

# Réseau avec Windows 2000 ou 2003 serveur

*Ce document fait référence à Windows 2000. Sauf précision contraire, tout convient également pour Windows 2003.*

## Utilisation de Windows

### Aide

Avec l'aide de Windows 2000 ("Démarrer", "Aide") vous pouvez, en tapant un ou deux mots, obtenir des explications pas toujours simples mais souvent pertinentes.

Essayez par exemple les mots

"imprimante"

partition fat32

### Différentes versions de Windows

Versions de Windows	Type	Partitions utilisables
3.0, 3.1, 3.11	Client	Fat 16
3.51	Serveur	Fat 16 et NTFS
95	Client	Fat 16
95 Osr2, 98, 98SE, ME	Client	Fat 16 et Fat 32
NT4 WorkStation	Client	Fat 16 et NTFS
NT4 Serveur	Serveur	Fat 16 et NTFS
2000 Pro	Client	Fat 16, Fat 32, NTFS
2000 Serveur	Serveur	Fat 16, Fat 32, NTFS
XP Home édition		Fat 16, Fat 32, NTFS
XP Pro	Client	Fat 16, Fat 32, NTFS
2003 Serveur	Serveur	Fat 16, Fat 32, NTFS

## Microsoft Management Console

Lorsque vous appelez les outils d'administration, vous retrouvez toujours une présentation semblable. Les outils d'administration correspondent à des fichiers ayant pour extension .msc. Ces fichiers sont appelés par le programme MMC.EXE (Microsoft Management Console).

Le programme MMC.EXE et les fichiers msc se trouvent dans \windows\System32 ou \Windows\System32.

Par exemple "Démarrer", "Programmes", "Outils d'administration" et "Observateur d'événements" revient au même que d'appeler le programme MMC avec comme paramètre c:\winnt\system32\eventvwr.msc. On peut même se contenter d'un double clic sur eventvwr.msc.

De même l'outil "Gestion de l'ordinateur" correspond à MMC.EXE avec comme paramètre compmgmt.msc. Le "Gestionnaire de périphériques" peut être appelé par "devmgmt.msc". Etc.

## Gestionnaire de périphériques

Dans les "Outils d'administration", ouvrez "Gestion de l'ordinateur". Dans les "Outils système", vous trouvez "Gestionnaire de périphériques".

Vous pouvez comme avec Windows 9x, désinstaller un périphérique, vous pouvez également le désactiver, mettre à jour les pilotes...

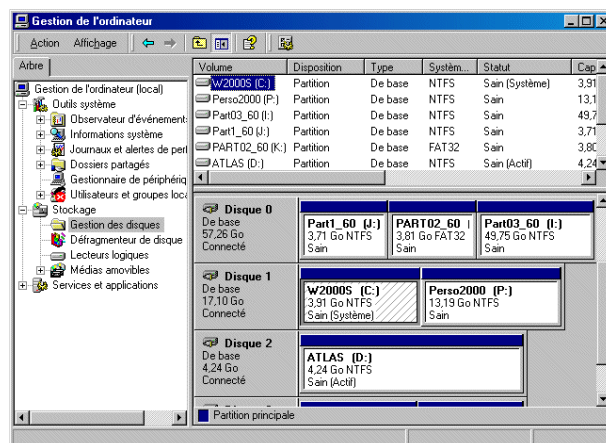
Vous pouvez également obtenir des informations très complètes sur le système en allant dans les "Outils système" et "Information système".

## Gestion des disques durs

Vous venez d'installer Windows (2000, XP ou 2003) dans une partition de 20 ou 30 Go. Il reste une place inutilisée (non alloué) sur le disque dur.

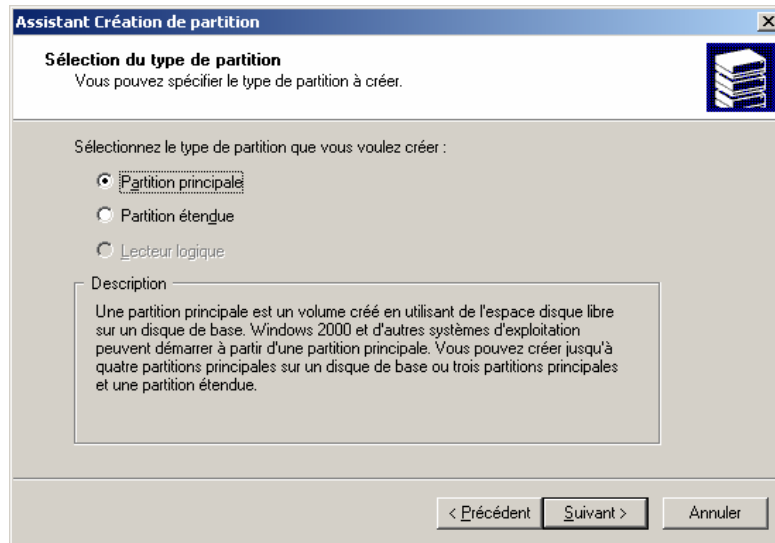
Pour profiter de cette place, il reste à définir la partition puis à la formater.

Dans les "Outils d'administration", ouvrez "Gestion de l'ordinateur" et placez-vous sur "Gestion des disques".



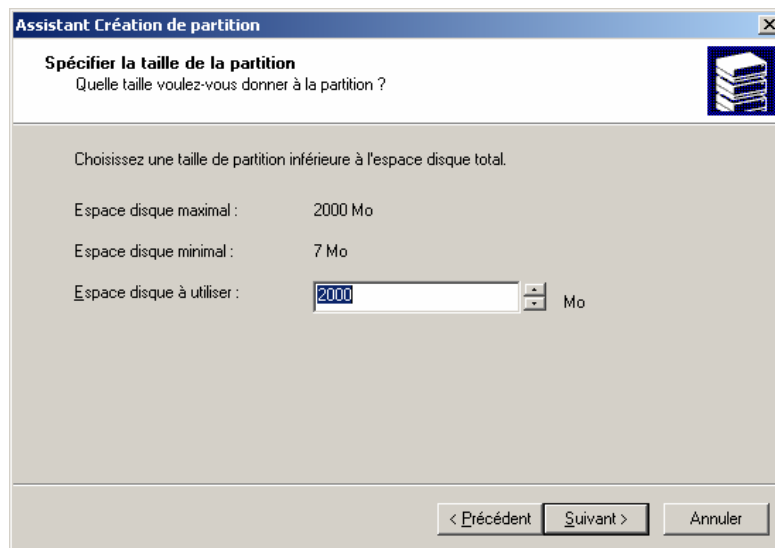
Soyez prudent, une mauvaise manipulation sur une partition contenant des données risque de faire perdre la partition et donc les données qu'elle contient.

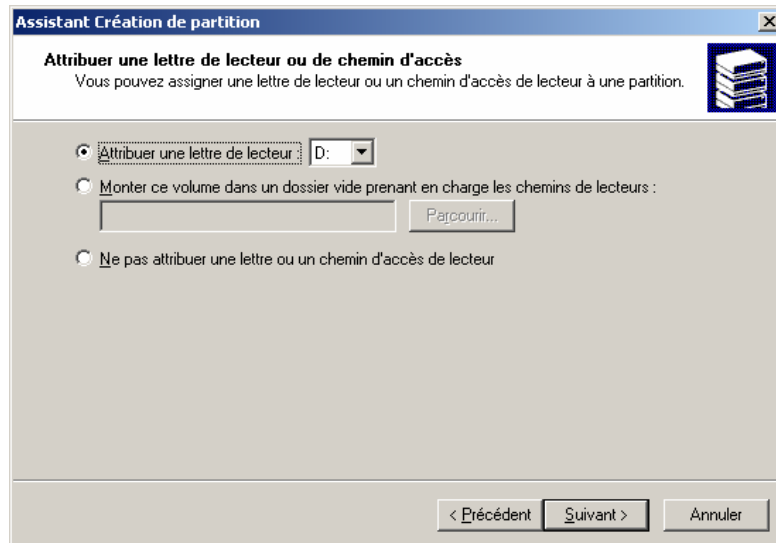
Si une partie du disque n'est pas encore allouée, vous pouvez "Créer une partition". Faites un clic droit sur la partie non allouée et "Créer une partition". Un assistant démarre...



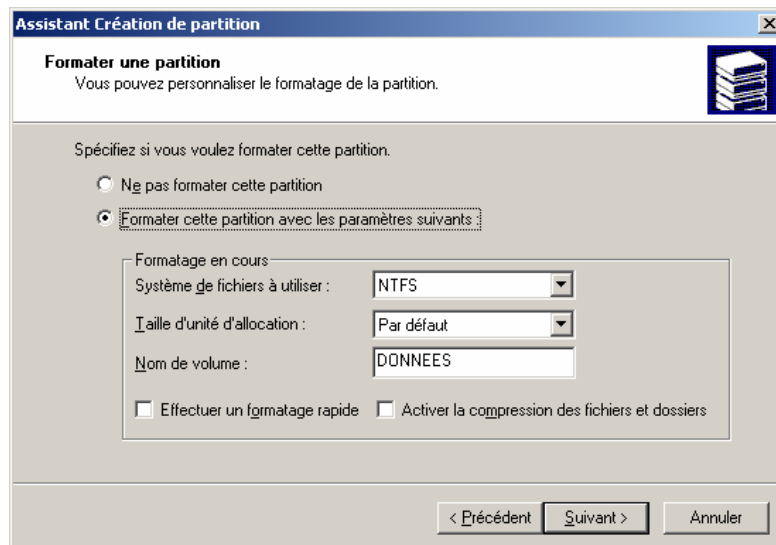
Un disque dur peut contenir de 1 à 4 (ou 5) partitions principales. A la place d'une partition principale, on peut créer une partition étendue dans laquelle on pourra créer des lecteurs logiques.

Si par exemple, Windows est installé sur une partition de 20 Go, on pourra créer une partition principale avec le reste du disque dur. Dans la copie d'écran suivante, il ne reste plus que 2 Go de libre sur le disque.





Il reste alors à formater la partition.



A partir de Windows 2000 il est possible de créer une partition sans lui attribuer de lettre. Une telle partition peut être "montée" dans un répertoire d'une autre partition. Si vous connaissez linux, vous êtes déjà familiarisé avec cette notion.

*Si on a créé une partition sans lui attribuer une lettre, on pourra par exemple créer un répertoire vide C:\UnRep, et monter cette partition dans C:\UnRep. Lorsque vous accédez au répertoire C:\UnRep, vous accédez en réalité à la partition. Une recherche dans les répertoires et sous-répertoires de C:\fera automatiquement une recherche également dans la partition montée.*

Le système de fichiers à utiliser peut être FAT (c'est à dire Fat16) ou FAT32 ou NTFS. Windows NT ne connaît pas la FAT32. On choisira en général NTFS car ce système de fichiers permet d'ajouter une fonctionnalité très importante : les **autorisations de sécurité** sur les répertoires et les fichiers.

## Que veut dire Activer une partition ?

En vous plaçant sur une partition, vous serez peut-être tenté de choisir "Activer" pensant qu'il s'agit de la rendre opérationnelle. En fait la partition "Active" est la partition qui est utilisée pour le démarrage. En général, il s'agit de la partition C.

Une seule partition par disque dur peut être active.



Si vous avez activé une mauvaise partition, vous n'aurez un problème qu'au prochain démarrage de l'ordinateur.

*Certains administrateurs ont "vécu heureux" pendant plusieurs mois après avoir activé une mauvaise partition. La mauvaise surprise n'arrive que lorsque le serveur pour une raison ou une autre a besoin d'être redémarré !*

Au démarrage l'ordinateur cherche le système d'exploitation sur le disque sélectionné au niveau du Bios et, sur ce disque, utilise la partition activée. Si cette partition ne contient pas de système d'exploitation l'ordinateur ne peut pas démarrer. Un message vous indique qu'il n'y a pas de système d'exploitation.

Que faire ?

Si vous avez activé une mauvaise partition mais que vous n'avez pas encore redémarré l'ordinateur, vous pouvez simplement activer la bonne partition à l'aide du gestionnaire de disques.

Si vous avez redémarré l'ordinateur et obtenu le message indiquant qu'il manque le système d'exploitation, il vous reste à utiliser une disquette Dos (Par exemple une disquette de démarrage obtenue avec Windows 98) et à utiliser FDisk pour activer la bonne partition.

## Disques en miroir

Appelé également RAID-1.

Il s'agit de deux disques durs, qui sont vus comme un seul disque dur. Les données sont enregistrées sur les deux disques en même temps et au même endroit. Deux disques de 20 Go ne vous donnent donc qu'une capacité de 20 Go.

Si un disque tombe en panne, l'autre permet de continuer. Bien sûr si un fichier est effacé, il l'est sur les deux disques, si un virus s'installe ou détruit des données, les deux disques sont modifiés.

## Disques en RAID-5

Il s'agit de plusieurs disques durs (au moins 3) branchées sur une carte contrôleur spéciale. Les données sont réparties sur les disques et un contrôle de parité permet de ne pas perdre les données lorsqu'un disque est en panne. Il est même en général possible de remplacer le disque sans arrêter l'ordinateur.

Les accès disques sont accélérés car l'écriture se fait sur plusieurs disques en même temps.

## Agrégat de partitions

Il est possible de regrouper plusieurs partitions appartenant au même disque ou à plusieurs disques.

L'ensemble de ces partitions est vu comme une partition unique. Lorsqu'une partition est pleine, la partition suivante est automatiquement utilisée.

C'est une solution qui permet d'obtenir une grande capacité mais les risques de panne sont augmentés. En effet, si pour une raison quelconque l'une des partitions n'est plus utilisable la totalité de l'agrégat est perdu.

Il est possible d'étendre un agrégat en ajoutant une ou plusieurs partitions sans perdre les données.

## Disques en RAID 0

Il est possible de regrouper deux disques de même taille afin de répartir les enregistrements sur les deux disques. Si l'un des disques est plus gros, seule une partie de la même taille que le petit sera utilisée.

L'écriture se fait par blocs en général de 64 ko sur les deux disques.

Cette solution est souvent proposée avec les disques SATA.

Par exemple deux disques de 60 Go donnent une unité de 120 Go et comme l'écriture se répartie sur les deux disques les accès sont accélérés.

Attention, la panne d'un des disques fait perdre toute l'unité.

## Changer la lettre attribuée au lecteur

Windows NT, 2000 ou 2003 accepte que vous changiez la lettre attribuée à un lecteur. Si ce lecteur n'a pas encore été utilisé, le changement n'aura aucune mauvaise conséquence. Si le lecteur a déjà été utilisé, et que vous changez sa lettre, il y a de grandes chances pour que des programmes aient retenu l'ancienne lettre dans des fichiers de configuration ou dans la base de registre et que votre changement cause des erreurs lors de l'utilisation de ces programmes.

Windows accepte que l'on change la lettre du lecteur sur lequel il est installé. Ne le faites pas ! En effet ce changement vous donnerait de nombreux dysfonctionnements.

## Le fichier Boot.ini

Exemple de fichier Boot.ini :

```
[boot loader]
timeout=30
default=multi(0)disk(0)rdisk(0)partition(1)\WINNT
[operating systems]
multi(0)disk(0)rdisk(0)partition(1)\WINNT="Microsoft Windows 2000 Server" /fastdetect
```

On y trouve le chemin utilisé pour indiquer l'emplacement des fichiers du système.

multi ou scsi permet de définir le type de carte contrôleur

multi(0) veut dire la première carte contrôleur IDE.

partition permet de définir le numéro de la partition à utiliser (commence à 1).

Remplacer partition(1) par partition(2) voudrait dire que les fichiers systèmes sont sur la deuxième partition. Si ce n'est pas le cas, Windows ne démarre pas.

Le fichier Boot.ini est un fichier texte caché et en lecture seule.

Il est situé sur la partition active (partition système).

## Service Pack

Microsoft fournit des correctifs sous forme de service pack.

Actuellement, le dernier service pack de NT est le 6a, le dernier service pack de 2000 est le Sp4, le dernier service pack de 2003 est le Sp1 et le dernier service pack de XP est le SP2.

Tout service pack contient les correctifs des précédents.

Avec Windows NT4, lorsque vous avez effectué des modifications qui ont nécessité de mettre le CD de Windows, il est conseillé de "repasser" le service pack.

NT4 sans au moins le service pack 4 n'est pas capable d'utiliser des disques durs de plus de 8 Go.

Les disques durs actuels dépassent souvent 128 Go mais Windows n'est pas toujours capable d'en profiter.

Windows 98 et NT4 ne sont pas capable d'utiliser l'espace au-delà des 128 Go des disques durs.

Windows 2000 a besoin du service pack 4 et d'une modification dans la base de registre pour dépasser cette limite.

*A faire seulement sur Windows 2000 SP4 si vous avez un disque de plus de 128 Go :*

*A la clé HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\Atapi\Parameters*

*Créer la valeur DWORD EnableBigLba et lui donner la valeur 1. Redémarrer.*

XP a besoin au moins du service pack 2 pour dépasser cette limite.

Windows 2003 n'est pas gêné par cette limite.

## Les services

Windows NT, 2000, XP et 2003 permettent l'utilisation de services.

Un service est un programme qui n'a pas besoin qu'une session soit ouverte pour être exécuté.

Par exemple, il n'est pas nécessaire qu'une session soit ouverte sur le serveur pour qu'il joue pleinement son rôle de serveur.

### Exercice 1 :

Ouvrez une fenêtre dos et tapez

```
NET SEND * "Hello !"
```

Ceci envoie le message 'Hello !' à tous les ordinateurs de votre domaine. Seuls les ordinateurs NT, 2000, 2003 ou XP recevront ce message.

Votre ordinateur faisant partie du domaine, reçoit également le message.

*Remarques :*

- À la place de l'étoile vous pouvez mettre le nom d'un ordinateur ou d'un utilisateur.
- Avec Windows 9x, exécutez Winpopup pour envoyer ou recevoir les messages.

Allez dans les "Outils d'administrations" et ouvrez "Services".

Faites un clic droit sur le service "Affichage des messages" et choisissez "Arrêter".

Recommencez l'envoi du message.

Vous ne recevez plus le message parce que le service qui traite l'arrivée des messages ne fonctionne plus.

Comme le service "Affichage des messages" démarre automatiquement lorsque Windows démarre, pour redémarrer le service, il serait possible de redémarrer l'ordinateur mais on peut se contenter de redémarrer seulement le service. Dans Services faites à nouveau un clic droit sur le service "Affichage des messages" et choisissez "Démarrer".

### Exercice 2 :

Certains services dépendent d'autres services. L'arrêt d'un service peut donc entraîner l'arrêt d'autres services. Placez-vous sur un service et dans les propriétés, regardez le volet "Dépendances".

Arrêtez le service Serveur. Vous êtes informé que d'autres services vont être arrêtés comme par exemples "Explorateur d'ordinateurs", "Ouverture de session réseau", "Système de fichiers distribués".

Vérifiez qu'il est maintenant impossible aux autres ordinateurs d'accéder à votre ordinateur (par exemple en faisant rechercher ordinateur).

Redémarrez le service Serveur puis les services qui dépendent de Serveur.

Vérifiez qu'il est possible à nouveau aux autres ordinateurs d'accéder à votre ordinateur.

# Windows 2003 serveur

## Domaines et Active Directory

### Windows 2000/2003 gère un domaine grâce à Active Directory

Avec NT4 serveur, l'installation de la partie gérant le domaine est "mélangée" avec l'installation de Windows.

Depuis Windows 2000 Serveur, L'installation d'Active Directory est bien séparée de l'installation de Windows 2000. Il est par exemple possible de supprimer Active Directory et de le réinstaller sans avoir à réinstaller Windows 2000/2003.

### Choix des noms de domaines

Windows 2000/2003 serveur est conçu pour fonctionner dans des environnements comportant un grand nombre de serveurs.

Ces serveurs sont regroupés en domaines.

Un serveur ne peut pas gérer plusieurs domaines.

Un domaine peut être géré par un seul serveur ou par plusieurs serveurs.

Dans un domaine, chacun des 5 rôles de "Maître d'opérations" est joué par un et un seul serveur afin de coordonner les changements. Un même serveur peut jouer plusieurs voire tous les rôles.

*Si Active Directory est installé et que votre domaine contient plusieurs serveurs, vous pouvez voir ou changer les maîtres d'opérations en ouvrant "Utilisateurs et Ordinateurs Active Directory", en faisant un clic droit sur la ligne "Utilisateurs et Ordinateurs Active Directory" et en choisissant "Maîtres d'opérations..."*

*Pour plus de détails voir la partie "Rôles des serveurs d'un domaine" plus loin.*

Avec Windows NT serveur tous les domaines étaient au même niveau. Avec Windows 2000 serveur, il est possible d'avoir une arborescence de domaines.

Par exemple

Domaine le plus haut : lycee.priv

Un domaine enfant : tertiaire.lycee.priv

Un autre domaine enfant de même niveau : info.lycee.priv

A partir d'un serveur du domaine tertiaire.lycee.priv, il est possible d'accéder en lecture aux propriétés des utilisateurs de lycee.priv.

A partir d'un serveur du domaine lycee.priv, il est possible d'accéder avec tous les droits aux propriétés des utilisateurs de tertiaire.lycee.priv ou info.lycee.priv.

En pratique dans un établissement scolaire, on n'utilisera pas les domaines enfants. On utilisera par exemple les domaines tertiaire.priv et info.priv. On pourra ensuite si on le souhaite établir des relations d'approbation entre ces deux domaines.

### Trois fonctions possibles

Lorsque vous installez Active Directory, vous devez choisir entre :

- **Contrôleur de domaine pour un nouveau domaine.**
- **Contrôleur de domaine supplémentaire pour un domaine existant.**

Vous pouvez également ne pas installer Active Directory, votre serveur sera alors un simple **serveur autonome** et si vous l'inscrivez dans un domaine (comme une simple station), il sera **serveur membre**.

### Contrôleurs de domaine

Dans chaque domaine, un serveur au moins doit être contrôleur de domaine.

Lorsque vous voulez ajouter un serveur à un domaine existant, vous devez le faire en étant connecté au serveur existant et choisir "Contrôleur de domaine supplémentaire pour un domaine existant". Lors de l'installation d'Active Directory, ce serveur récupère des informations indispensables à partir du serveur existant comme par exemple les identificateurs de sécurité (SID).

Attention, il arrive que des commerçants pensant bien faire, installent dans leurs ateliers, un serveur en lui donnant le même nom de domaine que celui que vous utilisez déjà sur votre serveur existant afin de vous permettre d'avoir un deuxième serveur pour votre domaine. Lorsque ce nouveau serveur est branché dans votre réseau, il n'est pas capable de s'intégrer correctement à votre domaine. Il y a même des conflits qui causent des lenteurs et des erreurs. La solution consiste à isoler le nouvel ordinateur et à désinstaller Active Directory. Il vous reste alors à mettre ce nouvel ordinateur dans votre réseau et à réinstaller Active Directory en présence du premier serveur.

## Installation d'Active Directory et de DNS

Voir les documents "Installation de Windows 2000 Serveur" et "Installation de Windows 2003 Serveur" qui décrivent, avec copies d'écran, une façon d'installer Active Directory et DNS dans le cas d'un domaine composé d'un seul serveur.

## Les comptes utilisateurs

Il est possible que vous ayez créé des utilisateurs ou des groupes avant d'installer Active Directory. Dans ce cas, il s'agissait d'utilisateurs ou de groupes de l'ordinateur. Vous avez pu faire cela en allant dans "Gestion de l'ordinateur" et en vous plaçant sur "Utilisateurs et groupes locaux" puis sur Utilisateurs (ou Users).

Depuis que Active Directory est installé, ces anciens utilisateurs ou groupes ont été supprimés. D'ailleurs en allant dans "Gestion de l'ordinateur" vous constatez que "Utilisateurs et groupes locaux" est supprimé ou est représenté par une croix rouge indiquant que la gestion des comptes locaux est désactivée.

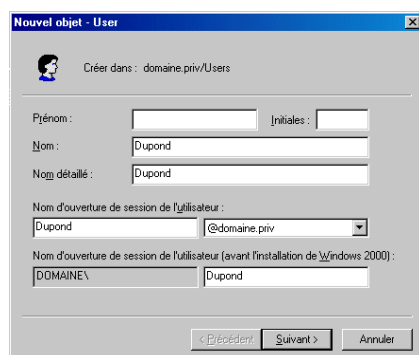
Les utilisateurs et les groupes que l'on va créer vont appartenir au domaine. Pour les créer on utilise "Utilisateurs et ordinateurs Active Directory".

Des serveurs contrôleurs d'un même domaine, possèdent la même base de données de l'annuaire (liste des utilisateurs). La modification d'un utilisateur sur l'un des serveurs, se répercute automatiquement sur les autres (la synchronisation peut se faire avec un retard de quelques minutes).

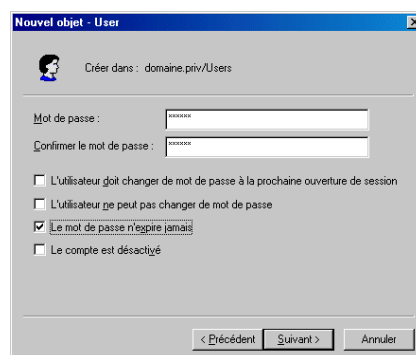
## Utilisateurs et groupes du domaine

### Création d'un nouvel utilisateur.

Dans les outils d'administration, ouvrez "Utilisateurs et ordinateurs Active Directory", placez-vous sur "Users".



The screenshot shows the 'Nouvel objet - User' dialog box. The title bar reads 'Nouvel objet - User'. Below the title bar, it says 'Créer dans : domaine.priv/Users'. The dialog has several input fields: 'Prénom :', 'Initiales :', 'Nom : Dupond', 'Nom détaillé : Dupond', 'Nom d'ouverture de session de l'utilisateur : Dupond @domaine.priv', and 'Nom d'ouverture de session de l'utilisateur (avant l'installation de Windows 2000) : DOMAINE\ Dupond'. At the bottom, there are three buttons: '< Précédent', 'Suivant >', and 'Annuler'.



The screenshot shows the 'Nouvel objet - User' dialog box, second step. The title bar reads 'Nouvel objet - User'. Below the title bar, it says 'Créer dans : domaine.priv/Users'. The dialog has two password input fields: 'Mot de passe :' and 'Confirmer le mot de passe :'. Below these are three checkboxes: 'L'utilisateur doit changer de mot de passe à la prochaine ouverture de session', 'L'utilisateur ne peut pas changer de mot de passe', and 'Le mot de passe n'expire jamais' (which is checked). There is also an unchecked checkbox for 'Le compte est désactivé'. At the bottom, there are three buttons: '< Précédent', 'Suivant >', and 'Annuler'.

Créez de la même façon quelques autres utilisateurs (Durand, Dubois, Duchemin, Dujardin...). Ces comptes seront utiles pour effectuer nos essais dans la suite.

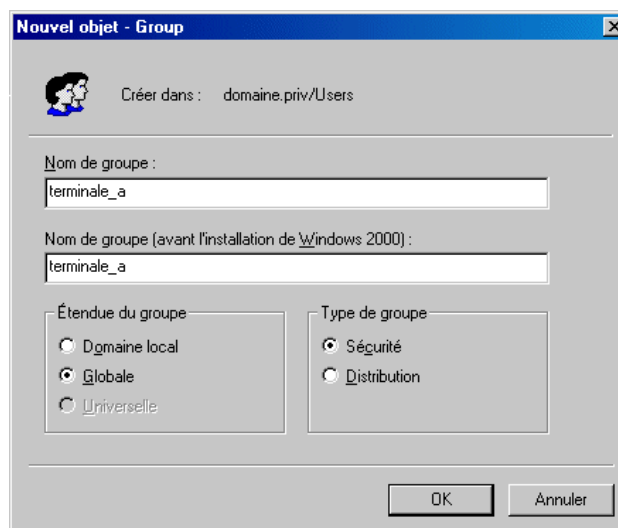
Il est important de remarquer que l'utilisateur créé n'a pas le droit de venir travailler sur le serveur. Il n'est pas autorisé à ouvrir une session sur le serveur.

L'utilisateur pourra cependant ouvrir une session sur un autre ordinateur et accéder par le réseau à certaines ressources situées sur le serveur (répertoires, fichiers, imprimantes...).

Il est toutefois possible de donner des droits différents à un utilisateur. Par exemple il suffit de mettre un utilisateur dans le groupe Administrateurs ou Admin du domaine pour que celui-ci obtienne le droit d'ouvrir une session sur le serveur ainsi que les droits d'administration au même titre que le compte Administrateur.

## Création d'un groupe

Vous pouvez de la même façon créer un groupe.



## Groupes globaux et groupes locaux

Groupe global : Il s'agit d'un groupe conçu pour regrouper des utilisateurs du domaine.

Groupe local : Il s'agit d'un groupe conçu pour attribuer des droits.

Un groupe global peut contenir :

- des utilisateurs du domaine

Un groupe local peut contenir :

- des utilisateurs du domaine
- des utilisateurs d'autres domaines
- des groupes globaux du domaine
- des groupes globaux d'autres domaines.

Prenons un exemple.

Vous avez quelques utilisateurs créés (Dupond..).

Vous créez un groupe global "terminale\_a" et vous mettez les utilisateurs comme membres du groupe "terminale\_a" (Dupond est membre de terminale\_a).

Vous créez un groupe local "impr\_couleur". Vous mettez "terminal\_a" comme membre de "impr\_couleur".

Vous donnez au groupe "impr\_couleur" le droit d'utiliser l'imprimante couleur (par défaut Tout le monde a le droit d'imprimer, vous enlevez Tout le monde et vous mettez "impr\_couleur" a le droit d'imprimer).

Un utilisateur du groupe "terminale\_a" aura alors le droit d'imprimer sur l'imprimante couleur.

**En pratique :**

Comme il est possible de donner des droits à un groupe global, on aura souvent tendance à ne pas beaucoup utiliser les groupes locaux dans un réseau d'établissement scolaire.

**Utilisateurs et groupes d'origine**

Lors de l'installation d'Active Directory, un certain nombre d'utilisateurs et de groupes sont créés automatiquement.

**Utilisateurs :**

Ouvrez "Utilisateurs et ordinateurs Active Directory" et placez-vous sur "Users". On y trouve essentiellement :

- Administrateur
- Invité

Invité est un compte désactivé.

**Groupes locaux :**

Ouvrez "Utilisateurs et ordinateurs Active Directory" et placez-vous sur "Builtin". On y trouve essentiellement (remarquez le pluriel) :

- Administrateurs
- Utilisateurs

**Groupes globaux**

Ouvrez "Utilisateurs et ordinateurs Active Directory" et placez-vous sur "Users". On y trouve essentiellement (remarquez le pluriel) :

- Admins du domaine
- Utilisa. du domaine
- Ordinateurs du domaine

"Ordinateurs du domaine" ne concerne pas les utilisateurs, nous verrons ce groupe plus tard.

Il existe également un groupe particulier nommé "Tout le monde".

Questions :

- Lequel des deux groupes "Administrateurs" et "Admins du domaine" est dans l'autre (est membre de l'autre) ?
- Administrateur est membre de quels groupes ?
- Lorsque vous créez un utilisateur, il est automatiquement membre d'un groupe, lequel ?

**Ordinateurs du domaine**

Les versions professionnelles (NT4 Workstation, 2000 Pro, XP pro) des stations peuvent être inscrites dans un domaine. Elles apparaissent alors dans l'entrée "Computers" de Active Directory.

# Stations dans le réseau

## Windows NT Workstation ou 2000 Pro ou XP Pro

Ces ordinateurs ne sont pas capables de gérer un domaine.

Ils peuvent être utilisés de façon autonome ou faire partie d'un domaine.

Dans la suite il est supposé que vous utilisez Windows 2000 Pro mais Windows NT Workstation et Windows XP Pro réagissent de façon semblable.

Attention : Windows XP édition familiale ne permet pas de fonctionner dans un domaine. On ne choisira donc pas cette version pour une utilisation dans un établissement scolaire.

## Windows 2000 Pro ou XP Pro utilisé de façon autonome

Dans les "Outils d'administration", ouvrez "Gestion de l'ordinateur".

*Si vous n'avez pas les "Outils d'administration" dans le menu programmes, vous pouvez le trouver dans le panneau de configuration.*

Ouvrez "Utilisateurs et groupes locaux".

*Vous pouvez également utiliser "Utilisateurs et mot de passe" dans le panneau de configuration.*

Créez un utilisateur. Il sera automatiquement membre du groupe "Utilisateurs" et à ce titre aura le droit d'ouvrir une session sur la station.

Cet utilisateur ne bénéficie pas des mêmes droits qu'un administrateur. Il ne peut pas par exemple créer des utilisateurs ou modifier les utilisateurs existants. Certains répertoires ne peuvent pas être modifiés. Il ne peut pas changer la sécurité sur les répertoires...

## Windows 2000 Pro ou XP Pro utilisé dans un domaine

Lorsqu'une station est jointe à un domaine, il est possible d'ouvrir une session avec un compte utilisateur local ou avec un compte utilisateur du domaine.

Le choix se fait dans la fenêtre d'ouverture de session en choisissant dans la liste à côté de "Se connecter à". Cette liste est formée du nom de la station et du nom du domaine.

*Si vous ne voyez que deux zones dans la fenêtre d'ouverture de session, utilisez le bouton "Options>>".*

## Accès à un Windows 2000 Pro ou XP Pro à partir d'autres ordinateurs

Si, à partir d'un ordinateur du réseau, vous essayez d'accéder à un répertoire partagé d'un Windows 2000 pro ou d'un XP Pro, il est possible qu'un nom et un mot de passe vous soient demandés. Tapez le nom et le mot de passe d'un compte existant sur la station que vous voulez atteindre (si la station est dans un domaine, un compte du domaine peut également convenir).

Si l'ordinateur à atteindre est un XP avec service pack 2, le compte à utiliser doit avoir un mot de passe non vide.

Attention, Windows 2000 Pro et XP Pro sont limités volontairement par Microsoft à 10 connexions simultanées. Cela signifie que si 10 ordinateurs du réseau sont en train d'accéder à des partages de cet ordinateur, alors il ne sera pas possible à un onzième ordinateur d'y accéder.

## Ajout d'une station dans un domaine

Les ordinateurs qui exécutent Windows 95 ou 98 ou ME n'ont pas besoin d'être déclarés dans le domaine.

Dans les propriétés réseau de la station, on choisira "Client pour les réseaux Microsoft" et il suffira alors d'ouvrir une session avec un nom d'utilisateur du domaine pour accéder au domaine.

Pour avoir le droit d'ouvrir une session avec un compte utilisateur du domaine sur une station NT Workstation ou 2000 pro ou XP pro il est nécessaire de commencer par joindre la station au domaine. Ce travail n'est à faire qu'une fois sur chaque station.

Comme une station ne peut appartenir qu'à un domaine, si on veut qu'elle appartienne à un autre domaine, on commencera par l'enlever de son domaine avant de pouvoir l'ajouter au nouveau domaine.

Pour faire appartenir la station à un domaine, plusieurs méthodes sont possibles. La suite décrit une méthode.

## Paramétrez le serveur

Si votre serveur est un 2000 ou un 2003, tout utilisateur du domaine a le droit d'inscrire des stations dans le domaine. Cependant un utilisateur ordinaire est limité à 10 inscriptions.

Si cette limite est gênante ou si votre serveur est un serveur NT4 alors, il vous reste trois possibilités :

- 1) Utiliser le compte Administrateur du domaine (ce compte n'est pas limité).
- 2) Donner le droit d'inscrire des stations dans le domaine à des utilisateurs ou à des groupes.
- 3) Sur le serveur, pré-inscrire la station dans le domaine en précisant éventuellement qui aura le droit d'effectuer cette inscription.

Si vous choisissez la solution 2, commencez par aller sur le serveur pour donner le droit à un utilisateur ou à un groupe d'ajouter des stations au domaine. Je suppose que le compte utilisé s'appelle "Chef"

Serveur NT : Ouvrez le gestionnaire des utilisateurs pour les domaines, Dans "Stratégies", "Droits de l'utilisateur". Sélectionnez le droit réseau "Ajouter des stations de travail au domaine". Ajoutez l'utilisateur ou le groupe (par exemple l'utilisateur Chef).

Serveur 2000 : Dans "Utilisateurs et ordinateurs active directory" et Users, faites un double clic sur l'utilisateur ou le groupe (par exemple l'utilisateur Chef) et, dans le volet "membre de" ajoutez "Opérateurs de compte".

Vous disposez maintenant d'au moins un compte capable d'ajouter des stations au domaine. Donnez le nom et le mot de passe de ce compte aux personnes chargées d'ajouter des stations au domaine.

Si vous choisissez la solution 3 avec un serveur 2000 ou 2003, allez dans "Utilisateurs et ordinateurs Active Directory" et dans "Computers", ajoutez un ordinateur. Indiquez le nom de l'ordinateur et le compte ou le groupe qui aura le droit d'inscrire cette station.

## Ajouter les stations

Avant de commencer, il est important de **vérifier quelques points** :

- Vérifiez que le service DNS est présent et fonctionnel sur le serveur.
- Vérifiez que la station a dans TCP/IP de ses propriétés réseau, l'adresse IP du serveur de son futur domaine comme serveur DNS. Par exemple PCA1 doit avoir l'adresse IP de SERVA1 comme DNS dans ses propriétés réseau.

*Si SERVA1 a des redirections, cette adresse IP suffit à PCA1 pour aller sur Internet. C'est cette solution qui est la meilleure car ajouter l'adresse IP d'un serveur DNS du fournisseur d'accès ferait apparaître des lenteurs.*

- Vérifiez que la station et le serveur sont dans le même fuseau horaire, ont le même choix de l'heure d'été, ont la même date et sont à la même heure (à quelques minutes près).

**Ouvrir une session avec un compte local** (par exemple avec le compte administrateur local) se fait en tapant le nom, le mot de passe du compte et en choisissant le **nom de la station** en troisième zone de la fenêtre d'ouverture de session.

**NTWS** : Pour faire appartenir la station à un domaine, ouvrez la session en tant qu'administrateur local et, dans les propriétés réseau, cliquez sur le bouton "Modifier". Indiquez que la station doit être membre du domaine. On peut, sans aller sur le serveur, créer un compte d'ordinateur dans le domaine en donnant le nom

et le mot de passe d'un compte autorisé à ajouter des stations au domaine (l'administrateur du domaine ou le compte Chef).

**W2KP** : Pour faire appartenir la station à un domaine, ouvrez la session en tant qu'administrateur local, dans le "Panneau de configuration", ouvrez "Système", dans le volet "Identification réseau" cliquez sur "Propriétés". Indiquez le nom du domaine. Il vous sera demandé "le nom et le mot de passe d'un compte autorisé à joindre le domaine", donnez l'administrateur du domaine et son mot de passe ou le nom défini précédemment et son mot de passe (le compte Chef).

*On peut accéder plus rapidement aux propriétés systèmes en faisant un clic droit sur le poste de travail et en allant dans "Propriétés".*

**XP** : Pour faire appartenir la station à un domaine, ouvrez la session en tant qu'administrateur local, dans le "Panneau de configuration", et "Performance et maintenance", ouvrez "Système", dans le volet "Nom de l'ordinateur" cliquez sur "Modifier". Indiquez le nom du domaine. Il vous sera demandé "le nom et le mot de passe d'un compte autorisé à joindre le domaine", donnez l'administrateur du domaine et son mot de passe ou le nom défini précédemment et son mot de passe (le compte Chef).

*On peut accéder plus rapidement aux propriétés systèmes en faisant un clic droit sur le poste de travail et en allant dans "Propriétés".*

Lorsque la station est ajoutée au domaine, son nom apparaît dans "utilisateurs et ordinateurs Active Directory" dans la partie "Computers" ainsi que dans le groupe "Ordinateurs du domaine" située dans "Users".

*Si la station a déjà été ajoutée puis enlevée, il est possible que son nom soit resté dans Active Directory. Dans ce cas l'ajout de cette station peut échouer. Allez dans Active Directory sur le serveur, supprimez cette station et recommencez l'ajout.*

## Enlever une station d'un domaine

**NTWS** : Pour enlever la station du domaine, ouvrez la session en tant qu'administrateur local et, dans les propriétés réseau, cliquez sur le bouton "Modifier". Indiquez que la station doit être membre de Workgroup.

**W2KP** : Pour enlever la station du domaine, ouvrez la session en tant qu'administrateur local, dans le "Panneau de configuration", ouvrez "Système", dans le volet "Identification réseau" cliquez sur "Propriétés". Choisissez "Membre de" et "Groupe de travail".

**XP** : Pour enlever la station du domaine, ouvrez la session en tant qu'administrateur local, dans le "Panneau de configuration", et "Performance et maintenance", ouvrez "Système", dans le volet "Nom de l'ordinateur" cliquez sur "Modifier". Choisissez "Membre de" et "Groupe de travail".

*Il arrive que la station ne soit pas enlevée automatiquement dans Active Directory sur le serveur. Allez sur le serveur et si vous constatez que la station est encore présente, vous pouvez l'enlever.*

Il est alors fort probable que l'adresse IP indiquée comme DNS dans le paramétrage TCP/IP ait besoin d'être changée.

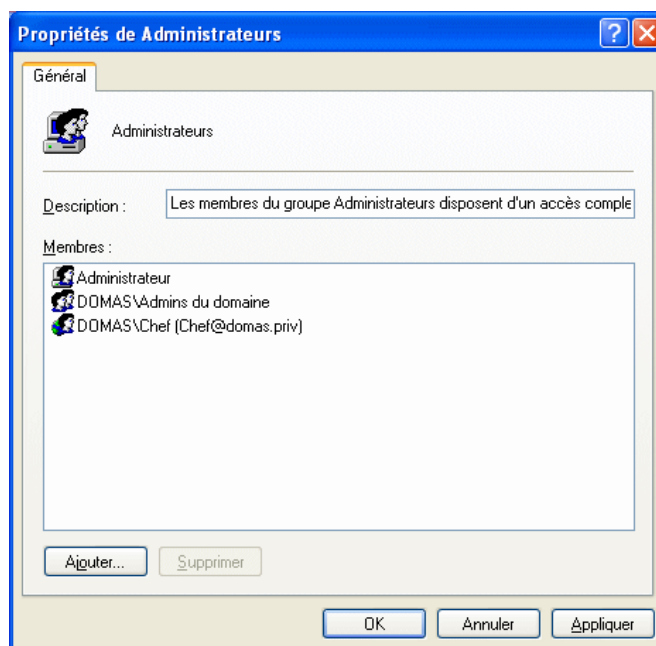
## Un compte du domaine avec des droits locaux

Il sera pratique d'avoir un compte utilisateur du domaine avec des droits d'administrateur local. Ce compte permettra d'ouvrir une session sur la station en ayant tous les droits sur cette station et en ayant accès au réseau et en particulier au serveur. Voici comment procéder :

Je suppose que nous allons utiliser le compte "Chef" créé précédemment sur le serveur.

Ouvrez une session sur une station en utilisant un compte d'administrateur local.

Allez dans "Gestion de l'ordinateur", dans "Utilisateurs et groupes", "Groupes" et Affichez les propriétés du groupe "Administrateurs". Utilisez "Ajouter" dans "Regarder dans" sélectionnez le nom du domaine et ajoutez "Chef".  
Validez.



Vous pouvez maintenant ouvrir une session sur la station avec le compte Chef et le nom de votre domaine comme domaine et avoir les droits d'administrateur de la station.

# Autorisations de partages et de sécurité

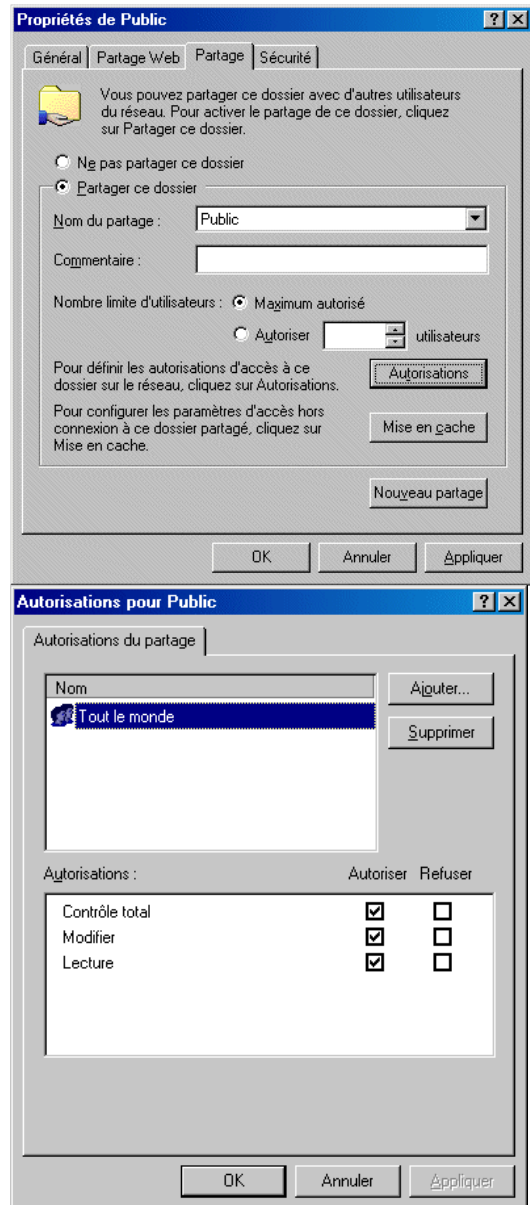
## Partage d'un répertoire

Un répertoire peut être partagé afin d'être accessible à partir des autres ordinateurs du réseau.

Dans les propriétés du partage, le bouton "Autorisations" permet de décider qui aura le droit d'accéder à ce répertoire à partir des autres ordinateurs du réseau.

Autorisations de partage :

Par défaut le groupe "Tout le monde" a un "Contrôle total" (NT et 2000) ou "Lecture" (2003, XP). Vous pouvez modifier ces autorisations en fonction de vos besoins.



### Exercice :

Dans les autorisations de partage du répertoire :  
Supprimez la ligne "Tout le monde".  
Ajoutez Dupond et Durand  
Donnez le droit "Modifier" à Dupond.  
Donnez le droit "Lecture" à Durand.

*Pour éviter les problèmes de droits d'ouverture de session, la suite de l'exercice pourra être faite sur un client Windows 9X. Si vous n'avez pas de 9x vous serez amené à donner un nom et un mot de passe pour accéder à l'ordinateur qui partage.*

Ouvrez une session sur un autre ordinateur du réseau en tant que Dupond et essayez d'accéder par le voisinage réseau au répertoire partagé du serveur.

*Si vous n'avez pas de Windows 9x pour faire cet exercice, ouvrez une session avec un compte quelconque sur une station 2000 ou XP et donnez le nom Dupond lorsque Windows vous demande un nom et un mot de passe pour accéder à l'autre ordinateur. Fermez la session et ouvrez à nouveau la session pour pouvoir faire un nouvel essai.*

Ouvrez une session sur un autre ordinateur du réseau en tant que Durand et essayez de même d'accéder au répertoire partagé du serveur.

Ouvrez une session sur un autre ordinateur du réseau en tant que Duchemin. Avez-vous le droit d'accéder au répertoire partagé du serveur ?

### **Rôle des coches dans la colonne "Refuser".**

Si un compte utilisateur ou un groupe est à la fois dans "Autoriser" et dans "Refuser", la ressource lui sera refusée car "Refuser" l'emporte sur "Autoriser".

Il peut être pratique d'utiliser "Refuser" pour un ou deux utilisateurs appartenant à un groupe alors que le groupe est autorisé. Cela reviendrait au même mais serait plus fastidieux d'autoriser un par un presque tous les membres du groupe.

### **Cas où un utilisateur a plusieurs autorisations**

Imaginons que Dupond possède un droit "Lecture" alors qu'un groupe auquel appartient Dupond possède un droit "Modifier". Dans ce cas Dupond obtient le droit de modifier.

On peut résumer ceci en disant que les autorisations s'ajoutent.

Attention si vous refusez un droit à une personne alors que cette personne appartient à un groupe qui possède le droit, c'est le refus qui l'emporte.

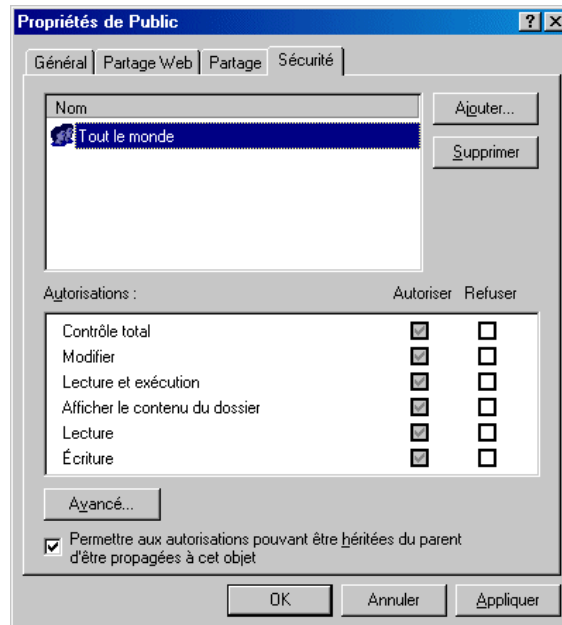
## **Sécurité sur un répertoire ou un fichier**

Faites un clic droit sur un répertoire et allez dans "Propriétés". Vous retrouvez le volet "Partage" mais si la partition est NTFS, vous avez également un volet "Sécurité".

Dans le volet "Sécurité", vous retrouvez un bouton "Autorisations".



Alors que les autorisations de partage ne concernent que les personnes accédant au répertoire à partir des autres ordinateurs du réseau, les autorisations de sécurité s'appliquent à tous (que l'on soit sur l'ordinateur ou sur un autre ordinateur du réseau).



Vous pouvez constater que la coche est mise dans la case "Permettre aux autorisations pouvant être héritées du parent d'être propagées à cet objet".

Cela signifie que les autorisations du répertoire père (le répertoire contenant ce répertoire) sont automatiquement appliquées à ce répertoire.

Pour supprimer un droit hérité, vous devez commencer par supprimer la coche de l'héritage (si vous oubliez, un message vous demandera confirmation pour la supprimer).



**Attention :** Ne changez pas la sécurité sur les répertoires créés par Windows sans savoir parfaitement ce que vous faites.

Une erreur par exemple consisterait à se placer sur C: et à modifier les autorisations de sécurité. Si en plus vous utilisez le bouton "Avancé" pour cocher "Réinitialiser les autorisations sur tous les objets enfants..." vous détruisez toutes les sécurités d'origine sur les différents répertoires de la partition Windows.

Retenez, cette règle simple : Ne modifiez les autorisations de sécurité que sur les répertoires ou fichiers que vous avez créés.

## Autorisations réelles

Lorsqu'un utilisateur accède à partir d'une station à un répertoire partagé du serveur, il doit "traverser" les autorisations de partage et s'il y arrive, doit encore "traverser" les autorisations de sécurité. L'autorisation réelle appliquée est donc l'intersection (au sens mathématique) des deux autorisations.

Lorsqu'un utilisateur accède à un répertoire situé sur son ordinateur, il n'a que les autorisations de sécurité à "traverser".

### Exercice :

Supposons qu'un répertoire E:\Documents\Public est partagé sous le nom Public.

Supposons que Dupond appartient au groupe terminale\_a.

Indiquez dans chaque cas (pour chaque ligne du tableau), les droits réels de Dupond

Autorisations de partage	Autorisations de sécurité	Droit réel de Dupond lorsqu'il est sur un autre ordinateur.	Droit réel de Dupond lorsqu'il est sur cet ordinateur (en supposant qu'il a le droit d'ouvrir une session).
Dupond : "Modifier" terminale_a : "lecture"	Tout le monde : "Modifer".		
terminale_a : "Lecture"	Dupond : "Modifier"		
terminale_a : "Modifier"	terminale_a : "Lecture"		
Dupond: "Modifer"	Tout le monde : "Lecture"		
Tout le monde : "Contrôle total" Dupond : "Lecture"	Dupond : "Lecture" terminale_a : "Modifier"		
Tout le monde : "Contrôle total"	terminale_a : "Modifier"		
terminal_a : "Lecture"	Tout le monde : "Contrôle total"		

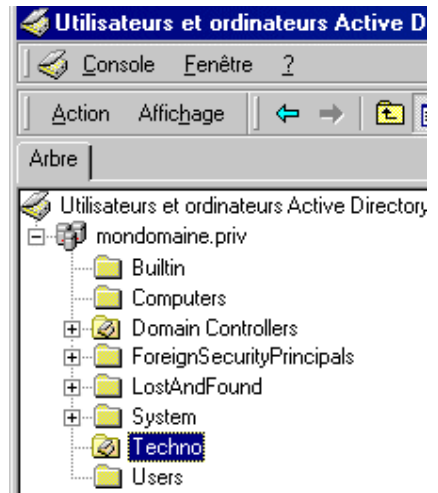
# OU : Unités Organisationnelles

Une unité organisationnelle permet de regrouper des utilisateurs et ordinateurs afin de ne pas les traiter comme les autres membres du groupe Users.

Ce que nous allons faire sur le serveur n'aura un impact que sur les stations 2000 Pro ou XP Pro.

Si toutes vos stations sont en Windows 9x ou ME ou NT4 Workstation les OU ne vous serviront pas.

Sur le serveur 2000 ou 2003, ouvrez "Utilisateurs et ordinateurs Active Directory". Placez-vous sur votre domaine et créez une nouvelle "Organizational Unit". Soit "Techno" le nom donné à cette OU.



## Mettre des objets dans une OU

Placez-vous sur Users et dans la partie droite, faites un clic droit sur un utilisateur ou un ordinateur. Choisissez "Déplacer.." et indiquez Techno.

*Windows 2003 accepte que l'on glisse les objets à l'aide de la souris.*

Un objet ne peut pas être placé dans plusieurs OU.

Une OU peut contenir des OU.

Un objet placé dans une OU qui est contenue dans une autre OU subira les stratégies des deux OU.

On peut créer autant d'OU que nécessaire mais plus le nombre est élevé, plus vous aurez du travail pour donner les droits et restrictions.

Il est possible à tout moment de déplacer un objet d'une OU vers une autre.

## Utiliser les OU pour restreindre les utilisateurs

Une restriction appliquée à un utilisateur, s'applique à cet utilisateur quelle que soit la station 2000 ou XP sur laquelle il ouvre une session.



Cela signifie que vous ne pouvez pas appliquer des restrictions différentes à un utilisateur en fonction de la station sur laquelle il ouvre une session.

*Ceci n'est pas tout à fait vrai, car il est possible de bloquer certaines stratégies en modifiant la sécurité sur ces stratégies.*

Placez-vous sur l'OU Techno, allez dans "Propriétés" et choisissez "Stratégie de groupe" (GPO). Créez une nouvelle stratégie de groupe que vous appellerez par exemple "Limitations".

Utilisez le bouton "Modifier"

Modifiez par exemple "Masquer l'écran de veille" que vous trouverez dans "Configuration de l'utilisateur", "Modèles d'administration", "Panneau de configuration" et "Affichage". En activant cette restriction, tout utilisateur de cette OU doit à sa prochaine ouverture de session sur une station du domaine ne plus avoir le volet "Ecran de veille" dans ses propriétés d'affichage.

**Que veut dire "Activer" ?**

La stratégie sera appliquée. Si elle est déjà présente sur la station, elle le restera, si elle ne l'est pas encore elle le deviendra.

**Que veut dire "Désactiver" ?**

La stratégie sera supprimée. Si elle est présente sur la station, elle sera supprimée, si elle ne l'est pas rien n'est fait.

**Que veut dire "Non configuré" ?**

La stratégie redeviendra comme si elle n'avait pas été activée.

Plus exactement, si une autre stratégie moins prioritaire existe, cette autre stratégie s'appliquera.

**Que se passe-t-il s'il existe des stratégies contradictoires ?**

Chaque stratégie s'applique dans un certain ordre. La dernière appliquée est donc celle qui l'emporte.

Les stratégies locales de la station s'appliquent en premier.

Les stratégies du domaine s'appliquent ensuite.

Les stratégies des OU s'appliquent enfin dans l'ordre d'imbrication.

**Où sont retenues les stratégies ?**

Lorsqu'une station subit une stratégie, elle effectue une modification dans sa base de registre.

Si la stratégie concerne l'ordinateur, la modification est souvent faite dans la clé

HKEY\_LOCAL\_MACHINE.

Si la stratégie concerne l'utilisateur, la modification est souvent faite dans la clé HKEY\_CURRENT\_USER.

Or cette dernière clé est retenue dans le profil de l'utilisateur (NTUSER.DAT). Chaque utilisateur qui a ouvert une session et qui a subit la stratégie a donc son NTUSER.DAT modifié.

# Profils utilisateurs

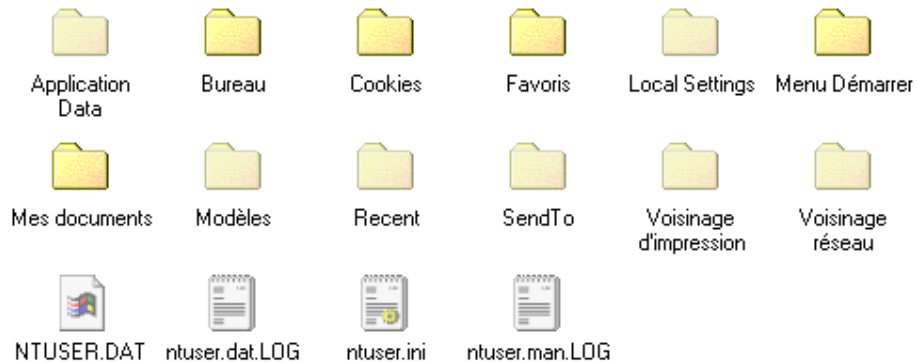
Windows 9x ou ME peut fonctionner avec ou sans les profils utilisateurs.

NT Workstation, 2000 Pro ou XP pro ne fonctionne qu'avec les profils utilisateurs activés.

## Profils locaux

Le profil de l'utilisateur est constitué d'entrées dans la base de registre et d'un répertoire souvent au nom de l'utilisateur. Ce répertoire se trouve dans le répertoire \Documents and Setting de la station.

On y trouve un certain nombre de fichiers et répertoires et en particulier le fichier caché ntuser.dat.



Il est de temps en temps nécessaire de supprimer les profils qui ne servent plus.



Cette suppression NE se fait PAS en supprimant le répertoire !

Cette suppression se fera sur chaque station en tant qu'administrateur et en utilisant "Panneau de configuration", "Système" et "Profils utilisateurs" (pour XP : "Panneau de configuration", "Système", "Avancé" et dans "Profils utilisateurs" utilisez "Paramètres").

L'utilitaire DelProf.exe (téléchargeable sur le site de Microsoft) permet de supprimer plusieurs profils en une seule opération.

Si le nombre d'utilisateurs est important et si les stations du domaine se ressemblent, on pourra préférer la solution des profils utilisateurs itinérants obligatoires.

## Profils utilisateurs itinérants

### Principe

Sur les serveur, dans les propriétés d'un utilisateur, en mettant dans le volet "Profil", un chemin de profil, l'utilisateur retrouvera son profil à partir de toutes les stations du réseau.

Cette solution a ses avantages et ses inconvénients.

**Avantages :** L'utilisateur conserve ses paramètres. Il retrouve son bureau, son menu démarrer, son répertoire Mes documents, ses cookies, ses fichiers temporaires Internet...

**Inconvénients :** Si les stations ne sont pas identiques, certains raccourcis ne seront pas opérationnels, certains programmes ne fonctionneront pas. Les stations seront longues au démarrage (recopie en local du répertoire profil situé sur le serveur), et longues à l'arrêt (recopie du profil local vers le répertoire du profil sur le serveur). Le répertoire du serveur contenant les profils grossira vite !

## Exercice

Vous devez commencer par créer un répertoire sur le serveur et le partager.  
Créez par exemple le répertoire D:\Profils et partagez ce répertoire avec Profils comme nom de partage.  
Mettez comme autorisations de partage :

Tout le monde : Modifier

Vérifiez que les permissions de sécurité possèdent au moins :

Administrateurs : Contrôle total

System : Contrôle total

Tout le monde : Modifier.

Dans le volet profil d'un utilisateur (par exemple de Dupond), mettez le chemin du profil :

\\ (nom du serveur) \Profils\%USERNAME%

*Vous mettrez bien entendu le nom réel de votre serveur.*

*Vous taperez %username% sans oublier les % ou, ce qui revient au même, vous taperez le nom de l'utilisateur sans les %.*

Ouvrez une session sur une station 2000 ou XP avec ce compte utilisateur (Dupond). Lorsque vous fermerez la session, le répertoire Dupond du serveur sera créé et recevra une copie de votre profil.

Ouvrez une session sur une autre station 2000 ou XP avec ce même compte utilisateur (Dupond) et vous retrouverez votre profil car le répertoire profil du serveur a été recopié en local dans votre répertoire profil.

## Profils utilisateurs itinérants obligatoires

### Principe

Il est possible d'imposer un profil à certains utilisateurs. Lorsqu'un utilisateur a utilisé au moins une fois son compte itinérant, le répertoire profil à son nom sur le serveur contient son profil.

En renommant le fichier ntuser.dat situé dans ce répertoire en ntuser.man, la station comprendra qu'il s'agit d'un profil obligatoire. Le profil sera alors copié du serveur vers la station lors de l'ouverture de session mais ne sera pas copié de la station vers le serveur lors de la fermeture de session.

### Exercice

Sur le serveur, recherchez dans le répertoire D:\Profils\Dupond le fichier ntuser.dat et renommez-le en ntuser.man (ntuser.dat ne doit plus exister).

*Ne confondez pas avec le fichier texte ntuser.dat.txt ou ntuser.dat.log qui peut éventuellement exister et qu'il est inutile de renommer.*

Ouvrez une session sur une station Windows 2000 ou XP pro en tant que Dupond. Faites des modifications, fermez la session et ouvrez une session sur la même station ou sur une autre station. Est-ce que vous retrouvez les modifications que vous venez de faire sur la première station ?

Enregistrez un document dans "Mes documents". Est-ce que vous retrouvez votre document après fermeture et ouverture de session sur cette station ? En ouvrant une session sur une autre station ?

### Profil obligatoire commun à plusieurs utilisateurs

Lorsque le nombre d'utilisateurs est important, il devient intéressant de ne stocker qu'un ou quelques profils sur le serveur et d'imposer un profil aux utilisateurs.

Il serait en effet fastidieux de rendre obligatoire les profils de nombreux utilisateurs. On peut utiliser le même répertoire profil pour définir le profil obligatoire de plusieurs utilisateurs.

Ouvrir une session sur une station 2000 ou XP avec un compte de préférence du domaine, ayant les droits d'administrateur sur la station, et n'ayant pas un profil itinérant. Utilisez tous les programmes au moins une fois afin que leur paramétrage utilisateur soit retenu.

Ouvrez une session sur cette station avec le compte Administrateur du domaine (depuis l'arrivée des XP, il est préférable d'utiliser ce compte car le répertoire qui va être créé sur le serveur doit avoir Administrateurs comme propriétaire).

Dans le "Panneau de configuration" et "System" utilisez le volet profil utilisateurs. Placez-vous sur le profil du compte utilisé précédemment et faites "Copier dans...". Indiquez comme chemin \\ (nom du serveur) \Profils\commun

Avant de valider, on peut constater que ce répertoire sera autorisé seulement à vous or nous voulons qu'il soit utilisé également par d'autres. Utilisez le bouton "**Modifier...**" pour donner l'autorisation au groupe "**Tout le monde**".

Si le répertoire commun n'existe pas, il sera automatiquement créé.

Lorsque vous validez, le répertoire commun est créé et le profil est copié dans commun. De plus les autorisations de sécurité permettront à tout le monde d'accéder à ce répertoire.

Cette méthode présente cependant un défaut. En effet nous venons de donner à "Tout le monde" le droit de modifier le contenu de ce répertoire. En modifiant les autorisations de partage du répertoire "Profils" avec Administrateurs en Contrôle total et Tout le monde en Lecture, ce problème n'existe plus.

## Oublier les profils itinérants sur la station

Il est possible de faire en sorte que le profil itinérant de l'utilisateur soit supprimé sur la station lorsque celui-ci ferme la session. Pour cela il suffit d'ajouter une valeur dans la base de registre de la station.

Créez un fichier de type texte avec comme extension .reg et mettez ceci dans ce fichier :

```
REGEDIT4
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon]  
"DeleteRoamingCache"=dword:00000001
```

Exécutez ce fichier sur la station.

Seuls les profils itinérants sont concernés par ce paramétrage, les autres profils ne sont pas supprimés. On utilisera en général cette solution avec les profils itinérants obligatoires.

Il est également possible d'utiliser les stratégies de groupe sur le serveur afin de demander à un ensemble de stations de supprimer les profils itinérants à la fermeture de session. Cela se fait en activant la propriété "Supprimer les copies mises en cache des profils itinérants".

## Comment ne plus rendre obligatoire un profil

Sur le serveur, avec "Utilisateurs et ordinateurs Active Directory", supprimez le chemin du profil pour cet utilisateur.

Sur les stations où cet utilisateur a ouvert une session, vous remarquerez certainement que le profil reste obligatoire. Ceci est dû au fait que le fichier ntuser.man a été copié dans le répertoire du profil de cet utilisateur sur les stations.

Vous pouvez alors ouvrir la station avec un compte d'administrateur pour supprimer le profil ou encore seulement renommer ou supprimer le fichier ntuser.man dans le répertoire du profil de cet utilisateur.

## Profils itinérants obligatoires et OU

Les stratégies de groupe des OU qui concernent les utilisateurs ne s'appliquent pas avec un profil itinérant obligatoire.

# Relations d'approbation

## A quoi ça sert ?

Lorsque deux serveurs appartiennent au même domaine, il est possible d'accéder aux comptes utilisateurs indifféremment à partir de chaque serveur. On ne parle pas de relation d'approbation puisqu'en fait, chaque serveur agit sur la même base de données de l'annuaire.

On ne peut parler de relation d'approbation qu'entre deux domaines.

Lorsqu'une relation d'approbation est établie entre deux domaines, il est possible d'accéder aux comptes utilisateurs d'un domaine à partir de l'autre.

Certaines relations d'approbations sont automatiques. C'est le cas des domaines enfants (info.lycee.priv et lycee.priv).

Lorsque les domaines sont indépendants (comme info.priv et tertiaire.priv), et qu'aucune relation d'approbation n'a été établie entre les deux, un utilisateur d'un domaine n'a pas d'accès à l'autre domaine. En particulier, un administrateur d'un domaine n'a pas accès aux comptes de l'autre domaine. Les stations 2000 ou XP d'un domaine ne permettent pas à un utilisateur d'un autre domaine d'ouvrir une session.

*Les stations 9x permettent de taper le nom du domaine alors que les stations 2000 ou XP ne permettent que le choix dans une liste. Dans ce cas, la liste est limitée au nom de la station et au nom du domaine dans lequel la station est inscrite.*

En établissant une relation d'approbation entre deux domaines on permet :

- Aux utilisateurs d'un domaine d'ouvrir une session sur les stations appartenant à l'autre domaine.
- Aux utilisateurs d'un domaine d'avoir des droits sur les ressources de l'autre domaine.
- Aux administrateurs d'un domaine d'avoir accès aux comptes de l'autre domaine.

*Attention : Si vous donnez le même mot de passe au compte Administrateur de deux domaines, vous pourrez constater qu'à partir d'un domaine vous aurez certains droits sur l'autre domaine, même sans relation d'approbation.*

La suite montre la méthode avec des serveurs 2000 et NT4.

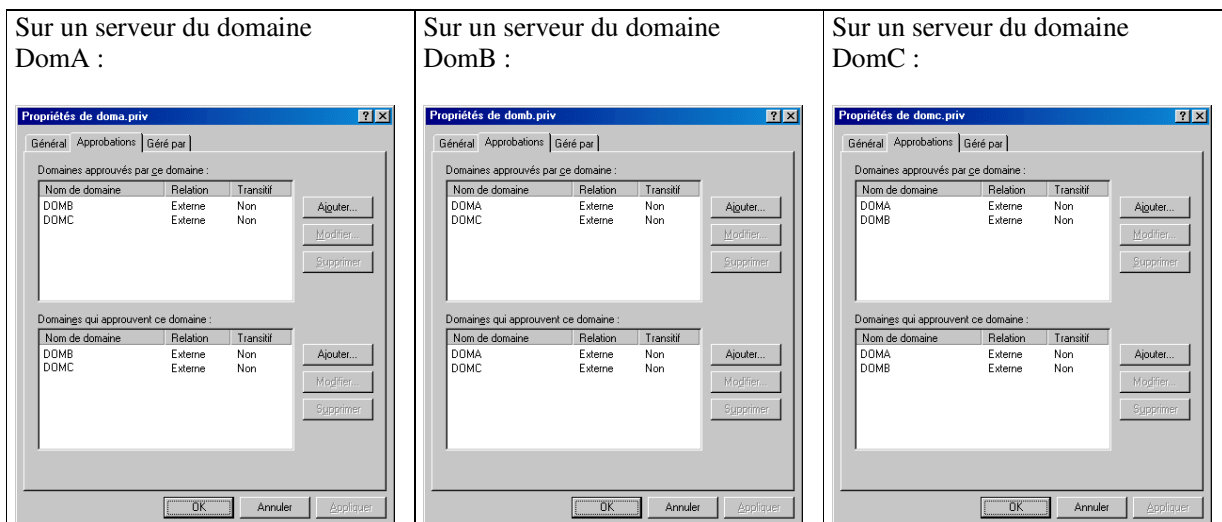
Avec des serveurs 2003, il est plus facile d'établir cette relation car il suffit de le faire sur un des serveurs. Le mot de passe de l'administrateur de l'autre domaine est demandé et la relation bidirectionnelle s'établit automatiquement.

## Vocabulaire :

DomX approuve DomY signifie que DomX accepte que les utilisateurs de DomY utilisent les ressources des serveurs de DomX.

*On pourrait dire aussi que DomX fait confiance aux utilisateurs de DomY.*

Le but est d'arriver à ceci :



## Avant de commencer

Avant de pouvoir établir des relations d'approbation, il est nécessaire que les serveurs soient à la même heure et de paramétrer le serveur DNS de chaque serveur afin qu'il connaisse l'autre domaine.

**Synchroniser l'heure.** Si les deux serveurs utilisent la même base de temps alors ils sont déjà à la même heure. Pour les mettre à la même base de temps vous pouvez taper sur les deux serveurs

```
net time /setsntp:ntp.unice.fr
```

ou encore

```
net time /setsntp:time.windows.com
```

Adresse donnant une liste de serveurs de temps :

[http://www.cru.fr/NTP/serveurs\\_francais.html](http://www.cru.fr/NTP/serveurs_francais.html)

L'effet n'étant pas immédiat, si vous voulez le rendre effectif immédiatement, arrêtez le service W32time et redémarrez-le :

```
net stop w32time
net start w32time
```

Si vous ne voulez plus de cette synchronisation avec un serveur de temps tapez :

```
net time /setsntp:
```

Si votre serveur est un 2003, vous pouvez faire la même chose en allant dans le volet "Temps Internet" que vous trouverez dans les Propriétés de "Date et heure".

Sans utiliser un serveur de temps, on peut seulement vérifier qu'à quelques secondes près les deux serveurs ont la même heure (en plus d'être au même jour, dans le même fuseau horaire et avec le même choix pour l'heure d'été).

**Modifier les serveurs DNS.** Sur l'un des serveurs par exemple SERVA1, allez dans DNS, dans la zone de recherche directe et allez dans les propriétés de votre zone (clic droit sur doma.priv et propriétés).

Dans le volet "Transfert de zone", autorisez le transfert de zone.

Sur l'autre serveur (SERVB1) faites un clic droit sur "Zone de recherche directe" et créez une nouvelle zone secondaire. Donnez comme nom le domaine du premier serveur (doma.priv) et indiquez l'adresse IP du premier serveur.

La copie de la zone doma.priv dans la zone secondaire du serveur DNS de SERVB1 peut prendre quelques minutes faites actualiser ou encore demandez le "Transfert à partir du maître".

Faites le même travail dans l'autre sens. De cette façon chaque serveur DNS possède une copie de la zone de recherche directe de l'autre serveur DNS.

## Etablir les relations d'approbation

Sur Windows 2000 Serveur, ouvrez "domaines et approbations Active Directory". Faites un clic droit sur votre domaine et choisissez "Propriétés". Dans le volet "Approbations". Ajoutez DomB dans la liste des "Domaines autorisés à approuver" ou "Domaines qui approuvent ce domaine" (la partie du bas). Donnez un mot de passe quelconque et confirmez-le.

Donnez à l'administrateur du domaine DomB le mot de passe que vous venez de taper lorsque vous avez ajouté DomB.

Cet administrateur peut ajouter DomA dans la liste des "Domaines approuvés" (la partie du haut) et doit pour cela taper le mot de passe que vous venez de lui donner.

*A partir de maintenant, un utilisateur de DomA est approuvé par le domaine DomB (l'utilisateur peut donc avoir le droit d'accéder aux ressources des serveurs de DomB). Cela signifie, qu'il peut ouvrir une session sur un ordinateur appartenant au domaine DomB en utilisant son nom, son mot de passe et en choisissant DomA comme nom de domaine.*

*Cet utilisateur a donc des droits sur des ressources de DomA et de DomB.*

*Un utilisateur appartenant au domaine DomB ne peut pas pour l'instant, ouvrir une session sur un ordinateur appartenant au domaine DomA.*

Demandez à l'administrateur de DomB d'ajouter DomA dans la liste de ses "Domaines autorisés à approuver" ou "Domaines qui approuvent ce domaine" (la partie du bas) et demandez-lui quel mot de passe il a utilisé. Ajoutez alors DomB dans votre liste des "Domaines approuvés" (la partie du haut).

La relation d'approbation est maintenant **bidirectionnelle**.

Recommencez avec DomA et DomC

Recommencez avec DomB et DomC

Maintenant tout utilisateur peut venir sur n'importe quelle station appartenant à l'un des trois domaines.

*Si vous ajoutez un domaine dans la liste des "Domaines qui approuvent ce domaine", ne cherchez pas à vérifier la relation d'approbation tout de suite, vous devez faire la partie correspondante dans l'autre domaine avant de pouvoir effectuer cette vérification.*

# Bureau à distance

En installant le **Service terminal server** (Windows 2000 serveur) ou le **bureau à distance** (Windows 2003 serveur) sur votre serveur, vous pourrez à partir d'une station même éloignée, prendre le contrôle de votre serveur.

Il est donc capital d'avoir pris conscience que les mots de passe doivent être suffisamment compliqués pour ne pas être devinés !

*Un logiciel comme Winvnc permet également de prendre le contrôle d'un ordinateur distant. Winvnc n'est pas limité à Windows 2000 ou 2003 serveur mais Winvnc est beaucoup plus lent que le bureau à distance.*

## Installation sur le serveur

### Si votre serveur est un 2000 :

Dans "Ajout/Suppression de programmes" et "Ajouter/Supprimer des composants Windows", cochez le composant "Services Terminal Server".

Choisissez "Mode Administration à distance". À la fin de l'installation, vous serez informé qu'il faut redémarrer le serveur.

### Si votre serveur est un 2003

Dans les propriétés système, allez dans le volet "Utilisation à distance" et cochez "Autoriser les utilisateurs à se connecter à distance à cet ordinateur".

## Installation sur le client

La solution proposée dans le paragraphe "En pratique" ci-après est la solution que j'utilise habituellement.

### Si votre serveur est un 2000 :

Sur le serveur où le Service Terminal Server est installé, allez dans les "Outils d'administrations" puis "Créateur de client Terminal Server". Choisissez "Client Terminal Server pour Windows x86 32 bits". Vous obtenez ainsi deux disquettes.

Pour installer le client (par exemple sur un Windows 98), exécutez le programme Setup de la première disquette. Une autre solution consiste à utiliser les deux fichiers comme pour un serveur 2003.

### Si votre serveur est un 2003

Il suffit de copier les fichiers mstsc.exe et mstscax.dll qui sont dans le répertoire System32 du serveur 2003 où le bureau à distance est installé et de les mettre-les dans un répertoire quelconque accessible de l'ordinateur client.

*Ces deux fichiers conviennent également lorsque le serveur est un Windows 2000.*

### En pratique :

Créez un répertoire sur le serveur 2000 ou 2003 dans lequel vous copiez ces deux fichiers. Partagez ce répertoire en lui donnant par exemple comme nom de partage **distance\$**. On pourra donner des autorisations en lecture pour tout le monde pour ce répertoire.

A partir d'une station quelconque (de Windows 98 à XP) sans avoir à installer quelque chose, tapez le chemin \\(nom du serveur)distance\$ et exécutez mstsc.exe.

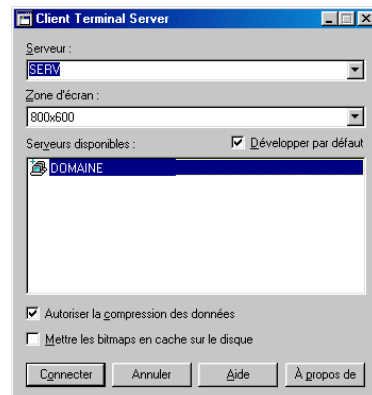
## Utilisation

Sur le client (98 XP...), exécutez mstsc ou, si vous avez installé le client, utilisez "Client Terminal Server".

Si vous êtes en réseau local, tapez le nom de votre serveur ou son adresse IP.

Vous serez amené à ouvrir une session sur votre serveur. Vous devrez donc utiliser un compte ayant le droit d'ouvrir une session (Administrateur par exemple).

**ATTENTION :** Il est très important de donner des mots de passe sérieux à tous les comptes utilisateurs ayant le droit d'ouvrir une session sur le serveur, spécialement si vous donnez la possibilité d'accéder à votre serveur à partir d'Internet.



## Passer un routeur

Le bureau à distance ou le service Terminal Server utilise le port 3389. Si votre serveur est derrière un routeur, vous devrez paramétrer votre routeur pour ouvrir le port 3389 et le diriger vers votre serveur.

## Pare-feu

Si vous utilisez un pare-feu, vérifiez que le port 3389 est autorisé.

# Internet Information Serveur

## Principe

Pour pouvoir utiliser cette fonctionnalité, IIS (Internet Information Serveur) doit être installé sur le serveur.

Si IIS n'est pas installé, vous pouvez l'installer.

Avec Windows NT4 Serveur, n'utilisez pas le CD de Windows pour installer IIS. En effet l'installation remplacerait certains fichiers par de vieux fichiers rendant certaines fonctionnalités indisponibles (en particulier la gestion des bases de données par ODBC).

*Si vous avez fait cette installation, il sera certainement nécessaire de réinstaller ODBC.*

L'installation de IIS sur un NT4 se fera à partir de **NTOptionPackSetupFiles** que vous pouvez télécharger sur le site de Microsoft. Ceci vous permettra d'obtenir un IIS version 4.

Avec Windows 2000 Serveur, allez dans "Ajout/Suppression de programmes", "Ajouter/Supprimer des composants Windows" et "Service Internet IIS"

Avec Windows 2003 Serveur, allez dans "Gérer votre serveur" et ajoutez le rôle IIS.

Rappel : Lorsque vous venez d'installer un composant à partir du CD de Windows NT, pensez à appliquer à nouveau le service pack pour que les fichiers installés à partir du CD soient remplacés par les versions récentes.

IIS permet d'utiliser votre serveur en serveur WEB. Par défaut, un seul site est prévu mais il est possible d'en ajouter.

Si votre serveur s'appelle serveur, le site principal est accessible à partir des navigateurs des stations à l'adresse

`http://serveur`

Si votre domaine s'appelle dom.priv, vous pouvez également utiliser

`http://serveur.dom.priv`

## Site par défaut

Le site par défaut est situé (sauf choix différent lors de l'installation) dans le répertoire C:\inetpub\wwwroot

Dans ce répertoire, mettez un fichier Default.htm correspondant à la page principale de votre site Web.

A partir du serveur ou d'une station, utilisez votre navigateur et tapez l'adresse `http://serveur`

*Vous remplacerez serveur par le nom réel de votre serveur.*

*Vous pouvez également utiliser le domaine `http://serveur.dom.priv` si votre serveur DNS est opérationnel.*

## Sous-sites

Créez un répertoire qui contiendra votre sous-site. On pourra créer ce répertoire dans C:\inetpub mais ce n'est pas obligatoire. Soit C:\inetpub\RepPourEssai ce répertoire.

Dans les "Outils d'administration", choisissez "Gestionnaire des services Internet".

Placez-vous sur "Site Web par défaut" et faites "Action", "Nouveau", "Répertoire virtuel". Un assistant démarre...

Mettez un alias. Il s'agit du nom qui sera utilisé pour accéder à ce sous-site. Ceci peut être comparé au nom de partage d'un répertoire. Soit Essai cet alias.

Indiquez le répertoire de votre sous-site (C:\inetpub\RepPourEssai).

Placez au moins un fichier Default.htm dans C:\inetpub\RepPourEssai.

Vérifiez le bon fonctionnement de votre sous-site à partir d'un navigateur en tapant  
<http://serveur/essai>

## FTP

Par défaut, avec Windows 2000 serveur, le serveur FTP est opérationnel et permet l'accès anonyme en lecture seule.

Pour installer le serveur FTP sur un Windows 2003 serveur, allez dans "Ajout et suppression de programmes", "Ajouter ou supprimer des composants Windows". Placez-vous sur "Serveur d'application", utilisez le bouton "Détails...", placez-vous sur "Services IIS", utilisez le bouton "Détails..." et cochez "Service FTP".

Le répertoire pour le FTP (sauf choix différent lors de l'installation) est le répertoire C:\inetpub\ftproot

Placez un fichier dans C:\inetpub\ftproot et à partir d'un autre ordinateur, tapez dans votre navigateur :  
<ftp://serveur>

*Remplacez serveur par le nom réel de votre serveur.*

## Conseils

Évitez les espaces et les caractères particuliers (accents, cédilles...) dans les noms de répertoires et de fichiers dans vos répertoires Web ou ftp.

Prenez l'habitude de respecter les majuscules et minuscules, même si un serveur Windows ne fait pas la différence. En effet si vous voulez placer vos pages sur un autre serveur sur Internet, il est possible que cet autre serveur fasse la différence (serveur Linux par exemple).

En installant PHP.EXE sur votre serveur, vous pourrez profiter de la puissance du langage PHP dans la création de vos pages Web. Vous pouvez trouver la version win32 de PHP sur le site <http://www.php.net>

## Liens divers

Ces liens sont actuellement opérationnels mais ils risquent de ne plus l'être dans l'avenir.

Gestion des disques :

<http://raphaello.univ-fcomte.fr/W2K/06-Administration/OutilsDisque.htm>

Historique des différentes versions de Windows

[http://www.ac-nancy-metz.fr/services/tec/les\\_os.htm](http://www.ac-nancy-metz.fr/services/tec/les_os.htm)

# Rôles des serveurs d'un domaine

## Cinq rôles

Chacun des deux rôles suivants doit être joué par un et un seul serveur de la forêt :

- Contrôleur de schéma
- Maître d'attribution de noms de domaine

Chacun des trois rôles suivants doit être joué par un et un seul serveur du domaine :

- Maître RID
- Émulateur PDC (contrôleur principal de domaine)
- Maître d'infrastructure.

### **Contrôleur de schéma**

Ce serveur a une vue d'ensemble sur les domaines de la forêt. Il permet des ajouts, des déplacements et des suppressions de domaines au sein de la forêt.

### **Maître d'attribution de noms de domaine**

Ce serveur vérifie que le nom du domaine n'est pas déjà utilisé dans la forêt.

### **Maître RID**

Un serveur de domaine dispose d'un ensemble de SID pouvant être utilisés par exemple pour la création d'un nouvel utilisateur. Lorsqu'il n'a plus assez de SID en réserve, il demande au maître RID un nouvel ensemble de SID. Si le renouvellement ne peut pas se faire, et qu'il a épuisé tous ses SID, toute création se solde par une erreur.

### **Émulateur PDC (contrôleur principal de domaine)**

Ce serveur traite les modifications de mot de passe et réplique les mises à jour sur les autres serveurs du domaine.

### **Maître d'infrastructure**

Ce serveur traite les modifications des groupes et des utilisateurs et réplique les changements sur les autres serveurs du domaine.

## Suppression d'un serveur d'un domaine

Si vous avez l'intention de supprimer le serveur qui joue ces rôles, il faudra commencer par donner ces rôles à un autre serveur du domaine. Les rôles seront donc déplacés.

Si le serveur jouant ces rôles tombe en panne, il faudra forcer l'attribution de ces rôles sur un autre serveur du domaine.

"Utilisateurs et ordinateurs active directory" permet de changer les rôles RID, PDC et Infrastructure. Faire un clic droit à la racine de l'arborescence et choisir "Maître d'opérations".

"Domaines et approbation Active Directory" permet de changer le rôle "Maître d'opération d'attribution de nom de domaine". Faire un clic droit à la racine de l'arborescence et choisir "Maître d'opérations".

Si on a "Schéma Active Directory" dans les outils d'administration, cela permet de changer le rôle "Maître d'opération schéma Active Directory". Faire un clic droit à la racine de l'arborescence et choisir "Maître d'opérations". Si on ne l'a pas, on peut utiliser ntdsutil.

## Utilisation de ntdsutil

Utilisation de ntdsutil pour changer le rôle "Schéma Active Directory" :  
Dans une fenêtre dos taper : **ntdsutil**

A toutes les étapes vous pouvez taper help pour obtenir de l'aide

tapez : **roles**  
tapez : **connections**  
tapez : **connect to server XXX** (où XXX est le nom du serveur)  
tapez : **quit**  
tapez : **transfer schema master**  
tapez : **quit**  
tapez : **quit**

Si le serveur jouant les 5 rôles est tombé en panne définitivement, il faudra forcer un autre serveur du domaine à jouer ces 5 rôles. On pourra alors utiliser ntdsutil de cette façon :

tapez : **roles**  
tapez : **connections**  
tapez : **connect to server XXX** (où XXX est le nom du serveur)  
tapez : **quit**  
tapez : **seize schema master**  
tapez : **seize domain naming master**  
tapez : **seize RID master**  
tapez : **seize PDC**  
tapez : **seize infrastructure master**  
tapez : **quit**  
tapez : **quit**

Il est possible que vous obteniez un message précisant que le serveur qui avait ces rôles n'a pas pu être contacté. Un tel message dans notre cas pourra être ignoré.

Un "nettoyage" pourra ensuite être fait dans "Utilisateurs et ordinateurs active directory" et "Sites et service Active Directory" afin de ne pas laisser de trace de l'ancien serveur.

Pour connaître les rôles d'un serveur donné, dans ntdsutil :  
Tapez : **domain management**  
Tapez : **connections**  
Tapez : **connect to server** (où XXX est le nom du serveur)  
Tapez : **quit**  
Tapez : **select operation target**  
Tapez : **list roles for connected server**

# DFS, Système de fichiers distribués

Si vous avez plusieurs serveurs dans votre domaine vous pouvez profiter du système de fichiers distribués. Il faut au moins un serveur de domaine, les autres serveurs peuvent être des serveurs de domaine ou des serveurs membres.

Dans la suite je suppose que vous avez deux serveurs de domaine dans votre domaine. Je suppose que votre domaine s'appelle d2003.priv et que vos serveurs sont nommés SERV et SERV2003.

## Scénario

Vous avez un répertoire important et souvent utilisé qui doit toujours rester disponible pour les utilisateurs. Ce répertoire est sur SERV et s'appelle REPA.

Vous voulez que le deuxième serveur possède une copie de ce répertoire et que, en cas d'arrêt de SERV, les utilisateurs puissent accéder à la copie sans s'en rendre compte.

## Principe

Utiliser DFS sur un serveur pour effectuer une répllication de REPA situé sur SERV vers un répertoire partagé (que l'on peut nommer également REPA) sur SERV2003.

Toute modification de \\serv\repa sera répliquée automatiquement dans \\serv2003\repa

Toute modification de \\serv2003\repa sera répliquée automatiquement dans \\serv\repa

Les modifications sur la sécurité des répertoires ou fichiers de l'un des répertoires se répercuteront également sur l'autre. Les éventuelles partages à l'intérieur de RepA ne se répliquent pas.

Les utilisateurs pourront donc indifféremment accéder à \\serv\repa ou à \\serv2003\repa

Mieux, les utilisateurs pourront accéder à \\d2003.priv\repa et ce sera le serveur disponible qui sera effectivement utilisé. La répllication vers l'autre serveur étant automatique.

## Avantages, inconvénients

### Avantages

Les données sont disponibles même si l'un des serveurs est en panne.

Le trafic réseau se répartit automatiquement entre les stations et les deux serveurs.

### Inconvénients

Un trafic réseau supplémentaire est généré entre les deux serveurs pour la répllication des répertoires.

Des lenteurs peuvent se produire si l'un des serveurs n'est pas présent.

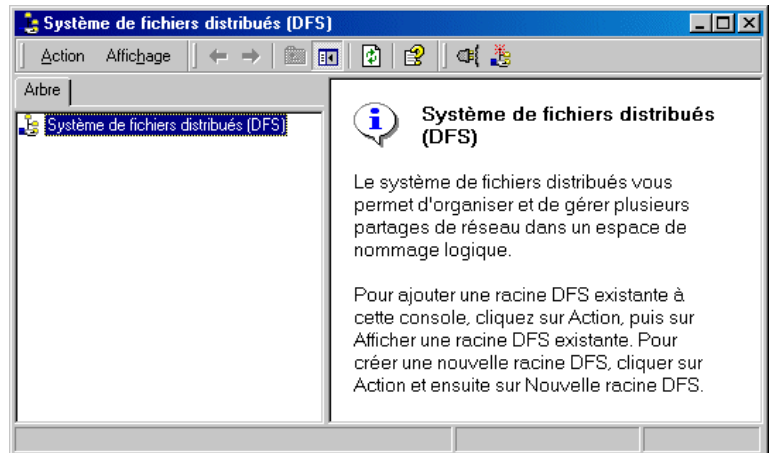
## Création de la racine DFS

Le système de fichiers distribués (DFS) est installé par défaut. Il est accessible par les "Outils d'administration".

Windows 2000 serveur et Windows 2003 serveur standard édition sont limités à une racine DFS.

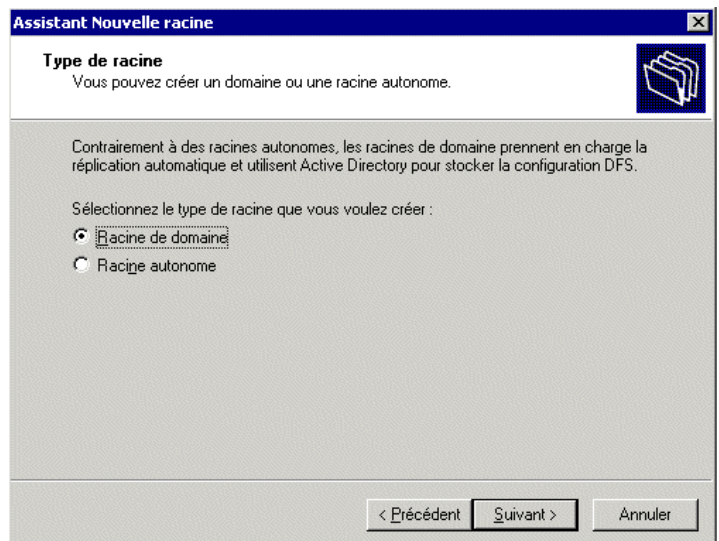
Nous travaillerons donc essentiellement au niveau des liens DFS.

"Outils d'administration", "Système de fichiers distribués (DFS)

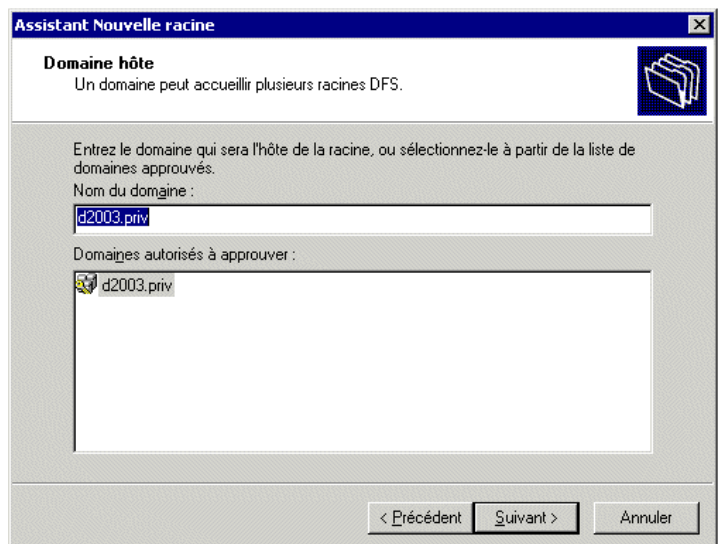


Faire un clic droit sur "Système de fichiers distribués (DFS)" et "Nouvelle racine". Un assistant démarre.

Choisissez "Racine de domaine"

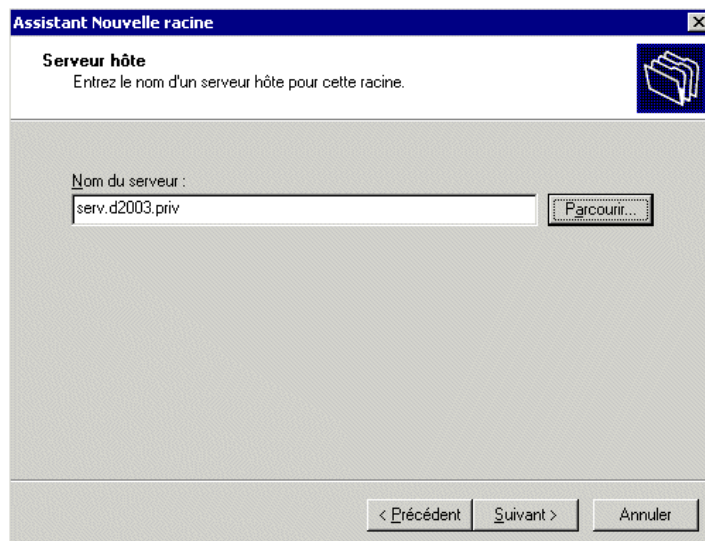


Laissez le nom du domaine proposé.



Choisissez un serveur. Comme le système DFS sera publié dans Active directory, le choix du serveur n'est pas important.

Ce serveur devra cependant être opérationnel si on utilise les chemins \\d2003\... ou \\d2003.priv\... sur les stations.

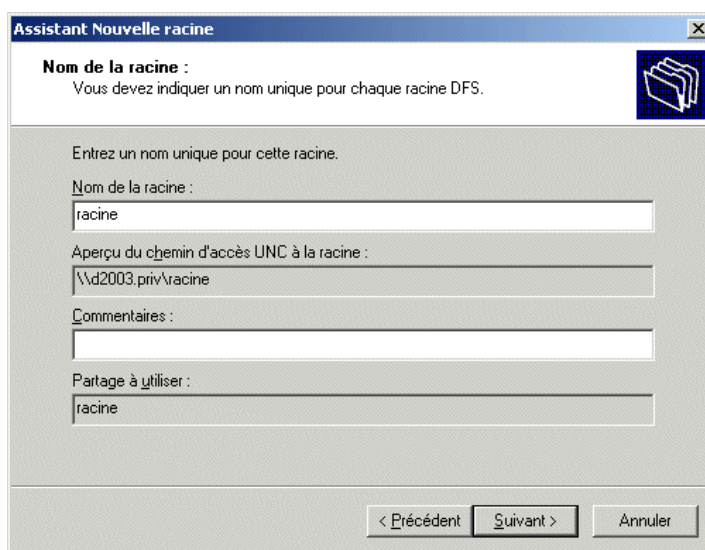


Avant de continuer, créez un nouveau répertoire C:\Racine et partagez ce répertoire en donnant les autorisations qui conviennent.

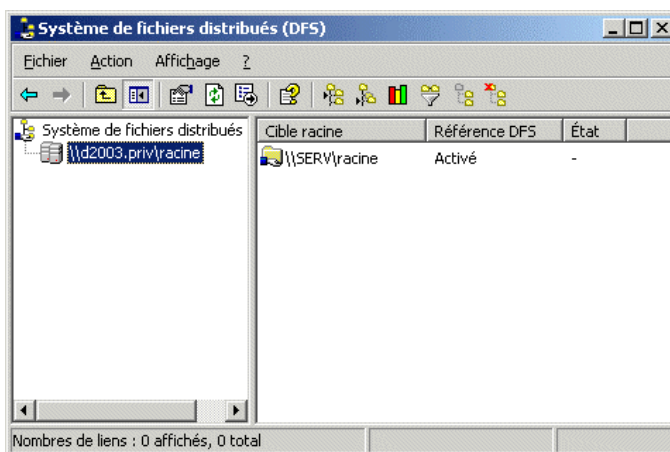
Si vous voulez que les utilisateurs puissent modifier mettez contrôle total à tout le monde pour les autorisations de partage, et donnez au moins le droit de modifier aux utilisateurs pour les autorisations de sécurité.

Indiquez le nom de la racine. Ce nom sera visible sur les stations comme un nom de partage du domaine.

La copie d'écran montre que la racine a été nommée "racine" (même nom que le répertoire créé ci-dessus).



Résultat obtenu



## Création des liens

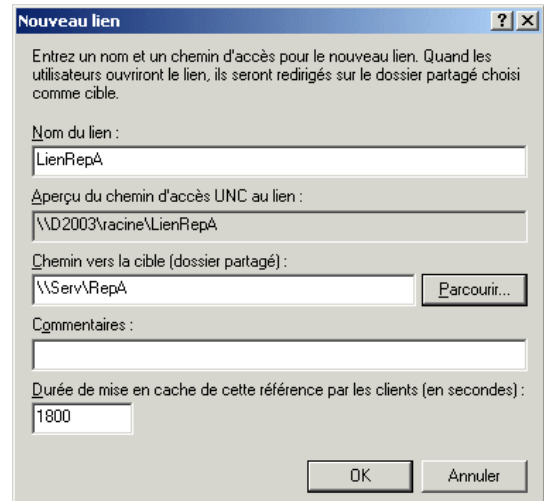
Nous allons créer un lien entre le répertoire REPA situé sur SERV et le répertoire REPA situé sur SERV2003.

Remarques : Il n'est pas nécessaire que les répertoires soient de même nom sur les deux serveurs. Avec un troisième serveur, on pourrait créer un lien entre trois répertoires.

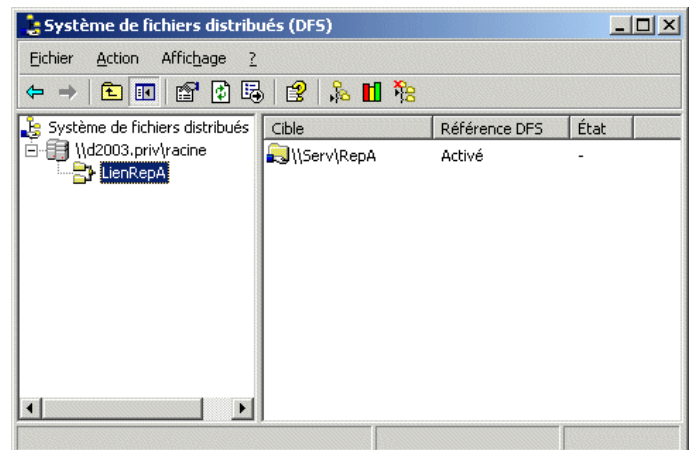
Clic droit sur la racine et "Nouveau lien".  
Vous pouvez donner le nom que vous voulez au lien. Par exemple "RepA".

Pour éviter de confondre le nom du répertoire et le nom du lien, dans la suite je nommerai le lien "LienRepA" (ce qui sera moins pratique que RepA mais plus pédagogique).

Le chemin vers la cible pointe sur le partage RepA de SERV



Résultat obtenu.

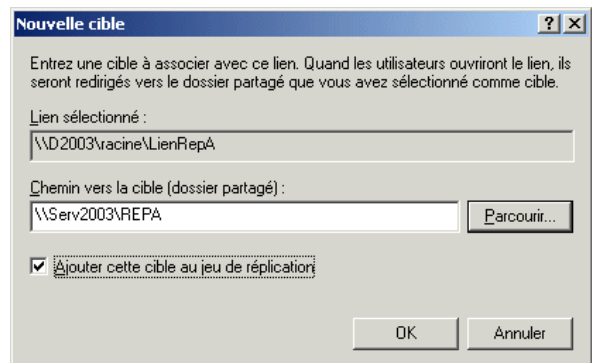


Il est nécessaire d'avoir au moins une deuxième cible pour ce lien afin de pouvoir activer la réplication.

Pour créer la deuxième cible, faites un clic droit sur le lien et "Nouvelle cible".

Choisissez le répertoire RepA de SERV2003 comme cible.

Validez. Il reste maintenant à configurer la réplication.



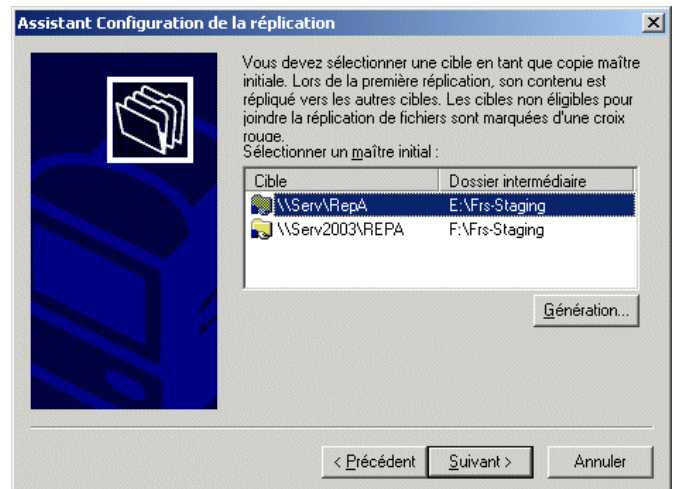
## Réplication automatique

La réplication va permettre au système DFS de répercuter automatiquement les modifications faites dans un répertoire vers l'autre répertoire.

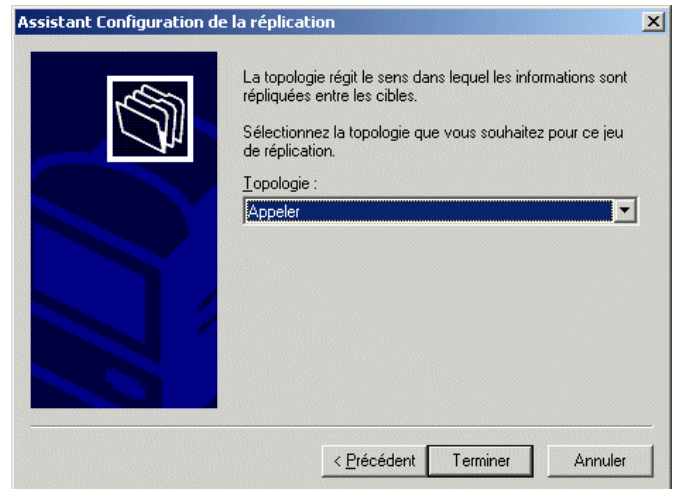
Si l'assistant de configuration de la réplication n'est pas démarré, faites un clic droit sur le lien et "réplication"

Si vos deux répertoires RepA ne sont pas vides, **il est important de bien choisir** ici le répertoire contenant actuellement les données.

Le répertoire choisi sera automatiquement recopié (synchronisé) vers l'autre répertoire. Le répertoire choisi est nommé "maître initial".

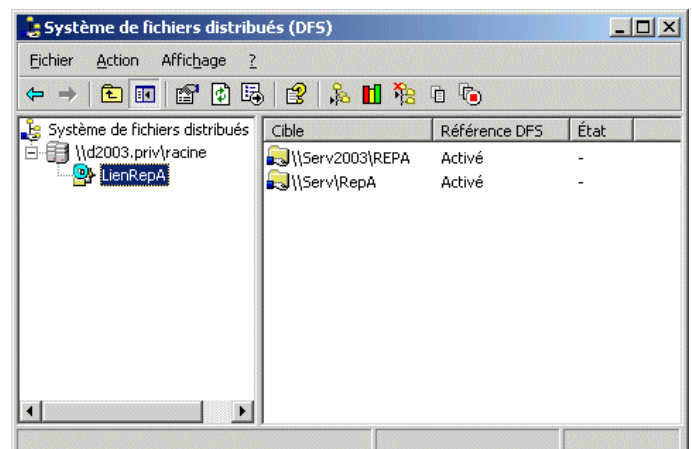


L'écran suivant demande le type de méthode à utiliser pour la réplication. Choisissez "Appeler".



Résultat obtenu.

Vous pouvez maintenant observer le répertoire RepA situé sur SERV2003, il va d'ici quelques minutes automatiquement devenir identique au répertoire RepA de SERV.



Il est maintenant possible à partir d'une station d'accéder à cette ressource, avec un chemin \\ (nom du domaine) \ (nom de la racine) \ nom du lien DFS \ ...

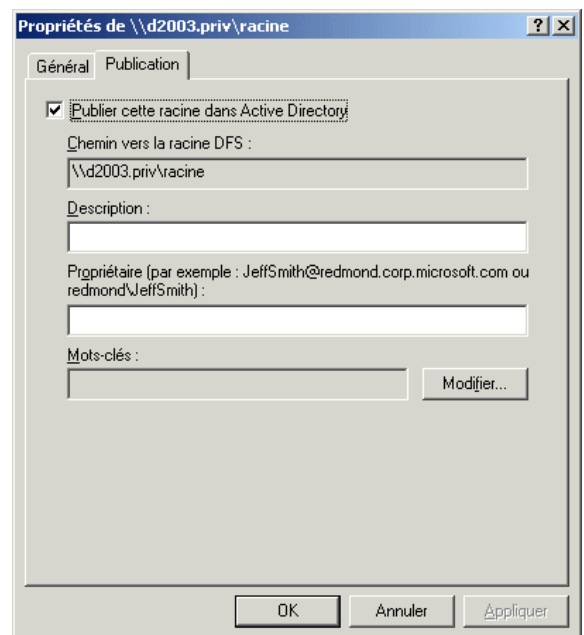
Pour accéder à la ressource, vous pouvez donc indifféremment utiliser un des chemins suivants :

\\Serv\Racine\RepA	(à condition que Serv soit opérationnel)
\\Ser2003\Racine\RepA	(à condition que Serv2003 soit opérationnel)
\\d2003\Racine\RepA	(à condition que Serv soit opérationnel)
\\d2003.priv\Racine\RepA	(à condition que Serv soit opérationnel)

## Publier la racine dans Active Directory

Cette partie n'existe que sur Windows 2003 serveur.

Faites un clic droit sur la racine et dans les "Propriétés" choisissez "Publication".  
Cochez "Publier cette racine dans Active Directory".



# Création d'un fichier MSI

## Principe

Certains programmes sont proposés avec une installation à partir d'un fichier ayant comme extension MSI. Ce type de fichier d'installation donne la possibilité de faire des installations automatiques.

Si votre programme ne s'installe pas à l'aide d'un fichier MSI, vous pouvez créer pour ce programme votre fichier MSI à l'aide du programme **WinINSTALL Discover**

Il est vivement conseillé d'utiliser une station ayant seulement le système d'exploitation installé. Ce travail se fait en suivant les étapes suivantes :

- 1) Sur une station où Windows est fraîchement installé, installez WinINSTALL Discover et sauvegardez la station afin de pouvoir faire plus tard d'autres fichiers MSI.
- 2) Démarrez WinINSTALL Discover et répondez aux différentes questions.
- 3) WinINSTALL Discover scanne alors votre disque afin de retenir ce qu'il contient.
- 4) WinINSTALL Discover vous demande ensuite d'effectuer l'installation du programme.
- 5) WinINSTALL Discover scanne une deuxième fois votre disque afin de déterminer ce qu'a modifié le programme d'installation.
- 6) WinINSTALL Discover fabrique un répertoire contenant les fichiers nécessaires à l'installation et en particulier le fichier MSI
- 7) Il est possible ensuite d'améliorer le fichier MSI à l'aide de "Software console" en supprimant certaines parties inutiles.

## Installation de WinINSTALL Discover

Installez SWIADMLE.MSI que vous pouvez trouver sur le CD de Windows 2000 serveur dans le répertoire \VALUEADD\3RDPARTY\MGMT

Deux raccourcis sont créés :

Le programme WinINSTALL Discover permet de créer un fichier MSI

Le programme WinINSTALL Software Console permet de corriger le fichier MSI.



A ce stade il serait souhaitable de sauvegarder votre station.

## Exemple concret

L'installation du programme GIMP (logiciel gratuit de dessin venant du monde linux) suppose que vous avez déjà installé "gtk+" avant de pouvoir installer "gimp". Je vous propose de créer un fichier msi effectuant ces deux installations en une seule.

Il va être possible avec Gimp de créer un fichier MSI qui permettra d'installer ce logiciel alors que personne n'a encore ouvert une session. Il sera alors possible d'effectuer un déploiement automatique sur un ensemble de stations ayant la même version de Windows.

Tous les logiciels ne permettent pas la création d'un fichier MSI. L'idéal étant bien sûr de disposer d'un programme d'installation sous forme de fichier MSI fourni par le créateur du programme.

Préparez sur le serveur un répertoire en lecture seule pour tout le monde mais avec le droit de modification pour vous.

Dans la suite je suppose que le répertoire est partagé sous le nom "logiciels".

\\serveur\logiciels

## Première exécution de VERITAS Discover

Exécutez VERITAS Discover.

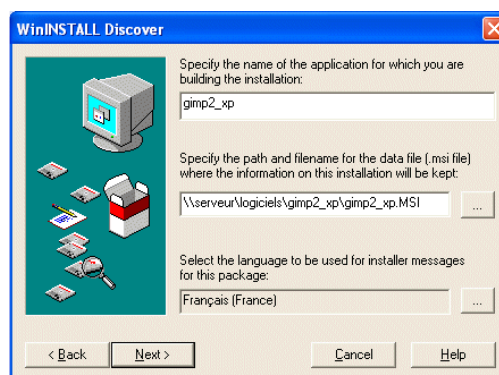


Indiquez le nom que vous voulez pour votre package.

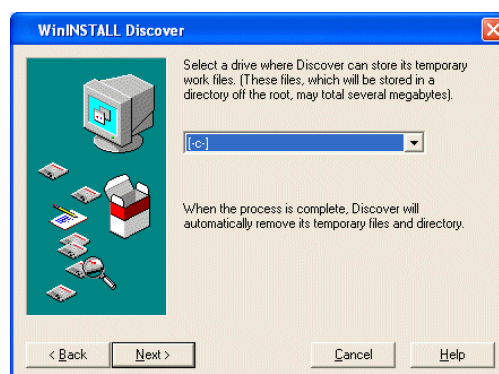
Donnez le chemin et le nom du fichier MSI à créer. Ce chemin devrait ressembler à ceci :

\\serveur\logiciels\gimp\gtk\_et\_gimp.msi

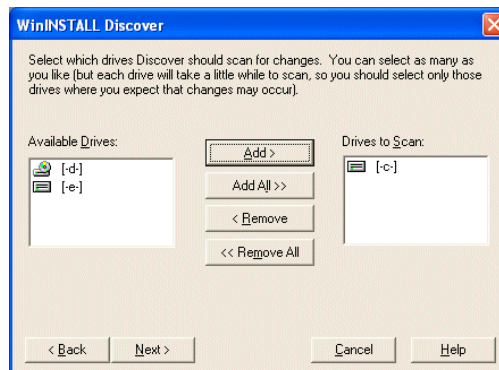
Le répertoire gimp sera créé et contiendra entre autres le fichier gtk\_et\_gimp.msi



Si votre station comporte plusieurs partitions, l'étape suivante consiste à choisir la partition ayant le plus de place libre à utiliser en tant qu'espace de travail temporaire pour Discover. En général, vous pourrez laisser C:



Puis Discover vous demande quels disques doivent être scannés. Ajoutez C dans la colonne "Drives to scan".



L'écran suivant vous permet d'ignorer certains fichiers ou répertoires.

- Si vous utilisez IACA, placez-vous sur C:\Windows\Profil et faites "Add". Cela ajoute la ligne

`C:\Windows\Profil\`

- Placez-vous sur "C:\Documents and settings" et faites "Add". Cela ajoute la ligne

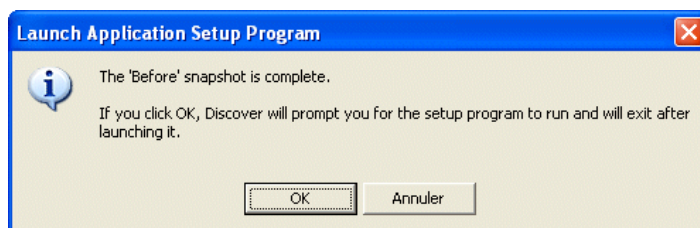
`C:\Documents and settings\`

- Utilisez le bouton "Files & Wildcard Entrées", placez-vous sur le répertoire C:\Windows\Prefetch laissez \*.\* et faites "Ouvrir". Cela ajoute la ligne

`C:\Windows\Prefetch\*.*`

Discover est prêt.

Tout ce que vous faites maintenant sera retenu dans le package.



## Installation de Gimp

Gimp utilise un répertoire qu'il place normalement dans Documents and Settings\nom de l'utilisateur. Il est plus pratique de modifier ceci en ajoutant la variable d'environnement système GIMP2\_DIRECTORY et en faisant pointer cette variable vers un répertoire comme C:\Gimp2

Pour ajouter cette variable d'environnement allez dans les propriétés du poste de travail, dans le volet "Avancé" et "Variables d'environnement". En dessous de la zone "Variables systèmes", utilisez le bouton "Nouveau" et donnez comme nom exactement GIMP2\_DIRECTORY et comme valeur par exemple C:\Gimp2

Faites l'installation de GTK puis l'installation de GIMP.

On pourra sélectionner toutes les extensions proposées pour l'utilisation avec Gimp.

Il est conseillé de démarrer au moins une fois Gimp.



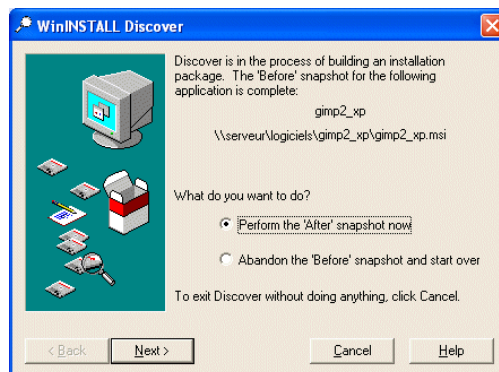
Evitez toute manipulation inutile.

## Deuxième exécution de VERITAS Discover

Exécutez à nouveau VERITAS Discover.

Laissez le choix proposé "Perform the 'After' snapshot now".

Discover va maintenant comparer C: et la base de registre avec l'état enregistré afin de déterminer ce qui a changé.



Le fichier MSI est créé avec quelques répertoires et fichiers nécessaires à l'installation.

La copie d'écran montre le contenu du répertoire obtenu.

Folder	Gimp2	
Folder	Program Files	
File	gimp2_xp.msi	385 Ko
File	gimp2_xp.NAI	461 Ko
File	gimp2_xp.REG	156 Ko

Lorsque le fichier MSI est créé, vous pouvez éventuellement le corriger en utilisant **WERITAS Software Console**

Quelques liens :

[http://www.laboratoire-microsoft.org/articles/network/creation\\_msi/](http://www.laboratoire-microsoft.org/articles/network/creation_msi/)

<http://www.ens-lyon.fr/Bibli/TSE/installations/msi.htm>

GTK et Gimp

<http://sourceforge.net>

ou en lien direct (sous réserve qu'il existe encore)

[http://sourceforge.net/project/showfiles.php?group\\_id=121075](http://sourceforge.net/project/showfiles.php?group_id=121075)

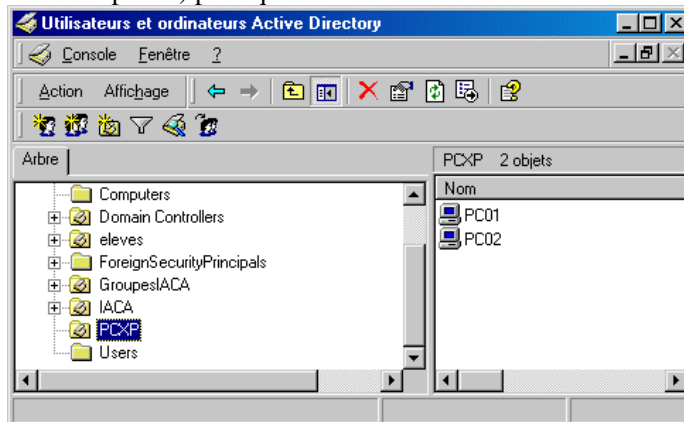
# Déploiement d'un fichier MSI

Vous pouvez exécuter le programme MSI sur chaque station ou faire un déploiement par l'intermédiaire des Stratégies de groupe (GPO) d'Active Directory.

Ce déploiement n'est possible que si vous avez au moins Windows 2000 en serveur et en stations.

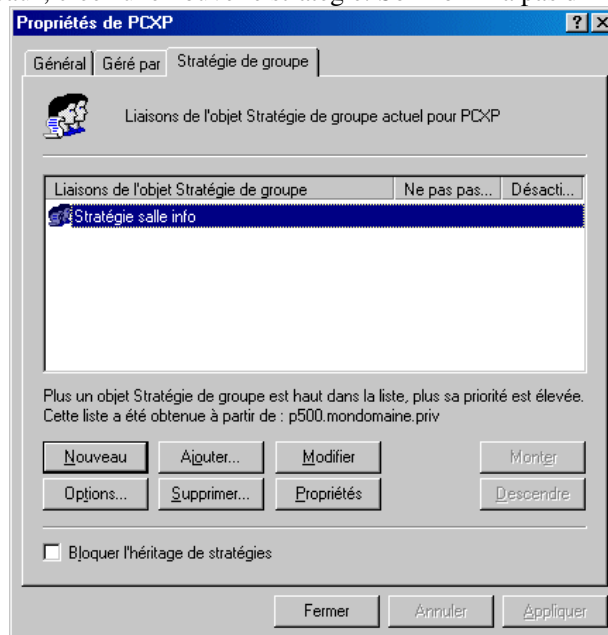
## Installation automatique sur les stations

Démarrez Active Directory, créez une OU que vous appellerez par exemple PCXP. Déplacez les stations XP (qui sont certainement dans Computers) pour qu'elles soient dans PCXP.

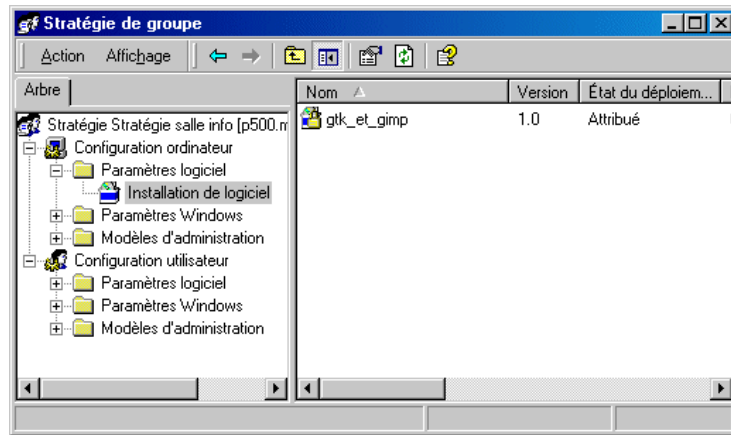


Faites un clic droit sur PCXP, allez dans les propriétés et choisissez le volet "Stratégie de groupe".

A l'aide du bouton "Nouveau", créez une nouvelle stratégie. Son nom n'a pas d'importance.



Utilisez le bouton Modifier et placez-vous dans "Configuration de l'ordinateur", "Paramètres logiciels" et "Installation de logiciel". Ajouter un nouveau Package et donnez le chemin réseau et le nom du fichier MSI. Le chemin de la source pour accéder au fichier MSI sera de la forme \\serveur\logiciel\gimp\gtk\_et\_gimp.msi



Le fichier MSI doit se trouver dans un répertoire partagé avec au moins les droits de lecture et exécution.

Démarrez une station faisant partie de l'OU. L'installation devrait se faire mais on pourra remarquer que l'installation ne réussit pas toujours au premier démarrage. Refaites un redémarrage de l'ordinateur si nécessaire.

Une ouverture de session ne suffit pas car l'installation est faite au niveau ordinateur.

Sur la station, juste avant l'ouverture de session, vous verrez successivement

"Préparation des connexions réseau"

"Activation des paramètres de sécurité"

"Installation du logiciel pris en charge gtk\_et\_gimp"

L'ouverture de session n'étant pas encore faite, le programme d'installation n'est pas capable d'écrire dans HKEY\_CURRENT\_USER ou dans le répertoire profil de l'utilisateur.

Souvent le logiciel effectue ces écritures lors de son premier démarrage.

Dans le cas de gimp, le répertoire ".gimp 2.2" ne sera pas installé pour l'utilisateur. Au premier démarrage de gimp ce répertoire sera créé. On peut remédier à ce problème en faisant en sorte de ce répertoire soit présent dans le profil et en utilisant les profils itinérants.

## Désinstallation

Le programme peut au choix être désinstallé sur chaque station en passant par "Ajout et suppression de programmes" ou en supprimant le package dans les stratégies de groupe ou encore en déplaçant la station pour la mettre dans une autre OU où ce package n'est pas installé.

# Sauvegardes

## Sauvegarder la partition système du serveur

Plusieurs solutions existent. Personnellement pour sauvegarder la partition système, j'utilise Ghost (produit de chez Symantec) ou éventuellement NTBackup (inclus dans Windows).

La sauvegarde sur lecteur de bandes est une solution assez chère qui, personnellement ne me donne pas satisfaction.

Il est possible d'installer Ghost sur le serveur ou seulement utiliser le programme Ghost.exe en environnement DOS. C'est cette deuxième solution que j'utilise habituellement.

Vous devez avoir au moins une partition suffisamment grande en plus de la partition système. Ghost 2003 permet d'enregistrer le fichier de sauvegarde sur une partition Fat ou sur une partition NTFS (les versions plus anciennes de Ghost étaient limitées aux partitions FAT ou ne permettaient d'utiliser les partitions NTFS que s'il n'existait pas de partition FAT)

Démarrez le serveur avec une disquette DOS ou un CD bootable en DOS.

Appelez le programme Ghost.exe

"Local", "Partition", "Vers image".

Choisissez le lecteur (donc le disque dur) contenant la partition à sauvegarder.

Choisissez la partition à sauvegarde (en général la première).

Choisissez la partition où sera enregistré le fichier de sauvegarde et indiquez le nom du fichier.

Pour économiser la place, vous pouvez choisir une compression élevée. La sauvegarde prendra un peu plus de temps.

La "Création de l'image de la partition" peut alors commencer.

Si votre intention est de créer des CD contenant le fichier de sauvegarde, il sera certainement nécessaire de fractionner ce fichier.

Personnellement j'utilise un fichier BAT contenant l'une des deux lignes :

```
ghost -CLONE,mode=PDUMP,src=1:1,dst=C:\SAV -SPLIT=680 -AUTO -Z9  
ghost -CLONE,mode=PDUMP,src=1:1,dst=1:2\SAV -SPLIT=680 -AUTO -Z9
```

src=1:1 signifie qu'il faut sauvegarder la première partition du premier disque dur.

src=2:1 voudrait dire la première partition du deuxième disque dur.

S'il existe au moins une partition FAT :

dst=C:\SAV correspond au nom du fichier qui sera créé. Vous pouvez choisir un autre nom que SAV mais il est conseillé de choisir un nom sans espace et court.

dst=SAV si le lecteur courant est celui qui doit être utilisé pour stocker le fichier de sauvegarde.

Pour sauvegarder le fichier sur une partition NTFS :

dst=1:2\SAV

1:2 signifie deuxième partition du premier disque. SAV donne le nom du fichier.

-SPLIT=680 permet le découpage en fichiers ayant une taille correcte pour être gravés sur CD

-AUTO la création des noms de fichiers sera faite automatiquement.

SAV.GHO pour le premier, SAV00001.GHS pour le second, SAV00002.GHS pour le troisième. Etc.

-Z9 impose une compression maximum.

## Restaurer le serveur

Démarrez le serveur avec une disquette DOS ou un CD bootable en DOS.

Appelez le programme Ghost.exe

"Local", "Partition", "Depuis image".

Indiquez le fichier contenant la sauvegarde (le premier fichier si la sauvegarde est morcelée).

Il vous est alors demandé "Sélectionnez la partition source depuis le fichier image". Le fichier image ne contenant qu'une partition, tapez simplement sur entrée.

A la question "Sélectionnez un lecteur de destination local en cliquant sur le numéro correspondant" choisissez le disque contenant la partition à restaurer.

A la question "Sélectionner la partition destination sur le lecteur Basique x", ce sera certainement 1 qu'il faudra répondre (si c'est la partition 1 que vous aviez sauvegardée).

Il est possible de restaurer dans une partition de taille différente.

## Sauvegarde des données

La solution proposée avec DFS n'est pas une solution suffisante. En effet, si une suppression est effectuée sur un répertoire d'un serveur, cette même suppression est effectuée aussitôt après sur l'autre. De même un virus sur l'un est aussitôt copié sur l'autre.

Il est donc nécessaire de faire une copie sur différents supports à des moments donnés.

### ***CopyReps en tâche planifiée.***

Le programme CopyReps peut être téléchargé dans les "Outils divers" sur le site de IACA. Il n'est pas nécessaire d'utiliser IACA pour pouvoir utiliser CopyReps.

Utilisez le bouton "Aide". Si vous souhaitez imprimer l'aide, utilisez la petite icône représentant une imprimante en bas à droite de la fenêtre d'aide.

CopyReps effectue une synchronisation des répertoires sources et destinations en se basant sur la taille, la date, le nom et le répertoire des fichiers afin de ne copier que ce qui est nécessaire.

CopyReps peut être appelé dans une tâche planifiée.

CopyReps ne copie pas les autorisations de sécurité des fichiers. La destination peut donc être un Windows 98 par exemple.

CopyReps peut envoyer un mail afin d'informer l'administrateur du déroulement de la copie.

### **Exemple**

Tâche planifiée qui se déclenche tous les Lundis, et Jeudis à 23h afin de copier vers un Windows 98 nommé PC01.

Tâche planifiée qui se déclenche tous les Mardis, et Vendredis à 23h afin de copier vers un Windows 98 nommé PC02.

Tâche planifiée qui se déclenche tous les Mercredis, et Samedis à 23h afin de copier vers un Windows 98 nommé PC03.

On peut aussi utiliser un seul Windows 98 et choisir des répertoires différents pour chacune des tâches.

### ***NTBackup***

Dans les accessoires, et "Outils système", utilisez "Gestion des sauvegardes".

Choisissez le volet "Sauvegarder". Cochez ce que vous voulez sauvegarder.

En utilisant le bouton "Démarrer", vous avez accès à la planification vous permettant de définir la tâche et les jours et heures.