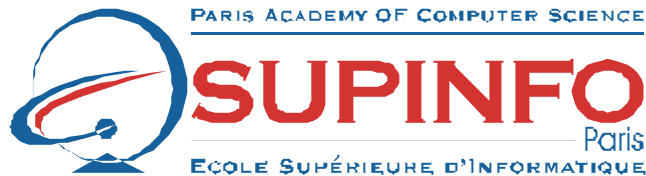


Administration de Windows NT 4.0

MEMENTO



Ecole Supérieure d'Informatique de Paris
23, rue Château Landon
75010 – PARIS

www.supinfo.com
www.laboratoire-microsoft.org

Caractéristiques

Statut	Interne ✍ Document de travail ✍ Livrable contactuel ✍
Réf. fichier	PC Word 2000 : Mémento Administration Windows NT4.doc

Mise à jour

Ver	Modification
0.9	Version initiale
1.0	Retouches diverses

Liste de diffusion

Organisme	Nom des destinataires	Nombre	Objet de la diffusion
ESI SUPINFO	LABORATOIRE MICROSOFT	1	Pour validation

Niveau de diffusion : Laboratoire
Confidentialité : Confidentiel Laboratoire

Historique du document

Version	Créé le	Par	Vérifié par	Livré le
0.9	28/12/2000	Ali NEDJIMI, Johann COLLOT	A. NEDJIMI	05/2000
1.0	04/01/2001	Guillaume DESFARGES, Jean-Luc MOUREAUX	JL. MOUREAUX	02/2001

GROUPES LOCAUX ET GLOBAUX

Les groupes **locaux** servent à donner aux utilisateurs des **permissions** d'accès à une ressource.
Les groupes **globaux** servent à **organiser les comptes** d'utilisateur de domaine.

Groupe Local	Groupe Global
<ul style="list-style-type: none"> • donne aux utilisateurs des permissions ou des droits • peut comporter depuis un domaine quelconque : <ul style="list-style-type: none"> - des comptes d'utilisateur - des groupes globaux 	<ul style="list-style-type: none"> • organise les comptes d'utilisateur par domaines • ne peut contenir aucun groupe • toujours créé sur le PDC dans le domaine du compte. • comptes d'utilisateur du même domaine • est ajouté à un groupe local de n'importe quel domaine (approbation).



REMARQUE sur les groupes globaux : Global signifie qu'il est possible d'accorder des droits au groupe lui permettant d'employer des ressources dans plusieurs (global) domaines.

Un groupe global ne peut pas être créé sur un ordinateur exécutant Windows NT Workstation ni sur un ordinateur installé comme serveur simple.

REMARQUE sur les groupes locaux : Local signifie qu'il est possible d'accorder des droits au groupe pour lui permettre d'employer des ressources dans un seul (local) domaine.

Pour ajouter des groupes globaux d'un domaine à des groupes locaux d'un autre domaine, il est nécessaire que la relation d'approbation appropriée ait été établie.

GROUPES PREDEFINIS

Les groupes prédéfinis sont des groupes qui ont des droits d'utilisateur déterminés. Ces groupes ne peuvent pas être supprimés ou renommés.

Les droits d'utilisateurs déterminent les tâches système qu'un utilisateur ou membre d'un groupe prédéfini peut exécuter.

Les serveurs membres NT possèdent les **Groupes Locaux** suivants :

1. Administrateurs
2. Utilisateurs
3. Invités
4. Opérateurs de sauvegarde
5. Utilisateurs avec pouvoirs (pas sur les contrôleurs de domaine).

Les contrôleurs de domaines comportent en plus les **Groupes Locaux** suivants :

1. Opérateurs de comptes
2. Opérateurs de serveur
3. Opérateurs d'impression

Les contrôleurs de domaines comportent les **Groupes Globaux** suivants :

1. Administrateurs du domaine
2. Utilisateurs du domaine
3. Invités du domaine

Il existe une **troisième catégorie** de groupe : les **Groupes Systèmes**

Ils sont présents sur tous les ordinateurs avec leur té de membre non modifiable. Les utilisateurs deviennent automatiquement membres pendant le fonctionnement du réseau

Ces groupes sont :

1. **Tout le monde** : comprends tous les utilisateurs locaux et distants qui ont un accès à l'ordinateur.
2. **Créateur Propriétaire** : l'utilisateur qui a crée ou pris possession d'une ressource.
3. **Réseau** (Network) : Comprend tout utilisateur connecté à une ressource partagée de l'ordinateur à partir d'un autre ordinateur sur le réseau.
4. **Interactif** (Interactive) : Inclut automatiquement tout utilisateur qui se connecte localement à l'ordinateur .Les membres interactifs ont accès aux ressources de l'ordinateur sur lequel ils se trouvent.

PARTAGES ET PERMISSIONS

Permissions de niveau partage

1. **Contrôle Total**
 2. **Modifier**
 3. **Lire**
 4. **Aucun accès**
- (Mnémotechnique : CLAM)**

S'appliquent uniquement lorsque l'utilisateur accède à un dossier (*sous NT un répertoire s'appelle un dossier*) à travers le réseau.

Lorsqu'un utilisateur est membre de plus d'un groupe, la permission effective est la combinaison la moins restrictive des permissions. Les permissions d'utilisateur sont cumulatives, aucune n'est donc prioritaire.

Aucun accès fait exception à cette règle elle outrepassé toutes les autres permissions. Peut être appliqué à des utilisateurs ou des groupes

La permission au niveau partage peut être accordée à des utilisateurs ou des groupes de domaines approuvés.

Des partages cachés peuvent être créés en ajoutant un \$ après le nom de partage.

Permissions NTFS

Sécurisent les ressources locales et les accès par le réseau
Peuvent être appliquées aux fichiers et dossiers.

Il y a six **permissions NTFS individuelles** :


1. **L**ire (R)
2. **E**crire (W)
3. **E**xécuter (X)
4. **S**upprimer (D)
5. **C**hanger les Permissions (P)
6. **P**rendre Possession (O)

(Mnémotechnique : LECEPS)

Les **permissions standards** pour les dossiers sont des combinaisons des permissions individuelles :

1. **A**ucun Accès
2. **L**ister (R+X)
3. **L**ire (R+X)
4. **A**jouter (W+X)
5. **A**jouter et Lire (R+W+X)
6. **M**odifier (R+W+X+D)
7. **C**ontrôle Total (R+W+X+D+P+O)

(Mnémotechnique : MALALAC)




REMARQUE : Contrairement à la permission Contrôle Totale, Modifier ne permet pas de changer les permissions ou de prendre possession. La permission Modifier, plus restrictive, est dans de nombreux cas préférable à Contrôle Total.

Les permissions standards pour les fichiers sont aussi des combinaisons des permissions individuelles :

1. **A**ucun Accès
2. **L**ire (RX)
3. **M**odifier (RWXD)
4. **C**ontrôle Total (RWXDPO)

La permission NTFS effective est combinaison des permissions de l'utilisateur et du groupe.
Aucun accès est prioritaire sur toutes les autres permissions.



REMARQUE : Les permissions NTFS des fichiers prévalent sur celles des dossiers. Cependant, il existe une exception : la permission Contrôle Total sur un dossier permet d'effacer les fichiers se trouvant dans ce dossier .

Explication : En plus des six permissions de base (RWXDPO) accordées à Contrôle Total, il y a une septième permission implicite appelée *File Delete Child* (FDC). FDC est présente pour des raisons de compatibilité avec POSIX et accorde à un utilisateur qui dispose du Contrôle Total sur un répertoire la possibilité de supprimer un fichier de niveau supérieur à l'intérieur de ce répertoire, même si cet utilisateur n'a pas la permission de suppression sur ce fichier particulier.

Seuls les fichiers de niveau supérieur peuvent être supprimés, et non les sous-répertoires et fichiers qu'ils contiennent.

Il existe deux solutions :

1. Utiliser les permissions d'accès spécial et choisir les six permissions plutôt que d'accorder le Contrôle Total
2. Ne jamais attribuer Contrôle Total sur quoi que ce soit, sauf à soi-même en tant que propriétaire.

Un peu de technique : CONTROLE D'ACCES DE NT AUX RESSOURCES NTFS

Comment NT prend-il la décision d'accorder l'accès à une ressource NTFS ?

Lorsqu'un utilisateur ouvre une session sur un ordinateur NT, le gestionnaire des comptes de sécurité génère un jeton d'accès pour la session courante de l'utilisateur, qui contient, entre autres choses, l'identifiant d'utilisateur et les identifiants de groupes de cet utilisateur (nous appellerons ces identifiants des SID : **S**ystem **I**dentifier).

Une ressource NTFS (ex: un dossier) possède une liste de ses permissions que l'on appelle ACL (Access Control List), chaque entrée dans cette liste s'appelle une ACE (Access Control Entry).

Lorsqu'un utilisateur demande un accès à une ressource NTFS (par exemple RX sur un fichier), un composant du système de sécurité de Windows NT appelé le Moniteur de référence de sécurité (SRM : Security Reference Monitor) analyse l'ACL en recherchant les références de tous les SID contenus dans le jeton d'accès de l'utilisateur. Cette recherche se fait jusqu'à ce que l'une des conditions suivantes soit remplie :

- ?? Le Moniteur de référence de la sécurité rencontre une interdiction (représentation interne d'Aucun Accès) pour un SID du jeton d'accès de l'utilisateur. La recherche s'arrête à ce point et l'accès est refusé
- ?? Le Moniteur de référence de la sécurité rencontre une autorisation pour un SID du jeton. La recherche s'arrête et l'accès est autorisé. Si l'autorisation spécifie certaines , mais pas toutes les permissions demandées, la recherche continue jusqu'à ce qu'on ait accumulé toutes les permissions, auquel cas l'accès est accordé. Si l'autorisation ne spécifie aucune des permissions demandées, la recherche continue.
- ?? Le Moniteur de référence de sécurité atteint la fin de l'ACL sans avoir accumulé toutes les permissions requises. L'accès est refusé. Aucun accès partiel ne peut-être accordé.

Il est intéressant de noter que ce procédé ne fonctionne que si les interdictions sont placées en tête de l'ACL. Si une permission précède une interdiction, un utilisateur peut obtenir l'accès même si Aucun Accès a été accordé à l'un des SID de son jeton d'accès. La recherche s'arrête dès que les permissions requises ont été accumulées et avant qu'on ait rencontré Aucun Accès. Windows NT place toutes les interdictions avant les autorisations.

Combinaison des Permissions de partage et des permissions NTFS

~~L~~ors de la combinaison des permissions de partage et NTFS, la permission effective est la plus restrictive.

~~L~~orsqu'un dossier est créé, il hérite des permissions du dossier dans lequel il a été créé.

Copie et déplacement de fichiers et Dossiers

- ☒ Un dossier ou fichier copié au sein d'une partition NTFS ou vers une autre partition NTFS hérite des permissions du dossier cible.
- ☒ Un dossier ou fichier déplacé au sein de la même partition NTFS conserve ses permissions.
- ☒ Un dossier ou fichier déplacé vers une autre partition NTFS hérite des permissions du dossier cible.
- ☒ L'utilisateur doit disposer de la permission Ajouter pour copier vers un dossier cible.
- ☒ L'utilisateur doit disposer de la permission Ajouter pour la destination et Supprimer pour la source pour pouvoir déplacer un objet.

GESTION DES ENVIRONNEMENTS UTILISATEUR

Création d'un nouvel utilisateur

- ☒ Cette opération se fait à l'aide de User Manager (*usrmgr.exe* pour les contrôleurs de domaine et *musmgr.exe* dans le cas d'une Workstation).
- ☒ Il n'y a que deux informations requises pour créer un compte utilisateur : le nom d'utilisateur et son mot de passe.
- ☒ Le nom entré dans le champ Utilisateur doit être unique dans la base de données d'annuaire de comptes dans laquelle il a été créé. Cela signifie qu'aucun autre utilisateur ou groupe dans un domaine donné ne peut posséder le même nom. Il peut comprendre **20 caractères** et les **majuscules ne sont pas différenciées des minuscules**.
- ☒ Le mot de passe différencie les majuscules/minuscules.
- ☒ Obliger l'utilisateur à changer son mot de passe et indiquer au système que le mot de passe du compte ne peut être modifié par l'utilisateur sont deux règles qui s'excluent mutuellement. Par conséquent, si vous cochez ces deux options à la fois, NT générera une erreur et empêchera la création du compte de l'utilisateur tant que l'une de ces options n'aura pas été modifiée.
- ☒ L'option 'compte désactivé' désactive le compte sans le supprimer. Cette méthode est conseillée dans le cas de départs non définitifs d'un utilisateur de la société. Il est aussi intéressant de systématiquement créer les comptes en désactivé lors de l'installation et de la configuration d'un nouveau contrôleur de domaine (éviter les ouvertures de sessions alors que l'accès aux ressources n'est pas encore sécurisé).
- ☒ Il est conseillé d'utiliser un modèle de compte pour créer les utilisateurs (copier avec F8) : Tous les éléments sont copiés sauf : Nom Utilisateur, Nom Complet, Compte Désactivé.
- ☒ Chaque utilisateur dispose d'un SID unique, la suppression d'un utilisateur est irrémédiable.

REMARQUE : Intérêt d'un Compte Local. Dans le bouton Compte, il est possible de spécifier si le compte créé est **Local** ou **Global**.

Un compte local de domaine est conçu pour permettre à des utilisateurs d'autres domaines, avec lesquels aucune relation formelle (approbation) n'a été établie, d'accéder à des ressources sur ce domaine. Il s'agit de ce que l'on appelle un "Compte local Correspondant" ("Local Matching Account").

Ainsi, si un utilisateur Dupont souhaite accéder à une ressource dans un domaine qui ne présente aucune relation d'approbation avec le sien, il est possible de créer un compte local possédant le même nom (Dupont) et le même mot de passe et de lui donner des permissions d'accès à la ressource (ex: un dossier).

Profils de l'utilisateur

Un **profil utilisateur** est stocké sur une machine locale.

Un **profil errant** est stocké dans un emplacement central (un partage réseau), il peut donc accompagner l'utilisateur.

Profils locaux :

• Situés sur la machine locale.

• Le sous-répertoire de profile de l'utilisateur se trouve sans <winnt_root>\profiles (exemple: c:\winnt\profiles\xxxx).

• Lorsqu'un utilisateur se connecte pour la première fois, le processus d'ouverture de session vérifie l'existence d'un profil errant dans la base de comptes. Si aucun chemin de profil n'est trouvé, Windows NT crée un sous-répertoire dans le répertoire <winnt_root>\profiles et obtient les informations de profil initiales à partir du profil utilisateur local par défaut se trouvant dans <winnt_root>\profiles\Default User. Windows enregistre toutes les modifications apportées au profil utilisateur dans le nouveau profil utilisateur local.

Profils errant :

• C'est un profil utilisateur centralisé

• Lorsque l'utilisateur se connecte, le processus d'ouverture de session vérifie si la base de compte contient un chemin de profil errant pour le compte. Si c'est le cas, NT contrôle si l'utilisateur a changé le type du profil pour qu'il devienne local (dans l'onglet Profils utilisateur dans l'utilitaire Système du Panneau de configuration). Si le type de profil est défini comme étant local, Windows NT utilise une version du profil stockée localement plutôt que de télécharger une nouvelle version à partir du chemin d'accès spécifié dans la base de données de comptes. Si l'utilisateur n'a pas défini le type du profil comme étant local, Windows NT compare la version locale avec le profil errant spécifié dans la base de comptes.

Si la version locale est plus récente, NT demande à l'utilisateur quelle versions du profil utiliser. Sinon, il télécharge le profil errant.


• Au moment de la fermeture de session, si l'utilisateur est un *Invité* ou si le profil est obligatoire (suffixe .MAN au lieu de .DAT pour le fichier **NTUSER.DAT**) , NT n'enregistre pas le profil utilisateur courant.

Nous avons vu que Windows NT crée automatiquement le profil. Dans le cas d'un profil errant. Cela implique qu'il existe un partage adéquat.
Exemple : \\SERVEUR\PROFILES\$

Il existe deux philosophies :

?La première consiste à donner la permission Modifier au Partage et Modifier (NTFS) au dossier partagé pour les Utilisateurs du Domaine. Ainsi le système va créer automatiquement les sous-répertoires des profils utilisateurs. Cependant, la racine (et la racine seulement) du dossier contenant les profils reste accessible en écriture à TOUS les utilisateurs du domaine.

?La seconde consiste à restreindre l'accès au dossier des profils en donnant par exemple la permission Lister sur le dossier lui-même (Contrairement à Lire (RX), la permission Lister (RX) ne permet pas de lire les sous-répertoires). Mais cette fois l'Administrateur devra créer lui-même les dossier des profils (à l'aide de Profils Utilisateurs de l'utilitaire Système du Panneau de Configuration).



REMARQUE : Le fichier NTUSER.DAT contient des informations de registre qui initialiseront le sous arbre **HKEY_CURRENT_USER**. Le fichier NTUSER.DAT.LOG quant à lui est un fichier d'enregistrement transactionnel. Ces deux fichiers se trouvent à la racine de chaque profil utilisateur. Lorsque l'utilisateur se déconnecte, NTUSER.DAT est mis à jour à partir de HKEY_CURRENT_USER de la base de registre.

En deux mots, NTUSER.DAT contient les informations de registres spécifiques à l'utilisateur (ex : les couleurs).

Pour rendre un profil obligatoire , il suffit d'aller dans le répertoire de profil d'utilisateur et de renommer NTUSER.DAT en NTUSER.MAN (man comme **mandatory** : obligatoire). Ainsi, les modifications ne seront pas prises en compte, le fichier devenant en quelque sorte en Lecture Seule.

Répertoire de base

Les informations de la section Répertoire de base servent chaque fois qu'un utilisateur ouvre ou enregistre un fichier dans une application, ou lorsqu'un utilisateur invoque une fenêtre d'invite de commandes. Le répertoire par défaut est \USERS\DEFAULT.

Il s'agit simplement de l'espace de travail par défaut qui leur est affecté au départ.

Le bouton Chemin Local permet de spécifier un chemin local pour le répertoire de base. Si ce chemin est un chemin réseau, il faudra cliquer sur le bouton Connecter, puis choisir une lettre de lecteur dans la liste déroulante et entrer le chemin réseau.

Pensez à partager le dossier pour que le Gestionnaire des utilisateurs crée automatiquement le répertoire de base. (L'administrateur doit avoir au moins la permission Modifier sur le partage et les permissions NTFS).

Lors de la création automatique sur une partition NTFS, l'utilisateur reçoit Contrôle totale comme permission par défaut sur ce dossier, et l'accès est interdit à tous les autres utilisateurs, y compris l'administrateur. (pour en modifier le contenu par la suite, il faudra en Prendre Possession).

Script d'ouverture de session

Il permet de spécifier un script d'ouverture de session pour l'utilisateur. Ces fichiers de script possèdent une extension de type CMD ou BAT. Ils sont généralement utilisés pour établir des connexions réseau

Seul le nom du fichier doit être entré et pas le chemin complet

Le dossier pour mettre les scripts est : <root_winnt>\SYSTEM32\REPL\IMPORTS\SCRIPTS

Exemples de commandes dans un script :

```
NET USE Z: \\SERVEUR\PARTAGE /PERSISTENT:NO
```

Explication de l'argument PERSISTENT : cet argument gère l'emploi des connexions réseau permanentes.

?? **yes**

Enregistre toutes les connexions à mesure qu'elles sont établies et les rétablit à l'ouverture de session suivante.

?? **no**

N'enregistre pas la connexion établie ni les connexions ultérieures ; les connexions existantes sont rétablies à l'ouverture de session suivante.

Servez-vous du paramètre /delete pour supprimer les connexions persistantes.

```
NET USE * \\SERVEUR\PARTAGE
```

Alloue la prochaine lettre de lecteur

```
NET TIME \\SERVEUR /SET /Y
```

Permet de synchroniser l'heure (le /Y évite la confirmation du changement par l'utilisateur)



REMARQUE : Le dossier <root_winnt>\SYSTEM32\REPL\IMPORTS\SCRIPTS est partagé en tant que NETLOGON, une pratique courante consiste à ajouter une permission Administrateur : Contrôle Total sur NETLOGON. L'accès à ce dossier lors de la modification des scripts sera ainsi bien plus rapide via le Voisinage Réseau.

Stratégie de compte

Dans User Manager : Menu Stratégies puis Comptes

La boîte de dialogue contient de nombreuses informations mais toutes les options sont centrées autour des mots de passe.

?? Durée maximale du mot de passe : définir une limite d'expiration

?? Durée minimale du mot de passe : un utilisateur forcé de changer son mot de passe peut le changer une première fois puis être tenté de le changer à nouveau pour revenir sur son mot de passe initial (qu'il préfère). Cette option évite ce genre de pratique.

?? Longueur minimal du mot de passe

?? Unicité du mot de passe : tient un historique des mots de passe et évite que l'utilisateur réutilise des mots de passe de façon cyclique.

L'option Mot de passe n'expire jamais outrepassa la Durée maximale du mot de passe.

Verrouillage de compte : NT verrouillera un compte après un certain nombre de tentatives. Si l'option de verrouillage permanent est sélectionnée, l'administrateur devra lui-même déverrouiller le compte. Il est impossible de verrouiller un compte manuellement. Seule la violation des règles d'ouverture de session provoque le verrouillage.

Le compte administrateur ne peut pas être verrouillé (sauf si l'on utilise l'utilitaire PASSPROP du Ressource Kit), ceci pour des raisons évidentes de sécurité.

Affectation de droits

Dans User Manager : Menu Stratégies puis Droits de l'utilisateur.

Une permission porte sur un objet spécifique (comme un dossier) , un droit se réfère à un droit général d'effectuer une action particulière sur le système.

Exemple :

- ?? Ouvrir une session localement
- ?? Arrêter le système
- ?? Restaurer des fichiers et des répertoires
- ?? Prendre possession des fichiers ou d'autres objets.

Audit des événements

Dans User Manager : Menu Stratégies puis Audit. On utilise cela pour garder la trace du succès ou de l'échec de certains événements. Ces événements sont consignés dans le Journal de Sécurité.

L'audit sur les fichiers et objets comporte deux phases :

- ?? activer l'audit en cochant le succès et/ou l'échec de l'Accès fichier et objets
- ?? puis en activant l'audit pour le dossier ou le fichier dans l'onglet Sécurité.

ETUDE DE CAS

Vous venez d'intégrer la structure de l'entreprise NAT. Vous voici désormais à la tête du réseau interne. A vous de faire les bons choix afin d'administrer correctement le parc informatique de notre entreprise.

Le matériel de notre entreprise se décompose comme suit : 200 postes, 4 serveurs sous Windows NT chacun ayant le protocole TCP/IP déjà installé.

Notre entreprise comporte plusieurs directions : une direction générale, une direction financière et une direction technique.

Chacune des directions souhaite avoir un espace disque commun à toutes les personnes de la direction.

Les membres de la direction générale doivent être capable de se connecter sur n'importe quelle machine appartenant au réseau de l'entreprise. De plus, ils voient tous les espaces disques.

Chacun des membres des autres groupes ne se connecte que sur les machines appartenant à leur groupe.

La répartition des machines se veut uniforme.

Je ne vais vous citer que quelques noms afin que vous puissiez me créer les utilisateurs correspondants. Les autres personnes de l'entreprise calquant leurs droits sur les comptes que vous allez créer (les modèles). Ainsi, nous avons dans la Direction Générale, monsieur Patrice Prut, dans la Direction Financière , madame Patricia Prut et enfin, dans la Direction Technique, nous voulons monsieur Jean Glouton.


Proposez une démarche de planification afin de gérer au mieux le réseau et ses utilisateurs.

PLANIFICATION

- ?? Définir la nomenclature pour les comptes : 8 caractères , 1 caractère du prénom + 1 séparateur (.) + 6 caractères du nom . Dans notre cas, il faudra ajouter un caractère de différenciation. (ex: P.PRUT1)
- ?? Groupes globaux à créer : Direction Générale, Direction Financière, Direction Technique.
- ?? Groupes locaux à créer : AccèsGénéral, AccèsTechnique, AccèsFinancier ...
- ?? Les profils sont stockés sur le serveur
- ?? Il y' a un dossier commun pour chaque service
- ?? Chaque utilisateur possède un dossier personnel.

MODE OPERATOIRE

1.CREATION DES DIFFERENTS DOSSIERS : LES RESSOURCES.

<p>Le dossier Commun contient un sous-répertoires pour chaque Direction. Le dossier Profiles contiendra les profils des utilisateurs Le Dossier Users contiendra les répertoires personnels des utilisateurs.</p>	
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------

Dossiers Communs

Partager DirFi en tant que [DirFi\\$](#), DirGen en tant que [DirGen\\$](#) et DirTech en tant que [DirTech\\$](#)

Utiliser les permissions suivantes :

NTFS	PARTAGE
Administrateurs : Contrôle Total	Administrateurs : Contrôle Total

- ?? Utiliser Administrateurs au lieu d'Administrateurs du Domaine qui est un groupe global. Administrateurs (G. Local) contient Administrateurs du Domaine (G. Global) qui contient lui-même le compte Administrateur.
- ?? Eviter de mettre plus de 8 caractères pour ce dossier si des clients sous MS-DOS doivent y accéder.

Le dossier pour les profils (partage : PROFILE\$)

Partager le dossier en tant que Profiles\$.

Utiliser les permissions suivantes :

NTFS	PARTAGE
Administrateurs : Contrôle Total	Administrateurs : Contrôle Total
Utilisateurs : Modifier	Utilisateurs : Modifier

Utilisateurs (G. Local) contient le groupe global Utilisateurs du Domaine. Chaque utilisateur ajouté fait automatiquement partie de ces groupes.

Attention : La racine du dossier reste accessible à tous les utilisateurs, mais cela permet au système de créer automatiquement les dossiers des profils pour tous les utilisateurs. Les dossiers de profils, quant à eux, sont convenablement protégés.

Le dossier pour les répertoires personnels (partage : USERS\$)

Partager le dossier en tant que Users\$.

Les dossiers des utilisateurs seront créés ici par la suite.

Partage USERS\$ purement administratif (notamment pour que le gestionnaire des utilisateur puisse créer les dossiers et attribuer les permissions adéquates).

NTFS	PARTAGE
Administrateurs : Contrôle Total	Administrateurs : Contrôle Total



REMARQUE : Penser à l'acronyme CGLP : **C**ompte - **G**roupe **G**lobal - **G**roupe **L**ocal - **P**ermissions
Il s'agit de la démarche logique conseillée par Microsoft pour la gestion des ressources sous Windows NT

2. CREATION DES GROUPES

Créer les groupes locaux : AccèsGénéral, AccèsTechnique et AccèsFinancier.

Créer les groupes globaux : Direction Financière, Direction Générale, Direction Technique.

Mettre les groupes globaux dans les groupes locaux :

Groupe Local	Contient (Groupe Global)
AccèsGénéral	Direction Générale
AccèsTechnique	Direction Générale Direction Technique
AccèsFinancier	Direction Générale Direction Financière

Les Directeurs généraux ont accès à tous les dossiers, ce qui explique leur présence au sein de tous les groupes locaux.

3. CREATION DES MODELES DE COMPTES

- ?? Permet la création simplifiée et sûre des comptes utilisateurs
- ?? Utiliser une nomenclature pour les différencier des comptes valides (une pratique courante consiste à utiliser un _ comme préfixe), ces comptes doivent être désactivés : _Directeur, _Financier, _Technicien
- ?? Dans les profils du modèle, spécifier les informations suivantes :

CHAMP	CONTIENT
Chemin du profil	\\SERVEUR\PROFILES\$\%USERNAME%
Script d'ouverture de session	Init_DG.cmd (pour Direction Générale), Init_DT.cmd (pour Direction Technique) et Init_DF.cmd (pour Direction Financière)
Dossier de Base	\\SERVEUR\USERS\$\%USERNAME%

- ?? Mettre les appartenances aux groupes globaux (le modèle _Directeur appartient au groupe Direction Générale).
- ?? Penser à supprimer le dossier du compte modèle que le gestionnaire des utilisateurs crée systématiquement.

4. MISE A JOUR DES PERMISSIONS

Revenons sur les permissions des dossiers communs et modifions les afin de prendre en compte les groupes locaux.

Les permissions deviennent, pour le dossier DirGen par exemple :

NTFS	PARTAGE
Administrateurs : Contrôle Total	Administrateurs : Contrôle Total
AccèsGénéral : Modifier	AccèsGénéral : Modifier

Avec la permission Modifier au lieu de contrôle total, les utilisateurs ne peuvent pas prendre possession ou changer les permissions des fichiers contenus dans le dossier commun.

5. SCRIPT D'OUVERTURE DE SESSION

Créer un fichier texte dans C:\WINNT\SYSTEM32\REPL\IMPORT\SCRIPTS\ pour chaque groupe : init_DG.cmd , init_DF.cmd , init_DT.cmd.

Le script doit connecter le lecteur partagé pour le département :
NET USE W: \\SERVEUR\DIRGEN\$/PERSISTENT:NO

Le script doit synchroniser l'heure de la station avec celle du serveur :

NET TIME \\SERVEUR /SET /Y

Ainsi, le script dans C:\WINNT\SYSTEM32\REPL\IMPORT\SCRIPTS\initDG.cmd contiendra par exemple :

```
@echo off
@rem Script de Connexion Direction GENERALE      28/03/2000
@echo Connexion au lecteur commun Direction Générale
NET USE W: \\SERVEUR\DIRGEN$/PERSISTENT:NO
@echo Connexion au lecteur commun Direction Financière
NET USE X: \\SERVEUR\DIRFI$/PERSISTENT:NO
@echo Connexion au lecteur commun Direction Technique
NET USE Y: \\SERVEUR\DIRTECH$/PERSISTENT:NO
NET TIME \\SERVEUR /SET /Y
```

6. CREATION DES COMPTES

- ?? Copier le modèle concerné avec F8, mettre le nouveau nom d'utilisateur ainsi que son mot de passe.
- ?? Si nous souhaitons que chaque utilisateur possède une unité connectée sur son répertoire personnel, nous devons partager ce dossier manuellement et mettre les permissions adéquates :
 - ?? Partager le dossier de l'utilisateur (partage caché avec \$) , exemple : PPRUT\$
 - ?? Mettre les permissions suivantes (dans le cas de l'utilisateur PPRUT)

NTFS	PARTAGE
Administrateur : Contrôle Total	Administrateur : Contrôle Total
PPRUT : Modifier	PPRUT : Modifier

- ?? modifier ensuite le chemin du Répertoire de Base en spécifiant le partage caché (par exemple : \\SERVEUR\USERS\$%\USERNAME% devient \\SERVEUR\PPRUT\$)

7. RESTRICTION DES ORDINATEURS POUR L'ACCES

Sur les Workstation, utiliser le gestionnaire des utilisateurs (musrmgr.exe), retirer le Groupe Global Utilisateurs du Domaine du Groupe local Utilisateurs.

Ajouter alors le groupe global autorisé pour l'accès dans le groupe local Utilisateurs.

Par exemple, nous retirerons Utilisateurs du Domaine pour ajouter le groupe global Direction Générale dans Utilisateurs