en même temps que le **Service de routage et accès distant**.

9.4- WINS

9.4.1- Présentation

Le service **WINS** (Windows Internet Name Service) n'est pas nécessaire dans un environnement Windows 2003 TCP/IP natif. Le serveur DNS suffit pour faire la correspondance entre les noms des ordinateurs et leurs adresses IP. Cependant sur un réseau, même si les serveurs sont des serveurs Windows 2003, il est fort probable que **toutes** les stations ne sont pas des stations Windows 2000.
Si un réseau possède des stations NT, 98 ou 95, le système mis en œuvre pour faire correspondre le nom NetBIOS avec leur adresse IP est le système WINS. Un des avantages de WINS par rapport à DNS est que la mise à jour de la base de données de correspondance nom / adresse IP se fait de manière automatique. Dans le système DNS pur, l'administrateur doit entrer les noms et les adresses de manière manuelle. La mise à jour doit aussi être faite manuellement lorsqu'on ajoute ou enlève un ordinateur. L'inconvénient de WINS est qu'il fait appel au nom NetBIOS qui est un concept utilisé par Microsoft et qui n'existe pas sous UNIX par exemple. Ce service d'implémentation Microsoft de résolution de noms NetBIOS, est un service dynamique (alors que DNS ne l'est pas avec NT4). Ce service va vous permettre de résoudre les noms NetBIOS. On peut rappeler qu'un nom NetBIOS est un nom composé de 16 caractères dont le denier caractère, hexadécimal, est caractéristique car il indique le service proposé.
Poste61maurice[20h] indique qu'il s'agit du service serveur de l'ordinateur **Poste61maurice**.
Afpacaen[1C] indique qu'il s'agit d'un contrôleur de domaine du domaine **AfpaCaen**.
En résumé ce service WINS existe toujours sous W2003 Server pour des raisons de compatibilité avec les versions antérieures à W2000 et va disparaître dans le futur...

9.4.2- Processus de résolution de noms WINS

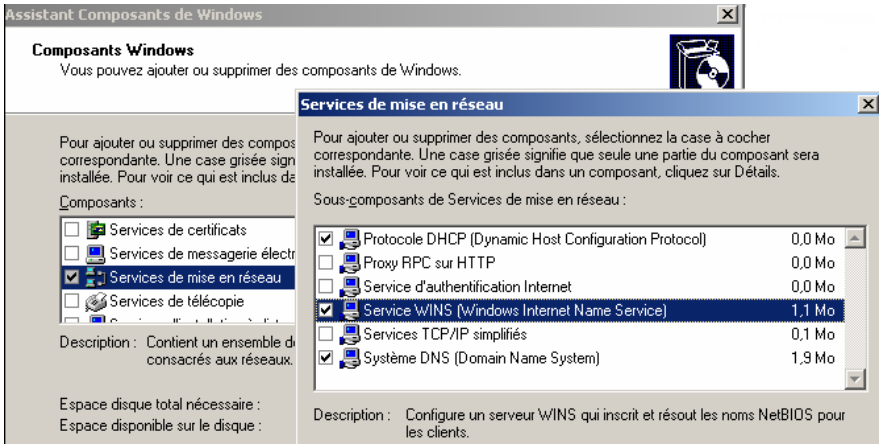


Le processus de résolution de noms WINS permet aux ordinateurs Microsoft du réseau de s'inscrire auprès d'un **serveur WINS.** La base de données de ce serveur renferme entre autres, leur nom NetBIOS et leur adresse IP. Voici les processus existants entre une station et le serveur WINS:

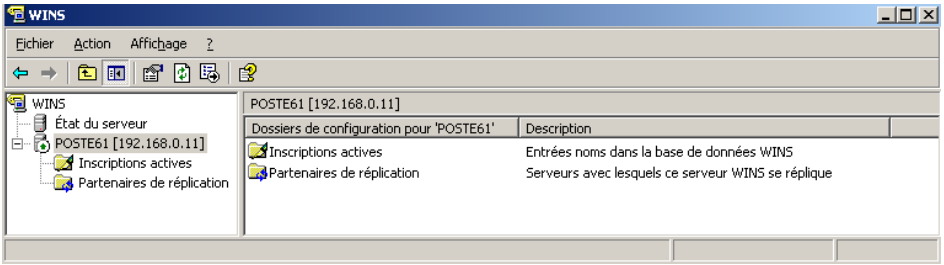
- **Inscription** : chaque fois qu'un client WINS démarre, il se fait connaître auprès du serveur WINS dont l'adresse IP a été entrée dans la configuration TCP/IP de l'ordinateur. Si l'ordinateur est aussi un client DHCP, c'est l'adresse IP fournie par ce serveur qui sera inscrite avec le nom NetBIOS dans la base de données **WINS**.
- **Résolution** : lorsqu'une commande contenant un nom NetBIOS, est envoyée par un client WINS, ce nom doit être remplacée par l'adresse IP correspondante. Le client WINS envoie la demande de correspondance au serveur WINS qui lui retourne l'adresse IP. La commande peut alors être envoyée sur le réseau vers l'ordinateur destinataire. Voir détails plus loin.
- **Renouvellement** : la durée du mappage (correspondance) entre le nom et l'adresse IP correspondante est limitée dans le temps. En effet, il est inutile qu'une station éteinte (de manière anormale) apparaisse dans la base de données WINS. Un **TTL** (Time To Live) est fixé et correspond à la durée du mappage dans le serveur WINS. Lorsqu'un huitième de la durée TTL s'est écoulée, le client renouvelle sa demande d'inscription et la durée est remise à la valeur correspondant au TTL. Si la station est arrêtée de manière anormale ou pour tout autre raison, lorsque la durée TTL est atteinte, le mappage est détruit.
- **Libération** : lorsqu'une station cliente WINS s'arrête de façon normale, avant de quitter le réseau, elle envoie une demande pour détruire le mappage entre son nom et l'adresse IP correspondante.

9.4.3- Implémentation du service WINS

L'installation du serveur WINS n'est pas incluse dans l'installation par défaut du serveur WINDOWS 2003. Cette installation se fait à partir du **Panneau de configuration – Ajout/Suppression de programmes - Ajouter/Supprimer des composants Windows**. Dans la fenêtre **Composant Windows**, sélectionnez **Services de mise en réseau**, puis **Service WINS….**

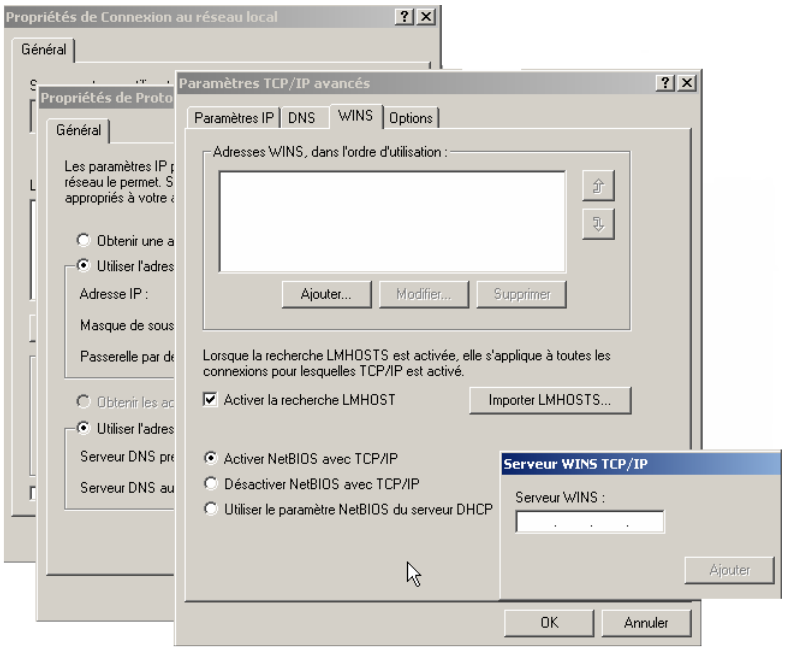


La gestion du serveur WINS, sauf cas spécial est réduite au minimum. Une console prédéfinie permet de gérer le serveur WINS grâce au composant logiciel enfichable **WINS** que l'on trouve dans les **Outils d'administration**. La console présente l'aspect suivant à son ouverture.

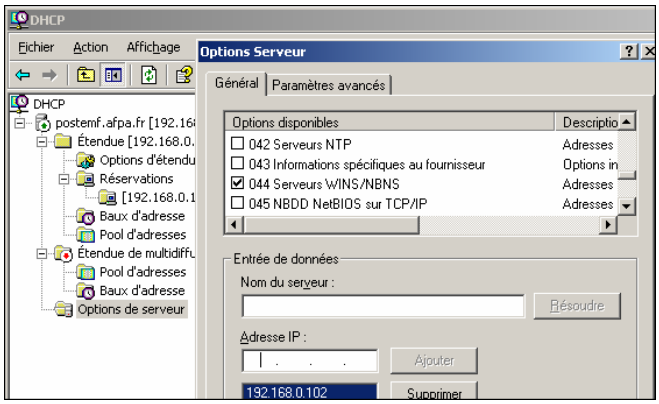


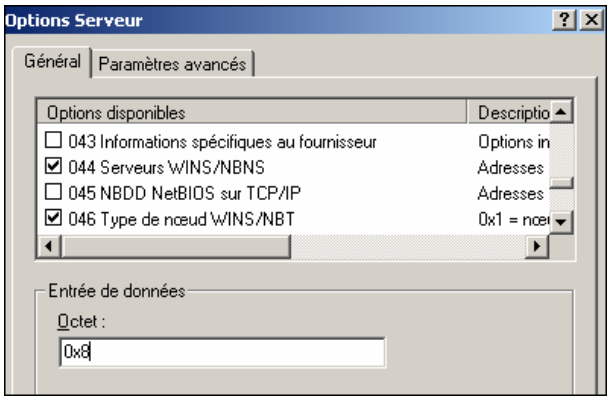
9.4.4- Configuration des Clients WINS

Configuration statique du client
A partir du poste client (ici cas de W2003 Server membre) **Propriétés** de TCP/IP ➔ **Avancé** ➔ **WINS** ➔ Ajouter l'adresse du serveur **WINS.**



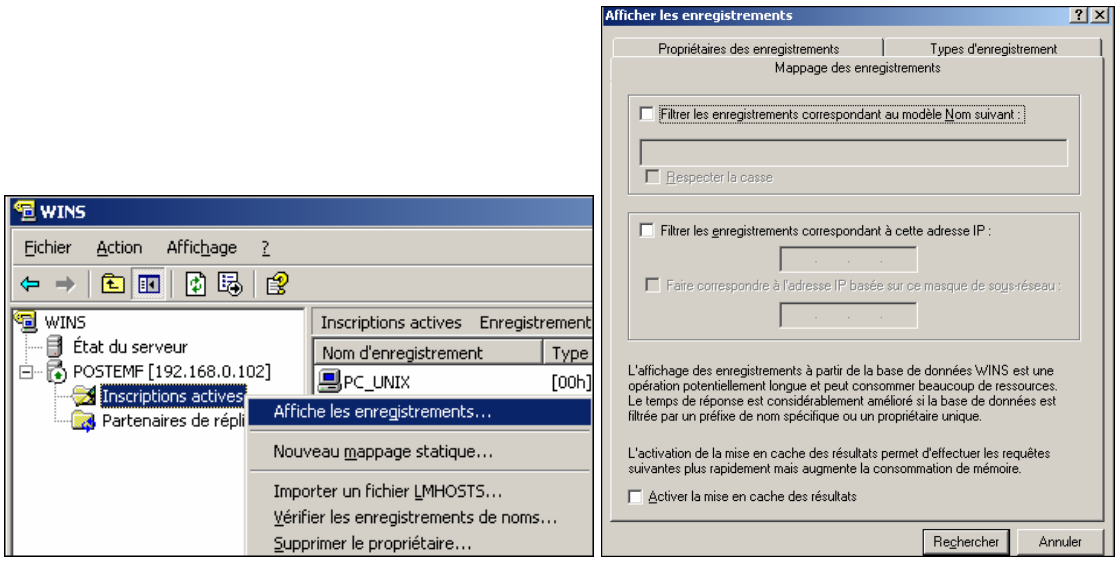
Configuration dynamique des Clients WINS et méthode de résolution des noms
Pour cela vous devez activer les options **044** et **046** d'un serveur DHCP.
046 Type de nœud WINS/NBT ➔ entrée des données.
Ox1 : **B-nœud :** les clients utilisent des diffusions pour résoudre les noms NetBios en adresse IP.
0x2 : P-nœud : les clients utilisent un serveur de noms afin de s'enregistrer et résoudre les noms NetBios en adresses IP.
0x4 : M-nœud : mode Mixte où les clients utilisent d'abord la diffusion puis un serveur de noms.
0x8 : type de nœud hybride permettant d'abord l'utilisation d'un serveur de noms, puis la diffusion si nécessaire.





9.4.5- Affichage de la base de donnés du serveur WINS

Si l'on veut rechercher un ordinateur dans la base de données pour l'afficher dans le volet droit de la console, il faut utiliser l'option **Rechercher par…** dans le menu contextuel de **Inscriptions actives**. Si on utilise le caractère générique ***** pour la recherche, tous les noms NETBIOS stockés dans la base de données apparaissent. Certains noms apparaissent plusieurs fois, mais affublés d'un numéro différent. Ces numéros correspondent à des types de noms NetBIOS.

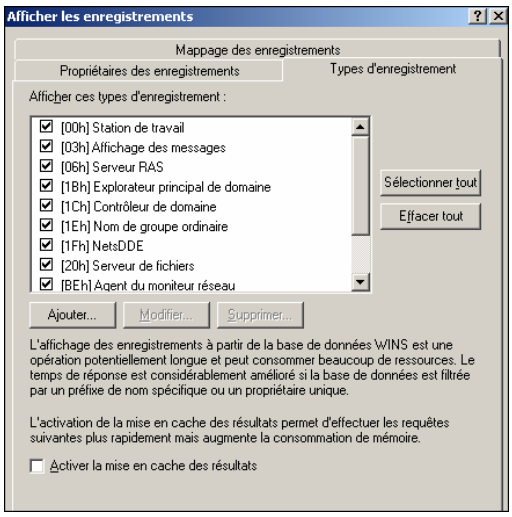


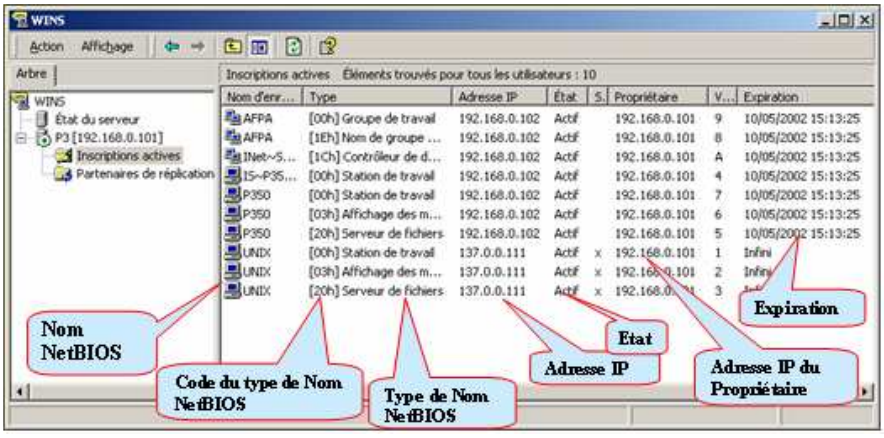
La fenêtre **Afficher les enregistrements** permet de définir des filtres d'affichage des enregistrements. Cette fenêtre possède 3 onglets :

Mappage des enregistrements : permet de sélectionner les enregistrements en fonction des noms de machine, de domaine, des adresses IP. Cochez **Activer la mise en cache des résultats** pour mise en cache local (RAM) les résultats de la recherche.

Propriétaires des enregistrements : permet de sélectionner les enregistrements en fonction de leur propriétaire. Le propriétaire est le serveur qui a inscrit l'enregistrement sur le serveur.

Types d'enregistrement : permet de sélectionner les enregistrements en fonction de leur type suivant la valeur du 16éme caractère du nom NetBIOS.





Quelques codes des types de nom NetBIOS

Nom et Code	Type	Description
Nom_d'ordinateur [00h]	Unique	Le nom correspond à une station de travail.
Nom_d'ordinateur [03h]	Unique	Le nom correspond au service affichage des messages. Il est associé à chaque utilisateur connecté.
Nom_domaine [1Bh]	Unique	Correspond au contrôleur de domaine.
Nom_ordinateur [20h]	Unique	Correspond à la fonction serveur d'un ordinateur.
Nom_utilisateur [03h]	Unique	Correspond à chaque utilisateur connecté.
Nom_domaine [00h]	Groupe	Indique le nom du domaine de la station.

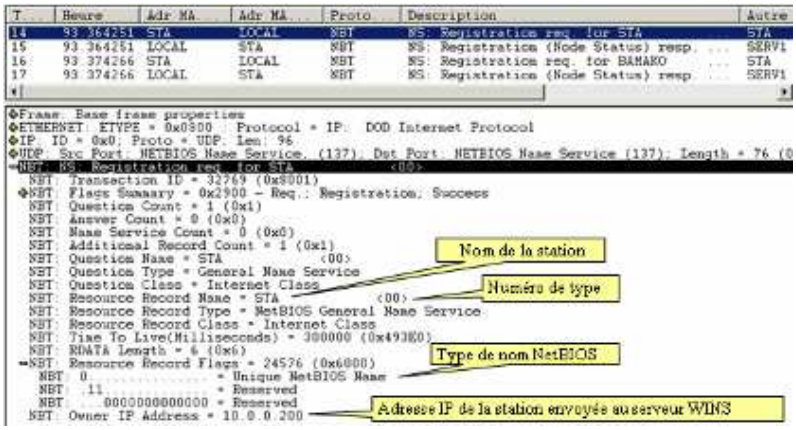
✋ La base WINS peut être exportée comme la base DHCP dans un fichier texte avec séparation par des virgules ou des tabulations.

Pour supprimer un enregistrement, il suffit de le sélectionner, puis avec un clic droit de valider l'option **Supprimer**. Dans la fenêtre **Supprimer la fiche**, deux possibilités s'offrent à vous :

- **Supprimer l'enregistrement sur ce serveur uniquement :** dans ce cas l'enregistrement est physiquement supprimé.
- **Répliquer la suppression de l'enregistrement sur d'autres serveur (désactiver) :** dans ce cas l'enregistrement ne sera pas supprimé, mais juste marquer comme étant désactivé et son numéro de version modifié afin de répliquer l'information vers les autres partenaires de réplication.

9.4.6- Séquences d'enregistrement NetBIOS WINS d'une station

Phase d'inscription du nom de la station (requête)



Phase de réponse du serveur

Phase d'inscription du nom de domaine

Phase de réponse du serveur de noms

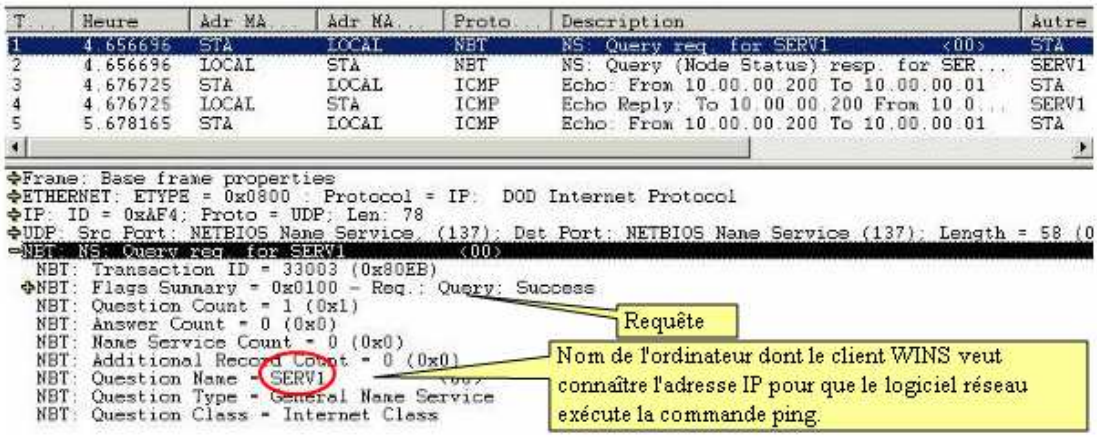
9.4.7- Résolution de nom

Le chapitre précédent décrivait comment une station s'inscrit auprès du serveur WINS. Mais que ce passe-t-il lorsqu'une station a besoin de connaître l'adresse IP d'un autre ordinateur dont seul le nom est connu ? Lorsque la station a déclaré une adresse de serveur WINS, elle devient client WINS et c'est un nœud NetBIOS hybride. Voici les phases de recherche d'une adresse IP d'un autre ordinateur du réseau par un client WINS :

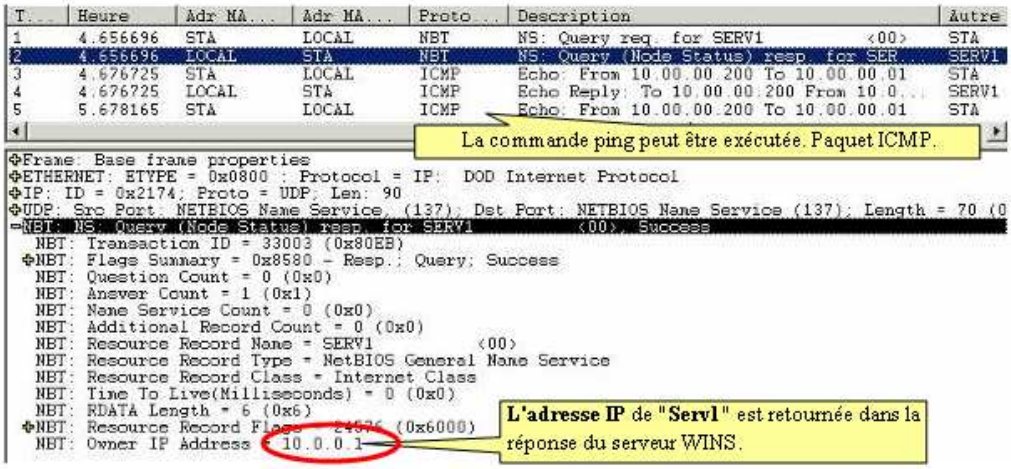
- Le client consulte son cache de noms NetBIOS afin d'y rechercher la correspondance entre le nom et l'adresse IP recherchée (adresse conservée dans le cache suite à une précédente recherche).
- Si le client ne possède pas l'adresse dans son cache, il fait une demande au serveur WINS principal.
- Si ce serveur ne répond pas, la requête est renouvelée deux fois.
- Le client tente de joindre un serveur WINS secondaire.
- Si aucun serveur WINS ne répond, le client procède en mode broadcast.

Exemple : tapons sur une station la commande **ping serv1**. Serv1 est un serveur du réseau. Pour exécuter la commande ping, le logiciel réseau de la station a besoin de connaître **l'adresse IP** de ce serveur. En supposant que DNS est invalidé et que WINS est validé dans cette station, le client WINS envoie une requête au serveur WINS qui va retourner l'adresse IP de SERV1 - qui est aussi dans cet exemple le serveur WINS (cas particulier). Une fois l'adresse connue, la commande ping peut être exécutée.

Requête du client WINS de la station

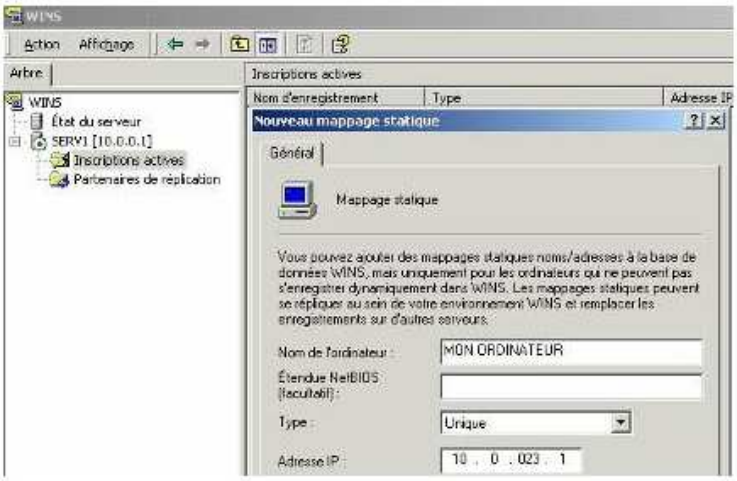


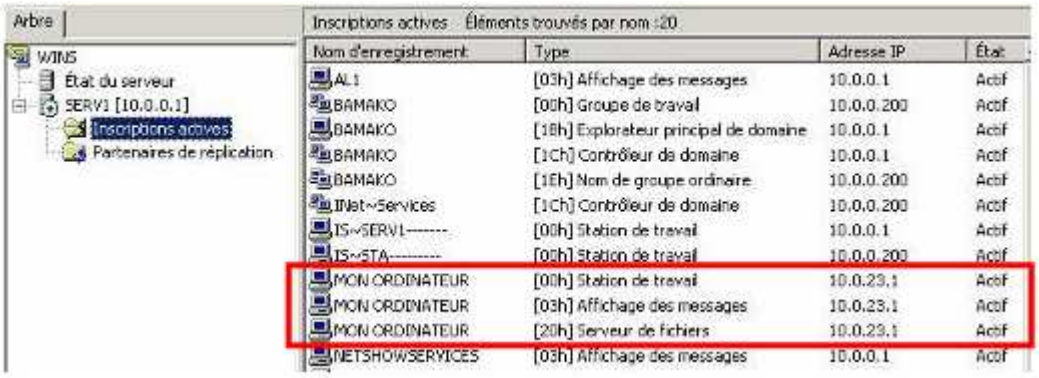
Réponse du serveur WINS



9.4.8- Correspondance statique

S'il existe sur le réseau des ordinateurs qui n'ont pas de client WINS, mais qui possèdent une adresse IP, vous pouvez créer manuellement un mappage entre le nom d'un de ces ordinateurs et son adresse IP. On parle alors de mappage statique. Pour ajouter un nom et une adresse, dans la console WINS, cliquer sur le sous-dossier **Inscriptions actives** et dans le menu contextuel, utiliser **Nouveau mappage statique…**. Dans la fenêtre qui s'ouvre, entrez le nom donné à cet ordinateur et son adresse IP.

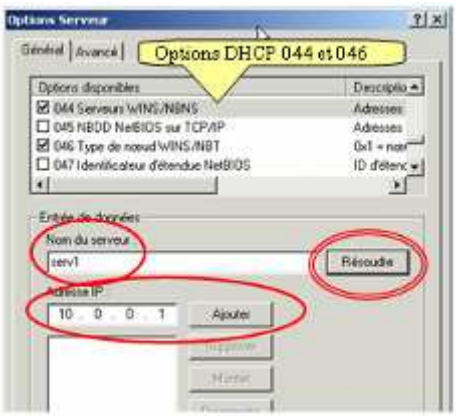




9.4.9- Déclaration d'un serveur WINS dans la configuration DHCP

Si une station est à la fois client WINS et client DHCP, on peut configurer le serveur DHCP, pour qu'il envoie directement l'adresse du serveur WINS dans la réponse. Ceci évite de paramétrer l'adresse du serveur WINS sur chaque ordinateur. Pour cela, ouvrir la console DHCP, dans **Options du serveur**.

- Cocher les options DHCP 044 et 046.
- Entrez le nom du serveur DHCP.
- Appuyer sur **Résoudre**.
- L'adresse IP apparaît, appuyer sur **Ajouter**.
- **OK**.

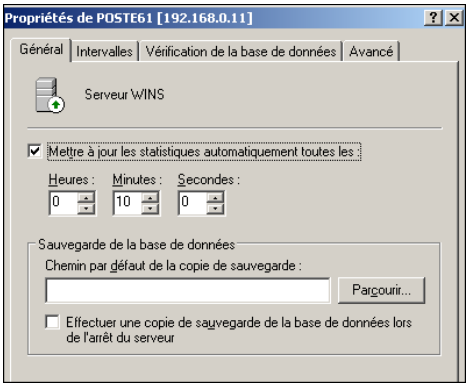


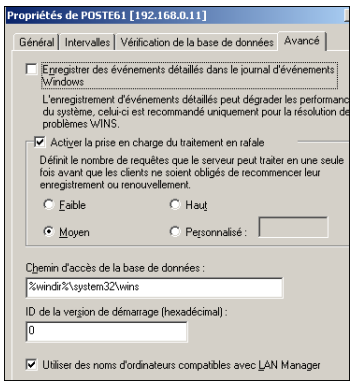
9.4.10- Partenaires de duplication d'un serveur WINS

Lorsque plusieurs serveurs WINS sont utilisés dans votre réseau, ils peuvent être configurés pour répliquer les enregistrements de leur base de données sur d'autres serveurs. Les partenaires de duplication permettent aux serveurs WINS de récupérer les bases d'enregistrements des serveurs partenaires. Sous NT4 on parle de **Partenaire** qui peut être **Tiré** (avec heures de duplication) ou de **Partenaire Poussé** avec le nombre de modification à atteindre avant une réplication.
Sous W2003 Server on emploie le terme **d'émission** pour poussé et **réception** pour tiré.
Dans le cas où vous avez paramétré votre serveur comme **tiré** vous devez entrer les heures de duplication.
Dans le cas d'un serveur de type **poussé** vous devez entrer le nombre de modifications à atteindre avant réplication.
Que vous ayez validé une ou les deux options vous devez cocher l'option **Utiliser une connexion permanente pour la réplication**.
Pour forcer une réplication à tout instant, validez **Répliquer maintenant** à partir d'un clic droit sur **Partenaires de réplication**.

9.4.11- Maintenance de la base WINS

Sélectionnez les propriétés du serveur WINS afin de visualiser les 4 onglets disponibles.
Général : permet d'entrer le chemin des sauvegardes par défaut de la base de données WINS, ainsi que l'intervalle de temps de mise à jour automatique des statistiques. Vous pouvez aussi décider de sélectionner une sauvegarde de la base à chaque arrêt du système.
Intervalles : identique au paramétrage du serveur WINS sous NT4 avec en particulier les intervalles de renouvellement, de libération, d'extinction et de vérification de la base.
Vérification de la base de données : permet de paramétrer les périodes de vérification de cohérence de la base avec les partenaires.
Avancé : permet de paramétrer le journal des enregistrements (détaillé et mode rafale). Vous pouvez aussi indiquer le chemin d'accès à la base de données WINS.

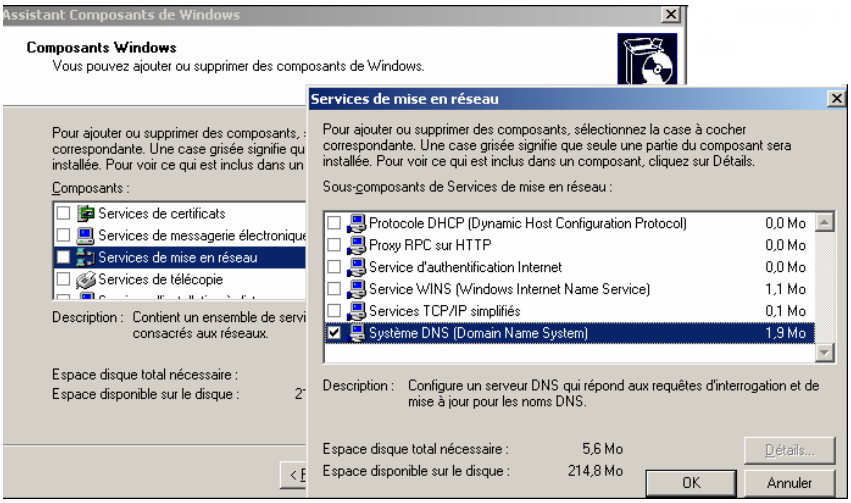




9.5- Système DNS

9.5.1- Installation et configuration du service DNS

Installation

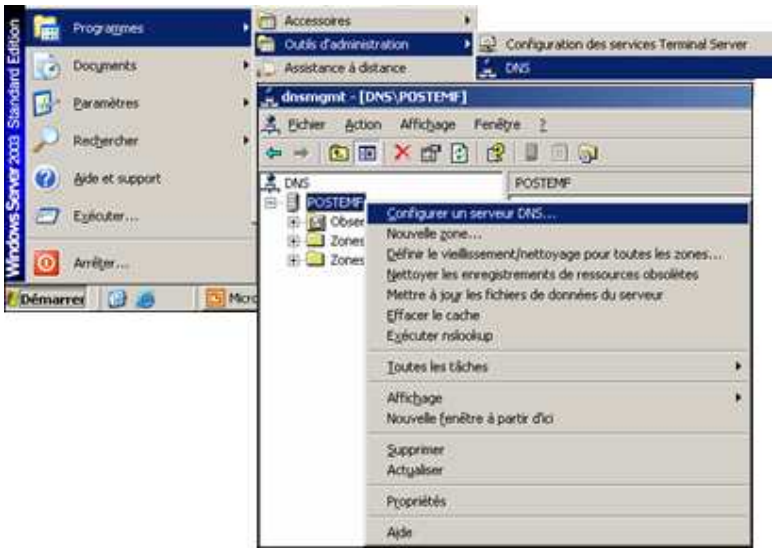


Si l'installation du serveur DNS n'a pas été faite au cours de l'installation première du serveur Windows 2003, il est possible de le faire soit à partir de **Configurer votre serveur - Mise en réseau – DNS** dans le menu **Outils d'administration**, soit à partir du **Panneau de configuration - Ajout:Suppression de programmes - Ajouter/Supprimer des composants Windows**. Le CD d'installation de Windows 2003 Server doit être disponible.

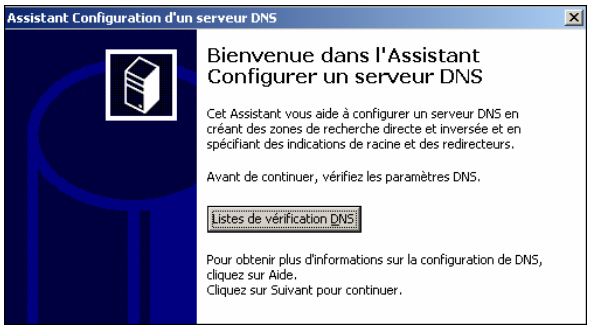
Configuration
Dans **Outils d'administration**, cliquer sur **DNS**. La console **DNS** s'ouvre.

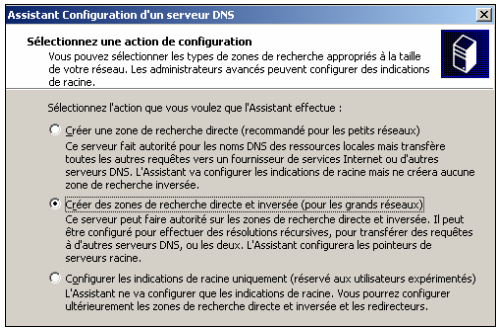
Console DNS

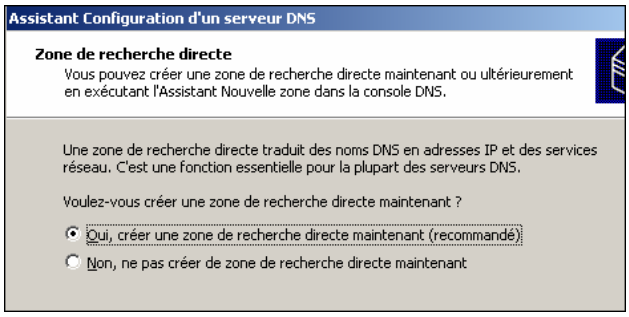
Cliquer sur le nom du serveur et dans le menu **Action**, sélectionner la ligne **Configurer le serveur…**. L'assistant s'ouvre. Si aucune zone n'existe ou si vous souhaitez en ajouter une nouvelle, l'assistant vous guide dans la création de zone de recherche directe, puis dans la création de zone inversée.

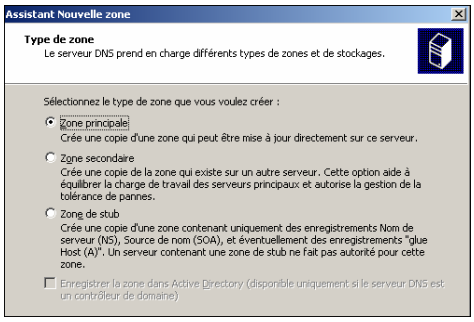


Création de zones de recherche directes





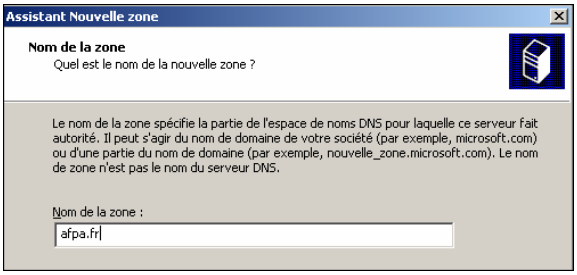


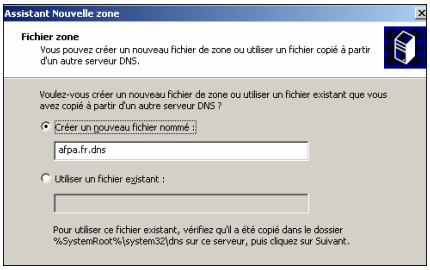


Quatre types de zone de recherche directe sont proposés :

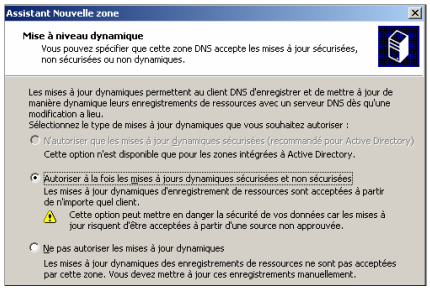
- **Zone intégrée à Active Directory** : ce type de zone est intégré à Active Directory. L'administrateur n'a pas accès à un fichier où se trouverait la liste des ordinateurs du domaine. Dès qu'un ordinateur est intégré au domaine, il est intégré à la zone Active Directory. Ce type de zone convient uniquement si tous les ordinateurs peuvent être inclus dans Active Directory, ce qui exclu les ordinateurs Windows 95, 98, NT ou Unix.
- **Zone principal standard** : ce type de zone correspond au type de zone utilisé sous Unix et dans les versions antérieures de Windows sous TCP/IP. Les noms des ordinateurs de la zone et leur adresse IP doivent être incorporés manuellement par l'administrateur (sauf si DDNS). Le fichier généré est un fichier texte compatible avec d'autres systèmes d'exploitation utilisant le protocole TCP/IP comme UNIX. C'est le type de zone proposée par défaut.

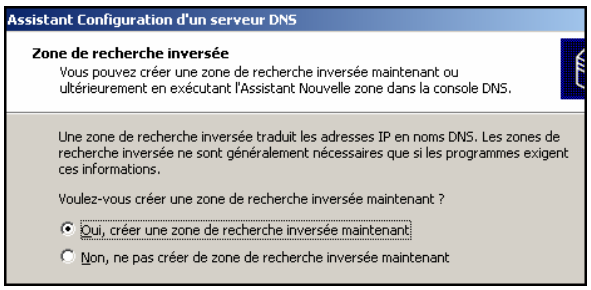
- **Zone secondaire standard** : ce type de zone est une réplique d'une zone existante. Le fichier de la zone principal qui se trouve sur le serveur DNS principal (Master) est dupliqué en lecture seule sur le serveur DNS où se situe la zone secondaire.
- **Zone stub** : c'est une nouveauté de W2003 Server. La zone **Stub** ne contient que les enregistrements nécessaires permettant d'identifier les serveurs DNS ayant autorité sur une zone. Cette zone Stub contient les enregistrements de type **SOA** (Start of Autority), **NS** (Name Server) ainsi que les enregistrements de type **A** (Adresse) nécessaires. Cette zone permet de retourner les adresses des serveurs DNS d'une zone comme lors des recherches de type itératives entre serveurs DNS.



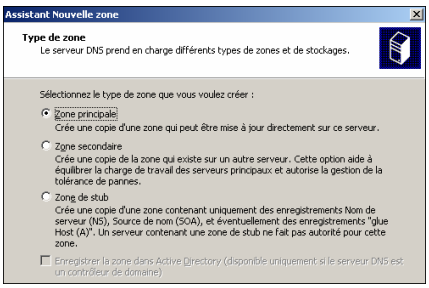


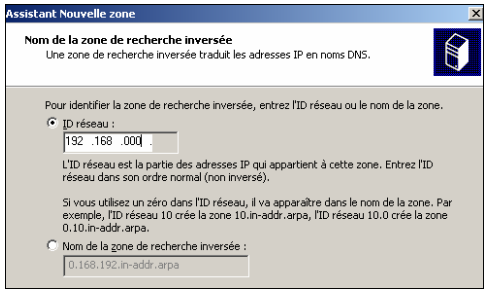
L'étape suivante permet de rentrer le nom de la zone, puis l'assistant propose automatiquement un nom de fichier DNS avec l'extension **.dns** précédé du nom de la zone.



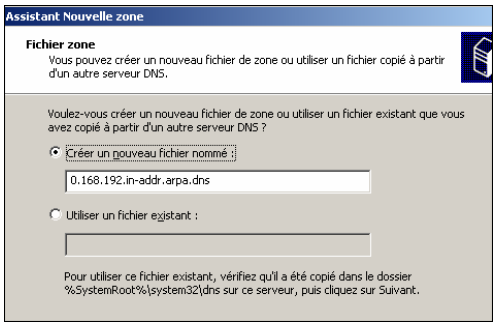


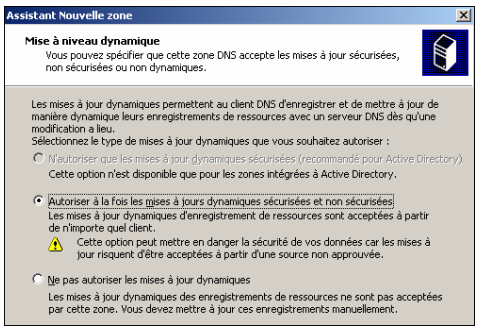
Création de zones de recherche inversée

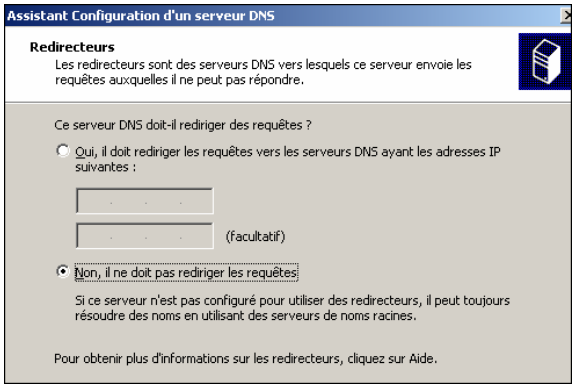


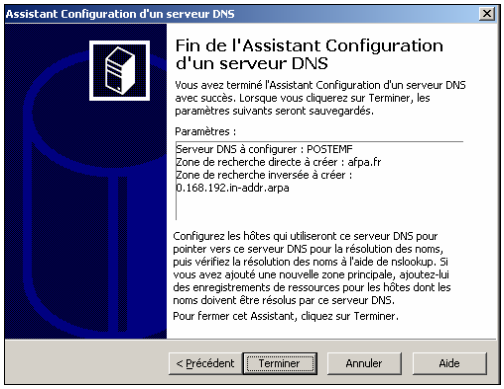


Le même processus est utilisé pour créer la zone de recherche inversée. Le nom de la zone est créé automatiquement à partir de l'adresse IP du réseau. La dernière étape est la création du fichier de zone de recherche inversée.



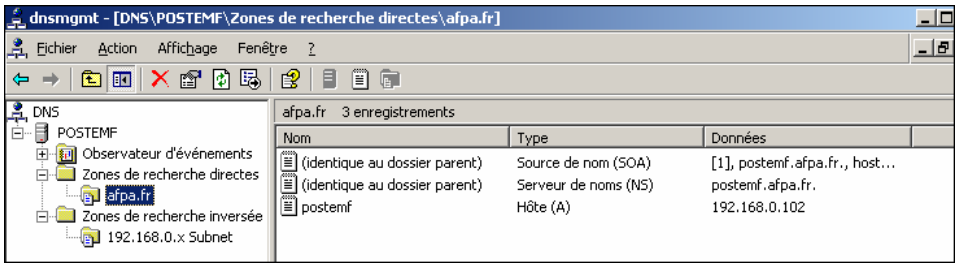






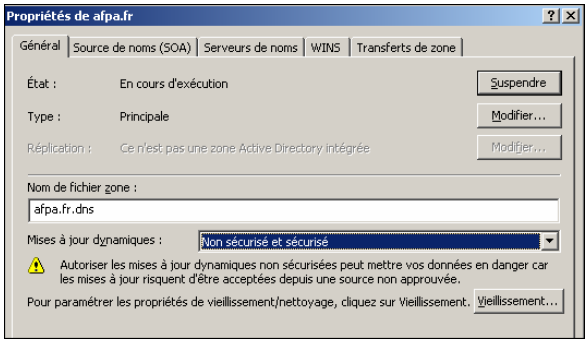
Configuration du système dynamique DDNS

DNS nécessite normalement une mise à jour manuelle des enregistrements **A** (enregistrement d'hôte) dans le fichier de zone. Avec **DDNS** (Dynamic Domain Name System) la mise à jour des noms d'hôtes peut se faire automatiquement par l'intermédiaire des contrôleurs de domaine, des serveurs WINS ou réseau.



On retrouve :

- La zone de recherche direct **afpa.fr**, avec les 3 enregistrements créés automatiquement, **SOA, NS** et **A.**
- La zone de recherche inverse **192.168.0.x Subnet.**

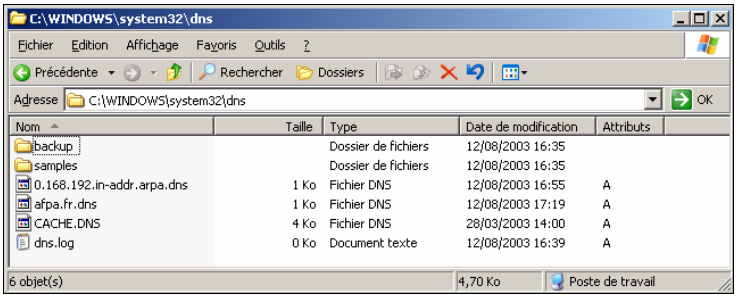


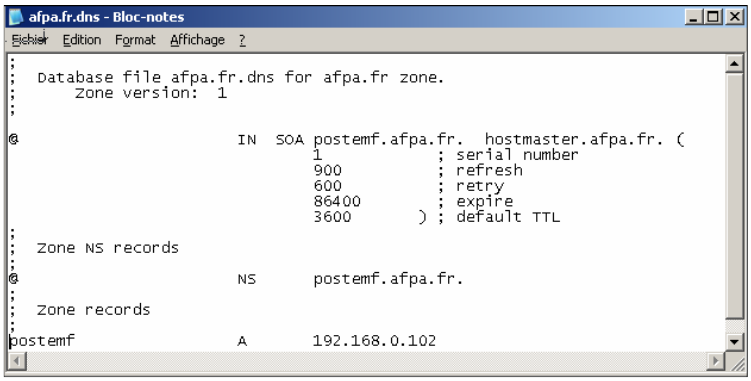
Pour activer DDNS, dans la console DNS, il suffit pour la zone considérée d'ouvrir les **Propriétés** de cette zone, puis dans l'onglet **Général** de valider **Autoriser les mises à jour dynamiques**.

- Le système DDNS fonctionne par défaut pour tous les clients Windows 2003 en utilisant le client DHCP qu'il soit validé ou non.
- Pour les autres clients Windows la mise à jour peut se faire par l'intermédiaire d'un serveur DHCP Windows 2003.
- Pour les clients UNIX, sauf pour des versions très récentes, la mise à jour du fichier de zone doit se faire manuellement.
- Onglet **général** permet à partir du bouton **Modifier** de changer le type de la zone :
  - **Principale.**
  - **Secondaire.**
  - **Stub.**
  - **Ou intégrée Active Directory.**

- Possibilité de définir le type de mise à jour à partir du champ **Mise à niveau dynamique.** Options possibles :
  - **AUCUN.**
  - **NON SECURISE et SECURISE.**
  - **SECURISE UNIQUEMENT** (si intégré Active Directory).

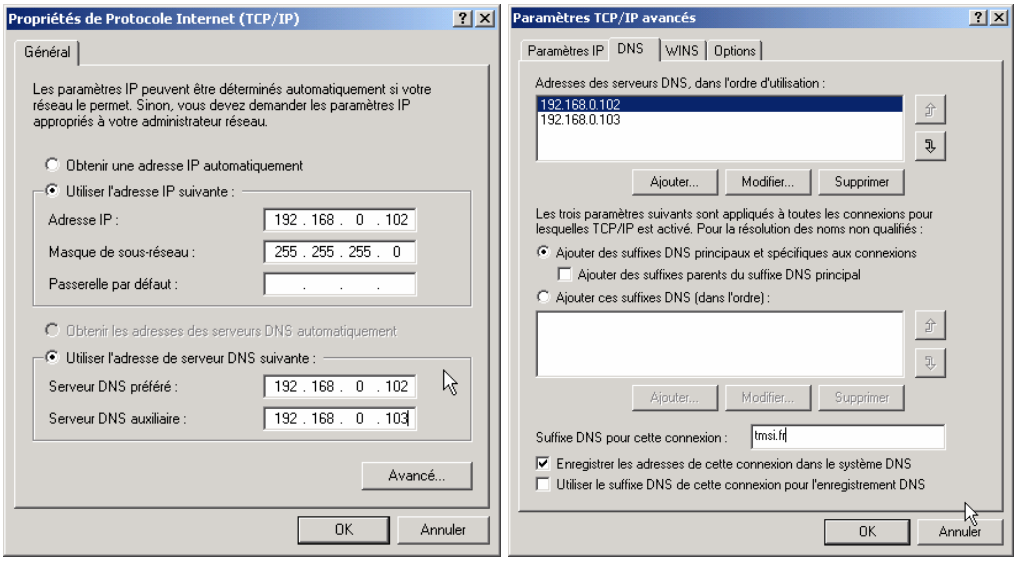
Fichier texte avec l'extension.**dns** en R/W pour le serveur DNS stocké dans le répertoire **%systemroot%\system32\dns.**



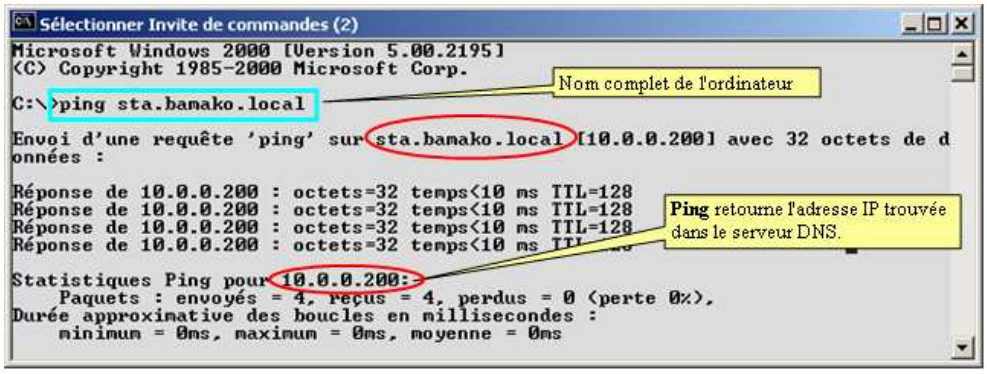


9.5.2- Configuration du client DNS

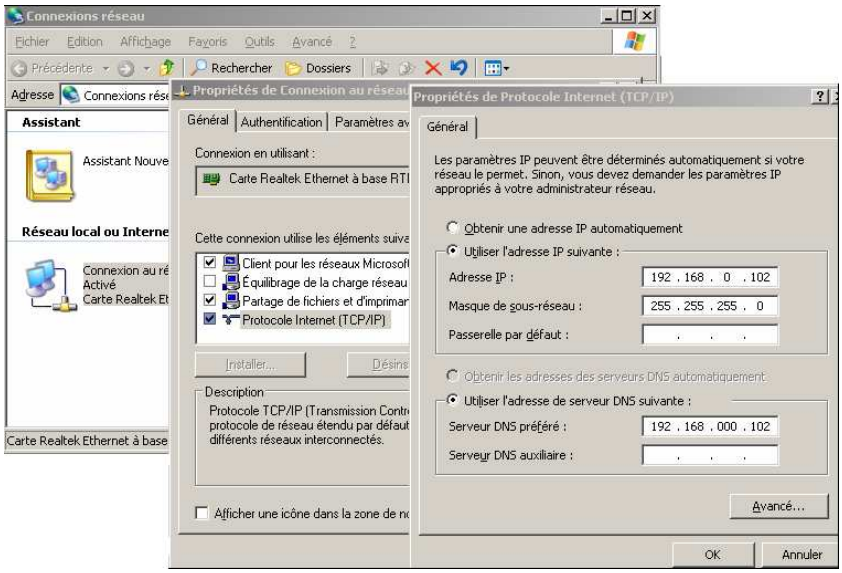
Pour qu'un ordinateur puisse utiliser la résolution de nom DNS, il faut qu'il connaisse l'adresse IP d'au moins un serveur DNS (Windows 2003 si possible). Pour indiquer cette adresse, il faut configurer les propriétés TCP/IP de ce client. Dans **Paramètres TCP/IP avancés**, onglet **DNS**, il est possible de rentrer plusieurs adresses IP de serveurs DNS et plusieurs autres paramètres concernant DNS.



Pour tester si le nom a bien été enregistré dans le fichier de zone, il suffit d'utiliser la commande **ping** suivie du nom complet de l'ordinateur.



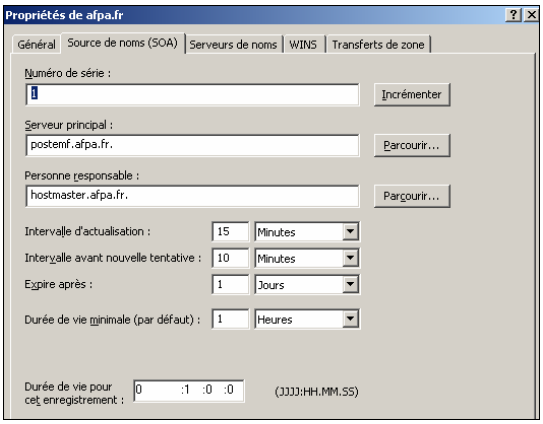
9.5.3- Mise en pratique du DNS - Référencer le serveur DNS



Cas où cohabite un serveur DNS maître/principal gérant un fichier de zone standard et un DNS gérant un fichier de zone secondaire standard. Nécessite la configuration d'un processus de transfert de zone afin que les deux serveurs mémorisent les mêmes enregistrements dans leur fichier zone.
Deux possibilités avec W2003 :

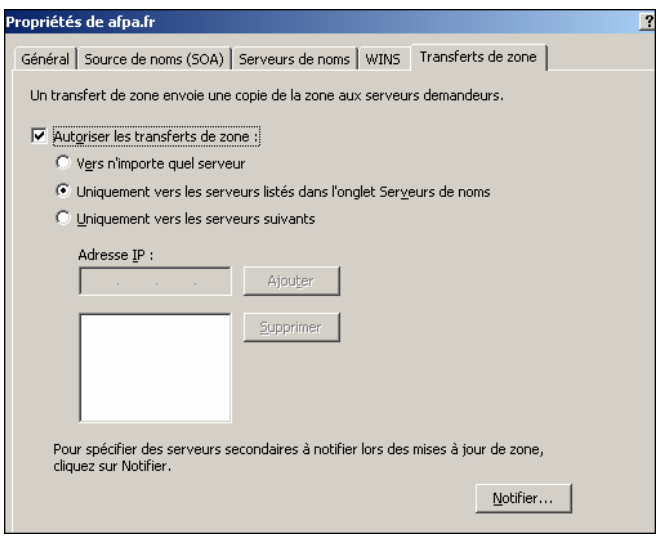
- Transfert de zone complet (intégralité du fichier zone transféré) **AXFR** (comme NT4).
- Transfert de zone incrémentiel nommé **IXFR** : ne transfert que les modifications ce qui permet un gain au niveau bande passante.

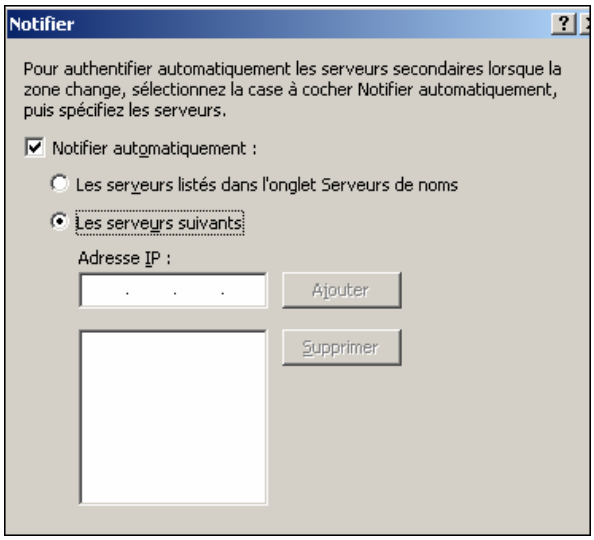
Transfert de zone AXFR



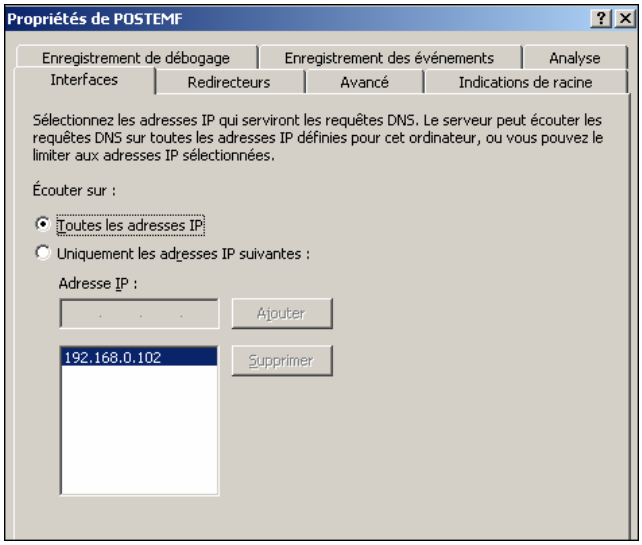
Principe :
Le serveur DNS secondaire envoie une requête auprès du serveur gérant la zone principale pour obtenir l'enregistrement SOA.
La requête du DNS secondaire en fonction de la valeur (temps) inscrite dans le champ **Intervalle d'actualisation** des **propriétés** de l'enregistrement source de noms SOA.
Ce même processus se réalise à l'initiative du DNS principal ou au démarrage du service serveur DNS sur un serveur DNS secondaire.
Dans ce cas il y a comparaison des numéros de série.
Si n° série identiques ➔ aucun transfert.
Si n° série du DNS principal > celui du secondaire ➔ transfert.

Transfert de zone IXFR
Transfert uniquement les informations modifiées. C'est un transfert de zone incrémentiel.
Principe :
LE serveur DNS secondaire reçoit l'enregistrement SOA du serveur principal, il le compare avec le sien. Si différent, le serveur principal effectue la différence entre le fichier de zone possédant le dernier n° SOA et celui du secondaire.
Le serveur principal transfère uniquement les modifications réalisées.
Ces informations remplacent les anciennes informations sur le DNS secondaire.





9.5.4- Configuration du serveur



Ecran avec 7 onglets :

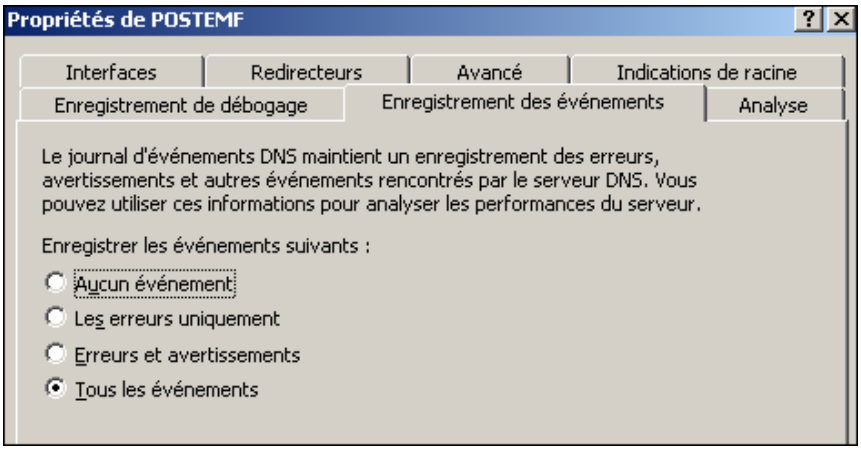
- **Interfaces** : indique l'@IP de l'interface sur laquelle le serveur DNS écoute les requêtes.
- **Avancé.**
- **Indications de racines** : indique le(s) serveur(s) raine(s).
- **Enregistrement de déboguage** (maintenance).
- **Enregistrement des événements :** indique le type d'événements à consigner dans le journal DNS.
- **Analyse** : vérifie si serveur Ok.
- **Redirecteurs** : redirige demandes non résolues vers d'autres serveurs DNS.

9.5.5- Outils de gestion, test et dépannage

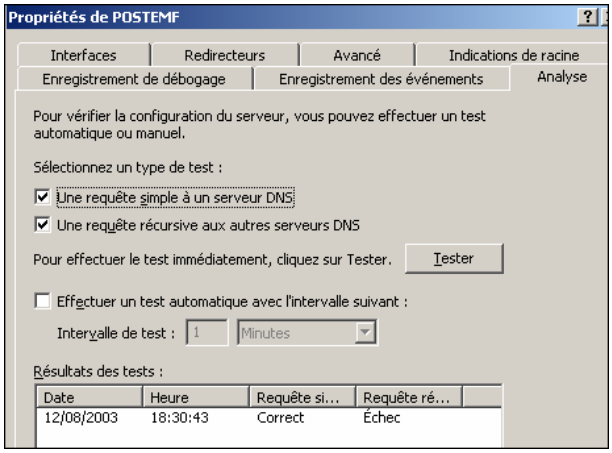
Outils disponibles :

- Console **DNS.**
- Utilitaire **NSLOOKUP.**
- Utilitaires **TCP/IP.**
- Journaux d'événements.
- Fichiers de **log.**

Observateurs d'événements

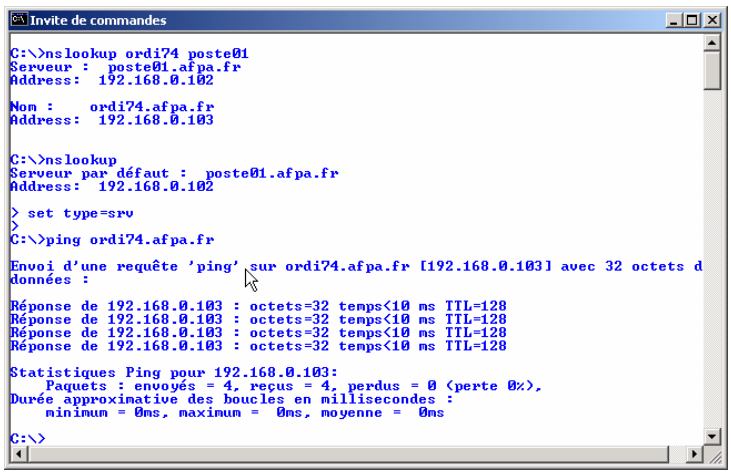


Console DNS



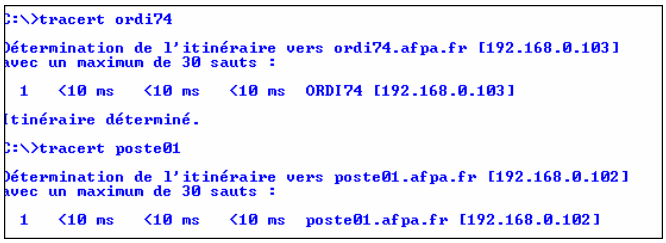
Utilitaire NSLOOKUP

Mode interactif ou non. **nslookup –option ordinateur_a_chercher serveur_dns_a_utiliser**.

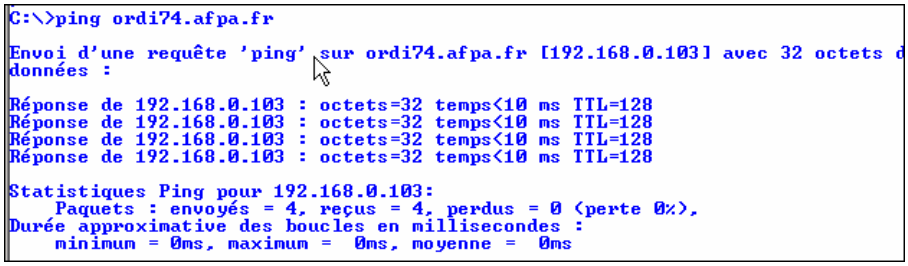


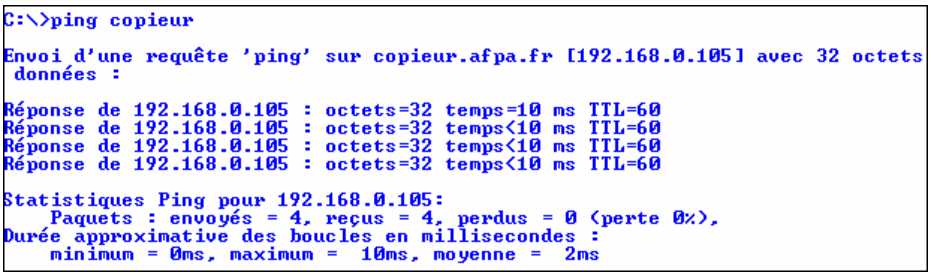
Pour voir toutes les options utilisables en mode interactif, tapez la commande **Help.**

Utilitaires TCP/IP



Tracert



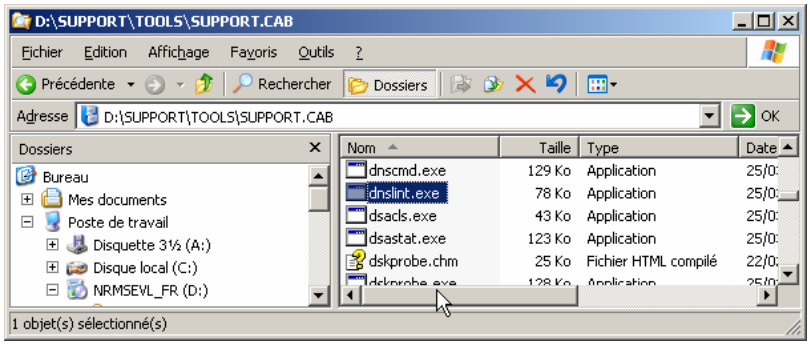


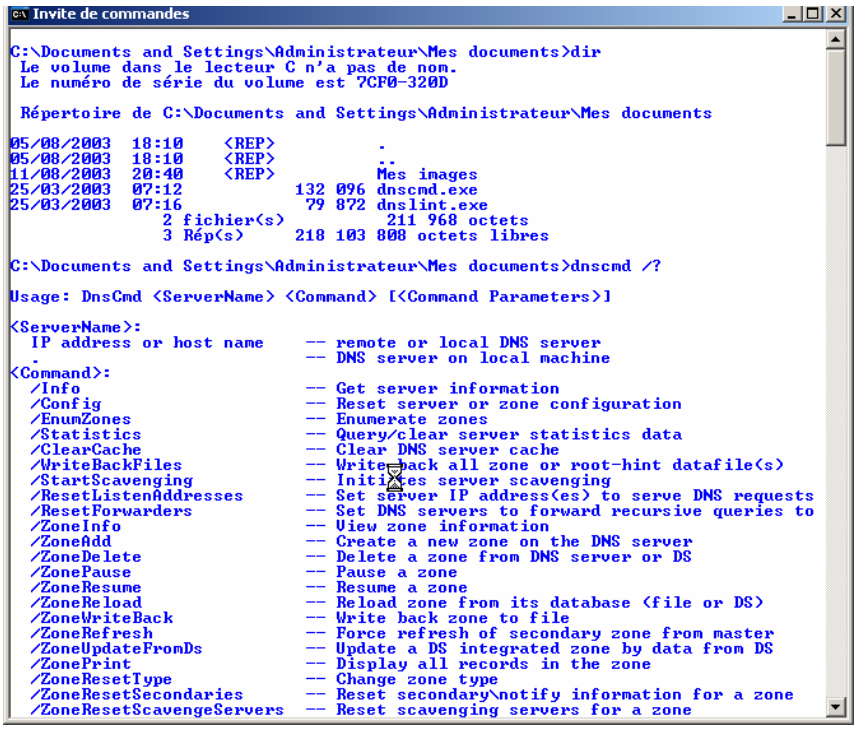
Outil de gestion en ligne de commande - DNSCmd

Fournit avec les **Support Tools** :

- Afficher ses paramètres en tapant DNSCmd /?.
- Permet de modifier la configuration d'un serveur DNS.
- Vider le cache DNS, créer, supprimer des enregistrements...
- Permet d'afficher les informations d'un serveur DNS.
- Statistiques, enregistrements de ressources de zones.
- …

DNSLint est aussi un autre outil de **Support Tools**.





9.6- Sécurisation du trafic réseau : IPSEC

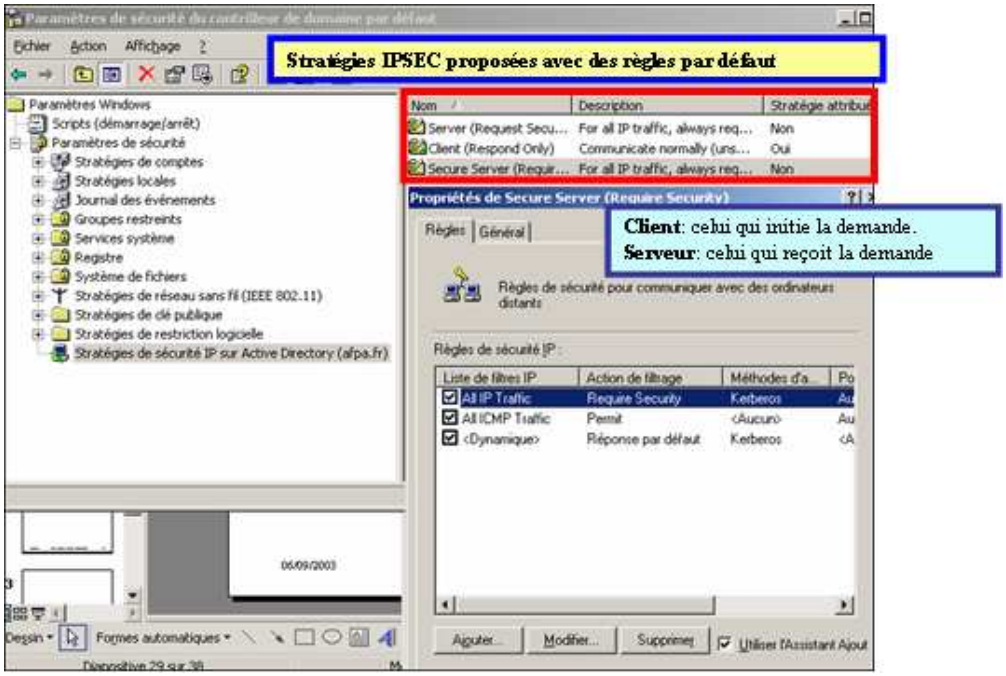
Il peut être nécessaire de crypter les trames circulant sur le réseau afin d'éviter que des outils d'analyse de réseau ne puisse les lire. Windows Server 2003 dispose du protocole **IPSEC** (IP Security). Il est très simple d'activer IPSEC sur le réseau via les stratégies de groupe.
Les fonctionnalités mises en œuvre par **IPSec** sont :

- **L'Authentification** mutuelle des ordinateurs via **Kerberos**, des certificats ou clés pré partagées.
- Le cryptage des trames réseaux afin qu'elles ne puissent être modifiées ou lues et IPSEC interdit certains types d'attaques.
- **IPSEC** est transparent pour les utilisateurs du réseau.
- La possibilité de ne crypter que certaines trames, filtrer les trames...

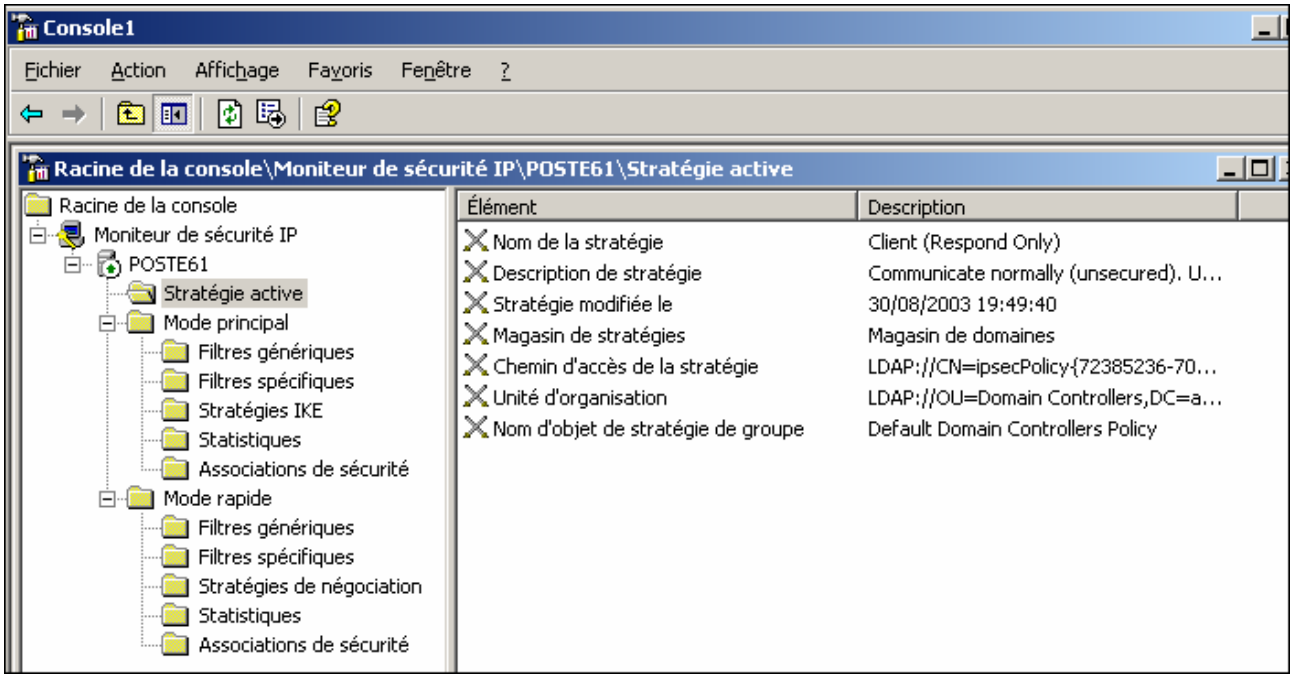
Initialement si deux micros communiquent en IPSec, ils vont établir une négociation afin de s'authentifier et ils vont négocier la mise en œuvre de la sécurité. Ils définissent un algorithme et la clé de cryptage qu'ils vont utiliser pour communiquer. Cette phase de négociation peut être capturée avec un analyseur réseau et porte le nom de protocole ISAKMP. Une fois que cette négociation est opérationnelle, la communication se réalise avec le protocole ESP par défaut. W2003 Server propose des règles déjà paramétrées dans les stratégies de groupe que vous pouvez utiliser. Ces règles de stratégies IP peuvent se retrouver au niveau d'Active Directory (client/serveur) ou sur un poste local (groupe de travail). Dans la console **Editeur d'objets de Stratégie groupe** et dans la rubrique **Stratégies de sécurité IP sur Active Directory** par exemple, vous avez 3 stratégies IPSec proposées par défaut. Vous pouvez créer vos propres règles.

Ces règles dans l'exemple ci-dessous sont :

- **Server** (Request Security) : dans ce cas le serveur tente de négocier une communication en IPsec mais si cela est impossible il va quand même communiquer avec le client en clair.
- **Client** (Respond only) : le client fait une demande classique et si le serveur veut communiquer en IPSec il va négocier la communication.
- **Secure Server** (Require Security) : dans ce cas le serveur n'accepte que les communications IPSec, et si ce n'est pas réalisable il n'y aura pas de communication.



Si vous souhaitez activer une stratégie IPsec, vous devez cliquer droit sur la stratégie que vous désirez puis valider **Attribuer**. Vous pouvez utiliser la **Console Moniteur de Sécurité IP** et en cliquant sur **Stratégie active** vous obtenez des informations sur la stratégie IPSec en cours.

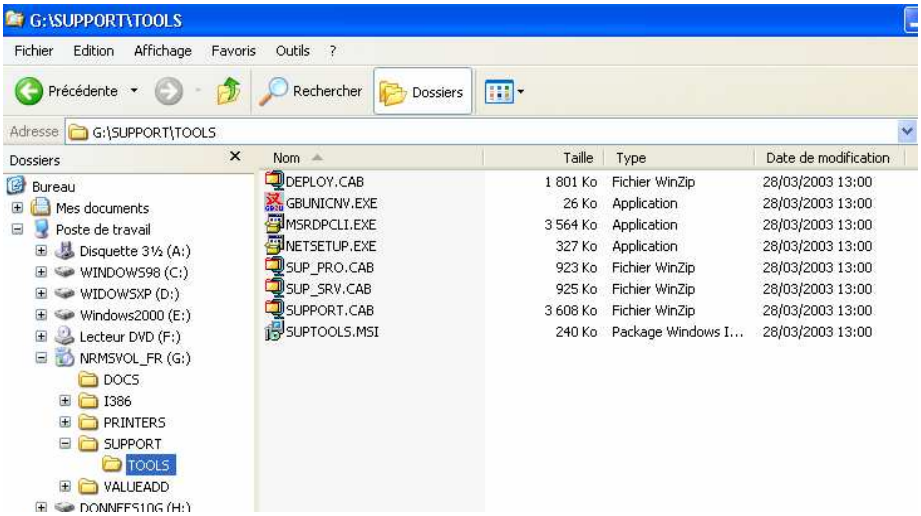


X- SUIVI ET OPTIMISATION DES PERFORMANCES

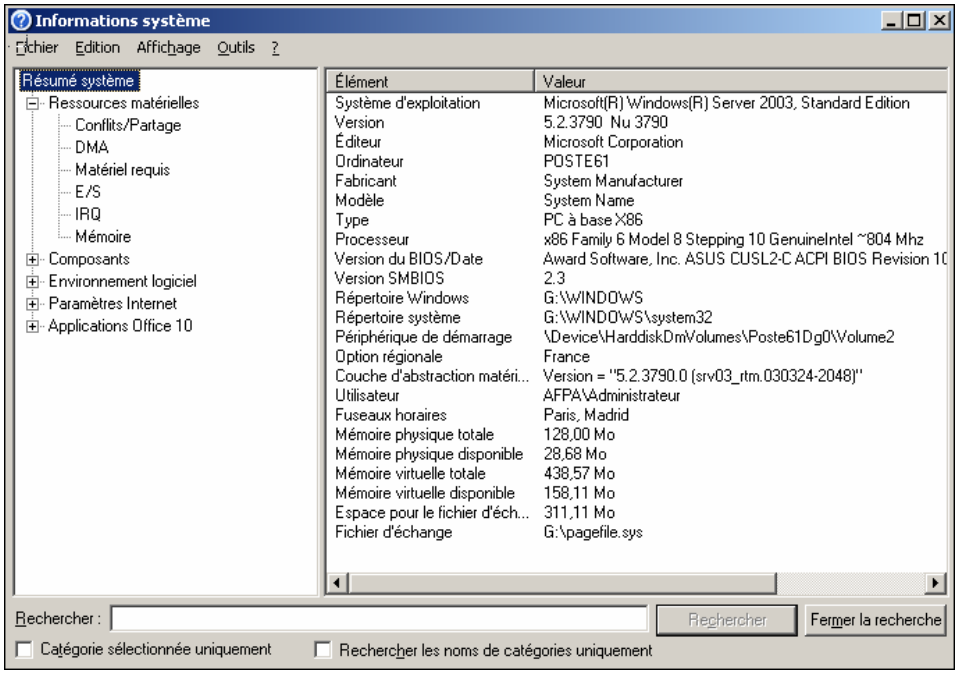
Vous allez découvrir les outils disponibles pour tester, surveiller et optimiser le bon fonctionnement de votre serveur W2003.

10.1- Outils complémentaires du CD-ROM

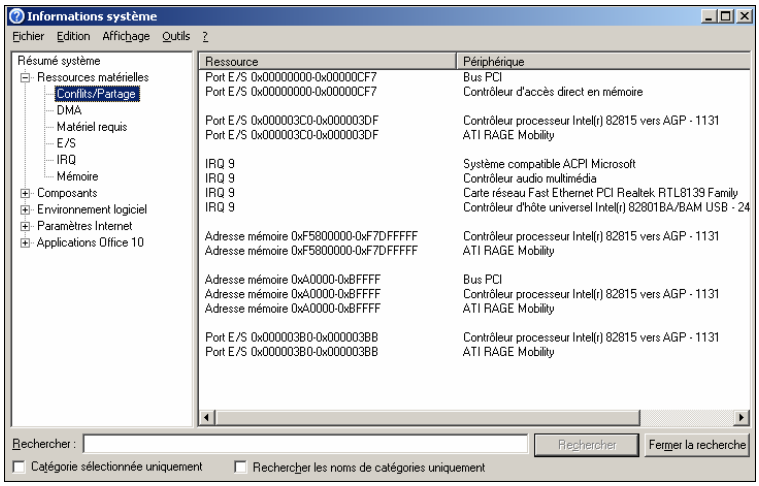
En plus des outils classiques disponibles à partir de l'interface graphique de W2003 ou en mode commande, vous pouvez utiliser le centre d'aide et de support à partir de votre menu **Démarrer** ou bien les outils supports localisés sur le CD dans le répertoire **\support\tools**.



Informations système - Résumé
Outil très complet et fréquemment utiliser pour tester et obtenir une vision globale de tous les éléments matériels et logiciels de votre machine.
Pour lancer le programme, cliquez sur **Démarrer ➔ Tous les programmes ➔ Accessoires ➔ Outils systèmes ➔ Informations Système**.

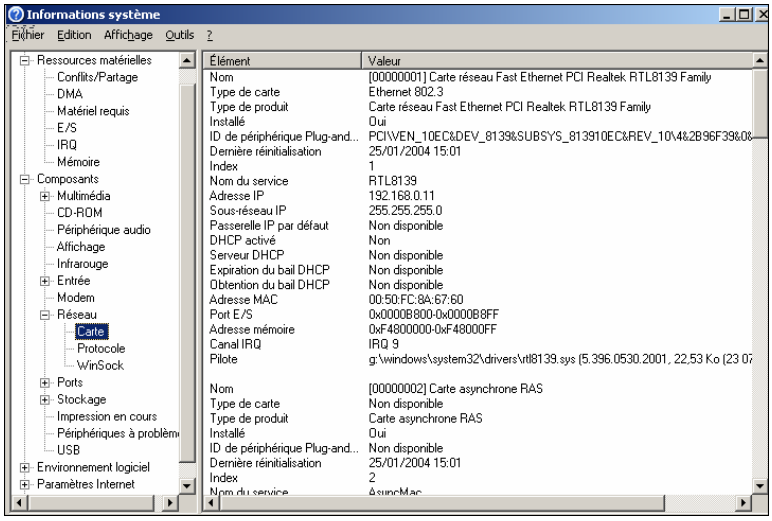


Informations Système – Exemple des Ressources Matérielles

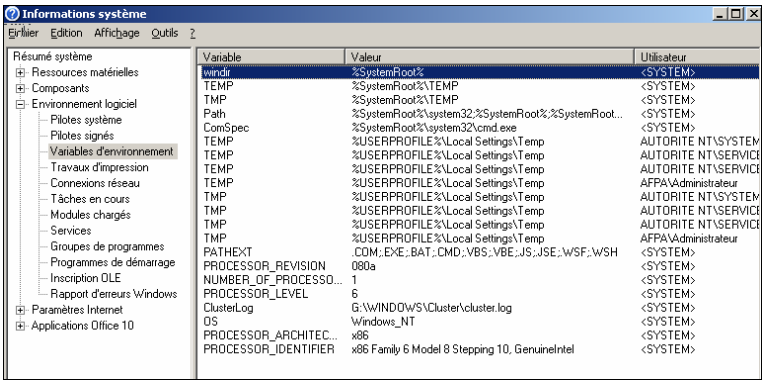


Cet écran vous donne de nombreuses informations sur les éléments matériel de votre machine (Conflits/partage, IRQ, mémoire, I/O…).

Informations Système Composants – Exemples des cartes réseau
Affiche et donne des informations sur les périphériques triés par catégorie comme le fabricant, la version des pilotes, les ressources matérielles.

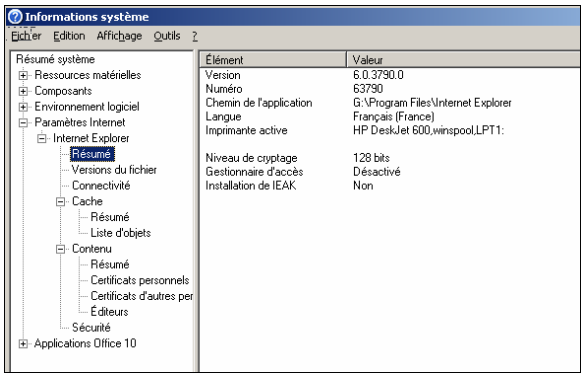


Informations Système - Environnement Logiciel, exemple des variables d'environnement



Cet écran vous permet de visualiser les éléments logiciels comme les applications installées, les services et aussi les variables d'environnement.

Informations Système – Internet Explorer



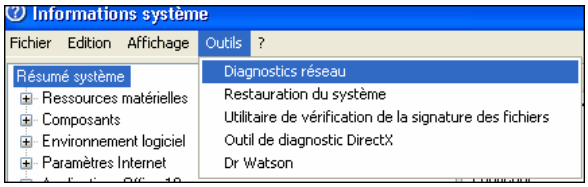
Cet écran vous donne le maximum d'information sur Internet Explorer, la gestion des caches, les paramètres Proxy...

Tous les paramètres que vous venez de consulter peuvent être imprimés ou stockées dans un fichier texte.

Outils complémentaires d'informations système

Le menu **Outils** de la fenêtre **Informations système** vous donne directement accès à quatre outils supplémentaires :

- **Diagnostic réseau.**
- **Utilitaire de vérification de la signature des fichiers.**
- **Outil de diagnostic Direct X.**
- **Dr Watson.**

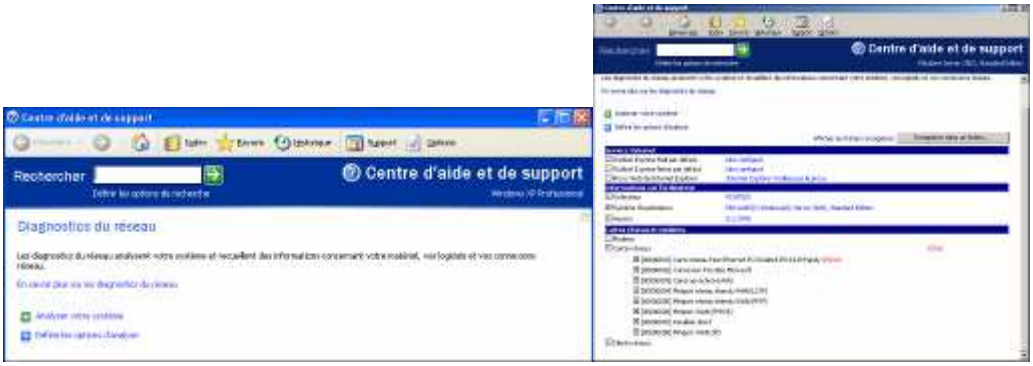


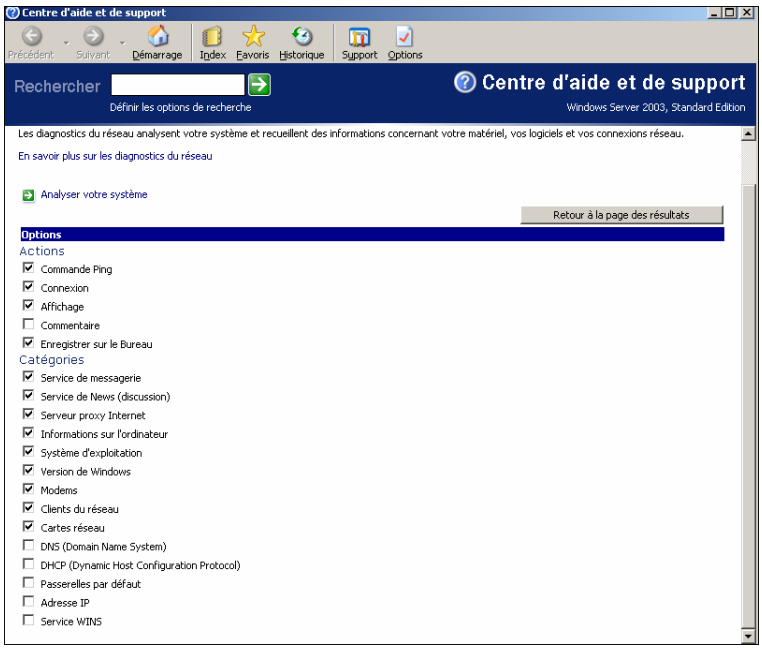
10.2- Diagnostic Réseau

W2003 met à votre disposition un outil performant de diagnostic du réseau. Pendant le test une barre de progression s'affiche. Lorsque les tests sont terminés les résultats sont affichés à l'écran.
Cet utilitaire vous permet de résoudre les problèmes de :

- **Connectivité réseau.**
- **Service Internet (messagerie, groupe de discussion et proxy).**
- **Modems, clients réseau et cartes réseau.**
- **Configuration DNS, DHCP et WINS.**
- **Passerelles et adresses IP par défaut**.

Vous pouvez définir les options d'analyse pour réaliser des tests plus approfondis.

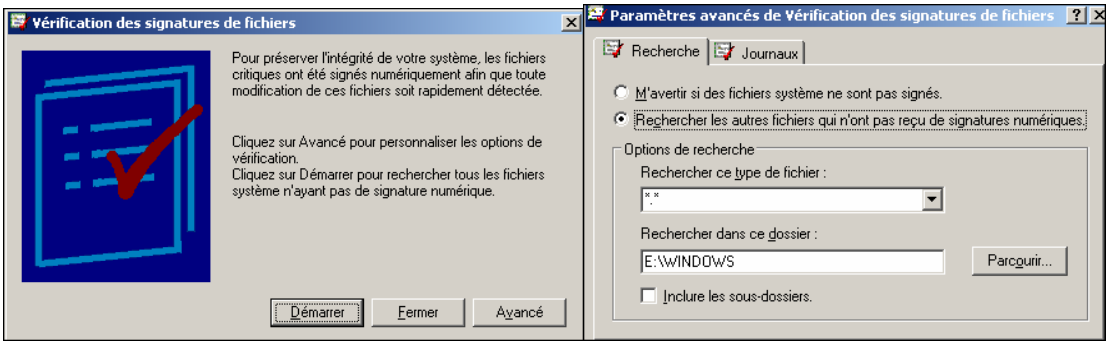


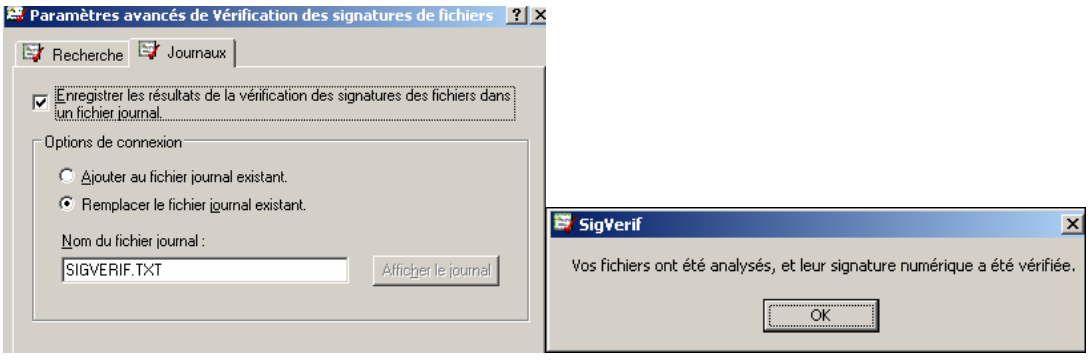


Utilitaire de vérification de la signature des fichiers

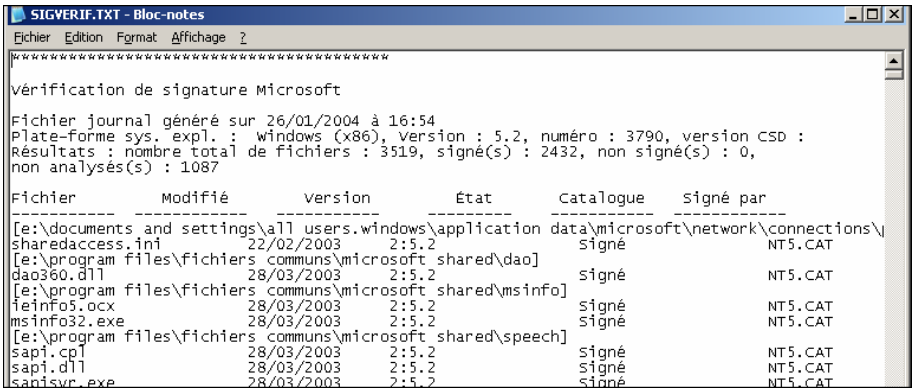
Les fichiers des pilotes de périphériques et du système d'exploitation fournis avec Windows ont une signature numérique donnée par Microsoft. Elle indique qu'un pilote ou fichier précis a atteint un certain niveau de test, et qu'il n'a pas été endommagé ou remplacé un autre programme. Les pilotes de périphériques destinés aux produits matériels présentant les logos **Conçu pour Microsoft Windows XP** ou **Conçu pour Microsoft Windows Server 2003** possèdent une signature numérique de Microsoft, qui indique que la compatibilité du produit a été testée avec Windows et n'a pas été modifiée depuis le test.

En fonction de la façon dont l'administrateur a configuré l'ordinateur, Windows ignore les pilotes de périphérique qui n'ont pas été signés numériquement, affiche un message d'avertissement lorsqu'il détecte des pilotes de périphérique non signés numériquement (comportement par défaut), ou vous empêche d'installer des pilotes de périphérique ne disposant pas d'une signature numérique.



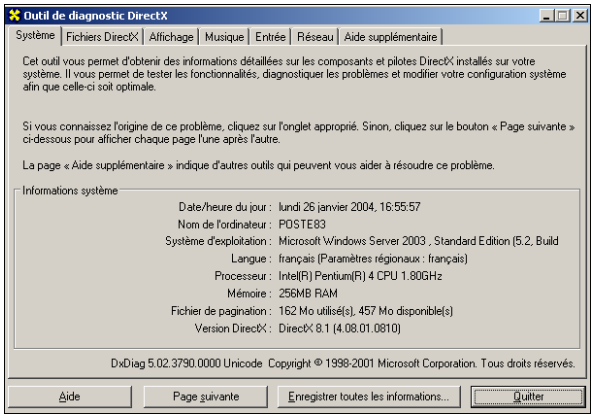


Possibilité de lire le contenu du fichier résultat **SIGVERIF.TXT.**



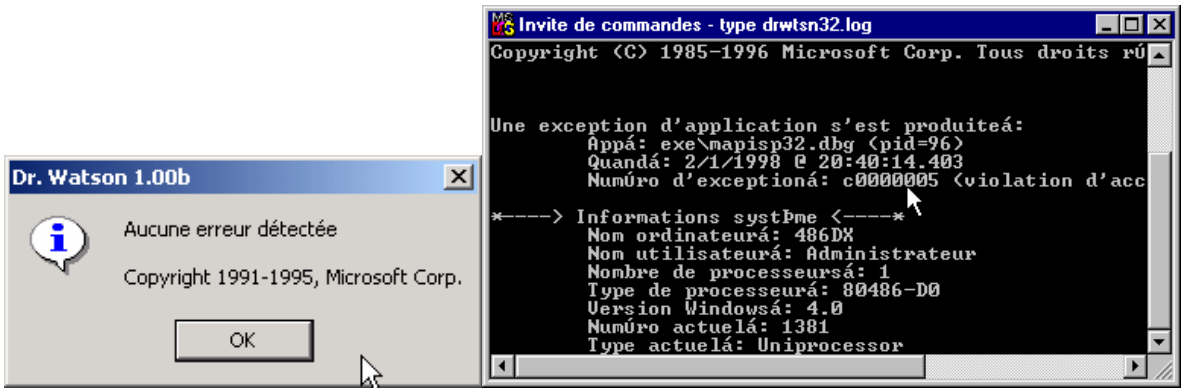
Outil de diagnostic DirectX

Cet outil vous permet de diagnostiquer et résoudre les problèmes liés à **DirectX**, aux jeux et applications multimédias. **L'Outil de diagnostic DirectX** vous aide à tester la fonctionnalité de DirectX, à diagnostiquer les problèmes et à ajuster le niveau de support matériel utilisé par DirectX, qui peut être utilisé pour éviter des problèmes sur certains lecteurs multimédias.

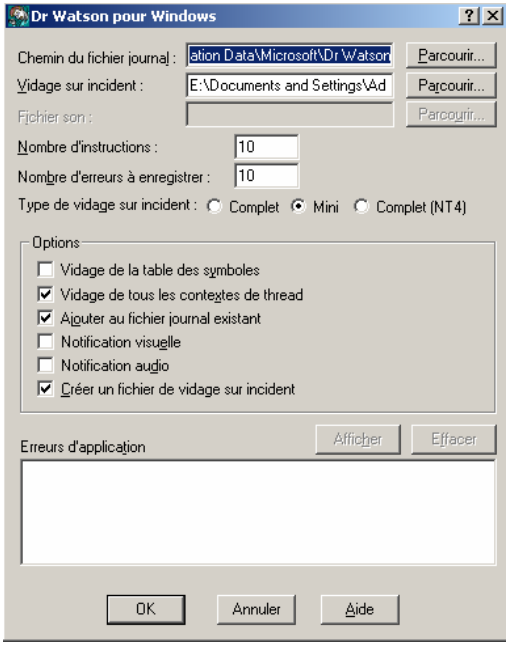


Utilitaire Dr Watson

Dr Watson est un outil très intéressant pour l'utilisateur de W2003, car aussitôt qu'une erreur se produit, il démarre automatiquement et vous voyez apparaître une fenêtre en premier plan de votre écran. Dr Watson est un outil de maintenance qui vous renseigne lors du plantage d'une application et qui mémorise les informations lors de l'arrêt d'une application dans un fichier historique, **drwtsn32.log.** Le contenu est visualisable par l'utilisateur, soit par la commande type ou à partir du **Journal d'erreurs**.



Il est possible d'activer la création d'un **fichier de vidage** sur incident. C'est un fichier binaire destiné au déboguage d'incident (user.dmp).

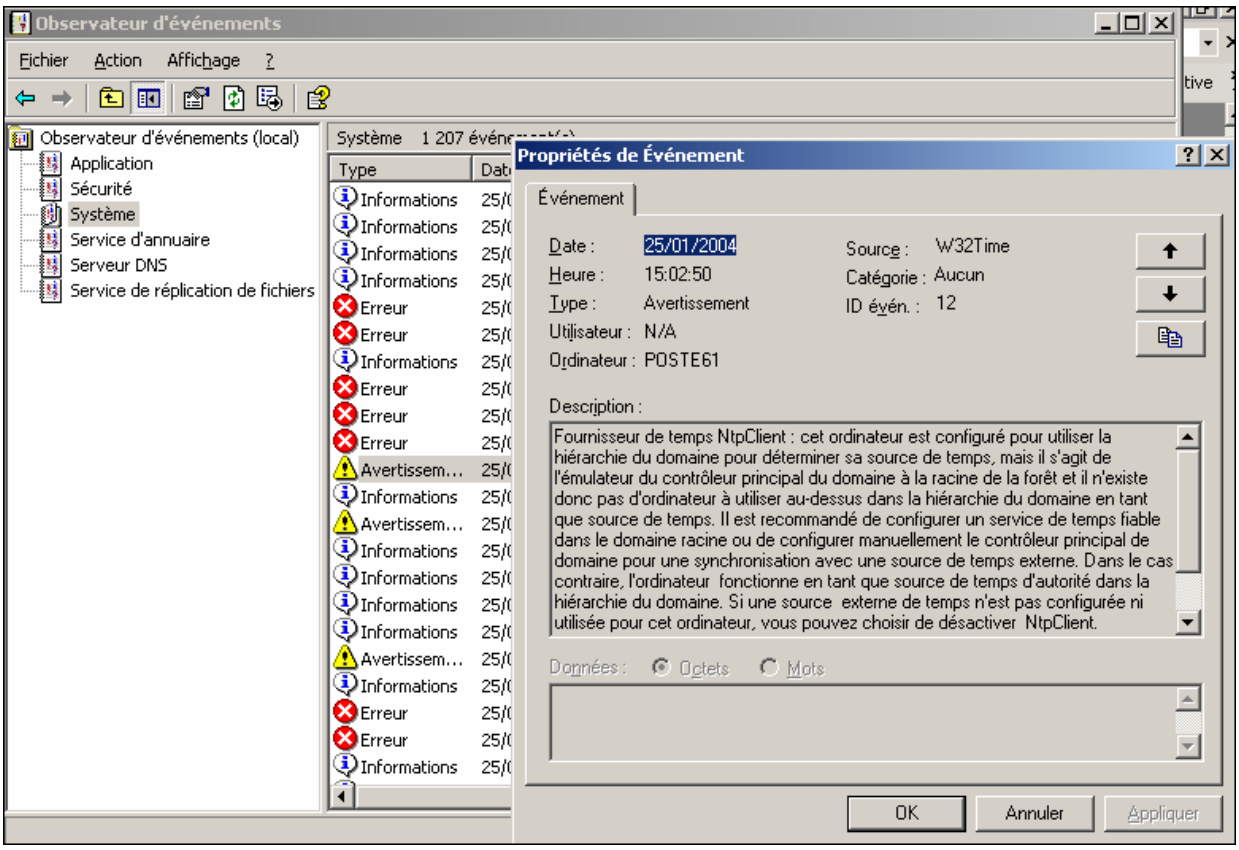


10.3- Gestion et optimisation de W2003

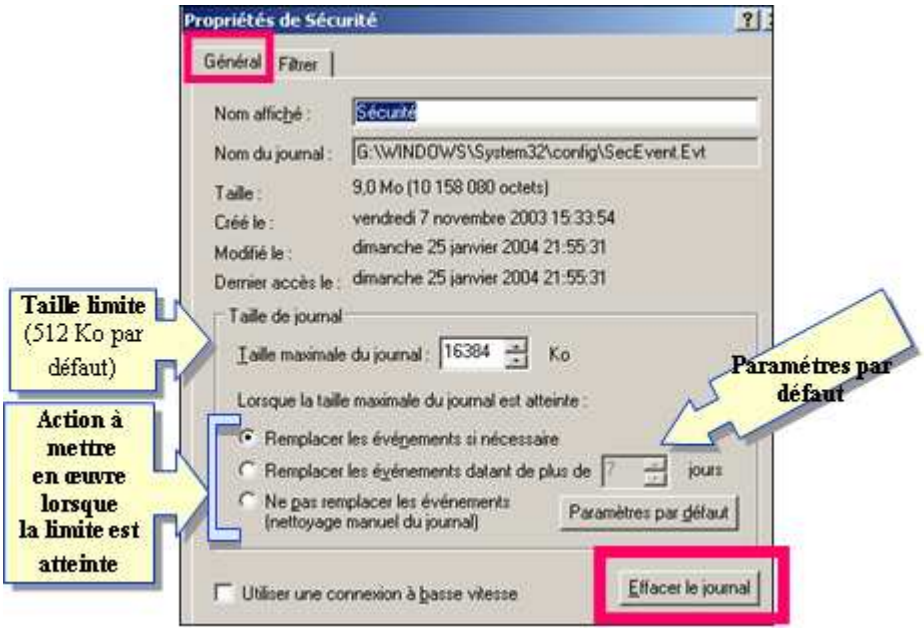
10.3.1- Observateurs d'événements

Le **Journal système** contient des événements consignés par les composants système de Windows 2003. Le **Journal applications** contient des événements consignés par les applications ou les programmes. **Le Journal sécurité** contient des événements de sécurité liés aux tentatives d'ouverture de session et à l'utilisation des ressources.

Journal des événement	Description	Processus de sélection des événements
Système	Erreurs, avertissements ou informations générées par le système.	La sélection des événements est prédéfinie par le système d'exploitation.
Sécurité	Tentatives d'ouverture de session valides ou non valides, et événements relatifs à l'utilisation des ressources telles que la création, l'ouverture ou la suppression de fichiers.	Le contrôle de l'audit des événements de sécurité est défini dans le menu Stratégie du gestionnaire des utilisateurs.
Application	Erreurs, avertissements ou informations générées par les logiciels d'applications.	Les événements à contrôler sont choisis par les développeurs de l'application.



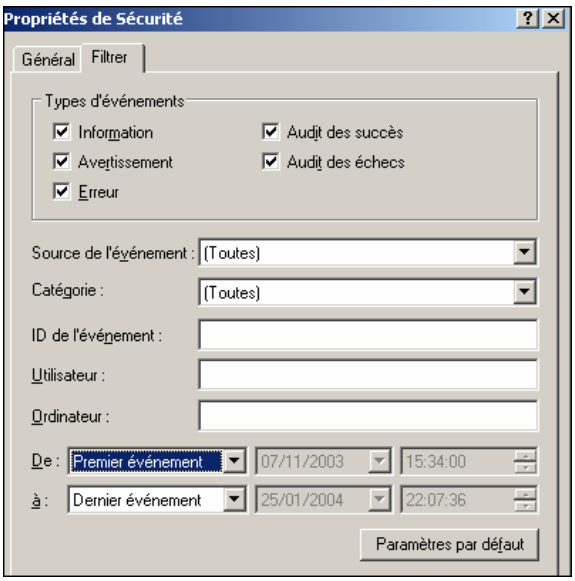
Vous pouvez paramétrer le journal de sécurité à partir de l'onglet **Général.**



Par défaut la taille du journal est de **512** Ko, mais vous pouvez la modifier. Vous pouvez aussi paramétrer les actions à réaliser lorsque le journal est plein.

✋ Toutes ces valeurs peuvent être positionnées par les stratégies de groupes.

En plus des 3 journaux de base **d'autres journaux peuvent être présents**, surtout si vous êtes en Active Directory (service d'annuaire, DNS, service de réplication des fichiers…). Vous pouvez aussi réaliser une fonction de **Filtrage** si vous avez de nombreux enregistrements pour faciliter les recherches. Si vous avez réalisé une stratégie d'audit pensez à **consulter** fréquemment le **journal de Sécurité**.



10.3.2- Gestion des journaux d'événements

Archivez les journaux d'événements pour :

- Dégager des tendances afin de déterminer l'utilisation des ressources.
- Effectuer le suivi de l'utilisation non autorisée des ressources.
- Conserver des enregistrements lorsque la loi le réclame.
- Choisissez un format de fichier pour afficher les journaux archivés dans d'autres applications.
- Format de fichier journal (.evt).
- Format de fichier texte (.txt).
- Format de fichier texte délimité par des virgules (.csv).
- Effacez les journaux d'événements lorsque vous décidez de ne pas les remplacer.

Analyseur de performances

C'est un outil graphique qui permet d'évaluer les performances d'un ordinateur fonctionnant sous W2003 Server. Il permet de visualiser sous forme graphique ou texte (rapports) le comportement d'objets tels que :

- Le processeur.
- La mémoire cache.
- Les processus et les threads.
- Le disque dur.
- L'activité du réseau...

Les administrateurs utilisent cet outil pour plusieurs raisons :

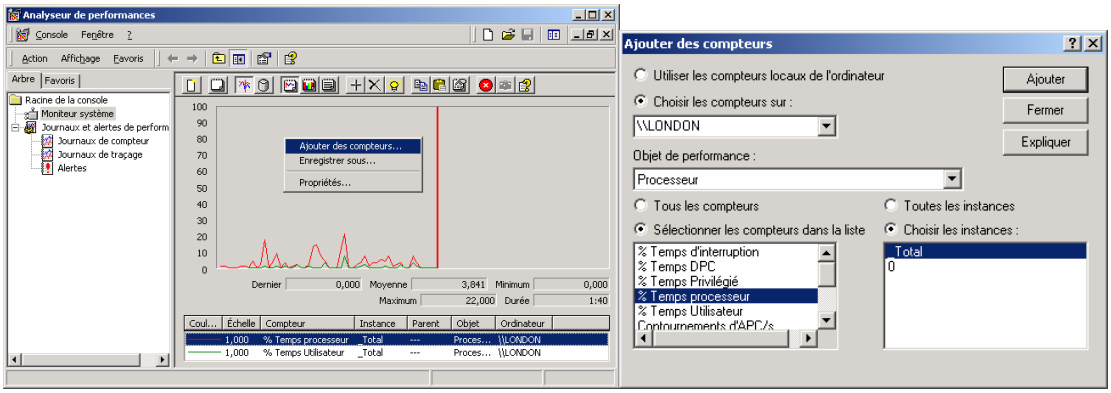
- Améliorer les performances en fonction de la configuration existante (détection des goulots d'étranglement).
- Faciliter la planification des capacités.
- Maintenir des ressources matérielles adaptées.
- Fournir des informations pour la détection des problèmes matériels.
- Vérifier que les modifications apportées au système ont bien amélioré les performances.

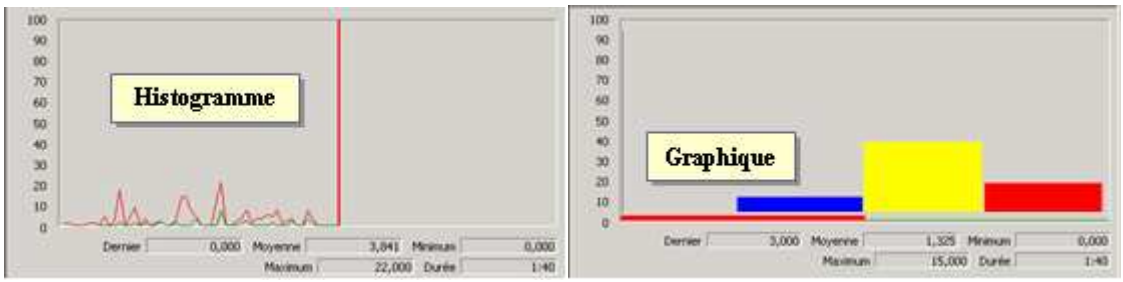
L'administrateur peut s'apercevoir que :

- Le volume de travail sur un serveur est beaucoup plus important que sur un autre et ainsi répartir différemment les applications d'un serveur à l'autre,
- Le serveur pagine excessivement parce qu'il ne dispose pas d'une quantité de mémoire suffisante.
- Un disque d'un serveur est entièrement saturé.

10.3.4- Ajout de compteurs

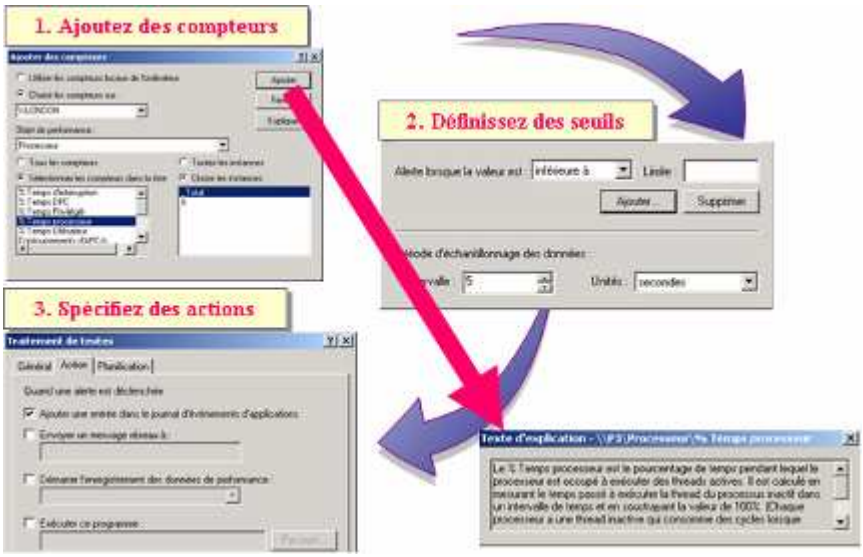
Ajoutez des compteurs pour afficher des données dans le graphique. L'utilisation de **graphes** est intéressante dans le cas d'une surveillance de courte durée.





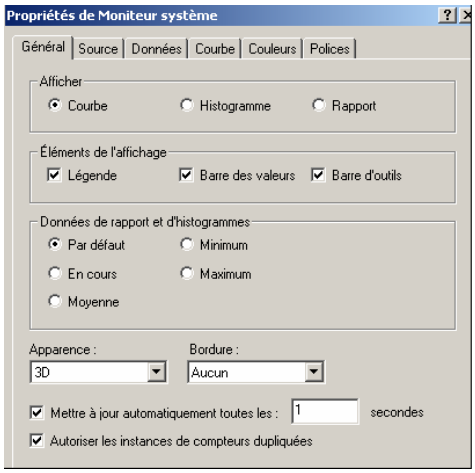
10.3.5- Utilisation d'alertes

Vous pouvez définir des **alertes** pour vous avertir de l'arrivée de certains événements ou bien de l'atteinte de certains seuils de performances. Ces alertes peuvent être transmises sous forme de message réseau ou bien lorsque ces messages entrent dans le journal des événements applicatifs.



10.3.6- Moniteur système

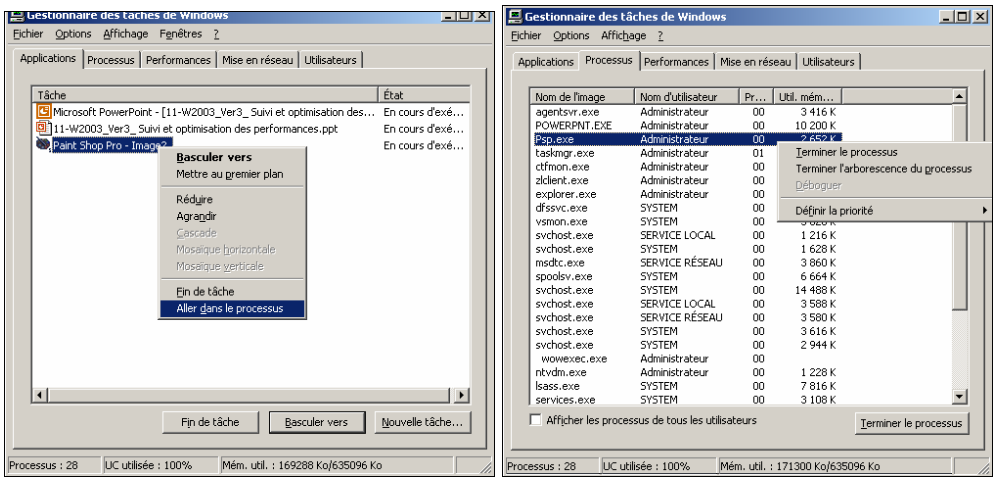
Vous pouvez à partir de la fenêtre ci-dessous paramétrer le **Moniteur Système.**



10.3.7- Gestionnaire des Tâches

Pour gérer les processus et les applications du système, l'outil principal est le gestionnaire des tâches. Pour le lancer vous pouvez :

- Appuyer sur les touches **CTRL + MAJ + ECHAP.**
- Appuyer sur les touches **CTRL + ALT + SUPPR,** puis cliquer sur le bouton **Gestionnaire des tâches**.
- Taper taskmgr à partir de l'utilitaire **Exécuter** ou à **l'invite de commande**.
- Cliquer sur le bouton droit de la barre des tâches puis sélectionner **Gestionnaire des tâches** dans le menu contextuel.

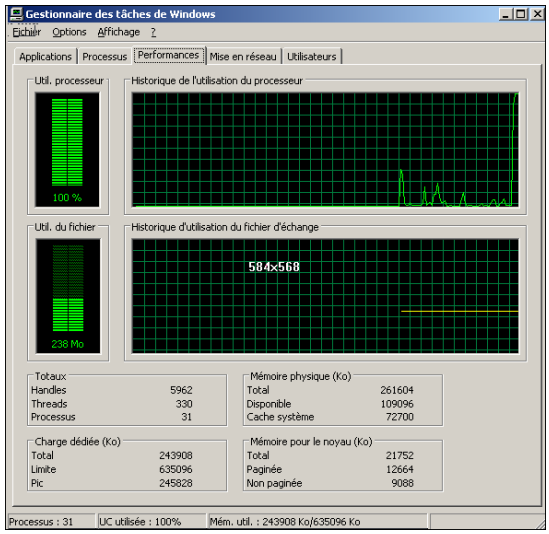


Pour terminer un processus, il suffit de faire un clic droit dessus puis valider **Terminer le Processus**. Cela aura pour effet de supprimer tous les processus qui sont liés. Chaque processus possède un niveau de priorité d'exécution. Ils sont au nombre de 6 :

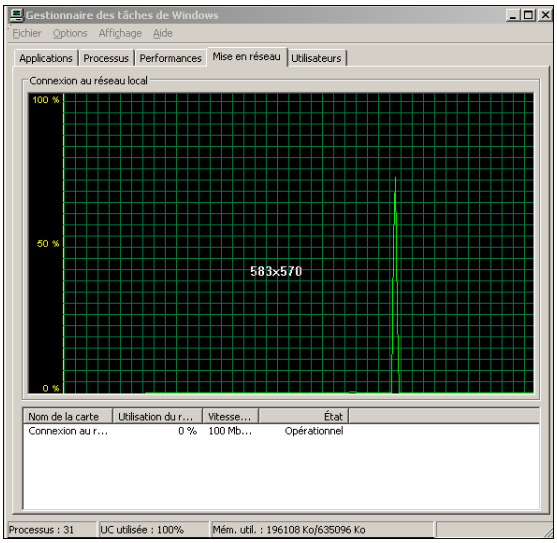
- Temps réel.
- Haute.
- Supérieure à la normale.
- Normale.
- Inférieure à la normale.
- Basse.

Par défaut toute application que vous lancez aura la priorité à normale, par contre vous pouvez manuellement définit les priorités que vous désirez.

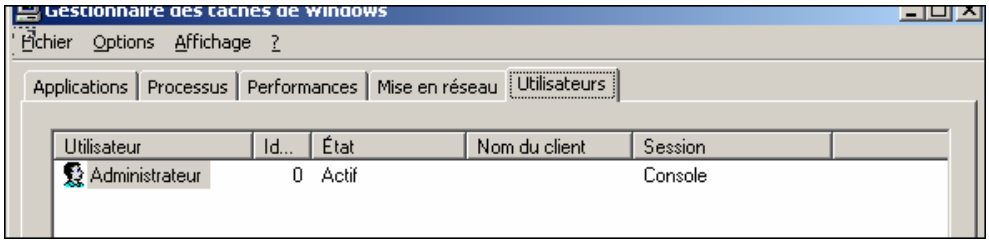
→ Onglet Performances du Gestionnaire des Tâches
Cette fenêtre vous donne une multitude de renseignements intéressants sur l'utilisation du processeur, l'utilisation de la mémoire...



→ Onglet Mise en Réseau du Gestionnaire des Tâches
Permet l'affichage d'un graphe sur l'activité du réseau et visualiser à tout instant sa bande passante.



→ Onglet Utilisateurs du Gestionnaire des Tâches
Permet de visualiser les utilisateurs connectés.

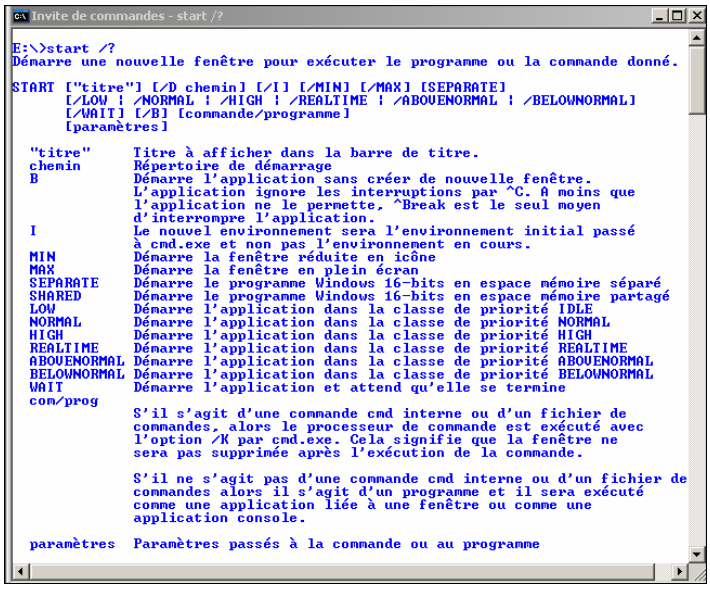


10.4- Gérer les processus par ligne de commande

W2003 Server possède 4 commandes pour vous aider à gérer les processus. Vous pouvez soit générer ou détruire des processus ou des tâches actives.

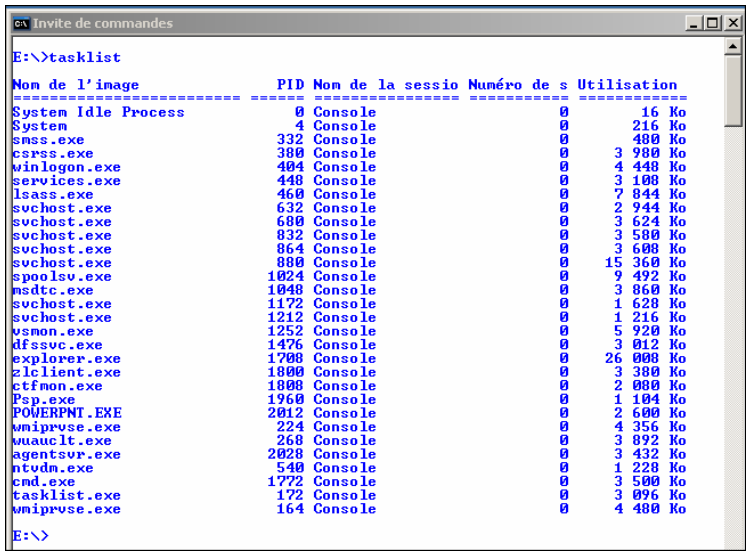
10.4.1- Commande START

Pour lancer une application (et les processus liés) avec le niveau de priorité de votre choix vous pouvez utiliser la commande **START /niveau_de_priorité Commande ou Programme**.



10.4.2- Commande TASKLIST

Affichage de la liste des processus en cours.



TASKLIST [/S système [/U utilisateur [/P mot_de_passe]]]] [/M [module] | /SVC | /V] [/FI filtre] [/FO format] [/NH]

Description : cet outil affiche une liste des processus actuellement en cours sur un ordinateur local ou un ordinateur distant.

Liste de paramètres :

/S système	Spécifie le système distant auquel se connecter.
/U [domaine\]utili.	Spécifie le contexte utilisateur sous lequel la commande doit exécuter.
/P [mot_passe]	Spécifie le mot de passe pour le contexte utilisateur donné. Il est demandé s'il est omis.
/M [module]	Liste toutes les tâches utilisant le nom de fichier exe ou dll donné. Si le nom de module n'est pas spécifié, tous les modules chargés sont affichés.
/SVC	Affiche les services hébergés dans chaque processus.

/V	Affiche les informations de tâches détaillées.
/FI filtre	Affiche un ensemble de tâches qui correspond au critère spécifié par le filtre.
/FO format	Spécifie le format de sortie. Valeurs valides : "TABLE", "LIST", "CSV".
/NH	Spécifie que les en-têtes de colonnes ne être affichée sur la sortie. Valide uniquement pour les formats "TABLE" et "CSV".
/?	Affiche l'aide.

Filtres :

Nom du filtre	Opérateurs valides	Valeurs valides
STATUS	eq, ne	RUNNING | NOT RESPONDING | UNKNOWN.
IMAGENAME	eq, ne	Nom d'image.
PID	eq, ne, gt, lt, ge, le	Valeur PID.
SESSION	eq, ne, gt, lt, ge, le	Numéro de session.
SESSIONNAME	eq, ne	Nom de session.
CPUTIME	eq, ne, gt, lt, ge, le	Heure valide au format hh:mm:ss.
MEMUSAGE	eq, ne, gt, lt, ge, le	Mémoire utilisée, en Ko.
USERNAME	eq, ne	Nom d'utilisateur [domaine\].
SERVICES	eq, ne	Nom de service.
WINDOWTITLE	eq, ne	Titre de la fenêtre.
MODULES	eq, ne	Nom de DLL.

Exemples :

```
TASKLIST
TASKLIST /M
TASKLIST /V /FO CSV
TASKLIST /SVC /FO LIST
TASKLIST /M wbem*
TASKLIST /S système /FO LIST
TASKLIST /S système /U domaine\utilisateur /FO CSV /NH
TASKLIST /S système /U utilisateur /P mot de passe /FO TABLE /NH
TASKLIST /FI "USERNAME ne AUTORITE NT\SYSTEM" /FI "STATUS
```

10.4.3- Commande TSKILL

Arrêt d'un processus en cours

TSKILL IDprocessus | NomProcessus [/SERVER:NomServeur] [/ID:IDsession | /A] [/V]

ID_processus	ID du processus devant être arrêté.
NomProcessus	Nom du processus devant être arrêté.
/SERVER:NomServeur	Serveur contenant l'ID de processus (ID actuel par défaut). /ID ou /A doit être spécifié lorsqu'un nom de processus et /SERVER sont utilisés.
/ID:ID_session	Arrêt du processus exécuté au cours de la session spécifiée.
/A	Arrêt du processus exécuté au cours de TOUTES les sessions.
/V	Affichage d'informations sur les actions exécutées.

10.4.4- Commande TASKILL

Arrêt d'un ou plusieurs processus en cours (plus élaboré que TSKILL).

TASKKILL [/S système] [/U utilisateur [/P mot_de_passe]]] {[/FI filtre] [/PID ID_processus | /IM image]} [/T] [/F]

Description : cet outil est utilisé pour arrêter des tâches par id de processus (PID) ou nom d'image.

Liste de paramètres :

/S système	Spécifie le système distant auquel se connecter.

/U [domaine\]utili.	Spécifie le contexte utilisateur sous lequel la commande doit s'exécuter.
/P [mot_de_passe]	Spécifie le mot de passe pour le contexte utilisateur donné. Il est demandé s'il est omis.
/FI filtre	Applique un filtre pour sélectionner un ensemble de tâches.
/PID ID_processus	Spécifie le PID du processus à arrêter. Utilisez Tasklist afin d'obtenir le PID.
/IM nom_image	Spécifie le nom d'image du processus à terminer. Le caractère générique * peut être utilisé pour spécifier toutes les tâches ou les noms d'images.
/T	Met fin au processus spécifié et tous les processus enfant qu'il a démarrés.
/F	Force les processus à se terminer.
/?	Affiche l'aide.

Nom du filtre	Opérateurs valides	Valeurs valides
STATUS	eq, ne	RUNNING | NOT RESPONDING | UNKNOWN.
IMAGENAME	eq, ne	Nom d'image.
PID	eq, ne, gt, lt, ge, le	Valeur PID.
SESSION	eq, ne, gt, lt, ge, le	Numéro de session.
CPUTIME	eq, ne, gt, lt, ge, le	Heure valide au format hh:mm:ss.
MEMUSAGE	eq, ne, gt, lt, ge, le	Mémoire utilisée, en Ko.
USERNAME	eq, ne	Nom d'utilisateur dans [domaine\].
MODULES	eq, ne	Nom de DLL.
SERVICES	eq, ne	Nom de service.
WINDOWTITLE	eq, ne	Titre de la fenêtre.

Exemples :

```
TASKKILL /IM notepad.exe
TASKKILL /PID 1230 /PID 1241 /PID 1253 /T
TASKKILL /F /IM cmd.exe /T
```

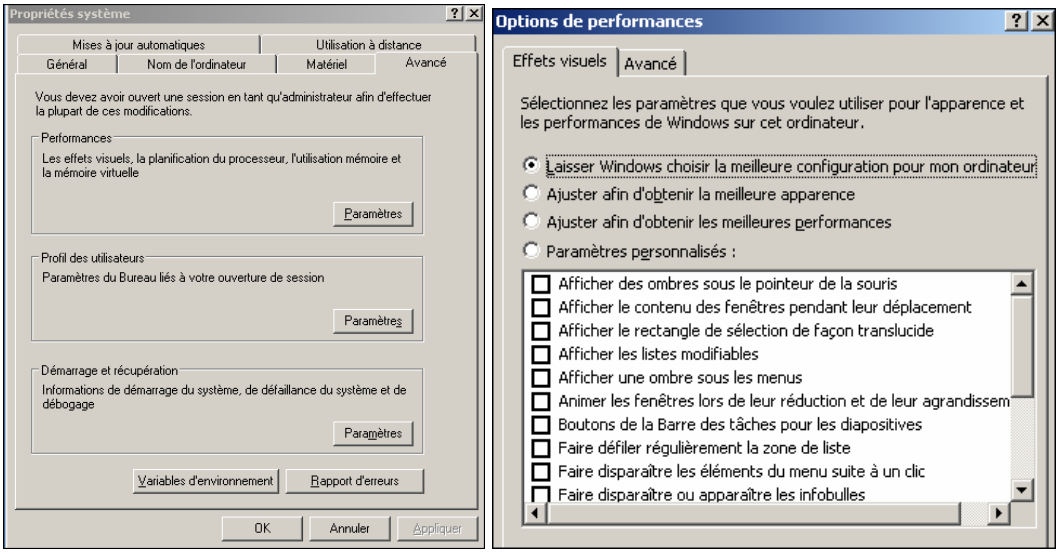
10.5- Optimiser les Performances

Pour optimiser les performances de votre ordinateur, vous devez appliquer de nombreuses phases de nettoyage des services et applications inutilisées.

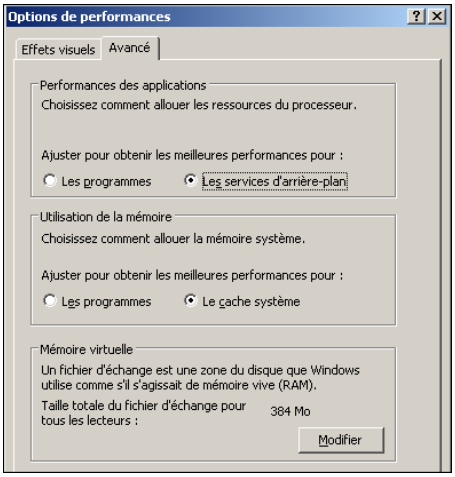
10.5.1- Temps Processeur

La première optimisation est de définir la répartition du temps processeur entre les applications tournant en avant-plan et les applications ou services tournant en arrière plan. Par défaut un serveur donnera la priorité aux services d'arrière-plan au détriment de l'interface utilisateur.
Rappel : les effets visuels sont sur toutes les machines de grands consommateurs de ressources processeur.
Pour optimiser les réglages, cliquez droit sur **Poste de Travail** ➔ onglet **Avancé** ➔ cliquez sur le bouton **Paramètres** de la rubrique **Performances**.
L'onglet **Effets visuels** vous permet de paramétrer et d'ajuster les animations et effets graphiques pour améliorer l'utilisation de l'interface utilisateur tout en dégradant légèrement les performances.

Par défaut laissez cocher l'option **Laisser Windows choisir la meilleure configuration pour mon ordinateur**.

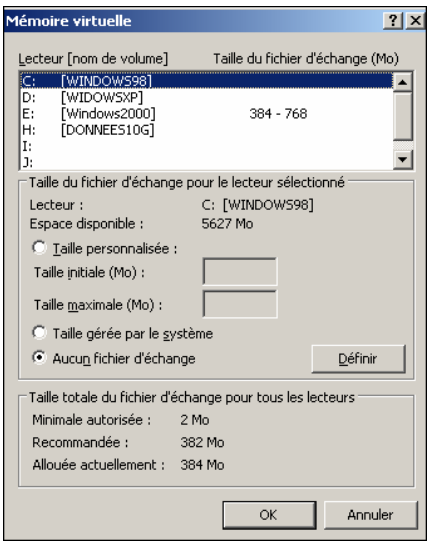


L'onglet **Avancé** permet de définir la répartition des ressources du processeur et de la mémoire virtuelle (fichier d'échange ou Swap).
En multitâche, l'application tournant en premier plan est celle dont le titre est en couleur bleu clair (par défaut). C'est celle sur laquelle l'utilisateur est en train de travailler.



10.4.2- Mémoire Virtuelle

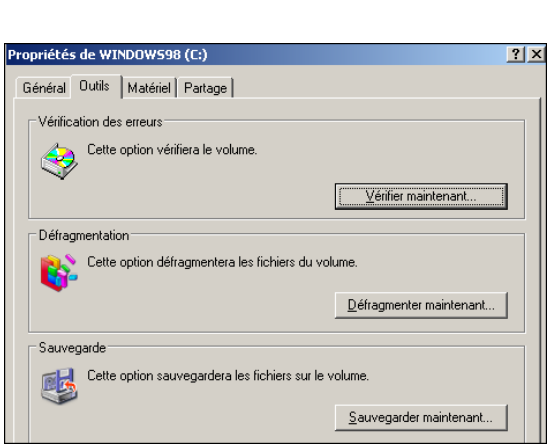
Fonctionnalité très importante des systèmes informatiques permettant de travailler avec une quantité de mémoire supérieure à la mémoire RAM physique disponible. Cette mémoire est disponible via la gestion d'un ou plusieurs fichiers d'échange situés à la racine du volume.
Par défaut il se situe à la racine de la partition contenant les fichiers système (%systemdrive%). Il porte le nom de **PAGEFILE.SYS** (fichier caché).
En standard sa taille est égale à 1,5 fois la taille de la mémoire vive de l'ordinateur et sa taille maximale au double de la taille initiale (ou 3 fois la taille de la mémoire vive).
Au dessus d'une certaine valeur il ne sert à rien de continuer à augmenter la taille du fichier d'échange.
Par contre vous pouvez décider de réaliser une répartition de plusieurs fichiers d'échange (un seul par partition).
Pour modifier la taille et l'emplacement du fichier swap, il vous suffit à partir de la fenêtre **Mémoire Virtuelle**, de sélectionner la partition de disque sur laquelle vous souhaitez ajouter, modifier ou supprimer le fichier d'échange. Vous pouvez cocher sur **taille personnalisée** afin de **Définir** vous même la taille initiale et maximale.
Nota : les modifications du fichier d'échange nécessitent un redémarrage du système pour être prises en compte.

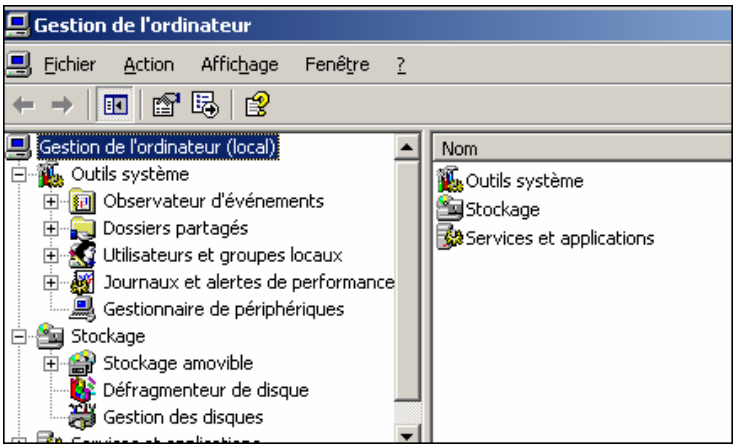


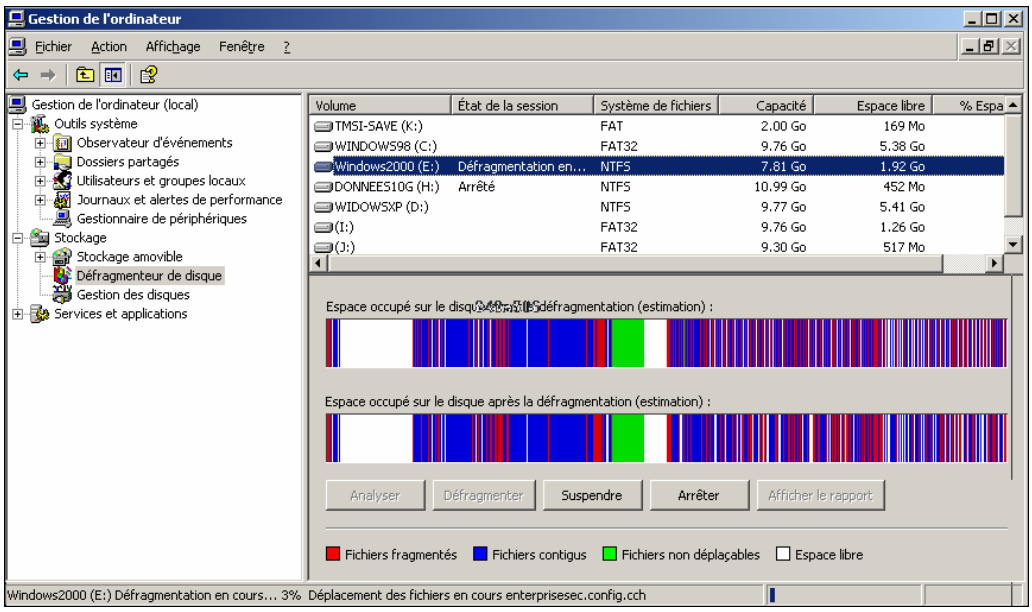
10.6- Les outils disques

10.6.1- Défragmenteur de Disque

Comme nous l'avons déjà vu avec les systèmes d'exploitation précédents, l'utilisation importante des fichiers de votre micro entraîne une fragmentation de ceux-ci. La fragmentation implique l'enregistrement des fichiers sur des clusters (espace disque) non contigus. Techniquement vous n'avez pas de problèmes, par contre cela peut entraîner un ralentissement du système (cela nécessite de nombreux déplacements des têtes). Vous devez donc fréquemment exécuter l'**Outil de défragmentation** de W2003 Server. Vous pouvez le lancer de plusieurs manières.
A partir de l'**Explorateur Windows** puis en sélectionnant le lecteur à défragmenter. Puis clic droit ➔ **Propriétés** ➔ **Outils** ➔ **Défragmenter**.
A partir du menu **Démarrer** ➔ **Tous les programmes** ➔ **Accessoires** ➔ **Outils Systèmes** ➔ **Défragmenteur de disques**.
A partir de la console **Gestion de l'ordinateur** et dans la zone **Stockage**, sélectionnez **Défragmenteur de disque**.
Sélectionnez ensuite le volume à défragmenter dans la partie haute du cadre, puis cliquez sur le bouton **Analyser afin de savoir s'il faut réaliser une défragmentation**. A la fin de l'analyse, vous pouvez afficher un rapport puis cliquer sur le bouton **Défragmenter** pour lancer aussitôt le processus de défragmentation.





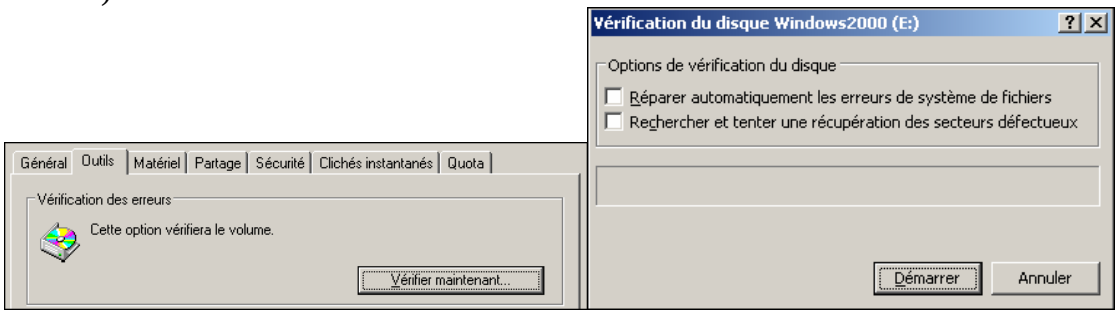


L'image du rapport vous donne des informations détaillées sur le volume et la fragmentation de chaque fichier. Les informations peuvent être ensuite enregistrées dans un fichier texte et être imprimées.
On peut utiliser le défragmenteur de disque avec la commande DEFRAG.
defrag <volume> [-a] [-f] [-v] [-?]

volume	Lettre de lecteur ou point de montage (d: ou d:\vol\mountpoint).
-a	Analyse uniquement.
-f	Force la défragmentation même si l'espace libre est bas.
-v	Sortie détaillée.
-?	Affiche ce texte d'aide.

10.6.2- Vérification du Disque

En plus d'une fragmentation qui ralentit votre travail, vous pouvez avoir des secteurs instables sur le disque dur. Ceci arrive lors d'un accès en lecture ou écriture à une zone endommagée. Dans ce cas votre fichier ne peut être ni lu ou écrit. W2003 Server propose l'outil **Vérificateur de disque**. Pour le lancer cliquez sur le lecteur à contrôler ➔ **Propriétés ➔ Outils ➔ Vérifier maintenant**. Vous pouvez éventuellement cocher les options pour la réparation automatique et la récupération des erreurs. Les blocs récupérés sont stockés sur la racine du volume avec l'extension **.CHK (File000x.chk**).



Vous avez la possibilité de réaliser cette opération en mode commande avec CHKDSK.
Vérifie un disque et affiche un rapport d'état.
CHKDSK [volume[[chemin]nom_de_fichier]] [/F] [/V] [/R] [/B] [/L[:taille]]

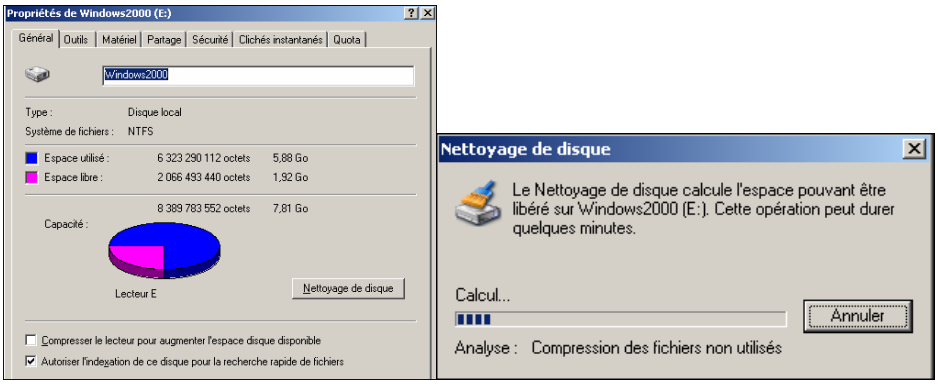
volume	Spécifie la lettre de lecteur (suivie de deux-points), le point de montage ou le nom de volume.
nom_de_fichier	FAT/FAT32 seulement : spécifie les fichiers dont la fragmentation est à vérifier.

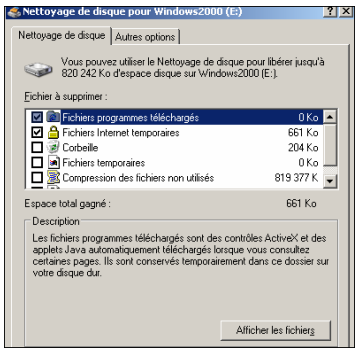
/F	Corrige les erreurs sur le disque.
/V	FAT/FAT32 : affiche les chemin d'accès et nom complets de tous les fichiers du disque. Sur NTFS : affiche également les éventuels messages de nettoyage.
/R	Localise les secteurs défectueux et récupère informations lisibles (implique /F)
/L:taille	NTFS seulement : change la taille du fichier journal pour la valeur spécifiée en kilo-octets. Si aucune taille n'est donnée, affiche la taille actuelle.
/X	Force le démontage préalable du volume si nécessaire. Les handles ouverts vers le volume ne seront alors plus valides (implique /F).
/I	NTFS seulement : vérifie sommairement les entrées d'index.
/C	NTFS seulement : ignore la vérification des cycles à 'intérieur de l'arborescence de dossiers.

Les options /I ou /C réduisent le temps d'exécution de CHKDSK en ignorant certaines vérifications sur le volume.

10.6.3- Nettoyage du disque

Un des facteurs agissant sur la dégradation des performances est la saturation de l'espace sur votre disque. Vous devez vérifier régulièrement le taux de remplissage de vos volumes. Et si l'espace vient à manquer vous pouvez être amenés à **Purger** certains fichiers, mails... Pour cela W2003 Server possède l'outil **Nettoyage de disque**. Cliquez sur **Démarrer ➔ Tous les programmes ➔ Accessoires ➔ Outils systèmes ➔ Nettoyage de disque.**





10.7- Examen des Performances

→ Paramètres de la Mémoire

- Définition d'une plage de valeurs normales pour permettre l'identification des tendances et des problèmes.
- Examen de la mémoire à l'aide de compteurs.
  - Surveillance des pages par seconde.
  - Surveillance des octets disponibles.

- Examen des fichiers d'échange.
  - Une pagination fréquente indique une mémoire insuffisante.
  - Vérification de la taille du fichier d'échange.
  - Utilisation de compteurs pour surveiller la taille du fichier d'échange.

→ Paramètres du processeur

- Examen des performances du processeur à l'aide de compteurs.
- Examen des valeurs d'utilisation pour les postes de travail.
  - Un taux d'utilisation élevé peut signifier une gestion efficace.
- Examen des valeurs d'utilisation pour les serveurs.
  - Un taux d'utilisation élevé est inacceptable.
  - Un taux d'utilisation élevé peut générer des goulets d'étranglement.

→ Paramètres du disque

- Surveillance des objets Disque physique et Disque logique pour examiner les performances.
- Utilisation de compteurs pour examiner l'activité du disque et déterminer les éléments suivants :
  - Pourcentage d'espace disque non alloué.
  - Volume des opérations d'E/S.
  - Vitesse de transfert des données.
  - Vitesse de transfert des octets.
  - Nombre de lectures et d'écritures réalisées par seconde.

Rappels et conseils pour un examen des performances du réseau

- Optimisation du temps processeur entre l'application d'avant plan et les applications d'arrière plan.

- Optimisation de la mémoire virtuelle

- Créer un fichier d'échanges dont la taille est adaptée au volume des applications utilisées.
- Par défaut le fichier d'échange (Swap) a une taille de 1,5 fois la RAM du micro.
- Empêcher un fichier d'échange de s'étendre.
- Définir un minimum et un maximum de mémoire identique.
- Créer plusieurs fichiers d'échange sur les volumes les moins sollicités (éviter celui d'amorçage).

- Identifier les goulets d'étranglement

- **MEMOIRE**
  - Paginée (virtuelle) et non paginée (RAM).
  - Fautes de pages matérielles (un taux élevé indique un accès fréquent au swap disque).
    - **Mémoire ➔ Fautes de pages / seconde >> 5** indique que la mémoire est un goulet pour le système.
    - **Mémoire ➔ Pages /secondes >>5** Indique le nombre de pages qui ne sont pas immédiatement disponibles en RAM, et devant être rapatriées à partir du disque dur ou qui doivent être écrites sur le disque dur pour libérer de la RAM pour d'autres pages.
- **PROCESSEUR** : **processeur %Temps processeur >> 80%** indique la durée ou le processeur est occupé (si > 80 % en permanence goulet d'étranglement).
- **DISQUE**
  - Activer les compteurs disque (commande Diskperf).
  - %Temps disque : si taux proche de 100 % il y a un problème.
  - Longueur de la file d'attente disque. Si > 2 en permanence ➔ goulet pour le disque.
- **RESEAU** : suivre sur le serveur ➔ **Total octets/seconde et Ouvertures de sessions /seconde.**

XI- DEPANNAGE

11.1- Etapes de démarrage

- Tests des composants matériels (séquence POST).
- Lecture du MBR (Master Boot Record).
- Examen par le MBR de la table des partitions.
- Recherche de la partition active dans la table en contenant 4 Maximum.
- Exécution du secteur de démarrage (pré chargeur du système d'exploitation) de la partition active.
- Chargement par le pré chargeur du chargeur du système d'exploitation qui au final va véritablement charger le système d'exploitation.

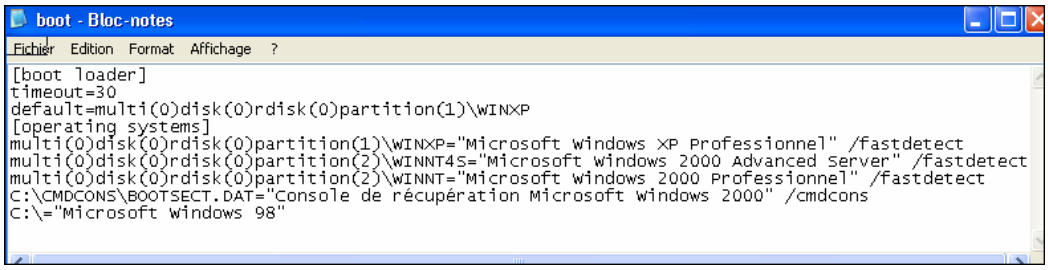
11.1.1- Etape 1

Lecture de NTLDR (identique à IO.sys de Dos). NTLDR fait passer le processeur du mode réel en mode mémoire linéaire 32 bits. Le démarrage des pilotes de mini système de fichiers FAT et NTFS permet l'accès aux systèmes de fichiers afin d'amorcer complètement 2003. NTLDR lit le contenu du fichier Boot.ini afin de construire le menu du chargeur d'amorçage.

11.1.2- Etape 2 : fichier BOOT.INI

Fichier texte permettant d'amorcer Windows 2003 ou de démarrer sur un autre système d'exploitation.

Exemple

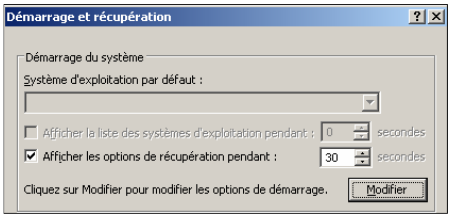


Le fichier BOOT.INI comprend deux sections **[boot loader]** et **[operating systems].** C'est un fichier système caché en lecture seule (**S, R, H**) créé automatiquement à l'installation de Windows 2003 sur la partition système des plateformes Intel.

➔ **Section [boot loader]**

- **timeout = 30** : permet de régler un temps d'attente pour faire un choix de démarrage parmi les systèmes d'exploitation installés. Ici 30 secondes.
- **timeout = 0** : démarrage immédiat du système d'exploitation qui est défini dans la ligne default.
- **timeout = -1** : le temps d'attente est infini, le choix est obligatoire. Il faut mettre cette valeur manuellement.

Cette valeur peut être modifiée par le **panneau de configuration**, **système**, onglet **général** ou directement dans le fichier boot.ini. Lorsque le délai du Timeout est dépassé, le système utilise le chemin décrit dans la ligne **Default** pour rechercher le répertoire d'installation de WINDOWS 2003.



Noms Arc (ADVANCED RISC COMPUTING).
Avec disque IDE : default=multi(x)disk(0)rdisk(z)partition(n)
Avec disque SCSI : default=Scsi(x)disk(y)rdisk(0)partition(1)

- **SCSI(x) ou MULTI(x) : x** désigne le numéro de contrôleur matériel SCSI dans l'ordre d'initialisation.
- **DISK(y)** : correspond pour les contrôleurs SCSI multibus au numéro de bus. Toujours égal à 0 pour les contrôleurs multi.
- **RDISK(z)** : z indique le numéro de disque sur le contrôleur pour les composants multi. Toujours égal à 0 pour les disques SCSI.
- **PARTITION(n)** : n indique le numéro de la partition de 1 à n sur le disque.

Par exemple**,** sur un disque géré par un contrôleur IDE, la deuxième partition du deuxième disque physique, du premier contrôleur sera référencée par :
Multi (0) disk(0) rdisk(1) partition(2).

➔ **Section [operating systems]**
Cette section énumère les systèmes d'exploitation disponibles. Chaque entrée inclut le chemin vers la partition d'amorçage du système d'exploitation.

Les commutateurs de boot.ini : ils sont insensibles à la casse.

- **/basevideo** : démarre l'ordinateur avec le pilote vidéo VGA standard.
- **/crashdebug** : charge le débogueur au démarrage de WINDOWS NT. Il reste inactif tant qu'une erreur n'est pas détectée.
- **/debug** : le débogueur est chargé au démarrage.
- **/maxmem :n** : spécifie la quantité mémoire maximale (RAM) que 200 peut employer. Utiliser cette option lors, de problème avec des barrettes mémoire.
- **/nodebug :** aucune information de déboguage.
- **/sos** : affiche les noms des pilotes de périphériques au fur et à mesure de leur chargement.

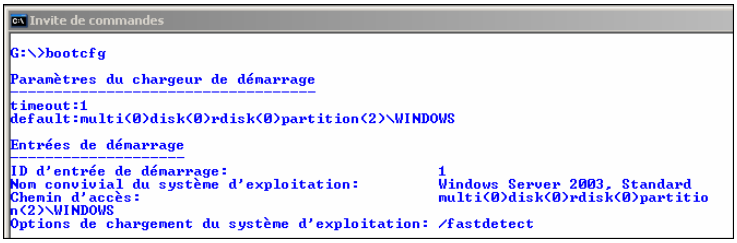
BOOTCFG mode commande
BOOTCFG /paramètre [arguments]
Cet outil de ligne de commande peut être utilisé pour configurer, interroger, modifier ou supprimer les paramètres de l'entrée de démarrage dans boot.ini.
Liste de paramètres :

- /Copy : effectue une copie d'une entrée de démarrage existante.
- /Delete : supprime une entrée de démarrage du fichier boot.ini.
- /Query : affiche les paramètres actuels d'entrée de démarrage.
- /Raw : autorise l'utilisateur à spécifier les options à ajouter.
- /Timeout : autorise l'utilisateur à modifier la valeur du délai d'attente.
- /Default : autorise l'utilisateur à modifier le système par défaut.
- /EMS : permet à l'utilisateur de paramétrer l'option /redirect pour la prise en charge du mode sans affichage.
- /Debug : autorise l'utilisateur à spécifier le port et le taux en bauds pour le débogage à distance.
- /Addsw : autorise l'utilisateur à ajouter des commutateurs prédéfinis.
- Rmsw : autorise l'utilisateur à supprimer des commutateurs prédéfinis.
- /Dbg1394 : autorise l'utilisateur à configurer le port 1394 pour le débogage.
- /? : affiche l'aide.

Exemples :

BOOTCFG /Copy /?
BOOTCFG /Delete /?
BOOTCFG /Query /?
BOOTCFG /Raw /?
BOOTCFG /Timeout /?
BOOTCFG /EMS /?

BOOTCFG /Debug /?
BOOTCFG /Addsw /?
BOOTCFG /Rmsw /?
BOOTCFG /Dbg1394 /?
BOOTCFG /Default /?
BOOTCFG /?



Message d'erreur d'un nom ARC erroné :
« Windows 2003 n'a pas pu démarrer car le fichier suivant est manquant ou endommagé »: %systemroot%\System32\ntoskrnl.exe
Veuillez installer une copie du fichier ci-dessus ».
Bien souvent en éditant le fichier boot.ini, vous résolvez le problème. Une erreur sur un nom ARC peut arriver suite à la création d'une nouvelle partition principale lorsque la partition d'amorçage 2003 est dans un lecteur logique d'une partition étendue.

11.1.3- Etape 3 : chargement et exécution de NTDETECT.com

Chargement et exécution de NTDETECT.com. C'est un programme de détection matérielle générant la clé volatile HARDWARE. Si un système d'exploitation autre que Windows 2003 est sélectionné, le fichier BOOTSEC.DOS (copie de l'ancien secteur de démarrage avant l'installation de 2003) permet d'exécuter le pré chargeur de cet autre système.

11.1.4- Etape 4

Menu de démarrage Profil Matériel/Récupération de configuration puis chargement du système Windows 2003.

11.1.5- Options de démarrage

Description des options
Appui sur la touche **F8** au démarrage du système.

- **Mode sans échec :** démarre le système en chargeant le minimum de pilotes. Création d'un fichier Ntbtlog.txt sous le répertoire %systemroot% qui recense les pilotes chargés et non chargés.
- **Mode sans échec avec prise en charge du réseau :** identique précédemment + prise en charge du réseau.
- **Invite de commandes en mode sans échec :** Win2003 s'exécute en mode sans échec sans charger l'interface graphique.
- **Inscrire les événements de démarrage dans le journal :** lance Win2003 normalement en créant un rapport de tous les pilotes et services chargés durant le démarrage (fichier NTBLOG.txt).
- **Démarrage en mode VGA :** Win2003 démarre avec le pilote graphique VGA standard (à utiliser si vous avez un problème de carte graphique).
- **Dernière bonne configuration connue :** vos derniers paramètres fonctionnels.
- **Mode restauration Active Directory (contrôleurs de domaine. Windows 2003) :** démarrage de Win2003 sans charger Active Directory dans le but de restaurer l'annuaire (sur un contrôleur de domaine uniquement).

- **Mode déboguage :** envoie les informations de déboguage à un autre ordinateur relié par un câble série.
- **Démarrer Windows normalement (choix par défaut).**
- **Redémarrer.**
- **Revenir au menu de sélection du système d'exploitation.**

Au démarrage Windows 2003 gère 3 jeux de configuration et démarre dans la majorité des cas avec la configuration par défaut ou CurrentControlSet **(HKEY_LOCA_MACHINE\System).**
Par défaut Win2003 enregistre une configuration comme dernière bonne configuration dès l'instant où l'utilisateur réussit à ouvrir une session (même si il y a des erreurs).
En cas d'erreur de démarrage du type Au moins un pilote ou service n'a pas pu démarrer à l'amorçage du système, vous devez arrêter puis redémarrer en choisissant Dernière Bonne Configuration connue.

11.1.6- Disquette d'amorçage (démarrage)

Création d'une disquette d'amorçage
La disquette d'amorçage (FAT) a pour but de lancer W2003 que le système de fichiers soit FAT ou NTFS :

- S'il est installé sur un autre disque que C: alors que C: est en panne.
- S'il existe un miroir du système d'exploitation.

Pour créer une disquette d'amorçage, il faut :

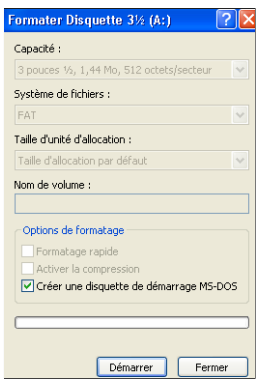
- Ouvrir une session en tant qu'administrateur.
- Puis formater une disquette, en utilisant l'outil de formatage WINDOWS 2003 ou NT4/ W2000.

Pour créer la disquette de restauration, formatez une disquette en utilisant le système d'exploitation Windows 2003 (obligatoire pour que le pré chargeur 2003 soit installé sur la disquette, charge le NTLDR), puis copiez les fichiers suivants sur cette disquette.
Ces fichiers sont situés dans le répertoire racine de la partition système :

- **Ntldr.**
- **Ntdetect.com.**
- **Ntbootdd.sys** : requis seulement si la partition d'amorçage est située sur un disque SCSI et que le BIOS n'est pas activé sur le contrôleur. Ce fichier est le pilote miniport SCSI employé pour rechercher le disque miroir.
- **Boot.ini** : avec un chemin d'accès de remplacement pointant sur la copie miroir de la partition système, spécifiée à l'aide des conventions de dénomination ARC.
- **Bootsect.dos** : seulement sur les ordinateurs à amorçage double.

Les 3 étapes précédentes du démarrage s'effectuent à partir de la disquette.

Création d'une disquette de démarrage MS-DOS
Disquette vierge ➔ **Poste de travail** ➔ clic droit sur lecteur de disquette ➔ **Formater** ➔ **Créer une disquette de démarrage MS-DOS** ➔ **Démarrer**.
Disquette permettant d'amorcer votre micro sous MS-DOS (donc en Fat16).



11.1.7- Démarrage à partir du CD-ROM Windows 2003

Votre BIOS doit permettre le démarrage à partir du CD-ROM.
Ecran de démarrage :

Installation de Windows 2003 Professionnel
Bienvenue !
Cette partie du programme d'installation prépare l'installation de Microsoft ® Windows 2003 ® sur votre ordinateur.
Pour installer Windows 2003 maintenant, appuyez sur ENTREE.
Pour réparer ou récupérer une installation de Windows 2003, appuyez sur R.
Pour quitter le programme d'installation sans installer Windows 2003.
Appuyez sur F3.
ENTREE=Continuer R=Réparer F3=Quitter

11.1.8- Console de Récupération

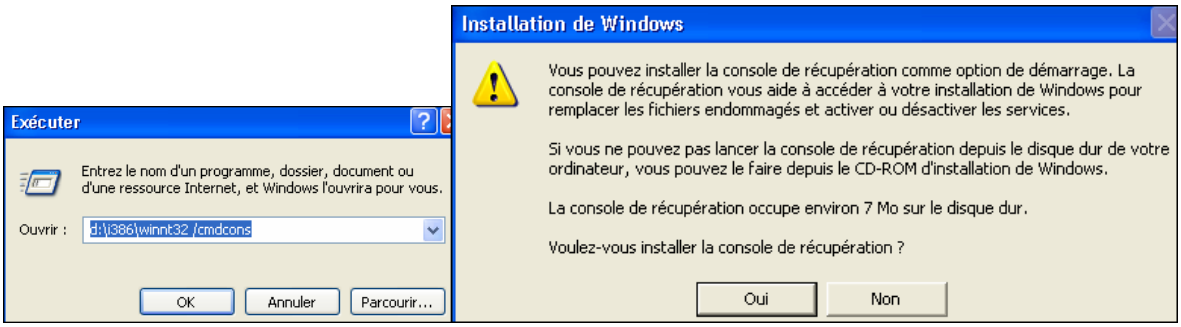
Présentation
C'est une interface en mode texte mettant à votre disposition un certain nombre de commandes permettant de réparer le système si vous ne pouvez plus démarrer Windows 2003.

- Permet d'arrêter ou démarrer des services qui seraient susceptibles d'empêcher le démarrage du système.
- Permet de formater les disques durs, ainsi que de lire des données situées sur les disques (FAT ou NTFS).
- Permet de créer un secteur d'amorçage et un enregistrement principal (MBR).
- Permet de copier des fichiers à partir du CD-ROM d'installation du système d'exploitation ou à partir d'autres supports amovibles.

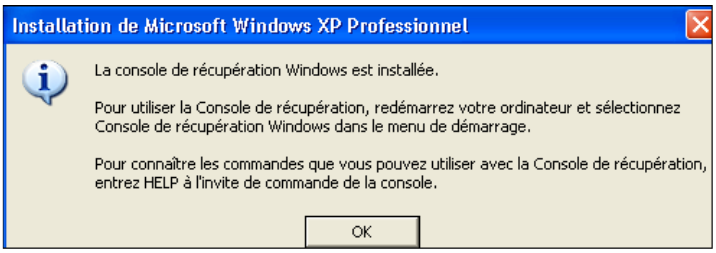
2 méthodes pour exécuter la console de récupération :

- Démarrer avec le CD de Win2003 ➔ puis appuyer sur la touche C pour démarrer la console de récupération.
- Accéder à cette console par le menu démarrage de Windows2003, si elle est déjà installée.

Installer la console de récupération
Répertoire \I386 du CD Win2003. Taper la ligne de commande \winnt32 /cmdcons puis validez **Oui**.



Redémarrez votre micro.



Démarrage de la Console de Récupération
Après redémarrage l'option Console de récupération Microsoft Windows apparaît comme choix de démarrage. Le fichier Boot.ini est modifié :

```
[boot loader]
timeout=30
default=multi(0)disk(0)rdisk(0)partition(1)\WINXP
[operating systems]
multi(0)disk(0)rdisk(0)partition(1)\WINXP="Microsoft Windows XP Professionnel" /fastdetect
multi(0)disk(0)rdisk(0)partition(2)\WINNT4S="Microsoft Windows 2000 Advanced Server"
/fastdetect
multi(0)disk(0)rdisk(0)partition(2)\WINNT="Microsoft Windows 2000 Professionnel" /fastdetect
C:\="Microsoft Windows 98"
C:\CMDCONS\BOOTSECT.DAT="Console de récupération Microsoft
Windows XP" /cmdcons
```

Console de récupération Microsoft Windows 2003 ™.
La console de récupération fournit une réparation du système et des fonctionnalités de récupération.
Entrez « exit » pour quitter l'invite de commandes et redémarrer le système.

1: c:\Win2003
2: f:\Winnt
3: f:\Winnt4s
4: p:\Windows

Sur quelle installation de Windows 2003 voulez-vous ouvrir une session (Appuyer sur ENTREE pour annuler) ? **1**
Entrez le mot de passe Administrateur: ***********

C:\Win2003

Commandes de la console de récupération
Les commandes suivantes peuvent s'utiliser avec la console de récupération, et sont visibles avec la commande Help.

- **Attrib** : change les attributs d'un fichier ou d'un répertoire.
- **Batch** : exécute les commandes spécifiées dans le fichier texte.
- **Bootcfg** : configuration du fichier d'amorçage (boot.ini) et récupération.
- **ChDir (Cd)** : affiche le nom du répertoire en cours ou change de répertoire en cours.
- **Chkdsk** : vérifie un disque et affiche un rapport d'état.
- **Cls** : efface l'écran.
- **Copy** : copie un fichier à un autre emplacement.
- **Delete (Del)** : supprime un ou plusieurs fichiers.
- **Dir** : affiche la liste des fichiers et des sous répertoires d'un répertoire.
- **Désactiver** : désactive un service système ou un pilote de périphérique.
- **Diskpart** : gère les partitions de vos disques durs.
- **Activer** : démarre ou active un service système ou un pilote de périphérique.
- **Exit** : arrête la console de récupération et redémarre l'ordinateur.
- **expand** : extrait un fichier d'un archive compressée.
- **Fixboot** : écrit un nouveau secteur d'amorçage sur la partition spécifiée.
- **Fixmbr** : répare le secteur de démarrage principal du disque spécifié.
- **Format** : formate un disque.
- **Aide** : affiche la liste des commandes à votre disposition dans la console de récupération.
- **Listsvc** : répertorie les services et les pilotes disponibles sur l'ordinateur.
- **Logon** : ouvre une session sur une installation Windows.
- **Map** : affiche les mappages de lettre de lecteur
- **Mkdir (Md)** : crée un répertoire.

- **More** : affiche un fichier texte.
- **Net use** : connecte un partage réseau à une lettre de lecteur.
- **Rename (Ren)** : renomme un fichier.
- **Rmdir (Rd)** : supprime un répertoire.
- **Set** : affiche et définit des variables d'environnement.
- **Systemroot** : définit comme répertoire en cours le répertoire racine_système de l'ordinateur sur lequel vous conduisez votre session.
- **Type** : affiche un fichier texte.
- **Fixmbr :** répare l'enregistrement de démarrage principal du disque de démarrage. La commande **fixmbr** n'est disponible que si vous utilisez la console de récupération.
  - **fixmbr** [nom_de_périphérique].
  - **Paramètre :** nom_de_périphérique. Périphérique (lecteur) sur lequel vous souhaitez écrire un nouveau secteur de démarrage principal. Ce nom peut être obtenu à partir de la sortie de la commande **map**. Exemple de nom de périphérique correct : **\Device\HardDisk0.**
  - **Exemple** : l'exemple suivant écrit un nouveau secteur de démarrage principal sur le périphérique spécifié : **fixmbr \Device\HardDisk0.**
- **Fixboot :** écrit un nouveau secteur d'amorçage de partition sur la partition système. La commande **fixboot** n'est disponible que si vous utilisez la console de récupération.
  - **fixboot** [lecteur].
  - **Paramètre** : lecteur sur lequel un secteur de démarrage sera écrit. Ce paramètre remplace le lecteur par défaut qui représente la partition système à laquelle vous êtes connecté. Exemple de lecteur : **D:.**
  - **Exemple :** l'exemple suivant écrit un nouveau secteur de démarrage de partition sur la partition système du lecteur D : **fixboot d:.**
- **Bootcfg :** la commande **bootcfg** est utilisée pour la configuration de démarrage et la récupération (boot.ini pour la plupart des ordinateurs). La commande **bootcfg** n'est disponible que si vous utilisez la console de récupération. Elle est associée à des paramètres différents et disponible à partir de l'invite de commande.
- **Net use :** connecte un partage réseau à une lettre de lecteur. La commande **net use** n'est disponible que si vous utilisez la console de récupération. La commande **net use** associée à des paramètres différents est disponible à partir de l'invite de commande.

11.2- Sauvegardes et Restauration

11.2.1- Présentation

La sauvegarde de données a pour objectif de restaurer des données perdues. Des autorisations et des droits d'utilisateur sont nécessaires pour sauvegarder et restaurer les données. Win2003 possède un outil de sauvegarde performant intégré. Il est possible de réaliser des sauvegardes sur périphériques à bandes, lecteurs logiques, disques amovibles ou sur des CD-ROM enregistrables. Le logiciel de sauvegarde supporte les volumes FAT ou NTFS. La réalisation s'effectue via l'assistant ou manuellement.

Lorsque vous créez une opération de sauvegarde, vous devez indiquer les éléments suivants :

- Les lecteurs, dossiers ou fichiers à sauvegarder.
- Une destination de sauvegarde.
- Le chemin d'accès et le nom du fichier de sauvegarde, ou une bande à utiliser.
- Les options de sauvegarde.
- La description de l'opération de sauvegarde.
- La présence ou non de sauvegardes existantes sur le support de sauvegarde.
- Les options de sauvegarde avancées.
- Possibilité de lancer en mode commande **NTBACKUP.**

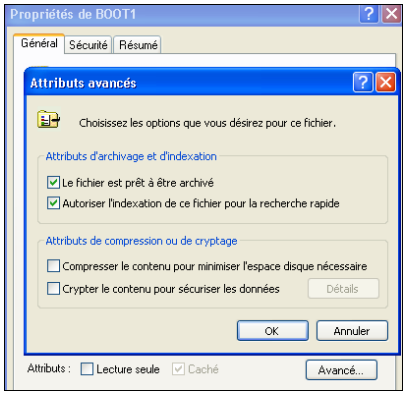
11.2.2- Planification d'une sauvegarde

- Spécifiez un nom et un compte d'utilisateur pourvu des autorisations appropriées.
- Spécifiez le nom de l'opération.
- Spécifiez la date, l'heure et la fréquence.

11.2.3- Sauvegardes des données

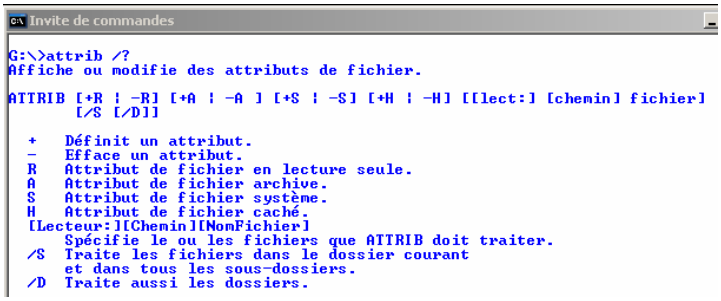
Chaque fichier et dossier possède un attribut d'archive.

- S'il est modifié, le fichier ou dossier a été modifié depuis la dernière sauvegarde.
- Dès qu'un fichier est modifié, cet attribut est automatiquement activé, il sera sauvegardé lors de la prochaine sauvegarde (visualisable par les propriétés d'un fichier ou par un clic sur **Avancés**).
- Si l'option **Le fichier est prêt à être archivé** est cochée cela indique que l'attribut est positionné.



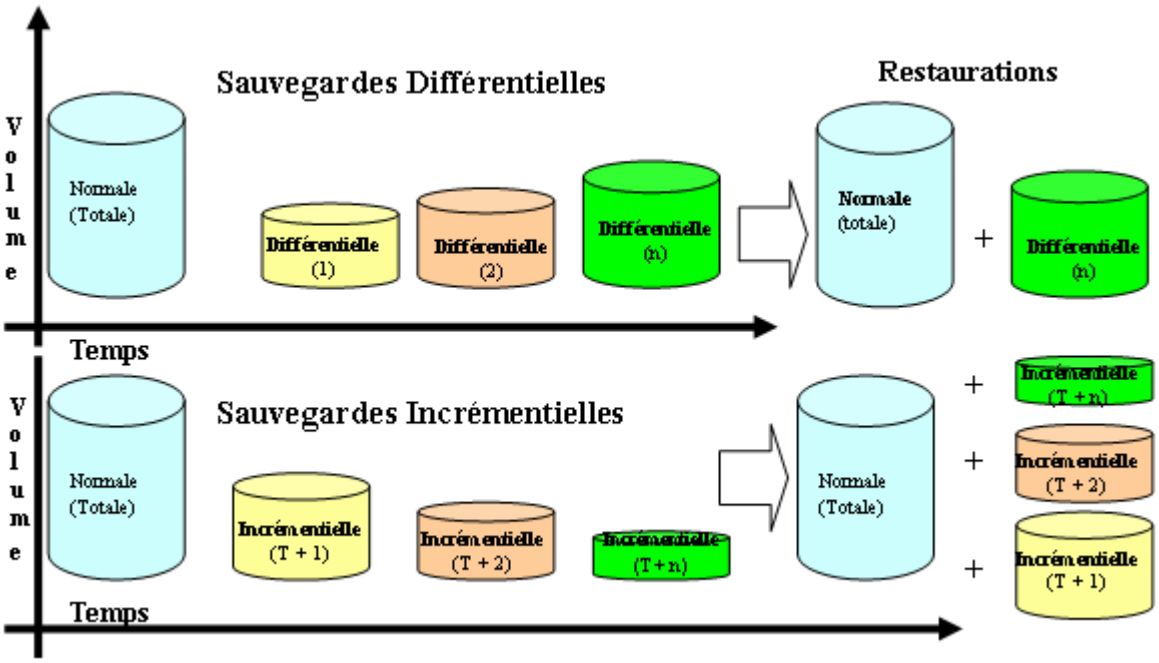
Utilitaire ATTRIB

Permet la visualisation ou la modification de l'attribut d'archive à partir d'une invite de commande.



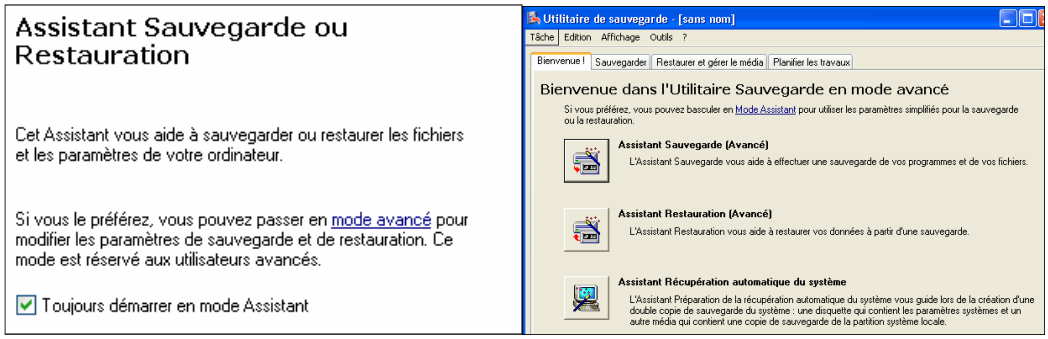
11.2.4- Types de sauvegardes

Type	Sauvegarde	Suppression d'attribut d'archive
Normale	Tous les Fichiers et dossiers sélectionnés.	Oui
Copie	Tous les Fichiers et dossiers sélectionnés.	Non
Différentielle	Tous les Fichiers et dossiers sélectionnés qui ont été modifiés depuis la dernière sauvegarde.	Non
Incrémentielle	Tous les Fichiers et dossiers sélectionnés qui ont été modifiés depuis la dernière sauvegarde.	Oui
Tous les jours ou quotidienne	Tous les Fichiers et dossiers sélectionnés qui ont été modifiés pendant la journée.	Non

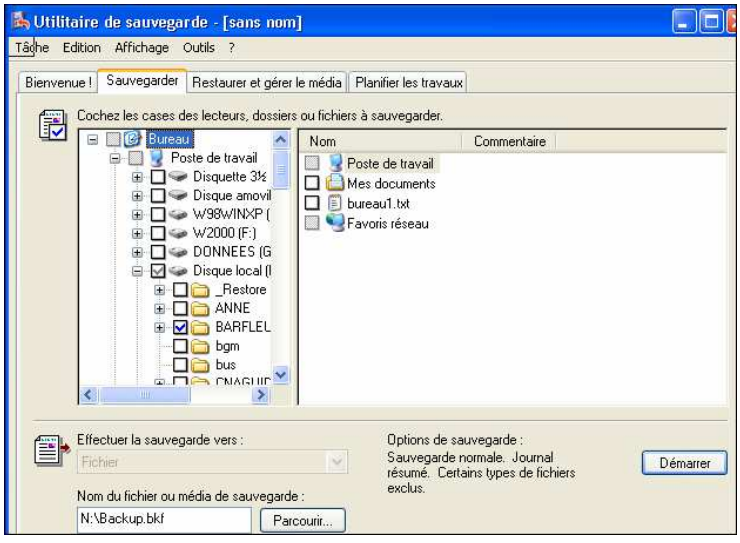


11.2.5- Sauvegardes des données

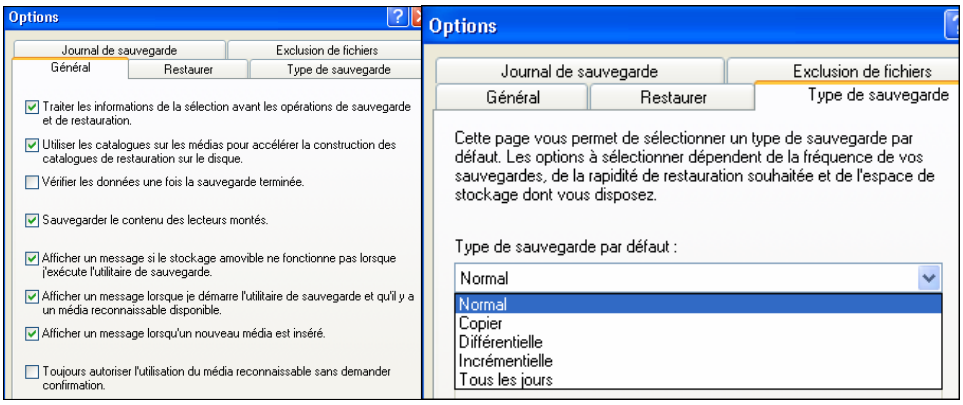
Démarrer ➔ Accessoires ➔ Outils systèmes ➔ Utilitaire de sauvegardes. L'assistant démarre. Vous avez la possibilité de démarrer directement la sauvegarde ou la restauration. Ou cliquez sur **Mode Avancé** pour poursuivre avec l'assistant. Le menu de **Bienvenue** attend votre sélection.



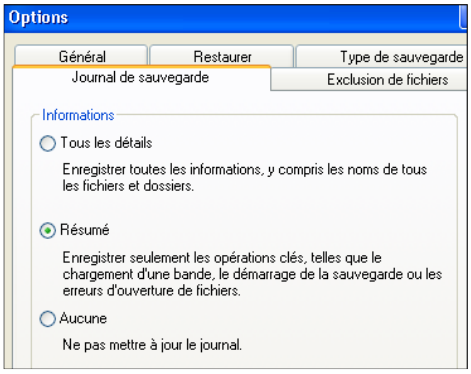
Onglet **Sauvegarder** ➔ Sélectionnez les dossiers ou fichiers à sauvegarder.



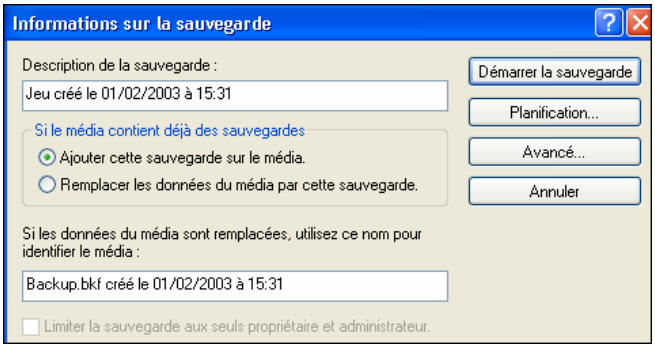
Menu **Outils ➔ Options ➔ Type de sauvegarde ➔ OK.**



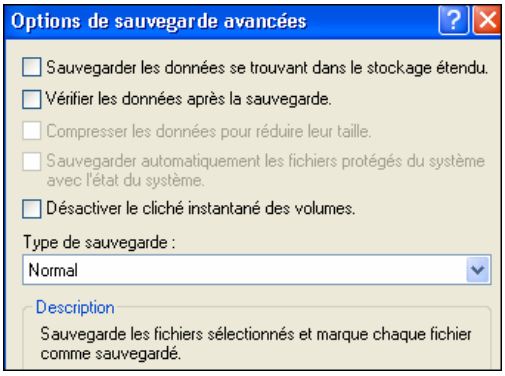
Entrez le nom du fichier de sauvegarde et le lecteur de sauvegarde ➔ **Démarrer.**



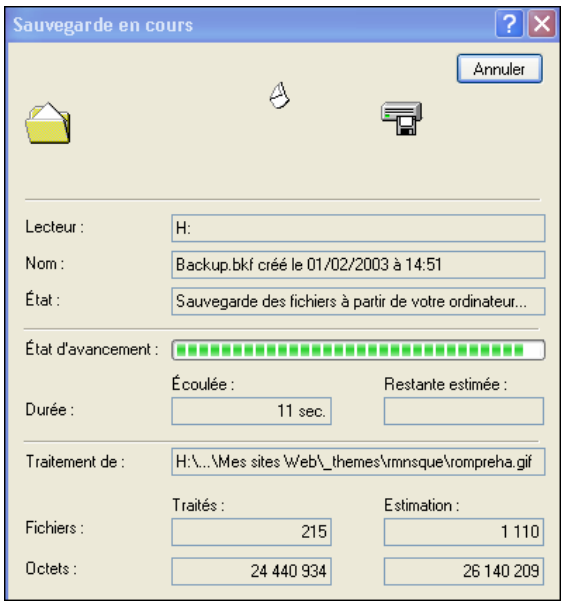
Entrez une description pour votre sauvegarde (par défaut la date de création).



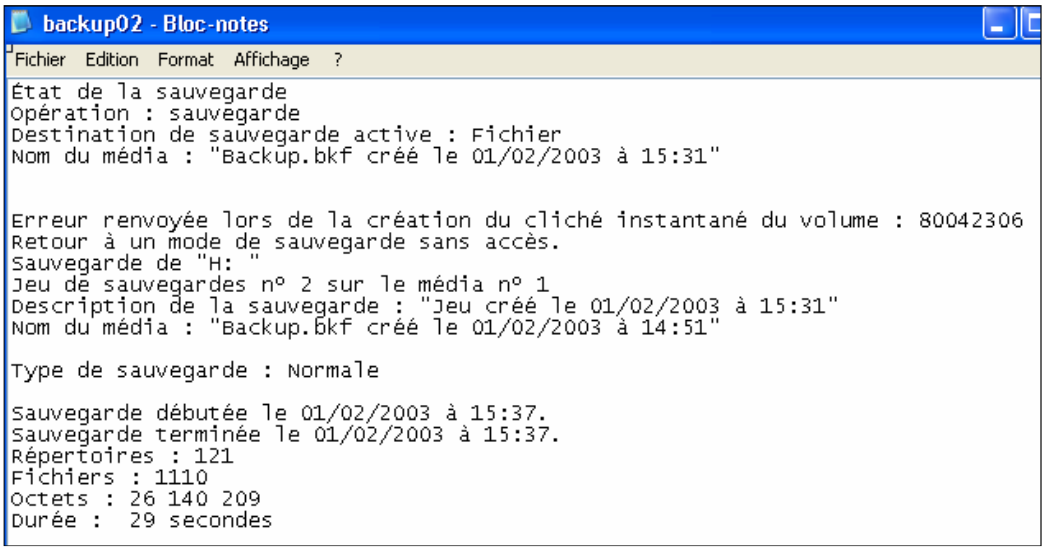
Le bouton **Avancé** vous permet de choisir le type de sauvegarde (identique au menu Outil précédent).



Démarrage de la sauvegarde.



Visualiser le journal de sauvegarde.



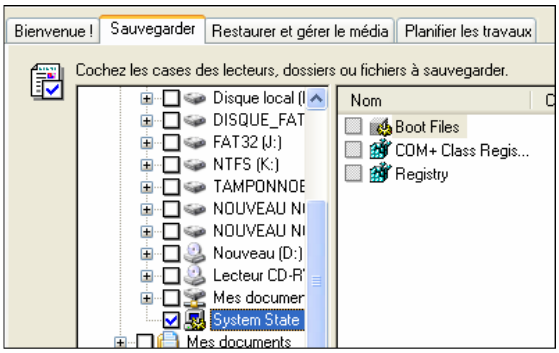
Visualiser l'icône de sauvegarde (Backup).

✋ Les permissions NTFS associées aux fichiers et dossiers ainsi que le cryptage sont conservées lors de la restauration sur une partition NTFS.

11.2.6- Sauvegardes de l'état du système

- Base de registre.
- Fichiers de démarrage du système...

Ces composants ne peuvent pas être sauvegardés individuellement.

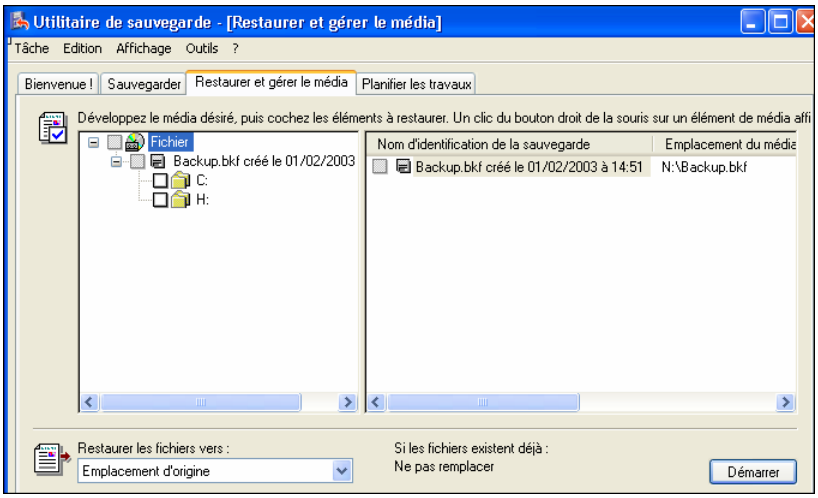


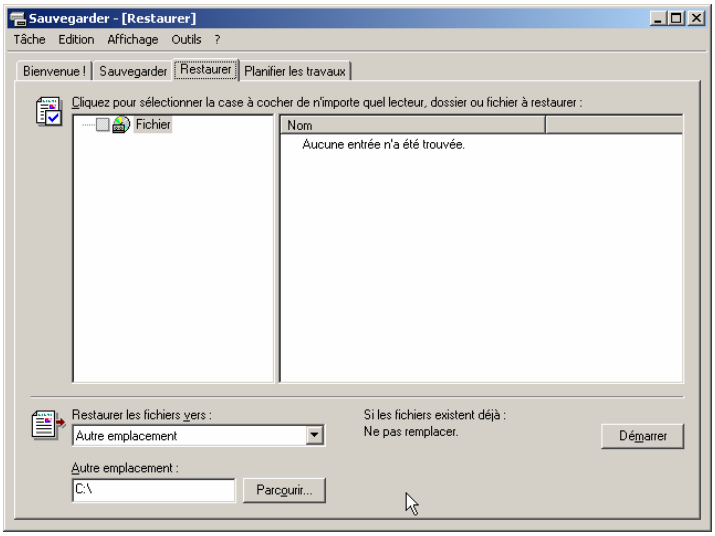
11.2.7- Planification des travaux de sauvegarde

Onglet **Planifier les travaux ➔ Utilitaires de sauvegarde ➔ Ajouter une opération.**

11.2.8- Restauration des fichiers et des dossiers

- Dossiers et fichiers à restaurer.
- Emplacement de restauration.
- Options de restauration.





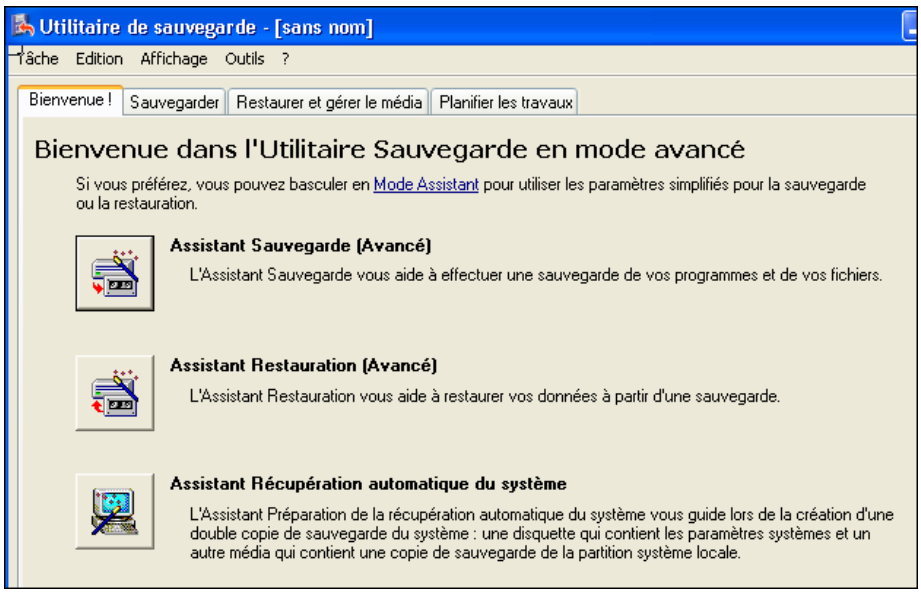
11.2.9- Restauration de l'état du système

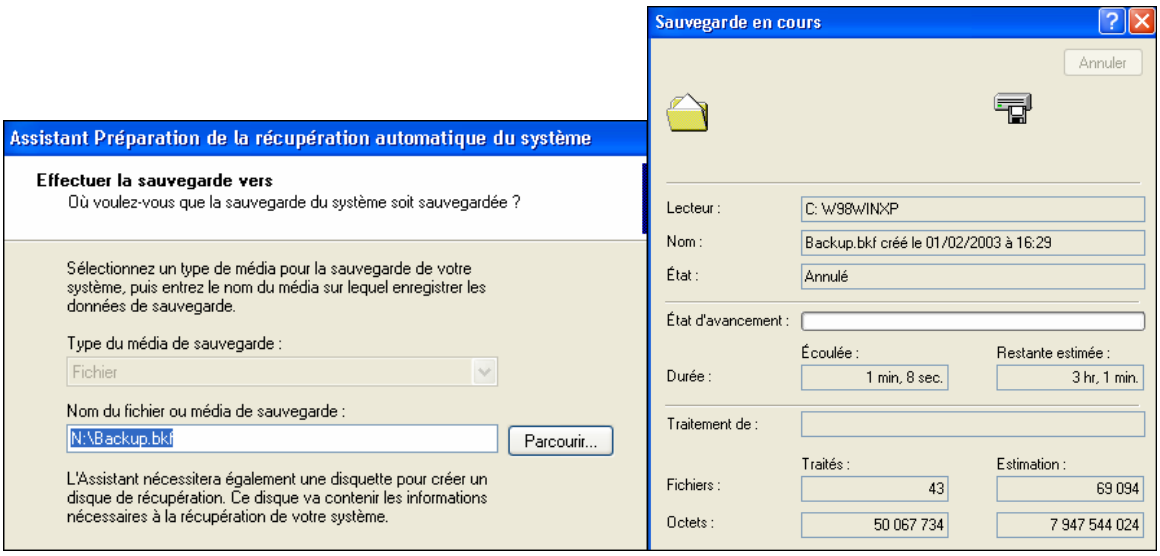
Elle supprime l'état en cours pour le remplacer. Il est impératif de réaliser des sauvegardes régulières. Si le micro tombe complètement en panne, il est possible de restaurer l'état du système de l'ancien poste sur le nouveau pour obtenir les mêmes caractéristiques (même nom, même base de registre). Réinstallez 2003 en conservant les options d'installation par défaut, puis réinstallez toutes les applications qui se trouvaient sur le poste. Ensuite à l'aide du programme **Utilitaire de sauvegarde**, restaurez l'état du système à partir de la plus récente sauvegarde.

11.2.10- Restauration automatique du système ASR (Automatic System Recovery)

- Il existe la possibilité de redémarrer une version de Windows 2003 lorsque le système refuse de démarrer, même avec l'option **Dernière configuration connue** et **Mode sans Echec**.
- Récupération de la configuration des disques.
- Cette option permet de sauvegarder la partition contenant les fichiers système de Windows 2003. En plus sauvegarde de certaines informations stockées sur une disquette.
- Disquette de restauration du système.

Création d'une disquette en même temps que le jeu de sauvegarde de la partition d'amorçage de Windows 2003.





11.2.11- Utiliser le jeu de récupération

- Nécessite la disquette de récupération automatique.
- CD-ROM Windows 2003 (amorçable).
- Dernier jeu de sauvegarde.
- Redémarrer le micro ➔ touche F2 ➔ introduire la disquette de récupération système ➔ suivre les indications.