

FORMATION MICROSOFT WINDOWS 2000 / 2003 SERVER

PLAN

1. WINDOWS 2003 SERVER

- RESUME
- VERSION DISPONIBLE
- CONFIGURATION NECESSAIRE
- FONCTIONNALITES
- Active directory
- AD 2003 ET AD 2000 compatible ?

2. INSTALLATION DU SYSTEME D'EXPLOITATION

- PARTITIONNEMENT
- TYPE DE FICHIER NTFS / FAT / FAT32
- TYPE DE LICENCE
- RESEAUX

3. PARAMETRAGE

- gestion des disques
- CONFIGURER ADRESSE IP
- INSTALLATION ACTIVE DIRECTORY
- STRATEGIE DE SECURITE LOCALE (LONGEUR MOT DE PASSE, CLIENT 95)
- INSTALLATION ET PARAMETRAGE DU SERVEUR DNS
- INSTALLATION ET PARAMETRAGE DU SERVEUR WINS
- INSTALLATION ET PARAMETRAGE DU SERVEUR DHCP
- INSTALLATION WINDOWS RESSOURCE KIT
- INSTALLATION D'Une CONSOLE PERSONNalisé
- INSTALLATION DES OUTILS D ADMINISTRATION DISTANT (LA CONSOLE GPMC etc...)

4. gestion des partages et de la securite

5. ORGANISATION DE L'AD

- NIVEAU MACHINE
- NIVEAU UTILISATEUR (groupe)
- SCHEMA

6. CREATION DES UTILISATEURS

- SERVER ADMINISTRATIF (ADDUSER.EXE)
- SERVEUR PEDAGOGIQUE (GESTION 5)

7. CREATION D'UNE STRATEGIE de groupe (UTILISATEUR / MACHINE)

- installation des imprimantes réseaux
- suppression du profils local (cache)
- restriction poste client

8. Poste client xp / 2000

- configuration réseau (WINS, DNS, passerelle)
- faire rentrer un poste xp / 2000 dans un domaine
- création de profils itinérant, obligatoire, local
- Les UTILISATEURS ET LES DROITS

9. Mise à jour des clients

- shlavik
- sus
- sms

10. Sauvegarde client et serveur

- robocopy
- cobian
- xcopy32
- ghost / drive image
- SYNCHROPARC
- L'UTILITAIRE DE SAUVEGARDE MICROSOFT

11. OUTILS DIVERS

WINDOWS 2003 SERVER

De nombreuses entreprises et agences gouvernementales ont trouvé dans Microsoft Windows 2000 Server une réponse à leurs besoins à même de satisfaire le niveau élevé de leurs exigences, comme en témoignent les estimations de International Data Corporation. D'après IDC, en 2001, plus de 60 % de l'ensemble des serveurs livrés dans le monde étaient fournis avec un système de la famille Windows Server, un ratio qui a connu une croissance à deux chiffres au cours des dernières années.1

Cette confiance des organisations induit des attentes auxquels la famille Microsoft Windows Server 2003 doit répondre de manière à améliorer encore fiabilité, performances et connectivité et avec un rapport qualité/prix sans précédent. Les nombreux commentaires et remarques des clients et des partenaires ainsi que les tests indépendants réalisés par des milliers de personnes ont été pris en compte par Microsoft dans la définition des spécifications et le développement de la famille Windows Server 2003.

Ainsi, pour permettre aux entreprises de mettre en relation aisément et en toute transparence informations, personnes, systèmes et périphériques, Windows Server 2003 intègre en mode natif les technologies Microsoft .NET (notamment avec l'intégration du .NET Framework) et des technologies basées sur des standards officiels ou standards de fait de l'industrie informatique. Windows Server 2003 constitue la base d'un niveau d'intégration logicielle encore jamais atteint grâce à l'utilisation de services Web XML.

Création de valeur par la famille Windows Server 2003

Le système d'exploitation Windows Server 2003 constitue une plate-forme d'infrastructure caractérisée par une extrême productivité pour le fonctionnement des applications, réseaux et services Web connectés, depuis le groupe de travail jusqu'au centre de données (ou " Data Center " en Anglais).

Intégré et productif

Windows Server 2003 intègre en standard de nombreux services à l'origine de la polyvalence de ce système d'exploitation serveur. Les scénarios d'utilisation possibles sont très variés : serveur de fichiers et d'impression, serveur de bureautique, serveur de solutions Internet (site Web, services Web, commerce électronique...), serveur d'applications... Windows Server 2003 permet une administration centralisée, avec possibilités de délégation, d'un parc de postes de travail et une infrastructure de services réseaux, de communication et de sécurité à l'échelle de l'entreprise. Il reprend les caractéristiques de Windows 2000 Server dont il étend les possibilités afin de simplifier la mise en œuvre et l'exploitation au quotidien.

Tous ces services sont intégrés et leur fonctionnement conjoint a déjà été testé et validé. Nul besoin, comme sur d'autres plates-formes, de rechercher des briques hétérogènes et de réaliser un fastidieux travail d'intégration spécifique présentant des risques de compatibilité et de support technique global de par l'hétérogénéité des briques assemblées.

Windows Server 2003 améliore sensiblement la productivité, aussi bien pour les administrateurs informatiques que pour les utilisateurs finaux. Des outils de gestion et de déploiement remaniés, en particulier pour la mise en œuvre du service d'annuaire Active Directory®, simplifient le travail des administrateurs. D'autres innovations telles que VSS (Volume ShadowCopy Services) améliorent la productivité des utilisateurs finaux en leur permettant de retrouver des versions antérieures de leurs documents ou de récupérer des fichiers détruits par erreur.

Digne de confiance - Les entreprises découvriront dans le système d'exploitation Windows Server 2003 un environnement informatique fiable, conçu expressément pour l'entreprise et bénéficiant d'améliorations importantes pour aller encore améliorer encore les niveaux de fiabilité, de disponibilité, d'évolutivité et de sécurité déjà atteints avec Windows 2000 Server.

De nombreuses innovations facilitent la montée en charge : support de systèmes multiprocesseurs jusqu'à 64 processeurs, maximum de 512 Go de mémoire vive pour les plus gros besoins applicatifs, support de l'architecture 64 bits Itanium d'Intel ...

Sur le plan de la disponibilité, le travail commun effectué avec certains constructeurs a permis de répondre à des demandes d'engagement sur une disponibilité à 100% des serveurs. La continuité service sera renforcée avec la possibilité de mettre en œuvre des clusters comportant jusqu'à 8 serveurs, serveurs qui pourront être distants d'un maximum de 100 km pour former des clusters distribués ou géo-clusters.

Enfin, la sécurité, préoccupation parmi les plus importantes actuellement, a fait l'objet d'un soin tout particulier : premier produit issu de l'initiative Trustworthy Computing initiée par Microsoft en janvier 2002, Windows Server 2003 a été conçu dans le souci de fournir une plate-forme hautement sécurisée. Ce souci de la sécurité a été pris en compte par design lors de la définition des spécifications (architecture du serveur Web intégré Internet Information Services 6.0, par exemple), par défaut (certains services et protocoles ne sont plus installés ou activés par défaut afin de réduire les risques d'attaque), par déploiement (meilleur contrôle des conséquences liées aux changements de configuration). Enfin, Microsoft s'engage à fournir une documentation très complète décrivant les méthodes recommandées pour la configuration et l'exploitation au quotidien de Windows Server 2003.

Ouvert - Windows Server 2003 fait partie intégrante de la vision Microsoft .NET. A ce titre, Windows Server 2003 supporte les standards et normes applicables aux services Web, notamment le langage XML et le protocole UDDI. Windows Server 2003 peut s'intégrer dans tout environnement hétérogène au travers de services Web.

Grâce à l'intégration du .NET Framework et de ASP.NET, aux améliorations apportées à IIS (Internet Information Services), et à l'ajout de nombreuses fonctionnalités nouvelles et modifiées, la famille Windows Server 2003 constitue la plate-forme idéale pour développer, déployer et héberger des applications de services Web.

Rentable - Windows Server 2003 repose sur la robustesse de la famille Windows 2000 Server alliée à une évolutivité accrue qui en font un serveur exceptionnel à un prix raisonnable. Cette plate-forme informatique est idéale pour toute entreprise, quelle que soit sa taille.

S'appuyant sur les caractéristiques de Windows 2000 Server, le système d'exploitation Windows Server 2003 permet aux entreprises de préserver et même de valoriser leurs investissements informatiques actuels tout en réduisant les coûts informatiques globaux.

Une mise à niveau depuis Windows NT Server 4.0 vers Windows Server 2003 permet de bénéficier de performances et d'une fiabilité considérablement accrue. Windows Server 2003 peut travailler avec des systèmes et des domaines Windows NT Server 4.0 et Windows 2000 Server ce qui permet une mise à jour progressive.

- **Présentation de la famille Windows Server 2003**

La famille Microsoft Windows Server 2003 s'inscrit dans la lignée des systèmes d'exploitation constituant la plate-forme Windows Server dont la première version a été mise sur le marché il y a près de 10 ans. Windows Server 2003 s'inspire de la fiabilité, de l'évolutivité et de la simplicité de gestion reconnues de Windows 2000 Server pour offrir aux utilisateurs la plate-forme d'infrastructure la plus productive pour le fonctionnement des applications, des réseaux et des services Web connectés, depuis le groupe de travail jusqu'au centre de données (" data center ").

Windows Server 2003 offre la souplesse nécessaire pour répondre rapidement et efficacement aux exigences sans cesse renouvelées des environnements informatiques professionnels d'aujourd'hui tout en procurant la qualité que sont en droit d'attendre les utilisateurs d'un système d'exploitation serveur complet en termes de fiabilité, d'évolutivité et de sécurité.

Éditions de la famille de produits

La famille Windows Server 2003 se décline en quatre éditions :

- **Windows Server 2003 Datacenter Edition**

Destiné à la mise en œuvre d'applications critiques et volumineuses, Windows Server 2003 Datacenter Edition répond aux besoins des plus grosses bases de données, systèmes transactionnels et applications métiers spécifiques. Il constitue une plate-forme idéale pour la consolidation de serveur, y compris pour des applications hétérogènes. Afin de répondre aux exigences spécifiques des environnements de production informatique intensifs, l'édition Datacenter est accompagnée d'offres de services spécifiques pouvant aller jusqu'à un engagement de garantie sur la disponibilité. Datacenter est proposée en version 32 bits ou 64 bits.

- **Windows Server 2003 Enterprise Edition**

Conçu pour les moyennes et grandes entreprises, Windows Server 2003 Enterprise Edition permet la mise en œuvre d'une infrastructure d'entreprise (services réseau, communication, sécurité, administration), l'exploitation d'applications métiers, de progiciels ou d'applications tournées vers l'Internet comme les services Web et le commerce électronique. Il répond aux besoins de montée en charge et permet la mise en œuvre de solutions de haute disponibilité. Les applications nécessitant de gros volumes de données et une forte puissance de calcul trouveront une réponse appropriée avec la version 64 bits de Windows Server 2003 Enterprise Edition qui permet la mise en œuvre de serveurs basés sur les processeurs Intel® Itanium™.

- **Windows Server 2003 Standard Edition**

Windows Server 2003 Standard Edition est un système d'exploitation serveur réseau polyvalent. Il répond aux besoins des petites et moyennes organisations et des services départementaux ou groupes de travail. Il permet le partage de fichiers et d'imprimantes, la mise en œuvre d'une connectivité Internet sécurisée, le déploiement d'application bureautique centralisée et la collaboration performante entre les employés, les partenaires et les clients. C'est le système d'exploitation serveur polyvalent par excellence.

- **Windows Server 2003 Web Edition**

Nouveau produit dans la famille des serveurs Windows, Windows Server 2003 Web Edition est optimisé pour la mise en œuvre de solutions Web. Il peut être utilisé aussi bien par les fournisseurs de services Internet que par les organisations qui ont choisi d'héberger elles-mêmes leurs serveurs Web. Cette édition constitue une plate-forme particulièrement adaptée pour le développement et le déploiement rapide de services et d'applications Web.

Éditions à diffusion limitée

Certains constructeurs informatiques (OEMs) ont proposé à partir de juin 2001 des éditions préliminaires spécifiques appelées " éditions limitées " de Windows Server basées sur le code de Windows Server 2003. Ces éditions ont rapidement

connu un succès important. Windows Advanced Server Limited Edition fut le premier système d'exploitation serveur Windows 64 bits de Microsoft à prendre en charge les processeurs Itanium d'Intel. Il est fondé sur le code préliminaire 64 bits de Windows Server 2003 Enterprise Edition, optimisé pour les applications de bases de données, scientifiques ou graphiques nécessitant beaucoup de mémoire ou de calculs.

- **Configuration de Windows Server 2003**

Evolution naturelle des serveurs Windows 2000, Windows Server 2003 reprend les technologies déjà présentes dans Windows 2000 Server en les améliorant afin d'accroître leur fiabilité et leur simplicité d'utilisation.

Par ailleurs, Windows Server 2003 s'enrichit d'un large éventail de nouvelles fonctionnalités et technologies.

Le tableau qui suit récapitule les fonctionnalités et technologies de Windows Server 2003, nouvelles ou améliorées.

Configuration nécessaire au fonctionnement de Windows Server 2003


Configuration requise	Windows Server 2003 Web Server	Windows Server 2003 Standard Server	Windows Server 2003 Enterprise Server	Windows Server 2003 Datacenter Server
Vitesse minimale du processeur	133 MHz	133 MHz	133 MHz pour les ordinateurs x86 733 MHz pour les ordinateurs Itanium	400 MHz pour les ordinateurs x86 733 MHz pour les ordinateurs Itanium
Vitesse recommandée du processeur	550 MHz	550 MHz	733 MHz	733 MHz
Quantité minimale de RAM	128 Mo	128 Mo	128 Mo	512 Mo
Quantité minimale de RAM recommandée	256 Mo	256 Mo	256 Mo	1 Go
Quantité maximale de RAM supportée	2 Go	4 Go	32 Go pour les ordinateurs x86 64 Go pour les ordinateurs Itanium*	32 Go pour les ordinateurs x86 512 Go pour les ordinateurs Itanium*
Support des systèmes multiprocesseurs**	Jusqu'à 2 processeurs	Jusqu'à 4 processeurs	Jusqu'à 8 processeurs	Système supportant un minimum de 8 processeurs Maximum de 64 processeurs
Espace disque pour l'installation	1,5 Go	1,5 Go	1,5 Go pour les ordinateurs x86 2 Go pour les ordinateurs Itanium	1,5 Go pour les ordinateurs x86 2 Go pour les ordinateurs Itanium

Tableau récapitulatif des nouveautés et des améliorations

Légende :

 = Fonction incluse

 = Fonction partiellement prise en charge

 = Fonction non supportée

Fonction / Service	Web Edition	Standard Edition	Enterprise Edition	Datacenter Edition
Evolutivité et montée en charge				
Support des systèmes à base de processeurs Intel® Itanium®	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
Ajout de mémoire à chaud ^{1,2}	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
Support des systèmes NUMA (Non-Uniform Memory Access)	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
Programme Datacenter	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Mémoire maximale supportée				
2 Go	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
4 Go	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
32 Go	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
64 Go ³	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
512 Go ⁴	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Nombre maximal de processeurs par système symétrique (SMP)				
2 processeurs	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
4 processeurs	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
8 processeurs	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
32 processeurs	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
64 processeurs	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Services d'annuaire				
Active Directory™	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
Prise en charge des services de méta annuaire MMS	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
Services de sécurité				
Pare-feu de connexion Internet	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Infrastructure de clés publiques, services de certificats et cartes à puce	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
Services de Terminaux				
Administration avec le bureau à distance	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
Services de terminaux (mode serveur d'application)	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
Annuaire de sessions des services de terminaux	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
Technologies de clustering				
Équilibrage de la charge réseau	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
Clusters de serveurs	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
Services de communications et de réseau				
Prise en charge du réseau privé virtuel (VPN)	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
Service d'authentification Internet (IAS)	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
Pont inter réseaux locaux	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
Partage de connexion Internet	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
IP v6				
Services d'impression et de fichiers				
Système de fichiers				

- ACTIVE DIRECTORY

<http://www.supinfo-projects.com/fr/2002/decouverte%5Factive%5Fdirectory/>

Objectifs

Cet article a pour but de présenter au lecteur les éléments techniques d'Active Directory, le service d'annuaire de Microsoft introduit dans Windows 2000.

Il s'agit ici de se concentrer sur le contenu technique immédiatement utile à la mise en œuvre et à la compréhension du système.

Les éléments réseau utilisés par Active Directory sortent du cadre de cet article. Il ne s'agit pas d'un essentiel ; les manipulations purement pratiques, les explications purement théoriques, ou les détails de fonctionnement internes ne sont pas abordés.

Un service d'annuaire

Autrefois, Windows NT4 obligeait à disposer les ressources informatiques de l'entreprise (les objets) dans un grand récipient (le domaine), en grand désordre. Impossible dans ces conditions de s'y retrouver, de mettre en place un contrôle précis sur des catégories d'objets, de suivre l'évolution du système ou même de parvenir à un semblant d'organisation.

Active Directory est le service d'annuaire de Microsoft, conçu afin d'organiser les ressources informatiques de l'entreprise. Active Directory a pour objectif de permettre la gestion des comptes, des ordinateurs, des ressources et de la sécurité de façon centralisée, dans le cadre d'un domaine.

Depuis NT4, un domaine constitue un ensemble d'utilisateurs et de machines dont le contrôle est centralisé. Active Directory lui apporte l'organisation structurée dont il a besoin. Cette structuration permet des contrôles plus fins sur chaque élément sans entraîner une complexification du système.

Les ressources informatiques peuvent ainsi être gérées plus efficacement par les administrateurs du réseau informatique de l'entreprise.

En entreprise

Nombre d'entreprises ont mis en place Novell Netware dans les années 90. Son service d'annuaire NDS (Novell Directory Service) n'avait jusqu'ici pas d'équivalent dans le monde Windows.

Microsoft a conçu Active Directory pour apporter aux domaines NT ce qui leur manquait, tout en éliminant les structures d'annuaire NDS. De plus en plus les entreprises remplacent leurs serveurs vieillissant sous Netware par des architectures Windows 2000 Active Directory, ce qui n'était pas possible avec NT4.

Vous pouvez étudier Active Directory avec une architecture de test très simple : deux ou trois machines en réseau sous Windows 2000 suffisent.

Active Directory et Windows

Si Active Directory prend en compte Windows 95, 98 et NT4, il nécessite des ordinateurs membres du domaine fonctionnant sous Windows 2000 pour offrir la totalité de ses fonctionnalités.

Pour la gestion des domaines, Active Directory nécessite Windows 2000 Server (minimum). Active Directory remplace la gestion de domaines classique de NT4. L'annuaire contient notamment des objets comptes d'ordinateurs, les utilisateurs, les groupes, mais également objets contacts, imprimantes, dossiers partagés...

Certains de ces objets existent uniquement dans l'annuaire : les groupes, comptes d'utilisateurs et comptes d'ordinateurs. D'autres objets ne sont que des références publiées dans l'annuaire : dossiers partagés, imprimantes. Ces objets se trouvent en réalité sur des ordinateurs membres du domaine.

Ces références ont pour but de faciliter la recherche des ressources. En effet, Active Directory permet aux utilisateurs de rechercher rapidement une ressource partagée dans le domaine et publiée dans l'annuaire. Active Directory permet à la fois de centraliser les ressources pour en faciliter l'administration, et d'en faire une exploitation décentralisée puisque l'annuaire est accessible à chaque utilisateur, l'administration elle-même pouvant être déléguée.

Forêts et Domaines

Nommage et hiérarchie des domaines d'une forêt

Active Directory est directement lié au DNS (Domain Name System) notamment pour le nommage des domaines. Active Directory impose une organisation hiérarchique des domaines, qui se retrouve dans le nommage hiérarchique des noms de domaines dans le DNS.

Active Directory est donc une structure hiérarchique. La forêt regroupe des arborescences qui regroupent des domaines. Le premier domaine créé dans la forêt est le domaine racine. De ce domaine dépendent l'administration de la forêt et l'ajout de nouveaux domaines.

=> Une forêt est un ensemble de domaines dont l'espace de nommage est contiguë et qui s'approuvent mutuellement.

Le nom d'un domaine est utilisé directement dans le DNS. Le nommage hiérarchique fait qu'un domaine domaine.dom pourra avoir pour fils fils.domaine.dom. Ces deux domaines forment ici une arborescence.

Une arborescence est composée par un domaine père et sa lignée de domaines enfants, petits-enfants... Dans une forêt, tous les domaines ont pour « ancêtre commun » le domaine racine.

NetBios

Pour rester compatible avec les versions précédentes de Windows, le nom FQDN (Fully Qualified Domain Name) du domaine (contenu dans le DNS) est associé à un nom Netbios.

Pour mémoire les noms Netbios sont formés de 15 caractères et ne sont pas hiérarchiques.

Lorsque vous créez un domaine, Windows 2000 vous propose un nom Netbios par défaut, tiré des premiers caractères du nom FQDN que vous avez choisi. Le nom proposé par défaut peut en fait déjà appartenir à un autre domaine, si les deux noms de domaine sont longs et que leurs premiers 15 caractères sont identiques. Vous devez veiller à ce que le nom Netbios soit unique sur votre réseau, sinon cela provoquera une erreur à la création du domaine. Vous devrez alors choisir un autre nom Netbios.

Chaque domaine aura donc un nom FQDN (exemple : domaine55.entreprise3.dom) et un nom Netbios (exemple : DOMAINE55).

Au format Netbios et sur les anciens Windows, un nom complet d'utilisateur sera :
FILS\Utilisateur

1.2. Modifications du schéma

Comme dans une base de données, chaque objet est associé à des propriétés. L'ensemble des propriétés possibles pour n'importe quel objet, et la définition de tous les objets pouvant exister forment le schéma de la forêt.

Seuls les membres du groupe Administrateurs du schéma peuvent modifier celui-ci, par le biais de la console MMC (Microsoft Management Console) d'Administration du Schéma. Cette console n'est pas installée par défaut, vous pouvez l'installer à partir du package adminpak.msi situé sur le CD Windows 2000 Server.

Microsoft déconseille très fortement de modifier le schéma par défaut. Vous pouvez détruire la forêt en cas de changement inconsidéré. Cependant certains logiciels modifient néanmoins le schéma, comme par exemple Exchange 2000. L'installation d'Exchange 2000 dans un domaine quelconque de la forêt nécessite donc qu'un administrateur du schéma exécute la partie de l'installation visant à modifier le schéma.

1.3. Gestion des contrôleurs de domaine (DC – Domain Controller)

Un contrôleur de domaine est un Windows 2000 Server ou plus. Vous pouvez transformer un serveur en contrôleur de domaine (le promouvoir) ou de le rétrograder en simple serveur membre du domaine, sans avoir besoin de réinstaller le système d'exploitation (contrairement à NT4) : il suffit de lancer DCpromo.EXE.

Active Directory dépend étroitement du DNS, la procédure d'installation d'Active Directory propose donc l'installation et la configuration automatiques du service approprié, s'il n'existe pas déjà, et si le serveur est le premier contrôleur de domaine de la forêt. Vous devez sinon vous assurer auparavant que le serveur utilise bien le DNS contenant la zone pour le domaine.

Physiquement, Active Directory est stocké dans plusieurs fichiers de base de données du répertoire NTDS, et les stratégies dans le répertoire SYSVOL. Les propriétés du système de fichiers NTFS sont utilisées par Active Directory : journal USN (Unique Serial Number), service de réplication... Aussi, vous devrez formater le système de fichier de la partition d'amorçage (celle qui contient Windows) en NTFS et disposer de 250 Mo libres pour mettre en place Active Directory sur un serveur.

1.4. Authentifications, domaines et approbations

Une approbation entre deux domaines est une relation entre ces domaines qui permet aux objets (utilisateurs, groupes...) d'un domaine d'être visibles et authentifiables sur l'autre domaine.

Pour voir et configurer les approbations, vous utiliserez la console MMC Domaines et approbations Active Directory.

Il existe plusieurs types d'approbations entre domaines.

Active Directory introduit l'approbation bidirectionnelle transitive.

Dans une forêt, les domaines père et fils sont automatiquement et implicitement liés par une approbation mutuelle : une approbation bidirectionnelle transitive implicite.

L'approbation est bidirectionnelle : elle est valable dans les deux sens.

La transitivité signifie ici que cette approbation est également valable et visible par les domaines parents et enfants de ces deux domaines.

Elle est implicite car automatique.

Dans une forêt tous les domaines s'approuvent donc, directement ou indirectement.

Pour raccourcir le chemin entre domaines, parcouru lors des authentifications (appelé chemin d'approbation), vous pouvez créer manuellement une approbation bidirectionnelle transitive explicite entre deux domaines très éloignés. Vous pouvez ainsi accélérer les authentifications entre domaines éloignés dans la forêt.

Entre les forêts, ou vers des domaines NT4, il faut avoir recours aux anciennes approbations : les approbations unidirectionnelles non transitives. Un domaine en approuve un autre. Vous devrez répéter l'opération dans le sens inverse pour obtenir l'équivalent d'une approbation bidirectionnelle.

Mode du domaine

Par défaut, à l'installation ou après une migration depuis NT4, le domaine est en mode mixte. Ce mode vous permet de maintenir dans le domaine vos vieux contrôleurs de domaines secondaires fonctionnant sous NT4 (des BDC – Backup Domain Controller).

Il s'agit donc d'un mode de compatibilité, mais qui limite les possibilités d'Active Directory.

Chaque domaine peut être basculé en mode natif. Il perd alors la possibilité de conserver des BDC NT4, mais acquiert plusieurs possibilités nouvelles :

- Les groupes universels de sécurité deviennent disponibles (voir plus loin).
- L'imbrication des groupes devient possible et leur visibilité est améliorée (voir plus loin).
- Les clients pré-Windows2000 ont accès aux approbations transitives entre les domaines de la forêt.

Le mode natif permet toujours bien entendu aux anciens clients (tels les clients et serveurs NT4 membres) de se connecter au domaine.

Le basculement est irréversible.

Utilisateurs, Groupes et permissions

Utilisateurs et groupes

Les utilisateurs et les groupes existent à la fois dans la base des utilisateurs locale de chaque ordinateur (appelée base SAM) et dans l'annuaire Active Directory.

Avec Active Directory, les groupes les plus importants sont les groupes de sécurité. Ils peuvent être utilisés dans le cadre des DACL (Listes d'accès fixant les permissions – Discretionary Access List). Par exemple vous pouvez donner à un groupe de sécurité l'autorisation de lire le contenu d'un répertoire NTFS.

En revanche, les groupes de distribution n'intéressent que les administrateurs de messageries comme Exchange, et permettent comme leur nom l'indique de sélectionner des groupes d'utilisateurs pour la distribution des messages.

L'administrateur du domaine racine fait partie de plusieurs groupes spécifiques :

- Le groupe Administrateurs de l'Entreprise (unique à la forêt), qui lui permet d'intervenir sur tous les domaines de la forêt et d'ajouter des domaines.
- Le groupe Administrateurs du Schéma (unique à la forêt), qui lui permet d'intervenir sur le schéma de la forêt.
- Le groupe Administrateurs du Domaine pour son domaine (il s'agit en l'occurrence du domaine racine). Dans chaque domaine de la forêt, il existe un tel groupe.

Etendue des groupes

Il existe trois types de groupes, chacun pouvant être de sécurité ou de distribution.

En l'absence de BDC NT4, il est possible et conseillé de basculer le domaine en mode natif. Ce basculement irréversible permet d'exploiter totalement les avantages d'Active Directory par rapport aux anciens domaines, en offrant notamment de nouvelles possibilités concernant les groupes dans le domaine.

Contrôleurs de domaine, sites et réplication

Types de contrôleurs

Certains contrôleurs de domaine peuvent être configurés comme « contrôleurs de catalogue global » (ou GC – Global Catalog) par le biais de la console MMC Sites et Services Active Directory. Ces catalogues contiennent non seulement les données de leur propre domaine mais également certaines informations des autres domaines de la forêt. Ils permettent d'accélérer les recherches d'objets dans la forêt.

En mode Natif, il est important de noter qu'un contrôleur de catalogue global doit être disponible dans le site pour que les utilisateurs puissent se connecter dans le domaine : en effet ces contrôleurs permette de vérifier l'appartenance des utilisateurs à des groupes universels.

En cas de panne de ces contrôleurs, seuls les administrateurs du domaine peuvent se loguer. Vous aurez donc besoin de placer suffisamment de GC pour assurer une redondance en cas de panne. Vous devez cependant noter que la réplication de leurs informations est plus volumineuse en données sur le réseau que pour les autres contrôleurs.

Fonctionnement à maître unique

<http://support.microsoft.com/default.aspx?scid=kb;fr;197132>

Pour certaines tâches, Active Directory utilise un fonctionnement à maître unique au lieu d'un fonctionnement multi-maître. Il existe 5 types de maîtres, qui sont les seuls à pouvoir remplir leur fonction dans leur forêt ou dans leur domaine

Maître	Existence	Rôle
Contrôleur de schéma	1 par forêt	Permet de modifier le schéma de la forêt (par les membres du groupe Administrateurs du Schéma).

Contrôleur d'attribution de nom de domaine	1 par forêt	- Permet d'ajouter des domaines à la forêt. - Est également contrôleur de catalogue global.
Emulateur de PDC	1 par domaine	- Mode Natif : Synchronise les heures des DC ; bénéficie d'une réplication immédiate des mots de passe modifiés pour permettre aux autres DC de vérifier qu'il ne vient pas d'être changé avant de rejeter une tentative de login. - Mode Mixte : Gère également la réplication des informations de domaine vers les BDC sous NT4.
Maître RID (d'identificateur relatif)	1 par domaine	Distribue des plages de numéros aux DC pour éviter les doublons lors de l'attribution des SID (identificateurs uniques) aux objets.
Maître d'infrastructure	1 par domaine	- Met à jour les références vers les objets d'autres domaines. - Ne doit pas être contrôleur de catalogue global (sauf contrôleur unique).

En cas de perte du contrôleur de domaine hébergeant un ou plusieurs rôles, ou simplement si le besoin de transférer un rôle apparaît, vous avez la possibilité de transférer ou de saisir ce ou ces rôles sur un autre contrôleur.

Vous pouvez effectuer cette procédure dans deux situations.

- S'il s'agit d'un transfert entre serveurs en activité, vous pourrez utiliser l'interface graphique (Consoles Sites et Services pour les trois maîtres de domaine, console Schéma d'une part et console Domaines et approbations d'autre part pour les deux maîtres de forêt). Vous pouvez aussi avoir recours à l'outil en mode texte ntdsutil (fonction « transfer »).
- S'il s'agit de saisir un rôle perdu en raison d'un maître définitivement hors-ligne, seul ntdsutil (fonction « seize » pour « saisir » le rôle) est utilisable.

Organisation logique

Active Directory permet d'organiser une forêt en arborescences, domaines, Unités Organisationnelles (OU).

Une OU est un conteneur dans un domaine, permettant d'organiser les différents objets, et qui peut contenir à son tour d'autres OU. Il est donc fréquent de déplacer des comptes de leur emplacement par défaut vers des OU. Les délégations de tâches administratives s'effectuent au niveau de l'OU.

Parallèlement, il existe également un autre type de structure, commun à toute la forêt : les Sites, qui permettent d'optimiser les répliquions et les logins. Au départ, il n'existe qu'un site : le Premier-site-par-défaut. Il n'y a ni imbrication de sites ni hiérarchie de sites.

Par défaut, plusieurs conteneurs existent à la création d'un domaine ; l'un est une OU (et contient même une GPO par défaut) mais la plupart sont des conteneurs par défaut qui ne permettent ni de leur appliquer directement des stratégies de groupe, ni de créer des OU filles.

On trouve ainsi :

Builtin	Contient les utilisateurs et groupes de sécurité existant par défaut.
Computers	Reçoit par défaut les comptes d'ordinateur.
Domain Controllers (OU)	Reçoit par défaut les comptes d'ordinateurs Contrôleurs de Domaine. Une GPO est appliquée par défaut à ce conteneur.
ForeignSecurityPrincipal	Contient les identificateurs de sécurité (SID).
Users	Reçoit par défaut les comptes d'utilisateurs.
LostAndFound	Accueille les objets orphelins dont le conteneur n'existe plus.

System	Contient des paramètres systèmes.
--------	-----------------------------------

Sites, serveur et réplication

Le bon fonctionnement d'Active Directory dépend de la réplication des données entre tous les contrôleurs de domaine. En effet Active Directory fonctionne suivant le principe de la réplication multi-maître, et chaque contrôleur de domaine peut être utilisé pour modifier les objets du domaine (création d'utilisateurs, modification de stratégie, etc...). Il importe donc que les données soient bien synchronisées entre les contrôleurs. Cependant, il importe également que le trafic utilisé par la réplication ne devienne pas trop important.

Réplication intra-site

La réplication est automatiquement prise en charge, et dans un site unique les informations mises à jours sont transférées toutes les 5 minutes aux autres contrôleurs. Pour éviter toute désynchronisation, l'ensemble des données est répliqué toutes les 24h.

Certaines données très urgentes sont cependant répliquées immédiatement (modification de mots de passe...). Cette réplication immédiate dépend du bon fonctionnement de l'émulateur de PDC.

Réplication inter-sites

La réplication Active Directory fonctionne différemment lorsqu'il est question de liaisons WAN plus lentes, et donc de sites multiples. Il est important de déclarer des sous-réseaux IP différents pour chaque site, et de déclarer chaque site (et les DC qu'il contient) dans la console MMC Sites et Services. Les clients s'authentifieront sur les DC les plus proches (les DC de leur site) grâce à ces différences de sous-réseaux IP.

Vous devez vous assurer que chaque site contient un ou plusieurs GC.

Un processus appelé KCC (Knowledge Consistency Checker) est lancé à intervalles réguliers sur chaque DC (par défaut toutes les 15 minutes), et prend en charge l'établissement de liaisons virtuelles entre les DC, en vue de la réplication.

=> Attention, il ne s'agit pas ici des liens inter-sites, mais plutôt du routage virtuel des informations de réplication. Les liens inter-sites doivent exister pour que le KCC fonctionne ; ils sont abordés plus loin.

Pour chaque site, le KCC déclare automatiquement un DC en tant que « serveur tête de pont ». Celui-ci assurera à lui seul pour ce site la communication vers les contrôleurs des autres sites. En cas de modification de la topologie réseau ou en cas de panne, le KCC modifiera en conséquence cette attribution. Vous pouvez cependant forcer un serveur tête de pont dans le cas par exemple où un firewall serait configuré pour ne laisser sortir du site qu'un seul DC bien précis.

Liens inter-sites

Vous créez les liens dans la console MMC Sites et Services. Après avoir créé des liens, vous devez les utiliser pour relier vos sites. Si les sites ne sont pas reliés par ces liens, ils ne pourront pas communiquer.

Deux types de liens existent : les liens IP (le cas général) et les liens SMTP.

Les liens IP nécessite une liaison fiable, ils peuvent relier n'importe quels sites quel que soient le ou les domaines qui y sont présents.

Les liens SMTP (Simple Mail Transfert Protocol) ne doivent être utilisés que dans le cas où la liaison est peu fiable, et uniquement entre domaines différents. Ils font appel à la transmission par e-mail.

Les réplications par lien IP peuvent faire l'objet d'une planification. Les paramètres disponibles sont la fréquence de réplication (par défaut, toutes les 180 minutes), et les horaires durant lesquelles la réplication peut avoir lieu. Ces horaires doivent être assez étendus pour que la fréquence choisie puisse donner lieu à réplication.

Les réplications SMTP ne peuvent faire l'objet d'aucune planification.

Coût des liens

A chaque lien inter-site est affecté un coût pour la liaison (par défaut : 100). Ce coût s'apparente à la métrique des routeurs. Ainsi, pour joindre un site distant de plusieurs autres sites, le coût total sera pris en compte pour la détermination des liens à utiliser.

Les liens intra-sites sont cryptés. Les liens inter-sites sont cryptés et compressés.

Un DC ne peut appartenir qu'à un seul site.

Pour les architectures les plus complexes, il est à noter qu'un même domaine peut être réparti (présence de contrôleurs et/ou de clients) sur plusieurs sites de la forêt ; au moins un GC par domaine et par site est à prévoir.

Stratégies de groupes (Group Policies / GPO)

Présentation des stratégies de groupe

Les stratégies de groupe ou les stratégies systèmes permettent de configurer administrativement des restrictions ou des paramètres à appliquer sur tel ou tel ordinateur, sur tel ou tel compte utilisateur.

Sous Windows NT4, les stratégies systèmes étaient implémentées par le biais de l'outil POLEDIT, qui permettait de créer un fichier config.pol. Ce fonctionnement reste d'actualité pour les NT4 membres d'un domaine Active Directory (et ce fichier sera placé dans le répertoire partagé NETLOGON).

Les stratégies de groupe (GPO), quant à elles, n'ont un effet que sur les ordinateurs fonctionnant sous Windows 2000 ou ultérieur. Leur fonctionnement est tout à fait différent. Elles sont à la fois détaillées et souples et permettent de configurer les différents paramètres de façon très précise.

Les GPO ne peuvent être appliqués qu'à des conteneurs : un site, un domaine ou une OU. Leur contenu aura effet sur les comptes d'ordinateurs et d'utilisateurs contenus dans le conteneur concerné, et ses enfants par héritage.

L'ordre d'application, du moins prioritaire au plus prioritaire, est globalement du plus éloigné au plus proche, à l'exception de la stratégie locale présente sur chaque ordinateur, qui est la moins prioritaire :

Local → Site → Domaine du plus lointain au plus proche → OU de la plus lointaine à la plus proche

Chacun des multiples paramètres d'une GPO peut être configuré ou pas. Si un paramètre n'est pas configuré, il ne provoque pas de conflit.

Si des paramètres configurés entrent en conflit, l'échelle de priorité précédente détermine le paramètre à appliquer.

Si vous appliquez directement plusieurs GPO sur une OU, la GPO la plus élevée (la première) est la plus prioritaire ; la dernière, la moins prioritaire.

Héritage des stratégies de groupe

Les GPO appliquées à des sites ne sont pas concernées puisque les sites ne sont pas organisés hiérarchiquement.

Par défaut :

- Les GPO appliquées à un domaine sont héritées de domaine père en domaines fils.
- Les GPO appliquées à une OU sont héritées d'OU mère en OU filles.

Exceptions : Elles sont deux, configurables pour chaque conteneur (Domaine ou OU) :

- Bloquer l'héritage : Si cette case est cochée, aucune GPO supérieure ne sera héritée par ce conteneur.
- Ne pas passer outre : Si une GPO dispose de ce paramètre, elle sera malgré tout obligatoirement héritable par les conteneurs inférieurs, même si ceux-ci sont configurés pour bloquer l'héritage.

Cas particulier : Certains paramètres font exception à l'ordre d'application et aux possibilités d'héritage. Les paramètres de mots de passe (longueur, complexité) et de verrouillage de compte sont définis une seule fois pour tout le domaine dans la première GPO du domaine. Pour ces paramètres, aucun blocage n'est possible dans le domaine. Si ces paramètres sont définis à un autre emplacement, ils n'ont aucun effet.

Application des stratégies de groupe

Si les GPO peuvent être appliquées uniquement à des conteneurs, elles ont avant tout pour objectif d'être prises en compte par des comptes d'utilisateurs et/ou des comptes d'ordinateur.

C'est pourquoi les GPO peuvent faire l'objet d'un filtrage : chaque GPO est associée à une ACL (Liste d'accès) qui permet de déterminer quels seront les comptes qui seront ou pas concernés, dans le ou les conteneurs.

Note : Il est pratique d'utiliser un groupe pour effectuer un tel filtrage plutôt que d'attribuer des permissions pour chaque objet. Cependant, vous devrez utiliser de préférence des groupes globaux.

Application des GPO selon les objets :

-Pour les comptes utilisateurs : Les comptes sur lesquels la GPO prend effet doivent avoir les permissions Lire et Appliquer la Stratégie, ou faire partie du groupe approprié. Par défaut le groupe « Utilisateurs authentifiés » dispose de ces permissions dans l'ACL d'une GPO, donc par défaut une GPO est valable pour tous les utilisateurs.

- Pour les comptes de machine : La GPO est valable pour tous les comptes de machine par défaut (y compris les contrôleurs de domaine) dans les conteneurs concernés. Les machines qui ne doivent pas être concernées par la GPO (ou leur groupe) doivent faire l'objet d'une permission « Refuser l'application ».

Précision : il semble contradictoire d'indiquer que les GPO ne s'appliquent qu'à des conteneurs alors que la permission « Appliquer la GPO » existe pour les utilisateurs, ordinateurs et groupes. En fait, la GPO s'applique sur un conteneur, et les objets ordinateurs/utilisateurs appliquent la GPO.

GPO par défaut

Chaque domaine dispose d'une GPO vide par défaut, ainsi que d'une GPO sur le conteneur Contrôleurs de Domaine (qui interdit notamment aux simples utilisateurs de se connecter sur les Contrôleurs de Domaine).

Contenu des GPO

Une GPO est divisée en deux parties : Ordinateur et Utilisateur.

Les paramètres de chacune des parties permettent de configurer de nombreux éléments de l'environnement utilisateur, de la sécurité, du fonctionnement de l'ordinateur...

Scripts

Les GPO permettent en outre de spécifier des scripts de démarrage (exécutés par l'ordinateur au lancement de Windows, avant tout login), ainsi que des scripts d'ouverture de session (exécutés au login de l'utilisateur). Les scripts d'ouverture de session permettent notamment de créer des lecteurs réseau (lettre de lecteur associée en réalité à un partage réseau) en fonction des utilisateurs et des groupes.

Par défaut les scripts de démarrage s'exécutent en mode synchrone (les uns après les autres, et aucun login n'est possible avant la fin de leur exécution) et de façon invisible.

En revanche, toujours par défaut, les scripts d'ouverture de session s'exécutent en mode asynchrone (tous en même temps au login) mais restent invisibles.

Vous devez placer les scripts sur n'importe quel DC du domaine (grâce à la réplique), dans le sous répertoire du domaine destiné aux scripts, situé dans le partage SYSVOL.

Les deux parties des GPO

Il n'est pas rare que seuls certains paramètres d'une GPO soient configurés.

Si les objets présents dans le conteneur (OU) et ses enfants sont des ordinateurs, la partie Utilisateur de la GPO n'est pas utilisée. Si les objets sont des utilisateurs, c'est la partie Ordinateur qui est inutilisée. Si les deux types d'objet existent, chaque partie de la GPO configure uniquement le type d'objet qui lui correspond.

Ainsi, sur un ordinateur avec un utilisateur connecté, se trouvent simultanément appliquées :

- par l'ordinateur, les parties Ordinateur des GPO reçues par le compte ordinateur, en fonction de l'emplacement de ce compte dans Active Directory.
- par l'utilisateur, les parties Utilisateurs des GPO reçues par le compte utilisateur, en fonction de l'emplacement de ce compte dans Active Directory.

Il est clair ici que les paramètres Utilisateur d'une GPO ne sont utilisables que s'ils sont appliqués par un objet utilisateur. Les paramètres Utilisateur ne peuvent pas provenir d'une GPO appliquée uniquement par des comptes d'ordinateurs.

Cependant, vous pouvez vouloir modifier ce fonctionnement, dans le cas où la machine est dans un environnement peu sûr (Kiosque, accès libre, laboratoire...). Le paramètre de GPO « Bouclage » permet à l'ordinateur de prendre lui-même en compte la partie Utilisateur de la GPO qu'il utilise ; ces paramètres supplantent voire éliminent totalement les paramètres de GPO normalement appliquée par le login de l'utilisateur. Ainsi vous pourrez facilement définir pour un ordinateur un environnement utilisateur qui sera par exemple très limité, quel que soit l'utilisateur logué.

Techniquement, il est intéressant de rappeler qu'en réalité ce sont les ordinateurs eux-mêmes qui lisent les GPO reçues depuis les DC, et mettent en oeuvre leurs paramètres en fonction de toutes ces règles, pour eux-mêmes et pour les utilisateurs qui se loguent. Cela explique du reste que NT4 ou les autres anciens systèmes ne puissent en bénéficier.

Délai d'application

Par défaut les ordinateurs vérifient qu'ils utilisent la dernière version des GPO toutes les 90 minutes environ (+/- 0 à 30 minutes aléatoires). Ce paramètre est configurable dans la GPO elle-même.

Vous pouvez forcer le rafraîchissement sur chaque machine en utilisant les commandes suivantes (l'une pour les paramètres d'ordinateur, l'autre pour les paramètres utilisateurs) :

(Secedit /refresh machine_policy ; Secedit /refresh user_policy) pour Windows 2000

(GPUPDATE) pour Windows 2003

Divers

Délégation de contrôle

Un des avantages d'Active Directory est la possibilité de déléguer des tâches d'administration de façon très précise (au niveau des OU) à certains utilisateurs, sans leur remettre l'intégralité des permissions d'administration.

Ainsi dans une entreprise il sera très facile de confier la gestion des utilisateurs d'un département à un certain administrateur désigné à cet effet, de permettre à un autre d'appliquer des GPO, voire d'en créer, etc...

Techniquement il s'agit de modifier les ACL des OU en attribuant une ou plusieurs des nombreuses permissions possibles à des utilisateurs, voire à des groupes.

Les permissions dans les ACL d'Active Directory doivent en principe porter sur des groupes globaux.

Vous utiliserez la console Utilisateurs et ordinateurs Active Directory.

Afin de simplifier toutes ces procédures assez techniques, il existe plusieurs assistants qui permettent de déléguer certaines tâches et procédures prédéfinies de façon très simplifiée. L'entrée des informations est facilitée, l'assistant se chargeant d'affecter les permissions ad hoc.

Exemples :

- Un utilisateur peut créer une GPO s'il est dans le groupe « Propriétaires Créateurs de la Stratégie de Groupe ». Il pourra appliquer une GPO à un conteneur s'il dispose des permissions Lire et Ecrire sur le conteneur.
- Un utilisateur pourra ajouter des machines sur le domaine s'il dispose de la permission Créer des objets Ordinateur dans le conteneur Ordinateurs (par défaut tout utilisateur a le droit d'insérer 10 ordinateurs dans le domaine ; cette délégation est nécessaire au delà).

Note :

L'onglet Sécurité des conteneurs n'apparaît que lorsque l'affichage de la console MMC Active Directory appropriée est en mode Fonctionnalités avancées.

Publication de ressources

Active Directory permet de publier des ressources dans l'annuaire : des imprimantes, des contacts, des répertoires partagés. L'intérêt est de permettre à toute personne dans l'entreprise de rechercher des ressources par le biais de la fenêtre de recherche Active Directory disponible sur son poste client. La localisation des ressources est donc facilitée. Les fonctions de recherche ne sont plus limitées aux comptes d'utilisateurs et ordinateurs.

Les imprimantes partagées peuvent par exemple être publiées automatiquement à leur installation sur un ordinateur. Les objets publiés, sortes de « pointeurs », ont une vie indépendante de l'entité réelle dont ils proviennent. Par exemple, pour un répertoire partagé, les permissions du partage sont toujours fixées au niveau du partage lui-même ; des permissions posées sur l'objet dans Active Directory n'auront aucun effet sur les accès réseau au partage.

Scripts et outils

Active Directory peut être modifié par le biais de scripts qui permettent d'insérer, de modifier ou de déplacer de façon plus simple de grandes quantités d'objets. Certains outils en mode texte existent à cet effet.

Le déplacement d'objets entre domaines de la forêt s'effectue avec `movetree`.
L'insertion ou l'exportation de comptes s'effectuent avec `csvde`.
Les insertion, exportation, modification et effacement de comptes s'effectuent avec `ldifde`.

L'outil en mode texte `ntdsutil` permet de régler certains problèmes, en permettant l'accès à des fonctions avancées non disponibles par l'interface graphique. Ainsi vous avez vu qu'il permettait de récupérer un rôle de maître unique en cas d'urgence. Il peut également, entre autres, vous permettre d'effacer d'Active Directory un contrôleur détruit : si vous n'avez pas pu faire un `DCPROMO` pour le rétrograder avant sa disparition, vous ne pouvez pas l'effacer directement de l'annuaire. Vous utiliserez alors la fonction `metadata cleanup` de `ntdsutil`.
`Ntdsutil` permet aussi de défragmenter les fichiers de la base Active Directory (la base doit être hors ligne, vous devez donc redémarrer le DC en mode Restauration Active Directory).

Sauvegarde et restauration

En matière de sauvegarde des contrôleurs de domaine, l'utilitaire de sauvegarde intégré à Windows 2000 sauvegarde les données Active Directory lorsque les données « Etat du système » sont sauvegardées.

La restauration d'Active Directory sur une machine peut être non autoritaire (restauration normale : après la restauration le DC récupérera les dernières informations disponibles auprès des autres DC), ou en mode autoritaire avec `ntdsutil`, qui permet d'indiquer que certains des objets récupérés sont prioritaires et doivent être insérés sur les autres DC. Vous utiliserez cette dernière fonction pour récupérer un objet effacé ou modifié alors que la réplication a déjà eu lieu.

Enfin, il existe un conteneur `LostAndFound` à la racine de chaque domaine. Lorsque deux administrateurs font des modifications sur deux DC différents, il peut arriver par exemple qu'un utilisateur soit déplacé vers une OU qui vient d'être effacée sur l'autre DC, alors que la réplication n'a pas encore eu lieu. Dans ce cas, à la réplication, les objets déplacés (qui deviennent alors orphelins) sont mis dans `LostAndFound` en attente de suppression ou de nouveau déplacement par l'administrateur (qui peut par exemple choisir de recréer l'OU).

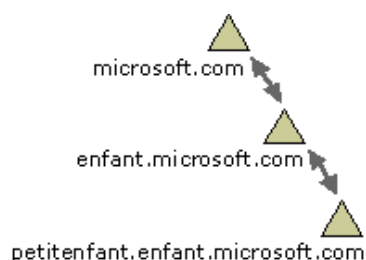
Compatibilité avec les anciennes versions de Windows

NT4, Windows 95 et 98 ne sont pas prévus pour Active Directory ; ils s'y connectent comme à un domaine NT.

Cependant, il est possible de leur ajouter les fonctions de recherche et de parcourir des partages DFS de domaine (Distributed File System) en leur installant le client Active Directory, disponible sur le CD Windows2000 Server pour Win9x, et sur le site web Microsoft pour NT4.

DFS permet d'accéder par un nom de partage unique à des répertoires partagés et répliqués sur plusieurs serveurs du domaine afin d'avoir une tolérance de panne.

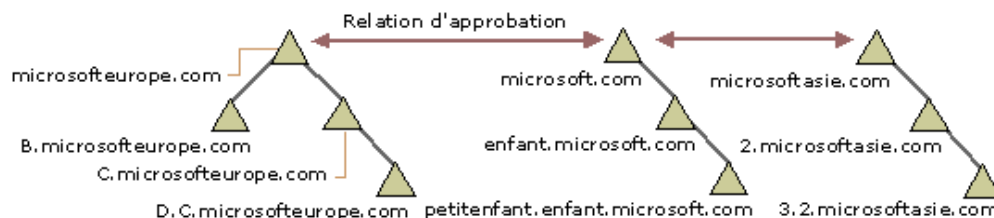
Présentation des arborescences de domaine et des forêts



Chaque domaine de l'annuaire est identifié par un nom de domaine DNS et nécessite un ou plusieurs contrôleurs de domaine. Si votre réseau requiert plusieurs domaines, vous pouvez facilement les créer.

Un ou plusieurs domaines qui partagent un schéma commun et un catalogue global sont appelés forêt. Si plusieurs domaines à l'intérieur d'une forêt ont des noms de domaine DNS contigus, tel qu'il apparaît dans la première illustration, la structure est appelée arborescence de domaine.

Si, tel qu'il apparaît dans la seconde illustration, plusieurs domaines ont des noms de domaine DNS non contigus, ils forment des arborescences de domaine différentes à l'intérieur de la forêt. Une forêt peut contenir une ou plusieurs arborescences de domaine. Le premier domaine d'une forêt est appelé domaine racine de la forêt.



Vous créez un domaine en installant le premier contrôleur de domaine pour un domaine. Au cours de l'installation du premier contrôleur de domaine, l'Assistant Installation de Active Directory utilise les informations que vous fournissez pour installer le contrôleur de domaine et créer le domaine à l'intérieur du contexte (s'il en existe un) existant de relations avec d'autres domaines et contrôleurs de domaine. Ce contexte peut être le premier domaine dans une nouvelle forêt, le premier domaine dans une nouvelle arborescence de domaine ou un domaine enfant d'une arborescence de domaine existante.

Après avoir installé le premier contrôleur de domaine pour un domaine, vous pouvez en installer d'autres dans un domaine existant afin de garantir la tolérance de panne et une haute disponibilité de l'annuaire.

Attribution de noms de domaine

Les domaines qui forment une arborescence de domaine unique partagent un espace de noms contigu (hiérarchie de nommage). Selon les normes DNS, le nom de domaine complet d'un domaine qui fait partie d'un espace de noms contigu est le nom de ce domaine ajouté aux noms du domaine parent et du domaine racine séparés par un point (.). Par exemple, un domaine qui porte le nom NetBIOS « petitenfant » et qui a un domaine parent nommé parent.microsoft.com, a comme nom de domaine DNS complet petitenfant.parent.microsoft.com.

Les arborescences de domaine associées dans une forêt partagent le même schéma Active Directory, ainsi que la même configuration d'annuaire et les mêmes informations de répliquon, mais elles ne partagent pas un espace de noms de domaine DNS contigu.

La combinaison des arborescences de domaine et des forêts vous offre des options d'attribution de noms de domaine flexibles. Vous pouvez inclure des espaces de noms DNS à la fois contigus et non contigus dans votre annuaire.

Pour plus d'informations sur Active Directory et DNS, consultez [DNS \(Domain Name System\)](#)

Relations d'approbation

Pour les ordinateurs Windows 2000, l'authentification de compte entre les domaines est activée par des approbations transitives à deux sens, basées sur le protocole de sécurité Kerberos V5.

Les relations d'approbation sont créées automatiquement entre domaines adjacents (domaine parent et domaine enfant) lorsque vous créez un domaine dans une arborescence de domaine. Dans une forêt, une relation d'approbation est créée automatiquement entre le domaine racine de la forêt et le domaine racine de chaque arborescence de domaine ajoutée à la forêt. Ces relations d'approbation étant transitives, les utilisateurs et les ordinateurs peuvent être authentifiés entre tous les domaines de l'arborescence de domaine ou de la forêt.

Lors de la mise à niveau d'un domaine Windows vers Windows 2000, les relations à sens unique existant entre ce domaine et d'autres domaines sont maintenues. Ceci inclut toutes les approbations avec des domaines antérieurs à Windows 2000. Si vous installez un nouveau domaine Windows 2000, et vous souhaitez établir des relations d'approbation avec des domaines antérieurs à Windows 2000, vous devez créer des approbations externes avec ces domaines.

AD 2003 ET AD 2000 compatible ?

Malheureusement pas entièrement, il faut migrer l'ad en version 2003 avant de pouvoir insérer un serveur 2003 dans un AD 2000

La clé des relations 2000/2003 c'est adprep : prépare Windows 2000 pour une mise à jour ou accueil de Windows 2000 server.

Vue d'ensemble : Mise à niveau de contrôleurs de domaine Windows 2000 vers Windows Server 2003

La commande adprep de Windows Server 2003 que vous exécutez à partir du dossier \I386 du support de Windows Server 2003 prépare une forêt Windows 2000 et ses domaines à l'ajout de contrôleurs de domaine Windows Server 2003. La commande adprep /forestprep de Windows Server 2003 ajoute les fonctionnalités suivantes :

- Descripteurs de sécurité par défaut améliorés pour les classes d'objet
- Nouveaux attributs d'utilisateur et de groupe
- Nouveaux objets et attributs de schéma tels que inetOrgPerson

L'utilitaire adprep prend en charge deux arguments de ligne de commande :

adprep /forestprep : exécute les opérations de mise à niveau de la forêt.
adprep /domainprep : exécute les opérations de mise à niveau du domaine.

La commande adprep /forestprep est une opération unique effectuée sur le maître de l'opération du schéma (FSMO) de la forêt. L'opération forestprep doit s'achever et se répliquer vers le maître d'infrastructure de chaque domaine pour que vous puissiez exécuter adprep /domainprep dans ce domaine.

La commande adprep /domainprep est une opération unique que vous exécutez sur le contrôleur de domaine du maître des opérations d'infrastructure de chaque domaine dans la forêt qui hébergera des contrôleurs de domaine Windows Server 2003 nouveaux ou mis à niveau. La commande d'adprep /domainprep vérifie que les modifications de forestprep ont été répliquées dans la partition du domaine, puis opère ses propres modifications dans la partition du domaine et les stratégies de groupe dans le partage Sysvol.

Vous ne pouvez pas exécuter l'une ou l'autre des actions suivantes si les opérations /forestprep et /domainprep ne se sont pas terminées et répliquées sur tous les contrôleurs de domaine dans ce domaine :

- Mettre à niveau des contrôleurs de domaine Windows 2000 vers Windows Server 2003 en utilisant Winnt32.exe.

Remarque : Vous pouvez à tout moment mettre à niveau les serveurs et les ordinateurs membres Windows 2000 vers Windows Server 2003.

- Promouvoir de nouveaux contrôleurs de domaine Windows Server 2003 dans le domaine en utilisant Dcpromo.exe.

Le domaine qui héberge le maître d'opérations du schéma est le seul domaine où vous devez exécuter `adprep /forestprep` et `adprep /domainprep`. Dans tous les autres domaines, il vous suffit d'exécuter `adprep /domainprep`.

Les commandes `adprep /forestprep` et `adprep /domainprep` n'ajoutent pas d'attributs à l'ensemble partiel d'attributs du catalogue global n'entraînent pas de synchronisation complète du catalogue global. La version RTM de `adprep /domainprep` provoque une synchronisation complète du dossier \Policies dans l'arborescence Sysvol. Même si vous exécutez `forestprep` et `domainprep` plusieurs fois, les opérations effectuées ne sont exécutées qu'une seule fois.

Une fois les modifications de `adprep /forestprep` et de `adprep /domainprep` répliquées, vous pouvez mettre à niveau les contrôleurs de domaine Windows 2000 vers Windows Server 2003 en exécutant `Winnt32.exe` à partir du dossier \I386 du support de Windows Server 2003. De plus, vous pouvez ajouter de nouveaux contrôleurs de domaine Windows Server 2003 au domaine en utilisant `Dcpromo.exe`.

Mise à niveau de la forêt à l'aide de la commande `adprep /forestprep`

Pour préparer une forêt et des domaines Windows 2000 de manière à accepter des contrôleurs de domaine Windows Server 2003, effectuez ces étapes dans un premier temps dans un environnement de laboratoire, puis dans un environnement de production :

1. Assurez-vous que vous avez effectué toutes les opérations de la phase "Inventaire de la forêt" en faisant particulièrement attention aux éléments suivants :
 - a. Vous avez créé des sauvegardes de l'état du système.
 - b. Tous les contrôleurs de domaine Windows 2000 de la forêt disposent de tous les correctifs logiciels et Service Packs appropriés.
 - c. La réplication de bout en bout d'Active Directory s'exécute partout dans la forêt
 - d. FRS réplique correctement la stratégie du système de fichiers dans chaque domaine.
2. Ouvrez une session sur la console du maître d'opérations de schéma à l'aide d'un compte qui est membre du groupe de sécurité Administrateurs de schéma.
3. Vérifiez que le schéma FSMO a exécuté la réplication entrante de la partition du schéma en tapant le code suivant à une invite de commandes Windows NT :

```
repadmin /showreps
```

(repadmin est installé à partir du dossier Support\Tools de Active Directory.)

4. La documentation précédente de Microsoft vous recommande d'isoler le maître d'opérations du schéma sur un réseau privé avant d'exécuter `adprep /forestprep`. Néanmoins, la pratique indique que cette étape n'est pas nécessaire et peut provoquer le rejet des modifications du schéma par un maître d'opérations du schéma lorsqu'il est redémarré sur un réseau privé. Si vous souhaitez isoler les ajouts du schéma opérés par `adprep`, Microsoft vous recommande de désactiver temporairement la réplication sortante d'Active Directory avec l'utilitaire de ligne de commande `repadmin`. Pour cela, procédez comme suit :

- a. Cliquez sur Démarrer, sur Exécuter, tapez `cmd`, puis cliquez sur OK.
- b. Tapez la commande suivante et appuyez sur ENTRÉE :

```
repadmin /options +DISABLE_OUTBOUND_REPL
```

5. Exécutez `adprep` sur le maître d'opérations du schéma. Pour ce faire, cliquez sur Démarrer, sur Exécuter, tapez `cmd`, puis cliquez sur OK. Sur le maître d'opérations du schéma, tapez la commande suivante :

```
X:\I386\adprep /forestprep
```

, où X:\I386\ est le chemin d'accès du support d'installation de Windows Server 2003. Cette commande exécute la mise à niveau du schéma à l'échelle de la forêt.

Remarque Vous pouvez ignorer les événements portant l'ID 1153 enregistrés dans le journal des événements Service d'annuaire, tel que l'exemple qui suit : Type d'événement : Erreur

Source de l'événement : NTDS Général

Catégorie de l'événement : Traitement interne

ID de l'événement : 1153

Date : JJ/MM/AAAA

Heure : HH:MM:SS

Utilisateur : Ordinateur Tout le monde : <des contrôleurs de domaine>

Description : L'identificateur de classe 655562 (nom de classe msWMI-MergeablePolicyTemplate) a une superclasse 655560 non valide. Héritage ignoré.

6. Vérifiez que la commande `adprep /forestprep` s'est exécutée avec succès sur le maître d'opérations du schéma. Pour ce faire, vérifiez les éléments suivants à partir de la console du maître d'opérations du schéma :

- La commande `adprep /forestprep` s'est terminée sans erreur.
- L'objet `CN=Windows2003Update` est écrit sous `CN=ForestUpdates, CN=Configuration, DC = domaine_racine_forêt`. Enregistrez la valeur de l'attribut `Revision`.
- (Facultatif) La version du schéma a été incrémentée à la version 30. Pour cela, observez l'attribut `ObjectVersion` sous `CN=Schema, CN=Configuration, DC = domaine_racine_forêt`.

Si `adprep /forestprep` ne s'exécute pas, vérifiez les éléments suivants :

- Le chemin complet pour le fichier `Adprep.exe` situé dans le dossier `\i386` du support d'installation a été spécifié lors de l'exécution de `adprep`. Pour cela, tapez la commande suivante :
`x:\i386\adprep /forestprep`
où `x` est le lecteur contenant le support d'installation.
- L'utilisateur connecté qui exécute `adprep` appartient au groupe de sécurité `Administrateurs de schéma`. Pour le vérifier, utilisez la commande `whoami /all`.
- Si `adprep` ne fonctionne toujours pas, affichez le fichier `Adprep.log` dans le dossier `%systemroot%\System32\Debug\Adprep\Logs\Dernier_journal`.

7. Si vous avez désactivé la réplication sortante sur le maître d'opérations du schéma à l'étape 4, activez la réplication afin que les modifications du schéma effectuées par `adprep /forestprep` puissent être propagées. Pour cela, procédez comme suit :

- a. Cliquez sur `Démarrer`, sur `Exécuter`, tapez `cmd`, puis cliquez sur `OK`.
- b. Tapez la commande suivante et appuyez sur `ENTRÉE` :
`repadmin /options -DISABLE_OUTBOUND_REPL`

8. Vérifiez que les modifications de `adprep /forestprep` se sont répliquées sur tous les contrôleurs de domaine de la forêt. Ceci est utile pour surveiller les attributs suivants :

- a. Incrémentement de la version du schéma
- b. `CN=Windows2003Update, CN=ForestUpdates, CN=Configuration, DC = domaine_racine_forêt` ou `CN=Operations, CN=DomainUpdates, CN=System, DC = domaine_racine_forêt` et les GUID d'opérations au-dessous se sont répliqués.
- c. Recherchez les nouvelles classes, objets, attributs ou autres modifications de schéma ajoutés par `adprep /forestprep`, par exemple `inetOrgPerson`. Affichez les fichiers `SchXX.ldf` (où `XX` est un nombre entre 14 et 30) dans le dossier `%systemroot%\System32` pour déterminer quels objets et attributs devraient s'y trouver. Par exemple, `inetOrgPerson` est défini dans `Sch18.ldf`.

9. Recherchez les noms complets LDAP décomposés.

Si Exchange 2000 a été installé avant que vous ayez exécuté la commande `adprep /forestprep` de Windows Server 2003, consultez la section "Identification des attributs de nom décomposés" de l'article suivant de la base de connaissance Microsoft.

[314649](#) La commande ADPREP de Windows Server 2003 provoque une déformation d'attributs dans les forêts Windows 2000 qui contiennent des serveurs Exchange 2000

Si vous trouvez des noms décomposés, passez au Scénario 3 de la section "Exchange 2000 dans les forêts Windows 2000" de cet article.

10. Connectez-vous à la console du maître d'opérations du schéma avec un compte appartenant au groupe de sécurité de `Administrateurs du schéma` de la forêt qui héberge le maître d'opérations du schéma.

Mise à niveau du domaine avec la commande `adprep /domainprep`

Exécutez `adprep /domainprep` après la réplication complète des modifications de `/forestprep` vers le contrôleur de domaine du maître d'infrastructure dans chaque domaine qui hébergera des contrôleurs de domaine Windows Server 2003. Pour cela, procédez comme suit :

1. Identifiez le contrôleur de domaine du maître d'infrastructure dans le domaine que vous mettez à niveau, puis connectez-vous avec un compte qui est membre du groupe de sécurité Administrateurs de domaine dans le domaine que vous mettez à niveau.

Remarque : L'administrateur de l'entreprise peut ne pas être un membre du groupe de sécurité Administrateurs du domaine dans les domaines enfants de la forêt.

2. Exécutez `adprep /domainprep` sur le maître d'infrastructure. Pour ce faire, cliquez sur Démarrer, cliquez sur Exécuter, tapez `cmd`, puis sur le maître d'infrastructure tapez la commande suivante :

```
X:\I386\adprep /domainprep
```

où `X:\I386\` est le chemin d'accès du support d'installation de Windows Server 2003. Cette commande exécute des modifications à l'échelle du domaine dans le domaine cible.

Remarque : la commande `adprep /domainprep` modifie les autorisations de fichiers dans le partage Sysvol. Ces modifications provoquent une synchronisation complète des fichiers dans cette arborescence.

3. Vérifiez que la commande `domainprep` s'est exécutée avec succès. Pour cela, vérifiez les éléments suivants :

- La commande `adprep /domainprep` s'est exécutée sans erreur.
- Le `CN=Windows2003Update,CN=DomainUpdates,CN=System,DC=chemin d'accès du nom du domaine à mettre à niveau` existe

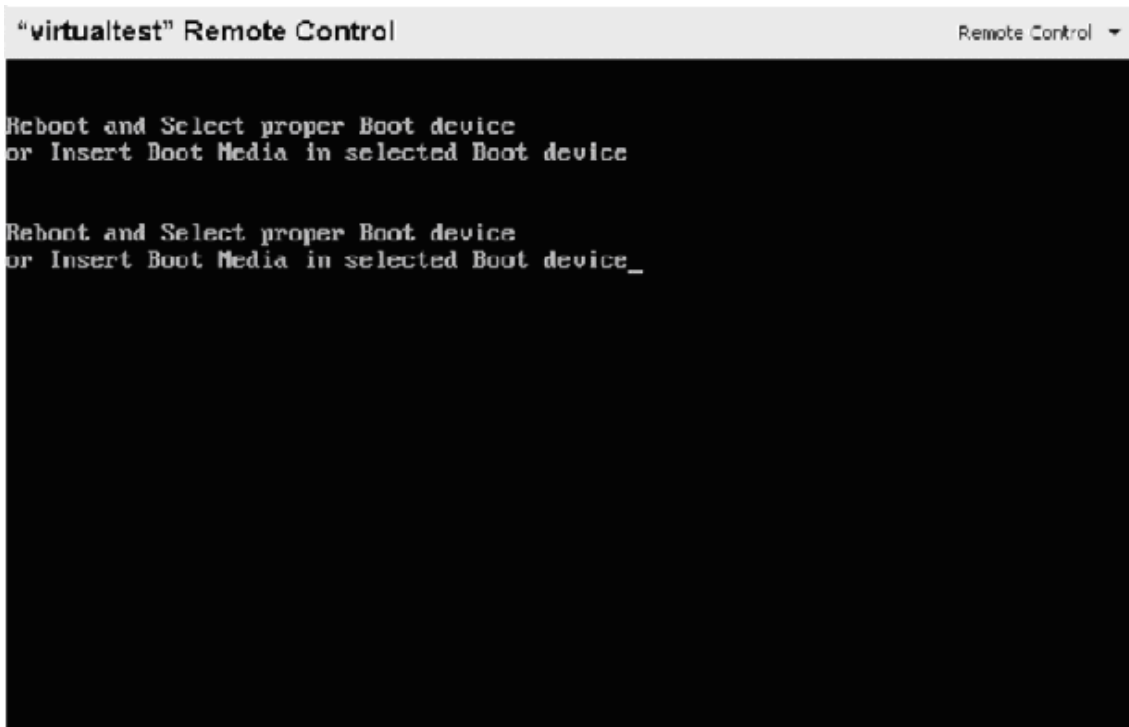
Si `adprep /domainprep` ne s'exécute pas, vérifiez les éléments suivants :

- L'utilisateur connecté qui exécute `adprep` appartient au groupe de sécurité Administrateurs du domaine dans le domaine que vous mettez à niveau. Pour cela, utilisez la commande `whoami /all`.
- Le chemin complet pour le fichier `Adprep.exe` situé dans le répertoire `\I386` du support d'installation a été spécifié lors de l'exécution de `adprep`. Pour cela, tapez la commande suivante à une invite de commandes :
`x:\i386\adprep /forestprep`
où `x` est le lecteur qui héberge le support d'installation.
- Si `adprep` ne fonctionne toujours pas, affichez le fichier `Adprep.log` dans le dossier `%systemroot%\System32\Debug\Adprep\Logs\Dernier_journal`.

4. Vérifiez que les modifications de `adprep /domainprep` se sont répliquées. Pour ce faire, vérifiez les éléments suivants pour les autres contrôleurs de domaine :

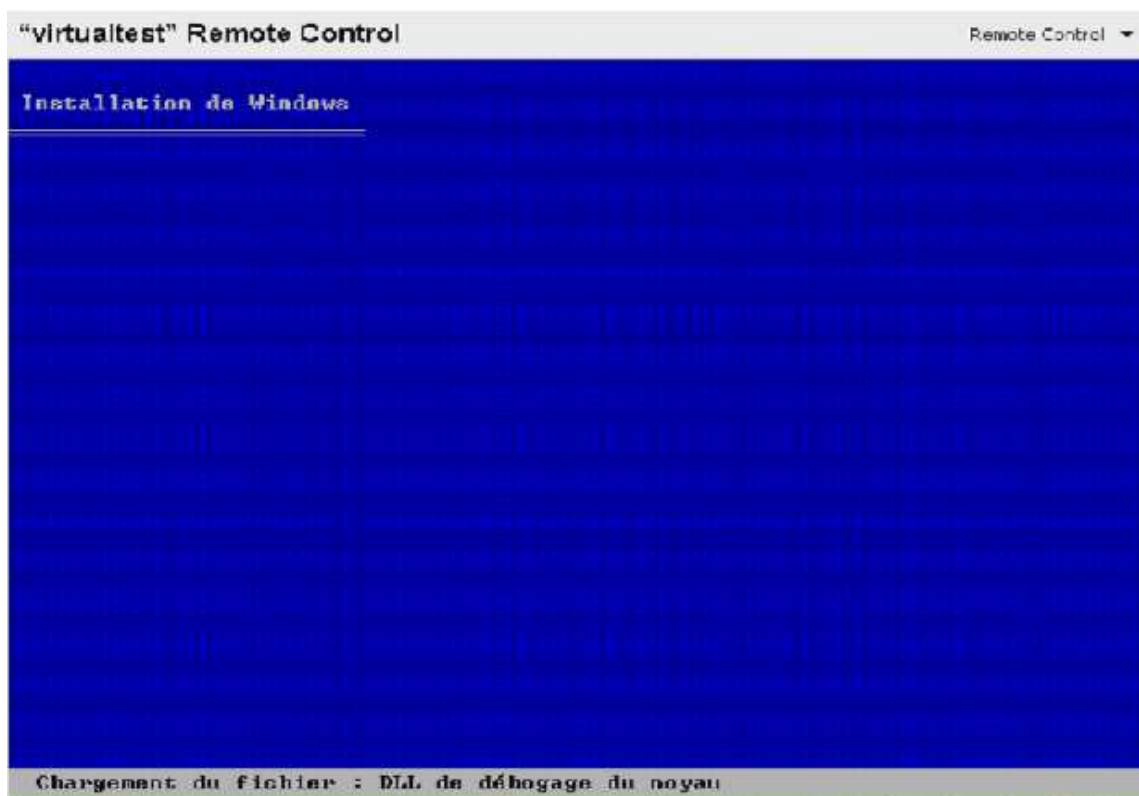
- L'objet `CN=Windows2003Update,CN=DomainUpdates,CN=System,DC = chemin d'accès du nom du domaine à mettre à niveau` existe et la valeur de l'attribut Révision correspond à la valeur du même attribut sur le maître d'infrastructure du domaine.
- (Facultatif) Recherchez les modifications d'objets, d'attributs ou de liste de contrôle d'accès (ACL) qu'a ajoutées `adprep /domainprep`.

INSTALLATION SERVEUR 2003 STANDARD



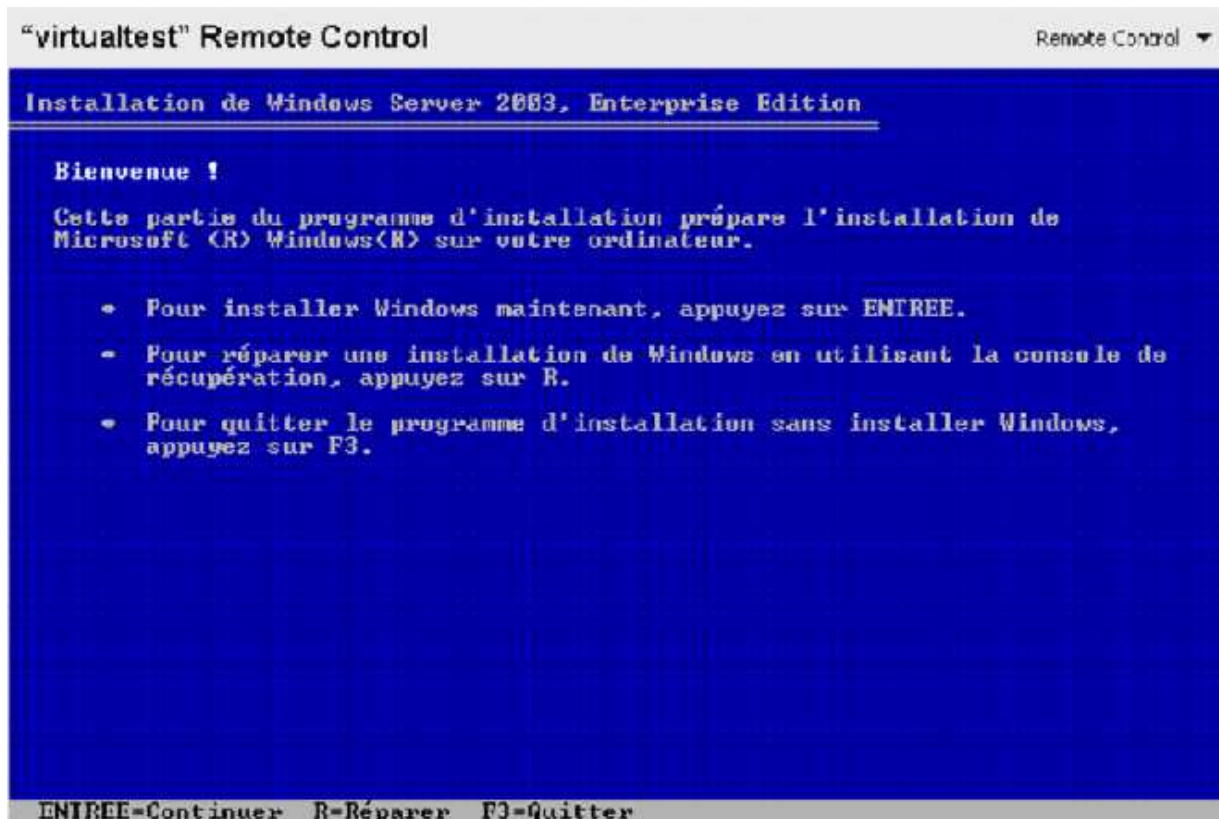
Mise en oeuvre : A ma disposition, un CD-ROM d'installation bootable de Windows 2003. Démarrage de l'ordinateur avec option de boot par le lecteur CD-ROM, Appuyer sur une touche pour lancer la procédure d'installation.

Chargement des pilotes RAID et SCSI comme sous Windows 2000, appuyer sur F6 si vous avez besoins d'installer un pilote très spécifique à votre configuration.





Appuyer sur la touche **ENTRER**



Appuyer sur la touche **ENTRER**

Contrat de licence de Windows

CONTRAT DE LICENCE UTILISATEUR FINAL POUR
LOGICIEL MICROSOFT

MICROSOFT WINDOWS SERVER 2003, STANDARD
EDITION
MICROSOFT WINDOWS SERVER 2003, ENTERPRISE
EDITION

VEUILLEZ LIRE ATTENTIVEMENT CE CONTRAT DE
LICENCE UTILISATEUR FINAL (« CLUF »). EN INSTALLANT
OU EN UTILISANT LE LOGICIEL QUI ACCOMPAGNE CE
CLUF (LE « LOGICIEL »), VOUS RECONNAISSEZ ÊTRE LIÉ
PAR LES TERMES DU PRÉSENT CLUF. SI VOUS ÊTES EN
DÉSACCORD AVEC LES TERMES DE CE CLUF, VEUILLEZ
NE PAS UTILISER LE LOGICIEL ET, LE CAS ÉCHÉANT,
RETOURNEZ-LE À L'ENDROIT OÙ VOUS VOUS L'ÊTES
PROCURÉ, AFIN D'EN OBTENIR LE REMBOURSEMENT
INTÉGRAL.

CE LOGICIEL NE TRANSMET AUCUNE INFORMATION
D'IDENTIFICATION PERSONNELLE DE VOTRE SERVEUR
AUX SYSTÈMES INFORMATIQUES DE MICROSOFT SANS
VOTRE CONSENTEMENT.

1. DISPOSITIONS GÉNÉRALES. Le présent CLUF constitue
un contrat entre vous (personne physique ou personne
morale unique) et Microsoft Corporation (« Microsoft »). Le
présent CLUF régit l'utilisation du Logiciel, qui inclut des

F8=J'accepte ECHAP=Je n'accepte pas PG.SUIV=Page suiv.

Puis appuyer sur la touche **F8** du clavier pour accepter la licence

Installation de Windows Server 2003, Enterprise Edition

La liste suivante affiche les partitions existantes et l'espace
non partitionné sur cet ordinateur.

Utilisez les flèches HAUT et BAS pour sélectionner un élément dans la liste.

- Pour installer Windows à l'emplacement sélectionné,
appuyez sur ENTREE.
- Pour créer une partition dans l'espace non partitionné, appuyez sur C.
- Pour supprimer la partition sélectionnée, appuyez sur S.

le disque 0 de 16379 Mo ayant l'ID 0 du bus 0 sur atapi [MBR]

C: Partition1 [FAT32] 16379 Mo < 16374 Mo libres>

ENTREE=Installation S=Supprimer une partition F3=Quitter



Ensuite, choisissez le format de disque NTFS, adoptez le **NTFS**. Appuyer sur la touche **ENTER** du clavier pour formater le disque dur.



Le formatage commence et peut durer quelques minutes





Appuyer sur SUIVANT



Entrer le numéro de série (sur la boîte)



Sélectionnez le type de licence que vous possédez



Entrez un nom de serveur et un mot de passe



Les consignes de sécurité pour votre mot de passe du compte administrateur





Configuration du réseau, nous verrons plus tard comment faire, faire **Suivant**

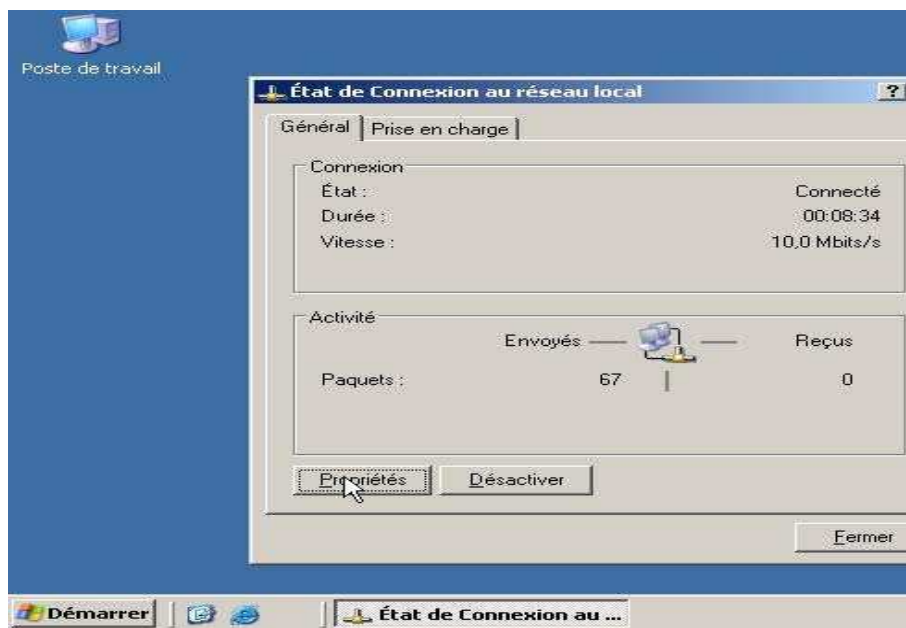


Nous laissons par défaut le serveur dans le WORKGROUP, faire **Suivant**.

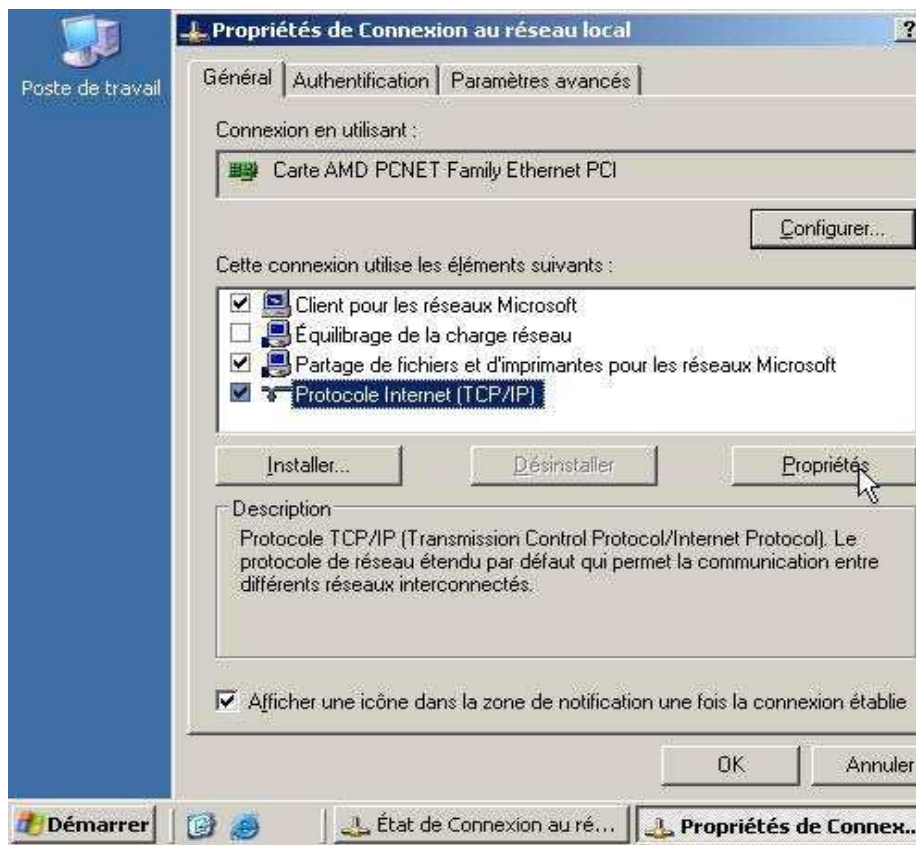


Le serveur redémarre et voilà, Windows 2003 Serveur est installé !

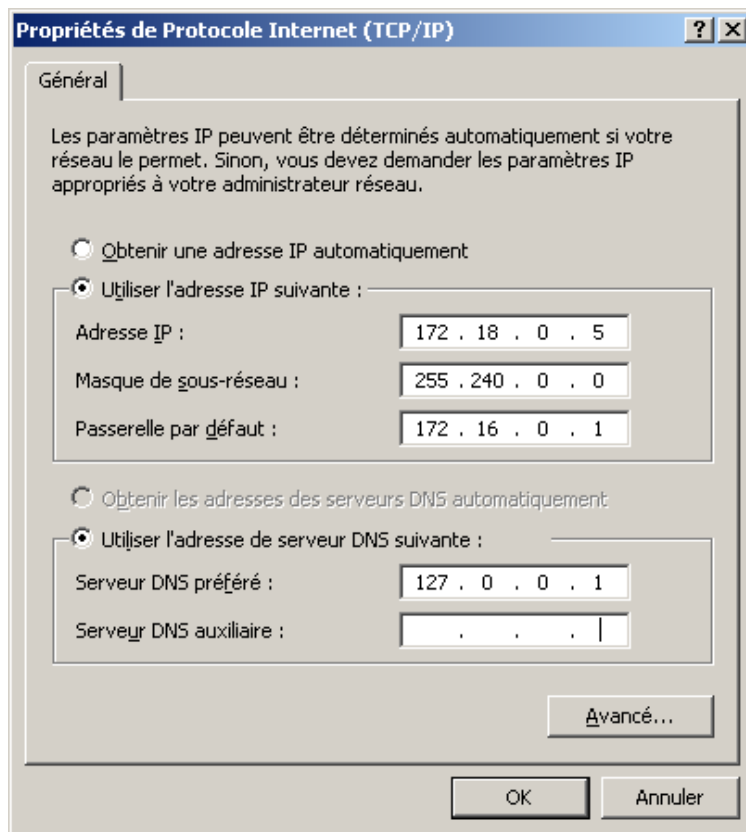
CONFIGURER ADRESSE IP



Allez dans les propriétés du protocole TCP/IP de la carte réseau.

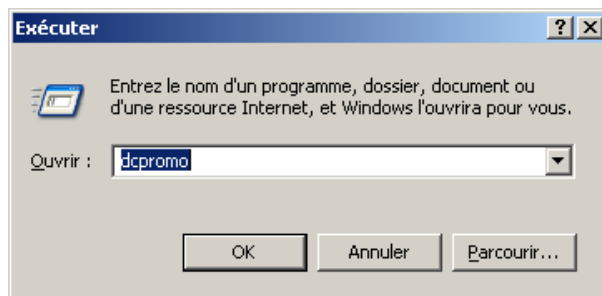


Fixez une adresse IP et mettez la même adresse IP pour le DNS ainsi qu'une adresse de passerelle pour un routeur internet.

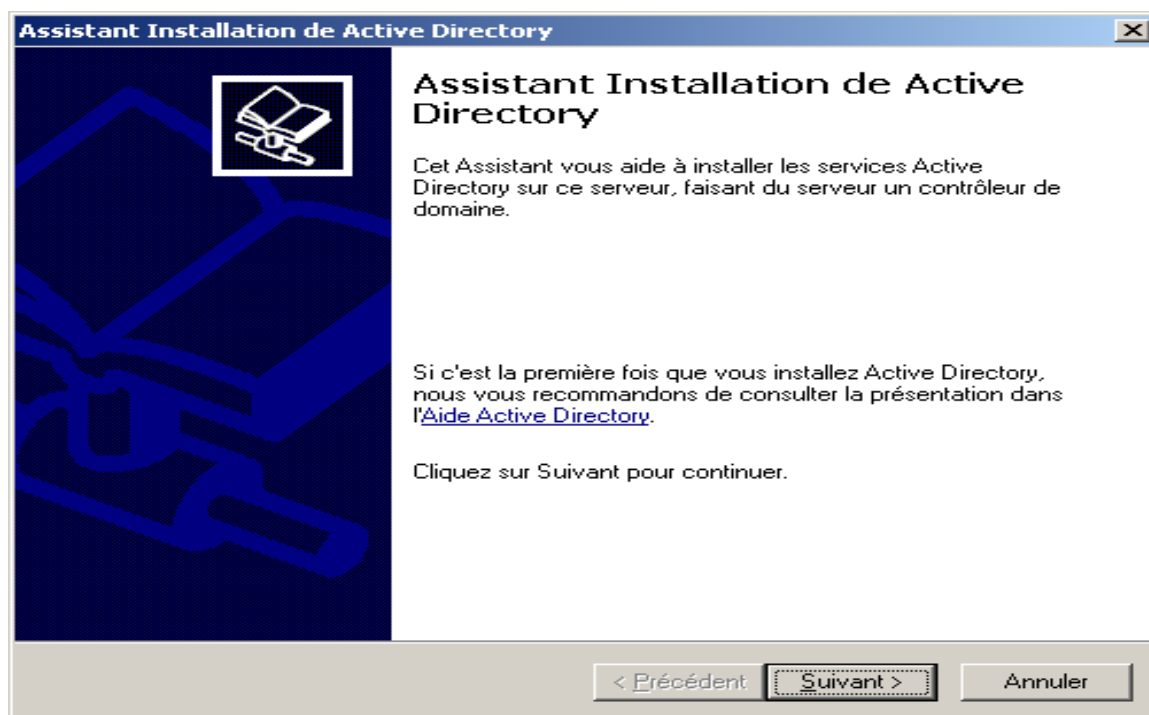


Voilà notre carte réseau est maintenant configurée.

INSTALLATION ACTIVE DIRECTORY

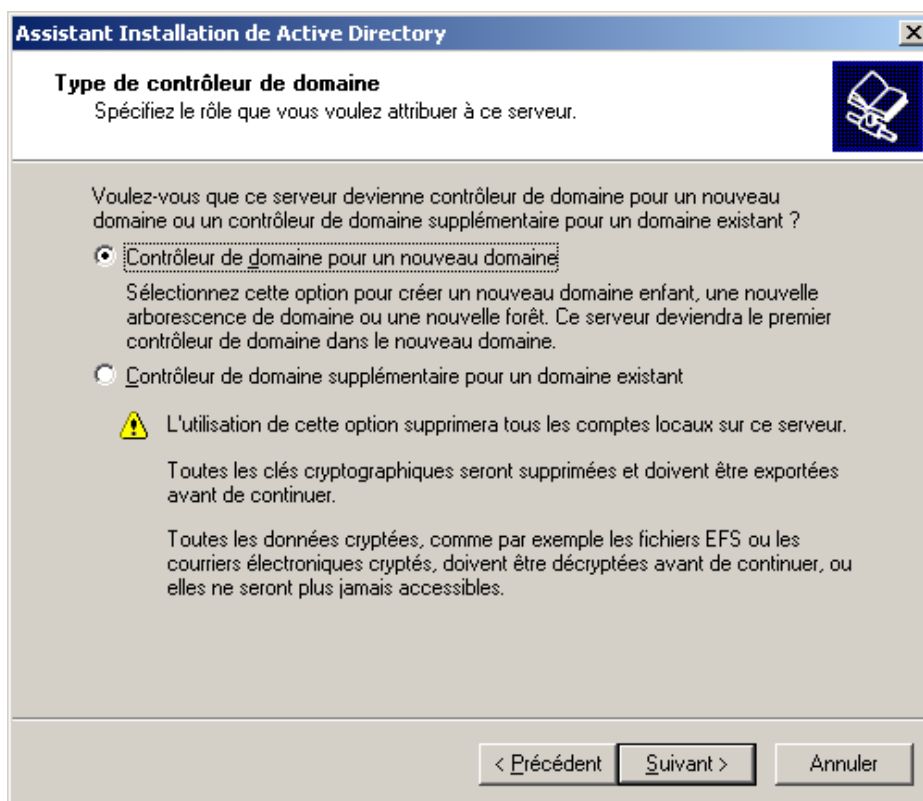


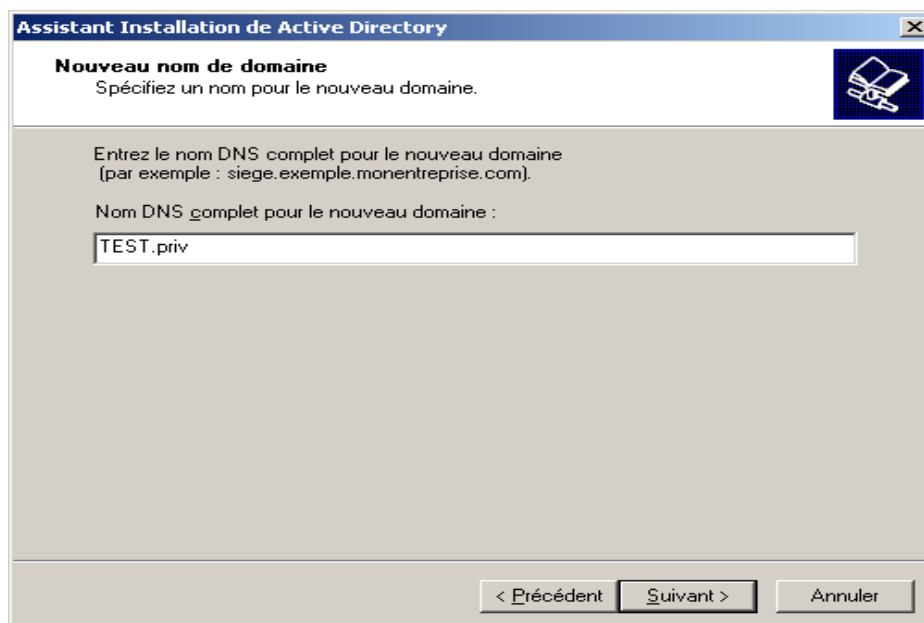
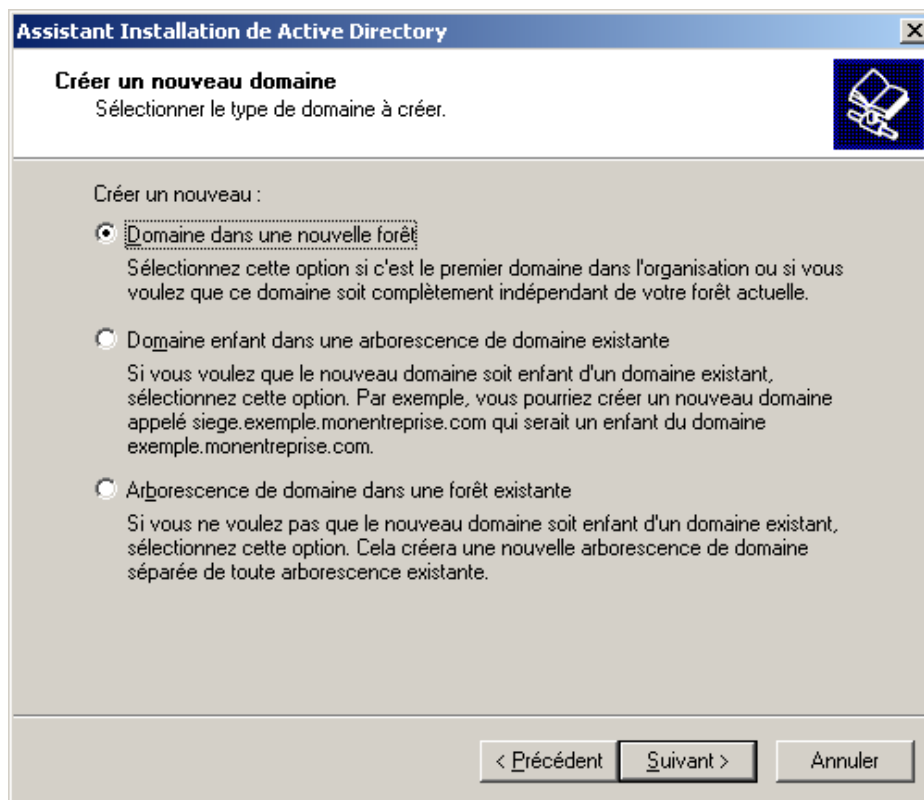
DEMARRER > EXECUTER > DCPROMO



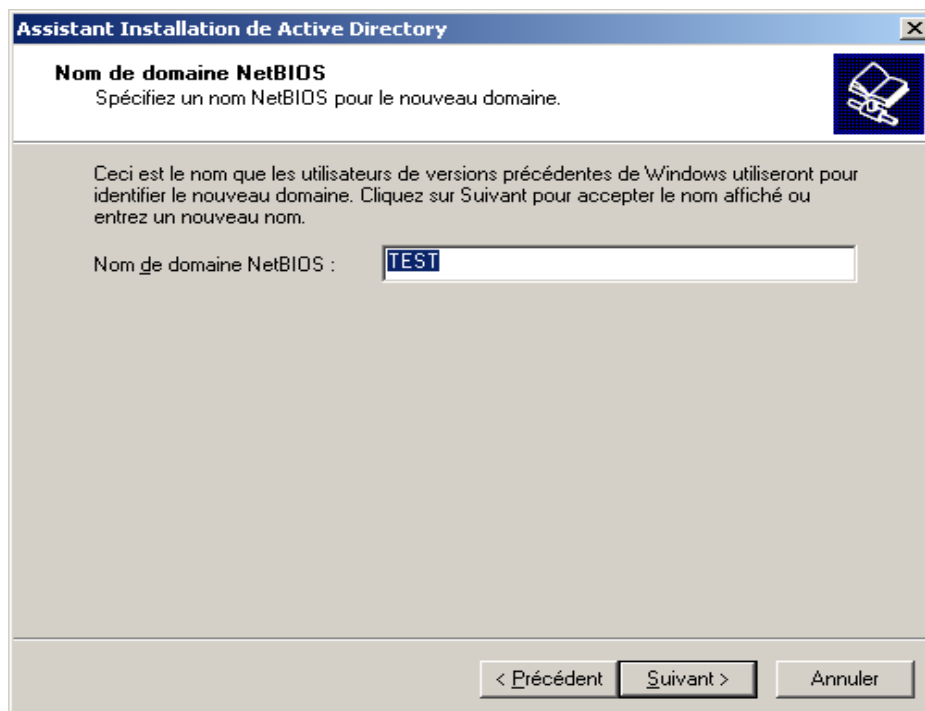
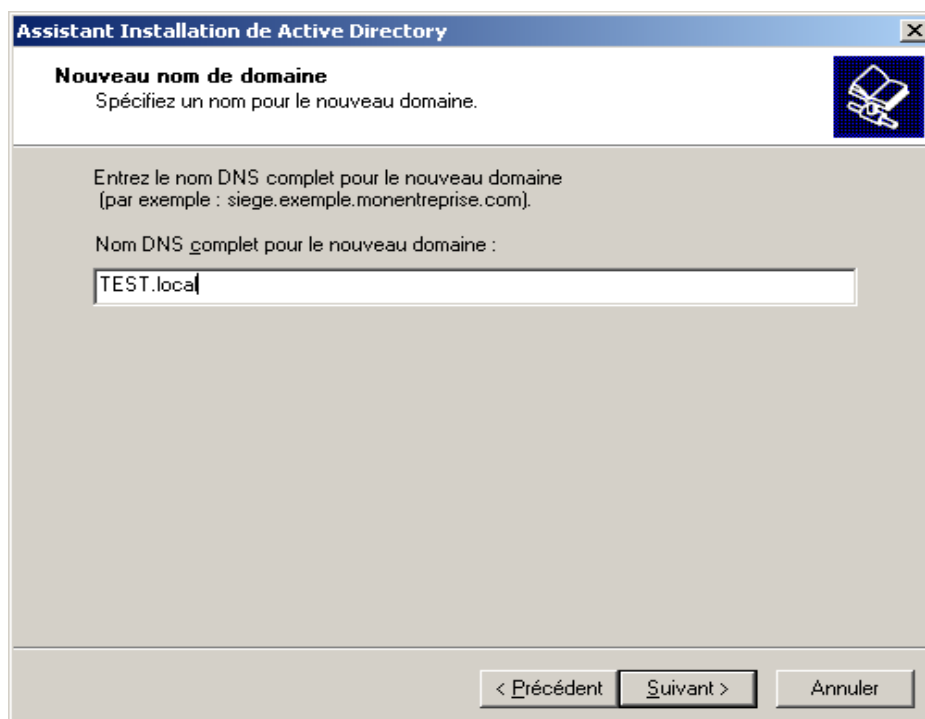
Vous serez informé que les stations 95 ne fonctionneront pas avec votre serveur. Les stations NT4 ayant un service pack inférieur au 4 devront être mises à jour pour être utilisées. Si vous possédez des stations 95 il sera tout de même possible de les utiliser mais pour cela il faudra réduire la sécurité du serveur 2003 (décrit plus loin).

Choisissez "Contrôleur de domaine pour un nouveau domaine".





Les domaines locaux ont l'extension PRIV ou LOCAL



Assistant Installation de Active Directory

Dossiers de la base de données et du journal
Spécifiez les dossiers qui vont contenir la base de données et le journal Active Directory.

Pour de meilleures performances et une meilleure récupération, stockez la base de données et le journal sur des disques durs distincts.

Où voulez-vous stocker la base de données Active Directory ?

Dossier de la base de données :

Parcourir...

Où voulez-vous stocker le journal Active Directory ?

Dossier du journal :

Parcourir...

< Précédent Suivant > Annuler

Assistant Installation de Active Directory

Volume système partagé
Spécifiez quel dossier doit être partagé en tant que volume système.

Le dossier Sysvol stocke la copie pour le serveur des fichiers publics du domaine. La liste du contenu du dossier Sysvol est répliquée vers tous les contrôleurs de domaine dans le domaine.

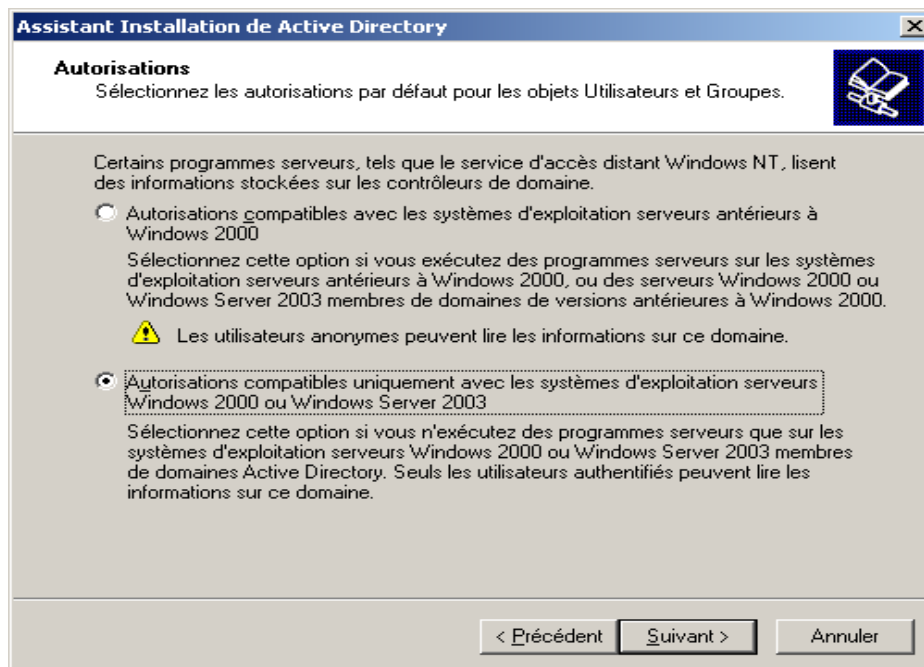
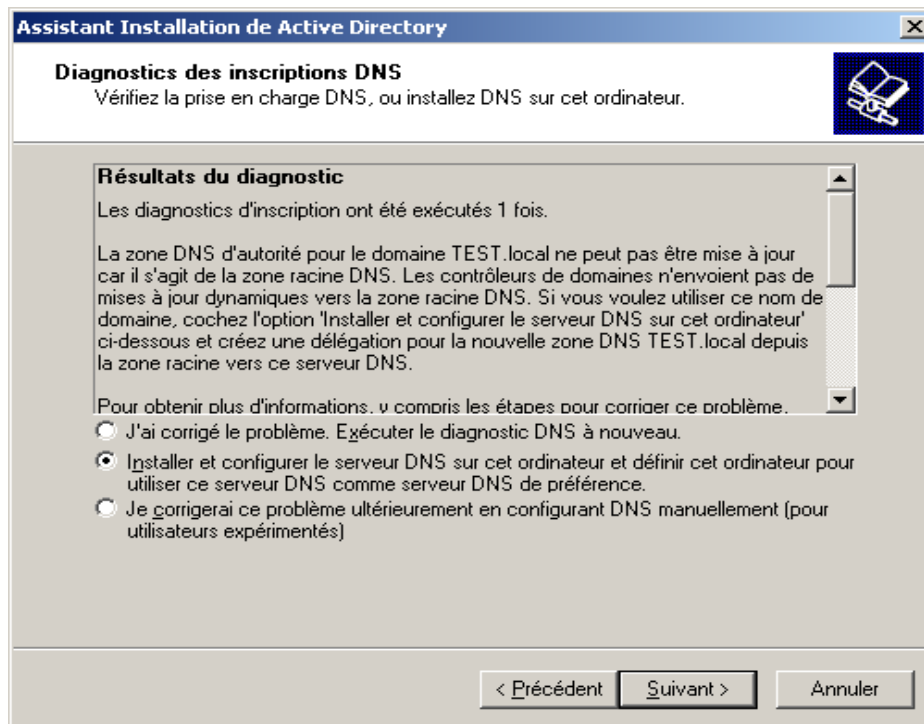
Le dossier Sysvol doit être situé sur un volume .

Entrez un emplacement pour le dossier Sysvol.

Emplacement du dossier :

Parcourir...

< Précédent Suivant > Annuler



Assistant Installation de Active Directory

Mot de passe administrateur de restauration des services d'annuaire
Ce mot de passe est utilisé lors du démarrage de l'ordinateur en mode Restauration des services d'annuaire.

Entrez et confirmez le mot de passe que vous voulez attribuer au compte Administrateur de ce serveur, qui sera utilisé lorsque l'ordinateur sera démarré en mode Restauration des services d'annuaire.

Le compte Administrateur du mode de restauration est différent du compte Administrateur du domaine. Les mots de passe pour les comptes peuvent être différents, assurez-vous de vous rappeler de chacun d'entre eux.

Mot de passe du mode Restauration :

Confirmer le mot de passe :

Pour obtenir plus d'informations sur le Mode de restauration des services d'annuaire, consultez l'[aide Active Directory](#).

< Précédent Suivant > Annuler

Assistant Installation de Active Directory

Résumé
Vérifiez et confirmez les options que vous avez sélectionnées.

Vous avez choisi de :

Configurer ce serveur en tant que premier contrôleur de domaine d'une nouvelle forêt d'arborescences de domaines.

Le nouveau nom de domaine est TEST.local. C'est aussi le nom de la nouvelle forêt.







Le nom NetBIOS du domaine est TEST.

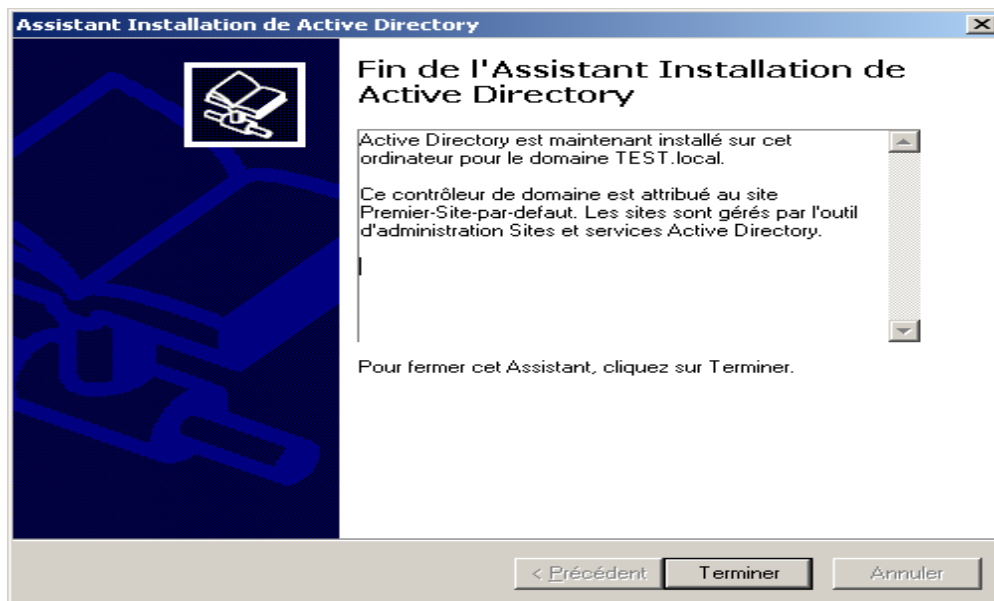
Dossier de la base de données : C:\WINDOWS\NTDS
Dossier du fichier journal : C:\WINDOWS\NTDS
Dossier Sysvol : C:\WINDOWS\SYVOL

Le service DNS sera installé et configuré sur cet ordinateur. Cet ordinateur sera

Pour modifier une option, cliquez sur Précédent. Pour commencer l'opération, cliquez sur Suivant.

< Précédent Suivant > Annuler

<p>Assistant Installation de Active Directory</p> <p>L'Assistant effectue la configuration de Active Directory. Ce processus peut durer quelques minutes ou quelques heures, en fonction des options que vous avez sélectionnées.</p>  <p>Configuration du service TrkWks</p> <p>Annuler</p>	<p>Assistant Installation de Active Directory</p> <p>L'Assistant effectue la configuration de Active Directory. Ce processus peut durer quelques minutes ou quelques heures, en fonction des options que vous avez sélectionnées.</p>  <p>Démarrage...</p>
<p>Assistant Installation de Active Directory</p> <p>L'Assistant effectue la configuration de Active Directory. Ce processus peut durer quelques minutes ou quelques heures, en fonction des options que vous avez sélectionnées.</p>  <p>Protection de c:\windows\system32\dlcache</p> <p>Annuler</p>	<p>Assistant Installation de Active Directory</p> <p>L'Assistant effectue la configuration de Active Directory. Ce processus peut durer quelques minutes ou quelques heures, en fonction des options que vous avez sélectionnées.</p>  <p>Configuration en cours d'un contrôleur de domaine local pour héberger Active Directory</p> <p>Annuler</p>
<p>Assistant Installation de Active Directory</p> <p>L'Assistant effectue la configuration de Active Directory. Ce processus peut durer quelques minutes ou quelques heures, en fonction des options que vous avez sélectionnées.</p>  <p>Configuration du service DNS en cours sur cet ordinateur...</p> <p>Ignorer l'installation du service DNS</p>	<p>Assistant Installation de Active Directory</p> <p>L'Assistant effectue la configuration de Active Directory. Ce processus peut durer quelques minutes ou quelques heures, en fonction des options que vous avez sélectionnées.</p>  <p>Création en cours de la partition d'annuaire : CN=Schema,CN=Configuration,DC=TEST,DC=local; 1585 objets restants</p> <p>Annuler</p>

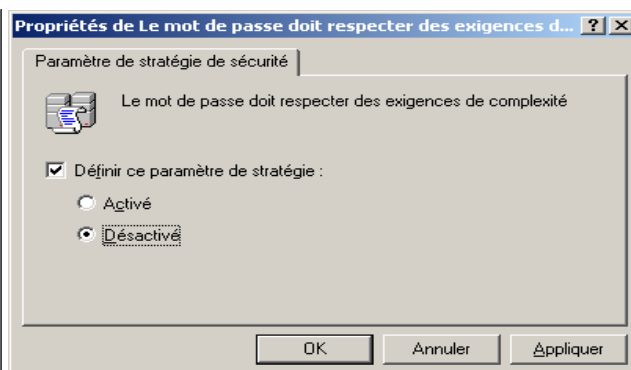
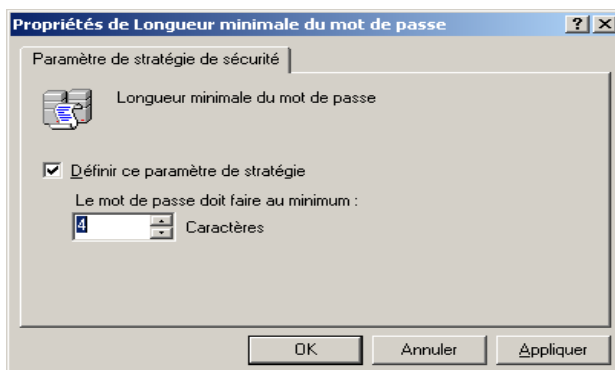
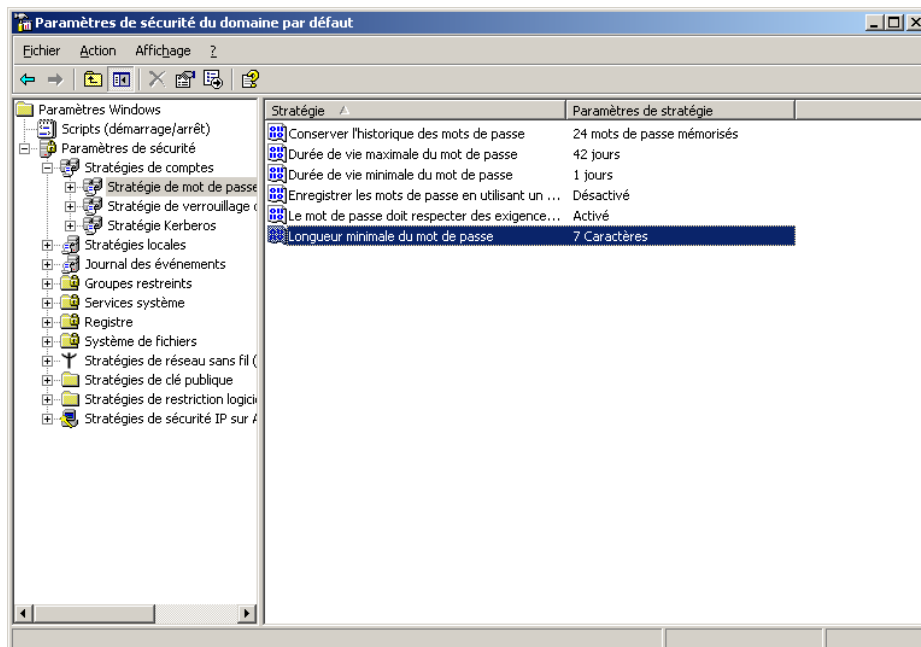


STRATEGIE DE SECURITE LOCALE (LONGEUR MOT DE PASSE, CLIENT 95)

Afin de pouvoir utiliser des postes sous NT4 et Windows 95 il faut modifier certaines sécurités natives de WINDOWS 2003

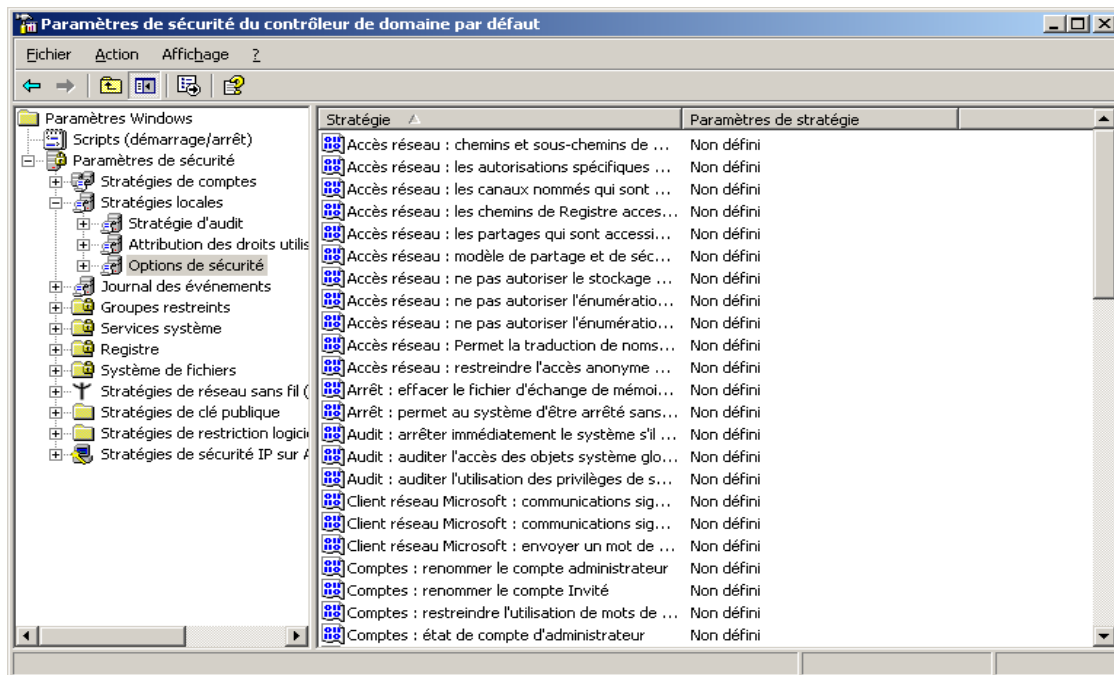
Menu Démarrer > Programmes > Outils d'administration > Paramètres de sécurité du domaine

(Paramètres de sécurité > Stratégie de mot de passe > Longueur minimale du mot de passe)

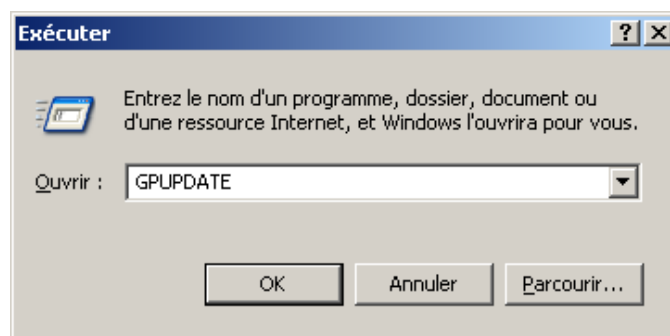


Menu Démarrer > Programmes > Outils d'administration > Paramètres de sécurité du contrôleur de domaine

(Paramètres de sécurité > Stratégies locales > Options de sécurité > Serveur réseau Microsoft : communication signé numériquement)



GPUPDATE permet de rafraîchir !!! (Stratégie sécurité, GPO)



PARAMETRAGE DU SERVEUR DNS

Définition de DNS

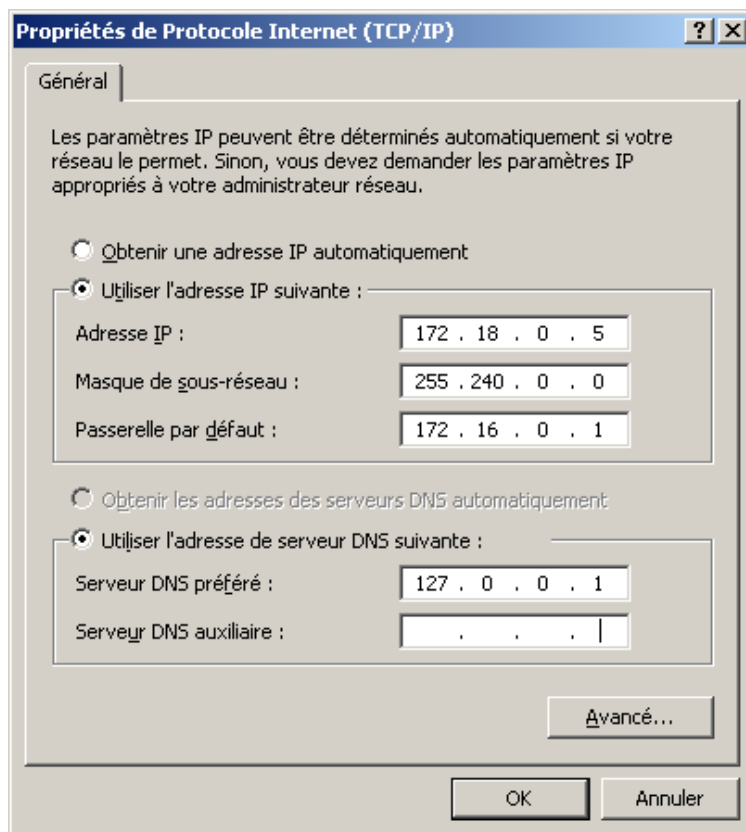
DNS (Domain Name System, système de noms de domaine) est un système de noms pour les ordinateurs et les services réseau organisé selon une hiérarchie de domaines. Le système DNS est utilisé dans les réseaux TCP/IP tels qu'Internet pour localiser des ordinateurs et des services à l'aide de noms conviviaux. Lorsqu'un utilisateur entre un nom DNS dans une application, les services DNS peuvent résoudre ce nom en une autre information qui lui est associée, par exemple une adresse IP.

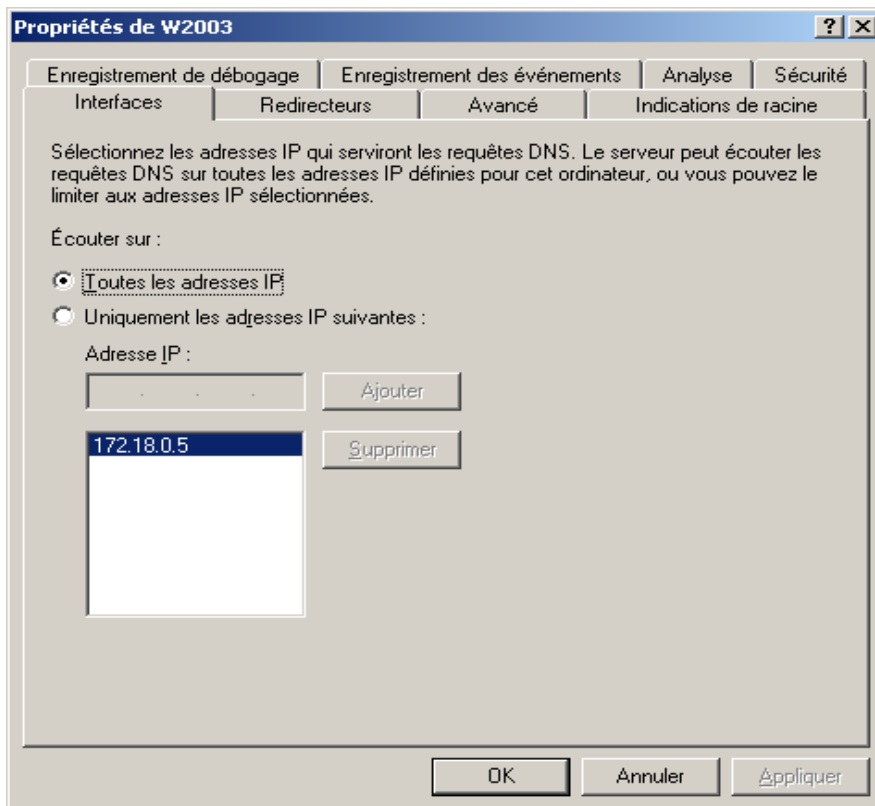
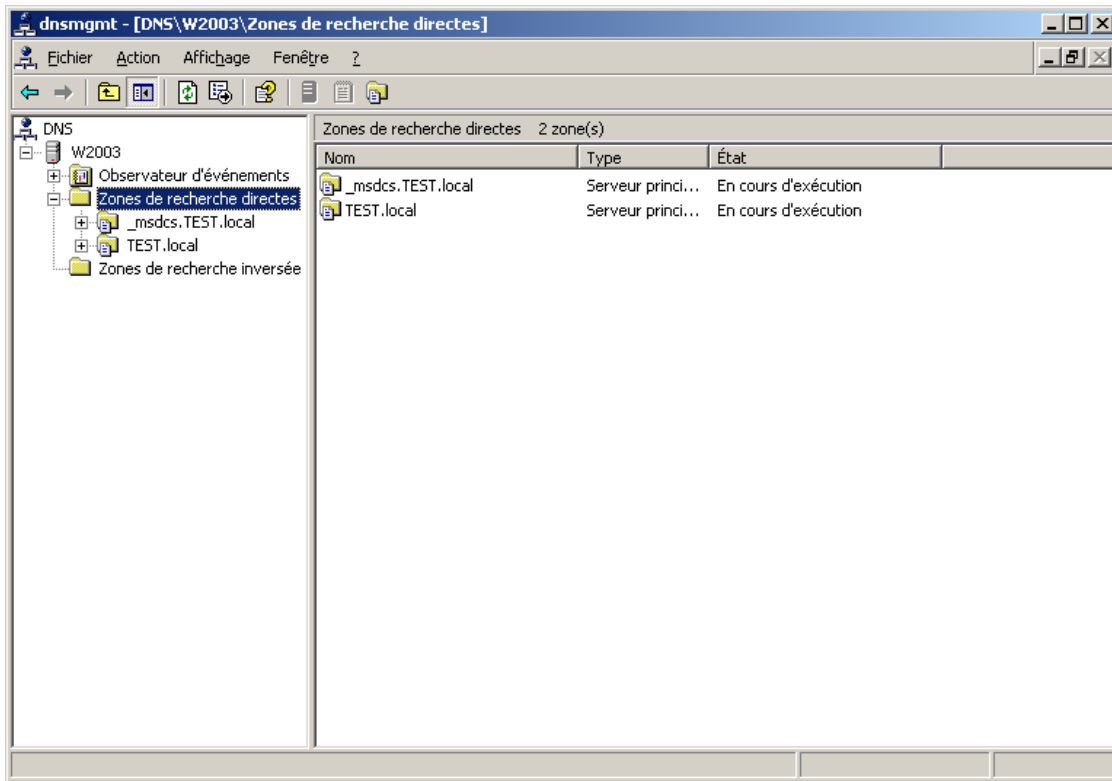
La plupart des utilisateurs préfèrent en effet un nom convivial comme exemple.microsoft.com pour accéder à un ordinateur tel qu'un serveur de messagerie ou un serveur Web dans un réseau. Un nom convivial est plus facile à retenir. Cependant, les ordinateurs utilisent des adresses numériques pour communiquer sur un réseau. Pour faciliter l'utilisation des ressources réseau, des services de noms comme DNS fournissent une méthode qui établit la correspondance entre le nom convivial d'un ordinateur ou d'un service et son adresse numérique. Si vous avez déjà utilisé un navigateur Web, vous avez utilisé DNS.

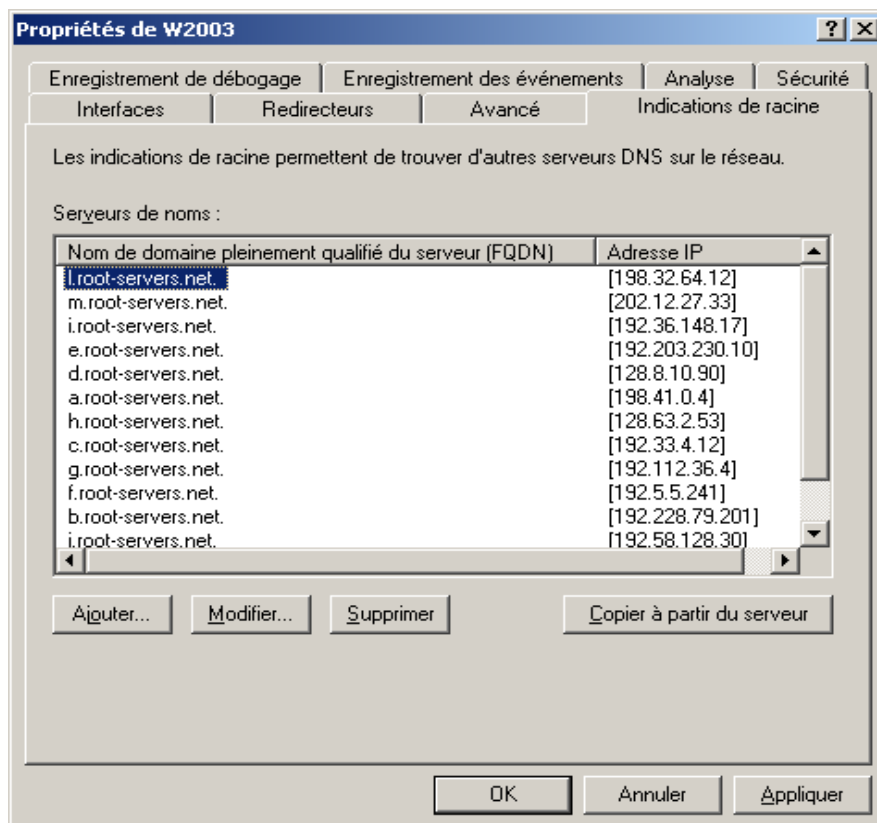
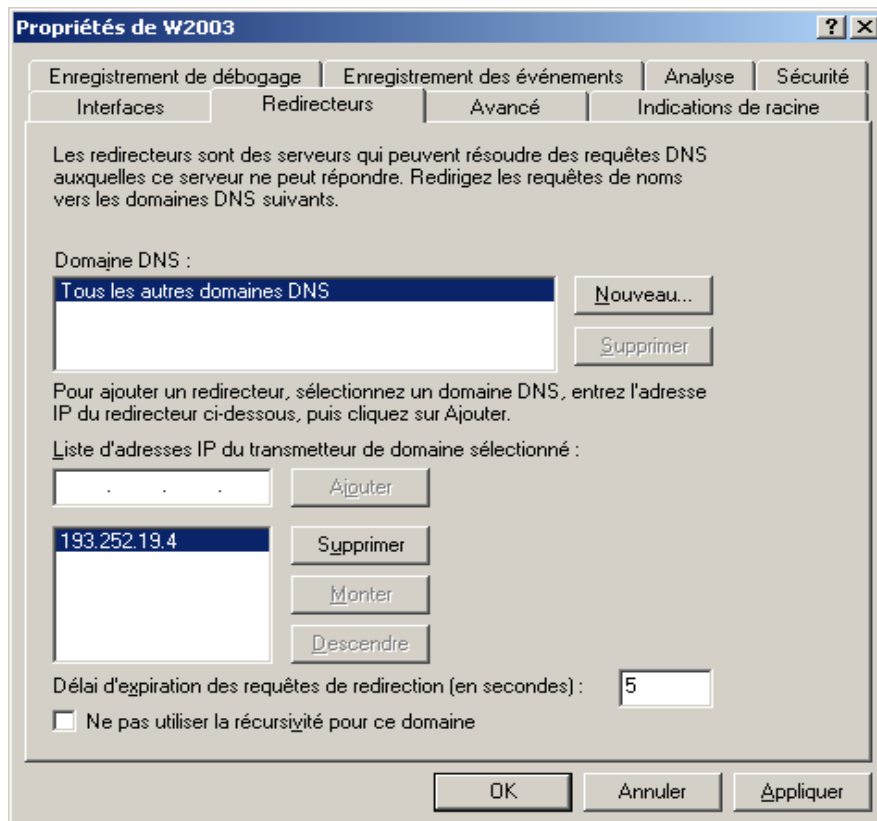
L'illustration suivante représente une utilisation élémentaire de DNS qui consiste à trouver l'adresse IP d'un ordinateur à partir de son nom.



Dans cet exemple, un ordinateur client interroge un serveur pour lui demander l'adresse IP d'un troisième ordinateur configuré pour utiliser le nom de domaine DNS hote-a.exemple.microsoft.com. Le serveur étant en mesure de répondre à cette requête en interrogeant sa base de données locale, il renvoie une réponse qui fournit l'information demandée, c'est-à-dire un enregistrement de ressource A (adresse d'hôte) contenant l'adresse IP correspondant à hote-a.exemple.microsoft.com.







Assistant Nouvelle zone

Type de zone
Le serveur DNS prend en charge différents types de zones et de stockages.

Sélectionnez le type de zone que vous voulez créer :

- Zone principale**
Crée une copie d'une zone qui peut être mise à jour directement sur ce serveur.
- Zone secondaire**
Crée une copie de la zone qui existe sur un autre serveur. Cette option aide à équilibrer la charge de travail des serveurs principaux et autorise la gestion de la tolérance de pannes.
- Zone de stub**
Crée une copie d'une zone contenant uniquement des enregistrements Nom de serveur (NS), Source de nom (SOA), et éventuellement des enregistrements "glue Host (A)". Un serveur contenant une zone de stub ne fait pas autorité pour cette zone.

Enregistrer la zone dans Active Directory (disponible uniquement si le serveur DNS est un contrôleur de domaine)

< Précédent Suivant > Annuler Aide

Assistant Nouvelle zone

Étendue de la zone de réplication de Active Directory
Vous pouvez sélectionner la façon dont les données DNS doivent être répliquées sur votre réseau.

Choisissez la façon dont les données de la zone doivent être répliquées :

- Vers tous les serveurs DNS de la forêt Active Directory TEST.local
- Vers tous les serveurs DNS du domaine Active Directory TEST.local
- Vers tous les contrôleurs de domaines du domaine Active Directory TEST.local**
Choisissez cette option si la zone doit être chargée par des serveurs DNS Windows 2000 s'exécutant sur les contrôleurs de domaine présents au sein du même domaine.
- Vers tous les contrôleurs de domaine spécifiés dans l'étendue de la partition de l'annuaire d'applications suivante :

< Précédent Suivant > Annuler Aide

Assistant Nouvelle zone

Nom de la zone de recherche inversée
Une zone de recherche inversée traduit les adresses IP en noms DNS.

Pour identifier la zone de recherche inversée, entrez l'ID réseau ou le nom de la zone.

ID réseau :

L'ID réseau est la partie des adresses IP qui appartient à cette zone. Entrez l'ID réseau dans son ordre normal (non inversé).

Si vous utilisez un zéro dans l'ID réseau, il va apparaître dans le nom de la zone. Par exemple, l'ID réseau 10 crée la zone 10.in-addr.arpa, l'ID réseau 10.0 crée la zone 0.10.in-addr.arpa.

Nom de la zone de recherche inversée :

Cliquez sur Aide pour obtenir davantage d'informations concernant la création d'une zone de recherche inversée.

< Précédent Suivant > Annuler Aide




Assistant Nouvelle zone

Mise à niveau dynamique
Vous pouvez spécifier que cette zone DNS accepte les mises à jour sécurisées, non sécurisées ou non dynamiques.

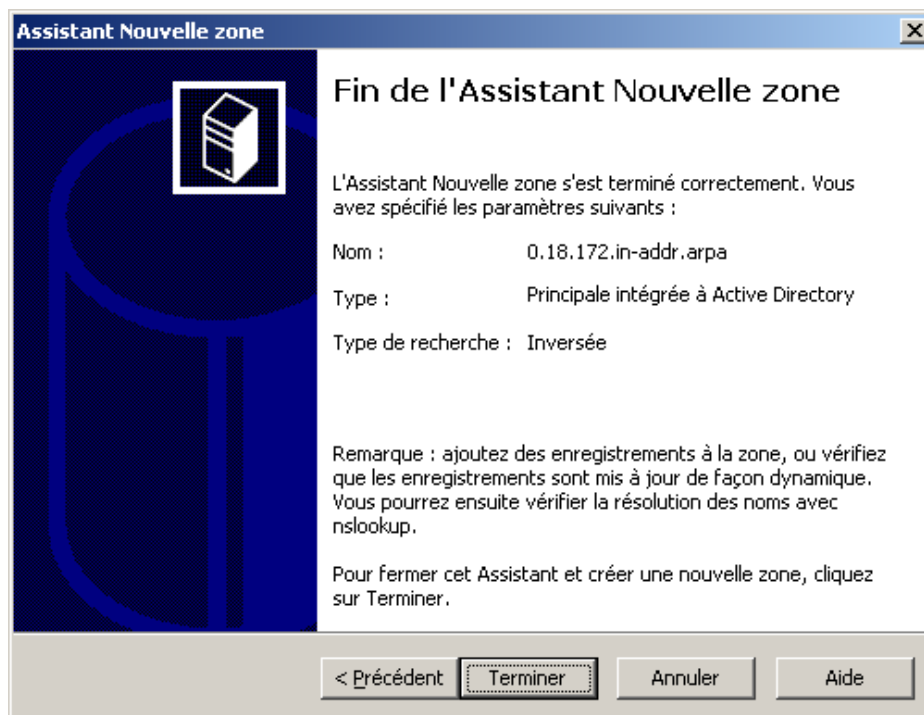
Les mises à jour dynamiques permettent au client DNS d'enregistrer et de mettre à jour de manière dynamique leurs enregistrements de ressources avec un serveur DNS dès qu'une modification a lieu.
Sélectionnez le type de mises à jour dynamiques que vous souhaitez autoriser :

N'autoriser que les mises à jour dynamiques sécurisées (recommandé pour Active Directory)
Cette option n'est disponible que pour les zones intégrées à Active Directory.

Autoriser à la fois les mises à jour dynamiques sécurisées et non sécurisées
Les mises à jour dynamiques d'enregistrement de ressources sont acceptées à partir de n'importe quel client.
 Cette option peut mettre en danger la sécurité de vos données car les mises à jour risquent d'être acceptées à partir d'une source non approuvée.

Ne pas autoriser les mises à jour dynamiques
Les mises à jour dynamiques des enregistrements de ressources ne sont pas acceptées par cette zone. Vous devez mettre à jour ces enregistrements manuellement.

< Précédent Suivant > Annuler Aide



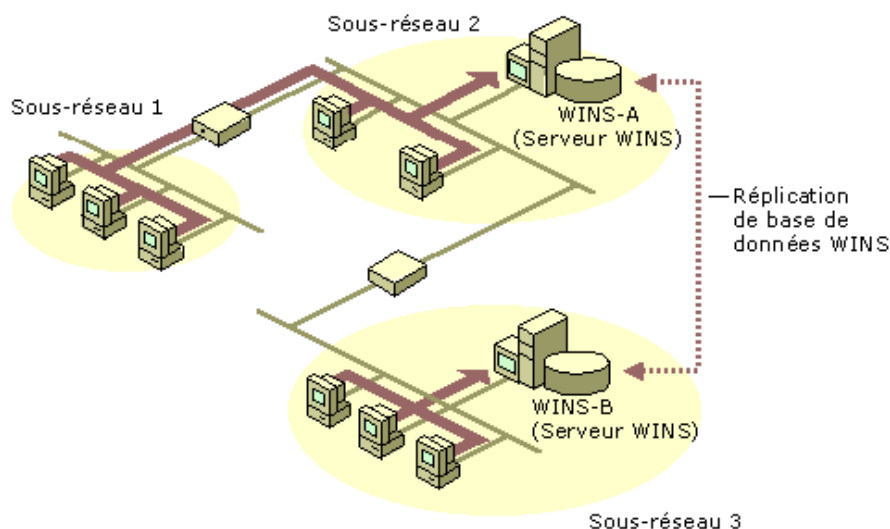
INSTALLATION ET PARAMETRAGE DU SERVEUR WINS

Les [serveurs WINS \(Windows Internet Name Service\)](#) mappent dynamiquement les adresses IP aux noms d'ordinateurs (noms NetBIOS). De cette manière, les utilisateurs peuvent accéder aux ressources au moyen du nom d'ordinateur et non de son adresse IP. Si vous souhaitez que l'ordinateur en question assure le suivi des noms et des adresses IP des autres ordinateurs du réseau, configurez-le comme un serveur WINS.

WINS est constitué de deux composants principaux : le serveur WINS et les [clients WINS](#)

Le serveur WINS gère les requêtes d'inscription de noms à partir des clients WINS, enregistre leur nom et adresse IP et répond aux requêtes de noms NetBIOS soumises par les clients, en retournant l'adresse IP d'un nom de requête s'il est listé dans la base de données du serveur.

De plus, comme l'indique le graphisme suivant, les serveurs WINS peuvent répliquer le contenu de leur base de données (contenant des mappages de nom d'ordinateur NetBIOS vers des adresses IP) vers les autres serveurs WINS. Lorsqu'un ordinateur client WINS (tel qu'un ordinateur de station de travail sur le sous-réseau 1 ou 2) est démarré sur le réseau, son nom et son adresse IP sont envoyés dans une requête d'inscription directement vers son principal serveur WINS configuré, WINS A. WINS A étant le serveur qui enregistre ces clients, il est considéré comme étant le propriétaire des enregistrements de clients dans WINS.



Dans cet exemple, le serveur WINS A possède des clients enregistrés avec lui qui sont à la fois locaux (c'est-à-dire des clients sur le sous-réseau 2 où il se trouve) et distants (clients situés dans un routeur du sous-réseau 1). Un deuxième serveur WINS, WINS B, est situé sur le sous-réseau 3 et ne contient que des mappages pour les clients locaux faisant un enregistrement du même sous-réseau. WINS A et WINS B peuvent ensuite effectuer une réplication de leur base de données afin que les enregistrements des clients des 3 sous-réseaux se trouvent dans la base de données WINS sur les deux serveurs. Pour plus d'informations, consultez [Réplication WINS](#)

Serveurs WINS principaux/secondaires

Les serveurs WINS sont utilisés par les clients de l'une des deux manières suivantes : soit sous forme de serveur WINS principal, soit sous forme de serveur WINS secondaire.

La différence entre le serveur WINS principal et secondaire ne réside en aucun cas dans les serveurs (qui sont, d'un point de vue fonctionnel, identiques dans WINS). La différence réside dans le client qui diffère et ordonne la liste des serveurs WINS lorsque plusieurs serveurs WINS sont utilisés.

Dans la plupart des cas, le client contacte le serveur WINS principal pour toutes ses fonctions de service de noms NetBIOS (inscription de noms, changement de noms, libération de noms ainsi que requête et résolution de noms). Le seul cas dans lequel les serveurs WINS secondaires sont toujours utilisés est celui où le serveur WINS principal est :

soit non disponible sur le réseau lors de la requête de service ;

soit incapable de résoudre un nom pour le client (dans le cas d'une requête de nom).

Dans le cas d'une défaillance du serveur WINS principal, le client demande la même fonction de service à ses serveurs WINS secondaires. Si plus de deux serveurs WINS sont configurés pour le client, les serveurs WINS supplémentaires sont testés jusqu'à ce que la liste soit exhaustive ou qu'un des serveurs WINS secondaires parvienne à traiter et à répondre avec succès à la requête. Une fois qu'un serveur WINS secondaire est utilisé, un client tente régulièrement de rebasculer sur son serveur WINS principal pour de futures requêtes de service.

Pour les clients WINS les plus récents (Windows 2000 et Windows 98), une liste de 12 serveurs WINS secondaires maximum peut être configurée (manuellement via des propriétés TCP/IP ou dynamiquement par un serveur DHCP fournissant une liste utilisant une option DHCP de type 44). Cette fonctionnalité est utile dans un environnement contenant un grand nombre de clients mobiles et de ressources NetBIOS et si les services sont souvent utilisés. Étant donné que dans ce type d'environnements, la base de données WINS n'est peut-être pas cohérente à travers le réseau des serveurs WINS, à cause de problèmes de convergence, il peut être utile pour les clients de pouvoir interroger plusieurs serveurs WINS.

Cependant, cette option ne doit pas être utilisée de manière excessive car elle représente un compromis en termes d'avantages réels pour l'ajout de tolérances aux défauts en listant les serveurs WINS supplémentaires. L'avantage de cette fonctionnalité doit être pondéré par le fait que pour chaque serveur WINS supplémentaire listé, le temps nécessaire pour traiter entièrement une requête dans WINS augmente de manière incrémentielle. Par exemple, si un client WINS teste au moins trois serveurs WINS avant de connaître une défaillance, il peut retarder de manière substantielle le traitement de la requête de nom avant que d'autres méthodes de résolution soient testées, telles que la recherche d'un fichier local Hosts ou la requête d'un serveur DNS.

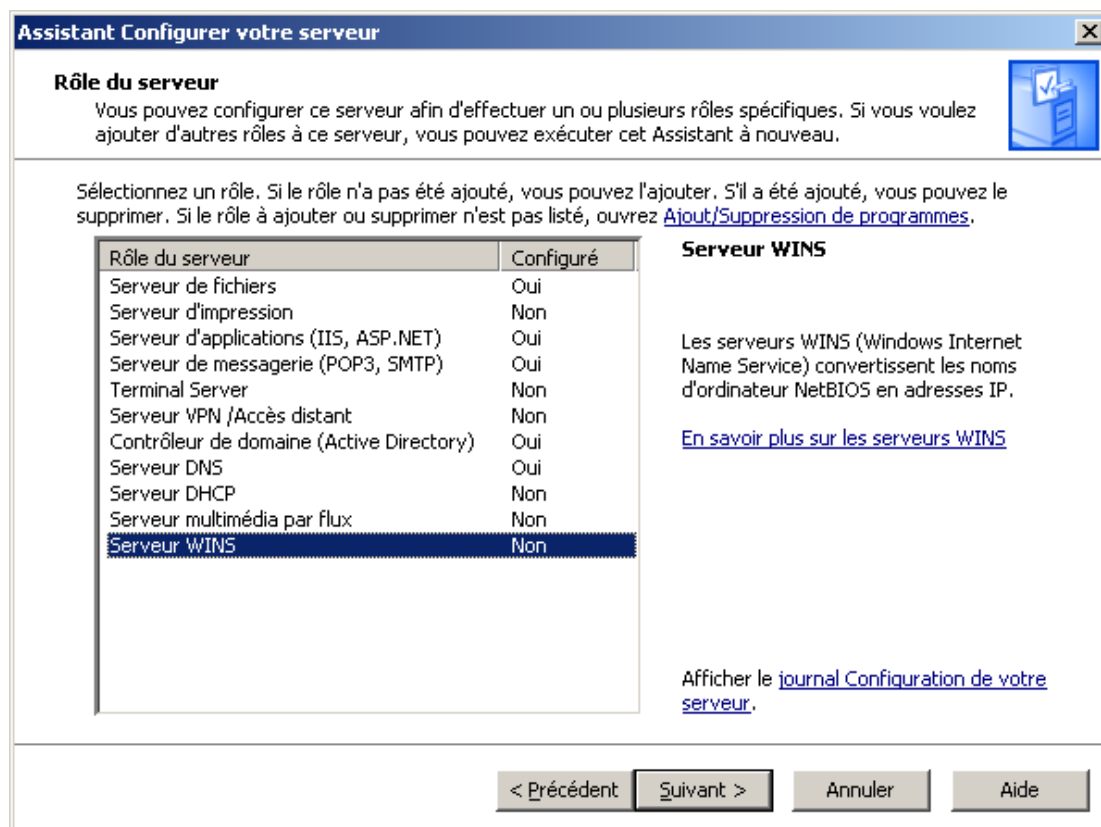
Le principal outil que vous utilisez pour gérer les serveurs WINS est la console WINS, qui est ajoutée aux Outils

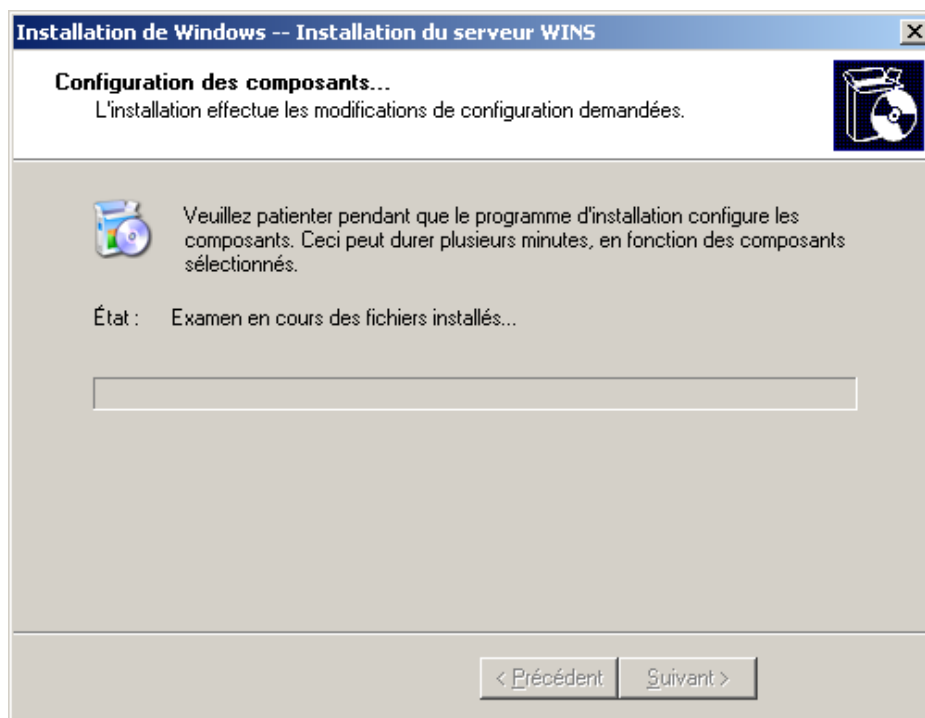
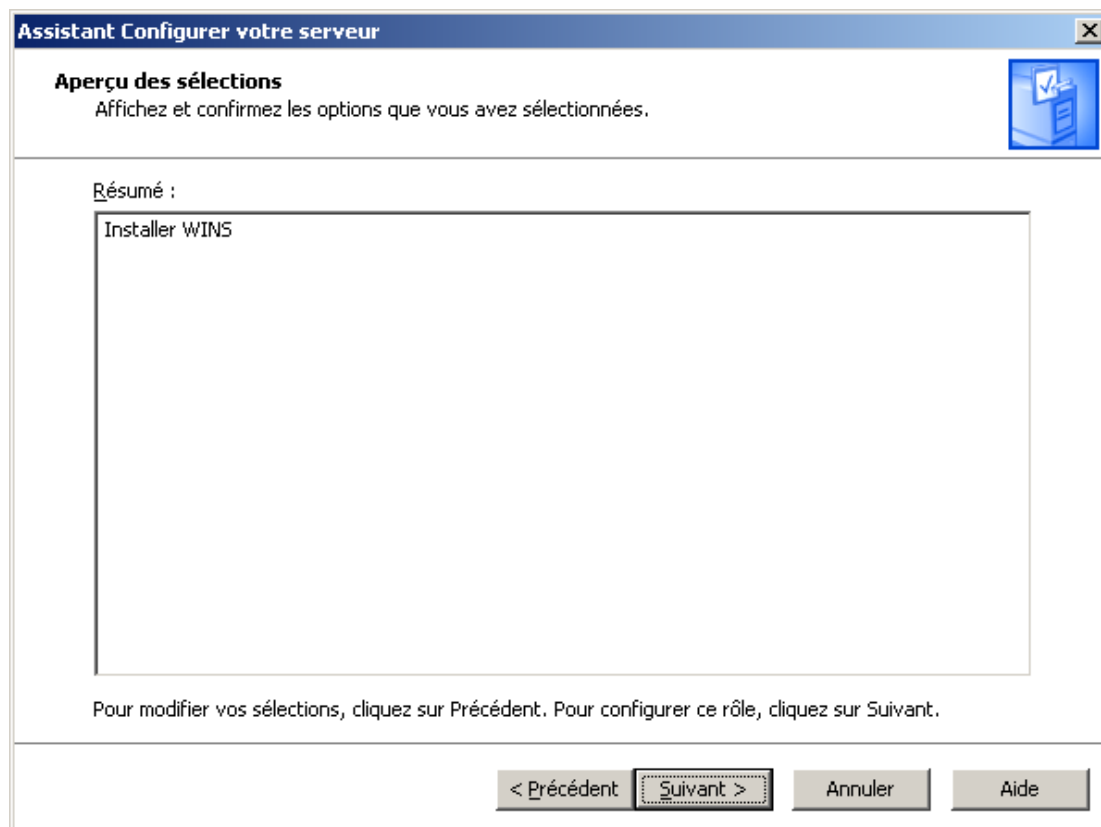
d'administration lorsque vous installez WINS. Dans Windows 2000 Server, la console WINS fonctionne à l'intérieur de la console MMC (Microsoft Management Console), afin d'intégrer complètement l'administration WINS dans la gestion totale de votre réseau.

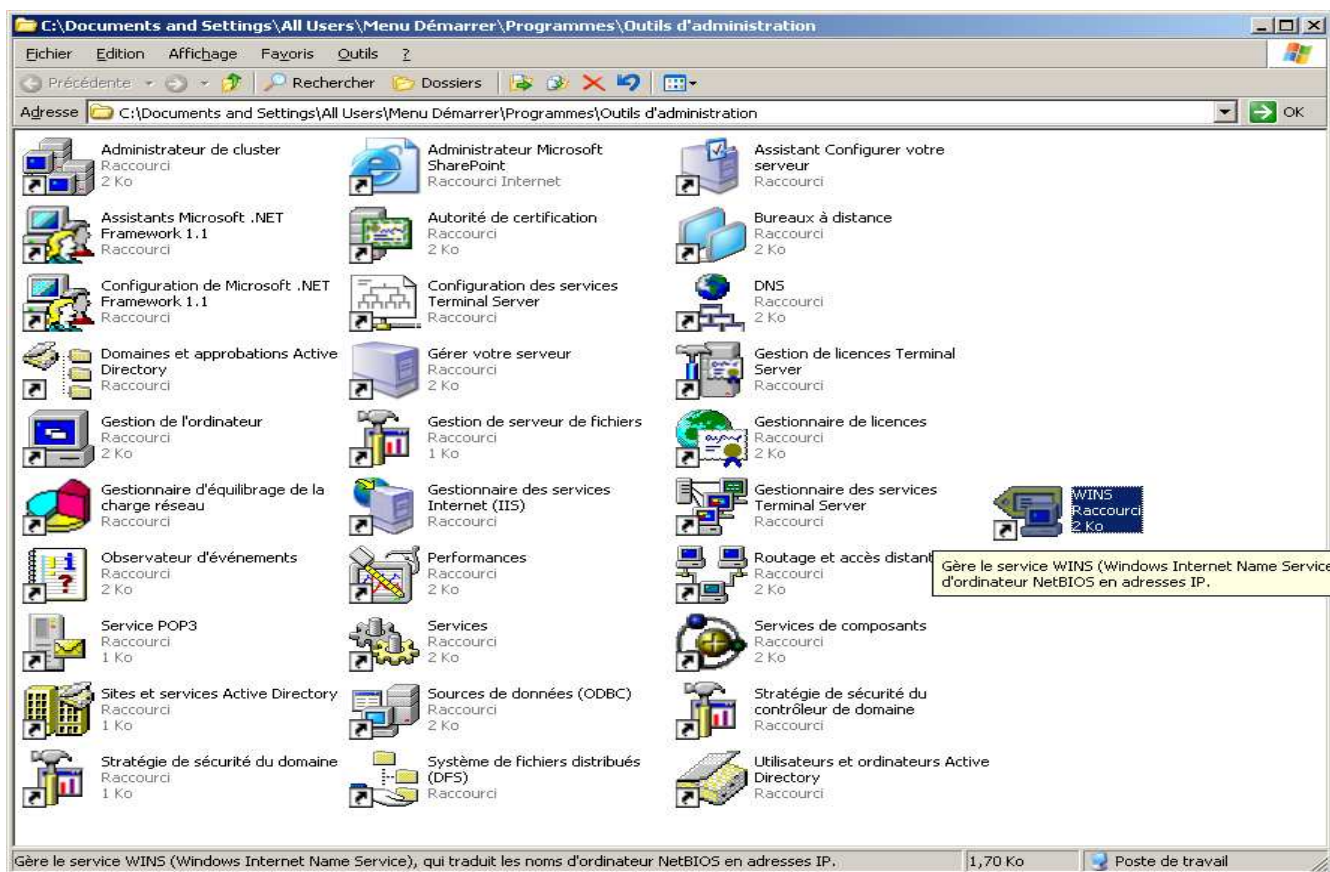
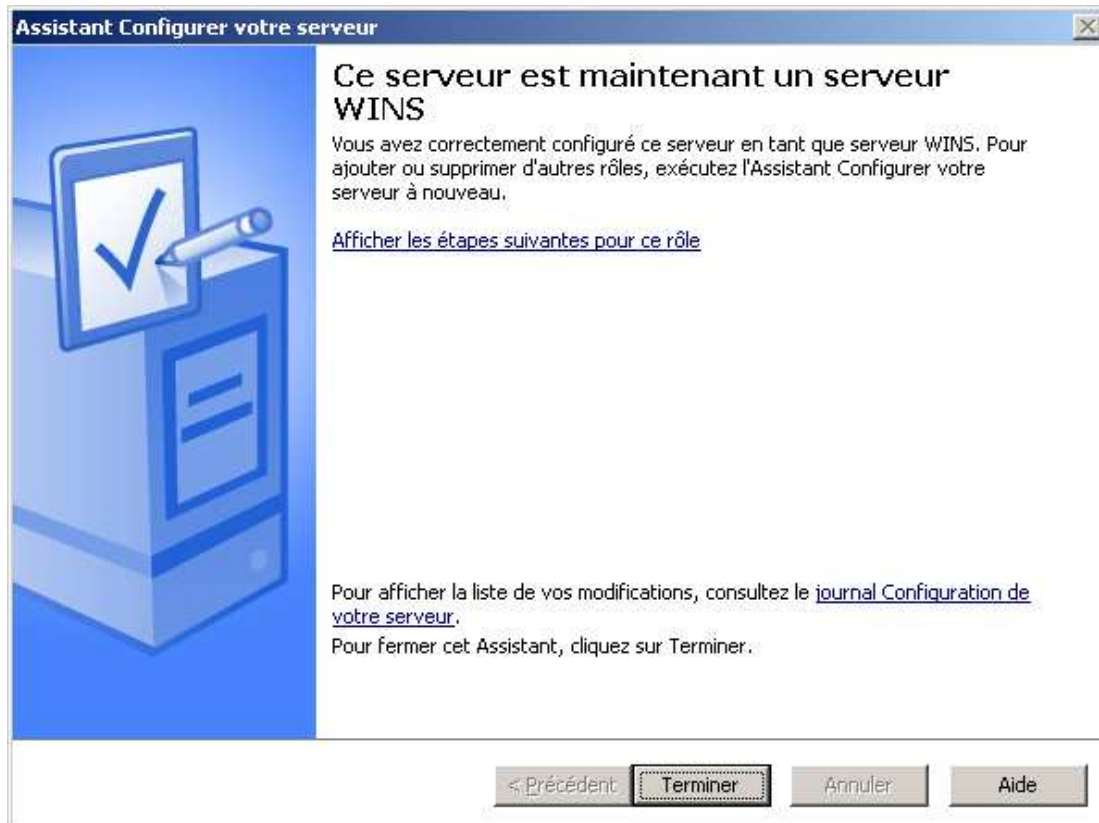
Après avoir installé un serveur WINS, vous pouvez utiliser la console WINS pour accomplir les tâches de base d'administration du serveur suivantes :

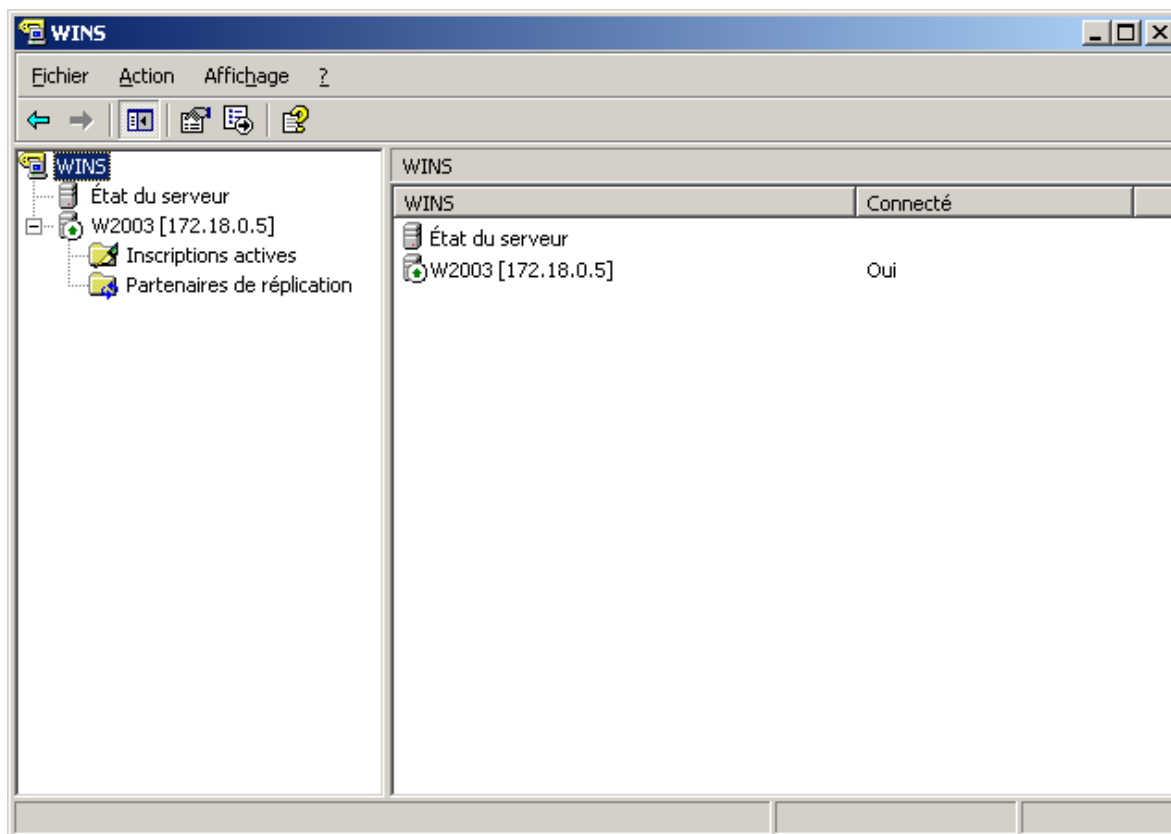
Afficher et filtrer les inscriptions de nom NetBIOS stockées sur le serveur WINS pour les noms de client utilisés sur votre réseau.

- Ajouter des partenaires de réplication à un serveur WINS et les configurer.
- Exécuter des tâches relatives à la maintenance, y compris la sauvegarde, la restauration, le compactage et le nettoyage de la base de données du serveur WINS.
- De plus, vous pouvez utiliser la console WINS pour effectuer les tâches de configuration facultatives ou avancées suivantes :
- Afficher et modifier les propriétés WINS, telles que l'Intervalle de renouvellement, ainsi que d'autres intervalles utilisés lors de l'inscription, du renouvellement et de la vérification des enregistrements de noms stockés dans la base de données du serveur.
- Ajouter et configurer des mappages WINS statiques, si leur utilisation est indispensable sur votre réseau.
- Supprimer ou désactiver des enregistrements WINS qui s'affichent dans les données du serveur WINS utilisées sur votre réseau.





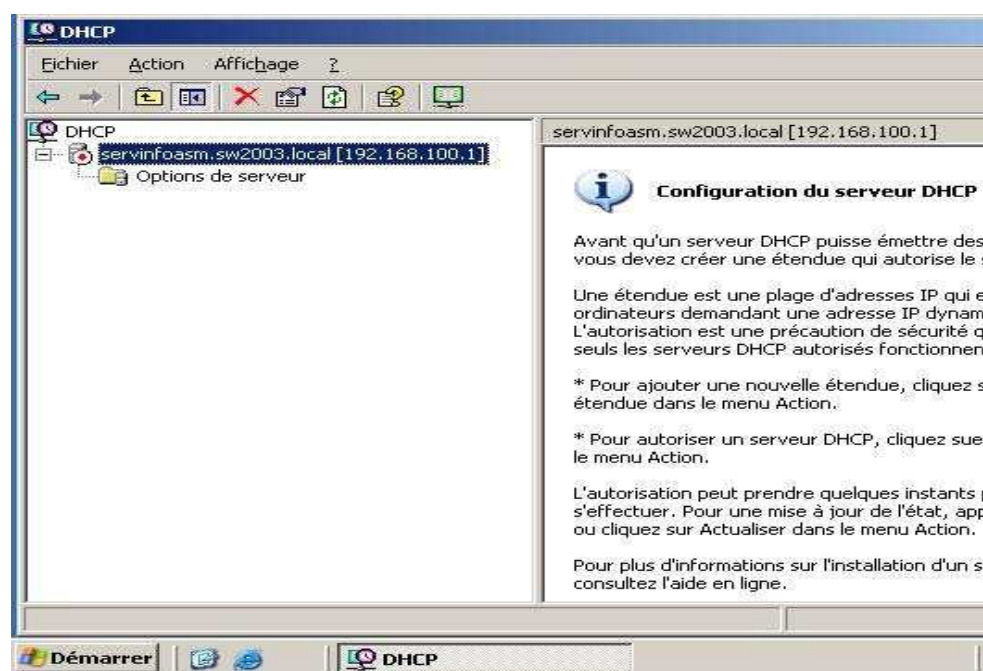




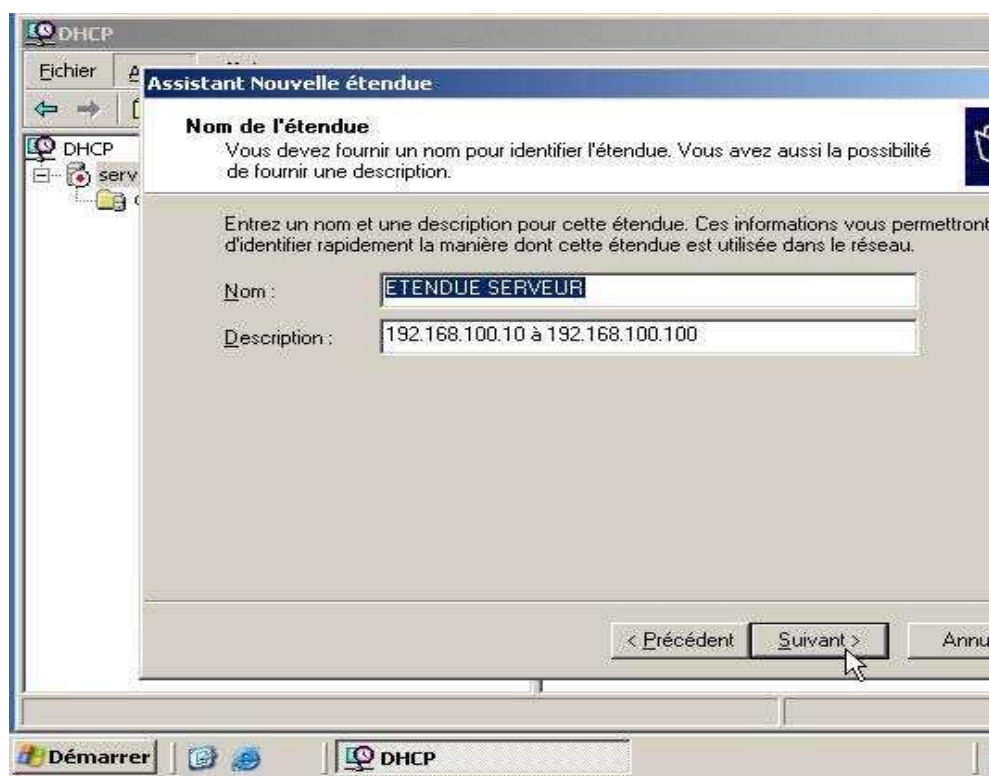
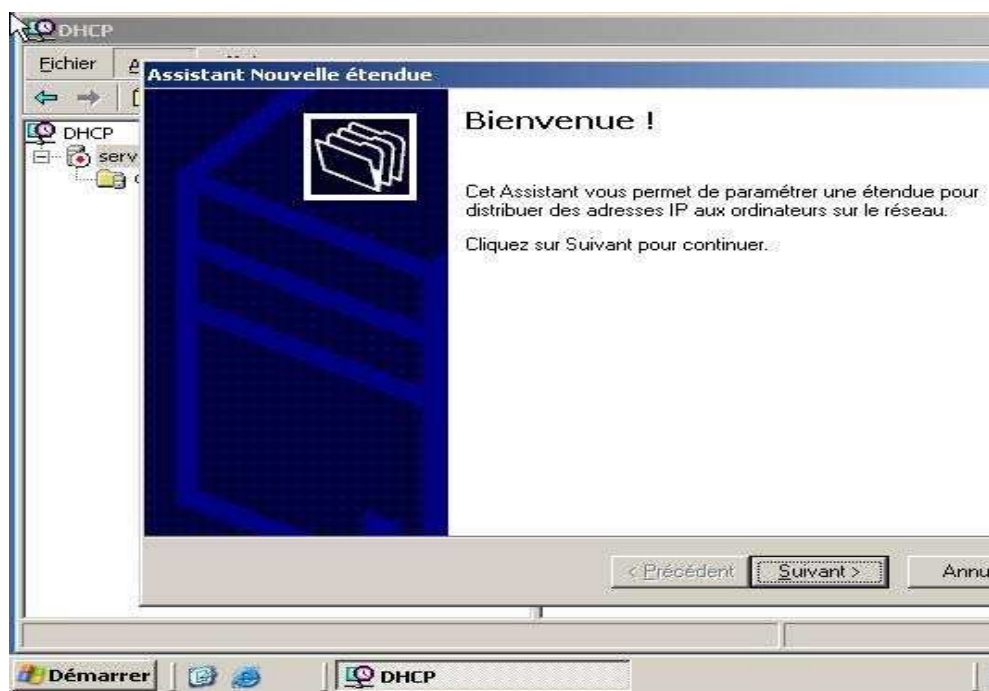
Le service WINS est actif quand la petite flèche sur le conteneur est verte

INSTALLATION ET PARAMETRAGE DU SERVEUR DHCP

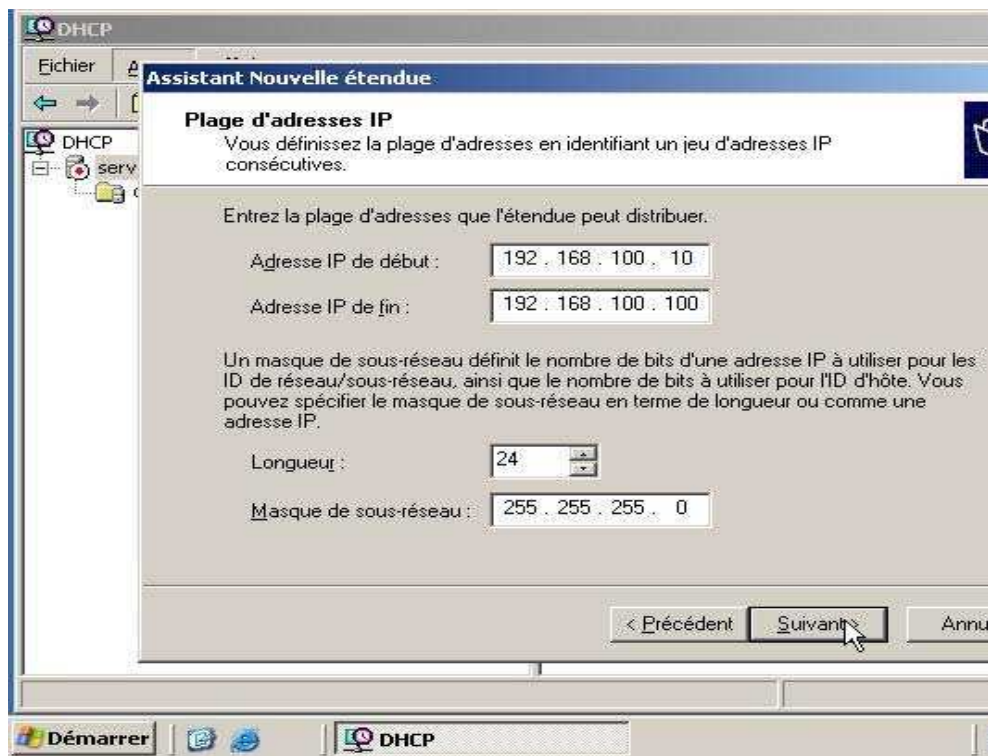
Serveur DHCP Ouvrir la console MMC DHCP par les outils d'administration.



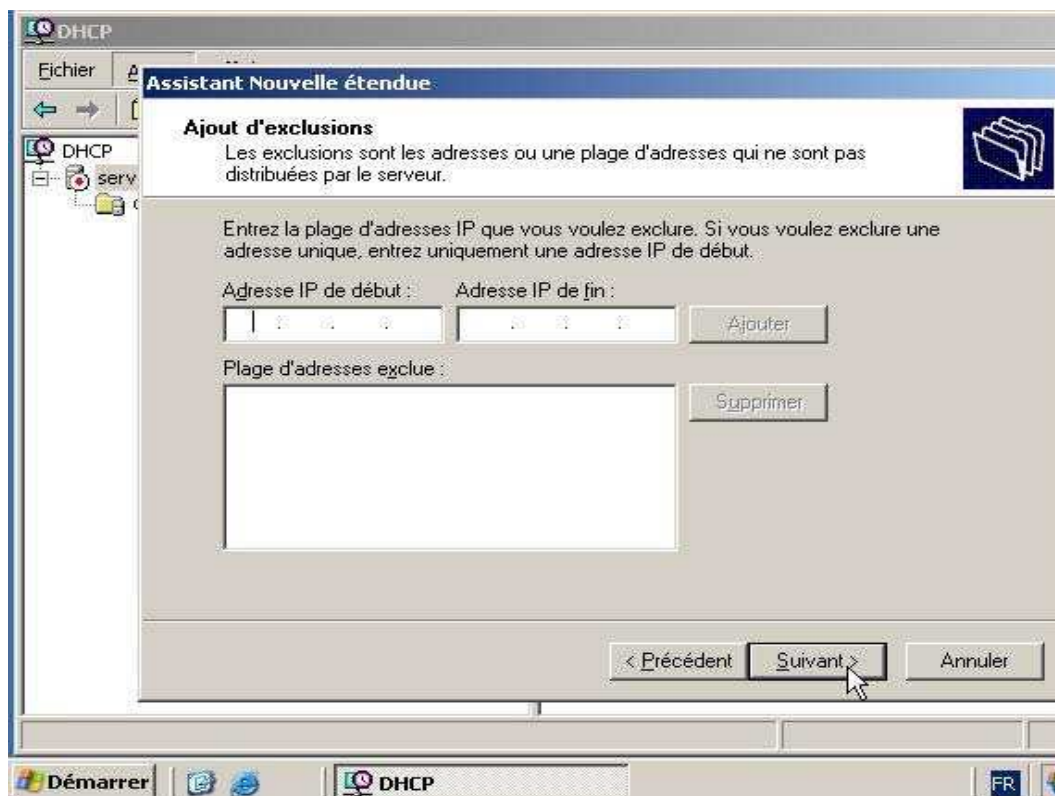
Création de l'étendue du serveur DHCP, allez dans le menu Action, choisissez Nouvelle étendue...et faite Suivant. Donnez un nom à votre étendue et faite Suivant.



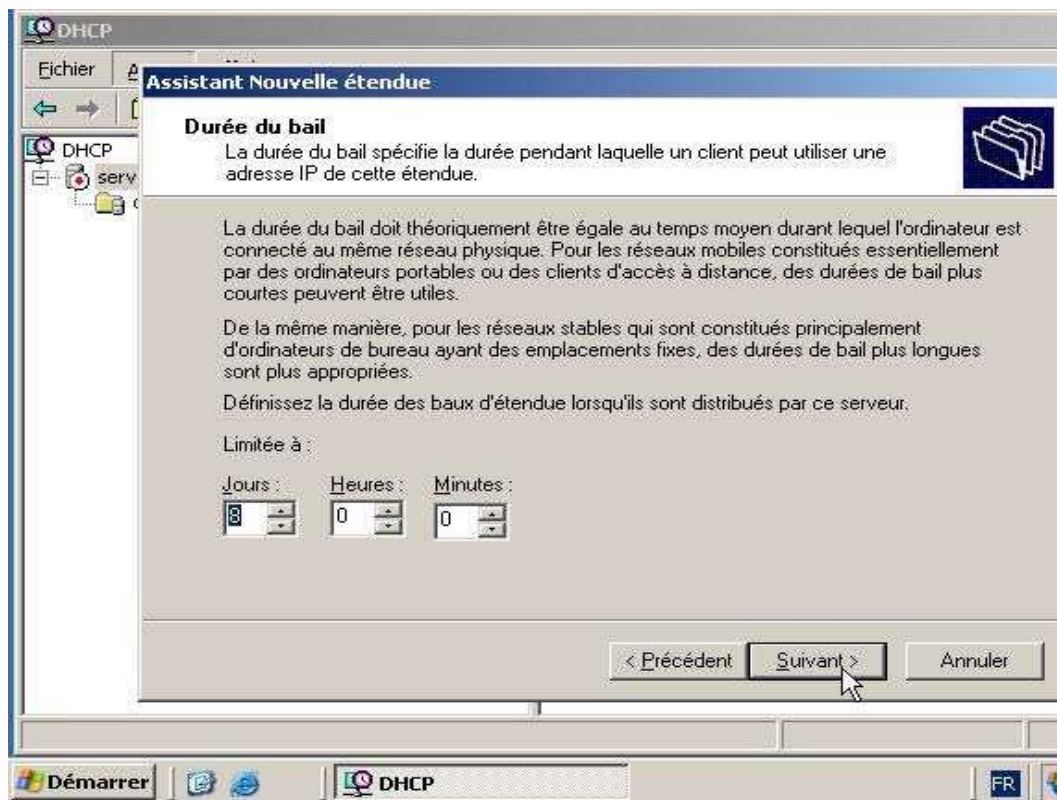
Mettez les adresses de début et de fin réservées à votre étendue et faite Suivant.



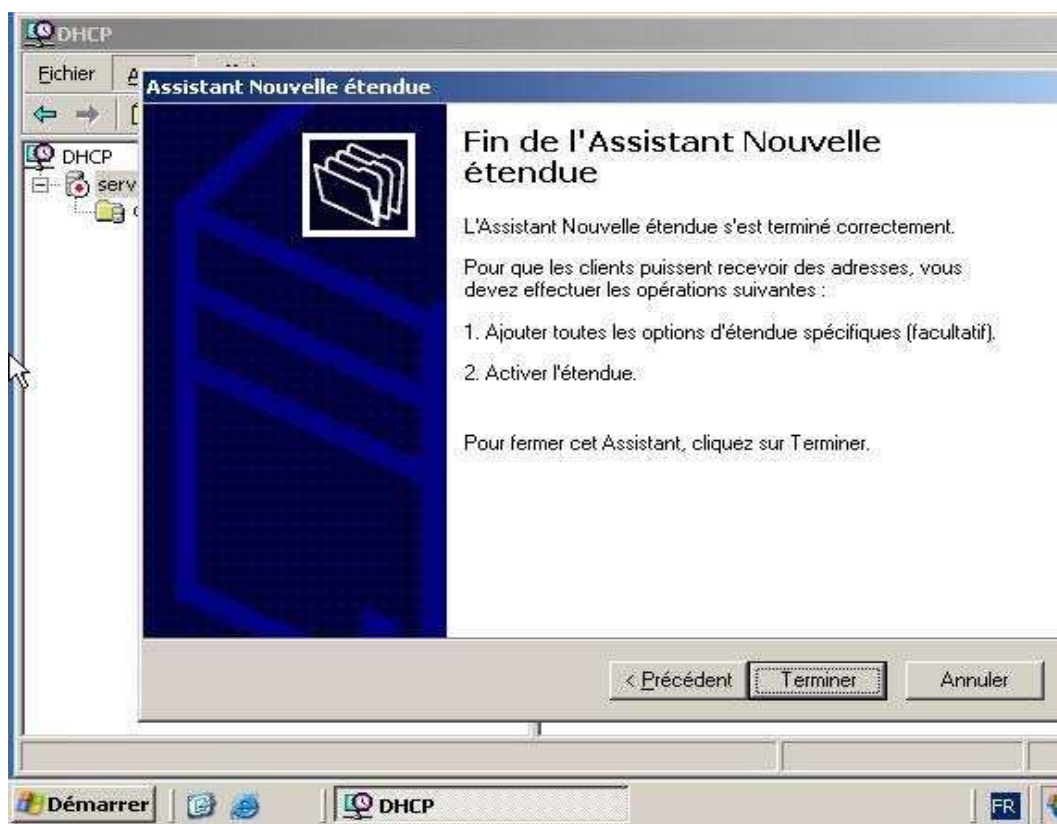
Mettez les adresses à exclure, dans mon cas j'en ai aucune et faite Suivant.



Mettez la durée du bail de renouvellement des adresses IP via le serveur DNS et faite Suivant.

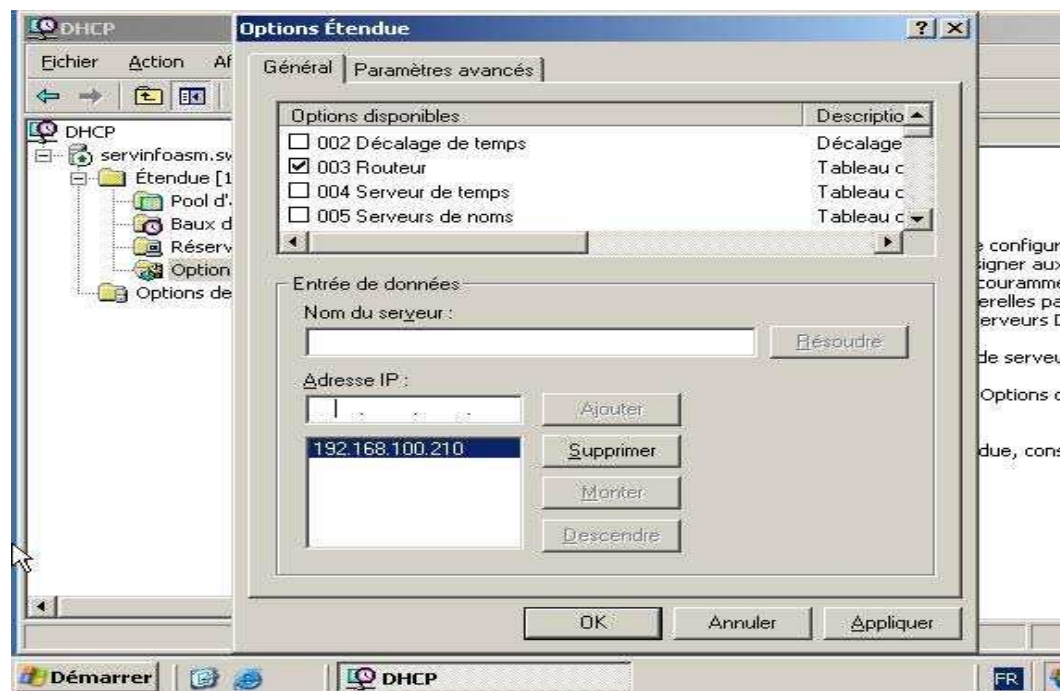


Voilà nous avons fini de configurer l'étendue et faite Terminer.

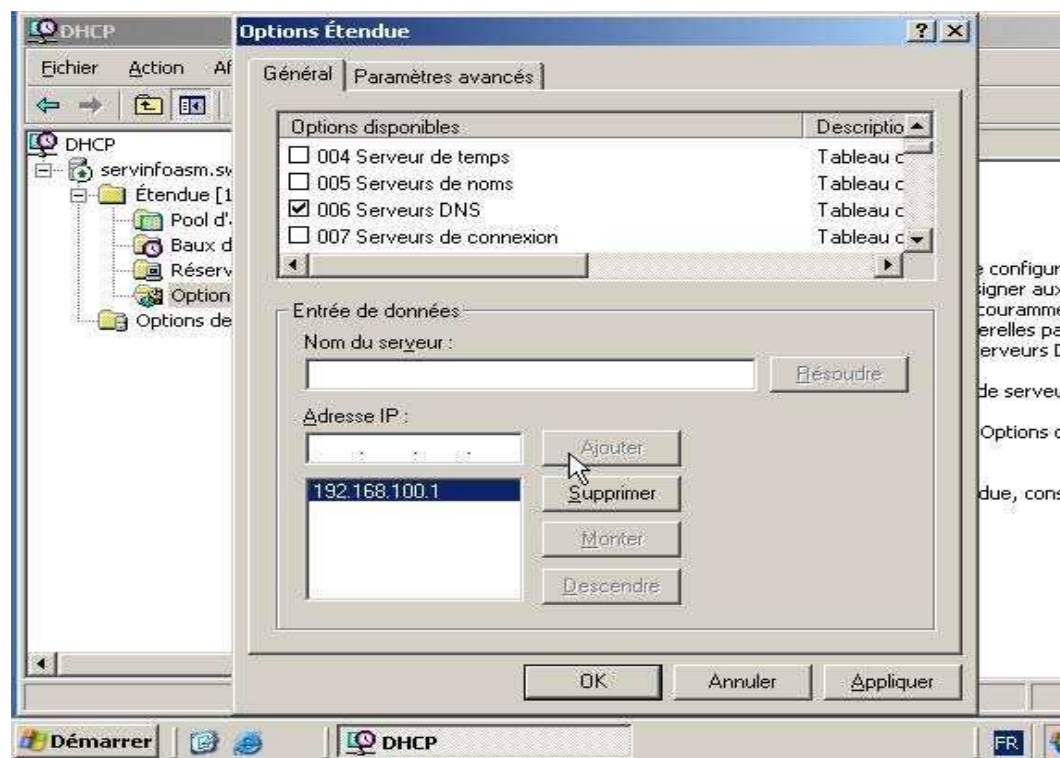


Configuration des options de l'étendue, on sélectionne Options d'étendue et par le menu Action on choisit Configurer les options ..., dans mon cas j'aurais une connexion Internet via un modem ou un routeur.

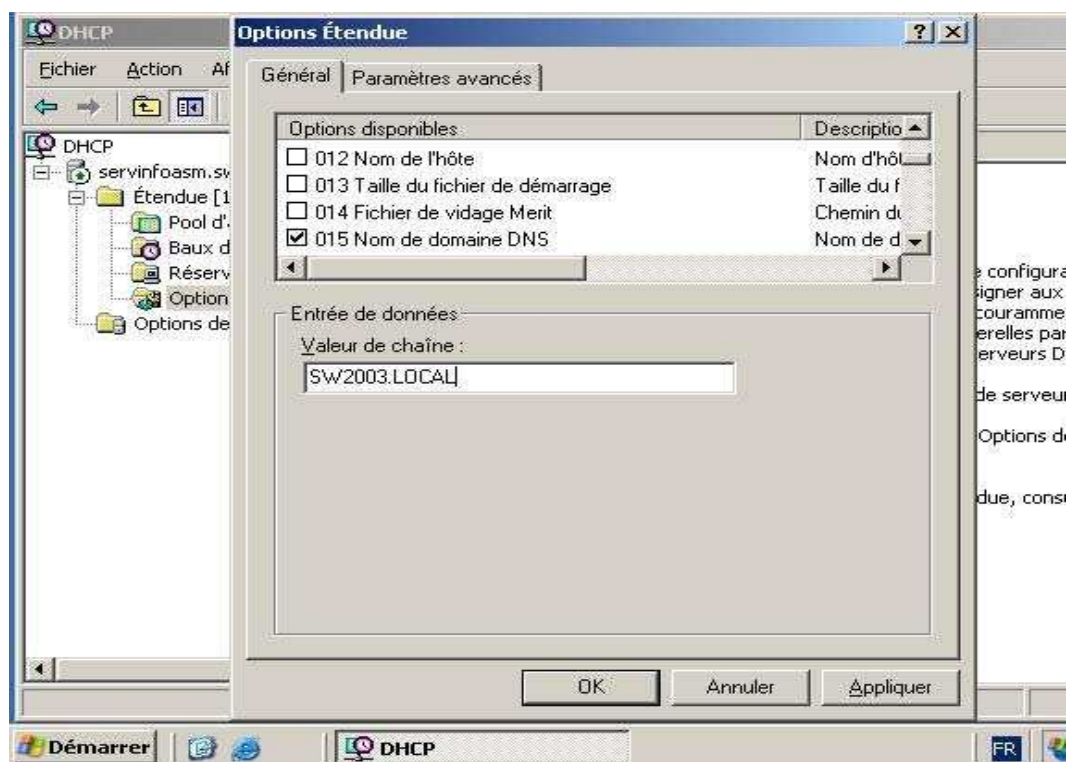
Sélection de l'option 003 Routeur, elle vous permet d'attribuer une adresse IP via une passerelle.



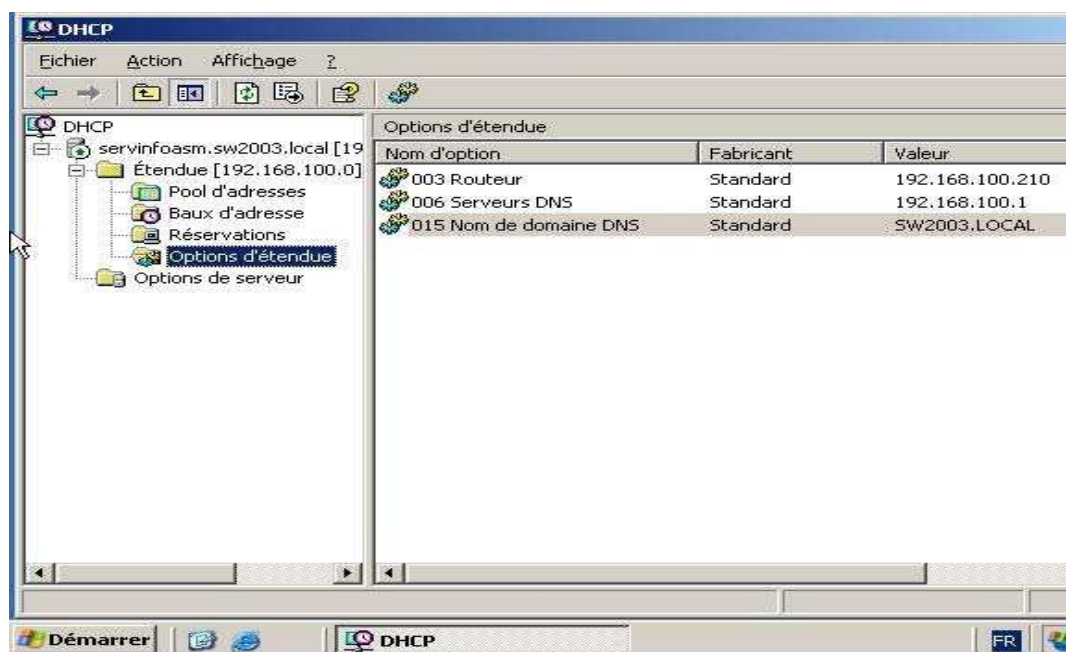
Sélection de l'option 006 Serveur DNS, elle est obligatoire pour correspondre avec le serveur DNS.



Sélection de l'option 015 Non de domaine, elle vous permet d'avoir les noms DNS des clients.



Voilà les principales options pour votre étendue, rien ne vous empêche d'en mettre d'autre pour vos besoins.



Il nous reste à activer l'étendue et à autoriser pour cela sélectionnez **Étendue [192.168.100.0]** puis par le menu **Action** choisissez **Autoriser**.

INSTALLATION WINDOWS RESSOURCE KIT

Ce kit gratuit comporte énormément d'utilitaires qui rendent de nombreux services !

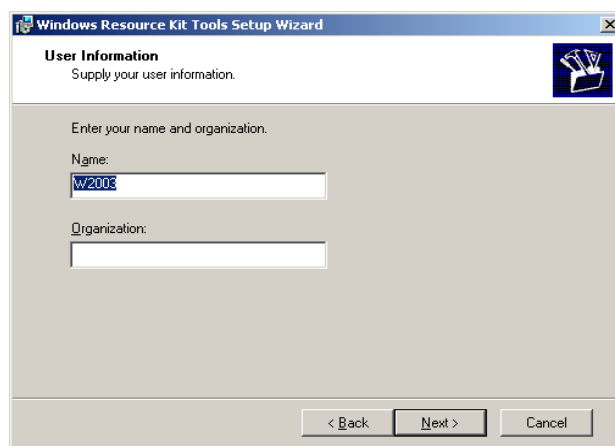
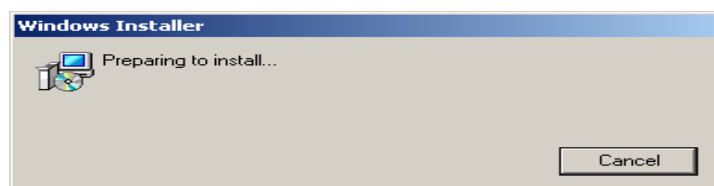
Ressource kit 2003 Windows Server 2003 Resource Kit Tools

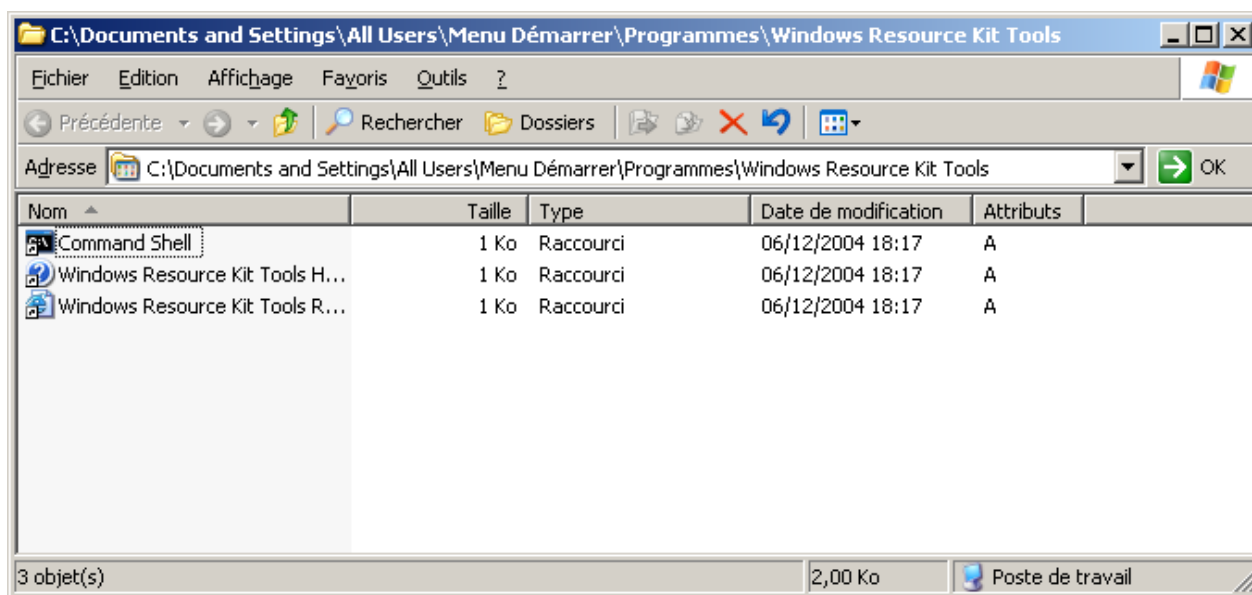
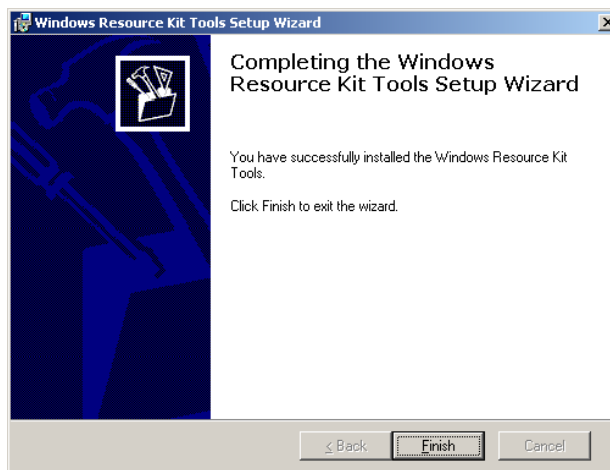
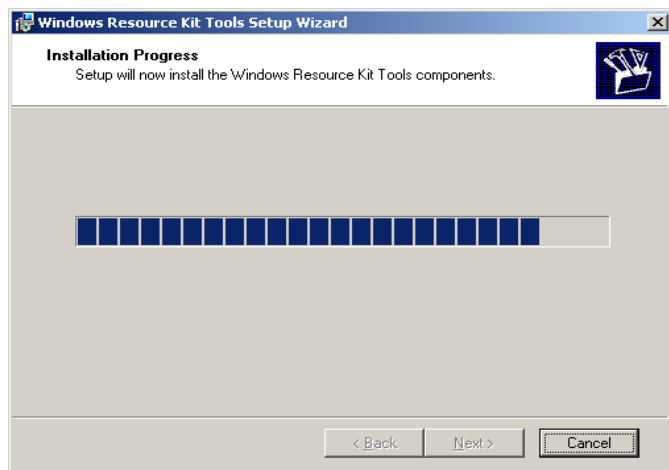
<http://www.microsoft.com/downloads/details.aspx?familyid=9d467a69-57ff-4ae7-96ee-b18c4790cffd&displaylang=en>

L'adresse des dernières versions disponible

<http://www.microsoft.com/windowsserver2003/techinfo/reskit/tools/default.msp#>

<http://www.microsoft.com/windowsserver2003/downloads/tools/default.msp#>





Liste des UTILITAIRES

Acctinfo.dll (documented in Readme.htm)

Adlb.exe: Active Directory Load Balancing Tool

Admx.msi: ADM File Parser

Atmarp.exe: Windows ATM ARP Server Information Tool

Atmlane.exe: Windows ATM LAN Emulation Client Information

Autoexnt.exe: AutoExNT Service

Cdburn.exe: ISO CD-ROM Burner Tool

Checkrepl.vbs: Check Replication

Chklnks.exe: Link Check Wizard

Chknic.exe: Network Interface Card Compliance Tool for Network Load Balancing

Cleanspl.exe: Spooler Cleaner

Clearmem.exe: Clear Memory

Clusdiag.msi: Cluster Diagnostics and Verification Tool

Clusfileport.dll: Cluster Print File Port

Clusterrecovery.exe: Server Cluster Recovery Utility

Cmdhere.inf: Command Here

Cmgetcer.dll: Connection Manager Certificate Deployment Tool

Compress.exe: Compress Files

Confdisk.exe: Disk Configuration Tool

Consume.exe: Memory Consumers Tool

Creatfil.exe: Create File

Csccmd.exe: Client-Side Caching Command-Line Options

Custreasonedit.exe: Custom Reason Editor (documented in Readme.htm)

Delprof.exe: User Profile Deletion Utility

Dh.exe: Display Heap

Diskraid.exe: RAID Configuration Tool

Diskuse.exe: User Disk Usage Tool

Dnsdiag.exe: SMTP DNS Diagnostic Tool (documented in Readme.htm)

Dumpfsmos.cmd: Dump FSMO Roles

Dvdburn.exe: ISO DVD Burner Tool

Empty.exe: Free Working Set Tool

Eventcombmt.exe: Check Replication

Fcopy.exe: File Copy Utility for Message Queuing

Frsflags.vbs

Getcm.exe: Connection Manager Profile Update

Gpmonitor.exe: Group Policy Monitor

Gpotool.exe: Group Policy Objects

Hlscan.exe: Hard Link Display Tool

Ifiltst.exe: IFilter Test Suite

Ifmember.exe: User Membership Tool

Inetesc.adm: Internet Explorer Enhanced Security Configuration

Iniman.exe: Initialization Files Manipulation Tool

Instcm.exe: Install Connection Manager Profile

Instsrv.exe: Service Installer

Intfiltr.exe: Interrupt Affinity Tool

Kerbtray.exe: Kerberos Tray

Kernrate.exe: Kernel Profiling Tool

Klist.exe: Kerberos List

Krt.exe: Certification Authority Key Recovery

Lbridge.cmd: L-Bridge

Linkd.exe

Linkspeed.exe: Link Speed

List.exe: List Text File Tool

Lockoutstatus.exe: Account Lockout Status (documented in Readme.htm)

Logtime.exe

Lsreport.exe: Terminal Services Licensing Reporter

Lsview.exe: Terminal Services License Server Viewer

Mcast.exe: Multicast Packet Tool

Memmonitor.exe: Memory Monitor

Memtriage.exe: Resource Leak Triage Tool

Mibcc.exe: SNMP MIB Compiler

Moveuser.exe: Move Users

Msccep.dll: Certificate Services Add-on for Simple Certificate Enrollment Protocol

Nlsinfo.exe: Locale Information Tool

Now.exe: STDOUT Current Date and Time

Ntimer.exe: Windows Program Timer

Ntrights.exe

Oh.exe: Open Handles

Oleview.exe: OLE/COM Object Viewer

Pathman.exe: Path Manager

Permcopy.exe: Share Permissions Copy

Perms.exe: User File Permissions Tool

Pfmon.exe: Page Fault Monitor

Pkiview.msc: PKI Health Tool

Pmon.exe: Process Resource Monitor

Printdriverinfo.exe: Drivers Source

Prnadmin.dll: Printer Administration Objects

Qgrep.exe

Qtcp.exe: QoS Time Stamp

Queryad.vbs: Query Active Directory

Rassrvmon.exe: RAS Server Monitor

Rcontrolad.exe: Active Directory Remote Control Add-On

Regini.exe: Registry Change by Script

Regview.exe (documented in Readme.htm)

Remapkey.exe: Remap Windows Keyboard Layout

Robocopy.exe: Robust File Copy Utility

Rpccfg.exe: RPC Configuration Tool

Rpcdump.exe

Rpcping.exe

RPing: RPC Connectivity Verification Tool

Rqc.exe: Remote Access Quarantine Client

Rqs.exe: Remote Access Quarantine Agent

Setprinter.exe: Spooler Configuration Tool

Showacls.exe

Showperf.exe: Performance Data Block Dump Utility

Showpriv.exe: Show Privilege

Sleep.exe: Batch File Wait

Sonar.exe: FRS Status Viewer

Splinfo.exe: Print Spooler Information

Srvany.exe: Applications as Services Utility

Srvcheck.exe: Server Share Check

Srvinfo.exe: Remote Server Information

Srvmgr.exe: Server Manager

Ssdformat.exe: System State Data Formatter

Subinacl.exe

Tail.exe

Temon.exe: Traffic Control Monitor

Timeit.exe (documented in Readme.htm)

Timezone.exe: Daylight Saving Time Update Utility

Tsctst.exe: Terminal Server Client License Dump Tool

Tsscalling.exe: Terminal Services Scalability Planning Tools

Uddicatschemeeditor.exe: UDDI Services Categorization Scheme Editor

Uddiconfig.exe: UDDI Services Command-line Configuration Utility

Uddidataexport.exe: UDDI Data Export Wizard

Usrmgr.exe: User Manager for Domains

Vadump.exe: Virtual Address Dump

Vfi.exe: Visual File Information

Volperf.exe: Shadow Copy Performance Counters

Volrest.exe: Shadow Copies for Shared Folders Restore Tool

Vrfydsk.exe: Verify Disk

Winexit.scr: Windows Exit Screen Saver

Winhttpcertcfg.exe: WinHTTP Certificate Configuration Tool

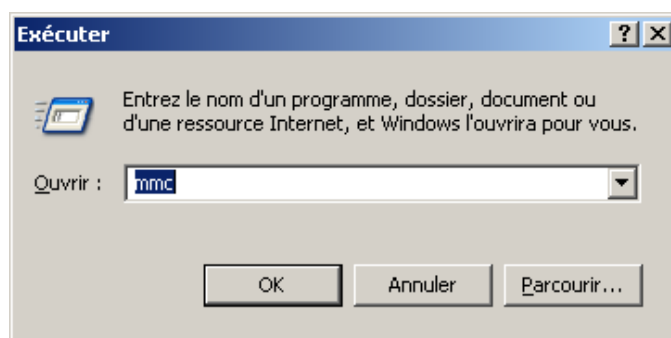
Winhttptracecfg.exe: WinHTTP Tracing Facility Configuration Tool

Winpolicies.exe: Policy Spy

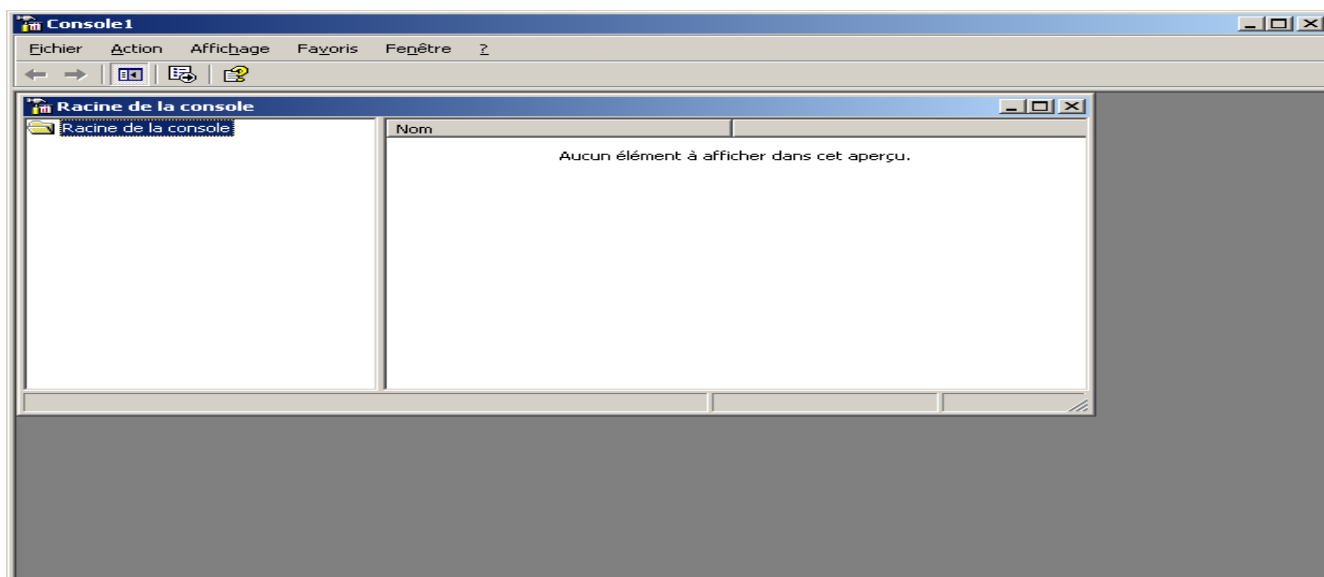
Wins.dll: WINS Replication Network Monitor Parser

Wlbs_hb.dll & Wlbs_rc.dll: Windows Load Balancing Server Network Monitor Parsers

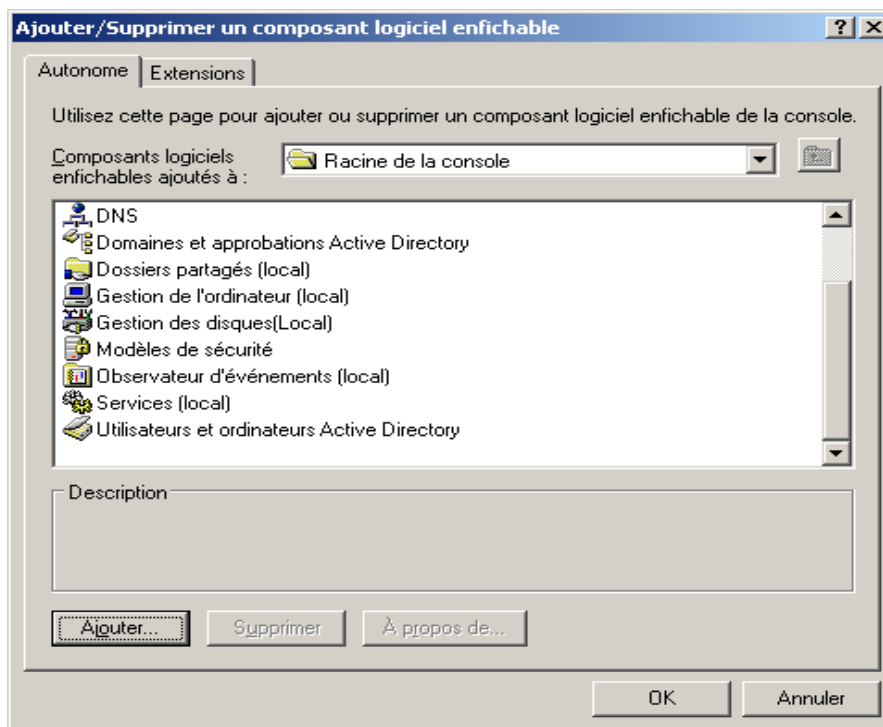
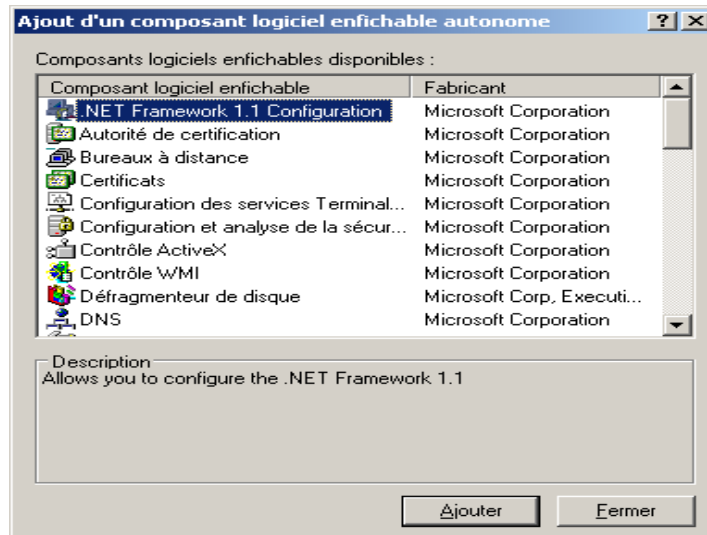
INSTALLATION D'UNE CONSOLE PERSONNALISÉ

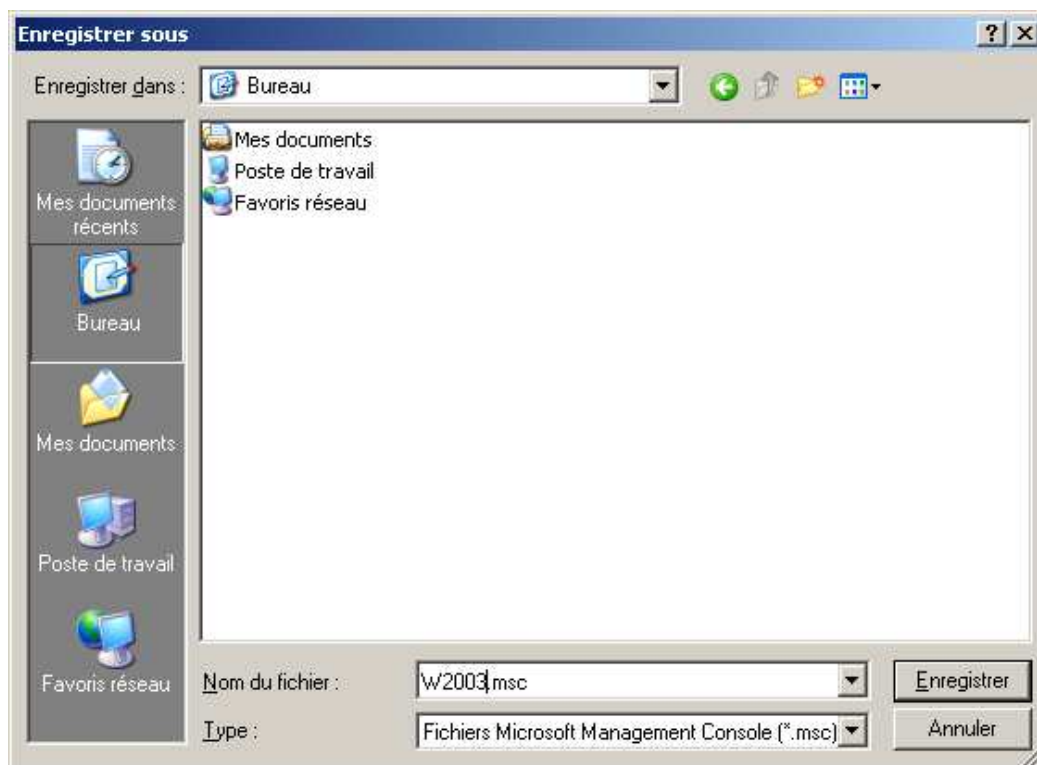
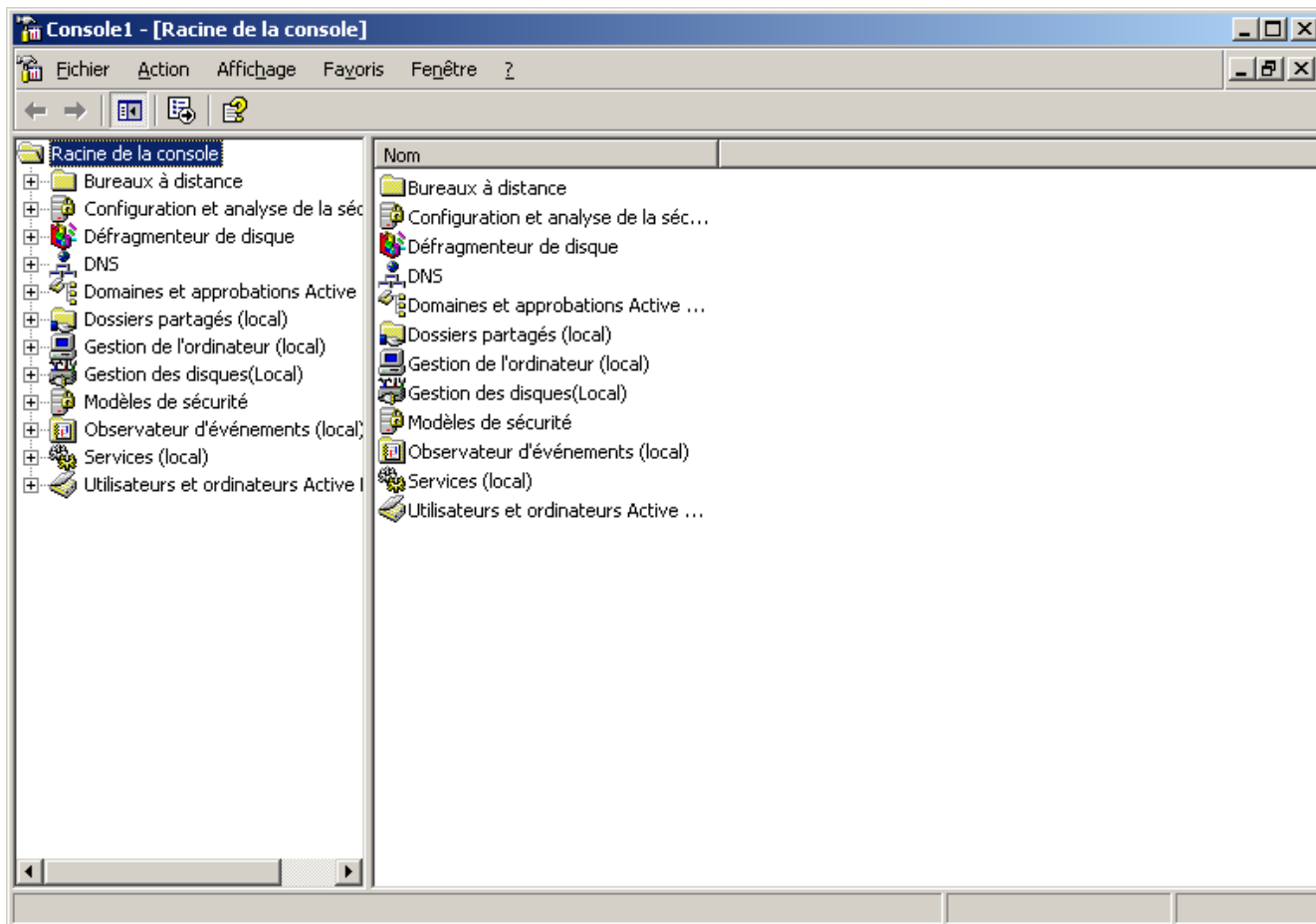


DEMARRER > EXECUTER > MMC



Ajouter ou supprimer éléments enfichables





INSTALLATION DES OUTILS D'ADMINISTRATION DISTANT

Les outils d'administration de base

Adminpak.msi

Le package Adminpak.msi contient tous les outils d'administration de Windows Server 2003. Il est possible de l'installer sur un poste client afin de disposer de ces outils. Le package se trouve sur le CD-ROM de Windows Server 2003 dans le répertoire I386 ou est téléchargeable sur le site de Microsoft et ne peut être installés que sur des ordinateurs fonctionnant sous Windows Server 2003 ou Windows XP Professionnel. Une fois ces outils installés sur notre poste de travail, il nous suffit de lancer l'outil dont nous avons besoin via les Outils d'administration se trouvant dans le Panneau de configuration :



Le simple fait d'appartenir au domaine permet à l'outil que nous avons choisi d'afficher les informations relatives à notre domaine. Cette solution est pratique si nous voulons avoir la possibilité d'administrer nos serveurs à partir de n'importe quel poste du réseau (surtout si celui-ci est vaste).

Il faut savoir que pour lancer ces outils à partir d'un ordinateur client, nous devons utiliser un compte possédant les droits suffisants pour ouvrir les différentes consoles ou un compte à qui a été délégué certaines tâches administratives. Cependant si nous utilisons un compte avec de simples droits d'utilisateur, il est possible d'utiliser une fonctionnalité apparue avec Windows 2000 : la commande Exécuter en tant que...

1.2 Exécuter en tant que...

Comme dit précédemment il est possible de lancer des outils d'administration avec un simple compte d'utilisateur. Le principe consiste à utiliser les informations d'authentification d'un compte ayant des droits d'administration pour lancer les consoles. Pour ce faire, il faut effectuer la combinaison SHIFT + clic droit de la souris sur l'outil choisi. Voici le résultat :



Dans le menu contextuel nous choisissons donc "Exécuter en tant que..." Voici la fenêtre qui apparaît :



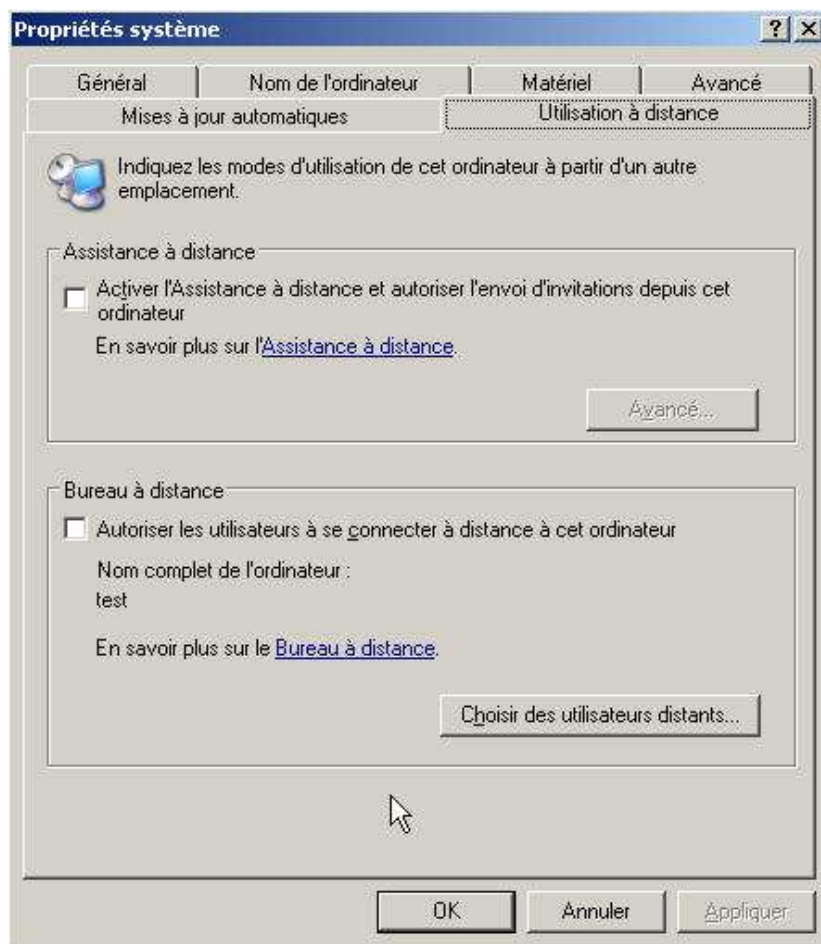
Nous devons sélectionner le bouton radio "L'utilisateur suivant" afin de lancer la MMC avec des informations d'authentification d'un utilisateur habilité à le faire. Faites attention car par défaut, c'est l'Administrateur local qui est spécifié dans le champ "Nom d'utilisateur" situé sous le bouton radio. Il faudra indiquer le nom d'un utilisateur du domaine pour ouvrir une MMC d'un domaine. De plus, il faudra respecter la nomenclature suivante : nom_du_domaine\nom_d'utilisateur. Autrement et même si vous spécifiez bien un utilisateur du domaine mais sans renseigner également son domaine d'appartenance, vous recevrez ce message :



Cette technique qui pourra être utilisée dans les environnements où la politique de sécurité est élevée par exemple : les administrateurs posséderont ainsi des comptes d'utilisateurs simples et utiliseront cet outil pour effectuer des tâches administratives.

Le bureau à distance

Le bureau à distance équivaut aux services Terminal Server en mode Administration de Windows 2000 Server. Cette fonctionnalité est installée par défaut mais elle est désactivée. Pour l'activer, il suffit d'ouvrir les Propriétés systèmes, d'aller dans l'onglet "Utilisation à distance" et de cocher la case "Autoriser les utilisateurs à se connecter à distance à cet ordinateur".

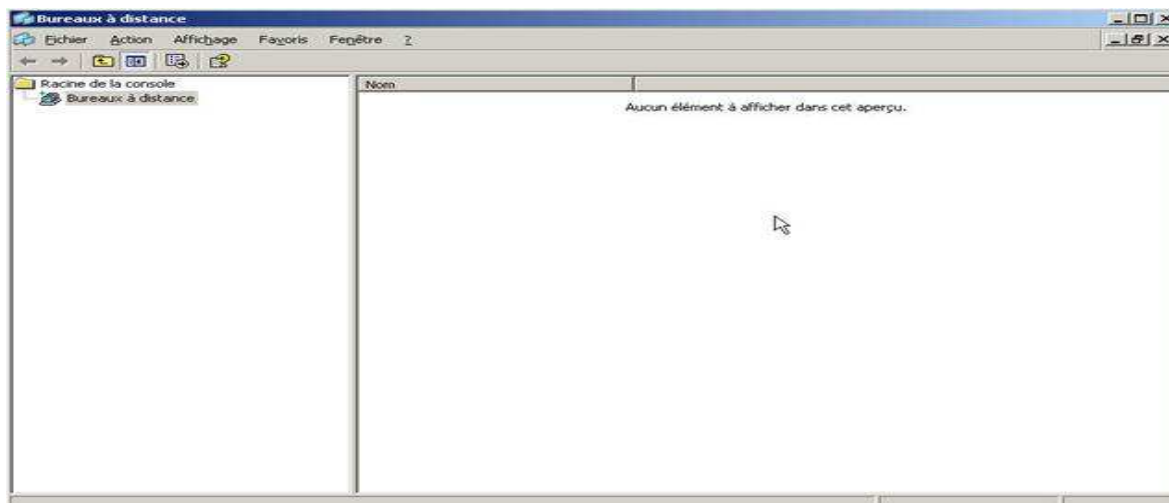


En revanche il est inutile d'ajouter des utilisateurs via le bouton "Choisir les utilisateurs distants" car les membres du groupe "Administrateurs" ont les droits suffisants pour se connecter à distance sans pour autant faire partie du groupe "Utilisateurs du bureau à distance". A noter que le fait d'ajouter des utilisateurs via le bouton précédemment cité ajoute en fait des utilisateurs au groupe "Utilisateurs du bureau à distance". Suite à cette manipulation, 2 administrateurs peuvent se connectés simultanément à leurs serveurs via les services Terminal Server.

La MMC "Bureaux à distance"

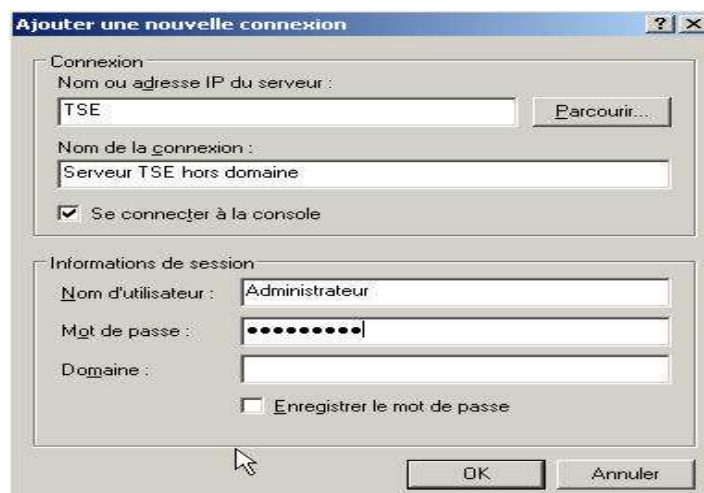
Disponible dans les Outils d'administration, cette console regroupe en fait tous les serveurs sur lesquels nous avons activé le bureau à distance (pour Windows Server 2003) ou les services TSE en mode Administration (pour Windows 2000 serveur). En effet l'un des avantages de cette console est qu'elle permet de gérer aussi bien des serveurs sous Windows 2000 que sous Windows 2003. Un autre avantage est que l'on peut aussi bien administrer des Contrôleurs de domaine que des serveurs membres ou encore des serveurs autonomes.

Voici comment se présente cette console :



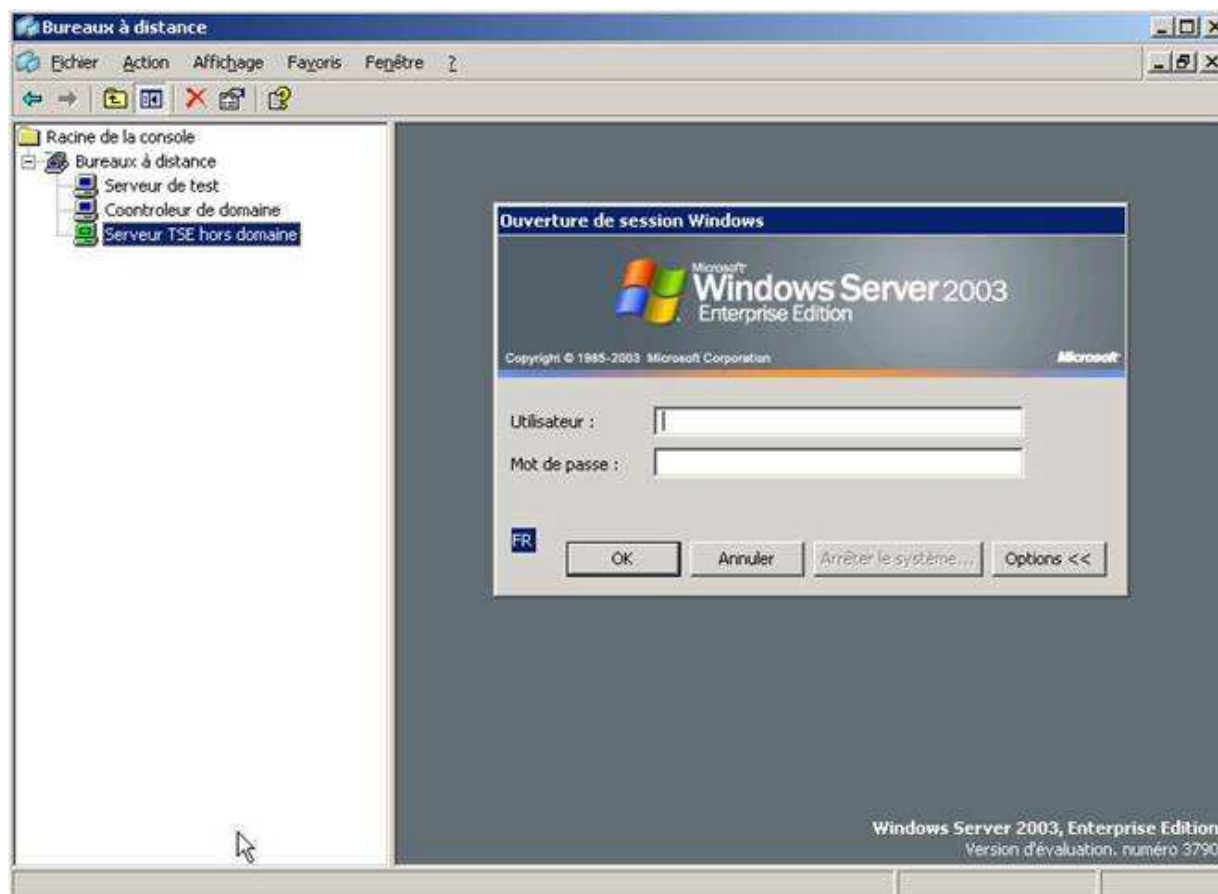
Pour ajouter un serveur à notre console, il suffit de faire un clic droit sur Bureaux à distance et de choisir "Ajouter une nouvelle connexion...". Pour ajouter ce nouveau serveur, nous pouvons soit taper son adresse IP, soit son nom de machine. Le bouton "Parcourir" nous permet de rechercher les serveurs sur lesquels sont installés les services Terminal Server. Si nous nous trouvons dans un domaine, la recherche se limitera à notre domaine. Et si notre domaine ne contient aucun serveur hébergeant les services TS, nous en serons avertis. Les serveurs membres ou autonomes ayant le bureau à distance activé ne sont pas pris en compte. Cela ne nous empêche pas d'ajouter ces serveurs à notre liste.

Nous pouvons également donner un nom convivial à la connexion que nous venons de créer. Enfin nous pouvons, comme pour un client RDP, pré-remplir les informations d'authentification afin de nous connecter directement à notre serveur :

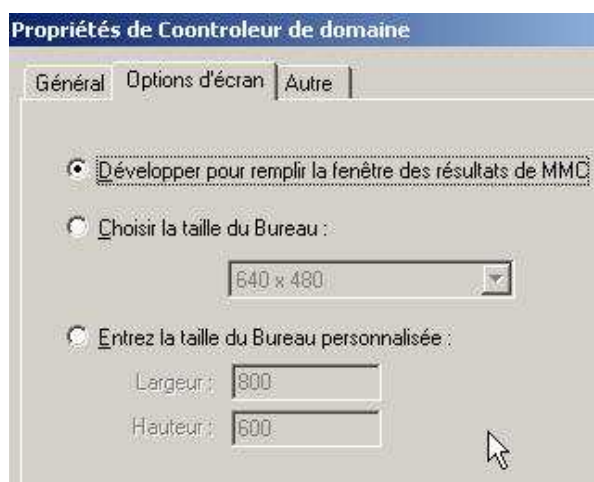


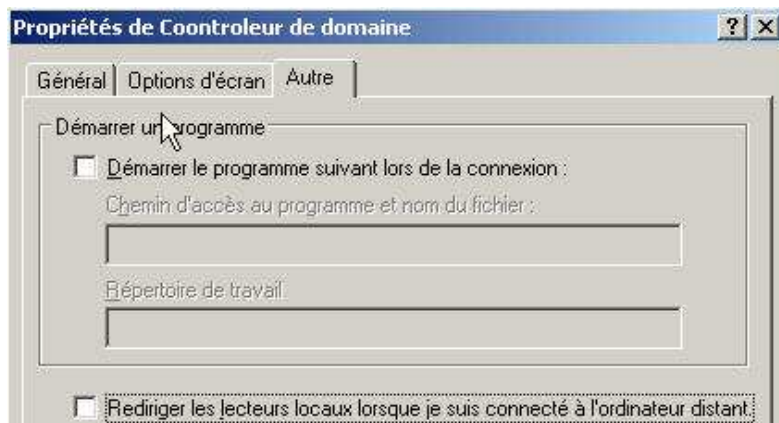
Le bouton "Se connecter à la console" nous permet d'ouvrir une session directement sur le serveur comme si nous nous trouvions physiquement devant (voir plus haut).

Une fois connecté à notre serveur, le contenu s'affiche dans la fenêtre de droite :



Il est possible dans les propriétés de notre connexion de définir certaines options comme la résolution de l'écran ou encore le fait de lancer un programme particulier à la connexion ou non :





Attention lorsque que vous saisissez le nom ou l'adresse IP du serveur que vous désirez ajouter à votre liste de bureaux à distance, aucunes vérifications n'est faite : tous serveur que vous ajouterez sera donc listé. Il ne sera cependant pas possible de s'y connecter si les services TS ou bureau à distance ne sont pas installés et activés.

Administration Web

L'une des nouveautés de Windows Server 2003 en matière d'administration est la possibilité d'utiliser un navigateur Web pour administrer à distance ses serveurs. Cette fonctionnalité s'appelle Web Interface for Remote Administration (Interface Web pour Administration à Distance). Pour être mise en œuvre, elle nécessite les services IIS 6 installés sur les serveurs. Il est important de noter que cette fonctionnalité est installée par défaut sur la version Web Edition de Windows Server 2003. Pour les autres éditions, il faut l'installer à la main. Comment cela se passe-t-il ?

Installation

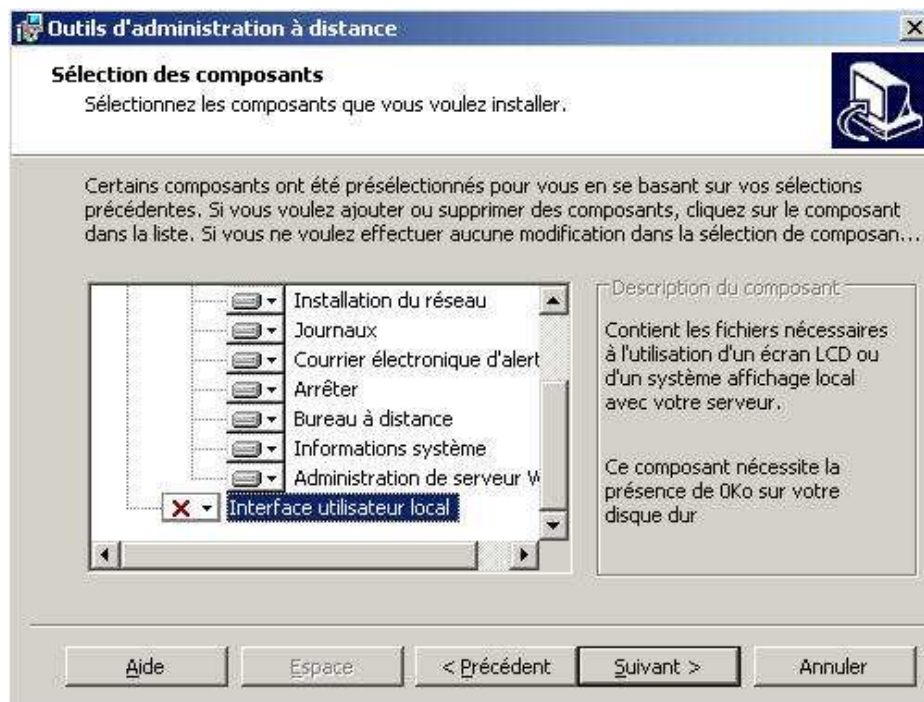
Tout d'abord, il faut que les services IIS soient installés sur le serveur. Lorsque l'on se rend dans "Ajout/Suppression de composants Windows" pour ajouter les services IIS, il est possible (et même nécessaire) via le bouton détails d'ajouter le composant "Administration à distance (HTML)".



Ensuite, il faut lancer le package MSI suivant dans Démarrer\Exécuter : sasetup.msi. Une fois lancé, un assistant apparaît pour nous guider dans l'installation de ce composant :



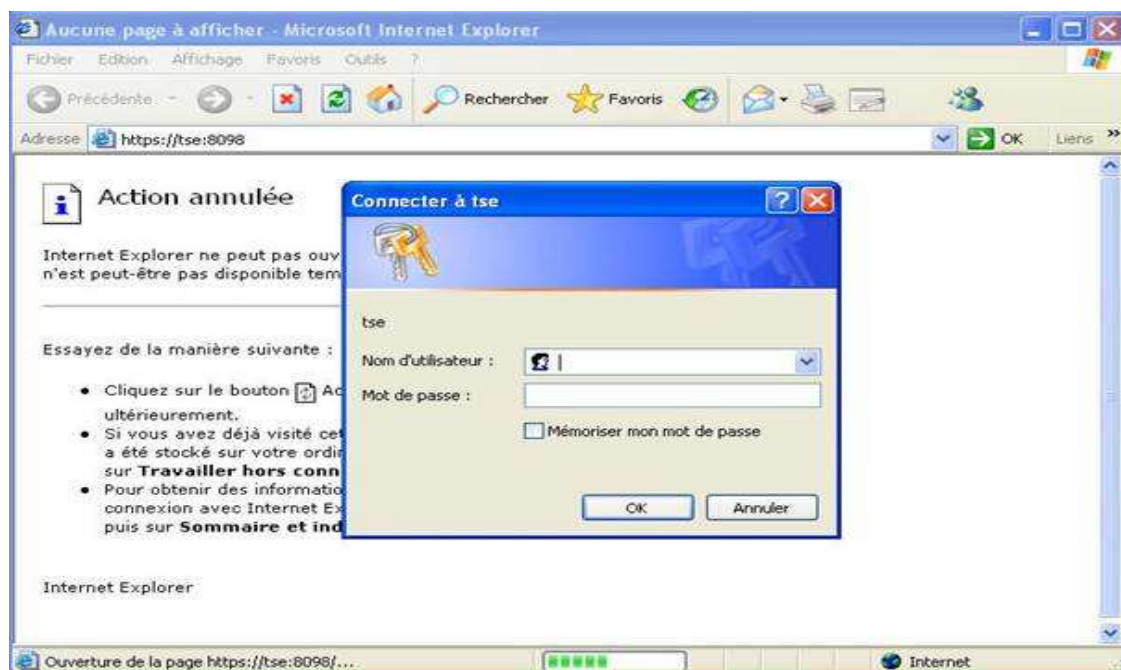
Par défaut, tous les composants qui forment ce package sont installés sauf l'Interface Utilisateur Local. Nous pouvons choisir de l'installer ou non, cela n'aura que peut d'influence sur le fonctionnement de l'interface d'administration Web :



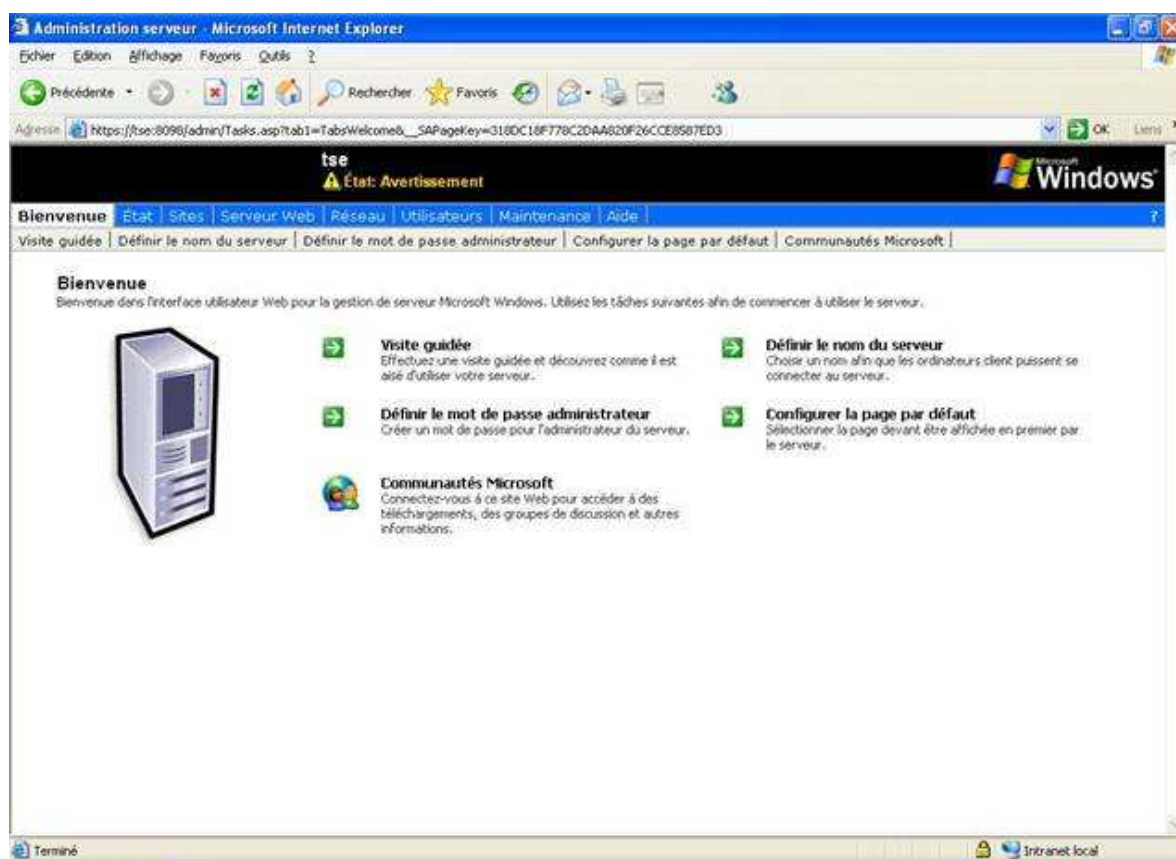
Le fait d'installer ce composant modifie l'installation des outils d'administration à distance.

Utilisation

Une fois le composant installé, il faut ouvrir une fenêtre d'Internet Explorer et taper dans la barre d'adresse : https://nom_du_serveur:8098. Des informations d'authentification nous sont alors demandées : il faut saisir les nom et mot de passe d'un utilisateur ayant des droits suffisant d'administration :



Une fois ces informations renseignées, nous arrivons sur l'interface d'administration Web. Une aide nous est proposée afin de nous guider dans nos tâches administratives via cet outil.



Il nous est possible d'effectuer toutes les actions possibles d'administration et de configuration de notre serveur comme si nous étions devant :

- Administrer les services Web :

Nous pouvons créer des sites, leur attribuer des ports, arrêter/redémarrer un site, configurer le répertoire de base des sites, limité l'accès à un nombre de personnes définis, etc...

- Administrer les services réseaux :

Il est possible de modifier le nom du serveur, le workgroup auquel il appartient, l'intégrer à un domaine, configurer les interfaces réseaux en spécifiant si elles seront gérées via DHCP ou leur attribuées des adresses IP fixes, etc...

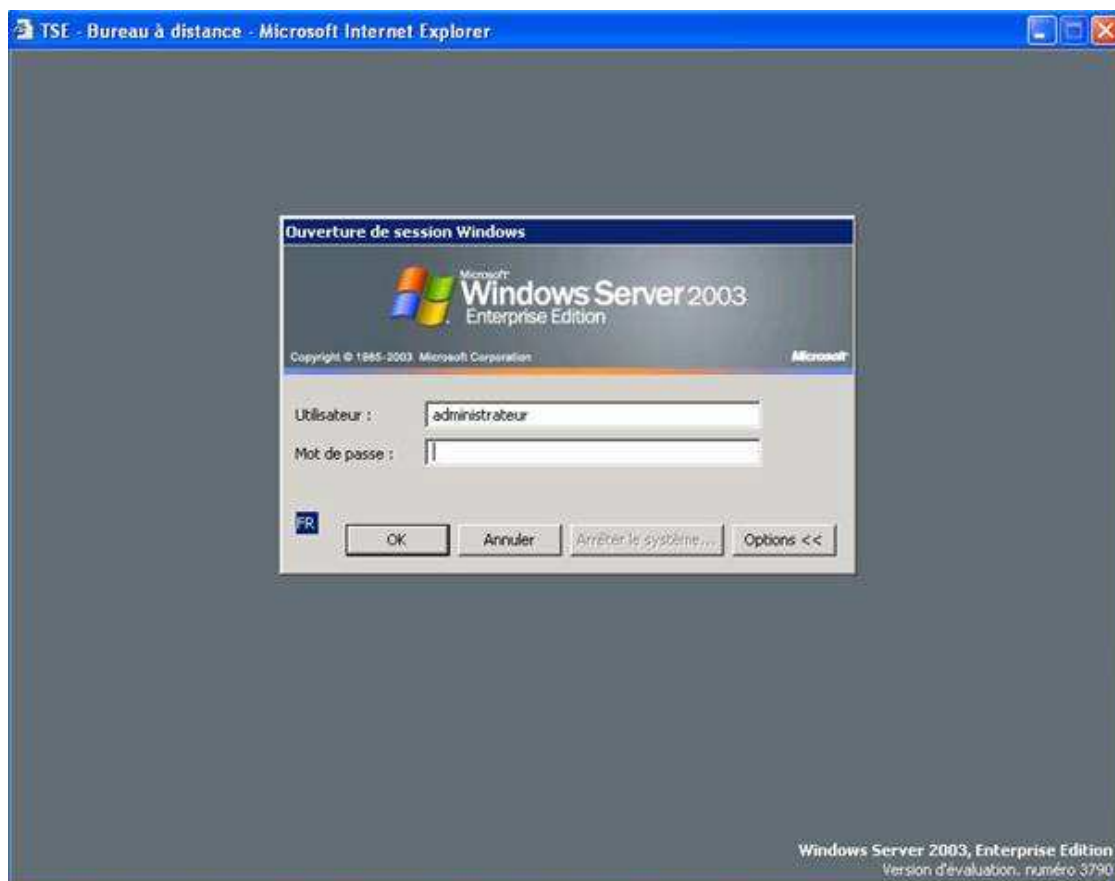
- Gérer les utilisateurs et les groupes locaux :

Là, nous créons, modifions, activons/désactivons et supprimons des utilisateurs et des groupes locaux.

- Bureau à distance via Internet

Enfin, il est possible de se connecter via les services Terminal Server en passant par notre navigateur web :

Par exemple si nous voulons partager un répertoire à distance mais que la machine sur laquelle nous travaillons ne possède pas de client RDP, nous avons la possibilité de nous connecter à notre serveur en TSE via Internet Explorer.



Microsoft annonce GPMC

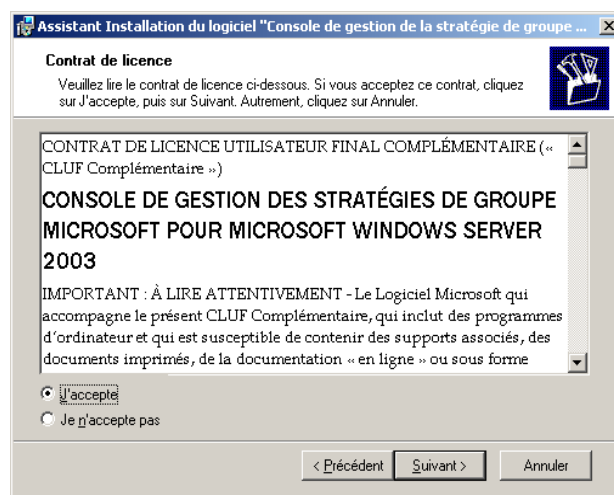
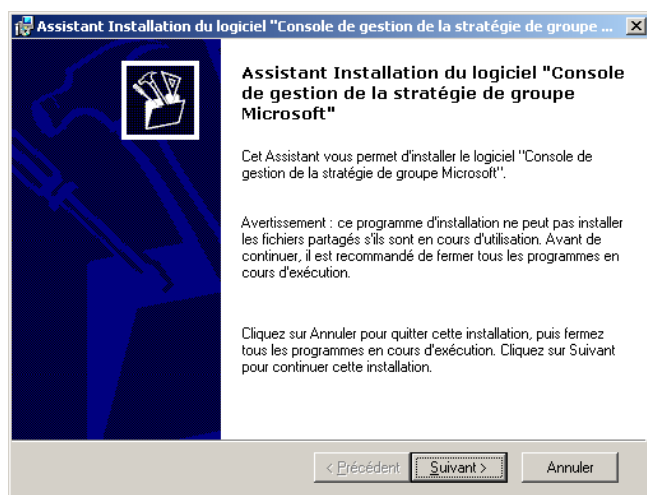
Microsoft vient d'annoncer la sortie de Group Policy Management Console (GPMC), un nouvel outil gratuit de gestion des GPO pour Windows Server (2000 et 2003).

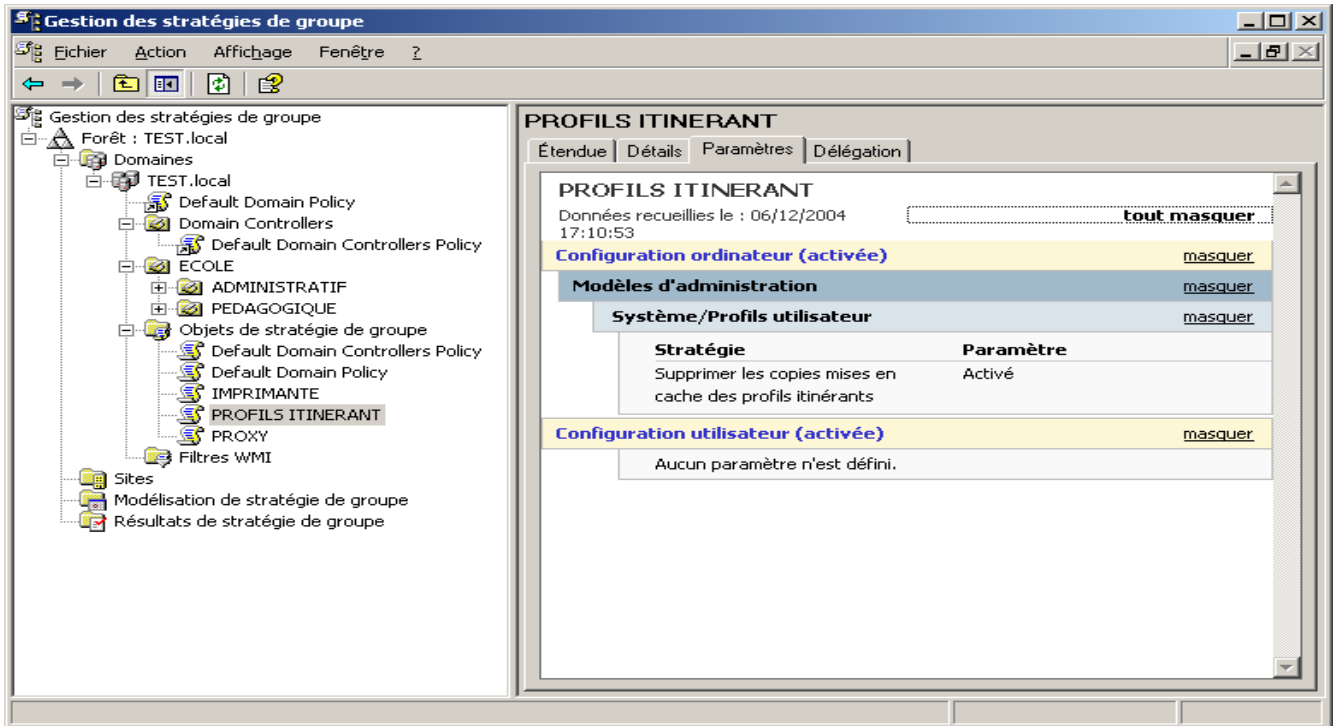
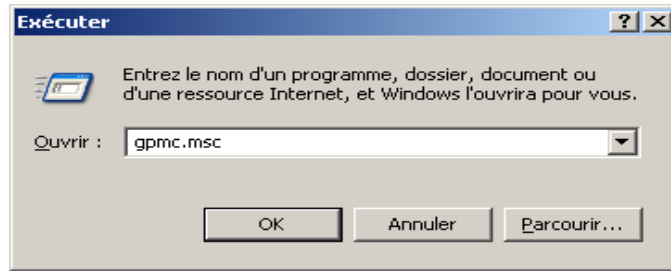
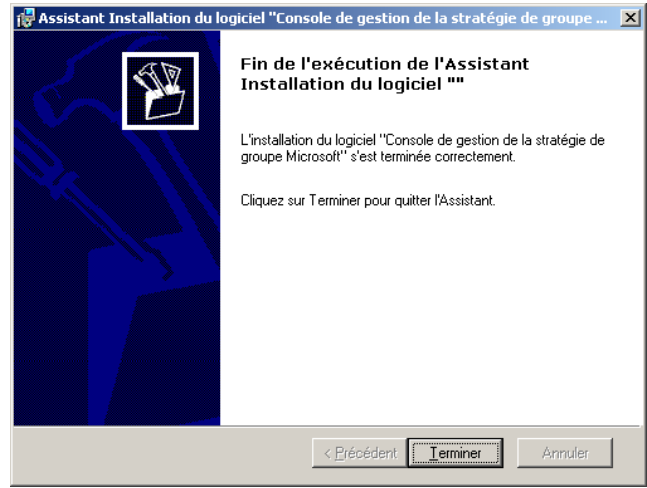
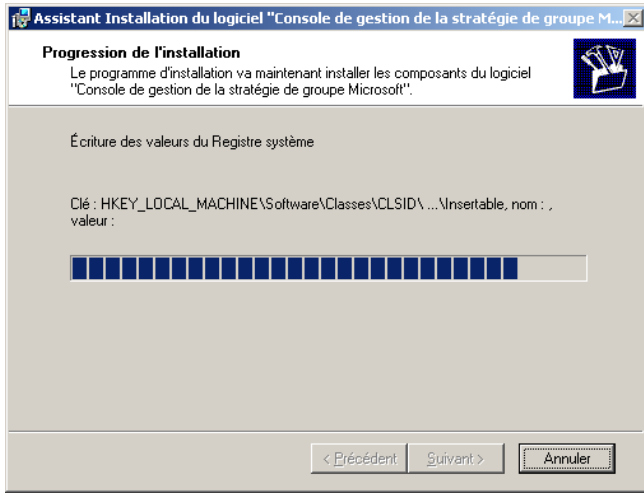
GPMC est un snap-in MMC permettant une visualisation centralisée des GPOs, des unités organisationnelles (OUs), des domaines et des sites, fournissant ainsi un point d'accès unique pour toutes les tâches (import, export, copier, coller, reporting,...) relatives à la gestion des GPOs.

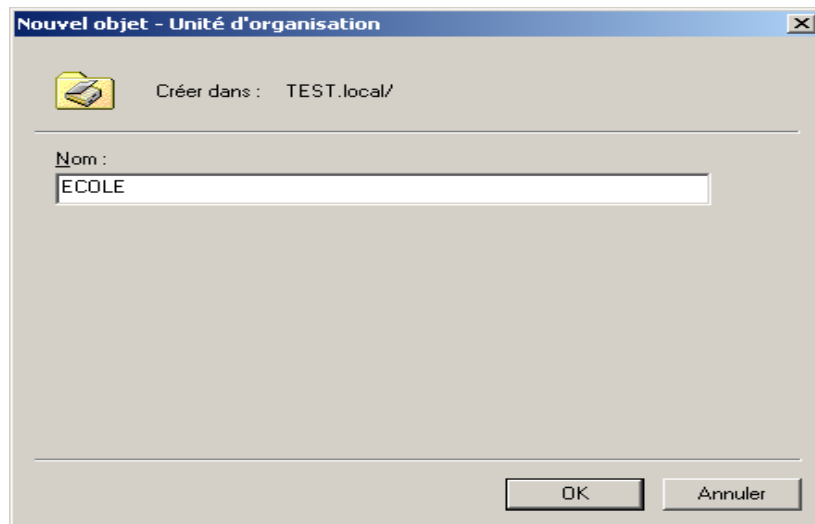
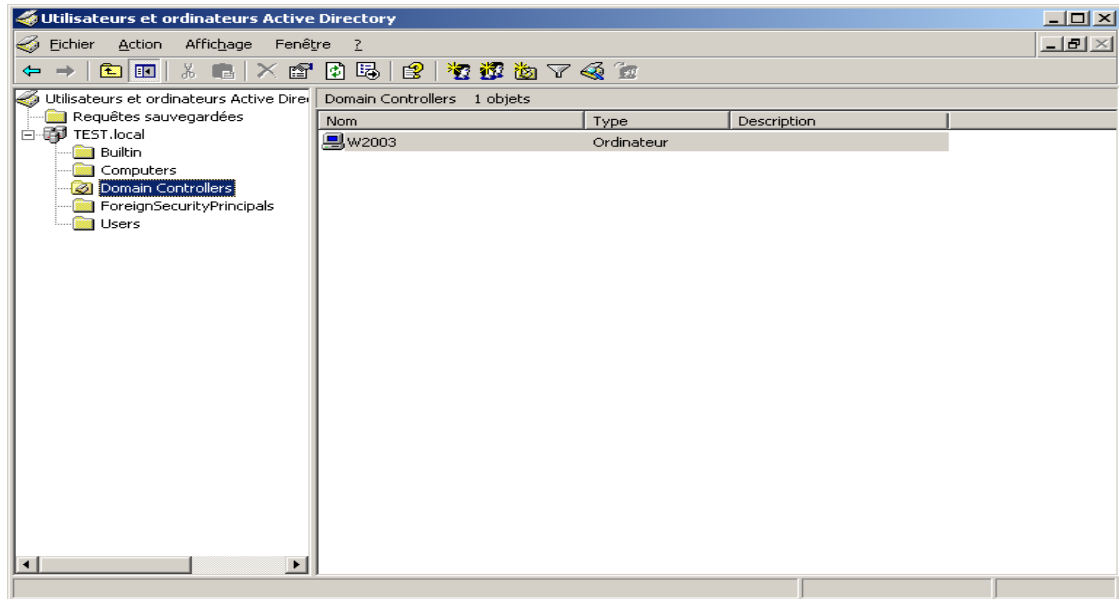
GPMC est compatible avec les domaines Windows 2000 et Windows Server 2003, mais doit être installé sur un système Windows XP SP1 ou Windows Server 2003.

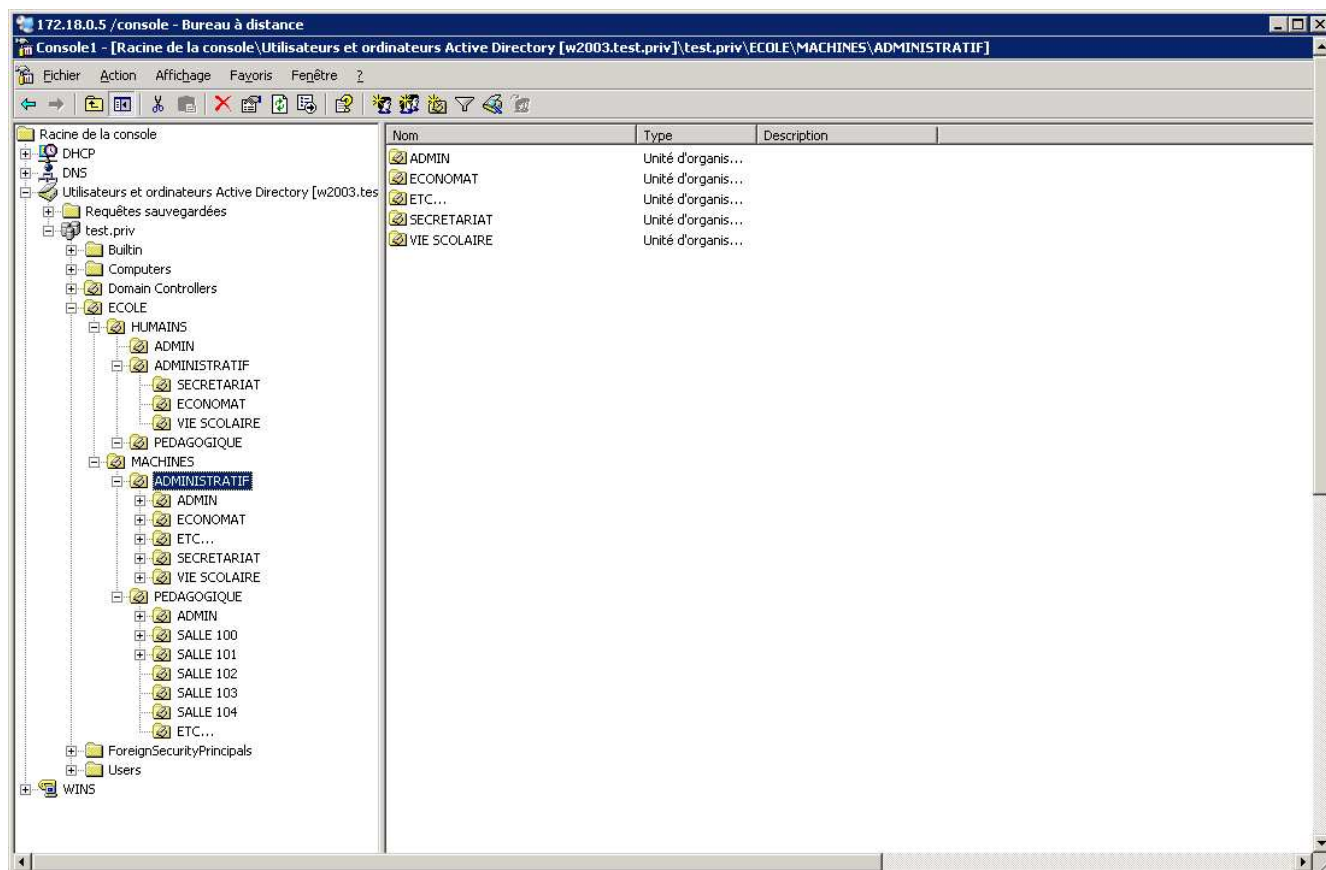
GPMC est disponible en téléchargement (version anglaise uniquement) à partir du site Microsoft.

[Informations détaillées et téléchargement de GPMC \(4,5 Mo\)](#)









Les unités d'organisation sont empilables, emboîtables à volonté avec comme limite une arborescence de 250 Niveaux !

L'AD est organisée en objet concret (COMPUTERS, USERS) et des objets qui ne sont pas forcément sur le serveur mais référencé dans l'AD (PARTAGE, IMPRIMANTE)

CREATION DES UTILISATEURS POUR UN SERVEUR ADMINISTRATIF

ADDUSERS.exe disponible sur le site ci-dessous :

<http://tech.cuip.net/logins/docs/Addusers-overview.htm>

http://perso.wanadoo.fr/college_magalas34/nt4_addusers.htm

`addusers /c <file name>` (Création)

`addusers /e <file name>` (Suppression)

`addusers /b <file name>` (Récupère les comptes utilisateurs, groupes locaux ou globaux et les copie vers le fichier)

`addusers [\Nom d'ordinateur] [{ /c | /d | /e } Nom du fichier] [/s:x] [/?]`

En résumé :

/c	créé les comptes utilisateurs, groupes locaux ou groupes globaux spécifiés dans le fichier texte
/d	Récupère les comptes utilisateurs, groupes locaux ou globaux et les copie vers le fichier (sans les mots de passe)
/e	Efface les comptes utilisateurs spécifiés dans le fichier

Le script de création des utilisateurs est un simple fichier texte avec la syntaxe suivante :

```
[Users]
<Nom d'utilisateur>,<Nom détaillé>,<Mot de passe>,<Répertoire Home>,<Chemin vers Home>,<Profil>,<Script>
```

```
addusers /c c:\fichier.csv /p:lce >fic.txt
```

Les utilisateurs n'auront pas à changer leur mot de passe,

Ne pourront pas en changer,

Le mdp n'expire jamais,

En prime un CR de l'opération est sauvegardé dans « fic.txt »

Création des répertoires personnels :



J'utilise deux fichiers BAT, RMTSHARE.exe, Xcacds.exe de Microsoft pour créer les répertoires personnels à partir de la liste des utilisateurs

<http://www.microsoft.com/windows2000/techinfo/reskit/tools/default.asp>

<ftp://ftp.microsoft.com/bussys/winnt/winnt-public/reskit/nt40/i386/>

```
MakeListPerso.bat
```

```
echo off
```

```
cls
```

```
echo.
```

```
echo -----
```

```
echo Création de tous les dossiers personnels de tous les utilisateurs
echo -----
echo.
echo.
echo.
::
if EXIST %1 GOTO OK
echo.
echo Le fichier %1 est introuvable.
echo Le processus est arrêté !
echo.
pause
::
GOTO FIN
:OK
::
:DEJA_V
FOR /F "tokens=1" %%A IN (%1) DO call creathome %%A
:FIN
```

```
creathome.bat
md c:\users\%1
xcaccls c:\users\%1 /g "TEST\%1":C /y
xcaccls c:\users\%1 /e /g "TEST\administrateur":F /y
rmtshare \\172.18.0.5\%1$c:\users\%1
```

CREATION D'UN SCRIPT DE DEMARRAGE

- Pour un poste XP/2000
- Pour un poste 98, 98se, ME

Script XP /2000

Le script utilise IFMEMBER de chez Microsoft, il est téléchargeable gratuitement (copier le dans le NETLOGON) :

<ftp://ftp.microsoft.com/bussys/winnt/winnt-public/reskit/nt40/i386/>

Commencer par créer un script login.bat qu'il vous suffit d'éditer avec Notepad

Le principe est très simple :

Si vous êtes membre d'un groupe Admin alors ça exécute une commande qui mappe une ressource du réseau sinon ça passe à la suite, etc...

Ex :

```
login.bat - Bloc-notes
Fichier Edition Format Affichage ?
@ if [%OS%]==[windows_NT] net use * /delete /y
ifmember ADMIN
if not errorlevel 1 goto suite
net use J: \\w2003\outils$ /persitent:no >nul
:suite
```

Il existe une variante avec KIX32 mais plus complexe à mettre en place (mais fonctionne avec XP /2000 /98/ 98se /Me)

<http://www.kixtart.org>

Script 98, 98se, Me

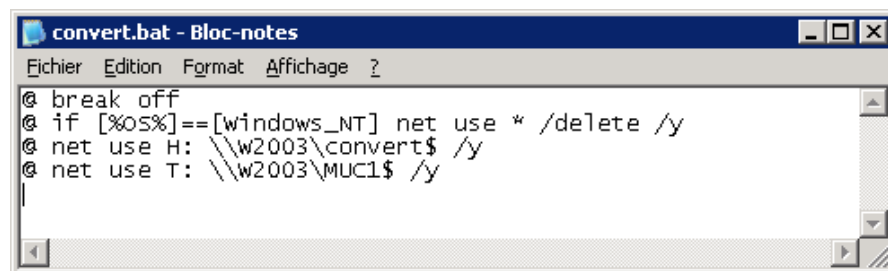
Le script est personnel puisqu'il est unique à chaque utilisateur :

La commande utilisé est NET USE (NET USE ?)

NET USE
[nom de périph.*] [\Ordinateur\Partage[volume] [mot de passe *]]
[/USER:[nom de domaine\]nom d'utilisateur]
[/USER:[nom de domaine avec points\]nom d'utilisateur]
[/USER:[nom d'utilisateur@nom de domaine avec points]
[/SMARTCARD]
[/SAVECRED]
[[/DELETE] [/PERSISTENT:{YES NO}]]
NET USE [nom de périphérique *] [mot de passe *] [/HOME]

```
NET USE [/PERSISTENT:{YES | NO}]
```

Ex:



```
convert.bat - Bloc-notes
Fichier Edition Format Affichage ?
@ break off
@ if [%OS%]==[windows_NT] net use * /delete /y
@ net use H: \\w2003\convert$ /y
@ net use T: \\w2003\MUC1$ /y
```

Il existe un logiciel très agréable et gratuit pour écrire des fichiers BAT, il se nomme astase PowerBatch.

www.astase.com

Voici des liens sur les fichier Bat

<http://www.pointbat.be.tf/>

<http://www.autourdupc.com/index.php?sImp=&sType=SFT&sOS=&sOSver=&sRub=&sSvce=&sNoFrm=&sPage=Logiciel/Scripts/Cmd2000.htm>

<http://www.fpschultze.de/bsc.htm>

GESTION 5

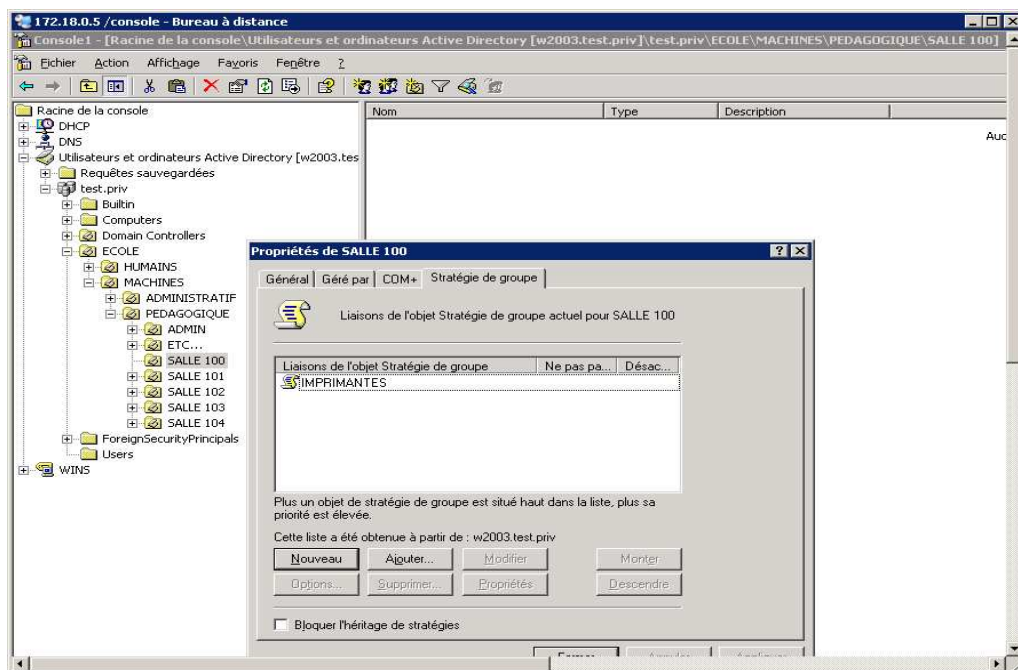
<http://www.ac-amiens.fr/pedagogie/tice/reseaux/outils/nt4/default.htm>

CREATION D'UNE STRATEGIE de groupe (UTILISATEUR / MACHINE)

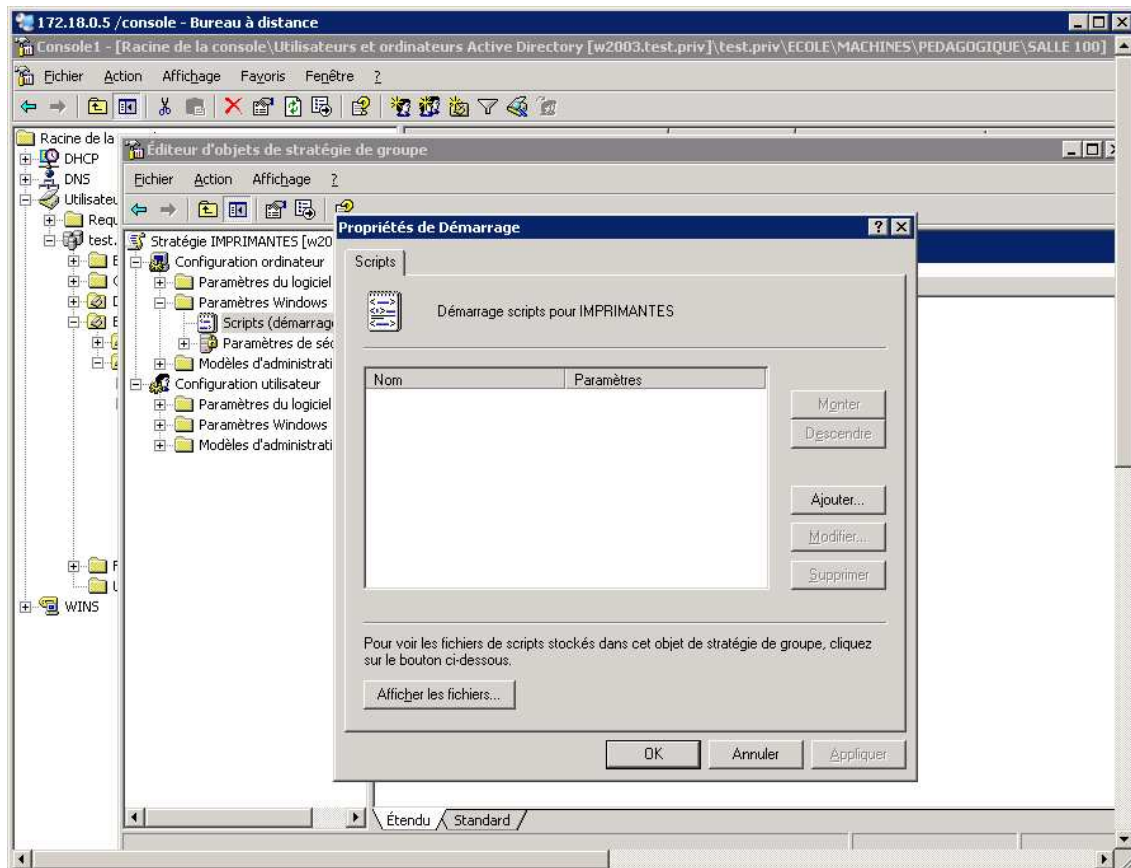
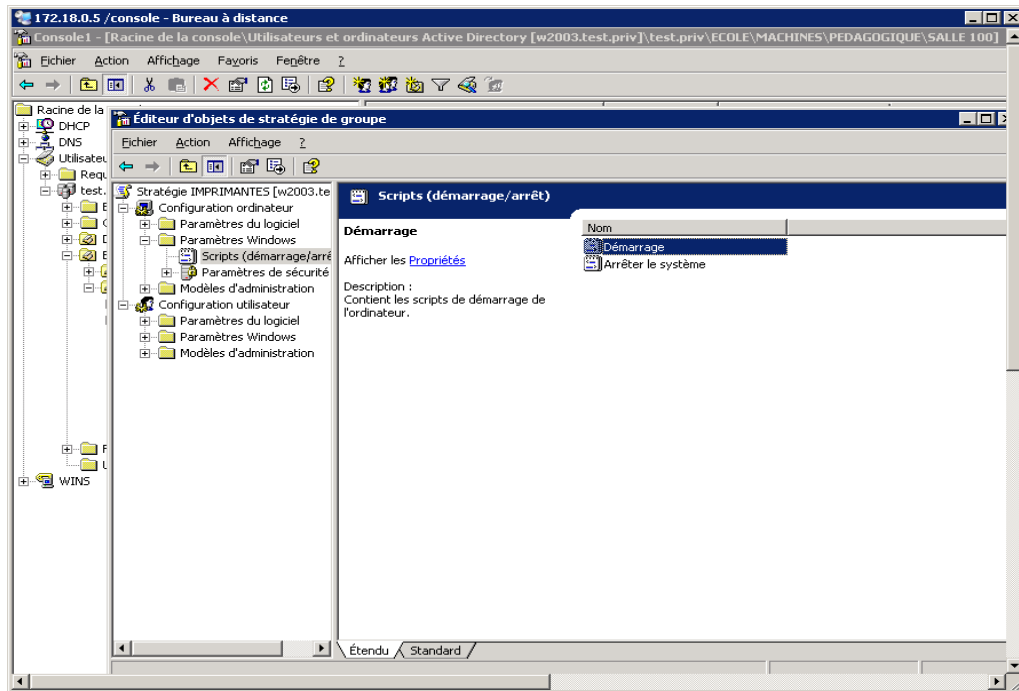
- installation des imprimantes réseaux

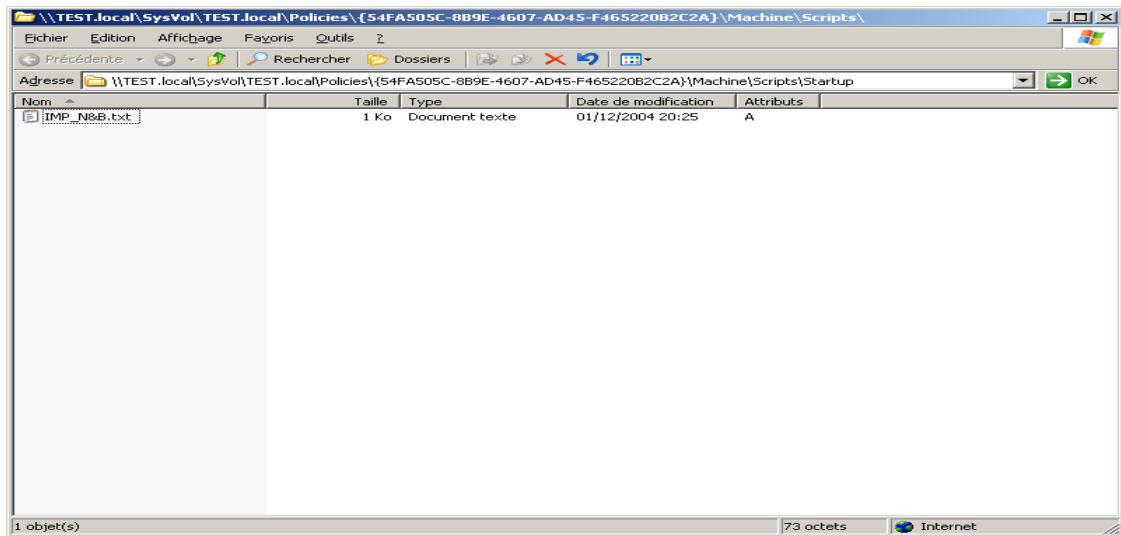
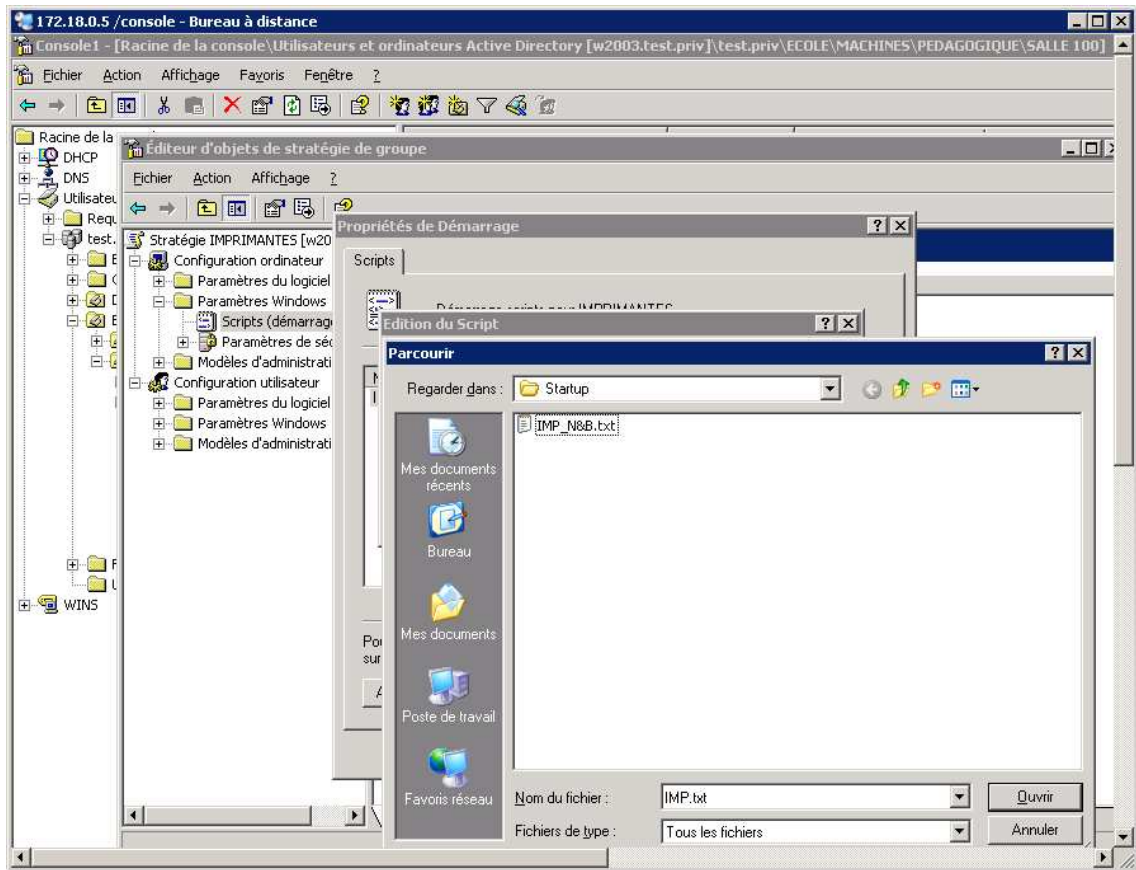
Il faut créer une stratégie de groupe nommé imprimante dans une OU

CONFIGURATION ORDINATEUR > PARAMETRE WINDOWS > SCRIPTS > DEMARRAGE



Le script qui va nous servir à installer les imprimantes doit être utilisé en fonction de la position géographique des PC et du nom des utilisateurs, il convient donc de le placer dans la partie script de démarrage de la machine (COMPUTER)



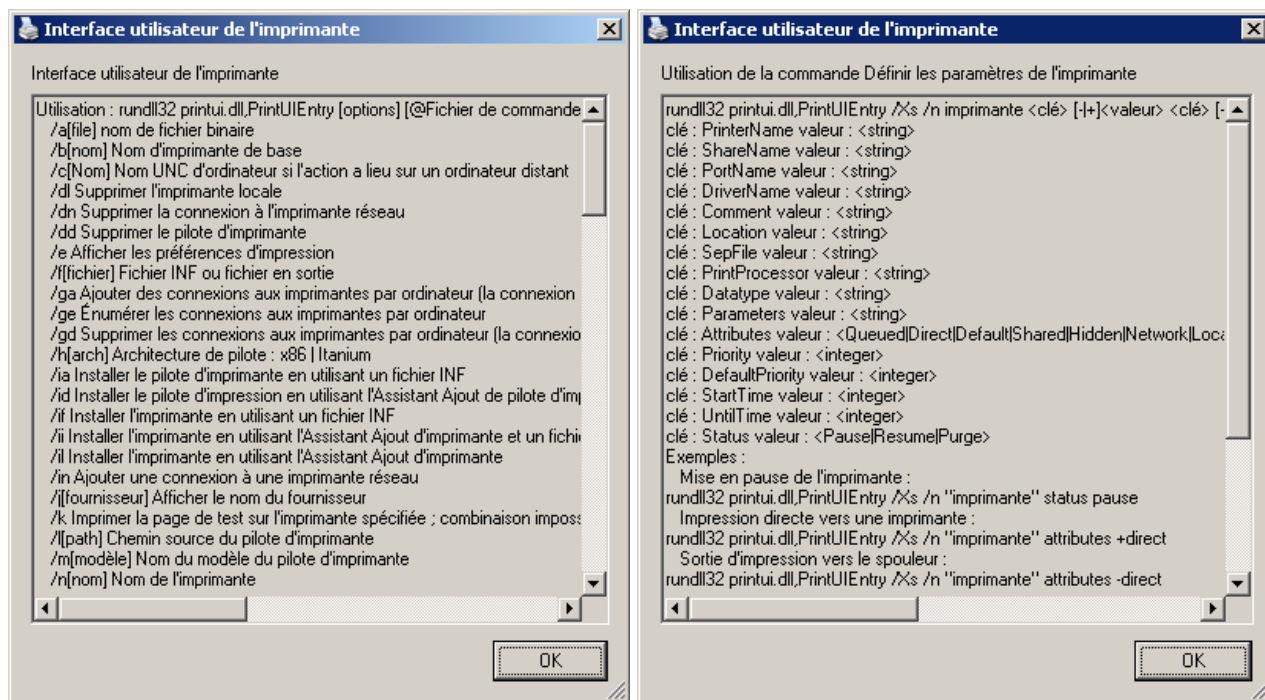


La commande utilisé est `rundll32 printui.dll,PrintUIEntry`

Pour plus d'info, faite `DEMARRER > EXECUTER > rundll32 printui.dll,PrintUIEntry /?`

Pour plus d'info, faite `DEMARRER > EXECUTER > rundll32 printui.dll,PrintUIEntry /Xs /n "printer" ?`

<http://support.microsoft.com/default.aspx?scid=kb;en-us;189105>



```

imp01.bat - Bloc-notes
Echier Edition Format Affichage ?
echo off
REM Installation automatique de l'imprimante IMP01
rundll32 printui.dll,PrintUIEntry /in /n "\\TEST\imp_509" /m "kyo509" /u
Ln 3, Col 49

```

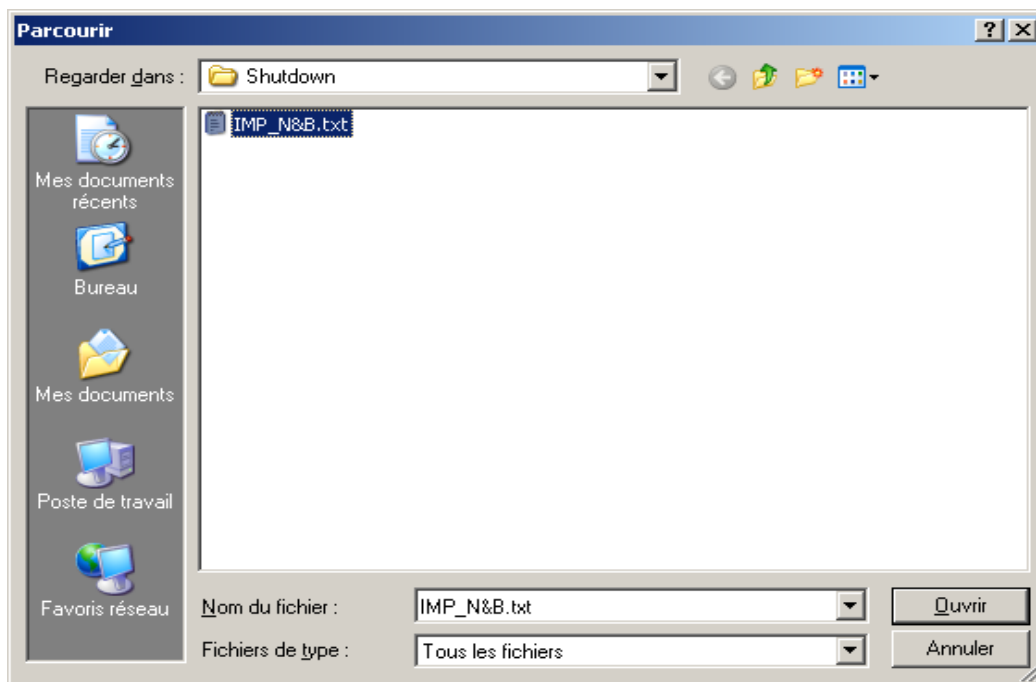
Un script similaire à quelques paramètres près permet de désinstaller les imprimantes après la déconnection.

Il est a placer dans la partie « Arrêter le système »

```

Del_Printer.bat - Bloc-notes
Echier Edition Format Affichage ?
rundll32 printui.dll,PrintUIEntry /dn
Ln 2, Col 1

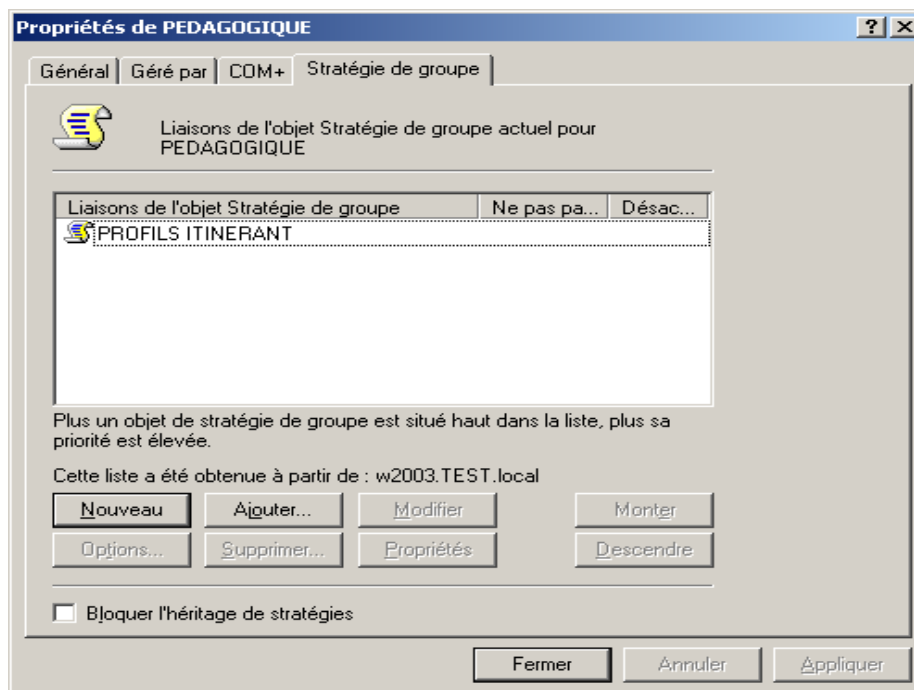
```

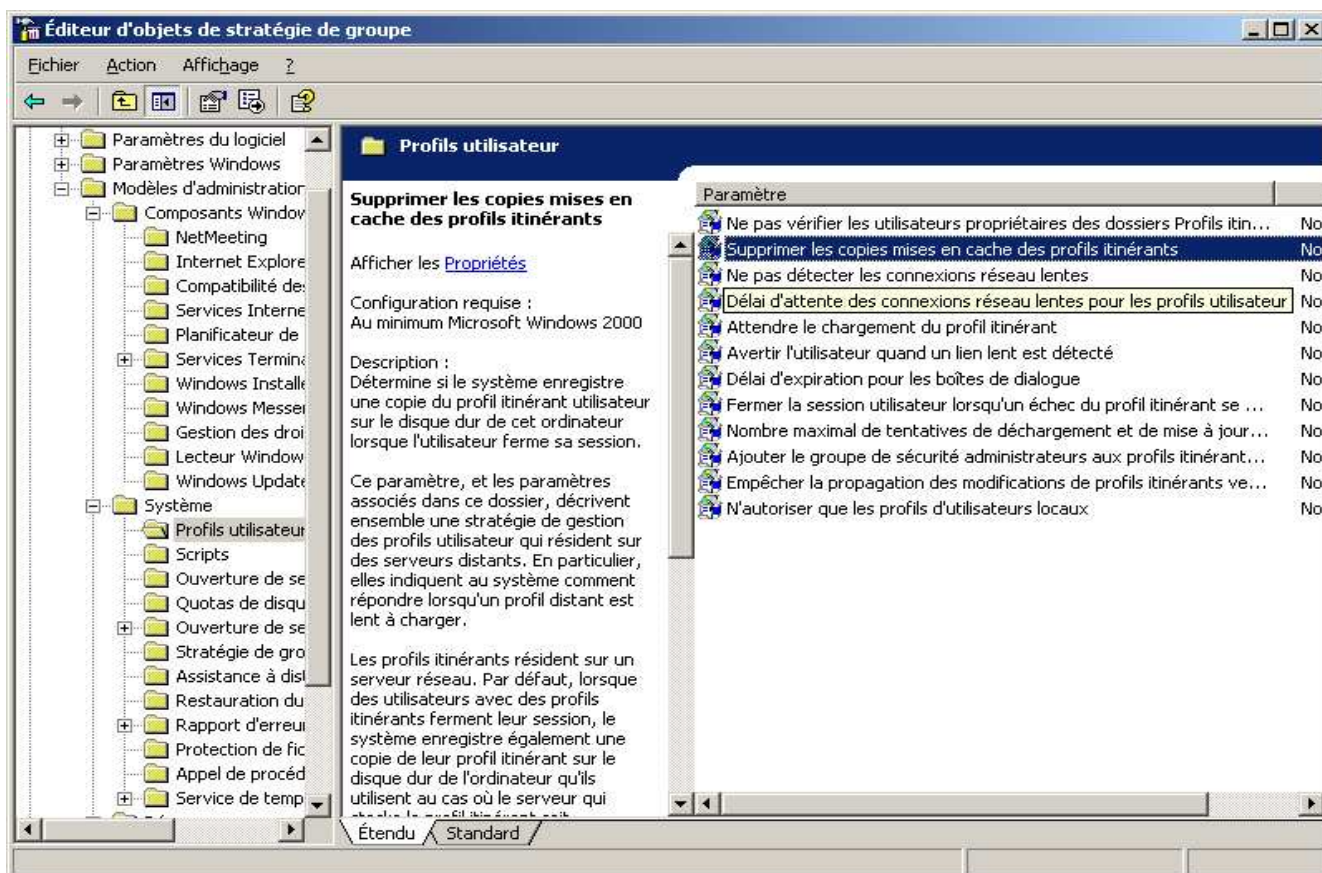
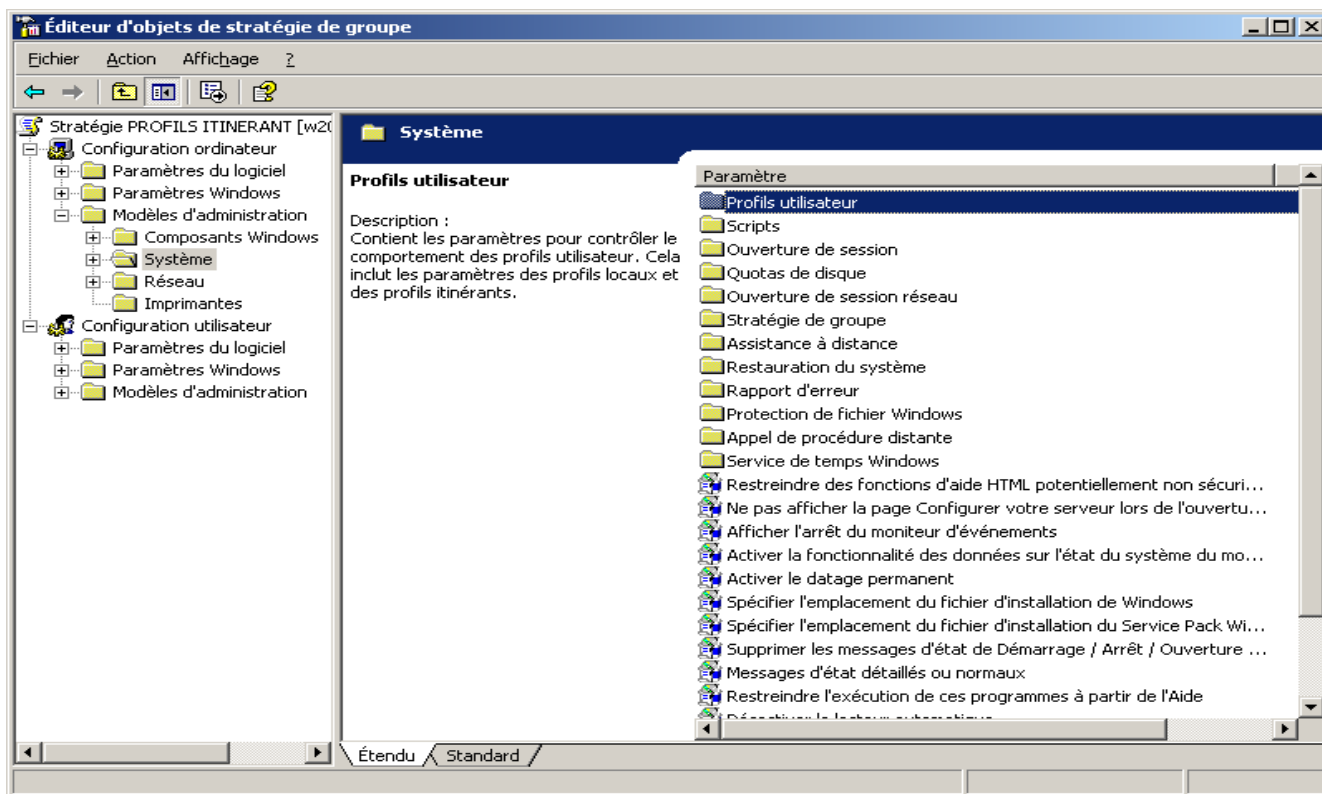


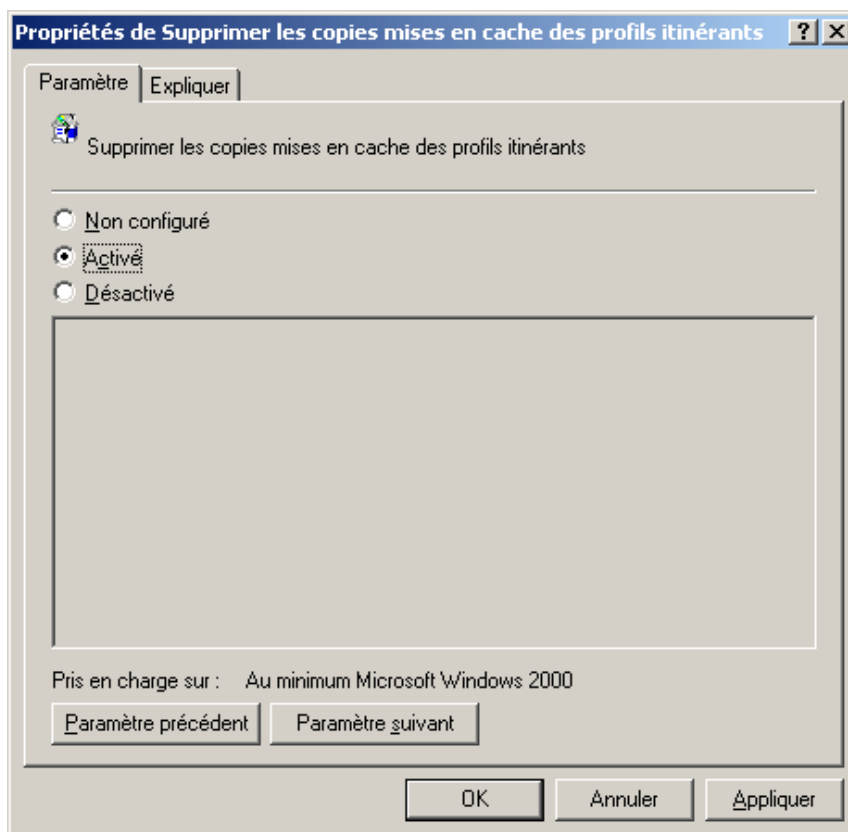
- suppression du profils local (cache)

Il faut créer une stratégie de groupe au niveau machine

CONFIGURATION ORDINATEUR > MODELES D'ADMINISTRATION > SYSTEME > PROFILS UTILISATEUR







Détermine si le système enregistre une copie du profil itinérant utilisateur sur le disque dur de cet ordinateur lorsque l'utilisateur ferme sa session.

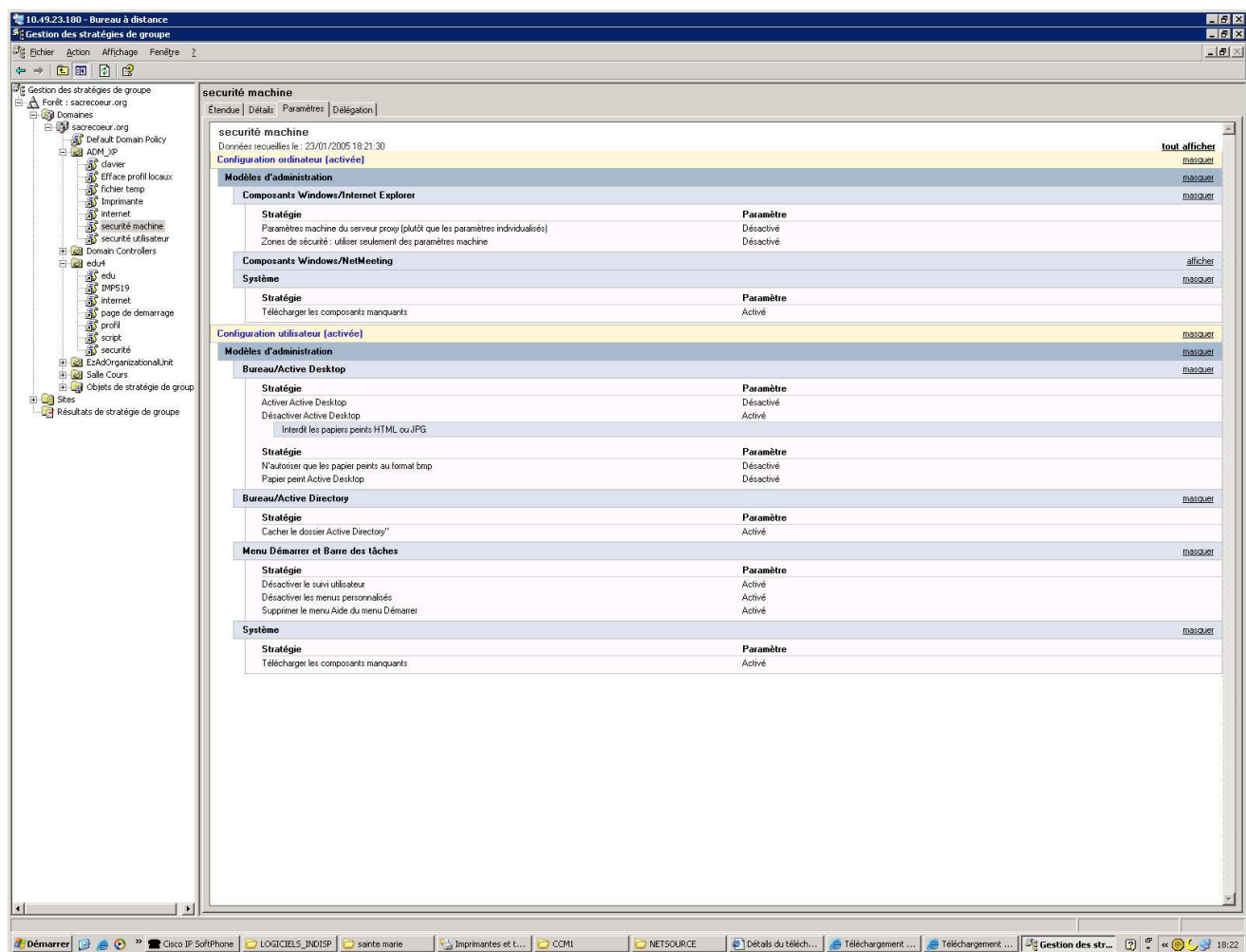
Ce paramètre, et les paramètres associés dans ce dossier, décrivent ensemble une stratégie de gestion des profils utilisateur qui résident sur des serveurs distants. En particulier, elles indiquent au système comment répondre lorsqu'un profil distant est lent à charger.

Les profils itinérants résident sur un serveur réseau. Par défaut, lorsque des utilisateurs avec des profils itinérants ferment leur session, le système enregistre également une copie de leur profil itinérant sur le disque dur de l'ordinateur qu'ils utilisent au cas où le serveur qui stocke le profil itinérant soit indisponible lors de l'ouverture de session suivante. La copie locale est également utilisée lorsque la copie distante du profil itinérant de l'utilisateur est lente à charger.

Si vous activez ce paramètre, toutes les copies du profil itinérant utilisateur sur cet ordinateur seront supprimées à la fermeture de session de l'utilisateur. Le profil itinérant est conservé sur le serveur réseau qui le stocke.

Important : n'activez pas ce paramètre si vous utilisez la fonction de détection des liens lents de Windows 2000 Professionnel et de Windows XP Professionnel. Pour répondre à un lien lent, l'ordinateur nécessite une copie locale du profil itinérant de l'utilisateur.

restriction poste client



Il est important de créer une structure pour gérer les stratégies de sécurités :

- Stratégie de sécurité du menu démarrer
- Stratégie de sécurité du Bureau
- Stratégie de sécurité du panneau de configuration

- Etc...

Il existe des restrictions incontournables

- Interdire la modification de l'affichage
- Interdire l'accès au panneau de configuration
- Interdire active-desktop
- Interdire changement de mot de passe
- Etc...

Poste client xp / 2000

configuration réseau (WINS, DNS, passerelle)

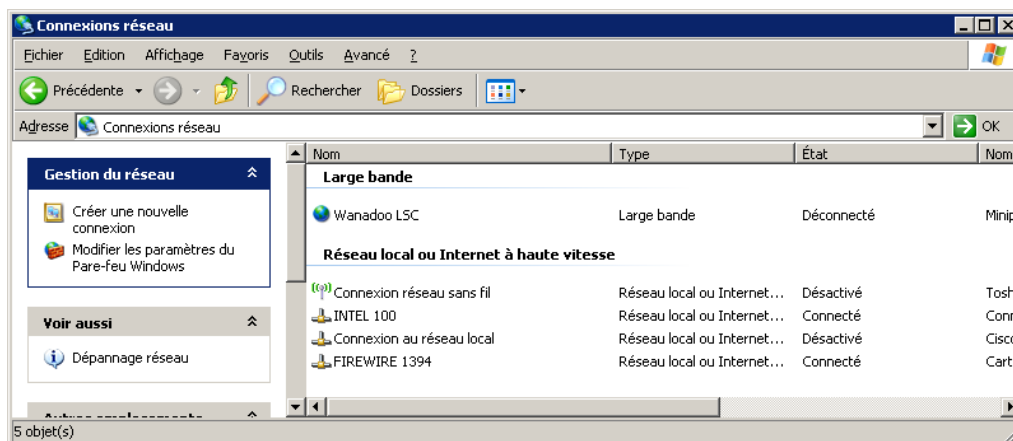
La configuration du réseau est importante pour faire entrer un poste dans le domaine :

- **La plage d'adresse IP** doit être compatible (IP et Masque de sous réseau)
- **La DNS** est primordiale : elle doit renseigner l'adresse IP du serveur et nom celle de **Wanadoo** ou de votre **Routeur** Internet (TEST.PRIV ou TEST.LOCAL sont des noms de domaine que Wanadoo ne sera pas renseigné, et donc échec assuré pour faire entrer un poste dans le domaine !!!)

Si vous modifier la DNS après avoir fait rentré un poste sur le domaine vous risquez certainement d'avoir des lenteurs à l'ouverture de session (il peut arriver que la durée dépasse 5 minutes !).

- **Le WINS** est important si vous utiliser des VLAN avec routage de niveau 3 ou un Routeur logiciel (IPCOP, ESMITH) pour passer un réseau à un autre (ADMINISTRATIF à PEDAGOGIQUE)
- **La passerelle** est importante si vous utiliser des VLAN avec routage de niveau 3 ou un Routeur logiciel (IPCOP, ESMITH) pour passer un réseau à un autre (ADMINISTRATIF à PEDAGOGIQUE) elle devra pointer sur le routeur niveau 3 ou le Routeur logiciel

Mise en œuvre : Lorsque le poste client est démarré, aller dans les connexions réseau et accès distant (Poste de travail/panneaux de configuration/connexions réseau et accès distant).



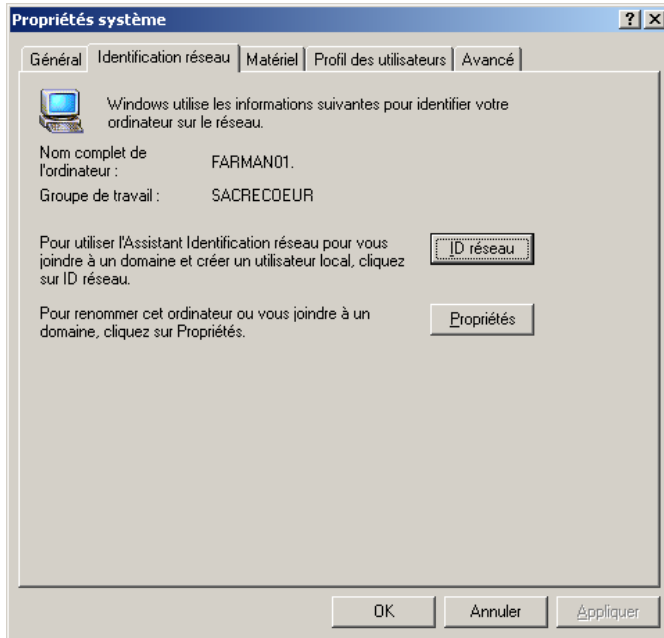
Cliquer sur Connexion au réseau local pour afficher une fenêtre



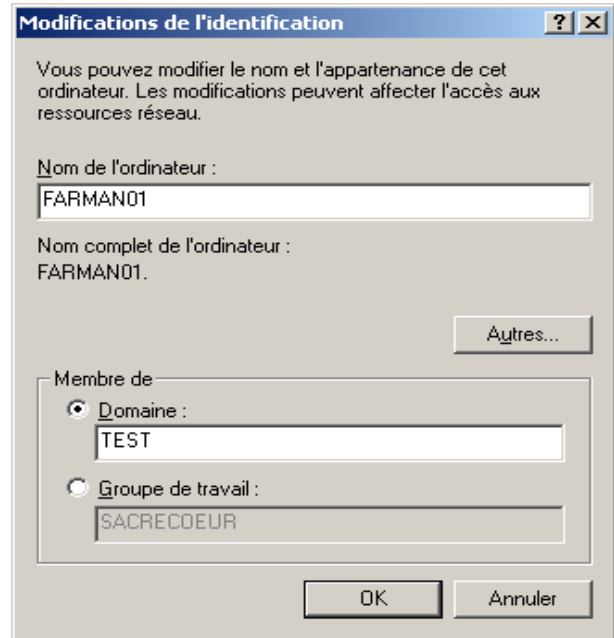
Aller ensuite dans les **propriétés** du **Protocoles Internet (TCP/IP)** pour ouvrir une nouvelle fenêtre.

Cocher « **Utiliser l'adresse IP suivante** » et indiquer toutes les adresses IP dans les champs proposés. Cliquer sur ok pour enregistrer les modifications

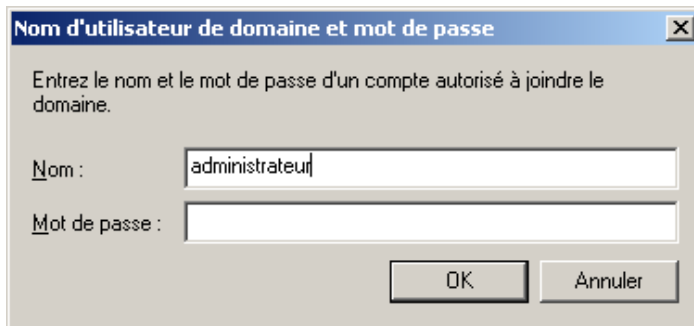
faire rentrer un poste xp / 2000 dans un domaine



Cliquez sur PROPRIETES

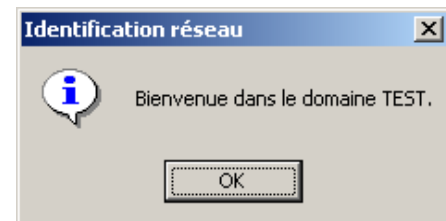


Membre de : indiquez le domaine (TEST, TEST.priv)

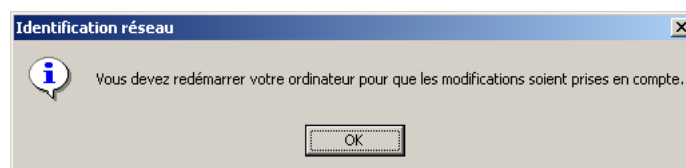


SEUL un compte administrateur peut autoriser cette action

Ne pas confondre "Administrateur" qui est le compte LOCAL pour la station avec "Administrateur" qui est le compte de l'administrateur sur le serveur



Voilà vous êtes dans le domaine TEST



Un redémarrage est nécessaire pour rentrer dans le domaine

création de profils itinérant, obligatoire, local

Profils

Les profils sont automatiquement activés sur les stations NTWS/W2KP/XP. Suivant le nombre d'utilisateurs susceptibles de venir sur les stations on pourra utiliser différentes solutions.

1) Solution avec peu d'utilisateurs (**profil Local**)

Si le nombre d'utilisateurs n'est pas important, la place occupée par ces profils restera acceptable.

On sera cependant certainement amené à supprimer de temps en temps les profils inutiles. Cette suppression se fera sur chaque station en tant qu'administrateur en utilisant "Panneau de configuration", "Système" et "Profils utilisateurs" (pour XP : "Panneau de configuration", "Système", "Avancé" et dans "Profils utilisateurs" utilisez "Paramètres").

2) Solution avec beaucoup d'utilisateurs, généralités. (**Profil itinérant**)

On utilise habituellement un profil itinérant obligatoire avec suppression des copies en cache des profils.

La solution habituelle consiste à placer le répertoire contenant le profil commun à tous les utilisateurs dans un répertoire partagé sur le serveur. Cette solution convient si votre réseau ne comporte que des NTWS ou que des 2000 pro ou que des XP pro (sachant que les Windows 9x n'utilisent habituellement pas les profils, le réseau peut en plus être composé de 95, 98 et ME sans que cela gêne).

Pourquoi ne pas mélanger les versions ?

Supposons pour simplifier que votre réseau contienne un NTWS et un XP et que le profil ait été créé à partir du XP (copie d'un profil utilisateur du XP vers le répertoire commun du serveur). Si l'utilisateur Dupond a un profil itinérant obligatoire, lorsque qu'il ouvre une session il reçoit le profil obligatoire. S'il ouvre la session sur le XP tout va bien mais s'il ouvre la session sur le NT4 beaucoup de fichiers et de clés de la base de registre ne conviennent pas.

Lenteur :

Lorsque tous les utilisateurs ouvrent une session à la même heure, le réseau est très sollicité car le profil commun est rapatrié sur toutes les stations en même temps.

Technique :

Créer un répertoire pour le profil

Créer un répertoire sur le serveur (par exemple C:\Profils)

Partagez ce répertoire avec par exemple Profils comme nom de partage. Mettez comme autorisations de partage :

Administrateurs : Contrôle total

Tout le monde : Lire

Vérifiez que les autorisations de sécurité possèdent au moins :

Administrateurs : Contrôle total

System : Contrôle total

Tout le monde : Modifier.

Si les autorisations de sécurité comportent la ligne "Tout le monde" avec "Contrôle total" cela convient. Dans ce cas, il est inutile d'ajouter d'autres lignes.

Créer un sous répertoire CommunXP.

Si le serveur s'appelle w2003 et si vous avez utilisé les répertoires proposés, le chemin d'accès du profil à partir des stations sera : <\\W2003\Profils\CommunXP>

Créer un UTILISATEUR « Modèle » qui n'a pas de profile

Créer le profil

Ouvrir une session sur une station en tant qu'utilisateur « Modèle » qui n'a pas de profil itinérant, le profil sera local et ne sera pas supprimé automatiquement.

Utilisez au moins une fois "Internet explorer", "Outlook Express", "Microsoft Word", StarOffice...
Fermez la session.

Ouvrez une session sur cette station avec le compte "Administrateur" du serveur. La fenêtre d'ouverture de session doit donc contenir "Administrateur", le mot de passe de l'administrateur du domaine et en troisième zone le nom du domaine. Dans "Panneau de configuration", "Système", "Avancé" et "Profils utilisateurs", placez-vous sur le profil utilisé précédemment (donc Modèle) et faites "Copier vers..."
Dans "Copier le profil vers", mettez le chemin d'accès du profil (\\W2003\Profils\CommunXP). Dans "Autorisé à utiliser", utilisez le bouton "Modifier" et tapez "Tout le monde" pour permettre au groupe "Tout le monde" d'utiliser ce profil. Effectuez la copie.

Rendre le profil obligatoire (Profil obligatoire)

Renommez le fichier ntuser.dat qui est dans \\w2003\Profils\CommunXP en le nommant exactement ntuser.man
Ne confondez pas avec le fichier texte ntuser.dat.txt qui peut éventuellement exister et qu'il est inutile de renommer.

LES UTILISATEURS ET LES DROITS

Privège/Groupe	Admin.	Utilisateur avec pouvoirs	Utilisateurs	Invités	Tout le monde	Admins du domaine
Ouvrir une session localement	X	X	X	X	X	X
Accéder à cet ordinateur à partir du réseau	X	X	X	X	X	X
Arrêter le système	X	X	X	X	X	X
Changer l'heure du système	X	X	-	-	-	X
Forcer l'arrêt à partir d'un système distant	X	X	-	-	-	X
Sauvegarder et restaurer des fichiers et des répertoires	X	-	-	-	-	X
Charger et décharger des pilotes de périphérique	X	-	-	-	-	X
Ajouter des stations de travail à un domaine	-	-	-	-	-	X
Créer et gérer des comptes d'utilisateur	X	X	-	-	-	X
Créer et gérer des groupes locaux	X	X	-	-	-	X
Gérer l'audit des événements système	X	-	-	-	-	X
Assigner des droits aux utilisateurs	X	-	-	-	-	X
Formater le disque dur de l'ordinateur	X	X	-	-	-	X
Créer des groupes communs	X	X	-	-	-	X
Partager et cesser de partager des répertoires	X	X	-	-	-	X
Partager et cesser de partager des imprimantes	X	X	-	-	-	X



Sauvegarde client et serveur

- robocopy
- cobian
- xcopy32
- ghost / drive image

WINDOWS 2003 Server innove en terme de sauvegarde de fichier en utilisant la technologie des **clichés instantanés**

<http://www.microsoft.com/france/entrepreneur/solutions/sgc/articles/ntbackup.msp#EEAA>

ROBOCOPY (copie et synchro de fichiers très évoluée Res. Kit)

Intérêt

Permet de synchroniser en ligne de commande les contenus de deux répertoires (ou arborescences). c'est donc utilisable dans des tâches planifiées (commande at de Windows NT/2000 ou gestionnaire de tâches de Windows 2000).

Syntaxe

robocopy repertoire_source repertoire_destination [fichier ou masque de fichiers à copier] [options]

Pour obtenir la syntaxe de base :

robocopy /?

Pour plus d'options :

[robocopy /???](#)

Sinon, se référer au manuel qui contient une abondante documentation.

Quelques options parmi les plus utiles

Options les plus utiles	Rôle
/E	Traiter les sous-répertoires même vide
/R:0 (ou autre valeur faible)	Eviter les ré-essais sur les fichiers ou répertoires dont les accès sont bloqués. Attention méfiance ! Quand vous utilisez l'option de test ("/L") les fichiers bloqués ne stoppent pas le traitement, mais quand vous voulez passer à l'action ils deviennent bloquants. En effet la valeur par défaut du nombre de tentatives est de 1000000 ("/R:1000000") et le temps entre deux tentatives à comme valeur par défaut 30 ("/W:30"). Autant dire que c'est carrément bloquant !
/W:5	Si vous avez choisi /R:n avec n différent de 0, alors choisissez une valeur faible pour ce paramètre qui définit le temps d'attente entre deux tentatives.
/XO	Les fichiers plus vieux sur la source que sur la destination sont exclus du traitement (ils ne sont pas recopiés).
/SEC	Copie les infos de sécurité

/MIR	Equivalent à /E /PURGE. Permet d'effectuer un véritable mirroring entre deux arborescences, allant jusqu'à supprimer de la destination les fichiers disparus de la source. A l'issu de l'opération, les deux arborescence seront strictement semblables, à moins, peut-être, que l'on ait spécifié des exclusions (ce dernier point à vérifier quand même).
/LOG:chemin_fichier	Permet d'enregistrer un journal des répertoires traités et des actions effectuées.
/LOG+:chemin_fichier	Idem ci-dessus mais ajoute à la fin du fichier journal au lieu de l'écraser.
/L	Pour simuler, seulement, et prendre la mesure des changements à effectuer. N'effectue aucune action sur les fichiers. Permet quand même d'enregistrer le journal des actions. Attention méfiance ! Quand vous utilisez l'option de test ("/L") les fichiers bloqués ne stoppent pas le traitement, mais quand vous voulez passer à l'action ils deviennent bloquants. En effet la valeur par défaut du nombre de tentatives est de 1000000 ("/R:1000000") et le temps entre deux tentatives à comme valeur par défaut 30 ("/W:30"). Autant dire que c'est carrément bloquant !

Il existe une version graphique : **Robocopy Wizard**

http://www.opaleds.com/products/robocopy_wizard.html#d

Version 1.0.1.7 - 29 octobre, 2004

Robocopy Wizard (ex: Robocopy Assistant) est une interface graphique permettant d'utiliser l'utilitaire Microsoft Robocopy provenant des ressources kit NT, 2000, et Serveur 2003.

Cet utilitaire console puissant est très largement utilisé dans les entreprises, il a la particularité d'effectuer des reprises de transfert après un problème ou une coupure réseau.

Sous forme d'un assistant pas à pas, Robocopy Wizard permet de s'affranchir des lignes de commandes.

Très simple d'utilisation, il offre une interface moderne, simple et fonctionnelle.

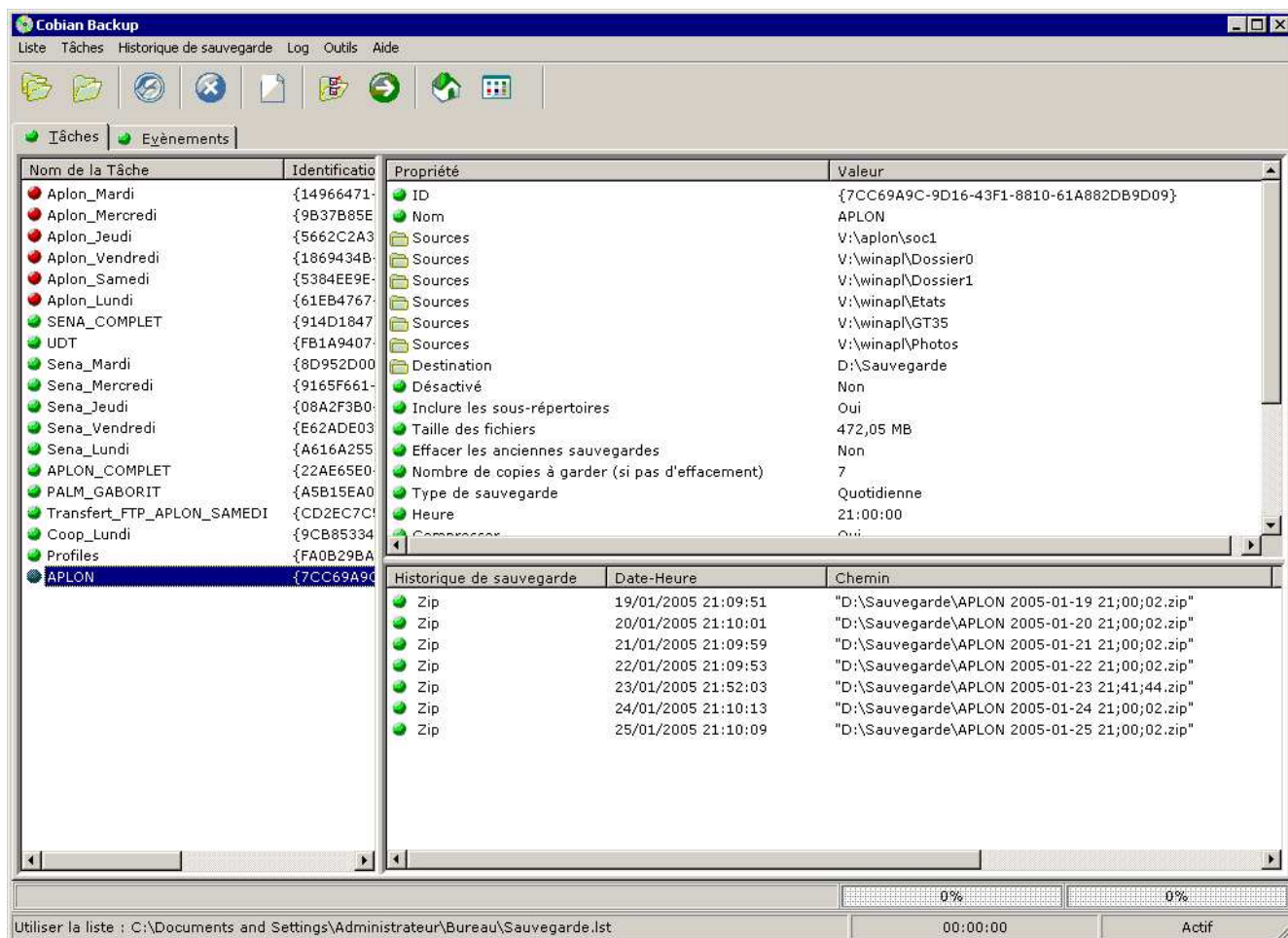
Cette version s'appuie désormais sur Robocopy Version XP010 issu du ressource kit server 2003 de Microsoft.

cobian

Cobian Backup est, comme son nom l'indique, un logiciel de sauvegarde. L'interface, assez classique pour un logiciel de ce genre, affiche la liste des plans de sauvegarde dans un tableau récapitulatif avec leur nom, les répertoires source et destination ainsi que la fréquence et la taille des sauvegardes.

La sauvegarde peut se faire dans un répertoire local ou bien à distance (par l'intermédiaire du client FTP inclus). Les options relatives à chaque sauvegarde sont nombreuses et claires (compression, sauvegarde incrémentale, récursivité dans les répertoires, exclusions par masque, lancement de programmes avant et après le backup...).

A noter que le logiciel comprend une option de mise à jour par Internet et que le passage en version française se fait par l'intermédiaire du menu Tools/Options(c'est l'anglais qui est installé par défaut).



Il est très pratique pour la sauvegarde d'APLON, de BCDI, des PROFILS sur 7 jours (ou plus)

xcopy32

Commande externe. Fonctionne sur la ligne de commande ou dans un batch. Uniquement sur windows 9x

Copie les fichiers et répertoires du disque.

Syntaxe

XCOPY source [destination] [/A | /M] [/D[:date]] [/P] [/S [/E]] [/W] [/C] [/I] [/Q] [/F] [/L] [/H] [/R] [/T] [/U] [/K] [/N]

Parametres

source Fichiers a copier.

destination Emplacement ou nom de fichiers.

/A Copie les fichiers avec l'attribut archive, ne modifie pas l'attribut.

/M Copie les fichiers avec l'attribut archive,desactive l'attribut archive.

/D:date Copie les fichiers modifies a la date ou apres la date donnee. Sans date specifiee, copie que les fichiers dont l'heure source est anterieure a l'heure destination.

/P Avertit avant de créer chaque fichier destination.

/S Copie les répertoires et sous-répertoires non vides.

/E Copie tous les répertoires et sous-répertoires. Identique a /S /E. A utiliser pour modifier /T.

/W Demande d'appuyer sur une touche avant la copie.

/C Continue la copie meme en cas d'erreurs.

/I Si la destination n'existe pas lors de la copie des fichiers, suppose que la destination est un repertoire.

/Q N'affiche pas le nom des fichiers lors de la copie.

/F Affiche les noms complets de la source et de la destination.

/L Affiche les fichiers qui sont copies.

/H Copie aussi les fichiers systeme et caches.

/R Ecrase les fichiers en lecture seule.

/T Cree une arborescence sans copier les fichiers. N'inclut pas les répertoires et sous-répertoires vides. /T /E inclus les répertoires et sous-répertoires vides.

/U Met a jour les fichiers dans destination.

/K Copie attributs. Normal Xcopy efface attributs lecture seule.

/Y Ecrase les fichiers sans avertir.

/-Y Avertit avant l'ecrasement des fichiers.

/N Copie avec les noms courts (moins de 9 caracteres) generes.

Il existe une version graphique WinXcopy qui fonctionne sur windows 2000 /XP

<http://www.ubiq.be/freeware/winxcopy/winxcopy.html>

ghost / DRIVE IMAGE

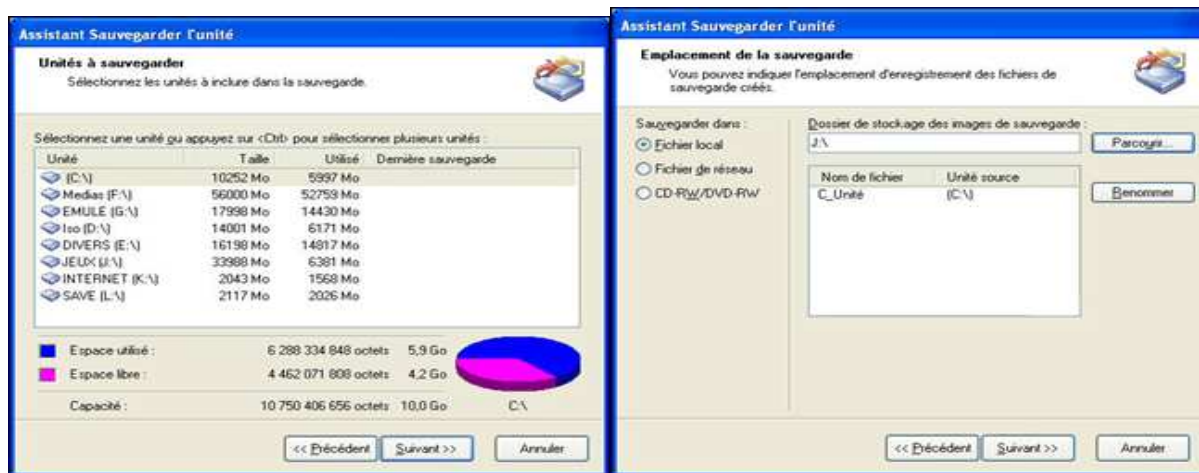
Un seul et même produit puisque Symantec à racheter Powerquest

Norton Ghost 9 sait tout faire : il peut placer les images des disques sur tous les supports possibles, et il sait gérer les planifications des sauvegardes incrémentielles, ce que ses concurrents ne savent pas tous faire. Il dispose également de Backup Image Browser, un utilitaire dédié au parcours des images créées. Ce dernier n'autorise toutefois que la visualisation ou la restauration de fichiers vers leur emplacement d'origine. Il est donc impossible de prélever directement un fichier.

Sauvegarde d'unités

Cette fonctionnalité permet donc de sauvegarder l'intégralité d'une partition. Il peut s'agir de n'importe quelle partition, y compris la C:\ et la manipulation se fait directement depuis Windows. Il n'est donc pas nécessaire, comme avec les anciennes versions, de redémarrer sous DOS. Avec cette méthode, il n'est cependant pas possible de sauvegarder un disque entier avec son architecture. Il faut entendre par là que vous ne pouvez pas faire en sorte de sauvegarder votre disque primaire, par exemple, avec toute l'architecture de partitions qu'il comporte. Cependant vous pouvez effectuer la sauvegarde de toutes les partitions d'un seul coup, à l'aide d'une sélection multiple. Ainsi vous aurez une archive pour chaque partition.

Là où cela devient intéressant c'est sur la possibilité de sauvegarder directement sur un CD ou un DVD. Il s'agit d'une fonctionnalité utile car cela vous procure un gain de temps assez appréciable si vous désirez par la suite garder les images sur médias amovibles. Une autre possibilité est celle de sauvegarder vos fichiers sur le réseau.



Cliquez pour agrandir

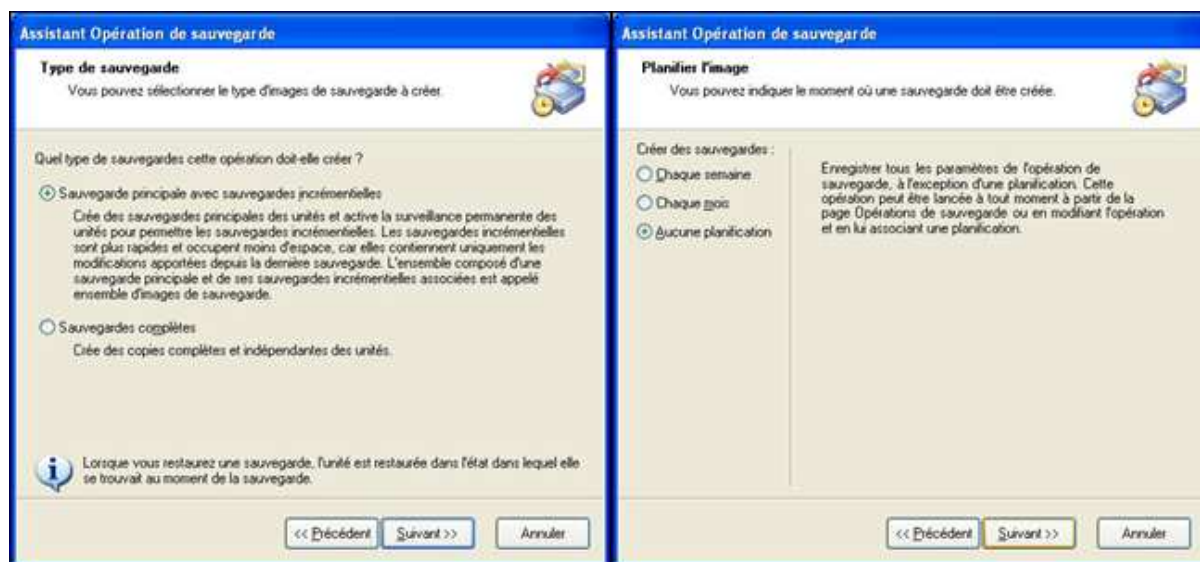
Quatre modes de compression sont proposés : Aucun, Standard, Moyen et Elevé. Bien entendu plus le mode de compression est élevé, plus de temps prendra l'opération. Suivant la taille de la partition il sera donc plus ou moins propice de choisir une compression importante ou non. Petite fonctionnalité assez sympathique : la possibilité de fractionner les images en X Mo. Ainsi si vous désirez graver votre image sur CD ou DVD, cela sera bien plus pratique. Bien entendu il est aussi possible de protéger les archives en les dotant d'un mot de passe. Pour information il nous aura fallu environ 15 minutes afin de sauvegarder notre partition C:\ de 8 Go. Opération effectuée en continuant de surfer sur Internet, preuve que la sauvegarde à chaud est d'une réelle efficacité.



Cliquez pour agrandir

Planification de sauvegardes incrémentales

Comme son nom l'indique, cette option sert à effectuer des sauvegardes incrémentales de manière planifiée. Ainsi Ghost sauvegardera la partition désirée à un moment que vous aurez prédéfini. Mais le détail c'est qu'il ne va pas "bêtement" sauvegarder l'intégralité de votre partition et remplacer l'archive précédente. Effectivement Ghost va uniquement sauvegarder les fichiers qui ont été modifiés / ajoutés / supprimés et les implémenter dans une autre archive, ce qui permet de gagner un temps énorme. C'est ainsi un "groupe d'images" qui est créé et ce de manière totalement transparente. Le choix au niveau des sauvegardes est très vaste, ce qui représente un bon point afin de faire des sauvegardes à des moments où le poste n'est pas utilisé.

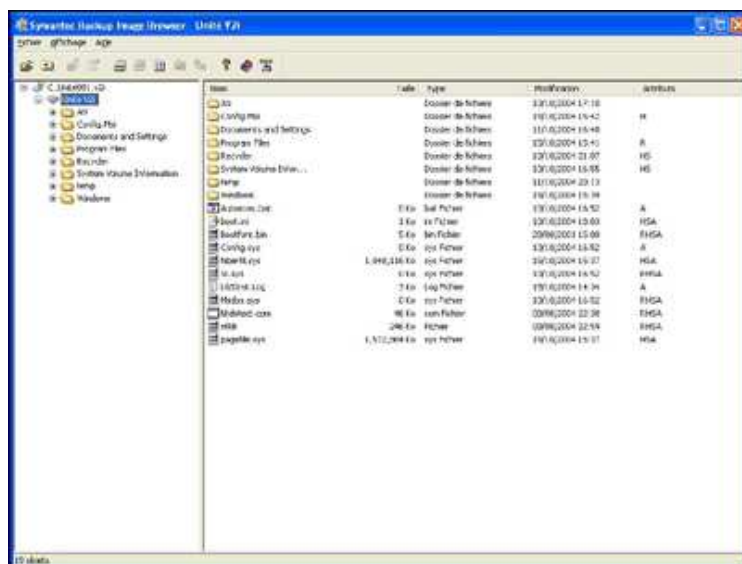


Les tâches de restauration

Maintenant que les diverses fonctions de sauvegarde ont été passées en revue, nous allons nous pencher sur les méthodes de restauration que propose Norton Ghost. Il existe deux méthodes différentes : la restauration d'unité et la restauration de fichiers ou dossiers. C'est sur cette dernière que nous allons nous pencher dans un premier temps.

Restaurer des fichiers ou des dossiers.

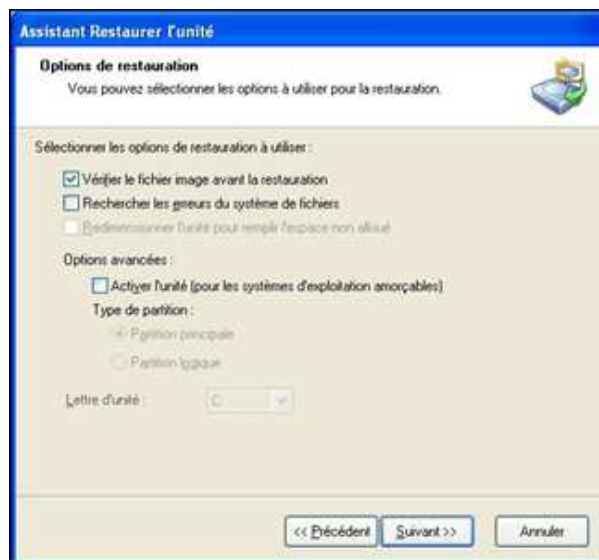
Cette fonction permet de restaurer uniquement, comme son nom l'indique, des fichiers ou des dossiers. Très utile donc si par mégarde vous avez supprimé quelque chose que vous ne vouliez pas. En cliquant sur le bouton c'est tout simplement Symantec Backup Image Browser qui s'ouvre. Cet utilitaire, présent avec toutes les versions de Ghost permet justement d'ouvrir les archives créées lors des sauvegardes. Inutile donc de passer par le centre de commande de Ghost, car si vous double cliquez sur une archive, le Backup Image Browser se lancera automatiquement.



Cliquez pour agrandir

Restaurer une unité

Cette méthode de restauration est celle qui va remettre en place l'intégralité de votre partition. Lorsque vous utilisez cette fonction, votre partition sera écrasée et les fichiers contenus dans l'archive seront mis à la place. C'est cette fonction qui ravit les personnes dont la machine fonctionne de manière aléatoire. Par contre cela peut s'avérer assez traître dans le sens où si vous aviez des documents importants présents sur la partition et qui n'ont pas été sauvegardés lors de la création de l'archive, ni même lors de la création de l'archive incrémentale, ces fichiers seront tout simplement perdus.

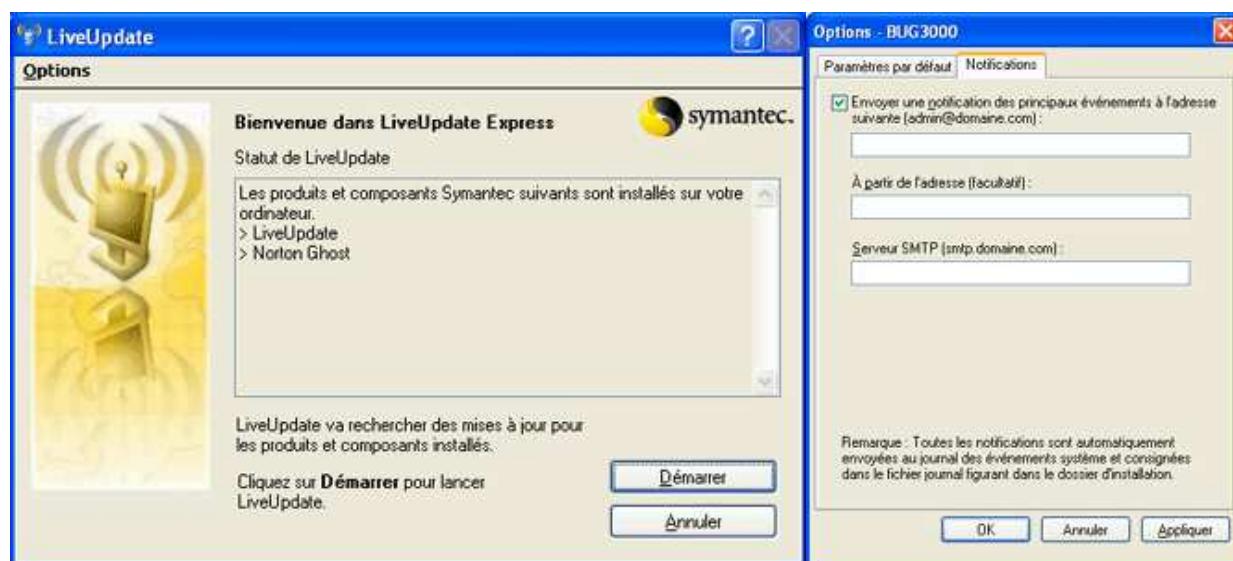


Fonctionnalités annexes

Pour ce qui est des petites fonctionnalités annexes, rien de bien surprenant, ni de bien fondamental. Bien entendu LiveUpdate, le logiciel de mise à jour de Symantec, est au rendez-vous et vous permettra de maintenir à jour votre Norton Ghost 9.0 et ce, de façon totalement automatique, lorsque l'ordinateur est connecté à Internet.

Dans la partie avancée, vous disposez d'un historique des sauvegardes afin de voir si vos incréments s'exécutent sans problème. En cas de problème justement, vous pouvez compter sur un journal des événements, toujours disponible en mode avancé. Pour en finir avec ce mode, les opérations de sauvegardes programmées sont présentes dans un onglet prévu à cet effet et permettant de les modifier à souhait.

Dans les options, rien de réglable, si ce n'est la possibilité d'envoyer par mail les principaux événements. Fonction réservée à une clientèle un peu plus professionnelle, il est vrai.



CD-Rom Bootable

Le CD-Rom d'installation est bootable. Ainsi vous pouvez procéder uniquement à la restauration de vos images. Fonction très importante pour les utilisateurs dont la machine ne daigne plus redémarrer. Une fonction anti-virus est aussi présente, cependant il faudra disposer des dernières mises à jours de celui-ci quelque part sur disquette, CD/DVD ou sur le disque dur.

Petit bémol cependant : la nécessité d'avoir de bonnes ressources systèmes, car le service utilise toute de même pas loin de 20mo ! Ceci peut s'avérer contraignant pour les machines disposant de peu de mémoire vive. D'autant plus que lors d'archivage, la machine est relativement ralentie. Inutile donc d'essayer de jouer à votre FPS favori tout en sauvegardant une partition. Mais ceci n'enlève rien à l'utilité d'un tel logiciel pour les personnes gérant des parcs informatiques, si l'on se cantonne à la clientèle professionnelle, ou pour les particuliers souhaitant sauvegarder leurs données ou ceux installant/désinstallant des logiciels qui pourraient un jour les amener à réinstaller Windows... Avec un logiciel comme Ghost, nul besoin de tout réinstaller, il suffira en effet de restaurer une image préalablement créée.

SYNCHROPARC

<http://crdp.ac-reims.fr/synchroparc/>

SynchroParcXP permet de sauvegarder un ensemble d'ordinateurs sur le disque dur d'un ordinateur du réseau. Chaque sauvegarde est composée d'un fichier (extension ASB) contenant la liste des fichiers sauvegardés et l'endroit (dans le répertoire DATAXP) où chaque fichier est sauvegardé. Avec cette technique, un même fichier appartenant à plusieurs ordinateurs n'est sauvegardé qu'une fois, d'où un gain de temps et de place.

Depuis la version 1.01 de SynchroParcXP, il est possible de créer des sauvegardes multi-ordinateurs (clonage).

SynchroParcXP permet de restaurer les ordinateurs dans l'état exact où ils étaient lors de la sauvegarde. Toute modification faite depuis la sauvegarde est oubliée. Les fichiers qui ont été supprimés sont remplacés, les fichiers qui ont été modifiés sont restaurés, les fichiers qui ont été ajoutés sont supprimés.

SynchroParcXP permet également une restauration partielle bien utile si on vient de supprimer un fichier ou un répertoire par erreur et que l'on souhaite seulement restaurer ce fichier ou ce répertoire. Cette restauration partielle ne supprime pas de fichiers.

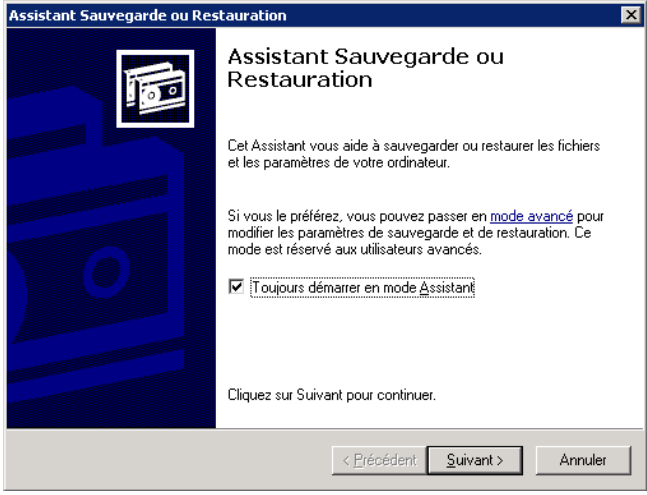
Remarque : La comparaison de deux fichiers se fait en comparant le nom, le répertoire, la taille et la date à la seconde près. Il est donc théoriquement possible que deux fichiers soient différents et considérés comme identiques par SynchroParcXP, mais la probabilité est tellement faible qu'en pratique elle peut être considérée comme nulle. En effet, dès qu'un fichier est modifié, sa taille a de grandes chances de changer et la date change pour indiquer le moment précis de l'enregistrement.

La documentation complète sur le site :

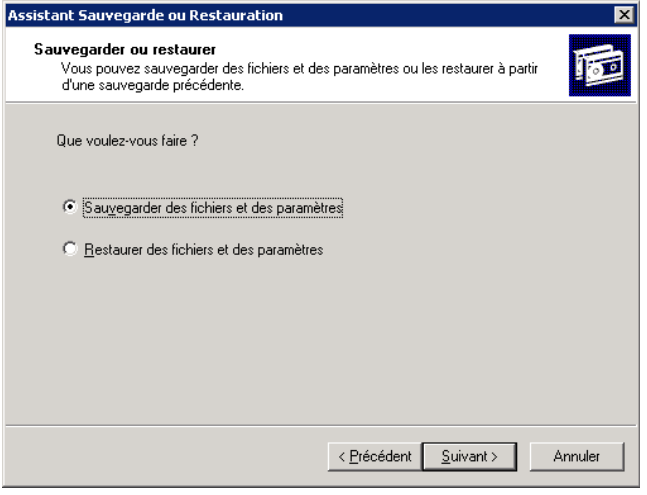
<http://crdp.ac-reims.fr/synchroparc/docxp.htm>

L'UTILITAIRE DE SAUVEGARDE MICROSOFT

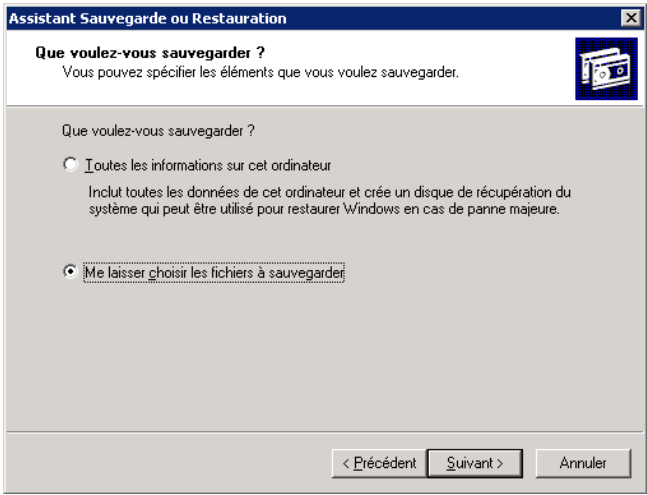
L'utilitaire est basic mais pourra être fort utile pour sauvegarder la totalité du system sur bande ou simplement le contenu de l'AD (Active directory)



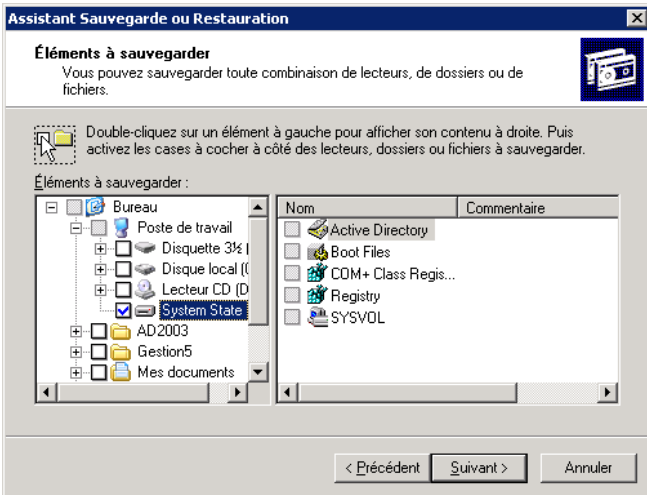
Utiliser l'assistant si vous n'êtes pas sur de vous



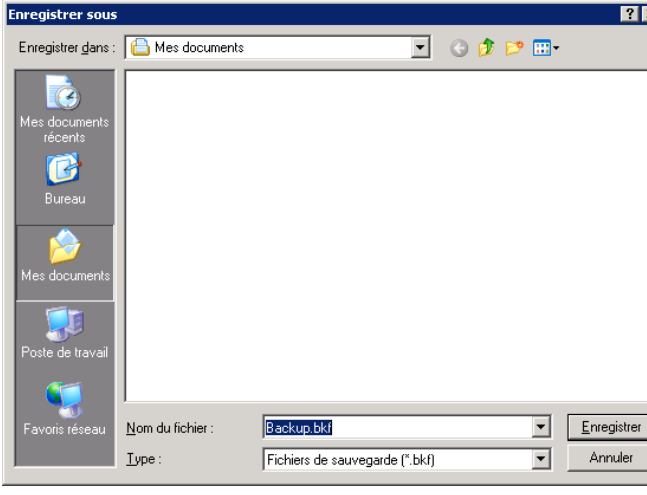
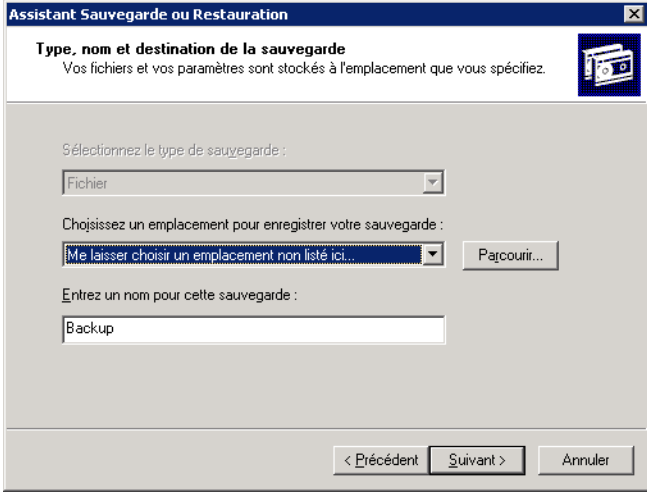
Cliquez sur sauvegarder et suivant



La première étape est de sauvegarder l'AD, donc je choisis « Me laisser choisir les fich... »



Le système contient : l'AD, Boot files, la base de registre et le SYSVOL



Je choisis un lieu de stockage: bande ou disque dur et je fais enregistrer

OUTILS DIVERS

SUPEREXEC

<http://www.bellamyjc.net/fr/superexec.html>

Cet outil permet l'Exécution d'applications sous un compte administrateur (GRATUIT)

Le site est assez extraordinaire par son contenu !

REMOTEXEC

<http://www.isdecisions.com/index.cfm?p=products-remotexec>

Cet outil permet l'exécution d'un programme (Mise à jour Windows, fichier REG, fichier MSI, etc...) sur plusieurs PC simultanément et avec les droits administrateurs (PAYANT MAIS VERSION ILLIMITE 10 POSTES)

Security Explorer 4

<http://www.scriptlogic.com/>

La demo est visible à cette adresse : http://www.scriptlogic.com/eng/products/productdemos/Security_Explorer_Webinar_09222004.asx

Cet outil permet une gestion plus fine des droits, des partages de Windows 2000 /2003 serveur

Il permet aussi de sauvegarder les sécurités et les partages, de cloner les droits d'un dossier pour mettre sur un autre etc...

Adminscripteditor

<http://www.adminscripteditor.com/main.asp>

Un site consacré au script (Bach, kix, vb etc...) !!!! INCONTOURNABLE !!!!

ASTASE

www.astase.com

Une suite de logiciel gratuit pour la sauvegarde, la sécurité, le développement, le multimédia

!!! INCONTOURNABLE !!!

