Sommaire

I. Présentation générale

A. Un accouchement dans la douleur

1992 : Naissance de Cairo, système entièrement objet
1993 : lancement de Windows NT 3.1
1994 : lancement de NT 3.51
1995 : sortie de NT 4
Août 1995 : Windows 95
1995 : Microsoft envisage des versions beta pour 1996 du successeur de Windows NT 4
1996 : Cairo assemble les technologies de NT4 et NT 5. Est abandonné le projet d'annuaire global. Microsoft opte pour un mélange de X500 et de DNS. Cairo est conçu comme un ensemble de technologies s'appuyant sur Nt.
1997 : Cairo devient NT5. NT5 est prévu pour fin 1998
Août 1998 : Windows 98
Septembre 1998 : première version beta de NT5. Nom de code : Memphis
Octobre 1998 : NT5 s'appellera Windows 2000. Il n'est plus question de concurrencer Unix Sur le haut de Gamme. Bille revoit ses ambitions à la baisse !
1998 : Moshe Dunie, chef du développement de Windows 2000, prend une année sabbatique
Mars 1999 : il n'est plus question de fusionner les noyaux Windows 98 et Nt
Juillet 1999 : Windows 98 Se
Août 1999 : Windows 2000 n'est prévu que pour des processeurs X86
Septembre 1999 : Data Center est prévu pour mi-2000
Février 2000 : Windows 2000
Mi-2000 : Millenium

B. Les caractéristiques du système d'exploitation

Multitâche préemptif
Multithreading : le thread est une micro-tâche à l'intérieur d'un espace mémoire commun au process parent qui représente l'application.
Multiprocessing : dans le mode asymétrique, un processeur peut être dédié au fonctionnement du système alors que d'autres peuvent être dédiés au fonctionnement des applications ; dans le mode symétrique, la charge est répartie entre les différents processeurs. Pour sa part Windows 2000 ne gère que le SMP
Adressage 32 bits
Un système à 4 neufs : 99.99%, soit une heure d'indisponibilité par an. Le Cabinet Aberdeen Group a démontré que Windows 2000 Server assure un fonctionnement continu sur 99.95% du temps annuel.

C. Les technologies utilisées

1. Les nouveautés du système

- Prise en charge de l'architecture WDM (Windows Drivers Model) : 6500 périphériques pris en compte. Les pilotes, sur option, doivent être certifiés.
- Intégration de DNA : Distributed iNternet Applications, reposant lui-même sur COM (Component Object Model)
- Gestion de la mémoire EMA (Enterprise Memory Architecture) : Windows 2000 gère aujourd'hui jusqu'à 32 Go de mémoire contre 4 Go pour son prédécesseur.
- Prise En charge du Plug And Play, de l'USB et de la gestion de l'énergie fondée sur la technologie ACPI (Advanced Configuration and Power Interface)
- Sysprep : cet utilitaire vous offre la possibilité de cloner en régénérant le SID (l'indentificateur de sécurité) au réamorçage du PC
- Prise en charge de FAT16, FAT32, NTFS4, NTFS5
- EFS (Encrypting File System) : cryptage en mode NTFS5 utilisant des clés symétriques pour crypter et décrypter. Ls clés Sont cryptés par le certificat X.509 V3 de l'utilisateur.
- Prise en charge du multi-écrans : 10 maximum
- Windows File Protect : l'utilitaire SFC vous permet de régler le niveau de protection de votre système et de purger le répertoire %windir%\SYSTEM32\DLLCACHE qui contient tous les fichiers de secours (DLL, pilotes)
- L'équilibrage de charge au sein des clusters est assuré par les fonctions NLB (Network Load Balancing) et CLB (Components Load Balancing).

2. L'implémentation de nouvelles technologies réseaux

- Kerberos (RFC 1510) : c'est le mode d'authentification utilisé par 2000 Pro. Vous pouvez désactiver NTLM (Netbios) qui utilisent les ports 137,138,139. Dans ce cas, les autres machines ne peuvent plus s'y connecter sauf à utiliser ftp et http ou nfs via les SFU.
- Active Directory : technologie d'annuaire implémentée dans Windows 2000 Server concurrençant Novell Directroy Services et eDirectory de Novell. Les limites de l'annuaire sont de plusieurs millions d'objets… en relation avec la puissance du système !!!
- Intellimirror
- Prise en charge d'IPP (Internet Printing Protocol
- DFS (Système de fichiers distribués) : module de recherche des ressources partagés à partir du poste client
- Serveur DDNS : avec le serveur DHCP fourni avec Windows 2000 Server, l'enregistrement des clients lors D'une mise à jour de Leur adresse Ip auprès du serveur DNS peut se faire automatiquement.
- Gestionnaire de sites
- Prise en charge des VPN (Virtual Private Network) : le transit des paquets IP dans le tunel est assuré par les protocoles PPTP (Point to Point Tuneling Protocol) ou L2TP (Layer 2 Tunneling Protocol) ; l'authentification passe par le service RADIUS (Remote Authentification Dial In User Service)
- IPSec : le pilote réseau permet de crypter tout le trafic réseau. Il est fortement conseillé au niveau des VPN qui relient deux nœuds distants
- Implémentation du protocole IPP (Internet Printing Protocol) : avec votre liaison distante sécurisée, vous pouvez imprimer de votre domicile sur l'imprimante de Votre bureau.
- Service RIS (Remote Installation Service) : outil de déploiement de Windows 2000 Pro qui permet à partir d'une disquette bootable ou d'une PROM d'une carte réseau de procéder à l'installation à distance.
- Prise en charge de RIP2 (Routing Internet Protocol) adapté aux petits réseaux et de OSPF (Open Shortest Path First) adapté lui aux grands réseaux
- Terminal Server : aujourd'hui, avec l'adjonction de cette technologie, vous transformez votre serveur en un véritable serveur d'applications bureautique et diminuant le TCO
- ARAP (Appletalk Remote Access Protocol) : serveur d'accès distant pour clients Mac
- Relations d'approbations transitives

D. L'offre

- Windows 2000 Pro : 4Go de Ram, 2 processeurs
- Windows 2000 Server : 4 Go de mémoire, 4 processeurs
- Windows 2000 Advanced Server : 4 processeurs par nœud, prise en charge des clusters, de 8Go de mémoire, 8 processeurs par nœud, 2 noeuds
- Windows 2000 Datacenter Server : 32 processeurs par grappe, 64 go de Ram en s'appuyant sur la technologie PAE (Physical Address Extension), 8 processeurs par noeud, implémentation de la technologie OLPT (On Line Processing Transaction)

II. Installation et déploiement

A. La liste du matériel compatible

Consultez le site http://www.microsoft.com/hcl/default.asp ou alors les documents mis à jour au niveau du site ftp://ftp.microsoft.com/services/whql/HCL/ .
Vous pouvez lire le fichier HCL.TXT présent sur le CDROM.

B. Remarques préliminaires à l'installation

Au niveau du Bios auquel vous accédez généralement par la touche Suppr lors de la mise sous Tension, pensez à désactiver l'antivirus. Eventuellement, désactivez tous les ports inutilisés : USB, COM1, COM2, LPT1 ou PS/2.
Pour ma part, afin de bénéficier des outils de réparation fournis par Winternals, j'installe un Windows 98Se sur une première partition de 2 Go en Fat16. A vous de voir !!! Mais, pour d'anciens périphériques non reconnus par Windows 2000, Windows 98 peut vous offrir une Véritable solution.

C. Générer les disquettes de boot

Sur le CDROM, recherchez le fichier makeboot.bat. Double-cliquez sur ce programme. Il vous faudra quatre disquettes.

D. Mise à jour de votre système

Winnt32 /checkupgradeonly Permet de connaître la liste du matériel compatible au niveau du système à mettre à jour.

E. Les programmes d'installation

WINNT.EXE
WINNT32.EXE

F. Remarques sur le système de fichier

Pour installer Active Directory, vous devez disposer d'une partition NTFS. En cas d'oubli, vous pourrez sous Windows 2000 taper convert lecteur : /FS :NTFS

G. La console de récupération

1. Installation

Winnt32.exe /cmdcons

2. Réparations possibles

- Créer, éditer ou copier le fichier boot.ini : vous disposez de la commande attrib
- MBR écrasé ou endommagé : utiliser fixmbr (identique à fdsik /mbr). Vous pouvez employer fixboot pour recharger l'adresse du lanceur dans le MBR.
- Restituer les ruches dans %systemroot%\system32\config
- Désactiver un service défaillant : Listsvc permet de lister tous les services. Disable vous offre la possibilité de désactiver tel ou tel service.
- Altération d'un fichier ou d'un disque : employer chkdsk
- Défaillance créé par un événement : démarrer en mode sécurisé et utiliser la commande type.

3. Autres Commandes

Diskpart	permet le partitionnement de votre disque
Enable	Permet de lancer un service
Exit	Redémarre la console
Expand	Décompresse un fichier à partir d'un fichier cab
Format	Formatage format g:/Q FS :fat32
Logon	Connexion à une autre partition
Map	liste toutes les lettres d'unité associées aux partitions
Systemroot	fixe le répertoire courant comme étant le répertoire de Windows Nt (généralement c:\winnt)

H. Utilisation de SYSPREP

1. Commutateurs de Sysprep

-quiet Force sysprep Quelque soit le type de licence
- reboot Permet de rebooter
- quiet Mode silencieux

2. Paramètres de Sysprep

OemSkipEula Désactive la Eula (End User License Agreement)
ProductID Affiche l'identité du produit
Fullname Nom de l'utilisateur
Orgname Nom de l'organisation
ComputerName Nom de la machine
AdminPassword Mot de passe administrateur
OEMBannerText Chaîne à afficher en haut à gauche de l'écran
OEMLogoBitmapFile Affiche une image bitmap en haut à droite de l'écran
OEMBackGroundBitmapFile Affiche une image en arrière-plan
OEMSkipWelcome Affiche la page d'accueil
OEMNoWaitAfterGUIMode Rédémarre automatiquement
NoSidGen Désactive le générateur de SID automatique
, employez le commutateur -defeat.

I. Clonage

Après avoir installé Windows 2000 et après avoir utilisé SYSPREP, vous pouvez employer les outils de clonage tel que :
Powerquest Drive Image pro
Symantec Norton Ghost
Altiris Rapideploy
Storagesoft ImageCast

J. Mise à jour

L'emploi de Windows Update pose plus de problèmes qu'il en résout :
Des informations confidentielles sont transmises au serveur Microsoft
Le trafic réseau peut augmenter et être fortement pénalisés par des mises à jour en série.
Pensez à désactiver cette fonction en désinscrivant les DLL

K. Remarques sur le mode sans échec

En mode sans échec, le fichier ntbtlog.txt est créé dans %systemroot%
Dans ce mode, l'USB n'est pas pris en charge. Donc… gare aux souris et aux claviers full USB !

L. Les fichiers de log

Setupact.log : liste des fichiers copies lors de l'installation
Setuperr.log : liste des erreurs durant l'installation
Setupapi.log : liste des pilotes copiés Durant l'installation
Setuplog.txt, : infos supplémentaires sur les pilotes

M. Setup Manager

A l'instar de Windows NT 4, le Resource Kit pour windows 2000 fournit l'outil SetUp Manager qui permet de générer les fichiers de réponse automatique unattended.txt.

N. Installation via RIS (Remote Installation Services)

1. Présentation

A base d'architecture PXE (Preboot Execution Environment) qui fait partie de l'initiative d'Intel WfM (Wired for Management), le service RIS permet à une machine disposant d'une simple carte réseau doté d'une PROM. Il ne fonctionne que sous Active Directory. Vous devez disposer d'un serveur Dhcp. Après obtention de l'adresse Ip, le serveur envoie via le protocole TFTP (Trivial FTP) une image contenant le programme d'amorçage.

2. Installation du serveur RIS

Ajoutez le composant parmi des composants Windows.

3. Configuration

Exécutez risetup.exe.

4. Créer une disquette de boot

Rbfg.exe (Remote Boot Floppy Generator)

5. Image des machines par riprep.exe

O. Le boot

1. Les chemins ARC multi(W)disk(X)rdisk(Y)partiton(Z)

Parameter	Multi Parameter Definitions
W	The number of the adapter, usually 0.
X	Always 0.
Y	The number for the disk on the adapter, usually between 0 and 3.
Z	The partition number. All partitions that are in use receive a number. Primary partitions are numbered before logical drives. The first valid number for Z is 1; W, X, and Y start at 0.

2. Les commutateurs du fichier boot.ini

/PAE	Indique à NTLdr de charger NtKrnLpa.exe qui est une version x86 du noyau qui sait utiliser les extensions d'adresses physiques d'Intel (Physical Address Extensions, PAE) même quand un système a une mémoire vive inférieure à 4Go. Les PAE permettent au x86 d'adresser jusqu'à 64Go de mémoire, mais les systèmes d'exploitation destinés à travailler au dessus de 4Go doivent être entièrement refaits, car 4Go est la limite standard pour les x86. Le noyau PAE de Windows 2000 possède des adresses physiques aux pilotes de 64 bits, ce paramètre est donc utile pour tester les pilotes sur des systèmes dotés de beaucoup de mémoire.
/NOPAE	Indique à NTLdr de charger la version non-PAE du noyau de Windows 2000, même si le système prend en charge les extensions PAE et possède plus de 4Go de mémoire vive.
/NOLOWMEM	/PAE doit être activé et le système doit posséder plus de 4Go de mémoire vive. La version PAE du noyau de Windows 2000 n'utilisera pas les 4 1ers Go de mémoire vive. Tous les pilotes et programmes seront chargés au dessus des 4 1ers Go. Utile pour tester les pilotes sur des systèmes dotés de beaucoup de mémoire.
/NOGUIBOOT	Empêche l'initialisation du pilote VGA qui affiche les images graphiques lors du démarrage de Windows 2000. Le pilote sert à afficher des informations sur l'évolution du processus de démarrage et à afficher les écrans bleus des traps. Désactiver ce pilote aura donc aussi pour conséquence d'empêcher NT d'afficher les traps.
/FASTDETECT	Si vous utilisez un gestionnaire d'amorçage pour choisir entre Windows NT 4.0 et Windows 2000, le processus de démarrage utilise NTDetect.com. Dans Windows 2000, ce sont les pilotes de périphériques plug and play qui détectent les ports série et parallèles, mais Windows NT 4.0 s'attend à ce que ce soit NTDetect.com qui s'occupe de cette détection. /FASTDETECT indique à NTDetect.com d'ignorer la détection de ces périphériques pour Windows 2000. Si vous omettez /FASTDETECT, NTDetect.com recherche les ports série et parallèles pour Windows NT 4.0. L'installation de Windows 2000 reconnaît les configurations dual boot et paramètre /FASTDETECT pour Windows 2000.
/BOOTLOG	Indique à Windows NT de générer un fichier journal du démarrage dans %SystemRoot% \NTBtLog.txt. Les entrées du journal détaillent les pilotes chargés ou non lors du démarrage. Voici un exemple de journal Loaded driver \WINNT\System32\ntoskrnl.exe Loaded driver \WINNT\System32\hal.dll

	Loaded driver \WINNT\System32\bootvid.dll Loaded driver pci.sys Loaded driver isapnp.sys Loaded driver intelide.sys
/SAFEBOOT:	Vous ne devriez jamais avoir à indiquer cette valeur à la main puisque NTLdr le fait pour vous quand vous utilisez F8 pour démarrer en mode sans échec. A la suite du double point dans le paramètre, vous devez indiquer MINIMAL, NETWORK, ou DSREPAIR. MINIMAL : Mode sans échec sans support réseau, NT charge uniquement les pilotes et services qui apparaissent dans la sous-clé HKLM \System \CurrentControlSet \Control \SafeBoot NETWORK : Mode sans échec avec support réseau DSREPAIR : Directory Services Repair permet de restaurer NT à partir d'une sauvegarde dont vous disposez ALTERNATESHELL : Indique à Windows NT de charger l'interface graphique indiquée dans HKLM \System \CurrentControlSet \SafeBoot \AlternateShell à la place d'Explorer.exe
/PERFMEM= /PERFPAGES=	Ces paramètres ont peu de chances d'être implémentés dans le version finale de Windows 2000 car il servent à faire des tests de mémoire. Il ne faut pas indiquer les 2 paramètres en même temps. Voir le transcript sur le site de Microsoft du 2 février 1999. PERFMEM : Indique la quantité de mémoire en Mo à réserver PERFPAGES : Indique le nombre de pages mémoire à réserver
/INTAFFINITY	Indique à la HAL multiprocesseur HALMPS.dll de paramétrer les interruptions de manière à ce que seul le processeur au nombre le plus élevé d'un SMP reçoive des interruptions. Sans ce paramètre, la HAL permet à tous les processeurs de recevoir des interruptions.
/MAXPROCS PERCLUSTER=	La HAL multiprocesseur HALMPS.dll de Windows 2000 peut travailler avec des multiprocesseurs faits de minuscules clusters de petits multiprocesseurs regroupés ensemble. Dans un système 8-way faits de 2 clusters 4-way, il faut indiquer l'ID de chaque processeur à la HAL d'une façon orientée cluster. La taille maximum d'un cluster est 4. La taille par défaut est 0 (le système n'est pas basé sur des clusters).
/TIMERES=	La résolution par défaut est de 7.8ms. Sur la HAL multiprocesseur HALMPS.dll, cette option paramètre l'horloge système. L'argument est un nombre de centaines de nanosecondes, mais le système va choisir la valeur la plus élevée supportée par la HAL. La HAL supporte les résolutions ci-dessous. Centaines de nanosecondes 9766 19532 39063 78125
/YEAR=	Permet de rendre certains BIOS compatibles an 2000. Oblige l'horloge interne de Windows NT à ignorer l'heure de l'horloge en temps réel du BIOS et à utiliser celle indiquée. Cette modification affecte toutes les applications installées sur le système, y compris le noyau de Windows NT. Disponible à partir de Windows NT 4.0 Service Pack 4 ou de Windows 2000.
/CLKLVL	Indique à la HAL x86 multiprocesseur HALMPS.dll de se configurer pour une horloge système level-sensitive au lieu d'une horloge edge-triggered.
/USE8254	Destiné aux BIOS anciens, indique à la HAL d'utiliser le chip d'horloge 8254.

	Voir l'article KB Q169-9-01 pour de plus amples informations.
/MAXMEM=	Indique à Windows NT de limiter l'utilisation de la mémoire vive à la quantité indiquée en Mo.
/BURNMEMORY=	Indique à Windows NT d'ignorer la quantité de mémoire vive indiquée en Mo.
/ONECPU	Limite à 1 le nombre de processeurs utilisés sur une machine multiprocesseur.
/NUMPROC=	Indique à Windows NT de n'utiliser que le nombre de processeurs indiqués sur une machine multiprocesseur.
/SOS	Imprime un journal des pilotes chargés lors du démarrage.
/BASEVIDEO	Utilise le pilote VGA lors de l'ouverture de l'interface graphique.
/NODEBUG	Empêche l'initialisation du débogage en mode noyau. Annule les paramètres /DEBUG, /DEBUGPORT et /BAUDRATE.
/CRASHDEBUG	Charge le débogueur du noyau au démarrage. Le débogueur reste inactif sauf si une erreur se produit. Permet de rendre disponible un port COM pendant que la machine tourne.
/DEBUG	Active le débogage en mode noyau.
/DEBUGPORT=	Active le débogage en mode noyau et indique le port COM sur lequel est connecté le debogee.
/BAUDRATE=	Active le débogage en mode noyau et indique le taux en bauds auquel sera connecté le debogee, 19200 par défaut.
/BREAK	Provoque une pause de la HAL lors de l'initialisation. La 1ère chose que fait Windows NT au démarrage est d'initialiser la HAL, donc cet arrêt a lieu au tout début du démarrage du système. La HAL attendra indéfiniment jusqu'à ce qu'une connexion avec un débogueur ait eu lieu. Sans /DEBUG, ce paramètre provoque un trap de code STOP 0x00000078 (PHASE0_EXCEPTION).
/KERNEL= /HAL=	Permet de choisir d'autres fichiers comme fichiers images à la place de NTOSKrnl.exe dans %SystemRoot% \System32 et de HAL.dll. Utile pour tester des pilotes dans un environnement au noyau vérifié ou libre. Pour démarrer dans un environnement avec un noyau et une HAL vérifiés, procédez comme suit : 1. Copiez la version vérifiée du noyau de votre CD vers %SystemRoot% \System32, en la renommant NTOSkChk.exe. Sur une machine uni processeur copiez NTOSKrnl.exe, sinon copiez NTKrnlMP.exe. 2. Copiez la version vérifiée de la HAL de votre CD vers %SystemRoot% \System32, en la renommant HalChk.dll. Pour savoir quelle HAL copier, ouvrez %SystemRoot% \Repair \Setup.log. Recherchez HAL.dll, vous trouverez une ligne du genre \WINNT\System32\HAL.dll="HALMPS.dll","1a01c". Le nom qui figure à droite su signe égal est le nom de la HAL à copier. 3. Dans Boot.ini, indiquez une chaîne qui précise que cette option démarre dans un environnement vérifié. 4. Ajoutez ces paramètres dans la nouvelle option. /KERNEL=NTOSKCHK.EXE /HAL=HALCHK.DLL
/3GB	Apparu dans le Service Pack 3, permet de répartir la mémoire de façon différente. Avec /3GB : 2Go utilisateur + 2Go système Sans /3GB : 3Go utilisateur + 1Go système Donner plus d'espace mémoire aux applications gourmandes en mémoire comme les bases de données améliore leurs performances. Conditions : le système doit faire partie de Windows NT Enterprise Suite, ce qui n'est pas le cas du SP3. L'application doit comporter le label 3GB-aware. Voir l'article KB Q171-7-93 pour de plus amples informations.
/WIN95	Ce paramètre est pertinent sur un système triple-boot DOS, Windows 95 et Windows NT. Indique à NTLdr de booter sur le secteur DOS de BootSect.w40. Voir l'article KB Q157-9-92 pour de plus amples informations.
/WIN95DOS	Ce paramètre est pertinent sur un système triple-boot DOS, Windows 95 et Windows NT. Indique à NTLdr de booter sur le

	secteur DOS de BootSect.dos. Voir l'article KB Q157-9-92 pour de plus amples informations.
/PCILOCK	Empêche Windows NT d'attribuer dynamiquement des adresses I/O ou des interruptions IRQ aux périphériques PCI et conserve les paramétrages du BIOS. Voir l'article KB Q148-5-01 pour de plus amples informations.
/NOSERIALMICE =[COMx | COMx,y,z...]	Désactive la détection des souris sur le port COM indiqué. A utiliser si un périphérique autre qu'une souris est connecté sur ce port. L'utilisation de /NOSERIALMICE sans indiquer de port COM désactive la détection des souris sur tous les ports COM. Voir l'article KB Q131-9-76 pour de plus amples informations.
/SCSIORDINAL:	L'ajout d'un périphérique SCSI sur le système peut provoquer un changement d'ID SCSI si vous avez déjà un contrôleur SCSI embarqué sur votre carte mère. Indique à Windows NT l'ID du contrôleur SCSI. Voir l'article KB Q103-6-25 pour de plus amples informations.
/BASEVIDEO	The computer starts up using the standard VGA video driver. If you have installed a new video driver and it is not working correctly, you can select the Windows 2000 entry with this switch to start the computer and change to a different driver.
/BAUDRATE=nnnn	Specifies the baud rate to be used for debugging. The default baud rate is 9600 if a modem is attached, and 19200 for a null-modem cable. Including this switch in the Boot.ini file causes the /DEBUG switch to activate.
/CRASHDEBUG	The debugger is loaded when you start Windows 2000, but remains inactive unless a kernel error occurs. This switch is useful if you are experiencing random kernel errors.
/DEBUG	The debugger is loaded when you start Windows NT, and can be activated at any time by a host debugger connected to the computer. Use this switch when you are debugging problems that are regularly reproducible.
/DEBUGPORT= comx	Specifies the communications port to use for debugging, where x is the communications port that you want to use. Including this switch in the Boot.ini file causes the /DEBUG switch to activate.
/MAXMEM:n	Specifies the maximum amount of RAM that Windows 2000 can use. Use this switch if you suspect that a memory chip is bad.
/NODEBUG	No debugging information is being used.
NUMPROC=x	Allows you to force a multiprocessor computer to start up with < n processors.
/FASTDETECT =[COMx | COMx,y,z...]	Turns off serial and bus mouse detection in NTDETECT. Use this switch if you have a component other than a mouse attached to a serial port during the startup process. If you use /FASTDETECT without specifying a communications port, serial mouse detection is disabled on all communications ports.
/SOS	Displays the device driver names as they are being loaded. Use this switch when startup fails (while loading drivers), to determine which driver is triggering the failure.
/PAE	Specify the /PAE switch with the corresponding entry in Boot.ini to allow a computer that supports physical address extension (PAE) mode to start normally. In safe mode, the computer starts using normal kernels even if the /PAE switch is specified.
/NOGUIBOOT	Démarrage en mode texte (renommez bootfont.bin)
/BOOTLOG	Démarrage en générant le fichier BOOTLOG.TXT
/SAFEBOOT	/SAFEBOOT:MINIMAL /SAFEBOOT:NETWORK /SAFEBOOT:MINIMAL(ALTERNATESHELL)
/BOOTLOG	Création d'un fichier journal
/FASTDETECT	Paramètre standard pour la détection des périphériques principaux.

	Si la souris n'est pas détectée (p.ex.), supprimer ce paramètre.
/NOGUIBOOT	Désactivation de l'interface graphique au démarrage
/SAFEBOOT:<type>	Démarrage en mode sans échec : <type> peut prendre les valeurs suivantes : MINIMAL :démarrage minimal MINIMAL(ALTERNATESHELL) : mode ligne de commande NETWORK : avec réseau DSREPAIR : réparation de l'Active Directory (Contrôleurs de domaine uniquement)
/SAFEBOOT:MINIMAL /SOS /BOOTLOG /NOGUIBOOT	Mode sécurisé
/SAFEBOOT:NETWORK /SOS /BOOTLOG /NOGUIBOOT	Mode sécurisé avec réseau
/SAFEBOOT:MINIMAL(ALTERNATESHELL) /SOS /BOOTLOG /NOGUIBOOT	Mode sécurisé en ligne de Commande
/BOOTLOG	Crée un fichier de log
/BASEVIDEO	Mode VGA 16 couleurs
/SAFEBOOT:DSREPAIR /SOS	Restitution de Active Directory (seulement pour contrôleur de domaine)
/DEBUG	Mode debug

III. La configuration de l'environnement

A. Tuning post installation

1. Les propriétés d'affichage

Désactivez tous les effets visuels qui ralentissent outrageusement l'apparition des boîtes de dialogue.

2. Les options de l'explorateur

Pensez au niveau de l'explorateur à afficher les extensions de fichiers et autres fichiers systèmes et cachés.
Désactivez Active Desktop

3. Envoyer vers

Le dossier SendTo

4. Voir tous les menus

Les paramètres avancés de la barre de tâches

5. Pilotes

Gestion des pilotes non signés : Win+Pause onglet matériel

6. Ajouter l'invite de commandes

```
Clé : HKEY_CLASSES_ROOT\Directory\shell\Invite Commandes\Command
Valeur par défaut : @="cmd.exe /K cd %1"
```

7. Entrer un commentaire au niveau d'un dossier

Dans le fichier desktop.ini, entrez :
[.ShellClassInfo]
InfoTip=DSFC

8. Lancer une application sous un autre compte

Maintenir Shift et choisissez dans le clic Droit Exécuter en tant que.

9. Désactiver la fonction autorun des Cdroms

Clé : \HLM\System\CurrentControlSet\Services\Cdrom
Valeur : Autorun (REG_DWORD)=0

10. Clavier

HU\.DEFAULT\Control panel\Keyboard
Valeur : InitialKeyBoardIndicators =2

11. Couleur de fonds de la console

\HCU\Software\Microsoft\Command processeur
DefaultColor (REG_DWORD)=F0 (Blanc sur noir)1e (jaune sur bleu)

12. Utilisation de la tabulation

\HCU\Software\Microsoft\Command processeur
CompletionChar(REG_DWORD)=9

13. Afficher le bureau après l'exécution du script de connexion

HLM\Microsoft\Windows Nt\CurrentVersion\WinLogon
RunLogonScriptSync=1

B. Disquette de boot

Copiez ntldr, ntdetect.com, bootsect.dos, boot.ini, ntbootdd.sys.

C. Le registre

Les ruches
Les clés
Les valeurs

D. Les variables d'environnement

A partir de l'interpréteur de commandes CMD.EXE, employez la Commande SET :
ALLUSERSPROFILE=C:\Documents and Settings\All Users
APPDATA=C:\Documents and Settings\Administrateur\Application Data
CommonProgramFiles=C:\Program Files\Fichiers communs
COMPUTERNAME=STATION
ComSpec=C:\WINNT\system32\cmd.exe
HOMEDRIVE=C:
HOMEPATH=\
LOGONSERVER=\\STATION
NUMBER_OF_PROCESSORS=1
OS=Windows_NT
Os2LibPath=C:\WINNT\system32\os2\dll;
Path=C:\WINNT\system32;C:\WINNT;C:\WINNT\System32\Wbem
PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH
PROCESSOR_ARCHITECTURE=x86
PROCESSOR_IDENTIFIER=x86 Family 6 Model 2 Stepping 1, AuthenticAMD
PROCESSOR_LEVEL=6
PROCESSOR_REVISION=0201
ProgramFiles=d:\Program Files
PROMPT=PG
SystemDrive=C:
SystemRoot=C:\WINNT
TEMP=C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp
TMP=C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp
USERDOMAIN=STATION
USERNAME=administrateur
USERPROFILE=C:\Documents and Settings\Administrateur
windir=C:\WINNT

E. Performances

Régler la mémoire virtuelle à 1.5 la ram
Fixer la priorité à l'avant-plan si vous disposez d'un serveur d'applications et l'arrière plan pour un AD ou un serveur d'infrastructure réseau
Vous pouvez modifier la priorité des processus dans le gestionnaire de tâches (TASKMAN.EXE).
En cas de charge CPU important, n'hésitez pas à configurer des alertes par le biais du moniteur (perfmon.msc).

F. Les consoles

1. Gpedit.msc

Stratégies des utilisateurs et des groupes locaux

2. Ipsecmon.msc (Server)

Gestion de la sécurité réseau
Client (réponse Seule) mode non crypté par défaut. Répond en mode crypté aux clients qui en font la demande
Sécuriser le serveur (nécessite la sécurité) communication en mode crypté
Serveur Requêtes clientes non cryptées. Envoie les messages en mode crypté.

3. Dskmgmt.msc

Gestionnaire de disque

4. Secpol.msc

Paramètres de sécurité locaux

5. Services.msc

6. Devmgmgt.msc : les périphériques

Vous pouvez y accéder aussi par les propriétés du poste de travail et choisir Gérer.

7. Compmgmt.msc

Equivaut à Gérer dans les propriétés du poste de travail.

8. Eventwr.msc : l'observateur d'événements

Du fait de la transposition du modèle C2 hérité de Windows NT4, vous pouvez tracer tous les événements de l'utilisateur.

9. Diskmgmt.msc : la gestion des disques

a) Le système NTFS

Du fait de sa structure B-Tree, le temps de réponse pour une recherche parmi N éléments est de N/2 dans les systèmes classiques et Log N pour les architectures B-Tree

b) Formater les Systèmes FAT32

Vous pouvez choisir la taille des blocs de 512 octets à 64 Ko
Format lecteur : /A :Taille_Blocs

c) Les disques dynamiques

Les systèmes RAID1 et RAID5 sont disponibles uniquement sur Windows 2000 Server.

d) Les agrégats de partition et par bandes

Windows 2000 Server permet les agrégats de partition et par bandes.

e) Le système DFS (Distributed File System)

Véritable système à tolérance de pannes, chaque nœud DFS peut gérer 32 réplicas.

f) Les quotas

Ils consistent à limiter la place utilisé par les utilisateurs sur chaque volume.

G. L'impression

1. Les processeurs d'impression

On utilise :
RAW pour le PostScript
EMF pour le PCL

2. Spooler

Par défaut, le spooler se trouve dans \WINNT\SYSTEM32\SPOOL\PRINTERS.
Il est contrôlé au niveau du registre par :
Clé : HLM\SYSTEM\CurrentControlSet\Control\Print\Printers
Valeur : DefaultSpoolDirectory (REG_SZ)

H. Le réseau

1. Les protocoles

Il faut éviter le chargement de tous les protocoles (NETBEUI et IPX/SPX). Il multiplie le broadcast au niveau des services d'exploration.

2. Les ports TCPIP

Vous pouvez consulter les numéros de ports dans le fichier %systemroot%\system32\drivers\etc\services et aussi les numéros de protocoles dans %systemroot%\system32\drivers\etc\protocol
Il sont disponibles à partir du site : http://windows.microsoft.com/windows2000/reskit/webresources.

3. Adressage ip

a) Automatique

Si vous passez en mode DHCP et si vous ne disposez d'aucun serveur Dhcp dans votre réseau local, votre PC s'attribue une adresse comprise entre 169.254.0.1 et 169.254.255.254 (masque 255.255.0.0 / Classe B).
Pour désactiver l'adressage automatique, modifiez la base de registre :
Clé : HLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\GUID_de_la_carte
Valeur: IPAutoconfigurationEnable (Reg_DWord)=0

b) Les classes

Classe A : le premier octet identifie le réseau
Classe B : les deux premiers octets identifient le réseau
Classe C : les trois premiers octest identifient le réseau.

c) L'adressage réseau

Il se fait sur la base d'un ET logique entre l'IP et le masque.

d) Le multihoming

Vous pouvez associer plusieurs adresses IP à un même adaptateur.

4. Le routage d'accès distant

Cette fonctionnalité vous permet de vous connecter à Internet ou de transformer votre machine en routeur RIP ou OPSF.

5. Les outils console

ping
arp
ipconfig (ipconfig /setclassid : spécifie l'ID de classe)
telnet
tracert
nslookup
ftp

6. Les partages : fsmgmt.msc

a) Envoyer des messages console

Cet outil vous permet d'envoyer des messages aux personnes connectées. Vous pouvez employer net send.

b) Créer un partage

N'oubliez d'accorder les permissions au niveau sécurité en mode NTFS.

c) Désactiver les partages administratifs

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters]
"AutoShareServer"=dword:00000000
```

7. L'impression LPR (Line Printer Remote)

L'installation des services d'impression LPR amène l'utilisation des DLL suivantes :
LPDSVC.DLL démon LPD
LPRMON.DLL CLIENT LPR

8. L'agent relais Dhcp

Il permet au niveau d'un pont-routeur (machine disposant de deux adaptateurs Ethernet par exemple) d'utiliser le serveur DCHP appartenant à un autre réseau ou sous-réseau (subnetting).

9. PPP sous Windows 2000

a) Fonctionnement

- Couche Physique

- PPP composé de :
  - LCP (Link Control Protocol chargé de l'authentification)
  - NCP (Network Control Protocol niveau 3)
- Couche réseau : IP

b) Protocoles d'authentification

PAP	Password Atuthentification Protocol (mot de passe en clair)
SPAP	SHIVA PAP Spécifique à Shiva (mot de passe crypté)
CHAP	Challenge Handshape Authentification Protocol : le serveur d'accès distant renvoie un challenge, un identifiant généré aléatoirement et envoyé au client. Le client Envoie son mot de passe « haché » par l'identifiant utilisant le procédé MD5 (Message Digest). Le serveur reconsititue le mot de passe et vérifie s'il s'agit du bon utilisateur.
MS-CHAP	Microsoft CHAP. vous pouvez alors employer le Cryptage MPPE (Microsoft Point-to-point Protocol)
MS-CHAP2	Compatible si le client dispose de Windows 2000
EAP	Extensible Authentification Protocol

I. Terminal Server

1. Touches

CTRL+ALT+SUPPR	CTRL+ALT+Fin
ALT+TAB	ALT+PageDown
ALT+Echap	ALT+INSER

2. Installation d'applications

change user/install
change user/execute

3. Augmenter le cache du client

Employez TSREG.EXE (RK Windows 2000) pour avoir un outil qui vous permet de régler cette clé graphiquement.
Clé : HCU\Software\Microsoft\Terminal Server Client
Valeur BitMapCacheSize(REG_DWORD)

J. La sécurité

1. Configuration IE/Outlook

Si vous souhaitez employer Internet Explorer et Outlook Express, vous devez régler les options de sécurité pour l'un et les options générales Du logiciel pour l'autre (menu Outils).

2. La gestion des utilisateurs : lusrmgr.msc

Cette console vous permettra de créer les comptes utilisateurs et les groupes auxquels ils se rattachent. Les mots de passe sont limités à 15 caractères pour des raisons de compatibilité. Dommage !
A chaque utilisateur est associé un SID présent dans la ruche HKEY_USERS.

3. Changment de mot de passe

a) Utilisateur local

net user administrateur mot_de_passe

b) Au niveau d'un domaine

net user administrator mot_de_passe/domain

c) Mot de passe aléatoire sous Windows 2000

cusrmgr -u Administrator –p

4. Les groupes

a) Les groupes prédéfinis

Interactif	Utilisateur de Terminal Server

b) Les types de groupe

Groupe de domaine local
Groupe global Relatif au domaine
Groupe universel N'existent pas en mode mixte

c) Les administrateurs d'entreprise

Ils ont les droits pour intervenir au niveau du changement des rôles afférant à chacun des contrôleurs.

5. La console de sécurité locale : secpol.msc

a) Les stratégies de droit

Elles permettent de définir le comportement général en matière de sécurité.

Privilège	**Description**
Agir en tant que partie du système d'exploitation	Permet à un processus de s'authentifier comme un utilisateur et d'obtenir ainsi l'accès aux ressources auxquelles peut accéder un utilisateur. Seuls les services d'authentification de bas niveau ont besoin de ce privilège. Notez que la possibilité d'accès ne se limite pas aux accès associés à l'utilisateur par défaut ; le processus appelant peut demander que des privilèges supplémentaires arbitraires soient ajoutés au jeton d'accès. Le processus appelant peut aussi créer un jeton d'accès qui ne fournit pas d'identité principale pour le suivi des événements dans le journal d'audit. Les processus nécessitant ce privilège doivent utiliser un compte l'incluant déjà, c'est-à-dire un compte LocalSystem, plutôt qu'un compte d'utilisateur séparé auquel le privilège a été affecté spécialement.
Ajouter des stations de travail au domaine	Permet à l'utilisateur d'ajouter un ordinateur à un domaine spécifique. Pour que le privilège prenne effet, il doit être attribué à l'utilisateur en tant que partir de la Stratégie des contrôleurs de domaine par défaut pour le domaine. Un utilisateur bénéficiant de ce privilège peut ajouter jusqu'à 10 stations de travail au domaine. Les utilisateurs peuvent également être autorisés à joindre un ordinateur à un domaine en leur attribuant l'autorisation Créer des objets Ordinateur pour une unité d'organisation ou pour le conteneur Ordinateurs dans Active Directory. Les utilisateurs qui bénéficient de l'autorisation Créer des objets Ordinateur peuvent ajouter un nombre illimité d'ordinateurs au domaine, qu'ils aient ou non été affecté du privilège Ajouter des stations de travail au domaine.
Ajuster les quotas de mémoire pour un processus	Détermine les comptes pouvant utiliser un processus bénéficiant d'un accès Propriété d'écriture sur un autre processus pour augmenter le quota de processeurs attribué à l'autre processus. Ce droit utilisateur est défini dans l'objet Stratégie de groupe du contrôleur de domaine par défaut (GPO) et dans la stratégie de sécurité locale des stations de travail et des serveurs. Paramètres par défaut : Administrateurs
Arrêter le système	Permet à un utilisateur d'arrêter l'ordinateur local. Paramètres par défaut : Administrateurs, Opérateurs de sauvegarde, Utilisateurs avec pouvoir et Utilisateurs sur stations de travail. Sur les serveurs membres, ce privilège est attribué aux Administrateurs, aux Utilisateurs avec pouvoir et aux Opérateurs de sauvegarde. Sur les contrôleurs de domaine, il est attribué aux Administrateurs, aux Opérateurs de compte, aux Opérateurs de sauvegarde, aux Opérateurs d'impression et aux Opérateurs de serveur.

Augmenter la priorité de planification	Autorise un processus bénéficiant de l'accès de propriété en écriture à un autre processus à augmenter la priorité d'exécution de l'autre processus. Un utilisateur bénéficiant de ce privilège peut modifier la priorité de planification d'un processus dans le Gestionnaire des tâches. Paramètres par défaut : Administrateurs
Charger et décharger les pilotes de périphérique	Permet à un utilisateur d'installer et de désinstaller des pilotes de périphériques Plug-and-Play. Ce privilège n'affecte pas la capacité d'installer des pilotes pour les périphériques qui ne sont pas Plug-and-Play. Seuls les Administrateurs peuvent installer les pilotes de périphériques non Plug-and-Play. Paramètres par défaut : Administrateurs Il est recommandé de ne pas attribuer ce privilège aux autres utilisateurs. Les pilotes de périphériques s'exécutent en tant que programmes dignes de confiance (ou hautement privilégiés). Un utilisateur bénéficiant du privilège Charger et décharger les pilotes de périphérique risquerait de l'utiliser de manière incorrecte par inadvertance, en installant un code nuisible se faisant passer pour un pilote de périphérique. Les administrateurs sont supposés exercer ce privilège de manière plus attentive et installer uniquement des pilotes comportant des signatures numériques vérifiées.
Créer des objets partagés permanents	Autorise un processus à créer un objet répertoire dans le gestionnaire d'objets de Windows XP Professionnel. Ce privilège est utile pour les composants en mode noyau qui étendent l'espace de nom de l'objet. Les composants qui s'exécutent en mode noyau bénéficiant déjà de ce privilège de manière intrinsèque, il n'est pas nécessaire de le leur attribuer. Paramètres par défaut : Aucun.
Créer un fichier paginé	Permet à l'utilisateur de créer un fichier paginé et d'en modifier la taille. Pour ce faire, il faut spécifier la taille d'un fichier de pagination pour un lecteur particulier sous Options de performances, sous l'onglet Avancées des Propriétés système. Paramètres par défaut : Administrateurs
Créer un objet-jeton	Permet à un processus de créer un jeton et de s'en servir pour accéder aux ressources locales lorsqu'il utilise NtCreateToken() ou une autre API de création de jeton. Les processus nécessitant ce privilège doivent utiliser un compte l'incluant déjà, c'est-à-dire un compte LocalSystem, plutôt qu'un compte d'utilisateur séparé auquel le privilège aurait été affecté spécialement. Paramètres par défaut : Aucun
Déboguer des programmes	Permet d'associer un débogueur à un processus quelconque. Ce privilège fournit un accès puissant aux composants sensibles et critiques du système d'exploitation. Paramètres par défaut : Administrateurs
Forcer l'arrêt à partir d'un système distant	Permet à un utilisateur d'arrêter un ordinateur à partir d'un emplacement distant sur le réseau. Voir aussi le privilège Arrêter le système. Paramètres par défaut : Administrateurs sur les serveurs et les stations de travail membres. Sur les contrôleurs de domaine, il est attribué aux Administrateurs et aux Opérateurs de serveur.
Générer des audits de sécurité	Autorise un processus à générer des entrées dans le journal de sécurité. Le journal de sécurité sert à suivre les accès non autorisés au système. Voir aussi le privilège

	Gérer le journal d'audit et de sécurité. Paramètres par défaut : LocalService et NetworkService.
Gérer le journal d'audit et de la sécurité	Permet à un utilisateur de spécifier les options d'audit de l'accès à des objets tels que des fichiers, des objets Active Directory et des clés de Registre, c'est-à-dire des ressources individuelles. L'audit d'accès aux objets n'est actuellement pas effectué, sauf si vous l'avez activé dans Stratégie d'audit (sous Paramètres de sécurité, Stratégies locales). Un utilisateur disposant de ce privilège peut également consulter et supprimer le journal de sécurité à partir de l'Observateur d'événements. Un utilisateur disposant de ce privilège peut également consulter et supprimer le journal de sécurité à partir de l'Observateur d'événements. Paramètres par défaut : Administrateurs
Modifier les valeurs d'env. de microprogrammation	Autorise la modification des variables d'environnement système par un processus via une API ou par un utilisateur via les Propriétés système. Paramètres par défaut : Administrateurs
Modifier l'heure système	Permet à l'utilisateur de définir l'heure de l'horloge interne de l'ordinateur. Paramètres par défaut : Administrateurs, Utilisateurs avec pouvoir, LocalService et NetworkService sur les serveurs et les stations de travail membres. Sur les contrôleurs de domaine, ce privilège est attribué aux Administrateurs, aux Opérateurs de serveur, à LocalService et à NetworkService.
Optimiser un processus	Autorise un utilisateur à exécuter les outils d'analyse des performances de Windows XP Professionnel pour analyser la performance des processus non système. Paramètres par défaut : Administrateurs et Utilisateurs avec pouvoir sur les serveurs et les stations de travail membres. Sur les contrôleurs de domaine, il est attribué uniquement aux Administrateurs
Outrepasser le contrôle de parcours	Autorise l'utilisateur à passer par les dossiers pour lesquels il ne bénéficie sinon d'aucun accès, lorsqu'il parcourt le chemin d'accès à un objet dans le système de fichiers NTFS ou dans le registre. Ce privilège n'autorise pas l'utilisateur à afficher la liste du contenu d'un dossier ; il l'autorise uniquement à traverser ses répertoires. Paramètres par défaut : Administrateurs, Opérateurs de sauvegarde, Utilisateurs avec pouvoir, Utilisateurs et Tout le monde sur les serveurs et les stations de travail membres. Sur les contrôleurs de domaine, ce privilège est attribué aux Administrateurs, aux Utilisateurs authentifiés et à Tout le monde. Paramètres par défaut : Aucun.
Permet d'approuver des comptes d'ordinateur et d'utilisateur pour la délégation	Autorise l'utilisateur à modifier la valeur de Approuvé pour la délégation sur un objet utilisateur ou ordinateur dans Active Directory. L'utilisateur ou l'ordinateur qui bénéficie de ce privilège doit également avoir un accès en écriture aux indicateurs de contrôle de compte sur l'objet. La délégation de l'authentification est une fonctionnalité utilisée par des applications client/serveur à plusieurs niveaux. Elle autorise un service frontal à utiliser les informations d'identification d'un client pour s'authentifier auprès d'un service principal. Pour que cela soit possible, le client et le serveur doivent être exécutés sous des comptes approuvés pour la délégation. Une utilisation incorrecte de ce privilège ou du paramètre Approuvé pour la délégation peut rendre le réseau vulnérable aux attaques

	complexes sur un système qui utilise des programmes du type Cheval de Troie ; ceux-ci empruntent l'identité de clients entrants pour utiliser leurs informations d'identification de sorte à accéder aux ressources réseau. Paramètres par défaut : Ce privilège n'est pas affecté à tout le membre sur les serveurs et les stations de travail membres, étant donné qu'il ne signifie rien dans ces contextes. Sur les contrôleurs de domaine, il est attribué par défaut aux Administrateurs.
Prendre possession des fichiers ou d'autres objets	Autorise un utilisateur à prendre possession d'un objet sécurisable dans le système, notamment des objets Active Directory, des fichiers et dossiers NTFS, des imprimantes, des clés de registre, des services, des processus et des threads. Paramètres par défaut : Administrateurs
Régler les performances système	Autorise un utilisateur à exécuter les outils d'analyse des performances pour analyser la performance des processus système. Paramètres par défaut : Administrateurs
Remplacer un jeton au niveau du processus	Détermine les comptes utilisateur pouvant initialiser un processus pour remplacer le jeton par défaut associé à un sous-processus démarré. Ce droit utilisateur est défini dans l'objet Stratégie de groupe du contrôleur de domaine par défaut et dans la stratégie de sécurité locale des stations de travail et des serveurs. Paramètres par défaut : Local Service et Network Service.
Restaurer des fichiers et des répertoires	Autorise un utilisateur à se soustraire aux autorisations sur les fichiers et les répertoires lors de la restauration de fichiers et de répertoire sauvegardés et à définir une entité de sécurité valide comme propriétaire d'un objet. Voir aussi le privilège Sauvegarder des fichiers et des répertoires. Paramètres par défaut : Administrateurs et Opérateurs de sauvegarde.
Retirer l'ordinateur de la station d'accueil	Autorise l'utilisateur d'un ordinateur portable à le déconnecter de la station d'accueil en cliquant sur Éjecter le PC dans le menu Démarrer. Paramètres par défaut : Administrateurs, Utilisateurs avec pouvoir et Utilisateurs
Sauvegarder des fichiers et des répertoires	Permet à l'utilisateur de contourner les autorisations sur les fichiers et les répertoires pour sauvegarder le système. Le privilège est sélectionné uniquement lorsqu'une application tente un accès via l'interface de programmation d'applications (API) de sauvegarde NTFS. Sinon, les autorisations normales sur les fichiers et les répertoires s'appliquent. Paramètres par défaut : Administrateurs et Opérateurs de sauvegarde.
Synchroniser les données du service d'annuaire	Autorise un processus à fournit les services de synchronisation d'annuaire. Ce privilège concerne uniquement les contrôleurs de domaine. Paramètres par défaut : Aucun
Verrouiller des pages mémoire	Autorise un processus à conserver des données en mémoire physique, évitant ainsi au système de paginer les données sur la mémoire virtuelle du disque. L'attribution de ce privilège peut entraîner une dégradation importante des performances du système. Paramètres par défaut : Attribué à personne. Certains processus système bénéficient de ce privilège de manière intrinsèque.

b) Audit

Après Avoir activé les événements d'audit, vous pouvez dans l'observateur d'événements les visualiser dans le journal d'événements.

6. Le composant Configuration et Analyse de la sécurité

A partir de la console MMC.EXE, ajoutez le composant Configuration et analyse de la sécurité.

7. Les modèles de sécurité

A partir de MMC.EXE, ajoutez le composant enfichable Modèles de sécurité. Les modèles sont stockés dans %systemroot%\Security

K. La sauvegarde

Elle se fait avec NTBackup.

L. Les outils de maintenance et d'entretien

1. defrag

Cet outil ne vaut pas les outils spécialisés tels que Norton Speedisk, Copernet PerfectDisk, Executive Software Diskeeper.

2. Libérer de la place en désactivant l'hibernation

Désactivez la mise en veille prolongée.

3. Les outils Winternals : NTFS for Dos

Avec cet outil, vous pouvez accéder à votre partition NTFS avec une simple disquette de boot.

4. Configuration du WPF (Windows Protect File)

a) La clé

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon]
"SfcQuota"=dword:00000000
"SFCDisable"=dword:00000000
"SFCScan"=dword:00000000 (0   aucun scan|1    scan à chaque boot| 2  1 seul scan)
"SFCShowProgress"=dword:00000000
"SFCDllCacheDir"=hex(2):25,00,73,00,79,00,73,00,74,00,65,00,6d,00,72,00,6f,00,\
  6f,00,74,00,25,00,5c,00,73,00,79,00,73,00,74,00,65,00,6d,00,33,00,32,00,5c,\
  00,64,00,6c,00,6c,00,63,00,61,00,63,00,68,00,65,00,00,00
```

b) Le fichier unattended

```
[SystemFileProtection]
SFCShowProgress=0|1
SFCQuota=0xffffffffh
SFCDllCacheDir= »c:\winnt\system32\dllcache
```

c) L'outil SFC

```
/SCANNOW      Scanne tous les fichiers protégés maintenant
/SCANONCE     Scanne tous les fichiers protégés une fois seulement
/SCANBOOT     Scanne tous les fichiers à chaque boot
/CANCEL       Annule l'opération de contrôle
/QUIET Répare sans interaction
/PURGECACHE   Vide le cache et scanne les fichiers protégés
/CACHESIZE=x  Taille du cache en mégabytes
```

5. cleanmgr

```
/d Lettre_Lecteur:    Choix du lecteur à effacer
/sageset: n           définition des options de cleanmgr (0 à 65536 possibilités)
/sagerun: n           Nettoyage automatique en fonction de l'option n
```

Autres commutateurs :

- Temporary Setup Files

- Downloaded Program Files
- Temporary Internet Files
- Settings\Temporary Internet Files\Content.IE5 folder.
- Old Chkdsk Files
- Recycle Bin
- Temporary Files
- Temporary Offline Files
- Offline Files
- Compress Old Files
- Catalog Files for the Content Indexer

IV. Active Directory

A. Présentation

La base d'annuaire est répliquée sur tous les contrôleurs de domaine et permet toutes les opérations en lecture / écirture à partir de n'importe quel contrôleur. Dans Windows NT4, en cas d'absence du contrôleur principal, les contrôleurs secondaires, à moins de les promouvoir, ne pouvaient que valider les utilisateurs sur le domaine.
Active Directory permet l'interopérabilité avec LDAP, dans la mesure où ce service s'exécute sur les contrôleurs s'appuyant sur Active Directory.

B. Installer Active Directory

DCPROMO

C. Le Serveur DNS

1. Côté serveur

Sous Windows 2000 Server, alors que les entrées faites dans les zones principales et secondaires sont stockées dans des fichiers dns situés dans %systemroot%\system32\dns, Active Directory stocke les informations relatives au domaine dans sa propre base d'annuaire %systemroot%\NTDS\NTDS.DIT.
Le serveur DNS De Windows 2000 répond aux préconisations des serveurs DDNS définies au niveau des RFC 2136 et 2137.
En cas de transfert de zone entre deux partenaires de réplication, vous pouvez utiliser avec AXFR le transfert total ou bien avec IXFR le transfert incrémentiel.

2. Côté client

N'oubliez pas de spécifier le serveur DNS au niveau du client. Le processus d'authentification n'en est que plus rapide.

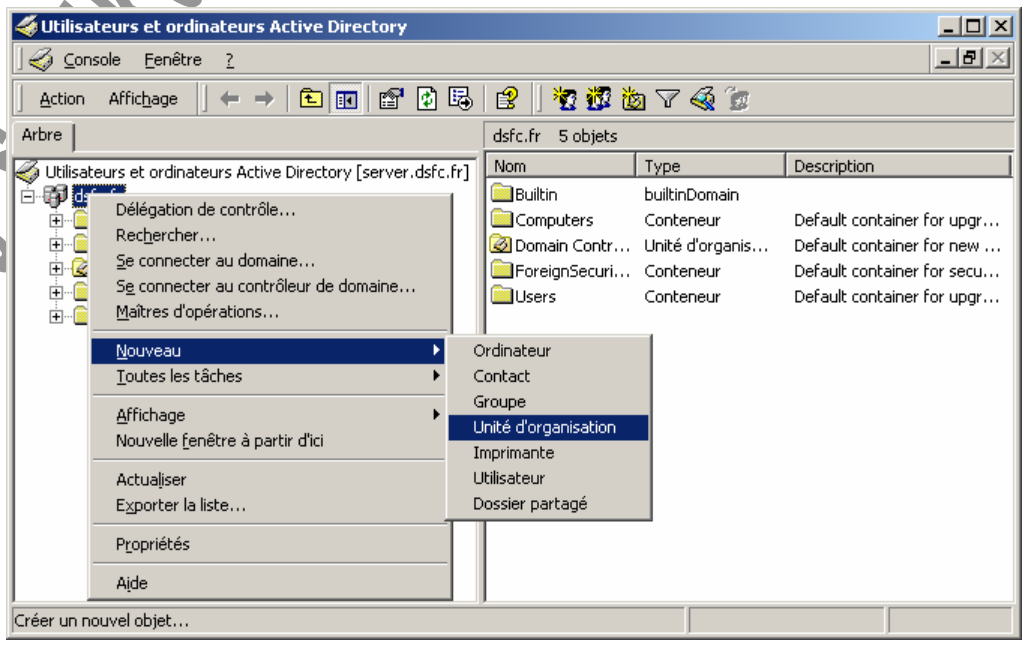
D. Les consoles Active Directory

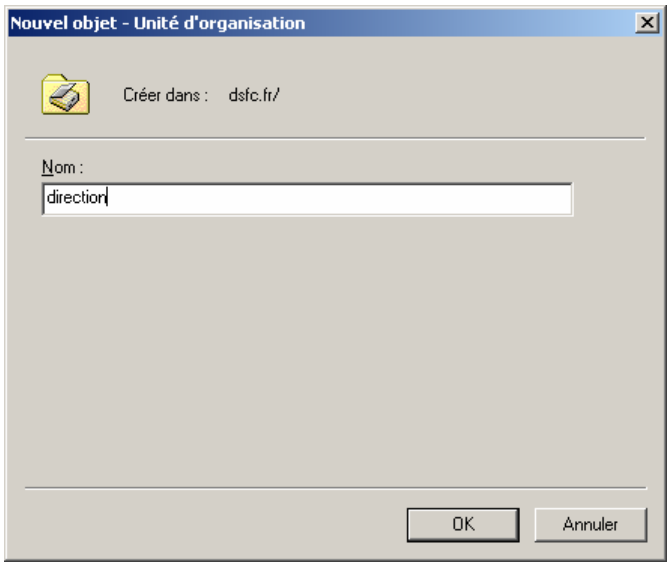
Dsa.msc (Server) : Utilisateurs et ordinateurs Active Directory
Dssite.msc (Server) : Gestionnaire de sire
Domain.msc (Server) : Relations d'approbations
Dompol.msc (server) : Stratégie pour le domaine

E. Les objets Active Directory

1. Création d'une organisation

A partir de la console dsa.msc (Utilisateurs et ordinateurs Active Directory), faites un clic droit sur le domaine. Sélectionnez Nouveau | Unité d'organisation.

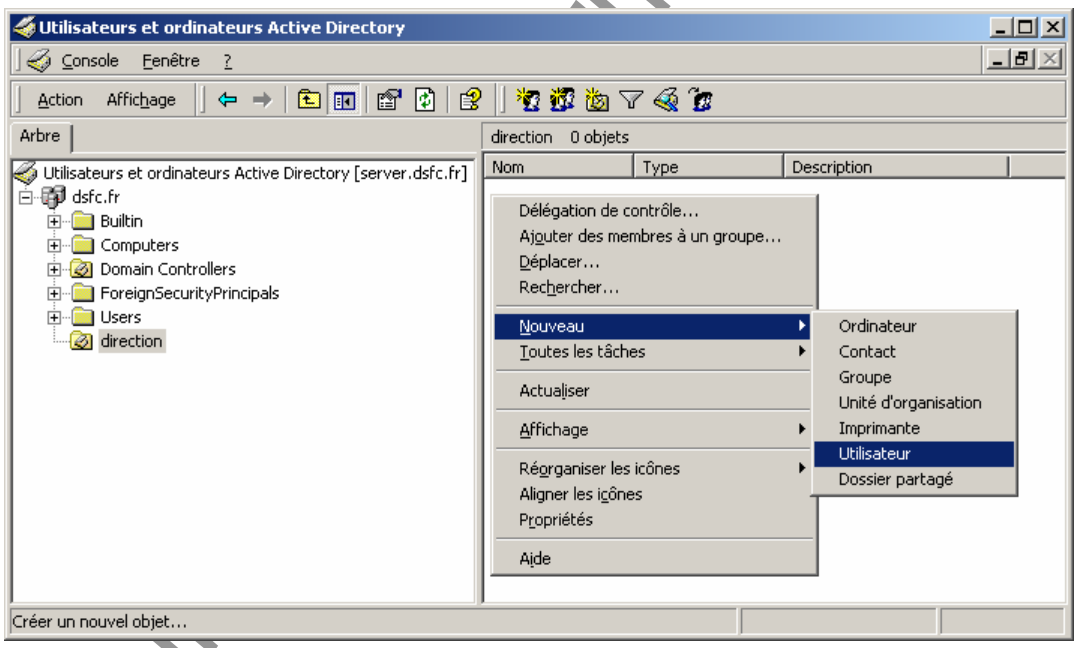


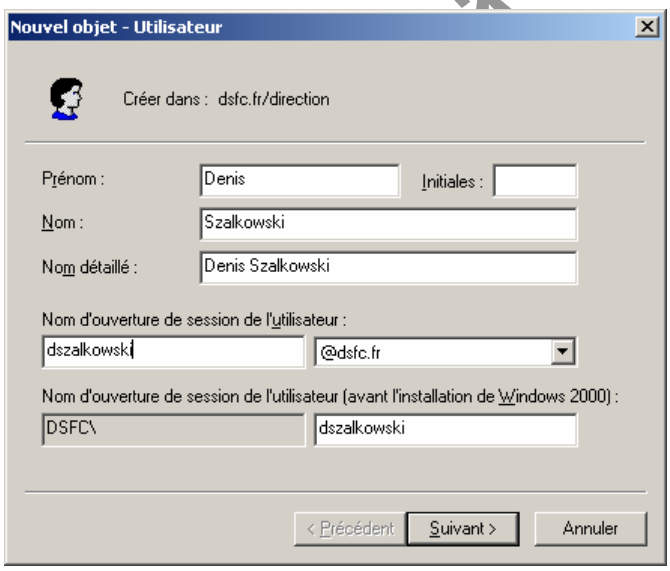


Entrez le nom de l'organisation (service, site, pays). Vous pouvez subdiviser l'unité d'organisation selon la complexité de votre entreprise

2. Création d'un utilisateur

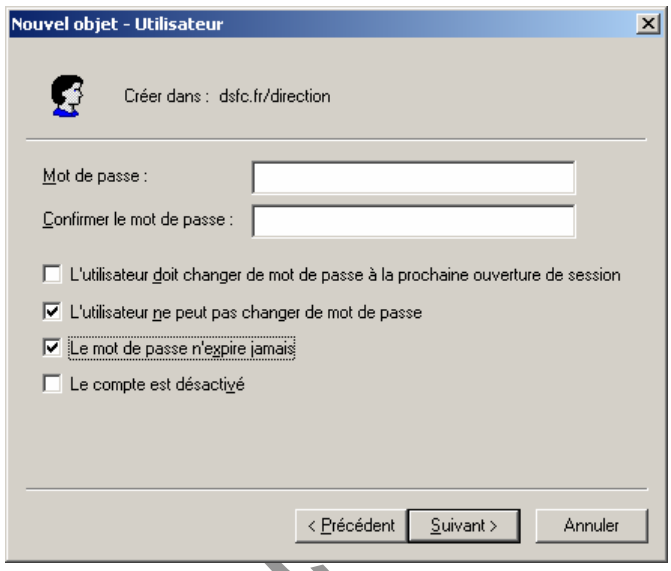
A partir de l'organisation, par un clic droit, allez dans Nouveau | Utilisateur.

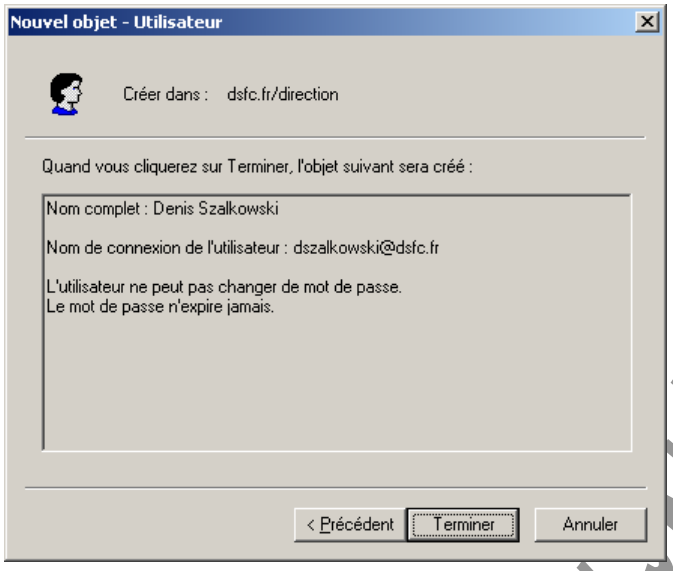




Entrez les caractéristiques de l'utilisateur. Le nom de login est le nom d'ouverture de session.

Entrez la stratégie de mot de passe. L'exemple montre une gestion centralisée de la gestion des mots de passe.

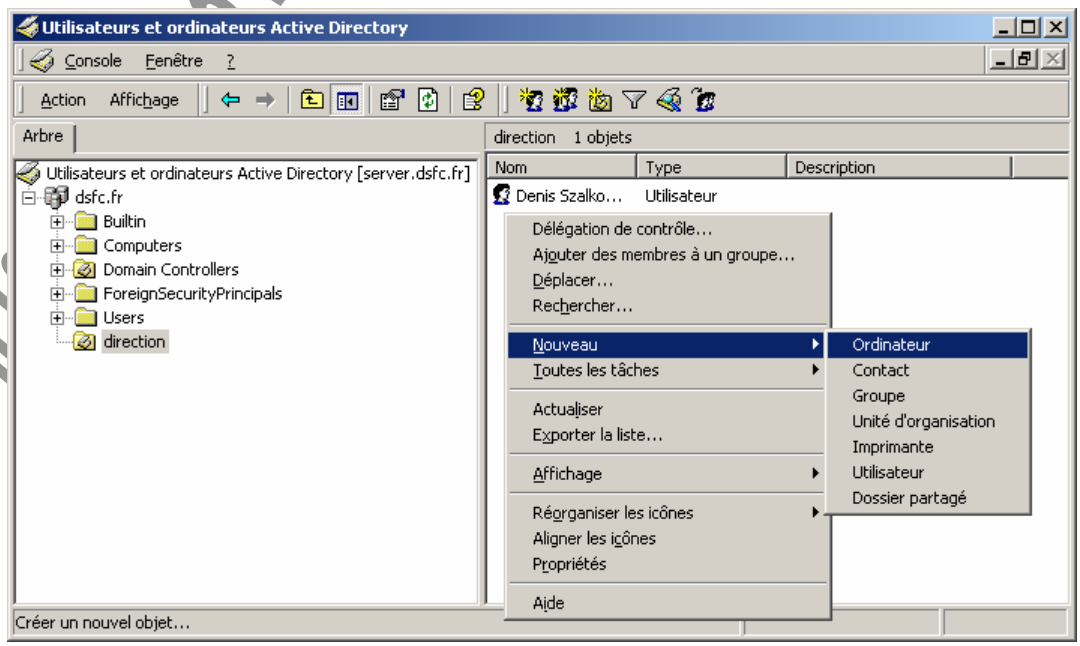


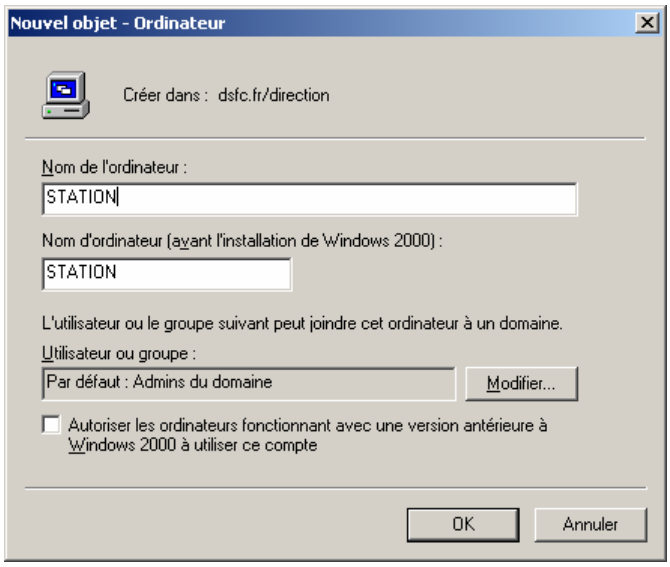


Des fois que vous ne sachiez plus ce que vous avez pu faire !

3. Création d'un ordinateur

A partir de l'organisation, par un clic droit, allez dans Nouveau | Ordinateur.





Entrez les caractéristiques de l'ordinateur. Seuls les administrateurs sont habilités à joindre cet ordinateur au domaine.

F. Les GP0 (Group Policies Object)

Elle s'appuie sur le mécanisme de l'héritage.

1. GPC et GPT

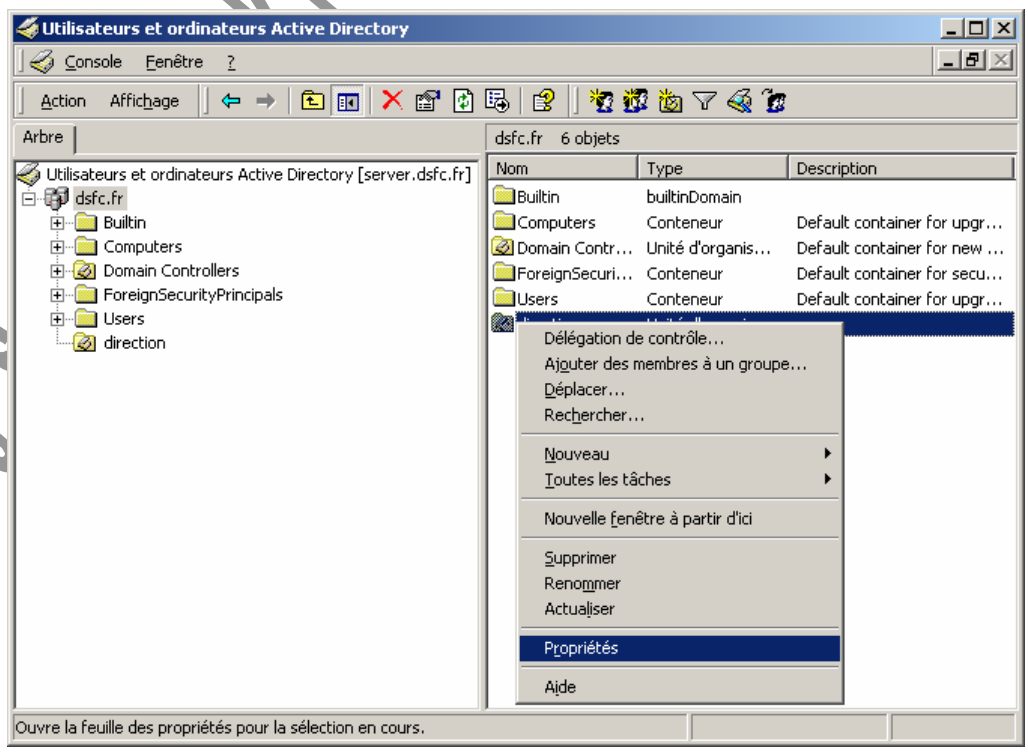
GPC Group Policy Container : C'est l'objet représentant les stratégies dans Active Directory.
GPT Group Policy Template : modèle employé pour définir les stratégies

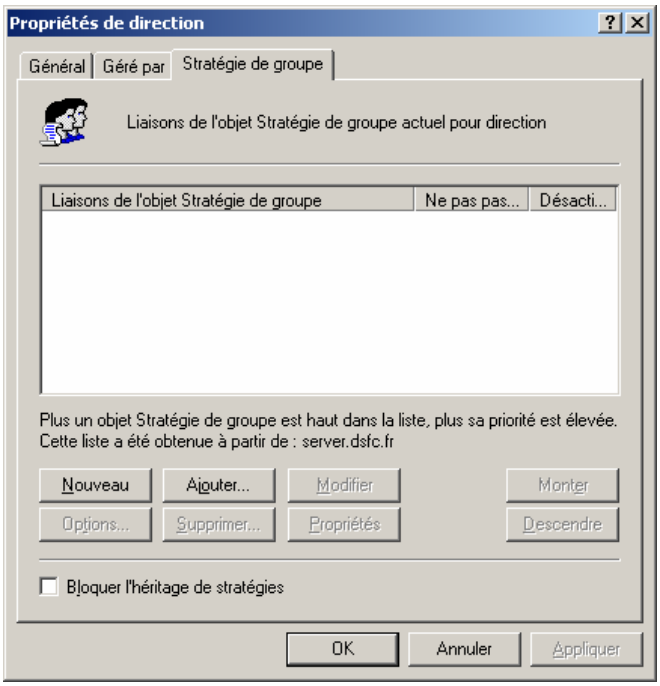
2. Ouverture de session

A l'ouverture de session, l'utilisateur lit le fichier Registry.POL du dossier SYSVOL du contrôleur de domaine. Concernant les paramètres de l'utilisateur, vous modifiez la ruche HCU. Au niveau des paramètres de la machine, vous modifiez la ruche HLM.

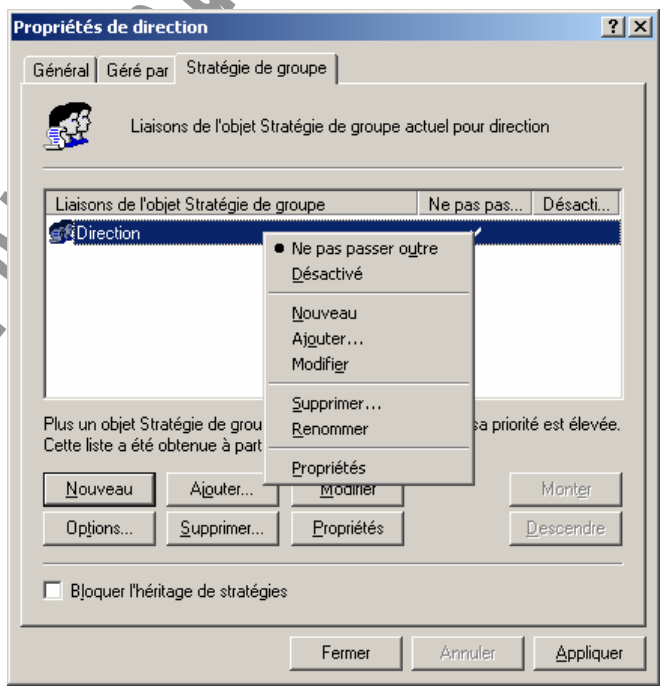
3. Appliquer une stratégie à une organisation

A partir de l'organisation, par un clic droit, allez dans les Propriétés.



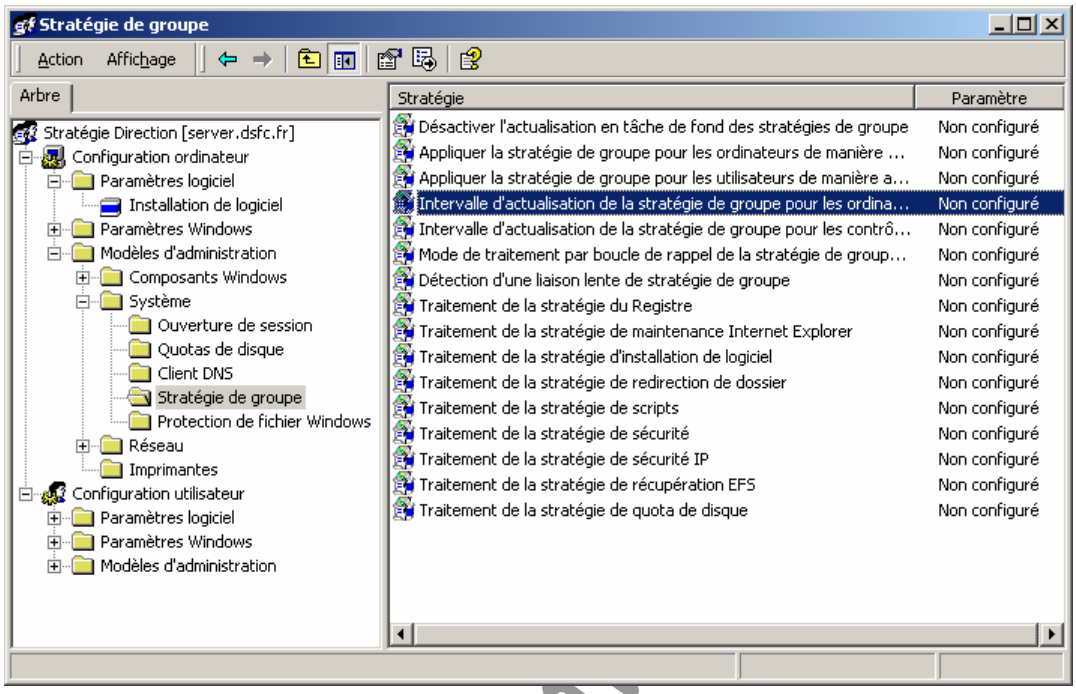


Cliquez sur l'onglet Stratégie de groupe.

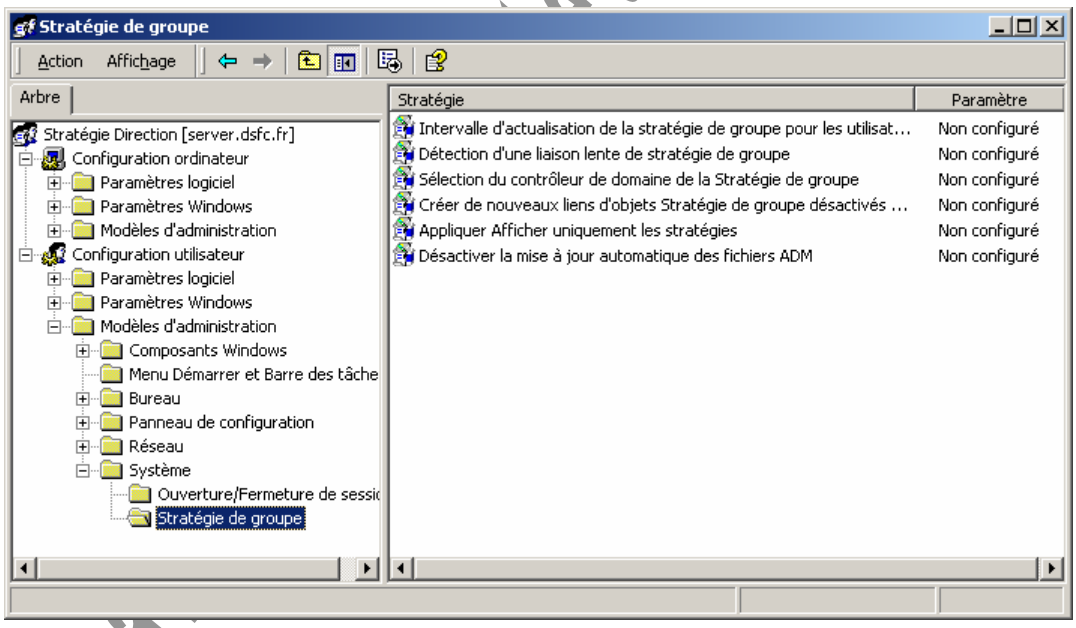


Décochez Désactivé et Ne pas passer outre si vous souhaitez voir s'appliquer les choix déterminés Au niveau de cette stratégie. Cliquez sur le bouton Modifier.

N'oubliez pas de déterminer un intervalle d'actualisation au niveau de Configuration ordinateur | Modèles d'administration | système | Stratégie de groupe.



De la même façon, n'oubliez pas de déterminer un intervalle d'actualisation au niveau de Configuration utilisateur | Modèles d'administration | système | Stratégie de groupe.



G. Type d'installation et rôles

1. Type d'installation

Contrôleur de domaine, serveur autonome, serveur membre

2. Les rôles

La base Active Directory est répliquée sur tous les contrôleurs de domaine. Mais certains contrôleurs (Flexible Single Master Operation) peuvent jouer des rôles différents :

maître de schéma	unique dans la forêt : il maintient les mises à jour et les modifications apportées au schéma. Ce rôle est assuré par le premier contrôleur installé.
maître d'infrastructure	unique : il vérifie la cohérence des SID au niveau de la forêt.
émulateur de contrôleur principal de domaine	unique dans le domaine : il joue le rôle d'un CPD. C'est une passerelle qui permet de synchroniser les BDC avec l'AD. Cela suppose d'être en mode mixte.
maître de nommage du domaine	unique dans la forêt : il contrôle l'adjonction et la suppression de domaines dans la forêt. Ce rôle est tenu par le premier contrôleur

maître d'identificateur relatif (Relative Identifier) unique dans le domaine : ils délivrent les SID (Security Identifier) attribués à chaque objet créé dans le domaine.

Pour modifier le rôle d'un serveur, allez dans Domaines et approbations Active Directory. Par un clic droit sur Domaines et approbations Active Directory, vous accédez à Maître d'opérations.
Au sein de l' Active Directory, chaque objet possède un GUID unique, numéro sur 128 bits.

3. Outil ntdsutil.exe

Pour prendre le rôle de maître d'infrastructure
Cliquez sur Démarrer, sur Exécuter, puis tapez cmd.
À l'invite de commande, tapez ntdsutil.
À l'invite ntdsutil, tapez roles.
À l'invite fsmo maintenance, tapez connections.
À l'invite server connections, tapez connect to server, suivi du nom de domaine complet.
À l'invite server connections, tapez quit.
À l'invite fsmo maintenance, tapez seize infrastructure master.
À l'invite fsmo maintenance, tapez quit.
À l'invite ntdsutil, tapez quit.

H. Changement de mode

En mode mixte, il y a compatibilité avec les serveurs NT4 et les clients Windows 9X et NT4.
Pour basculer en mode natif, allez dans les propriétés du domaine. Cette opération est irréversible.

I. Réplique de Active Directory

Au niveau d'un site distant, afin de minimiser le trafic Wan, il peut être intéressant de posséder un copie locale de l'annuaire. Au niveau de la console Sites et services Active Directory, choisissez le site dans lequel vous souhaitez faire une réplique de l'annuaire.
Développez le dossier Serveurs. Faites un clic droit sur le connecteur NTDS et, dans les propriétés, au niveau de l'onglet général, cochez Catalogue global.

J. Les sites et la duplication

La création de sous-réseaux s'avère très vite indispensable afin de minimiser le trafic entre les contrôleurs de domaine qui voient l'annuaire se répliquer automatiquement à l'aide de contrôleurs de cohérence ou KCC (Knowledge Consitency Checker).
Elle est automatique au bout de 6 heures si les contrôleurs de domaine ne reçoivent aucune notification. En cas de modification, la réplique se fait sur la fréquence de 5 minutes en s'appuyant sur le protocole RPC ou SMTP (si vous êtes reliés par une liaison de type WAN).

K. Outils Active Directory

Outil	Description
MoveTree	Permet de déplacer des objets d'un domaine à un autre.
SIDWalker	Permet d'appliquer les listes de contrôle d'accès à des objets qui appartenaient à des comptes déplacés, isolés ou supprimés.
LDP	Permet d'effectuer des opérations LDAP par rapport à Active Directory. Cet outil dispose d'une interface utilisateur graphique.
DNSCMD	Permet de vérifier l'inscription dynamique des enregistrements de ressources DNS, y compris la mise à jour sécurisée du DNS, ainsi que la suppression des enregistrements de ressources.
DSACLS	Permet de visualiser ou de modifier les listes de contrôle d'accès des objets d'annuaire.
NETDOM	Permet le traitement par lots des approbations, l'ajout de nouveaux ordinateurs aux domaines, la vérification des approbations et des canaux sécurisés.
NETDIAG	Permet de vérifier les fonctions de réseau et de services distribués de bout en bout.
NLTest	Permet de vérifier que le localisateur et le canal sécurisé fonctionnent.
REPAdmin	Permet de vérifier la cohérence de réplication entre partenaires de réplication, de surveiller le statut de réplication, d'afficher les métadonnées de réplication, de forcer des événements de réplication et de forcer Knowledge Consistency Checker (KCC) à recalculer la topologie de réplication.

REPLMon	Permet d'afficher la topologie de réplication, de surveiller l'état de la réplication (y compris les stratégies de groupe), de forcer des événements de réplication et de forcer Knowledge Consistency Checker (KCC) à recalculer la topologie de réplication. Cet outil dispose d'une interface utilisateur graphique.
DSAStat	Permet de comparer les données d'annuaire sur les contrôleurs de domaine et de détecter toute différence.
ADSIEdit	Composant logiciel enfichable MMC utilisé pour visualiser tous les objets de l'annuaire (y compris les données de schéma et de configuration), modifier les objets et appliquer des listes de contrôle d'accès aux objets.
SDCheck	Permet de vérifier la propagation et la réplication des listes de contrôle d'accès pour des objets d'annuaire spécifiques. Cet outil aide l'administrateur à déterminer si l'héritage des listes de contrôle d'accès est correct et si les modifications des listes sont bien répliquées d'un contrôleur de domaine à l'autre.
ACLDiag	Permet de déterminer si un utilisateur dispose ou non des droits d'accès sur un objet d'annuaire. Cet outil peut également servir à réinitialiser les listes de contrôle d'accès à leur état par défaut.
DFSCheck	Utilitaire de ligne de commande qui permet d'administrer tous les aspects des systèmes de fichiers distribués (DFS), de vérifier la cohérence de configuration des serveurs DFS et de visualiser la topologie DFS.

L. Convertisseur d'annuaires NT et NDS vers Active Directory

Mission Critical Software Domain Administrator
Entevo DirectMigrate 2000

M. ADSI (Active Directory Server Interface)

Il s'agit d'une possibilité d'administrer par des scripts l'Active Directory.

N. Le processus d'authentification Kerberos

1. Rappel

Sur Windows Nt4, l'authentification se fait au travers de NTLM (New Technology Lan Manger) qui a su montrer toutes ses limites. Microsoft, conscient de ses propres faiblesses, a choisi d'implémenter l'authentification Kerberos V5. Ce protocole a été mis au point par le MIT (Masschussets Institute of Technology). Le chiffrement à la base de Kerberos consomme plus de ressources au niveau CPU.

2. Mécanisme d'authentification Kerberos

Sous Windows 2000, Kerberos est le protocole de sécurité principal pour les authentifications réalisées dans un domaine inscrit dans l'annuaire Active Directory ou même localement à la machine. Ainsi il permet d'éviter toute usurpation d'identité sur le réseau.
Le serveur dispose d'un KDC (Key Distribution Center), c'est-à-dire d'un centre de distribution de clés à codage symétrique. La même clé est utilisée pour coder et décoder. Cette clé sert à enregistrer le mot de passe crypté dans un ticket émis par le KDC : le TGT (Ticket Granting Ticket). C'est ce ticket qui permet à l'utilisateur de se connecter notamment à l'Active Directory au travers d'une double vérification appelée authentification mutuelle et dans la transparence la plus totale s'appuyant sur le TGS (Ticket Granting Service) côté serveur. C'est grâce au ticket de service émis par le TGS que le serveur connaît l'identité des destinatiares des paquets demandés.

3. Les stations de travail

Elle ne possède qu'un client Kerberos. Cela signifie que l'authentification sur le réseau se fait, lorsqu'elles mettent à disposition leurs propres ressources sur le NTLM.

4. Les relations d'approbation

Il est tout à fait possible de construire une relation d'approbation entre un domaine Kerberos et un Active Directory.

O. Utilitaires d'import et d'export d'annuaire

LDIFDE	Permet d'exporter et importer des données dans Active Directory.
CSVDE	Permet d'exporter et importer des données provenant de fichiers compatibles avec le format CSV, utilisé dans des applications telles que Microsoft Excel.

P. Les profils errants

Pour appliquer un profil errant obligatoire (mode lecture seule), renommez le fichier ntuser.dat en ntuser.man (comme Mandatory)

Q. Démarrage et ouverture de session

- Démarrage des services Réseau RPC (RPCSS Remote Procedure Call System Service + MUP Multiple Universal Naming Convention Provider)
- Stratégie de groupe pour l'ordinateur (celle de l'Active Directory si l'ordinateur appartient à un domaine Windows 2000) appliquée dans l'ordre suivant :
  local, site, domaine, unité d'organisation
- Script de démarrage (600 secondes maximum)
- CTRL+ALT+DEL
- Stratégie liée à l'utilisateur
- Script d'ouverture de session asynchrone
- Script lié à l'utilisateur

V. Utilitaire d'administration du serveur Telnet tlnadmn.exe

A. Intérêt

Telnet est un protocole applicatif utilisant le port 23 permettant la prise de contrôle.
Cet utilitaire tlnadmn.exe vous permet de démarrer ou arrêter le serveur Telnet.
Vous pouvez aussi lister les utilisateurs en cours, fermer la session d'un utilisateur.

B. Options de l'utilitaire d'administration tlnadmn.exe

1. Option	Nom	Description
0	Quitter cette application	Met fin à la session de l'utilitaire d'administration du serveur Telnet.
1	Afficher les utilisateurs en cours	Donne la liste des utilisateurs en cours, y compris leur nom d'utilisateur, domaine, ordinateur distant, identificateur de session et durée de connexion
2	Terminer une session utilisateur	Met fin à une session utilisateur sélectionnée.
3	Afficher/modifier les paramètres du Registre	Fournit la liste des paramètres du Registre que vous pouvez modifier. Voir le tableau ci-dessous.
4	Démarrer le serveur	Démarre le serveur Telnet.
5	Arrêter le serveur	Arrête le serveur Telnet.

C. Les paramètres du Registre du serveur Telnet

Option	Nom	Description et valeurs autorisées	Valeurs conseillées
0	Quitter ce menu	Quitte ce menu et revient aux options d'origine de l'utilitaire d'administration du serveur Telnet.	Non applicable
1	AllowTrustedDomain	0: N'autorise pas l'accès aux utilisateurs de domaine (n'autorise que les utilisateurs locaux). 1: Autorise l'accès aux utilisateurs de domaine dont les domaines entretiennent une relation d'approbation.	1
2	AltKeyMapping	Autorise la fonctionnalité de la touche ALT (ne fonctionne que sur VT100). 0: CTRLA est considéré comme CTRLA. 1: CTRLA est considéré comme ALT.	1
3	DefaultDomain	Defaultdomain peut être défini pour tout domaine entretenant une relation d'approbation avec cet ordinateur. Si AllowTrustedDomain est défini comme étant égal à 1, mais que vous souhaitez établir le domaine local comme domaine par défaut, définissez la valeur à " . ".	Null
4	DefaultShell	Affiche le chemin d'accès de l'installation shell.	%systemroot%\System32\Cmd.exe /q /k
5	LogonScript	Affiche le chemin d'accès au script d'ouverture de session du serveur Telnet. L'administrateur peut obliger le script d'ouverture de session de ce serveur à effectuer certaines opérations pour chaque utilisateur.	%systemroot%\System32\login.cmd
6	MaxFailedLogins	Affiche le nombre maximum de tentatives de connexions infructueuses avant interruption d'une connexion.	1
7	NTLM	Options d'authentification. 0: N'utilise pas l'authentification NTLM. Permet de se connecter vers, ou à partir, d'autres systèmes d'exploitation. 1: Essaie d'abord l'authentification NTLM. En cas d'échec, nomutilisateur et motdepasse sont utilisés. Permet d'établir des connexions entre des ordinateurs	1

		exécutant Windows NT ou Windows 2000, et des ordinateurs exécutant d'autres systèmes d'exploitation. 2: Utilise uniquement l'authentification NTLM. Permet d'établir des connexions entre des ordinateurs exécutant Windows NT ou Windows 2000.	
8	TelnetPort	Affiche le port sur lequel le serveur Telnet écoute les requêtes Telnet.	23

D. Exemple de fichier login.cmd

```
@echo off
echo Bonjour %USERNAME% ! Vous vous connectez à partir de %COMPUTERNAME%
prompt TELNET [ $P ]
cd %HOMEDRIVE%%HOMEPATH% /d
```

E. Utilisation de Telnet

Avec la commande Net, vous pouvez recueillir en autre à distance les informations sur les utilisateurs connectés.

VI. Commandes de Windows 2000

A. Commandes spécifiques

Commande	Fonction
at	Programme l'exécution de commandes et de programmes sur un ordinateur aux date et heure spécifiées.
cacls	Affiche ou modifie des listes de contrôle d'accès (ACL, Access Control List) relatives aux fichiers.
convert	Convertit des systèmes de fichier FAT ou FAT32 en partitions NTFS.
dosonly	Empêche le démarrage d'applications ne fonctionnant pas sous MS-DOS à partir de l'invite de Command.com.
echoconfig	Affiche des messages lors de la lecture du fichier Config.nt du sous-système MS-DOS.
endlocal	Met fin à la localisation des variables d'environnement.
findstr	Recherche du texte dans des fichiers à l'aide d'expressions régulières.
ntcmdprompt	Exécute l'interpréteur de commandes de Windows 2000, Cmd.exe, au lieu de Command.com, après l'exécution d'un programme résident en mémoire ou après le lancement de l'invite de commandes à partir d'une application pour MS-DOS.
popd	Revient au dernier répertoire défini à l'aide de la commande pushd.
pushd	Enregistre le répertoire en cours en vue de son utilisation par la commande popd, puis passe au répertoire spécifié.
setlocal	Commence la localisation des variables d'environnement.
start	Exécute un programme spécifié ou une commande dans une fenêtre secondaire et dans son espace mémoire propre.
Title	Définit le titre de la fenêtre dans laquelle se trouve l'invite de commandes.
&&	La commande qui suit ce symbole n'est exécutée que si l'exécution de la commande précédente a réussi.
||	La commande qui suit ce symbole n'est exécutée que si l'exécution de la commande précédente n'a pas réussi.
&	Sépare plusieurs commandes sur la ligne de commandes.
( )	Groupe des commandes.
^	Caractère d'échappement. Permet de taper des symboles de commande sous forme de texte.
; ou ,	Sépare des paramètres.

B. Modifications apportées aux commandes MS-DOS

Commande	Fonctionnalités modifiées
chcp	Modifie les pages de codes en mode plein écran seulement.
cmd	Cmd.exe remplace Command.com.
del	De nouveaux commutateurs fournissent davantage de fonctions.
dir	De nouveaux commutateurs fournissent davantage de fonctions.
diskcomp	Les commutateurs /1 et /8 ne sont pas pris en charge.
diskcopy	Le commutateur /1 n'est pas pris en charge.
doskey	Disponible pour tous les programmes de caractères qui acceptent des entrées mises en mémoire tampon. Doskey bénéficie de plusieurs améliorations.
format	Prise en charge du lecteur optique de 20,8 Mo. Les commutateurs /b, /s et /u ne sont pas pris en charge.
label	Les symboles ^ et & peuvent être utilisés dans les noms de volume.
mode	Nombreux changements.
more	De nouveaux commutateurs fournissent davantage de fonctions.
chemin	La variable d'environnement %PATH% ajoute le chemin en cours à un nouveau paramètre à l'invite de

	commandes.
print	Les commutateurs /b, /c, /m, /p, /q, /s, /t et /u ne sont pas pris en charge.
prompt	De nouvelles combinaisons de caractères vous permettent d'ajouter des signes ($a), des parenthèses ($c et $f) et des espaces ($s) à l'invite de commandes.
recover	Ne restaure que des fichiers.
rmdir	Le nouveau commutateur /s permet de supprimer des répertoires contenant des fichiers et des sous-répertoires.
sort	Ne requiert pas la variable d'environnement TEMP. Il n'y a pas de limite à la taille des fichiers.
xcopy	De nouveaux commutateurs fournissent davantage de fonctions.

C. Commandes MS-DOS non disponibles

Commande	Nouvelle procédure ou raison de l'abandon
assign	Non prise en charge dans Windows 2000.
backup	Non pris en charge actuellement.
choice	Non pris en charge actuellement.
ctty	Non pris en charge actuellement.
dblspace	Non pris en charge.
defrag	Windows 2000 optimise automatiquement l'utilisation du disque. Pour optimiser manuellement un disque, cliquez dessus avec le bouton droit dans Poste de travail, cliquez sur Propriétés, puis, dans l'onglet Outils, cliquez sur Défragmenter maintenant.
deltree	La commande rmdir /s supprime les répertoires qui contiennent des fichiers et des sous-répertoires.
diskperf	Non pris en charge actuellement.
dosshell	Superflue avec Windows 2000.
drvspace	Le programme Drvspace n'est pas pris en charge à l'heure actuelle.
emm386	Superflue avec Windows 2000.
fasthelp	Cette commande MS-DOS 6.0 est identique à la commande Windows 2000 help. Windows 2000 fournit aussi des références de commande en ligne.
fdisk	L'Administrateur de disques prépare les disques durs pour Windows 2000.
include	Les configurations multiples du sous-système MS-DOS ne sont pas prises en charge.
interlnk	Le programme Interlnk n'est pas pris en charge.
intersrv	Le programme Intersrv n'est pas pris en charge.
join	L'augmentation de la taille des partitions et un système de fichiers amélioré rendent superflue la jointure de lecteurs.
memmaker	Windows 2000 optimise automatiquement l'utilisation de la mémoire du sous-système MS-DOS.
menucolor	Les configurations multiples du sous-système MS-DOS ne sont pas prises en charge.
menudefault	Les configurations multiples du sous-système MS-DOS ne sont pas prises en charge.
menuitem	Les configurations multiples du sous-système MS-DOS ne sont pas prises en charge.
mirror	Non prise en charge dans Windows 2000.
msav	Le programme Msav n'est pas pris en charge.
msbackup	Windows 2000 fournit l'utilitaire de sauvegarde (dans le groupe Outils d'administration du Panneau de configuration) pour les ordinateurs qui disposent de lecteurs de bande ou la commande xcopy pour les ordinateurs ne disposant pas de ce type de lecteur.
mscdex	Il n'est pas nécessaire de configurer le sous-système MS-DOS pour utiliser un lecteur de CD-ROM. Windows 2000 offre l'accès aux lecteurs de CD-ROM pour le sous-système MS-DOS.
msd	Utilisez le composant logiciel enfichable Informations système. Pour le démarrer, cliquez sur Démarrer, sur Exécuter, puis tapez msinfo32.
numlock	Non pris en charge actuellement.
power	L'utilitaire Power n'est pas pris en charge.
restore	Non pris en charge actuellement.

scandisk	L'utilitaire Scandisk n'est pas pris en charge.
smartdrv	Windows 2000 fournit la mémoire cache automatique au sous-système MS-DOS.
submenu	Les configurations multiples du sous-système MS-DOS ne sont pas prises en charge.
sys	Une disquette 1,2 Mo ou 1,44 Mo standard ne peut pas contenir Windows 2000.
undelete	Non prise en charge dans Windows 2000.
unformat	Non prise en charge dans Windows 2000.
vsafe	Le programme Vsafe n'est pas pris en charge.

D. Autres outils console

1. Irftp

Cet outil vous permet de faire des transferts de machine à machine.

2. Cipher

Cipher /D enlève le cryptage

3. Compact

4. Rasdial

Permet d'effectuer une connexion distante par batch.

VII. Le Resource Kit

A. Réseau

1. Tester RPC

Sur l'ordinateur distant, exécutez rpings.exe (TEXTE)
Sur l'ordinateur local, exécutez rpingc.exe (GUI)
Le port utilisé est le 2256 (port sans privilège).

2. Exploration réseau

BROWMON.exe (GUI)

3. Statistiques d'exploration

BROWSTAT.exe (texte)

4. Détecter les serveurs dhcp

Dhcploc.exe (texte)

5. Gestion d'un serveur Dns

Dnscmd.exe (texte)

6. Surveiller les connexions entre contrôleurs de domaine

Dommon.exe

7. Obtenir la Mac (Media Access Control) adresse

Getmac.exe

B. Registre

1. Gestion de la base de registres

Reg.exe (texte)

2. Vidage des clés de registres

Regdmp.exe (texte)

3. Importation de clés

Regini.exe (texte)

4. Outil de recherche

Scanreg.exe (texte)

C. Processus, performances, services

1. Temps de session

Uptime.exe (texte)

2. Liste et arrêt des processus distants

Wrkill.exe (serveur) : client graphique rkill
Rkill.exe (texte) : client texte rkill
Rkillsrv.exe (texte) : il s'agit du service

3. Arrêt d'une machine distante

Shutdown.exe (texte)

4. Liste et état des services

Netsvc.exe (texte)

5. Liste des processus

Pulist.exe (texte)

6. Contrôle des services

Sc.exe (texte)

7. Liste des Services

Srvinfo.exe (texte)

D. Administration

1. Gestion des utilisateurs et des groupes

Cusrmgr.exe (texte)

2. Création des utilisateurs

Addusers.exe (texte)

3. Définition des stratégies

Auditpol.exe (texte)

4. Effacer les profils inactifs

Delprof (texte)

5. Vider le journal d'événements

Dumpel.exe (Texte)

6. Recherche d'un utilisateur dans un groupe

Findgrp.exe (texte)

7. Obtenir le SID

Getsid.exe (texte)

8. Obtenir les utilisateurs d'un groupe global

global.exe (texte)

9. Obtenir les utilisateurs d'un groupe local

Local.exe (texte)

10. Générer un événement

Logevent.exe (texte)

11. Changer de logon

Su.exe (gui)

12. Créer un compte d'ordinateur

Netdom.exe (texte)

13. Etat en temps réel des relations d'approbation

Nlmon.exe (texte)

14. Test du processus Netlogon

Nltest.exe

15. Gestion des stratégies de droits

Ntrights.exe (texte)

16. Copie des permissions au niveau des partages

Permcopy.exe (texte)

E. Fichiers, répertoires, disques

1. Fichiers dupliqués

Dupfinder (GUI)

2. Comparaison d'informations

Vfi.exe (GUI)

3. Recherche de Fichiers

Where.exe (texte)
Il peut utiliser les chemins UNC (Universal Naming Convention) et les variables d'environnement.

4. Recherche d'une chaîne dans un fichier

Qgrep.exe (texte)

5. Remplacement d'une DLL ou d'un pilote verrouillé

Infile.exe (texet) : la modification prend effet au prochain démarrage.

6. Comparaison de fichiers

Windiff.exe (gui)

F. Développement

1. Implémentation de ActivePerl

Activeperl.exe

VIII. Sites Web

http://www.ntfaq.com/
http://www.virtualdr.com/
http://www.bhs.com/
http://www.betaos.com/
http://www.windows2000advantage.com/common/adv-resources.asp
http://www.microsoft.com/france/windows/professionnel
http://www.win2kworld.com/
http://www.labmice.net/
http://proxad.tucows.com/win2k/
http://www.winportal.com/
http://www.zao.co.uk/
http://www.searchnt.com/
http://searchwin2000.techtarget.com/
http://www.isaserver.org/
http://www.generation-nt.com/
http://dszalkowski.free.fr/
http://www.whitehatinc.com/w2ktools/index.html
http://www.ortizonline.com/
http://www.edelweb.fr/EdelStuff/EdelPages/DC2000/
http://www.edelweb.fr/EdelStuff/EdelPages/
http://www.zao.co.uk/win2k/1.htm