http://WWW.CABARE.NET ©

XP & Système Fichier NTFS – sys 20 - sys 22– cours & tp-

Le Système de Fichier NTFS sous XP

Michel Cabaré – Ver 1.2 – Janv 2008-

Xp & Système Fichiers NTFS
Cours - TP

Michel Cabaré – Ver 1.2 – janvier 2008

www.cabare.net ©

TABLE DES MATIÈRES

FAT 32 - NTFS 4

SYSTEME DE FICHIER FAT-FAT32-NTFS : 4
Quant utiliser FAT32 : 4
Quand utiliser le Système NTFS : 5
VERSIONS-NTFS : 5

ACCES AUX PERMISSIONS NTFS 6

DESACTIVATION PARTAGES SIMPLIFIES : 6
AFFICHER PARTAGE ET SECURITE : 7
LE CAS XP HOME : 7

SECURITE NTFS 9

ACL ET ACE : 9
PERMISSIONS SUR DOSSIERS : 9
PERMISSIONS SUR FICHIERS : 10
PERMISSIONS STANDARD ET SPECIALES : 10
COMBINAISON FICHIER – DOSSIER EN NTFS: 12
Exemple 1 : (fichier contre dossier) 12
Exemple 2 : (combinaison sur dossier) 12
Exemple 3 : (combinaison dossier - fichier) 12
PERMISSION NTFS ET D'AUTORISATIONS DE PARTAGE (RESEAU): 13
Exemple 1 : 13
Exemple 2 : 13

HERITAGE NTFS 14

NOTION D'HERITAGE 14
CASSER UN HERITAGE 15
RECREER UN HERITAGE 15
RECREER PLUSIEURS HERITAGES 16

PROPRIETE NTFS 17

NOTION DE PROPRIETE 17
PRENDRE POSSESSION DES DOSSIERS ET FICHIERS 17
REGLES "D'AFFECTATION" DES PERMISSIONS NTFS: 19

COPIER-DEPLACER EN NTFS 20

CREER – COPIER- - DEPLACER 20
SENSIBILISATION AUX FINESSES DE L'INTERFACE 20
XCOPY 21
CACLS 22
XCACLS 22
SUBINACL 22

PERMISSIONS NTFS PAR DEFAUT 23

SUR UNE MACHINE INSTALLEE EN FAT PUIS CONVERTIE EN NTFS : 23
SUR UNE MACHINE INSTALLEE EN NTFS : 23
DISQUE SYSTEME XP : 24

VOIR LES AUTORISATIONS NTFS 25
AUTORISATIONS EFFECTIVES : 25
UTILITAIRE ACCESSCHK 26
TP DROITS NTFS 1° 28
OBJECTIF : 28
PERMISSIONS DE PARTAGE : 28
PERMISSIONS DE SECURITE : 28
NOTION DE CREATEUR PROPRIETAIRE : 30
TP DROITS NTFS 2° 31
OBJECTIF : 31
GROUPES ET COMPTES : 31
PARTAGES : 32
PERMISSIONS NTFS : 32
CREATEUR PROPRIETAIRE : 34
TP APPROPRIATION DE FICHIER 35
DESCRIPTIF DU PROBLEME : 35
RAISONNEMENT : 36
TP COPIE FICHIER - PERMISSIONS 38
OBJECTIF : 38
COMMANDE XCOPY : 38
COPIE DE PARTAGE ? : 39

FAT 32 - NTFS

Système de Fichier Fat-Fat32-NTFS :

Comparaison des caractéristiques principales

	NTFS 4.0 – 5.0	FAT – FAT32 – FAT32X
Sécurité	Quels utilisateurs / Groupes bénéficient des différents types d'accès à un fichier ou à un répertoire.	Les fichiers ne sont pas protégés.
Journal des activités	journal des activités permettant de restaurer le disque si problèmes	pas de journal.
Services	Cryptage, Quota…	Aucun service
Compression de fichier	Prend en charge la compression flexible par fichier.	La compression de fichiers n'est pas prise en charge.
Compatibilité du système d'exploitation	NT2000 gère NTFS 4.0 et 5.0 NT 4.0 >= Sp4 gère NTFS 4.0 et lit NTFS 5.0 (mais ne gère pas les nouveautés…) NT4.0 < Sp4 gère que NTFS 4.0	Permet l'accès aux fichiers lorsque l'ordinateur exécute un autre système d'exploitation, tel que MS-DOS

Comparaison des tailles de disques et de fichiers

NTFS	FAT	FAT32-FAT32X
taille minimale recommandée 10 Go taille maxi recommandée 2 Téraoctets	Volumes compris entre la taille d'une disquette et 2 Go	Volumes compris entre 512 Mo et 32 Go
Ne peut pas être utilisé sur des disquettes		formate jusqu'à 32 Go (peut lire plus…)
La taille des fichiers est limitée que par la taille du volume	Taille maximale des fichiers : 2 Go	Taille maximale des fichiers : 4 Go

Quant utiliser FAT32 :

Le système de fichiers FAT32, version améliorée du système de fichiers FAT, peut être utilisé sur les disques durs d'une taille comprise entre 512

mégaoctets (Mo) et 2 téraoctets (To) Mais seuls 32Giga sont adressables par Windows 2000-XP.

- Formatez la partition avec FAT32 si la partition d'installation est supérieure à 2 gigaoctets (Go) et si vous utilisez un double amorçage de Windows 2000 avec Windows 95OSR2, Windows 98.

N.B: Si vous choisissez un formatage FAT lors de l'installation de Windows 2000 avec une partition supérieure à 2 Go, le formatage se fera en FAT32.

N.B: Pour une partition de plus de 32Giga, seul NTFS sera proposé

Quand utiliser le Système NTFS :

- Une sécurité d'accès pour les fichiers.
- Pour implémenter **Active Directory** sur un serveur
- Cryptage des fichiers : via **EFS** notamment.
- Quotas de disque : Analyse / contrôle d'espace utilisée par personne.
- La prise en charge de disques durs de très grande capacité très largement supérieure à celle des systèmes FAT32

N.B: Si vous formatez une partition avec NTFS seul Windows NT… pourra accéder aux fichiers créés ultérieurement sur cette partition.

Versions-NTFS :

Il est possible d'avoir les versions du système NTFS par la commande

fsutil fsinfo ntfsinfo x:

```
C:\Users\Administrateur>fsutil fsinfo ntfsinfo C:
Numéro de série du volume NTFS :   0xe63cb4f03cb4bd3d
Version :                          3.1
```

les versions stables les plus répandues sont:

1.2 présente avec Windows NT 4.0

3.0 dite aussi 5.0 apparue avec Windows 2000

Apparition de la notion de quota

3.1 dites aussi 5.1, apparue avec Windows XP, Windows Server 2003,

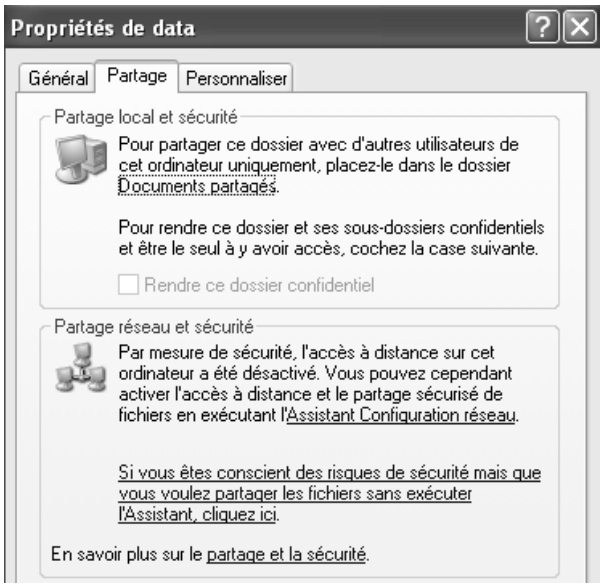
avec Vista, puis Seven apparition de la notion de lien symbolique vers un autre système de fichier, un dossier ou un fichier

ACCES AUX PERMISSIONS NTFS

Désactivation partages simplifiés :

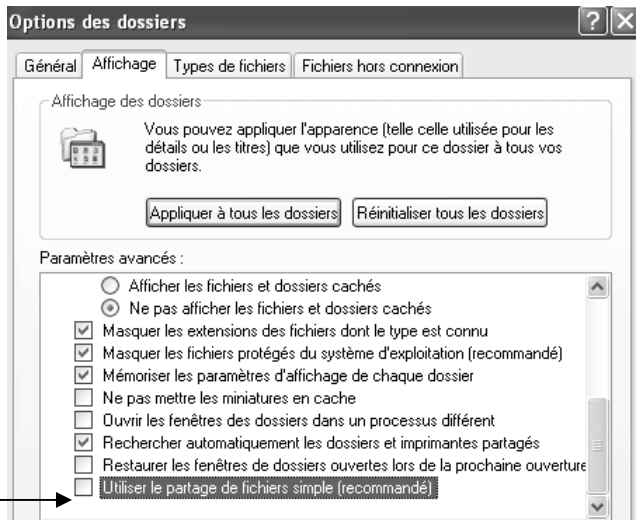
Par défaut Sous un poste Xp (hors domaine) on effectue un amalgame partage réseau/ sécurité fichier

Cette valeur cochée par défaut fait que lorsque l'on demande les propriétés d'un dossier on trouve un seul onglet **Partage**



Lorsque l'on désactive les partages simplifiés, dans le menu

outils / options des dossiers / affichage



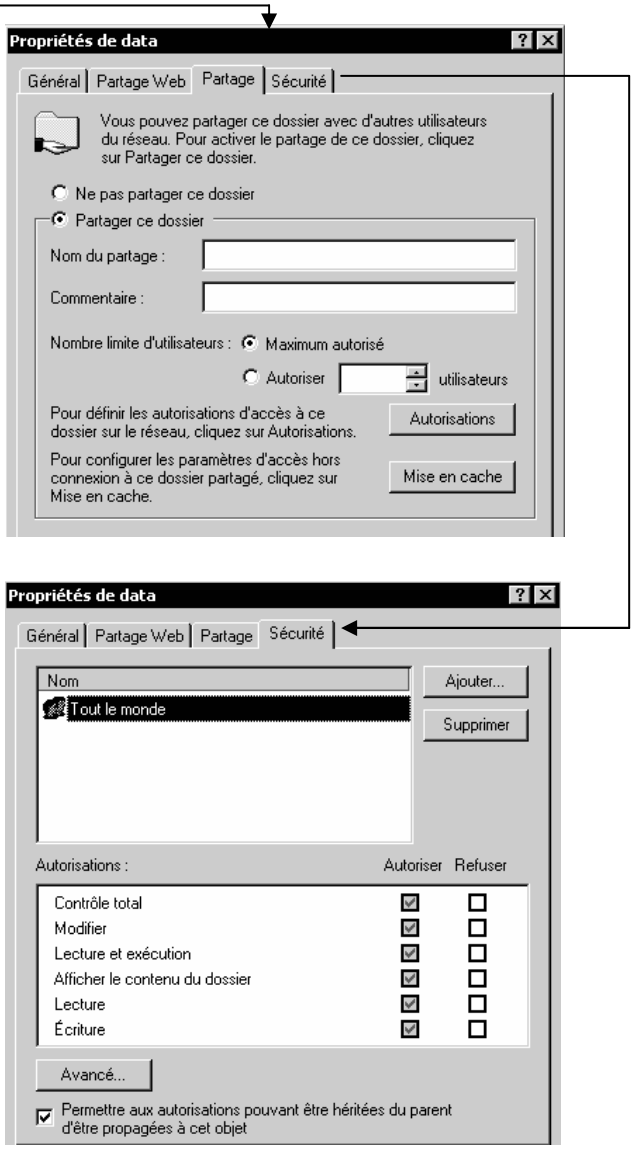
Alors on distingue **Partage**, et **Sécurité** – (Protection des fichiers) comme dans le chapitre suivant.

Afficher Partage et Sécurité :

A partir du moment ou l'on se trouve sur un lecteur en NTFS en cliquant sur **propriété** ...

On a bien accès a l'onglet "**Partage**"

mais aussi à un onglet "**Sécurité**



Le système NTFS sécurise l'accès au fichiers et au dossiers non seulement depuis les accès réseaux mais également depuis les accès locaux. A ce titre on sait que les permissions sont inclues dans les fichiers, dossiers, au niveau du disque lui-même

Sur un lecteur formaté NTFS on pourrait continuer à travailler avec l'onglet Partage en demandant Autorisation pour gérer les demandes d'accès depuis le réseau, mais il vaut mieux utiliser l'onglet "**Sécurité**" pour la sécurité. En effet ce sont les droits les plus restrictifs qui prédominent, par conséquent au niveau "Partage" on laissera le Contrôle Total à Tout le monde et on travaillera au niveau de l'onglet Sécurité

Le cas XP HOME :

Affichage « temporaire » des sécurité NTFS

Sur un poste XP home, l'onglet sécurité n'apparaît pas… vous pouvez accéder tout de même à l'onglet sécurité après avoir

- démarré en mode sans échec (via F8 lors du boot)
- et s'être connecté avec le compte Administrateur (celui crée lors de l'installation de XP, et pas simplement un compte ayant des droits d'administration)
- Désormais si le lecteur est en NTFS, les propriétés du dossier affichent un onglet sécurité !
- Après modifications éventuelles et re-démarrage, l'onglet disparaît…

L'idée générale est donc de ne pas permettre en standard l'affichage du panneau sécurité NTFS pour un poste Windows HOME

Affichage « permanent » des sécurité NTFS

Malgré ce que l'on vient de dire précédemment, il est possible de demander de faire afficher systématiquement l'onglet de gestion de la sécurité NTFS, mais cette opération n'est pas supportée par microsoft, et ne doit en aucun cas être généralisée…

Avec un fichier scesp4i.exe (en provenance serveur FTP microsoft)

1. Télécharger le "**Security Configuration Manager**" de Windows NT4, disponible chez Microsoft :

   ftp://ftp.microsoft.com/bussys/winnt/winnt-public/tools/scm/scesp4i.exe (Taille : 2.68 Mo)

2. Ne pas exécuter directement le fichier **scesp4i.exe**, mais le décompresser (avec Winzip, Winrar,..) dans un dossier quelconque (par exemple c:\scesp4i).

3. Effectuer un clic droit sur le fichier SETUP.INF qui se trouve dans ce dossier (attention, il existe plusieurs fichiers xxxx.INF), puis sélectionner "Installer"

   En effet, si on l'exécute, une routine de détection de version du système est lancée, et, constatant qu'on n'est pas sous NT4, refuse l'installation !

4. Un écran vous demande alors si vous souhaitez remplacer le fichier ESENT.DLL, refusez en cliquant sur NON POUR TOUS (Ne cliquez en aucun cas sur oui, cela rendrait votre système instable!)

5. Redémarrer votre poste de travail

Avec un fichier **ntfs.exe** (en provenance de NT4.0)

1. installer l'utilitaire NTFS.EXE

2. Dans le répertoire de décompression, sélectionnez SETUP.INF,click droit/Installer

3. Un écran vous demande alors si vous souhaitez remplacer le fichier ESENT.DLL, refusez en cliquant sur NON POUR TOUS (Ne cliquez en aucun cas sur oui, cela rendrait votre système instable!)

4. Redémarrer votre poste de travail

SECURITE NTFS

ACL et ACE :

Le système NTFS stocke une liste de contrôle d'accès nommée **ACL** (**Access Control List**) associée à chaque fichier et dossier d'une partition NTFS.

La liste ACL contient tous les groupes d'utilisateurs; tous les utilisateurs bénéficiant de l'accès au dossier ou au fichier, avec le type d'accès qui leur est accordé.

Pour qu'un utilisateur puisse accéder à un fichier ou à un dossier, la liste **ACL** de ce fichier dossier doit contenir une entrée, appelée **ACE** (**Access Control Entry**) auquel l'utilisateur est associé.

Si aucune entrée **ACE** n'existe dans la liste **ACL** de la ressource, l'utilisateur ne peut accéder à cette ressource.

Permissions sur Dossiers :

Il est possible en NTFS de définir 6 sortes principales de permissions sur un dossier, via l'onglet **Sécurité**

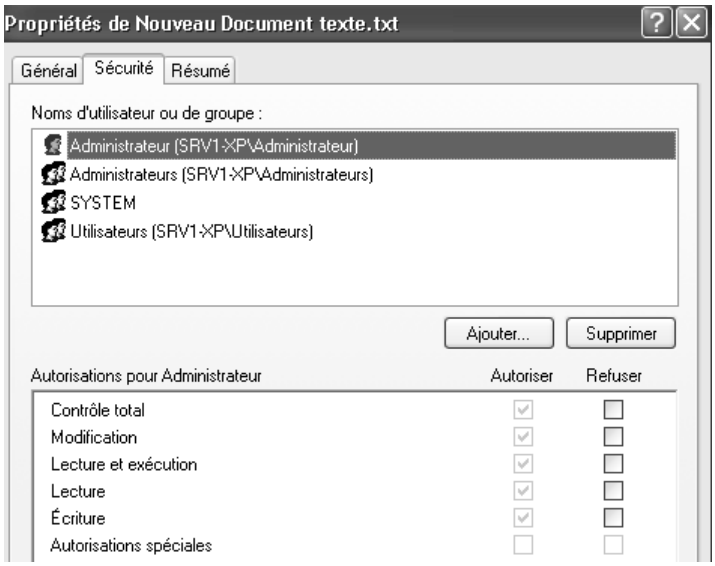
Ces 6 combinaisons standard, peuvent être **héritées** (dans ce cas elles sont grisées)

Et ont deux valeurs possibles **Autoriser**, ou **Refuser**

Les autorisations Spéciales ne sont que des combinaisons particulières (détaillées dans permissions spéciales plus loin) , posées entre les dossiers et les fichiers… Il n'est pas nécessaire de s'en préoccuper car elles sont gérées automatiquement souvent par le système

Permissions sur fichiers :

Il est possible en NTFS de définir 5 sortes principales de permissions Il manque afficher) sur un fichier, via l'onglet **Sécurité**



Ces 5 combinaisons standard, peuvent être **héritées** (dans ce cas elles sont grisées)

Et ont deux valeurs possibles **Autoriser**, ou **Refuser**

N.B: DANS UN SOUCIS DE SIMPLIFICATION, ON NE DEVRAIT JAMAIS DONNER DES PERMISSIONS AU NIVEAU DES FICHIERS, MAIS TOUJOURS PLUS GLOBALEMENT AU NIVEAU DES DOSSIERS

Permissions standard et spéciales :

En fait, les permissions standards, ne sont qu'une combinaison prédéfinie d'un certain nombre de permissions spéciales, plus fines

Autorisations de fichier et de dossier

Autorisations spéciales	Contrôle total	Modifier	Lire & exécuter	Afficher le contenu du dossier (dossiers uniquement)	Lecture	Écriture
Parcourir le dossier / Exécuter le fichier	x	x	x	x		
Liste du dossier / Lecture de données	x	x	x	x	x	
Attributs de lecture	x	x	x	x	x	
Lire les attributs étendus	x	x	x	x	x	
Création de fichiers / Écriture de données	x	x				x
Création de dossiers / Ajout de données	x	x				x
Attributs d'écriture	x	x				x
Écriture d'attributs étendus	x	x				x
Suppression de sous-dossiers et de fichiers	x					
Supprimer	x	x				
Autorisations de lecture	x	x	x	x	x	x
Modifier les autorisations	x					
Appropriation	x					
Synchroniser	x	x	x	x	x	x

N.B: ici il y a une différence importante entre **Modifier** et **Contrôle Total**, c'est la possibilité de supprimer ou non les sous-dossier …

N.B: DANS UN SOUCIS DE SIMPLIFICATION, ON NE DEVRAIT JAMAIS DANS UN 1° TEMPS TRAVAILLER AU NIVAU DES PERMISSIONS SPECIALES MAIS TOUJOURS AU NIVEAU DES PERMISSIONS STANDARDS…

Microsoft détaille les permissions spéciales ainsi:

Parcourir le dossier / Exécuter le fichier	**Pour les dossiers :** L'autorisation Parcourir le dossier permet à l'utilisateur de se déplacer dans les dossiers pour atteindre d'autres dossiers ou fichiers, même s'il n'est pas muni des autorisations correspondant aux dossiers ainsi parcourus (cette autorisation s'applique uniquement aux dossiers). Elle n'est effective que lorsque le groupe ou l'utilisateur n'a pas reçu le droit **Outrepasser le contrôle de parcours** dans le composant logiciel enfichable Stratégie de groupe (par défaut, ce droit est octroyé au groupe Tout le monde). **Pour les fichiers :** L'autorisation Exécuter le fichier permet ou interdit l'exécution de fichiers programmes (cette autorisation s'applique uniquement à des fichiers). L'établissement de l'autorisation Parcourir le dossier sur un dossier n'entraîne pas automatiquement l'établissement de l'autorisation Exécuter le fichier sur tous les fichiers contenus dans le dossier.
Liste du dossier / Lecture de données	L'autorisation Liste du dossier permet ou interdit l'affichage des noms des fichiers et des sous-dossiers contenus dans le dossier. Cette autorisation affecte uniquement le contenu de ce dossier et n'a aucune influence sur l'affichage ou non du dossier pour lequel vous définissez l'autorisation. Cette autorisation s'applique uniquement aux dossiers. L'autorisation Lecture de données permet ou interdit l'affichage des données des fichiers (cette autorisation s'applique uniquement aux fichiers).
Attributs de lecture	Permet ou interdit l'affichage des attributs d'un fichier ou d'un dossier, tels que les attributs Lecture seule ou Masqué. Les attributs sont définis par le système de fichiers NTFS.
Lire les attributs étendus	Permet ou interdit l'affichage des attributs étendus d'un fichier ou d'un dossier. Les attributs étendus sont définis par des programmes et peuvent varier selon le programme utilisé.
Création de fichiers / Écriture de données	L'autorisation Création de fichiers permet ou interdit de créer des fichiers au sein du dossier (cette autorisation ne s'applique qu'aux dossiers). L'autorisation Écriture de données permet ou interdit de modifier le fichier et d'en remplacer le contenu actuel (cette autorisation ne s'applique qu'aux fichiers).
Création de dossiers / Ajout de données	L'autorisation Création de dossiers permet ou interdit de créer des dossiers au sein du dossier (cette autorisation ne s'applique qu'aux dossiers). L'autorisation Ajout de données permet ou interdit de modifier la fin du fichier mais pas de modifier, de supprimer ou de remplacer les données existantes (cette autorisation ne s'applique qu'aux fichiers).
Suppression de sous-dossiers et de fichiers	Permet ou interdit de supprimer des sous-dossiers et des fichiers même si l'autorisation Supprimer n'a pas été octroyée pour le sous-dossier ou le fichier concerné (cette autorisation s'applique à des dossiers).
Supprimer	Permet ou interdit de supprimer le fichier ou le dossier. Vous pouvez supprimer un fichier ou un dossier sur lequel vous ne possédez pas l'autorisation Supprimer si vous disposez de l'autorisation Suppression de sous-dossiers et de fichiers relative au dossier parent.
Autorisations de lecture	Permet ou interdit les autorisations de lecture du fichier ou du dossier, telles que Contrôle total, Lecture et Écriture.
Modifier les autorisations	Permet ou interdit de modifier les autorisations du fichier ou du dossier, telles que Contrôle total, Lecture et Écriture.
Appropriation	Permet ou interdit de prendre possession du fichier ou du dossier. Le propriétaire d'un fichier ou d'un dossier peut en modifier les autorisations à tout moment, indépendamment des autorisations existantes.

Avec encore

Attributs d'écriture	Permet ou interdit de modifier les attributs d'un fichier ou d'un dossier tels que les attributs Lecture seule ou Masqué. Les attributs sont définis par le système de fichiers NTFS.
Écriture d'attributs étendus	Permet ou interdit la modification des attributs étendus d'un fichier ou d'un dossier. Les attributs étendus sont définis par des programmes et peuvent varier selon le programme utilisé. L'autorisation Écriture d'attributs étendus n'implique pas la création ou la suppression de fichiers ou de dossiers ; elle inclut uniquement l'autorisation de modifier les attributs d'un fichier ou d'un dossier. Pour
Synchroniser	Permet ou interdit que des threads différentes attendent le handle du fichier ou du dossier et se synchronisent à une autre thread qui l'a signalé. Cette autorisation s'applique uniquement aux programmes multi-thread et multitraitement.

Combinaison Fichier – Dossier en NTFS:

Plusieurs règles régissent les combinaisons de permission NTFS

1. Les permissions de fichier **sont prioritaires** par rapport aux permissions affectées aux dossiers qui les contiennent :
2. la permission effective de l'utilisateur est la permission la moins restrictive obtenue par la **combinaison des différentes permissions**
3. si la permission "aucun accès" est donnée, cette dernière **prime sur les autres permissions**, et la permission effective est "aucun accès"

Donc si l'utilisateur est membre de plusieurs groupes, la permissions résultant finale est :

la somme de toutes les permissions définies à travers chacun des groupes,

sauf si la permission "aucun accès" est spécifiée pour au moins un groupe !

Exemple 1 : (fichier contre dossier)

Un utilisateur ayant le droit "**lire**" pour un **dossier**, et un droit "**écrire**" pour un **fichier de ce même dossier**,

alors il pourra modifier le fichier (écrire dedans) mais pas créer un autre fichier dans ce dossier…

Exemple 2 : (combinaison sur dossier)

Un utilisateur **Util1** dispose de la permission **Ecrire** sur un dossier **Données**

mais **Util1** est également membre d'un groupe "**Tout le monde**" qui dispose de la permission **Lire** sur ce même dossier

Util1 se retrouve avec la permission **Lire** et **ecrire** sur ce dossier **Données**

Exemple 3 : (combinaison dossier - fichier)

Un utilisateur **Util1** dispose de la permission **Lire** et **Ecrire** sur un fichier **Fichier1** du dossier **Données**

mais **Util1** est également membre d'un groupe "**commerciaux**" qui dispose des permissions **lire** sur ce même dossier **Données**

Util1 se retrouve avec la permission **Lire** sur ce dossier **Données** mais avec **Lire** et **Ecrire** sur le fichier **Fichier1** du dossier **Données**

Permission NTFS et d'Autorisations de partage (réseau):

Dans ce cas, la résultante est la combinaison la plus restrictive des deux

Exemple 1 :

Un utilisateur **Util1** dispose lors d'une connexion réseau de l' **autorisation** "**lire**" au niveau du partage pour un dossier partagé nommé **public** ,sur un **ordinateur1** et de la **permission NTFS contrôle total** sur un **fichier A** s'y trouvant.

Q: Quelle est la permission effective de **Util1** lorsqu'il accède au fichier **A** à travers **l'accès réseau** au dossier partagé **Données** ?

R: Depuis un accès réseau la permission effective de Util1 pour le fichier A est lire car celle-ci est plus restrictive que celle attribuée en NTFS localement, et s'applique

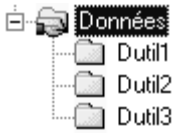
Q: Quelle est la permission effective de **Util1** lorsqu'il accède au fichier **A** à travers **une session locale** sur la machine ?

R: Depuis une session locale sur ordinateur1 la permission effective de Util1 pour le fichier A est contrôle total

Exemple 2 :

Un dossier **Données** est crée avec à l'intérieur 3 sous-dossiers nommés **Dutil1**, **Duitl2** et **Dutil3** respectivement

Le dossier **Données** est partagé avec l'autorisation **contrôle total** pour un **groupe Utilisateurs.**



Les 3 Utilisateurs **Util1**, **Util2** et **Util3** font partie du **groupe Utilisateurs** mais ne disposent de la permission **NTFS contrôle total** que pour leur **propre dossier**

Q : Quelle est la permission effective de **Util1** lorsqu'il accède au dossier **Dutil1** à travers **l'accès réseau** au dossier partagé **Données** ?

R : Util1 dispose de la permission contrôle total sur le dossier Données et son dossier Dutil1

Q : Quelle est la permission effective de **Util2** pour le dossier **Dutil1**

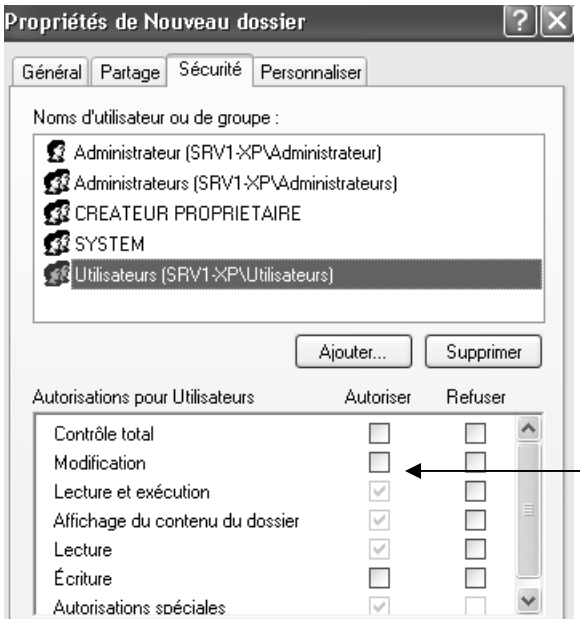
R : Util2 ne bénéficie pas de l'accès au dossier Dutil1 car la permission NTFS contrôle total sur ce dossier à été attribuée uniquement a Utils1

HERITAGE NTFS

Notion d'héritage

Donc lorsque l'on **crée** un dossier (ou respectivement un fichier) , celui-ci **hérite** des droits du dossier à l'intérieur duquel il a été crée

Visuellement cela se traduit par le fait que les propriétés sont grisées, et semblent donc non modifiables.



Ici le groupe des utilisateurs est manifestement en lecture seule, non modifiable…

Il serait possible de rajouter des permissions

Modification

Mais pas de modifier les permissions existantes

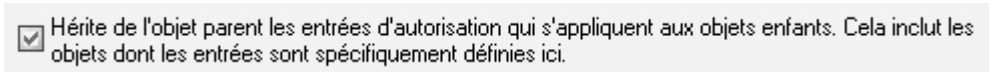
Si on modifie les permissions des parents, seuls sont concernés alors ensuite dans l'arborescence ceux qui ont accepté l'héritage (sous NT 4 on demandait d'appliquer au dossier et aux fichiers … sans discrimination !)

NB : Si les autorisations de l'objet ont été **héritées** de l'objet parent. Les modifications peuvent s'effectuer de trois manières :

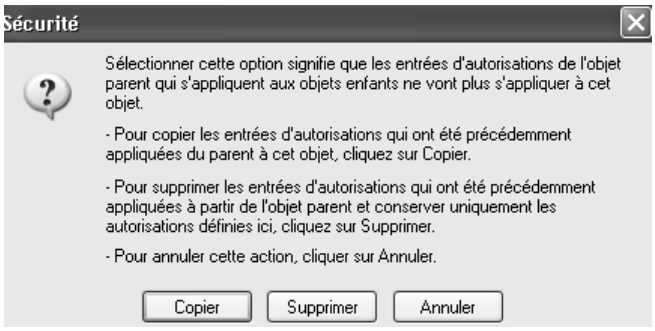
- Exécutez les modifications sur l'objet parent ; l'objet héritera alors de ces autorisations.
- Sélectionnez l'autorisation opposée (**Autoriser** ou **Refuser**) pour substituer l'autorisation héritée.
  PEU CONSEILLE !
- Casse l'héritage en désactivant la case à cocher
  Permettre aux autorisations pouvant être héritées du parent d'être propagées à cet objet.
  On peut alors modifier les autorisations et supprimer des utilisateurs ou des groupes. Mais l'objet n'héritera plus de l'objet parent…

Casser un héritage

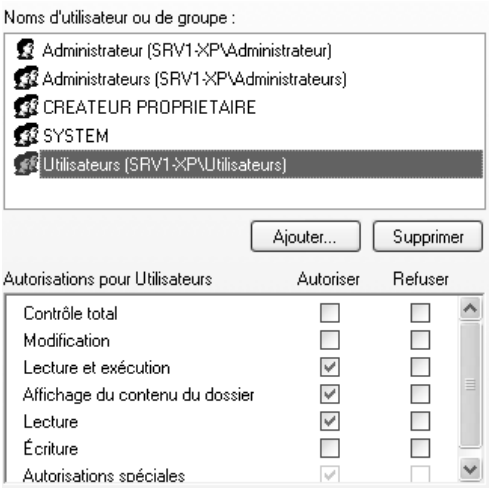
N.B : si on veut pouvoir modifier directement les permissions, il est nécessaire d'abords de désactiver la case à cocher « Permettre aux autorisations pouvant être héritées du parent… »



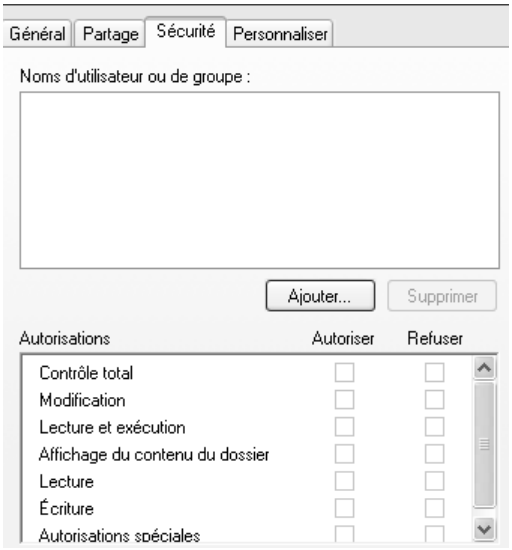
Dans ce cas, on peut choisir si on veut les supprimer complètement ou les appliquer à notre arborescence mais pouvoir les modifier…



Si **Copier**



Si **Supprimer**



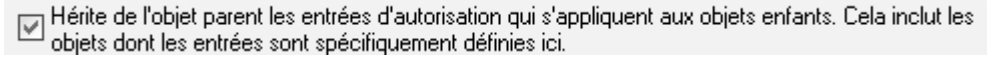
Recréer un héritage

Soit un dossier **test-ntfs**, sur lequel , après avoir cassé l'héritage en supprimant toutes les permissions, on a posé la sécurité suivante :

Compte Administrateur	Contrôle Total
Groupe Tout le Monde	Lecture Seule

On crée un sous dossier **sous-test**. Vérifier de quoi ce sous dossier hérite…

En se replaçant sur le dossier **test-ntfs** on reconstruit l'héritage d'origine en cochant **Hérite de l'objet parent…**



Vérifier les nouvelles permissions …

Recréer plusieurs héritages

Soit un dossier **test-ntfs**, sur lequel , après avoir cassé l'héritage en supprimant toutes les permissions, on a posé la sécurité suivante :

Compte Administrateur	Contrôle Total
Groupe Tout le Monde	Lecture Seule

On construit trois sous-dossiers, respectivement **sstest1, sstest2, sstest3**, qui héritent donc de la sécurité du dossier parent.

pour **sstest1** on, casse l'héritage en copiant les permissions

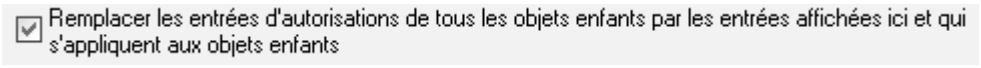
pour **sstest2** on, casse l'héritage en supprimant les permissions

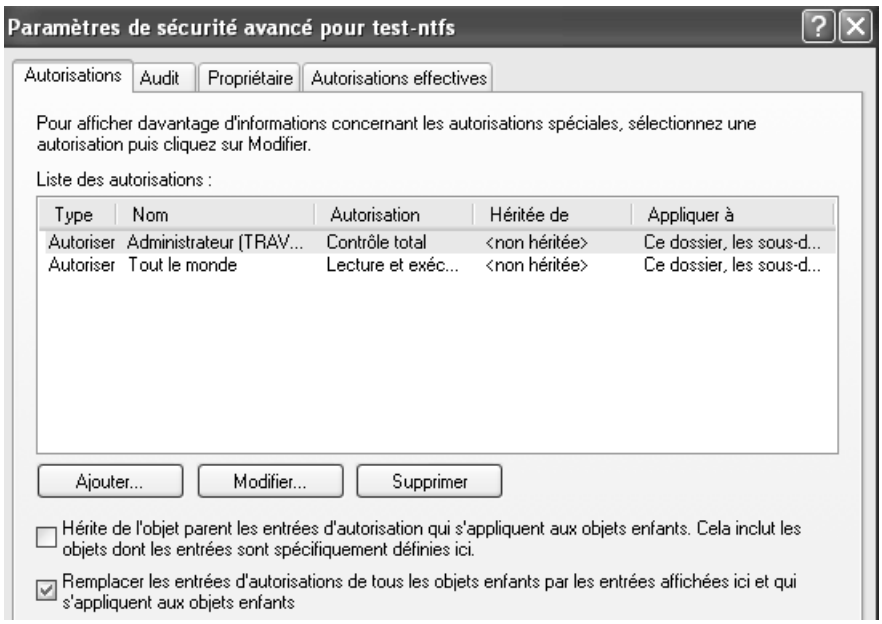
pour **sstest3** on, casse l'héritage en copiant les permissions et ajout du groupe des utilisateur- en Modifier

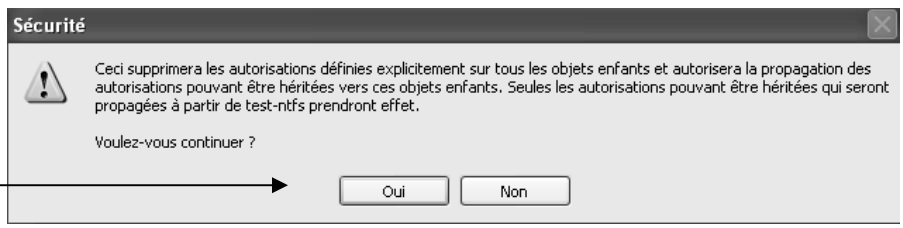
On souhaite ensuite "retrouver" notre structure de départ :

Il faut depuis le dossier **test-ntfs**, demander la case à cocher

Remplacer les entres d'autorisation de tous les objets enfants…







PROPRIETE NTFS

Notion de Propriété

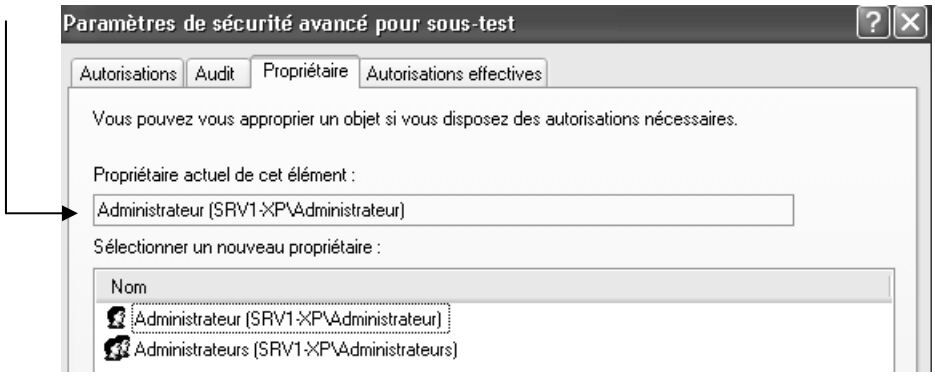
Par défaut l'utilisateur qui crée un dossier ou un fichier en est le propriétaire.

C'est la raison du groupe prédéfini **Créateur Propriétaire**, qui est géré automatiquement par Windows (on ne peut spécifier qui fait partie de ce groupe, ni savoir qui en fait partie… cela dépends de l'objet que l'on pointe !)

N.B : En tant que propriétaire on peut toujours redéfinir des permissions de dossier ou son fichier.

Un utilisateur peut attribuer la permission "**Prendre possession**" aux autres utilisateurs ou groupe

Pour connaître qui est propriétaire d'un objet, on demande pour un dossier-fichier Paramètres avancés onglet **Propriétaire**



Prendre possession des dossiers et fichiers

On peut s'approprier un objet :

- si on en a les droits
- si l'on est administrateur

Mais on ne peut pas « rendre » la propriété… Un administrateur ne peut pas "donner" une ressource, le futur propriétaire doit toujours se l'approprier…

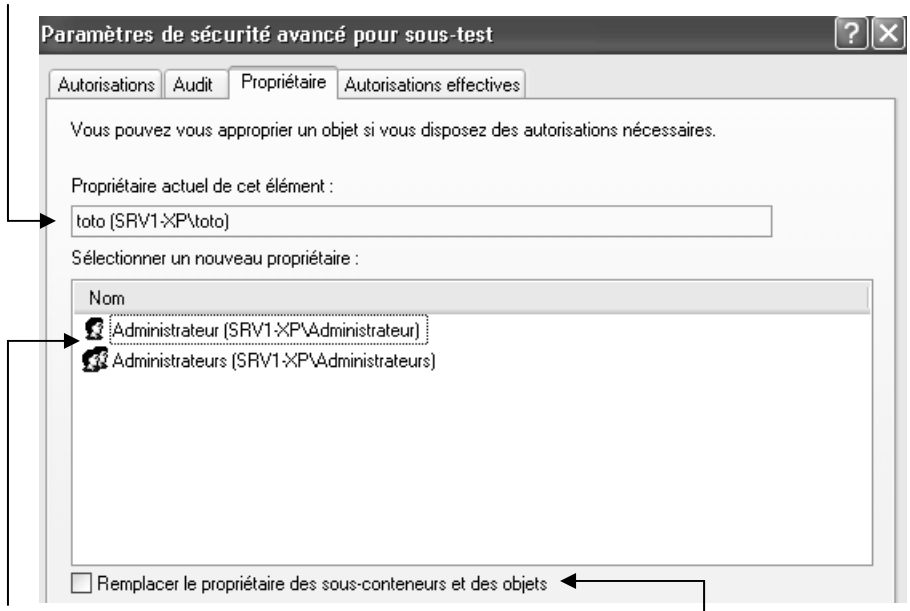
Ce qui fait que cela ne peut pas se faire à l'insu du propriétaire légitime…

par défaut les membres du groupe Administrateurs ont toujours la possibilité de prendre possession d'un fichier :

- en ouvrant une session en tant qu'Administrateur
- a partir de l'onglet sécurité on peut demander **avancé** pour déterminer le propriétaire ou sur **Appropriation** pour "devenir" le propriétaire

imaginons que cela soit toto qui ait crée le dossier sous-test

En tant qu'administrateur, si on va regarder qui est propriétaire de ce dossier on trouve normalement toto…

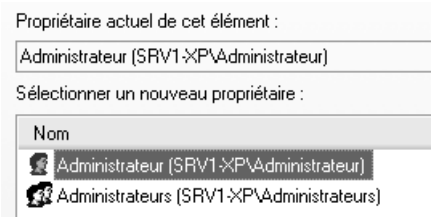


Mais on peut s'approprier l'objet

Et éventuellement tout le contenu de l'arborescence…

N.B : cela ne change en aucune manière pour l'instant les permissions existante, sauf que maintenant l'administrateur aussi a le droit de travailler et modifier la sécurité dans ce dossier…

N.B : mais pas à l'insu de l'utilisateur toto, qui, s'il demande qui est le propriétaire de son dossier va voir désormais



EXEMPLE :

Si un utilisateur quitte la société (compte supprimé) , l'administrateur prends possession du fichier, et modifie les permissions afin de ré-autoriser l'accès à cette donnée à un autre utilisateur, qui pourra alors s'approprier cette donnée…

Règles "d'affectation" des permissions NTFS:

Deux règles essentielles existent

Pour les dossiers contenant des programmes

1. Enlever la permissions par défaut "Contrôle total" attribuée à tout le monde, et la donner uniquement au Groupe des administrateurs
2. Pour les responsables des mises à jour, donner une permissions contrôle total
3. Pour les utilisateurs, s'ils doivent avoir accès au dossier, donner une permissions lecture seule

Pour les dossiers contenant des données

1. Enlever la permissions par défaut "Contrôle total" attribuée à tout le monde, et la donner uniquement au Groupe des administrateurs
2. Pour les utilisateur donner la permission lire et modifier, et au groupe Créateur Propriétaire la permission Contrôle Total. Cela permet aux utilisateurs locaux de ne détruire ou de modifier que les dossiers et les fichiers qu'ils copient ou créent sur l'ordinateur local

COPIER-DEPLACER EN NTFS

Créer – Copier- - Déplacer

Lorsque l'on **crée** un dossier, celui-ci hérite des droits du dossier à l'intérieur duquel il a été crée

Lorsque l'on **copie** un dossier ou des fichiers, les permissions **héritées** sont celles du dossier de destination. De plus, l'utilisateur qui réalise la copie **devient le propriétaire** du dossier ou du fichier.

Pour une **copie**, les permissions nécessaires sont les suivantes :

permission **lire** sur le **dossier d'origine**

permission **ajouter** sur le **dossier de destination**

Lorsque l'on **déplace** un dossier ou un fichier à l'intérieur de la même unité de disque, ses permissions d'origine ainsi que son appartenance sont maintenues. Mais si on effectue le déplacement entre différentes unités de disque; on se retrouve comme pour une copie !

Pour un **déplacement**, les permissions nécessaires sont les suivantes :

permission **ajouter** sur le **dossier de destination**

permission **Modifier** ou **Contrôle total** sur le **dossier d'origine**

N.B: bien sur toute copie/déplacement sur des unités FAT entraîne alors une perte de toutes les permissions !

Sensibilisation aux finesses de l'interface

Penser à sensibiliser vos utilisateurs à l'interface graphique ne faisant pas la même chose selon ce que :

- On glisse dans le même lecteur… (déplacer)
- On glisse d'un lecteur à l'autre… (copier)
- On glisse avec CTRL appuyé… (copier)

Et aux… copier/couper/coller…

Xcopy

Il est possible de copier les fichiers en gardant leur permissions, mais en utilisant une commande en ligne

```
C:\>xcopy /?
Copie des fichiers et des arborescences de répertoires.

XCOPY source [destination] [/A | /M] [/D[:date]] [/P] [/S [/E]] [/V] [/W]
                           [/C] [/I] [/Q] [/F] [/L] [/H] [/R] [/T] [/U]
                           [/K] [/N] [/O] [/X] [/Y] [/-Y] [/Z]
                           [/EXCLUDE:fich1[+fich2][+fich3]...]
```

parmi la multitude d'option, les plus intéressantes dans notre cas sont

/o /s

voire une combinaison du genre **/s /e/c /o** ou du genre **/c /h /o /s /e** …

```
/A          Copie uniquement les fichiers ayant l'attribut archive, ne
            modifie pas l'attribut.
/M          Copie uniquement les fichiers ayant l'attribut archive,
            désactive l'attribut archive.
/D:m-j-a    Copie les fichiers modifiés à partir de la date spécifiée.
            Si aucune date n'est donnée, copie uniquement les fichiers dont
            l'heure source est plus récente que l'heure de destination.
/EXCLUDE:fich1[+fich2][+fich3]...
            Spécifie une liste de fichiers contenant des chaînes. Quand une
            de ces chaînes se retrouve dans le chemin d'accès absolu au
            fichier à copier, ce fichier est exclu de la copie. Par exemple,
            spécifier une chaîne telle que \obj\ ou .obj exclura tous les
            fichiers du répertoire obj ou tous les fichiers dont l'extension
            est .obj, respectivement.
/P          Avertissement avant la création de chaque fichier de destination.
/S          Copie les répertoires et sous-répertoires sauf ceux qui sont
            vides.
/E          Copie les répertoires et sous-répertoires, y compris vides.
            Identique à /S /E. Peut être utilisé pour modifier /T.
/V          Vérifie chaque nouveau fichier.
/W          Vous demande d'appuyer sur une touche avant la copie.
/C          Continuer la copie même si des erreurs se produisent.
/I          Si la destination n'existe pas et que plus d'un fichier est
            copié, assume que la destination est un répertoire.
/Q          N'affiche pas les noms de fichiers lors de la copie.
/F          Affiche les noms source et de destination complets à la copie.
/L          Affiche les fichiers qui seraient copiés.
/H          Copie également les fichiers cachés et les fichiers système.
/R          Remplace les fichiers en lecture seule.
/T          Crée la structure de répertoires mais ne copie pas les fichiers.
            N'inclut pas les répertoires ou sous-répertoires vides. /T /E
            inclut les répertoires et sous-répertoires vides.
/U          Copie seulement les fichiers qui existent déjà en destination.
/K          Copie les attributs. Xcopy normal rétablira les attributs de
            lecture seule.
/N          Copie en utilisant les noms courts générés.
/O          Copie les informations d'appartenance et d'ACL des fichiers.
/X          Copie les paramètres d'audit de fichiers (implique /O).
/Y          Supprime la demande de confirmation de remplacement de
            fichiers de destination existants.
/-Y         Provoque la demande de confirmation de remplacement d'un fichier
            de destination existant.
/Z          Copie les fichiers du réseau en mode redémarrable.
```

Sur une commande du genre, histoire de garder une trace des messages d'erreur, il semblerait bon de rediriger la sortie par défaut dans un fichier texte

Genre **xcopy c:*.* d:*.* /s/e/c/o > info.txt**

ici **> info.txt** permet de rediriger le flux de la sortie video par défaut dans un fichier nommé **info.txt**

Cacls

En standard, depuis 2000 PRO, Permet d'avoir un information sur les permissions NTFS, voire de les modifier.

```
E:\data>cacls
Affiche ou modifie les listes de contrôle d'accès (ACL) des fichiers

CACLS nom_de_fichier [/T] [/E] [/C] [/G util:perm] [/R util [...]]
                     [/P util:perm [...]] [/D util [...]]
   nom_de_fichier  Affiche les ACL.
   /T              Modifie les ACL des fichiers spécifiés dans le
                   répertoire en cours et tous les sous-répertoires.
   /E              Édite l'ACL au lieu de la remplacer.
   /C              Continue la modification des ACL en ignorant les erreurs.
   /G util:perm    Donne à l'utilisateur spécifié les droits d'accès.
                   Perm peut être : R  Lecture
                                    W  Écriture
                                    C  Modification (en écriture)
                                    F  Contrôle total
   /R util         Retire les droits d'accès de l'utilisateur (avec /E).
   /P util:perm    Remplace les droits d'accès de l'utilisateur spécifié.
                   Perm peut être : N  Aucun
                                    R  Lecture
                                    W  Écriture
                                    C  Modification (en écriture)
                                    F  Contrôle total
   /D util         Refuse l'accès à l'utilisateur spécifié.
Des caractères génériques peuvent être utilisés pour préciser plusieurs
fichiers dans une commande. Vous pouvez spécifier plus d'un utilisateur dans
une commande.
```

Xcacls

Utilitaire fourni avec le kit de ressource technique 2000 Pro,

Quick Details	
File Name:	xcacls_setup.exe
Version:	1.00.0.1
Date Published:	5/15/2002
Language:	English
Download Size:	582 KB

SubInACL

Utilitaire fourni avec le kit de ressource technique 2000 Pro,

Quick Details	
File Name:	subinacl.msi
Version:	5.2.3790.1180
Date Published:	6/14/2004
Language:	English
Download Size:	371 KB

PERMISSIONS NTFS PAR DEFAUT

Sur une machine installée en FAT puis convertie en NTFS :

De manière générale les permissions données sur le disque sont partout de type **Everyone – Full Control**

Sur une machine installée en NTFS :

Les dossiers Program Files et Documents & settings

```
C:\Program Files and <subfolders>
   Administrators - Full Control
   Creator/Owner - Full Control
   Users - Read
   System - Full Control
   Power Users - Change
   Terminal Server User - Change

C:\Documents and Settings
   Administrators - Full Control
   Power Users - Read
   Everyone - Read
   Users - Read
   System - Full Control
```

```
C:\Documents and Settings\Administrator and <subfolders>
   Administrator - Full Control
   Administrators - Full Control
   System - Full Control

C:\Documents and Settings\All Users and <subfolders>
   Administrators - Full Control
   Power Users - Change
   Users - Read
   Everyone - Read
   System - Full Control

C:\Documents and Settings\Default User and <subfolders>
   Administrators - Full Control
   Power Users - Read
   Users - Read
   Everyone - Read
   System - Full Control
```

Les dossiers %SystemRoot%

```
C:\%SystemRoot%
   Administrators- Full Control
   Creator/Owner - Full Control
   Everyone - Read
   Power Users - Change
   Users - Read
   System - Full Control
```

```
C:\%SystemRoot%\System
   Administrators- Full Control
   Creator/Owner - Full Control
   Power Users - Change
   Users - Read
   System - Full Control

C:\%SystemRoot%\System32
   Administrators- Full Control
   Creator/Owner - Full Control
   Power Users - Change
   Users - Read
   Everyone - Read
   System - Full Control
```

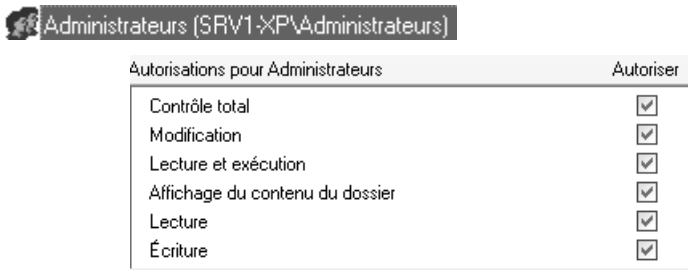
```
C:\%SystemRoot%\System32\Config
   Administrators- Full Control
   Creator/Owner - Full Control
   Power Users - Read
   Users - Read
   System - Full Control

C:\%SystemRoot%\System32\Dhcp
   Administrators- Full Control
   Creator/Owner - Full Control
   Power Users - Read
   Users - Read
   System - Full Control
```

et de manière générale

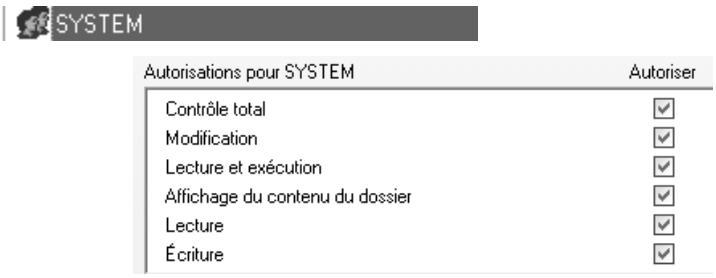
```
Any other folders
   Administrators- Full Control
   Creator/Owner - Full Control
   Power Users - Change
   Users - Read
   System - Full Control
```

Disque système XP :



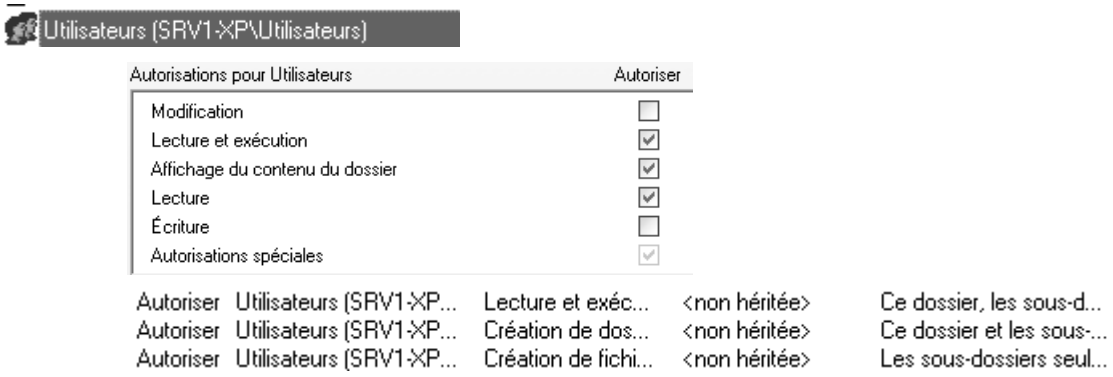
Dieu a tout pouvoir…

Si j'ai pu créer , j'ai tout pouvoir dans les sous-dossier et fichiers



Windows a tout pouvoir…

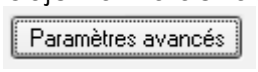
Tout le monde (authentifié) peut lire la racine du disque …



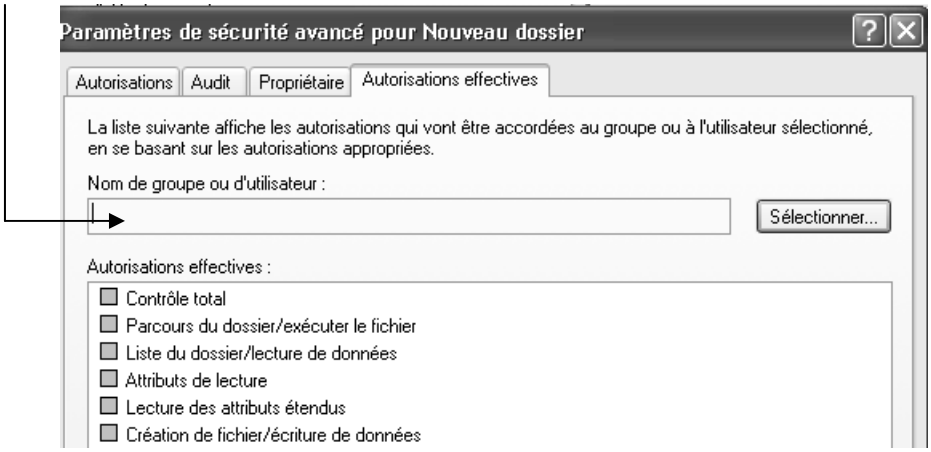
Les utilisateur (de ce poste) peuvent tout lire, créer un dossier et des sous dossier, et des fichier dans les dossiers et sous dossier, mais pas à la racine du disque.

VOIR LES AUTORISATIONS NTFS

Autorisations effectives :

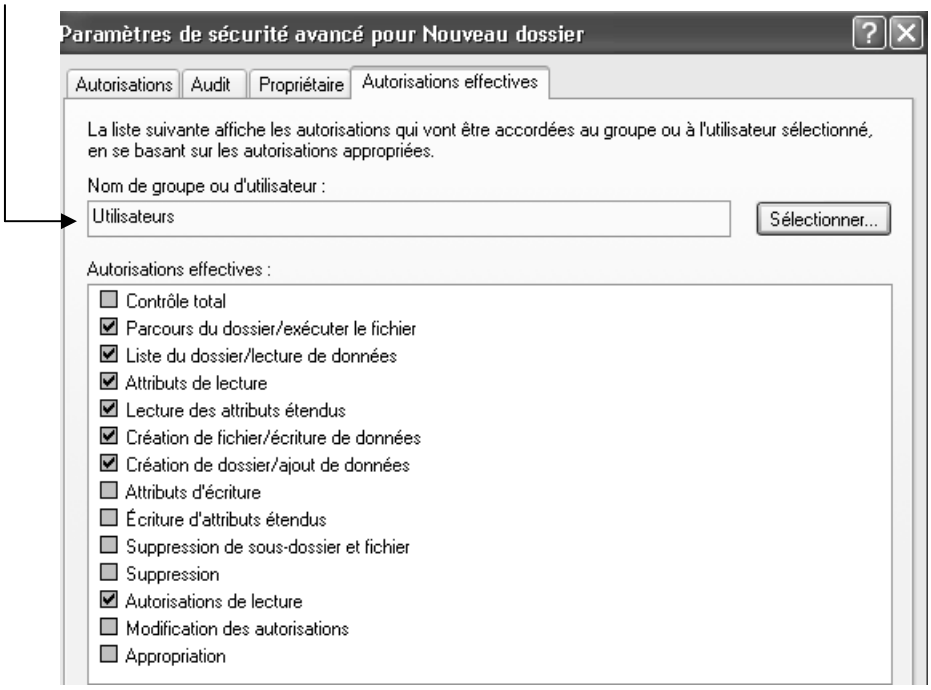
On peut connaître les autorisations qu'un utilisateur ou un groupe possède sur un objet à l'aide des autorisations effectives. On demande pour un dossier 

Et dans l'onglet **Autorisations effectives** on peut alors donner un nom

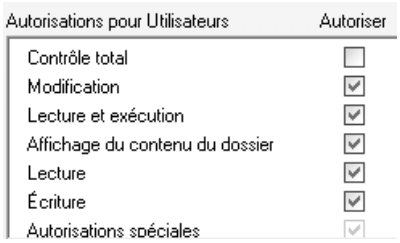


Pour obtenir par exemple

Pour le groupe **utilisateur**



Qui avait ces droits de donnés :

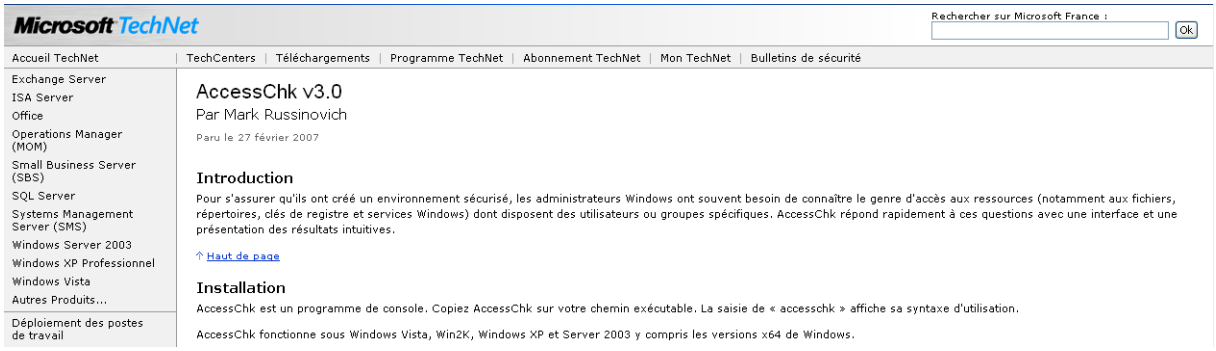


Le calcul ne tient pas compte des identificateurs de sécurité suivants :

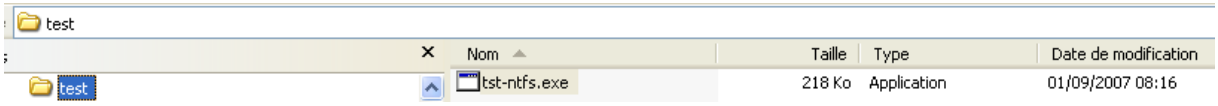
- Ouverture de session anonyme
- Utilisateurs authentifiés
- Créateur propriétaire.

Dans Windows XP Professionnel, le groupe Tout le monde ne contient plus le groupe Ouverture de session anonyme.

Utilitaire Accesschk

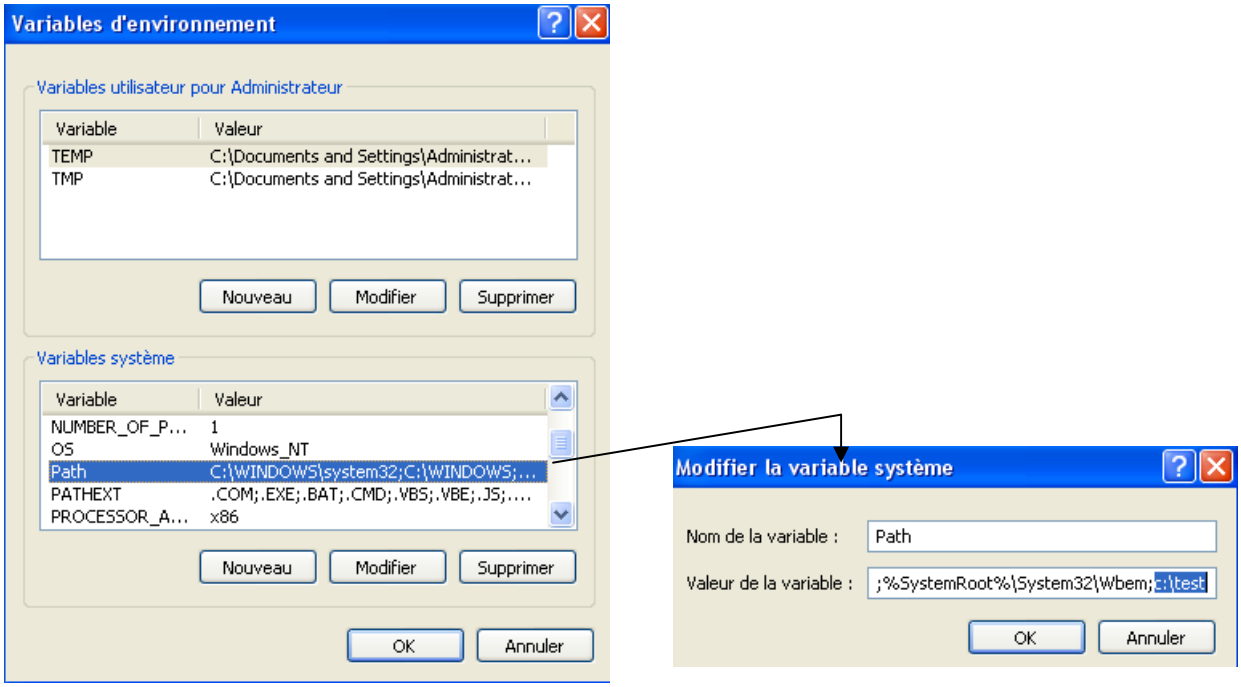


L'utilitaire téléchargé est petit



On peut renommer le fichier, et intégrer sont chemin dans le système

dans les propriétés système/ onglet avancées



Si la syntaxe complète est lourde, la base est simple

Ici dans l'exemple l'utilitaire à été renommer en **tst-ntfs.exe**, et donc ici en

tst-ntfs xxxnomutilisateurxxx xxxchemin-dossier-fichierxxxx

```
C:\test>tst-ntfs toto c:\*.*

AccessChk v4.02 - Check access of files, keys, objects, processes or services
Copyright (C) 2006-2007 Mark Russinovich
Sysinternals - www.sysinternals.com

RW c:\$oem$
R  c:\AUTOEXEC.BAT
   c:\boot.ini
R  c:\Bootfont.bin
R  c:\CONFIG.SYS
RW c:\data
RW c:\deuxieme site
R  c:\Documents and Settings
RW c:\drivers2k
RW c:\driversxp
R  c:\IO.SYS
R  c:\MSDOS.SYS
   c:\MSOCache
RW c:\Nouveau dossier
   c:\NTDETECT.COM
```

Les options intéressantes (et cumulables) :

- n

pas d'accès

- r

accès en lecture

-w

accès en ecriture

-d

uniquement les dossiers

TP DROITS NTFS 1°

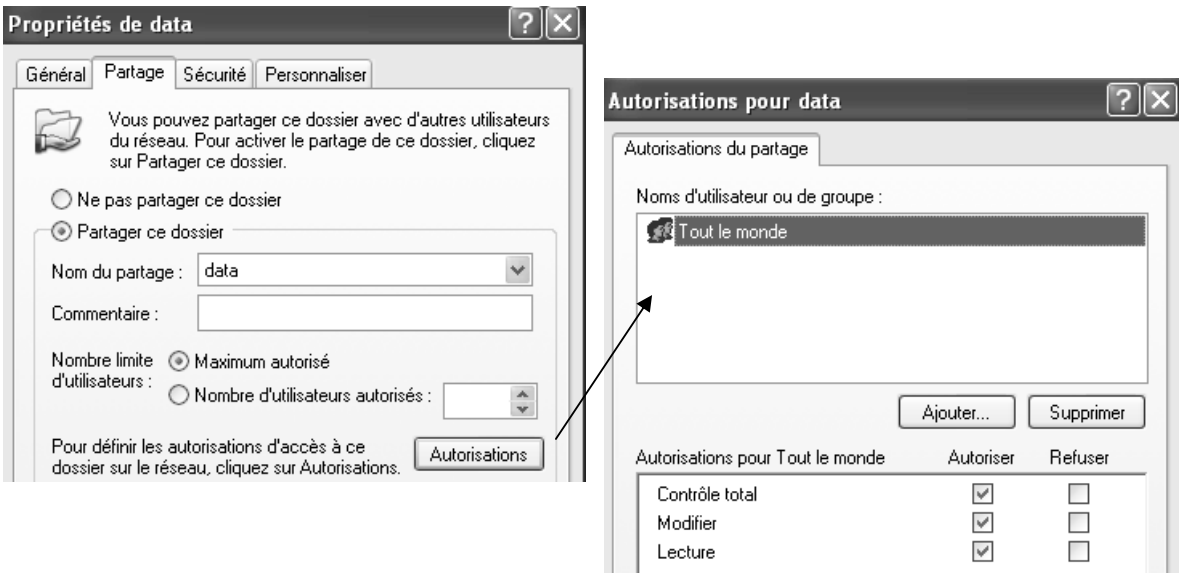
Objectif :

Faire que chaque utilisateur , andre, bertrand...puisse "tout faire chez lui", sauf détruire son répertorie de base(ici homonyme) !

Le disque sur lequel on travaille à des permissions NTFS par défaut,

Permissions de partage :

On pourrait commencer par **partager** le dossier **data** (en contrôle total pour tout le monde)



Ainsi les accès depuis le réseau sont possible. (cela n'est pas obligatoire !)

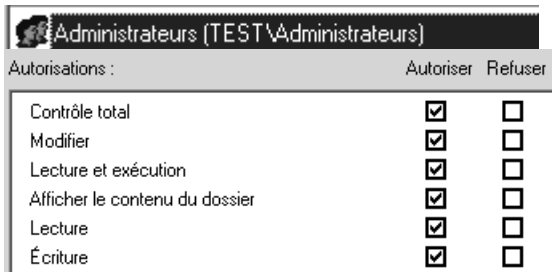
Permissions de sécurité :

On va donc retirer l'héritage, (en demandant **de supprimer les permissions**)

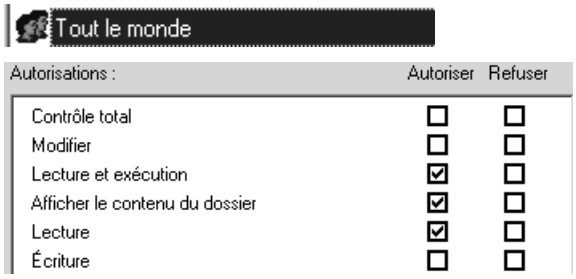
Ensuite on pose

- le groupe **tout le monde** en **Lecture et éxecution** - **Afficher le contenu** - **Lecture** (c'est le mode par défaut lorsque l'on ajoute une permission)
- le compte **Administrateur** en **Contôle total**

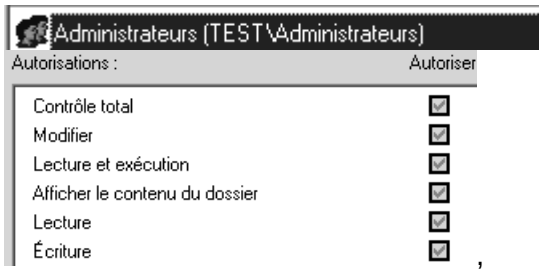
on a donc



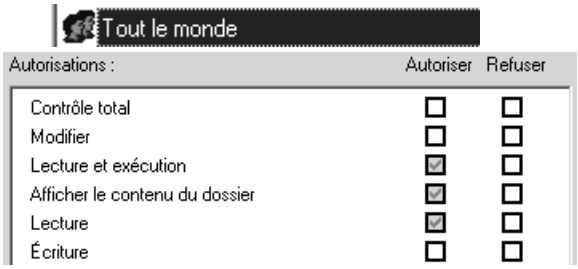
et



sur le dossier de **andre**, et **bertrand** donc, par défaut les permissions de sécurités sont celles **heritées** du dossier **data** et on aura donc



,

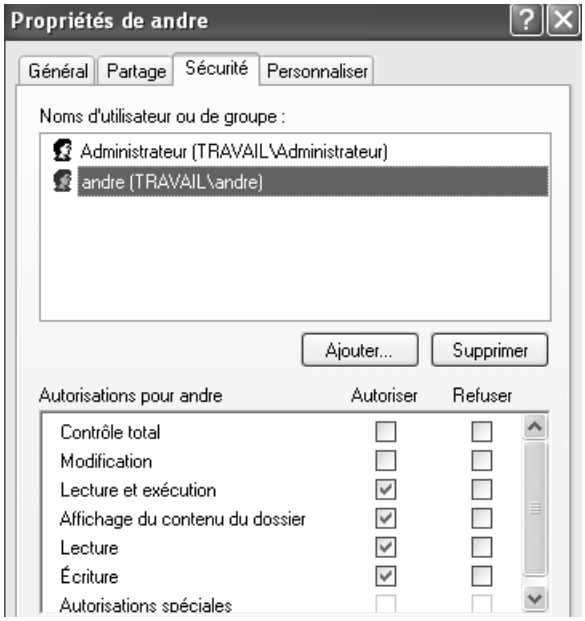


à l'heure actuelle les dossiers **andre** et **bertrand** sont en lecture seule pour tout le monde... Il faut maintenant autoriser andré a pouvoir aller que chez lui, et exclure tout le monde (et idem pour bertrand...)

donc pour le dossier **andre**, après avoir refusé l'héritage il faut avoir au final

l'utilisateur **andré** en (**Lecture et exécution** - **Afficher le contenu** - **Lecture**) plus **Ecriture**

L'**administrateur** en **contrôle total**



N.B : bien faire attention aux permissions effectives, qui peuvent varier selon ce que sous 2000 NT4 ou XP on copie ou supprime les permissions lors de la rupture de l'heritage !

Donc désormais ici andré peut travailler chez lui, et pas chez bertrand. Ça c'est bien

Mais si andré peut créer un dossier (ou un fichier chez lui), il ne peut pas supprimer ce dossier (fichiers), ni même le renommer un fichier de son propre dossier, voire modifier son contenu. Il ne peut que créer... cela c'est embêtant...

Pour l'instant c'est normal car il n'a pas les droits de suppression – modification

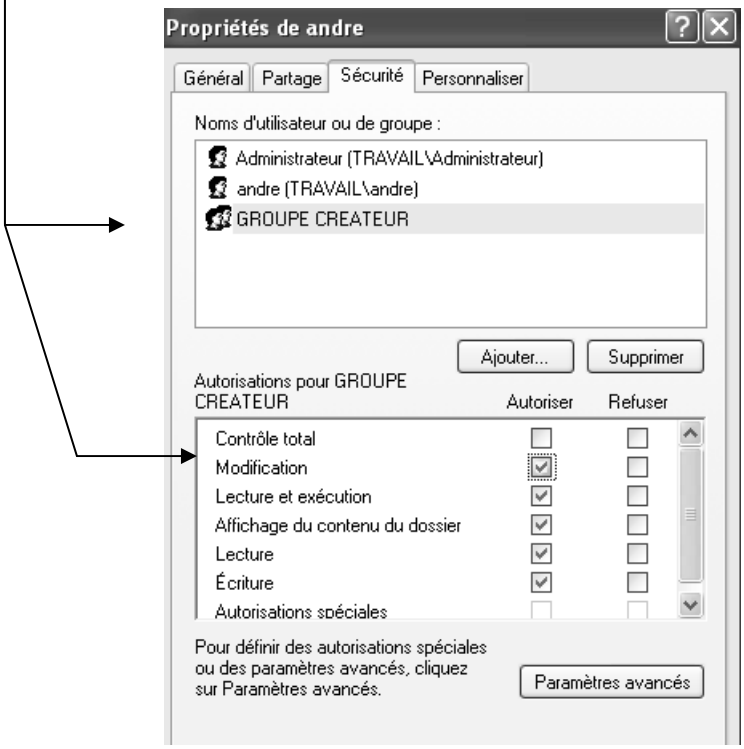
---

Notion de Créateur Propriétaire :

Si on donne le droit à andré de modifier chez lui, il pourra aussi supprimer son propre dossier…. Et cela aussi c'est embêtant...

la notion de **Créateur propriétaire** devrait résoudre le ce problème

en effet lorsque andré crée un dossier ou un fichier, il en est le propriétaire, et si on donne au **groupe créateur** le droit de **modifier** leurs documents, alors le tour est joué (chacun à droit de vie ou de mort uniquement sur ce qu'il a personnellement crée !)



N.B: Maintenant, si andré essaye de supprimer son propre dossier de base, ils ne peut pas car ils n'en est pas propriétaire (c'est l'administrateur qui l'a crée). il peut éventuellement le vider de tout le contenu dont il est le propriétaire...

N.B: Maintenant, si l'administrateur pose un fichier dans le dossier de André ou Bertrand, celui-ci pourra le lire, mais pas le modifier ou le supprimer (mais il pourra faire un enregistrer sous…)

TP DROITS NTFS 2°

Objectif :

Soit un groupe d'utilisateurs répartis en 2 catégories, des **commerciaux**, et des **secrétaires**...

Chaque **commercial** peut avoir globalement accès a :

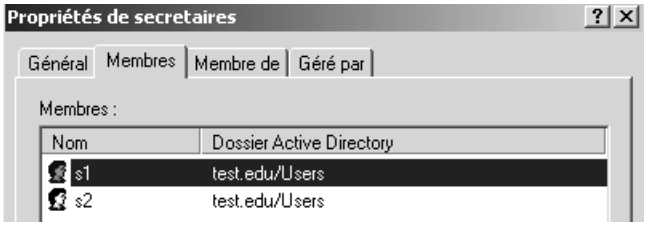
- son dossier, (de manière complète)
- aux dossiers des collègues (en lecture seule)
- au dossier commun des commerciaux (de manière complète)
- mais n'a pas accès aux dossier des secrétaires....

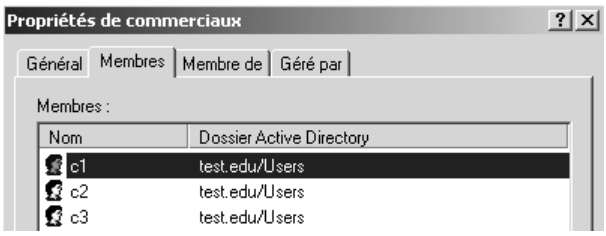
De manière analogue, les **secrétaires** peuvent avoir accès a :

- leur dossier, (de manière complète)
- aux dossiers des collègues (en lecture seule)
- au dossier commun des secrétaires (de manière complète)
- mais n'a pas accès aux dossier des commerciaux....

Groupes et comptes :

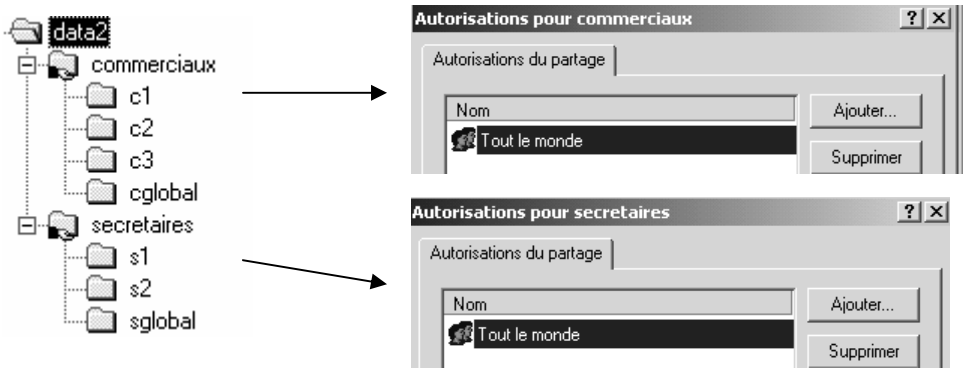
il faut créer un groupe global des secrétaires et y rentrer les utilisateurs appropriés (s1,s2...)., et un groupe global des commerciaux, et y rentrer les utilisateurs appropriés (c1, c2...).





Partages :

Puis il faut **partager** (**accès réseau**) le dossier **commerciaux** en **contrôle total - tout le monde** et **partager** (**accès réseau**)le dossier **secrétaire** en **contrôle total - tout le monde**,

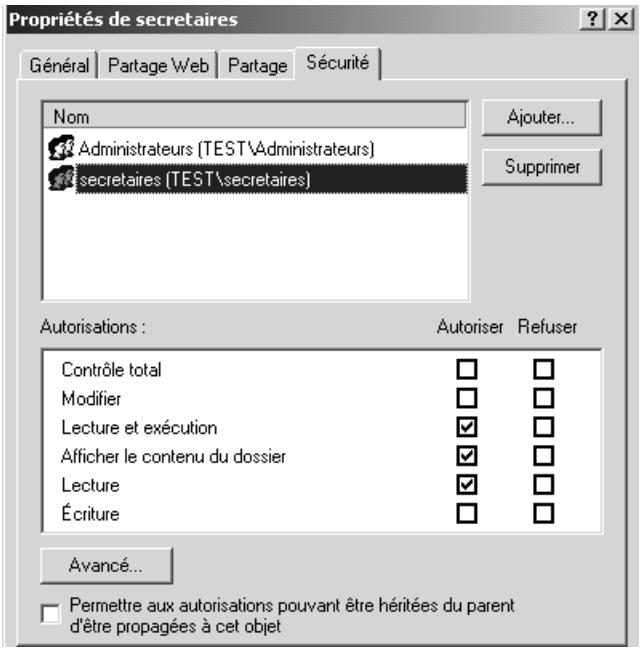


N.B: on pourrait décider de ne faire qu'un seul partage

Permissions NTFS :

sur le dossier général des secrétaires **secretaires**; il faut bloquer l'héritage, (en supprimant les permissions)

puis donner au **Administrateur** une permission **contrôle total**, et au groupe des **secretaires** une permission **Lecture exécution - affichage - Lecture**



(et respectivement le groupe des commerciaux dans le dossier commerciaux...)

maintenant, les commerciaux peuvent aller chez eux, les secrétaires chez elles, mais uniquement en lecture seule...

N.B: si on veut que les secrétaires puissent ajouter des choses chez elles à ce niveau de la structure, il faut ajouter la permissions écriture...., a ce stade, ce n'est pas forcement souhaitable

Pour l'instant tous les "droits pratiques", pour lire un document dans n'importe quel dossier…, mais pas pour le créer, et encore moins le modifier / supprimer !

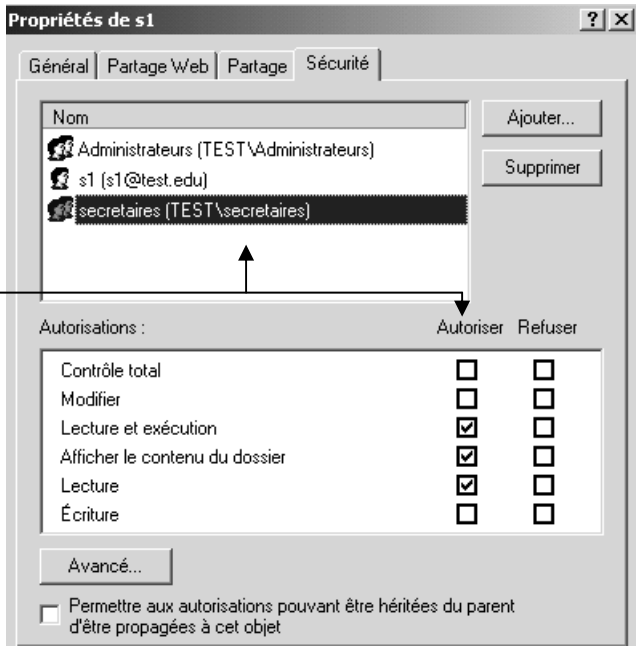
Pur chaque dossier individuel, **S1 S2** etc il faut autoriser l'utilisateur **S1** à **créer** chez lui, (mais pas **modifier**, sinon il pourrait supprimer son propre dossier) et les **administrateurs** en **contrôle total**

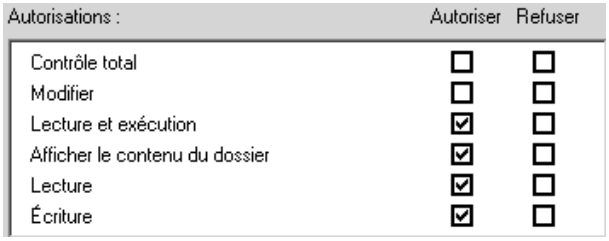
Donc on **supprime l'héritage**, (en supprimant les droits)

puis on ajoute le groupe des **Administrateurs** en **Contrôle total**,

le groupe **secretaires** en **Lecture-Afficher-Lecture** seulement

et enfin l'utilisateur **S1** en permission **Lecture-Afficher - lecture** plus **écriture**





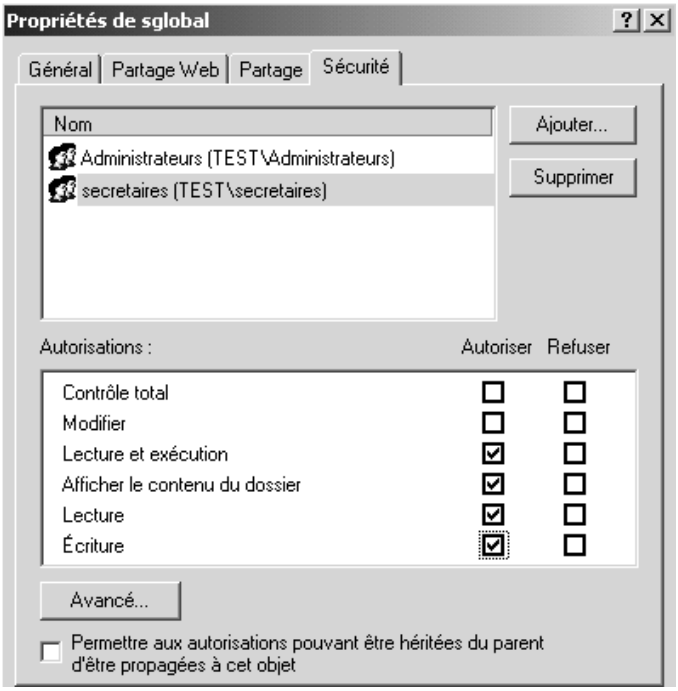
Pour le dossier **sglobal** il faut autoriser chaque secrétaire à pouvoir y écrire, ainsi que l'administrateur

on supprime l'héritage

on ajoute le groupe Administrateur en **Contrôle Total**

et le groupe **secretaires**

en **lecture-Afficher-Lecture** et aussi **écriture**



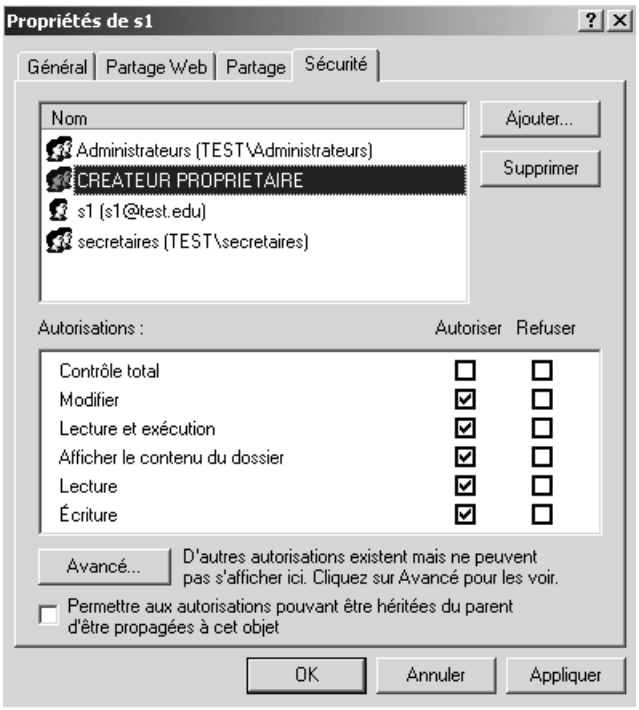
Créateur propriétaire :

Maintenant, les secrétaires peuvent aller chez elles, **S1** peut créer chez elle, et dans **sglobal**, et ne peut que lire chez **s2**. de même **S2** peut créer chez elle et dans **sgloba**l, mais ne peut que lire chez **s1**

mais ni **S1** ni **S2** ne peuvent renommer ou supprimer quelque chose qu'elle aurait crée !

ce qui s'arrange avec la notion de créateur propriétaire...

que l'on ajoute en modifier pour les dossier **S1**, **S2** et **sglobal**



N.B: dans un tel schéma, si l'administrateur pose un fichier dans le dossier d'une secrétaire, celle-ci pourra le lire, mais pas le modifier ou le supprimer (mais elle pourra faire un enregistrer sous…)
Même raisonnement lorsque une secrétaire crée ou dépose un document dans l'espace commun, ses copines peuvent s'en servir mais pas le modifier ou le supprimer…(mais elle pourront faire un enregistrer sous…)

N.B: Maintenant, si s1 essaye de supprimer son propre dossier, elle ne peut pas car elle n'en est pas propriétaire (c'est l'administrateur qui l'a crée) mais elle le videra de tout le contenu dont elle est le propriétaire...

TP APPROPRIATION DE FICHIER

Descriptif du problème :

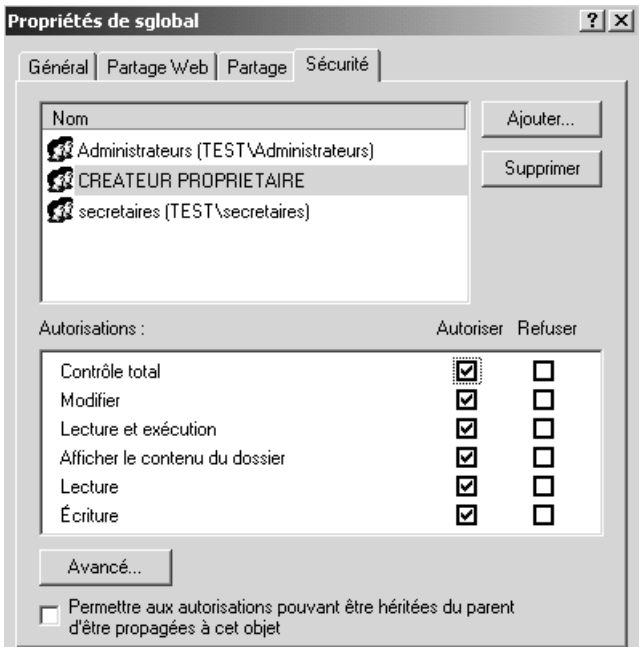
Imaginons un ensemble de secrétaires ayant chacune un espace propre réservé nommé **s1**, **s2** etc et disposant d'un espace commun à toutes nommé **sglobal** (pour secrétaire global)

les permissions du dossier **sglobal** sont les suivantes :

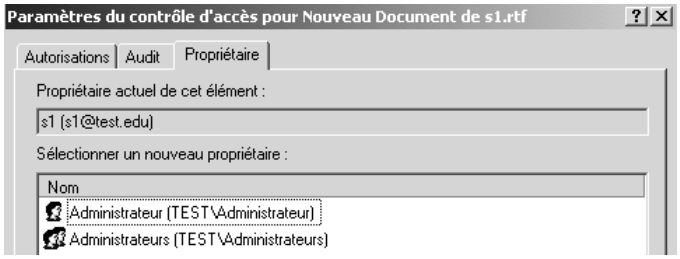
Administrateur en **Contrôle total**

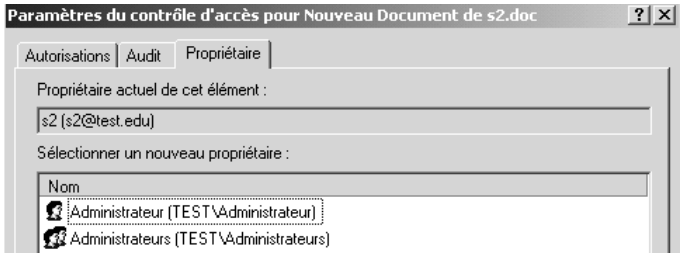
Créateur propriétaire en **contrôle total**

Le groupe **secrétaire** en **Lecture-Affichage-Lecture** et **écriture**



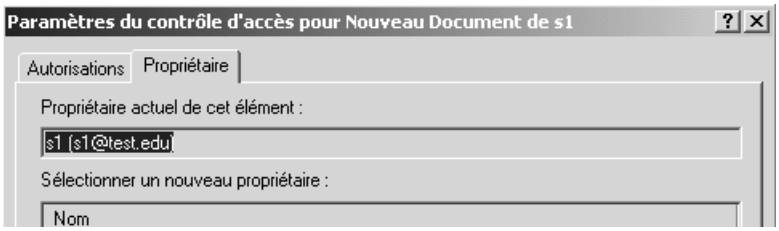
on peut donc arriver à ce que dans ce dossier, il y ait des documents de divers propriétaires...





s2 peut lire un document fait par **s1**, mais si **s2** essaye de modifier le nom du document ou de le supprimer, alors il y a refus ce qui est normal car seul le "créateur propriétaire" à ces droits...

si **s2** insiste sur vouloir modifier un document appartenant à **s1**, en tentant de se l'approprier, il essuie un refus (seul l'administrateur peut toujours s'approprier un document), et il ne peut bien sur pas changer les permissions!



Comment aider **S2** à modifier le document créer par **S1** ?

Raisonnement :

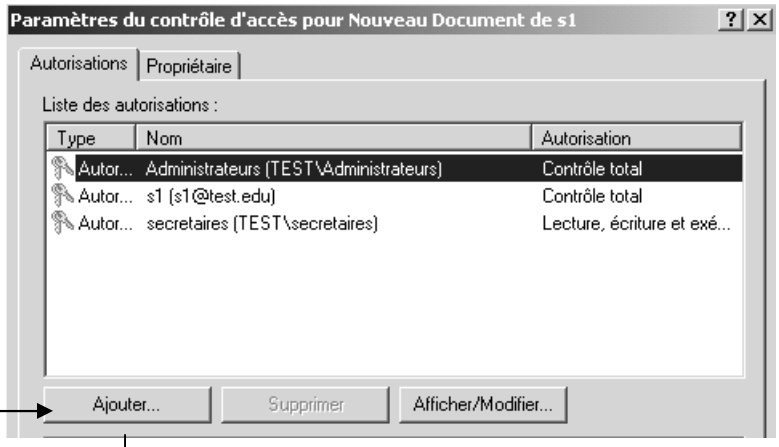
Pour que **s2** puisse s'approprier le document...(depuis un poste NT...) **s1** doit donner à **s2** la permission voulue, voire la permission de prendre possession de ce fichier...:

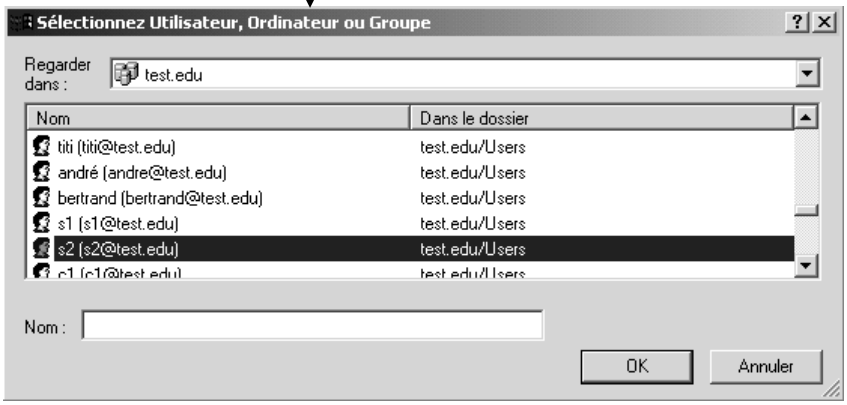
N.B: il ne peut le faire que s'il a un contrôle total sur ce fichier (la différence entre contrôle total et modifier c'est que modifier ne permet pas de changer les permissions, et donc d'ajouter ou d'enlever des droits à des utilisateurs...)

s1 modifie les permissions du fichiers pour lequel il souhaite laisser une prise de possession,

dans **permissions - securité - avancées** -

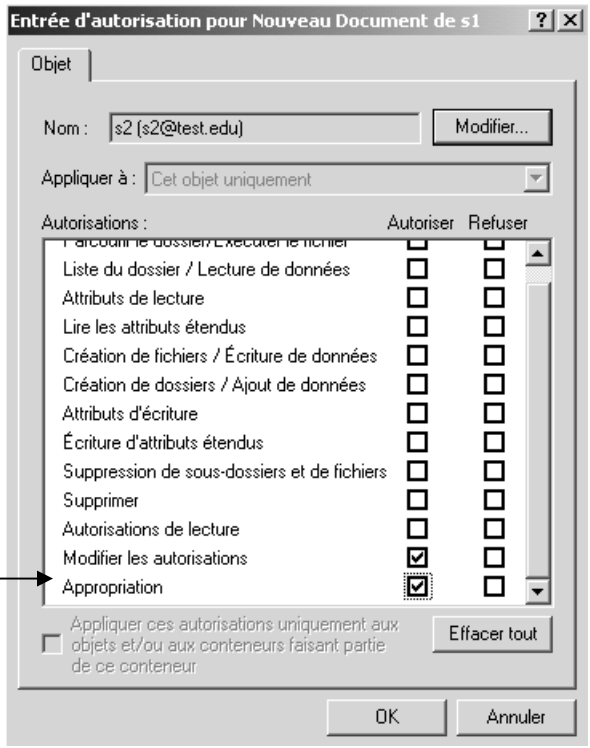
on demande **Ajouter**



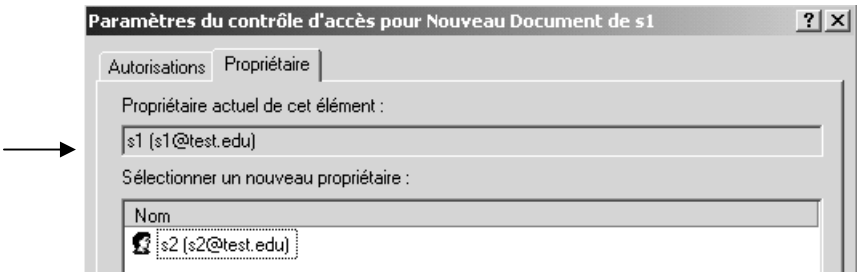


sélectionner **s2** puis valider

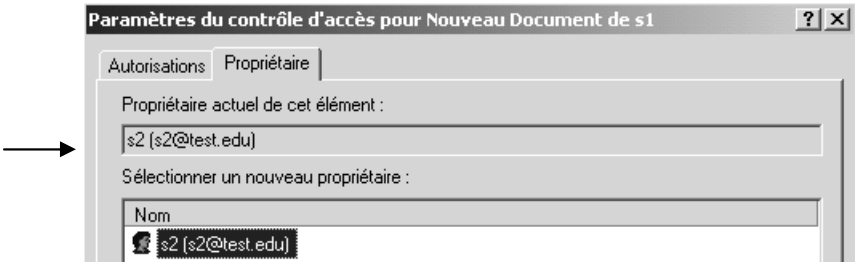
NB: il faut ici cocher au minimum **modifier** et **appropriation**, . .



Désormais **s2** lors de sa session peut s'approprier ce document…



pour obtenir



en résumé :

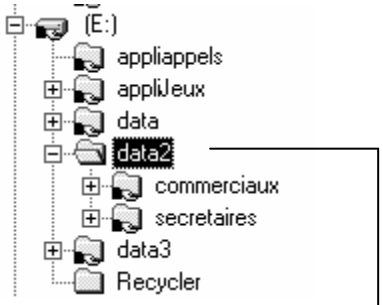
- Si ici on donne au groupe **Créateur propriétaire** le droit **contrôle total** (ici c'est le cas), **s2** pourrait modifier un document créé par **s1** à condition que **S1** ait au préalable modifié les permissions sur son fichier pour y inclure **s2**...
- Si ici on donne au groupe **Créateur propriétaire** le droit **modifier**, au lieu de **contrôle total**, alors **s2** ne pourra jamais modifier un document créé par **s1**
- L'**administrateur** peut lui toujours s'approprier le fichier pour en faire ce qu'il veut…

TP COPIE FICHIER - PERMISSIONS

Objectif :

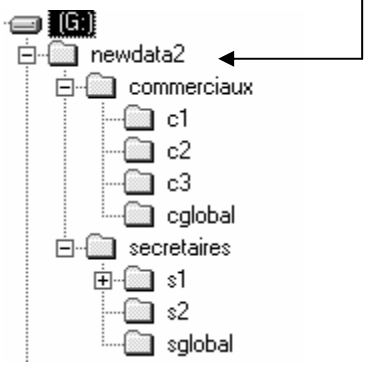
Lorsque l'on copie des fichiers, sur un volume NTFS, on sait que les permissions obtenues sur les fichiers "copiés" sont celles "héritées" des dossiers de destination…

Soit ainsi l'arborescence **data2** donnée suivante située sur le disque E: avec un certain nombre de permissions NTFS posées, et que l'on souhaiterais transférer pour des raison de maintenance sur un disque G: (G:) …



Si on copie cette structure classiquement on obtiendra bien

Mais toutes les permissions NTFS ont été héritées du dossier de destination, à savoir newdata2, c'est à dire **Contrôle total** pour **tout le monde** !



commande xcopy :

Il existe une comande en ligne, nommée **xcopy.exe** permettant de copier les fichiers avec leurs permissions de sécurité. La mise en œuvre pourrait être

D: \>xcopy e:\data2 g:\newdata2 /o /a

N.B: si le nouveau disque G: doit remplacer l'ancien D:, on

- arrête le service server,
- on renomme les lecteurs,
- et on re-démarre le service server…
- Il ne reste plus que les partages à refaire !

Copie de partage ? :

La copie de partage elle aussi devient tentante, mais il faut savoir qu'elle est plus risquée, non supportée "officiellement", et remplace tous les partages d'une machine par ceux "récupérés" depuis la machine d'origine, on ne peut donc pas récupérer que les partages de telle ou telle lecteur ou branche d'arborescence !

Une fois l'arborescence copiée avec **xcopy**, on

1. enregistre les partages à recopier, (sur la machine dont on veut copier les partages…) en lançant regedit32, Se placer sur la clé
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Shares
   Et sauvegarder sur disquette depuis le menu de l'éditeur de registre
2. copie ce fichier sur la machine de destination
3. sur la machine de destination, en lançant regedit32, Se placer sur la clé
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Shares
   Et restaurer depuis la disquette depuis le menu de l'éditeur de registre
4. répondre OK

NB: tous les partages de la machine de destination sont remplacés par les partages existant sur la machine d'origine !

NB: Dans la ces ou des autorisations de partages auraient été données, on peut essayer de les retrouver avec la clé du dessous **\Security**