Microsoft Windows NT4

1 GENERALITES

Windows NT 4 est un O.S. multitâche préemptif (une tranche de temps est allouée à priori à une tâche, si celle-ci ne répond plus le système continue de fonctionner). Sorti en octobre 1996, il reprend les fonctions de NT 3.51 mais avec l'interface (bureau) de Windows 95.

NT n'est pas « plug and play » mais l'utilisation du pilote PNP de certains équipements est parfois possible. NT n'utilise pas le BIOS mais contrôle directement le « hardware », il est donc prudent de vérifier la HCL (« *hardware compatibility list* » sur ***www.microsoft.com/hwtest*** avant de procéder à l'installation.

Pour fonctionner, NT demande un PC 486/25 min., avec 16Mo de RAM et 150Mo de disque (PC pentium, 32Mo, >1Go dans la pratique).

NT4 peut lire des partitions FAT ou VFAT (mais pas FAT32) et NTFS (attributs des répertoires/fichiers plus nombreux donc sécurisation d'accès plus grande). Pour un serveur on conseille de partitionner :

- FAT 250Mo : amorçage, pilotes....
- NTFS 500Mo : OS, spooler imprimantes...
- NTFS .... : Applications, données ...

1.1 Versions :

Il existe 2 versions de NT possédant le même noyau (mais pas le même prix ni la même configuration des registres) :

- NT server (prévu pour les serveurs de réseaux locaux, fourni avec les outils serveur internet IIS, DNS, DHCP et frontpage ...)
- NT workstation (poste de travail similaire à W95 en plus stable, max. 10 connexions entrantes).

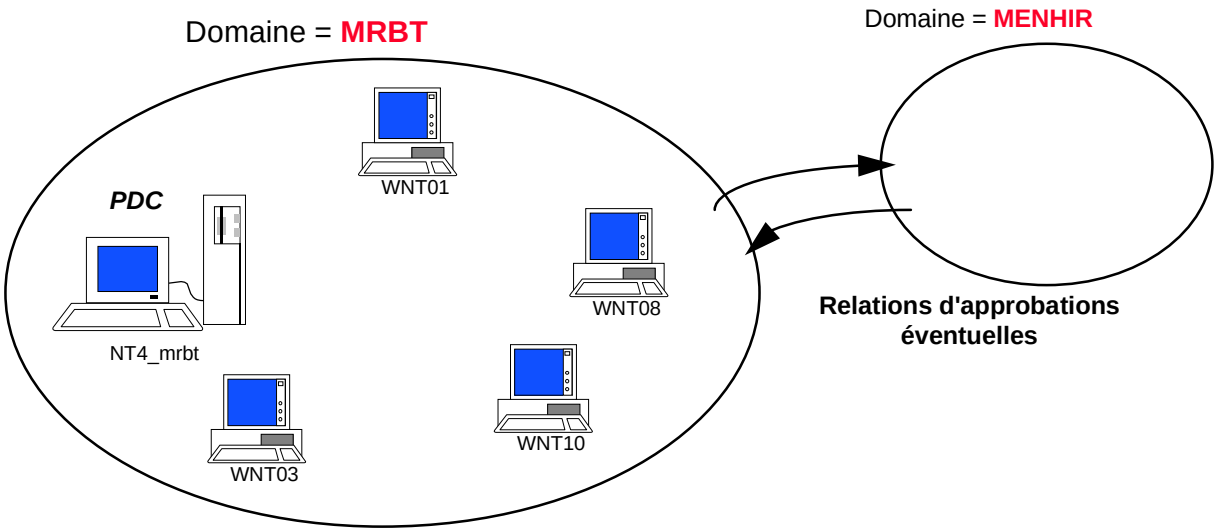
Une version **NT Terminal server** vient de sortir, elle permet d'utiliser un PC peu puissant (486...) comme station NT. Le PC sera simplement client et offrira l'apparence d'une station NT mais les applications seront toutes exécutées sur le serveur.

NT impose l'ouverture d'une session et ceci par l'appui des touches CTRL+ALT+Suppr (afin d'éviter le piégeage du mot de passe par un «cheval de Troie»). Les comptes utilisateurs peuvent être définis en **« workgroup »** (chaque station gère son accès) ou en **« domaine »** (un serveur centralise la gestion des accès). On évitera de mélanger les deux modes de fonctionnement dans un même réseau !

Lorsqu'une session est ouverte, CTRL+ALT+Suppr permet l'accès à la boite de sécurité NT pour gérer les tâches, changer le mot de passe, verrouiller la station (absence, les programmes en cours restent actifs) ...

1.2 Domaines :

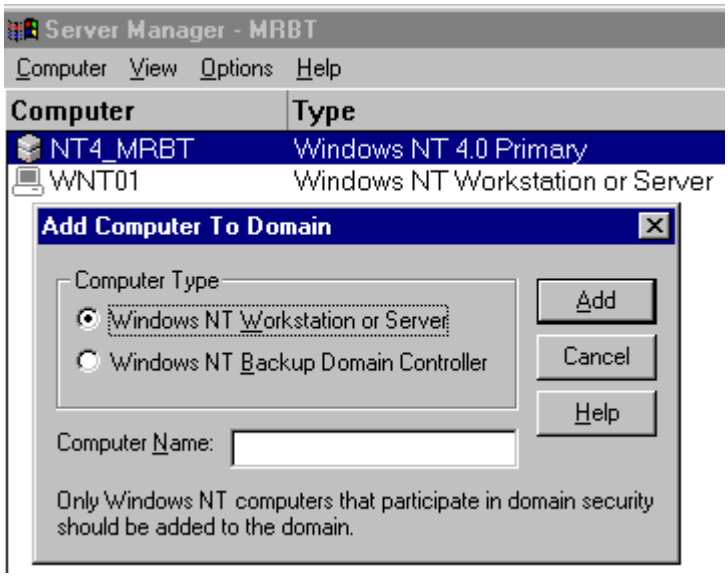
Toutes les machines doivent être nommées. Les listes étant alphabétiques on conseille A..., B... pour les serveurs et WS... pour les stations.



1.3 Types de serveurs :

PDC ("Primary Domain Controler") :

Un seul par domaine, il contrôle les accès aux ressources du réseau. On conseille de créer un domaine pour une cinquantaine de postes. Toutes les machines (stations, serveurs) devant faire partie du domaine doivent être déclarées (« *gestionnaire du serveur, ordinateur, ajouter au domaine* »...).



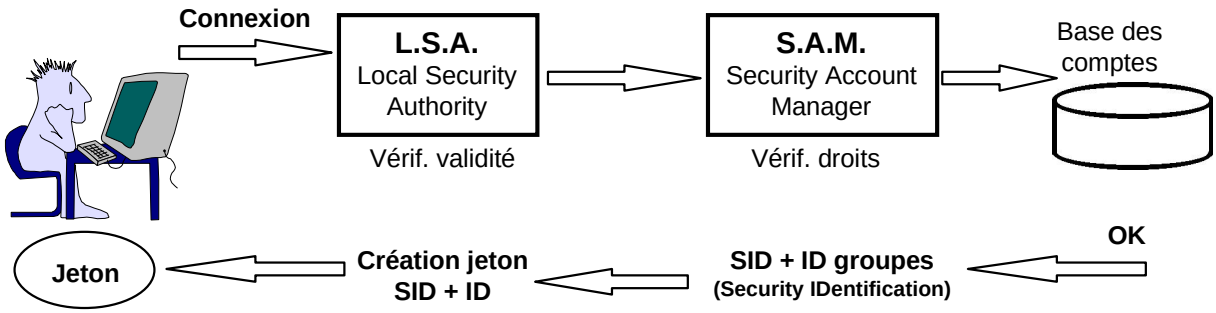
BDC ("Backup Domain Controler") :

Copie(s) synchronisée(s) (toutes les 5 minutes) du PDC. Permet au réseau de continuer à fonctionner en cas de panne du PDC (mais pas d'administrer les comptes). Le BDC doit être déclaré au PDC.

Serveur simple :

En général serveur d'applications qu'on ne veut pas charger par des tâches de contrôles d'accès.

1.4 Contrôle d'accès :



Le jeton est ensuite utilisé pour le lancement de chaque processus

2 ADMINISTRATION DES COMPTES

2.1 Comptes utilisateurs :

La définition des comptes se fait via le « *Gestionnaire des utilisateurs du domaine, utilisateur* ». Il faut posséder au moins le droit d'administrer les comptes ("account operator" = Opérateurs de comptes).

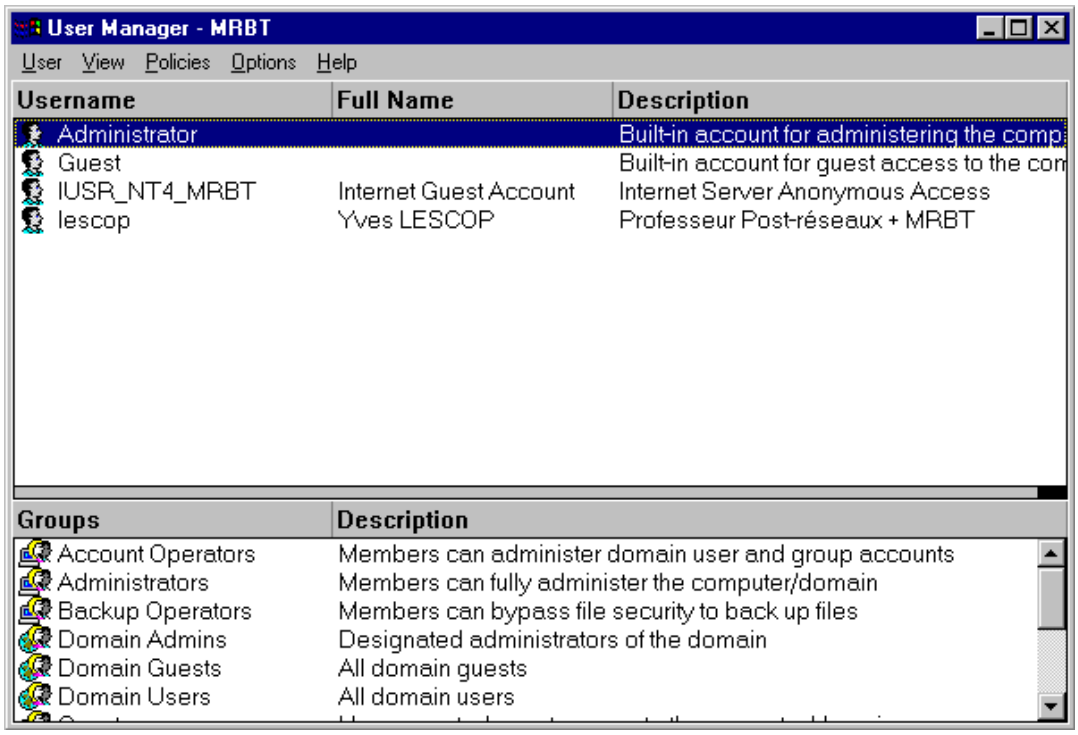
L'imposition du type de mot de passe, du verrouillage sur accès frauduleux... est unique pour le domaine « *Gestionnaire des utilisateurs du domaine, stratégies, stratégie de compte* ».

Ordre des opérations :

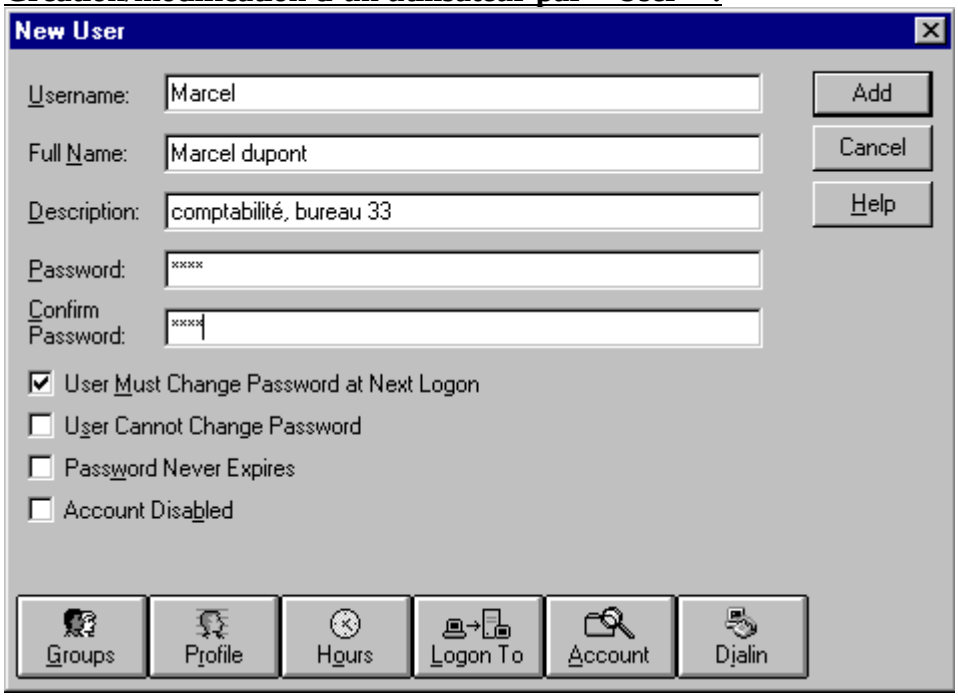
- Créer les utilisateurs (remplissage des champs... ajouter..)
- Modifier les caractéristiques des utilisateurs (CTRL+clic pour sélectionner plusieurs).

« User manager » :

A partir de « user » on peut créer un nouveau compte ou groupe, copier un compte, supprimer un compte (attention, même si on recrée le compte avec le même nom la définition de ses droits sera perdue), renommer un compte (sans changer ses droits)...
« Policies » = stratégies : permet de définir des options communes à tout le domaine (taille du mot de passe, verrouillage sur accès frauduleux).



Création/modification d'un utilisateur par « User » :

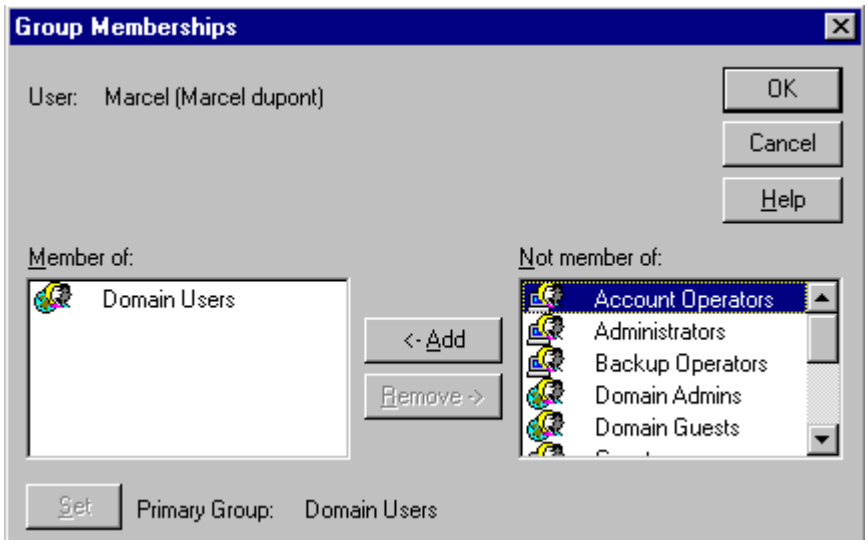


Caractéristiques des utilisateurs :

- « User name » = Utilisateur : nom du compte (« logon »).
- « Full Name » = Nom détaillé : nom complet (option)
- « Description » : titre, département ... (option)
- « Password » = mot de passe : 1er mot de passe...

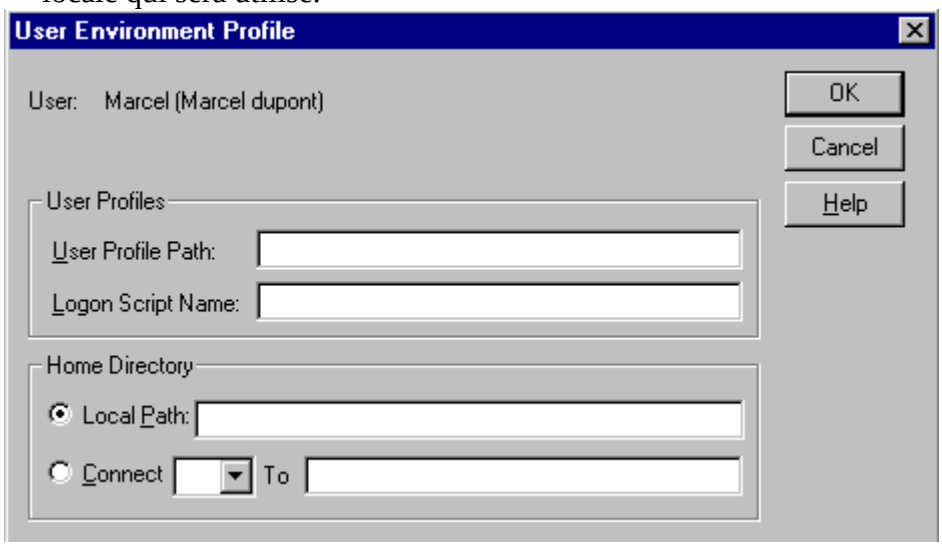
Il est possible de désactiver provisoirement le compte (vacances ...)

- ***« Groups » = Groupes*** : pour l'accès aux ressources ...

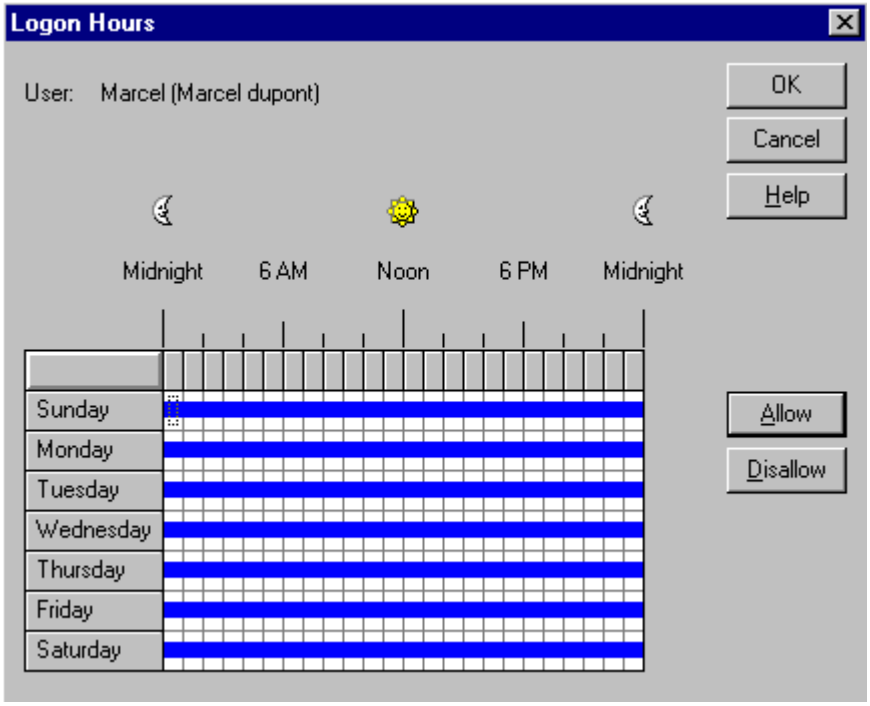


- ***« Profile » = Profil*** : lorsqu'un utilisateur se connecte pour la première fois, un profil par défaut est créé sur la station (dans \winnt\profiles\....), il contient les réglages de l'utilisateur (bureau, imprimantes...). Si l'utilisateur se connecte à partir d'une autre station, un nouveau profil par défaut sera créé sur celle-ci.

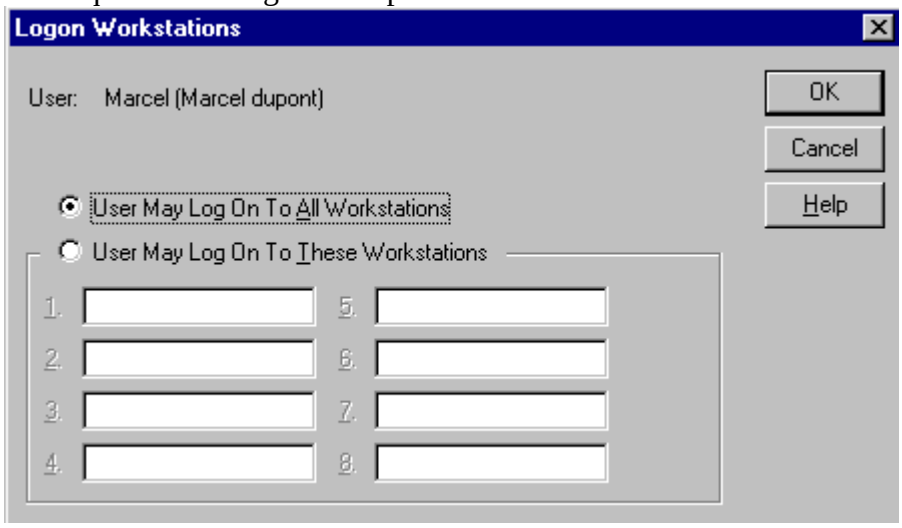
  On peut définir un profil errant pour l'utilisateur, il sera enregistré sur le serveur et l'utilisateur retrouvera son environnement quelque soit la station utilisée, mais le téléchargement du profil générera du trafic dans le réseau. Ce profil errant peut être personnel (modifiable) ***(.dat)*** ou obligatoire ***(.man).*** Dans cette boîte on pourra définir aussi le chemin du répertoire de base (connecter à ***\\SERVXX\repxx\...***). En l'absence de répertoire personnel sur le serveur c'est le répertoire ***\users\default*** de la machine locale qui sera utilisé.



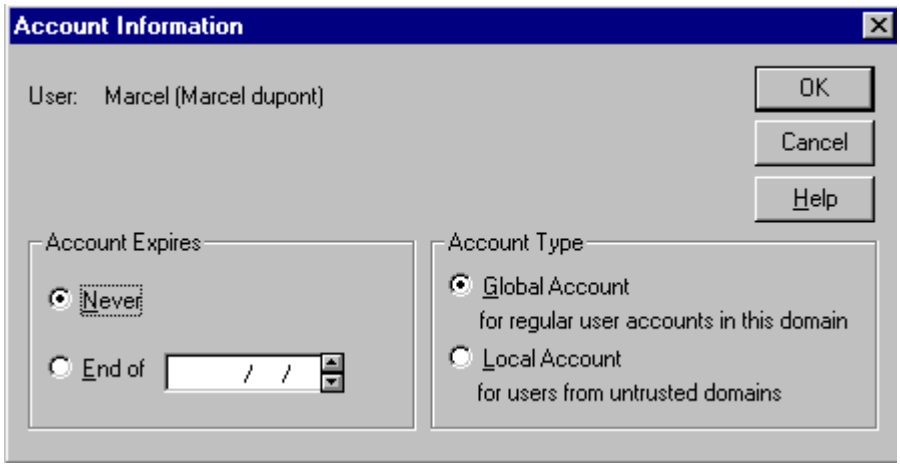
- ***« Hours » = Horaires*** : définition des plages de connexion autorisée.



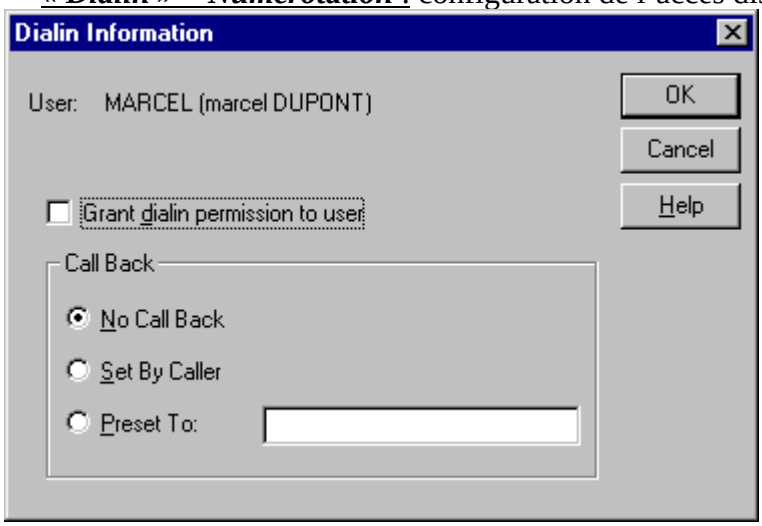
- ***« Logon To » = Accès depuis*** : limitation éventuelle des stations à partir desquelles le « logon » est possible.



- ***« Account » = Compte*** : définit une date de fin éventuelle, et le type (global normalement, local uniquement pour donner accès à certaines ressources à un utilisateur d'un autre domaine non approuvé).



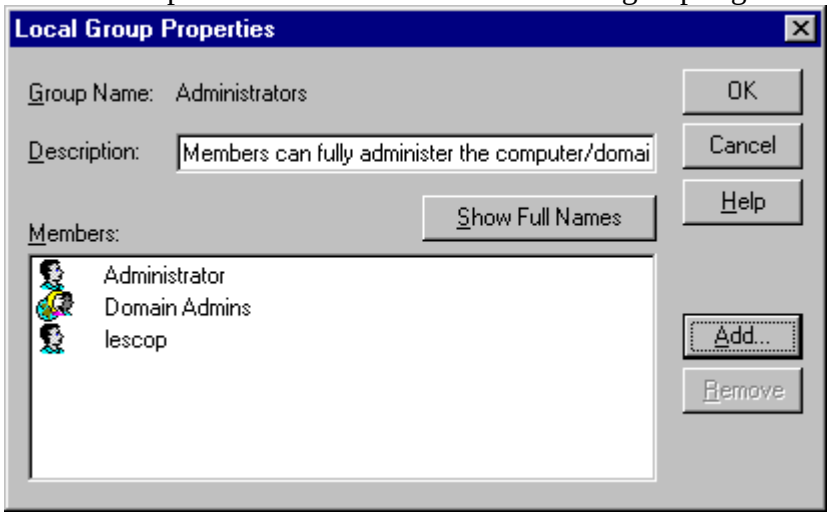
- ***« Dialin » = Numérotation*** : configuration de l'accès distant éventuel.



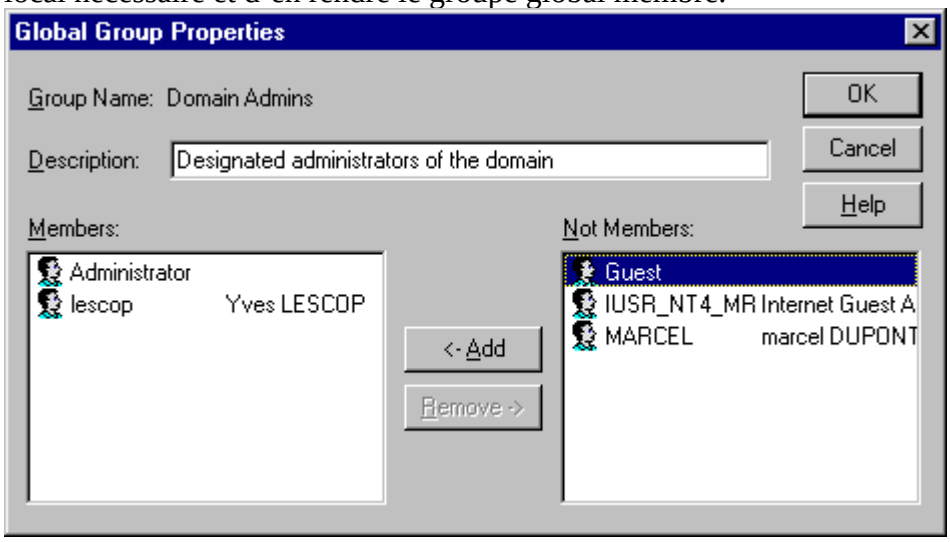
2.2 Groupes :

Les groupes facilitent l'affectation des permissions. NT définit deux types de groupes :

- ***Groupe local :*** situé sur une machine locale, il définit les permission d'accès à une **ressource** de la machine (répertoire/fichier, imprimante ...). Les membres peuvent être des utilisateurs ou des groupes globaux.



- ***Groupe global :*** sert seulement à regrouper logiquement des utilisateurs du domaine. Pour accéder à des ressources il est préférable de créer le groupe local nécessaire et d'en rendre le groupe global membre.



2.3 Opérateurs de comptes :

Il est possible de déléguer une partie des tâches administratives à un opérateur de compte. Il suffit d'ajouter au groupe prédéfini *« opérateur de compte »* l'utilisateur concerné. Les droits de ce groupe peuvent éventuellement être corrigés *(« stratégie, droits de l'utilisateur ... »).*

TD : PRISE DE CONTACT

- Démarrez vos machines sous Windows NT Workstation.
- Connectez vous dans le domaine prévu (MRBT) avec le compte d'administration qui vous a été attribué. Si votre station ne connaît pas le domaine prévu il faut modifier sa configuration *(connexion sur le compte administrateur local de la machine, modif des paramètre réseaux ...).* Si votre machine n'est pas déclarée dans le domaine, on peut le faire directement sur le PDC (via *srvmgr*...) ou la station vous proposera d'ouvrir une session d'administrateur du domaine afin de le faire.
- Ajoutez sur votre bureau les deux outils que nous utiliseront couramment : *\winnt\system32\usrmgr.exe* et l'explorateur NT.
- Lancez *usrmgr* et vérifiez votre compte. Quels sont vos droits (groupes...) ?
- Créez un compte, que se passe t'il si vous tentez de le rendre membre du groupe *domain admins* ? ...
- Connectez vous sur ce compte (logon), quel est votre bureau ? vérifiez la présence de ce profil sur le disque dur local ...

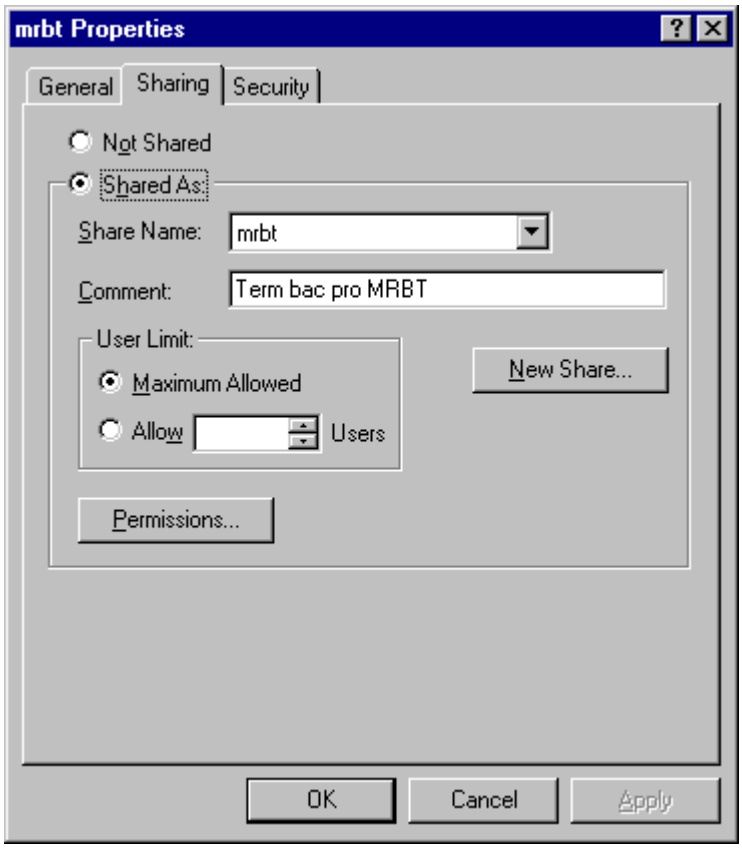
3 REPERTOIRE ET FICHIERS

3.1 Partage des répertoires :

Attention : Si le dossier concerné se trouve sur un disque du serveur, il faut donner à l'utilisateur le droit d'ouvrir une connexion locale. Par défaut (sécurité) ce droit est accordés aux seuls groupes locaux "administrators" et "account operators". Faire « *Gestionnaire des utilisateurs du domaine, stratégies, droits de l'utilisateur, ouvrir une session localement …ajouter l'utilisateur ou le groupe* » ou « *User manager for domains, policies, user rights, logon locally …* »

Pour qu'un dossier, sur partition FAT ou NTFS, puisse être accessible à d'autres machines du réseau il doit être **partagé (share).** Un main apparaît sur l'icône du dossier partagé lors d'un parcourt du disque local par l'explorateur.

Pour partager un dossier il faut ouvrir une session d'administrateur local sur la machine concernée. Le partage se fait par l'explorateur (clic droit sur le dossier ...).



- **Nom de partage** : C'est le nom qui sera donné aux utilisateurs effectuant un parcourt du voisinage réseau. Par défaut, c'est le nom du dossier qui est donné, on pourra mettre un nom plus explicite (attention aux utilisateurs sous Windows 3.x pour lesquels l'affichage des noms est limité à 8.3 caractères). Si le nom donné est terminé par le caractère **$** le dossier sera invisible tout en étant accessible (fichiers exécutables système..., *\winnt* est ainsi partagé en *ADMIN$* pour permettre une administration à distance). L'accès à un dossier partagé caché pourra se faire par *« démarrer, exécuter, ouvrir : \\nommachine\nomsecret$ ».*

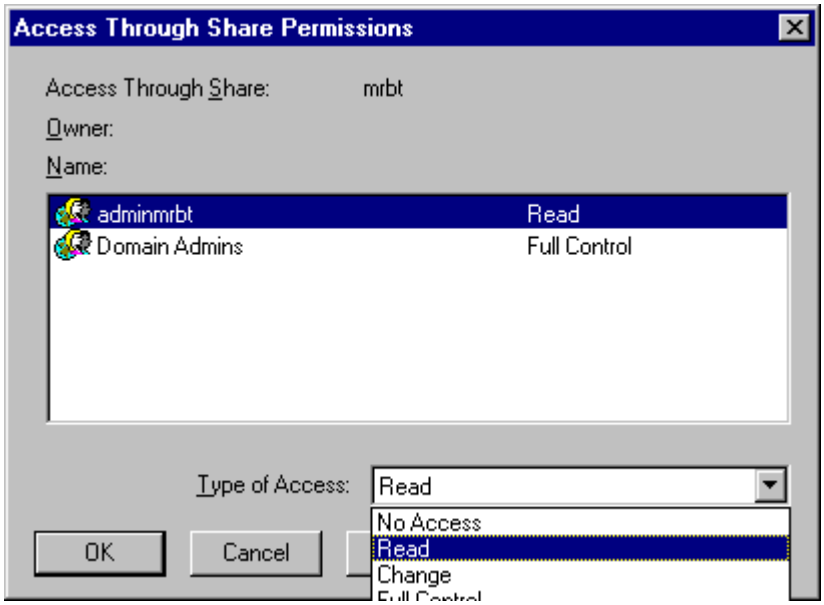
- **Commentaire** : il permet un complément d'information.
- **Limitation des utilisateurs** : on peut limiter le nombre d'accès simultanés (On pourra par exemple limiter à un l'accès en écriture d'un fichier client...). Le maximum sera de 10 sur une machine sous NT Workstation.
- Plusieurs noms de partage avec permissions différentes d'un même dossier sont possible (à éviter si non indispensable).

Permissions de partage :

Par défaut : le droit « contrôle total » est accordé à « tout le monde ». *(full control to Everyone).* Si le dossier est sur une partition NTFS, on aura intérêt à garder cette configuration et on pourra alors gérer plus précisément les droits d'accès par les permissions NTFS.

Sur une partition FAT, la seule sécurité possible est l'attribution de permissions de partage. **Attention : pas de protection contre les sessions locales.**

Le partage d'un dossier donne accès à ses sous-répertoires (un filtrage est possible s'il est en partition NTFS).



- **Contrôle total (full control)** : Modification des permissions, prendre possession (NTFS), + modifier, + lire.
- **Modifier (change)** : Créer/ajouter/modifier/changer les attributs des fichiers, détruire, + lire.
- **Lire (read)** : Afficher noms et attributs, lire les données, exécuter les exécutables, accéder aux sous-répertoires.
- **Aucun accès (No access)** : accès interdit, sert à masquer les droits hérités (contrôle d'accès du type : *accès accordé à xxxx* ***sauf*** *à yyyy*).

TD : PARTAGE DE DOSSIERS

- Ouvrez une session « administrateur » locale sur votre machine NT Workstation.

- Partager un dossier de votre disque dur qui est en partition FAT (essai..) avec diverses permissions.
- Vérifier les possibilités d'accès (voir, lire, créer un fichier/répertoire, effacer ...). Il est possible de vérifier les accès en restant sur la même machine via le parcours réseau de l'explorateur.
- Vérifier que sur un dossier autorisé à un seul utilisateur, l'administrateur ne peut y accéder directement. Il peut en prendre possession mais l'utilisateur peut s'en apercevoir.

Remarque : Pour que votre machine soit visible des autres (id Workgroup), il faut que la liaison « serveur » soit établie *(paramètres, réseau, liaison, activer serveur...).*

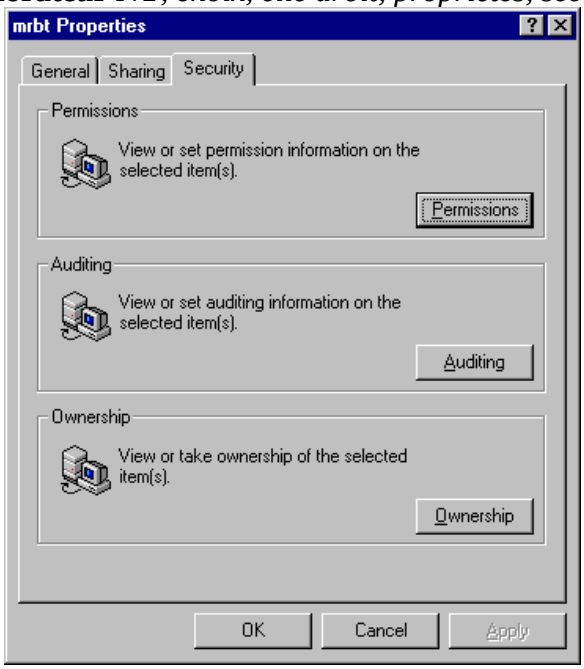
3.2 Permissions NTFS :

Les partitions NTFS permettent de définir des droits d'accès assez élaborés aux répertoires et aux fichiers. Par défaut, le groupe *« everyone »* à un accès total. Contrairement aux partitions FAT (où seul le partage est définit), le droit d'accès à un répertoire NTFS n'implique pas obligatoirement l'accès aux sous-répertoires.

Un utilisateur cumule ses permissions individuelles et celles des groupes auquel il appartient (sauf *« aucun accès »* qui filtre tout).

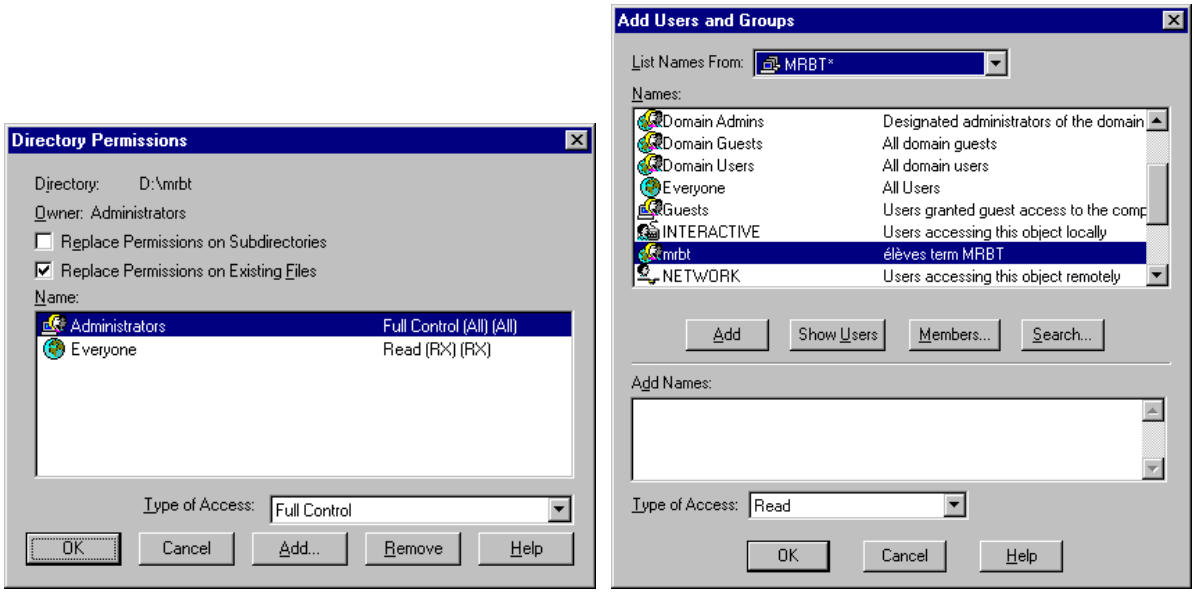
Les permissions de partage sont testées **avant** les permissions NTFS, ce sont donc les plus restrictives des deux qui s'appliquent effectivement.

La définition des permissions sur un répertoire/fichier se fait à partir de **l'explorateur NT**, *choix, clic droit, propriétés, sécurité, permissions...*



Il y a 6 attributs NTFS qui peuvent être accordés à des utilisateurs ou groupes, chaque fichiers/répertoire possède un propriétaire (le créateur par défaut), il est impossible de donner la possession à un autre : le responsable de la modification d'un fichier doit assumer !

Afin de permettre un déblocage de certaines situations, l'administrateur possède un droit de prise de possession non masquable (il pourra alors rétablir les droits perdus...).



3.2.1 Permissions standards sur les répertoires (dossiers) :

Aucun accès	Aucune permission.
Lister (RX)	Afficher les nom, attributs, propriétaires de fichiers ou dossiers.
Lire (RX)	Lire le contenu d'un fichier, exécuter un programme.
Ajouter (WX)	Ajouter des fichiers ou des dossiers.
Ajouter et lire (RWX)	Ajouter + lire/exécuter.
Modifier (RWXD)	Ajouter + lire/exécuter + détruire.
Contrôle total (RWXDPO)	tout (modifier les permissions, prendre possession).

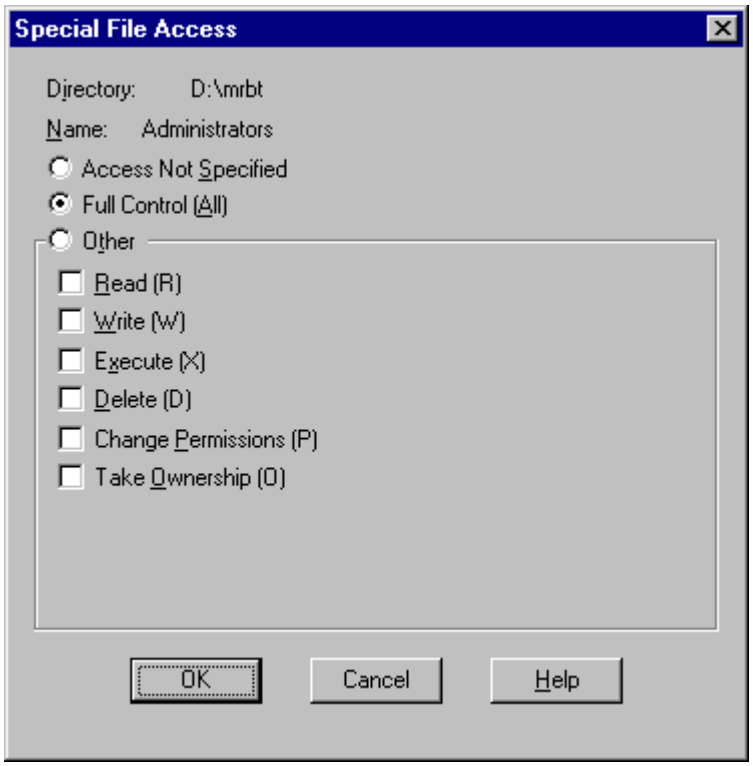
Par défaut, un répertoire fils hérite des propriétés du répertoire père lors de sa création.

3.2.2 Permissions standards sur les fichiers :

Aucun accès	Aucune permission.
Lire (RX)	Lire le contenu d'un fichier, exécuter un programme.
Modifier (RWXD)	Ajouter + lire/exécuter + détruire.
Contrôle total (RWXDPO)	tout (modifier les permissions, prendre possession).

Pour des situations particulières, il est possible d'être plus précis dans la définition des permissions : à partir de l'explorateur NT, choix, clic droit, propriétés, sécurité, permissions, sélectionner en type d'accès « accès spécial.. » ...

3.2.3 Permissions spéciales (détaillées) sur les répertoires ou fichiers :



Lire *(Read)*	Afficher les noms, attributs, propriétaire, permission. lire le fichier.
Ecrire *(Write)*	Ajouter des dossiers, modifier un fichier.
Exécuter *(eXecute)*	Afficher attributs, propriétaire, permissions, exécuter un programme.
Détruire *(Delete)*	Effacer un fichier ou dossier.
Modifier les permissions *(change Permissions)*	Modifier les permissions d'un fichier/dossier.
Prendre possession *(take Ownership)*	Devenir propriétaire d'un fichier/dossier.

3.2.4 Copie ou déplacements de fichiers :

⇒ Un fichier copié reçoit les permissions du dossier receveur et l'utilisateur devient propriétaire de la copie (il doit posséder le droit « ajouter » sur le dossier receveur).
⇒ Un déplacement d'une unité de disque à une autre est une copie.
⇒ Un déplacement dans la même unité de disque n'est possible que si l'utilisateur possède les droits « ajouter » sur le dossier receveur et le droit « détruire » sur le dossier origine. Le fichier déplacé conserve ses attributs.

TD : PERMISSIONS NTFS

- Ouvrez une session dans le domaine.
- Quels sont les répertoires accessibles sur la partition NTFS du serveur ?

- Quels sont les permissions de partage et les permissions NTFS sur votre répertoire personnel (\\nt4_mrbt\mrbt\TMRBTx) ? Expliquez.
- Modifier les permissions sur votre répertoire personnel et ses sous-répertoires/fichiers et vérifier les possibilités d'accès.
- Vérifier que sur un dossier autorisé à un seul utilisateur, l'administrateur ne peut y accéder directement. Il peut en revanche en prendre possession mais l'utilisateur peut s'en apercevoir.
- Effectuez des copies de fichiers (du ou vers le répertoire commun serveur ou autre machine...) et observez les propriétaires et attributs.

TD : CREATION DE COMPTES

Objectif : Créer tous les éléments nécessaires à une société selon un cahier des charges.

Matériel : 1 PC avec connexion Ethernet, 1 serveur NT 4.0 avec un compte administrateur.

Cahier des charges :

Une société est divisée en 3 structures : Administration, comptabilité et service technique. Chaque personne de la société possède un compte avec un répertoire personnel sur le serveur qu'eux seuls peuvent consulter (sauf indication contraire) et pour lequel on prévoira une connexion automatique, l'accès aux logiciels de « MSOFFICE » et l'accès sans restrictions à un répertoire commun. Pour chaque structure de la société on a les particularités suivantes :

ADMINISTRATION :

- 1 patron, par sécurité il ne peut se connecter qu'à partir d'une seule station. Il fait partie du groupe « facture ». Un des ses sous-répertoire ne sera pas accessible directement à l'administrateur.
- 1 secrétaire, elle ne peut se connecter qu'aux heures ouvrables, elle peut lire le répertoire du « patron ».

COMPTABILITE :

- 1 groupe facture ayant accès a un répertoire particulier : « facture »
- 4 ou 5 personnes dont 2 font partie du groupe facture. Ils ont tous accès au logiciel « NOTES ».
- Un des utilisateur sera « opérateur de compte ».

SERVICE TECHNIQUE :

- 3 techniciens ayant accès au logiciel « PCPLUS ».

TRAVAIL A EFFECTUER :

- Connectez vous en administrateur dans le domaine concerné.
- Créez les répertoires communs dans votre répertoire sur le serveur.
- Créez les groupes nécessaires à votre société (attention aux type des groupes). Attribuez les droits et limitations ...
- Vérifiez les droits et possibilités des différents utilisateurs en vous connectant sous leur nom.

4 IMPRESSIONS SUR NT4

Sous NT, un serveur d'impression reçoit et traite les documents des clients. Il n'existe pas de file d'attente au sens « Netware ou OS2 » mais un « spooler » d'impression qui est un ensemble de DLL qui reçoit, traite et planifie l'impression. Lorsque l'on imprime, NT crée des fichiers .EMF (fichier metafile étendu) et rend rapidement la main à l'application, ces fichiers sont ensuite traduits et transmis en tâche de fond à l'imprimante.

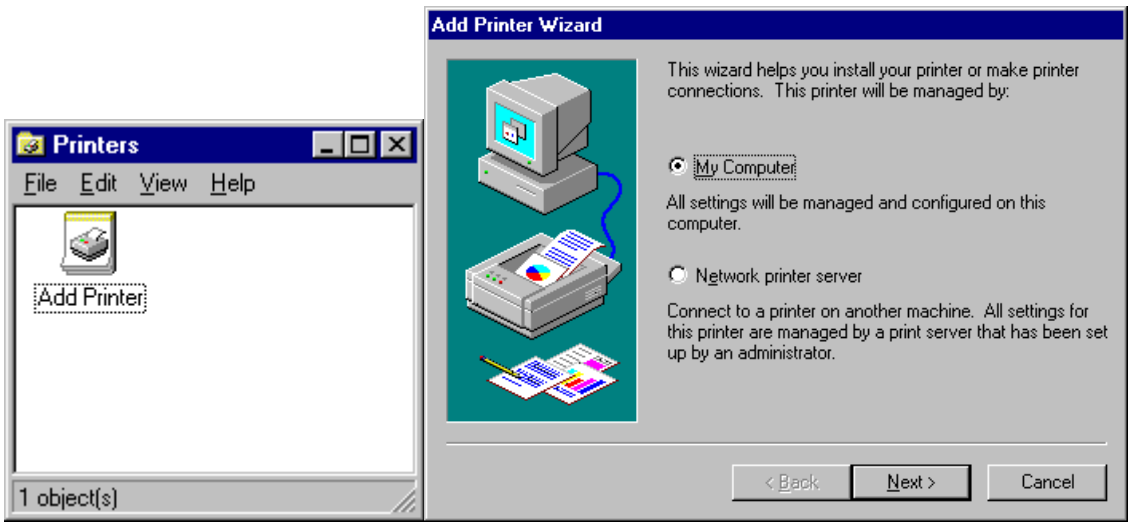
Le fait de déclarer une imprimante crée un spooler, il est possible de créer plusieurs imprimantes pour le même équipement d'impression (même port..) mais avec des propriétés différentes (droits d'accès, priorité...).

4.1 Serveur d'impression :

N'importe quelle machine NT peut être serveur d'impression. Les clients peuvent être sous NT, W95, W3.11, OS2, UNIX (+ Mac et Netware si NT serveur).

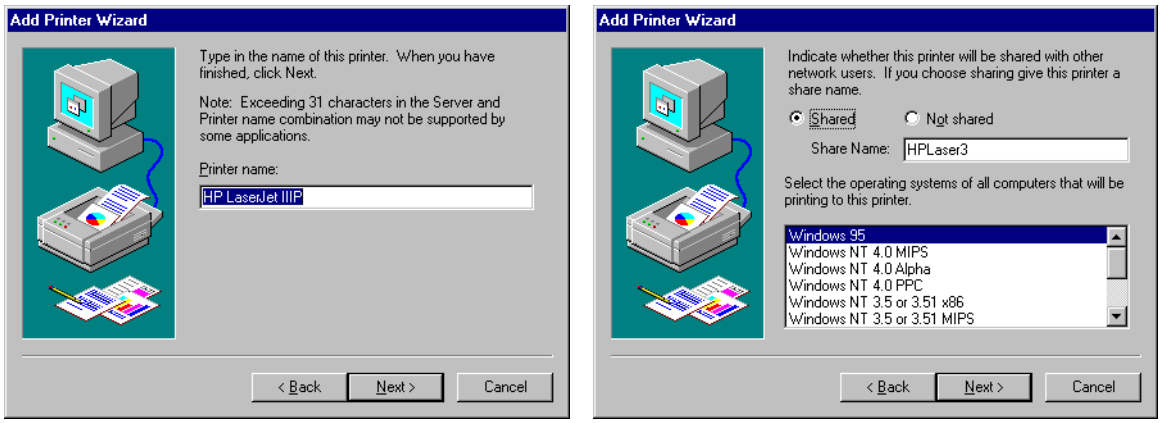
4.1.1 Ajout d'une imprimante partagée :

La procédure est similaire à celle de Windows 95.



L'imprimante doit être sur cet ordinateur (My computer).

On choisit ensuite l'imprimante (constructeur/type...), si l'imprimante est dans la liste, le pilote est fournit par NT.



L'imprimante doit être déclarée partagée (shared) et nommée (nom d'accès).

On choisit les OS des postes clients (copie des pilotes correspondants sur le serveur d'impression rendant inutile l'installation de ceux-ci sur les clients).

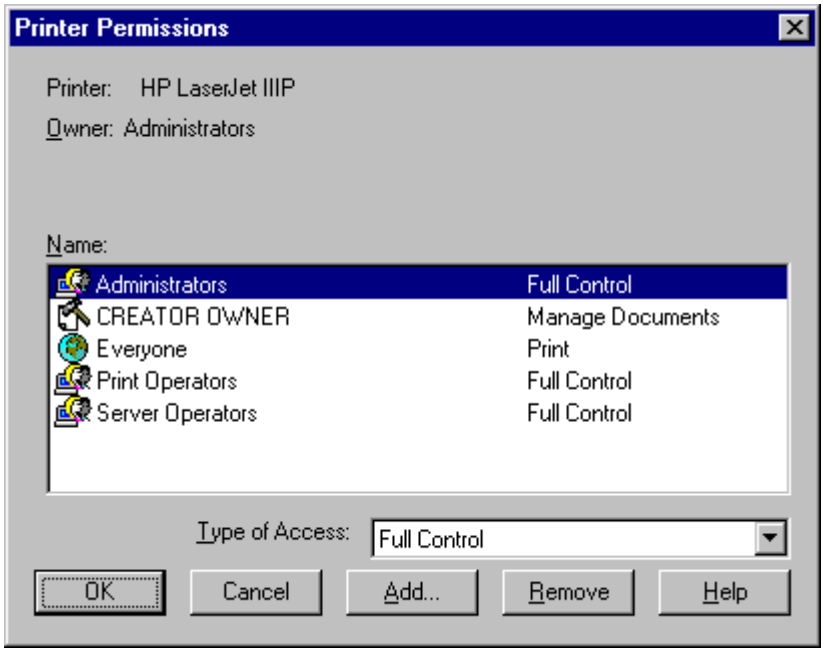
Il est possible de revenir sur ces paramètres ultérieurement (propriétés, partage).

4.1.2 Permissions d'accès :

On créera un groupe local (accès à la ressource) pour lequel on définira les droits d'accès. On rendra membre de ce groupe local les groupes/utilisateurs du domaine *(imprimante, propriétés, sécurité, permissions)*.

Il y a 4 permissions d'accès :

- **Aucun accès** *(No access).*
- **Imprimer** *(print)*: impression possible, suspendre/annuler ses travaux. Accordé à tout le monde par défaut.
- **Gestion documents** *(manage documents)*: contrôler tous les travaux + imprimer.
- **Contrôle total** *(full control)*: Modifier les permissions, partager/supprimer imprimante + gestion + imprimer.



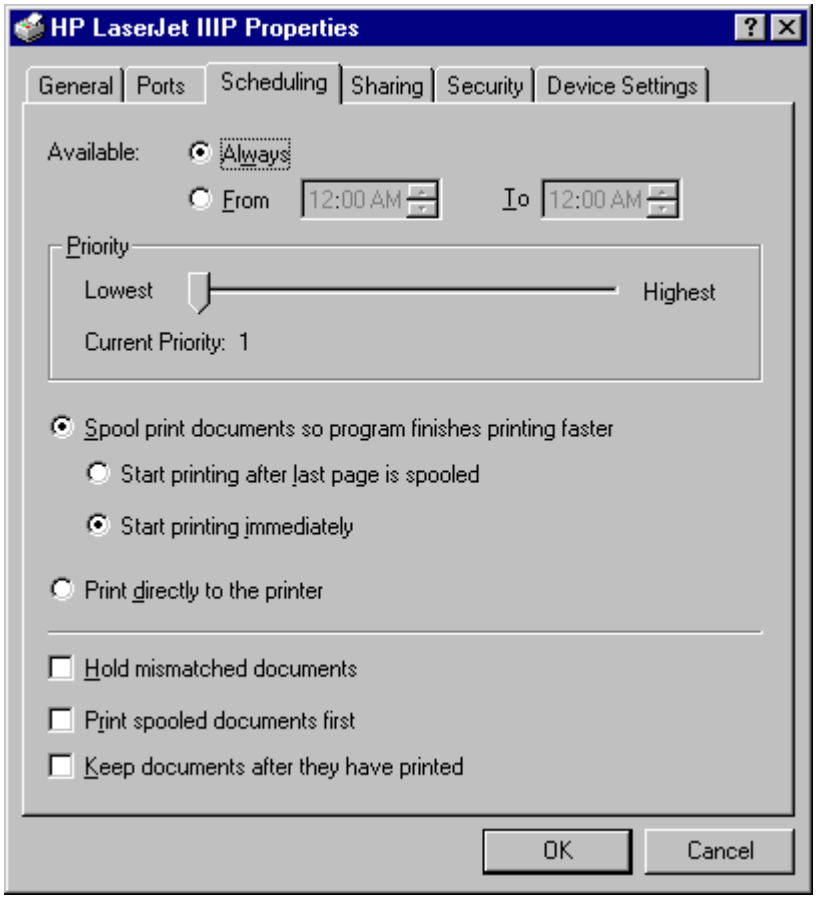
4.2 Postes clients :

- **W95/NT** : rien à faire, le client reçoit automatiquement le pilote lorsqu'il veut imprimer. (Attention, sur W95 le pilote ne sera pas mis à jour automatiquement sur le client).
- **W3.x, MSDOS, OS2** : Il faut installer le pilote sur le client.
- **Autres** (Mac, Netware, Unix) : Il faut installer le pilote et le service adapté.

4.3 Situations particulières :

4.3.1 Priorité d'accès :

- Ajouter une imprimante (même port ...) avec des droits d'accès éventuellement différents.
- Définir une priorité entre les imprimantes *« Propriétés, planification (scheduling) ... »* 1=mini et 99=maxi.
- Il est possible de restreindre les tranches horaires (travaux lourds la nuit...) ...



4.3.2 Redirection :

En cas de panne il pourra être nécessaire de rediriger les travaux vers une autre imprimante : *« imprimante.., propriétés, ports »*

- Changer le port (si l'imprimante destinataire est sur la même machine)
- Supprimer le port existant et ajouter *« nouveau port = \\autre_serveur\autre_imprimante ».*

4.3.3 Pool d'impression :

Un pool d'impression est le regroupement de plusieurs imprimantes sous un seul périphérique d'impression pour les clients (augmentation du débit d'impression). Celles-ci seront toutes branchées sur la même machine et il est préférable qu'elle soient du même type (même pilote utilisé).

Imprimante, propriétés, ports : activer le pool d'impression, ajouter les ports...

TD IMPRESSION

Sur votre station, connectez vous en administrateur et installez une des imprimantes disponible avec les caractéristiques suivantes :

- clients W95 possibles
- Accès à tous les utilisateurs du domaine avec priorité faible
- Accès prioritaires à quelques utilisateurs
- L'administrateur peut modifier toutes les propriétés
- Un utilisateur particulier peut gérer les imprimantes

Testez les impressions (locale et distante)

Mettez l'imprimante hors service, envoyez des travaux d'impressions de la part de plusieurs utilisateurs. Vérifiez les droits de gestion des travaux des différents utilisateurs.

5 SECURITE SUR Windows NT4

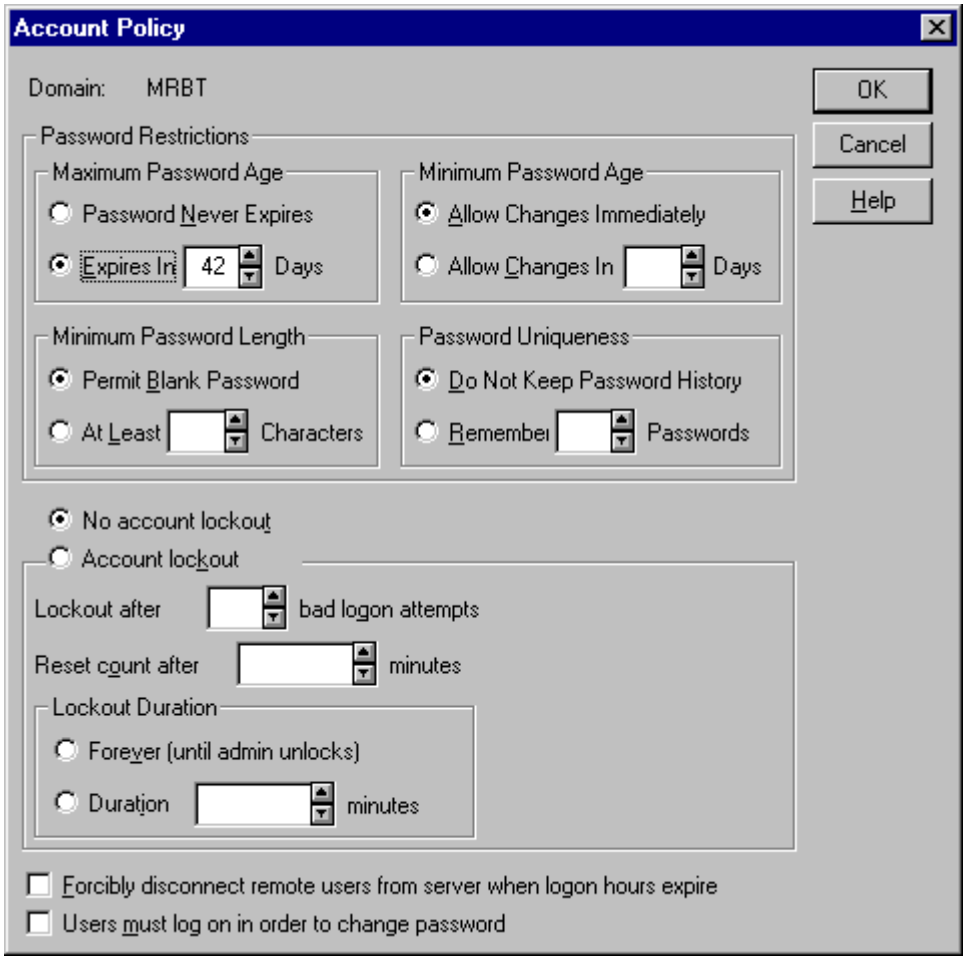
Sous NT, il existe divers moyens permettant de limiter l'accès à certaines ressources, d'imposer une configuration à l'utilisateur, de savoir ce qui c'est passé...

www.nt.bug.traq.com recense les problèmes de sécurité d'accès à NT.

5.1 Stratégies des comptes utilisateurs :

5.1.1 Accès au compte :

Dans un domaine on peut définir les caractéristiques communes à tous les accès aux comptes *(usrmgr, stratégie (policies), comptes (account)...*



Pour la sécurité on prévoira :

- Un mot de passe d'une longueur minimum assez importante s'il n'a pas de date d'expiration,
- Un verrouillage sur accès frauduleux.
- Le nom du compte ne sera pas directement celui de la personne.
- Pas de sessions locales sur les stations NT aux utilisateurs (éventuellement une session d'administrateur ou mieux rendre l'administrateur du domaine membre de l'administration locale).
- On pourra cacher le nom du dernier « logon » (affiché automatiquement) en modifiant la base de registre :

HKEY_LOCAL_MACHINE
\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon
« ReportBootOK » choisir « Nouveau/valeur chaîne » et entrer « DontDisplayLastUserName, REG-SZ, 1 ».

5.1.2 : Comptes spéciaux :

Compte administrateur :

Ce compte est créé lors de l'installation, pour ce compte ayant des droits étendus on conseille :

- N'utiliser ce compte que pour l'administration (l'administrateur possédera un compte ordinaire pour travailler).
- Mot de passe élaboré.
- Eventuellement renommer ce compte.
- Eventuellement limiter le « logon » de ce compte à une station précise.

Compte invité (GUEST) :

Ce compte est créé lors de l'installation, pour plus de sécurité on conseille de supprimer ce compte.

5.2 Protection des répertoires et fichiers :

5.2.1 Principes généraux :

On évitera les partitions FAT pour lesquelles seule la protection de partage est possible. Les clients W3.x et W95 ne peuvent cependant pas accéder aux partitions NTFS. Attention, il n'y a pas de protection possible sur les partitions FAT lors d'une connexion locale, aussi interdira t'on souvent les sessions locales sur les serveurs.

Règles générales :

- Inventorier les partages nécessaires.
- Hiérarchiser les dossiers et donner des noms évocateurs
- Retirer *« contrôle total »* à *« everyone »*.
- Effectuer les permissions NTFS avant les permissions de partage (+ sûr).
- Donner seulement les droits R/X pour les exécutables (évite les virus).

5.2.2 Principaux dossiers :

Dossiers programmes :

- *« Lire »* pour les utilisateurs.
- *« contrôle total »* (*« change Permissions »* au minimum) pour les administrateurs ou personnes chargées de la mise à jour.

Dossiers données :

- *« Lire et modifier »* pour les utilisateurs.

Dossiers personnels :

- Tout regrouper en NTFS (facilités de Backup...)
- « Contrôle total » à tous les utilisateurs sur la racine des rep. persos.
- « Contrôle total » à l'utilisateur concerné seul sur son répertoire.

5.3 Profils utilisateurs :

Le profil de l'utilisateur contient les réglages du bureau (barre des tâches, panneau de configuration, imprimantes, accessoires), des logiciels (Explorer, Applis NT ...). Il fait au minimum 150ko.

Par défaut, le profil de l'utilisateur est sauvegardé sur sa station (dans \winnt\profiles\nom_utilisateur...). Si l'utilisateur change de station, il ne retrouve pas son profil mais un nouveau profil par défaut est créé sur cette station !

5.3.1 : Profil errant :

Afin de permettre à un utilisateur changeant souvent de station de retrouver son profil, celui-ci doit être « errant », c'est à dire chargé sur le serveur. En contre partie le « logon » est plus long et le trafic réseau plus important. Ce profil est mis à jour sur le serveur à chaque fermeture de session.

Mode opératoire :

- Créer et partager sur le serveur un répertoire pour les profils (***profiles*** par exemple)
- Ouvrir une session utilisateur (utilisateur « modèle » éventuellement), modifier les réglages..., fermer la session.
- Ouvrir une session administrateur et copier le profil sur le serveur dans le répertoire partagé *« Panneau config, système, propriétés, profils utilisateurs, choisir.., copier vers : \\nom_serveur\profiles\nom_utilisateur ».*
- Indiquer qui à le droit d'utiliser les profils (dans la boîte *copier vers* précédente choisir *modifier*, sélectionner l'utilisateur du domaine).
- Définir dans le compte de l'utilisateur le chemin du profil *(usrmgr, ... profil, chemin = \\nom_serveur\profiles\nom_utilisateur)*

5.3.2 : Profil obligatoire :

Pour plus de sécurité (postes en libre service...) on pourra être amené à imposer le profil de l'utilisateur. La procédure est quasiment identique à celle du profil errant mais le profil ne peut être mis à jour.

Mode opératoire :

- Créer et partager sur le serveur un répertoire pour les profils (***profiles*** par exemple)
- Ouvrir une session utilisateur (utilisateur « modèle » de préférence), modifier les réglages..., fermer la session.

- Ouvrir une session administrateur et copier le profil sur le serveur dans le répertoire partagé *« Panneau config, système, propriétés, profils utilisateurs, choisir.., copier vers : \\nom_serveur\profiles ».*
- Indiquer qui à le droit d'utiliser le profil (dans la boîte *copier vers* précédente choisir *modifier*, sélectionner l'utilisateur du domaine).
- Renommer le fichier profil *ntuser.dat* en *ntuser.**man*** afin de le rendre non modifiable !
- Définir dans le compte de l'utilisateur le chemin du profil *(usrmgr, ... profil, chemin = \\nom_serveur\profiles\nom_utilisateur)*

TD PROFILS

- ♦ Pour un des utilisateur du domaine que vous avez créer modifiez son profil (ajout de raccourcis, fond d'écran...) et rendez le errant.
- ♦ Vérifiez en ouvrant une session de cet utilisateur, modifier le profil et fermer la session.
- ♦ Ouvrez une session sur un autre poste et vérifiez ...

- ♦ Créez un profil simple qui devra servir de profil obligatoire à l'un des groupes du domaine.
- ♦ Affectez ce profil obligatoire, vérifiez qu'il est bien chargé et qu'une modification du bureau n'est pas enregistrée...

5.4 AUDIT des événements :

Un Audit est un enregistrement dans un fichier journal des événements ou actions dont on désire surveiller le déroulement (quoi, qui, quand) pour la maintenance, la sécurité ou l'optimisation de certaines ressources (statistiques).

Un journal système recense les erreurs et avertissement du système NT.

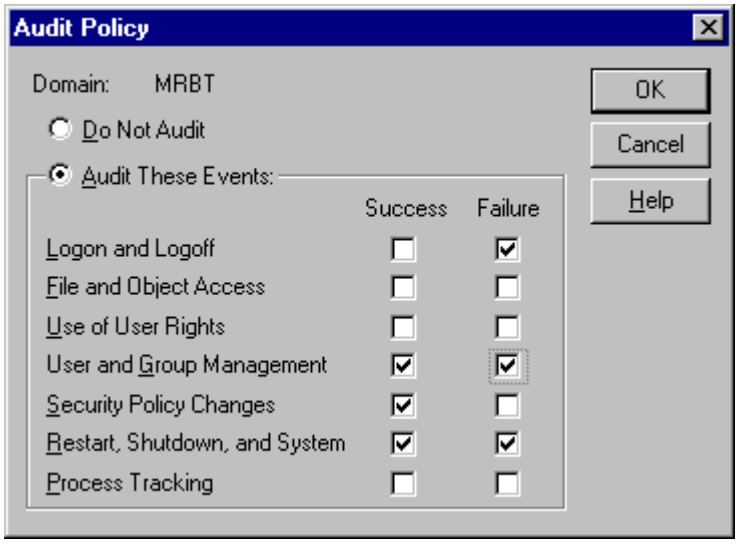
Un journal de sécurité contient les événements dont on à programmé l'audit.

L'audit est propre à chaque machine (stations ou serveurs). Les journaux peuvent être consultés via le réseau : *« observateur événements, journal, choix machine... »*

La taille du journal est de 512Ko par défaut (modifiable).

5.4.1 Choix des événements :

« Gestionnaire des utilisateurs (du domaine), stratégie, audit.. » pour définir les événement

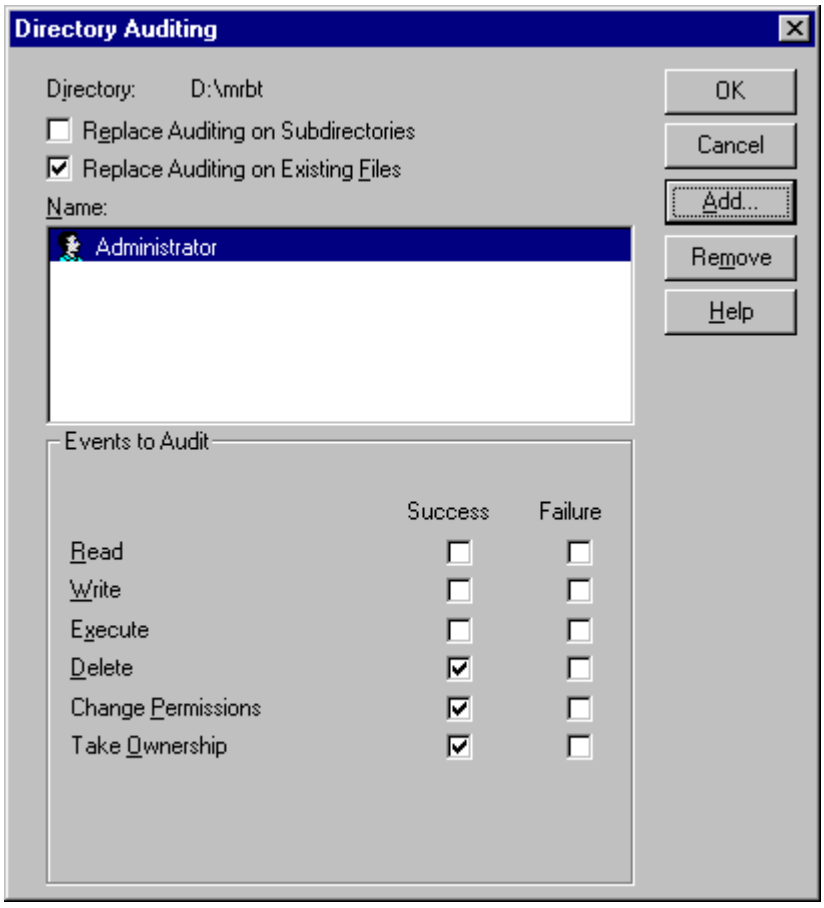


Pour permettre l'audition des accès aux dossier/fichiers et aux imprimantes il faut valider ***File and Object Access*** *(Accès fichiers et objets).*

L'audit étant consommateur de ressources CPU on conseille de n'auditer que ce qui est réellement utile (actions infructueuses, données sensibles...).

5.4.2 Audit des Dossiers/fichiers (NTFS) :

Via l'explorateur, choix dossier, clic droit, *propriétés, sécurité, audit*.



Name : liste des utilisateurs concernés par l'audit, ***« tout le monde »*** par défaut (utilisateurs du domaine ou non).

5.4.3 Audit des impressions :

Similaire à l'audit sur répertoire et fichiers, l'audit de « imprimer » permet une facturation éventuelle...

5.5 Sauvegardes :

5.5.1 Minimum de sécurité :

- Il faut sauvegarder au minimum tous les paramètres du système (base de données des utilisateurs...) situés sur *\winnt\system32\config* .
- Après chaque installation matérielle ou logicielle il faut recréer une disquette de réparation d'urgence par *RDISK.EXE*
- On recréera les 3 disquettes d'installation de NT par *winnt32 /ox.*
- En cas de problèmes de périphériques *makedisk.bat* permet de créer une disquette de Boot. Démarrer avec puis exécuter à partir du CD-ROM *\Support\Hqtools\Nthq* .

5.5.2 Gestionnaire de sauvegarde :

Windows NT possède un gestionnaire de sauvegarde **(uniquement pour des unités de bandes magnétiques compatibles !).** La base de registre de la seule machine ou sera installé le lecteur de bande pourra être sauvée, on l'installera donc de préférence sur le PDC.

Tous les utilisateurs peuvent sauver les répertoire/fichiers sur lesquels ils ont le droit « lire ». La restauration n'est possibles que par des utilisateurs avec droits.

Si le système est détruit, il faut d'abord le réinstaller avant de restaurer.

Différentes sauvegardes :

- ***Normale :*** sauvegarde totale, longue, restauration aisée.
- ***Différentielle :*** enregistrement des différences avec la dernière sauvegarde normale, assez rapide, restauration assez facile.
- ***Incrémentielle :*** seules les dernières modifications sont sauvées, très rapide, restauration compliquée (il faut repartir de la dernière sauvegarde normale puis passer par toutes les sauvegarde incrémentielles).

5.6 Quelques outils :

Convert.exe : permet de convertir une partition FAT en NTFS (inverse impossible).

Delprof.exe : permet un nettoyage des profils.

Shutcmd.exe : permet une fermeture de session à distance.

Winmsd.exe : effectue un diagnostic de la machine (détail des configurations matérielles).