Microsoft Windows 2000 :

Implémentation de Windows 2000 Professionnel et Serveur

Essentiel

de préparation aux certifications 70-210 / 70-215

Par :
NEDJIMI Brahim
THOBOIS Loïc

sur une base de O. Boisne, J.L. Moureaux, A. Nedjimi

23, rue Château Landon
75010 – PARIS
www.supinfo.com

Table des Matières

Module 1
Installation de Windows 2000 ou mise à niveau vers Windows 2000

1 Premier aperçu de Windows 2000

Parmi les produits de la famille Windows 2000, il existe quatre systèmes d'exploitation : Windows 2000 Professionnel, Windows 2000 Server, Windows 2000 Advanced Server et Windows 2000 Datacenter. Mis à part le nombre de processeurs supporté par chacun de ces systèmes, peu de choses les différencient. Les deux systèmes que nous allons étudier, Windows 2000 Professionnel et Server supportent respectivement jusqu'à deux et quatre processeurs (la version Advanced Server en supporte jusqu'à huit et la version Datacenter jusqu'à trente-deux).

Le tableau suivant indique la configuration minimale requise pour l'installation de chacun de ces deux systèmes.

	Windows 2000 Professionnel	**Windows 2000 Server**
 Processeurs	Pentium 133 ou plus (supporte 2 processeurs au plus)	Pentium 133 ou plus (supporte 4 processeurs au plus)
 Mémoire vive	32Mo minimum 64Mo recommandés 4Go maximum	64Mo minimum (jusqu'a 5 clients) 128Mo recommandés 4Go maximum
 Disque dur	Disque de 2Go avec au moins 650Mo d'espace libre	Disque de 2Go avec au moins 1Go d'espace libre

Avant d'installer Windows 2000, il faut vérifier que l'ensemble du matériel utilisé figure dans la Hardware Compatibility List (HCL) disponible sur *www.microsoft.com/hcl*.

2 Installation de Windows 2000

Elle se déroule en quatre étapes:

i. Préparation des disques et copie les fichiers nécessaires (mode texte). Un redémarrage a nécessairement lieu à la fin de cette étape.

ii. Assistant d'installation (mode graphique) : saisie d'informations additionnelles telles la clé du produit, le nom de l'organisation, le mot de passe administrateur, les paramètres régionaux, ...

iii. Installation du réseau : détection des cartes réseaux, installation des composants réseau (client pour les réseaux Microsoft, partage de fichiers et d'imprimantes) et installation du protocole TCP/IP (les autres protocoles peuvent être installés par la suite). On a aussi la proposition de jonction à un domaine ou à un groupe de travail. A la suite de ces choix, les composants sont configurés, des fichiers additionnels sont copiés et le système redémarre.

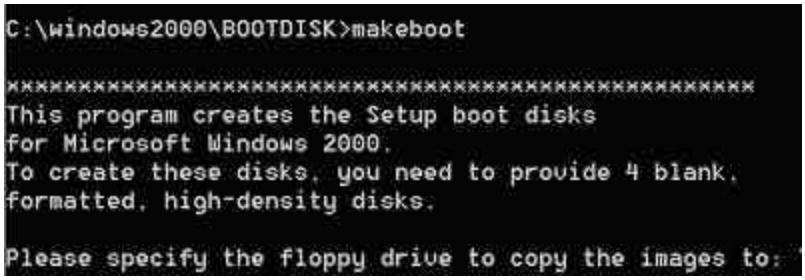
iv. Fin de l'installation : Mise en place du menu Démarrer, enregistrement des composants, sauvegarde de la configuration, suppression des fichiers temporaires et dernier redémarrage.

a) Installation depuis un CD-ROM

L'installation peut se faire directement a partir du CD-ROM, en bootant sur ce dernier.

Lorsqu'il n'est pas possible de booter depuis le CDROM, on a recours aux deux autres méthodes suivantes :

?? Grâce aux disquettes d'installations Windows 2000 : Pour créer les disquettes, il faut exécuter makeboot (on peut préciser le lecteur : makeboot a:) depuis le répertoire \i386\bootdisk sur le CD ROM d'installation. Cela crée un jeu de quatre disquettes.



?? Avec une disquette de démarrage Windows 98 (avec le support du CD-ROM) : on exécute winnt.exe depuis le répertoire i386 sur le CD.

b) Installation via le réseau

Ce type d'installation requiert la mise en place d'un serveur de fichiers avec un partage contenant les fichiers d'installation de Windows 2000 Professionnel.

Les clients pourront lancer l'installation via une disquette de démarrage et un client réseau (il faudra alors exécuter winnt.exe) ou directement a partir de Windows (9x, Me, NT 3.51/4) s'il s'agit d'une mise à jour (lancer winnt32.exe).

Les postes clients nécessitent environ 685Mo d'espace disque libre pour les fichiers du système ainsi que 100 à 200Mo pour la copie des fichiers temporaires liés a la première phase de l'installation.

Commutateurs pour *winnt.exe* (en ligne de commande) :

/a	Active les options d'accessibilité
/e[:command]	Spécifie une commande à exécuter à la dernière étape de l'installation
/r[:folder]	Spécifie un dossier supplémentaire à installer. Ce dossier n'est pas supprimé après l'installation
/rx[:folder	Spécifie un dossier optionnel à copier. Ce dossier est supprimé après l'installation
/s[:sourcepath]	Spécifie la source des fichiers d'installation (locale ou réseau)
/t[:tempdrive]	Spécifie le chemin des fichiers temporaires
/u[:answer file]	Spécifie le chemin du fichier réponse (nécessite /s)
/udf:id [,UDF_file]	Spécifie l'ID pour la personnalisation d'un fichier de réponses avec un fichier UDF (Uniqueness Database File)

Commutateurs pour *winnt32.exe* (en ligne de commande) :

/checkupgradeonly	Ne lance pas l'installation. Il sert à vérifier la compatibilité du système avec Windows 2000 (génère un rapport)
/copydir:folder_name	Crée des répertoires supplémentaires dans %systemroot% . Conservé après l'installation
/copysource:folder_name	Crée des répertoires supplémentaires dans %systemroot% .Détruits après l'installation
/cmd: command_line	Exécute une commande avant la dernière étape de l'installation
/cmdcons	Installe la console de récupération
/debug[level] [:file_name]	Crée un journal de déboguage contenant les informations suivant les niveaux de gravité suivants : 0=erreurs graves, 1=erreurs standard, 2=avertissements 3= informations, 4= informations détaillées pour deboguage. Chaque niveau inclue les niveaux qui le suivent (le niveau 0 inclue tous les autres,...)

/m:folder_name	Force le processus d'installation à rechercher les fichiers dans un répertoire donné en premier lieu. S'il ne les trouve pas, il poursuit dans le chemin par défaut
/makelocalsource	Force la copie des fichiers source pour permettre de poursuivre l'installation si ceux-ci deviennent indisponibles.
/nodownload	Utilisé pour la mise à jour de Windows 9x. Il force la copie de winnt32.exe et des fichiers rattachés localement afin d'éviter les problèmes de congestion du réseau lors de l'installation.
/noreboot	Empêche le redémarrage après la première étape d'installation
/s:source_path	Spécifie l'emplacement des sources. Plusieurs chemins peuvent être utilisés simultanément.(mais le premier chemin doit être valide)
/syspart:drive_letter	Copie tous les fichiers de démarrage sur le disque et marque le disque comme actif. On peut déplacer le disque vers un autre ordinateur et celui-ci va redémarrer automatiquement au second stade de l'installation. (nécessite le switch /tempdrive)
/tempdrive:drive_letter	L'installation utilise le chemin spécifié pour les fichiers temporaires. Utile quand l'espace disque est limité
/unattend: [number] [:answer_file]	Spécifie le chemin du fichier réponse (nécessite /s)

c) Installation a distance avec les services RIS

La fonction d'installation à distance de Windows 2000 permet d'utiliser les services RIS (Remote Installation Service) pour effectuer une installation automatisée de Windows 2000 Professionnel.
Il faut prendre en considération les points suivants :

- Actuellement, seul Windows 2000 Professionnel peut être installé via ce procédé
- Cette fonctionnalité nécessite un serveur RIS sur le réseau. Les services suivants doivent aussi être présents sur le réseau :Active Directory (pour localiser les serveurs RIS), DNS (requis pour Active Directory), DHCP (pour que le client puisse obtenir une adresse IP).
- RIS doit être installé sur un disque partagé, différent de celui qui contient Windows 2000 Server, et doit être formaté en NTFS.
- Le volume partagé doit être assez grand pour supporter RIS et les différentes images disques Windows 2000 Professionnel.
- Les images RIPRep peuvent avoir des applications pré-installées. Les identifiants uniques tels que les SID sont supprimés au moment où les images RIPRep sont générées.
- L'installation utilise des fichiers .SIF, variante des fichiers unattend.txt.

Une fois que RIS est installé sur le serveur et qu'il est fonctionnel, utilisez le Remote Boot Disk Generator (RBFG.EXE) afin de créer des disquettes d'installation bootables. Ces disquettes ne supportent que les cartes réseau PCI. Cependant, si la machine dispose d'une carte réseau PXE ou s'il s'agit d'un NetPC, les disquettes de démarrage ne sont pas nécessaires.

Les ordinateurs client peuvent être constitués de matériel hétérogène à condition que les composant utilisent la même HAL (Hardware Abstraction Layer).

Utilisez *riprep.exe* pour démarrer l'Assistant RIS.

3 Travailler avec Sysdiff

Sysdiff est employé pour installer des applications, en utilisation conjointe avec un fichier de réponses **Unattend.txt**. Sysdiff vous permet de « prendre une photo » de l'état original de votre machine, d'installer des

applications, et de répertorié les changements intervenus dans un seul fichier qui peut être ensuite appliqué sur d'autres machines.

Faites votre installation de base dans un premier temps. Ensuite, prenez une photo avant d'installer des applications. La syntaxe est la suivante : ***sysdiff /snap fichier_photo***

Installez les applications désirées sur la machine. Ensuite gênerez le fichier contenant les différences grâce à : ***sysdiff /diff fichier_photo fichier_différences***

Maintenant, vous pouvez appliquer ces différences sur d'autres machines de destination avec la commande: ***sysdiff /apply \\setupserver\w2k\fichier_differences.***

4 Utilitaire de préparation de système Sysprep

Il s'agit d'un outil simplifiant le clonage de machines. Il permet le retrait des éléments spécifiques au clone (nom de la machine, numéro de série,...). Cela supprime notamment le problème de SID dupliqués de Windows NT 4.

Sysprep se trouve dans le package **DEPLOY.CAB** localisé dans le dossier *support**tools* du CD-ROM de Windows 2000.

Sysprep lance un assistant lors du premier redémarrage de la machine qui va permettre de configurer les informations spécifiques à l'ordinateur.

Il est possible de créer un fichier **SYSPREP.INF** en utilisant Setup Manager, qui se trouve lui aussi dans le dossier *support**tools* du CD ROM d'installation de Windows 2000.

5 Mise à jour depuis une version précédente

Lancez ***winnt32.exe*** depuis le répertoire i386 du CD-ROM de Windows 2000 pour faire une mise à jour depuis une version précédente de Windows.

Windows 2000 va mettre à jour et préserver les paramètres des systèmes d'exploitation suivants : Windows 95, 98 et Me (toutes les versions), Windows NT Workstation 3.51 et 4.0 .

Windows NT 3.1 ou 3.5 doivent subir une mise à jour intermédiaire en NT 3.51 ou NT 4.0 avant de pouvoir migrer en Windows 2000.

A cause des différences de registre entre Windows 9x et Windows 2000, des packs (dlls) de mise à jour peuvent être nécessaires, le logiciel d'installation les recherche dans le dossier \i386\Win9xmig sur le CD-Rom de Windows 2000.

Pour vérifier si une mise à jour peut s'opérer dans de bonnes conditions, lancez ***winnt32 /checkupgradeonly***. Cela va générer un rapport qui va souligner les éléments potentiellement problématiques pour votre mise à jour. Vous pouvez aussi utiliser l'outil ***chkupgrd.exe*** disponible à partir du site Microsoft (www.microsoft.com/windows2000).

✍ Si Windows 98 et Windows NT sont installés sur la même machine, la mise à jour ne peut pas s'effectuer à partir de Windows 98. Elle doit être faite depuis Windows NT.

6 Fichiers et journaux de l'installation

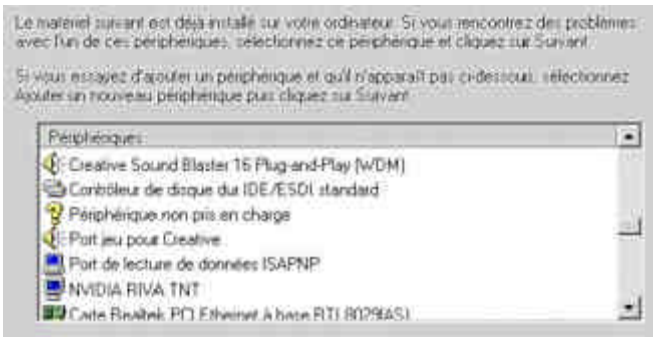
Le programme d'installation crée les journaux suivants :

Setupact.log (journal des actions)	Il enregistre les actions de modification dans un ordre chronologique. Il inclue les fichiers copiés et les entrées du Registre, ainsi que les entrées faites dans le fichier error log.

Setuperr.log (journal des erreurs)	Il enregistre toutes les erreurs qui arrivent durant les installations en incluant le niveau d'importance des erreurs.
Comsetup.log	Il est utilisé par le Optional Component Manager et les composants COM+.
Setupapi.log	Il enregistre une ou plusieurs entrées à chaque fois qu'une ligne d'un fichier .INF est exécutée (lors de la mise en place des fichiers .INF).
Netsetup.log	Il enregistre les activités de jonction à un domaine ou un groupe de travail.
Mmdet.log	Il enregistre la détection des périphériques multimédias ainsi que certaines propriétés de ces derniers, telles que les adresses d'entrée sorties.

Module 2
Configuration de l'environnement de Windows 2000

1 Configuration des périphériques



Windows 2000 supporte pleinement le Plug-and-Play. Ainsi, le système détecte immédiatement un nouveau périphérique lorsque celui-ci est connecté. S'il le peut, Windows 2000 installera lui même les pilotes correspondants.

Utilisez la Boite de Dialogue « Informations Système » (clic droit sur Poste de Travail\Gérer) pour afficher les informations sur la configuration de votre ordinateur . Vous pourrez, par l'intermédiaire de l'option « Gestionnaire de périphérique », afficher des informations utiles sur les Conflits/Partages, DMA, IRQ, E/S ou encore la mémoire.

Le matériel peut être ajouté ou retiré en utilisant l'icône « Ajouter/Suppression de Matériel » du Panneau de configuration.

L'ensemble des périphériques de votre ordinateur peut être configuré via le Gestionnaire de périphériques (accessible via l'outil d'administration Gestion de l'ordinateur).

En cas de problème, vous pouvez utiliser l'outil de résolution de problèmes disponible dans l'onglet Général des propriétés du périphérique en question.

2 Signature des pilotes

a) Configurer la signature des pilotes

Elle s'effectue via la fenêtre Système du panneau de configuration, dans l'onglet Matériel.

En cliquant sur 'Signature du pilote' on a les options suivantes:

Ignorer (Ignore) Installe n'importe quel pilote, peu importe qu'il soit signé ou non.

Avertir (Warn) affiche un message d'avertissement avant d'installer un pilote sans signature

Interdire (Block) Empêche l'installation d'un fichier non signé

La case à cocher Définir les paramètres en tant que paramètres par défaut n'est disponible que pour les Administrateurs.

b) Vérification de signature (sigverif.exe)

L'utilitaire sigverif.exe a pour but de vérifier que les fichiers système d'origine installés par Windows n'ont pas été remplacés par des versions non signées. Il peut aussi vérifier les fichiers non-système si besoin est. Les résultats seront enregistrés dans le fichier Sigverif.txt.

c) Utiliser le vérificateur de fichiers système (sfc.exe)

Cet utilitaire vérifie les fichiers système protégés. Il peut être lancé avec plusieurs options :

/scannow	Vérifie immédiatement tous les fichiers systèmes protégés
/scanonce	Vérifie tous les fichiers systèmes protégés au prochain redémarrage
/scanboot	Vérifie tous les fichiers systèmes protégés à chaque démarrage
/cancel	Annule toutes les vérifications en attente
/quiet	Remplace les fichiers incorrects sans demander de confirmation
/enable	Active la protection des fichiers de Windows par défaut
/purgecache	Purge les fichiers de cache et demande uen vérification immédiate
/cachesize=x	Fixe la taille du cache fichiers

3 Mise à jour des pilotes

Les pilotes sont mis à jour via le Gestionnaire de périphériques. Sélectionnez le pilote, faites un clic-droit puis Propriétés et sélectionnez Mettre à jour le pilote.

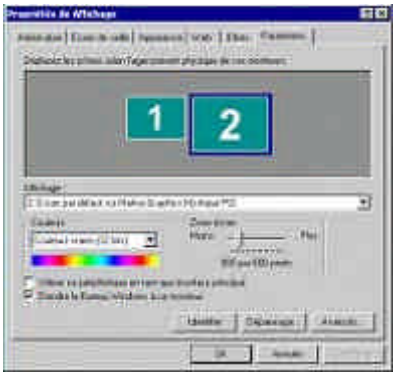
✍ Il est conseillé d'utiliser des pilotes signés afin de garantir une stabilité optimum.

Le fichier ***driver.cab*** qui se trouve sur le CD ROM de Windows 2000 contient tous les pilotes livrés avec le système d'exploitation. Pour toute mise à jour de pilote, Windows 2000 vérifiera ici s'il dispose ou non d'une version plus récente. Ce chemin peut être modifié via la clé :

HKLM\Software\Windows\CurrentVersion\Setup\DriverCachePath

✍ Le vérificateur de pilote peut être utilisé pour retrouver les pilotes non-signés sur un système. Lancez pour cela ***verifier.exe*** en ligne de commande.

4 Configuration de l'affichage



Les périphériques d'affichage sont installés, retirés ou mis à jour (pilote) au niveau de "Carte graphique" dans le Gestionnaire de Périphériques. Ils sont configurés via l'onglet Paramètres de la fenêtre Propriétés de l'Affichage (taille de la zone d'écran, profondeur des couleurs, etc.).

L'utilisateur peut changer l'apparence de son bureau, comme par exemple l'arrière plan ou l'économiseur d'écran.
Windows 2000 propose un support multi-moniteurs nécessitant des cartes graphiques PCI ou AGP pour fonctionner. Ainsi, il vous est possible d'étendre votre environnement de travail sur 10 moniteurs dont vous choisirez la disposition grâce à l'onglet Paramètres de la fenêtre Propriétés de l'Affichage.

Une fois le moniteur supplémentaire branché et ses pilotes installés, il vous suffit de le sélectionner dans cet onglet et de cocher la case Etendre le Bureau Windows à ce moniteur. Vous pouvez l'aligner horizontalement ou verticalement par rapport a votre écran principal actuel en déplaçant tout simplement son icône. Vous pouvez aussi définir ce nouveau moniteur comme votre moniteur principal en cochant la case correspondante.

5 Le support du fax

L'applet Fax apparaît dans le panneau de configuration uniquement lorsqu'un périphérique de fax (modem) est installé.

L'onglet Options Avancées permet de configurer l'émission/réception de fax, le nombre de tentatives d'émission, le chemin de stockage des fax reçus et envoyés, les permissions de sécurité des utilisateurs, etc

Si cet onglet n'est pas accessible, il faut se déloguer et se reloguer en tant qu'Administrateur.

✍ L'imprimante Fax dans le dossier des Imprimantes ne peut pas être partagée.

6 Les services d'accessibilité

Touches rémanentes (StickyKeys) : elles permettent de faire des combinaisons de touches (par exemple CTRL-ALT-SUPPR) en ne pressant qu'une seule touche à la fois.

Touches filtres (FilterKeys) : permettent d'ignorer les répétitions brèves des touches.

Son texte (SoundSentry) : affiche un avertissement visuel lorsque votre ordinateur émet un son (pour les malentendants).

Sons visuels (ShowSounds) : permet de faire clignoter une zone de l'écran a chaque fois qu'un son système est émis.

Touche souris (MouseKeys) : vous permet de contrôler la souris grâce au pavé numérique.

Loupe (Magnifier) : agrandit une partie du bureau (pour les malvoyants).

Narrateur (Narrator) : vous lit les menus d'option, grâce à la synthèse vocale (pour les malvoyants).

7 Prise en charge des processeurs multiples

Windows 2000 Professionnel supporte an maximum 2 processeurs, Windows 2000 Server en supporte 4, Advanced Server peut en gérer 8 et Datacenter Server peut prendre en charge jusqu'à 32 processeurs.

Pour passer d'un système mono-processeur à un système multiprocesseurs, il faut mettre à jour votre pilote Windows vers un pilote compatible MPS (Multi-Processor Specification) via le Gestionnaire de périphériques.

8 Installer et gérer des périphériques réseau

Les périphériques réseau sont installés via Ajout/Suppression de matériel dans le Panneau de configuration.
Chaque carte réseau possède une icône qui apparaît automatiquement dans «Connexions réseau et accès à distance ». Faites un clic-droit sur cette icône pour définir ou modifier ses propriétés, installer des protocoles, changer des adresses, etc...
Pour modifier l'ordre de liaison des protocoles et des fournisseurs, utilisez le menu Paramètres avancés dans le menu Avancé de « Connexions réseau et accès à distance ».

9 Processus de démarrage Windows 2000

Le processus de démarrage de Windows 2000 est similaire à celui de Windows NT 4.
Les fichiers mis en oeuvre restent identiques quelle que soit la version :

Ntldr	Charge l'OS.
Boot.ini	Construit le menu de sélection.
Bootsect.dos	Chargé par Ntldr en vue d'une utilisation alternée avec un autre OS.
Ntdetect.com	Recherche le matériel disponible.
Ntbootdd.sys	Pour l'amorçage à partir d'un disque SCSI dont le bios du contrôleur est désactivé.
Ntoskrnl.exe	Noyau NT (system32).
System	Paramètres de configuration (system32\configuration).

Hal.dll	Couche HAL. Rend Ntoskrnl indépendant de la plate-forme sur laquelle il va fonctionner.

Etape 1 - La séquence POST - Power On Self Test

Test de la mise sous tension, de la quantité de mémoire, des composants matériels.
Chargement en mémoire de l'enregistrement d'amorçage principal (MBR).
Analyse de la table de partition.
Chargement et initialisation de Ntldr (bootstrap loader).

Etape 2 - Sélection du système d'exploitation

Ntldr fait passer le processeur du mode réel au mode mémoire linéaire 32 bits.
Ntldr démarre les pilotes de système de fichiers appropriés (FAT ou NTFS).
Ntldr lit Boot.ini et affiche les sélections.
Ntldr charge l'OS sélectionné.
Si Windows 2000 est sélectionné, Ntldr charge Ntdetect.com (sinon, Bootsect.dos).
Ntldr charge Ntoskrnl.exe, Hal.dll et la ruche "system".

Etape 3 - Chargement du noyau (Kernel)

Cette phase commence par le chargement de ntoskrnl.exe et du fichier hall.dll. NTLDR va lire la ruche SYSTEM du registre et la mettre en mémoire puis va sélectionner la configuration matérielle et le control set qui seront utilisés pour ce démarrage. Si vous avez plus d'un profil matériel, vous pourrez faire la sélection à ce niveau. NTLDR va aussi charger tous les pilotes de périphériques dont la valeur de démarrage (dans le Registre : HKEY_LOCAL_MACHINE\SYSTEM \CurrentControlSet\Services) est 0x0.
Si vous ajoutez le switch /SOS dans le boot.ini, il vous sera possible de voir les pilotes chargés.

Etape 4 – Initialisation du noyau

Dès l'initialisation de ntoskrnl.exe, ce dernier crée le Clone control set en copiant le Control Set courant. Il va aussi créer la ruche HARDWARE dans le Registre en utilisant les informations collectées précédemment par ntdetect.com. Ntoskrnl.exe va ensuite initialiser les pilotes de périphériques chargés précédemment, puis va scruter le registre pour les pilotes de périphériques qui ont une valeur de chargement de 0x1.

Etape 5 - Chargement des Services

Cette étape commence avec le chargement du processus Session Manager (smss.exe). Il va lancer les programmes présents dans l'entrée BootExecute du Registre ainsi que les sous-systèmes requis. Le sous-système Win32 va ensuite charger Winlogon.exe qui va lancer la LSA : Local Security Administration (Lsass.exe). La fenêtre Winlogon sera alors visible.
Le contrôleur de services (screg.exe) va ensuite scruter le Registre à la recherche de services qui ont une valeur de démarrage de 0x2 et va les charger. Les services doivent être lancés dans une certain ordre, en fonction de leurs dépendances vis à vis d'autres services.
Les services marqués en 0x3 sont démarrés manuellement. Les services en 0x4 sont désactivés.

10 Fonctionnement des chemins ARC

Prenons par exemple la ligne suivante, extraite d'un fichier boot.ini :

multi(0)disk(0)rdisk(1)partition(2)

Multi : correspond au contrôleur (la numérotation commence à 0).
Disk : type de disque (la numérotation commence à 0).
Rdisk : quel disque (la numérotation commence à 0).
Partition : quelle partition (la numérotation commence à 1).

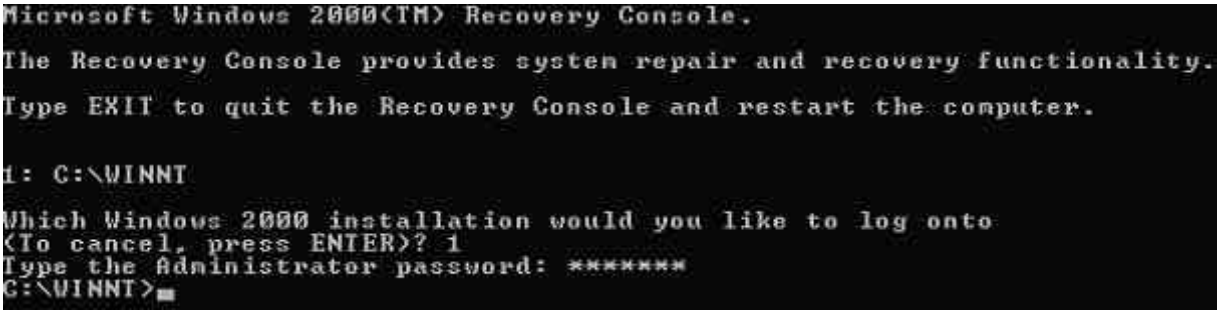
Lorsque l' on a un disque SCSI où le bios n'est pas activé, on a alors : scsi(0)disk(0)rdisk(0)partition(1).
En revanche, si le Bios est activé, multi remplacera scsi.
Disk est utilisé pour la numérotation uniquement lorsque l'on a un disque SCSI.

Les paramètres de BOOT.INI

/basevideo	Force le système a utiliser le mode VGA 640x480
/fastdetect=[comx,y,z]	Désactive la détection de la souris en spécifiant son port
/maxmem :n	Limite la quantité de mémoire disponible à n Mo
/noguiboot	N'affiche pas l'image Windows lors du démarrage
/sos	Affiche les noms des pilotes lors du démarrage
/bootlog	Active l'enregistrement des événements de démarrage
/safeboot	Minimal - démarrage en mode sans échec
/safeboot	Minimal(alternateshell) - mode sans échec avec console DOS
/safeboot	Network - mode sans échec avec prise en charge réseau

11 Utilisation de la console de récupération

L'installation de la console de récupération se fait via la commande winnt32 /cmdcons



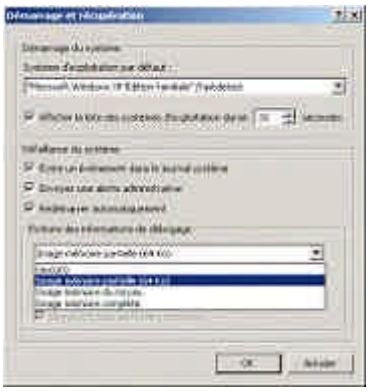
Vous devez vous connecter en tant qu'Administrateur pour utiliser la console de récupération.

Les commandes suivantes sont disponibles :

attrib	Permet de changer les attributs d'un fichier ou d'un dossier
batch	Permet d'exécuter les commandes spécifiées dans un fichier texte
chdir	Permet d'afficher le dossier courant et de naviguer dans l'arborescence
chkdsk	Permet de vérifier le disque et présente un rapport
cls	Permet d'effacer l'écran
copy	Permet de copier un fichier vers un autre emplacement
delete	Permet de supprimer un ou plusieurs fichiers
dir	Permet d'afficher une liste de fichiers et dossiers
disable	Permet de désactiver un service système ou un driver
diskpart	Permet de gérer les partitions sur les disques
enable	Permet de démarrer un service ou un driver
exit	Permet de quitter la console de récupération
expand	Permet d'extraire un fichier compressé
fixboot	Permet d'écrire un nouveau secteur d'amorce sur la partition système
fixmbr	Permet de réparer le MBR du secteur de boot de la partition
format	Permet de formater un disque
help	Affiche les commandes disponibles
listsvc	Permet d'obtenir la liste des services et pilotes disponibles sur l'ordinateur
logon	Permet de se connecter à une installation Windows 2000
map	Affiche les mappings de lecteurs
mkdir	Permet de créer des dossiers

more	Permet d'afficher le contenu d'un fichier texte
type	Permet aussi d'afficher le contenu d'un fichier texte
rename	Permet de renommer un fichier unique
rmdir	Permet de supprimer un dossier
set	Affiche et positionne des variables d'environnement
systemroot	Positionne le dossier courant sur le dossier racine du système (ex: c:\WINNT)

12 Les options de démarrage et paramètres de récupération



On y accède via le Panneau de Configuration, icône Système, onglet Avancé et enfin Démarrage et Récupération.

Les dumps (photo instantanée du contenu de la mémoire) sont sauvés en memory.dmp. Une version allégée de ce fichier, pouvant faire 64Ko, est enregistrée dans %systemroot%\minidump.
On utilise dumpchk.exe pour examiner le contenu de memory.dmp

Le fichier de pagination doit se trouver sur la partition système pour que le vidage mémoire puisse s'effectuer. Il doit aussi faire 12 Mo de plus que la quantité de RAM installée.

13 La disquette de réparation d'urgence

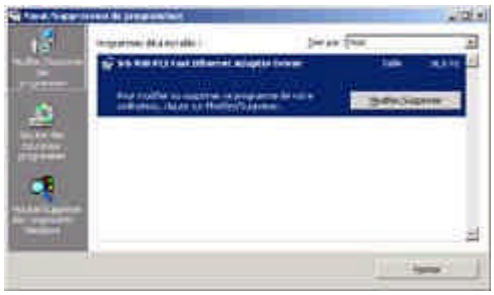
RDISK n'existe plus sous Windows 2000. Vos disquettes de réparation d'urgence se font exclusivement avec l'utilitaire ntbackup.exe.

La disquette de réparation d'urgence devient maintenant une disquette d'amorçage.

Pour créer en créer une, lancez ntbackup.exe, choisissez Disquette de Réparation d'urgence et insérez une disquette dans votre lecteur.
Vous aurez aussi la possibilité de copier le registre vers %systemroot%\repair\regback avec ntbackup.

Votre Disquette de Réparation d'urgence contient entre autres les fichiers suivants : autoexec.nt, config.nt et setup.log.

14 Gestion des applications



Via Ajout/suppression de programmes, qui se trouve dans Panneau de configuration, il vous est possible de gérer facilement les applications de votre ordinateur. Ce programme vous permet d'installer, de désinstaller, de modifier et de réparer toute application certifiée Windows 2000. Dans le cas d'une installation, la source peut se trouver soit sur CD ROM, sur disquette, sur un réseau ou sur Internet.

Windows 2000 vous propose de classer l'affichage des applications installées sur votre système soit par nom, par taille, par fréquence d'utilisation ou par date de dernière utilisation.

Vous pouvez aussi publier les applications dans Active Directory en passant par la console Stratégie de Groupe. Pour cela, les applications devront inclure des fichiers d'extension .MSI.

15 Utilisation de l'installateur de Packages Microsoft

Les packages Microsoft sont reconnaissables par leur extension en .MSI.
L'installation d'un package .MSI fait appel au service Windows Installer intégré a Windows 2000.

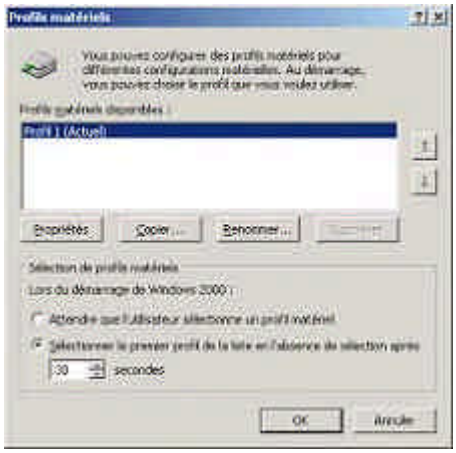
Vous pouvez assigner ou publier des packages logiciels.
La publication d'une application place un raccourci dans le menu Démarrer qui installe l'application lors de sa première exécution. L'assignation, quant à elle, installe le logiciel à la prochaine connexion de l'utilisateur.

Afin de pouvoir déployer un package logiciel, une stratégie de groupe doit être créée et appliquée aux utilisateur nécessitant l'application.
Le fichiers .MSI du package devra se situer sur un partage réseau accessible par les clients.

Les programmes non-MSI peuvent être publiés à l'aide de fichiers .ZAP, ou transformées en packages .MSI a l'aide de l'utilitaire WinInstall (Veritas Software).
Dans le cas d'une publication à l'aide de fichiers .ZAP, les applications ne peuvent pas tirer partie des possibilités offertes aux packages .MSI telles que les privilèges d'installation élevés, l'annulation d'installation infructueuse, l'installation à la première utilisation d'un logiciel, etc

16 Profils matériels

Comme sous Windows NT 4, il est possible de créer des profils matériels.

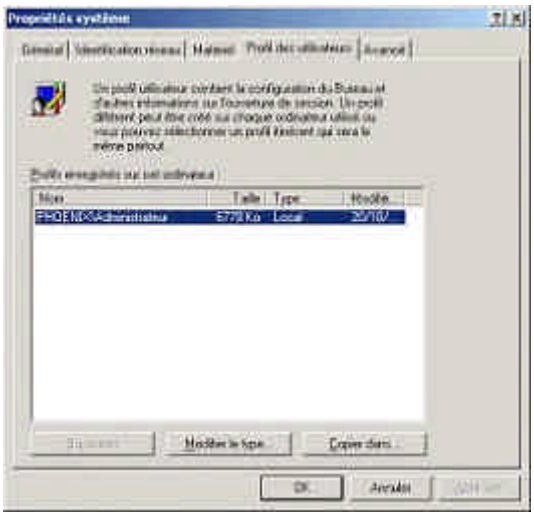


Il sont utilisés pour enregistrer les différents éléments de configuration afin de répondre aux différents besoins des utilisateurs. Ils sont souvent employés pour les ordinateurs portables, afin de définir si un ordinateur est connecté à sa station d'accueil ou non. S'il est connecté à sa station, il y a de fortes chances pour que cette dernière soit déjà équipée d'une carte réseau, auquel cas, il faudra désactiver la carte réseau de l'ordinateur portable.
L'utilisateur choisi le profil désiré par le biais d'un menu affiché au démarrage de Windows 2000.

Les profils sont créés par le Panneau de Configuration > Système > Matériel > Profil matériel . Les périphériques sont activés ou non suivant le profil par l'intermédiaire du Gestionnaire de Périphériques.

17 Profils utilisateurs

C'est une collection de données et de répertoires qui contiennent l'environnement de travail de l'utilisateur, les réglages des applications ainsi que des données personnelles relatives à l'utilisateur.



Quand un utilisateur ouvre une session sur une machine sous Windows 2000 Professionnel, il recevra toujours son environnement personnalisé et ses connexions de travail indépendamment du nombre de personnes qui utilisent cette machine.

Un utilisateur peut changer son profil en modifiant les réglages de son bureau – quand il ferme sa session, Windows 2000 incorpore les changements à son profil.

Rendre le profil obligatoire annule tous les changements effectués par l'utilisateur pendant la session. A la prochaine ouverture de session, il récupèrera son profil initial.

Les profils utilisateurs sont stockés dans le dossier %systemdrive%\Documents and Settings\%username%.

✍ Dans le cas d'une migration à partir de Windows NT 4, les profils seront stockés dans le répertoire %systemroot%\profiles\%username%.

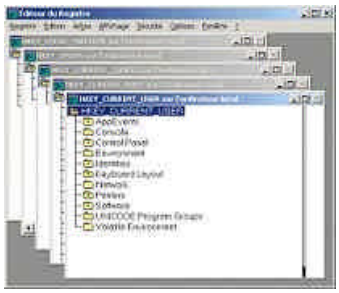
Les profils itinérants sont utilisés dans les domaines Windows 2000 pour les utilisateurs qui emploient différentes machines mais qui requièrent un environnement de travail persistant.

18 Support multi-langages et multi-locations

Les modifications de ces options se font par l'intermédiaire de l'icône Options Régionales du Panneau de Configuration. Vous pouvez par ce biais ajouter toutes les langues dont votre système a besoin pour votre travail.

Dans l'onglet Général de la fenêtre Options Régionales, vérifiez dans la partie « Votre système est configuré pour prendre en charge la lecture et l'écriture des documents en plusieurs langues » quelles sont les langues actuellement supportées par votre système ainsi que la langue actuelle qui se trouve dans la partie « Paramètres de l'utilisateur actuel ».

19 Le registre de Windows 2000



Cette base de données enregistre la configuration de Windows 2000 pour tous les logiciels installés, le matériel et l'architecture hiérarchique des utilisateurs. Il y a plusieurs sous-arbres principaux :

HKEY_CLASSES_ROOT	Contient les données de configuration logicielle, les associations de fichiers et les données OLE (object linking and embedding).
HKEY_CURRENT_CONFIG	Contient les données sur le profil matériel actuel.
HKEY_CURRENT_USER	Contient les données sur l'utilisateur actuel, ces données sont extraites de HKEY_USERS et des informations additionnelles sont ajoutées lors de l'authentification par Windows.
HKEY_LOCAL_MACHINE	Contient toutes les données relatives au matériel, aux logiciels, aux drivers de périphériques et aux informations de démarrage de l'ordinateur local. Ces informations sont identiques quelque soit l'utilisateur.
HKEY_USERS	Contient les données sur l'identité de l'utilisateur, son environnement et ses différents réglages, etc…

L'éditeur de base de Registre (regedt32.exe) dispose d'un mode lecture-seule, d'un menu de sécurité et supporte les données de type REG_EXPAND_SZ et REG_MULTI_SZ. L'application regedit.exe (un autre éditeur de base de registre installé par Windows 2000) ne possède pas ces caractéristiques mais il permet de faire des recherches sur plusieurs sous-arbres en même temps, tandis que regedt32.exe ne le permet pas. L'éditeur de base de Registre enregistre automatiquement tous les changements qui sont faits.

20 Support des ordinateurs mobiles

Windows 2000 dispose d'une panoplie d'options particulièrement adaptées aux ordinateurs mobiles. Parmi celles-ci, on a :

le support des interfaces PCMCIA (PC Card), USB ports, IEEE 1394 (FireWire), et infrarouge.
le support de la norme Advanced Power Management (APM) et Advanced Configuration and Power Interface (ACPI).
Un mode « hibernation » intégré (arrêt complet du système et vidage du contenu de la mémoire dans un fichier).

Le support des fichiers hors connexion

a) Utiliser les fichiers Hors Connexion

Les fichiers Hors Connexion remplacent le Porte-Document et fonctionnent de manière similaire à l'option « Visualiser Hors-Connexion » d'Internet Explorer 5.

Partagez un dossier et activer son cache afin de le rendre disponible hors connexion.

Il existe trois types de mise en cache :

- **Cache manuel pour les documents** : réglage par défaut. Les utilisateurs doivent spécifier quels documents ils souhaitent rendre disponibles hors connexion.

- **Cache automatique pour les documents** : tous les fichiers ouverts par un utilisateur sont mis en cache sur son disque dur pour une utilisation hors connexion – les versions anciennes du document sur le disque sont automatiquement remplacées par des versions plus récentes du partage quand elles existent.

- **Cache automatique pour les programmes** : même principe que le cache automatique de documents mais appliqué aux programmes.

Lorsque vous synchronisez, si vous avez édité un fichier hors connexion et qu'un autre utilisateur a fait de même, alors, il vous sera demandé si vous souhaitez:
Garder et renommer votre exemplaire
Écraser votre exemplaire avec la version disponible sur le réseau
Écraser la version disponible sur le réseau et perdre les modifications de l'autre utilisateur

L'utilitaire de Synchronisation, vous permet de spécifier les fichiers qui seront synchronisées, le type de connexions employée pour cette synchronisation (pour empêcher par exemple une synchronisation lorsque l'on est connecté au réseau à distance via un modem) et le moment où cette synchronisation est effectuée (lors d'une connexion, d'une déconnexion, lorsque l'ordinateur est en veille,...).

Module 3
Connexion d'ordinateurs clients Windows 2000 a des réseaux

1 Gestion des protocoles

Windows 2000 installe automatiquement la suite de protocoles TCP/IP. Les autres doivent être installés manuellement.

a) Protocole TCP/IP

C'est une suite de protocoles standardisée. Il est routable et est utilisable sur de nombreuses topologies de réseau. C'est le protocole qui est à la base d'Internet.

Il est installé par défaut dans Windows 2000.

Il peut être utilisé pour connecter des systèmes hétérogènes.

Il utilise l'interface Microsoft Windows Sockets (Winsock)

Les adresses IP peuvent être entrées manuellement ou assignées automatiquement par un serveur DHCP.

DNS est utilisé pour résoudre les noms d'ordinateur (noms d'hôtes) en adresses IP.
WINS est utilisé pour résoudre les noms NetBIOS en adresses IP.

Masque de sous-réseau : c'est une valeur qui est utilisée pour distinguer la partie identificateur de réseau et la partie identificateur d'hôte d'une adresse IP.

Passerelle par défaut : adresse IP utilisée pour indiquer la machine (le plus souvent un routeur) capable de transmettre les paquets a une machine cible qui ne se trouve pas sur le même réseau ou sous réseau que la machine source.

b) Configuration de TCP/IP

Configuration manuelle de TCP/IP

La configuration manuelle des paramètres TCP/IP va nous permettre de spécifier l'adresse IP, le masque de sous-réseau ainsi que la passerelle par défaut. Il nous est aussi nécessaire d'indiquer l'adresse d'au moins un serveur DNS. Windows 2000 utilisant intensivement ce service, il est important de bien le configurer.

L'écran de configuration des paramètres TCP/IP est accessible à partir de "Connexion Réseau et accès à distance", en affichant les propriétés (clic-droit) de la connexion.

Configuration dynamique

La configuration dynamique des propriétés TCP/IP va utiliser DHCP pour l'attribution des paramètres et options TCP/IP. Les mécanismes sont identiques à Windows NT 4.

Il existe cependant une nouveauté intéressante : l'adressage IP privé automatique (APIPA – Automatic Private IP Addresing).
Windows 98 et Windows 2000 supportent cette nouvelle fonctionnalité : lorsque l'option « Obtenir automatiquement une adresse IP » est activé, mais que le client est incapable de contacter un serveur DHCP ou d'obtenir une adresse de ce dernier, l'adressage automatique prend le relais:

L'adresse IP générée est de type : 169.254.x.y (où x.y est l'identifiant de l'ordinateur). Le masque de sous réseau est de 16-bits (255.255.0.0).
L'ordinateur diffuse cette adresse sur le sous réseau local.
Si aucun autre ordinateur ne répond à cette adresse, alors l'ordinateur la garde.
Quand l'attribution automatique d'adresse IP privée est utilisée, seuls les ordinateurs situés sur le même réseau local et utilisant le même type d'adresse (169.254.x.y) et le même masque de sous réseau pourront communiquer ensemble.

✍ La plage d'adresses 169.254.0.0 - 169.254.255.255 a été réservée pour cette utilisation par l'IANA (Internet Assigned Numbers Authority).

2 Outils de dépannage en ligne de Commande

Ipconfig	Affiche la configuration TCP/IP actuelle.
Ping	Teste les connexions et vérifie les configurations.
Nbtstat	Affiche les statistiques des connexions utilisant NetBIOS sur TCP/IP.
Netstat	Affiche les statistiques et les connexions pour le protocole TCP/IP.
Tracert	Analyse le chemin emprunté par les paquets jusqu'à un système distant.

a) Procédure de Dépannage

Microsoft recommande l'utilisation de la démarche de dépannage suivante :

Exécuter Ipconfig et vérifier la cohérence des paramètres réseau
faire un **Ping** de 127.0.0.1
faire un **Ping** de l'adresse IP de l'ordinateur local
faire un **Ping** de l'adresse IP de la passerelle
faire un **Ping** de l'adresse IP de l'ordinateur distant

✍ Les problèmes TCP/IP sont souvent causés par des définitions de sous-réseaux incorrects et de mauvaises passerelles.

✍ Si une adresse IP fonctionne mais que le nom d'hôte ne répond pas, vérifiez la configuration DNS.

3 Configuration de NWLink (IPX/SPX) et Netware

NWLink (l'implémentation Microsoft du protocole IPX/SPX) est le protocole utilisé par Windows 2000 pour permettre aux systèmes Netware d'accéder à ses ressources. NWLink est tout ce dont vous avez besoin pour permettre à des clients Windows 2000 de faire fonctionner des applications client/serveur depuis un serveur NetWare. NWLink supporte les Sockets Windows et Netbios.

La seule présence de Netware Link va permettre à un client Netware d'accéder à un serveur Windows 2000, notamment a des applications telles SQL Server par exemple.

On peut facilement installer NWLink sur un serveur Windows 2000 et donc intégrer Windows 2000 dans un environnement Netware. En revanche, NWLink ne suffit pas pour partager des ressources car Windows 2000 utilise SMB, non pris en charge par Netware (qui utilise NCP).

a) Installation de NWLink

L'installation de NWLink se fait à partir des propriétés de la connexion Réseau.

Le type de trame standard pour Netware 3.2 est 802.2. Les versions antérieures utilisaient des trames 802.3
Windows 2000 détermine automatiquement le type de trames. Si plusieurs types sont détectés il prendra 802.2 par défaut.

Le type de trame du protocole NWLink doit correspondre à celui de l'ordinateur avec lequel le système Windows 2000 tente de communiquer. Si le type de trame ne correspond pas, il y aura des problèmes de connexion.
Quand NWLink est configuré pour détecter automatiquement le type de trame, il ne détectera qu'un seul type avec par ordre de préférence : 802.2, 802.3, ETHERNET_II et 802.5 (Token Ring).

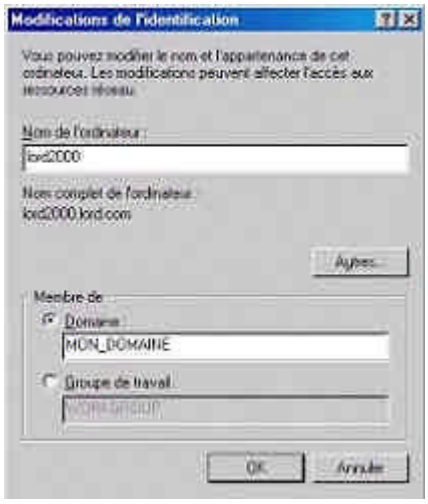
4 Connexion à un réseau Microsoft

Le client réseau Microsoft est installé par défaut lors de la mise en place de Windows 2000. L'installation des services clients Microsoft se fait aussi automatiquement.

a) Ajout de la station ou du serveur au domaine

L'ajout d'une station Windows 2000 Professionnel ou d'un serveur membre à un domaine Windows 2000 se fait via l'identification réseau. Le principe reste identique à la version 4 : un compte machine va être créé dans Active Directory pour l'ordinateur qui intègre le domaine.

Vous pouvez créer ce compte machine automatiquement lors de l'ajout sur le domaine. Vous pouvez aussi le créer dans un premier temps sur le serveur (dans Active Directory) puis ajouter la machine sur le domaine. Les administrateurs et opérateurs de comptes peuvent ajouter des machines au domaine.



b) Connexion à une ressource distante

La connexion à une ressource distant peut se faire via une commande NET USE, via l'explorateur Windows en saisissant un chemin UNC ou encore, via un clic-droit sur Voisinage Réseau puis Connecter un lecteur réseau. Soulignons que cette dernière méthode de connexion va nous permettre de spécifier un utilisateur et un mot de passe pour créer la connexion.

5 Connexion à un réseau Novell Netware

a) Clients pour réseau Netware

Pour permettre le partage de fichiers et d'imprimantes entre Windows 2000 et un serveur NetWare, CSNW (Services Client pour NetWare) doit être installé sur le système Windows 2000.

b) Services Passerelle pour Netware

Les Services Passerelle pour NetWare (Gateway Services for NetWare) peuvent être implémentés sur votre serveur Windows 2000 afin de permettre aux clients Microsoft d'accéder à votre serveur NetWare en utilisant votre serveur Windows 2000 comme passerelle.

Pour configurer SPNW, il faut activer la passerelle et fournir un compte possédant des privilèges de superviseur pour le serveur Netware en question. C'est la passerelle qui va partager les ressources Netware. Toutefois, elle ne peut accorder des permissions plus importantes que ne l'autorisent les droits Netware. Le compte de passerelle doit exister sur le serveur Netware et être membre du groupe NTGATEWAY.

Les serveurs Netware 3 utilisent Bindery Emulation (Preferred Server dans CSNW). Les serveurs Netware 4.x et suivants utilisent NDS (arbre et contexte par défaut).

✍ . Il y a deux façons de changer un mot de passe sur un serveur NetWare :- SETPASS.EXE et l'option Changer le Mot de Passe (depuis la boîte de dialogue CTRL-ALT-SUPPR). L'option Changer le Mot de Passe n'est disponible que sur les serveurs NetWare 4.x et suivants utilisant NDS.

6 Autres protocoles

DLC est un protocole à utilisation spéciale. Il n'est pas routable et est utilisé par Windows 2000 pour dialoguer avec les mainframes IBM, AS400 et les imprimantes Hewlett Packard.

AppleTalk permet à des ordinateurs Windows 2000 Professionnel d'utiliser des imprimantes Apple. Ne pas confondre avec le service Serveur de Fichiers pour Macintosh qui permet aux client Apple d'utiliser les ressources d'un serveur Windows 2000.

NetBEUI est exclusivement utilisé par les systèmes Microsoft. Il n'est pas routable et est basé sur la diffusion.

7 Outils de connectivité

a) Coté Serveur

Serveur Telnet
Windows 2000 inclue un service serveur telnet (net start tlntsvr) qui est limité à une interface en ligne de commande et à deux connexions concurrentes. Définissez les options de sécurité de votre serveur telnet grâce à l'utilitaire d'administration tlntadmn.

Serveur Web
Windows 2000 Professionnel propose une version allégée du serveur Web IIS5. Il est limité à 10 connexions. Il doit être installé et le service doit être lancé avant de pouvoir partager vos imprimantes en utilisant le serveur Web d'imprimantes ou l'impression via internet. Il peut être géré via le snap-in IIS ou le Personal Web Manager, une version allégée du même snap-in IIS, pour les utilisateurs novices.

Serveur FTP
Windows 2000 Professionnel propose une version limitée du serveur FTP de Internet Information Server 5 (IIS5), limitée à 10 connexions mais administrée comme la version Serveur en utilisant le snap-in IIS ou le Personal Web Manager.

Extension Serveur de FrontPage 2000
Ce composant permet d'étendre les fonctionnalités du serveur Web et est inclus à Windows 2000 Professionel pour développer et tester les sites web avant des les déployer sur un serveur de production.

Serveur SMTP
Il n'a pas de limitation en nombre de connexion. Il possède une intégration avec LDAP et est utilisé pour la réplication d'Active Directory.

b) Utilitaires TCP/IP Client

Client Telnet – peut être utilisé pour ouvrir une session en mode texte sur une console UNIX, Linux et les systèmes Windows 2000 (commande : ***telnet Nom_ou_IP_serveur***).

Client FTP – en ligne de commande – simple et puissant (commande ***ftp Nom_ou_IP_serveur***).

Internet Explorer 5 – le navigateur Internet de Microsoft.

Outlook Express 5 – Gestionnaire de courrier électronique supportant SMTP, POP3, IMAP4, NNTP, HTTP, et LDAP.

c) Services pour Unix v2.0

Le protocole TCP/IP est requis pour communiquer avec les machines UNIX.

Windows 2000 utilise CIFS (Common Internet File System) qui est une version évoluée du protocole SMB (Server Message Block).

Les Services d'impression pour UNIX permettent la connexion à des imprimantes contrôlées par des serveurs UNIX (LPR).

UNIX partage ses ressources fichiers sur le réseau grâce à NFS (Network File System).

Client pour NFS

Cela installe un client compatible Network File System (NFS) qui va s'intégrer dans l'Explorateur Windows. Il est disponible sur les versions Windows 2000 Professionnel et Server.

Les utilisateurs peuvent naviguer et mapper des lecteurs vers des volumes NFS, mais aussi, accéder à des ressources NFS aux travers du Voisinage Réseau. Microsoft recommande cette méthode plutôt que d'installer un serveur SAMBA (service de fichier SMB pour les clients Windows).

Les partages NFS peuvent être atteints en utilisant la syntaxe standard de NFS (nom_de_serveur:/partage) ou en utilisant la syntaxe UNC (\\nom_ou_IP_serveur\partage).
Si le login et/ou le mot de passe employés pour se connecter a un serveur UNIX diffèrent de ceux utilisés pour ouvrir la session Windows, il faudra cliquer sur « Se connecter en utilisant un nom d'utilisateur différent ».

Les utilitaires suivants sont installés quand on ajoute le client pour NFS (liste non complète):

grep	Cherche les fichiers contenant une chaîne et affiche le résultat contenant la chaîne
Ps	Liste les processus et leur état
sed	Copie les noms de fichiers vers une sortie standard
Sh	Lance le Korn shell
tar	Utilisé pour créer des fichiers archives et pour ajouter/extraire des fichiers à une archive
Vi	Lance l'éditeur de texte VI

L'utilitaire en ligne de commande nfsadmin est utilisé pour configurer et administrer le client pour NFS. Ses options sont:

fileaccess	Permissions des fichiers UNIX en lecture, écriture, exécution
mapsvr	Nom d'ordinateur du serveur mappé
mtype	Méthode de Mount (HARD ou SOFT)
perf	Méthode pour déterminer les paramètres de performance (manuel ou par défaut)
preferTCP	Indique s'il faut utiliser TCP (OUI ou NON)
retry	Nombre d'essais pour un montage ('mount') soft à la valeur par défaut est 5

rsize	Taille du buffer de lecture en KB
timeout	Timeout en secondes pour un appel RPC
wsize	Taille du buffer d'écriture en KB

Serveur pour NFS

Permet aux clients NFS (UNIX/Linux) d'accéder à des fichiers sur un ordinateur Windows 2000 Professionnel ou Server.
Il est géré via le snap-in d'administration UNIX (***sfumgmt.msc***).

Passerelle pour NFS

Permet aux clients Windows non-NFS d'accéder à des ressources NFS en se connectant à un serveur Windows ayant la possibilité d'y accéder.

Se comporte comme une passerelle/traducteur entre le protocole NFS utilisé par UNIX/Linux et le protocole CIFS utilisé par Windows 2000.

Elle n'est pas disponible sur les versions Windows 2000 Professionnel (Server seulement).

Serveur pour PCNFS

Il peut être installé sous Windows 2000 Professionnel ou Server.

Il fournit un service d'authentification pour les clients NFS (UNIX) qui ont besoin d'accéder à des ressources NFS.

Serveur pour NIS

Doit être installé sur un Windows 2000 Server configuré en tant que Contrôleur de Domaine. Il permet au serveur de travailler en tant que NIS master pour un domaine UNIX particulier. Il peut authentifier les requêtes des partages NFS.

Module 4
Gestion de comptes d'utilisateurs

1 Installation des outils d'administration

Les outils d'administration permettent la gestion des serveurs à distance. Ils peuvent être installés sur n'importe quelle machine sous Windows 2000 par l'intermédiaire de ***adminpak.msi*** qui se trouve dans le dossier i386 du CD ROM d'installation du système.

Les outils d'administration sont installés par défaut sur le contrôleur de domaine.

✍ . Il peut être utile, pour des raisons de sécurité, d'utiliser les outils d'administration en étant loggé avec votre compte de domaine basique, en utilisant la commande Exécuter en tant que.

2 Comptes d'utilisateurs locaux et de domaine

Les comptes d'utilisateurs locaux résident sur la machine locale. Les comptes locaux ne peuvent pas accéder à des ressources de domaine Windows 2000 et ne devraient pas être créés sur des machines qui font parties d'un domaine.

Les comptes d'utilisateurs de domaine résident dans Active Directory, sur des contrôleurs de domaine et peuvent accéder à toutes les ressources sur le réseau, à condition d'avoir les privilèges nécessaires.

Les comptes prédéfinis sont : Administrateur et Invité (désactivé par défaut).

3 Convention de nommage

Les noms de compte utilisateur ne peuvent pas dépasser 20 caractères et ne peuvent contenir les caractères suivants : " / \ [ ] : ; | = , + * ? < >. Ils ne sont pas sensibles à la casse.

Les mots de passe peuvent faire jusqu'à 128 caractères. Les caractères non autorisés dans les noms de comptes le sont aussi au niveau des mots de passe.

4 Gestion des comptes

a) Comptes locaux

Ils sont créés par l'intermédiaire de la console de Gestion de l'ordinateur.
Les comptes locaux ont la particularité d'être enregistrés dans la base de données de comptes locale : la SAM. De plus, le nombre d'options de configuration est restreint. Ils ne sont pas enregistrés dans Active Directory.
Il est déconseillé de créer des comptes locaux sur des machines rattachées à un domaine, car les utilisateurs n'auront accès qu'aux ressources locales de la machine.

b) Comptes de domaine

Les comptes de domaines permettent aux utilisateurs de se connecter depuis n'importe quelle station de travail, et d'avoir accès à toutes les ressources du réseau.
Les comptes de domaines sont gérés par la console Utilisateurs et Ordinateurs Active Directory

5 Gestion des dossiers de base

Les dossiers de base permettent aux utilisateurs de stocker leurs documents. Ces dossiers peuvent se trouver soit sur un serveur, soit sur l'ordinateur de l'utilisateur.

6 Gestion des profils utilisateurs

Profil d'utilisateur par défaut : il est la base des autres profils utilisateurs qui sont créés à partir de ce dernier.

Profil d'utilisateur local : ce profil est créé la première fois qu'un utilisateur ouvre une session sur un ordinateur. Il se trouve sur l'ordinateur local. Plusieurs profils utilisateurs peuvent se trouver sur la même machine.

7 Profil d'utilisateur itinérant

Il est créé par l'administrateur et est stocké sur un serveur. Il est disponible quelle que soit la machine à partir de laquelle l'utilisateur ouvre une session.
Les modifications sont sauvegardées lors de la déconnexion de l'utilisateur.
Le fichier Ntuser.dat contient la portion de Registre qui s'applique au compte d'utilisateur, il contient les paramètres du profil de l'utilisateur.

8 Profil d'utilisateur obligatoire

Il est lui aussi crée par l'Administrateur, il peut être local ou itinérant. Il ne permet pas à un utilisateur d'enregistrer ses paramètres.
Pour rendre un profil obligatoire, vous devez renommer le fichier Ntuser.dat en Ntuser.man (man pour mandatory = obligatoire).

Module 5
Gestion de l'accès aux ressources à l'aide de groupes

Sous Windows NT 4, nous avions à notre disposition des groupes locaux et des groupes globaux :

Les groupes locaux servaient à affecter aux utilisateurs des permissions d'accès à une ressource.
Les groupes globaux servaient à organiser les comptes d'utilisateurs de domaine.

Groupe Local	Groupe Global
?? affecte aux utilisateurs des permissions ou des droits ?? peut comporter depuis un domaine quelconque : - des comptes d'utilisateur - des groupes globaux	?? organise les comptes d'utilisateur par domaines ?? ne peut contenir aucun groupe ?? toujours créé sur le PDC dans le domaine du compte. ?? comptes d'utilisateur du même domaine ?? est ajouté à un groupe local de n'importe quel domaine (approbation).

(sous Windows NT 4.0)

1 Les groupes dans un groupe de travail

Règles d'adhésion

Un groupe local ne peut contenir que des comptes utilisateurs (locaux).
Un groupe local ne peut pas être membre d'un autre groupe.

Groupes locaux

Vous pouvez les créer sur des machines sous Windows 2000 Professionnel ou Server. Ils servent à contrôler l'accès aux ressources sur l'ordinateur local et à réaliser des tâches dites systèmes pour l'ordinateur local.

Groupes locaux intégrés

Ces groupes sont automatiquement créés lors de l'installation de Windows 2000. Vous ne pouvez pas les supprimer.

Groupe locaux prédéfinis

Administrateurs	Peuvent effectuer toutes les taches administratives sur le système local. Le compte prédéfini administrateur est automatiquement membre de ce groupe par défaut.
Opérateurs de sauvegarde	Peuvent sauvegarder et restaurer des données.
Invités	Accès temporaire et limité aux ressources
Utilisateurs avec Pouvoirs	Peuvent créer et modifier des comptes locaux sur l'ordinateur, partager des ressources ou installer des pilotes de périphériques.
Duplicateurs	Gèrent la réplication sur un domaine.
Utilisateurs	Les utilisateurs peuvent effectuer des tâches pour lesquelles les permissions leur ont été assignées. Tout nouveau compte créé sur une machine Windows 2000 est ajouté à ce groupe. Quand un ordinateur ou un serveur membre disposant d'un client réseau Microsoft joint le domaine, alors, Windows 2000 ajoute les utilisateurs du domaine au groupe local Utilisateurs.

Les groupes à identités spéciales (groupes spéciaux) permettent d'organiser automatiquement les utilisateurs pour l'utilisation du système.

Groupes spéciaux prédéfinis

Tout le monde	Inclue tous les utilisateurs qui accèdent à l'ordinateur
Utilisateur authentifié	Inclue tous les utilisateurs avec un compte utilisateur sur l'ordinateur ou sur le

	domaine – utilisé pour éviter les accès anonymes à des ressources
Créateur propriétaire	Inclue le compte utilisateur pour l'utilisateur qui a créé ou pris possession d'une ressource
Réseau	Inclue tout utilisateur avec une connexion courante depuis un autre ordinateur du réseau vers une ressource partagée de l'ordinateur
Interactif	Inclue le compte utilisateur pour l'utilisateur qui est loggé sur l'ordinateur. Les membres de ce groupe ont accès aux ressources de l'ordinateur sur lequel ils se trouvent physiquement
Utilisateur Anonyme	Tout utilisateur que Windows n'a pas authentifié
Accès Distant	Tout utilisateur employant une connexion d'accès réseau à distance.

La stratégie de gestion des ressources dans un groupe de travail est **ALP** : **A**ccount - **L**ocal group - **P**ermission. L'on crée le compte, on l'ajoute dans un groupe local, puis ensuite, on positionne les permissions.

2 Les groupes dans un domaine

Windows 2000 propose deux types de groupes dans un domaine : sécurité et distribution.

a) Les types de groupes

Groupe de sécurité : Ils permettent de gérer les autorisations d'accès à une ressource. Ils permettent aussi de gérer des listes de distributions de messagerie. L'on peut imaginer une application comme Microsoft Exchange 2000 qui va utiliser les groupes de sécurité Windows 2000 en tant que liste de distribution.

Groupes de distribution : ils ne servent qu'a des fonctions non liées à la sécurité comme l'envoi de messages. Vous ne pourrez pas gérer d'autorisations avec ces groupes.

b) L'étendue des groupes

L'étendue d'un groupe est sa portée et son champ d'utilisation.

Etendue de groupe globale : il s'agit de l'équivalent des groupes globaux sous Windows NT 4.
Ils permettent d'organiser les utilisateurs qui ont les mêmes besoins d'accès à des ressources.
Les règles d'adhésion sont les suivantes :
Vous pouvez ajouter des comptes d'utilisateurs à partir du domaine dans lequel vous créez le groupe global.
Vous pouvez ajouter des groupes globaux à partir du domaine dans lequel vous créez le groupe global : les groupes globaux peuvent être imbriqués dans d'autres groupes globaux.
Vous pouvez ajouter votre groupe global à un groupe de domaine local ou un groupe universel.

Etendue de groupe de domaine local : Ils permettent d'accorder des autorisations sur les ressources du domaine. Attention : il s'agit du même domaine que celui sur lequel le groupe local a été crée. On peut les considérer comme l'équivalent des groupes locaux sous Windows NT 4.0 sauf qu'ils ne sont pas stockés dans la base SAM de chaque machine mais dans l'annuaire Active Directory. Les ressources peuvent donc être situées n'importe où sur le domaine.
Les règles d'adhésion sont les suivantes :
Un groupe de domaine local possède une adhésion illimitée. Vous pouvez y ajouter des comptes d'utilisateurs, des groupes universels et des groupes globaux d'un domaine quelconque.
Les groupes de domaine local ne peuvent pas être imbriqués dans d'autres groupes.

Etendue de groupe de domaine universelle : Ils permettent d'accorder des autorisations sur des domaines connexes. Contrairement aux groupes de domaine local, vous pouvez accorder des autorisations d'accès sur les ressources situées dans tout domaine.
Les règles d'adhésion sont les suivantes :
Les groupes universels ont une adhésion illimitée. Tous les groupes et comptes d'utilisateur de domaine peuvent en être membres.

Les groupes universels peuvent être imbriqués dans d'autres groupes du domaine. Vous pouvez ajouter un groupe universel à un groupe de domaine local ou universel de tout domaine.

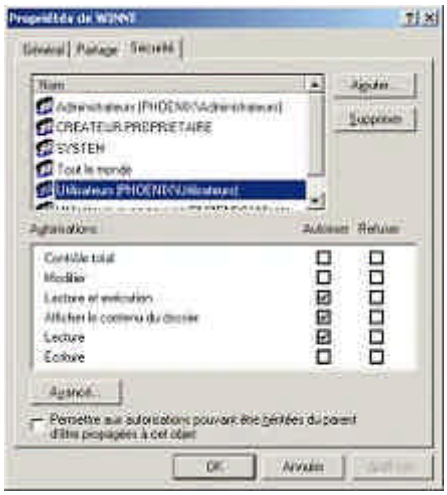
La stratégie de gestion des ressources dans un groupe de travail est **A G DL P** : **A**ccount - **G**lobal group - **D**omain **L**ocal group - **P**ermission. On crée le compte, on l'ajoute dans un groupe global, puis l'on ajoute ce dernier dans un groupe de domaine local puis ensuite l'on positionne les permissions.

✍ . Les groupes universels ne sont pas disponibles lors de l'installation de Windows 2000. Vous devez passer en mode natif pour pouvoir les utiliser.

Module 6
Gestion de données à l'aide du système de fichiers NTFS

1 Les autorisations NTFS

Les autorisations NTFS permettent de fixer le niveau d'accès qu'ont les utilisateurs (au niveau compte utilisateur, au niveau groupe d'utilisateurs ou au niveau ordinateur) sur une ressource. Ces autorisations peuvent être cumulées, excepté pour Aucun Accès, qui les outrepasse toutes.
Les autorisations sur les fichiers sont prioritaires sur les autorisations appliquées aux dossiers.



Il est à noter que l'autorisation Refuser est prioritaire sur les autres autorisations.

Autorisations NTFS sur les dossiers : Lecture, Ecriture, Afficher le contenu du dossier, Lecture et exécution, Modifier, Contrôle Total.

Autorisations NTFS sur les fichiers : Lecture, Ecriture, Lecture et exécution, Modifier, Contrôle Total.

✍ . Par défaut, dans une partition NTFS, Windows 2000 accorde Contrôle Total au groupe Tout le Monde.

✍ . cacls.exe est utilisé pour modifier les permissions des volumes NTFS en ligne de commande.

2 Principe d'héritage des autorisations NTFS

Sous Windows 2000, les autorisations que vous accordez à un dossier parent sont héritées et propagées à tous les sous-dossiers, et les fichiers qu'il contient. Tous les nouveaux fichiers et dossiers créés dans ce dossier hériteront aussi de ces permissions.

Par définition, toutes les autorisations NTFS d'un dossier créé seront héritées par les dossiers et fichiers qu'il contiendra.

3 Principe de blocage de l'héritage

Il est possible de bloquer cet héritage (pour des raisons de sécurité) afin que les permissions ne soient pas propagées aux dossiers et aux fichiers contenus dans le dossier parent.

Pour bloquer l'héritage des permissions, afficher les propriétés du dossier, allez dans l'onglet Sécurité, puis désactiver la case à cocher 'Permettre aux autorisations pouvant être héritées du parent d'être propagées à cet objet'. Dans la nouvelle fenêtre, cliquer Copier si vous souhaitez garder les autorisations précédemment héritées sur cet objet, ou alors cliquer Supprimer afin de supprimer les autorisations héritées et ne conserver que les autorisations explicitement spécifiées.

4 Autorisation Refuser

Elle est toujours appliquée au cas par cas pour les utilisateurs ou les groupes. Elle est prioritaire sur toutes les autres autorisations. Ainsi, un utilisateur qui appartient à un groupe dont la permission sur un certain dossier est Contrôle Total et qui fait l'objet d'une autorisation Refuser, n'aura pas d'accès au dossier car l'autorisation Refuser annule toutes les autres.

✍ . L'autorisation Refuser n'est utilisée que dans le cas où l'accès à une ressource doit être interdit à un groupe ou à un compte donnée.

5 Autorisations NTFS spéciales

a) Modifier les autorisations

Dans le cas où les autorisations NTFS standard ne correspondent pas à ce que vous souhaitez, alors, vous pouvez les créer sur mesure. Il suffit d'aller sur la fenêtre de propriétés du dossier ou du fichier, dans l'onglet Sécurité. En cliquant sur le bouton Avancé, on affiche la fenêtre des Paramètres du contrôle d'accès. Il suffit alors de cliquer sur le bouton Afficher/Modifier. Une boite de dialogue s'ouvre vous alors, permettant de choisir exactement les permissions que vous souhaitez appliquer à l'utilisateur ou au groupe choisi.

b) Appropriation

Elle peut s'effectuer sur un fichier ou un dossier. Pour prendre possession vous devez être soit : le créateur propriétaire, soit l'administrateur, soit avoir la permission Contrôle total ou l'autorisation d'accès spéciale Appropriation dans le cas ou vous êtes un utilisateur (ou membre d'un groupe ayant cette permission).

Si quelqu'un prend possession d'un fichier ou d'un dossier, il en devient le propriétaire.

Pour pouvoir accorder l'autorisation Appropriation sur une ressource, il faut soit être le propriétaire, soit faire partie du groupe Administrateurs ou encore avoir l'autorisation Contrôle total sur la ressource.

6 Copie et déplacement de fichiers et de dossiers

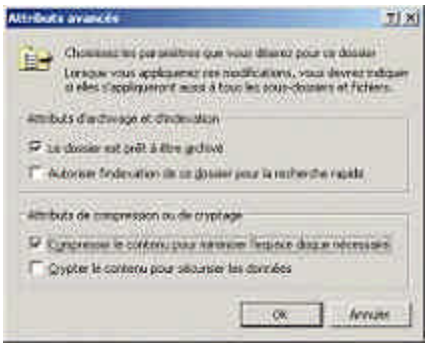
Toutes les opérations de copie héritent des autorisations du dossier cible. Seul le déplacement vers la même partition permet le maintien des autorisations.

Les fichiers déplacés depuis une partition NTFS vers une partition FAT ne gardent pas leurs attributs et leurs descripteurs de sécurité, mais ils conservent leur nom de fichier long.

Les attributs de fichiers pendant la copie/le déplacement d'un fichier à l'intérieur d'une partition ou entre deux partitions sont gérés ainsi:

Copier à l'intérieur d'une partition	Crée un nouveau fichier identique au fichier original. Il hérite des permissions du répertoire de destination..
Déplacer à l'intérieur d'une partition	Ne crée pas un nouveau fichier. Il y a seulement une mise à jour des pointeurs du dossier. Garde les permissions appliquées à l'origine au fichier.
Déplacer vers une autre partition	Crée un nouveau fichier identique à l'original et détruit le fichier original. Le nouveau fichier hérite des permissions du répertoire de destination.

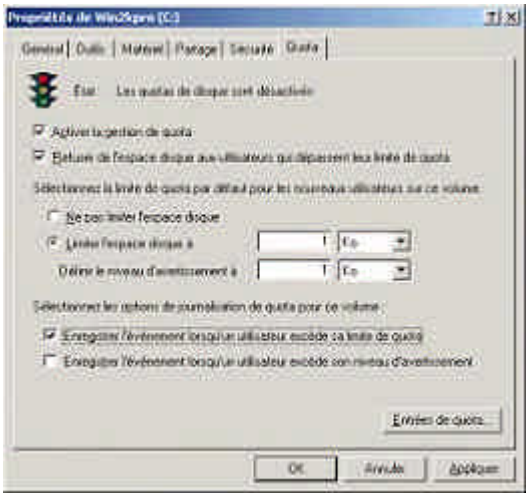
7 Compression de fichiers et dossiers



Comme sous Windows NT 4, il est possible de compresser vos dossiers et fichiers. Les règles de conservation de l'attribut de compression sont les mêmes que pour les autorisations. Ainsi, toutes les opérations de copie héritent de l'attribut de compression (compressé ou non compressé). De plus, seul le déplacement vers la même partition permet le maintien de la compression.

✍ . Pour faire apparaître un dossier compressé dans une autre couleur, utiliser la case à cocher 'Donner une couleur différente aux fichiers et dossiers compressés', dans l'onglet Affichage du menu Options de dossiers de l'Explorateur.

8 Utilisation des quotas de disques



Ils permettent de limiter la quantité d'espace disque disponible pour un utilisateur. Windows 2000 effectue Une gestion des quotas de disque de façon indépendante pour chaque partition.

Pour mettre en œuvre les quotas, vous devez dans un premier temps les activer pour une partition. Il est possible d'appliquer une limite globale pour tous les utilisateurs (dans la zone Limiter l'espace disque à).

Il vous est aussi possible de définir des quotas par utilisateur à partir de la boite de dialogue Propriétés d'un disque puis onglet Quota puis Entrées de quota.

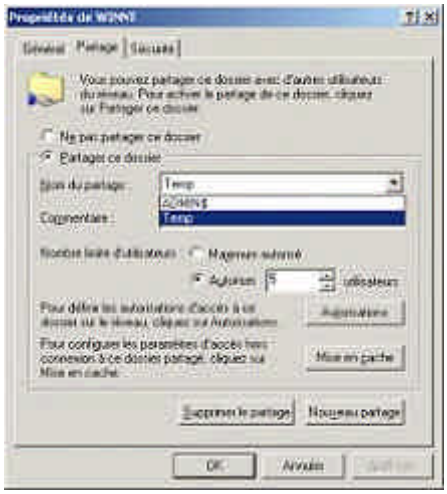
a) Options de quotas

Activer la gestion de quota	Active la gestion de quota sur le disque sélectionné
Refuser de l'espace disque aux utilisateurs qui dépassent leur limite de quota	Quand un utilisateur dépasse la quantité d'espace à laquelle il a droit, il ne peut plus écrire
Ne pas limiter l'espace disque	Pas de limitation d'espace disque
Limiter l'espace disque à	Espace disque auquel ont droit les utilisateurs
Définir le niveau d'avertissement	Un événement pourra être consigné dès que ce seuil sera atteint
Entrées de quota	Permet d'Ajouter/supprimer des entrées de quota, d'afficher les propriétés des utilisateurs auxquels vont être appliqués les quotas

✍ . On ne peut appliquer de quota ni à un groupe, ni à un répertoire.

Module 7
Accès aux ressources disques

1 Création de dossiers partagés



Les administrateurs et les utilisateurs avec pouvoirs peuvent créer des partages sur des machines Windows 2000 Professionnel. Les administrateurs et opérateurs de serveurs peuvent effectuer cette tâche sur Windows 2000 Serveur.

a) Partages administratifs

Windows 2000 crée des partages administratifs comme Windows NT 4. Les noms de ces partages se terminent avec un caractère $ qui permet de cacher le partage lors de l'exploration par le réseau. Le dossier système (Admin$), la localisation des pilotes d'impression (Print$) ainsi que la racine de chaque volume (c$ ..) constituent autant de partages administratifs.

b) Partage d'un dossier et permissions

Les permissions de niveau partage sur les dossiers s'appliquent uniquement si l'accès se fait via le réseau. Par défaut, le groupe Tout le Monde possède la permission Contrôle Total pour tous les nouveaux partages.

c) Autorisation sur les dossiers partages

Contrôle Total	- Est assigné au groupe Tout le monde par défaut. - Permet aux utilisateurs de prendre possession de fichiers ou de dossiers. - Les utilisateurs peuvent changer les droits d'accès aux fichiers. - Donne aux utilisateurs toutes les permissions assignées par les niveaux Changer et Ecrire.
Modifier	- Les utilisateurs peuvent ajouter et créer des fichiers. - Donne la possibilité de modifier les fichiers. - Les utilisateurs peuvent changer les attributs des fichiers. - Les utilisateurs peuvent effacer les fichiers. - Donne aux utilisateurs les permissions assignées par le niveau Lire.
Lire	- Les utilisateurs peuvent visualiser et ouvrir les fichiers. - Les utilisateurs peuvent visualiser les attributs des fichiers. - Les utilisateurs peuvent exécuter les fichiers exécutables.
Aucun Accès	- Les utilisateurs ne peuvent pas visualiser, accéder ou modifier les fichiers.

Lorsqu' un utilisateur est sujet aussi bien aux 5 niveaux de permissions NTFS qu'aux permissions de sécurité de partage, ses permissions effectives s'obtiennent en combinant les niveaux maximum des deux types de sécurité (en prenant bien en compte qu'il n'y a pas de permission 'Aucun Accès') et en prenant les plus restrictives.

✍ . Windows 2000 Professionnel est limité à 10 connexions concurrentes pour un fichier ou un service d'impression.

2 Choisir un système de fichiers

NTFS propose un grand niveau de sécurité et d'efficacité grâce à sa capacité à bloquer l'accès à un fichier ou à un répertoire pour un seul utilisateur. Les capacités avancées telles que la compression de disque, les quotas de disque et le cryptage font de ce système un système recommandé par des professionnels.

FAT et FAT32 sont utilisés généralement pour faire du dual boot entre des systèmes Windows 2000 et d'autres systèmes d'exploitation tels que DOS 6.22, Win 3.1 ou Win 95/98.

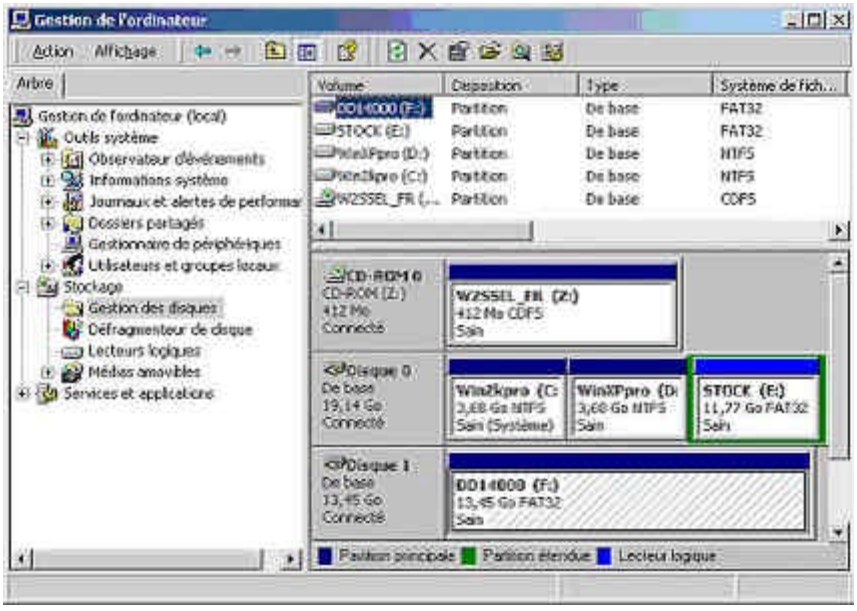
Les partitions système de type NTFS NT 4.0 seront mises à jour vers le NTFS de Windows 2000 automatiquement. Si vous voulez faire un dual-boot entre NT4.0 et 2000, vous devez déjà installer le SP4 sur la machine NT4.0. Cela permettra de lire les partitions NTFS mises à jour, mais les fonctions avancées telles que EFS et les quotas de disque seront désactivées.

✍ . Utilisez ***convert.exe*** pour convertir les partitions FAT ou FAT32 vers NTFS. Les partitions NTFS ne peuvent pas être converties vers FAT ou FAT32 – la partition doit alors être effacée et recréée en tant que FAT ou FAT32.

3 Les capacités de protection de fichiers de Windows (WFP : Windows File Protection)

Nouveauté de Windows 2000, il évite le remplacement de certains fichiers systèmes qui sont surveillés par le système (les DLL importantes et les EXE qui se trouvent dans le dossier %systemroot%\system32).
Ce système utilise les signatures de fichiers et le codage pour vérifier si les fichiers systèmes protégés sont bien des versions Microsoft.
WFP ne génère pas de signature.
Les DLL critiques qui ont été modifiées sont restaurées depuis le dossier %systemroot%\system32\dllcache.

4 Les volumes sous Windows 2000



Windows 2000 supporte deux types de disques : basique et dynamique.

En mode basique vous scindez le disque dur en partitions. Windows 2000 reconnaît les partitions primaires et étendues. Un disque initialisé en mode basique est appelé disque de base, il peut contenir des partitions primaires, étendues et des lecteurs logiques. Les disques basiques doivent être utilisés dans le cas de dual-boot entre Windows 2000, DOS, Windows 3.x, Windows 9x/Me ainsi que toute version de Windows NT.

En mode dynamique (uniquement sous Windows 2000 et XP) il est possible de créer une seule partition contenant le disque dur complet. Un disque initialisé en mode dynamique est appelé Disque dynamique. Les disques dynamiques sont divisés en volumes qui peuvent inclure un ou plusieurs disques. Ils peuvent être redimensionnés sans avoir besoin de redémarrer le système d'exploitation. Une partie de l'espace (à la fin du disque) est réservée pour stocker les informations de description du disque dynamique.

Il existe trois types de volumes

Volume Simple : contient l'espace d'un seul disque.

Volume Multiple : contient l'espace de plusieurs disques (maximum de 32). Les disques y sont utilisés successivement (Le premier disque est rempli, puis le deuxième,...) de façon transparente pour l'utilisateur. Il s'agit en fait d'un agrégat de partition. Si un disque ne fonctionne plus, alors, toutes les données sont perdues. Les performances sont dégradées avec ce type de volume car les disques sont lus séquentiellement.

Agrégat par bande sans parité : il contient l'espace libre de plusieurs disques (maximum de 32) en un seul volume logique. Cela augmente les performances car les données sont lues et écrites sur tous les disques à la même vitesse. Si un disque est perdu, alors, toutes les données sont perdues.

Etats d'un Volume Dynamique

Erreur	Le volume ne peut pas être automatiquement redémarré et doit être réparé.
En état	Est accessible et n'a pas de problème connu
En état (avec risque)	Accessible, mais des erreurs d'E/S ont été détectées sur le disque.
Initialisation	Le volume est en train d'être initialisé et sera réputé 'en état' dès la fin du processus

Limitations des volumes dynamiques

Ils ne sont pas accessibles par DOS, Win95/98 ni aucune version de Windows NT lorsque vous utilisez le dual-boot. Ils n'utilisent pas le schéma traditionnel d'organisation des disques en partitions et volumes logiques. Le MBR des disques dynamiques contient un pointeur vers les données de configuration du disque qui se trouvent dans le dernier méga-octet à la fin du disque.

Les volumes dynamiques qui ont été mis à jour depuis une partition basique ne peuvent pas être étendus, surtout si ils contiennent les fichiers nécessaires au démarrage de Windows 2000 et le volume de boot. Seuls les volumes créés après la mise à jour vers un volume dynamique peuvent être étendus.

Lorsque vous installez Windows 2000, si un volume dynamique a été créé à partir de l'espace non alloué du disque, alors Windows 2000 ne pourra pas être installé sur ce volume.

Ils ne sont pas supportés par les ordinateurs portables et les médias amovibles.

La conversion d'un disque de démarrage (initialement un volume basique) vers un volume dynamique est irréversible. Il ne pourra plus être converti dans l'autre sens (vers un volume basique).

Traduction de termes entre disques basiques et dynamiques

Disques Basiques	Disques Dynamiques
Partition Active	Volume actif
Partition étendue	Volume et espace non alloué
Disque Logique	Volume Simple
Ensemble Miroir	Volume Miroir (Server seulement)
Partition primaire	Volume Simple
Agrégat par bande	Volume agrégé

Agrégat par bande avec parité	Volume RAID-5 (Server seulement)
Partitions système et de boot	Volumes Système et de boot
Jeu de Volume	Volumes étendu

Pour gérer des disques sur un ordinateur distant vous devez créer une console sur mesure configurée pour cet ordinateur.

Choisir Démarrer > Exécuter, taper **mmc** et presser Entrée. Dans le menu de la console, cliquer sur Ajouter/Supprimer Snap-in. Cliquer Ajouter. Cliquer Gérer les Disques, puis cliquer Ajouter. Quand la boite de dialogue 'choisir un ordinateur' apparaît, choisir l'ordinateur distant.

Windows 2000 supporte maintenant les quotas sur plusieurs disques. Les quotas peuvent être définis sur des volumes NTFS, mais pas sur des volumes FAT ou FAT32. Les quotas ne peuvent pas être fixés sur des dossiers à l'intérieur d'une partition NTFS.

Les informations de disque sont maintenant enregistrées physiquement sur le disque lui-même, ce qui permet de déplacer facilement le disque d'un système à l'autre. L'utilitaire **dmtool.exe** a été développé afin de faciliter la gestion de grandes quantités de disques.

Il faut utiliser le snap-in Gestionnaire de disques :
A chaque fois que vous ajoutez un nouveau disque dans un ordinateur, il apparaît en tant que Basique
Dès que vous ajoutez ou que vous enlevez un disque de votre ordinateur, vous devez choisir Re-vérifier les Disques. Les disques qui ont été enlevés d'un autre ordinateur vont apparaître comme « étrangers ». Choisir « Importer disque étranger » (un assistant apparaît pour vous guider).
Pour des disques multiples enlevés d'un autre ordinateur, ils vont apparaître en tant que groupe. Faire un clic-droit sur l'un des disques et choisir 'Ajouter Disque'.

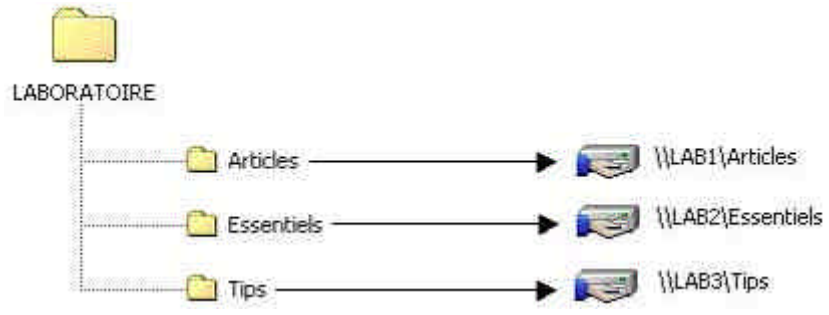
Les disques peuvent être mis à jour depuis le niveau basique vers un niveau dynamique à n'importe quel moment, pourvu qu'il y ait un Mo d'espace non-alloué sur le disque.

5 DFS : Distributed File System

DFS (Distributed File System) fournit aux utilisateurs un moyen simple d'accéder à des données reparties et distribuées sur un réseau. Un dossier partagé DFS sert de point d'accès à d'autres dossiers sur le réseau.

a) Présentation

DFS est un système de fichier logique et hiérarchique. Il organise des ressources partagées sur plusieurs ordinateurs partagées sur plusieurs ordinateurs pour fournir une arborescence logique.



Notre dossier (Laboratoire) va être le point d'entrée unique vers les ressources partagées sur les trois serveurs (Lab1, Lab2, Lab3). Les utilisateurs accèdent à ces ressources sans avoir à se soucier de connaître le serveur sur lequel se trouve la ressource.

Un partage DFS utilise une structure arborescente qui contient une racine et des liens DFS. Pour créer un partage DFS, il faut en premier lieu créer une racine DFS. Chaque racine peut avoir de multiples liens DFS qui pointent

chacun vers un dossier partagé sur le réseau. Les liens DFS de la racine représentent des dossiers partagés sur d'autres serveurs.

b) Les avantages de DFS

Le client DFS est intégré à Windows NT4 et Windows 2000 et permet de simplifier l'administration. Si un serveur n'est plus disponible, vous pouvez déplacer le lien DFS vers un autre dossier, les utilisateurs ne verront pas de différence puisque le nom de partage (racine DFS) restera inchangé malgré cette redirection. Il permet aussi de mettre en œuvre de l'équilibrage de charge et de la tolérance de panne puisqu'il est possible de créer des liens redondants à partir de serveurs multiples.

c) Restrictions de DFS

Les clients Windows 98 nécessitent l'installation d'un client DFS.

Microsoft nous fournit au niveau des limitations de DFS les valeurs suivantes :
- nombre maximum de connexion pour un chemin : 260
- nombre maximum de racine DFS par serveur : 1
- nombre maximum de racine DFS de domaine : illimité
- nombre maximum de volumes hébergés dans un domaine ou une entreprise : limité par les ressources système

d) Les types de racines DFS

Deux racines DFS peuvent être configurées sous Windows 2000 : autonome et de domaine (ou racine à tolérance de panne).

e) Racine DFS autonome

Les racines DFS autonomes sont stockées dans le registre et fournissent un seul niveau de lien DFS. Les racines DFS autour peuvent être localisées sur tous les systèmes de fichiers (FAT 16, FAT 32, NTFS). Elles n'offrent pas de processus de réplication ou de sauvegarde.

f) Racine DFS de domaine

Une racine DFS de domaine utilise Active Directory pour stocker la topologie de l'arborescence. Les changements dans un arbre DFS sont automatiquement synchronisés avec Active Directory.
Il est possible de créer des liens alternés avec les racines DFS de domaine afin de fournir une tolérance de panne à l'ensemble. Pour être fonctionnelles, les racines DFS à tolérance de panne doivent se situer sur des partitions NTFS.

6 Tolérance de pannes

La tolérance de panne est la capacité du système à trouver une compensation en cas de défaillance d'un dispositif matériel (en l'occurrence, un disque dur). Le standard en matière de tolérance de panne est connu sous le nom de RAID (Redundant Array of Inexpensive Disks). RAID est formé de plusieurs niveaux de protection.

Windows 2000 Server permet la mise en œuvre des niveaux 1 (mirroring) et 5 (agrégat par bandes avec parité) sur les disques dynamiques uniquement.

Avec l'agrégat par bandes avec parité, Windows 2000 Server écrit les données sur une série de disques dynamiques (de 3 à 32). Les données ne sont pas dupliquées sur le disque, mais Windows 2000 Server enregistre des informations de parité qu'il peut ensuite utiliser pour régénérer les données manquantes si un disque tombe en panne.

Si l'on utilise la mise en miroir, Windows 2000 Server écrira les mêmes données sur deux disques. Si l'un des deux tombe en panne, les données sont toujours disponibles sur l'autre.

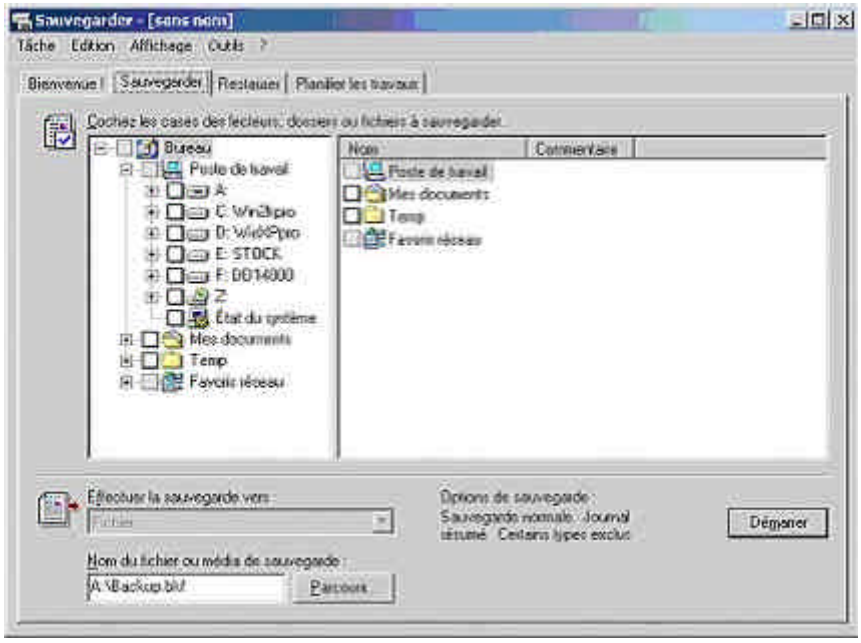
L'intérêt du RAID niveau 5 réside dans la disponibilité de plus d'espace disque. En effet, l'utilisation d'un miroir nécessite 50% de l'espace total (pour répliquer les données) alors que le RAID niveau 5 n'occupe que 20%.
En terme de performances, le RAID 5 est plus rapide en lecture car il peut lire les données à partir de plusieurs disques simultanément. Par contre en écriture, il se révèle moins performant que le RAID 1, car il est nécessaire de réaliser des calculs de parité pour écrire les données sur les disques.

Pour mettre en place la tolérance de panne, on utilise le snap-in Gestion de disque. On fait alors un clic droit sur une zone non allouée d'un disque dynamique, on choisit créer un volume. Un assistant apparaît alors, permettant de configurer entre autres la tolérance de panne.

✍ . Il n'y a pas de tolérance de panne avec Windows 2000 Professionnel. La tolérance de panne (RAID 1 et 5) est disponible seulement dans la famille Windows 2000 Server.

✍ . Si vous utilisez un système RAID 5 et que rencontrez un problème de disque, commencez par vérifier leur état dans le dans le Gestionnaire de Disques. Si l'un d'entre eux est marqué comme manquant, tentez tout d'abord de le réactiver avant d'entreprendre son remplacement.
Dans un système en RAID 1 (mirroring), le cheminement légèrement différent : si la réactivation ne donne rien, il faudra d'abord casser le miroir avant de remplacer le disque. Ensuite, il faut reformer le miroir.

7 Sauvegarde et Récupération des données



L'outil de sauvegarde de Windows 2000 est lancé par Panneau de Configuration > Outils système > Sauvegarde ou en lançant directement la commande ***ntbackup.exe*** depuis Démarrer >Exécuter.

Les utilisateurs peuvent Sauvegarder leurs propres fichiers et les fichiers sur lesquels ils ont au moins une des permissions suivantes : lecture, écriture, exécution, contrôle total.

Les utilisateurs peuvent aussi restaurer les fichiers sur lesquels ils ont au moins une des permissions suivantes : écrire, modifier, contrôle total.

Les Administrateurs et les Opérateurs de Sauvegarde peuvent sauvegarder et restaurer n'importe quel fichier en passant outre leurs permissions.

Les différents types de sauvegarde

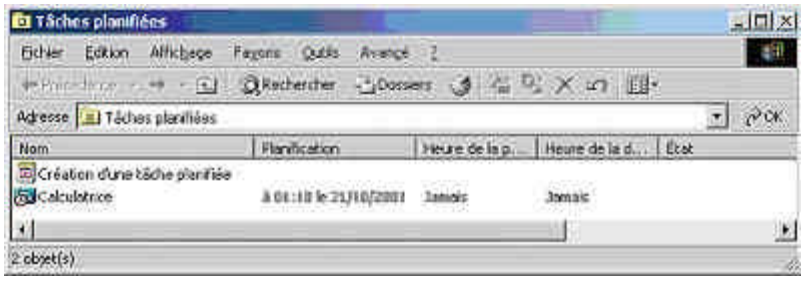
Normale	Tous les fichiers et dossiers sélectionnés sont sauvegardés. L'attribut d'archive est enlevé s'il existe, cela accélère la restauration.
Copie	Tous les fichiers et dossiers sélectionnés sont sauvegardés. L'attribut d'archive n'est pas enlevé.
Incrémentielle	Seuls les fichiers dont l'attribut Archive a été placé sont enregistrés et leur attribut est ensuite enlevé.
Différentielle	Seuls les fichiers dont l'attribut Archive a été placé sont enregistrés mais leur attribut n'est pas enlevé.
Journalière	Tous les fichiers sélectionnés et les dossiers qui ont changé pendant la journée sont sauvegardés. Les attributs Archive sont ignorés durant la sauvegarde et ne sont pas enlevés après.

a) Sauvegarde des données sur l'état du système

L'outil de sauvegarde de Windows 2000 permet aussi de sauvegarder des données système qui pourraient permettre de reconstruire un serveur défaillant.
Ces données sont notamment: le Registre, le service d'annuaire Active Directory (uniquement sous 2000 Server en tant que contrôleur de domaine) , le dossier Sysvol (uniquement sous 2000 Server en tant que contrôleur de domaine), les fichiers système de démarrage, etc...

Module 8
Surveillance et optimisation des performances dans Windows 2000

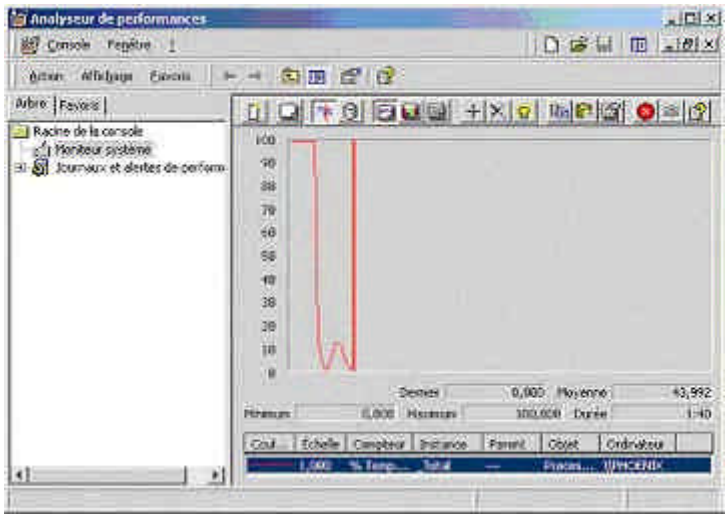
1 Planification des tâches



Elle est utilisée pour automatiser certains évènements tels que les scripts ou les sauvegardes systèmes.
Les tâches sont enregistrées dans le Gestionnaire de Tâches planifiées du Panneau de Configuration.

✍ . Il est possible de définir le compte d'utilisateur a employer pour exécuter une tâche.

2 L'analyseur de Performances



Il vous permet de vérifier si votre système ou un système distant est optimisé. Il offre la possibilité de vérifier l'activité réseau, le processeur, la mémoire ou encore les disques.

Chacune de ces données est relative à un objet, c'est à dire un composant principal de la machine. Quand on parle d'instance, on fait référence à plusieurs fois le même objet. Les compteurs captent et analysent l'activité des objets et de leurs instances, ils peuvent afficher des graphes correspondant à ces données.

Les objets importants sont cache (utilisé pour mettre en cache les données physiques du système), mémoire (physique et virtuelle/paginée du système), disque physique (vérifie le disque comme un tout), disque logique (disques logiques, bandes et volumes), et processeur (vérifie la charge CPU).

Processeur - **% Temps Processeur Time** mesure le temps que le processeur met pour effectuer une tâche non cachée. Si ce temps est toujours d'au moins 80%, il est recommandé de mettre un processeur plus puissant.

Processeur – **Longueur de Queue Processeur** – plus de 2 threads dans la queue indique que les performances systèmes sont limitées par le processeur (goulet d'étranglement).

Processeur - **% CPU temps DPC** (deferred procedure call) mesure les interruptions logicielles.

Processeur - % Temps d'interruption mesure les interruptions matérielles. Si le temps processeur excède 90% et que le temps d'interruptions/secondes est de plus de 15%, on a peut être affaire à un driver mal écrit (de mauvais drivers peuvent générer des interruptions excessives) ou bien, il faut prendre un processeur plus puissant.

Disque Logique – **Longueur de Queue de Disque** – si la moyenne est supérieure à 2, l'accès au lecteur est bridé. Remplacez votre disque par un modèle plus performant, utilisez un meilleur contrôleur de disque, ou implémentez un jeu de bandes (stripe set)

Disque Physique - **Longueur de Queue de Disque** – idem Disque Logique – Longueur de Queue de Disque

Disque Physique - **% Temps Disque** – si le temps est supérieur à 90%, déplacez les données ou le pagefile vers un autre disque, ou remplacez votre disque par un modèle plus performant.

Mémoire - **Pages/sec** – plus de 20 pages par seconde représente un fort taux de mise en pagefile – ajoutez de la RAM

✍ . La commande ***diskperf*** qui active les compteurs disque n'est pas supporté dans Windows 2000.

3 Les alertes et le journal de performance

Les Journaux d'Alerte sont comme les journaux d'événement, mais ils ne font que tracer un événement, envoyer un message ou lancer un programme quand une limite définie vient d'être dépassée.
Le journal de compteur enregistre les données depuis le système local ou un système distant sur l'utilisation matérielle et l'activité des services système.

Les journaux de trace permettent d'analyser des données telles que les E/S et fautes de pagination.

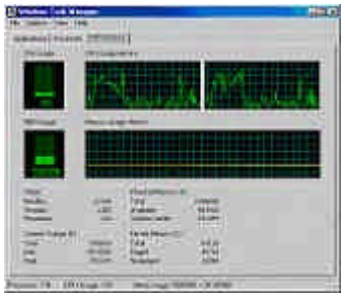
Par défaut, les fichiers de log (ou de journal) sont enregistrés dans le dossier \Perflogs sur la partition de boot.

Les logs sont enregistrés au format CSV (Comma Separated Value) ou TSV (Tab Separated Value) pour qu'ils puissent être importés par des programmes tels Excel.

CSV et TSV doivent être écrits en une seule fois. Ils ne supportent pas que l'écriture soit arrêtée puis reprise. Utiliser plutôt des fichiers binaires pour enregistrer des évènements écrits par intermittence.

4 Surveillance des processus (Gestionnaire des tâches)

Il permet de vérifier en temps réel les performances du système. Il montre les applications et les processus qui tournent et renseigne sur l'occupation du processeur et de la mémoire. Il permet de fermer les applications et les processus qui ne répondent plus. Il met à disposition 23 mesures qui permettent d'avoir des critères de classement des processus actifs.



Le gestionnaire de tâche se lance par l'intermédiaire la combinaison de touches : CTRL+ALT+SUPPR ou CTRL+SHIFT+ESC.

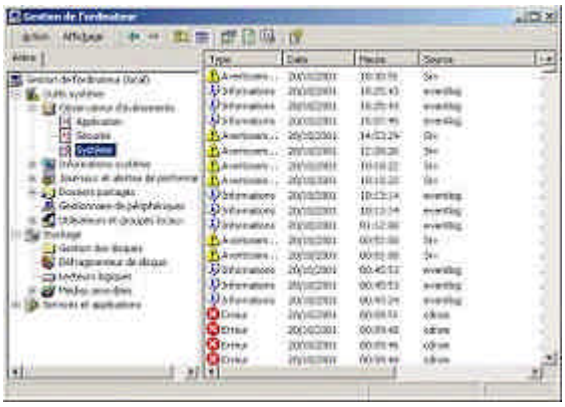
5 Journal des évènements

Il gère l'historique des évènements survenus sur la machine, au niveau matériel, logiciel et ayant trait à la sécurité et au système. Il contient trois journaux différents :

Le journal système qui contient les évènements en provenance des composants système (échec de chargement du pilote de carte graphique, etc...).

Le journal application contient les évènements générés pas les applications.

Le journal sécurité rassemble les évènements liés à la sécurité du système tels que la suppressions d'un fichier ou l'échec d'ouverture d'une session.

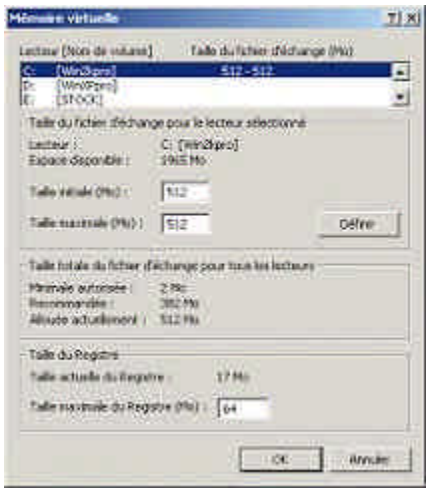


Chaque événement est soit une information (par exemple, le service Serveur DHCP a démarré avec succès), un avertissement (un problème est survenu, mais il n'est pas critique, par exemple lorsque l'espace disque disponible est très faible), ou une erreur (problème important lié au système - par exemple, le service Serveur n'a pas pu démarrer).

On trouve le journal des évènements dans : Menu démarrer > Programmes > Outils d'administration > Observateur d'évènements.

La taille du fichier de journal peut être limitée et les données peuvent être enregistrées afin de faire un suivi des performances du système.

6 Mémoire virtuelle et fichier de pagination



La taille minimum recommandée pour le fichier de pagefile est de 1.5 fois la taille de la mémoire RAM installée. Un système qui a 64 MB devrait avoir un pagefile de 96 MB. La taille maximum du pagefile ne doit pas excéder 2.5 fois la taille de la RAM installée.

On paramètre ces propriétés via l'onglet Performance de la boîte de dialogue des Propriétés du Système (bouton Changer).
Le pagefile est le plus efficace quand il est réparti sur plusieurs disques, mais pas sur les partitions système ou de boot.

✍ . La taille maximum du registre peut aussi être changée par la boite de dialogue de Mémoire Virtuelle.

Module 9
Implémentation de la sécurité dans Windows 2000

1 Stratégie de groupe

Les stratégies de groupe sont une collection de variables d'environnement utilisateur qui sont imposées par le système d'exploitation et non modifiables par l'utilisateur.

Le snap-in Stratégie de Groupe (gpedit.msc)

Il est exclusif à Windows 2000 et succède à l'Editeur de Stratégies Système. Il utilise des modèles de sécurité incrémentiels. C'est à dire que chaque modèle de sécurité est plus sécurisé que le précédent.

Il ne peut être appliqué que sur un système installé initialement sur une partition NTFS. Pour les partitions NTFS dont les systèmes ont été mises à jour depuis Windows NT 4 ou antérieur, seuls les modèles de sécurité de base seront appliqués.

Les réglages peuvent être enregistrés localement (ou dans Active Directory). Ils sont sécurisés et ne peuvent être modifiés que par les membres du groupe Administrateurs.

Il est plus flexible que l'Editeur de Stratégies Système car les réglages peuvent être filtrés en utilisant Active Directory.

Les réglages sont importés en utilisant des fichiers .INF. Le snap-in Stratégie de Groupe peut être employé pour une machine locale ou distante.

Modèles de sécurité prédéfinis de Windows 2000

Modèle	Fichier	Description
De base	basicwk.inf ou basicsv.inf ou basicdc.inf	Configure la station avec un niveau de sécurité basique
Compatible	compatws.inf	Offre un niveau de sécurité supérieur à celui du modèle de base, tout en garantissant le fonctionnement de toutes les applications.
Sécurisé	securews.inf ou securedc.inf	Il améliore les variables de sécurité pour les Stratégies de Compte et d'Audit. Enlève tous les membres du groupe Utilisateur avec Pouvoir. Les ACL ne sont pas modifiées. Il ne peut garantir le bon fonctionnement de toutes les applications (et leurs fonctionnalités).
Hautement sécurisé	hisecws.inf ou hisecdc.inf	Modèle le plus sûr mis à disposition des machines qui utilisent Windows 2000 en mode natif seulement. Il demande à ce que toutes les connexions réseau soient signées et cryptées de manière digitale. Il ne permet pas la communication avec des machines employant des modèles plus anciens de clients Windows. Il ne se soucie pas du bon fonctionnement des applications.

Si aucun des modèles de sécurité ne convient à vos besoin, vous pouvez en créer sur mesure en partant d'un modèle existant.

a) Stratégie de Groupe locale

Il existe deux types d'objet Stratégie de Groupe : les stratégies de groupe locales et les stratégies de groupe non locales. Chaque système Windows 2000 ne peut avoir qu'un seul objet Stratégie de Groupe Locale. L'ordre d'application est : locale, site, domaine et enfin unité organisationnelle. Les stratégies locales ont la préférence la moins grande alors que l'unité organisationnelle à la plus grande.

b) Stratégie de Groupe non-locale (enregistrée dans l'Active Directory)

Elle peut être liée à un site grâce aux Sites & Services de l'Active Directory afin d'être appliquée à tous les domaines du site. Quand elle est appliquée à un domaine, cela affecte tous les utilisateurs et les ordinateurs du domaine et (par héritage) tous les utilisateurs et ordinateurs de l'Unité Organisationnelle.

c) Config.pol, NTConfig.pol et Registry.pol

Windows 2000 utilise le format registry.pol. Deux fichiers sont créés : un pour la configuration de la machine (enregistré dans le sous-répertoire \Machine) et un pour la configuration de l'utilisateur (enregistré dans le sous-répertoire \User).

Le fichier registry.pol peut être utilisé avec Windows 95/98, Windows NT 4.0 et Windows 2000. NTConfig.pol concerne les systèmes sous Windows NT 4 alors que config.pol concerne Windows 9x/Me.
Les fichiers .POL peuvent être lus grâce à l'utilitaire regview.exe du Ressource Kit de Windows 2000.

d) Editeur de Stratégies Système (poledit.exe)

Windows NT 4, Windows 95 et Windows 98 l'utilisent pour spécifier la configuration ordinateur et utilisateur qui est enregistrée dans le Registre. Cependant, cette méthode n'est pas sûre car les variables peuvent être modifiées par n'importe quel utilisateur possédant l'Editeur de Registre (regedit.exe). Les variables sont importées et exportées en utilisant des modèles .ADM .

Les stratégies appliquées à l'aide de poledit.exe sont persistantes. Les propriétés sont intégrées à la base de Registre de façon permanente et continuent d'agir même lorsque la stratégie n'est plus appliquée.

2 Configuration de la sécurité

Afin d'assurer la cohérence du système au niveau de la sécurité, on utilise le snap-in "Configuration et analyse de la sécurité" (accessible uniquement par la création d'une nouvelle mmc). Il permet de configurer et d'analyser la sécurité de Windows 2000. Il est basé sur le contenu d'un modèle de sécurité créé en utilisant le snap-in "Modèle de Sécurité".

✍ . Il existe une version en ligne de commande de cet outil: secedit.exe.

Par défaut, Windows 2000 Professionnel ne demande pas à l'utilisateur l'appui de CTRL-ALT-SUPPR pour se connecter. Pour renforcer la sécurité, on peut désactiver cette fonction et forcer l'utilisateur à appuyer CTRL-ALT-SUPPR (fixer ce paramètre en utilisant le snap-in Stratégie de Groupe).

Pour désactiver l'accès à une station de travail, mais permettre aux programmes de continuer à tourner, utiliser l'option Verrouiller la Station (depuis la boite de dialogue CTRL-ALT-SUPPR).

Pour désactiver l'accès à une station de travail et ne pas permettre aux applications de continuer à tourner, utiliser l'option Se Déconnecter (depuis la boite de dialogue CTRL-ALT-SUPPR).

Pour verrouiller une station après une certaine période d'inactivité, il est conseillé d'utiliser un mot de passe pour l'économiseur d'écran.

3 Gestion de l'audit

L'Audit peut-être activé par Démarrer > Programmes > Outils d'Administration > Stratégie de Sécurité Locale. Double-cliquez sur Stratégies Locales puis cliquer sur Stratégies d'audit. Sélectionnez l'événement que vous voulez auditer et dans le menu Action, cliquer Sécurité. Définir les propriétés pour chaque objet et redémarrer l'ordinateur pour que la nouvelle stratégie prenne effet.

La suppression du fichier pagefile.sys lorsque l'ordinateur s'arrête n'est pas active par défaut. On peut la paramétrer via l'Editeur de Stratégie Locale, ce qui empêchera une personne malveillante d'extraire des informations depuis le pagefile.sys de votre machine.

Pour éviter que le nom du dernier utilisateur soit affiché à la demande de logon (comme le fait Windows 2000 Professionnel par défaut), il faut utiliser le snap-in Stratégie de Groupe, Stratégie de l'Ordinateur local.

Lorsque vous utilisez l'Observateur d'Evènements, seuls les Administrateurs locaux peuvent voir le journal de sécurité, mais Tout le Monde (par défaut) peut voir les deux autres journaux.

4 Système de cryptage de fichier (EFS : Encrypting File System)

a) A propos D'EFS

Le système de cryptage EFS fonctionne uniquement sous Windows 2000 et requiert des partitions NTFS v.5 ou ultérieur. Il est transparent pour l'utilisateur.

Il utilise un algorithme de cryptage asynchrone (clé privée/clé publique) pour l'encodage des clés de cryptage synchrones qui servent à encoder les fichiers. Cela offre une sécurité maximale pour les fichiers.

Un agent de récupération doit être configuré afin de pouvoir récupérer les fichiers cryptés dans le cas, par exemple, du départ d'un employé ou de la perte de sa clé privée.

EFS est présent dans le noyau de Windows et utilise un pool de mémoire non paginée pour enregistrer les clefs de cryptage – cela signifie que personne ne pourra les extraire de votre fichier de pagination.

Les fichiers cryptés peuvent être sauvegardés en utilisant le programme Utilitaire de Sauvegarde, ils préserveront leur état de cryptage tant que les permissions d'accès sont préservées.

Pour crypter un dossier : dans la boite de dialogue Propriétés pour le dossier, cliquer sur l'onglet Général, ensuite, cliquer sur le bouton Avancé et sélectionner la case à cocher « Crypter le contenu pour sécuriser les données ». Le dossier n'est pas crypté, mais les fichiers qui y seront placés seront cryptés. Décocher la case si vous souhaitez que les fichiers ne soient plus cryptés.

Il est à noter que le cryptage par défaut est sur 56 bits. Dans les états l'autorisant, il est possible de pousser le cryptage à 128 bits. De plus, les fichiers compressés ne sont pas cryptés et vice versa.

✍ . Vous ne pouvez pas partager des fichiers cryptés.

Il existe deux programmes utiles qui concernent le cryptage des données : la commande cipher.exe qui permet de crypter des fichiers et l'utilitaire efsinfo.exe qui se trouve dans le Ressource Kit de Windows 2000 qui permet à l'administrateur d'obtenir des informations sur les fichiers cryptés.

Utiliser la commande CIPHER

/a	Applique les opérations spécifiées aussi bien sur les dossiers que sur les fichiers
/d	Décrypte les dossiers spécifiés et les marque pour que les fichiers qui y seront ajoutés ne soient pas cryptés
/e	Crypte les dossiers spécifiés et les marque pour que les fichiers qui y seront ajoutés soient cryptés
/f	Force le cryptage des fichiers spécifiés, même ceux qui le sont déjà
/h	Affiche les fichiers avec les attributs système/cachés qui ne sont pas visibles par défaut
/i	L'opération spécifiée continue même si des erreurs surviennent durant l'opération
/k	Crée une nouvelle clé de cryptage pour les utilisateurs qui lancent la commande Cipher – ne peut pas être utilisé conjointement avec d'autres options
/q	Ne montre que les informations essentielles

/s	Applique les opérations spécifiées aussi sur les sous-dossiers
Nom_de_fichier	Spécifie un modèle, un fichier, un dossier

5 IPSec

Le protocole IPSec (Internet Protocol Security) permet d'assurer la protection des paquets IP. Il utilise un modèle de sécurité de bout en bout, ce qui signifie que seuls l'émetteur et le récepteur doivent avoir connaissance de la protection IPSec. Cela permet aux routeurs de ne pas avoir à implémenter ce protocole.

IPSec peut être implémenté dans un domaine Windows 2000 utilisant Active Directory ou sur une machine Windows 2000 au travers de ses réglages de Sécurité Locale. Il n'est pas disponible pour Windows 95/98 ou Windows NT 4.

IPSec est constitué de quatre protocoles. Les deux principaux sont :

- AH (Authentication Header) qui gère l'authenticité des données.
- ESP (Encapsulated Security Payload) qui gère aussi l'authenticité des données mais qui peut aussi en assurer le cryptage.

Les méthodes d'authentification supportées par IPSec sont :

- Kerberos v5
- Autorité de Certification des Clés Publiques.
- Serveur de Certificats Microsoft.
- Clés Pré partagées.

L'agent de stratégie IPSec Policy Agent est un service Windows 2000 qui tourne dans le processus lsass.exe et peut être visible dans le snap-in Services du MMC. Il est chargé et démarré à la mise en route du système et retrouve la stratégie IPSec soit dans l'Active Directory, soit dans le Registre local. Une fois que la stratégie IPSec a été obtenue, elle va être appliquée à tout le trafic IP reçu ou envoyé par cette machine.

Avant que deux ordinateurs ne puissent communiquer, ils doivent négocier une Security Association (SA Association de Sécurité). La SA définit en détail l'utilisation IPSec par ces ordinateurs, les clés employées, la durée de vie de ces clés, le cryptage et le protocole d'identification qui seront utilisés.

Quand cela s'applique à un domaine Windows 2000, les stratégies IPSec sont stockées dans l'Active Directory. Mais sans lui (l'Active Directory), elles sont enregistrées dans les clés de Registre suivantes :

Stratégie de Groupe :
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\PolicyAgent\Policy\Cache

Stratégie Locale :
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\PolicyAgent\Policy\Local

Utilisez le Moniteur IPSec (ipsecmon.exe) pour voir le statut d'IPSec sur une machine Windows 2000. L'analyseur de trames de Windows 2000 Server peut être utilisé pour voir les paquets AH et ESP. Les logs de l'agent de Stratégie IPSec sont enregistrés dans le fichier ipsecpa.log.

6 Le second service de connexion (Exécuter en tant que)

Relativement similaire à la commande su sous UNIX.

Cette commande est utilisée pour tester des réglages avec un compte particulier alors que vous êtes loggé avec un compte différent.

Sélectionner l'icône de l'application faisant un simple clic gauche. Ensuite, enfoncer la touche Shift et faire un clic droit sur l'icône. Quand le menu contextuel apparaît, sélectionner Exécuter en tant que. Cela fait apparaître une

fenêtre qui a pour nom 'Exécuter l'application en tant qu'un autre utilisateur' – entrer login/mot de passe et cliquer sur OK.

Module 10
Configuration de l'impression

1 Les périphériques d'impression locaux et en réseau

a) Terminologie

Un périphérique d'impression est ce que l'on appelle en général une imprimante, c'est à dire un matériel qui permet d'éditer des documents, de les imprimer.

Une imprimante est l'interface logicielle qu'il y a entre le périphérique d'impression et Windows.

Le serveur d'impression contient le pilote d'imprimante propre à chacun des périphériques d'impression connectés. Ce pilote est disponible dans la version de chacun des clients qui vont utiliser le serveur pour demander des travaux d'impression (Windows 95, 98, NT, 2000...).

b) Ajout d'une imprimante

Vous devez avoir les privilèges d'Administrateur afin d'ajouter une imprimante à votre serveur. L'assistant d'Ajout d'imprimante vous guide pendant tout le processus qui vous permettra de définir quel périphérique d'impression est disponible, sur quel port physique le périphérique d'impression est branché, quel pilote utiliser, ainsi que le nom du périphérique d'impression sera connu sur le réseau.

c) Partage d'une imprimante

Le partage d'une imprimante se fait dans les mêmes conditions que l'ajout d'une imprimante, c'est à dire qu'il faut être Administrateur. Un clic droit sur l'imprimante, puis Propriétés, là il faut choisir l'onglet Partage. Choisir le nom de partage de l'imprimante sur le réseau, et ensuite ajouter tous les pilotes nécessaires aux clients qui vont utiliser cette imprimante (en cliquant sur 'Pilotes supplémentaires').

✍ . Une imprimante partagée sous Windows 2000 se retrouve automatiquement publiée dans Active Directory. Si Active Directory n'est pas implémenté sur le domaine, alors les utilisateurs devront parcourir le réseau pour trouver l'imprimante partagée.

d) Partage et permissions

Une fois l'imprimante partagée, il est utile d'affecter aux « bons » utilisateurs les bonnes permissions. Pour cela, on se rend dans l'onglet Sécurité, puis on commence par supprimer le groupe Tout le Monde. Ensuite, on clique sur Ajouter, on choisit les utilisateurs et/ou les groupes voulus puis on leur affecte les permissions requises.

e) Gestion des priorités

Les priorités d'impression sont fixées en créant plusieurs imprimantes logiques qui pointent vers le même périphérique d'impression et en leur assignant individuellement des priorités. L'échelle des priorités va de 1 (la plus faible, par défaut) à 99, la plus forte.

Pour mettre en place les priorités d'une imprimante, il suffit de se rendre dans l'onglet Avancé, puis de remplir la zone 'Priorité' avec la valeur voulue.

f) Configuration des clients

Windows 2000 Professionnel télécharge automatiquement les drivers pour les clients qui tournent sous Windows 2000, Windows NT 4, Windows NT 3.51 et Windows 95/98.

g) Création d'un pool

Vous avez aussi la possibilité d'utiliser une ou plusieurs imprimantes identiques pour n'en faire qu'une seule logique. C'est le Print Pooling (Pool d'impression). Le pool d'impression ne comporte pas nécessairement que des périphériques d'impression locaux, il peut aussi comporter des périphériques d'impression munis de carte (interface) réseau.

Quand un travail d'impression sera réceptionné par le serveur, alors, il sera envoyé au premier périphérique d'impression qui sera disponible.

Pour créer un pool d'impression, il faut cette fois-ci se rendre dans l'onglet Port, puis cliquer la case 'Activer le pool d'imprimante' et enfin il ne reste plus qu'à choisir sur quels ports sont connectés les périphériques d'impression.

h) Impression Internet

L'impression Internet est une nouveauté de Windows 2000. Vous pouvez utiliser une URL pour votre imprimante. Le serveur d'impression doit être sous Windows 2000 Server disposant d'Internet Information Server ou sous Windows 2000 Professionnel disposant de Personal Web Server.

Toutes les imprimantes partagées peuvent être vues sur http://nom_de_serveur/printers.

2 Pour aller plus loin

Windows 2000 Professionnel supporte les ports d'impression suivants : Line Printer (LPT), COM, USB, IEEE 1394, et les périphériques réseaux attachés.

Windows 2000 Professionnel ne peut fournir des services d'Impression qu'à des clients Windows et UNIX. Windows 2000 Server est requis pour supporter les clients Apple et Novell.

Vous pouvez utiliser des pages de séparation pour séparer les travaux d'impression d'une imprimante partagée. Un modèle de page de séparation peut être créé et enregistré dans le dossier %systemroot%\system32 avec une extension .SEP.

Vous pouvez utiliser Recommencer dans le menu de l'imprimante pour réimprimer un document. Cela peut se réveler utile lorsque l'imprimante se bloque en cours d'impression. L'option Continuer peut être sélectionnée pour reprendre le travail là où vous l'avez arrêté.

Vous pouvez changer le dossier où se trouve le spooler d'impression dans les propriétés avancées de l'imprimante. Pour 'réparer' un spooler, vous devez arrêter puis redémarrer le service spooler dans le snap-in Services des Outils d'Administration du Panneau de configuration.

Utiliser l'utilitaire en ligne de commande fixprnsv.exe pour résoudre les problèmes de compatibilité d'imprimante.

L'activation de l'option « disponibilité » permet à l'Administrateur de spécifier à quelle heure l'imprimante est disponible.

Module 11
Installation et configuration des services Terminal Server

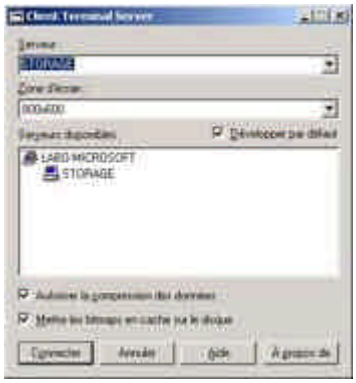
1 Fonctionnement des services de terminaux

a) Le serveur

Il permet de gérer les ressources liées à la session de chaque utilisateur. Ce dernier reçoit les frappes au clavier et les clics de souris et achemine le résultat du système d'exploitation au client approprié.

b) Le client

La session Terminal Server se présente sous la forme d'une fenêtre. L'ordinateur ou le périphérique client a uniquement besoin de la puissance de traitement nécessaire pour la connexion au serveur. Ce dernier exécute la quasi totalité des traitements. Les clients Terminal Server sont parfois appelés des clients légers (thin clients).



c) Le protocole RDP

Le protocole Remote Desktop Protocol prend en charge la communication entre l'ordinateur client et le serveur. Il est optimisé pour l'affichage des éléments de l'interface graphique sur l'ordinateur client. Il s'agit d'un protocole de la couche application qui utilise TCP/IP pour effectuer le transfert des données sur le réseau. Le protocole RDP repose sur le standard ITU T 120.

d) Installation des services Terminal Server

Deux méthodes permettent d'installer les services Terminal Server : au cours de l'installation de Windows 2000 ou après l'installation en utilisant le groupe Ajout/Suppression de programmes du Panneau de configuration.

e) Les deux modes d'installation

Lors de l'installation, vous aurez le choix entre deux modes :

- ***administration à distance*** : il va vous permettre de vous connecter sur votre serveur pour en assurer l'administration. Windows 2000 va limiter à 2 le nombre maximal de connexions.

- ***serveur d'application*** : il s'agit du mode de fonctionnement normal des services de terminaux. Ce mode va permettre à vos utilisateurs de se connecter avec pour seule limitation le nombre de licences Terminal Server (TS CAL) dont vous disposez.

f) Configuration pour l'accès client

Pour pouvoir ouvrir une session Terminal Server, les comptes de vos utilisateurs doivent être modifiés.
Dans les propriétés de comptes, onglet Profil des services Terminal Server, cochez la case Autoriser l'ouverture de session Terminal Server puis Appliquez.
Vous pouvez aussi spécifier des dossiers de base et des profils pour les utilisateurs. Vous pouvez affecter un profil à un utilisateur qui s'applique uniquement aux sessions Terminal Server. Cette procédure vous permet de créer des profils utilisateur pour l'environnement des services Terminal Server.

2 Connexion sur un serveur de terminaux

a) Installation du client des services Terminal Server

Créateur de disquettes client

Vous pouvez utiliser le créateur de disquettes client pour mettre en place vos client de serveurs de terminaux.
Il est installé parmi les Outils d'administration lorsque vous installez Terminal Server
Vous pourrez sélectionner le type de client à créer: Client Terminal Server pour Windows 16 bits (4 disquettes sont nécessaires) ou Client Terminal Server pour Windows 32 bits (2 disquettes sont nécessaires).

Téléchargement du logiciel client depuis un serveur Terminal Server

Vous pouvez rechercher les fichiers source du client des services de Terminal Server dans le dossier *Racine_système\system32\tsclient* sur le serveur Terminal Server. Ce dossier contient les sous-dossiers Net, Win16 et Win32.
Les utilisateurs peuvent ensuite lancer setup.exe à partir de l'un des dossier partagés.

Utilisation du composant ActiveX

Il vous est possible de télécharger à partir du site Microsoft un client ActiveX pour votre serveur de terminaux.

b) Etablissement d'une connexion

Lorsqu'un utilisateur se connecte, la boite de dialogue Client des services Terminal Server s'affiche. Vous pourrez y configurer la zone d'écran qui correspondra à une résolution d'affichage. Vous pouvez aussi décider d'établir une connexion à basse vitesse si vous utilisez un modem ou si le réseau est lent. Il est possible d'accélérer la vitesse de réponse en mettant en cache les bitmaps, dans ce cas, votre client va enregistrer les éléments d'affichage du bureau dans un cache local.

c) Fin d'une session Terminal Server

Les services Terminal Server permettent aux utilisateurs de mettre fin à une session Terminal Server à l'aide des deux méthodes suivantes :
Déconnexion : vos application vont continuer à s'exécuter sur le serveur. L'utilisateur peut se reconnecter au serveur et reprendre la session.
Fermeture d'une session :
La fermeture d'une session met fin à son exécution sur le serveur. Les applications exécutées au cours de la session sont fermées.

d) Gestion des licences

Un serveur de licences stocke toutes les licences des services Terminal Serveur qui sont installées pour un groupe de serveur Terminal Server.
Un domaine ou un site hébergeant des serveurs Terminal Server doivent également héberger un serveur de licences.

e) Types de licences client

Le serveur de licences gère les types de licences répertoriés ci-dessous :

Licences d'accès client pour les services Terminal Server : elles sont acquises pour des périphériques connus, autres que Windows 2000, se connectant à un serveur Terminal Server.

Licences Internet connector pour les services Terminal Server. Cette licence permet aux internautes d'utiliser de façons simultanée et anonyme un serveur Terminal Server.

Licences intégrées. Les ordinateurs clients qui exécutent Windows 2000 sont automatiquement licenciés en tant que clients des services Terminal Server.

Licences provisoires. Lorsqu'un serveur Terminal Server demande une licence et que le serveur de licences n'en a aucune à donner, une licence provisoire lui est délivrée. Le serveur de licences effectue le suivi de la délivrance et de l'expiration des licences provisoires.

f) Gestion des applications

Permet l'exécution d'une application par plusieurs utilisateurs. Son programme d'installation doit copier les fichiers vers une localisation centrale.

Vous disposez de deux méthodes pour l'installation :

Ajout/Suppression de programmes du panneau de configuration ou la commande ***change user*** à l'invite : après avoir ouvert une session en tant qu'administrateur, tapez ***change user /install*** , installez l'application puis ensuite à l'invite tapez ***change user /execute***.

Module 12
Implémentation de serveurs Windows 2000

1 Vue d'ensemble d'Active Directory

Le service Active Directory (Active Directory) permet une gestion centralisée. Cela vous donne la possibilité d'ajouter, de retirer et de localiser les ressources facilement. Il offre une avancée significative au-delà des limitations du modèle de sécurité du domaine Windows NT.

Ainsi, nous avons :

- **Une administration simplifiée**: Active Directory offre une administration de toutes les ressources du réseau d'un point unique. Un administrateur peut se loguer sur n'importe quel ordinateur pour gérer les ressources de tout ordinateur du réseau.

- **Une mise à l'échelle**: les domaines NT 4 ont une limitation pratique de 40 000 objets. Active Directory repousse cette limite à plusieurs millions si cela est nécessaire.

- **Un support standard ouvert**: Active Directory utilise DNS pour nommer et de localiser des ressources, ainsi les noms de domaine Windows 2000 sont aussi des noms de domaine DNS. Active Directory fonctionne avec des services de clients différents tels que NDS de Novell. Active Directory supporte le http. Cela signifie qu'il peut chercher les ressources au travers d'une fenêtre d'un browser web. De plus, le support de Kerberos 5 apporte la compatibilité avec les autres produits qui utilisent le même mécanisme d'authentification.

2 Structure d'Active Directory

La structure d'Active Directory est hiérarchique, elle se décompose comme suit :

- **Objet** : représente une ressource du réseau qui peut-être par exemple un ordinateur ou un compte utilisateur.

- **Classe** : groupement logique d'objet tels les comptes d'utilisateurs, ordinateurs, domaines, ou unités organisationnelles.

- **Unité organisationnelle (OU)** : container utilisé pour organiser les objets d'un domaine à l'intérieur de groupes administratifs logiques tels les ordinateurs, les imprimantes, les comptes d'utilisateurs, les fichiers partagés, les applications et même d'autres unités organisationnelles.

- **Domaine** : chacun des objets d'un réseau existe dans un domaine et chaque domaine contient les informations des objets qu'il contient. Un domaine est sécurisé, c'est à dire que l'accès aux objets est limité par des ACL (Access Control List). Les ACL contiennent les permissions, associées aux objets, qui déterminent quels utilisateurs ou quels types d'utilisateurs peuvent y accéder. Dans Windows 2000, toutes les stratégies de sécurité et les configurations (telles les droits administratifs) ne se transmettent pas d'un domaine à l'autre. L'administrateur de domaine peut déterminer les stratégies uniquement à l'intérieur de son propre domaine.

- **Arbre** : c'est un groupement ou un arrangement hiérarchique d'un ou plusieurs domaines Windows 2000 qui partagent des espaces de noms contigus (par exemple : administration.supinfo.com, comptabilité.supinfo.com, et training.supinfo.com). Tous les domaines d'un même arbre partagent le même schéma commun (la définition formelle de tous les objets qui peuvent être enregistrés dans une architecture d'Active Directory) et partagent un catalogue commun.

- **Forêt** : c'est un groupement ou un arrangement hiérarchique d'un ou plusieurs arbres qui ont des noms disjoints (par exemple : laboratoire-microsoft.org et supinfo.com). Tous les arbres d'une forêt partagent le même schéma commun et le même catalogue, mais ont des structures de noms différentes. Les domaines

d'une forêt fonctionnent indépendamment les uns des autres, mais les forêts permettent la communication d'un domaine à l'autre.

?? **Sites** : combinaison d'une ou plusieurs IP de sous réseau connectés par des liens à hauts débits. Ils ne font pas partie d'un espace de nommage d'Active Directory, et ils contiennent seulement les ordinateurs, les objets et les connexions nécessaires pour configurer la réplication entre sites.

3 Réplication de sites

Un contrôleur de domaine est un ordinateur sous Windows 2000 Server qui contient une réplique de l'arborescence du domaine (ce n'est pas le cas des serveurs membres). Active Directory utilise une réplication *multimaîtres*, c'est-à-dire qu'aucun contrôleur de domaine n'est contrôleur principal de domaine, tous les contrôleurs de domaine sont au même niveau.

Disposer de plus d'un contrôleur de domaine dans un domaine permet la tolérance de panne. Si un contrôleur de domaine tombe en panne, un autre est capable de continuer à authentifier les demandes de connexion et d'assurer les services demandés grâce à sa copie de l'Active Directory.

Les informations de l'Active Directory sont répliquées entre les contrôleurs de domaines (DC) et assurent que les changements effectués sur un contrôleur seront répliqués sur les autres contrôleurs du domaine. Le contrôleur de domaine garde une copie de toutes les informations contenue dans l'annuaire Active Directory de son domaine. Il gère les changements et se charge aussi de répliquer ces changements aux autres contrôleurs du même domaine. Les contrôleurs de domaine dupliquent eux-même tous les objets du domaine vers les autres contrôleurs du même domaine. Quand vous modifiez des informations dans Active Directory, vous effectuez ces changements sur un seul des contrôleurs de domaine.
La réplication est automatique et utilise une topologie en anneau pour s'effectuer dans un même domaine et un même site. L'anneau assure que si un contrôleur de domaine est en panne, il y aura quand même une possibilité de répliquer ses informations vers les autres contrôleurs de domaine.

Les administrateurs peuvent spécifier le nombre de réplications faites, l'heure a laquelle elles s'effectuent ainsi que la quantité d'information pouvant être transmise.

Les contrôleurs de domaine répliquent immédiatement les changements tels que la désactivation d'un compte utilisateur.

4 Concepts de l'Active Directory

a) Schéma

Il contient une définition formelle du contenu et de la structure de Active Directory tel que les attributs, les classes et les classes de propriétés. Pour une classe d'objet, le schéma est : quels attributs l'instance d'une classe doit posséder, quels attributs additionnels sont autorisés et quelle classe d'objet peut être son parent.
Installer Active Directory sur le premier ordinateur d'un réseau crée le domaine et le schéma par défaut contiendra les objets fréquemment utilisés. Des extensions peuvent être ajoutées au schéma lorsque cela est nécessaire. Par défaut, l'accès en écriture au schéma est limité aux membres du groupe Administrateurs.

b) Catalogue Global

C'est là que sont stockées les informations liées aux objets d'un arbre ou d'une forêt. Active Directory crée automatiquement un catalogue global à partir des domaines qui composent l'Active Directory par le processus de réplication. Les attributs stockés dans le catalogue global sont ceux qui font le plus souvent l'objet de requête dans les opérations de recherche (tels que les noms d'utilisateurs, les noms de login, etc.) et sont utilisés pour localiser une réplique exacte de l'objet. Pour ces raisons, le catalogue global peut être utilisé pour trouver des objets partout sur le réseau sans besoin de réplication entre les contrôleurs de domaine.

5 Convention de nomenclature d'Active Directory

?? **Nom Distinct (DN)** : chacun des objets d'Active Directory dispose du sien. Il identifie de manière unique un objet et contient assez d'information pour qu'un client de l'Active Directory puisse le retrouver dans l'Active Directory. Il inclue le nom de domaine qui contient l'objet ainsi que le chemin complet pour se rendre jusqu'à lui. Les noms distincts doivent être UNIQUES, Active Directory n'acceptera pas de doublons.

?? **Nom Relatif Distinct (RDN - Relative Distingushed Name)** : si le nom distinct est inconnu, vous pouvez chercher un objet par ses attributs. Le nom relatif distinct est une partie du nom qui est un attribut de l'objet lui-même (par exemple, Michel Dupont pourrait avoir *CN = Michel Dupont* comme RDN).

?? **Identifiant Global Unique (GUID - Globally Unique Identifier)** : c'est un nombre de 128 bits unique assigné à l'objet lorsqu'il est créé. Cette valeur ne change JAMAIS même si l'objet est renommé ou déplacé. Ce numéro peut être utilisé pour localiser l'objet.

?? **Nom Principal d'Utilisateur (UPN - User Principal Name)** : c'est le nom donné à un compte utilisateur (par exemple labo-microsoft@supinfo.com).

Module 13
Services d'accès a distance (RAS – Remote Access Services)

Les services d'accès à distance de Windows 2000 intègrent les fonctionnalités d'accès distant ainsi que des fonctionnalités de routage.

1 Protocoles d'authentification

EAP (*Extensible Authentication Protocol*) : il s'agit d'un complément du protocole PPP permettent à ce dernier la prise en charge de nouvelles méthodes d'authentification (cartes à puces par exemple). MD5-CHAP et EAP-TLS sont deux exemples d' EAP.

EAP-TLS (*Transport Level Security*) : utilisé en particulier pour les certificats digitaux. Avec EAP-TLS, le serveur et le client doivent s'authentifier mutuellement.

MD5-CHAP (*Message Digest 5 Challenge Handshake Authentication Protocol*): crypte les logins et les mots de passe avec un algorithme MD5.

RADIUS (*Remote Authentication Dial-in User Service*): spécification pour l'authentification distante de constructeurs indépendants. Windows 2000 Professional ne peut être QUE client RADIUS.

MS-CHAP v1 et v2 (*Microsoft Challenge Handshake Authentication Protocol*): crypte la session complète, contrairement a MD5-CHAP. La version 2 est supportée par Windows 9x/Me, NT4 et 2000 pour les connexions VPN. MS-CHAP ne peut pas être utilisé par des clients non-Microsoft.

SPAP (*Shiva Password Authentication Protocol*) : utilisé par les clients Shiva LAN Rover. Il crypte le mot de passe, mais pas les données.

CHAP (*Challenge Handshake Authentication Protocol*) :crypte le login, le mot de passe mais pas les données. Il peut fonctionner avec les clients non-Microsoft.

PAP (*Password Authentication Protocol*) : il envoie le login et le mot de passe en clair.

2 Réseau Privé Virtuel (VPN - Virtual Private Network)

La mise en place d'un VPN nécessite l'un de ces protocoles :

PPTP (*Point to Point Tunneling Protocol*) : il crée un tunnel crypté au travers d'une liaison réseau jugée peu sûre (du point de vue de la confidentialité des informations qui y transitent).

L2TP (*Layer Two Tunneling Protocol*): il fonctionne comme PPTP car il crée un tunnel, mais il ne propose pas le cryptage des données. La sécurité est mise à disposition par le biais de technologies comme IPSec.

Voici un comparatif des fonctionnalités de chacun d'entre eux :

Caractéristiques	PPTP	L2TP
Compression d'en-tête	Non	Oui
Authentification du tunnel	Non	Oui
Cryptage intégré	Oui	Non
Transmission sur des réseaux basés sur IP	Oui	Oui
Transmet sur des réseaux basés sur UDP, Frame Relay, X.25 ou ATM	Non	Oui

3 Support Multi-lien (Multilink support)

Le mutli-lien vous permet de combiner un ou plusieurs modems ou adaptateurs ISDN en un lien logique qui augmentera la bande passante.

BAP (Bandwidth Allocation Protocol) et BACP (Bandwidth Allocation Control Protocol) améliorent le multilinking en augmentant et diminuant de manière dynamique la bande passante. Les caractéristiques sont configurées au travers des stratégies du RAS.

Il est activé depuis l'onglet PPP de la boîte de dialogue Propriétés du serveur RAS.

4 Configurer la sécurité du rappel (Callback)

L'utilisation du rappel permet la prise en charge des frais téléphoniques de l'utilisateur qui se connecte a distance par la société. C'est aussi un moyen d'accroître la sécurité (rappel a un numéro prédéfini).
Pour faciliter l'utilisation de l'accès a distance par des itinérants (tels les VRP),il faudra pourtant choisir l'option« Permettre à l'appelant de fixer le numéro de rappel » (sécurité moindre).

5 Accès réseau à distance

La documentation technique de Microsoft se réfère en général à *Accès Réseau à Distance* lorsque l'on parle de connexion vers l'extérieur. Les connexions entrantes sont connues sous le nom de Remote Access Services (RAS).

Toutes les nouvelles connexions sont ajoutées via l'assistant « Nouvelle connexion ».

Pour créer une connexion VPN, choisir Numéroter vers un réseau privé, spécifier si vous devez établir une liaison par un provider avant, entrer le nom d'hôte ou l'adresse IP de l'ordinateur/du réseau auquel vous voulez vous connecter, et enfin spécifier si la connexion est pour votre profil uniquement ou pour tout le monde.

Ces entrées peuvent être créées pour des connexions modem, LAN, lien direct par câble, et infrarouge.
PPP est choisi en général parce qu'il supporte de nombreux protocoles, cryptages et l'attribution dynamique d'adresse IP. SLIP est un protocole plus ancien qui ne supporte que TCP/IP.

Toutes les connexions réseau, entrantes et sortantes, sont représentées par des icônes séparées et toutes les options peuvent être configurées de manière individuelle.