



<http://WWW.CABARE.NET> ©

# **SEVEN- Système Fichier NTFS – sys 20 - sys 22– cours & tp-**

**Système de Fichier NTFS Windows Seven**

**Michel Cabaré – Ver 2.0 – mars 2010-**

**SEVEN Système Fichiers NTFS  
Cours - TP**

**Michel Cabaré – Ver 2.0 – mars 2010**

[www.cabare.net](http://www.cabare.net) ©

# TABLE DES MATIÈRES

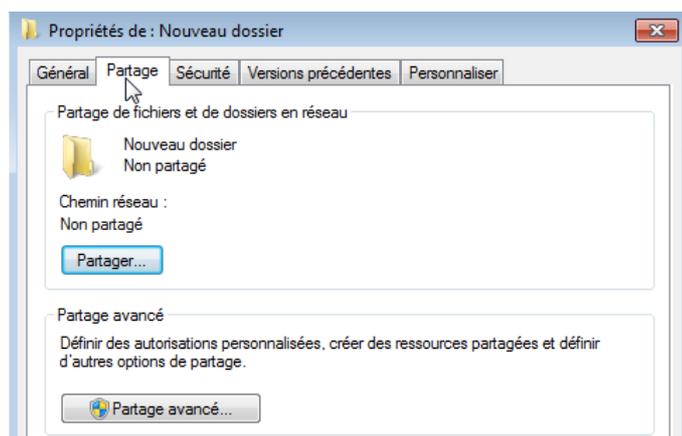
<b>ACCES AUX PERMISSIONS NTFS</b> .....	<b>4</b>
PARTAGE ET SECURITE : .....	4
<b>SECURITE NTFS</b> .....	<b>5</b>
ACL ET ACE : .....	5
PERMISSIONS SUR DOSSIERS - FICHIERS: .....	5
PERMISSIONS STANDARD ET SPECIALES : .....	6
COMBINAISON FICHIER – DOSSIER EN NTFS:.....	8
<i>Exemple 1 : (fichier contre dossier)</i> .....	8
<i>Exemple 2 : (combinaison sur dossier)</i> .....	8
<i>Exemple 3 : (combinaison dossier - fichier)</i> .....	8
PERMISSION NTFS ET D’AUTORISATIONS DE PARTAGE (RESEAU): .....	9
<i>Exemple 1 :</i> .....	9
<i>Exemple 2 :</i> .....	9
<b>HERITAGE NTFS</b> .....	<b>10</b>
NOTION D’HERITAGE .....	10
CASSER UN HERITAGE.....	11
RECREER UN HERITAGE .....	13
RECREER UN OU PLUSIEURS HERITAGES.....	14
<b>PROPRIETE NTFS</b> .....	<b>16</b>
NOTION DE PROPRIETE .....	16
PRENDRE POSSESSION DES DOSSIERS ET FICHIERS .....	17
DONNER LA POSSESSION DES DOSSIERS ET FICHIERS .....	18
REGLES "D’AFFECTATION" DES PERMISSIONS NTFS: .....	19
<b>VOIR LES AUTORISATIONS EFFECTIVES</b> .....	<b>20</b>
AUTORISATIONS EFFECTIVES : .....	20
UTILITAIRE ACCESSCHK.....	21
<b>COPIER-DEPLACER EN NTFS</b> .....	<b>24</b>
CREER – COPIER- - DEPLACER.....	24
SENSIBILISATION AUX FINESSES DE L’INTERFACE.....	24
XCOPY .....	25
SAUVEGARDE DE FICHIERS.....	26
ROBOCOPY INVITE DE COMMANDE .....	28
<b>LIENS SYMBOLIQUES</b> .....	<b>29</b>
LIENS SYMBOLIQUES - RACCOURCIS: .....	29
LIENS SYMBOLIQUES – MKLINK : .....	29
COPIE DE LIENS SYMBOLIQUES:.....	31
JONCTIONS DE REPERTOIRE – JONCTION: .....	32
LIENS SYMBOLIQUES - REELS SUR FICHIERS : .....	33

<b>TP DROITS NTFS 1°</b> .....	<b>34</b>
OBJECTIF : .....	34
PERMISSIONS DE PARTAGE : .....	34
PERMISSIONS DE SECURITE : .....	34
NOTION DE CREATEUR PROPRIETAIRE : .....	36
<b>TP DROITS NTFS 2°</b> .....	<b>37</b>
OBJECTIF : .....	37
GROUPES ET COMPTES : .....	37
PARTAGES : .....	38
PERMISSIONS NTFS : .....	38
CREATEUR PROPRIETAIRE : .....	40
<b>TP APPROPRIATION DE FICHIER</b> .....	<b>41</b>
DESCRIPTIF DU PROBLEME : .....	41
RAISONNEMENT : .....	42
<b>RICHCOPY</b> .....	<b>44</b>
INSTALLER RICHCOPY 4.0 : .....	44
<b>TP COPIE FICHIER – PERMISSIONS (XP)</b> .....	<b>45</b>
OBJECTIF : .....	45
COMMANDE XCOPY : .....	45
COPIE DE PARTAGE ? : .....	46

# ACCES AUX PERMISSIONS NTFS

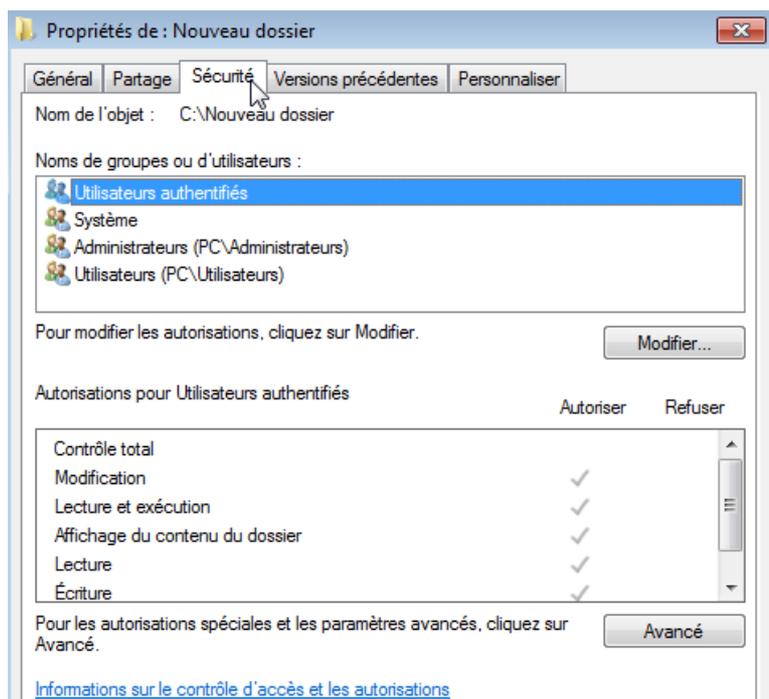
## Partage et Sécurité :

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



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

mais aussi à un onglet "**Sécurité**"



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

On pourrait continuer à travailler avec l'onglet Partage et demander Autorisation pour gérer les demandes d'accès depuis le réseau, mais comme 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 essentiellement au niveau de l'onglet Sécurité

# 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.

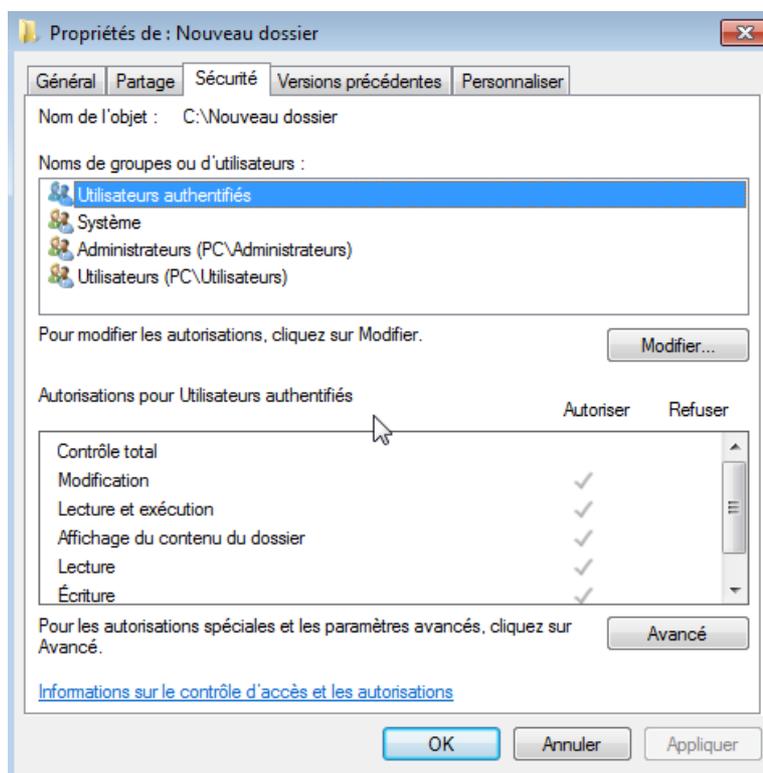
La liste ACL contient tous les groupes d'utilisateurs; tous les utilisateurs bénéficiant de l'accès au dossier ou au fichier, avec le type d'accès qui leur est accordé.

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 - Fichiers:

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

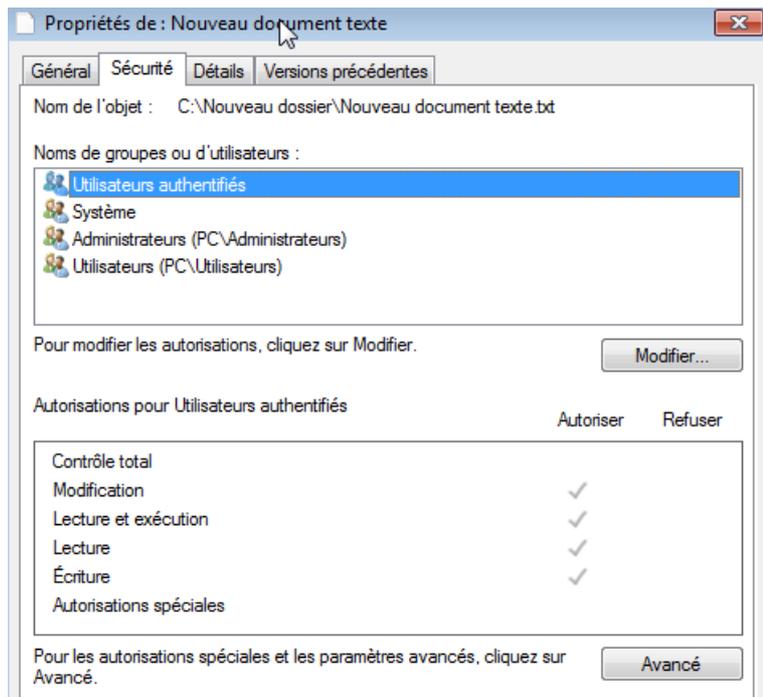


Ces 6 combinaisons standard, peuvent être **héritées** (dans ce cas elles sont grisées)

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

Sur un fichier il est possible en NTFS de définir 5 sortes principales de permissions (il manque afficher), 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 :

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:** 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 NIVEAU DES PERMISSIONS SPECIALES MAIS TOUJOURS AU NIVEAU DES PERMISSIONS STANDARDS...

Microsoft détaille les permissions spéciales ainsi:

<b>Parcourir le dossier / Exécuter le fichier</b>	<p><b>Pour les dossiers :</b> 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 <b>Outrepasser le contrôle de parcours</b> dans le composant logiciel enfichable Stratégie de groupe (par défaut, ce droit est octroyé au groupe Tout le monde).</p> <p><b>Pour les fichiers :</b> L'autorisation Exécuter le fichier permet ou interdit l'exécution de fichiers programmes (cette autorisation s'applique uniquement à des fichiers).</p> <p>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.</p>
<b>Liste du dossier / Lecture de données</b>	<p>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.</p> <p>L'autorisation Lecture de données permet ou interdit l'affichage des données des fichiers (cette autorisation s'applique uniquement aux fichiers).</p>
<b>Attributs de lecture</b>	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.
<b>Lire les attributs étendus</b>	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.
<b>Création de fichiers / Écriture de données</b>	<p>L'autorisation Création de fichiers permet ou interdit de créer des fichiers au sein du dossier (cette autorisation ne s'applique qu'aux dossiers).</p> <p>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).</p>
<b>Création de dossiers / Ajout de données</b>	<p>L'autorisation Création de dossiers permet ou interdit de créer des dossiers au sein du dossier (cette autorisation ne s'applique qu'aux dossiers).</p> <p>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).</p>
<b>Suppression de sous-dossiers et de fichiers</b>	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).
<b>Supprimer</b>	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.
<b>Autorisations de lecture</b>	Permet ou interdit les autorisations de lecture du fichier ou du dossier, telles que Contrôle total, Lecture et Écriture.
<b>Modifier les autorisations</b>	Permet ou interdit de modifier les autorisations du fichier ou du dossier, telles que Contrôle total, Lecture et Écriture.
<b>Appropriation</b>	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

<b>Attributs d'écriture</b>	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.
<b>Écriture d'attributs étendus</b>	<p>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.</p> <p>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</p>
<b>Synchroniser</b>	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 multitraitements.

---

## 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 **écrire** 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

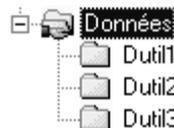
- Q:** Quelle est la permission effective de **Util1** lorsqu'il accède au fichier **A** à travers **une session locale** sur la machine ?
- R:** Depuis une session locale sur ordinateur1 la permission effective de **Util1** pour le fichier **A** est **contrôle total**

### Exemple 2 :

Un dossier **Données** est crée avec à l'intérieur 3 sous-dossiers nommés **Dutil1**, **Dutil2** 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**

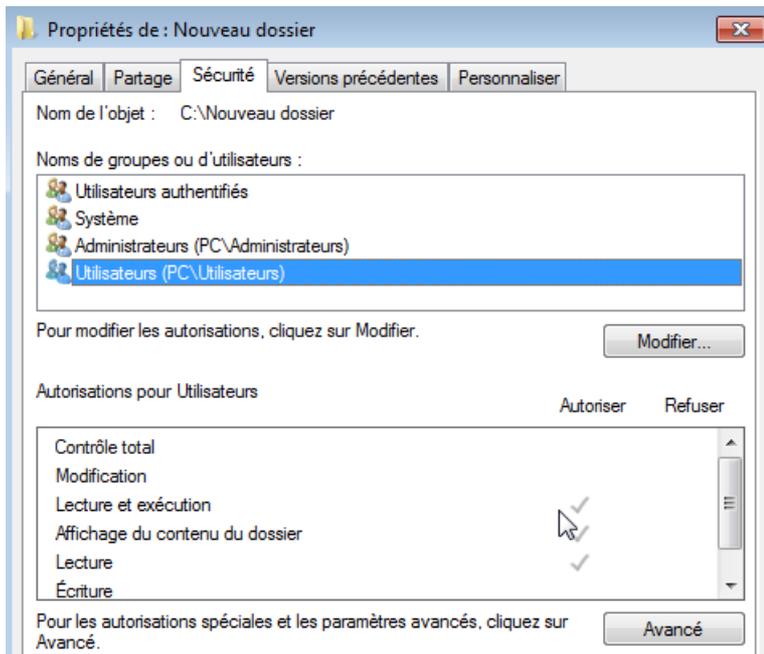
- Q :** Quelle est la permission effective de **Util1** lorsqu'il accède au dossier **Dutil1** à travers **l'accès réseau** au dossier partagé **Données** ?
- R :** **Util1** dispose de la permission **contrôle total** sur le dossier **Données** et son dossier **Dutil1**

- 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 **Util1**

# HERITAGE NTFS

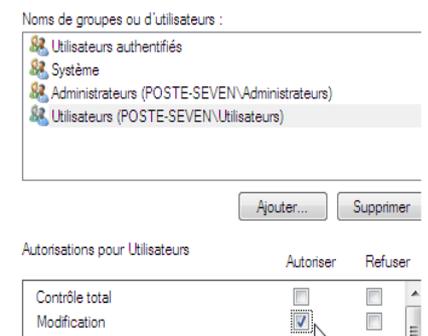
## Notion d'héritage

Donc lorsque l'on **crée** un dossier (ou respectivement un fichier) sur le disque dur, celui-ci **hérite** des droits du dossier à l'intérieur duquel il a été créé : la racine du disque ! Visuellement cela se traduit par le fait que les propriétés sont grisées, et semblent donc non modifiables.



Ici le groupe des **Utilisateurs** est en "**lecture seule**", par héritage...

On peut rajouter des permissions, via **Modifier...**



Si on modifie les permissions des parents, seuls sont concernés alors ensuite dans l'arborescence ceux qui ont accepté l'héritage.

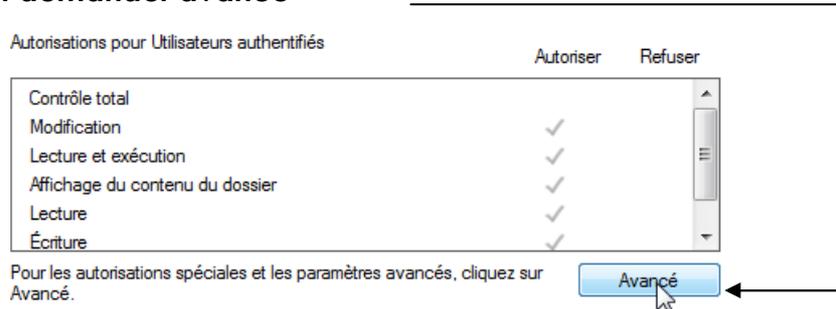
**NB :** Si les autorisations de l'objet ont été **héritées** de l'objet parent. Les modifications peuvent s'effectuer de trois manières :

- Exécutez les modifications sur l'objet parent ; l'objet héritera alors de ces autorisations.
- Sélectionnez l'autorisation opposée (**Autoriser** ou **Refuser**) pour contrer 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...

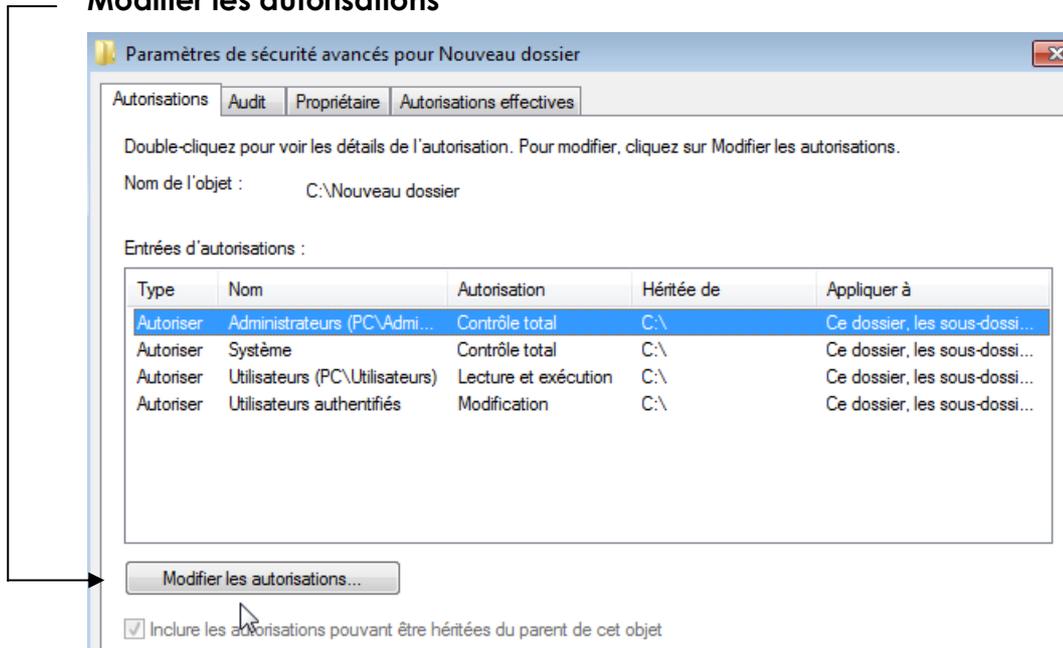
## Casser un héritage

**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... »**

**Il faut demander avancé**



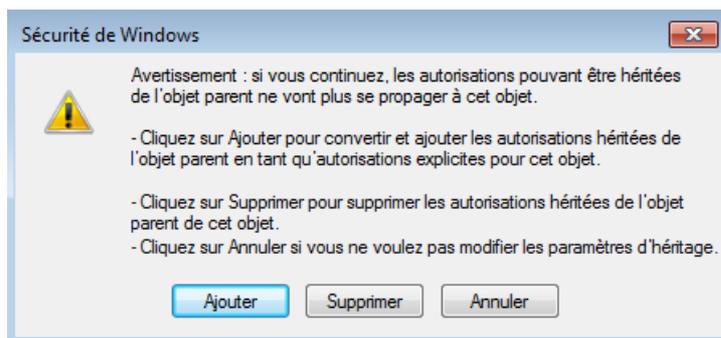
## Modifier les autorisations



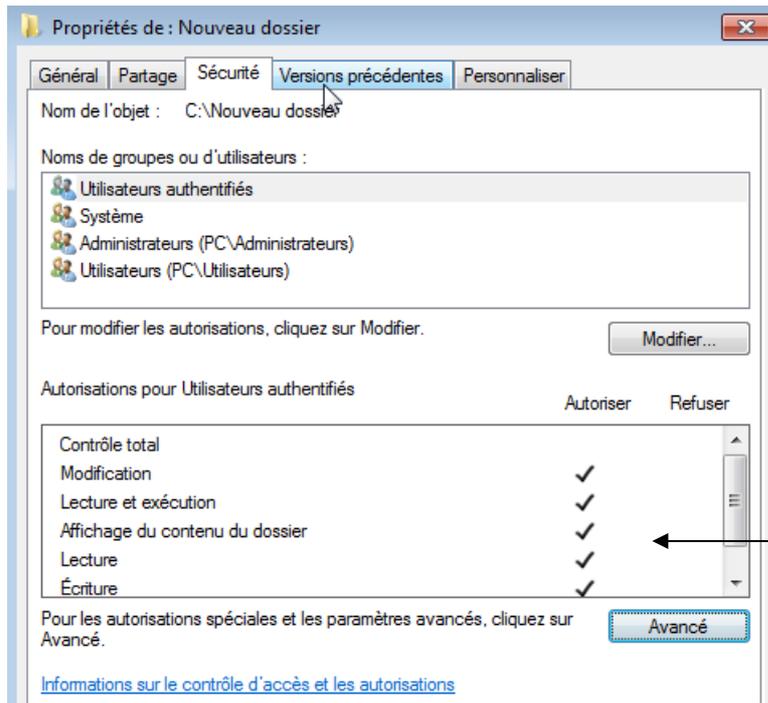
## Décocher



Dans ce cas, on peut choisir si on veut les **supprimer** complètement ou les **ajouter** à notre arborescence (et pouvoir ensuite les modifier...)



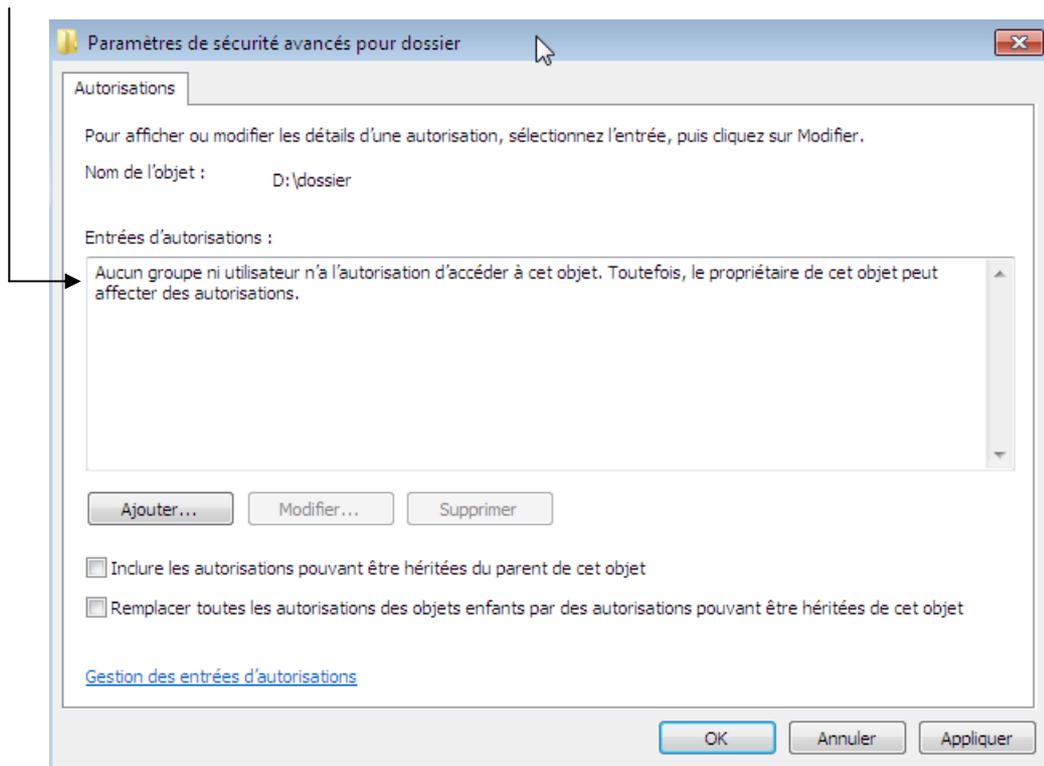
Si on demande **Ajouter** suivit de **Ok / Ok**



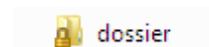
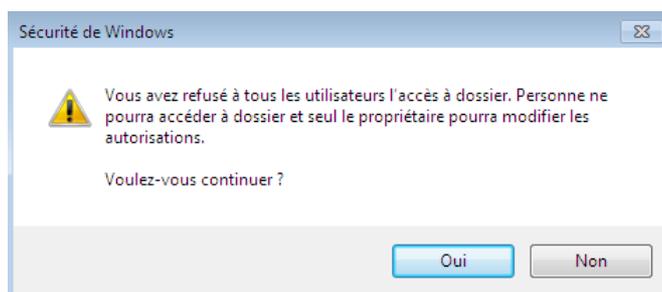
Ces 5 combinaisons standard, ne sont plus **héritées** (dans ce cas elles sont noires)

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

Si on demande **Supprimer** Seven nous informe...



Si on valide, une 2° mise en garde apparaît... mais bon...

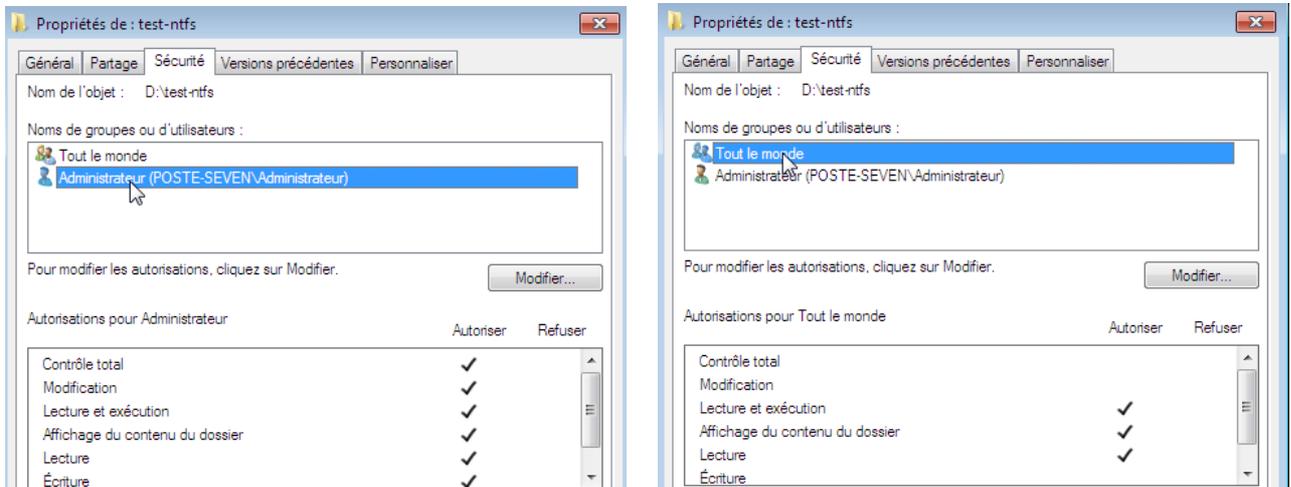


Seul le propriétaire pourra modifier ce dossier désormais...

## 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 :

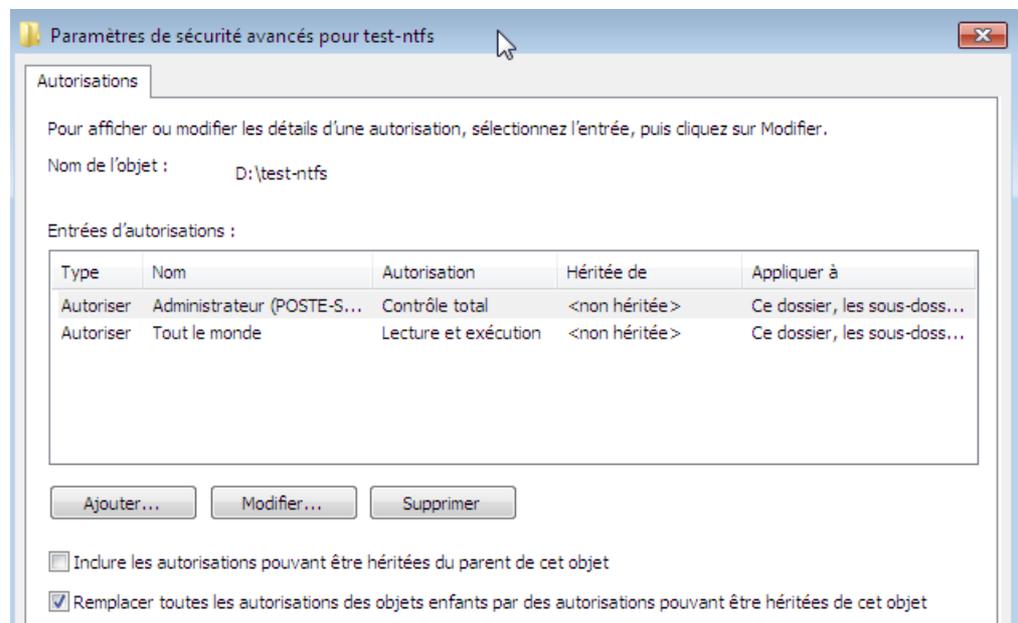
Compte Administrateur    Contrôle Total  
Groupe Tout le Monde    Lecture Seule



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

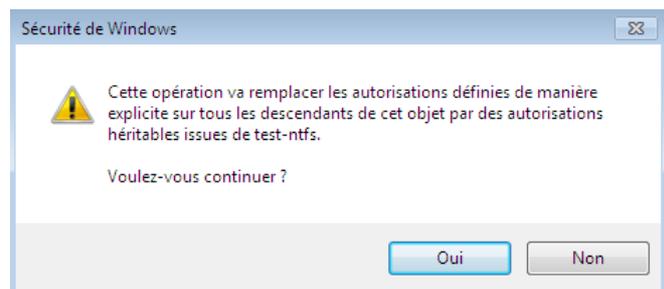


En se replaçant sur le dossier **test-ntfs** on reconstruit l'héritage d'origine en cochant **Hérite de l'objet parent...**



on confirme

Vérifier les nouvelles permissions héritées...



## Recréer un ou plusieurs héritages

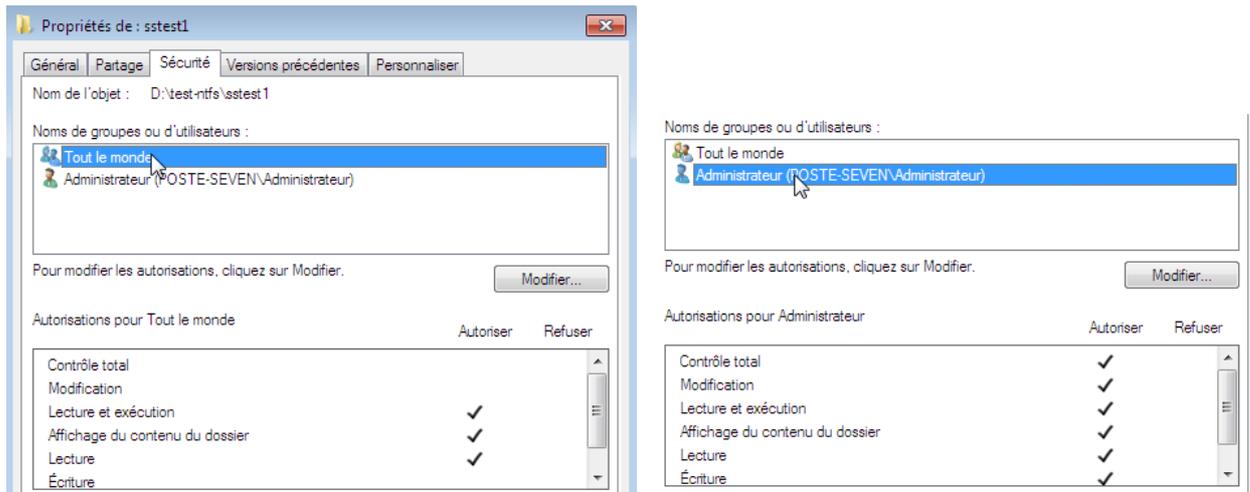
Soit un dossier **test-ntfs**, sur lequel, après avoir cassé l'héritage en supprimant toutes les permissions, on a posé la sécurité suivante :

Compte Administrateur    Contrôle Total  
Groupe Tout le Monde    Lecture Seule

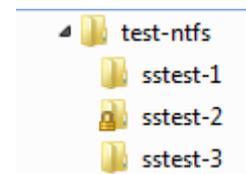
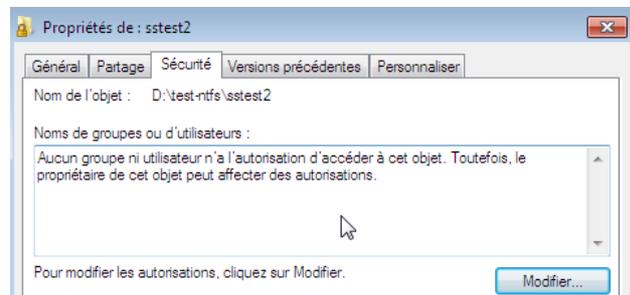


On construit trois sous-dossiers, respectivement **sstest1**, **sstest2**, **sstest3**, qui héritent donc a priori de la sécurité du dossier parent.

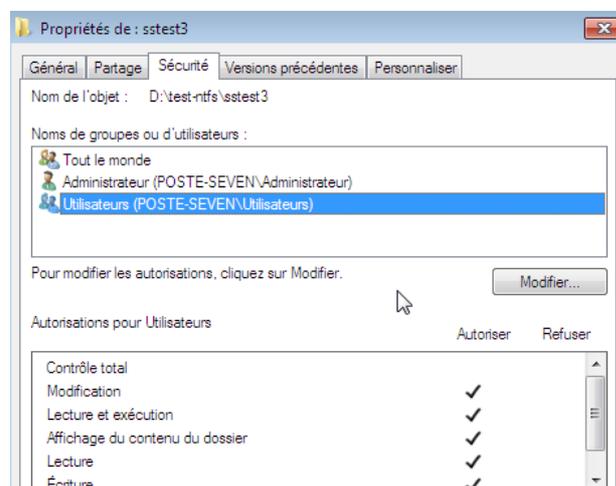
pour **sstest1** on, casse l'héritage en copiant les permissions...



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



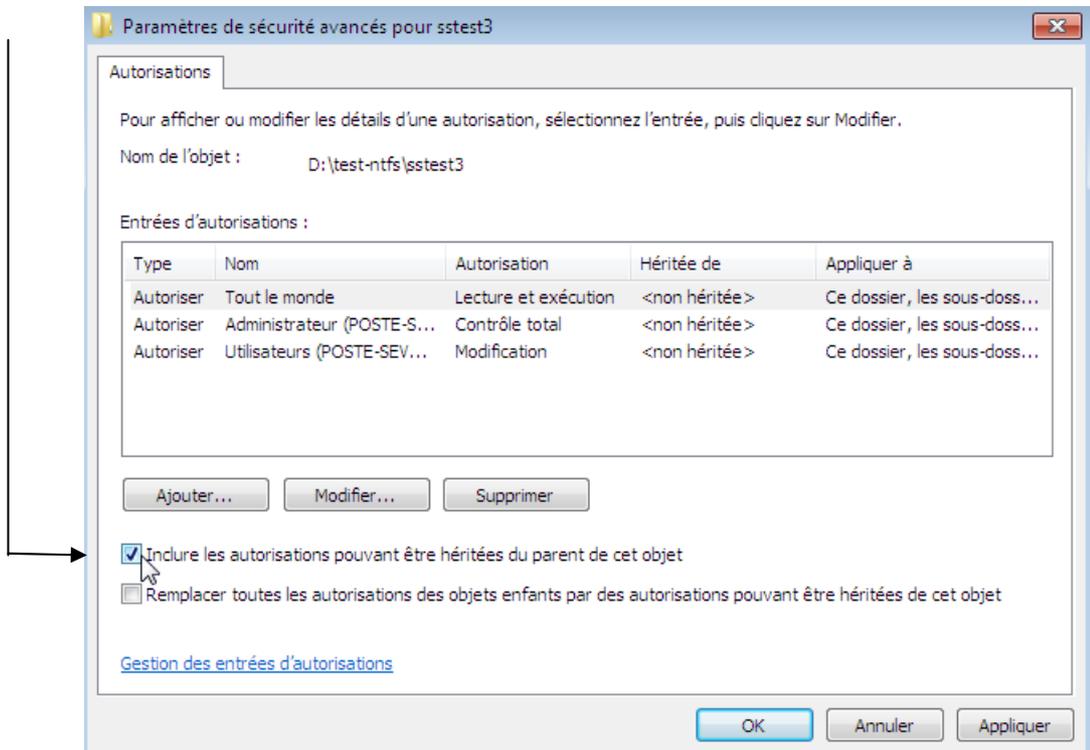
pour **sstest3** on, casse l'héritage en copiant les permissions et ajout du groupe des **Utilisateurs-** en Modifier...



On souhaite pour le dossier **sstest3** "retrouver" notre structure de départ.

Il faut depuis le dossier **sstest3**,

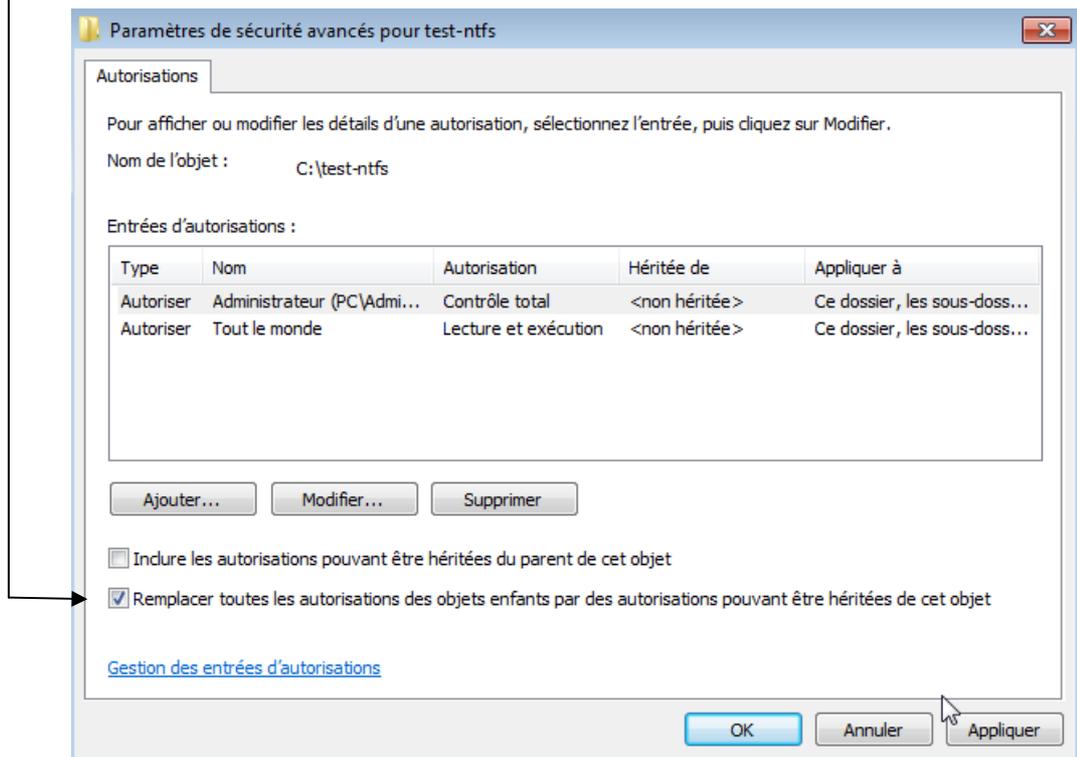
1. Demander d'effacer toute la sécurité
2. Demander la case à cocher **Inclure les autorisations pouvant être héritées du parent de cet objet**



On souhaite ensuite "retrouver" toute 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

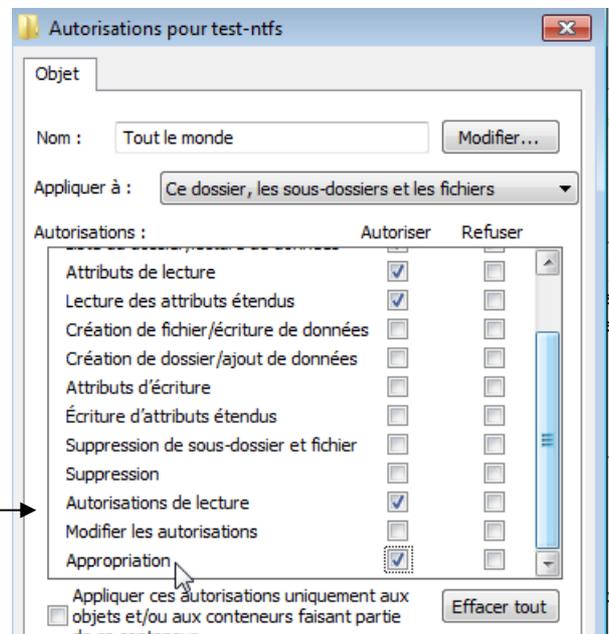
## Notion de Propriété

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

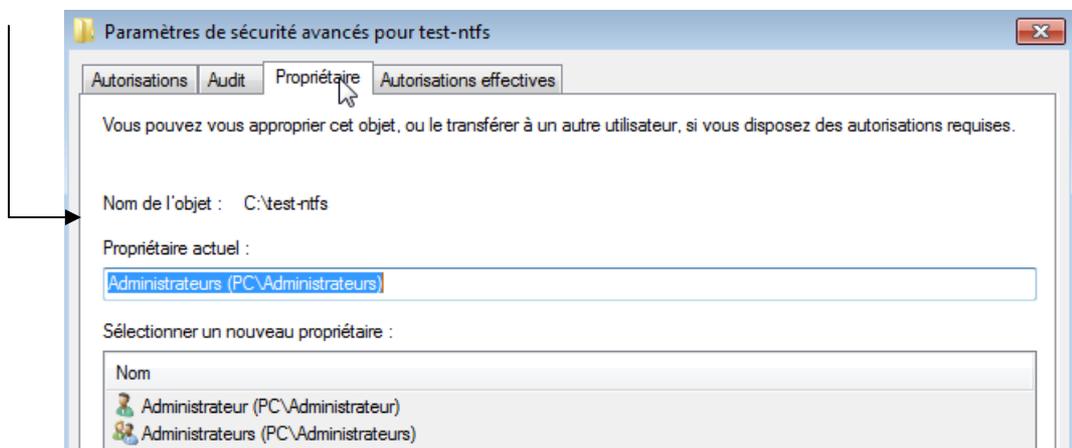
C'est la raison du groupe prédéfini **Créateur Propriétaire**, qui est géré automatiquement par Windows (on ne peut spécifier qui fait partie de ce groupe, ni savoir qui en fait partie... cela dépend de l'objet que l'on pointe !)

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

Un utilisateur peut attribuer la permission "**Appropriation**" aux autres utilisateurs ou groupe en passant pas les autorisations avancées...



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



## Prendre possession des dossiers et fichiers

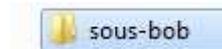
On peut s'approprier un objet :

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

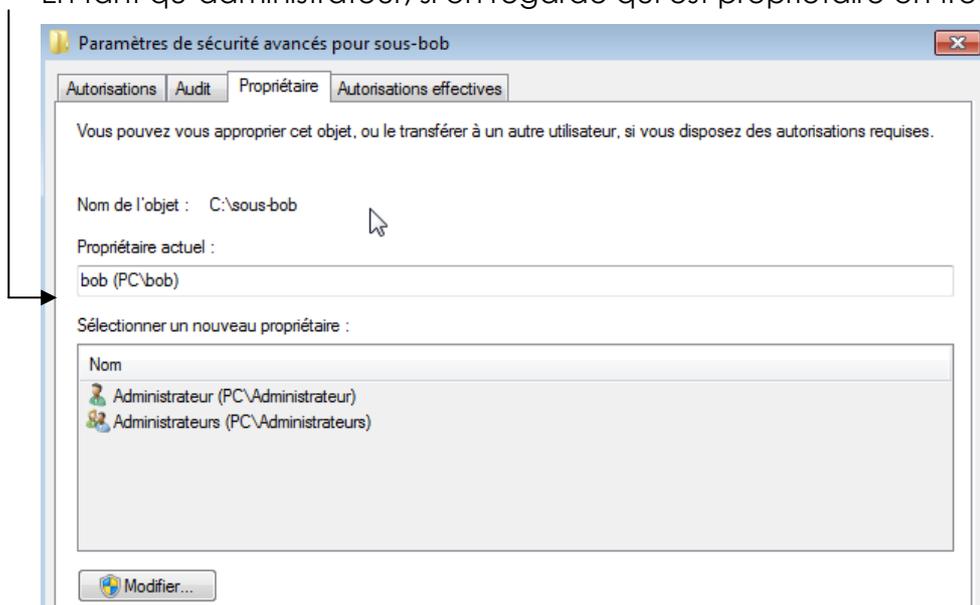
Par défaut les membres du groupe **Administrateurs** ont toujours la possibilité de prendre possession d'un fichier :

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

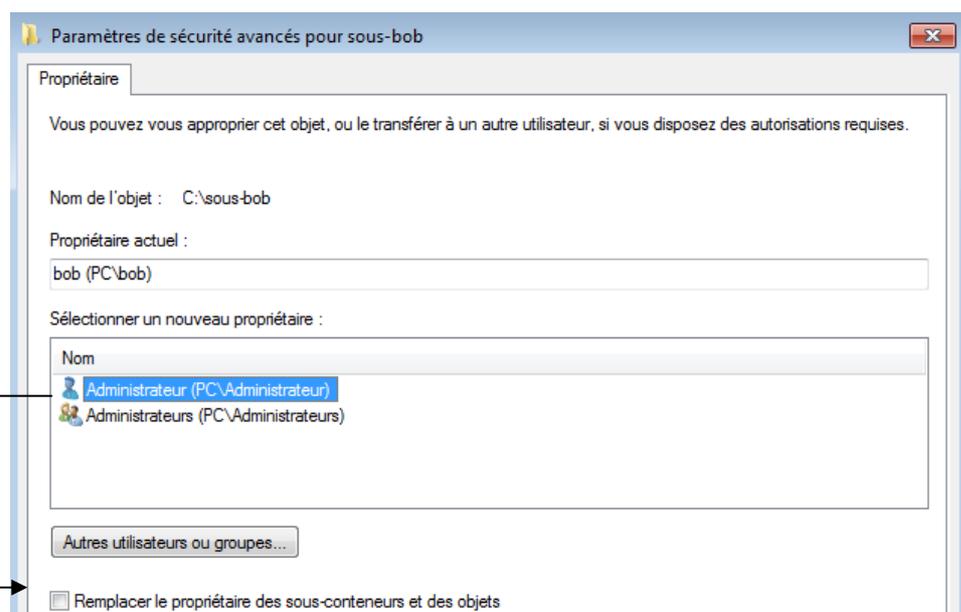
Imaginons que cela soit bob qui ait créé le dossier **sous-bob**



En tant qu'administrateur, si on regarde qui est propriétaire on trouve bob...

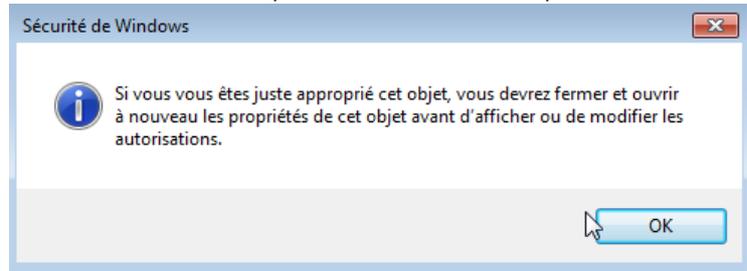


Mais on peut s'approprier l'objet

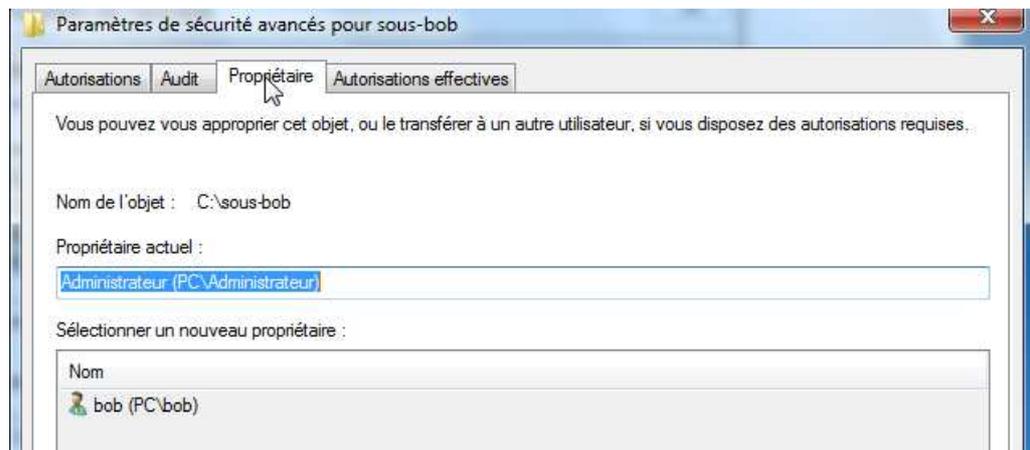


Et éventuellement tout le contenu de l'arborescence...

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



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

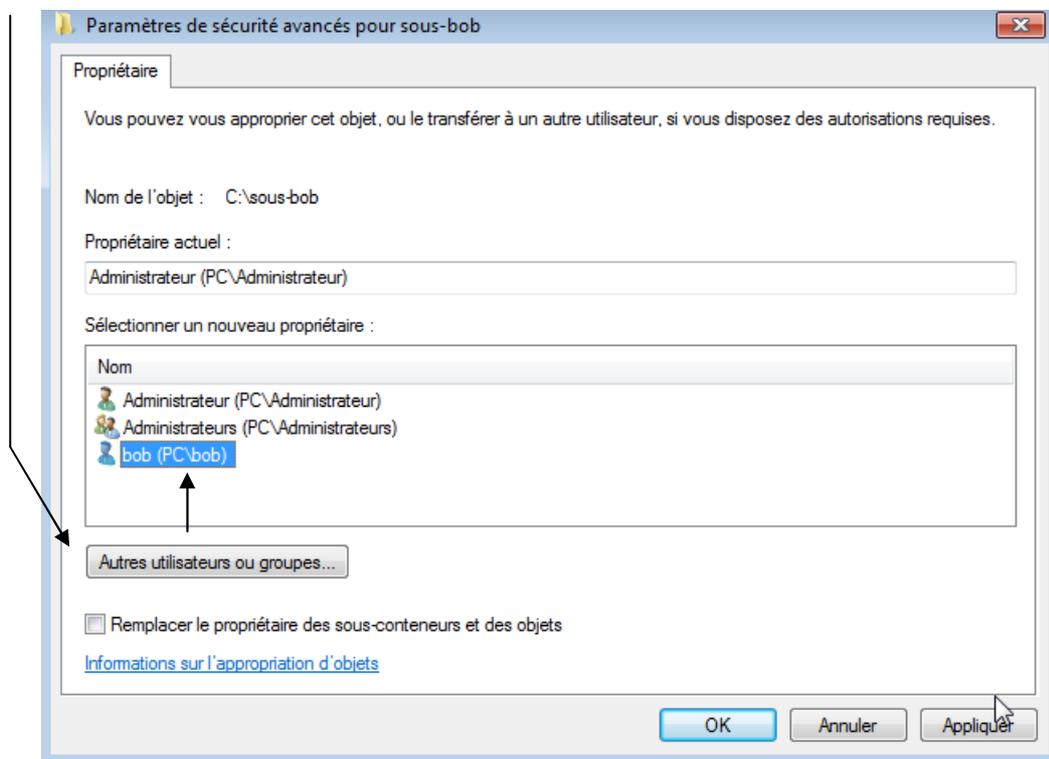


## Donner la possession des dossiers et fichiers

On peut « rendre » la propriété !!!

On fait apparaître bob via **Autres utilisateurs ou groupes...** et le tour est joué

...



---

## Règles "d'affectation" des permissions NTFS:

Deux règles essentielles existent

### Pour les dossiers contenant des programmes

1. Enlever la permission 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 permission contrôle total
3. Pour les utilisateurs, s'ils doivent avoir accès au dossier, donner une permission lecture seule

### Pour les dossiers contenant des données

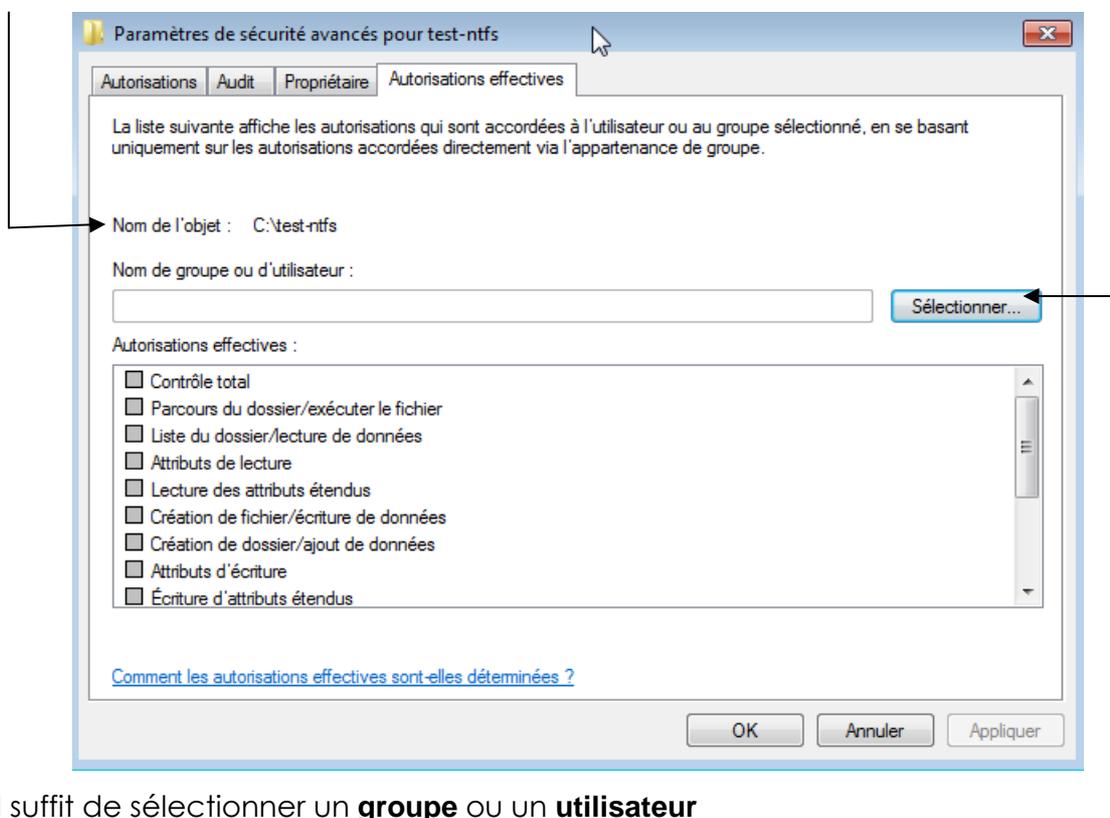
1. Enlever la permission par défaut "Contrôle total" attribuée à tout le monde, et la donner uniquement au Groupe des administrateurs
2. Pour les utilisateurs donner la permission lire et modifier, et au groupe Créateur Propriétaire la permission Contrôle Total. Cela permet aux utilisateurs locaux de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

# VOIR LES AUTORISATIONS EFFECTIVES

## Autorisations effectives :

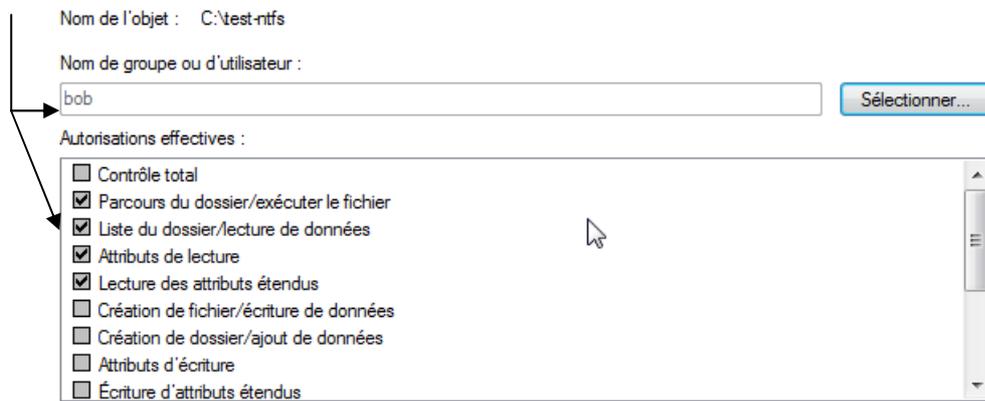
On peut connaître les autorisations qu'un utilisateur ou un groupe possède sur un objet à l'aide des **Autorisations effectives**. On demande pour un dossier 

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



Il suffit de sélectionner un **groupe** ou un **utilisateur**

Pour visualiser clairement ses droits



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

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

## Utilitaire Accesschk

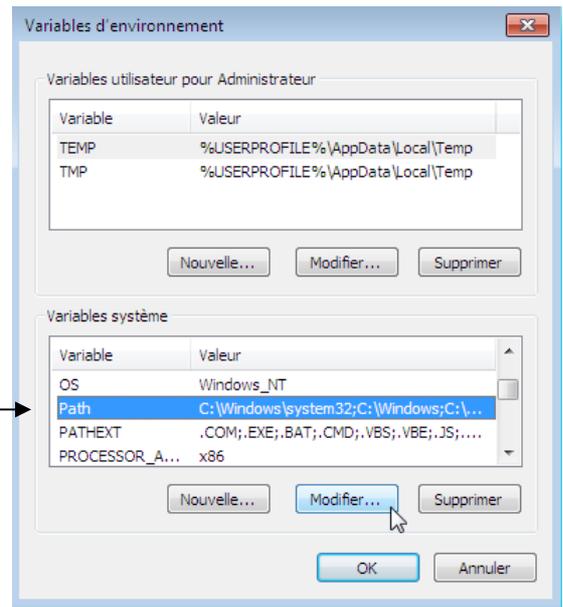
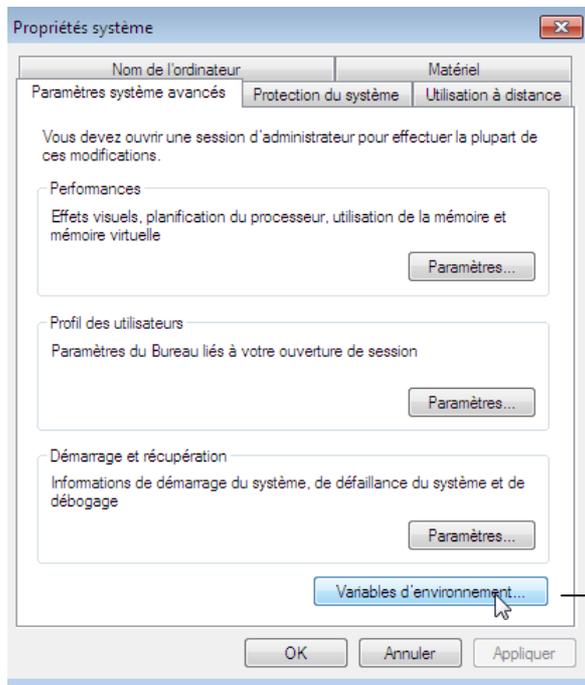


L'utilitaire téléchargé est petit



On peut renommer le fichier, et le copier dans **Windows\system32**,

On peut intégrer son chemin dans le système via les **propriétés** de **ordinateur** onglet **Paramètres système avancés**, puis **Variables d'environnement**



Dans l'exemple l'utilitaire à été renommer en **tst-ntfs.exe**, et donc si la syntaxe complète est lourde, la base est simple

**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

Donc quel accès le groupe des administrateurs sur le dossier windows

```
C:\Users\Administrateur>ntfs "administrateurs" c:\windows\ -d
Accesschk v5.01 - Reports effective permissions for securable objects
Copyright (C) 2006-2010 Mark Russinovich
Sysinternals - www.sysinternals.com
RW c:\Windows
```

Quel accès le groupe des Utilisateurs avec pouvoir a sur le dossier windows

```
C:\Users\Administrateur>ntfs "Utilisateurs avec pouvoir" c:\windows\ -d
Accesschk v5.01 - Reports effective permissions for securable objects
Copyright (C) 2006-2010 Mark Russinovich
Sysinternals - www.sysinternals.com
c:\Windows
```

# 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 créé

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 leurs permissions, avec **XCOPY**

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

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


```

parmis 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:j-m-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. Chaque
chaîne doit être placée sur une ligne dans le fichier.
Lorsque l'une des chaînes est trouvée dans le chemin d'accès
absolu du fichier devant être copié, ce fichier est exclu de la
copie. Par exemple, spécifier une chaîne telle que \obj\
ou .obj exclura respectivement tous les fichiers situés sous
le répertoire obj ou tous les fichiers dont l'extension
est .obj.
/P Confirmer la création de chaque fichier
de destination.
/S Copie les répertoires et sous-répertoires à l'exception des
répertoires vides.
/E Copie les répertoires et sous-répertoires, y compris les
répertoires vides.
Identique à /S /E. Peut être utilisé pour modifier /T.
/U Vérifie la taille de 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, considérer la destination comme devant être
un répertoire.
/Q N'affiche pas les noms de fichiers lors de la copie.
/F Affiche les noms de source et de destination complets lors
de la copie.
/L Affiche les fichiers devant être copié.
/G Permet la copie des fichiers chiffrés vers des destinations qui
ne prennent pas en charge le chiffrement.
/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
incluent les répertoires et sous-répertoires vides.
/U Copie seulement les fichiers existants déjà dans la
destination.
/K Copie les attributs. La commande normale Xcopy rétablira les
attributs de lecture seule.
/N Copie en utilisant les noms courts générés.
/O Copie les fichiers d'appartenance et les informations d'ACL.
/X Copie les paramètres d'audit de fichiers (sous-entend /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.
/B Copie le lien symbolique et non pas la cible du lien.
/J Copie avec E/S sans mémoires tampons. Recommandé pour les gros fichiers.


```

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**



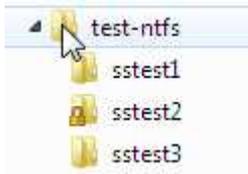
ici **> info.txt** permet de rediriger le flux de la sortie video par défaut dans un fichier nommé **info.txt**

**N.B:** Sous Seven une nouvelle options **/B** permet de copier les liens symboliques (et non pas la cible...)

```
/Z Copie les fichiers du réseau en mode redémarrable.
/B Copie le lien symbolique et non pas la cible du lien.


```

Soit une arborescence de dossier telle que

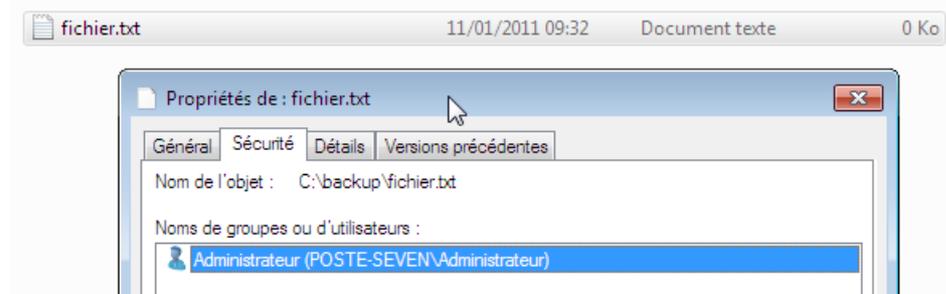


que l'on voudrait sauvegarder sous D:\backup, réservé à l'administrateur...

Si on fait uniquement un **xcopy**...

```
C:\Users\Administrateur>xcopy d:\test-ntfs\*. * c:\backup\*. *
D:\test-ntfs\fichier.txt
1 fichier(s) copié(s)
```

On a bien une copie du fichier, mais uniquement l'administrateur peut le re-lire...



Si on fait uniquement un **xcopy.../O /S** ou **/C/H/O/S/E** c'est mieux... mais pas parfait !

## Sauvegarde de Fichiers

C'est sans doute la solution la plus pratique... dans **Maintenance**, on demande **Sauvegarder et restaurer**

Planification : Aucune. Sélectionnez Sauvegarder maintenant pour lancer une sauvegarde.  
[Activer la planification](#)  
[Modifier les paramètres](#)

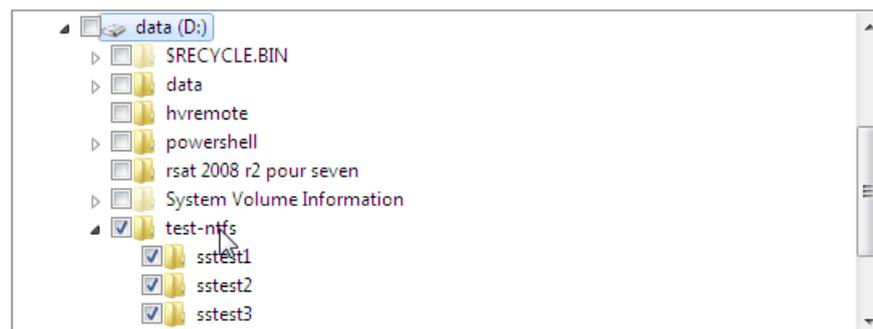
Si au moins une sauvegarde à déjà été faite, on demande **Modifier les paramètres**

On choisit un emplacement de sauvegarde, et on demande de choisir....



Que voulez-vous sauvegarder ?

Activez la case à cocher des éléments à inclure dans la sauvegarde. [Quels fichiers sont exclus par défaut de la sauvegarde ?](#)



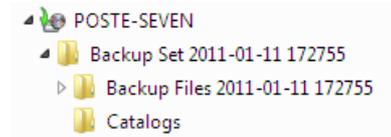
On enregistre les paramètres, et l'on quitte.

Il ne reste plus qu'à exécuter la sauvegarde

## Sauvegarder ou restaurer des fichiers



Sur la cible de destination, une structure est créée



Effectuons la restauration, que nous allons faire dans le dossier **C:\backup** (et non pas le dossier d'origine... pour mieux comparer)

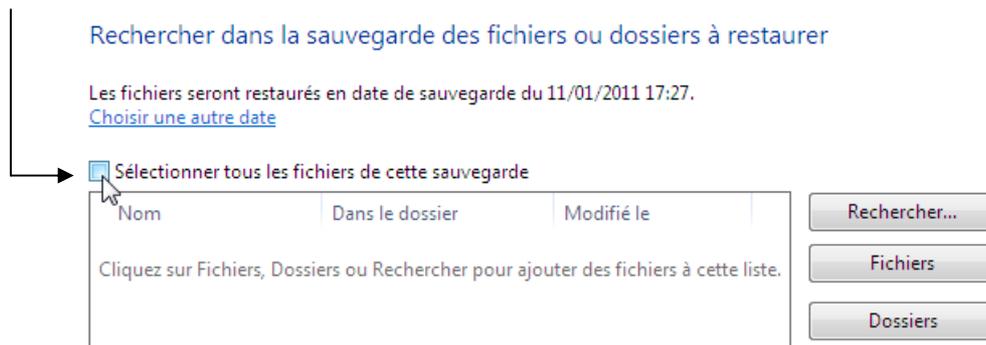


### Sélectionner la sauvegarde à partir de laquelle vous voulez restaurer des fichiers

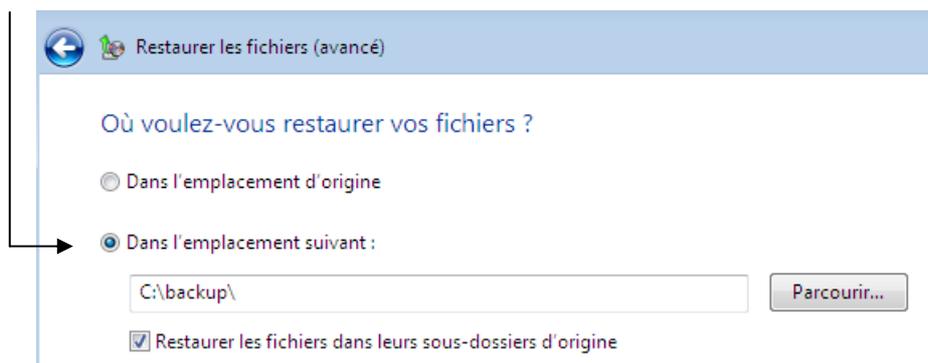
Si l'emplacement de sauvegarde voulu n'est pas répertorié ci-dessous, connectez le périphérique contenant la sauvegarde à cet ordinateur et cliquez sur Actualiser.

Période de sauvegarde	Ordinateur	Emplacement de sauvegarde
De 11/01/2011 à 11/01/2011	POSTE-SEVEN	KINGSTON (F:)

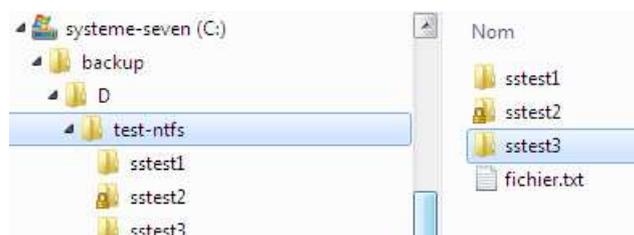
On sélectionne tous les fichiers de la sauvegarde



Et dans notre emplacement "autre", donc C:\backup



C'est parfait ! (et toute la sécurité NTFS est reproduite à l'identique...)



## ROBOCOPY invite de commande

Il est possible de copier les fichiers en gardant leurs permissions, également avec un autre outils **ROBOCOPY** (Une version graphique existe... RICHCOPY)

```
C:\Users\Administrateur\Desktop>robocopy

-----
ROBOCOPY  ::  Copie de fichiers robuste pour Windows
-----

Début : Wed Jan 12 10:43:41 2011

Syntaxe simple :: ROBOCOPY source destination /MIR
                source :: répertoire source (lecteur:\chemin ou \\serveur\partage\chemin).
                destination :: rép. de destination (lecteur:\chemin ou \\serveur\partage\chemin).
                /MIR :: met en miroir une arborescence complète.

Pour plus d'informations sur son utilisation, exécutez ROBOCOPY /?
```

Quelques exemples :

- Pour copier simplement un dossier vers un autre...

```
robocopy C:\test-ntfs C:\backup /E
```

- Pour copier un dossier avec toutes les informations **/COPYALL**, (équivalent à **/COPY:DATSOU**, **D**=Data, **A**=Attributes, **T**=Timestamps, **S**=Security=NTFS ACLs, **O**=Owner info, **U**=aUditing info),

Sans recommencer sur un echec à cause d'un fichier verrouillé **/R:0**

En gardant l'horodatage de départ **/DCOPY:T**

```
robocopy C:\test-ntfs C:\backup /COPYALL /E /R:0 /DCOPY:T
```

```
C:\Users\test\Desktop>robocopy D:\test-ntfs C:\backup /COPYALL /E /R:0 /DCOPY:T

-----
ROBOCOPY  ::  Copie de fichiers robuste pour Windows
-----

Début : Wed Jan 12 11:19:19 2011

Source : D:\test-ntfs\
Dest : C:\backup\

Fichiers : *.*

Options : *.* /S /E /COPYALL /DCOPY:T /R:0 /W:30

-----
100% *Rép. SUPPL. 1 D:\test-ntfs\
Nouveau fichier -1 C:\backup\D\ fichier.txt
Nouveau rép. 0 D:\test-ntfs\sstest1\
Nouveau rép. 0 D:\test-ntfs\sstest2\
100% Nouveau rép. 1 D:\test-ntfs\sstest3\
Nouveau fichier 0 a util.txt

-----
Rép : Total Copié IgnoréDiscordance ÉCHEC Extras
Fichiers : 4 3 1 0 0 1
Octets : 2 2 0 0 0 0
Heures : 0:00:00 0:00:00 0 0 0:00:00 0:00:00

Terminé : Wed Jan 12 11:19:19 2011
```

- Effectuer une copie "miroir", en supprimant de la cible les fichiers plus présent sur l'origine **/MIR** et en mode ré-exécutable si de perte de connexion réseau **/Z**

```
robocopy C:\test-ntfs \\serveur\backup /MIR /Z
```

**N.B:** Sous Seven des options **/XJ** permet d'ignorer les liens symboliques (on ne peut pas de copier des liens symboliques sur des dossiers)

# LIENS SYMBOLIQUES

## Liens Symboliques - Raccourcis:

Différence entre liens symboliques et raccourcis:

- Un **Raccourci** est une redirection au niveau du système d'exploitation, SEVEN. C'est un fichier avec une extension **.lnk**
- Un **Lien symbolique** est une redirection au niveau du système de fichier, NTFS . Ce n'est pas un fichier, Il n'a pas de poids, il est stocké dans l'index du système de fichier du disque.

**N.B:** on peut lister les liens avec **dir /a** ou mieux **dir /al**

```
C:\Users\admin>dir /al
Le volume dans le lecteur C s'appelle systeme-seven
Le numéro de série du volume est F8F5-FEF5

Répertoire de C:\Users\admin
10/12/2010 12:09 <JUNCTION> Application Data [C:\Users\admin\AppData\Roaming]
10/12/2010 12:09 <JUNCTION> Cookies [C:\Users\admin\AppData\Roaming\Microsoft\Windows\Cookies]
10/12/2010 12:09 <JUNCTION> Local Settings [C:\Users\admin\AppData\Local]
```

Le lien garde les propriétés du dossier-fichier vers lequel il pointe, ce n'est pas fichier **xxx.lnk**. Ce lien se comporte comme le dossier-fichier "original".

En effet dans les propriétés d'un "raccourci" est-ce utile de savoir que c'est un fichier lnk de 800 octets ?, alors qu'avec un lien symbolique, nous pourrions savoir combien pèse le dossier cible, gérer son partage, ses accès... exactement comme si vous regardiez les propriétés du vrai dossier.

Par exemple si certains dossiers sont perdus dans l'arborescence complexe de votre système et on veut les gérer depuis le bureau, il vous suffira de créer des liens symboliques sur le bureau avec ces dossiers.

Un lien symbolique ou simlink (ou simlinkD), c'est donc un alias avec le dossier/fichier sur lequel on se lie...

Si on supprime le lien symbolique, le dossier/fichier n'est pas supprimé.

## Liens Symboliques – mklink :

La commande **mklink** crée des liens symboliques vers dossier ou fichier

```
C:\Users\admin>mklink /?
Crée un lien symbolique.

MKLINK [[/D] | [/H] | [/J]] Lien Cible

/D      Crée un lien symbolique vers un répertoire. Par défaut,
        il s'agit d'un lien symbolique vers un fichier.
/H      Crée un lien réel à la place d'un lien symbolique.
/J      Crée une jonction de répertoires.
Lien    Spécifie le nom du nouveau lien symbolique.
Cible   Spécifie le chemin d'accès <relatif ou absolu> auquel
        le nouveau lien fait référence.
```

**mklink /D** crée un Lien Symbolique vers un dossier - répertoire

**mklink** sans commutateur crée un Lien Symbolique vers un fichier....

Donc dans la commande **mklink /D lien cible**

"lien" = Si le chemin du lien est absolu (c:\un-dossier\un-sous-dossier\cible) le lien symbolique est dit absolu. Il est placé là où on l'a indiqué.

"lien" = Si le chemin du lien donné est relatif (\un-dossier\un-sous-dossier\cible) le chemin est dit relatif. Il est placé là où l'on se trouve au moment où l'on tape la commande mklink

- "lien" absolu

Soit un dossier **c:\data**, pour lequel on voudrait avoir un lien symbolique direct nommé **direct**...dans le disque c: ... avec la commande

**mklink /D c:\direct c:\data**

```
C:\>mklink /D c:\direct c:\data
Lien symbolique créé pour c:\direct <<===>> c:\data
```

Donnant

```
C:\>dir
Le volume dans le lecteur C s'appelle systeme-seven
Le numéro de série du volume est F8F5-FEF5

Répertoire de C:\
10/06/2009  22:42                24 autoexec.bat
11/01/2011  17:34                <REP>         backup
10/06/2009  22:42                10 config.sys
12/01/2011  08:50                <REP>         data
12/01/2011  08:52                <SYMLINKD>    direct [c:\data]
14/07/2009  03:37                <REP>         PerfLogs
06/01/2011  09:26                <REP>         Program Files
06/01/2011  10:16                <REP>         Users
03/12/2010  13:09                <REP>         utilitaires
12/01/2011  07:35                <REP>         Windows
                2 fichier(s)                34 octets
```

Dans l'explorateur cela apparaît ainsi

direct	12/01/2011 08:52	Dossier de fichiers
data	12/01/2011 08:50	Dossier de fichiers

Que l'on effacera via **RD direct**...

On sait maintenant se créer un lien symbolique sur n'importe quel dossier, n'importe où... **d**: étant un lecteur externe, réseau...

**mklink /D c:\direct d:\data**

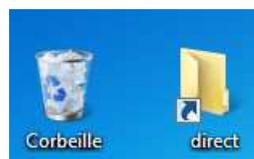
- "lien" = relatif

On se place sur le bureau du compte administrateur, on crée le lien symbolique suivant :

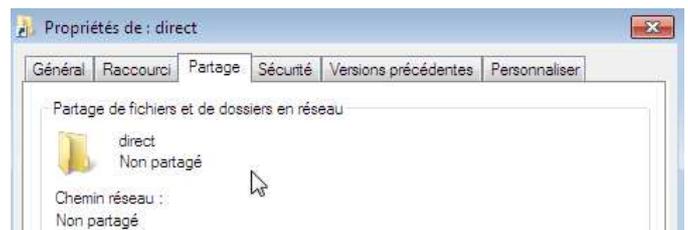
**mklink /D direct c:\data**

```
C:\Users\Administrateur\Desktop>mklink /D direct c:\data
Lien symbolique créé pour direct <<===>> c:\data
```

On obtient sur le bureau



et les propriétés sont bien celles d'un dossier...



**N.B.**: effacer le lien symbolique n'efface pas le dossier physique "data"

On peut créer le même lien symbolique sur une cible en relatif

### Mklink /D direct \data

```
C:\Users\Administrateur\Desktop>mklink /D direct2 \data
Lien symbolique créé pour direct2 <<===>> \data
```

On obtient

```
Répertoire de C:\Users\Administrateur\Desktop
15/03/2010  07:21    <REP>          .
15/03/2010  07:21    <REP>          ..
14/03/2010  12:48    <REP>          autre
14/03/2010  12:39    <SYMLINKD>     direct [c:\data]
15/03/2010  07:21    <SYMLINKD>     direct2 [..\data]
```

### Copie de Liens Symboliques:

Il faut faire attention aux outils que l'on emploie, car par défaut lorsque l'on copie un lien symbolique, ce n'est pas le lien qui est copié mais sa cible !

Vérifions :

1. Soit un lien symbolique "**stock**" pointant sur un dossier **C:\stock** (contenant des fichiers et des dossiers) et posé sur le bureau de l'administrateur...

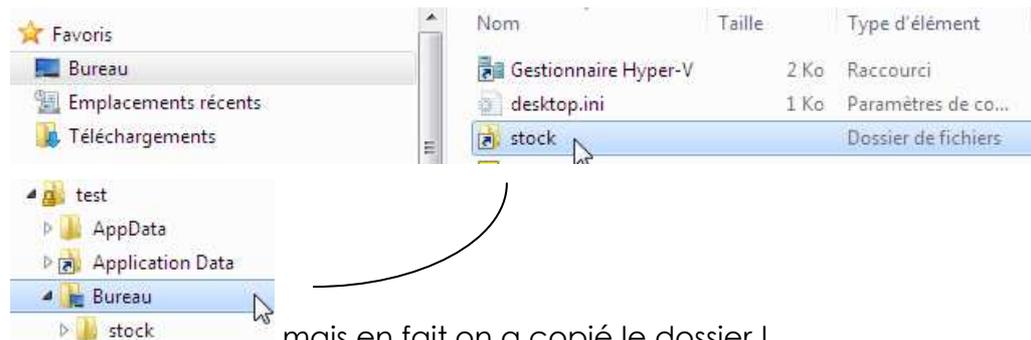
```
C:\Users\Administrateur\Desktop>mklink /D stock c:\stock
Lien symbolique créé pour stock <<===>> c:\stock
```



Sur le bureau de l'administrateur on a bien l'icône stock...

2. On souhaite copier ce lien pour un utilisateur "**Test**" existant ...

On peut le faire par l'explorateur ...



On peut s'en rendre compte si on regarde de près l'icône, (pas de flèche...) ou par la commande **dir /al** sur le dossier...

```
C:\Users\test\Desktop>dir /al
Le volume dans le lecteur C s'appelle systeme-seven
Le numéro de série du volume est F8F5-FEF5

Répertoire de C:\Users\test\Desktop
Fichier introuvable
```

Donc si util "travaille" dans son dossier stock, ce n'est pas le même que celui utilisé par l'administrateur.

Pour copier un lien il faut utiliser des commandes en ligne, telles que **XCOPY**, avec comme option **/B...** ou avec **ROBOCOPY**, avec comme option **/XJ...**

3. On souhaite copier ce lien pour un utilisateur "Test" existant ...

```
XCOPY stock ..\..\test\desktop\stock /B
```

Et répondre R

```
C:\Users\Administrateur\Desktop>xcopy stock ..\..\test\desktop\stock /B
Est-ce que ..\..\test\desktop\stock désigne un nom de fichier
ou un nom de répertoire de la destination
(F = fichier, R = répertoire) ? r
0 fichier(s) copié(s)
```

On peut aussi taper la commande... (pour éviter la réponse...)

```
XCOPY stock\*.* ..\..\test\desktop\stock\*.* /B
```

```
C:\Users\Administrateur\Desktop>xcopy stock\*.* ..\..\test\desktop\stock\*.* /B
0 fichier(s) copié(s)
```

On peut s'en rendre compte si on regarde de près l'icône, (présence de la flèche...) ou par la commande **dir /al** sur le dossier...

Nom

stock  
desktop.ini

```
C:\Users\test\Desktop>dir /al
Le volume dans le lecteur C s'appelle systeme-seven
Le numéro de série du volume est F8F5-FEF5

Répertoire de C:\Users\test\Desktop

12/01/2011 10:56 <SYMLINKD> stock [c:\stock]
0 fichier(s) 0 octets
1 Rép(s) 28 343 021 568 octets libres
```

## Jonctions de répertoire – Jonction:

commande **mklink**

Jonction de répertoire (uniquement) avec des chemins absolus

**Mklink /J** crée une jonction de répertoire (chemin absolu)

**N.B:** Les jonctions de répertoire font "double emploi" avec les liens symboliques, (pour des raisons de compatibilité). Elles ne peuvent être donnée que avec des chemins absolus ! Donc

**Mklink /J autre c:\ c:\data**

```
C:\Users\Administrateur\Desktop>mklink /J autre c:\data
Jonction créée pour autre <<==>> c:\data
```

On obtient

```
C:\Users\Administrateur\Desktop>dir
Le volume dans le lecteur C n'a pas de nom.
Le numéro de série du volume est F2F4-F37C

Répertoire de C:\Users\Administrateur\Desktop

14/03/2010 12:50 <REP> -
14/03/2010 12:50 <REP> ..
14/03/2010 12:50 <JUNCTION> autre [c:\data]
14/03/2010 12:39 <SYMLINKD> direct [c:\data]
```



C'est-à-dire

## Liens Symboliques - Réels sur fichiers :

Différence entre liens symboliques et liens réels:

- Un **Raccourci** est une redirection au niveau du système d'exploitation, SEVEN. C'est un fichier avec une extension **.lnk**
- Un **Lien symbolique** est une redirection au niveau du système de fichier NTFS. Ce n'est pas un fichier, il n'a pas de poids, il est stocké dans l'index du système de fichier du disque.

Il apparaît comme un raccourci graphiquement, lorsqu'on le supprime, le fichier pointé n'est pas supprimé. Un lien symbolique peut "pointer" du vide si le dossier est effacé.

- Un **Lien réel** est une autre entrée au niveau du système de fichier NTFS. Ce n'est pas un fichier, il n'a pas de poids, il est stocké dans l'index du système de fichier du disque.

Il apparaît comme le fichier d'origine, (duplicata) Ce n'est que lorsqu'on supprime tous les liens réels que le fichier est supprimé.

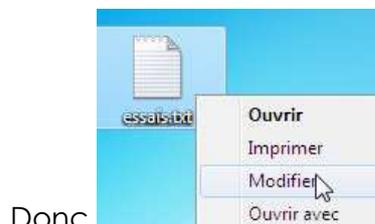
Soit un fichier **texte.txt** stocké en **c:\data...**



On peut rendre ce fichier "accessible" sur le bureau via

**Mklink /H essais.txt c:\data\essais.txt**

```
C:\Users\Administrateur\Desktop>mklink /H essais.txt c:\data\essais.txt
Liaison permanente créée pour essais.txt <==> c:\data\essais.txt
```



Donc

On peut le "supprimer" dans c:\data.... Il restera utilisable via le bureau !

```
C:\Users\Administrateur\Desktop>fsutil hardlink create
Syntaxe : fsutil hardlink create <nouveau nom de fichier> <nom de fichier
          existant>
Par ex. : fsutil hardlink create c:\foo.txt c:\bar.txt
```

**N.B:** une commande Fsutil existe également

**N.B:** sur les fichiers word, excel, le fonctionnement est assez aléatoire !

```
C:\Users\Administrateur\Desktop>fsutil hardlink create new.txt c:\data\new.txt
Liaison permanente créée pour C:\Users\Administrateur\Desktop\new.txt <==> c:\data\new.txt
```

```
C:\Users\Administrateur\Desktop>fsutil hardlink create new.doc c:\data\new.doc
Liaison permanente créée pour C:\Users\Administrateur\Desktop\new.doc <==> c:\data\new.doc
```

# TP DROITS NTFS 1°

## Objectif :

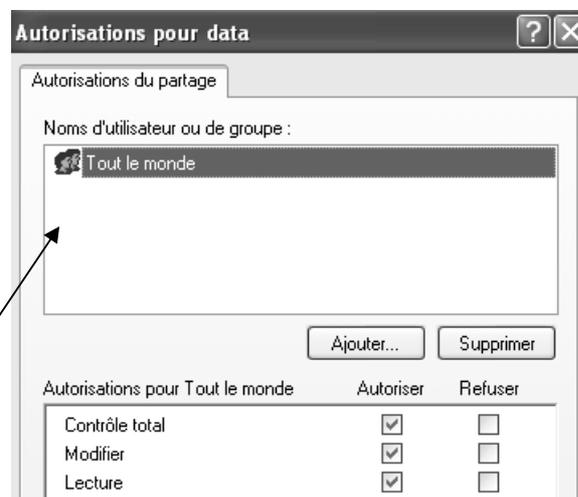
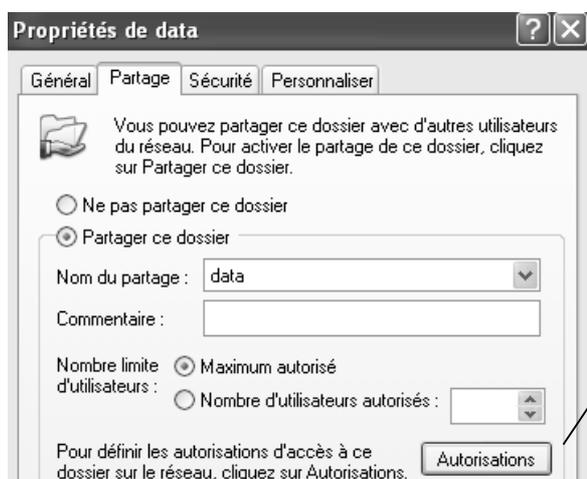


Faire que chaque utilisateur , andre, bertrand...puisse "tout faire chez lui", sauf détruire son répertoire de base( ici homonyme) !

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 !)

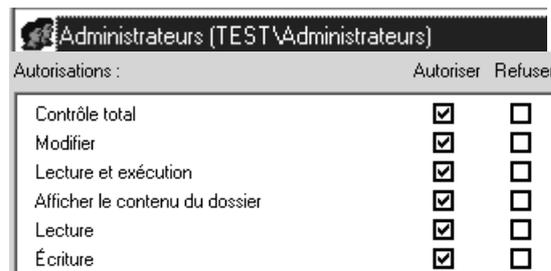
## Permissions de sécurité :

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

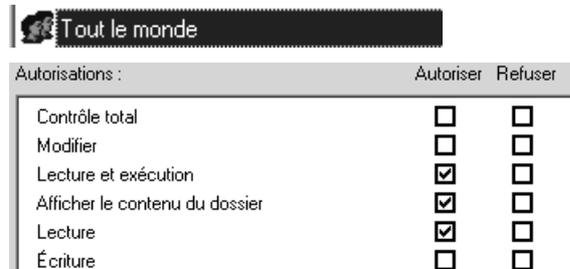
Ensuite on pose

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

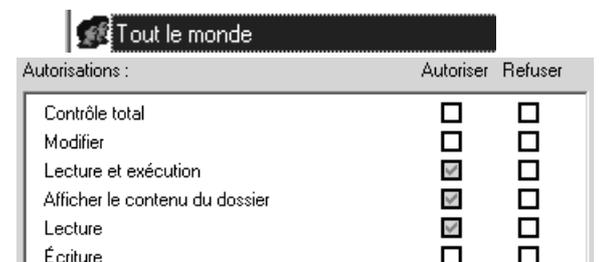
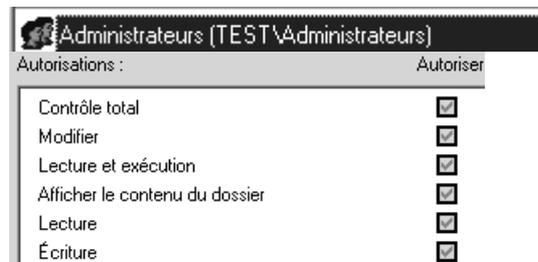
on a donc



et



sur le dossier de **andre**, et **bertrand** donc, par défaut les permissions de sécurité sont celles **héritées** 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

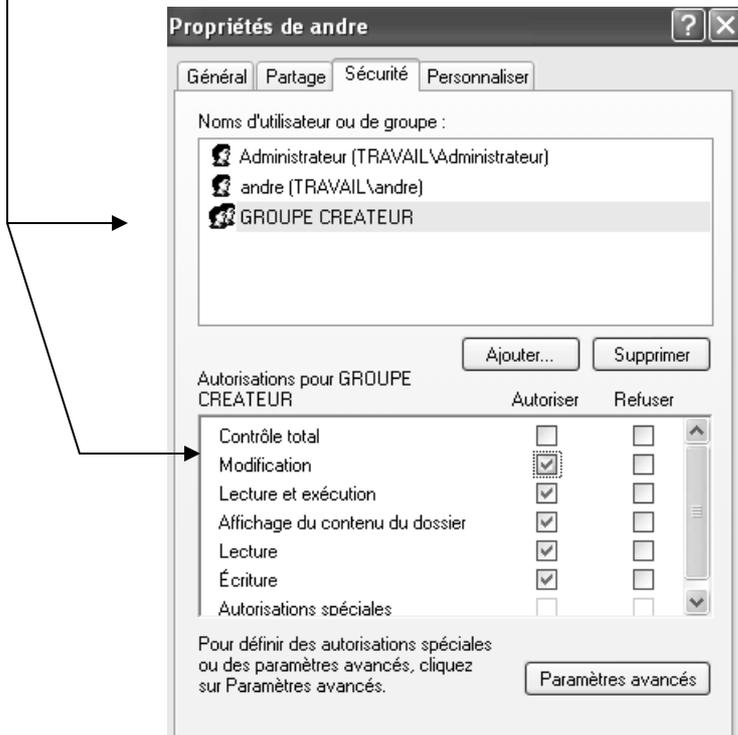
---

### 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 à :

- 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....

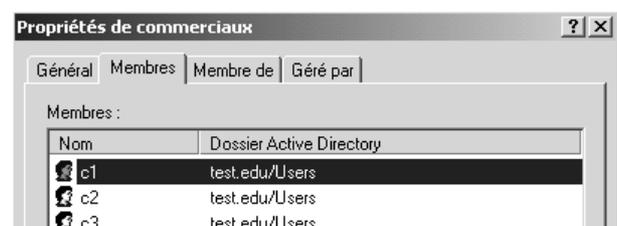
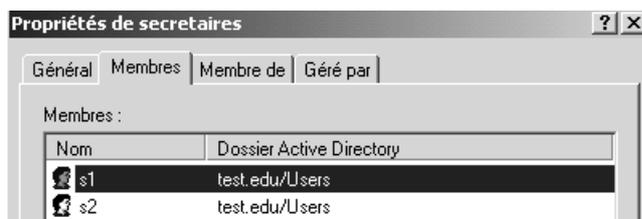
De manière analogue, les **secrétaires** peuvent avoir accès à :

- 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 :

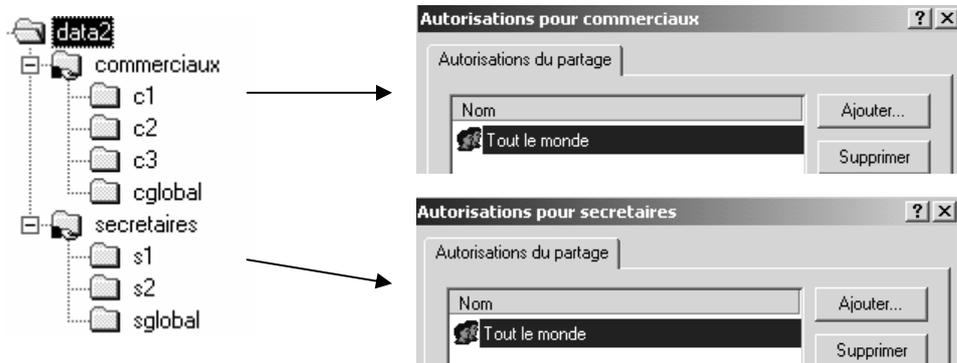
il faut créer un groupe global des secrétaires et y rentrer les utilisateurs appropriés (s1,s2...), et un groupe global des commerciaux, et y rentrer les utilisateurs appropriés (c1, c2...).

 secretaire	Groupe de sécurité - Global
 commerciaux	Groupe de sécurité - Global
 s1	Utilisateur
 s2	Utilisateur
 c1	Utilisateur
 c2	Utilisateur
 c3	Utilisateur



## Partages :

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

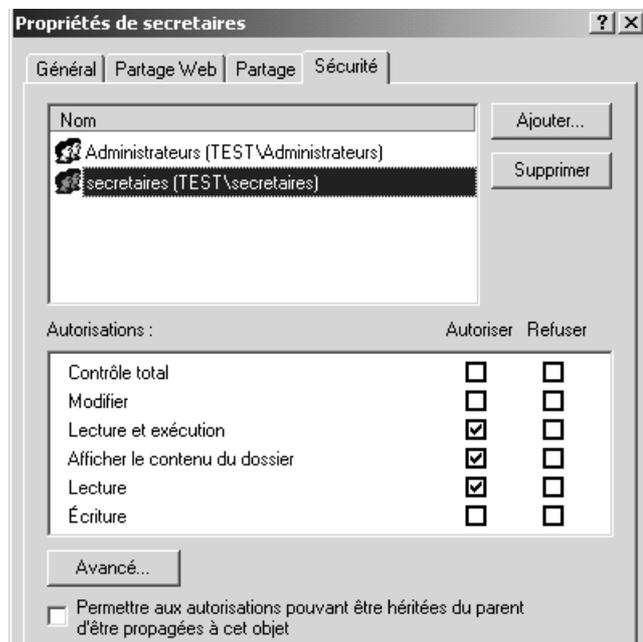


**N.B:** on pourrait décider de ne faire qu'un seul partage

## Permissions NTFS :

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

puis donner au **Administrateur** une permission **contrôle total**, et au groupe des **secrétaires** 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 forcément 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 !

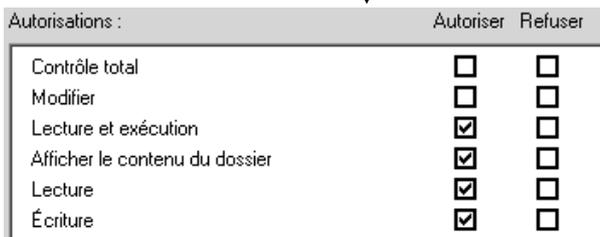
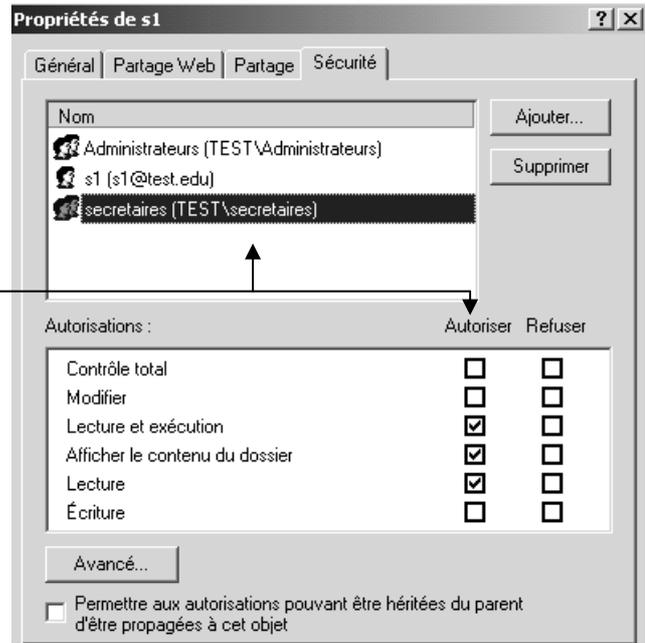
Pur chaque dossier individuel, **S1 S2** etc il faut autoriser l'utilisateur **S1** à **créer** chez lui, (mais pas **modifier**, sinon il pourrait supprimer son propre dossier) et les **administrateurs** en **contrôle total**

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

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

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

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



Pour le dossier **sglobal** il faut

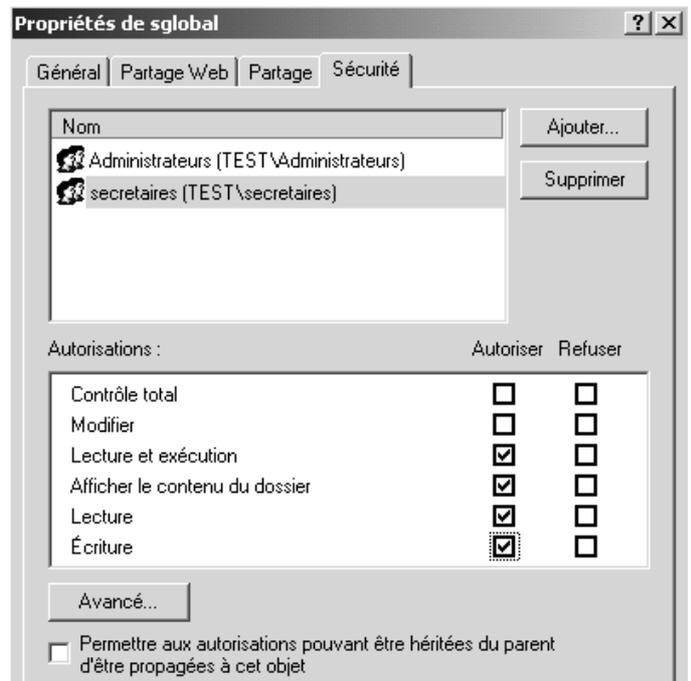
autoriser chaque secrétaire à pouvoir  
y écrire, ainsi que l'administrateur

on supprime l'héritage

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

et le groupe **secrétaires**

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



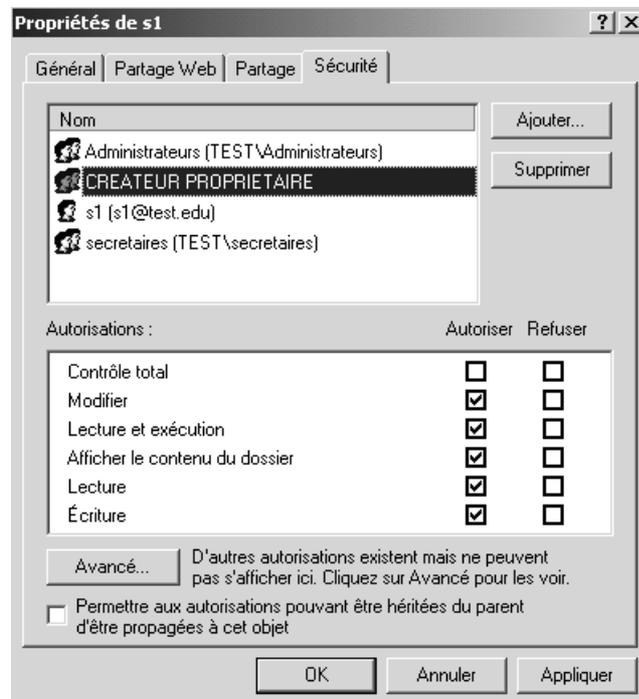
## Créateur propriétaire :

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 **sglobal**, mais ne peut que lire chez **s1**

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

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 créée) mais elle le videra de tout le contenu dont elle est le propriétaire...

# TP APPROPRIATION DE FICHER

## Descriptif du problème :



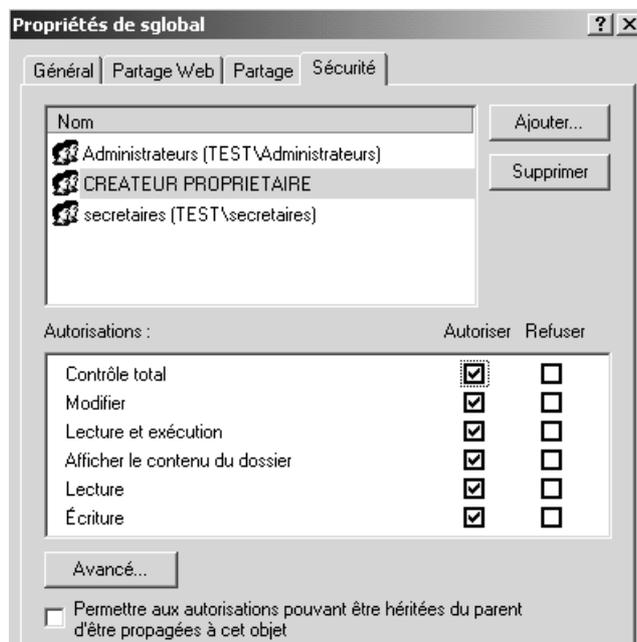
Imaginons un ensemble de secrétaires ayant chacune un espace propre réservé nommé **s1**, **s2** etc et disposant d'un espace commun à toutes nommé **sglobal** (pour secrétaire global)

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

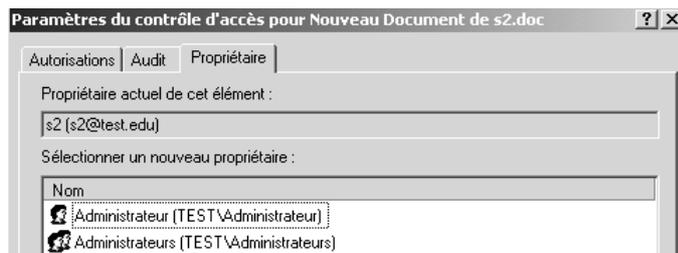
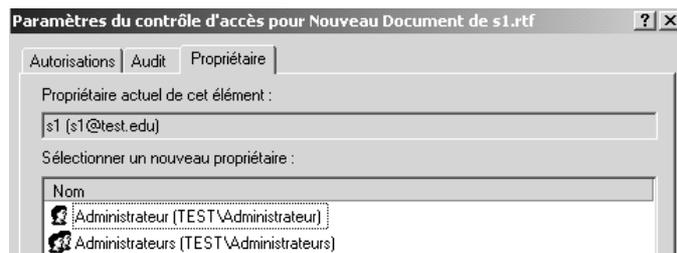
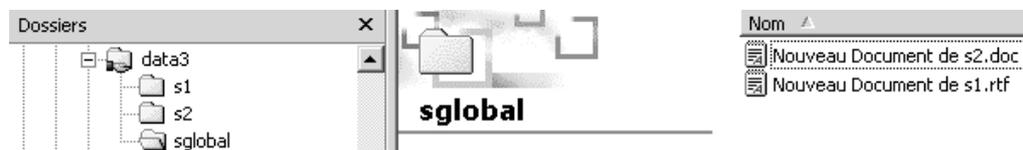
**Administrateur en Contrôle total**

**Créateur propriétaire en contrôle total**

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

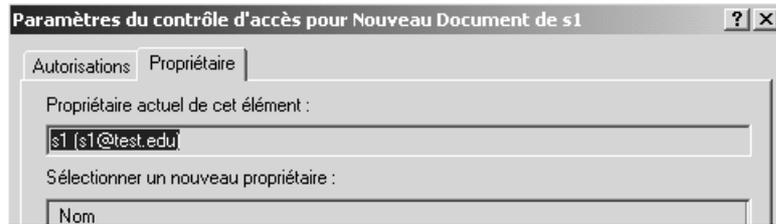


on peut donc arriver à ce que dans ce dossier, il y ait des documents de divers propriétaires...



**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 :

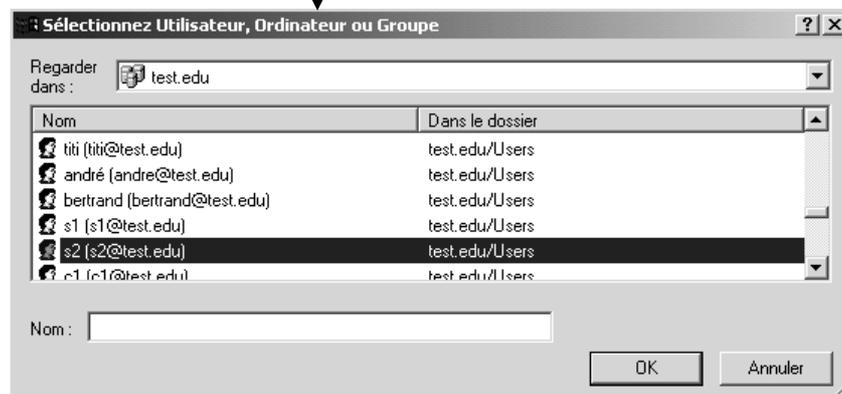
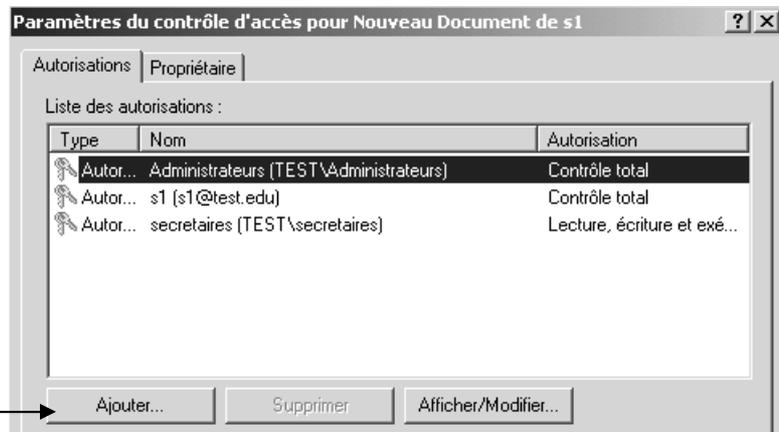
Pour que **s2** puisse s'approprier le document...(depuis un poste NT...) **s1** doit donner à **s2** la permission voulue, voire la permission de prendre possession de ce fichier...:

**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,

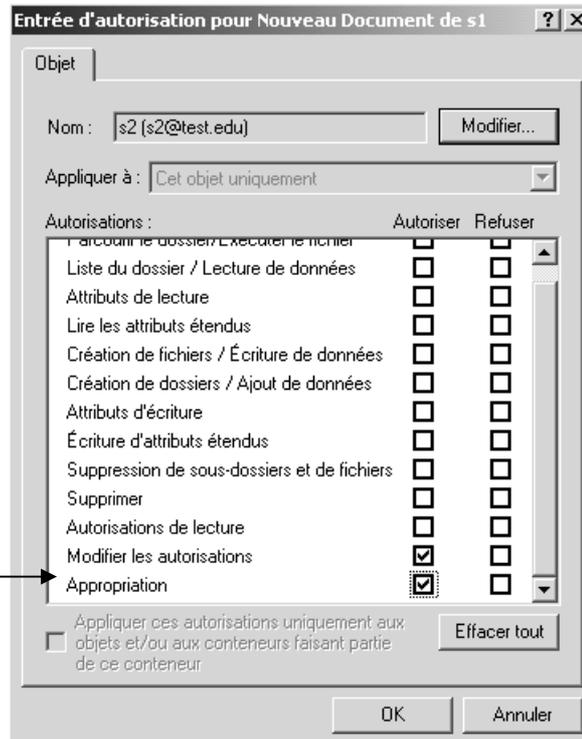
dans **permissions - sécurité - avancées -**

on demande **Ajouter**

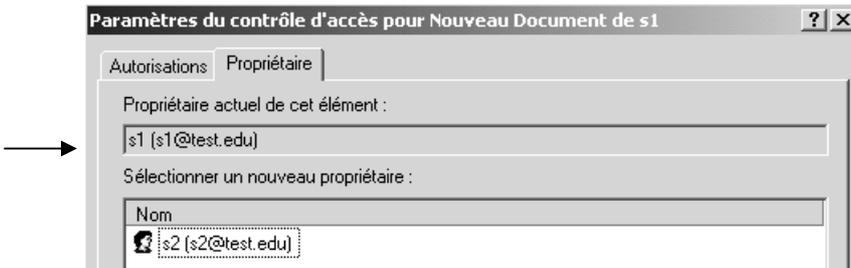


sélectionner **s2** puis valider

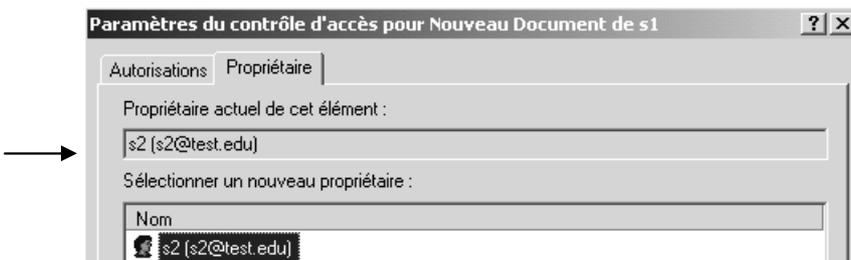
**NB:** il faut ici  
cocher au  
minimum  
**modifier** et  
**appropriation**,



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...

# RICHCOPY

## Installer RichCopy 4.0 :

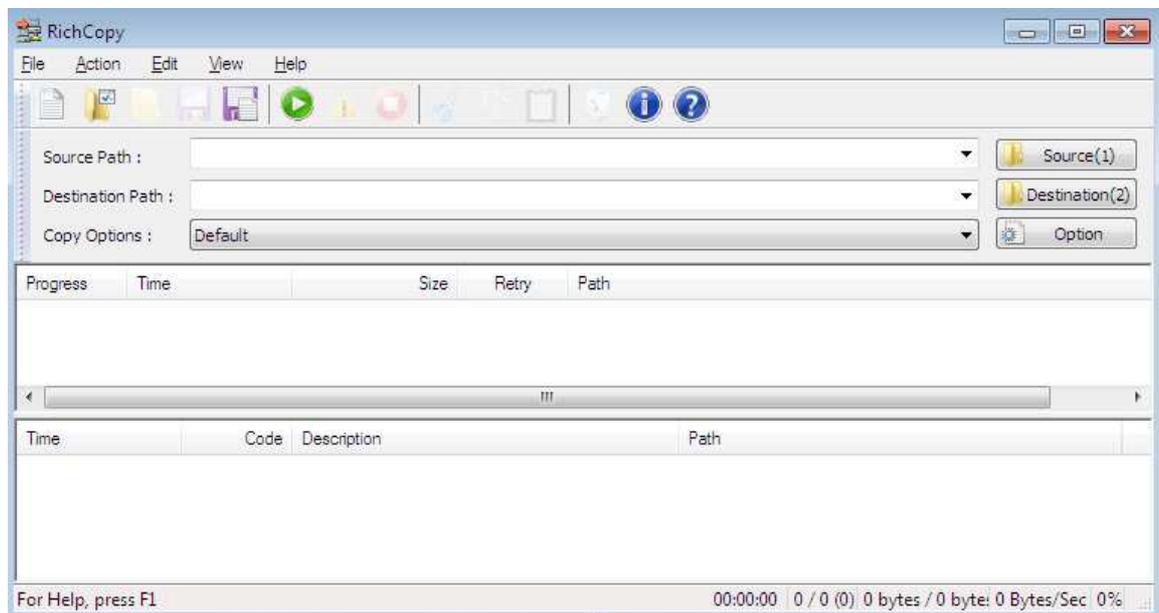
Une fois récupérer le paquetage, il faut le désarchiver

 EULA.doc	02/12/2002 14:59
 readme.txt	18/05/2009 12:40
 RichCopy.chm	20/05/2009 21:17
 RichCopySetup.msi	11/06/2009 01:32
 setup.exe	11/06/2009 01:32

L'installation est basique, et elle occupe 16 Mo



Le lancement donne ensuite

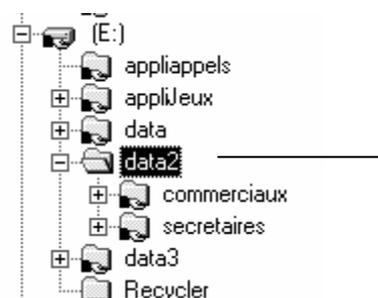


# TP COPIE FICHIER – PERMISSIONS (XP)

## Objectif :

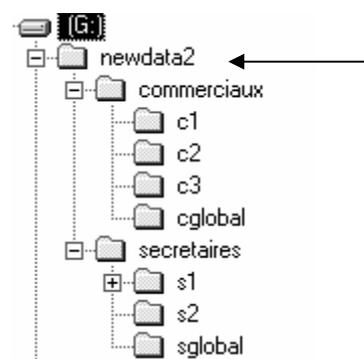
Lorsque l'on copie des fichiers, sur un volume NTFS, on sait que les permissions obtenues sur les fichiers "copiés" sont celles "héritées" des dossiers de destination...

Soit ainsi l'arborescence **data2** donnée suivante située sur le disque E: avec un certain nombre de permissions NTFS posées, et que l'on souhaiterait transférer pour des raisons 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 commande 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**